令和 3 年度我が国におけるデータ駆動型社会に係る基盤整備
（データの越境流通に関連する諸外国の規制制度等調査事業）

西村あさひ法律事務所

令和 3 年 7 月 30 日

目　次

別紙

【図表 2：各国における域外移転規制の概要(現行法)】

【図表 3：各国におけるローカライゼーション規制の概要(現行法)】

【図表 4：各国において審議・検討中の法案等の概要】

第 1 総論

1. はじめに

データ流通は、今日のデジタル化され、グローバルに相互接続された世界を支えている。グループ間でのデータ共有やベンダーへのデータ移転が国境を超えることはごく一般的になってきており、クラウドコンピューティングやビッグデータ分析といった技術革新や膨大な個人データを含む SNS の浸透等も相まってここ数年でますますその勢いを増している[1]。他方で、様々な背景事情の下で、各国において国境を超えたデータ移転に関する規制が存在するところである。

データの域外移転を含む流通・利活用に影響を与える制度は、GDPR の登場の前後で大きくグローバルの潮流が変化し、世界各国で相次ぎ立法が整備されてきている状況にある[2]。2020 年時点で累計 200 を超えるとの調査結果も存在し[3]、各国における規制の在り方が各者各様であるため、それに対応していく手法も各々異なり、グローバルにデータ移転を伴うビジネスを行う事業者にとっては、対応が容易でないという実態がある。

その最たる障壁となっているのは各国におけるデータ保護主義的な規制、すなわち、データのグローバルな流通に一定の制約をかけたり、自国内へのデータ保存を求めるといった規制の存在である。国内産業の保護や安全保障を第一に考える場合、データ流通の円滑化という目的は一歩後退するが、過度な規制がなされると長期的にはグローバルな投資の減少を引き起こすことになりかねない。

本調査では、日本企業にとって特に重要性の高い国に焦点を当て、規制の有無及び内容の把握を行い、その結果、日本企業がどのような対応を求められているかにつき、整理を行うものである。

また、データのグローバル化への対応は、国際協調の下で進める必要があるため、各国間ないし複数国間での対話の在り方として、日本政府としてデータ流通の円滑化のためにどのような対応を行っていくことが考えられるかといった点にも目を向けてみたい。

---

1 例えば以下のサイトにおいて調査結果が公表されている。

https://www.jetro.go.jp/biz/areareports/2018/380fd5f0d9c4bb4d.html

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd131110.html

2 EU はその市場の巨大性等を背景として、いわゆる Brussels Effect を及ぼしているとの指摘がなされることもある。すなわち、EU の規制が EU 域外において、法的効果がないにもかかわらず、事実上の影響を及ぼしているということであり、GDPR はこの Brussels Effect の最たる事例である(Anu Bradford, The Brussels Effect: How the European Union Rules the World (2020)参照)。今後も、EU の各種政策のうち、環境、データ、ビジネスと人権の分野において、この傾向は続くとみられる。

3 Francesca Casalini et al., *Mapping Commonalities in Regulatory Approaches to Cross-border Data Transfers*, OECD Trade Policy Papers No. 248 (May 2021), p. 8, available at <https://www.oecd-ilibrary.org/docserver/ca9f974e-en.pdf?expires=1622781847&id=id&accname=guest&checksum=5F6908D563E26CDCDBA2882AFCA24B17>.

「信頼性のある自由なデータ流通(Data Free Flow with Trust)」を促進していくに当たって、各国の法制度・実務の内容を正しく理解し、過度に萎縮することなくグローバルでのデータ管理に取り組んでいけるよう、本調査の内容が実務対応やその環境整備のための一助となれば幸いである。なお、本調査においては、各国において広く適用される規制を整理しているものであって、産業分野別に適用される域外移転規制及びローカライズ要求を含む規制全てを網羅しているものではない。

2. 各国法制の概要

(1) 導入・制度の存否

以下、本レポートにおいては、基本的に 2021 年 4 月 30 日時点での情報を整理しているが、同日以降に特に重要なアップデートが生じている事項については、個別に解説を行っている。

まず、データ保護主義的な規制として、個人データの保護を目的として、個人データに適用される域外移転規制と、必ずしも個人データの保護のみを目的とするわけではなく、より広範囲のデータに適用され得るローカライゼーション規制とがあるところ、両者はデータ保護主義的な規制であるという点において共通項はあるものの、制度としては区別して整理することにしたい。

域外移転規制は、個人データが国境を超える際に、個人情報保護が不十分な国へと個人データが移転されることによって当該データが侵害される事態を防ぐため、移転元の国の個人情報保護法制の趣旨を及ぼすという観点からの規制である。他方で、ローカライゼーション規制は、国内産業の保護や安全保障の観点からデータを国内にとどめるべきという観点からの規制であって、データが特定の法域内で、排他的又は非排他的に、保管又は処理されることを義務付けるものである[4]。域外移転を完全に禁止するのであれば、データローカライズも達成されるという関係にある[5]。

本調査においては、EU、中国、シンガポール、タイ、インド、ベトナム及びインドネシアといった日本企業がその内容を知るニーズの特に高い国・地域における域外移転規制及びローカライゼーション規制を整理した。事業展開に当たっては今後の展望を知る必要があることから、中国、タイ、インド、ベトナム及びインドネシアについては、現行法令のみならず、今後施行される法令や法案についても整理の対象に含めている。他方で、特定

---

[4] Dan Svantesson, *Data Localisation Trends and Challenges Considerations for the Review of the Privacy Guidelines*, OECD Digital Economy Papers No. 301 (Dec. 2020), pp. 8 and 33 available at <https://www.oecd-ilibrary.org/docserver/7fbaed62-en.pdf?expires=1626654411&id=id&accname=guest&checksum=CEC930BC8D07B42C237E39A4E5FB83D3>.

[5] Casalini et al., *supra* note 3, p. 10.

の事業者のみを対象とする法制については検討の対象に含めていないため、営んでいる事業によってはそのような法制の下で規制が存在する可能性があることに留意されたい。

概要、各国における制度の存否は**図表１**のとおりとなっている。

【図表１：各国における規制の有無（現行法）】

	EU	中国	シンガポール	タイ	インド	ベトナム	インドネシア
域外移転規制	○	○	○	○	－	－	○
ローカライゼーション規制	－	○	－	－	－	○	△（公共サービス電子システム提供者のみ）

※　○＝制度が存在する、－＝制度が存在しない

(2) 各規制の概観

ア　域外移転規制（現行法）

域外移転規制は、1995年に制定されたDirective 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data（以下「EUデータ保護指令」という）において初めて導入された[6]。EUデータ保護指令は、1993年にEUが確立したことに伴い、EU加盟国間での個人データ保護のレベルを統一することを目的として、域外移転規制を含む統一的な個人データ保護の枠組みを設けたものである[7]。各国における個人データ保護の制度の相違を背景に、米国EU摩擦をはじめとしたグローバルな動向を経て、各国制度は現状の形に変容を遂げている。その過程では米国とEU間のデータ移転をセーフハーバーやプライバシーシールドといった枠組みで認めていたこともあったが、これらは現在全て無効となっている[8]。

6　須田祐子『データプライバシーの国際政治 越境データをめぐる対立と協調』（勁草書房、2021年）18頁。

7　同上。

8　セーフハーバーについては、2015年10月6日に欧州司法裁判所によって無効にされた（Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362&from=EN>）。プライバシーシールドは、2020年7月16日に欧州司法裁判所によって無効にされた（Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, available at <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311>）。

現状の各国における域外移転規制には多岐にわたる枠組みが存在し、例えば国又は地域ごとに移転の可否が定まるもの(GDPR における十分性認定がこれに該当する)、同意や契約といった措置[9](GDPR における標準契約条項(SCC)や拘束的企業準則(BCR)等の適切な保護措置がこれに該当する)の実装により域外移転を許容するもの、各事業者における措置ではなく、当局による個別の制約又は個別の承認により域外移転の可否が定まるもの、が挙げられる。これらのうち複数の手段を組み合わせた規制も存在する。各国における規制の概要は、別紙**図表 2** のとおりである。

各国の域外移転規制の内容を検討する際には、次のようなポイントを念頭において情報を整理するのが有用である。

- 移転するための方法として、どのような選択肢があるか：**第 2** の各国の解説の中で**(3)エ**の中で記載
- 各方法に優先順位があるか、それともいずれの方法を利用するのでも差し支えないか：**第 2** の各国の解説の中で**(3)オ**として記載
- 十分なデータ保護の水準が認められることを理由に移転できる場合については、当局の認定が必要か、事業者の判断で足りるか：該当する制度がある場合には、**第 2** の各国の解説の中で**(3)エ**の中で記載
- (契約に基づいて移転する場合)契約に規定すべき内容は法令又はガイドラインで決まっているか、決まっていないとしても実務的に確立しているか：該当する制度がある場合には、**第 2** の各国の解説の中で**(3)エ**の中で記載
- (同意に基づいて移転する場合)同意の要件：該当する制度がある場合には、**第 2** の各国の解説の中で**(3)エ**の中で記載

イ　ローカライゼーション規制(現行法)

データのグローバルな流通が促進されることと並行し、デジタル保護主義の台頭や、各国間の国際的緊張の高まり等を受けた牽制措置として、特にスノーデン事件以降に顕著にローカライゼーション規制が導入されてきている。ローカライゼーション規制をデータのグローバルでの自由な流通への障壁として認識する考え方を指摘しつつ、2020 年以降のパンデミック危機によって、ローカライゼーション規制をはじめとする内向政策が更に強化される可能性を指摘する論調も存在する[10]。

---

[9] 前掲脚注 3 の OECD のレポートによれば、公共の利益ないし正当な利益に依拠した域外移転を許容している法制や、同意に基づく域外移転を認めている法制は、全法制のうち 6 割近くを占めるとされており、これらの域外移転の根拠はグローバルに広く認められていると解される。

[10] Svantesson, *supra* note 4, p. 6.

ローカライゼーション規制についても、その規制の内容にバリエーションがある。①データのコピーを国内で保存する義務を定めるもの(データの域外移転やデータ処理が国外で行われる可能性を許容する)、②データのマスターを国内で保存する義務を定め、国外での保存を認めないもの(データ処理が国外で行われる可能性を許容するが、処理後は国内への返却を求める)、③データの域外移転や国外でのデータ処理にも制約を課しつつ、データを国内で保存することを求めるもの、といった分類が考えられる[11]。同じくデータの国内保存義務を定めるものであっても、当該義務の対象となる事業者の範囲やデータの種類も各国法制により異なる。

各国における規制の概要は、別紙**図表 3** のとおりである。

ウ　域外移転規制又はローカライゼーション規制を定める審議・検討中の法案等

上記では既に制定・公布されている法令に基づく規制について述べたが、2021 年 4 月 30 日時点で各国において審議又は検討されている法案・政令案[12]においても、域外移転規制又はローカライゼーション規制を定めているものが存在する。これらの法案等は未だ審議・検討の途中であるため、その規制内容は同日時点では未確定であり今後変更され得るものであるが、現時点の規制の概要は別紙**図表 4** のとおりである。詳細な定義等は変更され得るため、制度の大枠を紹介するに留めた。

3.　日本企業への影響と各国規制への対応の方向性

(1) 域外移転規制

域外移転規制に対応するためには、まず、移転元事業者の所在する国の法制の内容を確認する必要がある。別紙**図表 2** のとおり、各国法制において域外移転を許容する根拠は多様である。域外移転の根拠の選択肢としては類似するように見える法制同士であったとしても、全ての根拠が同等・並列に採り得る選択肢として整理されている法制と、例えば同意を得ることが原則とされており、その他の根拠はあくまで同意が得られない場合の例外として位置付けられている法制とで、実際上の対応の在り方は異なり得る。また、法制の仕組みそれ自体のみならず、各国での実務に即した対応が求められることも言うまでもない。

グローバルな視点から見ると、実務的には、契約又は同意に基づく移転が認められることが多い。もっとも、契約の様式の有無や契約に規定すべき項目、同意を取得するための

11　Casalini et al., *supra* note 3, pp. 10-11.

12　なお、中国のデータセキュリティ法については同日以降に成立したものであるが、2021 年 9 月に施行が迫っているため、本報告書においては確定済みの内容として反映している。

要件、同意の際に示すべき情報といった規制については各国各様である。国によっては、契約に基づく移転がメニューとして十分に整備されていない場合(そもそも契約に基づく移転がメニューにない、あるいは、メニューにはあるものの政府が公表することになっている契約の様式が未だ公表されていない等)であっても、契約締結を通じて移転元に適用される法制と同水準の保護の確保を移転先に課すことによってリスクを低減する実務も見られる。

データの域外移転に関する国際的な制度の統一については顕著なニーズが存在するところではある[13]が、少なくとも当面は各国の法制に個別に対応していかざるを得ないと考えられる。そのような中で近時注目すべき動きとしては、ASEAN において個人データの域外移転に関するモデル契約[14]が公表されたことが挙げられる。ASEAN 各国の規制に対応するためにこのモデル契約をそのまま利用できるわけではないが、データの域外移転に当たってのスタンダードを示すものとして注目すべき取り組みである。

(2) ローカライゼーション規制

多くの国において、ローカライゼーション規制は敷かれていないため、規制の存在する国において特に配慮を行えば対応としては足りることにはなる。

しかしながら、別紙**図表 3** のとおり、本調査の対象となる国だけでも、ローカライゼーション義務を負う事業者の範囲は各国によりバリエーションが存在する。また、ローカライゼーション義務の内容としても、同じ国内保存義務であってもその対象となるデータの種類や定義について各々異なるものとなっている。これらの義務の範囲を画するための各国法制の定義や解釈についても現状では未確定であったり、条文構造が難解であったりと、各事業者における義務の内容は一義的に明らかなものでもない。

さらには、ローカライゼーションの要請に対応することが実際上難しい場合も考えられる。例えば、ある国の法律の適用対象とはなるものの、当該国にサーバーを設置していないケース等では、ローカライゼーションの要請として国内保存義務が定められている場合にはサーバーを設置しなければ対応は不可能である。このように、ローカライゼーション規制への対応については、規制の存在する国へのサーバーの設置が求められる等、実際上・物理上のアクションが必要となることも少なくなく、日本企業のグローバルでの活動に一定の障壁となる側面は否定できない。そのような規制があることを前提に、規制の回

---

13 経済産業省「国際的なデータ移転・活用に関する企業アンケート結果 ―DFFT の更なる具体化の検討―」(2021 年 5 月)4 頁<https://www.meti.go.jp/press/2021/05/20210531001/20210531001-1.pdf>。

14 ASEAN, ASEAN Model Contractual Clauses for Cross Border Data Flows, available at <https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf>.

避、又はコストへの折り込み等を図っていくことが、競争力の維持にとっては必要となると考えられる。

4. 国際ルールに基づく提案の方向性

上記のとおり、各国は、それぞれ様々な政策的意図や目的に基づいて、域外移転規制やローカライゼーション規制を設けており、現状、事業者としては、これらの規制の内容を把握し、法的リスクに適切に対応することが重要である。

もっとも、理想論としては、各国の規制への対応を個別に行うよりは、域外移転に関する国際的に統一されたルールを構築し、各国及び各国事業者がそれを遵守するのが望ましいと考えられる。

そのためには、日本政府としては、データ保護を意識しつつ、日本企業によるデータ流通やその利活用を促進する国際的枠組みの構築や、日本企業の足かせとなる規制制度を採用する国への働きかけのために、関連する国際ルールに基づく提案を行うことも考えられる。

このような国際ルールは、大きく分けて、加盟国/締約国による貿易制限措置に対する規律を定めた WTO 協定等の貿易協定と、プライバシー分野における国際ルールが存在する[15]。

(1) 貿易協定

WTO 上、データの越境流通は、何らかのサービスの提供の一環として行われることが多いことから、GATS における規律が関連し得る。域外移転規制・ローカライゼーション規制との関係で主に問題となる義務は、次の 4 つである。

① 内国民待遇義務
② 最恵国待遇義務
③ 市場アクセス義務
④ 国内規制の合理的実施義務

---

[15] 前掲脚注 3 の OECD のレポートでは、データの越境流通を促進するための手段を、①単独メカニズム(Unilateral mechanism)、②複数国間の取り組み(Plurilateral arrangements)、③貿易協定及びパートナーシップ(Trade agreement and partnership)、④標準及び技術によるイニシアチブ(Standard and technology-driven initiative)に分類している。本報告書では、これらのうち、各国の域外移転規制及びローカライゼーション規制を分析する上で特に有益と思われる②及び③を取り扱う。

①及び②は、問題となっている措置が、差別的な待遇を伴う場合、③は、問題となっている措置が、サービス提供者の数の制限又はサービスの総産出量の制限に該当する場合、④は、問題となっている措置が、サービスの質を確保するために必要である以上の負担を課したり、合理的・客観的・公平でない態様により適用された場合に問題となる。

もっとも、仮に各国の域外移転規制やローカライゼーション規制が上記の義務に抵触する場合であっても、GATS14 条の一般的例外(公衆の道徳の保護又は公の秩序の維持のために必要な措置(同条(a)号)及び(ii)GATS に反しない法令の遵守を確保するために必要な措置(同条(c)号))及び安全保障に基づく例外によって、正当化される可能性がある。前者については、問題となっている措置が、同条各号の目的との関係で「必要な」措置であること、また、「恣意的若しくは不当な差別の手段となるような態様で又はサービスの貿易に対する偽装した制限となるような態様で適用」されていないことが必要である。一方、後者については、加盟国/締約国に対して広範な裁量が認められている。

また、CPTPP や RCEP においては、域外移転規制及びローカライゼーション規制を原則として禁止している。これらの義務への抵触は、「公共政策の正当な目的」によって正当化される可能性があるが、CPTPP においては、当該措置が「恣意的又は不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用」されていないこと、及び、「目的の達成のために必要である以上に情報の移転に制限を課すものではないこと」が必要である。一方で、RCEP においては、公共政策目的や安全保障に基づく例外について、締約国に広範な裁量が認められている。

各国における域外移転規制やローカライゼーション規制の内容やその運用が、日本企業に対してその政策意図との関係で過剰な負担を課す場合や、日本企業を差別的に取り扱うものである場合には、当該規制の実施国に対して、貿易協定と整合的となるように、提案を行っていくことが考えられる。その際には、当該規制の政策意図やその内容・運用状況を把握し、分析することが重要である。

(2) プライバシー保護に関する国際ルール

プライバシー保護の分野では、非拘束的なソフトローを含め、多くのルールが策定されている。このうち、本報告書の分析対象とした各国との関係性が深いものは下記のとおりである。

① OECD プライバシーガイドライン
② 欧州 108 号条約
③ APEC プライバシーフレームワーク
④ ASEAN PDP フレームワーク

いずれも、プライバシーの保護とデータの越境流通の促進のバランスを図ることを企図しており、基本的には、プライバシーに対する十分な保護が与えられている場合や、本人の利益になる場合(本人の同意がある場合を含む)に、データの越境流通を認めるという構造になっている。このことから、プライバシーの保護を目的とした域外移転規制やローカライゼーション規制が、十分なプライバシー保護の水準を保っているような場合や本人の同意があるような場合にまでデータの越境流通を制限するのであれば、こうしたプライバシー保護に関する国際ルールとの関係で問題があることを指摘することが考えられる。

また、APEC や ASEAN においては、CBPR システムや ASEAN モデル条項のような、複数国間によるデータ域外移転促進に向けた仕組み作りがなされている。そのため、こうした取り組みがプライバシーの保護とデータの越境流通の促進のバランスをとるものであるとして、これらを参考にした具体的な協力の枠組みの構築を提案することも考えられる。

第 2 各国法制の整理

1. EEA

(1) 政策的意図・目的

従前、EEA 域内では、EU データ保護指令が EEA 域内の個人データ保護について規律しており、EU データ保護指令の下で、各 EU 加盟国が個人データの保護に関する法令を制定していた。EU データ保護指令は直接的に国内法規としての効力を有するものではなく、各 EU 加盟国による法制化を必要としていたため、データ保護に関する規制は EU 加盟国ごとに区々であった。

このような状況下で、EEA 域内において一貫性のある個人データの保護を確保し、EEA 域内の個人データの流通の障害を除去するために、各 EU 加盟国における個人データの保護に関する規律を統一する必要が生じていたことに応えて、2018 年 5 月 25 日、REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(欧州一般データ保護規則、以下「GDPR」という)が施行された。

GDPR は、個人データの処理と関連する自然人の保護に関する規定及び個人データの自由な移動に関する規定を定めるものであり(GDPR1 条 1 項)、自然人の基本的な権利及び自由、特に個人データ保護の権利の保護を、その目的として掲げている(GDPR1 条 2 項)。

EEA 域内の各国への対応としては、この GDPR に加え、各国固有の規制への対応が必要となる場合もあるが、本調査報告では対応の基礎となる GDPR に対象を限定して情報を整理している。

(2) 域外移転規制及びローカライゼーション規制に関する担当省庁・部局

欧州委員会が執行を行う EU 競争法とは異なり、域外移転規制を含め、GDPR は各 EU 加盟国(ドイツは各州)に設置されたデータ保護当局が所轄している[16]。

また、各 EU 加盟国のデータ保護当局の代表者と欧州データ保護監督機関(European Data Protection Supervisory)から構成される欧州データ保護評議会(European Data

[16] https://www.ppc.go.jp/enforcement/cooperation/cooperation/EU-DPA/
https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

Protection Board。以下「EDPB」という)が、GDPR の解釈に関する多数のガイドラインを公表している。

(3) 域外移転規制

ア　域外移転の定義

GDPR において、域外移転は、EEA 域外の第三国又は国際機関への個人データの移転として定義されている(GDPR44 条)。同一法人間の移転であっても EEA 域外への移転であれば、域外移転に含まれる。また、同じ国の中の移転であっても、EEA 域外の国にある第三者への移転(例えば、GDPR が適用される米国法人 A から米国法人 B への移転)であれば、域外移転に該当することにも注意が必要である。この「移転」を GDPR は直接定義していないが、EEA 域内に所在する個人データを EEA 域外の第三国又は国際機関に物理的に移転する場合のみならず、EEA 域外の第三国又は国際機関から EEA 域内に所在する個人データへのアクセスを認める場合等も含まれると解される。

なお、GDPR においては、EEA 域外の第三国に個人データが移転した後の、当該第三国から別の EEA 域外の第三国への個人データ移転(Onward Transfer)についても、GDPR の域外移転規制が及ぶことが明記されている(GDPR44 条)。Onward Transfer についても GDPR は直接定義していないが、例えば、EEA 域内の企業が、米国のベンダーに個人データを移転し、当該ベンダーが EEA 域外にある再委託先に個人データを移転する場合には、後者の移転にも GDPR の域外移転規制対応が必要ということを意味する。

