【講演レポート】JIPDEC セミナー

法制度動向を踏まえた今後のデータ管理の留意点～事前の質問を中心に～

牛島総合法律事務所
弁護士　影島　広泰氏

本講演では、今後のデータ管理の留意点について事前にいただいた多くの質問を踏まえ、４つのポイントに分けて解説します。

データ管理環境の変化と必要な対応

海外事業者への委託と提供について

海外のクラウドサービスを利用する場合の個人情報保護法（以下、「保護法」）の規制対応については、クラウドサービス提供事業者（以下、「ベンダー」）に個人データを提供するか否かにより異なります。提供の場合は、保護法第 28 条に基づき、本人の同意を取る、相当措置としてベンダーと契約を締結するなどの対応をとる、または EU や英国など十分性認定が認められている国の企業と取引を行うなどで対応します。相当措置や十分性認定国の場合、第三者提供であれば本人同意が、委託の場合は委託先の監督がそれぞれ必要となります。また、提供していない場合であっても、安全管理措置上の対応として、外的環境の把握が必要です。

通則ガイドラインでは、提供は「自己以外の者が利用可能な状態に置くこと」と定義しており、該当の個人データ／個人情報をベンダーが利用可能か否かで判断します。ベンダーのサーバーにデータを保存した場合、ベンダー自体がデータを取り扱わなければ提供したことにはなりません。取り扱わないと判断する基準は、①ベンダーが保存された個人データを取り扱わないことが契約で定められ、②適切にアクセス制御を行っている場合等が挙げられます。この２つが満たされていればベンダーは利用可能ではない、と考えられています（いわゆる「クラウド例外」）。

提供の基準について、政府の公式見解では「一律の回答が難しい」とされていますが、結論としては、「ベンダーがサーバーに保存された個人データの編集、分析等処理を行う場合は、ベンダーが当該データを取り扱わないこととなっている場合には該当しない」と考えられています。提供か否かの判断は難しいのですが、個人情報保護委員会（以下、「委員会」）Q&A で、ベンダーが保守サービスの委託中にインシデント対応等で個人データを閲覧する機会があった場合、記録・閲覧まで行うことが可能であれば「提供」に該当すると例示されており、提供についてはケースバイケースで考えなければなりません。

契約条項に限らず安全管理体制などを確認し、ベンダーが利用可能になっていない状態か、クラウド例外（提供に該当しない）か判断することが法的な結論となります。

第三者提供と委託の違い

収集情報を提供先が利用目的外の目的で利用する場合は「第三者提供」となるため本人同意が必要です。一方、自社の利用目的のために委託先企業がデータを利用する場合は「委託」となります。

なお、ベンダーが自社の技術改善のために委託元のデータを利用する場合、一見ベンダーの利用目的で使っているように受け取れますが、委託元がベンダーの技術向上も含めて委託していると整理できれば、個人データの利用は「委託」の範囲内と捉えることができます。

外的環境の把握の義務

安全管理措置の一環として「外的環境の把握」が令和 2 年改正法（2022 年施行）で追加されました。海外で個人データを取り扱う場合、その国の法規制を調査し、①強い Government Access（政府が民間企業のデータにアクセス可能な規制）があるか、②Data Localization（データの国内保管の義務付け）を調査したうえで安全管理措置を講じなければなりません。米国は両規制がなく特段何もしなくてもよいとされていますが、中国の場合は①、②ともに規制があるため、適切な安全管理措置が必要です。

具体的な対応についてガイドラインに例示はありませんが、同様の対応が GDPR の TIA（Transfer Impact Assessment）に示されているので、参考にしてください。（図 1）

