（資料３）

検討の拡充に向けた視点へのコメント

本資料は下記に対してコメントしたものです。
「個人情報保護法のいわゆる３年ごと見直しの検討の充実に向けた視点」の（参考４）視点の例

各ページのタイトルの数字と小番号（①②③…）は参考４の項番に対応します。

2024年12月3日
NTT社会情報研究所
高橋克巳

1 本人の関与により規律しようとする仕組みの実効性 ①

①自律的ガバナンスの考え方

「利用目的内での利用義務、通知・公表、本人関与で事業者が是正」
＋「社会によるモニタリング」でガバナンス(検討拡充視点より)

- 上記の全体構図に疑問を持たない
- 実際上、本人関与(前項)を行使できる人は少なく、社会モニタリング頼りになる
- 本人関与が困難な理由
  - 利用目的の理解ができない
  - 理解できてもオプトアウトの仕組みがない*

＊ オプトアウトの仕組みがない

- 方法が用意されていない
- 用意されていても見つけられない／使い方が難しい
- オプトアウトすると不利になると思い込まされる
- オプトアウトすると不利になる（サービスが実質上受けられない）

１ 本人の関与により規律しようとする仕組みの実効性 ②④

②利用目的やデータ処理の態様の説明の在り方

- 個情法は抽象的・一般的ではなく、具体的な利用目的の特定を求めているが、そのことの弊害がありうる
- 弊害の可能性例
  - 詳細な説明が熟練者や専門家でないとわからない
  - 詳細な説明が多数列挙される場合、把握できない(見落とし)
- 「本人にとって一般的かつ合理的に想定できる」ことの徹底を提案
  - 抽象化した説明を推奨し、その徹底にモニタリング等ガバナンスを効かせてはどうか
  - 社会モニタリングにおいても高い抽象度で見ることに実現可能性がある
    - 個別の詳細事象のチェックは実質上困難
  - 抽象化した利用目的説明の例→次ページ(参考1)
- ④利用目的の「関連性を有する合理的な範囲」も同様に(抽象化レベルで)

(参考1) 利用目的の抽象化

- 理解しやすい利用目的の説明方法案

	必要	追加的	第三者への提供
個人単位	A	C	E
全体・集団（統計的）	B	D	F

A)　サービスの提供に必要で個人単位に使うもの
B)　サービスの提供に必要でお客様全体で使うもの
C)　新しいサービスの提案等個人単位に使うもの
D)　サービスの企画開発や調査に使うもの

E)　第三者に提供して、提供先で個人単位で使うもの
F)　第三者に提供して、提供先で統計的に使うもの

- 補足
  - 具体的な説明も併用する(抽象化カテゴリの下にぶら下げる等)
  - 本マトリックスで拾えていない性質もある
    - 自動的な評価・判断をするかどうか(プロファイリング関連)

１ 本人の関与により規律しようとする仕組みの実効性 ③

③こどもの保護

- こどもの保護は必要
- こどもの個人情報の取扱いの悪影響の全貌は、まだわかっていないと考えられる
  - 親も判断できないものがあるのでは？
- したがって、一旦抑制的にした上で、有効な補完的な仕組みを見出し、それに応じて利用を進めるのが良いのでは
  - 補完的な仕組みの検討・後押しは規制側の協力も必要
    - 補完的な仕組みとは、こどもの判断等を代替できる技術やガバナンスの仕組みを想定しています

１ 本人の関与により規律しようとする仕組みの実効性 ⑤

⑤本人関与に依存せず、事業者判断と結果責任のアプローチ

- 本人関与のアプローチには一定の限界があると考えられる
  - 高い抽象度による説明アプローチを提案したところ
- これにも限界がある場合には、結果責任を問わざるを得なくなると考えられる

１ 本人の関与により規律しようとする仕組みの実効性 ⑥

⑥本人の権利利益に相当な影響を与えるプロファイリング等

- 論点とプロファイリングの概念を確認したい
- 「個人のデータを用いた自動的な処理で、本人の権利利益に相当な影響を与えるもの」*が、本論点と考えて話を進める
  - 自動的な処理による弊害は現在過小評価されている状況
  - 看過できない理由
    - 不正確な情報による処理
    - 本人の知らぬところでの、本人への評価・判断
    - 不公平な処理、機会損失
    - (プライバシー、自己情報コントロール、…)
  - 少なくとも論点の処理*が行われる場合は、はっきりと本人に理解させる必要がある
- プロファイリングの整理→次ページ(参考2)

