グローバル越境プライバシールール（GCBPR）システムの普及促進に関する調査業務

調査報告書

令和 7 年 12 月1日

一般財団法人日本情報経済社会推進協会

目　　次

I. 調査概要

1. 件名

「グローバル越境プライバシールール（GCBPR）システム[1]の普及促進に関する調査業務」（以下、「本調査」という。）

2. 実施目的

2025 年 6 月 2 日より Global CBPR Forum（以下、「GCBPR フォーラム[2]」という。）が運営する GCBPR が正式に稼働を開始した。

一定の個人データの保護要件を満たしている事業者を国際的に認証する制度である GCBPR の普及啓発のため、個人情報の越境移転に係る実態等を調査・分析し、効果的に広報・アウトリーチ活動を実施するための資とすることを目的とする。

3. 実施内容及び実施体制

3.1. 実施内容

(1) 業務管理

原則月 1 回、進捗状況等を報告する会議（以下、「月例進捗報告」という。）を実施し、報告書、全体スケジュール、添付資料等の必要資料は会議の 3 営業日前までに送付し、適宜、現状把握、課題及び対応策の協議、全体スケジュールの調整を行った。

(2) 個人情報の越境移転に係る実態調査・分析等

令和6年度に経済産業省にて「越境プライバシールール（CBPR）認証制度の普及等に向けた調査（以下、「R6 調査[3]」という）」が実施されたが、本調査では、R6 調査の結果を踏まえ、さらに詳細検討すべき項目及び R6 調査では対象に出来なかった項目について、「2.1.業種ごとの越境移転ニーズ等アンケート調査」、「2.2.調査 2.1.を踏まえた企業ヒアリング」、「2.3.GCBPR の強み・利点の詳細分析等」、「2.4.企業認証プロセスの詳細分析及び効率化の検討」、「2.5. GCBPR メンバー間の個人データの越境移転において認証事業者が受ける利点調査」、「2.6. 各国法令と GCBPR のプログラム要件とのマッピング分析」を実施し、それらの結果をとりまとめた。

---

[1] システムを表す場合は GCBPR を使用する。GCBPR の認証の種類としてはグローバル CBPR とグローバル PRP があるため、認証の種類を表す場合をカナ表記として区別する。

[2] 越境する個人データに関して、事業者等が一定の保護要件を満たしていることを国際的に認証する制度で、2022 年 4 月 21 日に、APEC の枠にとらわれず、より広範囲での個人データの円滑な越境移転や各国における規律の相互運用性を促進させること等を目的として、世界中の国及び地域が参加可能な枠組みである「GCBPR フォーラム」の設立が宣言された。

[3] 経済産業省 Web サイト「R6 調査の報告書（以下、「R6 調査報告書」という。）」
https://www.meti.go.jp/policy/external_economy/cbpr/202501.pdf

(3) 広報・アウトリーチ活動に関する提言

(2)の調査結果を踏まえ、GCBPR の周知のための広報活動並びに参加法域数及び参加事業者数の増加に向けてアウトリーチ活動を効果的に実施するために、普及促進度合いを測る上で有効な指標や具体的な提言策を導出した。

II. 情報の越境移転に係る実態調査・分析等

1. 実施概要

GCBPR の普及促進のため、効率的に広報・アウトリーチ活動を実施するための資料とすることを目的として、R6 調査では対象にできなかった項目や、さらに詳細検討すべき項目について調査・分析する。

2. 実施結果

2.1. 業種ごとの越境移転ニーズ等アンケート調査

(1) 調査目的

日本国内の事業者に対して、業種[4]毎に越境移転ニーズ等（業種ごとの越境移転の実施の有無や越境移転を実施する上での懸念点、新規参加することで認証取得の誘因となる法域等を指す。）を定量的に調査・分析するため、郵送及び Web 回答のアンケート形式で調査を実施した。

また、このアンケート調査結果をもとに、GCBPR 取得のニーズがあると判明した業種等を中心に、アンケート項目に対するより詳細な質問や、GCBPR 取得のボトルネック及び認証取得のインセンティブを探るべく 2.2 に記載する事業者ヒアリングの対象事業者を選定した。

さらに、アンケート調査結果より、日本事業者が個人情報の越境移転先として取引の多い国や地域のうち、GCBPR への参加意思を示している法域、参加見込みが低い法域、GCBPR メンバー法域を除いた結果、2.6 に記載する各国法令と GCBPR のプログラム要件とのマッピング分析を行う法域を選定した。

(2) 実施期間

2025 年 10 月 2 日（木）～2025 年 11 月 3 日（月）

(3) 調査対象

事業分野や事業規模に偏りが出ないよう 20 業種各 100 社、計 2,000 社及び JIPDEC の DM 配信希望者として登録している約 22,500 社を抽出し、特に個人データの取扱いが多いと想定される製造業、情報通信業、卸売業・小売業、金融業・保険業、サービス業等を中心にアンケート調査を実施した。

[4] 業種は、日本標準産業分類（平成 25 年 10 月改定）における大分類及び中分類を指す。以降同じ。

図表 1　調査対象 20 業種の内訳

	日本標準産業分類		日本標準産業分類
1	農林漁業、鉱業、砕石業、 砂利採取業、建設業	11	情報通信業
2	製造業（食料品、飲料・たばこ・ 飼料）	12	運輸業、郵便業
3	製造業（繊維工業、木材・木製品、 家具・装飾品）	13	卸売業、小売業
4	製造業（パルプ・紙・紙加工品、 印刷・同関連業）	14	金融業、保険業
5	製造業（化学工業、石油製品・ 石炭製品）	15	不動産業、物品賃貸業
6	製造業（プラスチック製品、 ゴム製品、窯業・土石製品）	16	学術研究、専門・技術サービス業
7	製造業（鉄鋼業、非鉄金属、 金属製品）	17	宿泊業、飲食サービス業、 生活関連サービス業、娯楽業
8	製造業（機械器具・デバイス・ 電子回路、電気機械器具）	18	教育、学習支援業
9	製造業（情報通信機械器具、 輸送用機械器具）	19	医療、福祉
10	電気・ガス・熱供給・水道業	20	複合サービス事業、サービス業 （他に分類されないもの）

(4)　回答事業者数

634 社から有効回答を得た。

(5)　調査方法

①　郵送

対象事業者 2,000 社に対し、調査票を URL 及び QR コード付きで郵送し、Web にて回答を回収した。

②　メール配信

JIPDEC データベース登録者 22,500 件に対し、調査票の URL をメール配信し、Web にて回答を回収した。

(6) 質問項目

アンケートの質問数は回答率が低下しないよう 10 問とし、事業者の基本情報と個人データの越境移転に関する詳細な項目について質問を行った。基本情報に基づく主な質問項目は、クロス集計が行いやすい項目を以下のとおり設定した。

＜個人データの越境移転について＞

基本情報＜属性情報＞

- 業種:農林漁業から複合サービス事業まで、20 業種区分から選択
- 従業者数:1～4 名から 10,000 名以上まで、10 区分から選択
- 売上高:5,000 万円未満から 1,000 億円以上まで、8 区分から選択
- 資本金:200 万円未満から 100 億円以上まで、9 区分から選択
- 個人情報に係る第三者認証の取得状況:取得している認証制度名、取得していない理由、検討中の認証制度名

Q1:越境移転の目的

個人データを越境移転する目的について、以下の選択肢から複数選択可能とした。

- ❑ 自社の事業に係るサービス提供のため
  (サービス改善、新規サービス開発、業務効率化を含む。以下同じ。)
- ❑ 自社の人事情報の管理等業務のため
- ❑ 自社と第三者との共同事業に係るサービス提供のため
- ❑ 自社の事業／自社と第三者の共同事業に係る広告/マーケティングのため
- ❑ 第三者の事業に係るサービス提供のため
- ❑ 第三者の事業に係る広告/マーケティングのため
- ❑ その他

Q2:移転先の属性

提供先の属性について、以下の選択肢から複数選択可能とした。

- ❑ グループ会社
  (選択した場合の追加質問)拠点数、職員数、所在国・地域
- ❑ 広告配信事業者(広告配信を主たる事業とする者)
  (選択した場合の追加質問)所在国・地域
- ❑ クラウドサービス事業者(SaaS 等の利用)
  (選択した場合の追加質問)利用サービス数、サービス内容、事業者名、データの移転先(国・地域)
- ❑ 広告配信事業者・クラウドサービス事業者を除く事業者
  (選択した場合の追加質問)所在国・地域
- ❑ 行政機関等

（選択した場合の追加質問）データの移転先（国・地域）

❑ その他

Q3:移転する情報の種類

提供する個人データの項目について、従業員情報と顧客等情報に分けて、該当するものをすべて選択し、情報の種類ごとに件数規模を（10 件単位、100 件単位、1,000 件単位、10,000 件を超える）1つだけ選択するよう求めた。

❑ 従業員情報

- 氏名
- 住所、電話番号、性別、メールアドレス
- 顔画像
- 生体情報等の個人識別符号（法第 2 条第 2 項第 1 号）
- パスポート番号、免許証番号、被保険者証番号等の個人識別符号（法第 2 条第 2 項第 2 号）
- 要配慮個人情報（法第 2 条第 3 項）
- 位置情報、行動履歴、フィジカル空間のログ情報
- Web サイトの閲覧履歴、オンラインにおける購買履歴等、デジタル空間におけるログ情報

❑ 顧客等情報（従業員以外）

- 氏名
- 住所、電話番号、性別、メールアドレス
- 顔画像
- 生体情報等の個人識別符号（法第 2 条第 2 項第 1 号）
- パスポート番号、免許証番号、被保険者証番号等の個人識別符号（法第 2 条第 2 項第 2 号）
- 要配慮個人情報（法第 2 条第 3 項）
- 位置情報、行動履歴、実店舗における購買履歴等、フィジカル空間のログ情報
- Web サイトの閲覧履歴、オンラインにおける購買履歴等、デジタル空間におけるログ情報
- その他

Q4:移転先での利用目的

提供先における利用態様等について、該当するものをすべて選択するよう求めた。

❑ 本人への連絡、広告配信等の接触

❑ 人事情報の管理等業務

❑ 提供先が有する他の個人情報又は個人関連情報との突合

❑ 分析・プロファイリング

- ❑ 統計情報の作成、統計的分析
- ❑ その他
- ❑ 分からない

Q5:個人データの移転根拠

個人データの移転根拠について、該当するものをすべて選択するよう求めた。

- ❑ GDPR:十分制認定
- ❑ GDPR:BCR(拘束的事業者準則)
- ❑ GDPR:SCC(標準契約条項)
- ❑ 個別契約の締結
- ❑ 本人同意
- ❑ APEC/Global CBPR システム
- ❑ その他

Q6:本人同意とサービスの利用

本人が同意をしなかった場合にいかなる影響を受けるかについて、以下から1つ選択するよう求めた。

- ❑ 本人は提供行為に同意しない場合であってもサービスの提供を受けることができる
- ❑ 本人は提供行為に同意しない場合にはサービスの提供を受けることができない
  (選択した場合の追加質問)
  - サービス提供のために提供行為が不可欠であり、同意を取得しないと、サービスを提供することができないため
  - 同意管理が困難/コストがかかるため
  - その他( )

Q7:越境移転における課題

個人データの越境移転において、課題と思われる項目について、該当するものをすべて選択するよう求めた。

- ❑ 移転先のデータ保護規制の理解と対応に時間を要する
- ❑ 日本と移転先国のデータ保護ルールに違いがあるため調整が困難
- ❑ 現在の対応が双方の法制度において安全管理が十分か不安である
- ❑ 契約の締結、規制等への対応コスト(法務含む)が負担である
- ❑ 日本と同等の取扱いルールに応じてもらえない(必要情報の非開示を含む)
- ❑ 分からない
- ❑ 特に課題は感じられない。この項目を選択した場合、その理由を教えてください。
  理由:( )
- ❑ その他

Q8:今後拡大予定の移転先の国や地域

個人データの越境移転先国や地域として、今後拡大予定或いは直近で拡大した国や地域について、以下から1つ回答するよう求めた。

- ❑ 直近(3 年以内程度)で新たに移転を開始した国や地域
- ❑ 今後予定している越境移転先の国や地域
- ❑ 現状の移転先から拡大の予定はない
- ❑ 移転先の国や地域を縮小予定である(理由記述)

◆越境移転に限らない情報の取扱い全般に対する取組

個人情報の取扱いに関する取組全般について、現在、又は今後予定されていることも含め、取組状況の回答を求めた。

Q9:個人情報の適正な取扱いに対する取組

個人情報の取扱いに関する、顧客の声・懸念を反映させるための体制構築や広報活動等、個人情報の適切な取扱いについて、どのような取組を行っているのかを、例示を記載し自由記述で回答するよう求めた。

Q10:本人同意を要しない情報の利活用等

目的外利用や第三者提供に係る本人同意を取得することなく個人情報を利活用するために行っている施策について、該当するものをすべて選択するよう求めた。

- ❑ 個人情報を統計情報に加工して利用している
- ❑ 仮名加工情報制度を利用している
- ❑ 匿名加工情報制度を利用している
- ❑ 個人情報の取得時に、将来行う可能性がある利用目的も含めて、幅広に利用目的を特定している/将来行う可能性がある個人データの第三者への提供行為も含めて、幅広に同意を取得している
- ❑ 行っていることはない
- ❑ その他

(7) 調査結果

① 個人データの越境移転の目的(Q1)

個人データを越境移転する目的は、「移転先なし」と回答した企業を除く279社[5]のうち、「自社の事業に係るサービス提供のため」(180 件、64.5%)と、「自社の人事情報の管理等業務のため」(130 件、46.6%)が上位を占めた。これは、自社サービス提供や従業員に関わる個人情報管理が越境移転の主要な目的であることを示している。

一方、広告/マーケティングを目的とした越境移転は低い数字に留まっており、「第三者の事業に係る広告/マーケティングのため」(15 件、5.4%)と、最も少ない件数を示した。

② 移転先の属性(Q2)

移転先の属性は、「移転先なし」と回答した企業を除く 257 社のうち、「クラウドサービス事業者(SaaS 等の利用)」(87 件、33.9%)と「グループ会社」(82 件、31.9%)が高い割合を示した。詳細は以下のとおり。

図表 2 移転先の属性

移転先の属性	属性ごとの主な内容
クラウドサービス事業者 (87 件)	・クラウドサービスの利用社数は、5 社以下(72 件、82.8%)が 8 割を超える結果である一方、21 社以上(4 件、4.6%)利用している企業も僅かに見られた。データの移転先は1か国(55 件、63.2%)が最も多く、次いで 2 か国(16 件、18.4%)であった。 ・なお、多く利用されているサービスは、ストレージ・グループウェア系、コミュニケーション系、勤怠管理、安否確認等の業務管理系、基盤系サービスであった。 ＜多く利用されているサービス＞ ※%は 87 件に占める利用率 • Microsoft 365(Teams、Outlook、OneDrive 等): 約 60% • Google Workspace(Gmail、Drive、Meet 等): 約 40% • AWS(Amazon Web Services): 約 25% • Zoom: 約 20% • Slack、Box、Salesforce:それぞれ約 15%
グループ会社 (82 件)	・現地法人の拠点数は、5 拠点以下(56 件、68.3%)が最も多く、次いで 51 拠点以上(10 件、12.2%)であった。職員の数は、101 名以上(34 件、41.5%)が 4 割を占めた以外は、職員数の数による違いは見られなかった。

[5] Q1 は、調査対象としての母数は n=634 であるが、その他の選択肢に「移転先なし」と回答した 355 社を除く、279 社を分母として算出。Q2～Q7 は、回答に正確を期すために、アンケート回答欄に「移転先なし」と回答があった企業を除いたものを母数として集計を行ったため、質問毎に分母が異なる。

移転先の属性	属性ごとの主な内容
	・また、所在する国や地域は、1 か国（41 件、50%）が最も多く、次いで、5 か国（15 件、18.3%）となっており、拠点数と同様に、少ないか多いかに二分される結果となった。

③ 移転する情報の種類（Q3）

移転する個人データの種類は、「移転先なし」と回答した企業を除く 284 件のうち、「従業員情報」（194 件、68.31%）と、「顧客等情報（従業員以外）」（137 件、48.24%）が一定割合存在した。また、「従業員情報」と回答した 194 件のうち、従業員情報の内訳は、「氏名」（191 件、98.5%）、「住所、電話番号、性別、メールアドレス」（164 件、84.5%）が主要な項目となっている。顧客等情報においても同様に 2 項目が高い割合を示した。

④ 移転先での利用目的（Q4）

提供先における利用態様等は、「移転先なし」と回答した企業を除く 338 件のうち、「人事情報の管理等業務」（126 件、37.3%）が一番多く、「本人への連絡、広告配信等の接触」（93 件、27.5%）と続いた。

⑤ 個人データの移転根拠（Q5）

個人データの移転根拠は、「移転先なし」と回答した企業を除く 272 件のうち、「本人同意」（202 件、74.3%）が最も多く、「個別契約の締結」（119 件、43.8%）が続く。

一方で「GDPR：十分性認定」（68 件、25.0%）や、BCR、SCC を含む GDPR を移転根拠と回答した企業は少なかった。「その他」と回答した多くは「該当なし」であったが、「分からない」とした回答も相当数見られた。

⑥ 本人同意とサービス利用（Q6）

本人が同意しなかった場合の影響は、約7割の事業者が「サービスの提供を受けることができない」（454 件、71.6%）という結果となった。

また、その理由は、「移転先なし」と回答した企業を除く 253 件のうち、「サービス提供のために提供行為が不可欠であり、同意を取得しないと、サービスを提供することができないため」（236 件、93.3%）が 9 割以上を占めた。情報の提供行為がなければ、ほぼサービスを利用することができない現状が明らかになった。

⑦ 越境移転における課題（Q7）

個人データの越境移転における課題は、「移転先なし」と回答した企業を除く524件のうち、「移転先のデータ保護規制の理解と対応に時間を要する」（195 件、37.2%）、「日本と移転先国のデータ保護ルールに違いがあるため調整が困難」（166 件、31.7%）が上位となった。

また、「分からない」（174 件、33.2%）との回答も多く見られた。

⑧　今後拡大予定の移転先の国や地域（Q8）

今後拡大予定の越境移転先について、多くの事業者が現状維持の傾向を示した。また、拡大を予定している事業者の越境移転先は、米国、欧州、東南アジア、中東、アフリカとなっており、特定の地域に偏ることなく様々な国や地域を検討していることが分かった。

越境移転先を縮小予定であると回答した事業者は少数であり、縮小の理由は「費用削減及びカントリーリスクの低減」等が挙げられた。

⑨　個人情報の適正な取扱いに対する取組（Q9）

個人情報の適正な取扱いに関する取組として、多くの事業者が「個人情報の取扱いに特化した顧客の声を受付ける窓口の設置」や「自社 Web サイトでの個人データ利活用に関する取組の紹介」を実施していることが分かった。プライバシーマーク[6]（以下、「P マーク」という。）付与事業者では、構築運用指針に基づき、JIS Q 15001 に準拠した体制構築や定期的な内部監査・教育を実施している事例が多く見られた。

⑩　本人同意を要しない情報の利活用等（Q10）

本人同意を要しない個人情報の利活用施策は、「行っていることはない」（436 件、69.5%）と回答した企業が最も多かった。

また、実施していると回答した内容は、「個人情報の取得時に、将来行う可能性がある利用目的も含めて、幅広に利用目的を特定している」（98 件、15.6%）、「個人情報を統計情報に加工して利用している」（61 件、9.7%）の順となった。

(8) アンケート調査結果のまとめ

本調査により、日本企業における個人データの越境移転は、主に自社サービスの提供や人事情報の管理を目的として、クラウドサービス事業者及びグループ会社への移転が行われており、本人同意を移転根拠としたものが主であった。

一方で、各国のデータ保護規制の理解と対応に時間を要することや日本と移転先のデータ保護ルールの違いによる調整の困難さが、越境移転時の主要課題として明らかになった。

2.2. 調査 2.1.を踏まえた企業ヒアリング

(1) 調査目的

調査 2.1.を踏まえ、GCBPR のニーズがあると判明した業種の企業を対象として、アンケート項目に対する詳細な回答や、GCBPR 取得のボトルネック等についてヒアリングを行い、GCBPR を含む第三者認証制度の課題を整理する。

---

[6] 個人情報を適切に管理する体制を整備していると評価された事業者（企業や団体）が使用できる、信頼の証となるマーク。

(2) 実施期間

2025 年 11 月 11 日(火)～2025 年 11 月 27 日(木)

(3) 調査対象

調査 2.1.のアンケートで、ヒアリングに応じても良いと回答した事業者の中から、業種、事業分野、事業規模等も検討し、GCBPRの認証を取得している事業者(以下、「認証事業者」という。)1 社を含む計 9 社に対し、ヒアリングを行った。

なお、本調査の契約期間内にヒアリングの日程調整が可能な事業者(日本の認証事業者を含む)に対して実施した。また、個人データの越境移転が発生していない事業者、対応可能であると誤って回答した事業者は除いた。

ヒアリング対象事業者の概要は、以下のとおり。

図表 3 ヒアリング調査実施記録

	実施日時	対象事業者
1	2025/11/11(火) 13:00-14:00	A 社(複合サービス事業、サービス業) ＜イベント・体験型マーケティング＞
2	2025/11/12(水) 13:30-14:30	B 社(情報通信業) ＜システム開発・保守＞
3	2025/11/14(金) 14:00-15:00	C 社(複合サービス事業、サービス業) ＜IT 分野・人材サービス＞
4	2025/11/20(木) 10:00-11:00	D 社(情報通信業) ＜電子決済サービス＞
5	2025/11/21(金) 10:30-11:30	E 社(情報通信業) ＜ソフトウェア開発他＞
6	2025/11/25(火) 10:00-11:00	F 社(情報通信業) ＜コンサルティング＞
7	2025/11/25(火) 16:00-17:00	G 社(教育、学習支援業)
8	2025/11/26(水) 10:00-11:00	H 社(学術研究、専門・技術サービス業)
9	2025/11/27(木) 10:00-11:00	I 社(複合サービス事業、サービス業) ＜システム販売・保守＞

図表 4 ヒアリング対象事業者の属性

業種	従業員数	売上高
情報通信業	20～49 名	1～10 億円未満
情報通信業	100～299 名	10～50 億円未満
情報通信業	1,000～4,999 名	100～500 億円未満
情報通信業	5,000～9,999 名	1,000 億円以上
複合サービス事業、サービス業（他に分類されないもの）	50～99 名	10～50 億円未満
複合サービス事業、サービス業（他に分類されないもの）	50～99 名	50～100 億円未満
複合サービス事業、サービス業（他に分類されないもの）	500～999 名	100～500 億円未満
教育、学習支援業	1,000～4,999 名	50～100 億円未満
学術研究、専門・技術サービス業	50～99 名	10～50 億円未満

(4) 調査項目

ヒアリング項目は、16 項目（計 27 の設問）で、個人データの越境移転が生じる業務形態や越境移転先の国や地域及び委託先、委託先との契約等において困っていることの有無、GCBPR の認知度や取得へのインセンティブ、GCBPR 以外の認証制度の取得状況や国内での GCBPR 普及・拡大等を設定した。

具体的なヒアリング項目は、以下のとおり。

図表 5 ヒアリング項目

設問内容
1. 個人データの越境移転を行う業務は次のどちらに該当しますか？ ① 業務委託（移転先や委託先が複数ある） ② 現地法人と従業員情報のやり取りをする程度（移転先は限定的）

設問内容
2. 個人データの越境移転の状況や移転先での個人データの取扱いの状況についてお聞かせください。 ① 個人データの移転先（国や地域）はどれ位ありますか？ ② また、移転先との契約等において困っていることがありましたら教えてください。 例）移転先の法制度の理解と付随するコスト、契約書の作成に要する労力等 ③ 個人データの委託先はどれ位ありますか？ 例）クラウドサービス（SaaS 等）を使った業務委託の状況等
3. Global CBPR 認証[7]又は APEC CBPR 認証についてお聞きになったことはありますか？（理解度：聞いたことがある／調べたことがある／取得を検討している等）
4. CBPR 認証制度の所管官庁（個人情報保護委員会、経済産業省）や審査機関（JIPDEC）等の Web サイトで CBPR 認証事業者が公表されていることを知っていますか？
5. Global CBPR 認証又は APEC CBPR 認証について、取得に至っていない理由は何ですか？
6. 取得を検討するとしたら最も重要な決定要素は何ですか？
7. CBPR 認証の取得を検討する場合（既に検討している場合を含む）、CBPR 認証制度の所管官庁（個人情報保護委員会、経済産業省）や審査機関（JIPDEC）が提供する HP における公開情報について、CBPR 認証制度の一般的な説明に加え、検討の便宜に資する情報があれば教えてください。 例）具体的な費用の目安、取得までに要する期間、日本・他国の認証事業者の情報、既に認証を受けている事業者の認証取得による具体的なメリット等の意見　等
8. 以下の選択肢は取得のインセンティブになり得ますか？ • Q4 に記載の所管官庁や審査機関 Web サイト等での事業者名の公表 • 認証事業者、所管官庁、審査機関等との間で CBPR を通じた越境データの適正な取扱いに関するエコシステム（ネットワーク）の形成
9. 同業他社や取引先事業者（海外事業者含む。）で、Global CBPR/APEC CBPR 認証を取得している事業者はありますか？
10. Global CBPR 認証は、事業者にとって有効（必要）だと思いますか？ 回答：はい・いいえ　理由：
11. GDPR 等の規則や法（例：十分性認定/BCR/SCC）等と比較した場合、Global CBPR 認証/APEC CBPR 認証のメリット及びデメリットは何ですか？

[7] 報告書本文で認証制度を表記する場合、「GCBPR」としているが、ヒアリング項目はヒアリングを受ける事業者に分かりやすいよう「GCBPR 認証」とした。

設問内容
12. CBPR 以外の認証を取得していますか？ ➢ している ① 認証制度名 ② 認証取得の理由 ③ 認証制度の効果 ④ 申請手続き・認証取得後の運用等で改善して欲しいことはありますか？ ➢ していない： ① 理由： ② 今後取得の予定 - あり：取得予定の認証制度名 - なし：理由
13. CBPR 認証や他の認証制度も含め、第三者認証制度の効果として最も期待することは何ですか？
14. 日本では導入されていない GCBPR のグループ認証についてお尋ねします。 ※グループ認証とは、親会社と同じプライバシーポリシーに基づく情報の取扱いを行っている前提で、子会社も含めて認証されることを言います。現在、日本では個社単位での認証となりますが、アメリカ、シンガポールでは、グループ認証を取得することができます。 ➢ 日本子会社： 国内に子会社がある場合、子会社もまとめて認証される運用（親会社と同一ポリシーが徹底されていることが前提）は、CBPR 認証を取得する動機に繋がりますか？ ➢ 海外子会社： 海外に子会社がある場合、子会社もまとめて認証される運用（親会社と同一ポリシーが徹底されていることが前提）は、CBPR 認証を取得する動機になりますか？ ➢ 子会社の有無を問わず、グループ認証はあった方が良いと思いますか？ 回答：はい・いいえ　理由：
15. 日本では導入されていない GCBPR の PRP 認証についてお尋ねします。 ※PRP 認証とは、プロセッサー（ベンダーやクラウド事業者等、顧客データをクライアントから預かって処理を行う事業者）向けの認証です。日本では、コントローラーやプロセッサーの区別が法の定義上なく「個人情報取扱事業者」のみのため未実施。 ➢ PRP 認証が開始された場合に CBPR 認証を取得する動機になりますか？ ➢ プロセッサーであるか否かを問わず、PRP 認証はあった方が良いと思われますか？ 回答：はい・いいえ　理由：

設問内容
16. Global CBPR 認証の日本での拡大についてお尋ねします。 ➢ 認知度を高めるために、どのような方法が効果的だと思いますか？ ➢ 拡大フェーズの施策として、審査料が一定期間無料になる等の特典は認証事業者数拡大に有効だと思いますか？ ➢ CBPR 認証のような越境移転ツールが、日本でより多くの事業者が取得したいと思われるようになるためには、何が必要だと思いますか？ 例）コンプライアンス又はアカウンタビリティを示すツールとして有効であることをPR する、契約の獲得に影響する（新規契約、政府の受託事業等）

(5) 実施方法

Web 会議によりヒアリングを実施した。また、ヒアリングは個人情報保護委員会より趣旨説明を行った後、実施機関が事業者へのヒアリングを行い、必要に応じて、回答に関連する詳細を確認する形式とした。

(6) 調査結果[8]

Q1. 個人データの越境移転を行う業務は次のどちらに該当しますか？

① 業務委託（移転先や委託先が複数ある）

【概観】

①に該当すると回答した事業者は 9 社中 6 社であった。これらの事業者は、海外の開発拠点への業務委託や、クラウドサービス（SaaS）の利用を通じて個人データを越境移転している。移転先は主にアメリカが中心であるが、インド、欧州、中東、東南アジア等複数の国・地域にわたるケースも見られた。大規模なユーザー情報を扱う事業者では、海外拠点での開発業務にユーザー情報や従業員情報を移転する形態が確認された。また、シンクタンク業務として海外調査を行う事業者では、取材や調査の外注先が複数国に存在するという特徴が見られた。

また、公共団体向け事業を行う事業者では、GIS（地理情報システム）関連のクラウドサービスを利用しており、サーバーが海外にあるため越境移転が発生しているケースも確認された。翻訳・通訳業務を行う事業者では、翻訳支援ツールやオンライン会議ツール等の複数の SaaS を利用しており、委託先が 40 社以上に上るケースも見られた。

＜各社の主な意見＞

- 越境移転という観点では、例えば、Box、OneDrive 等、海外のクラウドサービスの利用時に個人情報を扱っている。
- 海外の現地法人と従業員情報のやり取りはあるが、業務委託が主な業務である。

[8] ヒアリング項目の Q1～Q16 は、全ての事業者に共通する項目であり、認証事業者へは別途追加の 4 問をヒアリングしている。

② 現地法人と従業員情報のやり取りをする程度（移転先は限定的）

【概観】

②に該当すると回答した事業者は 9 社中 3 社であった。いずれも親会社又は提携先が海外にあり、従業員情報や学生情報といった特定の情報のみを限定的にやり取りする形態であった。移転先はアメリカ又は EU 圏の 1 か国に限定されており、業務委託型と比較すると移転の範囲は狭い。ただし、親会社が海外にある場合は、本社のルールやシステムに従う必要があり、現地の法制度への対応が課題であることが示された。

＜各社の主な意見＞

- 海外の大学と提携し、日本の学生情報を当該大学に提供している。業務委託でも現地法人でもない形態だが、海外へ個人情報の移転が発生している。弁護士事務所を通じて海外の法域を含む契約を締結しており、今後、アジア地域への展開も視野に入れている。
- 現地法人はアジア圏にあり、従業員情報のやり取りを行っている。

③ その他（どちらにも明確に該当しない例）

一部の事業者では、①②のいずれにも明確に該当しないケースが見られた。具体的には、業務委託や現地法人は持たないものの、クラウドサービス（ファイル共有サービス、名刺管理サービス等）の利用を通じて、意図せず個人データが海外に移転している可能性がある事業者である。こうした事業者は、自社が越境移転を行っているという認識が薄く、移転先の国や地域も正確には把握できていない状況にあった。

Q2. 個人データの越境移転の状況や移転先での個人データの取扱いの状況についてお聞かせください。

① 個人データの移転先（国や地域）はどれ位ありますか？

【概観】

移転先の国・地域数は事業者の業態や事業規模によって大きく異なった。最も多いパターンは、クラウドサービスの利用に伴うアメリカへの移転であり、ほぼすべての事業者がこれに該当した。一方、海外に開発拠点や現地法人を持つ事業者、海外調査業務を行う事業者では、アジア、中東、欧州等複数の国・地域への移転が発生していた。また、クラウドサービスを利用している事業者の多くは、サービス提供事業者の本社所在地は把握しているものの、実際のサーバー所在地までは正確に把握できていないという実態が明らかになった。

さらに、クラウドサービス事業者に問い合わせてもサーバーの具体的な所在地が明かされないケースがあり、「分散バックアップにより安全性を担保している」という説明を受けても、利用事業者側からは「情報の拡散が広がっている」という懸念を感じるとの声もあった。

＜各社の主な意見＞

- アメリカに本社があり、共通の人事管理システムを利用している。本社所在地は把握しているが、システムのサーバーがどこに置かれているかまでは把握していない。
- 利用しているクラウドサービス事業者の本社所在地に基づき、アメリカ、スイス、ドイツが主な移転先となっている。
- クラウドサービス（ファイル共有サービス等）を利用しているが、サービス提供事業者の業務がどこで行われているかは見えず、移転先の国を特定できていない。

② 移転先との契約等において困っていることはありますか？

【概観】

契約締結の段階で直接的に困っているという回答は少数であった。しかし、移転先国の法制度への理解不足、法改正情報の入手困難、クラウドサービス事業者との交渉力の格差、サービス終了時のデータ取扱いの不透明さ等、越境移転を行う事業者に共通する課題を多く抱えていることが明らかになった。

具体的には、SaaS の利用においては一般的である利用規約での契約は、利用規約をどこまで読み込めばよいのか判断が難しいこと、海外事業者への問い合わせ先が分かりにくいこと、提供される資料が日本語でないこと等から、情報収集に工数がかかるという課題が指摘された。特に、親会社や提携先が海外にある事業者では、現地の個人情報保護に関する法制度等への対応が課題となっていた。また、中小企業からは、大手クラウドサービス事業者との契約において、自社の要望がとおりにくいのではないかという懸念も示された。

＜各社の主な意見＞

- 海外の親会社が準拠する現地法と日本の個人情報保護法の両方に対応する必要があり、現地法が改正された際に情報が入ってこないことが課題である。入社時の同意書に記載された外国法に基づく情報の取扱いは、担当者レベルでは説明が難しい。
- 日本と海外の両方に事務所を持つ弁護士事務所に対応を依頼しており、契約上の困りごとは現時点ではないが、専門家を探すこと自体は大変であった。
- 現状ではクラウドサービスの利用が主であるため大きな困りごとはない。しかし、今後顧客から海外でのサービス利用に関し、何らかの注釈がついた場合、大手サービス事業者と綿密な連絡が必要になる可能性があり、自社のような小規模事業者の要望が通るか不安がある。クラウドサービス利用における事業者の選定・評価段階で、公開されていない情報をどこまで掘り下げて調査すべきかが課題である。特に、サービス終了時に委託している個人情報がどのように扱われるかがほぼ明示されておらず、突然終了通知を受けた場合の対処が不明確である。

③　個人データの委託先はどれ位ありますか？

【概観】

委託先の数は事業者によって異なるが、多くの事業者がクラウドサービス（SaaS）を利用しており、これが実質的な委託先となっている。具体的には、ファイル共有・ストレージサービス、人事管理システム、名刺管理システム、クラウドインフラ（AWS、Google Cloud 等）等が挙げられた。委託先の数は 2～3 社から 40 社以上まで幅があった。翻訳・通訳業務のように多数の SaaS を利用する業態では、クラウド事業者だけで 25 社、それ以外を含めると 40 社以上の委託先を管理しているケースも確認された。

一方で、クラウドサービスの利用を「委託」として認識していない事業者も見られ、越境移転に関する認識の差にバラツキが確認された。また、できるだけ国内サーバーを利用するよう方針を定めている事業者もあったが、一部の機能で海外のサーバーを経由する可能性を完全に排除できていない状況も見られた。

＜各社の主な意見＞

【10 社未満】

- 本社とファイル共有サービスの 2 社程度である。ファイル共有サービスを委託先として認識していなかったが、情報を管理しているという意味では該当する。
- 委託はしていない。オンライン会議ツール等は使用しているが、国内のみでの使用であり、越境移転は発生していない。
- ファイル共有サービス 2 社と名刺管理サービス 1 社の計 3 社を利用している。名刺管理サービスが海外にサーバーを持っているかどうかまでは把握できていない。

【10～30 社未満】

- 利用しているクラウドサービスとして、大手 IT 事業者やクラウドストレージ、オンライン会議ツール、リモートアクセスツール、クラウドインフラ等約 10 社程度が挙げられる。

【30 社以上】

- クラウド事業者が 25 社、それ以外（親会社への業務委託、レンタルサーバー、配送業者等）が 18 社である。

Q3. Global CBPR 認証又は APEC CBPR 認証についてお聞きになったことはありますか？

【概観】

認知度は総じて低い水準にとどまっていることが明らかで、認知の状況は大きく 3 つのカテゴリに分類できた。

第一に、「今回初めて知った」という完全に認知していなかったケース。

第二に、「名称を聞いたことがある程度」というごく表面的な認知にとどまっているケース。

第三に、「セミナー等で情報を得たことがある」というケースである。

最も多かったのは第二のパターンであり、審査機関からのニュースレターや案内メール、ウェブサイト等で名称を目にしたことがあるものの、制度の詳細までは理解していないという事業

者が多数を占めた。特に、SaaS を利用する側の事業者からは、CBPR は「SaaS を提供している会社が取得すべきもの」という認識があり、自社が取得すべき立場にあるという理解が追いついていないとの声もあった。

また、認知していた事業者であっても、自社での取得検討には至っていないケースがほとんどであり、「必要性を感じていない」「検討したことがない」という回答が目立った。認知から検討・取得へのステップに大きなギャップが存在することが示唆された。

＜各社の主な意見＞

【初めて知った】

- GCBPR を初めて知った。越境移転の認証取得は、これまで検討したことがない。
- GCBPR を初めて知った。第三者認証（越境移転含む）の取得は検討したことがない。

【名称を聞いたことがある程度】

- 審査機関のホームページを確認していた際に目にしたことがある程度であり、「聞いたことがある」というレベルの認識にとどまっている。
- 個人情報の担当になったのがここ半年程度のため、名称を聞いたことがあるレベルである。今回の問い合わせを受けて、「何か共通的な制度を作ろうとしているのだな」という程度の認識である。

【セミナー等で情報を得たことがある】

- GCBPR のセミナーに参加したことがある。海外との事業連携が始まる頃に、きちんと学んでおく必要があると考えて聞きに行った。ただし、「聞いたことがある」というレベルの理解にとどまっている。

Q4. CBPR 認証制度の所管官庁（個人情報保護委員会、経済産業省）や審査機関（JIPDEC）等の Web サイトで CBPR 認証事業者が公表されていることを知っていますか？

【概観】

認証事業者の公表を事前に認知していた事業者は１社のみであり、大多数の事業者は「知らなかった」又は「今回のヒアリングをきっかけに初めて確認した」という状況であった。

認知状況は大きく 3 つのカテゴリに分類できた。

第一に、「以前から知っていた」という事業者。

第二に、「今回のヒアリングをきっかけに確認した」という事業者。

第三に、「全く知らなかった」という事業者である。第二・第三のパターンが大多数を占めており、認証事業者の公表情報が事業者に十分に届いていない実態が明らかになった。

＜各社の主な意見＞

【以前から知っていた】

- 知っている。（審査機関からのニュースレター等で制度を調べたことがあり、その過程で公表情報も把握していた）

【今回のヒアリングをきっかけに確認した／全く知らなかった】

- このヒアリングの話をいただいた後に確認を始めた段階である。所管官庁や審査機関等で認証事業者が 4 社程度公表されているという情報と、過去のレポート等に目を通し始めたところであり、正しい認識を持つには至っていない。
- 今回のヒアリングに先立ち、メールで案内された URL を確認して初めて知った。

Q5. Global CBPR 認証又は APEC CBPR 認証について、取得に至っていない理由は何ですか？

【概観】

取得に至っていない理由は、複数の要因が複合的に作用していることが明らかになった。

最も多く挙げられた理由は「自社業務における必要性を感じていない」というものであり、海外との直接的な個人情報のやり取りがない、又は限定的であるという認識に基づいていた。次いで多かったのは「認知度・理解度の不足」であり、制度の存在自体を知らない、あるいは知っていても詳細を理解していないため検討段階に至っていないというケースであった。また、「メリットが不明確」「費用対効果が見えない」という声も複数あり、取得によって得られる具体的なベネフィットが経営層や社内に説明しにくいという課題が示された。

さらに、外資系事業者の日本法人特有の事情として「本社への影響」を懸念する声や、「大企業向けの認証という印象」から自社には関係ないと感じているケースも見られた。

また、SaaS を利用する側の事業者からは、「自社はサービスを利用する立場であり、認証を取得すべきは SaaS 提供事業者側ではないか」という意見も示された。「グローバル CBPR を取得することで、自社にどのようなメリットがあるのかが理解できていない」という声もあり、制度の理解促進が課題として浮かび上がった。

＜各社の主な意見＞

【自社業務における必要性を感じない】

- 基本的に顧客から個人情報を取り入れることがなく、社内情報の管理以外に個人情報を扱っていない。そのため、グローバルな認証まで取得する必要性を感じていない。
- 当社の事業は日本の個人情報を海外に提供する形態であり、海外から個人情報を持ってくるわけではないため、現時点では該当しないという認識である。ただし、今後必要になる可能性があることは認識しており、動向は注視している。

【認知度・理解度の不足】

- クラウドサービス利用において、実際は個人情報が越境移転しているという認識で業務を行っているメンバーはいるが、その認識は一部に限られており、組織全体としての認識に至っていない。
- 知らなかったということ以外では、知って調べてみて、これを自社が取るべきなのか、委託先が取るべきなのかを考えた。おそらく委託先の会社が取るべきなのではないかという認識でいる。
- こういった認証があることを知らなかったのが一番大きな理由である。自社はサービスを利用する側の立場であり、取得すべき立場にあるという理解がまだ追いついていない。SaaS 提供会社が認証を取っていれば、そういうサービスを選択できるが、自社が取得することでどんなメリットがあるのかまだ分からない。

【メリットが不明確・費用対効果が見えない】

- メリットが明確ではない。他の保有認証も費用対効果を検討しているため、説得力のある利点がなければ取得は難しい。
- コストと労力に見合う効果がどのくらい出るのか分からない。体制構築や手続き、更新手数料等のコストを考えると、効果が不明確な状態では取得の判断ができない。

【外資系事業者特有の事情】

- 本社が海外にあるため、日本法人が単独で取得すると本社への影響が懸念される。「何を勝手にやっているのか」と言われる可能性があり、子会社の立場としては本社からの指示で取得する方が対応しやすい。

【大企業向けという印象】

- 大手企業が取得する認証という印象がある。取得している 4 社を見ても、規模感が全く違う事業者が取得しているため、自社には関係ないという印象を持っている。

Q6. 取得を検討するとしたら最も重要な決定要素は何ですか？

【概観】

取得検討における決定要素は大きく 3 つのカテゴリに分類できる。

第一に、「外的要因・ビジネス上の必要性」である。顧客からの要請、取引条件への組み込み、入札参加資格としての要件化等、外部からの要求があれば取得を検討するという回答が最も多かった。現時点では顧客や取引先から CBPR の取得について問われることがないため、検討に至っていないという実態が浮き彫りになった。

第二に、「事業環境・業務内容の変化」である。海外との取引再開、海外顧客の受け入れ開始、個人情報を社内で取り扱う業務の発生等、自社の事業環境が変化した場合に検討するという回答があった。

第三に、「既存認証との整合性・追加負担の軽減」である。P マークや他の既存認証を保有している事業者からは、CBPR との重複部分が大きく、追加的な書類作成や運用負担が少なければ検討しやすいという声があった。

その他、外資系事業者の日本法人からは、本社からの指示があれば対応しやすいという、グループ事業者特有の事情も示された。

＜各社の主な意見＞

【外的要因・ビジネス上の必要性】

- ビジネス上の取引要件として、認証事業者であることが求められる場合が決定要素となる。契約に関わる部分でメリットが明示されなければ、取得に動くことははない。
- 顧客から認証取得の依頼があった場合に検討する。現時点では、取引先からのチェックでＰマークやISMSは問われるが、GCBPRは聞かれたことがない。
- おそらく安全対策になると思う。認証を取ることによって、どこまで安全対策が担保できるかということになる。

【事業環境・業務内容の変化】

- 海外の技術者とのやり取りが復活する場合、又は個人情報を社内に持ち帰るような業務が発生した場合に必要になる。
- 海外の顧客を受け入れられる状態になったタイミング、あるいは法制度が変わったタイミングで必要になると認識している。現時点ではすぐに必要という状況ではない。

【既存認証との整合性・追加負担の軽減】

- 現在Ｐマークを取得しているため、CBPR認証との相違が小さい、あるいは延長的に対応できるという点が重要である。申請先が増えるだけで書類作成内容がほぼ同じ、運営コストがほぼ変わらないといった点があれば検討しやすい。
- Ｐマーク用とCBPR用に別々の資料作成を求められると、複数の書類を作成する必要が生じるため、取得の動機が減ってしまう。
- コストと労力に対する効果が決定要素となる。費用対効果が明確でなければ、検討に踏み切ることは難しい。

【グループ事業者特有の事情】

- 本社が海外にあるため、日本法人が独自に取得すると本社への影響が懸念される。本社からの指示で取得するよう言われた方が、子会社の立場としては対応しやすい。

Q7. CBPR 認証制度の所管官庁や審査機関が提供する HP における公開情報について、検討の便宜に資する情報があれば教えてください。

【概観】

事業者が求める情報は大きく 6 つのカテゴリに分類できる。

第一に、「取得プロセス・費用・期間に関する情報」である。申請から認証取得までの流れ、必要な準備、所要期間、費用等の実務的な情報を求める声が多かった。

第二に、「認証事業者の事例・メリットの具体例」である。どのような業種・規模の事業者が取得しているのか、取得によってどのようなメリットを得ているのかといった、実際の活用事例を知りたいという要望が多く寄せられた。

第三に、「自社に必要かどうかの判断基準」である。どのような業務を行っている場合に認証が必要なのか、明確な基準や事例を示してほしいという声があった。

第四に、「中小企業でも取得可能であることの周知」である。現在の取得事業者が大企業中心という印象があり、中小企業でも取得できることを具体的に示してほしいという要望があった。

第五に、「越境移転の実態に関する啓発情報」である。クラウドサービス利用によって意図せず越境移転が発生していることへの認識が低いため、この点に関する情報発信が必要という指摘があった。

第六に、「他の認証制度との関係性・優先順位の整理」が挙げられた。P マーク、ISMS、経済産業省のセキュリティ格付け制度等複数の認証制度が存在する中で、どの認証を優先すべきか判断が難しいという声があった。特に、資金や人材に制約のある事業者からは、CBPR と他の認証制度との関係性、グローバル展開する事業者向けか国内取引中心の事業者向けかといった棲み分けの情報があると、優先順位を付けやすいとの要望が示された。

＜各社の主な意見＞

【取得プロセス・費用・期間に関する情報】

- 費用面、期間、他国の認証状況等、具体的な情報が記載されていることが望ましい。新たに取得する事業者にとって参考になる。

【認証事業者の事例・メリットの具体例を求める意見】

- 取得されている事業者がどのようなメリットを感じているか、どのような点が便利だったかといった情報があると参考になる。
- 同業他社の取得状況も説得材料になる。「皆が取得しているなら」という横並び意識も、取得判断の要素になり得る。
- セミナー実施後の報告として、どのような事業者が参加し、どのような意見があったかを掲載すると、同規模の事業者も目指しているとわかり参考になる。
- 検討している事業者がどこでつまずいているのか、そのポイントが解消できるような具体的情報があると検討が進むのではないか。

【自社に必要かどうかの判断基準】

- 必要性が考えられる具体的な事業分野や業務内容の例示があると参考になる。

- 「こういう場合は絶対必要です」という明確な基準と事例があればよい。

【中小企業向けの事例】

- 現在の取得事業者を見ると大企業ばかりという印象があり、どの程度の規模の事業者が取得しているかがわかると参考になる。
- 中小企業でも取得可能であることを、文字情報だけでなく、事業者の実際の事例や声、図表やイラストを用いて示す方がわかりやすい。

【越境移転の実態に関する啓発情報】

- JIPDEC の Web サイトにある動画の紹介は視聴した。動画と併せて、資料としてホームページに情報が掲載されていると、合わせて確認できてよい。
- 認証制度の説明以前に、クラウドサービス利用時に実は海外への情報移転が起きているという認識が極めて低い。海外拠点や取引がある事業者には理解されやすいが、国内のみで事業展開する事業者には受け入れられていない。この点を発信していく必要がある。
- コンサルティング会社と契約しているが、こういう認証が始まったという話が一切ない。審査機関からコンサルティング会社への情報展開があると、事業者への情報到達が早くなるのではないか。

【他の認証制度との関係性・優先順位の整理

- 既に P マークを取得している場合、それプラス何が必要か、P マークの審査範囲外で何がカバーできるのかという情報がほしい。
- 経産省のセキュリティ格付け制度等複数の認証がある中で、どれを優先したらいいのかという情報がほしい。資金的・人材的制約がある中で、グローバル展開する会社向け、国内取引中心の会社向けの情報があると優先順位を付けやすい。

Q8. 以下の選択肢は取得のインセンティブになり得ますか？

① 所管官庁や審査機関 Web サイト等での事業者名の公表

【概観】

9 社ほぼすべての事業者が一定の効果を認めつつも、その評価には温度差が見られた。

肯定的な意見としては、「対外的な信頼性のアピールになる」「顧客への安心感につながる」「社内への取組周知にも活用できる」といった声があった。特に、既に P マークで事業者名公表の効果を実感している事業者からは、同様の効果が期待できるとの回答があった。

一方、慎重・条件付きの意見としては、「公表だけでは大きなメリットを感じない」「海外との取引を本格的に行う場合にはインセンティブになる」「海外の人が実際に参照できるサイトでなければ意味がない」といった指摘もあった。現時点で CBPR について取引先から問われることがないため、公表の実質的な効果を実感しにくいという声も複数あった。

＜各社の主な意見＞

【インセンティブになる】

- 社名の公表はインセンティブになる。自社ホームページ上で GCBPR の特集ページを作成してアピールしており、公表は有効なので継続をお願いしたい。
- 社名の公表に加え、個別記事として取り上げてもらえると良い。社内外（個人のお客様情報を扱う業種は特に）へのアピールになるためインセンティブにつながる。

【インセンティブにならない】

- インセンティブになるかは判断が難しい。海外の人たちが「この事業者は GDPR にきちんと対応できるのか」を確認できるサイトになっていればよい。所管官庁のサイトのトップページから海外の人たちも手軽にアクセス可能な環境であることが重要。
- 社名の公表のみでは、大きなメリットが感じられない。

