生成AIと個人情報保護法
（クラウド例外を含む個人データの第三者提供を中心に）

松　尾　剛　行

第１章　はじめに

2023年春のChatGPTブーム後、本稿執筆時点である2024年夏の段階では、生成AIの利用が定着し、生成AIが広く利用されている。筆者はこれを「イン

フラ化」と呼んでいる[(1)]。例えば、2030年には生成AI市場は約1100億ドル規模にまで拡大するという予測が公表されている[(2)]。

ここで、生成AIの利活用との関係で重要な問題とされているものの一つが個人情報の保護に関する法律（以下「個人情報保護法」という。）、とりわけ、同法27条のいわゆる第三者提供規制との関係である。即ち、生成AIサービス利用企業（以下、サービス利用企業を総称して「ユーザ」という。なお、本稿では、ユーザ及び次に述べるベンダのうち、「個人情報取扱事業者」（個人情報保護法16条2項）であるものを念頭に置いている。）が生成AIに個人情報を含むデータを投入することが、生成AIサービス提供企業（以下、サービス提供企業を総称して「ベンダ」という。）に対する個人データの第三者提供ではないかが問題となっている。つまり、ユーザが、生成AIに「個人データ」（個人情報保護法16条3項）を投入することを通じて、ベンダに対して個人データを第三者提供しているとみなされ、第三者提供に関する規制が適用される、すなわち、原則として本人同意が必要となるのではないか（個人情報保護法27条1項柱書）、という問題意識が存在するのである。

ここで、生成AIサービスの典型例であるChatGPT等は、いわゆるクラウドサービス[(3)]として提供されている。個人情報保護法の第三者提供規制とクラウドサービスに関しては第2において後述するクラウド例外と呼ばれる例外が存在することから、生成AI利用に関する個人情報保護法の第三者適用規制につき、クラウド例外を利用することができないかが論じられている。

このような状況を踏まえ、本稿においては、このような生成AIと個人情報保護法の間の重要問題である、クラウド例外を含む個人データの第三者提供規制について検討する。

なお、本稿は、生成AIと個人情報保護法の全面的検討を行うものではない。例えば、2023年6月2日には、個人情報保護委員会が「生成AIサービスの利用に関する注意喚起等について」（以下「生成AI注意喚起」という。）を公表している[(4)]。注意喚起においては、第三者適用規制以外についても、例えばChatGPTを提供するベンダであるOpenAIに対するものとして、要配慮個人情報の取得の論点、ユーザに対するものとして、利用目的の論点等が提起されている。加えてAIサービスが外国企業によって運営されていれば外国第三者提供（個人情報保護法28条）の論点についても検討が必要である。もっとも、本稿

はこれらの、「(国内) 第三者提供規制」以外の個人情報保護法上の論点を論じるものではない[5]。

第 2 章　クラウド例外とは

第 1 節　概説

いわゆるクラウド例外は第三者提供規制につき、一定の要件を満たすクラウドの利用を第三者提供ではないとみなすものである。つまり、クラウドサービスの利用に伴い、クラウド上に個人データを保管することが、第三者提供として原則として本人同意を要するのか、という問題につき、一定の要件を満たせば第三者提供ではなく、本人同意を不要としたものである。

第 2 節　前提となる第三者提供規制

個人情報保護法 27 条は、個人データの第三者提供について以下のいずれかの根拠が充足されることで正当化されることを求める。

- 同意（同法 27 条 1 項柱書）
- 法令等（同法 27 条 1 項各号）
- オプトアウト（同法 27 条 2 項）
- 委託（同法 27 条 5 項 1 号）
- 事業承継（同法 27 条 5 項 2 号）
- 共同利用（同法 27 条 5 項 2 号）

そして、法令等であれば「他の法令により個人情報を第三者へ提供することを義務付けられている場合」か、「他の法令に、個人情報を第三者に提供することについて具体的根拠が示されている（が提供すること自体は義務付けられていない）場合」が挙げられる[6]。このような法令が存在すれば法令等を根拠に（本人同意がなくても）第三者提供を行うことができるが、そのような場合は少なくともクラウドを利用する場合全般にあてはまるものではない。

