Miura&Partners

Data and Digital Insights Vol.9

クラウド例外の射程と生成 AI 時代の「取扱い」（後編）

2026 年 2 月 3 日

弁護士 中島 稔雄
弁護士 小 倉　徹

目次

1. はじめに

前編では、日本の個人情報保護法における「取扱い」概念、いわゆる「クラウド例外」の解釈について再考しました。後編では、その際の整理を生成 AI（LLM）によるデータ処理に対する当てはめを行い、最後に今後の「委託」に関する規律の改正見通しについても言及します。

2. 試論 2 ― LLM における「意味」と「推論」の実体

(1) LLM とクラウドサービス

今日の LLM の多くは、クラウドサービスとして提供されています。LLM による計算処理のためには、高性能な GPU と GPU に割り当てられた大きなメモリ領域が要求され、これらの計算手段を継続的に供給するための電力や通信手段を考えると、クラウドコンピューティングでの処理と相性がいいのは当然と言えます。

したがって、本稿においてはクラウドサービスとしての LLM を念頭に、生成 AI とクラウド例外の交錯について考えてみることとします。

なお、福岡真之介弁護士は、生成 AI においても、SaaS 的なものと、PaaS 的（あるいは IaaS 的）なサービスを区別して論ずるべきであると述べられており[1]、これには完全に賛同いたします。PaaS や IaaS の環境で、クラウド上のマシンリソースによる計算処理の提供のみを受けている場合、クラウドサービス提供事業者が提供するのはペイロードとしてのデータへの計算のみであり、前編において述べたところを敷衍して、クラウド提供事業者による「取扱い」はないと考えております。一方で、生成 AI における PaaS の定義には難しいところもあり、ユーザ事業者に割り当てられたクラウド（物理的または論理的に切り分けられたテナント領域）のみで処理が完結しない、つまり、パイプライン処理、プロンプトの保管・監査、その他の管理機能、GUI といった機能はユーザ事業者の管理領域で完結するものの、主要な LLM による処理については、クラウド提供事業者が管理する LLM を API 経由で呼び出して処理させている場合もあるように思われます。そのような場合にも「PaaS ではアプリ領域（生成 AI）はユーザが管理」していると言えるのかは、サービスの内容を十分に観察した上で判断する必要があるかと思います。

また、LLM にはプロンプトを学習のために利用することを認めるものがありますが、学習のプロセスへの利用については、クラウド例外の適用の余地がないと思われるため、これも除外して、通常のプロンプトの処理（順伝播）を念頭に検討します。

(2) LLM における「意味」と「推論」の実体

さて、まずは、そもそも LLM はプロンプトをどのように処理しているのかを概観したいと思います。

入力されたテキストは、まずトークン（単語や文字の断片）に分解され、トークンとして LLM に入力され、あとは、数値ベクトルとして、過去の学習で調整されたパラメータ（重み）を用いて繰り返し行列演算を受けます。これは、今日においては良く知られるようになりましたが、トークン（言葉）の次に来る確率が最も高いトークン（言葉）を算出するプロセスです。そこには、人間のような「認識」や「理解」という認知プロセスは存在せず、入力値を変換して出力値を弾き出す決定論的・純粋関数的な計算処理であると言えます[2]。

(3) 「取扱い」該当性に関する当てはめ

ア. 要件再検討

前編では、SaaS のソフトウェアによるデータ処理が「取扱い」に該当するか否かの判断基準について、データの内容に着目した処理を目的とせず、汎用的なデータ処理手段であるか否かとしました。

[1] https://note.com/shin_fukuoka/n/n4a964b4a41bd

[2] 実際に演算の結果として出力されるのは確率分布であって、サンプリングによる揺らぎが発生することから、同一の入力に対して同じ出力が返されるわけではありません。したがって、関数による計算結果そのもの LLM のアウトプットだと捉えるとやや誤謬を含むこととなります。

ただ、この要件には、LLM による処理に適用するには不十分なあいまいさが残ることを認めなければなりません。

まずは、この「目的」を誰の立場に基づいて判断すべきか、という問題が生じます。利用者の目的によって決まるという考え方もありますが、私としては、ソフトウェアの処理の実態で決まるべきであると考えており、基本的にはソフトウェアを設計したサービス提供事業者の目的を中心に据えつつ、機能的に何が行われているのかを補助的に参照するのが良いのではないかと思います。

