経済産業省

産業データの越境データ管理等に関するマニュアル

令和７年１月27日

経済産業省

目次

参考資料

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。それらの中には、個人情報を含むか否かを問わず、企業が保有する産業データ全般を対象として、データの越境移転の制限（データローカライゼーション）や、政府による広範なアクセス（ガバメントアクセス）を可能とする規則[1]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、国際的な企業活動における制約要因になることに加えて、中長期的に我が国の産業全体での競争力の強化及び企業横断でのデジタル基盤の確立・普及に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、これまで議論が積み重ねられてきた個人情報保護法制以外のデータ関連法に焦点を当て、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ことを目指し、企業における産業データの越境・国際流通に係るデータ管理（以下「越境データ管理」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・利活用に取り組む際の主要な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の創造や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の強化や、企業横断的なデジタル基盤の確立にも寄与することを狙う。

[1] 本マニュアル 4「主要な関連法規制（EU・中国・米国）」参照

1.2 想定読者と留意点

- 本マニュアルは、企業の規模によらず、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、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等の実務担当者を、主要な読者と想定する。データ管理に関連する部門や担当者が限定的と考えられる中小企業においても、データを国際的に共有・利活用する際のデータ管理の考え方・プロセスを知り、その重要性を理解する一歩として、本マニュアルが活用されることを想定する。
- 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、越境データ管理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、まずは越境データ管理のステップを示すとともに、いくつかの想定リスクの提示を通じて、適切な情報提供を目指す。
  - 本マニュアル 5「想定リスクと打ち手」に、想定されるリスクと企業による対応の具体例を記載する。ただし、これらは、4「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を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用されるものではない。
- 本マニュアルは、法令のように強制力のある規律を設けたり、各国の法規制について公式な解釈を示すものではなく、現在の越境データ管理において生じ得るリスク及び打ち手の具体例を取りまとめ、企業・産業横断的な共通認識の形成を促すものである。

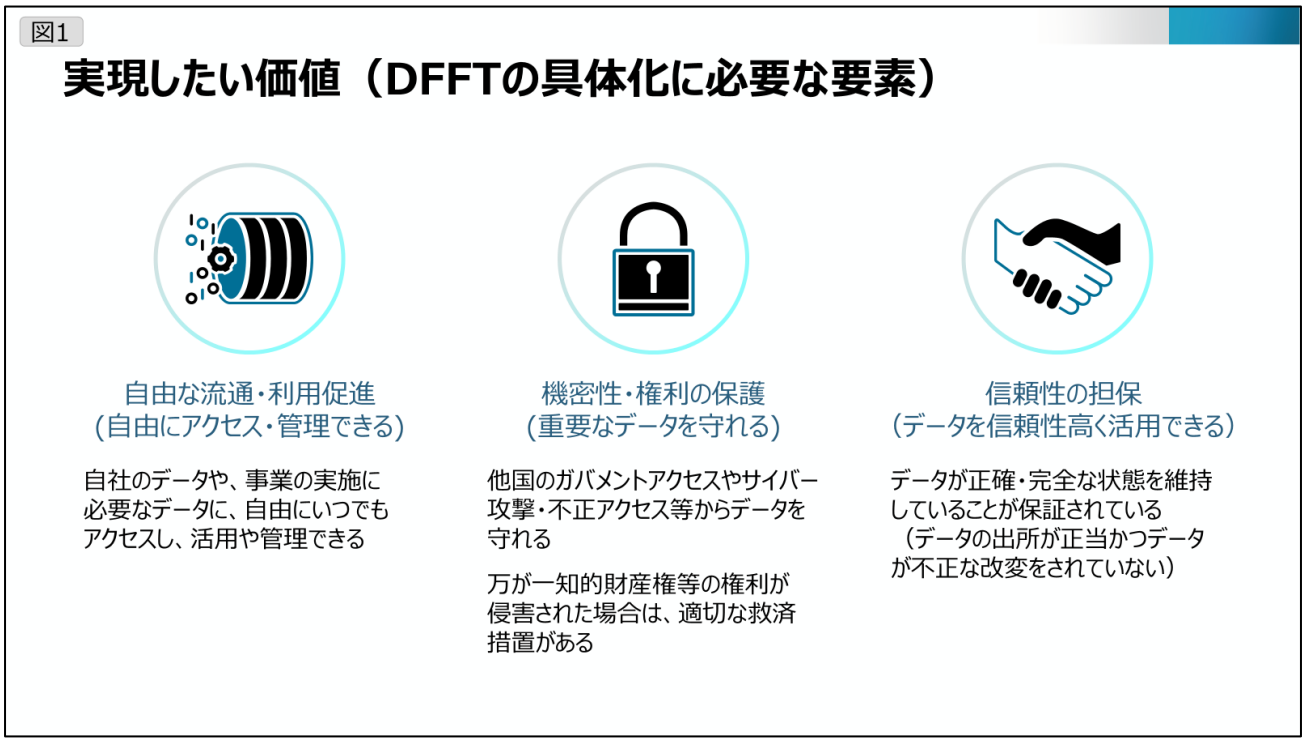
2 検討の範囲と位置付け

2.1 検討の範囲

2.1.1 検討の前提

- 本マニュアルは、データが国際的に共有・利活用される場面に焦点を当てる。
  - 国内・海外等で生成・取得されたデータが海外・第三国等に越境移転する場面に加えて、必ずしも越境移転しなくとも海外で生成・取得されたデータが同じ域内・国内で共有・利活用される場面も対象に含むものとする。
- 日本政府は、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[2]。本マニュアルでは、DFFT の具体化に必要な要素である「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（図 1）。

図1

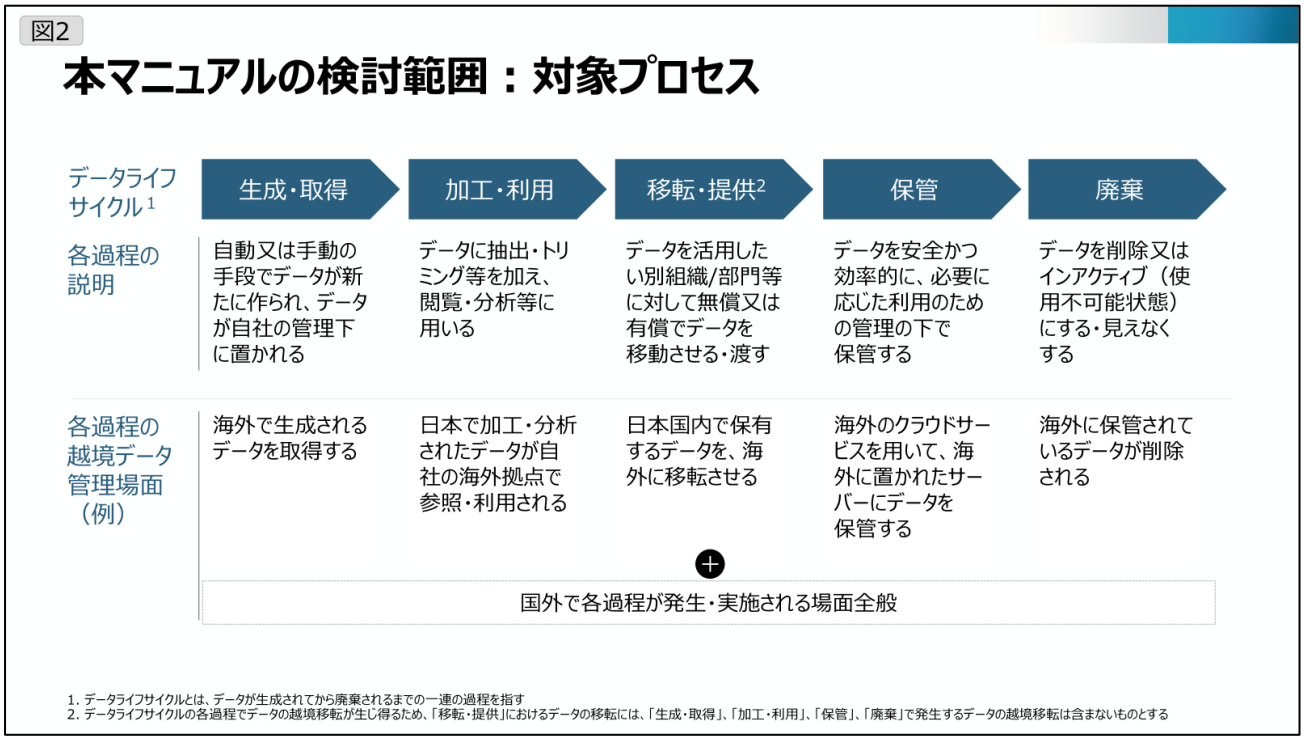


[2] デジタル庁「DFFT」 https://www.digital.go.jp/policies/dfft

2.1.2 検討の対象（プロセス、データ、リスク）

- 企業におけるデータ共有・利活用は、その性質上、広範な企業活動が対象に含まれ得る。本マニュアルにおける検討の範囲として、「対象となるプロセス」、「対象となるデータ」、「対象となるリスク」を定義する。
- 「対象となるプロセス」（図 2）については、データライフサイクルにおける各過程おいて、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ことや見えなくすることも含まれる。