② 認証事業者、所管官庁、審査機関等との間で CBPR を通じた越境データの適正な取扱いに関するエコシステム（ネットワーク）の形成

【概観】

エコシステム（ネットワーク）の形成は、9 社すべてから肯定的な評価を得た。①の事業者名公表と比較して、より具体的なメリットを感じるという意見が多かった。

期待される効果として、「情報収集・情報共有の場として活用できる」「海外法制度の変更等の最新情報を得られる」「新規ビジネスや取引先開拓のきっかけになり得る」「所管官庁や他の認証事業者との関係構築ができる」といった点が挙げられた。

特に、海外法制度の追跡が困難であるという課題を抱える事業者からは、法改正情報等を共有してもらえる場があれば非常に有益との声があった。また、認証取得を検討する段階においても、ネットワークを通じて先行事業者の知見を得られることへの期待が示された。

＜各社の主な意見＞

【インセンティブになる： 期待される効果】

- 所管官庁とセミナー等でお会いする機会があり、コミュニケーションの場があるのは望ましい。データに関して重要性を認識している事業者とのエコシステムという観点でも望ましく、新しい取引に発展する可能性もある。
- 横のつながりがきっかけでニュービジネスもあり得る。官公庁との取引もあるため、認証を取得することで委託先として安心していただき、イベントや事業受注につながる可能性が広がる。
- 是非ともお願いしたい内容である。審査機関からの案内、イベントやミーティング開催の報告、参加者レポート等の情報を、ウェブ開催を含めて提供いただきたい。どのような人的ネットワーク活動が行われているかを報告会等で示していただければ、盛り上がりを感じ取ることができる。
- 事例やケーススタディを学ばせていただく必要があり、類似事例があれば、通すべきところと守るべき内容を確認できるのでありがたい。

Q9. 同業他社や取引先事業者（海外事業者含む）で、Global CBPR/APEC CBPR 認証を取得している事業者はありますか？

【概観】

同業他社や取引先事業者における認証取得状況の認知は極めて低い水準にあることが明らかになった。

回答は大きく 3 つのカテゴリに分類できた。

第一に、「全く知らない・把握していない」という事業者が最も多かった。

第二に、「調べたが自社との関連性が見出せない」という事業者があった。

第三に、「認証事業者を認識しているが直接取引はない」という事業者が一部見られた。

また、取引先の選定基準や委託先評価の項目に CBPR 取得の有無が含まれていないという回答が複数あり、現時点では市場において認証取得が取引要件として機能していない実態が浮き彫りになった。

＜各社の主な意見＞

【全く知らない・把握していない】

- 自分たちの地域の個人情報は守るとしても、海外に対してはどのような対応をしているのか疑問があり、提携先の海外の大学が認証を取得しているか気になる。
- 取引先に認証企業はいると思うが、きちんと調べたことがない。また、取引先が認証を取得しているかどうかは、委託先の選定基準にも具体的には含まれていない。
- 同業他社での取得の有無は聞いたことがないので分からない。同業の大手企業等は取得しているのだろうか。

【調べたが自社との関連性が見出せない】

- 簡単には調べたが、まだピンとこない。自社と直接関係があるという感じではない。取得している事業者は大企業すぎて、自社はそのレベルではないため参考にならない。

【認証事業者を認識しているが直接取引はない】

- 日本の認証事業者の名前はよく耳にする。直接的な取引はないが、つながりがあるという認識は持てる事業者である。

【その他】

- 提供された動画を視聴したところ、海外事業者が取得しているという紹介があり、その中には取引先も含まれていた。

Q10. Global CBPR 認証は、事業者にとって有効（必要）だと思いますか？

【概観】

今回のヒアリング対象 9 社すべてから回答を得ることができた。GCBPR の有効性・必要性に対する評価は、事業者の業態や海外との関わりの度合いによって大きく異なった。

回答は大きく 3 つのカテゴリに分類できた。

第一に、「有効である」と積極的に評価する事業者。これらは海外との取引が多い、又は認証を既に取得している事業者であった。

第二に、「条件付きで有効」と評価する事業者。海外取引がある事業者や特定の業種には有効だが、自社には直接的な必要性を感じていないというスタンスであった。

第三に、「自社には必要ない」と回答した事業者。海外との直接的なやり取りが限定的であることや、実際は認証を持っていても、サービス選定時にアンケート調査が実施されているから、という理由が挙がった。

また、公共団体向け事業を行う事業者からは、「公共団体は情報管理を特に厳しく問われることが多く、認証があれば対外的な説明材料になる」との意見があり、業種・顧客特性によっては認証の有効性が高まることが示唆された。

＜各社の主な意見＞

【有効である】

- GCBPR は対象エリアが拡大されており、多くの事業者・多くの対象地域との円滑なデータ流通を行えるという観点で有効だと考えている。一部の契約のスキップや確認作業のスキップができるため、効率化につながる。
- 認証されていることで、国内だけでなくグローバルにおいても法的リスクの軽減につながる。信頼性の向上により競合他社との差別化にもつながり有効である。
- 取引先が、個人情報の取扱いに一定水準の管理体制を備えていることの証明になる点で、有効だと考える。P マークは国内に限定されるが、海外を含めた評価が可能な認証であれば、取引先選定が容易になり、その点で有効性がある。

【条件付きで有効】

- ビジネス上においては必要な場合があると思う。特に欧州圏とのやり取りをするような事業者は、少なくとも認証を取っておいた方がいいと思う。
- 海外との取引を通じ、個人情報を取り扱う機会が多い会社にとっては有効だと思う。メーカー等、様々な商品を取り扱っているところは持っていた方がいいのではないか。
- 組織規模とのバランスが課題である。企業規模により有効性が異なる可能性がある。

【自社には必要ない】

- それほど必要ないと考えている。理由は、海外移転が非常に限定的であるため。海外に子会社があるわけでもなく、あまり影響がないと考えている。
- 他社からの監査では、認証の取得は関係なくアンケート調査が行われるため。

Q11. GDPR 等の規則や法（例：十分性認定/BCR/SCC）等と比較した場合、Global CBPR 認証/APEC CBPR 認証のメリット及びデメリットは何ですか？

【概観】

今回のヒアリング対象 9 社すべてから回答を得たが、法律と認証制度の比較に関し、明確に回答できた事業者は限定的であった。多くの事業者が「詳しく検討していない」「比較したことがない」「よく分からない」と回答しており、GDPR や各種越境移転ツールの理解が十分でない実態が明らかになった。

法と第三者認証を比較した場合、メリットとしては「第三者の審査に基づく認証により信頼性を客観的に証明できる」「法令遵守の状況を可視化できる」「海外事業者への説明の容易さ」等が挙げられた。一方、「費用対効果」「運用にかかる労力」「取得に向けた支援が他の認証制度ほど整っていない」等が、認証の取得が進まない課題として指摘された。

＜各社の主な意見＞

【GCBPR のメリット】

- 最大のメリットは、第三者認証を得て、安全性や信頼を受ける事業者ということを客観化して示せる点である。
- 取引相手が一定水準を備えていることのアピールになり、取引先選定が容易になる。日本の制度に精通していない海外事業者に対しても、共通ルールの基準を満たしていることが明確になる点がメリットである。
- 各国の法律は全然分からないし、どうしたらいいか分からないというのが実際の感覚である。グローバルで統一された認証があれば、それを取っているなら安全だろうという判断がしやすくなるので、統一認証があるのは嬉しい。

【GCBPR のデメリット】

- デメリットとしては費用対効果が挙げられる。また、現時点では参加メンバーが限定的であり、利用する機会が限られている点がある。対象となる国や地域、対象事業者が増えていくことを期待している。
- デメリットというよりは、運用がどこまで必要なのか細かくわかっていないため、結構大変そうな印象がある。認証を取るのにすごく労力がかかりそうだ。また、サポートしてくれるコンサルタントも少ないのではないか。中小企業にとっては人的リソースをそこに割けず、人員がなかなか確保できない。

【法と第三者認証の比較】

- 法律は守らなきゃいけないもの。GDPR が 2018 年に導入された時、大騒ぎになったと記憶しており、法令遵守に向けて必死に調べた。ただし、第三者認証の取得の要否は企業により異なり、取得しても継続しなければそれまでのものである。
- 法律は間違いなく守らなければならないので、多少のコストをかけてでもやっていくという力学が働きやすい。一方、認証制度はなかなかそこまでいかないケースも出てくる。「なぜ必要なのか」という点が社内で説明しにくい面がある。

【理解不足を示す意見】

- 正直な話、分からない。いろんな種類があることを最近知った。比較したこともない。
- 中身が正しく認識できていないため、はっきりとした回答は困難である。GDPR でさえも、どの範囲に及ぶのかが不明確な状況にある。

Q12. CBPR 以外の認証を取得していますか？

① 認証制度名

【概観】

今回のヒアリング対象 9 社すべてが何らかの認証を取得していた。最も多く取得されていたのは P マークであり、9 社中 8 社が取得済みであった。次いで ISMS（情報セキュリティマネジメントシステム）が複数の事業者で取得されており、全社取得又は一部事業部での取得という

パターンが見られた。その他、ISO[9] 9001（品質）、ISO 14001（環境）、PCI DSS（クレジットカード業界のセキュリティ基準）等を保有する事業者もあった。

また、公共系事業を行う事業者では、QMS（品質マネジメントシステム）を保有しているケースも確認された。

＜各社の主な意見＞
- Pマークの付与事業者である。
- ISMS、PCI DSS、Pマークを取得している。
- Pマークは全社で、ISMSは事業部単位で取得している。
- 事業部門ではISMSをすべての部署で取得済みである。
- ISO 9001と14001はグループ認証で取得している。

② 認証取得の理由

【概観】

認証取得の理由は大きく3つのカテゴリに分類できた。

第一に、「取引要件・入札参加資格としての必要性」であり、顧客や取引先から認証取得が求められるケース、官公庁の入札参加資格として必要なケースが多く挙げられた。

第二に、「事業者としての信頼性・管理水準の証明」であり、個人情報や情報セキュリティに関する適切な管理体制を対外的に示すためという理由があった。

第三に、「法制度への対応」であり、個人情報保護法の施行を契機として取得に動いた事業者もあった。

＜各社の主な意見＞

【取引要件・入札参加資格】
- 顧客から個人情報の取扱いを含む業務を受託しているため、P マークの付与事業者であることが取引の条件になっている。
- 公共系の仕事が多いということが理由である。入札の条件に入っていることもある。
- 入札案件で翻訳事業として応募する際に、ISO27001 が条件になっていることが非常に多い。大型案件になるほど求められるということで取得を決意した。

【事業者としての信頼性・管理水準の証明】
- 当時の代表がISO 9001、14001とPマークの三つを同時に取得する方針を決定したが、それらは事業者として一定の管理水準にあることを示すことが目的だった。
- 事業等で個人情報の取扱いが多いため、基本的に必要と考えて取得した。

[9] 国際標準化機構（International Organization for Standard：ISO）（以降、「ISO」という。）

③　認証制度の効果

【概観】

認証制度の効果として最も多く挙げられたのは「取引・入札における優位性」であった。特に官公庁案件や大手企業との取引において、認証を取得していることが参加資格や評価基準となっているケースが多い。次いで「社内のガバナンス強化・従業員意識の向上」が挙げられ、認証取得・維持のプロセスを通じて組織的な管理体制が整備されるという効果が認識されていた。一方で、「認証取得が当たり前になり差別化効果が薄れている」「取引先からの調査対応の負担が増えている」という課題も指摘された。

＜各社の主な意見＞

【効果がある】

- 官公庁案件が多いため、入札参加資格として P マーク、ISO、ISMS 等の保有を求められることがあり、入札参加資格を得る効果は大きい。
- P マークがあることでガバナンスが効き、社員・従業員の異なる認識の統一が図れた。
- 顧客によっては、当社での取扱い方法や体制、規程の整備状況、事故時の罰則等を確認するため監査が入る。P マークを運用していてこうした点がカバーされており、効果的である。

【効果が感じられない】

- 最近はほとんどの取引先同士がお互い P マークを持っているので、あまり効果を感じない。
- 認証制度の取得に関係なく取引先からの情報セキュリティ調査票のやり取りが煩雑になっている。認証を取得していても調査は来るので、認証があるから大丈夫ということにはなっていない。
- 20 名程度の小規模企業でも取得している一方で、大手企業でも取得に至っていない例が多く見られる。社会的な認知度が低い点が課題である。

④　申請手続き・認証取得後の運用等で改善してほしいこと

【概観】

改善要望は、大きく 4 つのカテゴリに分類できた。

第一に、「申請のデジタル化」が挙げられ、紙ベースの申請からオンライン化への要望があった。

第二は、「法改正情報の事前周知」で、審査期間中の法律変更について事前にアナウンスがあると助かるという声があった。

第三は、「更新負担の軽減」で、前年度からの差分を見る仕組みや、継続年数に応じた工数削減への期待があった。

第四は、「制度の社会的認知度向上」で、認証制度への社会的なバックアップが必要という指摘があった。

一方、「特に改善要望はない」「よくできている制度」という評価もあった。

＜各社の主な改善要望＞

【申請のデジタル化】

- 申請手続きは紙ではなくデータで申請できるようにしてほしい。社内は全部データで管理しているが、申請のためだけに出力してファイリングしなければならない。デジタル化を希望する。

【法改正情報の事前周知】

- 審査から次の審査までの 2 年間に変わった法律について、「ここが変わっているので注意してください」と事前にアナウンスがあるとありがたい。

【更新負担の軽減】

- 更新の工数がどんどん減っていくのが望ましい。前年度からの差分をしっかり見ていただけるような制度設計や運用があるとよい。
- 認証制度の審査は審査員のバラツキが大きい気がする。前回の審査の内容が引き継がれていない印象がある。「前回の改善の機会についてどうしましたか」というフィードバックがあり、継続して一緒に作り上げていく仕組みがほしい。

【制度の社会的認知度向上】

- Pマーク取得事業者数がもっと伸びてしかるべき。社会的なバックアップが必要だと感じている。CBPR 認証についても同様に、制度の効果は相乗的なバックアップ体制があってこそではないか。
- この認証があることのメリットが、より社会で認められるような仕組みができたらいい。

⑤ 今後の認証取得予定

【概観】

今後の認証取得予定は、「現状で充足している」「特に予定はない」という回答が多数を占めた。ただし、ISMS の取得・拡大を検討している事業者が複数見られた。その背景には、取引先からの要求で ISMS 保有を問われる機会が増えていること、入札参加資格として ISMS が求められるケースがあること等があった。一方で、取得に向けた人的リソースの確保が課題となっており、必要性は認識しつつも実行に移せていないという実態も明らかになった。また、「顧客から求められれば検討する」という外的要因に依存する姿勢も見られた。

＜各社の主な意見＞

【認証取得予定（検討含む）】

- ISMS の全社取得をいつ取るか検討中である。取引先のヒアリングが厳しくなってきており、必要になってくるのではないかという危惧がある。
- ISMS は時々検討に上がる。サービスを始めるにあたって入札条件に ISMS 保有が指定されれば、真剣に検討しなければならない。

- 認証の効果は主にPR効果であり、入札加点の対象となるといった（個人情報やセキュリティとは関係のないプラチナくるみん認定の取得も検討中）実質的なメリットが重要である。

【認証取得の予定なし】

- 今のところ予定はない。ただし、顧客から求められれば取引のために検討しなければならない。
- 現時点で、P マークや ISMS の更新をやめるとか新たな認証を取得するという情報は持っていない。必要性がある制度があれば取得に動くと思う。

Q13. CBPR 認証や他の認証制度も含め、第三者認証制度の効果として最も期待することは何ですか？

【概観】

今回のヒアリング対象 9 社すべてから回答を得ることができた。第三者認証制度に期待する効果は大きく 4 つのカテゴリに分類できた。

第一に、最も多く挙げられたのは「対外的な信頼性の証明・安心感の提供」である。取引先や顧客に対して、自社が適切な管理体制を備えていることを客観的に示すことができるという点への期待が高かった。

第二に、「取引・契約の円滑化」が挙げられた。認証を取得していることで、取引先からの調査対応や確認作業が軽減され、ビジネスがスムーズに進むことへの期待があった。

第三に、「社内ガバナンスの維持・強化」が挙げられた。定期的な審査により運用の形骸化を防ぎ、継続的な改善につながるという効果への期待があった。

第四に、「制度的な優遇措置」への期待があった。漏洩報告の軽減や国の調達におけるベネフィット等、認証取得による具体的なインセンティブを求める声があった。

＜各社の主な意見＞

【対外的な信頼性の証明・安心感の提供】

- 取引先や顧客に対する安心感が最も重要である。
- 継続して契約してもらえることや、顧客からの信頼性が重要である。P マークは一般的に信頼度が高いと考えている。
- 第三者認証は、当社が正しい取扱いをしていることの証になるので、正しく存在感のある保証になってほしい。

【取引・契約の円滑化】

- できれば、委託先調査や取引先調査において、認証制度を取得しているから安心してくださいで終わってほしい。（現状は認証があっても取引先からの調査がある）
- 外注先に対してアンケート調査等の実施を依頼する際、P マークを示せば「適切に管理している」という理解が得られる。保有していなければ具体的な管理体制や規則を逐一確認する必要があり、管理コストが増加するため、その点での有効性は大きい。

- 取引先から「この会社はしっかりしている、情報の管理に問題ない」と認識してもらえること。それで仕事が増えるということを事業的には求めている。信頼性のアピールのためである。

【社内ガバナンスの維持・強化】

- 定期的に審査が入ることで、運用が形骸化しないという効果がある。改めてきちんとできているかのチェックもできる。社内の安全性の担保という点で期待している。
- 社内の意識向上である。見られている、検査されるからちゃんとしておこうというところがあり、継続して体制を整えておかないといけないという意識につながっている。

【制度的な優遇措置】

- 信頼性の観点に加えて、第三者認証を得ているからこその漏洩報告の軽減化や減免措置、国の調達に関してのベネフィット等、そういったものがあるとよいと考えている。

Q14. 日本では導入されていない GCBPR のグループ認証についてお尋ねします。

① 日本子会社:国内に子会社がある場合、子会社もまとめて認証される運用は、CBPR 認証を取得する動機に繋がりますか？

【概観】

国内子会社を対象としたグループ認証は、9 社中 6 社が「動機につながる」「あった方がよい」と肯定的な評価をした。その主な理由として、「個社別での認証取得・維持の負担軽減」「グループガバナンスの効率化」「取得のハードルの低下」等が挙げられた。特に、既に ISO 等でグループ認証を経験している事業者からは、同様の効果が期待できるとの声があった。

一方、1 社からは「親会社と子会社で個人情報に対する捉え方が異なることが多いため、グループで統一すると実態が伴わない」との慎重な意見があり、個社単位での認証の方が実質的な信頼獲得につながるとの指摘があった。また、子会社が P マーク等（他の認証を含む）を取得していない場合、グループ内のやり取りでも「他人行儀」に扱う必要があり、手間が生じているという実態も示された。グループ認証があれば、こうしたグループ内での情報共有の負担軽減にもつながるとの期待が示された。

＜各社の主な意見＞

【認証取得の動機になる】

- P マークで子会社があった時代、個社別でやっていると負担感が非常に強かった。ほぼ同一パッケージでやっていたが、手間暇が二重にかかっていた。グループ認証があると非常に良い。
- 子会社の中には調査業務を行う事業者があり、グループ単位での認証取得ができれば、グループ全体の事務負担が軽減される。品質・環境関連の認証ではグループ事業者をまとめて申請しているので、同様の効果が期待できる。

【認証取得の動機にならない】

- 個人的には反対である。親会社と子会社で個人情報に対する捉え方の度合いが大きく異なることが多い。グループで統一されると認証制度の広がりにはなるが、実態は伴わない。個社単位での信頼獲得の方がより実質的である。

② 海外子会社:海外に子会社がある場合、子会社もまとめて認証される運用は、CBPR 認証を取得する動機になりますか？

【概観】

海外子会社を対象としたグループ認証も、概ね肯定的な評価が得られた。特に、海外子会社を持つ事業者からは「グローバルな越境移転を扱う認証として、海外子会社も含めた認証の方が本来の趣旨に合っている」との意見があった。

ただし、「海外子会社の場合は管理体制の実現可能性に疑問がある」「距離的に管理が難しい」といった実務上の懸念も示された。国内子会社と比較して、ポリシーの徹底や管理体制の維持に課題があるとの認識が複数の事業者から示された。

＜各社の主な意見＞

【認証取得の動機になる】

- 国内外の子会社間で差はない認識である。この制度がスタートした際は、メリット・デメリットを検討して利用できるものであれば取得する。選択肢があるのはメリットである。
- 海外のグループ会社の方が本来はこの認証が必要だと思うので、グループ全体でできた方が対応しやすい。

【認証取得の動機にならない】

- 国内子会社の場合は近距離での管理が容易だが、海外子会社の場合は管理体制の実現可能性に疑問がある。

③　子会社の有無を問わず、グループ認証はあった方が良いと思いますか？

【概観】

グループ認証制度の必要性は、9 社中 6 社が「あった方がよい」と回答した。その理由として、「コスト・労力の効率化」「取得ハードルの低下」「選択肢の拡大」等が挙げられた。特に、グループで取り組むことで馬力が出る、協力し合って取得しやすくなるという意見があった。

一方、「グループ認証と個社認証の選択ができる柔軟性」を求める声も複数あった。グループ内でも文化や事業内容が異なる場合があるため、一律にグループ認証を強制するのではなく、事業者の実情に応じて選択できる仕組みが望ましいとの指摘があった。

また、グループ認証の運用上の課題として、「本体のルールをそのまま子会社に適用すると条件が合わない場合がある」「部分的なカスタマイズができると良い」「事業所単位ではなく子会社単位で審査してほしい」といった具体的な要望も示された。

＜各社の主な意見＞

【あった方が良い】

- 一社だけではなくグループで取る方がコストや労力の面でも協力し合って取りやすくなる。取得のハードルが下がるのかもしれない。
- 社内リソースの効率化という面で使いやすいところを使えばいい。個社単位での取得という選択もできる。会社ごとに選択があった方がいい。
- ISO をグループ認証で取得しているので、もし親会社がグループで取ろうという話になったらやりやすい。
- グループ内で選択の自由があり、文化が似ているところはグループ認証、そうでないところは個社単位とする柔軟性があれば、グループ全体の事務負担も軽減され、よりパフォーマンスをコントロールできるのではないか。
- 関連会社との間で、現在のポリシーの共通化等も進めており、グループガバナンスが効くように、この制度を利用する選択肢があるのはメリットになる。

【反対／どちらとも言えない】

- グループ内でも個人情報に対する考え方が異なる場合があり、教育が行き届かない場合、形骸化する恐れがある。
- 本体のルールをそのまま子会社に導入すると条件が合わないこともあるので、部分的にカスタマイズできるとやりやすい。
- 親会社の意向によるため、子会社の立場での判断が難しいが、グループ内の人的コスト等の節約にもなるため、今後検討の機会があるかもしれない。

Q15. 日本では導入されていない GCBPR の PRP 認証についてお尋ねします。

① PRP 認証が開始された場合に CBPR 認証を取得する動機になりますか？

【概観】

事業者の立場（コントローラーかプロセッサーか）によって、PRP 認証（データ処理事業者向け認証）が取得動機になるかどうか、評価が大きく分かれた。

コントローラー（データ管理者）の立場にある事業者からは、「自社の取得動機にはならないが、委託先が PRP 認証を取得していれば選定の材料になる」という意見が示された。一方、プロセッサー（データ処理者）の立場にある事業者からは、「顧客から求められれば検討するが、現時点では積極的な動機にはならない」という慎重な姿勢が見られた。

＜各社の主な意見＞

【認証取得の動機になる】

- 取得企業にとって、動機になり得る。
- 事業分野がクラウドのため、取得しなければならない事業者に該当するのではないかと思う。

【認証取得の動機にならない】

- コントローラーの立場であるため、自社の取得動機にはならないが、クライアントがこうした認証を取得することは望ましい。
- プロセッサーの立場であるが、クライアントから要請がない限り取得の予定はない。
- プロセッサーの立場である事、取得したくてもできない可能性があるため。

② プロセッサーであるか否かを問わず、PRP 認証はあった方が良いと思われますか？

【概観】

PRP 認証制度の必要性は、「あった方がよい」とする意見が多数を占めたが、その評価には条件や留保が付くケースが多かった。

肯定的な意見としては、「委託先・取引先の管理において区別しやすくなる」「プロセッサーが法を遵守していることの証明になる」「選択肢が増えることは良い」といった点が挙げられた。

一方、懸念点として、「コントローラーとプロセッサーの両方の性質を持つ場合、複数の認証が必要になる」「棲み分けがわかりにくい」「認知度が低ければ効果が不明」といった指摘があった。また、「1 つの認証で両方の観点をカバーできる方が良い」という意見もあった。

＜各社の主な意見＞

【あった方が良い】

- 委託先や取引先の管理という観点では、そういう認証を取得していることで非常に区別しやすくなり、分かりやすいと思う。
- 委託先がグローバル PRP を取っているというのは選定の材料になるので、制度がある方が望ましい。
- 自社がプロセッサーの立場で法を遵守していることが証明されるのであれば価値はある。ただし、認知度が低ければ持っていても効果が分からないので、コストや労力を考えた上で必要かどうか検討する。

【どちらとも言えない】

- 専業でデータ処理を行う事業者であれば管理しやすいと考えられるが、自社の場合はコントローラーとプロセッサー両方の性質があるため、複数の認証対応が必要になり、実質的な効果は限定的である。
- あえて分けると監査の仕方が変わるのかなと思うが、自社は委託も再委託もするので、両方の観点で 1 つの認証で取れてもいいかなとは思う。
- 実際に分からないというのが正直な話である。グローバル PRP を取るべきなのか、P マーク等で済むのかという線引きが難しい。自社サーバーがあれば自分たちがグローバル PRP を取らなければいけないのか、クラウドサービスを使えばその事業者側の認証で済むのか等、棲み分けが想像できない。

Q16. Global CBPR 認証の日本での拡大についてお尋ねします。

① 認知度を高めるために、どのような方法が効果的だと思いますか？

【概観】

認知度向上のための効果的な方法は、9 社すべてから具体的な提案を得ることができた。回答は大きく 6 つのカテゴリに分類できた。

第一に、「具体的なメリット・費用対効果の明示」が最も多く挙げられた。認証取得によって何が得られるのかを明確に示すことが、認知から検討への移行を促す鍵になるとの認識が共有されていた。

第二は、「認証事業者の事例紹介」で、同業種・同規模の事業者の成功事例、中小企業でも取得可能であることの周知が効果的との意見があった。

第三は、「大企業からの波及効果の活用」で、大企業が率先して取得し、取引先にも求めていくことで一気に広がるとの指摘があった。

第四は、「クラウドサービス利用と越境移転の関係の啓発」で、国内のみで事業を行っていると思っている事業者も、実はクラウドサービス利用により越境移転が発生していることへの認識を高める必要があるとの指摘があった。

第五は、「セミナー・情報発信の充実」で、啓発セミナーや意見交換の場の提供、P マーク付与事業者への追加認証としての位置づけの明確化等の提案がなされた。

第六は、「SaaS 提供事業者からの情報発信」であった。認証取得企業がアピールすることで、目につく機会を増やすことが効果的との理由から、SaaS 提供事業者が認証事業者となり、サービス利用者に対し、「GCBPR を取得しています」とアピールすることで、認知が広がるのではないかとの意見があった。

＜各社の主な意見＞

【具体的なメリット・費用対効果の明示】

- メリットを事業者に明確に示すことが重要である。
- 費用対効果がわかれば、導入の検討に踏み切る会社も多いと思う。自社は関係ないと思っているところが多いので、どのくらいの越境移転をする会社だったら取った方がいいのかがわかるとよい。

【認証事業者の事例紹介】

- 身近な会社の成功事例があるとわかりやすい。啓発セミナーや意見交換ができる場があるといい。大企業だけでなく中小企業の前例がわかると効果的である。

【大企業からの波及効果の活用】

- 大企業が取っておくべきだと思う。目につく機会も増えて、皆興味を持つのではないか。大企業が取引先にも求めてくるという流れがあると、一気に広がる。

【クラウドサービス利用と越境移転の関係の啓発】

- 「クラウドサービスを利用している会社も本当は必要ですよ」ということがあるなら、そこがアピールポイントになる。クラウドサービス利用による越境移転の実態を強調すると効果的ではないか。
- クラウド利用の範囲でも個人情報が海外に越境移転しているという認識からスタートすることが重要である。その部分だけを取り上げた動画配信は有効だと思う。

【セミナー・情報発信の充実】

- P マーク付与事業者に対して、追加で取得できますよという形で示すと、既に取得している事業者は取りやすいのではないか。
- 制度そのものが何であるかがわかりやすく説明されることが重要である。十分な理解がなければ検討段階に到達しない。
  セミナーの案内を全て見ているわけではないので、題名に「○○認証が始まりました！」や「○○認証取ってないけど大丈夫？」等のキャッチーなセミナータイトルがあると良い。そうしたタイトルを拾って見に行っているケースが多いため。

【SaaS 提供事業者からの情報発信】

- SaaS を利用している側からすると、ツール選定時にベンダーが「GCBPR を取得しています」とアピールしていただくとチェックポイントになる。取得している事業者にどんどんアピールしてもらって目につくようになると効果的である。

② 拡大フェーズの施策として、審査料が一定期間無料になる等の特典は認証事業者数拡大に有効だと思いますか？

【概観】

審査料無料の特典は、評価が分かれた。9 社中 2 社から「有効である」という回答が得られた。7 社からは「有効ではない」という回答であったが、うち 4 社からは「短期的には良い」「検討のタイミングであれば効果的」等の条件付きで、「有効になり得る」という意見を得た。

なお、「有効ではない」と回答した 7 社全社から、取得した後の「工数・労力・維持管理」に対する懸念が寄せられた。

＜各社の主な意見＞

【有効である】

- とても良いと思う。上層部にアピールするなら、クラウドサービスを使っている事業者向けに、このタイミングでいかがですかという形だと効果的ではないか。
- インセンティブになると思う。認証のセール、「今ならお得」みたいなことをされる印象がないので、非常にインパクトがある。イメージがない分、かなりインパクトが強い。

【一定の条件下で有効である】

- 拡大フェーズでは、一定期間審査料が無料になるのは短期的な観点で、有効かもしれない。
- 一定程度有効だとは思う。ただし、どれほどの人員コストや期間がかかるかを考えると、無料だから良いというわけではない。試験的にやってみるというのはありかもしれない。
- 必要性がある程度迫られた中での無料というのは効果がある。ただし、まずは必要性のところがあって、その中で制度が広まった上で、取ろうとした時にこういう施策があれば効果的である。維持のランニングコストも考える必要がある。

【有効ではない】

- 事業者の規模によると思うが、自社ではあまりインセンティブは働かない。必要があれば多少のコストをかけても取得するというスタイルであり、「無料だから取得してみよう」ということにはならない。ただし、検討しているタイミングで無料であれば、それなら取得しようということになるかもしれない。
- メリットが明確でなければ、無料でも取得には至らない。維持管理と更新にかかるコストと労力、メリットのバランスが取得判断の鍵になる。

③ CBPR 認証のような越境移転ツールが、日本でより多くの事業者が取得したいと思われるようになるためには、何が必要だと思いますか？

【概観】

より多くの事業者が取得を望むようになるために必要なこととして、最も多く挙げられたのは「外的要因の創出」であった。取引先からの要求、入札参加資格への組み込み等、「取得しなければ取引できない」という状況が生まれれば、取得が進むとの見方が多数を占めた。

次いで「費用対効果・メリットの明確化」が挙げられた。担当者が経営層に説明できる具体的なメリットがあれば、取得に向けた動きが生まれるとの指摘があった。

また、「大企業の先行取得と取引先への波及」「無意識の越境移転への啓発」「既存認証との連携・効率化」等も重要な要素として挙げられた。

さらに、既存の認証審査への組み込みという提案もあった。具体的には、P マークの審査において越境移転に関する確認を行うことで、事業者が越境移転の実態を認識せざるを得なくなり、CBPR への関心も高まるのではないかとの意見があった。

＜各社の主な意見＞

【外的要因の創出】

- 外的要因が重要である。政府の受託事業の条件にするというのは強制的すぎるかもしれないが、外的要因があった方が事業者は取らざるを得ないという形に追い込まれる。
- 入札の条件として、クラウドサービスを使っているところは認証を取得した方がいい等の要件があると、やむを得ず取らなくてはいけないという形になる。

【費用対効果・メリットの明確化】

- 費用対効果が明確であれば、担当者も取りたいとなり、経営層に便宜を図っていくという循環になる。
- 費用対効果がわかれば、導入の検討に踏み込みやすい。大手企業だけでなく中小企業も対象であることがわかるとよい。

【大企業の先行取得と取引先への波及】

- 大企業が海外とやり取りしているのにこれを使わない理由を突き詰める必要がある。ほとんどの事業者は大企業と取引しているので、「この認証がないと事業ができません」と言われれば広がる。

【無意識の越境移転への啓発】

- まず越境移転が起きているという認識を正しく持ってもらう必要がある。認証を取得している事業者と、認識がない事業者を比較して、メリット・デメリットをわかりやすく見せる情報発信が必要である。

【依存認証との連携・効率化】

- P マークを持っている事業者なら、ここの部分の審査は外して追加で取れますよという形にすると取りやすいのではないか。審査のタイミングも一緒にやってもらえると、重なる部分も多いと思うので負担が減る。
- P マークで海外移転が取り上げられることが今までに一度もなく、審査でも突っ込まれない。P マークの審査や ISO に取り込んでいくと、やらざるを得ないということになる。SaaS 提供側がもっと認識を持ってもらうことと合わせて、やっていくことでかなり広まるのではないか。

【認証事業者への質問】

上記 Q1.～Q16.以外に、認証取得済みの事業者に対し、追加質問を行っている。その概要は以下のとおりである。

＜追加質問＞

Q1. CBPR 認証取得を検討したきっかけや取得の決め手となった要因は何ですか？

【概観】

取得のきっかけ・決め手として挙げられたのは、海外拠点でユーザー情報や従業員情報を取り扱うことから、顧客の重要な情報を適切に取り扱っていることを第三者認証によって証明することが重要と判断したことが、認証取得決定の主要因であった。

＜主な意見＞

- 海外にも開発拠点があり、情報連携を行っている。従業員データだけでなく、ユーザー情報も海外拠点で取り扱うため、ユーザーの大事な情報を適切に取り扱えるかという観点で、第三者認証を得ることは非常に重要だと考えた。こうした観点が取得を決定した大きな要因であった。

Q2. GCBPR 認証の審査プロセスについてお尋ねします。

① 認証取得や更新の準備（必要書類の作成等）にはどの程度工数がかかりますか？また、審査について特に負担になっていることがあればお教えください。

【概観】

認証取得・更新の準備には一定程度工数がかかることが示された。特に、申請時に提出する根拠資料の更新や前年度の指摘事項への対応で工数を取られているが、初年度が最も重く、ノウハウの蓄積により 2 年目以降は工数が減少していく傾向が示された。

また、提出資料の種類・内容に関し、どこまで準備すれば審査が開始・終了できるのか不明確な部分があり、取得を検討する事業者にとってのハードルになっているのではないかとの指摘があった。

＜主な意見＞

- 毎年度、申請時に根拠資料を複数用意している。再申請や前年度の指摘事項への対応等も含め工数がかかっている。維持するのが大変という印象である。
- 慣れやノウハウの蓄積により、ドキュメント準備の工数は減っていく。初年度が最も重い。これが他事業者の取得が伸び悩んでいる要因の 1 つではないか。
- 審査の開始に必要な資料を正確に把握せずに、準備を進めるのは困難である。経営層に承認をお願いする上でのハードルにもなっている。
- 事業者ごとの業態やサービスによって審査内容が異なるため、どこまでが自社に求められているのかが分かりづらい。
- ある程度の認証審査のゴールを示すこと、ドキュメントのひな型・見本を増やすことがあれば負担軽減につながる。

② 認証審査プロセスについて、改善してほしいことはありますか？
（ISMS との重複について）

【概観】

ISMS を同時に取得している場合の工数削減効果について確認したところ、一部のドキュメントは共通化しているものの、社内の別部門が対応しているため、社内の運用課題も含め大幅な工数削減にはつながらないことが示された。また、情報資産と個人情報の管理を申請時にどのように取り扱うのかを整備することで、認証審査のハードルを下げる可能性についても言及があった。

＜主な意見＞

- GCBPR と ISMS は別部門が対応している。一部のドキュメントは共通化しているが、参照する台帳は同一でも GCBPR 用に加工が必要であり、ISMS を取得していることで工数が大幅に減るわけではない。
- 無関係な情報が入らないよう、全量チェックや一部削除、、複数の台帳を合わせての提出等を行っている。
- 情報管理をしている会社は多いが、個人情報管理まで単独でやっているところは少ない。そこをうまくアプローチできれば、認証審査のハードルの低さにもつながるのではないか。

Q3. Global CBPR 認証取得の効果についてお尋ねします。

① 御社の事業において、Global CBPR 認証を活用するのはどのような場面でしょうか？

【概観】

対外的には、新規取引先とのビジネス開始時に認証書を示すことで信頼性を証明できる点、対内的には認証取得に向けた準備を通じて社員の意識向上や組織体制の整備につながった点が、認証取得の効果として挙げられた。

＜主な意見＞

- 新規取引先とビジネスを開始する際に、情報管理体制の確認において認証書を提示することで、最初の安心感を得るという観点で活用できている。
- 社内においては、認証取得に向けた準備を通じて、社員の意識が変わり、組織体制も変わった。内部・外部の両面で GCBPR が有効に活用できている。

② Global CBPR 認証を取得したことにより、ビジネス面で恩恵を受けたという事例はありますか？

【概観】

ビジネス面での恩恵として、セミナーの登壇や APEC イベントへの招待等対外発信の機会が得られている点が挙げられた。また、取引先選定において GCBPR 取得の有無をチェック項目としており、認証事業者との取引は実際に発生している。信用度の証明としての効果は高く、取引先評価において追加確認事項を減らせる等、手続きがスムーズになる効果は感じている。

一方、認証制度は継続しない可能性もあるため、事業者間契約の簡素化は、認証取得のみにより解決が図られるわけではないと、認証制度の持つリスクの観点から意見があった。

＜主な意見＞

- セミナーでの登壇機会や APEC の大型イベントへの招待等、対外発信の機会として活用している。
- 取引先選定において、相手方が GCBPR を取得しているか、GDPR に準拠した体制をとっているか等をチェック項目として設けており、認証事業者との取引は実際に発生している。
- 事業者間契約が簡素化というところまでは、なかなかつながりづらいのが実態である。認証は更新制※のため、契約時点で取得していても後に更新されない可能性があり、認証だけをもって契約簡素化はリスクがある。

※1年毎に再申請を行う仕組みである。

③ Global CBPR 認証事業者として、どのような業種・事業者に CBPR 認証を取得してほしいと考えていますか？

【概観】

特に、アメリカで多く取得されているクラウドサービス分野で、日本の同業者が取得すれば、自社が利用するサービスの円滑化につながるとの期待が示された。

＜主な意見＞

- アメリカでは CBPR 認証事業者が多いので、クラウドサービス事業者の日本版のような類似事業者があれば、取得を第一に考えてほしい。自社が利用するサービスでの円滑化につながる。
- 日本全体でこの制度を利用していくことで、確認事項のスキップや効率化、データ流通の活性化につながるという観点で望ましい。

Q4. Global CBPR の普及が進まない理由について、お考えがあれば教えてください。

【概観】

普及が進まない理由として「目に見えるメリットの不足」が挙げられた。

具体的な普及促進策として、漏洩等報告の免除、国の入札条件への組み込み等、目に見えるメリットの創出が提案された。

＜主な意見＞

【具体的なメリットの創出】

- 普及促進策として、漏洩等報告の免除、国の入札条件として ISO や P マークと並んで GCBPR の取得を明記する等、目に見えるメリット・費用対効果が示せると取得が進むのではないか。
- 越境移転にあたって外国法制度の調査コストがかかっている。所管官庁による外国法制度調査の対象国拡大や更新頻度の向上があれば、事業者側の負担軽減につながる。メリットが示せることに加えて、こうした事業者負担を減らす取組も普及促進に有効ではないか。

(7) ヒアリング調査結果のまとめ

本調査の結果、GCBPR の認知度は総じて低い水準にとどまっていることが明らかになったが、認証に至らない要因で最も多く挙げられたのは、「自社業務における必要性を感じていない」という点で、海外との直接的な個人情報のやり取りが限定的であるという認識に基づいた理由であった。次いで「認知度・理解度の不足」であり、制度の存在自体を知らないか、知っていても詳細を理解していないため検討段階に至っていないケースが多かった。

事業者の認証取得に対するインセンティブについては、現在日本で導入されていないグループ認証は、ほぼ全ての事業者から条件付きも含め「あった方が良い」と回答があり、複数の認証制度を運用する上で、企業の運用・維持コスト等の削減につながるという理由であった。また、日本で導入されていないグローバル PRP 等も、条件付きで一定程度効果があるという意見はあったが、コントローラーの立場にある企業は委託先に対して認証取得を希望し、プロセッサーの立場にある企業は、必要性が感じられないという意見も複数挙げられ、全体の意見は二分された。

なお、取得の検討における決定要素としては、「外的要因・ビジネス上の必要性」が最も多く挙げられたことから、現在日本で取得企業数が多い P マークや ISMS 等の取得動機と同様に、外的要因（新規取引時の選定要件や行政受託事業の入札参加資格）が求められている実態が明らかになった。

一方 GCBPR を取得している 1 社からは、対外的な信頼性の証明から新規取引がスムーズになった点、社内における従業員意識の向上や組織体制の整備につながった点が認証取得のメリットとして挙げられた他、現状の課題を踏まえ、申請時の負担を軽減するために、他の認証取得における優遇措置の設定等の意見があった。

2.3. GCBPR の強み・利点の詳細分析等

(1) 調査目的

プライバシー情報マネジメントシステム（Privacy Information Management System：PIMS[10]（以下、「PIMS」という。）について GCBPR のプログラム要件との比較分析を実施し、R6 調査の結果とも合わせ、他の制度に対するより詳細な GCBPR の強みや利点を整理することを目的とする。

(2) 調査対象

PIMS が適切に導入、実施されていることを示す ISMS-PIMS、R6 マッピング調査[11]の結果を分析対象として、PIMS と GCBPR のプログラム要件との比較分析を行った。

なお、R6 調査では、GCBPR の取得を検討する事業者は、既に個人情報や情報セキュリティに関する第三者認証を取得している可能性が高いという仮説の元、日本における代表的な認証制度の内、特に取得数の多い P マークと ISMS について、CBPR のプログラム要件とのマッピング調査が実施された。ISMS-PIMS は R6 調査においても、日本における代表的な認証制度として整理されたが、P マークや ISMS に比べ、認証事業者数が限定的であったこと、ISMS-PIMS は ISMS の認証事業者が拡張版として選択できる認証制度であったこと等から、日本の事業者が多く取得している認証制度という選択要件に該当しなかったためマッピング調査の対象とはされなかった。

---

[10] （3） ISMS-PIMS 認証、PIMS 認証の概要参照。2025.10 より ISMS-PIMS が PIMS として独立した規格となったため、2.3 の調査対象は、マッピング分析は PIMS との比較を行い、認証事業者数等、実績を示す数値等は ISMS-PIMS として表記している。

[11] R6 調査報告書 第 2 章 CBPR の普及等に向けた活動 2.1.2 マッピング調査（16 頁～48 頁）を指す。

本調査では、情報セキュリティに主眼を置いた ISMS の拡張版としての規格から、プライバシー対策のための要求事項を主軸としつつ、情報セキュリティとプライバシー対策の要件を併せ持つ PIMS として独立したことが GCBPR に及ぼす影響を調査するため、ISMS-PIMS と PIMS を対象とする。

(3) ISMS-PIMS、PIMS の概要

① ISMS-PIMS

近年、GDPR（EU 一般データ保護規則）をはじめとして、世界各国でプライバシー保護に関する法規制が強化されていることを受け、組織はこれらの法令に対応するため、個人情報の取扱いに関する包括的な管理体制の構築が求められている。

ISO/IEC 27701 に基づく PIMS は、PII（Personally Identifiable Information：個人識別可能情報）の収集・利用・保管・加工等の処理に関するリスクを管理し、プライバシー保護を実施するための国際規格で、2019 年に発行された ISO/IEC 27701:2019[12]は、情報セキュリティマネジメントシステム（Information Security Management System：ISMS）の認証基準である ISO/IEC 27001 を拡張して、プライバシー対策のための要求事項を追加した規格である（それゆえ、ISO/IEC 27701:2019 の適合性評価制度は、「ISMS-PIMS」と呼ばれる）。

ISMS-PIMS を取得しようとする場合、ISMS を先に取得していることが前提となる。日本国内では、2021 年から ISMS-PIMS の審査が開始され[13]、約 4 年（2025 年 11 月 14 日時点）で、68 組織が認証を取得しており、アメリカ、中国、インドをはじめとする各国でも認証が取得されている。

② PIMS

2025 年 10 月に、ISO/IEC27701 が改訂され、ISO/IEC27701:2025 が発行された。 改訂された規格は、ISO 事務局におけるマネジメントシステム規格[14]に関する方針により、ISMS の認証基準である ISO/IEC 27001 の拡張ではなく、ISO/IEC 27001 から独立したマネジメントシステム規格となった。

これにより、ISO/IEC 27701:2025 の内容は、他のマネジメントシステムと整合した形とするため、ISO/IEC 27701:2019 から大幅に変更されたものの、プライバシー情報保護のための

---

[12] ISO/IEC 27701: 2019 Security Techniques － Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management － Requirements and guidelines（なお、この国際規格をもとに、技術的内容及び構成を変更することなく策定された日本工業規格「JIS Q 27701:2024 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 JIS Q 27001 及び JIS Q 27002 の拡張―要求事項及び指針」も発行されている。）

[13] BSI Web サイト「ISO/IEC 27701:2019、国内第一号として ISMS-AC（一般社団法人情報マネジメントシステム認定センター）から認定取得」ページ https://www.bsigroup.com/ja-JP/insights-and- media/media-centre/press-releases/2021/january/ISMS-AC/

[14] ISO には、組織の運営や管理の仕組みを整えるための ISO9001 や 14001、27001 等の「マネジメントシステム規格」、ISO26262 や 13485 等の「製品・技術仕様に関する規格」の他、認証を受けるのではなく、ISO26000 のような「自己宣言型（自己適合宣言）」の規格等がある。

要求事項に大きな変更はないとされている[15]。認証の移行期間は、規格発行月の月末（2025年 10 月 31 日）を起点として 3 年間（2028 年 10 月 31 日まで）となっており、本調査時点（2025 年 11 月時点）は、認証の移行期間中にあたる。

図表 6 ISMS-PIMS、PIMS の概要

項目	説明
略称	• ISMS-PIMS（ISO/IEC27701：2019） • PIMS（ISO/IEC27701：2025）
審査対象	• PII（Personally Identifiable Information：個人識別可能情報）の収集・利用・保管・加工等の処理に関するリスクを管理し、プライバシー保護を実施するための枠組み。 • 個人を特定できる情報であるPIIを取り扱うPII管理者（私的な目的でデータを使う個人を除く、PII を処理するための目的及び手段を決定するプライバシー利害関係者）とPII処理者（PII管理者に代わり、かつ、その指示に従ってPII を処理するプライバシー利害関係者）を対象としている。 • ※ISMS-PIMS、PIMS 共通
準拠法令・規格等	• ISMS-PIMS：ISO/IEC 27701:2019「Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines」 • PIMS：ISO/IEC 27701:2025「Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance」
認証機関/審査機関	• 日本における認定機関：一般社団法人情報マネジメントシステム認定センター（ISMS-AC） • 日本における認証機関：7 審査機関 （いずれも、2025 年 11 月 14 日時点）[16] ※ISMS-PIMS から PIMS への移行 認定機関は、ISO/IEC27701:2025 を用いる認証機関に対する認定審査を 2026 年 7 月 30 日までに開始し、認証機関は、認定の移行日に基づいて、ISO/IEC27701:2025 での審査を開始し、2028 年 10 月 31 日までにすべての非認証組織に対して ISO/IEC27701:2025 を使用することとされている。
申請/認証単位	組織、部門単位・サービス単位[17] ※ISMS-PIMS、PIMS 共通

[15] 一般社団法人情報マネジメントシステム認定センター（ISMS-AC）Web サイト「PIMS 適合性評価制度」ページ https://isms.jp/pims.html

[16] 一般社団法人情報マネジメントシステム認定センター（ISMS-AC）Web サイト「ISMS-PIMS 認証機関一覧」ページ https://isms.jp/lst/isr/index-isms-pims.html

[17] 規格の中で明文化されていないが、ISO マネジメントシステム規格に共通した原則として、申請組織が認証の適用範囲を組織全体でも、一部の部門や特定のサービスに限定しても良いとされている。

項目	説明
認証数	登録 68（公表 65）（2025 年 11 月 14 日時点）[18] ※ISMS-PIMS の認証数
更新期間	3 年間（毎年の定期審査と、3 年ごとの更新審査） ※ISMS-PIMS、PIMS 共通
認証の開始年	• ISMS-PIMS：2021 年 • PIMS：2026 年 8 月～2028 年 10 月に開始 （移行日に基づく）
公式情報	https://isms.jp/pims.html

また、ISMS-PIMS、PIMS では、組織の役割を PII 管理者（PII コントローラー）と PII 処理者（PII プロセッサー）に分類[19]し、管理策を規定している。GCBPR も同様に、コントローラーとプロセッサー向けの認証を取得することが可能であり、審査範囲も PII であり、親和性が高い。

(4) PIMS と GCBPR プログラム要件との比較分析

GCBPR は、9 つの GCBPR プライバシー原則[20]に基づいて策定された個人情報管理者（Personal Information Controllers：（以下、「コントローラー」という。））向けのグローバル CBPR 及びプロセッサー向けのグローバル PRP が提供されている。

グローバル CBPR は、コントローラーに関連するデータ保護及びプライバシーに係る義務を遵守する能力を証明することを支援するために設計されている。グローバル CBPR を取得する際には、これらのプログラム要件が反映された「GCBPR 事前質問書」（Global Cross-border Privacy Rules(CBPR) System Intake Questionnaire）を用いて、申請事業者がその遵守状況を評価しなければならない。

