資料１－１

個人情報保護委員会
「いわゆる３年ごと見直し」
ヒアリング

2024年6月12日

国立情報学研究所

佐藤一郎

3年ごと見直しに向けて

- 3年ごと見直しにおいて検討すべきこと
  - 課徴金、団体訴訟制度、未成年者の保護、生体情報の保護強化
  - 仮名加工情報に関わる規律
  - データ類型の再整理
  - プロファイリング規制の明確化
  - AIと個人情報保護法
  - 体制及び３年ごと見直しに関して
  - 企業の自主的取り組み

佐藤一郎（国立情報学研究所）

課徴金、団体訴訟制度他

- 課徴金は導入すべき
  - 理由：海外制度との整合性に加えて、悪質事案の対策。なお、悪質、重大事案が対象であれば「萎縮」を懸念することはないのではないか
- 団体訴訟制度は導入すべき
  - 理由：少額大量被害の場合、現状、訴訟は被害者に不利益であり、その緩和が必要ではないか
- 未成年者の保護は導入すべき
  - 理由：海外制度との整合性に加えて、ネット利用の拡大により、未成年者が個人情報に関わるトラブルに巻き込まれるリスクが高まっている
- 生体情報の保護強化は導入すべき
  - 理由：生体認証の普及により、生体情報の取得・利用機会が増えている。また、今後、センサー及びカメラの性能向上により、本人が気がつかずに生体情報の取得利用が増えると予想される

仮名加工情報の規律の明確化(1/4)

- 法第41条(第9項)により、仮名加工情報は漏えい報告義務がない
  - しかし、仮名加工情報の加工は限定的なため、例えば会員番号などの公知または他事業者と共有される識別子などは、仮名加工情報にそのまま残存することから、仮名加工情報が漏洩したときは、個人が特定される可能性が高く、さらにその仮名加工情報に含まれる情報から個人の権利利益の侵害が起きるリスクも高い
  - 従って、仮名加工情報にも漏洩報告義務を課すべきである
  - 加えて、そもそも仮名加工情報はデータ分析を想定したデータ類型であること、前述の情報漏洩時のリスクを考慮すると、法41条５項の当該個人データ等を遅滞なく消去については努力規定から義務規定に変更することと、個々のデータ分析作業時に仮名加工情報を作成し、分析作業終了後に直ちに削除することも検討すべき

- 備考：産業界からは、仮名加工情報以外を含めて個人情報の情報漏洩の報告について、「おそれ」の段階は報告義務から外す意見もあるようだが、情報漏洩時、その漏洩の影響は事業者であっても正確に把握・予測できるとは限らないことから、「おそれ」の段階であっても、漏洩報告を求めるべきである

仮名加工情報の規律の明確化(2/4)

法41条7項　仮名加工情報取扱事業者は、仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合してはならない。

- 仮名加工情報は個人を識別する目的でなければ、他の情報と照合できることになるが、仮名加工情報に含まれる各個人に関する情報と、別の情報のその個人に関する情報を連結した情報は、各個人に関する情報が詳細かつ巨大化しやすい
  - その連結して作られた情報は、個人の想像を超えて詳細かつ巨大化しやすい
  - また漏洩時の権利利益の侵害リスクも高い
- 多様な事業を行っている事業者は、それぞれの事業の利用目的のための個人データを仮名加工情報に加工して、それらを連結して、個人に関する詳細かつ巨大な情報を作り、それをさらに目的外に利用できる
- 個人情報の本人を識別する目的か否かは事業者の判断に依存しやすく、外部的観測も難しいことから、違反行為があっても個情委は指摘・摘発が難しいのではないか
- 従って、仮名加工情報と別の情報（仮名加工情報を含む）の照合には一定の制限が求められるべき
  - さらに事業者には仮名加工情報の照合範囲と照合により連結された情報に関する詳細な説明を公表する等の義務化を検討すべきである

仮名加工情報の規律の明確化(3/4)

- 利用目的の異なる複数の個人情報について、それらを連結した仮名加工情報の作成する方法として、
  - 方法①利用目的が異なる個人データから仮名加工情報を作成し、その仮名加工情報同士を突合（個人ごとに情報を連結）する
  - 方法②利用目的が異なる個人データを、個人データのまま突合し、その突合した個人データから仮名加工情報を作成する
  - がありえる

