GDPR 対応の手順とスケジュール

ジェトロ海外調査部欧州ロシア CIS 課　　根津　奈緒美

2018年5月25日から EU では「一般データ保護規則（GDPR）」が施行される。日本企業は何から対応すればよいのか――GDPR 対応の主な手順を整理して紹介する。

施行開始に向けて

EU の一般データ保護規則（GDPR：General Data Protection Regulation）の施行開始が着々と近づいている。個人情報（データ）の保護という個人の基本的権利を確保することを目指す同規則は、欧州におけるデジタル単一市場（DSM）実現のための域内環境整備の重要な柱と位置付けられている。欧州経済領域（EEA：EU 加盟 28 カ国にノルウェー、アイスランド、リヒテンシュタインを含めた 31 カ国）と個人データをやり取りする日本の企業、機関、団体は基本的に GDPR の適用対象となる。同規則への違反行為には高額の制裁金が科されるリスクがある。中小企業や公的機関も例外ではない。

GDPR 対応の必要性については、欧州では広く認識され、具体的な準備段階に入っている企業も多い。日本においても、17 年に入ってからは、欧州ビジネスを行う企業の間でにわかに認知度が高まりつつある。ジェトロでも、セミナーの開催や実務対応のレポート「EU 一般データ保護規則（GDPR）実務に関わるハンドブック」（16 年 11 月に入門編、17 年 8 月に実践編）の公開などを通じて関連情報を発信している。

では、具体的に GDPR 対応に必要な準備とは何か。GDPR に関する加盟各国国内法の準備状況、第 29 条作業部会[注1]による GDPR を実践するために必要な各種ガイドラインの公表スケジュールはどうなっているのか。個人データの適法な処理の最も基本的な要件であるデータ主体（同データが関連する当該個人）の最も基本的な要件である「同意」のポイントとは――。

まずはデータの整理と社内体制づくりを

GDPR には、EEA 内で取得した個人データを「処理」し、EEA 外の第三国に「移転」するために満たすべき法的要件が規定されている。

関係する企業や団体が取るべき対策とは、GDPR において定められたデータ主体（個人データが関連する当該個人）の権利確保のための対応、それ以外にデータの管理者もしくは処理者に課されている、主にコンプライアンスのための義務の履行、また、GDPR の順守を裏付ける文書の準備……などである。これを踏まえた主な手順および各手順で具体的になすべき事項は以下のとおりである。

①現状評価（データマッピング）：保有データの整理と方針決定

まず、自社で保有している EEA 内の個人データを書き出す。それら個人データの自社における管理・処理・移転の方法およびデータ主体との関係を整理する。

次に、当該処理行為が GDPR で求められている個人データ処理その他の法的要件を満たしているかどうか。これについて、GDPR の規定、関係する加盟国の国内法（今後各国が制定するもの）および各種ガイドライン（第 29 条作業部会が公表済み、もしくは、今後公表するもの）と照合しながら一つ一つ確認する。

こうした確認により、まず現状の企業グループ内の対応として GDPR の要求に十分に応えられていない部分を洗い出す。そして、対策の優先順位などを社内で検討し、対応方針を固める。同時に、こうした作業の過程をとりまとめ、監督当局から照会を受けた際には、自社が適切に対応できる体制をとっていることを説明できるよう準備をしておく。

②データ保護責任者（DPO）の選任

データ処理を行う国および処理内容を踏まえ、自社が GDPR に定められる「データ保護責任者（DPO）選任義務」を負うべき企業に該当する場合（本誌 p.58、

新ドイツ連邦データ保護法の例を参照）には、その選任を行う。任務遂行のための体制づくりや研修参加などを通じたノウハウ構築についても検討する。

③リスク評価

自社が行うデータ処理のリスク評価を行い、GDPRで求められているケースに該当する場合には、同法に定められた項目に基づき、「データ保護影響評価（DPIA）」を行う必要がある。またDPIAの結果によっては、データの処理行為を実施する前に処理を行う国の監督機関に相談する必要がある。

④適法に処理されていることを示す根拠の確認

GDPRは、個人データを適法に処理するための要件を定めている。まずは自社が行う全てのデータ処理行為について、適法であると説明するための根拠を確認する。GDPRには、適法な処理の要件が六つ（表1）挙げられている。データ主体から「同意」を得ていること、管理者などが正当な利益を得るために処理が必要であることなどがこれに含まれる。

