

# 個人情報保護法3年ごと見直し令和6年に対する意見

国立研究開発法人産業技術総合研究所 高木浩光

2024年6月12日

## 目次

1. 主要意見
  - 1.1. 目的内の提供
  - 1.2. 統計量への集計
  - 1.3. 要配慮個人情報の取得
  - 1.4. 個人データへの統一
2. 総論
  - 2.1. 個人情報保護法の法目的
  - 2.2. 特別カテゴリの意義
3. 各論

## 1. 主要意見

我が国の個人情報保護法（日本法）は、1980年のOECDガイドラインの8原則に準拠する形で規律が構成されているとされる<sup>1</sup>ものの、実際には、その8原則の肝心の趣旨（後述）を踏まえておらず、準拠というには不足する規制がある一方で、8原則が求めている過剰な規制が含まれていることから、そのことが、昨今の経済界の改善要望<sup>2</sup>につながっているものと思われる。

平成27年改正で附則に3年ごと見直しが規定されたのは、こうした規律の凹凸の存在が認識されたからこそであり、今回の見直しもその観点で取り組むべきものとする。そのような観点で見直す余地のある「過剰な規制」と「不足する規制」には、以下のものがある。

### 1.1. 目的内の提供

第1に、個人データの第三者提供の規律が、民間部門においては、目的外での提供だけでなく目的内での提供をも本人同意を原則とする規制となっているが、OECD 8原則は、目的外の利用・提供を問題にしているにすぎない。EU法においても、GDPRでは、その前身である1995年のデータ保護指令（DPD）の時点から、問題としているのは基本的には目的外の利用・提供であって、目的内の提供については、適法性根拠の「契約の履行」「正当な利益」に該当する場合には、例外としてではなく、本人同意によることなく許される規律となっている。日本法も、公的部門については、昭和63年法<sup>3</sup>の時点から目的外の利用・提供のみを制限しており、現行法もそれを踏襲している。

経済界の要望には、EU法に倣って「契約の履行」「正当な利益」に基づく第三者提供を可能にするべきとの意見が含まれており、これらは目的内の提供に相当するものである。しかし、その要望を取り入れるには、いくつかの点で現行法の構造が障害となる。

EU法において「正当な利益」を適法性根拠とする際にはバランステストが要求されるように、「正当な利益」の規律を導入するためには、そのような個人データ処理が「正当な」ものと言えるかの何らかの判断基準が必要なのであって、そのような判断基準として参照されるべき「基

<sup>1</sup> 国会会議録第201回国会衆議院内閣委員会第13号（令和2年5月22日）其田真理政府参考人答弁

<sup>2</sup> 第281回個人情報保護委員会（令和6年4月24日）資料1

<sup>3</sup> 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（昭和63年法律第95号）

本原則」(GDPRでは5条)の存在が大前提である。しかし、日本法はそのような前提に不可欠な「基本原則」を欠いていることから、現行法の構造のままでは経済界の要望を実現することはできない。

大前提となる「基本原則」のうち重要なのは、OECD 8原則の第2原則に含まれる「関連性の原則」と「正確性の原則」である。OECDガイドラインはEU法と同様に「データ保護(data protection)」を実現するものであり<sup>4</sup>、データ保護が保護する核心的利益は、個人データ処理による個人に対する評価・決定の適切性確保(後述)の利益である<sup>5</sup>。「正確性の原則」は、個人に対する評価・決定が正確に行われることを要求するものであり、この正確性には、データの内容自体が正確であることだけでなく、評価・決定に用いるロジック(アルゴリズム)が正確な結果をもたらすという意味で適切であることを含む。「関連性の原則」は、個人に対する評価・決定が公平(非差別)なものとなることを要求するものである(後述)。

しかし、日本法は、昭和63年法以来、この意味での「関連性の原則」と「正確性の原則」を全く取り入れてこなかった。関連性の原則は完全に見落とされており、必要性の概念と混同されてきた<sup>6</sup>。正確性の原則については、データに誤りがないという意味での正確性でしかなく<sup>7</sup>、評価・決定に用いるロジックの正確性の観点を欠いてきた。このことは、日本法が、その法目的の理解において、「個人データ処理による個人に対する評価・決定の適切性確保」の理解が希薄であった(後述)ことによる。

OECDガイドラインもEU法もそのことが法目的の核心的利益である<sup>8</sup>ことからすると、日本法に「正当な利益」に基づく第三者提供規制の緩和を導入するためには、まず、このような法目的の理解から立て直すことが不可欠である。

また、第三者提供時の利用目的拘束の仕組みが欠如していることも、経済界の要望を取り入れるには障害となっている。現行法の民間部門の規定では、個人データを第三者に提供すると、提供を受けた第三者は新たに独自の利用目的を自由に設定できる。したがって、提供元における提供の目的が正当であっても、提供先において同じ目的で利用される保証がなく、提供元にも責任がない<sup>9</sup>。このことが、第三者提供時に本人同意を要することとせざるを得ない原因となっており、「契約の履行」「正当な利益」に基づく本人同意なき第三者提供を可能とするためには、この構造を改め、提供先においても同じ利用目的で利用されることが保証される「第三者提供時の利用目的拘束」を何らかの形で規定することが不可欠である<sup>10</sup>。

さらに、有効な利用目的拘束を実現するためには、利用目的を十分に仔細な粒度で特定させる

<sup>4</sup> 高木浩光「個人情報保護から個人データ保護へ(6)——法目的に基づく制度見直しの検討」情報法制研究12号(2022)49頁以下、第3節「データ保護とは何か」(57頁以下)

<sup>5</sup> 前掲注4、第4節「意思決定思考利益モデルと関連性の原則」(1)「Bingの説明」(71頁以下)

<sup>6</sup> 前掲注4、第4節「意思決定思考利益モデルと関連性の原則」(2)「日本法での理解」(75頁以下)

<sup>7</sup> 公的部門の「正確性の確保」(65条)は「過去又は現在の事実と合致するよう」求めているだけ(昭和63年法でも同様)であり、民間部門も、ガイドライン通則編が「入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備……を行うことにより、個人データを正確かつ最新の内容に保つよう」求めているように、データに誤りがないという意味での正確性でしかない。

<sup>8</sup> 高木浩光「個人情報保護から個人データ保護へ(7)——法目的に基づく制度見直しの検討」情報法制研究13号(2023)114頁以下、VIII章「概念の起源」(114頁以下)

<sup>9</sup> 個人情報保護制度の見直しに関するタスクフォース「個人情報保護制度の見直しに向けた中間整理」(令和2年8月)32頁注68

<sup>10</sup> 「個人情報の保護に関する法律に係るEU及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」(補完的ルール)において、第2項で、「個人情報取扱事業者は、法第30条第1項及び第3項の規定に基づき確認し、記録した当該個人データを当初又はその後提供を受ける際に特定された利用目的の範囲内で利用目的を特定し、その範囲内で当該個人データを利用することとする」とされているのは、EU・英国領域から提供を受けた個人データに対してそのような利用目的拘束を課しているものである。

必要がある。特に、「個人データ処理による個人に対する評価・決定」を行うか否か、行う場合には、どのような「評価・決定」を行うのか、事業者が行う評価・決定の処理ごとに、当該評価・決定に対する利用するデータ項目のその決定目的との関連性の有無を判断できる程度に仔細な粒度で利用目的を特定させる必要がある。

現行法には、「評価・決定」の概念が存在しない<sup>11</sup>ため、そのような特定を義務付けることができていない<sup>12</sup>。したがって、まず「評価・決定」の概念を明文で導入し、利用目的を特定する義務をこの概念を用いて規定することが不可欠である。経済界がこれらを忌避する限りは、その要望を実現することはできない。

## 1.2. 統計量への集計

第2に、民間部門において、個人データを統計量に集計する利用に対して、第三者提供の制限が過剰な規制となっている。公的部門では「専ら統計の作成……のために保有個人情報を提供するとき」には目的外の利用・提供が許されることが規定されているが、民間部門にはこれに相当する規定がなく、ガイドラインQ&Aで「統計データへの加工を行うこと自体を利用目的とする必要はありません。」(Q2-5)とされているだけである。OECDガイドラインにはこの点について明確な記載がないが、EU法は、適切なセーフガードの下での統計量への集計は目的外利用とみなさないとする規定(5条1項(b))を置いている。

