個人情報保護委員会事務局レポート：
匿 名 加 工 情 報
Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information

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
Towards Balanced Promotion of Personal Data Utilization and Consumer Trust

2017 年 2 月

February 2017

個人情報保護委員会事務局

Personal Information Protection Commission Secretariat

目次
Teble of Contents

【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）

[Abbreviations]

"Personal Information Protection Act," "Act" Act on the Protection of Personal Information (Act No. 57 of 2003)

"Enforcement Order" Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003)

"Enforcement Rules" Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of 2016)

"Guidelines" Guidelines on the Act on the Protection of Personal Information (Anonymously Processed Information) (Public Notice of the Personal Information Protection Commission No. 9 of 2016)

"Guidelines on General Rules" Guidelines on the Act on the Protection of Personal Information (General Rules) (Public Notice of the Personal Information Protection Commission No. 6 of 2016)

"Amendment Act" Act for Partial Revision of the Act on the Protection of Personal Information and Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 65 of 2015)

※ 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。

*Unless otherwise noted, article numbers for the Act on the Protection of Personal Information appearing in this report are as of the date on which amendments to the Act on the Protection of Personal Information based on the Amendment Act fully come into effect (May 30th, 2017).

はじめに

Preface

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。

The acquisition, collection, analysis and distribution of personal data including personal information are becoming to play increasingly important roles in social and economic activities, innovation and economic growth. As the permeation of IoT[1] and AI[2] is expected to enable ever-more-massive data acquisition and analysis in the future, the importance of arranging the environment for utilization of personal data including personal information is increasing.

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。

In addition, as international information distribution is accelerated and it gets easier to provide services to overseas clients and receive services from overseas providers, it is extremely important to develop an environment where Japanese companies and relevant organizations are able to provide various services using a wide range of domestic and overseas personal data including personal information, while also securing user confidence through proper handling of such data.

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。

The anonymously processed information system was introduced to meet such need. The minimum matters are provided in the law, cabinet order, regulation and guidelines. In addition to these, it is expected that accredited personal information protection organizations (hereinafter referred to as "accredited organizations") and trade associations will formulate voluntary regulations that provide specific processing standards for anonymously processed information according to the characteristics, etc. of personal data they are handling.

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

[1] Internet of Things：モノのインターネット
Internet of Things

[2] Artificial Intelligence：人工知能
Artificial Intelligence

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。

Meanwhile, the Personal Information Protection Commission has formulated this report (hereinafter referred to as the "Report") to provide information that will help accredited organizations set processing standards for anonymously processed information and prepare personal information policies and help trade associations develop voluntary rules, etc. Besides promoting the formulation of such policies, etc., this Report is also aimed at providing a reference to be used by individual companies and relevant organizations in preparing anonymously processed information.

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。

We hope that this Report will be of benefit to accredited organizations that will formulate policies, etc. concerning anonymously processed information as well as to companies and relevant organizations that are interested in the creation and handling of anonymously processed information.

1. イントロダクション

1. Introduction

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

1.1 Backdrop of the Introduction of the Anonymously Processed Information System by the Amended Personal Information Protection Act

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。

The Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the "Personal Information Protection Act" in 1.1) was promulgated on May 30, 2003 and fully came into effect on April 1, 2005. In the ten years since the enforcement of this Act, the situation surrounding personal information has dramatically changed due to the rapid development of information and communication technologies.

「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。

In relation to personal information, etc., the Declaration on the Creation of the World's Most Advanced IT Nation (decided by the Cabinet on June 14, 2013) states as follows. "In order to create an environment for data utilization and promote the use of open data and big data, a new investigative organization will be immediately established under the IT Strategic Headquarters. This new organization will work to develop data utilization rules, which promote data utilization while also securing the protection of personal information and privacy, at the earliest time possible by the end of this year. At the same time, policies for the review of the system will be also formulated by the end of this year with an eye to the introduction of new legal measures, such as the establishment of a third organization with monitoring, supervising, complaint and dispute resolution functions."[3] Following this decision, the Study Group on

[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。
http://www.kantei.go.jp/jp/singi/it2/pdf/it_kokkasouzousengen.pdf At P.7, it states "as for the handling of 'personal data,' i.e. data related to individuals' actions, status, etc., which is seen as being particularly useful among other kinds of big data, the government will create a project environment that will facilitate the utilization of such data, while

Personal Data was established under the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society. Discussion concerning "anonymization" was also carried out by this Study Group.[4] In December 2013, the Study Group announced the Policies for the Review of the System Concerning Personal Data Utilization. Reports[5] were submitted by the subordinate Technical Study Working Group.

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

---

also securing the protection of personal information and privacy." It also states that "the government will promote the dissemination of measures taken so far in areas for which rules have already been established, such as the handling of smartphone user information."

[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。

The Regulatory Reform Implementation Plan (approved by the Cabinet in June 2013) (http://www.kantei.go.jp/jp/kakugikettei/2013/__icsFiles/afieldfile/2013/06/20/20130614-03.pdf), which was formulated based on the reports of the Council for Regulatory Reform, requested the Cabinet Secretariat and the Consumer Affairs Agency to "formulate guidelines that specify the details of reasonable anonymization measures" by the end of first half of 2014. In the report by the Council's Business Working Group (June 2013) (http://www8.cao.go.jp/kisei-kaikaku/kaigi/publication/130605/item5.pdf), FTC's three requirements are cited and a "concern" was expressed as follows. "If a company (X) has both original data and new data, i.e. processed data with which specific individuals are not identifiable, and X provides only new data to a third party (Y), there is no risk of infringement of these individuals' rights and interests, as long as re-identification by Y is prohibited under the agreement between X and Y. Then, Japan should also clearly stipulate that new data does not fall under the category of 'personal information.'"

[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）

Study Group on Personal Data, "Report by the Technical Study Working Group" (December 2013) (http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf) and "Report by the Technical Study Working Group: Examination of 'Quasi-Personal Information (Tentative Name)' and 'Data with Reduced Identifiability (Tentative Name)' from Technical Perspectives" (May 2014) (http://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou1-2.pdf).

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]。

The Outline of the System Reform Concerning Personal Data Utilization decided by the Headquarter on June 24, 2014, states that it is desirable that by enabling the collection and analysis of mass data of various kinds, i.e. big data, it will contribute to the creation of new industries and services and solution of social challenges in Japan, and that on the other hand Japan needs to create a system to secure consumer trust through the proper handling of personal data, which need to be protected, as consumers' awareness toward personal information and privacy is heightening.[6] It also refers to the need to address the "gray area" arising from ambiguity in the legal interpretation of the scope of personal information,[7] while information other than personal information has been out of the scope of regulation. The Outline of the System Reform points out the issue of the "wall of utilization," referring to a state where potential information users hesitate to promote personal data utilization out of fear of privacy-related criticism from the public, as they are uncertain of how they can handle information properly from the perspective of privacy and the Personal Information Protection Act. The document states that it is necessary to create an environment to realize data utilization while enhancing the protection of personal information and privacy. Specifically, it shows the direction that the basic principles concerning a fundamental system which will enable the provision of personal data processed into "data with reduced identifiability" to a third party without consent from a principle of such data, will be established under the law[8], that details concerning such system will be provided by cabinet orders, ministerial orders,

---

[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。
Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, "Outline of the System Reform Concerning Personal Data Utilization" (June 2014) (http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20140624/siryou5.pdf). In addition, it is not particularly rare that information that is already accumulated in a great amount is not fully utilized.

[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。
The Outline points out that "there is ambiguity concerning the scope of protection and information handing rules to be followed by companies, in relation to personal data that is likely to be linked to specific individuals, even though such data itself does not identify any specific individuals, and thus entails a risk that individuals' rights and interests may be infringed due to improper information handling."

[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。
The Outline states that proper information protection and utilization should be promoted, since there is much information that needs to be handled properly but is hoped to be used more often to contribute to individual and public interests, such as medical information.

regulations and guidelines, and that use of voluntary regulation rules will be also promoted for the private sector at the same time.[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。

The Act for Partial Revision of the Act on the Protection of Personal Information and Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 65 of 2015; hereinafter referred to as the "Amendment Act"), which was enacted in September 2015, was formulated based on the content of the Outline of the System Reform. As one of the contents of amendments, a system named "anonymously processed information" was introduced. In addition, the Cabinet Committees expressed the following in the supplementary resolution based on the Diet deliberations concerning the revision bill: "In light of the purpose of the provisions concerning anonymously processed information, that is, to promote the utilization of such information, standards that are to be established under the Rules of Personal Information Protection Commission should be stipulated with consideration of effective information utilization." (Cabinet Committee, House of Representatives) "In light of the purpose of the provisions concerning anonymously processed information, that is, to promote the utilization of such information, the Personal Information Protection Commission should give due consideration to this purpose when establishing standards that are necessary for personal information handling business operators in preparing anonymously processed information." "After the enforcement of this Act, ... efforts must be made to gain public understanding and confidence concerning information utilization by means of public relations campaigns and other activities, while

[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。

The Outline states as follows: "In light of the usefulness and variety of data, methods for processing data and reducing the level of identifiability are not to be standardized; instead, it has to be ensured that data can be processed by an optimal means according to the characteristics of projects, etc." In relation to such processing methods, it states that private bodies are to formulate voluntary regulation rules and acquire accreditation for such rules or for private bodies themselves from an independent organization (Personal Information Protection Commission). It also states that best practices concerning proper processing methods need to be shared.

ensuring the proper handling of personal information and anonymously processed information." (Cabinet Committee, House of Councilors)

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。

As symbolized by such keywords as IoT and big data, how data collection, analysis and commercial utilization are made is considered to be important factors in securing competitiveness in today's business world. It is expected that the anonymously processed information system will contribute to the promotion of active data utilization, while securing safety, by compliance with the processing standards and other rules.

1.2 本レポートの位置付け

1.2 Positioning of This Report

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。

Article 36, paragraph (1) of the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the "Act") provides that the processing of anonymously processed information is to be carried out in accordance with standards prescribed by rules of the Personal Information Protection Commission.[10] Said rules provide minimum standards that apply to companies of all industries, while the Guidelines explain the aforementioned rules as well as the definition, etc. of anonymously processed information.

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。

On the other hand, specific means for processing personal information in accordance with the standards stipulated in the rules and guidelines are to be decided in　personal information protection guidelines and other voluntary rules prepared by accredited organizations, since such means should be determined according to the characteristics of the personal information they are handling, situation of handling of such information, etc.

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。

This Report mainly focuses on approaches and methods for creating anonymously processed information (related to Article 36, paragraph (1) of the Act), prohibition against the act of identifying (related to Article 36, paragraph (5) and Article 38 of the Act), and security control actions for processing method, etc.-related information (Article 36, paragraphs (2) and (6) and Article 39 of the Act), and provides information and ideas that may be useful for accredited organizations, trade associations, etc. in creating rules on the preparation of anonymously processed information, and for private companies in actually creating anonymously processed information.

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

[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。
The processing standards for anonymously processed information are provided in Article 19 of the Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3).

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。

As this Report provides only a brief introduction to other obligations for personal information handling business operators and anonymously processed information handling business operators (such as the disclosure obligation, which applies when anonymously processed information is created or provided to a third party), those who wish to learn more about these obligations are advised to see the Guidelines on the Act on the Protection of Personal Information (Anonymously Processed Information) (Public Notice of the Personal Information Protection Commission No. 9 of 2016; hereinafter referred to as the "Guidelines").

2. 個人情報とその取扱いにおける制約

2. Personal Information and Restrictions on Its Handling

2.1 個人情報の定義

2.1 Definition of Personal Information

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。

Article 2, paragraph (1) of the Act provides the definition of personal information as follows.

法第2条第1項

Article 2　(1)

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。

Article 2　(1)　"Personal information" in this Act means that information relating to a living individual which falls under any of each following item:

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。）

(i)　those containing a name, date of birth, or other descriptions etc. (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other forms that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph, item (ii)); the same shall apply in Article 18, paragraph (2)); hereinafter the same) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual)

二　個人識別符号が含まれるもの

(ii)　those containing an individual identification code

「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。

"A specific individual can be identified" means that a specific individual can be identified in general social term by using information stored alone or in combination with other information, and it depends on whether ordinary people would be able to arrive at identifying said information with a living person, with their ability to judge and understand information.

「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。

The phrase "readily collated with other information" refers to what is called "identifiability." Although identifiability of data needs to be determined case by case according to the situation of business operators, it is basically defined as a state wherein the information can be readily collated with other information by a means that is ordinarily used in usual business operation.

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。

An individual identification code, which was introduced under Article 2, paragraph (1), item (ii) of the Act through the law amendment, is defined as follows under Article 2, paragraph (2) of the Act.

法第2条第2項

Article 2　(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。

(2)　An "individual identification code" in this Act means those prescribed by cabinet order which are any character, letter, number, symbol or other codes falling under any of each following item.

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

(i)　those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily partial feature of the specific individual has been converted in order to be provided for use by computers

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

(ii)　those character, letter, number, symbol or other codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or, stated or recoded for the said user or purchaser, or recipient of issuance

「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。

An "individual identification code" is any character, letter, number, symbol or other codes falling under any of the items of Article 2, paragraph (2) of the Act stated above, and also is prescribed by a cabinet order. The Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; hereinafter referred to as the "Enforcement Order") and the Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of 2016; hereinafter referred to as the "Enforcement Rules") provide the definition of an individual identification code in a detailed and exhaustive manner as shown in Figure 2-1.

図表 2-1 個人識別符号に係る法・施行令・施行規則の関係

Figure 2-1 Relationship among the Act, Enforcement Order and Enforcement Rules concerning individual identification codes

法 Act	施行令（第1条） Enforcement Order (Article 1)	施行規則（第2条～第4条） Enforcement Rules (Articles 2 to 4)
第１号関係 Related to item (i)	(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 Those character, letter, number, symbol or other codes produced by having converted any of the following bodily features therein to be provided for use in computers and which conform to standards prescribed by rules of the Personal Information Protection Commission as sufficient to identify a specific individual. イ ＤＮＡを構成する塩基の配列 (a) base sequence constituting DNA; 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 (b) appearance decided by facial bone structure and skin color as well as the position and shape of eyes, nose, mouth or other facial elements; ハ 虹彩の表面の起伏により形成される線状の模様 (c) a linear pattern formed by an iris' surface undulation; ニ 発声の際の声帯の振動、声門の開閉並び	（第2条） (Article 2) 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。 Standards in the character, letter, number, symbol or other codes produced by having bodily features therein converted to be provided for use in computers shall be converted for the purpose of being provided for use in computers in an appropriate scope by using an appropriate method so as to ensure the level of ability to identify a specific individual.

