個人情報保護法等改正法案と生成AIを徹底解説

～ 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 ～

弁護士法人 三宅法律事務所
弁護士　渡邉　雅之
同　　越田　晃基
同　　岩田　憲二郎
同　　出沼　成真

ご相談は以下にご連絡ください
03-5288-1021（代表）
m-watanabe@miyake.gr.jp
k-koshida@miyake.gr.jp
k-iwata@miyake.gr.jp
n-idenuma@miyake.gr.jp

総論 — 改正法案と生成AIの関係

参考URL

- 「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」の閣議決定について（令和８年４月７日）（https://www.ppc.go.jp/news/press/2026/260407/）
- 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）
- 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）

改正法案は生成AIをどう規律するか

- 2026年4月7日閣議決定法案は、生成AIを名指しで規律するものではない
- しかし、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・営業活用に広く影響する
- 中心は**「統計作成等」**の新特例だが、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・罰則まで及ぶ

ポイント
生成AIは名指しされていないが、改正法案は広い範囲で生成AIに影響する

開発段階と利用段階という分析軸

- 生成AI事業は**「開発段階」**と**「利用段階」**に大きく分かれる
- 「開発段階」は、学習データ収集、モデル構築、ファインチューニング、評価の工程
- 「利用段階」は、API提供、SaaS運用、出力制御、ユーザー対応の工程
- 改正法案の各条文がどちらの段階に関連するかは、論点ごとに異なる
- 本資料では、各論点が主として開発段階か、利用段階か、両段階にまたがるかを明示する

ポイント
生成AIへの影響は、開発段階と利用段階に分けて検討する必要がある

本資料で扱う論点の全体像

- 統計作成等（2条13項）と、その取得特例・公表義務・目的外利用禁止・第三者提供ルート
- 委託を受けた事業者の規律（30条の3、58条の2）
- 連絡可能個人関連情報（2条8項、31条の2）
- 特定生体個人情報（16条5項、21条の2、27条2項、35条7項・8項）
- 本人同意例外（18条3項、20条2項、27条1項）
- 16歳未満の者の保護（35条9項・10項、40条の2、58条の3）
- 命令・課徴金（148条、148条の3以下）、不正取得罪（180条）
- ChatGPT、Claude、Geminiの規約・ポリシーとの関係

ポイント
統計作成等を中心としつつ、複数の規律が生成AIに重層的にかかる

改正の基本思想と生成AIへの含意

- 利活用ルートの整備により、使えるデータは使えるようにする方向
- 停止請求・命令・課徴金・罰則の強化により、逸脱や悪質利用には重い責任を課す
- 利活用の特例設置と、透明性・用途限定・本人関与・制裁強化を同時に進める
- 単純な規制緩和でも単純な規制強化でもなく、両方向の見直しを組み合わせた改正
- 生成AIにとっては、入口が開く一方で出口の管理責任が重くなる構造

ポイント
利活用拡大と規律強化はセットであり、生成AI事業はその両面を同時に設計する必要がある

統計作成等（2条13項）の定義

統計作成等とは ― 現行法の状況

- 現行法でも、個人に戻らない一般的・集計的な統計情報の作成自体は、中心規制の外側で整理されやすかった
- 個人情報保護法は、特定個人を識別できる情報等を「個人情報」とし、「個人情報」概念を中核として利用目的特定・目的外利用制限・第三者提供規制等を課す
- 他方、特定個人との対応関係が排斥された統計・集計結果は、通常、直接の規律対象とはならないと理解されてきた
- しかし、どこまでが「個人に戻らない分析」かは条文上明示されていなかった

ポイント
現行法では、統計的処理の外延が条文上明確でなかった

現行法における生成AI学習の不透明さ

- 大規模言語モデルの事前学習が現行法上の利用目的規制の対象であるかは明確でなかった
- 学習済みモデルが「個人データの保有」に当たるかも明確でなかった
- 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示されている

ポイント
AI学習のような大量データ解析の法的位置付けが不明確なまま事業が進められていた

統計作成等の定義（2条13項）

- 統計作成等（2条13項）は、**大量の情報から要素情報を抽出し、分類・比較その他の解析を行う行為**
- その結果として、**大量情報の傾向又は性質に係る情報を作成するもの**をいう
- 「個人に関する情報であるもの」は、作成対象から除かれる
- **「個人の権利利益を害するおそれが少ないもの」**として、委員会規則で定めるものに限られる
- 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推進の中核概念として法定化された

ポイント

統計作成等は、大量データから個人に戻らない傾向・性質を取り出す低リスクの分析に限定された概念

統計作成等の定義の4つのポイント

1. 「大量の情報」を対象とする行為であり、少数の個人を個別評価する行為は入りにくい
2. 要素情報の抽出・解析を通じて、元データではなく傾向又は性質に係る情報を作成する行為
3. 作成される情報から「個人に関する情報であるもの」は除かれ、個人別スコアや個人再接続結果は外れ得る
4. 「権利利益を害するおそれが少ないもの」に限られ、具体的範囲は委員会規則に委任される

ポイント

「大量データ分析」一般が自由化されるのではなく、低リスク類型に限定される

統計作成等の構造的特徴

- 従来、実務で暗黙に「統計処理だから比較的自由」と整理されていた領域を放置しない構造になる
- 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
- 入口の特例と出口の拘束を一体で設計している点が今回改正の特徴
- 「統計だからフリー」という従来感覚は、法定概念の中で条件と責任が明確化される方向に変わる

ポイント

統計作成等は、利活用ルートであると同時に、責任を伴う法定の枠組み

統計作成等の生成AIへの影響（事前学習）

【主として開発段階。利用段階にも波及】

- 最大の論点は、自社学習パイプラインのどこ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かの線引き
- 事前学習（プレトレーニング）は、数兆トークン規模から言語の一般的パターン・世界知識を学習する工程
- 特定個人に関する情報を作成するものではないため、統計作成等に整理される可能性が高い
- もっとも、事前学習後の工程は個別の検討が必要

ポイント

事前学習は統計作成等に整理され得るが、それ以降の工程は別途検証が必要

統計作成等の生成AIへの影響（学習後工程）

【主として開発段階。利用段階にも波及】

- 「ファインチューニング」のうち一般知識付加は含まれ得るが、個人の嗜好・行動履歴に基づくカスタマイズは個人情報作成に転じ得る
- 「RLHF」も、匿名化された一般的品質評価なら含まれ得るが、特定個人の選好学習は範囲外となり得る
- 「RAG」や「プロンプト内個人情報の処理」は、統計作成等とは別の法的根拠で整理する必要がある
- 生成AI事業者は、モデル開発工程を技術的に分節し、各工程の該当性を個別に検証する体制が必要

ポイント

「AI開発だから統計作成等」という一括整理は危険であり、工程ごとの法的分析が不可欠

【用語解説】ファインチューニング・RLHF・RAG

「ファインチューニング」（ fine-tuning）

- 事前学習済みモデルに特定の業務・分野・用途の追加データを学習させ、出力の精度や適合性を高める手法。
- 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、その領域に即した応答をしやすくする。

「RLHF」（Reinforcement Learning from Human Feedback：人間のフィードバックによる強化学習）

- AIの出力に対し人間が望ましさ・有用性・安全性等の観点から評価し、そのフィードバックを用いて応答を改善する学習手法
- 人間の意図や社会的に望ましい基準に出力を近づけるために用いられる

「RAG」（Retrieval-Augmented Generation）

- 回答生成時に事前学習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、その結果を参照して回答を生成する仕組み
- 最新情報や個別資料に基づく回答を可能にし、誤回答の抑制に用いられる

ポイント

ファインチューニング・RLHF・RAGは、いずれも統計作成等への該当性が工程ごとに分かれる点で重要

統計作成等の規律①
公開要配慮個人情報の取得特例（30条の2第1項）

公開要配慮個人情報の取得 ― 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である（20条2項）
  ⇒情報がインターネット上に公開されている場合でも原則として適用される
- 大規模学習データ収集との間に深刻な緊張があり、数十億ページのクローリングで個別同意取得は物理的に不可能
- 闘病記録、宗教的信条、犯罪歴情報、障害に関する情報等が不可避的に混入する
- これら要配慮個人情報が本人その他正当な者による公開（現行法20条2項7号参照）であるかを判別することは困難

