弁護士法人　三宅法律事務所

Miyake　& Partners

Miyake newsletter

個人情報保護法ニュースＮｏ.17

個人情報保護法等改正法案と生成 AI

― 2026 年 4 月 7 日閣議決定法案が生成 AI 事業に及ぼす影響の体系的整理 ―

平素より大変お世話になっております。

さて、今回は個人情報保護法ニュース**「令和８年改正個人情報保護法案逐条解説―2026 年 4 月 7 日閣議決定法案を踏まえた詳細解説 ―」**をご案内させていただきます。

令和８年５月６日

弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。

弁護士法人三宅法律事務所

弁護士渡邉雅之、弁護士越田晃基、弁護士岩田憲二郎、弁護士出沼成真（執筆者）

TEL 03-5288-1021 FAX 03-5288-1025

Email: m-watanabe@miyake.gr.jp

k-koshida@miyake.gr.jp

k-iwata@miyake.gr.jp

n-idenuma@miyake.gr.jp

個人情報保護法等改正法案と生成 AI

― 2026 年 4 月 7 日閣議決定法案が生成 AI 事業に及ぼす影響の体系的整理 ―

はじめに

2026 年 4 月 7 日に閣議決定された「個人情報の保護に関する法律等の一部を改正する法律案」は、生成 AI を名指しで規律するものではない。しかし、生成 AI の**学習データ収集、モデル開発、ファインチューニング、外部委託、SaaS 提供、マルチモーダル利用、子ども向けサービス、広告・営業への活用**に対して、かなり広い範囲で影響を及ぼす。とりわけ中心となるのは「統計作成等」に関する新たな特例であるが、影響はそこにとどまらない。委託規律、連絡可能個人関連情報、特定生体個人情報、16 歳未満保護、不正取得罪、本人同意例外、命令・課徴金・罰則まで広く及ぶ。

本ニュースレターでは、これらの各論点について、**現行法の規律、改正法の内容、生成 AI への影響**の順で整理する。さらに、代表的な AI サービスとして、ChatGPT、Claude、Gemini について、その規約・ポリシーとの関係もあわせて検討する。

なお、生成 AI 事業は大きく**「開発段階」**（**学習データ収集、モデル構築、ファインチューニング、評価**）と、**「利用段階」**（**API 提供、SaaS 運用、出力制御、ユーザー対応**）に分かれ、改正法案の各条文がどちらの段階に影響するかは論点ごとに異なる。本ニュースレターでは、各論点の生成 AI への影響を述べる際に、それが主として開発段階の論点か、利用段階の論点か、あるいは両段階にまたがるかを明示する。これは制度改正方針[1]が、利活用促進と権利利益保護・執行強化を同時に扱っていることとも整合的である。

1　統計作成等の定義（第 2 条第 13 項）

(1) 現行法の規律

現行法の下でも、個人に戻らない一般的・集計的な統計情報の作成それ自体は、個人情報保護法の中心規制の外側で整理されやすかった。そもそも個人情報保護法は、「生存する個人に関する情報」であって、特定の個人を識別できるもの又は個人識別符号を含むものを「個人情報」とし、その取扱いに対して、利用目的の特定、目的外利用の制限、第三者提供規制、安全管理措置等義務を課している。他方で、統計情報や集計情報のように、特定の個人との対応関係が排斥され、個人に関する情報そのものではない結果物については、通常、個人情報保護法の直接の規律対象とはならないと理解されてきた。

しかし、現行法は、どこまでが「個人に戻らない分析」といえるのか、また、AI 学習のような大量データ解析が、取得・利用・第三者提供の各場面でどう評価されるのかを、条文上明示

[1]　『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（令和８年１月９日・個人情報保護委員会）』（https://www.ppc.go.jp/files/pdf/01-1_seidokaiseihousin.pdf）

していなかった。とくに、大規模言語モデルの事前学習では、インターネット上の膨大なテキストデータを収集し、言語パターンや知識構造を学習するが、この工程が現行法上の「利用」にあたるのか、また学習済みモデルが「個人データの保有」にあたるのかについて、明確な法的整理は存在しなかった。その結果、生成 AI 開発事業者は、大量データの取得・利用について、法的リスクの不透明さを抱えたまま事業を進めざるを得ない状況が続いていた。制度改正方針でも、AI・デジタル活用に対応した適正なデータ利活用ルールの必要性が明示されている。

(2) 改正法の内容

改正法案は、第 2 条第 13 項に「統計作成等」を新設する。これは、**統計の作成その他の大量の情報から当該情報を構成する要素に係る情報を抽出して分類比較その他の解析を行うことにより、当該大量の情報の傾向又は性質に係る情報（個人に関する情報であるものを除く。）を作成する行為のうち、個人の権利利益を害するおそれが少ないものとして個人情報保護委員会規則で定めるもの**をいう。これは、2026 年 1 月 9 日の制度改正方針が掲げた**適正なデータ利活用の推進**の中核概念として法定化されたものであり、4 月 7 日に公表された法律案要綱・新旧対照条文でも、その定義新設が条文上明示されている。

この定義には、少なくとも四つのポイントがある。

① 「大量の情報」を対象とする行為であること。したがって、少数の個人について個別に評価・推論する行為は、そもそもこの概念には入りにくい。

② 「要素情報の抽出」「分類比較その他の解析」を通じて、元データそのものではなく、そこから導かれる**傾向又は性質に係る情報**を作成する行為であること。

③ その結果物として作成される情報から、**個人に関する情報であるものを除く**と明記されていること。ここが極めて重要であり、個人ごとのスコアリング、個人別のレコメンド、個人に再接続される推論結果等は、ここから外れ得る。

④ 「個人の権利利益を害するおそれが少ないもの」に限られ、その具体的範囲は委員会規則に委任されていること。つまり、「大量データ分析」一般が自由になるわけではなく、あくまで低リスク類型として位置付けられるものに限定される。

このように、改正法は、従来の実務で暗黙のうちに「統計処理だから比較的自由」と整理されていた領域を、そのまま放置するのではなく、**法定概念として切り出し、後続の取得特例・提供特例・目的外利用禁止・課徴金制度と結び付ける**構造に改めている。ここに、今回改正の特徴がある。

(3) 生成 AI への影響

【主として開発段階の論点。利用段階にも波及】

生成 AI 事業者にとっての最大の論点は、自社の学習パイプラインのどの段階までが統計作成等に収まり、どこから個人に関する利用に転ずるのかの線引きである。

大規模言語モデルの事前学習（プレトレーニング）は、数兆トークン規模のテキストデータから言語の一般的パターン、文法構造、世界知識を学習する工程であり、特定個人に関する情報を作成するものではない。この工程は、統計作成等に整理される可能性が高い。

しかし、事前学習後の工程は個別に検討が必要である。ファインチューニングのうち、特定ドメインの一般知識を付加する工程は統計作成等に含まれ得るが、個人の嗜好、行動履歴、属性に基づいてモデルをカスタマイズする工程は、「個人に関する情報」を作成する方向に転じ得る。RLHF[2]についても、フィードバックデータが匿名化された一般的品質評価であれば統計作成等に含まれ得るが、特定個人の選好を学習する場合は範囲外となる可能性がある。

さらに、RAG[3]やプロンプトに含まれる個人情報の処理は、事前学習とは性質が異なり、統計作成等とは別の法的根拠で整理する必要がある。したがって、生成 AI 事業者は、自社のモデル開発工程を技術的に分節し、各工程について統計作成等への該当性を個別に検証する体制を整える必要がある。「AI 開発だから統計作成等」という一括整理は危険であり、工程ごとの丁寧な法的分析が不可欠である。

2　統計作成等の規律①：公開要配慮個人情報の取得特例（第 30 条の 2 第 1 項）

(1) 現行法の規律

現行法では、要配慮個人情報の取得には原則として本人同意が必要とされている。要配慮個人情報とは、人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないよう特に配慮を要する記述等が含まれる個人情報であり、その取得については、法第 20 条第 2 項により、法令に基づく場合等の限られた例外を除いて、本人同意が必要とされてきた。これは、情報がインターネット上に公開されている場合であっても、原則として適用される。

この規律は、生成 AI の大規模学習データ収集との間に深刻な緊張を生んでいた。大規模言語モデルの事前学習では、インターネット上のテキストを包括的にクローリングして収集するが、その中には要配慮個人情報が不可避的に含まれる。たとえば、ブログに書かれた闘病記録、SNS に投稿された宗教的信条、報道記事に含まれる犯罪歴情報、障害者支援団体のウェブサイトに掲載された障害に関する情報などである。数十億ページに及ぶウェブクローリ

---

[2] RLHF（Reinforcement Learning from Human Feedback）とは、AI の出力に対して人間が望ましさ・有用性・安全性などの観点から評価を行い、そのフィードバックを用いて AI の応答を改善する学習手法をいう。生成 AI の回答を、より人間の意図や社会的に望ましい基準に沿ったものに近づけるために用いられる。

[3] RAG（Retrieval-Augmented Generation）とは、AI が回答を生成する際に、事前学習した知識だけに依存せず、外部データベースや社内文書等から関連情報を検索し、その検索結果を参照して回答を生成する仕組みをいう。最新情報や個別資料に基づく回答を可能にし、生成 AI の誤回答を抑制する手法として利用される。

ング[4]において、これらの要配慮個人情報について個別に本人同意を取得することは、物理的に不可能である。制度改正方針でも、AI 学習との関係で、現行法がデータ利活用面で十分整理し切れていない領域があることが問題意識として示されている。

こうした状況の下、個人情報保護委員会は、令和 5 年 6 月 1 日付けで、ChatGPT を開発・提供する OpenAI, L.L.C.及び OpenAI OpCo, LLC に対し、法第 147 条の規定に基づき、要配慮個人情報の取得に関する注意喚起を行った（令和 5 年 6 月 2 日公表[5]）。同注意喚起は、あらかじめ本人の同意を得ないで、利用者及び利用者以外の者を本人とする要配慮個人情報を取得しないこと（法第 20 条第 2 項各号に該当する場合を除く。）を求めた上で、機械学習のための情報収集について、①収集する情報に要配慮個人情報が含まれないよう必要な取組を行うこと、②収集後できる限り即時に、収集した情報に含まれ得る要配慮個人情報をできる限り減少させるための措置を講ずること、③①及び②の措置を講じてもなお要配慮個人情報が含まれていることが発覚した場合には、できる限り即時に、かつ、学習用データセットに加工する前に、当該要配慮個人情報を削除し又は特定の個人を識別できないようにするための措置を講ずること、④本人又は個人情報保護委員会等が、特定のサイト又は第三者から要配慮個人情報を収集しないよう要請又は指示した場合には、拒否する正当な理由がない限り、当該要請又は指示に従うこと、の四点を遵守事項として示した。さらに、利用者が機械学習に利用されないことを選択してプロンプトに入力した要配慮個人情報について、正当な理由がない限り取り扱わないことも併せて求められた。同注意喚起は、現行法第 20 条第 2 項の本人同意原則を前提として、生成 AI 事業者によるウェブクローリング等を通じた要配慮個人情報の取得行為に対し、混入回避・即時削除・第三者要請への応諾という具体的行為規範を課したものであり、現行法の解釈・運用の枠内にとどまる対応であった。生成 AI 開発事業者がウェブ上の公開情報から要配慮個人情報を取得することそのものの法的不透明さは、依然として残されたままであった。改正法案による特例の新設は、この不透明さを立法的に解消することを目指すものである。

(2) 改正法の内容

改正法案は、第 30 条の 2 第 1 項により、個人情報取扱事業者が、次のいずれかの目的で、現に公開されている要配慮個人情報を取り扱う必要がある場合において、所定の公表を行っているときは、第 20 条第 2 項にかかわらず、本人同意なく当該要配慮個人情報を取得

---

[4] **ウェブクローリング（web crawling）**とは、プログラムがウェブサイト上のページを順次巡回し、情報を自動的に取得・収集する技術をいう。検索エンジンのインデックス作成、情報収集、データ分析等に用いられるが、対象サイトの利用規約、robots.txt、著作権・個人情報保護等への配慮が必要となる。

[5] 「OpenAI に対する注意喚起の概要」（令和５年６月２日・個人情報保護委員会）（https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf）

することができるとする。これは、今回改正の中核的な利活用特例として位置付けられている。

取得が認められる目的は、①統計作成等目的[6]及び②第三者提供目的[7]である。いずれの場合も、事業者名、取得した要配慮個人情報を用いて行おうとする統計作成等の内容又は提供目的その他必要事項を公表していることが要件となる。この特例が成立するための要件は、少なくとも次の四つである。

①取得目的が統計作成等又は法定提供目的であること。つまり、単なる一般的な業務利用では足りず、後続条文に接続する特例利用として位置付けられる必要がある。

②対象情報が「現に公開されている」こと。したがって、非公開情報、限定公開情報、又は取得時点で既に削除されている情報は、この特例の外にある可能性が高い。

③事業者名が公表されていること。

④統計作成等の内容又は提供目的その他必要事項が公表されていること。

すなわち、この特例は、単に「公開情報だからよい」というものではなく、**公開情報＋低リスク目的＋透明性確保**の三要素を組み合わせて初めて成り立つ。

また、この特例は、現行法の一般的な要配慮個人情報取得規制を全面的に緩和するものではない。あくまで、公開されている要配慮個人情報を、統計作成等という限定された類型に用いる場合に限って、本人同意の要件を外すものである。その意味で、改正法は、要配慮個人情報の保護の重み自体を弱めたのではなく、**生成 AI や統計的解析に必要な範囲で、例外的な法定ルートを新設した**と理解すべきである。

