生成AIと個人情報保護法

一般財団法人 情報法制研究所
副理事長 高木浩光

昨年ChatGPTで騒然

- イタリアのデータ保護機関GPDPがOpenAIのChatGPTにGDPR違反の懸念を通告、利用停止に（3月31日）
  - イタリア副首相「行き過ぎ」と苦言、他国も調査を開始と発表
  - 4月末までに対策を求める（4月12日）禁止を解除（28日）
    - GDPRが要求する公表事項を公表すること
    - 学習のための利用者の個人データ処理の適法性根拠を「契約の履行」でなく「同意」か「正当な利益」とすること
    - 不正確に生成された個人データの修正・削除の請求権行使に対応すること、「正当な利益」の場合、アルゴリズムに異議を唱える権利にも対応すること
    - 未成年者の利用制限を実装すること
    - 学習に個人データを使用していることを知らせるキャンペーンを実施すること
  - 調査は継続
- 日本の個情委が注意喚起（6月2日）
  - G7サミット（6月13日-15日）に間に合わせた？

個情委の注意喚起

- 2つの注意喚起
  - 生成AIサービスの利用に関する注意喚起等
  - OpenAIに対する注意喚起（の概要が公表）
- 利用に関する注意喚起
  - プロンプト入力に個人情報を含む場合、利用目的の達成範囲内であることを確認
  - 個人データをプロンプト入力したものが出力以外に取り扱われる場合は第三者提供制限に違反する可能性があるので、当該データが学習に利用されないことを確認
  - 入力された個人情報が学習され正確・不正確な内容で出力されるリスクがあるので、個人情報を入力「等」する際はリスクを踏まえて判断
  - 応答結果に不正確な内容の個人情報が含まれるリスク、生成AIサービスを利用して個人情報を取り扱う際にはそのリスクを踏まえて判断
  - 利用規約やプライバシーポリシー等を確認し適切に判断

疑問点

- プロンプト入力が学習される？
  - 出力の改善に使うことがあることと、学習の入力になることは別では？
    - 出力の改善：どんなプロンプト入力でエラーが出たかを確認するなど
    - 第三者提供制限違反は、どの段階から？
    - プロンプト入力中の個人情報が学習に利用され出力されるリスク？
  - 一般的なSaaS利用時の注意点と同じでは？
    - Google検索利用時の注意点と何が違う？
- 応答結果に不正確な内容の個人情報が含まれる？
  - 何を問題にしているのか？
- 問題にすべきは、生成AIを用いた個人データ処理では？
  - 教員が児童生徒の採点や成績評価をLLMで自動処理とか

OpenAIへの注意喚起

- 要配慮個人情報の取得
  - 学習のための情報収集について以下の4点を実施すること
    - 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
    - 収集後できる限り即時に、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
    - それでもなお含まれていることが発覚した場合は、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
    - 本人又は個情委が特定のサイト又は第三者から要配慮個人情報を収集しないよう要請又は指示した場合には、拒否する正当な理由がない限り、当該要請又は指示に従う
- 利用目的の通知等
  - 利用者と利用者以外の本人に利用目的を通知又は公表

疑問点

- 違法なのに「できる限り」でいいの？
  - できる限り減少させる、できる限り即時に、発覚した場合は
- 収集しないよう要請、個情法の根拠規定ある？
  - 要配慮個人情報の取得制限にオプトアウト方式はないのだが
- 検索エンジンのクローラだって同じなのに？なぜ今？
  - どのように解決するのか？
- そもそも違法ではないのでは？
  - 「要配慮個人情報の取得」とは如何なる意味かの問題
- 利用目的の公表なんて意味なくない？
  - 利用者はともかく、利用者以外の本人に対して？
- そもそも個人情報として取り扱っていないのでは？
  - いわゆるクラウド例外（Q7-53）「クラウドサービス提供事業者が、個人データを取り扱わないこととなっている場合」