ポイント
現行法の本人同意原則と、生成AIの大規模学習との間に構造的緊張があった

令和5年6月のOpenAIへの注意喚起

- 個人情報保護委員会は、令和5年6月、OpenAIに対し法第147条に基づく注意喚起を行った
- 本人同意なく要配慮個人情報を取得しないこと（法定例外を除く）を求めた
- 混入回避の取組、収集後の即時減少措置、発覚時の削除・非識別化措置を遵守事項として示した
- 本人や委員会等から特定のサイト等からの収集停止の要請・指示があった場合、拒否する正当な理由がない限り従うことも求めた
- これは現行法20条2項を前提としつつ、解釈・運用の枠内の対応を目指すものであった（実際には超法規的措置の色彩もあった。）

ポイント

注意喚起は、一応、現行法の枠内の行為規範とされたが、取得そのものの法的不透明さは残されていた

取得特例の改正内容（30条の2第1項）

- 改正法案は、現に公開されている要配慮個人情報を、本人同意なく取得できる特例を新設する取得が認められる目的は、①統計作成等目的、②第三者提供目的である
- 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の公表が要件となる
- 特例成立には、目的限定＋現に公開＋事業者名等の公表という三要素が必要
- 要配慮個人情報の保護の重み自体を弱めるのではなく、限定された例外ルートを新設するものである

ポイント
公開要配慮個人情報の取得は、公開情報＋低リスク目的＋透明性確保で初めて成り立つ

取得特例の生成AIへの影響（基盤の安定）【開発段階の論点】

- 事前学習のコーパス（自然言語（人間の言葉）の文章や会話のデータを大量に収集し、コンピュータで検索や分析ができるように整理した「言語データのデータベース」）に要配慮個人情報が含まれても、**統計作成等目的**かつ公表を行えば本人同意なく取得できる
- 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
- これは生成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
- 他方で、いくつかの実務上の課題が残る

ポイント

取得特例は生成AI開発の法的基盤を安定させるが、運用課題は残る

取得特例の生成AIへの影響（残る実務課題）【開発段階の論点】

- 公表義務の具体的実装が論点であり、記載粒度が事業機密性との間で緊張を生む
- 特例の適用に際しても、注意喚起のあった不適切なウェブサイトからの情報収集停止要請は尊重されるべき行為規範
- 海外サーバ上のデータへの適用や外国法制との整合性は、別途検討が必要な論点である

ポイント

取得は容易になるが、公表設計・不適切なウェブサイトからの収集遮断、国際整合は引き続き重い課題

統計作成等の規律②
継続公表義務（30条の2第2項・第3項）

継続公表義務 — 現行法の状況

- 現行法では、利用目的の公表は取得時等に行えばよく、継続的公表が明確な義務とはされていなかった
- プライバシーポリシーを一度掲載すれば、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・目的・用途が開発過程で変化することが多い
- 事前学習からファインチューニング、外部提供・API公開へと用途が拡大しても、十分な透明性メカニズムがなかった

ポイント
現行法は、生成AI開発の用途変化に対応した継続的透明性を提供していなかった

継続公表義務の改正内容

- 改正法案では、取扱期間中、事業者名・統計作成等の内容等を継続して公表しなければならない
- 公表事項の変更時は、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
- 公表の「継続」とは、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
- 変更時事前公表の例外範囲や軽微変更の扱いは、委員会規則に委ねられている

ポイント

透明性は一回的ではなく、取扱期間全体を通じて継続的に求められる

継続公表義務の生成AIへの影響（運用体制）

【開発段階・利用段階の双方にまたがる論点】

- 開発サイクルが高速なため、学習データ追加・モデル更新・用途変更のたびに事前公表の要否確認が必要になる
- 開発・法務・広報部門の間で、変更の有無と公表要否を継続確認するプロセスが必要となる
- 公表の粒度（抽象度）を、事業機密性と透明性のバランスで設計する必要がある
- 記載の具体性については、今後の委員会ガイドラインやFAQの整備を待つ必要がある

ポイント

継続公表義務は、データガバナンスの運用体制そのものに大きく影響する

継続公表義務の生成AIへの影響（学習完了後）

【開発段階・利用段階の双方にまたがる論点】

- 学習完了後も学習データを保持・管理する限り「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、公表維持が必要となり得る
- オープンソースモデルの公開時、利用者による再利用・再配布と元の公表義務の関連が新たな論点となる
- 公表義務の継続期間の管理は、実務上重要な設計事項となる

ポイント

公表義務は学習完了後も継続し得るため、終期管理を含めた設計が必要となる

統計作成等の規律③
目的外利用禁止・第三者提供制限
（30条の2第4項以下）

目的外利用禁止 — 現行法の状況

- 現行法でも個人情報の利用目的の制限（法第18条）は存在し、必要な範囲を超えた取扱いは禁じられている
- 他方、利用目的の変更は「関連性を有すると合理的に認められる範囲」で許容され（法第17条第2項）、判断に幅があった
- 生成AIでは、事前学習用データが評価・ベンチマーク・営業デモ・顧客カスタマイズ等に横展開されやすい
- こうした二次利用が現行法上どこまで許されるかは必ずしも明確でなく、整理が分かれやすかった

ポイント

現行法には、特例取得データを特例の範囲に厳格拘束する専用の出口規制がなかった

目的外利用禁止・第三者提供制限の改正内容

- 統計作成等用要配慮個人情報等は、公表した内容を実現するため必要な範囲を超えて取り扱ってはならない（第30条の２第４項）
- 通常の利用目的制限と異なり、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もの
- 第三者提供も原則禁止され、提供先にも継続公表義務・変更公表義務が連鎖する（第30条の2第6項・第7項・第8項）
- 個人関連情報ベースの特例提供にも、同様の継続公表・変更公表の仕組みが設けられる（第31条の３）
- これらの特例違反は課徴金制度（148条の3以下）と密接に結び付いている（第30条の2第4項以下・第148条の3以下）

ポイント

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」強い拘束を課す

目的外利用禁止の生成AIへの影響（データ管理）

【開発段階・利用段階の双方にまたがる論点】

- 事前学習用に収集した特例データを、ファインチューニング、個人向けカスタマイズ、ターゲティング広告、採用・与信モデルに転用すると目的外利用となり得る
- 個人別の推論・選別・配信最適化は「傾向又は性質に係る情報」の枠を外れやすく、特例の趣旨と最も衝突しやすい
- どのデータセットが特例取得データか、どの工程まで利用可能かを通常データと別建てで管理する必要がある
- 研究・製品・営業・マーケティング部門間の社内横展開も、公表内容を超えれば目的外利用となり得る

ポイント

特例取得データを「後で何にでも使えるデータ」にしない厳密な分別管理が求められる

目的外利用禁止の生成AIへの影響（社内統制と課徴金）

【開発段階・利用段階の双方にまたがる論点】

- 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、承認フロー等の社内統制が適法性の中核となる
- 特例違反の目的外利用・第三者提供は、利得剥奪型課徴金に直結し得る
- 生成AI事業はデータ利活用が収益に直結しやすく、違法な横展開は事業収益に跳ね返る
- 経営リスクとなる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となる

ポイント

社内統制と課徴金リスクの直結により、目的外利用防止は経営課題となる

目的外利用禁止の生成AIへの影響（世代交代と提供後）

【開発段階・利用段階の双方にまたがる論点】

- 第一世代の特例取得データを次世代モデルにも用いる場合、同一の統計作成等の範囲内かが論点となる
- モデルの目的・機能・対象市場・出力の性質が大きく変われば、新たな公表や別の法的根拠が必要となり得る
- モデルのバージョンアップを、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
- 提供先との契約・継続公表確認・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する必要がある

