EUにおける「一般データ保護規則（GDPR）」への企業の対応

2016年4月14日、欧州議会において、欧州連合（European Union／以下「EU」）の新しい個人データ保護法である「一般データ保護規則（General Data Protection Regulation／以下「GDPR」）」が採択された。現在もEUデータ保護指令に基づく加盟国法としてのデータ保護法が欧州経済領域（European Economic Area／以下「EEA」）[1]の各国に存在するが、2018年5月24日をもってこれらの加盟国法は廃止となり、2018年5月25日からEEA全体で一つのデータ保護法が効力を持つことになる[2]。

本稿では、GDPRの概要、企業が準備・検討しておくべき項目およびEEA域内における企業の取組みについて、ウィルマーヘイル法律事務所ブリュッセルオフィス・弁護士の杉本武重氏に解説いただいた。

1．GDPRの概要

GDPRは、EEA域内において「個人データ」を「処理」し、個人データをEEA域内から第三国へ「移転」するために満たすべき法的要件を規定している。EEA域内において、コンプライアンス対応を何も取らずに個人データの処理や移転を行えば、原則GDPRに違反し違法行為となる。GDPRの目的が、EU基本権憲章というEU法体系の根幹をなす法において保障されている「個人データの保護に対する権利という基本的人権の保護」であるため、企業・団体にとって厳しい制度となっている。GDPRは、基本的人権という重要な価値を保障するため、違法となる場合を広く規定し、違反に対し行政罰を定めている。

行政罰とは、GDPRに違反した場合に科せられる可能性のある制裁金のことである。義務違反の類型ごとに2種類の制裁金の範囲が用意されている。

- 1,000万ユーロ以下または管理者[3]または処理者[4]の全世界年間売上高の2%以下のいずれか高い方（事業者以外の場合は、1,000万ユーロ以下）
- 2,000万ユーロ以下または管理者または処理者の全世界年間売上高の4%以下のいずれか高い方（事業者以外の場合は、2,000万ユーロ以下）

「個人データ」とは、識別された、または識別されうる自然人（データ主体）に関するすべての情報をいう。個人データには、自然人の氏名、識別番号、所在地データ、メールアドレス、オンライン識別子（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が含まれる。およそ個人の特定につながる情報は、個人データに該当する。

[1] EU加盟国28カ国＋アイスランド、リヒテンシュタイン、ノルウェー。
[2] 一定の事項、例えば雇用関係の個人データ処理については、加盟国が個別のルールを立法できるとされていることに留意が必要である。
[3] 単独または他と共同して、個人データの処理の目的および手段を決定する自然人、法人、公的機関、行政機関またはその他の団体
[4] 管理者のために個人データの処理を行う自然人、法人、公的機関、行政機関またはその他の団体

「処理」とは、個人データまたは個人データの集合に対して行われるあらゆる単一の作業、または一連の作業をいう。この作業は、取得、記録、編集、構造化、保存、修正または変更、復旧、参照、利用、移転による開示、周知またはその他周知を可能なものにすること、整列または結合、制限、消去または破壊することをいう。

「個人データ」の「処理」の例は以下の通りである。

- クレジットカード情報の保存
- メールアドレスの収集
- 顧客の連絡先詳細の変更
- 顧客の氏名の第三者への開示
- 従業員業務評価の閲覧
- オンライン ID の削除
- 全従業員の氏名や社内での職務、事業所の住所、写真を含むリストの作成

個人データの「移転」には、GDPR 上は明確な定義がなされておらず、個人データを電子メールによって、EEA 域内（例えば、ベルギーのブリュッセル）から EEA 域外（例えば、日本の東京）へ送信すること等がこれにあたる。

GDPR は、EEA 域内の管理者または処理者の拠点（EEA 域内に所在する子会社、支店、駐在員事務所等）の活動に関連してなされる個人データの処理（処理が EEA 域内または域外でなされるか否かを問わない）に適用される。また、GDPR は EEA 域内に拠点のない管理者または処理者による EEA 域内に所在するデータ主体の個人データの処理に対しても、処理活動が次に掲げる項目に関連しているものであれば適用される（域外適用）[5]。

- EEA 域内に所在するデータ主体[6]に対する商品、またはサービスの提供（データ主体に支払が請求されるか否かを問わない）に関する処理
- EEA 域内で行われるデータ主体の行動の監視に関する処理