イ　域外移転規制の対象となるデータの種類・定義

域外移転規制の対象となる個人データとは、識別された自然人又は識別可能な自然人(データ主体)に関する情報を意味し、識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す 1 つ又は複数の要素を参照することによって、直接的又は間接的に識別され得るものをいう(GDPR4 条 1 項)。ある自然人が識別可能かどうかを判断するには、管理者やそれ以外の者が個人を直接又は間接に識別するために合理的に使用可能な全ての手段、すなわち、費用、時間等の識別に必要な一切の客観的要因及び処理の時点で利用可能な技術や技術的進歩を勘案した手段を考慮する必要がある(GDPR 前文 26 項)。なお、統計情報等、完全に不可逆な態様でデータから個人を特定できないよう匿名化した場合は個人データに該当しないが、匿名化が認められるハードルは高いとされている。

ウ　域外移転規制の対象となる者の定義・範囲

GDPR 上の管理者(自然人、法人、公的機関、部局又はその他の組織であって、単独又は他の者と共同で、個人データの処理の目的及び方法を決定する者、GDPR4 条 7 項)及び処理者(管理者のために個人データを処理する自然人、法人、公的機関、部局又はその他の組織、GDPR4 条 8 項)が、域外移転規制の対象とされている(GDPR44 条)。管理者から委託を受けて個人データを処理する者は処理者に該当し、例えば、管理者が利用しているクラウドサービスプロバイダや給与計算代行会社等が処理者に含まれ得る。

エ　域外移転の条件

GDPR 上、個人データを EEA 域外に移転することは原則として禁止されている(GDPR44 条)が、次のいずれかを満たす場合には、例外的に域外移転を行うことができるというのが基本的な建て付けである。

大きな枠組みとしては、まず、欧州委員会が、十分なデータ保護の水準を確保していると認定した国、地域又は国際機関[17]へのデータ移転については、追加して特段の対応を行わずに域外移転が許容される(GDPR45 条 1 項)。

移転先の国が十分性認定を取得していない場合、GDPR46 条に規定された以下の保護措置に準拠して域外移転を行うことが可能である。これらの保護措置のうち、現在の実務においては、ほとんどの場合、欧州委員会が採択した SCC が利用されている。

- 公的機関又は公的組織の間の法的拘束力・執行力のある文書
- 拘束的企業準則(Binding Corporate Rules。以下「BCR」という)
- 欧州委員会が採択した標準契約条項(Standard Contractual Clauses。以下「SCC」という)
- 監督機関が採択し、欧州委員会が承認した SCC
- GDPR40 条の行動規範
- GDPR42 条の認証制度
- 監督機関の個別的な承認を受けた契約条項又は取決め

十分性認定を取得しておらず、かつ、上記の適切な保護措置を講じることができない場合には、GDPR49 条に規定された例外事由(Derogations)を満たす場合に限り域外移転を行うことができる。

以下では、これらの域外移転の根拠のうち、代表的なものについて内容を紹介する。

①　移転先の国が欧州委員会の十分性認定を取得している場合(GDPR45 条):**(ア)**

[17] この認定を受けているのは、日本の他、アンドラ、アルゼンチン、カナダ(商業組織のみ)、フェロー諸島、ガーンジー、イスラエル、マン島、ジャージー、ニュージーランド、スイス、ウルグアイ、英国である。

② BCR の策定による適切な保護措置が提供されており、データ主体の執行可能な権利とデータ主体の効果的な司法的救済が確保されている場合(GDPR46 条 2 項(b)号、47 条):**(イ)**

③ 移転元と移転先との、欧州委員会が採択した SCC を含む契約の締結による適切な保護措置が提供されており、データ主体の執行可能な権利とデータ主体の効果的な司法的救済が確保されている場合(GDPR46 条 2 項(c)号):**(ウ)**

④ 適切な保護措置を適用するための拘束力があり、執行可能な第三国の管理者又は処理者の約定を伴った、GDPR40 条に基づく行動規範による適切な保護措置が提供されており、データ主体の執行可能な権利とデータ主体の効果的な司法的救済が確保されている場合(GDPR46 条(e)号):**(エ)**

⑤ 適切な保護措置を適用するための拘束力があり、執行可能な第三国の管理者又は処理者の約定を伴った、GDPR42 条に基づく認証制度による適切な保護措置が提供されており、データ主体の執行可能な権利とデータ主体の効果的な司法的救済が確保されている場合(GDPR46 条(f)号):**(オ)**

⑥ データ主体が適切な保護措置が講じられていない域外移転に伴うリスクについて情報提供を受けた上で域外移転について明示的に同意している又はデータ主体との間の契約の履行のために必要である等、所定の例外事由に該当する場合(GDPR49 条):**(カ)**

(ア)十分性認定

欧州委員会が、GDPR 相当の十分な水準の保護を確保していると認定した国、地域又は国際機関に対しては、特別な手続を経ることなく個人データを移転することが可能である(GDPR45 条 1 項)。

欧州委員会が、十分な水準の保護を確保しているか否かを評価する際には、以下の要素を考慮することとされている(GDPR45 条 2 項)。

①	法の支配、人権及び基本的自由の尊重、公安、国防、国家安全保障及び刑事法を含む、一般的又は分野別の関連法令、公的機関による個人データへのアクセス、並びにそのような法令の実施、他の第三国又は国際機関への個人データの再移転に関する規定であって、当該国、地域又は国際機関が遵守する法令を含む、データ保護規則、職業上の準則及び保護措置、判例法、並びに効果的かつ執行可能なデータ主体の権利、その個人データが移転されるデータ主体のための行政上及び司法上の救済
②	適切な執行権限を含む、データ保護法令の遵守の確保及び執行に関する機能、データ主体がその権利を行使する際に支援し助言することに関する機能、並びに EU 加盟国の監督機関との協力に関する機能を担う独立の監督機関が存在し、かつ効果的に機能していること
③	当該国、地域又は国際機関が加入している国際的な取決め、特に、個人データ保護に関する法的拘束力のある条約又は法律文書から生ずるその他の義務、及び多国間システム又は地域システムへの参加に基づく義務

日本は十分性認定を取得しているが、十分性認定に依拠して日本への域外移転を行った場合には、移転先において個人情報の保護に関する法律に係る EEA 及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール(以下「補完的ルール」という)を遵守する必要がある。

(イ) 拘束的企業準則(BCR)

BCR とは、企業グループあるいは共同経済活動に従事する事業者のグループの構成企業同士で、1 ヵ国又は複数の第三国における管理者又は処理者に対して個人データ移転又は一連の個人データ移転のため、策定・遵守される個人データ保護のためのグループ内規である(GDPR4 条 20 号)。BCR は、個人データの移転について十分な保護措置を策定し、それを欧州の主要拠点がある国の監督機関の審査を経て承認を受けるものである。

BCR による個人データの移転はグループ企業間に限られ、かつ、グループ全体として策定した準則に法的に拘束されることとなる(GDPR47 条 1 項(a)号参照)。公表資料によれば、欧州を拠点とする世界的な企業を中心に 140 社ほどが BCR の承認を受けているが、大半が GDPR 施行前に取得されたものである[18]。日本企業では、楽天[19]が BCR を導入しているほか、公表事例では IIJ[20]や富士通[21]が BCR の承認申請を行ったようである。

BCR の承認を受けることで、監督機関からのお墨付きを得るものであるため、執行リスクが減り、また、新たな種類のデータ移転が生じる都度契約の別紙を修正するといった手続の煩がないというメリットがある。他方で、GDPR 施行前から多くの BCR の承認申請が出されてきたが、ようやく 2019 年の秋から少しずつ承認される事例が現れてきているにとどまり[22]、多くの事例は 3～4 年経過しても承認を得ることができていないというのが現在の状況であり、新たに BCR の承認を得るには相応の時間を要する可能性があるというデメリットがある。

BCR に定めるべき内容は以下のとおりである(GDPR47 条 2 項)。これらの BCR の項目はあくまでモデルであり、グループ企業の構造を考慮に入れてカスタマイズされることが想定されており、また、プライバシーポリシーにも実際に反映されている必要がある。

---

18 https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en
https://edpb.europa.eu/system/files/2021-03/edpb_information_20210126_pre-gdpr_bcrs_overview.pdf

19 https://corp.rakuten.co.jp/privacy/bcr.html

20 https://www.jipdec.or.jp/library/report/20190711-1.html

21 https://pr.fujitsu.com/jp/news/2018/01/19-1.html

22 https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en

①	グループ及びそれぞれのメンバーの体制と詳細な連絡先
②	個人データの種類、処理の種類とその目的、影響を受けるデータ主体の種類、及び問題となっている第三国を含むデータ移転
③	国内及び国外双方における法的拘束性
④	一般的なデータ保護の原則の適用
⑤	処理に関するデータ主体の権利及び当該権利の履行手段
⑥	EEA 域内に拠点のない主体による BCR の侵害に関して責任を有する、管理者又は処理者の承諾
⑦	データ主体に提供される、BCR についての情報の通知方法
⑧	データ保護責任者等の業務
⑨	不服申立手続
⑩	BCR の遵守の有効性を検証することを確実にするグループ内の仕組み
⑪	規定変更を報告及び記録し、当該変更を監督機関に報告する仕組み
⑫	グループ内の主体によって遵守されていることを確実にするための監督機関との協力の仕組み
⑬	グループ内の第三国にある主体が従い、かつ、BCR によって提供される保障に実質的悪影響を及ぼすおそれのある法的要件を管轄監督機関に報告する仕組み
⑭	個人データに永続的に又は定期的にアクセスする人材への適切なデータ保護の訓練

BCR を取得しようとする者は、自社グループにおける個人データの処理の実情等を踏まえた準則の規定を作成し、各国のデータ保護当局の承認を得る必要がある。承認を得る過程で、申請に必要な書類の他、監督機関がその判断の基礎とすべく、個人データの管理体制や管理状況を示す資料を提出することが求められる。

(ウ) 欧州委員会が採択した SCC

SCC とは、個人データの域外移転のための契約の雛形であり、EEA 域外の企業も、EEA 域内の企業と雛形どおりの契約を締結することによって、個人データの域外移転が可能になる。BCR とは異なり、グループ外の企業との間の個人データの移転にも用いることができる。

SCC の中には、データの移転元(輸出者)とデータの移転先(輸入者)の義務が規定されており、大要、①EEA 域内からデータ移転を受けた場合に、当該データの処理に際しては移転先においても EU と実質的に同水準の個人情報保護が要請されること、②輸入したデータを更に第三者提供する際(Onward Transfer を行う際)には原則として GDPR に定める域外移転規制への対応が必要になること、③EEA 域内のデータ主体から直接権利主張を受ける可能性があること、という内容になっている。

SCC の締結に当たっては、公表されている SCC の内容自体を修正することはできない。もっとも、他の条項の追加は、当該条項が SCC と矛盾せず、かつ、データ対象者の人権を侵害しない限りでは可能であると解されている(GDPR 前文(109)号)。基本的には SCC の別紙に記載すべき事項の内容を検討し、締結することとなる。

これまでの SCC は、管理者(Controller)同士で締結するものが 2 セット、管理者から処理者にデータ移転を行う場合に締結するものが 1 セットの合計 3 セットが存在し、いずれも公開されている。

2020 年 7 月 16 日の欧州司法裁判所の判決(Schrems II 判決)において、SCC の締結等の適切な保護措置を根拠として域外移転を行う場合、移転先国において公的機関による個人データへのアクセスが行われる可能性がある場合には、そのような可能性を考慮した上で、移転先において EEA 域内と本質的に同様のデータ保護が確保されるようにする必要がある旨が示された。

公的機関による個人データへのアクセスが行われる可能性がある場合とは、例えば、個人データの移転に関して、The Foreign Intelligence Surveillance Act of 1978 (以下「FISA」という)702 条が適用される場合が挙げられる。同条が適用される場合には、暗号化されていない個人データへの政府によるアクセスを阻止できるような技術的措置を講じない限り、移転先において EEA 域内と本質的に同様のデータ保護を確保できていると認められる場合は極めて限られていると言われており、暗号化等の技術的措置を講じる必要性が高まっている。

また、Schrems II 判決も踏まえて、2021 年 6 月 4 日、欧州委員会は新たな SCC(Annex to the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679)を採択した。従前公表されていた SCC は、2021 年 9 月 27 日には効力を失い、新たに締結することができなくなるが、それまでに締結済みの SCC については、契約が対象としている個人データの処理に変更がなく、かつ、SCC に依拠することによって個人データの移転が適切な保護措置の対象となることが確保される限りにおいて、2022 年 12 月 27 日まで引き続き有効という移行期間が設けられている(COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EEA) 2016/679 4 条)。したがって、SCC に依拠して域外移転を行っている全ての企業において SCC の差替えの対応が必要となり、現時点で域外移転に関する SCC を締結済みの企業においても、2021 年 9 月 26 日より前に改定前の SCC を新たに締結しようとする企業においても、2022 年 12 月 27 日までに新 SCC を締結し直す必要がある。

従来は、管理者から管理者への域外移転と、管理者から処理者への域外移転について、それぞれ別々の SCC が存在していたが、新たな SCC は、①管理者から管理者への域外移転、②管理者から処理者への域外移転、③処理者から管理者への域外移転、④処理者から処理者への域外移転について、1 つの契約条項の中で選択可能なモジュールをそれぞれ用

意している。このうち、②と③のモジュールは、処理者に個人データの処理を委託する場合に締結することが義務付けられている、GDPR28 条 3 項に準拠したデータ処理契約の内容を含むものとなっているため、新たな SCC を締結すれば、別途データ処理契約を締結する必要はなくなる。

また、新たな SCC では、当事者は、公的機関による個人データへのアクセスに関するものを含む、移転先国の法制度及び実務により、移転先における SCC の遵守が妨げられないことを保証する必要がある(SCC14 条(a)項)。その際には、データ移転の具体的状況や移転先の国の法制度及び実務を調査し、データ保護のために実施する補完的措置を考慮した上で、データ移転のリスクに関する影響評価(Transfer Impact Assessment。以下「TIA」という)を実施し、当局からの求めに応じて提出できるよう、その結果を文書化することが義務付けられている(SCC14 条(b)項、(d)項)。このため、新たな SCC を締結する際には、あわせて TIA を実施の上、その結果を文書化することが必要となる。

TIA においては、移転先国の法制度だけではなく、当該法制度の実務上の運用まで考慮する必要があるとされ、一見して問題のない法制度であっても、実務の運用上、公的機関による不当な個人データへのアクセスが認められているならば、補完的措置を講じる等の対策が必要となる。

また、2021 年 6 月 18 日、EDPB は、補完的措置に関するレコメンデーションの最終版(Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data。以下「レコメンデーション」という)を採択した。レコメンデーションによれば、仮に、移転先国の法制度及び実務が、公的機関による個人データへのアクセスを認める等問題があるものであったとしても、当該法制度及び実務が、当事者の行おうとする具体的なデータ移転には適用されないと評価できる場合には、補完的措置を実施せずに、個人データの域外移転を実施することができるとされている(レコメンデーション 43.3 パラグラフ)。

移転先の事業者や個人データの移転に対して移転先国の法制度及び実務が適用されるリスクを検討するに当たっては、移転先の事業者が過去に公的機関から個人データへのアクセス要求等を受けたか否かを考慮することができるとされており、いわゆるリスクベースのアプローチが許容されている(SCC 脚注 12、レコメンデーション 47 パラグラフ)。もっとも、移転先の事業者の過去の経験を考慮するためには、当該経験が他の公開情報との間で矛盾しないか、適切な内部手続に則って当該経験が文書化されているか等の事情も合わせて検討する必要があるとされ、移転先の事業者において、公的機関から個人データへのアクセス要求等がなされたことがなかったからといって、当該事業者に対して、直ちに個人データの域外移転が認められるようになるわけではなく、TIA の実施が必要であることに変わりはない点に留意が必要である。

この他、SCC の締結に際しては、SCC の別紙に、当事者、移転の内容、管轄監督機関、技術的・組織的措置、復処理者といった所定の情報を記入することが必要である。

(エ) 行動規範

行動規範は、管理者や処理者の業界団体が制定する自主ルールのことであり、GDPR が特定の業界や活動分野においてどのように適用されるべきかを実務的に定めるものである。中小事業者[23]の要件を特に勘案するものである(GDPR 前文 98 項)。行動規範には、各国レベルのものと EU レベルのものとがあり、監督機関が適切な安全措置を備えているとして承認することによって成立するものとされている。事業者団体が行動規範を策定し、監督機関が承認することが想定されている。

行動規範には、以下の内容を定めるべきとされている。これらの項目は、修正や拡張をすることも可能である(GDPR40 条 2 項)。

①	公正及び透明性のある処理
②	特定の文脈において管理者によって追求される正当な利益
③	個人データの収集
④	個人データの仮名化
⑤	公衆及びデータ主体に対して提供される情報
⑥	データ主体の権利行使
⑦	子どもに対して提供される情報及び子どもの保護、並びに、子どもに対して親権者としての責任を負う者から同意を得るための方法
⑧	GDPR24 条(管理者の責任)及び 25 条(Data protection by design and by default)で定める措置及び手続、並びに、32 条に規定する処理の安全性を確保するための措置
⑨	監督機関に対する個人データ侵害の通知及びデータ主体に対するその個人データ侵害の通知
⑩	第三国又は国際機関に対する個人データの移転
⑪	GDPR77 条(監督機関に異議を申立てる権利)及び 79 条(管理者又は処理者を相手方とする効果的な司法救済の権利)によるデータ主体の権利を妨げることなく、管理者とデータ主体との間の処理に関する紛争を解決するための裁判外の手続及びそれ以外の紛争解決手続

行動規範を取得しようとする者は、上記の事項を踏まえた行動規範を策定し、監督機関に対して承認を求めていくこととなる。

(オ) 認証制度

データ保護の認証制度とは、管理者や処理者のデータ保護措置が、GDPR を遵守していることを認証する制度であり、認証は権限ある監督機関又は認証を行うことが正当に認可さ

[23] 250 人未満の従業員を雇用しており、かつ、年間売上高が 5000 万ユーロを超えず、及び/又は、年次貸借対照表の合計が 4300 万ユーロを超えない事業者と定められている(GDPR 前文 13 項、委員会勧告 2003/361/EC 別紙 2 条 1 項)。

れた機関によって付与される(GDPR42 条 5 項)。そして、認証を取得するために満たさなければならない水準は、権限ある監督機関若しくは EDPB(GDPR42 条 5 項)、又は欧州委員会(GDPR43 条 8 項)によって策定される。

認証を希望する者は、認証機関又は監督機関に対して、全ての情報及び認証手続の実施のために必要な個人データの処理活動へのアクセスを提供しなければならない(GDPR42 条 6 項)。

(カ) GDPR49 条の例外事由の充足

GDPR49 条は、以下の例外事由を充足する場面では、十分性認定や適切な保護措置がない場合であっても、個人データの域外移転を許容している。

① データ主体が適切な保護措置が講じられていない域外移転に伴うリスクについて情報提供を受けた上で、域外移転について明示的に同意している場合
② データ主体との間の契約の履行又はデータ主体が要請する契約締結前の措置の実施のために必要である場合
③ 第三者との間の、データ主体の利益になる契約の履行又は締結のために必要である場合
④ 公共の重大な利益のために必要である場合
⑤ 法的主張の立証又は攻撃・防御のために必要である場合
⑥ データ主体が物理的又は法的に同意できない場合で、データ主体又は第三者の生命に関する利益を保護するために必要である場合
⑦ EU 法又は EU 加盟国の国内法に従う一定の登録機関からの移転である場合

GDPR49 条規定の例外事由のうち、同意については、GDPR4 条 11 号において、自由に(freely)、特定された(specified)、十分な情報に基づく(informed)、不明瞭ではない(unambiguous)データ主体の意思表示であることと定義されている。GDPR49 条 1 項(a)号において、当該データ移転の潜在的リスクについての情報が提供された後に、データ主体がその移転について明示的に(explicitly)同意した場合という要件が加重されている。同意の要件のうち、「自由に」との関係では、雇用関係のある従業員との関係ではこの要件の充足が難しいと解されており 、従業員の個人データを域外移転しようとする場合には、同意以外の根拠に依拠することが無難であるものと考えられる。

また、GDPR 上の同意の要件が厳格であることから、域外移転の根拠をこの合意のみに依拠することによって、事後的に同意の要件を欠いていた、すなわち同意が無効であったことが判明したり、同意の撤回(GDPR7 条 3 項)がなされたりすることにより、域外移転の根拠を喪失してしまうことになるというリスクがある。また、そもそも関係する個人全てから GDPR 上の要件を充足した同意を取得できるとも限らないケースもある。以上を踏まえると、安定的な域外移転を行うためには、同意以外の根拠に依拠したデータ移転を行うことが重要となる。

オ　実務上の対応

上記**エ**記載の**(ア)**～**(カ)**の中で実務上利用されることが多いのは、域外移転先が日本のように十分性認定を得ている場合には、**(ア)**の十分性認定又は**(ウ)**の SCC、域外移転先が十分性認定を得ていない場合には SCC である。**(イ)**の BCR を利用する例も存在するものの、十分性認定や SCC と比較すれば、現在のところ利用例は少数に留まっている。

もっとも、このような実務は、2021 年 6 月 4 日に欧州委員会が新たな SCC を採択するまでの間に形成されたものであり、新たな SCC では、旧来の SCC よりも移転先に GDPR の水準に近いデータ保護の体制整備が求められることになるため、今後は、SCC の利用に対してより慎重な態度を取る事業者が増える可能性もある。例えば、従来は、十分性認定を得る前に SCC を締結済みであった企業を中心に、十分性認定を得ている日本への域外移転の場合にも SCC を利用する例が少なからず見られたが、今後は、日本への域外移転の際には、SCC ではなく十分性認定を利用する例が増えることも想定される。もっとも、EEA 域内から、日本以外にあるグループ会社やベンダーに個人データを移転する場合には引き続き SCC を利用する必要があるため、結局のところ、現在 SCC を締結している企業においては、期限までに新たな SCC を締結し直すという動きが主流になるように思われる。

カ　域外移転先への域外移転規制の域外適用の有無

域外移転先であることのみを理由とした域外移転規制の域外適用の条文は存在しない。ただし、域外移転先が域外移転を受ける以外の理由で GDPR の適用を受ける場合には、域外移転先にも GDPR の域外移転規制の遵守が必要となる。

一般的な GDPR の地理的適用範囲については、まず、管理者又は処理者の EEA 域内の拠点の活動に関連する個人データの処理であれば、実際に個人データの処理が EEA 域内で行われるか否かを問わず、GDPR が適用される(GDPR3 条 1 項)。また、EEA 域外の管理者又は処理者であっても、EEA 域内に所在するデータ主体の個人データに対して、①データ主体による対価の支払いを要するか否かを問わず、EEA 域内に所在するデータ主体に対する商品やサービスの提供に関連した処理を行う場合、又は②EEA 域内で起こるデータ主体の行動の監視に関連した処理を行う場合については、GDPR が適用される。①の具体例としては、EEA 域内に居住する個人を対象とする日本企業のサービス提供に伴う個人データの処理が、②の具体例としては、EEA 域外の事業者による、EEA 域内における個人の嗜好や行動の分析を目的として、Web の閲覧履歴や商品購買履歴を追跡することが、それぞれ挙げられる。このうち、GDPR3 条 2 項に基づいて GDPR が域外適用される場合には、管理者又は処理者は、書面により EEA 域内に代理人を指名しなければならない(GDPR27 条 1 項)。