ポイント

モデル更新・再利用・提供のたびに、法的根拠を再点検する必要がある

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

第三者提供ルート ― 現行法の状況

- 現行法では、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（法27条1項）
- 第三者が統計的・分析的処理のために個人データを受け取ることを本人同意なく広く許容する一般ルートはない
- 匿名加工情報への加工はコストと情報量の損失を伴い、大量データの個別同意取得も実務上困難
- 「本人同意」も「匿名加工情報」も使いにくいが、一定の透明性・拘束の下で第三者に渡したいニーズの受け皿が不足している

ポイント
目的外利用禁止（第30条の2第4項）が「出口規制」であるのに対し、第三者提供ルート（第30条の2第5項以下）は「提供ルートの新設」という別の機能を持つ

第三者提供ルートの改正内容（要件）

- 第三者が個人情報を統計作成等目的でのみ取り扱う場合に、本人同意なく提供できる新ルートを設ける（第30条の2第5項、第18条・第27条第1項の適用除外）
- 要件①は、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である（第30条の2第5項）
- 要件②は、提供元・提供先双方が、双方の氏名等・統計作成等の内容等を公表していることである（第30条の2第5項）
- 要件③は、提供元と提供先の書面又は電磁的記録による合意で特例に基づく旨が明確に定められていることである（第30条の2第5項）
- 単に内部理解では足りず、公表＋契約明記が法定要件として置かれている（第30条の2第5項、個人関連情報につき第31条の3）

ポイント

統計作成等目的の第三者提供は、公表＋契約明記を法定要件とする（第30条の2第5項・第31条の3）

第三者提供ルートの改正内容（提供後の拘束）

- 提供を受けた個人情報取扱事業者は「特例個人情報受領者」として継続公表義務を負う（第6項）
- 公表事項の変更は、原則事前公表、例外的に事後速やかな公表が求められる（第7項・第8項）
- 提供統計作成等用個人情報等は、公表された統計作成等に必要な範囲を超えて取り扱ってはならない（第9項）
- 統計作成等用要配慮個人情報等・提供統計作成等用個人情報等は、原則として再提供が禁止される（第10項）
- 第31条の3は、個人関連情報についても同様の統計作成等目的提供ルートを設ける（第31条の3）

ポイント

自由なデータ流通市場ではなく、提供先を特定した高透明・高拘束型の連携ルートである（第30条の2第6項～第10項・第31条の3）

第三者提供ルートの生成AIへの影響（提供類型）

【主として開発段階。利用段階にも波及】

- 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新たな法的ルートを提供する（第30条の2第5項）
- AI開発受託では「委託なのか特例提供なのか」をより意識的に設計する必要がある（委託は第30条の3、特例提供は第30条の2第5項）
- 医療・創薬等の業界横断的データ連携に、匿名加工・個別同意以外の第三の選択肢が与えられる（第30条の2第5項）
- グループ企業間連携も、双方公表・契約明記・継続公表・目的外利用禁止が課され、緩くはならない（第30条の2第5項・第6項・第9項）
- Cookie・行動ログ等の個人関連情報ベースの開発・分析にも、第31条の3の適用可能性がある（第31条の3）

ポイント

統計作成等目的の第三者提供ルート（第30条の2第5項以下）で適法に渡し、目的外利用禁止（第30条の2第4項以下）でその後の利用を厳格に縛るという関係に立つ

第三者提供ルートの生成AIへの影響（限界）

【主として開発段階。利用段階にも波及】

- 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
- 提供を受けたデータの別案件流用・別顧客向け転用・再度の外部提供は原則として許されない
- 学習済みモデルの第三者ライセンスは自動的に自由とはいえず、データ残存性・復元可能性の分析が必要である
- 委託契約・データ提供契約では、利用可能工程、評価利用可否、モデル提供先制限、契約終了時削除等を精緻化する必要がある

ポイント

統計作成等目的の第三者提供ルート（第30条の2第5項以下）で適法に渡し、目的外利用禁止（第30条の2第4項以下）でその後の利用を厳格に縛るという関係に立つ

委託を受けた事業者の規律
（30条の3、58条の2）

委託先規律 — 現行法の構造

- 現行法でも委託先は委託元と一体として扱われ、委託業務の範囲外利用は許されないと考えられてきた
- ただし、その構造は主として委託元の監督義務（25条）を通じて間接的に実現されていた
- 委託先自身に対する「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は、法文上正面から置かれていなかった
- 範囲外利用は、条文構造上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

ポイント
現行法は委託元の監督義務が中核で、委託先の直接義務が不明確であった

委託先規律 — 現行法の限界

- 印字・封入・発送等の機械的・受動的処理では、委託先の裁量は小さく支障は生じにくかった
- クラウド、SaaS、BPO、AI開発受託、ログ解析等では、委託先が裁量をもって取扱方法を決める場面が増えた
- 「単なる委託先か、独立したデータ取扱主体か」「サービス改善利用は委託の範囲内か」が曖昧になりやすかった
- いわゆる「クラウド例外」も、保守・障害対応・学習利用・品質向上利用等が問題となり、前提維持が論点であった

ポイント
クラウド・SaaS・AI受託のような新しい処理形態で、委託の範囲が見えにくかった

委託先規律の改正内容（直接義務）

- 第30条の3を新設し、委託先自身に、委託業務遂行に必要な範囲を超えて取り扱ってはならない直接義務を課す
- 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、委託先固有の法的義務として法文化した
- 委託先は単なる補助者ではなく、自ら違法な取扱いを行い得る主体として捉え直されている
- 受託データを自社分析・品質向上・別サービス開発・汎用AI学習に転用する行為は、契約・実態上明確でない限り問題化しやすい

ポイント

「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」へ整理が改められた

委託先規律の改正内容（適用調整）

- 第58条の2を新設し、機械的・受動的受託処理には本法の一部規定を適用しない仕組みを設ける
- 適用調整の要件は、①委託契約で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いること、②取扱いが委託業務遂行に必要な範囲内であること、③実際の運用が契約どおりであること
- 詳細指示に従ったデータ入力・印字・発送・スキャン・形式変換等、受託者が自ら処理内容を決めない処理が想定される
- 単なる秘密保持条項や一般的善管注意義務条項では足りず、事故報告・取扱状況把握・権限管理・再委託条件等を含む具体的な契約設計が求められる
- 独自判断を伴う委託先には第30条の3の直接義務、機械的受託者には第58条の2の限定的適用調整という二段構造である

ポイント
誰がどこまで取扱方法を決めているかに応じて規律を組み分ける方向へ進んだ

委託先規律の生成AIへの影響（開発段階）

【開発段階・利用段階の双方にまたがる論点】

- 生成AIは「受託」「API」「SaaS」の形をとりつつ、ログ保持・モデル改善・品質評価等で広くデータにアクセスし得る
- AI開発受託で、顧客提供データを自社の汎用基盤モデル学習や他案件向け改善に流用する行為が範囲外利用の典型となる
- 「品質向上のため」「サービス改善のため」という説明だけでは足りず、委託業務遂行に必要な範囲かが問われる
- 受託データを汎用学習に使うなら、委託という整理では不十分で、別の法的構成・契約・同意・提供ルートの検討が必要となる

ポイント

受託データの汎用学習・別案件流用は、委託の整理だけでは正当化できない

【補足】いわゆる「クラウド例外」とは

- クラウド例外とは、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の整理
- この場合、第三者提供にも委託にも当たらないとする整理が、個人情報保護委員会のQ&A（Q7-53）で認められてきたもの
- 前提は、外部事業者が当該個人データを「取り扱わない」状態が契約とアクセス制御により確保されていること（取り扱わない場合の安全管理措置の考え方はQ7-54）
- 2024年3月には、現実に個人データを取り扱うクラウド事業者には規律が及ぶ旨の注意喚起が個人情報保護委員会からなされた
- 改正後もクラウド例外自体が消えるわけではないが、「取り扱わない」前提が維持できるかがより厳密に問われる

ポイント

クラウド例外は個人情報保護委員会のQ&A（Q7-53・Q7-54）で認められた整理であり、「クラウドだから当然に例外」ではなく取り扱わない実態が確保されているかが問われる

