経済産業省 委託事業

調査報告書

令和5年度補正

グローバルサウス未来志向型共創等事業

（DFFTに係るグローバルサウスへのアウトリーチのための調査）

令和 7 年 3 月

ボストン・コンサルティング・グループ合同会社

目次

1. 検討の目的/背景

デジタル時代において、データは付加価値の源泉であり、企業活動にとってデータの流通・活用により、その価値を引き出すことの重要性が増している。デジタル経済の健全な発展には、国際的に信頼ある自由なデータ流通を確保することが必要であり、日本は2019年に“Data Free Flow with Trust (DFFT)”を提唱し、その具体化に向けた取組を進めている。

国際的なDFFTの実現にあたって、アジアをはじめとするグローバルサウスとも連携した形で実現することが重要である。特に新興国ではデータ保護法制が不十分であったり、保護主義的な規制を行っている場合もあり、データのセキュリティや知的財産権保護の重要性も高まる中、こうした国々との間で、 DFFTの価値観を共有し、信頼性を確保したデータ管理・利活用のためのデータガバナンスの在り方の整理、国際的なルール整備の推進が欠かせない。

こうした背景の下、本事業では、グローバルサウスを含む各国・地域で導入されているデータ越境移転に関する規制やガバメント・アクセスの制度等を整理し、こうした規制を前提に企業の越境データのガバナンスの在り方について、有識者含め具体的な検討を行う。加えて、越境プライバシールール（CBPR）認証制度のアジアをはじめとするグローバルサウスへの普及や利活用促進に向けた調査を行い、今後の政策的検討に資する情報収集を目的とする。

上記の背景・目的の元、本事業において下記取組・調査を実施した。

① 産業データサブワーキンググループの実施運営

② 産業データの越境データ管理等に関するマニュアル作成

③ 越境プライバシールール（CBPR）認証制度の普及等に向けた調査

2. 産業データサブワーキンググループの実施運営

「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」（デジタル庁・経済産業省共催）の下、2024年5月30日に「産業データサブワーキンググループ」を設置し、産業データの国際的な共有・利活用に伴うリスクと企業が取り得る打ち手等について、特に越境移転に焦点を当て、整理を行った。

（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

産業データサブワーキンググループは、以下の通り開催された。

開催回	議論の流れ	主な論点
第 1 回 (5/30)	● 前提・背景の確認 ● 議論のスコープや方向性の議論 ● データ共有・活用の類型の確認・議論 ➢ 実例の洗い出し	● 目的・背景を踏まえ、検討の全体像に追加すべき点はあるか ● 対応策検討の際の考慮要素の整理をどう考えるべきか ● データ越境のパターン・リスク等の各要素に追加すべきものはあるか ● 代表的な例として、取り上げるべき実例はあるか
第 2 回 (7/30)	● 有識者のご意見照会結果をもとにした検討の方向性のご相談 ➢ ガイドラインの構成 (記載の重複部分の取り扱い等) について ➢ 原則の内容・要素・それぞれの関係性について ➢ 用語の定義について	● データ越境に伴い発生するリスク及び対応策の紹介 ➢ 特に大きなリスクに対する有効な「打ち手」の実例 ● 「打ち手」のあり方の方向性の検討 ➢ 組織・オペレーション的に有効な打ち手の検討 ➢ 越境するデータに関する契約において、どのような項目が含まれるべきか ➢ 特に有効な技術の活用事例のインプット
第 3 回 (9/24)	● ユースケースのご紹介 ● 第2回の残論点に関する議論	
第 4 回 (12/9)	● 取りまとめの骨子案・記載内容の確認 ● 本検討の国内外への周知のあり方の議論	● これまでの議論が過不足なく反映されているか ➢ ユーザーにとって分かりやすい記載となっているか ● 取りまとめた内容を、誰に、どのように打ち出していけると良いか

3. 産業データの越境データ管理等に関するマニュアル作成

産業データサブワーキンググループでの議論を踏まえ、「産業データの越境データ管理等に関するマニュアル」を策定した。本マニュアルは、「パーソナルデータ」以外のデータ（マニュアル中では「非パーソナルデータ」という。）にも焦点を当てた初めてのマニュアルになり、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目指している。

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。

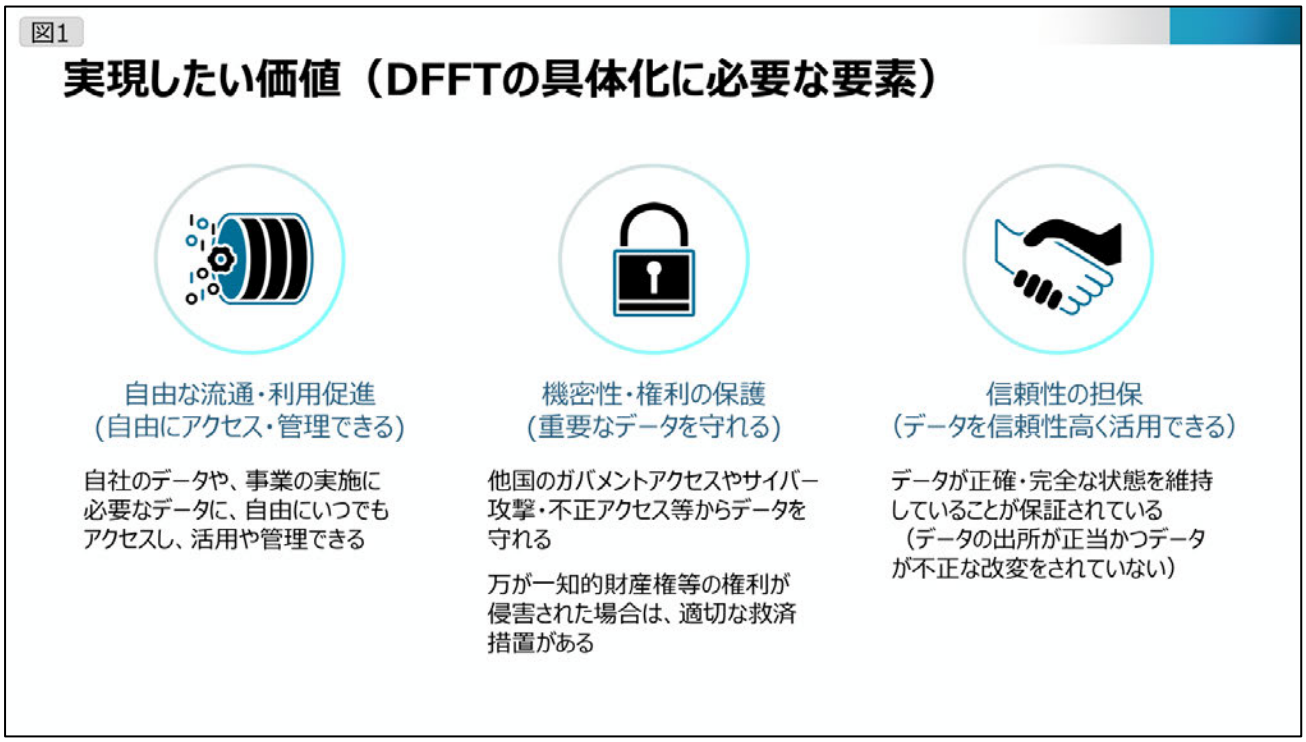
2 検討の範囲と位置付け

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）。

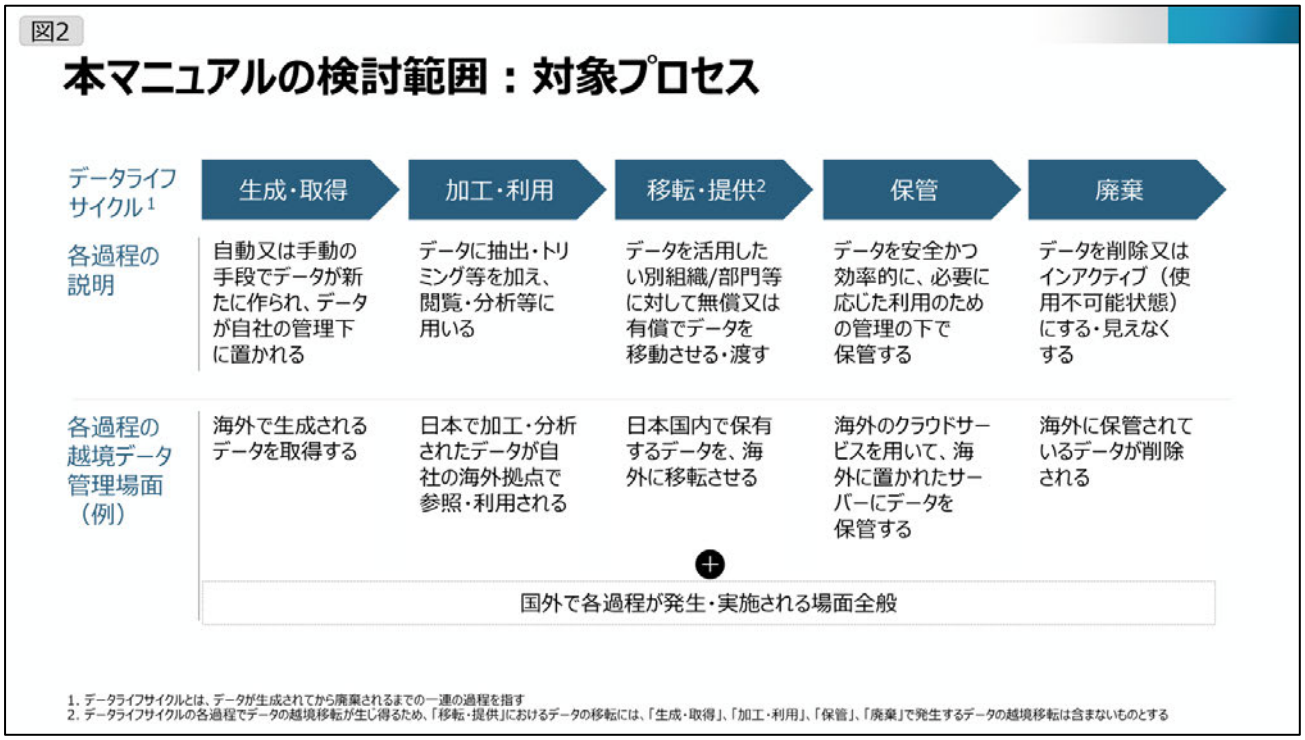
図1



[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。



- 「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

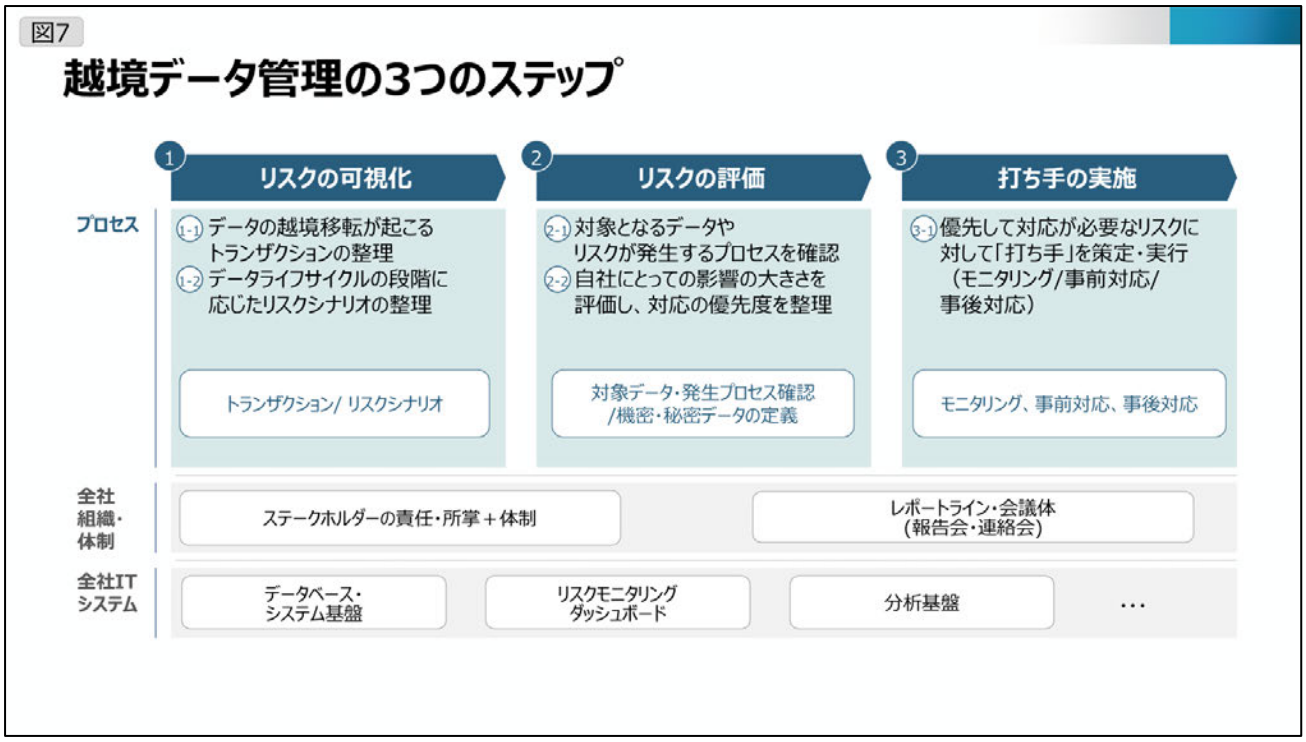
本マニュアル(章)		関連ガイドライン	主要参照先	概要
3 越境データ管理の3つのステップ	3.2 第1のステップ (リスクの可視化)	1 協調的なデータ利活用に向けたデータマネジメント・フレームワーク	2. 本フレームワークにおけるデータマネジメントのモデル • 2-2-1 モデル化（「イベント」）	データライフサイクルの定義及び代表的なリスクの記載
		4 限定提供データに関する指針	Ⅲ.「不正競争」の対象となる行為について (総論)	データライフサイクルの過程における不正競争の対象となる行為の定義
	3.3 第2のステップ (リスクの評価)	2 秘密情報の保護ハンドブック	2章 保有する情報の把握・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

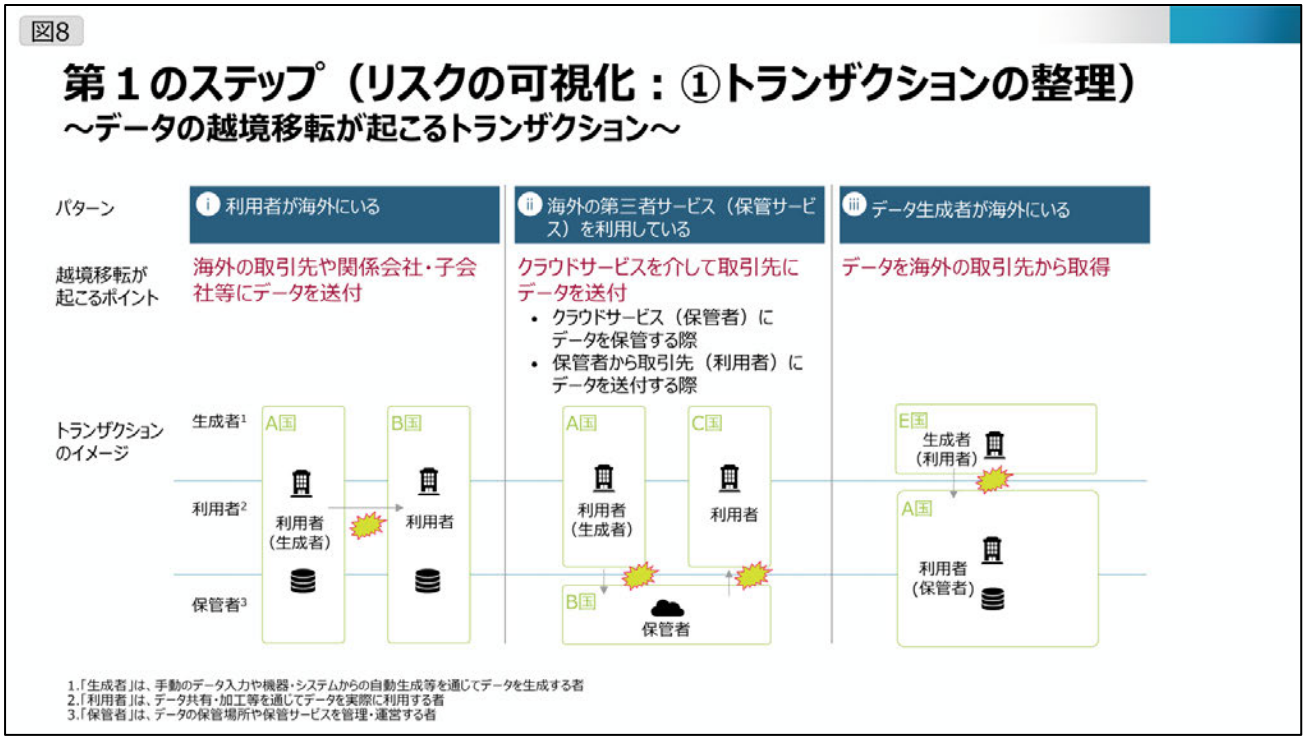


3.2　第 1 のステップ（リスクの可視化）

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）。

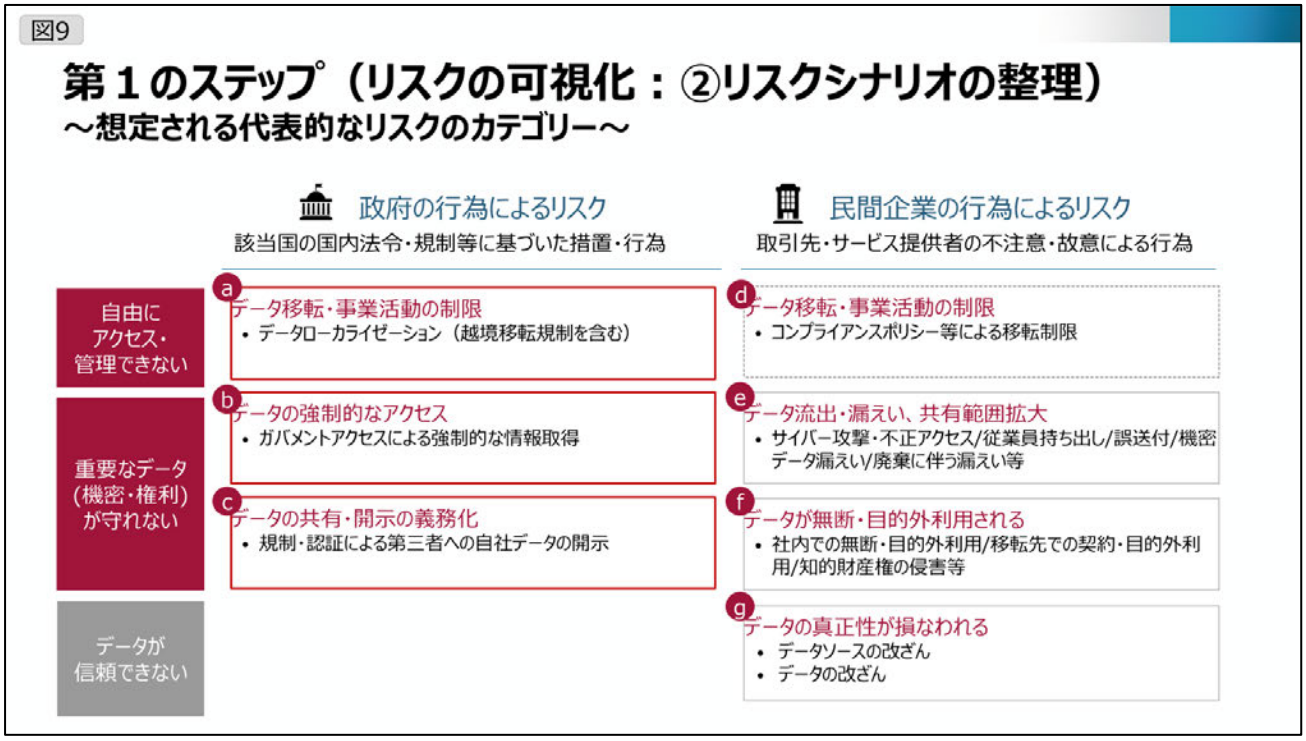
図8



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。

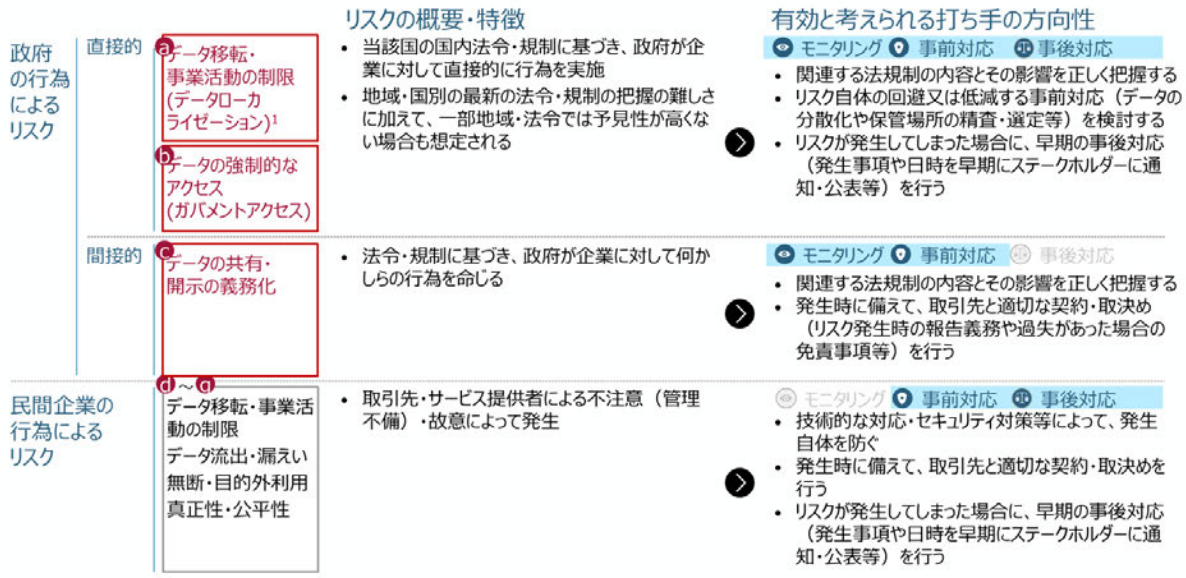
なお、「民間企業の行為によるリスク」は、企業における不注意やガバナンスの不足によって発生する場合が多い。商慣習や管理体系の異なる海外企業との取引が増えることによる間接的な影響は想定されるが、データの国際的な共有・利活用や越境移転によって直接的に発生するリスクではない。

