5　GDPRの概要

弁護士　上里 美登利

Q5－1　GDPRとは

EUで制定されたGDPRとは何ですか。EU域内に拠点を持たない日本企業にも適用されるのですか。

A5－1

GDPRとは、General Data Protection Regulationの略称で、2018年5月25日に施行されています。EU域内に拠点を持たない日本企業であっても、欧州経済領域（EEA）に在住する自然人の個人データを扱う場合、GDPRの適用対象となり得ます。

解説

EUで制定されたGDPR とは、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）を指している。GDPRは、2016年4月に制定され、2018年5月25日に施行された。

GDPRは、EU加盟国の法規制整備を求めるEUデータ保護指令と異なり、EU加盟国に直接適用される。また、欧州経済領域（EEA）協定に結合されたことから、EU加盟国に加え、アイスランド、リヒテンシュタイン、ノルウェーにも適用されることとなった。もっとも、GDPRが適用領域に関して「the Union」という用語を用いていることから、本稿では適用領域に関して「EU」と表記している。

GDPRは、基本的権利及び自由と、特に個人データの保護に関する権利の保護を目的とし、個人データの取扱いに係る自然人の保護に関する規定等を定めている（Article1（1）（2））。

企業等の拠点がEU域外にある場合でも、①EU在住のデータ主体に対して商品またはサービスを提供する場合（データ主体に支払が要求されるか否かに関わらない）、②EUのデータ主体の行動を監視する場合には、GDPRの適用が及ぶ（Article3（2））ため、注意が必要である。

例えば、EU域内に現地法人や支店等の物理的施設を有しなくとも、EU向けのwebサイトを開設し、日本国内からインターネット取引でEUに在住する個人の氏名やメールアドレス、クレジットカード番号等の情報を取得する場合には、GDPRの適用対象となる。

なお、2018年5月25日の施行から2年が経過し、欧州委員会は、2020年6月24日にGDPR導入後2年間の成果の検証と見直しに関する最初の報告書[1]を公表した。同報告書によれば、EUでの個人データに関する権利意識が高まっていることなどが報告されている。

Q5－2　GDPRの主な規制内容

GDPRの主な規制内容を教えてください。

A5－2

GDPRは、個人データの取扱い及び移転に関する規律を定めると共に、データ主体の権利、個人データ侵害が生じた場合の措置、規則違反に対する制裁等も定めています。

解説

GDPRは、保護の対象である「個人データ」を、「識別された、または識別され得る自然人に関するすべての情報」と定義している（Article4（1））。また、識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の物理的、生理的、遺伝子的、精神的、経済的、文化的又は社会的な同一性を示す一つ又は複数の要素を参照することによって、直接的又は間接的に、識別され得る者をいうとされている（Article4（1））。

GDPRは、この個人データの取扱い及び移転に関する規律を定める他、データ主体には、原則として個人データの消去を請求する権利（忘れられる権利/Article17）等を始めとする権利を保障している。

また、EU域外への個人データの移転は、GDPRが認める条件下に限り認められる（Article44）。GDPR施行時には、日本は、例外的に移転が認められる十分性認定（Article45（1））を受けておらず、EUからの個人データの移転を可能とするための対応に相当な労を要していたが、2019年1月23日に十分性認定を受けるに至った。

個人データの侵害が生じた場合、72時間以内に管轄監督機関へ規定事項を含む通知が必要であり（Article33）、データ主体に対しても、自然人の権利及び自由に対する高リスクを引き起こし得る場合は原