また、オプトアウトは実務上、一定の場合（例えば、住宅地図会社が地図上に所有者の氏名を記載する行為）には利用することもあるものの、いわゆる「名簿屋」対策として届出等の規制が厳しいことから少なくとも一般的には利用されていない。

更に、事業承継は合併や事業譲渡等の場面では利用可能であるが、少なくと

もクラウドを利用する場合全般にあてはまるものではない。

加えて、共同利用については、「本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲」[7]でなければならない。なお、既にユーザの手元にある個人データを生成 AI に投入することを通じてベンダという第三者に提供する場合に、共同利用スキームを利用するのであれば、「既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合」として「当該共同利用は、社会通念上、共同して利用する者の範囲や利用目的等が当該個人データの本人が通常予期し得ると客観的に認められる範囲内である必要がある」[8]。そこで、例えば、グループ企業間で相互に個人データを提供し合う場面等、実務上共同利用がふさわしい場面も存在するものの、少なくともクラウドを利用する場合全般にあてはまるものではない。

上記の法令等、オプトアウト、事業承継及び共同利用を利用することが通例ではない場面において、第三者提供を正当化する方法としては、例えば本人同意を得るとか、委託スキームを利用することが考えられる。なお、委託の場合においては監督（個人情報保護法 25 条）が必要である。監督方法として、適切な委託先の選定、委託契約の締結及び委託先における個人データ取扱状況の把握が挙げられる（ガイドライン通則編 3-4-4）。実務上、個人データ取扱委託覚書（以下「委託覚書」という。）等を締結して監督することが頻繁に見られる。

第 3 節　クラウド例外が必要とされた背景

上記を踏まえると、クラウド上に個人データを保管し、管理する場合であっても、例えば本人同意を取得したり、クラウドベンダに対して「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当該個人データ」を提供した上で（個人情報保護法 27 条 5 項 1 号）、クラウドベンダを監督（個人情報保護法 25 条）する等、通常の第三者提供規制と同様に対応すれば良いだけのようにも思われる。

しかし、すべてのデータについて本人同意を得ることが現実的でないところ、クラウドベンダの中には監督のためのユーザ雛形での委託覚書の締結に応じてくれないところも多いという実情が存在する。その結果として、もし、同意スキームも委託スキームも使えないとすると、クラウドサービス上で個人データを保管・管理することができず、結局のところクラウドサービスを利用

できない（又はクラウドサービスを利用したければ個人データが含まれないよう注意しなければならない）、ということになってしまう。ますますクラウドサービスの利用が一般化する中、どのように整理することでクラウドサービス上で個人情報（個人データ）を保管管理できるようにするか、これがクラウド例外が必要とされた背景であった[9]。

第 4 節　クラウド例外の内容

⑴　Q&A7-53

クラウド例外を定めるのはQ&A7-53 であり、その内容は、以下において引用するとおりである（強調筆者）。

> **Q7-53** 個人情報取扱事業者が、個人データを含む電子データを取り扱う情報システムに関して、クラウドサービス契約のように外部の事業者を活用している場合、個人データを第三者に提供したものとして、「本人の同意」（法第 27 条第 1 項柱書）を得る必要がありますか。または、「個人データの取扱いの全部又は一部を委託」（法第 27 条第 5 項第 1 号）しているものとして、法第 25 条に基づきクラウドサービス事業者を監督する必要がありますか。
>
> **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のかどうかが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にはならないため、「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とは、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。なお、法第 28 条との関係についてはQ12-3 参照。

要するに、「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」「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のかどうかが判断の基準とな」るとする。

⑵　クラウド例外の適用要件

クラウド例外の適用要件、つまり、ユーザがクラウド上に個人データをアップロードしても、第三者提供（法第 27 条第 1 項）に該当しない場合とは、ベンダ（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、具体的には、ユーザとベンダ間の契約条項によって当該ベンダ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である[10]。

