【講演レポート】JIPDECセミナー

「令和2年改正 越境移転データの取扱いの実務」

桃尾・松尾・難波法律事務所パートナー弁護士
松尾　剛行氏

2022年4月に全面施行された令和2年改正個人情報保護法においては国際関係に関する規律が強化されました。本セミナーは特に実務対応が難しいとされる「越境移転データ」をテーマに、第三者提供、外的環境の把握、安全措置について、規制の概要と類型ごとの実務対応について解説するものです。外国と日本の間の越境移転との関係では、補完ルールの改正[1]や、各国法の規制[2]も重要ですが、ここでは省略します[3]。

凡例
通則編：個人情報の保護に関する法律についてのガイドライン（通則編）[4]
外国第三者提供編：個人情報の保護に関する法律についてのガイドライン（外国第三者提供編）[5]
Q&A：「個人情報の保護に関する法律についてのガイドラン」に関するＱ＆Ａ[6]

各国の規制の概要に関する参考資料
「外国における個人情報の保護に関する制度等の調査」（個人情報保護委員会）
（ https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaikoku ）

1　「改正個人情報保護法」規制の概要

(1) 個人データの外国第三者提供に関する規律の概要

令和2年改正前個人情報保護法（以下「旧法」といいます。）から既に、外国の第三者への提供時の本人同意（旧法第24条）が必要となりました。令和2年改正個人情報保護法（以下「法」といいます。）においては本人同意規制を前提に、同意スキームなのか、相当措置スキームなのか等という外国第三者提供類型に応じて規制が強化されました（法28条。図1参照）。

[1] https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf

[2] 中国に関するものとして松尾剛行「中国の個人情報保護法とデータ運用に関する法制度の論点」情報通信政策研究5巻2号(https://www.soumu.go.jp/main_content/000800520.pdf)参照

[3] なお、法28条が適用除外される結果、法28条による法27条の適用除外が適用されなくなった場合の対応についても触れない。

[4] https://www.ppc.go.jp/files/pdf/211116_guidelines01.pdf

[5] https://www.ppc.go.jp/files/pdf/211029_guidelines02.pdf

[6] https://www.ppc.go.jp/files/pdf/220401_APPI_QA.pdf

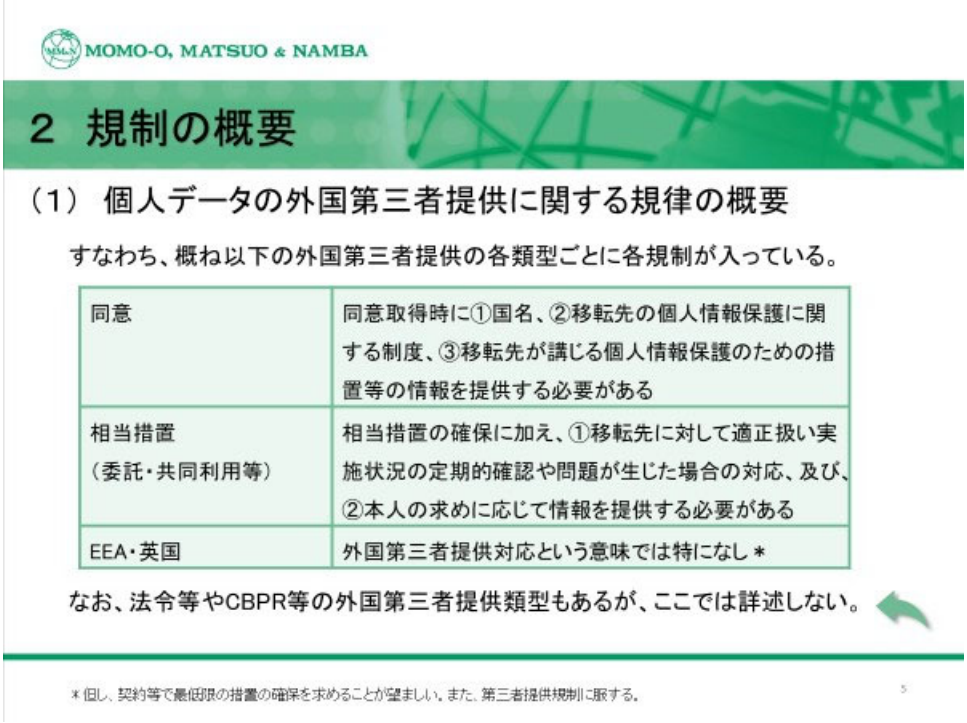

図1．個人データの外国第三者提供に関する規律の概要

（2）外的環境の把握の概要

インターネット等を通じ自社の個人データに関する外国第三者提供の機会が増える中、海外において個人データを取り扱った場合においても、日本国内と同等の安全管理措置（法23条）を講じるだけで十分なのか、という問題意識を踏まえ、外国で個人データを取り扱う際には外的環境を把握し、追加の安全管理措置を講じるという規制が追加されました。

