参考資料２

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

個人情報保護委員会

【目次】

【凡例】

政令	個人情報の保護に関する法律施行令（平成15年政令第507号）
規則	個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第３号）
通則ガイドライン	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年個人情報保護委員会告示第６号）
平成27年改正法	個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成27年法律第65号）
令和２年改正法	個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第44号）
令和３年改正法	デジタル社会の形成を図るための関係法律の整備に関する法律（令和３年法律第37号）
委員会	個人情報保護委員会
GDPR	個人データの取扱いに係る自然人の保護及び当該データの自由な移転並びに指令95/46/ECの廃止に関する欧州議会及び欧州理事会規則（一般データ保護規則）（REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)）

第１　はじめに（中間整理の位置づけ等）

個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）は、平成 15 年（2003 年）に制定された後、平成 27 年（2015 年）、令和２年（2020 年）、令和３年（2021 年）と、国際的動向、情報通信技術の進展、新産業の創出・発展の状況等を踏まえた改正が行われてきた。このうち、令和２年改正法は、附則第 10 条において、「政府は、この法律の施行後三年ごとに、個人情報の保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、新個人情報保護法の施行の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。」としている。

委員会は、同規定を踏まえ、令和５年（2023 年）９月の第 255 回個人情報保護委員会及び同年 10 月の第 258 回個人情報保護委員会において、令和２年改正法及び令和３年改正法の施行状況を確認した上で、同年 11 月の第 261 回個人情報保護委員会において、いわゆる３年ごと見直しに関する検討を開始した。その後、令和６年（2024 年）２月の第 273 回個人情報保護委員会において「個人情報保護法　いわゆる３年ごと見直し規定に基づく検討項目」を公表し、関係団体や有識者からのヒアリングを実施するとともに、各検討項目について議論を重ねてきた。

本文書は、「中間整理」として、これまでの議論や検討を踏まえた現時点における委員会の考え方をまとめたものである。本文書は、パブリック・コメントに付すこととしており、そこで寄せられた意見を踏まえて最終的な方向性のとりまとめを行う予定である。また、パブリック・コメント終了後も、ステークホルダーと継続的な議論を行っていくものであり、こうしたプロセスを踏まえて、各検討項目の方向性を見直すことも想定されるものと考えている。また、本中間整理に挙げているものにとどまらず、今後提起された論点や検討項目についても、必要に応じて実態把握や影響分析なども行いながら、オープンな議論を続けていく必要があると考えている。

特に、課徴金、団体による差止請求制度や被害回復制度については、事業者、個人それぞれに与える影響が大きく、今後とも一層の意見集約作業が必要と考えられることから、ステークホルダーと議論するための場を設けつつ、令和６年（2024 年）末までを目途に議論を深めていくこととするが、更なる検討項目の追加等については、上記プロセス等の状況を踏まえて引き続き検討する。

第２　個別検討事項

１　個人の権利利益のより実質的な保護の在り方

情報通信技術等の高度化に伴い、大量の個人情報を取り扱うビジネス・サービス等が生まれる一方で、プライバシーを含む個人の権利利益が侵害されるリスクが高まっている。

破産者等情報のインターネット掲載事案や、犯罪者グループ等に名簿を提供する悪質な「名簿屋」事案等、個人情報が不適正に利用される事案も発生している。

こうした状況に鑑み、技術的な動向等を十分に踏まえた、実質的な個人の権利利益の保護の在り方を検討する必要がある。

⑴個人情報等の適正な取扱いに関する規律の在り方

ア　要保護性の高い個人情報の取扱いについて（生体データ）

【我が国の現状等】

現行法上、政令第１条第１号に規定する身体の特徴のいずれかを電子計算機の用に供するために変換した符号のうち、本人を認証することができるようにしたものは、個人識別符号に該当し、個人情報に該当する。なお、現行法において、このような生体データの取扱いについて、生体データであることに着目した特別の規律は設けられていない。

我が国における、生体データの取扱いに関連する社会的反響の大きかった事例として、次のようなものがある。

- 人流を把握し防災に活用する目的で、ある駅を中心とした駅ビルに多数のカメラを設置して通行人を撮影し、災害発生時等の安全対策に資する人流統計情報の作成が可能かを検証する実験を実施することを発表した事例
- 顔識別技術を有した防犯カメラを導入し、刑務所からの出所者・仮出所者を含む不審者等を検知するセキュリティ対策を、交通拠点において実施していた事例
- ある地区のスマートシティ化等を目的として、ある駅周辺に多数のAIカメラを設置し、人流データの取得・解析を開始することを発表した事例

欧州連合（EU）、アメリカ合衆国（カリフォルニア州）、中華人民共和国、インド共和国、ブラジル連邦共和国、オーストラリア連邦、大韓民国においては、自然人を一意に識別することを目的とする生体データは、センシティブデータに該当するとされている。センシティブデータの取扱いについては、一般的な個人データとは異なる特有の規律として、原則として本人同意の取得を要求する例や、本人にオプトアウト権を認める例がある。生体データの取扱い関連する執行事例も、各国において確認されている。

【考え方】

生体データは、長期にわたり特定の個人を追跡することに利用できる等の特徴を持ち得るものであり、特に、特定の個人を識別することができる水準が確保されている場合において、通常の個人情報と比較して個人の権利利益に与える影響が大きく、保護の必要性が高いと考えられる。他方、生体データは本人認証に広く利用されているほか、犯罪予防や安全確保等のために利用することも想

定されるものである。これを踏まえ、生体データの取扱いについて、諸外国における法制度なども参考にしつつ、特に要保護性が高いと考えられる生体データについて、実効性ある規律を設けることを検討する必要がある。この点について、関係団体からは、事業者の自主的な取組を促進すべきとの声もあるが、本人関与や安全管理措置等を通じた個人の権利利益の保護とのバランスを踏まえ検討を進める必要がある。

まず、現行法上、個人情報の利用目的については、「できる限り特定」しなければならないとされているが（法第 17 条第１項）、生体データの要保護性を踏まえると、生体データを取り扱う場合においては、例えば、どのようなサービスやプロジェクトに利用するかを含めた形で利用目的を特定することを求めることが考えられる。

また、個人の権利利益の保護という観点からは、生体データの利用について、本人がより直接的に関与できる必要がある。そのため、生体データの取扱いに関する一定の事項を本人に対し通知又は十分に周知することを前提に、本人による事後的な利用停止を他の保有個人データ以上に柔軟に可能とすることが考えられる。

このほか、必要となる規律の在り方について、事業者における利活用の実態やニーズ、運用の負担、利用目的の違いによる影響なども考慮して検討する必要がある。

イ　「不適正な利用の禁止」「適正な取得」の規律の明確化

【我が国の現状等】

現行法では、法第 19 条に「不適正な利用の禁止」が、法第 20 条１項に「適正な取得」が規定されている。法第 19 条にいう「違法又は不当な行為」とは、法その他の法令に違反する行為、及び直ちに違法とはいえないものの、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をいう。不正取得・不適正利用に該当する具体的な事例は、通則ガイドラインにおいて、６事例ずつ記載されている。

委員会が、不適正利用等に該当するものとして行政上の措置を講じた事案として、次のようなものがある。

- 官報に掲載されている破産手続開始決定を受けた個人の氏名や住所等の個人データを地図と紐づく形でインターネット上に公表した事案（以下「新破産者マップ事案」という。）について、個人データの提供の停止を求める命令を発出したもの
- 小売電気事業者が、電気事業法（昭和 39 年法律第 170 号）により禁止されているにもかかわらず、新規参入の小売電気事業者の顧客情報を含む個人データを取得した事案について、指導を行ったもの
- 名簿販売事業者が、販売先が、法に違反するような行為を行う者にも名簿を転売する転売屋だと認識していたにもかかわらず、意図的に販売先での名簿の用途を詳しく確認せず、転売屋に名簿を販売した事案について、指導を行ったもの