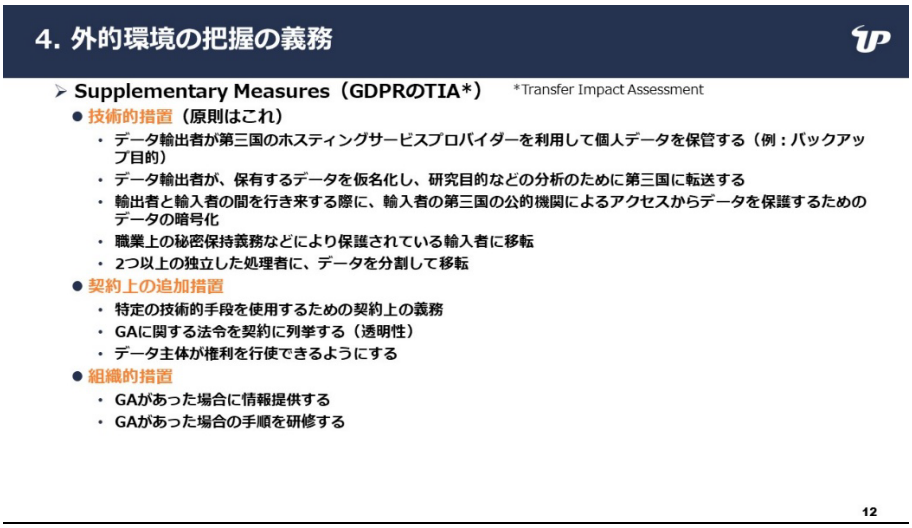

図 1. GDPR の TIA

企業における生成 AI 活用の留意点

保護法と生成 AI 規制について、2023 年 6 月に委員会が個人情報取扱事業者に対し「生成 AI サービスの利用に関する注意喚起等」を公表しました。（図 2）

要約すると、個人情報を入力する場合は利用目的の範囲内であること、また生成 AI サービス提供企業が機械学習に利用しないこと等、を十分に確認することが必要です。

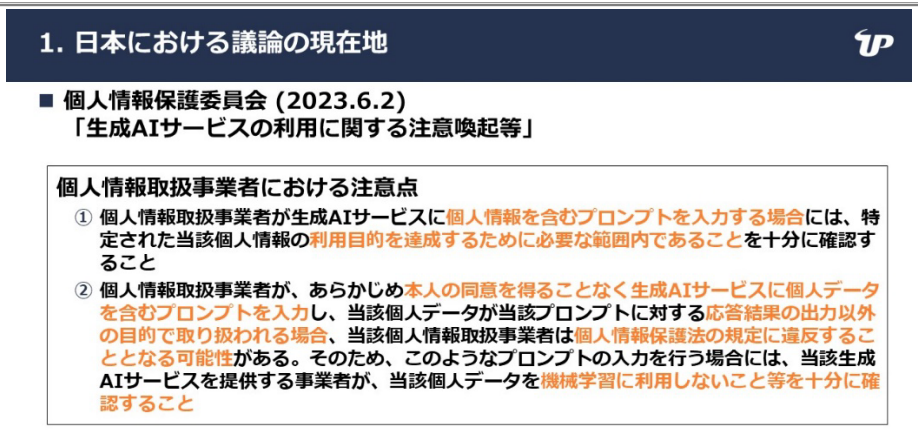

図 2. 個人情報保護委員会「生成 AI サービスの利用に関する注意喚起等（2023 年 6 月）[16]

①について、個人データをプロンプトに入れた場合、生成 AI 企業が機械学習で利用可能の場合は「提供」となりますが、海外生成 AI 企業と相当措置に関する契約締結は困難と思われるので、入力したプロンプトが生成 AI 企業の機械学習に利用されない状態で利用することが一般的には必要と考えられます。

プロンプトに個人情報を入力する際の規制

利用目的については保護法第 17 条で「できる限り特定」が必要とされており、情報分析にあたりインプット／アウトプット情報がどういうものか、を具体的に特定する必要があります。たとえばターゲティング広告の場合、単に「広告配信のために利用する」と説明するのではなく、「取得した閲覧履歴等の情報を分析し、趣味・嗜好に沿ったサービスに関する広告のために利用する」と具体的に説明する必要があります。これは生成 AI の場合も同様で、何のためにどのような情報を入力・分析しているかの特定と通知が必要です。重要なのは、生成 AI に個人情報を利用する場合の利用目的を特定することであり、ベンダーへの提供については、機械学習に使用しないサービスを選択すれば多くのケースでクリアできると考えられます。

仮名加工情報の活用

仮名加工情報は、利用目的が関連性のある範囲内に限定される個人情報とは異なり、当初の利用目的とは異なる利用目的を新たに設定することが可能なので、たとえば利用目的の変更のために本人の同意を取得することが難しい場合は、個人情報を仮名加工情報に変換すれば利用範囲が広がります。