⑶　クラウド例外の効果

クラウド例外が適用されることの効果は、ユーザがベンダに個人データを（第三者）「提供」したことにはならないことである。その結果、同意スキームや委託スキームの利用は不要である。よって委託先に対して行うべき「監督」（個人情報保護法 25 条）をクラウドベンダに対して行うことも不要である[11]。

但し、Q7-54 が「クラウドサービスを利用する事業者は、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要があります」とするとおり、法的にはユーザ自身がクラウド上の個人データを取り扱っていることになるため、ユーザが安全管理措置（個人情報保護法 23 条）を講じなければならない。

⑷　クラウド例外のロジック

なぜこのようなクラウド例外が認められているのだろうか。

ここで、配送業者や倉庫業者等[12]につき、個人データを封緘して倉庫業者や配送業者に預けた場合、少なくとも中身の個人データについて、当該業者に個人データの取扱いを委託したとは言えないとされる。以下で引用するQ&A7-

35（強調筆者）は、「配送事業者を利用する場合、通常、当該配送事業者は配送を依頼された中身の詳細については関知しないことから、当該配送事業者との間で特に中身の個人データの取扱いについて合意があった場合等を除き、当該個人データに関しては取扱いの委託をしているものではないものと解されます」としている。そこで、配送業者等を利用するユーザは配送業者等に個人データの第三者提供をしていないとみなされる。そして、第三者提供をしていない以上、物理的には配送業者等の手元にあっても、それはユーザが管理をする個人データであって、ユーザは安全管理措置（個人情報保護法 23 条）を講ずる義務を負う。

Q7-35 配送事業者、通信事業者等の外部事業者を利用して、個人データを含むものを送る場合は、当該外部事業者に対して当該個人データの取扱いを委託（法第 27 条第 5 項第 1 号）しているものと考えられますか。

A7-35 一般的に、外部事業者を利用して、個人情報データベース等に含まれる相手の氏名、住所等宛に荷物等を送付する行為は、委託に該当すると解されます。ただし、配送事業者を利用する場合、通常、当該配送事業者は配送を依頼された中身の詳細については関知しないことから、当該配送事業者との間で特に中身の個人データの取扱いについて合意があった場合等を除き、当該個人データに関しては取扱いの委託をしているものではないものと解されます。また、通信事業者による通信手段を利用する場合も、当該通信事業者は、通常、通信手段を提供しているにすぎず、通信を依頼された中身の詳細について関知するものでないことから、同様に通信の対象である個人データについてはその取扱いを委託しているものではないものと解されます。なお、いずれの場合も、外部事業者を利用する個人情報取扱事業者には、安全管理措置を講ずる義務が課せられているため、中身の個人データが漏えい等しないよう、適切な外部事業者の選択、安全な配送方法の指定等の措置を講ずる必要があります。

そして、クラウド例外はまさにそれと同様に、ベンダがいわば封緘された中身である個人データを取り扱わないのであれば、そのような場合には第三者提供とせず、ユーザ自身が安全管理措置を講じれば良いとしたものである。

第 5 節　クラウド例外の適用範囲

⑴　クラウド例外の適用要件の充足が厳格に精査されるべきこと

まず、前提として、クラウド例外というのは上記で述べた適用要件を充足した場合にのみ適用されるのであり、かかる要件を充足しなければ、原則通り第三者提供規制が適用される。当然のことながら、単にそれがクラウドサービスであるというだけで、適用要件の充足の有無を問わずクラウド例外が直ちに適用されるものではない。よって、クラウド例外の適用要件の充足の有無が厳格に精査されるべきである。

ここで、ランサム攻撃を原因とする社労士向けクラウドシステムの情報漏洩事件[13]をきっかけに個人情報保護委員会は 2024 年 3 月 25 日に「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について（注意喚起）」[14]（以下「クラウド注意喚起」という。）を公表した。すなわち、個人情報保護委員会は、この事案において、クラウド例外の要件が充足されておらず、ベンダが、ユーザから個人データの取扱いの委託を受けて個人データを取り扱う関係にあったと認定した。その理由として、以下が挙げられている。

