個人情報保護の私法的基礎に関する序論的考察（2）

――財産権と人格権の交錯する領域における理論的課題――

山　田　　希*

目　　次

Ⅱ．個人情報保護法の実体規律と運用課題

本章では、Ⅰで整理したデータ・ライフサイクルの主要4段階――取得、保管・管理、利用・提供、消去・廃棄――を前提に、個人情報保護法（以下、「個情法」という）の実体規律と運用実態とのギャップを分析する。加えて、これら各段階を横断する救済手段とその実効性を検証し、国際社会で伝統的に広く共有されてきた目的限定モデル（purpose-limitation model）――なかでも日本法が採用する「利用目的中心主義」――の限界を踏まえて、リ

＊　やまだ・のぞみ　立命館大学法学部教授

スクベース型・デューデリジェンス型の統制で補完するための要件を導き出す。本章の構成は、次のとおりである。まず 1 で利用目的中心主義の構造と限界を明らかにし、続く 2 でデータ・ライフサイクルの各段階における私法的含意を、3 で同意メカニズムの 5 場面におけるリスク分析を、4 で本人請求権と救済スキームをそれぞれ検討したうえで、最後に 5 で日本型モデルの強みと課題を総括する。

1．利用目的中心主義の構造と限界

本節では、日本の個人情報保護法制を特徴づける「利用目的中心主義」（目的限定原則を個人情報保護の中核とみなし、通知・同意に過度に依存する規制理念）の構造を概観したうえで、その制度的限界を① 通知・同意の形式化、② 技術革新への不適合、③ 救済手段の脆弱性という 3 つの次元に分けて検討する。以下では、まず（1）で制度設計上の構造を整理し、（2）で判例・行政事例に見る運用上の機能不全を分析し、最後に（3）で次節以降につながる課題を提示する。

⑴ 包括的目的設定と拡大する情報非対称性

個情法は、制定当初から――そして、その後の改正を通じても一貫して――利用目的中心主義、すなわち「利用目的の特定・通知」を規制の中核とする制度モデルを採用してきた[1)]。2020年（令和 2 年）改正では、重大な漏えい等についての報告・通知義務（26条）が新設され、法人の罰金上限を 1 億円以下に大幅に引き上げる（184条）など、リスク管理型の規律強化が図られたが、依然として利用目的に関する各種規定（17～19・21条）が実体面での「第一関門」、すなわち個人情報の取扱開始時点で最初に充足すべき要件であり、かつ、その後の取扱段階における各種義務の適法性判断の基準となるという構造は維持されている。

ところが近年、多くの事業者が、① 個人情報の用途を利用目的として網羅的に列挙したり、②「サービス向上」等の包括的な表現に多種多様なサービスを包摂したり、あるいは③「商品開発、製品改良、サービス向上、品質改善」のように、同義語や重複項目を累積的に列挙する手法をとるようになった[2)]。たとえば、EC サイトが利用目的を、「当社サービスの提供・改善、新サービス開発、提携企業のマーケティング」と掲げる場合、サービス利用者は、実際のデータフローや提供先を具体的に推測することができず、自分にとってのリスクやメリットを適切に評価できないまま、結局はサービスの享受と引き換えに個人情報の提供を迫られることになる。その結果、利用者の選択的自己決定――本人が提供する情報の範囲を自ら取捨選択し、その選択の判断材料をもとにサービス利用の可否を決める権限――は名目的なものとなり、その一方で、事業者が負う利用目的の通知・公表義務は、抽象的な目的の提示さえすれば「説明責任を果たした」と主張し得る事実上の免責条項へと変質して、本来は縮減すべき情報非対称性がかえって拡大するという逆説的状況が生じている[3)]。

⑵ 判例・行政事例が示す機能不全

利用目的の特定義務（17条）、通知・公表義務（21条）、目的外利用の制限（18条、19条）といった利用目的規定は、本来、個人情報の取扱い範囲を事前に明確化し、その枠を超える処理を抑止することにより実体規律として機能するはずである。しかし、近時の紛争事例をみると、違法性判断の重心は、利用目的の逸脱そのものではなく、事後的な安全管理措置の適否へと傾斜し、利用目的の遵守が主要な争点となる例はほとんどみられない。

実際、ベネッセ名簿大量流出事件（最決令和２年12月22日[4)]）では、第一審が委託元の注意義務違反を否定したのに対し、控訴審は Android 4.0の普及状況や DLP ソフトの市販状況を根拠に委託元にも監督義務違反を認定したうえで一人当たり3,300円（慰謝料・弁護士費用）の損害賠償請求を認容したが、名簿転売による情報拡散を違法性判断の重要な要素として位置づけ

つつ、利用目的の逸脱それ自体を独立した違法事由として正面から論じることはなかった。最高裁が上告受理申立てを不受理とした結果、目的限定原則違反の法的評価は明確化されないままとなった。

リクナビ内定辞退率事件では、就職活動支援サイト運営事業者が学生のサイト内閲覧履歴等をもとに内定辞退確率を AI で算出し、本人の同意なく採用企業に販売していた事案を受けて、個人情報保護委員会が事業者の同意取得回避の事実を摘示し、是正勧告を行った[5]。しかし、委員会の判断は個人データの取扱い手続の不備に集中し、AI スコアリングが、当初掲げた「採用支援目的」の範囲を実質的に逸脱していたかどうかという目的限定原則の核心的問題については明確な判断を示さず、企業側の再発防止策の整備を求めるにとどまった。

2021年に発覚した LINE 社の国外アクセス問題でも、海外の委託先企業が国内ユーザーの個人情報にアクセス可能な状態となっていた事案において、当局はアクセス権限や組織ガバナンスの是正を主眼とした行政指導を行い、越境移転の適法性や利用者同意の再取得要否といった本質的論点には触れなかった[6]。

上記 3 事件ではいずれも、① 利用目的の逸脱が発覚した後に論点が安全管理論へと収斂し、② 民事訴訟では少額慰謝料の認容にとどまり、行政処分でも限定的な勧告・指導を超えることがなく、目的限定原則は実効性を欠く名目規範と化していた。

⑶ 小　　括——「目的限定」から「リスク限定」への転換課題

以上の検討が示すとおり、わが国の利用目的中心主義には、① 通知される利用目的が抽象的・包括的になりやすく、情報主体が実質的に同意・不同意を選択することができない（同意の形骸化）、② AI プロファイリングやクロスボーダー処理など二次利用を把握しきれない（追跡可能性の欠如）、③ 目的外利用が発覚しても少額の損害賠償にとどまり、行政処分も限定的な勧告・指導を超えない（救済手段の脆弱性）という三重の限界が存在する。

そこで次節では、データの取得・保管・提供・消去というライフサイクルの各段階で私法上課される注意義務・安全管理義務に着目し、従来の通知・同意モデルを補完する「リスクベース型統制」の可能性を追求する。

２．ライフサイクル４段階の私法的含意

本節では、個人データが誕生してから消滅に至るまでの流れを――取得、保管・管理、利用・提供、消去・廃棄という――4つの連続的局面に区分したうえで、それぞれの局面で事業者に課される私法上の注意義務と安全管理義務がどのように段階的に質量を変え、相互に重層化していくかを追跡する。各フェーズの義務構造を精査し、通知・同意に過度に依拠する「利用目的中心主義」が抱える抑止力の空洞化を補完し得る統制手法として、リスクの具体的性質と重大性に応じた責任再配分――リスクベース型統制――の私法的基盤と実効性を検証し、次章以降で展開する具体的制度設計の理論的土台を提供することが、本節の狙いである。

⑴　取得段階――適法取得義務

個人情報を取得する場面では、利用目的をあらかじめ特定・明示しなければならない義務（17条１項）と、要配慮個人情報について原則として本人の事前同意を得る義務（20条２項）が中核的な統制要素となる。これらは一見すると行政法上の遵守事項にとどまるように見えるが、私法的観点からは、不法行為責任の成否や契約上の付随義務違反を判断する際の重要な指標ともなる。適法取得義務を怠ったまま個人情報を収集すれば、取得者は単に行政上の制裁を受けるにとどまらず、情報主体に対して損害賠償責任（民法709条）や信義則上の義務違反を理由とする責任（同１条２項）を負うことになる。事業者と本人の間に利用規約や入会契約といった私法上の関係が存在する場合には、取得目的の範囲を逸脱した情報の収集行為が契約上

の付随義務違反として債務不履行責任を構成する可能性も否定できない[7]。

この点を端的に示したのが、いわゆる早稲田大学江沢民主席講演会名簿提出事件である（最判平成15年 9 月12日民集57巻 8 号973頁）。大学が講演会参加者の学籍番号、氏名、住所、電話番号を本人の同意なく警察に提供した本件で、最高裁は、「学籍番号、氏名、住所及び電話番号は、早稲田大学が個人識別等を行うための単純な情報であって、その限りにおいては、秘匿されるべき必要性が必ずしも高いものではない」と前置きしつつも、「本人が、自己の氏名、住所等を大学に知らせた目的、提供した状況等に照らし、これを警察等の捜査機関に提供することは、本人の意思に反する目的外使用であって、プライバシーを侵害するものとして、不法行為を構成する」と判示した。なお、この事件では不法行為責任の成否が争われたが、大学と学生の間には在学契約という継続的契約関係が存在し、個人情報の適切な管理も契約上の付随義務として位置づけ得ることから、契約責任の成立余地も十分に認められると解される。実際、裁判例には、銀行取引や医療契約など多様な契約関係において情報の適正取扱義務を認め、その違反に対する債務不履行責任が問題となったものもある[8]。いずれにせよ、本判決は、個人情報の収集時に設定された「取得目的」が、後続段階――とくに第三者提供――の適法性を統制する基準として機能することを鮮明に示している。

