

2024 年 6 月 3 日

個人情報保護委員会「いわゆる 3 年ごと見直し 有識者ヒアリング」資料

いわゆる 3 年ごと見直しに関する意見

山本龍彦（慶應義塾大学）

5 1. 全体の問題意識

○個人情報保護の「本丸」としてのプロファイリング

(ex.) ケンブリッジアナリティカ事件、リクナビ事件、「ラベンダー (Lavender)」

10 ※ラベンダー：AI を用いて、ガザ地区住民の危険性を 1~100 でスコアリング (AI がハマス工作員の特徴を学習。頻繁に住所を変更、携帯電話番号を変更するなどの情報も利用)。ハマスの戦闘員かどうかを選別。殺害の標的に (精度は 90% とも)。

○心理的傾向 (精神状態) や人格的側面 (政治的信条を含む) に関する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)

15 →個人レベル：マインド・ハッキング (自律的な意思決定への介入)、差別 (AI 法、DSA の意識)

→社会レベル (民主主義への影響)：政治的マイクロターゲティング、フィルターバブル、エコーチェンバー

20 →デジタル社会、AI 社会の様々な課題の多くは、プロファイリングやスコアリングと関連している。

○個人情報保護法第 20 条 2 項との関係

→プロファイリングによる要配慮個人情報の迂回的取得

25 「本人の同意なしにプロファイリングによって要配慮個人情報を新たに生み出すことは、要配慮個人情報の『取得』に当たると解するべきかという重要な解釈問題が存在する」 (宇賀克也『新・個人情報保護法の逐条解説』〔有斐閣、2021 年〕215 頁)

○EU の関連立法

・GDPR (※個人情報保護委員会の仮訳)

30 第 21 条 異議を述べる権利

1. データ主体は、自己の特別な状況と関連する根拠に基づき、第 6 条第 1 項(e)又は(f) に基づいて行われる自己と関係する個人データの取扱いに対し、それらの条項に基づくプロファイリングの場合を含め、いつでも、異議を述べる権利を有する。管理者は、データ主体の利益、権利及び自由よりも優先する取扱いについて、又は、訴えの提起及び攻撃防御

35 について、やむをえない正当な根拠があることをその管理者が証明しない限り、以後、その個人データの取扱いをしない。

2. 個人データがダイレクトマーケティングの目的のために取扱われる場合、データ主体は、いつでも、そのようなマーケティングのための自己に関する個人データの取扱いに対して、異議を述べる権利を有する。その取扱いは、そのようなダイレクトマーケティングと関係する範囲内で、プロファイリングを含む。

- 5 ※第6条第1項(f)：管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く。

第22条 プロファイリングを含む個人に対する自動化された意思決定

- 10 1. データ主体は、当該データ主体に関する法的効果を発生させる、又は、当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含むもっぱら自動化された取扱いに基づいた決定の対象とされない権利を有する。

※米国でも、カリフォルニア州、コロラド州等のデータプライバシー法が、GDPRを参考に、プロファイリングについて具体的に規定。例えば、2021年コロラド州プライバシー法(CPA)は、「消費者に関する法的または類似の重大な影響をもたらす意思決定を促進するためのプロファイリング」を目的に行われる個人データ処理からオプトアウトする権利を保障。

15

第17条 消去の権利（「忘れられる権利」）

- 20 1. 以下の根拠中のいずれかが適用される場合、データ主体は、管理者から、不当に遅滞することなく、自己に関する個人データの消去を得る権利をもち、また、管理者は、不当に遅滞することなく、個人データを消去すべき義務を負う。

(a)

(b)

- 25 (c) そのデータ主体が、第21条第1項によって取扱いに対する異議を述べ、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、第21条第2項によって異議を述べた場合。

・デジタルサービス法(DSA。暫定訳)

30 第26条 オンラインプラットフォームにおける広告

3. オンラインプラットフォームのプロバイダは、GDPR第9条(1)で言及される特別カテゴリーの個人データを使用して、……プロファイリングに基づいて、サービス受領者に広告を提示してはならない。

35 第28条 未成年者のオンラインでの保護

2. オンラインプラットフォームのプロバイダは、サービス受領者が未成年者であることを

合理的な確実性をもって認識している場合、サービス受領者の個人情報を使用して、GDPR 第 4 条 (4) に定義されるプロファイリングに基づく広告をそのインターフェイス上で提示してはならない。

- 5 ※第 38 条 レコメンダーシステム：第 27 条に定める要件（注：レコメンダーシステムの透明性）に加え、レコメンダーシステムを使用する超大規模オンラインプラットフォームおよび超大規模オンライン検索エンジンのプロバイダは、GDPR 第 4 条 (4) に定義されるプロファイリングに基づかない少なくとも 1 つのオプションを各レコメンダーシステムに提供しなければならない。

10 ・デジタル市場法 (DMA。暫定訳)

