

【ディスカッションレポート】JIPDECセミナー「グローバルビジネスにおけるデータの利活用と保護  
～データ越境移転ルールの最新動向～」

ディスカッション「越境データビジネスの未来」

パネリスト：渥美坂井法律事務所 弁護士 松岡 史朗氏

渥美坂井法律事務所 弁護士 藤原 理氏

JIPDEC 認定個人情報保護団体事務局 主任研究員 大下 奈美

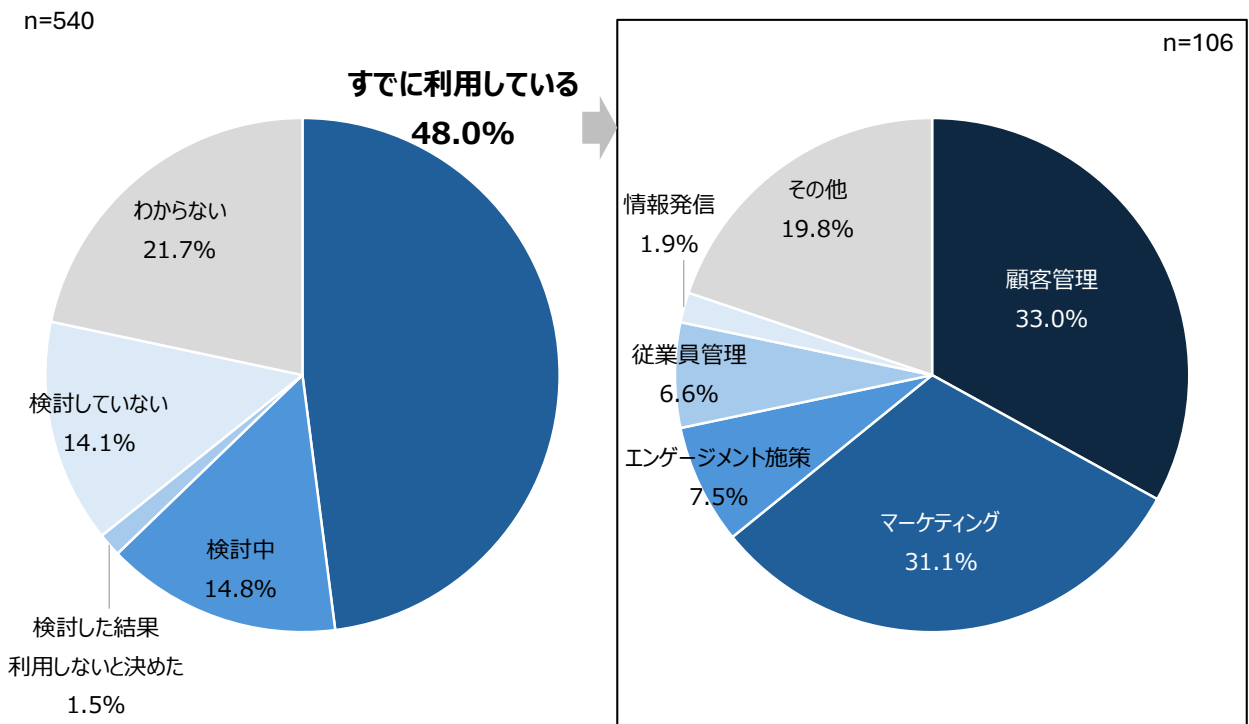
モデレータ：JIPDEC 電子情報利活用研究部 グループリーダー 松下 尚史

事前アンケート結果から

松下 セミナーにご参加いただいている皆さまより事前に頂戴したアンケート結果をご覧くださいながら、ディスカッションを進めてまいります。

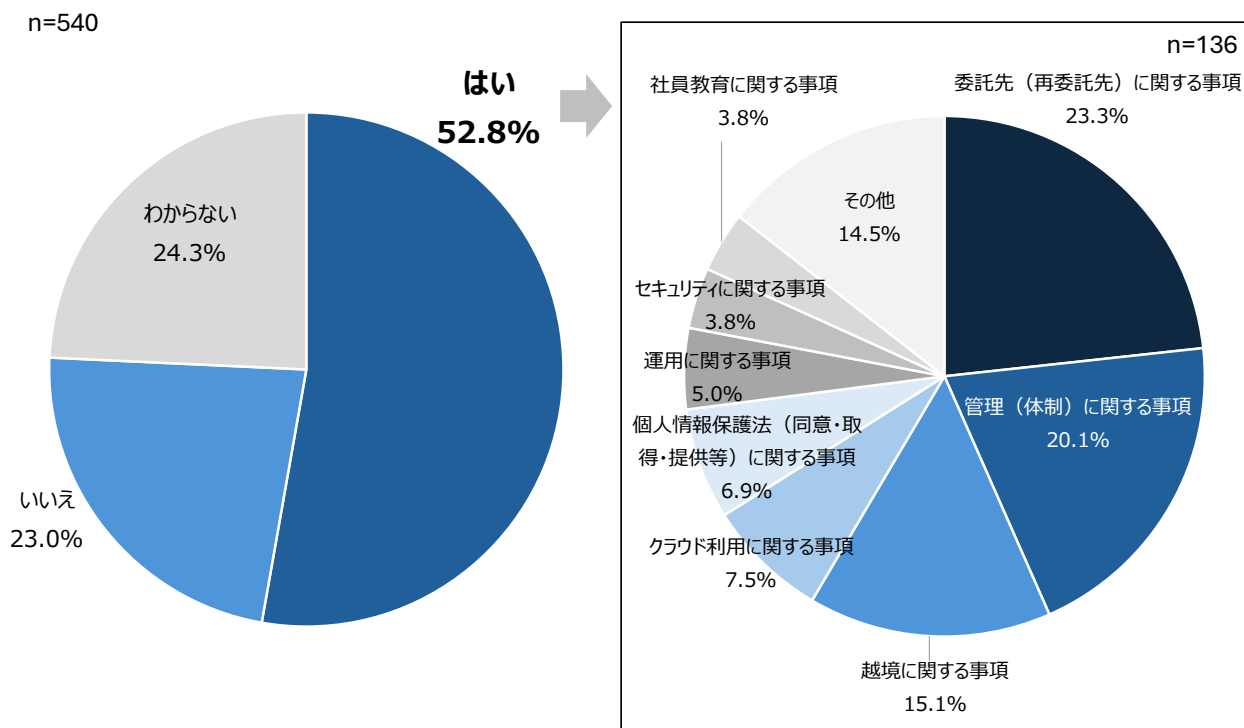
まずは、個人情報の利活用状況（図1）についてですが、既に利活用しているとの回答が48%と過半数、検討中も約15%でした。利用方法としては、顧客管理・マーケティングなどの社外の方々の個人情報を扱う利用方法が64.1%、エンゲージメント施策や従業員管理などの社内の方々の個人情報を扱う利用方法が14.1%という結果になりました。

貴社にて個人情報（従業員の情報含む）の利活用を検討していますか。



また、個人情報、個人データの管理で苦慮されていることがありますか？という問（図2）に関しては、半数を超える約53%の方が「はい」と回答されています。詳しく見てみると、一番多いのが「委託先（再委託先）に関する事項（23.3%）」、次いで「管理（体制）に関する事項（20.1%）」、「越境に関する事項（15.1%）」に多く声が集まった結果となっています。