一方、グローバル PRP は、個人情報処理者（Personal Information Processors：（以下、「プロセッサーという。」））に関連するデータ保護及びプライバシーに係る義務を遵守するうえで、コントローラーを支援する能力を実証することを支援するために設計されているものである。

本調査においては、GCBPR の強みや利点の分析を行うため、GCBPR のプログラム要件と、2025 年 10 月に発行された ISO/IEC 27701:2025（PIMS）の比較分析を行った。

ISO/IEC 27701：2025 は、マネジメントシステム規格であり、組織は、プライバシーリスクアセスメントの結果を考慮して、プライバシーリスク対応の選択肢を選定し、その実施に必要なすべての管理策を決定することが求められる。組織は、決定した管理策を、PIMS（ISO/IEC 27701：2025）の付属書 A に示される管理策と比較し、必要な管理策が見落とされていないこ

[18] 一般社団法人情報マネジメントシステム認定センター（ISMS-AC）Web サイト「ISMS-PIMS 認証取得組織一覧」ページ https://isms.jp/isms-pims/lst/ind/index.html

[19] PII 管理者とは、私的な目的でデータを使う個人を除く、PII を処理するための目的及び手段を決定するプライバシー利害関係者を指す。PII 処理者とは、PII 管理者に代わり、かつ、その指示に従って PII を処理するプライバシー利害関係者を指す。

[20] 被害の防止、通知、収集制限、個人情報の利用、選択、個人情報の完全性、安全管理、アクセス及び訂正、アカウンタビリティ

とを検証することが求められるが、必要な場合には、組織は、管理策を追加、除外することもできる。付属書 A に定められる管理目的や管理策は、PII 管理者のためのもの、PII 処理者のためのもの、PII 管理者及び PII 処理者の共通のものに整理されている。

これらを踏まえ、本調査では、GCBPR のプログラム要件と、規格本文及び付属書 A の PII 管理者のための管理目的及び管理策、PII 管理者及び PII 処理者のための管理目的及び管理策を比較分析することとした。(ただ、実際には、それぞれの組織のリスクアセスメントの結果により、付属書 A の管理策に追加の管理策を含めている場合もあれば、管理策を除外している場合も想定されていることに留意いただきたい。)結果を(5)に示す。

また、同様に、グローバル PRP システムについても、グローバル PRP のプログラム要件と、PIMS(ISO/IEC 27701:2025)の規格本文及び付属書 A の PII 処理者のための管理目的及び管理策、PII 管理者及び PII 処理者のための管理目的及び管理策を比較分析した。

(5) グローバル CBPR のプログラム要件との比較

以下にグローバル CBPR のプログラム要件と比較結果を示す。プログラム要件と同等の要求事項がある場合は「○」、無い場合は「該当なし」、類似の要求事項があるが同等とは考えられない要求事項は「△」評価としている。また、プログラム要件が複数の選択肢を展開している場合、冒頭の質問部分は回答可能な場合を除き、選択肢のみを比較対象とする項目は斜線としている。[21]

① 通知

グローバル CBPR の「通知」に関するプログラム要件は、収集された個人情報、個人情報の譲渡先、及び個人情報の利用目的に関する貴社の方針を個人が理解できるようにすることや、通知の提供に関する適格性を条件として、個人情報がいつ収集され、誰に譲渡され、どのような目的で使用されるかを、個人が知ることができるようにすることを求めている。

PIMS においても、プライバシー方針を確立することが求められており、管理策としても、目的の特定、PII 主体のための情報の決定・情報の提供等が示されている。

図表 7 「通知」に関する GCBPR プログラム要件との比較

質問	PIMS
1. 上記の個人情報を管理する実務と方針について、明確で簡単にアクセスできる声明(プライバシーステートメント)を提供していますか？「はい」の場合、該当するすべてのプライバシーステートメントのコピー及び/又は同ステートメントへのハイパーリンクを提供してください。	○
a) プライバシーステートメントには、貴組織が個人情報を収集する方法が記載されていますか？	○

[21] プログラム要件の構成上、質問自体に回答する場合(例:質問1)と、選択肢のみに回答する場合(例:質問5)があり、後者の場合質問の比較欄は斜線としている。

質問	PIMS
b) このプライバシーステートメントには、個人情報を収集する目的が記載されていますか？	○
c) このプライバシーステートメントは、個人情報を第三者に提供するかどうか、またその目的は何かについて、個人に通知していますか？	○
d) このプライバシーステートメントでは、個人情報の収集の際に、個人情報の取扱いや慣行に関する連絡方法を含め、会社名及び所在地を開示していますか？「はい」の場合、以下に記述してください。	○
e) このプライバシーステートメントは、個人の個人情報の使用と開示に関する情報を提供していますか？	○
f) このプライバシーステートメントには、個人が自分の個人情報にアクセスし、訂正することができるかどうか、またその方法に関する情報が記載されていますか？	○
2. 以下の資格[22]に従うことを条件に、個人情報の収集時に（直接であるか、又はあなたの代理として行動する第三者を通じてであるかを問わず）、そのような情報が収集されていることを通知しますか？	○
3. 以下の資格に基づき、個人情報を収集する際、（直接であるか、代理で行動する第三者を通じてであるかを問わず）個人情報を収集する目的を明示していますか？	○
4. 個人情報を収集する際に、以下の資格の範囲内で、個人情報が第三者と共有される可能性があることを通知していますか？	○

② 取得の制限

GCBPR の「取得の制限」に関するプログラム要件は、情報の収集が、その情報が収集される目的に限定されていることを確認することを求めている。

PIMS においても、管理策として、PII の収集を目的との関係で制限することや、適法な根拠の特定等が示されている。

図表 8 「取得の制限」に関する GCBPR プログラム要件との比較

質問	PIMS
5. 個人情報をどのように取得していますか。	
a) 本人から直接取得していますか？	○
b) 第三者から取得していますか？	○
c) その他。該当する場合、具体的に説明してください。	○

[22] 資格とは、「GLOBAL CROSS-BORDER PRIVACY RULES SYSTEM（CBPR）PROGRAM REQUIREMENTS MAP」 https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Program-Requirements_Final.pdf の P.5～6 に記載される「Qualifications to the Provision of Notice」を指す。（以降、本報告書内のプログラム要件 2～4 について同じ。）

質問	PIMS
6. 個人情報の収集（直接であるか、又は第三者に代行してもらうかを問わず）を、収集の目的、又はその他関連のある、又は関連する目的を達成するために必要な範囲に限定していますか？	○
7. 個人情報の収集（直接であるか、又は第三者の代行によるものであるかを問わない）を、当該個人情報の収集を管轄する法域の要件に合致した、合法的かつ公正な手段によって行っていますか？「はい」の場合は、その内容を説明してください。	○

③ 個人情報の利用

GCBPR の「個人情報の利用」に関するプログラム要件は、個人情報の利用が、収集目的及びその他の適合又は関連する目的の達成に限定されることを保証することを求めている。

PIMS においても、管理策として、目的の特定、適法な根拠の特定等が示されている。

図表 9 「個人情報の利用」に関する GCBPR プログラム要件との比較

質問	PIMS
8. プライバシーステートメント及び/又は収集時に提供された通知で特定されているように、収集した個人情報の使用を（直接であるか、又はあなたの代理としての第三者の使用を通じてであるかを問わず）、情報が収集された目的、又はその他の互換性のある、又は関連する目的に限定していますか？必要に応じて、以下の空欄に説明を記入してください。	○
9.「いいえ」と答えた場合、収集した個人情報を、以下のいずれかの状況下で、関連性のない目的のために使用しますか？以下に記述してください。	
a) 本人の明示的な同意に基づくものですか？	○
b) 適用される法律により義務付けられている場合ですか？	○
10. 収集した個人情報（直接、又は貴社に変わって代行する第三者の利用を問わず）を他の個人情報管理者に開示しますか？「はい」の場合、説明してください。	○
11. 個人情報を個人情報処理業者に転送しますか？「はい」の場合、説明してください。	○
12. 質問 10 及び／又は質問 11 に「はい」と答えた場合、開示及び／又は移転は、収集の当初の目的、又は互換性のある別の目的もしくは関連する目的を果たすために行われますか？以下に記述してください。	○
13. 質問 12 に「いいえ」と答えた場合、又はその他適切な場合、開示及び/又は移転は以下のいずれかの状況下で行われますか？	
a) 本人の明示的な同意に基づくものですか？	○
b) 個人から要求されたサービスや製品を提供するために必要な場合ですか？	○
c) 適用される法律により義務付けられている場合ですか？	○

④ 選択

GCBPR の「選択」に関するプログラム要件では、個人情報の収集、利用及び開示に関連して、個人に選択肢が提供されることを確保することを求めている。

PIMS においても、管理策として、同意のタイミングの決定、同意取得、PII 主体に提供する情報の決定、情報提供等が示されている。GCBPR プログラム要件の質問 19 は、PIMS では管理策で、PII 主体へ明確かつ容易にアクセス可能な方法で情報提供を求めるものがあるものの、「手ごろなもの（affordable）」については明確な言及がないため、「△」評価としている。

図表 10 「選択」に関する GCBPR プログラム要件との比較

質問	PIMS
14. 個人情報の取得に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○
15. 個人情報の利用に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○
16. 個人情報の開示に関して個人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○
17. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示又は提供されていますか？	○
18. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それらは明瞭に表現され、容易に理解できるものですか？	○
19. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、その選択は簡単に利用でき手ごろなものですか？「はい」の場合、説明してください。	△
20. 必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄又は必要に応じて添付資料として説明を添えてください。	○

⑤ 個人情報の完全性

GCBPR の「個人情報の完全性」に関するプログラム要件では、記録の正確性と完全性を維持し、それらを最新の状態に保つことを確保することを求めている。

PIMS においても、管理策として、正確性及び品質に係る内容や、アクセス、訂正、削除に係る内容等が示されている。

図表 11 「個人情報の完全性」に関する GCBPR プログラム要件との比較

質問	PIMS
21. 利用目的に必要な範囲内において、保有する個人情報が最新かつ正確で完全なものであることを確認するための措置を講じていますか？「はい」の場合、その内容を説明してください。	○
22. 利用目的に必要な範囲内において、不正確・不完全、又は古い個人情報を修正する仕組みがありますか？必要に応じて、以下の空欄又は添付ファイルにその内容を記載してください。	○
23. 不正確・不完全、又は古い情報が利用目的に影響し、情報の移転後に修正が行われる場合、個人情報が移転された個人情報処理業者、代理人、又はその他のサービス提供者に修正内容を伝えていますか？「はい」の場合は、その内容を説明してください。	○
24. 不正確・不完全、又は古い情報が利用目的に影響し、情報の開示後に訂正が行われる場合、個人情報の開示先である他の第三者に訂正を伝えていますか？「はい」の場合は、その内容を説明してください。	○
25. 個人情報の処理者、代理人、又はその他のサービス提供者が、不正確・不完全、又は古い情報に気づいた場合、貴組織に通知することを要求していますか？	○

⑥ セキュリティ対策

GCBPR の「セキュリティ対策」に関するプログラム要件では、個人が組織に情報を預ける際に、個人情報の紛失や不正アクセス、情報の不正な破壊、使用、修正、開示、その他の悪用を防ぐために、合理的なセキュリティ保護措置によって情報が保護されることを保証することを求めている。

PIMS においても、リスクアセスメントの実施、結果を考慮したリスク対応が求められ、情報セキュリティの管理策が示されている。

GCBPR プログラム要件の質問 30 の c)及び質問 32 のセキュリティ障害の検知、防止、対応は、PIMS では、ログの取得、分析からの不正行為を見分けることに言及があるため「○」評価としたが、ISMS にあるような監視活動や、脆弱性情報の取得、マルウェアの検出等の管理策はない。

質問 30 の d）物理的セキュリティは、ISO/IEC27701:2019 では、「物理的セキュリティ境界」「物理的入退」「オフィス、部屋及び施設のセキュリティ」が管理策として含まれていたが、2025 年改正で N/A となっているため「△」評価としている。

質問 33 の安全対策の有効性テストは、PIMS に管理策として PII 処理に関連するソフトウェア及びシステムのセキュリティに配慮した開発のための規則の確立や適用が示されているが、開発や受入れのセキュリティテスト等は管理策として含まれていないため「△」評価としている。

質問 35a)の個人情報の処理者等へ、情報の機微性に応じた情報セキュリティプログラム導入及び c）のセキュリティ侵害時の迅速な措置を求めているかは、PIMS では、PII 管理者は PII 処理者と契約によって、全般的に、PII 処理者が、PII 管理者の義務を支援する役割を果

たすことが管理策として求められているものの、具体的な情報セキュリティに係る管理策としては、PII の送信の管理策の実施に対処することが示されている限りであったため「△」評価としている。また、b）のインシデント時の個人情報の処理者から管理者の速やかな通知は、PIMS でも通知は概念としてはあるがその実施タイミングまでの言及がなかったため「△」評価としている。

図表 12 「セキュリティ対策」に関する GCBPR プログラム要件との比較

質問	PIMS
26. 情報セキュリティポリシーを導入していますか？	○
27. 個人情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用等のリスクから個人情報を保護するために実施した物理的、技術的、管理的な保護措置について説明してください。	○
28. 質問 27 への回答で特定した保護措置が、脅威となる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明してください。	○
29. 個人情報のセキュリティ維持の重要性を従業員にどのように認識させているか説明してください（定期的な研修や監督等）。	○
30. 脅威となる危害の可能性と重大性、情報の機密性、及び情報が保持される状況に応じた保護措置を実施していますか？	
a) 従業員研修・管理、その他の組織的安全対策	○
b) ネットワークやソフトウェアの設計、情報の処理、保存、転送、廃棄を含む情報システムと管理	○
c) 攻撃、侵入、その他のセキュリティ障害への検知、防止、対応	○
d) 物理的セキュリティ	△
31. 個人情報を安全に廃棄するためのポリシーを導入していますか？	○
32. 攻撃、侵入、その他のセキュリティ障害を検知、防止、対応するための対策を実施していますか？	○
33. 上記の質問 32 で言及した安全対策の有効性をテストするためのプロセスを設けていますか？以下に説明してください。	△
34. 第三者認証やその他のリスク評価を利用していますか？以下に説明してください。	○
35. 個人情報を移転する情報処理業者、代理人、請負業者、又はその他のサービス提供者に対して、情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用から保護することを要求していますか？	
a) 提供される情報及びサービスの機密性に見合った情報セキュリティプログラムを導入していますか？	△
b) 貴組織の個人情報のプライバシー又はセキュリティの侵害の発生に気付いた場合、速やかに貴組織に通知していますか？	△
c) プライバシー侵害又はセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じていますか？	△

⑦ アクセス及び訂正

GCBPR の「アクセス及び訂正」に関するプログラム要件では、個人が自分の情報にアクセスし、修正できることを保証することを求めている。

PIMS においても、管理策として、PII 主体の要請の処理、処理される PII の複製の提供、アクセス、訂正、削除に係る内容等が示されている。

GCBPR プログラム要件の質問 37 の a)アクセスを要求する個人の身元確認は、PIMS において、PII 主体からの正当な要請に対応することは管理策で示されているが、身元確認まで明確に言及されておらず「△」評価としている。

質問 37 の d)の本人の個人情報へのアクセスの提供時に、本人との通常の対話形式に適合した方法での提供を求める点は、PIMS において、PII 主体への明確かつ容易にアクセス可能な方法との管理策はあるが、通常の対話形式へ適合までは言及されていないため「△」評価としている。

質問 37 の e)アクセス提供する場合の料金が過大でないことを求める点は、PIMS において、開示に係る手数料に法的に許可される場合があることに言及があるものの、料金設定は言及がないため、「該当なし」としている。

図表 13 「アクセス及び訂正」に関する GCBPR プログラム要件との比較

質問	PIMS
36. 要求があった場合、要求された個人に関する個人情報を保有しているかどうかの確認を行っていますか？以下に説明してください。	○
37. 要求に応じて、貴組織は個人に対して、貴組織が保有する個人情報へのアクセスを提供していますか？「はい」の場合、質問 37(a)～(e)に答え、アクセス要求の受付及び処理に関する組織の方針／手順を以下に記述する。「いいえ」の場合は、質問 38 に進んでください。	
a) アクセスを要求する個人の身元を確認する手段を講じていますか？「はい」の場合、説明してください。	△
b) 個人からのアクセス要求後、合理的な期間内でアクセスを提供していますか？「はい」の場合、詳細を説明してください。	○
c) 情報は、一般的に理解できる合理的な方法（読みやすい形式）で伝えられていますか？説明してください。	○
d) 情報は、本人との通常の対話形式（電子メール、同じ言語等）に適合した方法で提供されていますか？	△
e) アクセスを提供するために料金を請求しますか？「はい」の場合、その料金の根拠と、料金が過大でないことを保証する方法を以下に記述してください。	該当なし
38. 個人が自分の情報の正確さに異議を唱え、それを修正、補完、変更、及び/又は削除することを許可していますか？この点に関する組織の方針／手順を以下に記述し、質問 38 (a)～(e)に回答してください。	

質問	PIMS
a) アクセス及び訂正の仕組みは、明確かつ目立つように表示されていますか？必要であれば、以下の空欄又は添付ファイルにその説明を記入してください。	○
b) 個人情報が不完全又は不正確であると、本人から申し出があった場合、要求された訂正、追加、又は適切な場合には削除を行いますか？	○
c) 個人からの訂正又は削除の要求後、合理的な期間内にそのような訂正又は削除を行っていますか？	○
d) 訂正された個人情報のコピーを本人に提供するか、データが修正又は削除されたことを本人に確認していますか？	○
e) アクセス又は修正が拒否された場合、アクセス又は修正が提供されない理由を、アクセス又は修正の拒否に関する問い合わせ先とともに、本人に説明していますか？	○

⑧ 責任

GCBPR の「責任」に関するプログラム要件では、プライバシー原則を実現するための措置を遵守する責任があることを確認することを求めている。

PIMS においても、プライバシー方針や、役割、責任、権限、コミュニケーション、資源、力量、認識等に関する要求事項が定められており、管理策としても、PII 主体に対する義務の決定やその履行、適法な根拠の特定、共同 PII 管理者との間の役割や責任の決定、PII 処理者との契約等が示されている。

質問 39 及び質問 46 の、「自主規制機関の規範及び/又は規制の遵守」は、PIMS においては、組織及び状況の理解として、組織の目的や PIMS の意図した結果を達成する組織の能力に影響を与える、内部及び外部の課題を決定することを求めているが、自主規制機関の規範や規制には言及がないため、「△」評価としている。

GCBPR プログラム要件の質問 41 の苦情受付・調査・対応及び質問 42 の苦情に対する改善措置の説明は、異議申し立てや要請の処理に関する管理策はあるものの、質問 41 に関しては、調査についての明確な言及がないため、質問 43 に関しては、要請への対応は概念としてあるものの、改善措置の説明とまでの言及がないため、「△」評価としている。

質問 44 の苦情への対応を含む個人情報保護方針及び手順に関しての教育は、適切な教育は要求事項に含まれているものの、苦情への対応等の内容について具体的な言及はないため、「△」評価としている。

質問 47 の、個人情報の処理者等に GCBPR のプライバシーポリシーと慣行に従うことを求めること、実質的に類似したプライバシー慣行を求めること、その管轄区域において GCBPR 認定を受けることを求めること等は、GCBPR 特有の質問であり、「該当なし」とした。

質問 48 の、個人情報の処理者等に契約等の遵守を確認する自己評価の提出を求めるとの点、質問 49 の個人情報の処理者等への検査や監査の実施は、PII 処理者との契約において、取引先の義務の遵守を実証可能なように、場合によっては監査を含む適切な情報を取

引先に提出することが望ましいとされているが、それ以上の言及はないため「△」評価としている。

図表 14 「責任」に関する GCBPR プログラム要件との比較

質問	PIMS
39. 貴組織は、グローバル CBPR プライバシー原則を確実に遵守するために、どのような手段を講じていますか？該当するものをすべてチェックし、以下に説明してください。	
・ 内部指針又は方針（該当する場合、どのように実施しているか説明）	○
・ 契約	○
・ 適用される業界又はセクターの法律及び規制の遵守	○
・ 自主規制機関の規範及び/又は規則の遵守	△
・ その他	該当なし
40. 貴組織は、グローバル CBPR プライバシー原則を遵守する組織全体の責任者を任命していますか？	○
41. 貴組織は、プライバシーに関する苦情を受け、調査し、対応するための手順を備えていますか？説明してください。	△
42. 貴組織は、個人が苦情に対するタイムリーな回答を確実に受け取るための手順を備えていますか？	○
43. 「はい」の場合、この回答には、苦情に関する改善措置の説明が含まれていますか？説明してください。	△
44. 個人情報保護に関する苦情への対応方法を含め、個人情報保護方針及び手順に関して従業員を教育するための手順を設けていますか？「はい」の場合、説明してください。	△
45. 個人情報の開示を要求するものも含め、司法その他の政府による召喚状、令状、命令に応じるための手続きを定めていますか？	○
46. 個人情報を処理する個人情報処理者、代理人、請負業者、又はその他のサービス提供者との間で、個人に対する貴組織の義務が確実に果たされるような仕組みを設けていますか（該当するものすべてにチェックを入れてください）？	
・ 内部指針又は方針	○
・ 契約	○
・ 適用される業界又はセクターの法律及び規制の遵守	○
・ 自主規制機関の規範及び/又は規則の遵守	△
・ その他（記述）	
47. これらの仕組みは、一般的に、個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に要求しますか？	
・ プライバシーステートメントに記載されているグローバル CBPR に準拠したプライバシーポリシーと慣行を遵守すること	該当なし
・ 貴組織のプライバシーステートメントに記載されているポリシー又はプライバシー慣行と実質的に類似したプライバシー慣行を実施すること	該当なし

質問	PIMS
・ 個人情報の取扱い方法に関して、貴組織に提供された指示に従うこと	○
・ 貴組織の同意がない限り、下請けに制限を設けること	○
・ 管轄区域において、フォーラムが認定した AA からからグローバル CBPR の認定を取得すること	該当なし
・ その他（記述）	該当なし
48. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、貴組織の指示及び/又は契約の遵守を確保するための自己評価を提供するよう求めていますか？「はい」の場合、以下に説明してください。	△
49. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者について、貴組織の指示及び/又は合意/契約が遵守されていることを確認するために、定期的な抜き打ち検査又は監視を行っていますか？「はい」の場合、以下に記述してください。	△
50. 上記のような受領者によるグローバル CBPR システムの遵守を保証するデューディリジェンスや仕組みが現実的でない、又は不可能である状況において、個人情報を他の個人情報管理者に対して開示しますか？	○

(6) グローバル PRP のプログラム要件との比較

以下にグローバル PRP のプログラム要件と比較結果を示す。プログラム要件と同等の要求事項がある場合は「○」、無い場合は「該当なし」、類似の要求事項があるが同等とは考えられない要求事項は「△」評価としている。また、プログラム要件が複数の選択肢に展開している場合における、冒頭の質問部分等、比較対象として扱わない項目は斜線としている。

① 安全管理措置

グローバル PRP では 8 つの「安全管理措置」に係る要件を求めている。

PIMS においても、リスクアセスメントの実施、結果を考慮したリスク対応が求められ、情報セキュリティの管理策が示されている。

質問 4 のセキュリティ障害の検知、防止、対応は、PIMS には、ログの取得、分析からの不正行為を見分けることに言及があるため「○」と評価したが、ISMS にあるような監視活動や、脆弱性情報の取得、マルウェアの検出等の管理策はない。

質問 5 のセーフガードの有効性テストは、管理策として PII 処理に関連するソフトウェア及びシステムのセキュリティに配慮した開発のための規則の確立や適用が示されているが、開発や受入れのセキュリティテスト等は管理策として含まれていないため「△」評価としている。

図表 15 「安全管理措置」に関するグローバル PRP プログラム要件との比較

質問	PIMS
1. 貴組織は、管理者に代わって処理される個人情報をカバーする情報セキュリティ方針を実施していますか？	○
2. 貴組織の安全対策を実施するための物理的、技術的、管理的な保護措置について説明してください。	○

質問	PIMS
3. 貴組織で、従業員に個人情報のセキュリティ維持の重要性を認識させている方法を説明してください。	○
4. 貴組織は、個人情報に関連する攻撃、侵入、その他のセキュリティ障害を検出、防止、及び対応するための対策を実施していますか？	○
5. 貴組織は、上記の質問で言及された保護措置の有効性をテストするためのプロセスを備えていますか？説明してください。	△
6. 貴組織は、個人情報のプライバシー又はセキュリティの侵害が発生した場合、管理者に通知するプロセスを設けていますか？	○
7. 貴組織は、管理者の指示があった場合、又は契約が終了時に、個人情報を安全に廃棄又は返却するための手順を実施していますか？	○
8. 貴組織は、第三者認証やその他のリスク評価を利用していますか？説明してください。	○

② 説明責任措置

グローバル PRP では 10 の「説明責任措置」に係る要件を求めている。

PIMS においても、役割、責任、権限、資源、力量、認識に係る要求事項が定められており、管理策として、取引先の合意、取引先の指示のためだけに処理すること、PII 主体に対する義務の遵守、PII の返却、移転、処分、開示請求の通知、委託先等の開示、関与等に係る内容が示されている。

質問 13 は、苦情を処理者から管理者に転送する手順や、管理者の指示を処理する手順に関するものであるが、管理策として、処理者は管理者が PII 主体に対する義務を遵守する手段を提供することが望ましいとされているものの、質問 13 の観点ではそれ以上の具体的な言及がないため「△」評価としている。

質問 17 の c)の、サブプロセッサに、グローバル PRP を取得することを求めるという点は、グローバル PRP 特有の質問であり、「該当なし」としている。

質問 17 の d)の、サブプロセッサに契約等の遵守を確認する自己評価の提出を求めるとの点、e)の個人情報の処理者等への検査や監査の実施は、管理策では、PII を処理する委託先には契約に従って従事させることが求められており、取引先の義務の遵守を実証可能なように、場合によっては監査を含む適切な情報を取引先に提出することが望ましいとされているが、それ以上の言及はないため「△」評価としている。

質問 18 は、従業員の教育は要求事項であるが、「関連する顧客指示」を教育するかまでは定められていないため「△」評価としている。

図表 16 「説明責任措置」に関するグローバル PRP プログラム要件との比較

質問	PIMS
9. 貴組織は、個人情報の処理を管理者によって指定された目的に限定していますか？	○
10. 貴組織は、管理者からの要求に応じて情報を削除、更新、修正する手順を備えていますか？	○
11. 貴組織は、個人情報処理活動に関する管理者の指示を遵守するために、どのような措置を講じていますか？説明してください。	○
12. グローバル PRP システムの要件への全体的な準拠に責任を持つ個人を任命していますか？	○
13. 貴組織は、プライバシーに関連する個人の要求又は苦情を管理者に転送する手順、又は管理者から指示があった場合にそれらを処理する手順を備えていますか？	△
14. 貴組織は、法律で禁止されている場合を除き、個人情報の開示を要求する司法その他の政府による召喚状、令状、命令を管理者に通知していますか？	○
15. 貴組織は、サブプロセッサとの契約について管理者に通知する手順を備えていますか？	○
16. 貴組織は、個人情報が PRP に基づく義務に従って処理されることを保証するために、サブプロセッサと連携する仕組みを持っていますか？説明してください。	○
17. 上記で言及された仕組みは、一般的にサブプロセッサに対して以下を要求しますか？	
a) 個人情報の取扱いに関して貴組織から提示された指示に従うこと	○
b) 二次処理に制限を設けること	○
c) 各管轄地域のフォーラム認定 AA からグローバル PRP 認定を受けること	該当なし
d) 指示や合意/契約の遵守に関する自己評価やその他の証拠を組織に提供すること 「はい」の場合、説明してください。	△
e) 貴組織は、定期的な抜き打ち検査やその他の監視活動を行うことができますか？「はい」の場合、その内容を教えてください。	△
f) その他（記述）	該当なし
18. 個人情報保護に関する方針、手順及び関連する顧客指示に関して、従業員を訓練するための手順を設けていますか？説明してください。	△

③ 比較結果の分析

グローバル CBPR の 8 つの原則「通知」「取得の制限」「個人情報の利用」「選択」「個人情報の完全性」「セキュリティ対策」「アクセス及び訂正」「責任」ごと、グローバル PRP の「安全管理措置」「説明責任措置」ごとに、質問項目の数と、合致率を整理すると下表のとおりである。合致率は、「○」を 1、「△」を 0.5、「該当なし」を 0 の数値を設定して算出した。

グローバル CBPR の「通知」「取得の制限」「個人情報の利用」「個人情報の完全性」のプログラム要件は合致率が高い結果となった。一方で、合致率が100%を下回ったのはグローバル CBPR の「選択」「セキュリティ対策」「アクセス及び訂正」「責任」のプログラム要件、グローバル PRP の「安全管理措置」「説明責任措置」のプログラム要件である。グローバル CBPR のプログラム要件が求める具体的な管理策が、手ごろなもの、個人とのやり取りにおける身元確認の求め、対話形式の規定、苦情に係る調査の求め等、PIMS の管理策では、同等の粒度で示されていないものが見られた。また、セキュリティ対策は、ISMS 管理策には含まれる、物理的入退、マルウェア対策、脆弱性情報収集等が、PIMS の管理策には含まれていないのもあり、十分な合致と判断できない質問もあった。また、いわゆる委託先の管理（グローバル CBPR であれば処理者の管理、グローバル PRP であればサブプロセッサの管理）について自己評価の提出を求めたり、監査・検査の実施を求めたりしていることに対して、PIMS 側では概念できる管理策はあるものの、十分明確には示されていなかった。

図表 17 グローバル CBPR 及びグローバル PRP のプログラム要件と PIMS の合致率

区分	原則	質問数	○の数	△の数	該当なし	合致率	傾向
グローバル CBPR	通知	10	10	0	0	100%	
	取得の制限	5	5	0	0	100%	
	個人情報の利用	10	10	0	0	100%	
	選択	7	6	1	0	93%	選択肢が affordable であるかどうかについては PIMS 側では明確に示されていなかった。
	個人情報の完全性	5	5	0	0	100%	
	セキュリティ対策	15	10	5	0	83%	具体的にセキュリティに係る管理策は PIMS 側で十分示されていないものがあった。
	アクセス及び訂正	11	8	2	1	82%	身元確認や対話形式等具体的な管理策は PIMS 側で同様の粒度で示されていないものがあった。
	責任	22	12	7	3	70%	苦情や教育に係る具体的な管理策は PIMS 側で同様の粒度で示されていないものがあった。 GCBPR、グローバル PRP 特有の質問は合致しなかった。

区分	原則	質問数	○の数	△の数	該当なし	合致率	傾向
							処理者との契約においては、自己評価の提出や、監査・検査の実施等 PIMS 側では明瞭に示されていないものがあった。
グローバル PRP	安全管理措置	8	7	1	0	94%	具体的にセキュリティに係る管理策は PIMS 側で十分示されていないものがあった。
	説明責任措置	14	9	4	1	79%	サブプロセッサとの契約においては、自己評価の提出や、監査・検査の実施等 PIMS 側では明瞭でない部分があった。

(7) 他の制度に対するより詳細な GCBPR の強みや利点の分析

以上を踏まえ、R6 マッピング調査と合わせ、他の制度に対するより詳細な GCBPR の強みや利点について、以下のとおりそれぞれの観点から分析した。

① 制度概要の特性

GCBPR は、国境を越えて移転する個人情報の保護を目的とする点が、他の類似の認証制度と比較して審査範囲が明確であることが特徴的である。

また、他の規格が ISO/IEC の国際規格や、日本産業規格に基づいた認証制度であるのに対し、GCBPR は GCBPR フォーラムにおいて、各国政府機関の参画の下、独自のプライバシー原則、フレームワーク、プログラム要件等を構築し、申請事業者がコントローラー又はプロセッサー、或いは両方なのか、その役割と責任を個別に規定し認証する仕組みである点も他の認証制度とは異なる独自性の 1 つである。

さらに、GCBPR の特徴的な枠組みとして、グローバル CAPE(プライバシー執行のためのグローバル協力協定)がある。プライバシー執行機関(PEA)が国境を越えたデータ保護とプライバシー執行において協力するための実用的な多国間で、プライバシー執行機関が自主的に情報を共有し、特定の方法で支援を要請及び提供できる枠組みを構築することで実現されている。グローバル CAPE は、プライバシー執行機関間の協力を促進することにより、グローバル CBPR 及びグローバル PRP における信頼性と説明責任を備えた越境個人情報の流通基盤を提供する。

その他、盤石な紛争処理の仕組みがある点も挙げられる。GCBPR の AA は、自国の政府機関と共に苦情処理にあたるが、こうした制度としての機能が情報提供者の信頼を得る仕組みと言える。

それら苦情処理等の統計データや事例を各国 AA から1年に1度収集し、メンバー国内で共有する仕組みがあり、制度全体の信頼性の高さだけでなく、各国の審査機関の審査技術の

向上や標準化の促進につながっている。異なる法域の民間団体（政府組織が AA を担う国・地域もある）が AA として機能する上で、自浄作用が期待される重要な仕組みである。

なお、ISMS、PIMS 等に関しては、国際認定フォーラム（IAF-International Accreditation Forum, Inc.）が、マネジメントシステム、製品、要員等の適合性評価活動に関わる認定機関、審査機関協議会、各国の産業団体等からなる国際組織が組成されており、世界的に整合性のとれた適合性評価システムの開発や、認定された認証の信頼性の保証によるリスク低減が目指されている[23]。

② 認証単位

ISMS や ISMS-PIMS は組織単位での認証なので、利活用実態に応じて事業者が適切にマネジメントシステムの範囲を定めることができる点は、合理的であり、利点である。ただし、事業や部門ごとの取得となるため、認証制度の運用管理を一元化・統一化できず、複数部門で認証コストが発生する等、個社単位の GCBPR よりも、高コストになる可能性がある。また、ISMS や ISMS-PIMS の認証事業者が GCBPR の申請を検討する場合、審査範囲の変更や、自社内の申請状況を集約する等、別途認証単位のための工数が必要な点に留意する必要がある。

③ 認証期間[24]

GCBPR は 1 年ごとに再申請（半年でモニタリング）を行う仕組みである。ISMS や ISMS-PIMS は 3 年ごとだが、認証期間内にサーベイランス審査があるため、年 1 回審査があるのは同じである。ただし、初回審査や再認証審査に比べ審査範囲は軽度である。P マークは 2 年ごとの更新審査を実施する仕組みで、審査の範囲も全ての業務ではない。

認証期間は、賛否の分かれるところではあり、申請事業者は運用・管理面で労力の負担が大きいことも否めないが、毎年第三者が全ての業務を審査していることは、組織の信頼性を高めることにつながるので、強みであると言える。

④ 認証費用

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

P マークは、事業者の規模、新規又は更新かのみにより、審査費用があらかじめ定められており、固定料金である。

ISMS や PIMS は、CBPR と同様に、審査の対象とする組織の範囲やロケーション、要員数によって工数と金額が異なるため、見積りによる変動料金である。なお、ISO の審査工数の決定方法は、限定的ではあるが国際的な基準が示されており、認証機関に対する要求事項で

[23] ISMS-AC Web サイト「ISMS 適合性評価制度」パンフレット https://isms.jp/doc/ismspamph.pdf
[24] GCBPR は更新制ではないため、更新期間ではなく認証期間とした。

は、最低ラインとしての「審査工数」のみが決められているため、同じ条件で審査を申請した場合、審査機関により異なる。

図表 18 （参考）GCBPR と既存認証制度概要の比較

	項目	GCBPR	P マーク	ISMS	ISMS-CLS[25]	ISMS-PIMS	ISMAP/LIU[26]	27018[27]
1	管理対象	越境個人データ	個人情報	情報資産	クラウド	個人情報	クラウド	クラウド個人情報
2	目的と管理対象	国境を越えて移転する個人情報の保護	個人情報の保護と利用（事業の用に供しているすべての個人情報が対象）	情報資産の適切な管理	クラウドサービス提供利用時の固有の管理	PII（個人識別可能情報）の適切な管理	政府情報システムのためのセキュリティ基準	パブリッククラウド上の PII の保護
3	規格等	GCBPR 要求事項	P マーク運用指針	27001 要求事項	27017 要求事項	27701 要求事項	ISMAP 管理基準	27018 実施基準[28]
4	適合	要求事項をすべて満たす	要求事項をすべて満たす	要求事項と管理策を全て満たす必要	－	要求事項はすべてに足す必要（管理策は追加、除外可能）	－	－
5	開始年[29]	2025	1998	2002	2016	2021	2020	－
6	認証単位	法人（日本）（対象事業を特定した上で法人単位）	法人（日本）（学校法人、医療法人例外あり）	組織（範囲を指定可）	ISMS 範囲か一部	組織（範囲を指定可）	クラウドサービス	－

[25] ISMS 認証を前提としたアドオン認証となっており、クラウドサービス固有のリスクに対するセキュリティ対策の実施を確認する制度で、国際規格「ISO/IEC27017」を対策基準としている。

[26] ISMAP とは、政府情報システムのためのセキュリティ評価制度の一つ。セキュリティリスクの低いサービスを取り扱う SaaS 事業者が対象となる認証として、経済産業省に制定された評価基準。

[27] 「ISO/IEC 27018」は、クラウドサービス事業者がパブリッククラウド上で管理する個人情報の保護に焦点を当てた国際規格で、クラウドサービスを運営している組織（PII 管理者）向けの規格。

[28] 審査機関が定めた認証基準

[29] 開始年とは、制度自体が開始された年ではなく、日本で認証が開始された年を表す。

	項目	GCBPR	P マーク	ISMS	ISMS-CLS[25]	ISMS-PIMS	ISMAP/LIU[26]	27018[27]
7	更新期間	1 年（半年でモニタリング）	2 年	3 年（審査は 1 年ごと）	3 年（審査は 1 年ごと）	3 年（審査は 1 年ごと）	1 年 4 か月	–
8	取得数（国内）	4	17707	8009	615	68	77/1	–
9	審査機関数（国内）	1	20	27	18	5	4	–
10	審査費用	見積り	固定料金	見積り	見積り	–	–	–
11	審査方式	事業者の自己評価を審査（文書審査、現地審査）	個人情報保護マネジメントシステムを審査（文書審査、現地審査）	情報セキュリティマネジメントシステムを審査（初期審査では①第 1 段階審査と②第 2 段階審査）	プライバシー情報マネジメントシステムを審査（初期審査では①第 1 段階審査と②第 2 段階審査）	–	–	–

⑤　プログラム要件の観点

プログラム要件の観点では、GCBPR と P マークや PIMS は総じて合致率が高く、合致率が低い項目でも 70%以上の合致率であった。合致率が低いのは、「情報セキュリティ」や「委託先管理」に関連する要件となった。

個別の認証制度等との比較では、ISMS は情報資産を対象とした情報セキュリティマネジメントシステムであるため、「情報セキュリティ」においては、GCBPR よりも ISMS の方に具体的な管理策が定められており、合致率の高い結果となった。プライバシー原則や固有のプログラム要件には合致しないが、PIMS は原則のレベルで見れば、すべてカバーされているものの、ISMS 同様マネジメントシステム認証であり、基本的にはリスクアセスメントを踏まえてその対応が判断されるものである。P マークもマネジメントシステムであることから、同様の事が言える。

そのため、ISMS、PIMS、P マークの管理策は、相対的に抽象度が高い内容で示されている側面が見受けられ、GCBPR のプログラム要件が具体的であり実効的な側面があることが強みとして確認された。

図表 19 （参考）R6 調査結果の P マーク及び ISMS の CBPR プログラム要件との比較

原則	R6 調査結果		本調査	傾向
	P マーク	ISMS	PIMS	
通知	100%	10%	100%	方針の定めはどちらも要求されているが、ISMS の要求事項に通知内容の詳細な要求はない。
取得の制限	100%	0%	100%	P マーク、PIMS は 100%合致しているが、ISMS は必ずしも個人情報が含まれるものではないため合致度が低く、認証の趣旨の違いが反映されている。
個人情報の利用	100%	0%	100%	P マーク、PIMS は 100%合致しているが、ISMS は必ずしも個人情報が含まれるものではないため合致度が低く、認証の趣旨の違いが反映されている。
選択	100%	0%	93%	P マーク、PIMS は合致度が高いが、ISMS は必ずしも個人情報が含まれるものではないため合致度が低く、認証の趣旨の違いが反映されている。
個人情報の完全性	100%	100%	100%	P マーク、ISMS、PIMS はともに合致しており、情報の完全性はどちらも重要な要求事項であることが分かる。
セキュリティ対策	83.3%	100%	83%	ISMS では 100%合致しているが、P マーク、PIMS の管理策には十分な内容が示されていないものがあった。
アクセス及び訂正	100%	0%	82%	P マーク、PIMS は合致度が高く、ISMS は必ずしも個人情報が含まれるものではないため合致しておらず、認証の趣旨の違いが反映されている。
責任	91.3%	91.3%	70%	P マーク、ISMS との合致度は高いが、調査項目の解釈の見直しの影響により、PIMS は他の 2 つより合致率が低くなっている。

⑥ 根拠資料

日本においては、GCBPR 申請事業者は、「GCBPR 事前質問書」と各 AA の認証基準との適合を示す「追加質問書」に回答し、自己点検を行うとともに、その点検結果の根拠資料を提出する。GCBPR は、それぞれの質問表に回答された点検内容について、根拠資料を元に文書審査を行う。

GCBPR の申請事業者が用意する代表的な根拠資料（例）をポリシー・規程類と、記録類に対して、PIMS の規格本文や PII 管理者のための管理策において文書化や記録が要求されているものとの比較を行った。同等の内容の文書化が求められている場合は「〇」、同等とはいえないが類似の内容の文書化が求められている場合は「△」、該当しない場合は「該当なし」の表記とした。

GCBPR 審査で必要とされる自己点検結果を裏付ける根拠資料の例（ポリシーと規程類）と PIMS の規格本文や管理策の比較の結果は、下表のとおりである。

図表 20 GCBPR 審査で想定される根拠資料の例（ポリシーと規程類）

	GCBPR 審査で想定される根拠資料の例（ポリシーと規程類）	PIMS
1	プライバシーポリシー（プライバシーステートメント、個人情報保護方針等）	〇

	GCBPR 審査で想定される根拠資料の例（ポリシーと規程類）	PIMS
2	個人情報を特定する手順に関する規程	△
3	法令、国が定める指針その他の規範の特定、参照及び維持に関する規程	○
4	個人情報に関するリスクの認識、分析及び対策の手順に関する規程	○
5	事業者の各部門における個人情報を保護するための権限及び責任の規程	該当なし
6	緊急事態（個人情報を漏えい、滅失又はき損等）への対応に関する規程	○
7	個人情報の取得、利用及び提供に関する規程	○
8	個人情報の適正管理に関する規程（委託先に関する規程、従業者管理に関する規程、安全管理に関する規程等）	△
9	教育に関する規程	○

1、3、4、6、7、9 に関しては「○」とした。PIMS においては、規格本文や PII 管理者のための管理策において、プライバシー方針、PII 処理に関連する適法な根拠、プライバシーリスクアセスメント・リスク対応のプロセス、情報セキュリティインシデントへの対応手順、同意プロセス、力量等は、文書化の言及がある。

「2 個人情報を特定する手順に関する規定」に関しては、PIMS には目的の特定は文書化を求めているが、個人情報の特定は明確に求められていない。ただし、PII の処理に関連する記録は管理策が定められているため「△」とした。

「5 事業者の各部門における個人情報を保護するための権限及び責任の規程」に関しては、PIMS でも責任や権限の割り振りは求められているものの、その文書化は明確に求められていないため「該当なし」とした。

「8 個人情報の適正管理に関する規程（委託先に関する規程、従業者管理に関する規程、安全管理に関する規程等）」に関しては、情報セキュリティの管理策の一部に限られることと、PII 処理者との間も契約が想定されていること、従業者管理も秘密保持契約や守秘義務契約が想定されていること等から、本表では比較対象が（「契約書」ではなく）「規程」であることも踏まえ、「△」とした。

次に、GCBPR 審査で必要とされる事故点検結果を裏付ける根拠資料の例（記録類）と PIMS の規格本文や管理策の比較の結果は、下表のとおりである。

図表 21 GCBPR 審査で想定される根拠資料の例（記録類）

	GCBPR 審査で想定される根拠資料の例（記録類）	PIMS
1	組織図、GCBPR 体制	該当なし

	GCBPR 審査で想定される根拠資料の例（記録類）	PIMS
2	システム構成（システム構成図やネットワーク図等システム仕様の文書）	該当なし
3	セキュリティポリシー（情報セキュリティ基本方針等）	○
4	リスク分析及びリスクに対して講ずべき対策の一覧	○
5	個人情報取得時に本人に通知している文書	○
6	個人情報を特定し管理する台帳	○
7	委託先及び提供先の一覧	該当なし
8	委託先及び提供先を評価選定した記録	該当なし
9	委託先及び提供先との契約書	○

3、4、5、6、9 に関しては「○」とした。PIMS においては、情報セキュリティのための方針群を含む情報セキュリティプログラム、プライバシーリスクアセスメントの結果や対応結果の文書化や、PII 処理に関連する記録の維持、同意の取得及び記録が求められている。また、PIMS においては PII 処理者や共同 PII 管理者との間の契約が想定されている。

1、2、7、8 に関しては、PIMS において明確に文書化は求められていないため「該当無し」とした。委託先及び提供先との間で取り扱う PII は、契約書の確認が根拠となり、組織体制やシステム構成並びに委託先及び提供先の状況や選定基準等、運用を確認する根拠資料の文書化は求められない。

以上より、GCBPR 審査で必要とされる代表的な根拠資料（例）は、PIMS 審査で文書化や記録が求められるものと合致するものが複数あることがわかった[30]。

＜参考文献一覧＞

- GLOBAL CROSS-BORDER PRIVACY RULES SYSTEM (CBPR) PROGRAM REQUIREMENTS MAP
- GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEM PROGRAM REQUIREMENTS MAP
- ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

2.4. 企業認証プロセスの詳細分析及び効率化の検討

(1) 調査目的

[30] 根拠資料全てを意味するものではない。代表的な根拠資料（例）において GCBPR と PIMS との間で合致する点が見られた。

調査 2.3.、R6 マッピング調査及び R6 AA アンケート[31]の比較分析の結果を踏まえ、AA における企業認証プロセスを効率化するための方策を検討した。

(2) 実施期間

2025 年 10 月 23 日(木)～2025 年 11 月 19 日(水)

(3) 調査対象

調査 2.3.、R6 マッピング調査及び R6 AA アンケートの比較分析の結果を踏まえ、認証プロセスの詳細分析と効率化の検討に資する情報を収集するため、GCBPR フォーラムの認定を受けた 8 つの AA にアンケート調査への協力を依頼し、JIPDEC を含む計 9 つの組織を調査対象とした。

図表 22 アンケート調査実施機関

2025 年 11 月 30 日閲覧時点

	機関名称	概要		
		運営母体	認証開始	認証数[32] CBPR／PRP／両方 (認証事業者数)
1	Trust Arc(アメリカ)	民間	2013	32／25／6 (51)
2	Schellman(アメリカ)	民間	2019	5／12／3 (14)
3	NCC Group(アメリカ)	民間	2020	5／6／5 (6)
4	BBB National Program (アメリカ)	民間 (非営利)	2021	7／7／2 (12)
5	VeraSafe(アメリカ)	民間	2025	－／－
6	IMDA(シンガポール)	政府機関	2019	12／6／4 (14)
7	KISA(韓国)	政府委託	2019	12／－ (12)
8	III(チャイニーズ・タイペイ)	政府機関	2021	1／－ (1)
9	JIPDEC(日本)	民間 (非営利)	2016	4／－ (4)
認証事業者 合計				114[33]

[31] R6 調査報告書 第 2 章 CBPR の普及等に向けた活動 2.1.3 AA へのアンケート調査(49 頁～53 頁)を指す。
[32] GCBPR フォーラム https://www.globalcbpr.org/privacy-certifications/directory/
なお、グローバル CBPR とグローバル PRP の認証数は、1つの事業者が両方の認証を取得している場合、それぞれ1とカウントされるため、認証数の合計は認証事業者数と異なる。認証事業者数は( )内のとおり。
[33] 114 社は認証事業者数の合計。

(4) 調査項目

審査プロセスと重点を置いているプロセスを中心に、3 つのカテゴリで計 5 項目の質問を設定した。

＜アンケート調査項目＞

Assessment Questionnaire Response Form

■Questions Regarding efficiency in the review process
These Questions focus on the efficiency of the review process. For Q1 through Q3, please provide as much detail as possible regarding the review procedures.

Question 1
Please describe the specific steps of the review process, along with the man-hours and number reviewers, using the format below. *Sample (next page: Process by JIPDEC)

Question 2
Please mark ● in the critical process item within the review process and explain why you consider them important.

Reason:

Question 3
Please explain the basis for determining the number of Assessors (e.g., data volume, company requests, number of operations under evaluation).

Question 4
Are there forms or checklists used by Assessors during the audit process? (Y/N)
If "Yes", please list them below by audit stage.

Process Stage	Form Name and Purpose
Document Review	1. (Purpose/Description)
	2. (Purpose/Explanation)
Hearing	3. (Purpose/Description)
Report	4. (Purpose/Description)

Question 5
Please tell us about the review fees.

