Miura & Partners

Data and Digital Insights Vol.8

クラウド例外の射程と生成 AI 時代の「取扱い」（前編）

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

本稿では、日本の個人情報保護法（個人情報の保護に関する法律をいいます。以下同じ）における「取扱い」概念、特に、いわゆる「クラウド例外」の解釈について、技術的なレイヤー構造とデータ処理の実態に基づいた再定義を試みました。

後編ではクラウドストレージのような SaaS（Software as a Service）とクラウドベースの LLM（Large Language Model）サービスとの間に、個人情報保護法上の「取扱い」の有無を判断する上で質的な差異が存在するのかという問いについて検討いたします。

(1) 個人情報の「取扱い」概念の意義

個人情報の「取扱い」は、個人情報保護法上の極めて重要な概念です。個人情報取扱事業者が「個人情報」を「取り扱う」場合に、同法の各種義務規定が適用されることになるためです。

しかしながら、個人情報保護法には「取扱い」の定義規定が存在しません。この点について、「『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」（以下「Q&A」といいます）Q2-3 は、「利用」について「取得及び廃棄を除く取扱い全般」を意味するとしていることから、「取扱い」は個人情報の「取得」から「廃棄」に至るすべての活動（入力、蓄積（保管）、編集・加工、出力、提供、消去等 [1]）を包含する概念であることが示唆されています。

なお、GDPR においては、「processing」について積極的な定義規定が置かれており、「自動的な手段によるか否かにかかわらず、収集、記録、編集、構造化、保存、修正若しくは変更、検索、参照、利用、送信による開示、配布若しくはその他利用可能化、整列若しくは結合、制限、消去又は破壊のような、個人データに対して実施される操作又は一連の操作」と定義されています（GDPR 第 4 条(2)）。

これに対し、日本法では「取扱い」を原則的に広く捉えつつも、Q&A 等により個別の場面ごとに「取扱い」を狭く解釈することがあります。

(2) クラウド例外の概要

ア. クラウド例外の成立経緯

[1] 岡村久道『個人情報保護法〔第 4 版〕』（商事法務, 2022 年）219 頁

クラウドサービスの利用が拡大する中で、個人情報保護法との関係においては、クラウドサービスに個人データを含むデータを保存する際に、ユーザ事業者からクラウド事業者に対する第三者提供（もしくは委託による提供）となるか、自らによる取扱いとなるかが、しばしば論点となってきました。

「取扱い」が、個人情報の「取得」から「廃棄」に至るすべての活動を包含する概念であるとすれば、クラウドサービス提供事業者による「保管」についても取扱いに該当すると考えるのが自然とも思われるところですが、2015 年 4 月にマイナンバー法（行政手続における特定の個人を識別するための番号の利用等に関する法律をいいます。以下同じ）の Q&A において一定の要件の下、「提供」に該当しない（自らによる取扱いとなる）とする解釈が示され[2]、その後、平成 29 年 2 月に個人情報保護法の Q&A において、提供に該当しない場合があるという解釈を踏襲しました。

この解釈は一般に「クラウド例外」と呼ばれています。

イ．Q&A 7-53 の内容

現在の「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 7-53 を以下に引用します。

> 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。

[2] マイナンバー法においては、再委託について本人同意が必要となるため、クラウドサービスの利用が委託に当たるか自らによる取扱いとなるかで、効果において大きな差異があったことが背景にあったと思われます。

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（中略）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。

クラウド事業者が「当該個人データを取り扱わないこととなっている場合」、すなわち「①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、②適切にアクセス制御を行っている場合等」には、ユーザ事業者は個人データを提供したことにはならないとしています（丸数字は筆者による）。

また、クラウド例外が適用される場合、クラウド事業者自身による個人データの取扱いは観念されず、ユーザ事業者が自ら安全管理措置を講ずる必要があり（Q&A 7-54）、報告対象となる漏えい等事案が発生した場合に自ら報告・本人通知を行うこと（Q&A 6-22）が必要となります。また、この例外が適用される場合においても、ユーザ事業者自らがサーバの所在国を含めて外的環境を把握すること（Q&A 10-25）にも留意が必要です。

ウ．例外に該当するための要件

要件①には「取扱い」という概念が用いられているため、この要件そのものから、どのような条件を満たせば「取り扱わないこととなっている場合」に該当するかを導くことは困難です。

要件②には「アクセス制御」という言葉が出てきます。アクセス制御（access control）とは、資産へのアクセスが、事業上及びセキュリティ要求事項に基づいて認可及び制限されることを確実にする手段[3]とされており、より簡単にいうと、正当な権限を持つ者やシステムだけが情報やシステムにアクセスできるよう制限・管理することやその手段を指すことが多いかと思います。これは情報セキュリティ上の重要な管理策（control）の一つであり、こと複数の主体が同一のシステム基盤を共同利用する環境においては極めて重要な要素ではありますが、「取扱い」に該当するアクセスと、そうでない「アクセス」の違いが明確にならない限り、どのようなポリシーで制御がなされているべきなのかを導くことができません。