例えば、汎用的な表計算ソフトが SaaS 提供されたとして、それを利用者が個人情報データベースの構築基盤として用いるという場面が考えられます。これは、前編で述べたような個人情報の管理を目的とするサービスとは異なるものであり、一般的な計算ソフトとして提供されており、実際に個人データの管理に特化した機能がないのであれば、ユーザ事業者が入力したデータに含まれる個人データの「取扱い」には該当しないと考えます。

イ．当てはめ

上記のように考えた場合であっても、LLM による処理をデータの内容に着目した処理か否か論理的に判断するのは非常に困難です。

LLM は、自然言語の入力に対し、自然言語の出力を返すという、極めて汎用的なサービスであり、固有の処理目的を備えたソフトウェアではないと評価することはできると思います。

その一方で、学習の結果としてモデルの中に蓄積された「重み」には、固有名詞や人名を含むあらゆる単語やコンテクストの意味座標とその距離の情報が凝縮されており、よりコンテクストに沿った出力を返すという目的のためにモデルが改善されつづけてきました。LLM の急速な進歩の背景には提供事業者間の競争があり、人間的な目的の達成度合いをさまざまな観点から測定するために用意されたベンチマークの結果で競いあって、モデルを最適化してきた果てに現在の LLM が存在すると言えると思います。これを考えると、LLM の提供には、入力されたデータについて、あたかもその意味内容を人間が把握・理解した結果のように、出力するという目的が内在しており、その達成の手段の一部として、入力されたデータに含まれる固有名詞や人名を識別して文脈を把握するという機能は当然に内包されているとも評価することができると思います。

このように考えると、その処理内容がいかに数理的であって汎用的であっても、LLM によるデータ処理は、データの内容に着目した処理のひとつの形であり、投入されたデータの中に個人データが含まれている場合には、LLM を提供する事業者が個人データを取り扱っていると考えるのが自然ではないかと考えられます。

(4) 不正監視のための処理と「取扱いの委託」

上記の LLM によるデータ処理とは独立した生成 AI サービス特有の論点として、Abuse Monitoring（悪用監視） があります。多くの提供事業者は、Usage Policy という形で、違法行為、権利侵害行為、及び倫理的に問題のある方法等による利用を禁止し、これを防ぐために、入力されたデータを一定期間保存し、内容を精査する場合がある旨定めています。 この処理は

平文での解析を伴い、場合によってはクラウド提供事業者の従業員による人的レビューがなされる場合もあります。

このような提供事業者によるデータ保存と解析が「取扱い」に該当するという指摘もなされており、実際のところ、これは「取扱い」に他ならないと考えられます。提供事業者によるこのような取扱いが、個情法 18 条 3 項 2 号／27 条 1 項 2 号「人の生命、身体又は財産の保護のために必要がある場合」等の例外事由に該当すると整理可能な場合があるという指摘も見られます[3]。

たしかに、不正監視の対象が人の生命、身体又は財産の保護のために必要がある場合に該当するような事態に限定されていれば上記のような整理の余地もあろうと思いますが、実際の禁止事項には、人の生命、身体又は財産の保護に直接には関連しない、より高度に公益的・倫理的な観点から禁止されている事項[4]やサービスの可用性維持を目的とした事項も見られますので、「提供」に該当する（その上で委託該当性や基準適合体制を満たすかについて検討する）と整理せざるを得ない場合が多いと考えられます。

この点に配慮し、一部、申請に基づき個別の合意により Zero Data Retention（ZDR）とするオプションを用意するサービスも見られますので、これらの利用も検討の対象になるかと思います[5]。

3. 現状とこれから（委託に関する規律の見直し）

生成 AI のリスクや法的問題について検討する際に、実はその中の多くが、生成 AI 固有のものではなく、クラウドサービス利用に伴うリスクや法的問題ではないか、と思われる場面が少なくありません。その点が十分に整理・解決されないままクラウドの受容が進んできましたが、生成 AI の導入という段階で改めて立ち止まって考えてみると、「そもそもクラウド上でのデータ処理について、どう整理すべきだったのか」が分からなくなっている、という状況に直面している事業者も多いのではないかと拝察します。

生成 AI と提供規制の問題が議論されるようになってから数年が経過し、生成 AI はいよいよ実用段階に入り、広く花開いてきました。それでもなお、本論点については、どのように整理すればよいのかが分からない、という感覚が拭えません。そもそも、前編でも述べたとおり、現時点において、クラウドサービスによるデータ処理が、データに含まれる個人データの「取扱

