個人情報保護法におけるデータと個人の対応関係といくつかのプライバシー保護の数理的定義

紀伊 真昇[1,a)]　高橋 克巳[1]　藤村 明子[1]　荒岡 草馬[1]　岡村 優希[1]　三浦 尭之[1]　津川 天祐[1]

概要：個人情報保護法における個人情報や匿名加工情報の定義では、「特定の個人を識別することが出来る」情報、という概念が非常に重要である。どのような情報ならば「特定の個人を識別することが出来る」かは、（あえて）解釈の余地を残してあるため、判断が難しい。一方でプライバシー保護技術の研究では現実を模した仮定を置き、「安全性」を明確に判断する基準を作ろうとする。このように両者では認識の枠組みが大きく異なる。本稿の目的は個人情報保護法とプライバシー保護技術における認識の枠組みの「中間点」を目指して、新しい認識の枠組みを作ることである。本稿前半では「特定の個人を識別することが出来る」についての議論のために必要な概念を分別し、注意点を述べ、その論点を絞る。本稿後半では論点の中でも難しい「加工前後の関係の強弱」の解釈として、加工後データから加工前データを逆推測する難しさによる解釈を提案する。さらに幾つかの安全性の数理的定義がこの解釈と整合することを指摘する。データ間の関係の強弱の解釈とは考えられない数理的定義の例も挙げた。本稿前半で記述する認識の枠組みは個人情報保護法の専門家とプライバシー保護技術の専門家がともに議論する際の大きな助けとなる、と期待している。

キーワード：個人情報保護法、統計情報、匿名加工情報、識別可能性

Relationship between data and individuals under the Act on the Protection of Personal Information and several mathematical definitions of privacy protection

Masanobu Kii[1,a)]　Katsumi Takahashi[1]　Akiko Fujimura[1]　Soma Araoka[1]　Yuki Okamura[1]
Takayuki Miura[1]　Hiromasa Tsugawa[1]

Abstract: In the definition of personal information and anonymized processed information under the Act on the Protection of Personal Information, the concept of “information that can distinguish a specific individual” is extremely important. What constitutes “information that can distinguish a specific individual” is intentionally left open to interpretation, making it difficult to determine. On the other hand, research on privacy protection technology establishes assumptions based on real-world scenarios and seeks to create clear criteria for determining “safety.” Thus, the two approaches have fundamentally different frameworks of understanding.The purpose of this paper is to create a new framework of understanding that aims to find a middle ground between the Act on the Protection of Personal Information and privacy protection technology. In the first half of this paper, we will distinguish the concepts necessary for discussing “distinguishable,” point out points to note, and narrow down the issues.In the latter half, we propose an interpretation of the difficult issue of “the strength of the relationship before and after processing” based on the difficulty of inferring the original data from the processed data. We also point out that several mathematical definitions of security are consistent with this interpretation. We also provide examples of mathematical definitions that cannot be interpreted as the strength of the relationship between data.We expect that the conceptual framework described in the first half of this paper will serve as a valuable tool for discussions between experts in Act on the Protection of Personal Information and experts in privacy protection technology.

Keywords: Act on the Protection of Personal Information, statistical information, anonymized data, identifiability

1. 導入

本稿は個人情報保護法で用いられる「特定の個人を識別することができる」という概念を扱う。この概念は短く「個人識別性」とも呼ばれることが多い。以下に引用する個人情報保護法 第二条 [7] のとおり、個人識別性は個人情報を特徴づける重要な概念である。強調は筆者による。

> この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
>
> 一　当該情報に含まれる氏名、生年月日その他の記述等（[筆者注：括弧内略]）により**特定の個人を識別することができる**もの（他の情報と容易に照合することができ、それにより**特定の個人を識別することができる**こととなるものを含む。）
>
> 二　個人識別符号が含まれるもの

また個人識別性は匿名加工情報の定義でも重要な条件である。個人識別性は「個人情報の保護に関する法律についてのガイドライン」に関するQ＆A [8] では次のように説明されている。

> **Q1-1.** 「特定の個人を識別することができる」とは、どのような意味ですか。
>
> **A1-1.** 「特定の個人を識別することができる」とは、社会通念上、一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認めるに至ることができることをいいます。

したがって個人識別性の判断は、判断する者によって変わる。これは事前に想定しきれない個々の場面での事情を判断者が汲むことを許すために、一般論が保持するべき解釈の余地である。

