JIPDEC 事務局レポート

個人情報の域外移転

～グローバル・ビジネスにおける域外移転対策の具体的アプローチ～

EU の GDPR（一般データ保護規則）施行が 2018 年 5 月に迫り、ビジネスをグローバルに展開する企業・組織にとって、個人情報の域外移転対策は急務となっています。また、アジア太平洋地域においても、APEC CBPR システムの運用が本格化するなど、データ流通に関する様々な規制・枠組みの導入は EU だけでなく世界的な潮流となっています。

このような中、あらゆる情報がデータとして流通するビジネスの現場では、各国の規制動向を把握し、自社の状況に合わせた対策を講じ、リスクマネジメントを行うことが急務となっています。

本レポートは、2018 年 3 月 13 日に JIPDEC が開催した個人情報の域外移転に関するセミナーの要旨をまとめたものです。個人情報の域外移転における最新動向について、第一線の研究者や弁護士の方から解説いただいた法制度面での特徴や、グローバル・ビジネスを展開するにあたっての具体的対応策（特に GDPR 関連）の概要をご紹介します。

個人情報の域外移転に関する政府の取り組み

■データ流通環境整備への取り組み

様々な機器や情報システムがネットワークにつながり、リアル空間のデータ収集が可能となっている IoT 社会においては、収集したデータを分析し、利活用することが、社会課題の解決や産業競争力強化につながると期待されている。

過去に起きた大きな社会変化は、技術革新がその萌芽となって産業の在り方が変化し、それが社会の変化へとつながっている。IoT、AI 等の新たな技術を今後の社会変化にまでつなげるためには、データ利用に関連した制度の整備が不可欠であり、政府としても産業データや個人情報等様々なデータの利活用に関する制度整備を進めている。

■APEC CBPR への期待

データフリーフロー（情報の自由な流通）については、日米欧ともに推進の立場を取っているが、その実現に向けた課題は各国及び各国間で異なる。個人に関するデータの取り扱いについては、EU は GDPR、日本では改正個人情報保護法において個人データの越境移転をルール化しており、EU-米国間はプライバシー・シールドで担保している。

現在、G7 や G20、OECD、APEC 等の多国間フォーラムでもデータフリーフローに関する議論が活発に行われており、日本もその中で各国との連携調整等を行っているところである。

このうち、APEC には全世界の GDP の 55%を占める 21 の国と地域が参加しており、世界的にも影響力が大きい。ここでルール化された域外移転の仕組みである CBPR（Cross Border Privacy Rules：越境プライバシールール）システムの普及が進むことで、世界的な情報流通環境が整うことが期待できる。すでに、米国では IBM、Apple、HP 等が CBPR の認証を受けており、日本でも 1 社が認証を受けている。

CBPR 認証については、改正個人情報保護法において個人情報の第三国移転の際の条件として位置づけられ、取得が推進されている。また、現在 APEC のデータ・プライバシー・サブグループ（DPS）と EU 間で、CBPR と GDPR の相互運用性に関する検討が行われており、今後の手続きの簡素化等が期待される。さらに、CBPR への参加を表明する APEC 加盟国も増加しており、APEC 全体での関心が高まっていることから、多くの可能性を持つ CBPR の認証取得が望まれる。

■各国との連携に向けた状況

情報技術の飛躍的発展によって、個人情報は簡単に国境を超えることができるようになったが、その取扱いは各国の政治や文化、経済状況により建付けが異なる各国の法律が適用される。我が国では、個人情報保護委員会が各国との対話を重ねながら協調関係の構築を進めている。

EU では、1995 年から越境移転の枠組みが導入され、域外移転は制約されていた。個人情報保護委員会では、事業者負担となるこれらの制約を解消し、円滑な移転を可能とするための枠組み構築に向け、EU との調整を行っている。また、EU からの離脱が決定した英国に関しても、EU 離脱後も円滑な個人データ移転が可能となるよう個別に対話を行う等、EU・英国に対しては、国の施策としてデータ利活用の円滑化に向けた取り組みを行っている。

一方、米国・アジア太平洋地域については、APEC CBPR システムの推進によってプライバシー保護の向上を図りつつ越境移転を促進させる、いわば個人情報保護を前面とした施策となっている。

すでに、日と EU は越境移転規制についてほぼ同等の制度が構築されているので、2018 年度第 1 四半期で十分性認定・国指定に関し最終合意する方向で調整が進んでいる。これが実現することで、SCC（Standard Contractual Clauses：標準契約条項）、BCR（Binding Corporate Rules：拘束的企業準則）等、これまで企業にとって負担となっていた対応が大幅に軽減されることが期待されている。

十分性認定の合意に向けた調整の中では、要配慮個人情報の範囲、開示請求権、利用目的の特定、日本から外国への個人データの再移転、匿名加工情報、についてはすり合わせが必要とされている。これらの 5 項目に関しては、今後ガイドライン等の整備により対応して

