

## Miyake newsletter

### 個人情報保護法ニュースNo. 7

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『「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』をご案内させていただきます。

令和6年4月1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

弁護士渡邊雅之、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

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）2月21日に公表した『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』（委員長預かりで会議後に修正した資料）<sup>1</sup>（令和6年2月21日 個人情報保護委員会事務局）および関係団体へのヒアリングにおける資料を参考に、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（星（5段階）で評価。★の個数が多いほど実現可能性が高いと考える。たとえば、「★★★☆☆」は、5段階中、星3つの評価である。）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。

#### （スケジュール）

##### 2023年

9月27日 「改正個人情報保護法の施行状況について①」<sup>2</sup>公表（第255回委員会）

10月18日 「改正個人情報保護法の施行状況について②」<sup>3</sup>公表（第258回委員会）

11月15日 「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」<sup>4</sup>公表

11月下旬～ 関係団体等ヒアリングを順次実施

##### 2024年

2月21日 「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」公表

2月下旬～ 有識者ヒアリングを順次実施

春頃 「中間整理」公表

#### （関係者ヒアリング）

<sup>1</sup> [https://www.ppc.go.jp/files/pdf/240221\\_shiryoku-4syuuseigo.pdf](https://www.ppc.go.jp/files/pdf/240221_shiryoku-4syuuseigo.pdf)

<sup>2</sup> [https://www.ppc.go.jp/files/pdf/230927\\_shiryoku-1.pdf](https://www.ppc.go.jp/files/pdf/230927_shiryoku-1.pdf)

<sup>3</sup> [https://www.ppc.go.jp/files/pdf/231018\\_shiryoku-1.pdf](https://www.ppc.go.jp/files/pdf/231018_shiryoku-1.pdf)

<sup>4</sup> [https://www.ppc.go.jp/files/pdf/231115\\_shiryoku-2-1.pdf](https://www.ppc.go.jp/files/pdf/231115_shiryoku-2-1.pdf)

2023年11月29日	一般社団法人日本情報経済社会推進協会（JIPDEC） <sup>5</sup> （第262回委員会）
2023年12月6日	欧州ビジネス協会（EBC） <sup>6</sup> （第263回委員会）
2023年12月15日	新経済連盟 <sup>7</sup> （第264回委員会） 日本IT団体連盟 <sup>8</sup> （第264回委員会）
2023年12月20日	在日米国商工会議所（ACCJ） <sup>9</sup> （第265回委員会）
2023年12月21日	電子情報技術産業協会（JEITA） <sup>10</sup> （第266回委員会） 全国商工会議所 <sup>11</sup> （第265回委員会）
2024年1月23日	消費者支援機構関西 <sup>12</sup> （第268回委員会） 日本商工会議所 <sup>13</sup> （第268回委員会）
2024年1月31日	日本経済団体連合会 <sup>14</sup> （第270回委員会）
2024年2月7日	日本インタラクティブ広告協会（JIAA）（第271回委員会）
2024年2月14日	京都府 <sup>15</sup> （第272回委員会） 岡山市 <sup>16</sup> （第272回委員会） 都城市 <sup>17</sup> （第272回委員会） 上里市 <sup>18</sup> （第272回委員会）

<sup>5</sup> [https://www.ppc.go.jp/files/pdf/231129\\_shiryoku-1.pdf](https://www.ppc.go.jp/files/pdf/231129_shiryoku-1.pdf)

<sup>6</sup> [https://www.ppc.go.jp/files/pdf/231206\\_shiryoku-2.pdf](https://www.ppc.go.jp/files/pdf/231206_shiryoku-2.pdf)

<sup>7</sup> [https://www.ppc.go.jp/files/pdf/231215\\_shiryoku-1-1.pdf](https://www.ppc.go.jp/files/pdf/231215_shiryoku-1-1.pdf)

<sup>8</sup> [https://www.ppc.go.jp/files/pdf/231215\\_shiryoku-1-2.pdf](https://www.ppc.go.jp/files/pdf/231215_shiryoku-1-2.pdf)

<sup>9</sup> [https://www.ppc.go.jp/files/pdf/231220\\_shiryoku-1-2.pdf](https://www.ppc.go.jp/files/pdf/231220_shiryoku-1-2.pdf)

<sup>10</sup> [https://www.ppc.go.jp/files/pdf/231221\\_shiryoku-1-1.pdf](https://www.ppc.go.jp/files/pdf/231221_shiryoku-1-1.pdf)

<sup>11</sup> [https://www.ppc.go.jp/files/pdf/231221\\_shiryoku-1-2.pdf](https://www.ppc.go.jp/files/pdf/231221_shiryoku-1-2.pdf)

<sup>12</sup> [https://www.ppc.go.jp/files/pdf/240123\\_shiryoku-1-1.pdf](https://www.ppc.go.jp/files/pdf/240123_shiryoku-1-1.pdf)

<sup>13</sup> [https://www.ppc.go.jp/files/pdf/240123\\_shiryoku-1-2.pdf](https://www.ppc.go.jp/files/pdf/240123_shiryoku-1-2.pdf)