さらに、不正に取得された名簿を購入した第三者が、名簿が違法に流出したものであることを知り、または通常の注意を尽くせば容易に知り得たと評価される事情があった場合、その売買契約は、社会通念上看過しがたい取引として公序良俗（民法90条）に反し、無効となる余地がある[9]。この場合、名簿データは法律上の原因を欠いた受領物となり、買主は返還義務（具体的には媒体の返却または完全な消去を行う義務）を負う。個人情報の消去請求については、在日台湾人身上調査訂正請求訴訟判決[10]において、事実に反する個人情報により社会生活上不利益を被る蓋然性がある場合には、人格権に基づき情報保有者に対して「個人情報中の事実に反する部分の抹消・

訂正を請求しうる」と判示されており、このことを踏まえるなら、不正取得名簿についても、プライバシー侵害の継続を排除するための完全消去請求が人格権を根拠として構成されると解される。

加えて、当該名簿を利用して本人のプライバシーを侵害したときは、契約の無効とは別に、不法行為責任（民法709条）を問われる可能性も高い。実際、宇治市住民票データ流出事件[11)]では、市の委託先従業員が住民基本台帳データを不正にコピーして名簿業者に販売し、その名簿業者がさらに他の業者に転売するという一連の流通過程を前提として、住民に対するプライバシー侵害を理由とする市の損害賠償責任が認定されており、不正流出データの売買取引それ自体が違法な権利侵害の一環として扱われている。

⑵　保管・管理段階――安全管理措置と委託監督

膨大な個人情報を恒常的に保持・加工する現在の企業活動では、保管・管理フェーズにおける安全管理措置の欠落は、単なる抽象的注意義務の問題ではなく、具体的な法的責任を生じさせる重大な義務違反となる。典型例がベネッセ名簿大量流出事件である。同事件では、前掲最判平成29年10月23日が個人情報の漏えい自体によりプライバシー侵害に基づく精神的損害が生じ得るという法理を確立したほか、別の訴訟である東京高判令和２年３月25日（LEX/DB 文献番号25566660）は、第一審（東京地判平成30年12月27日判タ1460号209頁）が MTP 通信による情報漏えいの予見可能性を否定したのに対し、これを覆して予見可能性を肯定し、委託先の書き出し制御義務違反および委託元の監督義務違反に基づく共同不法行為責任を認定し、その判決が上告審決定（前掲最決令和２年12月22日）により確定している。とりわけ後者の判決は、大規模データ保有事業者に対する高度の注意義務や委託連鎖の末端まで及ぶ監督義務の射程について重要な判断を示している。すなわち、ライフサイクルの保管・管理段階では、データの保有規模や業務遂行における個人情報処理への依存度の高まりに応じて注意義務が質的に強化され、委託関係の存在が責任の軽減理由とはならないという方向性

が固まりつつある。

⑶ 利用・提供段階――契約責任と違法提供

利用・提供フェーズでは、「本人同意原則」が建前として掲げられる一方（個情法27条１項）、事前同意の例外としてオプトアウト規定が維持されてきた。前述した早稲田大学江沢民主席講演会名簿提出事件は、取得目的を逸脱した第三者提供による目的外利用の典型例であり、ベネッセ名簿大量流出事件は大量個人情報の違法流通における委託元責任を示した代表例である。これらのほかにも、形式的要件の充足だけでは実質的な法的義務を果たしたとは認められないとした裁判例が蓄積されている。

たとえば、HIV 感染看護師事件（福岡地判平成26年８月８日判時2239号88頁）では、医療機関が広範な利用目的を掲げていたにもかかわらず、診療契約に基づいて取得した患者情報を本人の同意なく労務管理目的に転用したことが個情法16条１項（当時）に違反し、「目的外利用に当たるといわざるを得ない」として200万円の慰謝料が認められた。裁判所は、情報の取得経緯および収集目的の特定性に照らして、利用目的の範囲を超える取扱いには「本人の同意を得ることが必要」であると判示して、目的外利用の限界を明確に示した。

また、住民情報漏洩事件（山口地判平成21年６月４日自保ジャーナル1821号145頁）では、受託企業が形式的な安全管理体制（規則・研修等）を構築していたものの、個人情報を含む業務用パソコンの私的持出やデータ消去に関する従業員への指導・監督を実質的に欠いていたことが安全管理義務違反に当たると認定され、913万円余の損害賠償が命じられた。裁判所は、Winny による情報漏洩事故がすでに社会で多発しておりリスクが予見可能であったにもかかわらず、個別的かつ実効的な監督を怠った点を重視し、安全管理義務の履行における具体的かつ継続的な「指導・監督」の必要性を説いた。

2020年改正では提供記録義務（29条１項・２項、30条１項・３項）を導入し、

後追い検証と立証負担の緩和を狙ったものの、再提供制限を契約条項に明示しないまま名簿が流通し続ける実態はなお改善途上である。

利用・提供段階における法的責任は、従来の同意取得方法の適否にとどまらず、提供後の追跡可能性の確保や再提供の封じ込めといった事後的統制の枠組みへと重点が移行しつつあり、違法提供が発覚した場合もまた、保管・管理段階における安全管理義務違反と同様に厳格な責任追及の対象となっている。

⑷ 消去段階――ライフサイクルの終点と再活用

データ・ライフサイクルの終点に位置づけられる消去フェーズでは、2020年改正により、利用停止・消去請求権（35条）が強化された。この請求権は、事業者に対して、「個人情報を保持する必要性」と「本人利益」とを比較衡量する義務を課し、削除義務の実効性を高めるものとなっている。一方、同改正が導入した仮名加工情報制度は、社内での再利用を条件に目的外利用（目的変更）を許容する枠組みであり、同意を中心とする従来モデルを補完する、リスクベース型統制の先駆的試みとなった。

この領域における重要な判例として、まずGoogle検索結果削除事件決定（最決平成29年１月31日民集71巻１号63頁）が挙げられる。児童買春をしたとの被疑事実に基づき逮捕された事実が検索結果に表示されることについて、その削除を求める仮処分が申し立てられた事案において、最高裁は、「当該事実を公表されない法的利益が優越することが明らか」な場合に限り削除を求めることができるという厳格な基準を確立した。そのうえで、削除請求の認否を判断する要素として、事実の性質・内容、伝達される範囲・具体的被害の程度、社会的地位・影響力、記事の目的・意義、掲載時の社会的状況とその後の変化、記事における事実記載の必要性等の比較衡量を示し、検索事業者が「インターネット上の情報流通の基盤として大きな役割を果たしている」ことを重視した。同事件では、児童買春が社会的に強い非難の対象であることから、当該情報が「今なお公共の利害に関する事項」に

該当するとして削除請求を棄却した。

これに対し、Twitter 投稿削除事件判決（最判令和 4 年 6 月24日民集76巻 5 号1170頁）では、建造物侵入により逮捕された事実に関するツイートの削除が求められた訴訟において、最高裁は、削除請求の判断基準として「公表されない法的利益が優越することが明らかな場合」に限るとした原審の基準を明示的に否定し、単に「優越する」ことが認められれば足りるとして、Google 事件の基準より緩和した。同判決は、逮捕から約 8 年が経過し、刑の効力も失われていること、元の報道記事がすでに削除されていること、本件ツイートが「速報することを目的」としたもので「長期間にわたって閲覧され続けることを想定してされたものであるとは認め難い」こと等の事情を考慮して削除請求を認容した。

両判例の結論が分かれた要因として、第一に犯罪の性質の相違（児童買春事件の報道については継続的公共性が認められたのに対し、建造物侵入事件の報道については時間経過による公共性の減退が認定された）、第二に時間経過の評価（Google 事件では逮捕から 3 年余りで刑の効力は継続していたのに対し、Twitter 事件では逮捕から約 8 年が経過し刑の効力も失効していた）、第三に媒体特性（Google の情報流通基盤性が重視されたのに対し、Twitter の投稿プラットフォーム性が考慮された）、第四に周辺事情（元記事の存続が前提とされた場合と削除が考慮された場合とで状況が異なっていた）が挙げられる。また、草野耕一裁判官の補足意見は、公的立場にない犯罪者の実名報道について制裁的機能や社会防衛機能の限界を指摘し、「負の外的選好」（他者の不幸を見て満足する利己的な傾向）を社会的利益として評価することを否定するなど、理論的深化を示している。

なお、個人情報の削除をめぐる判例法理は多層的に発展している。公的機関による大規模情報管理については、住基ネット訴訟（最判平成20年 3 月 6 日民集62巻 3 号665頁）やマイナンバー訴訟（最判令和 5 年 3 月 9 日民集77巻 3 号627頁）が「具体的危険」の存在を削除・差止めの要件とする判断枠組みを確立した。他方、同和地区関連情報削除訴訟（東京高判令和 5 年 6 月28日判

タ1523号143頁）では、センシティブ情報の公開について「人間としての尊厳を否定するものに等しく、許容することができない」として、より強い保護を認めている。これらの裁判例は、情報の性質や管理主体に応じた多様な削除基準を形成しており、個情法上の消去請求権の解釈・運用にも影響を与えるものと考えられる。

上記の判例は、個情法33条の消去請求権とは異なる法的根拠（人格権・プライバシー権）に基づくものの、情報削除の判断枠組みとして重要な意義を有する。個情法上の消去請求が「保持の必要性」と「本人利益」の比較衡量を求めるのに対し、判例は「公共性・公益性」と「プライバシー保護」の比較衡量を行っており、判断枠組みには相違がある。しかし、時間経過による公益性の減退、刑の効力失効、実害の発生等の考慮要素は共通しており、個情法上の消去請求においても参考となる基準を提示している。

