資料３－２

個人情報保護委員会事務局レポート：

匿 名 加 工 情 報

パーソナルデータの利活用促進と
消費者の信頼性確保の両立に向けて

2017 年 2 月

個人情報保護委員会事務局

目次

【凡例】

「個人情報保護法」・「法」	個人情報の保護に関する法律（平成 15 年法律第 57 号）
「施行令」	個人情報の保護に関する法律施行令（平成 15 年政令第 507 号）
「施行規則」	個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号）
「ガイドライン」	個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）（平成 28 年個人情報保護委員会告示第 9 号）
「通則ガイドライン」	個人情報の保護に関する法律についてのガイドライン（通則編）（平成 28 年個人情報保護委員会告示第 6 号）
「改正法」	個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成 27 年法律第 65 号）

※ なお、特に断りのない限り、本レポートにおいて示す個人情報の保護に関する法律の条番号は、改正法のうち個人情報の保護に関する法律に係る改正が全面的に施行される日時点の条番号を示すものとする。

はじめに

個人情報を含むパーソナルデータの取得・収集・分析・流通が社会経済活動及びイノベーションや経済成長における重要な役割を果たすようになっている。今後、IoT[1]・AI[2]等の普及に伴い、従来よりも更に多くのデータを取得・分析することが可能となっていく中、個人情報を含むパーソナルデータの利活用の環境を整える重要性が増している。

また、国境を越えた情報の流通が加速し、国境を越えて海外へサービス提供を行うことも海外事業者のサービス提供を受けることも容易となる中で、適正な取扱いを確保し利用者の信頼を得ながら、我が国の事業者や関係機関が国内外の様々な個人情報を含むパーソナルデータを活用して多様なサービスを提供できる環境整備が極めて重要である。

匿名加工情報の制度は、このような要請に応えるために創設された制度であり、法律・政令・規則・ガイドラインにより必要最低限の事項については定められている。加えて、認定個人情報保護団体（以下「認定団体」という。）や事業者団体の自主規制等において、取り扱う個人データの性質等に応じた匿名加工情報の具体的な加工基準等が策定されることが期待される。

一方、法令及びガイドラインに加えて、認定団体による匿名加工情報の加工基準や安全管理措置等を含む個人情報保護指針の作成又は事業者団体が自主ルール等の策定を行う際に参考となるような情報を取りまとめることにより、指針等の策定を促し、また個別の事業者や関係団体等が匿名加工情報を作成しようとする場合にも参照いただけるように、個人情報保護委員会事務局レポート（以下「本レポート」という。）を作成した。

本レポートがこれから匿名加工情報に係る指針等を作成する認定団体や匿名加工情報の作成・取扱いに関心を持つ事業者や関係団体に役立つものとなることを期待する。

[1] Internet of Things：モノのインターネット

[2] Artificial Intelligence：人工知能

1. イントロダクション

1.1 個人情報保護法改正により匿名加工情報制度が導入された背景

平成 15 年（2003 年）5 月 30 日に公布され、平成 17 年（2005 年）4 月 1 日に全面施行された個人情報の保護に関する法律（平成 15 年法律第 57 号。以下 1.1 において「個人情報保護法」という。）の施行後 10 年余りが経過し、情報通信技術の飛躍的な進展等により個人情報を取り巻く状況は大きく変化した。

「世界最先端 IT 国家創造宣言」（平成 25 年(2013 年)6 月 14 日閣議決定）において、個人情報等については、「オープンデータやビッグデータの利活用を推進するためのデータ利活用環境整備を行うため、IT 総合戦略本部の下に、新たな検討組織を速やかに設置し、データの活用と個人情報及びプライバシーの保護との両立に配慮したデータ利活用ルールの策定等を年内できるだけ早期に進めるとともに、監視・監督、苦情・紛争処理機能を有する第三者機関の設置を含む、新たな法的措置も視野に入れた制度見直し方針を年内に策定する」[3]とされ、高度情報通信ネットワーク社会推進戦略本部の下に「パーソナルデータに関する検討会」が設置されて「匿名化」の議論もこの場で行われることとなった[4]。同検討会は平成 25 年(2013 年)12 月に「パーソナルデータの利活用に関する制度見直し方針」を発表し、同検討会技術検討ワーキンググループから報告書[5]が提出された。

平成 26 年(2014 年)6 月 24 日に同本部が決定した「パーソナルデータの利活用に関する制度改正大綱」において、多種多様かつ膨大なデータ、いわゆるビッグデータの収集・分析を可能とし、我が国の新産業・新サービスの創出や社会的課題の解決に貢献することが期待される一方で、個人情報及びプライバシーに対する消費者の意識が拡大しつつあり、保護されるべきパーソナルデータが適正に取り扱われることにより消費者の安心感を生む制度の構築が望まれるとされた[6]。また、これまでも個人情報ではない情報については法規制の対象外ではあったものの、個人情報の範囲に関する法解釈の曖昧さ[7]に起因する「グレーゾーンへの対応」の必要性が指摘され、当該情報を活用しようとした者が、個人情報保護法及びプライバシーの観点からどのようにすれば適切な取扱い

---

[3] http://www.kantei.go.jp/jp/singi/it2/pdf/it_kokkasouzousengen.pdf P.7 において「「ビッグデータ」のうち、特に利用価値が高いと期待されている、個人の行動・状態等に関するデータである「パーソナルデータ」の取扱いについては、その利活用を円滑に進めるため、個人情報及びプライバシーの保護との両立を可能とする事業環境整備を進める」とされており、「既に、スマートフォンの利用者情報の取扱いなど先行的にルール策定が行われた分野については、取組の普及を推進する」とされている。

[4] 規制改革会議の答申を踏まえた「規制改革実施計画」（2013 年 6 月閣議決定）（http://www.kantei.go.jp/jp/kakugikettei/2013/__icsFiles/afieldfile/2013/06/20/20130614-03.pdf）において、「ビッグデータ・ビジネスの普及（匿名化情報の取扱い）」として内閣官房及び消費者庁が「合理的な匿名化措置の内容を明確化したガイドラインを策定する」ことを平成 26 年上期までに措置することを要請し、同会議の創業等ワーキンググループ報告（2013 年 6 月）（http://www8.cao.go.jp/kisei-kaikaku/kaigi/publication/130605/item5.pdf）において、米国 FTC3 要件が引用され、「我が国でもある事業者（X）が元データと加工等により特定の個人を識別できなくなった新データの両方のデータを保有し、新データのみを第三者（Y）に提供する場合において、X・Y 間の契約で Y による再識別化が禁止されているときは、個人の権利利益の侵害のおそれはないのであるから、新データは「個人情報」に該当しない旨を明確すべきではないか」との「問題意識」が示された。

[5] 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」（2013 年 12 月）（http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf）及び「技術検討ワーキンググループ報告書 ～「（仮称）準個人情報」及び「（仮称）個人特定性低減データ」に関する技術的観点からの考察について～」（2014 年 5 月）。（http://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou1-2.pdf）

[6] 高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」（2014 年 6 月）(http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20140624/siryou5.pdf)。既に多くの情報が収集蓄積されていたとしてもその情報が十分活用されていない状況も多く見られるようになっている。

[7] 大綱において、「特定の個人が識別された状態にないパーソナルデータであっても、特定の個人に結びつく蓋然性が高いなど、その取扱いによっては個人の権利利益が侵害されるおそれがあるものに関して、保護される対象及びその取扱いについて事業者が尊重すべきルールが曖昧」であることが指摘されている。

をできるのかが不明瞭であることから、プライバシーに係る社会的な批判を懸念してパーソナルデータの利活用に躊躇するという「利活用の壁」が同大綱において指摘され、個人情報及びプライバシーの保護を図りつつ、利活用を実現する環境整備を行うことが求められるとされた。具体的には、個人データ等から「個人の特定性を低減したデータ」に加工し第三者提供等を本人の同意がなくても行うことを可能とする基本的制度について法律で大枠を定め [8]、具体的な内容は政省令、規則及びガイドラインにより対応するとともに、民間の自主規制ルールの活用を図ることとされた [9]。

平成 27 年（2015 年）9 月に成立した「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」（平成 27 年法律第 65 号。以下「改正法」という。）は、この大綱の内容を踏まえて検討を進められたものであり、改正項目の一つとして「匿名加工情報」という制度が新設された。加えて、改正法案に関する国会審議を踏まえた附帯決議において、「匿名加工情報については、その規定の趣旨が利活用を促進するものであることに鑑み、個人情報保護委員会規則で基準を定めるに当たっては、効果的な利活用に配慮すること」（衆議院内閣委員会）、「匿名加工情報の規定の趣旨が個人情報の利活用を促進するものであることに鑑み、個人情報取扱事業者が匿名加工情報を作成する際に必要となる基準を個人情報保護委員会で定めるに当たっては、その趣旨について十分に配慮すること」、「本法の施行後も…広報その他の活動を通じて、個人情報及び匿名加工情報の適正な取扱いの下での利活用の推進に関する国民の理解と信頼を深めるよう努めること」（参議院内閣委員会）が表明された。

IoT やビッグデータというキーワードに象徴されるように、いかにデータを収集・分析して事業に活かすかが昨今のビジネスシーンにおいて競争力を確保する上で重要であると認識される中、匿名加工情報制度は、加工基準に従った加工その他の一定のルールを義務付けることで、安全性を確保しつつデータの積極的な利活用の推進に寄与することが期待されている。

[8] 大綱において、医療情報等のように適切な取扱いが求められつつ、本人の利益・公益に資するために一層の利活用が期待される情報も多いことから、適切な保護と利活用を推進するとされた。

[9] 大綱において、「個人が特定される可能性を低減したデータへの加工方法については、データの有用性や多様性に配慮し一律には定めず、事業等の特性に応じた適切な処理を行うことができることする」とされた。さらに、当該加工方法については、民間団体が自主規制ルールを策定し、第三者機関（個人情報保護委員会）が当該ルール又は民間団体の認定等を行うこと、適切な加工方法についてはベストプラクティスの共有等を図ることとされた。

1.2 本レポートの位置付け

匿名加工情報は、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 36 条第 1 項により、個人情報保護委員会規則で定める基準[10]に従い加工することとされているが、当該規則ではあらゆる業界の事業者に共通するような最低限の規律を定め、ガイドラインにおいては、匿名加工情報の定義等とともに、当該規則について解説する内容となっている。

一方、これら個人情報保護委員会規則で定める基準及びガイドラインに従って事業者が具体的にどのような加工を行うかについては、取り扱う個人情報の性質、取扱い実態等に応じて定めることが望ましいことから、認定団体が作成する個人情報保護指針等の自主的なルールに委ねることとしている。

本レポートは、主に、匿名加工情報を作成するための考え方や手法（法第 36 条第 1 項関連）及び識別行為の禁止（法第 36 条第 5 項及び第 38 条関連）、加工方法等情報や匿名加工情報の安全管理措置（法第 36 条第 2 項及び第 6 項並びに第 39 条）に焦点を当てて、認定団体及び事業者団体等が匿名加工情報の作成に関するルールを検討したり、民間事業者が実際に匿名加工情報を作成したりする際に参考となる事項、考え方を示そうとするものである。

なお、その他の個人情報取扱事業者や匿名加工情報取扱事業者に課せられる義務（匿名加工情報を作成した際及び第三者提供した際の公表義務等）については、本レポートでは紹介程度にとどめるため、詳細については「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」（平成 28 年個人情報保護委員会告示第 9 号。以下「ガイドライン」という。）を参照されたい。

[10] 匿名加工情報の加工基準は、個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号）第 19 条において定められている。

2. 個人情報とその取扱いにおける制約

2.1 個人情報の定義

個人情報の定義は、法第 2 条第 1 項において次のように規定されている。

法第 2 条第 1 項

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（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第 2 号において同じ。）で作られる記録をいう。第 18 条第 2 項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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

「特定の個人を識別することができる」とは、情報単体又は複数の情報を組み合わせて保存されているものから社会通念上そのように判断できるものをいい、一般人の判断力又は理解力をもって生存する具体的な人物と情報の間に同一性を認めるに至ることができるかどうかによるものである。

「他の情報と容易に照合することができ」るとは、いわゆる容易照合性と呼ばれているものであるが、事業者の実態に即して個々の事例ごとに判断されるべきであるものの、通常の業務における一般的な方法で、他の情報と容易に照合することができる状態をいうものとされている。

今回の改正により新たに設けられた同項第 2 号の個人識別符号は、法第 2 条第 2 項において、次のように定義されている。

法第 2 条第 2 項

この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。

一　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

二　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

「個人識別符号」は、上記の法第 2 条第 2 項各号に該当する文字、番号、記号その他の符号のうち、政令で定めるものが該当するとされ、個人情報の保護に関する法律施行令（平成 28 年政令第 507 号。以下「施行令」という。）及び個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号。以下「施行規則」という。）において、図表 2-1 に示す内容が個人識別符号に該当するものとして、細かく限定的に規定されている。

図表 2-1　個人識別符号に係る法・施行令・施行規則の関係

法	施行令（第 1 条）	施行規則（第 2 条～第 4 条）
第1号関係	(1)　次に掲げる身体の特徴のいずれかを電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、特定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するもの イ　ＤＮＡを構成する塩基の配列 ロ　顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌 ハ　虹彩の表面の起伏により形成される線状の模様 ニ　発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化 ホ　歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様 ヘ　手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状 ト　指紋又は掌紋	（第 2 条） 身体の特徴を電子計算機の用に供するために変換した符号のうち個人識別符号に該当するものの基準は、特定の個人を識別することができる水準が確保されるよう、適切な範囲を適切な手法により電子計算機の用に供するために変換することとする。
第2号関係	(2)　旅券の番号、 (3)　基礎年金番号、 (4)　運転免許証の番号、 (5)　住民票コード (6)　個人番号	
	(7)　国民健康保険、後期高齢者医療制度及び介護保険の被保険者証にその発行を受ける者ごとに異なるものとなるように記載された個人情報保護委員会規則で定める文字、番号、記号その他の符号	（第 3 条） (1)　国民健康保険の被保険者証の記号、番号及び保険者番号 (2)　後期高齢者医療制度及び介護保険の被保険者証の番号及び保険者番号
	(8)　上記(1)～(7)に準ずるものとして個人情報保護委員会規則で定める文字、番号、記号その他の符号	（第 4 条） 健康保険の被保険者証等の記号、番号及び保険者番号、公務員共済組合の組合員証等の記号、番号及び保険者番号、雇用保険被保険者証の被保険者番号並びに特別永住者証明書の番号　等

法第２条第２項第 1 号に定める個人識別符号については、図表 2-1 における施行令第 1 条(1)イ～トに列挙される生体データのうち、施行規則で定められた基準（「特定の個人を識別することができる水準が確保されるよう、適切な範囲を適切な手法により電子計算機の用に供するために変換すること」）に適合するものとは、

イの DNA を構成する塩基の配列については、「ゲノムデータのうち、全核ゲノムシークエンスデータ、全エクソームシークエンスデータ、全ゲノム一塩基多型（single nucleotide polymorphism：SNP） データ、互いに独立な 40 箇所 以上の SNP から構成されるシークエンスデータ、9 座位以上の 4 塩基単位の繰り返し配列（short tandem repeat：STR）等の遺伝型情報により本人を認証することができるようにしたもの」であり、ロ～トについては、「該当する生体データから抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの」となっている [11]。

同項第 2 号に定める個人識別符号としては、マイナンバー等、公的付番の符号が規定されており、民間付番のサービス ID や携帯電話番号、クレジットカード番号等は規定されていない。しかしながら、これら民間付番の符号は個人識別符号ではなくても、単体あるいはその他の情報と組み合わせられること等により法第 2 条第 1 項第 1 号の個人情報に該当する場合があることに留意する必要がある。

2.2 個人情報を取り扱う上での制約

個人情報をデータベース化した上で事業の用に供している者は個人情報取扱事業者と呼ばれ（法第 2 条第 4 項及び第 5 項）、個人情報を取り扱う際には、法第 4 章で規定される義務を遵守する必要がある。代表的な規律としては、次のようなものが挙げられる（匿名加工情報との関係が深い部分を中心に抜粋）。

① 取り扱う個人情報の利用目的を特定する必要があること。また、利用目的の変更は、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えないこと（法第 15 条）
② 本人の同意を得ずに、特定した利用目的の範囲を超えて個人情報を取り扱ってはいけないこと（法第 16 条）
③ 偽りその他不正の手段により個人情報を取得してはならないこと（法第 17 条）
④ 個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならないこと（法第 18 条）
⑤ 法令に基づく場合等の一部の例外を除き、あらかじめ本人の同意を得ないで個人データを第三者提供してはいけないこと、あるいはオプトアウトの手段を用意した上で第三者提供を行うこと（法第 23 条第 1 項及び第 2 項）

一方、事業者としては、新しい分野のサービスや製品の導入を行う場合等には、取得時に特定した利用目的とは関連性が低い新しい目的のために個人情報を利用したいニーズが生じ得るが、法第 16 条に基づき全員から利用目的の変更の同意を再取得することは、コストやスピードの観点からはデメリットも小さくなく、過去のデータの利用にまで遡っての同意の取得や、多数のユーザーからの同意の取得が困難なケースも想定される。

改正前の法においても、個人情報を加工して統計情報等の特定の個人との関係が排斥され特定の個人を識別できないようにした情報は、法規制の対象外と位置付けられて上記の制約を受けることなく活用することができた。一方、「どこまで加工すれば個人情報でなくなるのか」といった点について一定のルールやコンセンサスが共有されておらず、例えば、鉄道系 IC カードの乗降履歴の第三者提供について、個人情報に対する匿名加工の処理が十分であるか、利用者への十分な説明やプライバシーへの配慮が必要ではないか等の指摘により提供を中断した事例 [12]も見られた。

---

[11] 詳しくは、「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年個人情報保護委員会告示第 6 号）2-2 を参照のこと。

[12] Suica に関するデータの社外への提供に関する有識者会議「Suica に関するデータの社外への提供について 中間とりまとめ」（2014 年 2 月）（http://www.jreast.co.jp/chukantorimatome/20140320.pdf）。移動履歴について k -匿名化を行うと、多くの

このように、個人情報の範囲及び匿名加工の方法の解釈にグレーゾーンがあり、プライバシーに係る社会的な意識が拡大する中で、我が国の事業者や団体等が有する個人情報を含むパーソナルデータを多様な目的のために利活用する場合又は第三者提供をする場合の適正な取扱いに関するルール及びコンセンサスを共有することにより、パーソナルデータの利活用に関する社会的信頼を確保した上で、様々な目的のための利活用及び第三者提供へのハードルを取り除き、適正な利活用の推進を促進することが重要である。

データを削除することとなりデータ有用性が下がることから、当面は JR において統計処理を行ってから外部提供を行うこと等も課題解決の一つとされた。

3. 匿名加工情報とは

3.1 匿名加工情報を利用するアドバンテージ

匿名加工情報の制度は、個人情報を特定の個人を識別できないように加工した情報について、一定のルールの下で本人の同意を得ることなく目的外利用及び第三者提供を可能とすることにより、事業者間におけるデータ取引やデータ連携を含むパーソナルデータの利活用を促進しようとするものであり、新事業や新サービスの創出、ひいては、国民生活の利便性の向上につながることが期待される。

匿名加工情報については、法第 2 条第 9 項で定義が示されるとともに、その取扱いに関するルールについては、法第 36 条～第 39 条で規定されている。これらのルールを守り匿名加工情報を作成し取り扱うことにより、個人情報取扱事業者は法的枠組みの下で本人の同意を得ることなく、特定された利用目的外での利用や第三者への提供が安定的に可能となるものであり、匿名加工情報取扱事業者は幅広く様々な種類の匿名加工情報を入手して利用することが可能となるものである。

また、匿名加工情報の加工基準及びその適正な取扱いについて、第三者機関である個人情報保護委員会が一元的に最低限の基準を示し、認定団体等が個人情報保護指針等により具体的な自主ルールを策定し対象事業者にその遵守を促すこと等により、国民にとっても安心できる形で適正なパーソナルデータの利用が確保されることが期待される。

匿名加工情報の利活用による事例として、例えば、

① ポイントカードの購買履歴や交通系 IC カードの乗降履歴等を複数の事業者間で分野横断的に利活用することにより、新たなサービスやイノベーションを生み出す可能性

② 医療機関が保有する医療情報を活用した創薬・臨床分野の発展や、カーナビ等から収集される走行位置履歴等のプローブ情報を活用したより精緻な渋滞予測や天候情報の提供等により、国民生活全体の質の向上に寄与する可能性

等が期待されている[13]。

3.2 匿名加工情報の定義

匿名加工情報は、法において次のように定義されており、また、ガイドラインにおいて次のように解説している。

法第 2 条第 9 項

この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。

一　第 1 項第 1 号に該当する個人情報　当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

二　第 1 項第 2 号に該当する個人情報　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

ガイドライン 2-1 匿名加工情報（法第 2 条第 9 項関係）

「匿名加工情報」とは、個人情報を個人情報の区分に応じて定められた措置を講じて特定の個人を識別

[13] 2015 年 5 月 8 日衆議院・内閣委員会における政府答弁。

することができないように加工して得られる個人に関する情報であって、当該個人情報を復元して特定の個人を再識別することができないようにしたものをいう。

法第 2 条第 1 項第 1 号に該当する「当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの（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。）」である個人情報の場合には、「特定の個人を識別することができないように個人情報を加工」とは、特定の個人を識別することができなくなるように当該個人情報に含まれる氏名、生年月日その他の記述等を削除することを意味する。

法第 2 条第 1 項第 2 号に該当する「個人識別符号が含まれる」個人情報の場合には、「特定の個人を識別することができないように個人情報を加工」とは、当該個人情報に含まれる個人識別符号の全部を特定の個人を識別することができなくなるように削除することを意味する（この措置を講じた上で、まだなお法第２条第 1 項第 1 号に該当する個人情報であった場合には、同号に該当する個人情報としての加工を行う必要がある。）。

「削除すること」には、「当該一部の記述等」又は「当該個人識別符号」を「復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む」とされている。「復元することのできる規則性を有しない方法」とは置き換えた記述から、置き換える前の特定の個人を識別することとなる記述等又は個人識別符号の内容を復元することができない方法である。

なお、法において「特定の個人を識別することができる」とは、情報単体又は複数の情報を組み合わせて保存されているものから社会通念上そのように判断できるものをいい、一般人の判断力又は理解力をもって生存する具体的な人物と情報の間に同一性を認めるに至ることができるかどうかによるものである。匿名加工情報に求められる「特定の個人を識別することができない」という要件は、あらゆる手法によって特定することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人及び一般的な事業者の能力、手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により特定できないような状態にすることを求めるものである。

また、「当該個人情報を復元することができないようにしたもの」とは、通常の方法では、匿名加工情報から匿名加工情報の作成の元となった個人情報に含まれていた特定の個人を識別することとなる記述等又は個人識別符号の内容を特定すること等により、匿名加工情報を個人情報に戻すことができない状態にすることをいう。

「当該個人情報を復元することができないようにしたもの」という要件は、あらゆる手法によって復元することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人及び一般的な事業者の能力、手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により復元できないような状態にすることを求めるものである。

匿名加工情報を作成するときは、法第 36 条第 1 項に規定する個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第３号。以下「規則」という。）で定める基準に従って加工する必要があり、法第 2 条第 9 項に定める措置を含む必要な措置は当該規則で定めている。（匿名加工情報の作成に必要な加工義務については、3-2（匿名加工情報の適正な加工）参照）

なお、「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、改正前の法においても規制の対象外と整理されており、従来同様に規制の対象外となる。

匿名加工情報は、個人情報から作成されるものであり、特定の個人を識別することができず、かつ、元となる個人情報を復元することができない、個人に関する情報である。個人に関する情報であるということは、すなわち情報の単位としては一人ひとりに対応した情報であることが許容されるものである [14]。なお、匿名加工情報の集合体としては、法第 2 条第 10 項において、「匿名加工情報データベース等」という言葉が定義されている。

3.2.1 「特定の個人を識別することができない」とは

ガイドラインにも記載されているように、法において「特定の個人を識別することができる」とは、情報単体又は複数の情報を組み合わせて保存されているものから社会通念上そのように判断できるものをいい、一般人の判断力又は理解力をもって生存する具体的な人物と情報の間に同一性を認めるに至ることができるかどうかによるものである。匿名加工情報に求められる「特定の個人を識別することができない」という要件は、あらゆる手法によって特定することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人及び一般的な事業者の能力、手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により特定できないような状態にすることを求めるものである。

3.2.2 「当該個人情報を復元することができないようにしたもの」とは

ガイドラインにも記載されているように、「当該個人情報を復元することができないようにしたもの」とは、通常の方法では、匿名加工情報から匿名加工情報の作成の元となった個人情報に含まれていた特定の個人を識別することとなる記述等又は個人識別符号の内容を特定すること等により、匿名加工情報を個人情報に戻すことができない状態にすることをいう。

「当該個人情報を復元することができないようにしたもの」という要件は、あらゆる手法によって復元することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人及び一般的な事業者の能力、手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により復元できないような状態にすることを求めるものである。

