2019年4月18日
JIPDECセミナーレポート

十分性認定後の日本企業のGDPR対応
越境データ移転を中心に

ひかり総合法律事務所
弁護士　　板倉　陽一郎氏

序論：欧州一般データ保護規則（GDPR）の概要

GDPR とは何か

EU 法の種類には一次法と二次法、判例法がある。一次法は、日本で言う憲法レベルのもので、一次法に反した二次法は無効になる。二次法が普通の法律で、規則、指令、決定、勧告、意見がある。また、EU 司法裁判所の判例は、先例拘束性はないが相当程度参考とされる。GDPR は二次法であり、今回指令から規則に格上げとなった。

二次法の規則とは、各国の国内法に優先して適用されるもので、各国でそのまま法律として効果がある。一方、指令は EU 域内の条約のようなもので、実施に当たっては各国が個別に立法していくことになる。

GDPR の名前の一般とは、刑事データ保護指令に対するものである。つまり、GDPR は安全保障、捜査に関するデータを対象としていない。今回指令から規則に格上げされたことで、各国が GDPR をもとに対応することになるが、実施法は各国が定める部分が残っているため、実務に関しては各国法まで見る必要はある。

例えば、研究または統計目的の場合の、データ主体の権利の一部除外を認める 89 条 2 項への対応や、従業員データの処理に当たっての対応については、各国で定めることが可能となっているが、国ごとに対応はかなり異なる。さらに、データ保護法で定める必要はないため、例えば従業員データに関しては労働法を見なければならないという場合も多い。

GDPR の適用範囲

GDPR は、EU28 か国＋EEA3 か国の計 31 か国に適用される。なので、永世中立国であるスイスや、モナコ、アンドラ、サンマリノ等の小国も対象外である。

実体的範囲

日本の個人情報保護法では、個人情報データベース等に格納された個人情報である個人データを対象としているが、ヨーロッパでは全部または一部が自動的な手段による個人データの取扱いに適用される。また、ファイリングシステム（電子的なもの、非電子的なものを含め何らかの方法で検索することが可能（または可能になる予定）なデータベース）の一部または一部にすることが意図された個人データ（例えば、名刺アプリで管理する予定の名刺等）は、自動的な手段でなくても対象となる。

地理的範囲

GDPR 3 条では地理的範囲として、

- 直接適用：EU 域内に拠点・事業所がある管理者または処理者がその拠点に関連した個人データを取り扱う場合（拠点/事業所基準）
- 域外適用：EU 域内に拠点がない管理者または処理者が欧州市民に対する商品・サービスの提供（対価の要求有無を問わない）、行動監視（ターゲティング広告等）に関連して個人データの取り扱う場合（標的基準）

を定めている。現時点のガイドライン案によると、直接適用に関しては、単純に受託・委託するだけですべて適用されるとは解釈されないように見られる。

よく混同されているケースが見受けられるが、今あげた点はあくまでも適用に関する内容であり、越境移転の話とは異なる。域外適用と越境移転は全く別の問題で、域外適用は GDPR が適用されるかどうか、越境移転は GDPR のルールの一つである。

GDPR は原則、処理も移転も禁止しており、行うためには適法化事由が必要となる。同意はあくまでも適法化事由の一つに過ぎず、さらに撤回が認められているというリスクがある点、また、十分性認定はあくまでも越境移転を適法化するための事由の一つに過ぎないという点に留意が必要である。実務の中では、域外適用される場合で越境移転するというケースも想定されるが、その場合は GDPR にも日本の個人情報保護法にも対応することになる。

第 1 部：EU から日本への移転

EU からの十分性認定の意義、今後のレビューと見通し

越境データ問題には、データの移転そのものの制限に関する問題（通常個人データにかかってくる）と、データローカライゼーションの問題（個人データに限らず重要データを自国内サーバーに保存することを求めるもの　中国、ロシア、ベトナム等）があり、どちらに対応する必要があるかを理解する必要がある。十分性認定は、前者の問題に関するものとなる。

欧州では、国により程度は異なるが個人データ保護は人権そのものであるという考え方から、基本的人権を守れない国に対しての移転は原則禁止としている。一方、米国系の立場は、基本的にデータは自由に流通するもので、例外的に流通の制限が可能としている。ただし、GDPR の正式名称からも見てとれるように EU も自由なデータ流通の必要性は認識している。