## 貴社において、個人情報、個人データの管理で苦慮されていることはありますか。



JIPDEC ©2024 JIPDEC All Rights Reserved.

図2：セミナー事前アンケートから「貴社で個人情報、個人データの管理で苦慮していることは？」

### 越境移転とは？ 移転に際し注意点は

松下 上記を踏まえ、そもそも越境移転とはどういったものが該当するのかという点について、弁護士の松岡先生、藤原先生にご解説をお願いします。

松岡 「越境移転」は、海外へ個人データを移転することをいいますが、その概念・範囲を正確に把握する必要があります。個人情報保護法28条1項は、外国にある第三者への個人データの提供を規制しているところ、この「第三者」は本人以外の者を言い、法人格を有するか否かが基準となるとされています。このことから、例えば、日本の会社が自ら外国にサーバを設置して運営している場合、その外国にあるサーバにおいて個人データを保存したとしても、個人情報保護法28条1項は適用されない、つまり、「越境移転」には該当しないとされています。

また、サーバと「越境移転」との関係では、「クラウド例外」も把握しておく必要があります。「クラウド例外」は、サーバ内の個人データを取り扱わないこととなっている場合、クラウド業者に個人データを渡すように見える場合でも、個人情報法上、例外的に第三者提供には該当しないとします。こ

のクラウド例外は、法律の明文で認められた例外ではなく、解釈上認められている例外であり、第三者提供を規律する個人情報法27条、外国の第三者提供を規律する個人情報法28条の解釈として議論されています。