上記のとおり、「特定の個人を識別することができない」及び「復元することができないようにしたもの」の何れも一般人及び一般的な事業者の能力や手法等を基準として判断されるものであり、例えば、スーパーコンピュータのような高度な機能を有する資源を利用したり、高度なハッキング・スキルを利用したりする等のあらゆる手法によって特定や復元を試みたとしてもできないというように、技術的側面から全ての可能性を排除することまでを求めるものではない。

3.2.3 一部の情報が復元できた場合について

「当該個人情報を復元」とは、特定の個人の識別につながる情報が復元されることを指す。つまり、匿名加工情報から元の個人情報を全て復元することだけではなく、一部ではあっても元の個人情報の本人を特

[14] 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」（2013 年 12 月）にある「非識別非特定情報」（一人ひとりが識別されない（かつ個人が特定されない）状態の情報）だけでなく、「識別非特定情報」（一人ひとりは識別されるが、個人が特定されない状態の情報）も匿名加工情報に該当する場合があると考えられる。

定し得る情報が復元されることも「復元」に該当する。

一方、特定の個人の識別につながらないような部分の情報の復元については、ここでいう「復元」には当たらない。例えば、匿名加工情報の作成の際に、元の個人情報から「電話番号」の情報の項目が全部削除されている場合に、匿名加工情報に含まれている郵便番号や居住エリア（市町村名）の情報に基づいて、電話番号の市外局番を復元することも想定し得る。但し、その市外局番を復元できたことをもって特定の個人の識別ができる程度に復元されたりするものでなければ、「当該個人情報を復元」には該当しないと考えられる。

3.2.4 「復元することのできる規則性を有しない方法により他の記述等に置き換えること」とは

特定の個人を識別することができないように個人情報から匿名加工情報への加工を行う際には、必要に応じて対象となる記述等を削除することのほか、置き換えられた記述等から元の記述等へ戻すことができない方法（復元することのできる規則性を有しない方法）により他の記述等へ置き換えることも可能である。

ここで「復元することのできる規則性を有しない方法」とは、あくまで、置換え後の記述等から元の個人情報の記述等への変換の規則性を有しない方法を意味し、記述等を置き換えるための規則性を有しないことまで求めるものではない。

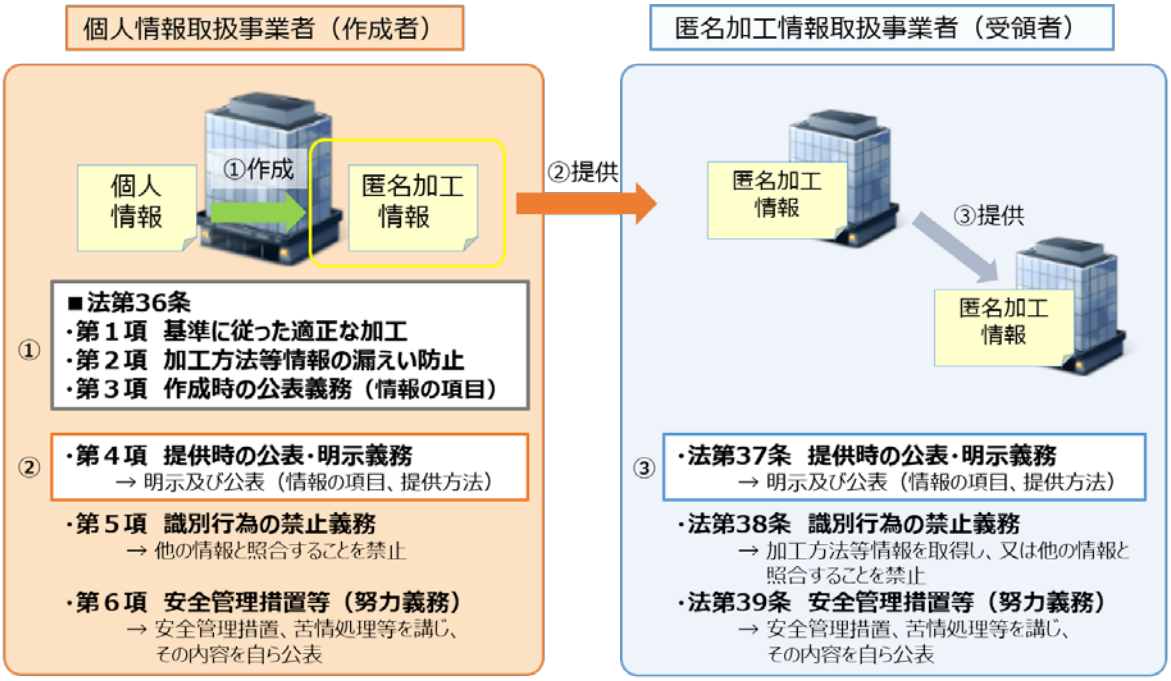
3.3 匿名加工情報を取り扱う上での制約

匿名加工情報(匿名加工情報データベースを構成するものに限る)を作成し、それを取り扱うときには、個人情報取扱事業者は法第 36 条の規定を順守する必要がある。匿名加工情報を作成する個人情報取扱事業者としては、法第 36 条第 1 項の適正加工義務のほか、加工方法等の情報の漏えいを防止するための安全管理措置や匿名加工情報を作成した場合及び匿名加工情報を第三者に提供する場合の公表義務、識別行為の禁止等がかかることになる。

また、他の事業者が個人情報を加工して作成した匿名加工情報の提供を受けてこれを事業の用に供している匿名加工情報取扱事業者は法第 37 条～第 39 条の規定を順守する必要がある。匿名加工情報の提供を受ける匿名加工情報取扱事業者は、識別行為の禁止義務、匿名加工情報の安全管理措置等の努力義務、及び、さらなる第三者提供を行う場合の公表義務がかかることになる。なお、匿名加工情報を作成した個人情報取扱事業者が当該匿名加工情報に係る匿名加工情報データベース等を事業の用に供する場合は、当該個人情報取扱事業者は匿名加工情報取扱事業者にも該当するが、法第 37 条～第 39 条は、「自ら個人情報を加工して作成した匿名加工情報」以外の匿名加工情報の取扱いに当たって生じる義務であるため、法第 37 条～第 39 条の義務の対象とはならない（ただし、個人情報取扱事業者が自ら個人情報を加工して作成した匿名加工情報を取り扱う際には法第 36 条の規定が適用される。）。

この法第 36 条～第 39 条の関係を図にしたものが、図表 3-1 である。

図表 3-1　匿名加工情報の作成者・受領者が順守すべき規定



3.4　匿名加工情報に関する留意点

3.4.1　統計情報について

個人情報と匿名加工情報は、それぞれ法第 2 条第 1 項及び第 9 項の定義にあるように、「個人に関する情報」である。一方、「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等を数量的に把握するものである。ガイドラインでは「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、改正前の法においても規制の対象外と整理されており、従来同様に規制の対象外とされている。」と記載している。したがって、適切に加工された統計情報は、個人情報にも匿名加工情報にも該当しないものである[15]。

ただし、例えば、統計情報の作成において、ある項目の値を所定範囲ごとに区切る場合、その範囲の設定の仕方によってはサンプルが著しく少ない領域（高齢者、高額利用者、過疎地における位置情報等）が生じる可能性がある。このような場合については、誰の情報であるか特定されやすくなることもあり得る。統計情報という形になっていればよいというものではなく、個人との対応関係が十分に排斥できるような形で統計化されていることが重要であるといえる。

3.4.2　容易照合性との関係

匿名加工情報を作成した事業者は、その作成に用いた個人情報を保有しており、また、当該個人情報を匿名加工する方法に関する情報として匿名加工情報と元の個人情報との対応関係を示す対応表等を保有し得るが、この個人情報や対応表について法第 2 条第 1 項第 1 号括弧書のいわゆる「容易照合性」があるとして、作成した匿名加工情報は個人情報に該当し、個人情報の取扱いに関する各義務（法第 4

[15] このような統計情報の例としては、個別の調査結果を集計して、統計作成者の責任の下で、統計情報として公開して一般に利用可能とされているもの、あるいは第三者に提供されているものがあり、例えば、公的統計の公表された統計表のほか、業界団体や民間調査会社等が作成する民間統計がある。

章第 1 節）を守らなければならないのではないか、との懸念が想定される。

匿名加工情報は、特定の個人を識別することができず、作成の元となった個人情報を復元することができないように加工したものであり、さらに、個人情報に係る本人を識別することを禁止する等の制度的な担保がなされていることから、作成の元となった個人情報を通常の業務における一般的な方法で照合することができる状態にある（すなわち容易照合性がある）とはいえず、個人情報に該当しないとされるものである。

したがって、匿名加工情報を作成した事業者がこれを当該事業者内部で取り扱うに当たっても、匿名加工情報の取扱いに関する義務（法第 36 条）を守ることにより自由な利活用が認められることとなる。

匿名加工情報については、法第２条第９項の規定に基づき、特定の個人を識別することができないものであり、個人情報を復元することができないようにしたものであることが求められるものであり、この際の「特定の個人を識別することができない」の判断基準については、法第２条第１項第１号の括弧外と同様に一般人及び一般の事業者の判断力や理解力をもって行われるものであり、かつ、「復元することができない」の判断基準についても一般人及び一般の事業者の判断力や理解力をもって行われるものである。

匿名加工情報は、その立法趣旨からも、本来の利用目的外で利用する場合あるいは他の匿名加工情報取扱事業者に提供する場合等により、利用・流通過程における安全性を確保しつつ個人に関する情報の利活用を図る制度であり、個人情報に対して一定の加工及び規律を課した上で第三者提供等を可能とするものであるため、一般人及び一般の事業者における判断力や理解力を考慮した上で安全性を判断することが妥当であると考えられる。

なお、匿名加工情報の作成事業者内部において、匿名加工情報に加工される前の元となる個人情報や加工方法等に関する情報が保存されることは制度的に前提とされており、作成事業者の内部に存在し、かつ識別行為の禁止義務の対象である対応表について、特別に危険視することは適当ではないものの、識別行為の禁止及び加工方法等情報の安全管理措置等の匿名加工情報の取扱いに関する義務を守ることが当然に必要である。

(参考)「容易照合性」

「容易照合性」とは、それ自体では特定の個人を識別することができない情報であっても、その情報を取り扱う事業者が、特別の調査を行ったり特別の費用や手間をかけたりすることなく、当該事業者が行う業務における一般的な方法で、他の情報との照合が可能な状態にあることをいう。法では、このような状態にあることによって「特定の個人を識別することができることとなるもの」を個人情報に含め、保護対象としている。

「容易照合性」の判断要素としては、保有する各情報にアクセスできる者の存否、社内規程の整備等の組織的な体制、情報システムのアクセス制御等の技術的な体制等が挙げられ、これらを総合的に勘案して「特定の個人を識別することができる」か否かが判断されるものであり、取り扱う個人情報の内容や利活用の方法等、事業者の実態に即して個々の事例ごとに判断されることとなる [16]。

例えば、事業者の各取扱部門が独自に取得した個人情報を取扱部門ごとに設置されているデータベースにそれぞれ別々に保管している場合において、双方の取扱部門やこれらを統括すべき立場の者等が、特別の費用や手間をかけることなく、通常の業務における一般的な方法で双方のデータベース上の情報を照合することができないよう、規程上・運用上、双方のデータベースを取り扱うことが厳格に禁止されていて、特別の費用や手間をかけることなく、通常の業務における一般的な方法で双方のデータベース上の情報を照合することができない状態であれば、「容易に照合することができ」るとはいえないものと考えられる。

[16] 瓜生和久編『一問一答　平成 27 年改正個人情報保護法』（商事法務、2015 年） P13（Q8）。

一方、双方の取扱部門の間で、通常の業務における一般的な方法で双方のデータベース上の情報を照合することができる場合は、「容易に照合することができ」る場合に当たると考えられる[17]。

なお、法第 2 条第 1 項第 1 号括弧内の容易照合性は、上記のように事業者内部における照合性を意味するものであり、これは法第 4 章第 1 節の個人情報取扱事業者の義務（第 15 条～法第 35 条）における「個人情報」の定義において共通的に適用されるものと考えられるため、法第 23 条の第三者提供の制限においても「個人情報」[18]に関する容易照合性の判断は事業者内部における照合性を意味することとなる。

また、法第 2 条第 1 項第 1 号括弧外の「特定の個人を識別することができる」の要件は、情報単体又は複数の情報を組み合わせて保存されているものから、社会通念上そのように判断できるもの、すなわち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の間に同一性を認めるに至るかどうかが判断基準となっている。

3.5 匿名加工情報の作成とは

匿名加工情報については、法第 36 条第 1 項で規定されているように、施行規則で定める基準に従って個人情報を加工することとされている。

法第 36 条第 1 項

個人情報取扱事業者は、匿名加工情報（匿名加工情報データベース等を構成するものに限る。以下同じ。）を作成するときは、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするために必要なものとして個人情報保護委員会規則で定める基準に従い、当該個人情報を加工しなければならない。

また、「匿名加工情報の作成」については、ガイドラインでは次のように解説している。

ガイドライン 3-2 匿名加工情報の適正な加工（法第 36 条第 1 項関係）

個人情報取扱事業者は、匿名加工情報（匿名加工情報データベース等を構成するものに限る（※1）。以下同じ。）を作成するとき（※2）は、特定の個人を識別できないように、かつ、その作成に用いる個人情報を復元できないようにするために、規則第 19 条各号に定める基準に従って、当該個人情報を加工しなければならない。なお、「個人情報保護委員会規則で定める基準に従い、当該個人情報を加工」するためには、加工する情報の性質に応じて、規則第 19 条各号に定める加工基準を満たす必要がある。

（※1）匿名加工情報の取扱いに係る義務（法第 36 条～第 39 条）は、匿名加工情報データベース等を構成する匿名加工情報に課されるものであり、いわゆる散在情報となる、匿名加工情報データベース等を構成しない匿名加工情報の取扱いに係る義務は課されていない。

（※2）「作成するとき」は、匿名加工情報として取り扱うために、当該匿名加工情報を作成するときのことを指す。したがって、例えば、安全管理措置の一環として氏名等の一部の個人情報を削除（又は他の記述等に置き換え）した上で引き続き個人情報として取り扱う場合、あるいは統計情報を作成するために個人情報を加工する場合等については、匿名加工情報を「作成するとき」には該当しない。

[17] 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』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関するＱ＆Ａ」（2017 年 2 月） A1-15。

[18] 法第 23 条は「個人データ」の取扱いに関する義務であるが、「個人データ」は法第 2 条第 6 項の定義から明らかなように、法第 2 条第 1 項で定義される「個人情報」の解釈に依拠するものである。

ガイドライン 3-4 匿名加工情報の作成時の公表（法第 36 条第 3 項関係）（抜粋）

個人情報取扱事業者は、匿名加工情報を作成したとき（※1）は、匿名加工情報の作成後遅滞なく（※2）、インターネット等を利用し、当該匿名加工情報に含まれる個人に関する情報の項目を公表（※3）しなければならない。

（※1）ここで「匿名加工情報を作成したとき」とは、匿名加工情報として取り扱うために、個人情報を加工する作業が完了した場合のことを意味する。すなわち、あくまで個人情報の安全管理措置の一環として一部の情報を削除しあるいは分割して保存・管理する等の加工をする場合又は個人情報から統計情報を作成するために個人情報を加工する場合等を含むものではない。

また、匿名加工情報を作成するために個人情報の加工をする作業を行っている途上であるものの作成作業が完了していない場合には、加工が不十分であること等から匿名加工情報として取り扱うことが適切ではない可能性もあるため「匿名加工情報を作成したとき」とは位置付けられない。

ガイドライン中で上記に示した「3-2 匿名加工情報の適正な加工（法第 36 条第 1 項関係）」の（※2）及び「3-4 匿名加工情報の作成時の公表（法第 36 条第 3 項関係）」の（※1）に記載されているように、「匿名加工情報を作成する」とは、匿名加工情報の作成意図をもって、法で規定された匿名加工情報として取り扱うことを目的として匿名加工情報を作成するときのことを指すものである。「法で規定された匿名加工情報として取り扱う」とは、本人同意を得ないで新たな目的のために活用する場合や、第三者に提供するような場合等が想定される。

つまり、匿名加工情報を作成する意図がなく、かつ、個人情報として取り扱うことを前提にしたデータの加工については、法律上の「匿名加工情報の作成」に該当するものではないのであり、このようなデータの加工に対して、匿名加工情報に係る義務が発生するものではない。このようなデータの加工としては、主として、次のようなケースが該当すると思われる。

(1) 社内での安全管理上、氏名等を削除して扱うデータ

事業者が個人情報を取り扱う中で、ユーザーの傾向やマーケット全体の分析等を行うに当たって、安全管理上、氏名等の分析に必要のない個人情報を削除するケースがよくある。また、その分析を他の事業者に委託する場合にも、一部の情報を削除して提供する場合も想定される。

このような扱いについては、匿名加工情報の作成意図はなく、個人情報として引き続き取り扱う前提である場合には、法律上の「匿名加工情報の作成」には該当しない。

(2) 統計情報を作成するために個人情報を加工したデータ

取得した個人情報の利用態様の一つとして、ユーザーの傾向分析等を行うために個人情報を加工して統計情報を作成することが想定される。

こういった統計情報を作成する際に、個人情報のデータセットからそのまま集計表を作成することで統計化する場合だけでなく、一旦、個人情報から氏名等を削除するとともに、住所や年齢等の項目を一定のカテゴリーに分類（例：東京都千代田区→東京都、25 歳→20 代等）した上で集計して統計化することも想定される。

このような個人情報から適切な加工を施して統計化を行う作業の途上で生成される加工データについては、匿名加工情報の作成意図はないことから、法律上の「匿名加工情報の作成」には該当しない。

(3) 匿名加工情報を作成する途上で発生するデータ

匿名加工情報を作成する際には、データとしての有用性や再識別リスク[19]の評価等に伴い、複数の匿名加工手法を試行したりノイズの量や情報の丸めの程度等のパラメータを変更したりする等、匿名加工処理を何度もやり直したり、加工方法を調整しながら一連の匿名加工情報を作成することも想定される。

ガイドラインにもあるように、匿名加工情報を作成するために個人情報の加工をする作業を行っている途上であるものの作成作業が完了していない場合には、加工が不十分であること等から匿名加工情報として取り扱うことが適切ではない可能性もあるため、法律上の「匿名加工情報を作成したとき」には位置付けられないこととなる。

最終的に匿名加工情報とするための加工作業が完了したことをもって「匿名加工情報を作成」したことになり、匿名加工情報の作成・第三者提供に係る公表義務や安全管理措置等を履行するとともに、匿名加工情報として取り扱うことが可能となる。

[19] 当該匿名加工情報の作成に用いられた個人情報に係る本人が識別されるリスク。

4. 匿名加工情報の作成に当たって求められる加工

4.1 匿名加工情報の加工基準（施行規則第 19 条）について

法第 36 条第 1 項では、匿名加工情報を作成するに当たっては、施行規則で定める基準に従うこととされており、その基準については、施行規則第 19 条で規定されている。施行規則第 19 条は全 5 号で構成されており、匿名加工情報を作成する際は、各号を選択的に講ずるのではなく、各号全ての措置を行う必要がある（ただし、該当する情報がない場合は、この限りではない）。

4.1 においては、施行規則第 19 条各号に規定する措置について、その具体的な手法を検討する。

4.1.1 第 1 号（特定の個人を識別することができる記述等の削除）

施行規則第 19 条第 1 号

個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

ガイドライン 3-2-1 特定の個人を識別することができる記述の削除

個人情報取扱事業者が取り扱う個人情報には、一般に、氏名、住所、生年月日、性別の他、様々な個人に関する記述等が含まれている。これらの記述等は、氏名のようにその情報単体で特定の個人を識別することができるもののほか、住所、生年月日など、これらの記述等が合わさることによって特定の個人を識別することができるものもある。このような特定の個人を識別できる記述等から全部又はその一部を削除するあるいは他の記述等に置き換えることによって、特定の個人を識別することができないよう加工しなければならない。

なお、他の記述等に置き換える場合は、元の記述等を復元できる規則性を有しない方法でなければならない（※）。例えば、生年月日の情報を生年の情報に置き換える場合のように、元の記述等をより抽象的な記述に置き換えることも考えられる。

【想定される加工の事例】

事例 1）氏名、住所、生年月日が含まれる個人情報を加工する場合に次の 1 から 3 までの措置を講ずる。

1）氏名を削除する。

2）住所を削除する。又は、○○県△△市に置き換える。

3）生年月日を削除する。又は、日を削除し、生年月に置き換える。

事例 2）会員 ID、氏名、住所、電話番号が含まれる個人情報を加工する場合に次の 1、2 の措置を講ずる。

1）会員 ID、氏名、電話番号を削除する。

2）住所を削除する。又は、○○県△△市に置き換える。

（※）仮 ID を付す場合には、元の記述を復元することのできる規則性を有しない方法でなければならない。

例えば、仮にハッシュ関数等を用いて氏名・住所・連絡先・クレジットカード番号のように個々人に固有の記述等から仮 ID を生成しようとする際、元の記述に同じ関数を単純に用いると元となる

記述等を復元することができる規則性を有することとなる可能性がある場合には、元の記述（例えば、氏名＋連絡先）に乱数等の他の記述を加えた上でハッシュ関数等を用いるなどの手法を検討することが考えられる。なお、同じ乱数等の他の記述等を加えた上でハッシュ関数等を用いるなどの手法を用いる場合には、乱数等の他の記述等を通じて復元することができる規則性を有することとならないように、提供事業者ごとに組み合わせる記述等を変更し、定期的に変更するなどの措置を講ずることが望ましい。

施行規則第 19 条第 1 号は、法第 2 条第 9 項第 1 号の規定に基づき、法第２条第 1 項第１号に該当する個人情報について、特定の個人を識別することができる記述等の全部又は一部を削除する [20]措置を定めるものである。

法第２条第 1 項第１号に基づき「特定の個人を識別することができるもの(記述)」については、「個人情報の保護に関する法律についてのガイドライン（通則編）」（以下「通則ガイドライン」という。）において次のような事例が例示されている。

通則ガイドライン 2-1

事例 1）本人の氏名

事例 2）生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報

事例 3）防犯カメラに記録された情報等本人が判別できる映像情報

事例 4）本人の氏名が含まれる等の理由により、特定の個人を識別できる音声録音情報

事例 5）特定の個人を識別できるメールアドレス（kojin_ichiro@example.com 等のようにメールアドレスだけの情報の場合であっても、example 社に所属するコジンイチロウのメールアドレスであることが分かるような場合等）

事例 6）個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できる場合は、その時点で個人情報に該当する。）

事例 7）官報、電話帳、職員録、法定開示書類（有価証券報告書等）、新聞、ホームページ、SNS（ソーシャル・ネットワーク・サービス）等で公にされている特定の個人を識別できる情報

施行規則第 19 条第 1 号において措置を求められる「特定の個人を識別することができる記述等」は、ガイドラインに記載の【想定される加工の事例】のように、情報単体又は組合せにより特定の個人を識別することができる個人情報といえるものが対象になる。

講ずるべき措置として、「記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）」が求められている。単独で特定の個人を識別することができる記述等（氏名、顔画像等）についてはその全部を削除するとともに、組合せで特定の個人を識別することができる記述等についてはその組合せが特定の個人を識別することができる記述にならないように、記述等の全部又は一部を削除する必要がある。

[20] 法第 2 条第 9 項第 1 号で「・・・記述等の一部を削除」とあるのに対して、ここで「・・・記述等の全部又は一部を削除」となっているのは、例えば、特定の個人を識別することができる情報が氏名しかない場合等については、記述等を削除する場合に全部を削除することも当然にあり得るため、そのことを単に明確に示したものである。

具体的な加工方法としては、ガイドラインの事例にあるように、例えば、住所であれば「○○市」まで（人口の多い都心部であれば、「○○区」まで）、生年月日であれば「生年月」まで、あるいは「生年」までといったように、情報の項目それぞれについて一定程度曖昧化されるように部分的な削除や置換えを行う考え方が想定される。また、住所・生年月日・性別等の複数の項目の組合せで一意にならないように各項目の加工レベルを調整する考え方も想定される[21]。

また、携帯電話番号や電子メールアドレス、SNS 等の ID[22]、クレジットカード番号等は、法人の所有する番号との区別がつかない等の理由により特定の個人を識別し得る符号ではないとして、個人識別符号からは除外されているものではあるが、一般的に本人と密接に関係する情報であり、事業者において単体又は他の情報との組合せによりこれらの情報が特定の個人のものとして認識されている場合については、個人情報として扱われるべきものである。

特に、これらの情報については、多数の事業者においてそれぞれユーザーから取得されていることを踏まえると、他の事業者が保有している個人情報との間で識別子的な機能も有することから、部分的な削除だけでは、残った情報を起点として個人の特定につながる可能性も高くなると思われるため、基本的には、全部削除することが望ましい[23]。