図2



- 「対象となるデータ」（図 3）については、データが国際的に共有・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[3]。個人情報保護の観点から議論が積み重ねられてきた「パーソナルデータ」に比べ、これまで体系的な検討が限られていた「非パーソナルデータ」の領域に焦点を当て、事例の深堀を行う。
  - 本マニュアルにおいては、「パーソナルデータ」には、個人情報、仮名加工情報、匿名加工情報、個人関連情報を含む情報等、日本の個人情報保護法及び各国・地域の個人情報保護法

[3] 越境データ管理に関わる各国の個人情報保護法制への対応については、例えば個人情報保護委員会「民間企業における個人データの越境移転、海外法規制対応に関する実態調査」（2023 年 12 月）<https://www.ppc.go.jp/enforcement/international_materials/?_ga=2.261802949.956306041.1737598960-1996458472.1737598960> 等を参照されたい。

制の保護対象となるデータが含まれるものとする。「非パーソナルデータ」は、データ全般のうち「パーソナルデータ」に該当しないものをいい、本マニュアルでは特に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」を念頭に置く。

- 実務上、上記の「パーソナルデータ」と「非パーソナルデータ」の区分は、各国・地域の法制によるため、相対的・流動的になり得る。そのため、非パーソナルデータに関する対応を行う際にも、日本及び各国・地域の個人情報保護法制の遵守に留意する必要がある。

図3

本マニュアルの検討範囲：対象となるデータ

データカテゴリ		データカテゴリの概要	データ例
非パーソナルデータ[1]	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 • 社会基盤を支える重要なインフラに関する技術情報や運用データ • 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	• 取引先に関するデータ（取引価格、取引先情報等） • 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データ等） • 取引先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） • 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） • 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、安全保障・営業・技術データ以外の事業活動に伴う情報	• 経営戦略に関わるデータ（事業計画、投資計画に関するデータ等） • 企業のセキュリティに関するデータ（インフラ、BCPに関するデータ等）
パーソナルデータ		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） • 仮名加工情報（他の情報と照合しないと特定の個人を識別できない情報） • 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） • 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）

1. 非パーソナルデータは、データ全般のうち「パーソナルデータ」に該当しないものを指す

- 「対象となるリスク」については、前記「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」ことを対象とする（図 4）。

図4

本マニュアルの検討範囲：対象となるリスク

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

自社のデータや、事業の実施に必要なデータに対して、自由にアクセスできない、活用や管理が行えない

重要なデータ（機密性・権利）が守れない

他国のガバメントアクセスやサイバー攻撃・不正アクセス等によってデータに強制的にアクセスされ、自社の重要なデータの機密性や権利が守れない

データが信頼できない

データが正確・完全な状態を維持していることが保証されていない（データの出所、データが不正な改変がされていないことが担保されていない）

2.2 検討の位置付けと関連ガイドライン

- 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において公表予定の「データガバナンス・ガイドライン（案）」は、経営者視点からデータガバナンス全般について広範に捉えている。本マニュアルは、「データガバナンス・ガイドライン（案）」の「越境移転の現実に即した業務プロセス」に対応しており、実務的な側面に焦点を当てる。
- 加えて、関連する内容が取りまとめられたガイドライン等が複数存在している（図 5）。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、取りまとめたものである。
  - 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」[4]、「秘密情報の保護ハンドブック」[5]、「AI・データの利用に関する契約ガイドライン」[6]、「限定提供データに関する指針」[7]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 6）。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。

[4] https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework_1_1.pdf
[5] https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf
[6] https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pdf
[7] https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf

図5

関連ガイドラインの概要

	目的	想定される対象読者	本マニュアルと関連する内容	発行年
1 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 (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 • 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 システム設計・運用に関わるエンジニア 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 • 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 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 • 最終改訂 2024年
2 秘密情報の保護ハンドブック (経済産業省 知的財産政策室)	企業における秘密情報漏えい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 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 • 情報の評価、秘密情報の決定 情報漏えい対策の選択及びそのルール化 秘密情報の管理にかかる社内体制の在り方	2016年 • 最終改訂 2024年
3 AI・データの利用に関する契約ガイドライン -データ編- (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 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 • クロス・ボーダー取引における留意点 主な契約条項例	2018年 • 最終改訂 2019年
4 限定提供データに関する指針（参考） (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 企業の契約担当者や法務担当者 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 • 最終改訂 2024年

図6

本マニュアルに対する関連ガイドラインの主要参照先

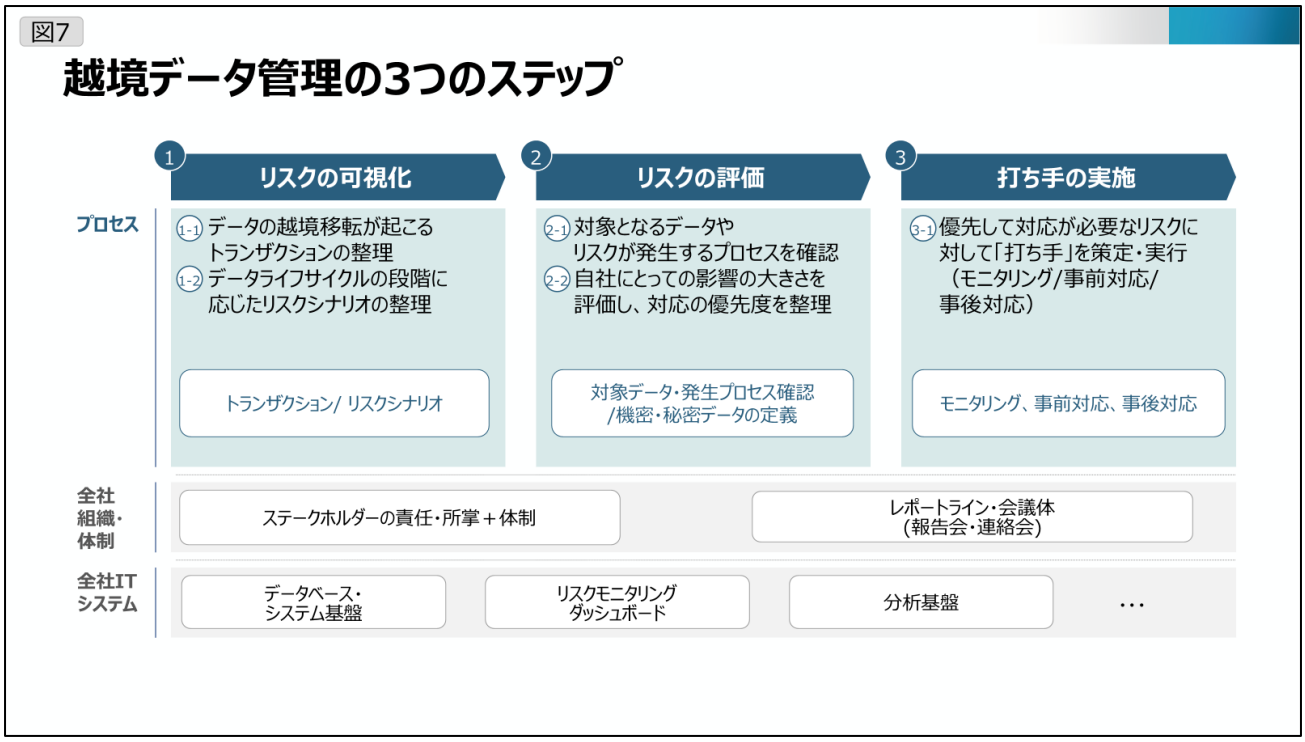
本マニュアル(章)		関連ガイドライン	主要参照先	概要
3 越境データ管理の3つのステップ	3.2 第１のステップ (リスクの可視化)	1 協調的なデータ利活用に向けたデータマネジメント・フレームワーク	2. 本フレームワークにおけるデータマネジメントのモデル • 2-2-1 モデル化（「イベント」）	データライフサイクルの定義及び代表的なリスクの記載
		4 限定提供データに関する指針	Ⅲ.「不正競争」の対象となる行為について (総論)	データライフサイクルの過程における不正競争の対象となる行為の定義
	3.3 第２のステップ (リスクの評価)	2 秘密情報の保護ハンドブック	2章 保有する情報の把握・評価、秘密情報の決定 • 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、機微技術情報等）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 主要な関連法規制（EU・中国・米国）		1 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 • 2-2-1 モデル化（「場」）	データに対する規範の例示 • 各国・地域の法令、組織の内部規則等
		3 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） • (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 • 越境移転規制、外為法、準拠法等
5 想定リスクと打ち手		2 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 • 3-2 分類に応じた情報漏えい対策の選択 • 3-3 秘密情報の取扱方法等に関するルール化 • 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
		3 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 越境データ管理の 3 つのステップ