資料(図3)は[個人情報保護法27条1項](#)ですが、これは第三者提供をしてはならないという条文です。

また、[Q&A7-53](#)がクラウド例外を定めています。ここに書いてある通り、個人データを取り扱わない旨が定められている場合については、提供に該当しないということになり、27条や28条の規律には引っかけられません。

ではなぜ、クラウド例外がここまで議論をされているのかといいますと、法律実務的には日本企業の多くがクラウド例外を根拠として、27条や28条の適用を受けないものとしてクラウドサービスを提供する企業に情報を提供しています。しかし、現実的にクラウドサービスを提供する企業は、契約書に「必要がある場合、個人データを取り扱う」旨を書いていたり、実際に個人データを取り扱っていたという事例が珍しくはないからです。そのため、クラウド例外を根拠としてクラウドサービスを提供する企業に情報を提供しておきながら、実はクラウド例外が当てはまらないのではないかという問題意識が存在します。

## 個人情報及びQ&A



### 個人情報27条1項

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

### Q&A7-53

クラウドサービスには多種多様な形態がありますが、クラウドサービスの利用が、本人の同意が必要な第三者提供(法第27条第1項)又は委託(法第27条第5項第1号)に該当するかどうかは、保存している電子データに個人データが含まれているかどうかではなく、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているかどうか判断の基準となります。

**当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことはならないため、「本人の同意」を得る必要はありません。**

また、上述の場合は、個人データを提供したことにならないため、「個人データの取扱いの全部又は一部を委託することに伴って・・・提供される場合」(法第27条第5項第1号)にも該当せず、法第25条に基づきクラウドサービス事業者を監督する義務はありません。

当該クラウドサービス提供事業者が当該個人データを取り扱わないこととなっている場合の個人情報取扱事業者の安全管理措置の考え方についてはQ7-54参照。

当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合は、**契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等**が考えられます。

図3：個人情報保護法27条1項、Q&A7-53より(渥美坂井法律事務所 作成資料より)

議論を惹起させた資料の一つとして、昨年、個人情報保護委員会から出された「[生成AIサービスの利用に関する注意喚起等](#)」があります。これによれば、生成AIサービスを提供する事業者が、当該個人データを機械学習に利用しないこと等を十分に確認することと記載されており、機械学習をさせなければ

27条、28条にある提供に当たらないのではないかと読めるという説がかなり有力に唱えられています。ただし、このAIサービスを提供する企業も、学習させない場合でもその他の必要な場合には、個人データにアクセスすることが想定されますので、上記の注意喚起はクラウド例外を拡張することを意味するのか、あるいはAIについては提供の規律に該当しないとして特別に拡張することを意味するのかという点については議論がされています。

さらにもう1点、2024年3月に個人情報保護委員会が公表した「行政上の対応」によって、この「クラウド例外」の要件が実は守られていないのではないかと問題が明確になりました。すなわち、その行政上の対応の対象となった会社の契約書には個人データにアクセスする場合があると記載されており、実際に個人データを取り扱っていた実績もあると事実認定がされています。そのため、個人データを取り扱わないこととなっている場合とは言えず、クラウド例外には当たらず、提供を行っているという判断にいたりました。[27条5項1号](#)の通り、委託によるものであれば、きちんと委託契約書を定める必要があるので注意してください。

**藤原** 私からは、電子データを取り扱う情報システムの保守サービスについてご説明します。事業者が単純なハードウェア・ソフトウェアの保守サービスのみを行う場合においては、先程のクラウド例外の基準に類似して、契約条項によって当該保守事業者が個人データを取り扱わない旨が定められており、かつ、個人データが閲覧可能であっても、記録や印刷などをしない等の適切なアクセス制御が行われているときには、個人情報を取り扱うことにならないということがQ&A7-55で公表されています。かかる規律がどの範囲まで適用されるのかは実態に沿って考える必要があると思いますが、クラウド事業者が単純な保守サービスのみを行う場合はこのような例外もあるため注意しつつ検討していただければと思います。

また、松岡も申し上げましたが、実務を行っていく上では、これらの例外に該当するか契約書や利用規約をしっかりとチェックして、個人情報の取り扱い範囲を明確にするために、必要であれば事業者に問合せも行ってください。これらにより本当に個人情報を取り扱っていないと言えるのか否かを見極める必要がありますが、実際には正確な回答が返ってこない場合もあるため、かかる場合には個人データの移転先が基準適合体制に該当するのか等を、相当措置の継続的な実施を確認する方法を含め検討を行うことになるかと思われます。

