JILISレポート
論文 Date: 2025.03.28
https://jilis.org/report/2025/jilisreport-vol7no5.pdf

個人情報保護法の論点

情報法制研究所上席研究員
弁護士・情報処理安全確保支援士
那須　翔

はじめに

令和5年9月から始まった個人情報保護法（**「個情法」**、**「法」**、**「平成15年法」**、**「日本法」**）の3年ごと見直し（**「本見直し」**）は、制度の基本的な在り方をも対象とする大掛かりなものとなっている。本稿は、本見直しで提起された論点及び今後論点となりうる事項について、議論を整理した上で検討を加え、今後の議論のための理論的基礎を提供することを試みるものである[1)]。

なお、本稿は、筆者の個人的見解であり、筆者が所属し又は過去に所属していた組織とは無関係であることをお断りしておく。

1. 保護法益

本見直しにおいては、その前提として、個情法の保護法益が論点とされている。個人情報保護委員会（**「個情委」**、**「委員会」**）は、考えられる保護法益として、①個人の評価・選別に関連するリスク、②個人に対し勧誘その他の働きかけを行うことのリスク、③秘匿したい情報他人に知られるリスク、④自身のデータを制御できないことそれ自体によるリスクを例示している[2)]。また、事務局ヒアリングでは、⑤意思決定の自律性とも言うべき利益が議論されている[3)]。

①は、高木浩光が、個人情報保護の真の目的と指摘してきたものである[4)]。昭和63年法制定時、同法の目的は、(a)個人の秘密が公開されないこと、(b)誤った情報や不完全な情報により誤った判断がなされないこと、(c)自己の情報を知ることと説明されており[5)]、①は(b)に相当する。現行法においても、例えば、正確性確保は、①を保護するものである。プロファイリングは、①が問題となる典型的場面である。個情委は、評価・決定の適切性の利益に着目して、非決定利用[6)]を目的とする場合の第三者提供制限の緩和を提案しているが、このことは、翻って、評価・決定について監督を強化する必要性をも基礎付ける。EUではAI法がGDPRを補っているが[7)]、日本では包括的なAI規制は検討されておらず、AIの個人に対する適用は、個情法が担う必要がある。

②は、名簿に関連するリスクであり、本人以外（典型的には名簿業者）から連絡先等を取得した事業者による不招請勧誘、闇名簿を利用した犯罪[8)]、名簿業者が個人情報の不正な持出しを助長すること[9)]などが含まれる。昭和63年法においては、行政事務処理用統一コードの検討やOECDガイドラインなどを背景と

1）本見直しの解説としては、金融法務事情2252号の特集「個人情報保護法の課題と3年ごとの見直し」がある。
2）個情委「個人情報保護法のいわゆる3年ごと見直しの検討の充実に向けた視点」（令和6年10月16日）4頁、8頁（**「視点」**）。
3）事務局ヒア（令和6年12月3日）8頁、20頁〔森亮二、山本龍彦〕（令和6年11月～12月に行われた事務局ヒアリングの議事概要をこのように引用する。）。
4）高木浩光「個人情報保護から個人データ保護へ(9)―法目的に基づく制度見直しの検討」情報法制研究16号97頁（2024）（**「高木連載⑨」**）、高木浩光「個人情報保護から個人データ保護へ(6)―法目的に基づく制度見直しの検討」情報法制研究12号71頁（2022）（**「高木連載⑥」**）。
5）総務庁行政管理局監修『逐条解説個人情報保護法 新訂版』41頁（第一法規、1991）（**「昭和63年逐条」**）。
6）GDPR recital 162、高木浩光「医療データ二次利用の基本的考え方～仮名加工医療データの統制された非選別利用に向けた立法論」情報法制レポート4号36頁（2023）。
7）EUにおけるGDPRとAI法の補完関係について、第279回委員会（令和6年4月3日）1頁～7頁〔生貝直人〕（合議体としての個情委の議事録をこのように引用する。）。
8）犯罪対策閣僚会議の令和5年～令和6年の各文書を参照。
9）ベネッセ事件、NTTマーケティングアクトProCX事件がこれに該当する。

して、①が問題とされた[10]のに対し、平成15年法の背景にあったのは、情報漏洩と名簿の問題であり[11]、②こそが主たる関心事であった[12]。日本法が第三者提供を厳格に制限してきたのも、名簿業者の活動に事実上の制約を課す狙いがあったものと思われる[13]。なお、EU法のダイレクトマーケティング規制と比較したとき、日本では、不招請勧誘自体は、勧誘の方法や対象となる取引に着目した個別的な規制が志向されてきたこと[14]、日本法の名簿業者規制にはより組織犯罪対策的な側面があることに留意すべきである。

③は、私法上の、伝統的な意味でのプライバシーである[15]。第三者提供制限や安全管理措置はこれに関連するが、この意味でのプライバシーには、要保護性（秘匿性）が要求される一方、その保護が必要な場面は、個人データの「取扱い」に限られないことに留意すべきである。

④は自己情報コントロール権であるが、専門家間では、コントロールそれ自体が保護法益なのではないとする意見が有力である[16]。一方で、近時の自己情報コントロール権説の代表的論者である山本龍彦が指摘してきた監視社会リスク[17]は、評価・決定の適切性との関係でも重要であり、立案・監督にあたって参照されるべきである[18]。

⑤は、個人の脆弱性の悪用[19]に関する。脆弱性の悪用は、（ダークパターンがそうであるように）必ずしも個人情報の「取扱い」によって行われるわけではないが、特定の脆弱な状態（属性）を推論し、当該属性を有する者を「狙い撃ち」して働きかけを行うことを、個情法で規制することは考えられる[20]。

各保護法益間の関係について、高木は、個情法の規制対象は①によって画定されるべきことを主張する[21]。後述のとおり、個情委も同様の方向性と考えられるが、このことは、保護法益間の優劣とは別問題であると思われる。後者の問題は、石井夏生利や曽我部真裕の指摘するように、具体的な場面に応じて論じるほかない[22]。

個別の規定を検討するに当たっては、以上の保護法益のいずれが問題となるのか、当該保護法益が具体的にどのような態様で害されること（セオリーオブハーム）に対処しようとするのかを検討する必要がある。

2. 個人情報・個人データ概念

本見直しでは、個人情報・個人データ概念は、「今後に向けて考慮していくべき点」とされているが[23]、具体的な論点として、①識別性、②散在情報の規制、③体系的構成要件が考えられる。

(1) 識別性―「特定の」個人に意味はある（べき）か？

個人情報の定義中、「特定の個人を識別することができる」とは、「社会通念上、一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認めるに至ることができること」をいうとされ、Cookie IDを含む一般的なIDは、単体では、これを満たさないとされる[24]。ここでは、「具体的な人物」に、単なる識別（single outないしdistinguish[25]）を超

10）昭和63年逐条22頁。

11）園部逸夫＝藤原靜雄編著『個人情報保護法の解説 第三次改訂版』14頁（ぎょうせい、2022）（**「園部藤原」**）、藤原靜雄『逐条 個人情報保護法』7頁（弘文堂、2003）、吉田正彦「個人情報保護法制定の経緯と制定時における基本的考え方」西村あさひ法律事務所編『個人情報保護法制大全』9頁（商事法務、2020）。

12）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―現行法（2021年法）3年ごと見直しへの示唆」情報法制レポート5号26頁（2024）。

13）松本亮孝「共同利用」NBL 1260号90頁注4（2024）〔曽我部真裕〕がいう「明示されていない理由」とは、このようなものではないか。

14）事務局ヒア（令和6年11月22日）10頁〔曽我部真裕〕、事務局ヒア（令和6年12月4日）11頁〔宍戸常寿〕も参照。なお、個情法35条2項に関する立案担当者の解釈（佐脇紀代志編著『一問一答 令和2年改正個人情報保護法』83頁（商事法務、2021）（「令和2年一問一答」）には、私生活の平穏に関する判例（最判平成元年12月21日民集43巻12号2252頁）に照らして疑義がある。

15）東京地判昭和39年9月28日下民集15巻9号2318頁、最判昭和56年4月14日民集35巻3号620頁、最決平成29年1月31日民集71巻1号63頁。

16）事務局ヒア（令和6年11月21日）4頁～6頁〔板倉陽一郎、鈴木正朝、高木浩光〕、事務局ヒア（令和6年11月22日）5頁〔曽我部真裕〕、6頁〔石井夏生利〕、事務局ヒア（令和6年12月4日）11頁〔宍戸常寿〕。

17）例えば、山本龍彦『プライバシーの権利を考える』（信山社、2017）。

18）高木浩光「個人情報保護から個人データ保護へ―民間部門と公的部門の規定統合に向けた検討(2)」情報法制研究2号89頁～99頁（2017）（**「高木連載②」**）。萎縮効果は関連性のないデータによる評価・決定の弊害ともいいうる。

19）「消費者法制度のパラダイムシフトに関する専門調査会 中間整理」（令和6年10月17日）。

20）WP29, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251 rev.01, p. 10 (Feb. 6, 2018). AI法5条1項(a)(b)も参照。Targetの妊娠状態に関する事例も、このような問題として位置付けることも可能であると思われる。

21）高木連載⑨97頁。特にプライバシーとの関係について、昭和63年逐条42頁、OECD, Explanatory Memoranda of the OECD Privacy Guidelines, OECD Digital Economy Papers, No. 360, p. 26 (Oct. 2023)（**「OECD説明覚書」**）も同趣旨。

22）事務局ヒア（令和6年11月22日）5頁～6頁〔石井夏生利、曽我部真裕〕、事務局ヒア（令和6年12月4日）11頁〔宍戸常寿〕。

23）個情委「「個人情報保護法 いわゆる3年ごと見直しに係る検討」の今後の検討の進め方について」（令和7年1月22日）8頁（**「進め方」**）。

24）Cookie IDについて個情委「株式会社リクルートキャリアに対する勧告等について」（令和元年12月4日）（**「リクナビ勧告」**）、オンラインゲームのIDについて個情委「「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」（平成29年2月16日（令和6年3月1日更新））1-9（**「Q&A」**）。令和2年一問一答15頁も参照。

25）WP29, Opinion 4/2007 on the Concept of Personal Data, WP136, p. 15 (June 20, 2007).