また、域外移転先が SCC を締結した場合、域外移転先は、SCC に基づいて、GDPR 上の域外移転規制と類似した契約上の義務を負うこととなる。

(4) ローカライゼーション規制

GDPR 上、ローカライゼーション規制は存在しない。

(5) EEA における企業活動の留意点

日本企業による対応のポイントとしては、まずはそもそも GDPR への対応が必要かという入口の理解が不可欠である。具体的には、GDPR の域外適用を受けるか、また、EEA 域外への個人データの域外移転規制への対応が必要かという点である。もちろん、EEA 域内にグループ会社等の現地拠点を有している場合には、当該拠点において GDPR 全般への対応を検討しなければならないことはいうまでもない。

その上で、域外移転規制の対応が必要となる場合には、いずれの根拠に拠って域外移転を行うかを検討することとなる。日本は欧州委員会から十分性認定を受けているため、補完的ルールを遵守する限り、SCC を締結しなくとも、日本への域外移転を十分性認定に基づいて行うことは可能である。SCC の締結に伴う移転するデータの内容の特定といった事務的な手間や、SCC によって課される厳格なデータ保護に関する義務の負担に鑑みれば、EEA 域内から日本への域外移転を行うときは、十分性認定に依拠して、補完的ルールを遵守することで域外移転規制への対応を行うことがシンプルな選択肢になると考えられる。十分性認定に基づく対応を行う場合、補完的ルールを遵守すべく、社内規定類を整備する必要がある。

他方で、グローバルに個人データの移転を頻繁に行う必要がある日本企業においては、日本に対するデータ移転のみが十分性認定でカバーできたとしても、EEA 域内から EEA 域外の日本以外の地域への域外移転のケースに、グループとして対応を行う必要があることも少なくない。このような場合は、日本企業を含めるか否かは検討の余地があるとしても、グループ全体としては、グローバルに SCC を締結し、それに依拠して域外移転を行うというのが、基本的に唯一の選択肢である。SCC の改定により、複数当事者間での SCC の締結や、SCC 締結後に契約当事者を追加できる Docking Clause の整備等が進んだことにより、グローバルでの多数当事者間での SCC の締結がより行いやすくなった側面はある。また、データの具体的な移転状況を踏まえ、移転先国ごとに、その法制度及び実務を調査の上、移転先国の政府による個人データへのアクセスが行われる法令・実務が存在する場合には、必要な補完的措置を講じた上で、域外移転のリスクを評価する必要がある。

2. 中国

(1) 政策的意図・目的

ア 各法律の概況

(ア) 個人情報保護法案

これまで中国においては、各法令に個人情報保護関連の規定が分散しており、個人情報保護法の起草の試みが度々なされては見送られてきていたところ、世界的な個人情報の保護の重要性の高まりや米国における対中政策等への抵抗の対抗措置のニーズ等を背景として、GDPR 等の他国の有益な法制を参照しつつ立案した、統一的な個人情報保護法(原文表記「个人信息保护法」)の制定がいよいよ実現しそうなものである。同法の法案(以下、本項において「個人情報保護法案」という)は 2021 年 4 月 29 日に第二次審議案が公示され、同年 5 月 28 日まで意見募集が行われた。

同法は、個人情報に関する権利利益を保護し、個人情報の取扱活動を規範化し、個人情報が法に基づき秩序だって自由移動することを保証し、個人情報の合理的利用を促進することを目的とする(個人情報保護法案 1 条)。

(イ) サイバーセキュリティ法

中国におけるサイバーセキュリティ法(原文表記「中华人民共和国网络安全法」、「ネットワーク安全法」と訳されることもあるが、以下、本項において「サイバーセキュリティ法」という)は、インターネットの急速な普及による諸問題への対応として、中国のサイバーセキュリティ分野における初めての基本法として 2016 年 11 月 7 日に公布され、2017 年 6 月 1 日に施行された。

同法は、ネットワークの安全を保障し、ネットワーク空間の主権並びに国の安全及び社会の公共の利益を保ち、公民、法人その他の組織の適法な権利利益を保護し、かつ経済・社会の情報化の健全な発展を促進することを目的とする(サイバーセキュリティ法 1 条)。

(ウ) データセキュリティ法

サイバーセキュリティ法の保護対象が電子データ・サイバー空間におけるデータのみであったのに対し、全ての電子的又は非電子的形態の情報に対する保護を拡大することを目指す法律である。このデータセキュリティ法(原文表記「中华人民共和国数据安全法」、以下、本項において「データセキュリティ法」という)は 2021 年 6 月 10 日に公布され、同年 9 月 1 日より施行される。

同法は、データ処理活動を規律し、データの安全を保障し、データの開発利用を促進し、公民や組織の合法的な権益を守り、国家の主権、安全と利益発展を維持することを目的とする(データセキュリティ法1条)。

(2) 域外移転規制及びローカライゼーション規制に関する担当省庁・部局

ア　各法律の規定

(ア) 個人情報保護法案

国家ネットワーク情報部門は、中国国家ネットワーク情報弁公室[24]が担当部局である。同室は、個人情報保護に関する統括・監督管理を職掌とし(個人情報保護法案59条)、個人情報の宣伝・教育、指導、個人情報取扱者の個人情報保護の実施に対する指導や監督、個人情報保護に関する申立て、通報の接受や処理、違法な個人情報処理活動の調査や処理等を担当する(同法案60条)。

(イ) サイバーセキュリティ法

国家ネットワーク情報部門、電信主管部門及び公安部門が関連する主管部門である(サイバーセキュリティ法8条)。

国家ネットワーク情報部門は、中国国家ネットワーク情報弁公室が担当部局である。同室は、インターネットセキュリティに関する統括・監督管理を職掌とし、サイバーセキュリティ法(中国工業情報化部、中国公安部と共管)や重要情報インフラ安全保護条例、サイバーセキュリティ有事対応プラン等を所管する。

電信主管部門は、中国工業情報化部[25]・サイバー安全管理局・サイバー及びデータセキュリティ処が担当部局である。同部は、ブロードバンドやインターネット業界の監督、電気通信、インターネット、専用通信ネットワークといった通信業の所管や標準の制定、政策実施を行い、サイバーセキュリティ有事対応プランを所管する。

公安部門[26]はいわゆる警察組織である。

---

24 http://www.cac.gov.cn

25 http://www.miit.gov.cn/
https://www.miit.gov.cn/jgsj/waj/jgzz/art/2020/art_4646354791574be7b6971ba29254e910.html

26 http://www.mps.gov.cn/

(ウ) データセキュリティ法

中央国家安全指導機関は、中央国家安全委員会が担当部局である。同委員会は、データセキュリティに関する決定及び統括、国家データセキュリティ戦略及び関連の重大方針政策の研究・制定及び指導・実施を職掌とする(データセキュリティ法5条)。

また、各地区及び各部門は、当該地区及び当該部門において業務中に収集し、及び生じたデータ並びにデータの安全につき責任を負うこととされている(同法6条1項)。

国家ネットワーク情報部門は、中国国家ネットワーク情報弁公室が担当部局である。同室は、ネットワークデータセキュリティに関する統括・監督管理を職掌とする(同法6条4項)。

公安部門及び国家安全機関等は、各自の職責範囲内においてデータセキュリティに関する監督管理を職掌とする(同法6条3項)。また、工業、電信、交通、金融、自然資源、衛生・健康、教育、科学技術等の主管部門は、当該業種及び当該分野のデータセキュリティに関する監督管理を職掌とする(同法6条2項)。

(3) 域外移転規制

ア　域外移転の定義

個人情報保護法案、サイバーセキュリティ法、データセキュリティ法においては域外移転の定義は不見当である。

他方で、いずれも内容が確定していないものではあるが、サイバーセキュリティ法の下位法令と位置付けられる、2017年4月11日に公示された個人情報及び重要データ域外移転安全評価弁法案(原文表記：个人信息和重要数据出境安全评估办法。以下、本項において「2017年弁法案」という)17条[27]においては、域外移転とは、ネットワーク運営者が中国国内

[27] 安全評価に関連する弁法案には未確定のバージョンが二種類あり、2017年弁法案及び2019年5月28日に公示された個人情報域外移転安全評価弁法案(原文表記：个人信息出境安全评估办法。以下、本項において「2019年弁法案」という)が存在する。

運営[28]において収集し、発生した個人情報及び重要データ[29]を、中国国外にある機構、組織又は個人に対し提供することと定義されている。

また、データ域外移転安全評価ガイドライン案[30]3.7 条においては、域外移転とは、ネットワーク運営者がネットワーク等の方法により、中国国内運営において収集し、発生した個人情報及び重要データを、中国国外にある機構、組織又は個人に対し、直接提供又は業務展開、サービス・製品提供等の方法により提供する一回限りの又は継続的な活動と定義された上で、以下の場面もこの域外移転に該当することとされている。

① 中国の司法管轄に属さず又は中国国内[31]で登記されていないものの、中国国内にある機構、組織又は個人(すなわち中国から見て外国企業や外国人)に対し、個人情報及び重要データを提供する場合

---

28 データ域外移転安全評価ガイドライン案においては、外国企業が中国国内で登記をしているか否かにかかわらず、中国国内において何らかの経営活動を行い、又は中国国内に製品又はサービスを提供する場合には、中国国内の「運営」に該当するとされている(同ガイドライン案 3.2 条)。この中国国内の運営の該当性の判断要素としては、①取引における中国語の使用の有無、②決済通貨としての人民元の使用の有無、③中国国内への配送・物流の有無等が存在する。

29 2017 年弁法案 17 条によれば、重要データとは、国の安全、経済発展、並びに社会的及び公的利益に密接に関連するデータをいい、その具体的な範囲は国の関連基準及び重要データ識別ガイドラインを参照するとされている。加えて、データ域外移転安全評価ガイドライン案の別紙 A によれば、重要データとは、関連する組織や個人が中国国内において収集し、又は発生する、国家機密には該当しない国の安全、経済発展、又は公共の利益に密接に関連するデータ(生データ及び派生データを含む)であり、かつそのデータが同意なしに公開、紛失、濫用、改竄あるいは廃棄され、又は分析等を経た後、①国家の安全や国防利益を害すること、国際関係の破壊、②国有財産、公共の利益及び個人の合法的な利益を害すること、③産業スパイや軍事スパイ活動、組織犯罪等に対する国家の予防・取締りに影響すること、④行政機関による違法、汚職行為に対する調査に影響すること、⑤政府の行政活動の妨害、⑥国家の重要インフラ、重要情報インフラ、政府システムの情報システムの安全を害すること、⑦経済及び金融の秩序を害すること、⑧国家機密又はセンシティブデータにアクセスし得ること、⑨その他国家の安全事項を害することをもたらす可能性があるものをいう。なお、同ガイドラインでは、通信、鋼鉄、金融、電子商取引、食品薬品等 27 のカテゴリーが設けられ、業界分野ごとに重要データの範囲が規定されている。

また、同じくサイバーセキュリティ法を前提とする 2019 年 5 月 28 日公示の「データセキュリティ管理弁法(意見募集案)」38 条においては、重要データとは、漏洩により国家安全、経済安全、社会安定性、公共健康及び安全に直接に影響を及ぼし得るデータをいい、具体的には未公開の政府情報、広範囲の人口、遺伝子健康、地理、鉱物資源等が含まれるとされている。

これらのいずれの弁法案が内容として確定していくのかは未定であるが、解釈の参考となる情報と言える。

さらに、データセキュリティ法において、重要データのデータ分類制度を確立し、経済社会発展におけるデータの重要度並びに改ざん、破壊、漏洩又は不法取得及び不法利用にひとたび遭遇した場合における国家安全、公共利益又は個人若しくは組織の適法な権益にもたらす危害のレベルに基づき、重要データ目録を国が制定する旨が規定されている(データセキュリティ法 21 条)ため、今後、重要データ目録の制定・公布動向を注目している必要がある。

30 https://www.tc260.org.cn/file/20170830203000000004.docx

31 香港、マカオ、台湾を含まない中国本土の意。「国内」と表現されることもある。以下同じ。

② データが中国国外の地域に移転・保存されないものの、中国国外の機構、組織又は個人がアクセスして閲覧できる場合(公開情報、ホームページのアクセスを除く)
③ 企業グループ内部におけるデータの域外移転であっても、中国国内運営において収集し、発生した個人情報及び重要データに関わる場合

他方で、同条では、以下の場面は域外移転には該当しないとされている。

① 中国国内運営において収集しておらず、又は、中国国内運営において発生したものではない個人情報及び重要データを、変更や加工処理を経ずに中国を経由して中国国外に移転する場合
② 中国国内運営において収集し、発生したものではない個人情報及び重要データが中国国内での保存･加工処理を経てから国外に移転されるものの、中国国内運営において収集し、発生した個人情報及び重要データに関わらない場合

以上を踏まえると、企業グループ内での情報の移転であっても、以下の場合には域外移転に該当する可能性があると考えられる。

① 中国国外にあるシステムを利用している場合(中国子会社が日本本社のシステムを利用する場合等)
② 中国国内のシステムから中国国外のシステムへデータを同期している場合
③ 中国国外のクラウドサービスを利用している場合

イ　域外移転規制の対象となるデータの種類・定義

(ア) 個人情報保護法案

個人情報が対象となる。個人情報とは、電子的又はその他の方式で記録した、既に識別され又は識別可能な自然人に関連する各種情報をいう。なお、非電子の情報も含むが、匿名化された情報を含まない(個人情報保護法案 4 条)。

(イ) サイバーセキュリティ法

個人情報及び重要データが対象となる。

個人情報とは、電子又はその他の方式で記録した単独又はその他の情報と組み合わせて自然人(個人)の身分を識別することができる、自然人の氏名、生年月日、身分証番号、個人の生体認証情報、住所、電話番号等を含むがこれらに限らない各種情報をいう(サイバーセキュリティ法 76 条 5 号)。

(ウ) データセキュリティ法

国の安全と利益の維持、国際的義務の履行の維持に関連する管理品目に該当するデータ(データセキュリティ法 25 条)及び重要データ(同法 31 条)。

このうち管理品目とは、両用品目、軍需品、核並びにその他の国の安全及び利益の維持・保護、拡散防止等の国際義務の履行に関連する貨物、技術、サービス等の品目を指し、品目関連の技術資料等のデータを含むが、管理品目に該当するデータであるか否かは、国所定の規制リストや基準をもって判断することになる(輸出管理法 2 条、4 条)。

また、重要データのうち、(i)重要情報インフラ[32]の運営者が中国国内での運営において収集し、生じた重要データの域外移転の安全管理については、サイバーセキュリティ法の規定が適用されるが、(ii)その他のデータ処理者が中国国内での運営において収集し、生じた重要データについては、データセキュリティ法において、国家ネットワーク情報部門が国務院の関係部門と共同して域外移転の安全管理に係る弁法[33]を制定する旨が定められている(データセキュリティ法 31 条)。

ウ　域外移転規制の対象となる者の定義・範囲

(ア) 個人情報保護法案

個人情報取扱者(個人情報保護法案 72 条 1 号)。個人情報の処理目的、処理方法等の事項を自主的に決定する組織及び個人をいう。

(イ) サイバーセキュリティ法

重要情報インフラの運営者[34](サイバーセキュリティ法 37 条後段)。

32　公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務等の重要な業界及び分野、並びにその他の一旦破壊され、機能を喪失し、又はデータが漏洩すると国の安全、国の経済と人民の生活、公共の利益に深刻な危害が及ぶおそれのあるその他の重要情報インフラをいうとされている(サイバーセキュリティ法 31 条)。その更に具体的な内容は、重要情報インフラセキュリティ保護条例案 18 条が定めており、①政府機関及びエネルギー、金融、交通、水利、衛生医療、教育、社会保険、環境保護、公的事業等の業界・領域の組織機構、②電気通信ネットワーク、ラジオ・テレビ放送ネットワーク、インターネット等の情報ネットワーク及びクラウド、ビッグデータその他大型の公共情報ネットワークサービスの組織機構、③国防・科学技術工業、大型装備、化学工業、食品薬品等の業界・領域における科学研究・生産の組織機構、④ラジオ局、テレビ局、通信社等のマスメディア、並びに⑤その他の重要な組織機構が運営し、管理するネットワーク施設及び情報システムで、一旦破壊され、機能を喪失し、又はデータが漏洩すると国の安全、国の経済と人民の生活、公共の利益に深刻な危害が及ぶおそれのあるものとされている。

33　2021 年 4 月 30 日時点で、詳細を定めた下位法令は不見当である。

34　2017 年弁法案においては、域外移転規制の適用対象となる者を重要情報インフラの運営者から、全てのネットワーク運営者(サイバーセキュリティ法 76 条 3 号に基づき、ネットワークの所有者、管理者及びインターネットサービスプロバイダをいうこととされている)に拡大している。かかる規定が実現すると、中国国内のネットワークを利用する事業者が広く域外移転規制の対象となってくるため、留意が必要である。

(ウ) データセキュリティ法

データ処理者(データセキュリティ法 27 条以下)。

エ　域外移転の条件

(ア) 個人情報保護法案

次の条件のいずれかを満たす域外移転のみが認められる(個人情報保護法案 38 条)。

個人情報処理者のうち、重要情報インフラの運営者又は当局の定めた数以上のデータを処理する個人情報処理者は、以下のうち②ないし④の根拠に拠ることはできず、域外移転の必要がある場合、法律、行政法規又は国家ネットワーク情報部門により免除がなされている場合を除き、事前に当局による安全評価に合格する必要がある(個人情報保護法案 40 条)。

① 個人情報保護法 40 条の規定に基づく国家ネットワーク情報部門による安全評価[35]に合格した場合
② 国家ネットワーク情報部門の規則に基づく専門機構による個人情報保護の認証を得ている場合
③ 中国国外の移転先と契約[36]を締結し、双方の権利と義務を約定し、かつ移転先における個人情報処理活動につき、個人情報保護法に規定された内容を満たしていることを監督する場合
④ 法律、行政規定又は国家ネットワーク情報部門の規定するその他の条件[37]

以上の根拠のいずれかを充足することに加え、個人情報取扱者は、中国国外への個人情報の提供時において、中国国外の受領者の身分、連絡先、取扱目的、取扱方法、個人情報の種類、個人情報保護法の定める権利の個人から中国国外の受領者への行使方法等の事項を個人に告知し、かつ、当該個人の個別の同意を取得しなければならない(個人情報保護法案 39 条)。この「個別の」同意は、例えば個人情報を第三者に提供することへの同意[38]と、中国国外に移転することの同意と、別途得ることが必要となるという意味に解されている。

---

35 詳細については下位法令の案も規定されていない状況ではあるが、個人情報保護法案 40 条の安全評価はサイバーセキュリティ法 37 条の「重要情報インフラ運営者による個人情報と重要データの安全評価」のうちの「重要情報インフラ運営者による個人情報の安全評価」の適用主体を拡大したものであるとの解釈もあり、その考え方に従えば、2017 年弁法案及び 2019 年弁法案の内容を参考にすることが可能である。

36 この契約のフォーマットは今後政府から公表される予定。

37 2021 年 4 月 30 日時点で、詳細を定めた下位法令は不見当である。

38 個人情報保護法案 13 条 1 号において、個人情報の処理の根拠の 1 つとして、同意が規定されている。

(イ) サイバーセキュリティ法

域外移転を行うことに業務上の必要性がある場合には、国家ネットワーク情報部門が国務院の関係部門と共同して制定する弁法[39]に従い安全評価を行わなければならず、かつ、国の関連規定及び関連基準の要求に従わなければならない(サイバーセキュリティ法 37 条後段)。この点、下位法令においては、域外移転に係る安全評価を行うことが求められている[40]。いずれもまだ確定した内容は定められておらず、採るべき手法について定まった方向性はない。

(ウ) データセキュリティ法

国の安全と利益の維持、国際的義務の履行の維持に関連する管理品目に該当するデータに対して、法に基づき輸出管理を実施する(データセキュリティ法 25 条)。

いかなる国又は地域も、データ及びデータ開発利用技術等に関連する投資、貿易において、中華人民共和国に対して差別的な禁止、制限又はその他類似の措置をとる場合、中華人民共和国は、実際の状況に基づき、当該国又は地域に対して相応の措置をとることができる(同法 26 条)。

また、重要データのうち、重要情報インフラの運営者以外のデータ処理者が中国国内での運営において収集し、生じた重要データについては、国家ネットワーク情報部門が国務院の関係部門と共同して域外移転の安全管理に係る弁法[41]を制定することとなっている(同法 31 条)。

オ　実務上の対応

サイバーセキュリティ法、データセキュリティ法上の域外移転規制の対応について、後者は制定後間もないこともあり、前者については具体的な措置が確定していないことから、実務としての対応は未了であるケースが多いと思われる。また、個人情報保護法案に

39　2017 年弁法案及び 2019 年弁法案の双方を含み得る。このうち、2019 年弁法案においては、中国国内に所在するネットワーク運営者と中国国外の事業者が個人情報の域外移転を伴う契約を締結する際の規律を定めている。当該規律には、個人が損害を被った際の賠償請求や、漏えい等の際の当局による情報の域外移転の停止措置の権限、中国国外のネットワーク運営者がその責任・義務を履行すること等に係る規定を含む。

40　2017 年弁法案(及びデータ域外移転安全評価ガイドライン案)においては、域外移転に係る安全評価が、自己安全評価と監督官庁による安全評価(1 年以内の個人情報の域外移転の数量が監督官庁の報告要請要件に達した等の場合)の双方の手段が規定されているのに対し、2019 年弁法案では、一律に監督官庁による審査・安全評価が要求され、より厳格な仕組みとなっている。また、2017 年弁法案では、ネットワーク運営者が 50 万人以上を含む又は累計で 50 万人以上を含む個人情報を域外移転する場合には、安全評価を行うことが規定されている(2017 年弁法案 9 条)。いずれのバージョンについても賛否両論があり、どちらのスキームを基礎として実際の制度設計がされていくかは未だ不透明であるため、今後の動向を注視していく必要がある。

41　2021 年 4 月 30 日時点で、詳細を定めた下位法令は不見当である。

定める域外移転の根拠のうち、いずれの根拠が実務上一般的に採られていくかは今後の動向を注視していく必要がある。

カ　域外移転先への域外移転規制の域外適用の有無

(ア) 個人情報保護法案

組織及び個人が、中国国内で自然人の個人情報を処理する活動、及び中国国外で中国国内の自然人の個人情報を処理する活動のうち次に該当する場合に適用される(個人情報保護法案3条)。かかる要件を充足する限りにおいて、域外移転先にも同条の規定は適用される。