委託先規律の生成AIへの影響（利用段階・クラウド例外）

【開発段階・利用段階の双方にまたがる論点】

- API・SaaS型生成AIで入力・会話ログをモデル改善等に使う実務が、当然に受託処理の範囲に入るとは言いにくくなる
- ログ分析・入力学習には独自判断が介在するため、機械的受託処理の適用調整に乗りにくい可能性が高い
- 生成AIは従来型クラウドより厳しく見られやすく、クラウド例外への安易な依存は維持しにくい
- 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い

ポイント

受託処理と自社利用の境界を、契約・技術・運用の三面から可視化する必要がある

連絡可能個人関連情報
（2条8項、31条の2）

連絡可能個人関連情報 — 現行法の状況

- 「個人関連情報」とは、生存する個人に関する情報であって、個人情報・仮名加工情報・匿名加工情報のいずれにも該当しないもの（第2条第7項）
- 令和2年改正で個人関連情報の第三者提供規律（第31条）が導入され、2022年4月に施行
- 第31条は主として「提供先で個人データとして取得されることが想定される場合」を捉える規律
- 特定個人に連絡・接触・到達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ではない
- 電話番号・メールアドレス等が直ちに個人情報に当たらないと整理されると「比較的自由」と理解されやすい

ポイント

現行法は、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ていなかった

連絡可能個人関連情報の改正内容

- 「連絡可能個人関連情報」とは、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個人関連情報をいう（新設：改正法案第2条第8項）
- 対象となる記述等は、①住居・勤務先その他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等を識別する符号、⑤その他委員会規則で定めるもの
- これらが直接含まれていなくても、他の情報と容易に照合してこれらの記述等を特定できるものも対象に含まれる
- 第31条の2で、違法・不当な行為を助長・誘発するおそれがある方法による利用を禁止し、さらに偽りその他不正の手段による取得も禁止する
- (i)個人関連情報に関する新類型の法定（第2条第8項）、(ii)不適正利用禁止、(iii)不正取得禁止（いずれも第31条の2）という三段構えを採る

ポイント

「個人に到達し、接触し、働きかけることができるか」に着目した新たな保護類型である

連絡可能個人関連情報の生成AIへの影響（利用段階）

【主として利用段階。開発段階にも波及】

- 生成AIによる営業リスト補強、自動営業文面生成、送客DB分析、勧誘スクリプト生成等が直接問題となる
- 連絡先情報を含む出力生成（見込み顧客リスト作成等）も、利用態様によっては不適正利用を助長し得る
- 「断りにくい相手」「心理的に脆弱な相手」への最適化された接触戦略は、不適正利用と評価され得る
- 生成AIの導入で営業・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認識する必要がある
- 出力段階のフィルタリング、危険用途検知、利用規約上の禁止、監査ログ保存が重要となる

ポイント

営業・広告精度の向上と法的リスクの上昇が比例する関係を直視する必要がある

連絡可能個人関連情報の生成AIへの影響（開発段階）

【主として利用段階。開発段階にも波及】

- ウェブクローリングで学習データに電話番号・メールアドレス・所在地等が大量に混入し得る
- 公開情報からの取得であっても、アクセス制御の潜脱・利用規約違反の自動取得・なりすまし登録等の取得態様は「偽りその他不正の手段」に当たり得る（第31条の2）
- 営業特化型・採用候補者接触支援型・送客支援型モデルでは、訓練の結果として連絡先がそのまま再出力されたり、接触行動を最適化する方向に学習されたりするリスクがある
- そのため、連絡可能個人関連情報を含むデータには、学習対象からの除外・マスキング・出力フィルタリング等の統制を講じることが望ましい
- 取得段階・学習段階・出力段階を通じた一貫した設計が必要となり、利用規約や安全性評価との整合も求められる

ポイント

連絡可能個人関連情報は、学習データに紛れ込みやすく出力にも影響するため、取得・学習・出力の各段階で一貫した統制が必要である

特定生体個人情報
（16条5項、21条の2、27条2項、35条7項・8項）

特定生体個人情報 — 現行法の状況

- 現行法には「特定生体個人情報」の類型はなく、生体情報は一般的な個人情報規律の適用にとどまっていた
- 顔特徴データのテンプレートの扱いが実務上分かりにくく、専用の保護ルールがなかった
- オプトアウト第三者提供から特定の生体情報類型を名指しで除外する仕組みもなかった
- 利用停止等請求権も一般の保有個人データの枠組みで処理されるにすぎなかった

ポイント

一般規律だけでは、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不十分であった

特定生体個人情報の新設（改正案16条5項）

【定義の二段階構造】
①「特定生体個人識別符号」を定義し、②それを含む個人情報を「特定生体個人情報」とする。要配慮個人情報とは別個の新たな高リスク類型
【識別符号の二要件（AND条件）】
(ア)取得容易性　特別の技術・多額の費用を要しない方法で取得できる身体特徴を変換した符号であること。
(イ)被認識困難性　取得されていることを本人が容易に認識できないものとして政令で定めるもの。
【意義・想定対象】
両要件の掛け合わせにより、本人の関与・認識を経ず第三者が一方的に収集できる類型に限定。指紋・静脈等は本人の接触・協力を要するため射程外。主として顔特徴データ（防犯・街頭カメラによる特徴量抽出）を想定。生体情報一般の一律規制ではなく、リスク類型を狙い撃ちする立法技術。

ポイント
特定生体個人情報＝「容易に取得でき、本人が取得に気づきにくい」生体識別情報（主に顔特徴データ）を狙い撃ちした高リスク類型

特定生体個人情報の改正内容（三つの特則）

特定生体個人情報には、①取得時の透明性、②流通の制限、③本人による離脱可能性という三方向から規律がかかる。本人が気づかないうちに取得され得る類型であることに対応した、重層的な手当てである。

【① 周知義務（21条の2）— 取得時の透明性】

- 取扱いの事実・利用目的・身体特徴情報の内容等を、本人に分かる形で示させる。本人が「自分の生体情報が取り扱われている」と認識できる契機を制度的に確保する趣旨。被認識困難性という類型の弱点を、事業者側の能動的な周知で補う。

【② オプトアウト第三者提供の禁止（27条2項）— 流通の制限】

- オプトアウト方式（本人の求めがあれば停止するが、原則は通知・公表のみで提供可）による第三者提供を認めない。本人関与の弱いまま生体識別情報が流通することを遮断する。要配慮個人情報と同様の流通制限が及ぶ

【③ 利用停止等請求権の拡張（35条7項・8項）— 離脱可能性】

- 利用停止・消去等を本人が請求できる範囲を拡張し、本人が「離脱したい」と求めやすくする。事後的に流通から抜ける手段を強化するもの

ポイント

特定生体個人情報には、**周知義務・オプトアウト禁止・利用停止等請求権の三本柱**がかかる

特定生体個人情報の生成AIへの影響（学習データ取得）

【開発段階・利用段階の双方にまたがる論点】

- 顔認識AI・映像解析AI・マルチモーダルAIが顔画像・監視映像・SNS画像等を学習に使う場面が問題となる
- 顔画像を単に「画像」として学習させる場合と、顔特徴を抽出・変換してテンプレート生成する場合とで法的評価が大きく異なる
- 監視カメラ映像等は本人が認識しないまま取得された顔特徴を含み得るため、取得元の適法性点検が必要である
- 顔特徴データを含むデータセットの外部取得は、オプトアウト提供禁止との関係で流通ルート自体が違法となり得る

ポイント

自社モデルが顔特徴をどう処理しているかを技術的に検証し、サプライチェーン全体を点検する必要がある

特定生体個人情報の生成AIへの影響（停止請求対応）

【開発段階・利用段階の双方にまたがる論点】

- 最大の課題は利用停止等請求への対応である 学習済みモデルの重みからの特定データ除去（アンラーニング）は技術的に困難
- 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を止められるかを事前設計する必要がある
- 適法導入であっても停止請求は来得るため、応答可能範囲をあらかじめ設計しておく必要がある

