産業データの国際データガバナンス[1]に関するマニュアル（仮称）（案）

1206 時点版



[1] （本マニュアルの当該単語については、今後公表される「データガバナンス・ガイドライン」（デジタル庁）や国際データガバナンス検討会の議論を踏まえ調整。）

# 1　はじめに

## 1.1　背景と目的

- IoT や DX の普及、サプライチェーン透明化の要請等を背景に、企業における国際的なデータ共有・利活用の動きが拡大している。また、EU の GAIA-X 等をはじめ、産業横断でのデータプラットフォーム・基盤構築の動きも加速しており、我が国でも企業や業界、国境を越えたデータ連携を実現する取組である「ウラノス・エコシステム」が推進されている。
- 国際的なデータ共有・利活用の拡大と同時に、各国・地域においてデータに関する法制の整備も進められている。中には企業が保有する産業データを対象に、データの越境移転の制限や、政府に対する強制的な開示などを課すような規則[2]も存在し、こうした動きが加速していく可能性がある。
- こうした規制は、企業活動における制約要因になることに加えて、中長期的に産業全体での競争力の強化及び企業横断でのデジタル技術・基盤の確立・普及にも影響を及ぼすことも懸念される。
- こうした背景から、各国・地域における産業データのルール形成の動きを踏まえ、これまで個人情報保護の観点から議論が積み重ねられてきた「個人データ」以外のデータにも焦点を当て、現状の把握と対応の在り方を議論する必要性及び有用性が高まっている。
- これを受け、企業における安全・安心な形でのデータ共有・利活用を実現し、付加価値の創出を促進するため、企業における産業データの国際流通・越境に係るデータ管理と共有・利活用（以下「国際データガバナンス」という。）の指針となるマニュアル（以下「本マニュアル」という。）を作成する。
- 本マニュアルを通じ、企業が、国際的なデータ共有・利活用における主要な留意点・リスクを把握するだけでなく、データ共有・利活用を通じた事業価値創造・競争力強化に向けた適切な国際データガバナンスの考え方・プロセスの理解を深めることを目指す。加えて、個別企業におけるデータ共有・利活用の促進を通じて、中長期的な産業競争力・基盤確立にも寄与することを狙う。

## 1.2　想定読者と留意点

- 本マニュアルは、製造業や IT サービス業を含む幅広い産業を対象に、企業の事業部門における実務担当者・企画者及びリスク・コンプライアンス部門、法務部門、データマネジメント部門の担当者等を、主要な読者と想定する。
- 産業データに関する議論は未だ体系的な検討が十分蓄積されておらず、また国際データガバナンスに焦点を当てた議論も新しい検討領域となる。本マニュアルは、議論の網羅性を担保するものではなく、まずは国際データガバナンスの考え方の方向性を示すとともに、いくつかの具体例の提示を通じて、適切な情報提供を目指す。
    - 本マニュアル 4.3「主要なリスクと打ち手の詳細」に具体例を記載する。これらは、4.2「主要な関連法規制 (EU・中国・米国) 」を念頭に、想定される代表的なリスクと打ち手として

[2] 本マニュアル 4.2「主要な関連法規制 (EU・中国・米国) 」参照

記載しているものであり、企業や業務の置かれている状況によって必ずしも一律に適応されるものではない。

- 本マニュアルは、法令のように厳密な規定・義務を定めるものではなく、企業・産業横断的な共通認識の形成を促すものであり、留意点・リスク及び対応の方向性を取りまとめたものである。

## 2　検討の前提と考え方

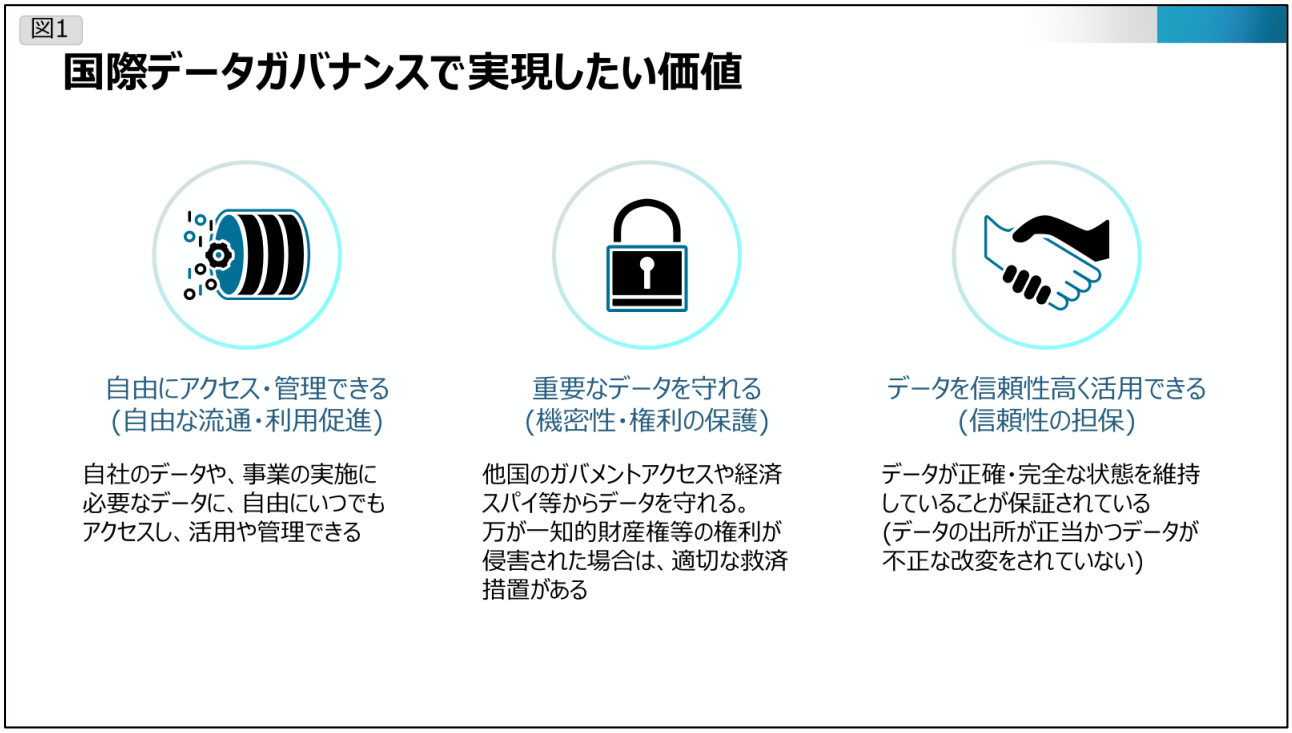
### 2.1　検討の範囲・スコープ

- 本マニュアルは、国際データガバナンスとして、データの越境及び国際的にデータが共有・利活用される場面に焦点を当てる。
  - 国内・海外等で生成されたデータが海外・第三国等に移転・越境する場面に加えて、必ずしも越境しなくとも海外で生成されたデータが同じ域内・国で共有・利活用される場面も対象に含むものとする。
- 企業におけるデータ共有・利活用は、その性質上、広範な企業活動をスコープに含め得る。対象となる範囲・スコープの明確化のため、３つの視点「実現したい価値」、「対象となるプロセス」、「対象となるデータ」から、本マニュアルにおける範囲・スコープを定義する。
- 「実現したい価値」（図１）に関して、我が国では、国際的に「DFFT(Data Free Flow with Trust：信頼性のある自由なデータ流通)」の理念を打ち出している。DFFT は、「プライバシーやセキュリティ、知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す」というコンセプトである[3]。
  - DFFT の理念に基づき、本マニュアルでは「自由な流通・利用促進」、「機密性・権利の保護」、「信頼性の担保」を実現したい価値と捉える。
  - その裏返しとして、「他国・地域に保管しているデータに自由にアクセス・管理できない」、「重要なデータ(機密性・権利)が守れない」、「データが信頼できない」ことを、主要なリスクと定義する。
- 「対象となるプロセス」（図 2）に関して、データライフサイクルの全体に対して、「データが国際的に共有・利活用される場面」を対象とする。
  - データライフサイクルは、データの「生成・取得」、「加工・利用」、「移転・提供」、「保管」、「廃棄」の過程・ステージを指す。なお、「廃棄」には、データの削除だけでなく、データをインアクティブにする・見えなくすることも含まれる。
  - データライフサイクルの各過程において、データが越境・移転されたり、海外で共有・利活用される場面全般を対象とする。
- 「対象となるデータ」（図 3）に関して、国際的にデータが共有・利活用される場面において取り扱われ得る産業データ全般を対象とする。対象となるデータをカテゴリーとして大きく「個人データ」と「非個人データ」に区分した上で、個人情報保護の観点から議論が積み重ねられてきた「個人データ」に比べ、これまで体系的な議論がなされてこなかった「非個人データ」の領域に焦点を当て、事例の深堀を行う。

[3] デジタル庁「DFFT」 https://www.digital.go.jp/policies/dfft

- 「個人データ」には、個人情報、仮名・匿名加工情報、個人関連情報を含む情報等が含まれる[4]。
- 「非個人データ」は、データ全般のうち「個人データ」に該当しないものをいい、企業活動に伴い収集・蓄積される「安全保障関連データ」、「営業データ」、「技術データ」、「その他・事業データ」が含まれる。
- 実務上、上記の「個人データ」と「非個人データ」の区分は相対的・流動的になる。

図1




[4] 個人情報の保護に関する法律（個人情報保護法）については、個人情報保護委員会のウェブサイトにおいて、関連法令・ガイドラインがまとめられている。https://www.ppc.go.jp/personalinfo/legal/

図2

## 対象プロセス：データライフサイクルと対象場面（例）

| | 生成・取得 | 加工・利用 | 移転・提供[1] | 保管 | 廃棄 |
|---|---|---|---|---|---|
| 各過程の説明 | 自動又は手動の手段でデータが新たに作られ、データが自社の管理下に置かれる | データの抽出・トリミング等を加え、閲覧・分析等に用いる | データを活用したい別の組織等に対して無償又は有償でデータを移動させる・渡す | データを安全かつ効率的に、必要に応じた利用のために管理の下で保存する | データを消去または、使用不可能状態(インアクティブ)にする |
| 各過程の対象場面(例) | 海外で生成されるデータを取得する | 日本で加工・分析されたデータが海外で参照・利用される | 日本国内で保有するデータを、海外に移転させる | 海外のクラウドサービスを用いて、海外に置かれたサーバーにデータを保存する | 海外に保管されているデータが消去される |