<sup>14</sup> [https://www.ppc.go.jp/files/pdf/240131\\_shiryoku-2.pdf](https://www.ppc.go.jp/files/pdf/240131_shiryoku-2.pdf)

<sup>15</sup> [https://www.ppc.go.jp/files/pdf/240214\\_shiryoku-2-1.pdf](https://www.ppc.go.jp/files/pdf/240214_shiryoku-2-1.pdf)

<sup>16</sup> [https://www.ppc.go.jp/files/pdf/240214\\_shiryoku-2-2.pdf](https://www.ppc.go.jp/files/pdf/240214_shiryoku-2-2.pdf)

<sup>17</sup> [https://www.ppc.go.jp/files/pdf/240214\\_shiryoku-2-3.pdf](https://www.ppc.go.jp/files/pdf/240214_shiryoku-2-3.pdf)

<sup>18</sup> [https://www.ppc.go.jp/files/pdf/240214\\_shiryoku-2-4.pdf](https://www.ppc.go.jp/files/pdf/240214_shiryoku-2-4.pdf)

## 第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広がっている。

◎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。

### 1. 不適正取得・不適正利用の適用の明確化

#### 【現行法の規律】

##### （不適正な利用の禁止）

**第十九条** 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。

##### （適正な取得）

**第二十条** 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。

#### 【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）

#### 【ヒアリング意見】

##### 【ヒアリングでの意見】

- 「不適正利用の禁止」の規定に関しては、通常考えられるビジネス上での適正な利用とは明らかに異なる不適正な利用など、当該規定に抵触することが**明らかな場合の明確化・例示を示すべき**。例えば、オプトアウト届出事業者が取得した個人情報をデータベース化して公開し、削除の求めに対しては対価を要求している場合などが挙げられる。また、こうした不適正利用事案については、**注意喚起にとどまらず、適切な執行が必要**ではないか。（新経済連盟）
- 「**不適正利用の禁止**」に関する規律がより**実効性のある形**になるよう、生成AIや認証技術の普及等、技術発展に伴う社会の変化を踏まえて、その考え方を検討すべき。（委員）

**【改正予想】（実現可能性★★★★★）**

個人情報保護法 19 条（不適正利用の禁止）、20 条 1 項の規定（不適正取得の禁止）の規定自体についての改正ではないが、通則編ガイドラインに不適正取得・不適正利用の対象となる法令・条項や具体例が追加されることが予想される（通則編ガイドラインには、不適正取得・不適正利用ともに 6 事例の具体例が既にある）。

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指導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。

法律の改正事項ではないので、「いわゆる 3 年ごとの見直し」に先行して、ガイドラインの改正がなされる可能性がある。

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<sup>19</sup>。

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	<ul style="list-style-type: none"><li>● 利用目的の通知・公表義務（法 21 条 1 項）</li><li>● 個人データの安全管理措置義務（法 23 条）</li><li>● 委託先の監督義務（法 25 条）</li><li>● 個人データの第三者提供の同意取得義務（法 27 条 1 項）</li><li>● 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）</li></ul>
事業者	<ul style="list-style-type: none"><li>● 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）</li><li>● 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）</li></ul>
訪問販売を行う販売業者又は役務提供事業者	<ul style="list-style-type: none"><li>● 若年者、高齢者その他の者の判断力の不足に乘じ、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）</li><li>● 顧客の知識、経験及び財産の状況に照らして不相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）</li></ul>

<sup>19</sup> 『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。

## 2. 生体データの取扱い

### 【現行法の規律】

- 以下の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（＝登録された生体情報のある人物の生体情報と照合することで、特定の個人を識別することができる水準であるもの）は、個人識別符号に該当し、個人情報に該当する（個人情報保護法2条・同法施行令1条1号・同法施行規則第2条）。
- 細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列
  - 顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌
  - 虹彩の表面の起伏により形成される線状の模様
  - 発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化によって定まる声の質
  - 歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様
  - 手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状
  - 指紋又は掌紋
  - 上記から抽出した特徴情報の組合せ
- 個人情報取扱事業者は、個人情報である生体情報を取り扱う場合、その他の個人情報を取り扱う場合と同様に、個人情報保護法第4章に規定する個人情報取扱事業者の義務を遵守する必要がある。
- なお、現行法において、個人情報である生体情報の取扱いについて、特別の規律は設けられていない（※）
- （※）金融分野ガイドライン第5条第1項第9号等は、金融分野における個人情報取扱事業者に対して、「機微（センシティブ）情報に該当する生体認証情報」（＝機械による自動認証に用いられる身体的特徴のうち、非公知の情報）について、本人の同意に基づき本人認証に用いる場合を除き、取得、利用又は第三者提供を行わない努力義務を課している。

### 【個人情報保護委員会Q&A】

個人情報保護委員会は、「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」を公表したこと等を踏まえて、2023年5月、「『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」を更新。

