欧州一般データ保護規則（GDPR）全面適用の情報サービス産業への影響

弁護士・ひかり総合法律事務所
理化学研究所革新知能統合研究センター客員主幹研究員
国立情報学研究所客員教授
板倉 陽一郎

1　はじめに～ GDPR の狙いと思想

欧州一般データ保護規則（GDPR）[1] が 2018 年 5 月 25 日に全面適用された。本稿は，本誌の主たる読者である，情報サービス産業に属する日本の事業者に対して，その影響を解説しようとするものであるが，その前提として，GDPR の狙いと思想を理解しておく必要がある。GDPR の狙いの一つは 1995 年 EU データ保護指令[2] から 20 年間のインターネット，情報技術の進展に対して，本人（データ主体）の権利を強化するという点にあり，この点が強調されがちである。確かに，GDPR で新たに忘れられる権利，データポータビリティの権利など，データ主体の権利の強化が議論され，一部は導入されたことは重要であるが，他方で，欧州の「『単一デジタル市場（digital single market）』の実現のためにも，EU 加盟国間における異なる法制度を克服し，行政の負担軽減（年間約 23 億ユーロの負担軽減と推定）とともに消費者と企業に分かりやすいデータ保護の原則を示す重要性」[3] について理解しておく必要がある。GDPR の対象は後述するように欧州連合 28 カ国と EEA（欧州経済領域）に属するアイスランド，ノルウェー，リヒテンシュタインの 3 カ国であるが，国内法化を必要とする EU データ保護指令では，例えば，欧州域内で情報サービス産業等を展開しようとすれば，31 カ国の法制に対応しなければならなかった。これは，明らかに欧州域内での多国間展開や，欧州への投資へのディスインセンティブとなるのであって，改善が求められていたのである[4]。

このように，GDPR の狙いはデータ主体の権利強化のみならず，単一デジタル市場の実現のために，統一的なルールを策定する点にもある。しかしながら，GDPR が経済ルールであるとか取引のルールであると理解するのは早計であり，本質を見誤ることになる。GDPR の背景には，あくまで個人データ保護は人権（基本権）保護の問題であると考える欧州流の考え方があるのであって，個人データが交渉の対象であるとか材料であると考えるのは間違いである。すなわち，藤原靜雄教授が端的に整理するように，「EU ではプライバシー権（EU 基本権憲章 7 条，欧州人権条約 8 条）も個人情報保護（リスボン条約による EU の機能に関する条約 16 条，EU 基本権憲章 8 条，GDPR の前文（検討理由）(1)）も基本権としての位置づけを得て」おり，「個人情報保護は情報化社会においてプライバシー権を保護するものである

1　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）（個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則（EU）2016/679（一般データ保護規則））。訳文については，夏井高人「個人データの処理と関連する自然人の保護及び個人データの自由な移転並びに指令 95/46/EC の廃止に関する欧州議会及び理事会の 2016 年 4 月 27 日の規則（EU）2016/679（一般データ保護規則）」法と情報雑誌 1 巻 3 号（2016 年）1-186 頁を主として参照している。

2　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（個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令）。

3　宮下紘『欧州一般データ保護規則』（勁草書房，2018 年）9 頁。

が，プライバシー権の拡大というより，『個人情報の自動処理に関する個人の法的保護』という手法で，欧州評議会第108号条約，EU指令，EU基本権憲章に位置づけられている。」そして，「EUの個人情報保護法制の請求権は対公的機関（行政機関法），対事業者（個情法）のみならず対個人にも及ぶものである。」とされる。この基本的な思想は，欧州委員会と日本の個人情報委員会の間の十分性認定（GDPR45条，後述）を巡るやり取りにも現れている。欧州委員会は決して個人データ保護を経済連携協定（EPA）の問題とは考えない。日EU経済連携協定（EPA）の主たる要素についての欧州委員会の文書[5]の中でも，「データ保護はEUにおいて基本的権利であり，交渉の俎上には上がらない（Data protection is a fundamental right in the European Union and is therefore not up for negotiation.）」と明言されている。欧州委員会と個人情報保護委員会のやり取りは決して「交渉（negotiation）」とはされず，「対話（dialogue）」と表現されている。例えば，2018年5月31日に公表された個人情報保護委員会熊澤委員と欧州委員会ヨウロバー委員による共同声明についても，欧州委員会のウェブサイトにおいては，「ヴェラ・ヨウロバー委員と熊澤晴陽個人情報保護委員会委員によるデータ保護に関する対話の現状に関する共同声明（Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection on the state of play of the dialogue on data protection）」と表現されているし[6]，個人情報保護委員会も，その資料において，「欧州委員会との対話の実績」，「司法総局との累次の対話」という表現を用いており[7]，「交渉」という語を意識的に用いていないことが分かる。このような事実は，事業者又は事業者団体において，欧州委員会や関係機関にロビイングするときにも把握しておく必要があろう。もちろん，欧州のデータ保護に関する法令とて不磨の大典ではないし，欧州データ保護ボード（EDPB，旧・29条作業部会）はガイドラインの策定に際してパブリックコメントを実施している。自社にとって，又は，例えば事業者団体が情報サービス産業協会であれば，会員の情報サービス産業にとって不都合，あるいは非現実的なルールについては積