3.1 全体像と検討のフレームワーク

- 本章では、越境データ管理について、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。フレームワークとして、3 つのステップ「①リスクの可視化」、「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 7）。
  - なお、越境データ管理のためには、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、これらは越境データ管理の観点だけからではなく、企業活動全般を踏まえて検討することになるため、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、越境移転の現実に即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。

図7

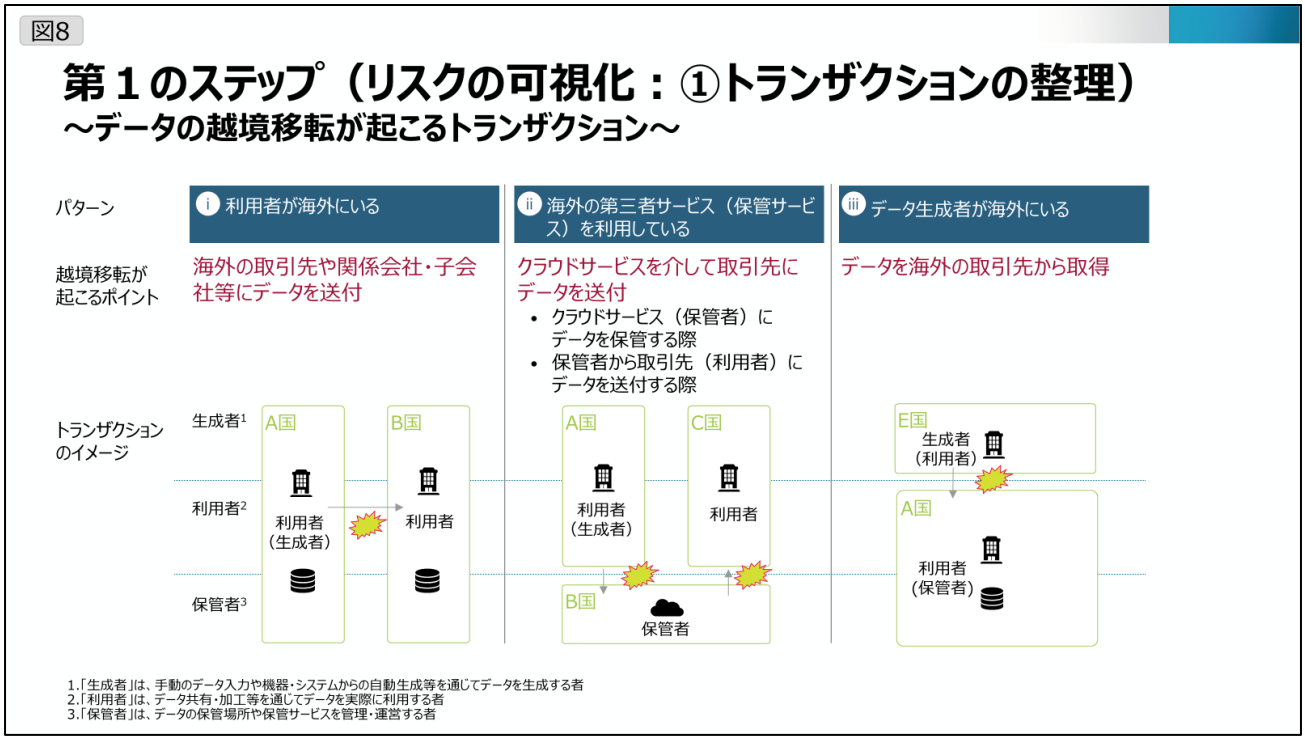


3.2 第 1 のステップ（リスクの可視化）

3.2.1 トランザクションの整理

- リスクの可視化では、まずは想定するデータの共有・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、どこで国際的な共有・利活用が行われ、越境移転が起こるか把握する。
- 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」は手動のデータ入力や機器・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。ただし、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。
  - 「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。
- 実務においては、事業内容によって、無数のトランザクションが存在する。ステークホルダーの分類を念頭に、トランザクション（何のデータが、ライフサイクルのどの段階で、誰から誰に、どのような手段で共有されるか）を整理し、その中に海外企業・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など、データのロケーションを把握することが重要となる。
- データの越境移転が起こるパターンとして、例えば、「利用者が海外にいる」、「海外の第三者サービス（保管サービス）を利用している」、「データ生成者が海外にいる」が想定される（図 8）。