要配慮個人情報の取得制限

- 20条（適正な取得）2項
  - 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。
    - 7号当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、第57条第1項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合
    - 8号 その他前各号に掲げる場合に準ずるものとして政令で定める場合
  - 施行令9条（要配慮個人情報を本人の同意なく取得することができる場合）
    - 1号 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を取得する場合
- 本人以外が公開している情報が問題となる
  - 個情委の注意喚起もそこ間違えてない？
- 疑問がいくつも
  - 「取得」とはどの段階？ なぜこの例外を設けた？ 本末転倒では？

そもそもおかしい規定

- 本末転倒な例外
  - 施行令9条1号 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を取得する場合（は取得OK）
  - ガイドライン通則編3-3-2
    - 例示「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（目視による取得）」
    - 検討時の理由「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」
- 取得とは記録した場合
  - 見るだけでは取得ではないとされている
  - 撮影での録画から除くことが難しいのはわかるが
  - 目視しても記録しないでおくことはできるのになぜ？

本来の方向性

- 個人データとして取得する場合を規律すべき
  - 個人情報データベース等を構成する個人情報として
- 法目的の観点から
  - 他人に知られたくない秘密の保護……ではない
    - それも一部ではあるが、事業者のデータベース管理の話
    - 「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」との正当化は、法目的を履き違えている
  - 差別的な決定がなされないことこそが保護すべき核心的利益
    - 「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（目視による取得）」をOKにしてどうする？
      - 身体障害者をデータベース化して差別的に対応（身体障害とは関連性のない決定の目的で利用）する行為を防げなくなっている

本来の法目的

- 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
  - データ処理とは、データに対して行われる操作の体系的実施
  - 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
- 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
  - 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）
    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）
  - 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）」でなければならず（関連性の原則）、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。
  - 「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とパラレルであり、非差別原則の実現にある
- 目的外利用禁止、提供制限等はその実現手段としての政策的規制にすぎない

GLOCOM
六本木会議

デジタル社会を駆動する
「個人データ保護法制」にむけて

2022 年 12 月

GLOCOM 六本木会議

個人情報保護は「個人データ保護」へ。
これからのデジタル社会をつくる次の１歩です。

Now 現状　個人情報保護、何を保護するのか見失っている。

- 「情報」の保護ではなく、個人データ処理からの「個人」の保護
- 「個人データ処理」を中心とした、法目的の再確認が必要

個人データ処理とは	検索できるよう体系的に構成された[1]個人情報（個人データ）に対する操作の体系的実施[2]（データ処理）。特に、操作の体系的実施によって個人に対する評価・決定[3]を行うこと、すなわち「データによる個人の選別」【☞p5 ①】を伴う処理。

法目的の理論化と立法が必要に

詳細は p4 へ

Then 課題　めざす未来と現行法のギャップ、どう解消する？

医療健康データ、分析のための二次利用[4]ルール	自動運転システム、映りこむ人の映像の扱い	教育データ、個別最適化選別アルゴリズムの適切性
		
Health Care Data	Moblity Data	Educational Data
統計量に集計して分析するだけでも本人同意が必要か？	処理対象としないのに本人拒否の機会が必要か？	現行の個人情報保護法を遵守すれば足りるのか？
統制された非選別利用	個人データ処理中心の規律	評価・決定の適切性確保

詳細は p6 へ

Logic 理論　法１条の「個人の権利利益」とは何か、理論的基礎を確立する。

1　個人データ保護の「決定指向」利益モデル[5]

個人データ処理による個人に対する評価・決定の適切性確保こそが、法が保護する「個人の権利利益」の中核的要素であり、個人データは、評価の目的に「関連する」情報のみから構成されなければならない（データ品質の「関連性」原則【☞p4 ②】）。安全管理や提供制限などのルールは、それを確保するための手段。

2　自己情報コントロール権ではなく、情報的他律からの自由

財産権的モデルの本人同意原則から脱却し、「決定指向」利益モデルに原点回帰する。本人が自己の情報の流れを自己で決定するということではなく、個人データ処理に基づく他者による評価・決定が本人の自己決定を阻害し得ることに対して本人が防御する権利であるということ。