これにより、令和 5 年 6 月の OpenAI に対する注意喚起が示した遵守事項のうち、公開要配慮個人情報の取得そのものに関する部分は、改正法第 30 条の 2 第 1 項の要件（統計作成等目的＋現に公開＋事業者名等の公表）を充足する限りにおいて、法定の特例ルートにより整理されることになる。もっとも、注意喚起が求めた混入回避措置（①）、収集後の即時減少措置（②）、発覚時の削除・非識別化措置（③）、収集停止要請への応諾（④）といった行為

---

[6] 「統計作成等目的」とは、個人を特定しない統計情報の作成やこれに準ずる目的として改正法が定める目的をいう。

[7] 「第三者提供目的」とは、第 30 条の 2 第 5 項（下記（５）参照）が定める特例的な第三者提供を行う目的をいう。同項は、一定の要件を満たす第三者（国内の個人情報取扱事業者・行政機関の長等、又は外国にある者にあっては相当措置のための基準適合体制を整備している者）が統計作成等目的のみで個人情報を取り扱う場合に、提供者・第三者双方による公表（事業者名・統計作成等の内容等）および両者間の書面合意を条件として、利用目的制限（第 18 条）および第三者提供の本人同意原則（第 27 条第 1 項）の適用を除外し、本人同意なしの提供を認める規定である。取り扱う目的の全部が統計作成等目的でなければならず、また、同項により一度提供された情報を再び同項に基づいて転々提供することは禁じられている。第 30 条の 2 第 1 項が「同条第 5 項の提供目的」を掲げるのは、この第三者提供の連鎖の起点として要配慮個人情報を取得する場面を想定しているためである。

規範は、改正法案によっても変更されるものではなく、後記(3)で述べるとおり、特例の運用上引き続き重要な実務指針として機能するものと考えられる。

(3) 生成 AI への影響

【開発段階の論点】

この特例は、生成 AI 開発にとって最も直接的かつ実務的に大きな影響を持つ。

まず、大規模言語モデルの事前学習において、ウェブクローリングで収集したコーパスに要配慮個人情報が含まれている場合でも、統計作成等目的であり、かつ所定の公表を行っていれば、本人同意なく取得できるようになる。これにより、従来の法的不透明さが相当程度解消され、大規模学習データ収集の法的基盤が安定する。

しかし、いくつかの実務上の課題が残る。

①**公表義務の具体的な実装**である。生成 AI 開発事業者は、自社のウェブサイト等において、事業者名、取得する要配慮個人情報を用いて行う統計作成等の内容、提供目的等を公表しなければならない。ここでの「統計作成等の内容」をどこまで具体的に記載するかは、事業の機密性との間で緊張が生じ得る。「大規模言語モデルの事前学習に使用する」程度の記載で足りるのか、学習データの具体的なカテゴリ、データソースの種類、学習の目的・用途まで記載する必要があるのかは、今後の委員会規則や Q&A の整備を待つ必要がある。

②**要配慮個人情報の混入管理の問題**がある。大規模クローリングでは、取得するデータに要配慮個人情報がどの程度含まれているかを事前に正確に把握することは困難である。改正法案の特例は、「取り扱う必要がある場合」に取得を認めるものであるが、積極的に要配慮個人情報を探して収集することを認める趣旨ではない。したがって、生成 AI 開発事業者としては、可能な範囲でフィルタリングを行いつつ、不可避的に混入する要配慮個人情報については特例に基づく取得として整理するという二段構えの対応が必要になる。この点について、令和 5 年 6 月の OpenAI に対する注意喚起が示した四つの遵守事項（収集前の混入回避取組、収集後の即時減少措置、発覚時の削除・非識別化措置、第三者からの収集停止要請への応諾）は、改正法施行後における特例の運用上も、要配慮個人情報の取扱いに関する実務指針として引き続き参照されるべきものと考えられる。特に、特定のサイト又は第三者から収集停止の要請を受けた場合の応諾義務は、改正法案の特例が「取り扱う必要がある場合」に限定された取得を認めるものであることと整合的であり、特例の適用に際しても尊重されるべき行為規範である。

③**マルチモーダル AI[8]との関係**がある。画像生成 AI、動画生成 AI の学習では、インターネット上に公開された画像・動画を収集するが、その中には、障害の状態が視覚的に分か

[8] **マルチモーダル AI**（multimodal AI）とは、テキストだけでなく、画像、音声、動画、センサー情報など複数種類のデータを統合的に処理・理解し、回答や生成を行う AI をいう。たとえば、画像を読み取って説明したり、音声を文字化・要約したり、文

る画像、宗教的行事に参加する人物の画像、犯罪報道に付された顔写真等、要配慮個人情報を含むものが存在する。テキストデータと異なり、画像・動画に含まれる要配慮個人情報のフィルタリングは技術的により困難であり、特例の適用範囲と混入管理の方法について、テキスト AI とは異なる検討が必要になる。

④**国際的なデータ収集との関係**がある。インターネット上に公開された情報は国境を越えて存在するが、改正法案の特例は日本の個人情報保護法上の整理である。海外サーバに存在するデータの収集にこの特例が適用されるか、また、外国の個人情報保護法制との整合性をどう確保するかは、グローバルに事業を展開する生成 AI 事業者にとって別途検討が必要な論点である。

3　統計作成等の規律②：統計作成等の内容・提供目的等の継続公表義務（第 30 条の 2 第 2 項・第 3 項）

(1) 現行法の規律

現行法において、個人情報取扱事業者は、利用目的の通知・公表義務を負っているが、これは取得時又は取得後速やかに行えばよく、その後の変更がない限り、継続的な公表を法律上の義務として明確に求められていたわけではない。プライバシーポリシーを一度策定して掲載すれば、更新しなくても直ちに違法になるわけではなかった。

生成 AI 開発では、学習データの収集対象、学習の目的、モデルの用途が開発過程で変化することが多い。事前学習段階では汎用的な言語能力の獲得が目的であっても、その後のファインチューニング[9]で特定分野への応用が加わり、さらに外部提供や API 公開を通じて用途が拡大する。こうした変化に対して、現行法は十分な透明性メカニズムを提供していなかった。制度改正方針も、利活用を認める代わりに透明性と統制を求める方向を示している。

(2) 改正法の内容

改正法案は、第 30 条の 2 第 2 項により、特例取得者は、その情報を取り扱っている期間中、事業者名、統計作成等の内容又は提供目的その他必要事項を継続して公表しなければならないとする。さらに、同条第 3 項により、公表事項の内容に変更があった場合には、原則として、あらかじめ変更内容を公表しなければならない。これは、取得時の一回的な公表で足りるのではなく、取扱期間全体を通じた継続的透明性を法律上の義務として課すものである。

章と画像を組み合わせて分析したりすることができる。

[9] **ファインチューニング**（fine-tuning）とは、事前学習済みの AI モデルに対し、特定の業務・分野・用途に関する追加データを用いて再学習させ、出力の精度や適合性を高める手法をいう。たとえば、法務、医療、金融など特定領域の文書や回答例を学習させることで、その領域に即した応答を行いやすくする。

公表の「継続」とは、単に一度掲載したページを削除しないということではなく、公表内容が現在の取扱実態を正確に反映している状態を維持することを意味すると解される。変更時の事前公表義務についても、「原則として」とされているため例外はあり得るが、その範囲は委員会規則に委ねられている。たとえば、軽微な変更まですべて事前公表が必要なのか、統計作成等の本質に影響しない技術的変更は事後報告で足りるのかは、今後の整備を待つ必要がある。

(3) 生成 AI への影響

【開発段階・利用段階の双方にまたがる論点】

生成 AI 開発事業者にとって、継続公表義務は、データガバナンスの運用面に大きな影響を与える。

まず、公表内容の管理体制の構築が必要になる。生成 AI の開発サイクルは高速であり、学習データの追加、モデルのバージョンアップ、用途の変更、API 提供先の拡大等が頻繁に行われる。これらの変更が公表事項に影響する場合、その都度、変更内容を事前に公表しなければならない。したがって、開発チーム、法務部門、広報部門の間で、変更の有無と公表の要否を継続的に確認するプロセスを整備する必要がある。

次に、公表の粒度の問題がある。「統計作成等の内容」をどこまで具体的に公表するかは、事業の機密性と透明性のバランスが問われる。たとえば、「自然言語処理モデルの事前学習のため」という抽象度で足りるのか、「日本語テキスト約 X 億トークンを使用し、汎用的な対話応答能力の向上を目的とする事前学習」程度の記載が必要なのか、さらにはデータソースの具体的カテゴリまで記載する必要があるのかが論点になる。この点については、今後、個人情報保護委員会のガイドラインや FAQ で示されることになるだろう。

さらに、学習完了後の公表義務の継続期間も実務上重要である。事前学習が完了し、モデルが本番運用に移行した後も、学習データを保持・管理している限り「取り扱っている期間」に該当し、公表義務は継続する。モデルの世代交代に伴い旧モデルの学習データを削除するまで、公表を維持する必要がある可能性がある。加えて、オープンソースモデルとの関係も問題になる。学習済みモデルをオープンソースとして公開する場合、モデルの利用者がそのモデルを再利用・再配布する行為は、元の特例取得者の公表義務とどう関連するのかは、新たな論点として浮上し得る。

4　統計作成等の規律③：特例取得された要配慮個人情報等の目的外利用禁止・第三者提供制限（第 30 条の 2 第 4 項以下）

(1) 現行法の規律

現行法においても、利用目的の制限は存在し、事業者は、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならないとされている。他方で、利

用目的の変更自体は、「変更前の利用目的と関連性を有すると合理的に認められる範囲」で許容される構造であり、その関連性判断には一定の幅があった。したがって、いったん適法に取得した個人情報について、その後の利用の広がりをどこまで許せるかは、個別事案ごとの評価に委ねられる面が大きかった。

このことは、生成 AI 開発の実務では特に問題になりやすい。事前学習用として収集したデータが、その後、ファインチューニング、評価用データセット、品質検証、ベンチマーク、モデルの安全性テスト、営業デモ、顧客向けカスタマイズ、広告最適化等へと横展開されることは珍しくない。しかし、こうした二次利用や目的の横展開が、現行法上どこまで「関連性を有すると合理的に認められる範囲」に入るのかは、必ずしも明確ではなく、事業者ごとに整理が分かれやすかった。特に、公開されている要配慮個人情報を含むデータを用いる場合には、本来強い保護が求められる一方で、現行法には、今回の改正法案のような「特例で取得したデータはその特例の範囲に厳格に拘束される」という専用の出口規制は存在していなかった。

(2) 改正法の内容

改正法案は、第 30 条の 2 第 4 項以下により、特例取得された要配慮個人情報等について、通常の個人情報よりも一段厳しい出口規制を設けている。

すなわち、**統計作成等用要配慮個人情報等**[10]については、原則として、公表された統計作成等の内容又は提供目的を実現するために必要な範囲を超えて取り扱ってはならないという構造が採られている。ここで重要なのは、通常の利用目的制限のような「関連性を有すると合理的に認められる範囲」での変更を広く認めるのではなく、**特例取得時に公表した内容に厳格に結び付けて利用を固定する**点である。つまり、改正法案は、入口で特例を認める代わりに、出口では「その特例のためにだけ使う」という強い拘束を課している。

また、第三者提供についても、改正法案は、一般の第三者提供規律とは異なる厳格な構造を採る。特例取得された要配慮個人情報等については、原則として第三者提供が禁止され、その上で、法が特に認めた場合に限って例外的に提供が可能となる。実

---

[10] **「統計作成等用要配慮個人情報等」**とは、第 30 条の 2 第 1 項の規定により本人同意なく取得された要配慮個人情報、又はその全部若しくは一部を複製し若しくは加工した生存する個人に関する情報をいう（第 30 条の 2 第 4 項）。ただし、同条第 5 項第 1 号の個人情報保護委員会規則で定める方法により第三者に提供された個人情報又はその全部若しくは一部を複製し若しくは加工した生存する個人に関する情報（「提供統計作成等用個人情報等」。同条第 6 項）は除かれる。

際、法案は、特例に基づいて個人情報の提供を受けた第三者について、**提供統計作成等用個人情報等**[11]として継続公表義務（第 30 条の 2 第 6 項）や変更公表義務（第 30 条の 2 第 7 項・第 8 項）を課し、その後の取扱いを独自に拘束している。

さらに、個人関連情報ベースの特例提供についても、**提供統計作成等用個人データ等**として同様の継続公表・変更公表の仕組みを設けている。これは、特例ルートに乗った情報について、提供元だけでなく提供先側にも、透明性と目的拘束を連鎖させる設計である。

さらに重要なのは、これらの特例違反が、課徴金制度と密接に結び付いていることである。改正法案は、第 148 条の 3 以下に課徴金制度を置き、統計作成等特例に基づき取得した個人情報を、特例に違反して目的外利用し、又は第三者提供する行為等を課徴金対象に含めている。したがって、今回の改正は、単に「特例データは厳格に使え」という義務規定にとどまらず、**逸脱した場合には経済的不利益を伴う制度**として構成されている。その意味で、特例取得された要配慮個人情報等の目的外利用禁止・第三者提供制限は、今回改正の中でも、入口と出口をもっとも強く結び付けた部分の一つである。

(3) 生成 AI への影響

【開発段階・利用段階の双方にまたがる論点】

この規律は、生成 AI 事業者のデータ利活用の全工程に影響する。

① 第一に、**学習データの目的限定管理**が不可欠になる。
事前学習目的で収集した公開要配慮個人情報を含むコーパスを、その後、ファインチューニング、個人向けサービスのカスタマイズ、ターゲティング広告の最適化、採用スクリーニング用モデルの構築、与信判断用モデルの構築等に転用することは、公表された統計作成等の内容を超える目的外利用と評価される可能性が高い。特に、個人別の推論、選別、配信最適化、判断支援のような利用は、「傾向又は性質に係る情報」の作成という統計作成等の枠を外れやすく、特例の趣旨と最も衝突しやすい。したがって、生成 AI 事業者は、**どのデータセットが特例取得データなのか、そのデータがどの工程まで利用可能なのか**を、通常データとは別建てで管理する必要がある。