に声道の形状及びその変化

(d) vocal cords' vibration, glottis' closing motion as well as the shape of vocal tract and its change when uttering;

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

(e) bodily posture and both arms' movements, step size and other physical appearance when walking;

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

(f) Intravenous shape decided by the junctions and endpoints of veins lying under the skin of the inner or outer surface of hands or fingers;

ト 指紋又は掌紋

(g) a finger or palm print.

第 2 号関係
Related to item (ii)

(2) 旅券の番号、

(ii) Passport number;

(3) 基礎年金番号、

(iii) Basic pension number;

(4) 運転免許証の番号、

(iv) Number of a driver's license;

(5) 住民票コード

(v) Resident record code;

(6) 個人番号

(vi) Individual number;

(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）

(Article 3)

(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

(i) Symbol and number of, and insurer's number on,

(vii) Those character, letter, number, symbol or other codes prescribed by rules of the Personal Information Protection Commission which are stated on a certificate of national health insurance, late-stage medical care system for the elderly, or long-term care insurance, in a way to give each person who receives the respective issuances a different one.	a certificate of national health insurance; (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 (ii) Number of: and insurer's number on, a certificate of late-stage medical care system for the elderly, or long-term care insurance.
(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 (viii) Any other character, letter, number, symbol or other codes prescribed by rules of the Personal Information Protection Commission as equivalent to (i) to (vii) above.	（第4条） (Article 4) 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 Symbol and number of: and insurer's number on, a certificate of national health insurance, symbol and number of: and insurer's number on, a member certificate, etc. of the Public Servants' Mutual Aid Association, insured person's number on an employment insurance-insured person's certificate, number of a special permanent resident certification, etc.

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]。

As regards an individual identification code as provided under Article 2, paragraph (2), item (i) of the Act, among biometric data as listed in (a) to (g) of Article 1 of the Enforcement Order in Figure 2-1 above that meets the

standards prescribed by the Enforcement Rules ("convert for the purpose of being provided for use in computers in an appropriate scope by using an appropriate method so as to ensure the level of ability to identify a specific individual"), "base sequence constituting DNA" as provided in (a) means "genome data that makes it possible to identify an individual based on genotype data, such as whole nuclear genome sequencing data, whole exome sequencing data, whole-genome single-nucleotide polymorphism (SNP) data, sequencing data comprised of 40 or more mutually independent SNPs, short tandem repeat (STR) with four bases repeated at nine or more loci, etc.," while those falling under any of (b) to (g) mean "feature information extracted from relevant biometric data that is made capable of identifying an individual when used by a device or software aimed at recognizing an individual."[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。

An individual identification code as provided in Article 2, paragraph (2), item (ii) of the Act includes publicly issued codes, such as an Individual Number, while privately issued codes, such as service ID, mobile phone number, and credit card number are not included. However, it should be noted that even though such privately issued codes themselves are not individual identification codes, they may be personal information falling under Article 2, paragraph (1), item (i) of the Act, solely or in combination with other information.

2.2 個人情報を取り扱う上での制約

2.2 Restrictions on the Handling of Personal Information

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）。

A person providing a personal information database etc. for use in business is called a "personal information handling business operator" (Article 2, paragraphs (4) and (5) of the Act), who is required to comply with the obligations provided under Chapter IV of the Act. Major disciplinary rules are as follows (cited with a focus on the matters that are closely related to anonymously processed information).

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）

(i) A personal information handling business operator must specify the purpose of utilizing the personal information. In addition, changes to said utilization purpose must not be made beyond the scope recognized reasonably relevant

[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。
For more details, see Section 2-2 of the Guidelines on the Act on the Protection of Personal Information (General Rules) (Public Notice of the Personal Information Protection Commission No. 6 of 2016).

to the pre-altered utilization purpose (Article 15).

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）

(ii) A personal information handling business operator must not handle personal information without obtaining in advance a principal's consent beyond the scope of the utilization purpose specified (Article 16).

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）

(iii) A personal information handling business operator must not acquire personal information by deceit or other improper means (Article 17).

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）

(iv) A personal information handling business operator must, in case of having acquired personal information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a principal of, or disclose to the public, the utilization purpose (Article 18).

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）

(v) Except in those cases provided by the law, a personal information handling business operator must not provide personal data to a third party, without obtaining in advance a principal's consent or by such means as introducing an opt-out clause (Article 23, paragraphs (1) and (2)).

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。

On the other hand, the introduction of a service or product in a new area often creates a need for business operators to use personal information for a new purpose that is poorly related to the utilization purpose that was specified upon the acquisition of said information. However, to re-acquire consent from all principals based on Article 16 of the Act may involve some significant demerits in terms of cost and speed. In some cases, it could be difficult to acquire consent from principals concerning past data utilization or to acquire consent from many users.

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。

Under the Act before the amendment as well, it was allowed to use information that is processed from personal information and made incapable of identifying a specific individual by eliminating the relationship between the information and said specific individual, such as statistical information, without the restrictions as stated above, since such information was positioned as being out of the scope of regulation by the law. Meanwhile, there was no shared rule or consensus concerning to what extent information needs to be processed in order for the information to no longer fall in personal information. For example, there was a case where a plan to provide transportation history data on railway IC cards to a third party was suspended, since some questioned whether anonymization processing for personal information was conducted to a sufficient extent, while others pointed out the need for providing adequate explanation for users and giving due consideration to privacy.[12]

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。

As seen above, as there are some gray areas around the scope of personal information and interpretation for anonymization processing methods, and as public awareness for privacy is heightening, it is important to secure social confidence concerning personal data utilization, to remove hurdles for data utilization for various purposes and provision to a third party, and to promote proper data utilization by establishing rules and consensus on the proper handling of personal data, including personal information held by business operators and organizations in Japan, which are to be followed when using such data for various purposes and providing such data to a third party.

---

[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。

Expert Panel on the External Provision of Suica Data "Interim Report on the External Provision of Suica Data" (February 2014) (http://www.jreast.co.jp/chukantorimatome/20140320.pdf). *K*-anonymization of transportation history data degrades data's usability as it requires massive data removal. As a solution for this problem, it was suggested that JR should apply statistical work to data before providing it to an external body.

3. 匿名加工情報とは

3. What is Anonymously Processed Information?

3.1 匿名加工情報を利用するアドバンテージ

3.1 Advantages for Utilizing Anonymously Processed Information

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。

The anonymously processed information system is intended to promote data transactions and personal data utilization, including data collaboration, among business operators by making it possible under certain rules to use de-identified personal information for a purpose other than the specified purpose and to provide such information to a third party without obtaining a principal's consent. This system is expected to create new business and services and eventually improve public convenience.

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。

The definition of anonymously processed information is given in Article 2, paragraph (9) of the Act and rules on its handling are provided in Articles 36 to 39 of the Act. By making and handling anonymously processed information in compliance with these rules, personal information handling business operators are able to use personal data for a purpose other than the specified purpose and to provide such data to a third party stably without obtaining a principal's consent under the legal framework. In return, anonymously processed information handling business operators are able to access and use a wide variety of anonymously processed information.

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。

In addition, regarding the processing and proper handling of anonymously processed information, a third party organization, namely the Personal Information Protection Commission, provides the minimum standards, while accredited organizations, etc. are to formulate personal information protection policies and other specific voluntary rules and promote compliance with such rules by relevant business operators. Such efforts are expected to secure proper personal data utilization that assures the public a sense of security.

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]。

Examples of the utilization of anonymously processed information include the following. [i] Creation of new services and innovations, through the cross-sectorial utilization of purchase history data on point cards and transportation history data on transportation IC cards among multiple business operators. [ii] Contribution to the drug development and clinical fields, through utilization of medical information held by medical institutions, and contribution to the improvement of the quality of life for the public, through the provision of accurate traffic forecasts and weather forecasts utilizing probe data, such as running history data obtained from a car navigation system, etc.[13]

3.2 匿名加工情報の定義

3.2 Definition of Anonymously Processed Information

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。

Anonymously processed information is defined as follows under the Act and explained as below under the Guidelines.

法第 2 条第 9 項

Article 2　(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。

(9)　"Anonymously processed information" in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

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。）。

(i)　personal information falling under paragraph (1), item (i); Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

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

[13] 2015 年 5 月 8 日衆議院・内閣委員会における政府答弁。
Government's statement at the meeting of the Cabinet Committee of the House of Representatives on May 8, 2015

含む。)。

(ii) personal information falling under paragraph (1), item (ii); Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes)

ガイドライン 2-1 匿名加工情報（法第 2 条第 9 項関係）

Guidelines 2-1 Anonymously Processed Information (Related to Article 2, paragraph (9) of the Act)

「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。

"Anonymously processed information" means information relating to an individual that can be produced from processing personal information in a manner to neither be able to identify a specific individual by taking action specified for each division of personal information nor to be able to restore the personal information to re-identify a specific individual.

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。

If personal information falls under the category of "those containing a name, date of birth, or other descriptions etc. whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual)" as provided in Article 2, paragraph (1), item (i) of the Act, the phrase "processing personal information in a manner to neither to be able to identify a specific individual" means to delete the name, date of birth, or other descriptions, etc. contained in said personal information so as not to be able to identify a specific individual.

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。)。

If personal information falls under the category of "those containing an individual identification code" as provided in Article 2, paragraph (1), item (ii) of the Act, the phrase "processing personal information in a manner neither to be able to identify a specific individual" means to delete all individual identification codes contained in said

personal information so as not to be able to identify a specific individual (if said personal information still falls under Article 2, paragraph (1), item (i) of the Act after this measure is taken, said personal information needs to be processed as personal information falling under said item as stated above).
「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。
It is provided that "deleting" includes "replacing the individual identification codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes." A "method with no regularity that can restore the individual identification codes" means a method with which the descriptions etc. that could identify a specific individual or individual identification code before the replacement cannot be restored from the descriptions after the replacement.

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。
Information "whereby a specific individual can be identified" appearing in the Act means information stored alone or in combination with other information, which is considered as such in general social terms when it is examined with their ability to judge and understand information whether ordinary people would be able to arrive at identifying said information with a living person. The requirement of anonymously processed information stating "so as neither to be able to identify a specific individual" does not necessarily require the elimination of every technical possibility that a specific individual could be identified, assuming every possible means. Instead, it requires anonymously processed information to be at least in a state wherein a specific individual cannot be identified by a personal information handling business operator or anonymously processed information handling business operator by an ordinary means, in light of the ability of and methods, etc. available to an ordinary person or business operator.

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。
In addition, the phrase "nor to be able to restore the personal information" means that anonymously processed information is in a state wherein personal information cannot be restored by an ordinary means, such as identifying from the anonymously processed information a description etc. that could identify a specific individual or individual identification code contained in personal information from which the anonymously processed information was derived.
「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。
The requirement stating "nor to be able to restore the personal information" does not necessarily require the elimination of every technical possibility that personal information could be restored, assuming every possible means. Instead, it requires anonymously processed information to be at least in a state wherein said personal information cannot be restored by a personal information handling business operator or anonymously processed information handling business operator by an ordinary means, in light of the ability of and methods, etc. available to an ordinary person or business operator.

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）
When creating anonymously processed information, information needs to be processed in accordance with the standards provided by the Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of 2016; hereinafter referred to as the "Enforcement Rules") as provided in Article 36, paragraph (1) of the Act. Necessary measures, including those provided in Article 2, paragraph (9) of the Act, are provided in said Rules. (For processing obligations that need to be followed when producing anonymously processed information, see Section 3-2 (Proper Processing of Anonymously Processed Information).)

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。

"Statistical information" means data that can be obtained by extracting items concerning a common element from information taken from multiple people and tallying them up by category, which is intended to quantitatively determine the tendency or characteristics of a group. Therefore, statistical information does not fall under the category of "information relating to an individual" as provided in the Act, as long as the corresponding relationship between said information and a specific individual is eliminated. Thus, the Act after the amendment, as well as before the amendment, defines statistical information as being out of scope of regulation.

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。

Anonymously processed information is information relating to an individual that is produced from personal information with which a specific individual cannot be identified and original personal information cannot be restored. Since it is information relating to an individual, unit information can be that corresponding to an individual person.[14] A collection of anonymously processed information is defined by the term "anonymously processed information database etc." under Article 2, paragraph (10) of the Act.

3.2.1 「特定の個人を識別することができない」とは

3.2.1 What Does the Phrase "not to Be Able to Identify a Specific Individual" Mean?

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。

As explained in the Guidelines, information "whereby a specific individual can be identified" refers to information

[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。

In addition to "non-individualized, non-identifiable information" (information in a state wherein individuals are not distinguished (and said individuals cannot be identified)) as referred to in the "Report by the Technical Study Working Group" (December 2013) by the Study Group on Personal Data, "individualized, non-identifiable information" (individuals are distinguished but cannot be identified) may also fall under the category of anonymously processed information in some cases.

stored alone or in combination with other information, which is considered as such in general social terms when it is examined with their ability to judge and understand information whether ordinary people would be able to arrive at identifying said information. The requirement of anonymously processed information stating "so as neither to be able to identify a specific individual" does not necessarily require the elimination of every technical possibility that a specific individual could be identified, assuming every possible means. Instead, it requires anonymously processed information to be at least in a state wherein a specific individual cannot be identified by a personal information handling business operator or anonymously processed information handling business operator by an ordinary means, in light of the ability of and methods, etc. available to an ordinary person or business operator.

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

3.2.2 What Does the Phrase "not to Be Able to Restore the Personal Information" Mean?

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。

As explained in the Guidelines, the phrase "not to be able to restore the personal information" means that anonymously processed information is in a state wherein personal information cannot be restored by an ordinary means, such as identifying from the anonymously processed information a description etc. that could identify a specific individual contained in personal information or individual identification code from which the anonymously processed information was derived.

「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。

The requirement stating "not to be able to restore the personal information" does not necessarily require the elimination of every technical possibility that personal information could be restored, assuming every possible means. Instead, it requires anonymously processed information to be at least in a state wherein said personal information cannot be restored by a personal information handling business operator or anonymously processed information handling business operator by an ordinary means, in light of the ability of and methods, etc. available to an ordinary person or business operator.

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。

As stated above, both of the requirements expressed in the phrases "so as neither to be able to identify a specific individual" and "nor to be able to restore the personal information" are to be determined based on the ability of and methods, etc. available to an ordinary person or business operator. They do not necessarily require the elimination of every technical possibility, such as identification and information restoration attempted with a supercomputer or other highly functional resources, or advanced hacking skills, for example.