要件①と②の関係としては、Q&A の文言から、両者は別個の要件であり、法的な義務がどうなっているか、その義務が情報セキュリティ上の control としてどのように担保されている

[3] JIS Q 27000: 2019 3.1 項

か、という違う側面から定めるものであるので、双方を満たす必要がある（①かつ②）との理解が一般的だと思われます。もっとも、「場合等」との文言からすれば、それ以外の場合も許容される余地があるように読めますし、①を中心的な要件と考えることも成り立つとする論考も見られます[4][5]。

(3) 2023 年 2 月：「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」

ここまで読むと、いくらかの方々は「もしかして、この"取扱い"というのは、自然人によるアクセスを念頭に置いているのではないか？」と思われるのではないかと思います。後述するとおり、クラウドサービス提供事業者のコンピューティングリソースの上でデータ処理をしつつ、クラウドサービス提供事業者による"アクセス"がないという状況は、直観的にイメージしづらいように思われるからです。

しかし、そう簡単ではありません。個人情報保護委員会は、2023 年 2 月に「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 Q&A 7-53 より踏み込んだ見解を示しています[6]。一般的なクラウドサービスにおいては「個人データに対する編集・分析等の処理」は自然人の個別の関与なく、アプリケーションプログラムを通じて提供されることが多いと考えられるところ、どうやら、その場合も「提供」があった（クラウドサービス提供事業者の「取扱い」に及ぶアクセスがあった）と考えられるようです。

(4) 2024 年 3 月：株式会社エムケイシステム事案についての判断

2024 年 3 月に個人情報保護委員会は、クラウド例外についての個別判断を示しました。

株式会社エムケイシステム（以下「エムケイ社」といいます。）は、社会保険労務士の業務支援システムである「社労夢」を SaaS 環境でクラウドサービスとして提供していましたが、エムケイ社のサーバがランサムウェア被害を受け、個人データの漏えいのおそれが生じました。

---

[4]小川智史「実務問答個人情報保護法 第 1 回 クラウド例外」（NBL No.1250（2023 年 9 月 15 日号）4 頁）は、配送事業者による個人データの「取扱い」に関する Q&A 7-35 において「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」としており、当事者間の合意が中心的な要素となっていることを論拠として挙げています。

[5] 板倉陽一郎＝寺田麻佑「クラウド・コンピューティングの利用と個人情報の取扱いの委託に関する考察」情報処理学会研究報告（EIP）69 巻 1 号(2015)は、端的に、「契約条項によって当該事業者が個人データをその内容に含むデータを取り扱わない旨が定められて」いるかどうかが要件であり、適切なアクセス制御の存在（要件②）や、「等」は、合意に関する評価根拠事実であって別の要件ではないと論じています。

[6] 規制改革ホットラインにおける「検討要請に対する所轄官庁からの回答」（令和 4 年度 No. 307）

この事案について、個人情報保護委員会は、エムケイ社が社労夢の提供において個人データを取り扱っていたと認定しました。

その際に検討された事項は以下の 4 点です。それぞれの要素がどのような関係にあるのかは、別途検討を要すると思いますが、個人情報保護委員会のクラウド例外に対する態度を考える上では重要な事案と言えます。

ア．利用規約

エムケイ社がサービスに関して保守運用上または技術上必要であると判断した場合、利用者がサービスにおいて提供、伝送するデータ等について、監視、分析、調査等、必要な行為を行うことができる旨が規定されていました。また、エムケイ社は、利用者の顧問先に係るデータを、一定の場合を除き、利用者の許可なく使用し、または第三者に開示してはならないという旨が規定されている点から、エムケイ社は、当該利用規約に規定される特定の場合には、社労士等の利用者の顧問先に係る個人データを使用等できると定められていたとされています。

イ．アクセス制御

エムケイ社は、保守用 ID を有しており、それを利用して社労夢内の個人データにアクセス可能な状態でした。また、エムケイ社による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は講じられていませんでした。

ウ．サービスの性質

社労夢は、利用事業者である社労士事務所や企業等が、社会保険および雇用保険の申請手続や給与計算等をオールインワンで行うことができるものです。すなわち、本件においてエムケイ社がクラウドサービス上で提供するアプリケーションは、利用事業者である社労士事務所や企業等が、個人の氏名、生年月日、性別、住所および電話番号などの個人データを記録して管理することが予定されているものであり、実際に大量の個人データが管理されていました。

エ．実際の取扱い例

エムケイ社が、利用事業者と授受確認書を取り交わした上で、実際に利用事業者の個人データを取り扱っていた実績がありました。

オ．個人情報保護委員会の結論

個人情報保護委員会は、上記の事実関係を考慮した場合、クラウドサービス提供事業者であるエムケイ社がガイドライン Q&A 7-53 の「個人データを取り扱わないこととなっている場合」とはいえず、また、個人データの取扱いを防止するための適切なアクセス制御は行われていなかった、すなわち、Q7-53 の要件①と要件②のいずれについても満たしておらず、したがって、クラウド例外の適用はなく、エムケイ社は、個人情報取扱事業者として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っていたと結論づけました。