詳細は p8 へ

Law 立法　理論に基づいた立法的解決へ。

3　「医療仮名加工情報」制度の創設

「統制された非選別利用」【☞p10 ③】を前提に、医療分野に限定して、仮名加工情報[6]の提供制限を緩和する。データによる個人の選別を伴わない「非選別利用」を条件とし、提供の範囲を限定する「統制」を法定することにより、個人の権利利益を害さない範囲で、医療分野での仮名加工情報を用いたデータ分析を促進する。

4　個人情報保護法、次の３年ごと見直しに向けて

公的部門では「個人情報ファイル」、民間部門では「個人情報データベース等」（個人データ）を中心とした規律であることを再確認し、個人データ処理（特に「データによる個人の選別」を伴う処理）の適切性確保のため、OECD 8 原則[7]が求めるデータ品質の「関連性」原則を保障する規律を個人情報保護法に組み込む。

詳細は p10 へ

Now
現状

個人情報保護、何を保護するのか見失っている。

- 「情報」の保護ではなく、個人データ処理からの「個人」の保護
- 「個人データ処理」を中心とした、法目的の再確認が必要

個人データ処理とは	検索できるよう体系的に構成された[1]個人情報（個人データ）に対する操作の体系的実施[2]（データ処理）。特に、操作の体系的実施によって個人に対する評価・決定[3]を行うこと、すなわち「データによる個人の選別」【☞p5 ①】を伴う処理。

法目的の理論化と立法が必要に

詳細は ⏩p4 へ

[1] 検索できるよう体系的に構成された

個人情報保護法は、個人情報の集合物であってそれぞれの個人情報を「検索することができるように体系的に構成したもの」を「個人情報ファイル」又は「個人情報データベース等」と呼び、その検索される一個の個人情報を「個人データ」と呼んでいます。「検索」とは「引き出す」の意（英語では retrieve に相当）であり、何らかの識別用の項目（氏名や番号）で一つひとつが取り出せるようになっている状態をいいます。つまり、複数の個人データに対してデータ処理（操作の体系的実施）ができる状態になっていることを指しています。

[2] 操作の体系的実施

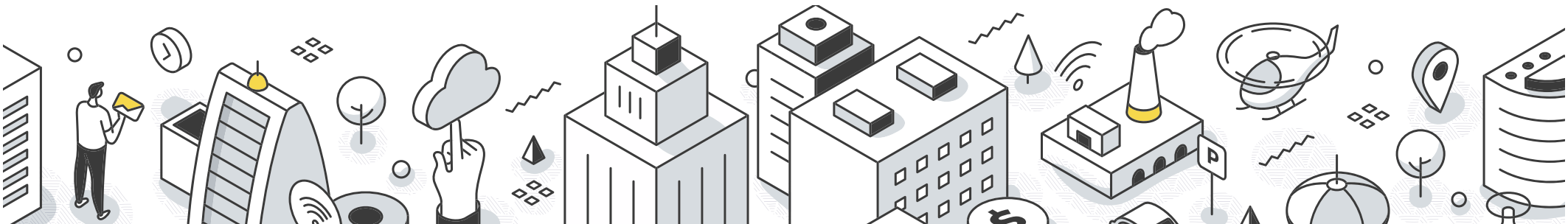
1974 年に制定された国際規格 ISO 2382-1 の日本版である JIS X 0001「情報処理用語――基本用語」は、「データ処理」を「データに対して行われる操作の体系的実施」と定義しています。当時のコンピュータの使い方は、データレコードのリストに繰り返し同じ操作を実施するものでした。同じ時期に欧米諸国で始まった個人データ保護の法制度は、元々はそのような処理を前提としていました。

[3] 個人に対する評価・決定

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何らかの決定をすること。統計量への集計の過程で一時的に各個人の評価データが生成されるに過ぎない場合のように、データ上の評価のみ行なって個人に対する決定に用いない場合は、これに該当しません。なお、ここでいう「決定」は、GDPR 22 条の「自動決定」（automated individual decision-making）とは異なるもので、評価結果から個人に対する「決定」の間に人の判断を挟む場合も該当しますし、「重大な影響を及ぼす」（significantly affects）場合に限られないものです。いかなる目的であれ、人を A グループと B グループに仕分けることが該当します。