また、現行法の個人情報の取扱いに係る規律は、本人が自らの個人情報の提供等について、自ら判断し、選択できる状況にあることが前提となっていると考えられる。他方、本人にとって個人情報取扱事業者の提供する商品・サービス等が他の事業者により代替困難であるにもかかわらず、本人が当該個人情報取扱事業者による一定の個人情報の取扱いを許容することが当該商品・サービス等の提供の事実上の条件になっている場合等、個人情報取扱事業者と本人との関係によっては、本人にそのような選択を行うことが期待できない場合があり得る。

国内の他法令においても、代替困難と評価し得る者に対する主な規律として、デジタルプラットフォーム事業者、与信事業者、雇用主に対するものが存在する。委員会において対応した事案の中には、代替困難と評価し得る者による事案も存在する。また、社会的反響が大きかった事例として、学校において、生徒が装着したウェアラブル端末から、心拍数や睡眠時間等を把握しようとしたり、脈拍を計測して集中度を推測したりしていた事例がある（事例の詳細は９頁参照）。

このほか、個人関連情報[1]については、一定の場合における第三者提供のみが規律の対象となっており、具体的には、提供元では個人データに該当しないが、提供先において個人データとなることが想定される個人関連情報の第三者提供について、本人同意が得られていること等の確認が、提供元に義務付けられている。

他方、国内における裁判例には、インターネット上の掲示板において携帯電話番号を記載した投稿を行った事例において、携帯電話番号は、その性質上、不特定多数の第三者に開示されることを望まない情報であるなどとして、プライバシー侵害を認めたものがある。また、海外の執行事例においても、アメリカ合衆国において、大手 SNS 事業者が利用者から二段階認証用などとして取得した電話番号及びメールアドレスをターゲティング広告に利用したことが問題視された事例などがある。その他関連する国内の事例として、電話番号を用いて、宅配便事業者や通信事業者になりすました SMS によりメッセージを送信し、不正アプリのダウンロード等を行わせるものがある。

【考え方】

不適正な利用の禁止、適正な取得の規定については、個人の権利利益の保護により資するものとするとともに、事業者による予測可能性を高める観点から、適用される範囲等の具体化・類型化を図る必要がある。具体化・類型化に際しては、これまでに問題とされた事例等を踏まえて検討することが必要である。

また、現行法の個人情報の取扱いに係る規律は、本人が、自らの個人情報の提供等について、自らの自律的な意思により選択をすることが可能である状況にあることを前提としていると考えられる。他方、個人情報取扱事業者と本人との関係によっては、本人にそのような選択を行うことが期待できない場合があり得る。そのため、こうした場合において、本人との関係に照らして当然認められるべき利用目的以外の利用目的で個人情報を取得・利用することや、当然認めら

[1] 個人関連情報とは、「Cookie 等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴」や「メールアドレスに結び付いた、ある個人の年齢・性別・家族構成」等がこれに該当する。ただし、これらの情報が個人情報に該当する場合には、個人関連情報には該当しない。

れるべき利用目的の達成に真に必要な範囲を越えて個人情報を取得・利用すること等について、不正取得や不適正利用等の規律をどのように適用すべきか、継続的に検討する必要がある。

個人関連情報については、事業者が、電話番号、メールアドレス、Cookie ID など、個人に対する連絡が可能な情報を有している場合[2]には、個人関連情報の取扱いによりプライバシーなどの個人の権利利益が侵害される蓋然性が認められ、その侵害の程度・蓋然性は、事業者による利用の方法によっては、個人情報と同様に深刻なものになり得ると考えられる。そのため、このような場合について、不正取得や不適正利用等への対応の在り方を検討する必要がある。

(2)第三者提供規制の在り方（オプトアウト等）

【我が国の現状等】

個人情報取扱事業者は、原則として、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない（法第 27 条第１項本文）。ただし、第三者に提供される個人データについて、本人の求めに応じて提供を停止することとしている場合であって、その名称や住所、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること、本人の求めを受け付ける方法等について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、委員会に届け出たときは、本人の同意を得ることなく第三者に提供することができる（同条第２項）。これは、個人情報を含むデータベースを販売する事業者や、住宅地図等で個人情報を提供している事業者等を念頭に置いて設けられた規定であり、個人情報取扱事業者に対し一定の義務を加重することにより、個人データの積極的な流通を認め、保護と利用のバランスを図ろうとするものである（いわゆるオプトアウト届出制度）。同制度に関しては、次のとおり、過去の改正により規律の整備が行われてきた。

- 平成 27 年改正法により、不正取得された個人情報が、名簿業者等に転売されることを防止するため、第三者から個人データの提供を受ける際には、取得の経緯を確認することとされた。また、委員会による監督を強化するとともに、法に定める事項を事前に本人が容易に知り得る状態を確保するため、オプトアウト届出事業者は一定の事項を委員会に届け出ることとし、委員会がこれを公表することとされた。
- 令和２年改正法により、不正取得された個人データをオプトアウト規定によって提供することが禁止された。また、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る個人情報の利用が禁止された。

その後、特殊詐欺の認知件数、被害額、検挙件数・人員が増加傾向にあることを踏まえ、令和５年（2023 年）３月 17 日に、犯罪対策閣僚会議において「ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン」が策定され、政府は同プランに基づく施策を強力に推進することとされた。

---

[2] なお、仮名加工情報を取り扱う場合には、電話をかけ、郵便若しくは信書便により送付し、電報を送達し、ファクシミリ装置若しくは電磁的方法を用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報の利用を行ってはならないこととされている（法第 41 条第８項）。

同プランにおいては、犯罪者グループ等が高齢者等の資力等に関する個人情報等を用いて犯行に及んでいる実態等に鑑み、「実行を容易にするツールを根絶する」ための対策を講じることとされ、当該対策の一環として、法の的確な運用等による名簿流出の防止等の「闇名簿」対策の強化が求められた。また、個人情報を悪用した犯罪被害を防止するため、犯罪者グループ等にこうした名簿を提供する悪質な「名簿屋」、さらに個人情報を不正な手段により取得して第三者に提供する者に対し、あらゆる法令を駆使した取締り等を推進することとされた。

委員会は、同プランが策定されたことも踏まえ、オプトアウトの届出を行った事業者を対象に、個人情報の適正な取扱いがなされているかについて把握するための調査（実態調査）を行った。主な結果は次のとおりである。

- 届出事項を本人が容易に知り得る状態に置くことについて、「自社コーポレートサイトに掲載している。」「ホームページで公表している。」「社内の壁面に掲示している。」「検索出来るようにしている。」といった回答があった。
- 提供しようとするデータが、法第 20 条第 1 項に違反して取得されたものでないことの確認方法について具体的な内容が不明確な回答が約２割あった。
- 個人データの第三者提供を受けているオプトアウト届出事業者のうち、提供元の事業者が法第 20 条第１項の「偽りその他不正の手段」に該当しない手段により個人情報を取得していることの確認方法について、回答に具体性がない又は無回答となっている事業者が約２割あった。
- オプトアウトにより個人データを提供するに当たって、提供先が提供を受けたデータを「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」で利用しないことを確認していないとの回答が約３割あった。オプトアウトによる個人データを提供するに当たり、提供先に対して、本人確認手続等を実施していないとの回答が約３割あった。

本実態調査により、取得や提供に際して不適切な対応があった事案が見られたことを踏まえ、委員会として指導等の対応を行った。当該事案の概要は次のとおりである。

- 販売先が、法に違反するような行為を行う者にも名簿を転売する転売屋だと認識していたにもかかわらず、意図的に販売先での名簿の用途を詳しく確認せず、転売屋に名簿を販売していた。また、個人データの第三者提供記録も作成していなかった事案
- 個人データの第三者提供記録を作成していなかった事案
- 個人データの第三者提供記録を作成していなかったことに加え、第三者から個人データの提供を受けるに際し、当該第三者の住所について、確認を行わなかった事案