(5) 実施方法

AA へのアンケートでは、調査対象組織及び GCBPR フォーラム、GCBPR の所管官庁である個人情報保護委員会（委託元）の同意を得て、書面によるアンケート調査を実施した。なお、アンケート調査は、認証プロセスの詳細な工程及び工数等の確認も含まれるため、認証プ

ロセスの効率化を目的としたものであること等をアンケートフォーム送付時に、趣旨説明書として記載し、調査への協力を促した。

(6) 設問ごとの調査結果

① 審査プロセスの具体的な工程、及び工数、審査員数について以下のフォーマットに記載してください。(Q1)

- **具体的な審査工程**

R6 調査では、審査プロセスに AA 間で大きな違いはなく、文書審査とそのレビューを複数回行い、審査報告書を作成し、申請者に是正を求め、完了後に認証を付与する流れであった。

本調査では、共通する審査工程を詳しく追及した結果、各 AA が独自の工程に基づき審査を行っていることが分かった。大きく異なるのは、現地審査を実施しているか否かで、現地審査を実施しているのは 6 機関であった。

各 AA の審査工程は、独自に設定しているものを除き、回答に基づく共通事項で評価した。

図表 23 審査工程の評価項目

審査工程	審査内容
文書審査	50 の質問の適合性評価
	不備事項と是正措置の確認
	二次審査及び最終評価
現地審査	現地評価
報告書	報告書作成とレビュー
	是正措置報告書の作成とレビュー
審査の適正性評価	報告書の審査
	認証付与に関する審議
認証付与	審査結果の通知と証明(認定)書の発行

なお、各 AA の詳細な評価結果は付属資料「AA アンケートまとめ_公開版_1」に記載のとおりである。

- **工数**

オンラインプラットフォーム[34]を使用している AA は、比較的少ない工数が示された。また、現地審査を実施している AA の工数は、実施していない AA の工数と比較して全体的に工数が多い傾向が見られた。

[34] アメリカ商務省が作成及び提供しているウェブ上の申請システム、又は AA 独自に開発したプラットフォーム。

現地審査を実施している場合も、オンラインプラットフォームの使用と併せた結果、少ない工数となっている AA も見られた。

各 AA の全体工数は以下のとおりである。時間で回答があった AA は、1 人 8 時間／日で換算している。なお、審査プロセス前後の工数は対象外とした。

図表 24　工数

審査機関	全体工数
A	回答無し
B	13.5～24.5 人日
C	非公開
D	1.3～1.7 人日
E	小規模：7～11 人日 大規模：12.3～18.3 人日
F	4.5～20.5 人日
G	132 人日
H	22～36 人日
I	44 人日

※図表 23 の審査機関 1～9 と図表 25 の A～I は順不同で同一ではない（以降同じ）。

図表 25　オンラインプラットフォーム使用との比較

	A	B	C	D	E	F	G	H	I
工数	－	多	－	少	少	少	多	多	多
オンライン	○	×	○	○	○	○	×	×	×

図表 26　現地審査の実施有無との比較

	A	B	C	D	E	F	G	H	I
工数	－	多	－	少	少	少	多	多	多
現地審査	×	○	○	×	×	○	○	○	○

- **期間**

審査期間は、図表 28 のとおりで、組織によって 2.25～6 ヶ月の範囲で報告があった。AA アンケートの結果からは、工数やオンラインプラットフォームの利用、現地審査の有無による審査期間との相関は見られなかった。

また、1つの AA は、初期認証に加えてモニタリングプロセスについても回答しており、モニタリングの工数 2.25 人日を含む審査期間は 9 か月であると回答している。

図表 27 審査期間

審査機関	期間
A	3～6 か月
B	3.3～4.3 か月
C	2.3～4 か月
D	回答無し
E	3.7～4.7 か月
F	回答無し
G	4 か月
H	4 か月（プラス現地審査は変動）
I	3.5～4 か月

- **1 社あたりの審査員数**

1 社あたりの各審査工程に係る審査員数は 1 名から 4 名で、9 組織中、不明の1組織を除き、審査員の最少単位を 1 名とする AA が 7 組織であった。また、最大人数は、5 組織が 3 名と過半を占めた。未回答や、人数は変動すると回答している工程も多くあった。審査員数の決定根拠は、Q3 で後述する。

図表 28 1 社あたりの審査員数

審査機関	審査員数
A	不明
B	1～3 名
C	1～3 名
D	1～2 名
E	1～3 名
F	1～2 名
G	1～4 名
H	1～2 名
I	2～3 名

② 審査工程で特に重要な工程に●を記載し、理由も教えてください（Q2）

ほとんどの AA が文書審査:「50 の質問の適合性評価」を特に重要な工程であると回答しており、次いで重要な工程として、文書審査:「不備事項と是正措置の確認」、現地審査:「現地評価」という回答が多かった。

各 AA から回答された審査工程は異なるため、共通する審査工程で評価した。

各 AA が重要であると位置付けている工程の内訳は、以下のとおりである。

- **最重要工程**

  文書審査:「50 の質問の適合性評価」は、8 つの AA が最重要工程として位置付けており、主な理由は、「認証制度としての基礎となるコンプライアンス評価であり、認証の信頼性を直接的に支える要素。」であった。

- **重要な工程**

  文書審査:「不備事項と是正措置の確認」は、6 つの AA が重要な工程としており、主な理由は、「準拠していない領域や不備を特定し、認証を付与する前にそれらに対処しておくことが肝要であるため。」であった。

  現地審査:「現地評価」は、実施している 6 つの AA のうち、4 つが重要な工程としている。主な理由は、「文書化された方針や手順の実装状況を現地で直接確認することが、認証の完全性を確保できるため。」であった。

- **その他の重要な工程**

  文書審査:「二次審査及び最終評価」、報告書:「報告書作成とレビュー」、及び審査の適正性評価:「認証付与に関する審議」を複数の AA が重要工程として挙げている。

  何れも、各審査工程には複数の視点を入れること、また、審査結果を別の第三者が審議・評価する工程を審査プロセスに導入すること等で、認証の品質確保と保証につなげる工夫を行っていることが分かった。

③ 審査員数を決定する根拠を教えてください(データ量、企業希望、審査対象業務数等)。(Q3)

1 社あたりの審査に係る審査員数は前掲のとおりであるが、ほとんどの AA が、審査対象となる個人データを取り扱う業務数やシステム及びデータフローの複雑さ、情報の種類(機密性)等を挙げており、その他、個人データの量や対象となる拠点数等により、審査員数を確定している。

各 AA の審査員数を決定する根拠の詳細は、以下のとおりである。

図表 29 審査員数を決定する根拠

機関名称	審査員数を決定する根拠
A	・環境の複雑性 通常 2 名で実施するが、機能が複雑な場合、データフロー量が多い場合、又は証明内容に不備があるため追加確認が必要な場合は 3 名となる場合がある。
B	・審査体制 2つの別々のチームによる審査が必要であり、そのうち 1 つのチームが認証決定を行う。これは、認証決定が包括的な審査に基づいていることを保証するため。
C	・環境の複雑性 主に申請者の業務のデータ量と複雑さに依存する。多数のデータフロー、子会社、又は複数管轄区域にわたる活動を有する組織では、徹底的かつ効率的な審査を確保するため、一般的に追加の審査員が必要となる。 ・チーム構成 割り当てられたスタッフの習熟度や経験にも影響される。チームメンバーの経験が浅い場合やGCBPRの審査プロセスに不慣れな場合には、より経験豊富な審査員をペアに配置し、監督と品質保証を行う。このアプローチにより、作業負荷のバランスが取れ、学習が促進され、認証結果の一貫性が維持される。
D	・評価業務の範囲設定 人月単位で行う。 例:①単純な範囲(セキュリティとプライバシー対策が分散型アプローチの場合): 1名 3 週間体制 ②集中型意思決定と多数の製品/サービスに跨る統制適用が必要なケース: 2名 2 週間体制 ・重要な考慮事項 審査対象となる業務の数、対象システムの規模、評価対象となるプライバシー通知の数等が、データ量よりも重要である。 ・工数と審査員の人数 組織における審査範囲の複雑さ、集中型か分散型か、外部サービス提供、内部営業/従業員データ、又はその両方の組み合わせを審査するかによって決まる。

機関名称	審査員数を決定する根拠
E	・環境の複雑性 複数の事業部門、多様なデータフロー、又は複雑な国際業務を抱える組織では、通常、評価のあらゆる側面を適切にカバーするために、より多くの評価日数が必要になる。 ・データ量と機密性 個人データ処理量の増加や、より機密性の高いデータカテゴリー（健康記録、財務情報等）は、プライバシー管理とリスク軽減策の徹底的な評価を確実に行うために、追加の評価日数が必要になる場合がある。 ・組織の規模と構造 複数の子会社、合弁会社、又は複雑な企業構造を持つ大規模な組織では、認証取得を目指すすべての組織におけるプライバシー慣行を適切に評価するために、より多くの評価日数が必要になる。
F	・評価の範囲 評価対象となるシステム、アプリケーション、及び業務の数。 ・リスク評価 取り扱われる個人データの量と機密性、及び当該組織が管理者（controller）として機能するか処理者（processor）として機能するかによって決定される。 ・環境の複雑性 複雑性が高い、又はデータ量が多いほど、より多くのテストと審査員が必要となる。 ・クライアントの要求又は範囲定義 追加のシステムやサービスを含めることを選択した組織は、評価の作業負荷が増加する。 ・内部スケジューリング及び構造的保護措置 業務は運用管理チームによって管理され、業務担当責任者によって承認され、適切な人員配置を確保し、利益相反を回避する。
G	・環境の複雑性 申請組織の個人データの取扱者数、個人データ量、情報システム数、下請け業者数（例： データ処理業者）を考慮。

機関名称	審査員数を決定する根拠
H	・データ量/複雑性 非常に大規模なユーザーデータベース、並列サンプリングを必要とする複数のデータカテゴリ。 ・評価対象となる業務の数 複数の異なる処理操作又は事業ライン。 ・サイト/管轄区域 複数拠点・複数管轄区域における処理及び転送。 ・セクター別リスク分析 金融・医療セクターではより深い技術的カバーが必要となる可能性がある。
I	・個人データの越境移転が生じる業務の数 ・データ量 ・移転先国・地域の数 ・委託先の数 ・データを取り扱うシステムの理論構成の複雑性及びデータフローの複雑性 ・個人データの移転根拠（国内法に基づく）の複雑性等

④ 審査プロセスで審査時に審査員が使用する様式やチェックシートはありますか？（Q4）

本調査の結果、すべての AA が審査プロセスで使用するフォームやチェックシートを保有していることが明らかになった。

各 AA が整備している様式は、以下のとおりである。

図表 30 様式やチェックシートの有無

機関名称	様式やチェックシートの有無
A	・報告書、テストと報告のレビューワークフロー等の複数の様式が全社横断的に活用されている。 ・特に品質保証（QA）及び報告プロセスでは、広範なチェックリストが用いられ、テスト、報告、証明書の観点から包括的な確認が実施されている。
B	・文書審査、ヒアリング、現地審査の各段階で使用される報告書形式が整備されている。 ・グローバル CBPR システムプログラム要件マップもしくはそれに基づく内部チェックリストを用いて、申請者が提出した文書を CBPR フレームワークが要求する各具体的な評価基準に対して体系的に照合する仕組みが構築されている。

機関名称	様式やチェックシートの有無
C	・文書審査、ヒアリング、報告書の各段階で使用するチートシート及び共通テンプレートが整備されている。 ・文書審査段階では、質問に関する根拠書類をサポートするチートシートが用いられ、十分な証拠の完備に必要な書類の完全なリストが含まれている。 ・ヒアリング段階では、事業者との協議事項や未解決事項は、不足した根拠に関して共通のテンプレートが使用される。 ・報告書段階では、調査報告書が作成され、事業者がすべての要件を満たしていることを詳細に記述する。
D	・プラットフォーム上で評価を実施しており、デジタル形式の評価ツールを活用している。
E	・複数の段階で異なる様式が使用されている。 ・文書レビュー段階では、CBPR 評価ワークシート、証拠要約チェックリスト、公式 CBPR 受付質問票が用いられ、各段階で完全な文書提出と証拠の管理が確認される。 ・ヒアリング段階では、キックオフ会議アジェンダテンプレートが申請者との初期協議を構造化するために活用されている。 ・報告書段階では、コンプライアンス結果の要約に使用するテンプレートもある。 ・プロジェクト管理アプリを用いて提出の進捗状況を監視し、必要な資料がすべてアップロードされていることを確認うる。
F	・アンケート及び文書審査の段階で複数の形式が利用されている。 ・具体的には、フォーム 1-1（申請書）、フォーム 1-2（事前調査質問票）、グローバル CBPR/PRP プログラム要件チェックリスト、適用範囲及びマッピングチェックリスト、レビュー/テスト作業記録、QA レビューチェックリスト、認証証明書一式及び認証契約書等、計 7 種類の形式を整備している。 ※様式は知的財産であり、詳細な公開は制限されている。
G	・事業者が提出する自己評価フォームの内容を、AA に任命された評価機関が審査する。評価機関が作成した報告書等を AA がレビューし、承認するプロセスを採用している。

機関名称	様式やチェックシートの有無
H	・文書審査、予備審査、現地審査、認証付与に関する審議の各段階で、複数の様式が使用されている。 ・具体的には、様式 1（申請書）、様式 2（事前質問書）、様式 3（プライバシー管理システム詳細仕様書）、様式 4（チェックリスト及び不適合報告書様式）、様式 5（監査報告書）を整備している。 ・フォーム 3 には、国境を越えたデータ移転の状況、法定認証スキームの取扱い、個人データ処理フロー等、詳細情報の入力が必要とされている。
I	・文書審査から認証審査会までの各段階で、5 種類の様式が整備されている。 ・具体的には、事業者からの申請内容が適正かを確認するため、文書審査の段階で使用する、様式 A（点検表）、様式 B1（移転先一覧）、様式 B2（移転先管理状況確認シート）がある。 ・審査途中の段階で、様式 A、B1、B2 における確認又は指摘を行うための様式 C（指摘事項一覧）がある。 ・全ての審査を終えた後に、様式 D（審査結果報告書）を用いて、審査結果がとりまとめられている。

各 AA の使用する様式やチェックシートは、審査品質の確保と透明性の維持に必要不可欠な仕組みとして位置付けられている。

⑤ 審査費用について教えてください。（Q5）

政府が審査を委託しているKISAが無料（一時的に政府資金で運営）としている以外は、US＄3,600 から US＄65,445 のレンジで回答があった（調査実施期間 2025 年 10 月 23 日～11 月 19 日時点）。ただし、ほとんどの AA で申請事業者の規模や収益、形態も踏まえて審査費用を設定しており、上限を設定していない AA もあった。

各 AA の審査費用の詳細は、以下のとおりである。

図表 31 審査費用

審査機関	審査費用
A	・グローバル PRP　US$8,000～ ・グローバル CBPR　US$18,000～
B	・基本料金 $10,000～
C	・小規模/成熟事業者　US$24,210～38,220 （割引価格 US$16,925～26,625）

審査機関	審査費用
	・大規模/複雑/初回 US$44,010～65,445 （割引価格 US$30,925～45,875）
D	US$3,800～US$15,000 ※申請組織の規模に準じる
E	US $ 3,600～ （認証申請料 US$900、文書審査料$1,800、 現地審査料 US$900/人・日）
F	無料 政府機関からの委託
G～H	非公開

(7) AA における認証プロセスを効率化するための方策

以上を踏まえ、調査 2.3.、R6 マッピング調査及び R6 AA アンケートと合せ、認証プロセスを効率化するための方策を以下の観点からまとめた。

① 審査プロセスの工数削減

ほとんどの AA が文書審査:「50 の質問の適合性評価」を重要な工程の一つとして回答しており、他の認証制度等との比較において、民間の審査機関における審査の質や一貫性の担保、制度としての信頼性確保等が課題視される中、各 AA が適正に審査を行うことの重要性を共通の認識としていることが明らかとなった。

この工程に重点を置き、その他の調査結果である審査期間が短く、審査員数の最小化等に基づく審査プロセスを構築することができれば、CBPR 全体の工数削減に繋がり、工数の削減による審査料等の軽減も可能になるであろう。

さらに、オンラインプラットフォームを利用している AA の工数が少ないことが明らかになったことから、審査プロセスにオンラインプラットフォームを適用した場合の影響等も継続して調査を行い、制度と運用の両面から工数削減が可能な要素を明らかにし、効果的な審査プロセスの工数削減を導出できることが望ましい。

なお、米国商務省から各 AA へ提供可能なシステムを使用する場合でも、各国の法規則に準拠させる必要がある。よって導入時に開発費用やリソース等、準備に相当の時間と労力が必要になる点は留意が必要である。

GCBPR の認証期間が 1 年であることは ISMS の 3 年と比較して短いが ISMS は 3 年間の間に毎年維持審査を実施している。GCBPR も認証品質を保証できる審査の仕組みを構築できれば、AA と申請事業者双方が共に一部のプロセスを省略し、運用コストを下げることができるかもしれない。

② 複数認証取得へのインセンティブ

調査 2.2.の企業ヒアリングパートでは、複数の事業者から認証を取得した後の運用が負担であるという声が挙がっており、審査料が無償化になることよりも、認証制度のオペレーションにかかる労力やコストがより深刻であるという意見が複数挙げられた。実際に ISMS を取得している事業者からは、現状は複数認証を取得している場合でも、参照するデータベー

スや台帳は同一であるが、各認証に提出する資料は個別の加工・整形の対応が必要であり、別途工数をかけているとのことであった。

GCBPR は、P マークや ISMS 等他の第三者認証の後発認証である。既に他の認証を取得している事業者に対しては、審査を簡略化できるような仕組みを構築できれば、審査工数も削減でき、事業者の運用コストもさがるため、認証事業者増につながる可能性がある。

また、AA アンケート調査で、1 つの AA は他の認証取得とのセット提供により低額になるケースもあると回答している。その他の AA でもこのようなケースは存在している可能性があり、審査費用だけではなく、審査プロセスや、提出書類で省略もしくは簡略化している点がないか、更なる調査を実施すべきと考える。

2.5. GCBPR メンバー間の個人データの越境移転において認証事業者が受ける利点調査

(1) 調査目的

GCBPR 認定制度に参加する国や地域の拡大に向けて、他法域の認証事業者が日本の認証事業者に個人データを送信する場合、享受できるベネフィットが、送信元の法制度において、どのように担保されているか調査した。具体的には、日本の『個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）』「規則第 16 条」において、GCBPR が、外国にある第三者について日本法上と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているのと同様に、各法域の越境移転に関する法令・ガイドラインにおいて、GCBPR が事業者の越境移転規制への対応において、日本法上の相当措置に類似するような何等かのベネフィットを与えているか分析した。

各法域で参照した法令、政省令、ガイドラインは、図表 33 のとおりである。なお、アメリカは州法でのプライバシー保護に関する規制もあるが（カリフォルニア州消費者プライバシー法(CCPA)等）、データの外国への移転、すなわち州際通商はアメリカ憲法上州に規制権限がないため州法は対象外としている。また、アメリカは包括的な連邦レベルの個人情報保護法を有していないが、連邦取引委員会法や児童オンラインプライバシー保護法等において規律を有しているため、これらを調査対象としている。

(2) 調査対象

調査対象とする法域は、GCBPR のメンバーであるオーストラリア、カナダ、韓国、メキシコ、フィリピン、シンガポール、チャイニーズ・タイペイ、アメリカ、ドバイ国際金融センター、及びアソシエイトであるイギリスを合わせた 10 法域としている。アソシエイトであるイギリスを調査対象として含めた理由は、EU 外の枠組みへの参加意欲が高い上、日本事業者の進出も進んでいるためである。

図表 32 越境移転規制の調査対象

	法域名・ GCBPR 加盟属性	参照元
1	オーストラリア （メンバー）	・ Privacy Act 1988 ・ Australian Privacy Principles（APP）
2	カナダ （メンバー）	・ Personal Information Protection and Electronic Documents Act (PIPEDA)
3	韓国 （メンバー）	・ Personal Information Protection Act (PIPA)
4	メキシコ （メンバー）	・ The Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP)
5	フィリピン （メンバー）	・ Data Privacy Act of 2012(DPA) ・ Implementing Rules and Regulations of Republic Act No. 10173, Also Known as the “Data Privacy Act of 2012”(IRR)
6	シンガポール （メンバー）	・ The Personal Data Protection Act 2012 (PDPA) ・ Personal Data Protection Regulations 2021 (PDPR)
7	チャイニーズ・ タイペイ （メンバー）	・ Personal Data Protection Act (PDPA)
8	アメリカ （メンバー）	・ 懸念国による大量の機微個人データ及びアメリカ政府関連データへのアクセスの防止に関する大統領令（EO14117）（2024 年 3 月 12 日号） ・ 米司法省最終規則 28 C.F.R. Part 202（Data Security Program）
9	ドバイ国際金融 センター （メンバー）	・ DIFC Law No. 5/ of 2020 on the Data Protection
10	イギリス （アソシエイト）	・ UK General Data Protection Regulation (UK GDPR)

(3) 調査項目

上記の対象において、以下 5 つの項目を調査している。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか。
2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか。
3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか。
4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか。
5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか。

1 から 3 の調査項目は、越境移転規制に関する全体像を把握するとともに、この中で他法域の認証事業者が日本の認証事業者に個人データを送信する場合に享受できるベネフィットを確認することが目的である。第一に越境移転規制が存在するのかを確認した上で、越境移転が例外的に許される条件はあるか、また GCBPR がその条件に当てはまるかを確認する。

(4) 調査結果概要

まず、国家・連邦単位での個人情報保護関連の法令において、越境移転規制が存在するのは、図表 33 のとおり、日本、オーストラリア、韓国、シンガポール、チャイニーズ・タイペイ、アメリカ、ドバイ国際金融センター、イギリスの 8 法域である。なお、アメリカの越境移転規制は懸念国（中国、キューバ、イラン、北朝鮮、ロシア、ベネズエラ）に対する移転にのみ適用されることに留意が必要である。カナダ、メキシコ、フィリピンでは、処理先が国内か国外かを問わずに、個人情報の処理に関する義務が課されているものの、越境移転に限った規制は存在していない。

図表 33 調査対象法域における越境移転規制の有無・内容

※凡例：明示的な規制がある場合は○、越境移転に限らない個人情報の処理に関する規制がある場合は△として記載

	法域名	越境移転規制の有無	規制内容
0	日本 （メンバー）	○	・ 個人情報保護取扱事業者は、外国にある第三者に個人データを提供する場合には、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得ること 【個人情報の保護に関する法律 第 28 条第 1 項】
1	オーストラリア （メンバー）	○	・ 個人情報を開示する前に、APP(Australian Privacy Principles)に違反しないよう合理的な措置を講じること【Privacy Act 1988 APP8.1】 ・ APP に違反する海外の受領者の行為又は慣行に対して、事業体が責任を負うこと【Privacy Act 1988 s 16C】
2	カナダ （メンバー）	△	・ 越境移転に限った規制は存在しない ・ ただし、越境移転に限らない個人情報の処理に関する義務として以下が規定： 処理のために第三者に譲渡された情報を含め、その所有又は保管中の個人情報について責任を負うこと。 また、情報が第三者によって処理されている間、同等のレベルの保護を提供するために、契約又はその他の手段を使用すること【PIPEDA 第 4 条第 1 項第 3 号】
3	韓国 （メンバー）	○	・ 原則として、個人情報管理者による個人情報の委託処理・保管（越境移転）は認められない。 例外に当てはまる場合のみ、個人情報の越境移転が認められる 【PIPA 第 28 条の 8】
4	メキシコ （メンバー）	△	・ 越境移転に限った規制は存在しない ・ ただし、越境移転に限らない個人情報の処理に関する義務として以下が規定： 個人情報管理者が、委託先以外の国内又は外国の第三者に個人データを移転しようとする場合、これらの第三者に対し、プライバシー通知及び、データ主体がその取扱いに同意した利用目的を通知すること。データの

	法域名	越境移転 規制の有無	規制内容
			取扱いは、プライバシー通知で定められた内容に従って行わなければならず、この通知には、データ主体が自身のデータ移転を承諾するか否かを明示する条項を含めること。また、第三者受領者は、データを移転した管理者と同等の義務を負うこと 【LFPDPPP 第 35 条】
5	フィリピン （メンバー）	△	・ 越境移転に限った規制は存在しない ・ ただし、越境移転に限らない個人情報の処理に関する義務として以下が規定： 各個人情報管理者は、自らが管理又は保管する個人情報について責任を負う。これには、国境を越えた取決め及び協力のもと、国内又は海外を問わず、処理のために第三者に移転された情報も含まれる (a)個人情報管理者は、第三者が情報を処理している間も、契約その他の合理的な手段を用いて、同等の保護水準を確保するものとする (b)個人情報管理者は、組織を代表してこの法律を遵守する責任を負う個人（複数も含む）を指名しなければならない。当該指名された個人の氏名等は、データ主体からの請求に応じて開示されるものとする 【DPA 第 21 条】
6	シンガポール （メンバー）	○	・ 組織は、シンガポール国外の国又は地域にいかなる個人データも移転してはならない。ただし、当該移転される個人データに対し、本法による保護と同等の水準の保護が提供されることを確保するために、PDPA に基づき定められた要件に従う場合は、この限りでない【PDPA 第 26 条】 ・ (1)PDPA 第 26 条の規定に基づき、シンガポールから国外へ個人データを移転する組織（移転組織）は 2021 年 2 月 1 日以降に個人データをシンガポール国外の国・地域へ移転する場合、当該個人データの受領者が法的拘束力のある義務（PDPR 第 11 条に準拠）により、移転された個人データに対して、PDPA が定める保護水準と同等以上の保護水準を提供することを確実にするため、適切な措置を講じなければならない【PDPR 第 10 条】
7	チャイニーズ・ タイペイ （メンバー）	○	・ 政府以外の主体が以下のいずれかの状況下で個人データを国境を越えて移転する場合、当該業界を担当する中央政府機関は、その移転に対して制限を課すことができる： 1. 国家の重大な利益に関わる場合 2. 国際条約又は協定で規定されている場合 3. 個人データの受領国に適切な個人データ保護規制が存在せず、その結果データ主体の権利及び利益が侵害されるおそれがある場合 4. 個人データを第三国（地域）へ移転することが PDPA を回避するためである場合 【PDPA 第 21 条】
8	アメリカ （メンバー）	○	・ 懸念国（中国、キューバ、イラン、北朝鮮、ロシア、ベネズエラ）に対する「大量の機密個人データ」又は「アメリカ政府関連データ」の移転を禁止【大統領令（EO14117）第 2 節(a)】 ・ 「大量の機密個人データ」には以下のカテゴリが存在し、それぞれのカテゴリで「大量」とみなされる定義が存在

	法域名	越境移転 規制の有無	規制内容
		※懸念国への移転のみ制限	1. ヒト・オミックスデータ、又はヒトゲノムデータ 2. 生体識別子 3. 正確な位置情報データ 4. 個人健康データ 5. 個人財務データ 6. 特定の個人識別子 7. 結合データ（上記の組み合わせによるもの） 【28 C.F.R. Part 202 第 205 条】
9	ドバイ国際金融センター：DIFC（メンバー）	○	・ 第三国又は国際機関への個人データの移転は、以下のいずれかの場合にのみ行うことができる 1. 当該個人データに対して、適用法により適切な保護水準が確保されている場合（コミッショナーが越境移転先の第三国又は国際機関の保護水準を判断） 2. 第 27 条の例外条件に当てはまる場合 【DIFC Law No. 5/ of 2020 on the Data Protection 第 26 条第 1 項】
10	イギリス（アソシエイト）	○	・ 特定の条件を満たす場合にのみ越境移転が可能【UK GDPR 第 44A 条：移転に関する一般原則】

個人情報の移転に関する規制が存在する場合、どのような条件で移転が認められるかを図表 34 にまとめている。

なお、図表 34 では、例外条件としては規定されておらず、移転に関する規制そのものに含まれる内容も「○（条件が存在する）」としてカウントしている。例えば日本では、個人情報の保護に関する法律第 28 条第 1 項にて、「個人情報取扱事業者は、外国にある第三者に個人データを提供する場合には、前条第 1 項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。（注釈は省略）」とある。「前条第 1 項各号に掲げる場合」が例外条件であるが、規制そのものに含まれている「本人の同意」を得た場合についても、移転が認められる条件として「○」としてカウントされる。

本調査は、他法域の認証事業者が日本の認証事業者に個人データを送信する場合、享受できるベネフィットが、送信元の法制度において、どのように担保されているかを確認することが目的である。

移転が認められる条件として、「越境移転先が自法域と同等の水準の個人情報保護制度を有している場合」、いわゆる相当措置を認めている法域は、日本、オーストラリア、韓国、シンガポール、ドバイ国際金融センターの 5 法域である。

そのうち、GCBPR の取得が越境移転時の例外条件として明示的に認められている法域は、シンガポール、ドバイ国際金融センターの 2 法域である。この 2 法域は、認証事業者間で個人データを送信する際にベネフィットを享受できるとみなせる。

図表 34　調査対象法域において越境移転が認められる条件

※凡例：◎は GCBPR の取得が越境移転時の例外条件として明示的に認められている法域

法域名	越境移転先が自法域と同等の水準の個人情報保護制度を有している場合	データ主体の明示的な同意*に基づく場合 *同意の留意事項は各法域詳細を参照	法令や裁判所命令に基づく場合	外交・領事・国防活動において必要な場合や、国際協定に基づく場合	契約履行のために必要な場合	人々の生命・健康・安全等に関わる場合	公共機関が法令上で定められた機能を果たすために必要な場合 （犯罪捜査等）	その他
日本	○	○ ※1	○	—	—	○	○	—
オーストラリア	○	○	○	○	—	○	○	—
カナダ	—	—	—	—	—	—	—	—
韓国	○	○	—	○	○	—	—	※2
メキシコ	—	—	○	○	○	○	○	※3

法域名	越境移転先が自法域と同等の水準の個人情報保護制度を有している場合	データ主体の明示的な同意*に基づく場合 *同意の留意事項は各法域詳細を参照	法令や裁判所命令に基づく場合	外交・領事・国防活動において必要な場合や、国際協定に基づく場合	契約履行のために必要な場合	人々の生命・健康・安全等に関わる場合	公共機関が法令上で定められた機能を果たすために必要な場合（犯罪捜査等）	その他
フィリピン	—	—	—	—	—	—	—	—
シンガポール	◎	○	—	—	—	—	—	—
チャイニーズ・タイペイ	—	—	—	—	—	—	—	※4
アメリカ	—	—	—	○	—	—	○	※5
ドバイ国際金融センター（DIFC）	◎	○	○	—	○	○	○	※6
イギリス	—	○	○	—	○	○	○	※7

※1：日本の個人情報の保護に関する法律における「本人の同意」とは、個人関連情報取扱事業者が第三者に個人関連情報を提供し、当該第三者が当該個人関連情報を個人データとして取得することを承諾する旨の当該本人の意思表示のことである。データ主体の明示的な同意として、以下の6つの事例が挙げられる。

【個人情報の保護に関する法律についてのガイドライン（通則編）】
事例 1）本人からの同意する旨の口頭による意思表示

事例 2)本人からの同意する旨の書面(電磁的記録を含む。)の受領
事例 3)本人からの同意する旨のメールの受信
事例 4)本人による同意する旨の確認欄へのチェック
事例 5)本人による同意する旨のホームページ上のボタンのクリック
事例 6)本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

※2:韓国では以下の例外あり。

【PIPA 第 28 条の 8 第 1 項】
4.個人情報の受領者が、第 32 条の 2 に基づく個人情報保護認証等、保護委員会が定めて公示した認証を取得し、次のすべての措置を講じた場合
(a)個人情報の保護に必要な安全措置及び情報主体の権利を保障するために必要な措置
(b)個人情報の移転先国において、認証事項を実施するために必要な措置

※3:メキシコでは以下の例外あり。また、処理先が国内か国外かを問わず、個人情報の処理に関して課されている義務の例外条件であることに留意。

責任者の共通の支配下にある親会社、子会社、又は関連会社、あるいは同一グループに属し、同一のプロセス及び内部方針に基づいて運営されている会社に対して移転が行われる場合

※4:チャイニーズ・タイペイでは、越境移転規制の例外条件は存在していない。PDPA そのものの例外条件として、以下が含まれている。

【PDPA 第 51 条】
1.個人が自身の個人的又は家庭内の活動目的のみで個人データを収集、処理、又は使用する場合
2.音声・映像データが公共の場や公共の活動において収集、処理、又は使用される場合であって、他の個人データと関連付けられていない場合

※5:アメリカでは以下の例外あり

【28 C.F.R. Part 202】
以下の活動に伴うデータ移転の場合は、全て越境移転規制の対象外とされる
1. 個人間通信(第 501 条)
2. 情報あるいは情報資料(第 502 条):表現的な内容に限定。出版物・映画・ポスター・レコード等
3. 渡航(第 503 条)
4. 金融サービス(第 505 条)
5. 事業者グループ間取引(第 506 条)
6. CFIUS の審査対象となる投資契約(第 508 条) :外国人・外国法人等がアメリカ事業者又はアメリカ内事業に関与する取引のこと
7. 電気通信サービス(第 509 条)
8. 医薬品、生物学的製剤、及び医療機器の承認に関する規定(第 510 条)
9. その他の臨床試験及び市販後調査データ(第 511 条)

司法省から一般ライセンス(第 801 条)や個別ライセンス(第 802 条)を取得することで、上記に当てはまらない移転も可能となる

※6:ドバイ国際金融センター(DIFC)では以下の例外あり

【DIFC Law No. 5/ of 2020 on the Data Protection 第 27 条第 3 項】
h. 移転が、一般に公開されることを目的とした登録簿から行われ、かつ次の条件を満たす場合:
   (i) 公衆全体、又は正当な関心を有する者によって閲覧できる
   (ii) 適用法及びデータ最小化の原則(第 9 条第 1 項(f))に従っている
j. 国際的金融基準に基づき、移転が国際金融市場で認められる管理者の正当な利益を維持するために必要である場合。ただし、その利益がデータ主体の正当な利益によって上回らないこと

【DIFC Law No. 5/ of 2020 on the Data Protection 第 27 条第 4 項】

4. 第 27 条第 1 項～第 3 項、又は第 26 条のいずれの規定にも基づくことができない場合でも、以下の条件を全て満たすときに限り、第三国又は国際機関への移転を行うことができる

a. 移転が繰り返し行われるものではないこと

b. 限られた数のデータ主体に関するものであること

c. 移転が、データ主体の利益又は権利によって覆されない、管理者の強く正当な利益を目的とする場合であること

d. 管理者が、移転に関連するすべての状況について文書による評価を完了し、その評価に基づいて個人データの保護に関する適切な保護措置を提供したこと

※7:イギリスでは以下の例外あり

【UK GDPR 第 45A 条 規則によって承認された移転】

・ データ保護テスト(第 45B 条に規定)が満たされると判断する場合に限り、三国又は国際機関への移転を承認

【UK GDPR 第 49 条 特定の状況における例外】

(g) 移転が、国内法により公衆への情報提供を目的として設けられた登録簿から行われ、かつその登録簿が一般公衆又は正当な利益を有する者による閲覧に開放されており、かつ個別の事例において当該国内法に定められた閲覧条件が満たされている場合

・ さらに、UK GDPR の例外条件(図表 34 で〇評価をつけている項目、上記のデータ保護テスト(第 45B 条)、その他例外条件(第 49 条 g)のいずれか)に該当しない場合、以下の全ての条件を満たす場合は越境移転が許可

➢ その移転が反復的でないこと

➢ 限定された数のデータ主体にのみ関係すること

➢ 移転が、管理者の追求するやむを得ない正当な利益のために必要であり、データ主体の利益又は権利・自由によってこれが凌駕されないこと

➢ 管理者が移転の状況を評価し、適切な保護措置を講じたこと

続いて、調査対象法域において、データローカライゼーションの対象となるデータ、及びそれらを規定する法令・政省令・ガイドライン名を図表 35 にまとめている。また、図表 36 にて、データローカライゼーションの対象となるデータの種別をまとめている。医療・金融情報のデータローカライゼーションを義務付けている法域が多く見られたが、クラウド利用時のみに限定されることも多い。

図表 35 調査対象法域におけるデータローカライゼーション

法域名	データローカライゼーションの対象	データローカライゼーションを規定する法令・政省令・ガイドライン名	法令・政省令・ガイドライン等の詳細
日本	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	—
オーストラリア	・ 医療情報	1. My Health Records Act 2012	1. マイヘルスレコード及び関連情報は国外での保管・持ち出し・処理・取扱いが一切禁止（例外条件なし）【第 77 条】
カナダ	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	—
韓国	・ 医療情報 ・ 金融情報	1. 電子義務記録の管理・保存に必要な施設と装備に関する基準 2. 金融会社の情報処理業務委託に関する規定 3. 電子金融監督規定	1. 電子医療記録システム及びそのバックアップ装置の物理的な設置場所は、国内に限定 【別表：医療機関外の場所に電子医療記録を保管する際に必要な追加措置】 ※電子医療記録情報自体の越境移転を禁じる規則ではない 2. 個人顧客の固有識別情報（住民登録番号・パスポート番号・運転免許番号・外国人登録番号）は暗号化等の保護措置をしなければならず、特に国外に移転禁止【第 5 条第 1 項】 3. クラウドコンピューティングサービスを利用して固有識別情報又は個人信用情報（取引内容や信用度等を判断できる情報）を処理する場合、その情報処理システムの物理的な設置場所は国内に限定【第 14 条第 8 項】 ※個人信用情報自体の越境移転を禁じる規則ではない

法域名	データローカライゼーションの対象	データローカライゼーションを規定する法令・政省令・ガイドライン名	法令・政省令・ガイドライン等の詳細
メキシコ	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	―
フィリピン	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	―
シンガポール	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	―
チャイニーズ・タイペイ	・ 医療情報 ・ 金融情報	1. 医療機関の電子病歴の作成及び管理に関する規則 2. 金融機関が業務を第三者に委託する際の内部管理体制及び手続に関する規則	1. 医療記録のデータの収集や処理、利用等にクラウドサービスを利用する場合は、データの保存場所を国内に限定【第 8 条第 2 項】 2. クラウドサービスを利用する場合は、重要な消費者向け金融業務情報システムに関連する顧客データの保存場所は国内に限定【第 8 条第 2 項】
アメリカ	・ 金融情報	1. 内国歳入法ガイドライン	1. クラウド環境で財務取引情報（FTI）を受領・処理・保存・アクセス・保護・送信する場合は、処理の場所を国内に限定【2.E.6.1】
ドバイ国際金融センター（DIFC）	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	―
イギリス	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	―
ベトナム	・ 通信又はインターネットサービスの利用者情報・生成情報	1. サイバーセキュリティ法	1. ベトナムのサイバースペースにおいて、通信ネットワーク上、インターネット上、又はその他の付加価値サービスを提供する国内外の事業者は、ベトナムにおけるサービス利用者の個人情報・利用者間の関係に関するデータ・利用者によって生成されたデータを収集・利用・分析・処理する活動を行う場合、これらのデータを政府が定める一定の期間、ベトナム国内に保存しなければならない。外国事業者は、ベトナム国内に支店又は代表事務所を設置しなければならない【第 26 条第 3 項】

法域名	データローカライゼーションの対象	データローカライゼーションを規定する法令・政省令・ガイドライン名	法令・政省令・ガイドライン等の詳細
タイ	・ なし	・ 本調査で把握している限り、対象法域の単位でのデータローカライゼーション規制はなし	―
インドネシア	・ 公共部門の電子システムデータ ・ 金融情報	1. 電子システム及び電子取引の運用に関する規則 2. 非銀行金融サービス機関による情報技術の利用におけるリスク管理の実施 3. 商業銀行による情報技術の利用におけるリスク管理の実施	1. 公共部門の電子システム提供者は、電子システム・電子データの管理・処理・保存をインドネシア領域内で実施しなければならない【第 20 条】 2. インドネシア金融庁（OJK）の承認を得た場合を除き、電子システムのデータセンター又は災害復旧センターをインドネシア領域外に配置してはならない【第 23 条第 3 項】 3. 銀行は、情報技術を基盤とする取引処理をインドネシア領域内で実施しなければならない【第 23 条第 1 項】

図表 36 調査対象法域においてデータローカライゼーションの対象となるデータ

法域名	医療情報	金融情報	その他
日本	—	—	—
オーストラリア	○	—	—
カナダ	—	—	—
韓国	○	○（一部はクラウド利用時のみ※）	—
メキシコ	—	—	—
フィリピン	—	—	—
シンガポール	—	—	—
チャイニーズ・タイペイ	○（クラウド利用時のみ）	○（クラウド利用時のみ）	—
アメリカ	—	○（クラウド利用時のみ）	—
ドバイ国際金融センター（DIFC）	—	—	—
イギリス	—	—	—
ベトナム	—	—	通信又はインターネットサービスの利用者情報・生成情報
タイ	—	—	—
インドネシア	—	○	公共部門の電子システムデータ

※1：個人信用情報（取引内容や信用度等を判断できる情報）はクラウド利用時のみデータローカライゼーションが規定。個人顧客の固有識別情報（住民登録番号・パスポート番号・運転免許番号・外国人登録番号）はクラウド利用とは関係なく国外への移転が禁止。

調査対象法域において、ガバメントアクセスが認められている目的を図表 37 にまとめている。なお、個別に裁判所の令状審査が必要な法令・政省令・ガイドライン等は本調査の対象外としている。また、ガバメントアクセスを認める法令等の有無は、本調査で把握している情報に限られている。

令状審査なしでガバメントアクセスが認められる最も一般的な目的としては、犯罪捜査が挙げられる。犯罪捜査目的では、オーストラリア、シンガポール、チャイニーズ・タイペイ、アメリカ、イギリス、ベトナム、タイ、インドネシアの 8 法域でガバメントアクセスが認められている。

図表 37　調査対象法域においてガバメントアクセスの対象となるデータ

法域名	法令等の有無	目的					
		犯罪捜査	税務調査	国家安全保障	サイバー脅威の防止	外国刑法の執行支援	その他
日本	なし	—	—	—	—	—	—
オーストラリア	あり	○	○	—	—	○	—
カナダ	なし	—	—	—	—	—	—
韓国	なし	—	—	—	—	—	—
メキシコ	なし	—	—	—	—	—	—
フィリピン	あり	—	○	—	—	—	—
シンガポール	あり	○	—	—	○	—	—
チャイニーズ・タイペイ	あり	○	○	○	—	—	—
アメリカ	あり	○	—	○	—	—	—
ドバイ国際金融センター（DIFC）	なし	—	—	—	—	—	—
イギリス	あり	○	○	—	—	—	—
ベトナム	あり	○	—	○	○	—	※1
タイ	あり	○	—	—	○	—	—
インドネシア	あり	○	—	—	—	—	—

※1：ベトナムでは、監察・苦情・告発の解決、ならびに汚職対策に関連する調査もガバメントアクセスの対象となる。

ベトナム・タイ・インドネシアにおいて、ガバメントアクセスを規定する法令を図表 38 に詳細をまとめている。タイ・インドネシアは電子データのみが対象となっている（タイの特別事件捜査法を除く）一方で、ベトナムは国家安全保障・犯罪捜査・汚職解決のためであれば、それらの目的に関連するデータには全てアクセスできる法令になっている。

図表 38 ベトナム・タイ・インドネシアにおけるガバメントアクセス

法域名	目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等
ベトナム	・サイバーセキュリティ法違反の調査	・通信又はインターネットサービスの利用者情報	・公安省の専門サイバーセキュリティ部隊	・対応が必須	・サイバーセキュリティ法
	・国家安全保障の保護	・国家安全保障を脅かす恐れのあるデータ全般	・国家安全保障の保護を専門とする機関 ・政府機関	・速やかな対応が必須	・国家安全保障法
	・犯罪捜査	・証拠・資料・物品・電子データ	・訴訟手続を行う権限を有する機関	・対応が必須	・刑事訴訟法
	・監察・苦情・告発の解決、ならびに汚職対策	・監察内容に関連する情報	・監察決定者、監察団長、監察官等監察権限のある者	・対応が必須	・監査法
タイ	・特別事件※1 の捜査	・金融機関・政府機関・組織、国家機関・国営事業者・個人が保有する、犯罪に関連する帳簿・文書・証拠	・特別事件捜査官	・対応が必須	・特別事件捜査法
	・コンピューター犯罪の捜査	・暗号化されたものも含むコンピュータデータ、トラフィックデータ	・主管官	・要請を受けた日から 7 日以内、又は主管官が定める期間内での対応が必須	・コンピューター犯罪法

法域名	目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等
	・サイバー脅威が危機レベルに達している場合の予防等	・サイバー脅威に関連する情報	・国家安全保障会議の構成員	・遅滞のない対応が必須	・サイバーセキュリティ法
インドネシア	・法執行目的	・電子データ	・法により定められた権限を有する捜査官	・対応が必須	・電子システム及び電子取引の運用に関する規則

※1:特別事件とは、以下の 5 つの場合を指している

【特別事件捜査法 第 21 条】

1. 以下のいずれかの性質を有するもの

(a) 特別な調査、捜査、及び特別な証拠収集を必要とする複雑な刑事事件

(b) 公序良俗、国家安全保障、国際関係、又は国の経済もしくは財政に重大な影響を及ぼす、又は及ぼす可能性のある刑事事件

(c) 重大な国際犯罪である、又は組織犯罪グループによって犯された刑事事件

(d) 影響力のある人物が首謀者、扇動者、又は支援者である刑事事件

(e) 特別事件調査官でも特別事件担当官でもない行政官、又は上級警察官が、犯罪の合理的な証拠がある、又は容疑者・被告人である場合の刑事事件

2. (a)-(e)以外の刑事事件で合って、BSC がその現任の理事の 3 分の 2 以上の賛成により決議した場合

① オーストラリア

Privacy Act 1988 を対象とし、先述の 5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

APP（Australian Privacy Principles）の APP8.1 及び s 16C にて、越境移転に関する規制が定められている。APP とは、Privacy Act 1988 のために定められた 13 のプライバシー原則である。越境移転時は、下記のとおり APP の範囲内での合理的な措置と、事業体の責任が義務付けられている。

- 個人情報を開示する前に、APP に違反しないよう合理的な措置を講じること【APP8.1】
- APP に違反する海外の受領者の行為又は慣行に対して、事業体が責任を負うこと【s 16C】

なお、上記の合理的な措置とは、海外の受領者に対して、APP に従って個人情報を取り扱うことを義務付けるための強制力のある契約を締結することを指している。契約内容には、以下を含めることが推奨されている。

- 開示される個人情報の種類及び開示の目的
- 海外の受領者が、個人情報の収集、利用、開示、保管、破棄又は匿名化に関して、個人情報保護規則（APP）を遵守すること。また、海外の受領者が個人情報を開示する第三者（例えば、下請業者）とも同様の契約を締結すること
- プライバシーに関する苦情の処理プロセス
- 受領者は、データ侵害の疑いがある合理的な根拠がある場合に、オーストラリア側の事業者（APP エンティティ）に通知するためのメカニズムを含むデータ侵害対応計画を実施し、適切な是正措置（契約に基づいて取り扱われる個人情報の種類に基づく）を概説すること【APP 8.16】

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

APP 8.20 ～ 8.59 にて、越境移転規制における 7 つの例外条件が定められている。

① APP が情報を保護する方法と少なくとも実質的に類似した方法で情報を保護する効果を持つ法律、又は拘束力のあるスキームの対象者である上に、個人が法律又は拘束力のある制度による保護を強制するためのメカニズムにアクセスできること【APP 8.20】
② 規則で定められた国の法律の対象となる者、又は規則で定められた拘束力のある制度の参加者であり、国又は拘束力のある制度が条件付きで規定されている場合【APP 8.28】
③ 本人に明示的に通知された上で、本人の同意を得て、海外の受領者に個人情報を開示する場合【APP 8.31】
④ オーストラリアの法律又は裁判所/裁判所の命令によって、又はオーストラリアの法律又は裁判所/法廷命令に基づいて要求又は許可されている場合【APP 8.38】
⑤ 許容される一般的な状況が存在する場合【APP 8.41】
⑥ 情報共有に関する国際協定に基づいて要求又は許可された場合【APP 8.51】
⑦ 執行関連活動に基づく場合【APP 8.56】

①について、海外の受領者は、全体として、少なくとも APP が情報を保護する方法と実質的に同様の方法で情報を保護する効果を持つ法律又は拘束力のある制度の対象であり、かつ個人が法律又は拘束力のある制度による保護を強制するためのメカニズムにアクセスできる場合には、APP8.1 に従わずとも越境移転が認められている。「少なくとも APP が情報を保護する方法と実質的に同様の方法で情報を保護する効果を持つ法律又は拘束力のある制度」は、日本の『個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）』「規則第 16 条」の相当措置に値している。

②について、移転先がホワイトリストに定められた法域である場合、APP8.1 に従わずとも越境移転が認められている。ただし、本調査で把握している限り、2025 年 10 月時点でホワイトリストに定められた法域は存在しない。

③について、越境移転を行う際には、情報の取得事業者からデータ主体に対し、事前にリスクを通知する必要がある。越境移転先では、情報の取得事業者は Privacy Act 1988 の下で責任を負う必要がなくなること、一方のデータ主体は Privacy Act 1988 に基づく救済を求められなくなることがリスクとして挙げられる。越境移転先の法域では、APP の対象外となるためである。

なお、本人の「明示的な同意又は黙示的な同意」とは、以下の 4 つの要素から成り立っている。

- 個人は同意を与える前に十分な情報を得ている（この場合は「明示的に情報を得た」）
- 個人が自発的に同意を与える
- 同意は最新かつ具体的であり、
- 個人は同意を理解し、伝える能力を持っている。【APP 6.1】

④で想定されるユースケースとして、2006 年マネーロンダリング防止及びテロ資金対策法（連邦法）に基づき、オーストラリア側の事業者が外国政府に個人情報を開示する場合、又は、オーストラリア連邦警察法 1979（Cth）・刑事事件における相互援助法 1987（Cth）に基づき、海外の法執行機関等に個人情報を開示する場合等が挙げられる。

⑤において許容される一般的な状況とは、本項では以下の 5 つを指している【APP 8.42-8.50】

1. 生命、健康、又は安全に対する重大な脅威を軽減又は防止する場合
2. 違法行為又は重大な違法行為の疑いに関して適切な措置を講じる場合
3. 行方不明と報告された人物の特定に通ずる場合
4. 外交又は領事の機能又は活動に必要な場合
5. オーストラリア国外での特定の国防軍活動に必要な場合

⑥の国際協定には、国際法上拘束力のある文書（条約や協定等）だけでなく、国際法上拘束力のないその他の正式な文書（覚書や公式書簡交換等）も含まれている。これらに基づき、越境移転が要求又は許可された場合に、APP8.1 に従わずとも越境移転が認められている。

また、⑦では警察活動・犯罪捜査・公的収入の保護・罰金や制裁を科すための法律の執行を担当する連邦・州・準州の機関等が執行関連活動を行う際に、APP8.1 に従わずとも越境移転が認められている。

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

本調査で把握している限り、オーストラリア政府や監督機関が明示的に GCBPR を相当措置として認めた法令・発言等は見受けられない。ただし、以下の共通点から相当措置としてみなせる可能性が高い。