☞①「データによる個人の選別」とは、個人に対する評価・決定[3]の体系的実施[2]。

「選別」とは、Aグループと Bグループに仕分けること。個人に対する評価・決定を体系的に実施すると、限られたデータによる画一的な判断をもたらし、「関連性」のないデータを用いると、統計的差別を生むことがあります。



Logic
理論

法１条の「個人の権利利益」とは何か、理論的基礎を確立する。

1 個人データ保護の「決定指向」利益モデル[5]

個人データ処理による個人に対する評価・決定の適切性確保こそが、法が保護する「個人の権利利益」の中核的要素であり、個人データは、評価の目的に「関連する」情報のみから構成されなければならない（データ品質の「関連性」原則【☞p4 ②】）。安全管理や提供制限などのルールは、それを確保するための手段。

1. 本章の概要
2. 日本法の法目的についての政府見解と学説
   (1) 「個人の権利利益」とは何か
   (2) 疑問視する指摘
   (3) プライバシー保護法ではないということ
   (4) 「データ保護」であるということ
   (5) さらなる疑問視
   (6) プライバシーとは別の独自の法理
   (7) 「個人情報を保護する」とは規定していない
   (8) 何を拠り所とするか
3. 「データ保護」とは何か
   (1) OECDガイドライン制定までの経緯
   (2) OECDガイドラインとCoE条約108号の異同
   (3) 「プライバシー」の語が用いられた経緯
   (4) 「data protection」の起源
4. 意思決定指向利益モデルと関連性の原則
   (1) Bingの説明
   (2) 日本法での理解
   (3) Bing以外による説明
5. 小括