現行法でも、事業者内部での統計量への集計は、Q2-5により認められているものと解されるし、令和2年改正で導入された仮名加工情報の制度はそれを促進する意義がある<sup>13</sup>し、統計量への集計を外部に委託して処理させることもできる。しかし、問題となるのは、複数の事業者が保有している個人データを突合して統計量に集計する処理である。

突合のために複数の事業者から個人データを一箇所に集めるには、個人データの提供が不可避であり、委託によって個人データを提供する方法で実現しようとしても、委託先において異なる受託案件のデータを突合することは委託を逸脱することになる(Q7-43)ので、違法な第三者提供となって、実施できない。

経済界の要望には、統計利用の促進が含まれており、このような複数の事業者が保有する個人データの突合を可能にする制度改善が求められているものと思われる。

この要望を実現するためには、委託の概念を変更するのではなく、前記の目的内の提供の場合と同じく、「第三者提供時の利用目的拘束」の仕組みが必要である。委託は利用目的拘束の最も単純な形態の一つであるところ、委託に並ぶ他の形態が求められているということになる。その形態には様々な設計が考えられるが、少なくとも、利用目的拘束を実効性あるものとするために、データの転々流通を防止する規律が必要である<sup>14</sup>。

また、経済界の要望には、秘密計算技術などのPETsの利用を認めよとする意見が見られるが、PETsを導入したからといって第三者提供が許されてよいということになるわけではない。秘密計算や連合学習の技術を用いて、元の個人データを他の事業者に秘匿したまま計算を行う場合であっても、その目的が、例えば「見込み客を選び出す」ことにあるのであれば、それは「データ

<sup>11</sup> EU法では「measures or decisions」(措置又は決定)の語がこれに相当する意味で用いられている(DPD13条(2)、GDPR前文162)。

<sup>12</sup> 前回の3年ごと見直しの際には、「制度改正大綱」(令和元年12月)の時点で、「保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの」(32条1項4号)の公表事項に「保有個人データの処理の方法」を加えることが構想され、その中でこれに相当する概念(「プロファイリング」に付随する概念として)が組み込まれる余地があったが、経済界の反対意見があったことにより、令和2年改正では見送られている。

<sup>13</sup> 岩波祐子「個人情報保護とデータの利活用——デジタル化推進に向けた課題——」立法と調査430号(2020)26頁

<sup>14</sup> 高木浩光「医療データ二次利用の基本的考え方——仮名加工医療データの統制された非選別利用に向けた立法論」情報法制レポート4号(2023)36頁以下は、このことを提案している。

に基づく個人に対する評価・決定」にほかならず、決定の目的に対して関連性のないデータを用いたデータマッチングが行われるならば、そのような処理はデータ保護原則に反する。

秘密計算を用いたデータマッチングがデータ保護原則の観点で問題とならない用途は、一つには、統計量に集計する前段階として複数の事業者が保有する個人データを突合する場合である。秘密計算をPETsとして有効に利用するには、そのような用途に限って用いられることを保証する何らかの法的統制が必要である。

これに関連する論点として、「暗号化しても個人データに該当するのか」との議論がある（秘密計算も暗号の一種である）が、ガイドライン通則編2-1が「暗号化等によって秘匿化されているかどうかを問わない」としているように、復号が予定されている場合に限って個人データに該当するといった解釈は採用できない。その理由の一つは、秘密計算を用いて処理する場合であっても、通常、その出力は、暗号化前の元データに復号するものではないが、前記の「見込み客を選び出す」例のように、出力を個人に対する評価・決定に使用するものとなっている場合（この場合、出力は個人データである）には、そのような処理の全体を「個人データ処理」に該当するものとして扱う必要があるからである。

したがって、秘密計算の出力が統計量に集計されたものとなることが保証されている場合に限って、秘密計算への入力も個人データに該当しないものとして解釈することとする解決方法も考えられるが、個人データに該当しないものとした途端に法的統制が及ばなくなることからすれば、むしろ、個人データに該当するものとした上で、そのような第三者提供を可能とする規律に変更する解決方法の方が望ましい。

このことは、結局のところ、前記の「複数の事業者が保有する個人データの突合を可能にする制度改善」が実現されていれば、秘密計算を用いた同じ目的の処理も許されることを意味する。

このように、PETsを導入することで規制を迂回できるのではなく、合法的な処理においてPETsを利用できるということであり、その際のPETsの意義は安全管理措置上の安全性強化にある。日本法における真の課題は、PETsが利用できないことではなく、個人データを統計量に集計する利用に対して第三者提供の制限が過剰な規制となっているところにある。

### 1.3. 要配慮個人情報の取得

第3は、民間部門における要配慮個人情報の取得に対する過剰な規制である。近年問題となっているのは、大規模言語モデルを用いた生成AIに、モデルの学習入力として、Webサイトをクロールしたデータなどの公開情報を用いることが、要配慮個人情報の取得制限に違反し得るとして、個人情報保護委員会が生成AIのサービス運営者に対して注意喚起を行った<sup>15</sup>件である。

この注意喚起は、要配慮個人情報の取得について、「① 収集する情報に要配慮個人情報が含まれないよう必要な取組を行うこと。② 情報の収集後できる限り即時に、収集した情報に含まれ得る要配慮個人情報をできる限り減少させるための措置を講ずること。③ 上記①及び②の措置を講じてもお収集した情報に要配慮個人情報が含まれていることが発覚した場合には、できる限り即時に、かつ、学習用データセットに加工する前に、当該要配慮個人情報を削除する又は特定の個人を識別できないようにするための措置を講ずること。」などの事項を挙げ、遵守するよう求めた。

仮にこのような収集が本人同意のない「要配慮個人情報の取得」として違法であるなら、「できる限り即時に」「できる限り減少」させよとか、「発覚」したら「できる限り即時に」削除せよというのは、法を「遵守」することにはならないのであるから、奇妙な話である。今回の3年ご

<sup>15</sup> 個人情報保護委員会「OpenAIに対する注意喚起の概要」（令和5年6月2日）

と見直して既に高橋意見<sup>16</sup>が指摘しているように、Webサイトをクロールしたデータから「個人情報の完全な排除は技術的に困難」であり、現実的に実施が不可能な措置を求めるわけにはいかないというのは理解できる。

その点、EUでは、EDPBの「ChatGPT Taskforce」の作業報告書<sup>17</sup>が、「これらの要求事項の不遵守を正当化するために技術的不可能性を主張することはできない。」（7段落）と指摘している。これは誠にもっともな指摘であり、考慮すべきなのは、実施可能か不可能かではなく、データ保護原則に適合しているか否かである。

そもそも、平成27年改正で新設された要配慮個人情報の取得制限の規定は、当初からその解釈に疑義があった。我々は、平成27年改正時の個人情報保護法ガイドライン（案）へのパブリックコメント手続に対して、「要配慮個人情報の取得制限は、個人データとして取得する場合に限り適用されるものと理解してよいか」<sup>18</sup>との意見を提出している。これは、ガイドライン通則編が「法第20条第2項に違反している事例」として、「本人の同意を得ることなく、法第20条第2項第7号及び規則第6条で定める者以外がインターネット上で公開している情報から本人の信条や犯罪歴等に関する情報を取得し、既に保有している当該本人に関する情報の一部として自己のデータベース等に登録すること。」を掲げていることについて確認を求めたものである。

もちろん、「違反している事例」がこれ一つしか書かれていないことが、直ちに、それ以外の場合が違反しないものであることを意味するわけではないが、この意見で指摘したいのは、個人情報データベース等に登録することを予定していない個人情報の取得についてまでもが、本当に個人情報取扱事業者の義務に係るのかという疑義（後述）である。この疑問の余地は、要配慮個人情報の規定において特に顕著であり、以下に示すように、立法時の概念の混乱ぶりが施行令9条に表れている。