えた、「身元が分かること」[26]といった意味が込められている。

この解釈を前提に、個情委は、プロファイリング（リクナビ事件）、スミッシングなど、個人関連情報の「悪用」が問題となるごとに、断片的に規制を強化してきている（本見直しでは、不適正利用禁止規定が提案されている[27]。）。もっとも、これらのケースは、上記の識別性解釈が保護法益に照らして過少規制となっていることを示すものにほかならず、端的に識別性の解釈を改めるべきである[28]。

個情委も、常に「身元が分かること」を要求しているわけではない。個情委は、顔識別カメラシステムの文脈で、①ID（例：1）、②顔画像、③発生日時、④状況（例:ドアをこじ開け立入禁止区域に侵入した。）、⑤特徴（例：男性、スーツ、40代）というデータ項目からなるデータベースについて、レコード全体が個人情報に該当するとしているが[29]、ここには対象者の身元といえるような情報は含まれていない。

以上について、専門家間では、コンセンサスが形成されており[30]、文言又は解釈を修正する上での実際上のハードルは、識別性が認められた場合に適用される第三者提供制限の厳しさにある可能性がある[31]。例えばターゲティング広告のためのアドネットワークへの提供は、非決定利用とはいえないが、同意を要求するべきか、検討する必要がある。

(2) 散在情報の規制―維持すべきか？

個情法17条～21条は、文言上、「個人情報」を対象としており、データベース化を予定していない個人情報にも適用されるものと解されている[32]。

もっとも、立案担当者は、データベースは、「…特定の個人が検索可能なものについては、いったん不適正な処理がなされると、個人の権利利益に重大な侵害をもたらしたり、社会問題を引き起こす可能性が高い」[33]とした上で、個情法第4章は、「基本的に…個人情報データベース等を対象としている」[34]とし、「いずれ個人情報データベースに記録され「個人データ」となるものであっても、取得段階では「個人情報」の状態である」[35]ことから、（例外的に、）取得に関する規制は「個人情報」を対象とすることとした、と説明していた。取得に関する規制が個人情報を対象とする理由が、このようなものであるとすれば、データベース化を予定していない個人情報の取得に規制を及ぼす必要はないはずであり[36]、事務局ヒアリングでは、規制の対象を、個人データ（個人データとして「取り扱」うことが予定された個人情報を含む。）に統一することが議論されている[37]。

もっとも、そのような立法又は解釈[38]を行う場合、体系的構成要件が実際上のハードルとなる可能性がある。これについては、次節で述べる。

(3) 体系的構成要件―必須の要件であるべきか？

GDPRは、①自動化された手段による個人データ[39]の処理と、②ファイリングシステムの一部を構成し又は構成することが予定された個人データの、その他の手段による処理に適用される（2条1項）。②のファイリングシステムは日本法の個人情報データベース等に相当するが、①の基準が容易に適用される[40]結果、②の基準が適用されることは少ない。

①の基準があることで、日欧で規制対象かどうかが分かれると思われるのが、(a) 検索エンジン、(b) ChatGPTのようなLLM（を用いたチャットボット）、(c) 顔識別カメラシステム、(d) リアルタイムのバイオメトリック識別である。順に説明する。

26）注105も参照。

27）個情委「個人情報保護法の制度的課題に対する考え方について」（令和7年3月5日）5頁（**「考え方」**）。

28）堀部政男ほか「パネルディスカッション 個人情報保護法制のグローバルダイナミズム」情報ネットワークローレビュー 13巻1号157頁（2014）〔石井夏生利〕、宍戸常寿「3年ごと見直しの検討の充実に向けたヒアリングにおける意見」（令和6年12月4日事務ヒアリング資料1）2頁。高木②86頁～89頁。

29）個情委「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」（2023年3月）31頁（**「顔識別カメラ」**）。本文に述べたレコードの構造は、Cookie IDをキーとするWeb上での行動履歴のレコードとほぼ同じである。

30）第287回委員会（令和6年6月3日）11頁～12頁〔山本龍彦〕、17頁〔森亮二〕、第290回委員会（令和6年6月13日）3頁〔板倉陽一郎〕、事務局ヒア（令和6年11月21日）4頁〔高木浩光〕、高木浩光「「個人情報保護法のいわゆる3年ごと見直しの検討の充実に向けた視点」に対する意見」（令和6年11月12日事務局ヒアリング資料3）10頁（**「高木意見書②」**）、事務局ヒア（令和6年11月22日）1頁～2頁〔石井夏生利、曽我部真裕〕、事務局ヒア（令和6年12月4日）2頁〔宍戸常寿〕。

31）個人識別符号の検討過程について、高木連載②75頁～89頁。

32）Q&A 1-13、個情委「OpenAIに対する注意喚起の概要」（令和5年6月2日）（**「OpenAI注意喚起」**）、Q&A 4-5。

33）園部藤原84頁。

34）園部藤原174頁。

35）園部藤原149頁。

36）第289回委員会（令和6年6月12日）12頁～15頁〔高木浩光〕、高木浩光「個人情報保護法3年ごと見直し令和6年に対する意見」（第289回委員会資料1-2）9頁～12頁（**「高木意見書①」**）、第290回委員会（令和6年6月13日）1頁～3頁〔板倉陽一郎〕。

37）同前。

38）解釈による場合、取得に関する規制（及び不適正利用禁止規定）が適用される「個人情報取扱事業者」の定義（＝個人情報データベース等を事業の用に供している者。個人情報を取り扱う事業者ではない。）に着目した体系的解釈を施すことになろう。

39）識別され又は識別可能な自然人に関するあらゆるデータ（GDPR 4条(1)）。日本法の個人情報に相当する。

40）後掲のGoogle Spain事件のほか、Case C-101/01, Bodil Lindqvist, 2003 E.C.R. I-12971。

(a)検索エンジンの提供は、日本法では、「そのデータベース中に蓄積された情報に個人情報としての索引が付されているわけではない（同じ文字列であれば、地名や企業名等の個人情報でない情報も検索される。）」[41]ことから、体系的構成要件を欠き、個人情報の「取扱い」（第三者提供）に該当しないとされる。一方、EUのGoogle Spain事件[42]では、Googleが検索結果に含まれる個人データを処理しているかが問題とされたが、CJEUは、処理の定義規定（データ保護指令2条(b)）の文言解釈に基づいて、簡単に（自動）「処理」該当性を認めた。

(b)LLMの提供について、個情委は直接的には見解を明らかにしていないが、OpenAIに対する注意喚起[43]においては、要配慮個人情報の取得制限及び利用目的の通知・公表のみを問題とされているため、(a)と同様に、体系的構成要件を欠き、個人情報の「取扱い」（第三者提供）に該当しないと判断されている可能性がある。一方、EUでは、イタリアのデータ保護当局が、同社が個人データ処理を行っていたことを前提に、同社に制裁金を課している[44]。

(c)顔識別カメラシステムについては、様々な用途があるが、ここでは事前に登録された顔特徴データAと、リアルタイムで検出された顔に係る顔特徴データBをマッチングし、Aを検知するケースを考える。この場合、登録は必然的にデータベース化を伴うから、Aのデータは個人データに該当するのに対し、検知は必ずしもデータベース化を伴わないから、Bのデータは個人データに該当しない可能性がある。しかしながら、評価・決定の適切性の観点からは、Bの誤検知も、Aの誤登録と少なくとも同程度に重大な問題を引き起こしうる。

(d)リアルタイムのバイオメトリック識別とは、上記の顔識別カメラシステムのケースのうち、「検知」の段階だけを取り出したものに相当する。例えば、フランスの公立学校における体温測定器の使用について（自動）「処理」該当性を認めたConseil d'Étatの裁判が知られているが[45]、当該事案では、「測定された体温と平均体温との差を計算し、平均体温との比較で異常値を示すか否かを表示すること」[46]が、（自動）「処理」に該当するとされた。また、個情委も、「特定の個人を識別することができる顔画像を取得した後、顔画像から属性情報を抽出した上で、当該属性情報に基づき当該本人向けに直接カスタマイズした広告を配信する場合」には、個人情報の「取扱い」が認められるとし、利用目的に関する義務の遵守を求めている[47]。このように、リアルタイム処理によれば、データベース化なしに個人に対する評価・決定を行うことが可能であるが、そのような処理を適正化する上では、体系的構成要件は、狭すぎる可能性がある。

以上のうち、いずれを個情法の規制対象とすべきかは、演繹的に定まるものではない。(c)(d)が個人に対する評価・決定の問題であることは、比較的合意可能だと思われるが[48]、例えば、(b)がそうであるかについては、評価は分かれうる。また、例えば(a)(b)を個情法の規制対象とせず、(c)(d)を規制対象とする場合、どのような基準を設けるのかが問題となる[49]。いずれにしても、以上のような具体的なケースを踏まえて、体系的構成要件を必須の要件とし続けることの適切性を検討する必要がある。

3. コントローラー・プロセッサー

(1) 総説

本見直しにおいては、「個人情報取扱事業者等からデータ処理等の委託を受けた事業者に対する規律の在り方」が問題とされている[50]。まずは政府（個情委に限らない。）の監督強化によって対処すべきだと考えられるが、問題の本質は、個人情報の「取扱い」に関するサプライチェーンが複雑化する中で、誰にどのような責任を割り当て[51]、適正な個人情報の「取扱い」を達成するかにある。このことは、課徴金制度を導入するとき、特にクリティカルな問題となる。このよう

41）園部藤原86頁。

42）Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. I-317.

