弁護士法人　三宅法律事務所

Miyake　& Partners

Miyake newsletter

個人情報保護法ニュースＮｏ．９

「個人情報保護法　いわゆる３年ごとの見直しに係る中間整理」に見る

個人情報保護法の改正予想

はじめに、

平素より大変お世話になっております。

さて、今回は個人情報保護法ニュース**「『個人情報保護法　いわゆる３年ごとの見直しに係る中間整理』に見る個人情報保護法の改正予想」**をご案内させていただきます。

令和６年７月 23 日

弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。
弁護士法人三宅法律事務所
弁護士渡邉雅之、弁護士越田晃基、弁護士岩田憲二郎、弁護士出沼成真（執筆者）
TEL 03-5288-1021 FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp
k-koshida@miyake.gr.jp
k-iwata@miyake.gr.jp
n-idenuma@miyake.gr.jp

「個人情報保護法　いわゆる３年ごとの見直しに係る中間整理」に見る
個人情報保護法の改正予想

現在、個人情報保護委員会は、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４年４月１日全面施行）の附則第 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。」（いわゆる３年ごとの見直し規定）との規定がされていることに基づき、個人情報の保護に関する法律（「個人情報保護法」、「法」）の改正の検討を進めている。順調にいけば、令和７年（2025 年）には、個人情報保護法の改正法が公布されることが予想される。

本ニュースレターにおいては、個人情報保護委員会が令和６年（2024 年）６月 27 日に公表した『個人情報保護法　いわゆる３年ごとの見直しに係る中間整理』[1]（令和６年６月 27 日　個人情報保護委員会）を基に、個人情報保護法及び関連するガイドラインの改正を予想するものである。

あくまで、筆者らの独断による予想（実現可能性をパーセンテージで表示）によるものであり、内容を保証するものではないことにご注意いただきたい。

なお、弊職らが 2024 年４月２日に公表した『[miyakenews] 個人情報保護法ニュースＮｏ．７『「いわゆる３年ごとの見直し」の検討に見る個人情報保護法の改正予想』[2]も併せて参考にされたい。

第１．個人の権利利益のより実質的な保護の在り方

１．個人情報等の適正な取扱いに関する規律の在り方

（１）要保護性の高い個人情報の取扱いについて（生体データ）

ア．個人情報保護委員会の考え方

> **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**

[1] https://www.ppc.go.jp/news/press/2024/240627_02
[2] https://www.miyake.gr.jp/legalinfo/miyakenews-%e5%80%8b%e4%ba%ba%e6%83%85%e5%a0%b1%e4%bf%9d%e8%ad%b7%e6%b3%95%e3%83%8b%e3%83%a5%e3%83%bc%e3%82%b9%ef%bd%8e%ef%bd%8f-%ef%bc%97%e3%80%8e%e3%80%8c%e3%81%84%e3%82%8f%e3%82%86%e3%82%8b/

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．改正の方向性

①生体データの「要配慮個人情報」としての取扱い（実現可能性：70%）

個人情報保護法では、「要配慮個人情報」（法２条３項）については、取得に際して、原則として本人の事前の同意が必要となる（法 20 条２項）。

もっとも、現行個人情報保護法上、特定の個人を識別するに足りる生体認証情報等は「個人情報」（法２条１項２号、法２条２項、施行令１条１号）に該当するが、「要配慮個人情報」には該当せず、通常の個人情報と同様の取扱いをすれば足り、取得に際して本人の事前の同意は不要であり、生体データであることに着目した特別の規律は存在しない。

他方、諸外国では、GDPR 第８条など、「自然人の一意な識別を目的」とした生体データをセンシティブデータとして取り扱うことが求められている。

「個人情報保護委員会の考え方」においては、**「特に要保護性の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」と記載されているとともに、「**本人関与・・・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**」と記載されており、生体データが改正法により、「要配慮個人情報」（法２条３項）として取り扱われることになり、取得に際して本人の事前の同意（法 20 条２項）が必要となる可能性がある。

もっとも、全ての生体データにつき例外なく要配慮個人情報として取り扱うことが求められた場合、駅での人流データの取得・解析に用いるためのカメラ設置・撮影や顔認証技術を有した防犯カメラによるセキュリティ対策などができなくなるおそれがあるところ、規制の対象を特定の個人の識別を目的とした生体データとしたり、特定の個人の識別を目的としていたりしていたとしても個人情報ガイドライン Q&A1-14[3]の義務を果たしていれば問題ないとするなど、一定の例外を設けることが望まれるであろう。

②生体データに関する安全管理措置の上乗せ（実現可能性：70%）

「**個人情報保護委員会の考え方**」においては、上記①のように、生体データを要配慮個人情報として取り扱うことだけではなく、「**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**」と記載されていることから、金融分野実務指針のような安全管理措置の上乗せが設けられる可能性がある。

この点、個人情報保護法（及び通則編ガイドライン）上、要配慮個人情報について、安全管理措置について特別な取扱いは認められていない。

もっとも、金融分野など一部の業種においては、「機微（センシティブ）情報」と定義される機微性の高い一定の情報について、原則として取得、利用、第三者提供が禁止され（「金融分野における個人情報保護に関するガイドライン」５条１項）、安全管理措置についても特別の取扱いが求められている（「金融分野ガイドラインの安全管理措置等についての実務指針」（「金融分野実務指針」）別添２「金融分野における個人情報保護に関するガイドライン第５条に定める「機微（センシティブ）情報」（生体認証情報を含む。）の取扱いについて」参照）。

そこで、金融分野実務指針の安全管理措置を参考に、個人情報保護法（下位法令を含む）または通則編ガイドラインに、以下のような安全管理措置の上乗せが新たに規定されることが考えられる。

【取得・入力段階】

[3] https://www.ppc.go.jp/all_faq_index/faq1-q1-14_/

● 取得・入力を行う取扱者の必要最小限の限定
● 取得に際しての本人同意が必要である場合における本人同意の取得及び本人への説明事項
● なりすましによる登録の防止策
● 本人確認に必要な最小限の生体認証情報のみ取得
● 生体認証情報の取得後、基となった生体情報の速やかな消去

【利用・加工段階】
● 利用・加工を行う取扱者の必要最小限の限定
● 取得に際しての本人同意が必要である場合における本人同意の取得及び本人への説明事項
● 必要最小限の者に限定したアクセス制限の設定およびアクセス制御の実施
● 偽造された生体認証情報による不正認証の防止措置
● 登録された生体認証情報の不正利用の防止措置
● 残存する生体認証情報の消去
● 認証精度設定等の適切性の確認
● 生体認証による本人確認の代替措置における厳格な本人確認手続

【保管・保存段階】
● 保管・保存を行う取扱者の必要最小限の限定
● 必要最小限の者に限定したアクセス権限の設定及びアクセス制御の実施

【移送・送信段階】
● 必要最小限の者に限定したアクセス権限の設定及びアクセス制御の実施

【消去・廃棄段階】
● 消去・廃棄を行う取扱者の必要最小限の限定
● 生体認証情報を本人確認に用いる必要性がなくなった場合は、速やかに保有する生体認証情報を消去

【その他】
● 生体認証情報の取扱いに関して外部監査を実施

③利用目的の特定の方法（実現可能性：90%）

個人情報保護法上、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（法 17 条１項）。

「個人情報保護委員会の考え方」においては、「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。」とされている。

「利用目的の特定」に関しては、通則編ガイドライン 3-1-1（※１）において、「**本人が、自らの個人情報がどのように取り扱われることとなるか、利用目的から合理的に予測・想定できないような場合は、この趣旨に沿ってできる限り利用目的を特定したことにはならない。**」とされている。