#### 外的環境の把握に関する安全管理措置について

**松下** 続いて、外国のクラウドサービス事業者のサーバが日本国内にある場合、外的環境の把握に関する安全管理措置の適用があるのか否かに関して教えてください。

**藤原** 外国のクラウドサービスを利用すると、事業者は外国において個人データを取り扱うこととなるため、サーバが日本国内にある場合でも該当する可能性があります。すなわち、事業者は安全管理措置の一環として、外的環境の把握が必要となり、安全管理措置の責任者として個人情報保護法上の義務も負うため対応が必要となります。

**松岡** 海外企業に委託をし、サーバが日本国内の場合は、外的環境の中でもその海外企業の所在地、所在する国の外的環境を示す必要があります。例えば、インドの会社にデータを渡したが、サーバは日本

にあり、仮にインドの政府や治安機関がそのインドの企業に対してデータを提出させる権限を持っている場合、実質的に日本在住者の個人データの利益を害する可能性が出てきます。それを重視すれば、インドのガバメントアクセスについても情報開示は一定程度求められるべきだと思います。他方、サーバが日本にあり、海外政府の提出権限がおよぶ事態をほとんど懸念をする必要がない状況であれば、その海外政府のガバメントアクセスの詳細な開示までは必要のない場合もあり得るのではないかと思います。

**松下** データの越境移転を前提にすると、委託先の管理が非常に難しくなってくると思います。その視点で、委託先と契約を結ぶ上での注意点を藤原先生、お話しいただけますか。

**藤原** 個人情報法23条やガイドライン等では、外国にある委託先に対しては、日本の個人情報保護上自らが課されているのと同等の安全管理措置が講じられるように事業者が監督を行う必要がある旨が定められています。事業者は、基本方針の策定や個人データの取り扱いに関する規律の整備、組織的安全管理措置、人的、物理的、技術的な安全管理措置などさまざまな観点から措置を講ずる必要があります。

また、繰り返しになりますが、海外の委託先選定の際の注意点として「外的環境の把握」があります。外国において個人情報を取り扱う場合は外国の法制度等もしっかり把握した上で安全管理措置を講じるようにしてください。

#### 諸外国の情報収集について

**松下** 外国の委託先を選定する際はさまざまな安全管理措置を講じる必要があるということで、ガバメントアクセスも考慮すると複雑な対応が必要になると思います。諸外国の制度の情報を得るためのコツがあればぜひ教えてください。

**松岡** プライバシーに関連したサービスを提供する企業の中には、海外のプライバシーに関するルールについて説明しているところもあります。手始めにそういった情報サービスを使ってみるのもいいのではないかと思います。ただし、そのようなサービスの記載には間違っている記載も散見される場合があります。そのため、データ漏えいに対応する場合やデータ漏えいを生じさせないための体制を整えたいといったケースでは、そういったサービスだけでは足りないこともあるため、個別に専門家にご相談いただくのがよろしいかと思います。

**藤原** ご存じかと思いますが、個人情報保護委員会のWebサイトでも調査を元に作成された報告書も公開されていますし、我々のような弁護士事務所が独自に各国の法制度に関する調査を行い公表しているものもあるので、そういったものを活用いただければと思います。その意味では、ある程度はデスクトップサーチで把握できる部分も大きいとは思いますが、リサーチ後、実際に会社の方針を立てる際などは個別に相談いただくのが一番安全かと考えています。

#### CBPR認証について

**松下** 確かに、言語の違う外国の法制度となると難しいところもあると思います。専門の機関にご相談いただく、または自社の顧問弁護士にお尋ねいただくのがいいのかもしれない。



さて、少々話題を変えまして、現在デジタル赤字が拡大しているという話も耳にします。日本もDXが進んでいく中で、海外のサービスを採用するケースも非常に増えていくのではないかと思います。そこで出てくるのがCBPR認証などではないかと思えます。CBPR認証を取得することのメリットについて、大下さん、補足いただけますか。

**大下** 私は以前、情報システム部門の責任者の立場だったのですが、データの管理には非常に苦労しました。今、CBPRの事務局の立場で拝見していると、皆さんどこまでやったら正解なのかかわからないというのが正直なところだと感じています。実際、APECのCBPRの認証基準を[JIPDECのWebサイト](#)で公開していますが、まずはぜひご覧いただいて、自社のデータがどう管理されているのか、どのデータが越境しているのかなどを明確にしていきたいと思えます。その中で自己評価を行い、明らかになったものに対して、次のステップとしてCBPR認証を取得するのも有効な手段です。実際の審査では、CBPRの審査員が審査を行い足りない部分や気が付かなかった部分を指摘、改善をお願いする流れになりますので、自社が保有するデータの管理・活用に関して内部でも対外的にも明確にできるメリットがあると思えます。プライバシーマークやISMSなど色々な認証制度がある中で、自社がCBPR認証を視野に入れるべきか検討されている企業の皆さまには、データの越境があるか否かでご判断いただき選択肢として検討いただくのがよろしいかと思えます。

