

令和4年度
規制改革推進のための
国際連携事業
(データ保護ないし越境移転に関連する
諸外国の企業認証制度等に係る動向調査)

調査報告書

2023年2月



経済産業省
Ministry of Economy, Trade and Industry

本報告書の構成

1	本事業の位置づけ	P. 02 - 05
1.1	本事業の背景・目的と実施の基本方針	P. 03
1.2	本事業の全体のアプローチ	P. 04 - 05
2	データ越境移転関連調査	P. 06 - 94
2.1	調査の目的と調査結果サマリ	P. 07 - 14
2.2	調査結果詳細：規制/国際ルール	P. 15 - 49
2.3	調査結果詳細：越境移転ツール	P. 50 - 70
2.4	調査結果詳細：その他関連ツール	P. 71 - 94
3	事業者によるツール等の活用実態調査	P. 95 - 123
3.1	調査の目的・アプローチ	P. 96 - 100
3.2	調査結果サマリ	P. 101 - 106
3.3	調査結果詳細：事業者のヒアリング結果	P. 107 - 123
4	調査結果のまとめ	P. 124 - 127

Agenda

- 1. 本事業の位置づけ
- 2. データ越境移転関連調査
- 3. 事業者によるツール等の活用実態調査
- 4. 調査結果のまとめ

本事業の背景/目的と、実施の基本方針



背景/目的

本事業の背景:

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

データの流通や越境移転を促進するための手段として、企業認証制度が存在する。APECにおいて企業等の越境個人データの保護に関するプライバシー原則への適合性を認証するシステムであるCBPR (Cross Border Privacy Rules) は、2022年4月、APECの枠にとらわれないより裾野の広い国家間での自由なデータ流通圏を構築するための独立した新フォーラムとして立ち上げられることが宣言された

本事業の目的:

本事業では、この新しいフォーラムが効果的なデータプライバシーの保護や各国/地域におけるデータ保護関連の規律の相互運用性の促進を実現できるものとして構築されていくための設計の前提となる情報の収集・分析を行うべく、各国/各地域で検討、導入されているデータ (個人データに限らない) の越境移転に関する認証制度等の内容を詳細に調査する



実施の基本方針

昨年度までの検討* を踏まえて、以下を実施する

- 各国/地域で検討、導入されているデータの越境移転に関する規制/ツールの概念の整理
- 規制/ツールの内容の詳細な整理・分析
- 国内外の事業者インタビューを通じた既存ツールの課題、越境移転に関する事業者ニーズの洗い出し

*(参考)

我が国におけるデータ駆動型社会に係る基盤整備 調査報告書

https://www.meti.go.jp/meti_lib/report/2021FY/000376.pdf

データの越境移転に関する研究会

https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_itn/pdf/20220228_2.pdf

諸外国の個人情報保護制度に係る最新の動向に関する調査研究報告書

https://www.meti.go.jp/meti_lib/report/2021FY/000377.pdf

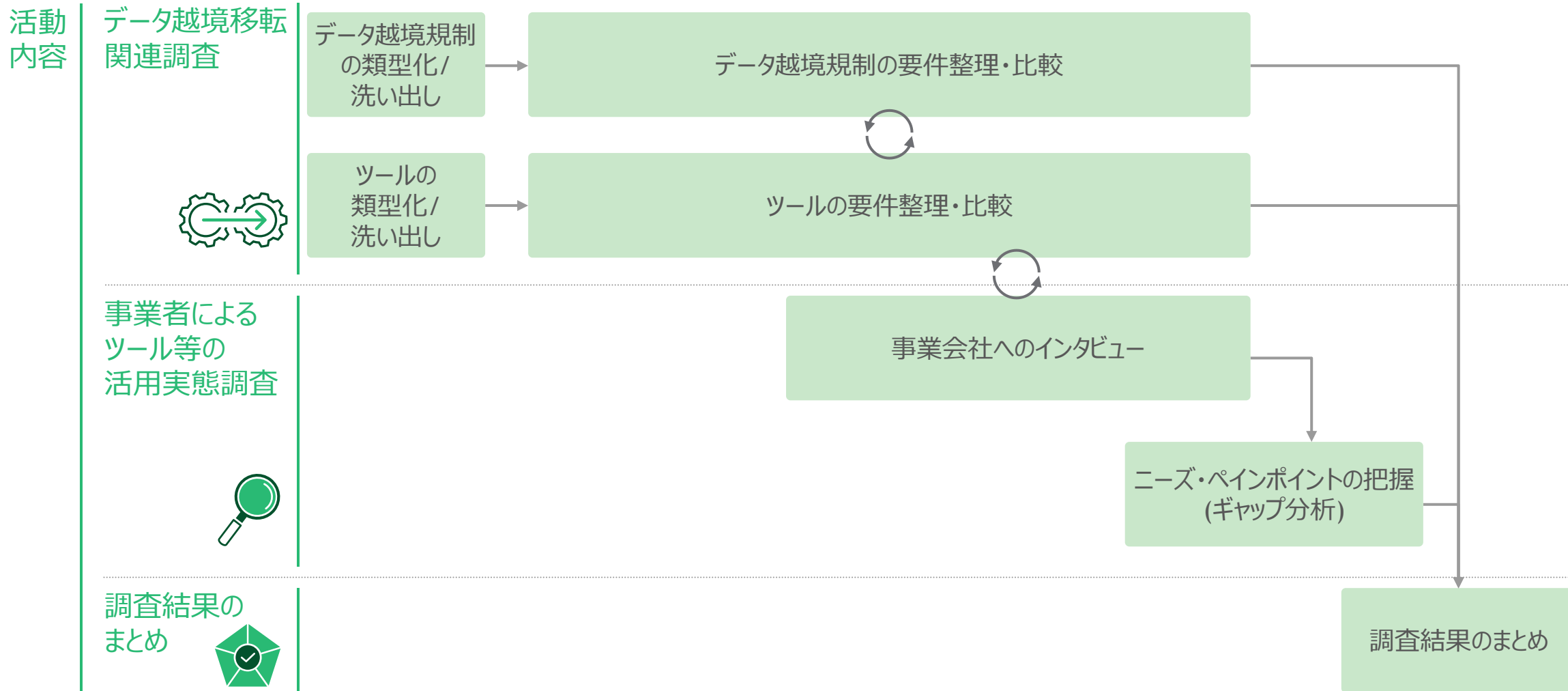
日米欧における個人データの越境移転に関する実態調査結果報告書

https://www.ppc.go.jp/files/pdf/nichibeiou_ekkyouiten_report.pdf



本事業のアプローチ

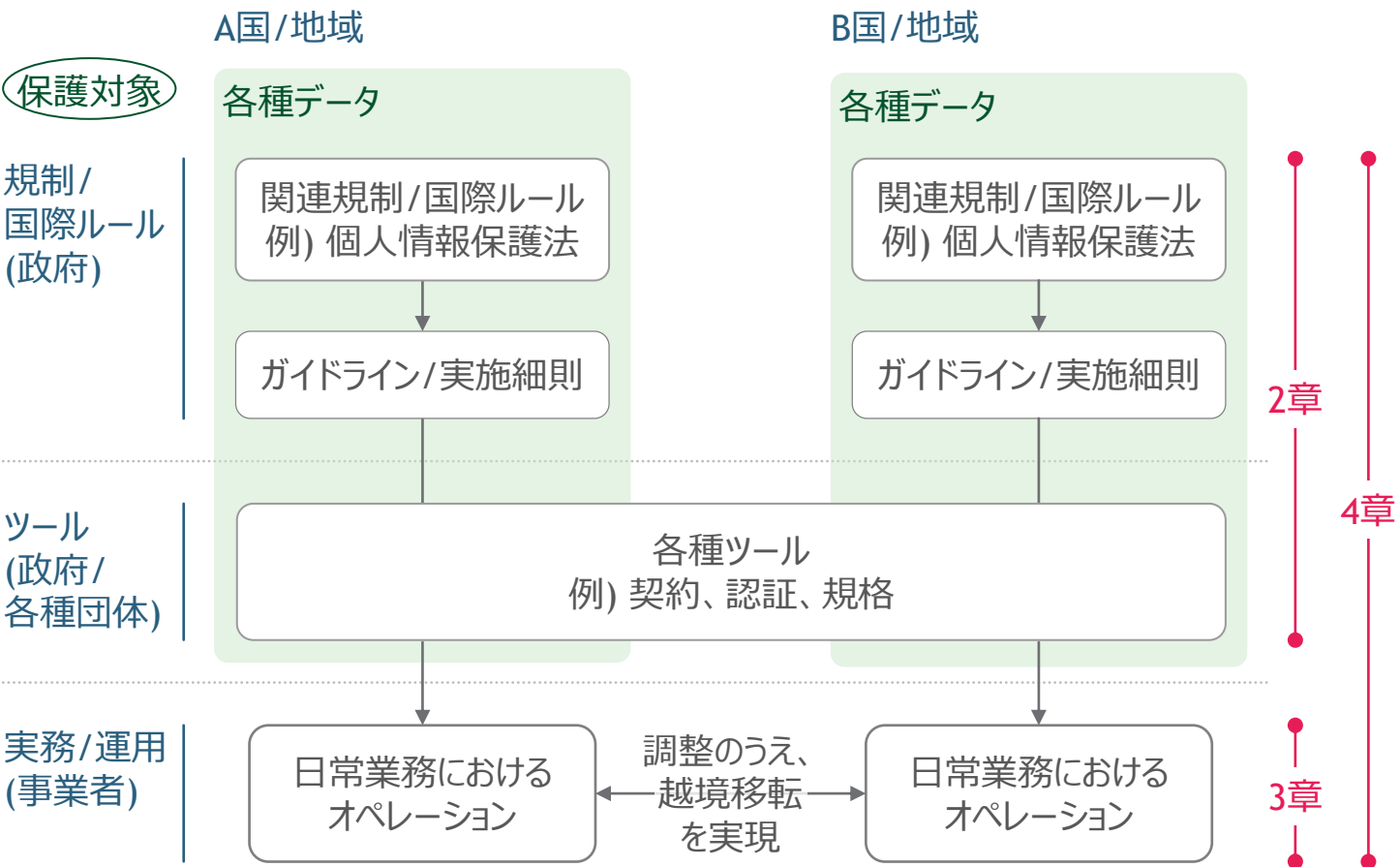
データの越境移転に係る規制やツールを洗い出した上で、事業者へのヒアリングを通じ活動実態を調査。ニーズやペインポイントを分析する



データ越境移転を巡る概念と全体のアプローチの整理

データの越境移転の実務

データの越境移転自体は、事業者の日常業務内で実現されるが、そのために、各事業者は、関連する規制の履行と、ツールの活用を行っている



アプローチ

本調査は「データ保護関連の規律の設計の前提情報の収集・分析」を目的としているが、「データ保護関連の規律」は、左記の流れで実務に転化されている

- 各国/地域の規制/国際ルールが越境移転の要件を規定
- 規制/国際ルールの履行に必要な詳細をガイドライン/実施細則が規定
- 事業者が実務化するための要件を整理し、活用可能にしたものとして、各種ツールが存在

そのため、本調査では、左記のデータの越境移転の実務を意識して、各種情報を整理する
まず、第2章でデータの越境移転のベースとなる規制/国際ルールやツールを整理し、データの越境移転の前提の理解をすすめる

第3章では、事業者の越境移転に関するオペレーションの実態を調査し、政府等の規制/国際ルール及びツールとのギャップ及び、それらに対する事業者の反応を明らかにする

最後に、第4章では、調査内容全体を取りまとめ、新フォーラムの検討に関する示唆を導出する

Agenda

1. 本事業の位置づけ
- 2. データ越境移転関連調査
 - 2.1 調査の目的と調査結果サマリ
 - 2.2 調査結果詳細: 規制/国際ルール
 - 2.3 調査結果詳細: 越境移転ツール
 - 2.4 調査結果詳細: その他関連ツール
3. 事業者によるツール等の活用実態調査
4. 調査結果のまとめ



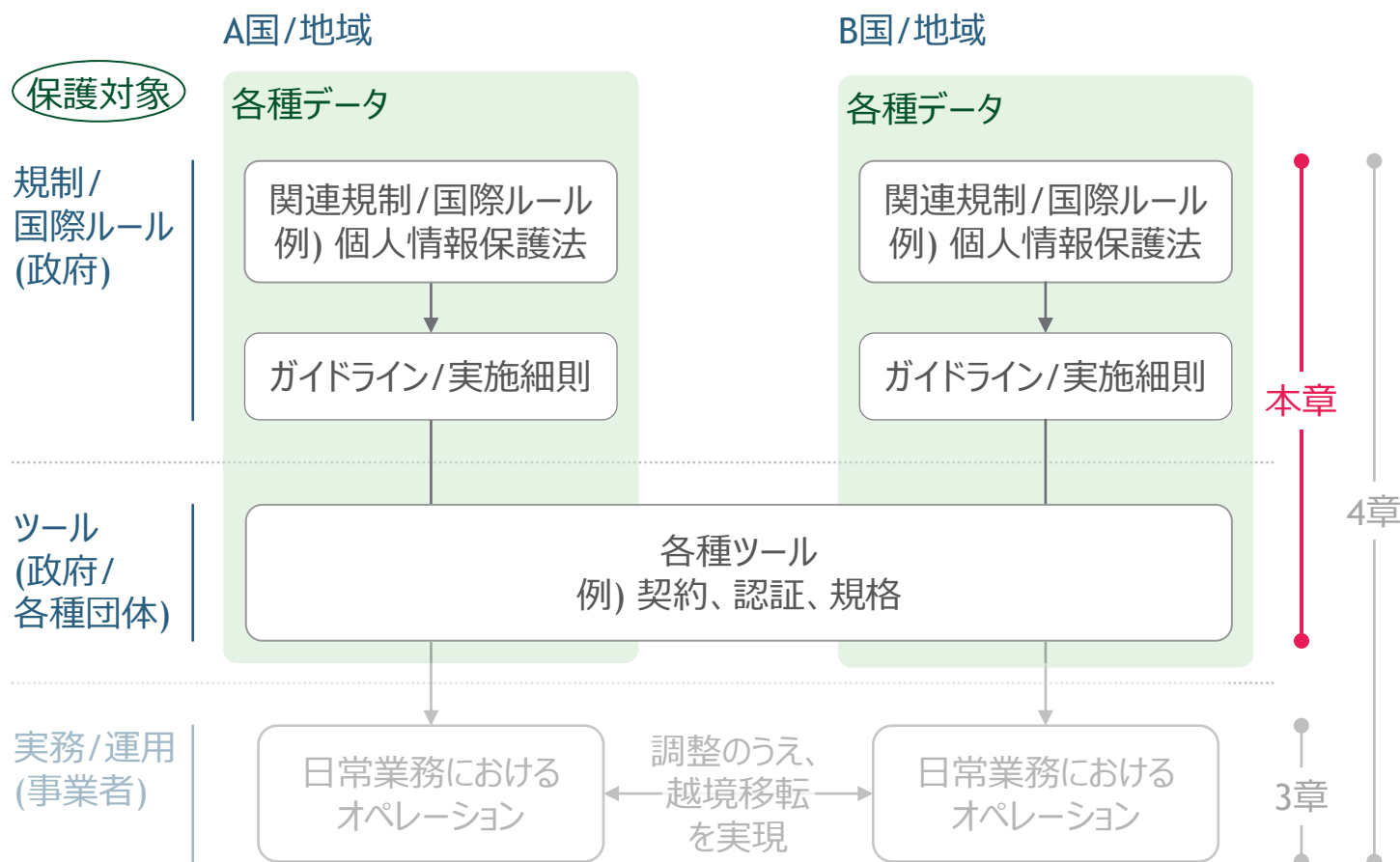
2.1

調査の目的と調査結果サマリ

本章の目的

データの越境移転の実務

データの越境移転自体は、事業者の日常業務内で実現されるが、そのために、各事業者は、関連する規制の履行と、ツールの活用を行っている



目的

第2章では、データの越境移転の大前提となる規制/国際ルールの概要の整理をおこなう。

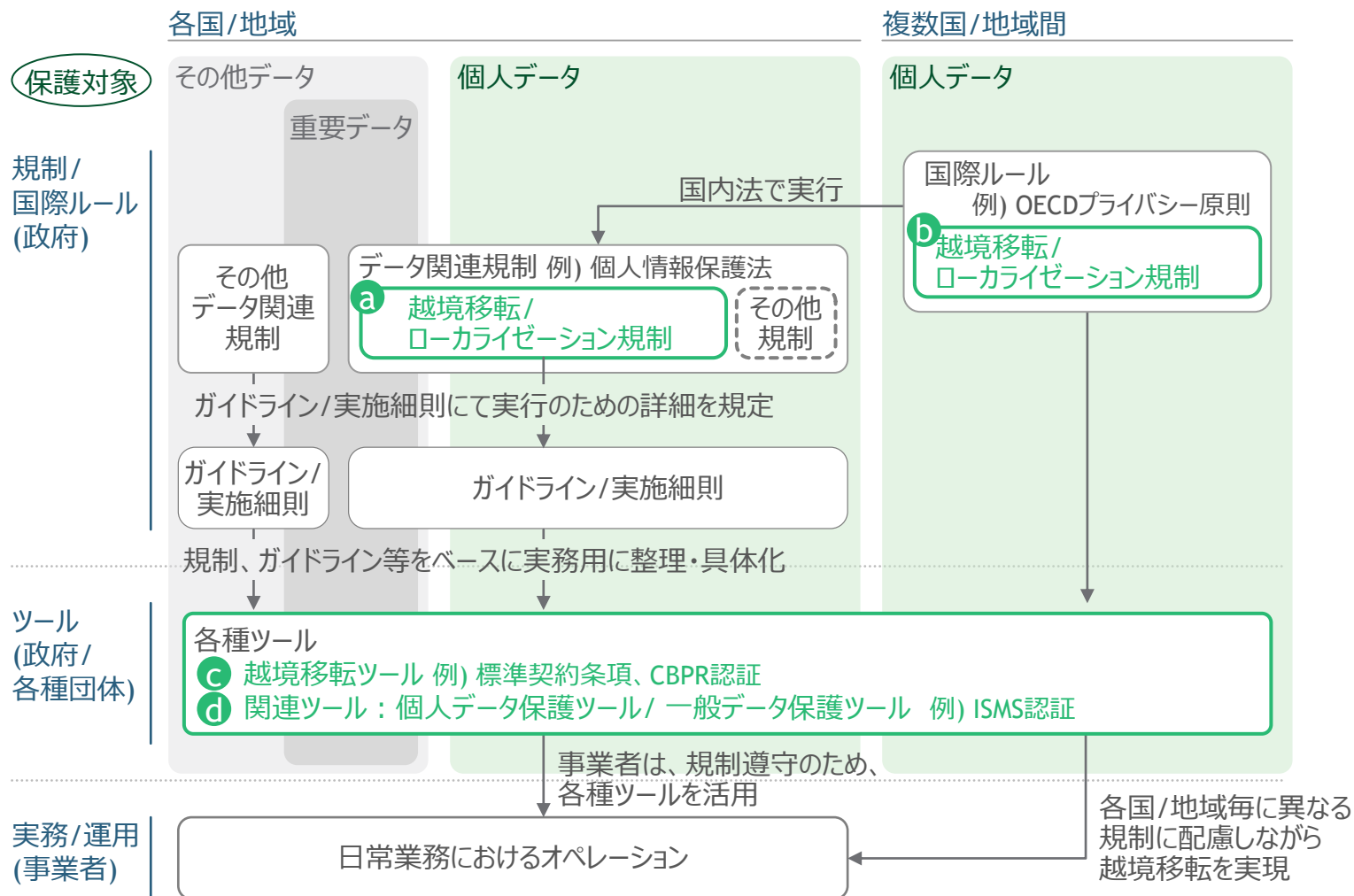
規制/国際ルールの整理を通じて、事業者がデータの越境移転をおこなう際に遵守すべき要件や、利用可能なツールを整理し、データの越境移転をめぐる現時点での国際的な動勢を観察する。

また、本章で得た情報を前提に、3章の実態調査をすすめる。

本章のアプローチ

本調査では、越境移転をめぐる概念を以下のように整理したうえで、**a** - **d** を調査範囲とする

データの越境移転をめぐる詳細



アプローチ

データの越境移転に関する規制/国際ルール、ツールは、より詳細には左記のように整理される。

具体的には、ほとんどの場合、各国/地域の個人情報保護法を中心としたデータ関連規制で、データの越境移転が規定されている。

データの越境移転規制には、越境移転そのものに関する規制 (越境移転規制) と、その規制に影響を与えるデータの国内保存義務等を含むローカライゼーション規制の2つが含まれている。

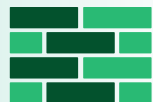
また、各国/地域レベルの規制は、各種国際組織が定める国際ルールの影響を受けているため、本調査でも、**2つの越境移転関連規制及び国際ルールを調査対象とする。**

なお、データの越境移転がグローバルに行われている現状を鑑み、**規制の調査対象として、日本を含めた22の国/地域及び関連する国際組織を選定。**

ツールに関しては、越境移転そのものに関するツールに加え、**関連する個人データ保護ツール及び一般データ保護ツールまで調査をおこなう。**

越境移転関連調査結果サマリ (1/3)

現状



個人データの越境移転には、国際ルール、規制、越境移転ツール、その他データ保護関連ツールなど多数の制度が関連。事業者がデータ流通をおこなうためには、その目的やデータ流通の範囲に応じて、個別に対応しなければならない

各制度は個々に独立しているものの、相互に影響し合っており、近年では、一定の方向性が見えつつある

- 国際ルール：OECD/APECのプライバシー原則が基本。内容に若干の相違はあるが、おおむね共通
- 各国/地域規制：
国際ルールを大原則としながら、各国/地域が個別に整備を進めており、現時点では大きく4つの流れが存在。中でも、EUが昨今の越境移転規制をリードしており、後進国を中心にGDPRに類する規制の採用が増えている
- 越境移転ツール：
GDPRで規定されるツールを中心に様々なツールが存在。特にSCC/MCCは、GDPR型の規制を持たない国（中国など）でも普及しつつあり、越境移転ツールとして最も多くの国に採用されている
 - ただし、SCC/MCCも各国/地域規制をベースとしているため、グローバルなデータ流通のためには複数ツールの併用が必要。一部、国際ツールも登場しているが、採用国が少ない
- データ保護ツール：各国/地域規制を根拠とした認証制度が多数存在。要求には共通性が見られるほか、越境移転ツールとの接続も図られており、個人データ保護/データ流通の利便性の向上もすすむ

今後の方向性 (案)



個人データの越境移転をめぐる多様な規制・ツールが存在するが、共通性も見られるため、グローバルでツール間の接続や統合が図られることが期待される

- 韓国では、データ保護関連認証が乱立したため、制度の統一が図られた例がある
- 現時点でも、台湾は自国の規制に基づく一般データ保護認証（範囲：国内）とグローバル認証を接続することで、個人データの越境移転の効率的な推進を推奨

越境移転関連調査結果サマリ (2/3)：越境移転/個人データ保護の主要要件比較

CBPR認証と個人データ保護認証の間では、データ主体の権利保障のための措置を除き、おおむね共通性が見られる

			越境移転認証		個人データ保護ツール									
			9 APEC CBPR認証	10 APEC PRP認証	1 1 GDPR -CARPA	2 2 dp.mark	3 3 DPTM	4 4 ISMS-P 認証	5 5 プライバシー マーク	6 6 JAPHIC マーク ¹	7 7 Euro PriSe	8 8 TRUSTe マーク	9 9 CNIL 認証	11 11 個人情報 安全規範
他ツールとの接続					✓ 46条で越境移転 の根拠と定義	✓ CBPRと合わせて 取得を推奨	✓ ISMS認証と 接続	✓ ISMS認証と 接続	✓ JISQを根拠 とする				責任者に 関連する 事項のみ 定義	✓ 越境移転の前提 として遵守が必須
基本 措置	プライバシー 原則遵守	処理制限	●	●	●	●	●	●	●	●	●	●		●
		通知/選択/公開	●		●	●	●	●	●	●	●	●		●
		正確性	●	●	●	●	●	●	●	●	●	●		●
		安全保護措置	●	●	●	●	●	●	●	●	●	●		●
		個人参加/アクセス	●		●	●	●	●	●	●	●	●		●
		損害回避	●											
		アカウントバリティ	●		●	3	●		3		●	3		●
	機微データの取扱い制限		●		●	●	●	●	●	●	●	●		●
	アセスメント (データ保護評価) の実施		●	●	●	●	●	●	●		●	●		●
	処理の記録		●		●	●	●	●	●	●	●	4		●
データ主体の権利を 保障するための措置	組織・技術的保護措置の実施		●	●	●	●	●	●	●	●	●	●		●
	移転/委託	委託先の評価	●		●	●		●	●	●	5	●	※次ページで 詳細比較	●
		制約・義務の文書化	●		●	●	●	●	●	●	5	●		●
		委託先の監督	●		●	●		●	●	●	5	●		●
		越境移転時の保護措置	2		●	●	●	●	●	●	●	●		●
	アクセス権の保障	アクセス権の保障	●		●	●	●	●	●	●	●	●		●
		自動処理のみによる決定 に服しない権利の保障			●	●					●			●
		苦情/異議申立の保障	●		●	●	●	6	●	●	●	●		●
		データポータビリティの保障			●	●	●		●	●	●	●		●
		児童の権利保障			●	●					●	●		●

1. 個人情報通則編を比較に利用 2. 該当項目はないが、そもそも越境移転を認証の目的・規制対象としている 3. 経営者層に結果・履行責任やコミットメントを要求 4. 第三者提供活動に関してのみ記録を要求
5. プロセッサーや共同管理者等に区別して定義 6. データ主体の権利保障のために求められる措置は、個人データの閲覧、訂正・削除、処理停止、異議申し立て、同意撤回要求への対応となっており、個人データの
開示や複製の文言は見られない
Source: 各種管轄団体のHP等

11

Copyright © 2023 by Boston Consulting Group. All rights reserved.

越境移転関連調査結果サマリ (3/3)：技術的・組織的保護措置の要件比較

大まかにはGDPR準拠の認証か否かで相違があるが、ISMS-P認証やTRUSTeマークはGDPR準拠の認証同様、詳細に措置を規定している

	越境移転認証		個人データ保護認証								9 CNIL 認証	11 個人情報 安全規範
	9 APEC CBPR認証	10 APEC PRP認証	1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P 認証	5 プライバシー マーク	6 JAPHIC マーク ¹	7 Euro PriSe	8 TRUSTe マーク		
個人データの仮名化及び暗号化の措置	2	●	●		5	●	適切な 保護措置の 実施要求 のみ 詳細要件の 例示等はない ⁸	●	●	●	責任者に 関連する 事項のみ 定義	●
システム/サービスの機密性・可用性及び 回復力を確保するための措置	3		●	●		●			●	●		
物理的技術的インシデント発生時に、データの 可用性とアクセスの復元を確保するための措置	●		●			●			●	●		
処理のセキュリティを確保するための技術的 組織的措置の有効性の定期的なテスト	●	●	●	●	●	●			●	●		
ユーザーの識別と認証のための措置	●	●	●	●		●		●	●	●		
移転中のデータ保護に関する措置	● ²		●			●			●	●		
保管中のデータ保護に関する措置	●		●			●		●	●	●		
個人データの処理がおこなわれる場所の物理的 セキュリティ措置	●	4	●	●	6	●		●	●	●		
イベントログの確保のための措置	●	●	●			●		●	●	●		
デフォルトを含むシステム構成確保のための措置	●	●	●	●	7	●		●	●	●		
内部IT及びITセキュリティのガバナンスと管理に 関する措置	●	●	●	●		●		●	●	●		●
プロセス及び製品の保証/認証のための措置	●		●	●	7	●			●	●		
データの最小化を確保するための措置			●	●		●		●	●	●		
データ品質を確保するための措置	●		●	●	●	●		●	●	●		
データ保持の限定性を確保するための措置			●		●	●		●	●	●		●
説明責任を確保するための措置			●						●			
データポータビリティと廃棄を確保するための措置			●						●	●		

Note: EU SCC Annex II に示されている技術的・組織的保護措置の具体例を軸に比較 Source: 各種管轄団体のHP等
1. 個人情報通則編を比較に利用 2. 暗号化に関しては、限定的な要求（個人情報の移送・通信時の対策として規定）に留まる（CBPR認証基準 別紙） 3. 「個人情報の機密性に応じた妥当な措置」の要求のみ（CBPR認証基準 6.3項） 4. 「物理的保護措置の説明」は要求するが、具体的な措置内容の記載はなし（PRP Intake Questioners #2） 5. 保管時に匿名化に関する方針を文書化することは要求しているが、匿名化自体を要求する項目はない（DPTM Checklist Rule3 #5） 6. 「物理的保護措置の実施」は要求するが、具体的な措置内容の記載はなし（DPTM Checklist Rule3 #1） 7. 具体的な措置内容の記載はないが、システム開発時のデータ保護設計を要求（DPTM Checklist Rule1 #7） 8. 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 J.9.2項 留意事項

参考) 要件比較項目：プライバシー原則

要件比較で用いたプライバシー原則の各項目は以下の内容で整理して、該当有無を調査

国際ルールで定められたプライバシー原則の該当項目				
要件名	OECD (8項目)	APEC (9項目)	ASEAN (7項目 ¹)	各ツールの該当項目 例: プライバシーマーク、EU SCC
処理の制限 	<div>① 収集制限の原則</div> <div>③ 目的特定化の原則</div> <div>④ 利用制限の原則</div>	<div>④ 個人情報の利用</div> <div>③ 収集の制限</div>	<div>① 同意、通知、目的</div> <div>⑥ データ保管</div>	<div>></div> <div><div>・ 利用目的の特定 (プライバシーマーク J.8.1項)</div><div>・ 目的の制限 (EU SCC8.1条)</div></div>
通知/選択/公開 	<div>⑥ 公開の原則</div>	<div>② 通知</div> <div>⑤ 選択の機会</div>	<div>① 同意、通知、目的</div>	<div>></div> <div><div>・ J.8.2項</div><div>・ 透明性 (EU SCC 8.2条)</div></div>
正確性 	<div>② データの質の原則</div>	<div>⑥ 個人情報の正確性</div>	<div>② 個人データの正確性</div>	<div>></div> <div><div>・ 正確性の確保 (プライバシーマーク J.9.1項)</div><div>・ 正確性及びデータの最小化 (EU SCC 8.3条)</div></div>
安全保護措置 	<div>⑤ 安全保護措置の原則</div>	<div>⑦ 安全保護措置</div>	<div>③ 安全保護</div>	<div>></div> <div><div>・ 安全管理措置 (プライバシーマーク J.9.2項)</div><div>・ 処理のセキュリティ (EU SCC 8.5条)</div></div>
個人参加/アクセス 	<div>⑦ 個人参加の原則</div>	<div>⑧ アクセス及び訂正</div>	<div>④ アクセス及び訂正</div>	<div>></div> <div><div>・ 個人情報に関する権利 (プライバシーマーク J.10.1項)</div><div>・ データ主体の権利 (EU SCC 10条)</div></div>
損害回避 	<div>—</div>	<div>① 損害の回避</div>	<div>—</div>	<div>></div> <div><div>・ 該当なし</div></div>
アカウンタビリティ 	<div>⑧ 責任の原則</div>	<div>⑨ アカウンタビリティ</div>	<div>⑦ 説明責任</div>	<div>></div> <div><div>・ 記録と本条項の遵守 (EU SCC 8.9条a)</div></div>

1. ASEAN PDPフレームワークの原則5 (越境移転) は、OECD/APECと共通性がないこと等から、原則外の項目として整理して要件を比較
Source: 堀部政男・新保史生・野村至「OECDプライバシーガイドライン—30年の進化と未来」2014年; APEC "APEC Privacy Framework (2015)" 2017; ASEAN "ASEAN Telecommunications and information technology ministers meeting (TELMIN) Framework on personal data protection" 2016; European Commission "Standard Contractual Clauses (SCC)"; JIPDEC「プライバシーマーク®制度」

参考) 要件比較項目：技術的・組織的保護措置

関連ツールでは、かなり具体的な技術対策の実施が確認される場合もあるため、具体事例がある場合は、以下のように整理して比較

EU SCCにおける技術的・組織的保護措置の具体例	各ツールで記されている具体的な対策例 ※黒字=技術的措置、青字=組織的措置、緑字=物理的措置
個人データの仮名化及び暗号化の措置	暗号化、匿名化、仮名化処理 等
システム/サービスの機密性・可用性及び回復力を確保するための措置	データのバックアップシステムの導入、各情報システムの同期 等
物理的技術的インシデント発生時に、データの可用性とアクセスの復元を確保するための措置	データのバックアップシステムの導入 等
処理のセキュリティを確保するための技術的組織的措置の有効性のテスト	技術的脆弱性の管理、定期監査の実施 等
ユーザーの識別と認証のための措置	ID/PWの利用 等
移転中のデータ保護に関する措置	ネットワークセキュリティ対策の実施、データ受け渡しのためのデバイスの識別管理 等
保管中のデータ保護に関する措置	データのバックアップシステムの導入、アクセス制御 等
個人データの処理がおこなわれる場所の物理的セキュリティ措置	サーバー/コンピューター利用区域の設置、入退室管理 等
イベントログの確保のための措置	ログファイルの作成、ログ記録/監視システムの導入 等
デフォルトを含むシステム構成確保のための措置	データ保護・バイ・デフォルト (バイ・デザイン) の実施、各種不正対策ソフトウェアの導入 (マルウェア対策、ファイアーウォール等)、ネットワーク制御 等
内部IT及びITセキュリティのガバナンスと管理に関する措置	ネットワーク管理、アクセス権限の管理 等
プロセス及び製品の保証/認証のための措置	ソースプログラム管理、テストデータの管理、開発プロセス (テスト・リリース等) の確立 等
データの最小化を確保するための措置	プライバシー原則を遵守するための措置及び、データ主体の権利保護のための措置と重複するため、 具体技術の例示はない ※ 比較表では、該当するプライバシー原則を遵守するための措置及びデータ主体の権利保護のための措置 に関する規定があった場合、該当あり (●) と判定
データ品質を確保するための措置	
データ保持の限定性を確保するための措置	
説明責任を確保するための措置	
データポータビリティと廃棄を確保するための措置	

Note: EU SCCでは、技術的・組織的保護措置 (Technical and Organizational Measures) と呼ばれているが、その内容は、技術的措置、組織的措置、物理的措置の3種を含む。SCC/MCC等の越境移転ツールにおいては、暗号化要求以外の具体的な措置 (例: ネットワーク制御 等) が示されるものは少なく、「物理的措置」「技術的及び管理的措置」といったレベルでの要求となっている。一方、一般データ保護ツールでは、より具体的に措置が列挙されている場合が多く、その場合には本頁の整理に沿って比較項目への該当を判断した