⊕ 国外で各過程が発生・実施される場面全般

Note 1. 各過程においてもデータ越境を伴う移動が生じうるため、ここでは「生成・取得」、「加工・利用」、「保管」、「廃棄」を伴わないデータ移動を指す

図3

## 対象データ：データのカテゴリ・例

| データカテゴリ | | データカテゴリの概要 | データ例 |
|---|---|---|---|
| 非個人データ※ | 安全保障関連データ | 軍事、重要インフラ、特定重要物資等の国家・産業の安全保障・維持の観点で重要性が高い情報 | • 安全保障貿易管理の対象となるデータ<br>• 社会基盤を支える重要なインフラに関する技術や運用データ<br>• 特定重要物資に関するサプライチェーン等のデータ |
| | 営業データ | 営業活動を通じて収集・蓄積する情報全般 | • 取引先に関するデータ（取引価格、取引先情報等）<br>• 取引先との契約に関するデータ（ライセンス契約・NDA等に基づき入手した他社データ等）<br>• 他社から入手した限定提供データ |
| | 技術データ | 技術的な知識やデータ、ノウハウ等で、技術的活動全般に関連する情報 | • 技術データ、ノウハウ（部品の組合せ、新規素材の成分、製造ノウハウ）<br>• 知的財産権で保護されるデータ：創作性が認められるデータ（例：ソースコードやアルゴリズム等の著作物、写真、音楽などのコンテンツ）<br>• 自社保管の他社データ（他社との間で限定共有されているデータ） |
| | その他・事業データ | 企業が生成・保管する、営業・技術データ以外の事業活動に伴う情報 | • 経営戦略に関わる情報（事業計画、投資計画に関するデータ等）<br>• 企業のセキュリティに関する情報（インフラ、BCPに関するデータ等） |
| 個人データ | | 個人情報、仮名・匿名加工情報、個人関連情報を含む情報 | • 個人情報（単独または複数で個人の識別が可能な記述・識別記号）<br>• 匿名加工情報（個人情報を加工し、特定の個人が識別できない情報）<br>• 個人関連情報（生存する個人に関する情報であって、個人情報・仮名加工情報・匿名加工情報のいずれにも該当しないもの） |

Note: 非個人データに関して、データ全般のうち「個人データ」に該当しないものを指す

### 2.2　関連する検討及びガイドラインとその位置付け

- 本マニュアルは、令和６年５月から12月にかけて実施された「産業データサブワーキンググループ」における検討結果を踏まえ、取りまとめたものである。
- 「産業データサブワーキンググループ」は、「国際データガバナンスアドバイザリー委員会」及び「国際データガバナンス検討会」（いずれもデジタル庁・経済産業省）の下に位置付けられる。

- 国内外におけるデータの共有・利活用に対して、「国際データガバナンスアドバイザリー委員会」及び「国際データガバナンス検討会」の議論を踏まえてデジタル庁と IPA において作成された「データガバナンス・ガイドライン（案）」[5]は、経営者視点からデータガバナンス全般の課題・打ち手を広範に捉えている。本マニュアルは、「データガバナンス・ガイドライン（案）」の「越境移転の現実に対応した業務プロセス」に対応しており、実務的な側面に焦点を当てる。

- 加えて、過去の検討において、関連する内容が取りまとめられたガイドラインが複数存在しており、本マニュアルは、これらの関連ガイドラインの内容も参照し、方向性を検討・作成している（図 4）。
  - 代表的なガイドラインとして、例えば、経済産業省にて取りまとめ・公表している「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」[6]、「秘密情報の保護ハンドブック」[7]、「AI・データの利用に関する契約ガイドライン」[8]、「限定提供データに関する指針」[9]が存在する。
  - 本マニュアルの構成に照らして、各関連ガイドラインにおいて関連・参考になる章・内容を主要参照先として取りまとめているため、本マニュアルの補足情報として参照されたい（図 5）。また主要参照先以外にも、参考になる考え方・内容が多く含まれるため、各関連ガイドラインに関して、全体を確認することが推奨される。

[5] （公表され次第 URL を追記）

[6] https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework_1_1.pdf

[7] https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

[8] https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pdf

[9] https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf

図4

## 関連ガイドラインの概要

| | 目的 | 対象読者（認識） | 関連する内容 | 発行年 |
|---|---|---|---|---|
| 1 データガバナンス・ガイドライン(案)<br>(デジタル庁) | 内容に合わせて更新 | | | |
| 2 協調的なデータ利活用に向けたデータマネジメント・フレームワーク<br>(経済産業省 商務情報政策局 サイバーセキュリティ課) | サイバー・フィジカル空間の融合が進む中、適切なセキュリティ・データの信頼性確保<br>• データライフサイクル全体で適切な管理を実施するためのフレームワーク提供 | データを管理・利用する企業や団体の担当者<br>システム設計・運用に関わるエンジニア<br>ガイドラインやルールの策定者 | データマネジメントのモデル化<br>• ライフサイクルを通じたデータ状態・リスクの可視化、セキュリティ確保<br>セキュリティ対策に関する外部規格・ガイドライン照会 | 2022年<br>• 最終改訂 2024年 |
| 3 秘密情報の保護ハンドブック<br>(経済産業省 知的財産政策室) | 企業における秘密情報漏洩防止のための保護力の強化、法的リスク低減 | 企業の経営者<br>企業の情報管理責任者・法務部門・コンプライアンス部門 | 企業が保有する情報の評価<br>• 情報の評価、秘密情報の決定<br>情報漏洩対策の選択及び、そのルール化<br>秘密情報の管理にかかる社内体制の在り方 | 2016年<br>• 最終改訂 2024年 |
| 4 AI・データの利用に関する契約ガイドライン -データ編-<br>(経済産業省 商務情報政策局 情報経済課) | 事業者がデータに関する契約を適切に締結するための一般的な契約事項、考慮要素の整理 | 企業の業務推進者・担当者<br>企業の契約担当者や法務担当者 | データ提供型契約における法的な論点<br>• クロス・ボーダー取引における留意点<br>主な契約条項例 | 2018年<br>• 最終改訂 2019年 |
| 5 限定提供データに関する指針(参考)<br>(経済産業省 知的財産政策室) | 不正競争防止法における「限定提供データ」として法的保護を受けるための要件・その考え方の整理 | 企業の業務推進者・担当者<br>企業の契約担当者や法務担当者<br>企業の情報管理責任者 | 不正競争の対象となる行為と対応策の紹介 | 2019年<br>• 最終改訂 2024年 |

図5

## 本マニュアルに対する関連ガイドラインの主要参照先

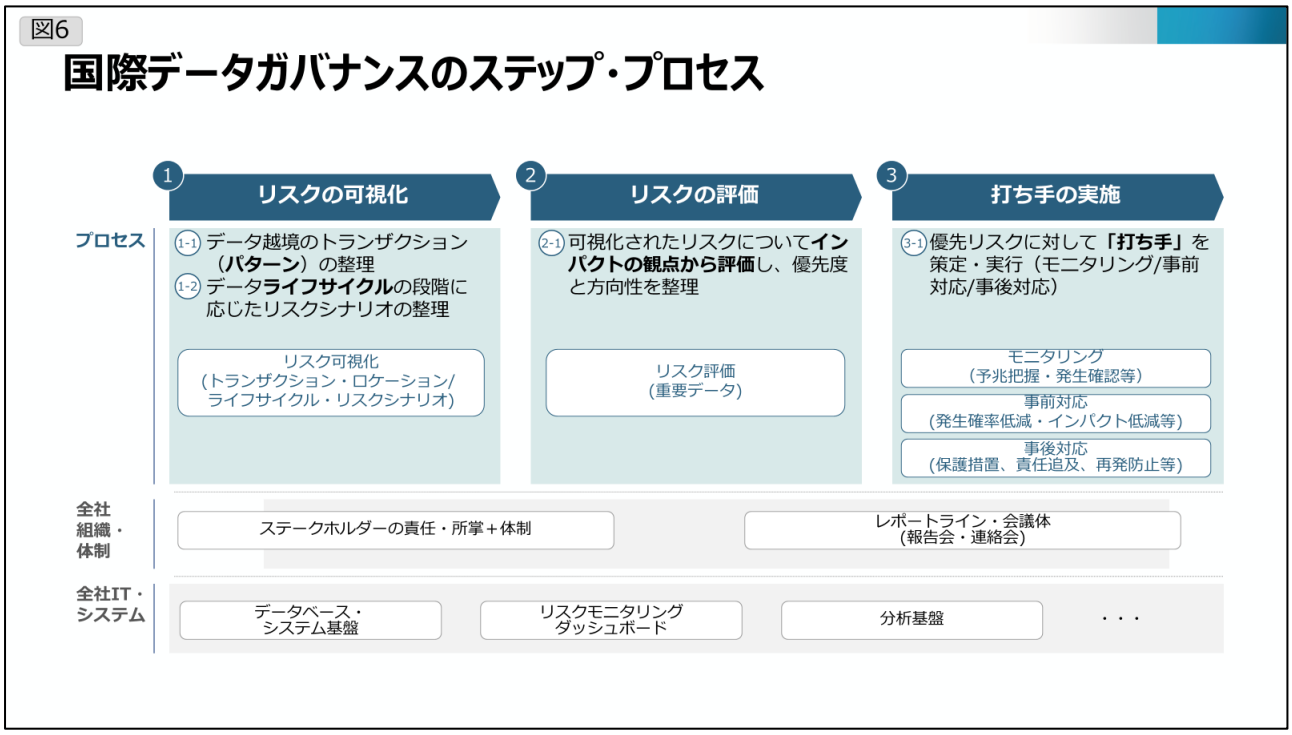
| 本マニュアル(章) | | 関連ガイドライン | 主な参照章 | 概要 |
|---|---|---|---|---|
| 3 国際データマネジメンのステップ | 3.2 リスクの可視化 | 2 協調的なデータ利活用に向けたデータマネジメントフレームワーク | 2. 本フレームワークにおけるデータマネジメントのモデル<br>• 2-2-1 モデル化（「イベント」） | データライフサイクルの定義及び、代表的なリスクの記載 |
| | | 5 限定提供データに関する指針 | Ⅲ. 「不正競争」の対象となる行為について(総論) | データライフサイクルごとの不正競争の対象となる行為の定義 |
| | 3.3 リスクの評価 | 3 秘密情報の保護ハンドブック | 2章 保有する情報の把握・評価、秘密情報の決定<br>• 2-2 秘密情報の決定 | 企業が保有する秘密情報（営業秘密、個人情報、機微技術情報など）の重要性評価、秘密情報決定にあたって考慮すべき観点の例示 |
| 4 想定リスクとその対応策詳細 | 4.2 主要な関連法規制 | 2 協調的なデータ利活用に向けたデータマネジメントフレームワーク | 2. 本フレームワークにおけるデータマネジメントのモデル<br>• 2-2-1 モデル化（「場」） | データに対する規範の例示<br>• 各国・地域の法令、組織の内部規則など |
| | | 4 AI・データの利用に関する契約ガイドライン- データ編 - | 第４「データ提供型」契約（一方当事者から他方当事者へのデータの提供）<br>• (5)クロス・ボーダー取引における留意点 | クロス・ボーダー取引で留意すべき海外法・規制の例示<br>• 越境移転規制、外為法、準拠法など |
| | 4.3 主要なリスクと打ち手の詳細 | 3 秘密情報の保護ハンドブック | 3章 秘密情報の分類、情報漏えい対策の選択及びそのルール化<br>• 3-2 分類に応じた情報漏えい対策の選択<br>• 3-3 秘密情報の取扱方法等に関するルール化<br>• 3-4 具体的な漏えい対策例 | 秘密情報を保有する者の意図しない情報漏えいに対する保護の方法、対策の例示 |
| | | 4 AI・データの利用に関する契約ガイドライン- データ編 - | 第7 主な契約条項例 | モデル契約書案の記載(データ提供型契約/ データ創出型契約) |