[3] 齋藤浩貴・上村哲史『生成 AI と知財・個人情報 Q&A』（商事法務、2024 年）195 頁。

[4] 主要なサービスの usage policy を見ると、性的なコンテンツの生成、セーフガードの回避、特定の場における個人の感情に関する推測、学問上の不正行為、高リスクな領域や重要な意思決定に関する（Human-in-the-loop でない）自動化、誤情報の作成、選挙活動への利用など、非常に広汎な制限事項が定められており、これらも不正監視の対象になると考えられます。

[5] 前掲 1 は、「ここで矛盾を感じるのは、人間による不正利用防止のためのモニターは、個人情報の入出力の不正利用を防ぐためにされているのに、クラウド例外にならないとなると、多くの企業は人間によるモニターを外す選択をするようになり、個人情報を悪用するための試みがかえって広がってしまいかねないことです。個人情報を守るべき個人情報保護法が、個人情報の悪用などの不正行為を防止しようとする活動を抑止してしまうことになるのは、腑に落ちない気がします。」と述べており、非常に重要な指摘かと思います。

い」に該当するかについて、ユーザ事業者の立場で明確な線を引くことは非常に困難です。このように不明確な状態が続いていること自体が、まさに問題であると言えるかと思います。

その一方で、クラウドの受容が深まってきた現実がある中で、今後の明確化の方向性次第では混乱が生じ得るという点は、確かに否定できません[6]。このような規律を保守的に解釈してクラウドサービスの利用自体を差し控えたり、自らオンプレミス環境を管理・維持する体制に移行する選択をしたりすることが、本当に望ましいのかについては疑問があります。

このジレンマを解決するためのひとつの方法は、委託として捉えた上で、委託に関する規律を見直していくことかと思います。

令和 8 年 1 月 9 日に公表された「第 347 回個人情報保護委員会　個人情報保護法　いわゆる 3 年ごと見直しの制度改正方針（案）について」[7]の中で、データ処理等の委託を受けた事業者に関する規律の見直しについての方針案が示されました。そこでは、「個人データ等の取扱いについて、実質的に第三者に依存するケースが拡大」しているという状況を踏まえ、「取扱いを委託された個人データ等を当該委託を受けた業務の遂行に必要な範囲を超えて取り扱ってはならない旨の義務を委託先に明文規定により課す」こととした上で、①委託先が取扱いの方法を決定しないケースにおいては、②委託契約において、取扱いの方法の全部について合意し、かつ③委託先における取扱いの状況を委託元が把握するために必要な措置等について合意した場合には、「当該委託先に対しては、法第 4 章の各義務規定の適用を原則として免除する」としています。

まず、「①委託先が取扱いの方法を決定しないケース」という要件については、「委託先が委託元から指示された方法で機械的に個人データ等を取り扱うのみの場合」と注記されているため、ソフトウェア的な自動処理の多くは該当すると考えられます。

「②委託契約において、取扱いの方法の全部について合意」という要件については、どのような粒度で特定した上での合意が必要なのかが検討の余地があります。「取扱い」は個人情報の「取得」から「廃棄」に至る全ての活動（入力、蓄積（保管）、編集・加工、出力、提供、消去等）を包含する概念であるという原則に立ち戻り、これらの活動のうち、どれを含むのかを明示すれば足るということであれば、それほど困難ではないように思われますが、本稿で述べたような処理の内容や目的に至るまでを合意する必要があるとすれば、これはやはり非常に困難であると言わざるを得ません。合意すべき事項を明確化し、契約・規約における定型的な記載として標準化される必要があると考えられます。

「③委託先における取扱いの状況を委託元が把握するために必要な措置等について合意した」という点については、「漏えい等が生じたことを知ったときに委託先が委託元に対して速やかにその旨を報告すること等を想定しているが、その他の具体的な内容は、制度が円滑に運用さ

[6] 一般社団法人日本経済団体連合会（経団連）デジタルエコノミー推進委員会データ法制 WG「個人情報保護法の 3 年ごと見直しに対する意見」（令和 6 年 1 月 31 日）において、「いわゆる「クラウド例外」については、現在の Q&A のアプローチに基づいて実務に定着し有効に機能しているところ、追加の条件等の付加には慎重を期し実務上の混乱なきよう進めるべき」との指摘がありますが、まさにそのとおりかと思います。