2.2

調査結果詳細：規制/国際ルール

規制/国際ルール 調査対象

本調査では、各国/地域規制から国際ルール・貿易協定まで幅広く関連規定を調査

	名称	対象国・地域	発効年
規制	 ① 主要国/地域における越境移転/ローカライゼーション規制	EU、米国、日本等 22カ国/地域	—
国際ルール	 ① OECDプライバシーガイドライン (OECD Guidelines governing the protection of privacy and transborder flows of personal data)	OECD (経済協力機構) 加盟国	1980年 (2013年改訂)
	② 個人データの自動処理に係る個人の保護に関する条約 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: 欧州評議会条約第108号)	55カ国 (欧州評議会メンバー46カ国及び、非加盟国9カ国)	1985年 (1999年改訂)
	③ APECプライバシー・フレームワーク (APEC Privacy Framework)	APEC (アジア太平洋協力) 加盟国	2004年 (2016年改訂)
	④ ASEAN 個人データ保護フレームワーク (ASEAN Framework on Personal Data Protection: ASEAN PDPフレームワーク)	ASEAN (東南アジア諸国連合) 加盟国	2016年
貿易協定	 ① サービスの貿易に関する一般協定 (General Agreement on Trade in Services: GATS)	WTO (世界貿易機構) 加盟国	1995年
	② 地域貿易協定 (Regional Trade Agreement: RTA) <ul style="list-style-type: none"> i) 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 (Comprehensive and Progressive Agreement for Trans-Pacific Partnership: CPTPP) 	日本、シンガポール、ベトナム、オーストラリア、ニュージーランド、カナダ、メキシコ、ペルー	2021年
	<ul style="list-style-type: none"> ii) 地域的な包括経済連携協定 (Regional Comprehensive Economic Partnership Agreement: RCEP) 	ASEAN10カ国、日本、韓国、中国、オーストラリア、ニュージーランド	2022年

規制/国際ルール 調査結果サマリ (1/2)

国際ルールを前提に各国/地域別で規制を整備。GDPRに類似する規制の整備が進む一方で、ローカライゼーションを整備する国も存在



特定の要件を満たした場合に個人データの越境移転を認めている規制が大半であるが、越境移転の要件は、各国/地域で異なる

- ほとんどの国/地域 (11カ国/地域) では、越境移転に際して、本人同意、移転先が自国と「同等」もしくは「十分な水準」のデータ保護制度を持つことを要件としている
- 11カ国/地域のうち、移転先の保護水準を公的に認証する制度 (充分性認定¹ 等) まで規定している国/地域は、7カ国/地域に留まる
 - 「同等の水準」「十分な水準」の規定はないが、類似する規定 (「データ輸出者がデータ輸入者と同じ義務を負う」) を持つメキシコを含めると8カ国/地域
- 本人同意、「同等」もしくは「十分な水準」の保護に加えて、当事者間での法的拘束力のある文書の締結や認証・シール、行動規範² を越境移転の要件として認める国/地域も4カ国/地域存在。いずれもGDPRに準じた規制を策定している
- なお、例外的に個人データの越境移転に関して特段の要件を定めていない国/地域も存在する



ローカライゼーション規制を持つ国/地域は多くはないが、中国、ロシアをはじめとしたいくつかの国/地域は、越境移転規制に加えて、データの国内保存などを定めている

- 中には、例外的に個人データの越境移転規制は持たないが、ローカライゼーション規制のみを持つ国/地域も存在する



複数国間に適用される要件も存在し、特に国際ルールはすべてのベースとして、各国/地域規制とも相互に影響し合っている

- OECD及びAPECのプライバシー原則はグローバルスタンダードして、各種データ保護規制・ツールに適用されている

1. 各国/地域の担当機関が個人データ取扱う対象が、その判断基準に照らして十分な個人データ保護水準を確保していると認める制度。充分性認定を受けた場合、その対象への個人データの移転が認められる
2. 事業者や団体が定める個人データ保護のルール・ポリシー

規制/国際ルール 調査結果サマリ (2/2) : 各国/地域規制の要件比較

各国/地域における越境移転の主な要件 (例外事由を除く) 及びローカライゼーション規制の存否は以下の通り

		越境移転規則（越境移転の要件）							規制	
		本人同意	移転先の保護制度		文書の締結（国際協定を含む）		認証、シール等		行動規範	その他
			同等/十分な水準	十分性認定	法的拘束力のある文書	SCC	BCR	その他		
GDPRに類似する 規制を持つ国/地域	EU			●	●	●	●	●	●	● 当局が承認した取決め等
	イギリス			●	●	●	●	●	●	● その他の条項/取決め
	シンガポール	●	●		●	●	●	●		● 当局の承認
	ブラジル	●		●	●	●	●	●	●	● 当局の承認等
移転に際し、 同等/十分な保護を 求める国/地域	日本	●	●	●				● ¹		
	ニュージーランド	●	●	●						
	オーストラリア	●	●							● 裁判所の承認等
	タイ	●	●				●			
	南アフリカ	●	●		●		●			● 契約に必要な場合等
	メキシコ	●	●							
	トルコ	●		●						● 書面及び当局の承認
	中国	●			●	●		●		● 当局の承認等
ローカライゼーション 規制を持つ国/地域	ロシア	●	● ²	● ²	●					● 当局の承認等
	インドネシア	●	●		●					● 大臣への連携、 国家間同意
	韓国	●								● 制度的技術的措置の 設置 ³
	ベトナム									
	インド									● 個別/分野法で規定
	サウジアラビア									● 生命の安全等、特定の 状況
										● 該当規制はないが、 実質的に制限
越境移転/ ローカライゼーション 規制を持たない 国/地域	カナダ									
	台湾									
	アメリカ									
	フィリピン									

1. ガイドラインでCBPRの利用を認めている (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」2019年) 2. 欧州評議会条約108号の批准国への移転を認めている 3. 重要データの場合



調査結果詳細：各国/地域規制

次ページ以降で以下の詳細を記載

	名称	対象国・地域	発効年
規制	① 主要国/地域における越境移転/ローカライゼーション規制	EU、米国、日本等 22カ国/地域	—
国際ルール	① OECDプライバシーガイドライン (OECD Guidelines governing the protection of privacy and transborder flows of personal data)	OECD (経済協力機構) 加盟国	1980年 (2013年改訂)
	② 個人データの自動処理に係る個人の保護に関する条約 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: 欧州評議会条約第108号)	55カ国 (欧州評議会メンバー46カ国及び、非加盟国9カ国)	1985年 (1999年改訂)
	③ APECプライバシー・フレームワーク (APEC Privacy Framework)	APEC (アジア太平洋協力) 加盟国	2004年 (2016年改訂)
	④ ASEAN 個人データ保護フレームワーク (ASEAN Framework on Personal Data Protection: ASEAN PDPフレームワーク)	ASEAN (東南アジア諸国連合) 加盟国	2016年
貿易協定	① サービスの貿易に関する一般協定 (General Agreement on Trade in Services: GATS)	WTO (世界貿易機構) 加盟国	1995年
	② 地域貿易協定 (Regional Trade Agreement: RTA)		
	i) 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 (Comprehensive and Progressive Agreement for Trans-Pacific Partnership: CPTPP)	日本、シンガポール、ベトナム、オーストラリア、ニュージーランド、カナダ、メキシコ、ペルー	2021年
	ii) 地域的な包括経済連携協定 (Regional Comprehensive Economic Partnership Agreement: RCEP)	ASEAN10カ国、日本、韓国、中国、オーストラリア、ニュージーランド	2022年



GDPRに準じた規制を持つ国/地域 (1/4)



EU

越境移転規制

対象法令

- 一般データ保護規則 (General Data Protection Regulation: GDPR)
 - 2016年発効、2018年完全施行

越境移転の対象となるデータ

直接的又は間接的に識別されうる自然人又は識別可能な自然人 (「データ主体」) に関する情報 (4条1項)

- なお、識別可能な自然人とは、「特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す1つ又は複数の要素を参照することによって、直接的又は間接的に、識別されうる者」をいう (4条1項)

越境移転規制の対象者

- 管理者: 自然人又は法人、公的機関、部局又はその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者 (4条7項)
- 処理者: 管理者の代わりに個人データを取扱う自然人もしくは法人、公的機関、部局又はその他の組織 (4条8項)

越境移転規制の内容詳細

越境移転は原則禁止だが、以下のいずれかの要件を満たす場合、域外移転が可能 (44条)

- ① 十分性認定に基づく移転 (45条)
- ② 適切な保護措置に従った移転 (46条)
十分性認定がない場合、aに加えて、b-hを提供することで、越境移転が可能
 - a. データ主体のための効果的な司法救済
 - b. 公的機関又は公的組織の間の法的拘束力及び執行力のある文書
 - c. 拘束的企業準則
 - d. 欧州委員会が採択したSCC (Standard Contractual Clauses: 標準契約条項)
 - e. 監督機関によって採択され、欧州委員会によって承認されたSCC
 - f. 承認された行動規範
 - g. 管理者又は処理者が適切な保護措置を適用することを示す認証
 - h. 監督機関の承認を受けた個別契約条項又は取決め
- ③ 特定の状況における例外 (49条)

ローカライゼーション規制

対象法令

該当法令なし



GDPRに準じた規制を持つ国/地域 (2/4)



英国

越境移転規制

英国の個人データ保護規制には、UK GDPRとDPA2018の2つが存在する。DPA2018は、英国におけるデータ保護法の枠組みを定めており、UK GDPRと並立し、UK GDPRを補足する役割を持っている。
越境移転に関しては、UK GDPR及びDPA2018がほぼ同様の内容を規定しているため、ここではUK GDPRを中心に紹介する。

対象法令

- 一般データ保護法 (General Data Protection Regulation: UK GDPR)
- 2021年施行

越境移転の対象となるデータ

- 識別された、又は識別可能な自然人（「データ主体」）に関するあらゆる情報（4条1項）
- なお、識別可能な自然人とは、「特に、氏名、識別番号、位置データ、オンライン識別子などの識別子、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的なアイデンティティに特有の1つ以上の要素を参照することによって、直接的又は間接的に、識別される者」をいう（4条1項）

越境移転規制の対象者

- 管理者: 自然人又は法人、公的機関、部局又はその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者（4条7項）
- 処理者: 管理者の代わりに個人データを取扱う自然人もしくは法人、公的機関、部局又はその他の組織（4条8項）

越境移転規制の内容詳細

越境移転は原則禁止だが、以下のいずれかの要件を満たす場合、域外移転が可能（44条）

- ① 十分性認定に基づく移転（45条）
- ② 適切な保護措置に従った移転（46条）
十分性認定がない場合、aに加えて、b-hを提供することで、越境移転が可能
 - a. データ主体のための効果的な司法救済
 - b. 公的機関又は公的組織の間の法的拘束力及び執行力のある文書
 - c. 拘束的企業準則
 - d. DPA2018年法17条C項もしくは119条A項に基づくSDPC
(Standard Data Protection Clauses: 標準データ保護条項)
 - e. 承認された行動規範
 - f. 承認された認証メカニズム
 - g. その他の個別契約条項又は取決め
- ③ 特定の状況における例外（49条）

ローカライゼーション規制

対象法令

該当法令なし



GDPRに準じた規制を持つ国/地域 (3/4)

シンガポール

越境移転規制

シンガポールの個人データ越境規制については、実施細則が詳細を規定しているため、包括法 (PDPA) に加えて、実施細則 (PDPR) も紹介する

対象法令①

個人データ保護法 (Personal Data Protection Act 2012: PDPA)

- 2012年施行

越境移転の対象となるデータ

真偽を問わず、その情報から、又は、その情報及び組織がアクセスする可能性のあるその他の情報から特定することができる自然人に関する情報 (2条)

越境移転規制の対象者

事業者

- なお、事業者は自然人、企業、団体・組織を含み、シンガポール国内での居住や居住の有無、法人か否かを問わない (2条)

越境移転規制の内容詳細

個人データは、原則移転禁止。以下のいずれかの要件を満たす場合にのみ、越境移転が可能 (26条)

- ① 移転されるデータに対して、PDPAと同等の保護水準を提供することを保障する要件を満たす場合
- ② 個人データ保護委員会 (Personal Data Protection Commission: PDPC) が許可した場合

対象法令②

個人データ保護規則 (Personal Data Protection Regulations 2021: PDPR)

- 2021年

越境移転の対象となるデータ

PDPA同様

越境移転規制の対象者

PDPA同様

越境移転規制の内容詳細

- 以下のような「PDPAと同等の保護水準の提供を法的拘束力のある義務を確保するための適切な措置」が認められる場合、越境移転が可能 (10-11条)
 - ① 法律
 - ② 契約
 - ③ 拘束的企業準則 (BCR)
 - ④ その他の法的拘束力のある文書
 - ⑤ 認証制度: CBPR、APEC PRP認証
- 加えて、PDPRは以下の場合にも、データ移転制限義務を満たすと見なせると規定 (10条)
 - ⑥ 本人同意
 - ⑦ 個人又は国家の利益のために必要であり、且つ合理的な措置が講じられている場合
 - ⑧ 個人データが転送中のデータである場合
 - ⑨ 個人データであってもシンガポールで一般に入手可能である場合

ローカライゼーション規制

対象法令

該当法令なし



GDPRに準じた規制を持つ国/地域 (4/4)



ブラジル

越境移転規制

対象法令

- 個人データ保護法 (Lei Geral de Protecao de Dados Pessoais: LGPD)
- 2018年制定後、段階的に施行

越境移転の対象となるデータ

識別された、または識別されうる自然人に関する情報 (5条1項)

越境移転規制の対象者

- ・ 管理者:個人データの処理に関して決定する責任を負う自然人又は法人 (5条6項)
- ・ 処理者:管理者のために個人データを処理する自然人又は法人 (5条7項)

越境移転規制の内容詳細

以下のいずれかの要件を満たす場合にのみ、越境移転が可能 (33-36条)

- ① 移転先国・国際機関において、LGPDと同程度の個人データ保護制度が定められている場合¹
- ② 規定された原則やデータ主体の権利、及び情報保護体制を確実に順守することを、以下の形式で管理者が保証・証明する場合
 - a. 特定の移転に関する特定の契約条項
 - b. 標準契約条項
 - c. 拘束的企業準則
 - d. シール、証明書及び行動規範
- ③ 国際司法共助のために必要である場合
- ④ 所有者又は第三者の生命・身体の安全のために必要である場合
- ⑤ データ保護局 (Autoridade Nacional de Proteção de Dados: ANPD) が移転を承認した場合

1. ANPDが対象国のデータ保護レベルを評価する (すなわち十分性認定をおこなう) と規程されている (34条)

- ⑥ 国際協定等で合意された約束に基づき必要である場合
- ⑦ 公共政策又はサービスの実施に必要である場合
- ⑧ 本人同意
(ただし、移転の国際的な性質に関する事前の情報共有及び他の目的と独立した同意である場合に限る)
- ⑨ 法令上の管理者の義務の順守のために必要である場合
- ⑩ データ主体の要請に従い、データ主体を当事者とする契約の締結・履行及び準備に必要な場合
- ⑪ 司法・行政手続きにおける通常の権利行使のために必要である場合

ローカライゼーション規制

対象法令

該当法令なし



移転先に「同等」もしくは「十分な」保護水準を求める国/地域 (1/5)



日本

越境移転規制

対象法令

個人情報保護法 (Act on the Protection of Personal Information: APPI)

- 2003年公布、2005年施行
- 2015年改正、2017年施行
- 2020年改正、2022年施行

越境移転の対象となるデータ

他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む特定の個人を識別することができる情報 (2条1項)

越境移転規制の対象者

個人情報取扱事業者: 個人情報を含むデータベース等を事業の用に供している者。ただし、国の機関、地方公共団体、独立行政法人等を除く (16条2項)

越境移転規制の内容詳細

以下の要件のいずれかの要件を満たす場合のみ、越境移転が可能 (28条1項)

- ① 本人の同意
- ② 移転先国が、個人情報保護委員会規則で定める我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国であること
- ③ 移転先事業者が個人情報保護委員会規則で定めるプライバシー保護に関する基準に適合する体制を整備した事業者であること

ローカライゼーション規制

対象法令

該当法令なし



ニュージーランド

越境移転規制

対象法令

プライバシー法 (Privacy Act 2020)

- 2020年施行

プライバシー法の対象者は、IPP (Information Privacy Principles: 情報プライバシー原則) を遵守する必要がある。なお、IPPの内容はプライバシー法の22条に盛り込まれている。

越境移転の対象となるデータ

死亡に関する情報を含む識別可能な個人に関する情報 (7条)

越境移転規制の対象者

国内および海外の事業者で、国内での登記の有無は問わない (1条)

越境移転規制の内容詳細

以下のいずれかの要件を満たす場合にのみ、越境移転が可能 (22条 IPP12)

- ① 移転先がプライバシー法に定める保護措置と同等の保護措置を提供しない可能性がある旨をデータ主体に通知した上で移転に関する同意を取得している場合
- ② 移転先にプライバシー法における情報保護措置と同等の義務が課される場合
- ③ データの保管又は処理をおこなう第三者へ送信される場合
- ④ 政府が自国と同等の保護措置を持つと認めた国の移転先への開示
- ⑤ その他例外事項に該当する場合
移転先がプライバシー法の適用対象である場合、公の情報である場合 等

ローカライゼーション規制

対象法令

該当法令なし



移転先に「同等」もしくは「十分な」保護水準を求める国/地域 (2/5)

オーストラリア

越境移転規制

オーストラリアにおける個人データ保護規制は、包括法であるAPAと個別法から成る。特定の事業別に個人データの取扱いについて定めた規制 (Spam Act 2003等) が存在するほか、いくつかの州法にも個人データ規定が含まれる。ここでは、オーストラリアの主要な個人データ保護規制であるAPAを紹介する。
なお、ニュージーランド同様、APAの対象者は、APP (Australian Privacy Principles: オーストラリア プライバシー原則) を遵守する必要があり、その内容はAPA内に盛り込まれている。

対象法令

連邦プライバシー法 (Australia Privacy Act 1988: APA)

- 1988年の初版以降、何度も細かな改正を重ねており、2022年に最新版を施行

越境移転の対象となるデータ

特定の個人又は合理的に特定可能な個人に関する情報又は意見であり、その真偽や有体物への記録有無は問わない (6条)

越境移転規制の対象者

年間売上が300万豪ドル以上のすべてのAPP事業者 (6条D項)

- なお、APP事業者には、民間組織 (自然人、法人、団体等)、連邦政府機関が含まれる (6条C項)

越境移転規制の内容詳細

- 移転先がAPPに違反しないための合理的な措置が設置された場合にのみ、越境移転が可能 (Schedule1 8.1条)
- ただし、以下の場合は、例外が認められる (Schedule1 8.2条)
 - ① 移転先がAPPと類似する個人データ保護制度・ツールの対象となっている場合
 - ② APP8.1項が適用されなくなる旨の明示と本人同意
 - ③ オーストラリア法又は裁判所/審判所で認められる場合
 - ④ 生命、健康又は安全に対する渋滞な脅威の緩和・予防に必要である場合
 - ⑤ 違法行為又はその疑いに対する措置を講じるために必要である場合
 - ⑥ 行方不明者の発見のために必要な場合

ローカライゼーション規制

対象法令

該当法令なし



移転先に「同等」もしくは「十分な」保護水準を求める国/地域 (3/5)



越境移転規制

対象法令

- 個人データ保護法 (Personal Data Protection Act, B.E. 2562: PDPA)
- 2019年一部施行、2022年完全施行

タイのPDPAについては、PDPC (Personal Data Protection Committee: 個人データ保護委員会) が下位規則で詳細を定めることが予定されている。しかしながら、2022年9月時点で該当する下位規則が制定されていないため、ここではPDPAで規定された越境移転規制の内容のみを紹介する。

越境移転の対象となるデータ

個人に関する情報で、直接又は間接を問わず、当該個人を特定することのできる情報で、故人に関する情報は含まない (6条)

越境移転規制の対象者

- 管理者: 個人データの収集、利用又は開示に関する決定権及び義務を有する個人又は法人 (6条)
 - 処理者: 管理者でない者であって、管理者の命令に従って、個人データの収集、利用又は開示に関して業務をおこなう個人又は法人 (6条)
- ※ なお、国内にいるデータ主体に対するサービス提供等をおこなう場合には、国外の管理者及び処理者も規制の対象となる (5条2項)

越境移転規制の内容詳細

越境移転は原則禁止されるが、以下の要件をすべて満たす場合、越境移転が可能 (28条)

- 移転先の国又は地域が、個人データ保護について「十分な水準」を満たしている
- PDPCが定める規則に従って移転がおこなわれる。ただし、以下のいずれかの要件を満たす場合には、越境移転が可能 (28-29条)
 - ① 以下の例外事由に該当する場合 (28条)
 - a. 法令による場合
 - b. 移転先が十分な個人データ保護措置を有していないことを通知したうえで、データ主体の本人同意を得た場合
 - c. データ主体が当事者である契約の履行のために必要な場合、又は契約の締結前にデータ主体の依頼に応じた措置を講じる必要がある場合
 - d. データ主体の利益のために管理者と他の個人又は法人との間で契約を遵守する必要がある場合
 - e. データ主体又はその他の生命、身体又は健康被害を防止・抑制するためであり、その時点でデータ主体の本人同意を取得できない場合
 - f. 重大な公共に基づく利益に関して活動をおこなうために必要な場合
 - ② グループ事業者間での移転であり、当事者間で個人データ保護委員会が承認する情報保護ポリシーを設けている場合 (29条)

ローライゼーション規制

対象法令

該当法令なし



移転先に「同等」もしくは「十分な」保護水準を求める国/地域 (4/5)

南アフリカ

越境移転規制

対象法令

- 個人情報保護法 (Protection of Personal Information Act: PoPIA)
- 2013年一部施行、2021年完全施行

越境移転の対象となるデータ

生存する識別可能な自然人、及び、該当する場合は存在する識別可能な法人から収集された個人情報 (1条)

越境移転規制の対象者

- 責任ある当事者: 単独又は他者と共同して個人情報の処理の目的及び手段を決定する公的又は私的な団体、又はその他の者 (1条)
- 処理者: 契約又は委任に基づき、責任ある当事者のために、その当事者の直接的な権限に属せずに個人情報を処理する者 (1条)

越境移転規制の内容詳細

以下のいずれかの要件を満たす場合のみ、越境移転が可能 (72条)

- ① 移転先が、適切な水準の個人データの保護措置を提供する法律、拘束力のある企業規則や契約の適用を受ける場合
- ② 本人同意
- ③ データ主体と当事者間の契約の履行又はデータ主体の要請に応じた対策に必要な場合
- ④ 当事者と第三者の間に締結されたデータ主体の利益に関する契約の履行に必要な場合
- ⑤ データ主体の利益に必要、且つ本人同意の取得が合理的に不可能である場合

ローカライゼーション規制

対象法令

該当法令なし



移転先に「同等」もしくは「十分な」保護水準を求める国/地域 (5/5)



メキシコ

越境移転規制

対象法令

- 民間保有個人データ保護法
(Ley Federal de Protección de Datos Personales en Posesión de los Particulares)
- 2010年施行

越境移転の対象となるデータ

識別された又は識別可能な自然人に関するあらゆる情報 (3条5項)

越境移転規制の対象者

- 管理者: 個人データの処理を決定する私的な性質を持つ自然人又は法人 (3条14項)
- 処理者: 単独又は他者と共同で管理者に代わり処理をおこなう自然人又は法人 (3条9項)
- 第三者: 管理者又は管理者以外の自然人又は法人で、国内外を問わない (3条16項)

越境移転規制の内容詳細

- 国内外を問わず、以下のすべての要件を満たす場合のみ、越境移転が可能 (36条)
 - 本人同意の取得
 - 国内外の第三者は管理者と同様の義務を負う
- ただし、以下の例外事由に該当する場合には、① 本人同意の取得 は不要となる (37条)
 - 法令又は条約に規定されている場合
 - 同一グループ内での移転の場合
 - 管理者とデータ主体又は移転先 (第三者) と法的関係の維持、契約に必要な場合
 - その他: 医療サービス、公共の利益、司法手続きに必要な場合

ローカライゼーション規制

対象法令

該当法令なし

1. 対象国は個人データ保護委員会 (Data Protection Board: DPB) が審査・決定する

Source: [LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES](#); [Personal Data Protection Authority "Personal Data Protection Law"](#)



トルコ

越境移転規制

対象法令

- 個人データ保護法 (Law on Protection of Personal Data: LPPD)
- 2016年施行

越境移転の対象となるデータ

識別された又は識別可能な自然人に関するあらゆる情報 (3条)

越境移転規制の対象者

- データ管理者: 個人データの処理の目的及び手段を決定し、システムの構築及び管理に責任を負う自然人又は法人 (3条)
- データ処理者: 管理者の承認に基づき、個人データを処理する自然人又は法人 (3条)

越境移転規制の内容詳細

- 本人の明示的同意がある場合にのみ、越境移転が可能 (9条1項)
- ただし、処理の例外事由 (5条2項及び6条3項) に該当し、且つ、以下のいずれかの要件を満たす場合には、本人同意なしでの越境移転が可能となる (9条2項)
 - 移転先国が適切な個人データ保護措置を提供している場合¹
 - 国内外の管理者が適切な保護を提供することを書面で確認し、DPBが承認した場合

ローカライゼーション規制

対象法令

該当法令なし



ローカライゼーション規制を持つ国/地域 (1/10)



中国

越境移転規制

対象法令①

- 個人情報保護法 (Personal Information Protection Law: PIPL)
- 2011年施行

越境移転の対象となるデータ

電子的又はその他の方法で記録された、識別された又は識別可能な自然人に関するあらゆる種類の匿名化されていない情報 (4条)

越境移転規制の対象者

- 処理者: 個人情報の取扱いにおいて、その目的及び方法を独自に決定する組織又は個人 (73条1項)

越境移転規制の内容詳細

本人同意の取得 (39条) に加えて、以下のいずれかの要件を満たす場合には、越境移転が可能 (38条)

- ① 国家インターネット情報部門による安全評価への合格
- ② 国家インターネット情報部門による認証
- ③ 移転先事業者との間での標準契約の締結
- ④ その他法令 (国際条約等) への準拠

対象法令②

- サイバーセキュリティ法 (Cyber Security Law: CSL)
- 2017年施行

越境移転の対象となるデータ

- 個人情報: 電子データその他の方式により記録され、単独またはその他の情報と組み合わせて自然人の身分を識別可能な各種情報 (76条5項)
- 重要データ

越境移転規制の対象者

重要データインフラ運営者 (37条)

越境移転規制の内容詳細

業務の必要性により、国外提供が必要となる場合には、安全評価を行わなければならない (37条)



ローライゼーション規制を持つ国/地域 (2/10)

中国 (続き)

(続き) 越境移転規制

対象法令③

- データセキュリティ法 (Data Security Law: DSL)
 - 2021年施行

越境移転の対象となるデータ

- 国家の安全と利益の保護及び国際的な義務の履行に関連する管理品目に属するデータ (以下、管理品目に属するデータ)
- 重要データ

越境移転規制の対象者

データの種別により、規制の内容が異なる

- 管理品目に属するデータ: 処理者
- 重要データ: 重要データインフラ運営者、その他の処理者

越境移転規制の内容詳細

データの種別により、規制の内容が異なる

- 管理品目に属するデータ: 輸出管理の実施 (25条)
- 重要データ: 対象者の種別により、規制の内容が異なる
 - 重要データインフラ運営者: サイバーセキュリティ法に準拠 (31条)
 - その他の処理者: 国家ネットワーク部門が関係部門とともに制定する弁法に従う (31条)

ローライゼーション規制

対象法令①

- 個人情報保護法 (Personal Information Protection Law: PIPL)
 - 2011年施行

越境移転の対象となるデータ

電子的又はその他の方法で記録された、識別された又は識別可能な自然人に関するあらゆる種類の匿名化されていない情報 (4条)

越境移転規制の対象者

- 国家機関
- 重要データインフラ運営者
- 国家インターネット情報部門によって定められた数を超える個人情報を処理する処理者
- 国内に保管されている個人情報を外国の司法機関又は法執行機関に提供する処理者

越境移転規制の内容詳細

- 個人情報は、原則、国内保存。以下の場合にのみ、越境移転が可能
 - 国家機関/重要データインフラ運営者/一定以上のデータを扱う処理者: 安全評価への合格を得た場合にのみ、越境移転が可能
 - 個人情報を外国機関に提供する処理者: 所管官庁の承認を得た場合にのみ、越境移転が可能



ローカライゼーション規制を持つ国/地域 (3/10)

中国 (続き)

(続き) ローカライゼーション規制

対象法令②

- サイバーセキュリティ法 (Cyber Security Law: CSL)
 - 2017年施行

越境移転の対象となるデータ

- 個人情報: 電子データその他の方式により記録され、単独またはその他の情報と組み合わせて自然人の身分を識別可能な各種情報 (76条5項)
- 重要データ

越境移転規制の対象者

重要データインフラ運営者 (37条)

越境移転規制の内容詳細

重要データインフラ運営者は、国内で収集した重要データ及び個人データは、国内で保存しなければならない (37条)

対象法令③

- データセキュリティ法 (Data Security Law: DSL)
 - 2021年施行

越境移転の対象となるデータ

- 重要データ
 - ※ ただし、次項で示す国内の組織又は個人に関しては、規制対象のデータに関して特段の記載が存在しない

越境移転規制の対象者

- 重要データインフラ運営者 (31条)
- その他の処理者 (31条)
- 国内の組織又は個人 (36条)

越境移転規制の内容詳細

規制対象者により、規制の内容が異なる

- 重要データインフラ運営者: サイバーセキュリティ法に準拠 (31条)
- その他の処理者: 国家ネットワーク部門が関係部門とともに制定する弁法に従う (31条)
- 国内の組織又は個人: 国外の政府機関への提供にあたっては、所管官庁の認可が必要 (36条)



ローカライゼーション規制を持つ国/地域 (4/10)



ロシア

越境移転規制

対象法令

ロシア連邦法第152-FZ号「個人データについて」

(Federal Law on Personal Data (no.152-FZ): ロシア連邦法第152-FZ号)

- 2006年施行

越境移転の対象となるデータ

特定の、又は識別可能な個人に直接的又は間接的に関連する情報 (3条1項)

越境移転規制の対象者

管理者

- 国家機関、自治体、法人又は民間企業で、単独又は他と共同で、個人データを処理し、その目的を決定する者 (3条2項)

越境移転規制の内容詳細

以下のいずれかの要件を満たす場合にのみ、越境移転が可能 (12条)

- ① 移転先国が欧州108号条約 (1980年) に加盟している場合
- ② 通信・情報技術・マスコミ監督庁が、移転先国が適切な個人データ保護が実施していることを認めた場合
- ③ 本人同意
- ④ ロシアが締結する国際協定での規定がある場合
- ⑤ 国家安全保障等のために必要な場合
- ⑥ データ主体が当事者となっている契約の履行を目的とする場合
- ⑦ データ主体又はその他の生命、健康又はその他の重要な利益を保護するために必要且つ、データ主体の書面による同意を得ることが不可能な場合

ローカライゼーション規制

対象法令

連邦法第152-FZ号「個人データについて」

(Federal Law on Personal Data (no.152-FZ): ロシア連邦法第152-FZ号)

- 2006年施行

越境移転の対象となるデータ

特定の、又は識別可能な個人に直接的又は間接的に関連する情報 (3条1項)

越境移転規制の対象者

管理者

- 国家機関、自治体、法人又は民間企業で、単独又は他と共同で、個人データを処理し、その目的を決定する者 (18条5項)

越境移転規制の内容詳細

インターネットを含む情報通信ネットワークを通じて個人データを収集する場合、管理者は、以下を除き、国内にあるデータベースを使用する義務を負う (18条5項)

- ① 国際協定又は法律で規定された目的を達成するために必要である場合
- ② 管理者が法律で課せられた機能、権限、義務の行使及び履行のためにデータの処理が必要である場合
- ③ 裁判手続きへの関与に関して、データの処理がおこなわれる場合
- ④ 国家行政機関及び自治体サービスのためにデータの処理が行われる場合
- ⑤ 創造的活動の目的を達成するために必要な個人データの処理が行われる場合



ローカライゼーション規制を持つ国/地域 (5/10)

インドネシア

越境移転規制

対象法令①

2016年規則

(Minister of Communications and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System: 電子システムにおける個人データ保護に関する2016年通信情報省規則20号)

- 2016年施行

越境移転の対象となるデータ

保管及び管理された一定の個人データであって、その秘密性が保護されなくてはならない情報 (1条1項)

越境移転規制の対象者

電子システム提供者

- なお、電子システム提供者とは、サービス利用者等のニーズのために、単独または他者と共同で電子システムを提供、管理、運用する個人、事業体及び組織を指す (1条6項)

越境移転規制の内容詳細

情報通信大臣との連携によって、越境移転が可能 (22条1項)。なお、連携の内容は以下を指す (22条2項)

- ① 移転先国、移転の相手方、移転日、移転理由、実施計画の報告
- ② 必要に応じた支援の要請
- ③ 移転結果の報告の実施義務

対象法令②

個人データ保護法 (Personal Data Protection Act: PDPA)

- 2022年制定

越境移転の対象となるデータ

電子又は非電子システムを介して直接的又は間接的に識別された又は識別可能な個人に関する情報 (1条1項)

越境移転規制の対象者

管理者 (49条)

越境移転規制の内容詳細

以下の要件のいずれかを満たす場合にのみ、越境移転が可能 (49条)

- ① 移転先国が同国と同等以上の個人データ保護制度を保有する場合
- ② 移転先国間との国家間同意がある場合
- ③ 移転元・移転先間でのデータ処理に関する契約の締結がある場合
- ④ 本人同意

長らく検討されていたインドネシアの個人データに関する包括法 (PDPA) が2022年9月20日に批准された。今後、2年の猶予期間を経て、適用される予定となっている¹。
なお、越境移転 (49条) を含め、詳細は、下位規則により今後規定される予定。

1. Hunton Andrews Kurth "Indonesia Enacts its First Data Protection Act" 2022

Source: Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016; Undang-undang Perlindungan Data Pribadi (Rancangan UU PDP Final)



ローカライゼーション規制を持つ国/地域 (6/10)

インドネシア (続き)

ローカライゼーション規制

対象法令

- 電子システム及び電子取引の実施に関する2019年政令71号
(Government Regulation No.71 of 2019 on the Administration of Electronic Systems and Transactions: 2019年政令)
- 2019年施行

越境移転の対象となるデータ

特にローカライゼーション規制の対象となるデータに関する記述はない

越境移転規制の対象者

公共部門の電子システム提供者 (20条2項)

越境移転規制の内容詳細

- 公共部門の電子システム提供者は、電子システム及び電子データについて、インドネシア国内で管理、処理又は保存する義務を負う (20条2項)
- ただし、国内で該当する保管技術が利用不可であると委員会が認めた場合には、国外での保存が認められる (20条3-4項)

韓国

越境移転規制

対象法令①

- 個人情報保護法 (Personal Information Protection Act: PIPA)
- 2020年施行

越境移転の対象となるデータ

生存する個人に関する情報であって、識別された又は識別可能な情報。他の情報と容易に結合して個人が特定できる情報、仮名情報を含む (2条1項)

越境移転規制の対象者

個人情報処理者

- 業務を目的として、個人情報を運用するために、自ら又は他人を通じて個人情報を処理する公共機関、法人、団体及び個人 (2条5項)

