EU一般データ保護規則（GDPR）の概要と企業が対応すべき事項

アドバイザリー事業部　公認会計士　梅澤　泉

▸ Izumi Umezawa
公認情報システム監査人、公認不正検査士。金融機関、製造業、小売業、サービス業などの会計監査を経て、個人情報保護をはじめとする情報セキュリティ監査やデータセンター事業者・クラウドサービス事業者の顧客向けサービスに係る内部統制の保証業務に従事。

Ⅰ　EU一般データ保護規則の概要

1. GDPRとは

EU一般データ保護規則（General Data Protection Regulation：GDPR）は欧州連合（EU）における新しい個人情報保護の枠組みであり、個人データ（personal data）の処理と移転に関するルールを定めた規則です。1995年から適用されたEUデータ保護指令（Data Protection Directive 95）に代わり、EU加盟諸国に対して直接効力が発生する法規制としてGDPRが2016年4月に制定されました。

2. GDPRの規制事項

(1) 個人データの処理

個人データを処理するに当たり、企業は管理者（Controller）として、次のような規制事項を遵守することが求められます。

- 個人データの処理および保管に当たり、適切な安全管理措置を講じなければならない。
- 処理を行う目的の達成に必要な期間を超えて個人データを保持し続けてはならない。
- 個人データの侵害（情報漏えい）が発生した場合、企業はその旨を監督機関に対し72時間以内に通知しなければならない。
- 定期的に大量の個人データを取扱う企業などでは、データ保護オフィサー（Data Protection Officer）を任命しなければならない。

(2) 個人データの移転

EEA（欧州経済領域）の域内から域外への個人データの移転は原則として禁止され、例えば日本のように欧州委員会によって適切な個人情報保護制度を有していると認められていない国への情報移転に当たっては、企業は拘束的企業準則（Binding Corporate Rules）の策定、標準契約条項（Standard Contract Clauses）の締結など、適切な施策の下で一定の要件を満たす必要があります。

(3) 基本的権利の保護

GDPRはデータ主体（Data Subject）すなわち本人の基本的権利を保護するという考え方が強く打ち出されています（GDPR第1条）。例えば個人データの取得に際しては、以下のようなルールが定められています。

- 企業は管理者として自らの身元や連絡先、処理の目的、第三者提供の有無、保管期間、データ主体の有する権利などについて、明瞭で分かりやすい表現によりデータ主体に通知しなければならない。
- 企業は前記に関して明確な方法により同意を得るとともに、データ主体が同意を自由に撤回することができる権利を適切に行使できるようにしなければならない。
- 個人データをデータ主体から直接取得していない場合、企業は当該情報の入手先を本人に通知しなければならない。

こうした主な規制事項を含め、GDPRでは全部で173項目の前文とともに99条にわたる規制事項がきめ細かく定められています。

Ⅱ　日本企業への影響

1. 影響を受ける企業

GDPRはEUで定められたルールですが、以下のような場合は日本の企業であっても適用対象となり、必ず

▶表1　制裁金と違反例

制裁金	違反例
最大で企業の全世界売上高（年間）の2%、または1,000万ユーロ*のうちいずれか高い方	▸個人データの取扱いに関し、適切な技術的、組織的安全管理対策を実施しなかった場合（そのような措置を取らない処理者に個人データの処理を委託する場合も含む） ▸個人データの処理に関する記録を残すことが義務付けられているにもかかわらず、記録を書面で保持していない場合 ▸個人データの侵害（情報漏えい）が発生したにもかかわらず、監督機関に対し適時に通知しなかった場合 ▸データ保護オフィサー（DPO）の選任が義務付けられているにもかかわらず、任命していない場合
最大で企業の全世界売上高（年間）の4%、または2,000万ユーロ*のうちいずれか高い方	▸個人データの処理に関する原則、適法な取扱い、同意に関する条件およびセンシティブ情報の取扱いを遵守しなかった場合 ▸個人データの域外移転に関するルールを遵守しなかった場合 ▸監督機関からの命令に従わなかった場合

＊　1ユーロ＝120円とした場合、1,000万ユーロは12億円、2,000万ユーロは24億円

しも無関係であるとは限らない点に注意が必要です。

(1) EUに子会社、支店、営業所を有している企業

EU域内に所在地がある当該子会社などにとってGDPRは直接の適用対象であり、当該企業は日本に本社を有している場合でも、管理者としてGDPRへの対応が必要となります。

(2) 日本からEUに商品やサービスを提供している企業

EU域内の個人（消費者）に対して日本から商品やサービスを提供している場合、たとえEU域内に子会社などがなかったとしても、当該企業は個人データの取得や処理に当たりGDPRに沿った手続を実施する必要があります。

(3) EUから個人データの処理について委託を受けている企業

データセンター事業者やクラウドベンダーなどのように、EU域内の企業から個人データの処理などを受託している日本企業の場合、当該受託企業は処理者（Processor）として個人データの域外移転に関してGDPRが定めるルールに準拠する必要があります。

2. 違反時のインパクト

Ⅰ 2. で述べたように、GDPRは適用対象となる企業に対しさまざまな義務を課すとともに、違反した場合には多額の制裁金を課すことでルールの遵守を厳格に働きかけています（GDPR第83条）（<表1>参照）。

Ⅲ　GDPRへの対応に向けて

日本においても個人情報保護法が改正され、2017年5月30日から全面施行となります。しかし、個人データを取扱う保護レベルとしては、日本はいまだ欧州委員会による十分性の認定を受けるに至っていません。このため、日本企業が事業活動を積極的にグローバル展開していく中で、個人データをEUとの間で円滑に流通させるためには、各企業がGDPRに沿った対応について自主的に取り組む必要があります。

GDPRの要求事項は多岐にわたるため、企業は各条文の内容の理解にとどまらず自社の置かれている状況を適切に把握した上で、次のような実務対応計画を慎重に進めていくことが望ましいと考えられます。

【準備フェーズ】

各拠点においてどのような個人データが存在し、どのような経路で流通しているのかについて現状を調査する（データマッピング）。その上でGDPR対応として必要な作業について担当部署、作業ボリュームを把握することにより、次フェーズに向けた全体計画およびスケジュールを決定する。

【対応フェーズ】

準備フェーズの計画に基づき、GDPR対応として求められる個人データ保護の管理態勢（組織内の役割分担、規程類の整備、運用ルールの決定など）を構築し、関係者に周知徹底する。

【運用フェーズ】

新たに制定した規程類、ルールにのっとって適切に運用が行われているかどうかを評価し、必要に応じて規程等の見直しまたは運用の改善を実施する。

以上を踏まえ、企業は18年5月の適用開始に向けて、限られた時間の中で効率的かつ速やかにGDPR対応を推進していくことが重要となってきます。