一方でプライバシー保護技術の研究では、研究のゴールである「安全なデータ」を数理的に、これ以上なく明確に定義する。これがなければ技術の良し悪しを判断できないからである。つまり、プライバシー保護技術の研究は現実の状況を理想化した仮定（モデル）を考え、「安全なデータ」を明確に定義することから始まる。また、研究者は考えている仮定は現実の多くの場面でも通用するし、通用するなら現実でも厳密な「安全なデータ」の定義が有意義であると信じている。

このように個人情報保護法とプライバシー保護技術の間には、個人識別性の判断の不確定性・解釈の余地について大きな溝がある。こうした状況で両者の間で個人情報保護について円滑に議論をするための認識の枠組みを作るのが本稿の目的である。そのために本稿では両者の翻訳をするのではなく、両者の中間点を探す。個人識別性の解釈の余地を出来るだけそのまま維持しながら、無用な曖昧さを出来るだけ減らす。

本稿の前半（2 節、3 節）では、データ／情報の個人識別性の考え方について、議論に不可欠な概念を分析し、分別する。そのなかで解釈の余地が残る点（論点）を三つに絞り込む。特に「加工前後の関係」の捉え方が大きな論点になることが示される。本稿の後半（4 節）では「加工前後の関係」について逆推定可能性に基づく考え方を例示する。さらに幾つかのプライバシー保護の数理的定義が、例示した考え方を数理的に定式化したものと捉えられることを指摘する。このプライバシー保護の数理的定義とはプライバシー保護技術である匿名化および統計的開示制御による保護の強弱を定量的に示すものである。したがって、これらのプライバシー保護の数理的定義については、個人識別性の妥当な解釈の一例として個人情報保護法の体系のなかに立ち位置が得られることになる。

本稿の貢献は以下のようにまとめられる。

- 個人情報保護法における個人識別性に関する議論に不可欠な概念を分析し、整理した。
- データの個人識別性についての論点が三点に絞り込めることを明らかにした。
- 論点の一つである「加工前後の関係」の解釈として、幾つかのプライバシー保護の数理的定義を利用できる可能性を示し、法と技術を接続する視点を提供した。
- データ間の関係の強弱の解釈とは考えられない数理的定義の例も挙げた。

本稿全体で提示する認識の枠組みが、個人情報保護法の専門家にとっては技術的な安全性指標の目的を理解しやすくなり、プライバシー保護技術の専門家にとっては法的要求を定量的評価へと翻訳する際の指針を得られる、両者の間の架け橋になると期待している。

1.1 個人情報保護法とプライバシー保護技術の考え方

個人情報保護法とプライバシー保護技術の議論をする際に共有されるイメージとして、概念図 1 を文献 [6] を参考に描いた。

個人情報保護法の議論では、「加工前データ」として個人データ（個人識別情報を含んでいる）を、「加工後データ」として文字通り加工された個人データを設定し、それぞれの個人識別性を考える。一方でプライバシー保護技術の議論では、「加工前データ」として何らかの機微な情報が含まれているとする。個人を識別できる情報が入っていなくても、個人の秘密ではなく営業上の秘密が含まれているとしてもよい。そして「加工後データ」にその加工前に含まれていた機微情報が含まれているかどうかを考える。

両者の違いが大きく出る加工処理の例として、入力を完全に無視して生存する個人の名前を出力するプログラムが

[1] NTT 社会情報研究所
NTT Social Informatics Laboratories
[a)] masanobu.kii@ntt.com

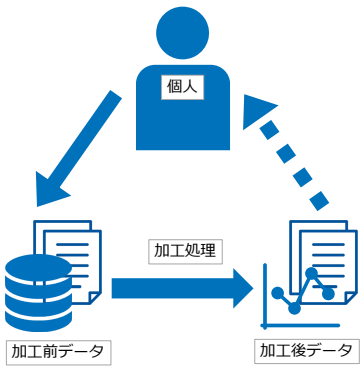

図 1 個人、加工前データ、加工後データの図。個人情報保護法とプライバシー保護技術で共通していると思われるイメージ。しかしそれぞれの分野で詳しい内容は異なる。

考えられる。この出力は個人情報保護法の文脈では問題視されるが、プライバシー保護技術の文脈では安全と判断される。また、個人情報保護法では公開情報も個人情報だが、プライバシー保護技術の文脈では公開情報を利用しても問題ないとされる。これはプライバシー保護技術が私秘情報の公開／漏洩だけを問題にするためである。

