「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）

2017 年 8 月

日本貿易振興機構（ジェトロ）
ブリュッセル事務所
海外調査部　欧州ロシア CIS 課

2018 年 5 月 25 日から適用が開始される EU「一般データ保護規則（General Data Protection Regulation: GDPR）」は、欧州経済領域（European Economic Area：EEA 、EU 加盟国 28 ヵ国、ノルウェー、アイスランド、リヒテンシュタイン）と個人データをやり取りする日本のほとんどの企業や機関・団体が適用対象となり、同規則への違反行為には高額の制裁金が科されるリスクもある。

ジェトロは 2016 年 11 月に同規則に関する「実務ハンドブック（入門編）」[1]を公開し、GDPR の基本的な構造と、基礎的な社内外の対応について概説した。本レポートは入門編に続く「実践編」として、GDPR に詳しいギブソン・ダン・クラッチャー法律事務所ブリュッセルオフィスの杉本武重弁護士（日本国、ブリュッセル（準会員）、米国ニューヨーク州）に作成を委託したものだ。

標準契約条項（Standard Contractual Clauses: SCC）と拘束的企業準則（Binding Corporate Rules: BCR）を中心に、企業で実際に GDPR へのコンプライアンス対応について 2017 年 7 月 31 日現在の情報を基に概説した。なお、GDPR の基本的な用語や仕組みについては、入門編を参照されたい。

[1] https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html

目 次

1. GDPR へのコンプライアンス対応を進める前に

Q1：EU 一般データ保護規則（General Data Protection Regulation: GDPR）への対応に向けて準備予算を確保するため、社内における問題の本質とは何か、今後、具体的に何をすべきか、社内で理解を得るために押さえるべきポイントを知りたい。

(1) 欧州連合（European Union: **EU**）の新しい個人情報保護法である GDPR に対するコンプライアンス対応に早めに取り掛からなければ、日本企業も、EU 加盟国のデータ保護監督当局によって高額の制裁金を課せられる恐れがある。EU の個人情報保護法対応は、**日本企業の欧州向けビジネスに大きな影響を与える経営事項**であり、高い優先順位をつけて対応を行う必要がある。

(2) GDPR は 2018 年 5 月 25 日から適用開始となる。欧州経済領域（European Economic Area: **EEA**、EU 加盟国 28 ヵ国、ノルウェー、アイスランド、リヒテンシュタイン）に子会社、支店、事業所などの拠点を持っている場合および EEA 内に拠点はなくとも EEA 内の所在者に向けて物・サービスを有償または無償で提供している場合、適切なコンプライアンス対応をとらなければ、事業者または団体は、高額の制裁金を課せられることになる恐れがある。

(3) GDPR は、EEA 内における個人データの処理と EEA 内から EEA 外への個人データの移転を原則違法とする法律である。また、GDPR は、標準契約条項（Standard Contractual Clauses: **SCC**）を締結することにより、適法に EEA 内から EEA 外へ移転させた個人データの処理についても、SCC によってデータ輸入者に義務を課すことを通じて、原則違法とする法律である。したがって、EEA 内外を問わず、EEA 外で取得された個人データであっても EEA 内において処理されたことがある場合は、当該個人データを処理する場合には、適切な GDPR コンプライアンス対応をとらない限り、知らぬ間に違法行為を行っていることになる可能性がある。

(4) GDPR へのコンプライアンス対応を実行するためには、社内の様々な関係者を関与させることが必須であり、実行には社内で処理する EEA 内データの種類や量にもよるが、どんなに急いでも、数ヵ月から 1 年前後を要する。GDPR の適用開始は、2018 年 5 月 25 日に迫っており、既に十分な時間は残されていない。

(5) 社内の様々な関係者には、総務部、法務部、コンプライアンス部、IT 部、情報・システム部、セキュリティー部、人事部、事業部（データを使ったビジネスを行う企業、そうした企業を顧客に持つ会社は特に）の関係者が含まれる。

(6) 社内の様々な関係者の数が多過ぎるため、GDPR 対応を専任で行うプロジェクトチームを組成することが望ましい。GDPR 対応専任プロジェクトチームの組成が難しい場合には、経営陣が、GDPR 対応をリーダーとして行う部署を指名し、他の社内の様々な関係者は、GDPR 対応をリーダーとして行う部署の協力要請に応じることが望ましい。

(7) GDPR 対応における社内検討の結果として、IT システムの改修・構築または実行中の IT システムの改修・構築を軌道修正することが必要となり、巨額の投資が必要となる恐れもある。IT システムの改修・構築のための投資費用を機動的に確保することは容易ではないことが多いため、必要最低限の GDPR の IT 対応を、急ピッチで行うことが望ましい。

(8) GDPR 対応がうまく行く企業は、経営陣が GDPR の制裁金リスクおよび事業リスクを敏感に察知し、十分な予算と権限を GDPR 対応チームに与えた企業である。GDPR 対応の成否は、経営陣にかかっていると言っても過言ではない。

2. 標準契約条項（SCC）と拘束的企業準則（BCR）による対応

Q2：標準契約条項（Standard Contractual Clauses: SCC）の本質を知りたい。

SCC とは、現行の「EU データ保護指令」に基づき EEA 加盟国で立法された各国個人情報保護法の適用対象となる個人データを、十分なレベルの個人データの保護が確保されているとみなされない EEA 外の国へと移転する際に、当該個人データに十分な保護を提供するための法的手段である。

別の角度から説明すれば、SCC とは、欧州委員会によって決定されたデータ移転の契約書の雛形であり、EEA 内のデータ輸出者と EEA 外のデータ輸入者の二当事者間で、当該雛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、適法なデータ移転を可能とするものである。

GDPR 上では、第 93 条 2 項で定める審査手続きに従って欧州委員会によって採択される「標準データ保護条項（Standard Data Protection Clauses: **SDPC**）」が、今後どこかのタイミングで作成されることになる（第 46 条 2 項(d)）。現在の SCC は、欧州委員会が EU データ保護指令の第 26 条 4 項に基づき決定として採択したものである。この決定は GDPR の施行開始後も、必要に応じて、GDPR の 46 条 2 項に従って採択された欧州委員会の決定によって修正、差し替え又は廃止されるまで有効とされている（第 46 条 5 項）。すなわち、SDPC が新たに採択され、SCC が欧州委員会の決定によって修正、差し替えまたは廃止されるまでは、現在の SCC が GDPR 上の域外移転規制対応としても有効であるということである。