- 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～



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）

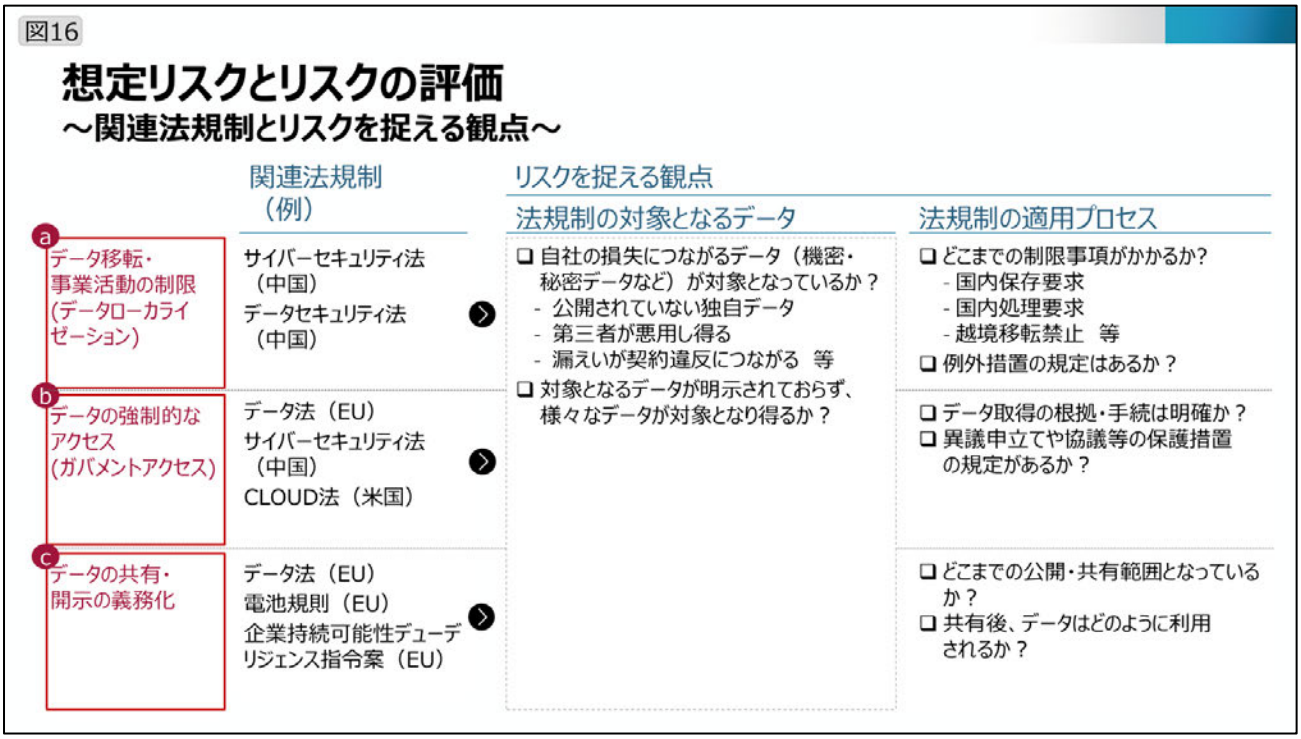
- 「a.データ移転・事業活動の制限」に関して、リスクの可視化において、関連法規制に基づき、データの国内保存の要求、当該国外への移転の禁止、当該国内データセンターの利用義務付け等の措置が課される懸念を把握する。
  - データローカライゼーション措置の分類[23]には、例えば、国内保存要求、国内処理要求、越境移転禁止規制が考えられる。国内保存要求は、データの保存場所を指定するものであり、データのコピーを国内に保存すれば、国外に移転し処理（使用、編集・変更等）することを認める場合を念頭に置いている。国内処理要求は、データの主要な取扱場所を指定し、国外における処理（使用、編集・変更等）は認められな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

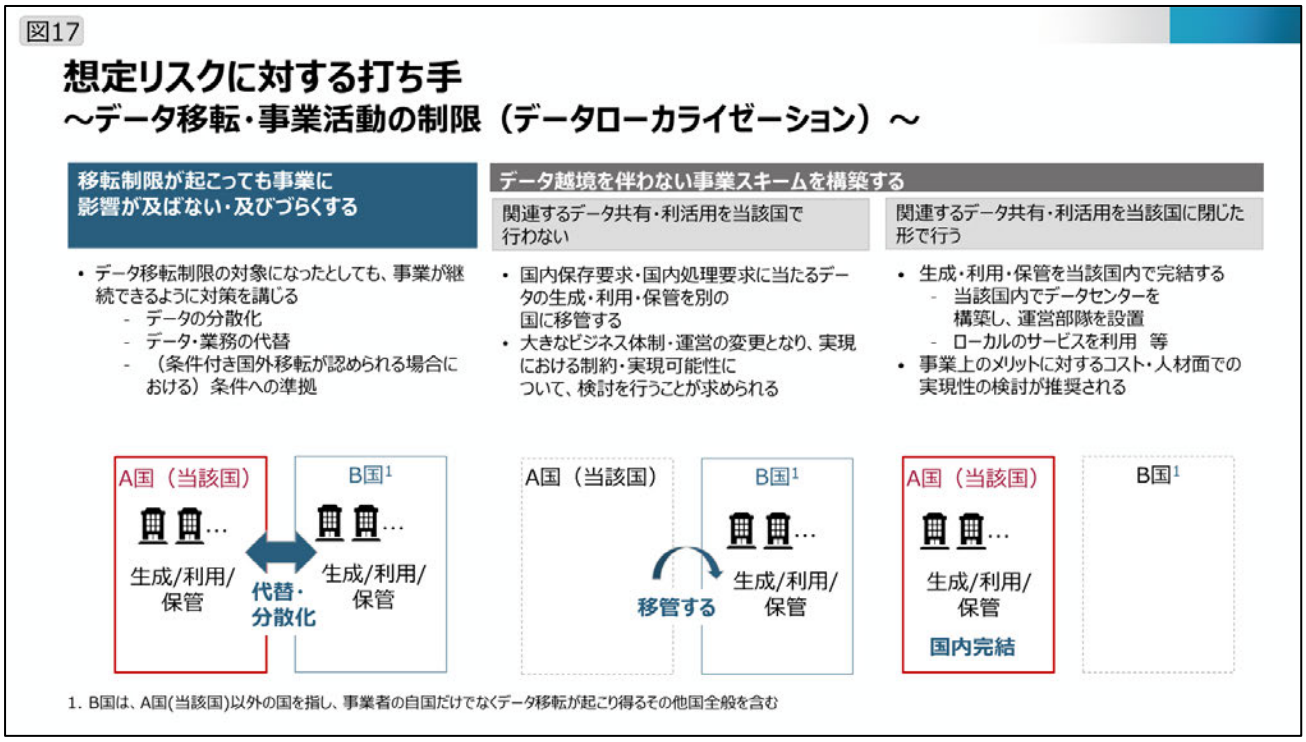


- 打ち手として、主に移転制限が起こっても事業に影響が及ばない・及びづらくする、移転制限自体が起こらないようにデータ越境を伴わない事業スキームを構築するといった対応の方向性が考えられる（図 17）。
  - 移転制限が起こっても事業に影響が及ばない・及びづらくする対応として、当該データが移転制限の対象となっても事業が継続できるように、データの分散化、データ・業務の代替等の打ち手が想定される。国内保存要求（越境移転の制限なし）が課されている場合には、データを複製して国外の拠点に分散して保管することが考えられる。また、国内処理要求又は越境移転禁止規制により国外での利用が制限される場合には、データ・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）

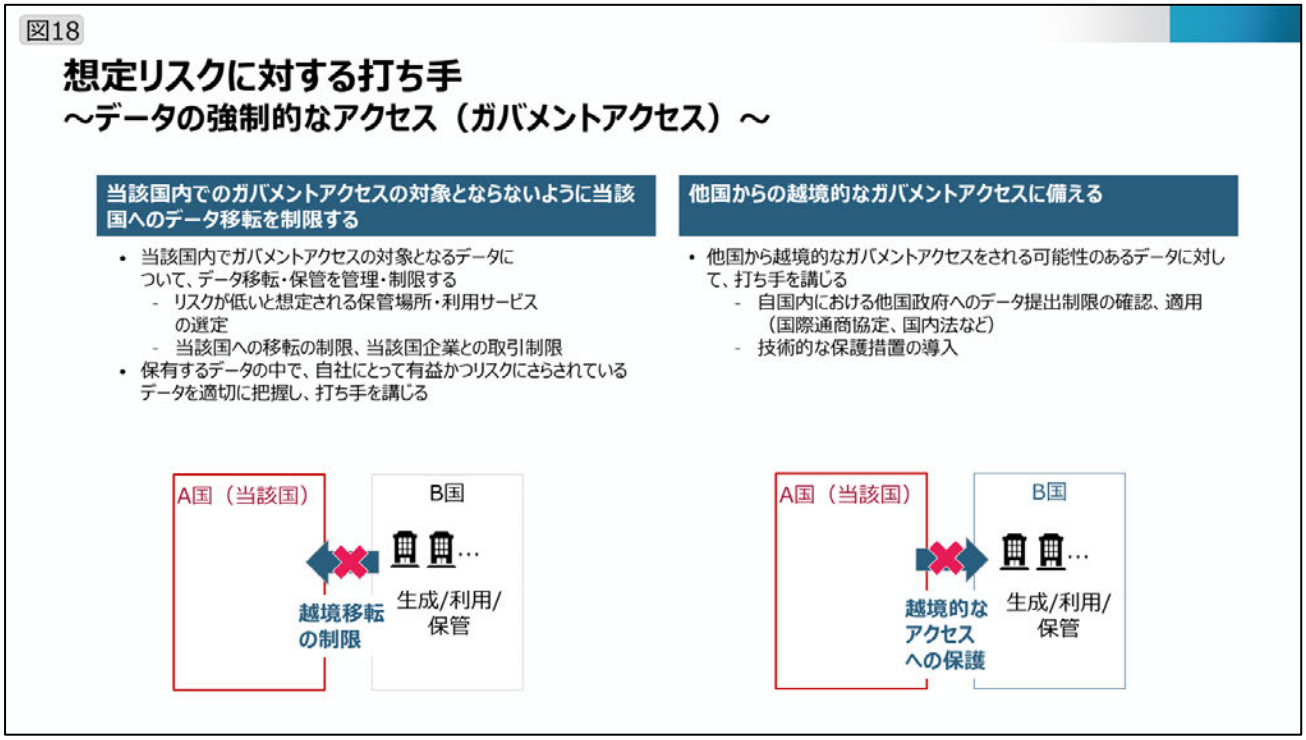
- 「b.データの強制的なアクセス」に関して、リスクの可視化において、関連法規制に基づき、主に緊急事態への対応や犯罪捜査、国家安全保障にかかわる場合等において、当局より機密・秘密データに対するアクセス・開示要求を課される懸念を把握する。
  - EU データ法、中国サイバーセキュリティ法、米国 CLOUD 法等において、緊急事態への対応や犯罪捜査、国家安全保障等を根拠に、ガバメントアクセスに関する規定が含まれている。
  - 一方、例えば WTO の「知的所有権の貿易関連の側面に関する協定（TRIPS）」の下、加盟国は、開示されていない情報を公正な商慣習に反する方法による保有者の承諾を得ない開示、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

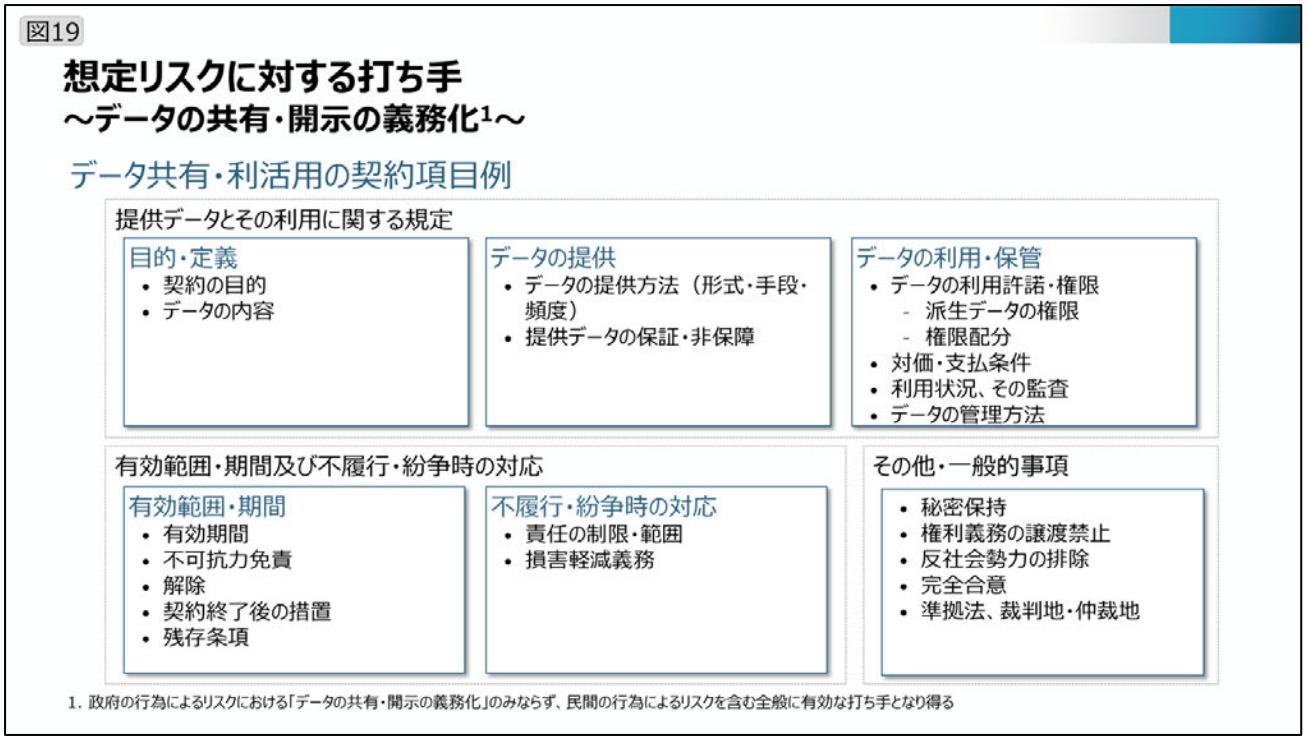
- 「c.データの共有・開示の義務化」に関して、リスクの可視化において、関連法規制に基づき、企業活動においてデータの共有・開示が義務付けられる懸念を把握する。
  - 例えば EU データ法においては、EU 域内のコネクテッド製品・サービスの生成・加工データを対象に、製品・サービスのユーザーに対して生成データへのアクセスを可能とすることや、 ユーザーの要求に応じたデータ提供や第三者への提供を義務付けている。製品製造者にとっては、製品開発・仕様変更等によるコスト増加や、提供・開示されるデータの範囲によっては製品のノウハウの流出が懸念される。
  - EU 電池規則においては、原料取得から最終廃棄・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



（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

関連資料

「産業データの越境データ管理等に関するマニュアル」に関して、付属資料として「参考資料A: 打ち手のリスト」および「参考資料B: 産業データサブワーキンググループ提出資料集 (企業事例と関連テーマの動向)」が公表されている。またマニュアルの本編および参考資料Aに関して、英語版も作成されている。以下URLにおいて、各関連資料が公表されているため、詳細内容に関して参照されたい。

資料名	HPアドレス
参考資料A: 打ち手のリスト	https://www.meti.go.jp/press/2024/01/20250127001/20250127001-2r.pdf
参考資料B: 産業データサブワーキンググループ提出資料集 (企業事例と関連テーマの動向)	https://www.meti.go.jp/press/2024/01/20250127001/20250127001-3.pdf
Manual on Cross-Border Industrial Data Management	https://www.meti.go.jp/english/press/2025/pdf/0127_001a.pdf
Reference Material A: List of actions	https://www.meti.go.jp/english/press/2025/pdf/0127_001b.pdf

4. 越境プライバシールール（CBPR） 認証制度の普及等に向けた調査

2022年に新たに設立が宣言された「グローバル越境プライバシールール（GCBPR）」の認証企業の増加に向けて、有効な普及啓発と制度の改善提案に繋げるべく、既存の認証制度との比較検討のマッピング調査および企業へのヒアリングを実施した。

経済産業省委託事業

令和５年度補正グローバルサウス未来志向型共創等事業

（ＤＦＦＴに係るグローバルサウスへのアウトリーチのための調査）

越境プライバシールール（ＣＢＰＲ）認証制度の普及等に向けた調査

調査報告書

令和７年１月

一般財団法人日本情報経済社会推進協会

目　次

第1章 調査概要

1. 実施目的

デジタル時代において、データは付加価値の源泉であり、企業活動にとって、データの流通・活用により、その価値を引き出すことの重要性が増している。このため、デジタル経済の健全な発展には国際的に信頼ある自由なデータ流通を確保することが必要であり、日本は 2019 年に“Data Free Flow with Trust（DFFT）”[1]を提唱し、その具体化に向けた取組を進めている。

国際的な DFFT の実現にあたり、アジアをはじめとするグローバルサウスとも連携した形で実現することが重要である。特に、新興国ではデータ保護法制が不十分である場合や、保護主義的な規制を行っている場合もある。データのセキュリティや知的財産権の保護の重要性も高まっている中で、こうした国々との間で、DFFT の価値観を共有し、信頼性を確保した形でデータを管理・利活用するためのデータガバナンスの在り方を整理し、国際的なルール整備を進めていくことが欠かせない。

こうした背景の下、DFFT の具体化ツールの一つとして、2022 年に新たに設立が宣言された個人データの越境移転に関する企業認証制度である「グローバル越境プライバシールール（以下、「GCBPR」という。）」[2]の認証企業増に向けて、既存の認証制度との比較検討のためのマッピング及び各国の審査機関が実施する審査工程に基づく制度の改善提案、並びに企業等へのヒアリングを行い、今後の政策的検討に資するための有効な情報を収集することを目的とする。

[1] デジタル庁ホームページには「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」というコンセプトです。DFFT は、2019 年 1 月にスイス・ジュネーブで開催された世界経済フォーラム年次総会（ダボス会議）にて、安倍総理（当時）が提唱し、2019 年 6 月の G20 大阪サミットにおいて各国首脳からの支持を得て、首脳宣言に盛り込まれた」とされており、本報告はこの定義に基づいて作成している。

[2] Global CBPR Forum が運営する企業のプライバシー原則への適合性を認証する CBPR（Cross Border Privacy Rules）システムは、APEC の CBPR システムをベースとして、その対象範囲を APEC 域外に拡大した政府支援の第三者認証制度で、運用の開始が期待されている。なお、現在認証制度として運用されているのは APEC の CBPR システム（（以下、「CBPR」）という。）だけであり、CBPR は、APEC 域内において国境を越えて流通する個人情報に対し、消費者や事業者、行政機関における信用を構築するシステムを言う。2011 年に開始され、日本は 2014 年 4 月に参加が認められた。）であるため、本調査報告書で他の法や認証制度と比較を行う元となる制度は APEC の CBPR を指す。

2. 実施内容及び実施体制

2.1 実施内容

本事業の実施内容は、以下のとおりであった。

(1) GCBPR の普及等に向けた活動

2022 年に新たに設立が宣言された個人データの越境移転に関する企業認証制度である GCBPR の認証企業増に向けて、既存の認証制度等との比較検討のマッピングを含む制度改善提案の検討をすべく、他の法・個人情報に関する第三者認証制度のギャップ分析を行う他、既存制度の実態や課題を把握するため、各国のアカウンタビリティ・エージェント（以下、「AA」という。）[3]へ審査プロセスの概要等についてアンケート調査を行った。また、GCBPR の普及啓発を目的として、企業計 11 社へヒアリングを行い、その結果をとりまとめた。

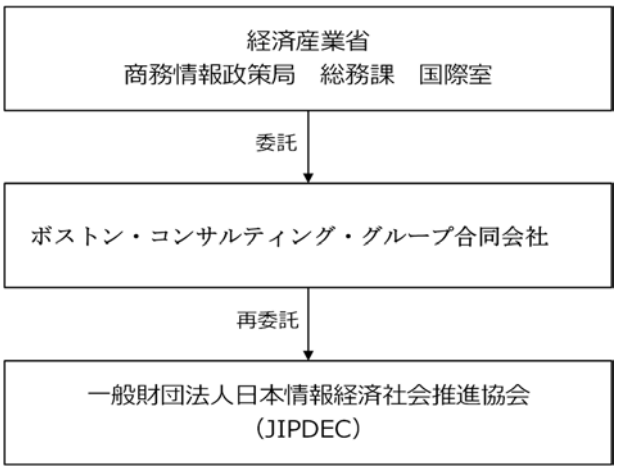
(2) 報告書の作成

上記の調査・検討を踏まえた調査報告書（本書）を作成した。

2.2 実施体制

本調査の実施体制を以下に示す。

図表 1 本調査の実施体制



本調査は、経済産業省商務情報政策局総務課国際室からの委託事業として、ボストン・コンサルティング・グループ合同会社が委託を受け、その再委託を受ける形で実施した。

[3] CBPR の認証を行う審査機関のことを指す。2016 年 1 月に、JIPDEC が日本初の AA として APEC から認定された団体となった。CBPR に参加するには、AA の設立が要件となり、同一の国・地域内で複数の設立が可能。

第2章　CBPR の普及等に向けた活動

1. 実施概要

(1) 目的

2022 年に新たに設立が宣言された個人データの越境移転に関する企業認証制度である GCBPR の認証企業数増に向けて、既存の越境移転制度等の改善提案を検討すべく、CBPR と他の法・個人情報に関する第三者認証制度のギャップ分析及び AA へ審査工程等に関するアンケート調査を行うと共に、GCBPR の普及啓発を目的として、業務上個人データの越境移転が生じる企業へヒアリングを行った。