施行令9条は、法20条2項の要配慮個人情報取得制限の例外規定のバスケットクローズである同項8号から委任された規定であり、その1号に、「本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報取得する場合」が規定されている。ガイドライン通則編3-3-2は、この規定について、「本人の意思にかかわらず、本人の外形上の特徴により、要配慮個人情報に含まれる事項（例：身体障害等）が明らかであるときは、あらかじめ本人の同意を得ることなく、当該要配慮個人情報取得することができる。」と説明しているが、なぜこの例外が加えられたのか。

要配慮個人情報の取得制限の解釈として、もし、身体障害のある人を目視するだけで当該個人が身体障害のある人であるという要配慮個人情報を取得することになると解するならば、本人同意なく身体障害のある人を目視するだけで要配慮個人情報の取得制限に違反することになるから、本人同意なく人を目視してはならないという不可能を強いることになるので、このような例外を設けて手当せざるを得ない。

しかし、目視しただけでは取得に当たらず、それを記録することによって取得に該当することになると解釈されている様子があり<sup>19</sup>、ガイドライン通則編3-3-2は、この例外に該当する事例として、「身体の不自由な方が店舗に来店し、対応した店員がその旨をお客様対応録等に記録した場

<sup>16</sup> 第279回個人情報保護委員会（令和6年4月3日）資料1-2 高橋克巳「AI利用と個人情報の関係の考察」9頁の表1行目

<sup>17</sup> European Data Protection Board 「Report of the work undertaken by the ChatGPT Taskforce」 23 May 2024

<sup>18</sup> 一般財団法人情報法制研究所個人情報保護法タスクフォース「個人情報の保護に関する法律についてのガイドライン（案）」に対する意見」（2016年11月2日）情報法制レポート1号（2021）144頁以下に収載、意見17（149頁）

<sup>19</sup> ガイドライン通則編3-3-1は、「取得」概念について、「個人情報を含む情報がインターネット等により公にされている場合であって、単にこれを閲覧するにすぎず、転記等を行わない場合は、個人情報を取得しているとは解されない。」と注記している。

合（目視による取得）」と記載している。そうであれば、本人同意なく記録しないことを求めるのは現実的に可能なことから、なぜこれを例外として手当てする必要があったのか疑問である。

むしろ、来店者が身体障害のある人である事実を記録する行為は、その記録を元に来店者に対する差別的取扱いがなされる危険性があるからこそ、この法に基づく規制が必要なのであって、この例外を設けたことは本末転倒である。我々は平成27年改正時の施行令（案）へのパブリックコメントで、「目視による取得は要配慮個人情報の取得制限から除外するべきではない」とする意見<sup>20</sup>を提出し、続く同ガイドライン（案）のパブリックコメントで、「店員が目視により認識した「身体障害者である」との事実を、差別的に対応するために記録し、その後の対応を差別的なものとする行為は、この法により制限されないということか。そうだとすれば、何のための要配慮個人情報の規定なのか。」と疑問視する意見<sup>21</sup>を提出している。

また、施行令9条1号の「撮影することにより」についても同様である。ガイドライン通則編3-3-2は、その事例として、「身体の不自由な方が店舗に設置された防犯カメラに映りこんだ場合（撮影による取得）」と記載しており、これが例外として規定された理由は、施行令改正の立案時の個人情報保護委員会の資料<sup>22</sup>によれば、「映像等に写りこんだ場合等の事業者の負担を勘案するもの」とされていた<sup>23</sup>。これに対し、我々は、パブリックコメントで、「「外形上明らかな要配慮個人情報」の取得を取得制限から除外するのは散在個人情報としての取得に限るべき」と指摘する意見<sup>24</sup>を提出している。

この意見の趣旨は、顔や歩容などから個人を識別することなく単に録画するだけであれば、個人データの取得には当たらず、散在情報としての要配慮個人情報の取得にすぎないところ、「映像等に写りこんだ場合等の事業者の負担を勘案する」必要があるのは、そのような識別を行わない

---

<sup>20</sup> 一般財団法人情報法制研究所個人情報保護法タスクフォース「「個人情報の保護に関する法律施行令の一部を改正する政令（案）」及び「個人情報の保護に関する法律施行規則（案）」に対する意見書についてのガイドライン（案）」に対する意見」（2016年8月31日）情報法制レポート1号（2021）134頁以下に収載、意見11「目視による取得は要配慮個人情報の取得制限から除外するべきではない」（137頁）は、①目視ただけで取得になるのか？ そうでないとするれば、③目視した人がメモに書いたり電子計算機に入力する場合まで除外する必要性は何なのか？を問い、⑤「目視による取得では、人が手作業をしない限り取得に至らないのであるから、「事業者の負担を勘案」する必要性はなく、これを除外するのは失当ではないか。」との指摘をしている。

<sup>21</sup> 前掲注18、意見16「目視により外形上明らかな要配慮個人情報を取得し差別的に取り扱う行為が制限されないことは、法の要配慮個人情報の趣旨に適うものなのか」（148頁）は、「目視による取得の例として、本件ガイドライン案は、「事例）」として、「身体の不自由な方が店舗に来店し、対応した店員がその旨をお客様対応録等に記録した場合」を記載しているが、同様に、店員が目視により認識した「身体障害者である」との事実を、差別的に対応するために記録し、その後の対応を差別的なものとする行為は、この法により制限されないということか。そうだとすれば、何のための要配慮個人情報の規定なのか。」との指摘をしている。

<sup>22</sup> 第10回 個人情報保護委員会 資料1「要配慮個人情報に関する政令の方向性について」（平成28年6月3日）

<sup>23</sup> 前掲注22、2頁「要配慮個人情報の取得時の本人同意の例外」に、「ある特定の個人が身体に障害を抱えている事実が映像等に写りこんだ場合等の事業者の負担を勘案するもの。外形から明らかであるため、本人にとっても社会生活を送るに当たって自己の要配慮個人情報に含まれる事項が公に認識されることは想定していると考えられる。もっとも、取得した要配慮個人情報を本人の知らないうちに第三者に提供されることがないように、第三者に提供するに当たっては、本人の同意を要することとしている。」と記載されている。

<sup>24</sup> 前掲注20、意見12「「外形上明らかな要配慮個人情報」の取得を取得制限から除外するのは散在個人情報としての取得に限るべき」（137頁）は、「本来、個人情報保護法の目的は、世界各国のデータ保護法制と共通するように、個人情報がコンピュータ処理されることによりもたらされ得る個人の権利利益侵害の未然防止にあるはずである。要配慮個人情報について規制を強める趣旨が、「本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要する」（法2条3項）からであるなら、要配慮個人情報がデータベース化されて「要配慮個人データ」となり、自動処理されることによって生じ得る本人の不利益こそが、未然防止すべき、法の主たる目的であるはずではないか。それにもかかわらず、本号は、散在要配慮個人情報の取得のみならず、要配慮個人データとして取得すること（個人データとして要配慮個人情報を取得すること）まで、例外としており、取得を制限しないことになってしまっている。本号を法17条2項の例外に加えた趣旨が、「映像等に写りこんだ場合等の事業者の負担を勘案するもの」であるならば、例外とするのは、散在個人情報としての取得に限るべきである。」との指摘をしている。

場合に限られるはずであって、事業者の目的が、映像から自動的に個人を識別し、身体障害のある人として処理することにあるのであれば、そのような場合にこそ要配慮個人情報の規律に服するものとするべきであり、これを例外として除いたのは本末転倒である旨を指摘したものである。

そもそも、当時の個人情報保護委員会が、この例外を設けることの正当性を、「外形から明らかであるため、本人にとっても社会生活を送るに当たって自己の要配慮個人情報に含まれる事項が公に認識されることは想定していると考えられる。」（前掲注23）としていたことからして適当でない。

個人情報保護法は、公開情報であっても個人情報に該当するものとして規律の対象としており、その趣旨は、データ保護が保護する核心的利益が、個人データ処理による個人に対する評価・決定の適切性確保（後述）の利益にあることからすれば、公開情報から作成した個人データであっても、評価・決定に使用されれば、その適切性に重大な影響を及ぼし得るからである。