## 3　国際データガバナンスのステップ

### 3.1　全体像・フレームワーク

- 本章では、国際データガバナンスについて、全体像と検討すべき項目を示すフレームワークを提示する。国際データガバナンスを捉えるフレームワークとして、３つのステップ「①リスク可視化」、「②リスクの評価」、「③打ち手の実施」及びその中に含まれるプロセスを定義する（図 6）。
  - なお、国際データガバナンスを実現するためには上記プロセスだけでなく、組織・体制及び IT・システムの整備も重要となる。ただし、これらは国際データガバナンスだけでなく、企業活動全般を踏まえて検討される内容となるため、本マニュアルではこれらの体系的な整理は行わない。
  - 前記「データガバナンス・ガイドライン(案) 」において、データガバナンスを実装するための柱として、越境移転の現実に対応した業務プロセスのほかに、データマチュリティ及びデータセキュリティについて記載されているため、参照されたい。

図6




### 3.2　リスクの可視化

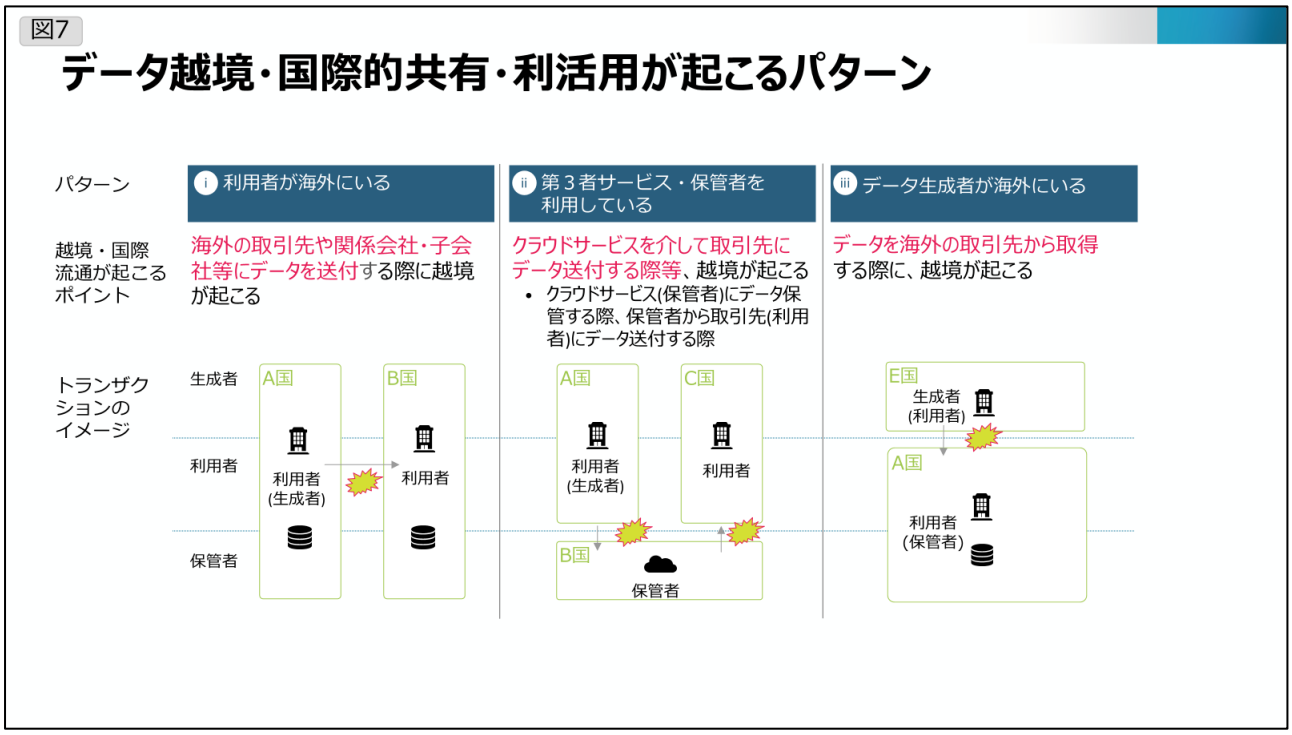
#### 3.2.1 データ越境・国際的な共有・利活用のトランザクション(パターン)の整理

- リスクの可視化では、まずは想定するデータ共有・利活用において、関連するステークホルダー及びデータとその所在を整理し、どこでデータ越境・国際的な共有・利活用が発生するか把握する。
- データの共有・利活用においては、ステークホルダーの分類として「生成者」、「利用者」、「保管者」が存在する。
  - 本マニュアルにおいて、「生成者」は手動データ入力や機器・システムからの自動生成等を通じてデータを生成する者、「利用者」はデータ共有・加工等を通じてデータを実際に利用する者、「保管者」はデータの保管場所や保管サービスを管理・運営する者を指す。

- 「生成者」「利用者」「保管者」は、トランザクションによって、同じステークホルダーが複数の役割を担うこともあれば、異なるステークホルダーが担う場合も存在する。
- また、本マニュアルの分類・用語定義は、各国法令における分類・用語定義と必ずしも一致しない。

- 実業務においては、企業・事業内容によって、無数のトランザクションのパターンが存在する。ステークホルダーの分類を念頭に、各トランザクションにおいて、海外企業・サービス提供者が存在するか、それはどこの国に当たるか、データのロケーションを把握することが重要となる。
  - データの越境・国際的な共有・利活用が発生する場合に、何のデータが対象となるか、どこのライフサイクルに当たるかも併せて確認することが推奨される。
- データ越境・国際的な共有・利活用が起こるパターンとして、想定されるパターンの類型を例示するため、参考にされたい（図 7）。

図7




### 3.2.2　リスクシナリオの整理

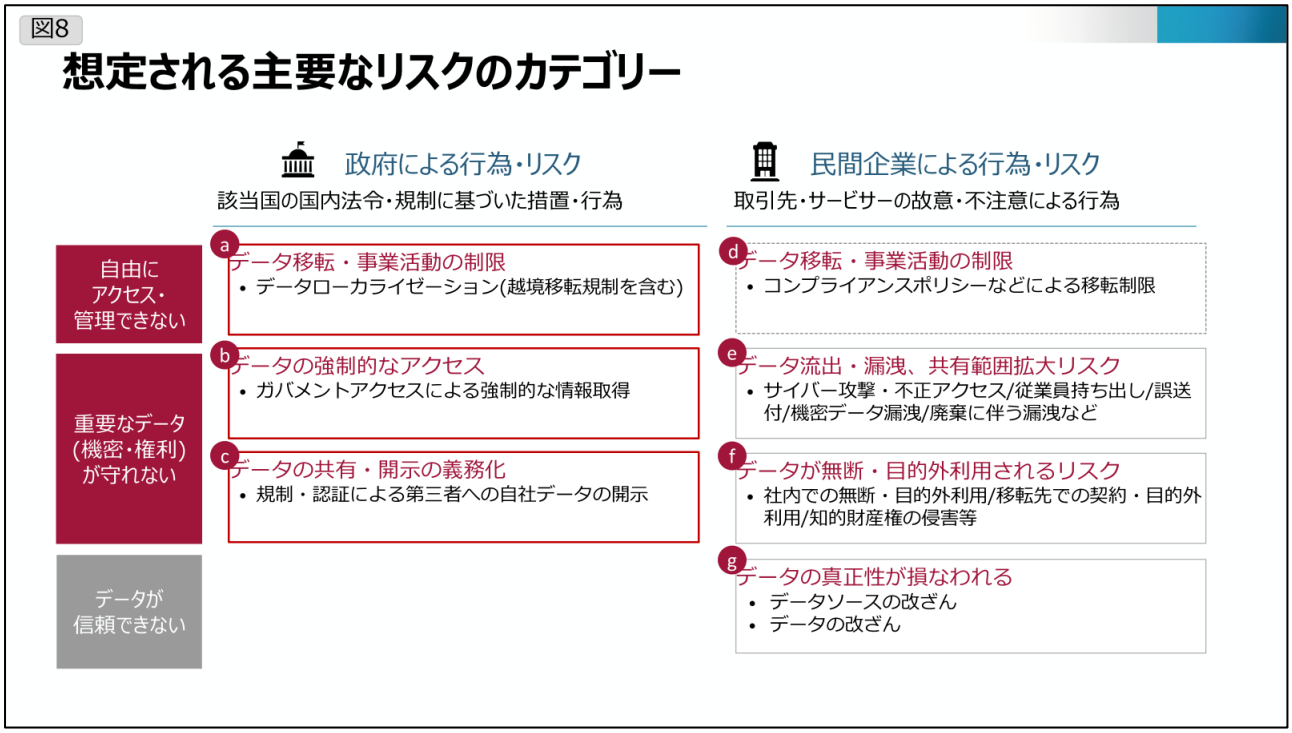
- リスクシナリオの整理では、3.2.1「データの国際流通・越境のトランザクション(パターン)の整理」で把握したデータのロケーション、データの内容・ライフサイクルを踏まえ、想定されるリスクシナリオを整理する。
- 前記 2.1「検討の範囲・スコープ」における記載のとおり、実現したい価値の裏返しとして、他国・地域に保管しているデータに自由にアクセス・管理できない、重要なデータ（機密性・権利）が守れない、データが信頼できないことを、主要なリスクと定義する。加えて、各リスクに対して、国内法令・規制など政府による行為で発生するリスク（以下「政府による行為・リスク」という。）と、取引先・サー