(2) 実施内容

「CBPR の普及等に向けた活動」として実施した内容は、以下のとおりである。

①　既存の認証制度との比較検討のマッピングを含む制度改善提案の検討

1) マッピング調査

既存の認証制度との比較検討のマッピングを含む制度改善提案の検討では、GCBPR の認証企業数拡大に向けて、以下のとおり CBPR との比較調査を行った。

比較対象としては、国際的な認証において最も関心の高い EU の GDPR（一般データ保護規則）で個人データの域外移転を可能にする方法の 1 つである BCR[4]を中心に、SCC（Standard Contractual Clauses：標準契約条項）や十分性認定なども考慮しながら、それぞれの制度の持つ意味や価値、そして改善点についての分析を行った。

また、GCBPR をこれから申請しようとする事業者（以下、「申請企業」という。）が、既にその他の第三者認証を取得している可能性が考えられるため、我が国において認証数が多いプライバシーマーク制度（以下、「P マーク」という。）と ISMS 適合性評価制度（以下、「ISMS」[5]という。）との比較調査を行い、審査プロセスや申請に必要となる根拠資料の親和性（要求事項、審査基準、申請が必要な根拠資料類、審査準備等）を調査し、新たな認証の取得に対する労力やコストの低減等への可能性について分析を行った。

[4] Binding Corporate Rules（拘束的企業準則）
[5] 本報告書では ISMS と表記する。ただし ISMS 適合性評価制度で用いられている用語とは異なる。

2) アンケート調査

CBPR に参加する 9 エコノミーのうち、AA を擁する米国、シンガポール、韓国、チャイニーズ・タイペイ、日本で審査を行っている計 8 つの AA に対し、4 つの大項目に基づき、21 の設問で構成されるアンケート調査を実施し、CBPR の審査プロセスの差異、及び具体的な審査概要の違い等、我が国との差異も踏まえて実態を把握し、認証企業数の拡大に向けて、信頼を確保しつつ事業者と審査機関双方の視点で認証審査に関わる改善案をとりまとめた。

図表 2　アンケート調査実施 AA

No	機関名称	概要		
		運営母体	認証開始	認証企業数 CBPR/PRP[6]
1	Trust Arc（米国）	民間	2013	37／30
2	Schellman（米国）	民間	2019	2／9
3	NCC Group（米国）	民間	2020	6／7
4	BBB National Program（米国）	民間（非営利）	2021	7／7
5	IMDA（シンガポール）	政府機関	2019	11／6
6	KISA（韓国）	政府委託	2019	13／－
7	III（チャイニーズ・タイペイ）	政府機関	2021	1／－
8	JIPDEC（日本）	民間（非営利）	2016	4／－

2025 年 1 月 23 日時点

②　ヒアリング：　普及啓発活動

日本の CBPR 認証企業 3 社を含み、業務として個人データを越境移転している企業計 11 社に対し 13 項目（計 22 の設問）のヒアリングをオンラインにより実施し、認知度、越境移転ツールのニーズ､法や規則と第三者認証制度を比較した場合のメリット･デメリット、認証取得へのインセンティブ、拡大に向けた意見等の観点で、課題の整理を行い、改善案をとりまとめた。

[6] 認証企業数は以下のサイトより
http://cbprs.org/compliance-directory/cbpr-system/
http://cbprs.org/compliance-directory/prp/

図表 3　ヒアリング調査実施記録

No	実施日時	対象企業
1	2024/10/8（火）13:00-14:00	A 社（J 金融業、保険業）
2	2024/10/17（木）11:00-12:00	B 社（G 情報通信業）
3	2024/10/17（木）13:00-14:00	C 社（G 情報通信業）
4	2024/10/22（火）11:00-12:00	D 社（G 情報通信業）
5	2024/10/23（水）11:00-12:00	E 社（G 情報通信業）
6	2024/10/24（木）14:00-15:00	F 社（R サービス業（他に分類されないもの））
7	2024/10/30（水）14:00-15:00	G 社（G 情報通信業）
8	2024/11/5（火）10:30-11:30	H 社（E 製造業）
9	2024/11/8（金）15:00-16:00	I 社（J 金融業、保険業）
10	2024/11/13（水）13:30-14:30	J 社（G 情報通信業）
11	2024/11/26（火）15:00-16:00	K 社（I 卸売業、小売業）

2.　実施結果

2.1　既存の認証制度との比較検討のマッピングを含む制度改善提案の検討

マッピング調査では、個人データを対象とした越境データに関する制度の中から認証制度として実態が認められるものを選び、それらと CBPR との相対的な関係性を分析した。個人データに関して並立関係にあるいくつかの他の認証制度は、取得を検討する企業の立場からは比較検討の対象として捉えられるため、CBPR の運営に関連する立場からはそのポジショニングを明確にして、説明可能性を高めておく必要がある。

今回の調査においては、マッピングは比較項目を作り、それぞれを文献及び実務者へのヒアリングによる確認を通じて行われるが、今回の CBPR を中心にしたマッピングに関しては以下の要素が含まれる。

- 比較を行う認証制度の目的、趣旨、基礎となる概念、運用実績等
- 認証における個別要求事項の共通点と差
- 認証の運用に関する事項（更新期間、費用、各国法制度との関連の有無）

なお、日本の個人情報の保護に関する法律（以下、「個人情報保護法」という。）個人情報保護法に基づくガイドラインにおいては、認証制度以外にも「相当措置」として、規定

される移転時に求められる必要事項[7]があるが、ここでは「認証制度」でもとめられる要求項目を主な比較対象とした。比較にあたり、マッピングの主対象としたのは以下の各認証制度であるが、これ以外に上記比較項目のいくつかについては導入的な分析を加えたものもある。比較対象となった認証制度は以下の 3 つである。

- GDPR（BCR を中心とする）
- P マーク
- ISMS

これら比較対象の選定にあたっては、取得数の多さ、申請候補企業から見た認証制度としての CBPR との類似性と関心の高さ、および各認証制度の情報へのアクセス性などを考慮した。

更に、現行の CBPR 審査の一貫性や効率性の観点から制度の改善提案を検討すべく、審査工程、制度の運用、各審査機関の法域内にある個人データに関する認証制度と CBPR 審査の関わり、今後の課題等に基づき日本を含む 8 つの AA に対してアンケート調査を行い、AA が課題と感じている事、AA 間での審査プロセスや運用の違いや類似性、我が国固有の課題等から得られた結果に対し、改善提案をとりまとめた。

2.1.1 BCR を中心とした GDPR との比較

(1) 目的と概要

GCBPR が世界的に見てどのようなポジションを得て、その価値を訴求できる可能性があるかについて考えるには、多くの企業の共通の関心である EU の GDPR とそれに付随する各制度との比較を行うことが考えられる。この章では、要求項目が比較的明確に記述されている BCR と CBPR 要求事項の比較について項目を分けて行い、CBPR のポジショニングの現状と今後の目指すべき方向について考えることとする。

APEC では 2014 年に BCR と CBPR のそれぞれの要求事項をマッピングするための実用的な比較を開発し公表している[8]。この文書（以下、「レファランス文書」という。）は、当時の一般データ保護指令にしたがって EU 加盟国で適用されるデータ保護法下で EU の域

[7] 個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）
https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/#a6-1
[8] “Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents“, https://www.apec.org/docs/default-source/groups/ecsg/20140307_referential-bcr-cbpr-reqs.pdf

内データ保護当局が BCR として制定したものと、APEC エコノミーで適用される規則に従って CBPR として認可を得るために提出されるプライバシーポリシーにおいて一般的に要求される主な要素を 1 つの文書にまとめたものである。また、EU の各国 DPA による BCR と APEC CBPR の両方の認証取得を検討している組織が使用することを想定した比較情報であり、両制度の要求事項に従い企業グループにおいて個人データ保護及びプライバシールールを適用することを容易にすることを意図している。

レファランス文書においては BCR と CBPR の両方で必要とされる共通または類似の要素のブロックがある。各 BCR 要件と CBPR 要件の追加ブロックが続き、2 つのシステムで異なる要素が列挙されている。今回はこの形式を踏襲して当時の情報をもとに、部分的にその後の変更点や論点を加味してまとめなおした。

共通ブロックは、BCR と CBPR において要求される事項の間に、ある程度の共通性を示すものであり、APEC の AA による認証や、EU の国内 DPA による承認を得なければならない。また、BCR の追加ブロックに含まれる要素も、各 DPA による BCR の承認を申請する組織が考慮しなければならない。なお、CBPR の申請企業は CBPR 認証基準に記載されているものも考慮しなければならない。

さらに、BCR の承認については特に EU データ保護法に由来する認可が必要で、EU の各国 DPA が一般的に課す要件と、CBPR の要件との間には、大きな違いが存在する可能性がある。また、BCR と CBPR の制度上のそれぞれの目的、範囲、審査プロセスにも違いがある。このような相違の結果、BCR と CBPR の要求事項の中には、完全に互換性のないものもある。したがって、適用される法律との抵触を避けるため、申請企業は、個人情報保護およびプライバシーに関する規則の適用範囲を明確にしなければならない。

なお、GDPR における他の 2 つの法的な越境移転が可能となる SCC と十分性認定については図表 7 にまとめてあるが、制度上の BCR との比較において、GDPR 全体と CBPR が根拠とする APEC プライバシーフレームワーク[9]の間の大まかな違いが見て取れる。

(2) BCR と CBPR における要求事項の比較

レファランス文書においては、GDPR における BCR と CBPR について要求項目の比較を行うに当たり、まず双方の要求項目の体系的な分類整理を行い、27 項目を比較対象とした。

[9] APEC 参加国・地域において活動する事業者に対し、認証審査を行う際に適合性を確認するために APEC が定める個人情報保護の枠組み（APEC プライバシーフレームワーク（以下、「フレームワーク」という。））を指す。

以下に比較結果の概要を示す。備考（事業者視点）に記述してあるのは、両者の比較が保つ意味について端的に表現したものである。

図表 4　BCR と CBPR における要求事項の比較

項目	BCR	CBPR	備考 （事業者視点）
1. 規則の目的	全メンバーと従業員に規則の解釈と尊重を義務付ける。	国内法が CBPR より厳しい場合は国内法が優先。CBPR が厳しい場合は自主的にその要件を満たす。	CBPR は多様性を尊重
2. 規則の範囲	公開された個人データを含む、EU 域外への転送対象データを全て保護対象とする。	APEC エコノミー内での国境を越えた転送を対象とする。	GDPR では公開情報も保護対象
3. 組織内の法的義務	法的拘束力のある措置、契約、宣言など、または従業員との個別契約、社内ポリシーで対応。	内部ガイドライン、契約、業界法等に対応。従業員トレーニングを通して周知徹底。	BCR は拘束力を強く要求
4. データ主体の救済	データ主体は、当事者となる事業者または DPA に対して請求を申し立てることができる。	管理者の苦情処理プロセスまたは AA の紛争解決プロセスを通じて権利を執行できる。	CBPR は認証機関の役割が大きい
5. 責任	原則として EU 域内の業務を代表する本社が責任主体となり是正措置を講じ、損害賠償を支払う。	法域の法制度に基づき子会社/関連会社とともに CBPR 受けた事業者が責任を負う。	CBPR は認証主体が責任負担の中心
6. 第三者移転	EU 域内または欧州委員会が認める適切な保護レベルを有する国への移転を原則とする。EU 域外への移転は欧州の規則を遵守。	第三者は移転元の管理者の指示に従い、セキュリティと機密性を確保。	BCR は法規則、CBPR は移転元指示
7. グループ内処理者	書面による契約手段が重要視される。	データ主体の同意のほかデューデリジェンス評価の実施も選択できる。	CBPR は具体的な要件規定
8. グループ外処理者	EU 規則による適切な保護レベルが前提。	処理者を含む事業者と外部者に求められる要件が具体的に記述。	CBPR は具体的要件記述
9. 定義	明確な定義を記述。	明示的要件ではない。	CBPR では柔軟な運用
10. 収集・処理・利用	明示的かつ正当な目的が求められる。	データ主体の同意があれば、収集目的と互換性の	CBPR は多様性を反映

項目	BCR	CBPR	備考 （事業者視点）
		ある、または関連する目的のために個人情報を使用できる。	
11. データの質	データの内容や保持期間について必要最小限であることが求められる。	追加要件はない。	BCR は利用の限定を重視
12. 処理の根拠	同意が根拠の場合は、明確、具体的、自由意思、情報に基づいたものでなければならない。同意以外の法的根拠も詳細に規定。	データ主体に選択肢を提供。暗黙同意が認められる処理も存在する。	CBPR は柔軟な根拠
13. 要配慮データ	データ主体が容易にアクセスできるプライバシーに関するプライバシーポリシーと、データ主体が情報に基づいた決定を下せるよう、必要な情報を提供。	データの収集方法や第三者への提供についても開示。データ主体に通知する義務が免除される例外的な状況を規定。	CBPR は例外規定を明記
14. 透明性	データ主体が容易にアクセスできるプライバシーポリシーに基づきデータ主体が情報に基づいた決定を下せるよう、必要な情報を提供。	データの収集方法や第三者への提供についても開示。データ主体に通知する義務が免除される例外的な状況を規定。	CBPR は例外規定を明記
15. データ主体の権利	EU 加盟国の国家安全保障や公共の安全などの理由で、権利が制限される場合もある。	データ主体の身元確認を必要とした上で、情報の提供方法、修正・削除の期限などを規定。アクセス要求を拒否する場合は正当な理由を説明。	BCR は安全保障上、制限の可能性
16. 異議申立て	いつでも異議を唱えることができ、ダイレクトマーケティングに利用される場合は事前に通知を受け、異議を唱える権利を持つ。	選択肢の提供が不要な場合もある。	CBPR は不要な場合もある
17. 自動化された決定	データ主体の正当な利益を保護するための適切な措置が求められる。	自動処理に関する具体的な規定はない。	
18. セキュリティ	最新技術と実装コストを考慮。情報セキュリティポリシーと安全な削除のポリシーが必要。	定期的なレビューと再評価。攻撃やセキュリティ障害への対策も必要。	BCR はポリシー、CBPR はレビュー重視
19. 研修	同等	同等	

項目	BCR	CBPR	備考 （事業者視点）
20. 監査	同等	同等	
21. コンプライアンス	同等	同等	
22. 苦情処理	同等	同等	
23. 規則の更新	同等	同等	
24. 抵触法・ガバメントアクセス	法執行機関からのアクセス要求は適用法と一致。	法執行機関からのアクセス要求に応じる前に、データ主体の権利と自由を保護するための措置を講じる。	CBPR はデータ主体の権利を重視
25. 執行協力	同等	同等	
26. 現地法との関係	EU データ保護規則が現地法より優先。	CBPR に従って定めた組織ルールと現地法どちらかのより厳しい方に従う。	GDPR は現地法より優位
27. その他	発効日を明確に示す。	発効日を明確に示す。	（同等）

この表は抽出した項目に関してそれぞれにおける両制度の特徴を抜き出して要約したものである。それぞれ共通項目、BCR に特有の項目、CBPR に特有の項目があるが、27 項目のうち 7 つについては、違いは少なく同等の要求となっていることがわかった。

前述のように備考欄でまとめられている CBPR の特徴に関して 27 項目を通じて見ると、CBPR の特徴的な点として注目すべき傾向は多様性、AA の役割、具体性の 3 点に集約して考えることができる。この 3 点を以下に示す。

図表 5　BCR との要求事項の比較マッピングから見た CBPR の特徴の概要

特徴	説明	例	利点
多様性の尊重	参加国（エコノミー）の多様な法制度や文化、データ保護のレベルの違いを尊重し、柔軟な枠組みを提供する。	項目 1：国内法が厳しい場合は国内法を優先し、CBPR が厳しい場合は自主的な対応を促す。 項目 10：データ主体の同意の前提で、関連する目的での利用を認める。	多様な参加国が参加しやすくなる。
認証機関の役割	APEC の AA が認証を行い、データ主体の権利保護においても重要な役	項目 4：データ主体は、AA の紛争解決プロセスを利用できる。	参加国間の信頼関係を構築し、制度の信頼性を高める。

特徴	説明	例	利点
	割を担う。		
具体的な要件記述	多くの項目で具体的な要件が記述されている。	項目 7, 8：グループ内外の処理者に対する要件を詳細に規定する。 項目 13, 14：要配慮データの取り扱い、透明性確保のための具体的な規定を設ける。	組織にとって遵守すべき基準が明確になり、運用しやすくなる。

表中の「項目」番号は前表における1から27までの項目を指す。

これらの特徴から見て、CBPRは多様性を尊重しつつ、具体的な要件を設けることで、実効性と柔軟性を両立させた制度と言える。

(3) 制度の背景、運用実態と要求事項から見た実効性比較

前項(2)で示した要求事項に加えて制度のそもそもの背景や運用実態について分析を加えて、両制度の実効性について比較分析を行う。BCR の具体的な取得プロセスについては以下の表にまとめるが、多くの点で CBPR とはかなり異なる手続きが必要とされる。特に承認の最終決定である欧州委員会の承認を得るまでの間、各国の DPA を主管監督機関として選定し、審査を得ることが必要で、二重の審査手続きを前提とした制度となっている点が大きく異なる。

図表 6　GDPR における BCR 取得手順

手順	内容
1.BCR の策定	企業グループ内で適用されるデータ保護ルールを策定する。GDPR の要件を満たす必要があり、データ主体の権利、データ処理の目的、データセキュリティ対策など、詳細な内容を盛り込む必要がある。
2.主管監督機関の選定	企業グループの拠点がある EU 加盟国のデータ保護機関の中から、主管監督機関を選定する。
3.主管監督機関への申請	策定した BCR を主管監督機関に申請する。
4.主管監督機関による審査	主管監督機関は、BCR が GDPR の要件を満たしているか審査を行う。
5.欧州データ保護会議（EDPB）の意見	主管監督機関は、EDPB に BCR の承認について意見を求める。
6.欧州委員会の承認	EDPB の意見を踏まえ、欧州委員会が BCR を承認する。
7.BCR の施行	承認された BCR を企業グループ内で施行する。
8.定期的な見直し	法令や技術の変化に対応するため、BCR を定期的に見直し、必要があれば更新する。

また、特に日本の企業は、CBPR の比較対象としては、ここまで取り上げた BCR に限定せず越境移転ツールとして比較することが多い。ただし EU 全域において認証制度として意味を持つ点で、その中でも BCR を主要な比較分析の対象としてきたが、SCC および十分性認定に基づく越境データ移転に関しても比較対象となりうる点もあるので、ここでは GDPR の中での越境移転ツールの比較をまとめる。

SCC については運用面において、コピーの保存や適時の更新、監査機関への協力などの義務が生じるほか、内容的には GDPR を根拠にしている点で、その厳格さや柔軟性については BCR に準じると考えて良い。

国・地域単位で成立する十分性認定については企業単位で有効化できるものではないので、各国政府による交渉が必要となる。その中には GDPR と国内法制度及びその運用に関して同等性を担保するための付加的措置（我が国においては規則・ガイドラインの改定）

により、対象国の個人データ保護制度そのものが変化する場合もあることが、企業にとっての重要な検討対象である。

図表 7　GDPR における３つの代表的なデータ移転ツールの比較

項目	BCR	SCC	十分性認定
法的根拠	GDPR 第 46 条	GDPR 第 46 条	GDPR 第 45 条
性質	多国籍企業グループ内規則	契約条項	欧州委員会による決定
対象	多国籍企業グループ内	データ移転元と移転先	第三国の法制度全体
承認	監督機関の承認が必要	欧州委員会の承認済み条項を使用	欧州委員会が決定
範囲	企業グループ全体	特定のデータ移転	第三国への全てのデータ移転
データ主体の権利	詳細な情報提供義務、権利行使手続きを規定	SCC の条項に基づく情報提供、権利行使手続き	第三国の法制度で保障
データ処理の目的	明確に定義	SCC に記載された目的に限定	第三国の法制度による
データセキュリティ	企業の規模・リスクに応じた対策	SCC 付属文書で特定	第三国の法制度で担保
第三者提供	グループ内ルールを規定	SCC のルールに従う	第三国の法制度による
責任分担	グループ内での責任分担を明確化	データ移転元と移転先の責任分担	双方の法制度に従うが、ケース毎に個別判断
監督	遵守状況の監視体制	データ移転元による監視	欧州委員会による定期的な見直し
柔軟性	高い	中程度	なし
費用	高い	低い	なし
更新	定期的な見直しと更新	欧州委員会による更新	欧州委員会による見直し

GDPR そのものは認証制度ではなく、この比較表にある通り BCR 以外の移転ツール（SCC と十分性認定）は、それぞれ目的や性質が異なる。したがって、CBPR 認証制度に対する直接の比較対象としては BCR を代表として扱うのが適切である。ただしいずれも越境データ移転ツールとしては EU 法（GDPR）を同一の根拠としているので、BCR と CBPR の

比較を中心に、事業者へ提供できる価値、個人情報政策上の効果を比較することができる。

(4) 制度概要・運用形式上の視点とプロセスの比較

申請企業への付加価値訴求においては、内容面としての要求項目とともに制度の運用などを加味した論点を以下の項目にまとめる。

- EU 法（BCR を例に）においては法的な規定はすべて GDPR に準拠していて整合性が強い。一方で、EU に関連する事業に伴う越境移転が対象であり、EU に関連しない事業については基本的に実効的ではない。
- BCR は企業グループ内の移転を適法化するためのものであるため、グループ外企業へのデータ移転は管理の対象として検討項目には入るが、BCR の承認により適法化されるものではない。また、CBPR は、申請企業の審査対象業務を審査し認証するため、BCR と比較して実効性が高い。
- 直接コストと必要な人的リソースについては、要件の具体性が事業者側の重要な関心事項である。前項のとおり、CBPR は具体的な要件記述がなされている点が BCR と比較して優位といえる可能性がある。したがって、柔軟性のほか、拡張性、予見可能性、将来性といった事業者にとって隠れコストとなり、またリスクとしてあらかじめ想定しておくことが必要な事項についても、AA が個人データの取扱いの適正性を詳細に審査し、第三者として認証することが CBPR の利点となることが考えられる。
- 各制度独自部分の量と内容面、および制度の広がり、支援体制（認証制度の理解、認証取得、運用の面での支援）から見ても両制度の性質が大きく異なる。データ主体から見た場合、BCR はデータ保護機関の目線で管理者・処理者の責任を規定する側面が大きい。BCR の承認を支援する社会的体制、しくみは任意に発展してゆくことが考えられる。一方、CBPR は各国 DPA のみならず、各国 DPA から認定を受けた AA が機能する。この点から見ても、企業の個人情報保護体制を総体的に支援する構成になっている。