2. 概念と構造の分析

この節では、個人情報保護法における認識の枠組みとプライバシー保護技術における認識の枠組みの中間点を目指して、新しい認識の枠組みを提案する。

以降では一貫して、データの個人識別性のことを**「特定の個人との対応関係」と表現する**。この表現は統計情報の説明に現れるものである。「個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）」[9] にある統計情報の説明を引用しよう。強調は筆者による。

> 「統計情報」は、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計して得られるデータであり、集団の傾向又は性質などを数量的に把握するものである。したがって、統計情報は、**特定の個人との対応関係**が排斥されている限りにおいては、法における「個人に関する情報」に該当するものではないため、規制の対象外となる。

この文章において「特定の個人との対応関係が排斥されている」は「特定の個人を識別することができない」と同義である。しかし「特定の個人との対応関係」は個人の判断から離れた静的なものの印象が有るため、あえて本稿ではこちらの表現を用いる。

2.6 節に要点をまとめているため、そちらだけ読んでから後の節を読んでも問題ない。

2.1 個人からデータが取得され、それが加工される

まずは基礎的なことを確認する。事業者が個人からデータを取得し、そのデータが加工されて最終的なデータが作られる。事業者はプライバシー保護技術の文脈では単にデータ収集者と呼ばれ、個人情報保護法の文脈では義務を負う（可能性がある）ものである。個人と最終的なデータが一対一に対応することもあれば、複数人のデータが一つのデータに関与していたり、一人のデータが複数のデータに関与することも多い。

2.2 生存する個人に関する情報だけが考慮される

導入で引用した個人情報保護法における定義のとおり、個人情報は「生存する個人に関する情報」に限定されている。このため個人情報保護法の法目的は生存する「個人の権利利益を保護すること」[*1]であり、架空の個人や死者の「権利利益」は考慮されない、と理解されている。したがって本稿が記述する「特定の個人との対応関係」を取り巻く概念と構造には、架空の個人、死者、無生物の情報のようなものは現れない。

この原則から即座に、生存する個人が関わるか否かを考慮しない安全性の定義は、個人情報保護法の主目的とは相容れないことが分かる。例えば一個人のプロフィールらしきものをランダムに作っても、このプロフィールが生存する個人の情報と一致すると分からない限り、これは誰の権利利益も害していないはずである。

2.3 直接個人特定情報は生存する具体的な個人を直接に識別できる

「何が個人識別情報なのか」という議論は本稿では扱いきれないほど多様な意見があるため、また本稿では個人識別情報の概念に独特の分析を加えるため、本稿に限って使う用語を導入する。

本稿での用語「直接個人特定情報」は、生存する具体的な個人を単独で直接に特定できる情報のことである。おおよそ「個人識別情報 (Personally Identifiable Information, PII)」という言葉と同義と考えるか、個人情報の定義にある「特定の個人を識別することができる」記述と「個人識別符号」を合わせたものと考えて差し支えない。なお「特定の個人を識別することができる」の意味については導入で引用した Q&A も確認いただきたい。

幾つか注意点を述べる。直接個人特定情報はそれだけで確実に個人を特定出来ると信じられる情報であり、直接個人特定情報の一部が削除されたものや加工されたものは直接個人特定情報ではない。なお「特定」と「識別」の違いは [6] では次のように説明されている。

> ここで「特定」とは、「ある情報が誰の情報であるかが分かること」である。一方、「識別」とは、「ある情報が誰か一人の情報であることが分かる

[*1] 法 [7] 第一条

こと」(ある情報が誰の情報であるかが分かるかは別にして、ある人の情報と別の人の情報を区別できること) である。

プライバシー保護技術のいくつかの教科書でも同様の説明がなされている。本稿でもこの定義に準じる。また、「直接に」特定できるとは、その情報が「具体的な個人を特定できる」と信じられる理由が、別の情報が「具体的な個人を特定できる」と信じられていることに帰着できない、という意味である。この点については詳しく具体例を挙げよう。