日本は「外国にある『第三者』への提供」を制限しており、自分の一部（子会社、グループ会社）が外国にある場合は越境移転とみなされないが、欧州では相手がどういう関係であれ国境を越えれば規制の対象となる。GDPR では、44 条で EU からの移転を原則禁止としており、それを解除する事由として、45 条で十分性認定、46 条で十分性認定がない場合の適切な安全管理措置を施した移転、49 条でそれ以外の場合の特則が示されている。

十分性認定とは

GDPR を制定したのは EU（国）だが、実際の十分性認定は欧州委員会（行政機関）が行う。十分性判定された国/地域は、ほぼ欧州域内と認識されるような小国、EU のタックスヘイブンである国々、旧領主国が強力に支援した国で、正面から十分性認定されたのは、カナダ（民間部門）、イスラエル、ニュージーランド、日本（個人情報保護法が適用される範囲）のみとなる。米国は個別企業ごとの EU-US プライバシーシールドというスキームで処理している。

十分性の評価ポイントは 44 条 2 項(a)(b)(c)にあるが、この中にある国防、国家安全保障のため民間企業が国にデータを提出する際の手続きに関して規定されている。また、3 項では見直しが規定されており、初回は 2 年、その後 4 年ごととなっている。

十分性認定にあたっては、必ずしも欧州の条項のコピーである必要はなく、実質的に同等かどうかが重要となってくる。欧州連合基本権憲章 7 条では基本的人権としてのプライバシー保護、8 条では個人データそのものの保護が書かれているが、これは単なるプライバシーだけでなく個人データの処理で生じる差別等についても憲法レベルで保護されているかを判断するものと見られている。

2018 年 9 月 5 日に欧州委員会による日本の十分性認定の草案が公表されたが、十分性認定に意見を出す役割を持つ欧州データ保護会議（EDPB：各国データ保護機関の合議体）での議論に時間がかかり、12 月になって条件付き承認の意見が提出された。その後、2019 年 1 月 23 日に日欧相互に十分性認定がなされた。

ただし、十分性認定がなされたのは個人情報保護法の対象範囲内に限定されており、それ以外の公的分野（行政、独立行政法人、自治体）や個人情報保護法の適用除外部分（学術機関が学術目的で利用する場合など）は十分性認定の対象外である。この状況は、大学や行政と連携して事業を実施する際に支障となるため、経済界からは個人情報保護委員会の所掌範囲に公的分野を含めることを求める声が出ている。

EDPB が出した日本の十分性認定に対する意見では、個人情報保護法に関する評価、捜査等のための公的機関からのアクセスに関する評価、安全保障目的によるデータへのアクセスに関する評価がなされている。個人情報保護法に関する内容としては、

- 補完的ルール自体は評価できるが、GDPR と本質的に同等か欧州委員会によるチェックが必要
- 補完的ルールにより、EU から移転された個人データをさらに第三国に再移転するための法的根拠(個人情報保護法 24 条）に APEC CBPR は含まれない
- 法執行（刑事法）分野では EU との本質的同等性が認められない（現在は十分性認定の対象外）
- 2 年ごとのレビュー実施が必要（通常は初回 2 年後、その後 4 年ごとと規定）
- プライバシーが憲法レベルで権利として認められている点は確認、一方で個人データの取り扱いが未定義であること、管理者、処理者の概念がない（日本は委託元、委託先として整理）点に関しては懸念
- 同意の撤回が可能かどうかの不透明さ
- 課徴金がない等権限は不十分

といった意見が出されている。

日本に移転されたデータへの法執行機関からのアクセスに関しては、警察からの照会（捜査事項照会）

に対し比較的容易にデータが提供されてきた現状を EDPB も把握しており、各都道府県警まで個人情報保護委員会の監督が及ばない点に懸念が示されている。また、各自治体の条例では法執行機関へのデータ提供に対する救済メカニズムがないため、個人情報保護委員会が EU 市民に限定した苦情申し立て取次窓口を設置しているが、実効性が疑わしい点を指摘されている。