したがって、当面の間の GDPR 対応としては、SCC を使用して対策すればよいものと考える。

SCC は、単に署名をしさえすれば後は保管しておけば良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。SCC によって負うデータ輸入者の義務の違反は、欧州委員会が設定した個人データ移転の条件の違反であるとされ、制裁金賦課の対象となるおそれがある。

表 1：SCC の種別

輸出者	輸入者	状況	現在の SCC の種類
管理者	管理者	個人データが EEA 内の管理者から EEA 外の管理者へ移転される場合	2 種類の SCC がある 2001 年 SCC(EC Decision 2001/497/EC) 2004 年 SCC(EC Decision 2004/915/EC)
管理者	処理者	個人データが EEA 内の管理者から EEA 外の処理者へ移転される場合	2010 年 SCC(EC Decision 2010/87/EC)
処理者	復処理者	個人データが、まず EEA 内で管理者から処理者へ移され、その後、その処理者から EEA 外にいる復処理者へ移転される場合	作業部会は 2014 年 3 月、**処理者-復処理者 SCC 案**を提案した(WP214)。しかし、欧州委員会はこれをまだ承認していない。欧州委員会は 2017 年 1 月の政策文書の中で処理者-復処理者の SCC 案を承認する予定がある旨を公表している。

- 2001 年 SCC(EC Decision 2001/497/EC)は、データ輸出者とデータ輸入者が、いずれかの当事者による標準契約条項の違反の結果、データ主体が被った損害について連帯責任を負うことを前提としている。データ主体は、第三者受益者の条項の下で、直接訴訟を提起する権利を有する。他方、2004 年 SCC(EC Decision 2004/915/EC)では、関連する違反に対して責任のある当事者に対してのみ、データ主体が自己の権利を行使することができる内容となっている。データ輸入者に責任がある場合に、仮にデータ主体がデータ輸入者に対して訴訟を提起することが困難な場合には、当該データ主体はデータ輸出者に対して、データ輸入者に SCC の下でのデータ輸入者としての義務を確実に履行させるための合理的な努力をデータ輸出者が行わなかった点について、訴訟を提起することができる可能性がある。実務上は、2001 年 SCC ではなく、2004 年 SCC が使われることが多い。
- EEA 内から EEA 外へ個人データを移転させるデータ輸出者が SCC の作成・締結に向けたイニシアチブをとることが必要である。

- SCC に基づいて EEA 外へ移転させた個人データの処理については、データ輸入者が SCC 上のデータ輸入者の義務を負うことになる結果、GDPR を遵守して行う必要がある。
- GDPR 上、原則違法となる EEA 内から EEA 外への個人データの移転を、SCC の別紙（管理者-管理者の 2004 年 SCC については Annex B、管理者-処理者の 2010 年 SCC については Appendix 1 および 2）において網羅的にカバーすることがポイントである。
- SCC 締結に係る代理権授与を行うことにより、EEA 内のデータ輸出者一社と EEA 外のデータ輸入者一社との間で締結する SCC の効力を、その他の EEA 内のデータ輸出者およびその他の EEA 外のデータ輸入者に対し帰属させることが可能となり、その結果として数多くの SCC をレビューしサインしなければならない事態を回避することができる（入門編 P.36「SCC による複数当事者間のデータ移転方法 3」を参照）。但し、データ保護監督当局によっては、処理の目的毎に別々の SCC を作成することを要求してくることもあるため、その場合には、代理権授与の方式による場合にも、締結する SCC の契約書数は複数となる。
- SCC を包括協定（Framework Agreement）の形で作成し、一通の契約書の中で、多数当事者間の個人データの域外移転について SCC を締結するという手法もある。
- SCC の締結後、データ輸出者側で新しい種類の個人データを EEA 外に移転させるニーズが生じたかどうかをどのように適切かつ確実に把握するかという問題がある。EEA 内のデータ輸出者毎に SCC を管理することができる場合には、データ輸出者側では代理権授与や包括協定の方法を用いず、EEA 内のデータ輸出者側で、締結済みの SCC によってカバーされている個人データの域外移転可否を判断し、カバーされていない新たな域外移転が生じる場合には、既存の SCC のリバイズまたは新たな SCC の締結を行うというやり方は一案である。事業者の EEA 内の各拠点の体制によっては、こうしたやり方は必ずしもうまくゆくとはいえないと考えられるが、事業者は、一旦 SCC 対応を完了させた後に、どのように SCC 対応を継続的に行っていくかを検討しておくことが望ましい。

- 事業者グループ内における EEA 内拠点から EEA 外拠点への個人データ移転に対する対応と、EEA 内拠点から事業者グループ外の第三者である EEA 外拠点への個人データ移転に対する対応とでは、対応方法は自ずと異なる。例えば、前者の場合は、後述の拘束的企業準則（Binding Corporate Rules: BCR）による対応が可能であるのに対し、後者の場合は BCR を使用できない。また、前者の場合には、事業者グループ内の EEA 内拠点と EEA 外拠点のそれぞれにおいてデータマッピングを行ったうえで SCC のドラフトを作成することが多いのに対し、後者の場合には、事業者グループ内の EEA 内拠点に対するデータマッピングの結果に基づいて SCC のドラフトを作成しそれを事業者グループ外の EEA 外拠点に対し送付して内容の確認と締結を依頼するという手順を経ることが多い。

Q3：拘束的企業準則（Binding Corporate Rules: BCR）の本質を知りたい。

(1) BCR の意義

「拘束的企業準則（Binding Corporate Rules: **BCR**）」とは、「事業者グループまたは共同経済活動に従事する事業者グループ内で、1 ヵ国または複数の EU 域外の第 3 国の管理者または処理者に向けて個人データ移転または一連の個人データ移転のため、EU 加盟国の領域上にある管理者または処理者によって遵守される個人データ保護方針」をいう（第 4 条 20 号）。BCR は、GDPR の対象である個人データが、十分なレベルの保護が確保されているとみなされない EEA 外の国に EEA 内から移転される場合に、当該個人データに対して適切な保護を提供する法的手段である。

(2) BCR の承認の要件

BCR の承認の要件は以下の通りであり、管轄監督当局はこれらの要件を遵守する BCR を、「一貫性メカニズム」[2]に従い承認しなければならない（第 47 条 1 項）。

(a) BCR が、法的な拘束力を有し、事業者グループまたは共同経済活動に従事する事業者のグループに関連したすべてのメンバー（従業員を含む）に適用され、遵守されている。