Then
課題

めざす未来と現行法のギャップ、どう解消する？

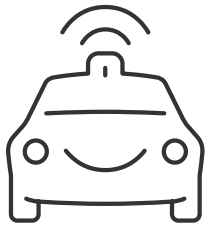
医療健康データ、分析のための二次利用[4]ルール

Health Care Data

統計量に集計して分析するだけでも本人同意が必要か？

統制された非選別利用

自動運転システム、映りこむ人の映像の扱い



Moblity Data

処理対象としないのに本人拒否の機会が必要か？

個人データ処理中心の規律

教育データ、個別最適化選別アルゴリズムの適切性

Educational Data

現行の個人情報保護法を遵守すれば足りるのか？

評価・決定の適切性確保

詳細は p6 へ

本来の法目的

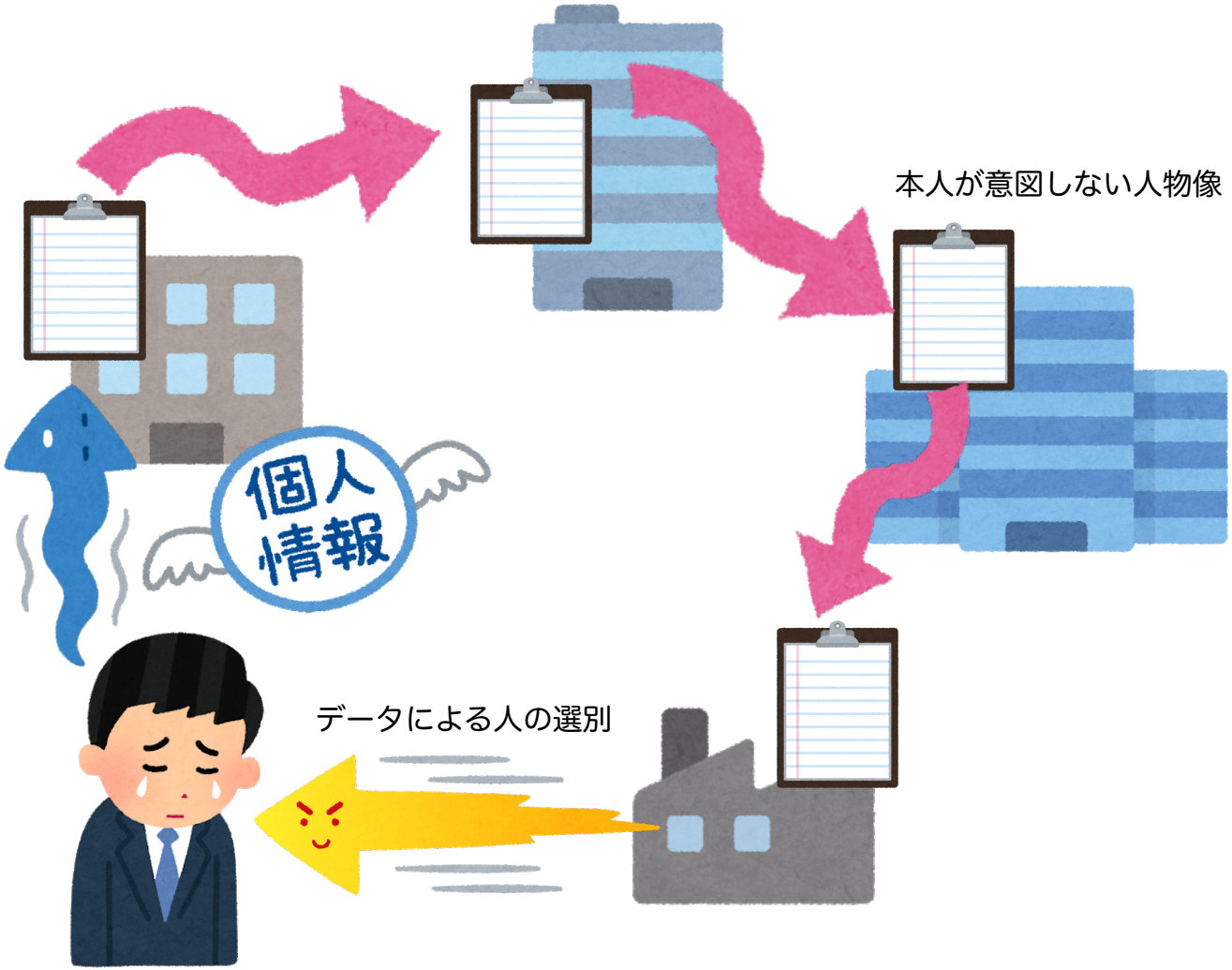
- データ保護が保護する核心的利益は
  個人データ処理による個人に対する評価・決定の適切性確保の利益
  - データ処理とは、データに対して行われる操作の体系的実施
  - 個人に対する評価・決定とは、各個人に対して当該個人の個人データを基に何らかの評価をしてその評価に基づく何らかの決定をすること
- 決定の「適切性確保」とは
  個人に対する決定が、その決定の目的に照らして、正確であり（広義の正確性）公平（fairness）なものとなることを要求するもの
  - 個人データの構成及び内容が適切であること（データの適切性）
    評価・決定の計算式及び判断基準（決定のロジック）が適切であること（ロジックの適切性）
  - 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）」でなければならず（関連性の原則）、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。
  - 「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とパラレルであり、非差別原則の実現にある
- 目的外利用禁止、提供制限等はその実現手段としての政策的規制にすぎない

取得ではなく決定

- プロファイリングの話でも
  - 推知が問題なのではなく、決定が問題
- つまり、「入力ではなく出力」の問題

みんな逆から見ていた

- どこから規制対象にするかは政策的な問題



生成AIへの当てはめ

- EDPB ChatGPT Taskforceの作業報告書（先月）
  - 「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
  - 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
- 個情法3年ごと見直し
  - 第289回個人情報保護委員会（６月12日）有識者ヒアリング
    https://www.ppc.go.jp/aboutus/minutes/2024/20240612/
    - 資料1-2 「個人情報保護法３年ごと見直し令和６年に対する意見」
    - 「1.3 要配慮個人情報の取得」で生成AIについて言及
  - 個人情報ではなく「個人データ（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）」の規律に変更するべき

著作権の場合との類似性

- 非享受目的の利用は許される（著作権の制限）
  - 34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）
- 個人情報に関する非享受利用？
  - 個人に対する決定に用いない個人データの利用（統計量への集計）
    - 本人に影響が及ばないということ
- 入力は問題ではなく出力が問題
- なぜ許されるか
  - 公益アプローチ？　権利間調整？ 内在的制約？
- 続きはこの後の上野先生と対談で