3.2.3 一部の情報が復元できた場合について

3.2.3 When a Part of Information Has Been Restored

「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定し得る情報が復元されることも「復元」に該当する。

To "restore the personal information" means to restore information that leads to the identification of a specific individual. In other words, the term "restoration" not only refers to the restoration of the entire original information from anonymously processed information, but also the restoration of a part of original personal information that can identify a specific individual.

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。

On the other hand, the term "restoration" does not include the restoration of a part of information that does not lead to the identification of a specific individual. For example, when all telephone numbers were removed from the original personal information to produce anonymously processed information, it is possible that dialing codes could be restored based on the postal codes and resident areas (municipalities) contained in anonymously processed information. However, even if such dialing codes could be restored, it would not constitute a state described in the phrase "restore the personal information," as long as information is not restored to an extent that a specific individual can be identified.

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

3.2.4 What Does the Phrase "Replacing Such Descriptions etc. with Other Descriptions etc. Using a Method with No Regularity That Can Restore the Descriptions etc." Mean?

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。

When personal information is processed to anonymously processed information in order for a specific individual not to be identified, replacing descriptions etc. with other descriptions etc. using a method with which the replacing descriptions etc. cannot be reversed to the original descriptions etc. (a method with no regularity that can restore the descriptions, etc.), as well as deleting relevant descriptions etc. as needed, is a possible method.
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。
Here, a "method with no regularity that can restore the descriptions etc." means a method that has no regularity in conversion from the replaced descriptions etc. to the descriptions etc. contained in original personal information. This provision does not necessarily require the lack of regularity for replacing the descriptions, etc.

3.3 匿名加工情報を取り扱う上での制約

3.3 Restrictions on the Handling of Anonymously Processed Information

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。
A personal information handling business operator is required to comply with the provisions of Article 36 of the Act when producing and handling anonymously processed information (limited to those comprising an anonymously processed information database). A personal information handling business operator producing anonymously processed information is subject to the obligation to take security control actions for preventing the leakage of processing method etc.,related information, disclosure obligation when producing anonymously processed information and providing it to a third party, prohibition against the act of identifying, etc. in addition to the obligation of proper proessing as provided in Article 36, paragraph (1) of the Act.
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。)。
In addition, an anonymously processed information handling business operator that receives anonymously processed

information processed and produced from personal information by another business operator and that utilizes it for business is required to comply with the provisions of Articles 37 to 39 of the Act. An anonymously processed information handling business operator that receives anonymously processed information is subject to prohibition against the act of identifying, the obligation to strive to take security control actions for anonymously processed information, and disclosure obligation when providing anonymously processed information to a third party. Note that if a personal information handling business operator that produced anonymously processed information provides an anonymously processed information database etc. concerning said anonymously processed information for use in business, said personal information handling business operator also constitutes an anonymously processed information handling business operator; however, obligations provided under Articles 37 to 39 of the Act do not apply to such business operator, since these obligations are applied to the handling of anonymously processed information other than "those which it produced itself by processing personal information" (the provisions of Article 36 of the Act are applied when a personal information handling business operator handles anonymously processed information it produced itself by processing personal information).

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。

Figure 3-1 shows the relationships stipulated by Articles 36 to 39 of the Act.

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

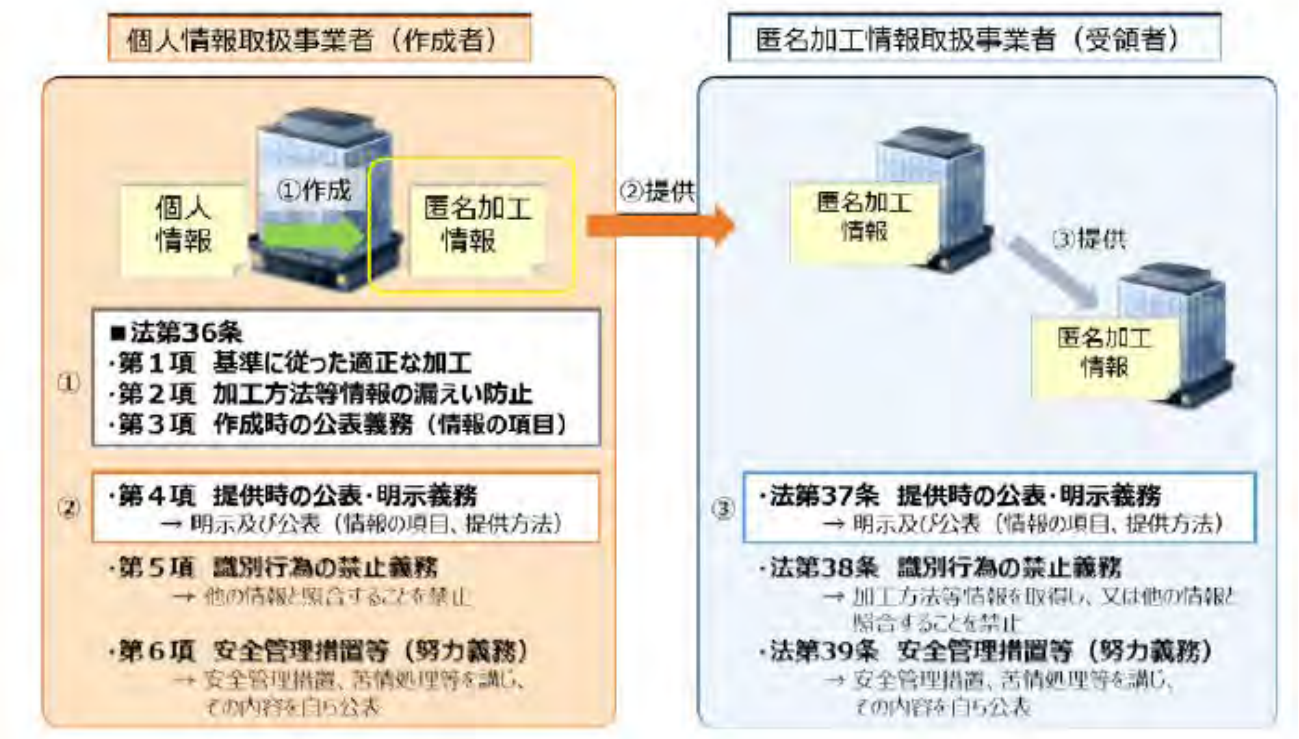
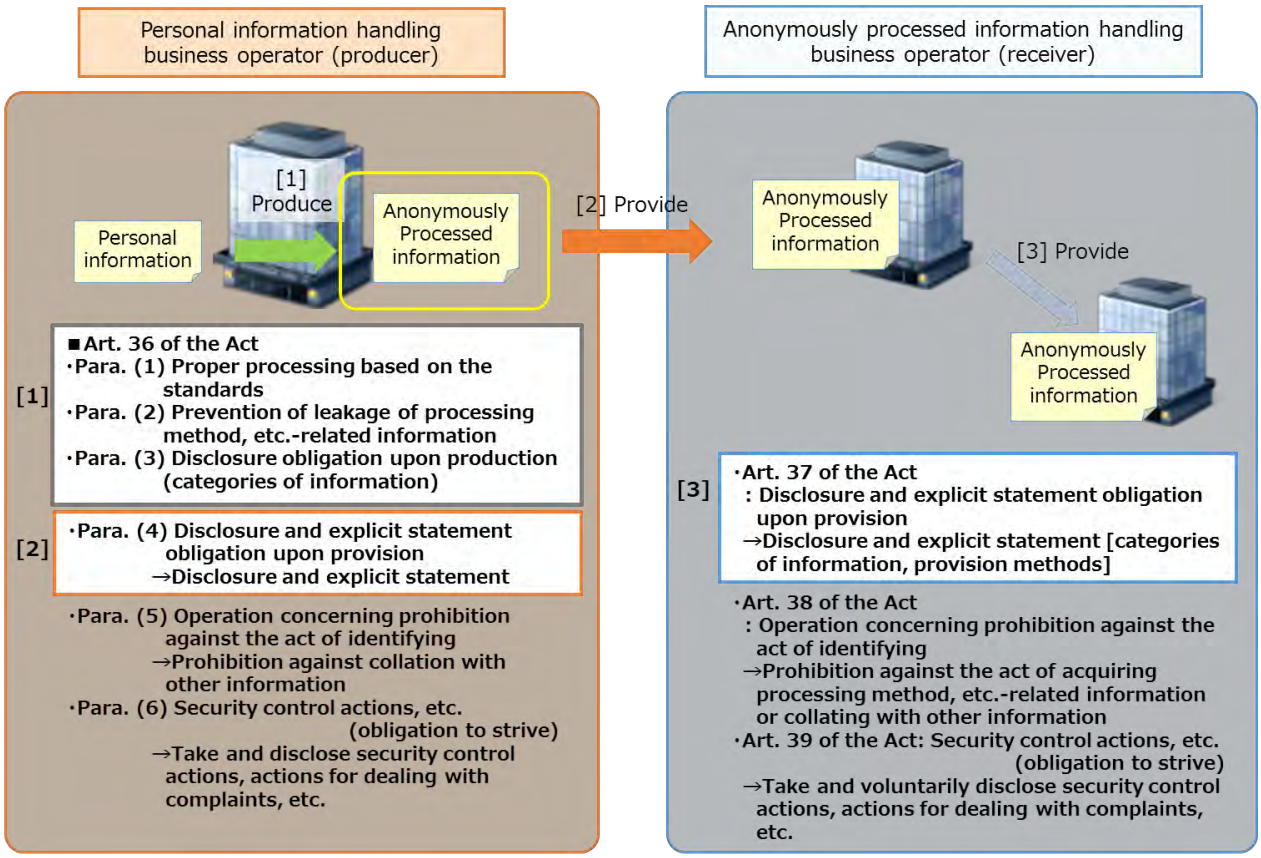


Figure 3-1 Provisions that must be complied with by producers and receivers of anonymously processed information



3.4 匿名加工情報に関する留意点

3.4 Things to Be Note Concerning Anonymously Processed Information

3.4.1 統計情報について

3.4.1 Regarding Statistical Data

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]。

As defined in Article 2, paragraphs (1) and (9) of the Act, personal information and anonymously processed information are both "information relating to an individual." Meanwhile, "statistical information" means data that can be obtained by extracting items concerning a common element from information taken from multiple people and tallying them up by category, which is intended to quantitatively determine the tendency or characteristics of a group. The Guidelines states as follows: "statistical information does not fall under the category of 'information relating to an individual' as provided in the Act, as long as the corresponding relationship between said information and a specific individual is eliminated. Thus, the Act before the amendment defined statistical information as being out of scope of regulation, and it has been so ever since then." Accordingly, statistical information that has been properly processed does not constitute personal information or anonymously processed information.[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。

However, in a case where statistical values are divided into certain ranges, for example, there could be a range where the volume of samples is extremely small, depending on the method for setting said ranges (such as information on elderly people, high-spending users, and locations in underpopulated areas). In such a case, statistical information could readily identify an individual. Beyond putting information into the form of statistical information, what is more important is that the information is processed into statistical information in a way that ensures the elimination of

[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。
Such Statistical information includes those created by tallying individual survey results, and disclosed and made available to the public or provided to a third party as statistical information under the responsibility of the producer of said statistical information. Examples of statistical information include publicized statistical charts from public statistical projects as well as private statistical information prepared by industry organizations and private survey companies, etc.

corresponding relationships with individuals to an adequate level.

3.4.2 容易照合性との関係

3.4.2 **Relationship to Identifiability**

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。

A business operator that produced anonymously processed information retains the original personal information and can retain a chart indicating the corresponding relationships between the anonymously processed information and original personal information. This gives a rise to a possibility that such personal information and chart are deemed to have what is called "identifiability" as described in the provision of Article 2, paragraph (1), item (i) of the Act in parentheses, that such anonymously processed information is still regarded as personal information, and thus that compliance with the obligations concerning the handling of personal information (Chapter IV, Section 1 of the Act) is required.

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。

Anonymously processed information is processed so that a specific person cannot be identified from it and that the original personal information from which the anonymously processed information is made cannot be restored, and also there is a systematic assurance that the act of identifying is prohibited. Therefore, anonymously processed information is defined as being out of the scope of personal information since anonymously processed information cannot be regarded as being in a state that allows for collation with the original personal information by a means that is ordinarily used in usual business operation (in other words, the information has identifiability)

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。

Therefore, a business operator that produced and uses internally anonymously processed information is also allowed to use said anonymously processed information freely by observing the obligation concerning the handling of anonymously processed information (Article 36).

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。

Anonymously processed information is required to be in a state wherein a specific individual cannot be identified and personal information cannot be restored. Whether "a specific individual cannot be identified" is to be determined based on the ability to judge and understand information of ordinary people and ordinary business operators, as is the case with the requirement stated in parentheses of Article 2, paragraph (1), item (i) of the Act. In addition, whether personal information "cannot be restored" is also determined based on the same criteria.

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。

In light of the purpose of the law, the anonymously processed information system is intended to promote the utilization of information relating to an individual, while securing safety in the course of utilization and distribution, for situations wherein said information is to be used for a purpose other than the original purpose or wherein said information is provided to another anonymously processed information business operator. Since this system is intended to allow for the provision of personal information to a third party while requiring processing and compliance with the regulations, it is considered to be adequate to determine safety with consideration to the judgment and comprehension abilities of ordinary people and ordinary business operators.

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。

Note that the system stands on the premise that a business operator that produces anonymously processed information internally retains original personal information from which the anonymously processed information is derived, and processing method, etc.-related information. While it is not appropriate to regard corresponding charts, which exists inside the said business operator and is subject to the obligation of prohibition against the act of identifying, as especially dangerous, such business operator is naturally required to comply with the obligations concerning the handling of anonymously processed information, including prohibition against the act of identifying and including security control actions for processing method, etc.-related information.

(参考)「容易照合性」

(Reference) "Readily Identifiable"

「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。

"Readily identifiable" refers to a state wherein, even if information itself cannot identify a specific individual, a business operator handling the said information can collate it with other information using a means ordinarily used in the business operation conducted by the said business operator, without conducting any special investigation, incurring any special costs or making any special efforts. The Act provides that information "whereby a specific individual can be identified" as a result of being in such state is subject to legal protection as it falls under the scope of personal information.