(5) 生成 AI サービスに関する個人情報保護委員会の見解

他方で、個人情報保護委員会は、生成 AI と個人情報保護法の関係に関して、令和 5 年 6 月 2 日、「生成 AI サービスの利用に関する注意喚起等」（以下「利用注意喚起」といいます）および「OpenAI に対する注意喚起の概要」を公表しました。利用注意喚起(1)②では、以下のように注意喚起がなされています。

> 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

そもそも個人情報保護法のどの規定への違反の可能性について述べているのかが明示されておらず[7]、生成 AI サービスを利用する際には機械学習に利用されないことを確認するよう注意喚起する以上のメッセージを読み取れるのかは微妙な文書ではあります。ただ、提供規制への違反可能性について説明した文書だと仮定すると、クラウド例外を従来よりも拡張解釈し、機械学習に利用しないことが担保されていれば、「提供」に該当しない場合があり得るように読めますし、実際にそのように整理可能と述べる文献も見られます[8]。また、上記のとおり、利用注意喚起(1)②の考え方を敷衍すれば、SaaS についてもクラウド例外を適用する余地があるのかという疑問が生じます。

2. これまでの議論

(1) 貸し倉庫／輸送業者のアナロジー

クラウド例外の理解において、しばしば用いられるのが「貸し倉庫」や「輸送業者」のアナロジーです[9]。倉庫事業者はスペースを貸し出すだけで、段ボールの中身には一切触れず、搬入出も利用者が行う場合、倉庫業者は中身の情報を「取り扱って」いるわけではありません。この比喩は、クラウド事業者がデータの内容に関知せず、単に物理的・論理的なストレージ領域を提供しているに

[7] 該当箇所の前に、「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。」と注意喚起していることを踏まえると、主として目的外利用の禁止（個人情報保護法 18 条 1 項）への違反可能性について注意喚起する文書と理解することもできます。その場合には、取扱いの委託による提供であることが当然の前提となっているものと理解することとなると思われます。なお、杉浦健二弁護士は、注意喚起の公表後に個人情報保護委員会が公表した広報パンフレットの記載を根拠に、この注意喚起が生成 AI サービスのプロンプト入力時における提供該当性について個情委が見解を示したものであると主張しており、これもたいへん説得力のある主張であると考えられます。https://storialaw.jp/blog/10005

[8] 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。

[9]前掲注[1]の 179 頁において「内容に触れることができないため個人情報であることを関知できないまま、他の有体物と同様に運送等を行うようなときは、個人情報として取り扱い得るものとはいえない」と述べつつ、クラウド例外について論じる箇所でも配送事業者の例に言及されています（同 313 頁）。

過ぎない場合には、「取扱い」には該当しないという解釈を説明するのに簡便だからだと思われます。輸送業者については、配送事業者による個人データの「取扱い」に関する Q&A 7-35 において、「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」としている点も、中身の詳細への関知や、当事者間の合意が中心的な要素として、取扱いに至らない伝送の受託があり得る点を示しているため、デジタルデータの取扱いへの一定の類推が可能だと思われます。

(2) IaaS／PaaS／SaaS の分類に着目した論

IaaS／PaaS／SaaS というクラウドサービスモデル上の区分[10]に従い、IaaS や PaaS の場合にはクラウド例外が適用できる余地があるが、SaaS の場合には適用できないとする見解も見られます[11][12]。

IaaS／PaaS においては、ユーザ事業者が OS やアプリケーションを管理し、クラウド事業者はインフラを提供するに留まることから、データそのものに関する管理権限をユーザが掌握しやすく、「取り扱わない」状態を作り出しやすいのではないか、という意味で、貸し倉庫のアナロジーを穏当に敷衍した論だと思います。先に断っておきますが、これは直観的に理解しやすく、説得力のある論だと考えていますし、SaaS はともあれ IaaS/PaaS にはクラウド例外が適用可能なのではないかという結論については現状において説得力があると考えております。しかし、純粋にサービス提供事業者が支配する計算リソースによる「アクセス」というものを考えるときには、アプリケーションによる処理と、インフラによる計算の提供の間にどのような差があるのか、あと一歩の説明を要すると思われます。

なぜなら IaaS／PaaS／SaaS のいずれにおいても、ユーザ事業者が入力したデータの処理のために、クラウド事業者が支配・提供するデータ処理のための計算リソース（CPU や GPU による演算処理）を利用する点で共通だからです。

多くの文献で言及される暗号処理による保護を念頭に置けば、IaaS／PaaS／SaaS は別に考え得るとの期待があるかもしれません。たしかに、クラウドサービスに保管されるデータについてユーザ事業者が管理する鍵で暗号化され、クラウド事業者が復号不可能な状態のまま保管、伝送されることがあります。IaaS／PaaS においては、クラウド事業者によって提供される KMS

[10] 利用者がソフトウェアスタックのどこまでを管理するか、という観点から NIST SP 800-145 や、146 等に示される区分です。本稿では詳細は省くが、図解がウェブ上に多数作成されているので参考としていたければと思います。

