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
# 概要

令和7年1月27日

# 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**。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」を推進**。
- 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展。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。

DFFT※の理念の下、国際的なデータ共有・利活用を拡大し付加価値の創出を促進することを目指して企業の事業部門、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向けに企業における**産業データの越境・国際流通に係るデータ管理の指針**となるマニュアルを策定

※ DFFT（Data Free Flow with Trust：信頼性のある自由なデータ流通）とは、「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 ｜ デジタル庁「DFFT」 https://www.digital.go.jp/policies/dfft

# 実現したい価値（DFFTの具体化に必要な要素）

- 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する

## 自由な流通・利用促進
（自由にアクセス・管理できる）

自社のデータや、事業の実施に必要なデータに、自由にいつでもアクセスし、活用や管理できる

## 機密性・権利の保護
（重要なデータを守れる）

他国のガバメントアクセスやサイバー攻撃・不正アクセス等からデータを守れる

万が一知的財産権等の権利が侵害された場合は、適切な救済措置がある

## 信頼性の担保
（データを信頼性高く活用できる）

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る
（データの出所が正当かつデータが不正な改変をされていない）

# 本マニュアルの検討範囲：対象プロセス

- データライフサイクルにおける各過程で、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[1] | 生成・取得 | 加工・利用 | 移転・提供[2] | 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 | データに抽出・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組織/部門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の管理の下で保管する | データを削除又はインアクティブ（使用不可能状態）にする・見えなくする |
| 各過程の越境データ管理場面（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自社の海外拠点で参照・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管する | 海外に保管されているデータが削除される |

＋

国外で各過程が発生・実施される場面全般

1. データライフサイクルとは、データが生成されてから廃棄されるまでの一連の過程を指す
2. データライフサイクルの各過程でデータの越境移転が生じ得るため、「移転・提供」におけるデータの移転には、「生成・取得」、「加工・利用」、「保管」、「廃棄」で発生するデータの越境移転は含まないものとする

# 本マニュアルの検討範囲：対象となるデータ

- 国際的にデータが共有・利活用される場面で取り扱われ得る産業データ全般を対象とする

| 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<br>• 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<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 | • 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データ等）<br>• 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）<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、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）<br>• 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）<br>• 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）<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） |

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

# 本マニュアルの検討範囲：対象となるリスク

- 実現したい価値の裏返しとして、「データに自由にアクセス・管理できない」、「重要なデータが守れない」、「データが信頼できない」ことを対象となるリスクとする

**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）

# 参考）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<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 |
| 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<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>情報漏えい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 |
| 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<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 |
| 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<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 |

# 参考）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<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 |
| | | 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<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<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）<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<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 |
| | | 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） |