ビス提供者の不注意・故意による行為など民間企業による行為で発生するリスク（以下「民間企業による行為・リスク」という。）が存在する。

- なお、「政府による行為・リスク」は、データローカライゼーションやガバメントアクセスといった禁止及び抑制行為を政府として規範化して執行する法規制（直接的）と、データの共有・開示の義務化といった企業に対して何かしらの行為を命じる規制（間接的）が存在する。政府が直接的、間接的に関与するかによって、取るべき打ち手の方向性も変わり得る。詳細について 4.1「リスクと打ち手の方向性（サマリ）」にて、整理を行う。

上記の考え方に基づき、代表的なリスクのカテゴリーとして、前記 2.1「検討の範囲・スコープ」の中で定義された「実現したい価値」に基づき、政府による行為・リスクとして「a.データ移転・事業活動の制限」、「b.データの強制的なアクセス」、「c.データの共有・開示の義務化」、民間企業による行為・リスクとして「d.データ移転・事業活動の制限」、「e.データ流出・漏洩、共有範囲拡大リスク」、「f.データが無断・目的外利用されるリスク」、「g.データの真正性が損なわれる」の大きく 7 つのカテゴリーを定義する（図 8）。

図8




## 3.3 リスクの評価

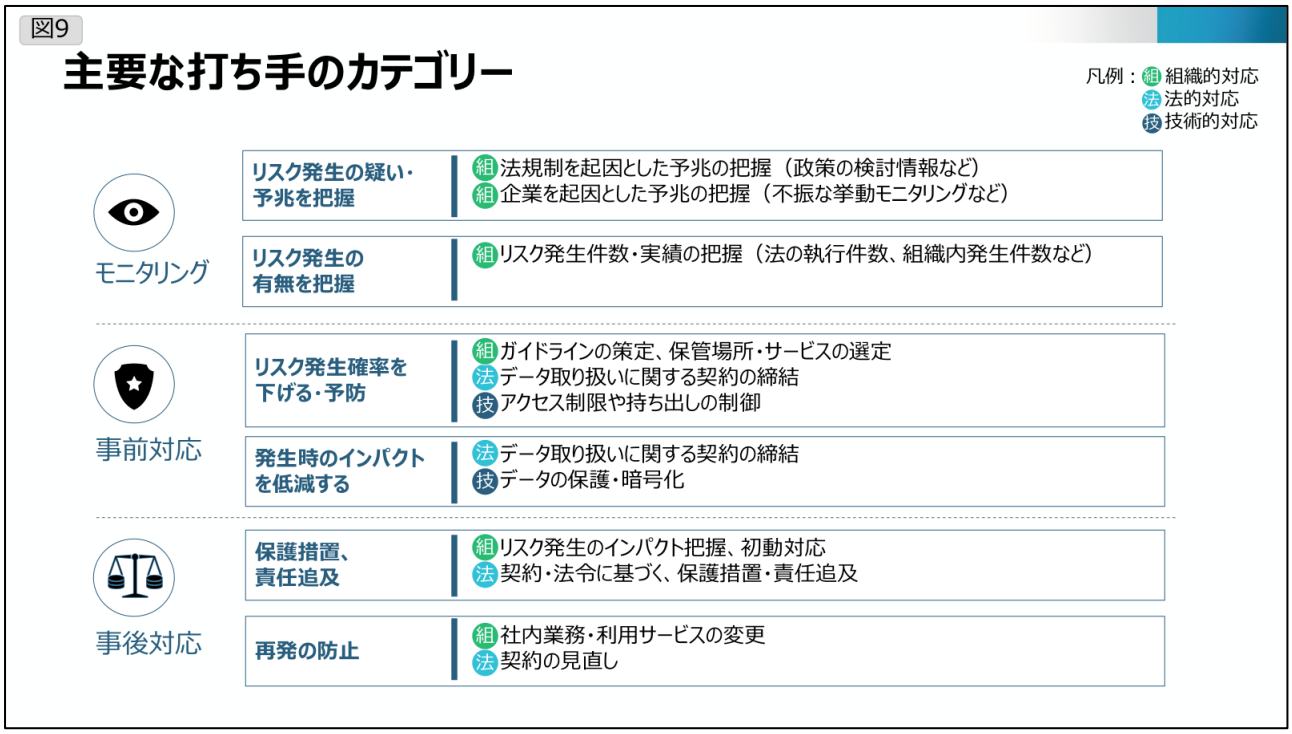
- 企業にとって、全てのリスクに対して一様の対応を行うのはリソースの制約から難しい場合があるため、リスク評価・優先度付けが有効と考えられる。
- リスクの評価として、インパクトの視点から、自社として保護すべき機密・秘密情報を定義・評価することが推奨される
  - 本マニュアルにおいて、企業にとって機密性が高い情報及び秘密保持契約の対象となる情報を合わせて、機密・秘密情報と定義する

- 機密・秘密情報の判断は、企業によって異なる。関連ガイドラインである「秘密情報の保護ハンドブック」における第 2 章「保有する情報の把握・評価、秘密情報の決定」において、秘密情報となり得る判断の基準の例が記載されているため、判断時に参照されたい。

### 3.4　打ち手の実施

- 主要な打ち手のカテゴリーとして、予兆・発生を検知する「モニタリング」、リスク予防・発生時のインパクトを低減する「事前対応」、発生後の回復・再発防止を行う「事後対応」が存在する（図 9）。
  - モニタリング：リスク発生の疑い・予兆を把握、リスク発生の有無を把握
  - 事前対応：リスク発生確率を下げる・予防、発生時のインパクトの低減
  - 事後対応：適切・迅速なステークホルダーへのレポート、保護措置・責任追及、再発の防止
- 打ち手のカテゴリーごとに、更に組織的な措置(ガイドライン策定・保管場所選定等)、技術的な措置(暗号化・アクセス制限等)、法的な措置(契約の締結等)が、具体的な打ち手として存在する。
- 詳細は 4.3「主要なリスクと打ち手の詳細」及び参考資料 A「打ち手・対応措置のリスト」を参照されたい。

図9



## 4. 想定リスクとその打ち手の詳細

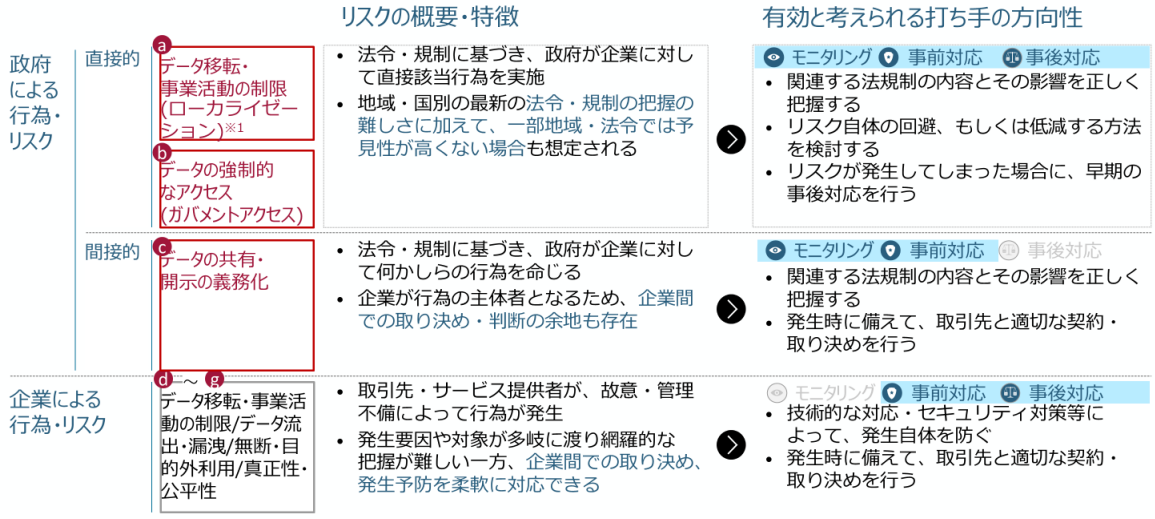
### 4.1 リスクと打ち手の方向性(サマリ)