そして、「**例えば、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。**」とされ、具体的な事例が記載されている。

生体データの取扱いについても同様に通則編ガイドラインに規定される可能性が高いと思

われる。

④本人による事後的な利用停止（実現可能性：70%）

現行個人情報保護法上、保有個人データの利用停止を求められる事由としては、①当該本人が識別される保有個人データが法 18 条若しくは法 19 条の規定に違反して取り扱われているとき、又は法 20 条の規定に違反して取得されたものであるとき（法 35 条１項）、または、②当該本人が識別される保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合、当該本人が識別される保有個人データに係る法 26 条１項本文に規定する事態が生じた場合その他当該本人が識別される保有個人データの取扱いにより当該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（法 35 条５項）に限定されている。

「個人情報保護委員会の考え方」においては、「**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。**」とされている。

生体データに係る保有個人データの利用停止をどのように柔軟化するのかは現状明らかではないが、**現行の保有個人データの利用停止事由が拡充される可能性**があるものと考えられる。

また、現行の個人情報保護法では、保有個人データの公表等に関して、「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。」（法 32 条１項）とされているところ、「**本人に対して通知又は十分に周知**」が必要となる点も厳格化されるものと考えられる。

（２）「不適正な利用の禁止」「適正な取得」の規律の明確化

ア．個人情報保護委員会の考え方

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。

イ．改正の方向性

①不適正取得・不適正利用の適用の明確化（実現可能性：90%）

近年の個人情報保護法委員会による不適正利用（法 19 条）や不適正取得（法 20 条１項）の処分事例を踏まえ、個人情報保護法（下位の政令・個人情報保護委員会規則を含む）の改正または通則編ガイドラインの改正により、不適正利用や不適正取得違反するケース（現在は 3-2 及び 3-3-1 に各６つずつ挙げられている）が明記・追加されることが想定される。近時、不適正取得、不適正利用に関する個人情報保護委員会の行政上の対応が相次いでいることに鑑みると、実現可能性は高いと考えられる。

（参考）個人情報保護委員会による行政上の対応

- 多数の破産者等の個人情報を個人情報保護法に違反（オプトアウトの届出せず）して取り扱っているウェブサイトの運営者（2022 年 11 月２日・命令）
- 大手電力会社各社による電気事業法 23 条の３で禁止されているグループ送配電会社からの顧客情報の取得（2023 年６月 29 日・行政指導）
- オプトアウト事業者による名簿の転売屋と認識しながらの名簿の提供（個人データの提供の記録義務違反あり）（2024 年１月 17 日・行政指導）

想定される不適正取得・不適正利用の対象となる法令・条項として、筆者らが予想するもの

は以下のとおり[4]。

主体	不適正取得・不適正利用の対象となる法令・条項
個人情報取扱事業者	● 利用目的の通知・公表義務（法 21 条１項） ● 個人データの安全管理措置義務（法 23 条） ● 委託先の監督義務（法 25 条） ● 個人データの第三者提供の同意取得義務（法 27 条１項） ● オプトアウトの手続違反（法 27 条２項） ● オプトアウトの提供先が違反業者であることを認識した上での提供 ● 第三者提供に係る記録の作成義務（個人情報保護法 29 条１項） ● 電気事業法 23 条等の他の法令で禁止されている個人情報の提供
事業者	● 事業者の労働者・役員等の範囲外共有を防ぐ措置、通報者の探索を防ぐ措置、違反者に対する懲戒処分その他適切な措置（公益通報保護法 11 条２項） ● 障害を理由として障害者でない者との不当な差別的取扱いをすることの禁止（障害を理由とする差別の解消の推進に関する法律８条１項）
訪問販売を行う販売業者又は役務提供事業者	● 若年者、高齢者その他の者の判断力の不足に乗じ、訪問販売に係る売買契約又は役務提供契約を締結させること。（特定商取引法７条１項５号・同法施行規則 18 条２号） ● 顧客の知識、経験及び財産の状況に照らして不適当と認められる勧誘を行うこと。（特定商取引法施行規則 18 条３号）

②本人の自律的な意思の選択が可能でない場合の不適正取得・不適正利用の規律の適用（実現可能性：60%）

「**個人情報保護委員会の考え方**」においては、「本人の自律的な意思の選択が可能でない場合」についての不適正取得（法 20 条）、不適正利用（法 19 条）の規律の適用が検討されている。

「本人の自律的な意思の選択が可能でない場合」とは、「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」などである。

具体的には、①個人情報取扱事業者が本人との関係で利用目的達成に必要な利用目的を超えた個人情報の利用目的の通知・公表（法 21 条１項）の明示（法 21 条２項）や、②本人との関係で必要のない利用目的の範囲外の目的外利用する場合の本人からの同意の取得（法 18 条１項）、本人との関係で個人データの提供の必要がない第三者への提供を認める包括的な第三

[4] 『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（個人の権利利益のより実質的な保護の在り方①）』（令和６年３月６日：個人情報保護委員会事務局）を参照。

者提供の本人からの同意の取得（法 27 条１項）などが想定される。

後者（②）については、代替困難なサービスの取引条件として個人情報の取扱いに関する同意が求められるなど、事実上、本人が自らの個人情報の提供等につき自ら判断・選択できないようなケースも問題視されている。

これは、「本人の同意の任意性」の問題でもあると考えられるが、個人情報保護法では、本人からの同意の取得について「任意性」が必要であることは定められていない。

GDPR（EU 一般データ保護規則）においては、データ主体からの同意取得には任意性が必要とされており（GDPR 第 4 条 11 号）、例えば、同意することがサービス提供等の条件とされている場合等については同意が自由に与えられていないとして任意性が否定されると考えられている。

改正の方向性としては、「本人の同意」の要件として、新たに「任意性」を追加するのではなく、**「本人の同意の任意性が認められない場合」を含む「本人の自律的な意思の選択が可能でない場合」について、不適正取得（法 20 条）、不適正利用（法 19 条）の規律を適用することが検討**されている。

これは、我が国の個人情報保護法においては「本人の同意」が重視されており、GDPR のように、「契約の履行」や「正当な利益」などの他の「取扱い（処理）」の適法性の根拠が認められておらず、現行実務に混乱を来たす可能性もあることから、同意の効力を緩める「同意の任意性」を認めるのは困難との判断に基づくものであると考えられる[5]。

もっとも、どのような場合が「本人の自律的な意思が選択できない場合」に該当するのかは判断が難しいものであり、事業者の萎縮的効果をもたらすものとして改正の可能性が必ずしも高いとは言えないかもしれない。

仮に、改正で追加される場合には、「本人の自律的な意思が選択できない場合」について、通則編ガイドラインなどにおいて具体例を列挙されることが望まれる。

③個人関連情報への不適正取得・不適正利用の規律の適用（実現可能性：80%）

いわゆる「リクナビ問題」などを受け、令和２年改正により、令和４年４月１日より、個人関連情報の規律が限定的であるが設けられた。

「個人関連情報」とは、生存する個人に関する情報であって、個人情報、仮名加工情報及び

[5] 同様に、「同意の撤回権」（GDPR７条３項参照）を設ける改正も、本人の同意の効力を弱めるものであり、実務の混乱を来たす可能性があるので困難であると考えられる。

匿名加工情報のいずれにも該当しないものをいう（法２条７項）。

たとえば、「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」が「個人関連情報」に該当する。ただし、他の容易に照合できる情報と紐づいて特定の個人を識別できる場合には個人情報に該当し、個人関連情報には該当しない。

令和２年改正により、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た（法 31 条）。

「**個人情報保護委員会の考え方**」においては、「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」として、**プライバシーなど個人の権利利益の侵害の蓋然性のある一定の個人関連情報について、不正取得・不適正利用等への規制を改正により追加**することが検討されている。