② 第二に、**社内での二次利用管理**が極めて重要になる。

---

[11] **「提供統計作成等用個人情報等」**とは、第 30 条の 2 第 5 項第 1 号の個人情報保護委員会規則で定める方法により第三者に提供された個人情報（統計作成等用要配慮個人情報等を含む。）、又はその全部若しくは一部を複製し若しくは加工した生存する個人に関する情報をいう（同条第 6 項）。

生成 AI 事業者は、研究部門、製品開発部門、営業部門、マーケティング部門、顧客導入支援部門等、複数の部門を持つことが多い。そのため、事前学習用に収集した特例取得データが、社内の他部門によって別目的で利用される危険が現実にある。改正後は、こうした社内横展開も、単なる内部利用だからといって当然に許されるわけではなく、**公表された統計作成等の内容を超えれば目的外利用**となり得る。したがって、アクセス制御、利用権限管理、利用目的の記録、データ分類表示、監査ログ、承認フローなど、社内統制そのものが適法性の中核になる。

③ 第三に、**課徴金リスクとの直結**がある。
統計作成等特例に違反した目的外利用や第三者提供は、単なる義務違反ではなく、課徴金対象行為に接続し得る。しかも、今回の課徴金制度は利得剥奪型であり、違反行為又はその中止の対価として得た財産上の利益相当額が問題になる構造である。生成 AI 事業は、モデル開発、API 提供、SaaS 課金、広告最適化、顧客向けソリューション提供など、データ利活用がそのまま収益と結び付きやすい。そのため、特例取得データを違法に横展開した場合、法的リスクは単なる指摘や是正命令にとどまらず、**事業収益そのものに跳ね返る経営リスク**となる。ここでは、目的外利用の防止は法務部門だけの課題ではなく、経営陣が関与すべき財務リスク管理の課題になる。

④ 第四に、**モデルの世代間でのデータ引継ぎ**の問題がある。
第一世代モデルの事前学習に使用した特例取得データセットを、第二世代モデルの事前学習や追加学習にも用いる場合、それが同一の統計作成等の範囲内といえるのか、それとも新たな統計作成等として改めて公表や整理が必要になるのかは、実務上の重要論点である。モデルの目的、機能、対象市場、出力の性質が大きく変わる場合には、もはや同一の「統計作成等の内容」とはいいにくく、新たな公表や別の法的根拠が必要になる可能性が高い。したがって、生成 AI 事業者は、**モデルのバージョンアップや世代更新を、単なる技術的継続としてではなく、法的に同じプロジェクトか別プロジェクトかという観点からも点検する必要**がある。

⑤ 第五に、**提供後のコントロール**も重要になる。
特例ルートで外部の共同研究先、受託先、グループ会社等にデータを渡す場合、渡した後の先方での取扱いが、提供統計作成等用個人情報等又は提供統計作成等用個人データ等として別途拘束される構造になっている。したがって、生成 AI 事業者は、単に自社内だけを統制すれば足りるのではなく、**提供先との契約、継続公表の確認、再提供禁止、目的外利用禁止、監査権限**まで含めて、出口管理を設計しなければならない。統計作成等特例は、自由な連携ルートではなく、**高透明・高拘束型の連携ルート**として理解すべきである。

要するに、この規律は、生成 AI との関係で、

① **特例取得データを「後で何にでも使えるデータ」にしないこと、**
② **社内外を通じて利用目的と利用工程を固定すること、**
③ **逸脱時には課徴金を含む重大リスクが生じること、**
④ **モデル更新や再利用のたびに法的根拠を再点検すること、**

を求めるものである。今回の改正により、公開要配慮個人情報を含む学習データの利活用は、入口で取りやすくなる半面、出口では従来よりはるかに厳しく管理しなければならない領域になる。

5　統計作成等の規律④：統計作成等目的のための第三者提供ルート（第 30 条の 2 第 5 項～第 10 項、第 31 条の 3）

(1) 現行法の規律

現行法の下では、個人データの第三者提供には原則として本人同意が必要であり、同意なき提供が認められるのは、法令に基づく場合、生命・身体・財産の保護に必要な場合、公衆衛生の向上に特に必要な場合等、限定的な例外に限られていた。そのため、**「第三者が統計的・分析的処理を行うために個人データを受け取る」こと自体を、本人同意なしで広く許容する一般的な法定ルートは存在していなかった**。生成 AI 開発の実態では、データ保有者から AI 開発事業者へのデータ移転、企業間の共同研究におけるデータ共有、AI 開発受託におけるデータ提供等が日常的に行われているが、これらの多くは、本人同意に基づくか、又は匿名加工情報・統計情報への加工を経たうえでの提供として整理されてきた。

しかし、匿名加工情報への加工にはコストと情報量の損失が伴い、また、大量の個人データについて個別に本人同意を取得することは実務上困難である。そのため、**本人同意も匿名加工も使いにくいが、なお一定の透明性・拘束の下で第三者に渡したい**というニーズに対する制度的受け皿が不足していた。ここが、前項の「特例取得された要配慮個人情報等の目的外利用禁止・第三者提供制限」と異なる出発点である。前項は、**特例で取得したデータをその後どう縛るか**という「出口規制」の話であったのに対し、本項は、**そもそも第三者にどう渡せるのか**という「提供ルートの新設」の話である。両者は連動するが、法的機能は異なる。

(2) 改正法の内容

改正法案は、**第 30 条の 2 第 5 項**により、個人情報取扱事業者が、第三者に対して個人情報を統計作成等目的で提供するための新たな法定ルートを設けている。条文上、第三者が個人情報を**統計作成等目的で取り扱う必要がある場合**であって、かつ、当該個人情報を取り扱う目的の全部が統計作成等目的である場合に限り、一定の要件の下で、**第 18 条（利用目的の制限）及び第 27 条第 1 項（第三者提供の制限）にかかわら**

ず、本人同意なく当該第三者に提供することができるとされている。すなわち、これは一般的な第三者提供規制の例外を、統計作成等に限って新設するものである。

この特例が成立するための要件は、条文上かなり明確である（以下の①から③までを全て満たす必要がある）。

① **提供先の第三者が、個人情報を統計作成等目的で取り扱う必要があること**。

② 提供元と提供先の双方が、インターネット利用その他規則で定める方法により、**双方の氏名又は名称、行おうとする統計作成等の内容その他規則事項を公表していること**。

③ 提供元と提供先との間の**書面又は電磁的記録による合意**により、当該提供がこの特例に基づくものである旨が明確に定められていること

である。つまり、単に「分析目的で渡します」と内部で理解していれば足りるのではなく、**公表＋契約明記**が法定要件として置かれている。

さらに、法案は、この特例ルートを通じて提供された後の情報についても、提供先側に独自の義務を課している。**第 30 条の 2 第 6 項**は、提供を受けた第三者のうち個人情報取扱事業者である者を「特例個人情報受領者」とし、その者が、提供を受けた個人情報又はその全部若しくは一部を複製し、若しくは加工した生存する個人に関する情報を取り扱っている期間、一定事項を**継続して公表**しなければならないとする。**第 7 項・第 8 項**は、その公表事項の変更について、原則事前公表、例外的に事後速やかな公表を求める。さらに、**第 9 項**は、提供統計作成等用個人情報等について、法令に基づく場合等を除き、**公表された統計作成等を行うために必要な範囲を超えて取り扱ってはならない**と定めている。したがって、この特例は、提供した瞬間に自由になるルートではなく、**提供先でも継続的透明性と目的拘束が続くルート**である。

加えて、**第 30 条の 2 第 10 項**は、**統計作成等用要配慮個人情報等**又は**提供統計作成等用個人情報等**である個人データについて、原則として第三者提供を禁止し、法定の場合を除くほか提供してはならないとする。これは、本項の特例が「一回限りの統計作成等目的提供」を認める一方で、そこから先の再流通を原則禁止する趣旨を明確にしている。つまり、この制度は、**自由なデータ流通市場を開くものではなく、提供先を特定し、その提供先による統計作成等のためだけに使わせる制度**なのである。

さらに、**第 31 条の 3** は、個人関連情報取扱事業者が、第三者に対して個人関連情報を統計作成等目的で提供する場合の特例を設けている。構造は第 30 条の 2 第 5 項以下とほぼ対応しており、提供先の目的限定、公表、契約明記、提供後の継続公表、目的外利用禁止等が連動している。したがって、本項の見出しを「第三者提供特例」とだけすると曖昧になりやすいが、実際には、**個人情報についての統計作成等目的提供ルート（30 条の 2 第 5 項以下）**と、**個人関連情報についての統計作成等目的提供ルート（31 条の 3）**を合わせた制度として理解するのが正確である。

(3) 生成 AI への影響

【主として開発段階の論点。利用段階にも波及】

この特例は、生成 AI のエコシステム全体に、**「本人同意なし・匿名加工なしで、一定の透明性と契約拘束の下にデータを渡す」ための新たな法的ルート**を提供する。前項が「特例で取得したデータをどう縛るか」という話だったのに対し、本項は、**データ保有者から AI 開発事業者、共同研究先、グループ会社、受託先へ、どう適法に渡すか**という入口の話である。その意味で、前項と重複するのではなく、むしろ生成 AI 実務では両者をセットで理解する必要がある。すなわち、**この項で適法に渡し、前項でその後の利用を厳格に縛る**という関係に立つ。

第一に、**AI 開発受託におけるデータ提供**が整理しやすくなる。事業会社がデータを保有し、AI 開発事業者がモデルを構築する場合、これまでは、委託、共同利用、匿名加工、本人同意のいずれで整理するかが難しい場面が多かった。改正後は、第三者である AI 開発事業者が、受け取ったデータを統計作成等目的で取り扱う必要があり、かつその目的の全部が統計作成等目的である限り、提供元・提供先双方の公表と契約明記を条件として、本人同意なく提供する道が開かれる。したがって、生成 AI 受託案件では、**「これは委託なのか、それとも特例提供なのか」**をより意識的に設計する必要がある。

第二に、**業界横断的なデータ連携**に法的根拠が与えられる。たとえば、医療機関、製薬企業、研究機関、保険関連事業者等が保有するデータを、医療支援 AI や創薬支援 AI のモデル開発のために生成 AI 事業者へ渡す場面では、従来は匿名加工情報に加工するか、個別同意を取るか、別制度を使うかという整理が中心だった。改正後は、統計作成等目的であり、公表と契約条件を満たす限り、個人情報のまま提供できる可能性が出てくる。その意味で、この特例は、**データ保有者と AI 開発者の間に、第三の選択肢を与える制度**である。

第三に、**グループ企業間のデータ連携**にも影響がある。親会社が保有する顧客データを、グループ内の AI 開発子会社や分析子会社に渡してモデル開発を行わせる場合、従来は共同利用又は委託で整理することが多かった。しかし、実態としては、子会社側が独自の統計作成等やモデル構築を担うのであれば、第三者提供特例に基づく整理も選択肢になる。もっとも、その場合でも、グループ内だから緩くてよいということにはならず、**双方の公表、契約明記、提供後の継続公表、目的外利用禁止**が課される点は同じである。グループ内であっても、法的には「限定的な提供ルート」であることに変わりはない。

第四に、**個人関連情報の提供**にも新たな意味が出る。生成 AI では、Cookie、閲覧履歴、位置情報、デバイス識別子、行動ログ等の個人関連情報を教師データ、補助特徴量、検索補助データとして使う場面が多い。第 31 条の 3 は、こうした個人関連情報に

ついても、統計作成等目的での提供ルートを設けているため、個人情報だけでなく、**個人関連情報ベースの生成 AI 開発・分析プロジェクトにも適用可能性**がある。とりわけ、個人関連情報を提供先で個人データ化することが想定されるような場面では、従来の個人関連情報規制との関係整理も含めて、制度上の位置付けがより明確になる。

他方で、この特例には重要な限界がある。最大の限界は、**提供先での目的外利用と再提供が厳しく制限されること**である。したがって、提供を受けた AI 開発事業者が、そのデータを別案件の学習に流用したり、別の顧客向けモデル開発に転用したり、再度外部の別事業者に渡したりすることは、原則として許されない。また、提供を受けたデータを使って構築した**学習済みモデル**をさらに第三者にライセンスする場合、そのモデルに元データ由来の情報がどこまで残っているのか、モデルの提供が再提供と評価されないか、といった問題も出てくる。法案は、この点を明示的に生成 AI モデルに即して書いているわけではないが、少なくとも、**学習済みモデルの提供であれば自動的に自由**とはいえず、データ残存性や復元可能性、モデルの性質に応じた慎重な分析が必要になる。

したがって、生成 AI 開発の委託契約やデータ提供契約では、従来以上に、**学習目的の限定、利用可能工程、評価・ベンチマーク利用の可否、モデル改善利用の可否、学習済みモデルの提供先制限、ログ管理、監査権限、契約終了時のデータ削除義務**等を精緻に作り込む必要がある。本項の特例は、自由度を高める制度ではあるが、同時に、**公表義務と契約拘束によって高い透明性と拘束性を要求する制度**でもある。したがって、実務的には、「データ提供がしやすくなる」だけでなく、「**契約と統制をきちんと組まないと使えない制度**」と理解するのが正確である。