> ◦利用規約において、クラウドサービス提供事業者が保守、運用上等必要であると判断した場合、データ等について、監視、分析、調査等必要な行為を行うことができること及びシステム上のデータについて、一定の場合を除き、許可なく使用し、又は第三者に開示してはならないこと等が規定され、クラウドサービス提供事業者が、特定の場合にクラウドサービス利用者の個人データを使用等できることとなっていたこと。
>
> ◦クラウドサービス提供事業者が保守用 ID を保有し、クラウドサービス利用者の個人データにアクセス可能な状態であり、取扱いを防止するための技術的なアクセス制御等の措置が講じられていなかったこと。
>
> ◦クラウドサービス利用者と確認書を取り交わした上で、実際にクラウドサービス利用者の個人データを取り扱っていたこと。

要するに、①利用規約上の十分な手当てがされておらず[15]、②アクセス制御がされておらず、③現に個人データの取扱を行っていたというように、

Q&A7-53 の要件を全く遵守していなかったため、当然のことながらクラウド例外を使うことができない場合であった。

ここまで遵守が徹底されていないのであれば、クラウド例外を利用できないことは明らかと思われるが、クラウド注意喚起は、あくまでもクラウド例外が、特定の要件を満たす場合にのみ適用される例外であるということを再度確認するものといえるだろう。

⑵　インフラクラウドが念頭に置かれていること

規制改革ホットラインにおける「検討要請に対する所管省庁からの回答」[16]によれば、「クラウドサービスの利用と個人データの『取扱い』の明確化」という論点に関し、「一般論として、当該クラウドサービス提供事業者が、サーバに保存された個人データに対して編集・分析等の処理を行う場合には、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』には該当しないと考えられます。」とする。そして、「この回答を前提とするとSaaSへのクラウド例外の適用は否定的に解されているように思われる」[17] と指摘されている。

要するに、クラウド例外はAWS等のインフラクラウドを念頭に設けられたものであって、いわゆるSaaS等の編集・分析等の処理を行うものは、まさに当該編集・分析等の処理をもってベンダが個人データを取り扱っていると解釈される可能性がある。

⑶　例外事由

ここで、クラウドの利用規約においては、例外が定められている場合が多い。すなわち、障害時の対応や、外国を含む政府機関からの要請があった場合等においてベンダによるアクセスや利用が認められている場合もあり、そのような場合においても、クラウド例外の前提が維持できるのかという疑問が生じる。この点については、「クラウド事業者によるデータへのアクセスが例外的な場合にとどまるとされている限り、平時における法的整理には影響せず、なおクラウド事業者は『個人データを取り扱わない』ものとして、クラウド例外の整理を維持できると考えられる」[18]とされている。

例えばAWSは、カスタマーアグリーメント1.4において、「アマゾンは本サービスを維持もしくは提供するのに必要な場合、または法律もしくは政府機関の拘束力ある命令を遵守するのに必要な場合を除き、サービス利用者コンテンツ

にアクセスもしくはそれを利用しない。」としている[19]。そして、上記のような限定的・例外的なアクセスはあっても、AWSは、少なくともそのような例外的な場合以外においては、依然としてQ&A7-53 が適用され、クラウド例外を適用してよいのだ、という立場に立っている[20]。

ここでクラウド注意喚起では「保守、運用上等必要であると判断した場合」といった条項が存在した事案において、結論として、個人データを取り扱っていると評価されている。

しかし、AWSのいう「本サービスを維持もしくは提供するのに必要な場合」というのがあくまでも例外であるのに対し、クラウド注意喚起の事案では現に個人データを取り扱っていたということであり、その意味で、クラウド注意喚起の趣旨として、個人データの取扱いが行われる場合が、あくまでも狭い例外の範囲に留まる実態があるAWSのような場合においてもなお、クラウド例外が使えなくなるとまで述べる趣旨ではないと理解される。

