

## 欧州「一般データ保護規則（GDPR）」施行

### ◆個人情報保護に関するEUの新法GDPRが2018年5月施行

欧州連合（EU）では、1995年以来適応されてきた個人情報保護に関する法律「データ保護指令」が改変され、「一般データ保護規則＝General Data Protection Regulation（GDPR）」が2018年5月25日に施行される予定だ。

新法は、インターネットの普及など急速な技術革新に対応したものとなっている。また、「指令」には国内法への転換時に各国に一定の裁量権があるが、国内法よりも優先される「規則」へ変更され、域内で一貫した制度となる。

### ◆EUの定める個人情報の範囲とは

GDPRでは、EUを含む「欧州経済領域（EEA）内で取得した個人データをEEA域外に移転すること」が原則禁止される。個人データは、域内の市民や居住者自身がコントロールするものであることを明確にしている。（EEA＝European Economic Area EUにアイスランド、ノルウェー、リヒテンシュタインを加えた枠組み）

個人データの「個人」とは、EEA 域内の居住者全般を指し、現地進出の日系企業に勤務する現地採用従業員や、日本から派遣されている駐在員も含まれる。

GDPRで対象となるのは、個人に関係するあらゆる情報である。氏名、住所、写真のような情報だけではなく、個人を特定することのできる関連情報のすべてが、「個人情報」とみなされる。たとえば、コンピュータのIP アドレスなども含まれており、日本の「改正個人情報保護法」との違いが見られる。（表1参照）

表1 個人データの例示

EU GDPR	日本 改正個人情報保護法
氏名、識別番号、 IP アドレス、クッキー識別子 身体的、生理学的、遺伝子的、精神的、 経済的、文化的、社会的固有性に関する 要因	氏名、生年月日 生体データの個人識別符号（DNA、顔、 虹彩、声紋、指紋など） 公的な個人識別符号（マイナンバー旅券 番号、基礎年金番号、免許証番号など）

GDPR (<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN> 英文)

個人情報保護法ハンドブック ([https://www.ppc.go.jp/files/pdf/kojinjouhou\\_handbook.pdf](https://www.ppc.go.jp/files/pdf/kojinjouhou_handbook.pdf))

さらに、健康情報などは「特別カテゴリーの個人データ」に該当し、特別な条件を満たさない限り取扱いが禁じられている（GDPR第9条）。日本と比較すると、民族、労働組合員資格、あるいは政治的思想に関する情報が含まれているところが、欧州の多様性や歴史的背景をうかがわせる。（表2参照）

表2 特に配慮が必要な個人データの例示

EU GDPR	日本 改正個人情報保護法
人種、民族的素性、政治的思想、宗教的もしくは哲学的信条、労働組合員資格、遺伝データ、生体認証データ、健康に関するデータ、性生活もしくは性的指向に関するデータ	人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実 身体障害、知的障害、精神障害 健康診断結果、保健指導、診療情報 刑事事件に関する手続が行われたこと

表1、表2ともにARCまとめ

#### ◆ プライバシーを重視、忘れられる権利＝削除権を明記

GDPRでは、「削除権」として、データの対象者（本人）に、関連する個人データの削除とそのデータの頒布の中止を、データ運営管理者に実行させる権利が認められているのが特徴的だ（GDPR第17条）。

インターネット上で、無関係の人が犯罪の関係者に仕立て上げられたり、個人にとって極端に不利な情報が検索サイトの上位に現れて炎上するケースが日本でもみられるが、デジタル化の進展により消したい個人情報も簡単に流布するようになってきている。欧州ではインターネット上の「忘れられる権利（right to be forgotten）」が、最近強く求められるようになってきた。裁判所が「忘れられる権利」を認める判決も出している。たとえば、14年にスペイン人男性が、自分の名前の検索結果に、所有していた不動産が競売に掛けられたことを報じた10年以上前の新聞記事が表示されることを、「プライバシーの侵害」としてグーグルを提訴した裁判で、EU司法裁判所が、検索企業にリンクの削除義務があるとする「忘れられる権利」を認める判決を下している。この判決を受けたグーグルは、EUの利用者を対象に、検索結果に含まれる自分に関する情報の削除要請を受け付けるサービスの運用を始めた。