第 15 条 監督の義務

1. 第 3 条に基づく指定後 6 ヶ月以内に、ゲートキーパーは、……そのコアプラットフォームサービスに適用している、またはそのコアプラットフォームサービス全体にわたって適用している消費者のプロファイリング技術について、独自に監査した説明を欧州委員会に提出しなければならない。欧州委員会は、監査済みの説明を欧州データ保護委員会に提出しなければならない。
- 15
2. 欧州委員会は、監査の方法および手順を策定するために、第 46 条(1)の(g)に言及する実施法を採択することができる。
3. ゲートキーパーは、第 1 項の監査された記述の概要を公開しなければならない。その際、ゲートキーパーは、その営業秘密を尊重する必要性を考慮する権利を有する。ゲートキーパーは、少なくとも年 1 回、その説明と概要を更新しなければならない。
- 20

第 46 条 実施規定

1. 欧州委員会は、以下の適用に関する詳細な取り決めを定めた実施法を採択することができる：(略)
- 25
- (g) 第 15 条(1)に規定されている、消費者のプロファイリングに使用される技術に関する監査説明の方法および手順。この目的のために実施法の草案を作成する場合、欧州委員会は欧州データ保護監督官に諮問するものとし、欧州データ保護会議、市民社会およびその他の関連専門家に諮問することができる；(略)

30

・AI 法 (暫定訳)

第 5 条 禁止される AI 実践

1. (a) 十分な情報に基づいた意思決定 (informed decision) を行う能力を著しく傷つけることによって、人または人の集団の振る舞いを実質的に歪め、それによって、その人、他者または人の集団に重大な損害を与える、または与える可能性のある方法で、その人が他の方法では行わなかったであろう意思決定を行わせる目的または効果を伴うかたちで、人
- 35

の意識を超えたサブリミナル的技法、または意図的に操作的もしくは欺瞞的な技法を展開する AI システムを市場に投入、サービス開始、または使用すること。

※プロファイリング&ダークパターン？

- 5 (b) 当該個人または他の者に重大な損害を与えるか、または与える合理的な可能性がある方法で、当該個人または当該集団に属する者の振る舞いを著しく歪める目的または効果を伴うかたちで、年齢、障害、または特定の社会的もしくは経済的状況に起因する個人または特定の集団の脆弱性を悪用 (exploits) する AI システムを市場に投入、サービス開始、または使用すること。

10

(c) 次のいずれか又は両方をもたらす社会的スコアをもって、社会的振る舞い又は既知、推論若しくは予測される個人的若しくは人格的特徴に基づき、一定期間にわたって自然人又は集団の評価又は分類を行う目的で AI システムを市場に投入、使用開始又は使用すること。

15

(i) データが当初生成または収集された文脈とは無関係な社会的文脈において、特定の自然人または集団全体に対して有害または不利な取扱いを行うこと。

(ii) 特定の自然人または集団に対して、正当化されない、又はその社会的振る舞いやその重大性に不釣り合いな有害または不利な取扱いを行うこと。

20

○総務省等での議論状況

- ・デジタル空間における情報流通の健全性確保の在り方に関する検討会
- ・同検討会ワーキンググループ
- ・利用者情報に関するワーキンググループ
- ・内閣府消費者委員会

25

➡プロファイリングは個人情報保護の「本丸」であり、個人情報保護法においても、さらに具体的な規律が必要になるのではないか。

30

2. プロファイリング

➡A I 等の高度な情報技術を用いて、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

35

➡かかる解釈（事前同意モデル）が困難である場合、少なくとも以下の規律が必要ではないか。

→要配慮プロファイリングについては、利用目的にその旨を明記し（透明性規律）、個人の関与を強化する（利用停止等、オプトアウト手続の整備）

5 3. ダークパターン

○問題状況

○諸外国の状況

10 ・「ユーザーの自律性、意思決定または選択を挫くまたは損なう実質的效果をもって設計または操作されたユーザー・インターフェース（a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice）」（CPRA、CPA）

→ダークパターンを用いて得られた同意は無効

15 ・「ユーザーを混乱させ、実際の選好とは異なる特定の行動を取らせるように意図的にデザインされた UI（user interfaces intentionally designed to confuse and manipulate users into taking certain actions that are not their actual preference.）」。Danyang Li, The FTC and the CPRA's Regulation of Dark Patterns in Cookie Consent Notices, 1 UNIV. CHI. BUSI. L. REV. 561, 562(2023); see also Jamic Luguri & Lior Strahilcivitz, Shining a Light on Darl Patterns, 20 13 J. LEGAL ANALYSIS 43, 48-51(2021).