データの利活用の推進の観点から、広告配信業者などの一部の事業者の反対は予測できるが、**プライバシー保護の観点から、個人関連情報のうち、「電話番号、メールアドレス、Cookie ID など、個人に対する連絡可能な情報を有している場合」には、個人情報と同様に、不適正取得・不適正利用の規律**が新たに設けられる可能性は大きいと思われる。

２．第三者提供規制の在り方（オプトアウト等）

（１）個人情報保護委員会の考え方

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。

（2）改正の方向性

①オプトアウト届出業者への提供先の利用目的や身元等を確認する義務の追加（実現が可能性：90%）

オプトアウト手続については、いわゆるベネッセ事件を受けて平成 27 年改正（平成 29 年５月施行）により厳格化された。具体的には、個人情報保護委員会への届出（個人情報保護法 27 条２項）や個人データの提供・受領の確認・記録義務が設けられた（オプトアウトの場合はガイドラインで解釈上の例外は認められない。）（同法 29 条・30 条）。また、要配慮個人情報を含む個人データについてオプトアウトは認められない。

もっとも、近時、オプトアウト事業者による名簿の転売屋と認識しながらの名簿の提供した事案に関して、個人情報保護委員会が行政上の対応をした[6]。

政府の犯罪対策閣僚会議が令和５年３月 17 日に公表した「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」[7]では、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、個人情報保護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**が求めている。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

[6] 「オプトアウト届出事業者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」（個人情報保護委員会・令和６年１月 17 日）
（https://www.ppc.go.jp/news/press/2023/240117_houdou）

[7] https://www.kantei.go.jp/jp/singi/hanzai/kettei/230317/honbun-1.pdf

した取締り等を推進することとしている。

また、犯罪閣僚会議が令和６年６月 25 日に公表した「国民を詐欺から守るための総合対策」[8]においても、「闇名簿対策」として、「名簿屋」等の事業者において、個人情報保護法の規定の下での個人データの適正な取扱いが確保されているかについて実態を把握するため、引き続き幅広く情報収集に努め、その結果等を踏まえ、必要に応じて指導等の権限行使を実施することとされている。

提供先の事業者による違法又は不当な行為を助長する「おそれ」が想定されるにもかかわらず、当該事業者に個人情報を提供する場合、不適正利用に該当する（法 19 条）。もっとも、提供先の第三者が当該個人情報の取得目的を偽っていた等、当該個人情報の提供の時点において、提供した個人情報が違法に利用されることについて、提供元が一般的な注意力をもってしても予見できない状況であった場合には、「おそれ」は認められない。現行法上、提供先の利用目的や提供先に対する身元確認方法等は、記録義務の対象に含まれていない[9]。

個人情報保護委員会のオプトアウトに関する実態調査によれば、オプトアウトにより個人データを提供するにあたって、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割であった。また、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割であった[10]。

名簿等の販売に対する処分事例や、社会背景として特殊詐欺が増加しており、それに名簿業者の個人情報が利用されていること等も踏まえ、オプトアウト届出事業者がそのような違法な名簿業者へ個人情報を提供したり、また、不正取得された個人情報の提供を受けてしまったりすることを予防するため、**「一定の場合における提供先の利用目的や身元等の確認」に関する確認義務が設けられる可能性が高い。**

「一定の場合」としては、個人情報保護委員会の行政上の対応で問題となった、名簿業者のケースが想定されるだろう。

この場合に、**「確認義務の要件」**及び**「住宅地図等を幅広く販売する場合の規律」**をどのよ

[8] https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf
[9] 第 281 回個人情報保護委員会（令和６年４月 24 日）（https://www.ppc.go.jp/aboutus/minutes/2024/20240424/）の資料２「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（個人の権利利益のより実質的な保護の在り方③」及び議事録・議事概要参照。
[10] 脚注９の資料等参照。

うに定めるかが問題になるだろう。

②オプトアウト届出事業者の取得元の身元や取得の適法性を示す資料等を確認する義務の追加（実現可能性：90%）

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。

個人情報保護委員会のオプトアウトに関する実態調査によれば、提供しようとするデータが、法第 20 条第 1 項（適正な取得）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割であった。また、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 20 条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割であった[11]。

そのため、一定の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。

「個人情報保護委員会の考え方」のとおり、**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が課される可能性**が高い。

「一定の場合」としては、上記（１）と同様に、名簿業者のケースが想定されるだろう。

この場合に、**「確認義務の要件」**及び**「対象の類型化」**が課題となる。

なお、不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合は、法 20 条 1 項の規定違反となる。個人情報取扱事業者は、第三者から個人データの提供を受ける際は、当該第三者に対して、当該第三者による当該個人データの取得の経緯を確認しなければならない（法 30 条）。もっとも、受領者にとって「個人データ」には該当しない個人情報として提供を受けた場合、後に当該個人情報を個人情報データベース等に入力したとしても、確認義務は適用されないことも問題とされている[12]。

そこで、名簿業者など一定の事業者が名簿等を取得する場合には、個人データとなっていない個人情報を取得する場合にも取得の経緯についての確認が義務付けられる可能性がある。

---

[11] 脚注９の資料等参照
[12] 脚注９の資料等参照。

③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（実現可能性：80%）

「個人情報保護委員会の考え方」では、「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」することとされている。

この点に関しては、現行個人情報保護法 27 条２項又は３項の「通知又は容易に知り得る状態に置く措置」は、「本人が法第 27 条第２項各号に掲げる事項を確実に認識できる適切かつ合理的な方法によること」とされているところである（個人情報保護法施行規則 11 条１項２号）。

通則編ガイドラインに 3-6-2-1 においては、「本人が容易に知り得る状態に該当する事例」として、以下の事例が掲げられている。

【本人が容易に知り得る状態に該当する事例】
事例 1）本人が閲覧することが合理的に予測される個人情報取扱事業者のホームページにおいて、本人が分かりやすい場所（例：ホームページのトップページから 1 回程度の操作で到達できる場所等）に法に定められた事項を分かりやすく継続的に掲載する場合
事例 2）本人が来訪することが合理的に予測される事務所の窓口等への掲示、備付け等が継続的に行われている場合
事例 3）本人に頒布されている定期刊行物への定期的掲載を行っている場合
事例 4）電子商取引において、商品を紹介するホームページにリンク先を継続的に表示する場合

それにもかかわらず、「個人情報保護委員会の考え方」で「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」について検討されているということは、上記の事例の措置では不十分ということだろう。

名簿屋等、特殊詐欺などの犯罪につながる一定の場合については、「本人が容易に知り得る状態に置く措置」は認めず、「通知」のみを認めるという改正もあり得るかもしれないが現実的ではないだろう。

たとえば、上記の通則編ガイドラインの事例を規則に規定することにより、実効性を高めることも考えられる。

名簿業者などには負担が大きくなるものの、事業者側の反対も少ないと思われることから、実現する可能性は高いかもしれない。

３．こどもの個人情報等に関する規律の在り方

（１）個人情報保護委員会の考え方

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[13]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。

（2）改正の方向性

①法定代理人の関与（実現可能性：80%）

個人情報ガイドライン Q&A1-62 では、「一般的には 12 歳から 15 歳までの年齢以下の子どもについて、法定代理人等から同意を得る必要があると考えられます。」としている。

もっとも、現行個人情報保護法上は、目的外利用の同意（法 18 条）、要配慮個人情報の取得（法 20 条２項）、個人データの第三者提供（法 27 条１項、法 27 条１項）の場合等、本人同意の取得が必要とされている場面において、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との法令上の規定は存在しない。