「個人識別情報」の定義は社会通念に依存するものであり、確定することはない。個人情報保護法の実運用上は事実とは一致しない感情でも考慮される可能性が有る。

2.3.1 直接個人特定情報の具体例

氏名やニックネームは「本人がそう名乗っているから」「そう呼べば本人が応えるから」「みんながその人をそう呼んでいるから」個人を識別できると信じられている。住所、電話番号、メールアドレスなどの連絡先情報は「連絡すればその人だけに繋がるから」個人を識別できると信じられている。生体識別情報も「そのような顔／指紋／声／DNA の人は一人しかいないから」個人を識別できると信じられている。政府が発行している「個人識別符号」の大部分も、「確実に本人確認して本人に直接交付したから」個人を識別できると信じられている。

一方で、組織内で使われる会員番号やシステム内部での処理用 ID などは「会員番号／処理 ID と直接個人特定情報を対応させるデータベースがあるから」個人を識別できると信じられている。こうした情報は別の情報が存在しなければ、個人を識別できていると信じられないため、直接個人特定情報ではない。

2.3.2 直接個人特定情報と個人の分離

本稿では明確に、直接個人特定情報と個人は分離して扱うことにする。その理由は二つ有る。

１つ目の理由は、実際に直接個人特定情報（一般に個人識別情報）と個人は全く別物だからである。「紀伊 真昇」は筆頭著者のことを指す直接個人特定情報だが、筆者ではない。名前は論文を書かない。これはただの文字列である。

２つ目の理由は、そう考えないと一つの情報と対応関係に有る個人の人数をうまく数えられないからである。本稿の後半では「このデータは何人の個人識別情報が入っているのか」を考え、かつ法と技術の接続を図る。もし仮に言葉通り「個人識別情報と一個人は一対一に対応する」と考えると、一個人の個人識別情報があるデータに多数入っているとき、そのデータは多数の個人に関するものだから「特定の個人との対応関係」がない、という結論になってしまう。

2.4 三種類のデータ間の対応関係を考える

この節で導入する「データ間の対応関係」は、個人情報保護法のなかの容易照合可能性と、加工前後のデータの近さをまとめた概念である。この定義はあまり見かけられないもので、多くの人にとって新しいものに見えるだろう。なお、本稿での「対応関係」は一対一対応ではなく、一体多、多対多、多対一も含む。数学で考えられる「対応」に近い。

被包含関係　は、データ A がデータ B に含まれている（あるいは等しい)、というもの。機械的に文字列を比較することで有無を判断できる。

リンケージ関係　は、データ A からデータ B へリンクが貼られている、というものである。容易識別可能性のような、内部用セッション ID を介して二つのデータが双方向リンクされている、という状況もこれに当てはまる。このような対応関係も機械的に有無を判断できる。

加工前後の関係　は、あるデータ A を加工・処理することで別のデータ B が得られた**可能性がある**、というものである。この関係があるかどうかは機械的に判定することは出来ず、来歴によっても定まらない。

いずれもデータ A からデータ B に向かって関係を持つ（非対称）だと考える。双方向に関係を持っている可能性はある。「関係を遡る」というときは関係を逆方向にたどることを指す。

加工前後の関係は他２つと異なり強弱の概念もあり、こちらは次節で扱う。

2.5 加工前後の関係の有無／強弱は不明瞭であり加工の詳細に依る

データ間の対応関係のうち、加工前後の関係の強さ、言い換えれば加工後データに加工前データがどの程度色濃く反映されているかは、通常は不明瞭である。判断するには処理の具体的内容を見なければわからないし、処理の具体的内容を見ても万人が影響の程度を同様に判断するとは限らない。本稿ではその不明瞭さ (fuzzy-ness) をそのまま扱うことにする。以下ではこのような加工前後の関係の強さには強弱があることを例を通して確認する。後の 4 節ではこの加工前後の関係の強さについてより深く考察する。

2.5.1 対応関係の強弱の例

例えば加工後のデータから加工前のデータが正確に復元できれば、対応関係は非常に強い。一方でどんな入力に対しても必ず同じデータが出力される処理を通すと、加工前後での対応関係はなくなる。あるいは入力と独立に、ランダムに出力が決まる処理でも、加工の前後で対応関係がない。同じ理由でデータのほとんど全部が削除されている場合には、加工前後で対応関係がない。

一般的な統計情報は少なくとも対応関係が非常に弱いとみなされるが、その程度は場合による。例えば、データベースから作られた、全属性についての集計表は、集計表と言ってもデータベース全体を完全に復元できる。一つの