43）OpenAI注意喚起。

44）ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro (Nov. 2, 2024) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432>

45）金塚彩乃「体温自動測定 GDPR 違反コンセイユデタ判例解説」情報法制研究11号68頁（2022）。

46）金塚・前掲注（45）69頁。

47）Q&A 1-16。個情委「JapanTaxi株式会社に対する指導について」（令和元年9月17日）も参照。

48）第289回委員会（令和6年6月12日）3頁〔佐藤一郎〕、佐藤一郎「個人情報保護委員会「いわゆる3年ごと見直し」ヒアリング」（同委員会資料1-1）8頁。

49）EU法の「処理」に体系性を見出す見解として、高木浩光「個人情報保護から個人データ保護へ(8)―法目的に基づく制度見直しの検討」情報法制研究14号136～149頁（2023）（**「高木連載⑧」**）、高木⑨126～127頁。高木意見書①7頁～9頁も参照。なお、EU法のような書き方以外にも、個人情報を体系的に処理する場合、当該個人情報は個人データとみなす、といった書き方もありうると思われる。

50）視点8頁、考え方5頁。

51）責任の機能的割当てについて、OECD説明覚書26頁、EDPB, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.1, para. 12 (Sep. 20, 2022)。

な問題意識の下では、①コントローラー概念、②プロセッサーの実効的な監督、③クラウド例外を維持すべきかが問題となる。

(2) コントローラー概念とアカウンタビリティ原則

日本法は、OECDガイドラインやEU法でいう「（データ）コントローラー」に相当する者と、「プロセッサー」（OECDガイドラインでは「サービスビューロー」）に相当する者を、特に区別することなく「個人情報取扱事業者」とした上で、安全管理に係る監督[52]、第三者提供制限の例外及びその解釈[53]、保有個人データに関する規律の適用[54]等（その多くはパブコメの対象とならないQ&Aで示されている。）を通じて、両者に実質的に異なる規制が行われている。

一方、OECDガイドラインは、個人データの内容と利用を決定する権限を有する者を「データコントローラー」と定義し、個人データ処理に関する責任をそこに集中的に帰属させるという建付けとなっており、このことが、アカウンタビリティ原則と呼ばれている[55]。

日本法の建付けは、単に規制の一覧性や行政手続の観点だけでなく、アカウンタビリティの観点からも、再検討に値する。[56]。例えば、スタディサプリの件[57]では、教育委員会が公立小中学校の児童・生徒に学習用アプリ（スタディサプリ）を使用させていたが、個人データ利用に関して、教育委員会がリクルートに委託して個人データを収集するのではなく、リクルートが個人データを収集し、教育委員会に提供するとともに、自らのために利用していた。この件は、教育行政の文脈で、文部科学省が委託スキームを採用する（すなわち、教育委員会がコントローラーとなる）よう通知することで対処されたようであるが、誰が児童・生徒の利用に責任を負うべきかは、個情法が客観的に定めるべきであり、そのためには、コントローラー概念の導入が有効であると思われる。

なお、委託の場合には、コントローラーに全責任を負わせれば、アカウンタビリティの欠如は生じないが（実効性の確保は別問題である。）、複数のコントローラーが関与する場合、アカウンタビリティの欠如が生じうる。GDPRのジョイントコントローラー制度は、このような場合に、契約締結義務と連帯責任を課すものであり[58]、仮にコントローラー概念を導入する場合、ジョイントコントローラー制度の導入も検討すべきだと思われる。

(3) プロセッサーの実効的な監督

本見直しにおいて、個情委は、委託を受ける事業者の規律について問題提起している。クラウドサービス提供者（CSP）を中心に、専門性、透明性の欠如、市場支配力などにより、委託元に対して交渉力を有する委託先が増えており、委託元による実効的な監督が困難となっているとの問題意識だと思われる[59]。

これに対する第一の解決策は、そのようなCSPに対する政府の監督を強化することであり、個情法がプロセッサーをも規制対象としている趣旨も、それを可能とすることにあるものと思われる。

その上で、実効的な監督のために特別の規定が必要かが問題となる。EU法は、適切なプロセッサーの選択、再委託の原則禁止に加え、コントローラーに契約締結義務を課し、その契約の内容を規律するという手法を取っている[60]。日本法においても、少なくとも、最低限合意すべき内容を法定するほか、コントローラーによる適切な選択に役立てるため、一定の事項について開示義務を課すことが考えられる。また、セキュリティが主たる問題なのだとすれば、個人情報保護制度とは別に、セキュリティに関する法制度を整備することも考えられる[61]。

(4) クラウド例外―維持すべきか？

Q&A 7-53は、「クラウドサービスの利用が、本人の同意が必要な第三者提供…又は委託…に該当する

52）個情法25条。なお、同条は、あくまで安全管理に係る監督義務を規定しているにすぎないことに留意する必要がある。高木意見書②10頁参照。

53）個情法27条5項1号、個情委「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）」（平成28年11月）（令和6年12月一部改正）（**「通則ガイドライン」**）3-6-3の(1)、Q&A 7-34～7-43、7-53～7-58。

54）Q&A 1-56。

55）OECD説明覚書26、31頁。なお、日本法も、昭和63年法においては、「保有」及び「保有機関」概念（同法4条1項、5条2項。なお、保有の対象は、個人情報ファイルであって、行政文書ではない。）を通じて、データコントローラーに相当する行政機関を主要な規制対象としていた。

56）事務局ヒア（令和6年11月21日）6頁～7頁〔板倉陽一郎、鈴木正朝〕。

57）読売新聞「学習端末で個人情報取得、文科省通知「自治体と学校が責任を」…リクルート側も運用見直し」<https://www.yomiuri.co.jp/kyoiku/kyoiku/news/20241224-OYT1T50159/>。

58）EDPB, supra note 51, at para. 163. 適用例として、Case C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629。共同利用とは趣旨が全く異なる。

59）総務省総合通信基盤局長・サイバーセキュリティ統括官「通信の秘密の保護及びサイバーセキュリティの確保の徹底について（指導）」（総基用第46号）（令和6年3月5日）4頁、10頁、「損害保険業の構造的課題と競争のあり方に関する有識者会議報告書―我が国保険市場の健全な発展に向けて―」（令和6年6月25日）のⅡも参照。

60）GDPR 28条。契約内容について同条3項。欧州委員会及び加盟国当局は、標準契約約款を定めることができる（同条7項、8項）。日本においても、例えば電気通信事業法19条、20条は、契約約款を規制している。

61）EUでは、NIS2指令（に基づく国内法）がデジタルインフラたるCSPにセキュリティに関する義務を課している。日本においても、経済安全保障推進法、重要電子計算機に対する不正な行為による被害の防止に関する法律案（サイバー対処能力強化法案）第2章、各種業法が、セキュリティに関する規制を課している。

かどうかは、保存している電子データに個人データが含まれているかどうかではなく、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準とな」る、「当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合とは、①契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、②適切にアクセス制御を行っている場合等が考えられ」るとしている（クラウド例外）。

このことを前提に、2022年、個情委が、「一般論として、当該クラウドサービス提供事業者が、サーバに保存された個人データに対して編集・分析等の処理を行う場合には、当該クラウドサービス提供事業者が当該個人データを「取り扱わないこととなっている場合」には該当しないと考えられ」[62]るとの見解を示し、2024年、エムケイシステムの件で、同社における「取扱い」を認めた[63]ことで、CSP、特にSaaS事業者の「取扱い」を否定できる場面は相当程度限定されてきている[64]。

このクラウド例外をどのように扱うかは、本見直しの論点とはされていないが、①によって個情委がCSPを監督する必要性が失われるわけではないし[65]、②の技術的措置（アクセス制御ではなく暗号化だと思われる[66]。）は、データを暗号化し、暗号鍵をユーザーが保持するという、Q&A 7-35（配送事業者・通信事業者）類似の状況でしか認められ（るべきでは）ないようにも思われる。いずれにしても、委託を受ける事業者の規律について見直しを行う場合、クラウド例外もその対象とすべきである。

4. 基本的な義務規定

(1) 総説

事業者に適用される基本的な義務規定として、利用目的による制限、不適正利用禁止、正確性確保がある。これらは本見直しでは論点とされていないが、評価・決定の適切性を確保する上で第一に重要なのは、これらの義務規定である。しかるところ、これらの義務規定の文言、解釈、適用は、保護法益に照らして十分なものとなっていないと思われる。以下、具体的に検討する。

(2) 利用目的による制限―個情法の「要」の機能不全

利用目的による制限は個情法の「要」であるが[67]、その違反を理由とした指導等はほとんど行われておらず、有効に機能しているとは言い難い。以下、これを有効に機能させるための解釈・適用を検討する。

ア　利用目的特定義務の程度―リスクの同質性

利用目的特定義務における特定の程度について、立案担当者は、「できる限り」（法17条1項）の解釈という形で、「個人情報取扱事業者において、個人情報をどのような目的で利用するかについて明確な認識を持つことができ、また、本人においても、自らの個人情報をどのような目的で利用されるのかについて一般的かつ合理的に予測・想定できる程度に、利用目的を特定すること」が必要であるとしている[68]。

「明確な認識を持つ」／「一般的かつ合理的に予測・想定できる」とは何かが問題であるが、個情委が、令和2年個情法改正後のガイドライン改正において、「本人から得た情報から、本人に関する行動・関心等の情報を分析する場合、個人情報取扱事業者は、どのような取扱いが行われているかを本人が予測・想定できる程度に利用目的を特定しなければならない。」とし、ターゲティング広告や信用スコアは独立の利用目的として特定すべきとしていること[69]が参考になる。特定された利用目的は、利用目的による制限及び正確性確保（データ品質）の基準として機能するが[70]、これらの義務規定は、主として評価・決定の適切性を保護するものである[71]。そうだとすると、利用目的の

62）規制改革ホットライン令和4年度回答307。

63）個情委「株式会社エムケイシステムに対する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6年3月25日）。

64）小川智史「クラウド例外」NBL 1250号8頁～9頁（2023）。なお、規制改革ホットライン回答と個情委「生成AIサービスの利用に関する注意喚起等」（令和5年6月2日）の整合性が問題とされているが、後者はOpenAIによる取扱いがあることを前提に、学習のための利用が行われている場合、委託とは整理できないことを述べているに過ぎないのではないか。