(5) BCR と CBPR との比較分析のまとめ

CBPR と BCR に代表される GDPR の目指すものは、1980 年の OECD プライバシーガイ

ドラインに記載された 8 原則[10]を共有し、越境データ移転に伴う個人情報保護を適切に高度化する点で同一であるが、その実現レベルにおいて大きく異なる点を改めて認識した上で、現実の業務に即した制度の適用について理解を訴求する必要がある。

CBPR は「相互運用」、「執行協力」が基礎で、定められたある範囲の中での多様性を前提にする。そこに利点欠点が存在する。GDPR は原則的には EU 加盟地域が対象となる範囲であり、データ移転もその地域を発信あるいは受信となる範囲において統一して適用されることを意図したものである。多義性や多様性を極力排除する構造となっている。

この 2 つの制度の比較を随時更新して理解を深め、正しい制度運用と事業者の越境データの移転を手助けできるような施策検討を進めていく必要がある。

図表 8　BCR と CBPR の違い

	項目	各認証制度が示す意味の違い
制度としての要求項目	多様性への対応	BCR ：基準を統一化して差異を最小限にする。 CBPR：多様性を前提に相互運用性を重視する。APEC 域内、GCBPR は APEC 域外の国・地域において比較的柔軟に受容される可能性が高い。
	認証機関の役割	BCR ：直接 DPA の執行対象となってしまう。 CBPR：AA が認証機関の役割に加えて、各国 DPA とともに監督、執行、苦情処理等の役割を持つ調整者となりうるため、柔軟性が高い。
	要求項目の具体性	BCR ：要求項目は、表現の解釈が必要になることが多い。 CBPR：質問形式で、記述が具体的である場合が多い。
運用面・執行面・手続き面	認証取得プロセスの違い	BCR ：主審査機関としての各国 DPA への申請を経たうえで欧州委員会が最終承認を行う。 CBPR：各国の AA が審査及び認証の主体となる。
	事故発生時・訴訟対応	BCR ：EU 域内に拠点を持っていることが前提であり、あらかじめ定められている手続きに従う CBPR：データ主体の居住地、CBPR 認証企業・AA の所在地を管轄する裁判所など。
	監督当局の役割・制裁	BCR ：DPA の監視・指導・勧告・命令などに従う必要がある CBPR：AA が上記執行等の一部分を柔軟に DPA と共に分担する体制となる。

[10] OECD が 1980 年に採択した「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」に記述されている 8 つの原則。フレームワークの 9 原則は OECD ガイドライン 8 原則を参考に作成された。

	項目	各認証制度が示す意味の違い
審査対象の違い	対象地域の違い	BCR ：EU 域内で取得した個人データの取扱い業務を行う事業者が対象。それ以外の地域における業務に関する越境データ移転については直接の効力を持たない。 CBPR：参加する国・地域（GCBPR は APEC 域内に限らない）

2.1.2 マッピング調査結果

(1) 日本の代表的な認証制度との比較

我が国では、ISO 規格に基づく ISMS 適合性評価制度[11]や JIS 規格に基づくプライバシーマーク制度など、情報の取扱いに関する第三者認証制度の認証企業が多数存在しており、新規の取引を始める場合や事業の入札に応募する際等、情報の取り扱いやセキュリティ体制のアカウンタビリティツールとして、第三者認証の取得状況を尋ねられる事も少なくない。GCBPR の申請企業が、既にこれらの第三者認証を取得している可能性が高いと考えられるため、まず、日本の代表的な認証制度を概観し、特に認証数の多い認証制度を比較対象として、分析を行った。

日本における代表的な認証制度・評価制度の認証数と、それぞれの認証制度・評価制度の概要は以下のとおりであった。

図表 9 日本の代表的な認証制度・評価制度の認証数

	認証制度・評価制度	認証数	調査日
1	プライバシーマーク制度	17,707	2025 年 1 月 7 日
2	ISMS 認証（ISMS 適合性評価制度）	8,009	2025 年 1 月 8 日
3	ISMS クラウドセキュリティ認証[12]	615	2025 年 1 月 8 日
4	ISMS-PIMS 認証	65	2025 年 1 月 8 日
5	ISMAP/ ISMAP LIU	77/1	2025 年 1 月 9 日

[11] ISMS 適合性評価制度とは、認証を公正に運用するために、国際的な枠組みがあり、第三者機関として組織の ISMS を審査、認証する ISMS 機関、それらの認証機関が適切に認証審査を実施できることを審査し確認する「ISMS 認定機関」からなる。
[12] ISMS クラウドセキュリティ認証、ISMS-PIMS 認証を取得するには、ISMS を取得している必要がある。

① プライバシーマーク制度

図表 10 プライバシーマーク制度の概要

項目	説明
概要	プライバシーマーク制度は、事業者の個人情報を取り扱う仕組みとその運用が適切であるかを評価し、その証として事業活動においてプライバシーマークの使用を認める制度
準拠法令/規格等	「個人情報保護法」 「JIS Q 15001：2023 個人情報保護マネジメントシステム―要求事項」 「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針 【JIS Q 15001:2023 準拠 ver1.0】」
付与機関/審査機関数	付与機関：（一財）日本情報経済社会推進協会（JIPDEC） 審査機関数：20[13]
申請/認証単位	法人単位（国内に活動拠点を持つ事業者）[14]
付与事業者数	17,707
更新期間	2 年
標準運用期間	6 か月～1 年
認証制度の開始年	1998 年
公式情報	https://privacymark.jp/

② ISMS 認証（ISMS 適合性評価制度）

図表 11 ISMS 認証（ISMS 適合性評価制度）の概要

項目	説明
概要	ISMS 認証は、第三者である ISMS 認証機関が、組織の構築した ISMS が ISO/IEC 27001（JIS Q 27001）に基づいて適切に運用管理されているかを認証する。
準拠法令・規格等	ISO IEC 27001:2022（JIS Q 27001:2023）情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項
認定機関/認証機関数	認定機関：（一社）情報マネジメントシステム認定センター（ISMS-AC） 認証機関数：27[15]

[13] https://privacymark.jp/system/institution/agency/member_list.html
[14] 医療法人および学校法人等については一部例外がある。
[15] ISMS 機関一覧 https://isms.jp/lst/isr/

項目	説明
申請/認証単位	組織 ※組織の必要に応じて定めることができる。必ずしも全社を範囲とする必要はないため、大企業等では同一企業内に複数の認証が存在する事もある。
認証数	8,009
更新期間	3 年ごと （1、2 年目サーベイランス審査、3 年目再認証審査）
標準運用期間	6 か月～1 年
認証制度の開始年	2002 年
公式情報	https://isms.jp/isms.html

③ ISMS クラウドセキュリティ認証

図表 12 ISMS クラウドセキュリティ認証の概要

項目	説明
概要	ISMS クラウドセキュリティ認証は、ISMS 認証の認証範囲内に含まれる組織のクラウドサービスの提供及び／又は利用に関して、ISO/IEC 27017 に規定されるクラウドサービス固有の管理策が適切に実施されていることを認証する。ISMS クラウドセキュリティ認証を取得するには、ISMS 認証を取得している必要がある。
準拠法令・規格等	ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517-1.0）[16]
認定機関/認証機関数	認定機関：（一社）情報マネジメントシステム認定センター（ISMS-AC） 認証機関数：18
申請/認証単位	ISMS 認証を取得していることが条件となり、ISMS 認証範囲をすべて含める必要はない。（対象はクラウドサービスプロバイダ、クラウドサービスカスタマ）
認証数	615
更新期間	ISMS 認証と同じ
標準運用期間	6 か月～1 年
認証制度の開始年	2016 年
公式情報	https://isms.jp/isms-cls.html

[16] JIPDEC が定めたもの

④ ISMS-PIMS 認証

図表 13 ISMS-PIMS 認証の概要

項目	説明
概要	ISMS-PIMS 認証は、ISMS 認証の認証範囲内に含まれる組織のマネジメントシステムが ISO/IEC 27701 に基づくプライバシー情報マネジメントシステムの要求事項に適合していることを認証する。 ISMS-PIMS 認証を取得するには、ISMS 認証を取得している必要がある。
準拠法令・規格等	ISO/IEC 27701:2019 プライバシー情報マネジメントのための ISO/IEC 27001 及び ISO/IEC 27002 の拡張 -要求事項及び指針-
認定機関/認証機関数	認定機関：（一社）情報マネジメントシステム認定センター（ISMS-AC） 認証機関数：7
申請/認証単位	ISMS 認証を取得していることが条件となり、ISMS の認証範囲をすべて含める必要はない。（対象は、PII[17]管理者、PII 処理者）
認証数	65
更新期間	ISMS 認証と同じ
標準運用期間	6 か月～1 年
認証制度の開始年	2021 年
公式情報	https://isms.jp/isms-pims.html

⑤ 政府情報システムのためのセキュリティ評価制度（ISMAP/ ISMAP LIU）

図表 14 ISMAP/ ISMAP LIU の概要

項目	説明
概要	政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービ

[17] 個人識別用情報（Personally Identifiable Information）を言う。個人情報保護法の「個人情報」や「個人データ」二兎留まらず、個人を識別するために使用される又はされ得る情報を指す。

項目	説明
	スの円滑な導入に資することを目的とした制度。 ISMAP 制度のうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とする仕組みの名称を、ISMAP for Low-Impact Use: ISMAP-LIU（イスマップ エルアイユー）としている。
準拠法令・規格等	「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」 （令和 2 年 1 月 30 日サイバーセキュリティ戦略本部決定）
運営/監査機関数	運営：内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省 （独）情報処理推進機構（IPA）は、本制度の制度運用に係る実務及び評価に係る技術的な支援を行う。 監査機関数：5[18]
申請/認証単位	クラウドサービス事業者（認証単位はクラウドサービス）
認証数	ISMAP　77（LIU　1）
更新期間	1 年 4 か月（毎年審査）
標準運用期間	1 年～1 年 6 か月
認証制度の開始年	2020 年
公式情報	https://www.ismap.go.jp/csm

⑥　日本の代表的な認証制度と CBPR

日本の代表的な認証制度と CBPR の概要を比較した結果を以下に示す。

図表 15　CBPR と日本の代表的な制度概要の比較

	認証/ 制度名	CBPR	P マーク	ISMS	ISMS クラウドセキュリティ	ISMS -PIMS	ISMAP /LIU
1	管理対象	越境 個人データ	個人情報	情報	クラウド サービス 上の情報	PII	クラウド サービス のセキュリティ
2	規格等	CBPR 要求事項	P マーク 運用指針	27001 要求事項	27017 要求事項	27701 要求事項	ISMAP 管理基準

[18] 監査機関リスト https://www.ismap.go.jp/csm?id=audit_institution_list

	認証/ 制度名	CBPR	P マーク	ISMS	ISMS クラウドセキュリティ	ISMS -PIMS	ISMAP /LIU
3	開始年	2016	1998	2002	2016	2021	2020
4	認証単位	法人 （日本）	法人 （日本）	組織（範囲を指定可）	ISMS 認証範囲か一部		クラウドサービス
5	更新期間	1 年	2 年	3 年 ※毎年審査を行う			1 年 4 か月
6	認証数 付与数[19]	4	17,707	8,009	615	65	77/1
7	審査 機関数	1	20	27	18	5	4

2025 年 1 月時点

CBPR は、越境する個人データの取扱い業務を審査対象[20]とするが、それ以外の制度はマネジメントシステムの運用状況を審査対象とする。

「更新期間」は、認証制度ごとに更新期間の差はあるが、P マーク以外は毎年審査を行っているため、適正な取り扱いがなされている事を年 1 回必ず確認できる制度である。

「認証数/付与数」は、1998 年に開始した P マークの付与数が 17,707 と最も多く、次に ISMS が 8,009 と続いている。いずれも開始から 20 年が経過し、個人情報と情報セキュリティに関するアカウンタビリティツールとして契約の場面で確認されることも多いことが、認証数/付与数の多さからも確認することができる。

(2) CBPR との制度比較

前項より、情報の取り扱いに関する第三者認証制度の中で、日本における代表的な認証制度・評価制度のうち認証数が最も多かったのは、P マークと ISMS であり、GCBPR の申請企業が、既に情報に関する何らかの認証制度を取得しているとした場合、この 2 つの制度である可能性が高いと想定される。複数の認証を取得しようとする場合、認証制度の運用・維持管理のため、申請企業は多くの労力とコストを負担しなければならず、新たな認証制度の取得におけるハードルになる可能性は否めない。そこで、CBPR とこれら 2 つ第

[19] 2025 年 1 月現在の調査数
[20] 審査対象は、各国の AA により異なる。

三者認証とを比較し、CBPR の要求事項、審査基準、審査に係る文書類、審査準備等を分析した結果をとりまとめた。

① 制度概要の比較

CBPR と P マーク及び ISMS の制度概要の比較を行った結果を以下に示す。

図表 16 制度概要の比較

認証/制度名 / 項目	CBPR	P マーク	ISMS
準拠法令・規格等（認証基準）	APEC プライバシーフレームワーク（各国法制度に従う）	JIS Q 15001：2023 個人情報保護マネジメントシステム―要求事項（プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針【JIS Q 15001:2023 準拠 ver1.0】）	JIS Q 27001 : 2022（JIS Q 27001:2023）情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項
目的	国境を越えて移転する個人データの適正な取り扱い	個人情報の保護と利活用	情報セキュリティマネジメントシステムを確立し、実施・維持し、継続的に改善する。情報資産を、「完全性」「機密性」「可用性」の三要素の観点から適切に管理する
管理対象	国境を越えて移転する個人データ	事業の用に供するすべての個人情報が対象	組織が保有する情報資産
要求事項の概要	フレームワークの原則に基づく個人データの取り扱い （通知、取得の制限、個人情報の利用、選択、個人情報の完全性、セキュリティ対策）	事業の要に供する個人情報の適切な取り扱い （個人情報の取得、利用、共同利用、委託、提供、安全管理（情報セキュリティ）、開示等要求対応、苦情対応など）	情報の機密性、完全性、可用性の維持 （情報資産の重要性、リスクに応じた適切な情報セキュリティ）
要求事項への適合	要求事項を全て満たす必要がある	要求事項を全て満たす必要がある	要求事項と管理策を全て満たす必要がある

項目＼認証/制度名	CBPR	P マーク	ISMS
			（一定条件による除外は可能）
アドオン	現時点では無い	現時点では無い	ISMS クラウドセキュリティ認証 ISMS-PIMS 認証
申請/認証単位	法人単位 （対象事業を特定したうえで法人単位）	法人単位 （国内に活動拠点を持つ事業者。学校法人、医療法人の例外あり）	組織 （組織の必要に応じて定めることができる。必ずしも全社を範囲とする必要はない）
認証数	4	17,707	8,009
更新期間	1 年	2 年	3 年 （1、2 年目にサーベイランス審査を行う）

「申請/認証単位」は、CBPR と P マークは日本に法人格のある組織単位での審査となるが、ISMS は組織として定めた範囲であれば、全社である必要はなく、プロジェクトや組織の一部でも可能である。また、国内に限らず、海外のグループ会社を適用範囲に指定できる点が大きく異なる。

「要求事項への適合」は、CBPR と P マークと ISMS はすべての要求事項に対応する必要がある。ただし、ISMS は組織内の事業において実施していない場合や、リスク分析の結果、管理策を除外できる。除外する場合は、その除外理由を明確にしなければならない。

「更新期間」は、CBPR が 1 年、P マークが 2 年、ISMS は 3 年となっている。ISMS は 3 年を 1 サイクルとし、サーベイランス審査が毎年実施される。初回審査や再認証審査に比べ審査範囲の差はあるが、1 年ごとに審査を実施するため事業者の状況を常に最新の状態で把握している点で、CBPR の 1 年と類似性がある。CBPR は、認証後半年を目途に「モニタリング」を行い、認証取得時点からの事業者の変更状況を確認している。

② フレームワークの原則との比較

CBPR の申請企業は、自社の越境する個人データの取扱いや情報を取り扱う推進体制等について自己評価を行う。自己評価を行う際に記入する「APEC 越境プライバシールールシステム事前質問書」（以下、「事前質問書」という。）はフレームワークの原則に基づき作

成された質問書であり、基本情報と 50 の質問項目[21]で構成されている。この原則は、世界各国の個人情報保護法制度の事実上の基礎となっている OECD プライバシーガイドラインの 8 原則に準拠するもので、被害の防止を加えた 9 つの原則（被害の防止、通知、収集制限、個人情報の利用、選択、個人情報の完全性、安全管理、アクセス及び訂正、アカウンタビリティ）から構成される[22]。なお、「事前質問書」は 9 つの原則から「被害の防止」を除いた、「1.通知」「2.取得の制限」「3.個人情報の利用」「4.選択」「5.個人情報の完全性」「6.セキュリティ対策」「7.アクセス及び訂正」「8.責任」の 8 つの原則の要求事項に基づいて作成されており、原則の項目毎に確認する内容を以下に示す。

図表 17　事前質問書で確認する原則に基づく内容

	原則	確認する内容
1	通知 (質問 1～4)	APEC 通知原則に照らし、①取得される個人情報、移転先、及び利用目的に関する貴社のポリシーを本人に必ず理解してもらっているか、②必要最低限の取得になっていることを条件として、本人の個人情報が取得されるタイミング、移転先、及び利用目的を本人に必ず通知しているか。
2	取得の制限 (質問 5～7)	APEC 取得原則に照らし、個人情報の取得がその取得のために表明した目的に確実に限定されているか。
3	個人情報の利用 (質問 8～13)	APEC 利用原則に照らし、個人情報の利用が取得目的及びこれらに適合又は関連するその他の目的を達成することに限定されているか。
4	選択 (質問 14～20)	選択手順に関する規定の条件に照らし、個人情報の取得、利用及び開示に関して本人が必ず選択できるようになっているか。
5	個人情報の完全性 (質問 21～25)	記録について正確性及び完全性を維持させ、並びに最新の状態に維持しているか。
6	セキュリティ対策 (質問 26～35)	個人がその個人情報を組織に預ける際に、個人情報の紛失、不正なアクセス、不正な破壊・利用・変更もしくは開示、又はその他の不正使用を防ぐために、その個人情報が合理的なセキュリティ対策によって確実に保護されているか。
7	アクセス及び訂正 (質問 36～38)	本人がその個人情報にアクセスして、訂正することができることを保障しているか。

[21] 50 の質問項目内に複数の選択肢が含まれるため、実際には 50 以上の回答が必要。
[22] 講演レポート「CBPR 認証の概要」（個人情報保護委員会）｜一般財団法人 日本情報経済社会推進協会
https://www.jipdec.or.jp/library/report/20240110-r02.html

	原則	確認する内容
8	責任 (質問 39～50)	APEC 原則の実施方法を遵守することについて確実に責任を果たしているか。また移転後にこの原則に従って個人情報を確実に保護するための合理的な措置を用意しているか。

続いて、フレームワークの原則ごとに確認する内容が、前述の日本の代表的な第三者認証制度の要求事項とどれだけ親和性があるのかを調査した。

図表 18　フレームワークの原則が含まれる割合

	原則	P マーク	ISMS	ISMS クラウドセキュリティ	ISMS -PIMS	ISMAP /LIU
1	通知	○	○	○	○	○
2	取得の制限	○			○	
3	個人情報の利用	○			○	
4	選択	○			○	
5	個人情報の完全性	○	○	○	○	○
6	セキュリティ対策	○	○	○	○	○
7	アクセス及び訂正	○			○	
8	責任	○	○	○	○	○
原則の項目との合致数		8/8	4/8	4/8	8/8	4/8

「個人情報」に関連した第三者認証制度である「P マーク」「ISMS-PIMS」は、フレームワークの原則と同様の要求事項が含まれることが確認できた。一方で、情報セキュリティやクラウドサービスの認証制度である「ISMS」「ISMS クラウドセキュリティ」「ISMAP」は、対象とする情報やシステムの違い（主にセキュリティ）から、フレームワークの原則と同様の要求事項が含まれないものもあった[23]。

[23] 国内法への準拠は前提であるが、ここでは各認証制度に同様の粒度での要求事項が存在するかを調査した。

(3) CBPR[24]と P マーク、ISMS の制度比較

前項の調査結果から、我が国で運用実績のある代表的な情報に関する認証制度のうち、GCBPR 申請企業の負担を軽減する要素の有無を確認するため、特に認証数の多かった P マークと ISMS と CBPR を、より類似性のある要求項目及び認証基準等の詳細な比較調査を行った。

① P マーク

P マークは 1998 年に認証制度の運用を開始し、27 年が経過した。現在は付与事業者数が 17,707 社（2025 年 1 月現在）となり、事業者の規模にかかわらず最も多く付与されている第三者認証制度である。2003 年に個人情報保護法が施行された事を契機として、事業者における個人情報の取扱いを評価する第三者評価のニーズや中小企業におけるアカウンタビリティツールとしての需要が高まり、付与事業者数が増加した。

後発の認証制度に比べると認知度が高く、顧客や取引先、省庁等の受託事業の入札時に個人情報の適切な管理やセキュリティ体制の証として、確認事項に含まれるケースもある。我が国の個人情報取扱事業者にとって、適正な取り扱いのアカウンタビリティや顧客の信頼を得るために、申請企業の人気が高まっており、付与数は現在も増加傾向となっている。

② ISMS 認証（ISMS 適合性評価制度）

ISMS 適合性評価制度は組織の情報セキュリティのための仕組みが国際規格に適合していることを評価する制度である。この国際規格は ISO/IEC 27001（JIS Q 27001）で定められている。「ISMS 認証」とは、第三者である ISMS 認証機関が、組織の構築した ISMS が ISO/IEC 27001（JIS Q 27001）に基づいて適切に運用管理されているかを、利害関係のない公平な立場から審査し証明したものである。ISMS 認証は、近年急速に増加している不正アクセスやランサムウェア等による被害及び内部不正や委託先事業者による情報漏えい等の脅威に対して、総合的な情報セキュリティ対策の基盤を実現するものとして活用されている。現在、認証組織数が 8,009 社（2025 年 1 月現在）となり、増加傾向にある。増加の一因として、情報セキュリティに対する企業意識の高まり、サイバーセキュリティの重要性

[24] 本調査報告書の作成時点において、CBPR システムの運用は APEC と Global CBPR Forum であるが、認証までを行っているのは APEC CBPR のみであるため、具体的な審査項目や認証基準の比較は、APEC CBPR システムとの比較とする。