その他、顧客情報又は住民等の情報、住民基本台帳のデータを、それぞれ従業員ないし委託先の職員が持ち出し、名簿業者に売却した事案もみられる。

加えて、委員会が運営する個人情報保護法相談ダイヤル[3]に対して、オプトアウト届出事業者に係る質問・相談等が寄せられている。当該質問・相談等において問題とされた事例には次のようなものがある。

---

[3] 委員会は、法第 169 条に基づき、法に関する一般的な解釈や個人情報保護制度に関する一般的な質問に

・ 名簿の販売が許容されていること自体が問題ではないかとしている事例
・ 名簿の入手先・取得元の問合せや第三者提供記録の開示を拒否された、あるいは適切な回答がされていない事例
・ 提供停止を求めるための連絡先が不明又は電話がつながらないなどの理由により停止してもらえなかった、あるいは一旦停止したものの、その後提供が再開された事例
・ 提供停止等を求めたところ、他の個人情報の提供、サービス登録、手数料支払等の条件を付けられた事例

【考え方】

オプトアウト届出事業者は、提供先の利用目的や身元等について、その内容や真偽を積極的に確認する義務まではないことから、明確に認識しないまま意図せず犯罪グループに名簿を提供してしまうことが生じ得る。そこで、一定の場合には提供先の利用目的や身元等を特に確認する義務を課すことについて検討する必要がある。その際、確認義務の要件についての検討や、住宅地図等を広く市販する場合など規律の在り方についても検討が必要である。

また、不正に名簿等を持ち出した者が、当該名簿等により利益を得る有力な方法として、オプトアウト届出事業者への販売が想定される。そのため、オプトアウト届出事業者には、取得元における取得の経緯や取得元の身元等の確認について、より高度の注意義務を課すことが考えられる。具体的には、一定の場合には取得元の身元や取得の適法性を示す資料等を特に確認する義務を課すことについて検討する必要がある。その際、確認義務の要件や対象の類型化についての検討が必要である。

さらに、本人が、オプトアウト届出事業者によって個人情報が提供されており、かつ、当該提供の停止を求めることができることを確実に認識できるようにするための措置など、本人のオプトアウト権行使の実効性を高めるための措置について、継続して検討する必要がある。

(3)こどもの個人情報等に関する規律の在り方

【我が国の現状等】

現行法上、こどもの個人情報の取扱い等に係る明文の規定は基本的になく、次の記載があるのみである。

・ 法第 32 条第２項以下の開示等の請求等及び法第 76 条第１項の開示請求については、未成年者の法定代理人によってすることができるとされている（政令第 13 条第１号、法第 76 条第２項）。
・ 「本人の同意」を得ることが求められている場面（目的外利用、要配慮個人情報の取得、第三者提供等）について、個人情報の取扱いに関して同意したことによって生ずる結果を未成年者が判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要があり（通則ガ

回答するとともに、個人情報等の取扱いに関する苦情の申出についての必要なあっせん及びその処理を行う事業者への協力等を行うための窓口として、個人情報保護法相談ダイヤルを設置・運用している。

イドライン)、一般的には、12 歳から 15 歳までの年齢以下のこどもの場合には法定代理人等から同意を得る必要があるとされている(「個人情報の保護に関する法律についてのガイドライン」に関する Q&A。以下「Q&A」という。)。

国際的な枠組みにおいては、児童の権利に関する条約に関して、2021 年３月２日に国連・子どもの権利委員会が公表した「デジタル環境との関連における児童の権利についての一般的意見 25 号」や 2021 年５月 31 日に OECD が改訂した「デジタル環境下のこどもに関する OECD 勧告」において、こどもの未熟さや脆弱性を踏まえ、プライバシーの保護のために必要な措置を求めている。

海外の法制度においては、EU、英国、アメリカ合衆国、中華人民共和国、大韓民国、ブラジル連邦共和国、インド共和国、インドネシア共和国においてこどもの個人情報等に関する規律が存在している。また、カナダにおいて制定が検討されている CPPA（Consumer Privacy Protection Act）の草案においては、未成年者の個人情報がセンシティブデータに該当する旨の規定が置かれている。各国法制における規律の在り方は、国・地域によって様々であるが、主として次のようなケースが確認された。

- こどもの個人情報等をセンシティブデータに分類した上で特別な規律の対象とするケース
- センシティブデータに関する規律とは別に、こどもの個人情報等に特有の規律を設けるケース
- オンライン分野等一定の分野に限定した上で、包括的な個人情報保護法令とは異なる法令において、こどもの個人情報等に関する規律を設けるケース

また、これらの規律を踏まえた執行事例も各国において存在しており、多額の制裁金の支払命令に至った事例も見られる。

国内においても、こどもの個人情報等に関する社会的反響が大きかった事例が見られる。全寮制の学校において、全生徒にウェアラブル端末を購入してもらい、心拍数、血圧、睡眠時間、入退室履歴等を把握し、生徒の健康管理に役立てる取組を実施することが報道された事例があった。また、別の学校では、生徒の手首に装着した端末で脈拍を計測して、授業中の集中度を測定する実証研究を行い、教員がそのデータを基に授業の振り返り等に活用することとしていた事例があった。

委員会においては、令和６年（2024 年）２月に、大手学習塾に対して、大量の児童の個人データを保有及び管理しているにもかかわらず、人的なリソース不足を理由にコンプライアンス及びリスク管理に関する部署を設置していなかった等の取扱いに問題があったとして、必要となる安全管理措置を講じるよう、指導を行った。

個人情報保護法相談ダイヤルに対しても、こどもの個人情報等に係る質問、相談等が寄せられている。特に頻度の多い事例としては、事業者において第三者提供や目的外利用等本人の同意が必要な行為を行う予定がある際に、法の規定上は「本人の同意」とあるが、本人が未成年である場合にはどう対応すればよいのか、といった事例が挙げられる。このほか、見知らぬ事業者によるこどもの個人

情報等の利用を不安視する相談や、こどもの個人情報等の開示や削除の依頼をしているにもかかわらずこれに応じない事業者に関する相談もあった。

【考え方】

こどもの個人情報の取扱いに係る規律については、こどもの脆弱性・敏感性及びこれらに基づく要保護性を考慮するとともに、学校等における生徒の教育・学習に関するデータの有用性も考慮する必要がある。これを踏まえ、主要各国においてこどもの個人情報等に係る規律が設けられており、執行事例も多数見られることも踏まえ、こどもの権利利益の保護という観点から、規律の在り方の検討を深める必要がある。

他方で、第三者が公開したこどもの個人情報を取得する場合などにおいては、取得した情報にこどもの個人情報とこども以外の者の個人情報が含まれている場合や、こどもの個人情報が含まれているかが明らかでない場合があり得ることから、こうした場合における事業者の負担を考慮する必要がある。

ア　法定代理人の関与

現行法上、原則として本人同意の取得が必要とされている場面（目的外利用（法第 18 条第２項）、要配慮個人情報の取得（法第 20 条第２項）、個人データの第三者提供（法第 27 条第１項、第 28 条１項）、個人関連情報の第三者提供（法第 31 条第１項）など）において、こどもを本人とする個人情報について、法定代理人の同意を取得すべきことを法令の規定上明確化することを検討する必要がある。

また、本人に対する通知等が必要となる場面（利用目的の通知（法第 21 条第１項）、本人から直接書面に記載された個人情報を取得する場合における利用目的の明示（同条第２項）、漏えい等に関する本人への通知（法第 26 条第２項）など）においても、こどもを本人とする個人情報について、法定代理人に対して情報提供すべきことを法令の規定上明文化することを検討する必要がある。