4　日本において，個人情報保護条例が地方公共団体ごとに策定され，その解釈権限も当該地方公共団体のみにあるという，いわゆる2000個問題も類似の問題であるといえる。2000個問題は国会でも取り上げられ，官民データ活用推進基本法（平成28年法律第103号）の審議において，「委員からも御指摘があったとおり、オープンデータについては、まだまだ取り組む地公体が少ないという状況でございまして、今、現状1788団体のうち233団体。あるいは、地公体ごとにシステムがばらばらということで、調達においても非常にデメリットもあるということで、互換性がない点についても御指摘がございました。そしてまた、さらに申し上げますと、個人情報保護条例というものが各地公体によって定められているわけでございますが、これがいわゆる2000個問題を引き起こしているわけでございます。こうしたところを鑑みますと、データの公開において非常に支障があるという状況でございます。」「本法案では、19条において、この2000個問題をしっかりと解決しなければいけないねということを、国あるいは地方公共団体が協力して進められるように条文を設けさせていただいているところでございます。…」との議論がなされている（第192回国会衆議院内閣委員会第7号（平成28年11月25日），濱村進議員発言）。それでも，政府においては2000個問題を抜本的に解決しようという動きは見られず，非識別加工情報についてすら，総務省『地方公共団体が保有するパーソナルデータの効果的な活用のための仕組みの在り方に関する検討会　報告書』（平成30年4月）は問題の先送り方針を明らかにしたため，規制改革推進会議『規制改革推進に関する第3次答申～来るべき新時代へ～』（平成30年6月4日）において，「例えば、ビッグデータの活用が進む中、匿名加工した個人情報について、国や民間企業には法律で同一ルールが定められたにもかかわらず、地方自治体が保有する個人情報は従来どおり条例で定めることとされている。その結果、多くの地方自治体で条例の検討が始まり、全国的利用が前提のビッグデータにおいて自治体ごとに異なるルールが整備される可能性が出てきている。所管府省では有識者会議を開催し、データ利活用のニーズがない中、検討すべき対応策を整理したと言うが、会議としては、ルール整備を怠っていると評価せざるを得ない。」（I.2.）との痛切な批判がなされる状況にある。欧州連合加盟国だけで日本の約11倍の総面積があり（外務省ウェブサイトより），主権国家が31存する中でもGDPRの成立にこぎ着けた欧州と比しても，まさに政府は「ルール整備を怠っている」との誹りを免れない状況である。

5　“Key elements of the EU-Japan Economic Partnership Agreement”, Strasbourg, 18 April 2018, http://europa.eu/rapid/press-release_MEMO-18-3326_en.htm

6　“Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection on the state of play of the dialogue on data protection”, Tokyo, 31 May 2018, http://europa.eu/rapid/press-release_STATEMENT-18-4021_en.htm

7　個人情報保護委員会『国際的な個人データの移転について』（2018年5月11日）（第14回新戦略推進専門調査会・第10回　官民データ活用推進基本計画実行委員会合同会議【資料2-2】）2頁。

極的に発言していくことが必要であるが，交渉材料としてデータ保護を捉えると，欧州の関係機関からは，思想を理解していないアウトサイダーとして，全く相手にされなくなることもあり得る。データ主体の基本権（データ保護の権利）の制限は原則として許されないのであって，どのような要件があれば許されるのかという判断方法に頭を切り替えなければならない[8]。

2 GDPRの本当の基本

GDPRについては様々な記事が現れているが，基本を理解することが重要である。その基本の一つが，前項で解説した，データ保護が基本権であるという思想であるが，もう一つ，その思想の反映でもある実体的内容として，個人データの処理と越境移転が原則禁止であるということが重要である。すなわち，GDPRにおいては，個人データの処理も越境移転も，原則違法（GDPR6条，44条）であって，例外的に，法的根拠があるときのみ許される。この発想は，少なくとも米国には存在せず[9]，日本の個人情報保護法制でも部分的にしか採用されていない。例えば，個人情報の保護に関する法律（平成15年法律第57号，以下，「個人情報保護法」という。）17条1項は，個人情報の取得について，「個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。」と定めている。つまり，「偽りその他不正な手段」による場合だけを許さないとしており，これは明らかに，処理が原則適法であるという設計の仕方である。他方，越境移転の原則違法については，概ね，個人情報保護法24条にGDPRと同様の規定がある（但し，24条の対象は「外国にある第三者」への提供であって，個人情報保護法は同一法人間における越境移転を安全管理措置だけの問題としているので，あくまで「概ね」である）。