の高まり、コロナ禍によるクラウドとリモートワークの普及が事業者の規模に関わらず広まったことで、組織の情報セキュリティ意識を継続的に向上させるために不可欠な取り組みとして認識されたことが挙げられる。

③　申請手続きの比較

CBPR、P マーク、ISMS の各制度における申請手続きについて、比較を行った結果を以下に示す。

図表 19　申請手続きの比較

比較項目	CBPR	P マーク	ISMS
申請に係る費用	（見積り） 情報の越境移転が発生する業務数、情報流の複雑さ、移転先（委託先・国や地域）等により異なる。 （法人単位の審査） モデル審査料 664,657 円 ・資本金 3 億円以上で、かつ従業員 301 人以上のサービス業（海外支店の従業員情報） 事業者：APEC 域内に向けてネット通販を行い、日本と APEC 域内の国との間で顧客データの取扱いを行っている。	（固定料金） 事業規模により異なる。 （法人単位の審査） 初回申請費用 小規模　314,288 円 中規模　628,573 円 大規模 1,257,144 円 ※申請料、審査料、付与登録料を含む。	（見積り） 組織の要員数に基づく工数の算定の目安[25]が定められている。ただし、サイト数や業務内容によって工数の調整が可能である。また、工数の単価は認証機関が決定する。 （組織単位の審査） 数 10 万～数 100 万円×組織数 ※大企業の個社単位では、数千万円を超える場合もある。
申請に必要な書類 （提出方法）	・申請書（統一様式） ※追加書類の設定可 ・根拠資料 （データ形式で提出）	・申請書（審査機関別） ・根拠資料 （申請様式や提出方法は審査機関で異なる）	・申請書（認証機関別） ・根拠資料 （申請様式や提出方法は認証機関で異なる）
審査概要	事前質問書に基づき、事業者が自己評価した内容がフレームワークに適合しているか、日本の認証	審査基準と事業者の定めた規定に従い、個人情報マネジメントシステムの対応状況を審査する。	要求事項と事業者が定めた規定及び管理策に基づき、情報セキュリティマネジメントシステムの対

[25] 27006 JIS Q 27006:2018 情報技術―セキュリティ技術―情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項

比較項目	CBPR	P マーク	ISMS
審査方法	基準を基に申請書と根拠資料の内容を審査する。 ・文書審査と現地審査 ・必要に応じて現地審査前のヒアリングを実施する ・認証取得後モニタリングを実施（半年後）	・文書審査と現地審査	応状況を審査する。 ・初回審査では①第一段階と②第二段階の審査を実施

1) 審査に係る費用

・CBPR：

情報の越境移転が発生する審査対象となる業務数、情報流の複雑さ、移転先の数（委託先、移転先の国や地域等）を勘案し、見積り方式で審査料の算定を行う。

・P マーク：

事業者の規模、新規又は更新かにより、予め費用が定められている固定料金制である。

・ISMS：

CBPR と同様に、審査の対象とする組織の範囲やサイト数、要員数によって工数と金額が異なる見積り方式で算定を行う。なお、一部の情報においては、算定の目安となる根拠が開示されている。また、認証単位は、CBPR と P マークは法人単位であるが、ISMS は組織単位のため、大手 SIer 等では事業部単位で ISMS を取得するケースもあり、個社として、全ての組織やプロジェクト単位での認証費用を合算すると、数千万円という額になる事業者も存在する。

2) 認証にあたり必要な書類

・CBPR：

「事前質問書」を含む申請書（様式類）と根拠資料のすべてを、データ化した状態で提出する。

・P マーク：

審査機関の様式に従い規程や記録類の根拠資料を提出する。

・ISMS：

認証範囲と審査費用の算定に必要な従業者数などの情報を事前に認証機関に提出する

が、申請様式の定めはない。

3) 審査方式

・CBPR：

申請書類の不備がないか事務局が確認を行った後、提出された様式及び根拠資料について審査員が文書審査を行い、指摘事項（是正含む）が改善されるまで事業者と対話型の審査を行う。初回申請や、新規業務が追加された場合等、提出資料では確認出来ない事項について、現地審査までに事前ヒアリングを実施する。現地審査を行い、指摘事項の改善後、審査会を経て認証が付与される。

・P マーク：

申請書類の不備がないか事務局が確認を行った後、審査員が文書審査を行い、現地審査前に文書審査の結果を事業者に提供する。現地審査で不備が見つかった場合、現地で不備の内容を伝え、後日書面でも改善すべき事項を通知する。指摘事項の改善後、審査会を経て P マークが付与される。

・ISMS：

初回審査は、第一段階と第二段階の 2 段階で実施される。第一段階審査では主に文書類や第二段階に進むため準備ができているか確認を行う。第二段階審査は運用状況を中心に確認する。不適合がある場合、その改善後に認証が付与される。

(4) CBPR 審査との比較

P マーク、ISMS と CBPR との共通点、相違点を明白にするために、審査項目や根拠資料等を、次の比較対象事項で確認した結果は以下のとおりであった。

- ・事前質問書
- ・認証基準
- ・安全管理措置
- ・根拠資料

① 事前質問書との比較

CBPR 申請企業は、越境する個人情報の保護に関する取り組みについて事前に整備状況

と運用状況の自己評価を行う。審査では提出された資料を元に、フレームワークに対する準拠状況、維持するための体制に関する適合性・取り組みの妥当性を確認する。具体的には、「事前質問書」と「JIPDEC 追加質問書」にて自己評価の結果を提示し、根拠資料でそれを説明する。

「事前質問書」は基本情報と 50 の質問項目で構成されている。ここでは、50 の質問と P マーク審査要求事項（審査指針）、ISMS 要求事項（要求事項と管理策）との比較を行う。なお、50 の質問の中には、枝番としての質問項目が含まれているものもあるが、質問番号のみに基づき下記に記載した。（質問項目について同等の要求事項がある場合は“○”、無い場合は“空欄”、事業者による選択が可能な要求事項は“△”の表記とした。）

1) 通知

「通知」では、APEC 通知原則に照らし、①取得される個人情報、移転先、及び利用目的に関する貴社のポリシーを本人に必ず理解してもらっているか、②必要最低限の取得になっていることを条件として、本人の個人情報が取得されるタイミング、移転先、及び利用目的を本人に必ず通知しているかを確認した。

図表 20 「通知」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
1	1.上記の個人情報に適用されるポリシー等を記載した「個人情報に適用される方針やルール（契約書や約款等）に関して明瞭かつ入手しやすい説明書」（以下、「プライバシーステイトメント」という）を提供していますか？「はい」の場合、該当する文書のコピーまたは当該文書へのハイパーリンクを提出してください。	通知（個人情報保護方針）	○	○
	a)このプライバシーステイトメントには、貴社がどのように個人情報を取得するのかが説明されていますか？	通知（個人情報の取得）	○	
	b)このプライバシーステイトメントには、個人情報が取得される目的が説明されていますか？	通知（利用目的）	○	
	c)このプライバシーステイトメントでは、個人情報を第三者が利用できるようにするかどうかについて、またその場合の目的について本人に通知していますか	通知（第三者提供）	○	
	d)このプライバシーステイトメントでは、貴社	通知（窓口）	○	

質問 No	質問内容	カテゴリ	P マーク	ISMS
	の名称と所在地（取得した個人情報の取扱いと慣行に関する貴社の連絡窓口情報を含む）について開示していますか？			
	e)このプライバシーステイトメントでは、個人情報の利用と開示に関する情報を本人に提供していますか？	通知（開示情報の提供）	○	
	f)このプライバシーステイトメントでは、自分の個人情報にアクセスし修正することができますか、また、その方法に関する情報を本人に提供していますか？	通知（開示等）	○	
2	2.個人情報の取得時（直接であるか第三者の代行によるかを問わない）に、そのような情報を取得している旨を通知していますか？	通知（個人情報の取得）	○	
3	3.個人情報の取得時（直接であるか第三者の代行によるかを問わない）に、個人情報を取得する目的を明らかにしていますか？	通知（利用目的）	○	
4	4.個人情報の取得時に、個人情報を第三者に提供する場合があることを本人に通知していますか？	通知（第三者提供の通知）	○	

P マークには、ほぼ同等の要求事項があった。しかし、ISMS には方針やポリシーについての要求事項はあるが、CBPR の質問項目の粒度での要求事項はないため共通項目が少ない結果となった。

2) 取得の制限

「取得の制限」では、APEC 取得原則に照らし、個人情報の取得がその取得のために表明した目的に確実に限定されているかを確認した。2)～4)について、P マークには、ほぼ同等の要求事項があった。ISMS には、2)～4)の項目について CBPR の質問項目の粒度での要求事項はないため、共通項目がない結果となった。

図表 21 「取得の制限」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
5.	5.個人情報をどのように取得していますか？	-	-	-
	a).当人から直接。「はい」の場合、具体的に説明してください。	取得（直接取得	○	

質問 No	質問内容	カテゴリ	P マーク	ISMS
	b).第三者が代行による。「はい」の場合、具体的に説明してください。	取得（第三者代行）	○	
	c).その他。「はい」の場合、具体的に説明してください。	取得（個人情報の取得）	○	
6.	6.個人情報の取得（直接であるか第三者の代行によるかを問わない）は、取得目的、又は取得目的に関連する他の目的の達成に関する個人情報に限定されていますか？	取得（利用目的）	○	
7.	7.個人情報の取得に適用される管轄権の要件に合わせて、適法かつ公正な手段で個人情報を取得していますか？（直接であるか第三者の代行によるかを問わない）？	取得（第三者提供の通知）	○	

3) 個人情報の利用

「個人情報の利用」では、個人情報の利用が取得目的及びこれに適合又は関連するその他の目的を達成することに限定されているかを確認した。

図表 22 「個人情報の利用」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
8.	8.プライバシーステイトメントまたは取得時に出した通知に特定した通り取得する（直接であれ第三者の代行であれ）個人情報の利用は、当該情報の取得目的またはその他の矛盾のない関連する目的に限定されていますか？	利用：利用目的の特定	○	
9.	9.質問 8 の回答が「いいえ」の場合、以下のいずれかの状況において、関連のない目的で集めた個人情報を利用していますか？下欄に説明してください。	利用：利用に関する措置	○	
	a)本人の明白な同意に基づいている場合	利用：利用に関する措置	○	
	b)本人が要請したサービスまたは製品を提供するために必要なものの場合	利用：利用に関する措置	○	
10.	10.（直接であれ第三者の代行であれ）取得する個人情報を他の個人情報取得者に開示していますか？	利用：第三者提供者の開示	○	
11.	11.個人情報を個人情報処理業者に転送していますか？	利用：第三者提供	○	
12.	12.質問 10 または 11 への回答が「はい」の場合、その開示または転送は、取得目的またはそ	利用：第三者提供	○	

質問 No	質問内容	カテゴリ	P マーク	ISMS
	の他の矛盾のない関連した目的を果たすために行われたものですか？			
13.	13.質問 12 の回答が「いいえ」の場合、または適切な場合は、その開示や転送は以下の状況のいずれかにおいて行われていますか？	-	-	-
	a)本人の明白な同意に基づいている場合	利用：明白な同意	○	
	b)本人が要請したサービスまたは製品を提供するために必要なものの場合	利用：サービスの提供のため	○	
	c)準拠法に従う場合	利用：法令による利用	○	

4) 選択

「選択」では、選択手順に関する規定の条件に照らし、個人情報の取得、利用及び開示に関して本人が必ず選択できるようになっているか確認した。

図表 23 「選択」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
14.	14.個人情報の取得に関連して本人が選択できる方法を提供していますか？	選択：個人情報の選択	○	
15.	15.個人情報の利用に関連して本人が選択できる方法を提供していますか？	選択：個人情報の利用	○	
16.	16.個人情報の開示に関連して個人が選択できる方法を提供していますか？	選択：個人情報の提示	○	
17.	17.個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示または提供されていますか？	選択：選択手順の表示	○	
18.	18.個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それは明瞭な表現ですぐ分かるようになっていますか？	選択：選択手順の明瞭さ	○	
19.	19.個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、その選択は	選択：選択の簡易さ	○	

質問 No	質問内容	カテゴリ	P マーク	ISMS
	簡単に利用でき手頃なものですか？			
20.	20.必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄または必要に応じて添付資料として説明を添えてください。	選択：選択手順の用意	○	

5) 個人情報の完全性

「個人情報の完全性」では、記録について正確性及び完全性を維持させ、並びに最新の状態に維持しているか確認した。

図表 24 「個人情報の完全性」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
21.	21.保管している個人情報が、利用目的に必要な限りにおいて、最新、正確、必要最低限なものであることを検証する措置を講じていますか？	個人情報の完全性：正確性	○	○
22.	22.利用目的上必要な限りにおいて、不正確、不十分で、古くなった個人情報を修正する方法を用意していますか？	個人情報の完全性：修正	○	○
23.	23.不正確、不完全、または古くなった情報が利用目的に影響すると思われ、当該情報の転送後に修正がなされた場合、その修正について、当該個人情報の転送先である処理業者等に連絡をしていますか？	個人情報の完全性：処理業者への連絡	○	○
24.	24.不正確、不完全、または古くなった情報が使用目的に影響すると思われ、情報の開示後に修正が行われた場合、その修正について個人情報の転送先であるその他の第三者に伝えていますか？	個人情報の完全性：その転送先への修正連絡	○	○
25.	25.不正確、不完全、または古くなった情報に気づいた場合は連絡をするよう、委託や共同利用等を行う事業者に求めていますか？	個人情報の完全性：委託や共同利用者への連絡	○	○

P マークには、ほぼ同等の要求事項があった。ISMS は CBPR の質問項目の粒度での要

求事項は無いが、ISMS は情報セキュリティの 3 要素[26]の一つである「完全性」に該当することから、全項目対象となった。

6) セキュリティ対策

「セキュリティ対策」では、個人がその個人情報を組織に預ける際に、個人情報の紛失、不正なアクセス、不正な破壊・利用・変更若しくは開示、又はその他の不正使用を防ぐために、その個人情報が合理的なセキュリティ対策によって確実に保護されているか確認した。

図表 25 「セキュリティ対策」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
26.	26.情報セキュリティ方針を実装していますか？	セキュリティ対策：セキュリティ方針	△	○
27.	27.個人情報を、情報の紛失または不正なアクセス、破壊、利用、修正または開示またはその他の悪用のリスクから保護するために実施している、物理的、技術的、運営上の安全保護策について説明してください	セキュリティ対策：物理的、技術的安全管理	○	○
28.	28.質問 27 に対応して特定した安全保護策が、脅かされる危害の可能性と程度、情報の機密性、また保管状況に鑑みてなぜ適当なのか説明してください。	セキュリティ対策：脅威への対応	○	○
29.	29.従業員に個人情報のセキュリティの維持の重要性についてどのように認識させているか説明してください（定期的な研修や監督など）	セキュリティ対策：教育と監督）	○	○
30.	30.次のような手段で、迫る危害の可能性と程度、情報の機密性、保管状況に適した安全保護策を実施していますか？	-	-	-
	a)従業員の研修や管理その他の安全保護策	セキュリティ対策：研修と安全保護	○	○
	b)ネットワークやソフトウェア設計、および情報処理、保存、転送、廃棄などの、情報システムや情報管理	セキュリティ対策：情報管理	△	○
	c)攻撃、侵入、その他のセキュリティ障害の検出、防止、対応	セキュリティ対策：脅威への対策	△	○
	d)物理的セキュリティ	セキュリティ対	○	○

[26] 情報セキュリティの 3 要素「機密性」「完全性」「可用性」

質問 No	質問内容	カテゴリ	P マーク	ISMS
		策：物理的セキュリティ		
31.	31.個人情報の安全な処分のための方針を実施していますか？	セキュリティ対策：廃棄	○	○
32.	32.攻撃、侵入、その他のセキュリティ障害を検出、防止、対応するための措置を実施していますか？	セキュリティ：脅威への対策	○	○
33.	33.上記質問 32 でふれた安全保護策の効果を試すためのプロセスが用意されていますか？	セキュリティ対策：対策の有効性	○	○
34.	34.リスク評価または第三者認証を利用していますか？	セキュリティ対策：リスク評価と第三者評価	○	○
35.	35.個人情報の転送先である処理業者、代理人、請負業者、その他のサービス業者に、以下の手段により、当該情報の紛失、または不正なアクセス、破壊、利用、修正、または開示その他の不正な利用から保護するよう求めていますか？	-	-	-
	a)提供された情報やサービスの機密性に対応した情報セキュリティプログラムを実施する。	セキュリティ対策：転送先へのセキュリティ要求（機密性）	△	○
	b)ネットワークやソフトウェア設計、および情報処理、保存、転送、廃棄などの、情報システムや情報管理	セキュリティ対策：転送先へのセキュリティ要求（情報管理）	△	○
	c)プライバシーの侵害または機密保持違反につながったセキュリティ障害の修正対応のための措置を速やかに講じる。	セキュリティ対策：転送先へのセキュリティ要求（脅威への対策）	△	○

「セキュリティ対策」では、P マークでは事業者が情報の取扱い量や事業の内容等を踏まえ、自ら設定したリスク分析とその対応に基づき、リスクベースによる安全管理措置の対応行う。ただし、CBPR の粒度での要求ではないため“△”とした。ISMS では、同等以上の管理策が要求されているため、全項目が合致した。

7) アクセス及び訂正

「アクセス及び訂正」では、本人がその個人情報にアクセスして、訂正することができることを保証しているか確認した。

図表 26　「アクセス及び訂正」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
36.	36.要請に応じて、要請者に関する個人情報を保有しているか確認していますか？	アクセス及び訂正：開示	○	
37.	37.要請があった場合、保管する個人情報の本人に当該情報へのアクセスを認めていますか？「はい」の場合、以下の質問 37(a)-(e)に回答し、アクセス要請を受け取り対応するための方針と手順について説明してください。「いいえ」の場合、質問 38 に進んでください。	アクセス及び訂正：開示	-	-
	a)あなたはアクセスを要請してきた人の身元を確認する措置を講じていますか？	アクセス及び訂正：開示	○	
	b)あなたは、アクセス要請があった場合、適当な期間内にアクセスを認めていますか？	アクセス及び訂正：開示	○	
	c)情報は基本的に理解しやすい妥当な方法で伝えられていますか（読みやすいフォーマットなど）？	アクセス及び訂正：開示	○	
	d)情報は、個人との通常の対話形式にあった方法で提供されていますか（電子メール、同一言語など）？	アクセス及び訂正：開示の情報の提供方法	○	
	e)アクセスの提供は有料ですか？「はい」の場合、料金設定基準とどのようにして法外ではない額に設定しているか説明してください。	アクセス及び訂正：開示の費用	○	
38.	38.情報の正確さについて個人が異議を唱え、それを修正、完成、改正、または削除させることを認めていますか？以下に関する申請者の方針と手順について説明し、質問 38(a)-(e)に回答してください。	-	-	-
	a)アクセス及び修正方法は明瞭かつ明確に表現されていますか？	アクセス及び訂正：開示手続き	○	
	b)個人情報が不完全または不正確であることを本人が実証した場合、要請のあった修正、追加、または適宜、削除を行っていますか？	アクセス及び訂正：開示の訂正削除	○	
	c)修正または削除の要請があってから適当な期間内にその修正や削除を行っていますか？	アクセス及び訂正：開示 訂正と削除の実施	○	
	d)修正された個人情報の写しを本人に送ったり、データが修正または削除されたという確認を出す等していますか？	アクセス及び訂正：開示 情報の提供方法	○	

質問 No	質問内容	カテゴリ	P マーク	ISMS
	e)アクセスの提供は有料ですか？「はい」の場合、料金設定基準とどのようにして法外ではない額に設定しているか説明してください。	アクセス及び訂正：開示 費用	○	

P マークには、ほぼ同等の要求事項があった。ISMS は CBPR の質問項目の粒度での要求事項は無いため共通項目が無い結果となった。

8) 責任

「責任」では APEC 原則の実施方法を遵守することについて確実に責任を果たしているか、また、移転後にこの原則に従って個人情報を確実に保護するための合理的な措置を用意しているか確認した。

図表 27 「責任」との比較

質問 No	質問内容	カテゴリ	P マーク	ISMS
39.	39.APEC 情報プライバシー原則に従うためにどんな措置を講じていますか？該当するものにすべてチェックし説明してください。	-	-	-
	内部指針または方針（該当する場合、どのように実施しているか説明）	責任：方針	○	○
	契約	責任：契約	○	○
	該当する業界または部門の規程類の順守	責任：業界の法令、必要な規程	○	○
	自主規制による申請者規範または規則の順守	責任：自主規制の実施の有無	○	○
-	その他（具体的に説明してください。）	責任：体制	-	-
40.	40.上記措置に対する組織全体の遵守について責任を持つ担当者がいますか？	責任：苦情および相談	○	○
41.	41.プライバシー関連の苦情の受付、調査、対応に関わる手順を用意していますか？	責任：苦情受付	○	○
42.	42.苦情申立てに適時に対応するための手順を用意していますか？	責任：苦情申立	○	○
43.	43.「はい」の場合、その対応では、苦情に関連した救済措置の説明もしていますか？具体的に説明してください。	責任：救済措置	○	○

質問 No	質問内容	カテゴリ	P マーク	ISMS
44.	44.プライバシー関連の苦情への対応方法をはじめ、プライバシーに関する方針や手順に関して社員を教育する手順を用意していますか？	責任：社員教育	○	○
45.	45.個人情報の開示が求められる場合をはじめ、裁判所またはその他政府の召喚令状、捜査令状や命令に対応するための手順を用意していますか？	責任：執行命令	○	○
46.	（個人情報が移転された場合の責任の維持） 46.代行して個人情報を処理する、処理業者、代理人、請負業者、またはその他のサービス提供者に関して、各個人に対するあなたの義務が必ず果たされるようにするための方法を用意していますか？（該当するものを全てチェック）	責任：移転先の責任の維持	-	-
	内部指針または方針（該当する場合、どのように実施しているか説明）	責任：移転先の責任の維持（方針）	○	○
	契約	責任：移転先の責任の維持（契約）	○	○
	該当する業界または部門の法規の順守	責任：移転先の責任の維持（業界部門の法規順守）	○	○
	自主規制による申請者の規範または規則の順守	責任：移転先の責任の維持（自主規制の実施の有無）	○	○
	その他（具体的に説明してください。）	-	-	-
47.	47.上記の契約では一般に個人情報の処理業者、代理人、請負業者またはその他のサービス業者に以下の行為を義務付けていますか？（該当するものを全てチェック）	責任：委託先の管理	-	-
	プライバシーステイトメントに明記されているAPEC 準拠のプライバシー方針や実務ルールに従う。	責任：委託先の管理（APEC 準拠）	-	-
	プライバシーステイトメントに明記されているプライバシー方針や実務ルールに実質的に類似したプライバシールールを実施する。	責任：委託先の管理（方針やルール）	○	○
	個人情報の取扱方法に関連して提供された指示に従う。	責任：委託先の管理（指示）	○	○
	あなたの同意がない場合には下請に制約を課す。	責任：委託先の管理（制約）	○	○
	各業者の管轄区の APEC アカウンタビリティ・エージェントに CBPR を認証させる。	責任：委託先の管理（CBPR 認		