また、利用目的の通知（法 21 条１項）、漏えい等に関する本人への通知（法 26 条２項）等、本人に対する通知等が必要となる場面において、こどもを本人とする個人情報について、法定代理人に対して情報提供すべきとの法令上の規定やガイドライン上の定めも存在しない。

他方、諸外国の規定をみると、GDPR では、個人データの処理の法的根拠が本人の同意に基

[13] https://www.ppc.go.jp/news/press/2023/240229_houdou/

づく場合（GDPR６条１項(a)）、直接こどもに提供されるオンラインサービス等において、本人が 16 歳未満であれば、親権者の同意による必要がある（GDPR８条１項）。この場合、個人データの管理者は、親権者から同意が得られたことを確認するための合理的な努力をしなければならない（同条２項）。

そこで、現行の通則編ガイドラインや GDPR の規定を参考に、**こどもを本人とする個人データについて、本人同意の取得が必要な場面は法定代理人の同意の取得を必要とし、本人に対する通知等が必要となる場面においては法定代理人に対する情報提供を必要とする個人情報保護法の改正**が考えられる。また、**法定代理人による同意を取得できたことを確認するよう努めなければならない等の要件が追加**される可能性も考えられる。

②利用停止請求権の拡張（実現可能性：60%）

現行の個人情報保護法では、本人が識別される保有個人データが本人の同意なく目的外利用されている場合（法 18 条違反）、不適正な利用がされている場合（法 19 条違反）、不正に取得されている場合や本人の同意なく要配慮個人情報が取得されている場合（法 20 条違反）等の法 18 条乃至 20 条に違反する場合に当該保有個人データの利用の停止又は消去（「利用停止等」）を請求することができる（法 30 条１項）。また、それ以外にも、本人が識別される保有個人データにつき、その利用する必要がなくなった場合で、法 26 条１項本文に規定する漏えい等事案が生じ、当該本人の権利又は正当な利益が害される恐れがある場合には、当該保有個人データの利用停止等を請求することができる（法 30 条５項）[14]。

他方、諸外国の規定をみると、GDPR では、以下の場合において、管理者に対し、個人データの消去を求めることができる（いわゆる「忘れられる権利」、GDPR17 条１項(a)乃至(f)）。なお、①から⑤については、こどもを本人とする個人データに限られるものではない。

①当該個人データが収集・取扱いの目的との関係で必要のないものとなった場合
②当該個人データの処理の法的根拠が本人の同意に基づく場合（GDPR６条１項(a)、９条２項(a)）において、同意が撤回され[15]、かつ、その取扱いのための法的根拠（GDPR６条１項(b)乃至(f)、９条２項(b)乃至(j)）がない場合
③そのデータ主体が、公共の利益又は公的権限の行使において行われる職務遂行において取り扱われる場合や正当な利益の目的のために取り扱われる場合において、その取扱いに対する異議を述べ（GDPR21 条１項）、かつ、その取扱いのための優先する法的根拠が存在しない場合、又は、ダイレクトマーケティングのために取り扱われる場合において

[14] このような未成年者を本人とする保有個人データの利用停止等請求をする場合は、法定代理人が行うことができる（法 37 条３項、施行令 13 条１号）。
[15] GDPR では、個人データの処理に関する同意をいつでも撤回することができる（GDPR７条３項）。

異議を述べた場合（GDPR21 条２項）
④当該個人データが違法に取り扱われた場合
⑤当該個人データが管理者の服する EU 法又は加盟国の国内法の法的義務を遵守するために消去されなければならない場合
⑥当該個人データがオンラインサービス等のこどもに対する提供との関係において収集された場合

個人情報保護委員会は、現状について、「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」としつつ、「**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。」としている。

GDPR の上記⑥の場合のように特定のサービス等において収集された情報を全て対象とすると現状の制度からあまりに厳格化されてしまうため、そのような改正は現実的ではないだろう。GDPR の上記①の場合を参考に、本人が識別されるこどもに関する保有個人データについて、例えば、単に利用目的との関係で必要のないものとなったものについて、漏えい等事案が生じたり本人の権利が害されたりする恐れ等がなくとも、利用停止等を請求することができるように改正がされることが考えられる。

また、個人情報保護委員会は、**「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。」**ともしており、**こどもを本人とする個人情報を取得する際に法定代理人の同意を取得している場合には、利用停止等の請求の対象としないような規定**になると想定される。

③安全管理措置義務の強化（実現可能性：60%）

現行の個人情報保護法では、その取り扱う個人データの漏えい、滅失又は毀損（「漏えい等」）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならない（法 23 条）とされている。この安全管理措置義務の内容は、通則編ガイドライン１０において定められており、大きく分けて「基本方針の策定」「個人データの取扱いに係る規律の整備」「組織的安全管理措置」「人的安全管理措置」「物理的安全管理措置」「技術的安全管理措置」「外的環境の把握」の７つがある。

もっとも、個人情報保護法やガイドライン等において、こどもの個人データの要保護性に着目し、こどもの個人データに関して講ずべき安全管理措置の内容を強化するなどの規律は存在しない。

他方、諸外国の規定を見ると、こどもの個人情報をセンシティブデータに分類したうえで特

別の規律の対象とするケース、センシティブデータ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うえで、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がある。

EU の Digital Services Act（DSA、デジタルサービス法）においては、１８歳未満の未成年者がアクセス可能なオンラインプラットフォームの提供者は、そのサービスにおいて、未成年者のプライバシー、安全及びセキュリティを高い水準で確保するために適切かつ相応の措置を講じなければならないとしている（28 条１項）。

英国の UK GDPR の遵守に関して定められた Children’s Code では、特にオンラインサービスに着目した規制がかけられており、次の１５の基準を満たすことが求められている。

①こどもの最善の利益の優先
②データ保護影響７の実施とリスクの評価・軽減
③年齢に応じて適切なレベルの規律を適用
④透明性
⑤未成年者の幸福に有害な使用等の回避
⑥自らの公表しているポリシーや基準の遵守
⑦デフォルトで高プライバシーに設定
⑧データの最小化
⑨正当な理由がある場合を除きこどものデータは非開示
⑩ジオロケーション（位置情報取得等）のデフォルトオフ
⑪親権者によるコントロール・監視をこどもに通知・明示
⑫プロファイリングのデフォルトオフ、プロファイリング時の有害コンテンツからの保護措置の実施
⑬ナッジテクニックの回避
⑭接続されるトイ、デバイスの本 Code への準拠
⑮こどもが権利行使をしやすいオンラインツールの提供

個人情報保護委員会は、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[16]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り、同事案に関する個人情報保護委員会の公表には、その具体的内容は明らかにされていないものの、こどもの個人データを取り扱うにあたって「多角的な観点からリスクを検討」することが必要としており、諸外国で求められているデータ保護影響評価の実施が改正により求められる可能性がある。

現在でも、個人情報保護委員会の HP においては「データガバナンス（民間の自主的取組）」として PIA（Privacy Impact Assessment、個人情報保護評価）の意義・手順等がまとめられ

[16] https://www.ppc.go.jp/news/press/2023/240229_houdou/

ている[17]ところ、これがベースとなることが考えられる。

しかし、現行の個人情報保護法においてはPIAの規定も存在しないところ、こどもの個人データに限ってデータガバナンスの規定が設けられる可能性は必ずしも高くはないのではないか。

④責務規定（実現可能性：80%）

現行の個人情報保護法では、「国は、この法律の趣旨にのっとり、個人情報の適正な取扱いを確保するために必要な施策を総合的に策定し、及びこれを実施する責務を有する。」（法４条）といった国の責務を定めた規定があるが、事業者における個人情報の取扱いに関する責務を定めた規定は存在しない。

