【EU】一般データ保護規則（GDPR）の適用開始

海外立法情報課　島村　智子

＊2018 年 5 月 25 日、EU の新たな個人情報保護の枠組みである一般データ保護規則（GDPR）の適用が開始された。GDPR は、データの対象である個人の権利、データ管理者の義務、データの域外移転などを規定している。

1　背景

EU 基本権憲章[1]は、全ての者が、自己に関する個人データの保護を受ける権利を有すると定めている（第 8 条第 1 項）。加えて、当該個人データが、明示された目的のため、かつ、当事者の同意又はその他法に基づく何らかの正当な理由に基づいて、公正に取り扱われなければならないこと、また、全ての者が、自己に関して収集されたデータにアクセスする権利、及びそれを訂正させる権利を有することを規定している（同条第 2 項）。EU の基本条約の 1 つである EU 運営条約も、自己に関する個人データの保護を受ける権利を規定しており、さらに、欧州議会及び EU 理事会に対し、個人データの取扱いに関しての個人の保護と当該データの自由移動に関するルールを定めるよう義務付けている（第 16 条）。このように、個人データの保護は、EU の法体系の基礎をなす法において、基本的な権利と位置付けられている。

個人データの保護について、EU ではこれまで、1995 年に制定されたデータ保護指令（Directive 95/46/EC）に基づき規制がなされてきた。EU 法における指令（Directive）は、達成すべき結果について加盟国を拘束するが、そのための形式・手段の選択は加盟国に委ねられている。各国が国内法を通じて指令の規定内容を実施するため、個人データの取扱いにおいて実際に適用されるルールの詳細は、国によって差異が生じていた。このため、社会経済活動におけるデータ収集・利用規模の拡大に対処すべく、より統一的な規制の枠組みを定め、域内全体で確かな保護水準を実現すると同時に、自由なデータ流通を促進することが目指されることとなった[2]。

また、デジタル経済に関連する諸規制の統一は、EU の重点政策であるデジタル単一市場（Digital Single Market）の構築に向けた取組の中でも重視されており、域内における競争の平等を保障し、事業者にとっての法的安定性を改善するためにも、データ保護に関する統一的な規制が必要とされるようになった[3]。

＊　本稿におけるインターネット情報の最終アクセス日は、2018 年 6 月 11 日である。

1 EU 基本権憲章（Charter of Fundamental Rights of the European Union）は、欧州議会、EU 理事会及び欧州委員会による政治的宣言として 2000 年 12 月に採択され、その後、リスボン条約（2009 年 12 月 1 日発効）によって、基本条約（EU 条約（Treaty on European Union）及び EU 運営条約（Treaty on the Functioning of the European Union））と同等の法的価値を有することが定められた。

2 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012.1.25, pp.1-2, 5-6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011>

3 *ibid.*

2　経緯

データ保護指令に代わる個人データ保護の枠組みとして、欧州委員会は 2012 年 1 月、一般データ保護規則（General Data Protection Regulation: GDPR）案を提案した[4]。指令と異なり、規則（Regulation）は、国内立法がなくとも加盟国に直接適用される。立法機関である欧州議会及び EU 理事会は、それぞれの修正案に基づく協議を行い、2015 年 12 月 15 日、規則案の事前合意に至った。規則案は、2016 年 4 月 8 日に EU 理事会で、同年 4 月 14 日に欧州議会で採択され、4 月 27 日に成立した。GDPR は、同年 5 月 4 日に EU 官報で公布、5 月 24 日に施行され、2018 年 5 月 25 日から適用が開始された[5]。以下では、全 11 章 99 か条から成る GDPR について、概要を紹介する。

3　GDPR の概要

（1）定義・適用範囲（第 1 章）

GDPR において、個人データとは、特定された又は特定され得る個人（データ主体）に関する全ての情報を指す。「特定され得る」とは、氏名、位置データ、オンライン識別子などの識別子によって、又は、当該個人に固有の要素（身体的、遺伝的、精神的、経済的、文化的、社会的な特徴等）を通じて特定が可能なことを意味している。適用の地理的範囲について、GDPR は、EU 域内の管理者（個人データ取扱いの目的・手段を決定する者）の事業所による活動の中で行う、域内外での個人データの取扱いに適用される。また、EU 域内の個人に対する商品・サービスの提供及び EU 域内の個人の行動の監視に関係する場合には、域外の管理者による、当該個人のデータの取扱いにも適用される[6]。