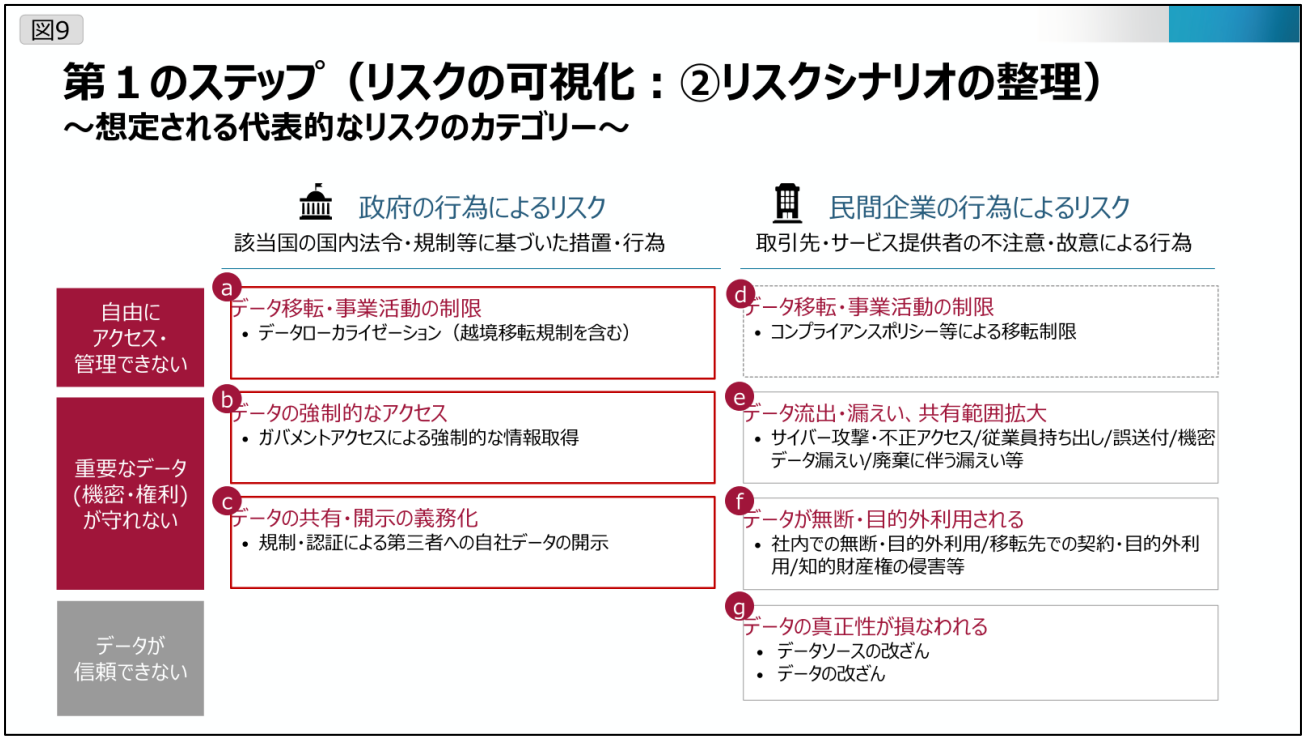
図8



3.2.2　リスクシナリオの整理

- 3.2.1「トランザクションの整理」で把握したデータのロケーション、データの内容、データ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。
- 本マニュアルでは、前記 2.1.2「検討の対象（プロセス、データ、リスク）」のとおり、「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」ことを検討対象のリスクとしている。各リスクには、当該国の国内法令・規制等に基づいた措置・行為によって発生するリスク（以下「政府の行為によるリスク」という。）と、取引先・サービス提供者の不注意・故意による行為等の民間企業の行為によって発生するリスク（以下「民間企業の行為によるリスク」という。）が存在する。
- これらのリスクで想定される代表的なカテゴリーとして、政府の行為によるリスクにおける「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」、民間企業の行為によるリスクにおける「d. データ移転・事業活動の制限」、「e.データ流出・漏えい、共有範囲拡大」、「f.データが無断・目的外利用される」、「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 9）。

図9



3.3 第 2 のステップ（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、第 1 のステップで可視化されたリスクについて評価し、対応の優先度を付けることが有効と考えられる。
- 想定されるリスクに関して、対象となるデータ（トランザクションの中で、何のデータがリスクの対象となるか）やリスクの発生プロセス（リスクを生じさせる行為の発生プロセスやその条件、関連する保護措置の有無等）を確認する。
- 対象となるデータやリスクの発生プロセスを踏まえ、自社にとっての影響の大きさを評価することで、対応の優先度を判断する。
  - 本マニュアルにおいては、企業にとって機密性が高いデータ及び秘密保持契約の対象となるデータを合わせて、機密・秘密データと定義する。自社として保護すべき機密・秘密データを定義し、リスクの対象となるデータにおいて、機密・秘密データに該当するものが含まれていないか確認を行うことが推奨される。
  - 機密・秘密データの判断は、企業によって異なる（図 10）。例えば、独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」[8]の第 2 部（8）「詳細リスク分析の実施方法」において、機密情報の評価基準が記載されている。また、「秘密情報の保護ハンドブック」[9]の第 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。加えて、リスクの発生プロセスを踏まえ、リスクの予見可能性（発生プロセスや条件が明確か）や、発生時の保護措置の有無とその適用可能性（意義申立てや協議が行えるか、損害が補填されるか等）についても、確認・評価を行うことが推奨される。
  - 一般的に、機密性のレベルが上がるほど、データの共有・利活用について考慮すべき事項が多くなる。

[8] https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

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

図10

第２のステップ（リスクの評価）
～リスクの評価の流れと秘密情報の決定に当たって考慮すべき観点～

リスクの評価の流れ

リスクの対象となるデータ・発生プロセスの確認

- 想定されるリスクに関して、対象となるデータ（トランザクションの中で、何のデータが対象となるか）やリスクの発生プロセス（リスクを生じさせる行為の発生プロセスや条件、関連する保護措置の有無等）を確認する

自社における影響の評価・対応優先度の整理

- 自社として保護すべき機密・秘密データを定義し、対象となるデータにおいて、機密・秘密データに該当するものが含まれていないか確認する
- リスクの発生プロセスを踏まえ、リスクの予見可能性や、発生時の保護措置の有無と適用可能性について、確認・評価を行う
- 自社のリソースを踏まえ、対応の優先度を決定する

機密・秘密データの決定に当たって考慮すべき観点の例

営業データ

- ❑ 自社独自のデータであり、それが漏えいした場合、自社の競争力が低下するものか否か（取引価格や取引先に関するデータ、接客マニュアル、公表前のデザイン等）
- ❑ その漏えいにより、法令違反や他社との契約違反等となり、自社の社会的信用の低下を招いたり、他社との信頼関係を毀損させるものか否か（顧客の個人情報、受託契約・ライセンス契約・Ｍ＆Ａ交渉におけるＮＤＡ等の他社との契約等により限定的に開示された営業データ・限定提供データ 等）

技術データ

- ❑ 市場に流通する自社の製品等を分析することによって容易にその製品に用いられている技術が判明してしまい、他社がすぐに追いつくことができる技術に関するものか否か
- ❑ 権利化した場合であっても、権利侵害の探知や立証が難しいものか否か
- ❑ その漏えいにより、法令違反や他社との契約違反等となり、当該他社との信頼関係を毀損させるものか否か
- ❑ 通信技術や試験方法等の社会基盤や技術標準となる技術データであり、自社利益の最大化のためには当該技術の市場の拡大が求められるものか否か

3.4　第 3 のステップ（打ち手の実施）

- 第 2 のステップで優先して対応が必要と判断したリスクに対して、打ち手を策定し、実行する。
- 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 11）。
  - 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：保護措置・責任追及（適切・迅速なステークホルダーへのレポート）、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）、法的な措置（契約の締結等）、技術的な措置（暗号化・アクセス制限等）に分けられる。
- 詳細は 5「想定リスクと打ち手」及び参考資料 A「打ち手のリスト」を参照されたい。

図11

3.5 リスクと打ち手の整理

- ここでは、3.2.2「リスクシナリオの整理」で定義した代表的なリスクのカテゴリーに対して、有効と考えられる打ち手を整理する。
- 有効と考えられる打ち手の方向性は、行為の主体（政府又は民間）によって異なる（図 12）。
- 「政府の行為によるリスク」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制限及び介入行為を国家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 13）。なお、データローカライゼーションに関する措置のうち、国内保存要求、国内処理要求、越境移転禁止規制[10]は、前者の「政府の行為によるリスク（直接的）」に、条件付きで越境移転を認める規制は、政府が企業に対して条件への準拠を求めることから、後者の「政府の行為によるリスク（間接的）」に該当すると考えられる。
  - 前者の「政府の行為によるリスク（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（モニタリング）し、打ち手を講じることが考えられる。主な打ち手として、リスクの発生確率を下げる及びインパクトを低減する事前対応（データの分散化や保管場所の精査・選定等）を検討すること、また、リスクが発生した際に早期の事後対応を行うことが有効と考えらえる。詳細を後記 5.1「データ移転・事業活動の制限（データローカライゼーション）」及び 5.2「データの強制的なアクセス（ガバメントアクセス）」に記載する。
  - 後者の「政府の行為によるリスク（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（モニタリング）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・取決め（リスク発生時の報告義務や過失があった場合の免責事項等）といった事前対応を行うことも有効であることが考えられる。詳細を後記 5.3「データの共有・開示の義務化」に記載する。
- 「民間企業の行為によるリスク」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、企業間における取決めや意思決定によって、柔軟に打ち手を講じることができる。打ち手として、例えば、技術的な対応・セキュリティ対策（アクセス制限や持ち出しの制御、データの保護・暗号化等）[11]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といった事前対応、発生事項や日時を早期にステークホルダーに通知・公表するといった事後対応が有効と考えらえる。

---

[10] データローカライゼーション措置の分類については、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」（2024 年 3 月）<https://www.rieti.go.jp/jp/publications/dp/24j007.pdf>を参考に、5.1「データ移転・事業活動の制限（データローカライゼーション）」に詳細を記載する。

[11] 日本の個人情報保護法について、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」<https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/>の「10-6 技術的安全管理措置」において手法の例示がされているため、参照されたい。