いく予定である。

また、現在では欧州委員会だけでなく、各国のデータ保護機関との連携に向けた対話が行われており、より円滑なデータ連携に向けた体制構築に向けた取り組みが行われている。

GDPR への具体的対応ポイント

■欧州における個人情報保護法制の特徴

GDPR は、個人自らが自身のデータをコントロールできる権利、個人情報保護に関する権利を人権として保護するための法律である。このため、罰則も厳しく、違反した場合はその企業の全世界の売上高 4 %以下の罰金となる。ここでいう企業の売上高にはグループ子会社のものも含まれるため、日本本社の下にある欧州子会社が GDPR に違反した場合、日本本社の下にある全世界の子会社の売り上げも含む総額に対して罰金が科される。

GDPR 施行の際の解釈に統一感を持たせるために、各国当局者の集まりである「第 29 条作業部会」が各種ガイドラインをまとめ、公開している。企業は、これらのガイドラインを参考に GDPR 対応を行うことになる。一方で、GDPR の適用により EU 加盟各国のデータ保護法は廃止されるが、GDPR に明記された一部事項（雇用、ジャーナリズム、研究等）に関しては EU 加盟各国が独自のデータ保護法により規制することが認められているため、自社がビジネス拠点を持つ各国のデータ保護法の動向にも目を配る必要がある。

なお、第 29 条作業部会は、GDPR 適用後に「欧州データ保護会議（European Data Protection Board：EDPB)」へと改組されることが決定しており、EDPB がガイドライン策定に加え、複数当局が関わる案件の調整役を務めることとなる。

1)対応のポイント

GDPR は、一言でいえば「個人データ」の「処理」と「移転」に関する法律である。対応にあたっては、個人データに対し、まずは自社でどのような処理・移転を行っているかを整理し、丁寧に分析していく必要がある。GDPR では、識別された/または識別可能な自然人に関するすべての情報が保護の対象であり、IP アドレスや cookie 識別子等も個人データとして位置づけられ、所持しているだけでも処理と見なされる。例えば、クラウド上でデータを管理している場合、クラウドに保管している＝処理していると見なされるため、GDPR 対応が必須となる。また、ドイツのサーバーに保管されたデータを日本から閲覧することも移転に当たる、という点にも注意が必要である。人権保護レベルが高い地域から、データを外に出すことはリスクととらえている。

もう一点、注意すべき点としては、十分性認定が有効なのは「移転」に対してのみであり、「処理」に関しては GDPR 対応が必須となる点である。

特別カテゴリの個人データ（人種、政治的見解、宗教や哲学的信念、労働組合への加入状況、遺伝子データ、生体データ、健康または性生活・性的嗜好等）は、例外を除き処理する

ことができない。例えば、食べ物に対するアレルギー等の調査も、人種や健康データに関わってくるため問題となる可能性があることに注意が必要である。

2）GDPR の適用範囲

GDPR の適用範囲は非常に広範にわたり、欧州経済領域（EEA）内の個人データを EEA 内の企業の活動のために処理する場合、実際の処理が行われている場所に関わらず、GDPR の適用対象となる。例えば、日本企業の英国子会社が英国人の応募者の個人データを収集し、日本企業に移転させるようなケースでは、理論上は十分性認定で解決可能となるが、実際にそのように判断されるか、については明確になっていない。さらに、EEA 内に拠点を持たない企業の場合でも、EC やプロファイリングを目的として EEA に所在する個人のデータを処理する場合は、GDPR の適用対象となる。

また、日本と EU では匿名化の定義が異なる。EU では完全に非個人データ（不可逆的であること）が求められる。匿名加工情報を取り扱う場合は、日本の個人情報保護法だけでなく、EU の基準である GDPR も満たしているかを確認する必要がある。

これらを踏まえ、実際にどの程度まで GDPR に対応するか、については、企業の業務内容等に基づいた経営判断となる。対応にあたっては、何をどのように（何を根拠として）遵守しているか、エビデンスをもとに説明責任を果たせるよう準備する必要がある。その際、根拠をどこに置くか（法的義務によるものなのか、本人同意によるものなのか、正当な利益のためなのか等）によって、その後の扱い方に違いが生じるため、事前に整理しておくことが重要である。

2018 年 5 月 25 日の施行まで時間が限られる中、正確な現状把握（データマッピング）、優先順位をつけた対応、社内規程・マニュアル等の整備、対応完了できない項目の洗い出しおよび対応完了に向けたロードマップ作成を行い、リスクを最小限に抑えることが急務となる。

グローバル・ビジネス展開で注視が必要な法制度動向

■注視が必要なアジア各国の動向

これまでの情報法は、主に米国、欧州の法律を参考に考えられていたが、最近はアジアの動向も注視する必要が出てきている。越境移転規制＝GDPR と捉えられているが、GDPR は対 EU であり、欧州以外の他国とのやりとりを解決するものではない。

訪日外国人観光者や EC の顧客の層を考えれば、日本のビジネスにおいてアジアとの連携は重要である。東アジアにおける越境個人情報移転規制を見ると、香港やマカオ、韓国、マレーシア等はすでに越境移転規制があり、その他の国々も対応を検討している状況である。