こうした判例の動向は、実務上の技術的課題とも密接に関連している。個人情報の完全削除には技術的限界があり、データのリンク可能性を完全に遮断することは困難である。また、バックアップ媒体に残存するデータをどこまで削除対象とみなすかという問題についても、判例上明確な基準は示されていない。判例が示した比較衡量の枠組みは、こうした技術的制約下での削除義務のあり方にも重要な示唆を与えるものと考えられる。

⑸　小　　括――段階的注意義務論の射程

本節の検討を通じて浮かび上がったのは、個人情報のライフサイクルの各段階で事業者に課される義務が、単に並列的に存在するのではなく、相互に連動して責任の質量を段階的に変化させる構造である。

具体的には、取得段階では早稲田大学江沢民主席講演会名簿流出事件が示したように、収集時に設定された利用目的が後続段階の適法性を統制する「基準点」として機能する。保管・管理段階に進むと、ベネッセ名簿大量流出事件が確立した法理により、データ量と処理依存度の高まりに応じて注意義務が質的に強化され、委託関係の存在も責任軽減の理由とはなら

ない。利用・提供段階では、目的外利用や違法提供による損害賠償リスクがさらに重層化し、最終的な消去段階では、Google 事件や Twitter 事件が示した比較衡量論により、削除義務が時間経過や公益性に応じて実質化される。

このような段階的責任強化の枠組みが整備されているにもかかわらず、この枠組みは現実には十分な抑止力として機能していない。その最大の要因は、各段階の義務違反を判断する前提となる「利用目的の特定・通知」という入口部分で、制度の骨抜きが生じているからである。多くの事業者が「サービス改善」「マーケティング全般」といった抽象的・包括的な利用目的を掲げることで形式的なコンプライアンスを満たす結果となり、利用者は自分のデータがどう扱われるかを実質的に把握できないまま同意せざるを得ない状況が生まれている。この情報非対称性は、AI プロファイリングや越境移転のような複雑な処理でさらに拡大し、仮に目的外利用が発覚しても、現行の救済手段では限定的な対処しか期待できない。

そこで次節では、このような同意モデルの「形骸化の現状」をより具体的に検証する。要配慮情報の一括包括同意、抽象目的による AI プロファイリングの無統制、オプトアウト制度の構造的欠陥、越境移転における本人同意の非現実性、そして個人関連情報をめぐるグレーゾーンという 5 つの典型場面を取り上げ、同意メカニズムがなぜ、どのように機能不全に陥るのかを明らかにしていく。

3．同意メカニズム 5 場面のリスク分析

前節で明らかにした段階的注意義務の枠組みが、利用目的の特定・通知という入口部分での制度の骨抜きにより十分な抑止力を発揮できていない現実を受けて、本節では、本人同意が実務の中で形骸化する具体的なメカニズムを検証する。とりわけ、① 要配慮個人情報の取得、② 利用目的変更、

③ 第三者提供、④ 越境移転、⑤ 個人関連情報の提供を取り上げ、それぞれの局面で同意手続の設計がどのように情報非対称性を温存し、リスク評価や事後統制を困難にしているかを明らかにする。これにより、同意モデルの限界をライフサイクル横断的に可視化し、次節以降で検討する救済・抑止メカニズムの再設計に向けた基盤を提示することが、本節の目的である。

⑴ 要配慮個人情報取得の同意――過剰同意と差別回避の狭間

個情法は、病歴・障害・社会的身分などの要配慮個人情報について、あらかじめ本人の同意を得て取得することを原則としている（20条２項）。しかし実務では、とりわけ医療・介護現場において、診療・ケアの連続性を確保する必要から、初診時や入所時に検査結果・紹介状・画像データ等を一括して第三者（提携医療機関・保険者など）へ提供できる旨の包括同意を求める運用が行われている[12)]。こうした包括的な同意取得は業務効率の向上には資するものの、詳細な説明書を患者や利用者が十分理解しないまま承諾する場合が多く、同意の自発性・特定性という保護趣旨が骨抜きになりやすい[13)]。

一方で、差別防止の観点から要配慮情報の取扱いを厳格に制限し過ぎると、感染症サーベイランスやレセプト分析のような公衆衛生上不可欠なデータ収集が停滞するおそれもある。個情法は公衆衛生目的等での例外規定を置いているものの[14)]、実務上は依然として迅速なデータ収集・分析に課題を抱えており、現場は、効率化を優先する「包括同意」と、人権保護を重視する「個別・逐次同意」のあいだで揺れ動いていると解される。

結果として、同意取得は、形式上は整備されても、利用範囲の具体的理解や差別回避策の周知が不十分であり、「同意取得＝リスク低減」という本来の機能が限定的にしか発揮されていないものと考えられる。

⑵ 目的外利用の同意――包括目的とプロファイリングの拡散

個情法は、利用目的の達成に必要な範囲を超えた個人情報の取扱いについて、あらかじめ本人の同意を得ることを義務づけている（18条 1 項）。この規定は、当初想定していなかった新たな用途でデータを利用する際の重要な歯止めの役割を担っている。

ところが実務では、この「同意」という歯止めが巧妙に回避されている。事業者が初期段階から「サービスの提供・改善」「新規サービス開発」「マーケティング全般」といった極めて広範・抽象的な目的を提示することで、後にどのような処理を開始しても「すでに通知済みの利用目的の範囲内」と主張できる構造を作り上げている[15]。

この抜け道の深刻さは、AI プロファイリングの文脈でとくに顕著に現れる。学習済みモデルが別のアルゴリズムで再学習（ファインチューニング）される過程でデータの二次・三次利用が繰り返されても、事業者は「サービス改善」という当初の包括目的に含まれると主張し、本来必要なはずの同意手続を一切行わずに済む[16]。前述のリクナビ内定辞退率事件は、この構造的問題の典型例である。同事件では、学生の閲覧履歴と Cookie ID を用いた高度な確率推定スコアリングが「サービス改善」という抽象目的のもとで実行され、本来であれば明確な目的外利用として同意が必要であったにもかかわらず、包括的な利用目的を盾に手続が回避された[17]。

その結果、同意制度は本来の「利用者保護手段」から「事業者の免責手段」へと性質を変え、目的外利用への歯止めは事実上機能しなくなっている。これは、目的外利用時の同意義務という制度設計そのものを骨抜きにする深刻な脆弱性であり、GDPR にあるような正当利益の比較衡量（6 条 1 項(f)）や追加的保護措置（46条）が制度化されていない日本法では、抽象目的を掲げるだけで目的外利用が実質的にノーチェックになる構造的欠陥を如実に示している[18]。

⑶　第三者提供の同意――オプトアウト規定の構造的欠陥

個情法27条１項は、原則として本人の同意なく個人データを第三者に提供することを禁止している。しかし、同条２項は、一定の項目を事前に本人へ通知・公表し、かつ個人情報保護委員会に届け出れば「オプトアウト方式」で提供を続けられる例外を認めている。もっとも、こうした通知・公表の仕組みだけでは、本人が自身のデータ移転を把握し、拒否することには限界があり、リストブローカーを介した転売が重なると、情報の流れを本人が追跡する術は完全に失われる。

この構造的欠陥の深刻さは、個人情報保護委員会も認識しており、2020年（令和２年）改正では、不正取得された個人データや他の事業者からオプトアウト提供された個人データについても、オプトアウトによる第三者提供が禁止されるなど、規制が厳格化された[19)]。

また、リクナビ内定辞退率事件やベネッセ名簿大量流出事件においても、複数の事業者間でのデータ流通において、本人がその流れを事後的に把握・統制することの困難さが浮き彫りとなった。さらに、2020年（令和２年）改正で新設された個人関連情報制度では、ウェブサイトの閲覧履歴等が提供先で個人データとなることが想定される場合に本人同意の確認が義務付けられたが、提供元と提供先で個人データ該当性の認識が異なることで、情報流通の追跡可能性が著しく制限される問題は根本的には解決されていない[20)]。

このように、オプトアウト手続については、本人が実質的に関与しないまま個人データが流通する「形骸化」が指摘されており、個人情報保護委員会による監督強化や法改正の背景にある構造的課題として公的に認識されている[21)]。

⑷　海 外 移 転――十分性認定と契約措置の限界

個情法は、外国にある第三者への個人データ提供について、原則として本人の事前同意を義務づけているが、一定の場合には例外を認めている（28

条）。具体的には、① 個人情報保護委員会規則で定める十分性認定を受けた国への提供、② 相当措置を継続的に講ずるために必要な基準に適合する体制を整備している者への提供については、同意を要しない。②の「相当措置」を講ずる体制には、標準契約条項（Standard Contractual Clauses: SCC）の締結や拘束的企業準則（Binding Corporate Rules: BCR）の策定などが含まれる。

しかし現実には、日本が十分性認定を行っているのは、EU、英国の 2 か国にとどまり[22]、国際的なデータ流通の規模から見れば極めて限定的である。とりわけアジア太平洋地域では認定国が存在せず、シンガポール、インド、中国といった主要なクラウド・BPO 拠点への移転には、実務上、本人同意または SCC 等の契約措置に依存せざるを得ない[23]。