欧州議会からは、パーソナルデータの範囲（個人情報の定義）が狭い点、捜査事項照会による任意なデータ提供が許されている点、捜査機関に対する拘束力があるかという点について疑念が指摘されており、これらは今後の個人情報保護法見直しの際に影響を与える可能性がある。

十分性認定以外の方法（SDPC、BCR、GDPR49 条）による移転との関係

SDPC（標準データ保護約款）は、日本が管理者、欧州が処理者となる場合の標準約款がなく、文言を変更して使用されているケースもあるが、約款の文言を変えてしまうと SDPC としての効力はなくなってしまう。GDPR 施行前の指令下で作成された標準契約条項（SCC）は経過措置として使用可能であるが、SCC の規定上移転元国の法律が準拠法となることに留意する必要がある。

BCR（拘束的企業準則）はグループ企業全体をデータ保護機関に認定してもらうことによりグループ内のデータ移転を可能とするもので、日本では楽天がすでに認定済み、IIJ、富士通が申請中である。

個別の事由による移転は GDPR49 条で定められており、その中の 1 つが明示的同意に基づいた移転である。ただしこれは、限定的な人数に関する適法化事由であると条文に明示されており、反復的な移転への適用は非推奨でありリスクがある。

十分性に基づいて日本に移転されたデータに関する「補完的ルール」

十分性認定に際し EU からは懸念事項が示されたため、十分性認定により移転された EU のデータの取り扱いに関してのみ適用される「補完的ルール」が制定されている。

主な内容は以下のとおり。

・性生活、性的指向又は労働組合に関する情報を要配慮個人情報と同様に取り扱う。
・保有個人データの 6 カ月制限は適用されない（開示等，本人からの請求等の対象となる）。
・提供先は、提供元の利用目的以上の目的を設定できない。
・外国にある第三者への提供の制限（APEC CBPR による再移転はできない）
・再移転の基準はあくまでも個人情報保護法 24 条であり、再移転先が GDPR 上適格であったとしても即再移転可とはならない。
・仮 ID を残した匿名加工情報は認められない。
これは、英国が EU 離脱した場合、EU 並びに英国に適用されることとなる

移転手段を複数用意しておくことは適切だが、実際にどの法的根拠によって移転するかはプライバシーポリシー等に明記が必要な通知事項となるため、事前にスキームを決めておく必要がある。

第 2 部　日本から EU にある第三者への提供

日本の個人情報保護法は、24 条で越境データ移転規制の例外として同等な保護水準にある外国への移転を認めている。ただし、同一法人内の場合は 24 条ではなく 20 条の安全管理措置の問題となる。移転

を認められる国の条件は、規則新11条に定められているが具体的な国名は告示にさらに委任されている。また、GDPR 同様、同等水準と認められる国について条件を付すことができ、認定後のレビューを前提としている。十分性が認められた国名は告示される。

同等性認定以外の方法としては、規則 11 条の 2（日本国法の遵守、国際的な枠組み（APEC CBPR 等））で定められているので、実務では NDA、契約書の中で個人情報保護法 24 条および規則 11 条の 2 およびガイドライン（外国にある第三者への提供編）の遵守を盛り込むことで手当てができるであろう。

第 3 部　EU 以外からの移転の制限

日本と同様に十分性認定された国でも、各国法の規制は異なっている。例えば、スイスはまだ未改正だが、原則個人データの移転禁止となるとみられている（GDPR とほぼ同様）のに対し、ニュージーランドは原則禁止とはしておらず、場合によりコミッショナーが禁止できることになっている。このため、十分性認定された国間の移転にあたっても、各国法の確認が必要となる。

最後に

日本としては、日・米・欧 3 極間のデータ流通を進めたいという意向がある。現状 APEC CBPR での再移転はできない状況なので、個人情報保護委員会としては APEC CBPR に「何か」を加えた認証方法を構築し、GDPR 認証と同等レベルにできないかが模索されているようである。

「十分性認定後の日本企業の GDPR 対応」に関する Q&A

ひかり総合法律事務所
弁護士　板倉　陽一郎氏

最初に：移転とは、先方が管理者または処理者の場合であり、相手がデータ主体の場合は移転の問題は起きない。

Q：人材育成サービスを提供しているが、グローバル展開している日本企業の EU 子会社等の従業員満足度調査実施を受託し、当社で EU 従業員のメールアドレスリストの提供を受け、メールを一斉配信して各従業員に回答してもらう場合、適正に個人情報を取得するためには、委託元が EU 子会社との間で何をすれば問題ないか