イ　利用停止等請求権の拡張

現行法上、利用停止等請求権を行使できる場面は、保有個人データについて違法行為があった場合等限定的であるが、こどもの要保護性を踏まえると、こどもを本人とする保有個人データについては、他の保有個人データ以上に柔軟に事後的な利用停止を認めることについて検討する必要がある。ただし、取得について法定代理人の同意を得ている場合等、一定の場合においてはその例外とすることも考えられる。

ウ　安全管理措置義務の強化

重大なこどもの個人情報の漏えい事件が国内で発生しており、委員会においても前述の大手学習塾に対する指導に際して「こどもの個人データについては、こどもの「安全」を守る等の観点から、特に取扱いに注意が必要であり、組織的、人的、物理的及び技術的という多角的な観点からリスクを検討し、必要かつ適切な安全管理措置を講ずる必要がある」旨述べているところである。そこで、こどもの個人データについて安全管理措置義務を強化することがあり得る。

エ　責務規定

上記アからウにかかわらず、各事業者の自主的な取組の促進という観点からは、こどもの個人情報等の取扱いについては、こどもの最善の利益を優先し特別な配慮を行うべき等、事業者等が留意すべき責務を定める規定を設けることも検討する必要がある。

オ　年齢基準

こどもの個人情報等の取扱いに係る年齢基準の考え方については、国内外の法制度において様々な年齢基準が設けられていることや、対象年齢によっては事業者等の負担が大きくなることも考慮する必要があるが、対象とするこどもの年齢については、Q&A の記載や GDPR の規定の例などを踏まえ、16 歳未満とすることについて検討を行う。

(4)個人の権利救済手段の在り方

【我が国の現状等】

個人情報保護法相談ダイヤル（民間部門）では、令和５年度（2023 年度）において、22,103 件の相談を受け付けた。当該相談のうち、苦情に係る受付件数は 6,941 件であり、そのうち開示等に係るものが 1,031 件あった。

本人は、当該本人が識別される保有個人データについて、法の規定に違反する場合や、本人の権利又は正当な利益が害されるおそれがある場合等に、個人情報取扱事業者に対して、当該本人が識別される保有個人データの利用停止等又は第三者提供の停止を請求することができる（法第 35 条）。

令和２年（2020 年）２月から３月に実施されたアンケート調査では、「保有個人データの利用停止・消去又は第三者提供の停止に関する請求を過去一年間で約何件受けましたか？」との質問に対して、回答のあった事業者（全 158 社）のうち 47%が「10 件未満」と回答した。

この点、消費者法分野においては、消費者被害には同種の被害が拡散的に多発するという特性がある一方で、消費者個人としては、被害の認識をしていないこと、救済を求めて請求できることを知らないこと、事業者との情報の質及び量並びに交渉力に格差があること、費用・労力の負担等により、自身の被害回復のための行動を採りにくく、「泣き寝入り」となりやすいことなどを踏まえ、内閣総理大臣が認定した消費者団体が、消費者に代わって事業者に対して訴訟等をすることができる制度があり、消費者契約法（平成 12 年法律第 61 号）には、適格消費者団体による差止請求の枠組みが規定されている。適格消費者団体とは、消費者契約法に定める要件を満たし、差止請求を行うのに必要な適格性を有するとして、内閣総理大臣が認定した消費者団体のことであり、「不当な勧誘」、「不当な契約条項」、「不当な表示」などの事業者の不当な行為をやめるよう求めることができる。差止請求の対象は、事業者が不特定かつ多数の消費者に対して消費者契約法、不当景品類及び不当表示防止法（昭和 37 年法律第 134 号。以下「景品表示法」という。）、特定商取引に関する法律（昭和 51 年法律第 57 号）等に規定された不当な行為を行っている、又は、行うおそれがあるときとされている。

適格消費者団体は、令和６年（2024 年）２月現在、全国に 26 団体あり、適格消費者団体による差止請求は、制度の運用開始後、令和５年（2023 年）３月末までの間に 966 件行われ、うち 85 件の差止請求訴訟が提起されている。なお、法令上の差止請求権の行使とは別に、適格消費者団体が事業者に対し、個人情報の取扱いの改善を求めた例もある。

現行法には、適格消費者団体の差止請求についての規定は設けられていない。また、差止請求を行うのに必要な適格性を有する団体を認定する制度も設けられていない。他方、委員会が行政上の対応を行った事案の中には、その取扱いが問題となった個人情報に係る本人が不特定かつ多数と評価し得るものがある。

【考え方】

法の規定に違反する個人情報の取扱いに対する抑止力を強化し、本人に生じた被害の回復の実効性を高めるという観点からは、適格消費者団体を念頭に置いた、団体による差止請求制度や被害回復制度[4]の枠組みは有効な選択肢となり得る。

このうち、差止請求制度については、法に違反する不当な行為を対象行為とすることを検討すべきである。差止請求の実効的な運用のためには、次の課題が指摘されている一方で、差止請求は個人の権利利益保護の手段を多様化する、委員会の監視・監督機能を補完し得るとの指摘もあることから、継続して検討する必要がある。

- 専門性の確保（法に精通した人材を各適格消費者団体が確保しているとは限らないため、研修等の実施や、制度導入初期段階での専門家確保のための施策が必要と考えられる。）
- 端緒情報等の共有・立証等における考慮（委員会が取得している情報のうち重大案件と考えられるものについて、事業者名を特定して適格消費者団体に提供できると、制度が効果的に機能すると考えられる。また、事業者の応答を促す仕組み等についても検討すべき。）
- 報告、監督窓口の一本化（年次の報告先等が２箇所となれば適格消費者団体の負担となる。）
- 資金を含む団体への援助（適格消費者団体は限られた資金の下ボランティアベースで運営されている団体が大多数。）

もう一方の被害回復制度については、差止請求制度の課題に加え、個人情報の漏えいに伴う損害賠償請求は極端な少額大量被害事案となる（過去の裁判例等を踏まえると、認容被害額は数千円から数万円程度と考えられる。）こと、立証上の問題があることが課題と考えられることから、更に慎重な検討が必要である。

他方で、団体による差止請求や被害回復の枠組みについては、関係団体からのヒアリングにおいて、その導入について強く反対との意見があったところであり、法に違反する行為や不法行為を対象とする場合であっても、萎縮効果の懸念が示されていることから、事業者の負担と個人の権利利益の保護とのバランス

---

[4] 消費者の財産的被害等の集団的な回復のための民事の裁判手続の特例に関する法律（平成 25 年法律第 96 号。以下「消費者裁判手続特例法」という。）に基づき、特定適格消費者団体が、多数の消費者に共通して生じた被害について、訴訟を通じて集団的な被害の回復を求めることができるとするもの。

を踏まえつつ、その導入の必要性を含めて多角的な検討を行っていく必要がある。

２　実効性のある監視・監督の在り方

破産者等情報のインターネット掲載事案、犯罪者グループ等に名簿を提供する悪質な「名簿屋」事案、転職先へのデータベースの ID・パスワードの不正提供事案等、個人情報が不適正に利用される事案や、同一事業者が繰り返し漏えい等を起こす事案が発生している。こうした悪質・重大な事案に対する厳罰化、迅速な執行等、実効性のある監視・監督の在り方を検討する必要がある。

(1)課徴金、勧告・命令等の行政上の監視・監督手段の在り方

【我が国の現状等】

現行法上の監視・監督の流れとしては、まず、個人情報保護法相談ダイヤル、個人情報取扱事業者からの漏えい等報告、その他メディア情報等の外部の情報源から、監視・監督に係る情報を得ている。

こうした情報を踏まえ、必要に応じて報告徴収・立入検査を行う。その結果により、指導・助言、勧告を行い、勧告を受けた個人情報取扱事業者等が正当な理由なく勧告に係る措置をとらなかった場合において、個人の重大な権利利益の侵害が切迫していると認められるときは、命令を発出する、という枠組みになっている。個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるとき等の一定の要件を満たす場合には、勧告を経ることなく命令（いわゆる緊急命令）を発出することも可能となっている。