(b) BCR が、個人データの処理に関し、データ主体に執行できる権利を明示的に与えている。

(c) BCR が、第 47 条 2 項に定められた要件（次項目参照）を満たしている。

GDPR の適用開始前は、現行の EU データ保護指令に基づく BCR の承認の要件を満たせば、BCR の承認がなされるが、GDPR の適用開始日が近づいてきたことから、EEA 加盟国のデータ保護監督当局は、既に GDPR 上の BCR の承認の要件を踏まえて、BCR 申請を行うことを推奨している。

(3) BCR の必要的記載事項

BCR は、少なくとも次に掲げる事項を明記しなくてはならない（第 47 条 2 項）。

(a) 事業者グループまたは共同経済活動に従事する事業者のグループおよび各々のメンバーの体制と連絡先詳細。

(b) 個人データの種類、処理の種類とその目的、影響を受けるデータ主体の種類、および（個人データ移転先となる）EU 域外の当該第三国もしくは複数の当該第 3 国の特定情報を含む、個人データ移転または一連の個人データ移転。

(c) 国内および国外双方における法的拘束性。

(d) 一般的なデータ保護の原則の適用。特に、目的の制限、データの最小化、保存期間の制限、データの品質、設計におけるデータ保護・初期設定におけるデータ保護、処理に関する法的根

[2] GDPR の統一的な施行を目的とする、加盟国の個人データ保護監督当局（および、必要に応じて欧州委員会）の協力の仕組み（第 63～67 条）

拠、特別な種類の個人データの処理、データセキュリティを確実にするための措置、および BCR によって拘束されない団体への再移転に関する要件。

(e) 処理に関するデータ主体の権利および当該権利の履行手段。第 22 条によるプロファイリングを含む自動的処理のみによる決定に服しない権利、管轄監督当局に不服を申し立てる権利、第 79 条により加盟国の管轄裁判所に不服を申し立てる権利、是正の権利および、適切な場合には BCR の侵害に関する補償を得る権利を含む。

(f) EEA 内に拠点のない、（データ移転に）関連するあらゆるメンバーによる BCR のあらゆる違反に対する責任を、加盟国の領域に拠点を有する管理者もしくは処理者が引き受けること。管理者または処理者は、当該メンバーが損害を生じさせた出来事に責任がないと証明する場合にのみ、全体または一部の当該責任が免除されるものとする。

(g) BCR に関する情報のデータ主体への通知方法。特に、本項(d)号、(e)号および(f)号で定める規定並びに第 13 条および第 14 条[3]で規定された情報。

(h) 第 37 条に従って選任されたあらゆるデータ保護責任者（Data Protection Officer: **DPO**）（後述）、または事業者グループもしくは共同経済活動に従事する事業者のグループ内の BCR の遵守並びにトレーニングおよび不服申立ての処理を監視する役目にあるその他の人または事業体の業務。

(i) 不服申立て手続き。

(j) BCR の遵守を確実に検証するための、事業者グループもしくは共同経済活動に従事する事業者のグループ内の仕組み。この仕組みはデータ保護監査およびデータ主体の権利保護のための是正措置を確実に行う手法を含む。この検証の結果は、(h)号で定める人または事業体、および事業者グループもしくは共同経済活動に従事する事業者のグループ内の事業管理に関する会議に通知されるものとし、要求に応じて管轄監督当局が入手できるようにしなければならない。

[3] 「データ主体から個人データを収集した場合に提供すべき情報」（第 13 条）および「データ主体以外から個人データを収集した場合に提供すべき情報」（第 14 条）

(k) BCR の規定変更を報告および記録し、当該変更を監督当局に報告する仕組み。

(l) 事業者グループもしくは共同経済活動に従事する事業者のグループのあらゆるメンバーによる確実な BCR の遵守を実現するための監督当局との協力の仕組み。特に(j)号で定める対策の検証の結果を監督当局が入手できるようにすること。

(m) BCR によって提供される保障に実質的悪影響を起こし得る、（EU 域外の）第 3 国にある事業者グループもしくは共同経済活動に従事する事業者のグループのメンバーに適用されるあらゆる法的要件を管轄監督当局へ報告する仕組み。

(n) 個人データに恒常的にまたは定期的にアクセスする人材へのデータ保護に関する適切な研修。

(4) BCR は、企業グループが処理するすべての個人データに適用されなければならないか？

第 29 条作業部会[4]は、事業者グループが EEA 外で処理したその他の個人データ（過去に EEA 内で処理されたことがないもの）は、必ずしも BCR の対象とする必要はないとしている[5]。

もっとも、BCR を使用している多国籍企業グループには、すべての処理を行う個人データを保護するための単一のグローバルポリシーまたはルールを策定することが第 29 条作業部会により強く推奨される。単一の一連のルールを有することによって、従業員が実施しやすく、データ主体が理解しやすいより簡潔かつ効果的なシステムが構築されるためと考えられる。

第 29 条作業部会は、BCR の承認取得により「事業者は、特定の法領域における所在地や法的要件に関わらず、すべてのデータ主体に対して高いレベルのプライバシー保護に向けた確固とした取り組みを事業者として行っていることを示すことができ、EEA 加盟国のデータ保護監督当局やデータ主体から、好ましい評価を受けることができるようになる。すなわち、BCR の承

[4] Article 29 Working Party、加盟各国の監督機関の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関（EDPS）の代表によって構成される。特定の問題に関して共通の解釈と分析を提供することにより、EU 加盟国のデータ保護法の解釈にある程度の調和をもたらす

[5] 第 29 条作業部会「BCR に関係する FAQ に関する作業文書」（2008 年 6 月 24 日作成、2017 年 2 月 7 日最終改訂）（WP155）

認を取得した事業者は、データ保護監督当局からは、データ主体に対して高いレベルのプライバシー保護を約束しているものと考えられることになる」としている。この表現は、第 29 条作業部会が、BCR の承認を取得した事業者は高いレベルのプライバシー保護を約束していると見なす立場にあることを明らかにしたものといえる。このことが事業者による BCR の承認取得がデータ保護監督当局による執行リスクを低く抑える効果を持つと考えられる所以の例である。実際に、データ保護監督当局の BCR 審査責任者からは、BCR の承認を取得した事業者が高いレベルのプライバシー保護を示すことができるという発言が頻繁に聞かれる。