「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]。

Criteria for determining whether "readily identifiable or not" include whether there is a person that can access retained information, an organizational structure for developing internal regulations, and technological framework for access control of the information system. Whether "a specific individual can be identified" is to be determined by comprehensively conducting examination in reference to these criteria case by case according to the situation of the business operator such as the content of handled personal information and methods for utilizing said information.[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。

For example, suppose a case where each department of a business operator stores acquired personal information in a separate database established for each department. If it is strictly prohibited for staff of these departments and database supervisors to handle said databases by means of regulation or operation, so that they cannot collate information on the databases using a means that is ordinarily used in usual business operation, and if information on said databases cannot actually be collated with each other using a means that is ordinarily used in usual business

[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）。
Compiled by Kazuhisa Uryu, "Ichimon Itto 2015 Amendment to the Act on the Protection of Personal Information" (Shoji Houmu, 2015) P. 13 (Q8)

operation and without spending special costs or making special efforts, it is deemed that such information is not in a state wherein it "can be readily collated with other information."

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]。

Meanwhile, if it is possible to collate information on both database using a means that is ordinarily used in usual business operation, it is considered to fall under the case wherein information "can be readily collated with other information."

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。

“Readily iIdentifiable” as referred to in parentheses of Article 2, paragraph (1), item (i) of the Act means the possibility to collate information with other information inside a business operator, as described above. Since this concept is considered to apply to the definition of "personal information" in the context of the obligations for personal information handling business operators as provided in Chapter IV, Section 1 of the Act (Articles 15 to 35 of the Act), identifiability concerning "personal information"[18] in the context of restrictions on the provision of information to a third party as provided in Article 23 of the Act is to be also determined based on the possibility to collate information with other information inside a business operator.

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。

In addition, the requirement that information "can specify a specific individual" as provided in Article 2, paragraph (1), item (i) of the Act outside of parentheses refers to information stored alone or in combination with other information, which is considered as such in general social terms when it is examined whether ordinary people would be able to arrive at identifying said information with a living person, with their ability to judge and understand information.

---

[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。
Personal Information Protection Commission "Guidelines on the Act on the Protection of Personal Information" and "Q&A on 'Response to an Incident of Personal Data Leakage, etc.'" (February 2017) 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。
Article 23 of the Act provides for obligations concerning the handling of "personal data." As it is clear from its definition in Article 2, paragraph (6) of the Act, "personal data" relies on the interpretation of "personal information" as defined in Article 2, paragraph (1) of the Act.

3.5 匿名加工情報の作成とは

3.5 What Does It Mean to Produce Anonymously Processed Information?

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。

As provided in Article 36, paragraph (1) of the Act, personal information must be processed in accordance with the standards provided by the Enforcement Rules in order to produce anonymously processed information.

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。

Article 36 (1) A personal information handling business operator shall, when producing anonymously processed information (limited to those constituting anonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production.

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。

The Guidelines give explanation on the "production of anonymously processed information" as follows.

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）

Guidelines 3-2 Proper Processing of Anonymously Processed Information (Related to Article 36, paragraph (1) of the Act)

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。

A personal information handling business operator must process personal information in accordance with the standards as provided in each item of Article 19 of the Rules when producing anonymously processed information (limited to those constituting an anonymously processed information database etc. (*1); the same applies hereinafter) (*2), so as neither to be able to identify a specific individual nor to be able to restore the personal information. In order to "process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission," the processing standards as provided in each item of Article 19 of

the Rules need to be met according to the nature of the information to be processed.

（※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。

(*1)While the obligations concerning the handling of anonymously processed information (Articles 36 to 39 of the Act) are applied concerning anonymously processed information constituting an anonymously processed information database, etc., they are not applied to handling of anonymously processed information that does not constitute an anonymously processed information database, or what is called "scattered information."

（※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。

(*2) The phrase "when producing" means when producing anonymously processed information in order to handle information related to individuals as anonymously processed information. Therefore, if information is still handled as personal information after deleting (replacing with other descriptions etc.) a part of personal information: such as names as part of security control actions, if personal information is processed into statistical information, etc., it is not deemed as a state that the phrase "when producing" anonymously processed information refers to.

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）

Guidelines 3-4 Disclosure upon the Production of Anonymously Processed Information (Related to Article 36, paragraph (3) of the Act) (Excerpt)

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。

In cases where a personal information handling business operator has produced anonymously processed information (*1), said personal information handling business operator must disclose the categories of information relating to an individual contained in the anonymously processed information (*2) without delay by utilizing the Internet, etc.(*3)

（※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。

(*1) Here, the phrase "in cases where ... produced anonymously processed information" means cases where the processing of personal information to handle it as anonymously processed information is completed. In other

words, this phrase does not include a case where information is stored, managed, etc. with a part of information deleted or divided as a part of security control actions for personal information or a case where personal information is processed in order to create statistical information from personal information.
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。
In addition, if the processing of personal information to produce anonymously processed information is still ongoing and has yet to be completed, it is not deemed as a state that the phrase "in cases where ... produced anonymously processed information" refers to, since such information has not been processed to an adequate level and thus it may be inappropriate to handle such information as anonymously processed information

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。
As stated in (*2) of "3-2 Proper Processing of Anonymously Processed Information (Related to Article 36, paragraph (1) of the Act)" and (*1) of "3-4 Disclosure upon the Production of Anonymously Processed Information (Related to Article 36, paragraph (3) of the Act)" of the Guidelines above, "when producing anonymously processed information" means when producing anonymously processed information with an intent to produce anonymously processed information for the purpose of handling information as anonymously processed information as provided in the Act. To "handle as anonymously processed information as provided in the Act" refers to cases where such information is used for a new purpose or provided to a third party without obtaining a principal's consent.
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。
In other words, processing of data conducted with no intent to produce anonymously processed information and based on the premise that said data is to be handled as personal information does not constitute the "production of anonymously processed information" under the law. Such data processing does not give a rise to an obligation concerning the handling of anonymously processed information. Major examples for such data processing are as follows.

(1) 社内での安全管理上、氏名等を削除して扱うデータ

(1) Data from which names, etc. are deleted from an internal security management perspective

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。

In handling personal information, business operators often delete unnecessary information identifying an individual such as name from the security management perspectivewhen analyzing the market or user tendency. A part of the information may be also deleted when entrusting such analysis work to another business operator.

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。

If such information handling is conducted with no intent to produce anonymously processed information and based on the premise that said information is to be continuously handled as personal information, it does not constitute the "production of anonymously processed information" under the law.

(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

(2) Data processed from personal information in order to create statistical information

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。

One of the ways to utilize acquired personal information is create statistical information by processing personal information in order to analyze user tendencies.

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。

When creating such statistical information, a business operator can produce a spreadsheet directly from the dataset of personal information, or tally data after deleting names, etc. from personal information and grouping items, such as address, age, etc. into categories (e.g. "Chiyoda-ku, Tokyo" to "Tokyo," "25 years old" to "20s").

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。

Such data generated in the course of processing properly personal information into statistical data does not constitute the "anonymously processed information" under the law, since it is conducted with no intent to produce anonymously processed information.

(3) 匿名加工情報を作成する途上で発生するデータ

(3) Data created in the course of producing anonymously processed information

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。

It is also possible that anonymously processed information is produced through trial and error or adjustment of processing information, such as when trying anonymization methods and changing parameters of noise volume and the level of vagueness based on the results of evaluation of data value and risks of re-identification.[19]

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。

As stated in the Guidelines, it is not appropriate in some cases that information of which the processing to produce anonymously processed information is ongoing and has not yet been completed be handled as anonymously processed information, since the level of processing that has been done may be insufficient. Therefore, such information is not deemed as being in a state referred to by the phrase "when having produced anonymously processed information" as stated in the Act.

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。

A business operator is deemed as "having produced anonymously processed information" upon the completion of processing information into anonymously processed information, and is able to handle said anonymously processed information based on the premise that it complies with the disclosure obligation concerning the production and provision to a third party of anonymously processed information, obligation to take security control actions, etc.

[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。
Risks that a principal concerning personal information that is used for the production of anonymously processed information may be identified

4. 匿名加工情報の作成に当たって求められる加工

4. Processing Required When Producing Anonymously Processed Information

4.1 匿名加工情報の加工基準（施行規則第 19 条）について

4.1 Regarding the Processing Standards for Anonymously Processed Information (Article 19 of the Enforcement Rules)

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）。

Article 36, paragraph (1) of the Act provides that a personal information handling business operator shall comply with standards prescribed by the Enforcement Rules when producing anonymously processed information. Said standards are set forth in Article 19 of the Enforcement Rules, which contains five items. These items are not to be selectively conducted; all of the measures provided under these items shall be taken (provided, however, this does not apply when information provided in these items is not contained).

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。

This Section (4.1) will discuss specific methods for carrying out measures as provided in the items of Article 19 of the Enforcement Rules.

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）

4.1.1 Item (i) (Deletion of Descriptions, etc. Which Can Identify a Specific Individual)

施行規則第19条第1号

Article 19 (i) of the Enforcement Rules

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。）。

(i) deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (including replacing the said whole or part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the whole or part of descriptions etc.)

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

Guidelines 3-2-1 Deletion of Descriptions, etc. which can identify a specific individual

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。

Personal information handled by a personal information handling business operator generally includes name, address, date of birth, gender and various other descriptions, etc. relating to an individual. Such descriptions, etc. include those that can identify a specific individual alone, such as name, and those that can identify an individual when combined with other descriptions, etc., such as address and date of birth. Personal information shall be processed so as not to be able to identify a specific individual by deleting a whole or part of those descriptions etc. that can identify a specific individual or by replacing such descriptions, etc. with other descriptions, etc.

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。

Replacement with other descriptions, etc. shall be done by a method with no regularity that can restore the original descriptions, etc. (*) Original descriptions, etc. can be replaced with more abstract descriptions, such as replacing date of birth with date of year, for example.

【想定される加工の事例】

[Possible Examples of Processing]

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。

Example 1) Measures 1 to 3 below are taken when processing personal information containing name, address, and date of birth.

1）氏名を削除する。

1) Name is deleted.

2）住所を削除する。又は、○○県△△市に置き換える。

2) Address is deleted or replaced with "△△ City, ○○ Prefecture"

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。

3) Date of birth is deleted or replaced with month and year of birth.

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。

Example 2) Measures 1 and 2 below are taken when processing personal information containing membership ID, name, address, and telephone number.

1）会員 ID、氏名、電話番号を削除する。

1) Membership ID, name, and telephone number are deleted.

2）住所を削除する。又は、○○県△△市に置き換える。

2) Address is deleted or replaced with "△△ City, ○○ Prefecture"

（※）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。

(*) When assigning temporary IDs, it shall be done with a method that has no regularity that can restore the original description.

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。

Take an example where temporary IDs are created from descriptions, etc. that are unique to individuals, such as name, address, contact, and credit card number with a fash function, etc. One of the ways to avoid a regularity that can restore the original descriptions, etc., which could occur when the same function is simply applied to the original descriptions, is to add other descriptions, such as random numbers, to the original descriptions (e.g. name and contact) before applying the hash function, etc. When adding the same set of random numbers or other descriptions, etc. before applying a hash function, etc. it is encouraged to change and regularly update the combination of descriptions, etc. for each business operator to which processed information will be provided, so as to prevent a regularity in the random numbers or other descriptions, etc. that can restore the original descriptions.

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。

Article 19, item (i) of the Enforcement Rules provides a measure to delete a whole or part of descriptions etc.[20] which can identify a specific individual in relation to personal information falling under Article 2, paragraph (1), besed on Article 2, paragraph (9), item (i) of the Act.

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。

[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。

The description in Article 2, paragraph (9), item (i) of the Act stating "deleting a part of descriptions, etc. ...) is changed to "delete a whole or part of descriptions, etc." here. This change was made to simply clarify that there can also be a case wherein the only information that can identify a specific individual is 'name' and thus a whole of descriptions, etc. is to be deleted.

The Guidelines on the Act on the Protection of Personal Information (General Rules) (hereinafter referred to as the "Guidelines on General Rules" list the following as examples for "those (descriptions) able to identify a specific individual" based on Article 2, paragraph (1), item (i) of the Act.

通則ガイドライン 2-1

Guidelines on General Rules 2-1

事例 1）本人の氏名

Example 1) Name of a principal

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

Example 2) Combination of name and such information as date of birth, contact (address, location, telephone number, and email address), post at company or affiliation

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

Example 3) Video information with which a principal can be identified, such as information recorded by a security camera

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

Example 4) Recorded audio information that can identify a specific individual, due to such reasons as containing a principal's name

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）

Example 5) Email address that can identify a specific individual (for example, email address "kojin_ichiro@example.com" alone can identify an individual named Kojin Ichiro that belongs to Example Company)

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。）

Example 6) Information relating to an individual that has been added after the acquisition of personal information (even if a specific living individual could not be identified upon the acquisition of information, said information is deemed as personal information if it becomes capable of identifying a specific living individual as a result of the addition of or collation with new information)

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

Example 7) Information that can identify a specific individual that has been publicized on an official gazette,

telephone book, list of government officials, statutory disclosure document (such as an annual securities report), newspaper, website, SNS (social network service), etc.

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。

"Descriptions, etc. which can identify a specific individual" for which Article 19, item (i) of the Enforcement Rules requires measures to be taken refer to personal information that can identify a specific individual alone or in combination with other information, as [Possible Examples of Processing] stated in the Guidelines.

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。

Said item has the requirement to "delete a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the whole or part of descriptions etc.)." Any descriptions, etc. that alone can identify a specific individual (such as name and facial image) shall be deleted, and a whole or part of descriptions, etc. that can identify a specific individual when combined with other descriptions, etc. shall be deleted.

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]。

Specifically, such descriptions, etc. can be partially deleted or replaced so that a certain level of obscurity is secured for each category of information, such as replacing address with "○○ City" (if it is a highly populated urban area, replacing with "○○ Ward") and replacing date of birth with month or year of birth, as shown in the examples in the Guidelines. Another approach than can be taken is to adjust the processing level from category to category so as to prevent the combination of multiple categories, such as address, date of birth, and gender, from having a unique meaning.[21]

[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。

"Report on the Proper Processing of Anonymously Processed Information" (Technical Study Working Group on Anonymously Processed Information) dated February 21, 2017 (http://www.nii.ac.jp/about/reports/pd/report-kihon-20170221.pdf) categorizes these methods into "single item- processing" and "multiple item processing."

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。

Mobile phone number, email address, ID on SNS, etc.,[22] credit card number, etc. do not fall under the scope of codes that can identify a specific individual, as they are not distinguishable from numbers held by corporations. However, such information is generally closely related to an individual. If such information alone or in combination with other information can be recognized as relating to a specific individual, it should be handled as personal information.