この命令に違反した場合には、法第 178 条により罰則の対象となる。法定刑は、行為者は１年以下の懲役又は 100 万円以下の罰金であり、法第 184 条の両罰規定により、法人等は１億円以下の罰金刑の対象となる。また、委員会への虚偽報告等についても、法第 182 条により行為者は 50 万円以下の罰金刑の対象となるほか、法第 184 条の両罰規定により、法人も 50 万円以下の罰金刑の対象となる。

ア　課徴金制度

法令に基づき賦課される金銭としては、法第 179 条に規定する個人情報データベース等不正提供等罪等に見られる罰金、科料、過料のほか、課徴金がある。

国内の他法令における課徴金制度としては、我が国では、私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号。以下「独占禁止法」という。）が昭和 52 年（1977 年）に課徴金制度を導入したのを皮切りに、金融商品取引法（昭和 23 年法律第 25 号）、公認会計士法（昭和 23 年法律第 103 号）、景品表示法、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（昭和 35 年法律第 145 号）に順次導入されている。また、例えば、独占禁止法については、制度導入後累次の改正により、対象行為の拡大、算定率の引上げ等を行っており、違反行為を抑止するため、違反行為に基づく不当利得相当額をベースとしつつ、不当利得相当額以上の金銭を徴収する仕組みとされている。

法の過去の改正においても、課徴金に関する議論がされている。平成 27 年改正法の検討時には、制度見直し方針の段階において、第三者機関に行政処分の権限を付与するとともに罰則の在り方を検討するとされた上で、制度改正大綱においては、課徴金制度の導入について、引き続き検討することとされた。また、令和２年改正法の検討時には、制度改正大綱において、「我が国の法体系、執行

の実績と効果、国内外事業者の実態、国際的な動向を踏まえつつ、引き続き検討を行っていく」とされた。

加えて、法案審議においては、参議院の内閣委員会における附帯決議で、「違反行為に対する規制の実効性を十分に確保するため、課徴金制度の導入については、我が国他法令における立法事例や国際的な動向も踏まえつつ引き続き検討を行うこと」とされた。

委員会が行政上の対応を行った、個人データの違法な第三者提供・不適正利用等に関連する事案として、次のようなものがある。

- 人材サービス事業者及びその関連事業者が、新卒向け就職情報サービスにおいて、いわゆる内定辞退率を提供するサービスを本人の同意を得ずに同サービスの利用企業へ提供する等した事案について、両事業者に対して勧告等を行ったもの。
- 新破産者マップ事案について、勧告、命令を順次実施し、さらに、これに係る措置が取られなかったことを理由に刑事告発を実施したもの。
- 海外プラットフォーム事業者のサービスの利用者が、ソーシャルプラグインであるボタンが設置されたウェブサイトを閲覧した場合、当該ボタンを押さなくとも、ユーザーID、アクセスしているサイト等の情報が同社に自動で送信されていた事案について、指導を行ったもの。
- 名簿販売事業者が、販売先が、法に違反するような行為を行う者にも名簿を転売する転売屋だと認識していたにもかかわらず、意図的に販売先での名簿の用途を詳しく確認することなく、転売屋に名簿を販売した事案について、指導を行ったもの。

委員会が行政上の対応を行った、事業者が漏えいの可能性を認識したにもかかわらず速やかに適切な措置を講じなかった事案として、民間事業者 30 社、独立行政法人１機関及び 38 の地方公共団体から委託を受けたコールセンターサービス事業者が行っていたコールセンター事業に関し、コールセンター業務で用いるシステムの保守運用を当該コールセンターサービス事業者から委託されたその関連事業者に所属し、システム保守運用業務に従事していた者が、委託元の顧客又は住民等に関する個人データ等を、長期にわたり反復的に不正に持ち出した事案がある。同事案について、委員会は、当該コールセンターサービス事業者及び当該関連事業者に対して、組織的安全管理措置の不備の是正のために必要な措置をとるよう勧告を実施したほか、指導、報告徴収を実施している。

委員会が行政上の対応を行った、指導を受けたにもかかわらず速やかに適切な措置が講じられなかった事案として、タクシー関連事業者が、タクシー車内に設置したタブレット端末付属のカメラを用いてタクシー利用者の顔画像を撮影して広告配信に利用していたが、その旨をタクシー利用者に対して十分に告知していなかった事案がある。同事案について、委員会は、タクシー利用者に対する分かりやすい説明の徹底等について指導を実施したが、改善策が実施されていなかったことが判明したことから、再度の指導を実施している。

個人情報の不適切な取扱いについて、金銭的不利益を課す行政上の措置を持つ外国制度として、次のようなものがある。

- EU は、GDPR の多くの条項が制裁金の対象となっており、違反状況に応じて、1,000 万ユーロ又は直前の会計年度における全世界総売上高の２％のうち

いずれか高い方、2,000 万ユーロ又は直前の会計年度における全世界総売上高の４％のうちいずれか高い方を上限として制裁金の額が算定される。英国の UK GDPR（UK General Data Protection Regulation）にも同様の規定が置かれている。

- アメリカ合衆国の連邦レベルでは、FTC 法（Federal Trade Commission Act）第５条が規定する「不公正・欺瞞的行為又は慣行」に当たる行為が民事制裁金の対象とされている。現在、連邦レベルの包括的な個人情報保護法制（連邦法）として制定が検討されている ADPPA（American Data Privacy and Protection Act）や APRA（American Privacy Rights Act）の草案（2024 年４月公表）においても、これらの法違反が FTC 法第５条違反とみなされる旨が規定されている。
- カリフォルニア州では、個人情報の販売・共有規制等に違反する行為が民事制裁金の対象とされている。
- カナダでは、現行法である PIPEDA（Personal Information Protection and Electronic Documents Act）においては、金銭的不利益を課す行政上の措置に係る規定は置かれていないものの、現在検討中の CPPA（Consumer Privacy Protection Act）においては、同法に定める規律に違反する場合において制裁金を課すことができる旨の規定が置かれている。
- 中華人民共和国、大韓民国においても、制裁金、課徴金の規定が置かれており、大韓民国については、事業者の全体売上高の３％以下の範囲で、課徴金額の算定が行われることとされている。

諸外国におけるこれらの規律については、多額の制裁金を課している執行事例も確認されている。

イ　勧告・命令の在り方

法第 148 条第２項において「勧告を受けた個人情報取扱事業者等が正当な理由がなくてその勧告に係る措置をとらなかった場合」と規定されているとおり、個人情報取扱事業者の義務違反の是正については、基本的に命令に勧告を前置することとされている。新破産者マップ事案については、半年を要して勧告、命令、告発という順次の対応に至った。

このような勧告前置の例外として、法第 148 条第３項に規定される緊急命令が存在する。もっとも、緊急命令の対象は一部の義務違反に限定されており、かつ、個人の重大な権利利益の侵害が現に発生していること等の要件も加重されている。

勧告・命令は、いずれも、法の規定に違反した「当該個人情報取扱事業者等」に対して行うものとされている。そのため、個人情報取扱事業者が、法に違反する個人情報の取扱いを第三者に委託している場合や、法に違反して個人情報を取り扱うに当たって第三者の提供するサービスを利用している場合において、当該第三者自身が法の規定に違反した「当該個人情報取扱事業者等」に当たらない場合は、当該第三者に対して直接勧告・命令を行うことは困難である。

勧告・命令は、いずれも、「当該違反行為の中止その他違反を是正するために必要な措置」をとるよう求めるものとされている。委員会は、これまで、法に違反する個人情報の取扱いを行った個人情報取扱事業者に対して、利用目的の通

知、公表等を適切に行うことや、適切な安全管理措置を講じるための組織体制を整備すること等を求めてきている。

【考え方】

ア　課徴金制度

課徴金制度については、関係団体からのヒアリングで強い反対意見が示されていることに加え、我が国の他法令における導入事例や国際的動向、個人の権利利益保護と事業者負担とのバランスを踏まえ、その導入の必要性を含めて検討する必要がある。