[11] 前掲注[4]は、「クラウド例外との関係では、一般に IaaS や PaaS の場合にはクラウド例外が適用できるが、SaaS の場合には、提供されるサービスの内容次第であるものの、適用が難しいと考えられてきた。」と整理しています。

[12] 岡田敦ほか『個人情報保護法』（商事法務、2024 年）は「IaaS（Infrastructure as a Service）や PaaS (Platform as a Service)のようにクラウド事業者がインフラや OS のみを提供する場面であればクラウド事業者がサーバ内の個人データにアクセスすることは想定されていないのが通常であるのに対し、SaaS（Software as a Service）のようにクラウド事業者がアプリケーションまで提供する場面であれば、提供サービスの内容次第ということになる。」と述べています。

（Key Management Service）により利用者側での鍵管理の設計や自由度が可能なことが多く、SaaS よりも暗号化処理や鍵管理に関するユーザ事業者側のイニシアチブが大きいと言えるでしょう。仮に「クラウド上では常に暗号化されており」かつ「クラウド事業者が復号のための鍵を行使できない」という条件がある場合には、クラウド事業者は技術的にデータの中身を知り得ないため、すくなくとも要件②（アクセス制御）は確実に満たすことが期待されます。また、このような場合にはデータを取り扱わないという合意をしていると考えられるため、要件①も満たすと期待されるのではないでしょうか。

しかし、現在の一般的なコンピュータアーキテクチャにおいて、CPU が演算を行うためには、データを暗号化されたストレージから読み出し、メモリ上で復号して平文にする必要があり、たとえ、保存時（At Rest）や通信時（In Transit）にはデータを暗号化していても、なんらかの処理をする時（In Use）には平文またはそれに近い形式でデータを扱わざるを得ません[13]。したがって、クラウドサービス事業者の計算リソースや関連プログラムは、ごく例外的な場合[14]を除き、ユーザ事業者がインプットしたデータに平文状態で必ず「アクセス」するのです。自然人によるアクセスという意味では、たとえばクラウドコンピューターの superuser の権限を持つクラウドサービス事業者の従業員は、原理的には、メモリにロードされた平文を入手することができますが、それは権限行使プロセスの制御によって一定の制御は可能でしょうし、実際に制御されています。一方で、クラウドサービス事業者の計算リソースや関連プログラムによる、ユーザ事業者のデータへの「アクセス」は、計算のために必要な事項ですから、回避ができません[15]。貸倉庫や運送事業者とは違ってクラウドサービスにおいては、渡されたデータの中身を平文で処理することが一定程度必要にあるという違いがあるわけです。

(3) それでは、すべての「アクセス」が「取扱い」なのか？

IaaS／PaaS／SaaS における計算リソースによるアクセスを一律に「取扱い」と考えるべきであるとの見解もあります。

前掲注[5]は、2017 年に個人情報保護委員会より Q&A 7-53 が示される以前の論考ではありますが、その時点までの議論を参照した後に、以下のように論じています。

[13] 前述の KMS について、復号鍵をユーザ事業者が保有する場合も、クラウド事業者が保有する場合もありますが、いずれにおいても計算処理を行うロードに先行して、クラウド事業者による復号処理が自動的に行われるのが通常です。さらに、仮に復号化がユーザ事業者によって行われることが徹底されていたとしても、最終的に復号化された平文のデータが CPU に投げ込まれる点に変わりはありません。

[14] 中身に着目しないデータ処理として、保管、複製、伝送、ファイルサイズ取得やタイムスタンプ操作のようなメタデータの操作、さらなる暗号化などは暗号化したままでも可能だと考えられます。また、本論とは逸れますが、準同型暗号（Homomorphic Encryption）を利用した、「秘密計算」という暗号化されたデータを暗号化されたまま計算処理できる技術も存在することから、（安全管理の観点からは活用が嘱望される技術ではあるものの）データが暗号化されて可読性を失っているからといって内容に着目した処理の余地がないとまで断定することは難しくなっていると考えられます。

[15] 一つの例外として、クライアントサイド暗号化（CSE）や二重キー暗号化（DKE）といったソリューションがオプションとして提供されることがあります。その場合、計算はクラウドで行わず、ユーザの手元の端末で行うという徹底した挙動を行います。

> クラウド・コンピューティングの利用は「保管等」である。クラウド事業者が会計サービスを提供しているような場合、グループウェアを提供しているような場合（SaaS）、当然に、その処理の容易化を伴っており、これが「個人データの取扱い」に該当することは争いがあるまい。問題は、個人データの内容にかかわらないクラウド・コンピュー ティングサービス（PaaS、IaaS）が「取扱い」に含まれるかである。「取扱い」について個人情報保護法は定義を定めていないが、個人情報保護法が行政法規であること、個人情報取扱事業者が取得、利用後、廃棄するまで保管している間にも当然に個人情報取扱事業者としての義務が掛かることに鑑みても、ここに主観的な要素や、制限を加える事は妥当ではあるまい。また、クラウド事業者において個人データの利用を感知しているかどうかも、判断に加えるべきではあるまい。クラウド・コンピュー ティングの利用の現状に鑑みれば、クラウド事業者における、利用者が個人データをクラウド・コンピューティングの利用から排除しているという期待を保護することは非現実的である。かくして、クラウド・コンピューティングの利用は、単なる保管であっても、原則としてクラウド事業者に対する個人データの取扱いの委託であると解すべきであろう。