ポイント

停止請求への応答可能範囲を、各データ段階で事前に設計しなければならない

特定生体個人情報の生成AIへの影響（ディープフェイク・本人確認）

【開発段階・利用段階の双方にまたがる論点】

【① 開発段階】

- 本人が知らないうちにSNS画像等から顔特徴を抽出し人物生成AIの学習に組み込む行為は、被認識困難性ゆえ本人が気づけず、不正取得（第20条第１項）・不適正利用（第19条）の射程に入り得る。

【② 利用段階】

- 特定個人の顔特徴で人物らしい画像・映像・音声を生成する行為は不適正利用（第19条）の射程に入り得る。生成AI提供者は実在人物の顔特徴の取扱制限・権利処理・危険出力防止を厳格に設計する必要がある。

【③ 顔認証・本人確認AI】

- (a) 周知義務（第21条の2）充足、(b) 利用停止等請求（第35条第7項・第８項）への対応、(c)第三者提供・共同利用ルート（第27条）の適法性、が実務上問われる。

ポイント

特定生体個人情報は、学習段階から運用段階まで一貫して別扱いすべき高リスク情報である

本人同意例外
（18条3項、20条2項、27条1項）

本人同意例外の見直し ― 二つの新例外

同意原則を維持しつつ、現行法の硬直性を①公益性・相当性、②本人の合理的期待の二軸で緩和する改正。

【改正が及ぶ条文】

- 利用目的による制限の例外（第18条第3項）／要配慮個人情報の取得制限の例外（第20条第2項）／第三者提供制限の例外（第27条第１項）の各号にまたがる横断的改正

【新例外①「相当の理由」の追加】（公益性・相当性の軸）

- 生命・身体・財産の保護等の例外に、「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。同意取得が困難な場合に限らず、同意を得ないことが正当化される合理的事情がある場合まで例外を拡張。

【新例外②「本人の意思に反しないことが明らかな場合」】（本人の合理的期待の軸）

- 新たな同意例外を新設。判断基準は事業者の都合ではなく、本人が通常その取扱いをどう期待するか（本人の合理的期待）。本人にとって不意打ちとならない範囲かが分水嶺

ポイント

公益性・相当性と本人の合理的期待という二軸で、現行法の硬直性を緩和する

本人同意例外の生成AIへの影響

【主として利用段階。開発段階にも波及】

- 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、契約履行に必要で本人が通常予期するため「本人の意思に反しない」と整理し得る
- 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となる
- 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 開発段階では、公衆衛生や災害対応で生成AIを活用する場合に「相当の理由」例外が適用される余地がある

ポイント

対話応答処理とモデル改善利用を切り分けて法的整理することが要点である

16歳未満の者の保護
（35条9項・10項、40条の2、58条の3）

16歳未満の者の保護 ― 現行法の状況

【明文特則の不存在】

- 現行個人情報保護法には、16歳未満（未成年者）について包括的な明文の特則がなく、一般ルール（利用目的の特定、同意取得、第三者提供制限等）の適用にとどまっていた。

【Q&A・ガイドラインによる運用】

- 未成年者対応は主として個人情報保護委員会のQ&A・ガイドライン・各事業者の自主運用に委ねられてきた。同Q&Aは、一般に法定代理人（親権者等）から同意を得るべき年齢の目安として「12歳から15歳まで」を一つの基準として示すにとどまり、法律本文に根拠を持つ規律ではなかった。結果として事業者間で対応にばらつきが生じていた。

【離脱権の不存在】

- 利用停止等請求権も、未成年者であること自体を理由に保護を強める仕組みではなかった。SNS・ゲーム・動画・教育サービス等で行動履歴が継続的に蓄積されても、未成年者固有の離脱権は存在しなかった。

ポイント

未成年者保護はQ&A・慣行レベルにとどまり、法律レベルの明文規律が必要であった

16歳未満の者の保護 — 改正内容

未成年者保護を、入口（同意取得）から事後的離脱、さらにサービス設計の適切性まで含む構造へと再構成。法定代理人関与の明文化・利用停止等請求権の強化・最善の利益の責務の三本柱

【① 法定代理人関与の明文化（第40条の2）】

- 同意取得・通知等について、原則「本人」とあるのを「法定代理人」と読み替える。これまでQ&A・慣行に委ねられていた法定代理人（親権者等）の関与を、初めて法律本文に明文化する

【② 利用停止等請求権の強化（第35条9項・10項）】

- 16歳未満の本人について利用停止等請求の要件を緩和し、離脱可能性を強める。蓄積された行動履歴等から未成年者本人が抜けやすくする、事後的救済の強化

【③ 最善の利益の責務（第58条の3）】

- 16歳未満の個人情報等の取扱いにつき、本人の最善の利益を優先的に考慮すべき責務規定を新設。同意の有無という形式論を超え、サービス設計・運用の実質に「子どもの最善の利益」という価値基準を持ち込むもの

ポイント

未成年者保護は、同意取得を超え、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進む

16歳未満の者の保護の生成AIへの影響（年齢確認・停止請求）

【主として利用段階の論点】

主として利用段階（運用）の論点。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等、16歳未満を含み得るサービスでは事前設計が不可避

【① 年齢確認・法定代理人同意の整備】

- 年齢確認、法定代理人同意の取得、通知、停止請求対応の体制整備が必要。ただし、過度な年齢確認はそれ自体が新たな個人情報の取得を伴うというジレンマがある。確認方法の相当性（目的に照らし過剰でないか）が論点となる。

【② 停止請求への対応設計】

- 対話・検索・学習・推薦・課金の各履歴は長期蓄積されやすい。35条9項・10項の利用停止等請求に対し、どのデータを・どこまで・どう消去/停止できるか、技術的・運用的な対応をあらかじめ設計しておく必要がある。

【③ ログ・データセットの切り分け】

- 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が混在すると停止請求対応が困難になる。利用目的別にログ・データセットを切り分けて管理する設計が、停止請求対応と最善の利益の責務（58条の3）の双方の観点から重要。

ポイント

16歳未満を含み得るサービスでは、年齢把握と停止請求対応の事前設計が不可避となる

16歳未満の者の保護の生成AIへの影響（サービス設計・二次利用）

【主として利用段階の論点】

主として利用段階の論点。第58条の3の最善の利益責務により、サービス設計そのものが法的評価の対象となる点で、利用段階への影響が最も大きい。

【① サービス設計が評価対象に】

- 最善の利益責務により、依存誘発的な設計、長時間利用を煽るUI、過剰な課金誘導、過度な擬人化等が評価対象となる。子ども向け生成AIでは、安全性評価や有害出力の抑制だけでなく、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。

【② 入力データの二次利用（モデル改善）】

- 子どもの入力データをモデル改善・学習に用いる場合、法定代理人の関与（40条の2）と最善の利益（58条の3）の観点から、二次利用の相当性が問われる。「同意を取れば足りる」ではなく、子どもの利益に照らした実質的な相当性判断が求められる。

【③ 未成年ユーザー由来データの別建て管理】

- 未成年ユーザー由来データは、通常ユーザーデータと別建てで管理し、学習利用の可否・条件をあらかじめ厳格に設計する必要がある。混在管理は二次利用の適法性確保を困難にする。

ポイント

サービス設計そのものが法的評価の対象となる点で、利用段階への影響が最も大きい

命令・課徴金
（148条、148条の3以下）

命令・課徴金 ― 現行法の状況

【現行の監督手段】

- 現行法にも、報告徴収・立入検査（第146条）、勧告（第148条1項）、命令（第148条2項・3項）といった監督手段は存在する。しかし、二つの大きな限界があった。

【限界① 本人保護命令としての弱さ】

- 現行の命令は、是正を事業者に求めるものが中心で、被害を受けた本人への通知・公表まで含めて本人を直接保護する命令としては弱かった。違反があっても、本人が自らの被害を知り対応する契機が制度的に十分確保されていなかった。

【限界② 利得剥奪手段の欠如】

- 悪質な取扱いによって経済的利益を得た事業者から、その利得を吐き出させる課徴金制度が存在しなかった。違反で得た利益が事業者の手元に残るため、「違反した方が得」という構造を是正できなかった。