質問 No	質問内容	カテゴリ	P マーク	ISMS
		証）		
	申請者の顧客の個人情報に関する違反があった場合は申請者に通知する。	責任：委託先の管理（違反の通知）	○	○
	その他（具体的に説明してください。）	-	-	-
48.	48.個人情報の処理業者、代理人、請負業者、その他のサービス業者に、指示または契約や合意に従わせるために監査の提出を義務付けていますか？	責任：委託先の管理（監査）	○	○
49.	49.指示または合意や契約に従わせるために、処理業者、代理人、請負業者、またはその他のサービス業者の定期的な検査やモニタリングを行っていますか？	責任：委託先の管理（モニタリング）	○	○
50.	50.CBPR を確実に遵守させるための事前評価及び方法が、個人情報の処理業者、代理人、請負業者、その他のサービス業者に難しいという場合であっても、個人情報を開示していますか？	責任：委託先の管理（必要な開示）	○	○

「責任」には CBPR と APEC に関する CBPR の特徴的な要求事項があり、この項目が合致しなかったが、その他の項目については P マークと ISMS に、ほぼ同等の要求事項があった。

9) ヒートマップ分析

ヒートマップ分析は類似する項目が複雑に交叉する複数の体系の比較を視覚的に行うための手段である。CBPR、P マーク、ISMS の質問項目の重なりを色分けとして分析してみることで、認証の性質の類似性と違いについて確認することができた。

フレームワークの原則「通知」「取得の制限」「個人情報の利用」「選択」「個人情報の完全性」「セキュリティ対策」「アクセス及び訂正」「責任」の質問項目ごとに、合致した結果を、質問項目の該当する原則ごとにヒートマップ化した。「合致するもの“○”」を「1」、「事業者のリスクベースに依存する項目“△”」を「0.5」の数値の重みを設定して計算式を作成した。結果は以下のとおりであった。

図表 28　CBPR 事前質問項目との比較ヒートマップ

原則	質問数	P マーク	ISMS	傾向
通知	10	100%	10%	方針の定めはどちらも要求されているが、ISMS の要求事項に通知内容の詳細な要求はなかった
取得の制限	5	100%	0%	P マークは合致率が高く、ISMS は合致率が低く、制度の趣旨の違いが反映されている
個人情報の利用	10	100%	0%	P マークは合致率が高く、ISMS は合致率が低く、制度の趣旨の違いが反映されている
選択	7	100%	0%	P マークは合致率が高く、ISMS は合致率が低く、制度の趣旨の違いが反映されている
個人情報の完全性	5	100%	100%	P マーク、ISMS 両方ともに合致率が高く、情報の完全性はどちらも重要な要求事項であることが分かる
セキュリティ対策	15	80%	100%	ISMS では合致率が高く、P マークでは事業者に応じた対応策に該当する項目以外は合致した
アクセス及び訂正	11	100%	0%	P マークは合致率が高く、ISMS は合致率が低く、制度の趣旨の違いが反映されている
責任	23	91.3%	91.3%	P マークも ISMS も高い合致率であった。100%ではないのは CBPR 特有の質問のためである

P マークは 6 つの項目で 100%の合致率であり、合致率の低い項目でも 80%以上の合致率だった。ISMS は個人情報に関する詳細な要求事項がある項目については合致せず、「セキュリティ対策」や「個人情報の完全性」、「責任」が、高い合致率となり、審査項目レベルでは、全体に高い類似性・親和性が確認できた。

②　CBPR 認証基準との比較

CBPR の文書審査において、「事前質問書」で回答された事業者の申請内容がフレームワークに適合しているかを判断すべく、AA は「認証基準」を用いるが、各国の個人情報に関する法制度で執行がかけられるよう、カスタマイズされている。「事前質問書」の補完的位置づけとなっており、JIPDEC では、申請企業が事前質問書の回答がどのように判断されるのかを分かりやすくするため、事前質問書の内容に紐づく評価基準を併記した様式を用意

している。

ここでは、前項で「事前質問書」と類似性・親和性があったと確認出来た項目について、さらに認証基準ベースで比較検証を行い、既に取得している第三者認証制度が申請企業の審査工数に影響し得るのか、その可能性について、CBPR の認証基準と P マーク、ISMS の要求事項に該当する要素について確認した。(P マークを“P”、ISMS を“I”と表記した。)

図表 29　CBPR 認証基準との比較

項番	CBPR 認証基準（要約）	P	I	項番	CBPR 認証基準（要約）	P	I
1.1	プライバシー原則の遵守	○	○	6.4	委託先の監督	○	○
1.2	個人情報の特定	○	○	6.5	定期的な見直し（※リスク）	○	○
1.3	利用目的の特定	○		7.1	個人情報についての事項の公表	○	
1.4	法令、国が定める指針、その他の規範	○	○	7.2	個人情報に関する権利	○	
1.5	リスクの認識、分析、対策	○	○	7.3	権利の手続き	○	
1.6	内部規程	○	○	7.4	利用目的の通知	○	
1.7	緊急事態	○	○	7.5	個人情報の開示	○	
2.1	プライバシーポリシー	○	○	7.6	（開示）訂正、追加、削除	○	
3.1	適正な取得	○	○	7.7	（開示）拒否	○	
3.1a	直接書面による取得	○		8.1	資源、役割、責任、権限	○	○
3.1b	書面以外の取得	○		8.2	苦情・相談の対応	○	○
3.1c	要配慮個人情報	○		8.3	従業者の管理	○	○
4.1	利用に関する措置	○		8.4	従業者の教育	○	○
4.1a	本人へのアクセス	○		8.5	個人情報の提供の手続き	○	
4.2	提供についての措置	○		8.6	委託先管理	○	○
5.1	本人の選択肢	○		9.1	内部監査	○	○
5.2	正確性の確保	○	○	9.2	内部監査計画書	○	○
6.1	安全管理措置	○	○	9.3	是正予防	○	○
6.2	リスクの特定、分析、評価	○	○		P マーク　○の合計	38	－
6.3	リスク対応及び安全管理	○	○		ISMS　○の合計	－	22

比較の結果、審査基準 38 項目中、P マークは 38 の認証基準の全てに該当する項目があ

り、認証基準でも類似性・親和性が高い事が分かった。ISMS は、個人情報の取扱いに関する詳細な要求事項がないため、認証基準では 38 項目中、22 項目となり、6 割程度が合致した。審査基準 38 項目にはそれぞれ、詳細な確認項目があり、CBPR 審査では「越境個人情報を扱う業務の概要」と「越境個人情報の情報流」を審査の対象とし、確認項目の回答をもとに審査を行う。

1) 越境個人情報を扱う業務の概要

越境個人情報を扱う業務は「事前質問書」の越境個人情報を扱う事業の概要で特定する必要がある。ここでは「業務」「種類」「件数（概数）」「取得方法」「外部委託」「越境個人情報の保管状況」について、特定を行う。

2) 業務内容のデータフロー図

特定した越境個人情報について、業務と個人情報の流れが分かるように業務内容を記載する。データフロー図または、情報流が分かるように記載が必要になる。例えば「情報資産台帳（個人情報管理台帳）」にリスト化された個人情報のどれが利用されるのか？「移転先管理台帳（委託先管理台帳）」の、どの移転先に個人情報を提供するのか？複数移転先がある場合はその移転先を全て明らかにする。

以上から、認証基準の合致率が高い項目については、審査準備の工数はそのまま軽減が可能である。ただし、CBPR 審査特有の「越境個人情報を扱う業務の概要」「データフロー図」で要求される情報の特定は、CBPR 審査でもっとも重要な情報であり、P マークも ISMS も CBPR で求められる内容は不要である。したがって、審査項目や認証基準では類似性や親和性が見られたものの、実際の審査プロセスでは、審査のスコープが異なるため、P マークや ISMS の認証企業だからといって、CBPR の審査の一部を軽減できると断定するところに至らず、更に詳細な検討が必要となる。

③ CBPR 安全管理措置との比較

ISMS では、管理策に物理的安全管理措置、技術的安全管理措置が要求されており、詳細な安全管理の要求事項が定められている。このため、CBPR で求める安全管理の内容を網

羅している。しかし、P マークの安全管理措置は、事業者のリスク分析に基づく。CBPR もリスクベースの安全管理基準ではあるが、一般的なリスク分析に見られる申請企業のリスクではなく情報提供者へのリスク分析に基づく対応が必須となる点が大きく異なるため、安全管理項目については、リスク分析の内容と対応の粒度等について精査が必要である。

そこで、CBPR 安全管理措置一覧[27]（CBPR 認証基準 別紙 1.「安全管理措置一覧」）を元に、P マークと ISMS の審査の確認項目について比較を行った結果を以下に示す。（同様の要求事項がある場合は“〇”、無い場合は“空欄”、事業者による選択が可能な要求事項は“△”の表記とした。）

図表 30　CBPR 安全管理措置一覧

管理措置		CBPR	P マーク	ISMS
Ⅰ物理的安全管理措置	1	入退室	〇	〇
	2	盗難防止	〇	〇
	3	機器・装置の物理的な保護	〇	〇
Ⅱ技術的安全管理措置	1	アクセス識別と認証	△	〇
	2	アクセス制御	△	〇
	3	アクセス権限管理	△	〇
	4	アクセスの記録	△	〇
	5	不正ソフトウェア対策	△	〇

④　CBPR 根拠資料との比較

CBPR 申請企業は、「事前質問書」と「追加質問」に回答し、自己点検を行う。その点検結果と根拠資料を提出する。CBPR 審査では、それぞれの質問表に回答された点検内容について、根拠資料を基に文書審査を行う。

P マークと ISMS では申請時の共通様式はなく、認証/審査機関が定める書類を提出する。いずれの審査でも、マネジメントシステムで利用する文書を文書審査または現地審査にて利用することになる。

申請企業が用意する代表的な根拠文書[28]と、P マーク、ISMS の審査において使用する文

[27] CBPR 認証基準　https://www.jipdec.or.jp/project/cbpr/JIPDEC_AOP_CBPR_005.pdf
[28] 「APEC CBPR 認証申請ガイドブック」3.6.2「根拠文書の例」参照

書類との比較を行った。代表的な根拠文書は下記図表に「CBPR の根拠資料の例」として表記した。結果を以下に示す。（同様の資料がある場合は“〇”、事業者により異なる資料は“△”の表記とした。）

図表 31　CBPR 根拠資料の例（ポリシーと規程類）

	CBPR 根拠資料の例（ポリシーと規程類）	P マーク	ISMS
1	プライバシーポリシー（プライバシーステイトメント、個人情報保護方針など）	〇	〇
2	個人情報を特定する手順に関する規程	〇	△
3	法令、国が定める指針その他の規範の特定、参照及び維持に関する規程	〇	〇
4	個人情報に関するリスクの認識、分析及び対策の手順に関する規程	〇	〇
5	事業者の各部門における個人情報を保護するための権限及び責任の規程	〇	〇
6	緊急事態（個人情報を漏えい、滅失またはき損など）への対応に関する規程	〇	〇
7	個人情報の取得、利用及び提供に関する規程	〇	〇
8	個人情報の適正管理に関する規規程（委託先に関する規程、従業者管理に関する規程、安全管理に関する規程など）	〇	〇
9	教育に関する規程	〇	〇

図表 32　CBPR 根拠資料の例（記録類）

	CBPR 根拠資料の例（記録類）	P マーク	ISMS
1	組織図、CBPR 体制	〇	〇
2	システム構成（システム構成図やネットワーク図などシステム仕様の文書）	△	〇
3	セキュリティポリシー（情報セキュリティ基本方針等）	△	〇
4	リスク分析及びリスクに対して講ずべき対策の一覧	〇	〇

	CBPR 根拠資料の例（記録類）	P マーク	ISMS
5	個人情報取得時に本人に通知している文書	○	△
6	個人情報を特定し管理する台帳	○	○
7	委託先及び提供先の一覧	○	○
8	委託先及び提供先を評価選定した記録	○	○
9	委託先及び提供先との契約書	○	○

CBPR の審査で必要となる代表的な根拠文書は、P マークと ISMS でも同様の文書を利用している。P マークは「システム構成図」や「セキュリティポリシー」は必須ではなく、事業者の業務に応じて用意する。ISMS は「個人情報を特定する手順」については、情報資産の特定と同様に扱う事業者もあれば、個人情報として個別に手順を用意するのは事業者判断となる。それぞれの認証制度の趣旨の違いから、事業者の判断に委ねられる文書はあるが、総合的にほぼ同様の文書を根拠資料として利用していることが分かる。

次に、P マークまたは ISMS の申請企業が、CBPR 認証申請のために必要になる作業を確認した結果を以下に示す。

図表 33　CBPR 審査のために新たに必要な作業

	作業	文書例	作業内容
1	既存資料への追加	セキュリティポリシー	ポリシーに越境情報の掲載
2		情報資産台帳	情報資産台帳に外国への移転情報の追加
3		リスク分析表	外国への移転に伴うリスクの洗い出し
4		委託先評価シート	委託先評価シートに外国にある第三者提供について項目の追加
5		委託先リスト	クラウドサービス・システム一覧にサービス元の国名を追加
6		データフロー図	データの越境状況をデータフローに追加
7	新規作成	事前質問書①	CBPR50 の質問書（様式 1-2）
8		事前質問書②	JIPDEC 追加質問書（様式 1-3）
9		その他	CBPR 申請に必要な書類の作成

CBPR 審査では個人情報の外国への移転状況について、既存の台帳や記録類への追加作業が発生する。業務フロー図やシステム構成図などを用意している事業者であれば、既存の文書を活用し、越境状況を追記したデータフロー図を作成できる可能性が高い。他方、情報資産台帳は、個人情報や個人データの概念が含まれないため、CBPR の審査対象となる越境移転が生じる業務で取り扱う個人データの情報と情報の流れを棚卸するのは、かなり労力を要する工程となる。

CBPR 審査で確認する根拠文書においては、P マークも ISMS もほぼ同様であったことから、CBPR でもマネジメントシステムの確認を一部実施していることが確認できたため、既存の根拠文書に、海外への移転状況に関する情報を特定し、記載することで審査用の根拠文書を初めから準備する必要がないものもあることが分かった。

⑤ CBPR と既存認証制度との比較結果

「事前質問書」「認証基準」「安全管理」「根拠資料」を調査した結果を以下にまとめる。

1) 事前質問書との比較

ヒートマップ分析により、P マークは「事前質問書」について、共通点が非常に多く、6 つの原則が 100%の合致率であり、残りの 2 項目も 80%以上合致した。ISMS は、セキュリティ体制が主なスコープとなるため、合致率は 100%と 0%が混在し、認証制度としての違いが明らかになった。

2) 認証基準との比較

CBPR の認証基準は 1.1～9.3 まで 38 項目に分類されている。P マークは 38 項目全ての認証基準に該当する審査項目があり、審査上の重なりが高い事が分かった。ISMS は 38 の基準に対し、22 の項目が合致した。約 6 割の合致率であったが、個人情報保護特有の審査基準について ISMS では詳細に設けられていないためである。審査基準に対して、合致率が高い場合、審査準備に係る工数の軽減は可能である。しかし、CBPR 審査特有の越境個人情報の業務を明らかにし、データ流を明確にする必要がある。これらの特定に係る工数は P マークも ISMS も同様に必要であることを示した。

3) 安全管理措置との比較

CBPR の認証基準にある安全管理措置は、「物理的安全管理」と「技術的安全管理」の 2 つのカテゴリに分かれている。P マークは、「技術的安全管理」については、CBPR の要求事項の粒度での対応を求めてはいない。

ISMS は情報セキュリティマネジメントシステムの管理策として、CBPR の要求事項よりも詳細な管理策を要求しているため、全ての項目が合致した。

4) 根拠資料との比較

P マークと ISMS はそれぞれマネジメントシステムが適切に運用されているかを審査する。マネジメントシステムで使用する文書類は共通性が高く、今回の調査でも CBPR 審査で使用する根拠資料の合致率が高いことを示した。CBPR 審査では越境する個人情報について、業務ごとに明らかにする必要があるが、データフロー図や業務フロー図などがある場合活用できる。すべての根拠資料を初めから作成する必要がないため、申請業務の作業工数を減らせる可能性を示した。

これらの調査結果から、P マークは「事前質問書」の項目、「認証基準」との共通点が多いことが示された。P マークを取得している事業者は、P マーク審査で利用する根拠文書を CBPR 審査で利用できるものがある事が示された。

ISMS は、個人情報の取扱いに関係する「事前質問書」の項目や「認証基準」については共通点が半分程度の結果となった。しかし、「安全管理措置」については ISMS の要求事項が多いため、全て共通していた。また、ISMS の根拠文書の多くが CBPR 審査で利用できる事も示された。

CBPR と P マーク及び ISMS の審査の類似性・親和性が明らかとなり、それぞれの制度で CBPR の申請企業は審査に係る工数の軽減が期待できる事が分かった。他方、CBPR の審査で重要となる越境移転が生じる個人データの棚卸と業務フローの整理、情報流と移転先・委託先の管理においては、詳細かつ正確なデータが求められることには変わりない。

2.1.3　アカウンタビリティ・エージェントへのアンケート調査

現行の APEC CBPR システムの実態や課題を把握し、GCBPR の拡大に向けた改善提案のため、APEC CBPR 認証制度の審査を行っている各国の AA へ、審査プロセスの概要等についてアンケート調査を行った。

(1) 調査概要

① 実施期間

2024 年 11 月 16 日（金）～2025 年 1 月 27 日（月）

② 調査対象

APEC 及び Global CBPR Forum に認定を受けた CBPR 審査機関、図表 2 に示した計 7 つの組織にアンケート調査への協力を依頼した。

③ 調査項目

CBPR 認証制度の認証取得企業増に向けた現状把握に基づく差異、並びに審査の効率性が比較できる項目にフォーカスし、認証審査の概要としては、審査プロセスに関する事項、運用面では、個人情報の取扱いに関連した国内の認証制度と審査プロセスへの関与状況、その他の審査機関としての課題等 4 つのカテゴリで計 20 項目の質問を設定した。

アンケート項目は、以下のとおり。

図表 34　アンケート調査項目

■Assessment Questionnaire Response Form

No	Question	Answer
1	**Details of the assessment process**	
	1) What is your assessment process?	
	2) How are regulators involved in the outcome of the assessment?	
	3) Do you conduct on-site assessment?	Yes/No
	If Yes, please describe the implementation.	
	If No, please state the reason.	
	4) Do you implement group certification?	Yes/No
	If Yes, please describe the assessment process.	
	If No, please state the reason.	
	5) Do you implement PRP certification?	Yes/No
	If Yes, please describe the review process.	
	If No, please state the reason.	