⑤ EEA外へのデータ移転の適法化

GDPRでは、EEA外へのデータ移転は原則として違法とされるが、以下のa. b. の場合については、移転が可能となる。

a.「十分性認定」（EUが十分な水準の個人データ保護がなされていると認定した国に与えられる）が与えられた国へのデータ移転。

b. それ以外の国・地域への移転に関して、例外的に適法と見なされる方法として定められた三つの方法のいずれかをとった場合。すなわち、「明らかな同意」による適法化、標準契約条項（SCC）による適法化、拘束的企業準則（BCR）による適法化である（SCC・BCR作成のポイントについては本誌p.56～を参照）。

日本は現時点ではa.には該当しないため、b.のいずれかの方法で適法化しておかない限り、GDPR施行後はEEA内から日本などの第三国にデータを移転した場合、違法行為と見なされ、制裁の対象となる。なお、日本に対する十分性認定については17年7月6日に、欧州委員会（以下、欧州委）のジャン＝クロード・ユンケル委員長と安倍晋三首相がデータの保護と活用に関する共同声明「個人データの越境移転に関する政治宣言」を発表。この宣言において両首脳は、「18年の早い時期」を目標として、相互のデータ移転を可能とするための努力を強化する旨を言及している。日本に対して十分性が認定されれば、上述のSCCやBCRの対応をせずとも、EU域内と同様に日本への個人情報の移転が原則として認められるようになる。

表1　個人データの適法な処理の要件

	適法な処理の要件（GDPR 第6条第1項）
(a)	データ主体が、一つ以上の特定の目的のために自己の個人データの処理に同意を与えた場合
(b)	データ主体が当事者となっている契約の履行のために処理が必要な場合、または契約の締結前のデータ主体の求めに応じて、手続きを実行するために処理が必要な場合
(c)	管理者が従うべき法的義務を順守するために処理が必要な場合
(d)	データ主体、または他の自然人の重大な利益を保護するために処理が必要な場合
(e)	公共の利益、または管理者に与えられた公的権限の行使のために行われる業務の遂行において処理が必要な場合
(f)	管理者または第三者によって追求される正当な利益のために処理が必要な場合。ただし、データ主体の、特に子どもがデータ主体である場合の個人データの保護を求める基本的権利および自由が、当該利益に優先する場合を除く

出所：ジェトロ調査レポート「EU一般データ保護規則（GDPR）に関わる実務ハンドブック（入門編）」

⑥データ侵害時の対応

GDPRでは、データが侵害された場合、72時間以内に監督機関に報告する義務が規定されている。万が一の際に迅速に対応できる体制を整えておく必要がある。侵害を受けたデータ主体への連絡体制も必要だ。

⑦データ主体の権利確保

その他のデータ主体が有する権利確保のため、データポータビリティー[注2]、削除権などをデータ主体から求められた場合に対応できるよう、社内システム上の対策を講じる必要もある。

加盟国法の整備状況

EUが定めるルールは、その加盟各国への拘束力の度合いに応じていくつかのレベルに分類される。GDPRは、EU加盟国に対し、国内法を介さずに、直接適用される「規則」として採択されており、18年5月の施行開始と同時に国内法に優先して適用される。ただしDPOの選任義務、DPIA実施が必要となるケースの判断など、一部の事項については、加盟国法で定めることができる余地を残しており、これについては加盟国法の内容を踏まえたデータ保護コンプライアンスを行う必要がある（本誌p.58～を参照）。

17年7月現在、GDPRを踏まえた新たなデータ保護に関する法律を既に立法したのはドイツのみである。米国ベーカー＆マッケンジー法律事務所が17年5月に発表した調査結果によると、その他にルクセンブルクやオランダではドラフトが公開されている。ルクセンブルクについては政府および監督機関であるデータ

保護国家委員会（CNPD）が、国内法をGDPRに置き換えることを既に決定している。オランダでは16年12月に、GDPRの実施法案が公表されている。

またフランスについても、デジタルリパブリック法案が16年10月に可決された。ただし同調査結果によると、フランスの監督当局フランスデータ保護当局（CNIL）は、現行法はGDPRにおける「子どもの同意の条件」、「特別カテゴリの個人データ」（本誌 p.58の2、3を参照）、「事前相談」といった事項に対応しておらず、法改正が必要だとしているという。同調査によれば、その他の多くの国については、いまだドラフトも発表されていない状況である。なお一部の国で公表されたドラフトについても、17年7月現在では英訳がなく自国民以外は内容を十分理解するのが困難なものもあるとしている。