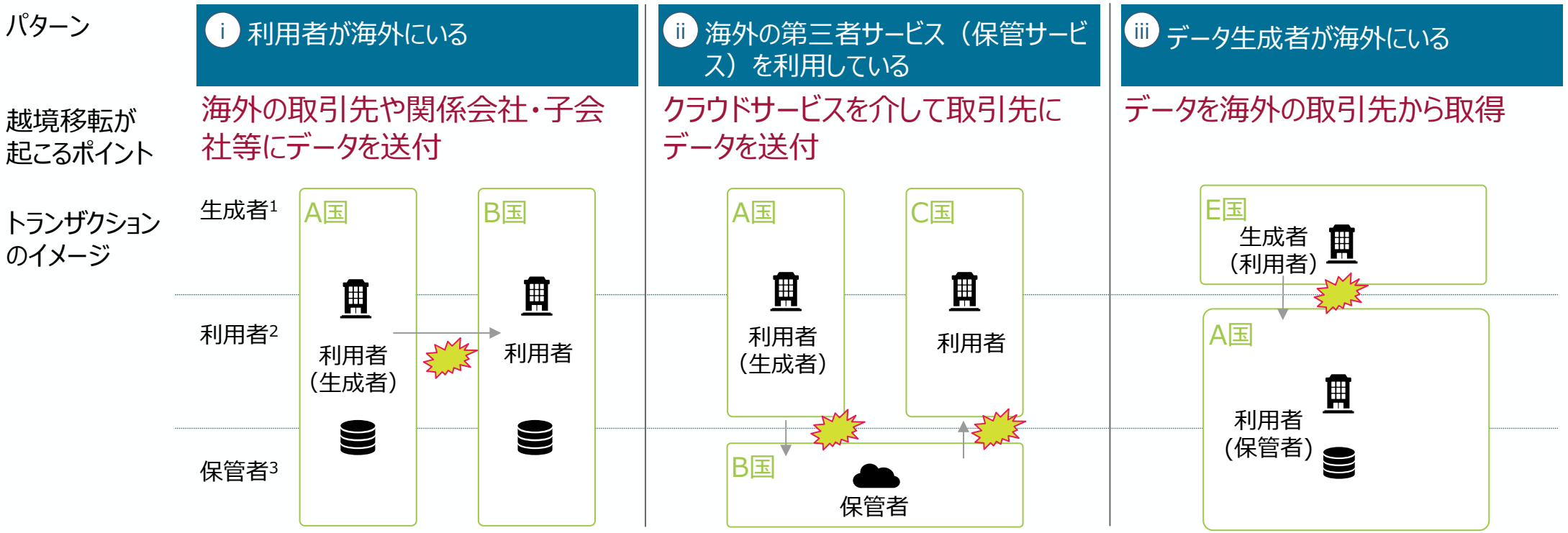
# 越境データ管理の3つのステップ

- 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（3つのステップとその中に含まれるプロセス）を定める

| | 1 リスクの可視化 | 2 リスクの評価 | 3 打ち手の実施 |
|---|---|---|---|
| プロセス | 1-1 データの越境移転が起こるトランザクションの整理<br>1-2 データライフサイクルの段階に応じたリスクシナリオの整理 | 2-1 対象となるデータやリスクが発生するプロセスを確認<br>2-2 自社にとっての影響の大きさを評価し、対応の優先度を整理 | 3-1 優先して対応が必要なリスクに対して「打ち手」を策定・実行（モニタリング/事前対応/事後対応） |
| | トランザクション/ リスクシナリオ | 対象データ・発生プロセス確認/機密・秘密データの定義 | モニタリング、事前対応、事後対応 |
| 全社組織・体制 | ステークホルダーの責任・所掌＋体制 | | レポートライン・会議体（報告会・連絡会） |
| 全社ITシステム | データベース・システム基盤 | リスクモニタリングダッシュボード | 分析基盤 ・・・ |

# 第１のステップ（リスクの可視化：①トランザクションの整理）
## ～データの越境移転が起こるトランザクション～

- 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




1.「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　2.「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
3.「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

# 第１のステップ（リスクの可視化：②リスクシナリオの整理）
## ～想定される代表的なリスクのカテゴリー～

- 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

| | 政府の行為によるリスク<br>該当国の国内法令・規制等に基づいた措置・行為 | 民間企業の行為によるリスク<br>取引先・サービス提供者の不注意・故意による行為 |
|---|---|---|
| 自由にアクセス・管理できない | a データ移転・事業活動の制限<br>• データローカライゼーション（越境移転規制を含む） | d データ移転・事業活動の制限<br>• コンプライアンスポリシー等による移転制限 |
| 重要なデータ（機密・権利）が守れない | b データの強制的なアクセス<br>• ガバメントアクセスによる強制的な情報取得<br>c データの共有・開示の義務化<br>• 規制・認証による第三者への自社データの開示 | e データ流出・漏えい、共有範囲拡大<br>• サイバー攻撃・不正アクセス/従業員持ち出し/誤送付/機密データ漏えい/廃棄に伴う漏えい等<br>f データが無断・目的外利用される<br>• 社内での無断・目的外利用/移転先での契約・目的外利用/知的財産権の侵害等 |
| データが信頼できない | | g データの真正性が損なわれる<br>• データソースの改ざん<br>• データの改ざん |