6　委託を受けた事業者に関する規律（第 30 条の 3、第 58 条の 2）

(1) 現行法の規律

現行法の下でも、委託先は委託元との関係で一体として扱われ、委託業務の範囲外で個人データを取り扱うことは許されないと考えられてきた。しかし、その構造は、主として**委託元の監督義務**を通じて間接的に実現するものであった。すなわち、現行法 25 条は、個人データの取扱いの全部又は一部を委託する場合に、委託元が委託先に対し必要かつ適切な監督を行うべきことを定めているが、そこでは、委託先自身に対して「委託業務の範囲を超えて利用してはならない」という**独立の直接義務**が、法文上正面から置かれていたわけではない。したがって、委託先の範囲外利用は、実務上は違法と整理されていても、条文構造としては、まず委託元の監督不十分の問題として把握されやすかった。

このことは、従来型の単純な受託処理では大きな支障を生じにくかった。たとえば、印字、封入封緘、発送、入力、スキャン、保管等のように、委託先が委託元の細

かな指示どおりに機械的・受動的に処理するだけの場面では、委託先が独自に取扱いの意味を決める余地は比較的小さかったからである。ところが、クラウド、SaaS、BPO、AI 開発受託、データ加工受託、コールセンター、保守運用、ログ解析など、近時のデータ処理は、委託先が実質的に大量データへアクセスし、一定の裁量をもって取扱方法を決める場面が増えている。その結果、「これは単なる委託先か」「それとも独立したデータ取扱主体なのか」「サービス改善や品質向上のための利用は委託の範囲内か」といった点が、現行法の枠内では曖昧になりやすかった。

また、いわゆる**「クラウド例外」**として、外部事業者が契約上・運用上、保存された個人データを「取り扱わないこととなっている」場合には、第三者提供にも委託にも当たらない、という整理が Q&A 上用いられてきた。しかし、SaaS や生成 AI 連携では、現実には、保守のためのアクセス、障害対応、ログ保持、解析、セキュリティ監視、学習利用、品質向上利用などが問題となることがあり、この「取り扱わない」という前提がどこまで維持できるのかが、従来から実務上の大きな論点であった。制度改正方針も、**データ取扱い態様の多様化に対応し、委託・受託の実態に即した規律整備が必要**との問題意識を示している。

要するに、現行法の下では、委託関係は、委託元による監督義務を中核として整理されており、委託先の範囲外利用禁止は実務上認められていても、法文上の直接義務としては明確でなく、しかもクラウド・SaaS・AI 受託のような新しい処理形態では、どこまでが委託の範囲内かが見えにくかった、というのが実情であった。

(2) 改正法の内容

改正法案は、まず**第 30 条の 3** を新設し、委託先自身に対し、**委託を受けた業務の遂行に必要な範囲を超えて個人情報を取り扱ってはならない**という直接義務を課す。これは、現行法下で事実上委託元の監督義務の反射として捉えられていた範囲外利用禁止を、委託先の**固有の法的義務**として法文化したものである。つまり、改正法は、委託先を単なる補助者としてではなく、少なくとも一定の場面では、**自ら違法な取扱いを行い得る主体**として捉え直している。

ここで重要なのは、第 30 条の 3 が、単に「委託元の指示に違反してはいけない」というレベルにとどまらず、**委託業務遂行に必要な範囲**という基準で、委託先の取扱可能範囲を法定している点である。このため、委託先が、受託データを自社の分析、品質向上、広告、営業、別サービス開発、汎用 AI 学習などに転用する行為は、そのような利用が契約上・実態上、委託業務の中に明確に位置付けられていない限り、原則として問題化しやすくなる。言い換えれば、改正法は、「受託したから使える」のではなく、「委託業務遂行に必要だから使える」という方向へ整理を明確に改めたのである。

他方で、改正法案は、委託先規律を一律に重くしているわけではない。**第 58 条の 2** を新設し、他の個人情報取扱事業者等又は行政機関等から取扱いの全部又は一部の委託を受けた者が行う個人情報等の取扱いについて、**委託契約において取扱方法として委員会規則で定める事項等が定められており、かつ、その取扱いが委託業務遂行に必要な範囲内で契約どおりに行われるとき**は、本法の一部規定を適用しない仕組みを設けている。これは、データ入力、印字、発送、スキャン、形式変換など、受託者が自ら処理内容を決めない**機械的・受動的受託処理**については、全面的に通常の個人情報取扱事業者として扱うのが過剰になるためである。

もっとも、この適用調整は広く自動的に認められるものではない。少なくとも、委託契約において、取扱方法や必要事項が**具体的に定められていること**、その取扱いが**委託業務遂行に必要な範囲内**であること、そして実際の運用が**契約どおり**であることが必要である。したがって、単なる秘密保持条項や一般的な善管注意義務条項だけでは足りず、事故報告、取扱状況把握、権限管理、再委託条件等も含めた相当程度具体的な契約設計が求められると考えられる。

このように、改正法は、委託先規律について、独自判断を伴う委託先には**直接義務**を課し、自ら取扱方法を決定しない機械的受託者には**限定的な適用調整**を認める、という二段構造を採っている。ここに今回改正の精緻化の特徴がある。従来の「委託か、委託でないか」という二分法から一歩進み、**誰がどこまで取扱方法を決めているのか**に応じて規律を組み分ける方向へ進んだと評価できる。

(3) 生成 AI への影響

【開発段階・利用段階の双方にまたがる論点】

生成 AI との関係では、この改正は極めて大きい。なぜなら、生成 AI サービスの多くは、形式的には「受託」「API 提供」「SaaS 提供」「クラウド提供」「業務委託」などの形をとりながら、実際には、ログ保持、モデル改善、品質評価、ガードレール調整[12]、安全性分析、性能評価、異常検知などの名目で、入力データや出力データに幅広くアクセスし得るからである。そのため、従来は契約実務上あいまいに処理されてきた「顧客データをどこまで自社で使えるのか」という問題が、改正後は**第 30 条の 3 違反になり得るか**という形で、より直接的に問われることになる。

開発段階では、たとえば AI 開発受託において、顧客から提供を受けたデータを用いて特定モデルを構築するはずだったのに、そのデータを自社の**汎用基盤モデルの学習**や、他案件向けモデルの改善、将来の汎用サービス向けの教師データ、ベンチマーク、評価セットとして流用する行為が、範囲外利用の典型例になる。委託先側として

---

[12] **ガードレール調整**（guardrail tuning）とは、生成 AI が不適切・危険な出力を抑制しつつ、過度に回答を拒否しないよう、出力制御の基準・閾値・ルール等を調整することをいう。安全性と有用性のバランスを確保するために行われる。

は「品質向上のため」「サービス改善のため」「一般的な安全性向上のため」と説明したくなるが、改正法の下では、そのような説明だけでは足りず、**それが本当に委託業務遂行に必要な範囲に含まれているか**、契約上・実態上明確に基礎付けられている必要がある。逆にいえば、受託データを汎用学習に使いたいのであれば、委託という整理だけでは不十分であり、別の法的構成や明示的な契約・同意・提供ルートの検討が必要になる。

利用段階でも同様である。API 提供型生成 AI や SaaS 型生成 AI では、ユーザーの入力データや会話ログを、モデル改善、品質向上、不正利用検知、安全性評価等に使う実務が広く見られる。しかし、改正後は、そのような利用が、単なる「受託処理」や「機械的処理」の範囲に当然入るとは言いにくくなる。特に、ログを分析してモデル応答を改善したり、ユーザー入力を学習素材にしたりする場合、そこには委託先又はサービス提供者の**独自判断**が介在するため、第 58 条の 2 のような機械的受託処理の適用調整には乗りにくい可能性が高い。そのため、生成 AI 事業者は、**どこまでが顧客のための処理で、どこからが自社のための利用なのか**を、契約・システム設計・内部ルールの三面から切り分ける必要がある。

また、いわゆるクラウド例外との関係でも、生成 AI は従来型クラウドより厳しく見られやすい。単なる保存インフラであれば「取り扱わないこととなっている」と整理できた場面でも、生成 AI では、保守、障害対応、ログ解析、プロンプトモニタリング[13]、モデル改善、ガードレール評価[14]など、**実際にデータへアクセスし得る・解析し得る・二次利用し得る**局面が多い。そのため、「これはクラウドだから自動的に例外」という発想は維持しにくくなり、むしろ、**委託先の直接義務が及ぶのか、機械的受託処理に当たるのか、そもそも委託ではなく第三者提供や共同利用として整理すべきなのか**を個別に見極めることが必要になる。

実務対応としては、まず契約面の見直しが不可欠である。生成 AI 事業者は、受託データや入力データについて、どのデータを何の目的で、どこまで保持し、誰がアクセスし、モデル改善や安全性評価に使うのかを、契約上明確にしなければならない。次に、技術面では、データ区分管理、権限分離、ログ管理、学習対象データの隔離、顧客別モデルと汎用モデルの切分けなどの統制が必要になる。さらに運用面では、営業

---

[13] **プロンプトモニタリング**（prompt monitoring）とは、生成 AI に入力されるプロンプトの内容を記録・分析し、不適切な利用、機密情報・個人情報の入力、プロンプトインジェクション等のリスクを検知・管理することをいう。生成 AI の安全な運用、利用実態の把握、ガードレール改善等のために行われる。

[14] **ガードレール評価**（guardrail evaluation）とは、生成 AI が不適切・危険・法令違反となり得る出力を行わないように設けられた制御措置（ガードレール）が、実際に有効に機能しているかを検証する評価をいう。たとえば、個人情報、差別的表現、違法行為の助長、機密情報の漏えい等に関する出力抑制の有効性を確認するために行われる。

資料やFAQで「入力データは改善に使われます」「使われません」と説明している内容と、実際の内部運用が一致していることが重要になる。改正後は、**契約上の整理、技術的アクセス制御、実際の運用実態**の三つがそろって初めて適法性を説明しやすくなる。

要するに、この改正は、生成AI事業者に対し、受託データを自社の汎用学習や別案件改善に流用しないこと、APIやSaaSの入力ログ利用を「当然の改善利用」とみなさないこと、クラウド例外に安易に依存しないこと、そして、契約・技術・運用の三面から**受託処理と自社利用の境界を可視化すること**、を強く求めるものである。生成AI分野では、この委託先規律の改正は、統計作成等特例と並んで、実務インパクトの大きい改正の一つといってよい。

7　連絡可能個人関連情報（第2条第8項、第31条の2）

(1) 現行法の規律

現行法でも、「個人関連情報」それ自体が全く無規制というわけではない。令和2年改正法により、**個人関連情報の第三者提供規制**が導入されており、提供元は、提供先において当該個人関連情報が個人データとして取得されることが想定される場合には、本人同意の有無等を確認した上で提供しなければならない、という仕組みが既に設けられている。すなわち、現行法は、Cookie、閲覧履歴、位置情報その他の個人関連情報が、提供先で個人データ化される局面については、一定の規律を及ぼしている。

もっとも、現行法の個人関連情報規制は、主として**「第三者提供先で個人データになるか」**という場面を捉えるものであり、個人関連情報そのもののうち、**特定個人に連絡し、働きかけ、情報を到達させることができる類型**を、独立のリスク類型として正面から規律する構造にはなっていなかった。そのため、電話番号、メールアドレス、所在地、端末識別子等が、直ちには個人情報に当たらない又は提供先で直ちに個人データ化されないという整理がされると、実務上は「比較的自由に使える」と理解されやすい余地があった。

しかし、制度改正方針は、この点に明確に問題意識を示している。すなわち、近年、電話番号、メールアドレス、住所、端末識別子等を用いた**詐欺、悪質勧誘、違法な送客、ストーカー的接触その他の権利利益侵害**が拡大しており、従来の「個人識別性」中心の整理だけでは、こうした被害リスクを十分に捉え切れないとされた。そのため、個人情報保護委員会は、**犯罪行為等の不適正利用形態による権利利益侵害リス**

クの高まりを受け、特定個人に働きかけ可能な個人関連情報について新たな規律が必要との方向を示した。

要するに、現行法の下では、

① 個人関連情報一般については一定の第三者提供規制がある、

② しかし、それは「提供先で個人データになるか」を中心にした規律である、

③ そのため、**個人に到達・接触できる情報そのものの危険性**を正面から捉えるには不十分であった、

というのが現状である。今回の改正は、このギャップを埋めるものとして理解すべきである。

(2) 改正法の内容

改正法案は、まず第 2 条第 8 項に**「連絡可能個人関連情報」**という新たな定義を設ける。これは、個人関連情報のうち、特定の個人に対する連絡その他の情報の伝達に利用することができる記述等を含むものをいう。法案上は、典型例として、①住居、勤務先その他の特定個人が所在し、又は所在していた場所の所在地、②電話番号、③電子メールアドレス、④電気通信設備の利用者又は電気通信設備を識別することができるように付された符号、⑤その他委員会規則で定めるもの、が挙げられている。また、これらに直接当たらなくても、他の情報と容易に照合することによりこれらの記述等を特定できるものも含まれる。つまり、改正法は、単に「個人が識別できるか」ではなく、**「その個人に到達し、接触し、働きかけることができるか」**に着目して、新たな保護対象を設定している。

次に、改正法案は、第 31 条の 2 を新設し、個人関連情報取扱事業者に対して、**違法又は不当な行為を助長し、又は誘発するおそれがある方法により、連絡可能個人関連情報を利用してはならない**とする不適正利用禁止を課す。これは、単に詐欺や違法勧誘の結果が生じた場合だけを問題にするのではなく、そうした違法・不当行為を助長又は誘発するおそれのある利用方法自体を規制対象にするものである。したがって、改正法は、結果規制ではなく、**リスクある利用態様の段階でブレーキをかける構造**を採っている。

