

「リスク分析を実施する事業担当者のための教本」より抜粋編集

情報銀行認定基準  
プロファイリングに関する  
審査の在り方と課題

2021年11月4日

情報銀行推進委員会  
認定分科会 認定事務局



## 0. はじめに

IT連盟の情報銀行認定においては、認定審査における“認定基準”及び“提出書類等”を規定した「『**情報銀行**』認定申請ガイドブック」と、認定基準の“確認方法(≒審査基準)”を記載した「『**情報銀行**』認定審査チェックシート」にて審査業務を運営しています。

2021年7月には、認定基準において「情報銀行」事業者に設置を求めているデータ倫理審査会の役割や審議すべき基本的な内容等についての共通認識を持てるよう、データ倫理審査会での審議を行うための、「情報銀行」の事例から消費者のリスク等について解説した『**データ倫理審査会審査員のための教本**』を公開。

また、併せて「情報銀行」の企画・設計・運営をしリスクアセスメントを実施する事業担当者に向け、リスク分析の考え方やその手順を解説した『**リスク分析を実施する事業担当者のための教本**』も公開いたしました。

本議事においては、この『**リスク分析を実施する事業担当者のための教本**』を元に、IT連盟の、「プロファイリング」や事業者が「個人に不当な差別や偏見その他の不利益を生じさせないように配慮しなければならない注意点」等について、事象を交えてご説明いたします。

ご参考：リスク分析を実施する事業担当者のための教本

<https://www.tpdms.jp/file/TPDMS-3200.pdf>

# 1. プロファイリングの妥当性

## 個人情報の項目の妥当性

不当な差別や偏見その他の不利益が生じる可能性がないかを確認する

個人情報の取扱いにあたっては、必要最小限の項目をもって利用目的を達成し、利用目的を超えた意味情報（行動の観測、**プロファイリング**情報等）の抽出を行わないこと（データ最小化の原則）

（IT連盟 情報銀行推進委員会）「情報銀行」認定申請ガイドブック 5.3プライバシー保護対策

取得した個人情報を利用目的の範囲内で**プロファイリング**し提供先を選別し、本人に提供先サービスを提案する際の留意事項

【本人のリスク】 **プロファイリング**のプロセスは不明瞭であるかもしれない。個人はプロファイル化されることを知らず、又は何が関係しているかを理解していないかもしれない

（GDPRに関するガイドライン）自動化された個人に対する意思決定と**プロファイリング**に関するガイドライン

「自分がどのように評価されているか」が、わからないと不安

「なぜ、自分が、このような評価なのか」理解できないと不満

「自分の知らないところで自分が評価される」のは不快

評価によって差別が助長される

対策（「わからない」ことがリスクのため、これを解決する）  
情報銀行からの個人情報の提供の提案に選別の条件がある場合、その条件を明示する  
例）〇〇地区にお住まいと推測される方に紹介するサービス

「**プロファイリング**」とは、自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の 業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱いを意味する。

GDPR 第4条（4）

## 2. 不当な差別や偏見その他の不利益が生じる可能性がないかを確認する

### 取得した個人情報の項目をプロファイリングしサービスを提案する際の留意事項

本人のリスク	「自分がどのように評価されているか」が、わからないと不安	要件	本人は <b>プロファイリング</b> に従わない権利を有する
	「なぜ、自分が、このような評価なのか」理解できないと不満		
	「自分の知らないところで自分が評価される」のは不快	対策	保護を確保するための適切な措置を実装する
	評価によって差別が助長される		



**オススメから興味のない商品を消したい** ← **プロファイリングに従わない権利の実装**

興味のない商品は、下記の手順で消すことができます。

1. 「Myページ」→「あなたにオススメ」を表示。
2. 消したい商品の「この作品に興味はありません」「この著者に興味はありません」いずれかをチェック。
3. 「チェックした評価でおすすめの商品を更新する」を選択。

「この著者に興味はありません」にチェックをすると、当該著者の別の作品もオススメされなくなりますのでご注意ください。

#### 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

1. データ主体は、当該データ主体に関する法的効果を生じさせる、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。
3. (中略) データの管理者は、データ主体の権利及び自由並びに正当な利益、少なくとも、管理者の側での人間の関与を得る権利、データ主体の見解を表明する権利及びその決定を争う権利の**保護を確保するための適切な措置を実装するものとする。**

GDPR 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

## 3. 過剰紐づけへのリスク対策

### データの最小化の原則（「情報銀行」認定申請ガイドブック）

個人情報の取扱いにあたっては、必要最小限の項目をもって利用目的を達成し、利用目的を超えた意味情報（行動の観測、**プロファイリング**情報等）の抽出を行わないこと

（IT連盟 情報銀行推進委員会）「情報銀行」認定申請ガイドブック 5.3プライバシー保護対策

### 目的を超えた紐づけ、事務に必要なのない情報との紐づけが行われないう、どのような対策を講じるか

個人情報<sup>が</sup>過剰に集約・使用されてしまうと、対象者について、業務に必要な範囲を超えて情報を得ることができ、人のプライバシーを不正に暴いてしまう恐れがある

個人情報<sup>が</sup>、使用目的を超えて取り扱われないう、また、業務に必要なのない情報と併せて取り扱われないう、合理的な対策が講じられるか、システムと人の操作の両面から検討

システム間ではさまざまな接続／連携がなされており、適切な制御をしなければ、別々のシステムで保有されている個人情報<sup>全て</sup>を紐づけ・参照等することもできてしまう

特に、さまざまな事務で共通基盤として用いられているようなシステムでは、一つの事務に必要な情報以外のさまざまな範囲の情報<sup>を</sup>保有することが考えられる

共通システムではない個別システムであっても、過剰紐づけ・参照等のリスクがある

システム上で適切な制御がなされていても、運用者がさまざまな権限を悪用して、業務と無関係な個人情報<sup>を</sup>手動で集めてしまうリスクもある

以上のリスクを防止するためのリスク対策を検討

## 4. 過剰紐づけの事例

**プロファイリングの結果、既知の個人情報から要配慮個人情報など本人の望まない個人情報が推測され過剰紐づけされた事例**

### 米国のスーパーマーケットTarget社

「無香料性ローション・特定サプリメント・大きめのバック」の購買履歴等から、妊娠している可能性が高いと推測した顧客に、ベビー服等のオファーを提供した。ティーンエージャーの娘に対して、一緒に住む彼女の父親が妊娠の事実を知る前に、妊娠に関連する広告が送られてきてしまった。

(出典：山本龍彦「ビッグデータ社会とプロファイリング」(『論究ジュリスト』2016年夏号所収))

### Facebookの「いいね！」を用いた研究

ある研究では、Facebookの「いいね！」の履歴と他の情報を組合せることで、男性利用者の性的指向の88%、利用者の民族的素性の95%、利用者がキリスト教徒かイスラム教徒かの82%を正確に予測することができた。また民主党支持か共和党支持かの85%、アルコール・ドラッグ・煙草を使用しているかの65～75%を正確に推測することができた。

(出典：Federal Trade Commission (FTC) 「Big Data: A Tool for Inclusion or Exclusion?」(2016年1月))

出典 水町雅子「パーソナルデータを巡る現状の問題点」平成25年10月  
<http://www.kantei.go.jp/jp/singi/it2/pd/dai3/siryoku6.pdf>

### 【対策として】 本人への説明

進学先情報等、取得した情報によりレコメンドが変化する場合、不当な差別とならないようレコメンドの選定基準も明らかにする。  
(例：○○地域にお勤めの方へのレコメンド、○○学校に通学のお子様がいる方へのレコメンド等)