65）当該契約条項が遵守されているかこそが監督の対象となるべきだからである。クラウド例外が適用される場合、ユーザーがCSPを監督する義務は失われないが（Q&A 7-54）、個情委のCSPに対する監督権限は失われる（高木意見書②9頁）。

66）個情委「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について（注意喚起）」（令和6年3月25日）2頁参照。アクセス制御は、権限のないエンティティ（ユーザーの従業員、CSPの従業員、第三者）がリソースにアクセスすることを防止するための措置であって、もとよりCSPによる「取扱い」を（技術的に）防止するための措置ではない。

67）園部藤原146頁、吉田・前掲注（11）13頁。

68）園部藤原149頁。なお、「できる限り」が義務を緩和する趣旨ではないことについて、昭和63年逐条74頁。

69）通則ガイドライン3-1-1。

70）利用目的が異なれば「利用目的の達成に必要な範囲」か、十分なデータ品質が確保されているかの評価が異なりうる。高木⑨100頁。

71）（伝統的）プライバシーは、目的外利用及び正確性確保とは関係がない。一方、「取扱い」の必要性は、プライバシーにも資するが、そこからターゲティング広告や信用スコアリングを独立した利用目的とすべきことは導かれない。

特定においても、評価・決定に関するリスクが考慮されるべきであるが[72]、そこでは、評価・決定が行われるか、どのような評価・決定が行われるかが重要である（例えばデータ分析、ターゲティング広告、与信判断、被疑者の捜索を想起・比較されたい。）。このように考えると、利用目的は、利用目的に含まれる「取扱い」のリスクが同質と言える程度まで特定すべき、言い換えれば、利用目的に含まれる典型的な「取扱い」とは異質のリスクを伴う「取扱い」を行おうとする場合には、当該「取扱い」の目的を独立の利用目的として特定すべきであり、上記のガイドラインの記載は、このことを、本人の視点から表現したものと言うことができるように思われる。

イ　「利用目的の達成に必要な範囲」の解釈・適用―合理的必要性

利用目的による制限における「利用目的の達成に必要な範囲」（法18条）は、OECDガイドライン第4原則に対応し、目的外利用を禁止するものであるが、同時に、「取り扱」う個人データは必要最小限のものでなければならないとする、OECDガイドライン第2原則（データ品質原則）の必要性要件を含むものと解釈されてきた[73]。

このことを前提に、「必要な範囲」について、事業者が主観的に必要とすれば満たされるかのような議論がされることがある。しかし、平成15年法の立案担当者により、「社会通念に基づき合理的に判断」するとの解釈が示されていることに留意する必要がある[74]。

これについて、個情法18条1項に類似する職業安定法5条の5第1項の解釈が参考となる。厚生労働省は、同項の解釈として、「次に掲げる個人情報を収集してはならないこと。ただし、特別な職業上の必要性が存在することその他業務の目的の達成に必要不可欠であって、収集目的を示して本人から収集する場合はこの限りでないこと。／イ 人種、民族、社会的身分、門地、本籍、出生地その他社会的差別の原因となるおそれのある事項／ロ 思想及び信条／ハ 労働組合への加入状況」とした上で[75]、イ～ハの例として、「家族の職業、収入、本人の資産等の情報（税金、社会保険の取扱い等労務管理を適切に実施するために必要なものを除く。）」、「容姿、スリーサイズ等差別的評価に繋がる情報」（以上イ関係）、「人生観、生活信条、支持政党、購読新聞・雑誌、愛読書」（ロ関係）、「労働運動、学生運動、消費者運動その他社会運動に関する情報」（ハ関係）を挙げている[76]。労働者の募集を行う者（同条の対象である。）には、主観的にはこれらの情報を必要とする者も多いと思われるが、「社会通念に基づき合理的に判断」すると、通常は「利用目的の達成に必要な範囲」とは認められないことを示すものと考えられる。

その上で、個情委がどの程度踏み込んで合理性を判断するか、言い換えれば、事業者にどの程度裁量を認めるかが問題となるが、「取扱い」のリスクを考慮して個別的に判断すればよいと思われる。最高裁も、憲法14条1項の合理的根拠に関してであるが、差別的取扱いの対象が何であるかによって、どの程度踏み込んだ判断をするかを変えており[77]、このような判断は（あるいはそれこそが）、「社会通念に基づ」いたものと考えられる。

このように考えると、リクナビ事件におけるスコアリングは、（識別性を措くと、）「「リクナビ2020」の会員となった学生等の人生をも左右しうる」[78]というハイリスクな状況で、利用目的の達成に厳密に必要とは言えないデータをもとに個人の評価を行っていたもので、「社会通念に基づき合理的に判断」すると、「利用目的の達成に必要な範囲」を超えた「取扱い」であった、と評価されるのではないか[79]。

なお、このような解釈を強調した場合、利用目的による制限は、OECDガイドライン第2原則の関連性要

72）データ品質原則の適用にあたって、データ品質が確保されなかった場合のリスクが重要な考慮要素となることについて、OECD説明覚書29頁。

73）瓜生和久編著『一問一答 平成27年改正個人情報保護法』66頁（商事法務、2015）（**「平成27年一問一答」**）。この点で、OECDガイドラインの第4原則は第2原則を担保するための要件であるという議論（高木連載⑨100頁）は、個情法18条1項と22条の関係には直ちには当てはまらない。

74）園部藤原153頁。

75）「職業紹介事業者、求人者、労働者の募集を行う者、募集受託者、募集情報等提供事業を行う者、労働者供給事業者、労働者供給を受けようとする者等がその責務等に関して適切に対処するための指針」（平成11年労働省告示第141号）（最終改正：令和4年厚生労働省告示第198号）第5の1(2)。

76）厚生労働省職業安定局「募集・求人業務取扱要領」（平成30年1月）Ⅳの1(7)イ（イ）、厚生労働省職業安定局「職業紹介事業の業務運営要領」（令和6年12月）第3（有料職業紹介事業許可基準）2(1)ハ。

77）最大判平成20年6月4日民集62巻6号1367頁。関連性原則と法の下の平等の構造的類似性について、高木⑨131～125頁。

78）リクナビ勧告。

79）厚生労働省職業安定局長「募集情報等提供事業等の適正な運営について」（職発0906第3号、第4号）（**「リクナビ通達」**）も、職業安定法5条の5第1項の内容を繰り返している。

件をもカバーするものであることになる[80]。

(3) 不適正利用禁止―法的根拠への移行？

個情法19条は、「個人情報取扱事業者は、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個人情報を利用してはならない。」と規定している。

この規定は、リクナビ事件を踏まえてプロファイリングを念頭に立案されたものであるが、法制局審査を経て現在の形となり[81]、ガイドラインには、「採用選考を通じて個人情報を取得した事業者が、性別、国籍等の特定の属性のみにより、正当な理由なく本人に対する違法な差別的取扱いを行うために、個人情報を利用する場合」という、リクナビ事件に似て非なる事例が記載されている[82]。同事件の問題の本質は、関連性を欠き、（社会通念に基づき合理的に判断して）利用目的の達成に必要とはいえないデータに基づいて、正確性も担保されていないスコアを算出し[83]、それにより学生が内定先から不利益に扱われかねなかったことにあると思われるが（同意取得や情報提供をしなかったことは、そのような不適正な利用についての拒否権行使の機会を奪った点で問題とされる[84]。）、現在の個情法及びその解釈を前提としたとき、そのような評価・決定が直ちに「違法又は不当な行為」と言えるかは、直ちには明らかでない。

一方、本見直しにおいては、「個人データの利用目的や利用態様などからその取扱いの正当性を裏付ける基準を導入する等の実体的ルールを設けることにより…適正な取扱いを担保するアプローチ」が検討された[85]。この「基準」が何を指していたのかは、必ずしも明らかではないが、EU法では、処理の法的根拠（GDPR６条）がそれに相当する機能を有している。

仮に処理の法的根拠を導入する場合、リクナビ事件におけるスコアリングは、（識別性が認められる前提で、）同意又は契約履行によることが考えられるが、十分な情報提供を行い、かつ契約締結の条件としない形でなければ、同意は無効とされ、また、スコアリングが契約の本質的内容となっていなければ、契約履行に必要な範囲を超えるとされると考えられる（しかし、スコアリングの影響に鑑みれば、いずれも満たすことが困難だったと思われる。）。

法的根拠による規制への移行は、いわばネガティブリストからポジティブリストへのドラスティックな転換であり、まずは利用目的による制限と正確性確保（データ品質）による適正化が必要かつ現実的だと思われるが[86]、内部利用と第三者提供のアンバランスさ[87]を論理的に解消できる、予測可能性が向上し、事業者と個情委[88]双方のコストを低減できるといったメリットもあり、検討に値すると思われる。

(4) 正確性確保（データ品質）

ア　アウトプットデータの正確性、ロジックの適切性

個情法22条は、「個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つ…よう努めなければならない[89]。」と規定する。

立案担当者は、本条について、「「正確かつ最新の

80）昭和63年法の立案の前提となった「行政機関における個人情報の保護に関する研究会意見」（昭和61年12月）（**「林研究会意見」**。昭和63年逐条所収）は、「第３保護対策の内容」「1　個人情報のファイルの設置」「(1)　関連性及び必要性による規制」の箇所で、「各行政機関等は、個人情報ファイルを設置するに当たっては、業務に関連性を有し、かつ必要な限度のものであることを常に吟味する必要がある。」とし（昭和63年逐条325頁）、同「4　個人情報の維持管理」「(2)　一般的な原則の規定」「ア　正確性の確保」の箇所で、OECDガイドラインのデータ品質原則に含まれる事項（完全性、関連性及び必要性、最新性）のうち、「関連性及び必要性については、既に、個人情報ファイルの設置に当たっての原則として採り上げている。」（同333頁）としていた。その上で、関連性要件が法文化されなかった理由が、（それが）必要性に含まれることにあったのだとすれば、本文に述べた帰結は、むしろ当然である。なお、高木連載⑥77頁も参照。