この，個人データの処理も越境移転も原則違法である，という基本を踏まえた上で，次項以降の解説をお読み頂く必要がある。

3 適用関係（特に，直接適用と域外適用）

情報サービス産業に属する事業者がGDPR対策を始めようというときには，まずは，GDPRが自社における個人データの処理に適用されるのかを検討する必要がある。その際に問題となるのが，実体的適用範囲（2条1項）と地理的適用範囲（3条1項，2項）である。順に見ていこう。

（1） 実体的適用範囲

GDPRにおける「個人データ」の定義は相当に広く（GDPR4条（1）），識別され，又は識別可能な自然人であるところのデータ主体に関する全ての情報が含まれる。識別可能な自然人であるかどうかは，何らかの識別子や，同一性を示す要素によって直接的又は間接的に識別され得るかどうかで判断される。しかしながら，実体的な適用範囲（GDPR2条1項）は無制限ではなく，「全部又は一部が自動的な手段による個人データの処理」又は，自動的でない場合，ファイリングシステムの一部を構成するか，それが予定されている場合にのみ適用される。「自動的な手段」と「ファイリングシステム」という概念である程度制限されているということである。このような制限によって，通常の会話の中で個人データが出てくるといったようなものにまでは適用されない。他方で，まだファイリングシステム（検索可能なデータベースシステム）にまだ入力していない名刺は

8 個人情報保護委員会が意見交換を行った米国系のプライバシーの専門家からも，「我々（米国系）の立場は、データの自由な流通が原則、個人情報の保護が例外であり、例外も自由な裁量に基づくのではなく、国際的な水準に従ったものであるべきというものである。ゆえに我々は、政府間の対話への参画を志向している。」との発言がある（第67回個人情報保護委員会（平成30年6月29日）【資料1-1】「国際的なプライバシー専門家等との意見交換の結果について」）。欧州と米国では原則例外がそもそも逆転していると理解できるであろう。

9 前掲注8参照。

どうか，という問題があるが，これはファイリングシステムの一部を構成することが予定されているということになり，適用対象である。GDPR に関する解説や報道は後述の地理的適用範囲（特に域外適用）に着目したものが多いが，実体的適用範囲の問題が先行することは理解しておかなければならない。

（2） 地理的適用範囲

ア　直接適用

地理的適用範囲の問題のうち，最もセンセーショナルに紹介されているのが GDPR3 条 2 項（a）（b）の域外適用の問題である。確かに域外適用は，欧州外で事業を行っているにもかかわらず GDPR を遵守しなければならないという点で強烈な条項であるが，こと，BtoB ビジネスを主とする情報サービス産業協会所属の会員企業においては，直接適用（GDPR3 条 1 項）の問題を把握しておく必要性が高い。

GDPR3 条 1 項によると，「欧州連合内にある管理者又は処理者の事業所の行為の遂行過程における個人データの処理に適用される」ため、支社・支店が欧州連合内にある場合には、当該支社・支店における個人データの処理について当然に適用される。問題は，欧州連合内に支社・支店が存在しないとき，適用があるのかということである。ここで，3 条 1 項は「その処理が欧州連合内で行われるものであるか否かを問わず」としている。つまり，支社・支店が存在しなくとも，欧州連合内の管理者の委託を受けて外国（日本）で処理者として処理を行う場合と，その逆，つまり，外国（日本国内）の管理者として，欧州連合内に処理を委託したため，欧州連合内に処理者がいる場合には，当該個人データの処理に関しては，GDPR が適用される。これが実際に生じたのが，2018 年 6 月に発生した仏・Fastbooking 社からの情報漏えいである[10]。同社のプレスリリースによれば「外部者による不正アクセス」により個人データが流出したものであるが，同社はホテルの自社サイトの予約システムの受託を主たる事業としていたため，流出した個人データは，管理者たるホテルのものであった。このホテルに，日本のホテルが多く含まれていたのである。外国（日本）に個人データの管理者（ホテル事業者）がいて，欧州連合内（フランス）の処理者（Fastbooking）に処理が委託されていたというパターンである。この場合，データ保護機関への通知義務を追うのは管理者であるので（GDPR33 条 1 項），日本のホテルには，フランスのデータ保護機関（CNIL）への通知義務が生じることとなった。情報サービス産業協会所属の会員企業は，どちらかといえば管理者よりは処理者の立場に立つことが多いであろうが，再委託先（復処理者）が欧州連合内であるような場合には，GDPR が適用され，個人データの侵害に関して管理者への通知義務（GDPR33 条 2 項）が適用されることもあり得る。個人データが，その流れの中で一部でも，欧州連合内の処理者によって処理されるような場合には，要注意である。