他方、諸外国の規定をみると、GDPRでは各国の監督当局はこどものデータ処理に関連するリスク等につき格別の注意を払わなければならないとされている（GDPR57条1項(b)）。英国Children’s Codeの基準の１つとして、①こどもの最善の利益の優先が挙げられている。また、OECDの「デジタルサービスプロバイダー向けガイドライン」においては、こども向けのデジタルサービスの提供者等について、こどもの個人データの収集・利用・提供をこどもの最善の利益のためのサービス提供の履行に限定すること等が要求されている。

個人情報保護委員会の考え方としては、「各事業者の自主的な取組の促進という観点」から、「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。」とされており、特段「こどもの最善の利益」のため具体的に個人データの制約を定めることは予定していないように見受けられるところ、**こどもを本人とする個人データを取り扱う可能性がある事業者について、こどもの最善の利益に配慮した個人情報の取扱いを確保するために必要な施策の策定・実施に努めることを求める規定が改正により追加**される可能性が考えられる。

⑤年齢基準（実現可能性：80%）

個人情報ガイドラインQ&A1-62では、「一般的には12歳から15歳までの年齢以下の子どもについて、法定代理人等から同意を得る必要があると考えられます。」としており、１６歳

[17] https://www.ppc.go.jp/personalinfo/independent_effort/

未満の者をこどもとし、法定代理人等からの同意を必要とする。もっとも、この点について個人情報保護法上の明文規定はない。

諸外国の規定をみると、GDPR では、子どもに対する直接的な情報社会サービスの提供に関し、子どもが 16 歳未満の場合、当該処理は、親権者によって同意・許可がなされる限りにおいて、適法とすることとされている（GDPR８条１項）。この規定は、こどもと関係する契約の有効性、締結又は法律効果に関する規定のような加盟国の一般的な契約法に対して影響を与えないとされている（GDPR８条３項）。

そこで、個人情報保護委員会の考え方にもあるとおり、**個人情報ガイドライン Q&A や GDPR の規定を踏まえ、16 歳未満のこどもについては法定代理人等の同意が必要となるとの年齢基準が設けられる**可能性が高い。

この場合、18 歳未満を未成年とする民法４条との平仄をどのようにとるかが問題となるが、GDPR 同様、契約法への影響がないような整理が望まれるだろう。

上記考え方によれば、業種に着目した規制まで設けることまでは想定されておらず、そのような改正の可能性は低いように思われる。もっとも、③（安全管理措置義務の強化）も想定されているところ、改正によりどの程度の強化がされるかは注目であろう。

４．個人の権利救済手段の在り方

（１）個人情報保護委員会の考え方

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。

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）改正の方向性

①差止請求制度（実現可能性：20%）

個人情報保護法には、本人が識別される保有個人データが法 18 条乃至法 20 条に反し利用・取得されている場合に事後的に利用停止等を請求することはできる（法 30 条 1 項）が、差止

請求権に関する規定は設けられていない。

他方、GDPR では、データ主体は、個人データの取扱いが違法であり、かつ、データ主体が個人データの消去に反対し、その代わりに、そのデータ利用の制限を求めている場合等に、当該個人データの取扱いを制限させる権利を有する（GDPR18 条 1 項(b)）。

個人情報保護委員会の考え方によれば、「**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の枠組みは有効な選択肢となり得る。**」とする。消費者契約法では、内閣総理大臣の認定を受けた適格消費者団体は、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等に違反する不当な行為を行っている、又は行うおそれがあるときに、かかる事業者の不当な行為をやめるよう求めることができる（消費者契約法１２条）。差止請求の流れは、概要、①消費者からの情報提供などにより被害情報を収集・分析・調査、②事業者に対し、業務改善を申入れ（裁判外の交渉）、③団体と事業者で協議、④（交渉成立の場合）事業者による業務改善、⑤（交渉不成立の場合）事業者に対し、提訴前の書面による事前請求をした上、裁判所へ訴え定期、⑥判決または裁判上の和解等といった流れである。

そこで、個人情報保護法の改正により、**差止請求を行う適格団体の認定や差止請求権が追加**される可能性がある。

しかしながら、「個人情報保護委員会の考え方」によれば「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」るとのことであり、また、「導入の必要性も含めて多角的な検討を行っていく必要がある」とトーンダウンした書き方がされていることからすると、**改正の実現可能性は低い**ように思われる。

②被害回復制度（実現可能性：20%）

現行の個人情報保護法には被害回復ないし損害賠償請求に関する規定は設けられておらず、現状は民法上の不法行為に基づく損害賠償請求（慰謝料）（民法 710 条）により現状は対応されている。実際の事例として、大学が取得した講演会の参加申込者らの学籍番号、氏名、住所及び電話番号等の個人情報に係る情報を無断で警察に開示した事案につき、本人らのプライバシーを侵害するものであるとして、慰謝料 5000 円ずつの支払いを命じた事案がある（最判平成 15 年９月 12 日、差戻審控訴審東京高判平成 16 年３月 23 日）。

他方、GDPR においては、自身に関する個人データの処理が GDPR 違反である場合には、監督当局への不服申立権（GDPR 第 77 条）、監督当局が不服申立てに対処しない場合の司法救済の

権利（GDPR 第 78 条第 2 項）、監督当局の決定に対する司法救済の権利（GDPR 第 78 条第 1 項第 3 項）が認められている。また、GDPR に違反する取扱いにより財産的な損害又は非財産的な損害を被った者は、管理者又は処理者から損害の賠償を受ける権利を有するとされている（GDPR82 条１項２項）。この場合、管理者又は処理者は、当該損害を生じさせた出来事につきいかなる意味においても責任を負わないことを証明したときは法的責任を免れるとされている（同条３項）。

個人情報保護委員会の考え方によれば、かかる被害回復制度についても、「**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の枠組みは有効な選択肢となり得る。**」としている。

適格消費者団体による被害回復制度の枠組みとして、消費者裁判手続特例法の共通義務確認の訴えがある。共通義務確認の訴えとは、消費者契約に関して相当多数の消費者に生じた財産的被害等について、事業者等が、これらの消費者に対し、これらの消費者に共通する事実上及び法律上の原因に基づき、個々の消費者の事情によりその金銭の支払請求に理由がない場合を除いて、金銭を支払う義務を負うべきことの確認を求める訴えのことをいう（同法２条４号）。共通義務確認の訴えは、適格消費者団体のうち、差止請求関連業務を相当期間にわたり継続して適正に行っており、被害回復のための組織体制や業務規程を適切に整備し、理事に弁護士を選任していること等の要件を満たし、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回復を求めるため裁判手続を行うのに必要な適格性を有するとして内閣総理大臣より認定を受けた者（特定適格消費者団体）が提起することができる（同法７１条）。従前、共通義務確認訴訟の対象となる損害に慰謝料（精神的損害）は含まれていなかったが、令和４年改正により、①その額の算定の基礎となる主要な事実関係が相当多数の消費者について共通するものであり、かつ、②財産的請求と併せて請求されるもので財産的請求と共通する事実上の原因に基づくもの、若しくは事業者の故意によって生じたものについても対象となった（同法３条２項６号）。実際の被害回復の流れは次のとおりである。まず、第１段階として、特定適格消費者団体が、事業者側の責任確定のために共通義務確認の訴えを提訴する。勝訴判決や和解等によって事業者側の責任が確定した場合、第２段階として、①特定適格消費者団体が裁判所に個別の消費者の債権を確定するための手続に入ることの申立て、②特定適格消費者団体・事業者から対象となる消費者へ情報提供、③消費者が特定適格消費者団体に依頼、④特定適格消費者団体は依頼のあった消費者の債権を集約して裁判所に届出、⑤事業者と特定適格消費者団体（消費者）間の協議による決着も可能だが、決着がつかない場合は裁