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]。

In particular, in light of the fact that many business operators acquire such information from their users, such information can function as an identifier for personal information held by other business operators. If such information is merely partially deleted, there would be a high risk that a specific individual may be identified from the remaining information. Therefore, such information should be wholly deleted in principle.[23]

【仮IDへの置き換えについて】

[Regarding Replacement with Temporary ID]

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。

In addition to deleting information that can directly identify a specific individual, anonymously processed information can be also produced by replacing the attributes that can directly identify a specific individual or combination thereof (e.g. name + contact) with other descriptions, etc., using a method with no regularity that can restore the original personal information. If the original personal information is replaced with a code, number, etc.,

[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。

In recent years, identification utilizing SNS ID can occur as there is a trend of using such ID as an account for other online services due to the rise of such systems as Open ID.

[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。

There is no problem with leaving the first three digits of a mobile phone number or issuer identification code contained in a credit card number as these codes have no ability to identify an individual. However, it is needless to say that such codes should be deleted too if there is no plan to use them for the purpose of analysis.

such code, number, etc. can be deemed as a temporary ID.
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。
A temporary ID can be assigned by allotting a number or code produced by a certain algorithm for each input of unique information (name, service ID, etc.) or an individual identification code or combination thereof, which can directly identify a specific individual. Another method for assigning temporary IDs is to allot random numbers or codes, etc. after deleting unique information, such as name and service ID, etc. Meanwhile, the requirement for anonymously processed information provides that information shall be "replaced by a method with no regularity that can restore" the original personal information. Therefore, temporary IDs also shall be created in a way that is not able to restore the original personal information. It is necessary to be aware of the advantages and disadvantages of replacement with temporary IDs.

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。
By assigning a temporary ID, it becomes possible to associate data concerning an identical person contained in different datasets. Extra care must be paid in such cases as follows.
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。
If multiple business operators receive data that uses a common temporary ID for a specific individual, said business operators may link their data with each other in relation to said specific individual. In order to prevent such situation, it is desired to use different temporary IDs for each business operator to which information is provided. This can be achieved by using a different temporary ID creation method for each receiver business operator. Otherwise, even when using the same ID creation method, different temporary IDs should be created by making use of some parameters. One of such methods is to add codes or random numbers, which are different for each receiver business operator, to the input information before applying a hash function.
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。
In addition, risks of identification of a principal concerning the original personal information can be also raised when multiple sets of anonymously processed information are provided to an identical business operator and information concerning an identical person is accumulated. Therefore, it is also desired to regularly change temporary IDs when providing information to the same business operator multiple times.
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。
Note that replacement with temporary IDs should be avoided if it is unnecessary, in order to reduce the risk of re-identification.

【ハッシュ関数による置き換えについて】

[Regarding Replacement using a hash function]

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。
Replacement with temporary IDs should be done in a way that is not able to restore or estimate the original descriptions. One of the major methods for such processing is hashing, which uses a hash function. Hashing is a method to replace the original data with random values of fixed size (called hash values), which are obtained from the original data by following a certain calculation process. By using a special calculation process called a hash function, seemingly randomized hash values of fixed size can be obtained from data of arbitrary size.
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。
While the same data always creates the same hash values, even a slight difference in the data makes the result hash values completely different. Since it is extremely difficult to estimate the original data from hash values or to create different datasets having the same hash values, it is often used as a method for creating temporary IDs for the purpose of anonymization.
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]。

However, the fact that the same data always creates the same hash values means that, if temporary IDs are created using the hashing method solely based on information that is held by many business operators, such as name, email address, and mobile phone number, it may be easy for a business operator that receives the processed data to estimate the original input information that was used for the creation of temporary IDs. Therefore, when creating temporary IDs with the hashing method, secret key codes should be added before applying a hash function (such as name + secret code or name + email address + secret code) (what is called a keyed hash function).[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。

It is encouraged to use an algorithm whose safety has been proved for a hash function. For example, hash functions included in the e-Government Recommended Ciphers List[25] which is publicized by CRYPTREC, are recommended from the security perspective.

4.1.2 第 2 号（個人識別符号の削除）

4.1.2 Item (ii) (Deletion of Individual Identification Codes)

施行規則第19条第2号

Article 19　(ii) of the Enforcement Rules

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。）。

(ii)　deleting all individual identification codes contained in personal information (including replacing such codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes)

ガイドライン 3-2-2 個人識別符号の削除

Guidelines 3-2-2 Deletion of Individual Identification Codes

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。

---

[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。
"Opinion 05/2014 on Anonymisation Techniques" by the Article 29 Data Protection Working Party also includes a statement to the effect that keyed hash functions using a sufficiently large and unpredictable key, in light of the fact that input values can be replayed and the issue of brute force attacks.

[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）。
CRYPTREC Ciphers List (e-Government Recommended Ciphers List) (http://www.cryptrec.go.jp/list.html)

If personal information to be processed includes any personal identification code, said personal identification code alone can identify a specific individual. Therefore, all personal identification codes must be deleted or replaced with other descriptions, etc. so as to prevent the identification of a specific individual.

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ある。

When replacing them with other descriptions, etc., it needs to be done with a method with no regularity that can restore the original descriptions, etc.

（参考）個人識別符号の概要

(Reference) Overview of Individual Identification Codes

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）

An individual identification code means information that can identify a specific individual alone as provided under the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; hereinafter referred to as the "Cabinet Order"), which falls under any of the following items (see Guidelines on General Rules 2-2 (Individual Identification Code) for details on the definition of an individual identification code).

（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

(1) Codes produced by having converted any of the bodily features of a specific individual so as to be provided for use in computers

・ 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】

・Biometric information (DNA, face, iris, voice print, physical appearance when walking, veins on hands or fingers, finger or palm print) converted into digital data, which conform to standards prescribed by the Rules as sufficient to identify a specific individual [Article 1, item (i) of the Cabinet Order, Article 2 of the Rules]

（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

(2) Different codes assigned in regard to the use of services or purchase of goods, or to a document, for each relevant person

・ 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】

・Numbers assigned by a public organization, such as passport number, basic pension number, driver's license

number, resident record code, individual number, and insurance number [Articles 2 to 7 of the Cabinet Order, Articles 3 and 4 of the Rules]

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。
Article 19, item (ii) of the Enforcement Rules provides for measures set forth in Article 2, paragraph (2), item (ii) of the Act.
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。
Individual identification codes provided in Article 2, paragraph (2), item (i) of the Act, which are able to identify a specific individual that are codes into which a partial bodily feature of the specific individual has been converted in order to be provided for use by computers, and individual identification codes provided in Article 2, paragraph (2), item (ii) of the Act, which include passport number, driver's license number, individual number, etc., are to be assigned to a specific individual and thus such codes alone constitutes information that can identify a specific individual. Therefore, all of such individual identification codes shall be deleted. As for replacement with temporary IDs, the approach explained in 4.1.1 applies.

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。
The Guidelines on General Rules explain that individual identification codes that meet the "standards prescribed by the rules" as referred to in Article 2, paragraph (2), item (i) of the Act are "codes that are made capable of recognizing a principal" (DNA) or "codes that are made capable of recognizing an individual when used by a device or software aimed at recognizing an individual."

4.1.3 第 3 号（情報を相互に連結する符号の削除）

4.1.3 Item (iii) (Deletion of Codes Linking Mutually Plural Information)

施行規則第19条第3号
Article 19 （iii）of the Enforcement Rules
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。)。

(iii)　deleting those codes (limited to those codes linking mutually plural information being actually handled by a personal information handling business operator) which link personal information and information obtained by having taken measures against the personal information (including replacing the said codes with those other codes which cannot link the said personal information and information obtained by having taken measures against the said personal information using a method with no regularity that can restore the said codes)

ガイドライン 3-2-3 情報を相互に連結する符号の削除

Guidelines 3-2-3 Deletion of Codes Linking Mutually Plural Information

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。

For example, a personal information handling business operator may divide or reproduce a whole or part of personal information that it acquired, so that it can carry out distributed management of said personal information to ensure security. In such case, a personal information handling business operator may assign an ID, etc. as a code to mutually link said personal information and information obtained therefrom after applying a measure. Since such an ID is used for linking personal information and information obtained therefrom after applying a measure, and can lead to the restoration of the identification of a specific individual or restoration of the original information, it must be deleted from the personal information subject to the processing or replaced with another code.

【想定される加工の事例】

[Possible Examples of Processing]

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。

Example 1) If information on subscribers to a service is divided into basic information, such as name, and purchase history for the purpose of distributed management and if such distributed information is linked with one another with management IDs, such management IDs are deleted.

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。

Example 2) When a part of personal information is provided to a contractor and the original personal

information and information created for the purpose of provision to said contractor are mutually linked by allotting management IDs, such management IDs are replaced with temporary IDs (*2).

（※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。
(*1) "Information being actually handled by a personal information handling business operator" means information that is being handled at the time of producing anonymously processed information, and does not include anonymously processed information that is to be produced.
（※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。
(*2) See (*) in Section 3-2-1 (Deletion of Descriptions, etc. Which Can Identify a Specific Individual) for things to be noted when assigning temporary IDs.

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。
Article 19, item (iii) of the Enforcement Rules requires the deletion of IDs, etc. that are assigned to mutually link divided databases for the purpose of distributed management or outsourcing of the handling, etc. of personal information.
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。
Business operators may divide personal information into multiple databases for the purpose of management, as shown in Figure 4-1, as part of security control measures to be taken when handling personal information or as part of management of personal information for joint use.

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

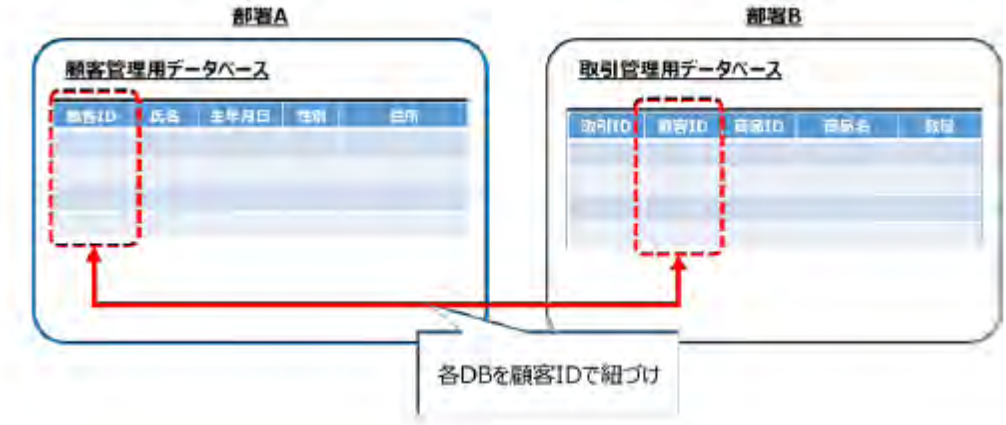
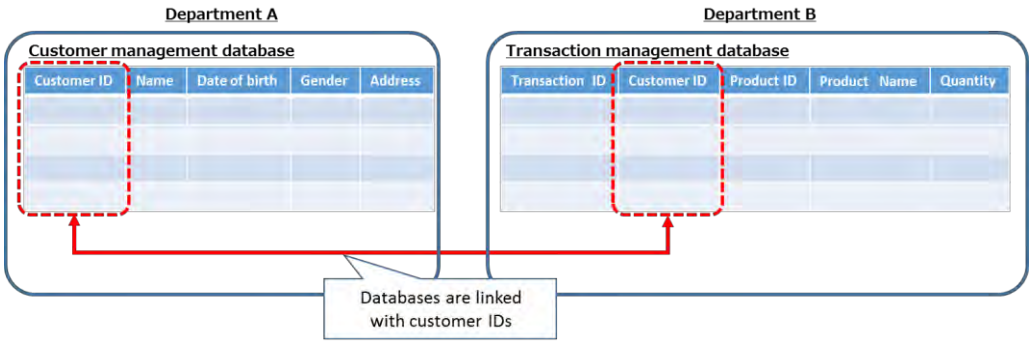


Figure 4-1 Concept of "codes" which are required to be deleted under Article 19, item (iii) of the Enforcement Rules



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。

Here, "codes linking" means codes that mutually link personal information and information obtained therefrom after applying a measure. Even if they do not take the form of an ID, other information concerning attributes (such as telephone number and email address) that is used for the purpose of linking is deemed as "codes linking" .

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。

However, this item only applies to codes that are actually being used for the purpose linking. Other information is not subject to the deletion measure as provided in item (iii) of said Article.

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。

Since codes subject to the deletion measure as provided in item (iii) of said Article are limited to those mutually linking information that is actually being handled by a personal information handling business provider, said item does not apply to codes that are newly created through processing into anonymously processed information.

4.1.4 第 4 号（特異な記述等の削除）

4.1.4 Item (iv) (Deletion of idiosyncratic descriptions etc.)

施行規則第19条第4号

Article 19**(iv) of the Enforcement Rules**

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。）。

(iv) deleting idiosyncratic descriptions etc. (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the idiosyncratic descriptions etc.)

ガイドライン 3-2-４ 特異な記述等の削除

Guidelines 3-2-4 Deletion of Idiosyncratic Descriptions, etc.

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。

Descriptions, etc. concerning a fact that is generally considered to be rare or descriptions that are extraordinarily distinct from other individuals could lead to the identification of a specific individual or restoration of the original personal information. Therefore, idiosyncratic descriptions, etc. must be deleted or replaced with other descriptions, etc. when producing anonymously processed information.

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。

Here, "idiosyncratic descriptions, etc." mean descriptions that are so unique that they may constitute descriptions, etc. that can identify a specific individual. Descriptions, etc. that are different from other individuals but entail no risk of leading to the identification of a specific individual do not fall under the scope of this term. Whether a description, etc. is idiosyncratic or not needs to be determined objectively case by case, taking into account the attribute of information, etc.

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。

When replacing idiosyncratic descriptions, etc. with other descriptions, etc., it has to be done by a method with no regularity that can restore the original descriptions, etc. For example, idiosyncratic descriptions, etc. can be replaced with more common descriptions, etc.

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。

Note that Article 19, item (iv) of the Rules applies to descriptions, etc. that are considered to be idiosyncratic in any general settings in general social terms. On the other hand, if identifiability is attributed to the attribute of a personal information database, etc., such as in the case where there is a significant difference between descriptions, etc. contained in personal information to be processed and descriptions, etc. contained in other personal information comprising the personal information database, etc. containing said original personal information to be processed, necessary measures as provided in item (v) of said Article need to be taken.