#### 【Q&A1-14の主な内容】

- 顔識別機能付きカメラシステムにより特定の個人を識別することができるカメラ画像やそこから得られた顔特徴データを取り扱う場合、従来型防犯カメラの場合と異なり、犯罪防止目的であることだけではなく、顔識別機能を用いていることも明ら

かにして、利用目的を特定しなければならない。

- 顔識別機能付きカメラシステムを利用する場合は、設置されたカメラの外観等から犯罪防止目的で顔識別機能が用いられていることを認識することが困難であるため、「取得の状況からみて利用目的が明らかであると認められる場合」（個人情報保護法第 21 条第 4 項第 4 号）に当たらず、個人情報の利用目的を本人に通知し、又は公表しなければならない。
- 本人から理解を得るためできるだけ分かりやすく情報提供を行うため、顔識別機能付きカメラシステムの運用主体、同システムで取り扱われる個人情報の利用目的、問い合わせ先、さらに詳細な情報を掲載した Web サイトの URL 又は QR コード等を店舗や駅・空港等の入口や、カメラの設置場所等に掲示することが望ましい。
- 照合のためのデータベース（検知対象者のデータベース）に個人情報を登録するための登録基準を作成するに当たっては、対象とする犯罪行為等をあらかじめ明確にし、当該行為の性質に応じ、利用目的の達成に必要な範囲を超えて、個人情報が登録されることのないような登録基準としなければならない（個人情報保護法 18 条 1 項）。

#### 【Q&A1-15 の主な内容】

- 当初防犯目的のために取得したカメラ画像やそこから得られた顔特徴データを、マーケティング等の商業目的のために利用する場合には、あらかじめ本人の同意を得なければならない（個人情報保護法 18 条 1 項）。

#### 【諸外国における生体データの取扱い】

以下の国・地域において、自然人を一意に識別することを目的とする生体データ（以下「生体データ」という。）は、センシティブデータに該当する。

EU（欧州連合）、米国（カリフォルニア州）、中華人民共和国、インド、ブラジル連邦共和国、オーストラリア連邦、大韓民国

#### 【ヒアリング意見】

- 顔識別機能付きカメラや AI の普及に伴い、個人を追跡することによる権利侵害のおそれや、プロファイリングに伴うリスクも高まっている。（委員）

#### 【改正予想】（実現可能性★★★★☆）

個人識別符号に該当する生体データ（特に顔識別データ）については、諸外国でセンシティブ情報として扱われているとおり、要配慮個人情報（個人情報保護法 2 条 3 項）に該当することになり、取得に際して原則として本人の同意が必要となる可能性がある（同法 20 条 2 項）。

もっとも、本人同意が必要となると、顔識別機能付きカメラシステムの利用が困難になる可能性があるため、本人同意が不要となるような例外（Q&A1-14に記載していることを遵守している場合は本人同意不要など）を設ける必要があると考えられる。

### 3. 本人の同意の任意性・同意の撤回権

#### 【現行法の規律】

個人情報保護法には本人からの同意の取得について「任意性（自発性）」が必要であることは定められていない。

#### 【ヒアリング意見】

- 本人同意があれば何でもよいということではなく、当事者の従属関係等も考慮して、実体的な権利利益保護の在り方を検討すべき。（委員）
- 個人情報を提供することがサービスを受けるための条件となっているケースが存在するが、個人情報の取得は、あくまでその目的との関係で必要最小限にとどめるべきではないか。（委員）

#### 【諸外国】

GDPR（EU 一般データ保護規則）では、データ主体（本人）からの「同意」の取得について、「自由に与えられていること」（freely given）として、いわゆる「任意性」が認められている（GDPR 4条(11)）。「同意ガイドライン」においては、同意の任意性について事例が多数提示されており、たとえば、雇用関係においては使用者が雇用者に対して優越的地位に立つため、「同意」を処理（processing）の根拠としてはならず、「契約締結に基づく場合」など他の処理の適法性の根拠によらなければならないとされている。また、データ主体の同意は自由に撤回できるものでなければならない（同意の撤回権）（GDPR 7条3項）とされている。

#### 【改正予想】（実現可能性★★☆☆☆）

いわゆる3年ごとの見直しでは、「代替困難な個人情報取扱事業者による個人情報の取扱いに係る規律の在り方」として議論されることになるが、「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、本人の同意を重視する我が国の個人情報保護法では、同意の効力を緩める方向の改正である「同意の任意性」や「同意の撤回権」を認めるのは困難ではないか。

仮に、取扱いの根拠として、「契約の履行」や「正当な利益」などが認められた場合には実現する可能性はあるが、個人情報の取扱いの法的根拠に係る抜本的な改正が必要となるため、改正の可能性は低いと考えられる。



もっとも、通則編ガイドラインの中で、努力義務的に「代替困難な個人情報取扱事業者」については、「同意の任意性」や「同意の撤回権」のようなものを努力義務的に認める可能性はある。