(参考2) プロファイリングの整理

- プロファイリングとは (wikipedia)
  - In information science, profiling refers to the process of construction and application of user profiles generated by computerized data analysis.
  - (訳) 情報科学におけるプロファイリングとは、**コンピュータによるデータ分析によって生成**された**ユーザープロファイルを構築し、適用する**プロセスを指す
  - GDPRにおける**個人データの自動的な取扱い**とも整合
- ２つのプロセス
  1. ユーザプロファイルを構築するプロセス
     - ユーザからデータを取得する
     - ユーザから取得したデータを用いユーザプロファイルを推定作成する
  2. ユーザプロファイルを適用するプロセス
     - ユーザプロファイルを用いて、サービスを提供する
       - 例）ターゲット広告表示
- 補足
  - このように見ると、プロファイリング自体に大きなタブーがあるわけではない
    - 「自動的な処理で相当な影響を与えるもの」が論点(前頁の再掲)
  - ユーザプロファイルとは個人情報の定義とほぼ同じ
    - 推知した属性等の位置付けが個情法的に不確定と考えられる

１ 本人の関与により規律しようとする仕組みの実効性 ⑦⑧

⑦事業者の自律的な改善の有効性

- 他の項目で論じた通り、自律的な改善には限界がある

⑧より能動的な本人関与(開示請求、 利用停止、 データポータビリティ等)

- 必要性に疑問を持たない
- 仕組みの強い義務化が形骸化実装されないよう、注意深いルール作りと運用が必要と考える
- 例えばデータポータビリティの有効で誠実な実装はかなり難しいと考える
  - 範囲や対象が不明確(場合によっては事業者の恣意性)
  - ポータブルにしたデータが活用できる社会的仕組み作りとセットでの推進することが大事

2 個人への直接的な影響が想定されない個人データの利用に対する規律
3 個人データの第三者提供を原則として禁止する仕組みの妥当性(1/3)

「個人への直接的な影響が想定されない個人データの利用」の規律等(検討拡充視点より)

- 利用目的の変更や第三者提供の可否(利用目的制限)は、データの個人識別性の有無で判断されていたと考えられる(以下は、従来の考え方を整理したもの)
  - 個人識別性があるデータは、個人への影響がある利用(個人への直接的な影響が想定される個人データの利用)をする場合、利用目的による制限を受ける → A,B
  - 個人識別性がないデータは、個人への影響がないとみなされ、制限を受けない→ C,D
  - Bがどうあるべきかが本論点

個人 識別性が		個人の権利利益への影響が	
		想定される利用	**想定されない利用**
あるデータ	利用目的制限あり	A	**B**
ないデータ	利用目的制限なし	C	D

- A 個人情報利用の基本的な規律が確立
- B **検討拡充視点の論点**
  - 利用目的の変更や第三者提供ができない → 本論点 できてもよいのでは？
- C やや混乱がある利用
  - そもそも個人を特定した利用ができない → 参考 個人を特定した利用の存在 (Cookie問題→令和2年改正)
- D 非個人情報としての利用規律が確立
  - 統計データは個人を特定して利用できない → 参考 匿名加工情報(平成27年改正)はこれに準ずる考え方

2 個人への直接的な影響が想定されない個人データの利用に対する規律
3 個人データの第三者提供を原則として禁止する仕組みの妥当性(2/3)