このような背景もあり、GDPRでは「削除権」が明記された。バックアップデータも含むすべてのデータが削除の対象となる。

#### ◆個人の権利の強化、個人データ侵害時には72時間以内に監督機関へ通知

削除権が示すように、GDPRでは、EEA域内の市民と居住者が自分の個人データをコントロールする権利、つまり個人の権利が強化されている。データの対象者（本人）がデータ処理業者などへデータの訂正を求める権利（第16条）、データへアクセスできる権利（第15条）などに加え、GDPRではデータを手にする権利（データポータビリティ）が新たに認められた。

「データポータビリティ」権利とは、個人データが電子的手段で処理される場合、データの対象者には、利用可能な電子的に構造化された共通フォーマットの形式で、データのコピーを管理者から入手する権利（第20条）をいう。

携帯電話のナンバーポータビリティにより、企業の囲い込みを受けずに他のサービスへの乗り移りが容易になったことをイメージするとわかりやすい。日本でも経済産業省と総務省が、個人が要求すればいつでも自分のデータを手元に引き出せる仕組みの検討に入ったところだ。

個人データの管理については、管理者は個人情報を適切に管理し漏洩防止などに努める必要があるが、万が一、「個人データ侵害」が発生した場合、データ管理者は72時間以内に監督機関に通知しなければならない。個人データ侵害に関する通知は遅延なくデータの対象者にも行わなくてはならない（第33条）。

個人データの侵害の例としては、サイバー攻撃による自社サーバに保管された個人データの漏洩などが考えられる。侵害が発生した際には、それを素早く検出して、72時間以内というタイムリミットの間に監督機関へ通知することが可能な体制を構築することが求められている。

#### ◆GDPR違反で、最大2,000万ユーロ、または年間世界売上高の4%の制裁金

GDPRに違反した場合には、最大2,000万ユーロ（約26億円）、または年間世界売上高の4%の高い方という巨額の制裁金を科される可能性がある。データ保護法の対象範囲も、EUを含む欧州経済領域（EEA）域内に拠点を置く企業・団体・機関だけではなく、EEA域内居住者のデータを処理する外国の企業にも拡大された。域内に子会社がある日本企業や、域内に拠点がなく日本企業でも、該当する個人データを扱う場合には対象となる。たとえば、域内個人向けに物品やサービスを提供、個人情報から生成されたデータを使用、行動モニタリングや市場調査

を行っているといったケースが当てはまる。

GDPRでは、EUを含むEEA域内で取得した個人データをEEA域外に移転することを原則禁止しているため、域外からのデータセンター等へのリモートアクセスでも、データ受信者のデータ保護レベルが十分でないと違反と見なされる。

#### ◆求められるのは適切な管理と、セキュリティの強化

GDPRへの対策として求められるのは、日本の「改正個人情報保護法」への対応と同様に、まずは個人情報の適切な管理だ。十分なセキュリティ対策が適切に実施されることを証明する義務を負い、その順守は管理される必要がある。本人からの個人データの請求や消去の要請にも応じなければならない。

個人データが日本に転送され、日本国内のサーバに保存される場合は、EEA域外に個人情報データを移転することを意味する。こうしたケースは、社内管理用であっても、GDPRの対象となる。たとえば、現地従業員の個人情報が日本本社のサーバに保存される場合が該当する。このような場合には、本人からの「積極的行為による」利用同意が必要となる。事前にチェックボックスに印が付いているものは認められない。

企業間の対策としては、データの輸出者とデータの輸入者で標準契約条項（Standard Contractual Clause：SCC）を締結する方法がある。SCCとは、欧州委員会によって決定された契約書の雛形であり、当事者間でこの雛形を使ってデータ移転契約を締結することで適切な保護措置を提供し、適法なデータ移転を行うものだ。将来的に、個人データ保護レベルについて日本が国としてEUから「十分性認定」を取得できれば、域外であっても個人データの自由な流通は保障されることになるが、厳しい審査があり認定取得には時間がかかると予想される。

各社・機関の置かれている状況や扱うデータの種類や数量によっても求められる対策は異なる。たとえば、人種や健康情報などの「特別カテゴリーの個人データ」を扱う場合や、大規模なデータ管理や大容量の重要データの処理を主に扱うような企業は、「データ保護責任者（Data Protection Officer：DPO）」を選任しなければならない。具体的に必要な対策については、ジェトロのハンドブックを参照したり、欧州の機関が行うセミナーで説明を受けたり、法律の専門家と相談するなどして確認し、早めに対応することが求められる。 【赤山英子】