第 3 章　生成AIにおけるクラウド例外の利用可能性

第 1 節　生成AI注意喚起の文言

生成AI注意喚起のうち、「生成AIサービスの利用に関する注意喚起等」は「個人情報取扱事業者における注意点」として以下を挙げる。

> ①　個人情報取扱事業者が生成AIサービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること。
> ②　個人情報取扱事業者が、あらかじめ本人の同意を得ることなく生成AIサービスに個人データを含むプロンプトを入力し、当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該個人情報取扱事業者は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成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。

前記のとおり、①は利用目的に関するものであることから、以下では、②を検討する。

第 2 節　生成AI注意喚起の文言の解釈

生成AI注意喚起は、「当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該個人情報取扱事業者は個人情報保護法の規定に違反することとなる可能性がある」「ため」ベンダが、「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」を求めている。もっとも、生成AI注意喚起は、ここでいう「個人情報保護法の規定」が個人情報保護法何条を指しているのかを明示しない。そこで、この文言の解釈としては、様々な可能性が考えられる。例えば、「応答結果の出力以外の目的」ということから、利用目的規制の話である可能性はゼロではない。これに対し、これを第三者提供規制に関するものと捉え、「学習さえオフにすれば、ベンダは個人情報を取り扱っていないので、クラウド例外が使える（本人の同意を取らずにAIに個人データを入れることができる）」という見解もあり得る[21]。

筆者は「一定の場合（学習に利用されず、当該個人データが当該プロンプトに対する応答結果の出力だけの目的で利用される場合）にクラウドの例外が利用可能だという趣旨にも読めなくはないが、不透明である。」と評したことがある[22]。

曽我部教授は生成AI注意喚起「について、生成AIサービスに個人データを含むプロンプトを入力し、その応答を得るというプロセスに関しては、個人データの「提供」に当たらないとする趣旨だと解釈する可能性が示された」としながらもその結論を否定し、生成AI注意喚起は、現時点で特に問題となる点を指摘したものにとどまると理解すべきではないかとする[23]。少なくとも実務対応としては、「従来の見解を前提に保守的に対応していくべき」ともされている[24]。なお、水井は、現在の個情委の見解も定かでない以上、そうした場合でも個人データの第三者提供規制に服することを前提に対応を検討することが無難とする[25]。

第 3 節　AIとクラウド例外

この点を考える上では、第 2 章・第 5 節(2)のとおり、SaaSに対しクラウド例外を利用することについて謙抑的に考えられていることが参考になるだろう。

そのことを前提に、生成 AI の利用においてクラウド例外が利用できるかは、あくまでも、クラウド例外の要件を充足するかという個別具体的な問題であって（第 2 章・第 4 節(2)参照）、具体的なベンダとの契約（DPA、Data Processing Addendum）次第である。ここで、例えば OpenAI の DPA[26] は、1 条 a 項で、「Open AI agrees to ... process Customer Data（強調筆者）」として顧客データ（DPA 前文によると顧客が OpenAI に提供する個人データであって、OpenAI が顧客に代わって本サービスを提供するために処理するもの）を OpenAI が処理する旨を明記している。

そうすると、一般的な SaaS に対するクラウド例外の適用を慎重に考えるべきであることに加え、少なくとも OpenAI や契約上 OpenAI と同様の条項を設ける生成 AI サービスにおいては、「契約条項」上も、当該ベンダがサーバに「保存された個人データを取り扱わない旨が定められて」いないことから、そのような場合においては、クラウド例外の適用を否定的に解するべき場合が多いだろう。

第 4 章　個人情報の生成 AI への投入と法

第 1 節　はじめに

上記のとおり個人データを生成 AI に投入することについて、クラウド例外によって正当化することは必ずしも容易ではない。しかし、個人情報を含むデータを生成 AI に投入するニーズは存在する。では、どのようにして適法に個人情報を含むデータを生成 AI に投入すれば良いだろうか[27]。