- 本章では、第 3 章「国際データガバナンスのステップ」の考え方を前提として、想定される主要リスクに対する留意点及び打ち手の整理・記載を行う。
- 前記のとおり、リスクは大きく「政府による行為・リスク」及び「民間企業による行為・リスク」に区分され、それぞれ主な対応の方向性・考え方が異なる（図 10）。
- 「政府による行為・リスク」は、データローカライゼーションやガバメントアクセスといった禁止及び抑制行為を政府として規範化して執行する法規制（直接的）と、データの共有・開示の義務化といった企業に対して何かしらの行為を命じる規制（間接的）が存在する（図 11）。
  - 前者の「政府による行為・リスク(直接的)」においては、法令に該当する場合にリスク自体の発生を避けることは難しい一方で、関連する法規制の内容とその影響を正しく把握し、対応を講じることが考えられる。主な打ち手として、関連する法規制の内容とその影響を正しく把握しつつ、リスク自体を回避・低減させる方策を検討すること、またリスクが発生してしまった際に早期の事後対応を行うことも有効と考えらえる。
  - 後者の「政府による行為・リスク(間接的)」においては、狭義で行為を行うのは企業であることから、関連する法規制の内容とその影響を正しく把握することに加えて、企業間の打ち手として、取引先と適切な契約・取り決めを行うことも有効であることが考えられる。
  - なお、データローカライゼーションに関しては、国内保存要求、国内処理要求、越境移転禁止規制を念頭に「政府による行為・リスク（直接的）」に分類している。ただし、一部、条件付きで越境移転を認めるものなど、「政府による行為・リスク（間接的）」に当たるものも含んでいる。
- 「民間企業による行為・リスク」は、発生の要因や対象が多岐にわたり網羅的な把握が難しい一方、企業間における取り決め・意思決定によって、柔軟に打ち手を講じることができる。例えば、技術的な対応・セキュリティ対策等によって、発生自体を防ぐことや、取引先企業によって適切な契約を結ぶことが有効と考えらえる（事前・事後対応）。
  - 企業間での契約においては、データ生成者（提供する側）の立場からはデータ保護について、データ利用者（提供を受ける側）の立場からは自社の事業に必要なデータの利用・開示の確保等について、それぞれの立場から適切かつ必要な条件を検討することが有用となる。
  - 「民間企業による行為・リスク」は、企業における不注意やガバナンスの不足によって発生する場合が多い。商慣習・管理体系の異なる海外企業との付き合いが増えることによる間接的な影響は想定されるが、データの越境・国際的な利活用によって直接的に発生するリスクではない。
  - データライフサイクルにおける「廃棄」には、データをインアクティブにする・見えなくすることも含まれる。実務上、データがどのような状況にあるか確かめることが難しい場合も多く、漏洩や目的外利用に対して特に留意が必要となる。

- 各リスクの特徴・打ち手の方向性も踏まえ、本マニュアルにおいては、特に「政府による行為・リスク」に焦点を当て、4.3「主要なリスクと打ち手の詳細」において、留意点と主要な打ち手の詳細の整理・記載を行う。

図10

## リスクと打ち手の方向性サマリ




1. データローカライゼーションの一部に条件付きで越境移転を認めるものも含み、当該措置は例外的に「政府による行為・リスク（間接的）」にあたるため、「政府による行為・リスク（間接的）」に対する打ち手が有効となる（企業間の契約で越境移転の条件に対応する旨取り決めを行うなど）

図11

## 政府による行為・リスク：主要な打ち手の例

4.2 主要な関連法規制 (EU・中国・米国)

- データに関連する各国の法規制は、国・地域ごとに多岐にわたり、また日々新しい法規制が検討・施行されている。ここでは、我が国との関係性において特に重要となる EU・中国・米国について整理を行う（図 12・図 13）。
- EU においては、個人データに加えて、産業データに対しても、域内におけるデータの利活用の促進及び権利保護を進める目的で、統括的なデータに関連する法規制の整備が進められている。
  - 個人データに関しては、GDPR(General Data Protection Regulation)[10]に基づき、個人データの保護に関する厳格な規定が定められている。GDPR において、個人データの越境移転（EEA 及び英国域外の第三国又は国際機関から別の第三国への個人データの再移転を含む。）は原則として禁止される（第 44 条）。例外的に個人データの越境移転が可能となるのは、移転先の第三国が十分性認定を取得している場合（第 45 条）、SCC や拘束的企業準則等の適切な保護措置に依拠する場合（第 46 条及び第 47 条）及び第 49 条の例外規定に依拠する場合である。
  - 産業データに関しては、データ法[11]において、コネクテッド製品及び関連サービスによって生じるデータを対象に、ユーザーに対するアクセスとユーザーの要望を前提とする第三者に対する FRAND 条件での開示や、ガバメントアクセスに対するルールが定められている。データ保有者は、原則として、合法的かつ容易に入手できる製品データや関連サービスデータについて、これらのメタデータとともに、データ保有者が入手可能なものと同じ品質で、無償で、技術的に可能な場合には継続的かつリアルタイムに、ユーザーがアクセスできるようにしなければならない旨を規定している（第 4 条第 1 項）。第 3 者開示に当たって、ユーザから要望があった場合に、データ保有者は容易に入手可能なデータを第三者（「データ受領者」）に提供するものとし（第 5 条第 1 項）、データ提供時の条件として、B to B 間でデータ共有が義務付けられる場合、データ保有者は、公正、合理的かつ非差別的な条件（いわゆる FRAND 条件）により、透明性のある方法で提供することが規定されている（第 8 条）。加えて、データ利用可能とする対価の考え方について、第 9 条に規定されている。また、公的緊急事態に対応するため必要がある等の例外的な必要性が認められる一定の場合に、公的部門機関等に対してデータを利用可能としなければならない旨を規定している（第 14 条及び第 15 条）。同法は 2024 年 1 月 11 日に採択され、原則として 2025 年 9 月 12 日に施行される予定となっている。
  - 加えて、EU 電池規則[12]を筆頭に、国際的にサステナビリティ・環境関連の法規制の整備が進む中で、データのトレーサビリティ・公開が求められるケースが増えてきている。

[10] 個人情報保護委員会 GDPR https://www.ppc.go.jp/enforcement/infoprovision/EU/

[11] European Commission, Data Act, https://digital-strategy.ec.europa.eu/en/policies/data-act

[12] European Commission, Batteries, https://environment.ec.europa.eu/topics/waste-and-recycling/batteries_en#law

- 中国においては、国家からのデータ統制として、いわゆるデータ 3 法(サイバーセキュリティ法、データセキュリティ法、個人情報保護法)を中心とした、国家の情報収集活動への協力及び越境移転規則（国内保存）が規定されている。
  - 中国データ３法のもとで国内保存義務が課せられているが、国内保存義務の対象者の範囲及び当該義務の対象となるデータの範囲それぞれについて、不明瞭な定義が残る。例えば、中国サイバーセキュリティ法において、重要情報インフラ運営者が中国国内での運営中に収集及び発生させた個人情報及び重要データは、国内で保存しなければならない。業務の必要性により、国外提供の必要が確かにある場合には、国家ネットワーク情報部門が国務院の関係部門と共同して制定する弁法に従い安全評価を行わなければならない旨を規定している（第３７条）。
  - 「重要データ」は、「ひとたび改ざん、破壊、漏えい又は不正取得、不正利用がされた場合、国家安全、公共利益に危害を及ぼす可能性がある電子的データ」をいう[13]。具体的には政府機関が定義することとされているが、現時点では重要データの目録や識別について定めた国レベルの法令・ガイドライン等は公開されていない。
- 米国においては、基本的に市場における自由な経済活動及びデータ流通が尊重・重視されており、データ越境に制限を課す法規制は少ないが、一部、州レベルでの個人情報保護法や、安全保障の観点での個人データや一部の機密・秘密情報に関する制限が設けられている。
  - 例えば、Cloud 法[14]において、非常時(犯罪捜査や国家安全保障にかかわるような状況)において、米国の政府機関が令状等により米国の管轄権に服するプロバイダーに対して、米国外に保有等しているデータの保存、バックアップ、開示を強制することができることが明確化（CLOUD Act 103 条(a)(1)、18 U.S.C. Sec. 2713）されているが、アクセス権が実際に行使された例は限定的となる。
- データに関連する法規制は、データアクセスの手段の多様化や、法規制の解釈の拡大・拡張などに伴い、足元での変化が激しいため、最新の動向を定期的に確認・把握することが重要となる。
  - 経済産業省や JETRO 等のウェブサイトにおける各国制度の記載・調査結果[15]も制度の確認に有用であり、影響が大きいと想定される法規制に関しては原文の確認及び専門家への相談が推奨される。
  - 法規制の問題点の把握に際し、相手国の合意する WTO 協定、経済連携協定等、既存の国際ルールとの整合性も確認する。

---

[13] https://www.rieti.go.jp/jp/publications/dp/24j007.pdf

[14] 西村高等法務研究所「CLOUD Act（クラウド法） 研究会報告書 Ver.2.0」（2023 年 4 月）
https://www.nishimura.com/ja/knowledge/publications/92692

[15] 不公正貿易報告書が一例として挙げられる。
https://www.meti.go.jp/policy/trade_policy/wto/3_dispute_settlement/32_wto_rules_and_compliance_report/321_past_report/compliance_report.html

図12

## 主要なデータ関連法規制 (EU)

| | 目的 | データに関する主要な要求 | 想定されるリスク | 施行状況 |
|---|---|---|---|---|
| データガバナンス法(EU) | • EU経済圏としてデータの利活用・公平性を確保する | • 特定の事業者によるデータの独占・データ主体者の権利が損なわれやすい個人データについて、GDPRに基づき、保護水準の担保が求められる<br>• 公共の利益や研究目的のため、公共機関が持つ一部データの公開が義務付けられる | データ共有・開示義務<br>• 公共機関が持つデータの一部は開示を義務付けられる可能性がある | • 2022年施行 |
| データ法(EU) | • 特に産業データについて、データの利活用・公平性を確保する | • EU域内のコネクテッド製品、または関連サービスの使用によって生じるデータやサービスデータが、利用者にアクセスできる形でなくてはならない<br>• 公的緊急事態に対応する必要がある場合に、公的部門機関等に対してデータを提供しなければならない | データ共有・開示義務<br>• データの開示義務に対応するため、追加的な工数が発生する、機密情報を公開しなければならない可能性がある<br>ガバメントアクセス<br>• 緊急時においてはガバメントアクセスの可能性がある | • 2024年1月発効<br>• 2025年9月施行予定 |
| 蓄電池規則(EU) | • 蓄電池の全ライフサイクルにわたる持続可能性、リサイクル、安全性の強化 | • バッテリーの透明性と持続可能性を担保するためのデータについて公開が義務付けられている<br>– ライフサイクル全体のカーボンフットプリント・リサイクル材料の割合<br>– バッテリーパスポート(モデル情報、性能、化学成分、寿命等を含む) | データ共有・開示義務<br>• バッテリーに関するデータを公開する中で、機密情報や、競争優位性に直結する情報を公開しなければならない可能性がある | • 2023年8月施行<br>• 2024年2月以降、段階的に適用 |