（2）原則（第 2 章）

個人データに関して、取扱いの適法性・公正性・透明性の確保、収集目的の限定、目的に対する必要最小限化、正確性の確保、保管期間の限定、データ保全などの原則を遵守する義務が定められている。データの対象である個人による取扱いへの同意があれば、取扱いは適法となるが、この同意については、自由になされた、特定の、情報提供を受けた上での、かつ、明白な意思表示と定義されている。同意は、いつでも撤回が可能である。16 歳未満の者については、原則として、親権者による同意を必要とする（加盟国は、国内法によって 16 歳より低い年齢（ただし 13 歳以上）を設定することができる）。なお、人種・民族、政治的思想、宗教・信条若しくは労働組合員に関する個人データ、遺伝データ、生体認証データ、健康データ又は性的

4　*ibid.*

5　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), OJ L119, 2016.5.4, pp.1-88. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> GDPR は、EU 加盟 28 か国とともに欧州経済領域（EEA）を構成するアイスランド、リヒテンシュタイン及びノルウェーにも 2018 年 7 月半ば頃から適用が開始される見込みとなっている。“Incorporation of the General Data Protection Regulation (GDPR) into the EEA Agreement and continued application of Directive 95/46/EC,” 2018.6.5. EFTA website <http://www.efta.int/About-EFTA/news/Incorporation-General-Data-Protection-Regulation-GDPR-EEA-Agreement-and-continued-application-Directive-9546EC-508856>

6　なお、個人データの取扱いのうち、①EU 法の適用範囲外の活動におけるもの、②共通外交安全保障政策の範囲内の活動で加盟国が行うもの、③専ら個人的な又は家庭的な活動の中で行われるもの、④犯罪の防止、捜査、訴追等の目的で管轄官庁が行うものについては、適用除外となっている。このうち、④については、警察・刑事司法分野の管轄官庁による個人データの保護を規定した指令（Directive (EU) 2016/680）が、GDPR と同日に別途制定された。

指向データについては、特別の類型の個人データとして、取扱いが原則禁止され、その例外が列挙されている。

（3）個人の権利（第 3 章）

個人データを収集する場合には、データの取得時に、データ管理者の身元及び問合せ先、データ取扱いの目的・法的根拠などの情報を本人に提供する義務が定められている。個人データを提供した本人は、自己の個人データ及びそれに係る情報へのアクセス権を有する。また、不正確な自己の個人データの訂正権、収集目的のために必要でなくなった場合や本人が同意を撤回した場合などの消去権（忘れられる権利）、取扱いを制限させる権利、提供した個人データを受け取り、他の管理者に送信できるデータポータビリティの権利、プロファイリング（業務実績、経済状況、嗜好、関心事など分析・予測を目的とする個人データの自動処理）を含め、取扱いに対して異議を申し立てる権利が規定されている。これらは、当該制限が基本的人権と自由を尊重し、国家安全保障、公共の安全、犯罪の防止・捜査・訴追などを擁護するために必要かつ均衡の取れた措置である場合には、立法により制限することができる。

（4）管理者の義務（第 4 章）

個人データの管理者には、GDPR に従ったデータの取扱いが行われるよう適切な技術的・組織的措置をとることが義務付けられており、当該措置は、見直し、必要な場合には更新されなければならない。管理者が EU 域外にある場合には、取り扱うデータの対象である個人が存在する加盟国のいずれかに、代理人を設置しなければならない。また、個人データの予期しない又は不法な破壊、喪失、改変、不正アクセス等に至る、保全違反である個人データ侵害があった場合、管理者は、発見後 72 時間以内に各国の監督機関に報告しなければならない。個人の権利・自由に対し高度なリスクをもたらすおそれがあるデータ侵害について、本人に通知する義務も定められている。このほか、データの取扱業務の体系的な記述やリスク評価を含む、データ保護への影響評価の実施や、専門的知識を有するデータ保護責任者の設置が規定されている。