第 2 節　オンプレミス（ローカル LLM）

そもそも、第三者提供を発生させない方法はあり得る。すなわち、OpenAI の ChatGPT 等、クラウド上で提供される生成 AI は多いものの、近時はローカル LLM と呼ばれる、オンプレミス上で利用することができる LLM もその性能が飛躍的に向上しつつある[28]。もし、個人データの利用範囲がユーザーの社内で閉じており、ベンダ等の第三者に提供されないのであれば、（少なくとも第三者提供規制との関係では）適法に個人情報を含むデータを生成 AI に投入することができる[29]。

第 3 節　同意

また、従業員情報の提供等、一定の場合には本人の同意を得てベンダに第三者提供することが考えられる。なお、その場合には、記録義務（個人情報保護法 29 条）等にも留意が必要である。

第 4 節　個人情報

更に、個人情報保護法 27 条が「個人データ」の第三者提供を規制することから、「個人情報」の第三者提供に留めることで、個人情報保護法上の第三者提供規制を回避することができる可能性がある[30]。

議事録生成 AI の文脈において、岡田らも、「議事録に出席者や発言者の氏名が記載されていても、それは散在情報としての個人情報に過ぎず個人データには該当しないことが通常であるため、その意味でも個人データの第三者提供規制は問題とならない」としている[31]。

この場合、金融機関における個人情報保護に関する Q&AII-7 ③が「『個人情報データベース等』から紙面に出力されたものやそのコピーは、それ自体が容易に検索可能な形で体系的に整理された一部でなくとも、『個人データ』の『取扱い』の結果であり、個人情報保護法上の様々な規制がかかります。『個人情報データベース等』から紙にメモするなどして取り出された情報についても、同様に『個人データ』に該当します。」としていることに留意が必要である。要するに、従業員名簿等のデータベースから一人分の情報を切り出してきても、なお個人データとして扱われる可能性があるということである。

なお、仮に提供するのが個人データではなく個人情報であるとして個人情報保護法 27 条の第三者提供規制を回避することができても、具体的状況によってはプライバシー侵害の不法行為や人格権侵害の問題が生じる可能性はゼロではないことには留意が必要である[32]。

第 5 節　委託

クラウド注意喚起は、以下のとおり、クラウドサービスの利用が委託に伴う個人データの提供であれば、適切に委託先を監督すべきことを示す。これは、ある意味において、クラウドだからといって委託スキームが全く利用することができないわけではないことを示唆する。

> ◦サービスの機能やサポート体制のみならず、サービスに付随するセキュリ

ティ対策についても十分理解し、確認した上で、クラウドサービス提供事業者及ビサービスを選択してください。

◦個人データの取扱いに関する、必要かつ適切な安全管理措置（個人データの取扱いに関する役割や責任の分担を含みます。）として合意した内容を、規約や契約等でできるだけ客観的に明確化してください[33]。

◦利用しているサービスに関し、セキュリティ対策を含めた安全管理措置の状況について、例えば、クラウドサービス提供事業者から定期的に報告を受ける等の方法により、確認してください。

すると、生成AIサービスの利用の文脈においても、このような各点に留意をした上で、ベンダに対し「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当該個人データ」を提供（個人情報保護法 27 条 5 項 1 号）し、監督（個人情報保護法 25 条）を行うという建て付けを採用することも全く不可能ではないだろう。この点につき、ベンダが入力された個人データを委託業務の目的外で利用しておらず、かつ個人データを区別せずに混ぜて取り扱っていない（Q&A7-37 等）といった、委託の限界を超えないかについてベンダの利用規約等で確認し、データ処理契約（Data Processing Agreement）の締結等によってベンダに対する監督を行うことが必要[34]と指摘がされていることにも留意が必要であろう。

第 6 節　ゼロ・データ・リテンション

最後に、OpenAIはAPIを通じてGPTモデルを利用する場合の一部の場合についてゼロ・データ・リテンション（zero data retention）が利用可能とする[35]。ゼロ・データ・リテンションが適用される場合、ユーザの提供するデータにログを取得せず、リクエストを処理するのに必要な限りでメモリ上に存在するに過ぎない[36]とされている[37]。