① 中国国内の自然人に製品又はサービスを提供することを目的とする
② 中国国内の自然人の行動を分析・評価する
③ 法律及び行政規定で規定されているその他の状況。

具体的な域外適用の範囲は、今後ガイドライン等でその趣旨が明確化にされると予想されるが、GDPR と一定程度類似の文言となっていることから GDPR の解釈を参考にすることができる。具体的には、e-Commerce 等のインターネットを通じて中国との取引を行っている企業等は、中国拠点の有無を問わず、個人情報保護法案対応を検討する必要があると思われる。

(イ) サイバーセキュリティ法

中国国内における、ネットワークの構築、運営、保守及び使用、並びにネットワークの安全[42]の監督管理にサイバーセキュリティ法が適用される(サイバーセキュリティ法2条)。かかる要件を充足する限りにおいて、域外移転先にも同条の規定は適用される。

(ウ) データセキュリティ法

中国国内において展開するデータ処理(収集、保存、加工、使用、提供、伝達、公開等)活動及びその安全監督管理に適用される。中国国外でデータ処理活動を展開し、中国の国の安全、公共の利益又は公民、組織の合法的な権利利益に損害を与えた場合、データセキュリティ法に基づいて責任を追及する(データセキュリティ法2条)。「中国国内において展開するデータ処理」の具体的に意味する内容は未だガイドライン等の形で明らかにされていないが、かかる要件を充足する限りにおいて、域外移転先にも同条の規定は適用され

---

[42] 必要な措置を講じることを通じて、ネットワークに対する攻撃、侵入、妨害、破壊及び不法使用、並びに突発的事故を防止し、ネットワークが安定かつ信頼可能な運行状態にあるようにし、並びにネットワークデータの完全性、秘密保持性及びユーザビリティを保障する能力をいう(サイバーセキュリティ法76条2項)。

る。また、「中国の国の安全、公共の利益又は公民、組織の合法的な権利利益」との文言が広汎に解釈される傾向があり、域外適用の有無にかかわらず、同条に基づき中国国内の個人や組織から責任追求の主張がなされる可能性は否定しきれない。

(4) ローカライゼーション規制

ア　ローカライゼーション規制の対象となる者の定義・範囲

(ア) 個人情報保護法案

重要情報インフラの運営者、又は当局による取扱量基準[43]以上のデータを処理する個人情報処理者(個人情報保護法案 40 条)。

同法案上にこの「重要情報インフラの運営者」の定義はなく、サイバーセキュリティ法と同様の範囲と解される可能性もあるが、今後、下位法令において別途定義規定が設けられる可能性もある。

(イ) サイバーセキュリティ法

重要情報インフラの運営者(サイバーセキュリティ法 37 条前段)[44]。

(ウ) データセキュリティ法

中国国内の組織又は個人(データセキュリティ法 36 条)。

イ　ローカライゼーション義務の内容(保管制限、データのコピーの移転の可否、データ処理要件等)

(ア) 個人情報保護法案

重要情報インフラの運営者、又は当局による取扱量基準以上のデータを処理する個人情報処理者は、中国で収集及び生成された個人情報は原則として中国国内に保存するべきとされる(個人情報保護法案 40 条)。

43　2021 年 4 月 30 日時点で、詳細を定めた下位法令は不見当である。

44　域外移転規制同様、データローカライゼーション義務についても、下位法令において対象となる者がネットワーク運営者全体に拡大される可能性がある。ただし、対象拡大に係る規定は 2017 年弁法案には見られるものの、2019 年弁法案では削除されているため、どのような形で実現するかは不透明である。

(イ) サイバーセキュリティ法

中国国内で業務を展開し、製品又はサービスを提供する活動を通じて収集した個人情報及び重要データについては、中国国内に保存する必要がある(サイバーセキュリティ法 37 条前段)。外国企業であってもかかる要件を満たす限り規制の適用を受け、収集した個人情報を中国国内のサーバーに保存する必要がある。

この規定との関係では、中国国内にデータのマスターがあれば、ローカライゼーション義務に違反のリスクは下がると解される。したがって、中国国内で収集・生成した個人情報や重要データは国外に設置されたサーバーに直接は保存せず、一度、中国国内に設置されたサーバーに保存した後に国外に移転させる等、システム面での対応が必要になる。

(ウ) データセキュリティ法

中国国内の組織又は個人が中国国内で保存されているデータの取り寄せを外国の司法又は法執行機関から要求された場合、中国主管部門の認可を経ずに当該データを提供してはならない。中国の締結又は参加する国際的な条約・協定に規定がある場合、当該規定によることができる(データセキュリティ法 36 条)。

同条は、2018 年に米国で施行された Clarifying Lawful Overseas Use of Data Act(CLOUD Act)に対して、中国側の主権を維持するための対抗的な規定であると考えられる。

(5) 中国における企業活動の留意点

以上整理してきたとおり、中国国外の企業であっても、重要情報インフラの運営者に該当する事業者については、域外移転に際しての安全評価を実施する必要があり、かつ、中国国内にデータを保存するローカライゼーション義務を負う。したがって、日本企業としては、まず、自社、自社グループ又は中国の取引先・提携先が重要情報インフラの運営者に該当するか否かを確認する必要がある。重要情報インフラの運営者の定義はまだ確定した法令で定義されているものではないものの、上述のとおり重要情報インフラ安全保護条例案 18 条の規定は十分に判断の参考となる。

重要情報インフラの運営者に該当する関係者がいるため、自社が域外移転規制やローカライゼーション義務の影響を受ける場合には、今後制定される法令の動向を注視し、適切な手続を踏めるよう体制整備を行うことが必要である。かかる手続の仮定では、特に安全評価の局面で中国当局の対応が必要となる等、相応のコストがかかることも考えられるため、場合によってはビジネススキームを再考し、これらの規制の制約を受けない形に変更することをも検討することはあり得る対応である。

他方、2017 年弁法案等の動向を見るに、域外移転規制やローカライゼーション義務の対象が拡大される可能性も一定程度存在する。自社グループや取引先に重要情報インフラの

運営者となる可能性のある事業者が含まれていなくとも、中国における法令につき無頓着で良いということにはならない。制定されていく法令の動向を注視することが重要である。

なお、以上とは別に、金融機関や信用調査会社の中には、既に個別の業法によってローカライゼーション義務等が定められている業種があるため、留意が必要である。

また、個人情報保護法案との関係では、重要情報インフラの運営者以外の事業者であっても幅広に規制を遵守する必要性があるため別途の留意が必要である。

例えば、中国子会社の運営上、親会社へ中国子会社の従業員の個人情報を提供させることが必要となる場合には、個人情報保護法案に従い、少なくとも子会社・親会社間で個人情報に関する契約を締結し、かつ、データ主体への説明・告知の上、同意を得るというプロセスが必要になる。なお、域外移転の同意に限らず、データ主体からの同意を得る際には、書面による同意を取得し、保管しておくことが実務上は望ましいと考えられる。

個人情報保護法及びデータセキュリティ法が施行された場合には、執行リスクは相当程度あると言わざるを得ない。公布時期等の情報を注視しておく必要がある。

3. シンガポール

(1) 政策的意図・目的・制度の概説

シンガポールにおける個人データの取扱いを定めた法律としては、Personal Data Protection Act 2012(以下、本項において「PDPA」という)が存在し、その下位規則として Personal Data Protection Regulation 2021(以下、本項において「PDP 規則」という)等の諸規則が存在している。また、PDPA の監督・執行機関として、Personal Data Protection Commission Singapore(以下、本項において「PDPC」という)が存在し、PDPA の重要な条項の解釈を示した ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT(以下、本項において「Key Concepts ガイドライン」という)をはじめとする各種ガイドラインが PDPC より発行されている。なお、PDPA 及び PDP 規則は、主に消費者の利便性向上及びデジタル経済の成長促進という観点から、Personal Data Protection(Amendment) Bill 2020 に基づき、2021 年 2 月 1 日付で改正されている。

シンガポールは、2012 年、東南アジア諸国の中でいち早く包括的なデータ保護法である PDPA を導入した(同時期にマレーシア及びフィリピンでも包括的なデータ保護法が導入されている)。シンガポールは多国籍企業のアジア統括拠点が置かれることが多く、アジア拠点が収集したデータがシンガポールのデータセンターで保存されることも多い。そのような背景もあって、シンガポール当局は、個人の権利を保護しつつも柔軟なデータ利活用の要請に応えられるようなデータ保護実務の構築・運用について積極的・継続的に取り組んできた。PDPA は、GDPR の前身である EU データ保護指令を参考にして立法されたものと思われるが、そのような取り組みの結果、施行から 10 年近く経過した現在、シンガポール独自のルールや実務も相当数存在している。

(2) 域外移転規制及びローカライゼーション規制に関する担当省庁・部局

域外移転規制及びローカライゼーション規制に限定せず、PDPA に関する事項一般を担当する組織として、上記(1)記載の PDPC が存在する。

(3) 域外移転規制

ア　域外移転の定義

PDPA では域外移転の定義はおかれておらず、組織等(organization)は、域外移転の対象となる個人データに対して、PDPA に基づく保護に相当する保護の基準を提供することができるようにPDPAに定められた規制に従う場合を除き、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持ち出してはならない(PDPA26 条 1 項)と定めるに留まる。

イ　域外移転規制の対象となるデータの種類・定義

PDPA では、域外移転規制の対象となるデータの種類に制限を設けておらず、個人データ一般が適用対象となる。

PDPA において、個人データとは、「真実であるか否かを問わず、当該情報から、又は当該情報とその組織等がアクセス可能なその他の情報とあわせて、その個人が識別可能な情報」を意味する(PDPA2 条)。ここで保護される「個人」とは自然人を意味するが(PDPA2 条)、死後 10 年を経るまでの死者の個人データについても一定の保護がなされている(PDPA4 条 4 項(b)号)。他方、100 年以上存在する個人データについては、PDPA による保護の対象外とされている(PDPA4 条 4 項(a)号)。Key Concepts ガイドラインでは、典型的な個人データとして、氏名、パスポート番号、ID 番号(シンガポール居住者の ID 番号である NRIC 番号)、個人の写真やビデオ画像、メールアドレス、指紋、DNA、住所等が挙げられている。

また、単なる個人的な目的だけのために提供されたものではない、個人の氏名、肩書、勤務先の電話番号・住所・メールアドレス等の情報については、「ビジネスコンタクト情報(business contact information)」として原則的に PDPA が適用されないこととなる(PDPA4 条 5 項)。Key Concepts ガイドラインにおいては、ビジネスの場での名刺交換により得られた情報がビジネスコンタクト情報に該当する一例であるとされている。

ウ　域外移転規制の対象となる者の定義・範囲

PDPA では、「組織等(organisation)」が規制を受ける対象とされている。「組織等(organisation)」は、シンガポールの法律に基づき設立されたか、又は承認されているかにかかわらず、また、シンガポール居住者か、シンガポールに事務所又は事業を行う場所があるか否かにかかわらず、個人、会社、アソシエーション又は社団等を含むものとして幅広く定義されている(PDPA2 条)。

また、別の組織等のために個人データの保管や所持等の処理を行う組織等である情報仲介者(data intermediary)に関しては、その情報の保管や所持等について、一部の規定(PDPA24 条及び 25 条)を除き、PDPA の規定が適用されない(PDPA4 条 2 項)。例えば、マーケットリサーチ会社やデータサーバー業者等が情報仲介者に該当し得る。ただし、情報仲介者についても、別の組織等のための個人データの保管や所持等以外の活動については、PDPA の規定が適用される。また、情報仲介者が個人データを保管、所持等する場合でも、情報の保管や所持等を委託した組織等には PDPA の規定の適用があり、委託した組織等は、自らが保管や所持等を行っているのと同様に PDPA の義務に服することになる(PDPA4 条 3 項)。

エ　域外移転の条件

上記**ア**記載のとおり、組織等は、域外移転の対象となる個人データが PDPA に基づく保護に相当する保護を受けることができるよう PDPA に定められた規制に従う場合を除き、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持ち出してはならない(PDPA26 条 1 項)。PDPA26 条 1 項を受けて、PDP 規則は、移転元の組織等が、適法で執行可能な義務を通じて、シンガポール国外における個人データの受領者に対して PDPA に基づく保護に相当する水準の個人データの保護義務を負わせるよう、適切な手段を講じる必要があると定めている(PDP 規則 10 条 1 項)[45]。

PDP 規則 10 条 1 項に定める「適法で執行可能な義務」には、以下の文書に基づく義務が含まれる(PDP 規則 11 条 1 項)。

①　法律(PDP 規則 11 条 1 項(a)号)[46]

---

[45] その他の方法として、組織等が PDPC に申請を行った場合、PDPC は、当該組織等による域外移転について PDPA26 条 1 項の規制を免除することができる(PDPA26 条 2 項)。なお、PDPA26 条 2 項が定める PDPC による免除制度は、GDPR の十分性認定とは異なるものであり、対象となるのは移転先の国ではなく組織等による特定のデータ移転であり、かつ、免除の事実は公表されなければならないものではない(PDPA26 条 3 項(b))。申請においては、申請を行う組織自体が規制を免除されるべき理由を、個別の事案に即して、証拠とともに示す必要があり、また免除の事実が公表されていないため、免除が認められる基準は必ずしも明らかではない。

[46] ①法律については、移転先の国に個人データ保護関連の法規制が存在しさえすれば「適法で執行可能な義務」が生じていることは明白なので、PDPA に基づく保護に相当する水準の個人データの保護が当該法規制によって提供されているかが問題となる。いかなる内容の法律であれば当該要件を満たすかという判断基準については、公表されているガイドラインには示されていないため、PDPC に匿名架電照会を行ったところ、個人データを受領する組織等が所在する国において個人データを保護する法令が施行されているか否か、また、かかる法令の性質、特にかかる法令が PDPA と同様のデータ保護条項を含んでいるか否かが主たる基準になるとの回答を受けた。GDPR や GDPR に基づく十分性認定を受けている日本の個人情報保護法が当該要件を満たすか否かについては、満たすと認められる可能性はあると思われるものの、その旨の公的な見解は発表されていない。

② 以下の要件を満たす契約(PDP 規則 11 条 1 項(b)号)(典型的には、当事者間のデータ移転契約)

(a) 受領者が、移転を受ける個人データについて少なくとも PDPA と同等の保護基準を提供することを義務付け(PDP 規則 11 条 2 項(a)号)、かつ

(b) 当該契約において移転先の国及び地域を特定(PDP 規則 11 条 2 項(b)号)する

③ 以下の要件を満たす拘束力がある社内規則(PDP 規則 11 条 1 項(c)号)[47]

(a) 個人データの移転を受ける受領者のうち、①、②及び④の文書に基づく義務を負っていない全ての者に、少なくとも PDPA と同等の保護基準を提供することを義務付け(PDP 規則 11 条 3 項(a)号)、かつ

(b) 当該拘束力がある社内規則が適用される個人データの受領者、当該拘束力がある社内規則によって個人データの移転を受ける国及び地域、並びに、当該拘束力がある社内規則に基づく(通常は移転する側と受領する側の関連する組織間の)権利及び義務を特定する(PDP 規則 11 条 3 項(b)号)

④ その他法的に拘束力がある法律文書(PDP 規則 11 条 1 項(d)号)

上記のうち、②契約については、Key Concepts ガイドラインによれば、PDPC の承認は不要とされているものの、規定すべき事項が公表されており、個人データの移転先が情報仲介者以外である場合には、以下の(a)から(g)に関する規定が置かれる必要がある。また、国外の情報仲介者に個人データを移転する場合には、以下の(c)、(d)及び(g)に関する規定が置かれる必要がある。

(a) 収集、利用及び開示の目的
(b) 正確性
(c) 安全管理措置
(d) 保有制限
(e) 個人データ保護の方針
(f) アクセス及び訂正
(g) データブリーチの通知

さらに、②契約については、PDPC によって承認された契約書の雛形も存在する。すなわち、第 1 回 ASEAN デジタル大臣会議にて、2021 年 1 月 22 日付で、ASEAN 域内での域外移転の根拠として契約を使用する場合における同契約書中の条項の雛形として、ASEAN Model

[47] PDP 規則では、③拘束力のある社内規則は移転元が移転先と関連する場合しか用いることができないとされ(PDP 規則 11 条 3 項(c)号)、移転先が移転元と関連している場合として、(a)移転先が移転元を、直接的若しくは間接的に支配している場合、(b)移転元が移転先を、直接的若しくは間接的に支配している場合、又は(c)移転先と移転元が、同一者により支配されている場合が挙げられている(PDP 規則 11 条 4 項)。要するに、個人データの受領者が移転元のグループ企業等である場合にしか依拠できないということである。

Contractual Clauses for Cross Border Data Flows(以下、本項において「ASEAN モデル条項」という)が公表されている[48]。PDPC からは、同日付で GUIDANCE FOR USE OF ASEAN MODEL CONTRACTUAL CLAUSES FOR CROSS BORDER DATA FLOWS IN SINGAPORE が出されており、域外移転の根拠となる契約として ASEAN モデル条項を使用することが推奨されている。一方で、PDPA に適合するよう、ASEAN モデル条項には以下の修正が必要とされている。

(a) PDPA の定義に適合するよう、ASEAN モデル条項中の“data subject”の定義に個人の死後も個人データが保護される旨を追記すること
(b) PDPA にて定められているデータブリーチ発生時の通知義務が履行されるよう、通知義務を規定すること。具体的には、

- データ仲介者は、データブリーチ発生後、遅滞なく組織等に対してデータブリーチの発生を通知すること
- 組織等は、可及的速やか、かつ 3 暦日以内に PDPC に対してデータブリーチの発生を通知すること
- データブリーチ発生時に、影響を受けるデータ主体に対して、可及的速やかにデータブリーチが発生したことを通知する責任のある者を定めること

加えて、PDP 規則は、上記①～④による措置を講じずとも域外移転が可能な場合として、以下の⑤から⑪を規定している(PDP 規則 10 条 2 項、12 条)。

⑤ データ主体が個人データの移転に同意する場合(PDP 規則 10 条 2 項(a)号)[49]
⑥ 移転に対する一定のみなし同意がある場合(PDP 規則 10 条 2 項(b)号)[50]
⑦ データ主体の同意が PDPA に基づき必要とされない一定の場合(PDP 規則 10 条 2 項(c)号)[51]

---

48 ASEAN モデル条項には、管理者から処理者への移転と管理者から管理者への移転を想定した二種類の雛形が存在する。

49 ⑤データ主体の同意については、同意を取得する前に、移転対象の個人データが移転先において PDPA に相当する保護が与えられる範囲を合理的に説明した文書が交付されなければ、有効な同意とはみなされない(PDP 規則 10 条 3 項(a)号)。当該文書の雛形や記載事項を定めたガイドライン等は存在しないが、当該規定が設けられた趣旨を踏まえると、移転先の国においてどのようなデータ保護法制が適用されるか具体的に記載することが望ましいと考えられる。

50 ⑥移転に対する一定のみなし同意がある場合とは、大要、データ主体が組織等との契約・取引又はデータ主体の要請等による組織等と国外の第三者との間の契約・取引の締結又は履行のために組織等に個人データを提供し、かつ、当該契約・取引のために当該組織等から国外の第三者へ当該個人データを開示することが合理的に必要な場合を意味する(PDP 規則 10 条 2 項(b)号、PDPA15 条)。

51 ⑦データ主体の同意が PDPA に基づき必要とされない一定の場合とは、大要、データ主体の生命、健康又は安全が脅かされる緊急な状況に対応するための使用又は開示等の一定の場合であって、かつ、組織等が、個人データがその受領者によりその他の目的のために使用又は開示されないようにする合理的な手段を講じている場合を意味する(PDP 規則 10 条 2 項(c)号)。

⑧　個人データが送信中の情報で、他の第三者にアクセスや利用をされることがなく他の第三者に開示されないものである場合(PDP 規則 10 条 2 項(d)号)
⑨　個人データがシンガポールで公開されている場合(PDP 規則 10 条 2 項(e)号)
⑩　受領者がデータ仲介者であり、アジア太平洋経済協力(Asia Pacific Economic Cooperation、以下「APEC」という)の処理者プライバシー認証(PRP)システム又は越境プライバシールール(CBPR)システムにおいて認定を受けている場合(PDP 規則 12 条 1 項、12 条 2 項(a))
⑪　受領者がデータ仲介者でない場合で、APEC クロスボーダープライバシールールシステムにおいてその他の認定を受けているとき(PDP 規則 12 条 1 項、12 条 2 項(b))

オ　実務上の対応

上記**エ**記載の域外移転の根拠のうち、現状、実務上よく利用されているのは、②の契約及び⑤のデータ主体の同意である。

ただし、このうち⑤のデータ主体の同意については、同意を取得する前に交付が必要とされている「移転対象の個人データが移転先において PDPA に相当する保護が与えられる範囲を合理的に説明した文書」につき、どのような内容でどの程度記載すべきかの指針が存在せず、具体的に採るべき措置が必ずしも明確とはいえない。また、合理的な必要性なく商品・サービス提供の条件とした同意は無効とされる可能性があり、同意の撤回も可能であることから、法的安定性に欠ける側面がある。さらに、データ主体から同意を取得する機会が存在しない場合もあり得る。そのため、Key Concepts ガイドラインによれば、データ主体の同意は他の措置が実施困難な場合に依拠すべきとされており、実務的には、契約によって対処することが可能な場合は契約に依拠する方針が採られることが多い。

その他、③の拘束力のある社内規則を用いることも考えられるが、当該措置はグループ会社内における移転にしか利用できないという限界がある。また、公表された雛形や詳細な指針も存在しない。

以上を踏まえると、Key Concepts ガイドラインにて規定すべき事項が公表されており、また ASEAN モデル条項が策定された②の契約について、今後は積極的に利用されていくことが予測される。

なお、その他の根拠が用いられる場合はケースバイケースであり、どの要件がよく用いられるかの順位を付けることは難しいが、その他の要件の 1 つに依拠して何らの補充的な措置も実施しない事例は実務上それ程見られない。

カ　域外移転先への域外移転規制の域外適用の有無

上記**ウ**記載のとおり、法令文言上は外国企業にも適用され得る。この点、PDPC は、外国に所在する組織等については、個人データの収集、利用又は開示をシンガポールで行っている場合に PDPA が適用されると考えているようである。

(4) ローカライゼーション規制

ア　ローカライゼーション規制の対象となる者の定義・範囲

ローカライゼーション規制にかかる規定がない。

イ　ローカライゼーション義務の内容(保管制限、データのコピーの移転の可否、データ処理要件等)

ローカライゼーション規制にかかる規定がない。

(5) シンガポールにおける企業活動の留意点

東南アジア諸国には、個人情報保護を定める規制が存在しても当局により監督・執行が行われないため違反しても実質的なリスクが乏しい国も存在するが、シンガポールでは状況は全く異なり、PDPC により積極的に監督・執行が行われている。