これは、IaaS／PaaS であっても個人データを含む電子データを保管するだけで「取扱い」に該当するという立場であろうと思います。無論、クラウド上の計算リソースで個人データを内容に含む電子データを平文状態でロードして計算するような場合にも、クラウドサービス提供事業者による個人データの取扱いがあるとの結論に至るかと思います。クラウド・コンピューティングの実態に照らして非常に明快で、一貫した論であり、「取扱い」を GDPR における processing に極めて近接した概念と捉えるものと思われますが、結論において、クラウド例外が現実的には存在できないとの結論に帰着していると思われる論でもあり[16]、この論文の後に個人情報保護委員会によって示された Q&A 7-53 が「取扱い」にならない「アクセス」や「保管」の存在を認めていること自体は明白であるところ、これと整合しないようにも思われることから[17]、現時点におけるクラウド例外を考える上で、そのまま採用することは困難だと考えられます。仮に、個人情報保護委員会がこの立場を採用するのであれば、エムケイ社の事案に

[16] 続く記述において「契約条項によって当該事業者が個人データをその内容に含む電子データを取り扱わない旨が定められて」いれば、自らの取扱いであると解して良いとしていますが、クラウド・コンピューティングの利用においてどのような条件が付加されれば、「当該事業者が個人データをその内容に含む電子データを取り扱わない」ことになるのかは不明です。さらに続けて、「このような私見に対しては、クラウド事業者にそのような契約条項を飲ませることは事実上不可能である（中略）との批判が存しよう」と自ら想定しつつ、さらに「クラウド事業者は、このような条項を入れることも入れないことも自由である。入れないことで、我が国のクラウド・コンピューティングの利用から排除されるとなれば入れるであろうし、そうでなければ蔑ろにし続けるのみであろう。法令上の義務について利用者が交渉できないとすれば、法執行に責任をもつ個人情報保護委員会が、クラウド事業者と調整することも必要になってくるであろう。」と続けており、現実的に締結が極めて困難な条項であると考えていらっしゃるようです。

[17] 板倉＝日置「個人情報保護法のしくみ」商事法務、2017 年において、Q&A 7-53 が示された後にも、「『個人データを取り扱わない旨』がクラウド事業者の利用規約又は約款に定められているか、これを交渉で獲得しない限り、個人情報取扱事業者のクラウドサーバの利用は、その形態（SaaS、PaaS、IaaS 等）にかかわらず、原則として委託に該当するということを前提とする必要がある。」と述べられています。

おいて、エムケイ社が管理する SaaS 環境において個人データを含む電子データの処理が行われていたというサービスの外形のみから「取扱い」があったとの認定がなされたはずであり、4つの事項についての詳細な検討はまったく必要でなかったと思います。

むしろ、「取扱い」に該当しない「アクセス」や「保管」が存在するという結論からスタートして論理を逆向きに組み立てていこうとするならば、前掲注[5]の論理展開において排除された理屈を読み込むことが重要だと思われます。つまり、クラウド例外を考える上で、①「取扱い」概念に対して「主観的な要素や、制限を加える」ものであると考えるべきであり、②「取扱い」に該当するかについて「クラウド事業者において個人データの利用を感知（原文ママ）しているかどうか」も、判断に加えるべきなのだろうと思われます。

特に②については、「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」としている Q&A 7-53 の文言[18]から、個人データを含む電子データを保存していたとしても、個人データを取り扱うことにならない場合があることが明確に示されており、非常に重要な観点だと考えられます。

前掲注[4]や前掲注[14]において示された IaaS／PaaS と SaaS の間の線引きも、存在することは示されている「クラウド例外」について一定の整理を試みているものだと言えますし、少なくとも IaaS／PaaS についてはクラウド例外が成立するのではないかという考え方については、説得力もあるように感じられます。

それでは、アプリケーションによる処理と、インフラによる計算の提供の間には「取扱い」概念の該当性を分かつ質的な差があるのでしょうか。あると仮定すれば、それは何なのでしょうか。そして、そもそもここでいう「アクセス」とは何を意味しているのでしょうか。

長い前置きになりましたが、ここからが試論となります。

3. 試論 1 —「取扱い」概念の再検討と技術的実態

(1) アクセスや処理においてデータの性質への着目があるか

結論から申し上げますと、個人データの「取扱い」に該当するアクセスや保管と、そうでないアクセスや保管を分ける分水嶺は、クラウド事業者が当該データを「個人データ（意味を持った情報）」として処理しているか、それとも「中身に関知しない単なるビット列（ペイロード）」として処理しているかの違いにあるのではないかと考えます。