- ここで、方法②は各個人に関して膨大な個人情報が生成されることと、それが漏洩すると、元の個人情報以上に、個人の権利利益の侵害が大きくなるおそれがある。従って、
  - 仮名加工情報の作成において、方法②を制限することを検討すべき

仮名加工情報の規律の明確化(4/4)と共同利用

- 仮名加工情報は第三者提供されない前提だが、ある共同利用に参加する事業者同士は、ある事業者が作成した仮名加工情報を、他の事業者と共有することや、個人の識別を目的としなければ、他の事業者は共有された仮名加工情報と他の情報を照合・連結することも許容されてしまう（法第41条第6項、第27条第5項、９項他）
  - しかし、共同利用においては、一定の説明があるにしても、仮名加工情報が個人の想定の範囲を超えて共有されうる、またその仮名加工情報の利用も個人から想定が難しいのではないか
    - 従って、共同利用における、仮名加工情報の共有を禁止すべき
- 現状の条文及びガイドラインだと、ある事業者が複数の共同利用に参加しているとき、その事業者はある共同利用において他の事業者から共有した仮名加工情報を、それが参加する別の共同利用において共有することが許容されてしまうのではないか（共同利用から別の共同利用へ、仮名加工情報を数珠繋ぎ的に拡散できる）
    - 加えて、複数共同利用を跨ぐ、仮名加工情報の共有も禁止すべき

- なお、仮名加工情報に限らず、共同利用はそれが可能な客観的範囲が不明確であり、第三者提供の制限規制の潜脱に使われるおそれがあるため、共同利用可能な範囲を明確に制限すべきである

技術的議論の必要性

- 仮名加工情報が導入された2020年改正案ができる前となる、第106回 個人情報保護委員会(2019年5月21日）において下記の発言をしております

> 取りまとめの資料に仮名化に関する議論がありました。仮名化に関しましては、ＧＤＰＲにあって、日本にないからというロジックは避けたいところですけれども、需要があれば、導入していただければと思いますが、ただ、技術的な議論は当然必要だと思っております。
>
> 8

個人情報保護委員会：第106回個人情報保護委員会議事録より

- 上記の発言はEU GDPRなどの仮名化を念頭に置いている。なお、GDPRの仮名化と仮名加工情報は相違しており、実際、EUの十分性認定においては個情法の仮名加工情報はEUから移転した個人に関するデータに適用できないのではないか
- 個情法の特性から、法律案及びガイドラインが決まる前に技術的議論が必要であり、それらが決まってからは、技術的な問題があっても対処が難しい
- 今後、AIやIoTの発展により、個人情報の取得技術、分析技術、利用は高度化すると予想される。そうした技術動向への対応には技術的議論が必要なはず

データ類型の再整理

- 個情法のデータ類型は現在の技術に適合しているのか

> 法第16条（第1項）この章及び第8章において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。
>
> (1) 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
>
> (2) 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

- 現在、全文検索や画像判定技術の進歩により、「体系的に構成」されていないデータであっても、検索可能であることは多い
  - テキスト中に散在的に含まれる個人情報も、現在の全文検索技術を用いれば検索可能
  - 現代の画像認識技術は、一定の解像度を持つ顔映像を含む画像であれば、顔画像の抽出と識別を可能にし、これは検索と等価な結果をもたらす
- 「個人情報データベース等」は、検索可能か否かが個人に関する情報の保護で重要な区分であり、「体系的に構成」されたデータを検索可能とする要件と捉えているのであれば、現在の技術水準と合致していないといえる。従って
- 「個人情報データベース等」の定義を「体系的に構成」から検索可能性に基づくものに変更すべき
  - なお、検索可能か否かとは別に、あるデータの利用が個人の権利利益に深刻な影響を与える場合かつ、事業者がデータに対して開示・修正・停止できない場合、そのデータの利用には一定の制限を検討すべき