ところが、クラウドサービスを利用する個人ユーザーが、自身のデータが米国、シンガポール、インドなど複数の国・地域のデータセンターを経由する複雑な内部フローや、各移転先国の個人情報保護法制の実効性を理解・評価することは、技術的・法的専門性の観点から非現実的である。個人情報保護法は同意について明確な定義を置いておらず（27条 1 項参照）、GDPR が求める「自由に与えられた、特定の、事情を知らされた上での、かつ曖昧でない同意」[24] という厳格な要件が存在しないため、このような制度的曖昧性の下では、利用者が移転に伴うリスクを具体的に把握し、真の選択を行うことはさらに困難となる。技術に詳しくない利用者や複雑なプライバシー設定を行う時間的余裕のない利用者――とりわけ高齢者や十分な教育機会を得られなかった者――にとって、このような判断は著しく困難である[25]。さらに、事前チェック済みボックスや複雑な階層構造による情報提示といった「ダークパターン」により、利用者の自律的意思決定が阻害される懸念も指摘されている[26]。

他方、契約措置についても構造的課題が存在する。個人情報保護委員会のガイドラインは、移転先の法制度について「一般的な注意力をもって適切かつ合理的な方法により確認」することを求めるにとどまり[27]、企業の

自己評価と契約文言の整備に過度に依拠している。EU の SCC では、移転先国の法制度や実務慣行を詳細に分析するデータ移転影響評価（TIA: Transfer Impact Assessment）の実施が求められているが[28]、これは事業者にとって相当の専門的負担となる。

さらに深刻なのは、クラウド事業者による再委託の重層化である。SCC が想定する一次移転者と一次受領者の一対一関係では、実際のマルチクラウド環境やサブプロセッサーの動的な追加・変更を把握することが困難である。提供元企業は委託先に対する監督責任を負い続けるものの[29]、たとえば OpenAI が顧客データを一定期間保持し、場合によっては人間の審査員がアクセスする可能性があることを公表しているように[30]、クラウド事業者の内部運用プロセスの実態把握は著しく困難である。

このように、越境データのフローの複雑性と処理速度が飛躍的に高まる一方で、本人同意と書面契約だけを主軸とする現在の枠組みは、実質的なリスク把握と権利保護を確保する限界点に達しつつある。この構造的課題に対応するため、EU では「プライバシー・バイ・デザイン（Privacy by Design）」の理念のもと、システム設計段階からデータ保護を組み込む技術的・組織的措置の義務化が進められている[31]。日本においても、同意原則の限界を補完する新たなアプローチ――リスクベース評価、継続的監査、技術的保護措置の標準化等――の制度化が急務となっている。

⑸　個人関連情報提供――「非個人情報」規制のグレーゾーン

2020年（令和２年）の改正で導入された個人関連情報制度は、クッキーID、広告識別子、位置情報、画像情報、SNS の書込みなど、単独では個人を識別できないが、他の情報と容易に照合することで特定個人の識別が可能となる「グレーゾーン情報」を対象とする[32]。同制度は、提供元では個人データに該当しない情報であっても、提供先において個人データとなることが想定される場合、提供者が「受領者において個人データとして取り扱われることとなることを想定することが合理的であるとき」に、本人同意の確

認等を義務づける[33]。

この規定は、リクルートキャリア社が就職活動学生のサイト閲覧履歴等から内定辞退率を AI を用いて予測し、本人の同意なく採用企業に販売した「リクナビ事件」を直接の契機として新設された[34]。同事件では、提供元（リクルートキャリア社）にとっては Cookie ID や閲覧ログといった「非個人情報」であっても、提供先（採用企業）が保有する学生の氏名・大学等と照合されることで容易に個人識別が可能となる構造が問題視された。

しかし実務では、提供側が受領側の再識別有無を事前に把握すること自体が極めて困難である。とりわけ問題となるのは、オンライン広告の RTB（Real-Time Bidding）である。RTB では、ウェブページの 1 インプレッション表示ごとに数十から数百の広告主・DSP（Demand Side Platform）・SSP（Supply Side Platform）が100ミリ秒以内のオークションに参加し、ユーザーの閲覧履歴、推定年収、興味関心カテゴリーなどのデータが瞬時に流通する[35]。この環境下では、どの事業者がどの程度の個人識別能力を有し、取得したデータをどのような外部データと照合するかを、提供側が合理的に予測することは技術的に不可能に近い[36]。

さらに深刻な問題は、RTB を通じた個人関連情報の大量流通が、マイクロターゲティング広告という高度な個人プロファイリング技術を可能にしていることである。アドテク事業者は、複数のサイトから収集した Cookie データとアルゴリズムを組み合わせることで、個々人の政治的志向、健康状態、経済状況等を推定し、特定の個人を狙い撃ちする精密な広告配信を実現している[37]。この過程で、提供元が想定していない再識別化や機微情報の推定が日常的に行われているが、31条 1 項の「個人データとして取得することが想定されるとき」という主観的要件では、こうした予期しない二次利用を効果的に規制できない。

この構造的欠陥は、同意取得プロセスの設計によってさらに深刻化している。多くのサイトは、IAB Europe の TCF（Transparency and Consent Framework）2.0に準拠した CMP（Consent Management Platform）を導入し、

クッキーバナーによる一括同意を実装している[38]。ところが実際には、数百社のベンダー名が階層的に表示され、それぞれの処理目的、保持期間、国際移転の有無などを利用者が個別に検証することは不可能である。このような複雑かつ大量の情報提示は、UI/UX 設計論で「ダークパターン」と呼ばれる手法――利用者を欺いて意図しない選択をさせる巧妙なインターフェース設計――の典型例であり[39]、前節で指摘した同意モデルの形骸化を技術的側面から裏付けるものである。

GDPR 第４条11号が求める有効な同意の要件――「自由に与えられた、特定の、事情を知らされたうえでの、かつ曖昧でない同意」――と照らし合わせると、現在の CMP による同意取得は、複数の観点で適法性に疑義がある[40]。第一に、サービス利用を条件とした同意要求は「自由性」を欠く可能性が高い。第二に、数百社への一括同意は「特定性」の要件を満たさない。第三に、技術に詳しくない利用者や時間的制約のある利用者――とりわけ高齢者や十分な情報リテラシー教育を受けていない者――にとって、膨大な情報の中から真に重要なリスクを識別することは著しく困難であり、「事情を知らされたうえでの同意」があったとは評価しがたい[41]。このような同意取得の構造的問題は、日本法においてより深刻な課題を提起する。日本の個人情報保護法は「個人情報の有用性に配慮しつつ、個人の権利利益を保護する」という保護と活用の「調和」を基本理念とするが（１条）、GDPR 第４条11号のような厳格な同意要件を明示していないため、形式的同意による免責構造がより容易に成立し得る。AI・ビッグデータ時代においては、本人が自身の個人情報の二次・三次利用を網羅的に予測し統制することがますます困難になっており[42]、個人関連情報と個人データの境界における広大な灰色領域と相まって、同制度の実効性には根本的な疑問が残る。

この状況は、個人情報保護委員会が「データ利活用の促進」と「個人の権利利益の保護」という相反する政策目標を同時に追求せざるを得ない制度的ジレンマを浮き彫りにしている[43]。従来の通知・同意モデルの限界が明白となった今、システム設計段階からプライバシー保護を組み込む「プ

ライバシー・バイ・デザイン（Privacy by Design）」や、処理の性質とリスクに応じた多層的統制を可能にするリスクベース・アプローチの導入が急務となっている[44)]。

⑹ 小　　括——同意モデルの構造的「形骸化リスク」

以上５つの局面の検討を通じて浮き彫りとなったのは、「同意モデル」が抱える三層の構造的脆弱性である。

第一に、情報非対称性の制度的温存がある。要配慮個人情報の「一括包括同意」、目的外利用における「サービス改善」等の抽象的目的設定、第三者提供での形骸化したオプトアウト通知、越境移転における複雑なデータフロー、個人関連情報の RTB 環境での瞬時流通——これらすべてに共通するのは、利用者が実際のデータ取扱いの範囲・リスク・影響を具体的に把握することが構造的に困難な制度設計となっていることである。抽象的・包括的な利用目的や同意文言は、本来縮減すべき情報非対称性をかえって拡大し、利用者の自律的意思決定を名目的手続へと変質させている。

第二に、事後統制メカニズムの機能不全が存在する。同意取得後のデータフローについて、事業者自身も監督機関も十分な監督・検証を行えない構造的欠陥が各局面で確認された。医療現場での提携機関への包括提供、AI プロファイリングでのファインチューニング、名簿ブローカーを介した転売の重層化、クラウド再委託の多段階化、RTB での数百社同時参加——これらの複雑なデータ流通において、個人情報保護委員会の事後的勧告・指導は限定的な効果しか持たず、本人による権利行使も費用負担・立証責任の高さから実質的に困難である。

第三に、技術革新に対する制度追随性の限界が明らかとなった。AI 学習や越境データフロー、リアルタイム入札といった新たな処理形態では、データ連携が時間的・空間的に際限なく拡散するため、取得時点での同意では将来のリスクを網羅的に予測・統制することが不可能である。とりわけマイクロターゲティング広告では、個人の政治的志向・健康状態・経済状況

等の機微情報が本人の認識しないまま推定・利用されており、31条１項の「個人データとして取得することが想定されるとき」という主観的要件では、予期しない二次利用を効果的に抑止できない。

これら三層の脆弱性が相乗的に作用した結果、同意は本来の利用者保護手段から事業者の免責手段へと性質を変化させている。形式的な同意取得手続を経てさえいれば、その後のデータ取扱いが本人の合理的期待を大幅に逸脱しても、法的責任を回避し得る「免罪符」として機能する構造が定着している。

そこで次節では、こうした限界が現実に権利侵害を生じさせた場合の救済スキーム――本人請求権、民事賠償、行政制裁――の実効性を検証する。そのうえで、従来の通知・同意に過度に依拠する枠組みを補完するため、データ・フィデューシャリー義務の明文化、リスクベース評価の制度化、集団救済メカニズムの導入といった多層的な制度再設計の必要性と具体的方向性を検討する。