例えば、文書を保管する貸倉庫業者が中身を見ずに保管する場合や、配送業者が封入物に関知せず伝送する場合と同様に、クラウド事業者がサービスの目的や処理のプロセスにおいて「デ

[18] なお、マイナンバー法上の委託に関する Q&A3-12 では、「当該事業者が当該契約内容を履行するに当たって個人番号をその内容に含む電子データを取り扱うのかどうかが基準となります。」（下線は筆者による。）との記載がなされており、現在も維持されています。

ータの意味や内容」に関知せず、機械的に計算リソースを提供している限りにおいては、「個人データの取扱い」とは評価されない余地があるのではないでしょうか。
この考え方は、個人情報保護委員会の「ガイドライン Q&A 7-53」において、「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」と述べられている部分を、最も自然に解釈したものかと思います。

(2) IaaS／PaaS と SaaS の区別｜アプリケーション層とそれ以外

IaaS／PaaS と SaaS の違いについても、この考え方を敷衍すれば整理が可能と考えられます。つまり、コンピューターを、概念的に、アプリケーション、ミドルウェア、OS、物理といったスタック・層（レイヤー）に分解して考えた際に、アプリケーション層は主に人間の解決したい課題や目的（What）を扱う領域ですが、それ以下の層はその手段やデザイン（How）を提供する層と言えます。特に CPU や GPU における計算レイヤーでは、命令の受信・解読・実行・返答という作業が行われるのみであり、データ（ペイロード）の中身が個人データであるか否かは考慮されません。これは「取扱い」という概念と言語的にも乖離があると言えるでしょう。したがって、アプリケーション層と切り離されたペイロードの処理のみを担当する IaaS／PaaS のクラウドサービス提供事業者においては、その処理する電子データに含まれる個人データの「取扱い」はない、と整理することが可能なのではないでしょうか。

(3) アプリケーションの性質による区分｜データの内容に着目するアプリケーションかそうでないか

一方で、アプリケーション層においては、給与計算や勤怠管理など「個人データの取扱い」そのものを目的とするサービスが存在し、これらはデータの内容や性質に関知することもあり得るため、処理するデータに含まれる個人データの「取扱い」に該当する可能性が生じると考えられます。エムケイ社の事案において、個人情報保護委員会が、アプリケーションの性質として、利用事業者である社労士事務所や企業等が、個人の氏名、生年月日、性別、住所および電話番号などの個人データを記録して管理することが予定されていたことを指摘しているのは、まさにアプリケーションの性質が「取扱い」の結論に影響を持つことを示しており、SaaS であればすべて「取扱い」が認められるわけではないと考える余地を残していると考えられます。

そこで考慮されるのは、個人情報保護委員会が「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」前掲注[6]で示された「個人データに対して編集・分析等の処理を行う場合」に該当するか否かだと考えられます。

例えば、個人情報データベースの管理のためのシステムがあったとします。つまり、個人データを入力するためのデータテーブルが用意され、id, name, age, gender 等と個人データの入力に最適化されたキーや列のタイトルが並び、そのように整えられたデータの取扱いを効率的に支援することを目的とするものです。これは、個人データに対して編集・分析等の処理を行う場合に該当することが比較的明白な例であると思われ、前掲注[5]の「処理の容易化」そのものでもあると言えます。エムケイ社の事案におけるシステムも、比較的この典型に当てはまるものであったと評価できるのではないかと思われます。

このことは、個人データを含む電子データに対する編集・分析等の処理を提供するアプリケーションであっても、その中の個人データに対する編集・分析等の処理を行わないアプリケーション、すなわち、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を提供するものについては「取扱い」に該当しない可能性を残す記載だと考えられます。そのような、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の最たるものが「保管（ストレージ）」だと考えられます。

前掲注[16]の前段に記載のとおり純粋な「保管」にとどまる限り、ユーザ事業者はデータを暗号化されたまま保持し続けることが可能です。実際に前掲注[17]のような、クラウドサービス提供事業者やサービス自体による復号化を完全に拒むサービスオプションも提供されていますし、ユーザ事業者が手元で自ら暗号化したデータをクラウドストレージにアップロードすることもできます。そのような場合、アップロード先が SaaS のストレージであれ、IaaS において提供される仮想ディスクであれ、事業者がデータをブロックに書き込むのみであれば、それは中身に着目しないペイロードとして処理するものに過ぎず、質的な違いはありません。このように、中身に全く着目しない処理であれば、「クラウド例外」の適用があると整理することが可能だと思われます。

(4) 平文処理と「取扱い」

ア．クラウドストレージにおける平文処理の実態

ただ、SaaS 型クラウドストレージの多くでは、利用者の利便性を確保するため、提供事業者によって格納された電子データに対する平文状態での処理が行われている場合が多いことも考慮する必要があります。特に近年のクラウドストレージサービスでは、標準機能としてテキスト全文検索やその前提としての OCR 処理、セキュリティ維持のためのマルウェアのスキャニングが提供されていることも多く、そのためにはバックエンドで様々な処理が行われていると考えられます。