課徴金制度を導入する必要があると考えられる場合には、次のような論点を整理する必要がある。

- 課徴金賦課の対象となる違法行為類型（現行法の指導・勧告・命令のみでは違反行為により得た利得が事業者の元に残ることとなり、事業者による個人の権利利益の侵害を効果的に抑止できないことを前提に、個人データの違法な第三者提供等の違反行為によって不当な利得を得ている場合や、個人データの漏えい等が発生している可能性を認識したにもかかわらず、適切な措置を講じることを怠る等の悪質な違反行為により、本来なすべき支払を免れた場合等について検討することが必要である。）
- 課徴金の算定方法（例えば、個人データを販売することを通じて違法に第三者に提供した場合については、販売による売上という不当な利益が生じている点に着目することが考えられる。他方、悪質な安全管理措置義務違反の場合には、本来なすべき支払を免れた結果として、事業活動から得られる利益が増加している点に着目することが考えられる。）
- 課徴金の最低額の設定、一定の要件を満たした場合の課徴金の加減算等

イ　勧告・命令の在り方

勧告・命令に関しては、個人情報取扱事業者等による法に違反する個人情報等の取扱いにより個人の権利利益の侵害が差し迫っている場合に直ちに中止命令を出すことの必要性や、法に違反する個人情報等の取扱いを行う個人情報取扱事業者等のみならず、これに関与する第三者に対しても行政上の措置をとることの必要性、法に違反する個人情報等の取扱いの中止のほかに個人の権利利益の保護に向けた措置を求めることの必要性の有無や手続保障など、その法制上の課題等について検討すべきである。

⑵刑事罰の在り方

【我が国の現状等】

現行法上、個人情報の不適切な取扱いについて、直接罰則が適用される規定（いわゆる直罰規定）は、法第 176 条、第 179 条、第 180 条、第 181 条及び第 184 条である。令和２年改正法においては、これらの規定のうち個人情報データベース等不正提供等罪（法第 179 条）について、法人両罰規定（第 184 条第１項第１号）の法定刑を引き上げた一方、行為者に対する罰則については、罰則が創設された平成 27 年改正法の施行（平成 29 年（2017 年）５月）から十分な時間が経過していないことも踏まえ、法定刑を維持することとされた。

昨今、個人データの取扱いに関し、内部的な不正行為に起因する悪質な事例が増加している傾向があるものと考えられる。例えば、①個人情報取扱事業者の元従業者が、元勤務先が管理する名刺情報管理システムのログイン認証情報を不正に転職先の従業者に提供し、同システムを第三者が利用可能な状態に置いた事例や、②大手学習塾の元塾講師が当該学習塾の児童の個人情報を SNS のグループチャットに投稿したとされる事例が発生しており、①、②ともに個人情報データベース等不正提供等罪等により各行為者が起訴され、有罪が確定している。また、個人データが不正に取り扱われ、個人の権利利益が侵害されるおそれが生じた事例も見られるところであり、例えば、個人情報取扱事業者の従業者が、関係法令に違反し、又はその趣旨に反するにもかかわらず、グループ会社が管理していた個人情報データベース等から個人データを取得し、当該個人情報取扱事業者の業務に係る営業活動等のために利用した事例がある。

個人情報の不正取得の事例も多く発生している。令和５年度（2023 年度）に法第 26 条第１項に基づき報告された漏えい等の報告のうち、規則第７条が定める報告義務の類型において、２番目に多く発生した類型は、不正アクセスや従業員による持ち出し等、不正の目的をもって行われたおそれのある個人データの漏えい等であり（同条第３号）、その件数は 574 件に上る。また、委員会の個人情報保護法相談ダイヤルに対しても、個人情報の不正取得行為に係る相談も寄せられている。加えて、行政機関が実施する調査であるかのような紛らわしい説明をして、個人情報等を聞き出す、いわゆる「かたり調査」のトラブルも発生している。

【考え方】

個人情報が不正に取り扱われた悪質事案の類型が様々であることを踏まえ、法の直罰規定がこれらの事案を過不足なく対象としているかを検証し、その処罰範囲について検討するとともに、法定刑の適切性についても検討する必要がある。

さらに、個人情報の詐取等の不正取得が多数発生している状況を踏まえ、こうした行為を直罰規定の対象に含めるべきかについても検討する必要がある。

(3)漏えい等報告・本人通知の在り方

【我が国の現状等】

現行法上、法第 26 条第１項に基づく漏えい等報告は、規則第７条各号に該当する事態について、速報及び確報に分けて行うこととされている。漏えい等報告の趣旨は、委員会が事態を早急に把握し、必要な措置を講ずることができるようにすることにあり、委員会は、漏えい等報告を受けた内容を踏まえ、関係する法令やガイドラインの説明を行いつつ、報告事項の記載について不明点等を確認し、個人情報取扱事業者に対し、本人通知義務を履行させ、再発防止に向けた安全管理措置義務に係る指導等を行っている。特に、速報を受領した段階においては、事案の規模や概要を把握して、事案の軽重を踏まえて今後の調査方針や権限行使の方向性について検討し、また、必要に応じて漏えい等事態が発生して間もない段階で個人情報取扱事業者として対応すべきことを助言し、個人情報取扱事業者における調査の一般的な手法やセキュリティに関する情報提供等を実施

している。さらに、不正アクセス事案の場合、個人情報取扱事業者に対し、警察など関係機関への連絡を行うこと等も助言している。

また、委員会への報告を要する事態が生じた場合には、本人への通知も行う必要がある。本人への通知の趣旨は、通知を受けた本人が漏えい等の事態を認識することで、その権利利益を保護するための措置を講じられるようにすることにある。本人通知は原則として本人に直接知らせる必要があるが、「本人への通知が困難な場合」には事案の公表を含む代替措置をとることが可能とされている。

委員会への漏えい等報告については、①概要、②漏えい等が発生し、又は発生したおそれがある個人データの項目（規則第７条第３号に定める事態については、同号に規定する個人情報を含む。以下同じ。）、③漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数、④原因、⑤二次被害又はそのおそれの有無及びその内容、⑥本人への対応の実施状況、⑦公表の実施状況、⑧再発防止のための措置、⑨その他参考となる事項を報告する必要がある。ただし、速報時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる。

本人へ通知すべき事項は、上記漏えい等報告における報告事項のうち、①概要、②漏えい等が発生し、又は発生したおそれがある個人データの項目、④原因、⑤二次被害又はそのおそれの有無及びその内容、⑨その他参考となる事項に限られる。

なお、現行法上、「個人データ」が違法に第三者に提供された場合[5]、委員会に対する報告及び本人通知を行う義務は存在しない。

令和２年改正法の施行により、令和４年度（2022 年度）から漏えい等報告が義務化されたこと等により、漏えい等報告の件数は増加しており、令和５年度（2023 年度）は 12,120 件となっている[6]。同一の事業者において繰り返し漏えい等が発生している事例も存在する。

漏えい等した個人データに係る本人の数は多くの事案において 1,000 人以下である[7]ものの、50,000 人超という非常に大規模な個人の権利利益の侵害に繋がるケースも存在する[8]。

具体的には、漏えい等した個人データに係る本人の数が 1,000 人以下の事案が全体の 96.0%（11,635 件）を占めており、中でも、漏えい等した個人データに係る本人の数が１人の事案が全体の 84.0%（10,184 件）を占めている。また、漏えい等した個人データに係る本人の数が２～10 人、11～100 人及び 101～1,000 人の事案が、それぞれ、全体の 7.6%（918 件）、2.8%（341 件）及び 1.6%（192 件）を占めている。漏えい等した個人データに係る本人の数が１人の事案としては、病院や薬局における要配慮個人情報を含む書類の誤交付又は紛失や、クレジットカードの誤送付などが多い。