また、各国の規制検討状況は、最近は数か月単位で変わってきている。独自の十分性認定

のしくみを持つ国もあり、例えばマレーシアは 2017 年に十分性認定に関するホワイトリストの草案を公表している。また、最近法制化した国では、その内容は GDPR に準拠したものになっている。

今後、さらに各国が独自の規制を導入していくなかで、円滑なデータ流通環境を構築するためには、APEC CBPR の広がりが非常に重要となってくるであろう。

■データローカライゼーション規制

ここ数年、特に新興国において、ICT サービス提供に必要なサーバー設備等の現地設置を義務付ける動きが拡大している。2017 年に施行された中国のサイバーセキュリティ法では、極めて広範な分野を対象としたデータローカライゼーション規制が 2019 年 1 月より施行されることとなっているし、韓国では公的情報、地図情報等がデータローカライゼーション規制の対象である。また、インドネシアでは一般的な ICT サービスについて 1 台以上のサーバー設置を義務付けている。このような各国の状況は、ITIF（Information Technology & Innovation Foundation）がまとめ、公表を行っている。

データローカライゼーション規制の特徴は、規制するデータが個人情報に限っておらず本人の同意というルールが使えないという点である。現在、各国で導入されている越境移転規制は人権・個人情報保護が目的だが、データローカライゼーション規制は国益確保が目的である点に注意が必要である。

一方、EU 諸国でもデータローカライゼーション規制の導入は拡大しつつある。この動きはデジタルシングルマーケットの阻害要因となるため、EU 内の規則として「非個人データの EU 域内自由流通枠組規制」案が提案され、データローカライゼーション規制の抑止（公共の安全以外の規制は禁止）、データ移植促進が謳われている。

また、米国や EU 等 70 か国が、近隣諸国にも広がりつつある中国のデジタル保護主義への対抗として、有志国協定締結に向けた調整が始められたとの報道も出ている。

今後、データ流通に関する規制のあり方を検討する上では、各国規制の動向や運用状況を継続的に情報共有する体制作りが重要となろう。リアル空間全体がデータに依存する第四次産業革命の時代に、データローカライゼーションという概念にどう向き合うかを検討していく必要がある。

■EU、北米、東アジアのデータ域外移転関連法制の動向と対応ポイント

米国には、包括的な個人情報保護法はなく、州法で対応している。EU との域外移転に関しては、プライバシー・シールドの枠組みを持つ。

カナダは、個人情報保護及び電子文書法（Personal Information Protection and Electronic

Documents Act：PIPEDA)、デジタルプライバシー法等によりデータ保護が規定されており、プライバシーコミッショナーが調査を行っている。域外移転規制は特にないが、移転に際しては PIPEDA 上の「説明責任」原則に従い、第三者への移転後も責任を負うため、移転させた情報の保護水準を保つための契約等手段を取ることとなる。

オーストラリアも、プライバシー法によりカナダ同様説明責任が求められる。細かい法改正が多く、動向への注意が必要となる。

ニュージーランドは、OECD の原則に基づき、第三国への移転が制限される。

ロシアは、個人データに関する連邦法を持つ。越境移転は、データローカライゼーション法に従って、個人データに関する一定の操作についてロシアに所在するデータベースの利用が求められる。

中国のサイバーセキュリティ法は、すでに執行事例が示されている。37 条で規定されている影響評価を行うことにより、一部移転は認められているが、当局が拒否する場合もあり厳しいものとなっている。個人情報保護に関する違反取り締まりは強化されている。

シンガポールは、一般的なものとして個人情報保護法がある。個人情報の国外移転について、契約に基づいて移転先に義務を課すことが規定されている。

韓国では、個人情報保護法において域外移転に関し情報主体の同意を求めている。また、情報通信網法では、技術的・管理的対策がなされていること、個人情報の侵害に対する苦情処理に紛争解決に関する事項等の保護措置が求められている。海外事業者への法執行が積極的に行われているという評価もある。

インドは、2000 年に IT 法、2011 年に個人情報規則が制定されているが、具体的なデータ保護法はなく、直接的な域外移転に関する規制はない。

フィリピンについては、第一義的にはデータプライバシー法があり、21 条で個人情報の管理・保護に関して個人情報保護管理者が責任を持つと定められている。また、第三者による処理がなされている間は同程度の保護管理措置が取られるよう契約の締結、責任者の選任等が義務付けられている。

タイは個人情報保護法の制定が検討されている。電気通信事業法では、電気通信事業者による電気通信利用者の個人情報の移転ないし送信について、利用者の同意等を定めている。現在検討中の個人情報保護法案では、国際的移転に関する規制を盛り込んでいる。

ベトナムは個別法の中で定められている。国際的な移転に関しては特に着目すべき点はないが、他方、昨年から継続審議となっているサイバーセキュリティ法案はデータローカライゼーションが含まれており、中国のサイバーセキュリティ法との類似が指摘されている。

インドネシアはいくつか法令が存在するが、2016 年の電子システムにおける個人データの保護に関する通信情報大臣規則において域外移転に関する規定があるが、遵守すべき具体的規則が制定されていない状態である。

このように、域外移転規制といっても各国で定めている点が異なるため、個別の対応が必要である。