## 対応事例：インターネットイニシアティブ(IIJ)

# 経営者との問題意識共有を

IIJ のオフィス（東京）

**IIJ（本社・東京）は、欧州に拠点を持つ日系企業に先駆けて EU 一般データ保護規則（GDPR）対策を進めている。同社の欧州拠点（英国）駐在中にその中心的な役割を担い、現在は日本企業への同対策コンサルティングを担当する、ビジネスリスクコンサルティング部の小川晋平部長に、GDPR 対応について聞いた。**

## IIJ のクラウド経由でデータ移転も容易に

1992 年に日本初のインターネットサービスプロバイダー（ISP）として設立された IIJ は、今や日本のインターネット基盤を支える企業の一つだ。従業員はグループ全体で約 3,200 人。主に事業者向けの BtoB ビジネスを手掛ける。一般消費者向け（BtoC）では、大手キャリアが持つ通信設備を借り受けることにより、通常よりも安価な通信料を設定できる格安 SIM サービスなどを提供している。本格的に海外に進出したのは 11 年から。09 年に開始したクラウドサービス[注1]を主力事業として現在は米国、東南アジア、中国、欧州で事業展開する。

**Q：GDPR への対応はどのように行っているか？**

**A：**当社では情報セキュリティーや災害対策を含めた総合的な危機管理を行う危機管理室が GDPR 対応も行っている。個人情報保護対策については拠点ごとに対応しているが、今後は EU に限らずシンガポールや中国などでも法整備が進むことを見越し、GDPR 施行を機に対策管理を本社に集約すべく社内体制を見直している。

まず、GDPR 対応として最初のステップとなる「現状評価」（データマッピング）の作業は、仮に 50 人規模の欧州拠点の BtoB 企業であれば、1 週間以内に完了できるだろう。ただしこれは、取り扱う個人情報が社内の人事情報と取引先情報に限られている場合である。実際に、当社で現状評価を実施した際も、2 人体制で、3 日ほどで完了した。当社のケースが短期間で完了できた要因は、欧州における当社のビジネスが比較的限定的で、個人消費者向けビジネスは格安 SIM サービスのみであること、またもともと社内でしっかりとした個人情報管理体制を整えていたことにある。

**表　GDPR 対応のうち、IIJ が弁護士に相談した内容**

| |
|---|
| ・個人情報取り扱いの契約文書の作成や文言のリーガルチェック |
| ・BCR の承認申請にかかる業務、監督機関との交渉 |
| ・BCR 承認取得後に使用する、各サービスの契約書の見直し |
| ・法的観点からのアドバイス全般 |

資料：IIJ への取材内容を基に作成

現状評価の次は、洗い出した個人データの処理にかかる「リスク評価」が必要だ。当社、欧州拠点である IIJ ヨーロッパでは、自社で開発した基幹システム（ERP）を用いて自社で行うデータ処理に関するリスク評価を実施。英国のシステムインテグレーターを買収して立ち上げた欧州拠点だが、幸い同社が、英国の国内制度に基づいたかなりしっかりしたデータ管理体制を取っていたため、基本的に既存の社内システムを活用して対応することができた。リスク評価の結果、欧州拠点の唯一の BtoC 事業である格安 SIM サービスについてはデータ保護影響評価（DPIA）（本誌 p.51、p.60 の 12 を参照）が必要と判断。GDPR のルールに則（のっと）り DPIA を実施した。万が一個人データが漏えいした場合のリスク検証なども実施した。

データ移転を GDPR 上、適法に行うことができるように、当社は 16 年 10 月に英国の監督機関（ICO）に対し、自社のクラウドサービスに関する BCR 取得（本誌 p.56～を参照）を申請した。18 年 5 月の GDPR 施行開始前に承認を得られる見通しで、承認が得られれば、顧客は当社のクラウドサービスを利用することで、欧州経済領域（EEA）内から域外へのデータ移転を自由に行うことができるようになる。データ処理に関しては各社での対応が必要になるが、当社では、顧客企業に対しデータ処理に関するアドバイスも行っている。

**Q：GDPR を巡り、欧州における状況は変化したか？**

**A：**GDPR 可決を境に、欧州全体で個人データ保護に関する意識が大きく変わった印象がある。GDPR の前身である EU データ保護指令が可決された 1995 年当時は、世界の状況としてインターネットがビジネスの基盤になっておらず、個人データを含む膨大な電子データが国境を越えて行き交う現在の姿を、当時は誰も想像し