【仮 ID への置き換えについて】

匿名加工情報の作成においては、特定の個人を直接的に識別可能とする情報を削除することのほか、「特定の個人を直接的に識別可能な属性又はその組合せ（例えば、氏名＋連絡先）を、元の個人情報を復元できる規則性を有しない方法により置き換えること」も認められている。この際、元の個人情報を符号や番号等で置き換えた場合には、当該符号や番号等は仮 ID と捉えることができる。

仮 ID を付す方法としては、例えば、特定の個人を直接識別し得る一意の情報（氏名やサービス ID 等）や個人識別符号、又はそれらの組合せからなる入力（以下「入力情報」という。）それぞれに対して、所定のアルゴリズムにより出力される数値や記号列を付番するほか、氏名やサービス ID 等の一意の情報を削除した後にランダムに番号や記号等を付番する処理等の手法が想定される。一方、匿名加工情報の加工の要件として、「復元できる規則性を有しないように置き換え」る必要があるため、仮 ID を用いる場合には、元の個人情報を復元することができないように仮 ID を生成する必要がある。仮 ID による置換えを行う場合は、その際に使用する手法の長所・短所を把握した上で行うことが必要である。

仮 ID を付与することにより、異なるデータセット間における同一人物のデータを紐づけることが可能となるため、特に次のような場合には注意が必要である。

ある個人に関する仮 ID を共通のまま複数事業者に提供した場合、それらの事業者間でその個人に関する手持ちのデータを連結できるおそれがある。こうした事態をさけるため、提供先事業者間で共通とならないような仮 ID を付番することが望ましい。このためには仮 ID の生成方法を提供する事業者に応じて変更するか、同一の生成方法であっても、何らかのパラメータによって、共通の仮 ID を付番しないようにすることが望ま

---

[21] 匿名加工情報に関する技術検討ワーキンググループ「匿名加工情報の適正な加工の方法に関する報告書 2017 年 2 月 21 日版」（http://www.nii.ac.jp/about/reports/pd/report-kihon-20170221.pdf）においては、「単項目型加工」と「複項目加工」という分類で解説されている。

[22] 近年は、Open ID の仕組み等により、SNS 等の ID を別の WEB サービスのアカウントとして使用するような動きも出てきているため、これらの ID による名寄せも起こり得ると考えられる。

[23] なお、携帯電話番号の最初の 3 桁やクレジットカード番号の発行者識別番号等の部分に個人の識別性はないため、この部分を残すことは問題ないと考えられるが、その部分を何らかの分析に使う目的等がなければ、削除しておくことが好ましいことはいうまでもない。

しい。その方法の 1 つは、ハッシュ関数等を用いる際に、その入力情報に提供する事業者ごとに異なる記号列や乱数等を加えることである。

また、同じ事業者に複数回にわたって匿名加工情報を提供する場合は、同一の人物の情報が蓄積され続けることにより、元の個人情報に係る本人を識別できるリスクが高くなることも想定される。したがって、同一事業者への提供であっても、定期的に仮 ID を変更することが望ましい。

なお、仮 ID が不要である場合には、再識別リスクを低減する意味からも、仮 ID への置き換えを行わないことが望ましい。

【ハッシュ関数による置き換えについて】

仮 ID に置き換える処理を行う際には、元の記述が復元されたり推定されたりしないようにすべきであり、その代表的な処理方法としてハッシュ関数を用いたハッシュ化がある。ハッシュ化とは、元のデータから一定の計算手順に従ってハッシュ値と呼ばれる規則性のない固定長の値を求め、その値によって元のデータを置き換える方法であり、ハッシュ関数と呼ばれる特殊な計算手順により、任意長の長さのデータから固定長の一見ランダムに思えるハッシュ値を得ることができる。

同じデータからは常に同じハッシュ値が得られる一方で、少しでもデータが異なるとまったく類似しない別のハッシュ値が生成されるため、ハッシュ値から元のデータを割り出したり、同じハッシュ値を持つ別のデータを生成したりすることは極めて難しいことから、匿名加工の際の仮 ID の生成方法の一つとして使用されることが多い。

ただし、同じデータからは常に同じハッシュ値が得られるということは、名前や電子メールアドレス、携帯電話番号等の多くの事業者が保有するような情報のみでハッシュによる仮 ID を生成すると、提供を受けた事業者において仮 ID の生成に用いられた入力情報を推測することが容易となるおそれがあることを意味する。したがって、ハッシュによる仮 ID 生成に当たっては、（氏名＋秘密の文字列）、（氏名＋電子メールアドレス＋秘密の文字列）といったように、鍵となる秘密の文字列を付加した上でハッシュ化をすること（いわゆる鍵付きハッシュ関数の利用）が望ましい[24]。

なお、ハッシュ関数のアルゴリズムについては、安全性が確立されたものを利用することが望ましいと考えられるところ、例えば、CRYPTREC により公開されている電子政府推奨暗号リスト[25]において挙げられているハッシュ関数を利用することも安全性の観点から推奨される。

4.1.2 第 2 号（個人識別符号の削除）

施行規則第 19 条第 2 号

個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

ガイドライン 3-2-2 個人識別符号の削除

加工対象となる個人情報が、個人識別符号を含む情報であるときは、当該個人識別符号単体で特定の個人を識別できるため、当該個人識別符号の全部を削除又は他の記述等へ置き換えて、特定の個人を識別できないようにしなければならない。

なお、他の記述等に置き換える場合は、元の記述等を復元できる規則性を有しない方法による必要が

[24] Article 29 Data Protection Working party（EU 第 29 条作業部会）によるオピニオン“Opinion 05/2014 on Anonymisation Techniques“においても、「入力値によるリプレイが可能であること、ブルート・フォース攻撃の問題があること等から、十分に大きく予測困難な鍵を用いた鍵付きハッシュ関数を利用する等の配慮が好ましい」旨についての記載がある。

[25] CRYPTREC 暗号リスト（電子政府推奨暗号リスト）（http://www.cryptrec.go.jp/list.html）。

ある。

（参考）個人識別符号の概要

個人識別符号とは、その情報単体から特定の個人を識別することができるものとして個人情報の保護に関する法律施行令（平成 15 年政令第 507 号。以下「政令」という。）で定めるものをいい、次のいずれかに該当するものである。（個人識別符号の定義の詳細については、通則ガイドライン 2-2（個人識別符号）参照）

（1）特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した符号

・ 生体情報（DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋）をデジタルデータに変換したもののうち、特定の個人を識別するに足りるものとして規則で定める基準に適合するもの 【政令第 1 条第 1 号、規則第 2 条】

（2）対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号

・ 旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証の番号等の公的機関が割り振る番号 【政令第 2 条～第 7 条、規則第 3 条、第 4 条】

施行規則第 19 条第 2 号は、法第 2 条第 9 項第 2 号で規定される措置を定めるものである。

個人の身体の一部の特徴を電子計算機の用に供するため変換し特定個人を識別することができる法第 2 条第 2 項第 1 号で規定される個人識別符号及び旅券番号や運転免許証の番号、個人番号等、法第 2 条第 2 項第 2 号で規定される個人識別符号については、その符号自体が特定の個人に割り当てられるものであり、個人識別符号単体で特定の個人を識別し得る情報であるとの位置付けから、それらを全部削除することが求められる。なお、仮 ID への置き換えについては、4.1.1 の考え方と同様である。

なお、法第 2 条第 2 項第 1 号で定める個人識別符号の「規則で定める基準」について、通則ガイドラインにおける個人識別符号の解説においては、「本人を認証することができるようにしたもの」（DNA）或いは「本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの」とされている。

4.1.3 第 3 号（情報を相互に連結する符号の削除）

施行規則第 19 条第 3 号

個人情報と当該個人情報に措置を講じて得られる情報を連結する符号（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該個人情報と当該個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。）。

ガイドライン 3-2-3 情報を相互に連結する符号の削除

個人情報取扱事業者が個人情報を取り扱う上で、例えば、安全管理の観点から取得した個人情報を分散管理等しようとするために、当該個人情報を分割あるいは全部又は一部を複製等した上で、当該個人情報に措置を講じて得られる情報を個人情報と相互に連結するための符号として ID 等を付していることがある。このような ID は、個人情報と当該個人情報に措置を講じて得られる情報を連結するために用いられるものであり、特定の個人の識別又は元の個人情報の復元につながり得ることから、加工対象となる個人情報から削除又は他の符号への置き換えを行わなければならない。

個人情報と当該個人情報に措置を講じて得られる情報を連結する符号のうち、「現に個人情報取扱事業者において取り扱う情報（※1）を相互に連結する符号」がここでの加工対象となる。具体的には、ここで対象となる符号は、匿名加工情報を作成しようとする時点において、実際に取り扱う情報を相互に連結するように利用されているものが該当する。例えば、分散管理のための ID として実際に使われているものであれば、管理用に附番された ID あるいは電話番号等もこれに該当する。

なお、他の符号に置き換える場合は、元の符号を復元できる規則性を有しない方法でなければならない。

【想定される加工の事例】

事例 1）サービス会員の情報について、氏名等の基本的な情報と購買履歴を分散管理し、それらを管理用 ID を付すことにより連結している場合、その管理用 ID を削除する。

事例 2）委託先へ個人情報の一部を提供する際に利用するために、管理用 ID を付すことにより元の個人情報と提供用に作成した情報を連結している場合、当該管理用 ID を仮 ID（※2）に置き換える。

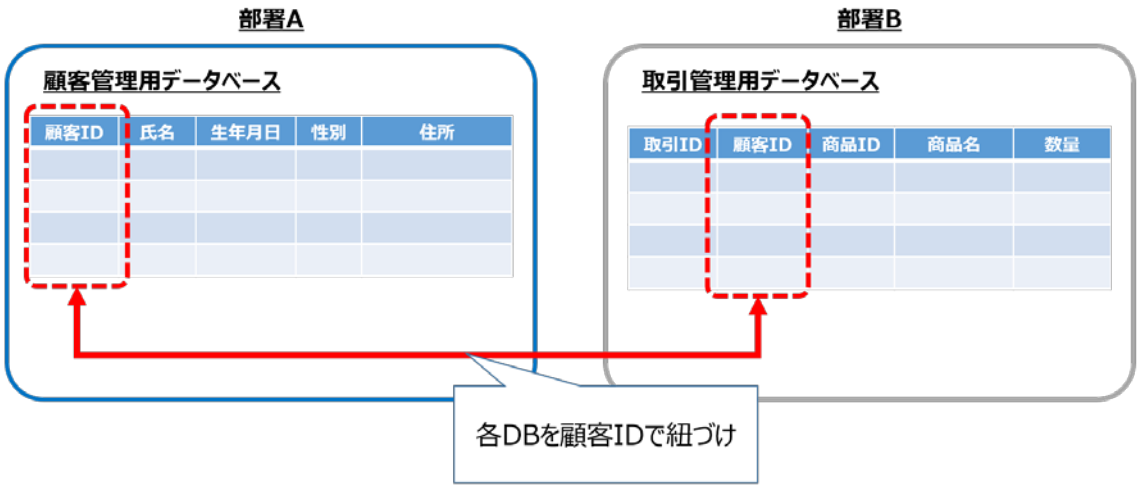
（※1）「現に個人情報取扱事業者において取り扱う情報」とは、匿名加工情報を作成する時点において取り扱われている情報のことを指し、これから作成する匿名加工情報は含まれない。

（※2）仮 ID を付す際の注意点については、3-2-1（特定の個人を識別することができる記述等の削除）の（※）を参照のこと。

施行規則第 19 条第 3 号は、事業者内で、個人情報を分散管理したり、取扱いの委託等をしたりするために、分けたデータベース等を相互に連結するために割り当てられている ID 等を削除することを求めるものである。

事業者においては、個人情報を取り扱う際の安全管理の一環や事業者間における個人情報の共同利用における管理の一形態として、図表 4-1 のように個人情報のデータベースを複数に分けて管理するような場合も想定される。

図表 4-1　施行規則第 19 条第 3 号で削除を求める“符号”のイメージ



なお、ここでいう「連結する符号」とは、個人情報と当該個人情報に措置を講じて得られる情報とを相互に連結する符号であり、ID ではなくても、実務上、他の属性情報等（例えば、電話番号や電子メールアドレス）を連結の目的で使用している場合には、当該属性情報も「連結する符号」とみなされる。

ただし、本号はあくまでも現に連結の目的で使用されている符号を対象としたものであり、それ以外の情報については、同条第 3 号による削除の対象とはされていない。

なお、同条第 3 号による削除の対象とされている符号は、現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限られるため、匿名加工情報への加工により新たに作成された符号を対象とするものではない。

4.1.4 第 4 号（特異な記述等の削除）

施行規則第 19 条第 4 号

特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

ガイドライン 3-2-4 特異な記述等の削除

一般的にみて、珍しい事実に関する記述等又は他の個人と著しい差異が認められる記述等については、特定の個人の識別又は元の個人情報の復元につながるおそれがあるものである。そのため、匿名加工情報を作成するに当たっては、特異な記述等について削除又は他の記述等への置き換えを行わなければならない。

ここでいう「特異な記述等」とは、特異であるがために特定の個人を識別できる記述等に至り得るものを指すものであり、他の個人と異なるものであっても特定の個人の識別にはつながり得ないものは該当しない。実際にどのような記述等が特異であるかどうかは、情報の性質等を勘案して、個別の事例ごとに客観的に判断する必要がある。

他の記述等に置き換える場合は、元の記述等を復元できる規則性を有しない方法による必要がある。例えば、特異な記述等をより一般的な記述等に置き換える方法もあり得る。

なお、規則第 19 条第 4 号の対象には、一般的なあらゆる場面において特異であると社会通念上認められる記述等が該当する。他方、加工対象となる個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等とで著しい差異がある場合など個人情報データベース等の性質によるものは同第 5 号において必要な措置が求められることとなる。

【想定される加工の事例】

事例 1）症例数の極めて少ない病歴を削除する。
事例 2）年齢が「116 歳」という情報を「90 歳以上」に置き換える。

施行規則第 19 条第 4 号で削除が求められる「特異な記述等」とは、一般的なあらゆる場面において特異であると“社会通念上認められる”記述等が該当する。具体的には、ガイドラインで例示されている「超高年齢」や「症例数の極めて少ない病歴」の他、超高身長であることや超高収入であること等、主に個人に関する基本的な属性に係る記述等が考えられる。

「どのような情報のどこからが特異な記述や特異値になるか」ということについては、その情報の項目の性質

や集団の大きさ、集団の分布の特徴等を考慮して判断されるべきものであるが、社会通念上特異であるものが対象になるため、特異であるものであっても、分布の調査結果が存在しないもの、存在したとしても一般人には知りえないものについては、本号の「特異」には該当しないものと考えられる。

なお、同条第 4 号は一般的に特異な記述等が対象となるため、加工対象となる個人情報からなるデータベース内において顕著な値である場合でも、それだけでは本号の「特異」には該当しない。加工対象のデータベース内において顕著な値については、同条第 5 号による措置の対象となり得るものである。

4.1.5 第 5 号（個人情報データベース等の性質を踏まえたその他の措置）

施行規則第 19 条第 5 号

前各号に掲げる措置のほか、個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し、その結果を踏まえて適切な措置を講ずること。

ガイドライン 3-2-5 個人情報データベース等の性質を踏まえたその他の措置

匿名加工情報を作成する際には、規則第 19 条第 1 号から第 4 号までの措置をまず講ずることで、特定の個人を識別できず、かつ当該個人情報に復元できないものとする必要がある。

しかしながら、加工対象となる個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等とで著しい差異がある場合など、加工の元となる個人情報データベース等の性質によっては、規則第 19 条第 1 号から第 4 号までの加工を施した情報であっても、一般的にみて、特定の個人を識別することが可能である状態あるいは元の個人情報を復元できる状態のままであるといえる場合もあり得る。そのような場合に対応するため、上記の措置のほかに必要となる措置がないかどうか勘案し、必要に応じて、別表 1（匿名加工情報の加工に係る手法例）の手法などにより、適切な措置を講じなければならない。

なお、加工対象となる個人情報データベース等の性質によって加工の対象及び加工の程度は変わり得るため、どの情報をどの程度加工する必要があるかは、加工対象となる個人情報データベース等の性質も勘案して個別具体的に判断する必要がある。

特に、購買履歴、位置に関する情報などを含む個人情報データベース等において反復して行われる行動に関する情報が含まれる場合には、これが蓄積されることにより、個人の行動習慣が分かるような場合があり得る。そのような情報のうち、その情報単体では特定の個人が識別できるとは言えないものであっても、蓄積されたこと等によって特定の個人の識別又は元の個人情報の復元につながるおそれがある部分については、適切な加工を行わなければならない。

【想定される加工の事例】

事例１）移動履歴を含む個人情報データベース等を加工の対象とする場合において、自宅や職場などの所在が推定できる位置情報（経度・緯度情報）が含まれており、特定の個人の識別又は元の個人情報の復元につながるおそれがある場合に、推定につながり得る所定範囲の位置情報を削除する。（項目削除／レコード削除／セル削除）

事例 2）ある小売店の購買履歴を含む個人情報データベース等を加工の対象とする場合において、当該小売店での購入者が極めて限定されている商品の購買履歴が含まれており、特定の個人の識別又は元の個人情報の復元につながるおそれがある場合に、具

体的な商品情報（品番・色）を一般的な商品カテゴリーに置き換える。（一般化）

事例 3）小学校の身体検査の情報を含む個人情報データベース等を加工の対象とする場合において、ある児童の身長が 170 ㎝という他の児童と比べて差異が大きい情報があり、特定の個人の識別又は元の個人情報の復元につながるおそれがある場合に、身長が 150cm 以上の情報について「150 ㎝以上」という情報に置き換える。（トップコーディング）

施行規則第 19 条第 5 号は、同条第 1 号～第 4 号の加工を施してもなお、「特定の個人を識別することが可能である状態あるいは元の個人情報を復元できる状態である」場合に、追加で講ずるべき措置である。第 5 号は、「個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案」することが必須であり、その結果、更に加工が必要と判断した場合に、追加的に措置を講ずることになる。

なお、ここで対象となる個人情報データベース等については、「「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A（平成 29 年 2 月 16 日 ）」でも説明があるとおり、事業者内にある個人情報データベース全部を対象とするものではなく、匿名加工情報データベース等を構成する匿名加工情報の作成の元となる個人情報で構成される個人情報データベース等の単位で検討することを求めるものである。

Q11-9

施行規則第 19 条第 5 号において、「個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し」とありますが、ここでの「当該個人情報を含む個人情報データベース等」については、事業者が保有する個人情報データベース等全体を勘案する必要がありますか。

A11-9

ここでの「当該個人情報を含む個人情報データベース等」とは、当該個人情報取扱事業者が匿名加工情報を作成する際に加工対象とする個人情報データベース等を想定しています。すなわち、匿名加工情報を作成する個人情報取扱事業者が保有する、加工とは無関係の個人情報を含むすべての個人情報データベース等の性質を勘案することを求めるものではありません。

4.1.5.1 「個人情報に含まれる記述等と～他の個人情報に含まれる記述等との差異」

「個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異」とは、加工対象である個人情報からなるデータベース内のある個人情報に含まれる記述と、当該データベースに含まれる他の個人情報に含まれる記述の間の差異をいう。また、これを勘案するとは、加工対象の個人情報からなる個人情報データベース等において値や記述等が相対的に特異であることによって特定の個人の識別につながり得るかを検討することを意味する。

例えば、都心部在住の人を対象としたデータベースと地方在住の人を対象としたデータベースでは、そのデータベースに含まれる人の年齢分布や職業分布等の構成が異なることが想定される。このように、日本全国を対象とする集団の分布とは異なるデータベースでは、そのデータベース内における値や記述

の特異性によって、特定の個人を識別しやすい状況が生じることが想定される。

4.1.5.2 「その他の～適切な措置」が求められる場合

例えば、詳細な位置情報（移動履歴）を扱うデータベースや、長期間の購買情報を扱うデータベースは、そこに蓄積される情報から、反復して行われる行動習慣や趣味・嗜好を読み取ることが可能である。そのような履歴情報から読み取れる行動習慣等ついては、一般的には特定の個人を識別することは困難であると思われるが、特に顕著な行動習慣等については特定の個人の識別につながることもあり得る[26]。

施行規則第 19 条第 5 号は、このような個人情報データベースに含まれる情報の性質に起因して生じる特定の個人の識別可能性を低減することを求めるものである。

【不変性の高い ID、多数の事業者で取得されるサービス ID 等】

不変性の高い ID として同条第 5 号で検討するものは、個人に密接に関係しかつ当該個人が容易に変更することができない外部から観察可能な符号のうち(a)個人識別符号及び(b)それ以外の単体で個人情報になるものを除いたものをいう[27]。具体的には、スマートフォンのように個人がある程度の期間使用しかつ日常的に携行する機器の ID 等がこれに当たる。

不変性の高い ID は、それをキーとする名寄せが可能であり、再識別につながる可能性のある情報と考えることができることから、原則としてこれを削除することが望ましい。

【時刻に関する情報について】

購買履歴やクレジットカードの利用履歴、移動履歴等の情報は、基本的に詳細な時刻情報とともにデータベースに記録されるのが一般的である。

例えば、店舗情報を含む購買履歴に関するデータベースからは、ある日時に買い物をした店舗を特定することができる。一方、移動履歴に関するデータベースからも、ある日時に滞在した場所に関する位置情報を確認することができる。この両者のデータベースを照合した場合、店舗の場所からおおよその緯度・経度（位置情報）を推定することが可能であるため、両者のデータベースが日時分秒まで記録されている場合には、両方のデータベースに含まれる同一人物の同定を比較的容易に行うことができる可能性がある。つまり、詳細な時刻情報は、位置や場所を表す情報とセットになることで、異なるデータセット間における共通の識別子として機能し得る。

したがって、詳細な時刻情報を含むデータベースを匿名加工情報として第三者提供をする場合には、時刻情報の必要性について確認した上で、データの性質に応じて、時刻と位置（場所）の情報の紐づけから特定の個人を識別するリスク等を低減するため、時刻情報を一定程度曖昧化したり、ノイズを加えて任意の日時や時刻に置き換えたりすることを検討する等、他のデータセットに含まれる時刻情報と紐づくリスクを低減することが望ましい。

---

[26] 購買履歴や移動履歴のような履歴情報については、個人の習慣的・反復的傾向が現れる可能性があり、これが異なるデータセット間における識別子として機能する可能性もある。そのようなリスクがあることを認識した上で、必要に応じて加工を行うことが望ましい。なお、匿名加工情報に関する技術検討ワーキンググループ「匿名加工情報の適正な加工に関する報告書　2017 年 2 月 21 日版」においても、「同一の本人の同一の履歴を同一の提供先に複数回提供する場合には、この履歴が仮 ID として機能する可能性があることに注意すべきである」と記載されている。

[27] 個人識別符号は施行規則第 19 条第 2 号により、それ以外の単体で個人情報となるものについては同条第 1 号により、既に削除又は置き換えがなされている。

【位置情報（移動履歴）について】

一般的に、位置情報それ自体のみでは個人情報には該当しないものではあるが、ある個人に関する位置情報が連続的に蓄積されるとその人の移動履歴を表し得る。特に、深夜に滞在している地点や日中に滞在している地点を表す位置情報からは、その移動履歴に係る本人の自宅や勤務先等の個人に関する基本的な属性を推測することも可能である。蓄積された位置情報や移動履歴等から自宅住所及び勤務先等の特定の個人に密接に結びつき得る情報が推定されるおそれがある場合には、当該情報等を用いて特定の個人の識別が可能となるリスクを十分考慮した上で移動履歴について加工を行うことが望ましい。

また、移動履歴は長くなるほど他人と重複する可能性が低く一意な情報となる[28]という特徴のほか、都市部と地方、昼間と夜間等、環境や状況に応じて同じ範囲から取得できる位置情報の数が変わる、といった特徴もあるため、位置情報や移動履歴の性質を考慮した上で、措置を講ずることが望ましい[29]。

4.2 匿名加工情報を作成する際に検討することが望ましい事項

匿名加工情報は、一般人及び一般的な事業者の能力や手法等を基準として「特定の個人を識別することができないように」かつ「復元されないように」加工することを求められるものであるが、匿名加工情報の作成に用いられる個人情報の性質のほか、匿名加工情報としての利用用途や再識別リスクの見積り方[30]によって、加工レベルに一定の幅が生じるものと考えられる。

したがって、匿名加工情報を作成する際の加工方針を決めるに当たっては、次のような事項について検討することが望ましい。

4.2.1 匿名加工情報の利用形態について

匿名加工情報への加工方針を検討する際、次に列挙するような匿名加工情報の利用目的・利用形態を予め検討することは、匿名加工情報の安全性と有用性を両立するために有用と考えられる。

（１） 匿名加工情報の利用目的は何か

匿名加工情報をどのような目的で利用するかによって必要とされる項目やその情報の粒度（精度）は異なり得る。利用目的に応じて不要な項目は削除し、必要な項目の情報粒度を細かくする等、全体として安全性と有用性の両立を図る加工方法を検討することが望ましい。