プロファイリング規制の明確化

第287回個人情報保護委員会の山本龍彦先生、森亮二先生の意見と重なる

- プロファイリングは、個人の想定を超える詳細化や、属性推定が行われ、さらに間違いも多く、個人からはそのプロファイリングが行われていることを含めて、その内容が見えないことから、個人の権利利益の侵害を生みやすい
- プロファイリングでは個人に関する情報の推知を広く行うが、個情委はQ&A4-9のように推知による情報は要配慮個人情報とは認めていないと解釈される
  - 利用目的の特定（17条）、不適正利用の禁止（19条）、開示請求（33条）、利用停止・消去（35条）などの規律はあるが
- これにより推知、さらにプロファイリングによる情報による個人の権利利益の侵害を防げないといえないか。これを是正するために
  - 推知も法的に「取得」として扱うべき。これにより推知による情報が（要配慮）個人情報に相当する場合は（要配慮）個人情報として扱うべき
  - 要配慮個人情報の推知を含めて、個人への影響が大きい情報のプロファイリングは、その影響の深刻度に応じて、その実施禁止や、事業者に詳細な説明義務や同意などを課すべき
  - 個人がその説明に納得せず、かつ推知の情報やプロファイリングの影響が深刻な場合、対象個人が開示・利用停止・消去が行えるべき

具体的には、例えばGDPRにおけるプロファイリングに関する規制を参考に、特定のデータ利用目的の明示、同意、誤情報に基づくプロファイリングの是正手続きなどを導入することを検討すべきではないか

備考：経済界からの19条の具体化の要望があるが、プロファイリングに関する規制を強化することは、その要望への実効的な解答となりえるはず

AIへの対応 (1/2)

- AIによる生成や判定の問題は、プロファイリングと重なる一方、AIによる推測や評価はプロファイリングよりも詳細かつ広範囲となりがちで、個人の権利利益の侵害が深刻化しやすい
  - 欧州のAI規制法は、個人のデータに関してはGDPRの規律を参照する構成
    - GDPRはプロファイリングを規制しており、AIによるプロファイリングも規制
  - 国内でAI規制の議論が進行中であるが、規制対象となるAIの定義が不明確であるため、実効的な規制の実施が困難となるおそれがある
    - その結果、事業者が実際にはAIを提供・利用しているにもかかわらず、これを否定する主張を行うことで規制を回避できる可能性があるのではないか
- 従って、今後、国内のAIの規制を強化する場合も、AIの提供・利用において、個人情報に関わる部分は個情法で規制すべき。一方、AIの規制における個人情報に関わる規律が含まれる場合、個情法に対する上乗せ規律となるべきである
  - その観点でも個情法によるプロファイリングの規制は不可避ではないか

- AIの結果は、間違いや偏りが大きい。一方で学習モデルは事業者であっても開示・修正・削除は困難である。従って、
  - AIの間違った判断・生成による個人の権利利益の侵害については、個人に開示及び修正の手段は用意すべき。だが、それが困難としても、何らかの救済手段を設けることを検討すべき

AIへの対応 (2/2)

第279回個人情報保護委員会の高橋克巳氏の意見と重なる

- 機械学習における学習モデルは統計的データであり、さらに一般には学習モデルの元となった訓練データに復元できないことから、学習モデルを個人情報及び個人データとして扱うべきではない
  - しかし、学習モデルの構築コストが大きいことから、学習モデルの第三者提供が広がる可能性が高い。このとき
    - 学習モデルは複雑で、学習モデルに訓練データを復元する仕組みを含んでいたとしても、学習モデルから仕組み等の発見は困難、従って、
    - 学習モデルは個人データではないと扱う場合、学習モデル全般ではなく、個人データを復元できない学習モデルに限定すべき

補足：個人データを提供先がAIの学習モデル構築に利用する場合に限り、同意なしでの第三者提供を許容する考え方もありえるが、 AIの結果は個人の権利利益の侵害につながりやすいことを考慮すると、その考え方は下記を要件にすべき

- 学習モデルの構築後、直ちに個人データが削除されることに加えて、その学習モデルから個人データまたはその一部が復元されないことを担保すること
- さらに個人に対してその第三者提供に関する説明は求められる。加えて
- 個人の権利利益の侵害が想定される場合、個人は第三者提供及び提供先におけるその個人に関する情報の利用の停止・修正・削除ができること