【帰結】

- 行政上の勧告・命令だけでは、経済的誘因のある大量・悪質な違反の抑止に限界があった。抑止力が違反による期待利益を下回る状態が放置されていた。

ポイント

本人保護命令の弱さと、利得剥奪手段の欠如が現行法の大きな限界であった

改正内容① ― 命令の強化（第148条・第148条の2）

事後的規律のうち「命令」を、事業者への是正要求から本人保護・違反の周辺遮断まで踏み込む構造へ改める

【第148条 ― 本人保護命令への改編】

- 従来の是正命令に加え、委員会が**本人への通知・公表その他本人保護のために必要な措置**を命じ得る構造に改める。違反の事実を本人が知り、自衛・救済に動く契機を制度的に確保する趣旨。「事業者を直す」だけの命令から、「本人を守る」命令へと性格を拡張するもの。

【第148条の2 ― 第三者への中止要請】

- **違反行為を補助等する第三者（違反を技術的・事業的に支える者等）に対し、中止のために必要な措置を要請**できる枠組みを新設。違反の実行者だけでなく、それを支える周辺事業者にも働きかけ、違反の継続・拡大を実効的に遮断する設計。

ポイント

命令は「事業者の是正」から「本人保護」「違反の周辺遮断」まで射程を拡張する

改正内容② ―利得剥奪型課徴金の導入（第148条の3以下）

違反で得た経済的利益を残さない仕組みを新設し、「違反した方が得」という構造を是正

【制度の性格 ― 利得剥奪型】

- 違法な取扱い等によって得た**財産上の利益相当額**を納付させる課徴金制度を導入。制裁額を一律に定めるのではなく、違反で得た利得を吐き出させる「利得剥奪型」である点が特徴

【対象行為】

不適正利用（第19条）、不正取得・不正利用（第20条）、違法な第三者提供（第27条）に加え、統計作成等特例（本改正で新設される特例）違反が対象に含まれる。

【重大事案への絞り込み要件】

- すべての違反ではなく、(a) 相当の注意を怠ったこと、(b) 対象となる本人が1,000人を超えること、(c) 権利利益の侵害が大きいこと等の要件により、重大・悪質事案に絞り込まれる。軽微な違反まで一律に課す制度ではない。

ポイント

利得剥奪型課徴金により、経済的誘因のある大量・悪質な違反を抑止する

命令・課徴金の生成AIへの影響（統計作成等特例違反）

【開発段階・利用段階の双方にまたがる論点】

開発段階（学習）と利用段階（運用）の双方にまたがる論点。統計作成等特例違反が課徴金対象に含まれることで、特例を使う案件ほど逸脱時の経済的不利益が重くなる。

【① 特例の射程を超えた利用＝課徴金リスク】

- 統計作成等特例で取得したデータを、統計作成の枠を超えて個人別配信・営業ターゲティング等に使えば、特例違反として課徴金の対象となり得る。特例は「統計作成等」という限定された目的の枠内でのみ有効である点に注意。

【② 生成AI特有の横展開リスク】

- 学習用に取得したデータは、評価・モデル改善・広告最適化・営業支援等へ横展開されやすい構造を持つ。この「使い回しやすさ」自体が、特例の射程を無意識に逸脱させ、特例違反リスクを構造的に高める。

【③ 別建ての区分管理が必須】

- 特例取得データは、(a) アクセス権限、(b) 利用可能な工程、(c) 再提供の可否、(d) 学習後の利用範囲を、通常データと別に区分管理する必要がある。混在管理は逸脱の温床となる。

【④ 従来運用の再評価】

- 「統計作成目的だから」と内部的に広く使ってきた取扱いも、課徴金リスクを伴う目的外利用として再評価が必要。従来は許容と整理していた運用が、制度上は重大リスクに変わり得る。

ポイント　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

命令・課徴金の生成AIへの影響（取得経路・第三者提供）

【開発段階・利用段階の双方にまたがる論点】

学習データの取得・利用・第三者提供の各場面が、それぞれ課徴金対象行為に接続し得る。

【① 取得経路の問題（第20条1項）】

- 不正取得・不正利用も課徴金対象。取得経路に問題のあるデータでモデルを構築すれば、経済的不利益に発展し得る。学習・評価データの取得経路、クローリング方法、ベンダー調達経路、契約上の取得権限を、**後から適法性を説明できる形で記録・審査**しておく必要がある。

【② 外部提供の法的構成（第27条1項）】

- API・SaaSの入力・ログ・画像等を外部に提供する場面で、法的構成（委託／第三者提供／共同利用）を誤れば、第27条第1項違反となり得る。

【③「委託」の実質判断】

- 「委託」と説明していた外部処理が、実質的にはベンダー側の独自利用・共同利用に近い場合、第三者提供・範囲外利用の問題が生じ得る。名目ではなく、データ利用の実質で判断される点に注意。

ポイント　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

命令・課徴金の生成AIへの影響（本人保護命令・経営リスク）

【開発段階・利用段階の双方にまたがる論点】

違反は技術・法務の問題にとどまらず、収益構造そのものに関わる経営管理の問題となる

【① 本人通知・公表命令の負荷（第148条）】

違反発覚時、委員会は影響を受けた本人への**通知や事実の公表**まで命じ得る。長期ログ蓄積型サービスや学習済みモデルが絡む場合、(a) 対象本人の範囲把握、(b) 通知方法そのものが技術的に困難となる。命令が出てから対応に着手したのでは間に合わない。

【② 事前のインシデント対応設計】

対象本人の特定、ログの遡及、連絡手段の確保、公表文面の準備までを含めて、あらかじめインシデント対応を設計しておく必要がある。「誰に・どう届けるか」を平時に決めておくことが、命令への実効的対応の前提となる。

【③ 課徴金による経営リスク化（第148条の3以下）】

利得剥奪型課徴金により、違反は売上・収益・事業価値に直接跳ね返る。違反による利得が吐き出される構造のため、コンプライアンス不全がそのまま財務インパクト・事業価値毀損に直結する。

ポイント

個人情報コンプライアンスは、収益構造そのものに関わる経営管理の問題となる

不正取得罪
（180条）

不正取得罪 — 現行法の状況

【一般的処罰規定の弱さ】
現行個人情報保護法には、不正取得そのものを正面から処罰する一般的な犯罪類型が弱かった。第20条1項は「偽りその他不正の手段による取得」を禁止するが、この禁止に**直ちに対応する固有の刑罰規定が明確でなかった**（命令違反等を介した間接的な担保が中心）

【他法令・民事の文脈に流れがちな構造】
その結果、違法なクローリング・スクレイピング等の悪質な取得行為は、主として民事責任・契約違反・他法令（不正競争防止法、不正アクセス禁止法等）の文脈で整理されがちであった。個人情報保護法そのものの刑罰で正面から問う筋道が立てにくかった。

【帰結 — 悪質性の評価の不安定さ】
取得態様がどれほど悪質でも、どこまでを個人情報保護法上の「違法取得」として刑罰で問えるかが見えにくく、悪質取得に対する抑止が安定しなかった。

ポイント　現行法では、不正取得の悪質性が他法令や契約違反の問題として整理されがちであった

不正取得罪の改正内容（第180条の新設）

不正取得を、行政・課徴金・刑罰の三層で重ねて対応する構造へ

【第180条 ― 不正取得罪の新設】
・目的要件：自己等の不正な利益を図る目的、又は加害目的（図利加害目的）があること
・行為要件：人を欺く・暴行・脅迫、又は保有者の管理を害する行為により個人情報等を取得したこと

【着目点 ―「何を」より「どう取ったか」】
取得した情報の内容そのものよりも、**どういう手段・目的で取得したか**という取得態様の悪質性に着目する構成。悪質な手段・目的を伴う取得を、刑事罰で正面から捕捉する。

【三層構造による重畳的対応】
不正取得は、(1) 行政法上の違反（第20条1項違反）、(2) 課徴金対象行為（第148条の3以下）、(3) 刑事罰（第180条）の三層で重ねて設計される。同一の悪質取得に対し、是正・利得剥奪・処罰が重畳的に作動する。