当時の個人情報保護委員会が、「外形から明らかであるため、本人にとっても……」との理由で除外して差し支えないと考えたのは、この法の目的を、他人に知られたくない秘密の保護（古典的な意味でのプライバシーの保護）にあると想定したものであろう。しかし、そのような秘密の保護も確かにデータ保護が保護する利益の一つではあるが、それは一部にすぎないのであって、むしろ、核心的利益の保護のためには、公開情報に対してこそデータ化に対する規制が必要である。

以上の考えから、要配慮個人情報の取得制限は「個人データとして取得する場合」に適用されるものと解するべきであるというのが、前掲注18の意見であった。

この考え方を、本節冒頭で述べた、今日問題となっている、大規模言語モデル（LLM）の学習入力にWebサイトをクロールしたデータなどの公開情報を用いる事案を当てはめると、そのような学習入力は「個人データとして取得する場合」に当たらないと解することができ、要配慮個人情報の取得制限に抵触しないと言うべきである。

このことは、前掲注16の高橋意見でも、「一般的なニューラルネットワーク（含む、LLM）の場合」「個人情報を扱うとはみなせないのではないか」（9頁の表4行目）と指摘されている<sup>25</sup>点が、同旨のものと思われる。

LLMには、入力された文章がそのまま記録されるわけではなく、入力された文章は、単語や文章の意味が高次元のベクトル空間に分解されて埋め込まれ、ベクトル空間全体に拡散して記憶される。そうして作成された学習済みモデルに対して、利用の段階で、プロンプトを与えて生成される文章が、誰かの個人情報として生成されることは起き得るけれども、それは利用者が生成させた文章であって、どんな文章でも生成させる余地があることからすれば、利用者の責任と言える。

このことは、著作権法の観点で生成AIへの学習入力が問題とされないことと類似している。著作権法30条の4（著作物に表現された思想又は感情の享受を目的としない利用）は、「情報解析の用に供する場合」などを例示しながら、「当該著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない場合」には（非享受目的）、「その必要と認められる限度において、いずれの方法によるかを問わず、利用することができる」とする。生成AIを利用することによって、何らかの著作物の著作権を侵害する生成物（類似性と依拠性によって判断される）が生成される可能性があるが、それは、そのような生成を指示した利用者が行ったこと<sup>26</sup>なのであって、学習の入力にそのような著作物が含まれていたからではない。この著作権法における「非

<sup>25</sup> いわゆる「クラウド例外」（Q7-53）に示されている、「当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合」の概念が、ここでいう「個人情報を扱う」と同様のものといえる。

<sup>26</sup> 文化審議会著作権分科会法制度小委員会「AIと著作権に関する考え方について」（令和6年3月15日）

享受目的」の考え方は、個人情報保護法における「個人データとして処理しない」と類似しており、学習入力に著作物を使用することが直ちに著作権侵害にならないのと同様に、学習入力に個人情報を使用することが直ちに個人の権利利益を害することになるわけではない。

個人情報保護法20条2項7号は、「当該要配慮個人情報、本人、……により公開されている場合」を、要配慮個人情報取得の本人同意原則の例外に規定しているが、Webサイトには、本人以外の者によって要配慮個人情報に相当する記述が記載されていることも多々あるので、この例外は、前記の「事業者の負担を勘案」したものとしては効果がない。このような記述がLLMの学習入力に使われることについて、本人によって公開されているものか、他人によって公開されているものかは、その結果に違いを生じさせないのであるから、この違いを区別する意味はない<sup>27</sup>。

むしろ、大規模言語モデルに対してデータ保護の観点で問題とすべきは、それをを用いて個人データを出力させる場合である。例えば、「データ保護分野で有能な弁護士トップ10を出力して」というプロンプトに対して、実在の弁護士がリストアップされたとしたら、その正確性が問われることになるし、どんなデータを基に判断したのかその関連性が問われる。より問題の大きい例は、「懲戒処分を受けた弁護士を悪い順に10人リストアップして」といったプロンプトに対する出力であろう。個人情報保護委員会は、このような出力を抑止しない生成AIを問題視するべきである。

こうした論点は、Webの検索サイト（検索エンジン）に対する個人情報保護法上の規制のあり方とも共通している。Webサイトをクロールして公開情報を入力とする点は、LLMも検索エンジンも同じである。検索エンジンのクローラーも要配慮個人情報を構成する文字列を収集しているが、個人情報保護委員会は、これまで検索エンジンを問題視したことがなかった。それなのに、なぜ、LLMに対しては問題視することができるのか。そこに理論的整合性があるようには見えない。

また、このことは、EU法における、欧州司法裁判所のいわゆる「忘れられる権利」を認めた2014年決定<sup>28</sup>が、検索エンジンの出力を問題視して入力を問題視しなかったことも共通する。

日本法は、検索エンジンの出力について「忘れられる権利」を認めておらず、検索エンジンは個人情報データベース等に該当しないとの解釈<sup>29</sup>がとられている。もし、日本法において、検索エンジンにおいて氏名の入力によって検索される結果について、EU法と同様の規律を必要とするのであれば、そのような処理の要求に応じて臨時の仮想的な個人情報ファイル（個人情報データベース等）概念が観念されるものとする解釈<sup>30</sup>で対処するか、さもなくば、EU法と同様に「processing of personal data」の概念<sup>31</sup>を導入する必要がある。LLMの出力に対して前記の規律を求める場合

<sup>27</sup> 前田健「生成AIの利用が著作権侵害となる場合」法学教室523号（2024）27頁以下は、著作権法30条の4ただし書「著作権者の利益を不当に害することとなる場合」に該当するのがいかなる場合かの論点において、「学習用データが海賊版などの違法コンテンツである場合」が該当するとする説があることに対して、「筆者に言わせれば、いずれも著作権者の利益を不当に害する場合には当たらない」と述べている。結果への影響に違いがないという点で、個人情報保護法20条2項7号の規定の無意味さと共通するところがある。

<sup>28</sup> Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12

<sup>29</sup> 園部逸夫・藤原静雄編・個人情報保護委員会著『個人情報保護法の解説《第三次改訂版》』（ぎょうせい、2022）86頁「インターネット上の検索エンジンについて」参照。

<sup>30</sup> 高木浩光「個人情報保護から個人データ保護へ——民間部門と公的部門の規定統合に向けた検討(3)」情報法制研究4号（2018）74頁以下、注32（81頁）参照。

<sup>31</sup> 高木浩光「個人情報保護から個人データ保護へ（8）——法目的に基づく制度見直しの検討」情報法制研究14号（2023）130頁以下、148頁以下の「(5)「processing」の解釈」で示したように、「processing of personal data」の「processing」は、単なる「取扱い」の意味ではなく、「データ対象者についてデータ処理する」という前提が含意されていることに注意されたい。

にも、同様の対処が必要となる。

なお、要配慮個人情報について、他の一般個人情報と区別して特別に規制することの必要性が何に依拠するのか、そもそも、OECDガイドラインはそれを求めていること（後述）に留意すべきである。

#### 1.4. 個人データへの統一

第4は、個人情報データベース等を構成することを予定していない個人情報（散在情報）に対する過剰な規制である。要配慮個人情報の取得制限については、前節で述べたとおり、法目的の観点から、個人データとして取得する場合に限り適用されるものとし、適用から除く例外を削減すべき（法20条2項7号、施行令9条1号を廃止）であるが、要配慮個人情報に限らず、一般個人情報についても、21条の利用目的の通知、20条1項の適正取得、19条の不適正利用禁止、18条の目的外利用禁止、17条の利用目的特定の各義務が、個人情報データベース等を構成することを予定していない個人情報に対してまで課されることは過剰規制である。

例えば<sup>32</sup>、ある会社が、重役会議の議題として、「ライバル会社のX社長が末期ガンが見つかり死期が近づいているらしい」との情報を得て、自社の経営方針を検討するときはどうか。「X社長は末期ガンである」という情報は個人情報であり、重役会議でこれを用いることは当該事業者による個人情報の取扱いということになる。この情報は、自社の個人情報データベース等から抽出したのではなく、ライバル会社に送り込んでいる協力者から聞いたもので、個人データに当たらない散在情報の個人情報である。このとき、その情報の利用目的を特定し、X氏に通知するか公表しなければ、17条、21条に違反ということになるのか。協力者が身分を隠して聞き出しているから20条1項にも違反するのか。