検索のためのもっとも基礎的な処理としてはインデックス処理が挙げられます。データが自然言語である場合、そのテキストデータを抽出し、形態素等の言語単位に関する解析等を用いてトークンに分解した上で、どのトークンがどの文書に含まれているかを示す索引データ（転置インデックス）を作成・保存します。ただ、ここでの分析は、自然言語における単語としての分節・分解であり、その中に含まれる具体的な単語の性質に着目した処理ではなく、結果として分節してインデックスされた単語に氏名等の個人データが含まれていたとしても、個人データの「取扱い」に必ずなるとは限らないように思われます。

近年の検索機能はさらに高度化し、ベクトル埋め込み（Vector Embedding）が行われることもあります。これは、テキストを高次元の数値ベクトルに変換し、テキストとテキストの意味的な類似性を計算するものです[19]。この処理は、自然言語を数理的な座標に変換する情報検索工学的な処理であり、人間が意味内容を理解・評価するプロセスとは質的に異なりますが、最終的には人間による検索語との関連性などを補助する目的で行われる処理であって、データの内

[19] 意味の空間に、単語ごとの座標を与え、単語と単語の距離を数値的に計算するようなことを想像いただければと思います。

容に着目した処理を目的としているか否かは極めて微妙です。データ提供事業者による「目的」の汎用性に着目するのであれば、データを特に「個人データ」として処理することを目的とするとまでは言えず、「検索対象のオブジェクト」として機械的に処理しているものであり、個人データに対する編集・分析等の処理ではないと整理する余地も残るのではないかと思われます。

イ．固有表現抽出等の処理

一方で、自然言語処理技術の中には、固有表現抽出（Named Entity Recognition：NER） のように、テキストから人名、組織名、場所名を積極的に識別する技術も存在します。Stanford NLP Group が開発した Stanford NER や、自然言語処理のライブラリである spaCy 等は、テキストから固有表現を抽出するためのプログラムであり、抽出した単語に対して"PERSON"や"ORG"といったタグを付与します。これは明確に個人を識別することを目的とするソフトウェアプログラムであるため、このような技術による個人名の特定やタグ付けが、個人データに対する編集・分析等の処理であると見なされる可能性はかなり高まると考えられます。

ウ．バックエンド処理を含む実態判断の難しさ

クラウド利用を自らの「取扱い」と同視する以上、自らが利用するクラウドサービスがデータに対してどのような処理をしているのかを、自らの「取扱い」として把握しようとする姿勢は不可欠です。公開されている技術資料や利用規約を精査し、可能な範囲で事業者の説明を理解しようとするプロセスは、データの安全管理を考える上で実質的な意義を持ち、クラウド例外の適用を受けるための欠くべからざるステップであり続けるでしょう。

もっとも、クラウド事業者がバックエンドでどのような解析を行っているかによって「クラウド例外」の適否が変わるとすれば、利用者がその詳細を知ることは極めて困難であるという課題が残ります。巨大なクラウド提供事業者と個別に詳細な技術的対話を行うことは現実的ではありませんし、仮に具体的な使用ライブラリのような粒度での情報開示を求めれば、それは攻撃者への情報提供にもつながり、サイバーセキュリティ上の新たなリスクを招きかねません。また、クラウド環境は常に更新され迅速に変わり続けるため、ある時点でその仕様を確認できたとしても、その後の継続的な同一性を保証するものではありません。したがって、利用者の努力義務を前提としつつも、現実的な「クラウド例外」の適否の判断においては、該当する処理内容が技術的に特定された上で、事業者自身によってその適合性が「表明」されるかどうかが重要になるのではないかと考えます。

なお、どのような処理が行われているか判然としない場合等には、前掲注[17]のようなオプション（CSE、DKE 等）を利用することで平文での取扱いの余地を技術的に排除することを検討すべき場合があるかと思います。ただし、こうした暗号化オプションの採用は、全文検索の無効化やコスト増のみならず、マルウェア探知機能の無効化や、外部との暗号・複合鍵の通信発生による総合的なセキュリティレベルの低下といった大きなトレードオフを伴うものであり、総合的なバランスの考慮が必要となります。あるいは「委託」に該当することを受け入れるという判断も必要となるかと思います。

(5) 保守・運用のためのアクセス

ア．概要

保守・運用に関わるアクセス権限の議論には様々な要素が含まれ、クラウド例外を考える上での重要な論点となっています。

まず、本論における分類を当てはめると、基本的にはアプリケーション層以外に対する保守・運用は、アプリケーション層で処理するデータの内容に着目したデータアクセスと無縁であり、そもそも取扱いに該当するかを検討しないといけない場面が極めて限定的であると考えられます。

また、アプリケーション層においても、保守・運用のためのシステムによる自動的なアクセスについては、基本的にはサーバの死活監視やメタデータの把握、脆弱性対応としての各種アップデート・パッチ対応といったサービスの管理・維持、整合性確保のための処理が中心であり、データの中身（意味内容）に深く立ち入ることは稀だと考えられます[20]。