イ　域外適用

GDPR3 条 2 項（a）（b）は域外適用について定める。域外適用は大いに誤解されており，単に欧州国籍のデータ主体の個人データが，日本国内で完結している処理でたまたま入っている場合であるとか，ウェブサイトを訪れる人の中に欧州国籍の人がいるとか，それだけで GDPR の適用があるというものではない。適用される場面は二つであり，1 つは（a）「データ主体の支払いが要求されるか否かを問わず，そのような欧州連合内のデータ主体に対する物品または役務の提供」であり、もう 1 つは（b）「データ主体の行動が欧州連合内で起きるものである限り，その行動の監視」である。

情報サービス産業協会所属の会員企業が主として気になるであろう（a）について見ていくと[11]，欧州在住のデータ主体に対して物品またはサービスを提供する場合は、直接この管理者または処理

10 「ファストブッキングサーバーへの不正アクセスによる 個人情報および暗号化されたクレジットカード情報の流出について」（2018 年 6 月 26 日），http://www.fastbooking.com/ja/newsfeeds/press-release-june-2018/

者に対してGDPRが適用される。物品の提供はシンプルである。欧州のデータ主体に対する通信販売がなされるのであれば，そのデータ主体についてはGDPRを遵守しなければならない。問題は役務（サービス）の提供であり，その解釈は前文（リサイタル）(23）をみることになる。ここでは，「管理者または処理者が欧州連合内のデータ主体に対して物品または役務を提供しているか否かを判断するために、欧州連合内の１または複数の構成国内のデータ主体に対して役務を提供しようとする意思が明確かどうかを確認しなければならない」，とされている。したがって、「役務を提供する意思」が問題となる。例えば、英国を例に挙げれば、その国で一般的に用いられている言語、英語でサービスを提供していて、かつデータ主体との金銭のやりとりがポンドだといった場合には適用される方向となる。もう一つは、欧州在住者向けサービスであると明示してサービスを提供するような場合には、欧州向けにサービスをやっているということで，適用される方向となる。単に英語のサイトが存在しているだけで，GDPRが域外適用されるものではないし，まして，たまたま日本に住んでいる欧州国籍のデータ主体の個人データを保有したからといって適用されるものでもない。域外適用されるということになると，当該個人データに関してはGDPRの条項全てが適用される他，欧州連合内における代理人の設置義務も生じる（GDPR27条１項）ため[12]，冷静な判断が求められる。

4　データ主体の権利への対応

前述の通り，GDPRは1995年からの情報技術，インターネットの発達に対応すべく，データ主体の権利を強化している。その内容は興味深いものであるが，削除権（忘れられる権利）(17条)，データポータビリティの権利（20条），プロファイリングを含む自動化された意思決定に従わない権利（22条）などへの対応はGDPR対応の中でも応用に位置するものであり，まずは６条に基づいた適法な処理がなされているかという点が最も重要である。また，適法な処理の中でも，同意についての考え方は，日本の個人情報保護法と大きく異なるため，まずはこれらを理解しておくことが必要である。ここで，６条のほか，５条も，個人データの処理に関する基本原則を定めており，理解しておくことが重要であるが（その違反についての課徴金は具体的な権利義務規定違反と同様に定められている），行為規範として遵守するには抽象的な内容であり，結局は独立して遵守するというよりは，権利義務規定を遵守することになるのではないかと考えられる。

繰り返しになるが，GDPRにおいて個人データの処理は原則違法であり，６条１項（a）ないし(f）のいずれかに当てはまらない限り処理できない。(a）が最も基本的な適法化事由であり，「処理についてデータ主体が同意を与えた場合」，つまり，データ主体の同意が挙げられている。しかしながら，同意が原則というわけではなく，(a）ないし（f）は並列であるし，それぞれの適法化事由において，当該事由が失われる要件も異なってくるので，複数の適法化事由を備えられないか，ということを考えてスキームを構築するのが重要である。GDPRにおける同意は撤回できる(7条３項，但し将来効）というデメリットもある。もっとも，(c）の法的義務は欧州法における義務と考えられるため，日本国内で直接適用または域外適用されるためにGDPRの遵守義務が生じている場合にはほぼ無関係であり，(d）(e）については極めて例外的な場面であるため，現実的には（a）(b）(f）を検討することが多くなる。(b）は「データ主体が契約当事者となっている契約の履行のために必要となる場合，または，契約締結の前に，データ主体の申込に応ずる手立て