No	Question	Answer
	6) What are you doing to improve the efficiency of the assessment process?	
	7) Are there any issues you feel are a challenge in the assessment process or that could be improved?	
2	**Institutional Design and Operation**	
	1) What are the required application documents?	
	2) Means of Application	
	3) How much are the assessment fees?	
	4) Is there any difference in fees between the initial application and the reapplication?	
	5) What is the basis for calculating the assessment fee?	
	6) How long does it take for the assessment process?	
	7) What is the status of prior consultation?	
	8) Do you collaborate with outside agencies?	Yes/No
	If Yes, please tell us who you are collaborating with and what is the purpose of the collaboration?	
3	**Relation to other certification systems**	
	1) Is there an independent certification system for personal information, etc. in your jurisdiction?	Yes/No
	If Yes, please tell us about the following	
	(1) Name and outline of the certification system	
	2) Is there any difference in the man-hours and costs for an assessment if a company has obtained the above certification systems or not?	Yes/No
	3) Of the certified companies, what percentage have obtained?	
	4) Do you think it is effective to have some kind of certification system in your jurisdiction to implement CBPR certification?	Yes/No
	If Yes, please give reasons.	
4	**Issue**	
	1) What do you consider to be the challenges in the expansion and operation of the CBPR certification system? (1) Consistency as an institution (2) Law awareness (3) Authentication deadline (4) Response to information leaks (5) Timely review of systems (AI, etc.) (6) Strengthen and clarify enforcement cooperation	Applicable items (Multiple selections allowed) [ ] Reasons for selection [ ]

No	Question	Answer
	(7) Formation of an ecosystem for the dissemination of the system	
	(8) Others (free)	8) Others (Please feel free to describe any points you notice) 〔　　〕

④　実施方法

アンケートは、調査対象組織及び Global CBPR Forum、CBPR 認証制度の所管官庁である経済産業省（委託元）、個人情報保護委員会の了解を得て、書面によるアンケート調査を実施した。なお、アンケート調査は、質問項目に基づき実態を把握し、制度の改善提案につなげる事を目的としたものである為、アンケートフォーム送付時に、趣旨説明書を添付し、調査への協力を促した。

(2) アンケート調査結果

各機関とも、個人情報保護の重要性を認識し、そのための取り組みを行っている。特に、CBPR 認証制度の運用に関して、中立性の確保を厳格に行いながら取り組む姿勢が見られた。前節の企業に対して実施したアンケート調査の結果は、以下のとおり。

①　審査プロセス

審査プロセスは、AA 間で大きな違いはなく、文書審査とそのレビューを複数回行い、審査報告書を作成し、申請者に是正を求め、完了後に認証を付与する流れであった。審査を行うのは AA 内外の審査員であるが、シンガポールの IMDA のみ認証の付与は行うが審査自体は審査機関に委託している。PRP 認証は、韓国、チャイニーズ・タイペイ、日本を除く米国、シンガポールが実施しており、グループ認証はチャイニーズ・タイペイと日本を除く AA で実施されている。審査プロセスにおける効率性を高める取り組みは、すべての AA が実施しているという回答だったが、課題をあげた AA はなく、審査プロセスは個々に確立された仕組みのもとで運用されている事が分かった。

②　制度設計・運用

申請資料は、JIPDEC を除くすべての AA がインテーク・クエスチョン（50 の質問への

回答書）と、それを裏付ける根拠資料の構成で、申請方法は、米国、シンガポールは専用のポータルから受付けている。審査プロセスの効率化の一環として導入している AA もあり、審査に係る工数が、申請者、AA 双方で軽減が図れているという事であった。

審査に要する期間はバラツキがあり、短い AA は 1 ケ月～1.5 ケ月、続いて JIPDEC の 3 ケ月、KISA の 4 ケ月（少なくとも）、IMDA の 6 ケ月～1 年と続く。

③　国内の認証制度との関連

ほとんどの AA が、国内で個人情報に関する認証制度があると回答しており、中には認証制度と一部一体化している国や地域もあった。他方、それらの認証制度を取得しているからといって、CBPR の審査工数の削減等、具体的な影響を受けない仕組みにしている AA もあり、審査工数に反映されている AA と運用の違いはあるものの、CBPR の運用においては何らかの個人情報に関する認証制度はあった方が、申請企業と AA 双方にメリットがあると回答が得られた。

④　課題

課題は、複数の事例（選択肢になりうる）を示したところ、最も多く選択された回答は「CBPR 普及のためのエコシステムの形成」であった。選択した理由としては、国境を越えた文字通り Global な関与主体を拡大することで、世界的な信頼性をアピールすることにつながり、より多くの企業間でのつながりを強固にするために CBPR 認証を取得する枠組みが形成されれば、制度の拡大になるという結果であった。

(3) 各 AA が実施する審査の実態に基づく制度の改善提案

審査プロセスに課題はないと回答しつつ、制度自体の課題としては、CBPR 認証制度の認知度が低いこと、執行協力の強化、認証期間が 1 年では短いこと等の指摘があった。改善提案としては次の対応が考えられる。

①　認知度の向上

認知度が低いという課題は、2022 年 4 月に Global CBPR Forum が旗揚げされた時から、半年毎に開催されてきたワークショップでも、各国の規制当局、CBPR に興味を持つ参加企業の他、CBPR に参加している国や地域の政府機関関係者、AA からも課題として取り上げられてきた。一朝一夕に解決することは難しい一方で、イベントや説明会等のように限定された短い期間に実施する手法だけでなく、例えば、大企業が自社のベンダーに認証へ

の参加や取得を要請する､委託先の選定基準の 1 つとして CBPR の取得状況を確認する等、事業活動の仕組みを利用して露出の機会を創出する事で、認知度は高まり、CBPR の制度としての有用性も拡散することが見込まれる。

② 執行協力の強化

CBPR は、政府支援の国際的な認証制度であるという点が大きな特長と言える。アンケート結果からも、政府機関が積極的にこの制度を推進していることの表明を希望する声があった。また、課題で最も選択された回答が「CBPR 普及のためのエコシステムの形成」であったと、(2)アンケート調査結果で触れたが、その意味するところは、国境を越えてより多くの主体が関与し、その結果、より多くの国や地域が GCBPR に参加するためには、政府機関に新たな国や地域が制度に参加するよう取組みを拡大させていくことへの期待が高まっていると言える。いつどのような形で誰に対して行うのか、効果的な実効性の高い取組みを、政府機関と AA が協働で実施する事が肝要である。

③ 審査に要する期間

アンケート調査の回答で、バラツキが顕著だったのが審査に要する期間であった。最も早いケースが 4 週間、最長で 1 年となれば、認証期限が 1 年の制度であるため、初回審査のハードルが上がるだけでなく、運用にも支障が出る事が想定される。今後、認証企業数を拡大していくのであれば、審査に要する時間はある程度の目安で統一されることが望ましい。効率的にダウンサイジングした審査プロセスの検討も必要になるであろう。最も短い期間内で審査が完了できるモデルや、数ケ月を要しているケース等、いくつかのユースケースに基づく審査プロセスのモデルケースを策定し、検証することも有効である。

2.1.4 マッピングのまとめと制度改善提案

この 2.1 節においては、CBPR との相対的な関係性を分析するために、GDPR との比較、プライバシーマーク制度、ISMS 適合性評価制度等の他の制度との比較、CBPR の AA へのアンケート調査を通じて、要求項目と運用実態についての比較検討調査を行ってきた。それぞれの調査項目より分析の結果明らかになった点を以下にまとめる。

- GDPR と CBPR の比較からは、内容面運用面双方で、根拠が異なる点が明確となった一方、BCR 認証制度との比較においては要求項目において同等とされるものも多く、

両者に特徴があることがわかった。運用面においては対象となる地域が異なるため、必要な場合は双方取得する必要がある。ただし、そうした事実への理解を第一に促進することが必要である。

- 国内での現存する認証制度との致命的に障害となる要素はなく、むしろそれぞれの認証制度の特徴を示す差異があるだけである。つまり、より効率的な認証制度運用については内容面からの障害は少なく、適切な運用体制が組めれば加入社数増加を実現することが可能である。
- 海外の AA での異なる運用実態の経験から学ぶ点も多い。政府内に強力なリーダーシップによる運営推進体制があり、短期間で多くの参加企業を得ている地域もある。我が国においても政府、認証機関を中心に推進体制を充実させ、各該当部署に適切な権限やリソースを割り当てることが必要と思われる。
- 取得企業の立場からは、認証取得に必要なコストや人的リソースの削減は大きな要望となる、制度の単純化や複数認証制度の間のポジショニングを明確に示し、それぞれの制度の対象、特徴と効力について、事業者の理解を深めることが必要である。そのうえで共通する要求項目の扱いを適切に効率化して、制度として充実させる必要がある。

2.2 普及啓発活動

CBPR の普及に向けて対象となる事業者に対して内容を明確に伝えるとともに、対象となる側が認める課題を分析することで、今後の活動に結び付けることができる。本調査においては、第 2 章 1 節で概要として「②ヒアリング : 普及啓発活動」において記した通り、企業計 11 社に対し 13 項目（計 22 の設問）について実施したオンラインヒアリング結果を分析した。

その結果、認知度、越境移転ツールのニーズとして法や規則と第三者認証制度を比較した場合のメリット・デメリット、認証取得へのインセンティブ、拡大に向けた意見等の観点で課題をまとめ、申請企業の立場での課題意識をもとにヒアリング調査結果に対する提案項目をまとめた。

2.2.1　ヒアリング調査概要

(1) 実施期間

2024 年 10 月 8 日（火）～2024 年 11 月 26 日（火）

(2) 調査対象

様々なサービスを通じて個人データの越境移転が起こり得る事業者、グローバルに事業を展開している事業者、ユーザー情報を多数保有する事業者等、23 企業・団体へ打診し、図表 3 で示した 11 企業を調査対象としてヒアリングを行った。

(3) 調査項目

CBPR の普及及び認証企業増に向けた現状把握並びに課題につながる項目にフォーカスし、制度の認知度、越境移転ツールの導入状況及び今後の導入見込み（CBPR 以外も含む）、CBPR の拡大に必要なこと等、13 項目の質問を設定した。ヒアリング項目は、以下のとおり。

図表 35　ヒアリング調査項目

No.	項目
1	個人データの越境移転を伴う業務において、外国にある第三者へ提供されていると思いますが、業務委託又は現地法人と従業員情報のやりとりをする程度のどちらに該当しますか？
2	上記の場合、現在の対応状況についてお聞かせください。 ①個人データの越境移転を伴う業務のうち、移転の根拠となる同意、相当措置は、それぞれどれ位の割合ですか？ ②データの移転先（国や地域）はどれ位ありますか？また、移転先との契約等において困っていることがありましたら教えてください。 （例：移転先の法制度の理解とそれに付随するコスト、契約書の作成に要する労力等） ③日本の個人情報保護法上では、越境移転にあたらないクラウド利用、SaaS サービスを使った業務委託等概要を教えてください。
3	APEC CBPRs についてお聞きになったことはありますか？ （理解度：聞いたことがある／調べたことがある／取得を検討している等）

No.	項目
4	Global CBPR についてお聞きになったことはありますか？ （理解度：聞いたことがある／調べたことがある／取得を検討している等）
5	Global CBPR 認証等、個人情報の新しい越境移転ツール（CBPR 等の第三者認証制度）は、事業者にとって有効（必要）だと思いますか？
6	GDPR 等の規則や法（例：十分性認定/BCR/SCC）等と比較した場合、越境移転ツール（例：APEC CBPR/Global CBPR 認証）等の第三者認証制度のメリット及びデメリットは何ですか？
7	CBPR 以外の認証を取得していますか？ ➢ している　：①認証制度名、②認証取得の理由、③認証制度の効果、④認証申請手続きで改善して欲しいことは何ですか？ ➢ していない：①理由、②今後取得の予定はありますか（ない：ない場合、もし取得を検討する場合、何が必要ですか。）、③認証取得の効果として期待することは何ですか？
8	日本では導入されていない CBPR 認証のグループ認証についてお尋ねします。 ※日本は個社単位での認証のみ。米国、シンガポールは親会社が認証を取得すれば、子会社も自動的に認証される事をグループ認証という。 ➢ （日本子会社）国内に子会社を持っている場合に、子会社もまとめて認証される運用（親会社と同一ポリシーが徹底されていることが前提）は、CBPR 認証を取得する動機になりますか？ ➢ （海外子会社）海外子会社を持っている場合に、子会社もまとめて認証される運用（親会社と同一ポリシーが徹底されていることが前提）は、CBPR 認証を取得する動機になりますか？
9	日本では導入されていない CBPR 認証の PRP 認証についてお尋ねします。 PRP 認証が開始された場合に CBPR 認証を取得する動機になりますか？ ※PRP 認証とは、プロセッサー（ベンダー等、顧客データをクライアントから預かって処理を行う事業者）向けの認証。日本は、コントローラーやプロセッサーの区別が法の定義上なく、「個人情報取扱事業者」のみのため未実施。

No.	項目
10	Global CBPR 認証等、個人情報の新しい越境移転ツールが、社会の信頼を獲得し、より多くの企業が取得したいと思えるようになるためには、何が必要ですか（コンプライアンス又はアカウンタビリティを示すツールとして有用である、他）？
11	CBPR 認証の認知度を高めるために、どのような方法が効果的だと思いますか？
12	個人データの移転を伴う、今後の海外との事業展開についてお伺いします。 （※特に直近のご予定がない場合も興味のある地域やセクターがありましたら教えてください。） ①対象となる国・地域は何処になりますか？ ②どのような事業または事業分野ですか？ ③ご意見等ありましたら教えてください。
13	外国市場における個人データ移転について教えてください。 ①データの自由度がどのように高まると事業がスムーズに進みますか？ ②データ移転の弊害として感じていることはありますか？ ③ご意見等ありましたら教えてください。

(4) 実施方法

ヒアリングは、調査対象者の同意を得て、CBPR の所管官庁である経済産業省、個人情報保護委員会同席の元、オンラインにて質疑応答を含むヒアリング調査を実施した。なお、ヒアリングは実態調査ではなく、質問項目に基づき事業者から忌憚のない意見をうかがうものである為、ヒアリング開始時に調査機関の経済産業省より主旨説明を行った。

2.2.2 ヒアリング調査結果

CBPR は、異なる法域間で情報の取り扱いが発生する場合、煩雑となりがちな事業者の課題を改善する選択肢の 1 つとして、期待が高まっている。現行の越境移転制度（APEC CBPR）を導入している CBPR 認証企業 3 社を含み、業務として個人データを越境移転している企業計 11 社に対し 13 項目（計 22 の設問）のヒアリングをオンラインにより実施し、越境移転ツールの有効性やメリット・デメリット、認証取得企業拡大へのインセンティブ等の視点から課題の整理を行い、今後に向けた有益な意見と共にとりまとめた結果を

以下に示す。

(1) 課題

① 第三者認証制度としての認知度に関する課題

ヒアリングに応じた企業・組織の多くは、AA アンケートで得られた回答と同様に、CBPR の認知度の低さを課題に挙げており、認証を取得するインセンティブとしての課題にもつながっている。他方、認知度の向上に向けた積極的な提案等も出され、政府機関の具体的な打ち手に対し、重要な示唆を与えられたものと考える。

なお、各項目欄の A 社等の表記は、別の項目欄に記載された当該 A 社と同一の事業者・組織ではない。アルファベットを無作為に割り当てている。

図表 36 第三者認証制度としての認知度に関する課題（抜粋）

区分	主な意見
認知度の低さ	■ 名前を知っている程度（A 社） ■ APEC と Global CBPR の違いが分からない社員もいる（B 社） ■ Web サイトで公表される情報の範囲で知っている程度（C 社） ■ 社内で知っている人と知らない人の差が激しい。会社全体での認知度が浸透しているということではない。（D 社） ■ APEC、Global 共に制度の概要程度は理解しているが、具体的な認証基準や審査プロセス等、制度の運用や審査の内容は把握できていない。（F 社） ■ 法務部のスタッフは良く知っており、特にアジアのオフィスでは APEC CBPR の話が話題にのぼる。ただし、社内のグローバルスタンダードは EU や UK の BCR や SCC、十分制認定で、コンプライアンス関連のスタッフは知っているが、営業やマーケティング部のスタッフは知らない職員も少なくない（E 社） （米国での認知度が高い） ■ 米国での認知度は非常に高く、毎年詳細な確認とレビューを審査によってカバーできる点が理解されている。日本の個人情報保護法（外国にある第三者への提供等を含む）を説明するのは大変だが、Apple や Mastercard が CBPR 認証を取得している事を説明するとスムーズである（C 社）

区分	主な意見
企業間取引における進まない活用	■ 移転先が認証を取得してくれていると、取引の判断がしやすいが、認証されるまでにどれくらいの時間やコストがかかるのか、どのような内容で審査されるのかが分かりづらい（A 社） ■ データの移転メカニズムがどの程度信頼出来るのかを判断するのは難しい。米国のプライバシーシールドがシュレムス判決で無効とされ、多くの米国企業は短期間の間に膨大な SCC を作成しなければならない事態に陥った（B 社、C 社）

② 越境移転ツールとしての有効性に関する課題（データの越境移転に関する課題より）

有効性があると回答した企業は多くみられ、「特に GCBPR になることで対象となる国や地域も拡大し、DFFT が更に促進され、経済的効果の点でも重要である。CBPR は相互運用性と柔軟性がある点が優れている」という意見や、「年次で運用を管理できているため、情報の取り扱いにおいて安心できるという評価を受けやすい」という意見があった。また、「利用が増加している SaaS サービス提供事業者や新規の取引先に対し、相当措置への基準適合体制等が一定の基準を満たしていることの確認が煩雑であるため、CBPR が判断材料の 1 つになれば有効な手段である」という意見は複数にのぼり、相当措置は CBPR の法的なメリットの事例として CBPR のワークショップ等で取り上げられる事もあるが、企業にとっては相当措置で移転した後の対応にやや負担を感じている実態がある事もが分かった。

次の GDPR 等の法制度と CBPR 等の第三者認証の比較による課題以降は、具体的な企業の声を抜粋し、課題をとりまとめた。

③ GDPR 等の法制度と CBPR 等の第三者認証の比較による課題

法や規則と第三者認証制度は、比べる対象としては類似性や目的が異なるため適切ではないが、令和 5 年に続き、令和 6 年の 10 月に開催された G7 データ保護・プライバシー機関が発表した「G7 DPA 行動計画（仮訳）」[29]には、まだ運用開始前ではあるが GCBPR と GDPR の相互運用性の検討（移転ツールの選択肢を増やす）を目的とした分析を行う事が明文化されており、個人データを越境移転する手段としてはベンチマークとなっている GDPR との比較は、現在の各国の政府機関の方向性とも合致している。

[29] 個人情報保護委員会 HP　https://www.ppc.go.jp/files/pdf/241011G7DPAs'-Action-Plan-jp.pdf

図表 37　法制度と第三者認証の比較による課題（取得・維持コスト他）（抜粋）

区分	主な意見
＜メリット＞ アカウンタビリティツール コンプライアンスツール	■ 法第 28 条や個人データの定義（個人関連情報等）やその概念的なものとして海外にないものの説明に苦慮しており、GDPR に準拠した取扱いになっていないが、説明時は GDPR に沿って説明している（法のアカウンタビリティツールとしての汎用性）（A 社）。 ■ データ移転について相談したいと顧客から要望があった際、国際企業の場合、CBPR/PRP 認証を取得していると伝えるだけで、取組みの詳細を割愛できるため、時間や労力が軽減できる。また、自社のコンプライアンスとしてもメリットがある（認証制度のコンプライアンス＆アカウンタビリティツールとしての機能）（B 社、C 社） ■ CBPR がシンガポールで効果が高いように、日本では P マークがある。法務部ではなく日本のマーケティング部門が契約のスムーズさから推奨してきた。国や地域により信頼される認証制度を取得することにビジネス上のメリットがある（D 社） ■ グローバルに統一的な認証制度であること。それぞれの国の制度を詳細に確認しながら対応しなくてもよい点がメリットになる（E 社）
＜デメリット＞ 契約時の課題	■ 近年、「データシェアリングアグリーメント」の締結を求められる。契約上の委託先にはあたらないが、委託先として扱うような契約を要求されることもあり、コントローラーとプロセッサーの契約に署名を求められることもある。GDPR のように契約上の免除や、セキュリティの遵守事項の確認において優位性を持てれば良いが CBPR はそれらがない（A 社）。 ■ グローバルにビジネスを展開する日本企業が、シンガポールや韓国と取引を考える際、CBPR や PRP は意味がある。他方、役割と責任が異なるため、特にシンガポールではプロセッサーとしての事業を行う企業が CBPR を持っていても全く意味をなさない（B 社） ■ 日本の法令や社内の基準に応じた個別の契約を求めても応じてくれず、確認したい事も回答が得られない。相当措置の監査も十分な内容になっていないのではと感じる（C 社）
コスト・工数の課題	■ マーケティングの需要としては BCR が目標となっている。ただし、お金と時間がかかるので大企業しか対象にならない。中小企業は SCC を使っているが EU 中心で、それ以外は法域により少しずつ異なり、法務コストがかさむ（A 社） ■ オンライン上で申請や回答ができると良いが、それが審査コストに影響するのは避けたい（B 社）。 ■ 資産台帳が色々なところで管理されるのは良くない。対象業務やデータの見方や扱いが変わると、小さな揺らぎも大きな話になりかねないので、懸念材料と考えている。その際、GDPR は個人情報保護法と（C 社） ■ 申請資料を簡素化して欲しい。また、越境審査対象となる業務の資産（データ）の洗い出し用のフォーマットを用意して欲しい。APEC CBPR の日本語訳が分かりにくいので、日本語ネイティブでも理解

区分	主な意見
	しやすい表現にして欲しい（D 社） ■ アジアの海外拠点からデータを越境移転する場合、政府機関への届け出が必要な国があり、一旦提出すると追加書類を求められ煩雑である。また、EU は同意のガイドラインが発行されて以降、JIS や日本の個人情報保護法と「同意」の定義に差分が生じ、例えば問い合わせのためのメールアドレスの取得時に同意しか選択の余地がない場合は無効とされてしまうケースがあり困っている。CBPR は法域を超えたやりとりが出来る点がメリットだが、実際は韓国も 2024 年に GDPR 寄りの同意にルールが変更されたため、日本と韓国で CBPR を取得した企業同士の場合、結局各国法に基づいた運用になってしまうのが悩みである。 もし、CBPR で同意がダメという事になれば、P マークでは同意を求められ、CBPR では真逆になる。認証基準が異なる制度はやめて欲しい。JIS や個人情報保護法は海外に近づいてきているが、認証基準に矛盾を生じさせず、P マークの上乗せで認証基準があることが望ましい（E 社、F 社）
制度の信頼性	■ EU で米国のプライバシーシールドが無効判決を受けた際、多くの米国企業が SCC の作成に追われた。データの移転メカニズムがどの程度信頼できるのか判断することは難しい（A 社）

④ 認証取得のインセンティブに関する課題（グループ認証、PRP 認証）

親会社と同一のポリシーや情報の取り扱いにおける慣行が統一されている場合（一部異なる場合も含まれる）、直接認証されるのは親会社のみだが、認証の範囲を子会社に広げても良いとされるもので（以下、「グループ認証」という。）、このグループ認証は CBPR のみならず、別の第三者認証の間でも個社単位ではない認証制度へのシフトが起こる等、新たな動きを見せている。

ただし、現在日本では導入されていないため、企業のニーズを把握するため、ヒアリング項目としたところ、グループ認証の導入を肯定的に捉える企業が多かった。個社単位の認証では、少人数で運営している国内外のグループ企業が認証を取得・維持するための人員やコストが負担になる可能性があるからである。グループ認証が可能になれば、個社単位では CBPR の取得が難しいケースでも、親会社のコントロールの元、認証が可能になる。他方、海外のグループ会社に対しては、グループ企業になった経緯や法人を設立した国や地域によって、企業風土や生活習慣・文化の違い等から、日本（親会社）と同じポリシーに基づく運用の困難さが課題として挙げられた。

その他、日本が実施出来ていないもう一つの制度として処理者向けの APEC Privacy

Recognition for Processors（PRP）がある。CBPR を取得していれば問題ないように見えるかもしれないが、ビジネスを行う国や地域によっては CBPR と PRP では求められる責任と役割が大きく異なるため、日本のように CBPR だけの運用では認証取得のメリットが十分享受できるわけではない。強く推進して欲しいという要望と、様子見の企業とに意見が分かれる結果となった。