越境移転規制の内容詳細

以下のすべての項目をデータ主体に通知のうえ、本人の同意を取得した場合にのみ、越境移転が可能 (17条2項)

- ① 個人情報の利用目的
- ② 移転する個人情報項目
- ③ 個人情報の利用及び保管期間
- ④ 同意を拒否する権利の存在及びそれによる不利益の有無とその詳細の説明



ローカライゼーション規制を持つ国/地域 (7/10)

韓国 (続き)

(続き) 越境移転規制

対象法令②

情報通信網利用促進及び情報保護等に関する法律

(Act on Promotion of Information and Communications Network Utilization and Information Protection: 情報通信網法)

- 1987年初版施行後、頻繁に改正を繰り返し、最新版は2020年改正版 (2021年施行)

越境移転の対象となるデータ

重要データ

- なお、重要データとは以下のような情報を指す (51条1項)
 - ① 国家安全保障に関連した保安情報及び主要政策に関する情報
 - ② 国内で開発された先端科学技術又は機器の内容に関する情報

越境移転規制の対象者

- 情報通信サービス提供者
- 情報通信サービス利用者

越境移転規制の内容詳細

以下すべての要件を満たす場合にのみ、重要データの国外移転が可能 (51条3項)

- ① 情報通信網の不当な利用を防止することができる制度的・技術的措置の設定
- ② 情報の不法破壊又は不法操作を防止することができる制度的・技術的措置の設定
- ③ 情報通信サービス提供者が、情報の取扱中に知り得た重要情報の漏洩を防止することができる措置

ローカライゼーション規制

対象法令

該当法令なし

データの国内保存を求める包括法は存在しないが、一部個別法にて、特定の場合に国内保存が求められる¹

- 行政機関及び公共機関に対してクラウドサービスを提供する場合
- 韓国国内に本店を置く金融機関の電算室、災害復旧センターの場合
- 医療機関が電子カルテシステムとそのバックアップ装置を外部で管理・補完する場合

1. JETRO「電子商取引の「TPP3原則」と中国・韓国の法制度の比較」2019年

Source: [Act on Promotion of Information and Communications Network Utilization and Information Protection](#)



ローカライゼーション規制を持つ国/地域 (8/10)



ベトナム

越境移転規制

現時点では越境移転規制が存在しないため、参考までに現在検討中の草案を紹介する

参考) 対象法令

- 個人データ保護規制政令案 (Draft Decree on Personal Data Protection: PDPD草案)
- 2021年意見募集

越境移転の対象となるデータ

個人に関する情報、又は特定の個人を識別可能な情報 (2条1項)

越境移転規制の対象者

国内で事業を営む国内外のすべての機関、組織及び個人 (1条1項)

越境移転規制の内容詳細

- 原則的には、以下の要件をすべて満たす場合にのみ、越境移転が可能 (21条1-2項)
 - ① 本人同意の取得
 - ② オリジナルデータの国内保存
 - ③ 移転先が、自国と同等又はそれ以上の水準の保護制度を有していることの証明
 - ④ 個人データ保護委員会による書面承認の取得
- 以下の①-④いずれか及び⑤⑥を満たせば、越境移転が認められる可能性がある (21条3-5項)
 - ① 本人同意の取得
 - ② 個人データ保護委員会による書面承認の取得
 - ③ 個人データ保護に関する処理者のコミットメント
 - ④ 処理者による個人データ保護措置を適用することへのコミットメント
 - ⑤ 移転元における移転履歴の保存システムの構築 (3年)
 - ⑥ 移転元における個人データ保護委員会による年1回の定期評価の実施

ローカライゼーション規制

対象法令①

- サイバーセキュリティ法 (Law on Cyber Security)
- 2019年施行

ローカライゼーション規制の対象となるデータ

個人データ又はサービス利用者の関係に関するデータ、又は国内サービス利用者によって作成されたデータ (26条3項)

ローカライゼーション規制の対象者

国内での通信ネットワーク、インターネット及びサイバースペース上のサービス又は付加サービスを提供する国内外の事業者 (26条3項)

ローカライゼーション規制の内容詳細

- 該当のデータを取扱う場合には、一定期間、国内に保存しなければならない (26条3項)
- 要件を満たす国外の事業者は、国内に駐在所又は支店を設定する義務を負う (26条3項)

対象法令②

- インターネットサービスに関する政令 (Decree No.72/2013/ND-CP)
- 2013年施行

ローカライゼーション規制の対象となるデータ

インターネット サービス、オンライン情報、オンライン ゲームに関する情報

ローカライゼーション規制の対象者

オンラインサービス事業者 (24-25条、28条)

ローカライゼーション規制の内容詳細

- 管轄当局の要求に応じて情報の検査、保管、提供、およびサービス提供に関する顧客の苦情の解決を行うため、少なくとも1 台のサーバーシステムをベトナムに設置する義務を負う (24-25条、28条)



ローカライゼーション規制を持つ国/地域 (9/10)



インド

越境移転規制

対象法令

該当法令なし

- 2011年IT規則 (Information Technology Rules 2011) に一部規定があるが、2000年IT法 (Information Technology Act 2000) に基づく施行細則であり、データ移転一般について、「法人または法人に代わる者と情報提供者との間の合法的な契約の履行に必要な場合、または当該者がデータ移転に同意している場合にのみ許可」と規定するに留まる (7条)

インド初の個人データに関する包括法として、PDPB (Personal Data Protection Bill 2019: 2019年個人データ保護法案) が上程され、審議がおこなわれていた。GDPRをベースとした2018年草案を経て作成されており、より厳格且つ広範な個人データ規定となることが期待されていたが、2022年8月、白紙撤回され、新法案を提出する予定となった¹

ローカライゼーション規制

対象法令①

支払システム情報の保存に関する政令 (DL規則)

- 2018年

ローカライゼーション規制の対象となるデータ

支払いメッセージ/指示の一部として収集/送信/処理される支払いまたは決済トランザクションに関するエンドツーエンドのトランザクションの詳細と情報 (2条1項)

ローカライゼーション規制の対象者

インド中央銀行 (Reserve Bank of India: RBI) が承認したすべての支払いシステム提供者

ローカライゼーション規制の内容詳細

全ての支払いシステム提供者は、自身が運営するシステムに関連するすべてのデータをインドのシステムにのみ保存することを保障しなければならない (2条1項)

対象法令②

統一ライセンス法

ローカライゼーション規制の対象となるデータ

国際ローミング及び請求書を除く、利用者のあらゆる財務及び利用者情報 (39.23条8項)

ローカライゼーション規制の対象者

ライセンスを受けた電気通信サービス事業者

ローカライゼーション規制の内容詳細

情報の国外への移転禁止 (39.23条8項)

1. TMI総合法律事務所「インド最新法令情報- (2022年8月号) インド個人情報保護法案の白紙撤回」2022年



ローカライゼーション規制を持つ国/地域 (10/10)

サウジアラビア

越境移転規制

対象法令

- 個人データ保護法 (Personal Data Protection Law: PDPL)
- 2022年公布、2023年3月発効予定

越境移転の対象となるデータ

個人の特定につながる、または直接的または間接的に個人を特定できるすべての情報 (1条)

越境移転規制の対象者

管理者 (1条)

越境移転規制の内容詳細

- データ主体の生命又は重大な利益の保護、及び感染予防・治療等に必要である場合のみ越境移転が可能 (29条)
- ただし、国を当事者とする契約に基づく義務の履行、又は、国益のため、規則で定められた他の目的のためである場合、以下のすべての要件を満たせば、越境移転が可能 (29条) (管轄当局が認めた場合、①以外のいずれかの要件は免除される可能性がある)
 - ① 移転・開示により国家安全保障又は国の重大利益を損なわれない場合
 - ② 個人データの気密性の維持のために法律及び規則で定められた手順を下回らない十分な保証の提供がある場合
 - ③ 移転・開示される個人データが必要最低限である場合
 - ④ 管轄当局による承認がある場合

ローカライゼーション規制

対象法令

該当法令なし

ローカライゼーションに関する規制は存在しないが、越境移転が認められる要件が、相当に限定的な状況となるため、実質的には国内保存が基本となる¹



越境移転/ローライゼーション規制を持たない国/地域 (1/3)



カナダ

越境移転規制

対象法令

個人情報保護及び電子文書法

(Personal Information Protection and Electronic Documents Act: PIPEDA)

- 2000年制定、2004年完全施行
- 頻繁に修正・改正が行われ、最新版は2019年版

越境移転の対象となるデータ

識別可能な個人に関する情報 (2条1項)

越境移転規制の対象者

個人情報を取扱うすべての民間組織 (4条1項) で、以下の組織を除く (4条2項)

- プライバシー法が適用される政府機関
- 私的目的で個人情報を収集、利用、開示する個人
- ジャーナリズム、芸術又は文学目的のみで個人情報を収集、利用又は開示する組織

越境移転規制の内容詳細

- PIPEDAには国内外を問わない個人情報の取扱いについて定めており、越境移転そのものに関する規定を持たない
- したがって、一般的に個人情報の越境移転が認められるが、越境移転をおこなう場合にも、PIPEDAに定められる個人情報の移転に関する一般規定が適用されることとなる
- 個人情報保護に関しては、PIPEDA Schedule1に示される個人情報保護原則 (Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96: 個人情報保護のためのモデルコードCAN/CSA-Q830-96に定められた原則) に取扱い原則が定められており、越境を含む移転でも本原則の遵守が必須

<個人データ保護原則>

① 説明責任

- 諸原則の遵守を監視するプライバシー保護の責任者の指名
- 第三者の処理に関する契約又は他の手段による同等の保護レベルの保証・提供
- 個人情報の保護手順を整備及び実務による原則の実現

② 目的の特定

- 個人情報の収集目的の特定・明確化
- 目的の通知 (特定した目的以外で利用する場合は再通知・同意が必要)

③ 同意

- 個人情報の収集、利用又は開示に対するデータ主体の「認識及び同意」の取得
- 製品またはサービスの提供条件としての個人情報の収集、利用又は開示への同意の取得の禁止

④ 制限的収集

- 組織が特定した目的に必要な範囲での個人情報収集の限定
- 適切且つ適法な手段による収集

⑤ 制限的利用、開示及び保持

- 収集目的外での利用又は開示の禁止 (個人の同意又は法に基づく場合を除く)
- 不要となった個人情報の破棄、消去又は匿名化

⑥ 正確性

- 利用目的に必要な範囲での個人情報の正確、完全且つ最新な状態の維持

⑦ 安全保護

- データの機微性に適した安全保護措置の実施 (物理的、組織的及び技術的措置を含む)



越境移転/ローライゼーション規制を持たない国/地域 (2/3)

カナダ (続き)

(続き) 越境移転規制

- ⑧ 公開
 - ・ 個人情報の管理に関する方針及び実務に関する情報に対する容易なアクセスの確保
- ⑨ 個人のアクセス
 - ・ 個人によるデータへのアクセス、情報の訂正の要求及び要求に対する組織の対応責任
- ⑩ 遵守
 - ・ 諸原則の遵守に関する問題に対応する遵守責任者の設置
 - ・ 苦情処理手順の設置

カナダは、個人データ保護は、長らく個別/分野法によて規定され¹、2000年のPIPEDAでようやく包括的な民間部門の個人情報保護法が成立した。そのため、カナダでは、カナダ規格協会による個人データ保護に関するモデルコード CAN/CSA-Q830-96 が法律に先行。そこで、包括法の整備に際して、カナダでは先行していた CAN/CSA-Q830-96を同法に取り込むという特殊な方法を採用し、個人情報保護原則を整備した。

ローライゼーション規制

対象法令

該当法令なし

台湾

越境移転規制

対象法令

個人データ保護法 (Personal Data Protection Act: PDPA)
- 2016年

越境移転の対象となるデータ

氏名、生年月日等、自然人を直接又は間接的に識別することができるあらゆる情報 (2条1項)

越境移転規制の対象者

自然人、法人又は団体等の非政府機関 (2条8項)

越境移転規制の内容詳細

個人データの越境移転は、一般的に許可されるが、以下の場合、当局は移転に制限を課することができる (21条)

- ① 主要な国益が関与する場合
- ② 国際条約又は協定に規定されている場合
- ③ 移転先国が個人データ保護に関する適切な規制を持たず、データ主体の権利と利益が損なわれる可能性がある場合
- ④ 第三国 (地域) への転送がPDPAに基づく制限を回避することである場合

ローライゼーション規制

対象法令

該当法令なし

1. PIPEDAと「実質的に類似」しているとみなされた州法を持つ場合、PIPEDAではなく州法の適用が認められる。2020年5月時点では、3州の民間部門のプライバシー法及び健康情報に関する4州の州法が「実質的に類似」と認められている (Office of the Privacy Commissioner of Canada "Provincial laws that may apply instead of PIPEDA")

Source: [Government of Canada "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96"](#); [Office of the Privacy Commissioner of Canada "Guidelines for processing personal data across borders"](#); [Personal Data Protection Act](#)



越境移転/ローカライゼーション規制を持たない国/地域 (3/3)

アメリカ

越境移転規制

対象法令
該当法令なし

ローカライゼーション規制

対象法令
該当法令なし

フィリピン

越境移転規制/ローカライゼーション規制

対象法令
該当法令なし




ローカライゼーション規制

対象法令
該当法令なし



調査結果詳細：国際ルール

次ページ以降で以下の詳細を記載

	名称	対象国・地域	発効年
規制	 ① 主要国/地域における越境移転/ローカライゼーション規制	EU、米国、日本等 22カ国/地域	—
国際ルール	 ① OECDプライバシーガイドライン (OECD Guidelines governing the protection of privacy and transborder flows of personal data)	OECD (経済協力機構) 加盟国	1980年 (2013年改訂)
	② 個人データの自動処理に係る個人の保護に関する条約 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: 欧州評議会条約第108号)	55カ国 (欧州評議会メンバー46カ国及び、 非加盟国9カ国)	1985年 (1999年改訂)
	③ APECプライバシー・フレームワーク (APEC Privacy Framework)	APEC (アジア太平洋協力) 加盟国	2004年 (2016年改訂)
	④ ASEAN 個人データ保護フレームワーク (ASEAN Framework on Personal Data Protection: ASEAN PDPフレームワーク)	ASEAN (東南アジア諸国連合) 加盟国	2016年
貿易協定	 ① サービスの貿易に関する一般協定 (General Agreement on Trade in Services: GATS)	WTO (世界貿易機構) 加盟国	1995年
	② 地域貿易協定 (Regional Trade Agreement: RTA)		
	i) 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 (Comprehensive and Progressive Agreement for Trans-Pacific Partnership: CPTPP)	日本、シンガポール、ベトナム、オーストラリア、 ニュージーランド、カナダ、メキシコ、ペルー	2021年
	ii) 地域的な包括経済連携協定 (Regional Comprehensive Economic Partnership Agreement: RCEP)	ASEAN10カ国、日本、韓国、中国、 オーストラリア、ニュージーランド	2022年



1 OECDプライバシーガイドライン

対象法令と基本方針

OECD加盟国に対しては、越境移転のみならず、プライバシー保護全般について定めたOECDプライバシーガイドラインの履行が求められる。

中核となるOECDプライバシー8原則には、越境移転に関する具体的な言及はないが、これらは個人データの取扱い原則として、越境移転の際にも当然守られるべき原則となっている。

法令の背景

1960年代以降のコンピューターの登場による個人データに対する懸念の高まりは、世界的なデータ保護議論を巻き起こし、1970年代には、一部先進諸国において、プライバシー法の制定が開始された。

それらのデータ保護に対する議論の高まりを受けて、OECDは、1980年に旧OECDプライバシーガイドライン (Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data) を1980年に採択した。この中でOECDは、プライバシー8原則を定めたうえで、加盟国に対して、「国内法での考慮」「プライバシー保護名目で不当に個人データの国際流通を阻害しないこと」「ガイドライン履行への協力」を求め、事実上の世界標準として用いられるに至った。

その後、インターネットの普及に伴い、ネットワーク社会が急速に進展。個人データ保護の問題の変容を受け、「変化する技術、市場及び利用者の行動、デジタル・アイデンティティの重要性の増加」の観点から、OECDはガイドラインの見直し議論を開始。ガイドライン制定30周年を契機に改正の本格議論が開始され、2013年は、改正版が採択された。

規制の詳細

対象範囲

OECDプライバシーガイドラインでは、以下を対象範囲としている。

- 公的部門及び民間部門 (すべてのステークホルダー)

OECDプライバシー8原則

① 収集制限の原則 (Collection Limitation Principle)

個人データの収集には制限を設け、いかなる個人データも、適法且つ公正な手段によって、また、データ主体への通知及びその同意を得て収集されなければならない

② データの質の原則 (Data Quality Principle)

個人データは、目的の範囲内において利用され、且つその目的達成に必要な範囲で、正確、完全、且つ最新のものでなければならない

③ 目的特定化の原則 (Purpose Specification Principle)

個人データの収集目的は、収集前に特定されなければならない、また、事後的な利用は目的達成に必要な範囲内でおこなわなければならない。加えて、その他の目的で利用を行う場合には、毎回その利用目的を特定しなければならない

④ 利用制限の原則 (Use Limitation Principle)

個人データは、データ主体の同意又は法の授權がある場合を除き、提供されてはならない

⑤ 安全保護措置の原則 (Security Safeguard Principle)

個人データは、滅失、棄損、不正アクセス、不正利用や改ざん、漏洩等の危険に対し、合理的な安全措置によって保護されなければならない

⑥ 公開の原則 (Openness Principle)

個人データの活用、取扱い、業務及び方針については公開された一般的な方針がなければならない。また、個人データの存在や性質、その利用目的、及びデータ管理者とその所在地を示されなければならない

⑦ 個人参加の原則 (Individual Participation Principle)

個人は、データ管理者がその個人データを保有しているか否か確認できる権利を有する。又、その管理者に対して、当該データについて、合理的な期間内に必要に応じて妥当な費用で、合理的且つ認識が容易な方法で、伝達することを要求する権利を持つ。なお、それらの要求が拒否された場合には、管理者に対して理由の説明及び意義の申し立てを要求することができる。異議が認められた場合、当該データの消去、訂正、完全化を要求できる。

⑧ 責任の原則 (Accountability Principle)

データ管理者は、各原則を実施するための措置を順守する責任を有する



2 欧州評議会条約第108号

対象法令と基本方針

欧州評議会を中心として、プライバシー保護について定められた規制として、欧州評議会条約第108号が存在する。

法的拘束力を持つ個人データ保護の枠組みとしては、最も古いものの1つとして数えられ、締約国間での越境移転の制限を原則禁止するなど、越境移転についても早くから言及している。

法令の背景

欧州では、1970年代に、欧州人権条約8条 (1953年) を参照しつつ、個人データの保護に関する議論が活発に行われた。議論は、OECD及び非加盟4カ国 (米国、日本、カナダ、オーストラリア) もオブザーバー参加のうえすすめられ、1981年には欧州評議会条約第108号が署名され、1985年に発効した。

欧州評議会条約第108号は、データ保護分野において唯一拘束力がある国際的文書として存在し、リスボン条約に伴う1999年改正、2001年の追加議定書採択 (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows) 等を経て、内容の充実が図られてきた。

2022年9月現在、計55カ国 (加盟46カ国及び非加盟9カ国) が批准しており、近年はさらなる現代化の議論が進められている。

規制の詳細

越境移転の定義

欧州評議会条約第108号12条1項は、越境移転について以下のように定義している

- 自動処理される個人データ又は自動処理される目的で収集された個人データが媒体の如何を問わず国境を越えて移転される場合

規制対象となるデータ

欧州評議会条約第108号は、条約の適用範囲を以下のように定める (3条1項)。

なお、12条1項の記述から、越境移転についても、同様のデータが対象となると解される

- 公的部門及び民間部門における自動処理個人データファイル及び個人データの自動処理

規定の内容

<欧州評議会条約第108号における規定>

欧州評議会条約第108号は、個人データ保護のみを目的とした他の締約国への越境移転の制限を原則禁止している。

ただし、以下のいずれかを満たす場合には、例外的に移転の制限が認められる。

- ① 特別な規定の存在 (条約第108号12条3項a)
特定の個人データ等に対し、データの性質を理由として、その国内法が特別の規定を含んでいる場合、例外的に他の締約国への移転の制限が認められる
ただし、移転先締約国の規定が同等の保護を定めている場合を除く
- ② 非締約国へのデータ移転 (条約第108号12条3項b)
締約国から他の締約国の仲介を経て、非締約国へと移転がおこなわれる場合、当該移転が締約国の法律の適用回避となることを防ぐため、移転の制限が認められる

<追加議定書における規定>

追加議定書2条では、条約の締結国の管轄下でない受領者への個人データの越境流通に関して、以下のように定められている

- ① 十分な保護レベルを保証する条約管轄外の国又は機関への移転 (2条1項)
条約の当事国ではない国又は機関の管轄下にある受領者への個人データの移転について、その国又は機関が十分な保護レベルと保証する場合に限り、おこなうことができる
- ② 例外事由 (2条2項)
以下の場合に、各締約国は、条約管轄外の受領者に対して、個人データの移転を許可することができる
 - a. 以下の理由により国内法で定められる場合
 - データ主体の特定の利益の実現のため
 - 正当且つ優越的な利益、特に重要な公的利益の実現のため
 - b. 契約条項に基づく安全措置が、移転について責任を負う管理者により定められ、関連機関がその措置を国内法に基づき充分であると認めた場合



3 APECプライバシー・フレームワーク

対象法令と基本方針

APEC加盟国には、APECプライバシー・フレームワークの実施が推奨されている。概ねOECDプライバシーガイドラインを踏襲した内容となっており、越境移転に関しては、本人同意の取得と原則の遵守を確保する合理的措置を要求している。

法令の背景

APECでは、1998年閣僚会議の合意を皮切りに個人データ保護の議論を開始し、2004年にAPECプライバシー・フレームワークを策定・承認した。

近年では、特にAPEC域内における個人データの越境移転の整備にも注力しており、2011年にCBPRシステム (APEC Cross Border Privacy Rules System) の運用が開始された。

APECプライバシー・フレームワーク自体も、2016年にアップデートがおこなわれ (改訂APECプライバシー・フレームワーク)、越境移転に関する規定が追加された。

規制の詳細

規制対象となるデータ

「個人データ」を「識別された又は識別可能な個人に関するあらゆる情報」と定めている (9条)

規制対象者

「個人データ管理者」について、「個人データの収集、保有、取扱いをおこなう者又は組織」と定める (10条)。なお、この定義には、他の者又は組織に対し、代理で個人データの収集等をするよう指示する者又は組織は含まれるが、指示される者又は組織は含まれない

APEC情報プライバシー諸原則

① 損害の回避 (Preventing Harm, 14条)

特定の義務は、個人データの不正使用により生じるリスクを考慮すべきであり、救済措置は、情報の収集、使用、移転による損害の可能性と重大性に比例するものでなければならない

② 通知 (Notice, 15-17条)

個人データ管理者は、個人データの収集の事実、目的、開示される第三者の種別、個人データ管理者の名称・所在、個人データの利用・提供の制限及び開示・訂正のための方法を含む個人データに関するポリシー及び体制等を、アクセス可能な方法で提供しなければならない

③ 収集の制限 (Collection Limitation, 18条)

個人データの収集は、目的の範囲内で、適法且つ公正な手段で収集されなければならない

④ 個人データの利用 (Use of Personal Information, 19条)

個人データの利用は、原則として、収集目的及び関連する目的の遂行に限定されなければならない。ただし、① データ主体の同意がある場合、② データ主体空依頼されたサービスや製品の提供のために必要である場合、③ 法令等に基づく場合 には例外が認められる

⑤ 選択の機会 (Choice, 20条)

個人データの収集、利用及び開示に関して個人が選択権を行使するために、明確、且つ、理解及びアクセスが容易な仕組みが提供されなければならない

⑥ 個人データの正確性 (Integrity of Personal Information, 21条)

利用目的に必要な範囲で、個人データは、正確で、完全で、最新でなければならない

⑦ 安全保護措置 (Security Safeguards, 22条)

個人データ管理者は、個人データの滅失、不正アクセスや破壊、利用、変更及び開示等のリスクに対する適切な安全保護措置を整備して、個人データを適切に保護しなければならない

⑧ アクセス及び訂正 (Access and Correction, 23-25条)

個人は、個人データ管理者によるデータ保有を確認することができる。十分な本人確認の後、合理的な方法で、個人データの伝達を受けることができる。情報の正確性に疑義がある場合は、訂正、削除等を要求でき、要求が拒絶された場合、その理由の開示を請求できる

⑨ アカウンタビリティ (Accountability, 26条)

個人データ管理者は、上記の原則を実現する責任を負う。個人データを移転する場合は、国内外を問わず、本人の同意の取得をおこなうか、移転先が上記の原則と同水準の保護を行うことを確保するための合理的な措置を取らなければならない

改訂版における越境移転に関する規定の追加

① 他の加盟エコノミーへの個人データの越境移転の制限回避 (69条)

加盟エコノミーは、以下の場合、越境移転の制限を避けなければならない

- ・ 移転国が、当該フレームワークを実現する法律等を導入している場合
- ・ 当該フレームワークの実現のために、個人データ管理者が実施する執行メカニズム及び適切な措置 (CBPR等) を含む十分な保護措置が存在する場合

② 越境移転の制限のリスク比例 (70条)

越境移転に対するいかなる制限も、想定されるリスクに比例していなければならない。リスクの検討にあたっては、情報の機密性、移転の目的及び状況を考慮しなければならない



4 ASEAN PDPフレームワーク

対象法令と基本方針

ASEAN加盟国に対しては、ASEAN PDPフレームワークで定められた個人データに関する基本原則の各国国内法での実現が推奨されている。
定められた原則自体は、先行するOECDプライバシーガイドラインやAPECプライバシー・フレームワークに類する内容となっており、越境移転に関しても、越境移転の通知、本人同意の事前取得及び原則が求めるレベルの個人データ保護を保証するための措置の実施を要求している。

法令の背景

東南アジア地域の経済成長や諸問題に関する協力を目的とするASEANでは、先行するOECDプライバシーガイドラインやAPECプライバシー・フレームワークをもとに、2016年にASEAN PDPフレームワークを採択した。
ASEAN PDPフレームワークは、先行する2原則同様、個人データ保護に関する基本原則を定めたうえで、加盟国に対して国内法における原則の実施を推奨している。
ASEANでは、PDPフレームワーク採択後も、域内のデータ流通の促進及び成長に向けて、ASEANモデル条項を制定するなど、データ流通の促進に向けた活動を継続している。

規制の詳細

規制対象となるデータ

「ASEANにおける個人データ保護の強化」を目的とするが、「個人データ」の具体的な内容に関する記載はない(1条)

規制対象者

ASEAN加盟国を対象とするが、以下の場合には適用されない(4条)

- ・ 加盟国が特定の地域、個人又は分野を当該原則の適用から除外する場合
- ・ 国家主権、安全保障、公共の安全、公共政策及び適用除外することが適切であると加盟国が考えるすべての政府活動に関連する事項

ASEAN 個人データ保護原則

① 同意、通知、目的 (Consent, Notification, and Purpose、6条a/b)

- ・ 組織は、以下の場合を除き、個人データを収集、使用又は開示してはならない
 - 個人データの収集、使用又は開示の目的が通知され、データ主体が同意する場合
 - 通知又は同意を伴わない収集、利用又は開示が、国内法令に基づき許可又は要求されている場合
- ・ また、組織は、状況から見て適切であると考えられる目的のためにのみ、個人データの収集、使用又は開示することができる

② 個人データの正確性 (Accuracy of Personal Data、6条c)

個人データは、目的に必要な範囲において、正確且つ完全でなければならない

③ 安全保護措置 (Security Safeguards、6条d)

個人データは、紛失、不正なアクセス・収集・利用・開示・複製・修正、破壊、又は同様のリスクから適切に保護されなければならない

④ アクセス及び訂正 (Access and Correction、6条e)

データ主体から要求があった場合、組織は以下の対応をおこなわなければならない

- ・ 保有又は管理する個人データに対するアクセスの合理的な期間内での提供
- ・ 個人データの誤り・欠損の訂正 (国内法令等による規定がある場合はこの限りではない)

⑤ 越境移転 (Transfers to Another Country or Territory、6条f)

越境移転に際しては、越境移転に関する本人同意の事前取得、移転先が当該原則と同レベルの個人データ保護を保証するための妥当な措置の実施を行わなければならない

⑥ データ保管 (Retention、6条g)

法令上又は業務上の目的に照らして、データの保持が不要となった時点で、組織は個人データを含む文書の保持又は個人を特定する手段の中止・削除をおこなわなければならない




⑦ 説明責任 (Accountability、6条h/i)

- ・ 組織は、当該原則を実現するための措置を遵守する責任を負う
- ・ 組織は、要求に応じて、保有又は管理下にある個人データに関するデータ保護方針及び実施内容について、明確且つアクセスが容易な形で情報提供しなければならない。
 - また、組織は、そのデータ保護方針及び実施内容について、組織に問い合わせる方法を提供しなければならない



調査結果詳細：貿易協定

次ページ以降で以下の詳細を記載

	名称	対象国・地域	発効年
規制	 ① 主要国/地域における越境移転/ローカライゼーション規制	EU、米国、日本等 22カ国/地域	—
国際ルール	 ① OECDプライバシーガイドライン (OECD Guidelines governing the protection of privacy and transborder flows of personal data)	OECD (経済協力機構) 加盟国	1980年 (2013年改訂)
	② 個人データの自動処理に係る個人の保護に関する条約 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: 欧州評議会条約第108号)	55カ国 (欧州評議会メンバー46カ国及び、非加盟国9カ国)	1985年 (1999年改訂)
	③ APECプライバシー・フレームワーク (APEC Privacy Framework)	APEC (アジア太平洋協力) 加盟国	2004年 (2016年改訂)
	④ ASEAN 個人データ保護フレームワーク (ASEAN Framework on Personal Data Protection: ASEAN PDPフレームワーク)	ASEAN (東南アジア諸国連合) 加盟国	2016年
貿易協定	 ① サービスの貿易に関する一般協定 (General Agreement on Trade in Services: GATS)	WTO (世界貿易機構) 加盟国	1995年
	② 地域貿易協定 (Regional Trade Agreement: RTA) <ul style="list-style-type: none"> i) 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 (Comprehensive and Progressive Agreement for Trans-Pacific Partnership: CPTPP) 	日本、シンガポール、ベトナム、オーストラリア、ニュージーランド、カナダ、メキシコ、ペルー	2021年
	<ul style="list-style-type: none"> ii) 地域的な包括経済連携協定 (Regional Comprehensive Economic Partnership Agreement: RCEP) 	ASEAN10カ国、日本、韓国、中国、オーストラリア、ニュージーランド	2022年



6 GATS

対象法令と基本方針

WTO加盟国には、GATSが適用される。本協定自体は、個人データ保護を主眼としたものではないが、データ流通は何らかのサービス提供の一環としておこなわれることが多いため、本協定が関連し得る。

主眼が異なるため、越境移転の制限・許可に関する直接的な記述はないが、越境移転規制の内容によっては、GATSが定める義務違反となる可能性がある。

法令の背景

GATSは、WTO協定の一部として、1995年に発行された。

WTO協定には、WTO設立協定 (Marrakesh Agreement Establishing the World Trade Organization: 世界貿易機関を設立するマラケッシュ協定) と附属書1-4が含まれる。WTOの加盟には、WTO設立協定及びGATS (附属書1B) を含む附属書1-3の一括受諾が必要であり、したがって、全WTO加盟国がGATSの適用対象となる。

規制の詳細

適用範囲

- GATSでは、一部義務を除き、各加盟国が約束表で定められた12のサービス分野ごとに、GATS上の義務の受け入れを選択することができる。
- データ流通については、電子計算機及び関連サービス (Computer and Related Services)、電気通信サービス (Telecommunications Services) が関連する

規制対象者

WTO加盟国

GATS上の義務とデータ流通との関連

データ流通に関連するGATS上の義務は、以下の4つ

1) 最恵国待遇義務 (2条)

いずれかの国に与える最も有利な待遇を全加盟国に与えなければならない。なお、最恵国待遇については、各加盟国の選択が認められず、全加盟国に一律に適用される

- したがって、他の加盟国のサービス及びサービス提供者に対して、越境移転規制等によって、均等ではない共創条件を課す場合、本義務違反の可能性が生じ得る

2) 国内規制の合理的実施義務 (6条)

加盟国は、自由化を約束したサービス分野において、一般に適用される加盟国の措置のうち、サービス貿易に影響を及ぼすものが、合理的、客観的かつ公平な態様で実施されることを確保しなければならない

- したがって、加盟国が他の加盟国のサービス及びサービス提供者に対して、合理的ではない態様で越境規制等を適用した場合、本義務違反の問題が生じる可能性がある

3) 市場アクセス義務 (16条)

加盟国は、市場アクセスを約束したサービス分野において、サービス提供者の数やサービスの総算出量の制限をおこなってはならない

- オンラインにおけるデータ処理やデータベースサービスに関して、越境移転規制等を導入した場合、サービス提供者の数の制限等に該当するとみなされる可能性がある

4) 内国民待遇義務 (17条)

他の加盟国のサービス及びサービス提供者に対して、同種の国内サービス及びサービス提供者と比べて不利でない待遇を与えなければならない

- 最恵国待遇義務同様に、越境移転規制等の内容によっては、本義務違反の可能性が生じ得る。特に、国内保存義務は、加盟国内へのサーバー等の設置を義務付けるものであり、他の加盟国のサービス提供者に対する追加負担となることから、本義務違反が生じる可能性がある

GATS上の義務の例外事由

以下の例外事由の要件を満たす場合には、GATS上の義務への抵触・違反は正当化される

- ① 一般的例外 (14条) : 公の秩序維持や、生命又は健康の保護のために必要な措置等
- ② 安全保障例外 (14条の2)



7 RTA

CPTPP

法令の背景と越境移転規制との関連

CPTPPは、環太平洋でモノの関税のみならず、サービス・投資の自由化を進め、さらには知的財産、電子商取引等の幅広い分野でルールを構築することを目的として、2021年に発効した。GATS同様、越境移転を主眼とした協定ではないものの、電子商取引に関する規定の中で、個人データを含むデータ流通に言及している。

規制対象となるデータ

- 特段の記述がない限り、情報一般を規制対象とする
- ただし、「個人データ」とある場合には、「特定された又は特定し得る自然人に関する情報（データを含む）」を指す（14章1条）

規制対象者

- 規制の対象者は一義的には締約国
- なお、越境移転の対象規定（14章11条）で言及される「対象者」は、「対象投資財産」「締約国の投資家」及び「締約国のサービス提供者」を指す（金融機関や金融サービスの提供者は除外）（14章1条）

規制の詳細

- CPTPPは、14章11条で情報の越境移転について定めており、原則、越境移転の規制を禁止している
 - 締約国は、対象者の事業の実施のために行われる場合には、情報（個人データを含む）の電子的手段による国境を超える移転を許可する（14章11条2項）
- ただし、以下の場合は、例外的に規制が認められる
 - 締約国が公共政策の正当な目的を達成するために必要な場合（14章11条3項）
 - GATS14条a-c（一般的例外）で定められる内容に該当する場合（29章1条3項）
 - 安全保障のための例外に該当する場合（29章2条）