11　自社サイトの解析ツールを設置しているような場合には（b）も適用され得る。前文（24）は前文（23）のような意思的要素を挙げておらず，サイト訪問者にCookieを発行して再訪問を「追跡」できるような場合にはGDPRが適用され得る。これを防ぐためには，欧州からの訪問者についてはCookieを発行しないなどの手段を講じる必要があると思われる。

12　GDPR3条１項によって直接適用される場合には代理人の設置義務は生じないことに注意すべきである。

を講ずるために処理が必要となる場合」である。例えば，銀行からの送金は，必然的に個人データの移転を伴うが，個別の同意があるかというと微妙なところである。しかし，これは銀行の約款（契約）で合意された義務の履行に必然的に伴うものであるから，(a) ではなく (b) で適法化される。(f) は「公正な利益（legitimate interest)」による場合である。比較的単純なダイレクトマーケティングや，公益通報などがこれに該当するとして扱われているが，その判断は容易ではない[13]。他の適法化事由がないのに事業者において「公正な利益」であると判断して個人データの処理スキームを構築するのは危険であろう。EDPBの意見書等を参照することが求められる。

GDPR はその条項の違反について広範囲に，上限額の極めて高い課徴金を課すことができる条項を有していることは広く報道されているとおりであるが，適法化根拠を欠いた処理は「分かりやすい」違反であり，その額も 2000 万ユーロ以下又は前会計年度の世界全体の売上総額の 4％以下のいずれか高額な方ということになる（GDPR83 条 5 項 (a)）。十分な注意が必要であろう[14]。

具体的な権利規定への対応については，紙幅の関係で簡単にしか述べられないが，GDPR13 条ないし 14 条は，日本の個人情報保護法でいう利用目的の通知または公表に対応するものである。もっとも，そこで求められる情報の量は極めて多く，例えば，6 条 1 項 (a) ないし (f) のどれを処理の根拠としているのか（13 条 1 項 (c)）なども情報提供しなければならない。もう一つ，日本法との大きな違いは，データ主体への情報提供が求められるのであって，公表では足りないということである。実務的には，日本法での利用目的の記載同様，プライバシーポリシーにおいて情報提供することになるが，単にウェブサイトに公表しておくだけでは足りず，情報提供としての実質が確保されなければならない。冒頭にもいくつか挙げた具体的な権利規定（GDPR15 条から 22 条）のポイントは，適法化根拠に対応して定められているということである。例えば，削除権（忘れられる権利）は，同意が撤回され，他の適法化根拠が無い場合を，権利行使の要件の一つとしている（GDPR17 条 1 項 (b)）。また，異議申立権（GDPR21 条）は，ダイレクトマーケティングの場合を除いては，6 条 1 項 (e) または (f) を処理の適法化根拠としている場合に行使される権利である。このように，どの権利規定に対応しなければならないかは，どの適法化根拠を用いたスキームであるのかと連動しているのであって，対応フローもそのように作成することとなる。

5　管理者等の義務

管理者等の義務のうち重要なのは，代理人設置義務（GDPR27 条），処理活動の記録義務（30 条），データ侵害通知義務（33 条），データ保護責任者（DPO）設置義務（37 条以下）であり，ここではこれらを概説する。

ア　代理人設置義務（GDPR27 条）

域外適用の項目でも既に述べたが，GDPR3 条 2 項 (a) (b) に該当し，GDPR が域外適用される場合，管理者または取扱者は欧州連合内の代理人を書面で明示しなければならない。処理者にも適用されるため，情報サービス産業協会所属の会員企業においても留意が必要である。この点は，石井夏生利博士も，「受託者を含めて EU のデータ全体に向けて商品やサービスを提供したり、行動追跡を行う場合は代理人を設置しなければならず，それを遵守しない場合は制裁の対象となる」と強調するとおりである[15]。代理人の不設置に対する課徴金は 1000 万ユーロ以下又は前会計年度の世界全体の売上総額の 2 ％以下のいずれか高額な方（GDPR83 条 4 項 (a)）であり，「分かりや

13　判断構造については前掲注 3・宮下 54–56 頁を参照されたい。
14　但し，条文上も，課徴金は「比例的」に課せられる（GDPR83 条 1 項）。その額はデータ保護機関の全くの裁量ではなく，行政法学上の比例原則に服するということであるし，GDPR83 条 2 項は，考慮要素を列挙している。上限額である 2000 万ユーロや総売上の 4％といった数字が独り歩きしている感は否めない。
15　石井夏生利『新版個人情報保護法の現在と未来　世界的潮流と日本の将来像』（勁草書房，2017 年）59 頁。