なお、「民間企業の行為によるリスク」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。商慣習や管理体系の異なる海外企業との取引が増えることによる間接的な影響は想定されるが、データの国際的な共有・利活用や越境移転によって直接的に発生するリスクではない。

- 企業間の契約においては、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。
- 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ことや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、漏えいや目的外利用に対して特に留意が必要となる。

- 本マニュアルにおいては、データの国際的な共有・利活用や越境移転を検討の範囲とする観点から、特に「政府の行為によるリスク」に焦点を当て、以後 4「主要な関連法規制（EU・中国・米国）」及び 5「想定リスクと打ち手」の記載を行う。

図12

リスクと打ち手～概要～

			リスクの概要・特徴	有効と考えられる打ち手の方向性
政府の行為によるリスク	直接的	a データ移転・事業活動の制限（データローカライゼーション）[1]	• 当該国の国内法令・規制に基づき、政府が企業に対して直接的に行為を実施 • 地域・国別の最新の法令・規制の把握の難しさに加えて、一部地域・法令では予見性が高くない場合も想定される	モニタリング ○ 事前対応 ○ 事後対応 • 関連する法規制の内容とその影響を正しく把握する • リスク自体の回避又は低減する事前対応（データの分散化や保管場所の精査・選定等）を検討する • リスクが発生してしまった場合に、早期の事後対応（発生事項や日時を早期にステークホルダーに通知・公表等）を行う
		b データの強制的なアクセス（ガバメントアクセス）		
	間接的	c データの共有・開示の義務化	• 法令・規制に基づき、政府が企業に対して何かしらの行為を命じる	モニタリング ○ 事前対応 ○ 事後対応 • 関連する法規制の内容とその影響を正しく把握する • 発生時に備えて、取引先と適切な契約・取決め（リスク発生時の報告義務や過失があった場合の免責事項等）を行う
民間企業の行為によるリスク		d～g データ移転・事業活動の制限 データ流出・漏えい 無断・目的外利用 真正性・公平性	• 取引先・サービス提供者による不注意（管理不備）・故意によって発生	モニタリング ○ 事前対応 ○ 事後対応 • 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 • 発生時に備えて、取引先と適切な契約・取決めを行う • リスクが発生してしまった場合に、早期の事後対応（発生事項や日時を早期にステークホルダーに通知・公表等）を行う

1. 条件付きで越境移転を認める規制も含まれ得るが、当該措置は政府が企業に対して何かしらの行為を命じる間接的な規制であるため、「政府の行為によるリスク（間接的）」に対する打ち手（企業間の契約で越境移転の条件に対応する旨の取り決めを行うなど）が有効となる

図13

リスクと打ち手
～政府の行為によるリスクと具体的な打ち手の例～

凡例 具体的な打ち手の例

		組織的		法的	技術的
		発生確率を下げる・予防	インパクトを低減する		
直接的	a データ移転・事業活動の制限（データローカライゼーション）[1]	重要データの分散化・複製 • 保管先・利用サービス確認 • 重要データの分散化 要望事項への対応 • ローカルデータセンター設立 • 現地運営チームの立上 例外措置への準拠・対応	代替データ選定・業務見直し • 代替業務・データによって影響を抑える	取引先との契約締結 • 移転・保管に関する許可取得義務 • 過失があった際の免責事項や賠償内容	暗号鍵の保管 • 暗号鍵の保管によって要望対応できるケースの場合
	b データの強制的なアクセス（ガバメントアクセス）	保管場所の精査・選定 • 保管先・利用サービス確認 • 保管場所の選定・データ移転 保管データの加工・匿名化 データ移転の社内ガイドライン策定	–	取引先との契約締結 • ガバメントアクセス発生時の報告義務 • 過失があった際の免責事項や賠償内容	データの暗号化 • 強制アクセスされた際に内容が分からないよう暗号化
間接的	c データの共有・開示の義務化	データ開示を前提とした戦略・業務の見直し	取引先との契約締結 • ガバメントアクセス発生時の報告義務 • 過失があった際の免責事項や賠償内容	取引先とのデータ連携・活用の契約、ガイドライン策定 • 対象データ、公開範囲や利用規約等を規定 • 法的要望の折り込み	電子すかし・ブロックチェーン • データの不正コピーや改善の防止

1. 条件付きで越境移転を認める規制も含まれ得るが、当該措置は政府が企業に対して何かしらの行為を命じる間接的な規制であるため、「政府の行為によるリスク（間接的）」に対する打ち手（企業間の契約で越境移転の条件に対応する旨の取り決めを行うなど）が有効となる

4 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、日本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。
- EU においては、パーソナルデータに加えて、広く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、包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（図 14）。
  - 個人情報保護法制に関しては、GDPR[12]において、データの越境移転（欧州経済領域（EEA）域外の第三国又は国際機関から別の第三国への再移転を含む。）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）、Standard Contractual Clauses （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、域内におけるデータ流通の促進および信頼性の確保のための法的枠組みとしてデータガバナンス法[13]が 2022 年 5 月に制定された。
  - さらに、2024 年 1 月に発効し、2025 年 9 月から段階的に施行予定のデータ法[14]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、ユーザーからのアクセス、ユーザーからの要求に応じた第三者に対する FRAND 条件（公正、合理的かつ非差別的な条件）での提供が定められている。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（第 4 条第 1 項）。ユーザーから要求があった場合に、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、FRAND 条件により、透明性のある方法で第三者に提供することが規定されている（第 8 条）。加えて、データを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など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が規定されている（第 14 条及び第 15 条）。

[12] 個人情報保護委員会「EU（外国制度）」https://www.ppc.go.jp/enforcement/infoprovision/EU/

[13] 国立国会図書館「【EU】データガバナンス法の制定」
https://dl.ndl.go.jp/view/download/digidepo_12360274_po_02930205.pdf?contentNo=1

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

- 加えて、EU 電池規則[15]を筆頭に、 Corporate Sustainability Reporting Directive（CSRD）[16]、 Corporate Sustainability Due diligence Directive（CSDD）[17]等、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、トレーサビリティに関わるデータの開示が求められるケースが増えてきている。

- 中国においては、習近平国家主席が提唱した「総体的国家安全観」に国家の安全の維持（経済社会の発展を含む）のための基本的方針が示されており[18]、国家安全法として具体化されている。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）において、国家の情報収集活動への協力やデータローカライゼーションに関して規定されている（図 15）。
  - サイバーセキュリティ法においては、重要情報インフラ運営者が中国国内での運営中に収集、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旨が規定されている（第 37 条）。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（同条）。
  - データセキュリティ法においては、重要情報インフラ運営者が中国国内で収集、発生した重要データの国外移転に係るセキュリティ管理についてサイバーセキュリティ法の規定を適用することが定められている（第 31 条）。重要データの違法な国外移転に対する罰則（第 46 条）がサイバーセキュリティ法よりも更に引き上げられている[19]。
  - 個人情報保護法においては、個人情報について、中国国外への越境移転に必要な対応や要件が定められている（第 3 章）。
  - データ 3 法の規制対象者の範囲及び当該義務の対象となるデータの範囲については解釈や運用において不明瞭なところが存在する。2022 年 9 月に「データ域外移転安全評価弁法」が公布され、重要データは、「一旦改ざん、破壊、漏えい又は違法取得、違法利用等を受けると、国の安全、経済運営、社会の安定、公共の健康及び安全等が脅かされる可能性のあ

---

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

[16] European Union「EN - CSRD Directive」https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464

[17]European Commission「Corporate sustainability due diligence」https://commission.europa.eu/business-economy-euro/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence_en

[18] 新華網「习近平主持召开中央国家安全委员会第一次会议强调 坚持总体国家安全观 走中国特色国家安全道路 李克强张德江出席」（2014 年 4 月）http://www.xinhuanet.com//politics/2014-04/15/c_1110253910.htm

[19] 独立行政法人日本貿易振興機構（ジェトロ）「「データセキュリティ法」の概要」https://www.jetro.go.jp/ext_images/_Reports/01/580a6448fa87f0bb/20210056_04.pdf