（5）域外へのデータ移転（第 5 章）

十分な個人データ保護水準を保っていると欧州委員会が決定した第三国又は国際機関に対し、個人データの移転が可能と定めている[7]。このような決定のない国・機関への移転については、監督機関の許可なく移転が認められるケースとして、①公的機関間の法的に拘束力があり執行可能な文書による場合、②監督機関の承認を受けた、企業グループ内の個人データの移転について定めた拘束力のある企業準則（binding corporate rules）による場合、③欧州委員会が採択した又は監督機関が採択し、欧州委員会が承認した、標準データ保護約款（standard data protection clauses）による場合、④所定の手続によって承認された、行動準則（code of conduct）あるいは認証（certification）による場合が規定されている。さらに、監督機関の許可を条件に移転が認められる場合、及び特定の状況に基づき例外的に移転が可能とされる場合について規定されている。

---

[7] 決定を受けている国等については、欧州委員会のウェブサイトを参照。“Adequacy of the protection of personal data in non-EU countries” European Commission website <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>

（6）独立監督機関・協力（第 6 章・第 7 章）

各加盟国は、GDPR の適用に関し、監視、啓発、国内機関への助言、苦情処理、調査等を担う監督機関を設置しなければならない。個人データの管理者・取扱者が、域内で国境を越えてデータの取扱いを行っている場合には、その主たる事業所がある加盟国の監督機関の所管となる。ただし、個人は、苦情の申立てを自国の監督機関で行うことが可能である。

また、各国の監督機関と欧州データ保護監督官[8]で構成される EU の組織として、欧州データ保護会議（European Data Protection Board）の設置が定められている。

（7）救済・罰則（第 8 章）

自己のデータの取扱いが規則に違反すると考える場合に、個人が、監督機関に対して苦情の申立てを行う権利と、監督機関の決定に対して司法的救済を受ける権利が定められている。また、規則違反による権利侵害に対する司法的救済と、損害に対する賠償を受ける権利が規定されている。さらに、違反に対して科される制裁金として、違反内容に応じ、最大で、①1000 万ユーロ[9]又は前会計年度の総売上高の 2%のうち、いずれか高い方、②2000 万ユーロ又は前会計年度の総売上高の 4%のうち、いずれか高い方の、2 段階が定められている。

4　国内法に基づく規定

加盟国が、国内法によって規定すべき事項及び規定することが可能な事項が含まれている。このため、GDPR の制定以降、各国で国内法の整備も進められている。各国が規定可能な主な項目には、取扱いの適法性に関する要件の一部（第 6 条）、情報社会サービスの提供に関する子供の同意に係る年齢制限（第 8 条）、特別な類型の個人データの取扱い（第 9 条）、消去権（第 17 条）、データ保護影響評価（第 35 条）、データ保護責任者の選任（第 37 条）及び地位（第 38 条）、雇用に関する従業員の個人データの取扱い（第 88 条）、守秘義務（第 90 条）などがある。また、各国は、上述（3（7））の制裁金の対象とならない違反行為に関して罰則規定を定めなければならず、当該規定を欧州委員会に通知しなければならない（第 84 条）。[10]

このように、指令から規則に変更後も、国内法でルールが定められる余地が残されているため、企業活動における実際の対応に際しては、各国の国内法の動向にも留意が必要との指摘が見られる[11]。

参考文献

・個人情報保護委員会及び日本情報経済社会推進協会（JIPDEC）は、各機関による GDPR 条文の仮日本語訳を次のとおり公開している。「GDPR（General Data Protection Regulation：一般データ保護規則）」個人情報保護委員会ウェブサイト <https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/>; 「EU 一般データ保護規則（仮訳）について」日本情報経済社会推進協会（JIPDEC）ウェブサイト <https://www.jipdec.or.jp/library/archives/gdpr.html>
・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, pp.37-242.

8 欧州データ保護監督官（European Data Protection Supervisor: EDPS）は、EU 諸機関における個人データの取扱いを監督する独立の機関。“About” European Data Protection Supervisor website <https://edps.europa.eu/about-edps_en>

9 1 ユーロは約 132 円（平成 30 年 6 月分報告省令レート）。

10 杉本武重「加盟国法を踏まえたデータ保護コンプライアンスを」『ジェトロセンサー』2017.10, pp.58-60. <https://www.jetro.go.jp/ext_images/biz/special/2017/37d786f4de44651c/11.pdf>; 鷲澤純「EU 加盟各国で整備が進む個人データ保護法―GDPR 施行開始に向けて―」2018.2.20. 日本貿易振興機構（ジェトロ）ウェブサイト <https://www.jetro.go.jp/biz/areareports/2018/bef14bc82cad6929.html>

11 同上