（２） 第三者提供時に、データの流通範囲が限定されているか、転々流通を許容するか

---

[28] Hiroaki Kikuchi＆Katsumi Takahashi, “Zipf Distribution Model for Quantifying Risk of Re-identification from Trajectory Data” Journal of Information Processing, Vol.24(2016) No.5, pp.816-823 では、鉄道の乗降履歴の履歴長（利用した駅の情報数）による一意性について報告されている。

[29] 位置情報に関しては、2014 年 7 月に総務省が公表した『位置情報プライバシーレポート』（http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000144.html）においても、位置情報の取扱いの在り方や匿名化手法の例が言及されている。

[30] 脅威のモデリングとリスクの定量化をして匿名化を検討するリスクベース方法論等もある（Khaled El Emam＆Luk Arbuckle 著（笹井崇司訳）『データ匿名化手法』（オライリー・ジャパン、2015 年）ほか）。

例えば、契約により提供先からの二次流通を禁止する等して特定の事業者に限定して提供する場合、提供先における匿名加工情報の利用目的を把握することが比較的容易である一方、提供先からのデータの転々流通を許容する場合、二次流通先での用途や他の情報との突合可能性について把握することが困難である。匿名加工情報が特定の会社だけに留まる場合と、制限なく流通する場合では、流通先における再識別リスクが異なることは、容易に想像できる。

（３） 提供するデータの期間

1 か月間のデータに含まれる履歴情報と 1 年間のデータに含まれる履歴情報とでは、そこから読み取れる履歴情報に係る本人の行動習慣には大きな差が生じ得る。その蓄積量によって特定個人の識別性や元の個人情報への復元性に影響するかどうかを検討することが望ましい。

また、一度に提供されるデータに含まれる履歴情報の期間が短くても、同一の事業者に対して継続的にデータが提供される場合、結果として、データに含まれるトータルの期間が長くなる。このような場合に再識別リスクを低減する方法の一つとして、定期的に仮 ID を変更することも有効である。

（４） 継続的に匿名加工情報を提供する場合

複数回にわたって匿名加工情報を提供する際に、各回のデータセット間での同一人物の紐づけを抑制すべく、仮 ID を付けずに提供したり、提供の度に仮 ID を変更したりするような場合も想定される。この場合に、都度提供される匿名加工情報データベースにおけるレコードの並びが同じであったり、提供されるデータセットが対象としている期間に重複があったりすると、データセット間の紐づけが容易となってしまう。したがって、複数回にわたって提供する匿名加工情報データベース間でレコードが紐づけられることを抑制したい場合は、レコードの並びを変更したり、データセットが対象としているデータに重複期間が生じないように加工したりすることが必要である。

また、過去に匿名加工情報を提供したことのある事業者に対して、異なる情報の項目からなる匿名加工情報を作成して提供しようとするときは、過去に提供した匿名加工情報と照合されることによって元の個人情報が復元されないよう、同じ仮 ID を使用しないようにする等の注意が必要である。過去に提供した匿名加工情報と異なる情報の項目からなる匿名加工情報については、新たに作成時や第三者提供時の公表義務が発生する点には注意が必要である。

4.2.2 他の情報を参照することによる識別の可能性について

匿名加工情報は「特定の個人を識別することができないように」加工することが求められるが、匿名加工情報の制度は、その流通過程における安全性を確保しつつパーソナルデータの利活用を図る制度であるため、一般的に入手し得る他の様々な情報と参照することによる識別の可能性を検討することが望ましい。

この検討に当たっては、3.2 の説明のとおり、一般人や一般的な事業者の通常の能力や取り得る手法等を基準となるが、例えば、「入手し得る情報の種類」と「情報のマッチングのしやすさ」の観点から考えることができる。

入手し得る情報の種類としては、次のようなものを想定することができる。

① 一般に広く公開、市販されている情報（例：電話帳）
② 多数の事業者がユーザー登録等により取得している情報（例：電子メールアドレス、電話番号等）
③ 関係の近い者のみが知り得る情報（例： SNS に掲載された情報のうち公開制限があるもの等）

一方、情報のマッチングのしやすさについては、次のような観点から分類することができる。

(i) 情報の項目とそれに対応する記述等が整理されており、機械的なマッチングがしやすい場合

(ii) 情報の項目とそれに対応する記述等が非定型であり、マッチングに複雑なアルゴリズムや機械学習等が必要な場合

入手し得る情報の種類のうち、①や②については入手が容易と考えられる一方、③については、一部の関係者のみが知り得る情報であり、一般人や一般的事業者を基準として入手容易とは言い難いと考えられる。

後者のマッチングしやすさについては、匿名加工情報の要件に係る判断基準からは(i)が対象であると考えられるが、その作成時点での技術水準が考慮されるべきであり、汎用的に使用できる機械学習ツール等が広く利用されるようになった場合には、それについても将来的に(i)に含み得る。

他の情報を参照することによる識別の可能性については、これらの組合せから総合的に判断することができるが、識別の可能性が高いと判断される場合には、匿名加工情報としての要件を満たすために、それぞれ対象となる情報の項目について、加工の程度を変更するほか、対象となるデータセットで情報の一意性を無くす等の措置を行うことが考えられる。

【他の情報を参照することによって再識別につながった事例】

次に示すケースは、一般に公開されたデータセット同士を突合したものであり、識別行為の禁止が前提となっている匿名加工情報の場合にそのまま当てはめて考えるべきものではないが、他の情報を参照することによって再識別された典型的なケースとして、加工レベルを検討する際の参考となるものである。

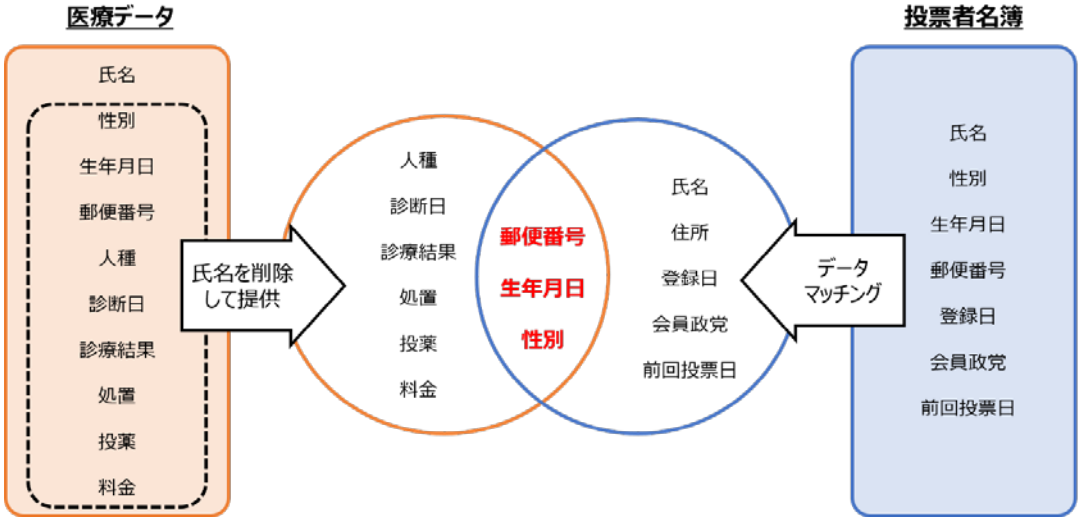
（例）性別と生年月日と郵便番号（居住エリア）の組合せによって再識別につながった事例

マサチューセッツ州は医療データから氏名等を削除したデータセットを公開しており、そのデータセットには、性別、生年月日、郵便番号が含まれていた。

これに対し、既に公開されている投票者名簿とマッチングしたところ、州知事と同じ生年月日のレコードが 6 人おり、うち 3 人が男性で、郵便番号から 1 人に特定された。[31]

[31] L.Sweeney, “k-Anonymity: A Model For Protecting Privacy” International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), pp. 557-570, 2002. は、このような他の情報と照合することよって特定の個人が識別されることを防止するための匿名性の評価指標として、“k-匿名性”を提案している。

図表 4-2　性別、生年月日、郵便番号により個人が特定された事例



日本の事情に関して考えると、全国の郵便番号の総数は約 12 万個であり、20 代の人の取り得る生年月日のパターンは、約 3650 通りとなる。ここに、性別の情報（男/女）が組み合わさると、同じ郵便番号×同じ生年月日×同じ性別を取り得る確率がいかに少ないかをイメージすることができる。

なお、情報が一意であることをもって直ちに匿名加工情報の要件を満たさないものではない。

4.3　匿名加工情報の作成のための参考情報

4.3.1　匿名加工に用いられる代表的な加工手法

個人情報の匿名加工に用いられる代表的な手法を、図表 4-3 に示す。なお、ここに示す各手法は、一般的な加工手法を例示したものであり、その他の手法を用いて適切に加工することを妨げるものではない。

図表 4-3　代表的な加工手法

手法名	解説
項目削除	加工対象となる個人情報データベース等に含まれる個人情報の項目を削除するもの。例えば、年齢のデータを全ての個人情報から削除すること。
レコード削除	加工対象となる個人情報データベース等に含まれる個人情報のレコードを削除するもの。例えば、特定の年齢に該当する個人のレコードを全て削除すること。
セル削除	加工対象となる個人情報データベース等に含まれる個人情報の特定のセルを削除するもの。例えば、特定の個人に含まれる年齢の値を削除すること。
一般化	加工対象となる情報に含まれる記述等について、上位概念若しくは数値に置き換えること。例えば、購買履歴のデータで「きゅうり」を「野菜」に置き換えること。
トップ（ボトム）コーディング	加工対象となる個人情報データベース等に含まれる数値に対して、特に大きい又は小さい数値をまとめることとするもの。例えば、年齢に関するデータで、80 歳以上の数値データを「80 歳以上」というデータにまとめること。
レコード一部抽出	加工対象となる個人情報データベース等に含まれる個人情報の一部のレコードを

手法名	解説
	(確率的に)抽出すること。いわゆるサンプリングも含まれる。
項目一部抽出	加工対象となる個人情報データベース等に含まれる個人情報の項目の一部を抽出すること。例えば、購買履歴に該当する項目の一部を抽出すること。
ミクロアグリゲーション	加工対象となる個人情報データベース等を構成する個人情報をグループ化した後、グループの代表的な記述等に置き換えることとするもの。
丸め(ラウンディング)	加工対象となる個人情報データベース等に含まれる数値に対して、四捨五入等して得られた数値に置き換えることとするもの。
データ交換 （スワッピング）	加工対象となる個人情報データベース等を構成する個人情報相互に含まれる記述等を（確率的に）入れ替えることとするもの。例えば、異なる地域の属性を持ったレコード同士の入れ替えを行うこと。
ノイズ（誤差）付加	一定の分布に従った乱数的な数値等を付加することにより、他の任意の数値等へと置き換えることとするもの。
疑似データ生成	人工的な合成データを作成し、これを加工対象となる個人情報データベース等に含ませることとするもの。

4.3.1.1 k－匿名性について

データの匿名性を評価する代表的な方法として、k-匿名性という評価指標がある [32]。対象となるデータセット内に、同じ属性を持つデータが k 件以上存在することを「k-匿名性を満たす」といい、k-匿名性を満たすようにデータを加工することで、個人が特定される確率を k 分の 1 以下に低減させることが可能である。

L.Sweeneyは、先に述べたマサチューセッツのケースにおいては、元のデータセットにある情報の項目のうち性別、生年月日、郵便番号の 3 つを、外部のデータセットと結びつくことにより個人の特定が可能な情報である準識別子（Quasi-Identifier）として、これら準識別子の情報を公開する場合には加工がされるべきとしている。

匿名加工情報は、上記ケースのように必ずしも一般公開されるものではないから、上記で準識別子とされている情報の項目について、匿名加工情報データベース等との関係で $k \geqq 2$ となるように加工することは必ずしも求められない。ただし、匿名加工情報が第三者に提供される態様や利用形態を考慮した上で、必要に応じてこのような考え方を取り入れることが望ましい。

4.3.1.2 レコード一部抽出について

レコード一部抽出とは、加工対象となる個人情報データベース等に含まれる個人情報（レコード）を一定の割合（あるいは一定の個数）抽出することである。いわゆるサンプリング [33]もこの手法に含まれる。

この手法は、それぞれの個人情報に対して加工を施す手法ではないため、情報自体の識別性を低減するものではないが、元の個人情報データベース等に含まれていた個人情報が匿名加工情報データベース等にも入っているか否かの確度を下げる効果がある。

---

[32] L.Sweeney, “k-Anonymity: A Model For Protecting Privacy”, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), pp. 557-570, 2002.

[33] 母集団の対象となる個人情報データベース等から、一部のレコードを無作為に抽出すること。

なお、レコード一部抽出を行ったとしても、個人情報データベース等を構成するそれぞれの個人情報に含まれる数値や記述等の傾向（例えば、年齢分布や地域分布）を維持するような形でレコードを抽出することにより、データの有用性を保つ効果も期待できる。

4.3.2 情報の項目と想定されるリスク及び加工例

特定の個人を識別できるリスクについては情報の性質によって異なることから、加工に当たっての参考となるよう、加工対象となる個人情報に含まれ得る各情報の項目に対する加工例を図表 4-4 に示す。ここでは、個人情報に係る本人の基本的な属性に関わる情報の項目を「個人属性情報」、個人の行動に伴い発生する行動の履歴に関わる情報の項目を「履歴情報」として分類している。

ただし、次に示す加工例はあくまで基本的な考え方に沿った一般的な加工の例示であり、次のとおりに加工すれば十分であることを意味するものでもなければ、これに縛られるものでもない。実際にどの情報の項目をどこまで加工するかということについては、業種やビジネスの業態、需要者のニーズ等を踏まえつつ、データベースに含まれる情報の項目やレコードの数等に応じて判断することが適当であることから、認定団体が策定する個人情報保護指針等の自主ルールにおいて適切に定められることが望ましい。

図表 4-4 情報の項目と想定されるリスク及び加工例

項目		想定されるリスク	加工例 （「削除」は置き換えも含む）
個人属性情報	**氏名**	・それ自体で個人を特定できる。	全部削除
	生年月日	・住所（郵便番号）、性別との組合せにより、個人の特定につながる可能性がある。	・原則として、年か日の何れかを削除する。必要に応じて生年月、年齢、年代等に置き換える。（丸め） ・超高齢であることが分かる生年月日や年齢を削除する。（セル削除/トップコーディング）
	性別	・住所（郵便番号）、生年月日との組合せにより、個人の特定につながる可能性がある。	・他の情報との組合せによって必要がある場合は削除する。（項目削除）
	住所	・生年月日、性別との組合せにより、個人の特定につながる可能性がある。 ・本人にアクセスすることができる。	・原則として、町名、番地、マンション名等の詳細を削除する。（丸め） ・レコード総数等に応じて、県単位や市町村単位へ置き換える。（丸め）
	郵便番号	生年月日、性別等との組合せにより個人の特定に結びつく可能性がある。	下 4 桁を削除する。（丸め）
	マイナンバー	それ自体で個人情報とされている。（個人識別符号）	全部削除する。（項目削除）
	パスポート番号	それ自体で個人情報とされている。（個人識別符号）	全部削除する。（項目削除）
	顔認証データ	それ自体で個人情報とされている。（個人識別符号）	全部削除する。（項目削除）

個人属性情報	**固定電話番号**	・多くの事業者が収集しており、異なるデータセット間で個人を特定するための識別子として機能し得る。 ・本人にアクセスすることができる。	原則として、加入者番号（下 4 桁）を削除。（丸め）
	携帯電話番号	・多くの事業者が収集しており、異なるデータセット間で個人を特定するための識別子として機能し得る。 ・本人にアクセスすることができる。	全部削除する。（項目削除）
	クレジットカード番号	・多くの事業者が収集しており、異なるデータセット間で個人を特定するための識別子として機能し得る。 ・本人に直接被害を与え得る。	全部削除する。（項目削除）
	サービス ID、アカウント ID	多くの事業者で共用される ID の場合は、個人を特定するための識別子として機能する。	全部削除する。（項目削除）
	電子メールアドレス	・多くの事業者が収集しており、異なるデータセット間で個人を特定するための識別子として機能し得る。 ・本人にアクセスすることができる。	全部削除する。（項目削除）
	端末 ID	多くの事業者で共用される端末 ID の場合は、個人を特定するための識別子として機能する。	全部削除する。（項目削除）
	職業	・住所や年収等との組合せにより、個人の特定につながる可能性がある。	・勤務先名を職種等のカテゴリーに置き換える。（一般化）
	年収	・職業や住所等との組合せにより、個人の特定につながる可能性がある。 ・超高年収の場合、それ自体から個人を特定できる可能性がある。	・具体的な年収を収入区分へ置き換える。（丸め） ・超高収入の値を削除する。（セル削除/トップコーディング）
	家族構成	・住所等との組合せにより、個人の特定につながる可能性が高くなる。	・具体的な家族人数を人数区分へ置き換える。（丸め） ・詳細な家族構成を世帯構成区分（単身、親子、三世帯等）へ置き換える。（丸め）
履歴情報	**購買履歴**	・購入店舗や購買時刻に関する情報と他のデータセットに含まれる位置情報等との組合せにより、個人の特定につながる可能性がある。 ・特異な物品の購買実績と居住エリア等との組合せにより、個人の特定につながる可能性がある。	・購入店舗や購買時刻の詳細な情報を削除する。（丸め） ・特異な購買情報（超高額な利用金額や超高頻度の利用回数等）を削除する。 （セル削除/トップコーディング）
	乗降履歴	・乗降実績の極めて少ない駅や時間帯の履歴から、個人の特定につながる可能性がある。 ・定期区間としての利用が極めて少ない駅の情報から、個人の特定につながる可能性がある。	・利用が極めて少ない駅や時間帯の情報を削除する。時刻情報を時間帯に置き換える。（セル削除/丸め） ・定期区間に極めて少ない利用駅が含まれるものを削除（セル削除）

履歴情報	**位置情報（移動履歴）**	・夜間や昼間の滞在地点から自宅や勤務先等を推定できる可能性あり。 ・詳細な位置情報と時刻情報の組合せが異なるデータセット間で識別子として機能し得る。 ・所定エリア内の位置情報が極めて少ない場合に、個人の特定に結びつく可能性がある。	・自宅や勤務地点等の推定につながる始点・終点を削除する。（丸め） ・位置情報若しくは時刻情報の詳細部分を削除する。（丸め） ・位置情報が少ないエリアの値にノイズを加える。（ノイズ付加） ・所定数以上の位置情報になるようエリアを区切る。（丸め）
	電力利用履歴	・特異な電力使用量と他の情報との組合せにより、個人の特定につながる可能性がある。 ・生活スタイルや家族構成を推定できる可能性がある。	・極めて大きい電力使用量の情報を削除する。（セル削除/トップコーディング）

（参考）

匿名加工情報の加工方法に関しては、平成 28 年 8 月 8 日に経済産業省が「事業者が匿名加工情報の具体的な作成方法を検討するにあたっての参考資料（「匿名加工情報作成マニュアル」）」（以下「経産省マニュアル」という。）を公表している。

匿名加工情報は、法第 36 条第 1 項に基づき、施行規則第 19 条各号に定める基準に従い加工する必要があるものであるが、経産省マニュアルは、施行規則が策定される前にその検討とは関わりなく、経済産業省において別途検討が進められ、公表されたものである。

経産省マニュアルにおいては、個人情報に含まれる記述等を①「識別子」、②「属性」及び③「履歴」の 3 つに分類した上で、次のとおり加工の方針を検討している [34]。

① 「識別子」とされたものは、個人識別のリスク [35]が高いため原則として削除を行う。
② 「属性」とされたものは、複数の属性が組み合わされることによる個人識別のリスクを検討する。
③ 「履歴」とされたものは、特異な値及び蓄積による識別の可能性を考慮する。

このようなリスク分析等の考え方については、検討を行う際の参考となる部分もあろうかと考えられることから、参考までに、経産省マニュアルと施行規則第 19 条各号に定める基準との関係を図表 4-5 に示す。

なお、図表 4-4 で示す「個人属性情報」は経産省マニュアルの分類における「識別子」及び「属性情報」に、「履歴情報」は「履歴情報」におおよそ対応しているものと考えられる。

[34] 経産省マニュアルの区分は適切に匿名加工を行うための便宜的なものであるとされ、必要に応じ仕分けを見直す必要が生じる可能性も想定されるとしている。（例えば、住所等については識別子と属性の双方に該当し得るとされている。）また、加工を「顧客属性データ」と「利用明細データ」の 2 区分のみに分けている事例もある。

[35] 個人が特定されるリスク、データが他の情報と照合されるリスク、データを用いて本人へアプローチされるリスク等が考慮されている。

図表 4-5 経産省マニュアルにおける分類と主に対応する施行規則の基準

分類 (主に対応する施行規則)	**定義**
識別子 (第 19 条第 1 号、第 2 号、第 3 号、第 5 号)	個人データを構成する情報であって、単体で個人を特定する可能性のある情報。 例：氏名、生年月日、アカウント ID、端末 ID、契約者 ID、電話番号、電子メールアドレス、詳細な住所(番地や住居番号含む)
属性情報 (第 19 条第 1 号、第 5 号)	個人データを構成する情報であって、経時的にデータが積み重ねられることのない情報で、単体では個人を特定することができないものの、他の属性との組合せや外部の情報との照合によって、個人を特定する可能性のある情報。 例：性別、年齢、郵便番号、住所（市町村まで）家族構成、年収　等
履歴情報 (第 19 条第 5 号)	個人データを構成する情報であって、個人の行動の履歴を蓄積し、経時的にデータが積み重ねられる情報で、一般に単体では個人を特定することができないものの、他の属性との組合せや外部の情報との照合によって個人を特定する可能性のある情報。 例：購買の履歴、ウェブの閲覧履歴、乗降履歴　等

※この他、施行規則第 19 条第 4 号における特定の個人の識別につながり得る特異なデータがある場合の処理があるが、これは主に属性情報（年齢等）に対応したものと考えられる。

5. 匿名加工情報等の安全管理措置

匿名加工情報を作成した場合は、法第 36 条第 2 項及び第 6 項に基づく安全管理措置を講ずる必要がある。前者は、匿名加工情報の加工方法等情報の漏えい防止に関する義務規定であり、後者は、匿名加工情報の取扱い全般の安全管理措置や苦情の処理等に関する努力義務規定となっている。

5.1 加工方法等情報の安全管理措置について

匿名加工情報の作成の際に行った加工の方法に関する情報（加工方法等情報）については、法第 36 条第 2 項に規定されているように、施行規則で定める基準に従って安全管理措置を講ずることとされている。

法第 36 条第 2 項

個人情報取扱事業者は、匿名加工情報を作成したときは、その作成に用いた個人情報から削除した記述等及び個人識別符号並びに前項の規定により行った加工の方法に関する情報の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、これらの情報の安全管理のための措置を講じなければならない。

施行規則第 20 条

法第 36 条第 2 項の個人情報保護委員会規則で定める基準は、次のとおりとする。

一 加工方法等情報（匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに法第 36 条第 1 項の規定により行った加工の方法に関する情報（その情報を用いて当該個人情報を復元することができるものに限る。）をいう。以下この条において同じ。）を取り扱う者の権限及び責任を明確に定めること。

二 加工方法等情報の取扱いに関する規程類を整備し、当該規程類に従って加工方法等情報を適切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を図るために必要な措置を講ずること。

三 加工方法等情報を取り扱う正当な権限を有しない者による加工方法等情報の取扱いを防止するために必要かつ適切な措置を講ずること。

ガイドライン 3-3-1 加工方法等情報等の安全管理措置等（法第 36 条第 2 項、第 39 条関係）

個人情報取扱事業者は、匿名加工情報を作成したときは、加工方法等情報（その作成に用いた個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報（その情報を用いて当該個人情報を復元することができるものに限る。（※））をいう。以下同じ。）の漏えいを防止するために、規則で定める基準に従い、必要な措置を講じなければならない。

当該措置の内容は、対象となる加工方法等情報が漏えいした場合における復元リスクの大きさを考慮し、当該加工方法等情報の量、性質等に応じた内容としなければならないが、具体的に講じなければならない項目及び具体例については、別表 2（加工方法等情報の安全管理で求められる措置の具体例）を参照のこと。

（※）「その情報を用いて当該個人情報を復元することができるもの」には、例えば、氏名等を仮 ID に置き換えた場合における置き換えアルゴリズムに用いられる乱数等のパラメータ又は氏名と仮 ID の対応表等のような加工の方法に関する情報が該当し、「年齢のデータを 10 歳刻みのデータに置き換えた」というような復元につながらない情報は該当しない。