AIとプライバシー

- 個情法は直接、プライバシーを保護するものではないが、AIを含む高度なデータ分析や大量かつ詳細データが増える状況を前提に、プライバシーの重視をすすめるべきである

- AIは人間が気がつかなかったような個人のプライバシーに関する情報を推知・評価する可能性がある、また生成AIなどは結果を予め予想できないことから
  - 対象個人はもちろん、AIの提供・利用事業者もプライバシーに関わる影響（個人の権利利益の侵害を含む）を予め想定できるとは限らない
- 従って、その場合
  - 事前（AIによる判定・評価・生成を行う前）には、AI提供・利用事業者であっても、「個人に対して適正な自己情報の取り扱い」を実現できるとは限らない
  - 事後には、 AI提供・利用事業者はAIが推知・利用したプライバシーに関する情報及びそれによる影響を知りえることもあるが、対象個人はそのプライバシーに関する情報及びそれによる影響を知りえるとは限らないことから、 AI提供・利用事業者と対象個人では情報の非対称性が生じる
    - 情報の非対称性を解消するためには、事業者は対象個人が自己の情報の利用の是非に関して判断できる程度の説明と、自己の情報をコントロールできる手段をその対象個人に提供することが求められるのではないか

独立性と３年ごと見直し

- 独立行政委員会である個人情報保護委員会は、国の産業推進策やIT推進策とは独立に、個人情報に関わる規律の整備（立法を含む）やその執行を担うべきである

- ３年ごとの見直しは堅持すべきであり、その背景には以下の理由がある
  - 2003年の個人情報保護法も制定の際、衆参両院は5年以内の見直しを付帯決議したが、2015年まで実施されなかった
  - ITの進化についていく観点から、３年ごと見直しが求められたはず
    - なお、生成AIの普及は3年前には想定できなかったように、３年ごとのサイクルでも技術進化に対して遅いというべき
    - ITの進化が次々と生み出す問題を、迅速に規律することが、個人が安心してITを利用できることになり、結果として産業界にとってもメリットが大きいはず
    - 一部事業者団体からの「見直し時期を延ばすべき」という主張は、ITの進化に適応する意欲の欠如と受け取られるのではないか
  - 法案化を含めて結論が早々に出る見直しについては３年ごと見直しサイクルで見直すべき
  - 一方、議論に時間がかかるものの見直し作業が遅れるのは仕方ないが、次の３年ごと見直しを待たず、早々に法案化を含めて、必要な見直しを行うべき
    - 法改正が連続する場合、個情委の負担は理解するが、個情法の特性上、短期の見直しサイクルは避けられないのではないか

プライバシーと個人情報保護

- 個人情報ではないが、プライバシーに関する情報の範囲が拡大している状況であり、本来、それにあわせて個人情報の範囲を拡大すべきであるが、個人情報の範囲は広がっているとはいえない
- 個人情報とプライバシーに関する情報は同じではなく、個人情報保護法を順守していても、プライバシー侵害が生じえる
  - さらに事業者は、プライバシー侵害によって裁判所で差止請求、損害賠償請求を受けると事業支障になることから
- 個人情報に該当しないプライバシー関連情報は、主に事業者の自主的な取り組みが期待される状況
  - 事業者は個人情報保護法順守のためのガバナンスのみならず、プライバシー侵害を防止するガバナンスが求められる
- 個人情報保護委員会は、事業者の自主的なプライバシー保護活動に積極的に関与すべきではないか
  - 例：経産省・総務省「プライバシーガバナンスガイドブック」(2023)などの民間のプライバシー保護に関わる取り組みがある（6月3日のヒアリングで、宍戸先生が言及）
    - 経産省及び総務省の判断にもよるが、経産省・総務省・個情委の共管によるプライバシーガバナンスガイドブックの整備を検討する価値はあるのではないか
  - 加えて、学術研究機関等が第59条に基づき自主規範を策定・公表する際の努力義務に対しても、個情委の啓蒙活動が期待される

ご清聴ありがとうございます

国立情報学研究所

佐藤一郎