４．本人請求権と救済スキーム

前節で明らかにした同意モデルが抱える三層の構造的脆弱性――① 情報非対称性の制度的温存、② 事後統制メカニズムの機能不全、③ 技術革新に対する制度追随性の限界――により、個人情報の取扱いが本人の想定を大幅に逸脱する事態が常態化している。このような状況下で、同意モデルの限界によって実質的な権利侵害が生じた場合、情報主体はいかなる救済手段を行使し得るのか。本節では、個情法が用意する三層の救済スキームの実効性を検証する。

具体的には、第一に、開示・訂正・利用停止等の本人請求権（33～35条）の実効性について、手数料負担・本人確認手続・立証責任といった行使上の障壁や対象範囲の限定性の観点から分析する。第二に、プライバシー侵

害やデータ漏えいに伴う民事賠償について、慰謝料算定の現状と集団的被害回復の制度的空白とを検討する。第三に、個人情報保護委員会による行政制裁について、執行頻度・制裁水準・抑止効果の観点から国際比較を交えて評価する。

これらの検証を通じて、現行救済スキームに内在する構造的問題を明らかにする。すなわち、費用対効果の面では情報主体にとって利用が困難であり、他方で事業者に課されるコストも、違反行為によって得られる経済的利益を相殺するほど高くはないという現行救済スキームの構造的アンバランスを描出する。そのうえで、自己情報コントロール権の法的地位の明確化、データ取扱者に対するフィデューシャリー義務の導入、集団差止め・賠償制度の創設、売上高連動型制裁金の導入といった多層的な制度補完策を検討し、データ・ライフサイクル全体を通じて実効性のある救済・抑止モデルを構築するための理論的基盤と具体的方向性を提示することが、本節の目的である。

⑴ 権利行使の実務――費用負担と立証責任・対象範囲

個情法は、「個人情報」「個人データ」「保有個人データ」を段階的に区分し、もっとも狭義の「保有個人データ」について開示・訂正・利用停止等の請求権を保障している（33～35条）。2020年（令和２年）改正では、開示方法について電磁的記録での提供を含め本人が指示できる権利が認められ（33条１項）、第三者提供記録も一定の場合を除き開示対象とされる（同条５項）など、手続面では相当の改善が図られた。しかし実務上は、依然として費用負担、立証責任、対象範囲という３つの阻害要因により、権利行使の実効性が著しく制限されている。

第一に、費用負担による行使阻害がある。個情法は開示等請求について「手数料を徴収することができる」旨を定めており（38条１項）、その水準は事業者の裁量に委ねられている[45]。個人情報保護委員会のガイドラインは「開示に多額の費用を要する場合」の配慮を求めるにとどまり[46]、実務では

事業者により手数料水準に大きな差が生じており、公的機関では数百円程度の低額な設定が多い一方、大手金融機関では数千円から１万円程度、取引内容によってはそれ以上の手数料を設定する例も見られる[47]。eKYC 等によるオンライン申請が普及し、手続きの利便性は向上しているものの、手数料や本人確認に要する実費は請求者の負担とされるため、軽微な被害や確認的な開示請求では、請求コストが便益を上回る構造的な問題が生じている。

第二に、立証責任の過重な負担が存在する。利用停止や訂正を求める際には、請求の根拠となる事実について本人が主張・立証責任を負うが（民事訴訟法179条）[48]、クラウドサービスを利用した多層的委託構造や、RTB に代表される複雑な広告システムでは、データの実際の処理状況を本人が把握することは事実上困難である[49]。個人情報保護委員会によるクラウドサービス提供事業者への注意喚起事例でも、責任の所在やデータ処理の透明性確保の困難さが指摘されており[50]、民事訴訟における因果関係の立証は「被害者救済の大きな障害」となっている[51]。さらに、不適正利用禁止規定（19条）も注意喚起のための規定として位置づけられており[52]、個人による直接的な違法性の立証には構造的限界がある。

第三に、対象範囲の制度的限定も看過できない。個人情報保護法の「個人情報」は「生存する個人に関する情報」に限定されるため（２条１項）、故人の情報は法の対象外となる。最判平成31年３月18日判時2422号31頁は、故人の情報について保有個人データ該当性を否定し、相続人による被相続人の取引履歴確認請求を認めなかった。この判断により、デジタル遺産の承継や故人の権利侵害の事後的救済において実務上の空白が生じている[53]。また、未成年者、精神障害者、意識不明患者など同意能力を欠く者について、本人に代わって権利行使を行う「代諾」制度が法定されていないことも、権利保護の間隙を拡大している[54]。

以上の検討から明らかなとおり、費用負担、立証責任、対象範囲という三重の制約が重なり、本人請求権は形式的には整備されているものの、実

質的な救済手段としては十分に機能していないのが現状である[55]。とりわけ、同意モデルの形骸化によりデータ取扱いの予見可能性が失われた現状では、事後的な権利行使による統制にも期待できず、予防的・包括的な保護メカニズムの必要性がいっそう高まっている。

⑵ 民事救済――低額慰謝料と集団救済の欠落

個人情報漏えい事件における民事救済は、慰謝料水準の低さにより十分な抑止機能を発揮していない。大量漏えい事件で認容される慰謝料は数千円から多くても数万円にとどまるのが一般的であり[56]、数百万件の個人情報が流出したベネッセ名簿大量流出事件で同様の水準にとどまった[57]。被害者個々の精神的損害を個別に評価する現在の枠組みでは、漏えい規模が数百万件に達しても、企業が負担する賠償額は回収コストや通知費用を除けば限定的であり、大規模データ保有事業者に対する行為抑止の機能は十全には働かない。

他方で、個人情報を「財産権」と構成することで救済が容易になると指摘する学説も存在する[58]。しかし現行の救済実務は、プライバシー侵害による精神的損害（慰謝料）の認定に依拠しており、その金額水準や算定基準の定型化・標準化は進んでいない[59]。その結果、大規模データ保有事業者に対する経済的インセンティブの観点からは、「賠償額より事故対応コストのほうが高い」という逆転現象すら生じ得る構造となっている[60]。

プライバシー侵害に対する民事救済については、判例法上、人格権に基づく差止請求権が認められてきた経緯がある[61]。個人情報保護法も、開示・訂正・利用停止等の本人請求権を規定し（33～35条）、個人情報取扱事業者の適正取扱義務を実効化する手段を提供している。しかし実務上は、差止請求の要件として「具体的危険」の立証が求められ、前述の住基ネット訴訟やマイナンバー訴訟においても、最高裁が具体的危険性の立証不十分として差止請求を棄却している。

さらに、プライバシー権の理解も「私生活をみだりに公開されない権利」

（古典的プライバシー権）から「自己に関する情報をコントロールする権利」（自己情報コントロール権）へと発展を遂げており[62]、憲法学説上も、情報主体による自己に関する情報の取扱い決定権を中核とする理解が定着しつつある。もっとも、マイナンバー訴訟判決は、「第三者に開示されない自由」を基礎に合憲性を判断したにとどまり、自己情報の取扱いに関する決定権を正面から基本権として認めるには至っていない[63]。したがって、現行の判例構造の下では、AI 分析やプロファイリングによる情報処理の差止請求を制度的に基礎づけることが困難な状況にある。

もっとも深刻な課題は、集団的被害回復手段の不備である。消費者裁判手続特例法は、消費者契約に関する財産的損害の集団的回復を想定しており、プライバシー侵害やデータ漏えいに典型的な非財産的損害（精神的損害）を直接の対象としていない（同法３条）。これに対し、フランスの集団訴訟制度はプライバシー侵害に伴う精神的損害の賠償も対象とし、米国のクラスアクションと同様の包括的救済を可能としている[64]。

日本では、このような包括的集団救済制度を欠くため、低額かつ個別の慰謝料請求が散発的に提起されるにとどまり、多数被害者の権利回復と事業者に対する経済的制裁を同時に実現する仕組みが存在しない。その結果、大規模個人情報侵害が発生しても、被害者の大部分は訴訟提起を断念し、事業者の違法行為に対する実効的抑止力は著しく制限されている。

⑶　行政救済・制裁――実効性の限界

2020年（令和２年）改正では、民事救済の限界を補完するため、個人情報保護委員会の監督権限が大幅に強化された。命令違反や不正提供等に関して、法人に対する罰金の上限は１億円に引き上げられ（184条１項１号）、外国事業者に対する域外適用も明文化された（183条）。また、個人データの漏えい等については、委員会への報告義務および本人通知義務が新設され（26条）、GDPR の72時間以内報告義務を参考とした制度整備が図られた[65]。

さらに2021年（令和３年）改正では、国の行政機関、独立行政法人、地方

公共団体の個人情報保護制度が一本化され、委員会が公的部門も一元的に所管することとなった。これらの改正は、EU からの「十分性認定」維持と国際的ハーモナイゼーションを企図したものである[66]。

しかし、制裁水準の国際比較では依然として大きな格差が存在する。GDPR では、違反に対し前会計年度の全世界年間売上高 4 %または2,000万ユーロ（約27億円）のいずれか高いほうが制裁金として課され得るのに対し（83条）、日本の 1 億円という上限は「甘い、安すぎる」との批判があり、法制度の違いを超えた「文化の差」「行政手法の差」とも指摘されている[67]。

具体的な執行状況をみると、個人情報保護委員会による命令・勧告等の件数は年間数十件規模にとどまっており[68]、国内で流通する個人データの規模と比較すると執行密度は極めて低い。象徴的事例であるリクナビ内定辞退率事件では、委員会が是正勧告を行い[69]、同事件は2020年（令和 2 年）改正で「個人関連情報」概念が新設される契機となったが、依然として事後的対応の域を出ていない。