この点、Q&A4-4 は確かに、適正取得（20 条 1 項）の文脈において、「単に閲覧するにすぎない場合には「個人情報を取得」したとは解され」ないとする。しかし、単に人間が目で見るだけなのではなく、OpenAIは実際にLLM上で個人データを処理する（個人データをGPTモデルに投入して処理結果を出力させる）のであり、むしろ上記第 2 章・第 5 節(2)で述べた「検討要請に対する所管省庁からの回答」でいう「編集・分析等の処理を行う場合」であることは

否定できないように思われる。そこで、ゼロ・データ・リテンションが適用されるというだけで、ただちに第三者提供にならないと解釈することはできないだろう。

第 5 章　おわりに

個人情報保護法は改正予定であり、既に 2024 年 6 月に中間整理[38]が公表されている。改正の動き等を踏まえると流動的な論点であるが、本稿が現時点の最新状況の検討として読者の皆様のお役に立てれば幸いである。

謝辞

本稿につき弁護士の加藤伸樹先生、大島義則先生及び数藤雅彦先生にご意見を頂戴し、本稿の脚注整理や校正等につき早稲田大学博士課程の宋一涵さんにご協力頂いた。心より感謝したい。但し、全ての誤りは筆者の責任である。

以上

---

(1)　松尾剛行『ChatGPT と法律実務』（弘文堂、2023 年）34 頁

(2)　*Generative AI Market Size To Reach $109.37 Billion By 2030*：*Generative AI Market Growth & Trends,* Feb. 2024, https://www.grandviewresearch.com/press-release/global-generative-ai-market

(3)　クラウドサービスの定義につき、松尾剛行『クラウド情報管理の法律実務』（弘文堂、第 2 版、2023 年）2 頁以下参照。

(4)　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について」（https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/）

(5)　この点については、松尾剛行『生成 AI と法律実務』（仮）（弘文堂、近刊予定）を参照されたい。

(6)　個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン」に関する Q & A」2024 年 3 月更新（https://www.ppc.go.jp/files/pdf/2403_APPI_QA.pdf）（以下、本文でも「Q&A」という。）7-14 参照。

(7)　「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）」2023 年 12 月（以下、本文でも「ガイドライン通則編」という。）（https://www.ppc.go.jp/files/pdf/240401_guidelines01.pdf）3-6-3（3）③参照。

(8)　ガイドライン通則編 3-6-3(3)③。なお、これがどのような場合かについては、「取得の際に通知・公表している利用目的の内容や取得の経緯等にかんがみて、既に特定の事業者が取得している個人データを他の事業者と共同して利用すること、共同して利用する者の範囲、利用する者の利用目的等が、当該個人データの本人が通常予期しうると客観的に認められるような場合をい」うとする Q&A7-52 も参照。

(9)　松尾・前掲注(3)197 頁

(10)　この「等」を重視して、契約条項の定めを中心的要件とする考えも存在することにつき岡田淳他『個人情報保護法』（商事法務、初版 2024 年）320 頁参照。

(11)　この点は、「クラウドサービスの利用が、法第 27 条の『提供』に該当しない場合、法第 25 条に基づく委託先の監督義務は課されません」とする Q7-54 も参照のこと。

(12)　倉庫業者について、中小規模事業者の安全管理措置に関するものであるが、「倉庫業、データセンター等の事業において、当該情報が個人情報に該当するかどうかを認識することなく預かっている場合」「事業の用に供しているとはいえ」ないとする Q&A10-4 も参照。