これに類する状況は、ビジネスマンの業務において大なり小なり日常的に存在するだろう。実際には誰もそのような場合に個人情報の利用目的を特定してなどいない。そんな理不尽な法的義務があるはずもないという直感から、個人情報とは氏名・生年月日・性別・住所のことだろう、それらを伏せてさえおけば問題ないのだろうといった誤った法理解を生み出してきた。そのことが、真に必要な個人データの利用目的の特定義務をおろそかにさせてきた。

そもそも、個人情報保護法の民間部門の規定は、個人情報データベース等を対象としたものであって、このような人の噂話を規制するものではない。そのことは、平成15年法の立案担当者らによる逐条解説書には説明がある<sup>33</sup>ものの、ガイドライン通則編には記載がなく、初期の担当者が前提としていたはずの理解が、その事情を知らない外部の有識者によって執筆された解説書が氾濫した結果、担当者も交代を繰り返すうちに、そうした解説書の影響を受けて、本来の理解が次第に忘れられてきているように見受けられる。このことは前回の3年ごと見直しでも指摘した<sup>34</sup>が、改善されていないように見受けられる。

今回の3年ごと見直しでも、個人情報保護委員会事務局が用意した検討資料には、このことが忘

<sup>32</sup> 高木浩光「IoTに対応した個人データ保護制度のあり方」法とコンピュータ34号（2016）47頁以下、68頁より。

<sup>33</sup> 前掲注29、58頁に、「他方、例えば、他人のうわさ話をする行為、上司に同僚の告げ口をする行為等も、外形的には他人の個人情報を第三者に提供する行為といえ、中にはこれにより精神的苦痛を被り、名誉を毀損される等個人の権利利益が侵害される場合もあり得る。しかし、これらの行為は、従来から個人のモラルに委ねられてきたところであり、その予防は社会全体の利益擁護の観点からの規範である法律で規制すべき問題ではない。本法は、あくまで、高度情報通信社会が進展している現状において、個人情報のコンピュータ処理等に伴う個人の権利利益侵害の危険性、本人の不安等の社会問題に対応しようとするものである。個人情報の取扱いに伴って、現実にはだれかの人権侵害等が発生した場合においては、民事事件における損害賠償の問題として、あるいは犯罪行為（名誉毀損等）を構成する場合は刑事事件の問題として、処理されるべきことはいうまでもない。」との記載がある。

<sup>34</sup> 第105回個人情報保護委員会 資料6「高木浩光氏御提出資料」（令和元年5月17日）15～17頁

れられていると思われる記載が多数ある。例えば、3月6日の資料<sup>35</sup>には、「事務局調べ」として様々な裁判例が掲載されているが、その多くが、個人データでない個人情報の事例になっている<sup>36</sup>。典型例を一つ挙げれば、「不適正取得・不適正利用に係る規律の在り方⑤」（22頁）に記載されている「個人情報の取扱いの適正性に関連する主な裁判例②」の表に示された東京地判令和2年1月20日の事例<sup>37</sup>は、個人データの話ではない<sup>38</sup>。

前掲注33に引用したように、このような事例は個人情報保護法の立法趣旨の外にあるものである。あらゆる取引には必然的に相手方の氏名を伴うが、そのことをもって個人情報保護法に絡め、あらゆる不法行為を個人情報保護法上の「不適正利用」に当てはめて規律しようとするのは、法の趣旨の逸脱である。個人情報保護法を気に入らない者を懲らしめる道具と化してはならない。個人情報保護法上の不適正利用の「不適正」は、データ処理それ自体の不適正性に着目して判断されるべきものであって、そのような不適正性の判断基準は、前記1.1節で述べたデータ保護の基本原則に反するか否かの観点を基準とするべき<sup>39</sup>である。

「個人関連情報」についての検討でも同様である。今回の検討では、「個人関連情報の適正な取扱いに係る規律の在り方」として、「現行法において、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。」として、その新設を検討するような記載ぶりになっているところ、そこに提示されている「個人関連情報の取扱いに起因する個人の権利利益の侵害に関連する主な裁判例」（27頁）2つ（東京高判令和4年9月15日、東京高判令和4年12月21日）は、いずれも個人データ<sup>40</sup>の話ではない。

前者は自治体の情報公開条例に基づく体罰事故報告書の不開示決定の事案、後者はSNSへの電話番号の投稿がプライバシー権の侵害とされた事案であり、事務局資料は、これらで問題とされた情報が、氏名を伴わない個人に関する情報といえることから、法の「個人関連情報」に該当すると考えたようであるが、これは令和2年改正の立法趣旨を逸脱するものである。

令和2年改正で新設された「個人関連情報」の規律は、用語の定義（2条7項）だけ見ればそのような情報が該当するかのようなようであるが、この用語は初出の31条1項で「個人関連情報（個人関連情報データベース等を構成するものに限る。以下この章及び第六章において同じ。）」と限定されており、個人関連情報の制度の全体が個人関連情報データベース等を構成するものに限る趣旨となっている。これは令和2年改正時の立案担当者にとっては当然の前提とされていたはずであるが、今回の3年ごと見直しの担当者はその前提を忘れているように見受けられる。

このような用語の規定ぶりは、平成27年改正で新設された匿名加工情報の規律の規定ぶり（43

<sup>35</sup> 第275回個人情報保護委員会 資料1「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）

<sup>36</sup> それに対して、「（出典）株式会社日本総合研究所「個人情報保護に係る主要課題に関する海外・国内動向調査 最終報告書」（2023年12月）等をもとに作成」とされた図表では、すべてが個人データに関する事例となっている。

<sup>37</sup> 「高額な取引をするのに必要な判断能力が相当程度低下した高齢男性（=X）に対して、Xの判断能力が相当程度低下している事実を認識し、又は容易に認識し得たにもかかわらず、また、Xにとって、その生活に通常必要とされる分量を著しく超えた過大な取引であることを認識していたにもかかわらず、宝飾品、時計、眼鏡、衣類等を販売し続けた」事実について、不法行為法上違法と評価されるべきものとして損害賠償を認めた事例。

<sup>38</sup> この事例の類例として、例えば、各顧客について「高額な取引をするのに必要な判断能力が相当程度低下」しているか否かを、顧客の取引履歴や外部から入手した個人データを用いた統計分析によって推定し、それに基づき該当する顧客について他の顧客とは異なる形で「販売し続けた」という事例であれば、「個人データ」の問題となり得る。

<sup>39</sup> その点、同表に記載の東京高判令和5年5月30日の事例は、大学入試において受験者の性別で加点調整を行なったものであり、入試の合格者を決定するという目的に対して「関連性」のない性別というデータ項目を用いたという点で、データ保護の基本原則に反するデータ処理を伴ったものといえ、こちらは「個人データ」の事例である。

<sup>40</sup> 正確には、ここでは個人情報ではない個人に関する情報の話をしているのだから、その点で「個人データ」でないことは当然であるが、ここでは、個人関連情報データベース等（31条1項）を構成する個人関連情報の話ではないという意味である。

条)を踏襲したもので、令和2年改正の仮名加工情報の規定ぶり(41条)も同じである。このように、匿名加工情報、仮名加工情報、個人関連情報のいずれも、その義務規定の全域において、それぞれ、匿名加工情報データベース等を構成する匿名加工情報、仮名加工情報データベース等を構成する仮名加工情報、個人関連情報データベース等を構成する個人関連情報に限定されている。一般化して記述すれば、「X情報(X情報データベース等を構成するものに限る。)」との規定ぶりである。