事業者グループは、BCR において要求される第三者受益権（BCR の当事者以外の第三者であるデータ主体に保障された権利）に関する要件の適用を EEA 内から移転された個人データのみに限定し、その他の個人データについては第三者受益権に関する要件を適用せずに、事業者グループ内で個人データ保護に関する一連のルールを持つことが可能であることに留意すべきである。

(5) BCR 自体に、グループ内における個人データの処理および移転について記載する必要があるか、また、どの程度のレベルで詳細に記載する必要があるか？

第 29 条作業部会は、「BCR には、個人データ処理の主な目的およびデータ移転の種類に関する一般的な記述を含める必要がある。例えば、事業者グループの状況に応じて、BCR において、『従業員の流動性を理由として全ての事業者においてデータ移転を行い、人事データを保管および保存を目的としてドイツ、米国およびシンガポールにあるグループの主なデータセンターに送信し、さらに、グループのグローバルな報酬戦略と福利厚生制度の決定のために本社に送信する』などの説明を記載することが考えられる」とする。

ここから分かることは、BCR の申請にあたって把握する必要のある個人データの流れはある程度限定的であるということである。したがって、BCR の適用範囲を事業者グループ内の個人データの移転すべてとする前提で BCR 申請を準備する場合には、BCR 申請の準備として必要となるデータマッピングは限定的でも構わない。もっとも、実際に日本企業による BCR 申請の検

討の過程を見ると、事業者グループ内での個人データの域外移転について適切な保護措置をSCCとBCRのどちらとするかについて、入念なデータマッピングを行ったうえで決定するケースが増えている。これは、BCR承認取得にあたり、事業者グループのEEA外の拠点におけるデータ保護の程度を高めることが事業遂行上の妨げにならないか、BCRにおける監査やトレーニングの遂行が過度の負担とならないかについて不安を覚える事業者が一定数存在するという状況を反映したものである。

(6) BCRにおける立証責任の転換は実務上どのような意味を有するか？

第29条作業部会は、「データ主体が、データ主体が損害を被ったことを証明することができ、かつ当該損害がBCRの違反により発生したであろうことを示す事実を示すことができる場合、EEA外の事業者グループのメンバーは当該損害につながったBCRの違反について責任を負っていないことの、または当該違反自体が生じなかったことを証明する責任を受け入れたEEAにおける当該事業者グループのメンバーは当該違反自体が生じなかったことの立証責任を負うことになる」としている。

(7) どのデータ保護監督当局が、BCRの実施を監督する権限を有するか？

第29条作業部会は、「権限あるデータ保護監督当局は、BCRの実施を監督する権限を有する。BCRは、グループのすべてのメンバーがデータ保護監督当局と協力し、BCRに関連するすべての問題についてデータ保護監督当局の助言を遵守し、監査を受け、要求に応じて監査の結果を提供するという明確な義務を含むものでなければならない。これらの義務は、主導監督当局（EEA内において個人データの管理者または処理者の主要な拠点が位置するEEA加盟国のデータ保護監督当局）のみとの協力または対応に限定されるべきではない。ただし、主導監督当局に対してのみ（主導監督当局との合意に従って）当該変更または更新の提出が通常行われ、当該主導監督当局がBCR文書の変更または更新について、BCRに関する権限を有する他の監督当局に対して意思疎通を図る旨をBCR方針において規定することができる。」としている。

すなわち、BCR において主導監督当局に対してのみ BCR の変更または更新の提出を行うことを定めておき、当該 BCR の承認を受ければ、BCR の承認を取得した事業者は、事業者グループ内での個人データ移転の内容の変更などによる EEA 加盟国のデータ保護監督当局への対応にかかる手間を少なくすることが可能である。

(8) BCR に関するどのような更新がデータ保護監督当局に提出されるべきか、またそれはいつ行われるべきか？

第 29 条作業部会は、「いかなる BCR の更新もデータ保護監督当局に対して提出されるべきである（主導監督当局を通じて行うことも可能）。変更が BCR によって提供される保護のレベルに影響を及ぼし得る場合（例えば、データ主体の権利に不利益をもたらすこと）または BCR に重大な影響を及ぼす場合（例えば、拘束力に関する変更）は、当該変更は速やかに主導監督当局に対して連絡され、当該当局は BCR のために行われた過去の承認に影響を及ぼすか否かを判断することになる。その他の変更点に関しては、年に 1 回の意思疎通で十分である」としている。

第 29 条作業部会は、現時点では、一度承認された BCR に関する更新について、EEA 加盟国のデータ保護監督当局への通知義務は最低限度のもので良いと考えている。例えば、BCR の承認を取得した事業者が、EEA 内の拠点をグループ内にもつ事業者を買収・合併した場合であっても、EEA 加盟国のデータ保護監督当局としては、被買収対象会社・被合併対象会社が承認された BCR を遵守する体制が整っていることを確認できさえすれば良いと考えていることが窺われる。

もっとも、これは、これまで BCR の承認を取得してきた事業者の数が限られており、EEA 加盟国のデータ保護監督当局として、未だかつて承認済みの BCR の有効性を否定した事案が存在しないことから、BCR の承認を取得した事業者への信頼感が醸成されているためであるともいえる。したがって、今後、GDPR 適用開始が近づくにつれて、BCR 承認を取得する事業者の数が爆発的に増えた場合、GDPR 適用開始後の将来の一時期に、EEA 加盟国のデータ保護監督当局が「BCR 承認を取得した事業者グループが、BCR を拘束的に運用しているかどうか」に関す

る調査を行うブームが到来することが予想される。当該調査の結果如何によっては、データ保護監督当局が、BCR の承認を取得した事業者への信頼感を低下させ、それに伴い、承認済みの BCR の更新に関する通知義務を拡大することで、BCR の承認を取得した事業者への監視の目を光らせ始めるという規制当局側の事情の変化が起こることも考えられる。