ていなかった。現行のEU各国の国内法は、この95年のデータ保護指令に基づき作られたものだ。

12年にGDPRのドラフトが発表され、翌13年の米国スノーデン事件[注2]をきっかけに、EU内では個人情報保護に関する意識に大きな変化があったと理解している。法案可決までの過程を見ても、従来であればEUにおける法案の可決にはドラフト作成から7～8年を要するところ、GDPRはドラフト発表から3年後の15年12月には最終案が発表され、翌16年4月に可決されたのは異例の速さであった。また違反時に課される課徴金についても、ドラフト段階で「グループ全体の売り上げの2%」だったものが、最終的には最大4%まで引き上げられた。このことも、法案可決までの過程で欧州域内において問題意識が高まったことの表れと言える。

**Q：英国のEU離脱（ブレグジット）の影響をどうみるか?**

**A：**予定では19年3月にブレグジットが完了するが、おそらく英国政府は、GDPRに関して英国に所在する企業への影響を最小限にとどめるべく何らかの対策をとると見ている。現時点で想像できるのは、GDPRをそのまま英国法として受け入れる可能性である。

EU・英国間のデータ移転に関しては、「十分性認定」の取得や「プライバシーシールド」を目指す可能性が十分考えられる（本誌p.51、p.43を参照）。だが、現在のEU・英国間のブレグジット交渉方針を踏まえると、離脱後の約束について議論を開始できるめどが、今しばらくは立ちそうもない。ブレグジット完了時点で英国が十分性認定を取得できる可能性は低いのではないだろうか。

## 経営者の理解が不可欠

IIJは他社に先行してGDPR対策を開始したことを強みとして、17年に日本企業へのGDPR対策コンサルティングサービスを開始した。同社ウェブサイトでは、実践的な対策方法を紹介。定期的な情報も提供されている。現状評価用テンプレートの作成・提供なども行われており、顧客企業に対し、自社で対策を行えるよう、体制づくりをサポートしている。

**Q：日本企業の対応状況について感じていることは？**

**A：**現在相談を受けている、欧州に拠点を有する日系企業は、現地担当者レベルでは既にほとんどの企業がGDPR対策の必要性を認識し危機感を抱いている。しかし、本社の経営レベルには依然として担当者の声が届いていない企業が多い。GDPRは、欧州拠点内の既存の体制のみで対応できるものではない。まずは経営者が対応の必要性を理解し、全社的な体制を整えることが不可欠だ。現時点で具体的な対応を開始しているのは、経営レベルに働きかけを行えるポジションの人間がキーパーソンとなって動いている企業に限られているという印象だ。

**Q：今後対応を行う企業に対し、プロセスごとのアドバイスをいただきたい。**

**A：**GDPRは基本的には法対策だが、現状評価については、法的観点とITの観点、双方からのアプローチが必要になる点に留意すべきだ。具体的な対策を検討する際、各個人データがどのような形で本社サーバーに保管されているか、どのようなプロトコル（通信規約）で送られたものか、移転された個人データのうちどの部分が暗号化されているかなどが情報として必要になる。システム上の情報を考慮せずに現状評価を行うと、結局、具体策を検討する段階で情報が足りないという事態に陥り、その段階で改めてIT部門に相談することになりかねない。こうしたロスを防ぐためにも、GDPR対策チームには弁護士だけでなく当初からIT部門の担当者に入ってもらうことが、効率的な対応のために不可欠だ。

データ保護責任者（DPO）を選任する際には、事業の必要性を理解しプライバシー保護と事業のバランスを考えられる人材を選ぶべきだ。DPOが常に「事業を前に進めるためにどうすればよいか」という意識を持って対策に臨まなければ、事業自体に支障を来しかねない。

さらに、EEA内からのデータ移転について、BCR対応を検討中の企業は早急に対応する必要がある。監督機関は基本的に各国1カ所のみ（ドイツのみ連邦16州それぞれに設置）なので、承認までのプロセスに非常に時間がかかるからだ。特にこれから対策をとる場合には、承認が下りるまでは標準契約条項（SCC）での個別対応が必要になる可能性も含めて対策を検討すべきだ。

（聞き手：根津　奈緒美／ジェトロ海外調査部欧州ロシアCIS課）

注1：従来は利用者が手元のコンピューターで使用していたデータやソフトウエアをネットワーク経由で使用できるようにするサービス。
注2：米国国家安全保障局（NSA）が極秘にグーグルなどのサーバーから大量に個人情報を入手していたことを、米中央情報局（CIA）元職員が告発。個人情報保護に関する世界の意識に影響を与えた。