図表 39 APP と GCBPR における個人情報保護要件の対応

	APP の個人情報保護要件	GCBPR の 個人情報保護要件
通知	・ 事業者は APP 5 事項を個人に通知するか、個人がそれらの事項を認識していることを確認するために、合理的な措置を講じること【APP 5.1】	・ プライバシーポリシーを通じて収集の方法、利用目的等を開示すること ・ 収集時に本人に通知すること
収集制限	・ 組織は、その機能又は活動の 1 つ以上に合理的に必要な個人情報のみを要求し、収集すること【APP 3.2】 ・ 合法かつ公正な手段によってのみ収集すること【APP 3.5】	・ 必要な個人情報のみ収集すること ・ 公正かつ合法的に個人情報を収集すること
個人情報の利用	・ 当該情報が収集された特定の目的のためにのみ、当該情報を使用又は開示すること【APP 6.2】	・ 利用目的による制限 ・ 開示、移転の制限
選択	・ 収集、利用、開示に関して個人が個別に選択できる権利は定められていない ・ ただし、いずれも本人同意は必須	・ 収集、利用、開示に関して個人が選択できる仕組みを提供すること
個人情報の完全性	・ 利用又は開示する個人情報が、利用又は開示の目的に鑑み、正確、最新、完全かつ関連性があることを確保するために、合理的な措置を講じること【APP 10.2】	・ 利用目的に必要な限度で個人情報を正確かつ最新に保つこと

	APP の個人情報保護要件	GCBPR の 個人情報保護要件
	・ 保有する個人情報を、その保有目的に鑑み、正確性、最新性、完全性、関連性、及び誤解を招くものではないことを保証するために、合理的な措置を講じて訂正すること【APP 13.1-2】	・ 個人情報の訂正に関して、移転先等第三者に対する通知手段を有すること
安全管理	・ 保有する個人情報を不正使用、妨害、紛失、不正アクセス、改ざん、開示から保護するために、状況に応じて合理的な措置を講じること【APP 11】	・ 情報セキュリティポリシーの実装 ・ 物理的、技術的、組織的安全管理措置の実装
開示及び訂正	・ 当該個人からの要請に応じて、当該個人に対し当該情報へのアクセスを許可すること【APP 12.1】 ・ 個人情報の訂正又は個人情報に声明を関連付けるという個人の要求に適時に応じること【APP 13.5】	・ 個人からの、個人情報取扱有無の確認、個人情報への開示、個人情報訂正に関する請求に応答すること
アカウンタビリティ	・ 個人情報をオープンかつ透明な方法で管理することを確保すること【APP1.1】	・ 責任者たる従業員の任命 ・ 苦情の処理 ・ ガバメントアクセスに対応する仕組みを備えること ・ 処理者/委託先が本個人情報保護要件を遵守するよう管理すること

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

オーストラリアでは、My Health Records Act 2012 第 77 条にて、マイヘルスレコード及び関連情報の国外での保管・持ち出し・処理・取扱いが一切禁止されている。例外条件は定義されていない。

その他、2024 年 11 月に施行された「デジタル ID 法」では、草案にデジタル ID 制度のデータを国内のみで保存すること（データローカライゼーション）に関する規則があった。しかし、2024 年 10 月に草案から削除され、法令には含まれないこととなった。そのため、オーストラリアでデータローカライゼーションの規制があるのは、マイヘルスレコード及び関連情報のみである。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

オーストラリアでガバメントアクセスが認められているのは、①発信元・宛先・発信時間・位置情報等通話・通信の利用状況（Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015）、②暗号化された通信データ（Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018）の二つである。いずれもガバメントアクセスにあたり、裁判所の令状は不要である。

① Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 では、第 178-179 条で既存の情報・文書、第 180 条で未来の情報・文書に対するガバメントアクセスが定義されている。既存の情報・文書というのは、アクセスの認可を受ける前にやり取りされた情報のことである。犯罪捜査や行方不明者の捜索等において、過去の発信データ等を参照する場合が想定される。未来の情報・文書というのは、重大犯罪（少なくとも 3 年以上の懲役刑）の捜査において、犯人逮捕のために新たに発生する情報を監視する場合が想定されている。ただし、表に記載のとおり、ガバメントアクセスが可能なデータは発信元・宛先・発信時間・位置情報等であり、通話内容や Web の閲覧履歴を取得するものではない。また、裁判所の令状は不要であるが、認可担当官から認可を受ける必要がある。

② Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 は、犯罪捜査・外国刑法の執行支援・国家安全保障の保護を目的として、保安情報機構や海外秘密情報局、法執行機関等が通信事業者に協力を求める法令である。①とは異なり、通話内容や Web の閲覧履歴等も含めて確認できる。任意で要請される TAR と強制力のある TAN（※TCN：技術開発支援は割愛）が存在し、TAN が発せられた場合は強制的に対応する必要がある。ただし、①と同様に、あくまでも重大な犯罪捜査等の一部のユースケースに限った場合でのみ通知される。

図表 40 オーストラリアにおけるガバメントアクセス

目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等	条文
犯罪捜査	1. 加入者・アカウント・サービス・通信機器等に関する情報 2. 通信の発信元 3. 通信の宛先 4. 通信又はサービス接続の日付・時刻・継続時間 5. 通信又は関連サービスの種類（音声かSMSか等） 6. 通信に使用された機器又は回線の位置 7. 暗号化された通信データ	・ オーストラリア連邦警察又は州警察等 法執行機関	・ 1-6 のデータについては、通信事業者は最低 2 年間のデータ保持義務を負い、通知があれば対応が必須 ・ 7 のデータについて任意対応の TAR と強制力のある命令である TAN が存在し、TAN の通知があれば対応が必須	・ Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 ・ Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018	・ 第 178 条：既存の情報又は文書へのアクセスのための認可―刑法の執行 ・ 第 180 条：将来の情報又は文書へのアクセスのための認可 ・ 317G：技術的要請支援（TAR） ・ 317L：技術的支援通知（TAN）
公的歳入の保護	1. 加入者・アカウント・サービス・通信機器等に関する情報 2. 通信の発信元 3. 通信の宛先	・ オーストラリア連邦警察又は州警察等 法執行機関	・ 通信事業者は最低 2 年間のデータ保持義務を負い、通知があれば対応が必須	・ Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015	・ 第 178 条 A：既存の情報又は文書へのアクセスのための認可―行方不明者の捜索 ・ 第 179 条：既存の情報又は文書へのアクセス

目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等	条文
行方不明者の捜索	4. 通信又はサービス接続の日付・時刻・継続時間 5. 通信又は関連サービスの種類（音声かSMSか等） 6. 通信に使用された機器又は回線の位置				のための認可―金銭的罰則を課す法律の執行又は公的歳入の保護
外国刑法の執行支援	・ 暗号化された通信データ	・ 保安情報機構（ASIO） ・ 海外秘密情報局（ASIS） ・ 信号局（ASD） ・ オーストラリア連邦警察又は州警察等法執行機関	・ 任意対応の TAR と強制力のある命令である TAN が存在し、TAN の通知があれば対応が必須	・ Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018	・ 317G：技術的要請支援（TAR） ・ 317L：技術的支援通知（TAN）

② カナダ

Personal Information Protection and Electronic Documents Act (PIPEDA)を対象とし、先述の 5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、Personal Information Protection and Electronic Documents Act (PIPEDA)では、越境移転に限った規制は存在しない。ただし、越境移転に限らない個人情報の処理に関する義務として、PIPEDA 第 4 条第 1 項第 3 号では以下が規定されている。

【PIPEDA 第 4 条第 1 項第 3 号】
- 組織は、自らが保有又は管理する個人情報（処理のために第三者に移転された情報を含む）に対して責任を負うこと
- 組織は、第三者が情報を処理している間、契約又はその他の手段を用いて同等のレベルの保護を提供すること

なお、アルバータ州 PIPA やケベック州法等、州法単位では越境移転規制が定められている。

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

PIPEDA では越境移転規制が存在しないため、2、3 についても同様に存在しない。

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、国家単位でのデータローカライゼーションの規制は存在していない。

ただし、ノバスコシア州の Personal Information International Disclosure Protection Act, SNS 2006 では、公的機関の保管・管理下にある個人情報は国外での保管・アクセスが禁止されている。例外条件として以下が規定されている。

【PIIDPA 第 5 条】
(a) 情報の対象である個人が、その情報を特定し、規則で定められた方法で、カナダ国外でその情報が保管され、又はカナダ国外からアクセスされることに同意している場合
(b) この法律に基づいて認められた開示の目的でカナダ国外で保存又はアクセスされる場合
(c) 公的機関の長が(2)項に従ってカナダ国外での保管又はアクセスを許可している場合
(2) 公的機関の長は、その保管又は管理下にある個人情報を、当該公的機関の運営に必要な要件を満たすものであると長が判断した場合には、長が適切と考える制限又は条件を付して、カナダ国外で保管又はアクセスすることを許可することができる。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、自国のデータに対し、ガバメントアクセスが認められる規制・制度は存在していない。

ただし、外国のデータに対するガバメントアクセスを認めた法令として、Communications Security Establishment Act が挙げられる。カナダに安全・安心・繁栄をもたらすために、以下の 5 つの目的において、防衛情報や金融情報、犯罪情報等にアクセスすることが認められている。

① 外国諜報
➢ カナダ政府の情報収集優先事項を達成するために、秘密裏にグローバルな情報インフラにアクセスすること
② サイバーセキュリティ及び情報保証

- ➢ カナダ政府及び政府にとって重要であると指定された電子情報・情報インフラを保護するために、グローバルな情報インフラやその他情報源から、参考になる情報を取得・使用・分析すること

③ 防衛的サイバーオペレーション

- ➢ カナダ政府及び政府にとって重要であると指定された電子情報・情報インフラを保護するために、防衛対策を取ること

④ 積極的サイバーオペレーション

- ➢ カナダ政府及び政府にとって重要であると指定された電子情報・情報インフラを保護するために、外国の個人・国家・組織、又はテロ集団の能力・意図・活動を妨害すること

⑤ 技術・運用支援

- ➢ 法執行機関・カナダ軍・国防省に対し、技術・運用上の支援を提供すること

③ 韓国

Personal Information Protection Act (PIPA)を対象とし、先述の 5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル(法令、政省令、ガイドライン等)において、どのような内容が規定されているか

PIPA の第 28 条の 8 では、以下のとおり、原則として越境移転が禁止されている。

【第 28 条の 8】
(1) 個人情報取扱事業者は、個人情報の国外への提供(照会を含む)、委託処理、又は保管(以下この条において「移転(transfer)」という)を行ってはならない。

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

上記の越境移転規制の例外として、以下の 5 点が定められている。2023 年 9 月の法改正前は、データ主体の同意取得でのみ越境移転を認めていたが、法改正を受けて第 2～5 号までの条件が追加されている。

【第 28 条の 8 第 1 項】
1. データ主体から別途の同意を得た場合
2. 個人情報の越境移転に関する特別な規定が、法律・条約(大韓民国が締結国であるもの)又はその他の国際協定に存在する場合
3. 情報主体との契約を締結・履行するために個人情報の処理を委託し、かつその個人情報を保持することが必要な次の各場合
(a) 第 2 項各号に掲げる事項が第 30 条のプライバシーポリシーにおいて開示されている場合
(b) 第 2 項各号に掲げる事項が、大統領令で定める方法(電子メール等)によりデータ主体に通知されている場合

4. 個人情報の受領者が、第 32 条の 2 に基づく個人情報保護認証等、保護委員会が定めて公示した認証を取得し、次のすべての措置を講じた場合

(a) 個人情報の保護に必要な安全措置及び情報主体の権利を保障するために必要な措置

(b) 個人情報の移転先国において、認証事項を実施するために必要な措置

5. 保護委員会が、個人情報の移転先国又は国際機関の個人情報保護制度、情報主体の権利保障の範囲、救済手続等が、本法の下での個人情報保護水準と実質的に同等であると認める場合

第 1 項の「別途の同意」の定義は、第 22 条（同意の取得方法）にて定められている。包括同意ではなく、越境移転における個人情報の収集・利用目的等を明確に示した上で別途の同意を得る必要がある。

(1) 個人情報取扱者は、同意を求める事項をそれぞれ明確に区別して提示し、明確に認識できる方法で情報主体に提示し、その同意を取得しなければならない。この場合、個人情報取扱者は、次の各号のいずれかに該当する同意を要する事項を分類し、それぞれについて同意を得なければならない。

- 8.情報主体を保護するために、同意を要する事項を分類して同意を得ることが必要であると大統領令で定めるその他の場合

(2) 個人情報取扱者が第 1 項に基づいて書面（電子文書及び電子取引の基本法第 2 条第 1 号の電子文書を含む）によって同意を得る場合、個人情報取扱者は、個人情報の収集及び利用の目的、収集・利用される個人情報の項目等、大統領令で定める重要事項を明確に記載し、個人情報保護委員会の告示で定める方法に従って理解しやすい方法で明示しなければならない。

第 2 項各号とは、以下の 5 点を指している。上記例外条件の第 1 項第 1 号におけるデータ主体の同意を得る際、また第 3 号の契約を締結・履行するために個人情報の処理を委託し、かつその個人情報を保持する際に、以下の 5 点をデータ主体に開示又は通知することが求められている。

【第 28 条の 8 第 2 項】

1. 移転対象となる個人情報の詳細
2. 個人情報の移転先の国、移転日及び方法
3. 個人情報の受領者の名称（受領者が法人である場合は法人名及び連絡先）

4. 受領者による個人情報の利用目的及び保有・利用期間
5. 個人情報の移転を拒否する方法及び手続、その拒否による効果

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

先述のとおり、第 28 条の 8 第 1 項第 5 号にて、相当措置による例外が認められている。

5. 保護委員会が、個人情報の移転先国又は国際機関の個人情報保護制度、情報主体の権利保障の範囲、救済手続等が、本法の下での個人情報保護水準と実質的に同等であると認める場合（再掲）

ただし、本調査で把握している限り、韓国政府や監督機関が明示的に GCBPR を相当措置として認めた法令・発言等は見受けられない。

PIPA では、第 3 条に 8 つの情報保護原則が定められている。GCBPR が相当措置になりうるかを確認するため、以下表にて、PIPA の個人情報保護原則と GCBPR の個人情報保護要件を比較している。

PIPA の情報保護原則のうち、(1)収集制限、(2)利用制限、(3)個人情報の完全性、(4)安全管理、(5)アクセス請求権は、GCBPR の個人情報保護要件とも一致している。

しかし、(6)プライバシー侵害可能性の最小化、(7)匿名化・仮名化の努力義務、(8)義務及び責任の遵守・履行に関しては、GCBPR の個人情報保護要件だけではカバーし切れていない可能性がある。そのため、必ずしも GCBPR が相当措置となるとは限らない。

図表 41　PIPA の個人情報保護原則と GCBPR の個人情報保護要件の類似性

項目	類似性	PIPA の情報保護原則 【第 3 条】	GCBPR の個人情報保護要件 における類似する項目
(1) 収集制限	・ 一致する	・ 個人情報取扱事業者は、個人情報を処理する目的を明確に特定しなければならず、その目的のために必要な最小限の範囲で、合法的かつ公正に個人情報を収集しなければならない	[項目：収集制限] ・ 必要な個人情報のみ収集すること ・ 公正かつ合法的に個人情報を収集すること
(2) 利用制限	・ 一致する	・ 個人情報取扱事業者は、個人情報を処理目的のために必要な適切な方法で処理し、その目的を超えて利用してはならない	[項目：個人情報の利用] ・ 利用目的による制限 ・ 開示、移転の制限
(3) 個人情報の 完全性	・ 一致する	・ 個人情報取扱事業者は、個人情報を処理目的に関連して必要な範囲内で、正確・完全・最新の状態に保たなければならない	[項目：個人情報の完全性] ・ 利用目的に必要な限度で個人情報を正確かつ最新に保つこと ・ 個人情報の訂正に関して、移転先等第三者に対する通知手段を有すること
(4) 安全管理	・ 一致する	・ 個人情報取扱事業者は、処理方法や個人情報の種類等に応じて、情報主体の権利侵害の可能性及びそのリスクの重大性を考慮し、個人情報を安全に管理しなければならない	[項目：安全管理] ・ 情報セキュリティポリシーの実装 ・ 物理的、技術的、組織的安全管理措置の実装
(5) アクセス 請求権	・ 一致する	・ 個人情報取扱事業者は、 第 30 条に基づくプライバシーポリシー及び個人情報処理に関するその他の事項を公開し、情報主体に対し、自身の個人情報へのアクセス請求権等の権利を保障しなければならない	[項目：開示及び訂正] ・ 個人からの、個人情報取扱有無の確認、個人情報への開示、個人情報訂正に関する請求に応答すること

項目	類似性	PIPA の情報保護原則 【第 3 条】	GCBPR の個人情報保護要件 における類似する項目
(6) プライバシー侵害可能性の最小化	・ 類似性が低い	・ 個人情報取扱事業者は、情報主体のプライバシーを侵害する可能性を最小化する方法で個人情報を処理しなければならない	[項目：安全管理] ・ 情報セキュリティポリシーの実装 ・ 物理的、技術的、組織的安全管理措置の実装
(7) 匿名化・仮名化の努力義務	・ 類似性が低い	・ 個人情報の収集目的を、匿名化又は仮名化した情報の処理によっても達成できる場合、個人情報取扱事業者は、可能な場合には匿名化を通じて、匿名化で目的達成が不可能な場合には仮名化を通じて、個人情報を処理するよう努めなければならない	[項目：安全管理] ・ 情報セキュリティポリシーの実装 ・ 物理的、技術的、組織的安全管理措置の実装
(8) 義務及び責任の遵守・履行	・ 類似性が低い	・ 個人情報取扱事業者は、本法及び関連法令で定める義務及び責任を遵守・履行することにより、情報主体の信頼を得るよう努めなければならない	[項目：アカウンタビリティ] ・ 責任者たる従業員の任命 ・ 苦情の処理 ・ ガバメントアクセスに対応する仕組みを備えること ・ 処理者/委託先が本個人情報保護要件を遵守するよう管理すること

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

医療法の「電子義務記録の管理・保存に必要な施設と装備に関する基準」と、「金融会社の情報処理業務委託に関する規定」、及び「電子金融監督規定」にてデータローカライゼーションが義務付けられている。

<u>医療分野</u>

「電子義務記録の管理・保存に必要な施設と装備に関する基準」とは、医療法第 23 条第 2 項、同条第 4 項及び同法施行規則第 16 条により、医療に関連した電子義務記録を安全に管理・保存するための施設及び装備に関する基準の具体的な内容を定めることを目的とした基準である。

上記基準の別表「医療機関外の場所に電子医療記録を保管する際に必要な追加措置」では以下の記述がある。ただし、下記は電子医療記録システムの物理的な設置場所を定めるものであり、電子医療記録情報自体の越境移転を禁じる規則ではないことに留意が必要である。

【別表「医療機関外の場所に電子医療記録を保管する際に必要な追加措置」】 電子医療記録システム及びそのバックアップ装置の物理的な設置場所は、国内に限定する。

<u>金融分野</u>

「金融会社の情報処理業務委託に関する規定」では、固有識別符号（住民登録番号・パスポート番号・運転免許番号・外国人登録番号）の越境移転が禁じられている。

【第 5 条(特定情報の保護) 】 ①第 4 条により情報処理を委託する場合、金融会社は、各関連法令上の安全性確保措置を忠実に履行しなければならない。このとき個人顧客の固有識別情報は暗号化等の保護措置をしなければならず、特に国外に移転されないようにしなければならない。

また、「電子金融監督規定」では、クラウドコンピューティングサービスを利用して固有識別情報又は個人信用情報を処理する場合、その情報処理システムの物理的な設置場所は国内に限定すると定められている。

【第 14 条の 2(クラウドコンピューティングサービス利用手続等) 】

①金融会社又は電子金融業者は、「クラウドコンピューティングの発展及び利用者保護に関する法律」 第 2 条第 3 号によるクラウドコンピューティングサービスを利用しようとする場合、次の各号の手続を実施しなければならない。

(中略)

⑧第 1 項の手続きを経たクラウドコンピューティングサービス提供者の情報処理システムが位置する電算室については、第 11 条第 1 号及び第 2 号、第 15 条第 1 項第 5 号を適用しない。ただし、金融会社又は電子金融業者(電子金融取引の安全性及び信頼性に重大な影響を及ぼさない外国金融会社の国内支店、第 50 条の 2 による国外サイバーモールのための電子支払決済代行業者は除く)が固有識別情報又は個人信用情報を適用し、該当する場合情報処理システムを国内に設置しなければならない。

個人信用情報とは、「信用情報の利用及び保護に関する法律」において、以下 5 点と定められている。

【第 2 条第 1 項】

(a) 特定の信用情報の保有者を識別できる情報

(b) 信用情報の保有者の取引内容を把握できる情報

(c) 信用情報の保有者の信用度を判断できる情報

(d) 信用情報の保有者の信用取引能力を判断できる情報

(e) 前(a)から(d)に掲げる情報と類似するその他の情報

ただし、「電子金融監督規定」は医療分野と同様に、情報処理システムの物理的な設置場所を定めるものである。「金融会社の情報処理業務委託に関する規定」でデータローカライゼーションが義務付けられている固有識別符号とは異なり、個人信用情報自体の越境移転を禁じる規則ではないことに留意が必要である。また、クラウドコンピューティングサービスを利用していない場合には、上記規定が義務付けられることはない。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

韓国の通信秘密保護法では、第 13 条（犯罪捜査のための通信事実確認資料提供の手続）にて、法執行機関が捜査や刑の執行のために通信事実の確認が必要な場合、資料の閲覧・提出を要請できることが定められている。ただし、要請理由や当該加入者との関連性、必要な資料の範囲を記録した書面で、管轄地方裁判所又は支院の許可、すなわち個別の令状審査を受ける必要があるため、本調査では掲載しない。

④ メキシコ

The Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP)を対象とし、先述の 5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、The Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP)では、越境移転に限った規制は存在しない。ただし、越境移転に限らない個人情報の移転に関する義務として、第 35 条では以下が規定されている。

> 【第 35 条】
> 個人データの管理者（責任者）が、受託者以外の国内又は国外の第三者に個人データを移転しようとする場合、当該第三者に対してプライバシー通知及びデータ主体がその取扱いに同意した目的を知らせなければならない。データの取扱いは、プライバシー通知に定められた内容に従って行われなければならず、プライバシー通知には、データ主体がそのデータの移転を承諾するか否かを示す条項を含めなければならない。同様に、受領する第三者も、データを移転した責任者と同じ義務を負うものとする。

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

LFPDPPP では越境移転規制が存在しないため、2、3 についても同様に存在しない。

ただし、越境移転に限らない個人情報の移転に関する義務を定めた第 35 条の例外として、第 36 条では以下が定義されている。

【第 36 条】
I. メキシコが締結国である法律又は条約において定められている場合
II. 医療の予防又は診断、医療支援の提供、治療、又は医療サービスの管理のために必要な場合
III. 責任者の共通の支配下にある親会社、子会社、又は関連会社、あるいは同一グループに属し、同一のプロセス及び内部方針に基づいて運営されている会社に対して移転が行われる場合
IV. 責任者と第三者との間で、データ主体の利益のために締結された、又は締結される予定の契約に基づいて移転が必要な場合
V. 公共の利益の保護、又は司法の追及もしくは執行のために必要又は法的に要求される場合。
VI. 司法手続において権利の認識、行使又は防御のために必要な場合
VII. 責任者とデータ主体との間の法的関係の維持又は履行のために必要な場合

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、データローカライゼーションの規制は存在していない。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

国家安全保障法、刑事訴訟法、誘拐犯罪の防止及び処罰に関する一般法、人身取引犯罪の防止・処罰・撲滅及び被害者の保護・支援に関する一般法、組織犯罪対策連邦法、不正に設立された事業の防止及び識別のための連邦法、国家警備隊法では、通信や金融情報へのアクセスが認められている。ただし、いずれも令状審査を受ける必要があるため、本調査では掲載しない。

⑤ フィリピン

Data Privacy Act of 2012(DPA) 及びその施行規則にあたる Implementing Rules and Regulations of Republic Act No. 10173, Also Known as the “Data Privacy Act of 2012”(IRR)を対象とし、5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

DPA では、越境移転に特化した規制は設けられていない。ただし、国内外問わず第三者への処理の委託についての規則が定められている。

【DPA 第 21 条】*IRR では第 50 条が該当し、同様の内容を定められている。

- 個人情報管理者は、国内・国外を問わず第三者に処理を委託している場合を含め、自らが管理又は保管するすべての個人情報について責任を負う。なお、国外への移転については越境に関する取決め及び協力に従うことを前提とする。

a) 個人情報管理者は、第三者が情報を処理している間も、契約その他の合理的な手段を用いて、同等の保護水準を確保するものとする

b) 個人情報管理者は、組織を代表してこの法律を遵守する責任を負う個人（複数も含む）を指名しなければならない。当該指名された個人の氏名等は、データ主体からの請求に応じて開示されるものとする

また、フィリピンでは少なくとも 1,000 人以上の個人データを取り扱う場合、情報の処理システムに関する情報を個人情報保護委員会に届け出る必要がある。越境移転の計画についても、個人情報保護委員会への届け出の対象となり得ることが IRR 第 47 条(a)5 にて定められている。（下線部参照）

【IRR 第 46 条】

個人情報保護委員会は、DPA の管理と実施を統括する権限に基づき、個人情報管理者が法令上の義務を遵守することを確保するため、以下の事項を義務付ける

a) 国内で運用され、1,000 人以上の個人に関する機微なデータへのアクセス又は処理を伴うシステムについては登録しなければならない。登録対象には、政府機関と契約を締結する受託業者及びその要因の個人データ処理システムも含む ※(b),(c),(d)は省略

【IRR 第 47 条】
a) 登録内容には以下が含まれるものとする。
1. 個人情報管理者又は個人情報処理者、及びその代表者（いる場合）の氏名・住所・連絡先
2. 処理の目的、及び処理がアウトソーシング契約又は下請け契約に基づいて行われているかどうか
3. データ主体のカテゴリ、及びデータ主体に関連するデータ又はデータのカテゴリの説明
4. データが開示される可能性のある受信者又は受信者のカテゴリ
5. フィリピン国外への個人データの移転の提案 ※6-10 は省略

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

越境移転に特化した規制がないため、例外条件も設けられていない。ただし、DPA そのものの例外として以下の条件が定義されている。他法域の越境移転規制における例外条件と同様に、法執行活動等、公共機関の活動に必要とされる場合は DPA の制約を受けずに個人情報を取り扱うことができる。

【DPA 第 4 条】
(a) 政府機関の職員又は元職員に関するすべての情報で、その職務内容や職務に関連するもの
※(a)の詳細は中略
(b) 政府機関との契約に基づき業務に従事している、又は過去に従事していた個人に関する情報で、当該業務の内容、契約条件、及び業務遂行中に提供された個人の氏名を含むもの
(c) 政府機関が個人に対して付与する免許・許可等の金融上の裁量的利益に関する情報。個人の氏名及び当該利益の内容を含む

(d) 報道、芸術、文学、又は研究目的のために処理される個人データ
(e) 公共機関がその憲法上及び法令上定められた機能を果たすために必要な情報。これには、独立中央金融当局及び法執行・規制機関が個人データを処理して憲法上・法令上の義務を履行することも含む
(f) 独立中央金融当局又はフィリピン中央銀行の管轄下にある銀行及びその他の金融機関が、改正後の反資金洗浄法（共和国法第 9510 号）及びその他の関連法令（共和国法第 9160 号）を遵守するために必要な情報
(g) 外国の管轄区域の法律に従い、その管轄区域の居住者から収集された個人情報（該当するデータ保護法を含む）で、フィリピン国内で処理されているもの

また、先述の IRR 第 46 条で定められている個人情報保護委員会への届け出についても、同様に例外条件が設けられている。

【IRR 第 47 条】
・ 従業員 250 人未満の個人情報管理者又は個人情報処理者は、以下の場合を除き、(IRR 第 46 条が定める)登録を行う必要はない:
① データ主体の権利及び自由を侵害するリスクがある場合
② 処理が偶発的なものではない場合
③ 少なくとも 1,000 人の個人に関する機微な個人情報を取り扱う場合

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

越境移転に特化した規制・例外条件が存在しないため、GCBPR 等の認証が相当措置とみなせるかについての記載も公式には見当たらない。

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、個人に関わるデータを域内で保管することを義務付けるデータローカライゼーションの規定は存在しない。

5. **ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか**

ガバメントアクセスを認める規制・制度として、テロ対策のための通信・通話データの傍受や収集を認めるAnti-Terrorism Act of 2020等が存在するが、裁判所の令状審査が必要である。例外的に、税務調査における口座情報の調査に関わる以下の制度では、裁判所の令状なくガバメントアクセスが認められる。ただし、情報開示の目的は限定されており、外国税務当局からの要請に基づく場合は調査対象者への書面通知が義務付けられる等の汎用防止のための規則が設けられている。

図表 42 フィリピンにおけるガバメントアクセス

目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等	条文
税務調査（遺産相続額の調査・税の減額調査・外国税務当局からの要請）	銀行口座情報	・ 歳入庁	・ 罰則規定あり	・ Exchange of Information on Tax Matters Act of 2009	・ 第6条：税務当局による課税評価及び追加要件の設定権限

⑥ シンガポール

The Personal Data Protection Act 2012 (PDPA) 及びその施行規則にあたる Personal Data Protection Regulations 2021 (PDPR) を対象とし、5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル(法令、政省令、ガイドライン等)において、どのような内容が規定されているか

PDPA では、一定の要件を満たない限りはデータの越境移転ができないことが定められている

【PDPA 第 26 条】
1. 組織は、シンガポール国外の国又は地域にいかなる個人データも移転してはならない。ただし、当該移転される個人データに対し、本法による保護と同等の水準の保護が提供されることを確保するために、PDPA に基づき定められた要件に従う場合は、この限りでない

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

データの越境移転が可能となる例外条件については、PDPA と PDPR でそれぞれ定められている。

PDPA の第 26 条第 1 項では「本法による保護と同等の水準の保護が提供されること」、つまり相当措置が認められている。さらに、第 2 項～第 4 項では、事業者が個人情報保護委員会に個別に申請し、書面で許可を得た場合にデータの越境移転が認められると定められている。

【PDPA 第 26 条】
1. 組織は、シンガポール国外の国又は地域にいかなる個人データも移転してはならない。ただし、当該移転される個人データに対し、本法による保護と同等の水準の保護が提供されることを確保するために、PDPA に基づき定められた要件に従う場合は、この限りでない。(再掲)

2. 個人情報保護委員会は、どのような組織についても、組織からの申請に基づき、書面により通知することによって、当該組織による個人データの移転に関し、前項に基づき定められた要件の適用を免除することができる。
3. 前項の適用除外の条件は、
a. 個人情報保護委員会が書面で指定する条件を付して付与することができ、かつ
b. 官報に掲載することを要せず、委員会はいつでもこれを撤回することができる場合
4. 個人情報保護委員会は、本条に基づき課した条件を、いつでも追加、変更、又は解除することができる。

PDPR では、第 10 条で個人の同意等による例外条件、第 12 条で CBPR 等の認証による例外条件が定められている。第 12 条では、相当措置として APEC CBPR が認められている。

個人の同意等による例外条件

【PDPR 第 10 条第 2 項】
a) 当該個人が、移転先の国又は地域における受取者へ個人データを移転することに同意した場合
b) PDPA 第 15 条第 3～8 項に基づき、当該個人が、移転元組織によるその個人データの当該受領者への開示に同意したとみなされる場合
c) 当該個人データの受領者への移転が不可欠であり、その個人データが PDPA 附表の第一部又は 第二部第二項※に基づいて利用又は開示されるために必要であって、かつ移転元組織が、移転された個人データが受領者により他の目的で利用・開示されないよう合理的な措置を講じている場合
※PDPA 附表第一部：個人データの利用・収集・開示が個人の明確な利益や生命の保護等に必要であり、かつ当該個人の同意を取得できない場合を規定
※PDPA 附表第二部第二項：個人データの利用・収集・開示が国家の利益に資する場合を規定
d) 当該個人データが転送中のデータである場合
e) 当該個人データがシンガポール国内で一般に公開されている場合

第 2 項(a)で求められている「同意」とみなされない場合ついて同条文の第 3 項で以下のように定義されている。

【PDPR 第 10 条第 3 項】

a) 個人が同意を与える前に、当該個人の個人データが当該国又は地域へ移転される際の保護水準が、本法に基づく保護水準と同等である範囲について、書面による合理的な概要が提供されていなかった場合;

b) 当該移転を行う組織が、個人に製品又はサービスを提供する条件として当該個人からの同意を要求した場合。ただし、その移転が当該個人に製品又はサービスを提供する上で合理的に必要である場合を除きます。あるいは

c) 移転を行う組織が、移転に関する虚偽又は誤解を招く情報を提供したり、その他の欺瞞的又は誤解を招く手法を用いたりして、個人から当該移転に対する同意を取得した、又は取得しようとした場合。

認証に関わる例外条件

【PDPR 第 12 条】

1. シンガポール国外の国又は地域において、個人データの受領者が当該個人データが移転された国又は地域の法令に基づき付与又は承認された特定の認証を保持しているときは、受領者は PDPR 第 10 条 1 項の規定に基づき、転送された個人データに対して PDPR 第 10 条に定める保護水準と同様以上の保護を提供する法的拘束力のある義務を負うとみなされる。
2. PDPR において、「特定の認証」とは、個人データの受領者に関する以下の認証を意味する

a. 受領者がデータ仲介者である場合:APEC PRP 又は APEC CBPR

b. その他の場合:APEC CBPR

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置(相当措置)として認められているか

先述のとおり、PDPR 第 12 条にて、APEC CBPR が相当措置として認められている。

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、データローカライゼーションの規則は存在しておらず、PDPA 及び PDPR での越境移転規制のみが存在する。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

シンガポールでは、領域ごとに複数の法令でガバメントアクセスを根拠づける規定が存在する。以下では、令状審査なしでガバメントアクセスが認められる法令を掲載している。

図表 43 シンガポールにおけるガバメントアクセス

目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等	条文
捜査・調査・裁判等のため	・ 文書・物品 ・ 金融機関の顧客情報 ・ コンピューター内のデータ ・ 暗号化されたデータの復号鍵等	・ 警察	・ 同条に罰則規定あり	・ Criminal Procedure Code 2010(CPC) ・ ※通常は令状審査が必要だが、審査が遅れることで捜査に影響が出ると判断された場合は令状なしで捜査可能	・第 20 条:文書・物品の提出命令 ・第 39 条:コンピューターへのアクセス ・第 40 条:復号情報へのアクセス
OCHA 法の運用(特定のオンラインサービスの停止やアクセス遮断等)のため	・指定オンラインサービス等に関し、本法の運用に必要とされる一切の情報(保存場所の国内外を問わない)	・ 警察、及びその他機関の任命された担当官	・ 同法第 53 条に不遵守への罰則規定あり	・ Online Criminal Harms Act 2023(OCHA)	・ 第 47 条:OCHA の運用に必要な情報
オンライン上での犯罪捜査のため	・オンライン活動に関する情報・オンラインアカウント・捜査に資するその他の情報				・ 第 48 条:特定犯罪の実行を目的としたオンライン活動に関する情報

⑦ チャイニーズ・タイペイ

The Personal Data Protection Act 2012 (PDPA) を対象とし、5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル(法令、政省令、ガイドライン等)において、どのような内容が規定されているか

PDPA では、当該業界を担当する中央政府機関ごとに、越境移転に関する規制を設けられることが定められている。なお、中央政府機関とは、例えば通信領域の國家通訊傳播委員會や金融領域の金融監督管理委員會等が当てはまる。

【第 21 条】
政府以外の主体が以下のいずれかの状況下で個人データを国境を越えて移転する場合、当該業界を担当する中央政府機関は、その移転に対して制限を課すことができる:
1. 国家の重大な利益に関わる場合
2. 国際条約又は協定で規定されている場合
3. 個人データの受領国に適切な個人データ保護規制が存在せず、その結果データ主体の権利及び利益が侵害されるおそれがある場合
4. 個人データを第三国(地域)へ移転することが PDPA を回避するためである場合

PDPA の上記条文に基づいて、業界ごとに中国大陸への越境移転に制限が加えられている。

具体的には、①通信分野では通信・放送事業者が持つ個人データ、②社会福祉分野では社会福祉事務所の支援対象者の個人データ、③職業紹介・求人分野では求職者や求人事業者の個人データを中国本土に移転することが禁じられている。

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

越境移転規制の例外条件は存在していない。ただし、第 21 条に記載されている 4 つの条件（1.国家の重大な利益に関わる場合、2.国際条約又は協定で規定されている場合、3.個人データの受領国に適切な個人データ保護規制が存在せず、その結果データ主体の権利及び利益が侵害されるおそれがある場合、4.個人データを第三国（地域）へ移転することが PDPA を回避するためである場合）に当てはまらない場合は、越境移転規制自体が課されないことに留意が必要である。

また、PDPA そのものの例外条件として、以下が定められている。

【第 51 条】
PDPA の適用が除外される場合は以下のとおり:
1. 個人が自身の個人的又は家庭内の活動目的のみで個人データを収集、処理、又は使用する場合
2. 音声・映像データが公共の場や公共の活動において収集、処理、又は使用される場合であって、他の個人データと関連付けられていない場合

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

上記のとおり、越境移転の例外条件に相当措置は存在しない。

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

データローカライゼーションは、医療分野と金融分野でクラウドサービスを利用する際の規定が定められている。

医療分野

チャイニーズ・タイペイでは、医療法第 69 条において、紙の書面の代わりに電子カルテによって医療記録を保存することが認められている。同条文基づいて定められた「医療機関の電子病歴の作成及び管理に関する規則」では、第 8 条第 2 項において、データの収集や処理、利用等にクラウドサービスを利用する場合には、データの保存場所が国内（チャイニーズ・タイペイ内）に設置することが求められている。

ただし、同項に医療法の主管機関にあたる衛生福利部（MOHW）の認可する場合には例外が認められることも定められている。

【医療機関の電子病歴の作成及び管理に関する規則 第 8 条第 2 項】
前項のクラウドサービスにおけるデータ保存場所は、国内に設置しなければならない。ただし、特別な事情がある場合で、中央主管機関の承認を得た場合はこの限りではない。

金融分野

金融監督管理委員會が定めた省令において、金融機関がクラウドサービスを利用する際のデータの保管場所について、一部の重要な顧客データは現属として国内に保存する義務が定められている。

【金融機関が業務を第三者に委託する際の内部管理体制及び手続に関する規則 第 8 条第 2 項】
6. クラウドサービス事業者に委託する顧客データ及びその保管場所については、以下の規定を遵守しなければならない。
(1) 金融機関は、自らが指定するデータ処理及び保管場所に対する権利を保持しなければならない。
(2) 国外の現地データ保護規制は、国内の要求水準を下回ってはならない。
(3) 重要な消費者向け金融業務情報システムに関連する顧客データの保管場所は、原則として国内に設置しなければならない。国外に設置する場合、主管当局の承認がある場合を除き、重要な顧客データは国内にバックアップを保管しなければならない。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

PDPA 第 20 条において、法律よって明示的に要求されている場合、又は公共の利益の保護を目的とする場合には、本人同意なく政府以外の機関が個人データを利用し得ることが定められている。ガバメントアクセスは、以下のとおり定められている。個別の令状審査が不要な場合のみを挙げた。

図表 44 チャイニーズ・タイペイにおけるガバメントアクセス

目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等	条文
銀行及びその顧客の業務・財務等の調査	貸借対照表、財産目録、その他関連書類	・ 金融監督当局	・ 同法に罰則規定あり	・ The Banking Act of The Republic of China	・ 第 45 条：銀行の秘密保持とその例外 ・ 第 48 条：金融監督当局による調査権限
国家安全保障	外国勢力又はその代理人による通信内容	・ 国家安全局	・ 同法第 14 条で ISP の協力義務が規定	・ The Communication Security and Surveillance Act（CSSA）	・ 第 7 条
犯罪捜査及び証拠収集	重大犯罪の捜査に必要な範囲での通信記録又はネットワークトラフィック記録	・ 検察官 ・ 司法警察機関			・ 第 11 条第 1 項

⑧ アメリカ

「懸念国による大量の機微個人データ及びアメリカ政府関連データへのアクセスの防止に関する大統領令（EO14117）」及び当該大統領令を受けて制定された米司法省最終規則「28 C.F.R. Part 202（Data Security Program）」を対象とし、5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

従来、アメリカの連邦法には越境移転規制は存在しなかったが、2024 年 2 月に署名された大統領令で懸念国へのデータ移転に関する制限が設けられることとなった。ただし、移転が規制されるのは、懸念国に対する「大量の機密個人データ」又は「アメリカ政府関連データ」の移転時のみである。

【懸念国による大量の機微個人データ及びアメリカ政府関連データへのアクセスの防止に関する大統領令（EO14117）】
第 2 節 禁止・制限対象取引について
(a) 本命令で規定する国家緊急事態に対処するため、司法長官は、国土安全保障長官と連携し、関係機関の長と協議した上で、パブリックコメント手続きを経て、外国又はその国民が何らかの利害関係を有する財産（取引）について、アメリカ人が以下の行為を行うことを禁止又はその他制限する規則を制定する:
(i) 本条に基づき司法長官が発出する規則でさらに定義される「大量の機密個人データ」又は「アメリカ政府関連データ」を取り扱う取引である場合;
(ii) 本条に基づき司法長官が発出した規則において、当該取引がアメリカの国家安全保障に対して容認できないリスクをもたらすと判断された取引類型に属するものであること。具体的には、当該取引を通じて懸念国又は対象人物が、本命令で記載された国家緊急事態に寄与する形で、大量の機密個人データやアメリカ政府関連データにアクセスすることが可能となるもの。
((iii) 以下略)

越境移転規制の具体的な内容は、当該大統領令を受けて制定された米司法省最終規則「28 C.F.R. Part 202（Data Security Program）」で定められている。同規則では、サブパート F でデータ移転が制限される懸念国として中国、キューバ、イラン、北朝鮮、ロシア、ベネズエラが挙げられている。

【28 C.F.R. Part 202 第 601 条 懸念国の決定】

(a) 懸念国

本命令及び本節の目的に限り、司法長官は国務長官及び商務長官の同意を得て、次の外国政府が「アメリカの国家安全保障」又は「アメリカ人の安全」に著しく不利益を及ぼす長期的又は重大な行為の実績を有し、かつ、政府関連データ又はアメリカ人の機微な個人データの大量データを悪用する重大なリスクをもたらすと判断した。

(1) 中国
(2) キューバ
(3) イラン
(4) 北朝鮮
(5) ロシア
(6) ベネズエラ

上記の懸念国に対する移転が規制されている「大量の機密個人データ」の基準は、28 C.F.R. Part 202 第 205 条にて定められている。なお、同じく移転が規制される「アメリカ政府関連データ」に関しては、取引される量を問わず、懸念国への移転が禁じられている。

【28 C.F.R. Part 202 第 205 条 大量（Bulk）】

「バルク（bulk）」とは、過去 12 か月間のいずれかの時点で、以下の閾値（※下記図表 46 参照）に達するか、又はそれを超える機微個人データの量を意味する。

これは、単一の「該当データ取引」による場合、又は同一のアメリカ人及び同一の外国人又は該当者を含む複数の該当データ取引を合算した場合のいずれでもよい。

図表 45 大量のアメリカ人の機密個人データに該当するデータ

カテゴリ	定義・例	閾値
(a)ヒト・オミックスデータ、又はヒトゲノムデータ	ゲノミクスデータ、プロテオミクスデータ、メタボロミクスデータ等	1,000 人以上（ヒトゲノムデータの場合は 100 人以上）のアメリカ人
(b)生体識別子	顔画像、声紋及び声のパターン、網膜及び虹彩スキャン、掌紋及び指紋、歩容、キーストロークパターン	1,000 人以上のアメリカ人
(c)正確な位置情報データ	リアルタイム又は過去のデータであって、個人又はデバイスの物理的位置を 1,000 メートル以内の精度で特定できるもの	1,000 台以上のアメリカのデバイス
(d)個人健康データ	身体的測定及び健康属性、社会的・心理的・行動的・医学的な診断・介入・治療の履歴、運動習慣記録、予防接種データ等	10,000 人以上のアメリカ人
(e)個人財務データ	購入及び支払履歴等、個人のクレジットカード、チャージカード、デビットカード、又は銀行口座に関するデータ	10,000 人以上のアメリカ人
(f)特定の個人識別子	社会保障番号、パスポート番号、口座番号、氏名、連絡先データ、IP アドレスを組み合わせたもの	100,000 人以上のアメリカ人
(g)結合データ	上記(a)～(f)に掲げる複数のカテゴリを含むデータ群、又は(a)～(e)のいずれかのカテゴリに関連づけられた特定識別子を含むデータ群であって、その中のいずれかのデータ種別が、そのカテゴリで定められた最も少ないアメリカ人又はアメリカデバイスの閾値を、合算して満たす場合をいう。	

「対象データ取引」「データ仲介」ついては、サブパートBで以下のとおり定義されている。

【28 C.F.R. Part 202 第210条 対象データ取引】
「対象データ取引」とは、懸念国又は対象人物による政府関連データ又はアメリカの機密個人データの一括取得を伴うあらゆる取引を指し、以下の要素を含む
(1) データ仲介業務
(2) ベンダー契約
(3) 雇用契約
(4) 投資契約
【28 C.F.R. Part 202 第214条 データ仲介】
「データ仲介」とは、データの販売、データへのアクセス権のライセンス付与、その他これに類する商取引(ただし、雇用契約・投資契約・ベンダー契約を除く)であって、ある者(「提供者」)から別の者(「受領者」)へデータを移転する行為をいう。
この場合、受領者は、当該収集又は処理されたデータに結び付けられている、又は結び付け可能な個人から、当該データを直接収集又は処理していないことを要する。

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

大統領令(EO14117)を受けた司法省最終規則においては、以下の活動に伴うデータ取引は、越境移転規制(28 C.F.R. Part 202全体)の対象外とされている。

- 個人間通信(第501条)
- 情報あるいは情報資料(第502条)
- 渡航(第503条)

ここで、第 502 条の情報又は情報資料とは、サブパート B で以下のように定義されている。

【28 C.F.R. Part 202 第 226 条】
「情報又は情報資料」は、表現的な内容に限定され、出版物、映画、ポスター、レコード、写真、マイクロフィルム、マイクロフィッシュ、テープ、コンパクトディスク、CD-ROM、美術品、及びニュースワイヤーフィード等を包含する。 技術的、機能的、又はその他の非表現的なデータは含まれない。

また、以下の活動に伴うデータ取引は、越境移転規制におけるサブパート C、D、J、K（ただし第 1102 条・第 1104 条を除く）の対象外とされている。なお、サブパート C において、懸念国に対する「大量の機密個人データ」又は「アメリカ政府関連データ」の移転が禁止されているため、サブパート C の対象外である以下の活動は、越境移転規制において、例外的に移転が許される条件としてみなせる。

- アメリカ政府の公的業務に関する取引（第 504 条）
- 金融サービス（第 505 条）
- 事業者グループ間取引（第 506 条）
- 連邦法又は国際協定により義務付けられている、又は許可されている取引、又は連邦法の遵守に必要な取引（第 507 条）
- CFIUS の審査対象となる投資契約（第 508 条）
  - CFIUS とは、外国人・外国法人等がアメリカ事業者又はアメリカ内事業に関与する取引のこと
- 電気通信サービス（第 509 条）
- 医薬品、生物学的製剤、及び医療機器の承認に関する規定（第 510 条）
- その他の臨床試験及び市販後調査データ（第 511 条）

さらに、サブパート H では、法務省が制限された取引を例外的に許可するためのライセンスを発行できることが定められている。汎用的に許可される一般ライセンス（第 801 条）と、一般ライセンス外の個別事象を許可する個別ライセンス（第 802 条）が存在する。

【28 C.F.R. Part 202 第 801 条 一般ライセンス】

a) 一般的な手続の流れ

司法省は、適切と認める場合には、本パートにおける禁止又は制限の対象となる取引について、適切な条件の下でこれを認可する一般許可を発行することができる。一般許可を発行するか否かを判断するにあたり、司法長官は、連邦のいずれの省庁からのものか、その他のいかなる情報源からのものかを問わず、機密指定の有無にかかわらず、司法長官が関連し適切と認めるいかなる情報又は資料も考慮することができる。

b) 個別ライセンスとの関係

司法省の方針として、一般ライセンスの規定が適用される取引については、それを認める個別許可の申請は許可しない。

c) 報告

特定の一般ライセンスの適用を受ける者は、当該一般ライセンス、当パート又は当該命令に定められた指示に従って、報告書や申立書の提出を求められる場合がある。そのような報告書又は申立書において要求されるすべての情報を期限内に提出しない場合、当該一般ライセンスにより本来与えられていた認可が無効となり、適用される禁止規定に対する違反（の外形）を構成しうるため、執行措置の対象となりうる。

【28 C.F.R. Part 202 第 802 条 個別ライセンス】

a) 一般的な手続の流れ

本パート又は当該命令により禁止又は制限の対象となる取引で、当パート又は一般ライセンスの下で他に許容されていないものは、適切な条件の下で、個別ライセンスによってのみ許容され得る。

b) 個別ライセンスの申請内容

個別許可の申請には、少なくとも以下の要件を含む、当該取引の性質に関する記述を含めなければならない。

1. 当該取引に関与する政府関連データ又はアメリカ人の大量の機微個人データの種類及び量
2. 取引当事者の身元（法人については所有関係、個人については国籍又は主たる居住地を含む）
3. データの最終用途及びデータ移転の方法
4. 司法長官が要求し得るその他一切の情報

（以下略）

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

本調査で把握している限り、越境移転の例外として、GCBPR 以外の認証制度も含め、相当措置を認めた法令や発言等は存在しない。

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

連邦レベルの規則でデータローカライゼーションを定めた規則として、内国歳入法ガイドラインが存在する。

内国歳入法（IRC, Internal Revenue Code）では、第 6103 条において、納税申告書及び申告情報は秘密であり、法が明示的に許す場合を除き開示してはならないと定められている。また、連邦・州・地方機関や請負業者が取得した財務取引情報（FTI）の保護措置も規定されている。