判所が簡易な手続のもとで決定を行う（簡易確定決定）、⑥協議内容や簡易確定決定に従い、事業者が金銭を支払う。

しかし、これはあくまで「消費者契約に関する」請求のみが対象となるため、「消費者契約に関する」ものではない個人情報保護法違反による損害賠償請求は対象とはならない（消費者裁判手続特例法３条１項柱書）。また、個人情報保護委員会は「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。」とする。

前者の問題点（極端な少額大量被害事案）については、通常、少額被害事例では、被害者が制度に参加するための費用負担の方が賠償額より大きくなる可能性が高く、また、被害回復業務に従事する特定適格消費者団体も、被害者から支払いを受ける報酬額だけでは回復業務に要する費用をまかなえない可能性が高い点が問題であるとされている。後者の点（立証の問題）については、個人情報漏えいやその他法令違反につき、先行した個人情報保護委員会による勧告・命令等がある場合には、委員会が有している情報に特定適格消費者団体がアクセスできるようにするなどの手当が必要だろう（なお、特定適格消費者団体において、消費者裁判手続特例法 96 条に同趣旨の規定がある）。

そこで、**個人情報保護法の改正により、同様に共通義務確認訴訟や同訴訟を行う適格団体の認定に関する規定が追加される可能性**がある。

しかしながら、個人情報保護委員会の考え方によれば「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」るとのことであり、また、「導入の必要性も含めて多角的な検討を行っていく必要がある」とトーンダウンした書き方がされていることからすると、**改正の実現可能性は低い**ように思われる。

第２　実効性のある監視・監督の在り方

１．課徴金、勧告・命令等の行政上の監視・監督手段の在り方

（１）課徴金制度

ア．個人情報保護委員会の考え方

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。

イ．改正の方向性

①課徴金制度の導入（実現可能性：70%）

課徴金制度は、個人情報の不適切な取扱いについて、金銭的な不利益を課す行政上の措置であり、我が国においては独占禁止法、景品表示法、金融商品取引法などにおいて導入されている。諸外国の個人情報保護法制にも目を向けると、EU や米国カリフォルニア州、カナダ、中

国、韓国においては、既に課徴金（制裁金）制度が導入されており、既に多額の制裁金を課している執行事例も確認されている。

我が国の個人情報保護法への課徴金制度の導入については、平成 27 年改正法、令和２年改正法の検討時においても議論されていたが、いずれも「引き続き検討」とされ、導入には至っていない。

もっとも、**今般の「３年ごと見直し」では、多くの有識者が課徴金制度の導入に積極的であり、何らかの形での導入が予想される。**

②「利益の吐き出し」に留まらない課徴金の賦課（実現可能性：40%）

課徴金制度の導入にあたっては、課徴金賦課の対象となる違法行為類型及び類型ごとの課徴金の算定方法が問題となる。個人情報保護委員会の「考え方」に例示される「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」については、日本における課徴金制度の多くが「利益の吐き出し」を主たる目的としていることとも整合的であり、導入のハードルはさほど高くないと思われる。

もっとも、「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」については、「本来なすべき支払」の算定にはフィクションを用いる必要があると考えられるし、その結果として「事業活動から得られる利益」の「増加」に係る算定についてもフィクションを用いる必要があろう。課徴金の算定に当たり幾重にもフィクションを重ねなければならないような制度設計の実現可能性には疑問の余地もあり、未だ課題が多いように思われる。

今般の改正により課徴金制度が導入されるとしても**「（名簿屋等がオプトアウト手続に違反する等して、）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」をなど、個人情報の不適切な取扱いと事業者の利益との繋がりが比較的明確な違法行為類型から「スモールスタート」する**ことになるのではないか。

（２）勧告・命令の在り方

ア．個人情報保護委員会の考え方

> **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。**

イ．改正の方向性

①緊急命令の要件緩和（実現可能性：30%）

個人情報保護委員会は、一定の個人情報保護法違反行為があった場合において、「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」は、勧告を前置することなく、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べきことを命ずることができる（いわゆる「緊急命令」。法 148 条３項）。

もっとも、個人情報保護員会が緊急命令を発した事案は、知る限りない。緊急命令の対象が一部の法令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しており、発動要件が厳格だからであろう。例えば、新破産者マップ事案についても、勧告、命令、告発という順次の対応に半年もの期間を要している。

その反面、未だ個人の権利利益の侵害が生じていないにもかかわらず、いきなり「命令」という強力な行政処分を行うことの是非については慎重な検討が要請される。むしろ新破産者マップ事案のような事案であれば現行法の解釈においても緊急命令を発する余地はあったと考えられることから、**法改正によらず、緊急命令の発動をより柔軟に運用することでも足りるのではないか。**

②第三者命令（実現可能性：50%）

第三者命令とは、一定範囲の第三者、すなわち、同法違反の事案であることを知りながら手を貸していると認められる第三者に対して行う措置命令をいう。個人情報保護委員会の「考え方」においても、「**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**」について検討することとされている。

例えば、違法に個人情報を晒すようなウェブサイトの運営者に対して「命令」や「緊急命令」を発出したとしても、当該ウェブサイト運営者が命令に従うとは限らないため、当該ウェブサイト運営者のみならず、例えば検索エンジン運営者等の周辺者に対しても一定の措置を命じ

ることは、迅速かつ実効的な権利利益の保護の観点から必要不可欠であると考えられるため、積極的な議論が望まれる。

もっとも、例えば第三者として典型的に想定されるであろう検索エンジン運営者の担う情報流通の基盤としての役割の重要性にかんがみれば、こうした価値との比較衡量においてなお**一定の行政上の措置を講ずべきといえるほどの必要性が要求されるべき**であろう。

２．刑事罰のあり方

（１）個人情報保護委員会の考え方

> **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。**

（２）改正の方向性

①個人情報の不正取得の直罰化（実現可能性：50%）

現行法において、民間事業者が直罰規定の対象となるのは、いわゆる「個人情報データベース等不正提供等罪」（法 179 条・法 184 条１項）のみである（そのほか「行政機関等の職員等」や「行政機関等の職員等であった者」を名宛人とする直罰規定がいくつか存在する。）。

もっとも、**近時の悪質事案の類型が様々である**こと、とりわけ**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、直罰規定の範囲拡大が検討されている。その背景として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が多数報告されていることや、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「かたり調査」のトラブルが発生していることが挙げられる。このようないわば「極悪層」による「個人情報の詐取等の不正取得」を法の直罰規定の対象に含めることについては積極的な議論が望まれる。

その一方で、直罰規定の新設がいわゆる「遵法層」を委縮させないようにすることも重要である。例えば「個人情報の詐取等の不正行為」は現行法の下でも法 20 条１項[18]違反であると解されるが、カメラによる個人情報の取得の場面においては、「カメラにより自らの個人情報

[18] 個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

が取得されていることを本人において容易に認識可能といえない場合には、容易に認識可能とするための措置を講じなければなりません（法第 20 条第１項）。」[19]とされており、とりわけ遵法層は、個人情報の取得が本人にとって「容易に認識可能」でなければ法 20 条１項違反となりかねないものとして慎重に対応している。

そのため、「個人情報の詐取等の不正取得」のような「極悪」行為を法の直罰規定の対象とするにしても、例えば法 20 条１項違反にそのまま直罰規定を置くべきではなく、要件を加重するなど「極悪層」を対象としていることが分かるような工夫が望まれる。

