寄稿

SCC・BCRによる対応のポイント

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　弁護士　　杉本　武重

本稿ではGDPR対応における標準契約条項（SCC）と拘束的企業準則（BCR）による対応のポイントについて概説する。

標準契約条項（SCC）による対応

SCCとは、欧州委員会（以下、欧州委）によって決定されたデータ移転の契約書を締結するという法的手段である。EUを含む欧州経済領域（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、SCCのひな型を使い当該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だ。

SCCは、単に署名をし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によるデータ輸出者とデータ輸入者の契約義務をそれぞれ履行できる体制を整えることが肝要だ。SCCによって負うデータ輸入者の義務違反は、欧州委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恐れがある。

SCC対応では、事業者グループ内のEEA内の拠点からグループ内外を問わずEEA外の拠点への個人データの移転について、関連するデータ主体、データ移転の目的およびデータの種類を、当該契約書の別紙で網羅的にカバーすることが重要だ。そのためには、現状評価（データマッピング）を入念に行うことが肝要である。入念なデータマッピングは、①データ移転に関する質問票（和英）の作成、②質問票回答のための社内関係者への説明・周知（EEA内・EEA外拠点ともに）、③質問票送付・回答準備（最低2週間）、④質問票回収・分析、⑤EEA拠点におけるインタビュー（セールス、マーケティング、人事、会計など）によって構成され、約2カ月から3カ月かかる。各企業において行っているビジネスもそれに伴う個人データの流れもさまざまだ。⑤のインタビューを行うことにより、質問票のやり取りでは明らかにならない個人データの流れやGDPR上、高リスクなデータ処理の存在が明らかになることが多い。

SCCの締結スキームについては、実際に使用されているものとしては「代理権授与方式」と「包括協定方式」の二つが挙げられる。

代理権授与方式は、EEA内のデータ輸出者1社とEEA外のデータ輸入者1社との間で締結するSCCの効力を、代理権授与を行ったデータ輸出者・輸入者に帰属させることで、締結するSCCの数を減らし、SCCの管理事務の煩雑さを減少させることができる。

包括協定方式は、SCCを多数当事者間の枠組み協定の中に組み込み、多数当事者の立場（管理者・処理者、EEA内・EEA外）をグルーピングして、一通の契約書の中で複数当事者間のSCCを締結する方法である。

拘束的企業準則（BCR）による対応

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カ国または複数のEEA外の第三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、EEA内に所在する管理者または処理者によって順守される個人データ保護方針」をいう。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見なされない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。

第29条作業部会（本誌p.53の注1を参照）は、「事業者は、特定の法領域における所在地や法的要件にかかわらず、全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が高いレベルのプライバシー保護を約束し

表　標準的契約条項（SCC）と拘束的企業準則（BCR）の比較

	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、本原稿執筆時点では、2016年12月以降の BCR 承認の取得済み事業者名の開示が欧州委員会のウェブサイトにおいてなされていない状況が続いている（データ保護監督当局において BCR の審査に遅れが生じていることが一因と考えられる）。もっとも、データ保護監督当局においては、BCR 承認取得済みの事業者リストが更新されていることが確認されており、当局側ではどの事業者が BCR の承認を取得したかに関する最新の状況を把握していると考えられる
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・事前承認申請手続をとる場合：【コスト高】 当該申請手続きを取らない場合：【コスト中】 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（SCC 対応を追加で行う必要があるため）：【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カ月から約24カ月はかかる：【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 においてあらかじ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。ただし、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

注：項目背景の色の濃度が濃いほど、注意が必要
資料：EU 一般データ保護規則（GDPR）を基に作成

ている、と見なすことを明らかにしたものといえる。これが、事業者が BCR の承認を取得することで、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ゆえんの一つである。実際に、データ保護監督当局の BCR 審査責任者からは、BCR の承認を取得することの意義について、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。

BCR の申請に当たっては、まず事業者グループ内で BCR を適用する範囲を決める必要がある。

第 29 条作業部会は、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。入念なデータマッピングの結果、EEA データを処理しないことが明らかとなった EEA 外拠点については、BCR の審査担当である主導監督当局[注1]に相談の上、BCR の対象から除外することが可能だと考えられる。

BCR の申請には、例えば管理者として EEA 内から EEA 外に個人データを移転させるためには、WP133（管理者 BCR の申請書）、管理者 BCR のドラフト、申請者の事業者グループの説明などを主導監督当局に提出することが必要である。

主導監督当局における審査に、約 4～6 カ月、二つの副主導監督当局による審査に約 4 カ月、相互認証枠組み[注2]に参加していない国の当局による審査に約 1～2 カ月かかる。そのため、GDPR の適用開始を 2018 年 5 月に控えていることを踏まえ、今後の BCR 申請にあたっては、GDPR に準拠した内容のドラフトの提出が求められる。

事業者グループ内の個人データ移転については、表のとおりである。

結語

欧州委による日本の十分性認定の動向やタイミングにかかわらず、日本企業の EEA 内拠点から日本以外の EEA 外拠点に対する個人データ移転への対応は必須であることから、企業はまず最低限 SCC による対応を完了させることに注力することが望ましい。

なお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（実践編）」（2017 年 8 月）にてより詳細な説明を行っているため、そちらも併せて参照されたい。

注1：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。

注2：現行指令の下では、EEA 内の21カ国（オーストリア、ベルギー、ブルガリア、キプロス、チェコ共和国、エストニア、フランス、ドイツ、アイスランド、アイルランド、イタリア、ラトビア、リヒテンシュタイン、ルクセンブルグ、マルタ、オランダ、ノルウェー、スロバキア、スロベニア、スペインおよび英国）が BCR の相互認証手続き（Mutual Recognition Procedure）に加盟しており、これらの国の監督当局のいずれかを主導監督当局および二つの副主導監督当局として承認を受けた BCR の取得企業グループ内では、上記21カ国から EEA 外への個人データ移転を BCR によって適法に行うことができることになる。BCR の取得企業が、上記21カ国以外の EEA 加盟国から EEA 外への個人データ移転を当該 BCR によって行う場合、当該 EEA 加盟国の監督当局から個別に当該 BCR の審査を受け承認を受ける必要がある。