すなわち、「X情報」という言葉が使われているが、実際にはX情報ではなく、「Xデータ」とでも呼ぶべき概念が用いられているのである。そうであれば、2条の用語定義において「X情報」を定義せず、「Xデータ」を直接定義すれば誤解を招かなかったとも考えられるところ、実際、平成27年改正時には、当初案では「匿名加工データ」の語が用いられていた。それが法制局予備審査の過程で、紆余曲折があり、現在の規定ぶりに直された経緯<sup>41</sup>がある。

このような用語の煩雑な定義が招く誤解の問題は、経済界からも不評のようで、用語を統一せよとの意見が出ている。「X情報」でも「Xデータ」でも、条文どおりに解釈すれば、規定された内容に違いがないことがわかるが、誤解されにくい規定ぶりへの改善(「Xデータ」への統一)の余地はあるだろう。実際、前記のように、事務局資料の作成者も誤解したわけであるから、瑣末な話ではない。

このように理解すると、「個人情報」及び「個人データ」についても共通する構造があることがわかる。個人データとは「個人情報データベース等を構成する個人情報」のこと(16条3項)である。しかし、匿名加工……、仮名加工……、個人関連……とは異なって、個人……については、義務規定の全域において「X情報データベース等を構成するものに限る」とされているわけではなく、17条乃至21条(とその他一部)に限って「個人情報」が対象とされている。

この違いについて、外部の有識者によって執筆された解説書では、積極的な区別を意図して規定されたものと解説するもの<sup>42</sup>があるが、立案担当者らによる逐条解説書(前掲注29)では、そのようには説明されておらず、単に、取得段階ではまだ個人データの状態にないから個人情報としか言いようがないという法技術的な都合にすぎない理由によるものと説明<sup>43</sup>されている<sup>44</sup>。そうであれば、この際、経済界の要望を受け入れて、義務の対象を「個人データ」に統一してはどうか。

4月24日の業界団体へのヒアリングの際に、浅井祐二委員から<sup>45</sup>、「個人情報保護法は、安全管理措置や第三者提供など規律の対象がデータベースを構成する個人情報、つまり「個人データ」に限定されており、事業者への負担を考慮して整備された経緯があると理解している。「複数の定義が乱立」との御指摘に従い、統合や整理をする方向性は、かえって規律の範囲を広げることに

<sup>41</sup> 行政文書ファイル管理簿に「法律案審議録 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案(平成27法律65)」の文書名で登録されている内閣法制局保有の文書の写し(内閣法制局への情報公開請求により取得)より。

<sup>42</sup> 宇賀克也『新・個人情報保護法の逐条解説』(有斐閣、2021)は、22条(正確性の確保)の解説において、「個人情報ではなく、個人データに範囲が限定されているのは、容易に検索しえない散在情報としての個人情報にまで正確性の確保を要求することは、個人情報取扱事業者に過度の負担を課すことになるからである。」(229頁)と説明し、23条(安全管理措置)についても、「個人情報全般ではなく、「個人データ」を対象を限定しているのは、個人データの安全管理が不十分な場合、個人データが漏えいし、他の個人データと容易に結合されること等により、個人の権利利益を侵害するおそれが大きいこと、個人情報全般に一律に具体的な安全確保義務を課した場合、個人情報取扱事業者に過大な負担を負わせるおそれがあることによる。」と説明している。

<sup>43</sup> 具体的には「なお、取り扱う対象を「個人情報」とし「個人データ」としていないのは、いずれ個人情報データベースに記録され「個人データ」となるものであっても、取得段階では「個人情報」の状態であることによる。」(149頁)と記載されている。

<sup>44</sup> このことは前回の3年ごと見直しの際にも指摘している(前掲注34)。詳しくは、前掲注32の71頁以下も参照。

<sup>45</sup> 第281回個人情報保護委員会(令和6年4月24日)議事概要

つながるのではないか。」との発言があったようであるが、個人情報保護法が規制の対象を個人データに限るのは、「事業者への負担を考慮して」というよりも、1.1節で述べたように、データ保護が保護する核心的利益が、個人データ処理による個人に対する評価・決定の適切性確保（後述）の利益にあるからで、個人データを構成しない個人情報（散在情報）については、そのような保護すべき利益を欠くからである<sup>46</sup>。

しかし、義務の対象を「個人データ」に限定すると問題となるのは、個人情報データベース等を構成することを予定しているが未だ構成していない段階の個人情報が義務の対象から外れてしまうことである。EU法では、「This Regulation applies to the processing of … personal data which form part of a filing system or are intended to form part of a filing system」（GDPR 2条1項）の「or are intended to」のように、個人情報データベース等を構成することを予定しているものを明文で含めている。

日本法では、従前、個人データを対象としている安全管理措置義務等において、そのような「個人情報データベース等を構成することを予定しているものの未だ個人データでない状態の個人情報」が義務の対象とならないとする運用を続けてきており、課題の一つであったが、今年のガイドライン通則編の改正により、「個人情報（個人データとして取り扱われることが予定されているものに限る。）」まで義務の対象が一部の規定で拡大された。

これは、元々そのような趣旨で平成15年法が立案されたものの、拙速な立法で十分に規定しきれていなかった不備を、解消しようとしているものと考えべきであり、このような規定ぶりが可能なのであれば、「個人データ」の定義に「（個人データとして取り扱われることが予定されているものを含む。）」を加えて、義務規定の全域において対象を「個人データ」に統一すればよい。

## 1.5. 小括

以上のとおり、経済界の要望を実現する観点から、目的内提供の制限が過剰であること、統計量への集計に際して第三者提供の制限が過剰であること、要配慮個人情報の取得制限が過剰であることを指摘し、過剰な規制を緩和するためには不可欠となる「不足する規制」の導入方法について提示し、用語の煩雑さの解消方法についても提示した。これらは互いに依存し合っており、どれか一つだけ実現するのでは不整合が生じるので、全体を一度に直す必要がある。

この意見は、前回の3年ごと見直しの際に主張していたことの延長であるが、当時は「ハードルが高い」として実現が容易でないと考えていたのが、令和2年改正と令和3年改正を経て、現在では十分に可能と考えるようになったものである。ただし、これらを一度に直すには大掛かりな改正が必要で、法制執務上の検討を十分に重ねる必要があると思われる。6月現在の検討状況を見るに、今からこれを検討しても、来年の通常国会への提出に間に合う立案は難しいようにも思えることから、この際、法案提出を再来年とし、1年かけて十分な議論をしてはどうか。

以上が主要な意見であるが、以下の3章に、個人情報保護委員会事務局が提示している検討資料の個別の論点についての残りの意見と、他の有識者意見に対する見解を記載したので、そちらも参照されたい。

## 2. 総論

前記の主要意見で、根拠を「後述」と記載した、意見の理論的背景について、個人情報保護法の法目的、特別カテゴリーの意義について、以下、簡単に述べる<sup>47</sup>。

<sup>46</sup> 「事業者への負担を考慮して」という面もあるかもしれないが、あるとすれば、それは「安全管理措置や第三者提供など」に限らず、利用目的の特定、目的外利用の禁止も含めた、義務規定の全域において考慮すべきことである。

<sup>47</sup> 意見資料の提出期限が短かったため、本章以下は未完成な簡単な説明にとどまっていることをお許し願いたい。詳細は、情報法制研究16号（2024年11月出版予定）で論ずる予定である。

## 2.1. 個人情報保護法の法目的

データ保護が保護する核心的利益は、個人データ処理による個人に対する評価・決定の適切性確保の利益である<sup>48</sup>。

ここでいう「データ処理」は、「データに対して行われる操作の体系的実施」のこと<sup>49</sup>であり、「個人に対する評価・決定」とは、各個人に対して当該個人の個人データを基に何らかの評価をしてその評価に基づく何らかの決定をすることをいう。そして、決定の「適切性確保」とは、個人に対する決定が、その決定の目的に照らして、正確であり（広義の正確性）公平（fairness）なものとなることを要求するものであり、そのために、評価の入力として用いる個人データの構成及び内容が適切であること（データの適切性）と、評価・決定の計算式及び判断基準（決定のロジック）が適切であること（ロジックの適切性）が要求される。データの適切性を確保するためには、データを構成するデータ項目の全てが、決定の目的に対して「関連するもの（relevant）」でなければならない（関連性の原則）、また、各データ項目の内容が、ロジックの適切性確保に必要な範囲で、正確で（狭義の正確性）、完全（complete）で、最新のものでなければならない。