A：EU 子会社の従業員データを送るために、日本企業が従業員に対しどのような説明がなされているか、処理の根拠は GDPR6 条のうちのどの項目としているかを確認しておくとよい（従業員の雇用管理そのものであれば、雇用契約（1 項(b)）を適法化根拠とすることも可能であろう。）

Q：以前の解釈では、EU 内の拠点の有無に関わらず、日本内でデータを処理すると GDPR 対象という認識だったが、EU 内に拠点がない企業でも、日本人が処理して OK な状況を教えてほしい。

A：ガイドライン案が出て解釈が変わった。条文を素直に読むと、直接適用は拠点の有無に関わらないと読めたが、ガイドライン案でそれぞれの拠点があるかどうかで判断するとなったため，現時点ではそのように解釈してよいであろう。

Q：同意の撤回については保護法でも検討されていると思うが、具体的にどのように対応していくのが良いか？

A：日本法では同意以外の処理方法が明確に定められていないため、同意の撤回が認められてしまうと実務では厳しい状況となる。これに関しては、同意の撤回を認めるのであれば契約に基づく利用を入れる等要請していく必要がある。GDPR では契約による利用を認めており（1 項(b)）、これは一方的には撤回できない。双方合意による契約解除が必要になる。

Q：日本本社が EU 支店在勤者（現地採用なし　顧客拠点での開発・設計業務であり、EU 一般市民の個人データの取扱いなし）の人事管理、給与計算を行っている場合、日本本社は GDPR 直接適用の対象とな

るか。

A：対象となるが、親会社というよりは子会社で行われている処理に対して適用される範囲に含まれるということになろう。

Q：GDPR では、管理者-処理者間の契約に「管理者の書面による指示、または EU 法、加盟国の国内法のみに基づいて処理を行う」ことを定める必要があるが、日本の処理者は日本の国内法に基づいた取り扱いも必要となるか？
令状に基づく情報提供など日本の国内法特有の取り扱いを行った場合、例えば管理者からの書面による指示として「日本法に基づく取扱い」を明記することで対応可能か？

A：日本法の例外処理が EU 法上の例外事由に当たる場合は EU 法で処理が可能と考えられる。それ以外の場合、データ主体から管理者からの指示として「日本法に基づく取扱い」を入れたとしても、事前にデータ主体に利用目的として通知し処理に同意を得なければ抵触することになってしまう。「抵触する場合がある」と割り切るのも一つの判断だろう。
外国法と抵触する場合に参考になるものとしては、SOX 法と内部通報制度の構築との関係についての 29 条作業部会意見書（Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP117, 1 February 2006）がある。

Q：Cookie 利用に関する通知・同意は一般的な記述のみでよいか？あるいは「Cookie A は〇〇に利用」「Cookie B は□□に利用」というレベルで記述する必要があるか？

A：欧州司法裁判所で Cookie を争点に行われている Planet49 に関する裁判について、先月出された法務官意見では、Cookie ポリシーを用意する等かなり詳細に通知することが求められている。また、CNIL は広告に関する通知が不十分として Google に 5000 万ユーロの制裁金を課しており、現在の流れはかなり丁寧に書くことを求められている。

Q：EU の管理者から匿名加工の委託を受けた日本の処理者が、管理者に加工データを戻す場合、処理者として守るべきルールはあるか？

A：管理者-処理者間の契約に必要な内容は GDPR28 条に規定されている。また特別カテゴリーデータを扱う場合は、9 条に基づき管理者が同意を取る必要があるので、心配な場合は管理者に確認すると良い。また、加工済みデータを日本から送る場合は個人データではないので、通常のデータとしての扱いで良い。

Q：日本に移転した EU の個人情報を元に、DM を送付する場合気を付ける点は？

A：十分性認定に基づいて移転したデータは、補完的ルールに基づいた取り扱いを行えばよい。ただし、日本法では第三者提供で取得したデータの利用目的は問われないが、補完的ルールにより EU から移転されたデータに関しては元の利用目的を超えて利用することはできないとなっている点に留意が必要となる。