(13) なお、ランサム攻撃につき、松尾剛行「ランサム攻撃に関する個人情報保護法、会社法、及び民法に基づく法的検討－情報セキュリティと法の議論枠組みを踏まえて－」情報ネットワーク・ローレビュー 21 号（2022 年）（https://www.jstage.jst.go.jp/article/inlaw/21/0/21_210005/_pdf/-char/ja）参照。
(14) 個人情報保護委員会「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について（注意喚起）」2024 年 3 月 25 日（https://www.ppc.go.jp/files/pdf/240325_alert_cloud_service_provider.pdf）
(15) 但し、本節の(3)も参照。なお、岡田他・前掲注(10)321 頁は「通常のサービス提供の過程でクラウド事業者がサーバ内の個人データを取り扱わないことが実質的に明確にされているのであれば、原則として個人データの提供に該当しないと整理して良いのではないかと考える」とする。
(16)「規制改革・行政改革ﾎｯﾄﾗｲﾝ検討要請項目の現状と対応策」2022 年度 No.307（https://www8.cao.go.jp/kisei-kaikaku/kisei/hotline/siryou2/k_siryou2_r4.pdf）
(17) 曽我部真裕監修・小川智史著「新連載　実務問答個人情報保護法（第 1 回）クラウド例外」NBL1250 号（2023 年）〔小川〕9 頁
(18) 曽我部監修・小川著・前掲注(17)〔小川〕7 頁
(19)「AWS カスタマーアグリーメント」2024 年 5 月 17 日（https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_2024-05-17_JA-JP.pdf）
(20) 松尾・前掲注(3)201 頁
(21) これに近い立場と思われるものとして、木村一輝『設例で学ぶ個人情報保護法の基礎』（商事法務、初版、2024 年）247 頁参照。
(22) 松尾・前掲注(1)79 頁
(23) 曽我部監修・小川著・前掲注(17)〔曽我部〕11 頁
(24) 曽我部監修・小川著・前掲注(17)〔小川〕9 頁。なお、生成 AI 注意喚起により生じたクラウド例外の柔軟な解釈が可能ではないかという問題意識に対し、クラウド注意喚起が「クラウド例外の安易な拡張解釈に対しては歯止めをかける趣旨とも評価できよう」とする岡田他・前掲注（10）324 頁も参照。
(25) 水井大「生成 AI と個人情報保護」会社法務 A2Z 2024 年 7 月号 26 頁
(26) OpenAI, *Data processing addendum,*Feb.15,2024,https://openai.com/policies/data-processing-addendum/
(27) なお、AI のみが個人データを取り扱うのであれば、そもそも個人データを取り扱うと言えないのではないか、と言った疑問もある。この点、OpenAI は（第 3 章第 6 節で述べるゼロ・データ・リテンションを除き）原則 30 日保管して必要なら従業員が確認するというポリシーを持っており、人間が個人データを取り扱う可能性が残っている。ただ、「絶対に人間が見ない」という扱いを採用した場合にどのように解釈されるべきかは興味深い問題である。なお、従来の解釈として「従来は入力された情報をもとに分析を行い、出力するという過程を経る場合は、たとえそれが人間の目に触れないとしても『提供』に該当すると言う考え方が一般的であった」とする岡田他前掲注（10）323 頁も参照。
(28) 佐々木峻「ローカル LLM を動かしてみる」Interface 2024 年 8 月号 118 頁以下
(29) 但し、利用目的規制等の他の問題の解決は必要である。AI と利用目的規制については、ガイドライン通則編 3-1-1*1 を参照。
(30) 松尾・前掲注(1)79 頁
(31) 岡田淳＝堺有光子「文書要約または文書作成に関する社内ルールの整備」ビジネス法務 2023 年 11 月号 25-26 頁
(32) 但し、議事録作成を想定する場合において、事前に録音して AI で議事録を作成する旨を通知していれば、具体的状況にもよるだろうが、プライバシー侵害として問題となる可能性は低いように思われる。
(33) Q&A5-8 参照。
(34) 水井・前掲注(25)26 頁
(35) Open AI, Enterprise privacy at OpenAI, available at https://openai.com/enterprise-privacy/ の「*How does OpenAI handle data retention and monitoring for API usage?*」参照。
(36) With zero data retention, request and response bodies are not persisted to any logging mechanism and exist only in memory in order to serve the request.
(37) OpenAI,*How we use your data,* https://platform.openai.com/docs/models/how-we-use-your-data
(38) 個人情報保護委員会「個人情報保護法いわゆる 3 年ごと見直しに係る検討の中間整理」2024 年 6 月 27 日（https://www.ppc.go.jp/files/pdf/chukanseiri_honbun_r6.pdf）