PDPC が公表しているところによれば、2016 年以降は、年間 20～30 件程度の執行事例が出ている。また、2019 年には約 59 件、2020 年には約 45 件(ただし、通常月 1 回公表されている執行決定が 4 月から 7 月には出されておらず、おそらくコロナ禍の影響があったためと思われる)の執行事例が出る等、年々執行が積極的に行われる傾向が強まっている。

例えば、公的医療機関を運営する企業の患者データベースがクラッキングされ医療関連個人情報が漏洩した事件では、ソフトウェアによるファイヤーウォールの不導入やパスワードの不適切な管理等、安全管理措置に問題があったとして、2019 年 1 月、IT 機能等をサポートしていた企業に個人情報保護法違反の制裁金としては過去最高額となる 75 万 S ドル(約 6000 万円)の制裁金、運営企業にも不十分な監督体制等を理由に 25 万 S ドル(約 2000 万円)の制裁金を課す決定が公表された。その他、従業員の個人情報を保護する合理的なセキュリティ措置をとらずランサムウェアに感染したとして日系企業が 16,000S ドル(約

120 万円)の制裁金の対象になった事例や域外移転規制違反を理由として制裁金が科された事例、シンガポールに拠点を有さない企業に対する命令が発出された事例等も存在する。

2021 年 2 月に PDPA 及び PDP 規則について大きな改正が行われ、関連するガイドライン等もアップデートされたため、シンガポールで企業活動を行う場合、最新の規制の内容を正確に把握し遵守する必要性は非常に高いと言える。

4. タイ

(1) 政策的意図・目的・制度の概説

Personal Data Protection Act, B.E. 2562 (2019)(以下、本項において「PDPA」という)が個人データ保護について横断的に規律している。

PDPA 制定の背景としては、世界的なビッグデータ活用の流れに伴ってデータ保護・利活用のための法整備の必要性が高まったことに加えて、GDPR の影響が挙げられる。2016 年に厳格な域外移転規制や域外適用の定めにより EU 域外にも大きな影響力を有する GDPR が採択され、その後世界的に GDPR のような統一的なデータ保護法制を導入する動きが活発化してきた。PDPA の制定は、このような流れを受けたものであり、2016 年に法案が提出され、パブリックコメント等を経て 5 度修正された上で、2019 年 2 月 28 日に国家立法議会により承認された。このような背景もあり、PDPA の規制内容は GDPR に非常に類似している。

PDPA は 2020 年 5 月 28 日から全面的に施行され、PDPA に基づく規則及び通知は PDPA の全面施行から 1 年以内に公表されることが予定されていた(PDPA96 条)。しかし、新型コロナウイルス感染症の世界的流行等を原因として、その全面施行は 2022 年 6 月 1 日まで延期されており、同時期まで一定の組織及び事業者たる個人データ管理者について、PDPA のうち第 2 章、第 3 章、第 5 章、第 6 章、第 7 章及び 95 条を適用しないこととされている。適用除外対象外となる組織及び事業者については、政府機関等に加え工業・商業をはじめとする幅広い業種の事業者を含むと規定されており、また、PDPA のうち 2019 年 5 月 28 日付で施行された個人情報保護委員会に係る部分以外のデータ主体の権利、個人情報管理者の義務、罰則等を含む主要な規定ほぼ全てが適用されないと定められているため、実質的に全面的な施行延期の状況となっている。ただし、PDPA は既に一部施行されており、全面施行予定日も決まっているため、本項では PDPA に基づく規制について記載する。

(2) 域外移転規制及びローカライゼーション規制に関する担当省庁・部局

域外移転規制及びローカライゼーション規制に限定せず、PDPA に関する事項一般を担当する組織として、個人情報保護委員会(Personal Data Protection Committee)が設立されることとされている(PDPA 第 1 章)。PDPA 上、同委員会は域外移転規制に関する規則等を制定する権限が付与されている(PDPA16 条)。

(3) 域外移転規制

ア　域外移転の定義

PDPA では域外移転規制自体は存在するものの、域外移転の定義はおかれていない。同規制の詳細は後記**エ**を参照。

イ　域外移転規制の対象となるデータの種類・定義

PDPA では、域外移転規制の対象となるデータの種類に制限を設けておらず、個人データ一般が適用対象となる。

PDPA において、個人データとは、生存する個人に関する情報であり、直接的か間接的かを問わず、当該個人を特定することができるもの(ただし、死者に関する情報は除く)をいう(PDPA6 条)。

ウ　域外移転規制の対象となる者の定義・範囲

PDPA では、域外移転規制の対象となる者に特に限定した規定はおいていないが、タイに所在する管理者又は処理者による個人データの開示については、かかる開示がタイ国内で行われるか否かを問わず PDPA が適用される。また、管理者又は処理者がタイ国外に所在する場合であっても、以下の活動に関する個人データの処理については PDPA が適用される(PDPA5 条)。

① タイに所在する個人に対する商品又はサービスの提供(本人が支払いを行うか否かを問わない)
② タイにおいて行われる個人の行動のモニタリング

エ　域外移転の条件

事業者が個人データを域外に移転する場合、原則として、当該移転先の外国は、個人情報保護委員会が定める個人情報保護の基準に従った十分な個人情報保護の水準を備えている必要がある。ただし、(1)以下のいずれかの要件を満たした場合、(2)企業グループ内の移転等について個人情報保護ポリシーを定めて個人情報保護委員会に認証された場合、及び、(3)同委員会の定める基準と方法に従い情報主体が自身の権利を行使することができる適切な保護措置を備えた場合には、上記規制は適用されない(PDPA28 条、29 条)。

① 法令に基づく場合
② データ主体に、移転先の国又は国際機関が適切な個人データ保護基準を有していないことを通知した上で、本人から同意を得た場合
③ データ主体が当事者である契約の履行のために必要な場合、又は契約を締結する前にデータ主体の依頼に応じた措置を講じるためである場合
④ データ主体の利益のために管理者と他の者又は法人との間で契約を遵守するためである場合
⑤ データ主体又はその他の者の生命、身体又は健康に危害が及ぶことを防止し又は抑制するためであり、その時点で当該データ主体が同意することができない場合
⑥ 重大な公共の利益に関して活動を行うために必要な場合

PDPA 上、個人情報保護委員会が、域外移転が可能となる「個人情報保護の基準に従った十分な個人情報保護の水準」や上記(2)及び(3)の措置の詳細を規定する基準を定めるものとされている。しかし、2021 年 4 月 30 日時点において当該基準は未だ公表されていないため、現時点では、上記(2)及び(3)の措置としてどのような具体的措置を実施すべきかについては不明確である。

オ　実務上の対応

上記**エ**記載のとおり、域外移転が可能となる「個人情報保護の基準に従った十分な個人情報保護の水準」や上記(2)及び(3)の措置の詳細を規定する基準が公表されていない現時点では、②データ主体からの同意を域外移転の根拠とせざるを得ない。ただし、データ主体に通知するべき「移転先の国又は国際機関が適切な個人データ保護基準を有していないこと」としてどのような内容を記載すべきかは必ずしも明確ではないため、今後個人情報保護委員会から公表される細則を確認する必要がある。

カ　域外移転先への域外移転規制の域外適用の有無

上記**ウ**記載のとおり、管理者又は処理者がタイ国外に所在する場合であっても、タイに所在する個人に対する商品又はサービスの提供(本人が支払いを行うか否かを問わない)又はタイにおいて行われる個人の行動のモニタリング活動を行っている場合には、当該活動に関する個人データの処理について PDPA が適用される。

(4) ローカライゼーション規制

ア　ローカライゼーション規制の対象となる者の定義・範囲

ローカライゼーション規制にかかる規定がない。

イ　ローカライゼーション義務の内容(保管制限、データのコピーの移転の可否、データ処理要件等)

ローカライゼーション規制にかかる規定がない。

(5) タイにおける企業活動の留意点

タイでは、PDPA 制定以前でも、最高裁判所が民商法典 420 条に基づき名誉権、プライバシー権が保護の対象になると判示していたため、個人データの不適切な取扱いはこれらの権利を侵害する不法行為とみなされ、損害賠償責任を生じさせる可能性があると解されていた。しかし、従前、タイにおける個人データ保護に関する意識は高いものではなく、当局による監督・執行も積極的に行われていなかった。

もっとも、近年データ漏洩等のセキュリティ事故が報道されるに伴い、人々の意識も変わりつつある。例えば、タイで 2 番目の規模の携帯電話会社である TrueMove H が、約 46,000 人のユーザーの個人データ(ID カード、パスポート、運転免許証のスキャン画像等を含む)を Amazon Web Services(AWS)のクラウドストレージから漏洩させた事件では、国家放送通信委員会が同社に対して質問の通知書を発行した。同社は、当該漏洩が悪質なクラッカーによるものであると説明し、直ちに対応措置を実施したため、同委員会は同社に対する処分等は行わなかった。

今後の見通しとしては、効果的な監督・執行を可能とする個人情報保護委員会の設立及び PDPA の全面施行に伴い、東南アジアの中で最も積極的に監督・執行を行っているシンガポール並に制裁金等の執行例が出てくる可能性もある(PDPA の下では、個人情報保護委員会は最大 500 万バーツ(約 1750 万円)の制裁金を科す権限を有する)。ただ、現実的には、これまでの実務を踏まえて、少なくとも当初は、制裁金等の罰則適用は控え目にして指導や監督を重視した姿勢になるとも思われる(近隣諸国であるマレーシア及びフィリピンも、シンガポール及びタイと同じく統一的な個人情報保護法及び監督・執行機関を有するが、現時点では制裁よりも指導や監督を重視する傾向が強い)。このあたりはまだ予想が付かないのが現状であるが、いずれにしても、従前に比べて当局の監督・執行への姿勢が

より積極的になることは確実だと思われるため、PDPA 遵守のための対応を進めることが重要である。

ただし、PDPA では、上記**(3)エ**記載のとおり、対応すべき具体的措置や基準を下位規則に委任している箇所が多々存在するところ、当該規則が未公表の現状では、対応すべき措置の内容が不明確なものも多い。また、タイでは法律の施行後もその解釈の詳細を定める下位法令や通知等の発出に時間を要することが通例であり(数年経過後も何らの下位法令や通知等も定められないという事態も見られる)、当該規則がいつ頃公表されるのか見通しは不明確なので、その動向を注視する必要がある。このような現状から、日系企業としては現時点でどこまでの対応を行うか悩ましいところであるが、GDPR と類似した規定が多いことに照らせば、GDPR 対応と同様の手順でタイの拠点のデータマッピングを行った上で、法令の文言から明らかな範囲で法令遵守対応を進めることで、個人情報保護に配慮した企業活動を行う必要があると思われる。

5. インド

(1) 政策的意図・目的・制度の概説

ア 各法令の概況

(ア) 現行法

インドにおいては、2021年4月30日時点では、個人情報の保護について包括的に定めた法律は存在しない。しかし、コンピュータに記録された電子データ等の情報の扱いを一般的に規定する2000年情報技術法(Information Technology Act, 2000)(以下、本項において「情報技術法」という)及びその下位規則である2011年情報技術(合理的安全管理措置及び手続並びにセンシティブ個人データ)規則(Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011)(以下、本項において「セキュリティ規則」という)が存在し、これらが個人情報保護について一定の規定を置いている。

(イ) 2019年個人情報保護法案

2018年7月、インド政府が設立した専門委員会から電子情報技術省に対して、2018年個人データ保護に関する法案が提出され、当該法案を元に、2019年12月11日に国会に個人情報保護法案(the Personal Data Protection Bill)が提出された(以下、本項において2019年12月11日に国会に提出された時点での法案(Bill No.373 of 2019)を「2019年個人情報保護法案」という)。2019年個人情報保護法案は、法案前文規定のとおり、インドにおける個人情報の保護について包括的に定める初めての法案であり、2021年4月30日時点において、国会で審議中である。本法案は、個人データ(Personal Data)に関連する個人のプライバシーの保護を規定し、個人データの利用等につき規定を設け、個人データを処理する者と事業体との間の信頼関係を創設し、個人データを加工される者の権利を保護し、データの加工に関する組織的及び技術的措置の枠組みを創設する等の目的で設けられたものである。また、本法案は、DPOの選任、data protection impact assessmentの実施、privacy by design policyの規定等、GDPRのコンセプトを取り入れているが、GDPRとは異なり、センシティブ個人データと重要個人データ(中央政府が指定する個人データ)という類型のデータについて域外移転規制及びローカライゼーション規制を課している。同法案の内容は未だ確定しておらず、現地報道によると、どのような形でローカライゼーション規制を規定するかについては特に議論が紛糾しているとのことである。

(ウ) Non-Personal Data Governance Framework

Non-Personal Data Governance Framework に関する専門家委員会は、インド電子情報技術省により構成された専門家委員会であり、2020 年 7 月と 12 月に、匿名化されたデータ等の個人データに該当しないデータ(非個人データ(Non-Personal Data))に関する規律についての報告書を提出している。当該専門家委員会の 12 月のレポートでは、非個人データに関する定義の検討や非個人データ種類ごとの考察(Public non-personal data、Community non-personal data、Private non-personal data の 3 分類に分けた考察)、2019 年個人情報保護法案との関係、非個人データに関する権利の考察、非個人データを管轄する当局(Non-Personal Data Authority)の設立にかかる提案等が行われている。報告書には、非個人データ一般につき、域外移転規制及びローカライゼーション規制を新たに設ける旨の提案は記載されていない。ただし、12 月に提出された改訂版報告書の 8.15 項では、非個人データは、人々の生活の様々な側面から取得されるものであり、匿名化の解除がされる可能性があり、公開された場合、プライバシーの重大な損失が生じてしまうことから、個人データから派生した非個人データは、元の個人データの機密性(sensitivity)を受け継ぐものとされている(同時に、この機密性は、2019 年保護法案記載のとおり、データの保存義務を要請するものであるとも記載されている)。このため、2019 年個人情報保護法案が法律として成立した場合、非個人データの元となるデータが、2019 年個人情報保護法案上の域外移転規制及びローカライゼーション規制に服するセンシティブ個人データ(定義につき、下記**(3)イ(イ)**参照)に該当するときには、匿名化された非個人データであっても域外移転規制やローカライゼーション規制に服すると解される可能性も否定できない。もっとも、この点について現時点で明確な見通しを立てることは困難である。

(2) 域外移転規制及びローカライゼーション規制に関する担当省庁・部局

現行法には、域外のものに限定せず、一般的に第三者に対する移転規制が設けられており(下記**(3)イ(イ)**参照)、当該規制は電子情報技術省が管轄省庁である。

2019 年個人情報保護法案も、電子情報技術省が主導する形で策定が進められている。本法案では、情報保護庁(Data Protection Authority)という当局を設立することとなっており(2019 年個人情報保護法案 41 条)、本法案に関する監督や執行は情報保護庁が管轄することとなっている(同法案 49 条 2 項(a))。後述するように、域外移転については、情報保護庁が承認した標準契約条項又はグループ内スキームに服して行われる場合や、特定の目的で移転を承認した場合等に認められるため、域外移転の承認についても、情報保護庁が主要な役割を果たしている。

(3) 域外移転規制

ア　域外移転の定義

インド現行法には、域外移転規制・ローカライゼーション規制が存在しない(後述するように域外・域内を問わず、一般的に情報の第三者に対する移転を規制する法令は存在する)。2019 年個人情報保護法案には、センシティブ個人データ等を「処理のためにインド国外に移転する」際に適用される域外移転規制及びローカライゼーション規制の制度が存在するが、法案上、それ以上に詳細な定義は不見当である。

イ　域外移転規制の対象となるデータの種類・定義

(ア) 現行法

現行法には域外規制特有の規定はないが、個人データの第三者に対する移転一般を規律するデータ移転規制は存在する。セキュリティ規則は、個人データの内容を定義するとともに、個人データの一部をセンシティブ個人データと定義付けている。

現行法では、個人データとは、「自然人に関する情報であって、事業者が保有し、又は保有可能性のある他の情報と合わせて、直接又は間接に、当該自然人を識別することができる情報をいう」と定義されている(セキュリティ規則 2 条(1)(i))。この中でも、より要保護性の高い類型として、センシティブ個人データという類型が定められており、センシティブ個人データとは、以下に関する情報からなる個人データを意味すると定義されている(セキュリティ規則 3 条。ただし、公表されている情報又は法令に基づいて提供される情報は、センシティブ個人データの定義から除かれる)。このセンシティブ個人データがデータ移転規制の対象となっている。

① パスワード
② 金融情報(銀行口座、クレジットカード情報、デビットカード情報その他の支払手段の詳細)
③ 身体的、生理的特徴又は精神衛生状況
④ 性的指向
⑤ 医療記録及び履歴
⑥ 生体認証情報
⑦ 事業者のサービス提供のために提供された、上記各号に関連する情報
⑧ 適法な契約その他の方法に基づき事業者が取扱い又は保管するため上記各号に従って受領した情報

(イ) 2019 年個人情報保護法案

2019 年個人情報保護法案では、個人データは、「オンラインかオフラインかを問わず、自然人のアイデンティティの特色、特性、属性、又はその他の特徴、あるいはそのような特徴との組み合わせを考慮して、直接的又は間接的に識別可能な自然人に関するデータを意味する。その他の情報、及びプロファイリングの目的でそのようなデータから引き出された推論を含むものとする」とされている(2019 年個人情報保護法案 3 条(28))。

このうち、特に要保護性の高い情報として、センシティブ個人データ、それよりも更に重要なデータ類型として、重要個人データ(critical personal data)が定められていて、これら 2 類型の情報は、域外移転規制の対象となるデータである。

センシティブ個人データは、以下を明らかにするか、以下に関連するか、又は以下を構成する個人データと定義されている(2019 年個人情報保護法案 3 条(36))。

① 金融データ
② 公的な識別情報
③ 性生活に関する情報
④ 性的指向
⑤ 生体認証データ
⑥ 遺伝データ
⑦ トランスジェンダーであるという情報
⑧ インターセックスであるという情報
⑨ カースト又は部族に関する情報
⑩ 宗教的又は政治的信念等
⑪ その他、2019 年法案 15 条に基づいてセンシティブ個人データとして分類されるデータ[52]

重要個人データ(critical personal data)については、2019 年法案 33 条 2 項の注記にて、通達により意味を定める旨が示されているものの、2021 年 4 月 30 日時点では、当該通達はまだ発出されていない。

[52] 2019 年法案 15 条では、インド政府は、関係当局と協議して一定のカテゴリーのデータをセンシティブ個人データとして指定しなければならないと規定されているが、法案が未成立であるため当該指定は未了であると思われる。

ウ　域外移転規制の対象となる者の定義・範囲

(ア) 現行法

情報技術法には、実体法上の適用範囲を制限する規定はないが、セキュリティ規則については、2011 年 8 月 24 日付電子情報技術省通知において、インドに所在する事業者に適用されることが明記されている。

(イ) 2019 年個人情報保護法案

2019 年法案は以下に対して適用があるとされている(2 条(A))。

① 個人データがインド国内において取得、開示又は共有等の処理がなされる場合の個人データの処理
② インド政府、インド企業、インドの個人若しくはインド法に基づいて設立・創設されたいかなる主体又はその集合体による個人データの処理
③ インドにおいて行われる事業、若しくはインド国内のデータ主体に提供される商品・サービスの計画的活動に関して、又はインド国内で、データ主体のプロファイリングに関する活動に関して、インド国内に所在しないデータ受託者(GDPR における管理者に相当する概念)若しくはデータ処理者により行われる個人データの処理

エ　域外移転の条件

(ア) 現行法

域外移転の場合に限定されない個人データの第三者への移転に対する規制は存在する。具体的には、事業者及び事業者に代わり行動する者は、センシティブ個人データを、セキュリティ規則に従って当該事業者が講じることと同レベルのデータ保護を確保するインド国内外の事業者や個人に対してのみ、移転することができる。さらに、当該移転は、移転元の事業者等とデータ主体との間の適法な契約の履行に必要な場合、又はデータ主体が当該データ移転に同意した場合にのみ認められる(セキュリティ規則 7 条)。なお、センシティブ個人データに該当しない個人データは当該規制の対象とはならない。

(イ) 2019 年個人情報保護法案

2019 年法案では、センシティブ個人データについて、データ主体の明確な同意を得た上で、当該個人データのコピーを国内に保存し、かつ、以下の条件に服することを条件としてのみ、処理のためにインド国外に移転することができるとされている(2019 年法案 34 条 1 項。なお、同条の義務は、個人情報一般ではなく、センシティブ個人データに限定して適用される)。

① 当該移転が、情報保護庁(Data Protection Authority)が以下の規定を備えるものとして承認した標準契約条項又はグループ内スキームに服して行われる場合
- 2019 年法案に基づくデータ主体の権利の効果的な保護についての規定
- 標準契約条項又はグループ内スキームの規定の不遵守によって引き起こされた損害に対するデータ受託者の責任についての規定

② インド政府が特定の国、国のある産業セクター、又は特定の国際組織への移転を以下の認定に伴い許可した場合(ただし、本認定は定期的に見直される)
- 適用法及びその他条約を考慮し、センシティブ個人データが十分なレベルの保護に服すること
- 情報の移転が適切な管轄権を持つ当局による関連する法律の執行に不利益な影響を与えないこと

③ 具体的な目的に照らした必要性に鑑み、当局が特定の移転を許可した場合

重要個人データについては、国内でのみ処理することが想定されているため原則として域外移転は許されず、以下の場合のみ例外的に国外に移転することができる。

④ 2019 年法案 12 条に定める目的のため即時の行動をとる厳格な必要性があって、健康に関するサービスや緊急サービスの提供を行う個人・組織へ提供する場合(ただし、所定の期間内に当局への通知が必要)

⑤ 上記②の場合で、かつ、インド政府が、移転が国家の安全と戦略的利益に悪影響を与えないという意見を有する場合

加えて、個人情報一般について、個人情報の収集時に、域外移転を行おうとすることの通知を行うべき義務が新設されるとともに(2019 年法案 7 条(h))、個人情報の処理に当たってはデータ主体の同意が必要とされている(2019 年法案 11 条 1 項)。

オ　実務上の対応

(ア) 現行法

センシティブ個人データを第三者に移転する方法については、上記**エ**記載のとおりである。

まず、移転の際の移転先の保護基準の確保については、具体的には、移転元と移転先の間で契約を締結し、当該契約において手当する方法が実務的に多くみられる。

これに加えて、「移転元の事業者等とデータ主体との間の適法な契約の履行に必要な場合、又はデータ主体が当該データ移転に同意した場合にのみ認められる」という要件については、実務的には、データ主体の同意を取得する方法が一般的であり、プライバシーポ