近頃、JIPDECは諸外国の方々と意見交換をする機会も多く、CBPRのアカウントビリティ・エージェント（AA）として各国のご招待を受けてお話する機会も多くあります。もちろん国内の事業者様からCBPR取得に関するお問い合わせも多くいただきますが、海外からの問い合わせも増えており、興味をお持ちだということを感じています。今後は認証企業が世界規模で増えていくと予想されます。私たちが海外の企業を選ぶのではなく、海外の企業から私たち日本の企業が選択されるためのツールとしても有効になってくるのではないかと期待しています。

**松下** 実際にCBPRをとられた事業者様の中には、まずは自社内でチェックしてみて、自社が国際的に通用するガバナンスを保持しているのかどうかを確かめたいといった声もいただきました。取得するしないに関わらず、チェックシート等はお試しいただけると良いかと思えます。

それでは、最後に松岡先生、藤原先生から本日のセミナーを総じて一言お願いいたします。

**松岡** 海外のデータ移転については、皆さま悩むところが多いと思えますので、あまり担当者おひとりで抱え込まず、まずはお気軽にご相談いただければと思います。

**藤原** 以前、個人情報保護委員会から依頼を受けて海外の個人情報保護法制、特に海外の監督機関の執行事例などを調査しましたが、やはり海外は日本に比べてセキュリティを含む安全管理措置が不十分であるなどとして厳格に執行するような事例が多いと認識しています。このような海外の傾向は今後も続くと思われ注意が必要ですが、一方で、やはりデータの利活用も重要です。データの利活用による事業を進めていく中で貴社の守り方について、不明点等ございましたらぜひ個別にご相談ください。

## パネリスト



渥美坂井法律事務所 弁護士 松岡 史朗氏

2005年京都大学法学部卒業。

2006年弁護士登録。

2016年から渥美坂井法律事務所・外国法共同事業にて執務。

2019年から一般社団法人日本DPO協会 顧問、2020年からステート・ストリート信託銀行株式会社 社外取締役（監査等委員）。



渥美坂井法律事務所 弁護士 藤原 理氏

2004年東京大学経済学部卒業。

2007年早稲田大学大学院法務研究科修了。

2009年弁護士登録。

オリック東京法律事務所・外国法共同事業にて執務後、2014年から渥美坂井法律事務所・外国法共同事業にて執務。株式会社海外需要開拓支援機構（クールジャパン機構）へ出向し、2015年コンプライアンス室長就任。

2018年コーネル大学ロースクール修了。

主な取扱分野は、データ法制（GDPR/個人情報保護法）、投資関連業務・M&A、一般企業法務、紛争解決等。



JIPDEC 認定個人情報保護団体事務局

主任研究員 大下 奈美

企業の情報システム部門の責任者として、インフラ管理、IT戦略、IT統制等に携わる。Pマーク、ISMS等の第三者認証事務局業務を多数の企業で行う。

2020年からJIPDECプライバシーマーク審査員。ISO審査員補資格等を複数保有。2024年より現職。

経済産業省、個人情報保護委員会の受託事業に従事するほか、CBPR普及啓発事業に携わる。

## モデレーター



JIPDEC 電子情報利活用研究部 調査研究グループ

グループリーダー 松下 尚史

青山学院大学法学部卒業後、不動産業界を経て、2018年より現職。

経済産業省、内閣府、個人情報保護委員会の受託事業に従事するほか、G空間関係のウェビナーなどにもパネリストとして登壇。その他、アーバンデータチャレンジ実行委員。

実施業務：

- ・自治体DXや自治体のオープンデータ利活用の推進
- ・プライバシー保護・個人情報保護に関する調査
- ・ID管理に関する海外動向調査
- ・準天頂衛星システムの普及啓発活動 など

本内容は、2024年9月20日に開催されたJIPDECセミナー「グローバルビジネスにおけるデータの利活用と保護～データ越境移転ルールの最新動向～」でのディスカッションを取りまとめたものです。