さらに深刻な問題は、「個人の権利利益を害するおそれが大きいもの」という漏えい報告要件の曖昧性である。報告義務が「非常に重く、かつ、実行の意義がよく分からない義務」となり、適切な対応を行う事業者が相対的に不利になる構造的問題が指摘されている[70]。名簿販売や Cookie 流用のような濫用的事例についても、実務上「制裁の対象件数、制裁までの時間とその制裁の内容から見ると、個人データの保護に対する影響力が実務上、殆どない」との指摘があり[71]、執行の迅速性確保が国際的課題であることを示している。

⑷ 制度改革への示唆――救済・抑止力の多層化

前項までの検討により、現行の本人請求権・民事救済・行政制裁という救済システムには、いずれも構造的限界が存在することが明らかとなった。とりわけ深刻な問題は、これらの救済手段がすべて事後的・対症療法的性格を有することである。同意モデルの形骸化により、データ取扱いの予見

可能性と事前統制が失われた現状では、権利侵害が発生してから対処する事後的救済に依拠する従来の枠組み自体の限界が露呈している。権利侵害の発生を未然に防ぐ予防的・包括的なメカニズムが必要である。

このような現状認識を踏まえると、従来の通知・同意モデルと事後的救済に過度に依拠する枠組みから脱却し、(1) 事前のリスク評価義務、(2) 継続的な監査・モニタリング、(3) 技術的保護措置の標準化、(4) 集団的救済手段の整備といった予防的・包括的な保護メカニズムを多層的に構築する制度再設計が急務である。

重要なのは、日本の個人情報保護法制が培ってきた柔軟性とソフトロー型ガバナンスという制度的強みを活かしつつ、権利保護の実効性を格段に向上させる「ハイブリッド型」の制度設計への転換である。これにより、技術革新への俊敏な追随性と個人の権利保護を両立させることが可能となる。

(5) 小　　括

本節の検討から浮かび上がったのは、① 本人請求権には手数料・立証負担・対象範囲といった高い行使コストが掛かり、被害の小さい事案では行使自体が割に合わないこと、② 民事訴訟による慰謝料は一人当たり数千円程度にとどまり集団救済の制度的手当ても欠如しているため、大規模侵害でも企業の経済的負担は限定的であること、③ 個人情報保護委員会による命令・勧告件数が年間数十件規模にすぎず、罰金上限も１億円（GDPR の最大制裁金である売上高４％または2,000万ユーロと比較して大幅に低い水準）にとどまるなど行政執行の密度と制裁水準が抑止力として十分ではないこと、という三重の限界である。

言い換えれば、同意モデルの形骸化によって侵害リスクが増大しても、これら三つの救済手段はいずれも個人の権利保護と事業者への抑止力の両面で機能不全に陥っている。この状況は、前項で指摘した事後的・対症療法的救済の限界と相まって、個人情報保護制度全体の実効性を根本から損なっている。

最終節では、このような救済・抑止手段の脆弱性を踏まえつつ、わが国の個人情報保護法制が培ってきた理念と運用特性を歴史的観点から再点検し、その強みと課題を体系的に分析する。この分析を基礎として、GDPR や米国 ADPPA 草案との比較を通じて制度ギャップを浮き彫りにし、日本型モデルの柔軟性という制度的優位を活かしながら、同意モデルの限界を克服し救済・抑止の実効性を向上させる制度再設計の方向性を提示する。

5．日本型モデルの強みと課題

本節では、これまでの検討で浮き彫りとなった「同意モデルの形骸化」と「救済・抑止手段の脆弱性」を踏まえつつ、わが国の個人情報保護法制がどのような制度理念と運用特性を備えてきたのかを再点検し、その強みと課題を対照させる。

具体的には、まず、行政指導主義から法執行主義、さらには「権利保護とデータ利活用の調和」を掲げる現行フェーズへと至る歴史的展開を概観する。そのうえで、匿名加工情報と仮名加工情報によるリスク層別モデル、ガイドライン・FAQ に代表されるソフトロー型ガバナンス、全国一元ルール化によるコンプライアンス負担の軽減といった柔軟性を強みとして位置づける。他方で、包括同意の温存、慰謝料・制裁金の低水準、集団救済制度の欠落、AI 高リスク処理に対するリスクベース原則の未成熟といった権利救済と抑止力の脆弱性を課題として整理し、国際的な制度動向との比較の必要性を確認する。この作業により、次章以降で検討する GDPR や米国 ADPPA 草案との制度比較と、日本型ハイブリッドモデルの制度再設計に向けた理論的基盤を提供することが、本節の目的である。

⑴ 歴史的展開と制度的特色

日本の個人情報保護法制は三つの段階を経て現在の姿に至っている[72)]。第

一段階に当たる2003年制定法は、通知・同意を中心とする実体規律を掲げつつ、違反時の是正手段を「主務大臣による指導・助言」に委ねる行政指導主義を採用した[73]。第二段階の2015年改正では、個人情報保護委員会が独立規制機関として創設され、報告徴収・立入検査・命令の権限を付与することで法執行主義へと舵を切り、さらに匿名加工情報制度を導入してデータ利活用の道を開いた[74]。第三段階に移行した2020年改正は、仮名加工情報や漏えい報告義務、法人罰金上限の引上げといったリスクベース規定を整備すると同時に、「権利保護とデータ利活用の調和」を明確な政策目標として位置づけ、行政ガイドラインやFAQなどソフトローを組み合わせた協調的ガバナンスを制度的特徴とした[75]。

このような変遷は、人格的権利の優先を貫く欧州GDPR型や、市場規律と州法パッチワークを前提とした米国型とは対照的である[76]。日本型モデルの独自性は、強制執行と行政指導、ハードローとソフトローを段階的に組み替えながら、法的安定性と技術革新への追随性のバランスを取る点にあるといえる。

⑵　強　　み――柔軟性と協調的ガバナンス

日本型モデルが備える最大の強みは、法的拘束力の異なる複数レイヤーを組み合わせることで、規制の安定性と技術革新への追随性を両立している点にある[77]。まず注目すべきは、2015年改正で創設された匿名加工情報と、2020年改正で追加された仮名加工情報という二層構造のデータカテゴリーである[78]。前者は個人識別性を事実上消滅させたデータとして外部提供を解禁し、後者は社内利用に限って目的変更を許容する[79]という区分により、データのリスクに応じて本人同意の要否を段階的に調整しつつ、企業内部でのAIモデル学習や統計分析を制度的に後押しした。

さらに、日本の個人情報保護委員会は、法律の想定を補完するかたちでガイドライン・FAQ・Q&Aを随時更新し、事業者ヒアリングを通じて現場の運用課題を吸い上げるソフトロー型ガバナンスを定着させている[80]。法

改正に数年を要する欧州や米国と比べ、新技術への対応を数か月単位でアップデートできる俊敏性は、日本型モデルが柔軟性を確保する実務的要因となっている[81]。

加えて、2021年改正で行政機関・独立行政法人・地方公共団体の個人情報法制を一本化した結果、民間部門と公共部門の境界で発生していたデータ連携の手続差や定義差が解消され、事業者は全国一元ルールでサービスを展開できる環境が整った[82]。これにより、複数の法源を読み替えるコンプライアンス負担が軽減し、事業者はリソースをデータ活用やセキュリティ投資に振り向けやすくなった。

以上のように、リスク層別データ区分、ソフトロー型ガバナンス、法体系の一元化が相乗的に作用し、日本型モデルは「変更の早さ」と「制度の一貫性」を同時に実現している点で独自の競争優位を有している。

⑶ 課　　題――権利救済と抑止力の脆弱性

もっとも、日本型モデルには二つの構造的弱点が残る。第一は、権利救済の脆弱さである。個人データの取扱いを是認する主たる根拠をいまなお本人同意に置く一方（個情法16条、17条参照）、その同意は「サービス改善」「マーケティング全般」といった包括的文言で取得されることが多く、利用者は実際のデータフローを把握できないままリスクだけを負わされる[83]。個人情報保護法上の同意要件には GDPR のような「任意性、特定性、事情を知らされたうえでの同意、明確性」の 4 要素が明示されておらず、他に特別な規定もないため、同意を通じて何が求められているかが不明確である[84]。さらに、利用者が一度同意すると、同意撤回権が法定されていないため、データフローの把握困難な状況が継続する[85]。加えて、前節で検討したとおり、民事救済も低額慰謝料と集団救済の欠落により機能不全に陥っている。

第二は、抑止力の不足である。法人罰金の上限は2020年改正で 1 億円に引き上げられたが、それでも GDPR が科し得る最大2,000万ユーロまたは前

会計年度の世界売上高４％のいずれか高いほうという制裁金（GDPR 第83条５項）に比較して大幅に低い水準にある。委員会による命令・勧告件数についても年間十数件規模にとどまり、継続的モニタリングや迅速執行の体制は十分とはいいがたい[86]。とりわけ AI プロファイリングやリアルタイム入札（RTB）のように高リスクかつ複雑な処理については、日本の個情法にはプロファイリングに関する基本的規定がなく、正当化事由や追加的保護措置をリスクに応じて段階的に設定するリスクベース原則が未成熟であり、違反を事前に抑止する歯止めは弱い。

この救済と抑止の双方の脆弱性は、同意モデルの形骸化と相まって、利用者の権利保護と企業の法令順守インセンティブを同時に損なう要因となっている。

⑷　制度的課題の国際的文脈

前節までの検討により、日本の個人情報保護法制は、(i)利用目的中心主義への依存度が高く体系的リスク評価が後追いであること、(ii)忠実義務型の行為規範が未整備であること、(iii)行政制裁金・集団救済の水準が国際的に低いこと、という構造的課題を抱えることが明らかとなった。