#### 4. 個人関連情報の適正な取扱いに関する規律

##### 【現行法の規律】

- 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、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいう（個人情報保護法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。
- 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（法31条）。
- 現行法においては、特定の個人を識別しないことを前提とする個人関連情報の取扱いに係る規律は設けられていない。

##### 【ヒアリング意見】

- 個人関連情報のようにそれ単体では特定の個人を識別することのできない情報であっても、その使い方によっては個人の権利利益が侵害される可能性もあると考える。こうしたリスクに対し、より実効性のある対応を検討すべきではないか。（委員）
- 特定の個人への連絡・接触が可能な個人関連情報等は、その取扱いにより特定の個人の権利利益が侵害されるおそれが高く、要保護性が高いといえるのではないか。（委員）

##### 【改正予想】（実現可能性★★★★☆）

「個人関連情報」についても、「個人情報」と同様に、「不適正取得」「不適正利用」の規律が設けられる可能性がある。

#### 5. オプトアウトの規律の厳格化

##### 【現行法の規律】

- いわゆるベネッセ事件を受けて平成27年改正（平成29年4月施行）により、オプ

トアウト手続が厳格化した。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はオプトアウトは認められない。

#### 【ヒアリング意見】

- 「不適正利用の禁止」の規定に関しては、通常考えられるビジネス上での適正な利用とは明らかに異なる不適正な利用など、当該規定に抵触することが明らかな場合の明確化・例示を示すべき。例えば、オプトアウト届出事業者が取得した個人情報をデータベース化して公開し、削除の求めに対しては対価を要求している場合などが挙げられる。また、こうした不適正利用事案については、注意喚起にとどまらず、適切な執行が必要ではないか。（新経済連盟）

#### 【改正予想】（実現可能性★★★★★）

不適正取得・不適正利用の具体例として、通則編ガイドラインなどにオプトアウト届出事業者が取得した個人情報をデータベース化して公開し、削除の求めに対しては対価を要求している場合などが具体例として追加される可能性がある。

### 6. こどもの個人情報等に関する規律の在り方

#### 【現行法の規律】

- 個人情報保護法には、こどもの個人情報の取扱いに関する規律は設けられていない。
- 「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&A1-62 には、「法定代理人等から同意を得る必要がある子どもの具体的な年齢は、対象となる個人情報の項目や事業の性質等によって、個別具体的に判断されるべきですが、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。」との回答がある。

#### 【ヒアリング意見】

- こどもに関する規律は多くの国が設定しており、何らかの規律を設定することが望ましい。（JIPDEC）

グローバルに事業を展開する事業者は対応済であるため、規律を導入した場合も負担なく実施できるのではないか。（例：Amazon）。

日本は、若者の多くがオンラインショッピングを利用したり、スマホ等の保有率利用時間も長時間化するなか、個人の権利利益侵害のリスクを防ぐ手段、或いは被害に遭った後の民事的な救済も、本人（保護者）が行わなければならない。

※JIPDEC 指針：子供、高齢者等からの不適正取得の独自事例を追記

対象事業者から、子供や高齢者の対象範囲について何らかの基準がないと対応が困難という意見もあり。

- こどもの権利利益の保護について、諸外国の議論の動向も考慮しつつ在り方を検討すべき（委員）。

### 【諸外国】

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 歳以上である場合、子どもの個人データの処理は適法とする。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（GDPR 8 条）。

### 【改正予想】（実現可能性★★★★☆）

個人情報保護法を改正して、GDPR のように親権者の同意を要する年齢を具体的に設定するのは、既存の Q&A や民法その他の法令との関係で困難かもしれない。

通則編ガイドラインなどにおいて、子どもの個人情報・個人データに関する不適正取得・不適正利用に該当する場合や同意の取得の方法について明記される可能性はある。

## 7. 個人の権利救済手段の在り方

### 【現行法の規律】

- 個人情報保護法には、個人の権利救済（差止め・損害賠償）に関する規定は設けられていない。
- 個人情報保護法違反に関する適格消費者団体による差止請求（消費者契約法 23 条）は、現状では消費者契約法 10 条（不当条項規制）の解釈等を媒介として取扱いを問題とするケースもあるが、迂遠である上、同条はいわゆる受け皿規定であり、適法・違法の判断が一義的ではない。
- 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。
- 改正消費者裁判手続特例法施行（2023 年 10 月 1 日）まで慰謝料請求が対象から除外されており、同施行後も情報漏洩による慰謝料請求の対象範囲は限定的である。

### 【ヒアリング意見】

- 個人情報保護法違反を根拠に差止請求を可能とすべき。また、消費者裁判手続特例法における請求権の対象制限を撤廃し、個人情報漏えい事案も制度の対象とすべき。（消費者支援機構関西）
- 個人の権利利益の行使ができる環境を、事業者が整備していない場合の対応も明確

化すべきではないか。(JIPDEC)

- 団体訴訟制度について、実務的な問題は存在するものの、個人の権利利益保護のための手段を増やすという観点から検討すべき。(委員)