○総務省等での議論状況

- ・利用者情報に関するワーキンググループ
- ・内閣府消費者委員会

25

→ダークパターンを用いた個人情報の取得は、個人情報保護法第 20 条 1 項の「不正な手段」による個人情報の取得に該当すると解釈すべきではないか（不正または欺瞞的 deceptive な手段?）。

30

4. 保護すべき情報の整理と保護の度合い

○問題状況

35 a. いわゆるクッキー情報等の識別情報は、プロファイリングと密接に関連。プロファイリングを目的とした識別情報の取扱いは、個人の権利利益に実質的な影響を与える（マイクロターゲティングは意思形成に影響を与える）。

b. メタバースなどの普及と生体情報（脳神経と関連した情報。脳波情報、視線情報 etc.）。
「内心」の読み取り可能性（ニューロマーケティング）

5 ○諸外国の状況

○上記 a については、まず、①識別情報のなかにも個人に戻るものと（個人界）、個人に戻らないものがある（集合界）との認識が必要。②前者（個人回帰型識別情報）については「個人情報」として取り扱うべきではないか。③こうした方向が困難である場合でも、少なくともその第三者提供等について透明性規律を設けたうえで、本人の関与を認めるべきではないか。

○上記 b については、①従来から顔特徴量データの要配慮性が指摘されてきたことに加え、脳神経と関連した情報が「内心の自由」（憲法 19 条）に対する侵害可能性をもつことを踏まえば、GDPR を参考に、生体情報を要配慮個人情報として扱う方向も検討すべきではないか。②こうした方向が困難である場合でも、少なくともその取扱いについて透明性規律を設けたうえで、オプトアウト等、本人の関与を認めるべきではないか。

20 **5. 経団連等の「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)について**

○GDPR を踏まえば、仮に「正当な利益」を導入する場合でも、後の本人関与の強化とセットで行わなければならない。

25

○「同意疲れ」の問題はダークパターンとも関係している。ダークパターンがそれなりに存在している状況を前提に「同意疲れ」を指摘し、同意の問題性や無意味さを主張することは可能なのか（同意疲れがあるならば、それを解消するためのUI等を積極的にデザインする方向で議論すべきではないか→2参照）。

30

○より実効的な執行のため、課徴金制度の導入、団体訴訟の導入は積極的に検討すべき。

○附則の「3年ごと見直し」規定は、機械的な見直しを要求しているのではない。テクノロジーの発展など、時代状況に照らしたアセスメントを行い、「必要があると認めるとき」に所要の措置を講ずるものであり、アジャイル・ガバナンスを推進するうえで必要な対応といえる。

35

○ビジネスにとって何がプラスなのか？

①グローバル・スタンダードからの乖離はビジネスにとって本当にプラスなのか。

②日本のデジタル化が進まない理由は、個人情報保護法が“厳格であること”が原因なのか。

5 日本の個人情報保護法は、GDPR や米国の一部の州法のような厳格さは有していない。その意味で、「緩い」立法であるが、それにもかかわらず、デジタル化が進んでこなかった。一層「緩く」することでデジタル化が進む保証はあるのだろうか。むしろ、個人情報保護法が「緩い」ことで、データ利用に対する不安が増大し、トラストが形成されてこなかったという側面もあるのではないか。

10 ※山本龍彦ほか編『個人データ保護のグローバル・マップ』〔弘文堂、2024年〕。日本では、データ保護等の権利についてよくわからないと答える者が多いが、プライバシー侵害への感受性は他国と比して非常に高い。実効的な規律を設ける方がトラストは形成され、利活用が進む可能性もあるのではないか。

15 6. 個人情報保護は「人権」(憲法 13 条)の問題であること

○個人情報保護法第 3 条「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに鑑み、その適正な取扱いが図られなければならない」。

→平成 16 年以降、政府が数次公表している「個人情報の保護に関する基本方針」は、いず
20 れも、この条文と憲法との関係を指摘。

→「〔個人情報保護〕法第 3 条は、個人情報が個人の人格と密接な関連を有するものであり、個人が『個人として尊重される』ことを定めた憲法第 13 条の下、慎重に取り扱われるものを示」している（平成 16 年「基本方針」）。

※園部逸夫＝藤原静雄編集『個人情報保護法の解説〔第 3 次改訂版〕』（ぎょうせい、2022 年）：法第 3 条
25 は『『人格尊重の理念』と規定することにより、憲法第 13 条の『すべて国民は、個人として尊重される』ことと本法との接点をも明確にされている」。

→直近の令和 4 年「基本方針」は、上記説明にさらに「プライバシー」の文言を追加
30 （「〔個人情報保護〕法第 3 条は、個人情報がプライバシーを含む個人の人格と密接な関連を有するものであり、個人が『個人として尊重される』ことを定めた憲法第 13 条の下……」）。

→個人情報保護法は、憲法具体化法としての側面を有する。プロファイリングは自律的な意思決定等に影響を与えるもので、法第 3 条とも密接に関連。AI 時代に、法第 3 条の趣旨を踏まえた「3 年ごと見直し」であるべき。