すい」違反であるので，避ける必要がある。域外適用されると判断されたのであれば，必ず代理人を確保しなければならないことに留意されたい。自然人，法人の別は問われない。また，GDPR3条1項の直接適用の場合には代理人設置義務は存在しない。

イ　処理活動の記録（GDPR30条）

日本の個人情報保護法は，改正に伴って，個人データの提供に関する確認記録義務を導入した（25条，26条）。これにより，個人情報取扱事業者は個人データの第三者提供に関する棚卸しを迫られたわけだが，GDPR30条は，管理者及び処理者に対し，「処理活動の記録」を要求する。要するに，管理者及び処理者は，個人データの処理を全て把握していなければならないということである。具体的には，各部署に，個人データの処理の洗い出しを要請し，担当部署においてこれを整理するという作業が必要になる（データマッピング）。その項目は極めて広範であり（GDPR30条1項（a）ないし（g），2項（a）ないし（d）），書面によることが求められる（電子的な方式，つまりログによることも可能）。そのため，GDPR対応はこのデータマッピングから始めることがセオリーである。

他方，処理活動記録義務には従業員250人未満の企業または組織には適用されないという、GDPRでは唯一の，従業員数を閾値とする適用除外条項が存在する（GDPR30条4項）。但し，特別類型のデータ等（GDPR9条，10条）を処理している場合には更に例外で，適用されることとなるので，注意が必要である。

ウ　個人データ侵害の監督機関への通知義務（GDPR33条）

GDPR33条は，個人データの侵害（漏えい等。GDPR4条（12））についての通知義務を定める。具体的には，個人データの侵害が発生した場合に，管理者に対して，不適切な遅滞なく，実施可能である場合には，侵害に気づいてから遅くとも72時間以内に，データ保護機関に対して通知しなければならないとし（1項），処理者に対しては，侵害に気づいた後，不適切な遅滞なく管理者に通知しなければならないとする（2項）。日本の個人情報保護法には通知義務は存在せず，「個人データの漏えい等の事案が発生した場合等の対応について（平成29年個人情報保護委員会告示第1号）」において個人情報保護委員会等への任意の報告を求めているのみであるが[16]，GDPR上の通知義務は違反であるとされれば課徴金の対象である（GDPR83条4項（a））。データ侵害に関する通知義務については欧州より米国が先行していた。具体的には，州法において義務付けられていた。欧州は，米国での侵害通知義務を更に厳しくした上でGDPRに導入しようとしたが，漏えい等の事案の直後に詳細な通知義務を課すというのは非現実的であり，最終的な条項は「実施可能である場合には72時間以内」というところに落ち着いた。通知義務が発生すると72時間以内に通知しなければということで焦る気持ちはよく分かるが，条文上，72時間はあくまで目安にしかなっておらず，これを1秒でも超えれば違法だとか，課徴金が課せられるとか，そのようなものではない。限られた時間の中でも，実のある通知を心がける方が重要であろう。

実務的な問題として，処理者が欧州域内におり，管理者が日本であった場合に，GDPR3条1項により直接適用されるという場面で，処理者が個人データの侵害を引き起こしたとき，日本所在の管理者は「どの国の」データ保護機関に通知しなければならないのか，という論点が存在する。通知すべきデータ保護機関はGDPR55条により決せられるとされ，29条作業部会も「管理者又は処理者の主監督機関を特定するためのガイドライン（Guidelines on The Lead Supervisory Authority, wp244rev.01_en）」を公表しているが，この点に

16　行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）29条の4は「個人番号利用事務等実施者は、個人情報保護委員会規則で定めるところにより、特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態が生じたときは、委員会に報告するものとする。」とし，特定個人情報の漏えい等が「重大な事態」に該当する場合に限って個人情報保護委員会への報告を法的義務としている。

ついての手がかりはない。処理者の所在国のデータ保護機関に通知しておくというのは，一つの方法であろう。また，GDPR3 条 2 項（a）（b）により域外適用される場合にも，通知先のデータ保護機関は上記ガイドラインから直ちには判明しない。代理人設置義務を遵守している場合には，代理人の所在国のデータ保護機関に通知することが現実的であろうが，これらの点について個人データの侵害後に十分に検討する余裕はないと思われるため，インシデント発生前から事業者において検討しておくことが必要であろう。

エ　データ保護責任者（DPO）（GDPR37 条以下）

GDPR37 条は，データ保護責任者（DPO）の指定義務を定める。GDPR 上は，データ保護責任者（DPO）の指定は例外的な義務であり，管理者又は処理者の中心的な業務がデータ主体の日常的かつ機械的な監視を大規模に行うことを求める処理業務である場合（GDPR37 条 1 項（b）），管理者又は処理者の中心的な業務が，特別類型データ等（GDPR9 条，10 条）の大規模な処理で構成されている場合（GDPR37 条 1 項（c））に要求される（（a）は欧州の行政機関の処理）。情報サービス産業協会所属の会員企業においてこれらの処理を「中心的な業務」としていることは稀であろう。