81）大島義則「個人情報保護法におけるプロファイリング規制の展開」情報ネットワーク・ローレビュー 20号37頁～ 46頁（2021）。第201回国会参議院内閣委員会第13号令和２年６月４日071以下も参照。

82）通則ガイドライン3-2の事例５。この事例は、むしろ東京医科大学事件に近い。同事件は、同大学が、その入学試験において、男性への加点等を行っていたものであるが、東京高判令和５年５月30日LEX/DB 25572936において、受験校を選択する自由の侵害とともに、性別による不合理な差別的な取扱いを理由として不法行為の成立が認められている。同事件と個人情報保護の関係について、第290回委員会（令和６年６月13日）１頁～３頁〔鈴木正朝〕。

83）この観点からは、この種のスコアないしサービスは、ユーザー企業への説明の仕方次第では、個人情報保護だけでなく、不公正な取引方法（ぎまん的顧客誘引）の問題ともなりうると思われる。

84）リクナビ通達は、リクルートキャリアの行為を、「本人同意なく、あるいは仮に同意があったとしても同意を余儀なくされた状態で、学生等の他社を含めた就職活動や情報収集、関心の持ち方などに関する状況を、本人があずかり知らない形で合否決定前に募集企業に提供することは、募集企業に対する学生等の立場を弱め、学生等の不安を惹起し、就職活動を萎縮させるなど学生等の就職活動に不利に働くおそれが高」いとした上で、「このことは本人同意があったとしても直ちに解消する問題ではない」いとし、「今後…このような事業を行わないようにすること」を要求している。

85）視点６頁。積極の意見として、事務局ヒア（令和６年11月22日）４頁〔石井夏生利〕。

86）第287回委員会（令和６年６月３日）８頁〔曽我部真裕〕、曽我部真裕「「個人情報保護法のいわゆる３年ごと見直しの検討の充実に向けた視点」について」（令和11月22日事務局ヒアリング資料）１頁（**「曽我部意見書」**）。

87）小向太郎=石井夏生利『概説GDPR―世界を揺るがす個人情報保護制度』65頁（NTT出版、2019）〔小向〕。

88）抽象的な規制の違反を理由に行政処分を行おうとするとき、行政庁は、裁判所によって当該行政処分が無効とされないよう、確実なロジック（証拠収集、法令の解釈・適用）を用意する必要に迫られる。しかし、このことが、迅速な措置を阻害し、ひいては権利侵害の防止（被害拡大防止を含む。）という個情法の目的の達成を困難にしてしまう可能性がある。

89）努力義務は法的義務であることに留意する必要がある（興津征雄『行政法I 行政法総論』178頁（新世社、2023））。なお、努力義務とされた理由は、「一般的に個人情報取扱事業者にとって、常時、正確かつ最新の個人データをすべて把握できる状況にはな」（園部藤原175頁）いためと説明されているが、「…保つために必要な措置を講じなければならない。」などとすることでも同趣旨は達成できる（GDPR５条１項(d)参照）。

内容」とは、取り扱われる個人情報の内容が、最も新しい事実と合致することをいい、主観的な評価・判断の是非まで本条で規律しようとするものではない。」、「個人データの正確性・最新性を確保するための具体的な措置としては、入力時の照合・確認、誤り等を発見した場合の訂正等のための手続の整備、一定期間ごとの記録事項の更新、データ内容に変更があった際の本人からの申し出の要請等が挙げられる。」と説明していた[90]。この説明は、昭和63年法から基本的に変わっていない[91]。

もっとも、昭和63年法において、評価・決定が対象とされなかったのは、評価・決定は、当然、人間が行うものであり、そのような評価・決定の誤りに起因する権利侵害は、同法が規制しようとする個人情報の電子計算機処理に起因する権利侵害ではないと考えられたからに過ぎないと思われる。翻って、現在、リクナビ事件がそうであったように、ルールベース処理か機械学習処理かを問わず、コンピュータが評価・決定を行い、それに基づいて事業者が個人に対し一人ひとりに応じた取扱いをすること（パーソナライゼーション）が一般化している。このような状況にあっては、アウトプットデータの正確性も重要であり、そのためには、処理のロジック（アルゴリズム）の適切性が要求されるべきである[92]。また、処理が機械学習によって行われる場合、学習用データの関連性、代表性（偏りのなさ）、信頼性といった要素が要求されるべきである[93]。

これに関して、EDPBの自動決定に関するガイドラインが、正確性の項で、以下のように述べていることが参考になる。「自動決定又はプロファイリングの過程で使用されるデータが不正確である場合、その結果として行われ（作成され）る決定やプロファイルも欠陥のあるものとなる。古くなったデータや外部データの誤った解釈に基づいて決定が行われる可能性がある。不正確なデータは、例えば、個人の健康、信用リスク又は保険リスクに関する不適切な予測や判断を引き起こす可能性がある。／たとえ生データが正確に記録されていたとしても、データセットが完全に代表性を持つとは限らず、分析に潜在的なバイアスが含まれている可能性もある。」[94]。

イ　関連性、完全性

OECDガイドライン第2原則（データ品質原則）は、「個人データは、それが利用される目的に関連（relevant）するものでなければならず、当該目的に必要な限りで、正確で、完全で、最新に保たれ（accurate, complete and kept up-to-date）なければならない。」としている。前半部分が関連性、後半部分が正確性、完全性、最新性を規定したものである。高木浩光は、このデータ品質原則こそが評価・決定の適切性を直接に確保しようとする規定であると指摘している[95]。

翻って、個情法22条は、データ品質原則に対応するものと説明されている[96]にもかかわらず、正確性要件及び最新性要件しか規定しておらず、関連性要件及び完全性要件を欠いている[97]。リクナビ事件の本質の一つは、不適正利用禁止規定の箇所で述べたとおり、無関係なデータによる評価・決定が行われていたことであったが、そのことを正面から問題とすることができなかったのは、個情法22条がその趣旨に照らして十分な内容となっていなかったからで（も）あると考えられる。

EUのAI法は、ソーシャルスコアリングを「受け入れ難い」として禁止しているが、そこで禁止されるのは、データが生成・収集された文脈とは無関係な文脈における不利益取扱いと、（スコアの元となった）社会的行動の重大性に釣り合わない不利益取扱いである[98]。リクナビ事件は、このどちらにも該当しうるものであり、個情委が「法の趣旨を潜脱した極めて不

90）園部藤原174頁～175頁。正確性の内容が事実との合致であるとの解釈は、正確性の実効性確保手段である訂正請求権の要件が「…保有個人データの内容が事実でないとき」（法34条1項）となっていることからも裏付けられる。

91）昭和63年法では、「処理情報が過去又は現在の事実と合致するよう努めなければならない。」とされ（同法5条2項）、その解釈として、評価・判断は「事実」には含まれないとされていた（昭和63年逐条85頁）。

92）高木連載⑨98頁

93）AI規則10条3項参照。

94）WP29, supra note 20, at pp. 11-12.

95）高木連載⑥71頁～75頁、高木連載⑨97頁、111頁。

96）園部藤原174頁。

97）なお、日本においても、昭和63年の検討過程においては、「正確性の意味に関しては、個人情報が事実に合致しているかどうかのほか、業務遂行上の社会通念に照らして、個人について誤解を生じさせることのないよう必要な事項をすべて含んでいるかどうか（完全性）、業務遂行上不必要な事項まで含んでいないかどうか（関連性及び必要性）及び過去の事実が現在と異なるとき、現時点の事実を示すものであるかどうか（最新性）といった事項まで含めて考えることが適当である」とされていた（林研究会意見第3の4(2)ア（昭和63年逐条解説333頁））。関連性及び完全性が法文化されなかったのは、法制局審査の結果であることが判明しているが（高木連載⑥77頁）、正確性確保の実効性確保手段である訂正請求に対する救済内容としては、「当該保有個人データの訂正、追加又は削除」（追加は不完全な情報を補うことである。園部藤原315頁）が残っている。

98）AI法5条1項(c)、recital 31。European Commission, Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, (Feb. 4, 2025)の4.2.2(b)も参照。

適切なサービス」と批難し[99]、厚生労働省が「募集情報等提供事業や職業事業等の本旨に立ち返り、このような事業を行わないようにすること」[100]まで要求したことは、既にそのような価値判断を前提としていたのではないか。

5. 第三者提供制限

(1) 見直しの前提

第三者提供制限は、個人データの第三者提供が適法とされる場合を列挙し、本人の同意がある場合、法令に基づく場合、生命・身体・財産保護に必要な場合、公衆衛生・児童健全育成に特に必要な場合等のみこれを認めるものである（法27条1項）。

第三者提供制限は、利用目的による制限の特則（追加的規制）であり、第三者提供により、「①本人の全く予期しないところで当該個人データが利用されたり、②他のデータと結合・加工されるなどして、③本人に不測の権利利益侵害を及ぼすおそれが高まる」（番号は筆者）ことから、一律に目的外利用と同様の規制が課されたものである[101]。①②は③の例示であるが、①は主として不招請勧誘・犯罪利用（名簿に関するリスク）、②は主として不適切な評価・決定を指すものと思われる。

EU法と比較すると、日本法は、内部利用に法的根拠が要求されない点でより緩やかであり、第三者提供が認められる場合のリストが法的根拠のリストよりも狭い点でより厳しいが、その背景には、特に①が重視されたこと、より端的に言えば、第三者提供制限に名簿業者規制としての側面があったことがあったものと思われる。