# 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～

- トランザクションとリスクシナリオを踏まえ、自社への影響の大きさを評価し対応優先度を判断する

## 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

# 第３のステップ（打ち手の実施）
## ～主要な打ち手のカテゴリー～

凡例：組 組織的措置
法 法的措置
技 技術的措置

- 対応が必要と判断したリスクに対して、適切な打ち手を策定し、実行する

モニタリング

| | |
|---|---|
| **リスク発生の疑い・予兆を把握** | 組 法規制を起因とした予兆の把握（政策の検討情報等）<br>組 企業を起因とした予兆の把握（不振な挙動等） |
| **リスク発生の有無を把握** | 組 リスク発生件数・実績の把握（法の執行件数、企業内発生件数等） |

事前対応

| | |
|---|---|
| **リスク発生確率を下げる・予防** | 組 ガイドライン策定、保管場所・サービス選定、代替データ・業務等<br>法 データ取扱いに関する契約の締結<br>技 アクセス制限や持ち出しの制御、不正アクセスの防止 |
| **発生時のインパクトを低減** | 組 ガイドライン策定、説明責任・透明性の確保<br>法 データ取扱いに関する契約の締結<br>技 データの保護・暗号化 |

事後対応

| | |
|---|---|
| **保護措置、責任追及** | 組 リスク発生のインパクト把握、初動対応<br>法 契約・法令に基づく保護措置・責任追及 |
| **再発の防止** | 組 社内業務、取引先、利用サービスの見直し<br>法 契約の見直し<br>技 技術的措置における課題の把握、対応の見直し |

# リスクと打ち手
## ～概要～

- 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

| | | | 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<br>• 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<br>• 関連する法規制の内容とその影響を正しく把握する<br>• 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<br>• 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<br>• 関連する法規制の内容とその影響を正しく把握する<br>• 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<br>データ流出・漏えい<br>無断・目的外利用<br>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<br>• 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<br>• 発生時に備えて、取引先と適切な契約・取決めを行う<br>• 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

# 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～

- 越境移転の観点から、特に「政府の行為によるリスク」に焦点を当て、打ち手を深堀する

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<br>• 保管先・利用サービス確認<br>• 重要データの分散化<br>要望事項への対応<br>• ローカルデータセンター設立<br>• 現地運営チームの立上<br>例外措置への準拠・対応 | 代替データ選定・業務見直し<br>• 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<br>• 移転・保管に関する許可取得義務<br>• 過失があった際の免責事項や賠償内容 | 暗号鍵の保管<br>• 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<br>• 保管先・利用サービス確認<br>• 保管場所の選定・データ移転<br>保管データの加工・匿名化<br>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<br>• ガバメントアクセス発生時の報告義務<br>• 過失があった際の免責事項や賠償内容 | データの暗号化<br>• 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<br>• ガバメントアクセス発生時の報告義務<br>• 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<br>• 対象データ、公開範囲や利用規約等を規定<br>• 法的要望の折り込み | 電子すかし・ブロックチェーン<br>• 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

# 参考）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<br>• 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<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<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<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）　等 | 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<br>• 2024年2月以降、段階的に施行 |

# 参考）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<br>• 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<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（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<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（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<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<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がある | • 2018年施行 |

