【講演レポート】「グローバル CBPR の展開・普及ワークショップ」（経済産業省/個人情報保護委員会共催）

「グローバル CBPR の展開・普及ワークショップ」質疑応答

Q: CBPR がグローバルに展開した場合、共産圏も対象になるのでしょうか？共産圏へのデータ移転に対するリスクをどのように捉えているか、どのように拡大していこうとしているのか伺いたい。

A: 私が認識している限り、もともと APEC の枠組みなので、ロシアや中国は参加できるが関心を持っていないという状況です。一方、ベトナムは興味を示していた時期はあります。グローバルサウスと言われる国々に働きかけていくことは考えられると思います。
日本も EU もロシアや中国を十分性認定することはないと思われますが、個々の企業を認証する CBPR のような仕組みは受け入れられやすいかもしれません。
CBPR というよりは、各国のガバメントアクセスに関する制度に起因するものなので難しい問題ではあります。CBPR 認証はあくまでも企業の取組みを確認するものですが、そのスキームを越えて政府がどの程度関与するかを考慮するのは難しいと思います。
アリババクラウドはシンガポールで CBPR 認証を取得しています[1]。中国進出を考える際に、いきなり中国のクラウドに預けるのではなく、CBPR のスキームが効くアリババクラウド経由で進出することも選択肢になるかと思われます。

Q: 以前、TRUSTe を取得すると CBPR 認証も併せて取得できるような仕組みがあったように思うが、普及の観点から、プライバシーマークの審査＋α で CBPR 認証も取得できるような仕組みは考えられていますか？また、CBPR 認証と ISO/IEC 27701（PIMS 認証）の関係や、CBPR と GDPR の BCR（拘束的企業準則）を連携させるような議論についてもご意見を伺いたいです。

A: 挙げていただいた認証制度は、取得する事業者から見ると同じように見える部分はあると思いますが、それぞれ枠組みが異なるため何かが一緒になったりするようなことはないと思います。ただし、取得に向けた取組みは同じような作業になるので、何かを取得する際に一緒に他の認証も申請するということは十分に考えられます。
一つ留意点としては、BCR はあくまでもグループ企業間でのデータ移転に限定されているので、CBPR 認証とはそもそもの射程範囲が異なります。GDPR の中で汎用性が高いのは SCC（標準契約条項）ですが、これもやはり少し建付けが異なるので、取得の目的にあった認証取得を検討する必要があります。

Q: 今後、プライバシーマークもデータが国内にあるという前提では成り立たなくなるので、国外も視野に入れていくことになると思います。そうなると素人目にはプライバシーマークと CBPR 認証の違いが良くわかりません。今後、プライバシーマークと CBPR 認証は並行していくのか、将来的には一本化することも検討されているのか教えてください。

[1] https://www.alibabacloud.com/ja/trust-center/cbpr

A: プライバシーマークは個人情報保護法で位置付けられているものではなく、日本産業規格のプライバシーマネジメントシステムを元にした認証制度です。他方で、CBPR はきちんと執行できることを制度上担保しなければならないので、認定個人情報保護団体の業務の一環に位置付けられており（「その他対象事業者の個人情報等の適正な取扱いの確保に関し必要な業務」（法第 47 条第 1 項第 3 号））、公的なバックグラウンドがある点が異なります。
認証制度である点は同じで、取得のための作業は似ているので、事業者側から見ると被っているところはあると思いますが、制度上は明確な違いがあるので、一本化することはないと思います。
現在の認証企業の中にはプライバシーマークを取得していないところもあります。なくても CBPR を取ることは可能です。CBPR 取得のプロセスの中で、データがどこにあって、どのように管理されていて、どのような運用になっているのかを全部洗い出すということになります。
審査の観点からいうと、プライバシーマークは国内におけるデータ移転を見ており、CBPR は越境移転を注視しているというイメージです。企業側からすると、どちらの制度も同じような対応が必要ですが、審査の視点が異なります。プライバシーマークの場合も越境移転の有無は確認しますが、詳細までは確認しません。一方、CBPR は越境移転がメインなので、その部分が細かく確認されます。

Q: プライバシーマーク付与事業者が CBPR 認証を取得する際に、大きな違いがある部分や別途対応が必要な部分はありますか？また、対応コストはどの程度となりますか？

A: プライバシーマークの審査では個人情報の管理状況全体について確認されますが、CBPR は管理体制が整備されている前提で、越境移転に関する業務フローを細かく確認されるので詳細な業務フロー図が必要になります。また、そこで使用しているシステムがあれば、そのシステム構成図も確認されるので、プライバシーマークの審査と一番異なるのは、業務フロー図とシステム構成図を用意する必要があるという点です。
また、プライバシーマークの審査ではシステム的な具体的な要件までは聞かれないこともありますが、CBPR では社内の不正侵入対策や IPS や IDS を導入しているかということなども聞かれます。ネットワークの不正侵入対策をしていれば問題ありませんが、対策が不十分な場合は自社の状況や費用対効果等も考慮しながら、対策を取る必要があります。「こういう対策でなければならない」ということではありません。
社内からの不正アクセスに対する技術的な対策を取っていますかという観点は JIS にはなく、CBPR では聞かれるので対策が必要になりました。IPS や IDS を導入すると時間とコストがかかってしまうので、それを避けるために外部のストレージサービスを使用する選択をしました。2 つの業務をそこに移せばよかったので、それほど手間ではありませんでした。

Q: 当社は地域通貨システムを運営していますが、海外政府等からの引き合いが多くなり、一部は海外でサービスインしています。アプリが海外で独り歩きする可能性がある状況でどのような対策を取ればよいか教えていただきたい。

A: 政府や自治体が越境データ移転が生じる事業を実施する際は CBPR 認証取得を要件とするような動きがあると、CBPR 認証の有無が事業の追い風にも逆風にもなります。今、CBPR 認証を取得すれば「関西エリア第一号」とアピールできるので、早めの取得を目指されると良いと思います。

ビジネスの拡大スピードに追いつくように内部管理体制の強化をすることはかなり大変です。海外からの引き合いが多数来ているということが分かっているのであれば、いまのうちに準備して取っておく方が事業拡大のスピードを落とさずに、安心いただけるサービスの提供につながるのではないかと思います。

本内容は、2023 年 12 月 14 日福岡、2024 年 1 月 10 日大阪で開催された「グローバル CBPR の展開・普及ワークショップ」パネルディスカッションでの質疑応答内容を取りまとめたものです。