【想定される加工の事例】

[Possible Examples of Processing]

事例1）症例数の極めて少ない病歴を削除する。

Example 1) Deleting a medical history for which the number of cases is extremely small

事例2）年齢が「116歳」という情報を「90歳以上」に置き換える。

Example 2) Replacing the age of "116 years old" with "90 years old and above"

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。

"Idiosyncratic descriptions, etc." that are required to be deleted under Article 19, item (iv) of the Enforcement Rules refer to descriptions, etc. that are considered to be idiosyncratic in any general settings "in general social terms." Specifically, this includes "extremely old age" and "medical history for which the number of cases if extremely small" as shown in the examples in the Guidelines, as well as other descriptions, etc. concerning basic attributes of an individual, such as extremely tall height or extremely high salary.

「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。

What kind of information constitutes idiosyncratic descriptions and from what level a value is considered to be idiosyncratic need to be determined with consideration to the attribute of the information category, size of the group, characteristics in the distribution of the group, etc. Since said item only applies to descriptions, etc. that are considered to be idiosyncratic in general social terms, descriptions, etc., which are peculiar, but for which no distribution survey results exist or for which distribution survey results exist but are not available to ordinary people, do not fall under the scope of "idiosyncrasy" as referred to in said item. Outstanding values contained in a database to be processed may be subject to measures provided in item (v) of said Article.

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）

4.1.5 Item (v) (Other Measures Based on the Attribute, etc. of Personal Information Database, etc.)

施行規則第19条第5号

Article 19**(v)** **of the Enforcement Rules**

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。

(v) besides action set forth in each preceding item, taking appropriate action based on the results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information

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

Guidelines 3-2-5 Other Measures Based on the Attribute, etc. of Personal Information Database, etc.

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。

When producing anonymously processed information, it has to be ensured that it cannot identify a specific individual or restore the original personal information, by taking measures as provided in Article 19, items (i) to (iv) of the Rules.

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。

However, information that has undergone processing as provided in Article 19, items (i) to (iv) of the Rules may still be in a state that allows for the identification of a specific individual or restoration of the original personal information in general terms, due to the attribute of personal information database, etc. from which processed information derives, such as in the case where there is a significant difference between the descriptions, etc. contained in personal information to be processed and the descriptions, etc. contained in other personal information comprising the personal information database, etc. containing said original personal information to be processed. In order to address such a case, business operators shall examine if measures other than those stated above are needed and take proper measures as necessary by such means as those provided in Appended Table 1 (Examples of Methods Concerning Processing of Anonymously Processed Information).

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。

Since the scope and intensity of processing may vary depending on the attribute of personal information database, etc. that is to be processed, business operators need to determine the scope of information that needs to be processed and the intensity of processing in detail, case by case, taking into account the attribute of personal information database, etc.

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。

In particular, regarding personal information databases, etc. containing information on purchase history and locations, etc., which includes information on repeated actions, it may become possible to determine the behavioral habitat of an individual, if such information has been accumulated. Proper processing must be conducted on the part of information that alone cannot identify a specific individual but may become able to identify a specific individual or restore the original personal information when accumulated, etc.

【想定される加工の事例】

[Possible Examples of Processing]

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）

Example 1) When processing a personal information database, etc. containing transportation history data, which includes location information (latitude and longitude information) that can lead to the estimation of the location of the home or workplace and thus entails a risk that a specific individual may be identified or the original personal information may be restored, deleting location information of a certain scope that can lead to said estimation (deleting information by category/deleting records/deleting cells)

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）

Example 2) When processing a personal information database, etc. containing purchase history data of a retail store, which includes purchase history data concerning a product whose consumers are extremely limited at said retail store and thus entails a risk that a specific individual may be identified or the original personal information may be restored, replacing specific product information (product number, color) with a more common product category (generalization)

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）

Example 3) When processing a personal information database, etc. containing information on physical examination at an elementary school, which includes information on a particularly tall student whose height is 170 cm and thus entails a risk that a specific individual may be identified or the original personal information may be restored, replacing information concerning students whose height is 150 cm or more with the information stating "150 cm or more" (top-coding)

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。

Article 19, item (v) of the Enforcement rules provides for measures that need to be taken additionally, when information is still "in a state that allows for the identification of a specific individual or restoration of the original personal information" after applying processing measures as provided in items (i) to (iv) of said Article. Item (v) has the requirement to "consider the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information

constituting the personal information database etc. that encompass the said personal information" and to take additional measures when further processing is found to be necessary as a result of such consideration.

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。

As explained in the "Guidelines on the Act on the Protection of Personal Information" and Q&A on "Response to an Incident of Personal Data Leakage, etc." (February 16, 2017), said item does not apply to entire personal information databases that exist at a business operator; instead, it requires consideration of additional measures for a personal information database, etc. comprised of personal information from which anonymously processed information comprising anonymously processed information database, etc. derives from.

Q11-9

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。

Article 19, item (v) of the Enforcement Rules states "considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information." Is it necessary to take into account entire personal information databases, etc. held by a business operator when considering a "personal information database etc. that encompass the said personal information" as referred to in this item?

A11-9

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。

Here, "personal information database etc. that encompass the said personal information" refers to a personal

information database, etc. that is to be processed by the personal information handling business operator when producing anonymously processed information. In other words, this item does not require the personal information handling business operator that produces anonymously processed information to consider the attribute of all personal information databases, etc. that contain personal information that has nothing to do with said processing.

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」

4.1.5.1 "A Difference between Descriptions etc. Contained in Personal Information and Descriptions etc. Contained in Other Personal Information"

「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。

"A difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information" means a difference between descriptions contained in personal information in a database comprised of personal information that is to be processed and descriptions contained in other personal information in said database. To "consider" such difference means to examine whether such relative uniqueness of a value or description, etc. in a personal information database, etc. comprised of personal information that is to be processed may lead to the identification of a specific individual.

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。

For example, a database regarding residents in urban areas and a database regarding residents in rural areas may be different from one another in terms of the structure of age distribution, job distributions, etc. of people contained therein. As such, a situation wherein a specific individual may be readily identified may occur for a database in which the distribution of a group is different from a database that covers the entire nation, due to the idiosyncrasy of values or descriptions contained in such database.

4.1.5.2 「その他の～適切な措置」が求められる場合

4.1.5.2 When Other "Appropriate Actions" Are Required

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]。

For example, if a database contains detailed location information (transportation history) or long-term purchase history data, it may be possible to estimate repeated behavioral habits or interests/tastes from accumulated information. Although it is generally difficult to identify a specific individual based on behavioral habits, etc. that can be estimated from such history information, behavioral habits, etc. that are particularly noticeable may lead to the identification of a specific individual.[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。

Article 19, item (v) of the Enforcement Rules requires that the identifiability of a specific individual that derives from the attribute of information contained in a personal information as stated above be reduced.

【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】

[Highly constant IDs, service IDs acquired by many business operators, etc.]

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。

Highly constant IDs that are to be considered in relation to item (v) of said Article are externally observable codes closely relating to an individual that cannot be readily changed by said individual, other than [a] individual identification codes and [b] other information, which can alone constitute personal information.[27] Specifically, an ID for a device that is carried around in everyday life and used by an individual for a certain period, such as a smartphone, would fall under this category.

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。

A highly constant ID should be deleted in principle, since it can be used as a key for identification and thus is considered as information that can lead to re-identification.

---

[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。

History information, such as purchase history and transportation history information, may present a habitual/repetitive tendency of an individual and function as an identifier for different datasets. It is desired to carry out necessary processing with an awareness of such risks. "Report on the Proper Processing of Anonymously Processed Information (February21, 2017)" by the Technical Study Working Group on Anonymously Processed Information also states that "when providing identical history data concerning an identical person to an identical receiver, the provider should note that there is a risk that said history data can function as a temporary ID."

[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。

Individual identification codes and other information, which can alone constitute personal information, have been already deleted or replaced with other descriptions, etc. in accordance with Article 19, item (ii) of the Enforcement Rules, and item (i) of said Article, respectively.

【時刻に関する情報について】

[Regarding Time information]

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。

History information, such as purchase history, credit card transaction data, and transportation history, are typically recorded on a database along with detailed time information.

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。

For example, a database concerning purchase history that includes store information allows for the identification of a store at which an individual made a purchase at a certain time and date. Meanwhile, a database concerning transportation history also allows for the determination of location information concerning a spot at which an individual visited at a certain time and date. When said two databases are collated with each other, it becomes possible to estimate approximate latitude and longitude (location information) based on the location of said store. If said two databases have recorded the hour, minute and second, it may be relatively easy to identify an identical individual who is contained in both databases. In other words, detailed time information can function as a common identifier for different datasets, when it is used along with information indicating a location or place.

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。

Therefore, when providing a database containing detailed time information to a third party as anonymously processed information, a provider business operator should examine if time information is needed and reduce the risks that a specific individual is identified through the linkage of time and location (place) information and linkage with time information contained in another dataset, by such means as obscuring time information to a certain extent and replacing time information with other arbitrary date and time by adding noise.

【位置情報（移動履歴）について】

[Location information (transportation history)]

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。

Typically, location information itself does not fall under the category of personal information. However, if location information concerning a specific individual is continuously accumulated, it may present the transportation history of said individual. In particular, information on locations where said individual stayed at midnight and during the day may allow for the estimation of the basic personal attributes of the principal of said transportation history, such as locations of home, workplace, etc. If there is a risk that accumulated location information and transportation history, etc. can lead to the estimation of information that is closely related to a specific individual, such as the address of his/her home, workplace, etc., transportation history should be processed with due consideration to the risk that a specific individual may be identified using said information.

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]。

In addition, transportation history has a characteristic that the longer the distance becomes, the lower the chances that it coincides with others becomes and the more unique said transportation history becomes.[28] Another characteristic is that the volume of location information that can be obtained from the same scope varies according to the environment and situation, such as whether information is taken from an urban area or rural area, or during the day or night. Necessary actions should be taken after fully examining the attribute of location information and transportation history.[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

4.2 Matters That Should Be Considered When Producing Anonymously Processed Information

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

[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。

“Zipf Distribution Model for Quantifying Risk of Re-identification from Trajectory Data” (Hiroaki Kikuchi & Katsumi Takahashi, Journal of Information Processing, Vol.24(2016) No.5, pp.816-823) reports the uniqueness of information arising from the length of railway travel (volume of information concerning visited stations).

[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。

"Location Information Privacy Report" published by the Ministry of Internal Affairs and Communications in July 2014 refers to approaches to the handling of location information and anonymization methods for such information.

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。

Anonymously processed information must be processed in a way that "a specific individual cannot be identified" and "personal information cannot be restored" based on the ability of and methods available to an ordinary person or business operator. The intensity of processing may vary within a certain range according to the purpose of anonymously processed information and methods for estimating re-identification risks.[30]

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。

When deciding processing policies concerning the production of anonymously processed information, the following matters should be examined.

4.2.1 匿名加工情報の利用形態について

4.2.1 Use of Anonymously Processed Information

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。

When considering processing policies for anonymously processed information, it is useful to examine its purposes and uses, such as those listed below, in order to secure the safety and usability of such information at the same time.

（１） 匿名加工情報の利用目的は何か

(1) What is the purpose of use of anonymously processed information?

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。

Necessary categories of information and granularity (accuracy) of said information may vary depending on the purpose of use of anonymously processed information. A provider business operator should seek a processing method that can ensure total safety and usability at the same time, such as deleting unnecessary categories and raising the information granularity of necessary information,

（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

(2) Whether the scope of data distribution is to be restricted or secondary distribution by the receiver is allowed

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

[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）。
There is also a risk-based methodology, which seeks an anonymization method through threat modeling and risk quantification. (Khaled El Emam & Luk Arbuckle (translated into Japanese by Takashi Sasai), "Anonymizing Health Data" (O'Reilly Japan, 2015) et al.)

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。

For example, if data is provided exclusively to a certain business operator based on a contract containing a clause on the prohibition of secondary distribution by the receiver, it would be relatively easy to understand the purpose for which the receiver uses anonymously processed information. Meanwhile, if secondary data distribution by the receiver is allowed, it would be difficult to identify the purpose of use and risks of collation with other information by the secondary receiver. It is readily understood that re-identification risks are different between a case wherein anonymously processed information remains at a certain company, and a case wherein said information is distributed without any limitations.

（３） 提供するデータの期間

(3) Period of data to be provided

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。

Behavioral habits of a principal that can be estimated from history information contained in one-month data and those that can be estimated from one-year data can be significantly different. Business operators are advised to examine if the accumulation volume influences the identifiability of a specific individual and restorability of the original personal information.

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。

Even if the period of history data contained in a dataset to be provided is short, the receiver may come to have long-term data in the future as a result of constant provision of such data to a certain business operator. To change temporary IDs regularly is one of the ways to reduce re-identification risks in such cases.

（４） 継続的に匿名加工情報を提供する場合

(4) When anonymously processed information is to be constantly provided

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。

When providing multiple sets of anonymously processed information, a business operator may provide such information without assigning any temporary ID or with a new temporary ID for each provision, in order to prevent linkage of data concerning an identical person among the datasets. In such case, linking of datasets would become easier if records contained in an anonymously processed information database are always listed in the same order or if the period of databases overlaps with one another. Therefore, it is necessary to change the order of records of process data so that the periods of data contained in the dataset do not overlap, if a business operator wants to reduce the risk of linkage of records among anonymously processed information databases that are provided over multiple times .

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。

In addition, business operators need to take care not to use the same temporary IDs when providing anonymously processed information comprised of categories of information other than those provided before to the same receiver business operator, so that the original personal information cannot be restored by collating newly provided information with the information provided in the past. Note that the disclosure obligation applies when producing or providing a third party new anonymously processed information comprised of information that falls under the categories other than those comprising an anonymously processed information that was provided in the past.

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

4.2.2 Identifiability through Reference to Other Information

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。

Anonymously processed information must be processed in a way that "a specific individual cannot be identified." However, as the purpose of the anonymously processed information system is to promote personal data utilization while ensuring the safety of its distribution process, business operators should examine if there is a risk of identifiability through reference to other various information that is generally available.

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。

This issue is to be examined based on the ability of and methods, etc. available to ordinary people and ordinary

business operators, as explained in Section 3.2. For example, such examination can be carried out from the perspectives of the "type of accessible information" and "ease of information matching."

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。

Possible types of accessible information are as follows.

① 一般に広く公開、市販されている情報（例：電話帳）

[i] Information that is publicly disclosed or sold (e.g. telephone book)

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）

[ii] Information that has been acquired by many business operators through user registration, etc. (e.g. email address, telephone number, etc.)

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）

[iii] Information that is only accessible for closely related people (e.g. information posted on SNS that is only disclosed to limited people, etc.)