データ保護がこのような「関連性の原則」を必要とする趣旨は、形式的平等が、人を区分する目的と区分に用いる特徴とが「一致」している（特徴が目的に関連性がある）ことを要求すること<sup>50</sup>とパラレルであり、非差別原則の実現にある。個人データ処理は、それが決定利用である場合には、データ対象者らを何らかのアルゴリズムで選別することになるものであり、形式的平等の本質が区別に用いる特徴の区別の目的との関連性にあるとされる<sup>51</sup>のと同様に、個人データ処理による決定の適切性の核心が、決定に用いられるデータ項目の決定の目的との関連性にあるのである。

ここで、「関連性がある（relevant）」という言葉の意味するところが、目的に対して「役に立つ」（fitting、applicable）の意ではないということに注意が必要である。決定の目的に対して用いるデータ項目が、統計的に相関性を有する場合には、目的に対して「役に立つ」データ項目ということになるが、関連性のないデータ項目を用いることは非差別原則に反することになる。

また、「必要性」とも別の概念であることにも注意が必要である。データに基づく個人に対する評価・決定を行おうとしている者にとって、決定の目的に対して統計的に相関性を有するデータ項目は「必要性」のあるものとなるかもしれないが、必要であっても「関連性」のないデータ項目を用いることは原則に反することになる。

## 2.2. 特別カテゴリーの意義

EU法が、特別カテゴリー（special categories）の個人データに上乘せの規制を設けているその理由は、GDPRにおいても必ずしも明確には説明されていない。OECDガイドラインでは、解説中に「sensitive data」への言及はあるが、8原則中でsensitive dataを特別に扱う規定はない。日本

<sup>48</sup> 総務庁行政管理局監修『新訂版 逐条解説 個人情報保護法』（第一法規、1991）は、昭和63年法について、「個人の権利利益を保護すること」の中身について、「電子計算機処理に係る個人情報の取扱いによって侵害されるおそれのある、あるいは個人情報の取扱いに伴って保護する必要のある個人の権利利益一般である。」とし、「①個人の秘密が公開されないこと。②誤った又は不完全な情報によって自己に関し誤った判断がなされないこと。③自己の情報を知ること。」（41頁）の3点を挙げていた。②の点が、この「個人データ処理による個人に対する評価・決定の適切性確保」に当たるものではあるが、「誤った判断がなされない」は「評価・決定の適切性確保」よりは狭い。

<sup>49</sup> ISO 2382-1:1974「Data processing — Vocabulary — Section 01 : Fundamental terms

<sup>50</sup> 松井茂記『日本国憲法 第3版』（有斐閣、2007）368頁

<sup>51</sup> Joseph Tussman and Jacobus tenBroek「The Equal Protection of the Laws」California Law Review 37巻3号（1949）341頁以下は、「良心的な立法者にとって、平等保護条項は、法律を制定する際、立法者が作成する区分が法律の目的に合理的に関連している（reasonably related）ことを要求するものである。その理想から様々な程度で過小包摂又は過大包摂で逸脱する場合は、そのような逸脱を正当化する要因を十分に考慮した上で行うことになる。」（365頁）と述べている。

法が、平成27年改正まで、要配慮個人情報の規定を設けなかったのは、OECDガイドラインの考え方に沿ったものだったと考えられる。

日本法がかつて要配慮個人情報相当の概念を設けなかった理由について、何をそれに含め、何を含まないかは、決めようがないから決めなかったと説明されることが多い。その理由として、何を他人に知られたくないかは人によって異なるから一律に決められないといった理由が添えられることもある<sup>52</sup>。しかし、OECDガイドラインがsensitiveカテゴリを設けなかった理由は、そのような意味での「できないから」ではないことが、OECDガイドライン立案時の専門家部会の議事概要を記したOECD部内文書から窺うことができる。

OECDの議事概要を見ると、フランス代表が、sensitiveカテゴリを入れるべきと繰り返し主張する一方、ドイツ代表ほか、どんな情報も評価・決定に用いることができるところに差別の危険が生じるのであるから、すべての種類のデータを対象にするべきで、区別してはいけないとする旨の指摘をしていた。こうした議論を経て、米国代表が「保護の必要性を生じさせるのは情報の性質ではなく、その目的と使用である」<sup>53</sup>と述べたことで話がまとまった様子がある。

このような、「情報の性質ではなく目的と使用である」とする指摘は、ドイツ法の文脈で頻繁に語られている。OECDの議事概要に明確な記載は見つかっていないが、このことは、第2原則前段の関連性要件に反する「目的と使用」がなされる場合に「保護の必要性」が生じるということ述べたものと考えられる。

EUのデータ保護指令も、1990年に欧州委員会が提案した初期案には、特別カテゴリは規定されていなかった。その後の修正で特別カテゴリが規定されることになったが、その理由は必ずしも明確でない。

### 3. 各論

#### 3.1. 「必要最小限」について

令和6年2月21日付の検討項目に、「目的との関係で必要最小限にとどめるべきではないか」との記載があるが、EU法のデータ最小化原則（data minimisation）は、「Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');」（GDPR 5条1項(c)）とあるように、adequate（十分性）、relevant（関連性）も要求しており、必ずしも「最小化」ではないことに留意する必要がある<sup>54</sup>。日本では長年、政府も学説もこの点を見落とししてきた経緯があり、法目的を見失って迷走する原因となっている。

#### 3.2. 「処理」と「取扱い」について

令和6年2月21日付の検討項目に、「処理」（GDPR）と「取扱い」（個人情報保護法）など、GDPRと個人情報保護法との間の定義を可能な範囲で調和させるべき」との記載があるが、そのような統一を図るのであれば、前記1.4節で述べたように、規律の対象を「個人データ」に統一した

---

<sup>52</sup> OECDガイドラインの解説メモランダムには、「専門家グループは、差別の危険性というような各種のセンシティブな基準について議論してきたが、センシティブと万人に認められるようなデータを定義付けることは、不可能であることがわかった。それ故、第7条は単に個人データの収集には限度があるという一般的表現に留めた。」（51段落）との記載があることから、そのような理解が広まったものと思われる。

<sup>53</sup> OECD「Expert Group on Transborder Data Barriers and the Protection of Privacy, Second Meeting, Summary Statement by the Chairman, 6th December, 1978」DSTI/ICCP/78.45（1978）

<sup>54</sup> 前掲注8、「3 関連性と十分性と完全性」（129頁以下）、表1「データ品質に係る原則の概念整理と日本法の対応状況」（130頁）参照。

上で、「取扱い」の語を廃止して「処理」の語を用いることが望ましい<sup>55</sup>。

### 3.3. 生体データの取扱い規律について

令和6年3月6日付の検討資料に、「生体データの取扱いに係る規律の在り方」として、生体データをセンシティブデータに加えることが検討されているようだが、なぜそうする必要があるので整理する必要がある。ただ単に「海外もそうしているから」という理由で進めてはならない。

EUのAI規制でいう「remote biometric identification」（遠隔生体計測学的個人識別）は、情報自体がセンシティブだからということではなく、公共空間において勝手に個人が識別され、あるいはトラッキングされてしまうことの脅威を問題にしたものであることに留意が必要である。

### 3.4. こどもの個人情報について

令和6年4月10日付の検討資料に、「こどもの個人情報等に係る規律の在り方」が記載されているが、なぜそうする必要があるので整理する必要がある。ただ単に「海外もそうしているから」という理由で進めてはならない。

特に、米国のCOPPAは、データ保護法制とは別の目的（児童の安全のため）を含んでいるので、同列に捉えるべきでない。児童の安全に係る問題は、個人情報保護法とは別の法制度によって解決すべきことである。

同資料11頁には、「事例B インターネット上で児童の個人情報を公開するに際し留意すべき事項は何か」「事例C 事業者がパンフレットに児童の個人情報を掲載しているが、当該掲載について児童から口頭で同意をとったのみであり、親には何ら連絡もなかった。」という事例が掲載されているが、これらは「個人データ」の話ではなく、個人情報保護法で対処すべき事案ではない。