### 【改正予想】(実現可能性(★☆☆☆☆))

個人情報保護法違反にも様々なものが考えられる(個人情報の不適正取得・不適正利用、本人の同意のない個人データの第三者提供、確認・記録義務違反、個人データの漏えい等)ことや、事前に防止する必要性の程度も様々であることに鑑みれば、端的に個人情報保護法違反を根拠に差止請求を認める制度を設けるのは、産業界からの反対も大きいと考えられ困難ではないかと思われる。

消費者裁判手続特例法による共通義務確認の対象とすることについては、改正消費者裁判手続特例法の導入にあたっても激しい議論があったところであり、また、個人情報漏えいに伴う損害賠償請求は典型的な少額大量被害事案(過去の裁判例による認容被害額は数千円から数万円程度)で被害回復業務に従事する特定適格消費者団体が被害者から支払いを受ける報酬額では回復業務に要する費用を賄えない可能性があることに鑑みると、現状では実現可能性は低いのではないかと思われる。

## 第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している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。

### 1. 課徴金、勧告・命令等の行政上の監視・監督手段の在り方／刑事罰の在り方

#### 【現行法の規律】

- 個人情報保護委員会は、個人情報取扱事業者に対して、報告徴求・立入検査(法146条)、指導・助言(法147条)、勧告・命令(法148条)の監督権限を有する。
- 個人情報保護委員会が個人情報取扱事業者に対して命令ができる場合は限定されている。①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るときに勧告に係る措置をとることを命ずることができ(法148条2項)、②個人情報取扱事業者が個人情報保護法の義務規定に違反した場合であって、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に、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(法148条3項)。

- 個人情報取扱事業者に対する課徴金制度は設けられていない。
- 個人情報保護法上、直接罰としては、個人情報データベース等不正提供罪（法 179 条）（1 年以下の懲役又は 50 万円以下の罰金）しか設けられていない。その他には、命令違反（法 148 条 2 項・3 項）があった場合（法 178 条）の間接罰（1 年以下の懲役又は 100 万円以下の罰金）が定められているのみである。

### 【ヒアリング意見】

- 個人情報を違法に利用等することで巨額の利益を上げる悪質な事案を抑止し、また、不当な利益を回収し得る、課徴金制度の導入等を検討することが望ましい。（日本 IT 団体連盟）
- 現行法における執行と運用の活用状況や効果を十分に分析した上で、更なる対策を講じるなど、罰則の強化や課徴金制度の導入の前の段階で検討することがあるのではないか。（ACCJ：在日米国商工会議所）
- 他国の執行状況も参考に、指導を中心とした対応に限らない実効性のある監視・監督を行ってはどうか。（JIPDEC）

例）グローバル企業が他国で巨額の罰金刑に処された事例への対応  
（Google、Meta 等韓国は罰金刑を執行）

- 海外の事例なども参考に、罰則の水準の引上げや課徴金の導入等を検討すべき。また、日本では「指導」が法執行の中心となっている一方で、主要国では「処分」の数が多くなっており、その背景等を含めて、十分に実効性のある監視・監督の在り方を検討する必要があると考える。（委員）
- いわゆる破産者マップのような特異な事例においては、緊急命令の活用も考えられる。（委員）
- 犯罪のための個人情報の悪用事案など、個人情報保護法単独での対応に限界がある事象についても、悪用の抑止や権益の保護の可能性を検討すべき。（委員）
- 重大な漏えい等事案は企業以外から発覚する事例が多いと考えられるため、虚偽報告だけでなく未報告を厳罰化してはどうか。（JIPDEC）
- 海外の事例なども参考に、罰則の水準の引上げや課徴金の導入等を検討すべき。また、日本では「指導」が法執行の中心となっている一方で、主要国では「処分」の数が多くなっており、その背景等を含めて、十分に実効性のある監視・監督の在り方を検討する必要があると考える。（委員）
- ペナルティの強化については、企業の個人データ利活用を阻害しないよう配慮しつつも、罰則などを引き上げる場合でもその引き上げ幅等については慎重にすべき。（委員）
- 明らかに悪意のあるデータの不正な取得や提供については、迅速な執行を確保するため、罰則の直罰化を検討してはどうか。また、漏えい等報告が義務であることをよ

り実効的に浸透させるため、報告を怠った場合に罰則の対象とすることも検討する必要があるのではないか。(委員)

### 【改正予想】

#### ○緊急命令（法 148 条 3 項）発動の柔軟化（★★★☆☆）

個人情報保護委員会による緊急命令の発動のためには、個人情報取扱事業者の個人情報保護法上の義務違反（不適正利用（法 19 条）、不適正取得（法 20 条）、本人の同意を得ない個人データの第三者提供（法 27 条 1 項）等）があり、かつ、「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」られる必要がある。

「個人の重大な権利利益を害する事実」としてはどのようなものが該当するか（破産者マップ事件など）、類型化してガイドライン等において規定しておけば、緊急命令の発動がしやすくなるのではないか。