（別表 2）加工方法等情報の安全管理で求められる措置の具体例

講じなければならない措置	具体例
①加工方法等情報を取り扱う者の権限及び責任の明確化 （規則第 20 条第 1 号）	・加工方法等情報の安全管理措置を講ずるための組織体制の整備
②加工方法等情報の取扱いに関する規程類の整備 及び当該規程類に従った加工方法等情報の適切な取扱い 並びに加工方法等情報の取扱状況の評価及びその結果に基づき改善を図るために必要な措置の実施 （規則第 20 条第 2 号）	・加工方法等情報の取扱いに係る規程等の整備とこれに従った運用 ・従業員の教育 ・加工方法等情報の取扱状況を確認する手段の整備 ・加工方法等情報の取扱状況の把握、安全管理措置の評価、見直し及び改善
③加工方法等情報を取り扱う正当な権限を有しない者による加工方法等情報の取扱いを防止するために必要かつ適切な措置 （規則第 20 条第 3 号）	・加工方法等情報を取り扱う権限を有しない者による閲覧等の防止 ・機器、電子媒体等の盗難等の防止 ・電子媒体等を持ち運ぶ場合の漏えい等の防止 ・加工方法等情報の削除並びに機器、電子媒体等の廃棄 ・加工方法等情報へのアクセス制御 ・加工方法等情報へのアクセス者の識別と認証 ・外部からの不正アクセス等の防止 ・情報システムの使用に伴う加工方法等情報の漏えい等の防止

匿名加工情報は、個人情報取扱事業者が自ら保有する個人情報を加工して作成するものであり、匿名加工情報を作成した当該事業者は元の個人情報とともに、加工の過程において個人情報から削除した記述等及び個人識別符号並びに法第 36 条第 1 項の規定により行った加工の方法 [36]に関する情報を保有し続けることが可能であるが、この情報の漏えいを防止するために施行規則第 20 条に定める基準に従い安全管理措置を講ずる必要がある。

ガイドラインに記載されているように、加工方法等情報（その作成に用いた個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報（その情報を用いて当該個人情報を復元することができるものに限る。）の漏えいを防止するための措置とは、対象となる加工方法等情報が漏えいした場合における復元リスク（その加工方法等情報を利用することによって元の個人情報を復元できるリスク）の大きさを考慮し、当該加工方法等情報の量、性質等に応じた内容とする必要がある。

[36] 加工の方法の中には、氏名等を仮 ID に置き換える際の置き換えアルゴリズムに用いられる入力情報に関する情報等や付加したノイズの割合等の加工手法に係るパラメータ情報のほか、元の個人情報と匿名加工情報に付された仮 ID 等の間の対応表等が該当し得る。

5.2　匿名加工情報の安全管理措置等について

法第 36 条第 6 項

個人情報取扱事業者は、匿名加工情報を作成したときは、当該匿名加工情報の安全管理のために必要かつ適切な措置、当該匿名加工情報の作成その他の取扱いに関する苦情の処理その他の当該匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

法第 39 条

匿名加工情報取扱事業者は、匿名加工情報の安全管理のために必要かつ適切な措置、匿名加工情報の取扱いに関する苦情の処理その他の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

ガイドライン　3-3-2　匿名加工情報の安全管理措置等（法第 36 条第 6 項、第 39 条関係）

個人情報取扱事業者又は匿名加工情報取扱事業者は、匿名加工情報の安全管理措置、苦情処理等の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

当該安全管理等の措置については、個人情報と同様の取扱いを求めるものではないが、例えば、法第 20 条から第 22 条までに定める個人データの安全管理、従業者の監督及び委託先の監督並びに法第 35 条に定める個人情報の取扱いに関する苦情の処理で求められる措置の例（※）を参考にすることも考えられる。具体的には、事業の性質、匿名加工情報の取扱状況、取り扱う匿名加工情報の性質、量等に応じて、合理的かつ適切な措置を講ずることが望ましい。

なお、匿名加工情報には識別行為の禁止義務が課されていることから、匿名加工情報を取り扱うに当たっては、それを取り扱う者が不適正な取扱いをすることがないよう、匿名加工情報に該当することを明確に認識できるようにしておくことが重要である。そのため、作成した匿名加工情報について、匿名加工情報を取り扱う者にとってその情報が匿名加工情報である旨が一見して明らかな状態にしておくことが望ましい。

（※）詳細は、通則ガイドライン「3-3-2（安全管理措置）、3-3-3（従業者の監督）、3-3-4（委託先の監督）、3-6（個人情報の取扱いに関する苦情処理について）」を参照のこと。

ガイドラインに記載されているように、個人情報取扱事業者又は匿名加工情報取扱事業者は、匿名加工情報に関する安全管理措置及び苦情処理等の必要な措置を自ら講ずる必要がある。これらの措置については、個人データの安全管理措置や苦情処理等の対応を参考にしつつ、匿名加工情報の性質を考慮して行われる必要がある。

6. 匿名加工情報の利用に当たっての留意点

6.1 識別目的の照合とは

法第 36 条第 5 項及び第 38 条で規定されているように、匿名加工情報の取扱いにおいては、元の個人情報に係る本人を識別する目的で他の情報と照合することが禁止される。

法第 36 条第 5 項

個人情報取扱事業者は、匿名加工情報を作成して自ら当該匿名加工情報を取り扱うに当たっては、当該匿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、当該匿名加工情報を他の情報と照合してはならない。

法第 38 条

匿名加工情報取扱事業者は、匿名加工情報を取り扱うに当たっては、当該匿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、当該個人情報から削除された記述等若しくは個人識別符号若しくは第 36 条第 1 項の規定により行われた加工の方法に関する情報を取得し、又は当該匿名加工情報を他の情報と照合してはならない。

ガイドライン 3-6 識別行為の禁止（法第 36 条第５項、第３８条関係）

匿名加工情報を取り扱う場合（※1）には、当該匿名加工情報の作成の元となった個人情報の本人を識別する目的で、それぞれ次の行為を行ってはならない。

（1）個人情報取扱事業者が自ら作成した匿名加工情報を取り扱う場合

・自らが作成した匿名加工情報を、本人を識別するために他の情報（※2）と照合すること。

（2）匿名加工情報取扱事業者が他者の作成した匿名加工情報を取り扱う場合

・受領した匿名加工情報の加工方法等情報を取得すること。

・受領した匿名加工情報を、本人を識別するために他の情報（※2）と照合すること。

【識別行為に当たらない取扱いの事例】

事例１）複数の匿名加工情報を組み合わせて統計情報を作成すること。

事例２）匿名加工情報を個人と関係のない情報（例：気象情報、交通情報、金融商品等の取引高）とともに傾向を統計的に分析すること。

【識別行為に当たる取扱いの事例】

事例１）保有する個人情報と匿名加工情報について、共通する記述等を選別してこれらを照合すること。

事例２）自ら作成した匿名加工情報を、当該匿名加工情報の作成の元となった個人情報と照合すること。

（※1）匿名加工情報については、当該匿名加工情報の作成の元となった個人情報の本人を識別する目的のために他の情報と照合することが禁止されている。一方、個人情報として利用目的の範囲内で取り扱う場合に照合を禁止するものではない。

（※2）「他の情報」に限定はなく、本人を識別する目的をもって行う行為であれば、個人情報及び匿名加工情報を含む情報全般と照合する行為が禁止される。また、具体的にどのような技術又は手法を

用いて照合するかは問わない。

これについては、識別ができるか否かを問わず、識別を目的とした照合行為自体がこれらの義務違反となる。

したがって、例えば、ある集団の傾向やマーケットの動向を分析するために他の情報と照合することについては、識別目的の照合には該当せず、義務違反とはならない。

例えば、異なる事業者から提供を受けた複数の匿名加工情報データベースのうち、類似の基本属性（年代、居住エリア等）を持つ匿名加工情報同士の購買情報等の履歴情報を組み合わせて、より詳細な統計情報を作成するようなことも可能である。

一方、第三者より提供を受けた匿名加工情報データベースと事業者内で保有する個人情報データベースとの間で、基本属性の類似度等から個人情報データベースに含まれる個人データと匿名加工情報に含まれる匿名加工情報とを紐付けることは、一般的には、識別目的の照合に該当すると考えられる。この結論は、当該紐づけがたとえ確率的に行われるものであっても変わらない。

6.2 加工方法の評価や再識別事案発生等における影響の範囲の確認等のための照合

3.2 でも述べたように、匿名加工情報における「特定の個人を識別することができない」及び「復元することができないようにしたもの」は一般人や一般的な事業者の能力、手法等を基準として判断されるものであり、技術的側面から全ての可能性を排除することまでを求めるものではない[37]。

匿名加工情報については、識別行為の禁止義務がある一方、施行規則第 20 条第 1 号では、加工方法等情報を取り扱う者の権限や責任が明確化され、同条第 3 号では、加工方法等情報を取り扱う正当な権限を有しない者に対する加工方法等情報へのアクセス制限が課されることになっている。また、法第 36 条第 6 項では、匿名加工情報の安全管理のために必要かつ適切な措置を講ずることが求められている。安全管理措置の一環として加工方法等情報を取り扱う正当な権限を有する者によりこのような評価や影響範囲の確認等のための照合が行われる場合には、安全管理措置として必要な限りにおいて認められるものであり、法第 36 条第 5 項で禁止される識別行為に該当するものではないと考えられる。

6.3 匿名加工情報を加工したものの扱い

作成された匿名加工情報は、提供された第三者のもとで、情報を付加したり、一部の項目を削除したりするような加工がされることが想定される。

元の匿名加工情報に情報を付加する加工を行った場合については、元の匿名加工情報の情報がそのまま残るものであるから、元の匿名加工情報と同一のものとして扱うべきものと考えらえる。

一方、元の匿名加工情報から情報を削除する場合については、削除される情報の程度によって変わり得るが、元の匿名加工情報との対応関係が明らかである限りは、同一の匿名加工情報として扱うものと考えることが妥当である。

[37] あらゆるデータに汎用的な匿名加工手法はなく、技術の進展によっても再識別リスクが変化し得ること、再識別リスクをモニタリングし匿名加工手法に対する評価や見直しを行うことが望ましいことについては、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」（2013 年 12 月）や Article 29 Data Protection Working Party（EU 第 29 条作業部会） “Opinion 05/2014 on Anonymisation Techniques”（2014 年 4 月）等においても指摘されている。

6.4　意図せず特定個人を識別してしまった場合の扱い

法第 36 条第 5 項や法第 38 条の義務は、識別目的の照合行為に限られるため、加工が不十分であったことにより偶発的に特定の個人を識別してしまった場合は、これらの義務違反として直ちに罰せられることにはならないが、再度同じような形で個人を識別することがないようにする必要がある。さらに、識別してしまった情報については、個人情報として適切な取扱いを行う必要がある。

また、加工が不十分であることにより通常の業務を通じて特定の個人が識別されてしまう場合には、匿名加工情報としての要件を満たしていないことから、個人情報としての取扱いが求められることになる。この場合、匿名加工情報を作成して自ら取り扱う事業者においては、本人の同意を取得した上で個人情報として適切な取扱いを行うか、情報の提供を受けた事業者において当該情報の削除を行うとともに利用を中止する等の対応が求められることになる。

7. 匿名加工情報のユースケースと加工例について

様々な個人情報取扱事業者が取得・蓄積している個人情報について、施行規則で定める加工基準に基づいて匿名加工情報を作成することにより、個人情報の取得時には想定していなかった新たな目的で利用したり、第三者提供を行ったりすることが可能となる。ここでは、想定され得るユースケースを念頭に、情報の項目に応じて考慮すべき事項とリスクに対応した具体的な加工方法について、有識者の意見を聴きながら、検討を行ったものを紹介する。

本レポートで示すユースケースのうち、7.1.2（購買履歴の事例２（クレジットカード利用情報））、7.2.1（乗降履歴の事例）、7.3（電力利用データの事例）の３つのユースケースについては経産省マニュアルにおいて行われた検討を参考にしつつ、個人情報保護委員会事務局で取りまとめたものとなっている。なお、本レポートで示すユースケースは、作成された匿名加工情報の一次流通までを想定し、二次流通は想定していない。

7.1 購買履歴の事例

購買履歴については、消費者向けに商品を販売する小売事業者、通信販売事業者、決済手段を提供するクレジットカード事業者、ポイントカード運営事業者等において様々な形で取得・蓄積されている。

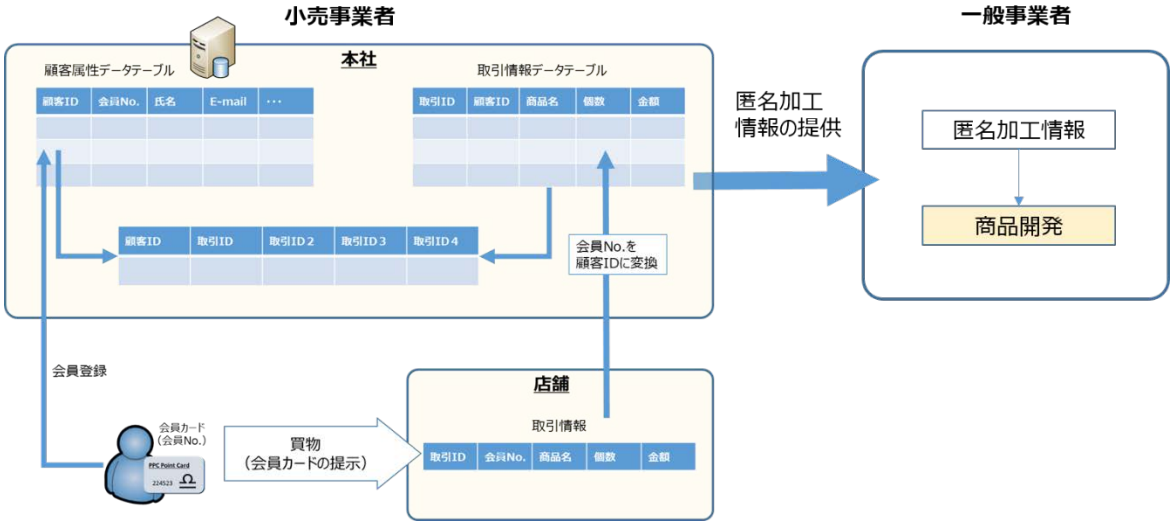
これらの購買履歴については、広告、マーケティング、商品開発等をはじめ様々な目的のために活用が想定されるものであり、例えば、小売事業者、クレジットカード事業者等について目的外利用あるいは第三者提供のために匿名加工情報を作成する次のようなユースケースが想定される。

7.1.1 購買履歴の事例１（ID-POS データ）

１）ユースケース

本ユースケースは、小売事業者が保有する購買履歴（ID-POS データ）について匿名加工を行ったうえで、匿名加工情報の枠組みを活用して、一般事業者へ提供するものである。一般事業者においては、そこに含まれる消費者の基本属性と購買傾向から、自社の新商品の開発や販売促進活動等に利用することが想定される。

図表 7-1 小売事業者が保有する購買履歴情報を第三者提供するユースケースのイメージ



本ユースケースでは、顧客属性テーブル、取引情報テーブル、購買履歴テーブルから構成される図表 7-2 のようなデータ構造を前提として検討する。顧客属性テーブルと取引情報テーブルは、会員 ID によって紐づけが可能であり、顧客別の購買履歴を表す購買履歴テーブルを作成できるようになっている。

図表 7-2　購買履歴（ID-POS データ）に関するデータのレイアウトイメージ

顧客属性テーブル

会員ID	氏名	生年月日	性別	住所	電話番号
224523	田中　一郎	1972年4月4日	男	神奈川県横浜市中区富士見町X-X-X	045-222-XXXX
225412	佐藤　幸子	1993年12月9日	女	千葉県船橋市西船Y-Y-Y	090-444-YYYY
231622	鈴木　博	1963年8月23日	男	東京都墨田区押上Z-Z-Z	03-1234-ZZZZ

取引情報テーブル

取引ID	会員ID	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	…
10032	224523	2016/8/2　18:25	KN013	みなとみらい店	101	151	午後のミルクコーヒー	1	…
11252	225412	2016/10/4　07:13	CB002	西船橋駅前店	305	288	近江屋チョコレート（ホワイト）	4	…
12003	231622	2016/11/30　11:59	TK101	錦糸町店	211	793	バンドウクジラぬいぐるみ（大）	1	…
…	…	…	…	…	…	…	…	…	…

購買履歴（顧客別）テーブル

会員ID	取引ID	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	金額	商品ID	商品名	…
224523	10032	2016/8/2 18:25	KN013	みなとみらい店	101	151	午後のミルクコーヒー	1	150	188	ふんわりつぶアンパン	…
224523	10125	2016/8/3 7:09	KN051	富士見店	004	874	BUSSコーヒー（無糖）	2	240	-	-	-
224523	10222	2016/8/5	KN043	横浜駅前店	017	342	フレッシュYシャツ（紺）	1	8980	321	慶事用ネクタイ（銀）	…
224523	…	…	…	…	…	…	…	…	…	…	…	…

2）考慮すべき事項とリスクに対応した具体的な加工方法の検討

①　含まれ得る情報の種類

図表 7-2 に示すデータテーブルを構成する各情報の項目は、次のように、個人属性情報と履歴情報とに分類することができる。

図表 7-3　購買履歴（ID-POS データ）に関するデータのレイアウトイメージ

顧客属性テーブル　個人属性情報

会員ID	氏名	生年月日	性別	住所	電話番号
224523	田中　一郎	1972年4月4日	男	神奈川県横浜市中区富士見町X-X-X	045-222-XXXX
225412	佐藤　幸子	1993年12月9日	女	千葉県船橋市西船Y-Y-Y	090-444-YYYY
231622	鈴木　博	1963年8月23日	男	東京都墨田区押上Z-Z-Z	03-1234-ZZZZ

取引情報テーブル　履歴情報

取引ID	会員ID	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	…
10032	224523	2016/8/2　18:25	KN013	みなとみらい店	101	151	午後のミルクコーヒー	1	…
11252	225412	2016/10/4　07:13	CB002	西船橋駅前店	305	288	近江屋チョコレート（ホワイト）	4	…
12003	231622	2016/11/30　11:59	TK101	錦糸町店	211	793	バンドウクジラぬいぐるみ（大）	1	…
…	…	…	…	…	…	…	…	…	…

購買履歴（顧客別）テーブル

履歴情報

会員ID	取引ID	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	金額	商品ID	商品名	…
224523	10032	2016/8/2 18:25	KN013	みなとみらい店	101	151	午後のミルクコーヒー	1	150	188	ふんわりつぶアンパン	…
224523	10125	2016/8/3 7:09	KN051	富士見店	004	874	BUSSコーヒー（無糖）	2	240	-	-	-
224523	10222	2016/8/5	KN043	横浜駅前店	017	342	フレッシュYシャツ（紺）	1	8980	321	慶事用ネクタイ（銀）	…
224523	…	…	…	…	…	…	…	…	…	…	…	…

② **どのように加工すべきか**

加工を検討するに当たっては、上記で分類した個人属性情報と履歴情報ごとに検討する。

【個人属性情報】

個人属性情報については、主として、施行規則第 19 条第 1 号～第 4 号の観点から加工を検討することになる。本ユースケースにおける個人属性情報には、会員 ID、氏名、生年月日、性別、住所、電話番号が含まれる。

＜会員 ID＞

このユースケースにおける会員 ID は、顧客に一意に割り当てることにより顧客を識別してその情報を管理するために用いられるほか、顧客属性テーブルと取引情報テーブルとを連結するための符号として機能している。したがって、施行規則第 19 条第 3 号に相当する個人情報と当該個人情報に措置を講じて得られる情報を連結する符号に該当するため、会員 ID については、仮 ID に置き換えることにより、全部を削除する。

＜電話番号＞

電話番号は、多数の事業者で収集されている情報であること、本人へアクセスできるリスクがあることから、個人の特定につながる可能性の高い情報である。したがって、電話番号については全部を削除する。なお、固定電話における市外局番や市内局番等の地域を表す部分については、住所に関する記述の曖昧化と平仄を揃える程度の情報を残すことは可能である。

＜住所＞

住所に関しては、多数の事業者で収集されている情報であることに加え、本人へアクセスできるリスクがあることから、個人の特定につながる可能性の高い情報である。一方、顧客の居住地を表す情報については、マーケティング等の観点から情報として有用である。住所を構成する記述のうち、県名や市名等の広いエリアを表す情報については個人の特定への影響が少ないことから、詳細なエリアを示す部分の情報を削除して情報を丸める（曖昧化する）。

なお、情報を丸める際には、データセットの大きさや他の情報（例えば、生年月日）の加工の程度を考慮して行う必要があるが、町村以下の情報は原則的として削除することが望ましい。また、人口の多寡に応じて同じデータセットでも丸めの度合を可変にする方法も考えられる。

＜生年月日＞

生年月日に関しては、少なくとも日に関しては削除することが望ましい。ただし、生年月にするか年齢

や年代に置き換えるか等どの程度まで情報を削除するかについては、前述の住所と同様に該当者の人数に応じて客観的に判断すべきであり、例えば、同年同月をその月に生まれた個人の人数が少ない場合は削除すべき対象となる。生年月日の情報をどこまで曖昧化するかについては、住所の加工と合わせて検討することが望ましい。

このほか、超高齢者等の生存者が極めて少ない生年月日に関しては、施行規則第 19 条第 4 号の特異値に該当する場合もあり得る。このような場合には、その生年月日に関する情報を削除するか、トップコーティングにより、「100 歳以上」といった区分に丸めることが考えられる。

＜性別＞

性別に関しては、男女による購買傾向の差異を分析したいニーズがあること、生年月日や住所に関する情報を丸めることにより個人の特定性を低減していることから、本ユースケースでは加工しない。

【履歴情報】

＜時刻情報及び店舗情報の取扱い＞

本ユースケースにおける履歴情報である取引情報には、その取引が発生した詳細な日時の情報と店舗名の情報が含まれている。一般に、時刻情報単体で個人の識別性はないが、「PPC マート霞が関店」等の店舗名からはおおよその位置を特定することが可能であるため、これらを組み合わせた情報は、位置情報と時刻情報を含む他のデータセットと照合することで、個人の特定につながる可能性がある。

したがって、時刻情報と店舗情報の少なくとも一方を曖昧化することが望ましい。本ユースケースにおいては、店舗名をそのまま使用したいニーズがあると想定されるため、時刻情報を丸める処理を行う。時刻情報は少なくとも秒単位の情報を削除することが望ましく、客数が少ないことにより個人の特定可能性が高くなる場合は、30 分単位や 1 時間単位等に情報を丸める単位を変更する等の措置も検討されるべきである。

＜商品の購買履歴（商品名、個数、金額）の取扱い＞

購買情報には一品ものや少数限定品、あるいは超高額の商品の購買記録が含まれる可能性がある。珍しい商品の購入を示す情報については、店舗名等との組合せにより個人の特定につながる可能性が高くなると考えられる。したがって、このような情報については、削除するか、商品名を商品カテゴリーに置き換えることが望ましい。

また、購入した商品がありふれたものでも購入個数が非常に多い場合は特異な記述等といえる場合がある。この場合、購入個数に関する情報を削除するか、ミクロアグリゲーションにより当該商品の平均的販売個数等に置き換える等の手法により加工を行うことが望ましい。

＜その他の情報の取扱い＞

本ユースケースにおいては、取引ごとに取引 ID を付しており、また、それぞれの取引情報には、その取引の担当者の担当者 ID や、取り扱った商品の商品 ID も含まれている。これらの情報については、本ユースケースにおいて想定される提供先にとって情報の有用性もないと思われること、匿名加工情報では、第三者におけるデータ利活用において不要と思われる情報は想定外の再識別リスクを低減する意味においても削除することが望ましいこととから、これらの情報については全部削除する。

以上の本ユースケースにおける各情報についての加工の方向性をまとめると、次のようになる。

図表 7-4　購買履歴（ID-POS データ）のユースケースにおける加工の方向性

項目	想定されるリスク	望ましい加工方法
①個人属性情報		
会員 ID	内部での分散管理用 ID としての機能を有しており、この ID を起点として、個人を特定できる可能性がある。	全部削除する、あるいは仮 ID に置き換える[38]。（項目削除）
氏名	単体で個人を特定できる。	全部削除する（項目削除）
生年月日	居住エリアや性別等との組合せにより、個人を特定できる可能性がある。	年代の 7 区分（20 歳未満/20 代/30 代/40 代/50 代/60 代/70 歳以上）に置き換える。（丸め）
電話番号	他の事業者でも収集している可能性が高く、それにより他の情報と照合して個人の特定につながる可能性がある。 また、本人にアクセスできるリスクがある。	全部削除する。（項目削除）
性別	生年月日や居住エリアとの組合せにより、個人の特定につながる可能性がある。	本ケースでは、生年月日と住所の加工により対応し、性別情報の有用性から加工をしない。
住所	生年月日や性別との組合せにより、個人の特定につながる可能性がある。 また、本人にアクセスできるリスクがある。	市区郡単位より細かい情報を削除する。（丸め）
②履歴情報		
利用日時	他のデータセットに含まれる位置情報との組合せにより、個人の特定につながる可能性がある。	秒単位の情報を削除し、分単位に置き換える。（丸め）
店舗 ID	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）
店舗名	店舗名から購買場所である位置を推定可能であり、他の情報に含まれる位置情報と連結されることにより、個人の特定につながる可能性がある。	本ケースでは、利用日時の加工により対応し、店舗情報の有用性から加工しない。
取引 ID	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）
担当者 ID	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）
商品 ID	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）
商品名	限定品や超高級品等の希少な商品の購買履歴と購買場所等の情報との組合せにより、個人の特定につながる可能性がある。	希少商品の購買実績を削除する。あるいは商品カテゴリーに置き換える。 （セル削除/丸め/一般化）