ポイント　不正取得は、行政・課徴金・刑罰の三層で対応される

不正取得罪の生成AIへの影響（自社収集）

【開発段階の論点】

「どうやって集めたか」が重大な刑事リスク論点

【① 収集手法が刑事評価の対象に】
学習データ収集段階に強く響き、取得手法の適法性が従来以上に厳しく問われる。具体的には、(a) アクセス制御の回避、(b) 認証の潜脱、(c) 規約違反スクレイピングの強行、(d) 虚偽登録によるアクセス等は、第180条の**「保有者の管理を害する行為」**と評価され得る。

【② 潜脱態様による刑事リスクの深刻化】
robots.txt、ログイン制限、API利用条件、レート制限等を**潜脱する態様**によっては、刑事リスクが深刻化し得る。技術的制限を意図的に回避するほど、図利加害目的・管理侵害性の双方が認定されやすくなる。

【③ リスクの質的転換】
クローリング・スクレイピングの適法性判断は、これまで中心であった「利用規約違反・民事リスク」の問題を超え、**刑事リスク**の問題にもなり得る。同じ収集行為でも、評価される法的レイヤーが一段重くなる。

ポイント　生成AI開発では「どうやって集めたか」が重大な刑事リスク論点になる

・**スクレイピング**：プログラムでWebサイトに自動アクセスし、掲載情報を機械的に大量収集する手法。クローリング（自動巡回）と一体で用いられ、生成AIの学習データ収集の主要手段。
・**robots.txt**：Webサイトの管理者が「どの範囲の自動アクセスを認める／拒否するか」を記載し、サイト側に置く取り決めファイル。クローラーに対する管理者の意思表示であり、これを無視した収集は管理者の管理意思に反する取得と評価され得る。

不正取得罪の生成AIへの影響（外部調達・評価データ）

【開発段階の論点】

自社収集だけでなく、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。
【関係条文】第180条（不正取得罪）／第148条の3以下（課徴金 ― 不正取得由来データの利用）

【① 調達元の取得態様が自社リスクに】

- 外部ベンダー・データブローカーからの調達でも、取得元がどう集めたか（取得元の取得態様）が法的リスク評価上重要になる。「買っただけ」では免責されず、調達元の不正取得が自社のリスクに連鎖する。

【② 不正取得由来データでのモデル構築】

- 不正取得に由来するデータでモデルを構築すること自体が、課徴金対象行為としても問題化し得る。汚染されたデータは、学習に使った時点で開発成果全体にリスクが及ぶ。

【③ 契約・監査・記録の重要性】

- データセット購入契約、ベンダーによる適法取得の保証、監査権限、取得経路の説明資料が従来以上に重要。調達元の適法性を契約と記録で担保し、後から説明できる状態にしておく必要がある。

【④ 評価・教師・RLHF・検索拡張データも同水準】

- 学習データに限らず、評価用・教師用・RLHF用・検索拡張（RAG）用データの取得態様にも、同水準の適法性審査が必要。「主たる学習データ以外は緩くてよい」とはならない。

ポイント　学習データだけでなく、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

代表的なAIサービスとの関係

代表的なAIサービスとの関係（総論）

生成AIの法的検討では、法令適合性とサービス規約適合性を一体として設計・運用する必要がある

【検討の出発点 ― 法令と規約の両輪】

- 生成AIの法的検討では、個人情報保護法等の法令だけでなく、各サービス提供者の**利用規約・ポリシー・データ利用ポリシー**の確認が不可欠。法令上適法でも規約違反となり得るし、その逆もあり得る。

【契約類型による前提の違い】

- 同じ「生成AI利用」でも、(a) 個人向け、(b) 法人向け、(c) API利用で、入力データの取扱い、モデル改善への利用、データ保持期間、禁止用途の前提がそれぞれ異なる。どの類型で使うかを誤ると、想定と異なるデータ利用が起こり得る。

【三段の切り分け】

検討は次の三段で切り分ける。
①日本法上適法か（個人情報保護法等）
②提供事業者の規約上許容されるか
③個人向け契約か／法人向け契約か（適用される規約・データ取扱いの確認）

【規約・ポリシーが法的評価に直結する】

- 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・相当の注意の各評価に密接に関係する。規約の理解不足は、そのまま法令上の評価（特に「相当の注意」を尽くしたか）に跳ね返る。

ポイント　法令適合性とサービス規約適合性を一体として設計・運用する必要がある

ChatGPT（OpenAI）— 抽出禁止と契約体系

個人向け画面・出力の大量取得は、規約違反と不正取得評価の双方に接点を持つ

【契約体系の区別】

- OpenAIは、(a) 個人向けの **Terms of Use** と、(b) 企業・開発者向けの **Services Agreement**（**Business terms**）を区別している。どちらが適用されるかで、データ・出力の取扱いの前提が大きく異なる。

【個人向けサービスの主な制限】

- データや**Output（出力）の自動的・プログラム的な抽出（scrape等）が禁止**されている ・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

【生成AI開発で問題となる典型場面】

- 個人向けChatGPTの画面・出力を大量取得し、自社モデルの学習・評価データに転用する行為は、上記の抽出禁止・競合モデル開発禁止に正面から触れ、**規約上強い問題**を生じ得る。

【改正法案との接点】

この種の取得は、規約違反にとどまらず、改正法案上の**不正取得罪（第180条）や取得態様の適法性評価**とも接点を持ち得る。アクセス制限・規約を潜脱する態様であれば、「管理を害する行為」としての評価リスクが生じる。

ポイント　個人向け画面・出力の大量取得は、規約違反と不正取得評価の双方に接点を持つ

ChatGPT（OpenAI）— 会話データの取扱い

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。

【① データ利用の基本説明】

- OpenAIは、個人向けサービスのデータを、サービスの提供・維持・開発・改善・安全確保等の目的に用いると説明。「会話＝サービス改善に使われ得る」ことが出発点

【② 個人向けでの学習利用コントロール】

- 個人向けChatGPTでは、(a) 設定により**モデル改善への利用をオフ**にできる、(b) **Temporary Chat** は履歴・メモリ・学習に使われない。ただし設定はユーザー側の操作に依存し、組織的に担保されるものではない。

【③ 第三者送信データの取扱い】

- GPTの**アクション機能**等で第三者サービスへ送信されたデータは、その第三者のポリシーに従う。OpenAIの設定だけでは取扱いを統制しきれない領域が生じる

【④ 契約類型による前提の違い】

- 企業利用では、個人向けプランか／法人向け・API向け契約かで入力データ取扱いの前提が異なる。日本法上の**委託・第三者提供・安全管理措置**を重視するなら、設定依存の個人向けではなく、**法人向け契約・管理機能を前提**とすべき

ポイント

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

Claude（Anthropic）— Constitution の位置付け

Constitution は外部ルールではなく、内部規範として理解するのが適切

【Claude's Constitution とは】

- Claude には、訓練の基礎文書である **Claude's Constitution**（Claudeの憲法）があり、**CC0**（パブリックドメイン相当）で公開されている。Claude がどのような価値・原則に基づいて振る舞うべきかを定めた基礎文書

【Anthropic による位置付け】

- Anthropic は、これを **Claude のあるべき姿に関する最終的な権威**として位置付けている。他方で、**実際の出力が常に Constitution どおりとは限らない**ことも明示している（理念と実挙動は完全には一致しない）

【法的性格 — 外部ルールではない】

- Constitution は、第三者を拘束したり事業者に義務を課したりする**外部的拘束力を持つルールではない**。モデルの設計・訓練・運用の基準となる**自主規律・内部規範**と理解すべき。法令・契約の代替物ではなく、提供者の自己規律の表明

【実務上の含意】

したがって、Claude を業務利用する際の適法性・契約上の可否は、Constitution ではなく、別途の**利用規約・データ利用ポリシー・法人向け契約**で判断する必要がある。