#### ○課徴金制度の導入（★★★☆☆）

個人情報保護法違反に関する課徴金制度の導入については従前から議論されてきたが、日本における課徴金制度が、「制裁」ではなく「利益の吐き出し」を主たる目的としていることに鑑みると、導入されるとしても、現行の個人情報保護法 179 条（個人情報データベース等不正提供等罪）などのように、自己又は第三者の不正な利益を図る目的で個人情報保護法を違法な取扱いを行った場合など、適用場面が限定されるのではないか。

#### ○新たな直接罰の導入（★★★☆☆）

個人情報取扱事業者に対する直接罰は現状、個人情報データベース等不正提供罪（法 179 条）のみである。同罪に関しては、2023 年中、転職従業員による名刺データベースへの不正アクセス<sup>20</sup>、大手学習塾の元講師による生徒のデータの持ち出しに適用事例があり、一定の効果があったと言える。

名簿屋から犯罪集団への名簿データの提供など、明らかに悪意のあるデータの不正な取得や提供については新たに直接罰が設けられる可能性があるが、まだ直接罰による適用事例も少ないので、刑罰による対応というよりは行政上の対応（指導・勧告）の強化による対応のフェーズであると考えられる。

#### ○厳罰化（★★★☆☆）

個人情報保護法上の直接罰である個人情報データベース等不正提供罪（法 179 条）は、「1 年以下の懲役又は 50 万円以下の罰金」、命令違反（法 148 条 2 項・3 項）があった場

<sup>20</sup> 「個人情報データベース等不正提供等罪の適用事例等を踏まえた安全管理措置及び漏えい等の報告に関する留意点に関する注意喚起について」（令和 5 年 11 月 16 日・個人情報保護委員会事務局）（[https://www.ppc.go.jp/news/careful\\_information/231116/](https://www.ppc.go.jp/news/careful_information/231116/)）

合（法 178 条）の間接罰は、「1 年以下の懲役又は 100 万円以下の罰金」と比較的刑罰が軽いので、厳罰化される可能性もあるが、まだ直接罰による適用事例も少ないので、刑罰による対応というよりは行政上の対応（指導・勧告）の強化による対応のフェーズであると考えられる。

#### 【ご参考】「指導」と「勧告」の運用について（★★★★★）

個人情報保護委員会による勧告事案は、破産者等情報のインターネット掲載事案<sup>21</sup>など、悪質性が極めて高い事案に限られており、多くの事案は行政指導に留まる。

もともと、個人情報保護法上は、個人情報取扱事業者に命令違反があるときに、その旨を公表することができることとされている（法 148 条 4 項）が、実際には、個人情報保護委員会から行政指導を受けただけでも公表されている。

犯罪者グループ等に名簿を提供する悪質な「名簿屋」事案など、特にオプトアウトの届出をしている名簿屋が犯罪者グループ等に名簿を提供するようなケースについては、不適正利用（法 19 条）や第三者提供の記録の作成義務違反（法 29 条）等により、勧告による対応をする事案が増加することが予想される。

また、行政指導事案も引き続き増えていくと考えられ、個人情報保護委員会による「公表」のサンクションもあるので注意を要する。

## 2. 漏えい等報告・本人通知の在り方

### 【現行法の規律】

- 令和 2 年改正（令和 4 年 4 月施行）により、個人情報保護委員会への漏えい等の報告および本人の通知が義務化され、報告対象となる事態は委員会規則において 4 つ明示されている（法 26 条）。
- 報告対象となる 4 つの事態には、それぞれ「又は発生したおそれがある事態」という報告対象が追加されている。

### 【ヒアリング意見】

- 現在の漏えい等報告の実態や事業者の業務負担の実態等を踏まえ、制度の趣旨・目的に照らしつつ、リスクベースアプローチを取って合理的な範囲に報告対象を絞り込むなど、現在の報告の在り方を見直してはどうか。また、本人通知についても、上記の実態等を踏まえ、その趣旨・目的に照らして必要性が高くないと考えられる場合には、不要としてはどうか。例えば、「漏えいのおそれ」がある事案の場合において、

<sup>21</sup> 「破産者等の個人情報を違法に取り扱っている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（令和 4 年 7 月 20 日）」

(<https://www.ppc.go.jp/news/press/2022/220720/>)

第三者に閲覧された可能性が限りなく低いと考えられる場合などには、報告を要しないか、きわめて簡易な報告を許容してはどうか。また、上記のような場合など、本人が自らの権利利益の保護に必要な措置を講じる必要性が低いと考えられる場合には、本人通知を要しないことを許容してはどうか。(新経済連盟)