リシーに条件として記載した上でデータ主体に同意してもらう方法、個別の同意書を取得する方法、データ主体との契約の条項に組み込む方法等がとられている。

(イ) 2019 年個人情報保護法案

まだ法案の段階なので、上記**エ**記載の法案の文言以上の実務等は存在しない。

カ　域外移転先への域外移転規制の域外適用の有無

(ア) 現行法

法令上明記されていない。

(イ) 2019 年個人情報保護法案

法案上明記されていない。

(4) ローカライゼーション規制

ア　ローカライゼーション規制の対象となる者の定義・範囲

(ア) 現行法

ローカライゼーション規制にかかる規定がない。

(イ) 2019 年個人情報保護法案

上記**(3)ウ(イ)**と同様。

イ　ローカライゼーション義務の内容(保管制限、データのコピーの移転の可否、データ処理要件等)

(ア) 現行法

ローカライゼーション規制にかかる規定がない。

(イ) 2019 年個人情報保護法案

上記**(3)エ(イ)**記載のとおり、2019 年法案では、センシティブ個人データをインド国外に移転する場合の要件の 1 つとして、当該データのコピーをインド国内でも保存することが義務付けられている(2019 年法案 33 条(1))。また、重要個人データは、原則としてインド国内でのみ処理することが義務付けられている(2019 年法案 33 条(2))。

(5) インドにおける企業活動の留意点

インドでは、従前個人データに対する法規制は厳しいものではなく、当局による監督・執行も積極的なものではなかった。

現在審議中の 2019 年法案は、そのような状況において、域外移転規制やローカライゼーション規制を含む厳格な法規制を導入するものであるため、インドにおける企業活動に大きな影響を与え得ると思われる。特にインドは、豊富な IT 人材を誇る国であり、外国企業からデータ処理等のアウトソーシングを受けている企業も多い。そのような企業にとっては、個人データの国外のみでの保存や国際的な移動を制約する規制が導入され監督・執行が活発化された場合、企業活動の大きな障害となり得る。そのような背景もあり、2019 年法案は、2021 年 4 月 30 日時点において未だ国会にて審議中であり、ローカライゼーション規制の要否及び内容については特に議論が紛糾している。そのため、2019 年法案は今後修正される可能性があり、いつ頃どのような内容で成立するか正確に予測することは困難である。

もっとも、2019 年法案がどのような内容で成立するとしても、現在のインドの個人情報保護関連規制を大きく変更・厳格化するものになり、今後個人情報関連規制の監督・執行が徐々に活発化していく可能性は高いと思われる。同法案の制定に伴って様々な法令対応作業も必要となり得るため、その動向を注視するとともに、インドにおいても個人情報保護に配慮して企業活動を行う必要があると思われる。

6. ベトナム

(1) 政策的意図・目的・制度の概説

ア 各法令の概況

(ア) 現行法

ベトナムには、包括的な個人情報保護法令や独立した監督・執行機関は存在せず、個別の法令がそれぞれ個人情報やプライバシーの保護に関する規定を定めている。

具体的には、民間事業者に一般的に適用される民法が「個人の私的生活に関する情報、家族の秘密に関する情報、個人の手紙・電話・電報・電子的データベースその他の私的情報」を対象として取得・第三者提供等の際の一般的な同意取得義務を定めている他に、近年主に問題となる情報技術を活用した個人情報の取扱いに適用され得る代表的な法令として、以下の①から⑥が存在する。

① サイバー情報セキュリティ法：ベトナムにおいてサイバー情報保護に直接従事又は関与する個人及び団体に適用される。
② 情報技術法：ベトナムにおいて情報技術の利用・開発に従事する個人及び団体に適用される。
③ 消費者権利保護法：ベトナムにおいて、商品・サービスを販売・提供する組織・個人(営利を目的とする市場において、商品の製造から販売又はサービスの提供までの投資行為の 1 つ、複数又は全てを行う組織・個人)及び消費者権利保護活動に関する機関・組織・個人に適用される。
④ 電子商取引に関する政令 52 号(以下、本項において「政令 52 号」という)：ベトナムの領土内で電子商取引活動(商業的な宣伝や商品又はサービスの販売を提供するウェブサイトを開設すること等)に従事する個人及び団体に適用される。
⑤ サイバーセキュリティ法：ベトナムにおいて電気通信ネットワーク又はインターネット上のサービスその他サイバー空間上の付加価値サービスを提供する国内外事業者等に適用される。
⑥ インターネットサービス及びオンライン情報の管理、提供及び利用に関する政令 72 号(以下、本項において「政令 72 号」という)：一定のオンラインサービス事業者に適用される(詳細は後述する)。

(イ) 個人情報保護に関する政令案

ベトナムで初めての統一的な個人情報保護法令になると予測される個人情報保護に関する政令の第一案が 2019 年 12 月、第二案が 2021 年 2 月にパブリックコメントのために公安省のウェブサイト上で公開された。当該第二案(以下、本項において「本政令案」という)を見る限り、日本の個人情報保護法のように、個人情報の保護に焦点を当てて、民間事業者の個人情報の取扱全般について規定する統一的な法令になると予想される。本政令案は、DPO の選任、data protection impact assessment の実施、データ処理の基本原則の規定等、一部GDPRのコンセプトを取り入れているが、GDPRとは異なり、センシティブ個人データの処理や個人データの域外移転について個人情報保護委員会の事前承認が必要となる等当局の関与が強い内容となっており、個人データの域外移転の要件の 1 つとしてローカライゼーション規制も導入している。同政令案の内容は未だ確定しておらず、今後パブリックコメントの結果を踏まえた改訂案が公表される可能性がある。

(2) 域外移転規制及びローカライゼーション規制に関する担当省庁・部局

現行法は法令によって管轄当局が異なっているが、ローカライゼーション規制については、公安省ハイテク犯罪防止サイバーセキュリティ局、情報通信省情報セキュリティ局等が主に管轄している。本政令案は公安省が管轄しており、公安省の下に個人情報保護委員会が設立されることが予定されている。

(3) 域外移転規制

ア　域外移転の定義

(ア) 現行法

域外移転規制にかかる規定がない。

(イ) 個人情報保護に関する政令案

「ベトナムの国境及び領土外に移転する」ことが規制されているが、それ以上の定義は存在しない。

イ　域外移転規制の対象となるデータの種類・定義

(ア) 現行法

域外移転規制にかかる規定がない。

（イ）個人情報保護に関する政令案

本政令案では、個人情報全般が域外移転規制の対象とされている。本政令案上、個人情報は、「個人に関する情報又は特定の個人の識別又は識別するための性質に関する情報」と広く定義された上で(本政令案 2 条 1 項)、基礎個人情報とセンシティブ個人情報に区分され、それぞれに以下の情報が含まれると規定されている。

a　基礎個人情報(本政令案 2 条 2 項各号)

① 氏名、ミドルネーム及び出生名、別名(存在する場合)
② 生年月日、死亡又は行方不明の日
③ 血液型及び性別
④ 出生地、出生登録地、永住地、現住居、出身地、連絡先アドレス及び電子メールアドレス
⑤ 学歴
⑥ 民族的出自
⑦ 国籍
⑧ 電話番号
⑨ ID カード番号、パスポート番号、市民識別番号、運転免許証番号、プレート番号、個人税識別番号及び社会保険番号
⑩ 婚姻状況
⑪ オンラインにおける活動又は活動履歴を反映した情報

b　センシティブ個人情報(本政令案 2 条 3 項各号)

① 政治的・宗教的見解に関する個人情報
② 個人の健康情報、すなわち医療サービスへの登録又は当該サービスの提供の過程で収集及び特定されたデータ主体の身体的・精神的健康状態に関する情報
③ 個人の遺伝的情報、すなわち各個人の遺伝された又は獲得された遺伝的特徴に関する情報
④ 個人の生体情報、すなわち個人の身体的・生物学的特徴に関する情報
⑤ 性別の状況に関する個人情報、すなわち男性、女性、ジェンダー中立、両性具有若しくは男性と女性の両方の特徴を有する又は出生時に同定された性別と異なる性別を自己認識する人々に関する情報
⑥ 生活及び性的指向に関する個人情報
⑦ 法執行機関が収集・保管する犯罪者や犯罪行為に関する個人情報
⑧ 個人金融情報、すなわち金融機関が個人に提供する口座、カード又は決済手段を識別するために使用される情報、又は、金融機関、原金融データ及び本人との関係に関する情報(記録、財政状態、信用履歴及び所得水準を含む)

⑨　個人の所在地情報、すなわち、個人の以前及び現在の物理的な所在地に関する情報
⑩　社会的関係に関する個人情報
⑪　その他法令に定める個人情報

ウ　域外移転規制の対象となる者の定義・範囲

(ア) 現行法

域外移転規制にかかる規定はない。

(イ) 個人情報保護に関する政令案

個人情報に関係する機関、組織及び個人に適用され(本政令案 1 条 2 項)、ベトナムで事業を行っている国内外の全ての組織、企業及び個人が違反の責任を負うと規定されている(本政令案 4 条 2 項)。

エ　域外移転の条件

(ア) 現行法

域外移転規制にかかる規定はない。もっとも、個人情報を第三者に移転することに対する規制は存在し、個人情報を第三者に開示するためにはデータ主体の同意を取得する必要がある。また、国家機密に該当する情報を外国の第三者に提供する場合は、当局の承認取得等の手続を実施する必要がある。ベトナム法上国家機密の内容は広く定義されており、その外延が不明確なものも存在する。

(イ) 個人情報保護に関する政令案

本政令案は、個人情報の域外移転規制及びローカライゼーション規制を有しており、具体的には、「ベトナム市民の個人情報は、以下の 4 つの要件が完全に満たされた場合、ベトナムの国境及び領土外に移転することができる」と定めている(本政令案 21 条 1 項)。

①　データ主体が移転に同意する
②　オリジナルの情報がベトナムで保存される
③　情報を受領する国、領土又は当該国若しくは領土内の特定の地域が、本政令に定める水準と等しい又はそれ以上の水準の個人情報保護に関する規制を有していることを証明する書類が付与される
④　個人情報保護委員会の書面による承認を得る

また、本政令案は、類似した規定として、「個人情報は、次の場合には本条第1項に定める要件(注：上記本政令案21条1項に規定された4要件)を満たさずにベトナム領域外に移転することができる」とも定めている(本政令案21条3項)。

① データ主体が移転に同意する
② 個人情報保護委員会の書面による承認を得る
③ 個人情報を保護するための情報処理者のコミットメントが存在する
④ 個人情報保護手段を実施するための個人情報タ処理者のコミットメントが存在する

本政令案の文言はベトナム語の原文でも趣旨不明瞭な部分が散見され、上記要件の詳細や、上記本政令案21条1項と3項の関係(どのような場合に本政令案21条3項に依拠してローカライゼーション義務を免れることができるか等)は現時点では不明確である。

オ　実務上の対応

ベトナムの現行法上、個人情報の域外への持ち出し又は域外の第三者への提供といった域外移転に当たり得るデータ処理について禁止又は制約する規制は存在しない。もっとも、個人情報を処理する場所がデータ主体への通知事項とされており、個人情報を取得して第三者に提供するためには原則データ主体からの同意取得が必要であるため、実務上、域外移転についてもデータ主体に通知して同意を取得することが多い。

カ　域外移転先への域外移転規制の域外適用の有無

(ア) 現行法

域外移転規制にかかる規定がない。

(イ) 個人情報保護に関する政令案

本政令案上明記されておらず不明確である。

(4) ローカライゼーション規制

ア　ローカライゼーション規制の対象となる者の定義・範囲

(ア) 現行法

a　サイバーセキュリティ法に基づく規制

サイバーセキュリティ法は、「ベトナムにおいて電気通信ネットワーク又はインターネット上のサービスその他サイバー空間上の付加価値サービスを提供する国内外事業者が、ベトナムにおける個人情報に関するデータ、サービス利用者の関係に関するデータ又はサービス利用者の作成したデータの収集、利用、分析又は加工を行う場合、ベトナム政府の定める一定期間中は、それらのデータをベトナムで保存しなければならない。本項に規定する外国事業者はベトナムに支店又は駐在員事務所を設けなければならない」と規定している(サイバーセキュリティ法 26 条 3 項)。

上記義務が適用される「ベトナムにおいて電気通信ネットワーク又はインターネット上のサービスその他サイバー空間上の付加価値サービスを提供する国内外事業者」は文言上全てのオンラインサービス事業者が含まれるかのようにも読み得るため、その外延は不明確である。また、上記義務の対象となる「個人情報に関するデータ、サービス利用者の関係に関するデータ又はサービス利用者の作成したデータ」についても、同法には「個人情報」の定義が存在せずその外延は不明確である。

当該義務は詳細な施行規則を政令で定めることとされているところ(同法 26 条 4 項)、当該政令は 2021 年 4 月 30 日時点で制定に至っていない。当該政令については、2019 年 1 月末までドラフトがパブリックコメントに付されており、当該ドラフトにおいては、①ローカライゼーション義務が適用されるサービスの内容が具体的に列挙されるとともに[53]、②事業者がサイバーセキュリティ法に違反し是正要求を受けたにもかかわらず是正措置を講じなかった場合に適用場面が限定され、③事業者の当該義務の履行について当局の要請から一定の猶予期間が与えられていた。しかし、2021 年 4 月 30 日時点でも、未だベトナム政府は当該政令案を検討中であるため、上記ドラフトと大きく異なった内容で政令が制定される可能性も否定はできない。

---

[53] ローカライゼーション義務が適用されるサービスとして、例えば、クラウド上のデータ保管・共有サービス、E メールサービス、SNS・ソーシャルメディアサービス、テレコムサービス、インターネット接続サービス、国内向けドメイン名提供サービス、オンライン決済サービス、支払仲介サービス、ｅコマース・オンラインビデオゲーム提供サービス等が列挙されていた。

もっとも、ベトナムが無制限なローカライゼーションを禁止する CPTTP 及び地域的な包括的経済連携(Regional Comprehensive Economic Partnership(以下「RCEP」という)に加入していることやサイバーセキュリティ法に基づくローカライゼーション義務が国内外で強く批判されたこと等に鑑みると、上記ドラフトの建付を大きく変更して無制限・広い範囲のローカライゼーション義務が規定される可能性は高くないものと考えられる。

b　政令 72 号に基づく規制

政令 72 号は、サイバーセキュリティ法が制定される以前から、以下のオンラインサービス事業者を対象として、サービス提供のためにベトナム当局におけるライセンス取得、登録、通知等の手続を求めるとともに、「情報通信省が定めるとおりサービス提供に関する顧客の苦情に対応するため、管轄行政当局による情報の検査、確認、保管及び提供の要求に対応可能なサーバーシステムを少なくとも 1 台ベトナムに設置する」義務を課している(政令 72 号 24 条 2 項、25 条 8 項、28 条 2 項及び 34 条 2 項)。

① 一般ウェブサイト[54]を開設する団体及び企業(所謂ニュース配信サービス等がこれに該当すると考えられる)
② ソーシャルネットワーキングサービスを提供する団体及び企業
③ 移動電気通信ネットワークにおいて情報コンテンツサービスを提供する団体及び企業(携帯電話網を用いて SMS 等で情報を配信するサービス等がこれに該当すると考えられる)
④ オンライン電子ゲームサービス事業者

(イ)個人情報保護に関する政令案

上記**(3)エ(イ)**記載のとおり、域外移転規制の要件の 1 つとしてローカライゼーション規制が定められている。当該規制の適用対象は、本政令案が適用される事業者であり、具体的には、上記**(3)ウ(イ)**記載のとおり、個人データに関係する機関、組織及び個人に適用され(本政令案 1 条 2 項)、ベトナムで事業を行っている国内外の全ての組織、企業及び個人が違反の責任を負う(本政令案 4 条 2 項)。

[54] 政令 72 号上、「一般ウェブサイト」とは「機関、団体又は企業のウェブサイトであって、正確に公式の情報源を引用し、かつ、その著者の氏名又は公式の情報源の機関の名称及び掲載又は放送の時期を明示した上で、一般的な情報を提供するもの」と定義されている(政令 72 号 20 条 2 項)。

イ　ローカライゼーション義務の内容(保管制限、データのコピーの移転の可否、データ処理要件等)

(ア) 現行法

a　サイバーセキュリティ法に基づく規制

上記(4)ア(ア)に記載のとおり、「個人情報に関するデータ、サービス利用者の関係に関するデータ又はサービス利用者の作成したデータ」(又はそのコピー)を国内に保存する必要がある。また、外国事業者はベトナムに支店又は駐在員事務所を設ける必要がある。

b　政令 72 号に基づく規制

上記(4)ア(ア)に記載のとおり、一定のオンラインサービス事業者は、管轄行政当局による情報の検査、確認、保管及び提供の要求に対応可能なサーバーシステムを少なくとも1台ベトナムに設置する必要がある。

(イ) 個人情報保護に関する政令案

上記(3)エ(イ)に記載のとおり、個人情報(又はそのコピー)を国内に保存することが要件とされているが、それ以上の詳細は現時点では不明確である。

(5) ベトナムにおける企業活動の留意点

ア　執行の傾向について

ベトナムでは、現行法においても民間事業者に対して個人情報の安全管理義務が課されており、個人情報漏洩事故も数多く発生しているものの、民間の情報漏洩事故や個人情報保護体制の不備等に対して当局が何らかの処分を下したという執行事例は(少なくとも公表情報を調査して把握できる限りでは)未だ存在しない。Electric Central や Vietnam Airlines の顧客情報流出事件が比較的目立った事例として報道されているが、当局は調査を行ったようであるものの、何らかの処分を行ったという情報は公になっていない。また、個人情報の漏洩や無断提供について消費者が訴訟を提起したという事例も、公開情報を調査した限りでは、銀行の顧客が銀行によって自らの個人情報が漏洩されたと主張し訴訟提起した事案が1件見当たったのみであった。

このように、ベトナム当局は、現状、個人情報保護という観点では執行に積極的ではない。しかし、治安維持や税務取締まり等のために自らにとって個人情報が必要な場面では執行に積極的な傾向があるため、留意が必要である。例えば、ベトナム当局が脱税その他

のベトナム法上の違法行為の捜査のために日系企業にベトナム人顧客の個人情報の提供を求めてくるような事態は実務的にも想定されるところである。

イ　ローカライゼーション規制について

また、近年、ベトナム当局が国外に所在するオンラインサービス事業者に対する法適用に積極的な姿勢を見せつつある。そのため、そのような法適用の実効性を確保するためのローカライゼーション義務についても留意する必要が高まっていると言える。

この点、現時点では、ベトナム当局が上記(4)記載のローカライゼーション規制違反を根拠にオンラインサービス事業者に罰則等を科した執行事例は公表されていない。しかし、公開情報を調査したところ、以下の報道のように、ベトナム当局がベトナム国内に拠点を置いていない外国の大手オンラインサービス事業者に対してベトナム法を遵守した対応等を求めている旨の報道が見当たっている。

① Facebook に対して、ベトナム法上違法とされるコンテンツ(中傷的な内容、反政府的な意見、個人や組織の名誉を損なう投稿等)をベトナムユーザーが投稿することを容認している点を問題視し、ベトナム法を遵守した削除等の対応を求めている旨の報道
② Netflix に対して、ベトナム法上違法なコンテンツの削除要請をした旨の報道やベトナムに納税するよう追徴課税をした旨の報道(この件については、ベトナム当局がNetflix に対してベトナム国内におけるサーバー設置や事業所開設を求めている旨や、Netflix サイドはそのような義務は負っていないと主張している旨も報道されている)
③ Apple Store や Google Play に対して、ベトナム法上違法なコンテンツを含むゲームを配信しないよう求めた旨の報道

ベトナム当局が上記のような要請を行っている背景として、上記で挙げた外国のオンラインサービスはいずれもベトナム国民の生活に与える影響が大きいということが挙げられる。例えば、Facebook はベトナムで最も利用されているソーシャルネットワーキングサービスであり、当該サービスを利用して、政府批判の運動や税務当局が補足できない私人間取引が行われていると言われている。また、Netflix は多数のベトナム人ユーザーを有しており、ベトナムで大きな売上を上げていると言われている。これらの事業者は、ベトナム当局からの要請についてベトナム当局と協議して、削除要請等については可能な範囲で対応しているようであるが、現状、ベトナム国内へのサーバー又は事業所の設置についてまで対応した旨の報道は見当たっていない。おそらく、ベトナム当局としては、外国に所在する事業者に対しては物理的な強制執行が難しいこともあり、少なくとも現時点では、当該事業者が任意で削除要請等に応じた場合には、それ以上にローカライゼーションを強硬に求めたり、罰則等を科したりする方針を採っていないように思われる。

もっとも、海外大手サービスプロバイダーの対応状況や今後制定されるサイバーセキュリティ法の施行規則を定める政令及び後述する個人情報保護に関する政令の内容次第では、このようなベトナム当局の対応がより強硬なものとなる可能性も存在する。そのため、特にベトナム人ユーザーの数が多くベトナム人の生活に与える影響が大きいサービスを提供するオンラインサービス事業者については、これらの政令の制定状況含め現地の最新の動向を注視しておく必要がある。

ウ　個人情報保護に関する政令案について

本政令案には 2021 年 12 月に施行される旨が規定されているが、ベトナムでは、政令が予定どおり施行されないことは珍しくない。また、2021 年 2 月に募集されたパブリックコメントでは厳格な域外移転規制やローカライゼーション規制について批判するコメントも相当数提出されたようなので、今後本政令案の内容が変更される可能性も相当程度ある。

もっとも、本政令案がどのような内容で成立するとしても、現在のベトナムの個人情報保護関連規制を大きく変更・厳格化するものになり、今後個人情報関連規制の監督・執行が徐々に活発化していく可能性は高いと思われる。本政令案の制定に伴って様々な法令対応作業も必要となり得るため、その動向を注視するとともに、ベトナムにおいても個人情報保護に配慮して企業活動を行う必要があると思われる。

7　その他(インドネシア)

東南アジア・南アジア地域では、従前包括的な個人情報保護法令や域外移転規制・ローカライゼーション規制が存在する国は少なかったが、従前から域外移転規制・ローカライゼーション規制が存在する国や、GDPR の影響を受けて域外移転規制を定める個人情報保護法令を導入する動きが見られる国も存在する。

特にインドネシアは ASEAN で最大の人口を有する国であり、日系企業の進出も盛んであることから、以下ではインドネシアの関連規制について簡単に紹介する。

ア　域外移転規制

(ア) 現行法

個人データのインドネシア国外への移転は、通信情報大臣とのコラボレーションにより実施されることとされている(電子システムにおける個人情報保護に関する 2016 年通信情報省規則第 20 号(以下、本項において「2016 年規則」という)22 条 1 項 a)。当該コラボレーションにおいては、①移転先の国、移転の相手方、移転日、移転の理由を最低限内容に含む報告の実施、②必要に応じた弁護活動の要請、及び③移転の結果報告の実施を行うことが規定されている(2016 年規則 22 条 2 項)。