[38] 本ユースケースにおいては、仮 ID を匿名加工後の顧客属性テーブルと購買履歴テーブルとを連結するための ID として使用している。他のユースケースにおいても同じ。なお、仮 ID の置換えについては、4.11 の【仮 ID への置き換えについて】を参照のこと。

項目	想定されるリスク	望ましい加工方法
数量	特定の商品に関する大量の購入実績から、個人の特定につながる可能性がある。	特異な購入実績を示す数量については削除あるいは平均的な値等に置き換える。 （セル削除/ミクロアグリゲーション）
金額	超高額の支払い実績から、個人の特定につながる可能性がある。	特異な購入実績を示す金額については削除あるいは○○円以上という区分に置き換える。 （セル削除/トップコーディング）

③ 加工後のデータのイメージ

上記の考え方に基づいて加工されたデータは、図表 7-5 のようになる。

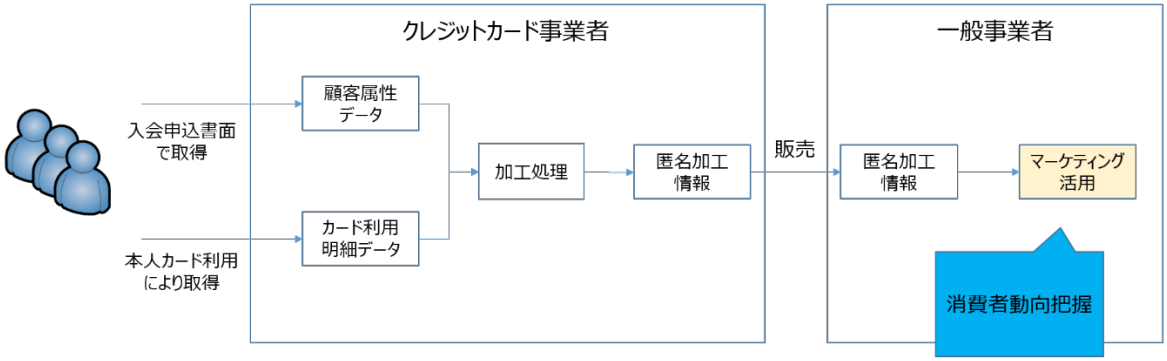
図表 7-5　購買履歴（ID-POS データ）のユースケースにおける加工後のデータのイメージ

7.1.2 購買履歴の事例２（クレジットカード利用情報）

１）ユースケース

本ユースケースは、クレジットカード事業者が保有するカード利用情報について、匿名加工を行った上で、匿名加工情報の枠組みを活用して、一般事業者へ提供するというものである。一般事業者においては、提供を受けた匿名加工情報に基づいて、年収や職業と利用加盟店等の関係を分析することにより、マーケティングに活かすことが想定される。

図表 7-6 クレジットカード事業者が保有するカード利用情報を第三者提供するユースケースのイメージ



本ユースケースにおいて加工対象となるデータセットは、①顧客属性データ及び②カード利用明細データの２種類からなり、いずれも契約者 ID（クレジットカード番号の変換番号）によって、リンクされている。

顧客属性データには、顧客の基本属性のほか、勤務先、年収及び決済金融機関の情報が含まれている。また、カード利用明細データは、クレジットカードの利用日時、利用加盟店、支払方法及び利用金額で構成されている。

図表 7-7 クレジットカード事業者が保有するカード利用情報におけるデータのレイアウトサンプル

顧客属性データ

契約者ID	氏名	クレジットカード番号	性別	生年月日	電話番号	住所	勤務先	年収	決済金融機関
11145687	田中 一郎	4999 XXXX XXXX XXXX	男	1972年4月4日	045-222-XXXX	神奈川県横浜市中区富士見町X-X-X	A商事	1800万	D銀行
11145688	佐藤 幸子	5999 YYYY YYYY YYYY	女	1993年12月9日	090-1111-YYYY	千葉県船橋市西船Y-Y-Y	B銀行	400万	E銀行
11145689	鈴木 博	6999 ZZZZ ZZZZ ZZZZ	男	1963年8月23日	03-1234-ZZZZ	東京都墨田区押上Z-Z-Z	C電器	750万	F信用金庫
…	…	…	…	…	…	…	…	…	…

システム的にリンク

カード利用明細データ

契約者ID	利用日時	利用加盟店	支払方法	利用金額
11145687	2016年12月23日 12:03	○○○○ みなとみらい店	1回	200,000
11145688	2016年12月24日 18:35	△△△△ 丸の内店	4回	50,000
11145689	2016年12月25日 20:13	□□□□ 押上店	1回	5,500

２）考慮すべき事項とリスクに対応した具体的な加工方法の検討

① 含まれ得る情報の種類

図表 7-7 に示すデータを、個人属性情報と履歴情報とに分類すると、次のようになる。

図表 7-8　クレジットカード事業者が保有するカード利用情報におけるデータのレイアウトイメージ

② **どのように加工すべきか**

本ユースケースにおいて、取扱いに注意すべき情報は、個人属性情報に含まれる勤務先や年収と、履歴データであるカード利用明細データにおける利用日や利用加盟店、利用金額に関する情報と考えられる。

【個人属性情報】

＜年収、勤務先＞

勤務先の情報は、例えば、住所との組合せにより個人の特定可能性が高くなることが想定される。また、更に年収の情報が組み合わさることによって、職層等を推定することも可能である。一方、職種についてはマーケティング等の観点から有用な情報であることから、勤務先の情報については全部削除ではなく、職種のカテゴリーに置き換える加工を行うことが考えられる。

年収については、本ユースケースでは勤務先や住所に関する情報とともに提供することを想定しているため、複数の年収区分に置き換える等の情報を一定程度丸める加工をすることが望ましい。また、超高収入である場合は、施行規則第 19 条第 4 号の措置の対象となり得るため、該当するものがある場合は、その情報を削除するかトップコーディングを行う必要がある。

【履歴情報】

＜カード利用明細データの取扱い＞

利用日時や利用金額と利用加盟店との組合せは、例えば、他の事業者が有する購買履歴情報と結びつくことにより、個人の特定につながる可能性がある。マーケティング等の観点から有用な情報であると考えらえるため、一部の情報を曖昧化することが望ましい。曖昧化に当たっては、例えば、利用日を月単位にすること、利用金額を複数の区分に置き換えることが考えられる。

また、利用加盟店のうちデータセットにおいてカード利用頻度の少ない加盟店、一回の利用における利用金額が極めて高額のもの、一定期間におけるカード利用回数が極めて多いものについては、その希少性から個人の特定につながる可能性があるため、トップコーディング等を行うことにより情報を加工する

ことが望ましい。

以上の本ユースケースにおける各情報についての加工の方向性をまとめると、次のようになる。

図表 7-9 購買履歴（カード利用履歴）のユースケースにおける加工例

項目	想定されるリスク	望ましい加工方法
① 個人属性情報		
契約者 ID	クレジットカード番号を変換しており、変換ルールが解読されることにより、個人を特定できる可能性がある。 また、作成事業者内部での分散管理用 ID として使用されている。	全部削除する、あるいは仮 ID に置き換える。（項目削除）
氏名	単体で個人を特定できる。	全部削除する。（項目削除）
クレジットカード番号	他の事業者でも収集している可能性の高い情報であり、他の情報と照合して個人を特定できる可能性がある。	全部削除する。（項目削除）
性別	生年月日と住所との組合せにより、個人の特定につながる可能性がある。	本ケースでは、生年月日と住所の加工により対応し、性別情報の有用性から加工をしない。
生年月日	住所や性別との組合せにより、個人の特定につながる可能性がある。	年代の 6 区分（～20 代/30 代/40 代/50 代/60 代/70 代～）に置き換える。 （丸め/トップコーディング）
電話番号	他の事業者でも収集している可能性が高く、他の情報と照合して個人を特定できる可能性がある。 また、本人にアクセスできるリスクがある。	全部削除する。（項目削除）
住所	生年月日や性別との組合せにより、個人の特定につながる可能性がある。 また、本人にアクセスできるリスクがある。	市区単位より細かい情報を削除する。（丸め）
勤務先	他の事業者でも取得している可能性があり、他の情報との組合せにより、個人の特定につながる可能性がある。	「農業」「製造業」「小売業」「金融業」等の職種分類に置き換える。 （一般化）
年収	超高収入の人物については、個人を特定できる可能性がある。	6 区分（300 万未満、300～600 万、600～900 万、900～1200 万、1200～1800 万、1800 万以上）に置き換える。 （丸め/トップコーディング）
決済金融機関	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）

項目	想定されるリスク	望ましい加工方法
②履歴情報		
利用日	利用加盟店や利用金額との組合せにより、個人を特定できる可能性がある。	利用月単位に置き換える。（丸め）
利用加盟店	カード利用頻度の低い加盟店の場合、個人の特定につながる可能性がある。	カード利用頻度が極めて低い加盟店情報を削除する。（セル削除）
支払方法	―	加工しない。
利用金額	超高額の利用金額については、利用加盟店情報等との組合せにより、個人の特定につながる可能性がある。	超高額な利用金額の情報を削除する。短期間における利用総額が大きい契約者の情報を削除する。（セル削除/レコード削除）

③ 加工後のデータのイメージ

上記の考え方に基づいて加工されたデータは、図表 7-10 のようになる。

図表 7-10　購買履歴（カード利用履歴）のユースケースにおける加工後のデータのイメージ

顧客属性データ

仮ID	性別	年代	居住エリア	職種	年収
ad38de089a	男	40代	横浜市	商社	1800万以上
16ad82be6b	女	20代	船橋市	金融業	300～600万
a75e7392f8	男	60代	墨田区	メーカー	600～900万
…	…	…	…	…	…

カード利用明細データ

仮ID	明細１			明細２			明細３		
	利用日	利用加盟店	利用金額	利用日	利用加盟店	利用金額	利用日	利用加盟店	利用金額
ad38de089a	2016年10月	○○○○ みなとみらい店	43,000	2016年11月	◇◇◇◇ 横浜店	23,800	2016年12月	▽▽▽▽ 渋谷店	200,000
16ad82be6b	2016年8月	△△△△ 丸の内店	6,500	2016年9月	×××× 津田沼店	29,800	2016年12月	○○○○ 新宿店	50,000
a75e7392f8	2016年6月	□□□□ 押上店	13,800	2016年7月	■■■■ 錦糸町店	8,200	2016年12月	□□□□ 押上店	5,500
…	…	…	…	…	…	…	…	…	…

7.2 乗降履歴・移動履歴の事例

乗降履歴については、非接触型 IC カードの普及に伴い鉄道会社（JR・私鉄・地下鉄等）あるいはバス会社等において取得・蓄積が進んでいる。また、カーナビゲーション（以下「カーナビ」という。）や自動車に搭載した GPS 受信機によって取得できる位置情報（移動履歴）についても、車載通信機の普及に伴い、カーナビメーカーや自動車メーカーにおいて蓄積・活用が進んでいる。

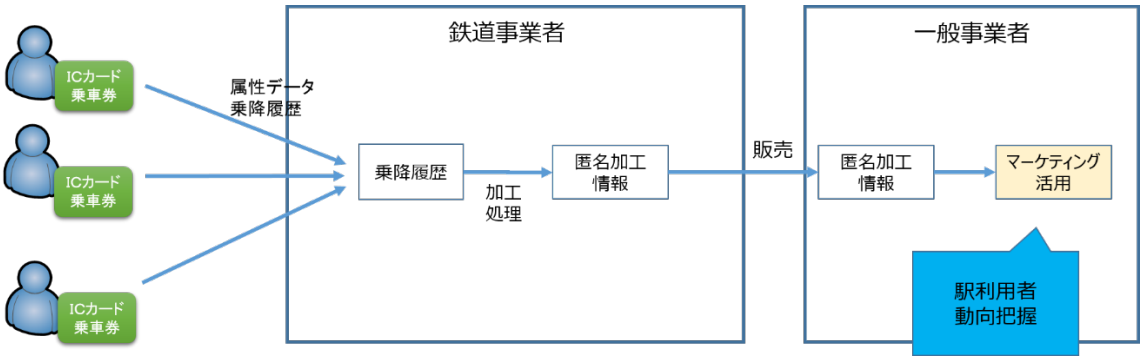
これらの乗降履歴・移動履歴については、各エリアや道路等の動線分析、通勤圏や商圏分析、地域開発、広告、マーケティング、商品開発等をはじめ様々な目的のために活用が想定されるものであり、例えば、鉄道会社・バス会社、カーナビメーカーや自動車メーカー等について目的外利用あるいは第三者提供のために匿名加工情報を作成する次のようなユースケースが想定される。

7.2.1 乗降履歴の事例

1）ユースケース

本ユースケースは、鉄道会社が保有する乗降履歴情報について、匿名加工を行ったうえで、匿名加工情報の枠組みを活用して、一般の事業者に提供するというものである。一般事業者においては、鉄道利用者の基本属性（年代、性別等）や鉄道の乗降履歴に基づいて、商圏分析やターゲティング広告の広告戦略に活用することが想定される。

図表 7-11 鉄道会社が保有する乗降履歴情報を第三者に提供するユースケースのイメージ



本ユースケースにおいて加工対象となるデータセットは、図表 7-12 に示すように、①顧客属性データ及び②IC カード利用データの 2 種類からなり、カード ID によって、リンクされている。

顧客属性データには、定期情報が含まれ、定期券の有効期間（定期券開始日及び定期券終了日）と定期券区間（定期券発駅及び定期券着駅）から構成されている。また、IC カード利用データは利用日時や入出場駅及びその際に使用した改札口、各乗降に伴う利用額及び IC カードにチャージされている残額等から構成されている。なお、IC カード利用データにおいて、SF 入場とは、定期券区間外の入場を意味し、SF 出場は定期券区間外での出場を意味する。

図表 7-12　鉄道会社が保有する乗降履歴に関するデータのレイアウトイメージ

ID	氏名	性別	生年月	郵便番号	住所	定期情報			
						定期券開始日	定期券終了日	定期発駅	定期着駅
234899	田中　一郎	男	1972年4月	231-0037	神奈川県横浜市	2016年12月1日	2017年5月30日	関内	みなとみらい
234900	佐藤　幸子	女	1993年12月	273-0031	千葉県船橋市	2017年1月4日	2017年4月3日	西船橋	東京
234901	鈴木　博	男	1963年8月	131-0045	東京都墨田区	—	—	—	—

ID	処理名称	年月日	時間	利用駅種別	改札口	入場駅	出場駅	利用額	残額
234899	出場	2016/12/17	9:30	SF入場SF出場	A6	関内	鎌倉	780	25,000
234899	入場	2016/12/17	14:20	SF入場	A5	鎌倉	–		25,000
234899	出場	2016/12/17	15:00	SF入場SF出場	B3	鎌倉	江の島	300	24,700
234899	入場	2016/12/18	8:45	SF入場	C4	江の島	–	0	24,700

2）考慮すべき事項とリスクに対応した具体的な加工方法の検討

①　含まれ得る情報の種類

図表 7-12 に示すデータセットを、個人属性情報と履歴情報とに分類すると、次のようになる。

図表 7-13　鉄道会社が保有する乗降履歴に関するデータのレイアウトイメージ

ID	氏名	性別	生年月	郵便番号	住所	定期情報			
						定期券開始日	定期券終了日	定期発駅	定期着駅
234899	田中　一郎	男	1972年4月	231-0037	神奈川県横浜市	2016年12月1日	2017年5月30日	関内	みなとみらい
234900	佐藤　幸子	女	1993年12月	273-0031	千葉県船橋市	2017年1月4日	2017年4月3日	西船橋	東京
234901	鈴木　博	男	1963年8月	131-0045	東京都墨田区	—	—	—	—

ID	処理名称	年月日	時間	利用駅種別	改札口	入場駅	出場駅	利用額	残額
234899	出場	2016/12/17	9:30	SF入場SF出場	A6	関内	鎌倉	780	25,000
234899	入場	2016/12/17	14:20	SF入場	A5	鎌倉	–	0	25,000
234899	出場	2016/12/17	15:00	SF入場SF出場	B3	鎌倉	江の島	300	24,700
234899	入場	2016/12/18	8:45	SF入場	C4	江の島	–	0	24,700

②　どのように加工すべきか

本ユースケースにおいて、特に取扱いに気をつける必要があるのは、定期券情報（定期期間、定期区間）、入場駅と出場駅及びそれに関する時刻の情報の取扱いであると考えられる。

【個人属性情報】

＜定期券情報の取扱い＞

まず、定期券区間情報（定期券発駅、定期券着駅）は、定期券区間外の移動傾向（例えば、休日の買い物に出かける場所）との相関等を分析するために有用であり、本ユースケースにおいても利用することが想定され得る。

一方、定期券区間の情報からは、自宅の最寄り駅と勤務先や通学先の最寄り駅を把握することができるが、定期券の発駅若しくは着駅の一方に、定期券としての利用が少ない駅が含まれている場合は、個人の特定につながる可能性が高くなるため、そのような情報については、削除する、あるいは別の駅名に置き換える等の措置を講ずることが望ましい。

【履歴情報】

＜入・出場駅及び時刻情報の取扱い＞

日々の乗降履歴としての入場駅・出場駅とそれに関する時刻情報からは、その情報に係る本人の行動パターン（例えば、通勤日や勤務時間帯、そして、週末に出かけるエリア等）を推測することができる。

一方、データセットに含まれる乗降履歴の期間が長いほどその情報は一意となり得るため、その一意性をもって直ちに個人を特定することができないとしても、一定の配慮（措置）をすることが望ましい。

例えば、入場駅・出場駅のそれぞれの利用時における単位時間当たりの利用者数を考慮して、利用者数が少ない駅の情報や利用者数が少ない時間帯の情報を削除することが望ましい。また、入出場時刻を表す詳細な時刻情報については、秒単位の情報を削除したり、30 分単位や 1 時間単位に情報を丸めたりすることが考えられる。

＜利用額・残額の取扱い＞

本ユースケースは商圏分析等を想定しており、IC カードへのチャージ額や利用額に関する情報の必要性が乏しいと考えられることから、利用額及び残額の情報については、その項目自体を削除する。

なお、IC カードの電子マネーとしての利用状況等の分析に用いる場合も想定し得るが、そのような場合には、各入・出場の履歴に関する利用額や残額の偏差から定期の利用有無及びその区間を判別することが可能であるため、定期券区間情報の取扱いとの相関があることに留意しておくことが必要である。

以上の本ユースケースにおける各情報についての加工の方向性をまとめると、次のようになる。

図表 7-14　鉄道の乗降履歴データのユースケースにおける加工例

項目	想定されるリスク	望ましい加工
①個人属性情報		
ID	顧客属性データと IC カード利用データとを紐づける内部管理 ID として使用されている。	全部削除する、あるいは仮 ID に置き換える。（項目削除）
氏名	単体で個人を特定できる。	全部削除する。 （項目削除）
性別	住所（居住エリア）や生年月日等との組合せにより、個人の特定につながる可能性がある。	本ケースでは、生年月日と住所の加工により対応し、性別情報の有用性から加工をしない。

項目	想定されるリスク	望ましい加工
生年月	住所や性別等との組合せにより、個人の特定につながる可能性がある。 また、超高齢である場合は、それにより個人の特定につながる可能性がある。	年代の 6 区分（～20 代/30 代/40 代/50 代/60 代/70 代～）に置き換える。 （丸め/トップコーディング）
郵便番号・住所	性別や生年月等の情報との組合せにより、個人の特定につながる可能性がある。	本ユースケースの住所情報は市区単位までしか入っていないため、加工しない。郵便番号は不要と考えられることから全部削除する。 （項目削除）
定期券有効期間（開始日/終了日）	（提供先にとって不要な情報と想定）	本ケースでは、提供先において不要な情報と考えられるため、全部削除する。（項目削除）
定期券区間 （発駅/着駅）	自宅最寄り駅と勤務先等の最寄り駅を推測できる。 また、他の情報との組合せにより、個人の特定につながる可能性がある。	定期区間として利用が少ない駅の情報を削除する。あるいは別の駅名に置き換える。 （セル削除/ノイズ付加）
②履歴情報		
処理名称 （出場/入場）		加工しない。
利用日時 （年月日・時間）	入場駅や出場駅に関する情報との組合せから、個人を特定できるリスク。	30 分単位に置き換える。 （丸め）
利用種別	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）
改札口	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）
入場駅／出場駅	入場駅と出場駅の組合せや利用時間帯によって、個人の特定につながる可能性がある。	入場駅、出場駅それぞれについて、利用者の少ない時間帯の情報を削除又は他の駅名に置き換える。（セル削除/ノイズ付加）
利用額	定期券区間に関する情報を復元することができる。 （提供先にとって不要な情報と想定）	本ケースでは提供先において不要な情報と考えられるため、全部削除する。（項目削除）
残額	定期券区間に関する情報を復元することができる。 （提供先にとって不要な情報と想定）	本ケースでは提供先において不要な情報と考えられるため、全部削除する。（項目削除）

③ 加工後のデータのイメージ

上記の考え方に基づいて加工されたデータは、次のようになる。

図表 7-15　鉄道の乗降履歴データのユースケースにおける加工後のデータのイメージ

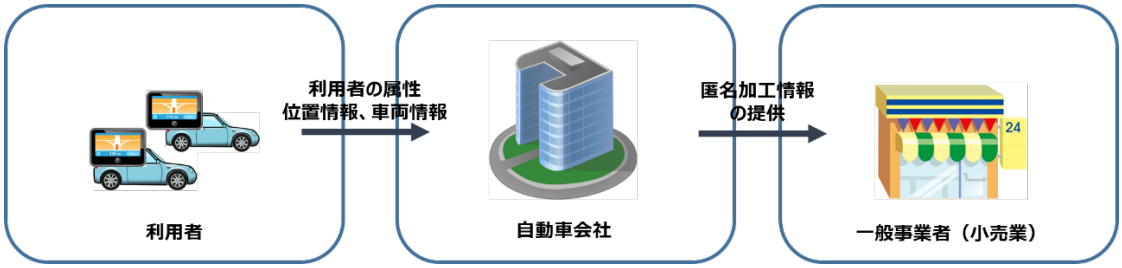
上記のユースケースは、鉄道の入場/出場の履歴に基づく人の動きに着目して分析する用途であるが、例えば、ある特定の駅における複数の改札口の利用人数等を細かく分析したい等のニーズもあり得る。このような場合には、より詳細な時刻が望ましい一方で、「どの駅で乗って、どの駅で降りたか」という一連の乗降履歴までは必要でない場合もあり得る。このようなケースにおいては、例えば、分析の対象外であるもう一方の入出場履歴を利用路線の情報に置き換えた上で詳細な時刻情報を残すような加工も考えられる。

7.2.2 移動履歴の事例

1）ユースケース

本ユースケースは、自動車会社が保有する移動履歴情報について、匿名加工を行ったうえで、匿名加工情報の枠組みを活用して、一般事業者（小売業）に提供するというものである。一般事業者においては、自動車の移動履歴とその所有者の年代や性別等の基本属性に基づいて、店舗における商品ラインナップの検討や新しい店舗の出店計画に活用することが想定される。

図表 7-16 自動車会社が保有する移動履歴情報を第三者に提供するユースケースのイメージ



本ユースケースにおいて加工対象となるデータセットは、①顧客属性データ及び②プローブデータの 2 種類からなり、ID によって、リンクされている。

顧客属性データには、顧客の基本属性のほか、車種名と車両識別番号が含まれている。一方、プローブデータは、各車両の車載通信機により定期的に自動車メーカーのデータセンターに送信されて蓄積されるものであり、日時と位置情報（緯度・経度）に加え、車両情報として車速及び ABS[39]作動フラグから構成されている。

図表 7-17 自動車会社が保有する移動履歴に関するデータのレイアウトサンプル

顧客属性データ

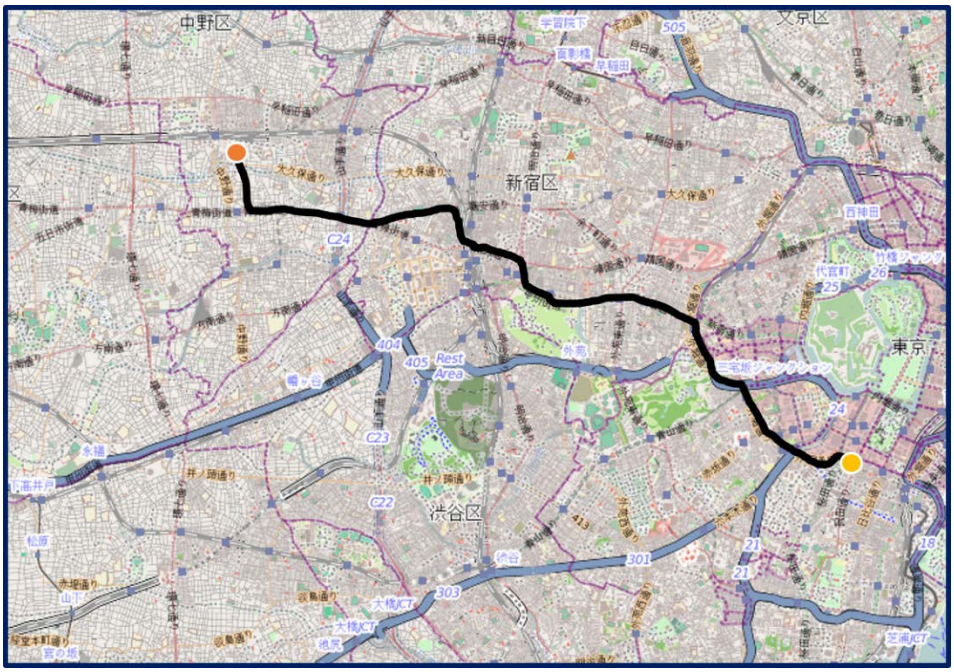
ID	氏名	性別	生年月日	電話番号	住所	車種	車両識別No.
53597201	田中 一郎	男	1972年4月4日	045-222-XXXX	神奈川県横浜市中区富士見町X-X-X	ロッソ	219YER9O
53012602	加藤 りえ	女	1983年12月9日	090-4444-YYYY	東京都千代田区霞が関Y-Y-Y	ベック	8L3JHE4K1
81567824	鈴木 博	男	1963年8月23日	03-0123-ZZZZ	東京都墨田区押上Z-Z-Z	ブラックバード	5H3QW2T3
…	…	…	…	…	…	…	…

プローブデータ

ID	日時分秒	緯度	経度	車速	ABS作動フラグ
53012602	2016/01/04 09:05:15	35.670186025715516	139.74682331068834	20km/h	0
53012602	2016/01/04 09:05:45	35.67040566777086	139.74502301216432	25km/h	0
53012602	2016/01/04 09:06:15	35.69364639843059	139.69933319458505	55km/h	0
53012602	…	…	…	…	…
53012602	2016/01/04 09:45:15	35.70323622947467	139.6699125759551	30km/h	0
53012602	2016/01/26 09:45:45	35.70364396678445	139.66972804017132	15km/h	0

[39] Antilock Brake System.