- 従来の**データの個人識別性有無**での利用目的制限を、**利用の個人への影響の有無**で制限してみる場合を考察する
- **利用の個人への影響の有無**による制限規律には一定の合理性があると考えられる
  - B領域の「利用データ品質問題」が解消できる（ニーズ例）
    - 第三者提供するデータを提供元で匿名加工・統計化をしてから提供する場合(D迂回)、提供先で利用できる統計等データの精度やバリエーションが限定されるため、提供先は個人識別性があるデータを自身で処理したい
  - ちなみに盲点となっていたC領域の混乱が整理できる
    - Cookieデータの第三者提供問題(実質個人情報の第三者提供問題)→令和２年改正で個人関連情報規律
    - 仮名データは第三者提供して良いという誤解の払拭 (個人識別性の有無に関わらず個人への影響があれば制約受けべき)
- 同、B領域でプライバシー上のリスクがある（リスク例）
  - 統計作成だけに限定して(個人識別性があるデータを)第三者提供したが、提供先で個人への影響がある利用をされてしまう
  - 提供先で統計やAI利用だけの限定利用が徹底されるが、巨大なデータベースが独占的に形成され脅威となる

(従来)データの個人識別性有無での利用目的制限(再掲)

個人 識別性が		個人の権利利益への影響が	
		想定される利用	**想定されない利用**
あるデータ	利用目的制限あり	A	**B**
ないデータ	利用目的制限なし	C	D

(考察)利用の個人への影響有無での利用目的制限

個人 識別性が	個人の権利利益への影響が	
	想定される利用	**想定されない利用**
	利用目的制限あり	利用目的制限なし
あるデータ	A	**B**
ないデータ	C	D

２ 個人への直接的な影響が想定されない個人データの利用に対する規律
３ 個人データの第三者提供を原則として禁止する仕組みの妥当性(3/3)

個人への直接的な影響が想定されない個人データの利用」に関する提案

- 従来の**データの個人識別性有無**での利用目的制限には、利用データ品質問題や、個人識別性の盲点があった
- **利用の個人への影響の有無**での制限にはプライバシー上の課題がある
- 同課題が解決される前提で、後者の規律も盛り込む検討の価値がある
- 課題の解決方法(案)
  - 透明性(実施の公表等)と セキュリティ(漏洩対策)が前提
  - 技術を含むガバナンスで、提供先に利用制限をさせることへの挑戦
    - 例えば、提供先で統計的にのみ利用される制限等
    - 実効性のある具体策を見出し、エンカレッジしてはどうか
    - PETs(プライバシー保護技術)の利用
    - 匿名加工情報はPETs利用ガバナンスの実現例

４ データの適正な取扱いに係る義務を負うべき者の在り方

- データコントローラーが責任を持つべき点は不変
- 委託やクラウド利用の実態を考えると、データプロセッサーが実質上の担い手なのは明らか
  - 少なくとも、データ処理の態様の詳細な説明はデータプロセッサーでなければできない
- データコントローラが本当に責任を果たせているかを確実にするために、プロセッサーへの規律を導入して、それを支援することは妥当

5 守られるべき個人の権利利益の外延

- 外延については、利用目的制限に関する**データの個人識別性有無**と、**利用の個人への影響の有無**の考察で論じた通り
  - 個人識別性の盲点の解消
    - データに個人識別性があろうがなかろうが、個人への影響があれば制約受ける
- リスクの整理
  - (A)(B)(C)(D)等のリスク視点と独立に「事業者想定」に関して以下の軸を提案
    - 本人が想定しない事業者に自分の個人情報を利用される
    - (想定する事業者だが)本人がそうとは知らず自分の個人情報が利用される
    - データの量や種類が想像を超えて集まり、本人が想像できない利用がされる

6 個人データそのものの特徴に起因する考慮要因(差別的評価等)

- 要配慮個人情報の利用を制限して、差別的評価等を制約する考えは妥当
- ただし、差別的評価は、要配慮個人情報だけを起因とするものではない
- とはいえ、仮に差別的評価に起因しうる個人属性をどんどん網羅して規制を強化するアプローチがあるとしたら、慎重に進めるべきと考える
  - 「長期的な本人の追跡」に規律を導入することには賛成するが、「その手掛かり」となる識別子を網羅し規制することの実効性や影響はよく議論したい
  - 差別的評価に起因しうる個人属性には、例えば年齢、性別があるが、これらを規制することの実効性や影響はよく議論したい
- 以上を考えると、データそのものの要因側規制をすることには疑問を持たないが、結果責任を考えざるを得ないと思われる

以上