Q4：事業者グループ内での個人データ移転に使用する場合、SCC と BCR のメリット・デメリットを知りたい。

SCC と BCR のメリット・デメリットは以下の通りである。

	SCC	BCR
効果	SCC によってカバーされている EEA 外への個人データ移転は適法となる。	BCR の対象となっている事業者グループ内での EEA 外への個人データ移転が適法となる。
対応を行うことによる当局による執行リスクの低減という効果の有無	無し。SCC 対応完了を行っている事実は、BCR の承認を取得した場合とは異なり、第三者に対して開示がなされないため、当局側は調査を行ってみなければ、事業者が個人データの域外移転規制対応を完了しているかわからないという姿勢で調査を行ってくる可能性が高い。	有り。BCR 承認を取得したという事実は、欧州委員会のウェブサイトで開示され、EEA のデータ保護監督当局によって知られることとなる。 なお、BCR 承認の取得済み事業者名について、2017 年 8 月 11 日の日付の入ったリストの形式で欧州委員会のウェブサイトにおいて開示されている。
対応にかかる費用・時間・人的コストの多寡	SCC による EEA 外への個人データ移転についてデータ保護監督当局への事前通知・事前承認申請手続き[6]をとる場合：コスト高（なお、データ保護監督当局に対する SCC による個人データの域外移転の事前通知・事前承認申請については、現行の EU データ保護指令に基づいて立法された EEA 加盟国法に基づく制度であるため、2018 年 5 月 24 日をもって廃止され、それ以降の対応は不要になる見込みである。） 当該申請手続きを取らない場合：コスト中	コスト高。BCR 対応は、BCR 申請準備開始から、当局との交渉を経て、当局からの BCR 承認取得、承認を受けた BCR の実行まで、約 15～24 カ月はかかる。BCR 対応に要する期間は、当局側の審査のリソースの充実度によって左右される部分が大きくなっているといえる。

[6] ジェトロ調査レポート「「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）」P.34 を参照

	当該申請手続きを取らない場合であっても、SCC 対応完了後に発生する新たな種類・目的・データ主体に関する個人データの EEA 外移転を行う場合については SCC 対応を追加で行う必要があるため、コスト高	
対応完了後に発生する新しい種類・目的・データ主体の個人データの EEA 外移転に対応できるか?（網羅的な対応の可能性）	当初の SCC 対応ではカバーできていないため、新たに SCC 対応を追加で行う必要がある。 SCC 対応を追加で行う必要性に気が付くためには、データ保護担当部署以外の部署（特に、事業部）において SCC の対象範囲から外れることとなる新たな種類の EEA 外への個人データ移転についてデータ保護担当部署に対し、報告してもらう必要があるが、実際には容易ではない。	対応できる。BCR において予め移転し得る全ての種類の個人データを対象としておけばよい。但し、BCR の適用対象とする個人データの移転の範囲を限定する場合にはこの限りではない。また BCR 作成時点で想定されなかった種類、目的の個人データの EEA 外移転の場合はこの限りではない。
対応完了後の M&A によって企業グループ内に迎える被買収企業グループからの/または当該被買収企業グループへの個人データの EEA 外移転に対応できるか?	対応できないため、追加で SCC 対応を行う必要がある。	BCR の改訂と BCR 上の主導監督当局への報告に関する規定に従って対応を行えばよい。

Q5：BCR による対応を目指す場合、SCC による対応を一切行わなくてよくなるのか?

後記の通り、2017 年 7 月現在、EEA 加盟国のデータ保護監督当局による BCR 審査が難航し始めているという現状を踏まえると、BCR による対応を行うのみならず、BCR 申請準備とともに SCC 作成と締結準備を並行して行うことが安全な対応である（もちろん、コスト効率との関係で、多少のリスクを取り、BCR 申請準備のみを進めるという選択肢もある）。

また、BCR による対応は、事業者グループ内での個人データ移転のみを対象としたものとなることが通常であるため、事業者グループ内の EEA 拠点から事業者グループ外の EEA 外の拠点への個人データの域外移転については、別途 SCC による対応を行う必要がある。

EEA 加盟国のデータ保護監督当局による BCR 審査が難航し始めているという現状に関する説明は以下の通りである。

2017 年 5 月下旬、英国のデータ保護監督当局である情報コミッショナーオフィス（Information Commissioner's Office: **ICO**）は、欧州議会における GDPR 採択後、大量の BCR 申請が殺到したため、将来的な BCR 申請の新規受理の停止の可能性について言及し始めた。より具体的には、ICO では BCR 審査の標準スケジュールから大幅な遅れが生じたことにより BCR 審査責任者が交代となり、新しい BCR 審査に関するグループマネージャーが選任されると同時に、BCR 審査チームに新しいメンバーが配置されることになった。にもかかわらず、ICO のトップである英国の情報コミッショナーは、こうした BCR 審査チームへの大幅なてこ入れとともに、将来的な BCR 申請の新規受理の停止の可能性に言及し始めた。これは、英国の ICO の読みとして、今後も ICO への BCR の新規申請件数が増大し続け、今回の BCR 審査チームの拡大によっても、BCR の審査スケジュールを正常化することが難しいというものを、反映したものではないかと考える。

また、BCR 審査について遅れが生じている状況は、英国の ICO においてのみではない。オランダのデータ保護監督当局（Data Protection Authority：DPA）においても、2017 年 6 月初めの時点で 21 件の申請済みの BCR があり、BCR 審査に多忙を極めている状況にある。これは、ドイツのデュッセルドルフを州都とするノルトライン・ヴェストファーレン州のデータ保護監督当局（主導監督当局[7]）の BCR 審査責任者が、BCR の審査において共同審査を行うデータ保護監

[7] EEA 内において個人データの管理者または処理者の主要な拠点が位置する EEA 加盟国のデータ保護監督当局。BCR 審査における副主導監督当局とは、主導監督当局が BCR を承認した後に、さらに BCR 審査を行う二つの監督当局のことを意味し、監督当局側で指定される。GDPR 適用開始後は、副主導監督当局による BCR 審査の代わりに、欧州データ保護会議（European Data Protection Board: EDPB）という第 29 条作業部会の後継の会議体による意見が出されることになる。

督当局（副主導監督当局）による審査の遅れにより、BCR 審査に時間がかかることが予想されるというコメントを 2017 年 7 月の時点で行っていることからも確認されている。すなわち、BCR 申請を巡る EEA のデータ保護監督当局の状況は、2017 年初頭から大きく変化してきている。

仮に、英国の ICO が新規の BCR 申請受理を停止することを決定し、当該決定に関するニュースが他の EEA 加盟国のデータ保護監督当局に伝わり、かつ他の EEA のデータ保護監督当局の中で処理能力を大きく超える数の BCR 申請が殺到している場合、英国 ICO と同様に新規の BCR 申請受理の停止を宣言する可能性がある。

主要な EEA 加盟国のデータ保護監督当局において、新規の BCR 申請受理が停止された場合、BCR 申請を検討している事業者側にも大きな混乱が生じることになる。