（3）保有個人データに関する事項の本人への周知について

保有個人データに関する事項の本人への周知（旧法27条、法32条）については、元々「保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの」が規定されていた（旧法27条１項４号）ところ、令和2年改正でもかかる規定は維持されました（法32条1項４号）。そして、令和2年改正に伴い改正された政令10条１号が「法第二十三条の規定により保有個人データの安全管理のために講じた措置（本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）」と定めており、これによって、安全管理措置に関する本人への周知に関する規定が入りました。そして上記の外的環境の把握が安全管理措置に含まれている以上、これも周知の対象となります（通則編3-8-1(1)参照）。

2　個人データの外国第三者提供に関する規律対応の実務

（1）外国第三者提供への該当性

最初に、そもそも自社が外国第三者提供を行っているか、及び行っているのであればそれがどのようなものかを確認すべきです。ただし、仮に外国第三者提供を行っていなくても外的環境把握等が必要な

場合があることから、「当社が外国第三者提供を行っていないことが確認された」というだけで必ずしも何もしなくてよくなる訳ではないことには留意が必要です。

たとえば、クラウドサービスを利用しているという場合において、個人情報取扱事業者との契約により、外国のクラウドベンダがそのサーバに保存された個人データを取り扱わず、なおかつ適切なアクセス制御を行っている場合は外国第三者提供になりません（Q&A12-4、7-53）。

（2）外国第三者提供スキーム別の要件

上記1（2）のとおり、どのスキームで外国第三者に提供するかに応じて行うべきことが変わりますので、スキームを把握した上で、対応を行う必要があります。主なスキームとして同意及び相当措置があります[7]。

・同意

同意スキームを利用する場合、本人が外国第三者提供同意の意味をわからないまま同意を取ったのでは、外国第三者提供に本人同意を要求するという趣旨が達成できません。そこで、本人に対し、以下の情報を提供し、本人が認識したうえで同意を取る必要があります。（法第28条第2項、規則第17条）

・提供先の第三者の所在国の名称
・適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報
・当該第三者が講ずる個人情報の保護のための措置に関する情報

・相当措置

旧法時代から、たとえば委託契約書や共同利用に関する契約書上、日本の個人情報保護法で求められる水準の内容を記載する、グループのポリシーで日本の個人情報保護法で求められる水準を確保させる等の相当措置の確保によって、外国第三者提供における本人同意が不要とされます。

令和2年改正により、相当措置スキームを採用した場合において、さらに３つの対応が義務化されました（図2参照）。

[7] なお、EEA・英国についてはここでは触れません。ただし、第27条（第三者提供の制限）で規定する同意、委託・共同利用等（同条第5項）に基づき日本企業へ提供する場合と同様の対応が必要となります（外国第三者提供ガイドライン2参照）ので留意が必要です。