図表 7-18 プローブデータ（緯度･経度情報）が表す移動履歴



2）考慮すべき事項とリスクに対応した具体的な加工方法の検討

① 含まれ得る情報の種類

図表 7-17 に示すデータを、個人属性情報と履歴情報とに分類すると、次のようになる。

図表 7-19 自動車会社が保有する移動履歴に関するデータのレイアウトサンプル

顧客属性データ

個人属性情報

ID	氏名	性別	生年月日	電話番号	住所	車種	車両識別No.
53597201	田中 一郎	男	1972年4月4日	045-222-XXXX	神奈川県横浜市中区富士見町X-X-X	ロッソ	219YER9O
53012602	加藤 りえ	女	1983年12月9日	090-4444-YYYY	東京都千代田区霞が関Y-Y-Y	ベック	8L3JHE4K1
81567824	鈴木 博	男	1963年8月23日	03-0123-ZZZZ	東京都墨田区押上Z-Z-Z	ブラックバード	5H3QW2T3
…	…	…	…	…	…	…	…

プローブデータ

履歴情報

ID	日時分秒	緯度	経度	車速	ABS作動フラグ
53012602	2016/01/04 09:05:15	35.670186025715516	139.74682331068834	20km/h	0
53012602	2016/01/04 09:05:45	35.67040566777086	139.74502301216432	25km/h	0
53012602	2016/01/04 09:06:15	35.69364639843059	139.69933319458505	55km/h	0
53012602	…	…	…	…	…
53012602	2016/01/04 09:45:15	35.70323622947467	139.6699125759551	30km/h	0
53012602	2016/01/26 09:45:45	35.70364396678445	139.66972804017132	15km/h	0

② どのように加工すべきか

本ユースケースにおいて取扱いに気を付けるべき情報は、個人属性情報に含まれる車種情報や、履歴情報に含まれる位置情報（緯度、経度情報）の扱いと考えられる。

【個人属性情報】

＜車種情報の取扱い＞

車種に関する情報は、自動車の使用スタイル等を読み取ることができ有用である一方で、住所（居住エリア）等の情報との組合せから、個人の特定につながる可能性がある。したがって、具体的な車種名を削除して車両カテゴリーに一般化する等の加工を行うことが望ましい。

＜車両識別番号＞

車両識別番号は個々の車両を識別するために一意に割り当てられるものであり、直ちに特定の個人の識別につながるものではないが、その起点となり得る可能性はあると考えられる。本ユースケースにおいては、提供先における有用性もないと考えられるため、想定外の再識別リスクを防ぐ意味からも全部削除することが望ましい。

【履歴情報】

＜位置情報の取扱い＞

詳細な時刻情報と紐づく位置情報の連続したデータからは、ある地点から別の地点への移動の経路のみならず、夜間に同じ場所に滞留している位置情報からは自宅を推定することができ、昼間に同じ場所に滞留している位置情報からは、勤務先や通っている学校等を推定することが可能である。

したがって、このような連続的な位置情報を扱うデータセットにおいては、自宅や勤務先を特定できるような部分の位置情報を削除することが望ましい。このような位置情報の削除の仕方としては、次のような方法が考え得る。

- 自宅住所に基づいて所定の範囲における位置情報を削除する。
- 各移動履歴（自動車のイグニッション ON からイグニッション OFF まで）における始点・終点から所定の距離・或いは時間を一律削除する。
- 各移動履歴の始点・終点から数%の位置情報を削除する。

＜車速情報の取扱い＞

車速情報は位置情報と組み合わせて道路の混雑状況を把握することが可能である。小売店における出店計画において交通状況に関する情報は有用であると考えられる。一方、車速情報は時刻情報と組み合わせて移動距離を算出することが可能であるため、削除した位置情報の復元に利用できる可能性があるため、削除した位置情報に対応する部分の車速情報を削除することが必要である。

また、本ユースケースにおいては、提供先において詳細な車速情報については不要であるため、10km/h 単位で丸めるとともに、50km/h 以上についてはトップコーディングを行うことが望ましい。

また、本ユースケースにおいては、提供先の事業者における商品ラインナップの検討や出店計画等への利用が想定されていることから、道路種別 ABS の作動状況に関する情報は不要と考えられるため、ABS 作動フラグは全部削除することが望ましい。

以上の本ユースケースにおける各情報についての加工の方向性をまとめると、次のようになる。

図表 7-20　自動車の移動履歴データのユースケースにおける加工例

項目	想定されるリスク	望ましい加工
①個人属性情報		
ID	顧客属性データと移動履歴データを連結する符号として利用されている。	全部削除する、あるいは仮 ID に置き換える。（項目削除）
氏名	単体で個人を特定できる。	全部削除する。 （項目削除）
性別	生年月日や住所との組合せにより、個人の特定につながる可能性がある。	本ケースでは、生年月日と住所の加工により対応し、性別情報の有用性から加工をしない。
生年月日	住所や性別との組合せにより、個人の特定につながる可能性がある。	年代の 6 区分（20 代/30 代/40 代/50 代/60 代/70 代～）に置き換える。 （丸め/トップコーディング）
住所	生年月日や性別との組合せにより、個人の特定につながる可能性がある。 また、本人にアクセスできるリスクがある。	市区単位より細かい情報を削除する。（丸め）
車種	住所や生年月日等との組合せにより、個人の特定につながる可能性がある。	「高級車」「コンパクトカー」等の車種カテゴリーに置き換える。 （一般化）
車両識別番号	（提供先にとって不要な情報と想定）	全部削除する。（項目削除）
②履歴情報		
日時分秒	詳細な時刻情報と位置情報に基づいて、個人の特定につながる可能性がある。	秒を削除し、分単位に置き換える。（丸め）
緯度・経度	夜間や昼間の位置情報に基づいて、自宅や職場等が特定される可能性がある。	所定時間以上滞留している地点から一定範囲の緯度・経度情報を削除する。あるいは、走行開始から数分間及び走行終了前数分間の緯度・経度情報を削除する。 （セル削除/丸め）
道路種別	（提供先において不要な情報と想定）	全部削除する。（項目削除）
車速	時刻情報と組み合わせることで、削除した位置情報を復元できる可能性がある。	・緯度・経度情報を削除する時間帯の車速情報を削除する。 （セル削除） ・車速を 6 区分（～10km/h /10km/h /20km/h /30km/h /40km/h /50km/h 以上）に置き換える。（丸め）
ABS 作動フラグ	（提供先において不要な情報と想定）	全部削除する。（項目削除）

③ 加工後のデータのイメージ

上記の考えに基づいて加工されたデータは、図表 7-21 のようになる。

図表 7-21　自動車の移動履歴データのユースケースにおける加工後のデータのイメージ

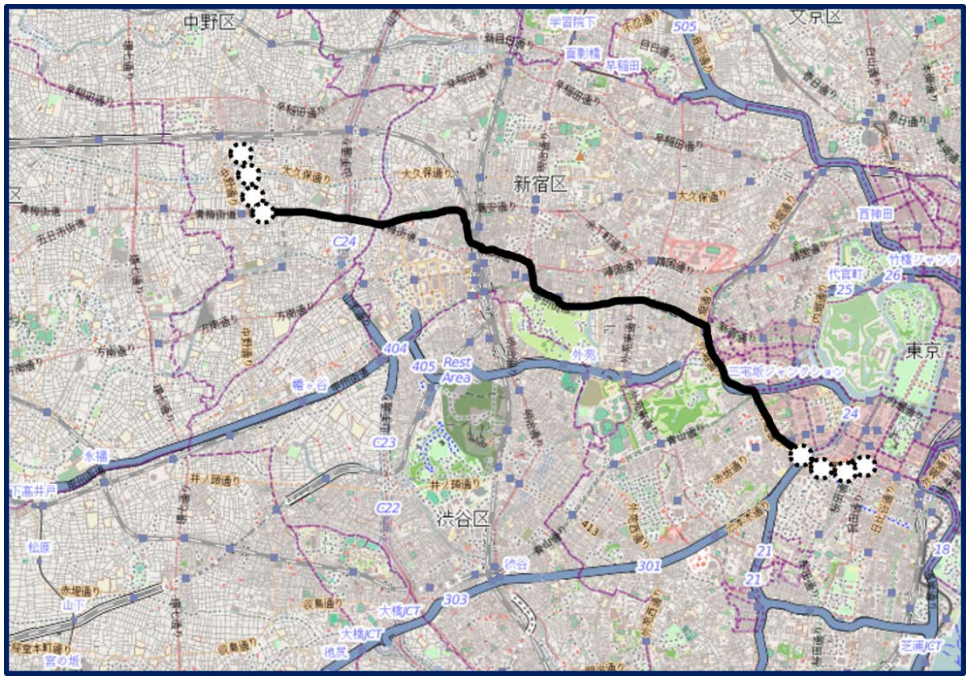
顧客属性データ

仮ID	性別	年代	車両タイプ	居住エリア
3e7ba68	男	40代	セダン	神奈川県横浜市
10d393f8	女	30代	コンパクト	千葉県船橋市
d416e64	男	60代	ミニバン	東京都墨田区
…	…	…	…	…

プローブデータ

仮ID	日時	緯度	経度	車速
10d393f8	2016/01/04 09:06	35.69364639843059	139.69933319458505	50km/h以上
10d393f8	2016/01/04 09:06	35.69467805968198	139.69868087166105	40km/h
10d393f8	2016/01/04 09:07	35.69782872486885	139.69727325020358	50km/h以上
10d393f8	…	…	…	…
10d393f8	2017/01/26 09:44	35.69746626454594	139.6710433899716	40km/h
10d393f8	2017/01/26 09:44	35.70244296802019	139.67199611244723	30km/h
10d393f8	2017/01/26 09:45	35.70261024687731	139.6699018428626	30km/h

図表 7-22　プローブデータ（緯度･経度情報）が表す移動履歴（加工後）



上記のユースケースは、自動車の移動履歴やその持ち主の基本属性に基づく小売店の出店計画や商品ラインナップの分析を目的としたものであるが、これ以外の用途として、例えば、地方公共団体が事故低減等に

向けた施策のための検討に活かしたり、保険会社が自動車の運転状況やその周囲の状況等の全体的な傾向を解析することにより保険の新プランの検討に活用したりすることが想定される。

このような場合には、車速や ABS 作動情報、道路種別の詳細な情報を必要とする一方で、長い移動履歴であったり、位置情報が不要なエリアがあったりすることが考えられるため、上記とは異なった方針による加工が想定される。

なお、本ユースケースは、自動車の移動履歴を扱うものであるが、スマートフォンアプリ等で取得される人の移動履歴を扱う場合は、移動の際の動きや速度が違うこと等への配慮が必要と考えられる。

7.3 電力利用履歴の事例

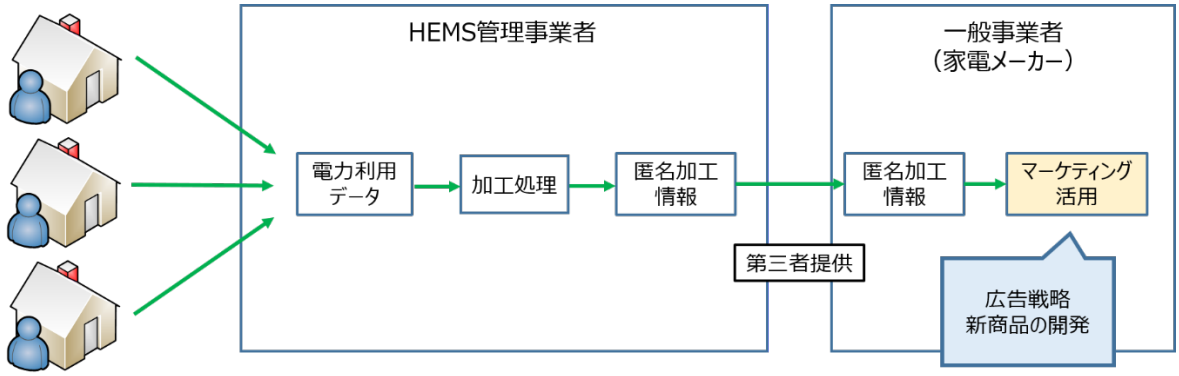
我が国において、2020 年代早期に家庭の全世帯にスマートメーターを導入することが、2014 年 4 月に閣議決定されたエネルギー基本計画[40]でも目標とされており、スマートメーターやネットワーク接続された分電盤等を通じて得られた家庭の電力使用量に係る履歴データが、今後、電力事業者、アグリゲーター、HEMS[41]サービサー等において取得・蓄積されていくことが想定される。

これらの電力利用データについては、電力使用パターンを踏まえた具体的な節電アドバイス、子供や一人暮らしの高齢者の見守り、生活様態推計を踏まえたマーケティング等の様々な目的のために活用が想定されるものであり[42]、例えば、電力事業者等について目的外利用あるいは第三者提供のために匿名加工情報を作成する次のようなユースケースが想定される。

1）ユースケース

HEMS 管理事業者が保有する電力利用量情報について、匿名加工を行った上で、匿名加工情報の枠組みを活用して、家電メーカー等の一般事業者へ提供するというものである。一般事業者においては、家族構成と各家電の使用状況とから生活スタイルの分析を行い、既存製品の広告戦略や新商品の開発に利用することが想定される。

図表 7-23 HEMS 管理事業者が保有する電力利用履歴情報を第三者提供するユースケースのイメージ



本ユースケースにおいて加工対象となるデータセットは、①顧客属性データ及び②電力利用データの 2 種類からなり、いずれも契約者 ID によってリンクされている。電力利用データのうち、推定使用家電については、各家庭の配電盤に設置されるエネルギー計測ユニットで計測される電流量の変化に基づいて、稼働中の家電の種類を推定している。

[40] http://www.enecho.meti.go.jp/category/others/basic_plan/pdf/140411.pdf

[41] Home Energy Management System.

[42] 経産省マニュアル P.15。

図表 7-24　HEMS 管理事業者が保有する電力利用履歴情報におけるデータのレイアウトイメージ

2）考慮すべき事項とリスクに対応した具体的な加工方法の検討

① 含まれ得る情報の種類

図表 7-24 に示すデータセットを、個人属性情報と履歴情報とに分類すると、図表 7-23 のようになる。

図表 7-25　HEMS 管理事業者が保有する電力利用履歴情報におけるデータのレイアウトサンプル

② どのように加工すべきか

本ユースケースでは、元の顧客属性データに詳細な住居情報や家族情報が含まれている。また、履歴情報については、電力利用量が詳細に把握できることに加え、その利用量の推移から使用している家電を推定することも可能となっている。これらの情報から、個人の特定につながる可能性に加え、生活パターン等のプライバシーに関わるような情報まで推測できる可能性があるため、それらに配慮した各情報の加工をするこ

とが望ましい。

【個人属性情報】
＜住居情報の取扱い＞
本ユースケースにおける住居情報は、住宅区分（戸建て/マンション）、施工年、延床面積からなっている。例えば、インターネット情報には、賃貸物件や分譲マンション等について、これらの情報を掲載するような住宅情報サービス等がある。したがって、一般的に容易に入手できる類の情報であり、特定の個人の識別につながる可能性があるため、一部の情報を削除したり丸めたりする必要がある。特に、施工年×延床面積の組合せによる特定リスクが高いと想定されるため、これらの情報について丸めることが望ましい。

＜家族情報の取扱い＞
家族情報は、家族の人数及び家族構成からなっている。HEMS 管理事業者が保有するデータには、住人（代表者）の基本属性に加えて、住所や住居に関する情報も含まれることから、家族情報とこれらの情報との組合せから個人の特定に至ることも想定される。
したがって、家族情報については、基本属性や住所・住居情報の加工度合いも鑑みながら、複数区分に置き換える等の加工を検討することが望ましい。

【履歴情報】
＜電力利用量の取扱い＞
電力の利用量については、その利用量の推移から、起床・就寝時間や在宅・不在等の生活パターンや、家族構成を推定することが可能である。その推定結果のみでは直ちに特定の個人の識別にはつながらないと考えられるが、特に顕著な利用量の推移（起床・就寝時間がデータセット内の他の人と比べて特異である等）が見られるものについて、加工を行うことが望ましい。取り得る加工手法としては、例えば、レコード自体の削除のほか、顕著な差異が見られる部分のデータを削除する等が考えられる。

＜推定使用家電＞
本ユースケースにおいては、電力利用量データに加えて、電流波形に基づいて使用されている家電のごとの使用状況を推定している。家電の使用状況から特定の個人を識別することは困難と考えられるが、電力利用量と家電の使用状況に他人との顕著な差異が見られる場合は、そこから読み取れる生活スタイル等の特異性に基づいて、個人の特定につながる場合も想定される。そのような場合には、そのレコード自体を削除することが望ましい。

以上の本ユースケースにおける各情報についての加工の方向性をまとめると、次のようになる。

図表 7-26 電力利用履歴のユースケースにおける加工例

項目	想定されるリスク	望ましい加工
①個人属性情報		
契約者 ID	内部での分散管理用 ID としての機能を有しており、この ID を起点として個人の特定につながる可能性がある。	全部削除する、あるいは仮 ID に置き換える。（項目削除）

項目	想定されるリスク	望ましい加工
氏名	単体で個人を特定できる。	全部削除する。 （項目削除）
電話番号	本人と密接な関係にある情報であり、他の事業者でも収集している可能性が高い。 また、本人にアクセスできるリスクがある。	全部削除する。 （項目削除）
性別	住所（居住エリア）や生年月日等との組合せにより、個人の特定につながる可能性がある。	本ケースでは、生年月日と住所の加工により対応し、性別情報の有用性から加工をしない。
生年月日	住所や性別等との組合せにより、個人の特定につながる可能性がある。 また、超高齢である場合は、それにより個人の特定につながる可能性がある。	年代の 6 区分（～20 代/30 代/40 代/50 代/60 代/70 代～）に置き換える。 （丸め/トップコーディング）
職種	少ない職種については、住所等他の情報との組合せにより、個人の特定につながる可能性がある。	少ない職種については、「その他」等に置き換える。（丸め）
住所	生年月日や性別との組合せにより個人を特定できるリスクがある。 また、本人にアクセスできるリスクがある。	市区単位より細かい情報を削除する。（丸め）
住居（竣工年）	居住エリア、延床面積との組合せにより、住所の特定につながる可能性がある。	築年数に変換するとともに、5 区分（5 年未満/5～10 年/10～15 年/15～20 年/20 年以上）に置き換える。（丸め）
住居（床面積）	居住エリア、築年数との組合せにより、住所の特定につながる可能性がある。	４区分（20 ㎡未満/20～40 ㎡/40～80 ㎡/80 ㎡以上）に置き換える。（丸め）
家族人数	大人数の家族に関する情報は、個人の特定の可能性を高めるおそれがある。	４区分（1 人/ 2 人/ 3 人/ 4 人以上）に置き換える。（丸め）
家族構成	家族人数や住所等の情報との組合せにより、個人の特定につながる可能性がある。	４区分（独居、夫婦のみ、親子、その他）に置き換える。（丸め）
②履歴情報		
日時	―	本ケースでは加工しない。
電力利用量	特異な電力使用量と他の情報との組合せにより、個人の特定につながる可能性がある。	極めて大きい電力使用量の情報を削除する。 （レコード削除/セル削除）
推定使用家電	電力利用量との組合せ等から特異な生活スタイル等が読み取れる場合に、個人の特定につながる可能性がある。	他人と顕著な差異が見られる人の情報を削除する。 （レコード削除）

③ 加工後のデータのイメージ

上記の考え方に基づいて加工されたデータは、次のようになる。

図表 7-27　電力利用履歴のユースケースにおける加工後のデータのイメージ

顧客データ

仮ID	性別	生年月日	職種	居住エリア	住居情報			家族構成	
					住宅区分	竣工年	延床面積	人数	家族構成
f261b69	男	1972/4/4	会社員	神奈川県横浜市中区	マンション	2005-2010	80㎡以上	2	妻、息子
c9b2786	女	1993/12/9	会社員	千葉県船橋市西船橋	マンション	2000-2004	20～40㎡	0	
88e53ac	男	1963/8/23	自営業	東京都墨田区押上	戸建	1985-1990	80㎡以上	3	母、妻、娘

電力利用データ

仮ID	日時	電力使用量	推定使用家電
f261b69	2016/12/23 19:00	610Wh	冷蔵庫、エアコン
f261b69	2016/12/23 19:01	607Wh	冷蔵庫、エアコン
f261b69	2016/12/23 19:02	612Wh	冷蔵庫、エアコン
f261b69	2016/12/23 19:03	1,042Wh	冷蔵庫、エアコン、ドライヤー
…	…	…	…

おわりに

我が国の様々な民間部門において、ビッグデータとして利用する有用性の高い様々なデータが蓄積されている。これらのデータの中でも特に顧客情報等と結びついてパーソナルデータとして蓄積されたデータは、データの信頼性・正確性も高く、有用性も高いものである。一方、これらについては、法上、当該民間部門（個人情報取扱事業者)において、個人情報として位置付けられるものが多く、第三者提供に際して法の観点あるいは顧客のプライバシーリスクへの懸念を払しょくする観点から、望ましい利活用の在り方が共有されず、「利活用の壁」という問題がある。

認定団体は、これまでも個人情報保護指針の作成及びこれを踏まえた事業者の自主的な取組を推進してきたところであるが、改正後の法に基づき、匿名加工情報の作成方法についても指針等において規定していくことが期待されている。

本レポートは、このような認識の下で取りまとめられたものであり、認定団体あるいは事業者団体等が指針あるいは業界自主ルール等を策定する際に匿名加工情報の作成方法について規定していくときに活用したり、事業者が直接参照して匿名加工情報を作成したりする際に参考となることを目的としたものである。

また、認定団体や事業者団体等においては、世界的な動向や技術の進展等も踏まえながら、個人情報保護指針及び業界自主基準等に加えて、具体的にどのような情報をどのような方法で加工すればよいのかということについて適切な事例を収集し発信したり、各認定団体や事業者団体における取組のベストプラクティスについて業界横断的に公表・共有していくことも有用であり、関係者が連携して取組を進めていくことが期待される。

匿名加工情報の制度は、個人情報及びプライバシーの保護を前提とした上で、民間部門に存在する有用性の高いパーソナルデータの第三者提供や目的外利用を可能とする制度である。関係者が連携して取組を進め、この制度が適切な形で幅広く民間部門に利用されることにより、消費者やサービス利用者の信頼を維持した形で安全にパーソナルデータの流通が促進され、新たな技術やサービスの創出につながることが期待される。

【参考資料】

I. 匿名加工情報に関連する法令の規定

I-1 個人情報の保護に関する法律（平成 15 年法律第 57 号。改正法全面施行時）（抜粋）

（定義）

第 2 条　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（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第 2 号において同じ。）で作られる記録をいう。第 18 条第 2 項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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

2　この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。

一　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

二　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

5　この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

一　国の機関

二　地方公共団体

三　独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）第 2 条第 1 項に規定する独立行政法人等をいう。以下同じ。）