# 想定リスクとリスクの評価
## ～関連法規制とリスクを捉える観点～

- 関連法規制における「対象となるデータ」と「適用プロセス」を踏まえ、影響の大きさを判断する

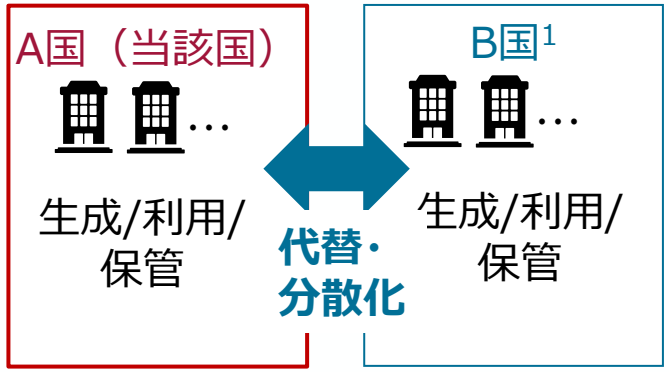
| | 関連法規制（例） | リスクを捉える観点 | |
|---|---|---|---|
| | | 法規制の対象となるデータ | 法規制の適用プロセス |
| a データ移転・事業活動の制限(データローカライゼーション) | サイバーセキュリティ法（中国）<br>データセキュリティ法（中国） | ❑ 自社の損失につながるデータ（機密・秘密データなど）が対象となっているか？<br>- 公開されていない独自データ<br>- 第三者が悪用し得る<br>- 漏えいが契約違反につながる　等<br>❑ 対象となるデータが明示されておらず、様々なデータが対象となり得るか？ | ❑ どこまでの制限事項がかかるか?<br>- 国内保存要求<br>- 国内処理要求<br>- 越境移転禁止　等<br>❑ 例外措置の規定はあるか？ |
| b データの強制的なアクセス(ガバメントアクセス) | データ法（EU）<br>サイバーセキュリティ法（中国）<br>CLOUD法（米国） | | ❑ データ取得の根拠・手続は明確か？<br>❑ 異議申立てや協議等の保護措置の規定があるか？ |
| c データの共有・開示の義務化 | データ法（EU）<br>電池規則（EU）<br>企業持続可能性デューデリジェンス指令案（EU） | | ❑ どこまでの公開・共有範囲となっているか？<br>❑ 共有後、データはどのように利用されるか？ |

# 想定リスクに対する打ち手
## ～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)～

- 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、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

### 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

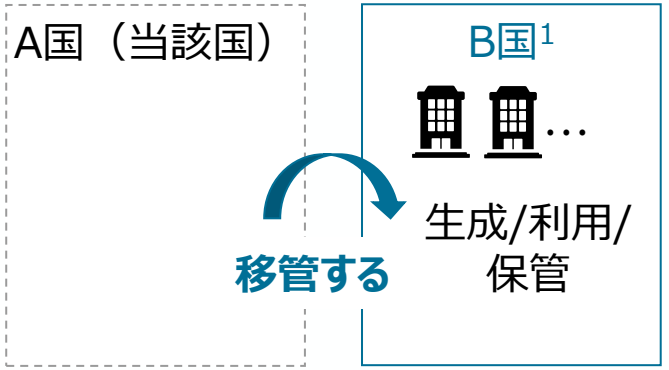
- データ移転制限の対象になったとしても、事業が継続できるように対策を講じる
  - データの分散化
  - データ・業務の代替
  - （条件付き国外移転が認められる場合における）条件への準拠




### データ越境を伴わない事業スキームを構築する

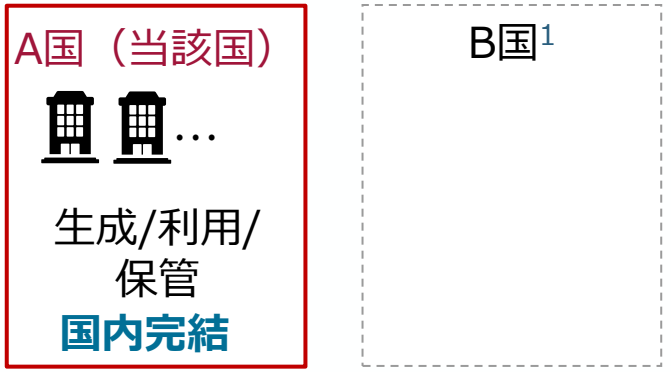
#### 関連するデータ共有・利活用を当該国で行わない

- 国内保存要求・国内処理要求に当たるデータの生成・利用・保管を別の国に移管する
- 大きなビジネス体制・運営の変更となり、実現における制約・実現可能性について、検討を行うことが求められる




#### 関連するデータ共有・利活用を当該国に閉じた形で行う

- 生成・利用・保管を当該国内で完結する
  - 当該国内でデータセンターを構築し、運営部隊を設置
  - ローカルのサービスを利用　等
- 事業上のメリットに対するコスト・人材面での実現性の検討が推奨される