2. 企業が準備・検討しておくべき項目

前述の通り、GDPR が適用される「個人データ」の「処理」や「移転」を行う場合には、一定の法的要件に対応しなければ違法となってしまい、制裁金の対象となりうる。

次項では、個人データの処理と移転のそれぞれについて遵守しなければならない法的要件を解説する。

[5] EEA 域内に拠点を持たない企業は代理人を選任しなければならない可能性がある。EEA 域内に支店や駐在員事務所は置いていないが、子会社がある場合は「拠点」を持つことになり、EU 代理人の選任は不要である。EU 代理人を個人データが処理されるデータ主体が居住する加盟国のうちの一つに設置する必要がある。代理人は GDPR 遵守に関し、管理者・処理者に加えて、または管理者・処理者の代わりに一切の問題に取り組むために、管理者・処理者により委任される必要がある。

[6] 識別されたまたは識別されうる自然人のこと。

（1）個人データの処理の法的要件への対応

日本企業にとって、速やかに対応を開始する必要性の高い個人データの処理の法的要件として、対応が求められる事項と具体的に必要な取組みは以下の通りである。特に重要なのが、データマッピングによって GDPR の適用対象となる「個人データ」の「処理」と「移転」が企業グループ内のどこで行われているかを明らかにすることである。

対応が求められる事項	具体的に必要な取組み
説明責任	個人データ処理の諸原則（①適法性、公平性および透明性、②目的の限定、③データの限定、④正確性、⑤保管の限定、⑥完全性と機密性）を遵守し、遵守を実証する
遵守を実証する方法の実行	▪ GDPR 遵守への第一歩としてデータマッピング[7]を行い、企業グループ内のどこでどのような EEA 域内における個人データ（以下「EEA データ」）を何の目的で処理するかを明らかにする ▪ データ保護方針の制定・施行[8] ▪ データ保護認証メカニズムが利用可能になった場合には利用を検討 ▪ 仮名化が可能な場合には行う ▪ 処理行為の記録保持義務の履行 ▪ GDPR を遵守する処理者の使用[9] ▪ 設計・初期設定におけるデータ保護の実践 ▪ データ保護影響評価／データ保護監督当局への事前相談の実行 ▪ データ保護責任者の選任
データセキュリティに関する義務	▪ 適切なセキュリティ対策の実施[10] ▪ 監督当局（72 時間以内）およびデータ主体（不当な遅滞なく）に対する個人データ侵害の通知義務を履行するための内部手続の構築
データ主体の権利の尊重	データ主体の権利（情報権、アクセス権、訂正権、削除権（忘れられる権利）、制限権、異議権、データポータビリティの権利、自動的な個人の意思決定に関する権利）の行使への対応

[7] 本社/子会社/支店が EEA 域内に所在する個人の個人データを処理しているかどうかを網羅的にチェックすることで、企業グループ内のどの範囲で GDPR を遵守する必要があるのかを明らかにする。これをきちんと行わなければ、漏れのないように GDPR 対応を行うことは難しい。

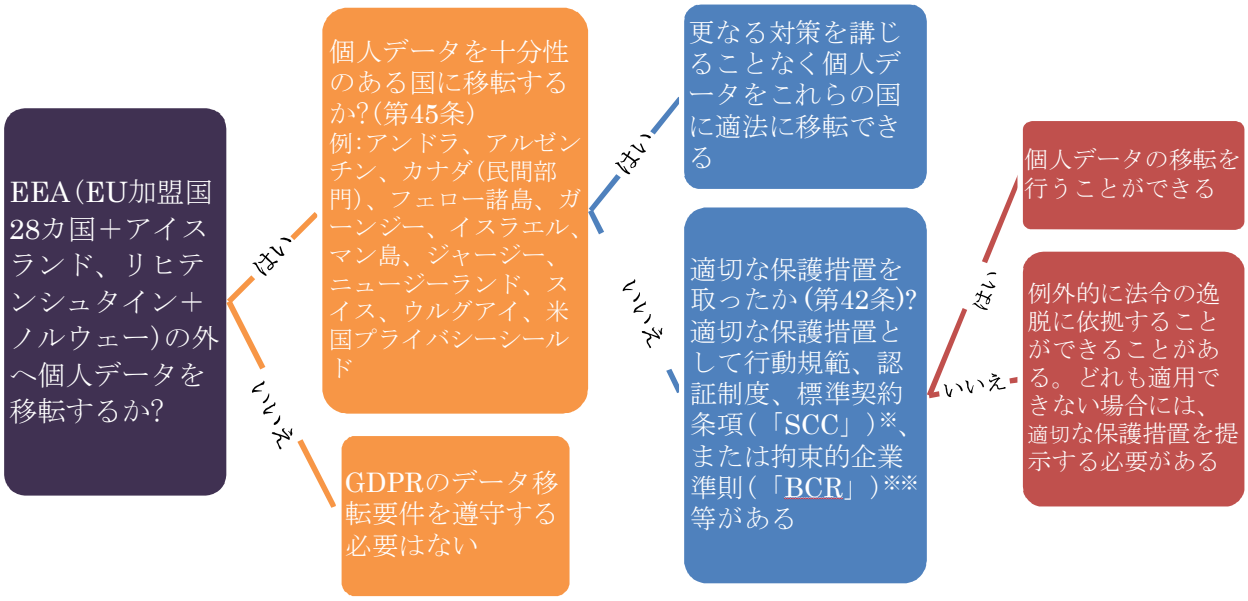
[8] 管理者は、GDPR を遵守しているだけではなく、どのように遵守しているかをデータ保護監督当局に対して説明する責任を負っている。そのため、EEA データを処理する日本企業が以下のように GDPR に対応したデータ保護方針を整備することは法的義務となったといえよう。
・EEA 域内の拠点における GDPR に対応した個人データ保護規程・プライバシーポリシーの整備
・日本本社や EEA 域外の拠点では EEA データを処理する担当者のみが遵守の必要がある GDPR に対応した EEA 個人データ保護規程・プライバシーポリシーの整備