もっとも、上記以上に詳細なガイドラインは存在せず、また、2021 年 4 月 30 日時点で通信情報省の公表情報を確認する限りは、当該コラボレーションの実施実績や実施方法についての情報は不見当である。したがって、2021 年 4 月 30 日時点では、個人データをインドネシア国外に移転する際に通信情報大臣といかなる方法でコラボレーションを行うか確認することは容易ではない。当職らの把握する限り、かかる域外移転規制に反して当局から何らかの指導や制裁が実施された実例も見当たらない。インドネシアにおける個人データの域外移転規制は、現時点では、ルールは存在するもののそれを遵守する方法が不明確で、実際に遵守をしている企業があるとの情報も得られておらず、遵守しなかった場合に生じる結果も不明であり、かかるルールは実態としては空文化しているように思われる。

なお、前提として、電子システムを利用する事業者が個人データを取得、収集、加工、分析、保存、表示、発表、送付、配布、公開又は消去するに際しては、原則として、書面又は電子的方法にて、インドネシア語を用いて、特定の個人を識別可能なデータに関する当該特定の個人の同意を取得する必要がある(2019 年政令 14 条 2 項、3 項、2016 年規則 6 条、1 条 4 項)。したがって、域外移転か否かにかかわらず、およそ個人データの第三者提供を行うに当たっては、当該特定の個人からの同意をインドネシア語を用いた書面により取得する必要がある。

（イ）個人データ保護法案

現在、インドネシア通信情報省とインドネシア法務人権省、更にはインドネシア金融サービス庁等の関連当局も巻き込んだ上で、個人データ保護に関する統一的な法令の制定に向けた活動が進められており、2020年1月24日には、個人データ保護法案が国会に提出された(以下、本項において「本法案」という)。本法案にはローカライゼーション規制は規定されていないが、以下の域外移転移転規制が定められている。

本法案49条では、域外移転の条件を以下のとおり定めることが予定されている。

① 移転先国にインドネシアと同等以上の個人データ保護規則があること
② インドネシアと移転先国の間の国家間同意があること
③ 移転元の個人データ管理者と移転先の個人データ管理者の間に個人データの処理に関する契約があること
④ データ主体の同意が得られていること

なお、本法案が提出されて以降、2021年4月30日時点では目立った動きはないものの、国会ウェブサイト及び通信情報省ホームページの2020年9月1日付公表記事によれば、国会に本法案を制定するための作業部会が設置され、早期制定に向けて対応が進められているとのことである。インドネシアにおいて法律の制定タイミングを予測することは非常に難しいものの、今後の動向を注視する必要がある。

イ　ローカライゼーション規制

電子システム及び取引の実施に関する2019年政令71号(以下、本項において「2019年政令」という)においては、公共部門の電子システム提供者は、インドネシア国内に電子システム及び電子データを管理、処理又は保存することが義務付けられている(2019年政令20条2項)。他方、民間部門の電子システム提供者は、インドネシア国外で電子システム及び電子データを管理、処理又は保存することができる(2019年政令21条1項)。

公共部門と民間部門の区別であるが、公共部門は中央及び地方の政府機関(金融サービス庁は除く)並びに政府機関から任命された者が該当する(2019年政令2条3項、4項)。民間部門は、政府機関により規制又は監督される電子システム提供者で、以下の目的に利用するウェブポータル、ウェブサイト又はアプリケーションを保有する者とされている(2019年政令2条5項)。

① 物又はサービスの申込み又は取引の提供、管理又は運営

② 金融取引サービスの提供、管理又は運営
③ ウェブポータル、ウェブサイト、電子メール、その他のアプリケーションを通じて利用者のデバイスにダウンロードすることによる資料又は有料コンテンツの配布
④ ショートメール、音声通信、ビデオ電話、電子メール、チャットルーム、ネットワーキングサービス、ソーシャルメディア等のコミュニケーションサービスの提供、管理又は運営
⑤ サーチエンジンサービス又はテキスト、音声、画像、アニメーション、音楽、ビデオ、映画、ゲーム若しくはこれらの組み合わせの形式における電子情報の提供サービス
⑥ 電子取引活動に関する公共の利益に資する活動のための個人データの処理

なお、公共部門の電子システム提供者に該当すると、電子システム及び電子データをインドネシア国内で保存する必要が生じるだけでなく、当該電子システム提供者向けに開発したソフトウェアのソースコードをインドネシア政府に提供する必要も生じる(2019 年政令 9 条 1 項)。公共部門と民間部門の区別は必ずしも明確ではないことから、公共サービスに近い事業を営む会社等は特に慎重に検討することが求められる。

第 3 データ越境流通に関連する国際ルール

1. 概要

第 2 にて整理したとおり、各国は、それぞれ様々な政策的意図や目的に基づいて、域外移転規制やローカライゼーション規制を設けており、事業者としては、これらの規制の内容を把握し、法的リスクに適切に対応することが重要である。

もっとも、日本政府としては、日本企業によるデータ流通やその利活用を促進する国際的枠組みの構築や、日本企業の足かせとなる規制制度を採用する国に対する働きかけのために、関連する国際ルールに基づく提案を行うこともあり得る。

このような国際ルールとしては、加盟国/締約国による貿易制限措置に対する規律を定めたWTO協定等の貿易協定と、OECDが1980年に採択したガイドラインを始めとした、プライバシー保護に関する国際ルールがある。

2. 貿易協定

WTO 協定上、域外移転規制やローカライゼーション規制それ自体を直接対象とした規律は存在しない。もっとも、一般的に、データの越境流通は、何らかのサービスの提供の一環として行われることが多いことから、サービスの貿易に関する一般協定(General Agreement on Trade in Services。以下「GATS」という)における規律が関連し得る。

また、近年、環太平洋パートナーシップに関する包括的及び先進的な協定(Comprehensive and Progressive Agreement for Trans-Pacific Partnership。以下「CPTPP」という)等の地域貿易協定(Regional Trade Agreement。以下「RTA」という)において、域外移転規制やローカライゼーション規制を直接対象とした規律が設けられるようになっている。

(1) GATS

各国の域外移転規制・ローカライゼーション規制がGATS違反となるか否かを分析するに当たっては、①当該規制がその国の自由化約束を行ったサービス分野に影響を与えるか、②当該規制が GATS 上の義務規定に抵触するか、③GATS 上の正当化事由の要件を満たし正当化されないかという観点から検討を行うことが有益である。

ア　自由化約束の範囲

後記**イ**で言及するGATS上の義務のうち、最恵国待遇義務を除いては、加盟国が約束表において自由化を約束したサービス分野に適用される。すなわち、加盟国は、各種のサービス分野について、4つのモード[55]ごとに、市場アクセス義務及び内国民待遇の義務を受け入れるか否かを決めることができる。また、この義務を受け入れる場合にも、内外差別的な措置を一定の範囲で留保でき(例えば、銀行業について預金業務を除いて内国民待遇を付与する等)、留保した場合、その内容を約束表に明記する必要がある。

加盟国は、1991年に国際連合が作成した暫定中央生産分類(Provisional Central Product Classification)に基づきWTO事務局が作成したサービス分類表(Servics Sectroral List, W/120)に従って、自由化の約束を行っている。サービス分類表では、様々なサービスが大きく12分野に分類されており、各分野ごとに細分類が設けられている。このうち、域外移転規制やローカライゼーション規制と特に関連し得るものとして、電子計算機及び関連のサービス(Computer and Related Services)及び電気通信サービス(Telecommunications Services)がある。前者は、「ハードウェア設置に関連する相談サービス」、「ソフトウェア実行サービス」、「データ処理サービス」及び「データ・ベースサービス」を含み、後者は、「パケット交換データ伝送サービス」、「回線交換データ伝送サービス」、「電子メール」、「情報及びデータベースのオンラインでの検索」等を含む。

また、WTO先例においては、加盟国が、あるサービス分野に関して、約束表上、無制限の自由化約束を行った場合、当該サービス分野については、電子的手段を含む、あらゆる手段について自由化約束を行ったものと解される[56]。そのため、例えば、「経営相談サービス」の越境取引(第1モード)について自由化約束を行った加盟国が、域外移転規制やローカライゼーション規制によって、オンラインでの国境を越えた経営相談サービスの提供に影響を与えた場合、GATS上の義務違反の問題が生じ得る。さらに、「小売サービス」の現地拠点を通じたサービス提供(第3モード)について自由化約束を行った加盟国が、域外移転規制やローカライゼーション規制によって、他の加盟国の事業者が現地拠点を通じて提供する小売サービスに影響を与えた場合(例えば、現地拠点が取得した購買データを分析のた

55　4つのモードとは、①越境取引(第1モード。ある加盟国のサービス事業者が、自国に所在しながら、他の加盟国に所在する顧客に対して、サービス提供を行う場合)、②国外消費(第2モード。ある加盟国のサービス事業者が、自国にやってきた他の加盟国の顧客に対して、サービス提供を行う場合)、③現地拠点を通じたサービス提供(第3モード。ある加盟国のサービス事業者が、他の加盟国に現地法人等の拠点を設置し、当該拠点からサービス提供を行う場合)、④人の移動(第4モード。ある加盟国のサービス提供者が、自らの従業員等を他の加盟国に派遣して、当該他の加盟国に所在する顧客にサービス提供を行う場合)をいう。

56　Panel Report, *US - Gambling*, para. 6.287.

めに本社に転送することが妨げられるような場合)にも、GATS 上の義務違反の問題が生じ得る[57]。

このように、域外移転規制やローカライゼーション規制は、様々なサービス分野に関連し得ることから、各国規制の GATS 整合性を分析するに当たっては、当該規制が約束表上のどのようなサービス分野に対して影響を与えるかを幅広く検討する必要がある。

イ　GATS 上の義務

域外移転規制及びローカライゼーション規制との関係で主に問題となる GATS 上の義務は、内国民待遇義務、最恵国待遇義務、市場アクセス義務及び国内規制の合理的実施義務の４つである。

(ア) 内国民待遇義務

GATS 17 条の内国民待遇義務は、他の加盟国のサービス及びサービス提供者に対して、同種の国内のサービス及びサービス提供者と比べて不利でない待遇を与えなければならないという原則である。

内国民待遇は、①法文上、他国のサービス又はサービス提供者を、自国のサービス又はサービス提供者より不利に取り扱っている場合(*de jure*)はもちろん、②事実上、他国のサービス又はサービス提供者を、自国のサービス又はサービス提供者より不利に取り扱っている場合(*de facto*)も含まれる(GATS 17 条 2 項、3 項)。なお、競争上不利に作用するかどうかは、競争関係に影響を与えるか(サービス提供において障害が課せられるか)との観点から検討される(GATS 17 条 3 項)[58]。

したがって、加盟国が、内国民待遇を約束したサービス分野において、域外移転規制やローカライゼーション規制によって、他の加盟国のサービス及びサービス提供者に対して、自国の同種のサービス又はサービス提供者と比べて、競争上不利な取扱いを行っている場合、内国民待遇義務違反の問題が生じ得る。特に、ローカライゼーション規制は、サービス提供者に対して自国内にサーバーやデータセンター等の設備等を義務付けるものであり、外国事業者に対して追加的な負担を課すものであることから、内国民待遇義務違反の問題が生じる可能性がある[59]。

57　阿部克則「データローカライゼーション措置と国際経済法上の規律―WTO と TPP における法的位置づけ―」フィナンシャル・レビュー140 号 25 頁、33-34 頁(2019)。

58　Appellate Body Report, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, paras. 137-138.

59　Daniel Crosby, “Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments”, E15 Initiative, Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the World Economic Forum.

(イ) 最恵国待遇義務

GATS 2条の定める最恵国待遇義務は、いずれかの国に与える最も有利な待遇を、他の全ての加盟国に対して与えなければならないという義務であり、最恵国待遇義務は、自由化約束の有無にかかわらず、一律に適用される。法文上(*de jure*)の不利取扱いのみならず、事実上(*de facto*)の不利取扱いも禁止される。各要件の解釈においては、基本的に、内国民待遇義務における議論が参照され得る。

したがって、加盟国が、域外移転規制やローカライゼーション規制によって、他の加盟国のサービス及びサービス提供者に対して、他国の同種のサービス又はサービス提供者と比べ、均等ではない競争条件を課しているような場合、最恵国待遇義務違反の問題が生じ得る。もっとも、GDPR における十分性認定のように、個人情報保護の水準に応じて他の加盟国を区別する場合、十分性認定がなされた国のサービスと、十分性認定がなされていない国のサービスは、そもそも「同種」のサービスではないとの整理もあり得る[60]。

(ウ) 市場アクセス義務

GATS 16 条 2 項は、加盟国が、市場アクセスを約束した特定のサービス分野について、サービス提供者の数の制限(同項(a)号)やサービスの総算出量の制限(同項(c)号)といった措置をとることを禁止している。

これに関して、WTO 先例上、米国が第 1 モードの賭博サービスの供給について、無条件の自由化を約束した事案で[61]、米国によるオンラインの越境賭博サービスの提供禁止措置は、数量制限の一種である「ゼロ割当て」であるとして、サービス提供者の数の制限(同項(a)号)及びサービスの総算出量の制限(同項(c)号)に該当するとした先例がある[62]。
このことから、オンラインによるデータ処理・データベースサービスにおいて市場アクセスを約束した加盟国が、域外移転規制を導入した場合、それが当該分野におけるサービス提供者の数の制限又はサービスの総産出量の制限に該当するとして、GATS 16 条違反の問題が生じる可能性が指摘されている[63]。

(エ) 国内規制の合理的実施義務

GATS 6条1項は、自由化約束を行ったサービス分野において一般に適用される加盟国の措置のうち、サービス貿易に影響を及ぼすものが、合理的、客観的かつ公平な態様で実施されることを確保する義務を定めている。同条に関する判断を示した WTO 先例は不見当だが、「合理的」といえるためには、必要性・比例性まで満たしている必要はなく、問題と

---

60 阿部克則「データローカライゼーション措置と国際経済法上の規律―WTO と TPP における法的位置づけ―」フィナンシャル・レビュー140 号 25 頁、34 頁(2019)。

61 Appellate Body Report, *US - Gambling*, paras. 214-215.

62 *Ibid.*, *US - Gambling*, paras. 224-239.

63 Andrew D. Mitchell & Jarrod Hepburn, "Don't Fence Me In : Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer", 19 Yale J.L. & Tech. 182 (2017).

なっている適用態様に合理的な理由が認められれば足りると解されている[64]。また「客観的」とは、措置の適用態様が恣意的でないことをいい[65]、「公平な」とは、ある者又はある商業上の利益に対して、特別な配慮や特権を与えないことをいうと解されている[66]。これら 3 要件は、密接に関連し、類似の機能を有するが、それぞれ独立した法的義務であると解されている[67]。

また、GATS 6 条 5 項、4 項(b)号[68]は、加盟国が、自由化約束を行ったサービス分野において、客観的な、かつ、サービスの質を確保するために必要である以上に大きな負担となるような態様で、免許要件、資格要件及び技術上の基準に関連する措置を適用することを禁じている。「サービスの質を確保するために必要である以上に大きな負担とならないこと」という要件は、措置の必要性に関するものであるが、GATS のその他の場面における必要性テストと異なり、貿易制限の程度との関係ではなく、サービス提供者に対する負担の程度との関係で評価される[69]。

したがって、加盟国が、自由化約束を行ったサービス分野において、域外移転規制やローカライゼーション規制によって、他の加盟国のサービス及びサービス提供者に対して、サービスの質を確保するために必要である以上の負担を課したり、合理的・客観的・公平でない態様によりこれらの規制を適用した場合には、GATS 6 条違反の問題が生じ得る。

ウ　正当化事由

仮に加盟国の措置が GATS 上の義務に抵触するものであったとしても、一般的例外又は安全保障例外の要件を満たせば、正当化され、GATS 違反とはならない。

---

64 Rüdiger Wolfrum, Peter-Tobias Stoll, and Clemens Feinäugle, WTO - TRADE IN SERVICES, p. 171 (2008).

65 *Ibid.*, p. 171 (2008).

66 *Ibid.*, p. 172 (2008).

67 *Ibid.*, p. 172 (2008).

68 本義務は、サービス貿易理事会が、GATS 6 条 4 項に基づき、当該サービス分野におけるサービス分野に対する不必要な障害を除去するための規律を定めるまでの義務であるが、本報告書作成日現在、「会計サービス部門における国内規制についての規律(Discipline on Domestic Regulation in the Accountancy Sector)」を除き、そのような規律は定められていない(WTO, WTO negotiations on domestic regulation disciplines , available at <https://www.wto.org/english/tratop_e/serv_e/dom_reg_negs_e.htm#:~:text=The%20mandate%20of%20the%20Working,the%20scope%20of%20the%20GATS>.)。

69 Wolfrum et al., *supra* note 64, pp. 187-188 (2008).

(ア)一般的例外(GATS 14 条)

GATS 14 条による正当化が認められるには、問題となっている措置が、①同条(a)号ないし(e)号のいずれか[70]に該当し、かつ、②同条柱書の要件を満たす必要がある。そして、①について、域外移転規制やローカライゼーション規制との関係では、特に(i)公衆の道徳の保護又は公の秩序の維持のために必要な措置(同条(a)号)及び(ii)GATS に反しない法令の遵守を確保するために必要な措置(同条(c)号)が問題となり得る。

まず、上記(i)について、「公衆の道徳」は、地域又は国により維持される又は代表される正邪に関する基準に言及したもの、「公の秩序」は、公共の政策及び法により反映される、社会の基本的な利益の保護に言及したものと解釈されている[71]。また、「公衆の道徳」及び「公の秩序」の意義や保護の度合いは、各国の制度及び価値観に基づく一定の裁量が認められている[72]。さらに、「必要な措置」といえるかの判断に当たっては、(i)当該措置が保護しようとしている利益の相対的な重要性、(ii)当該措置の目的達成に対する寄与の程度、(iii)当該措置の貿易制限的効果の程度、及び(iv)目的を達成するための、合理的に実施可能かつ WTO 協定に整合的な(又は WTO 協定違反の程度がより低い)代替措置の有無が考慮される[73]。

次に、上記(ii)について、まず、GATS に反しない法令か否かという点について、先例上、仮に法令の一部が GATS に整合しない場合でも、その他の規定が、GATS 不整合の規定の影響を受けず、GATS に整合するといえる場合には、当該 GATS に整合する規定は、「GATS の規定に反しない法令」に該当すると考えられている。そして、GATS 14 条(c)号は、正当化される措置の具体例として、「個人の情報を処理し及び公表することに関連する私生活の保護又は個人の記録及び勘定の秘密の保護」(同号(ii))及び「安全」(同号(iii))を例示している。また、「必要な(necessary)」措置といえるか否かの判断に当たっては、(i)法令の具体的な規範、義務又は要件の遵守を確保することの重要性、(ii)法令の具体的な規範、義務又は要件の遵守の確保に対する対象措置の貢献の程度及び(iii)対象措置の貿易制限的効果の程度を考慮して判断される[74]。

---

70 同条(b)号は「人、動物又は植物の生命又は健康の保護のために必要な措置」、(d)号は「取扱いの差異が他の加盟国のサービス又はサービス提供者に関する直接税の公平な又は効果的な賦課又は徴収を確保することを目的とする場合には、17 条の規定に合致しない措置」、(e)号は「取扱いの差異が加盟国の拘束される二重課税の回避に関する協定又は他の国際協定若しくは国際取極における二重課税の回避についての規定の結果による場合には、2 条の規定に合致しない措置」とされている。

71 Panel Report, *US - Gambling*, paras. 6.465 and 6.467.

72 *Ibid.*, *US - Gambling*, para. 6.461. Appellate Body Report, *US - Gambling*, paras. 308 and 311.

73 Appellate Body Report, *US - Gambling*, paras. 306-307 (Appellate Body Report, *Korea - Various Measures on Beef*, paras. 162, 164 and 166 を引用)。なお、Appellate Body Report, *Korea - Various Measures on Beef*, para. 165 も参照。

74 Appellate Body Report, *Argentina - Financial Services*, paras. 6.227-6.234.

最後に、同条柱書の要件である「恣意的若しくは不当な差別の手段となるような態様で又はサービスの貿易に対する偽装した制限となるような態様で適用しないこと」(上記②)に関しては、措置の構造等を踏まえ、(i)措置の適用が差別的か、(ii)当該差別が恣意的又は不当な性質を有するか、及び(iii)当該差別が同様の条件の下にある国の間で生じているかが検討される[75]。

第 2 において整理したとおり、各国の域外移転規制やローカライゼーション規制は、個人データの保護やサイバーセキュリティの確保等様々な政策意図に基づいてなされているところ、その多くは、GATS 14 条(a)号又は(c)号のいずれかには該当する可能性が高い。もっとも、GATS 14 条(a)号又は(c)号のいずれによる場合であっても、目的を達成するために必要な措置であることや、差別的な態様で適用されるものではないことは必要である。

(イ) 安全保障例外(GATS 14 条の 2)

GATS 14 条の 2 による正当化が認められるのは、加盟国が、①自国の安全保障上の重大な利益に反すると認める情報の提供を拒否すること(同条(a)号)、②自国の安全保障上の重大な利益の保護のために必要と認める(i)軍事施設のためのサービスに対する措置(同条(b)号(i))、(ii)核分裂物質等に関する措置(同号(ii))、又は(iii)戦時等の緊急時にとる措置をとること(同号(iii))、③国際の平和及び安全の維持のため国際連合憲章に基づく義務に従った措置をとること(同条(c)号)である。

これらの規定には、いずれも「必要と認める」等の自己判断的要素が含まれており、加盟国に広範な裁量が認められている。ただし、同様の条文構造を有する GATT 21 条(b)号(iii)についての先例では、同号(i)ないし(iii)が定める事由があったかどうかについては客観的な審査が及び、「安全保障上の重大な利益の保護のために必要であると認める」という文言も、同例外規定を援用する加盟国が、安全保障上の重大な利益の内容を明示する義務負うとの判断がなされており[76]、安全保障例外の援用が加盟国の自由裁量に完全に委ねられることが明らかになっている。

域外移転規制やローカライゼーション規制についても、規制の対象となるデータの種類によっては、特に上記②によって、自国の安全保障上の重大な利益を保護するための措置について、加盟国に広範な裁量が認められる可能性がある[77]。

---

[75] Panel Report, *Argentina – Financial Services*, paras. 7.745-7.746, citing Appellate Body Report, *US – Shrimp*, para. 184, Panel Report, *Argentina – Financial Services*, para. 7.748, citing Appellate Body Report, *EC – Seal Products*, para. 5.302.

[76] Panel Report, *Russia – Traffic in Transit*, paras. 7.101 and 7.134.

[77] Mitchell & Hepburn, *supra* note 63, pp. 205-206.

