2019年7月11日
JIPDECセミナーレポート

IIJにおけるGDPR対応とBCR申請について

株式会社インターネットイニシアティブ
ビジネスリスクコンサルティング本部長
小川　晋平氏

IIJ の GDPR 対応の経緯

■背景

IIJ は 2011 年からお客様のミッションクリティカルなシステムのデータベース等の管理を強みとするホスティッドプライベートクラウド「IIJ GIO」を米国、中国、シンガポール、英国と海外展開していったが、その責任者として 2014 年に IIJ Europe に赴任した英国で GDPR の危険性を認識した。当時はまだ可決まで時間がかかるものと思われていたが、2015 年 12 月に突如ファイナルドラフトが出され、そこで次四半期で可決成立を目指すとなっていたため、すぐに対応が必要な旨を IIJ 本社の経営トップに報告したところ GDPR 対応プロジェクトの責任者となり、2016 年 1 月より IIJ としての GDPR 対策を行うこととなった。

■対応の経緯

2016 年 1 月の時点で関係部署を巻き込み、会長・社長トップの下に、危機管理室（ありとあらゆるリスク・コンプライアンス対応の専門組織）が人事・IT 系への対応、法務・コンプライアンス部が顧客・外注先との契約関係、グローバル事業本部が海外拠点との調整を担う体制を整備した。創業当初からインターネットの安心安全は必要不可欠と考える文化だったので、社内の協力を得やすかった。また、体制作りと併せてトップから大枠の予算で承認をもらえたので、各担当部門が動きやすい環境を整えることができた。

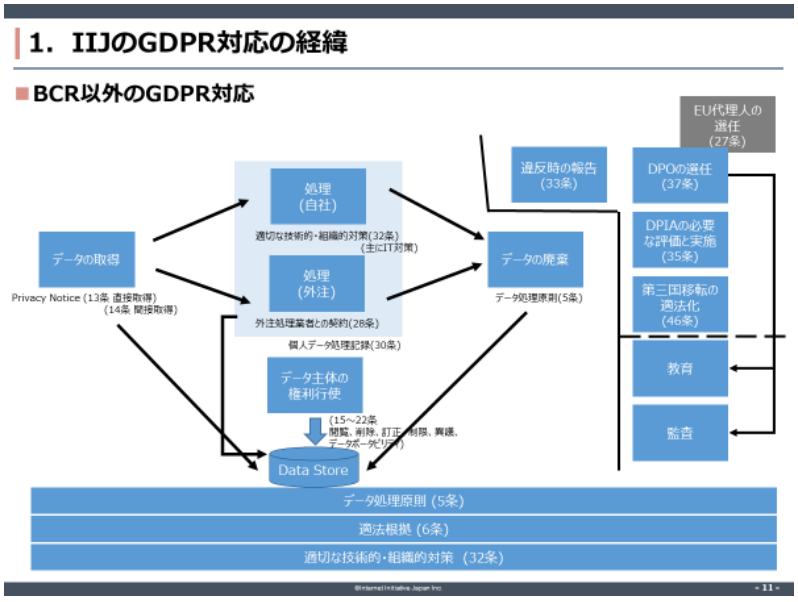
この 2 年ほど 130 社程度コンサルティングを行っているが、うまくいっていない企業の共通点は経営トップの理解がないこと。プロジェクトが進まない、予算がつかない、（特に海外との）協力関係が構築できないといった問題の原因は、経営トップの理解がない点に尽きる。

体制構築後、最初に行ったことはリスクの割り切りである。施行までの 2 年間に、限られたリソースで何を最優先して対策するかを考え、当社にとってリスクが高いのは自社の従業員データよりも IIJ GIO 顧客から預かる個人データであり、対策の最優先課題と捉え、BCR を作成し当局の承認を得ることに決定した。

その後、管理者となる IIJ Europe では、データマッピングを開始した。開始に先立ち、2016 年 1~2 月に GDPR だけでなく一般データ保護指令および関連文書すべてを、私を含め 5 名のコンサルタントで読み込み、対応方法を整理した。GDPR では、少なくとも EU に拠点がある日本企業約 2,700 社は対応が必須となる。しかし、人員が限られる海外拠点で各社が個々に対応することは非効率なため、コンサルティングサービスの提供を決定し、IIJ Europe 自身のデータマッピング作業と並行して、各社で使用できるテンプレートの作成、プロセス標準化を進めていった。その後、2016 年 5 月には IIJ Europe のデータマッピングを終了し、他国に移転したデータについてはグローバルビジネス本部経由で確認を依頼した。8 月からはコンサルティングビジネスをロンドンで開始した。

その間、日本側では危機管理室が法律事務所と共に BCR の準備を開始したが、その後 2016 年 6 月に Brexit が可決された。IIJ Europe の欧州総括拠点はロンドンのため、Brexit 前であれば所管当局は英国 ICO だが、離脱してしまうと IIJ Deutschland があるドイツ ノルトラインヴェストファーレン州が所管当局となりドイツ語への翻訳等負荷がかかる。このため、Brexit 前に英国で取得することを目指し、2016 年 7～10 月で一気に必要なドキュメントを整備し、10 月 14 日に英国 ICO に BCR を提出した。結果として、BCR 提出をきっかけにコンサルティング依頼が急増し、ビジネス的には良かったと思う。