数値についても数学的には平均値を定義でき、それは元の数値そのものである。他にも過学習してしまった機械学習モデルから個人を識別できる情報が取り出される危険性があることはよく知られている。こうした例を見ると、それぞれの情報と「特定の個人との対応関係が排斥されている」かどうかは通常、不明瞭であることがわかる。

本稿では一貫性を持たせるために、被包含関係とリンケージ関係にも強さがあるとする。そして被包含関係とリンケージ関係はどれも**最強の関係**であり、常に「加工前後の関係」より強いか同じ強さである、として扱う。これは被包含関係とリンケージ関係が機械的に有無を判断でき、曖昧さが無いためである。

2.5.2　加工前後の関係の強さは比較できることがある

加工前後の関係の強さには強弱があり、比較できない場合もあるが、比較できる場合もある。例えば、数値 X を含む 3 個の数値の平均と、数値 X を含む 10 個の数値の平均で比較すれば、数値 X との関係が強いのは前者であると考えられる。また、数値 X そのものを含むデータと X の関係は最強であるし、X と全く無関係に選ばれたデータは X との関係が最弱である。

2.5.3　データ間の対応関係の合成

被包含関係とリンケージ関係について、どちらも「最強」として強弱を定めることで、これら関係を「合成」した関係の強弱が考えられる。このアイデアについてはファジー関係 (fuzzy relation) の定義が参考になるだろう。

2.6　本節のまとめ

本節の要点は以下の 5 つにまとめられる。これらの関係を図 2 に図示した。

(i)　個人からデータを取得され、それが加工される
(ii)　生存する個人に関する情報だけが考慮される
(iii)　「直接個人特定情報」とは生存する具体的な個人を単独で直接に特定できる情報のことである
(iv)　データ間の対応関係には被包含関係、リンケージ関係、加工前後の関係の三種類がある
　(a)　被包含関係は、一方が他方に含まれているという関係であり、この有無は機械的に判定できる
　(b)　リンケージ関係は、一方から他方へ明示的なリンクがあるという関係であり、この有無は機械的に判定できる
　(c)　加工前後の関係は、一方を加工処理することで他方が生成された可能性があるという関係であり、この有無は明確には決まらない
(v)　加工前後の関係の強弱は不明瞭で、加工の詳細に依る
　(a)　加工前後の関係の強弱は比較できることがある
　(b)　データ間の対応関係の「合成」とその強弱を定義できる

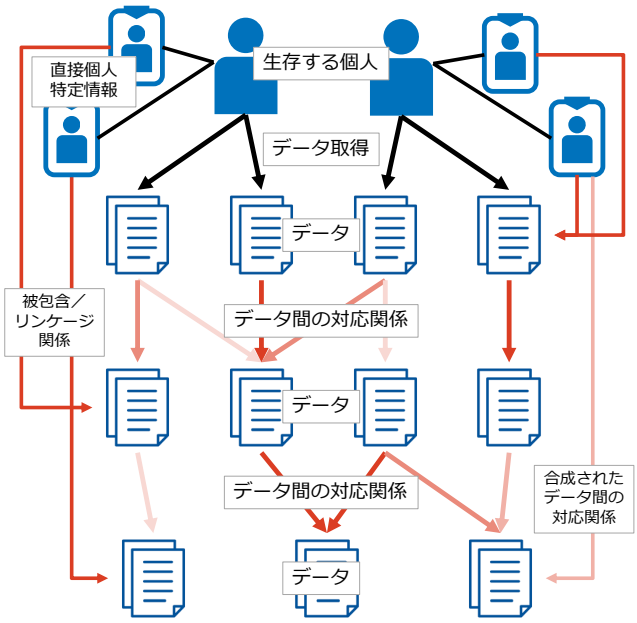

図 2　2.6 節の図示。個人、直接個人特定情報、データとデータ間の対応関係を示している。データ間の対応関係には被包含関係、リンケージ関係、加工前後の関係の三種類がある。一つの直接個人特定情報は一個人を指示している。一方で一個人には複数のデータ、直接個人特定情報が対応しうる。

3.　データと個人の対応関係

以上の構造を用いると、データと「特定の個人との対応関係」、すなわち個人識別性が詳しく述べられる。個人と対応関係があるデータとは、直接個人特定情報との対応関係があるデータのことであり、次のように分類できる。