他方，加盟国法で要求されている場合にも DPO の設置義務が生ずる（GDPR37 条 4 項）。典型的なケースはドイツであり，改正後の連邦データ保護法では 10 名以上の従業員を雇用する企業は DPO を選任する義務がある。また，GDPR を受けて改正された英国のデータ保護法も，DPO 設置義務を定めているようである。欧州に支社や支店を置く場合には，加盟国法で DPO 設置義務が定められていないか，必ず確認する必要がある。域外適用の場合に加盟国法が域外適用されるかというのは難問である。基本的には当該加盟国法において，GDPR における域外適用条項とは別に，域外適用条項を有していない限りは，DPO 設置義務が域外適用されることはないのではないかと思われるが，定説はない。DPO の地位は相当程度独立しており，「個人データの保護と関連する全ての事項について」「適切かつ適時に関与できることを確実にしなければならない」とされる。他方で，利活用側の担当者は DPO になることができない。取締役が兼職することは当然に出来ないが，例えば，マーケティング，人事，IT，法務などの担当者も兼職させることが出来ないので注意が必要である。実務的には，内部統制部局や，監査役から DPO を選ぼうとすることが多いようである。

6　越境移転（GDPR44 条以下）

GDPR44 条以下は越境移転を定めるが，越境移転も，処理同様，原則違法であるということを理解しておく必要がある。移転を可能にする根拠は大まかに分けて 3 つである。①欧州委員会による，適切な保護措置を備えた国又は地域に対する十分性認定，②適切な安全性確保措置，③特別の状態における特則である。そして，越境移転の方法によっては，直接適用や域外適用とは別に，移転先の事業者における GDPR への対応が必要となる場合がある。

（1）　十分性認定

十分性認定の制度や，既に十分性認定を受けた国又は地域等については多くの紹介があるので[17]，ここでは，日本の十分性認定についての対話の進展状況と，十分性認定がなされた場合，事業者にどのような影響があるかについて説明する。日本の個人情報保護委員会と欧州委員会（司法総局）は，欧州委員会から日本への十分性認定及び個人情報保護委員会から欧州（EEA を含む 31 カ国）への同等性認定（個人情報保護法 24 条，

17　前掲宮下・221-232 頁，前掲石井・156-163，166-172 頁，板倉陽一郎「越境データ移転－事業者が選択可能な方法と実務対応」ビジネス法務 17 巻 8 号（2017 年）36-40 頁。

個人情報保護法施行規則 11 条）を巡り，2016 年 4 月から 2018 年 5 月の間に，53 回（うち、ビデオ会議 37 回）もの対話を重ねており，2018 年 5 月 31 日の熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメントが到達点である。ここでは，「両者は、可能な限り早期に、お互いの手続を完了させるためのコミットメントを共有し、作業を加速することに同意した。具体的には、個人情報保護委員会が、個人情報保護法第 24 条に基づき我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として EEA を指定するとともに、欧州委員会が、GDPR 第 45 条に基づき我が国が十分な保護水準を確保していると決定することである。」とされている。日本側の，十分性認定のための準備は着々と進んでおり，EU から十分性認定に基づいて移転した個人データのみに適用され，①要配慮個人情報の範囲，②開示請求権等，③利用目的の承継，④日本から外国への個人データの再移転，⑤匿名加工情報といった 5 項目について上乗せ措置を定めた『個人情報の保護に関する法律についてのガイドライン（EU 域内から十分性認定により移転を受けた個人データの取扱い編）（案）』が2018年5月25日までパブリックコメントに付された他，2018 年 6 月 12 日には「個人情報の保護に関する基本方針」が一部変更（閣議決定）され，「個人情報保護委員会は、個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している国との間で、相互に円滑な個人データの移転を図るために、国際的に整合のとれた個人情報に係る制度を促進する方法としての枠組みを構築するための措置を講ずることとする。個人情報保護委員会は、個人情報保護法を所管する機関として、外国から移転される個人情報の適正な取扱いを確保する観点から、法第 6 条に基づき、日本と当該外国との間の制度及び運用の差異を埋めるために必要な措置を講ずる権限を有している。個人情報保護委員会は、必要に応じ、法及び政令で規定された規律（例えば、要配慮個人情報や保有個人データの定義に係る規律等）を補完し上回る、拘束力のある規律、すなわち、国内の個人情報取扱事業者に対して執行可能な、より厳格な規律を設けることを含め、一層の個人情報の保護を行う権限を有している。また、個人情報保護委員会は、当該外国当局との執行協力及び法制度の理解に関する対話を行うこととする。」(2（2）②個人データの円滑な国際的流通の確保のための取組）等の内容が加えられた。