そこで、筆者らとしては、個人情報の不正取得の直罰化についての実現可能性については、高くないものと考える。

３．漏えい等報告・本人通知の在り方

（１）漏えい等報告

ア．個人情報保護委員会の考え方

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**

[19] 「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&A１-13 参照

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。

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．改正の方向性

①認定個人情報保護委員会被確認事業者に対する漏えい等事案対応の緩和（実現可能性：80%）

「個人情報保護委員会の考え方」では、『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。』とされている。

「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た事業者」（以下「認定個人情報保護委員会被確認事業者」という。）としては、認定個人情報保護団体である一般財団法人日本情報経済社会推進協会（以下「JIPDEC」という。）のプライバシーマークを付与された事業者が想定される。プライバシーマーク制度は、事業者の個人情報を取扱う仕組みとその運用が適切であるかを評価し、その証として事業活動においてプライバシーマークの使用を認める制度である。プライバシーマーク制度は、日本産業規格「JIS Q 15001　個人情報保護マネジメントシステムー要求事項」（以下「JIS Q 15001」という。）をベースとした審査基準による審査を経て、事業者の個人情報の取扱いが適切であるかを評価する。JIS Q 15001は、個人情報保護法等、法令への遵守も包含している。

認定個人情報保護委員会被確認事業者における小規模漏えい等事案に関する速報義務の免除及び確報の一定期間ごとの取りまとめ報告については、金融分野における業法上の報告において一部導入されている。その内容は次のとおりであり、このような金融分野における取扱いは、今後の改正内容を占うにあたっても参考になるのではないかと思われる。

・ＦＡＸの誤送信、郵便物等の誤送付、メールの誤送信等については、金融機関が個別の事案ごとに、漏えい等した情報の量、機微（センシティブ）情報の有無及び二次被害や類似事案の発生の可能性等を検討し、「速やかに」報告を行う必要性が低いと判断したもので

あれば、業務の手続の簡素化を図る観点から、四半期に一回程度にまとめて監督当局に報告することも差し支えない。
・郵便局員による誤配等、金融機関の責めに帰さない事案については、監督当局に報告する必要はないと判断しても差し支えない。ただし、「本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さい」とはいえない場合には、漏えい等した情報の量、機微（センシティブ）情報の有無及び二次被害や類似事案の発生の可能性などを検討した上で、都度「速やかに」又は四半期に一回程度にまとめて報告を行う必要がある。
・いかなる場合でも、漏えい等事案の事実関係等を公表する場合には、都度「速やかに」監督当局に報告する必要がある。

②いわゆる「おそれ」要件の明確化（実現可能性：90%）

漏えい等事案に関するいわゆる「おそれ」要件については、その外縁が不明確であり、現状の実務においては、いわば“絶対大丈夫以外全部”「おそれ」要件を充足することが前提とされているように思われ、事業者に対して大きな負担が生じている。

産業界の各事業者団体からも「おそれのある事案」をすべからく報告するのは過度の負担であるとして緩和の強い要望がある[20]。

要望の具体的な内容は以下のとおりである。

- まずは、本法に基づく漏えい等報告によってこれまで蓄積されたデータベース（例：漏えい等報告の実態や報告の活用状況等）を踏まえ、エビデンスに基づき、検証した結果を公表すべき
- その上で、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

たとえば、アクセスログ等の網羅的な確認が困難な事案であったとしても、他に漏えい等の徴候が認められない場合には、漏えい等の「おそれなし」として良いのではないか。

なお、他の漏えい等の徴候にもグラデーションがあり、いわゆるダークウェブの調査等の積極的調査を要するのか、本人からの特段の被害申出がないことの確認をもって足りるのかは、漏えい等が疑われるデータの性質等に応じて柔軟な対応が許容されるべきである。

いわゆる「おそれ」要件の具体化は、法令改正というよりもガイドラインの改定により一定の手当がなされる可能性もあるが、まさに現在生じている実務上の混乱や過度な負担の軽減

[20] 「個人情報保護法の3年ごと見直しに対する意見」（2024年4月4日）（日本経済団体連合会、日本商工会議所、経済同友会、新経済連盟、日本IT団体連盟、Fintech協会、シェアリングエコノミー協会、プライバシーテック協会）（https://www.ppc.go.jp/files/pdf/240424_shiryou-1.pdf）において、「漏えい等報告等の負担軽減」が共通の意見として個人情報保護委員会に提出されている。

の観点から、より迅速なガイドラインの改定対応に期待したい。

（2）違法な第三者提供

ア．個人情報保護委員会の考え方

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。**

イ．改正の方向性

①違法な第三者提供の報告等（実現可能性：70%）

我が国における現在の実務上、「漏えい」と「提供」とは両立し得ない概念であり、両社の分水嶺は事業者の「意図」にあるとされる。その「意図」は、①第三者に提供する意図があるか（提供自体）、②意図した提供先に提供されているか（提供先）、③意図した個人データが提供されているか（個人データの対象・範囲）を踏まえて判断される[21]。

もっとも、このような「意図」は、本人の権利利益侵害のおそれとはさほど関係がないように思われ、違法な第三者提供であれば本人通知等のプロセスを経る必要がないとする現行法の規定にはややアンバランスな印象も拭いきれない。すなわち、過失によるうっかりの漏えいの場合は漏えい等報告が必要であるのに対して、故意による漏えいについては法 27 条の第三者提供制限の違反とはなるものの漏えい等報告は必要はないというのは不均衡であると考えられる。

海外に目を向けると、GDPR は、漏えいと違法な個人情報の取扱いとを区別せず、「データ侵害」との概念を用いている。このような GDPR における取扱いは、本項目に関する今後の改正内容を占うにあたっても参考になろう。

第３　データ利活用に向けた取組に対する支援等の在り方

１．本人同意を要しないデータ利活用等の在り方

（1）個人情報保護法保護委員会の考え方

[21] 椎名紗彩「実務問答個人情報保護法『漏えい』の考え方」NBL1262 号 46 頁参照

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）改正の方向性

①公共性が高いと考えられる技術やサービスについて（実現可能性：70%）

現行法において、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

るところ、例外は「法令に基づく場合」や「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」などに限定されている。このように、我が国の個人情報保護法は、本人の同意がなければ個人データの利活用が難しいところ、「**個人情報保護委員会の考え方**」によれば、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（生成 AI など）について、「**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**」とされた。

生成 AI と個人データとの関係では、事業者が AI を利用する場合との関係で、AI 事業者が個人データを機械学習目的に利用しないことの確認をもって、プロンプト入力を通じた個人データの送信が個人データの「提供」に該当するか否かという問題がある。この点について、「生成 AI など、…、**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**」とされ、個人データを生成 AI に入力することは、個人データの提供に該当するとも考えられる。すなわち、事業者が ChatGPT を利用して書類を作成する際、個人データを入力した場合、当該行為が個人データの第三者提供に該当し、本人の同意が必要になる可能性がある。

「公益性が高いと考えられる技術やサービス」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**」とされ、個人データの第三者提供の例外で対応するものと推測される。もっとも、「『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」とされており、現時点において、例外規定の内容は定まっていないと思われるが、生成 AI との関係では何らかの措置がとられると予想される。

個人情報保護委員会の有識者ヒアリングにおいては、「個人情報を AI が一般的な知識の一環として利活用すること」が個人情報保護法に例外規定として設けることが議論されている[22]。

ただし、例外規定を設ける場合には、一定の要件が必要であり、情報源とアーキテクチャが重要であり、インターネット上に公開されているデータの扱い方、たとえば、ニューラルネッ

[22] 第 279 回個人情報保護委員会（https://www.ppc.go.jp/aboutus/minutes/2024/20240403/）における、NTT 社会情報研究所高橋チーフ・セキュリティ・サイエンティストの提出資料「AI 利用と個人情報の関係の考察」に関する個人情報保護委員会委員との議論（議事録・議事概要参照）。