さらに、第 31 条の 2 は、**偽りその他不正の手段により、連絡可能個人関連情報を取得してはならない**という不正取得禁止も定める。これは、従来の個人情報についての不正取得禁止に対応する形で、連絡可能個人関連情報についても、取得段階から規律を及ぼすものである。たとえば、なりすまし、虚偽申告、権限逸脱、スクレイピング[15]

[15] **スクレイピング**（scraping）とは、ウェブサイトやアプリケーション上の情報を、

態様によっては、不正取得の問題が生じ得ることになる。つまり、改正法は、**利用段階だけでなく取得段階にも規律を入れる**ことで、連絡可能個人関連情報の流通経路全体をコントロールしようとしている。

このように、改正法は、

① 連絡可能個人関連情報という新たな類型を法定し、

② その不適正利用を禁止し、

③ その不正取得も禁止する、

という三段構えを採っている。したがって、今回の改正は、単なる定義追加ではなく、**個人関連情報のうち「人に届く」「人に接触できる」情報を、独立の危険類型として捉え直した制度改正**である。これにより、「個人情報ではないから自由」という従来の整理には、明確な歯止めがかかる。

(3) 生成 AI への影響

【主として利用段階の論点。開発段階にも波及】

利用段階では、生成 AI を使った**営業リスト補強、スクレイピングしたメールアドレスへの自動営業文面生成、送客 DB 分析、広告配信最適化、電話・メール勧誘スクリプト生成、ターゲット抽出**等の場面で、直接この規律が問題になる。特に、生成 AI は、大量の連絡先データや周辺属性データを入力すれば、誰にどのようにアプローチすべきか、どの文面・タイミングが効果的かを高度に最適化できるため、**違法又は不当な行為を助長・誘発するリスク**を一気に高め得る。したがって、改正後は、「営業効率化」「広告最適化」「リードスコアリング」といった名目であっても、その実質が詐欺的勧誘、違法送客、過度な接触、脆弱な相手への不当な働きかけにつながるなら、第 31 条の 2 の不適正利用禁止との関係が問題になり得る。

また、生成 AI が**連絡先情報を含む出力**を生成する場面にも注意が必要である。たとえば、ウェブ上の情報を要約させた結果として電話番号やメールアドレスを抽出して返す、あるいは「この業界の見込み顧客リストを作れ」「問い合わせ先を一覧化せよ」といったプロンプトに応じて、特定個人に接触可能な情報を整理・出力するような利用は、利用目的や利用態様によっては不適正利用を助長し得る。そのため、生成 AI サービス提供者にとっては、**出力段階でのフィルタリング、危険用途の検知、利用**

プログラム等により自動的に抽出・取得する技術をいう。特定ページから必要なデータを抜き出す用途で用いられるが、対象サイトの利用規約、著作権、個人情報保護、不正アクセス防止法等への配慮が必要となる。

規約上の禁止、監査ログの保存が重要になる。単に入力データの適法性だけでなく、**出力がどう使われるかまで見据えた制御**が必要になる。

さらに、広告・マーケティング分野では、生成 AI を用いて、連絡可能個人関連情報と周辺属性情報を結び付け、**「反応しやすい相手」「断りにくい相手」「心理的に脆弱な相手」に最適化された接触戦略を組み立てることが技術的には可能である。しかし、改正法の趣旨からすれば、こうした利用は、まさに違法又は不当な行為を助長・誘発するおそれがある方法**として評価され得る。したがって、生成 AI の導入によって営業・広告の精度が上がるほど、法的リスクも高まるという関係を、事業者は正面から認識しなければならない。

開発段階でも波及は大きい。ウェブクローリングやデータセット収集により、学習データの中に**電話番号、メールアドレス、所在地、端末識別子その他の連絡可能個人関連情報**が大量に含まれ得るからである。この場合、単に「公開されていたから取得した」で済むわけではなく、その取得態様が**偽りその他不正の手段**に当たらないかが問われる。たとえば、アクセス制御を潜脱した取得、利用規約に反する自動取得、なりすまし登録による取得、本人が容易に予期しない態様での大量抽出などは、不正取得性の評価に影響し得る。したがって、生成 AI 開発事業者は、学習データ収集段階においても、**どの連絡先データが含まれているか、どのような態様で取得されたか、除去・マスキング・利用制限をどう設計するか**を検討する必要がある。

さらに、生成 AI の評価・ファインチューニング段階でも問題は残る。たとえば、営業特化型モデル、採用候補者接触支援モデル、送客支援モデル、CRM 支援モデル等を訓練する際に、実在の電話番号やメールアドレスを含むデータセットを使えば、モデルが**連絡先情報をそのまま再出力したり、接触行動を最適化する方向に学習したりするリスク**がある。この意味で、連絡可能個人関連情報の規律は、単に「現場での使い方」の問題にとどまらず、**モデル設計・学習データ設計・安全性評価の問題**にも直結する。生成 AI 事業者としては、連絡可能個人関連情報を含むデータについて、通常の個人関連情報よりも一段慎重な取扱いを行い、必要に応じて**学習対象から除外する、匿名化・マスキングする、危険出力を抑制する**などの統制を講じることが望ましい。

要するに、連絡可能個人関連情報の新設は、生成 AI との関係で、

① **営業・広告・送客・接触支援といった利用段階**に直接効く、

② **学習データ収集・評価・ファインチューニングといった開発段階**にも波及する、

③ そのため、**入力規制・出力規制・利用規約・取得態様管理・学習データ管理を一体で設計する必要がある、**

という意味を持つ。今回の改正は、生成 AI を用いた「人に届く情報」の利活用に対し、従前と比較してかなり強い注意義務を課すものと理解すべきである。

8　特定生体個人情報（第 16 条第 5 項、第 21 条の 2、第 27 条第 2 項、第 35 条第 7 項・第 8 項）

(1) 現行法の規律

現行法には、「特定生体個人情報」という類型は存在しなかった。もちろん、顔画像、指紋、虹彩、静脈、声紋等の生体情報が、個人識別符号を含む個人情報又は通常の個人情報に該当する場合には、利用目的の特定、目的外利用の制限、第三者提供規制、安全管理措置、保有個人データに関する開示・訂正・利用停止等の一般規律は及んでいた。しかし、それはあくまで**一般的な個人情報規律の適用**にとどまり、今回の改正法案のように、**本人が容易に認識できない形で取得される顔特徴データ等**を特に切り出して、専用の保護ルールを設ける構造にはなっていなかった。

そのため、現行法の下では、顔識別機能付きカメラ、防犯カメラ連携の顔照合、来店者分析、入退館管理、本人確認用顔認証等について、個人情報保護法が全く及ばないわけではないものの、**「どのような生体情報が特に強い保護を受けるのか」「本人にどこまで分かる形で説明・周知すべきか」「本人が後から停止を求められる範囲はどこまでか」**が、法文上必ずしも明確ではなかった。特に、顔画像そのものではなく、顔の特徴点を抽出・変換したテンプレートデータや顔特徴データについては、実務上その扱いが分かりにくく、一般論としての個人情報規律だけでは対応が不十分との指摘があった。

また、現行法では、オプトアウト制度に基づく第三者提供についても、特定の生体情報類型を名指しで除外する仕組みは設けられていなかった。もちろん、要配慮個人情報や違法取得情報等には別の制約があるが、**生体情報が「変更困難であり、一度流通すると回復が困難で、監視・追跡・排除・差別に直結し得る」**という性質それ自体に着目した流通制限は、法文上は十分ではなかった。さらに、利用停止等請求権についても、一般の保有個人データの枠組みの中で処理されるにすぎず、顔特徴データのような継続利用リスクの高い情報について、本人の離脱可能性を特に広く認める明文の特則はなかった。

この点について、制度改正方針は、**顔特徴データ等について、その取扱いに関する一定の事項の周知を義務化し、利用停止等請求の要件を緩和するとともに、オプトアウト制度に基づく第三者提供を禁止する**方向を明確に示した。すなわち、現行法の一般規律では、生体情報、とりわけ**本人が認識しにくく、容易に取得され得る生体情報**の保護としては不十分であり、専用規律が必要だというのが今回改正の出発点である。

(2) 改正法の内容

改正法案は、第 16 条第 5 項に**「特定生体個人情報」**を新設する。条文上、これは、特定生体個人識別符号が含まれる個人情報をいう。そして、その前提となる「特定生体個人識別符号」は、第二条第二項第一号に該当する個人識別符号のうち、特別の技術又は多額の費用を要しない方法により取得することができる身体の一部の特徴に係る情報であって、当該情報が取得されていることを本人が容易に認識することができないものとして政令で定めるものを変換したものとされている。制度改正方針の概要資料は、ここで主として**顔特徴データ等**を想定していることを明示している。つまり、改正法は、生体情報一般ではなく、**本人が気づきにくく、かつ比較的容易に取得できる類型**を狙い撃ちして、新たな保護対象として切り出している。

その上で、改正法案は、少なくとも三つの特則を置いている。第一に、**第 21 条の 2** による周知義務である。制度改正方針は、顔特徴データ等について、**その取扱いに関する一定の事項の周知を義務化**するとしており、改正後は、事業者が特定生体個人情報を取り扱うに当たり、事業者情報、取扱いの事実、利用目的、身体の一部の特徴に係る情報の内容、開示等請求手続等を、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置くことが求められる。これは、単に一般的なプライバシーポリシーを置いておけば足りるという発想ではなく、**「顔認証等を使っていること自体」と「何の特徴情報をどう使うか」**を本人に分かる形で示させるものである。

第二に、**第 27 条第 2 項**によるオプトアウト第三者提供の禁止である。制度改正方針は、顔特徴データ等について、**オプトアウト制度に基づく第三者提供を禁止する**としている。これは、本人関与の弱い形で第三者提供を可能にするオプトアウト制度と、特定生体個人情報の強い保護必要性とは両立しないという判断に基づくものである。したがって、特定生体個人情報については、本人同意又は法定例外による場合を除き、**「後から止められるからよい」という仕組みでは流通させてはならない**ことが法文化される。

第三に、**第 35 条第 7 項・第 8 項**による利用停止等請求権の拡張である。制度改正方針は、顔特徴データ等について、**利用停止等請求の要件を緩和する**としている。これは、一般の保有個人データについての利用停止等請求よりも一段広く、本人が自らの特定生体個人情報の利用停止又は第三者提供停止を求めやすくする趣旨である。つまり、改正法は、特定生体個人情報について、**取得時の透明性、流通制限、本人による離脱可能性**の三方向から規律する構造を採っている。これは、生体情報が変更困難であり、一度流通・蓄積・照合されると、監視、追跡、排除、差別に直結し得ることを強く意識した改正である。

要するに、改正法案は、

① 特定生体個人情報という新たな保護類型を法定し、

② その取扱いを本人に分かるようにさせ、
③ オプトアウト流通を禁止し、
④ 本人が後から停止を求めやすくする、
という四段構えで、生体情報保護を一段引き上げている。これは、従来の一般的個人情報規律だけではカバーし切れなかった顔特徴データ等のリスクに、正面から対応するものである。

(3) 生成 AI への影響

【開発段階・利用段階の双方にまたがる論点】

開発段階では、画像生成 AI、顔認識 AI、映像解析 AI、マルチモーダル AI が、**顔画像・映像・監視カメラ映像・SNS 投稿画像・公開動画等を学習データとして収集・使用する場面**が、まず問題になる。改正法の想定する「特定生体個人情報」は、主として顔特徴データ等であり、かつ「本人が容易に認識できない形で取得され得る」類型であるため、生成 AI の学習データ収集が、単に一般的な画像データの取得ではなく、**顔特徴データを伴う取得**として評価される可能性がある。したがって、顔認証・人物識別・属性推定・人物追跡等の能力を持つモデルの学習では、どの段階で特定生体個人情報を取り扱うのか、どの範囲で周知義務が及ぶのか、収集元データが公開情報であるとしても別の専用規律がかかるのではないかを、慎重に整理する必要がある。

特に、顔画像を単に「画像」として学習させる場合と、そこから顔特徴を抽出・変換して人物識別可能なテンプレートを生成・利用する場合とでは、法的評価が大きく異なり得る。前者であっても、実質的に顔特徴抽出が組み込まれていれば、後者に近づく。したがって、生成 AI 開発事業者は、**自社モデルが画像をどう処理しているのか、顔特徴の抽出・保持・再利用があるのか、人物識別性が残るのか**を技術的に検証しなければならない。単に「画像生成 AI だから顔認証ではない」といったラベル付けでは足りず、実際のデータ処理内容が問われる。

また、学習データの取得元にも注意が必要である。監視カメラ映像、店舗来訪者映像、イベント会場映像、公共空間の動画等には、本人が容易に認識しないまま取得された顔特徴データが含まれている可能性が高い。こうしたデータを生成 AI の訓練に用いる場合、**元の取得段階で適法に周知されていたか**、再利用が許される範囲か、委託・第三者提供・共同利用のいずれで整理すべきかが重要になる。さらに、顔特徴データが含まれるデータセットを外部から取得する場合には、オプトアウト提供禁止との関係上、そのデータ流通ルート自体が違法となる可能性もある。そのため、生成 AI 開発事業者は、顔画像・映像データのサプライチェーン全体について、**取得元の適法性、契約上の利用可能範囲、再利用可否、第三者提供制限**を点検する必要がある。

利用段階では、最大の課題は**利用停止等請求への対応**である。本人から「自分の顔特徴データの利用をやめてほしい」「第三者提供を止めてほしい」と請求された場

合、通常のデータベースであればレコード削除や利用停止で対応できるが、生成 AI では、顔特徴データが既に学習済みモデルの重みに取り込まれている可能性がある。この場合、学習済みモデルから特定データだけを正確に除去する、いわゆる**アンラーニング**は技術的に困難である。したがって、改正法の下では、生成 AI 事業者は、**停止請求にどこまで応答可能か、学習前データ、ベクトル化データ、特徴抽出データ、評価用データ、モデル本体の各段階で何が止められるか**をあらかじめ設計しなければならない。