(A)　**直接個人特定情報**を包含しているデータ
(B)　十分強いデータ間の対応関係を遡っていくと**直接個人特定情報**へ到達できるデータ

2.4 節で述べた通り、データ間の対応関係には被包含関係」「リンケージ関係」「加工前後の関係」があり、「被包含関係」と「リンケージ関係」は常に「加工前後の関係」より強いもの（最強のもの）として扱っている。

「十分強いデータ間の対応関係を遡っていく」という部分は対応関係を何個も遡ることを念頭に置いているが、データ間の対応関係の「合成」(2.5.3 節）を定義すれば、データと直接個人特定情報の直接の関係について強弱を確かめることでも判断できる。

3.1　個人情報の定義との対応

当然に期待される通り、個人と明白な対応関係があるデータが個人情報である。個人情報は被包含関係とリンケージ関係だけを遡って直接個人特定情報に到達できる

データである。曖昧さがある加工前後の関係は考えない。

なお、あるデータが個人情報であるかどうかと、実際にそのデータがその直接個人特定情報で指示される個人から収集されたデータに対応関係があるかどうかは、関係がない。それが事実でなくとも、事実でないと知らない第三者が事実として扱ってしまう以上は、個人との対応関係があると見なさなくてはならない。これは直接個人特定情報で指示される個人の権利利益を、個人情報を参照した事業者等から守るために必要である。

3.2 「特定の個人との対応関係が排斥されている」とは何か

以上で導入した概念を用いて「特定の個人との対応関係が排斥されて」いない、すなわち個人識別性が有るデータを定式化すれば、次のようになる。あるデータが一つ以上の直接個人特定情報との間に十分に強いデータ間の対応関係を持っており、さらにそれら直接個人特定情報が全て 1 個人のものであるとき、このデータはその個人「との対応関係が排斥されて」いないデータである。以降ではこれを短く「1 個人に対応するデータ」という。ここでは加工前後の関係、すなわち一方を加工処理することで他方が生成された可能性があるという関係も考える。そのため個人情報ではない「特定の個人との対応関係が排斥されて」いないデータがありうる。

逆に、あるデータと対応関係にある個人が 1 人ではなく、0 人もしくは多数いたとすれば、そのデータは一般的な代表統計値と同様に「特定の個人との対応関係が排斥されている」と考えられる。したがってデータに対応する個人が 0 人であることを統計情報／安全性の定義とすることも、一定数以上いることを統計情報／安全性の定義とすることもできる。

ここで、あるデータが個人情報であるかどうかは来歴によって決まらないことを注意しておく。例えば記入してもらった無記名のアンケート用紙を個人から直接受け取ったとしても、そのアンケート用紙は個人情報ではない。無記名の回答が「あの人が書いたんじゃないか」と分かったときには、そのときになって個人情報になる。サードパーティクッキーなども同様で、個人情報ではなかった情報が後に直接個人特定情報との関係が生まれ、個人識別性をもつ可能性がある。

この定式化には当然ながら注意が必要である。個人情報保護法を運用する際には、仮に事実とは異なるとしても「このデータは私のものだと思う」という人がいれば考慮される可能性が有る。しかしこうしたプライバシー感情を考慮するとプライバシー保護技術の議論と接続できないため、本稿ではあえて無視する。

3.3 何が不確定なのか

以上の議論が妥当だとすれば、あるデータと「特定の個人との対応関係」があるか否か、あるデータに個人識別性があるか否かを判断するには、次の三点を特定すれば判断の根拠を明示できると分かる。

(S-1) 考えるべき直接個人特定情報は何か
(S-2) 加工前後の関係をどのように捉え、考えるか
(S-3) 加工前後の関係はいつあるのか、あるいはどの程度なら無視されるのか

プライバシー保護技術の運用で言えば、(S-2) はプライバシー保護の数理的定義や数値指標を選択することにあたり、(S-3) は安全／危険な状態を分ける数値指標の閾値を決めることにあたる。

4. 加工前後の関係といくつかのプライバシー保護の数理的定義

ここまでで論点を 3.3 にある 3 点にまとめることができた。それでも加工前後の関係、すなわち一方を加工処理することで他方が生成された可能性があるという関係をどのように考えるかは難しい。「可能性がある」といえば、どんなものでも多少は、何らかの処理を通じて可能性があるように思えるからである。十分に長いランダムなデータがあれば、適当な処理方法を選べば、そこからどんなデータでも「読み出せる」のである。そのため社会通念とも整合性が有る合理的な考え方で、加工前後の関係の強弱を評価しなくてはならない。