なお、英国はEU離脱後もGDPRを英国の国内法とし、「データ保護法」として施行するという立場をとっている。他方でEU離脱後は、英国は欧州委によるデータ保護に関する十分性認定の決定を受けない限り、EEAから英国への個人データ移転は原則として禁止されることになる。もちろん欧州委による十分性認定の決定が早期になされる可能性はあるが、現時点ではこの点に関する取り扱いは何も決まっていない状況だ。

ガイドライン公表見通しと「同意」の考え方

EEA内の個人データを扱う企業や団体は、18年5月25日の施行開始までにGDPR対応のための体制を整えておく必要がある。他方で、規則に則した運用に関しては、「データ保護影響評価（DPIA）」「データ移転」といった個別の項目について、第29条作業部会が順次公表するガイドラインを参照する必要がある。だが、「同意」「解析」など、17年7月時点でいまだにドラフトすら発表されていない項目も多い。個別項目のガイドラインについては第29条作業部会が作業の見通しを公表しており、現時点の予定は表2のとおり。

表2　ガイドライン公表スケジュール

時　期	内　容
（2016年5月24日）	EU「一般データ保護規則（GDPR）」発効
（2017年3月）	英国ICO「同意」ガイドライン案発表
（2017年4月）	「データ保護責任者（DPO）」「データポータビリティー」「主導監督当局の特定」に係る最終版ガイドライン発表
	「データ保護影響評価（DPIA）」ガイドラインドラフト発表
2017年10月	「データ保護影響評価（DPIA）」ガイドラインを最終採択予定
遅くとも2017年12月	「同意」「解析」「透明性」「データ侵害通知」「データ移転」に係るガイドラインを新規採択予定
2018年5月25日	規則の適用開始（実質的な施行日）

資料：EUのデータ保護指令第29条作業部会資料を基にジェトロ作成

GDPRにおいては、前述のとおり個人データの処理、移転を適法に行うための六つの要件が規定されている。データ主体から得る「同意」はそのうちの一つの手段である。「同意」はGDPR対応において最も基本的で重要な行為であるが、その具体的な方法については、遅くとも17年12月までに公表予定とされているガイドラインを踏まえる必要がある。ただし、この公表を待っていると、施行開始直前に超特急で方針を固めなければならなくなる恐れもある。他方、「同意」のガイドラインについては、17年4月に英国の監督機関（ICO：Information Commissioner's Office）が第29条作業部会の公表を待たずにドラフト（案）を発表している。最終的には同部会が示すガイドラインを確認する必要があるが、ICOのドラフトを参考に基本的な方針を社内で議論しておくのも一案だ。本誌で内容の一部を紹介する。なお、英国ICOのガイドラインについても、現在公表されているのはそのドラフトであり、パブリックコンサルテーションの結果を踏まえた最終版の公表後に変更点を確認する必要がある。

「有効な同意」とは

英国ICOのガイドラインのドラフトによると、「データ主体の同意」とは、「データ主体が、宣言または明らかな積極的行為によって、自己に関する個人データの処理に合意して表す、自由意思による、特定的で、（十分な）情報提供に基づく、あいまいでない意思表示」を意味する。個人データ処理の適法性の根拠となる同意を取得する際は、表3で示した同意の条件を満たしているかどうかのチェックが重要になる。同意を得る際、その意思表示が沈黙によるもの、あらかじめチェックマークが記入されているボックスを使用したもの、不作為で同意を得たものでは同意を得た

表3　データ主体の「同意」を得たと認められる条件

GDPR 第7条
1. 処理が同意に基づく場合、管理者は、個人データ主体が自己の個人データの処理に対して同意しているということを証明できるようにしなければならない。
2. 個人データ主体の同意が他の案件にも関係する書面において与えられている場合、その同意の要求は、明瞭かつ平易な文言を用い、理解しやすくかつ容易にアクセスし得る形で、その他の案件と明らかに区別できる方法によって明示されなければならない。
3. データ主体は、同意を与える以前に以下の事項が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。 ・データ主体は、いつでも同意を撤回する権利があること。 ・同意の撤回は、撤回前の同意に基づく処理の適法性に影響を与えない。
4. 同意が自由意思によりなされているかについて判断する際、サービス約款を含む契約の履行が、当該契約の履行に必要のない個人データの処理に対する同意を条件としているか否かについて、最大限の考慮が払われなければならない。