RCEP

法令の背景と越境移転規制との関連

RCEPは、締約国・地域における貿易・投資の促進及び、サプライチェーンの効率化に向けた市場アクセスの改善、締約国間での知的財産、電子商取引等の幅広い分野のルールの整備を目的として、2022年に発効した。

GATS、CPTPP等、その他の貿易協定同様、越境移転を主眼とした協定ではないものの、電子商取引に関する規定の中で、個人データを含むデータ流通に言及している

規制対象となるデータ

- 特段の記述がない限り、情報一般を規制対象とする
- ただし、「個人データ」とある場合には、「特定された又は特定し得る自然人に関する情報（データを含む）」を指す（1章1.2条u）

規制対象者

- 規制の対象者は一義的には締約国
- なお、越境移転の対象規定（12章15条）で言及される「対象者」は、「対象投資財産」「締約国の投資家」及び「締約国のサービス提供者」を指す（金融機関や金融サービスの提供者は除外）（12章1条）

規制の詳細

- RCEPもCPTPP同様、越境移転の規制を原則禁止している（12章15条）
 - 締約国は、情報の電子的手段による国境を超える移転が対象者の事業の実施のために行われる場合には、当該移転を妨げてはならない（12章15条2項）
- ただし、以下の場合は、例外的に規制が認められる
 - 締約国が公共政策の正当な目的を達成するために必要と認める場合。ただし、当該措置が恣意的もしくは不当な差別の手段となるような態様又は貿易に対する偽装した制限となるような態様で適用されないことを条件とする（12章15条3項a）
 - 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める場合（12章15条3項b）



2.3

調査結果詳細：越境移転ツール

越境移転ツール 調査対象

調査対象国/地域で採用されている越境移転ツールを中心に調査 (⑤ / ⑫ は詳細調査対象外)

		名称	対象範囲	根拠規制	制度運用開始年
国家単位 	認証 	① 十分性認定/ホワイトリスト	EU/英国→域外 日本→国外 ロシア→国外 トルコ→国外 ベトナム→国外 ブラジル→国外 タイ→国外	一般データ保護規則 (GDPR/UK GDPR) 日本 個人情報保護法 (APPI) ロシア連邦法第152-FZ号 トルコ 個人データ保護法 (DPL) ベトナム 個人データ保護政令案 ブラジル 個人データ保護法 (LGPD) タイ 個人データ保護法 (PDPA)	2016年- 2005年- 2006年 運用実績なし 法案未施行 制度未施行 (詳細未決) 制度未施行 (詳細未決)
	協定 	② 日本EU間補完的ルール ③ TADPF (Trans-Atlantic Data Privacy Framework: 大西洋間データプライバシーフレームワーク)	EU→日本 欧州⇄米国	一般データ保護規則 (GDPR) 一般データ保護規則 (GDPR)	2018年- 制度未施行 (原則合意段階)
企業/ 案件単位 	契約 	④ SCC/MCC (Standard/Model Contractual Clauses: 標準/モデル契約条項)	欧州/英国→域外 中国→国外 ニュージーランド→国外 ASEAN域内 イペロアメリカ諸国内 シンガポール→国外 ブラジル→国外	一般データ保護規則 (GDPR/UK GDPR) 中国 個人情報保護法 (PIPL) プライバシー法 ASEAN PDPフレームワーク イペロアメリカデータ保護ネットワーク規定 シンガポール 個人データ保護規則 (PDPR) ブラジル 個人データ保護法 (LGPD)	1995年- 制度未施行 (意見募集) 2020年- 2022年 2021年- 2022年- 制度未施行 (詳細未決)
	認証 	⑤ その他の契約等	多数	多数	—
		⑥ BCR (Binding Corporate Rules: 拘束的企業準則)	欧州/英国→域外 シンガポール→域外 ブラジル→国外	一般データ保護規則 (EU/UK GDPR) シンガポール 個人データ保護規則 (PDPR) ブラジル 個人データ保護法 (LGPD)	2016年- 2021年- 制度未施行
		⑦ データ域外移転安全評価	中国→国外	中国 個人情報保護法 (PIPL)	2022年-
		⑧ 個人情報越境処理保護認証	中国	中国 個人情報保護法 (PIPL)	制度未施行 (詳細未決)
		⑨ 越境プライバシールール (Cross Border Privacy Rules: CBPR認証)	加盟9カ国	APEC プライバシー・フレームワーク	2011年-
		⑩ APEC 処理者向けプライバシー認証 (APEC Privacy Recognition for Processors: APEC PRP認証)	APEC域内	APEC プライバシー・フレームワーク	2015年-
	行動規範 	⑪ 行動規範 (Code of Conduct)	欧州/英国→域外 ブラジル→国外	一般データ保護規則 (EU/UK GDPR) ブラジル 個人データ保護法 (LGPD)	2016年- 制度未施行 (詳細未決)
	その他 	⑫ 明示的な本人同意	多数	多数	—

越境移転ツール 調査結果サマリ (1/4)

各国/地域にとって、越境移転ツールの運用ハードルは高く、実際に運用が出来ている国/地域は一部



データ流通の活発化に伴い、複数国間ツールを含む様々な越境移転ツールが存在

- 規制同様、GDPRで規定されたツール (十分性認定、SCC/MCC、BCR、行動規範等) と同様もしくは類似するツールを各国/地域が個別に整備
- APEC、イberoアメリカなど地域レベルでの越境移転ツールの策定も進んでいるが、複数国/地域で利用可能なツールの場合、単一国/地域レベルで規定されるツールに比べて、内容が粗いものも散見される (例: ASEAN MCCs)



各国/地域で異なる要件を満たして越境移転を実現する難易度は相当に高いため、越境移転を実現するために必要な要件がひな形として整理・公表されているSCC/MCCの利便性は高く、2022年9月時点で最も多くの国/地域が採用しているツールとなっている

- 中国もSCCを公表しており、ローカライゼーションをすすめる国であっても、越境移転への対応は無視できない状況
- さらに、各国/地域のデータ流通に対する姿勢を問わず、利便性が高いツールとしてSCC/MCCが認められていることがうかがえる



ブラジル、シンガポールなど、EUと同様のツールを規定している国/地域は多いものの、ツールの運用のハードルは高く、2022年9月時点では、EU以外の国/地域における運用実績は多くない

- ブラジルは、GDPRに準じる規制を整備し、GDPR同様のツールを採用しているが、実際に運用できているツールはない
- シンガポールもGDPRに類するツールを採用しているが、地域レベルで規定されたツールを積極的に取り込むことで、運用コストを下げ、越境移転の利便性を担保している

越境移転ツール 調査結果サマリ (2/4)：越境移転ツールの要件比較

各ツールの目的/当事者により、要件に相違が出ているほか、基本であるプライバシー原則のカバー状況にも相違がある

		② 日本EU ④ SCC/MCC ※管理者-管理者の内容で比較								⑥ BCR			その他認証				⑪ 行動規範			
		補完ルール	EU	英国	中国	イバ	アメリカ	NZ	ASEAN	シンガポール	EU	英国	シンガポール	⑦ 安全評価	⑧ 越境認証	⑨ CBPR	⑩ PRP	EU	英国	
当事者の義務	プライバシー原則の遵守	●	●	●	●	●	●	●	●	ASEAN MCCsの利用を推奨 一部修正は必要	● ³	● ³	権利義務の明記を要求 明記すべき権利義務の個別指定はなし	●	●	●	●	●	●	
	処理の制限		●	●	●	●	●	●	●		●	●		●	●	●	●	●	●	●
	通知/選択/公開		●	●	●	●	●	●	●		●	●		●	●	●	●	●	●	●
	正確性		●	●	●	●	●	●	●		●	●		●	●	●	●	●	●	●
	安全保護措置		●	●	●	●	●	●	●		●	●		●	●	●	●	●	●	●
	個人参加/アクセス		●	●	●	●	●	●	●		●	● ³		● ³	●	●	●	●	● ⁸	● ⁸
	損害回避																● ⁵			
	アカウントビリティ		●	●	●	●	●	● ²	●		●	● ³		● ³		●	● ⁵			
	その他																			
	データ保護	●	●	●	● ¹	●	●	●	●		●	●		●	●	●	●		●	●
データ主体の権利	第三者の利用	●	●	●	●	●	●	●	●		●	●		●		●		●	●	
	アクセス権		●	●	●	●	●	●	●	●	●	●	具体事項の指定なし 安全保護措置違反時の救済/データ侵害時の 権益確保の方法の記載を要求	●	●	●	「データ主体の権利の行使」 に関する記載を要求			
	申立権/救済権			●	●	●	●	●	●	●	●	●		●	●					
	第三受益権		●		●	●	●	●	●			●		●	●					
	履行方法詳細		●	●	●	●	●	●	●	●	●	●		●	●					
個人データ侵害 (漏洩) 対応		●	●	●	●	●	●	●	●	●	●				● ⁶	●			●	●
紛争解決	当事者の責任請負	●	●	●	●	●	●	●	●	●	●									
公的機関による開示請求対応			●	●	●	●	●	●	●								●			
第三国法の影響評価			●	●	●	●	●	●	●				●	●						
監督	監督機関/裁判所		●	●	●	●			●						● ⁴			具体事項の指定なし 監督機関による監視の仕組み構築の要求のみ		
	組織内責任者		●				●		●		●	●		● ⁷	●	●				
	組織内の運用確立								●		●	●		●	●	●				
	関係者の教育								●		●	●		●	●	●				
詳細情報の記載/届出	データ主体の特定		●	●	●	●			●	●	●	●						●	●	
	個人データの特定		●	●	●	●	●	●	●	●	●	●		●	●		●	●		
	処理/移転目的		●	●	●	●	●	●	●	●	●	●		●	●					

※次ページで詳細比較

2023 by Boston Consulting Group. All rights reserved.

1. 中国SCCは、移転の必要性和移転によるデータ主体への影響の告知を求めるのみであり、取扱い制限や追加の保護措置の実施は求めている(2条2項) 2. 明確な履行責任/遵守に関する記載はないが、契約の遵守を監視する責任者の確保 (NZ MCC一般条項 1条7項) を明記 3. 「一般的なデータ保護の原則の適用」を要求 (GDPR/UK GDPR 47条2項d) 4. 個人情報保護責任者と個人情報保護団体の設置を要求 (個人情報跨境处理活动安全认证规范4条2項) 5. 「1.1 プライバシー原則の遵守」を要求 (CBPR認証基準) 6. 「1.7 緊急事態」項目等で漏洩対応を要求 (CBPR認証基準) 7. 用意すべき役割に個人データ保護責任者を列挙 (CBPR認証基準 8.1項) 8. 該当の記載はないが、「データ主体の権利の行使」内にアクセス権が含まれると想定される (EU/英国法で一般にデータ主体の権利としてアクセス権が認められているため)

越境移転ツール 調査結果サマリ (3/4)：安全保護措置¹の詳細要件比較

各国/地域が移転を含む個人データを処理する際の保護水準を提示しているが、その要求内容には差がある

●:該当項目あり	④ SCC/MCC							⑥ BCR			その他認証						
	EU	英国	中国	イバロアメリカ	NZ	ASEAN	シンガポール	EU	英国	シンガポール	⑦ 安全評価	⑧ 越境認証	⑨ CBPR	⑩ PRP	EU	英国	
個人データの仮名化及び暗号化の措置	●		●	●	具体事項の指定なし 「世界的/一般的に期待される業務水準」の保護措置の実施・維持を要求するのみ ⁴	具体事項の指定なし AMS法に準拠した又は当事者が合意した適切なセキュリティ措置の要求のみ ⁵	ASEAN MCCsの利用を推奨 一部修正は必要	具体事項の指定なし 「データの安全性の確保」の要求のみ ⁶	権利義務の明記を要求 明記すべき権利義務の個別指定はなし	具体事項の指定なし 「責任義務を履行する管理的及び技術的措置、越境データの安全性を保障する能力」の要求のみ ⁷	具体事項の指定なし 「関連法令に定める個人データ保護基準に適合する必要な措置」の要求のみ ⁸			●	●	●	
システム/サービスの機密性・可用性及び回復力を確保するための措置	●			●												●	●
物理的技術的インシデント発生時に、データの可用性とアクセスの復元を確保するための措置	●			●									●			●	●
処理のセキュリティを確保するための技術的組織的措置の有効性の定期的なテスト	●		●	●									●	●		●	●
ユーザーの識別と認証のための措置	●			●									●	●			
移転中のデータ保護に関する措置	●	●		●									●			●	●
保管中のデータ保護に関する措置	●	●		●												●	●
個人データの処理がおこなわれる場所の物理的セキュリティ措置	●			●									●				
イベントログの確保のための措置	●			●									●	●			
デフォルトを含むシステム構成確保のための措置	●			●													
内部IT及びITセキュリティのガバナンスと管理に関する措置	●		●	●									●	●	●	●	
プロセス及び製品の保証/認証のための措置	●			●										●			
データの最小化を確保するための措置	●			●												●	
データ品質を確保するための措置	●			●													
データ保持の限定性を確保するための措置	●			●													
説明責任を確保するための措置	●			●												●	
データポータビリティと廃棄を確保するための措置	●																
その他		具体列挙はほとんどなく、概要レベルの列挙のみ ²	具体列挙はほとんどなく、概要レベルの列挙のみ ³														

1. ツールにより表現が異なるため、ここでは「安全保護処置」として記載し、且つ、EU SCC Annex II の技術的・組織的措置を軸に比較
2. IDTA 第1部Table4 にOrganizational Security Measures、Technical Security Measures、Security of Transmission、Security of Processingの記載欄があるのみ。具体的な方法 (暗号化等) の指定はない
3. 中国SCC 2条4項には、「暗号化、匿名化、非識別化、アクセス制御等の技術的及び管理的措置」の記載のみ 4. NZ MCC 第2部一般条項 1条3項 5. ASEAN MCCs 3条2項
6. GDPR 47条2項d、UK GDPR 47条2項d 7. 数据出境安全评估办法 5条3項 8. 个人信息跨境处理活动安全认证规范 3条d

越境移転ツール 調査結果サマリ (4/4)：主要な事業者向け越境移転ツールの比較

事業者が越境移転を検討する際には、以下3つの越境ツールの検討が主となる

	SCC/MCC	BCR	CBPR
対応国	EU、英国、シンガポール、中国、ニュージーランド、ブラジル ¹ 、ASEAN、イベロアメリカ	EU、英国、シンガポール、ブラジル ¹	日本、米国、カナダ ² 、メキシコ ² 、シンガポール、韓国、オーストラリア ² 、台湾、フィリピン ²
制度の概要	<ul style="list-style-type: none"> データ輸出者/輸入者間で越境移転のために結ばれる契約 ひな形形式で公開されており、越境移転に求められる要件が網羅的/具体的に示される EUを筆頭に、ASEAN/イベロアメリカなどの地域機関のほか、採用国が増えている 	<ul style="list-style-type: none"> グループ企業間での越境移転を可能とする個人データ保護方針 利用には、企業内でデータ保護方針を整備のうえ、担当機関の承認を得る必要がある ひな形は公開されておらず、各国/地域規制で明記すべき主要な要件の概要が示されるのみ 	<ul style="list-style-type: none"> 加盟国内での越境移転を可能とする個人データ保護認証 求められる個人データ保護体制を整備し、審査を受けることで認証を得ることが可能 認証制度であるため明確且つ具体的に要件(基準や申請事項)が示される
採用国/地域別の差分	<ul style="list-style-type: none"> 国/地域別に記載事項のカバー範囲に大差はない(一部例外を除く) <ul style="list-style-type: none"> 個別要求レベルでは、粒度感に若干の相違がある 	<ul style="list-style-type: none"> 対応国が少ないにもかかわらず、各規制で定められる要求にはバラツキがある <ul style="list-style-type: none"> EU/英国が細かく、シンガポールは粗い 	<ul style="list-style-type: none"> なし
利用のメリット/デメリット	<ul style="list-style-type: none"> 要件が具体列挙されているため、利用者(企業)の対応事項が明確且つ、BCRに比べて相対的に低コストで対応が可能 ただし、複数国/地域、企業間で越境移転をおこなう場合、複数本の契約が必要となる 当事者間での権利・責任の明確化に主眼が置かれており、CBPRのように具体的な社内運用体制の確立を求める内容は含まれない 	<ul style="list-style-type: none"> SCC/MCCと異なり、示される要件が粗いため、具体化は各企業でおこなう必要があり、対応コストは重くなりがち 承認されれば、対象としたグループ企業すべてでの越境移転が認められる 個人データ保護方針の策定とその遵守の確立を求めるため、社内運用体制の確立も要求。ただし、その内容は、CBPRと比較すると粗い³ 	<ul style="list-style-type: none"> 国家間の規制に差分があっても、取得している企業間では越境移転が認められる 承認されれば、加盟国/認証企業間での越境移転が認められるが、加盟国/認証企業数が少ない 企業の個人データ保護体制を審査・承認するものであるため、各種手続きを含む体制・運用の確立が求められる

1. 規制内では、越境移転を認める要件としてSCC/MCC、BCRを規定しているが、実際の要件は未定(ガイドライン/実施細則等が未定)

2. アカウンタビリティ・エージェントを持たないため、実運用は始まっていない、3. 規制に記載された要件では、明確に細かな社内運用体制は求められていないが、最終稿では一部運用体制が記載される(申立手続等)



1 十分性認定

概要

十分性認定は、GDPRで定められた個人データの越境移転の要件の1つ。越境移転のホワイトリストと理解できる。GDPR以外にも、英国、日本など7カ国が同様の仕組みを採用しているが、運用には、認証機関の設置や認証制度の整備等が必要であり、2022年9月現在で実質的に運用ができているのは、EUのみと言える。

GDPRの十分性認定

正当化根拠
GDPR45条

認定対象
第三国、第三国内の地域又は特性の部門（複数部門含む）、国際機関

認定機関
欧州委員会

- 具体要件
- 欧州委員会は、特に以下を考慮してデータ保護水準の評価をおこなう（45条2項）
- 第三国における法の支配、人権及び基本的事由の尊重、公共の安全、国家安全保障等を含む法令、判例法、データ主体に認められる行政及び司法上の救済措置等の状況
 - 適切な執行権限等を有する監督機関の存在及び同機関の効果的な機能の実現
 - 第三国が加盟している個人データ保護に関する条約等

- 認定手続き
1. 欧州委員会からの提案
 2. 欧州データ保護委員会 (European Data Protection Board: EDPB) による意見提出
 3. EU加盟国代表による承認
 4. 欧州委員会による決定の採択 (=承認)

- 更新と取消
- 欧州委員会は、最低限4年ごとに認定の見直しを検討しなければならない（45条3項）
 - 欧州委員会は、認定対象が十分な保護水準を確保していないことが判明した場合、必要な範囲で認定を取消、修正又は停止しなければならない（45条5項）

各国/地域における認定状況

●:十分性認定国	EU	英国	日本	ロシア	トルコ	ベトナム	ブラジル	タイ
1 EU/EEA諸国		●	●	●	認定なし	認定なし	認定なし	認定なし
2 アゼルバイジャン				●		草案段階のため		実施細則が未設定
3 アルゼンチン	●	●		●				
4 アルバニア	●			●				
5 アルメニア	●			●				
6 アンドラ公国	●	●		●				
7 イギリス	●		●	●				
8 ウクライナ	●			●				
9 ウルグアイ	●	●		●				
10 ガーボベルデ	●			●				
11 北マケドニア	●			●				
12 グルジア	●			●				
13 サンマリノ	●			●				
14 スイス	●	●		●				
15 セネガル	●			●				
16 セルビア	●			●				
17 チュニジア	●			●				
18 トルコ	●			●				
19 ボスニア	●			●				
20 メキシコ	●			●				
21 モーリシャス	●			●				
22 モナコ	●			●				
23 モルドバ	●			●				
24 モロッコ	●			●				
25 モンテネグロ	●			●				
26 イスラエル	●	●						
27 英国領ガーンジー	●	●						
28 英国領ジャージー	●	●						
29 英国領マン島	●	●						
30 カナダ	●	●						
31 韓国	●							
32 日本	●	●						
33 ニューゼーランド	●	●						
34 フェロー諸島	●	●						



2 日本EU間補完的ルール

概要

日本-EU間では、各国/地域規制を根拠として、相手国/地域を個人データの越境移転を認めるために十分な保護水準を確保していると認定している。
しかしながら、日本-EU間の法制度には、いくつかの相違点も見られることから、EU域内から十分性認定により移転を受けた個人データについて高い水準の保護を確保するための追加的なルールの順守が求められる（日EU間補完的ルール）。

制定の背景

日本がGDPRに基づく十分性認定を取得したことに伴い、日本の個人情報保護委員会が「個人情報の保護に関する法律に関わるEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」として2018年に公表。

現在は、英国のEU離脱を受けて公表・成功された2019年改訂版が適用される。

正当化根拠

- 日本 個人情報保護法 28条
- GDPR 45条

詳細

適用範囲

補完的ルールの前文によると、当該ルールの適用範囲は以下の通り

- EU域内から十分性認定により移転される個人データ
- EUからの離脱後の英国域内から十分性認定により移転される個人データ

適用対象者

EU及び英国域内から十分性認定により移転される個人データを受領する個人情報取扱事業者（前文）

内容詳細

補完的ルールでは、以下の要件が定められている

1. 要配慮個人情報

- 十分性認定に基づき移転された個人データにGDPR及びUK GDPRで特別な種類の個人データと定義されるデータ（例：性的指向、労働組合に関するデータ等）が含まれる場合には、個人情報取扱事業者は、「要配慮個人情報」（APPI 2条3項）と同様に取り扱う必要がある

2. 利用目的の特定、利用目的による制限

- 個人情報取扱事業者は、十分性認定に基づいて個人データの提供を受ける場合、APPI 30条1項及び3項に基づき、利用目的を含め、取得の経緯を確認し、記録しなければならない（十分性認定に基づいて個人データの提供を受けた他の個人情報取扱事業者から、当該データの提供を受ける場合も同様）
- いずれの場合も、個人データの提供にあたっては、利用目的を特定し、且つその範囲内で利用しなければならない

3. 外国にある第三者への提供の制限

- 個人情報取扱事業者は、十分性認定に基づいて提供を受けた個人データを外国にある第三者に提供する場合には、APPI 28条の要件を満たす場合を除き、予め外国にある第三者への個人データの提供を認める旨の本人同意の取得が必要

4. 匿名加工情報

- 十分性認定に基づいて提供された個人データについて、個人情報取扱事業者が、加工方法等情報を削除することにより、匿名化された個人を再識別することを何人にとっても不可能とした場合に限り、匿名加工情報とみなされる



3 TADPF

概要

TADPFは、EU-米国間での個人データの越境移転のための最新のフレームワーク。個人データ保護の包括法を持たない米国は、EUの十分性認定を受けることが困難であるため、外交交渉のうえ、個別協定を締結し、個人データの越境移転を実現してきた。EU-米国の越境移転に関しては、グローバルBig Techによる個人データ活用をめぐり、EU市民による苦情申立、欧州司法裁判所による当該フレームワークの無効判決とそれに対するEU・米国両政府の対応が繰り返されてきた (右記参照)。

制定の背景

右記参照

正当化根拠

GDPR 45条

TADPFの詳細

主な原則

TADPFに関する最新の発表では、EUと参加する米国企業間での個人データの越境移転について、以下の原則が示されている。

- 米国情報当局によるデータへのアクセスの限定
- データ保護審査裁判所 (Data Protection Review Court) を含む独立した拘束力を持つ救済メカニズムの確立
- 移転された個人データの処理に関する企業に対する義務の継続
- 新しいモニタリングとレビューの仕組みの採用

ネクスト・ステップ

- 2022年3月に合意した原則の法的文書への変換
- 原則を盛り込んだ米国大統領令の発令
 - 欧州委員会による大統領令の妥当性判断

1. 公開情報よりBCG作成

Source: [European Commission "Trans-Atlantic Data Privacy Framework" 2022](#); [The White House "Fact sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework" 2022](#)

EU-米国間の個人データの越境移転をめぐる動き¹

- 1995年12月 EUデータ保護指令 施行
- 2000年07月 EU-米国間での個人データの越境移転のための枠組み
セーフハーバー協定 (Safe Harbor Privacy Principles) 導入合意
- 2001年07月 セーフハーバー協定 施行
- 2013年06月 マックス・シュレムス (Max Schrems) による個人データ保護に関する苦情申立
 - 米国当局の監視活動が、個人データの適切な保護を保証していないとして、オーストリアの弁護士であるマックス・シュレムスが、Facebookによる個人データの米国移転に対する苦情を、アイルランド データ保護委員会に申し立て
- 2013年06月 スノーデン事件
 - 元米国中央情報局職員であるエドワード・スノーデン (Edward Snowden) が、米国国家安全保障局による個人情報収集を暴露
- 2014年06月 マックス・シュレムスによる苦情申立の欧州司法裁判所への付託
- 2015年10月 欧州司法裁判所によるセーフハーバー協定無効判決 (Schrems I 判決)
- 2016年02月 新枠組み プライバシー・シールド (EU-US Privacy Shield) 導入合意
- 2016年07月 プライバシー・シールド 採択
- 2016年08月 プライバシー・シールド 施行
- 2016年12月 欧州委員会によるプライバシーシールドの十分性認定
- 2018年05月 GDPR 施行
- 2020年07月 欧州司法裁判所によるプライバシーシールド無効判決 (Schrems II 判決)
 - プライバシーシールド及びGDPR施行を受けてのシュレムスの申立の再構成に対する判決
 - なお、この判決では、プライバシーシールドの無効だけでなく、当時のSCC (旧 SCC) の不備も指摘
- 2022年03月 新枠組み TADPF 原則合意



4 BCR (1/2)

概要

BCRは、事業者グループ内での個人データの越境移転を承認する認証制度。GDPRで定められているほか、英国は勿論、近年はGDPRに類似した越境移転を持つ国でも同様の仕組みが越境移転の根拠として認められている（ブラジル、シンガポール）。

SCC/MCCでは複数の契約に分けなければならない状況であっても、BCRでは1つの申請のみでカバーされるため、一見、事業者グループ内の越境移転に関してはBCRの方が有用に思われる。しかし、BCRは、SCC/MCCのように具体的な契約ひな形が公表されているわけではなく、事業者が個別に文書化を行う必要があるため、実際には多大なコストを要する。そのため、利用企業が多いとは言えないのが現状となっている。

なお、GDPRの規定が最も詳細であるため、ここでは、GDPRにおけるBCRについて記載する。

正当化根拠

各国/地域規制

詳細

申請/認証対象

事業者グループまたは共同経済活動に従事する事業者グループ内での個人データの越境移転を予定する事業者

運営機関

管轄データ保護機関

認証取得事業者数

GDPR施行以降の承認事業者は、38社（2022年9月時点）¹

具体要件

<承認要件（47条1項）>

- BCRが、法的拘束力を有し、関連する全メンバーに適用され、遵守されていること
- BCRが、個人データの処理に関し、データ主体に執行できる権利を明示していること
- BCRが、GDPR47条2項に定められた要件（右記の必要記載事項）を満たしていること

<必要記載事項（47条2項）>

- 対象事業者の情報
- 取扱いデータ/処理/データ主体の種類及び越境移転の目的
- 国内/国外における法的拘束性
- 一般的なデータ保護原則の適用
- 処理に関するデータ主体の権利及び当該権利の履行手段
- EU域外の事業者によるBCRへの違反責任を、EU域内の事業者が引き受けることの確認
- BCRに関する情報のデータ主体への通知方法
- データ保護責任者の業務
- 不服申立手続き
- BCRの遵守を確実に検証するための仕組み（是正措置の確実な履行のための手段を含む）
- BCRの規定変更を記録・報告する仕組み
- 確実なBCRの遵守を実現するための監督当局との協力の仕組み
- BCRによって提供される保障に、実質的に悪影響を及ぼし得る法的要件の報告体制
- 個人データにアクセスする人材への適切な教育

手続き/作業

1. 必要情報の収集・承認要件への対応（データマッピング等）
2. 事業者による管轄データ保護機関へのBCR申請
3. 関係データ保護機関を含めた審査・決定草案の作成、欧州データ保護委員会への通知
4. 欧州データ保護委員会による意見・最終決定
5. 管轄データ保護機関によるBCRの承認

取得にかかる期間（目安）

数年²

更新と取消

- 承認は、必要に応じて管轄データ保護期間により修正・置換・廃止されるまで有効
- いかなる更新もデータ保護機関へ提出されなければならないが、個人データ保護のレベルに影響する変更又はその他重大な影響を及ぼす変更でなければ、年1回の確認で構わない

1. 2022年9月時点（EDPB "Approved Binding Corporate Rules"） 2. エキスパートインタビューより

Source: JETRO「EU一般データ保護規則（GDPR）に関わる実務ハンドブック（実践編）」2017年；個人情報保護委員会「一般データ保護規則（GDPR）仮日本語訳」



4 BCR (2/2) : 各BCRの要件比較

	欧州	英国	シンガポール	ブラジル
正当化根拠	GDPR 47条	UK GDPR 47条	PDPR 11条	
承認当局/申請先	所轄監督機関	ICO	—	
申請者/当事者	事業者グループまたは共同経済活動に従事する事業者グループ内の事業者	共同経済活動に従事する事業者グループ及びグループ内の関係者全員	移転元と移転元と関係がある組織	
認定取得事業者数	38社 ¹	27社 ²	n/a	
基本要件	<ul style="list-style-type: none"> 法的拘束力と全メンバーによる遵守 データ主体に執行できる権利の明示 必要記載事項の記載 	<ul style="list-style-type: none"> 法的拘束力と全メンバーによる遵守 データ主体に執行できる権利の明示 必要記載事項の記載 	<ul style="list-style-type: none"> 移転先が移転元と関係を有し、他の法的拘束力のある義務に服していないこと 	
必要記載事項	当事者情報			
	内部的/対外的拘束力			
	移転に関する情報			
	一般的なデータ保護原則の適用			
	データの最小化			
	保存期間の制限			
	取扱いの法的根拠			
	機微データの取扱い			
	第三者への再移転			
	自動処理のみによる決定に服しない権利			
	異議申立/救済/賠償を求める権利			
	法的責任の受け入れ			
	データ主体への情報提供方法			
	データ保護責任者の設置			
	苦情申立て/処理手続き			
	BCR遵守を確保するための仕組み			
	BCRの変更報告・記録			
	監督機関との連携・協力			
	データ保護教育の実施			
	その他	悪影響がある第三国法の特定と報告	悪影響がある第三国法の特定と報告	

- BCRは各国/地域規制で盛り込むべき内容が規定されるのみであるため、SCCに比べ、要件の粒度が粗い
- そのため、事業者は独自で内容を文書化せねばならず、取得コストが相対的に膨らむ
 - 取得企業数もEU全体で40社弱と多くはない
- 規制上で外部機関による承認が規定されている欧州/英国EUに対し、シンガポールのBCRは現時点では、第三者機関による承認に関する記述はPDPA/PDPR上に見当たらない。規制上の要求事項も欧州/英国に対して相当粗い内容となっている

詳細未定

具体事項の指定なし
「BCRで提供される権利及び義務」の記載のみ要求

● : 該当項目あり
● : 任意項目

1. 2022年9月時点 (EDPB "Approved Binding Corporate Rules") 2. Controller/Processorは区別せず。DPA2018に基づく承認22社、UK GDPRに基づく承認5社。2022年9月時点 (ICO "List of BCR Holders")

3. GDPR/UK GDPRでは、データ主体/個人データの種類、移転目的、取扱いの種類、第三国への移転内容が求められるが、PDPRで記載が求められるのは移転範囲 (国) のみ

Source: UK GDPR; GDPR; Personal Data Protection Regulations 2021



5 データ域外移転安全評価

概要

データ域外移転安全評価は、データ取扱者が、中国国内での事業運営を通じて収集・生成した個人データ及び重要データを域外に提供する場合の安全評価手続き。

制定の背景

安全評価自体は、データ3法内で制定されていたが、2022年9月の「データ域外移転安全評価弁法」の施行により、手続きの詳細が規定された。

正当化根拠

中国データ3法 及び その下位規則「データ域外移転安全評価弁法」

詳細

申請/認証対象

以下のいずれかに該当する事業者 (データ域外移転安全評価弁法4条)

- ① 重要データの域外提供を予定するデータ取扱者
- ② 重要情報インフラ運営者又は100万人分以上の個人データを取扱うデータ取扱者
- ③ 前年1月1日から累計10万人分の個人データ又は1万人分の機微な個人情報情報を域外に提供したデータ取扱者で個人データの域外移転を予定しているデータ取扱者
- ④ その他、国家ネットワーク情報部門が定めた必要事項に該当するデータ取扱者

運営機関

国家ネットワーク情報部門

- 厳密には、所在する省のネットワーク情報部門を通じて申請される

認証取得事業者数

n/a

具体要件

データ域外移転安全評価では、以下のような項目が審査項目となる。

<データ越境リスクの自己評価 (データ域外移転安全評価弁法5条)>

- ① データ越境及び国外受領者による個人データ処理の目的等の適法性、正当性、必要性
- ② 越境データの規模、種類、機微の度合い、国家の安全等にもたらす可能性のあるリスク
- ③ 国外受領者が負う責任責務、責任義務を履行する管理的及び技術的措置
- ④ データ越境時及び越境後の改ざん等のリスク、個人データの権利利益の保護方法等
- ⑤ 国外受領者との間で締結されたデータ越境関連契約又はその他の法的文書におけるデータセキュリティ保護の責任義務の取決めの十分性
- ⑥ データ越境の安全性に影響を及ぼす可能性のあるその他の事項

手続き/作業

データ域外移転安全評価弁法に定められた手順は以下の通り

1. データ越境リスクの自己評価
2. 所在省のネットワーク情報部門への書類提出・申請
3. 省級のネットワーク情報部門による完全性検査 (資料の不備確認等。5営業日以内)
4. 省級のネットワーク情報部門から国家インターネット情報部門への申請資料の送付
5. 国家インターネット情報部門による受理の判断 (7営業日以内)
6. 国家インターネット情報部門及び関連期間に抛る安全評価 (45営業日以内)
7. 申請者への評価結果の書面通知

取得にかかる期間 (目安)

ネットワーク情報部門への書類提出後、2カ月程度

更新と取消

- 評価結果発効から2年
 - 有効期間内に申請内容等に変化が生じた場合、有効期間満了後もデータ越境活動の継続が必要である場合には、再申告が必要 (データ域外移転安全評価弁法14条)
 - 国家インターネット情報部門は、評価済みのデータ越境活動が要求を満たさなくなったことを発見した場合、データ越境活動の是正・終了を判断できる (同法17条)



6 個人情報越境処理保護認証

概要

国内外の個人データ取扱事業者が、越境移転時に遵守すべき要件を遵守していることを認める制度。本認証の取得は、越境移転の要件の1つとしてPIPL上でも定められている。2022年に認証取得のガイドが公表されたが、認証機関など、認証制度の運営に必要な要件の一部は未定もしくは未実現のため、2022年9月時点では、越境移転の要件として本認証を利用することはできない。