この第 6103 条の規定は、ガイドラインで具体化され、その中にデータローカライゼーションに関わる規定が含まれる。クラウド環境で財務取引情報（FTI）を受領・処理・保存・アクセス・保護・送信する場合は、保存場所を国内に限定することが求められている。

【内国歳入法ガイドライン 2.E.6.1. クラウドコンピューティング】

- クラウド環境で財務取引情報（FTI）を受領・処理・保存・アクセス・保護・送信する場合には、事前に安全保護局への通知を要する。
- 当該通知の趣旨は、機関に対して以下を求めるものである。
  - FTI が国内に留まることを保障するため、FTI が処理される物理的所在地を文書化すること。
  - 安全保護局がクラウド・サービス・プロバイダ（CSP）施設の物理的セキュリティを評価する責任を負わないよう、当該 CSP の FedRAMP 認可を文書化すること。
  - 暗号化をどのように用いて、 CSP 従業員への不正開示を防止するかを説明すること。
  - 機関が管理するすべてのセキュリティ及びプライバシー管理策を文書化すること。

・ 機関が、CSP によるデータへの論理的アクセスを防止していることを立証できない場合、受託事業者又は下請受託者への開示に関する通知を提出しなければならない。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

アメリカでは合衆国憲法修正第 4 条で捜索・逮捕・押収にあたっての令状主義が定められており、ガバメントアクセスについても令状主義が基本である。例として、通話等のリアルタイム傍受や記録された情報の収集は通信傍受法（Wiretap Act）及び 1986 年電子通信プライバシー法（Electronic Communications Privacy Act, ECPA）により裁判所の令状が必要なことが定められている。

一方で、加入者情報や一部メタデータといった通信の内容に踏み込まない情報の傍受は、ECPA の保存通信法（Stored Communications Act, SCA）やペンレジスター・トラップ＆トレース法に基づき、大陪審・行政サブポエナのような令状取得よりも簡易的な手続きが用意されている。

以下には裁判所の令状発行やそれに類する手続きが不要なガバメントアクセスの制度を挙げる。

図表 46 アメリカにおけるガバメントアクセス

目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等	条文
外国勢力に限定した外国情報の収集（アメリカ人の通信は対象外）	外国勢力間の通信内容／外国勢力管理施設からの技術情報	・大統領（司法長官を通した認証が必要）	・事業者は指示に従う義務がある（秘密保持・補償規定）	・対外諜報活動監視法（Foreign Intelligence Surveillance Act of 1978 and Amendments(FISA)）	・50 U.S.C. §1802：裁判所命令を必要としない電子監視の許可；司法長官による認証；議会委員会への報告；封印による送付；通信事業者の義務と報酬；申請手続き；裁判所の管轄権
国家安全保障（対外諜報目的）	加入者情報、通話料金明細、電子通信取引記録	・FBI	・不履行、虚偽回答、守秘義務それぞれに対する罰則規定がある	・保管通信法（Stored Communications Act, SCA）	・18 U.S.C. §2709：電話料金記録及び取引記録への防諜アクセス（アメリカ愛国者法によって大幅に拡張・改正）
被害組織の同意に基づき、コンピューターへの侵入者の通信を傍受	侵入者の通信内容	・法執行機関	・法執行機関による通信傍受	・連邦盗聴法（Federal Wiretap Act）	・18 U.S.C. §2511：有線通信、口頭通信、又は電子通信の傍受及び開示の禁止（アメリカ愛国者法によって追加された条文）
マネーロンダリング・テロ資金等対策	CTR：$10,000 超の現金取引の報告書 SAR：疑わしい取引の報告書及び付随情報	・財務省	・金融機関に提出義務あり	・銀行秘密法（Currency and Foreign Transactions Reporting Act of 1970 (Bank Secrecy Act)）	・31 U.S.C. §5313：国内硬貨及び通貨取引に関する報告義務 ・31 U.S.C. §5318：遵守義務、適用除外、及び召喚権について

⑨ ドバイ国際金融センター（DIFC）

DIFC Law No. 5/ of 2020 on the Data Protection を対象とし、先述の 5 つの調査項目について調査を行った。

1. 法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

DIFC Law No. 5/ of 2020 on the Data Protection では、第 26 条及び第 27 条にて越境移転に関する規制が定められている。適切な保護水準が確保されていると認められる第三国又は国際機関への移転か、第 27 条第 3 項以降に定められている例外条件に当てはまる場合のみ、越境移転が認められている。

【第 26 条　適切な保護水準下にある DIFC 外への個人データの転送】

1. DIFC（ドバイ国際金融センター）から第三国又は国際機関への個人データの移転を伴う個人データの処理は、次のいずれかの場合にのみ行うことができる。

(a) 当該個人データに対して、適用法により適切な保護水準が確保されている場合
（第 26 条第 2 項及び第 3 項に定めるとおり。個人データのさらなる移転に関する保護を含む）

(b) 第 27 条に従って実施される場合

2. 第 26 条第 1 項の目的のために、コミッショナー（Commissioner）は、随時、第三国、特定の地域、当該第三国の一つ又は複数の特定部門、又は国際機関が適切なデータ保護水準を確保しているかを判断することができる。その際、次の要素を考慮するものとする。

(a) 法の支配、個人の権利に対する一般的な尊重、及び個人が行政的又は司法的救済を通じて権利を行使できる能力

(b) 公的機関による個人データへのアクセスの程度

(c) 実効的なデータ保護法の存在（第三国又は国際機関への個人データのさらなる移転に関する規定を含む）

(d) 十分な執行権限を有する独立した適格なデータ保護又は類似の監督当局の存在及び機能

(e) 当該第三国又は国際機関を拘束する国際的な約束及び条約、ならびにその多国間又は地域機構への加盟

3. コミッショナーは、他の適格なデータ保護当局による適正性決定に基づき、前記第 2 項(a)～(e)に示された要素が考慮されている場合に限り、任意で第三国、特定地域、部門、又は国際機関が適切なデータ保護水準を確保していると判断することができる。

（第 4 項以降は中略）

【第 27 条 適切な保護水準下にない DIFC 外への個人データの転送】

1. 第三国又は国際機関への個人データの移転、又は一連の移転は、次の条件のいずれかを満たす場合にのみ行うことができる。

(a) 当該管理者又は処理者が適切な保護措置（第 27 条第 2 項で説明される）を講じており、かつデータ主体の権利行使及び法的救済手段が実効的に利用可能であること

(b) 第 27 条第 3 項に定められる特定の例外のいずれかが適用されること

(c) 第 27 条第 4 項に定められる限定的な状況に該当すること

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

上記の越境移転規制の例外として、第 27 条第 3 項では以下の 11 条件が定められている。明示的な同意に基づく場合や法令・裁判所命令に基づく場合、契約履行のために必要な場合、人々の生命・健康・安全等に関わる場合、公共機関が法令上定められた機能を果たすために必要な場合といった、他法域でも一般的な条件のほか、(h)一般に公開されることを目的とした登録簿から行われる場合や、(j)移転が国際金融市場で認められる管理者の正当な利益を維持するために必要である場合といった、他法域にない条件も存在している。

【第 27 条 適切な保護水準下にない DIFC 外への個人データの転送】

3. 第 27 条第 1 項(b)で言及される例外は次のとおりとする。

(a) データ主体が、適正性決定又は適切な保護措置が存在しないことによる潜在的リスクについて説明を受けたうえで、明示的に移転に同意した場合

(b) 移転が、データ主体と管理者との間の契約の履行、又はデータ主体の要請に応じた契約締結前の措置の実施に必要である場合

(c) 移転が、管理者と第三者との間の契約の締結又は履行に必要であり、それがデータ主体の利益のためである場合
(d) 移転が、重大な公共の利益の理由により必要である場合
(e) 移転が、DIFC 又はその機関の利益において、職務を適正に遂行するために必要又は法的に求められる場合
(f) 移転が、法的請求の確立・行使・防御のために必要である場合
(g) 移転が、データ主体又は他の者の生命に関わる利益を保護するために必要であり、かつデータ主体が物理的又は法的に同意を与えられない場合
(h) 移転が、一般に公開されることを目的とした登録簿から行われ、かつ次の条件を満たす場合:
(i) 公衆全体、又は正当な関心を有する者によって閲覧できる
(ii) 適用法及びデータ最小化の原則(第 9 条第 1 項(f))に従っている
(i) 第 28 条に従い、次のいずれかに該当する場合:
(i) 管理者が従うべき適用法上の義務を履行するために必要
(ii) 規制当局、警察、その他の政府機関又は主管当局の合理的な要請に基づいて行われる
(j) 国際的金融基準に基づき、移転が国際金融市場で認められる管理者の正当な利益を維持するために必要である場合。ただし、その利益がデータ主体の正当な利益によって上回らないこと
(k) 移転が、マネーロンダリング防止(AML)又はテロ資金供与防止(CFT)の義務を遵守するため、又は犯罪の防止・検出のために必要である場合

さらに、第 27 条第 4 項では、(a)～(d)の全ての条件を満たす場合に限り、コミッショナーへの報告によって越境移転が認められると定められている。

4. 第 27 条第 1 項～第 3 項、又は第 26 条のいずれの規定にも基づくことができない場合でも、以下の条件を全て満たすときに限り、第三国又は国際機関への移転を行うことができる
(a) 移転が繰り返し行われるものではないこと

(b) 限られた数のデータ主体に関するものであること
(c) 移転が、データ主体の利益又は権利によって覆されない、管理者の強く正当な利益を目的とする場合であること
(d) 管理者が、移転に関連するすべての状況について文書による評価を完了し、その評価に基づいて個人データの保護に関する適切な保護措置を提供したこと
5. 管理者は、第 27 条第 4 項に基づいて移転を行った場合、コミッショナーに報告しなければならない。さらに、第 29 条又は第 30 条に定める情報を提供するとともに、データ主体に対し移転及びその「強く正当な利益」について通知しなければならない

なお、第 27 条第 3 項(a)における「明示的な同意」の条件は、第 12 条にて定義されている。

【第 12 条 同意】
1. 明確な肯定的行為によって自由に与えられ、同意の意思が曖昧でない形で示されなければならない
2. その同意が自由意思により与えられたものであることを証明できなければならない
3. 処理が複数の目的を対象とする場合、管理者は目的ごとに区別可能な形で同意を取得しなければならない
4. 個人データ処理に関する同意の要請は、他の事項と明確に区別可能な形で、理解しやすく、アクセスしやすい形式で、平易で明瞭な言葉を用いて提示しなければならない（原文から一部抜粋）

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

第 26 条及び第 27 条第 1 項(a)の「適切な保護水準」とは、第 27 条第 2 項において、以下のとおり定義されている。下線部：(e)第 50 条に基づき承認された認証メカニズムには、GCBPR が認められている[35]。

【第 27 条 適切な保護水準下にない DIFC 外への個人データの転送】
2. 第 27 条第 1 項(a)にいう「適切な保護措置」は、次のいずれかによって提供されるものとする。

[35] DIFC プレスリリース「Global CBPR Forum Endorses DIFC for Recognition as an Associate Member（2024/08/27）
https://www.difc.com/whats-on/news/global-cbpr-forum-endorses-difc-for-recognition-as-an-associate-member

(a) 公的機関間の法的拘束力を有する文書
(b) 拘束的事業者準則（Binding Corporate Rules, BCRs）（第 27 条第 6 項の条件に従う）
(c) コミッショナーが規則に基づいて採択した標準データ保護条項
(d) 第 48 条に基づき承認された行動規範であり、かつ第三国又は国際機関内の管理者又は処理者がデータ主体の権利に関する適切な保護措置を適用することを法的拘束力のある形で約束する場合
(e) 第 50 条に基づき承認された認証メカニズムであり、かつ第三国又は国際機関内の管理者又は処理者が、データ主体の権利に関する適切な保護措置を適用することを法的拘束力のある形で約束する場合

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、データローカライゼーションの規制は存在していない。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、DIFC においてガバメントアクセスが認められる規制は存在していない。ただし、UAE 単位では、マネーロンダリング、テロリズムへの資金供与及び違法組織への資金供与対策に関する連邦法（AML 法）が存在している。

⑩　イギリス

越境移転に関する規律は、UK General Data Protection Regulation（UK GDPR）と Data Protection Act 2018（DPA 2018）に定められている。ただし、DPA 2018 は警察・検察による法執行目的や情報機関による処理に伴う越境移転といった特定のケースを対象とする。事業者の通常業務における事業者内・事業者間のデータ移転は、原則として UK GDPR に基づくため、以下では UK GDPR を対象とし、先述の 5 つの調査項目について調査を行った。

1.　法令上越境移転に関する規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

まず UK GDPR では、第 5 章で包括的に個人データの越境移転について述べられており、同法第 44A 条において、特定の条件を満たす場合にのみ越境移転が可能なことが定められている。

【UK GDPR 第 44A 条：移転に関する一般原則】
1.　管理者又は処理者は、次の場合に限り、個人データを第三国又は国際機関へ移転することができる。
(a)　第 2 項の条件が満たされること。
(b)　当該移転が本規則の他の規定に適合して行われること。
2.　次のいずれかに該当する場合、第 1 項の条件は満たされる。
(a)　当該移転が、移転時に効力を有する第 45A 条に基づく規則により承認されていること。
(b)　当該移転が、適切な保護措置（第 46 条参照）の適用を受けて行われること。
(c)　当該移転が、特定状況のための例外（第 49 条参照）に依拠して行われること。
3.　当該移転が第 49A 条に基づく制限に違反する場合、又はその限度において、第 2 項(b)　又は(c)に依拠して移転を行うことはできない。

2. 越境移転規制において、例外的に移転が許される条件はあるか。例外条件がある場合、どのような内容が規定されているか

UK GDPR 第 44A 条では、個人データの越境移転が認められるための条件として、①規則による承認（第 45A 条）、②適切な保護措置が存在すること（第 46 条）、③特定の例外条件を満たすこと（第 49 条）が挙げられている。以下にそれぞれの具体的な内容を記す。

第 45A 条では、以下のように国務長官が定める規則により個人データの越境移転が承認されることが定められている。

【UK GDPR 第 45A 条 規則によって承認された移転】

1. 第 44A 条の目的のため、国務長官は規則により、個人データの移転先として次のいずれかを承認することができる。
   (a) 第三国、又は
   (b) 国際機関
2. 国務長官は、当該移転に関してデータ保護テストが満たされると判断する場合に限り、本条に基づく規則を制定して第三国又は国際機関への移転を承認することができる（第 45B 条参照）。

（以下省略）

国務長官が越境移転を承認する条件として、第 45B 条に定められたデータ保護テストをクリアすることが求められる。

【UK GDPR 第 45B 条 データ保護テスト】

1. 第 45A 条の目的のため、個人データを第三国又は国際機関へ移転することに関し、当該国又は当該機関による個人データの一般的な取扱いについてデータ主体に与えられる保護の水準が、次の各号に基づき又はそれにより、データ主体に与えられる保護の水準と実質的に同等以下ではない場合には、データ保護テストは満たされる。
   (a) 本規則
   (b) 2018 年法（Data Protection Act 2018）第 2 部
   (c) 同法の第 5 部から第 7 部（一般的な取扱いに関連する限度で）

2. 個人データを第三国又は国際機関へ移転することに関しデータ保護テストが満たされるかを検討するに当たり、国務長官は、その他の事項と併せて、次の点を考慮しなければならない。
   (a) 当該国又は当該機関における法の支配及び人権の尊重
   (b) 当該国又は当該機関において、個人データの取扱いに関しデータ主体の保護を執行する責任を負う権限当局の存否及びその権限
   (c) 当該取扱いに関連してデータ主体が利用できる司法上又は非司法上の救済手続
   (d) 当該国又は当該機関から他の国又は国際機関への個人データの移転に関する規則
   (e) 当該国又は当該機関の関連する国際的義務
   (f) 当該国又は当該機関の憲法、伝統及び文化

（以下省略）

また、第 45C 条では、第 45A 条に基づいて国務長官が越境移転先として承認した第三国及び国際機関の動向を継続的に監視する義務が定められている。第 45C 条は、2025 年 6 月に王室承認された条項である。

【UK GDPR 第 45C 条 規制によって承認された転送の監視】

1. 国務長官は、継続的に、第三国及び国際機関における、第 45A 条に基づく規則の制定、改正又は撤廃に影響を及ぼし得る動向を監視しなければならない。
2. 国務長官が、第 45A 条に基づく規則で承認された（又はその類型として承認された）個人データの移転について、もはや「データ保護テスト」を満たしていないことを認識した場合には、必要な限度で、当該規則を改正又は撤廃しなければならない。
3. 前項に従い第 45A 条に基づく規則が改正又は撤廃された場合、国務長官は、当該第三国又は国際機関と協議を開始し、当該国又は当該機関における個人データの取扱いに関してデータ主体に提供される保護の改善を図らなければならない。

（以下省略）

第 45A 条によって政府が承認した規則がない相手国、相手先に個人データを移転する際には、第 46 条の条件を満たすかがポイントとなる。第 46 条では、法的拘束力のある規則を用意することで移転が可能になることが定められている。第 46 条には以下のケースが挙げられている。

【UK GDPR 第 46 条 適切な保護措置が適用されるデータ移転】

(a) 公的機関と他の関連する者との間の法的拘束力及び執行可能な文書

(b) 第 47 条に従って承認された拘束的事業者準則

(c) 第 47A(1)条に基づき国務長官が制定した規則で定められ、現在有効な標準データ保護条項

(d) 2018 年法第 119A 条に基づき、情報コミッショナーが発行し文書に定められ、現在有効な標準データ保護条項

(e) 第 40 条に基づいて承認された行動規範であって、第三国の管理者又は処理者が当該行動規範で定める保護措置を適用する旨の拘束的かつ執行可能な約束を伴うもの（データ主体の権利に関する事項を含む）

(f) 第 42 条に基づいて承認された認証メカニズムであって、第三国の管理者又は処理者が当該メカニズムで定める保護措置を適用する旨の拘束的かつ執行可能な約束を伴うもの（データ主体の権利に関する事項を含む）。

さらに、第 45A 条と第 46 条のいずれの条件も満たされない場合でも、第 49 条が定める条件を満たす場合は例外的に個人データの越境移転が認められる。

【UK GDPR 第 49 条 特定の状況における例外】

・ 2018 年法第 17A 条に基づく十分性規則、又は第 46 条に基づく適切な保護措置が存在しない場合、第三国又は国際機関への個人データの移転又はその一連の移転は、次のいずれかの条件を満たす場合に限り行うことができる。

(a) データ主体が、十分性決定及び適切な保護措置が存在しないことによるリスクについて通知を受けたうえで、提案された移転に明示的に同意した場合

(b) 移転が、データ主体と管理者との契約の履行又はデータ主体の要請により取られた契約締結前の措置の実施に必要である場合

(c) 移転が、データ主体の利益のために管理者と他の自然人又は法人との間で締結された契約の締結又は履行に必要である場合

(d) 移転が、重要な公益上の理由によって必要である場合

(e) 移転が、法的請求の設定、行使又は防御に必要である場合

(f) 移転が、データ主体又は他者の生命に関わる利益を保護するために必要であり、データ主体が身体的又は法的に同意を与えられない場合
(g) 移転が、国内法により公衆への情報提供を目的として設けられた登録簿から行われ、かつその登録簿が一般公衆又は正当な利益を有する者による閲覧に開放されており、かつ個別の事例において当該国内法に定められた閲覧条件が満たされている場合

・ 第 45 条又は第 46 条に基づく移転ができず、上記の例外のいずれにも該当しない場合、第三国又は国際機関への移転は、次のすべての条件を満たす場合に限り許可される。
- その移転が反復的でないこと
- 限定された数のデータ主体にのみ関係すること
- 移転が、管理者の追求するやむを得ない正当な利益のために必要であり、データ主体の利益又は権利・自由によってこれが凌駕されないこと
- 管理者が移転の状況を評価し、適切な保護措置を講じたこと

・ この場合、管理者は情報コミッショナーに移転を通知し、さらにデータ主体に対し、第 13 条及び第 14 条に定める情報に加え、当該移転及びその際に追求されるやむを得ない正当な利益について通知しなければならない

3. 2.の条件において、GCBPR が自法域と同等以上の個人情報保護体制を構築する措置（相当措置）として認められているか

UK GDPR は第 45A 条によって、データ保護テストを含めた判断により、国全体、特定セクター、特定の制度等を移転先として承認する規則を設けることが可能であると定めている。

ただし、現時点では当該規則に GCBPR は含まれていない。また、データ保護テストの評価基準には事業者の裁量ではなく各国法において定まるものも多いため、GCBPR だけでは相当措置としては認められづらいと考えられる。

4. データローカライゼーションの規制はあるか。規制がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

本調査で把握している限り、個人に関わるデータを域内で保管することを義務付けるデータローカライゼーションの規定は存在しない。

5. ガバメントアクセスが認められる規制・制度等はあるか。規制・制度等がある場合、どのレベル（法令、政省令、ガイドライン等）において、どのような内容が規定されているか

以下では、令状審査なしでガバメントアクセスが認められる法令を掲載している。

図表 47 イギリスにおけるガバメントアクセス

目的	データの種類	アクセス権限のある機関	強制性	ガバメントアクセスが認められている法令・政省令・ガイドライン等	条文
・犯罪捜査 ・公共の安全維持	・電気通信システム又はそのデータ ※伝送中の通信の傍受は不可	・承認職員 （法執行機関において指定上級職員からデータにアクセスすることを認められた者）	・対応が必須	・Investigatory Powers Act 2016（IPA）	・第 61A 条
・不正受給等の調査・執行目的	・受給に係る情報 （労災年金の場合は事故・障害・疾病の情報も含む）	・受給調査に係る権限付与職員	・第 111 条に罰則規定あり	・Social Security Administration Act 1992	・第 109A 条 ・第 109B 条
・疑わしい金融取引の検知	・金融取引情報	・監督当局	・第 87 条に罰則規定あり	・Money Laundering Regulations 2017(MLR)	・MLR 21A 条（テロ資金疑惑の報告義務）

2.6. 各国法令とGCBPRのプログラム要件とのマッピング分析

(1) 調査目的

対象法域の個人情報保護関連法令と、GCBPR のプログラム要件とのマッピング分析を行うことで、制度間の整合性やギャップを明確化する。今後これらの法域が GCBPR への参加を促す際の連携方針、見込み、例えば GCBPR 加盟に向け法制度整備において不足している点や、その国内法化に向けた支援等の可能性を把握し、効果的なアウトリーチ活動を導出するための資料とする。

(2) 調査対象

調査 2.1.の結果、越境移転先としてニーズのある上位法域から、既に GCBPR に加盟している法域、参加意思を示している法域、参加見込みが低い法域を除いた結果、図表 48 のとおり、ベトナム・インド・インドネシアの三法域を選定した。

ベトナムの PDPL は 2026 年 1 月 1 日に施行される新法である。PDPL 第 39 条には経過規定があり、PDPL 施行前に PDPD（旧法）に基づいてデータ主体から同意を取得していた場合や、個人データ処理影響評価記録及び国外移転に関する個人データ移転影響評価記録を提出していた場合等も、新たに同意を取得したり、記録を作成したりする必要はないと定められている。PDPD から PDPL への移行期間がいつまで続くかは定かではないため、本調査では PDPD、PDPL の双方を対象に調査した。

(3) 調査項目

図表 48 マッピング分析の対象

	法域名	参照元
1	ベトナム	・ Decree No. 13/2023/ND-CP:Personal Data Protection Decree（PDPD） ・ Personal Data Protection Law (PDPL) ※2025 年 6 月 26 日に可決、2026 年 1 月 1 日より施行
2	インド	・ The Digital Personal Data Protection Act, 2023 (DPDP Act)
3	インドネシア	・ Law No. 27 of 2022 on Personal Data Protection (PDP Law)

GCBPR のプログラム要件は、GCBPR プライバシー原則 に基づいて 8 項目がどのように要求されているかを調査する。また、項目ごとに確認する内容は、R6 調査を参照する。

図表 49 GCBPR プログラム要件、及びマッピング分析時の観点[36]

分類	GCBPR プログラム要件		マッピング分析時の観点
通知	1	上記の個人情報を管理する実務と方針について、明確で簡単にアクセスできる声明（プライバシーステートメント）提供していますか？「はい」の場合、該当するすべてのプライバシーステートメントのコピー及び/又は同ステートメントへのハイパーリンクを提供してください。	個人情報を管理する実務と方針について、明確で簡単にアクセスできる声明（プライバシーステートメント）提供を義務付けているか
	a)	プライバシーステートメントには、貴組織が個人情報を収集する方法が記載されていますか？	プライバシーステートメントに、あなたの組織が個人情報を収集する方法を記載することを義務付けているか
	b)	このプライバシーステートメントには、個人情報を収集する目的が記載されていますか？	プライバシーステートメントに、個人情報を収集する目的を記載することを義務付けているか
	c)	このプライバシーステートメントは、個人情報を第三者に提供するかどうか、またその目的は何かについて、個人に通知していますか？	プライバシーステートメントに、個人情報を第三者に提供するかどうか、またその目的は何かについて含めることを義務付けているか
	d)	このプライバシーステートメントでは、個人情報の収集の際に、個人情報の取扱いや慣行に関する連絡方法を含め、会社名及び所在地を開示していますか？「はい」の場合、以下に記述してください。	プライバシーステートメントに、個人情報の収集の際に、個人情報の取扱いや慣行に関する連絡方法を含め、会社名及び所在地を記載することを義務付けているか
	e)	このプライバシーステートメントは、個人の個人情報の使用と開示に関する情報を提供していますか？	プライバシーステートメントに、個人の個人情報の使用と開示に関する情報を記載することを義務付けているか
	f)	このプライバシーステートメントには、個人が自分の個人情報にアクセスし、訂正することができるかどうか、またその方法に関する情報が記載されていますか？	プライバシーステートメントに、個人が自分の個人情報にアクセスし、訂正することができるかどうか、またその方法に関する情報を記載することを義務付けているか
	2	以下の資格に従うことを条件に、個人情報の収集時に（直接であるか、又はあなたの代理として行動する第三者を通じてであるかを問わず）、そのような情報が収集されていることを通知しますか？	個人情報の収集時に（直接であるか、又はあなたの代理として行動する第三者を通じてであるかを問わず）、収集する情報の種類を通知することを義務付けているか
	3	以下の資格に基づき、個人情報を収集する際、（直接であるか、代理で行動する第三者を通じてであるかを問わず）個人情報を収集する目的を明示していますか？	個人情報の収集時に個人情報を収集する目的の明示を義務付けているか

[36] 本項はプログラム要件と法制度をマッピングするものであるため、企業の運用を伺う質問は対象外とし、マッピング分析時の観点を斜線とした。また、、プログラム要件が複数の選択肢を展開している場合、冒頭の質問部分は回答可能な場合を除き、選択肢のみを比較対象とする項目は斜線とした。

分類	GCBPR プログラム要件		マッピング分析時の観点
	4	個人情報を収集する際に、以下の資格の範囲内で、個人情報が第三者と共有される可能性があることを通知していますか？	個人情報の収集時に個人情報が第三者と共有される可能性があることの通知を義務付けているか
取得の制限	5	**（企業の運用を伺う質問のため対象外）** 個人情報をどのように取得していますか。	
	a)	本人から直接取得していますか？	
	b)	第三者から取得していますか？	
	c)	その他。該当する場合、具体的に説明してください。	
	6	個人情報の収集（直接であるか、又は第三者に代行してもらうかを問わず）を、収集の目的、又はその他関連のある、又は関連する目的を達成するために必要な範囲に限定していますか？	個人情報の収集（直接であるか、又は第三者に代行してもらうかを問わず）を、収集の目的、又はその他の互換性のある、又は関連する目的を達成するために関連する情報に限定することを義務付けているか
	7	個人情報の収集（直接であるか、又は第三者の代行によるものであるかを問わない）を、当該個人情報の収集を管轄する法域の要件に合致した、合法的かつ公正な手段によって行っていますか？「はい」の場合は、その内容を説明してください。	個人情報の収集（直接であるか、又は第三者の代行によるものであるかを問わない）を、当該個人情報の収集を管轄する法域の要件に合致した、合法的かつ公正な手段によって行うことを義務付けているか
個人情報の利用	8	プライバシーステートメント及び/又は収集時に提供された通知で特定されているように、収集した個人情報の使用を（直接であるか、又はあなたの代理としての第三者の使用を通じてであるかを問わず）、情報が収集された目的、又はその他の互換性のある、又は関連する目的に限定していますか？必要に応じて、以下の空欄に説明を記入してください。	プライバシーステートメント及び/又は収集時に提供された通知で特定されているように、収集した個人情報の使用を（直接であるか、又は第三者の使用を通じてであるかを問わず）、情報が収集された目的、又はその他の互換性のある、又は関連する目的に限定することを義務付けているか
	9	「いいえ」と答えた場合、収集した個人情報を、以下のいずれかの状況下で、関連性のない目的のために使用しますか？以下に記述してください。	収集した個人情報を、以下のいずれかの状況下で、関連性のない目的のために使用することを認めているか
	a)	本人の明示的な同意に基づくものですか？	本人の明示的な同意に基づく場合は個人情報の利用を認めているか
	b)	適用される法律により義務付けられている場合ですか？	適用される法律によって強制される場合は個人情報の利用を認めているか
	10	**（企業の運用を伺う質問のため対象外）** 収集した個人情報（直接、又は貴社に変わって代行する第三者の利用を問わず）を他の個人情報管理者に	

分類	GCBPR プログラム要件		マッピング分析時の観点
		開示しますか？「はい」の場合、説明してください。	
	11	**（企業の運用を伺う質問のため対象外）** 個人情報を個人情報処理業者に転送しますか？「はい」の場合、説明してください。	
	12	12. 質問 10 及び／又は質問 11 に「はい」と答えた場合、開示及び／又は移転は、収集の当初の目的、又は互換性のある別の目的もしくは関連する目的を果たすために行われますか？以下に記述してください。	開示及び／又は移転は、収集の当初の目的、又は互換性のある別の目的もしくは関連する目的に限定することを義務付けているか ※質問 10 と質問 11 は対象外としているが、プログラム要件文は、オリジナルを記載しているため、後述の記載は(質問 10 及び／又は質問 11 に「はい」と答えた場合、)とする
	13	質問 12 に「いいえ」と答えた場合、又はその他適切な場合、開示及び/又は移転は以下のいずれかの状況下で行われますか？	開示及び/又は譲渡は以下のいずれかの状況下で行うことを認めているか
	a)	本人の明示的な同意に基づくものですか？	本人の明示的な同意に基づく場合は個人情報の開示及び移転を認めているか
	b)	個人から要求されたサービスや製品を提供するために必要な場合ですか？	個人から要求されたサービスや製品を提供するために必要な場合は個人情報の開示及び移転を認めているか
	c)	適用される法律により義務付けられている場合ですか？	適用される法律によって強制される場合は個人情報の開示及び移転を認めているか
選択	14	個人情報の取得に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	個人情報の取得に関連して本人が選択できる方法を提供することを義務付けているか
	15	個人情報の利用に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	個人情報の利用に関連して本人が選択できる方法を提供することを義務付けているか
	16	個人情報の開示に関して個人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	個人情報の開示に関連して個人が選択できる方法を提供することを義務付けているか
	17	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示又は提供されていますか？	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示又は提供することを義務付けているか
	18	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それらは明瞭に表	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それは明瞭な表現

分類	GCBPR プログラム要件		マッピング分析時の観点
		現され、容易に理解できるものですか？	ですぐ分かるようにすることを義務付けているか
	19	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、その選択は簡単に利用でき手ごろなものですか？「はい」の場合、説明してください。	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、その選択は簡単に利用でき手ごろなものであることを義務付けているか
	20	**（企業の運用を伺う質問のため対象外）** 必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄又は必要に応じて添付資料として説明を添えてください。	
個人情報の完全性	21	利用目的に必要な範囲内において、保有する個人情報が最新かつ正確で完全なものであることを確認するための措置を講じていますか？「はい」の場合、その内容を説明してください。	利用目的の達成に必要な範囲内において、保有する個人情報が最新かつ正確で完全なものであることを確認するための措置を講じることを義務付けているか
	22	利用目的に必要な範囲内において、不正確・不完全、又は古い個人情報を修正する仕組みがありますか？必要に応じて、以下の空欄又は添付ファイルにその内容を記載してください。	利用目的の達成に必要な範囲内において、不正確・不完全・古くなった個人情報を訂正する仕組みを設けることを義務付けているか
	23	不正確・不完全、又は古い情報が利用目的に影響し、情報の移転後に修正が行われる場合、個人情報が移転された個人情報処理業者、代理人、又はその他のサービス提供者に修正内容を伝えていますか？「はい」の場合は、その内容を説明してください。	不正確な情報、不完全な情報、又は古い情報が利用目的に影響し、情報の移転後に訂正が行われる場合、個人情報が移転された個人情報処理業者、代理人、又はその他のサービス提供者に訂正を伝えることを義務付けているか
	24	不正確・不完全、又は古い情報が利用目的に影響し、情報の開示後に訂正が行われる場合、個人情報の開示先である他の第三者に訂正を伝えていますか？「はい」の場合は、その内容を説明してください。	不正確な情報、不完全な情報、又は古い情報が利用目的に影響し、情報の開示後に訂正が行われる場合、個人情報の開示先である他の第三者に訂正を伝えることを義務付けているか
	25	個人情報の処理者、代理人、又はその他のサービス提供者が、不正確・不完全、又は古い情報に気づいた場合、貴組織に通知することを要求していますか？	個人情報の処理者、代理人、又はその他のサービス・プロバイダーが、不正確、不完全、又は古い情報に気づいた場合、データ処理者に通知することを義務付けているか
セキュリティ対策	26	情報セキュリティポリシーを導入していますか？	情報セキュリティポリシーを導入することを義務付けているか
	27	個人情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用等のリスクから個人情報を	情報の紛失、不正アクセス、破壊、使用、修正、開示、又はその他の悪用等のリスクから個人情報を保護す

分類	GCBPR プログラム要件		マッピング分析時の観点
		保護するために実施した物理的、技術的、管理的な保護措置について説明してください。	るために実施した物理的、技術的、管理的な保護措置を導入することを義務付けているか
	28	質問 27 への回答で特定した保護措置が、脅威となる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明してください。	質問 27 への回答で特定した保護措置が、脅かされる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明することを義務付けているか
	29	個人情報のセキュリティ維持の重要性を従業員にどのように認識させているか説明してください（定期的な研修や監督等）。	個人情報のセキュリティ維持の重要性を従業員に認識させることを義務付けているか
	30	脅威となる危害の可能性と重大性、情報の機密性、及び情報が保持される状況に応じた保護措置を実施していますか？	危害の脅威の可能性と重大性、情報の機微性、及び情報が保持される状況に応じ、以下の保護措置を義務付けているか
	a)	従業員研修・管理、その他の組織的安全対策	従業員の研修や管理、あるいはその他の組織的な安全対策の実施を義務付けているか
	b)	ネットワークやソフトウェアの設計、情報の処理、保存、転送、廃棄を含む情報システムと管理	ネットワークやソフトウェアの設計、情報処理、保存、送信、廃棄を含む情報システムの設置、及び管理を義務付けているか
	c)	攻撃、侵入、その他のセキュリティ障害への検知、防止、対応	攻撃、侵入、その他のセキュリティ障害を検知、防止、対応することを義務付けているか
	d)	物理的セキュリティ	物理的セキュリティ対策の実施を義務付けているか
	31	個人情報を安全に廃棄するためのポリシーを導入していますか？	個人情報を安全に廃棄するためのポリシーの導入を義務付けているか
	32	攻撃、侵入、その他のセキュリティ障害を検知、防止、対応するための対策を実施していますか？	攻撃、侵入、その他のセキュリティ障害を検知、防止、対応するための対策の実施を義務付けているか
	33	上記の質問 32 で言及した安全対策の有効性をテストするためのプロセスを設けていますか？以下に説明してください。	上記の質問 32 で言及したセーフガードの有効性をテストするためのプロセスの導入を義務付けているか
	34	第三者認証やその他のリスク評価を利用していますか？以下に説明してください。	第三者認証やその他のリスク評価の利用を義務付けているか
	35	個人情報を移転する情報処理業者、代理人、請負業者、又はその他のサービス提供者に対して、情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用から保護することを要求していますか？	個人情報の処理業者、代理人、請負業者、又は個人情報を転送するその他のサービス・プロバイダーに対して、情報の紛失、不正アクセス、破壊、使用、修正、開示、又はその他の悪用から保護するために、以下の措置を義務付けているか
	a)	提供される情報及びサービスの機密性に見合った情報セキュリティプログラムを導入していますか？	提供される情報及びサービスの機微性に見合った情報セキュリティプログラムの導入を義務付けているか
	b)	貴組織の個人情報のプライバシー又はセキュリティの侵害の発生に気	個人情報のプライバシー又はセキュリティの侵害の発生に気付いた場

分類	GCBPR プログラム要件		マッピング分析時の観点
		付いた場合、速やかに貴組織に通知していますか？	合、速やかにデータ処理者に通知することを義務付けているか
	c)	プライバシー侵害又はセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じていますか？	プライバシー侵害又はセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じることを義務付けているか
アクセス及び訂正	36	要求があった場合、要求された個人に関する個人情報を保有しているかどうかの確認を行っていますか？以下に説明してください。	要求があった場合、要求された個人に関する個人情報を保有しているかどうかの確認を義務付けているか
	37	要求に応じて、貴組織は個人に対して、貴組織が保有する個人情報へのアクセスを提供していますか？「はい」の場合、質問 37(a)～(e)に答え、アクセス要求の受付及び処理に関する組織の方針／手順を以下に記述する。「いいえ」の場合は、質問 38 に進んでください。	要求に応じて、個人に対して、データ処理者が保有する個人情報へのアクセスを提供することを義務付けているか
	a)	アクセスを要求する個人の身元を確認する手段を講じていますか？「はい」の場合、説明してください。	アクセスを要求する個人の身元を確認する手段の導入を義務付けているか
	b)	個人からのアクセス要求後、合理的な期間内でアクセスを提供していますか？「はい」の場合、詳細を説明してください。	個人からのアクセス要請後、合理的な時間枠内でアクセスを提供することを義務付けているか
	c)	情報は、一般的に理解できる合理的な方法（読みやすい形式）で伝えられていますか？説明してください。	情報は、一般的に理解できる合理的な方法（読みやすい形式）で伝えることを義務付けているか
	d)	情報は、本人との通常の対話形式（電子メール、同じ言語等）に適合した方法で提供されていますか？	情報は、本人との通常の対話形式（電子メール、同じ言語等）に適合した方法で提供することを義務付けているか
	e)	アクセスを提供するために料金を請求しますか？「はい」の場合、その料金の根拠と、料金が過大でないことを保証する方法を以下に記述してください。	アクセスを提供するために料金を請求することを許容しているか
	38	個人が自分の情報の正確さに異議を唱え、それを修正、補完、変更、及び/又は削除することを許可していますか？この点に関する組織の方針／手順を以下に記述し、質問 38 (a)～(e)に回答してください。	個人が自分の情報の正確さに異議を唱え、それを修正、補完、訂正、及び/又は削除することを義務付けているか
	a)	アクセス及び訂正の仕組みは、明確かつ目立つように表示されていますか？必要であれば、以下の空欄又は添付ファイルにその説明を記入してください。	アクセス及び訂正の仕組みは、明確かつ目立つように表示することを義務付けているか
	b)	個人情報が不完全又は不正確であると、本人から申し出があった場合、要求された訂正、追加、または適切な場合には削除を行いますか？	個人情報が不完全又は不正確であることを本人が証明した場合、要求された訂正、追加、又は適切な場合

分類	GCBPR プログラム要件		マッピング分析時の観点
			には削除することを義務付けているか
	c)	個人からの訂正又は削除の要求後、合理的な期間内にそのような訂正又は削除を行っていますか？	個人からの訂正又は削除の要請後、合理的な期間内にそのような訂正又は削除することを義務付けているか
	d)	訂正された個人情報のコピーを本人に提供するか、データが修正又は削除されたことを本人に確認していますか？	訂正された個人情報のコピーを本人に提供するか、データが訂正又は削除されたことを本人に確認することを義務付けているか
	e)	アクセス又は修正が拒否された場合、アクセス又は修正が提供されない理由を、アクセス又は修正の拒否に関する問い合わせ先とともに、本人に説明していますか？	アクセス又は訂正が拒否された場合、アクセス又は訂正が提供されない理由を、アクセス又は訂正の拒否に関する問い合わせ先とともに、本人に説明することを義務付けているか
責任	39	**（企業の運用を伺う質問のため対象外）** 貴組織は、グローバル CBPR プライバシー原則を確実に遵守するために、どのような手段を講じていますか？該当するものをすべてチェックし、以下に説明してください。 ・内部指針又は方針（該当する場合、どのように実施しているか説明） ・契約 ・適用される業界又はセクターの法律及び規制の遵守 ・自主規制機関の規範及び/又は規則の遵守 ・その他	
	40	**（企業の運用を伺う質問のため対象外）** 貴組織は、グローバル CBPR プライバシー原則を遵守する組織全体の責任者を任命していますか？	
	41	貴組織は、プライバシーに関する苦情を受け、調査し、対応するための手順を備えていますか？説明してください。	プライバシーに関する苦情を受け、調査し、対応するための手順を設けることを義務付けているか
	42	貴組織は、個人が苦情に対するタイムリーな回答を確実に受け取るための手順を備えていますか？	個人が苦情に対するタイムリーな回答を確実に受け取るための手順を設けることを義務付けているか
	43	「はい」の場合、この回答には、苦情に関する改善措置の説明が含まれていますか？説明してください。	苦情に関する改善措置の説明を含めることを義務付けているか
	44	個人情報保護に関する苦情への対応方法を含め、個人情報保護方針及び手順に関して従業員を教育するための手順を設けていますか？「はい」の場合、説明してください。	個人情報保護に関する苦情への対応方法を含め、個人情報保護方針及び手順に関して従業員を教育するための手順を設けることを義務付けているか

分類	GCBPR プログラム要件		マッピング分析時の観点
	45	個人情報の開示を要求するものも含め、司法その他の政府による召喚状、令状、命令に応じるための手続きを定めていますか？	個人情報の開示を要求するものも含め、司法その他の政府による召喚状、令状、命令に応じるための手続きを定めることを義務付けているか
	46	個人情報を処理する個人情報処理者、代理人、請負業者、又はその他のサービス提供者との間で、個人に対する貴組織の義務が確実に果たされるような仕組みを設けていますか（該当するものすべてにチェックを入れてください）？ ・内部指針又は方針 ・契約 ・適用される業界又はセクターの法律及び規制の遵守 ・自主規制機関の規範及び/又は規則の遵守 ・その他（記述）	個人情報を処理する個人情報処理者、代理人、請負業者、又はその他のサービス・プロバイダーとの間で、個人に対するデータ処理者の義務が確実に果たされるような仕組みを設けることを義務付けているか
	47	**（企業の運用を伺う質問のため対象外）** これらの仕組みは、一般的に、個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に要求しますか？ ・プライバシーステートメントに記載されているグローバル CBPR に準拠したプライバシーポリシーと慣行を遵守すること ・貴組織のプライバシーステートメントに記載されているポリシー又はプライバシー慣行と実質的に類似したプライバシー慣行を実施すること ・個人情報の取扱い方法に関して、貴組織に提供された指示に従うこと ・貴組織の同意がない限り、下請けに制限を設けること ・管轄区域において、フォーラムが認定した AA からからグローバル CBPR の認定を取得すること ・その他（記述）	
	48	個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、貴組織の指示及び/又は契約の遵守を確保するための自己評価を提供するよう求めていますか？「はい」の場合、以下に説明してください。	個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、データ処理者の指示及び/又は契約/契約の遵守を確認するための自己評価を提供させることを義務付けているか
	49	個人情報の処理者、代理人、請負業者、又はその他のサービス提供者について、貴組織の指示及び/又は合意/契約が遵守されていることを確認するために、定期的な抜き打ち検査又は監視を行っていますか？	個人情報の処理者、代理人、請負業者、又はその他のサービス提供者について、データ処理者の指示及び/又は合意/契約が遵守されていることの確認を行うことを義務付けているか

分類	GCBPR プログラム要件		マッピング分析時の観点
		「はい」の場合、以下に記述してください。	
	50	**（企業の運用を伺う質問のため対象外）** 上記のような受領者によるグローバル CBPR システムの遵守を保証するデューディリジェンスや仕組みが現実的でない、又は不可能である状況において、個人情報を他の個人情報管理者に対して開示しますか？	

(4) 分析結果概要

ベトナム・インド・インドネシアの個人情報保護関連法令と、GCBPR のプログラム要件とのマッピング分析結果は図表 50 のとおりである。プログラム要件について同等の要求事項がある場合は「○」、ない場合は「該当なし」、類似の要求事項があるが同等とは考えられない要求事項は「△」の評価としている。各国の評価基準や参照した条文については、後段のページをご参照いただきたい。

いずれの法令でも、1.通知、2.取得の制限、3.個人情報の利用、4.選択、5.個人情報の完全性、6.セキュリティ対策、7.アクセス及び訂正、8.責任に関する義務が課されている。しかし、通知時に個人情報処理者の会社名及び所在地の記載を義務付けたり(質問事項 1d)、訂正後に個人情報の移転先に訂正した旨を通知することを義務付けたり(質問事項 23)等、具体的な対応方法は、企業が個別に対応していることが多く、法令レベルでは言及されていないことが多い。

図表 50 各国法令と GCBPR のプログラム要件とのマッピング分析結果概要

※凡例:整合性が見られる場合は○、一部整合性がない場合は△で評価

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
通知	1	上記の個人情報を管理する実務と方針について、明確で簡単にアクセスできる声明(プライバシーステートメント)提供していますか？「はい」の場合、該当するすべてのプライバシーステートメントのコピー及び/又は同ステートメントへのハイパーリンクを提供してください。	○	○	△	○
	a)	プライバシーステートメントには、貴組織が個人情報を収集する方法が記載されていますか？	○	△	該当なし	△
	b)	このプライバシーステートメントには、個人情報を収集する目的が記載されていますか？	○	○	○	○
	c)	このプライバシーステートメントは、個人情報を第三者に提供するかどうか、またその目的は何かについて、個人に通知していますか？	○	○	△	△
	d)	このプライバシーステートメントでは、個人情報の収集の際に、個人情報の取扱いや慣行に関する連絡方法を含め、会社名及び所在地を開示していますか？「はい」の場合、以下に記述してください。	△	△	△	△
	e)	このプライバシーステートメントは、個人の個人情報の使用と開示に関する情報を提供していますか？	△	△	○	△
	f)	このプライバシーステートメントには、個人が自分の個人情報にアクセスし、	△	△	○	△

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
		訂正することができるかどうか、またその方法に関する情報が記載されていますか？				
	2	以下の資格に従うことを条件に個人情報の収集時に(直接であるか、又はあなたの代理として行動する第三者を通じてであるかを問わず)、そのような情報が収集されていることを通知しますか？	○	○	○	○
	3	以下の資格に基づき、個人情報を収集する際、(直接であるか、代理で行動する第三者を通じてであるかを問わず)個人情報を収集する目的を明示していますか？	○	○	○	○
	4	個人情報を収集する際に、以下の資格の範囲内で、個人情報が第三者と共有される可能性があることを通知していますか？	○	○	△	△
取得の制限	5	**(企業の運用を伺う質問のため対象外)** 個人情報をどのように取得していますか。				
	a)	本人から直接取得していますか？				
	b)	第三者から取得していますか？				
	c)	その他。該当する場合、具体的に説明してください。				
	6	個人情報の収集(直接であるか、又は第三者に代行してもらうかを問わず)を、収集の目的、又はその他関連のある、又は関連する目的を達成するために必要な範囲に限定していますか？	○	○	○	○
	7	個人情報の収集(直接であるか、又は第三者の代行によるものであるかを問わない)を、当該個人情報の収集を管轄する法域の要件に合致した、合法的かつ公正な手段によって行っていますか？「はい」の場合は、その内容を説明してください。	△	△	△	△
個人情報の利用	8	プライバシーステートメント及び/又は収集時に提供された通知で特定されているように、収集した個人情報の使用を(直接であるか、又はあなたの代理としての第三者の使用を通じてであるかを問わず)、情報が収集された目的、又はその他の互換性のある、又は関連する目的に限定していますか？必要に応じて、以下の空欄に説明を記入してください。	○	○	○	○

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
	9	「いいえ」と答えた場合、収集した個人情報を、以下のいずれかの状況下で、関連性のない目的のために使用しますか？以下に記述してください。				
	a)	本人の明示的な同意に基づくものですか？	○	○	○	○
	b)	適用される法律により義務付けられている場合ですか？	○	○	○	○
	10	**（企業の運用を伺う質問のため対象外）** 収集した個人情報（直接、又は貴社に変わって代行する第三者の利用を問わず）を他の個人情報管理者に開示しますか？「はい」の場合、説明してください。				
	11	**（企業の運用を伺う質問のため対象外）** 個人情報を個人情報処理業者に転送しますか？「はい」の場合、説明してください。				
	12	（質問 10 及び／又は質問 11 に「はい」と答えた場合、）開示及び／又は移転は、収集の当初の目的、又は互換性のある別の目的もしくは関連する目的を果たすために行われますか？以下に記述してください。	○	○	△	○
	13	質問 12 に「いいえ」と答えた場合、又はその他適切な場合、開示及び/又は移転は以下のいずれかの状況下で行われますか？				
	a)	本人の明示的な同意に基づくものですか？	○	○	○	○
	b)	個人から要求されたサービスや製品を提供するために必要な場合ですか？	○	○	○	○
	c)	適用される法律により義務付けられている場合ですか？	○	○	○	○
選択	14	個人情報の取得に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○	○	○	○
	15	個人情報の利用に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○	○	○	○
	16	個人情報の開示に関して個人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○	○	○	○
	17	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選	○	○	○	○