さらに、ディープフェイク生成や人物なりすまし生成との関係でも、この規律は重要である。特定個人の顔特徴データを用いて、その人物らしい画像・映像・音声を生成する行為は、単なる著作権や肖像権の問題にとどまらず、特定生体個人情報の取扱い、連絡可能個人関連情報との結合、不適正利用禁止、不正取得罪の射程にも入り得る。特に、本人が知らないうちに SNS 画像や公開動画から顔特徴を抽出し、人物生成 AI に組み込むような行為は、改正法の趣旨からすれば極めて危険である。したがって、人物生成 AI や映像合成 AI を提供する事業者は、**実在人物の顔特徴データの取扱いをどう制限するか、本人同意や権利処理をどう確保するか、危険出力をどう防止するか**を、従来以上に厳格に設計する必要がある。

また、利用段階では、入退館管理、本人確認、決済認証、オンライン本人認証等で生成 AI が顔照合・顔一致判定・異常検知に用いられるケースも増えている。このような場合、単に「精度が高いか」では足りず、**周知義務を満たしているか、停止請求にどう応じるか、第三者提供や共同利用のルートが適法か**が問われる。特に、顔認証を補助する生成 AI やマルチモーダル AI は、画像理解・属性推定・照合支援を一体で行い得るため、どこまでが「本人確認のための必要利用」で、どこからが過剰な分析利用かの線引きも重要になる。

要するに、特定生体個人情報の新設は、生成 AI との関係で、

① 顔特徴データを含む学習データの取得・再利用の適法性、

② 学習済みモデルに取り込まれた生体情報への停止請求対応可能性、

③ ディープフェイクや人物生成 AI の危険利用抑止、

④ 顔認証・本人確認 AI の透明性と利用統制、

という四つの大きな論点を生む。したがって、生成 AI 事業者にとっては、特定生体個人情報は、単なる「画像データの一部」ではなく、**特別に強い本人関与と流通制限を伴う高リスク情報**として、学習段階から運用段階まで一貫して別扱いすべき対象になる。

9　本人同意例外（第 18 条第 3 項、第 20 条第 2 項、第 27 条第 1 項）

(1) 現行法の規律

現行法でも、利用目的外利用（法 18 条1項）、要配慮個人情報取得（法 20 条2項）、第三者提供（法 27 条1項）について、一定の本人同意例外が存在していた。たとえば、法令に基づく場合、人の生命、身体又は財産の保護に必要な場合、公衆衛生の向上又は児童の健全育成の推進に特に必要な場合、学術研究機関等による学術研究に必要な場合等である。しかし、これらの例外には、「本人の同意を得ることが困難であるとき」という要件が付されるものが多く、実務上は比較的硬直的であった。つまり、本人に接触可能である以上、同意取得が原則であり、同意に依拠しないこと自体に合理性がある場合を十分に拾いきれていなかった。

また、契約履行に当然伴う処理であっても、個別の取得・利用・提供局面ごとに厳密に同意の要否を検討せざるを得ず、本人の合理的期待に沿った処理であるにもかかわらず、法的整理が複雑化しやすいという問題もあった。制度改正方針でも、本人関与に係る規律の在り方を見直す中で、こうした現行法の硬直性が論点として整理されている。

(2) 改正法の内容

改正法案は、生命・身体・財産保護、公衆衛生、児童健全育成等の例外について、従来の「本人の同意を得ることが困難であるとき」に加え、**本人の同意を得ないことについて相当の理由があるとき**を追加する。これは、第 18 条第 3 項第 2 号・第 3 号、第 20 条第 2 項第 2 号・第 3 号、第 27 条第 1 項第 2 号・第 3 号にまたがる改正である。すなわち、改正法は、単なる物理的・時間的な「困難性」だけでなく、本人同意に依拠しないことに公益上・実務上の合理性がある場合を拾う方向に踏み出している。

さらに、改正法案は、**「本人の意思に反しないことが明らかな場合」**という新たな同意例外を設ける。これは、第 18 条第 3 項第 7 号、第 20 条第 2 項第 7 号、第 27 条第 1 項第 8 号として新設されるもので、本人との間の契約の履行のために必要やむを得ないことが明らかな場合等、取得の状況からみて本人の意思に反せず、権利利益を害しないことが明らかな場合を想定している。ここでの判断基準は、事業者の都合ではなく、**本人の合理的期待**である。したがって、包括的な利用規約に書いてあるだけでは足りず、取得状況や取引の性質から、本人が通常予期する処理であることが必要になる。

このように、改正法は、本人同意例外を無限定に広げたのではなく、**公益性・相当性と本人の合理的期待**という二つの軸で、現行法の硬直性を緩和したものである。これは、本人関与の原則を維持しつつ、実態に即した運用可能性を高める改正と評価できる。

(3) 生成 AI への影響

【主として利用段階の論点。開発段階にも波及】

利用段階では、ユーザーが自ら入力した情報を対話応答のために処理することは、契約履行に必要かつ本人が通常予期する処理として、「本人の意思に反しない」と整理し得る。しかし、入力データをモデル改善に使う場合や別サービスに転用する場合は、「本人の意思に

反しない」とはいいにくく、別途の同意又は法的根拠が必要になる。したがって、入力データの対話応答処理とモデル改善利用は明確に分けて法的整理を行う必要がある。
開発段階への波及としては、公衆衛生や災害対応の場面で生成 AI を活用する場合に、「相当の理由」による例外が適用される余地がある。

10　16 歳未満の者の保護（第 35 条第 9 項・第 10 項、第 40 条の 2、第 58 条の 3）

(1) 現行法の規律

現行法には、16 歳未満の者の個人情報について、今回の改正法案のような包括的な明文特則は置かれていなかった。もちろん、未成年者の個人情報であっても、個人情報保護法の一般規律、すなわち利用目的の特定、目的外利用の制限、第三者提供規制、安全管理措置、保有個人データに関する開示・訂正・利用停止等の一般ルールは及んでいた。しかし、それはあくまで一般ルールの適用であり、「16 歳未満であること」それ自体に着目した特別の保護構造は、法文上は明確でなかった。

そのため、実務では、未成年者対応は主として個人情報保護委員会 Q&A やガイドライン、各事業者の自主的運用に委ねられていた。たとえば、未成年者からの同意取得については、本人の判断能力やサービスの性質に応じて、親権者等の関与を求める運用が行われることがあったが、これは法律上の統一的な明文ルールではなく、事業者ごとにばらつきがあった。また、未成年者本人に対して通知・公表を行えば足りるのか、法定代理人に対する説明や同意取得が必要なのかも、場面ごとに解釈と実務運用に委ねられていた。

さらに、現行法上の利用停止等請求権は、一定の違法性や要件該当性を前提とする一般的な構造であり、未成年者であること自体を理由として保護を強める仕組みにはなっていなかった。そのため、SNS、ゲーム、動画配信、教育サービス、位置情報サービス等において、子どもが長期にわたりサービス利用に組み込まれ、対話履歴、行動履歴、興味関心、学習履歴等が継続的に蓄積・利用される場面でも、法文上は未成年者固有の離脱権や特別な本人関与ルールが十分には整備されていなかった。

この点について、2026 年 1 月 9 日の制度改正方針は、16 歳未満の者が本人である場合、同意取得や通知等について法定代理人を対象とすることを明文化し、保有個人データの利用停止等請求の要件を緩和するとともに、未成年者の個人情報等の取扱いについて、本人の最善の利益を優先して考慮すべき旨の責務規定を設ける方向を明示した。すなわち、現行法下では Q&A・慣行レベルにとどまっていた未成年者保護を、法律レベルの明文規律へ引き上げる必要があるというのが、今回改正の出発点である。

(2) 改正法の内容

改正法案は、16 歳未満の者の保護について、第 35 条第 9 項・第 10 項、第 40 条の 2、第 58 条の 3 を中心に、複数の条文を組み合わせた包括的な保護構造を導入する。

これは単なる一つの条文追加ではなく、本人関与、法定代理人関与、事業者の行為規範を三方向から整備する改正である。

第一に、第 35 条第 9 項・第 10 項により、16 歳未満の者が本人である場合には、当該本人の保有個人データについて、利用停止等又は第三者提供停止を求めることができる場面が拡張される。個人情報保護委員会の概要資料と制度改正方針はいずれも、**「利用停止等請求の要件を緩和する」**と明示している。これは、現行法の一般的な利用停止等請求権よりも、16 歳未満本人については一段強い離脱可能性を認める趣旨である。すなわち、未成年者が継続的利用に巻き込まれやすく、かつ一度形成されたプロファイルや履歴の影響を長期に受け得ることを踏まえ、事後的に利用から離脱しやすくする方向に改めるものである。

第二に、第 40 条の 2 により、16 歳未満の者が本人である場合には、同意取得や通知等について、原則として**「本人」を「法定代理人」と読み替える**仕組みが導入される。これにより、これまで Q&A や実務慣行で処理されていた、親権者等の関与の要否が、法律上の明文規律として位置付けられることになる。つまり、16 歳未満の者については、単に本人に説明し、本人から形式的同意を取得すれば足りるという整理ではなく、法定代理人を正面から関与させることが、法文上の基本構造になる。これは、未成年者本人の理解力・判断力に限界があり得ることを前提に、本人保護の実効性を高めるものである。

第三に、第 58 条の 3 により、事業者に対し、16 歳未満の者の個人情報等の取扱いについて、本人の最善の利益を優先して考慮すべき旨の責務規定が設けられる。ここが今回改正の中でも特に重要である。この規定は、単なる同意手続や通知手続の整備にとどまらず、サービス設計や運用の実質に対して、「子どもの最善の利益」という価値基準を法的に持ち込むものである。制度改正方針と概要資料の双方が、この規定を 16 歳未満保護の柱として明示しており、形式的な同意の有無だけでは足りず、事業者の設計・運用全体が未成年者保護の観点から評価されることを意味する。

このように、改正法案は、16 歳未満の者の保護を、

① 法定代理人関与の明文化、
② 利用停止等請求権の強化、
③ 最善の利益の責務規定

という三本柱で再構成している。これにより、未成年者保護は、単なる同意取得の問題にとどまらず、事後的離脱可能性とサービス設計の適切性まで含む構造へと進む。

(3) 生成 AI への影響

【主として利用段階の論点】

利用段階では、教育サービス、子ども向けチャットボット、学習支援 AI、ゲーム内 AI、相談支援 AI、動画推薦 AI 等において、**年齢確認の仕組み、法定代理人からの同**

意取得手続、法定代理人向け通知、利用停止等請求への対応体制の整備が必要になる。現行法下では、未成年者対応は事業者ごとの運用に委ねられやすかったが、改正後は、16 歳未満である場合に法定代理人関与を前提とする以上、**年齢把握をどう行うか**が避けて通れない論点になる。もっとも、過度な年齢確認はそれ自体新たな個人情報取得を伴うため、どこまでの確認が必要か、どのような確認方法が相当かは、今後の委員会規則・Q&A を踏まえた設計が必要になる。

また、利用停止等請求の要件緩和は、生成 AI サービスにとって実務上かなり重い意味を持つ。子ども向けサービスでは、対話履歴、検索履歴、学習履歴、推薦履歴、位置情報、課金履歴等が長期に蓄積されやすい。改正後は、16 歳未満本人又は法定代理人から、これらの利用停止や第三者提供停止を求められる可能性が、現行法下より高くなる。したがって、生成 AI 提供者は、**どのデータが保有個人データに当たるか、停止請求に応じられる技術的・運用的体制があるか**を事前に設計しなければならない。特に、RAG 用ログ、推薦学習用ログ、プロファイリング用データセット等をどう切り分けて管理するかが重要になる。

さらに、第 58 条の 3 の**最善の利益の責務**により、生成 AI サービスの **UI/UX、対話設計、推薦ロジック、継続利用設計**そのものが法的評価の対象になり得る。たとえば、依存誘発的な対話設計、長時間利用を煽る UI、過度なエンゲージメント最適化、不適切応答の抑制不足、過剰課金誘導、年齢に不相応な推奨内容、心理的に過度に強い擬人化などは、「最善の利益を優先して考慮しているか」という観点から問題視され得る。したがって、子ども向け生成 AI では、**安全性評価や有害出力抑制だけでなく、サービス設計全体を未成年者保護の観点から再点検する必要**がある。サービス設計そのものが法的評価の対象になるという点で、利用段階への影響が最も大きい。

開発段階への副次的影響としては、子どもの入力データを学習データやモデル改善データに取り込むことの当否が問題になる。16 歳未満のユーザーの対話履歴、学習履歴、行動データ、フィードバックデータをモデル改善に使用する場合は、法定代理人の関与が必要となり得るし、最善の利益の観点からも、**そもそもそのような二次利用が相当か否か**が問われる。したがって、生成 AI 事業者は、未成年ユーザー由来のデータについて、**通常ユーザーデータとは別建てで管理し、学習利用の可否や条件を厳格に設計する必要**がある。

11　命令・課徴金

(1) 現行法の規律

現行法の下でも、個人情報保護委員会には、報告徴収・立入検査、勧告、命令といった監督手段が存在していた。しかし、その基本構造は、違反事実を把握した上で是正を求めるというものであり、**本人保護のための対外的措置まで機動的に命じる仕組**

みとしては十分とはいえなかった。とりわけ、違法な第三者提供や大規模な不適正利用があっても、本人への通知や事実の公表を、個人情報保護法上の命令としてどこまで直接求められるのかは、必ずしも明確ではなかった。