目標とされていた 2018 年第 1 四半期は経過しており，現時点で具体的な十分性認定の時期は不明であるが，欧州委員会から日本への十分性認定の手続は着実に進んでいるといえる。但し，注意しなくてはならないのは，十分性認定はあくまで越境移転の根拠に過ぎないということである。処理根拠（GDPR6 条 1 項）は別途備えている必要があるし，まして，域外適用されるかどうかとは全く関係がない。これらを混同してはならない。また，移転根拠についても，処理根拠同様，複数備えておくということも十分考慮に入れられるべきであって，十分性認定以外の移転根拠について知らなくてよいという訳にはいかない。

（2） 適切な安全性確保措置

適切な安全性確保措置のうち，現実的に利用されているものの一つは標準データ保護約款であり（GDPR46 条 2 項（c)），もう一つは BCR（拘束的企業準則）である（GDPR46 条 2 項（b)，47 条)。46 条にはそれ以外の移転根拠も定められているが，現実的にはこれら二つが選択肢になる。

BCR（拘束的企業準則）は、グループ全体のデータ保護に関するデータ保護機関の承認を得るという方法である。実務的には，提出先データ保護機関を含めた 3 つの機関が審査するようである。日本の企業では，楽天が既にルクセンブルクに申請し，承認を得ている他，IIJ（英国)，富士通（オランダ）が申請したと報道されている。BCR の承認が得られると，グループ企業間での移転根拠が備わることになり，グループ間での個人データのやり取りは容易になるが，多量な書面を提出してデータ保護機関とやり取りすることに

なるため，費用も時間も掛かることになる。

他方，データ保護約款，現在はEUデータ保護指令下のSCC（Standard Contractual Causes：標準契約約款）のみが認められているが（経過措置，GDPR46条5項），欧州委員会により認められた移転契約の雛形に従っている限り，移転根拠になりうるというものである。基本的には署名すれば良いだけである。管理者→管理者間のSCCが二種類（SET I，SET II），管理者→処理者間のSCCが一種類公表されている。SCCは簡便なやり方ではあるが，処理者→管理者間ではSCCが存在しないので用いることが出来ないし，同一法人間の移転で用いるというのは，契約というものの性質上無理がある。もっとも，後者については，データ保護機関において認める運用を採用している国も見られるようである。更に注意しなければならないのは，三種類のSCCは全て，準拠法が移転元国法となっているということである。すなわち，SCCを移転根拠とするのは簡便であるが，例えばリヒテンシュタインを移転元国として移転すると，日本においてほとんど情報の得られないリヒテンシュタイン法を準拠法として，SCCを守らなければならないということになる。本当にそれができるのか。さらに，管理者→処理者間のSCCを用いて移転されてきた個人データについて，そこから再委託（復処理）を行う場合，リヒテンシュタイン法に基づいた管理をしなさいといって本当に守れるのかという問題もある。

（3） 特別の状態における特則

十分性認定も，適切な安全性確保措置もない場合には，GDPR49条1項（a）ないし（g）の特別の状態における特則が唯一の移転根拠となる。もっとも，事業スキームにおいて処理根拠を複数備えることが適切であるように，十分性認定がされていたり，BCRやSCCによって移転根拠を備えていたとしても，49条1項のどれに基づいて移転が可能かを予め検討しておくことは重要である。(a) は同意に基づくものであるが，「移転がデータ主体に対して発生させる可能性のあるリスクについて情報提供」した上での，「明示の同意」が要求されている。GDPR6条1項（a）に比して要件は厳格であり，気軽に用いられるものでもない。(b) は契約に基づく移転であり，GDPR6条1項（b）と比較的近い。(c) は，例えば，個人データの管理者が第三者たる子会社と契約して，個人データをバックアップに取っているような場面では適用できるのではないかと思われる。(d) 以下が適用される場面は限定されるであろう。GDPR6条1項（f）に相当する条項は存在しない。

7 終わりに

GDPRについての情報は基本的には外国語であり，しかも，日本の個人情報保護法と比べても，その解釈は必ずしも安定していない。本稿では特に情報サービス産業の事業者を想定し，誤解のありそうな点，しばしば尋ねられる点を解説するように務めたが，基本的にはGDPR対応はデータマッピングから始まり，最低でも半年以上掛かるプロジェクトであり，手を動かし始めることが肝要である。一刻も早く着手することをお勧めする。