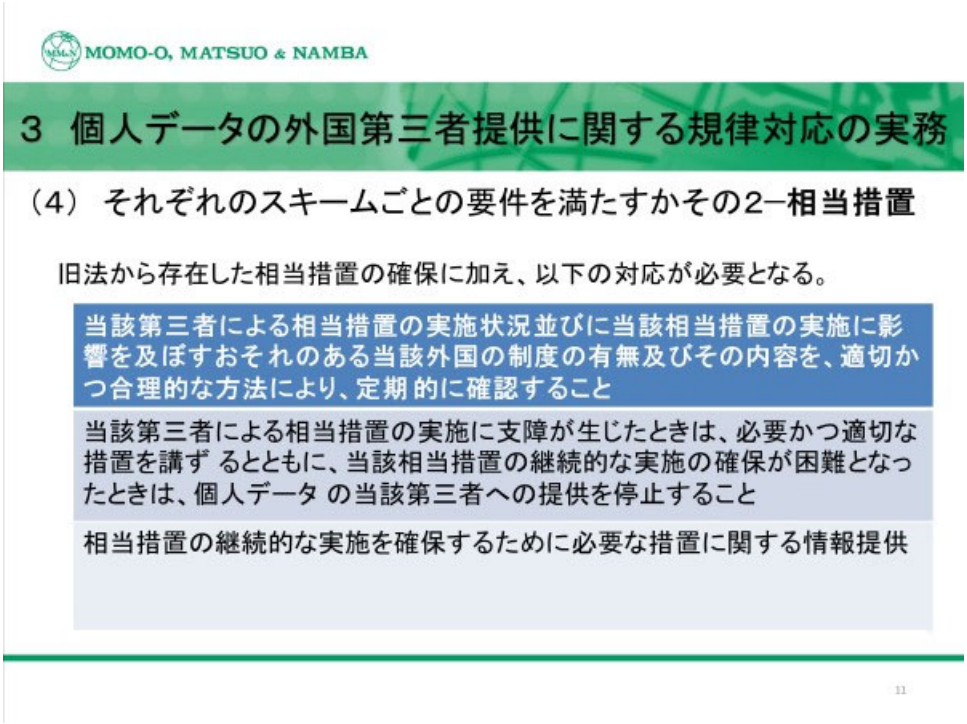

図2. 相当措置での必須対応内容

3 外的環境把握の実務

（1）外国における個人データの取扱いの有無の確認

外国において個人データが取り扱われる場合、外的環境把握の義務が発生します。

ポイントは２つです。1つ目は、外国第三者提供にあたらなくても外的環境把握義務が適用されることがあることです（典型的にはクラウドサービスの利用の場合で、上記2（1）の要件が満たされるため、外国第三者提供にならない場合）。2つ目は外国第三者提供に該当し、かつ、外的環境把握義務が適用されることがあることです（典型的には委託＋相当措置の場合）。

（2）外的環境の把握のパターン

日本企業に関する外的環境の把握が必要な典型的な場合として、3つのケースを紹介します[8]（図3参照）。

[8] なお、それ以外にも 外国企業が個人情報保護法の域外適用を受ける場合も外的環境の把握義務が生じます。

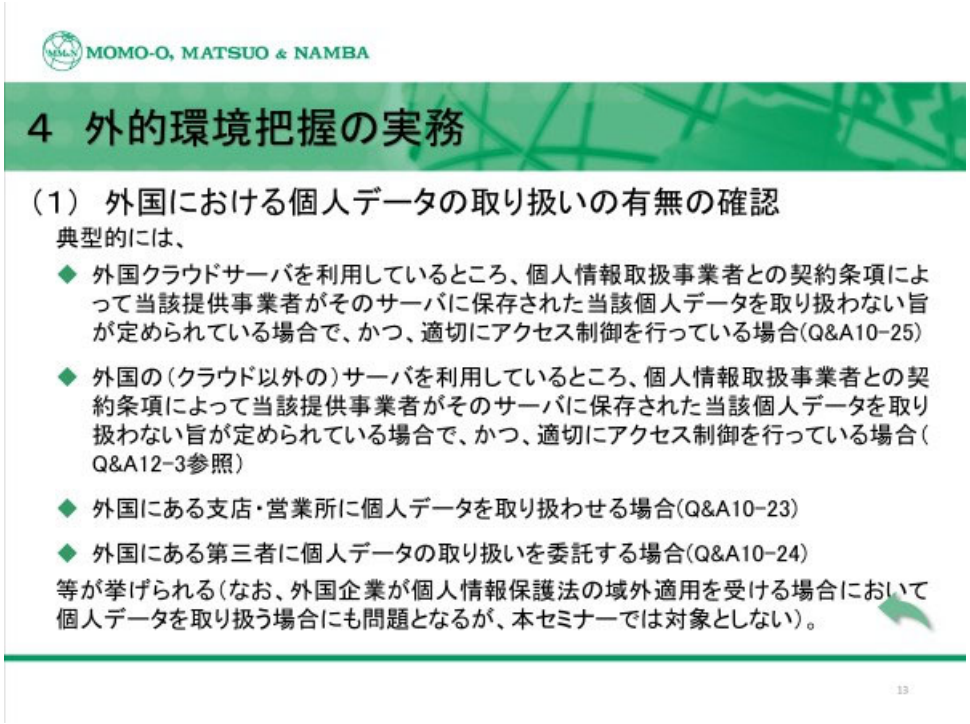

図3. 外国における個人データの取扱いの有無の確認

（3）外国のクラウド／クラウド以外のサーバを利用した場合

外国クラウド／外国サーバの利用において、契約により、外国のクラウドベンダがそのサーバに保存された個人データを取り扱わず、なおかつ適切なアクセス制御を行っている場合は外国第三者提供を行っていないことになります。しかし、そうであっても、外的環境把握義務がありますので、当該外国の個人情報保護法制度を把握し、個人データの安全管理のための適切な措置を講じることになります。

クラウドベンダの場合、当該適切な措置として覚書締結ができないことが多いものの、多くのクラウドベンダはホワイトペーパー等で基準・規格の準拠、認証所得、第三者監査等をうたっているケースが多いので、これらを確認することが安全管理措置の観点から重要となります。