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。

On the other hand, ease of information matching can be categorized from such viewpoints as follows.

(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

[i] When categories of information and corresponding descriptions, etc. are organized and can be readily matched mechanically

(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

[ii] When categories of information and corresponding descriptions, etc. are atypical and a complicated algorithm or machine learning is required to match information

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。

Among the categories of accessible information stated above, [i] and [ii] are considered to be readily accessed, while [iii] is found to be not so easy to access for ordinary people and ordinary business operators, as information falling under [iii] is only accessible for selected related people.

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。

Regarding the ease of information matching, only [i] would be an issue in terms of the criteria concerning the requirements of anonymously processed information. Since ease of information matching needs to be examined taking into account the technology standards as of the time of production of anonymously processed information. If

a machine learning tool, etc. becomes generally available in the future, it will be also included in the category of [i].

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。

Identifiability through reference to other information can be determined comprehensively based on the combination of the factors stated above. If it is determined that there is a high risk of identification, it should be addressed with such actions as changing the intensity of processing for information falling under relevant categories and eliminating uniqueness of information contained in relevant datasets, so as to fulfill the requirements of anonymously processed information.

【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】

[Case in which reference to other information resulted in re-identification]

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。

The following case does not directly apply to anonymously processed information, for which the act of identification is fundamentally prohibited, as in this case two publicly disclosed databases were collated with one another. However, the following is a typical case of re-identification through reference to other information and it can be used as a reference when determining the processing level.

<u>（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</u>

<u>(e.g.) Case of re-identification based on the combination of gender, date of birth and postal code (residence area)</u>

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。

Massachusetts had disclosed a medical dataset with name, etc. deleted. This dataset contained gender, date of birth, and postal code.

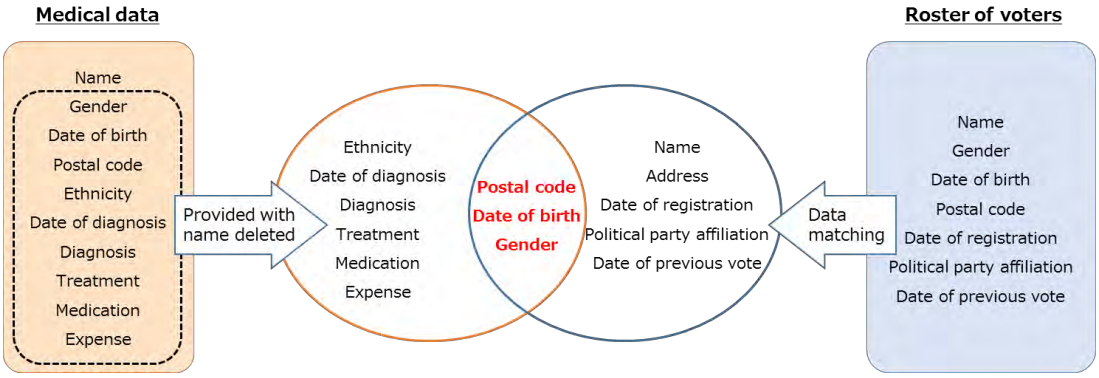
これに対し、既に公開されている投票者名簿とマッチングしたところ、州知事と同じ生年月日のレコードが6人おり、うち3人が男性で、郵便番号から1人に特定された。[31]

When the dataset is matched with a roster of voters that had already been disclosed, there were six records with the same date of birth as the governor's. Among these records, three records were concerning men, from which one record was identified based on the postal code.[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

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

Figure 4-2 Case in which a specific individual was identified based on gender, date of birth, and postal code



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。

Looking at the situation of Japan, there are approximately 120,000 postal codes in the country and approximately 3,650 patterns of date of birth for people in their 20s. If information on gender (male/female) is added to these, it can be easily imagined that the probability of having the same postal code, the same date of birth, and the same gender is extremely low.

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。

Note that information is not deemed as not fulfilling the requirements of anonymously processed information just because the information is unique.

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。

“k-Anonymity: A Model For Protecting Privacy” (L.Sweeney, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), pp. 557-570, 2002) proposes "k-anonymity" as an index for anonymity evaluation to prevent the identification of a specific individual through collation with other information.

4.3 匿名加工情報の作成のための参考情報

4.3 Reference Information for the Production of Anonymously Processed Information

4.3.1 匿名加工に用いられる代表的な加工手法

4.3.1 Major Processing Methods That Can Be Used for Anonymization

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。

Figure 4-3 shows major processing methods that can be used for the anonymization of personal information. Methods shown in this figure are examples of common processing methods and are not intended to preclude proper processing using other methods.

図表4-3 代表的な加工手法

Figure 4-3 Major processing methods

手法名 Method	解説 Explanation
項目削除 Deletion by category	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。 To delete a category of personal information contained in a personal information database, etc. that is to be processed. For example, to delete data on age from the entire personal information
レコード削除 Deletion of records	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。 To delete records of personal information contained in a personal information database, etc. that is to be processed. For example, to delete all records of individuals of a certain age
セル削除 Deletion of cells	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。 To delete certain cells containing personal information contained in personal information database, etc. that is to be processed. For example, to delete values of age contained in a specific personal data
一般化 Generalization	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。 To replace descriptions, etc. contained in information that is to be processed, with a more generic concept or value. For example, replacing the product name "cucumber" contained in purchase history data with the term "vegetable"
トップ（ボトム）コーディング Top- (bottom-) coding	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。 To censor particularly large or small values contained in a personal

	information database that is to be processed, with a more generic concept or value. For example, to compile age value data of 80 years old and above into data under the category of "80 years old and above"
レコード一部抽出 Partial extraction of records	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(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。 To (stochastically) extract a part of personal information contained in a personal information database, etc. that is to be processed. This also includes sampling.
項目一部抽出 Partial extraction of categories	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。 To extract a part of categories of personal information contained in a personal information database, etc. that is to be processed. For example, to extract a part of categories of information that constitute purchase history.
ミクロアグリゲーション Microaggregation	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。 Personal information comprising a personal information database, etc. that is to be processed is grouped and replaced with descriptions, etc. that represent said groups.
丸め(ラウンディング) Rounding	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。 To replace values contained in a personal information database, etc. that is to be processed with rounded values
データ交換 （スワッピング） Data swapping	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。 To (stochastically) swap descriptions, etc. contained in personal information comprising a personal information database, etc. that is to be processed. For example, to swap records that have different regional attributes
ノイズ（誤差）付加 Noise (error) addition	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。 To replace information with other arbitrary values, etc. by adding random

	values, etc. that are distributed in a certain way
疑似データ生成 Creation of pseudo-data	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。 To create artificially synthesized data and include such data in a personal information database, etc. that is to be processed

4.3.1.1 ｋ－匿名性について

4.3.1.1 *k*-Anonymity

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。

One of major ways to evaluate data's anonymity is to use an evaluation index called *k*-anonymity.[32] *k*-anonymity is deemed as being achieved if the number of data having the same attribute in the subject dataset is *k* or more. By processing data so as to achieve k-anonymity, the probability of identification of an individual is reduced to one-*k*th.

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。

Concerning the aforementioned Massachusetts case, L. Sweeney deems the three categories of information, namely gender, date of birth, and postal code, as "quasi-identifiers," which can identify an individual when linked with an external dataset. He argues said quasi-identifiers need to be processed when disclosing such information.

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≧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。

Since anonymously processed information is not always disclosed to the public in the manner of the above case, it is not necessarily required to process information so as to maintain k at 2 or more for information categories that are deemed as quasi-identifiers above, in relation to an anonymously processed information database, etc. However, it is encouraged to take into account such approach, according to the terms of provision to a third party and use of anonymously processed information.

---

[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.

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

4.3.1.2 レコード一部抽出について

4.3.1.2 Partial Extraction of Records

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。

The partial extraction of records means to extract a certain portion (or a certain number) of personal information (records) contained in a personal information database, etc. that is to be processed. This method also includes what is called "sampling."[33]

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。

Since this method does not process individual components of personal information, it does not reduce the identifiability of information itself. However, it has an effect to reduce the probability that personal information contained in the original personal information database, etc. is also contained in an anonymously processed information database, etc.

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。

Note that this method can also have an effect of maintaining the usability of data by partially extracting records in a way that maintains the tendencies of values and descriptions, etc. (for example, age distribution and regional distribution) contained in individual components of personal information comprising the personal information database, etc.

4.3.2 情報の項目と想定されるリスク及び加工例

4.3.2 Categories of Information, Their Potential Risks, and Examples of Processing

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。

Risks of identification of a specific individual vary according to the attribute of information. Figure 4-4 shows examples of processing for each category of information that can be contained in personal information that is to be processed, which can be referred to when processing information. Here, categories of information concerning the basic attributes of a principal concerning personal information are categorized into "individual attribute information," and categories of information concerning behavioral history derived from actions of an individual are categorized

[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。
To randomly extract a part of records from a personal information database, etc. constituting the whole population.

into "history information."

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。

The examples of processing shown below are examples of common processing methods. However, they are not intended to limit processing methods or to guarantee that these methods will always be sufficient. The categories of information to be processed and level of processing them should be appropriately determined according to the categories of information contained in a database, number of records, etc. Therefore, they should be established properly under personal information protection policies or other voluntary rules formulated by accredited organizations.

図表4-4 情報の項目と想定されるリスク及び加工例

Figure 4-4 Categories of information, potential risks and examples of processing

項目 **Category**		**想定されるリスク** **Potential risks**	**加工例** **（「削除」は置き換えも含む）** **Example of processing** **(To "delete" also includes to replace)**
個人属性情報 Individual attribute information	**氏名** **Name**	・それ自体で個人を特定できる。 ・This alone can identify an individual	全部削除 Delete entirely
	生年月日 **Date of birth**	・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。 ・Can identify an individual when combined with address (postal code) and gender	・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） ・Delete either year or date, in principle. If necessary replace with month and year of birth, age, decade, etc. (rounding) ・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）

		・Delete date of birth and age data that suggest an extremely old age (deletion of cells/top-coding)
性別 **Gender**	・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。 ・Can identify an individual when combined with address (postal code) and date of birth	・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） ・Delete gender as necessary, according to the combination with other information (deletion by category)
住所 **Address**	・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。 ・Can identify an individual when combined with date of birth and gender ・本人にアクセスすることができる。 ・Allows access to the principal	・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） ・Delete details, such as name of town, street address, name of apartment, etc. in principle (rounding) ・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） ・Replace with the name of prefecture or name of municipality, according to the total number of records (rounding)
郵便番号 **Postal code**	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。 Can result in identification of an individual when combined with date of birth, gender, etc.	下4桁を削除する。（丸め） ・Delete the last four digits (rounding)
マイナンバー **Individual number**	それ自体で個人情報とされている。（個人識別符号） This alone constitutes personal information (individual identification code).	全部削除する。（項目削除） Delete entirely (deletion by category)
パスポート番	それ自体で個人情報とされてい	全部削除する。（項目削除）

号 **Passport number**	る。 （個人識別符号） This alone can constitute personal information (individual identification code).	Delete entirely (deletion by category)
顔認証データ **Facial recognition data**	それ自体で個人情報とされている。 （個人識別符号） This alone can constitute personal information (individual identification code).	全部削除する。（項目削除） Delete entirely (deletion by category)
固定電話番号 **Landline phone number**	・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。 ・Can function as an identifier to identify an individual among different datasets, as it is collected by many business operators ・本人にアクセスすることができる。 ・Allows access to the principal	原則として、加入者番号（下4桁）を削除。（丸め） Delete the subscriber's number (last four digits) in principle (rounding)
携帯電話番号 **Mobile phone number**	・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。 ・Can function as an identifier to identify an individual among different datasets, as it is collected by many business operators ・本人にアクセスすることができる。 ・Allows access to the principal	全部削除する。（項目削除） Delete entirely (deletion by category)
クレジットカ	・多くの事業者が収集しており、	全部削除する。（項目削除）

ード番号 **Credit card number**	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。 ・Can function as an identifier to identify an individual among different datasets, as it is collected by many business operators ・本人に直接被害を与え得る。 ・Can directly cause harm to the principal	Delete entirely (deletion by category)
サービスID、アカウントID **Service ID, account 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。 Can function as an identifier to identify an individual, if the ID is commonly used by many business operators	全部削除する。（項目削除） Delete entirely (deletion by category)
電子メールアドレス **E-mail address**	・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。 ・Can function as an identifier to identify an individual among different datasets, as it is collected by many business operators ・本人にアクセスすることができる。 ・Allows access to the principal	全部削除する。（項目削除） Delete entirely (deletion by category)
端末ID **Terminal 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。 Can function as an identifier to identify an individual, if the ID is commonly used by many business	全部削除する。（項目削除） Delete entirely (deletion by category)

		operators	
	職業 **Job**	・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。 ・Can result in identification of an individual when combined with address, annual income, etc.	・勤務先名を職種等のカテゴリーに置き換える。（一般化） ・Replace the name of workplace with a category name, such as job type (generalization)
	年収 **Annual income**	・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。 ・Can result in identification of an individual when combined with job, address, etc. ・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。 ・In case of extremely high annual income, this alone can identify an individual.	・具体的な年収を収入区分へ置き換える。（丸め） ・Replace specific annual income data with salary range (rounding) ・超高収入の値を削除する。（セル削除/トップコーディング） ・Delete the values of extremely high salary (deletion of cells/top-coding)
	家族構成 **Family structure**	・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。 ・Probability to result in identification of an individual becomes higher when combined with address, etc.	・具体的な家族人数を人数区分へ置き換える。（丸め） ・Replace a specific number of family members with a range of number of family members (rounding) ・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） ・Replace detailed family structure with a classification of household structure (single, parents and children, three-generational household, etc.) (rounding)
履歴情報 **History**	**購買履歴** **Purchase**	・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	・購入店舗や購買時刻の詳細な情報を削除する。（丸め） ・Delete detailed information, such as

history	人の特定につながる可能性がある。 ・Can result in identification of an individual when information on a store at which purchase was made and time of purchase and information contained in another dataset are combined. ・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。 ・Can result in identification of an individual when a purchase record of idiosyncratic goods and residence area, etc. are combined	store at which purchase was made and time of purchase (rounding) ・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） ・Delete idiosyncratic purchase information (extremely high payment, extremely high purchase frequency, etc.) (deletion of cells/top-coding)
乗降履歴 **Transportation history**	・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。 ・Records concerning a station or time during which the number of passengers getting on and off the train is extremely small can result in identification of an individual. ・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。 ・Information concerning a station which is rarely included in a commuter pass area can result in identification of an individual	・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） ・Delete information concerning a station or time range with an extremely small number of users. Replace time information with a period of time (deletion of cells/rounding) ・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） ・Delete information on a commuter pass area that includes a station with an extremely small number of users (deletion of cells)
位置情報（移動履歴） **Location information (movement**	・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。 ・Location of home, workplace, etc. can be estimated based on the	・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） ・Delete information on start point and end point that may result in estimation of the location of home, workplace, etc.

history)	locations visited during the day and night. ・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。 ・Combination of detailed location information and time information can function as an identifier among different datasets. ・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。 ・Can result in identification of an individual when location information in a certain area is extremely small.	(rounding) ・位置情報若しくは時刻情報の詳細部分を削除する。（丸め） ・Delete detailed parts of location information or time information (rounding) ・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） ・Add noise to values for areas with small location information (noise addition) ・所定数以上の位置情報になるようエリアを区切る。（丸め） ・Separate areas so that each contains a certain volume or more of location information (rounding)
電力利用履歴 **Power consumption history**	・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。 ・Can result in identification of an individual when idiosyncratic power consumption is combined with other information. ・生活スタイルや家族構成を推定できる可能性がある。 ・Lifestyle and family structure can be estimated.	・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） ・Delete information on extremely large power consumption (deletion of cells/top-coding)

（参考）

(Reference)

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。

In relation to processing methods for anonymously processed information, the Ministry of Economy, Trade and Industry published "Reference Material to Help Business Operators Consider Methods for Producing Anonymously

Processed Information (Anonymously Processed Information Production Manual)" (hereinafter referred to as the "METI Manual") on August 8, 2016.