図13

## 主要なデータ関連法規制 (中国・米国)

| | 目的 | データに関する主要な要求 | 想定されるリスク | 施行状況 |
|---|---|---|---|---|
| 国家安全法(中国) | • 国家の安全(経済社会の発展を含む)の維持 | • 主に国防に関する原則事項を具体化し基本原則を定め、具体的な要求はデータ3法(サイバーセキュリティ法・データセキュリティ法・個人情報保護法)にて支えられる | • (下記にて詳述) | • 2015年施行 |
| サイバーセキュリティ法 | • サイバー空間における全体的なセキュリティ管理(ネットワークインフラ保護を主眼) | • 個人情報、重要データを中国内で保存することが求められる<br>• 公安機関又は国家安全機関が行う犯罪捜査に対し、必要に応じた技術協力及び政府へのデータ提供義務が課せられる | ローカライゼーション<br>• データが国家の安全に関わる場合は国外移転が禁止される<br>ガバメントアクセス<br>• 犯罪捜査で様々なデータの提供を求められる可能性がある | • 2017年施行 |
| データセキュリティ法 | • データ保護を重視し、重要データを定義・保護 | • 「重要データ」を中国から越境移転する場合、同法の規定に従うことが求められる<br>• データ処理者はセキュリティリスクに対処するため安全管理を実施しなければならない | ローカライゼーション<br>• 中国にとって重要と位置付けられたデータは国外への越境移転が困難となる可能性がある | • 2021年施行 |
| 個人情報保護法 | • データセキュリティ法の内、個人データの規制を補完 | • 企業や組織が中国国内から個人データを越境移転する場合、個別の同意の取得・セキュリティ要件の担保が求められる | ローカライゼーション<br>• 要件を満たせない場合、該当データの移転が行えない | • 2021年施行 |
| CLOUD法(米国) | • 国際的な捜査協力を強化し、国家安全保障を高める | • 米国に拠点を持つクラウドサービスプロバイダーは、米国外に保存されたデータでも、米国政府の要請に応じてそのデータにアクセス・提供する義務を負う可能性 | ガバメントアクセス<br>• 米国拠点のクラウドサービスプロバイダー経由で、日本企業の情報がガバメントアクセスの対象となる可能性 | • 2018年施行 |

### 4.3 主要なリスクと打ち手の詳細

#### 4.3.1 データ移転・事業活動の制限（ローカライゼーション）

- 「a.データの越境移転・事業活動の制限」に関して、法規制に基づき、データの国内保存の要求、当該国外への移転の禁止、当該国内データセンターの利用義務付け等の措置が課される懸念がある。

- データローカライゼーション措置の分類には、国内保存要求、国内処理要求、越境移転禁止規制が考えられる。国内保存要求は、データの保存場所を指定するものであり、データのコピーを国内に保存すれば、国外に移転し処理することを認める場合を念頭に置いている。国内処理要求は、データの主要な取扱場所を指定し、国外における処理（使用、編集・変更など）は認められない場合を念頭に置いている。越境移転禁止規制は、国外からのアクセスを含め、データの越境移転を禁止する措置を念頭に置いている（条件付きで越境移転を認めるものも含む）。
- 産業データに関しては、特に EU におけるデータガバナンス法やデータ法、中国におけるサイバーセキュリティ法やデータセキュリティ法等に留意が必要となる。前記のとおり、中国ではいわゆるデータ３法(サイバーセキュリティ法、データセキュリティ法、個人情報保護法)の下に国内保存義務が課せられているが、国内保存義務の対象者の範囲及び対象となるデータの範囲に関して、不明瞭な定義が残る。例えば、中国のサイバーセキュリティ法では、対象者の範囲が中国国内の重要情報インフラ運営者や 100 万人以上の個人情報を取り扱うデータ処理者など広範になっており、また、対象となるデータの範囲が自動車・軍事・工業分野など広範囲かつ不明瞭な定義を含む「重要データ」となっている。「重要データ」であるかどうかは、国家インターネット情報弁公室（CAC）に申請の上、評価が行われ、該当するとされた場合に越境移転が行えない。
- データローカライゼーション措置の分類や影響について、今野由紀子「データ・ローカライゼーションに関する考察：企業に与える影響と政策目的を踏まえたアプローチを中心に」[16]において取りまとめられているため、詳細について参照されたい。

- モニタリングにおいて、法規制の「対象となるデータ」、「実施プロセス」について把握を行い、リスクの影響と内容を検討しつつ、定期的に法規制の検討の進捗や内容の更新有無について確認することが推奨される（図 14）。
  - 対象となるデータに加えて、データローカライゼーション発生時に、前記データローカライゼーション措置の分類に従って、どのような制限事項となるのか、また例外措置が認められるか等、インパクトの大きさの把握に努めることが推奨される。特に、予見可能性が低く、越境移転制限の対象データか否かの判断について当局の裁量の幅が大きい国の場合、企業による移転可否判断が難しくなるため、留意が必要となる。
- 打ち手として、主に移転制限が起こっても事業に影響が及ばない・及びづらくする、移転制限自体が起こらないようにデータ越境を伴わない事業スキームを構築するといった対応の方向性が考えられる（図 15）。
  - 国内保存要求（越境移転の制限なし）が課されている場合に、「移転制限が起こっても事業に影響が及ばない・及びづらくする」対応として、当該データが移転制限の対象となっても事業が継続できるように、データの分散化、データ・業務の代替等の打ち手が想定される。データの分

[16] https://www.rieti.go.jp/jp/publications/dp/24j007.pdf

散化として、例えば分散型クラウドでサーバーをグローバルの複数拠点に設置し、データを国外にも分散させることで、データを活用できるようにすることが考えられる。また、国内処理要求又は越境移転禁止規制により国外での利用が制限される場合には、データ・業務の代替として、国外にある類似データを活用することが考えられる。例えば、機器の稼働データを取得し、当該国外で分析・故障予知をしている企業の場合、分析精度は下がってしまうと想定されるが、当該国内の稼働データは越境させず、当該国外で稼働する同じモデル・製品の稼働データ・実績を代替データとして、当該国内の機器の故障予知等に活用することなどが想定される。加えて、条件付きで国外移転が認められる場合には、その要件へ適合することも打ち手として想定され、特に、近時は複数の国の越境移転規制に同時に対応するために、それらの規制に準拠した条項を 1 つに組み込んで締結する Intra Group Data Transfer Agreement（IGDTA）が広く普及している。その際に、自社だけでなく、取引先に対しても移転の要件に適合するために必要な措置を採ることを、事前に契約の中に織り込むことも有用であると考えられる。

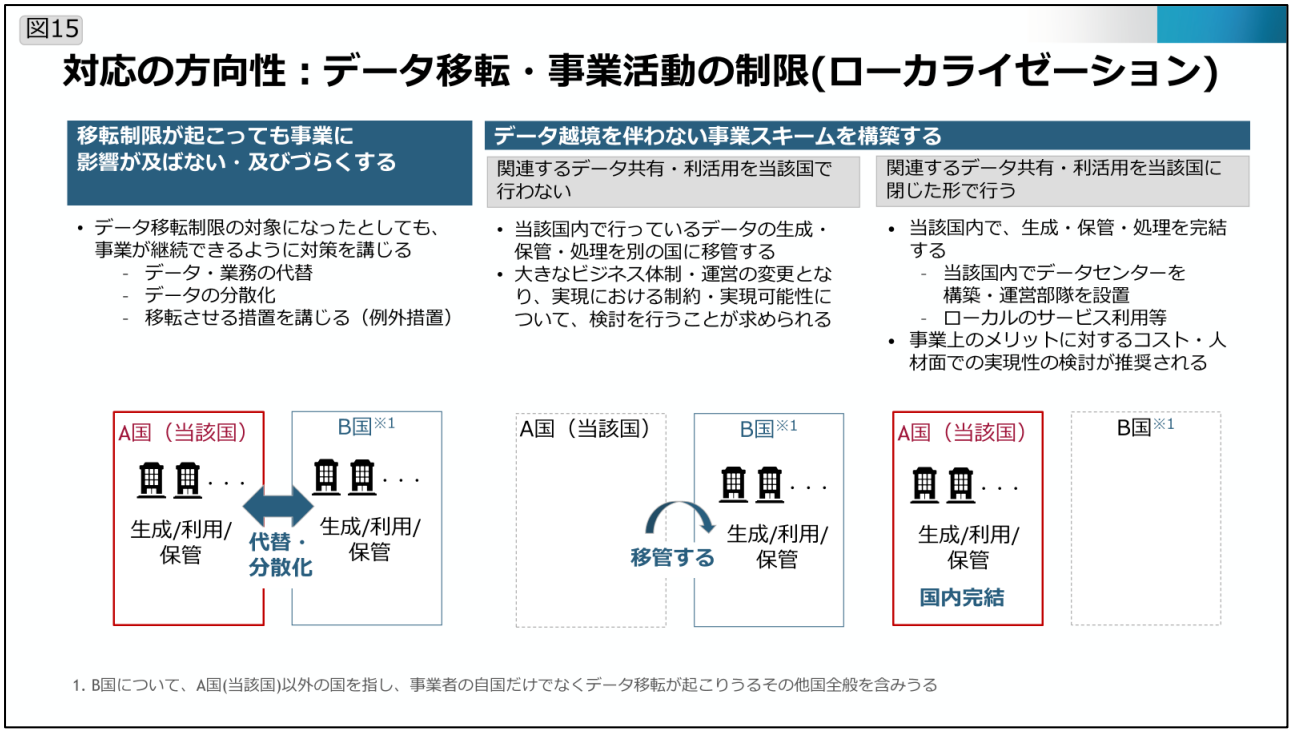
- 「データ越境を伴わない事業スキームを構築する」方法の 1 つとして、関連するデータ共有・利活用を当該国で行わないことが考えられる。例えば、法規制の導入が検討されているという段階では、当該国内で行っているデータの生成・保管・処理をそのまま別の国に移管するという打ち手が想定される。この場合に、大きくビジネス体制・運営の変更が求められることも想定されるため、実現可能性の検討が必要と考えられる。
- また、当該国内で生成・保管・処理を完結させることも考えられる。例えば、データ分析サービスを提供する場合に、当該国内に閉じて保管・分析等を行う現地チームの立ち上げを検討する等の打ち手が想定される。この場合にも、人材・コスト面での実現可能性を考慮した上で、事業上のメリット・必然性と比較し、意思決定を行うことが必要と考えられる。