個人情報を使った機械学習

個人情報を使って学習用データセットを作成し、その後学習用プログラムにより学習済みモデルを生成した場合、学習済みパラメーターが特定の個人との対応関係が排斥された統計情報であれば、個人情報には該当しません。この場合、学習のプロセスについて利用目的の特定は通常不要であり、機械学習への利用が可能です。一方で、LLM（大規模言語モデル）の場合、たとえば氏名を単語として覚えさせた場合、生成された学習済みモデルが個人情報となるケースがあります。このように、特定の個人との対応関係が排斥されない場合は、個人情報の利用に当たることになりますので、利用目的の特定が必要

となります。学習用データセットに用いる個人情報を仮名加工情報に処理し、利用目的（機械学習に利用する旨）を明確にすればよいのではないでしょうか。

生成 AI を業務で利用する際の法的問題点と対応策を図 3 にまとめています。

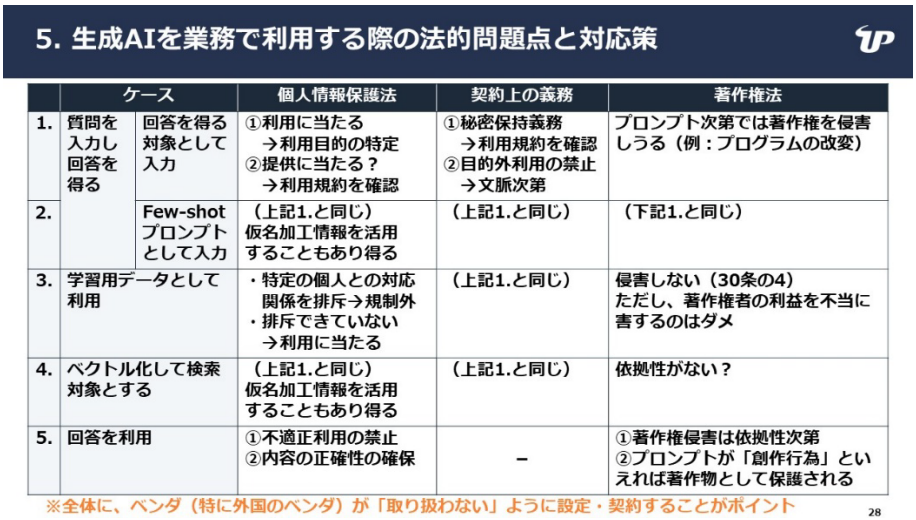

図 3. 生成 AI を業務で利用する際の法的問題点と対応策

Cookie 廃止後のマーケティング

保護法上の規制

保護法上、委託と第三者提供の切り分けには情報処理の仕方により細かいルールがあります。また、個人関連情報についても第三者提供先が個人データとして取得する場合は、本人同意を得て取得する必要があります。

電気通信事業法上の規制

電気通信事業法の場合、第 3 号事業を営む者（EC サイト、オンラインショッピングモール運営事業者などが該当）は利用者情報の外部送信について、通知公表、同意取得、オプトアウトのいずれかの対応を講じる必要があります。

利用者の PC やスマホに記録された利用者に関する情報が Cookie に保存されます。この Cookie 情報などを外部のサーバーに送信するよう指令することを「情報送信指令通信」といいますが、この指令通信にあたっては利用者に通知または公表等しなければなりません。

現在は、マーケティングに Cookie の代替としてコンバージョン API、デバイス・フィンガープリント、コンテキストベース、ファーストパーティ・データ等を使用して、広告配信や行動分析が行われていますが、これらの仕組みも技術的には異なっても、「利用者の意思に寄らず第三者に自信の情報が送信されている場合」に該当し得るため、規制対象となります。

保護法上の第三者提供と委託の切り分け

たとえば、単体では個人情報に該当しないメールアドレスも提供元の基準で顧客データと紐づけされていれば、個人データの提供となります。ベンダーが①独自の利用目的で個人データを利用する、②他の委託元のデータと区別せずに混ぜて取り扱う、③独自に取得した個人データや個人関連情報と本人ご