これらの課題に対する解決の方向性を明確にするためには、同様の課題に直面する国際社会がどのような制度的対応を図っているかを検討する必要がある。とりわけ、同意モデルの限界を克服する多層的アプローチを展開する EU の GDPR と、データ受託者に包括的忠実義務を課すことで従来の通知・同意の枠を超えた保護を実現しようとする米国の ADPPA 草案は、日本の制度再設計にとって重要な示唆を提供すると考えられる。

⑸　小　　括――比較法的検討への展望

以上の検討により、日本型モデルは柔軟性と協調的ガバナンスという独自の強みを有する一方で、権利救済と抑止力の脆弱性という構造的弱点を抱えることが確認された。この強みを活かしつつ弱点を克服する制度再設

計の具体的方向性を見出すためには、国際的な制度動向との詳細な比較検討が不可欠である。

次章では、GDPR および ADPPA 草案の制度理念・具体的仕組み・運用実態を詳細に分析し、日本法との制度比較を通じて、同意モデルの限界を克服し救済・抑止の実効性を向上させる制度改革の理論的基盤と具体的方向性を導出する。

1） 拙稿「個人情報保護の私法的基礎に関する序論的考察（1）――財産権と人格権の交錯する領域における理論的課題」立命館法学409号（2023年）474-475頁参照。

2） 岡村久道『個人情報保護法〔第 4 版〕』（商事法務、2022年）210-212頁、石井夏生利＝曽我部真裕＝森亮二『個人情報保護法コンメンタール』（勁草書房、2021年）147-149頁、152-154頁参照。

3） 岡村・前掲注（2）211-212頁はこの現象を制度趣旨に反する運用と捉え、リクナビ事件およびベネッセ名簿大量流出事件は、抽象掲示が逆転現象を招いた実例として位置づけられる。

4） 本件では原告（控訴人）と被告（被控訴人）の双方が上告・上告受理申立てを行ったため、2 つの上告審決定（令和 2 年(オ)第1097号〔LEX/DB 文献番号25590464〕と令和 2 年(オ)第1098号〔LEX/DB 文献番号25590463〕）がある。

5） 個人情報保護委員会「個人情報の保護に関する法律に基づく行政上の対応について」（令和元年12月 4 日）〈https://www.ppc.go.jp/files/pdf/191204_houdou.pdf〉

6） 総務省総合通信基盤局長・総務省サイバーセキュリティ統括官「社内システムに関する安全管理措置等及び利用者への適切な説明について（指導）」（令和 3 年 4 月26日）〈https://www.soumu.go.jp/main_content/000747402.pdf〉

7） 個情法18条参照。

8） 銀行と預金者の間の守秘義務違反による債務不履行（東京地判平成 3 年 3 月28日判時1382号98頁）、システム開発・保守委託契約におけるセキュリティ対策義務違反による債務不履行（東京地判平成26年 1 月23日判時2221号71頁）、退職時誓約書に基づく顧客情報利用制限義務違反による債務不履行（大阪地判平成30年 3 月 5 日 LEX/DB 文献番号25449512）など。これらの事例では、契約に明示されていない場合でも契約の性質や当時の技術水準から情報管理に関する付随義務が認定されたり、明示された契約内容の解釈を通じてその義務の範囲が確定されたりして、その違反が問題となっている。

9） 個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』に関するQ&A」（令和 7 年 6 月17日更新）Q3-1は、個人情報保護法19条の「違法又は不当な行為」を「個人情報保護法その他の法令の制度趣旨又は公序良俗に反する等、社会通念上適正とは認められない行為」と定義する。また、同 Q4-3は、相手方が不正の手段で個人情報を取得したことを「知り又は容易に知ることができたにもかかわらず当該個人情報を取得する

こと」は法20条１項に違反するおそれがあると解している。さらに、同法179条は個人情報データベース等の不正提供・盗用を刑事罰の対象としており、これらを総合すると、違法流出名簿の売買は社会通念上適正とは認められない行為として公序良俗違反を構成する余地がある。

10） 東京地判昭和59年10月30日判時1137号29頁。同判決は、個人情報が不適正に扱われている場合の消去請求権について人格権を根拠とする先駆的判断を示した。

11） 大阪高判平成13年12月25日判例地方自治265号11頁。

12） 山本龍彦「医学研究領域における医療情報の保護と利活用について」ジュリスト1534号（2019年）38頁以下、とくに39頁参照。

13） 米村滋人「個人情報の取得・第三者提供に関する『同意』の私法的性質」廣瀬久和先生古稀記念『人間の尊厳と法の役割』（信山社、2018年）321頁以下、とくに327頁参照。

14） 個情法20条２項。同項は、要配慮個人情報の取得について、法令に基づく場合（１号）、生命・身体・財産保護のために必要で同意取得が困難な場合（２号）、公衆衛生の向上又は児童の健全な育成の推進のために特に必要で同意取得が困難な場合（３号）など、複数の例外事由を定めている。

15） GDPR における包括的利用目的の実務動向については、石井＝曽我部＝森・前掲注（2）203頁参照。また、ルブルトン・カロリーヌ・マリ・ディアーヌ「潜在的多数被害者の観点から見たフランスの個人情報保護制度」法学志林120巻４号（2023年）85頁は、GDPR においても「白紙の同意は許されず」、特定の同意が要求されることを指摘している。

16） 福岡真之介ほか編『AI プロファイリングの法律問題――AI 時代の個人情報・プライバシー』（商事法務、2023年）参照。また、寺田麻佑「アフターコロナ時代の個人情報の利活用と保護」法学セミナー787号（2020年）76頁以下は、リクナビ問題を例に、「提供元では個人データに該当しないものの、提供先において個人データになることが明らかな情報」の本人同意なき提供問題を分析し、AI プロファイリングによる内定辞退率算出の構造的課題を指摘する。

17） 個人情報保護委員会・前掲注（5）引用文献。

18） 石井夏生利『個人情報保護法の現在と未来』（勁草書房、2021年）65頁、宇賀克也『新・個人情報保護法の逐条解説』（有斐閣、2021年）197頁以下参照。GDPR との比較法的観点から日本法の構造的問題を詳細に分析したものとして、小林和馬「GDPR に見る日本における個人情報取り扱いとその政策課題」中央学院大学商経論叢37巻１号（2022年）17-22頁も参照。同論文では、日本の個人情報保護法が「基本的人権であることの前提」（19頁）を欠くことにより、同意の撤回権の不存在、適法性要件の限定的適用（第17条の取得時のみ）、損害賠償基準の不明確性などの構造的欠陥が生じていることを指摘し、「どのような社会にするのか政策的議論を深める必要がある」（20頁）と論じている。

19） 個人情報保護委員会「個人情報保護法令和２年改正及び令和３年改正案について」参照。

20） 個情法26条の２（個人関連情報の第三者提供制限）参照。

21） リクナビ事件等を背景とした2020年（令和２年）改正個人情報保護法では、オプトアウトによる第三者提供について、要配慮個人情報の提供禁止、不正取得データ・他事業者からのオプトアウト提供データの再提供禁止等の規制強化が図られた（個人情報保護法27条２項・５項）。藤原静雄＝宍戸常寿「2020年個人情報保護法改正の背景と今後」ジュリスト

1551号（2020年）18-19頁、弁護士法人 One Asia 他「いまだから知っておきたい、2020年改正個人情報保護法」季刊事業構想2022年春号118頁参照。

22） 個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国は、EU 及び英国が該当する。個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（令和７年４月一部改正）３頁。なお、EU 及び英国の指定は、日 EU 間で相互の円滑な個人データ移転を図るために、欧州委員会による日本への十分性認定（GDPR 第45条に基づき、欧州委員会が、国又は地域等を個人データについて十分な保護水準を確保していると認める決定をいう。）に併せて行ったものである。

23） 個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制の基準については、規則第16条に規定されている。同基準の具体例として、提供元及び提供先間の契約、確認書、覚書等が挙げられており、これらは GDPR の標準契約条項（SCC）や拘束的企業準則（BCR）に相当する契約措置である。個人情報保護委員会・前掲注（22）14頁。

24） GDPR 第４条11号。個人情報保護法27条１項は同意の要件を定めるのみであるのに対し、GDPR は同意の有効要件として自由性・特定性・十分な情報提供・明確性の４要素を明示している。

25） 石井・前掲注（18）61頁以下参照。

26） Harry Brignull, “Dark Patterns: Inside the Interfaces Designed to Trick You,” The Verge (Aug. 29, 2013).

27） 個人情報保護委員会・前掲注（22）33頁。

28） European Data Protection Board, “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data” (June 18, 2021).

29） 個情法25条。

30） OpenAI, “How your data is used to improve model performance” https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance (last visited June. 2025). なお、具体的な保持期間や処理方法は変更される可能性がある。

31） GDPR 第25条（データ保護バイデザインおよびバイデフォルト）。Ann Cavoukian, “Privacy by Design: The 7 Foundational Principles” (2009). 同原則は、プライバシー保護を事後的対応ではなく、システム設計の初期段階から組み込むことを求める。

32） 個情法31条１項。同条にいう「個人関連情報」の定義は２条７項で規定されている。

33） 個人情報保護委員会・前掲注（9）Q3-6-1参照。

34） 個人情報保護委員会・前掲注（5）。

35） IAB Tech Lab, “Open RTB API Specification Version 2.5” (Dec. 2016). なお、その後も仕様は更新されているが、基本的なオークション構造は同様である。

36） 寺田・前掲注（16）78-80頁参照。

37） Shoshana Zuboff, “The Age of Surveillance Capitalism” (PublicAffairs, 2019), pp.76-97; 山本龍彦『プライバシーの権利を考える』（信山社、2017年）203-225頁。

38） IAB Europe, “Transparency & Consent Framework v2.0” https://iabeurope.eu/tcf-2-0/

(last visited Dec. 2024).