トワークにおいて、不適切なプロファイリングといった利用は禁止されるべきであるし、出力に関しても不適正な利用は問題となるとされている。

これに対して、AI の活用の観点から安全管理措置を追加的に講じることについては消極的な意見がなされている。

②医療機関等における研究活動等に係る利活用における例外（実現可能性：70%）

医療機関等における研究活動との関係でも、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。この例外が認められる場面は、「公衆衛生の…ために特に必要がある場合であって、本人の同意を得ることが困難であるとき」や学術研究目的で個人情報を取り扱う一定の場合（個人の権利利益を不当に侵害するおそれがある場合を除く）に限られており、その内容も明確とはいえない。

そこで、「**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**」とされ、医療に関するデータについても、本人の同意なく個人データの授受を行うことができる場面の例外規定が検討されている。

個人情報保護法の有識者ヒアリングにおいては、現行の個人情報保護法や次世代医療基盤法[23]について以下のとおり、個人データの取得・利用時の『同意』『匿名化』の偏重という課題が挙げられている[24]。

- 『同意』に関しては、最初の受診は同意を取って行うが、他の診療科を受診してもらう場合や救急の場合に患者が重篤でも同意を求めたり、高齢者の方にしっかりと説明をして同意してもらったりすることが、医療及び救急の現場で負担になっている。
- 緊急の場合や意思能力がない場合は、いわゆる公衆衛生例外（「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がある場合であって、本人の同意を得ることが困難であるとき」には、同意なき目的外利用（法 18 条３項３号）や同意なき第三者

[23] 正式名称は「医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律」である。
[24] 第 279 回個人情報保護委員会における、森田朗（東京大学名誉教授・（一社）次世代基盤政策研究所（NFI）代表理事）の「医療情報の利活用の促進と個人情報保護」に関する個人情報保護委員会委員との議論（議事録・議事概要参照）。

提供（法 27 条１項３号）を認める例外）が適用され得るが、医療現場では、その人に本当に意思能力があるのかを医師が容易に判断できない場合があり、明らかに同意が不要と判断できる場合もあるだろうが、同意を取るべきか否か判断が難しい領域が広く、医師としては判断を誤り、同意を取得できるのに取らなかった場合に責任を問われる可能性がある。そこで、しっかりと説明をして、説得して同意を取るための負担が発生する。公衆衛生例外は適用される場面が不明確である。

- 二次利用（医学研究）に関しては、多くの医学研究には、遡及的なデータの確認、事後的な追跡調査が必要であり、次世代医療基盤法の「匿名加工情報」では、研究や医薬品等の開発には利用できない。次世代医療基盤法の改正により、「仮名加工情報」の利用も可能となったが、丁寧なオプトアウトが求められているため負担が多く、現在このスキームに参加している医療機関等が限られているという問題がある。

有識者である森田朗東京大学名誉教授からは、欧州議会・理事会が暫定合意した EU における European Health Data Space（EHDS）を参考に以下のような新たな規制体系を設けることが提案されている[25]。

■ **「入口規制」から「出口規制」へ**
- 原則として、**データ取得時、新たな提供時の同意は不要**とし、取得したデータへの**アクセスを規制**する。

■ **一次利用**
- 本人の治療という目的のために必要な場合には、原則として同意なしに、関与する医療従事者にアクセスを認める。
- 関与した医療従事者の守秘義務による保護
  ※ データの欠落が医療の質を保証しないことを告げた上で、マスキング（アクセス制限）を認めるかは検討課題。

■ **二次利用**
- データの**利用目的、アクセス権、加工形態**に応じたアクセスの規制
- 仮名化を原則とし、匿名化、利用禁止等の措置は、現実的・具体的な**リスクベース**に基づいて行う（※ 特定の場合に、**オプトアウト**を認めるか否かは、検討課題）
- 利用規制（基準設定・利用許可・監視・利用状況の公表）のための**公的機関**の設置

■ 個人情報の保護に限らず、医療データの積極的な利活用を図るための基準・手続等を定めるために、利活用を目的とした**特別法（特例法）**の制定を検討すべき

■ **個人情報保護法との関係**
- 個情法の適用を受けない異なる体系の法を制定するのではなく、個情法に定める法令上の根拠として「生命、身体、財産保護」「公衆衛生」「学術研究」を上記の出口規制の趣旨を反映した同意を不要とする場合として具体化・明確化する
- 個情法の改正が必要な場合には、次期および次々期見直し期に検討

■ 次世代医療基盤法との調整
- 二次利用の制度として制定され、改正された次世代医療基盤法については、同様に３年後の見直しを機に、特別法に統合すべき

[25] 「医療情報の利活用の促進と個人情報保護」（森田朗東京大学名誉教授）（https://www.ppc.go.jp/files/pdf/240403_shiryou-1-3.pdf）参照。

森田名誉教授が提唱するような特別法が制定されるか否かは別として、医療現場（一次利用）における「同意」や「公衆衛生例外」については、法律上の見直しまたはガイドラインにおいて解釈規定が設けられる可能性があるだろう。

（3）「契約の履行」や「正当な利益」などの例外規定について

業界団体からは、目的外利用（法 18 条１項）や第三者提供（法 27 条１項）の同意に関する例外規定として、GDPR における「契約の履行」や「正当な利益」のように、一定の条件下で個人情報を本人同意なく取り扱うことができる場合について検討をすることが要望されている（EBC・新経済連盟）。

しかしながら、「個人情報保護委員会の考え方」においてはこれらの例外規定については明示的に検討対象となっていない。

我が国の個人情報保護法が「本人の同意」を重視する制度であり、本人の同意がない場合には原則として特定された利用目的の範囲でしか個人情報を利用できず、限られた公益的理由がなければ取扱いが認められない制度であることに鑑みると、柔軟性の高い「契約の履行」や「正当な利益」のような取扱いは困難と個人情報保護委員会が考えているのではないかと思われる。

２．民間における自主的な取組の促進

（1）個人情報保護委員会の考え方

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。

（2）改正の方向性

①PIA の義務化（実現可能性：50%）

PIA とは、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である[26]。

「**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**」とされ、PIA の導入が義務化される可能性は低いものの、その取組み自体は一層促進されると考えられる。

このような方針からすれば、PIA の導入は、安全管理措置に加え、レピュテーションの観点からも有用であると考えられる。

一方で、PIA の導入には相応のコストがかかることから、取り扱う個人データの性質や量を踏まえ、導入の可否やその内容を判断する必要があるように思える。

②個人データの取扱いに関する責任者の設置（実現可能性：60%）

「**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**」とされている。現在、海外の多くの個人情報保護法令において DPO（GDPR にいう DPO ではなく、一般的な意味での DPO）の設置が義務規定化されており、個人情報の保護と管理においてはこのような個人情報保護実務専門家の設置が必要不可欠になっていることからすると、法令上の努力義務など、現行の措置より踏み込んだ規制がなされることが予想される。

そこで、責任者の資格要件や設置を求める対象事業者の範囲が問題になるところ、各事業者の事業内容（例えば、当該事業者が扱う個人データの質や量等）や企業規模によって、責任者の要否や業務内容が変わると考えられる。また、国内の他の法令における事業者の責務として責任者を置く旨の努力義務が定められている（犯罪収益移転防止法 11 条、暴力団対策法 32 条の 2 等）ところ、これら責任者の業務内容との関係が問題になることもあろう。

---

[26] 個人情報保護委員会「PIA の取組の促進について-PIA の意義と実施手順に沿った留意点-」(2021 年 6 月 30 日)https://www.ppc.go.jp/personalinfo/independent_effort/