図14

## モニタリング: 関連法規制におけるリスクを捉える観点

| | 対象となるデータ | 実施プロセス |
|---|---|---|
| a データ移転・事業活動の制限（ローカライゼーション） | ❑ 自社の損失につながるデータが対象となっているか？<br>- 公開されていない独自情報<br>- 第 3 者が悪用しうる<br>- 漏洩が契約違反につながる<br>など | ❑ どの程度制限事項があるか?<br>- データ保管場所<br>- 運用場所 など<br>❑ 例外措置はあるか？ |
| b データの強制的なアクセス（ガバメントアクセス） | ❑ 対象となるデータが明示されておらず、様々なデータが対象となり得るか？ | ❑ データ取得の根拠・手続きは明確か？<br>❑ 異議申し立てや協議などの保護措置があるか？ |
| c データの共有・開示の義務化 | | ❑ どこまでの公開・共有範囲となるか？<br>❑ 共有後、データはどのように利用されるか？ |

図15




4.3.2 データの強制的なアクセス（ガバメントアクセス）

- データの強制的なアクセスに関して、主に犯罪捜査、国家安全にかかわる場合等の非常時の場面において、規制当局より機密・秘密情報に対するアクセス・開示要求を課される懸念がある。
  - EU データ法、中国サイバーセキュリティ法、米国 Cloud 法等において、緊急時の対応や安全保護等を根拠に、ガバメントアクセスに関する規定が含まれている。
  - 一方、WTO の「知的所有権の貿易関連の側面に関する協定(TRIPS) 」の下、加盟国は、開示されていない情報を公正な商慣習に反する方法による保有者の承諾を得ない開示、使用等から有効な保護を確保するという国際的な義務が課されている。
  - ただし、前記の中国データセキュリティ法においては、「重要データ」に関するデータの安全評価の要件として、中国サイバースペース管理局が移転されるデータの性質及び使用されるネットワークやサービスプロバイダーに関する情報提出を要求していると報じられており、留意が必要となる。
- モニタリングにおいて、4.3.1「データ移転・事業活動の制限」同様に、「対象となるデータ」、「実施プロセス」について把握を行い、リスクの影響と内容を検討しつつ、定期的に法規制の検討の進捗や内容の更新有無について確認することが推奨される。
  - 実施プロセスとして、ガバメントアクセスがどのような根拠・手続で発生するか、またどれほど保護措置があるかを確認することが推奨される。
  - 加えて、想定されるガバメントアクセスの特徴を把握するために、強制性（罰則等を伴うかにかかわらず強制によるものか、任意・自主的な提供かなど）、対象となるデータライフサイクル（データ取得時の行為に起因するか、改変や削除の要求を想定したものかなど）、データの提供先

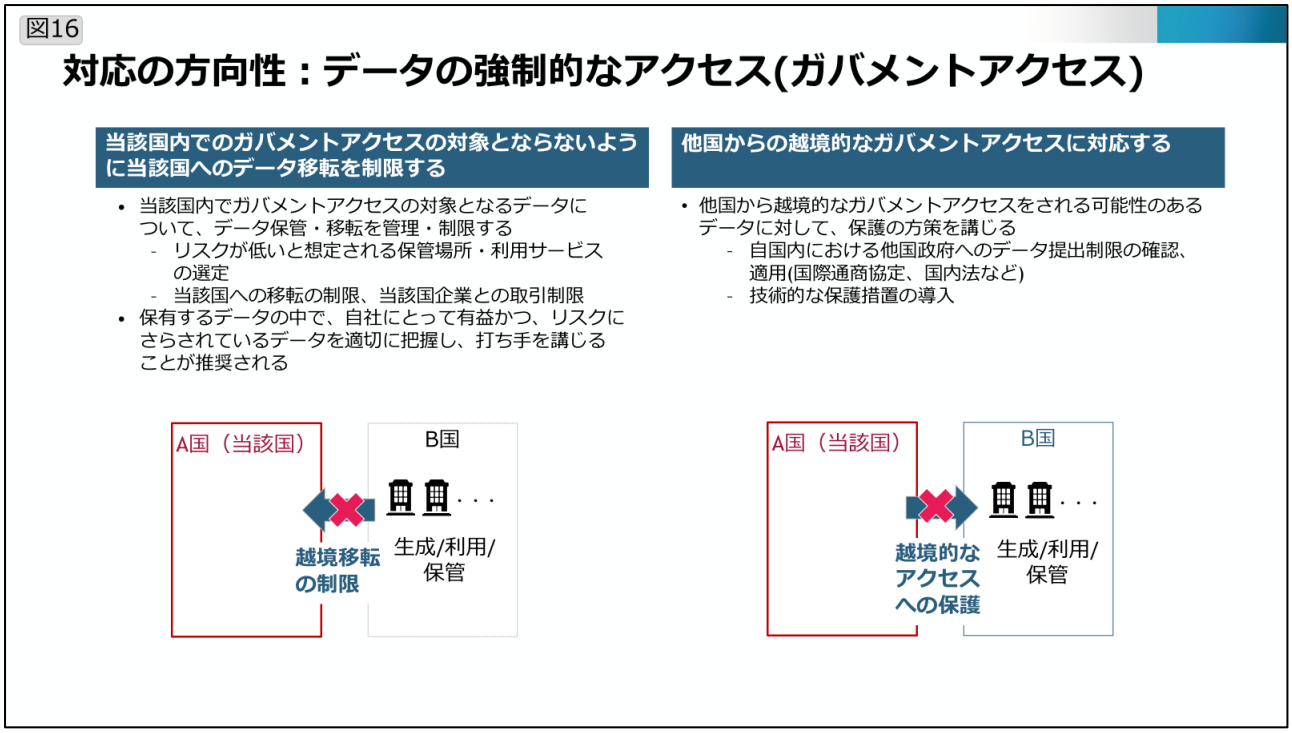
（政府への直接の提供か、政府が指定する組織(民間事業者含む)への提供かなど）についても確認することが推奨される。

- 個人データ・非個人データ双方を対象としたガバメントアクセスに関して、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報告書」（2022 年 11 月改訂版）[17]において、ガバメントアクセスの規律要素・事例の分析について取りまとめられているため、更なる詳細について参照されたい。なお、アップデートが多い領域となるため、最新の情報については別途確認が必要となる。

- 打ち手として、主に当該国内でのガバメントアクセスの対象とならないように当該国へのデータ移転を制限する、他国からの越境的なガバメントアクセスに対応する等の対応の方向性が考えられる（図 16）。
  - 「当該国内でのガバメントアクセスの対象とならないように当該国へのデータ移転を制限する」には、ガバメントアクセスの対象となるデータについて、データの保管・移転を管理・制限することが考えられる。保有するデータについて、自社にとって有益かつリスクにさらされている重要なデータを適切に特定・把握し、必要な打ち手を講じることが推奨される。その上で、例えば、リスクが低い(関連する規制がない・施行された実績がない・少ない、根拠・実施プロセスが明確で保護措置も定義されている等) と想定される保管場所・利用サービスを選定したり、当該国への移転及び当該国企業との取引制限を行うこと等の打ち手が想定される。
  - 「他国からの越境的なガバメントアクセスに対応する」には、越境的なガバメントアクセスをされる可能性のあるデータに対して、保護の方策を講じることが考えられる。例えば、自国内における保護措置・他国政府へのデータ提出制限として、OECD や G7、G20 等で議論されている国際的なガバメントアクセスに関するルール・原則に加えて、既存の国内法や国際通商協定等でも活用できる規定がないか、確認・検討することが想定される。具体例として、販売の承認の条件として政府に提出される医療品や農業用化学品の開示されていない試験データは、TRIPS 協定第 39 条第 3 項で保護されている。加えて、TPP 協定において（電子商取引章／ソース・コード）の輸入・販売条件として、他国の者が所有するプログラムのソースコードの開示・アクセスを禁止する条項（14.17 条）も存在する。
  - 加えて、技術的な保護措置を導入することも考えられる。例えば、ガバメントアクセスの要望に対して、事前にデータを暗号化する・匿名加工する等の打ち手が想定される。

[17] https://www.cfiec.jp/jp/pdf/gov/gov-2022-11-complete.pdf

図16




4.3.3 データの共有・開示の義務化

- データの共有・開示の義務化に関して、各国の法令等に基づき、企業活動においてデータの共有・開示が義務付けられる懸念がある。
  - 例えば EU データ法においては、EU 域内のコネクテッド製品・サービスの生成・加工データを対象に、製品・サービスの利用者・ユーザーに対して生成データへのアクセスを可能とすることや、ユーザーの要望に応じたデータ提供や第三者開示を義務付けている。製品販売者にとっては、製品開発・仕様変更等によるコスト増加や、提供・開示されるデータの範囲によっては製品のノウハウの流出が懸念される。
  - EU 電池規則においては、原料取得から最終廃棄・リサイクルまで製品ライフサイクル全体を通じて、カーボンフットプリント（CO2 排出量）や企業デューデリジェンス・監査（環境汚染・人権侵害のリスク）などの情報開示が義務付けられ、OEM（完成品メーカー）やサプライヤにとって、データの収集・可視化のためのコスト増加や、対応できなかった際の域内での販売差し止めが懸念される。また、欧州域内に拠点を置く認証機関が認証を行うと定められており、サプライチェーンの情報や電池組成（設計情報）が蓄積される機関や国・地域におけるリスクを適切に評価する必要がある。
  - また、今後、国際的に様々な ESG・サステナビリティに関連する規制が策定・施行されることが想定される。例えば、EU 企業持続可能性デューデリジェンス指令案（CSDDD 指令案）は、2027 年の適用開始を想定し、自社バリューチェーン上における人権、環境関連の悪影響を管理・特定・軽減する取組の実施と活動状況の公表を義務付けており、広範なデータ開示が求められる可能性がある。