出所：ジェトロ調査レポート「EU一般データ保護規則（GDPR）に関わる実務ハンドブック（入門編）」

とは見なされない。

「有効な同意」について、英国 ICO は GDPR に定められている表 3 記載の条件に加え、「管理者の氏名、処理の目的および処理行為のタイプを踏まえた上でなされた同意でなければならない」「同意は適切な時期に適切な形で見直され更新しなければならない」としている。

GDPR ではデータの「移転」を適法に行うための手段の一つとして「明らかな同意（explicit consent）」が挙げられている。英国 ICO は「明らかな同意」について、GDPR に定められているその他の「同意」と本質的に大きな違いはないと思われるとしている。「明らかな同意」のポイントは、明らかな声明の形で確認できなければならない点であると説明している。ICO は明らかな声明について「口頭か書面かを問わない」としているが、他方、明記されたものであっても「明らかな同意」とは見なされないケースもあるとしており、特に慎重な対応が求められる。

ケースに応じて使い分けを

英国 ICO はデータ主体に対し、「サービス提供の条件」としてデータ処理に係る同意を要求した場合、それは有効な同意とは見なされないケースがあると指摘している。例えば、当該データ処理がサービスを提供するために必要な場合、当該データ処理は表 1 の(a)「同意」ではなく(b)「データ主体が当事者となっている契約を履行するために処理が必要な場合」であることを適法性の根拠とするべきだというのだ。ただし、当該処理が契約履行のためではなく、マーケティングなどを目的として行われる場合には、上記の(b)の要件は適用されないため、(a)同意を根拠とする必要があるとしている。

さらに(b)が該当しない場合、すなわちデータ処理をサービス提供の条件としているものの、必ずしもサービスの提供のために当該データの処理が必要とはいえない場合には、(f)「管理者または第三者によって追求される正当な利益のために処理が必要な場合」という要件の適用を検討することになる。

「正当な利益」には商業的利益が含まれるため、これに該当することが説明できれば、同意や他の根拠なくデータの処理を行うことが可能だという。ただし英国 ICO は、その際の留意点として、データ主体である個人の権利や利益を害する恐れがないことを証明する必要があり、公正かつ透明性を持って説明責任を全うできるような体制を取っておかなければならないと強調している。また大前提として、データ主体の同意なしにデータ処理を行うことができる場合であっても、企業はコンプライアンスの観点からどのように個人データを扱っているかを監督当局に対して常に明確かつ分かりやすい形で情報提供できる体制を整えておく必要がある点を忘れてはならない。

従業員のデータ処理は同意以外を根拠に

英国 ICO の解釈では、データ処理者もしくは管理者が、（データを提供する）個人に対して明らかに優位な立場にある場合、データ主体による同意は自由意志に基づいた行為とは見なされない。このことから、基本的に「同意」は適切ではないとされる。この典型的な例として、「公的機関」や「従業員のデータを処理する雇用者」などを挙げている。すなわち、従業員の個人データの処理については表 1 で定められる処理の要件のうち、「同意」以外を根拠として適法化を行う必要がある。同意以外の可能性として英国 ICO は、民間事業者であれば表 1 (f)「管理者または第三者によって追求される正当な利益のために処理が必要な場合」が一つの選択肢になると示唆している。

なお、従業員の個人データに関する留意点として、データ「移転」を適法に行うための根拠の一つである「明らかな同意」について、一般に EEA 内のデータ保護監督機関は、従業員によるデータ移転の同意が「任意」のものと言えるかどうかについては非常に懐疑的であるとの立場を取っている。このことから、特に従業員のデータの移転について、「同意」を適法化の根拠とすることはリスクが高いと考えるべきだ。

英国 ICO のガイドラインのドラフトでは、上記の他に同意の取得方法および記録、管理方法や含めるべき情報、付録として同意取得のためのチェックリストを紹介している。

注1：加盟各国の監督機関の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関（EDPS）の代表によって構成される。特定の問題に関して共通の解釈と分析を提供することにより、EU 加盟国のデータ保護法の解釈にある程度の調和をもたらす。

注2：あるデータ管理者から別のデータ管理者へ個人データを転送する権利。個人から要求された場合に、当該個人のデータを再利用可能な形式で提供する義務が生じる。