るデータ」として定義された（第 19 条）。 そして、2024 年 3 月、国家インターネット情報弁公室（CAC）より、中国データ 3 法の施行について、「データ越境流動の促進および規範化に関する規定」が公布・施行された[20]。この規定により、データ取扱者は、関連規定に従い重要データを識別し、申告しなければならないとされているが、重要データの判断基準について関連部門又は地域から重要データとして告知又は公開・発表されていない場合には、データ取扱者は、重要データとしてデータ域外移転安全評価を申告する必要はないと定められている（第 2 条）。例えば、自動車分野については、「自動車データ安全管理若干規定（試行）」（2021 年 10 月施行）が定められている。

- 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制や、安全保障の観点でのデータに関する規律が設けられている（図 15）。
  - 例えば、CLOUD 法[21]では、犯罪捜査や国家安全保障にかかわるような状況に際して、米国の政府機関が、米国の管轄権に服するプロバイダーに対し、令状等により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（第 103 条(a)(1)、18 U.S.C. Sec. 2713）されている。
- 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・拡張等に伴い、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である。
  - 経済産業省や独立行政法人日本貿易振興機構（ジェトロ）等のウェブサイトにおける各国制度の記載・調査結果[22]も制度の確認に有用であり、必要に応じて、原文の確認が推奨される。また、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ことが推奨される。さらに、影響が大きいと想定される法規制に関しては、専門家への相談が推奨される。
  - 制度整備の際にパブリックコメントの募集が行われる場合には、それに参加し、企業としての懸念点の存在を可視化することも考えられる。

[20] 独立行政法人日本貿易振興機構（ジェトロ）上海事務所調査部「中国のデータ・個人情報の域外移転規制の最新動向（2024 年 3 月時点）」（2024 年 4 月）
https://www.jetro.go.jp/ext_images/_Reports/01/690307ed2a411652/20240004_02.pdf

[21] 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

[22] 経済産業省通商政策局編「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14

主要な関連法規制（EU）

	目的等	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経済領域のデータの流通の促進及び信頼性を確保する	• 域内におけるデータ流通の促進及び信頼性の確保のための法的枠組みが規定、提示されている	–	• 2022年6月発効 • 2023年9月施行
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又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 • 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 • データの開示義務に対応するため、追加的な工数が発生したり、機密データを公開しなければならない可能性がある ガバメントアクセス • 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 • 2025年9月以降、段階的に施行
電池規則（EU）	• 蓄電池（バッテリー）の全ライフサイクルにわたる持続可能性、リサイクル、安全性を強化する	• 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 – 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 – 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） 等	データ共有・開示義務 • バッテリーに関するデータを公開するため、追加的な工数が発生したり、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月発効 • 2024年2月以降、段階的に施行

図15

主要な関連法規制（中国・米国）

	目的等	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）を維持する	• 主に国防に関する原則事項を具体化し基本原則を定めている • データに関する具体的な要求は、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）に支えられる	–	• 2015年施行
サイバーセキュリティ法（中国）	• 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）する	• 個人情報、重要データを中国国内で保存することが求められる • 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 • 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 ガバメントアクセス • 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（中国）	• データ保護を重視し、重要データを定義・保護する	• 「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 • 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 • 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（中国）	• データセキュリティ法のうち、個人データの規制を補完する	• 企業や組織が中国国内から個人情報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 • 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がある	ガバメントアクセス • 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がある	• 2018年施行

5 想定リスクと打ち手

5.1 データ移転・事業活動の制限（データローカライゼーション）

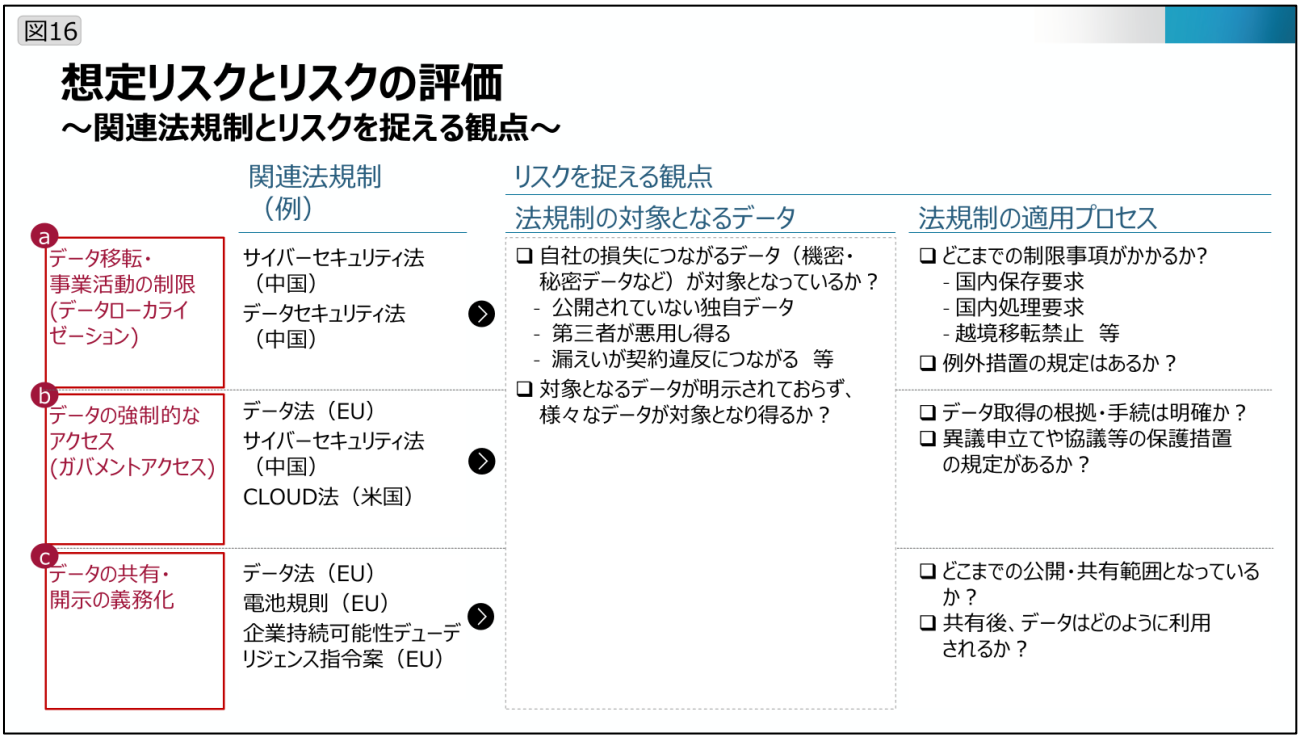
- 「a.データ移転・事業活動の制限」に関して、リスクの可視化において、関連法規制に基づき、データの国内保存の要求、当該国外への移転の禁止、当該国内データセンターの利用義務付け等の措置が課される懸念を把握する。
  - データローカライゼーション措置の分類[23]には、例えば、国内保存要求、国内処理要求、越境移転禁止規制が考えられる。国内保存要求は、データの保存場所を指定するものであり、データのコピーを国内に保存すれば、国外に移転し処理（使用、編集・変更等）することを認める場合を念頭に置いている。国内処理要求は、データの主要な取扱場所を指定し、国外における処理（使用、編集・変更等）は認められな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、例えば中国では、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）において、データローカライゼーションに関して規定されているが、その対象者の範囲及び対象となるデータの範囲に関して、広範かつ不明瞭な定義が残る[24]。例えば、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等といったように広範になっている。また、対象となるデータは、自動車・軍事・工業分野等広範囲にわたり、定義も不明瞭である。重要データであるかどうか、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は越境移転の制限を受ける。
- リスクの評価において、法規制の対象となるデータ及び適用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、自社にとっての影響・インパクトの大きさと対応優先度を判断することが推奨される（図 16）。
  - 法規制の対象となるデータに関して、自社の損失につながるデータ（機密・秘密データ等）が対象となっているか、確認することが推奨される。
  - 対象となるデータに加えて、法規制の適用プロセスとして、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こまでの制限事項があるか、例外措置があるかなどの把握に努めることが推奨される。
  - 特に、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く、制度の対象や解釈について予見可能性が低い場合、企業による移転可否判断が難しくなるため、留