(2) RTA

デジタル技術を活用した取引が増加するにつれ、そのような取引に関する国際的なルール作りの重要性が認識されるようになり、各国が締結する RTA においては、「電子商取引章」や「デジタル貿易章」が設けられ、域外移転規制やローカライゼーション規制を直接規律した条項が含まれるようになっている。

以下の**図表 5** は、日本が**第 2** で取り扱った各国との間で締結している RTA(①CPTPP、②RCEP、③経済上の連携に関する日本国と欧州連合との間の協定(Agreement Between the European Union andJapan for an Economic Partnership。以下「日 EUEPA」という)及び④日本国とインド共和国との間の包括的経済連携協定(Comprehensive Economic Partnership Agreement Between Japan and the Republic of India。以下「日印 EPA」という))における域外移転規制に関する規律及びローカライゼーション規制に関する規律の有無を示したものである。なお、日本は当事者ではないものの、ASEAN においては、域外移転規制及びローカライゼーション規制に関する規定を含む電子商取引に関する協定(Agreement on Electronic Commerce。以下「AEC」という)が締結されている[78]。また、APEC においても、デジタル貿易に関するルール作りに向けた動きが存在する[79]。

---

[78] ASEAN Agreement on Electronic Commerce, available at <http://agreement.asean.org/media/download/20190306035048.pdf>.

[79] 日本経済新聞「デジタル貿易で米中含むルール　アジア太平洋地域で検討」(2021 年 4 月 24 日)<https://www.nikkei.com/article/DGXZQOUA0982K0Z00C21A4000000/>。

【図表 5：国際的ルールにおける規律の整理】

	CPTPP	RCEP	日 EUEPA	日印 EPA	(参考) ASEAN AEC	(参考) APEC
日本	○	○	○	○		○
EU			○			
中国		○				○
シンガポール	○	○			○	○
タイ		○			○	○
インド				○		
ベトナム	○	○			○	○
インドネシア		○			○	○
域外移転規制に対する規律	○	○	×	×	△	－
ローカライゼーション規制に対する規律	○	○	×	×	○	－

なお、各 RTA においては、それぞれサービス貿易章も設けられており、各国は、市場アクセス義務及び内国民待遇義務に関して、GATS における約束を超えた約束を行っている。そのため、各 RTA において関連するサービス分野が自由化約束の対象となっている場合、当該 RTA におけるサービス貿易章における義務(前記**(1)**参照)の違反がないかを検討することも有益である[80]。

ア　域外移転規制に対する規律

(ア) CPTPP

CPTPP 14.11 条 2 項は、各締約国が、対象者の事業の実施のために行われる情報(個人情報を含む)の電子的手段による移転を許可しなければならないことを定めている。ここで

[80] この他、各 RTA においては、投資章も設けられているところ、域外移転規制やデータローカライゼーション規制については、間接収用の禁止や公正衡平待遇義務といった投資協定上の義務との関係が問題となる余地もある。もっとも、データが「投資財産」に該当するか否かが必ずしも明らかではないほか、ある措置が間接収用や公正衡平待遇義務違反に当たるか否かは、具体的な事実関係に依存する(Mitchell & Hepburn, *supra* note 63, p. 216)。

いう、「対象者」とは、「対象投資財産」[81]、「締約国の投資家」及び「締約国のサービス提供者」をいい、金融機関や金融サービスの提供者は除外されている(CPTPP 14.1 条)。このように、CPTPP の下では、域外移転規制は原則として禁止されている。

もっとも、CPTPP 14.11 条 3 項は、公共政策の正当な目的を達成するための措置が、①恣意的又は不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されず、②目的の達成のために必要である以上に情報の移転に制限を課すものではないことを条件に、正当化されることを認めている。ここでいう、「公共政策の正当な目的」の内容について、先例等はないものの、GATS 14 条と異なって限定列挙の形式をとっていないことから、様々な政策目的を含む可能性があり、その外延は明確ではない。一方、上記①及び②の文言は、GATS 14 条における同一又は類似の文言に関する先例上の解釈(前記**(1)ウ(ア)**)が参照され得る[82]。

また、CPTPP 29.1 条 3 項は、GATS における一般的例外(前記**(1)ウ(ア)**参照)を準用している。

さらに CPTPP 29.2 条は、安全保障例外として、①自国の安全保障上重大な利益に反すると当該締約国が決定する情報の提供又はそのような情報へのアクセスを拒否すること、②国際の平和等に関する自国の義務の履行及び自国の安全保障上の重大な利益の保護のために必要と認める措置の正当化を認めている。特に②は、「自国の安全保障上の重大な利益の保護のために必要と認める措置」という、GATS における安全保障例外(前記**(1)ウ(イ)**参照)と比較して一般的な文言を採用しているため、GATS よりも広範に正当化が認められる可能性がある。

(イ) RCEP

RCEP 12.15 条 2 項は、情報の電子的手段による国境を超える移転が対象者の事業の実施のために行われる場合には、当該移転を妨げてはならない旨を定めている。「対象者」の意義は CPTPP と同様である(RCEP 12.1 条)。このように、RCEP の下でも、域外移転規制は原則として禁止されている。

もっとも、RCEP 12.15 条 3 項(a)号は、CPTPP 14.11 条 3 項に相当する公共政策目的に基づく例外について、「締約国が公共政策目的を達成するために必要であると認める」という自己判断的な文言を採用した上で、注釈において「この(a)の適用上、締約国は、正当な公

---

81 一の締約国について当該一の締約国の領域内の他の締約国の投資家の投資財産であって、当該協定が効力を生ずる日に存在しているもの又はその後に設立され、取得され、若しくは拡張されるものをいう(CPTPP 9.1 条)。

82 Mitchell & Hepburn, *supra* note 63, pp. 209-210. なお、②については、「必要である以上に」という文言が、貿易の技術的障害に関する協定 2.2 条と共通していることから、同条における先例上の解釈が参照され、措置実施国の裁量が一定程度尊重されるのではないかとの指摘もある(米谷三以・藤井康次郎・河合優子「連載　TPP と政府・企業法務：第 9 回　電子商取引」NBL1080 号 84 頁、90 頁(2016))。

共政策の実施の必要性については実施する締約国が決定することを確認する」と明記しており、締約国に広範な裁量が認められることを明らかにしている。

また、RCEP 12.15 条 3 項(b)号は、協定全体に適用される安全保障例外である 17.13 条とは別に、「締約国が自国の安全保障上の重大な利益の保護のために必要であると認められる措置」が正当化される旨を規定している。さらに、同号は、「他の締約国は、当該措置については、争わない」と規定しており、安全保障に基づく例外についても、締約国に広範な裁量が認められることを明らかにしている。

(ウ) 日 EUEPA

日 EUEPA は、電子商取引に関する節(第 8 章第 F 節)を有するものの、域外移転規制に対する規律は含まれず、効力発生日から 3 年以内に、データの自由な流通に関する規定を含めることの必要性について再評価する旨の規定が置かれたのみである。

(エ) 日印 EPA

日印 EPA には電子商取引やデジタル貿易に関する章がなく、域外移転規制に対する規律も存在しない。

イ　ローカライゼーション規制に対する規律

(ア) CPTPP

CPTPP 14.13 条 2 項は、いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてサーバーやストレージといったコンピュータ関連設備を利用し、又は設置することを要求してはならないと定めている。このように、CPTPP の下では、ローカライゼーション規制は原則として禁止されている。

もっとも、CPTPP 14.13 条 3 項は、CPTPP 14.11 条 3 項(前記**ア(ア)**参照)と同様の、公共政策目的による例外を定めている。

また、CPTPP 14.13 条 2 項の義務の違反についても、同協定において適用される一般的例外規定及び安全保障例外(前記**ア(ア)**参照)によって正当化され得る。

(イ) RCEP

RCEP 12.14 条 2 項は、いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてサーバーやストレージといったコンピュータ関連設備を利用し、又は設置することを要求してはならないと定めている。このように、CPTPP の下においても、ローカライゼーション規制は原則として禁止されている。

もっとも、RCEP 12.14 条 3 項は、RCEP 12.15 条 3 項(前記**ア(イ)**参照)と同様に、締約国の広範な裁量を認める公共政策目的例外及び安全保障例外を定めている。

(ウ) 日 EUEPA

前記**ア(ウ)**に記載のとおり、日 EUEPA には、電子商取引に関する節が置かれているものの、ローカライゼーション規制に対する規律は存在せず、データの自由な流通に関する再評価条項が存在するのみである。

(エ) 日印 EPA

日印 EPA には電子商取引やデジタル貿易に関する章がなく、ローカライゼーション規制に対する規律も存在しない。

3. プライバシー保護に関する国際ルール

プライバシー保護の分野では、主に法的拘束力のないソフトローによって、各国が採用するプライバシー保護の取り組みについて、一定の枠組みが設けられている。以下では、こうしたプライバシー保護に関する国際ルールのうち、**第 2** で取り扱った各国との関係性が深いものについて、その概要及びデータの越境流通に係る枠組みを概説する。

(1) OECD プライバシーガイドライン

OECD は、1980 年 9 月 23 日、各国におけるプライバシー保護法を調和させるとともに、プライバシーに関する個人の権利を保護しつつ、国際的なデータの流通を促進することを目的として、プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告(Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data。以下「OECD プライバシーガイドライン」という)を採択した。OECD プライバシーガイドラインは、個人データ保護に関する 8 つの基本原則(①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全確保の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則)を定めており、非拘束的なソフトローであるが、個人データ保護の取り組みに関する国際的な標準となっている[83]。2013 年には、個人データの流通量の増加やリスクの変化、個人情報の取扱いに関するアプローチの変化を踏まえた改正がなされた。

データ越境流通に関して、OECD プライバシーガイドラインは、第 4 部において、以下の内容を定めている。

① データ管理者は、自らが管理する個人データに関して、当該データの所在場所にかかわらず責任を負う。

---

[83] 日本の個人情報保護法も、当該 8 原則に則っている(「OECD8 原則と個人情報取扱事業者の義務規定の対応」<https://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/pdfs/03.pdf>)。

② 加盟国は、自国と他の国との間における個人データの越境流通について、本ガイドラインに適合する継続的な保護の水準を保つため、(a)他の国が本ガイドラインを実質的に遵守している場合、又は(b)実効的な執行の仕組み及び個人情報管理者により導入される適切な措置を含む、十分な保護措置が存在する場合、当該越境流通を制限することを控えるべきである。

③ 個人データの越境流通に対するいかなる制限も、当該情報の機微性並びに域外移転の目的及び情況を考慮した、当該流通によって引き起こされるリスクに比例した制限でなければならない。

このように、OECD プライバシーガイドラインにおいては、個人の権利の保護と個人データの国際流通の促進のバランスをとるために、十分な保護の水準を保つことができる限りデータ越境流通を認めるという考え方がとられており、このような考え方は、GDPR における十分性認定等においても表れている。また、データ越境流通に対する制限は、リスクの程度に比例したものでなければならないとされていることから、政策意図との関係で必要な範囲を超えた域外移転規制やローカライゼーション規制は、OECD プライバシーガイドラインの観点からも問題があるということになると思われる。

(2) 欧州 108 号条約

欧州評議会(Council of Europe)は、1949 年に設立された、人権及び民主主義、法の支配の分野における条約策定や基準策定を主導する国際機関で、EU 加盟国、英国、旧ユーゴスラビア諸国、ロシア、ウクライナ、トルコ等、全 47 ヵ国が加盟している。

1981 年、欧州評議会は、個人データの自動処理に係る個人の保護に関する条約(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data。以下「欧州 108 号条約」という)を採択した。同条約は、個人データ保護の分野において法的な拘束力を有する唯一の条約である。同条約は、OECD プライバシーガイドライン類似の基本原則を定めており、批准国は、その内容を反映した個人データ保護に関する国内法を制定する義務を負っている(同条約 4 号)。本報告書作成現在、欧州評議会の加盟国全 47 国に、アルゼンチン、カーボベルデ、モロッコ、モーリシャス、メキシコ、セネガル、チュニジア及びウルグアイを加えた、全 55 ヵ国が欧州 108 号条約を批准している。また、同条約の諮問委員会には、批准国のほか、日本、米国、カナダ、オーストラリア、韓国等がオブザーバーとして参加している。

欧州 108 号条約は、12 条において、他の締約国へのデータ越境流通に関して、以下の内容を定めている。

① この規定は、自動処理される個人データ又は自動処理される目的で収集された個人データが媒体の如何を問わず国境を越えて移転される場合に適用する。
② 締約国は、プライバシー保護の目的のみを理由として、他の締約国の領域への個人データの越境流通を禁じ又は特別の許可に付してはならない。
③ しかしながら、各締約国は、次の場合、第2項の規定を制限する権利を有する。
(a) ある特定の種類の個人データ又は自動処理個人データファイルに対し、当該データ又は当該ファイルの性質を理由として、その国内法が特別の規定を含んでいる場合。ただし、相手側締約国の規定が同等の保護を定めている場合を除く。
(b) 締約国の領域から他の締約国の領域の仲介を経て非締約国の領域へ移転される場合において、当該移転が移転する締約国の法令の適用を回避することになることを防ぐため。

また、2001 年には、非締約国へのデータ越境流通に関する規定を含んだ追加議定書(Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows)を採択された。追加議定書における非締約国へのデータ越境流通に関する規定(2条)は、以下のとおりである。

① 各当事国は、条約の当事国でない国又は機関の管轄下にある受領者への個人データの移転は、その国又は機関が対象となるデータ移転について十分な保護レベルを保障する場合に限り、与えなければならない。
② 本議定書第2条第1項[注：上記①]を適用除外して、各当事国は、以下の場合に個人データの移転を許可することができる。
(a) 国内法で以下の理由により規定される場合
- データ主体の特別の利益
- 適法な社会的利益、特に重要な公的利益
(b) 特に契約の条項に基づく安全措置が、移転について責任を持ち、関連機関に国内法に基づき十分であると認められた管理者によって提供されている場合

上記のとおり、欧州 108 号条約及びその追加議定書においても、OECD ガイドライン同様、データ越境流通について、十分な保護の水準を確保している場合にこれを認めるという考え方が採用されているほか、データ主体自身の利益になる場合や、重要な公的利益に基づく場合にもデータ越境流通が許可され得ることが明確化されている。

なお、欧州評議会においては、現在欧州108号条約の現代化に向けた改正作業(Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)が進んでいる。改正後の条約(以下「欧州条約108号＋条約」という)においても、十分な保護の水準を確保している場合、データ主体の利益になる場

合又は重要な公的利益に基づいてデータ越境流通が許容され得るという基本的な考え方が踏襲されているものの、どのような場合に十分な保護の水準を確保しているといえるか(欧州条約 108 号＋条約 14 条 3 項)等、従来よりも詳細な規定によって明確化が図られている。

(3) APEC プライバシーフレームワーク

APEC は、1989 年に発足された、日本や米国、中国を含むアジア太平洋地域の 21 の国と地域(以下「APEC 加盟エコノミー」という)が参加する貿易・投資の自由化、ビジネスの円滑化等に関する経済協力の枠組みである。

APEC では、2004 年に APEC プライバシーフレームワーク(APEC Privacy Framework)が採択された。同フレームワークは、アジア太平洋地域における電子商取引の促進するために、APEC 加盟エコノミーにおけるプライバシー保護の枠組みの互換性を高めるために策定されたものであり、各 APEC 加盟エコノミーは、同フレームワークの実施を推奨している。その内容は、OECD プライバシーガイドラインを概ね踏襲したものであるが、OECD プライバシーガイドラインの 8 つの原則に加えて、「被害防止の原則」(Preventing Harm)(APEC プライバシーフレームワークパラグラフ 20)が定められていることが特徴的である。

データの越境流通に関して、APEC プライバシーフレームワークは、以下の内容を定めている(パラグラフ 69 及び 70)。

① 加盟エコノミーは、自らと他の加盟エコノミーの間における個人情報の越境流通につき、本フレームワーク並びにこれを実施する法及び政策に適合する継続的な保護の水準を保つため、(a)当該他のエコノミーが本フレームワークを実施する国内法又は政策を有している場合、又は(b)実効的な執行の仕組み及び個人情報管理者により導入される適切な措置(APEC 越境プライバシールール(以下「CBPR」という)等)を含む、十分な保護措置が存在する場合、当該越境流通を制限することを控えるべきである。

② 個人情報の越境流通に対するいかなる制限も、当該情報の機密性並びに域外移転の目的及び情況を考慮した、当該流通によって引き起こされるリスクに比例していなければならない。

このように、APEC プライバシーフレームワークにおけるデータの越境流通に関する定めは、OECD ガイドラインのものを概ね踏襲しているが、「個人情報管理者により導入される適切な措置」として、CBPR が例示されている点が特徴的である。

CBPR システムは、APEC が 2011 年に導入した個人情報の越境流通に関する枠組みであり、APEC 地域において活動する事業者による個人情報保護の取り組みが、APEC プライバシーフレームワークが定める 9 つの原則に適合するものであることを認証する制度であ

る。CBPR システムへの参加は各加盟エコノミーの自主的な判断に委ねられており、本報告書作成現在、日本及び米国を含む 9 の加盟エコノミーが CBPR システムに参加している。

(4) ASEAN PDP フレームワーク

ASEAN は、1967 年に設立された、①域内における経済成長、社会・文化的発展の促進、②域内における政治・経済的安定の確保、及び③域内諸問題に関する協力を目的とする国際機関であり、タイ、インドネシア、シンガポール、フィリピン、マレーシアのほか、東南アジア地域の全 10 ヵ国が加盟している。

APEC では、2016 年に、ASEAN 個人情報保護フレームワーク(Framework on Personal Data Protection。以下「ASEAN PDP フレームワーク」という)が採択された。同フレームワークも、OECD プライバシーガイドライン及び APEC プライバシーフレームワークにおける基本原則に由来した、個人情報保護に関する原則を定めた上で、加盟国に対して国内法において当該原則を実施することを推奨している。

そして、ASEAN が 2021 年に公表した ASEAN モデル条項(前記**第 2 の 3(3)エ**参照)において定められた義務は、ASEAN PDP フレームワーク及び国際的なベストプラクティスに由来している。ASEAN モデル条項は、ASEAN が 2018 年に承認したデジタルデータに関するフレームワーク(Framework on Digital Data Governence)の下における 4 つのイニシアチブの 1 つである ASEAN 越境データ流通(ASEAN Cross Border Data Flow。以下「ASEAN CBDF」という)メカニズムの下での取り組みである。ASEAN CBDF メカニズムの下では、ASEAN モデル条項のほか、データの域外移転に関する認証制度の導入が検討されている[84]。

[84] ASEAN, "Key Approaches for ASEAN Cross Border Data Flows Mechanism" available at <https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf>.

【図表2：各国における域外移転規制の概要(現行法)】

	EU	中国				シンガポール	タイ	インドネシア
		サイバーセキュリティ法		データセキュリティ法				
規制の対象となるデータ	個人データ	個人情報	重要データ	重要データ	国の安全等に関するデータ	個人データ	個人データ	個人データ
規制の対象となるデータの定義の概要	直接的又は間接的に識別された自然人又は識別可能な自然人に関する情報	重要情報インフラの運営者が中国国内での運営において収集し、生じた単独又はその他の情報と組み合わせて個人の身分を識別することができる各種情報	重要情報インフラの運営者が中国国内での運営において収集し、生じた国の安全、経済発展、並びに社会的及び公的利益に密接に関連するデータ(※1)	重要情報インフラの運営者以外のデータ処理者が中国国内での運営において収集し、生じた重要データ(※2)	国の安全と利益の維持、国際的義務の履行の維持に関連する管理品目に該当するデータ	真実であるか否かを問わず、当該情報から、又は当該情報とその組織等がアクセス可能なその他の情報とあわせて、個人が識別可能な情報	生存する個人に関する情報であり、直接的か間接的かを問わず、当該個人を特定することができるもの	保管及び管理された一定の個人情報であって、その秘密性が保護されなくてはならない情報
移転先において保護水準が十分であるとの当局の認証等に基づく移転	可能(十分性認定)	他の手続と組み合わせて可能(本人からの同意取得の上で当局による安全評価等(※3))		―		可能(CBPR認証、APEC認定)	可能だが、詳細の定めは未確定	―
所定の義務等を定めた契約に基づく移転	可能(SCC、ad hoc契約)	―		―		可能	―	―
拘束力のある社内規程等に基づく移転	可能(BCR)	―		―		可能	可能	―
本人の同意に基づく移転	可能	他の手続と組み合わせて可能(本人からの同意取得の上で当局による安全評価等(※3))		―		可能(みなし同意もあり)	可能	―
契約の履行等を確保するための移転	可能	―		―		(みなし同意が認められる一場面として)可能	可能	―
重大な公益・生命等の権利利益保護のための移転	可能	―		―		可能	可能	―
その他依拠することが可能な移転の根拠	・公的文書 ・行動規範 ・認証制度	―		―		・法令 ・公開された個人データの移転	・法令	・当局への報告等

※1 この「重要データ」の定義自体は未確定の下位法令において定められている。

※2 詳細はサイバーセキュリティ法上の「重要データ」と同一かどうかも含めて未定であり、今後「重要データ目録」が制定される予定である。

※3 詳細な手続は未定である。

【図表3：各国におけるローカライゼーション規制の概要（現行法）】

	中国		ベトナム		インドネシア
	サイバーセキュリティ法	データセキュリティ法	サイバーセキュリティ法	政令72号	
対象となる事業者	重要情報インフラ運営者	国内の組織又は個人	電気通信ネットワーク又はインターネット上のサービス等を提供する事業者	一般ウェブサイトを開設する事業者、SNS事業者、情報配信サービス事業者、オンラインゲームサービス事業者	公共部門における電子システム提供者
義務の内容	個人情報及び重要データの国内保存義務	外国の当局から国内に保存しているデータの提供を要求された際に、当局の認可を得る義務	個人情報に関するデータ、サービス利用者の関係に関するデータの一定期間の国内保存義務	当局の検査等に対応するためのサーバシステムを国内に設置する義務	・電子システム及び電子データを国内で保存する義務 ・開発したソフトウェアのソースコードの政府への提供義務

【図表4：各国において審議・検討中の法案等の概要】

	中国 （個人情報保護法案）	インド （2019年個人情報保護法案）	ベトナム （2021年個人情報保護に関する政令案）	インドネシア （2020年個人データ保護法案）
域外移転規制	個人情報の域外移転について安全評価＋同意の枠組みの他、専門機構による認証や契約＋同意の枠組みが追加される	センシティブ個人データの域外移転についてGDPR類似の枠組みによる規制が適用され、より限定された重要個人データは国外移転が原則禁止される	個人データの域外移転について個人情報保護委員会による事前承認等の複数の要件を満たす必要があり、GDPRの枠組みよりも当局の関与が強い規制が適用される	個人データの域外移転についてGDPR類似の枠組みによる規制が適用される
ローカライゼーション規制	重要情報インフラの運営者、又は当局による取扱量基準以上のデータを処理する個人情報処理者は、中国で収集及び生成された個人情報を原則として中国国内に保存するべきとされる	センシティブ個人データについて国内でのコピー保存が域外移転の要件の1つとされ、より限定された重要個人データは国外移転が原則禁止される	個人データについて国内でのコピー保存が域外移転の要件の1つとされる	－