39） Brignull, supra note 26.

40） GDPR 第４条11号。詳細は Article 29 Working Party, “Guidelines on consent under Regulation 2016/679” (WP259 rev.01, Apr. 10, 2018) 参照。

41） European Data Protection Board, “Guidelines 05/2020 on consent under Regulation 2016/679” (May 4, 2020), paras. 42-51.

42） 山本龍彦「ビッグデータ社会とプロファイリング」論究ジュリスト18号（2016年）35-38頁。

43） 曽我部真裕「個人情報保護と医療・医学研究」論究ジュリスト24号（2018年）111-114頁。

44） Ann Cavoukian, “Privacy by Design: The 7 Foundational Principles” (2009); GDPR 第25条（データ保護バイデザイン及びバイデフォルト）参照。

45） 個人情報保護委員会・前掲注（9）Q9-27は、開示等の手数料について「手数料の額は、実費を予測して平均的単価を算出して定めることが望ましい」とし、「業種や保有個人データの種類を勘案する必要があるため、統一的な相場を示すことは困難」と述べる。また、Q9-29は手数料が「実費を勘案して合理的であると認められる範囲内で定めなければならない」としつつも、具体的な上限額や算定基準は示していない。

46） 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」（令和７年４月一部改正）134頁。同ガイドラインは、本人が請求した開示方法について「当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法」により開示すればよいとし、費用負担への配慮を示している。

47） たとえば、三菱 UFJ 銀行では、基本情報の開示で1,320円、預金・投資信託・債券残高情報や貸付け・ローン残高情報の開示で7,370円、取引推移表５年分では26,400円の手数料を設定している（三菱 UFJ 銀行「個人情報開示等の請求に関する手続について」〈https://www.bk.mufg.jp/kojinjouhou/kaiji.html〉2025年６月30日最終閲覧）。一方、公的機関では日本政策金融公庫や独立行政法人情報処理推進機構が300円という低額な設定をしており（日本政策金融公庫「手数料」〈https://www.jfc.go.jp/n/publicinfo/p_fee.html〉、独立行政法人情報処理推進機構「個人情報に関する開示請求」〈https://www.ipa.go.jp/privacy/seikyu.html〉いずれも2025年６月30日最終閲覧）、事業者の規模や性質により手数料水準に大きな差が生じている。

48） 個情法18～20条違反や権利侵害のおそれの立証が必要。

49） 寺田・前掲注（16）203-210頁参照。

50） 個人情報保護委員会「クラウドサービス等を利用した個人データの取扱いについて」（令和４年７月）。

51） 神作裕之「判批」別冊ジュリスト249号（2019号）７頁以下。

52） 岡村・前掲注（2）233-236頁。

53） たとえば、故人の取引履歴を確認できないなど、情報承継に支障が生じる。

54） 米村・前掲注（13）334-338頁。

55） 菅原貴与志「改正個人情報保護法の課題――企業法務の視点から」慶應法学34号（2016年）42頁以下。開示請求権の発生要件が不明確であることや、認容判決後の執行手続が規定されていないため実効性に疑義が残ることを指摘する。

56） 升田純『現代社会におけるプライバシーの判例と法理――個人情報保護型のプライバシーの登場と展開』（青林書院、2009年）393頁は、京都府宇治市住民票データ流出事件で 1 人当たり 1 万円の慰謝料が認容された事例につき、金額の妥当性に疑問を呈している。始澤真純「個人情報の保護と利用」現代社会研究19号（2022年）143頁も参照。

57） 前掲東京地判平成30年12月27日、前掲東京高判令和 2 年 3 月25日等。具体的金額は事案により異なるが、一人当たり数千円程度の認定が多い。

58） 始澤真純「個人情報の保護の法的根拠――個人情報の財産権的価値についての考察」東洋大学大学院紀要58号（2022年）84頁以下は、個人情報を財産権として位置付けることで違法性認定や損害算定が容易となり、被害者救済の実効性が高まると指摘する一方、賠償額の低額化などの課題も指摘する参照。朱曄「民事法の視点から見たスマートシティ実現に向けての課題解決――AI 技術の進化による『市民データ権』の誕生」静岡法務雑誌12号（2021年）199頁以下は、個人情報を集合財産権として把握し、侵害者に不当利得の吐き出しまで求める高額賠償モデルを提示する。

59） 高松志直「個人情報漏えい事件最高裁判決の今後の展開と実務への影響」NBL 1109号（2017年）24頁は、精神的損害（慰謝料）の額は「漏えいした個人情報の内容、漏えいの態様、漏えい後の個人情報取扱事業者の対応等を勘案して」個別具体的に認定されると述べ、画一的な算定基準が確立していない現状を指摘する。小林直三「個人情報漏洩に関する損害の認定と算定のあり方に関する一考察」大阪経大論集76巻 1 号（2025年）28頁以下も、「現在の個人情報漏洩に伴う損害賠償額は必ずしも高額ではなく、その算定方法も十分に反映されていない」として、慰謝料水準の低さと算定基準未整備を問題視する。

60） JNSA「インシデント損害額調査レポート〔第 2 版〕」（2024年）によれば、事故対応費だけで DM1万人発送130万円、コールセンター 3 か月700～1,000万円、プリペイド見舞金650万円など、中小企業規模でも数千万円～数億円規模の費用負担が生じ得るとされる〈https://www.jnsa.org/result/incidentdamage/data/2024-1.pdf〉（2025年 6 月30日最終閲覧）

61） 東京地判昭和39年 9 月28日判時385号12頁（「宴のあと」事件）、最判平成14年 9 月24日判時1802号60頁（「石に泳ぐ魚」事件）等。

62） 山本・前掲注（37）44-45頁参照。従来の自己決定・同意モデルの限界を踏まえ、多元的・文脈依存的プライバシー論が提唱されている。

63） 音無知展「マイナンバー制度の合憲性」ジュリスト1597号（2024年）22-23頁。

64） ルブルトン・前掲注（15）94頁。

65） 個人情報保護委員会・前掲注（46）参照。

66） 個人情報保護委員会『令和 3 年度 年次報告』 9 頁。

67） 藤原靜雄「日本と EU の個人情報保護法制の比較」ジュリスト1521号（2018年）14頁。制裁金格差を「文化の差」「行政手法の差」として分析している。

68） 個人情報保護委員会『令和 5 年度 年次報告』（2024年）76-77頁。

69） 個人情報保護委員会「リクルートキャリア株式会社に対する勧告について」（2019年12月 4 日公表）。

70） 湯淺墾道ほか「〈座談会〉個人情報保護法からみたサイバーセキュリティ」ジュリスト1599号（2025年）14以下における寺門発言および蔦発言参照。

71） ルブルトン・前掲注（15）102頁は、「集団訴訟形式以外の CNIL に対する被害届の提出について、制裁の対象件数、制裁までの時間とその制裁の内容から見ると、個人データの保護に対する影響力が実務上、殆どないことは否定できない」と指摘している。

72） 藤原靜雄＝宍戸常寿「2020年個人情報保護法改正の背景と今後」ジュリスト1551号（2020年）14-29頁。

73） 鈴木正朝「個人情報保護法制における1988年法から2003年法への転換の意義」情報法制レポート５号（2024年）26-37頁。

74） 藤原＝宍戸・前掲注（76）16-17頁。

75） 藤原＝宍戸・前掲注（76）18-21頁。

76） 藤原靜雄「日本と EU の個人情報保護法制の比較」ジュリスト1521号（2018年）21-22頁。

77） 藤原＝宍戸・前掲注（76）25頁は、個情法の条文が規範的かつ抽象的であることを踏まえ、「本人の権利又は正当な利益が害されるおそれ」（35条５項）などの要件について、ガイドラインや Q&A によって明確化を図る必要があると指摘し、ガイドラインや Q&A が、法律の補完手段として、具体的な運用指針を提示する重要な役割を果たしていることを示す。

78） 匿名加工情報（個情法43条以下）、仮名加工情報（同41条以下）。

79） 仮名加工情報は法令で定める場合を除き第三者提供が禁止され（42条１項）、主に社内利用が想定される。個人情報保護委員会「仮名加工情報・匿名加工情報の適正な加工の方法等に関するガイドライン」（令和４年４月）参照。

80） 藤原＝宍戸・前掲注（76）頁25頁は、法律の抽象的な規定について、「ガイドラインや Q&A で明確化する際に消費者・事業者双方の意見を聴く」ことの重要性を強調している。なお、個人情報保護委員会のガイドライン・Q&A 体系については、同委員会ウェブサイト https://www.ppc.go.jp/ 参照。

81） 個人情報保護委員会「生成 AI サービスの利用に関する注意喚起等について」（令和５年６月２日）。

82） 慎祥揆「個人情報の保護に関する法律とビッグデータのための非識別化技術」東海大学紀要情報理工学部第23巻（2023年）1-9頁、とくに５頁参照。

83） たとえば、武田俊之「大学の授業と著作権・個人情報保護」関西学院大学高等教育研究13号（2023年）123-138頁。本人の知らないところで作成されたプロファイルに誤情報やバイアスが含まれていても、本人が訂正する手段がないというリスクを指摘する（134頁）。

84） GDPR 第４条11号の同意要件（自由性・特定性・十分な情報提供・明確性）と対照的である。

85） GDPR は同意撤回権を明文で保障する（７条３項）が、日本の個情法には対応する規定がない。

86） 個人情報保護委員会による体制強化の取組みについては、同委員会・前掲注（67）27頁参照。