仮に、EEA 加盟国のデータ保護監督当局が、事業者側から多くの抗議を受けた場合、批判の矛先が当局側に集中することを避けるため、事業者に対して、BCR を使わなくとも SCC による個人データの域外移転対応が可能であることを強調することが予想される。

当局が BCR 申請を行おうとしてできなかった事業者に対し SCC の使用の状況を確認した場合、2016 年 6 月に Adobe、ユニリーバなどの 3 社の米国企業に対して、SCC を使用せずに個人データを EEA から米国へ移転させていたことに対して、ドイツ・ハンブルグのデータ保護監督当局が制裁金を課したことを踏まえた対応が行われる恐れがある。すなわち、SCC などの適切な保護措置を取らず、かつデータ主体による同意などの法令上の例外に依拠することなく個人データの EEA 内から EEA 外への域外移転を行っており、かつ SCC などの適切な保護措置を取る計画を持っていないことが発覚した企業に対しては、データ移転規制違反に基づき制裁金を課す流れが加速する恐れがある。

したがって、現状において英国をはじめとする EEA 加盟国において BCR 申請を検討する事業者は、英国 ICO が BCR 申請の新規受理を停止するという最悪の事態に至ったとしても万全な備え、すなわち、BCR 申請と並行して事業者グループ内での個人データの域外移転に関する SCC の締結手続きも準備を進めるという備えを行う選択肢を検討するべきである。

こうすることによって、万が一、英国 ICO または今後処理能力の限界を迎える可能性のある他の EEA 加盟国のデータ保護監督当局が BCR 審査に長期間を要し、その間に GDPR が適用開始となったとしても、あるいは英国 ICO が BCR 申請の新規受理を停止するという最悪の事態に至ったとしても、個人データの域外移転規制への違反を理由として、事業者グループが、EEA 加盟国のデータ保護監督当局によって GDPR 違反の制裁金を課せられる事態を未然に防ぐことにつながる。また、仮に、英国 ICO によって事業者グループの BCR 申請が受理された場合、BCR 審査に多少時間がかかったとしても、事業者グループは GDPR の執行が本格化する頃までには BCR 承認を取得することができ、中期的に、GDPR の執行リスクを最小化することもできる。

Q6：SCC と BCR の対応準備のスケジュール・イメージを知りたい。どの程度の日程で準備を進めるべきか。

SCC と BCR の対応準備のスケジュール・イメージは以下の通りである。なお、以下 S5「データ保護監督当局に対する SCC による個人データの域外移転の事前通知・事前承認申請」については、現行の EU データ保護指令に基づいて立法された EEA 加盟国法に基づく制度であるため、2018 年 5 月 24 日をもって廃止され、それ以降の対応は不要になる見込みである。なお、現行の EU データ保護指令に基づいて立法された EEA 加盟国法においては個人データの処理行為の当局への登録義務という制度が存在する国が多く、これらの国で SCC に関する事前通知・事前承認申請を行う場合には、この処理行為の当局への登録手続を先立って行うのが通常である。この処理行為の当局への登録手続についても 2018 年 5 月 24 日をもって廃止され、それ以降は当局への登録に代わり、事業者において処理行為のログを残しておくという GDPR 上の義務へと変更となるため、SCC 対応の一部として処理行為の当局への登録手続を行う必要はなくなることになる。

データ移転規制対応	スケジュール目安	SCC のみによる対応 （S1-S6）	BCR による対応 （S1-S6 が SCC による対応。 B1-B6 が BCR による対応）
事業者グループ内での SCC 対応	1～3 ヵ月目	**S1: データマッピング：データフローの特定**（SCC による対応におけるデータマッピングは、現状および近い将来における事業者グループの EEA 拠点から EEA 外への個人データ移転を網羅的に把握する必要があることから、3 カ月ほどデータマッピングに要することも珍しくはない。） **S2: POA（代理権授与書）（データ輸出者側、データ輸入者側それぞれ）の作成**。包括契約（Framework Agreement）による対応の場合には、POA は不要なこともある。	**S1: データマッピング：データフローの特定** **S2: POA（代理権授与書）（データ輸出者側、データ輸入者側それぞれ）の作成**。包括契約（Framework Agreement）による対応の場合には、POA は不要なこともある。 **B1: BCR のスコープおよび主導監督当局の特定** **B2: BCR のドラフトおよび BCR 申請書のドラフトの開始**（並行して BCR のドラフトに記載する BCR 実行のための社内体制構築の開始）
	2～5 ヵ月目	**S3: SCC ドラフト（管理者-管理者の SCC、管理者-処理者の SCC）の作成** **S4: SCC ドラフトの加盟国法に基づくレビュー** **S5: データ保護監督当局に対する SCC による個人データの域外移転の事前通知・事前承認申請**（データ輸出を行う国によっては、当局対応が不要な場合あり）、事業者グループの EEA 拠点に Works Council があれば Works Council 対応 **S6: 代理権授与によって SCC を締結する方式、または包括契約方式の選択**※	**B3: BCR 申請、主導監督当局から BCR ドラフトへコメントがあり次第、コメントを踏まえた返答を繰り返し行う** **S3: SCC ドラフト（管理者-管理者、管理者-処理者の SCC）の作成** **S4: SCC ドラフトの加盟国法に基づくレビュー** **S5: データ保護監督当局に対する SCC による個人データの域外移転の事前通知・事前承認申請**（データ輸出を行う国によっては、当局対応が不要な場合あり）、事業者グループの EEA 拠点に Works Council があれば Works Council 対応 **S6: 代理権授与によって SCC を締結する方式、または包括契約方式の選択**
	6～10 ヵ月目	**（S5）** **（S6）**	**（B3）** **（S5）** **（S6）** **B4: 主導監督当局による BCR 審査の終了** **B5: 二つの副主導監督当局による共同レビューの開始**（GDPR 適用開始前の BCR 申請について、GDPR 適用開始後に二つのサブ主導監督当局による共同レビューが必要となるかは未定）

	11～15ヵ月目		**(B4)** **(B5)** **B6: 相互認証手続きの確認および様々な地域当局への BCR の申告**（GDPR 適用開始前の BCR 申請について、GDPR 適用開始後に相互認証手続きの履践が必要となるかは未定）
	16～21ヵ月目		**B7: BCR 利用**
事業者グループ外	1～3ヵ月目	**S1: データマッピング：データフローの特定** **S2: POA（代理権授与書）（データ輸出者側のみ）の作成。**包括契約（Framework Agreement）による対応の場合には、POA は不要な場合もある。	
	2～5ヵ月目	**S3: SCC ドラフト（管理者-管理者、管理者-処理者の SCC）の作成** **S4: SCC ドラフトの加盟国法に基づくレビュー** **S5: データ保護監督当局に対する SCC による個人データの域外移転の事前通知・事前承認申請**（データ輸出を行う国によっては、当局対応が不要な場合あり）、事業者グループの EEA 拠点に Works Council があれば Works Council 対応 **S6: 代理権授与によって SCC を締結する方式、または包括契約方式**	
	6～10ヵ月目	**(S5)(S6)**	