しかし、一方で、「自然人によるアクセス」を考えるとすれば、前項までで述べたような「純粋なコンピューティング処理か、意味内容の処理か」といった技術的な区分は、さほど重要ではなくなります。なぜなら、自然人がデータにアクセスする場合、そこには必ず何らかの「目的」が存在し、意識的か無意識的かを問わず、データの内容を認識し、その内容に注目してしまう蓋然性が高いからです。

イ．エムケイ社の事例における判断

このような「人間によるアクセス」のリスク管理について、エムケイ社に対する個人情報保護委員会の判断が重要な示唆を与えています。 同社のランサムウェア被害事案において、委員会は「クラウド例外」の適用を否定しました。その主な理由の一つとして、事業者が「保守用ID」を保有し、人間が個人データを閲覧可能な状態にあったにもかかわらず、「個人データの取得（閲覧にとどまらず、記録・印刷等をすること）を防止するための技術的な措置」が講じられていなかった点が挙げられました。また、利用規約において、保守運用上必要と判断した場合にデータの分析や調査ができる旨が規定されていたことも、例外非適用の判断要素となりました。アプリケーションの性質において、個人データの編集・分析等の処理を目的としていた場合、その自動的な処理に不具合が生じた時には、クラウドサービス提供事業者のエンジニアが管理者の特権アクセスを伴うアカウントによって不具合の再現を行う等の対応に当たることが通常だと考えられ、それは確かに、もはや個人データの取扱いに他ならないと考えられます。

ウ．技術的統制による例外適用の可能性

しかし、委員会が「技術的なアクセス制御等の措置が講じられているか否かが重要」であるとしている点は重要です。個人情報保護委員会がアクセス制御等の技術的な措置の有無を考慮事項としていることを考えると、単に「保守用 ID がある（人間がアクセスする可能性がある）」ことのみをもって、直ちにクラウド例外の適用余地を否定する趣旨ではなく、自然人はデータ

[20] 不具合の再現のために、データの内容に着目した機械的な処理がなされる可能性も排除できないでしょうが、現状ではやはり稀だと思われます。

の意味内容に着目したアクセスをするものであるという前提に立った上で、操作を適切に制限・監督し、データの持ち出し（コピー、印刷等）を物理的・技術的に制限する制御（Control）が徹底されていれば、エムケイ社の事例とは異なり、クラウド例外が適用される余地はあったと考えられます。筆者の考えとしては、取得を技術的に禁止することが必須というわけではなく、例えば特権 ID を管理するシステム[21]を用いて保守用 ID によるアクセスに対して事前承認や即時通知などの一定の牽制を行うこと、不正な取扱いをルールで禁止すること、不正な取扱いの否認（Repudiation）を防止できるだけの証跡を保全する技術的措置を講じること等の複数の control の組み合わせによる総合的なリスク低減等によって、「取扱い」の抑止がなされていたと認められる余地があるのではないかと思われます。正規の権限が目的外に濫用される可能性に対して、情報セキュリティの観点から実質的なリスク低減が図られていることこそが重要ではないかと考えられます。

また、自然人による「取扱い」の避けられない保守業務については、クラウドサービスの提供とは別個の独立した個人データの取扱いの委託と整理する余地もあったのではないでしょうか[22]。

4. 小括

本試論では、クラウドサービスにおける個人データの「取扱い」該当性について、技術的なレイヤー構造とデータ処理の質的実態に基づいた再定義を試みました。

結論として、個人データの「取扱い」の分水嶺は、事業者が当該データを「意味を持った情報」として利用・処理しているか、あるいは「中身に関知しない単なるビット列（ペイロード）」として処理しているかという点にあると考えられます。

この観点に立てば、アプリケーション層から切り離された IaaS／PaaS や、事業者がデータの内容に関与しないことが担保されている保管等のサービスについては「取扱い」に該当しないと整理する余地があると考えます。例えば、SaaS として提供されるクラウドストレージサービスにおける検索機能等についても、それが機械的なインデックス化や数理的な変換にとどまる限り、直ちに「取扱い」とは見なされない余地があると考えます。

また、保守・運用時のアクセス権限については、単に「物理的・技術的にアクセス可能か（Capability）」という二元論のみで判断するのではなく、特権 ID 管理や監査証跡といった技術的統制によって実質的に不正利用が抑止されているかを重視するという考え方もあり得るのではないかと指摘しました。

後編では、生成 AI の利用における「クラウド例外」の適用可能性について補論します。

---

[21] 特権 ID の管理は情報セキュリティ上も重要な施策であり、そのための機能として、PIM: Privileged Identity Management や PAM: Privileged Access Management などの名称で各種サービスにて提供されています。

[22] 実際に、SaaS ライセンスの提供とは別途、リセラーや提携企業によるエンジニアリングやサポートのサービスが提供されることも多いように思われ、契約形態等にもよりますが、そのような付随的なサポートを常に SaaS の提供と一体的に捉える必要はないと考えられます。

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。