なお、外国系のベンダであっても、日本法人でかつ日本サーバであれば、外的環境把握義務は発生しませんが、日本法人ではなく外国法人であるクラウドベンダであれば、サーバがどこにあっても外的環境把握義務は免れられません（「多くいただいたご質問と回答Q１」参照）。とはいえ、外国ベンダでかつサーバ所在地が外国であれば、その双方に対する外的環境の把握が必要になるところ、外国ベンダでも、サーバが日本にあれば、ベンダ所在地に関する外的環境の把握だけで足ります。そこで、サーバの所在国を選ぶことができるオプションが提供されているのであれば、特段の理由がない限り日本国内のサーバ（リージョン）を選ぶことを実務上検討すべきでしょう。

（4）外国にある第三者に個人データの取扱いを委託する場合

第三者に個人データの取扱いを委託した場合でも、なお委託元の個人データの取扱いであることに変わりはありません。委託先が外国であれば、委託元の（日本の）個人情報取扱事業者は委託先を通じて外国において個人データを取り扱うことになります。そこで、委託元としては安全管理措置の一環として、外的環境の把握が必要になります。

具体的には、委託先の所在国の個人情報保護法制度等を把握した上で、委託先の監督その他の安全管理措置を講じる必要があります。

ただし、外的環境把握と外国第三者提供規制は別の話ですので、上記2（2）の委託に対する外国第三者提供規制対応（特に相当措置スキームにおける令和2年改正で加重された対応）についてもきちんと対応していただく必要があります。

（5）個人情報取扱事業者が、外国にある支店・営業所に個人データを取り扱わせる場合

日本法人である個人情報取扱事業者の外国にある支店・営業所[9]は、個人情報取扱事業者（日本法人）の一部となるため、本店から支店・営業所に提供しても第三者提供にはならず、日本の個人情報保護法に準拠した日本法人の社内ルールの遵守が適用されます。しかし、外国で個人データを取り扱う以上、所在国のガバメントアクセスに関する規律等が適用されることから、適切な措置を取る必要があります。

Q＆A10-23において、「外国にある支店や従業者が日本国内に存在するサーバに保存されている個人データにアクセスして取り扱う場合でも同様に外的環境の把握の義務がかかり得る」とされていることもあわせてご留意ください。

コロナ禍でのテレワークの普及により、従業員が社外から、事業者の取り扱う個人情報データベース等に接続する場面が増えている中、従業員が外国に引っ越してテレワークを行い、移転国からデータベースにアクセスする場合、外的環境把握規制の対象となります。

4　保有個人データに関する事項の本人への周知について

これまで、保有個人データに関する事項の本人への周知対応（旧法27条）としてプライバシーポリシーを利用してきた会社がほとんどです。そして、外的環境を含む安全管理措置に関する本人への周知対応（法32条1項4号）についても、プライバシーポリシーを利用することが可能です。

通則編3-8-1(1)は「個人データを保管しているA国における個人情報の保護に関する制度を把握した上で安全管理措置を実施」するという記載方法を例示しています。

外国の支店・営業所の場合、外国の制度を把握したうえで安全管理措置を講じる場合、保有個人データの安全管理のために講じた措置として、支店・営業所の所在国の名称を明らかにし、本人の知り得る状態にしておく必要があります（Q&A10-23）。

委託の場合も、委託先が存在する外国の名称の表示、外国の制度を把握して講じた措置の内容を本人が知り得る状態にしておく必要があります（Q&A10-24）。

クラウドサービスの場合、クラウドベンダがどこに所在するのか、個人データを保存するサーバがどこに存在するか、を明らかにする必要があります。保存されるサーバの所在国が特定できない場合につき、「多くいただいたご質問と回答Q4」をご参照ください。

[9] なお、外国に子会社を設置せず支店を設置することが比較的多い金融機関等はそれぞれの分野ごとのガイドライン等が適用されることにも留意すべきである。金融分野に適用されるものとして「金融関連分野ガイドライン」（https://www.ppc.go.jp/files/pdf/kinyubunya_GL_220330.pdf ）を参照のこと。

このように、プライバシーポリシー上に法定の事項を記載することができるのであればそれで問題ありません。ただし、外国での個人データの取扱いが多数存在する等の場合には、実務上プライバシーポリシーに書くことが困難な場合もあります。

そのような場合、法32条1項柱書括弧書に基づき「本人の求めに応じて遅滞なく回答する場合」の方式の採用が可能です。

桃尾・松尾・難波法律事務所パートナー弁護士

松尾　剛行氏

第一東京弁護士会、NY州弁護士、東京大学法学士、ハーバード大学ロースクールLL.M.、北京大学博士(法学)、慶應義塾大学講師（非常勤）。
主な書籍に『士業のための改正個人情報保護法の法律相談』『最新判例にみるインターネット上のプライバシー・個人情報保護の理論と実務 』『ICT・AI時代の個人情報保護』『紛争解決のためのシステム開発法務』他。

本内容は、2022年4月12日に開催されたJIPDECセミナー「令和２年改正 越境移転データの取扱いの実務」講演内容を取りまとめたものです。