### 3.5. 韓国法の動向について

令和6年5月15日付の検討資料に、「本人同意を要しない個人情報の取扱いに関する外国制度等」の表がある（13頁）が、「韓国（個人情報保護法）」の欄を見ると、2020年改正のことが記載されていない<sup>56</sup>。

韓国では、2020年に「データ三法」と呼ばれる個人情報関連三法を一体的に改正し、新産業育成を趣旨とした「仮名情報」の概念を新設し、GDPRと同様に、仮名情報は個人情報に該当するものであるとしながら、統計作成、科学的研究、公益的記録保存等の目的であれば本人同意なしに処理できるとする特例を設けている。これは、まさしくここで検討されるべき事例であり、掲載されていないのは調査不足である。

### 3.6. 曾我部意見について

有識者ヒアリングでの曾我部真裕教授の意見<sup>57</sup>には、「利用目的の達成のために関連性であるとか比例性」（2頁）との記述があるが、OECD 8原則第2原則前段の「関連性」（relevancy）は、比例性（proportionality）とは別の概念であることに留意が必要である。

また、「例えば、第三者提供規律をよりフラットな比例原則に服させることも考えられないか。他方、日本法では黙示の同意、包括的同意、推定的同意も含め、同意の形式が幅広く認められており、第三者提供規律の柔軟化（事実上の比例原則の部分的採用）が図られている点にも留意が必要。」（5頁）との記載があるが、その方向性には反対である。

<sup>55</sup> 前掲注31参照。

<sup>56</sup> 表の注記には「（出典）令和5年度「個人情報保護に関する海外動向調査」（受託者：渥美坂井法律事務所・外国法共同事業）の調査結果等をもとに作成。」とあるが、この調査報告書が未公表であるため、元から記載されていなかったのか、事務局が記載しなかったのかは確認していない。

<sup>57</sup> 第287回個人情報保護委員会（令和6年6月3日）資料1-1「個人情報保護法見直しに関するコメント（京都大学 曾我部教授）」

第三者提供規律の柔軟化は、前記1.1節、1.2節で述べたように、目的内提供の制限が過剰であること、統計量への集計に際して第三者提供の制限が過剰であること、それぞれを解消する方法で解決すべきであり、その際には、利用目的拘束と基本原則の導入が前提である。こちらの方向性では、同意は原則違反の場合の特例であって、厳格な同意を求めべきであり、黙示の同意、包括的同意、推定的同意に頼らない規律を目指すべきであり、その場合には比例性で対処する必要はない。

### 3.7. 山本意見について

有識者ヒアリングでの山本龍彦教授の意見<sup>58</sup>には、「プロファイリングやスコアリング（要配慮個人情報の生成）」（1頁）との記述、「要配慮個人情報を推知する場合（要配慮プロファイリング）は、個人情報保護法第20条2項の「取得」に当たるとの解釈」（4頁）との記載があるが、プロファイリングやスコアリングで問題とすべきは、そうした方法による個人に対する「評価・決定」であって、「生成」ではない。生成はするが評価・決定に用いない場合（統計量に集計する場合）は問題とすべきではないので、この違いは重要である。また、プロファイリングやスコアリングで問題とすべきは、評価・決定の目的に照らして「関連性のない」データ項目による評価・決定のすべてであって、要配慮個人情報に相当するものに限るべきでない。

### 3.8. 森意見について

有識者ヒアリングでの森亮二弁護士の見解<sup>59</sup>では、「プライバシーの重視」が主張され、「「権利利益」の中心は、プライバシーであり、本法の目的の一つはプライバシー侵害の防止。」（2頁）と指摘されているが、OECDガイドラインはその表題とは裏腹にプライバシー保護というよりはデータ保護を実現するものであること<sup>60</sup>に留意が必要である。プライバシーは「権利利益」の一部ではあるが、その中心的なものとは言えない（前記1.1節、2.1節）。

また、「裁判所の長年の判断の積み重ねと離れて「権利利益」を考えることは、独善に陥る恐れがある。」とも指摘されているが、EU法も、判例に基づいて形成されてきたわけではなく、その立法趣旨はこれから判例で確認されていく状況にあることに留意が必要である。

また、「端末やブラウザの識別子、スマホの電話番号、メールアドレスなどを単体で個人情報とすべき」（4頁）との記述があるが、それらは「単体で個人を識別することができることとなる情報」とは言い得ても、それ単体が個人情報となるわけではない。生存する個人に関する情報の中に含まれていて初めて意味をなす概念であることに留意が必要である。

また、「特に広告IDやスマホの電話番号のような、一意性、共用性、本人到達性のある情報に紐づいたデータについては、氏名がなくとも、不適正利用の禁止や安全管理措置などの義務の対象にすべきことは明白」（4頁）との記載があるが、その主張に大筋で賛同するものの、「共用性」の要件は不要であり、個人を識別する識別子<sup>61</sup>はすべて対象とするべきであるし、「不適正利用の禁止や安全管理措置」に限定せず、すべての規律について対象とするべきである。

また、保有個人データについての「権限」について、「「開示できても訂正等はできない」ようなことは起こりうる。そのため、「保有個人データ」という概念をなくして、義務規定をたとえば「当該個人情報取扱事業者が当該個人データの開示を行う権限を有する場合には…」のようなものに改めることが考えられる」（5頁）との記載があるが、開示は訂正請求を要するか確認す

<sup>58</sup> 同 資料1-2 「いわゆる3年ごと見直しに関する意見（慶應義塾大学 山本教授）」

<sup>59</sup> 同 資料1-3 「3年ごと見直しヒアリング2024（英知法律事務所 森弁護士）」

<sup>60</sup> 前掲注4、第3節「データ保護とは何か」（57頁以下）参照。

<sup>61</sup> 昭和63年法では、個人情報の定義が「……その他の記述又は個人別に付された番号、記号その他の符号により当該個人を識別できるもの」と規定されていたように、個人を識別する識別子のすべては元々該当していた。

るための前段階の制度であり、訂正から切り離された開示を認める必要はないし、OECDガイドラインでいう「data controller」の役割であるから、訂正の権限を持つ事業者が開示に対応すべきものである。

また、「同じ問題は、22条（データ内容の正確性の確保等）についても存在するがこちらは個人データに対する義務になっており（正確な内容に変更する権限が前提になっておらず）現状では一貫性に欠ける」（5頁）とも指摘されているが、データ内容の正確性には少なくとも2つの意味があり、一つは、システム管理上データに誤りがないという意味での正確性であり、もう一つは、データの内容を決める過程での正確性であるところ、後者は確かに「保有個人データ」を取り扱う事業者には「正確な内容に変更する権限」がないが、前者は「個人データ」を取り扱う事業者一般（委託先を含む）に「正確な内容に変更する権限」があるので、指摘されるような一貫性の矛盾はない。

また、「利用停止・消去請求権の拡大」（11頁）として、無条件での利用停止・消去請求権の拡大が提案されており、JIS Q 15001でも「事業支障などの例外」を前提に認められているとされているが、無条件とするのではなく、前記の1.1節で述べた「正当な利益」に該当しないような原則違反の場合に限って認める方向性の方が適切であると考え。この場合、「事業支障などの例外」を認めるべきではない。

また、「連絡先情報の提供制限の緩和」（17頁）として、「当該個人データが、本人の事業用または本人の使用者の業務用の連絡先に関する情報であって、本人又は本人の使用者が名刺・ウェブサイト等により提供・公表しているものであるとき」は「同意のない第三者提供を認めることができる」とする提案がなされているが、そのようなデータをリスト化したファイルの表題が、例えば「修習資金の被貸与者」であれば、あるいは、表題が付けられていなくとも暗にそのようなデータであることが了解されているところでの提供であれば、法の規制対象とすべき理由は大きいのであるから、公表されている情報だから自由に使ってよいということにはならない。

以上のように、個人情報保護法の改正の方向性を検討するに際しては、法目的の観点から考えることが重要である。

以上