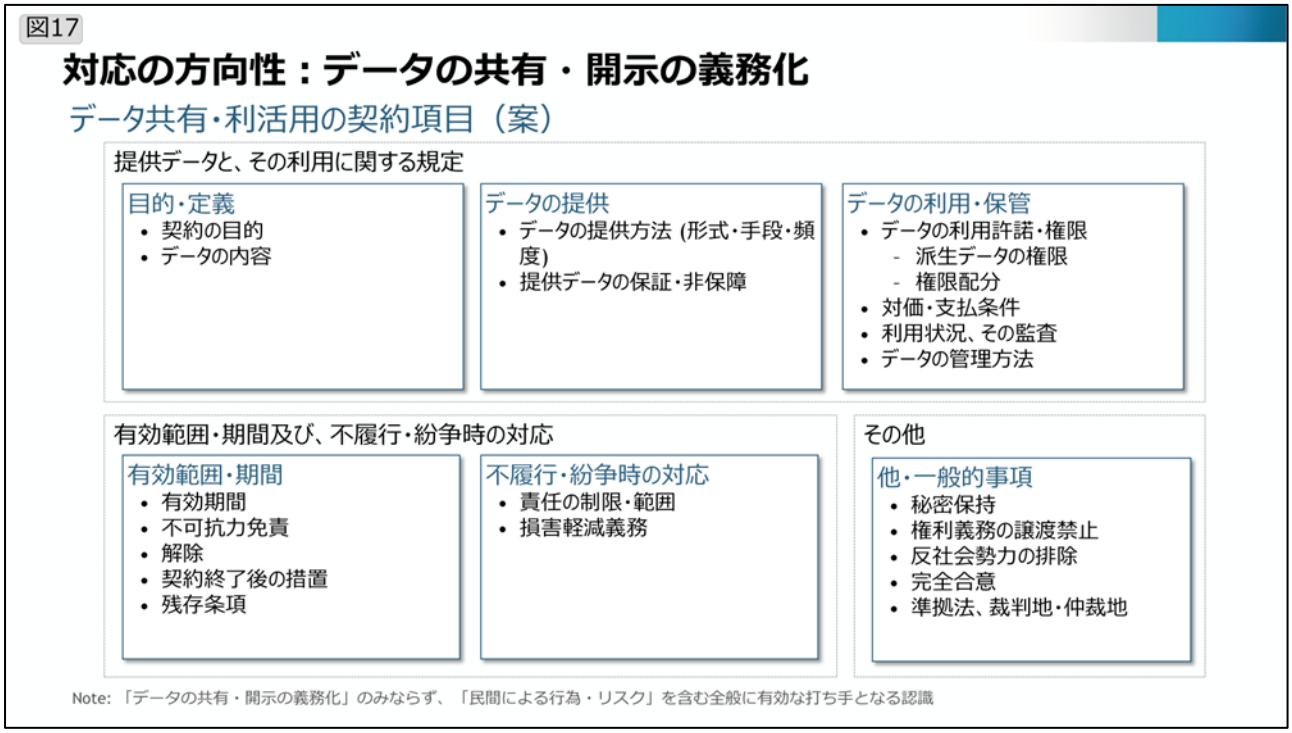
- これらの電池規則や ESG・サステナビリティに関連する規則では、各社が自社や取引関係(取引契約）の情報だけでなく、サプライチェーン全体にわたって直接取引のない企業の情報も集める必要があり、情報収集の負担・コストが大きいことが想定される。また、4.3.1「データ移転・事業活動の制限（ローカライゼーション）」で触れたような措置によって特定地域・国の取引先からデータの移転・取得が困難になった場合に、法令順守に必要な情報を開示できなくなるリスクが存在する。

- モニタリングにおいて、4.3.1「データ移転・事業活動の制限」と同様に、「対象となるデータ」、「実施プロセス」についての把握を行い、内容を検討しつつ、定期的に法規制の検討の進捗や内容の更新有無について確認することが推奨される。
  - 対象となるデータに関して、EU データ法においては、現状、コネクテッド製品又は関連サービス、データ処理サービスを提供する場面等を対象に、対象データの範囲・定義について EU のエキスパートグループにおける議論をはじめとして具体化が進められている。関連製品の販売者にとって、対象データが現在独占的に収集している保守のためのデータか、ユーザー開示・利用を前提としている機器の稼働データかによっても、受ける影響・インパクトが変わり得るため、今後法規制の具体化に伴い、対象となるデータの定義について注視が必要となる。
  - 実施プロセスに関して、データの開示に伴い、誰に・どの範囲まで公開されるか、公開先でどのように利活用されるかの想定等についても、把握・確認することが推奨される。
- 打ち手として、取引先の要望に応じたデータの公開・開示が想定される場合には、開示の範囲や開示に際する通知・対応等について、事前に取引先と適切な契約・取り決めを行うことが有効であることが考えられる。データ共有・利活用に係る契約に関して、基本的に合意すべき項目案は次のとおり（図 17）。なお、これは、本リスクのみならず、4.1「リスクと打ち手の方向性(サマリ)」における記載のとおり、「民間企業による行為・リスク」を含む全般に有効な打ち手となり得る。
  - 基本的に合意すべき項目の分類として、「提供データとその利用に関する規定」、「有効範囲・期間及び不履行・紛争時の対応」、「その他・一般的事項」等が考えられる。これらの関連項目について、全体的な合意が推奨される。
  - 上記の中で、法令ごとの内容・要望事項に応じて、適切に関係者間で取り決めを検討・合意することも有効と考えられる。例えば、EU データ法で、ユーザー又はユーザーの代理人による要求に応じて第三者に対するデータ開示を行う場合、製品の販売者にとって、ユーザーとの間で事前に第三者共有範囲やその条件を取り決めておくことは有効であると想定される。また、EU 電池規則で、サプライヤが OEM（完成品メーカー）へ CFP（CO2 排出量）や DD（環境汚染・人権侵害の違反リスク）のデータ開示・提供を求められる際、サプライヤにとって、OEM との間で効率的なデータ共有・連携のための提供内容・計算ロジックや提供方法・フォーマット方法等を取り決めておくことは有効であると想定される。
  - EU データ法との関係では、ユーザー・データ保有者、データ保有者・データ受領者、ユーザー・データ受領者の 3 つの契約関係を規律する Model Contractual Terms（MCTs）や、クラ

ウドサービス等のデータ処理サービスの提供者とそのユーザーとの間の契約についての Standard Contractual Clauses（SCCs）が検討されており、2025 年 9 月の適用開始までに公表される予定である。ただし、それらは、GDPR の越境移転規制に対応するための SCCs のように、そのまま利用するものではなく、それらをベースに事業者が契約条項を作成することが念頭に置かれていることに注意が必要である。

– 企業間におけるデータ共有・利用に関する契約については、「AI・データの利用に関する契約ガイドライン」[18]や「データ連携基盤規約 Ver.1.0」（経済産業省）[19]においてひな形となるモデル規約等が記載されており、更なる詳細内容に関して参照されたい。

図17




**（補論）法の抵触、越境データに関する政策インデックス**

- 企業のビジネスが複数国に展開される中で、異なる国・地域の法規制に対応すべき場面が増えている。
- 各国・地域で異なる法規制が存在する中で、内容を異にする複数の法律が同時に適用される法の抵触が生じていないかについても、認識・評価することの重要性が増している。
- 国際的な信頼できる自由なデータ流通・移転を通じて、デジタル経済の成長・技術革新を目指す業界横断型の企業連盟である Global Data Alliance では、100 の経済圏における越境データ

[18] https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pdf

[19] https://www.meti.go.jp/policy/mono_info_service/digital_architecture/model_kiyaku.pdf

政策を評価した[越境データ政策インデックス(Cross-Border Data Policy Index)][20]を 2023 年に発表している。地域別の政策の特性・概要を把握する上で、参考にされたい。

## 5 終わりに

- 第 1 章「はじめに」における記載のとおり、本マニュアルでは、議論の網羅性の担保ではなく、国際データガバナンスの考え方の方向性及びいくつかの具体例の提示を目指し、情報の整理を行った。本マニュアルで取り上げた主要リスク以外にも、企業におけるデータ共有・利活用には数多くの実例が存在し、その一部を参考資料 B 個別ケース・事例紹介として別添するため、参照されたい。
- （残論点、他検討との関係性・接続を更新）
- また本 Ver.xx は発行時点(2024 年 12 月)における制度・状況認識に基づいて作成されたものとなり、今後継続的なアップデート・更新を行うことを想定する。

[20] https://globaldataalliance.org/resource/cross-border-data-policy-index/

**参考資料 A　打ち手・措置のリスト**

**参考資料 B　個別ケース・事例紹介**

## 産業データサブワーキンググループ

参 加 者 一 覧

（委　　員）

| | | |
|---|---|---|
| 座長 | 生 貝　直 人 | 一橋大学大学院 法学研究科　教授 |
| | 石 井　啓 之 | トヨタ自動車株式会社 IT マネジメント部産業データ流通基盤 G　GM |
| | 石 原　　修 | 株式会社日立製作所 マネージド＆プラットフォームサービス事業部<br>主管技師長 |
| | 和 泉　恭 子 | 一般社団法人日本知的財産協会　常務理事 |
| | 河 野　浩 二 | 独立行政法人情報処理推進機構　総務企画部 特命担当部長<br>調査分析室長 |
| | 鈴 木　俊 宏 | 日本オラクル株式会社 事業戦略統括 スタンダードストラテジー＆<br>アーキテクチャ/政策渉外担当　シニアディレクター |
| | 直 江　智 子 | Global Data Alliance　BSA ｜ ザ・ソフトウェア・アライアンス<br>ディレクター ポリシー担当 |
| | 中 島　一 雄 | ロボット革命・産業 IoT イニシアティブ協議会<br>インダストリアル IoT 推進統括 |
| | 浜 田　理 恵 | 三菱電機株式会社　法務・知的財産渉外部 知渉四グループ 兼<br>DX イノベーションセンター 戦略企画部　グループマネージャー |
| | 平 見　健 太 | 長崎県立大学 国際社会学部　准教授 |
| | 藤井　康次郎 | 西村あさひ法律事務所・外国法共同事業　パートナー・弁護士 |
| | 若目田　光生 | 一般社団法人データ社会推進協議会　理事 |
| | 渡邉　真理子 | 学習院大学 経済学部経営学科　教授 |

（敬称略五十音順）

（オブザーバー）

デジタル庁 国民向けサービスG 国際戦略
総務省 国際戦略局 参事官室
個人情報保護委員会事務局

（事務局）

経済産業省　商務情報政策局　国際室
ボストン・コンサルティング・グループ合同会社