(2) 個情委の提案の概要

個情委は、次の提案をしている[102]（なお、これらの提案は、法的根拠による規制は導入しないことを前提とするものだと思われる。）。

すなわち、(a)「一般的・汎用的な分析結果の獲得と利用」（非決定利用）のみを目的とした第三者提供を認めること、(b)契約履行に必要不可欠であるなど、本人の意思に反しないため本人の権利利益を害さないことが明らかである場合の第三者提供を認めること、(c)生命保護等例外及び公衆衛生等例外（法27条1項2号、3号）の第2要件を、「本人の同意を得ることが困難であるときその他の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」とすること（現行法には「その他の」以下が存在しない。）、(d)学術研究例外（個情法27条1項5号～7号）の対象である「学術研究機関等」（同法16条8項）に病院・診療所（の開設者）を加えることである。

(a)においては、その担保のため、情報提供（提供元・提供先の名称、行おうとする統計作成等の内容等）、契約締結、目的外利用・第三者提供の禁止を義務付けることが提案されている。(b)においては、契約履行は例示であるが、契約履行以外の例は挙げられていない。(c)の「相当の理由」としては、「本人のプライバシー等の侵害を防止するために必要かつ適切な措置（氏名等の削除、提供先との守秘義務契約の締結等）」が講じられている場合が例示されている。

(3) 非決定利用のための提供

(a)は、評価・決定の適切性との関係では、第一に、個人データが評価・決定に用いられるかが問題であり、それに用いられないこと（非決定利用）が確保される場合には、そもそも第三者提供制限（やその一般法である利用目的による制限）を課す必要がないことを根拠に、非決定利用を確保するための代替的なセーフガードと引き換えに、同意を不要とするものである（評価・決定の利益に優越する他の利益が存在するからではない。）。このような考え方は、事業者内部における統計利用や仮名加工に係る規律との関係では、既に採用されていたものであり[103]、それ自体としては適切だと思われるが、仮名加工情報に係る規律との関係について、さらに検討を要すると思われる。

すなわち、仮名加工は、個人との対応関係を維持しつつ、他の情報と照合しない限り個人を識別できないようにすることであり（法2条5項）、仮名加工後に委託先に提供した場合、委託先にとっては識別性がないため、委託先には個人情報・個人データに係る規制は適用されないものと解されている[104]。(a)の下でも、（非決定）利用の目的に反しない限り、提供者側で仮名化を行うことは望ましいが、そうすることで、提供先に規制が及ばなくなってしまう可能性がある。これは、識別性解釈が保護法益に対して十分な

99）リクナビ勧告。これまで個情委がセキュリティ侵害以外の場面で勧告を行ったのは、本件と一連の破産者マップ事件に限られ、このことからも、個情委が同事件に与えた評価の一端が読み取れる。

100）リクナビ通達。

101）園部藤原196頁～197頁。

102）考え方1頁～3頁。

103）統計についてQ&A 2-5、仮名加工情報に係る規律の趣旨について令和2年一問一答11頁。

104）令和2年一問一答15頁、関口朋宏「共同利用先における「仮名化データ」の取扱い」NBL 1268号51頁～52頁（2024）。

ものとなっていないことに起因するものであるが[105]、識別性解釈を修正するのであれば、仮名加工に係る規律を併せて見直す必要があり、それを先送りするのであれば、受領者に適切な義務を課す必要がある。

(4) 契約履行のための提供

(b) は必ずしも活発な議論の対象となっていないが、次のような効果があると思われる。すなわち、従前、日本法においては契約履行のための提供が許容されていなかったため、契約履行に必要な提供について、利用規約やプライバシーポリシーに記載し（ただし提供先や提供先での利用目的は記載せず）、同意ボタンを押させることで包括的に同意を取得することが広く行われていた[106]。契約履行を同意から分離することで、契約履行に必要な提供については、真に必要な提供なのかを厳密に判断し、同意に基づく提供については、同意の任意性（例えば、必要な情報提供がなされているか、契約との「抱き合わせ」や複数の利用目的の「抱き合わせ」がなされていないか、力の不均衡がないか[107]）や提供が同意の範囲に含まれるかを、厳密に判断することができるようになる。

(5) 生命等保護・公衆衛生等・学術研究のための提供

(c)(d) のうち、公衆衛生例外及び学術研究例外については、(a) との関係を整理する必要がある。すなわち、現にニーズのある公衆衛生目的の提供及び学術研究目的の提供の少なくない部分は非決定利用であると思われるところ[108]、そのような利用は、(a) によって統制すべきである。この場合、公衆衛生例外及び学術研究例外（なお、これらが重複しうることにも留意すべきである。）は、決定利用に適用されることになるが、この場合、研究倫理指針などの代替的セーフガードが必要である。

一方、生命等保護例外（及び公衆衛生等例外）については、(i) 人格権が含まれるか明らかではない[109]、(ii) 財産の処分が含まれない（この結果、債権譲渡の文脈では、推定的同意すら認められている[110]。）、(iii)（必ずしも個々に権利保護を目的としたものとは言い難い）犯罪対策において、提供できる場合が限定される[111]といった問題が生じている。正当利益による第三者提供を認めないのであれば[112]、(i)(ii) については、別途権利行使のための提供を認め、(iii) については、公衆衛生等例外の拡張や別途情報共有のルールを定める[113]といったことを検討する必要があると思われる。

6. 追加的な義務規定（第三者提供制限以外）

個情法又はGDPRは、第三者提供制限以外にも、個人情報の種類や「取扱い」の態様に応じて、基本的な義務規定の実効性を担保するための追加的な義務を課している。①要配慮個人情報、②児童のデータ、③バイオメトリックデータ、④名簿業者による「取扱い」、⑤自動決定（プロファイリング）がこれに該当する。その内容は、基本的な義務規定を補うために何が必要かという観点から検討されるべきである。

(1) 要配慮個人情報の取得制限

個情委は、AI開発を含む非決定利用のための要配慮個人情報の取得を認めることを提案している。しかし、散在情報の規制の箇所で述べたとおり、(a) データベース化しない場合（LLM開発のために収集するテキストデータは通常ここに含まれる。）と (b) データベース化するが決定に利用しない場合は区別すべきであり、(a) はそもそも取得に関する規制の対象としないことが、個情法の体系に適合的である[114]。(b) は、LLMを含む生成AIというよりは、信用スコアリング

105) GDPRは、仮名化を、「個人データを追加情報の使用なしに特定のデータサブジェクトに帰属させることができなくなる（can no longer be attributed to a specific data subject）ような方法による個人データの処理」としている（4条5項）。EU法では、single outができれば識別可能であり、仮名化がされても、単体での識別性は直ちには失われない。これに対し、日本法は、識別性の内容として、EU法にいうattributionに相当するものが要求されているため（識別性の箇所を参照）、仮名加工がされると、たとえsingle outができるとしても、単体での識別性は失われ、専ら照合による識別性が残るにすぎない。

106) 第287回委員会（令和6年6月3日）8頁〔曽我部真裕〕、事務局ヒア（令和6年11月22日）8頁〔石井夏生利〕。

107) EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1 (May 4, 2020). 総務省「同意取得の在り方に関する参照文書」（令和3年2月25日）も、通信の秘密の侵害に係る同意取得について類似の解釈を示しており、個情法上の同意も、本来このようなものであるべきだと思われる（第290回委員会（令和6年6月13日）4頁〔板倉陽一郎〕、板倉陽一郎＝斉藤邦史『金融機関の個人情報保護の実務』146頁（経済法令研究会、2023）参照）。

108) 例えばQ&A 7-25。

109) これを認めるものとして、板倉陽一郎「個人データが含まれる証拠の裁判所への提供についての考察」情報ネットワーク・ロー・レビュー 19号184頁（2020）。

110) 個情委事務局・金融庁「金融機関における個人情報保護に関するQ&A」（令和5年3月）5-4。この見解について、板倉＝斉藤・前掲注（107）100頁。

111) 通則ガイドライン3-1-5の(2)。

112) EU法においては、正当利益が処理の法的根拠のバスケット条項として機能しているが（WP29, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, WP217, p. 9 (Apr. 9, 2014)）、特に比較衡量テストは、多様な利益を考慮することができる（EDPB, Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0, pp. 12-19 (Oct. 8, 2024)）一方、恣意的になりやすく、バスケット条項を置かないことにも一定の合理性がある。

113) そのような例として、学校設置者等及び民間教育保育等事業者による児童対象性暴力等の防止等のための措置に関する法律（こども性暴力防止法、日本版DBS法）がある。サイバー対処能力強化法案第3章～第9章、デジタル行財政改革会議データ利活用制度・システム検討会における議論も参考になる。

114) 高木意見書①4頁～7頁。

のような識別AI（非生成AI）の開発において問題となるが、要配慮個人情報の取得制限の保護法益（必ずしも第三者提供制限のそれとは同一ではないと思われる。）に照らした検討が必要である[115]。

(2) 児童（16歳未満者）のデータ

個情委は、16歳未満者のデータについて、「①心身が発達段階にあるためその判断能力が不十分であり、②個人情報の不適切な取扱いに伴う悪影響を受けやすいこと等」から、(a) 同意取得・通知等について法定代理人を対象とすること、(b) 要配慮個人情報の取得が認められる場合と同様の場合以外の場合には、利用停止請求を認めること、(c) 事業者及び法定代理人に最善利益義務を課すこと等を提案している[116]。

①②はそれぞれ適切だと思われるが、並列の関係であることに留意する必要がある。すなわち、①は本人関与の実効性が乏しいことを意味し、②は特に教育に関する個人データ利用がその後の人生を左右しうること[117]を意味する。①の観点からは、(a) は有効であり、これに関連する限りで、(c) の法定代理人に義務を課すことには一定の意味がある。一方、②の観点から必要なのは、利用目的による制限と正確性確保（データ品質）を中心とする基本的な義務規定を、そのリスクに比例して厳密に適用することである。(b) が必要かは、要配慮個人情報の取得制限の保護法益に照らして検討する必要があり、(c) については、最善利益を確保するための規定を具体的に定めるべきである。