準拠法令・規格

- 中国 個人情報保護法 (38条1項)
- 実践ガイド (网络安全标准实践指南—个人信息跨境处理活动安全认证规范: サイバーセキュリティ標準実践指針—個人データ越境処理保護認証規範)

制度の詳細

申請/認証対象

- 多国籍企業又は同一の経済・事業体の子会社・関連会社間で個人データの国境を越えた処理活動をおこなう個人データ取扱事業者¹
- PIPL3条2項が適用される中国国外の個人データ取扱事業者

申請/認証単位

法人

運営機関

認証取得に関する詳細は未定 (認証機関についても具体は未定)

認証取得企業数

運用開始前のため、該当企業なし

具体要件

- 認証の取得を申請する当事者は、前提として「個人データセキュリティ規範」²を遵守しなければならない。
- 加えて、越境移転をおこなう場合には、実践ガイドに定められる以下の基本原則及び基本要件も遵守する必要がある

<基本原則>

- ① 適法性、正当性、必要性、誠実性の原則
- ② 公開性と透明性の原則
- ③ 情報の質の原則
- ④ 同等保護の原則
- ⑤ 責任明確化原則
- ⑥ 自主認証の原則

<基本要件>

- ① 法的拘束力のある契約の締結
- ② 組織的管理体制の整備
(個人データ保護責任者の指定、個人データ保護組織の確立)
- ③ 個人データの越境処理に関する統一規則の遵守
- ④ 個人データ保護影響評価の事前実施

手続き/作業

認証取得に関する詳細は未定

取得にかかる期間 (目安)

認証取得に関する詳細は未定

更新と取消

認証取得に関する詳細は未定

1. いずれの場合も、認証の申請は国内の当事者がおこなわなければならない。PIPL3条2項に該当する場合は、領域内に設置する専門機関又は指定代理人による申請となる (実践ガイド2条)

2. 安全内参「国家标准《个人信息安全规范》2020版正式发布 (附下载)」

Source: 全国信息安全标准化技术委员会「关于发布《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》的通知」2022年、企業法務ナビ「中国『個人情報越境処理保護認証規範』の解説」2022年



7 CBPR (1/2)

概要

CBPRは、事業者等の個人データの越境移転に関して、APECプライバシー・フレームワークへの適合性を審査・認証する国際制度の1つ。日米をはじめとして、APEC加盟国のうち9カ国・地域が参加している(2022年4月時点)。

実際に、日本・シンガポールでは、個人情報保護法・ガイドラインにおいて、越境移転を認める「十分な保護水準を確保するための適切な措置」が認められる場合の1つとして、CBPRを認めており、越境移転の実現手段として活用されている。

制定の背景

2004年に承認されたAPECプライバシー・フレームワークをベースとして、2008年に開始された「APECデータプライバシーパスファインダープロジェクト」を通じて2009年のCPEA(：越境執行協力協定)に続いて、2011年に策定された。

正当化根拠

APECプライバシー・フレームワーク

詳細

申請/認証対象

事業者

- なお、日本では、JIPDECの認定個人情報保護団体の「対象事業者」であることが必要

運営機関

第三者認証機関であるアカウントビリティ・エージェントが審査・認定を実施する

- アカウントビリティ・エージェントは、APECに認定された独立機関
- 2022年9月時点で、CBPR参加9カ国・地域のうち、5カ国・地域の9団体が認定されている
- 日本では、JIPDEC(日本情報経済社会推進協会)がアカウントビリティ・エージェントとして認定されている

認証取得事業者数

52社(2022年9月時点)¹

- 国別では、米国：42社、日本：4社、シンガポール：6社

具体要件

JIPDECが公表している認証基準及び、認証申請で必要となる内容は次頁の通り

認定手続き

1. 必要情報の収集・対応、事前確認
2. 事業者によるCBPR認証の申請
3. 審査(文書審査、現地審査)
4. 認証決定
5. アカウントビリティ・エージェントによる認証取得事業者の公表とAPEC事務局への通知

取得にかかる期間(目安)

約4カ月

更新と取消

- APECは更新審査を認めておらず、1年ごとの再認証申請が必要
 - 毎年、再認証申請を行わない企業が散見される
- モニタリングにより、体制や取扱データ等の確認がおこなわれるほか、問題が発覚した場合には、その内容により、指導や認証の一時停止、認証の取消がおこなわれる

1. CBPRs "Compliance Directory" 2. JIPDEC「CBPR認証の意義と近時の取得動向について」2022年
Source: JIPDEC「APEC CBPR認証申請ガイドブック 第2.3版」2022年



7 CBPR (2/2)

CBPRに申請する事業者のための認証基準

JIPDECは、APECプライバシー・フレームワークへの準拠状況の確認のため、CBPRガイドラインに基づき、JIPDEC審査基準として以下を公表している。

- 1.1 プライバシー原則の遵守
- 1.2 利用する個人データ及び取得方法の特定
- 1.3 利用目的の特定
- 1.4 法令、国が定める指針、その他の規範の参照手順及び運用の確立
- 1.5 リスク対策の確立
- 1.6 内部規定の整備
- 1.7 緊急時の対応の確立
- 2.1 プライバシー・ポリシーの整備
- 3.1 個人データの適法且つ公正な手段による取得
- 4.1 特定された利用目的の範囲内での個人データの利用に関する措置
- 4.2/8.5 個人データの提供時の措置の整備
- 5.1/7.7 個人データの取得・利用・提供に関連した選択肢の提供と利用・提供拒否対応
- 5.2 個人データの正確性の確保
- 6.1/6.3 リスク対応及び安全管理措置の構築
- 6.2 個人データに関するリスク評価
- 6.4/8.6 委託先の監督・管理
- 6.5 定期的なリスク評価・対応の見直し
- 7.1 個人データに関する事項及び個人データのデータ主体への開示
- 7.2/7.3/7.5/7.6 個人データに関するデータ主体の権利の保障・対応 (開示・訂正・削除)
- 7.4 個人データの利用目的の通知
- 8.1 個人データ保護マネジメントシステムの確立・維持のための資源の用意
- 8.2 苦情・相談の対応
- 8.3/8.4 従業員の管理・教育
- 9.1/9.2 定期的な内部監査の計画・実施
- 9.3 是正処置・予防措置の確立

CBPRの認証申請で必要とされる主な情報

1. CBPR認証申請書
2. CBPRシステム事前質問書
事前質問書での主な確認事項は以下の通り
 - 基本情報
 - 認証申請組織及び該当組織により管理される子会社/支社の住所、役割等
 - 担当者情報
 - 個人データを取扱う事業・業務詳細
 - 個人データの取得及び移転が予定される国・地域
 - 通知：プライバシーステイトメントへの必要事項の反映状況
 - 取得
 - 個人データ取得要件
 - 個人データの方法
 - 利用：個人データの利用要件
 - 選択：個人データの取得・利用・開示に関するデータ主体への選択肢の提示状況
 - 個人データの完全性：取得した個人データの正確性・完全性・更新の対応状況
 - セキュリティ対策：セキュリティ対策の実施状況
 - アクセス及び訂正：データ主体の個人データに対するアクセス・訂正への対応状況
 - 責任：CBPRが求める基準への準拠責任を果たすための体制・措置の対応状況
3. JIPDEC追加質問書
 - 事前質問書で確認した移転に関する詳細情報：移転の法的根拠、概算データ件数等
 - JIPDEC審査基準に対する対応状況と根拠情報
4. 過去6ヶ月の事故等一覧



8 PRP認証

概要

PRP認証は、データ処理者が処理を行う際に、データ管理者に代わって、APECプライバシー・フレームワークに適合した個人データの保護水準を持つことを認証する制度。対象が限定されているため、APECプライバシー・フレームワークのうち2原則（安全保護措置と説明責任）に焦点が当てられており、CBPRより要件が少ない。

シンガポールでは、個人データ保護法において、越境移転を認める「十分な保護水準を確保するための適切な措置」が認められる要件の1つとして、PRP認証を認めている。

制定の背景

データ管理者に代わって個人データを処理するデータ処理者に特化したCBPRの付帯認証として、2015年に策定された。

CBPRに比べて2020年時点での参加国は米国とシンガポールのみ。

正当化根拠

APECプライバシー・フレームワーク

詳細

申請/認証対象

事業者（データ処理者）

運営機関

第三者認証機関であるAB（Assessment Body）が審査・認証を実施する

認証取得事業者数

44社（2022年9月時点）

- 国別では、米国：41社、シンガポール：3社

具体要件

APECでは、PRP認証の具体要件として以下を定義（ABがSelf-Assessmentシートとして提示）

1. 申請情報

- 基本情報
 - 認証申請組織及び該当組織により管理される子会社/支社の住所、役割等
 - 担当者情報

2. 事前質問事項

- 情報セキュリティ方針の実施状況及び詳細
- 個人データ保護・情報セキュリティに関する従業員教育の実施状況
- 安全保護措置の実施状況：有効性テスト、管理者への通知プロセス
- 個人データの廃棄・返却手順
- リスクアセスメントの利用状況
- 個人データの利用目的の限定の実施有無
- 管理者の指示に対する対応プロセスの詳細
- 責任者の設置
- 管理者への通知の対応状況

手続き/作業

- 必要情報の収集・対応、事前確認（Self-Assessment）
- 事業者によるPRP認証の申請
- ABによる審査（文書審査、現地審査）
- 認証決定
- ABによる認証取得事業者の公表

取得にかかる期間（目安）

n/a

更新と取消

- 基本的な条件はCBPR同様
 - 認証期間は1年で、1年ごとの再認証申請が必要
 - 申請内容に関する重要な変更等が発生した場合には、ABに通知しなければならない。内容によっては、審査が必要となり、ABは認証の有効性を判断する



9 SCC/MCC

概要

個人データの越境移転を可能とする措置の1つ。当事者間での契約書締結により越境移転を可能とするもので、契約書ひな形の形式で公開されている。BCRのように第三者認証を受けるものではないが、当事者間の契約で成り立つこと、さらにその契約書のひな形が公開されていることから、事業者の利便性は高い。近年では、国家単位で作成されているだけでなく、ASEANやイベロアメリカなど地域レベルでも広く採用・策定されている。

適用国/地域

欧州	Standard Contractual Clauses <ul style="list-style-type: none"> 1995年初版施行。最新版は2021年 管理者-管理者、管理者-処理者、処理者-処理者、処理者-管理者の4方式
英国	IDTA (International Data Transfer Agreement) <ul style="list-style-type: none"> 2022年施行 管理者-管理者、管理者-処理者の2方式を公開
中国	个人信息出境标准合同 <ul style="list-style-type: none"> 2022年6月パブリックコメント手続開始 個人情報処理者-国外受領者の1方式のみ公開
NZ	Model contract clauses for sending personal information overseas <ul style="list-style-type: none"> 2020年施行 開示者-受領者の1方式のみ公開
ASEAN	ASEAN Model Contractual Clauses for Cross Border Data Flows <ul style="list-style-type: none"> 2022年施行 管理者-管理者、管理者-処理者の2方式を公開
イベロアメリカ	Red Iberoamericana calausulas contractuales <ul style="list-style-type: none"> 2021年施行 管理者-管理者、管理者-処理者の2方式を公開
シンガポール	独自フォーマットなし (ガイドラインでASEAN MCCsの利用を推奨)
ブラジル	規制では越境移転のツールとしてSCCが規定されているが、詳細は未定 (実運用なし)

正当化根拠

各国/地域規制

詳細

契約当事者

データ輸出者と (域外/国外の) データ輸入者

- 各国/地域規制によっては、さらにデータ輸出者/データ輸入者の役割 (管理者、処理者等) に細分化される

適用期間/更新

当事者間での契約書に記載の期間

具体要件

- SCC/MCCは、当事者の義務等が列挙された契約書本文と、越境移転の詳細情報を記載する附属書 (もしくはテーブル) から成る
※ 本文で規定される主な事項や、附属書で求められる主な情報項目は次頁以降

手続き/作業

各国/地域により多少異なるが、基本的には以下の手順でSCC/MCCの締結がなされる

- ① 現状評価/必要情報の収集
- ② 対象となるデータ移転の方式別に、適切なSCC/MCCの契約条項を選択
- ③ 影響評価の実施
※データ移転の具体的な状況や移転先の法令や実務、保護措置の内容の評価
- ④ 締結



9 SCC/MCC : 各SCC/MCCの要件比較 (1/2)

※複数形式がある場合は、管理者-管理者の内容で比較

		欧州	英国	中国	ニュージーランド	ASEAN	イberoアメリカ	シンガポール	ブラジル
本文一般条項等で規定される主な事項	プライバシー原則の遵守	●	●	●	●	●	●	ASEAN MCCsの利用を推奨 データ主体/個人データの定義の見直し、データ侵害時の通知タイミングの明確化の追加・修正を提案	詳細未定
	処理の制限	●	●	●	●	●	●		
	通知/選択/公開	●	●	●	●	●	●		
	正確性	●	●	●	●	●	●		
	安全保護措置	●	●	●	●	●	●		
	個人参加/アクセス	●	●	●	●	●	●		
	説明責任	●	●	●	● ³	●	●		
	その他	●	●	●	●	●	●		
	データ保護	●	●	●	●	●	●		
	データの最小化	●	●	●	●	●	●		
	保管の制限	●	●	●	●	●	●		
	機微データの取扱い制限	●	1	2	●	●	●		
	第三者への転送	●	●	●	●	●	●		
	処理の記録と保管	●	●	●	●	●	●		
	データ主体の権利	●	●	●	●	●	●		
	アクセス権	●	●	●	●	●	●		
	自動処理のみに服さない権利	●	●	●	●	●	●		
	当局/裁判所への申立権	●	●	●	●	●	●		
	救済/補償を受ける権利	●	●	●	●	●	●		
	第三受益者としての権利	●	●	●	●	●	●		
	第三国の法律が悪影響を及ぼさない保証	●	●	●	●	●	●		
	個人データ侵害対応	●	●	●	●	●	●		
	通知	●	●	●	●	●	●		
	是正措置の実施	●	●	●	●	●	●		
	記録と保管	●	●	●	●	●	●		
	紛争解決	●	●	●	●	●	●		
	紛争解決への協力	●	●	●	●	●	●		
	当事国の決定の受入れ	●	●	●	●	●	●		
	違反責任の受入れ	●	●	●	●	●	●		
	公的機関の開示請求対応	●	●	●	●	●	●		
	通知	●	●	●	●	●	●		
	異議申立て	●	●	●	●	●	●		
	最低限のデータ提供	●	●	●	●	●	●		

1. 第1部Table2に記載欄あり 2. 移転の必要性和移転によるデータ主体への影響の告知の要求のみ (2条2項) 3. 履行責任/遵守に関する記載はないが、契約の遵守を監視する責任者の確保 (1条7項) を明記
Source: European Commission "Standard Contractual Clauses (SCC)"; ICO "Information Data Transfer Agreement"; 国家互联网信息办公室关于「个人信息出境标准合同规定 (征求意见稿)」; Privacy Commissioner "Sending information overseas"; ASEAN "ASEAN Model Contractual Clauses for Cross Border Data Flows"; Red Iberoamerica "Red Iberoamericana calausulas contractuales 2021"; PDPC "Guidance for use of ASEAN MCCs in Singapore"



9 SCC/MCC : 各SCC/MCCの要件比較 (2/2)

※複数形式がある場合は、管理者-管理者の内容で比較

		欧州	英国	中国	ニュージーランド	ASEAN	イberoアメリカ	シンガポール	ブラジル
詳細情報として記載が必要な事項（附属書等への記載事項）	当事者情報								
	名称 (事業者名)	●	●	●	●	●	●		
	役割 (管理者等)	●	●	●	●		●		
	担当者情報	●	●	●	●				
	データ主体								
	種類	●	●	●		●	●		
	個人データ								
	種類	●	●	●	●		●		
	数量/容量			●					
	技術的・組織的保護措置に関する情報 (内容等)	●	●		●		●		
	機微データの取扱い制限/追加措置の保護措置	●		● ²	●		●		
	処理/移転詳細								
	目的	●	●	●	●	●	●		
	移転頻度	●			●		●		
	処理の性質	●							
	処理/保管期間	●	●	●	●		●		
	第三者移転の有無/内容		●	●	●		●		
関連規制/文書との関係	準拠法	1	●		●		●		
	移転先の規制や関連契約による影響	1	●						
関連機関名 (データ保護機関、裁判所等)		●		● ³			●		

1. 本文で規定 (4-5条及び17条) 2. 機微データの種類のみの記載が必要 (付録1) 3. 仲裁裁判所の記載

Source: [European Commission "Standard Contractual Clauses \(SCC\)";](#) [ICO "Information Data Transfer Agreement";](#) [国家互联网信息办公室关于「个人信息出境标准合同规定 \(征求意见稿\)」;](#) [Privacy Commissioner "Sending information overseas";](#) [ASEAN "ASEAN Model Contractual Clauses for Cross Border Data Flows";](#) [Red Iberoamerica "Red Iberoamericana calausulas contractuales 2021";](#) [PDPC "Guidance for use of ASEAN MCCs in Singapore"](#)



11 行動規範 (1/2)

概要

行動規範は、越境移転に限らず、各種規制の各種業界への業界団体が定めるルールで、該当する規制の具体化を目的として作成される。

越境移転関連規制では、GDPRをはじめとしたいくつかの国で越境移転のツールの1つとして認められており、2022年9月現在、越境移転の根拠として行動規範を規定しているのは、欧州、英国及びブラジルの3か国・地域となっている。

英国・ブラジルはともに、GDPRをベースとした規制となっているため、ここではGDPRにおける行動規範について詳述する。

GDPRにおける行動規範

正当化根拠

GDPR40条

越境移転への適用

- GDPRにおいては、EU域外に個人データを移転する場合、移転先の企業が行動規範を遵守し、データ主体の権利などについて拘束力と執行力を持つ適切な保護措置を備えている場合、個人データの越境移転が認められる (40条3項)
- 行動規範が第三国の事業者に応用されるためには、欧州データ保護会議への提出が必要 (40条7項)

申請/認証対象

様々な類型の管理者又は処理者を代表する団体及びその他の組織 (40条2項)

運営機関

監督機関

具体要件

GDPRは、行動規範に盛り込むべき内容を40条2項で具体的に示している (次頁参照)

手続き/作業

行動規範は、1か国におけるデータの取扱を予定する場合と、複数国でのデータの取扱を予定する場合の2つの手続きが定められている。ここでは、越境移転の観点から、複数国でのデータの取扱を予定する場合の手続きについて詳述する (40条7-11項)。

- 行動規範案や既存の行動規範の修正・拡張案の監督機関への提出
- 監督機関から欧州データ保護会議への資料の提出
- 欧州データ保護会議による確認・意見
- 欧州データ保護会議の意見を受けて、監督機関が行動規範を承認
- 欧州データ保護会議から欧州委員会への意見提出
- 欧州委員会による行動規範に対する有効性の決定 (実装法令の採択)
- 欧州委員会による承認済みの行動規範の公表
- 欧州データ保護会議による承認済み行動規範の登録と利用開始

更新と取消

- 特に有効期間は定められていないが、承認された行動規範は、その遵守状況の監視を受ける。事業者が行動規範を遵守していないと認められた場合には、適切な対応がとられる (41条4項)。
 - 監視は、監督機関により認定された特定の認定団体によりおこなわれる (41条1項)



11 行動規範 (2/2)

- 行動規範を採用している3カ国/地域のうち、ブラジルは詳細を定める実行規則が未定のため、2022年9月時点で運用はおこなわれていない
- 運用中の欧州/英国の行動規範は、UK GDPRがGDPRを基に設計されているため、要求に差がない状況となっている
- 行動規範はBCR同様、規制上で要件が列挙されているのみであり、SCCのような具体性は乏しい。各組織は、業界の慣習や特性を踏まえて、各要求を具体化し、文書にしなければならない
- しかしながら、GDPR上は複数の構成国 (EU域外も含む) にまたがる行動規範を作成することができることから、EU域内外を問わず、同一の保護水準を作成し、個人データの越境移転をスムーズにできるというメリットがある
 - 例えば、GDPR違反判決を受けている米国のBigTech (Meta、Google等) も偽情報に関するEU行動規範に合意している

		欧州	英国	ブラジル
正当化根拠		GDPR 40条	UK GDPR 40条	
承認当局/申請先		所轄監督機関	ICO	
申請者/当事者		様々なタイプの管理者又は処理者を代表する団体及びその他の組織	管理者または処理者のカテゴリを代表する協会及びその他の団体	
行動規範に盛り込むべき事項	公正で透明性のある取扱い	●	●	詳細未定
	特定の状況において管理者が求める正当な利益	●	●	
	個人データの収集	●	●	
	個人データの仮名化	●	●	
	一般及びデータ主体に対して提供される情報	●	●	
	データ主体の権利の行使	●	●	
	子どもに提供される情報と親権者の同意の取得	●	●	
	管理者の責任及び初期設定等におけるデータ保護手段、並びに処理の安全性を確保する措置	●	●	
	監督機関及びデータ主体への違反の通知	●	●	
	個人データの第三国/国際機関への移転	●	●	
	管理者とデータ主体との間の紛争解決手続	●	●	

● : 該当項目あり
● : 任意項目






2.4

調査結果詳細：その他関連ツール

関連ツール 調査対象

調査対象国/地域で利用されているデータ保護関連ツールのうち、特に主要なものを列举

		名称	対象国/地域	準拠法令/規格	申請/認定対象
個人データ 保護	認証	 ① GDPR-CARPA	EU (ルクセンブルク)	一般データ保護規則 (GDPR)、 ISO規格 等	事業者、公共機関、その他団体等
		② dp.mark	台湾	台湾 個人データ保護法 (PDPA)、 その他国際ルール 等	事業者
		③ データ保護トラストマーク (Data Protection Trust Mark: DPTM)	シンガポール	シンガポール 個人データ保護法 (PDPA)	公共機関以外の組織
		④ 情報保護及び個人情報保護管理体系認証 (ISMS-P認証)	韓国	韓国 個人情報保護法 (PIPA)	データ通信サービス提供事業者 等
		⑤ プライバシーマーク (Pマーク)	日本	Pマーク運用指針 ※JIS Q 15001に準拠	事業者
		⑥ JAPHICマーク	日本	日本 個人情報保護法 (APPI)、 その他関連ガイドライン	事業者
		⑦ EuroPriSe	ドイツ	EuroPriSe基準 ※GDPRに対応	IT製品及びIT関連サービスベンダー
		⑧ TRUSTeマーク	グローバル	OECD プライバシーガイドライン	ドメイン、アプリ
		⑨ CNIL認証 (Certification des compétences du DPO: DPOスキル認定)	フランス	一般データ保護規則 (GDPR)、 フランス データ保護規則	個人データの処理者 (個人)
		⑩ ISMS-PIMS認証 ¹	グローバル	ISO/IEC 27701	事業者、事業者内の部門
一般データ 保護	規格	⑪ 個人情報安全規範	中国	—	—
		⑫ JIS Q 15001	日本	—	—
	認証	 ① ISMS認証 ¹	グローバル	ISO/IEC 27001	事業者、事業者内の部門
		② WebTrust	グローバル	認証局のためのWebTrust規準	事業者 (電子認証サービス事業者)
	規格	 ③ NIST SP800シリーズ	米国	—	—
		④ SOC2 (Service Organization Control Type2)	米国	—	—

1. ISO/IEC規格として整備されている規格のうち、いくつかの規格は、適合性評価制度を持つ。適合性評価制度を持つ場合、ISO/IEC規格への適合認証がなされる。ISO/IEC27001及び27701はいずれも適合性評価制度を持つため、ここでは規格ではなく認証として分類する

関連ツール 調査結果サマリ (1/4)

各国/地域規制を基に個人データ保護ツールが存在。一定の共通性が見られるほか、ツール間の連携・接続も一部ですすすめられている



個人データ保護の分野では、**各国/地域規制別を根拠とした個人データ保護認証が多数存在**。一方、一般データ保護 (セキュリティ) の分野では、国際認証が普及しているほか、近年は、**安全保障の観点から米国がデータ保護 (セキュリティ) 水準の評価基準を策定**しており、グローバルで普及しつつある

- 特にアジア圏では、調査対象国の多くが各国/地域規制を根拠とした個人データ保護認証制度を設けている
- EUにもGDPRを根拠とした認証制度が存在するが、EUの承認を得ている認証制度はGDPR-CARPAのみ
- 包括法を持たない北米発では、「個人データの健全なビジネス活用のためのトラスト確保」を目的とした認証制度 (TRUSTeマーク) が存在



各種個人データ保護認証が要求する内容は、**大項目レベルでおおむね共通**

- 詳細レベルでは、**アジア圏は組織的保護措置**に関する要求が多く、**EUでは技術的要求**を細かく定義する傾向



個人データ保護認証は、越境移転ツールとの接続も進められている

- 台湾では、個人データ保護と越境移転の効率的な推進のために、**個人データ保護認証 (Dp.mark) と越境移転認証 (CBPR) を合わせて取得することを推奨**
- EUは、特定のプロセスに則って承認された認証制度を越境移転の根拠として利用できると定めており (GDPR46条)、**GDPR-CARPAはその要件を満たすが、現時点では、EU域内 (ルクセンブルク) のみを対象範囲とする¹**
- 中国も制度の整備を進めており、その中で越境移転認証の前提として個人データ保護規格の遵守を必須化しているが、**あくまでも国内事業者の個人データ保護水準を測るものであり、移転先も含めた越境移転の両当事者を対象としないため、越境移転の実現には、別途SCC/MCC等が必要である (厳密には越境移転ツールと個人データ保護ツールが接続していると言えない)**

1. EU (ルクセンブルク) からデータを移転する場合に、移転元であるEU (ルクセンブルク) 事業者のGDPR準拠を認証するものであり、EU域外にある移転先 (日本等) は認証対象としない。したがって、越境移転の相互認証としては機能しない

関連ツール 調査結果サマリ (2/4)：個人データ保護ツールの主要要件の比較

各ツールの目的/当事者により、要件に相違が出ているほか、基本であるプライバシー原則のカバー状況にも相違がある

✓：他のツールと接続あり
●：該当項目

✓：接続を推奨

他ツールとの接続		1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P認証	5 プライバシーマーク	6 JAPHIC マーク ¹	7 EuroPriSe	8 TRUSTe マーク	9 CNIL認証	10 個人情報安全規範
		46条で越境移転の根拠と定義	CBPRと合わせて取得を推奨	ISMS認証と接続	ISMS認証と接続	JISQを根拠とする				責任者に関連する事項のみ定義	越境移転の前提として遵守が必須
基本措置	プライバシー原則遵守のための措置	●	●	●	●	●	●	●	●		●
	処理制限	●	●	●	●	●	●	●	●		●
	通知/選択/公開	●	●	●	●	●	●	●	●		●
	正確性	●	●	●	●	●	●	●	●		●
	安全保護措置	●	●	●	●	●	●	●	●		●
	個人参加/アクセス	●	●	●	●	●	●	●	●		●
	損害回避						●				
	アカウントビリティ	●	● ²	●		● ²		●	● ²		●
	機微データの取扱い制限	●	●	●	●	●	●	●	●		●
	アセスメント(データ保護評価)の実施	●	●	●	●	●		●	●		●
データ主体の権利を保障するための措置	処理の記録	●	●	●	●	●	●	●	● ⁵	※次ページ以降で詳細比較	●
	組織・技術的保護措置の実施	●	●	●	●	●	●	●	●		●
	移転/委託時の措置	●	●	●	●	●	●	● ⁴	●		●
	委託先の評価	●	●	●	●	●	●	● ⁴	●		●
	制約・義務の文書化	●	●	●	●	●	●	● ⁴	●		●
	委託先の監督	●	●	●	●	●	●	● ⁴	●		●
	越境移転時の保護措置	●	●	●	●	●	●	●	●		●
	アクセス権の保障	●	●	●	●	●	●	●	●		●
	自動処理のみによる決定に服しない権利の保障	●	●					●			●
	苦情/異議申立の保障	●	●	●	● ³	●	●	●	●		●
	データポータビリティの保障	●	●	●		●	●	●	●		●
	児童の権利保障	●	●					●	●		●

Note: プライバシーマークがJIS Q 15001を含むため、JIS Q 15001単体の比較は割愛。ISMS-PIMS認証は、具体要件は非公開のため、詳細比較から除外 Source: 各種管轄団体のHP等

1. 個人情報通則編を比較に利用 2. 経営者層に結果責任やコミットメントを要求 3. データ主体の権利保障のために求められる措置は、個人データの閲覧、訂正・削除、処理停止、異議申し立て、同意撤回要求への対応となっており、個人データの開示や複製の文言は見られない 4. プロセッサーや共同管理者等に区別して定義 5. 第三者提供活動に関してのみ記録を要求 6. データ保護一般位について定めるため、セキュリティリス74

ク対応のために必要な保護措置の要求に留まる (個人データに求められる技術的・組織的保護措置の重複も含む)

関連ツール 調査結果サマリ (3/4)：技術的保護措置の要件比較

EU SCCで提示されている項目をベースに比較。EUのツールでは技術的措置が詳細に定義される傾向にある

	1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P認証	5 プライバシー マーク	6 JAPHIC マーク ¹	7 EuroPriSe	8 TRUSTe マーク	9 CNIL認証	10 個人情報 安全規範
● :該当項目あり										
個人データの仮名化及び暗号化の措置	●		2	●	適切な 保護措置の 実施要求 のみ 詳細要件の 例示等はない ⁵	●	●	●	責任者に関連 する事項のみ 定義	●
システム/サービスの機密性・可用性及び 回復力を確保するための措置	●	●		●			●	●		
物理的技術的インシデント発生時に、データの 可用性とアクセスの復元を確保するための措置	●			●			●	●		
処理のセキュリティを確保するための技術的 組織的措置の有効性の定期的なテスト	●	●	●	●			●	●		
ユーザーの識別と認証のための措置	●	●		●		●	●	●		
移転中のデータ保護に関する措置	●			●			●	●		
保管中のデータ保護に関する措置	●			●		●	●	●		
個人データの処理がおこなわれる場所の物理的 セキュリティ措置	●	●	3	●		●	●	●		
イベントログの確保のための措置	●			●		●	●	●		
デフォルトを含むシステム構成確保のための措置	●	●	● ⁴	●		●	●	●		
内部IT及びITセキュリティのガバナンスと管理に 関する措置	●	●		●		●	●	●		●
プロセス及び製品の保証/認証のための措置	●	●	● ⁴	●			●	●		
データの最小化を確保するための措置	●	●		●		●	●	●		
データ品質を確保するための措置	●	●	●	●		●	●	●		
データ保持の限定性を確保するための措置	●		●	●		●	●	●		●
説明責任を確保するための措置	●						●			
データポータビリティと廃棄を確保するための措置	●						●	●		

Note: EU SCC Annex II に示されている技術的・組織的保護措置の具体例を軸に比較。また、JIS Q 15001・ISMS-PIMS認証は、前頁Note記載の通り、本比較から除外 Source: 各種管轄団体のHP等
1. 個人情報通則編を比較に利用 2. 保管時に匿名化に関する方針を文書化することは要求しているが、匿名化自体を要求する項目はない (DPTM Checklist Rule3 #5) 3. 「物理的保護措置の実施」は要求するが、具体的な措置内容の記載はなし (DPTM Checklist Rule3 #1) 4. 具体的な措置内容の記載はないが、システム開発時のデータ保護設計を要求 (DPTM Checklist Rule1 #7)
5. 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 J.9.2項 留意事項

関連ツール 調査結果サマリ (4/4)：組織的保護措置の要件比較

組織的保護措置の要件は、全体として大きな相違はないが、内容の具体性に大きな差分があり、特にアジア圏では詳細に規定される

		1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P認証	5 プライバシー マーク	6 JAPHIC マーク ¹	7 EuroPriSe	8 TRUSTe マーク	9 CNIL認証	10 個人情報 安全規範
		●:該当項目あり									
基本 措置	アセスメント (データ保護評価) の実施		●	●	●	●	●	●	●	責任者に 関連する事項 のみ定義	●
	責任者の設置		●	●	●	●	●	●	●		●
	データ保護方針の策定		●	●	●	●	●	●	●		●
	教育・訓練の実施		●	●	●	●	●	●	●		●
	評価 (内部監査)/改善		●	●		●	●	●	●		●
具体 措置	リスク対応 措置	データ主体への通知			●		●		●		●
		管轄機関への通知		●	●			●	●	●	●
		事象・対応の記録					●	●	●	●	●
	請求対応 措置	窓口の設置	●	●	●	●	●	●		●	●
		拒否理由の開示	●	●		●	●	●			●
	備考		データ保護に 影響を与える 決定事項や 保護措置内容 などの文書化 を要求			データフローなど システム関連 文書も含む様々 な事項の文書化 を要求		各種規程の 文書化を要求。 緊急対応から 罰則規定まで 10超の文書化 を要求			

Note: プライバシーマークがJIS Q 15001を含むため、JIS Q 15001単体の比較は割愛。ISMS-PIMS認証は、具体要件は非公開のため、詳細比較から除外
1. 個人情報通則編を比較に利用
Source: 各種管轄団体のHP等



関連ツール 調査対象

調査対象国/地域で利用されているデータ保護関連ツールのうち、特に主要なものを列举

	名称	対象国/地域	準拠法令/規格	申請/認定対象	
<div>個人データ保護</div> <div></div>	<div>認証</div> <div></div>	1 GDPR-CARPA	EU (ルクセンブルク)	一般データ保護規則 (GDPR)、ISO規格 等	事業者、公共機関、その他団体等
		2 dp.mark	台湾	台湾 個人データ保護法 (PDPA)、その他国際ルール 等	事業者
		3 データ保護トラストマーク (Data Protection Trust Mark: DPTM)	シンガポール	シンガポール 個人データ保護法 (PDPA)	公共機関以外の組織
		4 情報保護及び個人情報保護管理体系認証 (ISMS-P認証)	韓国	韓国 個人情報保護法 (PIPA)	データ通信サービス提供事業者 等
		5 プライバシーマーク (Pマーク)	日本	Pマーク運用指針 ※JIS Q 15001に準拠	事業者
		6 JAPHICマーク	日本	日本 個人情報保護法 (APPI)、その他関連ガイドライン	事業者
		7 EuroPriSe	ドイツ	EuroPriSe基準 ※GDPRに対応	IT製品及びIT関連サービスベンダー
		8 TRUSTeマーク	グローバル	OECD プライバシーガイドライン	ドメイン、アプリ
		9 CNIL認証 (Certification des compétences du DPO: DPOスキル認定)	フランス	一般データ保護規則 (GDPR)、フランス データ保護規則	個人データの処理者 (個人)
		10 ISMS-PIMS認証 ¹	グローバル	ISO/IEC 27701	事業者、事業者内の部門
<div>規格</div>	11 個人情報安全規範	中国	—	—	
	12 JIS Q 15001	日本	—	—	
<div>一般データ保護</div> <div></div>	<div>認証</div> <div></div>	1 ISMS認証 ¹	グローバル	ISO/IEC 27001	事業者、事業者内の部門
		2 WebTrust	グローバル	認証局のためのWebTrust規準	事業者 (電子認証サービス事業者)
	<div>規格</div> <div></div>	3 NIST SP800シリーズ	米国	—	—
		4 SOC2 (Service Organization Control Type2)	米国	—	—