また、現行法には、悪質な個人情報取扱いによって経済的利益を得た事業者に対して、その**利得を吐き出させる課徴金制度**は存在していなかった。そのため、大量の個人情報を不正又は不適正に利用・提供し、事業上の利益を得るような事案に対しては、行政上の勧告・命令だけでは抑止力に限界があると考えられていた。

要するに、現行法の下では、①命令は存在していても、**本人通知・公表まで含む本人保護命令としては弱かったこと**、また、②悪質な違反に対しても、**経済的不利益を直接課す制度が欠けていたこと**、この二つが大きな限界であった。

(2) 改正法の内容

改正法案は、まず命令関係について、**第 148 条**で、違反行為の是正にとどまらず、**本人に対する違反行為に係る事実の通知又は公表その他本人の権利利益の保護のために必要な措置**を命じ得る構造へと改めている。また、**第 148 条の 2** では、違反行為を補助等する第三者に対し、当該違反行為の中止のために必要な措置等をとるよう要請できる枠組みが置かれている。法案によれば、改正後の命令は、単なる内部是正命令ではなく、**本人保護命令**へと拡張されている。

次に、改正法案は、**第 148 条の 3 から第 148 条の 17 まで**を新設し、**課徴金納付命令等**の制度を導入している。法案によれば、個人情報の違法な取扱い等によって財産上の利益を得た場合に、個人情報保護委員会が課徴金納付を命ずる制度が設けられる。すなわち、売上高連動型ではなく、**違反行為によって得た利益を基礎とする利得剥奪型**の制度として設計されている。

課徴金の対象について、

① 法 19 条違反のうち一定の不適正利用、

② 法 20 条 1 項違反としての不正取得・利用、

③ 法 27 条 1 項違反としての本人同意なき第三者提供、

④ 統計作成等の特例に係る義務違反

が対象となる。とくに重要なのは、**統計作成等特例違反**が、単なる一般義務違反ではなく、課徴金対象行為に含まれていることである。法案によれば、統計作成等のために認められた取得・提供ルートを逸脱し、目的外利用や不適切な第三者提供を行った場合には、課徴金対象となり得る。

さらに、法案によれば、課徴金は、対象行為に当たれば当然に課されるわけではなく、少なくとも、

①相当の注意を怠ったこと、

②本人の数が 1,000 人を超えること、

③個人の権利利益を害する程度が大きくない場合に当たらないこと、

といった要件でさらに絞り込まれる。そして、課徴金額は、**対象行為又は対象行為をやめることの対価として得た財産上の利益相当額**とされる。つまり、今回の課徴金制度は、**悪質性・規模性・実害性を備えた違反行為について、違法利得を吐き出させる制度**として構成されている。

このように、改正法案は、

- **第 148 条による本人保護命令、**
- **第 148 条の 2 による違反補助者への要請、**
- **第 148 条の 3 以下による利得剥奪型課徴金制度**

を組み合わせることにより、事後的規律を一体的に強化している。ここが、現行法からの大きな転換点である

(3) 生成 AI への影響

【開発段階・利用段階の双方にまたがる論点】

生成 AI との関係では、まず開発段階において、**統計作成等特例に係る義務違反が課徴金対象に入っていること**の意味が極めて大きい。法案によれば、統計作成等のために新たに認められる取得・提供ルートは、利活用を可能にする一方で、そのルートを逸脱した場合には、単なる義務違反ではなく、**経済的不利益を伴う重大違反**として扱われる。したがって、生成 AI 開発事業者が、統計作成等特例に基づいて取得した個人情報や要配慮個人情報を、実際には**個人別の広告配信、営業ターゲティング、顧客企業向け配信サービス、統計化しないままの第三者販売**等に使えば、まさに特例違反として課徴金対象になり得る。

この点は、生成 AI の実務にとって特に重い。大規模言語モデルやマルチモーダルモデルの開発では、学習用に集めたデータが、その後、評価、ファインチューニング、モデル改善、広告最適化、営業支援、別サービス開発等に横展開されやすい。しかし、改正後は、**統計作成等特例で取得したデータは、その特例の範囲に厳格に結び付けて扱わなければならない**。したがって、生成 AI 事業者は、特例取得データについて、通常データとは別に、**アクセス権限、利用可能工程、再提供可否、学習後の利用範囲**を厳格に区分管理する必要がある。従来であれば「研究目的だから」「品質向上だから」と内部的に広く使っていた取扱いも、改正後は**課徴金リスクを伴う目的外利用**として再評価される。

また、開発段階では、取得経路に問題のあるデータを使ったモデル構築も、課徴金の文脈で重い意味を持つ。法案によれば、**法 20 条 1 項違反の不正取得・利用**も課徴金対象行為に含まれるため、取得手段に問題のあるデータを学習に使えば、刑事罰の問題にとどまらず、**経済的不利益の問題**にも発展し得る。したがって、生成 AI 事業者

は、学習データや評価データの取得経路、クローリング方法、ベンダーからの調達経路、契約上の取得権限等を、後から説明できる形で記録・審査しておく必要がある。

利用段階でも影響は大きい。API 提供型サービスや SaaS 型生成 AI において、**ユーザー入力、会話ログ、アップロード画像、フィードバックデータ**等を、別事業者、広告事業者、分析事業者、グループ会社、外部 AI ベンダー等に提供する場合、法的構成を誤れば、**法 27 条 1 項違反として課徴金対象**になり得る。また、委託と説明していた外部処理が、実質的には委託先の独自利用や共同利用に近い場合には、第三者提供又は範囲外利用の問題が生じ得る。生成 AI サービスは複数事業者が関与する構造をとりやすいため、**誰がどのデータを、どの法的立場で扱っているのか**を明確化しなければならない。

さらに、**第 148 条の本人保護命令**の強化も、生成 AI には重い意味を持つ。大規模な個人情報の不正利用、違法な学習データ利用、不適切な出力生成が発覚した場合、個人情報保護委員会は、単に「利用をやめよ」と命じるだけでなく、**影響を受けた本人への通知や事実の公表**まで命じ得る。生成 AI 事業では、データ処理が複雑で、本人にとって見えにくいことが多いからこそ、この通知・公表命令のインパクトは大きい。特に、長期ログ蓄積型サービスや学習済みモデルが絡む場合には、対象本人の範囲把握や通知方法自体が難しいため、**違反発覚後に対応を考えるのでは間に合わない**。事前に、対象特定、ログ遡及、連絡手段、公表文面まで含めたインシデント対応設計が必要になる。

とりわけ、生成 AI 事業は、モデル開発、API 提供、SaaS 課金、広告、データ分析、導入支援など、**データ利活用が直接収益に結び付く**構造を持つことが多い。そのため、利得剥奪型課徴金の影響は大きい。法案によれば、課徴金額は、対象行為又は対象行為をやめることの対価として得た財産上の利益相当額とされており、生成 AI 事業者にとっては、違反が単なるコンプライアンス問題ではなく、**売上・収益・事業価値に直接跳ね返る経営リスク**となる。特に統計作成等特例違反は、AI 利活用のために新たに開かれたルートを使うからこそ、その逸脱が重く評価されるという構造になっている。したがって、生成 AI 事業者に求められるのは、開発段階・利用段階の双方を通じて、**どの工程がどの法的根拠に基づき、どのデータがどの特例・同意・契約に基づいて使われ、どの統制が敷かれていたのかを後から説明できる体制**を整備することである。

要するに、命令・課徴金強化は、生成 AI との関係で、**①統計作成等特例を使う案件ほど、逸脱時の経済的不利益が重くなること、②学習データ取得・利用・第三者提供の各場面が課徴金対象行為に接続し得ること、③違反が発覚した場合には、本人通知・公表まで命じられ得ること**、そして、そのために**④法的根拠・契約・技術統制・運用記録を一体で管理する必要があること**を意味する。今回の改正により、生成 AI に

おける個人情報コンプライアンスは、もはや単なる法務問題ではなく、**収益構造そのものに関わる経営管理の問題**として扱うべき段階に入る。

12　不正取得罪（第 180 条）

(1) 現行法の規律

現行法には、**個人情報の不正取得そのもの**を、個人情報保護法上の一般的な犯罪類型として正面から処罰する規定は置かれていなかった。もちろん、現行法 20 条 1 項は、個人情報を**偽りその他不正の手段により取得してはならない**という不正取得禁止を定めていたが、これに違反した場合に直ちに対応する個人情報保護法固有の刑罰規定が明確に整備されていたわけではない。そのため、違法なクローリングやスクレイピング、なりすましによる取得、権限逸脱的な取得などについては、主として**民事上の違法性、契約違反、不正アクセス禁止法、業務妨害等**の文脈で整理されることが多く、個人情報保護法上の直接的な刑事罰との関係は、必ずしも明快ではなかった。制度改正方針も、現行法 20 条 1 項違反たる不正取得を、今回新たに強く問題化すべき違反類型の一つとして位置付けている。

また、現行法の下では、取得態様が悪質であっても、それが個人情報保護法上どこまで「違法取得」として摘発・制裁されるかが見えにくかった。たとえば、公開サイトからの大量取得であっても、アクセス制御を回避しているのか、利用規約に違反しているだけなのか、虚偽登録を伴うのか、認証情報の不正利用を伴うのかによって、適用し得る法規制が分散していた。その結果、個人情報の取得過程に問題がある場合でも、個人情報保護法上は主として行政上の不正取得禁止として処理され、**「不正に取ったこと自体」を個人情報保護法の刑罰で問う構造**は弱かったといえる。今回の制度改正方針が、規律遵守の実効性確保の一環として「詐欺行為等により個人情報を不正に取得する行為に対する罰則」を明記したのは、このギャップを埋める趣旨である。

要するに、現行法の下では、

① 不正取得禁止それ自体は存在した、

② しかし、不正取得を正面から処罰する個人情報保護法上の一般的犯罪類型は弱かった、

③ そのため、取得態様の悪質性は他法令や契約違反の問題として整理されがちだった、

というのが基本状況であった。今回の改正は、この点を大きく改めるものである。

(2) 改正法の内容

改正法案は、**第 180 条に不正取得罪を新設**する。制度改正方針は、これについて、**詐欺行為等により個人情報を不正に取得する行為に対する罰則を設ける**と明示してお

り、4 月 7 日の法案資料でも、罰則強化・不正取得対応は今回改正の重要な柱の一つとして位置付けられている。すなわち、改正法は、従来は主として行政法上・民事上・他法令上の問題として整理されていた不正取得を、**個人情報保護法固有の刑事規制**に接続する。

この不正取得罪のポイントは、単に「無断で取った」こと一般を処罰するのではなく、**取得態様の悪質性**に着目している点にある。ユーザーが引用している法案条文どおり、この罪は、自己若しくは第三者の不正な利益を図る目的、又は本人、個人情報を保有する者その他の者に損害を加える目的で、**人を欺き、人に暴行を加え、若しくは人を脅迫する行為により、又は個人情報を保有する者の管理を害する行為により**個人情報を取得した者を処罰対象とする構造である。したがって、ポイントは、取得の対象そのものというより、**どういう手段・目的で取得したのか**にある。制度改正方針が「詐欺行為等」と表現しているのも、この取得態様の悪質性を強調する趣旨である。

特に重要なのが、**「個人情報を保有する者の管理を害する行為」**という概念である。制度改正方針はこの文言自体を詳しく定義してはいないが、少なくとも、単なる閲覧や一般的収集ではなく、保有者が設けた管理の仕組み、アクセス管理、認証管理、利用条件、技術的制限等を害する形で取得する行為を、刑事罰の対象となり得る行為類型として取り込もうとしていると理解できる。ここにより、改正法は、取得手段の問題を、従来の「不正取得禁止」という抽象的行政規律から、**悪質な取得手段を伴う刑事罰規定**へと一段具体化している。

さらに、この改正は、今回全体の制度設計とも整合している。制度改正方針は、**不正取得（法 20 条 1 項違反）を課徴金対象行為の一つ**としても掲げている。つまり、改正法は、不正取得について、①行政法上の違反行為としての位置付け、②重大事案における課徴金対象行為としての位置付け、③そして悪質取得態様に対する刑事罰としての位置付け、を重ねて設計している。単に「不正取得はだめ」と言うだけではなく、**行政・経済的不利益・刑罰**の三層で対応しようとしている点が、今回改正の特徴である。

(3) 生成 AI への影響

【開発段階の論点】

生成 AI との関係では、この改正はとりわけ**学習データ収集段階**に強く響く。生成 AI 開発では、大量のウェブデータ、会話ログ、掲示板情報、画像、動画、メタデータ等を収集する実務が一般的であり、その取得手法の適法性が従来以上に厳しく問われることになる。制度改正方針が不正取得を主要な違反類型として位置付けた以上、生成 AI 開発事業者は、単に「データがネット上にあった」「技術的に取得可能だった」

というだけでは足りず、**どのような手段で取得したのか**を説明できなければならない。

具体的には、**アクセス制御の回避、認証の潜脱、利用規約で明示的に禁止されたスクレイピングの強行、技術的制限の回避、虚偽登録によるアクセス、権限外アカウントの利用、取得禁止設定を無視した大量取得**等は、「管理を害する行為」と評価されるリスクがある。特に、生成 AI の学習データ収集では、「公開ページの自動収集」と「管理を害する取得」との境界がしばしば問題になる。公開サイトであっても、robots.txt、ログイン制限、API 利用条件、レート制限、契約上の自動取得禁止等が設定されている場合、その潜脱態様によっては、不正取得罪との関係が一気に深刻化する可能性がある。したがって、クローリングやスクレイピングの適法性判断は、今後、単なる利用規約違反リスクの問題ではなく、**個人情報保護法上の刑事リスク**の問題にもなり得る。