則として遅滞なく通知が必要とされている（Article34）。

Q5－3　GDPRに基づく制裁金

GDPRに違反すると高額な制裁金が科せられると聞きましたが、本当でしょうか。また、施行後2年間で高額な制裁が科された事例はあるのでしょうか。

A5－3　GDPRに違反した場合の制裁金

GDPRは、高額な制裁金を定めています。施行後2年間で高額な制裁事例も出てきています。

解説

（1）GDPRは、違反に対する制裁が厳しく、義務違反の類型に応じて2種類の制裁金の上限を定めている（Article83（4）（5））。

ア　類型1

制裁金の上限額：最大1000万ユーロ、または事業である場合、全世界年間売上高の 2%のいずれか高い方（Article83（4））

違反事由の例：

・セキュリティレベルをリスクに見合ったものとする適切な技術的・組織的対策を実施しなかった場合（Article32）

・個人データ侵害を監督機関に通知する義務を怠った場合（Article33）、データ主体に通知しなかった場合（Article34）

・その他の事由（Article8,11,25,27,28,30,31,35,36～39,41（4）,42,43）

イ　類型2

制裁金の上限額：最大2000万ユーロ、または事業である場合、全世界年間売上高の 4%のいずれか高い方（Article83（5））

違反事由：

・個人データの取扱いに関する原則を遵守しなかった場合（Article5）

・個人データを適法に取り扱わなかった場合（Article6）

・同意の条件を遵守しなかった場合（Article7）

・その他の事由（Article9,12～ 22,44～ 49,58（1）（2））

（2）高額の制裁事例

違反に対して制裁金を科すのは、欧州委員会ではなく、EU加盟国それぞれが設置する監督機関とされている（Article58（2）（i））。GDPR施行後、現時点では、日本企業に対してGDPRに基づく制裁が科せられた件は見当たらない。他国では、制裁金が科せられた事例は多数存在し、高額の制裁金が科せられた事例もいくつか存在する。以下の事例はGoogleに対するものである。

2019年1月21日、フランスのデータ保護機関CNIL（Commission Nationale de l'Informatique et des Libertés）が、Google LLCに対して、5000万ユーロの制裁金の支払いを命じた[2]。ターゲティング広告目的の処理を行うためのデータ主体からの同意の取得方法に問題があり、同意は無効と判断したことを1つの理由としている。CNILの説明によると、2つの団体からの苦情申立てが調査の端緒だったようである。

Googleに対しては、2020年3月11日、スウェーデンのデータ保護監督機関（Datainspektionen）も、GDPRに違反しているとして、7500万スウェーデンクローネ（約700万ユーロ）の制裁金を科すこととした[3]。検索結果の削除に関して当機関が命じた措置を適切に実行しなかったことが理由に挙げられている。これは、Article17の忘れられる権利の関係の違反と考えられる。

Q5－4　日本企業の注意点

GDPRについて、特に日本企業が注意すべきポイントを教えてください。

A5－4

Q5－1のとおり、EU域内に拠点を置かない日本企業であっても適用される場合があること、日本の個人情報保護法とGDPRでは規律内容に違いが存在する部分があることに留意が必要です。

解説

Q5－1のとおり、日本企業であっても、EU域内に在住する自然人の個人データを扱う場合は、GDPRの適用対象となり得るため、注意が必要である。なお、データを扱う事業体の規模は問われず中小企業であっても適用対象となる。

日本が十分性認定を受けたことからも分かるように、日本の個人情報保護法とGDPRの内容は類似しているが、一部相違する部分がある。この点につき、日本の個人情報保護委員会は、「個人情報の保護に関する法律に係るEU及び英国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に関する補完的ルール」を定めており、EU域内及び英国域内から十分性認定により移転した個人データを受領する個人情報取扱事業者は、このルールも遵守する必要がある。また、全般的にGDPRの方が取扱いに関する厳格な規制やデータ主体の権利保護を定めているため、確認が必

要である。

また、前記のGoogle LLCに対するCNILの制裁事例も参考に、改めてGDPRにおける情報主体からの「同意」の取得要件に注意が必要と考える。「同意」については、Guidelines on consent under Regulation（同意に関するガイドライン）が存在し、仮訳[4]も存在するため、こちらも参照することが望ましい。

1　two years of application of the General Data Protection Regulation（https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en）
2　https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
3　https://www.datainspektionen.se/nyheter/the-swedish-data-protection-authority-imposes-administrative-fine-on-google/
4　https://www.ppc.go.jp/files/pdf/doui_guideline.pdf

【参照資料・URL】

・個人情報保護委員会 GDPR
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/
・General Data Protection Regulationの【条文】仮日本語訳（個人情報保護委員会による翻訳）
https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf
・JETRO EU 一般データ保護規則（GDPR）について
https://www.jetro.go.jp/world/europe/eu/gdpr/