ポイント　Constitution は外部ルールではなく、内部規範として理解するのが適切

Claude（Anthropic）— 外部ルールと改正法案との関係

Claude 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

【外部向けルールの体系】

- 外部向けルールとして、(a) **Consumer Terms**（個人向け）、(b) **Commercial Terms**（法人・API向け）、(c) **Usage Policy**（利用ポリシー）が存在する。前頁の Constitution（内部規範）とは性格が異なる

【個人向けの学習利用コントロール】

- 2025年8月の更新で、個人向けは、データを Claude の改善等に**使うかどうかを選択できる仕組み**が導入された。ユーザー側の選択に委ねられる構造である点に注意

【法人・API領域への不適用】

- Claude for Work・Government・Education・API 利用など **Commercial Terms 適用領域**には、上記の個人向け更新は及ばない。法人領域は別の契約前提で取扱いが規律される

【Usage Policy の役割】

- Usage Policy 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。技術的な利用態様に対する行為規範として機能する。

【二層構造での理解】

- **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。法令・契約上の判断は後者（外部ルール）に基づく。

ポイント　Claude 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

Gemini（Google）— 利用形態別の区別

個人向けでは、Activity や Temporary chats の設定が前提を大きく左右する

【① 利用形態の区別が出発点】

- **個人向け Gemini Apps** と、**Google Workspace 又は Google Cloud 上の法人向け利用**を分ける必要がある。両者は入力データ取扱いの前提が大きく異なり、企業利用では法人向け基盤の利用が原則

【② 個人向けの学習利用 — Activity 設定に依存】

- 個人向けでは、**Gemini Apps Activity がオン**のとき、会話等が Google の AI 改善に利用され得る。学習利用の有無がユーザー側の設定状態に依存する構造

【③ 学習に使われない条件】

- **Temporary chats** は AI モデルの学習に使われない ・Activity を**オフ**にし、かつフィードバックを送信しなければ、将来のチャットも改善に使われない

【④ 人間によるレビューの存在】

- 個人向け Gemini Apps では、**人間のレビュー担当者が会話を確認**し、サービス改善に用いる場合がある。機密・個人データの入力は、この点を踏まえて慎重に判断する必要がある

ポイント　個人向けでは、Activity や Temporary chats の設定が前提を大きく左右する

Gemini（Google）— 法人向け保護と禁止用途

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必要がある

【① 法人向けのデータ保護】

- 職場・学校アカウントで **enterprise-grade data protections** が適用される場合、会話等が**人間レビューや生成AIモデルの改善に使われない**旨が案内されている。個人向けとは前提が根本的に異なる。

【② Workspace 上の組織データの位置付け】

- 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**とされている。法人領域では「学習に使われ得る」前提が外れる。

【③ 禁止用途 — Prohibited Use Policy】

- **Generative AI Prohibited Use Policy** があり、違法・有害・詐欺的・権利侵害的な利用等が禁止されている。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。

【④ 改正法案との関係】

- 利用段階において、(a) 入力データの取扱い・保持、(b) モデル改善利用の有無、(c) 利用形態別の区別、(d) 禁止用途の確認、が重要となる。規約・ポリシーの確認が「相当の注意」を尽くしたかの評価に直結する。

ポイント　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必要がある

代表的なAIサービスとの関係（小括）

3社に共通する結論は一つ —— **法令適合性とサービス規約適合性は、一体で設計・運用しなければならない**。

【3社の要点】

- **ChatGPT（OpenAI）**：個人向け Terms of Use が自動抽出・競合モデル開発を禁止。法人向け・API には別建ての Services Agreement
- **Claude（Anthropic）**：内部原則の Constitution と、外部ルールの Consumer Terms・Commercial Terms・Usage Policy が並立。判断は外部ルールに基づく
- **Gemini（Google）**：個人向け Apps／Workspace 向け／Google Cloud 上で前提が異なり、利用形態別の切分けが不可欠

【3社に共通して確認すべき4点】

サービスを問わず、(a) どの契約体系が適用されるか、(b) モデル改善利用の有無、(c) 自動抽出・禁止用途への該当性、(d) 法人向け契約・管理機能の有無、を確認する必要がある。個人向けか法人向けかの切分けが共通の起点

【法的評価との不可分性】

これらの規約確認は、**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。規約の確認漏れは、そのまま「相当の注意」を尽くしたかの評価に跳ね返る。

ポイント　代表的なAIサービス利用企業は、法令適合性とサービス規約適合性を一体として設計・運用する必要がある

実務対応・まとめ

生成AI事業者が優先的に棚卸しすべき領域

開発段階・利用段階の双方を、データ類型別・工程別に棚卸しする必要がある

【① 学習データの取得経路（開発段階）】

- クローリング・スクレイピング・外部調達について、**どこから・どう取得したか**の経路と適法性を点検。不正取得罪（第180条）・課徴金との接点が最も強い領域

【② 各工程の特例該当性（開発段階）】

- 事前学習・ファインチューニング・RLHF・評価の各工程ごとに、**統計作成等特例に該当するか／その枠を超えていないか**を整理。工程をまたいだ横展開が逸脱の典型

【③ 高リスクデータ類型の混入確認】

- データセットに、**公開要配慮個人情報・連絡可能個人関連情報・顔特徴データ（特定生体個人情報）**が含まれていないかを類型別に確認。混入時の規律が重い類型。

【④ 入力・ログのモデル改善利用（利用段階）】

- API・SaaS の入力・会話ログをモデル改善に使う場合の、**委託／第三者提供／範囲外利用**の法的整理。名目ではなく実質で判断

【⑤ 未成年・利用サービスの規約（利用段階）】

- **16歳未満を含み得るサービス**かの確認と、利用している外部AIサービスの**規約・契約体系**（個人向け／法人向け）の確認

ポイント　開発段階・利用段階の双方を、データ類型別・工程別に棚卸しする必要がある

生成AI事業者が整備すべき体制

法的根拠・契約・技術統制・運用記録を一体で管理し、説明可能性を確保する必要がある

【① 特例データの隔離管理】

- 特例取得データを通常データと別建てで管理するアクセス制御・権限管理・監査ログ。混在を技術的に防ぎ、誰が・いつ・何に使ったかを残す

【② 継続公表の運用体制】

- 統計作成等特例等で求められる継続的な公表の管理体制と、変更時には事前に公表するプロセス。公表は一度きりでなく、運用として回す必要がある

【③ 説明可能性の確保（記録・審査）】

- 取得経路・契約・利用工程を、後から適法性を説明できる形で記録・審査する仕組み。「適法だったはず」ではなく、証跡で示せる状態にしておく

【④ インシデント対応設計】

- 本人通知・公表命令に即応できる設計 —— 対象本人の特定、ログの遡及、公表文面の準備まで平時に用意。命令後に着手したのでは間に合わない。

【⑤ 組織・ガバナンス連携】

- 法務・情報セキュリティ・事業部門・経営陣の連携と、取締役会への報告ルート。課徴金により経営リスク化するため、現場任せにせず経営マターとして扱う。

ポイント

法的根拠・契約・技術統制・運用記録を一体で管理し、説明可能性を確保する必要がある

おわりに ― 生成AI事業に求められる対応

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の三位一体の管理**である

【① 影響は「特例」にとどまらず重なり合う】

- 今回改正の影響は統計作成等の特例を中心としつつ、そこにとどまらない。**委託先二次利用規制・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・命令・課徴金・罰則**が重畳的に効く。論点は単独でなく、束として現れる

【② 求められるのは精緻なデータガバナンス】

- 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。「使えるか」の判断から、「説明できるか」の体制へと水準が上がる

【③ 一貫した設計・運用・説明が前提条件】

- 開発段階・利用段階の双方で、**どの工程が・どの法的根拠と統制に基づくか**を、一貫して設計・運用・説明できる体制が前提条件となる。工程ごとの場当たり対応では足りない

【④ サービス規約は日本法評価と不可分】

- ChatGPT・Claude・Gemini の規約・ポリシーは、日本法上の評価（委託・第三者提供・安全管理措置・不正取得・相当の注意）と切り離せない。規約確認は法令対応の一部である

ポイント　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の三位一体の管理である