(3) 顔特徴データ等（バイオメトリックテンプレート）

個情委は、バイオメトリックテンプレート[118]について、入手容易性（悉皆性と外部からの観察の容易性の2つを含むと思われる。）、一意性、不変性、①情報提供義務、②要配慮個人情報の取得が認められる場合と同様の場合以外の場合には、利用停止請求を認めること、③オプトアウトによる第三者提供の対象から除外することを提案している[119]。①は②の実効性確保手段として提案されている。③は第三者提供に係る拒否権行使（＝不同意）の機会を与えるためのものである。

個情委の問題意識は、それ自体としては適切だと思われるが、若干の補足を要する。すなわち、バイオメトリックテンプレートの高いリスクは、(a) それがクロスコンテクストな属性や行動履歴の紐づけを可能とすること（入手容易性、一意性、不変性はこの背景である。）と、(b) バイオメトリック識別の精度には限界があり、しかも、その精度にはしばしば偏りがあることに由来している[120]。これらの観点から第一に必要なのは、やはり、基本的な義務規定を、そのリスクに比例して厳密に適用することである。特に、(a) との関係では利用目的による制限とデータ品質のうち必要性・関連性が、(b) との関係ではデータ品質のうち正確性が特に重要である。

その上で、基本的な義務規定を補うために、①はバイオメトリック識別の存在を認識させる点で[121]、③はClearview[122]のようなブローカーの出現を防止する点で、それぞれ一定の意味がある。一方で、②が必要かは、要配慮個人情報の取得制限の保護法益に照らして検討する必要がある。

(4) 名簿業者規制

名簿業者規制として、個情委は、オプトアウト事業者に提供先及びそこでの個人データの利用目的の確認義務を課すことを提案している[123]。オプトアウト事

115）要配慮個人情報の保護法益は、必ずしも明らかではない。評価・決定の適切性との関係では、何のために情報を利用するのかが重要であり、情報の性質は重要ではない。プライバシーとの関係でも、Webに公開された情報は、非公知性を欠き、少なくとも収集に対しては保護されない可能性が高い。要配慮個人情報の出力（第三者提供制限の対象とならないと思われる。）の予防のために学習を規制することは考えられないではないが、要配慮個人情報を学習させなかったからといって、要配慮個人情報を出力しなくなるわけではない（LLMにおいて特定の学習用データが特定のパラメータの重みに与える影響は極めて小さく、特定のパラメータが出力に与える影響もまた極めて小さい。）。さしあたり、法的根拠による規制を一般的には行っていない日本法にあって、経験的に不適切に評価されやすい情報について、法的根拠を要求したものと理解した上で（平成27年一問一答19頁参照）、個別の場面ごとに保護法益を特定し、それに沿って規制を合理化していくほかないと思われる。高木意見書②11頁～13頁も参照。

116）考え方4頁。

117）リクナビ勧告に類似する。

118）考え方6頁は、個情法2条2項1号の個人識別符号を「顔特徴データ等」と呼んでいる。これは、EU法のbiometric dataに類似するが、単なる顔写真はこれに含まれないとされているため、一般名称としては、バイオメトリックテンプレートがより的確であると思われる。なお、個情委「個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理」（令和6年6月27日）（**「中間整理」**）は、biometric dataを「生体データ」と呼んでいたが、-metricのニュアンスが欠落する難点がある（高木意見書②13頁は、「生体計測データ」とする。）。また、中間整理（及び通則ガイドライン2-2）は、個情法2条2項1号の「当該特定の個人を識別することができるもの」を、「認証」と呼んでいるが、（一意の）識別と認証は区別すべきである（顔識別カメラ6頁、EDPB, Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement, paras. 10, 19-23 (May 17, 2023)）。

119）考え方6頁～7頁。

120）WP29, Opinion 3/2012 on Developments in Biometric Technologies, WP193, pp. 17-18 (Apr. 27, 2012).

121）この点で、①は、ターゲティング広告・信用スコアリングを独立の利用目的として特定させ、通知・公表させること（通則ガイドライン3-1-1）と同等の効果を有する。裏を返せば、情報提供を義務付ける上で、利用目的特定義務の解釈という形を取ることは、必須のものではない。

122）米国のClearview AI, Inc.がWebから顔写真を無差別にスクレイピングし、データベースを作成し、警察等に提供していた。米国で集団訴訟が提起され、イギリス、フランス、ドイツ、イタリア、カナダ、オーストラリア等のデータ保護当局が法執行を行った。AI法は、本事件を背景として、同種のデータベースを作成・拡張するAIシステムの上市・サービスとしての提供・使用を禁止している（5条1項(e)）。

123）考え方7頁～8頁。

業者に限定することの合理性は問題となりうるが、必要な規制であると思われる。もっとも、名簿業者が重要な犯罪インフラとなっているのであれば、注意喚起や指導にとどまらず、特定商取引法、金融商品取引法（適格機関投資家特例業務関係）等を参考に、届出を受けた場合には、必要な調査を行い、犯罪に加担している業者（オプトアウト届出をしていない者も含む。）を発見した場合には、迅速に（期限付き又は無期限で）第三者提供を包括的に禁止する緊急命令を発し、捜査機関と共同して事態に対処する、といったことも検討すべきだと思われる。

(5) 自動決定（プロファイリング）

自動決定（プロファイリング）は、「今後に向けて考慮していくべき点」とされているが[124]、評価・決定の適切性の観点からは、重要な問題である[125]。特に、AIの問題の多くは自動決定（プロファイリング）の問題でもあるところ、日本では包括的なAI規制は検討されておらず、個情法がこの問題に対処する必要性は高い[126]。もっとも、そこで第一に必要なのは、基本的な義務規定を、そのリスクに比例して厳密に適用することであり[127]、追加的な規制[128]（例えば情報提供[129]）の要否は、基本的な義務規定の実効性を確保するために何が必要かという観点から検討されるべきである。

7. エンフォースメント

(1) エンフォースメントの体系―自律的ガバナンス？

本見直しにおいて、個情法の規制が、「自律的ガバナンス」と表現されているが[130]、本人関与はあくまで義務規定の実効性を担保する手段であること、しかしそれでは十分ではないため、平成27年改正により、政府による監督が強化されたことに留意する必要がある。つまり、本人関与と個情委の監督は、義務規定の相互補完的なエンフォースメント手段である[131]。

このような理解は、エンフォースメントにおけるリソース配分の指針をも提供する[132]。すなわち、本人関与には、情報の非対称性（証拠収集ツールの不十分性を含む。）、経済的コスト、認知的コストなど、様々な限界があり、それゆえに、政府の監督が必要とされる。裏を返せば、そのように、本人関与を阻害する事情があり、本人関与に委ねたのではエンフォースメントが過小となる場面にこそ、個情委は優先的にリソースを投入する必要がある。そのような分野として、例えば、警察、入管、金融、教育、医療、雇用、優越的地位にある事業者による個人データ処理[133]、先端技術を用いた個人データ処理などが考えられる。

(2) 本人関与―情報提供と容易な方法による権利行使

個情法上、本人関与を保障する制度として、①利用目的の通知・公表、②目的外利用、要配慮個人情報の取得、第三者提供に係る同意、③保有個人データに関する事項の通知・公表、④開示請求権、⑤訂正等請求権、⑥利用停止請求権がある。このうち、個人情報の「取扱い」に直接に影響するのは、②⑤⑥であり、①③④は、それらの権利行使の機会を実質的に保障するための情報提供制度である。また、同意を実質化する場合、同意が有効となるために、一定の情報提供が必要となる場合がある。本見直しにおいては、本人関与の限界が強調されており、それ自体は適切だと思われるが、そうであるからこそ、（それが適切な場面では、）本人をエンパワーするために何をすべきかを検討する必要がある。

この観点から考えられる論点としては、(a) 利用目的だけでなく当該利用目的に対応するデータ項目を情報提供させること、(b) 同意の個別性を要求し、プライバシーポリシーや利用規約に対する包括的な同意を無効とすること、(c) 第三者提供における提供先、提供するデータ項目、提供先における利用目的、何に基づく提供かを情報提供させ、同意に基づく提供の

124) 進め方8頁。

125) 第287回委員会（令和6年6月3日）11頁〔山本龍彦〕、事務局ヒア（令和6年11月22日）10頁〔曽我部真裕〕。

126) 第279回委員会（令和6年4月3日）5頁〔生貝直人〕、第289回委員会（令和6年6月12日）4頁～5頁〔佐藤一郎〕参照。

127) 事務局ヒア（令和6年11月21日）3頁〔高木浩光〕。

128) 自動決定（プロファイリング）については、GDPR 22条が知られているが、それも、人間の介入なしに法的効果又はこれと同等の影響をもたらす自動決定についての追加的規制にすぎない。WP29, supra note 20, at pp. 8-9.