1. ISO/IEC規格として整備されている規格のうち、いくつかの規格は、適合性評価制度を持つ。適合性評価制度を持つ場合、ISO/IEC規格への適合認証がなされる。ISO/IEC27001及び27701はいずれも適合性評価制度を持つため、ここでは規格ではなく認証として分類する



1 GDPR-CARPA

概要

GDPR-CARPAは、ルクセンブルクの事業者等がGDPRに準拠していることを証明する外部認証制度。認証取得により、透明性とGDPRへの準拠が促進され、データ主体は製品・サービスの情報保護水準を容易に判断できるようになる。

制定の背景

GDPR42条でEUが推奨する認証・シールの1つとして2022年5月に採用された。
CNPD (Commission nationale pour la protection des données: ルクセンブルクデータ保護委員会) が2018年に起草し、約4年のやり取りを経て、EDPB (Europe Data Protection Board: 欧州データ保護委員会) による採用が決定した。
GDPRは認証・シールの採用を推奨しているが、現時点 (2022年9月) では、GDPR-CARPAがGDPRの下で認められた唯一の認証メカニズムである。

準拠法令・規格

- GDPR (42条、55-56条等)
- ISAE 3000 (監査及びレビュー業務以外の保証業務)
- ISQ 1 (品質管理)
- ISO 17065 (認証機関の認定)

制度の詳細

申請/認証対象

ルクセンブルクで設立された企業、公的機関、団体、その他の組織

申請/認証単位

法人

運営機関

- 全体運営：CNPD
- 審査：CNPDによって承認された認証機関

認証取得企業数

不明

具体要件

認証基準は3つのセクションで構成される¹

- セクション1：データ保護ガバナンス全般基準
 - 管理者、処理者を問わず適用される
 - 方針・手順、処理活動の記録、データ主体の権利、DPO、データ侵害 等
- セクション2：管理者のガバナンス基準
 - 管理者に適用される
 - GDPR 5条に基づく主要なデータ保護原則に準拠しているか否か 等
- セクション3：処理者のガバナンス基準
 - 処理者に適用される
 - 管理者との契約及び下請け、セキュリティ、個人データの第三国への移転 等

手続き/作業

1. 必要書類の提出・申請
2. 認証審査(ISAE 3000)
3. 付与適格決定
4. 証明書の発行

取得にかかる期間 (目安)

n/a

更新と取消

- 有効期間は3年
 - ただし、年次の監査に合格することが必要

1. 認証基準の詳細は、CNPDが公表している資料を参照 (CNPD "GDPR-Certified Assurance Report based Processing Activities Certification Criteria v1.0")
Source: CNPD "LE SCHÉMA DE CERTIFICATION "GDPR CARPA""



2 dp.mark

概要

台湾政府が推進する唯一の個人データ管理システムであるTPIPAS (Taiwan Personal Information Protection and Administration System: 台湾個人データ保護及び管理システム) のルールに基づいた運用であることを証明する認証制度。事業者がPDPAを遵守するために適切且つ十分な管理体制を規定していることを示す。認証の取得により、取得者は、その個人データ管理能力に対する信頼性を高めることができる。CBPRと組み合わせた場合、越境移転の要件遵守の効率化も実現可能となっている¹。

制定の背景

個人データ保護管理システム基準及び検証システムの確立の検討を担当していた経済部は、PDPAの改正 (2016年) に伴い、電子商取引の管理システムの構築と安全な個人データ保護環境の確立を模索。日本のプライバシーマーク、米国のTRUTeマーク等、海外の動向も踏まえ、2011年にTPIPAS管理システムの推進とDp.markの創設を発表²。

準拠法令・規格

- 台湾 個人データ保護法
- OECD、APEC、および個人データ保護要件に関するGDPRの重要な原則

制度の詳細

申請/認証対象

台湾に拠点を置く事業者

申請/認証単位

法人

運営機関

- 運営：資訊工業策進會科技法律研究所
- 審査：台湾検査技術有限公司 等 2社

認証取得企業数

25社

具体要件

- TPIPASの仕様 (台湾個人データ保護及び管理体制規範³) が、すなわちdp.markの認証基準となる。主な項目は以下の通り
 - 管理責任
 - 制度設計
 - 支援
 - 個人データ保護マネジメントシステムの実施
 - 改善
- なお、本規範内で、越境移転に関しては、国際認証(CBPR、GDPRに基づく認証) の取得することを推奨している (11条12項)

手続き/作業

- 申請
- 外部認証機関による申請審査
- 外部認証機関による文書審査
- 外部認証機関による現地審査 (訪問、インタビュー等)
- 付与適格決定・通知
- 認証マークの申請・使用

取得にかかる期間 (目安)

n/a

更新と取消

- 有効期間は2年間
 - 認証取得後、中間監査の実施が必要

1. CBPRとの接合については、TPIPAS (TPIPAS HP " 實施效益") だけでなく、運営を担うの資訊工業策進會科技法律研究所も言及している (資訊工業策進會科技法律研究所 "TPIPAS十週年")

2. 博仲法律事務所"DP MARK" 3. TPIPAS "臺灣個人資料保護與管理制度規範 TPIPAS: 2021"

Source: TPIPAS HP



3 データ保護トラストマーク

概要

データ保護トラストマーク (Data Protection Trust Mark: DPTM) は、事業者のデータ保護対応を促進し、それを証明することで、対外的な信頼を醸成することを目的とした事業者向けの任意の認証制度。DPTMの取得により、事業者が責任あるデータ保護対策を採用して個人データを管理していることを、顧客、ビジネスパートナー、規制当局に示すことができる。ISO/IEC27001及び27701を取得している場合には、すでに情報セキュリティ及びプライバシー管理基準の準拠が証明されているため、比較的容易にDPTMを取得することが可能。

制定の背景

シンガポール政府は、国際的なデータ流通を支えるデータハブとして発展することを目的としてデジタル経済戦略を推進。その政策の一環として、データハブとしての信頼性を確立すべく、DPTM制度を開発し、2019年1月より正式稼働を開始した¹。

準拠法令・規格

シンガポール 個人データ保護法

制度の詳細

申請/認証対象

- 以下のいずれかの要件を満たす公的機関以外の組織
- 国内の法律に基づき設立又は承認されている組織
 - 国内に居住している又は国内に事務所や事業所を有している

申請/認証単位

法人

運営機関

- 管轄: IMDA (Information Media Development Authority: 情報通信メディア開発庁)
- 認証審査: BSI Group Singapore 等 7社

認証取得企業数

118社²

具体要件

認証要件は4つの原則で構成されている

- ガバナンスと透明性
適切な方針と実践、説明責任、社内コミュニケーションと研修
- 個人情報管理
適切な目的の設定、適切な通知の実施、適切な同意の取得、適切な利用及び提供、コンプライアンスに基づく越境移転
- 個人情報の取り扱い
適切な保護の実施、適切な補完と廃棄、正確かつ完全な記録
- 個人の権利
同意の撤回、アクセス権及び訂正権の提供

手続き/作業

1. DPTM認証チェックリストを用いた事前評価
2. IMDAに必要書類を提出・申請
3. IMDAから提供される自己評価フォームに従い、自己評価を実施
4. 自己評価を提出し、審査を開始
5. 審査 (書類審査、現地審査)
6. 査定完了、認証判断
7. 認定書、マーク等の発行

取得にかかる期間 (目安)

n/a

更新と取消

3年



4 情報保護及び個人情報保護管理体系認証 (ISMS-P認証)

概要

ISMS-P認証 (Personal Information & Information Security Management System: 個人情報及び情報セキュリティマネジメントシステム) は、事業者の個人データ保護・セキュリティ対応に関する対外的な信頼の担保及びデータ侵害のリスク低減を目的とした認証制度。

制定の背景

複数の類似する認証制度 (PIMS認証 (Personal Information Management System: 個人情報マネジメントシステム認証) とISMS認証) による混乱及びコスト問題の解消のために、2018年に複数の認証制度が統合された統合認証として誕生。

準拠法令・規格

韓国 個人情報保護法

制度の詳細

申請/認証対象

<義務対象者>

- データ通信サービス提供者:
 - 電気通信事業法 (6条1項) に従って登録され、且つ、サービス提供地域が「ソウル特別市及びすべての大都市」である事業者
 - インターネットサービス、インターネット電話サービス、移動通信サービス等の事業者が含まれる
- データ通信総合設備運営者
 - 情報通信網法 (46条1項) に規定された他者の情報通信サービスを提供するための統合情報通信設備を運営・管理する事業者
- 一定規模以上の事業者¹で、且つ、大統領令が定める基準に該当する事業者

<任意申請者>

- すべての個人データの処理者 (公共機関、民間事業者、法人、団体及び個人を含む)

申請/認証単位

法人

運営機関

KISA (Korea Internet & Security Agency: 韓国インターネット振興院)

認証取得企業数

n/a

具体要件

以下3カテゴリ100項目の基準が定められている

- 管理体制の確立と運用 16項目
- マネジメントシステムの基盤整備、リスク管理 等
- 保護措置の要件 64項目
- 資産管理、アクセス制御、暗号化 等
- 個人データ処理の各段階における要件 22項目
- 個人データ収集時の保護措置、個人データの提供時の保護措置 等

手続き/作業

1. 管理システムの確立と運用 (最低2カ月の運用実績及び証拠の準備)
2. 試験計画書の作成・試験準備
3. 審査
4. 付与適格決定・通知
5. 証明書の発行

取得にかかる期間 (目安)

n/a

更新と取消

有効期間は3年

1. 年間売上又は歳入等が1,500億ウォン以上であるか、情報通信サービス部門の前年度売上が100億ウォン以上又は前年度末基準直前3か月の平均利用者数が100万人以上/日である場合

Source: PIPC "ISMS-P"、KISA "ISMS-P 인증기준 안내서 (2022.04)"



5 プライバシーマーク

概要

プライバシーマークは、個人データについて適切な保護措置を講ずる体制を整備している事業者等を評価し、その旨を示すマークの使用を認める制度。個人データ保護に関する消費者の意識向上及び、適切な個人データの取扱い・保護のインセンティブを事業者に与えることを目的として、1998年に運用が開始された。

制定の背景

1990年代後半、世界的に個人データ保護に関する取り組みが進む中で、関連法規制の整備が遅れていた日本では、世界の個人データ保護基準（特にEU）に対応するため、個人情報保護に関するガイドライン（1997年）を制定した。しかしながら、ガイドラインはあくまでも世界基準に対応するためのデータ保護水準の目安を示したものであったため、実際に個人データを取扱う事業者によるデータ保護の実装・推進のために本制度が創設された。また、並行して、規格の整備も実施された（JIS Q 15001）。このような設立の背景を反映して、プライバシーマークは、世界的な個人データ保護基準（特にGDPR）の動きを適宜反映し、さらにJIS規格とも足並みをそろえ、適宜改定が行われている。

準拠法令・規格

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 Q15001に準拠

制度の詳細

申請/認証対象

日本国内に拠点活動を持つ事業者

申請/認証単位

法人

運営機関

- ・ 付与：日本情報社会経済推進協会（JIPDEC）
- ・ 審査：情報サービス産業協会 等 19機関
- ・ 研修：関西情報センター 等 3機関

認証取得企業数

17,154社

具体要件

- ・ 詳細な審査基準は、JIPDECが専用サイトにて公開しているが、申請にあたっては、少なくとも以下の条件を満たしている必要がある
 - JISQ 15001に基づいた「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」に即し、個人情報保護マネジメントシステム（PMS）を定めていること
 - PMSに基づき、実施可能な体制が整備されて個人情報の適切な取扱いがおこなわれていること
 - PMSの運営体制として、正社員又は登記上の役員の従業者が2名以上在籍していること
- ・ 加えて、申請には、PMSを運用した記録と規程類の提出が必要であるため、マネジメントシステム原則に基づいた計画の作成（P）、実施（D）、点検・評価（C）、改善（A）というPDCAサイクルを少なくとも1回以上実施しておく必要がある

手続き/作業

1. PMS構築・運用
2. 必要書類の提出・申請
3. 審査
4. 付与適格決定・契約締結
5. マーク使用開始

取得にかかる期間（目安）

約1年程度（準備期間4カ月、審査期間6カ月～）

更新と取消

有効期間は2年



6 JAPHICマーク

概要

JAPHICマーク制度は、日本の個人情報保護法及び当該法に基づくガイドラインに準拠して、個人データについて適切な保護措置を講ずる体制を整備・運用している事業者を認定する制度。既に日本で広く普及しているプライバシーマークに類似している。プライバシーマークと比較して取得コスト（費用、時間）が低く、近年、中小事業者を中心に注目されている。

制定の背景

2003年のAPPI成立とその後の改正に伴い、個人データ保護体制の第三者認証を求める声が増加。既にプライバシーマーク制度が存在したものの、コスト負担（特に費用及び時間）の問題もあり、一部事業者にはハードルが高い面があった。

そのような状況を踏まえ、他の認証と比べて低コストで取得可能、且つ、プライバシーマークと同様に入札案件にも対応可能な資格として、JAPHICマークが創設された。

準拠法令・規格

- 日本 個人情報保護法
- 個人情報の保護に関する法律についてのガイドライン
- 特定個人情報の適正な取扱いに関するガイドライン

制度の詳細

申請/認証対象

日本国内に拠点を置く事業者

申請/認証単位

- 法人：法人又は事業部書単位
- 個人事業主：事業主単位

運営機関

- 運営：JAPHICマーク認証機構
- 審査：株式会社PICC 等 3機関

認証取得企業数

359社

具体要件

- 審査基準の詳細は、JAPHICマーク認証機構が自己評価表の形で公開している。各評価表で求められる主な事項は以下の通り
 - 個人情報保護法の基本事項
 - 個人データの取得、利用目的の制限、委託、漏洩対応 等
 - 特定個人データの取扱いに関する事項
 - 特定個人データの取扱制限、安全管理措置、漏洩対応 等
- 上記に加えて、外国にある第三者への提供等、のガイドラインが適用される事業者は、各ガイドラインに基づく審査も必要

手続き/作業

1. 申請資格の確認
2. 自己評価の実施
3. Web申請
4. 認定審査機関による審査（文書審査/現地審査）
5. 判定
6. マーク・認証書発行

取得にかかる期間（目安）

約1-2か月

- 認証日は毎月1日、審査完了翌月1日が認証日となる

更新と取消

1年



7 EuroPriSe

概要

IT製品およびITを利用したサービスが、欧州のデータ保護規制に準拠していることを認証する制度。透明性の高いプライバシー証明書を提供することで、消費者と市民権の保護、マーケティングメカニズムによるプライバシー保護を提供し、最終的にITへの信頼を高めることを目的としている。

なお、2022年9月時点で、EuroPriSeは、GDPR (42条) に定められたEDPBによる承認を受けていないため、EuroPriSeの取得がすなわちGDPRへの準拠を証明するものとはなっておらず、運営機関であるEuroPriSe GmbHは、EDPBによる認証の採用を目指している。

制定の背景

EUによるデジタルサービスの展開促進プログラムの一環としてドイツ シュレースヴィヒ=ホルシュタイン州のデータ保護局の下、2007年から試験的に運用が開始された。
2014年以降は、EuroPriSe GmbHが管理・運営を担当している。

準拠法令・規格

EuroPriSe基準

- GDPRのほか、ePrivacy Directiveなど、データ保護に関連する他の欧州のデータ保護規制の要件を統合

制度の詳細

申請/認証対象

IT製品及びIT関連サービスのベンダー

申請/認証単位

法人

運営機関

EuroPriSe GmbH

認証取得企業数

12社¹

具体要件

EuroPriSe Criteriaは、以下の4つの項目で構成される

- ① 基本事項の確認
 - データ利用目的やサービスの基本的な技術構成 等
- ② データ処理の正当性
 - データ処理の法的根拠 等
- ③ 技術的・組織的措置
 - データ処理のリスク判断及び、対象のセキュリティレベルが適正か 等
- ④ 個人データの権利
 - 通知義務やデータのアクセス/修正義務 等

手続き/作業

1. 必要書類の提出・申請
2. 契約書へのサイン
3. 審査
4. 付与適格決定
5. 証明書の発行

取得にかかる期間 (目安)

3-5カ月 ※申請者の事前準備期間を除く

更新と取消

2年

1. eTENプログラム。eTENプログラムは2006年に終了し、2007年以降は、ICT PSPに引き継がれた ([European Commission "eTEN programme"](#))

2. 2022年9月時点でEuroPriSe HP上で有効期間内となっている企業数をカウント

Source: [EuroPriSe GmbH "EuroPriSe Criteria for the certification of IT products and IT-based services \(v2710701\)"; EuroPriSe HP](#)



8 TRUSTeマーク

概要

TRUSTeマークは、対象のWebサイトのOECDプライバシーガイドラインの遵守を承認する制度。他の認証制度の多くが、事業者を対象としているのに対して、Webサイト、アプリを認証対象としている。また、運営機関がユーザーからの苦情の一次受けを担う、損害賠償保険を付帯しているなど、他の認証制度にはない多くの特徴を持つ。

発祥は米国だが、グローバルで多数の認証実績を持つため、認証の取得によりグローバルでの信頼性の醸成に有用。

制定の背景

1996年のPCフォーラムにおける「電子商取引の発展には、「信頼」が重要」という主張を受け、インターネット活動（電子商取引）の健全な発展を目的に1997年に米国で誕生。

準拠法令・規格

OECDプライバシーガイドライン

制度の詳細

申請/認証対象 (単位)

ドメインもしくはアプリ単位

運営機関

- 運営: TrustArc
- 審査: JPAC (日本プライバシー認証機構) 等 2機関

認証取得ウェブサイト数

529サイト

具体要件

- 審査基準として、個人データの取扱いに関する19項目が定められている
 - 取得の制限、保存、要配慮個人データの取扱い 等
- 実際の審査では、自己査定の内容が確認される。なお、自己査定書には以下のような項目が定められている
 - ① 個人データの取得・利用・保管 (取得する個人データの詳細等)
 - ② Webサイト利用者のへのアクセス
 - ③ 個人データの第三者提供の実現方法
 - ④ 個人データの正確性及び再申請の担保
 - ⑤ セキュリティ体制
 - ⑥ 個人データ保護マネジメント (データの取扱い方針)
 - ⑦ 苦情対応

手続き/作業

1. 自己査定
2. 認証機関への申請
3. 認証機関による審査
4. 審査完了・認証付与 (専用ページの作成、認証マークの付与)

取得にかかる期間 (目安)

約2カ月

更新と取消

1年



9 CNIL認証

概要

フランスのデータ保護機関CNIL (Commission nationale de l'informatique et des libertés: 情報処理及び自由に関する全国委員会) が運営する、個人データ処理に関して、十分な保護措置を講じていることを証明する認証制度。取得により、管理者は、個人データの処理に関する優位性や信頼性を証明することができる。

EuroPriSe同様、EDPBの承認を受けた認証ではないため、GDPRに定められたDPOの職務の遂行に必須の認証ではない。しかしながら、CNILは、GDPR違反をめぐりメガテックへの指摘をおこなうなど、個人データ保護に積極的であり、その期間が運営する認証として着目される。

制定の背景

CNILでは、EUデータ保護指令時代から、個人データ保護水準を証明する認証ラベルの発行をおこなってきた。

2018年のGDPR施行に伴い、EUデータ保護指令に準じたラベルの付与は終了され、GDPRに準拠したDPO (Data Protection Officer: データ保護責任者) 認証に移行した。

準拠法令・規格

- フランス データ保護規則
- GDPRセクション4第4章

制度の詳細

申請/認証対象

- フランスに事業所を有する又はフランスに居住し、以下のいずれかの要件を満たす個人データの処理者で、以下の要件を満たす者
 - 関連するプロジェクト、活動等における専門的な経験 (最低2年) 及びその証明
 - 個人データの保護に関するトレーニングの受講 (最低35時間)

申請/認証単位

個人

運営機関

- 運営: CNIL
- 審査: International Privacy Association of Privacy Professionals 等 9機関

認証取得者数

n/a

具体要件

DPO認証の審査については、以下の項目を含む17の認定基準が定められている

- 処理の合法性、目的の制限、データの最小化、データの正確性、限定的なデータ保持、完全性、機密性、および説明責任の原則の理解
- 内部データ保護ポリシーまたはルールの作成
- 監督当局及びデータ主体への通知を含む個人データ侵害時の対応の整備
- データ保護影響分析 (DPIA) の必要性の判断と実行
- スタッフ等の教育

手続き/作業

- 認定機関への申請
- 認定機関により事前審査 (申請資格の審査)
- 受験
- 結果通知、証明書発行

取得にかかる期間 (目安)

n/a

更新と取消

- 3年
 - 有効期間終了時の再受験、最低1年の専門的な経験の証明により、更新が可能



10 ISMS-PIMS認証 (ISO/IEC 27701)

概要

国際規格 (ISO/IEC 27701) に基づき、組織が有する多種の情報セキュリティ確保の仕組みへの適応性を評価する制度。正式名称である「ISO/IEC 27701:2019 セキュリティ技術—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への拡張—要求事項及び指針」が表す通り、プライバシー管理に特化した規格として、ISO/IEC 27001及び27002のアドオン規格 (認証)¹ の位置付けにある。認証の取得により、グローバル標準に従って、プライバシーを適切に保護・管理する体制を備えていることを対外的に証明できる。世界で個人データ保護規制が乱立する中、プライバシー管理に関する国際認証として注目が高まっている。

情報セキュリティに関する規格にはISO/IEC 27000や27001などが存在し、ISO/IEC 27000シリーズとして知られている。
ISO/IEC 27701もその中の1つであり、個人情報マネジメントシステム (Privacy Information Management System : PIMS) に特化していることから、通称ISMS-PIMSと呼ばれる

制定の背景

2019年8月に発行された比較的新しい認証 (規格)。ISMS-PIMS認証誕生以前も、ISO/IEC 27002及び29151を用いて個人情報保護対応とすることは可能であった。しかしながら、ISO/IEC 27002及び29151は、いずれも管理策の定義を主としており、運営フレームワーク (マネジメントシステム) を定義するものではなかったため、個人情報保護マネジメントシステムを定義する規格としてISO/IEC 27701が、その評価制度としてISMS-PIMS認証が開発された。

準拠法令・規格

ISO/IEC 27701

制度の詳細

申請/認証対象者

情報セキュリティマネジメントシステムの中で個人情報²を処理する管理者及び/又は処理者
- 公共及び民間企業、政府機関及び非営利団体を含むあらゆる種類及び規模の組織

1. 単独取得不可。ISO/IEC 27001認証 (ISMS認証) の取得が前提となる (ISO/IEC 27002には適応性評価制度がなく、認証として機能していないため、ISO/IEC 27002の認証は前提となり得ない) 2. 「PII (Personally Identifiable Information: 個人を識別できる情報)」 3. [ISMS-PIMS認証機関一覧](#) 4. [ISMS-PIMS認証取得組織一覧](#) (2022年12月時点) 5. 「ISO/IEC 29100:2011 情報技術—セキュリティ技術—プライバシーの枠組み」 6. 「ISO/IEC 27018:2019 情報技術—セキュリティ技術—PIIプロセッサとして作動するパブリッククラウドにおける個人識別情報 (PII) 保護のための実施基準」 7. 「ISO/IEC 29151:2017 情報技術—セキュリティ技術—個人を特定できる情報保護のための実施基準」 8. 有効期限が2024年1月までのISMS認証を持つ組織が、2023年1月にISMS-PIMS認証を取得した場合、ISMS-PIMS認証はISMS認証と同じ2023年1月有効期限となる
Source: [ISO "ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines"](#)

制度の詳細

申請/認証単位

法人・事業部門等

運営機関

- 管轄: ISO (International Organization for Standardization: 国際標準化機構)、IEC (International Electrotechnical Commission: 国際電気標準会議)
- 認証: 外部認定機関 (多数)³

認証取得企業数

- 日本は39社⁴

具体要件

- アドオン認証であるため、基本的にPIMS固有の要件 (追加要件) が列挙されている
- 個人情報保護においては、組織の状況や各国/地域規制等の前提条件により適用すべき要件が影響を受けるため、以下の規格/規制とのマッピングが附属書で定義されている
 - ISO/IEC 29100⁵で定義されたプライバシーフレームワークと原則とのマッピング (附属書C)
 - GDPRとのマッピング (附属書D)
 - ISO/IEC 27018⁶ 及び 29151⁷ とのマッピング (附属書E)

手続き/作業

- ISMS認証取得済みの場合は、追加要件部分のみの審査
- ISMS認証未取得の場合は、ISMS認証の取得手続きの中に織り交ぜて同時取得が可能

取得にかかる期間 (目安)

数か月 ※ISMS認証の取得状況により異なる

更新と取消

- 3年 ※ISMS認証のアドオンとなるため、ISMS認証の有効期限に影響を受ける⁸



11 個人情報安全規範

概要

国家情報安全規範 (GB/T 35273-2020 信息安全技術 个人信息安全规范) は、組織又は個人による個人データの処理¹に関する具体的な取扱いの基準を定めた国家標準。法的な強制力は持たないが、個人データ保護の取扱いについて、全般的に規定した国家標準として、実務上の重要なガイドラインとなっている。
個人データの越境移転においても、標準の遵守が大前提となる。²

制定の背景

2017年施行のCSLの下、個人データに関する全般的な取扱い規範として公布された (GB/T 35273-1717)。
その後のIT技術の進展を受け、2019年以降、時代に適応した新たな事項を追加する必要性が高まり、2020年に改正がおこなわれた (GB/T 35273-2020)。
改訂版では、個人データの収集に関する基準が厳格化され、新しいビジネスモデルに関する取扱い基準が追加されるなど、個人情報管理者への要請が強められている。

準拠法令・規格

- なし
- CSLの下で整備されているが、本規範自体が規格であるため、厳密には準拠法令・規格は存在しない

制度の詳細

管轄機関

国家標準化管理委員会

対象

個人データを取り扱う組織

規格要件

- 個人情報の使用・管理に関する基本原則を列举。特に個人情報の収集等に関しては、マーケティング (パーソナライズ) 等、具体的な利用状況を挙げたうえで、求められる要件を列举している
 - 情報主体の権利
 - 個人個人情報安全基本原則
 - 個人情報の収集
 - 個人情報の保存
 - 個人情報の使用
 - 個人情報の処理委託、共有、譲渡及び公開開示
 - インシデント対応
 - 組織の個人情報安全管理要求

1. 具体的には、収集、保存、使用、共有、譲渡、公開開示、削除等が含まれる 2. 個人情報越境処理保護認証前文

Source: 国家標準化管理委員会「标准号：GB/T 35273-2020」2020年；森・濱田松本法律事務所「中国最新法令 <速報>」2020年4月3日号



12 JIS Q 15001

概要

JIS Q 15001は個人データ保護を目的として、組織が個人データを適切に管理するためのマネジメントシステムの要求事項を定めた規格。JIS Q 15001に準拠することで、効果的・効率的な個人データ管理を実現することができる。また、ISO/IEC 27001と組み合わせることで、より強力な効果的なセキュリティ管理体制を構築することができる。

JIS Q 15001自体は認証ではなく規格だが、JIS Q 15001に基づく認証（プライバシーマーク）も提供されている。

制定の背景

1980年代以降、OECDプライバシーガイドラインの制定や、EUデータ保護指令の制定など、個人データ保護に関する国際的な機運の高まりを受けて、1998年にはPマーク制度が開始された。しかしながら、Pマーク制度は経済産業省が管轄するガイドラインをベースとしていたため、個人データ保護の取組みが経済産業省が管轄業界に限られることが懸念された。そこで、業界横断的な取組身としてのJIS化がすすめられ、1999年にJIS Q 15001が誕生した（JIS Q 15001:1999）。なお、当時の日本には個人データ保護に関する包括法が存在していなかったため、民間部門における個人データ保護に関するガイドライン¹とEUデータ保護指令をベースに規格化が図られた。

その後、日本における個人データ保護の包括法（APPI）の制定及び改正、国際的な動き（特にGDPR）を受けて、JIS Q 15001も改訂を重ねている（JIS Q 15001:2006 及び 2017）。

準拠法令・規格

なし

- JIS Q 15001自体が規格であるため、厳密には準拠法令・規格は存在しない。
- ただし、APPI、その他のマネジメントシステム規格と整合性が図られている

制度の詳細

管轄機関

JQA (Japan Quality Assurance Organization: 日本品質保証機構)

対象

- 個人データを取り扱う組織

規格要件

- 組織が利用する個人データに関するマネジメントシステムを確立するための要件を規定
- 特に附属書にて、詳細且つ具体的に管理項目を提示している
 - 附属表はISOとの近接性を保つ内容が規定されている²

1. 「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」（1997年）を指す（JADAC「JIS Q 15001 改正に至る経緯」日本データ通信 No.219（2018年））


2. JIS Q15001 解説において、個人情報保護と情報セキュリティとは安全管理措置の点で共通する事項が多いことから、統合版ISO 補足指針の附属書SLとの整合を意識している旨が記載されている

Source: JQA「JIS Q 15001（個人情報保護）」；JISA「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」



関連ツール 調査対象

調査対象国/地域で利用されているデータ保護関連ツールのうち、特に主要なものを列举

		名称	対象国/地域	準拠法令/規格	申請/認定対象	
個人データ 保護	認証		1 GDPR-CARPA	EU (ルクセンブルク)	一般データ保護規則 (GDPR)、 ISO規格 等	事業者、公共機関、その他団体等
			2 dp.mark	台湾	台湾 個人データ保護法 (PDPA)、 その他国際ルール 等	事業者
			3 データ保護トラストマーク (Data Protection Trust Mark: DPTM)	シンガポール	シンガポール 個人データ保護法 (PDPA)	公共機関以外の組織
			4 情報保護及び個人情報保護管理体系認証 (ISMS-P認証)	韓国	韓国 個人情報保護法 (PIPA)	データ通信サービス提供事業者 等
			5 プライバシーマーク (Pマーク)	日本	Pマーク運用指針 ※JIS Q 15001に準拠	事業者
			6 JAPHICマーク	日本	日本 個人情報保護法 (APPI)、 その他関連ガイドライン	事業者
			7 EuroPriSe	ドイツ	EuroPriSe基準 ※GDPRに対応	IT製品及びIT関連サービスベンダー
			8 TRUSTeマーク	グローバル	OECD プライバシーガイドライン	ドメイン、アプリ
			9 CNIL認証 (Certification des compétences du DPO: DPOスキル認定)	フランス	一般データ保護規則 (GDPR)、 フランス データ保護規則	個人データの処理者 (個人)
			10 ISMS-PIMS認証 ¹	グローバル	ISO/IEC 27701	事業者、事業者内の部門
規格			11 個人情報安全規範	中国	—	—
			12 JIS Q 15001	日本	—	—
一般データ 保護	認証		1 ISMS認証 ¹	グローバル	ISO/IEC 27001	事業者、事業者内の部門
			2 WebTrust	グローバル	認証局のためのWebTrust規準	事業者 (電子認証サービス事業者)
	規格		3 NIST SP800シリーズ	米国	—	—
			4 SOC2 (Service Organization Control Type2)	米国	—	—

1. ISO/IEC規格として整備されている規格のうち、いくつかの規格は、適合性評価制度を持つ。適合性評価制度を持つ場合、ISO/IEC規格への適合認証がなされる。ISO/IEC27001及び27701はいずれも適合性評価制度を持つため、ここでは規格ではなく認証として分類する



1 ISMS認証 (ISO/IEC 27001)

概要

国際規格 (ISO/IEC) に基づき、組織が有する多種の情報セキュリティ確保の仕組みの構築を認証する制度。組織が有するすべての情報資産を保護対象としており、認証の取得により、組織が広くデータ保護体制を整備していることが証明される。

情報セキュリティに関する認証には、同じISO/IEC内でもISO/IEC 27000、ISO/IEC27001などが含まれ、ISO/IEC27000シリーズとして知られている。
ここでは、情報セキュリティに関する要求事項を取扱うISO/IEC 27001を紹介する。

制定の背景

1999年に発行された英国の独自規格であるBS7799-2 (Information Security Management Systems: 情報セキュリティ管理システム仕様) を基に作成された。BS7799-2は、国際的な情報管理の動向も捉え、2002年にPDCAの考え方を組み込む改訂が行われ、一部国際規格との整合性が図られ、2005年にISO/IEC27001として採用・統一された¹。

準拠法令・規格

ISO/IEC 27001

制度の詳細

申請/認証対象者

情報セキュリティに関するリスク評価に基づき事業者が必要と判断した事業部門等

申請/認証単位

法人・事業部門等

運営機関

- 管轄: ISO (International Organization for Standardization: 国際標準化機構)、IEC (International Electrotechnical Commission: 国際電気標準会議)
- 認証: 外部認定機関 (多数)²

認証取得企業数

- グローバルでは、58,687社³
- 日本は6,587社³

具体要件

情報セキュリティに関する要件とは、具体的には「機密性」「完全性」「可用性」の3要素を指す

- 機密性: 許可されたユーザーのみが情報にアクセスできる状態
- 完全性: 情報が正確な状態で保存され、改ざんや消去ができない状態
- 可用性: 必要なときに許可されたユーザーがいつでも問題なく情報へアクセスできる状態

手続き/作業

1. 事前準備 (取得範囲の選定、体制の確立等)
2. 審査申込
3. 第1段階審査 (文書審査)
4. 第2段階審査 (現場審査)
5. 審査完了、認証取得

取得にかかる期間 (目安)

数か月

更新と取消

- 3年
 - 有効期間内に、半年～年1回、継続審査が必要
 - 更新には、有効期間終了前に更新審査が必要



2 WebTrust

概要

WebTrustは、北米で開発された国際的な電子商取引認証プログラム。インターネット事業者の国際的な電子商取引保証規準に基づく電子商取引を審査し、認証する。各種証明書を発行する事業者がWebTrustを取得することで、その事業者が提供・運用するサービスの信頼性を証明できる。北米発祥だが、現在は、グローバルに利用されている。

制定の背景

オンラインサービスの普及に伴うWeb上での購入に対する消費者の不安を和らげるため、開発された¹。

準拠法令・規格

なし

制度の詳細

申請/認証対象

すべての地域にある企業

申請/認証単位

法人

運営機関

- 管轄: CPA Canada (Chartered Professional Accountants Canada: カナダ公認会計士協会)²
- 認定審査: Deloitte 等 Practitionerとして認定された19社³

認証取得企業数

n/a

具体要件

申請者が提供するサービスにより、必要とされる基準が異なる

- Principles and Criteria for CA
- Principles and Criteria for CA - SSL baseline with Network Security
- Principles and Criteria for CA - Code Signing Baseline Requirements
- Principles and Criteria for CA - Extended Validation SSL
- Principles and Criteria for Verified Mark Certificates
- Principles and Criteria for Registration Authorities

以下の内容が主に審査される⁴

- 運営方式の開示
運営方式を開示し、開示した内容に基づき取引を実行していること
- サービスの完全性
消費者の同意通りに取引がなされ、正確に請求するための体制が整備されていること
- 情報の保護
消費者の個人情報について、開示している運営方式に定められていない利用から保護される体制が整備されていること