[9] 管理者は、GDPR の要件を満たす技術的、組織的な措置の実行を十分に保障できる処理者以外は使用してはならない。例えば、EEA 域内においてクラウドサービスを使用する場合には当該サービスのプロバイダーとしての処理者が GDPR を遵守するかどうかについて日本企業はチェックを行い、場合によってはプロバイダーを切り替える必要がある。

[10] 個人データ侵害のリスクに対して適切なセキュリティレベルを確保するため、適切な技術的・組織的対策の実施の方法を検討する。特に、日本企業の EEA 域内の拠点では IT 専任の担当者が社内にいないこともあり、また IT 投資を十分に行っていない場合も見受けられ、GDPR の観点から適切な技術的・組織的対策の実施が図られているかどうかについて、信頼できる GDPR の IT 対応の専門家による最低限のチェックを各 EEA 拠点において行うべきである。

（2）個人データの移転の法的要件への対応

日本は、欧州委員会からデータ保護に関する十分性の決定を受けていないため、EEA 域内から日本への個人データの移転は原則として違法である[11]。日本企業が EEA 域内から EEA 域外への個人データを適法に移転する際には、「適切な保護措置」を講じるか、「例外的に法令の逸脱」に依拠することが必要である。



※SCC とは、欧州委員会によって決定された契約書のひな型であり、二当事者間でこのひな型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、データ移転を適法化させることができるものである。SCC は単に署名さえすれば後は保管しておけばよいという性質のものではなく、SCC 中のデータ輸出者とデータ輸入者の義務をそれぞれ履行できる体制を整えることが肝要である。当該義務の違反は制裁金の対象となる可能性がある。

※※BCR とは、EEA 域内の事業者の拠点から EEA 域外の事業者の拠点への個人データ移転に関する事業者の内部方針を定義する内部行動規範である。データ保護監督当局によって承認された BCR に事業者が従っている場合には、全世界において事業者のグループ内での個人データ移転が可能である。

[11] 2016 年 6 月 6 日にはドイツ・ハンブルグのデータ保護監督当局が、違法に米国へ従業員および顧客の個人データを移転していた米国企業 3 社に対し制裁金を科したという取り締まりの実例もあり、日本企業は現行法の下においても早急に対策を講じなければならない状況におかれている。

現状では、多くの日本企業が EEA 域内から EEA 域外へ個人データを移転するにあたり、企業グループ内での EEA データの流れや流れの可能性を踏まえ、標準契約条項（Standard Contractual Clause: SCC）を網羅的に締結するという対応を開始している。