[7] https://www.ppc.go.jp/files/pdf/260109_shiryou-1-1.pdf

れるよう、改正の趣旨を踏まえつつ、委員会規則等で定めることを想定。」との注釈がありますので、クラウド利用等の実態を踏まえた明確化がなされるものと思われます。

「法第 4 章の各義務規定の適用を原則として免除する」という効果についても、「取扱い方法を決定する権限の存在を前提としない規定（委託を受けた業務の遂行に必要な範囲を超えて取り扱ってはならない旨の義務及び安全管理に係る義務）のみ適用する。」との注記にて、個人情報取扱事業者としての義務のすべてが免除されるわけではないとの留保がなされています。趣旨は論理的かと思われ、例示されている委託業務の範囲を超える個人データ利用の禁止、安全管理措置の実施、あとは委託元への事故・漏えい報告等が残ることは当然と思われますが、実際に何が免除の対象から除外されるのかは注視する必要があります。

重要な点として、これは委託先の義務の免除であり、委託元の監督義務等を緩和するものではありません。しかし、このような規律の見直しにより、クラウドサービスの利用においてクラウド提供事業者が、委託先という法的位置づけを受け入れることが、より現実的となります。したがって、これは、クラウド提供事業者を、委託を通じた個人情報保護法による統制に組み込むためのひとつの重要なステップであると推察されます。

当該方針案と合わせて公表された「『“個人情報保護法 いわゆる 3 年ごと見直しに係る検討”の今後の検討の進め方」に対して寄せられた意見の概要」の「個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方（ガバナンスの在り方）」という項目[8]においては「個人情報取扱事業者等（委託元）からデータ処理等の委託を受けた事業者である委託先が子会社等ではなく委託元よりも強い企業である場合、例えば、クラウド事業者等で個人情報の漏えいがあった場合に、委託元に現実に法執行することは困難であり、個人情報の取扱いの適正化にも資することにならない。適切な委託先の選定と監督者として委託元が行うべき行為規範の内容を具体化して義務違反とされる場合を限定する」べきであるという指摘がある一方で、「委託元による委託先の管理監督義務や、委託を受けた事業者の義務規定等の在り方については、実態を踏まえ、混乱を招かない規律とすべき」であるとの指摘や、「委託元の義務を軽減したうえで委託先の義務の在り方を考えるということであれば、もう少し具体的なケースを念頭に置いたうえで、実務実態に照らしてどのような影響があるのかも踏まえた慎重な議論が必要」との意見もあることから、委託元の義務軽減や、委託先への追加的な義務の設定については、必要性は認識されつつも先送りされたものと考えられます。

これらの規律の見直しが完了した後には、SaaS の利用の多くについては「委託」という概念に取り込まれた上で、現実的、データの安全管理のために実効的で、かつ明確な規律が、委託元と委託先の双方に対して課されることが期待されます。

4. さいごに

委託に関する規律の改正によって、「クラウド例外」という概念は、いずれその社会的役割を終えるのかもしれませんし、筆者としてはその方が望ましいと考えます。ただし、制度の改正

[8] https://www.ppc.go.jp/files/pdf/260109_shiryou-1-3.pdf （26 頁）

にはいくらかの時間を要することも見込まれるため、本稿が、制度改正に至るまでの判断の一助となれば幸いです。

もっとも、仮に委託に関する規律が見直された場合であっても、IaaS や PaaS の利用が「委託」に該当し得るのか（あるいは限定された「クラウド例外」として残存するのか）という問題は、なお残存するものと考えられます[9]。その意味では、本稿で示した考え方にも、引き続き一定の検討余地が残されているといえるでしょう。

なお、本論考の作成にあたっては、引用した論考以外にも多くの先行する論考を参考とさせていただきましたことについて、御礼申し上げます。また、技術的背景について可能な限り正確を期したつもりではありますが、誤りを含む可能性があることを、あらかじめお断りしておきます。

[9] 前掲注[6]においても、「現行のいわゆるクラウド例外の考え方を変更するものなのか、そうではなく追加的なものなのか、「データ処理等の委託」とは「個人情報の取り扱いの委託」とは違うのか、違うとすればどう違うのか、明確にする必要がある。」との指摘があります。

本ニュースレターは、法務等に関するアドバイスの提供を目的とするものではありません。
具体的な案件に関するご相談は、弁護士等の専門家へ必ずご相談いただきますよう、お願いいたします。
また、本ニュースレターの見解は執筆者個人の見解であり、当事務所の見解ではありません。