この節では加工前後の関係について逆推測可能性に基づく考え方を例示する。さらに幾つかのプライバシー保護の数理的定義が、例示した考え方を数理的に定式化したものと捉えられることを指摘する。このプライバシー保護の数理的定義とはプライバシー保護技術である匿名化および統計的開示制御による保護の強弱を定量的に示すものである。したがって、これらのプライバシー保護の数理的定義については、データと「特定の個人との対応関係」の妥当な解釈の一例として個人情報保護法の体系のなかに立ち位置が得られることになる。

4.1 記号と用語

いくつかの記号と用語を導入する。考える加工処理を固定して、一貫して加工前データの候補を $x \in \mathbb{X}$、加工後データを $y \in \mathbb{Y}$ と表記することにする。

また、加工前データの候補 x と加工後データ y の間にある関係の強さを $\mu(x, y)$ と書くことにする。これはただ一々日本語で書くと煩雑なので記号にしたというだけであり、内容が定まっていない状況は変わっていない。本稿全体で「$\mu(x, y)$」を機械的に「加工前データの候補……関係の強さ」と置き換えても意味は変わらない。

4.2 加工後データから加工前データへの逆推測可能性

既に定義した三種類のデータ間の対応関係を抽象化してみると、いずれも何らかの情報を共有・伝達している対応関係だと言えるだろう。この直観をもとにすれば、加工後データ y から加工前データ x の内容を推測することの易しさ／難しさのようなものを、加工前後の関係の強弱 $\mu(x, y)$ とするのは自然な発想だろう。このアイデアは 2.5.1 節で挙げた加工前後の関係の強弱の例と一貫している。

「加工後データ y から加工前データ x の内容を推定することの易しさ／難しさ」、短く言えば逆推測可能性（本稿でしか使わない言葉である）は様々な分野で様々に定式化されている。それぞれの分野での考え方を簡潔に紹介する。なお、ここでは加工前、加工後をそれぞれ入力、出力と表現する。

情報理論　主に離散値の推測を考える。出力 y を知ったときの入力 x に残る不確定さ、すなわち x としてあり得る値の候補それぞれの尤もらしさ・蓋然性を、確率分布を使って定式化する。逆推測可能性の指標の例には相互情報量など。

統計的推定理論　主に連続値の推測を考える。入出力の対応関係について確率的モデルを設定して推測を行い、推定の誤差や精度によって逆推測可能性を評価する。逆推測可能性の指標の例は Fisher 情報量や Cramér–Rao 下限など。

計算量理論　逆計算に必要な計算資源（計算時間や使用メモリ）の大きさによって逆推測可能性を評価する。逆推測可能性の難しさの定義として一方向性関数など。

暗号理論　出力から入力を推測しようとする「攻撃者」を想定し、「攻撃者」の推測能力を、実際に推測できるかどうかをテストするゲーム、実験を通じて定式化する。想定した条件下での推測の成功確率によって逆推測可能性を評価する。逆推測可能性の難しさの定義として識別不可能性、ゼロ知識性など。

機械学習　観測された出力や中間表現から入力の復元する機械学習モデルを主に研究し、実際に復元を試みたときの誤差や正答率によって逆推測可能性を評価する。

これらの考え方に基づくプライバシー保護の数理的定義がいくつか提案されている。例えばプライバシー保護技術の研究者の間でデファクトスタンダードとなっている差分プライバシーは、情報理論を通じて逆推測可能性を制約することが知られている [2, 3]。

4.3 プライバシー保護の数理的定義との対応

3 節の最後で、データに対応する個人が 1 人でなければそのデータは「特定の個人との対応関係」がない、すなわち個人識別性がない、という考え方を述べた。これを元にいくつかのプライバシー保護の数理的定義を分類してみる。

「データに対応する個人が 1 人でない」というアイデアを正確に述べると二つに分けられるので、それぞれについて例をあげる。k は自由に選べる 1 以上の整数である。

対応する個人が 0 人　あるデータがどの直接個人特定情報との間にも一定以上に強いデータ間の対応関係を持っていない

- 加工後データと加工前データの相互情報量や maximum information leakage を考えるもの
- 加工後データから推定される加工前データと実際の加工前データの距離を考えるもの
- 差分プライバシー、及びその派生物