- 「不正の目的によるおそれがある漏えい等」については、漏えいしたデータ項目や件数が極めて限定的な場合など、事案によっては個人の権利利益を害するおそれ大きいとは必ずしも整理できない場合もあり、現状一律に報告対象とされているのは事業者側の負担が大きいため、一律に報告対象とするのではなく、「不正の目的によるおそれがある漏えい等」については、漏えいした個人データが「氏名」や「公にされている個人情報」に限定されており住所・電話番号・メールアドレス等の連絡先を含まない場合は、一定件数を超える漏えい等とする。」など、一定の条件を付けることの検討をお願いする。(JEITA)
- 報告対象となる4つの事態には、それぞれ「又は発生したおそれがある事態」という報告対象が追加されているが、「発生したおそれがある」か否かは事業者での判断が難しく、また続発するサイバー攻撃において「おそれのある事案」をすべて報告することは、事業者にとって過度の負担が生じる可能性がある。ガイドラインには「個別の事案ごとに蓋然性を配慮して判断する」とあるが、「おそれのある事態」において実際に「漏えい等事案」となったケースは非常に少ないと考えられるため、個人データの漏えい等がほぼ確実になった段階で報告する等、「おそれのある事案」の定義に関して、個人の権利利益へのリスクと事業者の負担とのバランスを考慮した見直しをお願いする。(JEITA)

#### 【改正予想】(★★★★☆)

個人データの「漏えいのおそれ」が広すぎるという意見は、事業者全般に共通の認識であると考えられる。

「漏えいのおそれ」があれば幅広く報告することが実務上も定着してきているので、法改正の可能性が高いとはいえないが、ガイドラインにおいて、「おそれのある事案」について具体例が明示される可能性はある。

### 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

◎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。

#### 1. 本人同意を要しない公益に資するデータ利活用等の在り方



### 【現行法の規律】

- 個人情報保護法においては、個人情報の目的外利用（法 18 条）や個人データの第三者提供（法 27 条）について、本人の事前の同意の取得が原則とされており、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、公益性が認められる場合に限られる。

### 【ヒアリング意見】

- 個人の権利利益の保護とデータ利活用を実質的に両立する観点からは、個人データの第三者提供について、同意以外の方法についても検討することが適当。例えば、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処理できる場合について、検討を深めるべき。（EBC・新経済連盟）

### 【改正予想】（★★☆☆☆）

- 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」のような取扱いが認められる可能性は高くないと考えられる。
- 仮に、「契約の履行」や「正当な利益」が取扱いの根拠として認められる場合には、そのパートナーとして、「本人の同意」の適用が限定化・厳格化される可能性が高い（上記第 1. 3 参照）。

## 2. 民間における自主的な取組（PIA・DPO）の促進

### 【現行法の規律】

- 個人情報保護法には、GDPR のような PIA（プライバシー影響評価）の実施および DPO（データ保護責任者）の設置についての規定が置かれていない。

### 【ヒアリング意見】

#### OPIA（プライバシー影響評価）の努力義務規定化（JEITA）

- 最近のプライバシー問題はレピュテーションリスクであると同時に、最終的には法令リスク（個人情報保護法違反）となるケースが多く、個人情報保護法違反を防止するために PIA 制度を自主的に導入するケースも増えている。また、PIA は安全管理措置としても有効な措置であることを明確にするためにも、対象案件を限定した上で、努力義務規定化することが望ましいと考えます。

#### ODPO（データ保護責任者）設置の努力義務規定化（JEITA）

- 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

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。国際間でのハーモナイズされた法令遵守や、事業者における個人情報保護と管理の強化を実現するためには、対象事業者や事業分野を限定した上で、DPO 設置を努力義務規定化することが望ましいと考える。

#### 【諸外国】

GDPR では、個人データの処理が、個人の「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) の実施が義務付けている (GDPR35 条)。

また、上記の一般的な意味での「DPO」とは異なるが、GDPR では一定の場合にデータ保護責任者の選任を義務付けている (GDPR37 条)。

#### 【改正予想】 (★★★★☆)

我が国においてもデータガバナンス (プライバシーガバナンス) の重要性が増しており、PIA (プライバシー影響評価) の実施および DPO (データ保護責任者) の設置が努力義務化される可能性は高いと思われる。

### 第 4. ヒアリングに基づくその他の改正が予想される事項

#### 1. クラウド例外

##### 【現行法の規律】

➤ 個人情報保護法には規定はないが、「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 7-53 において、「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、当該個人情報取扱事業者は個人データを提供したことはない」とされており、この場合には、クラウドサービス提供事業者は「第三者」や「委託先」にも該当せず、本人の同意や委託先の監督も不要とされている。

##### 【諸外国の法令】

➤ 我が国のクラウド例外のような規定は見当たらない。  
➤ GDPR においては、クラウドサービス提供事業者も「処理者」(processor) として、個人情報保護法における「委託先」に近い取扱いとされている。

##### 【ヒアリング意見】

➤ 個人データを取り扱わないこととなっている場合に該当する (させる) ための標準的

な契約条項の記載例や、適切なアクセス制御例を具体的にガイドライン等で示すことの検討してほしい。(JEITA)

- いわゆる「クラウド例外」については、現在の Q&A のアプローチに基づいて実務に定着し有効に機能しているところ、追加の条件等の付加には慎重を期し実務上の混乱なきよう進めるべき。(経団連)