また、生成 AI 開発では、外部ベンダーやデータブローカーから学習用データセットを購入・調達する場面も多い。しかし、改正後は、自社が直接スクレイピングしていなくても、**取得元がどのような態様でデータを集めたのか**が、法的リスク評価上より重要になる。なぜなら、不正取得に由来するデータを使ってモデルを構築すること自体が、制度改正方針上、課徴金対象行為としても問題化し得るからである。つまり、生成 AI 事業者は、自社の取得手法だけでなく、**データサプライチェーン全体の取得適法性**を点検する必要がある。データセット購入契約、ベンダー保証、監査権限、取得経路の説明資料などが、従来以上に重要になる。

さらに、評価用データ、教師データ、RLHF 用データ、検索拡張用データなど、学習以外のデータ収集にも同じ問題が及ぶ。たとえば、他社サービスの画面出力や会話ログを自動的に大量取得して評価データに使う、登録制コミュニティに虚偽登録して投稿データを取得する、アクセス制御された掲示板から人物情報を大量抽出する、といった行為は、単なる「研究用データ収集」では済まされず、不正取得罪との関係で見られる可能性がある。生成 AI 開発では、学習用データだけでなく、**評価・検証・安全性テスト用データの取得態様**についても、同水準の適法性審査が必要になる。

要するに、不正取得罪の新設は、生成 AI との関係で、

①**クローリング・スクレイピングの手法そのもの**が刑事リスクになり得る、

②**外部調達データの取得経路**も問われる、

③学習用データだけでなく**評価用・教師用・検証用データ**にも同様に及ぶ、

④したがって、生成 AI 開発事業者は、データ取得の適法性審査を、従来以上に厳格に行う必要がある、

という意味を持つ。今回の改正により、生成 AI 開発では「何を学習したか」だけでなく、**「どうやって集めたか」**が、これまで以上に重大な法的論点になる。

13　代表的な AI への影響

― ChatGPT、Claude、Gemini の規約・ポリシーとの関係

(1)総論

生成 AI の利用をめぐる法的検討においては、個人情報保護法等の法令上のルールだけでなく、各 AI サービス提供者が定める利用規約、利用ポリシー、データ利用ポリシーも確認する必要がある。実務上は、同じ「生成 AI の利用」であっても、個人向けサービスなのか、法人向けサービスなのか、API 利用なのかによって、入力データの取扱い、モデル改善への利用の有無、保持期間、抽出禁止、禁止用途などの前提が異なるからである。

OpenAI は、個人向けサービスに適用される **Terms of Use** と、企業・開発者向けの **Services Agreement** を区別している。Anthropic も、**Claude's Constitution** という内部原則のほか、**Consumer Terms**、**Commercial Terms**、**Usage Policy** を区別している。Google についても、**Gemini Apps の個人向けヘルプ**、**職場・学校アカウント向け説明**、**Google の生成 AI 禁止用途ポリシー**が分けて整理されている。

したがって、生成 AI の利用実務では、第一に日本法上適法か、第二に提供事業者の規約・ポリシー上許容されるか、第三に個人向け契約か法人向け契約か、という三つを切り分けて検討する必要がある。また、改正法案との関係では、これらの規約・ポリシーは、委託、第三者提供、安全管理措置、不正取得、相当の注意の有無といった論点の評価に密接に関係する。以下、代表的な AI サービスとして、ChatGPT、Claude、Gemini の順に整理する。

(2)ChatGPT（OpenAI）の規約・ポリシーとの関係

まず、OpenAI の個人向けサービスに適用される Terms of Use では、ChatGPT 等の個人向けサービスについて、自動的又はプログラム的にデータや Output を抽出することが禁止されている。また、Output を用いて OpenAI に競合するモデルを開発することも禁止されている。さらに、利用者は、入力に必要な権利、許諾、権限を有していなければならず、Output を人に関する重要判断にそのまま使ってはならないとされている。したがって、個人向け ChatGPT の画面や出力を大量取得して自社モデルの学習データや評価データに転用する行為は、少なくとも個人向け利用規約との関係で強い問題を生じ得る。これは、改正法案上の不正取得罪や、取得態様の適法性評価とも接点を持ち得る。

次に、会話データの取扱いである。OpenAI は、個人向けサービスについて、個人データやコンテンツをサービスの提供、維持、開発、改善、安全確保等に用いると説明している一方、個人向け ChatGPT では、設定によりモデル改善利用をオフにでき、Temporary Chat は履歴に残らず、メモリにも使われず、モデル学習にも使われないとしている。Temporary Chat FAQ では、ただし GPT のアクションにより第三者へ送信されたデータは、その第三者のポリシーに従うとも説明されている。他方で、企業・開発者向けサービスには別建ての Services Agreement が適用される。したがって、企業が ChatGPT を業務利用する場合には、個人向

けプランを使っているのか、法人向け・API 向け契約を使っているのかによって、入力データの取扱いに関する前提が異なる。日本法上の委託、第三者提供、安全管理措置との整合性を重視するのであれば、個人向けサービスの設定に依存するだけでなく、法人向け契約・管理機能を前提にした構成を検討すべきである。

改正法案との関係では、ChatGPT については、主として**利用段階**での入力データの取扱い、モデル改善利用の有無、抽出禁止、第三者提供・委託の整理が問題になる。また、個人向け ChatGPT の出力や会話ログを収集して自社 AI 開発に使う場合には、**開発段階**にも波及し、不正取得、契約違反、取得態様の不適法性評価の問題が生じ得る。したがって、ChatGPT との関係では、個人向け規約、学習利用設定、法人向け契約の三つを分けて整理する必要がある。

(3) Claude（Anthropic）の Constitution・規約との関係

Claude との関係では、まず Claude's Constitution がある。Anthropic は、これを Claude の訓練過程において重要な役割を果たす基礎文書であり、Claude の行動を直接形作るものとして説明している。また、Anthropic は、Claude のあるべき姿に関する最終的な権威としてこの Constitution を位置付け、しかも CC0（Creative Commons Zero）[16]で公開している。もっとも、Anthropic 自身も、Claude の実際の出力が常に Constitution どおりになるとは限らないと明示している。したがって、Claude の Constitution は、法令や契約条項のような外部的拘束力を持つルールというより、まずはモデル設計・訓練・運用の基準となる自主規律・内部規範として理解すべきである。

他方で、Claude の外部向けルールとしては、Consumer Terms、Commercial Terms、Usage Policy 等が存在する。Anthropic は、2025 年 8 月の更新で、個人向けの Consumer Terms と Privacy Policy を改定し、Claude Free、Pro、Max について、一定の条件の下でデータを Claude 改善や安全対策強化に使うかを利用者が選択できる仕組みを導入した一方で、Claude for Work、Claude for Government、Claude for Education、API 利用など、Commercial Terms が適用される領域にはその更新がそのまま及ばないことを明示している。また、Usage Policy は、Claude の外部利用ルールとして、特に近時はサイバー利用やエージェント利用に関する禁止行為を明確化している。たとえば、悪意ある侵害行為は禁止される一方、システム所有者の同意を得た脆弱性調査のような正当な利用は支持すると説明している。

改正法案との関係では、Claude については二層で考えるのが適切である。第一に、Constitution は、生成 AI 事業者の自主規律、安全設計、誠実性確保の例として、課徴金制度における「相当の注意」や、安全性、透明性の設計論と一定の接点を持ち得る。第二に、

---

[16] CC0（Creative Commons Zero）とは、著作権者が法令上可能な最大限の範囲で著作権その他の権利を放棄し、当該著作物をパブリックドメインに提供することを宣言するクリエイティブ・コモンズのツールであり、第三者は出典表示等の義務を負うことなく自由に複製・改変・再配布・商業利用することができる

Consumer Terms、Commercial Terms、Usage Policy は、Claude 利用者に対する外部的な契約ルールであり、個人向けか法人向けか、また禁止用途に当たらないかを確認する必要がある。したがって、Claude との関係では、**Constitution＝内部原則、規約・ポリシー＝外部ルール**という二層構造で理解するのが実務的である。これは主として**利用段階**の論点であるが、Claude の出力や挙動を利用して別モデルを開発するような場合には**開発段階**にも波及する。

(4) Gemini（Google）の規約・ポリシーとの関係

Gemini との関係では、まず Gemini Apps の個人向け利用と、Google Workspace 又は Google Cloud 上の法人向け利用を分ける必要がある。Google の Gemini Apps Privacy Hub によれば、個人向け Gemini Apps では、Gemini Apps Activity がオンのとき、チャット内容や関連データが Google アカウントに保存され、Google AI の改善のために利用され得る。また、Temporary chats は AI モデルの学習には使われず、Gemini Apps Activity をオフにし、かつフィードバックを送らない場合には、将来のチャットを AI モデル改善に使わないとされている。さらに、Google は、個人向け Gemini Apps について、人間のレビュー担当者が会話を確認し、サービス改善に使う場合があることも説明している[17]。

これに対し、職場又は学校アカウントで Gemini Apps を使う場合について、Google は、データ取扱いが Workspace ライセンスにより異なるとしつつ、**enterprise-grade data protections** がある場合には、チャットやアップロードファイルが人間のレビュー担当者に見られず、生成 AI モデル改善にも使われない旨を案内している。Google Workspace 関連の FAQ でも、Education 向け等を含め、対象の仕事・学校アカウントでのチャットやアップロードファイルは、人間のレビューや生成 AI モデル改善に使われないと説明されている。また、Google Workspace with Gemini の案内では、Workspace 上の組織データは顧客のデータであり、Gemini モデルの訓練・改善や広告ターゲティングには使われないとしている。したがって、Gemini についても、個人向け Apps、Workspace 向け Gemini、Google Cloud 上の Gemini 系利用とで、入力データの取扱いに関する前提が異なる。

また、Google には Generative AI Prohibited Use Policy があり、違法、有害、詐欺的、誤認的、権利侵害的な利用等を禁止している。Google Terms も、サービス固有ポリシーとしてこの禁止用途ポリシーに従うべきことを示しており、Google Cloud のサービス固有条項でも生成 AI サービスについてこのポリシーを取り込んでいる。これは、日本法上の不適正利用、不正取得、権利利益侵害の防止と方向性が一致する。したがって、Gemini 利用者にとっても、日本法上適法かに加えて、Google の生成 AI 利用ポリシー上許容されるかを確認する必要がある。

---

[17] Google ヘルプ
（https://support.google.com/gemini/answer/13594961?hl=en&utm_source=chatgpt.com）

改正法案との関係では、Gemini は主として**利用段階**での入力データの取扱い、保持、モデル改善利用の有無、職場・学校アカウントとの区別、禁止用途の確認が重要になる。他方で、Gemini Apps の出力や会話を使って自社モデルの教師データや評価データを作る場合や、Vertex AI や Gemini 環境を組み込んで独自開発を行う場合には、**開発段階**にも波及する。そのため、Gemini との関係でも、個人向け Apps、Workspace 向け Gemini、Google Cloud 上の利用を切り分けて評価することが必要である。

(5) 小括

以上をまとめると、代表的な AI サービスについては、次のように整理できる。

まず、**ChatGPT** は、**個人向け Terms of Use** で自動抽出や競合モデル開発を禁止し、個人向けサービスでは会話のモデル改善利用について設定変更によるオプトアウトを認める一方、**法人向け・API 向け**には別建ての **Services Agreement** がある。したがって、個人向けか法人向けかの切分けが極めて重要である。

次に、**Claude** は、内部原則としての **Constitution** と、外部ルールとしての **Consumer Terms**、**Commercial Terms**、**Usage Policy** が並立している。したがって、Claude については、**内部規範**と**外部契約ルール**を分けて理解するのが適切である。

さらに、**Gemini** は、個人向け Apps、Workspace 向け Gemini、Google Cloud 上の利用でデータ取扱いの前提が異なり、個人向けでは Activity や Temporary chats の設定が重要である一方、職場・学校アカウントでは改善利用に使われない保護が明示される場合がある。したがって、Gemini も、利用形態別の切分けが不可欠である。

日本法上の個人情報保護実務との関係でいえば、代表的な AI サービスについて共通して重要なのは、

① どの契約体系が適用されるか、
② 入力データや会話がモデル改善に使われるか、
③ 自動抽出や禁止用途に当たらないか、
④ 法人向け契約・管理機能があるか、

を確認することである。今回の改正法案の下では、これらの規約・ポリシー確認は、委託、第三者提供、安全管理措置、不正取得の法的評価と切り離せない。したがって、代表的な AI サービスを使う企業にとっては、**法令適合性とサービス規約適合性を一体として設計・運用すること**が必要になる。

おわりに

今回の改正法案が生成 AI に及ぼす影響は、統計作成等の特例を中心にしつつも、それにとどまらない。統計作成等は生成 AI に新たな法定利活用ルートを与えるが、同時に、委託先の二次利用規制、連絡可能個人関連情報の利用規制、特定生体個人情報の専用規律、

16 歳未満保護、不正取得罪、命令・課徴金・罰則が重なることにより、生成 AI 事業者には従来以上に精緻なデータガバナンスと内部統制が求められる。

開発段階と利用段階の双方にわたり、どの工程がどの法的根拠に基づき、どの統制の下で行われているのかを一貫して設計・運用・説明できる体制の構築が、今後の生成 AI 事業の前提条件となる。さらに、ChatGPT、Claude、Gemini といった代表的な AI サービスを利用する場合には、それぞれの規約・ポリシーが、日本法上の委託、第三者提供、安全管理措置、不正取得の評価と切り離せない。したがって、生成 AI 事業者・利用企業に求められるのは、**法令適合性、技術設計、サービス規約適合性を三位一体で管理すること**である。

以　上