対応する個人が k 人以上　あるデータが一つ以上の直接個人特定情報との間に**十分かつ同程度に**強いデータ間の対応関係を持っていて、かつそれらがに対応する個人が k 人以上である

- k-concealment [4]、Plausible deniability[1] も、直接は逆推測可能性を考えていないものの、こちらに分類できる

その他にも、プライバシー保護の数理的定義のサーベイ論文 [5] において “information gain/loss”, “accuracy/precision”, “error” に基づくもの、と分類されているものも以下の二つに分類できる可能性がある。

4.4 $\mu(x, y)$ の定式化とは考えられない安全性の定義

少なくとも加工前後のデータの両方をその定義で考慮していないようなプライバシー保護の数理的定義は、加工前後の関係の強さ $\mu(x, y)$ とは考えられないだろう。そのような例としては、k 匿名性 (k-anonymity) やその強化版である ℓ-diversity, t-closeness がある。この他にもプライバシー保護の数理的定義のサーベイ論文 [5] で “data similarity” に基づくと分類されている 15 個の定義は、いずれも加工前のデータベースを考慮していない。

更にいえば、任意の k に対して、出力が k 匿名性を満たすような可逆な加工処理が存在する。この場合には k と関係なく加工前後の関係の強さが最強になってしまう。具体的には入力データベースの各レコードを k 個に複製し重複させる加工処理を考えれば良い。同様に複製やダミーレコードを用いることで、ℓ-diversity と t-closeness を満たす可逆な加工処理が考えられる。

5. 結論

本稿では、データの個人識別性に関わる概念を法と技術の両方の視点から整理した。前半で構成した概念体系（生データ、非・生データ、直接個人特定情報、データ間の対応関係の強弱）は、差分プライバシーや k-concealment のような数理的定義と接続可能な構造を提供する。また、以前から疑問が呈されていた 個人識別性と k 匿名性 の関係についても、前半で示した概念体系が説明を与えることを述べた。このような分析は、個人情報保護法の解釈と技術的

評価を一致させるための土台として機能し得る。今後は、国際的な法制度との比較や、この概念体系を用いた実システムの分析により、本稿の枠組みの実効性を検証することが望まれる。

参考文献

[1] Vincent Bindschaedler, Reza Shokri, and Carl A. Gunter. “Plausible Deniability for Privacy-Preserving Data Synthesis”. Aug. 26, 2017. arXiv: 1708.07975 [cs, stat].

[2] Paul Cuff and Lanqing Yu. “Differential Privacy as a Mutual Information Constraint”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’16. New York, NY, USA: Association for Computing Machinery, Oct. 24, 2016, pp. 43–54. ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978308.

[3] Theshani Nuradha and Ziv Goldfeld. “An Information-Theoretic Characterization of Pufferfish Privacy”. In: *2022 IEEE International Symposium on Information Theory (ISIT)* (June 26, 2022), pp. 2005–2010. DOI: 10.1109/ISIT50566.2022.9834520.

[4] Tamir Tassa, Arnon Mazza, and Aristides Gionis. “K-Concealment: An Alternative Model of k-Type Anonymity”. In: *Trans. Data Privacy* 5.1 (Apr. 1, 2012), pp. 189–222. ISSN: 1888-5063. DOI: 10.5555/2207141.2207142.

[5] Isabel Wagner and David Eckhoff. “Technical Privacy Metrics: A Systematic Survey”. In: *ACM Computing Surveys* 51.3 (3 June 12, 2018), 57:1–57:38. ISSN: 0360-0300. DOI: 10.1145/3168389.

[6] パーソナルデータに関する検討会. **技術検討ワーキンググループ 報告書**. 総務省, Dec. 10, 2013. URL: https://warp.ndl.go.jp/info:ndljp/pid/12251721/www.kantei.go.jp/jp/singi/it2/pd/dai5/gijisidai.html.

[7] **個人情報の保護に関する法律（平成十五年法律第五十七号）**.

[8] 個人情報保護委員会. **「個人情報の保護に関する法律についてのガイドライン」に関する** *Q&A*. July 1, 2025. URL: https://www.ppc.go.jp/personalinfo/faq/APPI_QA/.

[9] 個人情報保護委員会. **個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）**. Oct. 2021. URL: https://www.ppc.go.jp/personalinfo/legal/2009_guidelines_tsusoku/#a2-3.