---

[5] 個人情報取扱事業者が自らの意図に基づき個人データを第三者に提供する場合は、漏えいに該当しない（通則ガイドライン 3-5-1-2）。

[6] 令和元年度（2019 年度）：4,520 件、令和２年度（2020 年度）：4,141 件、令和３年度（2021 年度）：5,846 件、令和４年度（2022 年度）：7,685 件、令和５年度（2023 年度）：12,120 件

[7] 令和５年度（2023 年度）：11,635 件（全体の 96.0%）

[8] 令和５年度（2023 年度）：61 件（全体の 0.5%）

漏えい等の原因は、誤交付、誤送付等のいわゆるヒューマンエラーによる事案が多い[9]ものの、不正アクセスによるものも一定程度存在する[10]。不正アクセスを原因とする事案の中には、個人データに係る本人の数が 100 万人を超える漏えいのおそれが生じたものもあった。

報告義務該当事由の割合についてみると、要配慮個人情報を含むものが全体の 89.7%を占めている。

関係団体等からは、「制度の趣旨・目的に照らしつつ、リスクベースアプローチによる合理的な範囲に報告対象を絞り込むなど、現在の報告・通知の在り方を見直すべき」として、漏えい等報告及び本人通知の負担軽減を要望する声が上がっている。

GDPR は、個人データ侵害（personal data breach）が発生した場合に、原則として、各加盟国のデータ保護当局に対して通知を行うことを義務付けている[11]。また、個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、データ主体に対し、不当な遅滞なく通知することを義務付けている。

【考え方】

ア　漏えい等報告

漏えい等報告及び本人通知に関し、漏えい等報告の件数は、令和４年度（2022 年度）から漏えい等報告が義務化されたこと等により、令和元年度（2019 年度）以降全体として増加傾向にある一方で、関係団体等からはこれらの義務が事業者の過度な負担になっているという意見が示されている。

そこで、こうした意見も踏まえつつ、委員会がこれまでに受けた漏えい等報告の内容を検証した上で、上記制度の趣旨を損なわないようにしつつ、個人の権利利益侵害が発生するリスク等に応じて、漏えい等報告や本人通知の範囲・内容の合理化を検討すべきである。

この点、①上記のように、委員会がこれまでに受けた漏えい等報告を件数ベースでみると、漏えいした個人データに係る本人の数が１名である誤交付・誤送付案件が大半を占めているが、このようなケースは、当該本人にとっては深刻な事態になり得るものであり、本人通知の重要性は変わらないものの、本人通知が的確になされている限りにおいては、委員会に速報を提出する必要性が比較的小さい。また、②漏えい等又はそのおそれを認識した場合における適切な対処（漏えい等が生じたか否かの確認、本人通知、原因究明など）を行うための体制・手順が整備されていると考えられる事業者については、一定程度自主的な取組に委ねることも考えられる。そこで、例えば、体制・手順について認定個人情報保護団体などの第三者の確認を受けることを前提として、速報については、一定の範囲でこれを免除し、さらに①のようなケースについては確報について一定期間ごとの取りまとめ報告を許容することも考えられる。

---

[9] 令和５年度（2023 年度）で誤交付と誤送付を合わせて 5,708 件、全体の約 81%。

[10] 令和５年度（2023 年度）で 443 件、全体の 6.3%。

[11] 2022 年に各国当局が受領した漏えい等報告の件数は、ドイツ連邦共和国：10,614 件、フランス共和国：4,088 件、アイルランド：5,828 件、イタリア共和国：1,351 件、英国：9,146 件。

また、関係団体からは、いわゆる「おそれ」要件についての要望も示されている。「おそれ」については、個人の権利利益を害する可能性等を勘案してより合理的と考えられる場合に報告や本人通知を求めることが適当であるとも考えられるが、その具体的な当てはめについては、現実の事例に応じて精査する必要がある。事業者の協力も得ながら、実態を明らかにした上で検討を行い、必要となる要件の明確化を行うことが必要である。

イ　違法な第三者提供

現行法においては、事業者が個人データを違法に第三者に提供した場合について、報告義務及び本人通知義務は存在しないが、個人データが漏えい等した場合については事業者にこれらの義務が課されることとの均衡から、漏えい等との違いの有無も踏まえ、その必要性や報告等の対象となる範囲を検討する必要がある。

３　データ利活用に向けた取組に対する支援等の在り方

個々の事情や特性等に配慮した政策検討が進む等、健康・医療、教育、防災、こども等の準公共分野を中心に、機微性の高い情報を含む個人情報等の利活用に係るニーズが強い。こうした中、政策の企画・立案段階から関係府省庁等とも連携した取組を進める等、個人の権利利益の保護を担保した上で、適正な個人情報等の利活用を促す方策を検討する必要がある。

(1)本人同意を要しないデータ利活用等の在り方

【我が国の現状等】

法は、デジタル社会の進展に伴い個人情報等の利用が拡大している中で、第３条の基本理念に則し、プライバシーの保護を含めた個人の権利利益を保護することを目的としている。他方、法は、デジタル技術の活用による個人情報等の多様な利用が、個人のニーズの的確な反映や迅速なサービス等の提供を実現し、政策や事業活動等の面でも、国民生活の面でも欠かせないものとなっていることに配慮している。

個人情報の保護と有用性に関するこの法の考え方は、各主体における実際の個人情報等の取扱いにおいても、十分に踏まえる必要があり、個人情報の保護に関する施策を推進するに当たっては、個人情報の保護と適正かつ効果的な活用のバランスを考慮した取組が求められる。

法は、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱う場合（法第 18 条）、要配慮個人情報を取得する場合（法第 20 条）、個人データを第三者に提供する場合（法第 27 条）については、原則としてあらかじめ本人同意を取得することを求めている。各規律については、それぞれ例外規定が設けられているが、これらは、他の権利利益の保護を優先すべき場合や、本人の利益のために必要がある場合等を類型化したものとされている。

令和２年改正法の国会審議時においては、衆議院、参議院それぞれの内閣委員会において、附帯決議がなされており、個人情報の利活用について、民間の実態を常に広く把握し、制度面を含めた検討を随時行い、その結果に基づいて必要な措置を講ずることが求められている。

個人に関する情報について、高度なデジタル技術を用いた方法により、公益のために活用するニーズは、委員会としても、個人情報の保護に関する基本方針（平成 16 年（2004 年）４月２日閣議決定、令和４年（2022 年）４月１日一部変更。以下「基本方針」という。）等においてその認識を示し、施策を推進している。

また、政府全体においても、デジタル社会の実現に向けた重点計画（令和６年（2024 年）６月 21 日閣議決定）や規制改革実施計画（令和５年（2023 年）６月 16 日閣議決定）において、データ利活用の推進の必要性に言及がされている。

委員会としても、関係府省庁等が主催する検討会への参加や、ガイドライン等の策定に当たっての助言等を通じて、政策の企画・立案段階から連携して取組を進めているほか、公衆衛生例外により許容される取扱いについて、Q&A の改正を行った。

諸外国においても、本人の同意がなくとも、一定の場合に個人情報の取扱いが可能となっている。

【考え方】
昨今のデジタル化の急速な進展・高度化に伴い、生成 AI 等の新たな技術の普及等により、大量の個人情報を取り扱うビジネス・サービス等が生まれている。また、健康・医療等の公益性の高い分野を中心に、機微性の高い情報を含む個人情報等の利活用に係るニーズが高まっている。このほか、契約の履行に伴う個人情報等の提供や、不正防止目的などでの利活用についてもニーズが寄せられている。

こうした状況を踏まえ、法で本人同意が求められる規定の在り方について、個人の権利利益の保護とデータ利活用とのバランスを考慮し、その整備を検討する必要がある。この場合においては、単に利活用の促進の観点から例外事由を認めるのは適当ではなく、本人の権利利益が適切に保護されることを担保することが必要である。