※代理権授与によって SCC を締結する方式:

事業者グループの EEA 統括拠点（データ輸出者）と事業者グループ本社（データ輸入者）との間で管理者-管理者の SCC および/または管理者-処理者の SCC を締結する。

包括契約方式:

事業者グループの EEA 拠点と EEA 外拠点との間で包括契約（管理者-管理者の SCC および/または管理者-処理者の SCC を締結する。

3. データ保護責任者（DPO）の選任

Q7：GDPR の人事的な影響は何か？データ保護責任者（Data Protection Officer: DPO）の選任など人員配置上の課題を知りたい。

BCR を実施するために DPO を選任することは義務ではない。管理者および処理者は、次のいずれかの要件を満たす場合には DPO の選任義務がある（第 37 条 1 項、4 項）。

(1) 処理が公的機関または団体によって行われる場合（但し、司法権に基づく裁判所の行為を除く）

(2) 管理者または処理者の中心的業務が、その性質、適用範囲および/または目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする作業である場合

(3) 管理者または処理者の中心的業務が、第 9 条で言及された特別カテゴリーの個人データまたは第 10 条で定める有罪判決および犯罪に関する個人データを大規模に処理する場合

(4) EU または加盟国の法律(例：ドイツ)で DPO の選任が義務付けられている場合

- 2017 年 7 月 5 日、GDPR 施行のための新ドイツ連邦データ保護法が成立した。
- データ保護責任者の選任に関して、法案は現在のドイツデータ保護法の規定を維持しており、個人データの自動的処理に関して少なくとも 10 名の従業員を雇用する企業は、DPO を選任する義務を負う。GDPR では、例外的な場合においてのみ、企業に選任義務が課されている。
- 管理者および処理者は、GDPR 第 35 条に基づくデータ保護影響評価が必要な処理を行う場合、DPO を選任しなければならない。これは個人データが商業上のデータ移転またはマーケティングもしくは市場調査の目的で行われる場合にも当てはまる。

- このドイツ法上の DPO の選任義務は、GDPR 第 37 条 4 項[8]により GDPR 上の DPO の選任義務があることにつながる。

DPO については、GDPR 上、管理者・処理者からの独立性と強い地位・権限を保証されているため、日本企業としては、日本本社に DPO を選任するのか、それとも EEA 内の拠点に DPO を選任するのか、難しい判断を迫られる場合が多くなっている。これについては様々な考え方がありうるが、日本企業の中には GDPR の対応プロジェクトを日本本社主導で進めているケースは数多く見られるため、特に GDPR 適用開始直後については、EEA 加盟国のデータ保護監督当局や EEA 内のデータ主体への容易なアクセスと同時に、事業者内での高いデータ保護を実現させるためには、日本国内に DPO を設置することが合理的な場合が多い（すなわち、DPO の適任者が EEA 内拠点ではなく日本国内にいる）のではないかと考えられる。また、EEA 内拠点のマンパワーの問題等で日本国内に DPO を設置せざるを得ない企業も少なくないと考えられるが、こうした場合には、DPO が EEA 加盟国のデータ保護監督当局や EEA 内のデータ主体に現地語でタイムリー且つ容易にアクセスするため、日本企業の EEA 内拠点に、DPO チームの一員として DPO のサポートメンバーを配置することが考えられる。

Q8：DPO は他の業務との兼務は可能か。経営者自身が DPO になることは可能か。その課題は何か。

GDPR の第 38 条 6 項では DPO が「その他の作業および義務を遂行すること」が認められている。しかし、組織が「そのような作業および義務が利益相反をもたらさないこと」を保証することが義務付けられている。

[8] 同条文は、EU 法または加盟国法により定められている場合に、DPO の選任を義務付けている。

利益相反がないことは独立性を持って行動するという要件に密接に関連している。DPO は他の機能を持つことは認められているが、DPO は他の業務および義務によって利益相反が生じないという条件でのみ、これらの業務などを担当することができる。これは特に、DPO が組織の中で個人データの処理の目的および手段を決定するような地位に就けないことを意味している。これは、各組織の特定の組織構造により、ケースバイケースで検討されなければならない。

大体の目安として、相反する地位には、経営陣(例えば、最高経営責任者、最高執行責任者、最高財務責任者、最高医療責任者、マーケティング部門長、人事部門長または IT 部門長など)が含まれるがその他組織構造の中でのより低い役割であってもそのような地位や役割が処理の目的や手段を決定することにつながる場合も含まれる[9]。

したがって、経営者自身が、DPO を務めることは禁止されており、許されない。

[9] 第 29 条作業部会「DPO に関するガイドライン」（2016 年 12 月 13 日作成；2017 年 4 月改訂）。

4. その他（関連政策動向の影響など）

Q9：EU と域外の第三国政府間での「十分性認定」を通じて、GDPR 対応の問題は解決しないのか。どのような前提・条件が必要となるのか。

解決しない。欧州委員会が、日本の個人データ保護の十分性認定に関する決定を行った場合、EEA 内から日本への個人データの移転のみが適法となるにすぎない。本レポート執筆時点（2017 年 7 月）では、欧州委員会が日本の十分性認定を決定することになった場合の当該十分性決定の内容の詳細は決まっていないが、少なくとも以下の点において、欧州でビジネスを行う日本企業は GDPR 対応を行う必要があるものと考える。

第一に、欧州委員会による十分性認定の決定は、欧州においてビジネスを行う日本企業が EEA 内で行う個人データの処理との関係で GDPR 上負うことになる諸義務には影響を与えない。すなわち、EEA 内での個人データの処理に伴って生じる GDPR 上の諸義務へのコンプライアンス対応が必要となる。

第二に、多くの日本企業は、アジア、北米、南米、オセアニア、アフリカを含め EEA 外の世界各国でビジネスを行っており、EEA から日本以外の他の地域への個人データ移転は日常的に行われている。そのため、多くの場合、EEA から日本以外の他の地域への個人データ移転について SCC や BCR といった適切な保護措置を提供する必要がある。