[23] 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」（2024 年 3 月）https://www.rieti.go.jp/jp/publications/dp/24j007.pdf

[24] 同上

意が必要となる。また予見可能性に加えて、制度の運用の変更頻度や法令自体の撤廃の可能性等、制度の安定性についても、留意することが推奨される。

図16

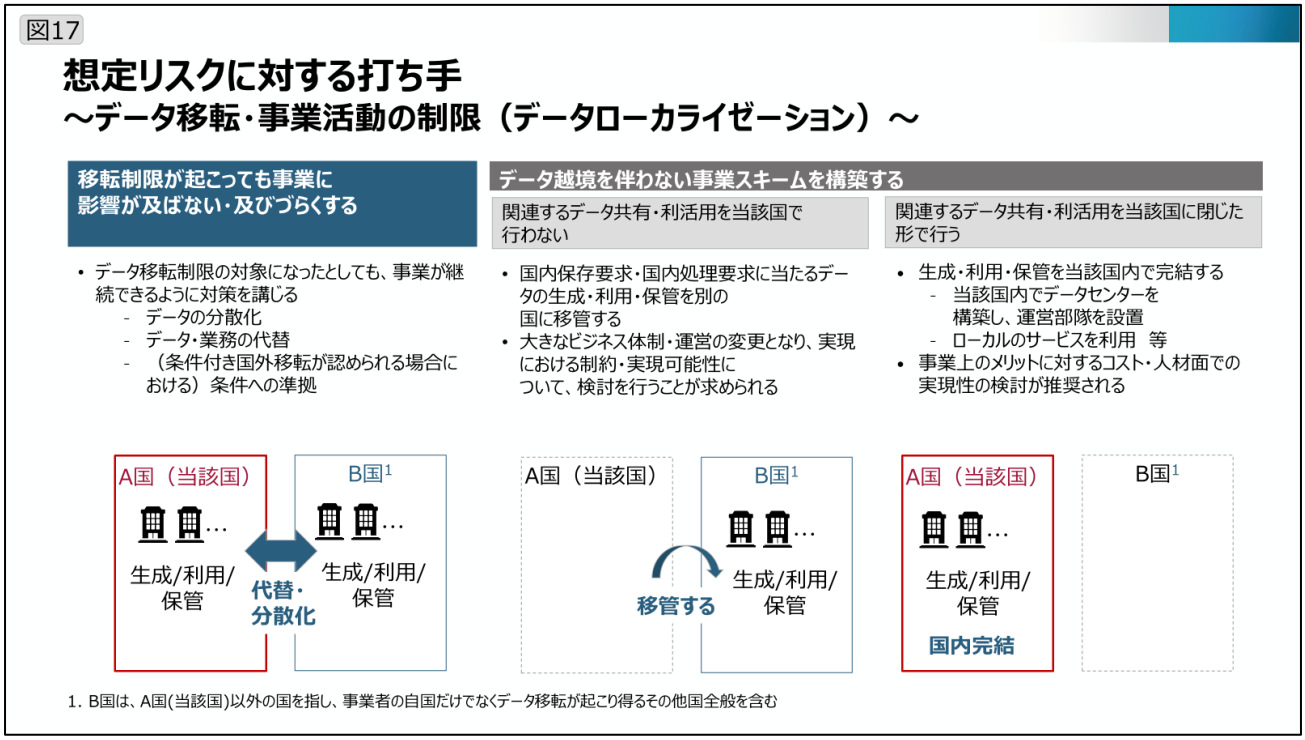


- 打ち手として、主に移転制限が起こっても事業に影響が及ばない・及びづらくする、移転制限自体が起こらないようにデータ越境を伴わない事業スキームを構築するといった対応の方向性が考えられる（図 17）。
  - 移転制限が起こっても事業に影響が及ばない・及びづらくする対応として、当該データが移転制限の対象となっても事業が継続できるように、データの分散化、データ・業務の代替等の打ち手が想定される。国内保存要求（越境移転の制限なし）が課されている場合には、データを複製して国外の拠点に分散して保管することが考えられる。また、国内処理要求又は越境移転禁止規制により国外での利用が制限される場合には、データ・業務の代替として、類似データの活用を検討することが考えられる。後者の場合について、具体例として、グローバルサプライチェーンマネジメントにおいて、各国の生産拠点から本社へ生産データ（稼働のひっ迫度、生産リードタイム、不良品率等）が共有され、本社でグローバルの供給計画が策定される場合を考える。この場合、もし当該国における関連データが越境移転禁止規制によって取得できない場合に、計画精度は下がってしまうと想定されるが、代替データとして過去の供給数の実績に基づき、見込み計画を策定することが想定される。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対応の１つとして、例えば、法規制の導入が検討されているという段階では、関連するデータ共有・利活用を当該国で行わずに、当該国内で行っているデータの生成・利用・保管をそのまま別の国に移管するという手法を取らざるを得ない場合も考えられる。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にも留意する必要がある。
- また、例えば、データ分析サービスを提供する場合に、国内保存要求や国内処理要求に当たる生成・利用・保管のプロセスを当該国内で完結し、サービス提供を行う現地チームの立ち上げを検討するなどの打ち手を検討せざるを得ない場合がある。当該国政府が、データローカライゼーションを義務付けるなど、事業又は株主の利益に深刻な法的リスクや事業リスクをもたらすような規制を措置しようと場合に、企業がこのような選択肢を検討することもあり得るが、この場合にも、複雑な経営判断が求められることに留意する必要がある。

図17



5.2 データの強制的なアクセス（ガバメントアクセス）

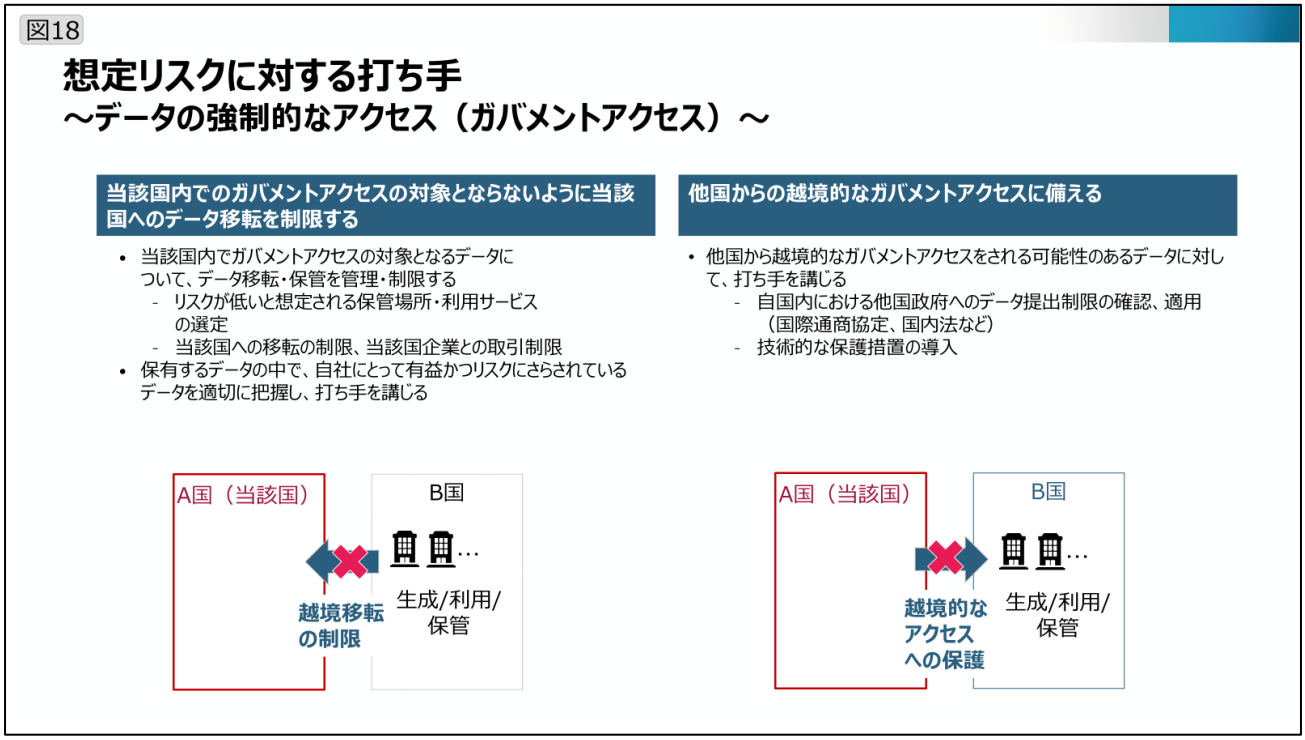
- 「b.データの強制的なアクセス」に関して、リスクの可視化において、関連法規制に基づき、主に緊急事態への対応や犯罪捜査、国家安全保障にかかわる場合等において、当局より機密・秘密データに対するアクセス・開示要求を課される懸念を把握する。
  - EU データ法、中国サイバーセキュリティ法、米国 CLOUD 法等において、緊急事態への対応や犯罪捜査、国家安全保障等を根拠に、ガバメントアクセスに関する規定が含まれている。
  - 一方、例えば WTO の「知的所有権の貿易関連の側面に関する協定（TRIPS）」の下、加盟国は、開示されていない情報を公正な商慣習に反する方法による保有者の承諾を得ない開示、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。
- リスクの評価において、法規制の対象となるデータ及び適用プロセスについて把握を行い、自社にとっての影響の大きさと対応優先度を判断することが推奨される。
  - 法規制の対象となるデータに関して、自社の損失につながるデータ（機密・秘密データ等）が対象となっているか、確認することが推奨される。
  - 法規制の適用プロセスとして、ガバメントアクセスがどのような根拠・手続に基づき発生するか、また異議申し立てや協議等の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・自主的な提供か等）、対象となるデータライフサイクル（データ生成・取得に起因するか、データ加工・利用に起因するものか等）、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）への提供か等）についても確認することが推奨される。
  - 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）[25]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備えるなどの対応の方向性が考えられる（図 18）。
  - 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対応として、ガバメントアクセスの対象となるデータについて、データの移転・提供や保管を管理・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