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
		択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示又は提供されていますか？				
	18	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それらは明瞭に表現され、容易に理解できるものですか？	○	○	○	○
	19	個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、その選択は簡単に利用でき手ごろなものですか？「はい」の場合、説明してください。	該当なし	該当なし	△	△
	20	**（企業の運用を伺う質問のため対象外）** 必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄又は必要に応じて添付資料として説明を添えてください。				
個人情報の完全性	21	利用目的に必要な範囲内において、保有する個人情報が最新かつ正確で完全なものであることを確認するための措置を講じていますか？「はい」の場合、その内容を説明してください。	△	△	△	○
	22	利用目的に必要な範囲内において、不正確・不完全、又は古い個人情報を修正する仕組みがありますか？必要に応じて、以下の空欄又は添付ファイルにその内容を記載してください。	○	○	△	○
	23	不正確・不完全、又は古い情報が利用目的に影響し、情報の移転後に修正が行われる場合、個人情報が移転された個人情報処理業者、代理人、又はその他のサービス提供者に修正内容を伝えていますか？「はい」の場合は、その内容を説明してください。	△	△	該当なし	該当なし
	24	不正確・不完全、又は古い情報が利用目的に影響し、情報の開示後に訂正が行われる場合、個人情報の開示先である他の第三者に訂正を伝えていますか？「はい」の場合は、その内容を説明してください。	△	△	該当なし	該当なし
	25	個人情報の処理者、代理人、又はその他のサービス提供者が、不正確・不完全、又は古い情報に気づいた場合、貴組織に通知することを要求していますか？	該当なし	該当なし	該当なし	該当なし

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
セキュリティ対策	26	情報セキュリティポリシーを導入していますか？	○	○	△	○
	27	個人情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用等のリスクから個人情報を保護するために実施した物理的、技術的、管理的な保護措置について説明してください。	○	○	○	○
	28	質問 27 への回答で特定した保護措置が、脅威となる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明してください。	該当なし	該当なし	△	○
	29	個人情報のセキュリティ維持の重要性を従業員にどのように認識させているか説明してください（定期的な研修や監督等）。	○	○	該当なし	○
	30	脅威となる危害の可能性と重大性、情報の機密性、及び情報が保持される状況に応じた保護措置を実施していますか？				
	a)	従業員研修・管理、その他の組織的安全対策	○	○	△	○
	b)	ネットワークやソフトウェアの設計、情報の処理、保存、転送、廃棄を含む情報システムと管理	○	○	△	○
	c)	攻撃、侵入、その他のセキュリティ障害への検知、防止、対応	○	○	△	○
	d)	物理的セキュリティ	○	○	△	△
	31	個人情報を安全に廃棄するためのポリシーを導入していますか？	○	○	△	○
	32	攻撃、侵入、その他のセキュリティ障害を検知、防止、対応するための対策を実施していますか？	○	○	△	○
	33	上記の質問 32 で言及した安全対策の有効性をテストするためのプロセスを設けていますか？以下に説明してください。	該当なし	該当なし	△	該当なし
	34	第三者認証やその他のリスク評価を利用していますか？以下に説明してください。	該当なし	該当なし	△	○
	35	個人情報を移転する情報処理業者、代理人、請負業者、又はその他のサービス提供者に対して、情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用から保護することを要求していますか？				
	a)	提供される情報及びサービスの機密性に見合った情報セキュリティプログラムを導入していますか？	○	○	△	○

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
	b)	貴組織の個人情報のプライバシー又はセキュリティの侵害の発生に気付いた場合、速やかに貴組織に通知していますか？	該当なし	該当なし	該当なし	該当なし
	c)	プライバシー侵害又はセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じていますか？	○	○	該当なし	○
アクセス及び訂正	36	要求があった場合、要求された個人に関する個人情報を保有しているかどうかの確認を行っていますか？以下に説明してください。	○	○	○	○
	37	要求に応じて、貴組織は個人に対して、貴組織が保有する個人情報へのアクセスを提供していますか？「はい」の場合、質問 37(a)～(e)に答え、アクセス要求の受付及び処理に関する組織の方針／手順を以下に記述する。「いいえ」の場合は、質問 38 に進んでください。				
	a)	アクセスを要求する個人の身元を確認する手段を講じていますか？「はい」の場合、説明してください。	該当なし	該当なし	該当なし	該当なし
	b)	個人からのアクセス要求後、合理的な期間内でアクセスを提供していますか？「はい」の場合、詳細を説明してください。	△	該当なし	該当なし	○
	c)	情報は、一般的に理解できる合理的な方法（読みやすい形式）で伝えられていますか？説明してください。	該当なし	該当なし	該当なし	○
	d)	情報は、本人との通常の対話形式（電子メール、同じ言語等）に適合した方法で提供されていますか？	該当なし	該当なし	該当なし	○
	e)	アクセスを提供するために料金を請求しますか？「はい」の場合、その料金の根拠と、料金が過大でないことを保証する方法を以下に記述してください。	該当なし	該当なし	該当なし	△
	38	個人が自分の情報の正確さに異議を唱え、それを修正、補完、変更、及び/又は削除することを許可していますか？この点に関する組織の方針／手順を以下に記述し、質問 38 (a)～(e)に回答してください。				
	a)	アクセス及び訂正の仕組みは、明確かつ目立つように表示されていますか？必要であれば、以下の空欄又は添付ファイルにその説明を記入してください。	該当なし	該当なし	該当なし	該当なし
	b)	個人情報が不完全又は不正確であると、本人から申し出があった場合、要	○	○	○	○

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
		求された訂正、追加、又は適切な場合には削除を行いますか？				
	c)	個人からの訂正又は削除の要求後、合理的な期間内にそのような訂正又は削除を行っていますか？	△	該当なし	該当なし	○
	d)	訂正された個人情報のコピーを本人に提供するか、データが修正又は削除されたことを本人に確認していますか？	該当なし	該当なし	該当なし	○
	e)	アクセス又は修正が拒否された場合、アクセス又は修正が提供されない理由を、アクセス又は修正の拒否に関する問い合わせ先とともに、本人に説明していますか？	○	○	該当なし	該当なし
責任	39	**（企業の運用を伺う質問のため対象外）** 貴組織は、グローバルCBPRプライバシー原則を確実に遵守するために、どのような手段を講じていますか？該当するものをすべてチェックし、以下に説明してください。 ・ 内部指針又は方針（該当する場合、どのように実施しているか説明） ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他				
	40	**（企業の運用を伺う質問のため対象外）** 貴組織は、グローバルCBPRプライバシー原則を遵守する組織全体の責任者を任命していますか？				
	41	貴組織は、プライバシーに関する苦情を受け、調査し、対応するための手順を備えていますか？説明してください。	該当なし	該当なし	○	△
	42	貴組織は、個人が苦情に対するタイムリーな回答を確実に受け取るための手順を備えていますか？	該当なし	△	○	△
	43	「はい」の場合、この回答には、苦情に関する改善措置の説明が含まれていますか？説明してください。	該当なし	該当なし	該当なし	△
	44	個人情報保護に関する苦情への対応方法を含め、個人情報保護方針及び手順に関して従業員を教育するための手順を設けていますか？「はい」の場合、説明してください。	△	△	該当なし	△
	45	個人情報の開示を要求するものも含め、司法その他の政府による召喚状、	○	○	該当なし	該当なし

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
		令状、命令に応じるための手続きを定めていますか？				
	46	個人情報を処理する個人情報処理者、代理人、請負業者、又はその他のサービス提供者との間で、個人に対する貴組織の義務が確実に果たされるような仕組みを設けていますか（該当するものすべてにチェックを入れてください）？ ・ 内部指針又は方針 ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他（記述）	○	○	○	○
	47	**（企業の運用を伺う質問のため対象外）** これらの仕組みは、一般的に、個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に要求しますか？ ・ プライバシーステートメントに記載されているグローバルCBPRに準拠したプライバシーポリシーと慣行を遵守すること ・ 貴組織のプライバシーステートメントに記載されているポリシー又はプライバシー慣行と実質的に類似したプライバシー慣行を実施すること ・ 個人情報の取扱い方法に関して、貴組織に提供された指示に従うこと ・ 貴組織の同意がない限り、下請けに制限を設けること ・ 管轄区域において、フォーラムが認定したAAからからグローバルCBPRの認定を取得すること ・ その他（記述）				
	48	個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、貴組織の指示及び/又は契約の遵守を確保するための自己評価を提供するよう求めていますか？「はい」の場合、以下に説明してください。	該当なし	該当なし	該当なし	△
	49	個人情報の処理者、代理人、請負業者、又はその他のサービス提供者について、貴組織の指示及び/又は合意/契約が遵守されていることを確認するために、定期的な抜き打ち検査又は監視を行っていますか？「はい」の場合、以下に記述してください。	該当なし	該当なし	△	○

分類	マッピング分析時の観点		ベトナム PDPD	ベトナム PDPL	インド DPDP Act	インドネシア PDP Law
	50	**（企業の運用を伺う質問のため対象外）** 上記のような受領者によるグローバルCBPRシステムの遵守を保証するデューディリジェンスや仕組みが現実的でない、又は不可能である状況において、個人情報を他の個人情報管理者に対して開示しますか？				

① ベトナム

Decree No. 13/2023/ND-CP:Personal Data Protection Decree（PDPD）、Personal Data Protection Law (PDPL)を対象とし、GCBPR のプログラム要件とのマッピング分析を行った。

1. 通知要件の比較

PDPD では、第 13 条にてデータの「処理」に関する通知要件が定められている。なお、「処理」の定義は、第 1 条第 7 項で以下のとおり定められている。「移転」が含まれていることから、質問事項 1(c)、2、3、4 で言及されている第三者提供に関する通知要件についても、第 13 条に含まれていると認識している。

【PDPD 第 1 条第 7 項】
個人データに影響を及ぼす一つ又は複数の行為をいい、これには以下のような行為が含まれる。
取得、記録、分析、確認、保管、変更、公表、結合、アクセス、検索、回復、暗号化、復号、複製、共有、送信、提供、移転、削除、破壊、又は個人データに関連するその他の行為。

質問事項 1(d)連絡方法・会社名・所在地の通知は、PDPD 第 13 条第 2 項(d)では、「処理目的に関連するその他の組織及び／又は個人に関する情報」と記載されているのみのため、「△」評価としている。

また、質問事項 1(e)個人の個人情報の使用と開示に関する情報、及び 1(f) アクセス・訂正の可否・方法の通知は、第 11 条 2(d)に同意を取得する際には、データ主体の権利・義務についての通知が必要と義務付けられており、第 9 条のデータ主体の権利に知らされる権利（第 1 項）、アクセス権（第 3 項）が定められている。しかし、権利について知らせることが義務付けられているのみであり、実際に使用と開示に関する情報やアクセス・訂正に関する方法といった詳細な情報の開示までは義務付けられていないため、「△」評価としている。

PDPL では、通知要件が定められた条文はなく、データ処理に関する同意を取得する条件として通知すべき項目が定められている。なお、データの処理には、別段の定めがある場合を除き、データ主体からの同意を取得することが義務付けられている（第 9 条第 1 項）。そのため、同意取得時の通知項目（第 9 条第 2 項）を PDPL の通知要件として解釈している。

また、PDPD と同様に、データ処理の定義には第 2 条第 6 項にて以下のとおり定められており、「移転」が含まれていることから、質問事項 1(c)、2、3、4 で言及されている第三者提供に関する通知要件についても、第 9 条第 2 項に含まれていると認識している。

【PDPL 第 2 条第 6 項】
個人データの処理とは、個人データに影響を及ぼす活動をいい、以下の一つ又は複数の活動を含む。すなわち、収集、分析、集約、暗号化、復号、訂正、削除、破棄、匿名化、提供、公開、移転、ならびに個人データに影響を及ぼすその他の活動をいう。

質問事項 1(a)個人情報を収集する方法の通知は、PDPD のように明確に収集方法を通知するとの記載がないものの、同意取得時に処理目的を通知する必要があること、処理目的ごとに同意を取得する必要があることから、収集方法がその一環で通知されることを見越し、「△」評価としている。

質問事項 1(d)連絡方法・会社名・所在地の通知は、PDPD と同様に、連絡方法や所在地等具体的な情報の通知までは条文に定められていないため、「△」評価としている。また、質問事項 1(e)個人の個人情報の使用と開示に関する情報、及び 1(f)アクセス・訂正の可否・方法の通知も、PDPD と同様に、データ主体の権利が通知されるのみであり、具体的な使用と開示に関する情報や、アクセス・訂正に関する方法の通知までは条文に定められていないため、「△」評価としている。

図表 51 「通知」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
1. 上記の個人情報を管理する実務と方針について、明確で簡単にアクセスできる声明（プライバシーステートメント）提供していますか？「はい」の場合、該当するすべてのプライバシーステートメントのコピー及び/又は同ステートメントへのハイパーリンクを提供してください。	○ 第 13 条	○ 第 9 条 第 2 項
a) プライバシーステートメントには、貴組織が個人情報を収集する方法が記載されていますか？	○ 第 13 条 第 2 項 c	△ 第 9 条 第 2 項 a ・ 第 9 条 第 4 項 a
b) このプライバシーステートメントには、個人情報を収集する目的が記載されていますか？	○ 第 13 条 第 2 項 a	○ 第 9 条 第 2 項 a
c) このプライバシーステートメントは、個人情報を第三者に提供するかどうか、またその目的は何かについて、個人に通知していますか？	○ 第 13 条 第 2 項 a,c	○ 第 9 条 第 2 項 a,b
d) このプライバシーステートメントでは、個人情報の収集の際に、個人情報の取扱いや慣行に関する連絡方法を含め、会社名及び所在地を開示していますか？「はい」の場合、以下に記述してください。	△ 第 13 条 第 2 項 d	△ 第 9 条 第 2 項 b

質問	ベトナム PDPD	ベトナム PDPL
e) このプライバシーステートメントは、個人の個人情報の使用と開示に関する情報を提供していますか？	△ 第 11 条 第 2 項 d ・ 第 9 条 第 1 項	△ 第 9 条 第 2 項 c ・ 第 11 条 第 1 項
f) このプライバシーステートメントには、個人が自分の個人情報にアクセスし、訂正することができるかどうか、またその方法に関する情報が記載されていますか？	△ 第 11 条 第 2 項 d ・ 第 9 条 第 3 項	△ 第 9 条 第 2 項 c ・ 第 13 条 第 1 項
2. 以下の資格に従うことを条件に、個人情報の収集時に（直接であるか、又はあなたの代理として行動する第三者を通じてであるかを問わず）、そのような情報が収集されていることを通知しますか？	○ 第 13 条 第 2 項 b	○ 第 9 条 第 2 項 a
3. 以下の資格に基づき、個人情報を収集する際、（直接であるか、代理で行動する第三者を通じてであるかを問わず）個人情報を収集する目的を明示していますか？	○ 第 13 条 第 2 項 a	○ 第 9 条 第 2 項 a
4. 個人情報を収集する際に、以下の資格の範囲内で、個人情報が第三者と共有される可能性があることを通知していますか？	○ 第 13 条 第 2 項 d	○ 第 17 条 a

2. 取得の制限

PDPD 第 3 条第 1 項では、「個人データは、適用される法令の規定に従って処理されなければならない」と定められている。法廷の規則に従うため、合法的な手段であると想定されるが、公正な手段であるかは不明なため、質問事項 7 は「△」評価としている。

PDPL 第 11 条第 1 項では、同意に基づくデータ取得が義務付けられている。一方、第 2 項では、「権限を有する党機関及び国家機関は、法令の規定に従い、指導、指揮、国家管理及び経済・社会発展の業務に供するため、自ら収集したデータ、又は共有、提供、移転、取得、利用されたデータ源から、個人データを分析及び集約することができる」と定められている。PDPD と同様に、合法的な手段であると想定されるが、公正な手段であるかは不明なため、質問事項 7 は「△」評価としている。

図表 52 「取得の制限」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
5. （企業の運用を伺う質問のため対象外） 個人情報をどのように取得していますか。		

質問	ベトナム PDPD	ベトナム PDPL
a) 本人から直接取得していますか？ b) 第三者から取得していますか？		
c) その他。該当する場合、具体的に説明してください。		
6. 個人情報の収集（直接であるか、又は第三者に代行してもらうかを問わず）を、収集の目的、又はその他関連のある、又は関連する目的を達成するために必要な範囲に限定していますか？	○ 第 3 条 第 3 項	○ 第 3 条 第 2 項
7. 個人情報の収集（直接であるか、又は第三者の代行によるものであるかを問わない）を、当該個人情報の収集を管轄する法域の要件に合致した、合法的かつ公正な手段によって行っていますか？「はい」の場合は、その内容を説明してください。	△ 第 3 条 第 1 項	△ 第 11 条

3. 個人情報の利用

個人情報の利用に関しては、PDPD・PDPL 共に、通知した目的の範囲内であること、及び本人の明示的な同意に基づくことが義務付けられている。ただし、質問事項 9(b)や 13(b)(c)にて言及されている、法律により強制的に個人情報の利用が必要な場合や、契約履行のために個人情報の利用が必要な場合については、同意の取得が不要であると定められている。

図表 53 「個人情報の利用」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
8. プライバシーステートメント及び/又は収集時に提供された通知で特定されているように、収集した個人情報の使用を（直接であるか、又はあなたの代理としての第三者の使用を通じてであるかを問わず）、情報が収集された目的、又はその他の互換性のある、又は関連する目的に限定していますか？必要に応じて、以下の空欄に説明を記入してください。	○ 第 3 条 第 3,4 項	○ 第 3 条 第 2 項
9.「いいえ」と答えた場合、収集した個人情報を、以下のいずれかの状況下で、関連性のない目的のために使用しますか？以下に記述してください。		
a) 本人の明示的な同意に基づくものですか？	○ 第 11 条 第 1 項	○ 第 9 条 第 1 項
b) 適用される法律により義務付けられている場合ですか？	○ 第 17 条	○ 第 19 条
10.（企業の運用を伺う質問のため対象外）		

質問	ベトナム PDPD	ベトナム PDPL
収集した個人情報（直接、又は貴社に変わって代行する第三者の利用を問わず）を他の個人情報管理者に開示しますか？「はい」の場合、説明してください。		
11. （企業の運用を伺う質問のため対象外） 個人情報を個人情報処理業者に転送しますか？「はい」の場合、説明してください。		
12. （質問 10 及び／又は質問 11 に「はい」と答えた場合、）開示及び／又は移転は、収集の当初の目的、又は互換性のある別の目的もしくは関連する目的を果たすために行われますか？以下に記述してください。	○ 第 3 条 第 3,4 項	○ 第 3 条 第 2 項
13. 質問 12 に「いいえ」と答えた場合、又はその他適切な場合、開示及び/又は移転は以下のいずれかの状況下で行われますか？		
a) 本人の明示的な同意に基づくものですか？	○ 第 11 条 第 1 項	○ 第 9 条 第 1 項
b) 個人から要求されたサービスや製品を提供するために必要な場合ですか？	○ 第 17 条 第 4 項	○ 第 19 条 第 1 項 d
c) 適用される法律により義務付けられている場合ですか？	○ 第 17 条	○ 第 19 条

4. 選択

同意取得時の要件として、PDPD 第 11 条第 3 項では、「データ主体の同意は、書面、音声、同意欄へのチェック、テキストメッセージ、技術的設定の選択、又はこれと同等の意思表示を示すその他の行為によって、明確かつ具体的に表明されなければならない」、PDPL 第 9 条第 3 項では、「個人データ主体の同意は、明確かつ具体的な方法により表示されなければならず、電子形式又は検証可能な形式を含め、印刷又は書面での複写が可能でなければならない」と定められている。

質問事項 17 及び 18 は満たしていると言える。しかし、質問事項 19：選択の簡単さ・手ごろさの言及がないため、「該当なし」としている。

図表 54 「選択」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
14. 個人情報の取得に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 11 条 第 4,7 項	○ 第 9 条 第 1 項 ・ 第 10 条

質問	ベトナム PDPD	ベトナム PDPL
		第 1 項
15. 個人情報の利用に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 11 条 第 4,7 項	○ 第 9 条 第 1 項 ・ 第 10 条 第 1 項
16. 個人情報の開示に関して個人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 11 条 第 4,7 項	○ 第 9 条 第 1 項 ・ 第 10 条 第 1 項
17. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示又は提供されていますか？	○ 第 11 条 第 3 項	○ 第 9 条 第 3 項
18. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それらは明瞭に表現され、容易に理解できるものですか？	○ 第 11 条 第 3 項	○ 第 9 条 第 3 項
19. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、その選択は簡単に利用でき手ごろなものですか？「はい」の場合、説明してください。	該当なし	該当なし
20. （企業の運用を伺う質問のため対象外） 必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄又は必要に応じて添付資料として説明を添えてください。		

5. 個人情報の完全性

PDPD・PDPL 共に第 3 条のデータ保護原則の中で、保有する個人情報が最新かつ正確で完全なものであること（完全性を保つこと）が義務付けられている一方、完全性を確認するための措置を講じることまでは義務付けられていない。そのため、質問事項 21 は、「△」評価としている。

【PDPD 第 3 条第 5 項】
個人データは、処理の目的に従って、更新及び補充されなければならない。
【PDPL 第 3 条第 3 項】
個人データの正確性を確保し、必要に応じて訂正、更新及び補完が行われること。個人データは、個人データ処理の目的に適合する期間保存されるものとし、法令に別段の定めがある場合を除く。

「1. 通知要件の比較」にて言及したとおり、データの処理には移転や開示も含まれているため、第 3 条のデータ保護原則は、移転後・開示後のデータにも適用されると考えられる。しかし、移転先や開示先の第三者に対し、訂正を伝えること自体は義務付けられていないため、質問事項 23 及び 24 は、「△」評価としている。

また、PDPD 第 15 条及び PDPL 第 13 条にて、個人情報の訂正権が定められているものの、不正確、不完全、又は古い情報に気づいた者がデータ管理者に対して通知する義務はないため、質問事項 25 は「該当なし」としている。

図表 55 「個人情報の完全性」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
21. 利用目的に必要な範囲内において、保有する個人情報が最新かつ正確で完全なものであることを確認するための措置を講じていますか？「はい」の場合、その内容を説明してください。	△ 第 3 条 第 5 項	△ 第 3 条 第 3 項
22. 利用目的に必要な範囲内において、不正確・不完全、又は古い個人情報を修正する仕組みがありますか？必要に応じて、以下の空欄又は添付ファイルにその内容を記載してください。	○ 第 3 条 第 5 項 ・ 第 15 条 第 1 項 b	○ 第 3 条 第 3 項 ・ 第 13 条 第 2 項
23. 不正確・不完全、又は古い情報が利用目的に影響し、情報の移転後に修正が行われる場合、個人情報が移転された個人情報処理業者、代理人、又はその他のサービス提供者に修正内容を伝えていますか？「はい」の場合は、その内容を説明してください。	△ 第 3 条 第 5 項	△ 第 3 条 第 3 項
24. 不正確・不完全、又は古い情報が利用目的に影響し、情報の開示後に訂正が行われる場合、個人情報の開示先である他の第三者に訂正を伝えていますか？「はい」の場合は、その内容を説明してください。	△ 第 3 条 第 5 項	△ 第 3 条 第 3 項
25. 個人情報の処理者、代理人、又はその他のサービス提供者が、不正確・不完全、又は古い情報に気づいた場合、貴組織に通知することを要求していますか？	該当なし	該当なし

6. セキュリティ対策

PDPD では第 3 条第 6 項、PDPL では第 3 条第 4 項に、個人データの保護のためにセキュリティ対策を講じることが義務付けられている。

【PDPD 第 3 条第 6 項】

個人データは、処理の過程において、個人データ保護に関する規定への違反からの保護及び、技術的措置を用いた事故による滅失、破壊又は損害の防止及び対策を含む、保護及び安全対策の対象とされなければならない。
【PDPL 第 3 条第 4 項】
個人データを保護するため、制度、技術及び人的側面に関する適切な措置・解決策を、同期的かつ効果的に実施すること。

ただし、講じられた保護措置が、脅かされる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明する義務は課されていないため、質問事項 28 は「該当なし」としている。質問事項 33 の有効性テストや質問事項 34 の第三者認証・その他のリスク評価も、法令上では言及されていないため、「該当なし」としている。また、いずれもデータ処理者(データ受託者)に課された義務であり、質問事項 35(b)のように、プライバシー・セキュリティ侵害に気づいた者に対する報告義務は明文化されていないため、「該当なし」としている。

図表 56 「セキュリティ対策」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
26. 情報セキュリティポリシーを導入していますか？	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項
27. 個人情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用等のリスクから個人情報を保護するために実施した物理的、技術的、管理的な保護措置について説明してください。	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項
28. 質問 27 への回答で特定した保護措置が、脅威となる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明してください。	該当なし	該当なし
29. 個人情報のセキュリティ維持の重要性を従業員にどのように認識させているか説明してください(定期的な研修や監督等)。	○ 第 26 条 第 2 項 a	○ 第 3 条 第 4 項
30. 脅威となる危害の可能性と重大性、情報の機密性、及び情報が保持される状況に応じた保護措置を実施していますか？		
a) 従業員研修・管理、その他の組織的安全対策	○ 第 26 条 第 2 項 a	○ 第 3 条 第 4 項
b) ネットワークやソフトウェアの設計、情報の処理、保存、転送、廃棄を含む情報システムと管理	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項

質問	ベトナム PDPD	ベトナム PDPL
c) 攻撃、侵入、その他のセキュリティ障害への検知、防止、対応	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項
d) 物理的セキュリティ	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項
31. 個人情報を安全に廃棄するためのポリシーを導入していますか？	○ 第 27 条 第 4 項	○ 第 14 条 第 3,4 項
32. 攻撃、侵入、その他のセキュリティ障害を検知、防止、対応するための対策を実施していますか？	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項
33. 上記の質問 32 で言及した安全対策の有効性をテストするためのプロセスを設けていますか？以下に説明してください。	該当なし	該当なし
34. 第三者認証やその他のリスク評価を利用していますか？以下に説明してください。	該当なし	該当なし
35. 個人情報を移転する情報処理業者、代理人、請負業者、又はその他のサービス提供者に対して、情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用から保護することを要求していますか？		
a) 提供される情報及びサービスの機密性に見合った情報セキュリティプログラムを導入していますか？	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項
b) 貴組織の個人情報のプライバシー又はセキュリティの侵害の発生に気付いた場合、速やかに貴組織に通知していますか？	該当なし	該当なし
c) プライバシー侵害又はセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じていますか？	○ 第 3 条 第 6 項	○ 第 3 条 第 4 項

7. アクセス及び訂正

PDPD では第 9 条第 3 項、PDPL では第 4 条第 2 項(c)に、アクセス及び訂正権が定められている。また、PDPD 第 15 条、PDPL 第 13 条に、訂正権の詳細が記載されている。

【PDPD 第 9 条第 3 項】
データ主体は、自身の個人データを閲覧し、訂正する、又は訂正を要求する権利を有する。ただし、法令に別段の定めがある場合を除く。
【PDPL 第 4 条第 2 項】
個人データのデータ主体の権利には以下が含まれる
c) 自身の個人データを閲覧し、訂正し、又は訂正を要求する権利。

しかし、法令レベルでは、身元確認の手段や情報の伝達手法等、具体的な要件は言及されていないため、質問事項 37（PDPD は(b)除く）、質問事項 38(a)、(c)（PDPD 除く）、(d)は「該当なし」としている。ただし、PDPD 第 15 条第 2 項は、訂正の要求を受けた後、できる限り速やかに訂正すること、また訂正が困難な場合には要求後 72 時間以内にその旨を通知することを義務付けているため、質問事項 37(b)及び 38(c)は「△」評価としている。また、PDPL 第 13 条第 3 項にも、訂正が困難な場合には、その旨をデータ主体に通知することが義務付けられているため、質問事項 38(e)は、PDPD・PDPL 共に「○」評価としている。

図表 57 「アクセス及び訂正」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
36. 要求があった場合、要求された個人に関する個人情報を保有しているかどうかの確認を行っていますか？以下に説明してください。	○ 第 9 条 第 3,7 項	○ 第 4 条 第 1 項 c,d
37. 要求に応じて、貴組織は個人に対して、貴組織が保有する個人情報へのアクセスを提供していますか？「はい」の場合、質問 37(a)～(e)に答え、アクセス要求の受付及び処理に関する組織の方針／手順を以下に記述する。「いいえ」の場合は、質問 38 に進んでください。		
a) アクセスを要求する個人の身元を確認する手段を講じていますか？「はい」の場合、説明してください。	該当なし	該当なし
b) 個人からのアクセス要求後、合理的な期間内でアクセスを提供していますか？「はい」の場合、詳細を説明してください。	△ 第 15 条 第 2 項	該当なし
c) 情報は、一般的に理解できる合理的な方法（読みやすい形式）で伝えられていますか？説明してください。	該当なし	該当なし
d) 情報は、本人との通常の対話形式（電子メール、同じ言語等）に適合した方法で提供されていますか？	該当なし	該当なし
e) アクセスを提供するために料金を請求しますか？「はい」の場合、その料金の根拠と、料金が過大でないことを保証する方法を以下に記述してください。	該当なし	該当なし
38. 個人が自分の情報の正確さに異議を唱え、それを修正、補完、変更、及び/又は削除することを許可していますか？この点に関する組織の方針／手順を以下に記述し、質問 38 (a)～(e)に回答してください。		
a) アクセス及び訂正の仕組みは、明確かつ目立つように表示されていますか？必要であれば、以下の空欄又は添付ファイルにその説明を記入してください。	該当なし	該当なし

質問	ベトナム PDPD	ベトナム PDPL
b) 個人情報が不完全又は不正確であると、本人から申し出があった場合、要求された訂正、追加、又は適切な場合には削除を行いますか？	○ 第 3 条 第 5 項 ・ 第 15 条 第 1 項 b	○ 第 3 条 第 3 項 ・ 第 13 条 第 2 項
c) 個人からの訂正又は削除の要求後、合理的な期間内にそのような訂正又は削除を行っていますか？	△ 第 15 条 第 2 項	該当なし
d) 訂正された個人情報のコピーを本人に提供するか、データが修正又は削除されたことを本人に確認していますか？	該当なし	該当なし
e) アクセス又は修正が拒否された場合、アクセス又は修正が提供されない理由を、アクセス又は修正の拒否に関する問い合わせ先とともに、本人に説明していますか？	○ 第 15 条 第 2 項	○ 第 13 条 第 3 項

8. 責任

責任の質問事項は、企業の具体的な運営方針について尋ねる項目が多く、法令レベルでは言及されていないため、質問事項 41、42（PDPL 除く）、43、48、49 は「該当なし」としている。

一方で、「△」評価をつけた質問事項は、以下のとおり解釈している。

質問事項 42 は、PDPL では第 4 条第 5 項に「個人データ主体の権利を実施するための請求を受領した場合、個人データ管理者及び個人データ管理者兼処理者は、法令の定める期間内に遅滞なく実施しなければならない」と定められているため、タイムリーな回答を確実に受け取るための手順が一定必要であると認識し、「△」評価としている。

質問事項 44 は、PDPD・PDPL 共に、個人情報保護のための組織的な措置は、必要に応じて更新することが義務付けられているため、従業員の教育手順も含まれると想定し、「△」評価としている。

【PDPD 第 38 条第 1 項】
個人データの処理が個人データ保護法に適合していることを示すために、組織的及び技術的な措置、ならびに適切な安全及びセキュリティ措置を実施し、必要に応じてこれらの措置を見直し、更新すること。
【PDPL 第 37 条第 1 項】
個人データ管理者の責任は、以下のとおりである。
c) 法令の規定に従い個人データを保護するための適切な管理措置及び技術措置を実施し、必要に応じてこれらの措置を見直し更新すること。

図表 58 「責任」に関する GCBPR プログラム要件との比較

質問	ベトナム PDPD	ベトナム PDPL
39. **（企業の運用を伺う質問のため対象外）** 貴組織は、グローバル CBPR プライバシー原則を確実に遵守するために、どのような手段を講じていますか？該当するものをすべてチェックし、以下に説明してください。 ・ 内部指針又は方針（該当する場合、どのように実施しているか説明） ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他		
40. **（企業の運用を伺う質問のため対象外）** 貴組織は、グローバル CBPR プライバシー原則を遵守する組織全体の責任者を任命していますか？		
41. 貴組織は、プライバシーに関する苦情を受け、調査し、対応するための手順を備えていますか？説明してください。	該当なし	該当なし
42. 貴組織は、個人が苦情に対するタイムリーな回答を確実に受け取るための手順を備えていますか？	該当なし	△ 第 4 条 第 5 項
43. 「はい」の場合、この回答には、苦情に関する改善措置の説明が含まれていますか？説明してください。	該当なし	該当なし
44. 個人情報保護に関する苦情への対応方法を含め、個人情報保護方針及び手順に関して従業員を教育するための手順を設けていますか？「はい」の場合、説明してください。	△ 第 38 条 第 1 項	△ 第 37 条 第 1 項 c
45. 個人情報の開示を要求するものも含め、司法その他の政府による召喚状、令状、命令に応じるための手続きを定めていますか？	○ 第 38 条 第 7 項	○ 第 37 条 第 1 項 i
46. 個人情報を処理する個人情報処理者、代理人、請負業者、又はその他のサービス提供者との間で、個人に対する貴組織の義務が確実に果たされるような仕組みを設けていますか（該当するものすべてにチェックを入れてください）？ ・ 内部指針又は方針 ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他（記述）	○ 第 39 条 第 1,2 項	○ 第 37 条 第 1 項 a
47. **（企業の運用を伺う質問のため対象外）**		

質問	ベトナム PDPD	ベトナム PDPL
これらの仕組みは、一般的に、個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に要求しますか？ ・ プライバシーステートメントに記載されているグローバルCBPRに準拠したプライバシーポリシーと慣行を遵守すること ・ 貴組織のプライバシーステートメントに記載されているポリシー又はプライバシー慣行と実質的に類似したプライバシー慣行を実施すること ・ 個人情報の取扱い方法に関して、貴組織に提供された指示に従うこと ・ 貴組織の同意がない限り、下請けに制限を設けること ・ 管轄区域において、フォーラムが認定したAAからからグローバルCBPRの認定を取得すること ・ その他（記述）		
48. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、貴組織の指示及び/又は契約の遵守を確保するための自己評価を提供するよう求めていますか？「はい」の場合、以下に説明してください。	該当なし	該当なし
49. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者について、貴組織の指示及び/又は合意/契約が遵守されていることを確認するために、定期的な抜き打ち検査又は監視を行っていますか？「はい」の場合、以下に記述してください。	該当なし	該当なし
50. **（企業の運用を伺う質問のため対象外）** 上記のような受領者によるグローバル CBPR システムの遵守を保証するデューディリジェンスや仕組みが現実的でない、又は不可能である状況において、個人情報を他の個人情報管理者に対して開示しますか？		

② インド

The Digital Personal Data Protection Act, 2023 (DPDP Act)を対象とし、GCBPR のプログラム要件とのマッピング分析を行った。

1. 通知要件の比較

DPDP では第 5 条第 1 項において個人情報の取得にあたって事前通知又は付随通知が義務付けられており、(i)において対象となるデータとその処理目的を通知に含めることが義務付けられている。ただし、データを収集する方法を通知することは義務付けられていないため、質問事項1は「△」評価、質問事項 1(a)は「該当なし」とした。

【DPDP 第5条第 1 項】
第 6 条に基づきデータ主体に対して同意を求めるあらゆる申請には、データ受託者がデータ主体に対して行う通知を付し、又は当該申請に先立ってその通知を行わなければならない。当該通知により、データ主体に対し次の事項を知らせるものとする。
(i) 処理されることが提案されている個人データ及びその処理目的
(ii) 第 6 条第 4 項及び第 13 条に基づく権利をデータ主体が行使する方法
(iii) 規定される方法及び様式に従い、データ主体が委員会に苦情を申し立てる方法

また、第三者への開示は、事前又は付随の通知ではなく、データ主体からの要請に基づく開示が義務付けられているのみであるため、質問事項 1(c) 及び質問事項4は「△」評価とした。

DPDP 第 6 条第 3 項では、個人情報の収集の責任者の連絡先を開示することは義務付けられているが、会社名・所在地までの開示は義務付けられていないため、質問事項1(d)は「△」評価とした。

図表 59 「通知」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
1. 上記の個人情報を管理する実務と方針について、明確で簡単にアクセスできる声明(プライバシーステートメント)提供していますか？「はい」の場合、該当するすべてのプライバシーステートメントのコピー及び/又は同ステートメントへのハイパーリンクを提供してください。	△ 第 5 条第 1 項・ 第 6 条第 3 項
a) プライバシーステートメントには、貴組織が個人情報を収集する方法が記載されていますか？	該当なし
b) このプライバシーステートメントには、個人情報を収集する目的が記載されていますか？	○ 第 5 条第 1 項(i)
c) このプライバシーステートメントは、個人情報を第三者に提供するかどうか、またその目的は何かについて、個人に通知していますか？	△ 第 11 条第 1 項(b)

質問	インド DPDP Act
d) このプライバシーステートメントでは、個人情報の収集の際に、個人情報の取扱いや慣行に関する連絡方法を含め、会社名及び所在地を開示していますか？「はい」の場合、以下に記述してください。	△ 第 6 条第 3 項
e) このプライバシーステートメントは、個人の個人情報の使用と開示に関する情報を提供していますか？	○ 第 2 章(x)・ 第 5 条第 1 項(i)・ 第 11 条第 1 項(a)(c)
f) このプライバシーステートメントには、個人が自分の個人情報にアクセスし、訂正することができるかどうか、またその方法に関する情報が記載されていますか？	○ 第 11 条・ 第 12 条
2. 以下の資格に従うことを条件に、個人情報の収集時に（直接であるか、又はあなたの代理として行動する第三者を通じてであるかを問わず）、そのような情報が収集されていることを通知しますか？	○ 第 5 条第 1 項(i)
3. 以下の資格に基づき、個人情報を収集する際、（直接であるか、代理で行動する第三者を通じてであるかを問わず）個人情報を収集する目的を明示していますか？	○ 第 5 条第 1 項(i)
4. 個人情報を収集する際に、以下の資格の範囲内で、個人情報が第三者と共有される可能性があることを通知していますか？	△ 第 11 条第 1 項(b)

2. 取得の制限

DPDP 第 4 条では、個人データの処理をデータ主体の同意もしくはその他の正当な利用目的のもとで合法的に行うことを義務付けているが、公正な手段であることを義務付ける条文は確認できないため、質問事項 7 は「△」評価とした。

図表 60 「取得の制限」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
5.（企業の運用を伺う質問のため対象外） 個人情報をどのように取得していますか。	
a) 本人から直接取得していますか？	
b) 第三者から取得していますか？	
c) その他。該当する場合、具体的に説明してください。	
6. 個人情報の収集（直接であるか、又は第三者に代行してもらうかを問わず）を、収集の目的、又はその他関連のある、	○ 第 5 条第 1 項(i)・ 第 6 条第 1 項

質問	インド DPDP Act
又は関連する目的を達成するために必要な範囲に限定していますか？	
7. 個人情報の収集（直接であるか、又は第三者の代行によるものであるかを問わない）を、当該個人情報の収集を管轄する法域の要件に合致した、合法的かつ公正な手段によって行っていますか？「はい」の場合は、その内容を説明してください。	△ 第 4 条

3. 個人情報の利用

DPDP では、第 2 条(x)において、「データの処理」に「開示」も含まれることが規定されており、第 4 条第 1 項に基づき、同意がある場合に開示が可能と規定されている。

【DPDP 第 2 条(x)】
「処理（processing）」とは、個人データに関して、デジタル個人データに対して全自動又は一部自動で行われる操作、又は一連の操作をいい、収集、記録、整理、体系化、保管、改変、検索、利用、照合又は結合、索引付け、共有、送信による開示、拡散、その他の方法による提供、制限、消去又は破壊等の操作を含む。
【DPDP 第4条第 1 項】
本法の規定に従い、かつ適法な目的のために限り、データ主体の個人データを処理することができる。その目的は、次のいずれかでなければならない。
(a) データ主体が同意を与えたもの
(b) 一定の正当な利用

収集された個人情報の処理は、同意の際に通知した目的に限定することが定められており、互換性のある目的という概念は想定されていないため、質問事項 12 は「△」評価としている。

図表 61 「個人情報の利用」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
8. プライバシーステートメント及び/又は収集時に提供された通知で特定されているように、収集した個人情報の使用を（直接であるか、又はあなたの代理としての第三者の使用を通じてであるかを問わず）、情報が収集された目的、又はその他の互換性のある、又は関連する目的に限定していますか？必要に応じて、以下の空欄に説明を記入してください。	○ 第 6 条第 1 項
9.「いいえ」と答えた場合、収集した個人情報を、以下のいずれかの状況下で、関連性のない目的のために使用しますか？以下に記述してください。	

質問	インド DPDP Act
a) 本人の明示的な同意に基づくものですか？	○ 第 6 条第 1 項
b) 適用される法律により義務付けられている場合ですか？	○ 第 7 条(d)(e)
10. **（企業の運用を伺う質問のため対象外）** 収集した個人情報（直接、又は貴社に変わって代行する第三者の利用を問わず）を他の個人情報管理者に開示しますか？「はい」の場合、説明してください。	
11. **（企業の運用を伺う質問のため対象外）** 個人情報を個人情報処理業者に転送しますか？「はい」の場合、説明してください。	
12. （質問 10 及び／又は質問 11 に「はい」と答えた場合、）開示及び／又は移転は、収集の当初の目的、又は互換性のある別の目的もしくは関連する目的を果たすために行われますか？以下に記述してください。	△ 第 6 条第 1 項・ 第 8 条第 2 項
13. 質問 12 に「いいえ」と答えた場合、又はその他適切な場合、開示及び/又は移転は以下のいずれかの状況下で行われますか？	
a) 本人の明示的な同意に基づくものですか？	○ 第 6 条第 1 項
b) 個人から要求されたサービスや製品を提供するために必要な場合ですか？	○ 第 7 条(a)
c) 適用される法律により義務付けられている場合ですか？	○ 第 7 条(d)(e)

4. **選択**

個人情報の取得、利用、開示は第 2 条(x)に基づいて「データの処理」としてまとめられており、第 6 条にて、データ処理に対するデータ主体の選択権が規定されている。ただし、同意の撤回については、同意の付与時と同等の容易さであることが定められているのみであるため、質問事項 19 は「△」評価とした。

【DPDP 第 6 条第 1 項】
データ主体が与える同意は、自由意思に基づき、特定され、十分な情報に基づくものであり、無条件かつ明確で、明確な積極的行為により、曖昧でないものでなければならない。また、当該同意は、特定の目的のために自己の個人データを処理することへの同意を示すものであり、その特定目的に必要な個人データに限られなければならない。
【DPDP 第 6 条第 3 項】
本法又は本法に基づき制定された規則の規定に基づくすべての同意の要請は、明確かつ平易な言葉でデータ主体に提示されなければならない。あわせて、当該要請を英語又は憲法別表第 8 に定めるいずれかの言語で閲覧できる選択肢を付与し、さらに、本法の規定に基づく

権利行使のためにデータ主体からの連絡に対応する、(該当する場合は)データ保護責任者の連絡先、又はデータ受託者が権限を付与したその他の者の連絡先を提供しなければならない。

【DPDP 第 6 条第 4 項】

データ主体が与えた同意が個人データ処理の根拠である場合、当該データ主体は、いつでも同意を撤回する権利を有する。この撤回は、同意を与えたときと同程度に容易でなければならない。

【DPDP 第 6 条第 6 項】

データ主体が(5)項に基づき個人データ処理への同意を撤回した場合、データ受託者は、合理的な期間内に、インドにおいてその時点で施行されている本法もしくは本法に基づく規則、又はその他の法律の規定により、当該同意なしに処理することが要求又は許可される場合を除き、当該データ主体の個人データの処理を停止し、かつ自己のデータ処理者にも停止させなければならない。

【DPDP 第 6 条第 7 項】

データ主体は、同意管理者を通じて、データ受託者に対する同意を付与し、管理し、見直し、又は撤回することができる。

図表 62 「選択」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
14. 個人情報の取得に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 6 条第 1 項・ 第 6 条第 4 項・ 第 6 条第 6 項
15. 個人情報の利用に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 6 条第 1 項・ 第 6 条第 4 項・ 第 6 条第 6 項
16. 個人情報の開示に関して個人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 6 条第 1 項・ 第 6 条第 4 項・ 第 6 条第 6 項
17. 個人情報の取得(質問 14)、利用(質問 15)、開示(質問 16)を制限する選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示又は提供されていますか？	○ 第 6 条第 3 項
18. 個人情報の取得(質問 14)、利用(質問 15)、開示(質問 16)を制限する権限を与える選択肢を個人に提供している場合、それらは明瞭に表現され、容易に理解できるものですか？	○ 第 6 条第 3 項

質問	インド DPDP Act
19. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、その選択は簡単に利用でき手ごろなものですか？「はい」の場合、説明してください。	△ 第 6 条第 4 項・ 第 6 条第 7 項
20. **（企業の運用を伺う質問のため対象外）** 必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄又は必要に応じて添付資料として説明を添えてください。	

5. 個人情報の完全性

DPDP 第 8 条第 3 項では、データ主体に影響を与える決定を行うために使用された場合、又は他のデータ受託者に開示される場合には、データの完全性、正確性、及び一貫性を確保することがデータ受託者に義務付けられている。ただし、その他の場合には本項は適用されないため、質問事項 21 及び 22 は「△」評価としている。

【DPDP 第 8 条第 3 項】
データ受託者により処理される個人データが、次のいずれかに該当する可能性がある場合、
(a) データ主体に影響を及ぼす決定を行うために利用される場合、又は
(b) 他のデータ受託者に開示される場合、
当該個人データを処理するデータ受託者は、その完全性、正確性及び一貫性を確保しなければならない。

また、移転先や開示先の第三者に対し、移転・開示後も継続して訂正を伝えること（質問事項 23 おおよび 24）、不正確、不完全、または古い情報に気づいた者がデータ管理者に対して通知すること（質問事項 25）は義務付けられていないため、質問事項 23～25 は「該当なし」としている。

図表 63 「個人情報の完全性」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
21. 利用目的に必要な範囲内において、保有する個人情報が最新かつ正確で完全なものであることを確認するための措置を講じていますか？「はい」の場合、その内容を説明してください。	△ 第 8 条第 3 項
22. 利用目的に必要な範囲内において、不正確・不完全、又は古い個人情報を修正する仕組みがありますか？必要に応じて、以下の空欄又は添付ファイルにその内容を記載してください。	△ 第 8 条第 3 項

質問	インド DPDP Act
23. 不正確・不完全、又は古い情報が利用目的に影響し、情報の移転後に修正が行われる場合、個人情報が移転された個人情報処理業者、代理人、又はその他のサービス提供者に修正内容を伝えていますか？「はい」の場合は、その内容を説明してください。	該当なし
24. 不正確・不完全、又は古い情報が利用目的に影響し、情報の開示後に訂正が行われる場合、個人情報の開示先である他の第三者に訂正を伝えていますか？「はい」の場合は、その内容を説明してください。	該当なし
25. 個人情報の処理者、代理人、又はその他のサービス提供者が、不正確・不完全、又は古い情報に気づいた場合、貴組織に通知することを要求していますか？	該当なし

6. セキュリティ対策

DPDPは、第10条第1項の基準に基づき、政府が重要データ受託者（SDF：Significant Data Fiduciary）を指定できることを定めている。質問事項 28, 33, 34 が要求するデータ受託者のセキュリティ対策は、SDF に指定されたデータ受託者にのみ義務付けられているため、いずれも「△」評価としている。

第8条第4項及び第5項において、データ受託者に対して技術的・組織的なセキュリティ対策を講じることが義務付けられているが、具体的な記述は削除や漏洩時の対策等に限定されているため、質問事項 26, 30, 31, 32 はいずれも「△」評価としている。

また、第8条第5項はセキュリティ対策の実施を求めているものの、それが提供される情報及びサービスの機微性に見合っていることまでは要求していないため、質問事項 35(a)は「△」評価としている。

【DPDP 第4条第4項】
データ受託者は、本法及び本法に基づき制定された規則の規定が実効的に遵守されることを確保するため、適切な技術的及び組織的措置を実施しなければならない。
【DPDP 第4条第5項】
データ受託者は、自己が保有し、又は管理下に置く個人データ（自己により、又は自己のためにデータ処理者によって行われるいかなる処理に関するものを含む）を、個人データ侵害を防止するための合理的なセキュリティ上の保護措置を講じることにより保護しなければならない。

また、個人情報のセキュリティ維持の重要性を従業員に認識させること（質問事項 29）、個人情報のプライバシーまたはセキュリティの侵害の発生に気付いた場合、速やかにデータ処理者に通知すること（質問事項 35(b)）、プライバシー侵害またはセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じること（質問事項 35(c)）は法令上で義務付けられていないため、「該当なし」としている。

図表 64 「セキュリティ対策」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
26. 情報セキュリティポリシーを導入していますか？	△ 第 8 条第 4, 5 項
27. 個人情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用等のリスクから個人情報を保護するために実施した物理的、技術的、管理的な保護措置について説明してください。	○ 第 8 条第 4, 5 項
28. 質問 27 への回答で特定した保護措置が、脅威となる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明してください。	△ 第 10 条第 2 項(c)(i)
29. 個人情報のセキュリティ維持の重要性を従業員にどのように認識させているか説明してください（定期的な研修や監督等）。	該当なし
30. 脅威となる危害の可能性と重大性、情報の機密性、及び情報が保持される状況に応じた保護措置を実施していますか？	
a) 従業員研修・管理、その他の組織的安全対策	△ 第 8 条第 4 項
b) ネットワークやソフトウェアの設計、情報の処理、保存、転送、廃棄を含む情報システムと管理	△ 第 8 条第 4, 7, 8 項
c) 攻撃、侵入、その他のセキュリティ障害への検知、防止、対応	△ 第 8 条第 5, 6 項
d) 物理的セキュリティ	△ 第 8 条第 5 項
31. 個人情報を安全に廃棄するためのポリシーを導入していますか？	△ 第 8 条第 7 項(a)(b)
32. 攻撃、侵入、その他のセキュリティ障害を検知、防止、対応するための対策を実施していますか？	△ 第 8 条第 5, 6 項
33. 上記の質問 32 で言及した安全対策の有効性をテストするためのプロセスを設けていますか？以下に説明してください。	△ 第 10 条第 2 項 (b)(c)(ii)
34. 第三者認証やその他のリスク評価を利用していますか？以下に説明してください。	△ 第 10 条第 2 項 (b)(c)(i)(ii)
35. 個人情報を移転する情報処理業者、代理人、請負業者、はその他のサービス提供者に対して、情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用から保護することを要求していますか？	
a) 提供される情報及びサービスの機密性に見合った情報セキュリティプログラムを導入していますか？	△ 第 8 条第 5 項