第三に、EEA データを日本へ移転させた後の、日本から第三国への個人データの再移転については GDPR が適用されるという立場を、EEA 加盟国のデータ保護監督当局が取る恐れがある。この点について、欧州委員会が、日本に関する十分性認定の決定を行う際に、EEA データの日本から第三国への再移転に対する GDPR の適用の有無について欧州委員会の立場を明示しない場合に、特に問題となり得ると考える。

したがって、日本が欧州委員会から十分性認定という決定を受けた場合、当該決定自体は日本国と日本企業にとって喜ばしいニュースであるが、日本企業が GDPR のコンプライアンス対応をとる必要性は依然として変わらないのが現実である。

もっとも、日本が十分性認定の決定を受けることにより、EEA 加盟国のデータ保護監督当局が、十分性認定を受けた日本という国の企業が、高いレベルのデータ保護を備えていると期待し、その結果、日本企業を GDPR の執行の対象として狙い撃ちしないという状況が生じることが期待される。

ただし、GDPR 施行後まもない時期に、幾つかの日本企業が GDPR 違反で制裁金を課せられる事態となった場合には、その後に日本企業が GDPR 執行の対象として狙い撃ちになる可能性は十分に考えられる。

Q10：2018 年 5 月以降、厳罰を伴う GDPR の運用が始まった場合、EU はどのような手法で、各企業の法令遵守状況を調査・摘発しようとするのか。

EEA 加盟国のデータ保護監督当局は、データ主体からの苦情申立て、事業者への GDPR の遵守状況に関する質問状の送付、具体的な嫌疑に基づく事業者への立入検査によって GDPR 違反に関する調査を行い、GDPR 違反を摘発しようとすることが考えられる。EEA 加盟国のデータ保護監督当局が管轄権を持つのは、あくまでも EEA 内に限られるため、GDPR に基づいて事業者への立入検査が行われる可能性があるのは現時点では EEA 内の拠点のみであると考えられる。

もっとも、EEA 加盟国のデータ保護監督当局は、事業者に対し、EEA 外を含む事業者グループとしての GDPR の遵守状況に関する質問状を送付してくることが予想され、その限度では、EEA 内のデータ保護監督当局が管轄を持たない EEA 外における GDPR の遵守状況、たとえば、SCC を締結した場合のデータ輸入者の義務や BCR の遵守状況を調査することが可能である。質

問状を受け取った事業者は、正しく回答することが義務付けられるため、質問状への回答を端緒として、当該事業者の EEA 内の拠点に対する立入検査が行われるおそれもある。

なお、中長期的には、EEA 加盟国のデータ保護監督当局が、EEA 外の他国のデータ保護監督当局との間で、データ保護法違反案件に関する国際的な調査協力の枠組みを強化していくことも十分に考えられる。

Q11：EU 離脱が想定される英国の GDPR 対応はどのように進めるべきか？今後の動向を含めて知りたい。

英国は EU 離脱後も GDPR を英国の国内法としてのデータ保護法として施行するという立場を取っている[10]。英国の EU 離脱（ブレグジット）後には、英国は欧州委員会によるデータ保護に関する十分性認定の決定を受けない限り、EEA から英国への個人データ移転は、原則として禁止されることが予想される。今後の欧州委員会と英国との EU 離脱交渉の経過によっては、英国がブレグジット完了後も GDPR を英国の国内法としてのデータ保護法としてそのまま継続して施行する場合に、例外的な取り扱いとして、欧州委員会による十分性認定の決定が（EU 離脱と

[10]英国政府（英国文化・メディア・スポーツ省）は 2017 年 8 月 7 日、現在の 1998 年英国データ保護法（DPA）に代わる、データ保護法案の意図に関する声明（ステートメント・オブ・インテント）を発表した。当該声明に記載されている法案には、ブレグジットが英国と他のヨーロッパ諸国との間のデータフローに及ぼす影響について懸念する事業者を安心させる意図がある。この法案は、EU から離脱する英国の移行をデータ保護の観点から可能な限り円滑にし、ビジネスおよび法執行のデータフローが、「英国が EU を離脱した後も中断されない」ことを確保するために、EU における GDPR および DPLED（Data Protection Law Enforcement Directive：データ保護法執行指令）から導かれる新しい 2 つの法を完全に実施するように設計されている。これは、ブレグジット後に欧州委から十分性の認定を受けることを英国が希望するという明確な声明ではないが、この法案は、個人の権利強化から管理者の説明責任の拡大に至るまで、GDPR に見られるすべての重要な側面を厳密に反映しており、英国が十分性の認定を受ける可能性が依然として明確に存在するといえる。さらに、当該声明は、法令上の例外となる GDPR 中の特定の項目に関して、英国がどのように裁量権を行使するかに関する情報を提供する。全般的に、当該声明は、GDPR および DPLED についても遵守しつつ、1998 年英国データ保護法の下で適法である処理がこの法案においても適法であることを確保するように設計されていると考えられる。データ保護法案の条文はまだ公表されておらず、英国で立法化されるまである程度の時間を要すると考えられる。

同時というタイミングを含め）早期になされる可能性はある。ただ、現時点では欧州委員会によるこの点に関する取り扱いは何も決まっていない。

企業としては、英国においても GDPR 対応を行っておくことが賢明である。なお、英国の EU 離脱後に英国が欧州委員会の十分性認定の決定を早期に受けられない場合、EEA から英国への個人データ移転について適切な保護措置を取ること、すなわち SCC や BCR を使用することが必要となる可能性はあるが、その場合には、EEA 加盟国のデータ保護監督当局から、少なくとも数ヵ月程度の移行期間が与えられ、その間にコンプライアンス対応を取ればよいことになるものと考える。2015 年 10 月に欧州委員会による米国のセーフハーバー決定が欧州連合司法裁判所において無効と判断された際、第 29 条作業部会が 2016 年 1 月末まで SCC や BCR による域外データ移転規制への対応を猶予した例もある。

以上

レポートをご覧いただいた後、アンケート(所要時間:約 1 分)にご協力ください。

https://www.jetro.go.jp/form5/pub/ora2/20170058

「EU 一般データ保護規則(GDPR)」

に関わる実務ハンドブック(実践編)

作成者　日本貿易振興機構(ジェトロ)

海外調査部 欧州ロシア CIS 課

〒107-6006　東京都港区赤坂 1- 12-32

Tel.03-3582-5569

2017.8