取得にかかる期間 (目安)

n/a

手続き/作業

大まかには以下の流れで手続きが進められるが、詳細は各Practitionerの指示に従う

- 事前準備
- 審査
- 認証 (保証書発行)

更新と取消

1年

1. [Journal of Accountancy "In CPAs We Trust" 1997](#) 2. 制度の開発は、AICPA (American Institute of Certified Public Accountants: 米国公認会計士協会) とCICA (Canadian Institute of Chartered Accountants: カナダ公認会計士協会) 4. CPA Canada HP上で2022年9月時点で公開されている事業者数をカウント 4. [GMOグローバルサイン「WebTrust \(ウェブトラスト\) について」](#)
Source: [CPA Canada "WebTrust Seal Program"](#)



3 NIST SP800シリーズ

概要

米国政府機関が定めたセキュリティガイドライン。Special Publications (SP) 800シリーズは、セキュリティマネジメントやリスクマネジメント、セキュリティ技術、セキュリティ対策状況の評価などが幅広く網羅されている。

同機関が定めるCyber Security Framework (CSF) の下位概念に位置する。SP800シリーズに比較して、CSFはより包括的な内容となっているため、実務者間では主にSP800シリーズが活用されている。

SP800シリーズには、SP800-53とSP800-171、SP800-40などいくつかに分けられる¹。ここでは、情報の機密性保護のために、政府が推奨するセキュリティ要件を提供しており、民間事業者向けの内容となっているSP800-171を紹介する。

制定の背景

ITの普及に伴い、ITが国家の重要インフラとなったことから、情報セキュリティ対策が経済だけでなく国家安全保障上も重要な課題となった。そこで米国政府は、2002年に連邦情報セキュリティマネジメント法 (Federal Information Security Management Act: FISMA) を制定し、各政府機関に対して情報セキュリティの開発・強化を義務付け、特に米国国立標準技術研究所 (National Institute of Standards and Technology: NIST) には、連邦政府のFISMA対応の支援が命じられた。

NISTでは2003年にFISMA導入プロジェクトを立ち上げ、各種規格・ガイドラインの制定をすすめるに至り、2015年にSP800-171が発効された (2020年に改訂)。

準拠法令・規格

なし

制度の詳細

管轄機関

NIST

対象

- 調達から販売・供給までの一連のサプライチェーンに存在する、業務委託先や関連企業のすべて
 - 例) システム開発ライフサイクル管理の責任者、取得または調達責任者、システム・セキュリティ・リスク管理及び監督の責任者、セキュリティ評価・監視責任者

規格要件

SP800-171 では、14種類のセキュリティ要件 (Security Requirements for Protecting the Confidentiality of CUI: 連邦政府外のシステム及び組織におけるCUIの機密性保護のセキュリティ要件) が定められている

1. アクセス制御
2. 意識向上と訓練
3. 監査と責任追跡性
4. 構成管理
5. 識別と認証
6. インシデント対応
7. メンテナンス
8. メディア保護
9. 人的セキュリティ
10. 物理的保護
11. リスクアセスメント
12. セキュリティアセスメント
13. システムと通信の保護システムと情報の完全性

1. SP800-53 は政府機関向け、SP800-40は脆弱性・パッチ管理について定めている



4 SOC2 (Service Organization Control Type2)

概要

SOC2 (Service Organization Controls 2) は、AICPAが定める委託会社の内部統制やサイバーセキュリティについての内部統制保証報告 (Service Organization Control Reporting: SOC報告書) の1つ。特に外部事業者がによるリスク統制に言及している。SOC2にはType1とType2があり、Type1は基準日時点での評価、Type2は1年など期間評価となっている。評価の結果、何らかの認証が付与されるものではなく、評価内容が報告書として公開され、それにより対象者のセキュリティ統制レベルを示すものとなっている。

制定の背景

2000年前半に相次いだ巨額粉飾事件を受けて、米国では内部統制を含む財務報告の有効性評価の義務付けがおこなわれ¹、AICPAはその有効性評価の保証基準としてSSAE16 (Statement on Standards for Attestation Engagements No.16) を2010年に発表。加えて、AICPAは、SSAE16に基づく報告枠組みとしてSOC²を開発・発表した。

準拠法令・規格

なし

制度の詳細

管轄機関

- AICPA

対象

米国を含む全世界の情報システムの関連事業者 (アウトソーシング事業者及びその顧客等)

規格要件

サービス規準 (Trust Service Criteria) には以下5つが含まれ、そのうちセキュリティは必須要件となっている

- セキュリティ: 不正アクセスに対する保護
- 可用性: プロセスの全般機能
- 処理のインテグリティ: 処理の適切性 (完全性、正確性、適時性等)
- 機密保持: 機密指定された情報の合意に準じた保護
- プライバシー: 個人データの取扱いの適切性

手続き/作業

報告書の作成は、おおまかには以下の流れで進められる。詳細は各監査機関の指示に従う

1. 事前準備
2. 審査
3. 認証 (保証書発行)

SOC2には、任意の規準を追加したSOC2+も存在する。

例えば、米国では、NIST SP800を追加したSOC2+評価等、積極的に利用されており、事業者のニーズに合わせた利用が推進されている。

1. SOX法 (Public Company Accounting Reform and Investor Protection Act of 2002) 2. SSAE16は財務報告に係る基準であり、SOC報告書の中でも財務報告にかかる内部統制について定めているのは、正確にはSOC1となる。SOC2及びSOC3は財務報告に関連しない内部統制について定めている

Source: AICPA "TSP Section 100 2017 Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy" 2020; EY「情報センサー2016年12月号 クラウドセキュリティに関する第三者評価・認証制度の概要ISO/IEC 27017認証、SOC2およびSOC2+」2016年

Agenda

1. 本事業の位置づけ
2. データ越境移転関連調査
- 3. 事業者によるツール等の活用実態調査
 - 3.1 調査の目的・アプローチ
 - 3.2 調査結果サマリ
 - 3.3 事業者のヒアリング結果 (詳細)
4. 調査結果のまとめ



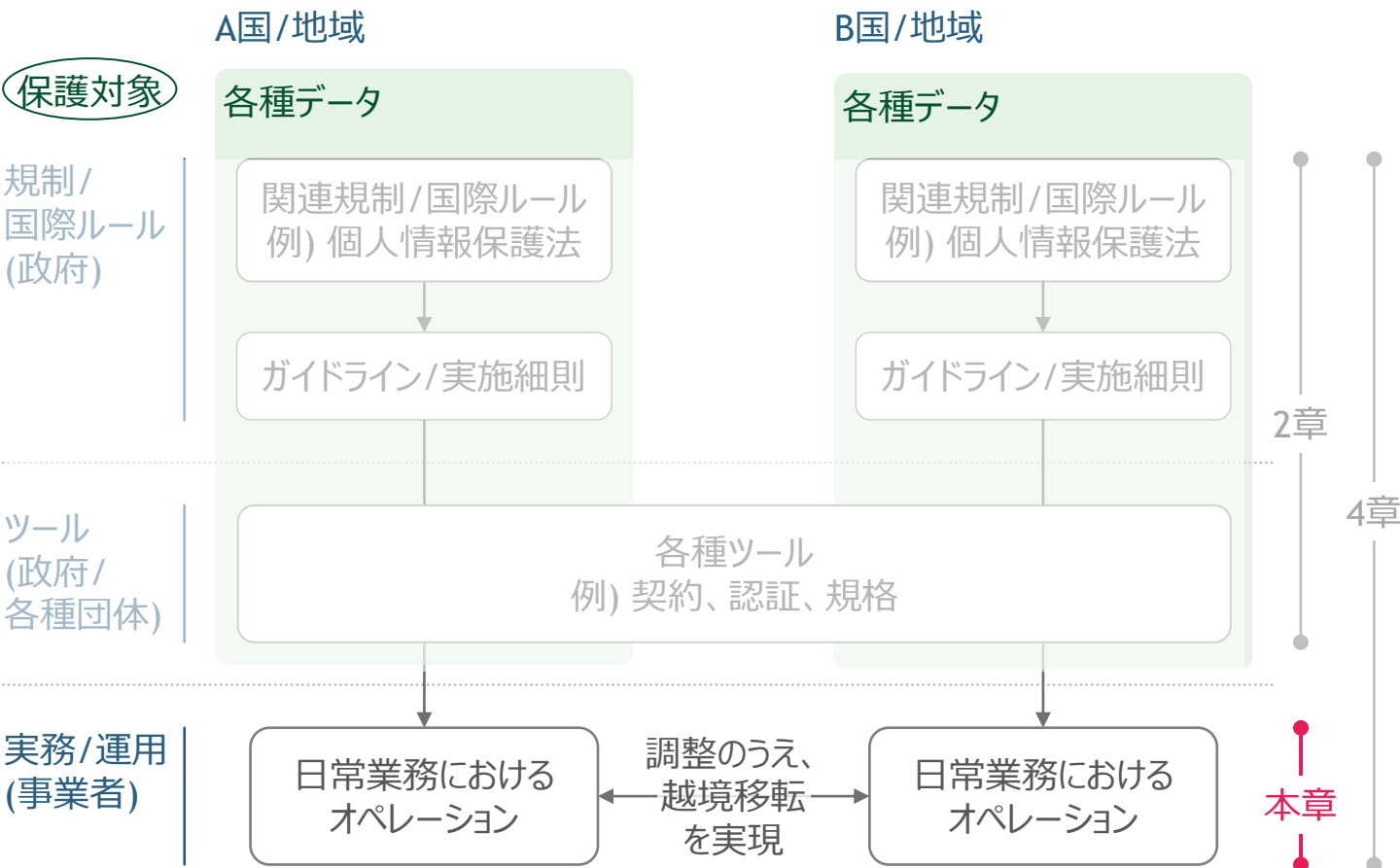
3.1

調査の目的・アプローチ

本章の目的

データの越境移転の実務

データの越境移転自体は、事業者の日常業務内で実現されるが、そのために、各事業者は、関連する規制の履行と、ツールの活用を行っている



目的

前章までの調査結果を踏まえて、実際にデータの越境移転を担う事業者の越境移転に関するニーズと、規制/ツールの現状とのギャップを明らかにする。

調査は、データの越境移転をおこなっている事業者へのインタビューを通じておこない、実際のデータの越境移転にあたり、各国/地域規制からどのような影響を受け、又、各ツールをどのように活用しているか、調査する。

「データ越境のパターン」×「ユースケース」の組み合わせを網羅するかたちで、対象事業者を選定、計16社に対し、インタビューを実施

データ越境のパターン：7種

欧州型: GDPRの対象地域

- ① 欧州 → 十分性認定あり
- ② 欧州 → 他地域 (SCC/BCR)
- ③ 欧州 → 米国

中国型: 国内保存義務を有する地域

- ④ 中国（インド/ベトナム）↔ 他国

アメリカ型: 欧州型、中国型以外の地域

- ⑤ 米国 → 他国

多国間枠組み型: CBPR参加地域

- ⑥ 枠組み内企業→枠組み内企業
- ⑦ 枠組み内企業→枠組み外企業



データユースケース：3種

a) 事業運営

- 利用者の個人情報やサービスで収集可能な情報を想定
- オフショア利用のため越境データの第三国への越境の例も含む

b) 研究開発

- 機器の稼働データ等の収集データ等、重要産業情報を想定

c) 社内運営

- 人事データ / グローバルITガバナンス等を想定

データ越境のヒアリング調査対象企業

	(a) 事業運営	(b) 研究開発 (重要産業情報)	(c) 社内運営 (人事/グローバルIT)
欧州型	① 欧州 → 十分性認定取得地域	① インタネットサービス会社 ② 鉄道会社 ③ アパレル会社	⑤ 製薬会社 ⑩ 住宅製品メーカー ⑪ 消費者調査会社
	② 欧州 → 他地域	③ アパレル会社	-
	③ 欧州 → 米国	-	⑨ 米国機器メーカー
中国型	④ 中国 (インド/ベトナム) ⇄ 他国	② 鉄道会社 ③ アパレル会社	⑤ 製薬会社 ⑩ 消費者調査会社
米国型	⑤ 米国 → 他国	① インターネットサービス会社 ② 鉄道会社 ③ アパレル会社	⑤ 製薬会社 ⑩ 住宅製品メーカー ⑪ 消費者調査会社
他国間 枠組み 型	⑥ 枠組み (CBPR) を活用している地域間	① インターネットサービス会社 ④ 中国ゲーム制作会社	⑩ 住宅製品メーカー ⑪ 消費者調査会社
	⑦ 枠組み (CBPR) 外 → 枠組み (CBPR) 内	-	⑤ 製薬会社
グローバル統一基準で管理	⑫ ネットワーク機器メーカー ⑬ インターネットサービス会社 ⑭ クラウドベンダ ⑮ IT会社 ⑯ インターネットサービス会社	-	-

事業者ニーズ・ギャップに関するヒアリング項目

カテゴリー

ヒアリング項目

前提の確認

- 関連規制/
越境データ 等

データの越境が発生している国 / 地域はどこか？
各国のデータ保存場所と保存方法はどこか？
各データの利用用途及び、利用者/ユースケースは何か？
各データ毎にどのような越境に関する規制が適用されるか？
越境するデータの種別 (マーケティング/人事/研究開発)/項目は何か？

各規制への対応

- 活用する
ツール等

各国の個人情報保護規制にどのように対応しているか？
現状、利用しているツールは何か？ (欧州型、米国型、他国枠組み型を確認)
なぜ、そのツールを利用しているのか？ どのように対応方針を策定したのか？
現状のツールやツールの利用に関する利点は何か？
現状のツールやツールの利用に関する課題や改善すべき点は何か？

- "そもそも活用できるツールがなく、越境できないことによりビジネスを諦めた"
- "ツールの対応や調査に要する費用/期間が負担"/"予見可能性が低い" 等

 ツール以外に、データ保護に影響を与える要因 (業界ルール等) と、その対応方法の確認は何か？

あるべきデータ流通

ある一定の基準／ハードルをベースに自由度の高い越境データ流通 (DFFT) が実現した場合、
どのようなビジネスチャンスが広がると考えるか？ 特にどのような地域/データにおいて、その重要性が高いか？

※「中国型」事業者への 確認事項

ビジネスの関係でデータ国内保存義務が発生する国と地域 (中国型を確認) はどこか？
国内保存義務が発生しているデータ種別と項目は何か？
各国におけるデータ保存場所と保存方法 (オンプレミス/クラウド?) は何か？
国内保存義務とそれ以外の国では、各データの現地での運用方法やユースケースは、どのように異なるか？
ビジネスの関係で、特に喫緊の改善が必要なポイントは何か？



3.2

調査結果サマリ

企業のニーズ/課題と、各越境ツールの導入メリット

越境ツール	事業会社 (取扱データ)	各社コメント (ニーズや課題)	各越境ツールの導入メリット/デメリット
BCR	クラウドベンダ (SaaS内の個人情報)	<ul style="list-style-type: none"> ある国のデータセンター内の顧客データを、SaaSサービス提供目的で他国のチームが触ることがある ⇒ SaaSのサービス運用上でのデータ越境ケースを見据えて、グローバルで共通のデータ越境ルールを持ちたい 	<ul style="list-style-type: none"> グローバルでデータ管理をするSaaSビジネスにおいては、一度承認されると世界各国のグループ内企業へ適用可能なBCRのスケールメリットが活かされる
	インターネットサービス会社 (EC顧客データ等)	<ul style="list-style-type: none"> 自社PFサービスのデータ運営体制のアピール・信頼獲得のために認証を取得 各国支社には、弁護士資格を有するものが存在し、逐次法規制や情勢を確認、その上でグローバルで統一されたデータガバナンスを実現している 	<ul style="list-style-type: none"> BCR対応の法務体制/データガバナンスが信用獲得効果を持つ 法的拘束力もあるため、各国データ保護規制の解釈や、それに準拠するための要件の具体化に関するコスト負担が重い BCRで明記されていないがデータガバナンス体制・運用の確立は必須 (認証要件ではないがCBPR相当が必要)
SCC	製薬会社 (カルテ/安全性情報、社内人事データ)	<ul style="list-style-type: none"> 基準が不明瞭で申請を棄却されるリスクのあるBCRを避けて、SCCを採用 	<ul style="list-style-type: none"> 法的解釈含めた要件の具体化の負担が大きいBCRと比較して、準拠要件が明確なSCCは初期対応のコストメリットが存在する
		<ul style="list-style-type: none"> グループ会社が多数あるため、SCCの締結対応にかなり時間がかかった。人事データ統合実現のために全グループ会社とSCCを締結する必要があった 規模の小さいグループ企業にSCCの必要性を理解してもらうのに時間がかかった 	<ul style="list-style-type: none"> グローバルワイドでのデータ越境ニーズに対応する場合は、各国/事業者間で個別契約が必要なSCCではスケールメリットがない
CBPR	IT会社/ネットワーク機器 (社内データ)	<ul style="list-style-type: none"> CBPRのフレームワークやガイドラインに従っていることを確認するためのプロセスや技術を持っていることを証明できるため、それがクライアントの信用に繋がる。ISOやNISTに近いイメージ CBPR自体はカリフォルニア・ニューヨーク州法をサポートしているわけではなく、GDPRのような法的拘束力はない。CBPR準拠 (認証と更新) にお金と時間を投資しなければいけない 	<ul style="list-style-type: none"> 審査基準に定義された各種手続きを含む体制・運用の確立を求められる面が、信用獲得の効果に繋がっている BCRのような法的拘束力がなく更新の必要な認証制度のため、コストに見合う信用獲得効果があるかが採用のポイント ※ ISMSのように公示案件の入札条件等に盛り込む等、一定の拘束力を付与することが求められる
	インターネットサービス会社 (EC顧客データ)	<ul style="list-style-type: none"> 予見可能性の低い (申請棄却/法的違反リスク) BCRを避けSCCを選択 SCCは目的別個別対応(A社とB社間でデータ種類・利用目的別に複数のSCCを結ぶ)であるに対し、CBPRの拡張対応 (A社とB社のデータガバナンス体制の不足分をAB各々対応して特定目的のために越境接合する) の特性に期待 Non-APEC拡大にも期待。中東・アフリカはEU以外の枠組待望 	<ul style="list-style-type: none"> CBPRのトラスト確保に関する拡張的な特性はメリットとして認知されている。 (BCRは予見可能性の低い (監査時の法的違反リスク等) 、個別対応のSCCはツールの拡張性に課題、そもそも中東・アフリカはGDPR以外の枠組待望等)

ヒアリング調査対象企業の越境移転ニーズと活用するツール

各事業者の導入ツールは、まず越境移転の範囲（グループ外企業への越境移転を含むか否か）で分かれる傾向にあった ※詳細次頁

- グループ外企業との越境移転ニーズがある場合：SCCを用い、各国/地域の個別規制に、都度対応することが一般
- グループ外企業との越境移転ニーズがない場合（越境移転ニーズがグループ内に留まる場合）：
 - グローバル共通のデータガバナンスの一括構築を目指す場合は、BCRを採用されることが大半
 - 一方、グローバル共通のデータガバナンスの一括構築を志向しない場合は、SCCが採用されている場合が多い
 - なお、GDPR対応の際、制裁リスクが比較的低いと判断される場合は、BCR/SCC等を用いず、本人同意の取得で対応する例も
- CBPRは、各国規制への対応というよりは、自社のデータガバナンスについて外部からの信用性を獲得するために採用されている
- また、現状、該当する越境移転ツールは存在しないが、グループ外企業とのデータのやり取りも含め、グローバルで体制を構築するニーズも存在している
- また、中国からの越境移転については、ニーズ自体は存在するものの、コストの大きさから断念している例が散見された

各企業がツールを活用する際、各国毎に規制が相違する点や、費用の大きさ、予見可能性の低さ等に負担感があつた

<企業の主な負担>

- **対応すべき規制の多さ**："各国の差分を各企業が都度判断することは負担感が大きい"、"各国の調査に多大な費用が発生"
- **費用/負担の大きさ**：
"数十億円相当の多額の費用を要した"、"対応に多大な人的リソースが必要"、"グループ内の企業との調整が手間"
- **予見可能性の低さ**："規制をどのように解釈すればよいかわからない"、"厳しい解釈をせざるを得ない"、"ユースケースを明らかにしてほしい"

ヒアリング調査対象企業の越境移転ニーズと活用するツール：詳細 (1/2)

越境移転ニーズ	活用する越境移転ツール	企業例
グループ外企業との越境移転ニーズ	A グローバル共通のデータガバナンスの一括構築	該当なし (ニーズはあるが対応できるツールなし)
	B 各国の個別の法規制への都度対応	SCC等の企業間契約 ② 鉄道会社 (現地企業を介する収集データ) ④ 中国ゲーム制作会社 (中国外のデータ) ⑥ 機器メーカ ⑬ インターネットサービス会社
グループ内企業との越境移転ニーズ	C グローバル共通のデータガバナンスの一括構築	BCR ① インターネットサービス会社 ⑫ クラウドベンダ ⑭ ネットワーク機器メーカ
	D 各国の個別の法規制への都度対応	SCC等の企業間契約 ⑤ 製薬会社 ⑨ 米国機器メーカ ⑩ 住宅製品メーカ ⑬ インターネットサービス会社
	D' 最低限の対応 (制裁リスクが低い場合)	社内でプライバシーデータ管理の基準を持ち、既存ツールを使用せず自主的にリスク対応 ① インターネットサービス会社 (BCR移行期間前)
		十分性認定+個人/法人同意 ⑦ 機器メーカ (構想段階、データの越境移転は未開始) ③ アパレルメーカ
グループ内外共通	E データガバナンスに係る信頼性の獲得	個人の同意取得 ② 鉄道会社(現地企業を介さず、ユーザから直接収集したデータ) ⑪ 消費者調査会社
		現行CBPR ⑫ ネットワーク機器メーカ ⑬ インターネットサービス会社 ⑮ IT会社 ⑯ インターネットサービス会社
F 越境を断念 (ニーズ自体は存在)	該当なし	③ アパレル会社: 中国専用の別アプリを作成 ⑤ 製薬会社: 中国データは越境を諦め、中国国内で対応 ⑥ 機器メーカ: 中国地理データは国外移転不可のため、戦略策定は現地法人任せ ⑧ 自動車部品メーカ: データをマスキングした状態で本社に集約

ヒアリング調査対象企業の越境移転ニーズと活用する：詳細 (2/2)

越境移転ニーズ

各ニーズの概要

グループ外企業との越境移転ニーズ	A グローバル共通のデータガバナンスの一括構築	グループ外企業とのデータのやり取りも含め、グローバルで体制を構築するニーズも存在 (現状は該当するツールは無し)
	B 各国の個別の法規制への都度対応	グループ外企業との越境はSCC等の企業間契約での対応のみが可能であるため、各社は越境移転元企業の法規制に即した形の企業間契約の作成が必要
グループ内企業との越境移転ニーズ	C グローバル共通のデータガバナンスの一括構築	グローバルでクラウドサービスを提供するなど、プラットフォームとして多数の法人顧客が想定される場合、BCR (グローバル共通のデータガバナンス実現) 取得が顧客の信頼獲得につながる
	D 各国の個別の法規制への都度対応	BCR取得には数十億円相当のコストが必要であるため、グループ企業間でSCC等の企業間契約を結ぶことを選択する企業が多く存在
	D' 最低限の対応 (制裁リスクが低い場合)	訴訟可能性が低い場合 (例: 扱うデータが社員データのみ) や制裁リスクが小さい場合 (例: 越境移転元国での事業規模がグループ全体比較で小さい) は、データ主体からデータ取扱い同意を取得するのみの対応とし、対応コストを抑えることも可能
グループ内外共通	E データガバナンスに係る信頼性の獲得	CBPRは、現状、各国法規制への対応というよりは、データガバナンス体制の構築についての顧客からの信頼を獲得するための手段として用いられている側面が強い
F 越境を断念 (ニーズ自体は存在)		中国に関しては個人情報及び重要産業データ (地理データ含む) の移転が原則不可のため、越境ニーズはあっても越境を断念する企業が存在

一方でグループ内での越境移転については、SCCのほか、BCRも選択可能。また、制裁リスクを低く見積もる場合はデータ主体の同意取得のみで対応するパターンも存在

取扱いデータ別の越境移転ニーズ及びツールの整理 (大まかな傾向)

越境移転のニーズ (目的)		クラウド/ネットワークサービス上のエンドユーザーの属性/業務データ、グループ内人事データ ¹		B2B顧客データ、研究開発データ、グループ内人事データ ¹		B2C顧客データ、グループ内人事データ ¹	
		C グループ内外を含む越境移転 ＞ データガバナンスに係る信頼性の獲得	E グループ内での越境移転 ＞ グローバル共通のデータガバナンスの一括構築	B グループ外との越境移転 ＞ 各国/地域の規制への個別対応	D グループ内越境移転 ＞ 各国/地域規制への個別対応	D グループ内での越境移転 ＞ 各国/地域規制への個別対応 ＞ 最低限の対応 (制裁リスク: 低)	
対応する越境ツール		✓	✓	✓	✓	✓	✓
ツール概要	対応する越境ツール	CBPR	BCR	SCC/MCC	十分性認定	本人同意	
	内容	<ul style="list-style-type: none">加盟国内での越境移転を可能とする個人データ保護認証求められる個人データ保護体制を整備し、審査を受けて認証を取得する認証制度であるため明確且つ具体的に要件 (基準や申請事項) が示される	<ul style="list-style-type: none">グループ企業間での越境移転を可能とする個人データ保護方針利用には、社内でデータ保護方針を整備のうえ、担当機関の承認取得が必要ひな形等は公開されておらず、各国/地域規制で要件の概要が示されるのみ	<ul style="list-style-type: none">データ輸出者/輸入者間で越境移転のために結ばれる契約ひな形が公開されており、越境移転の要件が網羅的/具体的に示されるEUを筆頭に、ASEAN/イペロアメリカ等の地域機関を含めて、採用が増加	<ul style="list-style-type: none">自国/地域と同等の保護水準を、対象国に対して認める制度	<ul style="list-style-type: none">越境移転理由や目的を通知のうえ、本人の同意を得る制度多くの規制で採用されている	
ヒアリング結果概要	取得難易度	★★★★★ 社内で個人データ保護体制の整備が求められるが、関連する認証 (Pマーク等) を取得している場合、対応コスト/難易度をより低く抑えられる	★★★★★ 規制の要件を基に、グループ共通の個人データ保護方針の策定が必要。承認申請も必要であるため、対応コスト/難易度は高め	★★★★★ SCC/MCCは契約条項が標準化されているため、対応コスト/難易度は低め	★★★★★ 自社サービス内で、利用規約と本人同意取得の整備を行えばよい。ため、対応コスト/難易度は相当低い		
	ヒアリング結果概要	<ul style="list-style-type: none">多くの事業者がCBPRを認知していない、又は詳細を理解していない (10社/16社)CBPRを正しく認知している事業者 (6社) で、実際にCBPRを取得している事業者は4社<ul style="list-style-type: none">ただし、取得にあたっては、越境移転自体より外部からの信用性獲得を目的としている事業者が大半一方で、CBPRのメリットも理解しているため、今後のCBPRの拡大を期待<ul style="list-style-type: none">✓ 採用国の拡大✓ 米国対応 (包括法がなく、州法の確認が必要。CBPRとの連結を期待)	<ul style="list-style-type: none">全事業者がBCRを認知 (16社/16社)。しかし、BCR取得企業は、3社のみ<ul style="list-style-type: none">➢ 取得ハードルが高く多くが未採用- 対象はグループ企業内のみ- 標準フォーマット等は存在しない- グループ内企業すべてに対し完全なガバナンスを実現するのは難しく、BCR違反のリスクは避け難い➢ 一方で、クラウドサービスのようにユーザのデータ保存場所や利用用途が確定していない、かつグローバルにサービスを提供したい企業はBCRを採用	<ul style="list-style-type: none">全事業者がSCCを認知 (16社/16社)。そのうち、約半数がSCC/MCCを選択 (7/16社)<ul style="list-style-type: none">➢ 契約フォーマットが標準化されているのに加え、企業間契約のみで対応が済むため広く普及➢ 一方で、データ種別と使用目的に合わせて複数のSCCが必要なケースもあり、グローバル企業の場合、コスト高になるケースもある	<ul style="list-style-type: none">自社サービス内での同意のみで完結できるが、GDPR準拠のための対応には負荷がかかっている<ul style="list-style-type: none">➢ CDO (Chief Digital Officer) の設置、ユーザ権利への対応余力確保、データ削除時期に関するSLA (Service Level Agreement) の作成等が必要➢ 欧州内でも同意可能年齢が13~16歳でばらつきがある		

1. グループ内人事データの越境移転は、ヒアリング⑩が該当。⑩以外の事業者でも人事データの越境移転はおこなっているが、主事業で利用している越境移転ツールを利用して移転



3.3

事業者のヒアリング結果 (詳細)

1 インターネットサービス企業のデータ越境に関するインタビュー

グループ内での越境移転が中心であり、グローバル共通のデータガバナンスの実現により顧客の信頼獲得を狙うため、BCRを選択

企業/事業概要

企業概要

- 業種：EC事業、通信事業

データ越境ニーズ

データ主体

顧客情報

データ種類

- 氏名
- 住所
- 電話番号
- サービス
使用履歴

利用目的

デジタルマーケティング
(CRM, WebAds等)

規制対応方法

規制対応 ツール

- グループの主要子会社及び一部合弁会社でBCRを取得し、越境を実現
 - 中国の開発センターにグループ内データを越境させることも可能
 - ビジネスパートナーや委託先についてはBCRでは対応できないため、情報プラバシーガバナンス担当部署及び各国の弁護士資格保有の担当者で対応

ツール 選択理由・ 検討経緯

- 2017のGDPR施行のタイミングで、グローバルで標準のデータガバナンスを実現しBCR取得を目指す方針を決定
 - 将来的に海外でプラットフォームサービスを浸透させるため、顧客の信用獲得を狙いBCRを選択。グローバルデータガバナンスに数十億円を投資
- A国本社チーム及び各国支社の弁護士資格保有者で対応
 - SCC締結等にリソースは割かず、BCR取得に向けた体制整備やISMS認証獲得に注力
 - また、グローバルで共通のデータガバナンスポリシーの策定も行う
- その結果約2年半でBCR取得に成功

ツール利用に おけるハードル 及びニーズ

- 出資比率の低い合弁会社はBCRの枠組みに含めることはガバナンスの問題で難しく、越境移転の必要がある場合の対応が課題

CBPRに関する コメント

- CBPRは、①GDPRとは違う形でのデータ運用の企業メリットが理解しにくい②対象国が少なく、CBPR認証取得企業が少ない③毎年再申請が必要、という3点で浸透しづらい状況
 - ①DFFTでビジネスチャンスがどう広がるのかを想像しにくい
 - ②そもそも取得企業数が少ないと取得メリットが少ないという仕組みであるため、プラットフォーム等が取得していかないと後につけない
 - ③セキュリティツールは、一般的に複数年ごとの更新かつ、前回からの取り組み差分を報告するものが多いが、CBPRは更新ではなく毎年ゼロベース審査されるように見受けられハードルが高そうに見える
- DFFTが進んでいくために、企業が利用しやすく、攻めと守りを両立したツールができることを期待

データの越境移転の流れと利用ツール

各データはリージョン内に保管し、データ分析もリージョン担当者が行うが、A国本社も閲覧利用可能にするため、データ越境が必要

①欧州・B国・C国 ⇔ A国 (本社所在地) : BCR

2 鉄道会社の国外からの旅行者の予約機能運用に関するインタビュー

グループ資本外の企業との越境移転が必要であるため、SCCを選択。しかし、グループが直接収集する他国民のデータについてはユーザの同意取得で対応

企業/事業概要

企業概要

- 業種：鉄道

訪日観光客チケット予約事業

- 欧州/米国/中国/B国圏で展開

データ越境ニーズ(チケット予約事業に限定)

データ主体	データ種類	利用目的
ユーザ	氏名・住所・ パスポート番号・ 請求先情報等	チケット予約及び 決済のため

規制対応方法

規制対応 ツール

- ① 欧州→A国
 - 欧州現地の旅行代理店経由の予約については、旅行代理店とSCCを締結することでデータ越境を実現
 - 一方で個人によるオンラインの予約は、HP上でGDPR準拠のプライバシーポリシーを提示し、個人情報利用の同意を取得
 - 十分性認定前後どちらも上記の対応を継続
- ② 中国・米国・B国→A国
 - プライバシーポリシーを提示し、個人情報利用の同意を取得

データの越境移転の流れと利用ツール

データは全てA国データサーバに集約

① 欧州→A国：SCCあるいはGDPR準拠のプライバシーポリシー

② 米国・中国・B国→A国：最低限のプライバシーポリシー

ツールの 選択理由・ 検討経緯

- 主事業の拠点があるEUは制裁リスクが大きいため、EUの規制対応に則してSCCを利用
- 一方で、中国・米国・B国については最低限の対応にとどめる方針
 - 中国：主事業の拠点がなく、制裁された場合のリスクが欧州より小さい
 - 米国・B国：欧州・中国と比較して制裁発生可能性が低い

ツール利用に おけるハードル・ ニーズ

- 十分性認定取得前だったこともあり、GDPR対応のための調査、SCCの締結、GDPR準拠のプライバシーポリシーの作成に数千万オーダーのコストが必要な点が必要なハードル
 - 外部のコンサルを利用しプライバシーポリシーのひな型を作成した際、法務部としてもリソースを多く割いた(現場でのデータ利用方法ヒアリング等)
 - SCCはひな型があるものの、締結先旅行代理店の法務対応力が低かったため、当社側のサポートが必要だった
- 規制の解釈を明瞭化し、ユースケースごとの対応方法提示のニーズあり
 - "EU現地企業は、常識的な範囲でGDPRを甘めに解釈していたが、A国企業としては制裁を危惧し最も厳しい解釈をせざるを得ない"
 - "ユースケースごとに、どの程度センシティブな対応を取る必要があるかを明確に示してほしい"

CBPRに関する コメント

(言及なし)

3 アパレル会社の海外SNS運用に関するインタビュー

越境移転による制裁リスクが低いため、GDPR十分性認定及び、GDPRに準拠したプライバシーポリシーの同意を選択

企業/事業概要

企業概要

- 業種：アパレル

ファッションSNS事業

- 2020リリース
- A国/米国/EU/中国で展開

データ越境ニーズ(SNS事業に限定)

データ主体

ユーザ

社員
(店舗スタッフ)

データ種類

投稿写真

投稿写真
名前
勤務店舗名

利用目的

他国ユーザによる閲覧
オフショアでのデータ検閲

規制対応方法

規制対応 ツール

- ①欧州→A国
 - A国へのデータ集約はGDPR十分性認定を利用。GDPRに準拠したプライバシーポリシーへの同意をユーザから取得
- ②米国→A国
 - カルフォルニア州民の投稿とそれ以外を選別する手間及び規制更新時の対応リスクを考え、米国全体に対してCCPAに準拠したプライバシーポリシーを示しユーザの許諾を取る
- ③A国→欧州・米国
 - A国に集約したデータの第三国への移転は、ユーザにデータの所在/利用目的を示し許諾を得る形で実現
- ④A国→フィリピン
 - フィリピンは欧州の十分性認定を受けていないが、プライバシーポリシー同意時に再移転がある旨、通知して本人同意を取ることで外部委託
- ⑤中国→A国
 - データセキュリティ移転評価の取得難易度が高く、データの越境移転を断念。テンセントと組み、中国国内のデータサーバーを利用し、サービスを展開