法的根拠		概要および現状況
適切な保護措置	SCC（標準契約条項）	多くの日本企業が指令に基づくまたは GDPR を見据えて SCC 対応を行っている。
	BCR（拘束的企業準則）	少なくとも 2 社の日本企業（名称が公表されているのは、株式会社インターネットイニシアティブ（IIJ／実際の申請者は IIJ Europe）のみ[12]）が BCR の申請を行った。BCR の承認を取得した日本企業は、2017 年 1 月 30 日時点で楽天株式会社グループがある。指令における SCC 対応よりも、BCR 対応（＋企業グループ外との関係で SCC 対応）の方が、執行リスクを減らす点でも費用対効果の点でも望ましいと思われる日本企業の数は多い。
	認証	認証制度は、日本企業が日本で取得した認証が、EU の認証制度との相互認証を得られるような場合、特に興味深い。しかしながら、現時点では何らのガイダンスも出されていない。
	行動規範	行動規範を取得する活動に加わることにより、コンプライアンス関連のコストを削減することができる可能性があることから興味深い。しかしながら、現時点では何らのガイダンスも出されていない。
同意/必要性の例外		同意は非常に制限的な例外であるが、個人データを移転するために依拠することが必要な場合も依然としてある。必要性に基づいて認められる例外も法定されているが、利用可能な場合は限定的である。
プライバシー・シールド		プライバシー・シールド[13]は、EEA 域内から米国へのデータ移転のみに利用可能である。プライバシー・シールドの有効性については現在、EU 裁判所で争われている。
十分性認定の取得		欧州委員会は 2017 年 1 月 10 日、2017 年に日本との十分性認定の議論を積極的に行うことを発表した。日本の十分性認定がなされるのか、なされるとして、いつ・どのタイミングでなされるのかは明らかではない。また、仮に日本が十分性ありと認定されたとしても、日本企業による EEA 域内から日本以外の第三国への個人データの移転（例えば、フランスからシンガポールへのデータ移転）は、別途適切な保護措置等を講じる必要があり、加えて上記個人データの処理の法的要件については、すべて別途対応しなければならない点に注意が必要である。

[12] http://www.iij.ad.jp/news/pressrelease/2016/1026.html

[13] EEA 域内から一定の条件の下に米国企業への個人データの移転を認める欧州委員会による決定

3. EEA域内における企業の取組み

日本企業・団体は、2018 年 5 月の GDPR 適用開始のタイミングに間に合うよう、GDPR へのコンプライアンス対応を既に開始させている。2 章（1）で説明した「個人データの処理の法的要件への対応」については、データ保護監督当局の代表者等によって構成される第 29 条作業部会による個別のガイドラインの公表を待って対応を開始する方が効率的であるため、まずは 2 章（2）「個人データの移転の法的要件への対応」を先に行う企業・団体が多いといえよう。

GDPR への対応は、企業・団体における法務部のみならず、総務部、IT・システム部、人事部、コンプライアンス部等、様々な部署が関与することになる。したがって、日本企業・団体の場合には、EEA 域内の子会社や駐在員事務所で GDPR 対応がなされる場合にも、日本企業の本社・団体の本部によって予算管理・プロジェクトチームの組成がなされる場合が多い。

EEA 域内で GDPR への対応の必要性に気付いた場合にまず行うべきことは、個別の対応ではなく、全社的・全団体的な対応である。例えば、企業においてデータ保護方針の制定・施行は、EEA 域内の子会社・駐在員事務所のみで行うことには無理があり、本社が企業グループ全体としての EEA データに関するデータ保護方針の制定・施行から始めなければならない。また、個人データの移転の法的要件への対応として、データ主体の同意を個別に取得して対応すればよいという場当たり的な対応も避ける必要がある。GDPR においては、個人データの移転は原則として禁止されており、企業グループ全体での個人データの移転を適法化しなければ、制裁金のリスクが残ってしまう。データマッピングを行った上で、企業グループの中で手当てをしなければならない GDPR の適用対象になる個人データの移転がどれだけあるのかを明らかにし、包括的な対応を行っていく必要がある。包括的な対応として有効なのは、SCC または BCR による対応である。

4. 結語

GDPR への対応は、制裁金のリスクが大きいことも相まって、EEA 域内でビジネス・活動を行う企業・団体にとっての経営上・事業上の課題である。確かに GDPR への対応は一大プロジェクトであるが、適用開始前に対応を完了させることは、将来の巨額の制裁金のリスクを低減させる上で重要な戦略的投資といえよう。

［2017 年 1 月 31 日発行］

【著者紹介】
杉本　武重　（すぎもと たけしげ）
ウィルマーヘイル法律事務所ブリュッセルオフィス・シニアアソシエイト・弁護士
慶応義塾大学法学部法律学科（法学士/2004 年）、最高裁判所司法研修所司法習得（59 期）、
シカゴ大学ロースクール法学修士（2012 年）、オックスフォード大学法学部法学修士（2013 年）。

2006年10月に長島・大野・常松法律事務所へ入所。2013年8月に同事務所を退所し、同月ウィルマーヘイル法律事務所へ入所。ブリュッセルオフィス・アソシエイトを経て現職。主な専門分野は、EU一般データ保護規則を含むEUの個人データ保護法、EUのサイバーセキュリティ法、EUカルテル規制・EU企業結合規制を含むEU競争法全般及び腐敗行為防止コンプライアンス。