■BCR 以外の GDPR 対応



BCR 以外の GDPR 対応は、個人データのライフサイクルに沿って対応を進めていった。データマッピング→30 条処理記録作成の段階のポイントとして、適法根拠と 30 条要件の記載に加え、関連 IT システムの対策状況、DPIA の必要性（非実施の場合の理由含む）を

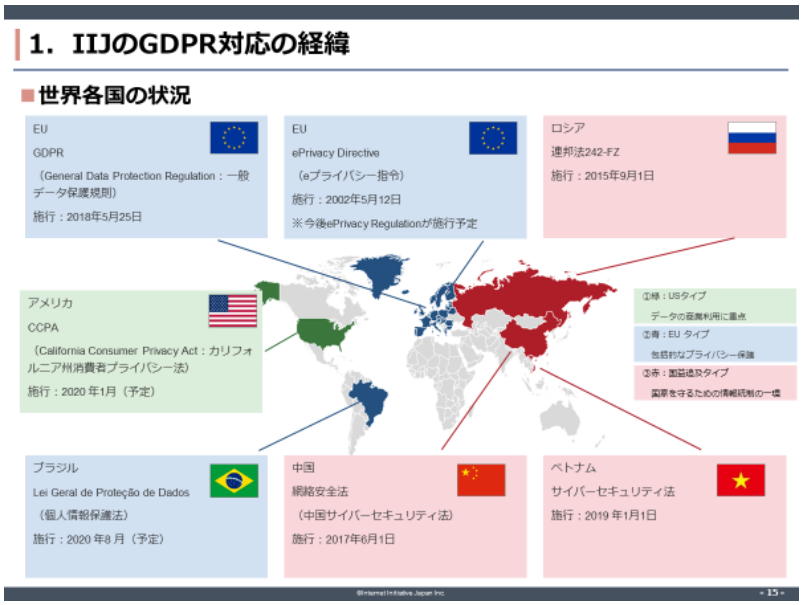
事前に整理しておくと、監督当局への説明の際に「きちんと対応している」心象を与え、ディフェンス力が高まるので、ぜひ実践していただきたい。

また、データ主体から権利行使要求があった際の本人確認プロセスや権利行使拒否が可能な場面の整理、対応手順書の作成、削除権行使時の関連データの削除方式の確認及びテスト、処理者との契約に関しては 28 条 3 項に基づく処理契約文言変更、プロセス終了後のデータ削除の徹底がある。特に、日本企業は個人データ取得後そのまま保持しているケースが多いが、GDPR では 5 条で処理終了後のデータ削除が明記されているので、徹底する必要がある。

データ保護違反時の報告対応については ISMS、P マークで整備済みのため、プロセスの一部修正・追加に留まった。この他には、DPO の選任、EU 代理人の必要性有無の確認、DPIA が必要なプロセスでの DPIA の実施、BCR 承認までの第三国移転の適法化措置としての SCC+DTA 締結、社内教育等を実施し、2018 年 5 月 25 日までに IIJ Europe と日本本社の GDPR 対応は完了した。その後、ビジネスの変化に合わせて日々対応しているが、グローバルで見るとレベル差があるため教育を徹底し底上げていく必要があると感じている。

■世界各国の状況

GDPR 対応を進める一方、世界各国で個人データ保護関連法制が新たな動きを見せておりそこへの対応も必要となってくる。中国、ロシア、ベトナムはデータローカライゼーションを掲げており、基本的に個人データは一旦その国に置く必要がある。



IIJ ビジネスリスクコンサルティング本部では、「ビジネスリスクマネジメントポータル」

で世界各国の法制度について情報提供を行うとともに、IIJ 自身を試験台にして対応ノウハウを蓄積し、各国の文化や執行力を見ながらどこで割り切る必要があるかを実務レベルでのアドバイスを行っている。

BCR の申請

そもそも論として、EU 域内での個人データ移転は自由、EU 域外への個人データ移転は原則禁止で、国として十分性決定を受けている場合または GDPR46 条 2 項に挙げられている適切なデータ保護策が取られている場合にのみ移転が許可される。通常採用される SCC 以外に、BCR や行動規範、認証メカニズム等が挙げられているが、行動規範や認証メカニズムはまだ欧州委員会からはどこも承認されていない。

我々が対応の検討を始めた 2016 年時点では、日本はまだ十分性決定されておらず、SCC 締結が一般的であった。当時は、管理者として従業員データの他に訪日外国人向け SIM（Japan Travel SIM）直販の顧客データを保持していたが、対応を機に SIM は間接販売にシフトすることに決定した。

一方､処理者としては 10,000 社を超える顧客を有する状態で SCC 締結が現実的なのか、BCR 取得では時間と費用に問題があるのではないか、等と様々な観点から議論を重ねた。その結果、顧客にとっても処理者が BCR 承認されていれば当局への説明負荷の軽減・ディフェンス力向上につながるため、BCR 取得は攻め（提供サービスの差別化）と守り（監督機関、EDPB との良好な関係構築）の両方で投資対効果があると判断した。

IIJ の BCR はまもなく承認される予定だが、プラットフォーマー以外は BCR を申請する必要はない。ただし、世界各国の法規制動向は注視し、常に現在のビジネス環境（利用サービス含め）が変化に対応しているか確認する必要はあり、当社としても情報提供等を通じて広くサポートしていきたいと考えている。