Q：ネット通販で EU の消費者から取得した個人情報の取扱いの注意点は？

A：欧州内のデータ主体に物品を送付するにあたり直接データを取得する場合は GDPR の域外適用となるので（3 条 2 項(a)）、当該処理に関しては GDPR 全体を遵守する必要がある。

Q：EU の管理者からの委託により、日本でデータ処理しそのデータや結果を EU 側に返却する際にも日本⇒EU のデータ移転に関する手続きがいるか、またはしなくてもよい根拠などはあるか？

A：日本法 24 条は個人データを外国にある第三者に提供する場合のことであり、委託に伴う提供は提供にあたるが、委託元に戻す場合が提供にあたるかは不明確。ただし、同等性認定の元では、委託に伴う提供は同意がいらないという解釈になると思われる。

Q：同意の撤回がなされた場合、同意の下で AI の学習等に提供するサービスでは撤回以前の学習結果も使用できなくなる可能性はあるか？

A:あくまでも客体の個人データに関する同意の撤回なので、学習により個人データでなくなったものに対しては権利が及ばない。

Q：会員番号を仮 ID にして処理・分析を行う際に EU（GDPR 対象）の個人データが含まれる可能性がある場合、匿名加工情報の取扱いとして問題があるか？

A：日本では仮 ID をつけた匿名加工情報を認めているが、EU ではデータが集積されることにより追跡可能になる可能性のあるデータは、あくまでも個人データとしての扱いとなる。
仮 ID を削除する、または毎回仮 ID を変更するなどの処理を行ったものに関しては EU も匿名加工情報としての取扱いをとやかく言わないようである。

Q：EU 域内の個人が、日本法人（例えば旅行代理店）の Web サイトから旅行の申し込みをした場合、当該 Web サイトが EU 域内にある場合は（表記等も英文）GDPR は適用されないのでしょうか？

A：日本法人の拠点が EU 域内にあれば直接適用となり、日本法人の拠点が EU 域内になくサーバーのみが置かれている場合は、GDPR3 条 2 項(a) (b) に該当すれば域外適用となる。

Q：EU 内に拠点はあるが、直接営業行為を行っていない場合に、GDPR で留意すべき点はあるか？

A：拠点での活動に関連する個人データの取扱いがない場合は、GDPR 適用外となる。

Q：十分性認定に基づく移転の場合、第三国への再移転の根拠として「EU から見て適法な移転先かどうかは無関係」とあるが、従来方式（SCC や BCR による移転など）の場合は、これは当てはまらないという理解で良いか（例：プライバシーシールドの参加企業に対するデータ再移転）

A：SCC（SDPC）に基づく移転で来たデータは補完的ルールの対象とはならないが、保護法 24 条、規則 11 条の 2 が適用されるのであって、再移転先がプライバシーシールドに参加しているかどうかは関係がない。

Q：日本法 24 条により移転が可能ということは、EU 十分性認定がない国・地域への再移転も可能か？

A：日本が EU の十分性認定を持たない国を同等性認定すれば、24 条により移転可能となる。その際に、その国が GDPR に対応しているかどうかは関係がない。

Q：Cookie を用いたプロファイリングは可能か？

A：GDPR3 条 2 項(b)に該当するため、GDPR の域外適用となる。

Q：十分性認定、標準データ保護約款、BCR 等それぞれの根拠による越境移転のメリット・デメリットを教えてほしい。

A：十分性認定の最大のメリットは個別の事業者が何もせずとも移転ができるということ。ただし移転さ

れた後の上乗せルールが厳しい場合は十分性認定による移転は向かない。SCC のメリットは書けばよいこと、ただし移転元の法律に準拠するため法律が良く分からない国では難しい。また、処理ごとに締結しなければならない点が煩雑になる。BCR のメリットは、十分性のような上乗せルールがなく、グループ企業間でデータのやり取りができる点。デメリットは取得までの時間と費用。

Q：企業グループ内で EU、日本、それ以外の国（米国等）の拠点で例えば顧客データを相互に移転している場合の対応の実務的なヒントについて

A：データ移転を行う前にスキームを固めることが重要。最初にどういった処理になるかを整理し、それに対して同意を取得すればそれ以上の負荷はかからない。後からいろいろな根拠に基づき移転しようとすると労力がかかることになる。

以上