まず、生成 AI などの、社会の基盤となり得る技術やサービスのように、社会にとって有益であり、公益性が高いと考えられる技術やサービスについて、既存の例外規定では対応が困難と考えられるものがある。これらの技術やサービスについては、社会的なニーズの高まりや、公益性の程度を踏まえて、例外規定を設けるための検討が必要である。この際、「いかなる技術・サービスに高い公益性が認められるか」について、極めて多様な価値判断を踏まえた上で高度な意思決定が必要になる。個人の権利利益の保護とデータ利活用の双方の観点から多様な価値判断が想定されるものであり、関係府省庁も含めた検討や意思決定が必要と考えられる。

また、医療機関等における研究活動等に係る利活用のニーズについても、公益性の程度や本人の権利利益保護とのバランスを踏まえて、例外規定に係る規律の在り方について検討する必要がある。例えば、医療や研究開発の現場における公衆衛生例外規定の適用のように、例外規定はあるものの、適用の有無に関する判断にちゅうちょする例があるとの指摘がある。こうした点等については、事業者の実情等も踏まえつつ、関係府省庁の関与を得ながら、ガイドラインの記載等についてステークホルダーと透明性のある形で議論する場の設定に向けて検討する必要がある。

(2)民間における自主的な取組の促進

【我が国の現状等】

ア　PIA (Privacy Impact Assessment)

PIA は、個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法を指すものである。

民間規律の分野においては、通則ガイドラインの中で、組織的安全管理措置として義務付けられる「個人データの取扱状況を確認する手段の整備」の例として、「個人データの取扱状況を把握可能とすること」が挙げられており、その手法として、委員会は、令和４年（2022 年）10 月にデータマッピング・ツールキットを公表している。

公的規律の分野においては、個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）（以下「事務対応ガイド」という。）の中で、「保有個人情報の取扱状況の記録」が挙げられている。

なお、現行法上、PIA は法律上の義務となっておらず、基本方針において一部言及があるのみである。

この点、GDPR においては、「取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合」にデータ保護影響評価（DPIA：Data Protection Impact Assessment）を実施しなければならないものとされている（GDPR 第 35 条第１項）。

EU 以外においても、1990 年代に提唱されたプライバシー・バイ・デザインの考え方の下、一定の要件の下に PIA を義務付ける例や、法律上の義務ではないがガイドライン等の公表をする例が散見される。

イ　個人データの取扱いに関する責任者

民間規律の分野においては、通則ガイドラインの中で、組織的安全管理措置として義務付けられる「組織体制の整備」の例として、「個人データの取扱いに関する責任者の設置及び責任の明確化」が挙げられており、大企業（中小企業基本法に定める中小企業者より規模の大きい企業）においては、既に 88.6%が個人データの取扱いに関する責任者を設置済みの状況である。

公的規律の分野においては、事務対応ガイドの中で、「総括保護管理者」や「保護管理者」の設置が規定されている。

この点、GDPR においては、一定の場合に DPO（Data Protection Officer）を選任する義務が生じる（GDPR 第 37 条第１項）。また、DPO は、資格要件として、データ保護の法令及び実務に関する専門知識並びに GDPR 第 39 条で定める DPO としての職務を遂行するための能力に基づいて指定される（GDPR 第 37 条第５項）。さらに、DPO による他の職務の遂行及び義務の履行は、利益相反するものであってはならず（GDPR 第 38 条第６項）、組織内において個人データの取扱いの目的及び方法を決めることにつながる地位に就くことができない点において、独立性の確保が要求されている。

【考え方】

PIA・個人データの取扱いに関する責任者は、データガバナンス体制の構築において主要な要素となるものであり、その取組が促進されることが望ましい。他方、これらの義務化については、各主体における対応可能性や負担面などを踏まえ、慎重に検討を進める必要がある。

PIA については、民間における自主的な取組という現状の枠組みを維持しつつ、その取組を一層促進させるための方策について、PIA の出発点となり得るデータマッピングを活用していくことを含め、検討を進める必要がある。

個人データの取扱いに関する責任者に関しては、現行の通則ガイドライン等で定める「組織体制の整備」を超えた措置の必要性について検討を進めるべきである。資格要件の要否、設置を求める対象事業者の範囲等によりその効果が変わ

ってくると考えられるところ、各企業の現状も踏まえ、現実的な方向性を検討する必要がある。

４　その他

上記のほか、プロファイリング（本人に関する行動・関心等の情報を分析する処理）、個人情報等に関する概念の整理、プライバシー強化技術（「PETs」：Privacy Enhancing Technologies）の位置づけの整理、金融機関の海外送金時における送金者への情報提供義務の在り方、ゲノムデータに関する規律の在り方、委員会から行政機関等への各種事例等の情報提供の充実などの論点についても、ステークホルダーの意見やパブリック・コメント等の結果を踏まえ、引き続き検討する。

また、個人情報保護及びその利活用とのバランスの在り方が国民各層にとって重要な課題であり、その重要性は以前にも増して高まっていることを踏まえ、委員会が関係の深いステークホルダーと透明性のある形で継続的に議論する場を設け、個人情報保護政策の方向性や、本人同意を要しない公益に資するデータ利活用に関係するガイドライン等の見直しの在り方などについて、検討していくこととすることも考えられる。

以　上

参考

中間整理の取りまとめに当たっては、ステークホルダーの意見も参考とさせていただいたところであり、今後も継続的な議論を行っていく。

１．関係団体ヒアリングの実施状況

回次	開催日	団体名
第262回	令和５年11月29日	一般財団法人日本情報経済社会推進協会
第263回	令和５年12月６日	欧州ビジネス協会
第264回	令和５年12月15日	・　一般社団法人新経済連盟 ・　一般社団法人日本IT団体連盟
第265回	令和５年12月20日	在日米国商工会議所
第266回	令和５年12月21日	・　一般社団法人電子情報技術産業協会 ・　全国商工会連合会
第268回	令和６年１月23日	・　特定非営利活動法人消費者支援機構関西 ・　日本商工会議所
第270回	令和６年１月31日	一般社団法人日本経済団体連合会
第271回	令和６年２月７日	一般社団法人日本インタラクティブ広告協会
第272回	令和６年２月14日	地方公共団体（京都府、岡山市、都城市、上里町）
第281回	令和６年４月24日	・　一般社団法人日本経済団体連合会 ・　日本商工会議所 ・　公益社団法人経済同友会 ・　一般社団法人新経済連盟 ・　一般社団法人日本IT団体連盟 ・　一般社団法人Fintech協会 ・　一般社団法人シェアリングエコノミー協会 ・　プライバシーテック協会

２．有識者ヒアリングの実施状況

回次	開催日	有識者氏名
第279回	令和６年４月３日	・生貝直人氏（一橋大学大学院法学研究科教授） ・高橋克巳氏（NTT社会情報研究所チーフ・セキュリティ・サイエンティスト） ・森田朗氏（東京大学名誉教授／一般社団法人次世代基盤政策研究所代表理事） ・横野恵氏（早稲田大学社会科学総合学術院社会科学部准教授）
第283回	令和６年５月10日	・林秀弥氏（名古屋大学大学院法学研究科教授） ・中川丈久氏（神戸大学大学院法学研究科教授）
第287回	令和６年６月３日	・曽我部真裕氏（京都大学大学院法学研究科教授） ・山本龍彦氏（慶應義塾大学大学院法務研究科教授） ・森亮二氏（弁護士法人英知法律事務所弁護士） ・宍戸常寿氏（東京大学大学院法学政治学研究科教授）
第289回	令和６年６月12日	・佐藤一郎氏（国立情報学研究所教授） ・高木浩光氏（国立研究開発法人産業技術総合研究所主任研究員）
第290回	令和６年６月13日	・板倉陽一郎氏（弁護士法人ひかり総合法律事務所弁護士） ・鈴木正朝氏（新潟大学大学院現代社会文化研究科／法学部教授）