図表 38　認証取得のインセンティブに関する課題（抜粋）

区分	主な意見
複数の認証取得	■ 競合他社との差別化のため複数の認証を取得している（A 社） ■ セキュリティファーストやガバナンスを効かせるためには、普段の用務に組込むことが大切。認証等を特別なものとして扱わず、サービスや業務の設計段階から予算にも組み込んで設定しておく必要がある（B 社） ■ 社会で広く要求されている場合、1,000 万円程度であれば要求が通りやすい。それ以上は、リターンの有無が議論になる。認証制度はすぐにリターンは出にくいが、申請時に取引の可能性がこれまでより広がり、優先的に取引をもらえる場が広がる場面を描けているかがポイントになる（C 社）
グループ認証の導入	＜メリットがある＞ ■ 非常にメリットがある。Apple 社の認証表記に日本の関連会社も入っており、信頼の証となる（A 社） ■ 運用面で工数がかかるため、小規模の子会社は個社単位での管理や体制を取ることが難しい。親会社の管理下で、規模を問わず認証されるのが良い（B 社） ■ 国内の子会社よりも海外の方がニーズは高い。各国の法制度によらずデータの越境移転が担保できるのは大きなメリットになる（C 社） ■ グループでの認証は心理的なハードルも下がりやすい（D 社） ＜懸念事項＞ ■ 買収した企業のビジネスが全く異なる分野の場合、親会社と同じポリシーの適用が難しい場合がある。また、自社も買収した会社も CBPR を取得していても、米国のように AA が複数ある場合異なる AA での認証は運用が異なる場合がある（A 社）
PRP 認証の実施	＜メリットがある＞ ■ 日本では PRP を是非導入した方が良い（特に SaaS プロバイダーにメリットがある：複数回答あり）。日本の個人情報保護法はコントローラーとプロセッサーの違いは曖昧だが、海外では全く責任が違う。自社もそれぞれ専用のポリシーを用意している（A 社） ■ ISMS で要求事項を拡張し、PII の安全管理措置も含めている。プロセッサーの安全管理措置は ISMS で対応している理解である。得意先が

区分	主な意見
	PRP 認証を希望すれば絶対的な動機になる（E 社） ■ 原則親会社と関連子会社は同じポリシーを利用する事にしているが、いくつかの子会社には CBPR を取得させておけばよいという声もある。（その場合、1 つのデータに 2 つのコントローラーが生じる。それらに似たような少し異なる運用を行うのは非効率なので、取り扱う部門を集約させた）（D 社） ■ 子会社もまとめて認証されるのは良いが、企業数が増えるほど認証審査が負担になるため、個社ごとで良いのではという味方もある。審査の重さと子会社を含めることのメリットをバランスさせる必要がある。資本関係等、ルール以外のすぐに変更が難しい部分が違う場合、調整が必要になるのではないか（E 社） ＜懸念事項＞ ■ いくつかの子会社とは原則ポリシーが同じだが、共通性が見いだせない場合は、個社単位の CBPR を検討中。クラウドサービスは PRP が良いのではないかと考えているが、国ごとに扱いが違うのは困る（D 社）

(2) 意見

CBPR の認知度向上や認証企業数の拡大に向けて寄せられた意見を、次のとおりとりまとめた。

図表 39　CBPR の認証企業増に向けた意見（抜粋）

区分	主な意見
認証企業が拡大していくために必要なこと	■ 必要に迫られないと取得は難しいので、契約に絡むレベルまで。GAFA のような企業が委託先の選定や自社サイトに認証取得をアピールすることでブランディングを行うと、効果がある（A 社）（D 社） ■ GDPR に入っている要素を反映できると良い（例：センシティブデータの取扱い、マーケティングのオプトアウト等）（B 社） ■ 移転先の企業が認証を取得していると、法律の要件を確認する手間が軽減されるため、当該事業者のみならず産業界にとっても大きなメリットがある（C 社） ■ GDPR のように制裁金の割引制度等、直接的なベネフィットが見えるようにする（D 社） ■ SNS や YouTube でのコマーシャルを打つ。年代問わず年齢が高い上司も見ている。また、「NewsPicks」というアプリを会社で法人契約しているが、ニュースのスクラップやテーマ性のある対談などもあるため、動画としてコンテンツを提供する等の広告戦略を有効である（E 社） ■ ISMS に手続きの煩雑さはないが、事業部単位やサービスで取得したため、1 つにまとめられると有効である。また、3 年に 1 回の審査は、数日間複数名の審査員が調査を行うため、日程調整や対応がやや負担。

区分	主な意見
	ISMAP は政府機関の制度であるが、OneGate だけでもかなりの費用がかかるので、公共向けなので検討して欲しい。また、監査法人が入らなければならないため、適正な競争と言えるのか疑問（F 社） ■ 米国では CBPR を取得している大企業が複数ある。現在 OneGate をフラッグシップに据えようと考えているが、CBPR が有名になると自社が提供するバリューもあがる（G 社）
制度の認知度を向上させるために必要なこと	■ 海外の企業は CBPR への関心が高いため、JIPDEC から英語での発信を充実させる（A 社） ■ AI のガバナンスプロセスが追加されること（中小企業は他社の LLM を利用することになるため、取引先への信頼の証になる）（B 社） ■ 日本の P マークは多くの企業が参加しているため、オプションで容易に取得できる仕組みになると DFFT や海外とのビジネスを推進したい企業に有効である（複数回答あり） ■ プライバシーガバナンスガイドブックのように、個人データの越境移転に対応するベストプラクティス等を紹介すると良い（C 社） ■ 「(データビジネスを) 海外展開したいあなた。個人情報の取扱いはどうしますか？」というメッセージをキャッチコピーとして問いかけてはどうか。DFFT と個人情報の越境移転を扱う業務がリンクしてきた。「ルールを守らなくてはいけない」という視点ではなく、「何かあったら守ってくれる制度」というふうに発想を転換すると受け入れやすい（D 社）

(3) その他

今後、事業を展開しようと考えている国や地域及び事業内容についてとりまとめた結果を以下に示す。アジア圏等はヒアリング企業に共通した国や地域が多数あがった。また、事業内容についても、企業のニーズを踏まえ、普及啓発活動を行う国や地域及び事業分野等の参考になる事業の名前があがった。なお、外国市場でのデータの越境移転で障壁となっている事や、自由度が高まったら良いと思う越境移転の現状については、多様な意見が出された。

図表 40　今後事業展開を予定する地域及び越境移転の現状（抜粋）

区分	主な意見
国や地域	■ インド、インドネシア、オーストラリア、韓国、シンガポール、タイ、中国、チャイニーズ・タイペイ、フィリピン、ベトナム、香港、マレーシア ■ アメリカ、イタリア、オランダ、ドイツ、デンマーク、フランス ■ EU、UK

区分	主な意見
事業分野	■ 事務業務のアウトソーシング （サービスインテグレーション及びシステムインテグレーション） ■ コミュニケーションアプリを含む、総合インターネットサービス ■ IT セキュリティ分野でのネットワーク認証を中心としたクラウドサービス、CtoC マーケットプレイス事業 ■ 従業員情報の共同利用
データの自由度に対する企業のニーズ	■ 越境移転の認証制度が CBPR 認証に限定されず、例えば、既に認証を取得している事業者が多い ISMS や、P マーク取得等に国際標準的な個人データの取り扱いルールが盛り込まれたうえで越境移転の認証制度として認められる様になれば、複数の認証を取得し運用する手間が削減され、また企業間でのデータのやりとりも行いやすくなり、事業がよりスムーズになる。 ■ プライバシーマーク審査（JIPDEC 審査基準ではなく、審査員の審査基準）と各国法の整合がとれるとスムーズに進む。 ■ 各国における越境移転ルールが統一されていないことによる企業側の負担が大きいため、各国間のルールをできる限り統一して欲しい。また、各国におけるデータのライフサイクルにおける規制が同一化、または一方の国の規制に沿っていればもう一方の国でも同等のことが可能になるような自由度が高まると、事業はよりスムーズになる。 例：「同意」の定義 ■ データ移転時のセキュリティの担保と各国の法制に則ったデータ処理の明確化 ■ Global CBPR 認証について、グループ認証、PRP 認証が可能であるのが望ましい。競合他社に後れを取る可能性がある。

2.2.3 普及啓発に向けた制度改善提案

ここまでのヒアリング内容を総括すると、CBPR 認証制度の普及に必要ないくつかの主要な改善項目があげられる。代表的なものとして、認知度向上、越境移転ツールとしての有効性向上が多く取り上げられた。また、取得・維持コスト削減、認証取得インセンティブ強化が不可欠であり、政府・企業・認証機関が連携し、国際的な議論も進めながら、事業者のニーズに即した制度設計と運用が求められる。

以下にまとめとして 4 項目についての詳細と求められる措置について整理する。

(1) 第三者認証制度としての認知度に関する課題

CBPR 認証は、2022 年 4 月に Global CBPR Forum が APEC 域内を超えたグローバルなデータの移転を視野に旗揚げし、これまで 6 ケ月に 1 度の間隔でワークショップを開催してきた。その際、規制当局、政府機関、各国の AA、CBPR 認証制度に興味のある企業等、様々なステークホルダーから認知度の向上は継続的な課題として語られることが多かった。新

しい制度であり、制度の運用・維持には、人員や認証取得コストがかかるため、費用対効果を検討する上で、認証制度としての有効性を示していく必要があるこれまで以上に、認知度を高めるための周知が重要であり、具体的には以下が考えられる。

- ✓ 政府支援の制度であることの周知を行い、新しい制度ではあるが枠組み自体の安全性や継続性を伝える
- ✓ 特に日本で CBPR 認証制度の普及展開セミナーを開催する場合、グローバルに事業を展開している世界的な企業やビックテック企業等をパネリストとして招き、国際動向も含め、第三者認証の有効性やユースケース等に接する機会を創出する
  ※著名な企業の Web サイト等で周知してもらい、一般の方の目に CBPR が触れる機会を増やす
- ✓ 認知度の向上だけでなく、認証の取得に一歩前進できるよう、この認証を取得したらどのようなメリットが事業者にあるのかを、具体的な事例と共に紹介する機会を作る
- ✓ ビジネスの仕組みの中に組み込まれるような仕掛けを政府機関主導で検討する
- ✓ 対面のセミナーだけでなく、SNS や Youtube 等、時代に合ったツールを使った周知活動を行う。
  例） NewsPicks 等、ビジネスマンが視聴者のオンラインサービスで露出を増やす

(2) 越境移転ツールとしての有効性に関する課題

企業において、各法域で異なる越境移転規制への対応が求められ、コスト・工数がかかっている。それを低減するために、グローバルに共通の越境移転ツールとして CBPR 認証への期待が寄せられている一方で、カバーされる地域が限定的な現状では、越境移転ツールとしての有効性が明確でないとの課題が示された。

新たな国や地域からの参加を可能とするグローバル CBPR フォーラムに係る取組を推進し、各国法において CBPR 認証が越境移転ツールに位置づけられるような働きかけを進める等、越境移転ツールとしての有効性を高めていくことが重要である。

(3) 法制度と第三者認証の比較による課題（取得・維持コスト及び工数等）

認証制度に関連するコストについては、取得・維持双方においてコストが負担になり、特に中小企業においては、認証取得費用の軽減策の導入も要望としてあがっていた為、重

要な検討要素となる。直接的な補助制度の検討と共に、複数の認証制度を取得することになる企業においては、既に取得している既存の認証制度と同一の評価項目がある場合、審査工数の削減につながる等の要件が設定されることも実利に叶う施策となろう。現在 CBPR の審査を行っている国や地域では独自の認証制度が存在する場合が少なくない。国際標準との適合性評価による認証制度等との比較も含め、CBPR 認証制度を導入している国と地域全てを対象とした施策として有効であると考えられる。

また、認証期限が１年という点も、維持コスト及び工数の両方に影響がある。他方、１年毎の見直しによるコンプライアンスの担保がメリットであるとする事業者もあり、引続き、企業や認証審査機関へのヒアリングを行い、実態を把握した上で検討していくことが必要であろう。

(4) 認証取得のインセンティブに関する課題（グループ認証、PRP 認証）

認証取得のインセンティブに関する課題として、グループ認証と PRP 認証を取り上げた。CBPR の制度運用が分かれる要素であり、日本では何れも導入されていない。ヒアリングの結果は、概ね導入に賛同する声が多くメリットがあると回答した企業が多かった。他方で、日本の親会社が海外の子会社に対してガバナンスを徹底することができるかどうかが鍵となり、言葉の問題、海外の文化や風土の違い、組織自体が少人数で運用されている企業も少なくないという現状も考慮する必要がある。なお、日本の親会社だけでなく海外の子会社における情報の取扱いにおいても第三者の評価を受け、適切な運用を徹底したいとの声もあった。

また、PRP 認証が日本ではまだ導入されていないことは前述したが、プロセッサーとして事業展開する企業も日本では多い為、PRP 認証制度の導入を望む声も多く、ヒアリングでも同様の意見があった。

インセンティブに直結する改善策は急務と考えられるが、法制度上の検討課題も関連する。日本企業が他の法域に所在する企業に比べて、認証取得やプロセス、ひいては、その認証が活用されるマーケットでの競争において不利にならないよう考慮しつつ、引続き申請企業のインセンティブがどこにあるのか、ヒアリング等を継続的に行い、企業の声に基づく制度設計を進めることが肝要である。

2.3　CBPR の普及等に向けた活動のまとめ

第 2 章においては、CBPR の認証企業数の増加に向けて必要な施策を検討するための基礎となる調査と分析を行ってきた。制度比較分析として、EU の GDPR において定められている越境移転ツールから特に BCR を比較対象としてとりあげ、国内ですでに運用されているプライバシーマーク制度と ISMS 適合性評価制度との比較マッピング分析を実施した。一方で各ステークホルダーの立場からの意見を集約すること、現行制度の審査プロセスや制度運営の一貫性を整備する観点から、CBPR の各 AA に新たに調査を実施した。同時に CBPR 認証企業を含めたヒアリングをもとにその課題意識や要望についてまとめた。その結果、改善の方向性としてまとめられた点について以下の表に再掲する。

図表 41　CBPR の普及等に向けた活動のまとめ

項目	内容
2.1 マッピング調査の提案事項からの提案事項	
(1)GDPR と CBPR の比較を明示	内容面・運用面双方で根拠が異なる点、同等とされるものを中心に両者に特徴を踏まえながら、事実への理解を第一に促進することが必要である。
(2)国内の現存する認証制度との関係性を明示	既に何らかの認証を取得している企業の申請手続きや審査上の負担を軽減できないかという点では、致命的に障害となる要素はなく、類似性・親和性が見られた。より効率的な認証制度の運用については、他の認証制度を CBPR に関連付けて審査を行っている AA をモデルケースとして適切な運用体制が組めれば認証企業数の増加を実現することが期待される。
(3)推進体制の明確化とリーダーシップの充実	海外 AA の運用実態を見ると、政府内に強力なリーダーシップによる運営推進体制があり、短期間で多くの参加企業を得ている地域もある。我が国においても政府、認証機関を中心に推進体制を充実させ、各該当部署に適切な権限やリソースを割り当てることが必要と思われる。
(4)申請企業の要望	認証取得に必要なコストや人的リソースの削減は大きな要望とな

への対応	る。制度の単純化や複数認証制度の間のポジショニングを明確に示し、それぞれの制度の対象、特徴と効力について、事業者の理解を深めることが必要である。そのうえで共通する要求項目の扱いを適切に効率化して、制度として充実させる必要がある。
2.2 普及啓発活動からの提案事項	
(1)第三者認証制度としての認知度に関する課題	CBPR 認証は、企業間でも、消費者においても認知度が低い点が課題として挙げられているので、必要な訴求ポイントを整理しつつ、施策に結び付ける必要がある。
(2)越境移転ツールとしての有効性に関する課題	企業では各法域で異なる越境移転規制への対応が求められ、コスト・工数がかかっていることが課題であり、グローバルに共通の越境移転ツールとして CBPR への期待が寄せられている。一方でより広い新たな国や地域からの参加を可能とするグローバル CBPR フォーラムに係る取組を推進し、各国法において CBPR が越境移転ツールに位置づけられるような働きかけを進めるなどの有効性を高めていくことが重要である。
(3)法制度と第三者認証の比較による課題（取得・維持コスト及び工数等）	認証の取得・維持双方においてコストが負担になり、特に中小企業においては、認証取得費用の軽減策の導入も要望としてあがっている。複数の認証制度を取得することになる企業においては、既に取得している既存の認証制度と同一の評価項目がある場合、審査工数の削減につながる等の要件が設定されることも実利に叶う施策であると考えられる。また、認証期限が 1 年という点も、維持コスト及び工数の両方に影響があるが、定期的なコンプライアンスの契機となる点がメリットであるとする事業者もある。
(4)認証取得のインセンティブに関する課題（グループ認証、PRP 認証）	日本で導入されていない 2 つの制度は、CBPR に参加する国や地域で差異がある事自体、1 つの制度としての有効性を欠くものであるため、早急に劣後した現状の改善が求められる。グループ認証についてはガバナンス面、情報取得、適切な運用などを踏まえて検討を進める必要がある。一方で、PRP の導入を望む声は多く、急務と考えられる。

本章の調査結果と分析からなるこれらの項目を念頭において、CBPR の推進にむけて議論を進めてゆくことが必要となる。

第3章 CBPR の普及と認証企業増に向けて

ここまで調査の概要と判明した CBPR をめぐる実態についてまとめてきた。事業者の関心事として、GDPR における越境移転ツールとの役割や法的な有効性の違いをはじめ、BCR や ISMS、P マーク等における要求事項との差異をマッピングにより明らかにした。また、ステークホルダー側の情報を集約するために、事業者ヒアリングと各国 AA へのアンケートを通じて課題を洗い出し、第 2 章までにまとめを行った。

以上の調査に基づく制度改善内容への方向性を踏まえたうえで、今後求められる実施項目について最終的なまとめを行う。まず、本章の以下の提言内容（アクションプラン）を基に、今後多くの意見を求めてさらに実効性の高いアクションプランに結び付けるための全体としての方向性を記しておく。

まず、企業へのヒアリング調査で度々挙げられた CBPR 取得による個人情報保護上の有効性、実際の手続きと利点、将来の発展構想などの実態を訴求する必要がある。また、そのための責任ある実施体制を作り、審査・取得プロセスの効率化とプロセスの可視化、合理化を図ることが求められている。行政を中心として推進体制の充実を図り、必要な権限と実施の体制をいち早く作り上げることで制度そのものの普及につなげることができる。一方で、CBPR を取り巻く周辺の状況についても十分な対応が必要であり、他の国内認証制度と運用を含む共通化の調整が求められる。海外の主体に対しても、事業者が通商上の具体的な利点と認識できるような制度を意識して、相手先の法制度・運用慣習の中で CBPR が持つ利点を有効化できるように議論を展開する必要がある。

以上を踏まえて、これまでの分析結果から提示されたアクションプランについて次の図表にまとめる。ここでは図表 42 の対象者を次の通り定義した。ただし、事業者だけはアクションの訴求対象者である。

＜訴求対象＞

・事業者：新規申請企業および認証企業

・外国政府：AA など関連する主体を含み制度運用をしている者

＜主体＞

・推進者：AA や関連する行政主体

・国内認証関係者：制度の運営に関連する者

・全体（行政）：我が国において制度の発展に司令塔としての役割を持つ行政機関

図表 42　CBPR の普及と認証企業増に向けたアクションプラン

対象	アクション	内容	根拠・理由
訴求対象			
事業者	認知度の向上	認証制度の存在そのものに対する認知度を向上させるために、普及啓発活動に注力する	CBPR 認証制度そのものに対する認知度が必ずしも十分とは言えない
事業者	有効性の訴求	GDPR など他の越境移転ツールに比較して CBPR が有効である業務を明確にする	事業者との対話においても GDPR など地域限定の越境移転ツールの有効性が過大に認知されている可能性がある
外国政府	柔軟性・具体性の訴求	世界規模でのデジタル変革とデジタル経済の発展のために、多様性を前提とした有効な越境データ移転ツールであることを踏まえ、その運用と執行協力の柔軟性、要件の具体性について訴求する	海外 AA の実態調査において、現実に各国多様な法制度を踏まえて運用されていることが明らかになった
外国政府	相互運用の拡大	国・地域限定の各国法制度下での越境移転ツールに対して、相互運用により広い範囲への越境移転を対象としたものである点を踏まえ、その対象となる国・地域の拡大を推進する	事業者ヒアリングにおいて、GDPR 関連の越境移転ツールの有効性（対象地域・業務）が過大に捉えられている傾向があった
訴求対象			
推進者	将来方針の明示と訴求	制度としての位置づけ（特に GDPR 関連の越境移転ツールとの違い、特徴）や目指している自由なデータ流通の構想の中での方針と制度の発展性を訴求する	事業者ヒアリングでも全体像、将来方針に付いての理解に結びつけられる課題が見受けられた
国内認証関係者	認証事務の共通化	ISMS や P マークの取得（候補）者に対して、書類作成や事務手続き上共通化できる部分を検討して、ワンストップ化に近づけトータルコストを削減に結	事業者ヒアリングでも認証事務の共通化による効率化は重要な要望としてあげられている

		び付ける（希望する企業にはオプションで CBPR の選択ができるようにすることも考えられる）	
国内認証関係者	各認証制度要求項目の整理	それぞれの認証制度が持つ独自性や目的の違いによる要求項目を可視化しポジショニングを明確にする	事業者ヒアリングにおいて、「わかりにくさ」に結びつく要素が多く見受けられた
全体（行政）	体制の充実・明確化	国内において明確で強力な推進体制（司令塔）が必要となる	海外 AA の運用方針では、強力なリーダーシップにより施策が講じられているケースがある
全体（行政）	PRP（プロセッサー向け認証制度）への対応	CBPR 認証制度の一部であり海外でも多くの認証企業を集めている PRP については、コントローラーとは異なる要求事項を踏まえ、を国内法・委員会規則・ガイドラインと整合させながら推進することも必要である	P マークの付与事業者を見ても相当数がプロセッサーであることから、PRP に対応することで認証企業が増加する可能性があるのではないか。対応しないと認証企業の増加は見込めない
全体（行政）	グループ認証（国内外のグループ企業も含めた認証）への対応	グループ認証については現在一部の国で実施されているが、我が国においては実施に向けた明確な方針が示されてないので早急に対応する必要がある	事業者ヒアリングにおいてグループ企業への信頼向上、審査事務の集約化（グループ内小規模会社も対象となる）、心理的ハードルの低減、トータルコストの削減を望む意見が出された

上記はあくまで提案事項を構成する要素の整理案であり、具体的な実施内容については、関係各方面で検討する必要がある。CBPR の普及には、制度の理解促進、コスト・工数の削減、インセンティブの導入、国際的な連携強化を含めて本報告書で分析の結果明らかになった事項を踏まえて、推進体制を充実させてゆくことが必要である。

GCBPR の運用が開始されれば、制度への参加対象は世界に広がり、そのための様々な準備も整えておく必要がある。今後は継続的な実態把握のための調査活動の他、表に掲げた各対象主体との対話を充実させ、アクションプランの確定と共有、優先順位を決めた着実な実行に向けての努力が求められることになる。