129) GDPR 13条2項(f)、14条2項(g)参照。高木意見書②3頁も参照。

130) 視点6頁。

131) 事務局ヒア（令和6年11月21日）3頁〔高木浩光〕、曽我部意見書2頁。独占禁止法（**「独禁法」**）における公正取引委員会（**「公取委」**）の権限行使と民事訴訟の関係はこれに類似するが、一方で、同法においては伝統的には公取委の権限行使が重視されてきたことに留意する必要がある。白石忠志『独占禁止法（第4版）』（有斐閣、2023）（**「白石」**）の第17章参照。

132) 宍戸常寿「パーソナルデータに関する「独立第三者機関」について」ジュリスト1464号22頁（2014）は、個情委が担うべき機能を具体的に明確化しなければ、「長期的には第三者機関の活動は実効性を失い、過去多くの独立行政委員会が経験したのと同じ末路を辿るおそれもあ」ると警告していた。

133) 公取委「デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」（令和元年12月17日）（改正：令和4年4月1日）参照。

場合、情報提供が不十分な場合には同意を無効とすること、(d) プロファイリング、バイオメトリックテンプレートなどのハイリスクなデータ処理について、追加的な情報提供を義務付けること[134]、(e) 権利行使の受付方法の説明と、容易な方法[135]による権利行使の受付けを義務付けること、(f) 以上の義務が履行されなければ本人関与の機会が奪われるため、それらの履行状況を個情委が積極的に監督するなどことがありうる。

(3) 個情委による監督

ア　実態調査（アドボカシー活動）

個情法が規制しようとするプラクティスは、他の規制法のそれと比較したとき、変化の激しさと、業種が限定されていないことによる多様性（言い換えれば、個人情報保護の問題の単位としての大きさ）によって特徴づけられる。このような状況では、当局側でリスクを識別し、低減措置を設計し、そのアウトプットとしての禁止・命令のリストを法律に書き込むことは困難であり、法律には基本的なフレームワークのみを書き込んだ上で、事業者と対話しながらその自主的な取組みの適切さをモニタリングするほかない[136]。

同様にデジタル化に直面している公取委の取組み[137]を参考に、個情委も、上記の優先的にリソースを投入すべき分野を中心に、個別分野の実態調査を行い、明らかになった具体的事実に即して個情法・個人情報保護政策上の問題を指摘することで、自主的な取組みを促すとともに、エンフォースメントに（も）役立てることが考えられる。

なお、この場合、個情委が、個人情報保護に影響を与える制度（例えば電磁的記録提供命令[138]）について牽制機能を発揮するためには、意見具申権限が必要であると思われる[139]。また、効果的なエンフォースメントを行う上では、現行法の勧告・命令の要件は過剰に抑制的である可能性があり、要件の緩和も検討されるべきである[140]。

イ　課徴金制度[141]

本見直しにおいては、課徴金制度は継続的な検討課題とされたが[142]、「個人情報保護法のいわゆる３年ごと見直しに関する検討会」（**「検討会」**）は、以下のような課徴金制度の導入を提案していた[143]。①要件は、(a) 事業者が利用目的による制限、不適正利用禁止、適正取得義務、第三者提供制限に違反し、これにより収益を得、(b) 当該違反について事業者が相当の注意を怠り（安全管理措置については相当の注意を著しく怠り）、(c) 当該違反により個人の権利利益が侵害され、又は権利利益が侵害されるおそれが生じ、(d) 違反行為に係る本人の数が1000人を超えたこととする。②算定方法は、(a) 安全管理措置以外の違反については、違反行為による収益とする。(b) 安全管理措置については、結論が出ていない（事務局は売上額に一定の算定率を乗じることを提案したが[144]、両論併記とされている。）。③ (a) 自主申告による減算規定、(b) 繰り返し違反による加算規定を設ける。

我が国の課徴金制度は、独禁法が先例となって形成されてきた[145]。独禁法においては、罰則（同法89条1項1号）との関係で、二重処罰禁止（憲法39条後段）への抵触が問題とされた。このため、不当な取引制限に係る課徴金制度の導入時（昭和52年改正）には、課徴金制度は、違反行為によって得られた利得を剥奪するためのものであることが強調され（不法利得剥奪論）、このため、課徴金の要件及び額は、非裁量的なものとされた。平成17年改正時に、公取委は、課徴金の正当化根拠としての不法利得剥奪論を明示的に放棄したが、その後も、不法利得は課徴金額の

134) 注121を参照。

135) 電気通信事業法上の電気通信事業者又は3号事業を営む者、特定商取引法上の通信販売を行う販売業者又は役務提供事業者等については、端的にオンラインでの権利行使の受付けを義務付けることも考えられる（令和6年法律第25号が施行された時点における特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律（情プラ法）22条2項参照）。

136) この意味で、個情法は本来的に共同規制である。「金融モニタリング有識者会議報告書―検査・監督改革の方向と課題―」（平成29年3月17日）、金融庁「金融検査・監督の考え方と進め方（検査・監督基本方針）」（平成30年6月）も参照。

137) 公取委「デジタル化等社会経済の変化に対応した競争政策の積極的な推進に向けて―アドボカシーとエンフォースメントの連携・強化―」（令和4年6月16日）。

138) 情報通信技術の進展等に対応するための刑事訴訟法等の一部を改正する法律案（令和7年2月28日閣議決定）が成立した場合の刑事訴訟法102条の2、218条1項。個人情報保護に関して、法制審議会刑事法（情報通信技術関係）部会第11回会議（令和5年8月4日）、第12回会議（同年9月15日）の議論を参照。個情委が3条委員会とされたのは、個情委に政府の内部統制機関としての役割が求められるからであり、警察による個人データ利用の適正化は、個情委の存在意義に関わる（宍戸・前掲注（132）23頁注19（2014）、同「安心・安全とプライバシー」論究ジュリスト18号59頁（2016））。

139) 個人情報保護制度の見直しに関するタスクフォース「個人情報保護制度の見直しに関する最終報告」（令和2年12月）27頁注54参照。

140) 第283回委員会（令和6年5月10日）13頁〔中川丈久〕。考え方8頁は権利侵害が切迫している場合にも緊急命令を可能にすることを提案しているが、勧告前置を原則とすること自体の合理性も検討されるべきである。当局の監督の下で事業者の自主的な取組みを促す観点からは、独禁法上の確約制度（独禁法48条の2～48条の9）のような仕組みも考えられる。白石668頁～669頁も参照。

141) 基本的な文献として、大島義則「個人情報保護法における課徴金制度の導入論」情報ネットワーク・ローレビュー19号1頁（2020）、宍戸常寿「課徴金制度をめぐる論点」法律のひろば73巻10号24頁（2020）。

142) 考え方10頁～11頁。

143) 「個人情報保護法のいわゆる３年ごと見直しに関する検討会報告書」（令和6年12月25日）15頁～29頁（**「検討会報告書」**）。

144) 令和6年11月28日第6回検討会議事録10頁～11頁、26頁。

145) 以下の記述に関して、白石715頁～720頁。「独占禁止法研究会報告書」（平成29年4月）も参照。

一応の基準とされ、令和元年改正では、裁量的要素が導入されたが、あくまで減算制度の適用に関するものにとどまっている。

以上の独禁法に関する議論と対比したとき、個情法違反は、必ずしも利得を目的として行われるわけではなく（これに対し、不当な取引制限は超過利潤を得ることを目的とする。）、利得の有無や金額が違反行為の悪質性[146]と相関するわけでもない。そのため、二重処罰禁止との関係はもとより、比例原則の関係でも、利得を要件又は課徴金額の基準とするのでは、その課徴金制度の導入の目的を達成できない可能性が高い。

また、個情法違反によって生じるリスクは具体的状況に応じて様々であり（不当な取引制限のように同質ではない。）、それに応じて事業者が取るべき行動も様々である。このような具体的状況を適切に考慮することは、行政庁の裁量（特に効果裁量である課徴金額[147]）を通じてでなければ行うことが困難であると思われる。

(4)「司法化」のタイミング

一方で、課徴金制度や消費者団体訴訟の導入の是非とは別に、導入のタイミングを考慮する必要がある。

仮に課徴金制度や消費者団体訴訟を導入した場合、ガイドラインやQ&Aに記載された解釈が裁判所で争われることになる（個情法の司法化[148]）。しかし、これらの文書は、裁判規範として用いられることは基本的には想定されておらず、このまま「司法化」すれば、解釈が分かれ、不適切な裁判例が蓄積されてしまう事態も否定できない。特に、消費者団体訴訟においては、事件選択や法律構成、救済の内容（請求の趣旨）の決定に個情委が関与が予定されないため、このおそれは大きい。

さらに、課徴金については、一度それを導入すれば、実績を挙げる必要に迫られるが、現在、安全管理以外の指導等の蓄積はほとんどないため、安全管理に偏った「手堅い」事件選択へのインセンティブが働き、現状を固定化してしまう可能性がある。

独禁法においては、不当な取引制限に係る課徴金制度の導入時には、既に多くの排除措置命令が行われており、判例が一定程度形成されていた。これに対し、優越的地位濫用については、そのような前提を欠いた状態で平成21年に課徴金制度が導入されたが、その後発せられた課徴金納付命令は全て争われ、平成26年を最後に排除措置命令・課徴金納付命令は行われていない[149]。導入のタイミングを検討するにあたっては、少なくとも以上のことを前提に、個情委が「司法化」に耐えうるよう、解釈を洗練させ、先例を形成するのに必要な期間を考慮する必要がある。

8. おわりに

本見直しは、「3年ごと見直し」制度に基づく2回目の見直しであり、平成27年改正以降4回目の改正に向けた見直しであるが、個情委は、今回初めて、保護法益を正面から取り上げ、それに沿った見直しを試みている。今後、（個情法全体及び個々の規制の）保護法益に照らした体系的な解釈・法執行が望まれるが、本稿がその一助となれば幸いである。

146）検討会では、終始、課徴金の対象とされるべき悪質な事案とは何かが問題とされたが、合意形成には至らず、検討会報告書は、課徴金制度を非裁量的なものとすることで、この問題自体を回避している。違反の悪質性は、当然、保護法益の侵害又は危殆化の程度によって判断されるべきであるが、検討会では、そのような議論は行われなかった。

147）検討会報告書は、注意懈怠を要件とすることを提案しているが、それが要件である限り、その判断はyes/noのデジタル（非連続的）なものとならざるを得ず、noとされた場合に課徴金額が直ちに0となることを考慮すると、注意懈怠がないと認められることはほとんどなくなってしまう可能性がある。

148）第287回委員会（令和6年6月3日）32頁〔宍戸常寿〕。

149）白石468頁、499頁。

情報法制研究所上席研究員
弁護士・情報処理安全確保支援士
那須　翔

2019年3月早稲田大学法学部卒業、2021年3月早稲田大学法科大学院法務研究科修了。2022年10月情報処理安全確保支援士登録、同年12月弁護士登録。G検定2024#4合格。情報法制学会、情報ネットワーク法学会、サイバーセキュリティ法制学会、金融法学会の各会員。

実務においては、個人情報保護、AIガバナンス、通信規制、金融規制（フィンテック）、セキュリティ・デジタルIDなどの法務を専門とする。論文として「電子計算機使用詐欺罪における「虚偽の情報」の解釈・適用」Law & Practice 17号（2024）がある。