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

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備える対応としては、越境的なガバメントアクセスが行わ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供制限として、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、環太平洋パートナーシップに関する包括的及び先進的な協定（CPTPP）の電子商取引章において、ソース・コードの輸入・販売等の条件として、他国の者が所有するソフトウェア等のソース・コードの開示・アクセスを禁止する条項（第 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求に対して、事前にデータを暗号化する・匿名化するなどの打ち手が想定される。

図18



5.3 データの共有・開示の義務化

- 「c.データの共有・開示の義務化」に関して、リスクの可視化において、関連法規制に基づき、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を把握する。
  - 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、 ユーザーの要求に応じたデータ提供や第三者への提供を義務付けている。製品製造者にとっては、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）等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、EU 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データや電池組成（設計データ）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制定・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 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）のデータだけでなく、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データも集める必要がある。また、5.1「データ移転・事業活動の制限（データ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、法令順守に必要なデータを開示できなくなるリスクが存在する。
- リスクの評価において、法規制の対象となるデータ及び適用プロセスについての把握を行い、自社にとっての影響の大きさと対応優先度を判断することが推奨される。
  - 法規制の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。

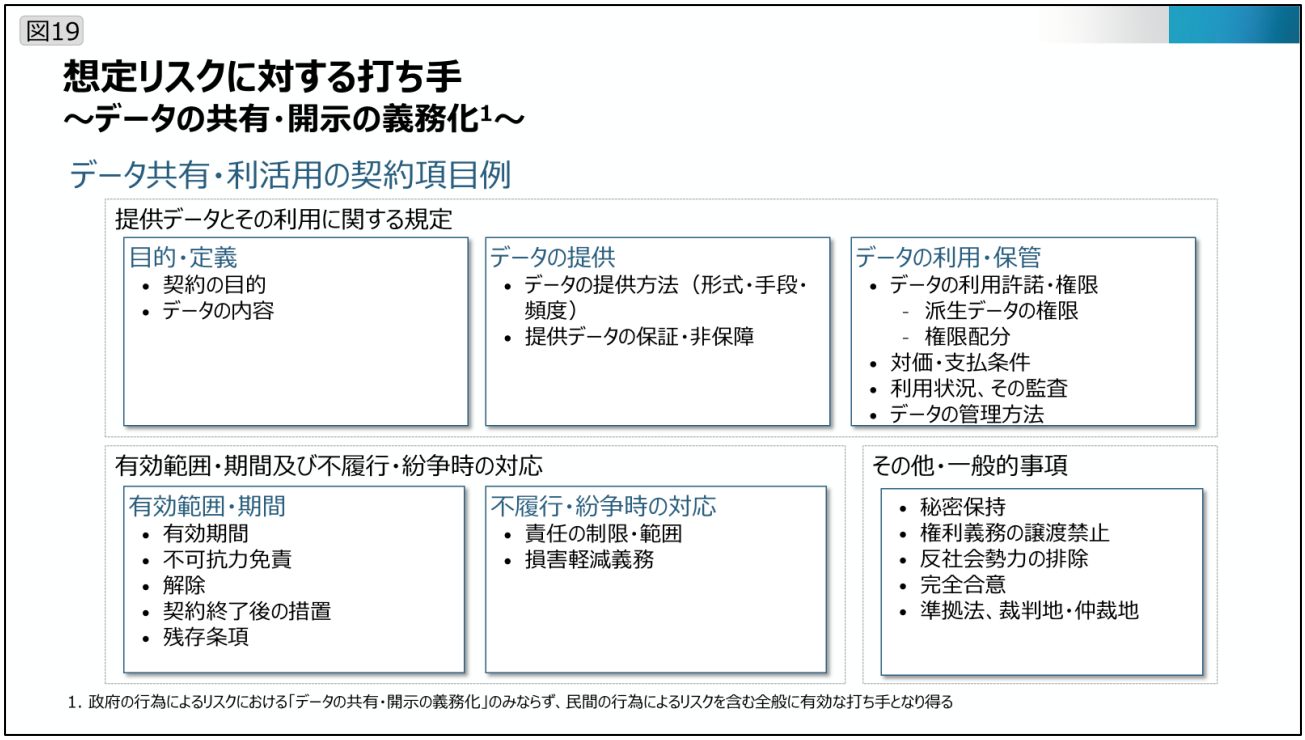
- 法規制の適用プロセスに関して、データの開示に伴い、誰に・どの範囲まで開示されるか、また共有後の開示先でどのように利活用されるかの想定等についても、把握・確認することが推奨される。

- 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である（図 19）。なお、3.5「リスクと打ち手の整理」における記載のとおり、「民間企業の行為によるリスク」においても、次に示すような取引先と適切な契約・取決めを行うことが有効な打ち手となる。
  - 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。
  - 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 つの契約関係についての Model Contractual Terms（MCT）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 SCC 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、経済産業省「AI・データの利用に関する契約ガイドライン」[26]や「データ連携基盤規約 Ver.1.0」[27]において、本マニュアルで言及された基本的に合意すべき項目の詳細及びひな形となるモデル規約等が記載されており、内容に関して参照されたい。

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

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

図19



（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政策を評価した「Cross-Border Data Policy Index」（越境データ政策インデックス）[28]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。

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

6 終わりに

- 各国のデータに関する規制や、企業における国際的なデータ共有・利活用の状況は、変化が目まぐるしく、また、関連するテーマも多岐に渡る。2024 年度の「産業データサブワーキンググループ」においては、今後深堀りすべき主要なテーマ・論点として、関連する法規制の情報更新や拡充（クラウドに関する法規制や、アジアやグローバルサウス諸国の法規制等）、打ち手の事例収集・発信（ベストプラクティスの収集や、セミナーや有識者によるパネルディスカッション等を通じた情報発信）、産業データに対する責任者・役割分担を含めた社内体制の在り方、中小企業等の人員・リソースに限りのある企業に対する支援の方向性等が挙げられた。国際・国内における関連する議論の内容と進捗を踏まえ、今後必要に応じた更新を行う。

産業データサブワーキンググループ　委員等名簿

（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 主管技師長
	和泉　恭子	一般社団法人日本知的財産協会　副理事長
	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 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＆ 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 / Business Software Alliance 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 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 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