#### 【改正予想】(★★☆☆☆)

- クラウド例外は、諸外国の個人情報保護法制から見ても緩い規制である。もっとも、実務上定着しているため、追加の条件等を付するなどの厳格化は困難ではないかと思われる。
- 近時、株式会社エムケイシステムに対する行政指導<sup>22</sup>を契機として、個人情報保護委員会により「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」(令和6年3月25日付)<sup>23</sup>が公表されたところであるため、これを踏まえたガイドラインによる具体化の可能性はある。  
具体的には、「単純なハードウェア・ソフトウェア保守サービスのみを行う場合で、契約条項によって当該保守サービス事業者が個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等には、個人データの提供に該当」しないこととされている(Q&A7-55)が、「保守サービス」について、上記行政指導・注意喚起指摘されたとおり、以下のような場合は、「クラウド例外」は使えず、「個人データの委託」とみなされ、委託先管理の対象となることが記載されると考えられる。

○ 利用規約において、クラウドサービス提供事業者が保守、運用上等必要であると判断した場合、データ等について、監視、分析、調査等必要な行為を行うことができること及びシステム上のデータについて、一定の場合を除き、許可なく使用し、又は第三者に開示してはならないこと等が規定され、クラウドサービス提供事業者が、特定の場合にクラウドサービス利用者の個人データを使用等できることとなっていたこと。

○ クラウドサービス提供事業者が保守用 ID を保有し、クラウドサービス利用者の個人データにアクセス可能な状態であり、取扱いを防止するための技術的なアクセス制御等の措置が講じられていなかったこと。

<sup>22</sup> 「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」(個人情報保護委員会・令和6年3月25日)

([https://www.ppc.go.jp/news/press/2023/240325\\_houdou/](https://www.ppc.go.jp/news/press/2023/240325_houdou/))

<sup>23</sup> [https://www.ppc.go.jp/news/careful\\_information/240325\\_alert\\_cloud\\_service\\_provider/](https://www.ppc.go.jp/news/careful_information/240325_alert_cloud_service_provider/)

○ クラウドサービス利用者と確認書を取り交わした上で、実際にクラウドサービス利用者の個人データを取り扱っていたこと。

- 産業界からの要望に応じて、クラウド例外についての「標準的な契約条項の記載例」、「適切なアクセス制御の例」に関する個人情報保護委員会の公式見解の公表にも期待したい。

## 2. 生成 AI が出力した個人情報の取扱い

### 【現行法の規律】

個人情報保護委員会が公表している「生成 AI サービスの利用に関する注意喚起」（令和 5 年 6 月 2 日）<sup>24</sup>においては、以下の注意喚起がなされている。

- 個人情報取扱事業者が生成 AI サービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること。
- 個人情報取扱事業者が、あらかじめ本人の同意を得ることなく生成 AI サービスに個人データを含むプロンプトを入力し、当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該個人情報取扱事業者は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成 AI サービスを提供する事業者が、当該個人データを機械学習に利用しないこと等を十分に確認すること。

上記のとおり、個人情報保護委員会の注意喚起においては、個人情報保護法の利用目的規制との関係では、一定の考え方が示されているものの、個人データの第三者提供規制との関係では、プロンプト入力を通じた個人データの送信が「提供」に該当しない場合についての考え方は示されていない。

### 【ヒアリング意見】

- 生成 AI が出力した内容に個人情報が含まれる場合、事業者はその個人情報をどのように取り扱うべきか（例えば、どのような場合に個人データに該当し個人データとして保護しなければならないか、出力内容に含まれる個人データの正確性をどのように確保したらよいか等）について、ガイドラインや Q&A において明確化（または論点整理）をお願いしたい。（JEITA）
- 個人の権利利益の保護や事業者の負荷軽減に資するガイドラインや Q&A の充実、適

<sup>24</sup> [https://www.ppc.go.jp/files/pdf/230602\\_alert\\_generative\\_AI\\_service.pdf](https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf)

宜修正は歓迎。生成 AI など日進月歩で発展する新しい技術については、関係事業者も交えた検討を進めつつ、イノベーションや健全な成長を阻害することがないように、ガイドライン等の記載は必要最小限にとどめるべき。(経団連)

**【改正予想】(★★★★☆)**

- 生成 AI のプロンプト入力個人データの第三者提供規制との関係でどう整理するかについては慎重に検討が進められるだろう。
- 個人情報保護委員会第(第 275 回)議事概要<sup>25</sup>においては、「三つ目に、新しい技術について、現状の生成 AI に見られるように、技術革新の行方を確実に予想することは困難かと思う。そのため、これらについては、安易に規制して、技術の進展を阻害することは避けるべきではないか。」(小川委員発言)として、生成 AI を含む新しい技術について規制方向での改正に慎重な発言もなされていることから、あり得るとしてもグレーゾーンを解消するようガイドラインにおいて具体化するに留まるのではないかとと思われる。特に、「クラウド例外」の考え方を類推適用して、学習モデルに利用されない場合には、「提供」に該当しないという考え方が示されるかが注目される。

---

<sup>25</sup> <https://www.ppc.go.jp/aboutus/minutes/2023/20240306/>