四　地方独立行政法人（地方独立行政法人法（平成 15 年法律第 108 号）第 2 条第 1 項に規定する地方独立行政法人をいう。以下同じ。）

8　この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

9　この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。

一　第 1 項第 1 号に該当する個人情報　当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

二　第 1 項第 2 号に該当する個人情報　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

１０　この法律において「匿名加工情報取扱事業者」とは、匿名加工情報を含む情報の集合物であって、特定の匿名加工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その他特定の匿名加工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（第36条第1項において「匿名加工情報データベース等」という。）を事業の用に供している者をいう。ただし、第五項各号に掲げる者を除く。

（匿名加工情報の作成等）

第36条　個人情報取扱事業者は、匿名加工情報（匿名加工情報データベース等を構成するものに限る。以下同じ。）を作成するときは、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするために必要なものとして個人情報保護委員会規則で定める基準に従い、当該個人情報を加工しなければならない。

2　個人情報取扱事業者は、匿名加工情報を作成したときは、その作成に用いた個人情報から削除した記述等及び個人識別符号並びに前項の規定により行った加工の方法に関する情報の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、これらの情報の安全管理のための措置を講じなければならない。

3　個人情報取扱事業者は、匿名加工情報を作成したときは、個人情報保護委員会規則で定めるところにより、当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならない。

4　個人情報取扱事業者は、匿名加工情報を作成して当該匿名加工情報を第三者に提供するときは、個人情報保護委員会規則で定めるところにより、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。

5　個人情報取扱事業者は、匿名加工情報を作成して自ら当該匿名加工情報を取り扱うに当たっては、当該匿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、当該匿名加工情報を他の情報と照合してはならない。

6　個人情報取扱事業者は、匿名加工情報を作成したときは、当該匿名加工情報の安全管理のために必要かつ適切な措置、当該匿名加工情報の作成その他の取扱いに関する苦情の処理その他の当該匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

（匿名加工情報の提供）

第37条　匿名加工情報取扱事業者は、匿名加工情報（自ら個人情報を加工して作成したものを除く。以下この節において同じ。）を第三者に提供するときは、個人情報保護委員会規則で定めるところにより、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。

（識別行為の禁止）

第38条　匿名加工情報取扱事業者は、匿名加工情報を取り扱うに当たっては、当該匿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、当該個人情報から削除された記述等若しくは個人識別符号若しくは第36条第1項の規定により行われた加工の方法に関する情報を取得し、又は当該匿名加工情報を他の情報と照合してはならない。

（安全管理措置等）

第 39 条　匿名加工情報取扱事業者は、匿名加工情報の安全管理のために必要かつ適切な措置、匿名加工情報の取扱いに関する苦情の処理その他の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

I-2 個人情報の保護に関する法律施行令（平成 15 年政令第 507 号。改正法全面施行時）（抜粋）

（匿名加工情報データベース等）

第６条　法第２条第 10 項の政令で定めるものは、これに含まれる匿名加工情報を一定の規則に従って整理することにより特定の匿名加工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情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。

I-3 個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第３号）（抜粋）

（匿名加工情報の作成の方法に関する基準）

第 19 条　法第 36 条第 1 項の個人情報保護委員会規則で定める基準は、次のとおりとする。

一　個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

二　個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

三　個人情報と当該個人情報に措置を講じて得られる情報とを連結する符号（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該個人情報と当該個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。）。

四　特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

五　前各号に掲げる措置のほか、個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し、その結果を踏まえて適切な措置を講ずること。

（加工方法等情報に係る安全管理措置の基準）

第 20 条　法第 36 条第 2 項の個人情報保護委員会規則で定める基準は、次のとおりとする。

一　加工方法等情報（匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに法第 36 条第 1 項の規定により行った加工の方法に関する情報（その情報を用いて当該個人情報を復元することができるものに限る。）をいう。以下この条において同じ。）を取り扱う者の権限及び責任を明確に定めること。

二　加工方法等情報の取扱いに関する規程類を整備し、当該規程類に従って加工方法等情報を適切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を図るために必要な措置を講ずること。

三　加工方法等情報を取り扱う正当な権限を有しない者による加工方法等情報の取扱いを防止するために必要かつ適切な措置を講ずること。

（個人情報取扱事業者による匿名加工情報の作成時における公表）

第 21 条　法第 36 条第 3 項の規定による公表は、匿名加工情報を作成した後、遅滞なく、インターネットの利用その他の適切な方法により行うものとする。

2　個人情報取扱事業者が他の個人情報取扱事業者の委託を受けて匿名加工情報を作成した場合は、当該他の個人情報取扱事業者が当該匿名加工情報に含まれる個人に関する情報の項目を前項に規定する方法により公表するものとする。この場合においては、当該公表をもって当該個人情報取扱事業者が当該項目を公表したものとみなす。

（個人情報取扱事業者による匿名加工情報の第三者提供時における公表等）

第 22 条　法第 36 条第 4 項の規定による公表は、インターネットの利用その他の適切な方法により行うものとする。

2　法第 36 条第 4 項の規定による明示は、電子メールを送信する方法又は書面を交付する方法その他の適切な方法により行うものとする。

（匿名加工情報取扱事業者による匿名加工情報の第三者提供時における公表等）

第 23 条　前条第 1 項の規定は、法第 37 条の規定による公表について準用する。

2　前条第 2 項の規定は、法第 37 条の規定による明示について準用する。

II. パーソナルデータの匿名加工を巡る海外の動向

ここでは、諸外国におけるパーソナルデータやプライバシーに関する法制化や議論等の動向うち、特に匿名加工[43]について取り扱っているレポート等を紹介する。

II-1 米国における動向

米国では個人データに関する包括的な法律が制定されておらず、個別分野ごとに個人データの取扱いに関する法律が規定されている。その個別分野の法律としては、「医療保険の相互運用性と説明責任に関する法律」（HIPPA[44]）、「児童オンラインプライバシー保護法」（COPPA[45]）がある。

個人データの匿名加工に関しては、商業活動における不公正・欺瞞的な行為や習慣を監視・監督する米国連邦取引委員会（FTC[46]）が、“Protecting Consumer Privacy in an Era of Rapid Change”[47]というタイトルのレポート（FTC スタッフレポート）を 2012 年に発行しており、この中で個人データの匿名加工（de-identification）について触れているほか、国立標準技術研究所（NIST[48]）が、“De-identification of Personal Information”[49]という個人データの匿名加工に関するレポート（NIST レポート）を 2015 年 10 月に公表している。

また、上記の医療分野に特化した例として、“Guidance Regarding Methods of De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act”[50]というガイドライン（HIPAA ガイドライン）が発行されている。

II-1-1 FTC スタッフレポート（2012 年 3 月）

FTC スタッフによる事務局レポートは、①プライバシー・バイ・デザイン、②消費者の選択肢の簡易化、③データの透明性の確保、という 3 つの観点から、事業者に対してレポートのプラクティスに沿った行動を促すとともに、プライバシー政策立案のための提言を行う内容となっている。

レポートで提案されるフレームワークは、特定の消費者に対して合理的に連結可能なデータを対象としており、事業者が 3 つの措置を講じている場合には、そのデータは「合理的に連結可能ではない」ものとして、フレームワークの対象外であるとしている。その 3 つの措置は、

① 合理的な匿名加工処理（de-identification）を行うこと。
② 匿名加工されたデータを再識別しないことにつき、公にコミットすること。
③ 匿名加工されたデータを第三者に提供するときは、当該第三者による再識別行為を契約で禁止すること

であり、いわゆる FTC3 要件とも呼ばれているものである。

特に、2 つ目の要件について、事業者がこれに違反した場合、FTC は連邦取引委員会法第 5 条で禁

---

[43] II.で紹介するレポート等では、“anonymisation”という言葉が用いられているものと”de-identification”という言葉が用いられているものとがあるが、本レポートにおいては「匿名加工」という表現で統一するとともに、括弧書きで、用いられている言葉を示すこととする。

[44] Health Insurance Portability and Accountability Act.

[45] Children's Online Privacy Protection Rule.

[46] Federal Trade Commission.

[47] https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

[48] National Institute of Standards and Technologies.

[49] http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

[50] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

止されている「不公正・欺瞞的行為」に当たるとして、当該違反行為に対して差止請求や民事制裁金の請求等を行うことができる。

II-1-2 NISTレポート（2015年10月）

このレポートは、行政機関や権利擁護団体（advocacy group）、研究者等を対象とした、個人情報の匿名加工（de-identification）に関する論点や用語についての概要をまとめたものになる。具体的には、データ共有モデル、匿名加工のアプローチと代表的な匿名加工手法、領域別の匿名加工に関する事例評価、再識別リスクの評価方法等について紹介している。ただし、このレポートが匿名加工の適切性や特別な匿名加工アルゴリズムについて推奨する位置付けのものではないことも明記されている。

匿名加工については、個人データについて直接識別子（Direct Identifier）と準識別子（Quasi-Identifier）それぞれについて、次のような形で加工すべきことを示している。

（１） 直接識別子

直接識別子の例として、氏名、社会保障番号、電子メールアドレスを挙げており、直接識別子については、削除若しくはランダムな値等に置き換える必要があるとしている。

（２） 間接識別子（Sweeney による論文の事例では、生年月日、郵便番号、性別の 3 つが間接識別子に該当するとしている）

間接識別子は、後の解析のために重要でありデータセットの有用性にも影響することから、再識別リスクとのバランスに注意して行う必要があるとしている。間接識別子の加工処理としては、削除（Suppression）、一般化（Generalization）、摂動（Perturbation）、スワッピング（Swapping）、サブサンプリング（Sub-sampling）について例示するとともに、Emam 氏と Malin 氏による匿名加工の 11 ステップについても紹介している。

その後、“De-Identifying Government Datasets”（NIST SP800-188）の 1st ドラフトが 2016 年 8 月に、2nd ドラフトが 2016 年 12 月に公開されている。これは、タイトルどおり、米国政府の所有するパーソナルデータを対象とした匿名加工（de-identification）に関するガイドラインであり、その内容は、NIST レポートを基本的に踏襲した上で、匿名加工のガバナンスやマネジメント（目標等の特定やリスクの評価、教育等）や、匿名加工の技術的ステップについて、より具体的なアプローチ方法を示した内容となっている。

II-1-3 HIPAA ガイドライン（2012年11月）

このガイドラインは、HIPAA 法の適用対象である事業者（ヘルスケアプロバイダ、ヘルスケア情報センター、医療保険関係者等）を対象に、HIPAA プライバシールールに規定される医療情報の匿名加工（De-identification）基準を満たすための方法に関して、Q＆A 形式で説明するものである。

HIPAA プライバシールールにおいては、匿名加工することにより法規制の対象外となることが明確に規定されており、その匿名加工の基準として次の二つを挙げている。

（１） 専門家による判定（Expert Determination）

匿名加工のための統計的かつ科学的な方法に関する知識がある人物が再識別のリスクがとても低いとの判断を下した書面を提出すること

（２） セーフハーバー（Safe Harbor）

氏名や地理的区分、電話番号等、18 の識別子を削除すること及び対象事業者は本人を識別するための実知識を持たないこと

HIPAA ガイドラインは３部構成となっており、最初に HIPAA プライバシールールにおける匿名加工に関する規定の解説があった後、匿名加工の基準（専門家による判定及びセーフハーバー）ごとに Q&A をそれぞれ記載している。特に、専門家による判定に関する Q&A では、専門家による識別リスク評価の方法やアプローチ方法等が例示を交えながら解説されている。また、セーフハーバーに関する Q&A では、削除しなければならない情報や許容される情報がどのような情報か等、細かく解説されている。

II-2 欧州における動向

欧州データ保護指令の前文(26)では、データ主体がもはや識別できないように匿名加工されたデータについては法規制の対象外であることが明記されており、2018 年施行予定の一般データ保護規則（GDPR[51]）においても、同様の記載がされている。

個人データの匿名加工に関しては、第 29 条作業部会[52]によるオピニオン“Opinion 05/2014 on Anonymisation Techniques”[53]と、英国の情報コミッショナー事務局（ICO[54]）によるレポート“Anonymisation：managing data protection risk code of practice”[55]がある。

II-2-1 第 29 条作業部会によるオピニオン（2014 年４月）

このオピニオンでは、個人を識別できるかの判断は、識別に用いられるあらゆる合理的な手段を考慮して行われるとされている。技術が進歩することを踏まえて、あらゆる状況で識別ができないことまでを求めるものではなく、識別にかかる労力やコスト等から合理的な匿名化レベルが求められることになる。

また、既存の匿名加工手法について、その効果や限界を分析するものであり、各手法について、(i) ある個人をシングル・アウト可能か、(ii) ある個人に関するレコードと連結可能か、(iii) 情報がある個人に関係していると推定可能か、という３つの観点からロバスト性について述べているものである。

各手法の評価は、次のようになっている（リスクの有無を評価するものであり、匿名性を担保できるかを測るものではない）。

---

[51] General Data Protection Regulation.

[52] Article 29 Data Protection Working Party. 欧州データ保護指令第 29 条に基づいて設置される、個人データの取扱いに係る個人の保護に関する助言機関であり（第 29 条第 1 項）、本指令に従って採択された各国の措置の統一的な運用のために、当該措置の適用を含むあらゆる問題点について検討等を行う権能を有する（第 30 条第 1 項）。

[53] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[54] Information Commissioner’s Office.

[55] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

図表 II―1　匿名加工手法における長所と短所

加工手法	シングルアウト・リスク	連結リスク	推定リスク
仮名化	あり	あり	あり
ノイズ付加	あり	低い	低い
置換え（スワップ）	あり	あり	低い
集約化/ｋ-匿名化	なし	あり	あり
ℓ-多様化	なし	あり	低い
差分プライバシー	低い	低い	低い
ハッシュ化/トークン化	あり	あり	低い

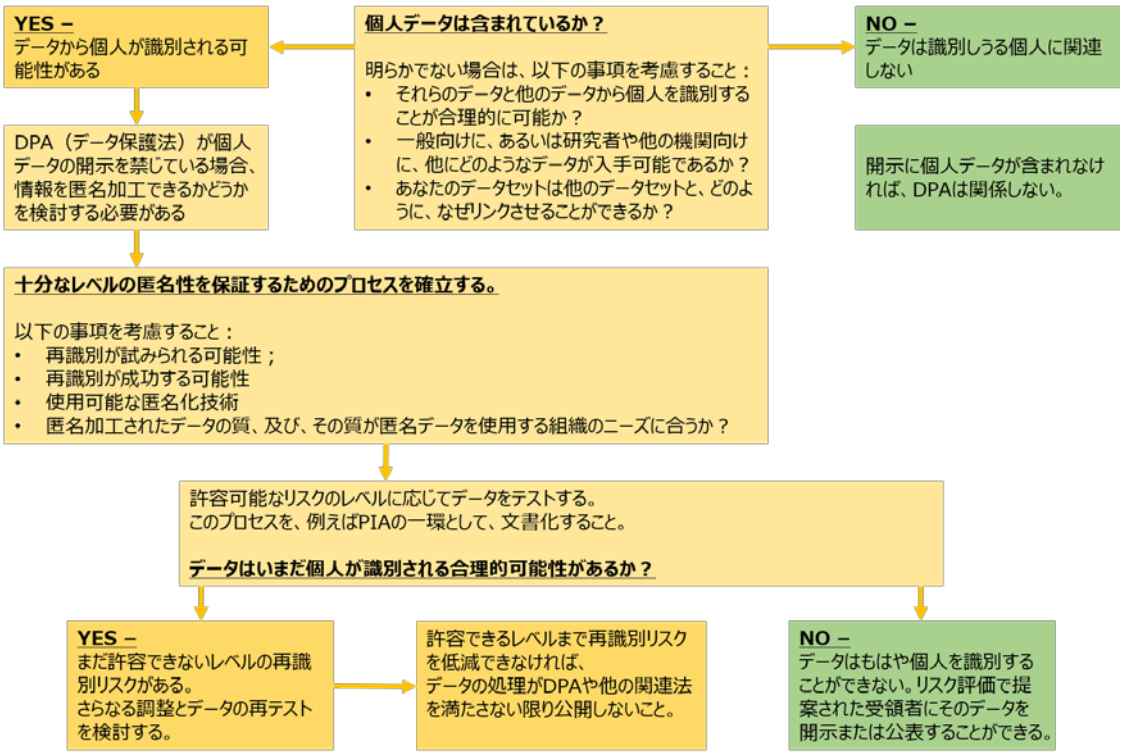
オピニオンでは、「匿名加工手法にはそれぞれ長所・短所が存在し、あらゆるデータセットに適用可能な最低限のパラメータを推奨することは不可能であり、ケース・バイ・ケースで考えるべき」と結論付けた上で、次のようなプラクティスを一般論として推奨するとともに、文脈的要素要素（contextual elements）及び技術要素（technical elements）についても、言及している。

- データ管理者（data controller）は、"リリース・アンド・フォーゲット"アプローチに頼らず、定期的に新しいリスクの特定や残存リスクの見直しや、認識しているリスクのコントロールが十分であるかを評価して必要に応じて調整する、等を行う必要があること
- 残存リスクの一部として、データセットの加工処理されていない部分の識別可能性を考慮すること。

II-2-2 英国 ICO レポート（2012 年 11 月)

このレポートは、英国における個人データの匿名加工のための実務指針として、個人データを匿名加工する意義やアドバンテージ、再識別リスク評価、ガバナンス等について述べているものである。事務局によるレポートという点は、FTC レポートや本レポートと同様の位置付けである。レポートにおいて、次のような匿名加工の検討フローも示されている。

図表 II-2　匿名データをいつどのように公表するかの検討フロー



また、レポートの付録として、匿名加工のケーススタディと匿名加工手法についての解説が用意されている。

II-3　その他の動向

II-3-1　オーストラリア

オーストラリアにおいては、2012 年改正のプライバシー法により、民間部門と公的分問に共通して適用されるオーストラリアプライバシー原則（APP[56]）というものがあり、その原則の一つとして「匿名性と仮名性（anonymity and pseudonymity）」（APP2）がある。

この APP2 においては、「本人は、APP 適用対象の組織に対して、識別しないよう、或いは、仮名化するよう求めることができる」とされ、個人が事業者等に要求することのできるオプションとして規定がされている。ただし、例外として匿名加工や仮名化が実用的でない場合等については、当該オプションを提供する必要がないことも認められている。

また、2014 年 4 月には、オーストラリア情報コミッショナー事務局により、“Privacy business resource 4: De-identification of data and information”というレポートが公表されている。

このレポートにおいては、「情報が、もはや個人を識別できる、あるいは合理的に識別できる状態でない」場合に、「匿名化（de-identification）された」としており、その判断基準としては、コスト、困難さ、実用性、再識別の見込みが挙げられている。なお、匿名加工の手法としては、次の 2 つのステップが記載されている。

① 氏名、住所、生年月日等の個人識別子（personal identifier）を削除すること

② 珍しい特徴やユニークな特徴の組合せにより特定の個人の識別にはつながり得る情報については、削除若しくは置換すること

[56] Australian Privacy Principles.

II-3-2 韓国

韓国では、情報技術の発展に伴うデータの利用の重要性から、2016 年 6 月に、6 機関[57]の合同で個人データの匿名加工（de-identification）に関するガイドライン[58]を公表している。

このガイドラインにおいては、匿名加工について、①事前レビュー、②匿名加工処理、③加工の十分性の評価、④再識別防止のためのフォローアップ・マネジメントの 4 つのフェーズで解説している。

匿名加工の対象となる属性情報としては、個人の特性（性別、年齢、住所、宗教、趣味嗜好等）、身体的特徴（血液型、体重、目の色、診療記録等）、信用情報（納税、信用格付け、収入レベル等）、経歴情報（学校名、専攻、職務経歴、勤務先等）、電子媒体に関する情報（クッキー、ログイン日時、アクセスログ、GPS データ等）、家族情報（配偶者や子供等に関する情報、法廷代理人等）等が例示されている。

また、加工の十分性の評価については、外部の専門家によって k-匿名性や ℓ -多様性等の評価手法を用いた評価が行われることとされている。

II-3-3 国際規格

個人情報やプライバシーの保護に関しては、国際規格化も行われており、代表的なものとして、“ISO/IEC 29100 Privacy Framework”や“ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”等がある。匿名加工に関しては、“ISO/IEC 20889 Privacy enhancing data de-identification techniques”（ISO/IEC 20889）として、規格化の議論がされている[59]。

ISO/IEC 20889 は、プライバシー強化技術（PET[60]）の一環として、データの匿名化（de-identification）に言及するものである。具体的には、再識別リスクに効果的に対処するためには状況に応じた匿名加工手法の選択が必要であり、匿名加工に係る用語を定義するとともに、特徴に応じた匿名加工手法の分類、再識別リスク低減の適用可能性（applicability）について明確化することを目的としている。

なお、“anonymization”及び“anonymous data”については、既に国際規格として成立している ISO/IEC 29100 “Privacy Framework“において、次のように定義されている。

anonymization:

process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

anonymous data:

data that has been produced as the output of a personally identifiable information anonymization process

---

[57] 国務調整室、行政自治部、放送通信委員会、金融委員会、未来創造科学部、保健福祉部。

[58] Guidelines for De-identification of Personal Data.
（https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000827254&fileSn=0）

[59] 2017 年 1 月時点で、委員会原案（Committee Draft）まで進んでいる。

[60] Privacy enhancing techniques.

III. 参考文献

【 報告書等 】

- 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「技術検討ワーキンググループ報告書」（2013 年 12 月）。
  http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf
- 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「技術検討ワーキンググループ報告書 ～「（仮称）準個人情報」及び「（仮称）個人特定性低減データ」に関する技術的観点からの考察について～」（2014 年 5 月）。
  http://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou1-2.pdf
- Suica に関するデータの社外への提供に関する有識者会議「Suica に関するデータの社外への提供について 中間とりまとめ」（2014 年 2 月）。
  http://www.jreast.co.jp/chukantorimatome/20140320.pdf
- Suica に関するデータの社外への提供に関する有識者会議「Suica に関するデータの社外への提供について とりまとめ」（2015 年 10 月）。
  http://www.jreast.co.jp/information/aas/20151126_torimatome.pdf
- 総務省 緊急時等における位置情報の取扱いに関する検討会「位置情報プライバシーレポート ～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～」（2014 年 7 月）。
  http://www.soumu.go.jp/main_content/000303636.pdf
- 経済産業省「事業者が匿名加工情報の具体的な作成方法を検討するにあたっての参考資料（「匿名加工情報作成マニュアル」）」（2016 年 8 月）。
  http://www.meti.go.jp/press/2016/08/20160808002/20160808002-1.pdf
- 国立情報学研究所 匿名加工情報に関する技術検討ワーキンググループ「匿名加工情報の適正な加工の方法に関する報告書 2017 年 2 月 21 日版」（2017 年 2 月）。
  http://www.nii.ac.jp/about/reports/pd/report-kihon-20170221.pdf
- Article 29 Data Protection Working Party, “Opinion 05/2014 on Anonymisation Techniques”, April 2014.
  https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf
- Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change”, March 2012.
  https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
- National Institute of Standards and Technologies, “De-identification of Personal Information”, October 2015.
  http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf
- National Institute of Standards and Technologies, “De-Identifying Government Datasets” (1st Draft, August 2016/2nd Draft, December 2016) .
  http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf
- Office for Civil Rights, U.S. Department of Health & Human Services, “Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule”,

November 2012.
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf
- UK Information Commissioner's Office, “Anonymisation: managing data protection risk – code of practice”, November 2012.
https://ico.org.uk/media/1061/anonymisation-code.pdf
- Office of the Australian Information Commissioner, Australian Government, “Australia Privacy Principles Guidelines”, February 2014.
https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf
- Office of the Australian Information Commissioner, Australian Government, “Privacy business resource 4: De-identification of data and information”, April 2014.
https://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy_business_resource_4.pdf

【 標準 】

- ISO/IEC 29100:2011, Information technology -- Security techniques -- Privacy framework.
- ISO/IEC 27018:2014, Information technology – Security techniques -- Code of practice for personally identifiable information (PII) protection in public clouds acting as PII processors.
- ISO/IEC 20889 Committee Draft 2016-12-02, Information technology –- Security techniques –- Privacy enhancing data de-identification techniques. 2016.

【 論文 】

- L. Sweeney, “k-Anonymity: A Model For Protecting Privacy”, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), pp.557-570, 2002.
- A. Narayanan and V. Shmatikov, “Robust de-anonymization of large sparse datasets”, In Proceedings of 2008 IEEE Symposium on Security and Privacy (S&P), pp.111-125, IEEE, 2008.
- Hiroaki Kikuchi, Katsumi Takahashi, “Zipf Distribution Model for Quantifying Risk of Re-identification from Trajectory Data”, Journal of Information Processing, Vol.24, No.5 pp.816-823, 2016.

【 書籍 】

- 瓜生和久編『一問一答 平成 27 年改正個人情報保護法』（商事法務、2015 年 12 月）
- 中川裕志『プライバシー保護入門』（勁草書房、2016 年 2 月）
- 佐久間淳『データ解析におけるプライバシー保護』（講談社、2016 年 8 月）
- Khaled El Emam, Luk Arbuckle（笹井崇司訳）『データ匿名化手法』（オライリー・ジャパン、2015 年 5 月）