ツール 検討経緯・体制

- A国/欧州/米の共通アプリについては、A国の個人情報保護法、欧州のGDPR、米のCCPAのうち一番厳しいGDPRをベースにルール作りを行い、追加でローカル対応する方針を選択
- 中国についてはデータ越境による制裁リスクを鑑み、現地法人と協力のもと中国内に閉じたアプリを作成

ツール利用に おけるハードル

- 十分性認定があっても、GDPR準拠のための企業対応は手間がかかる
 - CDO(Chief Digital Officer)設置、ユーザ権利への対応余力確保、データ削除時期に関するSLA(Service Level Agreement)作成等が必要
- 外部委託業者としてオフショアを利用するためには、委託先のセキュリティ確保のための管理・監視を企業の責任のもと行わなければいけない
- 国ごとの個別のルールを差分を企業として都度判断する負担軽減を希望
- 個人情報の取り扱い方法だけでなく、ユーザの許諾を得る際の年齢制限(契約への同意可能年齢)についても統一ルールを設けることを希望
 - 欧州内でも同意可能年齢が13~16歳でばらつきあり

CBPRに関する コメント

(言及なし)

データの越境移転の流れと利用ツール

- ①欧州→A国：GDPR十分性認定 + GDPR準拠のプライバシーポリシー
- ②米国→A国：CCPA準拠のプライバシーポリシー
- ③A国→欧州・米国：GDPRレベルのプライバシーポリシー
- ④A国→フィリピン：GDPRレベルのプライバシーポリシー
(外部委託先利用による再移転の同意)
- ⑤中国→A国：断念（中国国内サーバーを利用）

4 中国ゲーム制作会社のデータ越境に関するインタビュー

グループ資本内外両方の企業との越境移転が必要であるため、SCCを選択

企業/事業概要

企業概要

- 業種：ゲーム事業
- 中国の主要ゲーム会社であり、アジアや欧州にもサービスを展開
- 各国に子会社/合併会社を保有

データ越境ニーズ

データ主体

ユーザ

データ種類

- ユーザID
- ハードウェアデバイスのID 等

利用目的

- 他国ユーザとのゲームでの対戦
- 広報・マーケティング目的の分析

規制対応方法

規制対応ツール

- ユーザにはゲームのプラットフォーム参加時にデータ使用の許諾を取得
- データ越境が必要な企業間ではSCCを締結
 - 例：シンガポールのデータ管理事業者(グループ会社) 対 A国の広報・ゲーミングオペレーション企業(合併会社)
 - 例：自社 対 アメリカの開発ラボ
- 中国からの越境の実態についてはご回答をいただかず

データの越境移転の流れと利用ツール

アジアユーザデータは、シンガポールまたは香港サーバに集約

- 中国サーバは、国外ユーザ向けにはファイアウォールの関係で通信速度が担保できなく、またユーザからの批判もあったため、利用せず

欧州も同様に欧州内サーバに集約

①A国を含む複数カ国→シンガポール又は香港のサーバに集約：
社員と企業間でデータ利用の同意書を結び、データの収集の許諾を取得

(その他のデータ越境の流れについては明確な回答なし)

ツール 検討経緯・体制

- 中国HQの法務部および、各事業部ごとにデータプライバシーの担当者(弁護士)が対応方法を検討

データ越境 ツールへの ニーズ

- 中国企業からすると、GDPR等海外の規制は、データの保護基準や対応方法が不明瞭だと感じる
 - "中国のほうが対応すべき内容がはっきりしていて理解しやすい。GDPRはどこまでの対応が現実的に必要なのかが分かりにくい"
- 理想は全世界で共通の枠組みができることだが非現実的。欧州以外で縛りの弱めな枠組みができればビジネスチャンスは広がりそうだと考えている

CBPRに関する コメント

(言及なし)

5 製薬会社のデータ越境に関するインタビュー

グループ資本内の企業との越境移転に関して、BCRの基準が不明瞭であることから、SCCを選択

企業/事業概要

企業概要

- 業種：製薬
- グループ会社が国内外に200社弱存在

データ越境ニーズ(SNS事業に限定)

- ①臨床開発目的のデータカルテ情報
 - 名前、住所、年齢、薬の使用歴、効果、病歴等
 - 仮名化されているが、要配慮個人情報にあたる
- ②市販薬の安全性情報(国家機関に報告義務あり)
 - 薬の組み合わせ、副作用(血圧の数値等)、医師の知見が含まれ、要配慮個人情報にあたる
 - また、そのほかシリンジ等のデバイスとの情報も事案発生時の損害補償対応のために保有
- ③社内の人事データ
 - 社員の名前、性別、住所、経歴等

規制対応方法

規制対応 ツール

欧州・B国・C国他⇔A国

- BCRは基準が不明瞭で申請を棄却された企業の噂を聞き、リスクを取らずにSCCを利用

ツール 検討経緯・体制

- 三極(欧州、B国、C国)それぞれにプライバシーオフィサーが存在しており、この3名と法務部を中心に議論
- GDPR対応プロジェクトのマネジメントはPWCやKPMGといったコンサルを利用。また法律事務所にも複数協力を依頼
- SCCは本社と各グループ会社間で締結
 - インパクトアセスメントやセキュリティの監査も丁寧に実施したうえでSCCを締結
 - データ主体にはプライバシーノティスを実施
 - データ越境ニーズ①②③のデータは全て同じツールで対応
- グループ会社が200社弱存在したため、データ越境ニーズをもとに優先順位をつけ対応
 - 全グループ会社でデータ越境ニーズ①②のデータを扱うわけではないが、③の実現のためにも全グループ会社とSCCを締結する必要があった
 - 2017年に検討を開始し、SCCの対応を一通り終えたのが2020年になってから

ツール利用に おけるハードル

- 規模の小さいグループ企業とのSCC締結の際、なかなかSCCの必要性を理解してもらえず説得に時間がかかった
 - "SCC以外のもっと楽な電子承認はないのか？とグループ企業からしつこく問いただされた"
- その結果実務として情報共有はされているのにSCCが未締結という違反情報が一時期存在した
- データ流通を促進する規制には賛成
 - "データはただ集めるだけでは意味がない。A国の個人情報保護法のように、データの使用方法の規制によって安心してデータ利用が可能になるならば、規制はむしろ流通のサポートになっていると考えている"

CBPRに関する コメント

(言及なし)

データの越境移転の流れと利用ツール

①欧州・B国・C国他⇔A国：SCC + プライバシーノティス

②中国→A国：断念（中国国内サーバーを利用）

6 機器メーカーのデータ越境に関するインタビュー

グループ資本外の企業との越境移転が必要であるため、SCCを選択

企業/事業概要

企業概要

- 業種：建設メーカー
- 海外販売拠点数：54拠点

データ越境ニーズ(SNS事業に限定)

データ主体	データ種類	利用目的
ユーザ	<ul style="list-style-type: none">位置情報稼働情報燃費消費摩耗情報	<ul style="list-style-type: none">研究開発目的のため利用

データの越境移転の流れと利用ツール

欧米のデータは、A国本社のオンプレミスサーバーに集約
中国国内データは、中国現地法人サーバで管理

- ①欧州→A国：SCC + 販売契約時にデータ利用の同意を含む
- ②米国→A国：販売契約にデータ利用の同意を含む
- ③中国→A国：断念（中国国内サーバーを利用）

規制対応方法

規制対応ツール

- 欧州⇄A国
- 販売先の企業とSCCを締結。販売契約時に別途データの利用規約同意を取っている。
- 中国⇒A国
- 断念

ツール検討経緯・体制

- 中国進出時に、データの越境利用に関して中国当局より禁止されていること指示があり、利用を断念
- 現地法人にてデータ分析及び、マスキング等の1次加工を行っている。

ツール利用におけるハードル

- 中国に関しては、地理情報をマスキングされていることにより、どの地域で、どのような用途で利用されているのかなど把握できず、中国戦略方針が販社任せになっている。
そのため、A国本社上層部は、正しく中国販社がデータを活用できているなど不安がある。

CBPRに関するコメント

（言及なし）

7 機器メーカーのデータ越境に関するインタビュー (2020年当時の情報)

越境移転による制裁リスクが低いため、GDPR十分性認定を利用したデータ越境を構想

企業/事業概要

企業概要

- 業種：機器メーカー海外拠
点数：53拠点

データ越境ニーズ(SNS事業に限定)

データ主体

ユーザ

データ種類

- 位置情報
- 稼働情報
- 燃費消費
- 摩耗情報

利用目的

- 研究開発目的のため利用

規制対応方法

規制対応 ツール

欧州⇒A国

- EU内でのデータ収集及び域外移転は、クラウドサーバのセキュリティポリシーに
依拠 + GDPR十分性認定を想定 (データの越境移転は、20年時点で未開始)

米国⇒A国

- 業界規制に細かい規定があったため、収集項目及び個人データの取扱いにつ
いては、業界規制対応を優先(データの越境移転に関しては未検討状態)

中国⇒A国

- 中国へのデータアクセスは、データ保護3法及び、業界規制により断念

データの越境移転の流れと利用ツール

EU、米国のデータは現地クラウドサーバにて管理
中国版社のデータは現地法人のサーバで管理

<2020年当時はデータの越境は未開始(構想のみ検討)>

- ①欧州⇒A国：クラウドサーバのセキュリティポリシーに依拠 + GDPR十分性認定
- ②米国⇒A国：業界規制対応を優先 (データの越境移転に関しては未検討)
- ③中国⇒A国：断念 (中国国内サーバを利用)

ツール 検討経緯・体制

- A国本社の法務も各国法や規制に対する、情報収集機能は持ち合わせおら
ず事業部の相談ベースで対応

ツール利用に おけるハードル

- 海外版社はA国社員が幹部として赴任するため、言語的、関係的に各団体
の中に入り情報を仕入れるのが難しい
- そのため、規制に対応する製品開発が遅れたり、対応が後手に回るケースが
多い

CBPRに関する コメント

(言及なし)

8 自動車部品メーカーのデータ越境に関するインタビュー

個人情報に当たる項目が必要ないため、分析に必要な部分以外をマスキングしたデータを越境することを選択

企業/事業概要	データ越境ニーズ(コネクテッドカー事業に限定)			規制対応方法	
企業概要 <ul style="list-style-type: none"> 業種：自動車部品メーカー 国内外に36カ国に拠点 	データ主体	データ種類	利用目的	規制対応ツール	①欧州→A国 <ul style="list-style-type: none"> マスキングしたデータをA国へ共有 ②タイ、B国、C国→A国 <ul style="list-style-type: none"> マスキングしたデータをA国へ共有
	ユーザ	<ul style="list-style-type: none"> 位置情報 車両番号 車種 契約者名、 契約者住所 	<ul style="list-style-type: none"> 研究開発目的のため利用 データはマスキングして利用 	ツール 検討経緯・体制	<ul style="list-style-type: none"> 個人が特定できないようにマスキングした上で、データをA国に共有 全世界同様のマスキングルールでデータを越境
データの越境移転の流れと利用ツール				ツール利用におけるハードル	<ul style="list-style-type: none"> A国/欧州両法人の法律事務所やコンサル会社に確認し、マスキングルールを作成。ルール設定に数千万円の費用が発生 現地法人は、個人情報保護規制など法律面で調べるが、データの加工指示に関してはA国本社が主導 データ活用に関しては、2021年度にデータ活用推進室を設置し、データ活用戦略を検討中。今後具体的なニーズが出てくるとされる。
データ管理に関しては、各国のクラウドサーバを利用し、ローカル管理				CBPRに関するコメント	(言及なし)
<div> ①欧州→A国：マスキングした2次データをA国へ共有 ②タイ、B国、C国→A国：マスキングした2次データをA国へ共有 </div>					

9 米国機器メーカーのデータ越境に関するインタビュー

グループ資本内外両方の企業との越境移転が必要であるため、各国の法制度に合わせ、カスタマイズしたSCCを選択

企業/事業概要

企業概要

- 業種：建機メーカー
- 規模：NYSE上場

データ越境ニーズ(SNS事業に限定)

顧客データ

- 名前、住所、電話番号、国によっては個人識別番号、財務状況等
- 車両の売買及びその後のメンテナンス、マーケティング等の目的で使用

ディーラーの情報

- 各国のディーラーの社員情報
- 社内人事のため

その他マーケティングや業界の情報

- JDと他者間で、データの取引をすることも

規制対応方法

規制対応 ツール

- EU顧客データについてはGDPR準拠のSCC(アメリカHQ対EUエンティティ)を利用
- その他地域のデータについては、SCCをベースに各国の規制に合わせ項目を編集したSCCを締結
- グループ外のベンダーとデータ越境を行う際は、GDPR準拠のSCCを締結

ツール 検討経緯・体制

- HQ及び各リージョンごとに「プライバシーチャンピオン」と呼べる知見がある担当者が存在しており、HQが各リージョンの担当者と密に連携する形でツールを選択
- 公開されているCISCOの調査レポートを活用し、ベンチマーク事例と比較することで対応を議論することもある
- 運用としては、オプトイン及びオプトアウトを可能にする仕組みづくりを行う
 - 顧客の車両購入時に、自社プライバシーノティスを提示したうえで、「業務遂行のために利用してよいか」を各項目についてチェック方式で同意を取得し、同意取得項目のみを自社サーバーに保管するオプトイン方式
 - 全リージョンにプライバシー担当窓口が存在し、顧客のデータのオプトアウト要望に対応できる機能を保有

ツール利用に おけるハードル

- SCCで細かくデータの利用目的を定義することは現実的には難しく、変更があった際にはSCCの再締結が必要な点が不便
 - SCCではデータの種類(What)、使用方法(How)、仕様目的(Why)を明確にしなければいけない
 - データ利用制約によるという課題が今後発生するかも含め議論が必要だった
 - 特にAPI利用が進む時代において、SCCで許可されてないデータ利用が行われないことの確認も時間をとられる

CBPRに関する コメント

(言及なし)

データの越境移転の流れと利用ツール

各地域ごとにローカルデータサーバを用意して管理

- ①欧州→米国：SCC + 顧客個人の同意
- ②その他(中国を含まない)→米国：ローカライズしたSCC + 顧客個人の同意

10 住宅製品メーカーのデータ越境に関するインタビュー (2014-2015年当時の情報)

グローバル人事システム構築に向けて、GDPR発足前であったため、自社オリジナルでグループ会社と契約及び、社員個人の同意書を締結することを選択

企業/事業概要

企業概要

- 業種：住宅製品メーカー
- M&Aにより欧州・米国・中国にグループ会社を保有

データ越境ニーズ

データ主体

社員
(管理職)

データ種類

名前、年齢、
性別、住所、
顔写真、
経歴

利用目的

社員のキャリアディベロップ
メントのための、グローバル
共通評価制度の実現

規制対応方法

規制対応 ツール

欧州→A国

- A国親会社 対 各国の子会社/孫会社 間でデータの収集内容、使用目的について契約を結ぶ
 - 当時はGDPRのSCCひな型はなかったため、自社でオリジナルを作成
- 上記に加え、A国親会社 対 社員 間でデータの収集内容、使用目的への同意書を結ぶ

中国・B国・C国他→A国

- 2014年当時は中国の規制は厳しくなく、中国の子会社の社員情報もEUと同じ方法で対応

欧州→A国→アメリカ

- アメリカ社員がEU社員の管理を行うケースに対してはセーフハーバーを適用

ツール 検討経緯・体制

社内3人＋社外の弁護士で対応し、半年以内に第一弾対応を終了

- 対応チームは親会社人事部2名＋親会社の法務部1名。さらにA国国内の外資系法律事務所の担当者1名で個人情報保護の観点の検討を担当
- 2014年8月時点で、A国の親会社対子会社の契約のほか、社員個人の同意書も必要ということが判明し、1か月で同意書獲得に迫られる

2015年4月にCLO(法務責任者)が変わり、より厳格な対応が必要との指示があり、社員個人の同意書の内容を見直し

ツール利用に おけるハードル

当時はA国企業で海外子会社のデータ越境への規制対応に取り組む事例が少なく、法律事務所に問い合わせてもどのレベルの対応が必要なのかが明確でなかった

- GDPR施行前だったこともあり、あくまで従業員が訴えてくるリスクを減らすための施策であり、企業として善意で取り組んでいたという空気感

子会社、孫会社の社員から直接同意書を取得するには三か月程度時間がかかる

官には、民間企業の負担をすこしでも減らすサポートをしてほしい

- 十分性認定が取れても、結局SCCとかBCRとかが求められているなら工数は減っておらず、十分性認定を取った意味がないのではと感じる
- 社員の同意書のひな型の配布など、実務に沿ったサポートが必要

CBPRIに関する コメント

(言及なし)

データの越境移転の流れと利用ツール

①欧州・中国・B国・C国他→A国：

A国親会社 対 子会社・孫会社のSCC相当の契約 及び
A国親会社 対 社員個人の同意書締結

②欧州→米国：セーフハーバー協定

11 消費者調査会社の社内人事データ集約に関するインタビュー

越境移転による制裁リスクが低いいため、グループ企業間のデータ利用同意書のみで留めることを選択

企業/事業概要

企業概要

- 業種：調査会社
- A国に親会社が存在
- M&Aにより欧州の企業を子会社化

データ越境ニーズ

データ主体	データ種類	利用目的
社員	名前 住所 電話番号 経歴 等	グローバル人事制度の導入
アンケート回答者	— (集計加工してから越境)	—

規制対応方法

規制対応ツール

- ①イギリス・A国・B国他→シンガポールのサーバに集約
 - イギリス政府のテンプレートをを用い、社員とグループが契約を結ぶことで社員のデータ越境が可能
 - イギリス以外の地域についても同一の同意書を利用

②シンガポールのサーバ→A国

- 上述の同意書で、データ利用についても許諾を取得

ツール検討経緯・体制

- アンケートの回答結果等、利用者から収集したデータは個人が特定できないように加工したうえで集約しているため、データ越境規制対応は必要ない
- 社員情報はグローバル人事のため越境が必要だが、社員であるため一般市民データと比較すると制裁リスクは少なく、対応リソースは限定的にする方針
- 欧州子会社の本部（イギリス）にチーフプライバシーオフィサーがおり、法規制対応を主導

ツール利用におけるハードル

- イギリス以外の国について、データ利用同意書のローカリゼーションを行うリソースがなく、各国の法制に忠実な対応が取れない
- 本来はグループ内データ越境はBCR取得が望ましいものの、BCR取得のリソースを割けないため、同意書のパッチワークをせざるを得ない
 - "社員情報のグループ内越境を可能にするひな型ありのツールがあればぜひ利用したい"

CBPRに関するコメント

（言及なし）

データの越境移転の流れと利用ツール

①イギリス・A国・B国他→シンガポール：

社員と企業間でデータ利用の同意書を結び、データの収集の許諾を取得

②シンガポール→A国：

また、上記同意書でA国でのデータ利用許諾も取得

12 ネットワーク機器メーカーのデータ越境に関するインタビュー

ネットワークセキュリティ保証が経営戦略上最重要。そのためグローバルで共通のデータガバナンスを目指し、BCR、CBPRを選択

企業/事業概要

企業概要

- 業種：ネットワーク機器メーカー

データ越境ニーズ

データ主体

顧客企業の取り扱いデータのデータ主体

データ種類

顧客企業の取り扱いデータ

利用目的

- ネットワーク機器提供
- セキュリティサービス
- クラウドサービス

規制対応方法

規制対応ツール

- 各国法準拠のグローバル共通SDPA(Super Data Protection Agreement)を作成し、顧客企業とデータ利用の契約を結んでいる
- データの越境ツールとして、BCRやCBPRを利用

ツール選択理由・検討経緯

- データの越境ツールとして、BCRやCBPRを取得
- 体制は、各国にプライバシーデータチームと累計400人を超える弁護士を保有
 - 自社内にプライバシーポリシーを専門とするチームが各国に存在し、規制や要件を議論し、会社全体のプライバシーポリシーをアップデートする

ツール利用におけるハードル及びニーズ

- EUに関しては、連合であることから調査が簡単だがアジアや米国など、各国各々のデータ保護規制を採用しており、調査コストは非常に大きい
- 特に米国は州ごとに規制が存在するため、米国企業でさえ厳密に対処しようとすると相当負荷が大きい
- 規制の例外などレアケースに関しては、リスクを受け入れて対応しないなど内部で判断を行っている

CBPRに関するコメント

- CBPRは認証という証明書を得られる点及び、枠組みがあることで各国政府が個人情報のデータ移転に関して話し合うことが可能という点で優れている
- しかし、現状米国はCBPRを取得していたとしても各州の規制を一個一個調べなければならないので、この点解決できると非常に有意義なツールになる
- また欧州を主体とするデータ主権主義がメインストリームになる中で、データ流通を促進させるという目的をCBPRが持つならば、果たす役割はもっと重要になると考える

データの越境移転の流れと利用ツール

データはローカライゼーションしており、各国のデータセンターに顧客情報や問い合わせ情報などが保管されている

① 欧州⇄A国：BCR

② 日本、B国、C国他⇄A国：CBPR

13 インターネットサービス会社のデータ越境に関するインタビュー

グループ内での越境移転が中心だが、グローバルで支社数が多くデータガバナンスを効かないリスクもあるため、BCRは選択せずSCCで対応

企業/事業概要

企業概要

- インターネットサービス会社複数社での対応についてを総合的にご回答いただいた

データ越境ニーズ

①パーソナライゼーション目的

- ユーザによりよい検索結果や広告の表示等を行うため、ユーザの特性情報が必要

②AI学習目的

- 上記パーソナライゼーションの基礎となるようなAI学習のため、多数のユーザのデータが必要
- ただし、名前は必要なく、年齢もレンジを持たせるなどの匿名化されたデータで十分。スタンダードプラクティスとして、プロフィールを残しつつ詳細はぼかし、セグメンテーションを可能にしている

規制対応方法

規制対応ツール

グループ企業内、企業外のどちらの越境移転もSCCで対応

ツール 選択理由・ 検討経緯

- BCRはSCCと比較すると確かにグループ内での越境が容易になるが、ビックテック規模の企業の場合、全ブランチに対し完全なガバナンスを実現するのは難しく、BCRに違反するリスクが避けられないため、BCRは非現実的
 - BCRは監査が入ることがあるため、完全なガバナンスが効かない場合は監査がリスクになってしまうので使いづらい
 - ただし、BCR取得可能なレベルのデータ取扱いを実現するため、インターナルではBCR基準に照らし合わせながらSCCを作成
- SCCはアベンディックスの活用により各国の規制レベルに合わせた書き分けも可能であるため、企業の実態に合う形で作成が可能であり現実的

データの越境移転の流れと利用ツール

- ビックテックは基本データセンターを各国に保有しており、当該国で収集したデータは当該国内に保有し、上記①の目的で活用
- 一方で、データは複製可能であるため、EU内データセンターにもバックアップ(ただし匿名加工済)を保有し、上記②の目的で活用

欧州⇔A国 : SCC

ツール利用に おけるハードル 及びニーズ

- データセットを越境させるとき、データの種類と使用目的に合わせて複数のSCCのが必要であり、既に数千単位のSCCを作成。対応コストが大きいことが課題
- SCCで規定されているリスクのロングリストが網羅的すぎて現実的でない
 - "DTIA(リスクアセスメント評価)も手間がかかるため、より明確かつ必要最低限のチェック項目が必要"

CBPRに関する コメント

(注：エキスパートの理解に基づくため現実と違う可能性あり)

- 認証を得る過程で全社ガバナンスを整える必要があるが、CBPRがSCC (A社とB社間でデータ種類・利用目的別に複数のSCCを結ぶ) とは違い、対象社数や利用用途が増えたとしても包括対応可能な点及び、A社とB社のデータガバナンス体制の不足分がある場合、2社間の契約で十分としている点など、現実的な使いやすさの観点で高評価
- CBPRがAPAC外に広がろうとしている点を、中東やアフリカ企業の視点で評価
 - "中東、アフリカではEUの厳しい規制に対応していくより、南米、アメリカ、APACと組んでビジネスを広げていくほうが良いと考えている"
 - "現状6個しか認証局がないため認証を受けるまでに時間がかかってしまうだろう。認証ツールをもっと強くして、例えばアイリッシュ認証局も信用して認証付与ができるようにしてほしいと思う"

14 クラウドベンダーのデータ越境に関するインタビュー

自社サーバー間での越境移転ニーズがあり、サービス利用法人からの信頼獲得が経営戦略上重要。そのためグローバルで共通のデータガバナンスを目指し、BCRを選択

企業/事業概要

企業概要

- 業種：クラウドベンダー

データ越境ニーズ

データ主体

顧客企業の取り扱いデータのデータ主体

データ種類

顧客企業の取り扱いデータ

利用目的

クラウドサービス提供

規制対応方法

規制対応ツール

- グローバル共通のDPA*1(約20か国の法規制の最も厳しい基準に準拠)を作成し、DPAの記載内容を根拠にBCRを取得

ツール

選択理由・検討経緯

- 越境移転ニーズのあるクラウドサービス顧客が、データの取り扱い方法についてはクラウドベンダーのDPAに依拠できるため、DPAを詳細に検討
- また、クラウドサービス顧客からの信頼を獲得可能であるため、BCRを取得
 - "セキュアなサービスであるため、国内保存義務のある中国・ベトナム企業も当社のサービスを利用し、国外データセンターにデータを保有している"
- 体制としては、リーガルチームおよびインシデントチームを保有
 - 自社内に越境移転の規制の把握・対応を専門とするリーガルチームが存在し、数十億円以上のコストをかけて対応にあたった
 - またグローバル共通のインシデントチームも存在し、インシデント対応やグループ内での知見共有に努める

ツール利用におけるハードル及びニーズ

- "顧客企業の存在する全地域の規制の調査にコストがかかった点は大きなハードルであり、大規模なクラウドベンダーだからこそ対応できた"

CBPRに関するコメント

(言及なし)

データの越境移転の流れと利用ツール

データセンターは約20か国にそれぞれ存在し、顧客企業にはどのデータがどのデータセンターに保管されているかを明確に共有

欧州⇄A国、B国、C国他: BCR

*1.DPA=Data Processing Agreement: データ処理契約

15 米国大手IT企業のデータ越境に関するインタビュー

ネットワークセキュリティ保証が経営戦略上最重要。そのためグローバルで共通のデータガバナンスを目指し、BCR、CBPRを選択

企業/事業概要

企業概要

- 業種：業務用コンピュータ機器・ソフトウェア販売

データ越境ニーズ

データ主体

顧客企業の取り扱いデータのデータ主体

データ種類

顧客企業の取り扱いデータ

利用目的

- 業務用コンピュータ機器提供
- SaaS提供
- クラウドサービス

規制対応方法

規制対応ツール

- 「One Trust」という情報サイトのテンプレートを利用し、各国の個人情報保護法に対応
- データ越境ツール及び、クライアントの信用獲得のため、BCRやCBPRを利用

ツール選択理由・検討経緯

- CBPR取得理由は、フレームワークやガイドラインに従っていることを確認するためのプロセスや技術を持っていることを証明でき、クライアントの信用に繋がるので採用
- その他各国の個人情報保護法への対応は、プライバシーアセスメントを行い、データセットの中身と場所、アクティビティ(実施したいこと)、プロセス(処理方法)、アセット(ハード/ソフトウェア)を定義し、その上で「One Trust」から必要なテンプレートを利用

データの越境移転の流れと利用ツール

- ①欧州⇄A国：BCR
- ②日本、B国、C国他⇄A国：CBPR

ツール利用におけるハードル及びニーズ

- CBPR自体は、フレームワークなので各国個人保護法やアメリカ州法をサポートしているわけではなく、認証で得るものは信頼性であり、それ以上でもそれ以下でもない
- CBPR準拠対応のために、毎年金銭的/時間的コストがかかり、また更新期間も1年なのでグローバル企業のような体力がある企業しか取得が難しい

CBPRに関するコメント

- CBPRをより多くの国や企業に採用してもらうには、機能を拡張し利便性を高める必要がある。そのためには、各国の個人情報の差分などを洗い出し、共通部分は共通法として新しく定義し直し、国同士がコミュニケーションを取りやすくするべきである

16 インターネットサービス企業のデータ越境に関するインタビュー

ネットワークセキュリティ保証が経営戦略上最重要。そのためグローバルで共通のデータガバナンスを目指し、CBPRを選択

企業/事業概要

企業概要

- 業種：インターネットサービス

データ越境ニーズ

データ主体

ユーザデータ

データ種類

ネットサービスの
会員情報

利用目的

- 会員情報の連携

規制対応方法

規制対応 ツール

- CBPRを利用

ツール 選択理由・ 検討経緯

- GoogleやAmazonなど、グローバル企業はCBPRを取得しており、競合が取得している認証に関して遅れ劣らないようにCBPRを取得
- またプライバシー・セキュリティの認証をグローバル水準で取得しているという証明となり、ユーザーが安心して登録できるようになるため、会員登録促進目的もある

ツール利用に おけるハードル 及びニーズ

- CBPRが規制を包括して、一つの認証で各国の個人保護規制など上手く乗り越えられるツールがあると、企業の経済活用の合理性につながる

CBPRに関する コメント

- SCC<CBPR<BCRの認識
但し、取得経験がないため、聞いた話や個人の経験から判断
- 非常に複雑な規制ツールを理解することは事業者側からは難しく、各部門ごとに見る観点が異なるためコミュニケーション自体も難解である。そのため、ガイドラインやユースケースがあると便利だと考える

データの越境移転の流れと利用ツール

韓国⇄A国：CBPR

※その他詳細は不明

Agenda

1. 本事業の位置づけ
2. データ越境移転関連調査
3. 事業者によるツール等の活用実態調査
- 4. 調査結果のまとめ

調査結果のまとめ (1/2)

2章では、主要国について、各国/地域規制や越境移転等のツールの調査を実施した

- 特定の要件を満たした場合に個人データの越境移転を認めるとしている規制が大半であるが、越境移転の要件は、各国/地域で異なっている
 - 越境移転に際して、本人同意、自国と同等もしくは十分な水準の保護を持つ移転先を要件とすることが一般的
 - 本人同意、同等もしくは十分な水準の保護に加えて、当事者間での法的拘束力のある文書の締結や認証・シール、行動規範も越境移転の要件として認めている国/地域も4カ国/地域が存在
 - いずれもEU (EU加盟国及びEEA諸国) の GDPR (General Data Protection Regulation: 一般データ保護規則) に準じた規制を策定
- また、中国、ロシアをはじめとしたいくつかの国/地域は、越境移転規制に加え、ローカライゼーション規制を持っている

3章では、上述の調査結果のとおり各国/地域で異なる規制/ツールの現状に対し、事業者がどのようにツールを選択し、データの越境移転を実現しているか、ヒアリングを通じて、調査を実施した

- 主な規制であるGDPRについては、グループ外の企業との越境移転ニーズがある場合、SCC等を用いて、都度対応している例が一般的であった
- また、グループ内企業との越境移転ニーズについては、グローバル共通でのデータガバナンスの一括構築を目指す場合はBCRが採用され、また、それを特段志向しない場合は、SCCが採用されている場合が多かった
- CBPRは、自社のデータガバナンスについて、クレディビリティを獲得するために採用されていることが一般的であった
- なお、越境移転ニーズ自体は存在するものの、中国からの越境移転については、コストの大きさから、越境移転を断念している例が散見された

調査結果のまとめ (2/2)

事業者へのヒアリング結果を総合すると、事業者はデータ流通について、「適切な水準の保護を通じて規制には対応し、顧客等外部からのクレディビリティを確保しつつ、規制は必要最低限の水準に留まること」を、強いニーズとして有していると考えられる

このニーズと、「信頼性のある自由なデータ流通」の推進の観点からは、下記の要素を満たす越境移転の枠組みが求められると考えられる

- **規制への対応**：データが適切に保護され、各国/地域規制に対応できること
- **外部からのクレディビリティの獲得**：当局のみならず、顧客等の外部からもデータの取り扱いに関してクレディビリティを獲得できること
(これがビジネスチャンスにつながることを期待される)
- **必要最低限の規制**：手続きの簡素さ / 予見可能性の高さ
 - 一度の手続きでカバーされる対象範囲 / 地理的・時間的な範囲が広いこと
 - 具体的なユースケースが示されている/手続きに要する費用・期間が明確化されている等、事業者にとっての予見可能性が高いこと

今後の政策検討には、各国/地域の規制及びツールの制度設計の意図を踏まえた上で、上記のニーズを考慮した上で、どのような枠組みが必要となるか、考察をしていく必要があると考えられる

越境移転に関するツールのニーズと新フォーラムの目指すべき方向性 (仮説)

現状、グループ外の越境移転ニーズを満たすデータガバナンス構築のツールはない。また、CBPRは法規制への対応ツールというより、「クレディビリティ獲得のためのもの」という評価。よって「規制に対応可能 + グローバル共通ガバナンス一括構築」が、目指す方向性ではないか

越境移転ニーズ	活用する越境移転ツール	企業例
グループ外企業との越境移転ニーズ	A グローバル共通のデータガバナンスの一括構築	該当なし (ニーズはあるが対応できるツールなし) n/a
	B 各国/地域別の法規制に都度対応	SCC等の企業間契約 ・ 鉄道会社 ・ 中国ゲーム制作会社 ・ 機器メーカー ・ インターネットサービス会社
グループ内企業との越境移転ニーズ	C グローバル共通のデータガバナンスの一括構築	BCR ・ インターネットサービス会社 ・ クラウドベンダ ・ ネットワーク機器メーカー
	D 各国/地域別の法規制に都度対応	SCC等の企業間契約 ・ 製薬会社 ・ 米国機器メーカー ・ 住宅製品メーカー ・ インターネットサービス会社
		社内でプライバシーデータ管理の基準を持ち、既存ツールを使用せず自主的にリスク対応 ・ インターネットサービス会社
		D' 最低限の対応 (制裁リスクが低い場合) 十分性認定+個人/法人同意 ・ 機器メーカー ・ アパレルメーカー
グループ内外共通	E データガバナンスに係る顧客のクレディビリティの獲得	個人の同意取得 ・ 鉄道会社 ・ 消費者調査会社
		現行CBPR ・ ネットワーク機器メーカー ・ インターネットサービス会社 ・ IT会社 ・ インターネットサービス会社
F 越境を断念 (ニーズ自体は存在)	該当なし	・ アパレル会社 ・ 製薬会社 ・ 機器メーカー ・ 自動車部品メーカー

[方向性①]
現状、ニーズはあるものの対応可能なツールがない状況
この欠缺を埋めに行く

[方向性②]
現状、「クレディビリティの獲得」に実質的に留まっている効果を拡大し、各国/地域規制に対応なものとしていく



[bcg.com](https://www.bcg.com)