とに突合する場合は、いずれも第三者提供となるため、本人の同意が必要となり、①~③いずれも該当しなければ「委託」となり、同意は不要となります。

図 4 は委託か第三者提供のいずれに該当するかの例となります。

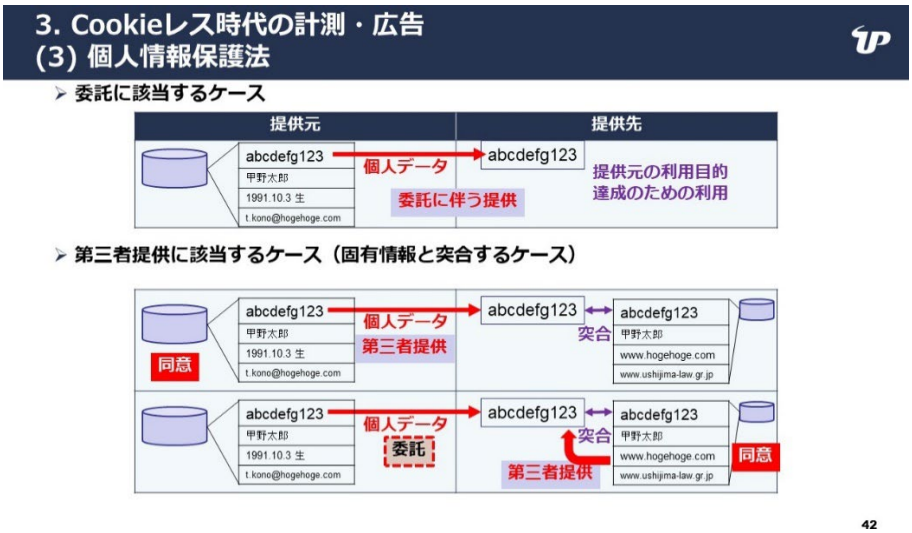

図 4. 個人情報保護法における委託と第三者提供の違い

なお、提供か否かに関わらず、利用目的の特定と通知等の規制は適用されるので、情報の分析にあたっては、インプット、アウトプットの具体的な特定が必要です。

各国個人情報保護法制動向と留意点

外国の第三者への個人データ移転

外国にある第三者への個人データ移転方法のうち、「相当措置」として規則が定める基準適合体制を整備している企業の対応について説明します。

実務としては、①契約状況やグループ内規で保護法を遵守していること。たとえば、海外企業に特定の業務を委託する際、日本法を守るという契約を締結すれば個人情報を提供できます。または②APEC CBPR 認証を取得するという方法があります。

保護法上、越境データ移転については EU や英国のように十分性認定を受けている国の企業への移転か、または APEC CBPR 加盟国の企業であれば移転が可能となります。基準適合体制を整備している場合は、外国にある第三者にはあたらず国内第三者と同じ扱いとなり、委託や共同利用が可能となります。

APEC CBPR 認証は、APEC がその企業が個人情報保護法規制やプライバシーを守っていることを認証するシステムです。日本はアカウンタビリティ・エージェント（AA）である JIPDEC の審査を受けて CBPR 認証を取得できます。

現在は APEC 域内に限らず、グローバル CBPR という、国際的な仕組みにする動きがあります。

米国では IBM や SalesForce など多くの企業が CBPR 認証を取得しているので、日本企業は認証取得企業にデータを越境移転することが可能です。

保護法ガイドラインでは日本の提供元企業が CBPR 認証を取得していれば委託については基準適合体制を整備していると判断されるため、海外委託先への移転が可能となります。CBPR 認証を取得すれば海外企業への委託がやりやすくなりますので、日本の企業も取得を検討されてはいかがでしょうか。

牛島総合法律事務所　　弁護士　影島　広泰氏

一橋大学法学部卒業、03 年弁護士登録、牛島総合法律事務所入所
自らアプリ開発を行う等 IT に精通し、IT システム・ソフトウェアの開発・運用、個人情報・プライバシー、ネット上のサービスや紛争に関する案件を中心に、企業法務の第一線で活躍。
The Best Lawyers™ in Japan 2024 の Telecommunications Law 部門の Lawyer of the Year 2024、Fintech Practice 部門及び Information Technology Law 部門選出（2023 年 4 月）
Thomson Reuters「ALB Asia Super 50 TMT Lawyers 2021」選出（2021 年 8 月）
【著作】
「法律家・法務担当者のための IT 技術用語辞典＜第 2 版＞」（商事法務）
「22 年施行　情報の『利用』を重視する　個人情報保護の規制強化」（週刊東洋経済、2021 年 3 月 6 日号）ほか多数

本内容は、2024 年 2 月 27 日に開催された JIPDEC セミナー「個人情報保護法規則/ガイドライン改正と、今後のデータ管理の要諦」講演内容を取りまとめたものです。