質問	インド DPDP Act
b) 貴組織の個人情報のプライバシー又はセキュリティの侵害の発生に気付いた場合、速やかに貴組織に通知していますか？	該当なし
c) プライバシー侵害又はセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じていますか？	該当なし

7. アクセス及び訂正

データ主体からデータ受託者に対する個人情報のアクセス及び訂正は、それぞれ第 11 条と第 12 条で規定されている。

ただし、アクセスや訂正の提供手段や期限までは、法令上では具体的に定められていないため、質問事項 37、質問事項 38(a)、(c)、(d)、(e)は「該当なし」としている。

図表 65 「アクセス及び訂正」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
36. 要求があった場合、要求された個人に関する個人情報を保有しているかどうかの確認を行っていますか？以下に説明してください。	○ 第 11 条第 1 項(a)
37. 要求に応じて、貴組織は個人に対して、貴組織が保有する個人情報へのアクセスを提供していますか？「はい」の場合、質問 37(a)～(e)に答え、アクセス要求の受付及び処理に関する組織の方針／手順を以下に記述する。「いいえ」の場合は、質問 38 に進んでください。	
a) アクセスを要求する個人の身元を確認する手段を講じていますか？「はい」の場合、説明してください。	該当なし
b) 個人からのアクセス要求後、合理的な期間内でアクセスを提供していますか？「はい」の場合、詳細を説明してください。	該当なし
c) 情報は、一般的に理解できる合理的な方法（読みやすい形式）で伝えられていますか？説明してください。	該当なし
d) 情報は、本人との通常の対話形式（電子メール、同じ言語等）に適合した方法で提供されていますか？	該当なし
e) アクセスを提供するために料金を請求しますか？「はい」の場合、その料金の根拠と、料金が過大でないことを保証する方法を以下に記述してください。	該当なし
38. 個人が自分の情報の正確さに異議を唱え、それを修正、補完、変更、及び/又は削除することを許可しています	

質問	インド DPDP Act
か？この点に関する組織の方針／手順を以下に記述し、質問 38 (a)～(e)に回答してください。	
a) アクセス及び訂正の仕組みは、明確かつ目立つように表示されていますか？必要であれば、以下の空欄又は添付ファイルにその説明を記入してください。	該当なし
b) 個人情報が不完全又は不正確であると、本人から申し出があった場合、要求された訂正、追加、又は適切な場合には削除を行いますか？	○ 第 12 条第 2, 3 項
c) 個人からの訂正又は削除の要求後、合理的な期間内にそのような訂正又は削除を行っていますか？	該当なし
d) 訂正された個人情報のコピーを本人に提供するか、データが修正又は削除されたことを本人に確認していますか？	該当なし
e) アクセス又は修正が拒否された場合、アクセス又は修正が提供されない理由を、アクセス又は修正の拒否に関する問い合わせ先とともに、本人に説明していますか？	該当なし

8. 責任

個人情報の処理者、代理人、請負業者等がデータ処理者の指示や契約等を遵守していることを確認する義務は、第 10 条第 2 項において重要データ受託者（SDF：Significant Data Fiduciary）に対してのみ義務付けられているため、質問事項 49 は「△」評価としている。また、苦情に関する改善措置の説明を含めること（質問事項 43）、個人情報保護に関する苦情への対応方法を含め、個人情報保護方針および手順に関して従業員を教育するための手順を設けること（質問事項 44）、個人情報の開示を要求するものも含め、司法その他の政府による召喚状、令状、命令に応じるための手続きを定めること（質問事項 45）、個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、データ処理者の指示および/または契約/契約の遵守を確認するための自己評価を提供させること（質問事項 48）は、法令上で言及されていないため、「該当なし」としている。

図表 66 「責任」に関する GCBPR プログラム要件との比較

質問	インド DPDP Act
39. （企業の運用を伺う質問のため対象外） 貴組織は、グローバル CBPR プライバシー原則を確実に遵守するために、どのような手段を講じていますか？該当するものをすべてチェックし、以下に説明してください。 ・ 内部指針又は方針（該当する場合、どのように実施し	

質問	インド DPDP Act
ているか説明） ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他	
40. （企業の運用を伺う質問のため対象外） 貴組織は、グローバル CBPR プライバシー原則を遵守する組織全体の責任者を任命していますか？	
41. 貴組織は、プライバシーに関する苦情を受け、調査し、対応するための手順を備えていますか？説明してください。	○ 第 8 条第 10 項・13 条第 1 項
42. 貴組織は、個人が苦情に対するタイムリーな回答を確実に受け取るための手順を備えていますか？	○ 第 13 条第 2 項
43. 「はい」の場合、この回答には、苦情に関する改善措置の説明が含まれていますか？説明してください。	該当なし
44. 個人情報保護に関する苦情への対応方法を含め、個人情報保護方針及び手順に関して従業員を教育するための手順を設けていますか？「はい」の場合、説明してください。	該当なし
45. 個人情報の開示を要求するものも含め、司法その他の政府による召喚状、令状、命令に応じるための手続きを定めていますか？	該当なし
46. 個人情報を処理する個人情報処理者、代理人、請負業者、又はその他のサービス提供者との間で、個人に対する貴組織の義務が確実に果たされるような仕組みを設けていますか（該当するものすべてにチェックを入れてください）？ ・ 内部指針又は方針 ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他（記述）	○ 第 8 条 1, 2 項
47. （企業の運用を伺う質問のため対象外） これらの仕組みは、一般的に、個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に要求しますか？ ・ プライバシーステートメントに記載されているグローバルCBPRに準拠したプライバシーポリシーと慣行を遵守すること ・ 貴組織のプライバシーステートメントに記載されているポリシー又はプライバシー慣行と実質的に類似したプライバシー慣行を実施すること ・ 個人情報の取扱い方法に関して、貴組織に提供され	

質問	インド DPDP Act
た指示に従うこと ・ 貴組織の同意がない限り、下請けに制限を設けること ・ 管轄区域において、フォーラムが認定したAAからからグローバルCBPRの認定を取得すること ・ その他（記述）	
48. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、貴組織の指示及び/又は契約の遵守を確保するための自己評価を提供するよう求めていますか？「はい」の場合、以下に説明してください。	該当なし
49. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者について、貴組織の指示及び/又は合意/契約が遵守されていることを確認するために、定期的な抜き打ち検査又は監視を行っていますか？「はい」の場合、以下に記述してください。	△ 第 8 条第 1, 2 項・ 第 10 条第 2 項 (b)(c)(ii)
50. （企業の運用を伺う質問のため対象外） 上記のような受領者によるグローバル CBPR システムの遵守を保証するデューディリジェンスや仕組みが現実的でない、又は不可能である状況において、個人情報を他の個人情報管理者に対して開示しますか？	

③ インドネシア

Law No. 27 of 2022 on Personal Data Protection (PDP Law)を対象とし、GCBPR のプログラム要件とのマッピング分析を行った。

1. 通知要件の比較

PDP Law では、通知要件が定められた条文はなく、データ処理に関する同意を取得する条件として通知すべき項目が定められている。なお、データの処理には、契約履行や生命保護等の理由がある場合を除き、データ主体からの同意を取得することが義務付けられている（第 20 条第 1,2 項）。そのため、同意取得時の通知項目（第 21 条第 1 項）を PDP Law の通知要件として解釈している。

また、データ処理の定義には第 16 条第 1 項にて以下のとおり定められており、「移転」が含まれていることから、質問事項 1(c)、2、3、4 で言及されている第三者提供に関する通知要件についても、第 21 条第 1 項に含まれていると認識している。

【PDP Law 第 16 条第 1 項】
個人データの処理には、以下が含まれる:
a. 取得及び収集
b. 加工及び分析
c. 保存
d. 修正及び更新
e. 表示、公表、移転、普及、開示、及び／又は
f. 削除又は破棄

質問事項 1(a)個人情報を収集する方法の通知は、明確に収集方法を通知するとの記載がないものの、同意取得時に処理の適法性(a)と処理目的(b)を通知する必要があることから、収集方法がその一環で通知されることを見越し、「△」評価としている。

また、質問事項 1(c)第三者提供の有無・目的、及び 1(d)連絡方法・会社名・所在地、質問事項 4 第三者提供の有無の通知について、第三者提供の有無や、連絡方法・所在地等具体的な情報の通知までは条文に定められていないため、「△」評価としている。

質問事項 1(e)個人の個人情報の使用と開示に関する情報、及び 1(f)アクセス・訂正の可否・方法の通知も、データ主体の権利が通知されるのみであり、具体的な使用と開示に関する情報や、アクセス・訂正に関する方法の通知までは条文に定められていないため、「△」評価としている。

図表 67 「通知」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
1. 上記の個人情報を管理する実務と方針について、明確で簡単にアクセスできる声明（プライバシーステートメント）提供していますか？「はい」の場合、該当するすべてのプライバシーステートメントのコピー及び/又は同ステートメントへのハイパーリンクを提供してください。	○ 第 20 条第 2 項 a
a) プライバシーステートメントには、貴組織が個人情報を収集する方法が記載されていますか？	△ 第 21 条第 1 項 a,b
b) このプライバシーステートメントには、個人情報を収集する目的が記載されていますか？	○ 第 21 条第 1 項 b
c) このプライバシーステートメントは、個人情報を第三者に提供するかどうか、またその目的は何かについて、個人に通知していますか？	△ 第 5 条
d) このプライバシーステートメントでは、個人情報の収集の際に、個人情報の取扱いや慣行に関する連絡方法を含め、会社名及び所在地を開示していますか？「はい」の場合、以下に記述してください。	△ 第 5 条
e) このプライバシーステートメントは、個人の個人情報の使用と開示に関する情報を提供していますか？	△ 第 21 条第 1 項 g 第 6 条
f) このプライバシーステートメントには、個人が自分の個人情報にアクセスし、訂正することができるかどうか、またその方法に関する情報が記載されていますか？	△ 第 21 条第 1 項 g 第 6 条
2. 以下の資格に従うことを条件に、個人情報の収集時に（直接であるか、又はあなたの代理として行動する第三者を通じてであるかを問わず）、そのような情報が収集されていることを通知しますか？	○ 第 21 条第 1 項 c
3. 以下の資格に基づき、個人情報を収集する際、（直接であるか、代理で行動する第三者を通じてであるかを問わず）個人情報を収集する目的を明示していますか？	○ 第 21 条第 1 項 b
4. 個人情報を収集する際に、以下の資格の範囲内で、個人情報が第三者と共有される可能性があることを通知していますか？	△ 第 27 条

2. 取得の制限

PDP Law 第 27 条にて「個人データ管理者は、個人データの処理を限定的かつ特定的で、法的に適法であり、かつ透明性のある方法で実施しなければならない」と定められている。合法的であることは義務付けられているが、公正な手段であるかは不明なため、質問事項 7 は「△」評価としている。

図表 68 「取得の制限」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
5. （企業の運用を伺う質問のため対象外） 個人情報をどのように取得していますか。	
a) 本人から直接取得していますか？	
b) 第三者から取得していますか？	
c) その他。該当する場合、具体的に説明してください。	
6. 個人情報の収集（直接であるか、又は第三者に代行してもらうかを問わず）を、収集の目的、又はその他関連のある、又は関連する目的を達成するために必要な範囲に限定していますか？	○ 第 28 条
7. 個人情報の収集（直接であるか、又は第三者の代行によるものであるかを問わない）を、当該個人情報の収集を管轄する法域の要件に合致した、合法的かつ公正な手段によって行っていますか？「はい」の場合は、その内容を説明してください。	△ 第 27 条

3. 個人情報の利用

目的の範囲内で個人情報を処理（利用を含む）することが義務付けられている。また、質問事項 9 や 13 にて言及されているとおり、本人の明示的な同意がある場合や、法律により強制的に個人情報の利用が必要な場合、契約履行のために個人情報の利用が必要な場合については、個人情報の処理（利用）が認められている。

図表 69 「個人情報の利用」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
8. プライバシーステートメント及び/又は収集時に提供された通知で特定されているように、収集した個人情報の使用を（直接であるか、又はあなたの代理としての第三者の使用を通じてであるかを問わず）、情報が収集された目的、又はその他の互換性のある、又は関連する目的に限定していますか？必要に応じて、以下の空欄に説明を記入してください。	○ 第 28 条
9.「いいえ」と答えた場合、収集した個人情報を、以下のいずれかの状況下で、関連性のない目的のために使用しますか？以下に記述してください。	
a) 本人の明示的な同意に基づくものですか？	○ 第 20 条第 1 項 a

質問	インドネシア PDP Law
b) 適用される法律により義務付けられている場合ですか？	○ 第 20 条第 1 項 d,e,f
10. **（企業の運用を伺う質問のため対象外）** 収集した個人情報（直接、又は貴社に変わって代行する第三者の利用を問わず）を他の個人情報管理者に開示しますか？「はい」の場合、説明してください。	
11. **（企業の運用を伺う質問のため対象外）** 個人情報を個人情報処理業者に転送しますか？「はい」の場合、説明してください。	
12. 収集した個人情報（直接、又は貴社に変わって代行する第三者の利用を問わず）を他の個人情報管理者に開示しますか？「はい」の場合、説明してください。	○ 第 28 条
13. 質問 12 に「いいえ」と答えた場合、又はその他適切な場合、開示及び/又は移転は以下のいずれかの状況下で行われますか？	
a) 本人の明示的な同意に基づくものですか？	○ 第 20 条第 1 項 a
b) 個人から要求されたサービスや製品を提供するために必要な場合ですか？	○ 第 20 条第 1 項 b,c
c) 適用される法律により義務付けられている場合ですか？	○ 第 20 条第 1 項 d,e,f

4. 選択

同意取得時の要件として、PDP Law 第 22 条第 4 項では、以下のとおり定められている。

【PDP Law 第 22 条第 4 項】
第 1 項に基づく同意が複数の目的を含む場合、当該同意の要請は、
a. 他の事項と明確に区別できるものでなければならない。
b. 理解可能で、かつ容易にアクセスできる形式で作成されなければならない。
c. 簡潔で明確な言語を使用しなければならない。

そのため、質問事項 17 及び 18 は満たしていると言える。しかし、質問事項 19:選択の簡単さ・手ごろさについては、「理解可能で、かつ容易にアクセスできる形式」との指定があるものの、「手ごろさ」に関する言及がないため、「△」評価としている。

図表 70 「選択」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
14. 個人情報の取得に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 8,9,10,11 条
15. 個人情報の利用に関して本人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 8,9,10,11 条
16. 個人情報の開示に関して個人が選択できる方法を提供していますか？「はい」の場合、その仕組みを説明してください。	○ 第 8,9,10,11 条
17. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示又は提供されていますか？	○ 第 22 条第 4 項 a
18. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する権限を与える選択肢を個人に提供している場合、それらは明瞭に表現され、容易に理解できるものですか？	○ 第 22 条第 4 項 b,c
19. 個人情報の取得（質問 14）、利用（質問 15）、開示（質問 16）を制限する選択肢を個人に提供している場合、その選択は簡単に利用でき手ごろなものですか？「はい」の場合、説明してください。	△ 第 22 条第 4 項 b,c
20. **（企業の運用を伺う質問のため対象外）** 必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄又は必要に応じて添付資料として説明を添えてください。	

5. 個人情報の完全性

PDP Law では、第 29 条にて個人情報の完全性、第 6 条にてアクセス・訂正権が定められている。データ主体の要求に応じてデータを訂正した後は、データ主体に対してその旨を通知する必要がある（第 30 条第 2 項）が、個人情報の移転先や開示先に通知する義務は定められていないため、質問事項 23、24 は「該当なし」としている。また、個人情報の訂正権が定められているものの、不正確、不完全、または古い情報に気づいた者がデータ管理者に対して通知する義務はないため、質問事項 25 は「該当なし」としている。

図表 71 「個人情報の完全性」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
21. 利用目的に必要な範囲内において、保有する個人情報が最新かつ正確で完全なものであることを確認するための措置を講じていますか？「はい」の場合、その内容を説明してください。	○ 第 29 条第 1,2 項
22. 利用目的に必要な範囲内において、不正確・不完全、又は古い個人情報を修正する仕組みがありますか？必要に応じて、以下の空欄又は添付ファイルにその内容を記載してください。	○ 第 6 条
23. 不正確・不完全、又は古い情報が利用目的に影響し、情報の移転後に修正が行われる場合、個人情報が移転された個人情報処理業者、代理人、又はその他のサービス提供者に修正内容を伝えていますか？「はい」の場合は、その内容を説明してください。	該当なし
24. 不正確・不完全、又は古い情報が利用目的に影響し、情報の開示後に訂正が行われる場合、個人情報の開示先である他の第三者に訂正を伝えていますか？「はい」の場合は、その内容を説明してください。	該当なし
25. 個人情報の処理者、代理人、又はその他のサービス提供者が、不正確・不完全、又は古い情報に気づいた場合、貴組織に通知することを要求していますか？	該当なし

6. セキュリティ対策

PDP Law 第 35 条では、以下のとおりセキュリティ対策が義務付けられている。技術的及び運用上の措置が定められているものの、物理的措置は言及がないため、質問事項 30(d)は「△」評価としている。また、セーフガードの有効性をテストするためのプロセスの導入までは指定されていないため、質問事項 33 は「該当なし」としている。

【PDP Law 第 35 条】
個人データ管理者は、自らが処理する個人データを保護し、その安全性を確保しなければならず、そのために次の措置を講じるものとする。
a. 法令の規定に反する個人データの処理の妨害から個人データを保護するための、技術的及び運用上の措置を策定し、かつ実施すること。
b. 個人データの処理において保護されるべき個人データの性質及びリスクを考慮して、個人データの安全性の程度を決定すること。

そのほか、第 34 条ではデータ処理における影響評価、第 37 条ではデータ処理に関わる者への監督義務、第 46 条ではデータ保護に失敗した場合の対応について定められている。一方、いずれもデータ処理者（データ受託者）に課された義務であり、質問事項 35(b)のように、

プライバシー・セキュリティ侵害に気づいた者に対する報告義務は明文化されていないため、「該当なし」としている。

図表 72 「セキュリティ対策」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
26. 情報セキュリティポリシーを導入していますか？	○ 第 35 条 a
27. 個人情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用等のリスクから個人情報を保護するために実施した物理的、技術的、管理的な保護措置について説明してください。	○ 第 35 条 a
28. 質問 27 への回答で特定した保護措置が、脅威となる危害の可能性と重大性、情報の機密性、及び情報が保有される状況にどのように比例しているかを説明してください。	○ 第 34 条、第 35 条 b
29. 個人情報のセキュリティ維持の重要性を従業員にどのように認識させているか説明してください（定期的な研修や監督等）。	○ 第 37 条
30. 脅威となる危害の可能性と重大性、情報の機密性、及び情報が保持される状況に応じた保護措置を実施していますか？	
a) 従業員研修・管理、その他の組織的安全対策	○ 第 37 条
b) ネットワークやソフトウェアの設計、情報の処理、保存、転送、廃棄を含む情報システムと管理	○ 第 39 条第 2 項
c) 攻撃、侵入、その他のセキュリティ障害への検知、防止、対応	○ 第 39 条第 1 項
d) 物理的セキュリティ	△ 第 35 条 a
31. 個人情報を安全に廃棄するためのポリシーを導入していますか？	○ 第 16 条第 2 項 g
32. 攻撃、侵入、その他のセキュリティ障害を検知、防止、対応するための対策を実施していますか？	○ 第 35 条 a
33. 上記の質問 32 で言及した安全対策の有効性をテストするためのプロセスを設けていますか？以下に説明してください。	該当なし
34. 第三者認証やその他のリスク評価を利用していますか？以下に説明してください。	○ 第 34 条第 1 項
35. 個人情報を移転する情報処理業者、代理人、請負業者、又はその他のサービス提供者に対して、情報の紛失、不正アクセス、破壊、使用、改ざん、開示、又はその他の悪用から保護することを要求していますか？	

質問	インドネシア PDP Law
a) 提供される情報及びサービスの機密性に見合った情報セキュリティプログラムを導入していますか？	○ 第 34 条、第 35 条 b
b) 貴組織の個人情報のプライバシー又はセキュリティの侵害の発生に気付いた場合、速やかに貴組織に通知していますか？	該当なし
c) プライバシー侵害又はセキュリティ侵害の原因となったセキュリティ上の不具合を修正／対処するために、直ちに措置を講じていますか？	○ 第 46 条第 2 項 c

7. アクセス及び訂正

PDP Law では第 7 条にアクセス権、第 8 条に訂正権、第 32 条にアクセス権の詳細、第 30 条に訂正権の詳細が定められている。また、第 13 条では、データ主体への情報提供の方法が定められている。

【PDP Law 第 7 条】
個人データ主体は、法令の規定に従い、自身に関する個人データにアクセスし、及びその写しを取得する権利を有する。
個人データの写しを取得する権利は、原則として無償で行われるものとする。ただし、一定の条件において費用を要する場合を除く。
【PDP Law 第 8 条】
個人データ主体は、法令の規定に従い、自身に関する個人データの処理を終了させ、消去し、及び／又は破棄する権利を有する。

法令レベルでは、質問事項 37(a)の身元確認の手段や、38(a)のアクセス・訂正の仕組みの表示といった具体的な要件は言及されていないため、「該当なし」としている。また、第 7 条にあるとおり、原則として無償でアクセスできるものの、一定の条件で費用を要する場合は除外されているため、質問事項 37(e)は「△」評価としている。

質問事項 38(e)は、第 33 条にデータのアクセス・訂正要求を拒否できる要件が定められているものの、拒否した際に理由を説明する義務は言及されていないため、「該当なし」としている。

図表 73 「アクセス及び訂正」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
36. 要求があった場合、要求された個人に関する個人情報を保有しているかどうかの確認を行っていますか？以下に説明してください。	○ 第 7 条
37. 要求に応じて、貴組織は個人に対して、貴組織が保有する個人情報へのアクセスを提供していますか？「はい」の場合、質問 37(a)～(e)に答え、アクセス要求の受付及び処理に関する組織の方針／手順を以下に記述する。「いいえ」の場合は、質問 38 に進んでください。	
a) アクセスを要求する個人の身元を確認する手段を講じていますか？「はい」の場合、説明してください。	該当なし
b) 個人からのアクセス要求後、合理的な期間内でアクセスを提供していますか？「はい」の場合、詳細を説明してください。	○ 第 32 条第 2 項
c) 情報は、一般的に理解できる合理的な方法（読みやすい形式）で伝えられていますか？説明してください。	○ 第 13 条第 1 項
d) 情報は、本人との通常の対話形式（電子メール、同じ言語等）に適合した方法で提供されていますか？	○ 第 13 項第 1 項
e) アクセスを提供するために料金を請求しますか？「はい」の場合、その料金の根拠と、料金が過大でないことを保証する方法を以下に記述してください。	△ 第 7 条
38. 個人が自分の情報の正確さに異議を唱え、それを修正、補完、変更、及び/又は削除することを許可していますか？この点に関する組織の方針／手順を以下に記述し、質問 38 (a)～(e)に回答してください。	
a) アクセス及び訂正の仕組みは、明確かつ目立つように表示されていますか？必要であれば、以下の空欄又は添付ファイルにその説明を記入してください。	該当なし
b) 個人情報が不完全又は不正確であると、本人から申し出があった場合、要求された訂正、追加、又は適切な場合には削除を行いますか？	○ 第 8 条、 第 30 条第 1 項
c) 個人からの訂正又は削除の要求後、合理的な期間内にそのような訂正又は削除を行っていますか？	○ 第 30 条第 1 項
d) 訂正された個人情報のコピーを本人に提供するか、データが修正又は削除されたことを本人に確認していますか？	○ 第 30 条第 2 項
e) アクセス又は修正が拒否された場合、アクセス又は修正が提供されない理由を、アクセス又は修正の拒否に関する問い合わせ先とともに、本人に説明していますか？	該当なし

8. 責任

苦情の権利に関しては、PDP Law では第 12 条に以下のとおり定められている。しかし、データ主体の権利を定めた条文であり、データ処理者に苦情の対応手順や改善措置の説明等を義務付けてはいないため、質問事項 41～43 は「△」評価としている。質問事項 45 の司法その他の政府による召喚状、令状、命令に応じるための手続きを定めることに関しては、法令上で言及させていないため、「該当なし」としている。

【PDP Law 第 12 条】
(1)
個人データ主体は、法令の規定に従い、自身に関する個人データの処理に関する違反について、訴えを提起し、又は損害賠償を受ける権利を有する。
(2)
前項にいう個人データ処理の違反及び損害賠償の賦課手続に関する詳細な規定は、政府規則により定めるものとする。

また、PDP Law 第 37 条では以下のとおり、個人データ管理者に対して監督義務が定められている。しかし、質問事項 44 のように、個人情報保護に関する苦情への対応方法を含めて従業員への教育手順を設けることや、質問事項 48 のように、その他のデータ処理者に対して自己評価を提供させることまでは義務付けていないため、質問事項 44、48 は「△」評価としている。

【PDP Law 第 37 条】
個人データ管理者は、自己の管理下において個人データの処理に関与するすべての者に対して、監督を行わなければならない。

図表 74 「責任」に関する GCBPR プログラム要件との比較

質問	インドネシア PDP Law
39. （企業の運用を伺う質問のため対象外） 貴組織は、グローバル CBPR プライバシー原則を確実に遵守するために、どのような手段を講じていますか？該当するものをすべてチェックし、以下に説明してください。 ・ 内部指針又は方針（該当する場合、どのように実施しているか説明） ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他	
40. （企業の運用を伺う質問のため対象外）	

質問	インドネシア PDP Law
貴組織は、グローバル CBPR プライバシー原則を遵守する組織全体の責任者を任命していますか？	
41. 貴組織は、プライバシーに関する苦情を受け、調査し、対応するための手順を備えていますか？説明してください。	△ 第 12 条
42. 貴組織は、個人が苦情に対するタイムリーな回答を確実に受け取るための手順を備えていますか？	△ 第 12 条
43. 「はい」の場合、この回答には、苦情に関する改善措置の説明が含まれていますか？説明してください。	△ 第 12 条
44. 個人情報保護に関する苦情への対応方法を含め、個人情報保護方針及び手順に関して従業員を教育するための手順を設けていますか？「はい」の場合、説明してください。	△ 第 37 条
45. 個人情報の開示を要求するものも含め、司法その他の政府による召喚状、令状、命令に応じるための手続きを定めることを義務付けているか	該当なし
46. 個人情報を処理する個人情報処理者、代理人、請負業者、又はその他のサービス提供者との間で、個人に対する貴組織の義務が確実に果たされるような仕組みを設けていますか（該当するものすべてにチェックを入れてください）？ ・ 内部指針又は方針 ・ 契約 ・ 適用される業界又はセクターの法律及び規制の遵守 ・ 自主規制機関の規範及び/又は規則の遵守 ・ その他（記述）	○ 第 37 条、 第 51 条第 1、3 項
47. （企業の運用を伺う質問のため対象外） これらの仕組みは、一般的に、個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に要求しますか？ ・ プライバシーステートメントに記載されているグローバルCBPRに準拠したプライバシーポリシーと慣行を遵守すること ・ 貴組織のプライバシーステートメントに記載されているポリシー又はプライバシー慣行と実質的に類似したプライバシー慣行を実施すること ・ 個人情報の取扱い方法に関して、貴組織に提供された指示に従うこと ・ 貴組織の同意がない限り、下請けに制限を設けること ・ 管轄区域において、フォーラムが認定したAAからからグローバルCBPRの認定を取得すること ・ その他（記述）	
48. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者に対し、貴組織の指示及び/又は契約の遵守を確保するための自己評価を提供するよう求めていますか？「はい」の場合、以下に説明してください。	△ 第 37 条、 第 51 条第 1、3 項

質問	インドネシア PDP Law
49. 個人情報の処理者、代理人、請負業者、又はその他のサービス提供者について、貴組織の指示及び/又は合意/契約が遵守されていることを確認するために、定期的な抜き打ち検査又は監視を行っていますか？「はい」の場合、以下に記述してください。	○ 第 37 条、 第 51 条第 1、3 項
50. **（企業の運用を伺う質問のため対象外）** 上記のような受領者によるグローバル CBPR システムの遵守を保証するデューディリジェンスや仕組みが現実的でない、又は不可能である状況において、個人情報を他の個人情報管理者に対して開示しますか？	

III. 広報・アウトリーチ活動に関する提言

1. 目的

Ⅱ. のアンケート・ヒアリング調査により、GCBPR の理解度・知名度が低い現状、及び事業者が求める情報や対象とすべき重点ターゲット等が明確になった。これらの詳細は、3.広報・アウトリーチ活動時の留意点で後述する。

本章では、調査結果を基に、GCBPR 周知のための広報活動並びに参加法域数及び参加企業数の増加に向けた効果的なアウトリーチ活動を導出し、有効な指標を提言する。

2. 広報・アウトリーチ活動の現状と課題

2.1. 情報発信の現状

①Web サイト

GCBPR に関する情報を入手しようとする場合、GCBPR の運営組織であるグローバル CBPR フォーラムの Web サイト(英語)で GCBPR の制度概要及び申請のために必要な手続き等、最も正確で最新の情報を取得することができる。国内で情報を入手する場合、GCBPR の所管官庁である個人情報保護委員会及び経済産業省、並びに日本の審査機関である JIPDEC の Web サイトからも GCBPR に関する情報を取得することが可能であり、潜在的な GCBPR 申請事業者がいつでも自由にアクセスできると考えられることから、制度の運営側及び申請者双方にとって、非常に有効な情報源である。

なお、これら以外の Web サイト上での情報発信の現状としては、認証事業者の Web サイトや GCBPR の取得支援を行うコンサルティング系事業者の Web サイト等からも情報を入手することができる。

②セミナー・シンポジウム

R6 調査でも触れていた GCBPR の普及啓発を目的としたセミナーやシンポジウム等の開催も、制度関係者及び認証事業者から直接対面で話を聞くことができるため、情報発信手段としては文字情報よりもさらに分かりやすく、不明な点を質問できる点も貴重な機会となる。

③その他

一般的な広報ツールとしては、パンフレット・リーフレット等もあるが、現在所管官庁や審査機関から発行されているものはない。

2.2. 課題

前項では情報発信の現状として、GCBPR に関する情報をどこでどのように入手できるのかを確認したが、本項では、今後の効果的な広報・アウトリーチ活動につなげるため、情報発信側並びに入手する潜在的な申請企業の視点で、現状の課題を整理する。なお、アクセシビリティ、内容、分かりやすさについては、ヒアリング調査で事業者から得られた意見が反映されて

いる場合は○、一部の対応はあるものの、十分でない場合は△、対応がないものは×評価とした。

(1) Web サイト

①GCBPR フォーラム

- アクセシビリティ: ○

  トップページに、グローバル CBPR とグローバル PRP システムの説明がある。

- 内容: △

  GCBPR に関する情報は、トップページ上部のメニューバーから必要な情報にアクセスする構成となっており、様式類もリンクからダウンロードできるようになっている。ただし、初めて Web サイトにアクセスした事業者にとって、GCBPR の詳細な制度概要や申請事業者にとっての具体的なメリット等の記載がない。

- 分かりやすさ: △

  トップページ上部のメニューで情報は分類されているが、各メニューページは文字情報が中心で視覚により理解を助ける構成になっていないこと、GCBPR を良く知らない場合、メニューにあるタイトルから必要な情報にたどりつくのに手間取ること等から、×に近い△である。

②GCBPR 所管官庁 (個人情報保護委員会、経済産業省)

- アクセシビリティ: ×

  トップページからのリンクがないこと、また、トップページで“CBPR”“GCBPR”を用語検索しても、検索結果リストから当該ページにたどりつくのか難しいこと等から、事業者が省庁の Web サイトにアクセスしても、情報の入手が困難である。

- 内容: △

  国際動向の把握はできるが、省庁の独自性がなく、グローバル CBPR フォーラム(制度の運営組織)のニュースリリースを日本語で案内している程度であるため、日本政府が支援する越境個人データに関する国際認証制度であることが伝わりにくい。また、制度自体のメリットは、個人情報保護委員会の Web サイトに英語版の資料が掲示されている。ただし、法的な要件が中心となっているため、個人情報保護法上の越境データの取扱いと GCBPR 制度上のメリットが整理できていないと理解が難しく、興味を持ってアクセスした企業のニーズに対応した情報が不十分であるため△とした。

- 分かりやすさ等: ×

  GCBPR の専用ページがなく、情報の発信が単発でつながりがないため、制度全体を把握することが困難。また、文字情報が中心となっているため、初めてサイトを訪れた事業者にとっては、GCBPR とは何かを省庁のサイトから読み解くことが難しい。

③JIPDEC(審査機関)

- アクセシビリティ: ○

  トップページの「事業から探す」の中に“CBPR 認証”というバナーが設置されており、制度の専用ページへ1クリックで遷移することができる。

- 内容：△

申請書式や認証基準等の申請に係る実務情報や認証事業者の事例紹介等はあるものの、GCBPR フォーラムのニュースリリースや所管官庁のニュースリリースへのリンクによる紹介に留まる等、審査機関独自の観点から制度の魅力やメリットを紹介する構成になっていない。

- 分かりやすさ等：△

専用ページの冒頭に「CBPR システムとは」というショート動画が設置されており、もっと詳しく知りたい事業者のための 6 分動画のリンクもあるため、目的に合わせて短時間で制度の理解を助ける工夫がなされている。他方、申請書類は Web サイトからダウンロードできるようになっているが、審査フローや書類の記入見本等に関する動画もあると、申請までの流れがより分かりやすくなる可能性がある。

④コンサルティングファーム

- アクセシビリティ：×

「CBPR コンサル」等のキーワードで表示された 3 社程度の事業者 Web サイトでは、トップページに CBPR のバナーを含め CBPR の専用ページは確認できなかった。

- 内容：△

所管官庁や審査機関がニュースリリースとして発信している情報を確認することはできたが、トップページで「CBPR」とキーワード検索をしても、専用ページが作成されている事業者は 1 社のみであった（報告書作成時点）。

- 分かりやすさ等：△

唯一専用ページが作成されている事業者の Web サイトも、文字情報が中心で、独自の視点で解説された情報等もないため、表示されている情報だけでは十分な理解が難しい。

(2) セミナー・シンポジウム

- アクセシビリティ：×

セミナーやシンポジウムの開催情報が所管官庁の Web サイトの深い階層下に埋もれており、その時々で開催業務の委託を受ける組織に依存するため、発信手段は個々の組織の Web サイト等での案内に留まり、ターゲット層に届いていない可能性が大きい。せっかく興味をもっている事業者がいた場合も、容易に探せない・たどりつけない状況がある。また、過去に開催された場所は、東京、大阪、福岡に留まり、近隣地域以外の事業者は開催地へのアクセスが困難であるため参加できない。

- 運用及び内容：△

過去に所管官庁で開催されたセミナーはあったが、単発的で継続性に乏しい。次の開催予定は不確実で、継続的な制度の理解やフォローアップの仕組みがセミナーやシンポジウムと連動していない。講演内容も、(1)Web サイトで触れた内容に関する課題と同様、それぞれの視点や立場に基づく制度の魅力やメリットが語られる場面が少ない。

- 分かりやすさ等：△

認証事業者の事例紹介や専門家によるパネルディスカッション形式等も実施されたが、文字情報を中心とした資料と基調講演という構成が主であるため、座学のみで当日聞いただけでは理解しづらい。

2.3. 改善策

前項までの現状と課題を踏まえ、本項では課題に対する改善策をとりまとめた。なお、Web サイトは、直接改善することが難しいため、GCBPR フォーラムは対象外とした。

(1) Web サイト

- トップページに GCBPR のバナーを設置する(所管官庁)。
- 所管官庁、審査機関独自の視点から制度のメリットや事例を豊富に紹介する。
- 大企業や中小企業、法務・情報セキュリティの専門家や当該部門の担当者だけでなく、中小企業も含め多用な主体を対象としていることを分かりやすく周知する。
- Web サイトへの流入を増やす手段を検討する(SNS や業界メディアとの連携)。
- 同一ページ内の情報は、文字だけでなく、図解やイラスト、動画等、視覚的に理解を助けるコンテンツを併用して構成する。
- 検索連動型広告等を利用して、能動的に情報を求めている層にアプローチし、Web サイトへのアクセスを促す。具体的には「越境移転」「個人情報　海外」「クラウドサービス個人情報保護」「GDPR 対応」「アジア進出　データ保護」「海外現地法人」「海外進出」等でキーワード検索を行った場合、GCBPR の情報ページへ誘導する広告を配信する。

(2) セミナー・シンポジウム

- 対面で開催する場合、大都市だけではなく地方都市でも複数回、定期的に開催する。
- オンラインで開催する場合、シリーズ化・アーカイブ化して、いつでも学べる環境を整備する。
- SNS や YouTube 等での告知・配信を強化し、多用な実務者へアウトリーチする工夫をする。
- 中小企業や初めて GCGPR を聞いた方向けに、参加者同士がディスカッション可能なワークショップスタイルのセッションを導入する。
- 開催した後も、参加者の声や Q&A を反映した FAQ を更新する等、実務支援を強化し、開催報告だけにならない仕組みとする。
- セミナー後のフォローアップ資料や相談窓口の案内を徹底し、参加した時から相談までの流れが途切れないよう工夫する(Web サイトの改善策と連動)。

(3) パンフレット・リーフレット

- 本報告書作成時点で、該当する広告物がないため、手に取っていただきやすい図解やイラスト等を使った1枚ものや、制度概要も記載された三つ折りのもの等、視認性が高く、

社内でのプレゼンにも役立つ作りのパンフレットやリーフレットを試験的に作成し、設置場所や掲載媒体等を工夫して、より多くの目にとまるようにする。

- ヒアリング調査で得られた、中小企業や固有の事業分野の事例、具体的な認証取得プロセスの工数、認証維持に必要な体制、費用対効果を可視化した情報等を網羅し、制度概要に留まらないものとする。
- 海外に現地法人を有している事業者や、これから進出を考えている事業者向けのサポートを実施している行政・公的機関や地方自治体等に設置を求める。

総評として、上記を踏まえ、制度の全体像から実務への連動、申請フォローまでがシームレスにつながるよう、所管官庁と審査機関の Web サイトの構成やリンクも工夫することが肝要である。

改善策で得られた具体的な施策と、施策を検証するための評価指標（KPI）は図表 75 のとおりである。

図表 75 広報・アウトリーチ活動の効果的な具体的手法と評価指標

対象	施策	KPI
①Web サイト	**1. 英語での情報発信強化** ・グローバル CBPR フォーラムの動きや日本の AA（JIPDEC）の役割を紹介 **2. 海外向けケーススタディの提供** ・日本企業とのデータ連携がスムーズになるメリットを強調 **3. 制度説明資料・情報の提供（多言語）** ・制度の目的、認証プロセス、国際的な位置づけを整理（Web サイトの構築） **4. わかりやすい動画・図解コンテンツの発信** ・「GCBPR とは何か」「認証事業者は何が安心なのか」等を説明 **5. SNS キャンペーン** ・個人データ保護の重要性を啓発 ・認証マークの認知向上 **6. メディア露出（ニュース、専門誌）** ・制度開始や認証事業者の増加をニュースとして発信	• 海外からの問合せ件数 • 海外企業（日本法人）の認証申請数 • 英語版サイトのアクセス数 • 国際イベントでのリード獲得数 • 認証マーク、制度の認知度調査 • 動画再生数 • SNS エンゲージメント（いいね、シェア、コメント） • メディア掲載件数

対象	施策	KPI
	7. 技術文書・審査ガイドラインの公開 ・透明性を高め、参入を促進 **8. セミナーやシンポジウムの配信** ・期間限定なしでアーカイブ配信を行う ・配布資料もダウンロードできるようにする	• ページビュー • ガイドラインダウンロード数 • 視聴数 • 資料ダウンロード数
②セミナー・シンポジウム	**1. 業界別セミナー・ウェビナーの開催** ・IT、EC、金融、SaaS 等、データの越境移転が多い業界に特化 ・所管官庁（個人情報保護委員会、経産省）や審査機関（JIPDEC）の最新情報を紹介 **2. 認証取得のメリット」事例紹介** ・既に認証を取得した企業を紹介 （例：日本の認証事業者、 他国の AA が認定した企業 等） ・海外展開時の信頼性向上、取引先要求への対応等を強調 **3. 中小企業向けワークショップ** ・実務上の課題をディスカッション、中小企業での導入自利やメリットの紹介、導入へのイメージ醸成、概要紹介	• セミナー参加者数、満足度 • 認証申請件数の増加 • 認証取得企業の業界分布の拡大 • 問合せ件数の推移 • セミナー参加者数 • 参加者の属性割合、変化率
③パンフレット・リーフレット	**1. パンフレット・リーフレットの作成** ・制度概要、申請手続きとフロー、事例紹介等、初めて手に取る人でも分かるもの **2. チェックリスト・ガイドブックの提供** ・認証取得プロセス、必要な体制整備、費用対効果を可視化	• 発行数、設置場所の数 • ガイドブックのダウンロード数

3. 広報・アウトリーチ活動時の留意点

3.1. 重点ターゲットの設定

(1) マネジメントシステム認証事業者

R6 調査で対象とした P マーク及び ISMS 及び本調査で対象とした PIMS に、アプローチするのが効果的である。既にいずれかのマネジメントシステム認証を取得している事業者は、GCBPR のプログラム要件への適合に向けた基盤を有しており、第三者認証の運用実績もあるため、事業者のニーズに GCBPR が必要なものであると分かれば取得に向けた推進力になるからである。

これらの認証事業者を重点ターゲットとして位置づけ、「既存のマネジメントシステム基盤を活かせば GCBPR 取得は大きなハードルではない」というメッセージを合致率の数値を根拠として具体的に伝えることで、検討段階に移行することが期待される。さらに、取得検討事業者の個別の状況（保有認証、事業内容、越境移転の実態等）に応じたきめ細かな情報提供を行うことで、より効果的な普及促進が可能となる。

(2) 事業者の属性別ターゲティング

アンケート調査結果から、普及促進の効率性を高めるため、以下の領域の事業者をターゲットと設定することが示唆された。

- クラウドサービスを積極的に利用している事業者
- SaaS 等クラウドサービスを提供している事業者
- アジア地域への事業展開を計画している製造業
- 越境 EC を展開している卸売業・小売業
- 製造業等、特定の事業分野で影響力のある Tier0[37]事業者

規模・業種を問わず多くの事業者がクラウドサービスを使用していることが明らかになったが、事業者は規約や約款のみで、契約書を締結せずにサービスを利用するケースが一般的であるため、自社と同等の情報の取り扱いに基づく相手方への要望や確認が困難であり、ヒアリング調査結果からも「詳細な情報が開示されない場合がある」と複数の声が挙がっていた。

したがって、クラウドサービス事業者が GCBPR を取得していれば、サービス事業者、サービス利用事業者、両者にメリットとなることをアピールできるため、GCBPR 取得の有力な候補と位置づけることができる。

3.2. 認知度向上・基礎理解の促進

(1) 「無意識の越境移転」への認識喚起

ヒアリング結果から、多くの事業者が自社は越境移転を行っていないと認識している一方で、クラウドサービス（AWS、Google Cloud、Box、OneDrive 等）の利用を通じて実質的に越境移転が発生している実態が明らかになった。事業者からは「クラウドサービス利用時に実は海外への情報移転が起きているという認識が極めて低い」「国内のみで事業展開する事業者には受け入れられていない」との指摘があった。

この「無意識の越境移転」への認識喚起は、GCBPR の必要性を事業者に理解してもらうための前提条件となる。クラウドサービス利用事業者に対して、自社が越境移転を行っている可能性があること、その場合にどのような対応が求められるかを分かりやすく伝える情報発信が、GCBPR の取得を検討する入口として有効と考えられる。

(2) 認知から検討への移行を促す情報提供

---

[37] 自動車業界の場合、メーカーを指す。その他、金融業界、ヘルスケア業界等がある。

ヒアリング事業者からは、検討段階に進むために必要な情報として、「具体的にどのような業務を行っている場合にこの認証が必要なのか」「どの程度の規模の事業者が取得しているか」「取得事業者がどのようなメリットを感じているか」といった点が挙げられた。

制度の一般的な説明に加えて、「なぜ自社に必要なのか」を事業者が判断できる情報（判断基準、セルフチェックツール等）の提供が、検討段階への移行を促す上で有効と考えられる。複数の認証制度が存在する中で、GCBPR と他の認証制度（P マーク、ISMS、経済産業省のセキュリティ格付け制度等）との関係性やメリット・デメリットを整理し情報提供することも、事業者の各種認証制度の取得に向けた優先順位を判断する上で重要な支援要素になると考えられる。

(3) 中小企業の取得可能性の周知

ヒアリング事業者からは、「現在の取得事業者を見ると大企業ばかりという印象があり、自社には関係ないと感じている」「大企業すぎて参考にならない」との声が寄せられた。現在の日本での認証事業者が大企業中心であることが、中小企業にとって自分事として検討されない心理的な障壁となっている可能性がある。

また、要望として、「中小企業でも取得可能であることを、文字情報だけでなく、事業者の実際の事例や声、図表やイラストを用いて示す方がわかりやすい」との意見が寄せられた。中小企業向けの対応としては、AA アンケートにおいても小規模事業者向け割引制度を設けている AA が存在することが確認された。

今後、中小企業の取得事例が生まれた場合には、その事例を積極的に発信することで、「自社でも取得できる」という認識を広げることが有効と考えられる。また、小規模事業者向け割引制度ができた場合には、積極的に発信することも有効である。

(4) Web サイト

ヒアリング事業者からは、「海外の法令は国によって異なり、法改正のタイミングも追い切れないので、そういう情報を提供してもらえると非常に助かる」「セミナー実施後の報告や参加者レポート等の情報を提供いただきたい」との声があった。

個人情報を取り扱っている担当者は、省庁の Web サイトで情報収集していることも分かったので、所管官庁の Web サイトには、GCBPR 専用ページへ誘導するバナーの設置やサブメニューに GCBPR 専用ページのリンクを追加する等対策することで訪問者の増加が見込まれる。なお、セミナーやネットワーキングイベントを開催する際は、ランディングページ[38]を作成しイベント別に告知をすることで、それぞれ効果測定することが可能となる。

[38] 広告や検索結果から訪問者が最初に着地するページで、特に資料請求や購入等の特定のアクション（コンバージョン）へ誘導することに特化した、通常は縦長の 1 ページ完結型の目的特化型の Web ページを指す。

3.3. アウトリーチの手段

認知度が極めて低い現状においては、GCBPR に関心を持つ可能性のある事業者に効率的にリーチする手段として、検索連動型広告やリーフレットの配布等、Web サイトを利用したオンラインと紙による 2 つの媒体を活用することが効果的と考える。

検索連動型はインターネット広告媒体費で約 40%を占める大きなシェアを持つ広告種別であり、効果測定や予算管理がしやすいというメリットがある。一方、紙媒体はデジタルに不慣れな層にも確実に届き、視認性も高い。特定のターゲット層に絞って設置場所を限定すれば、こちらも設定した予算内での運用がしやすいというメリットがある。

また、これらの手段を最大限に活かすためには、GCBPR 専用 Web サイトの作成が求められる。検索連動型広告や、紙媒体から流れてきた訪問者が、いかに有益な情報を得ることができるか、また最新の情報を収集できるかが重要となるため、継続的なメンテナンスが必要となる。

Ⅳ. その他

1. 制度設計への提言

1.1. 審査の効率化

認証事業者へのヒアリングにおいて、制度への改善等に対し、「慣れやノウハウの蓄積により、ドキュメント準備の工数は減っていく。初年度が最も重い」、「50 の質問に対する根拠資料は、何をどこまで出せば良いか分からない場合がある」と意見があった。

また、認証事業者以外の 8 社は、P マーク又は ISMS の取得事業者であるが、審査料が無料でも取得のインセンティブにはなりにくく、取得した後の「工数・労力・維持管理」に対する懸念が 7 社から寄せられた。ほぼ全ての事業者において、認証制度の運用にかかる労力やコスト、維持管理が課題となっていることが明らかになったため、具体的に対象となる P マーク、ISMS、PIMS 制度に対し、GCBPR の審査工程を軽減し、審査の効率化を検討することは非常に重要である。認証初年度と更新時での工数の差、業態別の対応ポイント等、認証事業者の実務的なノウハウを共有する仕組みも、検討事業者の意思決定支援に役立つ可能性がある。

なお、より一層検討事業者の GCBPR 取得に向けたインセンティブを高めるため、複数の認証を取得している場合を想定し、既存の審査工程の簡略化や審査工数の軽減を実現できれば、認証取得へのハードルが下がり、認証事業者数の増加に大きな効果をもたらすと思われる。

1.2. 認証単位及び審査範囲の拡充

GCBPR は、法人単位の認証であり、組織としての信頼を獲得しやすい特徴の一つとして挙げられる。本調査実施時点では、日本を含む、韓国、チャイニーズ・タイペイの AA は、個社単位での認証のみを行っているが、アメリカとシンガポールの AA は、選択制で個社又はグループ会社も含めて審査の範囲を選定することが可能である。

また、グローバル PRP の運用も、全 AA のうち、アメリカとシンガポールで審査が実施される等、各国の AA 間では認証単位と同様の差異がある。ヒアリング結果からも、プロセッサーとしての審査範囲が明確であるグローバル PRP は、選択肢としてあっても良いだろうという意見が寄せられた。

こうした制度上の柔軟性は、申請事業者にとって認証取得のインセンティブにつながることがヒアリングからも明らかである。同じ認証制度でありながら、提供できる審査内容に差異が生じる現象について、プログラム要件と国内法の執行関係との整理も含め、事業者のニーズに応える取組みが広がるよう、制度の窓口となる政府機関や AA の課題として、積極的な取組が期待される。

1.3. 外的要因の創出（中長期的取組）

ヒアリング結果から最も強く示唆されたのは、事業者の認証取得判断が「外的要因」に大きく左右されるという点である。事業者からは「取引するにあたって『これを取得していないとダメ』と

言われたら絶対に取得しに行く」「大企業が取引先に GCBPR の取得を求めてくるという流れがあると一気に広がる」「入札要件になると、やむを得ず取らなくてはいけないという形になる」との声が寄せられた。

グローバル事業を展開する事業者への働きかけ、公共調達における入札要件としての検討等、わが国における認証取得拡大に向けて大きな推進力となる外的要因を創出するための施策も、広報・アウトリーチ以外の取組としては、欠かせない要素である。

以上