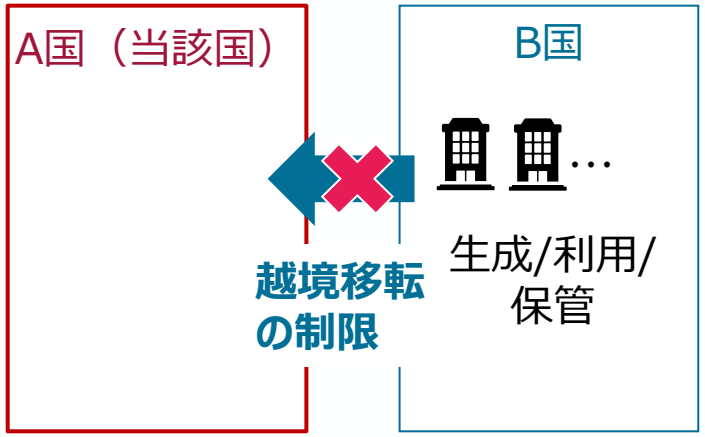

1. B国は、A国(当該国)以外の国を指し、事業者の自国だけでなくデータ移転が起こり得るその他国全般を含む

# 想定リスクに対する打ち手
## ～データの強制的なアクセス(ガバメントアクセス)～

- 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

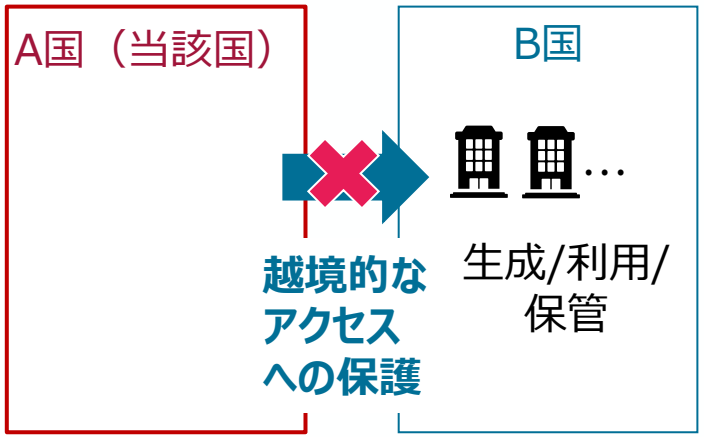
### 当該国内でのガバメントアクセスの対象とならないように当該国へのデータ移転を制限する

- 当該国内でガバメントアクセスの対象となるデータについて、データ移転・保管を管理・制限する
  - リスクが低いと想定される保管場所・利用サービスの選定
  - 当該国への移転の制限、当該国企業との取引制限
- 保有するデータの中で、自社にとって有益かつリスクにさらされているデータを適切に把握し、打ち手を講じる




### 他国からの越境的なガバメントアクセスに備える

- 他国から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、打ち手を講じる
  - 自国内における他国政府へのデータ提出制限の確認、適用（国際通商協定、国内法など）
  - 技術的な保護措置の導入



# 想定リスクに対する打ち手
## ～データの共有・開示の義務化[1]～

- 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と考えられる

### データ共有・利活用の契約項目例

提供データとその利用に関する規定

**目的・定義**
- 契約の目的
- データの内容

**データの提供**
- データの提供方法（形式・手段・頻度）
- 提供データの保証・非保障

**データの利用・保管**
- データの利用許諾・権限
  - 派生データの権限
  - 権限配分
- 対価・支払条件
- 利用状況、その監査
- データの管理方法

有効範囲・期間及び不履行・紛争時の対応

**有効範囲・期間**
- 有効期間
- 不可抗力免責
- 解除
- 契約終了後の措置
- 残存条項

**不履行・紛争時の対応**
- 責任の制限・範囲
- 損害軽減義務

その他・一般的事項
- 秘密保持
- 権利義務の譲渡禁止
- 反社会勢力の排除
- 完全合意
- 準拠法、裁判地・仲裁地

1. 政府の行為によるリスクにおける「データの共有・開示の義務化」のみならず、民間の行為によるリスクを含む全般に有効な打ち手となり得る