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。

In accordance with Article 36, paragraph (1) of the Act, anonymously processed information needs to be processed in compliance with the standards provided in the items of Article 19 of the Enforcement Rules. However, The METI Manual was published before the establishment of the Enforcement Rules as a result of discussions at the Ministry of Economy, Trade and Industry that were carried out independently from discussions on the formulation of the Enforcement Rules.

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]。

The METI Manual categorizes descriptions, etc. contained in personal information into [i] identifier, [ii] attribute, and [iii] history, for which processing policies are provided as follows.[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。

[i] Descriptions, etc. falling under the category of "identifier" are to be deleted in principle, as they entail a high risk of identification of an individual.[35]

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。

[ii] For descriptions, etc. falling under the category of "attribute," risks of identification of an individual when multiple attributes are combined are to be examined.

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。

[iii] For descriptions, etc. falling under the category of "history," risks of identification due to idiosyncratic values and accumulation are to be examined.

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。

As such approaches to risk analysis, etc. can serve as a reference when considering processing methods, the

[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。

The METI Manual states that these categories are provided for the sake of convenience in anonymization processing and thus it may be necessary to revise sortation (for example, it states that address, etc. may fall under both "identifier" and "attribute"). The METI Manual also includes cases wherein processing is categorized into two groups of "customer attribute data" and "usage detail data."

[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。

Here, risks of identification of an individual, risks of collation of data with other information, risks of access to a principal utilizing data, etc. are considered.

relationship between the METI Manual and standards provided in the items of Article 19 of the Enforcement Rules is shown in Figure 4-5.

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。

Roughly, "personal attribute information" as shown in Figure 4-4 is equivalent to "identifier" and "attribute" in the categories provided in the METI Manual, and "history information" in Figure 4-4 "history information" in the METI Manual.

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

Figure 4-5 Categories provided by the METI Manual and standards of the Enforcement Rules that mainly correspond thereto

分類 **Category** (主に対応する施行規則) (Enforcement Rules that mainly correspond)	**定義** **Definition**
識別子 **Identifier** （第19条 第1号、 第２号、 第３号、 第5号） (Article 19, items (i), (ii), (iii) and (v))	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。 Information constituting personal data, which alone can identify an individual 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) e.g. Name, date of birth, account ID, terminal ID, subscriber ID, telephone number, e-mail address, detailed address (including street address and room number)
属性情報 **Attribute information** （第19条 第1号、第５号） (Article 19, items (i) and (v))	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。 Information constituting personal data, which is not to be accumulated over time and which cannot identify an individual alone, but can identify an individual when combined with other attributes or through collation with external information 例：性別、年齢、郵便番号、住所（市町村まで）家族構成、年収 等 e.g. gender, age, postal code, address (to the municipality level), family

	structure, annual income, etc.
履歴情報 **History information** (第19条 第5号) (Article 19, item (v))	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。 Information constituting personal data that retains historical records of an individual's behavior, which is accumulated over time and which cannot alone identify an individual, but can identify an individual when combined with other attributes or collation with external information 例：購買の履歴、ウェブの閲覧履歴、乗降履歴 等 e.g. purchase history, web browsing history, transportation history, etc.

※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。

*In addition to the above, Article 19, item (iv) of the Enforcement rules provide for processing of idiosyncratic data that can result in the identification of a specific individual. This is considered to mainly correspond to attribute information (age, etc.)

5. 匿名加工情報等の安全管理措置

5. Security Control Actions for Anonymously Processed Information, etc.

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。

Security control actions based on Article 26, paragraphs (2) and (6) of the Act need to be taken when anonymously processed information has been produced. Paragraph (2) provides for an obligation concerning the prevention of leakage of processing method, etc.-related information concerning anonymously processed information. Paragraph (6) provides for an obligation to strive concerning general security control actions for the handling of anonymously processed information and actions for dealing with a complaint, etc.

5.1 加工方法等情報の安全管理措置について

5.1 Security Control Actions for Processing Method, etc.-Related Information

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。

As provided in Article 36, paragraph (2) of the Act, security control actions shall be taken for information relating to a processing method used for the production of anonymously processed information ("processing method, etc. related information") in accordance with the standards prescribed by the Enforcement Rules.

法第36条第2項

Article 36(2) of the Act

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。

(2) A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of information relating to those descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

施行規則第20条

Article 20 of the Enforcement Rules

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。

Article 20　Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (2) of the Act shall be as follows.

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。

(i)　defining clearly the authority and responsibility of a person handling processing method, etc. related information (meaning information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1) (limited to those which can restore the personal information by use of such relating information); the same applies hereinafter in this Article)

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。

(ii)　establishing rules and procedures on the handling of processing method etc. related information, handling appropriately processing method etc. related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement

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。

(iii)　taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc. related information from handling the processing method etc. related information

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）

Guidelines 3-3-1 Security Control Actions, etc. for Processing Method, etc.-Related Information (Related to Article 36, Paragraph (2) and Article 39 of the Act)

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。

A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with the standards provided in the Rules, so as to prevent the leakage of processing method, etc.-related information (meaning information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and

information relating to a processing method (limited to those which can restore the personal information by use of such relating information*); the same applies hereinafter) take necessary actions.
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。
The details of said actions need to be determined according to the volume, nature, etc. of the processing information, taking into account the significance of restoration risks in case of leakage of the relevant processing method, etc.-related information. See Appended Table 2 (Examples of Actions That Are Required for the Security Control of Processing Method, etc.-Related Information) for matters for which actions need to be taken and examples of actions.

（※）「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。
(*) "Those which can restore the personal information by use of such relating information" include parameters, such as random values used for replacement algorithm used when replacing 'name', etc. with a temporary ID, and information concerning a processing method, such as a chart indicating corresponding relationships between names and temporary IDs. This does not include information that does not lead to the restoration of the original personal information, such as information that "age data was replaced with 10-year age groups."

（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
(Appended Table 2) Examples of Actions That Are Required for the Security Control of Processing Method, etc.-Related Information

講じなければならない措置 Action that need to be taken	具体例 Example
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） [i] Defining clearly the authority and responsibility of a person handling process method, etc.-related information (Article 20,	・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 ・Establishment of an organizational structure to take security control actions for processing method, etc.-related information

item (i) of the Enforcement Rules)	
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） [ii] Establishing rules and procedures on the handling of processing method etc.-related information, handling appropriately processing method etc.-related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement (Article 20, item (ii) of the Enforcement Rules)	・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 ・Establishment of rules and procedures on the handling of processing method etc.-related information, and operation in accordance with such rules and procedures ・従業員の教育 ・Education of employees ・加工方法等情報の取扱状況を確認する手段の整備 ・Establishment of procedures to check the handling situation of processing method, etc.-related information ・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 ・Understanding of the handling situation of processing method, etc.-related information, and evaluation, revision and improvement of security control actions
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） [iii] Taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc.-related information from handling the processing	・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 ・Prevention of browsing, etc. of processing method, etc.-related information by a person with no authority to handle such information ・機器、電子媒体等の盗難等の防止 ・Prevention of theft, etc. of devices, electronic media, etc. ・電子媒体等を持ち運ぶ場合の漏えい等の防止 ・Prevention of leakage, etc. of electronic media, etc. during transportation ・加工方法等情報の削除並びに機器、電子媒体等の廃棄 ・Deletion of processing method, etc.-related information and disposal of devices, electronic media, etc.

method etc.-related information (Article 20, item (iii) of the Enforcement Rules)	・加工方法等情報へのアクセス制御 ・Control of access to processing method, etc.-related information ・加工方法等情報へのアクセス者の識別と認証 ・Identification and authentication of a person accessing processing method, etc.-related information ・外部からの不正アクセス等の防止 ・Prevention of external unauthorized access, etc. ・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 ・Prevention of leakage, etc. of processing method, etc.-related information associated with the use of an information system

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。

A personal information handling business operator produces anonymously processed information by processing personal information that it holds. Said business operator that has produced anonymously processed information is allowed to retain descriptions, etc. and individual identification codes, which are deleted from said personal information in the course of processing, and information relating to a processing method[36] that was carried out in accordance with the provision of Article 36, paragraph (1) of the Act, along with the original personal information. When doing so, said business operator shall take security control action in accordance with the standards provided in Article 20 of the Enforcement Rules in order to prevent leakage of such information.

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。

As stated in the Guidelines, action for preventing the leakage of processing method, etc.-related information (meaning information relating to those descriptions etc. and individual identification codes which were deleted

[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。

Information relating to a processing method includes information, etc. concerning input information that is used for a replacement algorithm for replacing 'name', etc. with temporary IDs, information on parameters concerning a processing method, such as ratio of added noise, and a chart indicating corresponding relationships between the original personal information and temporary IDs, etc. assigned to anonymously processed information.

from personal information used to produce anonymously processed information and information relating to a processing method (limited to those which can restore the personal information by use of such relating information)), according to the volume, nature, etc. of the processing information, taking into account the significance of restoration risks (risks that the original personal information is restored by using the processing method, etc.-related information) in case of leakage of the relevant processing method, etc.-related information.

5.2 匿名加工情報の安全管理措置等について

5.2 Regarding Security Control Action, etc. for Anonymously Processed Information

法第36条第6項

Article 36(6) of the Act

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。

(6) A personal information handling business operator shall, when having produced anonymously processed information, strive to take itself necessary and appropriate action for the security control of the anonymously processed information and necessary action for ensuring the proper handling of the anonymously processed information such as dealing with a complaint about the handling, including producing, of the said anonymously processed information, and strive to disclose to the public the contents of such action taken.

法第39条

Article 39 of the Act

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。

An anonymously processed information handling business operator shall strive to take itself necessary and appropriate action for the security control of anonymously processed information and necessary action to ensure the proper handling of anonymously processed information such as dealing with a complaint about the handling of anonymously processed information, and shall strive to disclose to the public the contents of such action taken.

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）

Guidelines 3-3-2 Security Control Action, etc. for Anonymously Processed Information (Related to Article 36, Paragraph (6) and Article 39 of the Act)

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。

A personal information handling business operator or anonymously processed information handling business operator must take necessary action for ensuring the proper handling of anonymously processed information at its own initiative, which includes security control action for anonymously processed information and action for dealing with a complaint, while making best efforts to disclose the details of such action.

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。

It is not required for said action, including security control action, to handle anonymously processed information in the same way as personal information. However, it is possible to refer to examples of the action* that is required for the purpose of the security control of personal data, supervision over employees, supervision over a trustee provided in Articles 20 to 22 of the Act and dealing with a complaint concerning the handling of personal information provided in Article 35 of the Act. Specifically, it is encouraged to take reasonable and proper action according to the nature of business, the handling situation of anonymously processed information, the nature and volume of handling anonymously processed information, etc.

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。

Since the obligation to prohibit the act of identifying applies in relation to anonymously processed information, it is important to make sure that it is clear for a person handling such information that the information he/she is handling constitutes anonymously processed information, so that he/she can prevent handling such information in an inappropriate way. Once anonymously processed information is produced, it is encouraged to keep said information in a state wherein it is immediately clear for a person handling said information that said information constitutes anonymously processed information.

（※）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。

(*) For details, see "3-3-2 (Security Control Action)," "3-3-3 (Supervision over Employees)," "3-3-4

(Supervision over a Trustee)," and "3-6 (Dealing with a Complaint Concerning the Handling of Personal Information)" of the Guidelines on General Rules.

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。

As stated in the Guidelines, a personal information handling business operator or anonymously processed information handling business operator must take necessary action at its own initiative, including security control action for anonymously processed information and action for dealing with a complaint. Such action needs to be taken with reference to security control action and action for dealing with a complaint concerning personal data, while taking into account the nature of anonymously processed information.

6. 匿名加工情報の利用に当たっての留意点

6. Matters to Keep in Mind When Using Anonymously Processed Information

6.1 識別目的の照合とは

6.1 What Is the Collation conducted for the Purpose of Identification?

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。

As provided in Article 36, paragraph (5) and Article 38 of the Act, it is prohibited to collate anonymously processed information with other information for the purpose of identifying a principal concerned with the original personal information.

法第36条第5項

Article 36(5) of the Act

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。

(5) A personal information handling business operator shall, when having produced anonymously processed information and making itself handle the anonymously processed information, not collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the said anonymously processed information.

法第38条

Article 38 of the Act

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。

An anonymously processed information handling business operator, shall, in handling anonymously processed information, neither acquire information relating to those descriptions etc. or individual identification codes deleted from the personal information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1), nor collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the anonymously processed information.

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）

Guidelines 3-6 Prohibition of the Act of Identifying (Related to Article 36, paragraph (5) and Article 38 of

the Act)

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。

When handling anonymously processed information (*1), any of the following acts must not be engaged in for the purpose of identifying a principal of personal information from which said anonymously processed information is derived.

（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

(1) When a personal information handling business operator handles anonymously processed information that it produced itself

・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。

・Collating anonymously processed information that it has produced with other information (*2) in order to identify a principal.

（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

(2) When an anonymously processed information handling business operator handles anonymously processed information produced by another person

・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。

・Acquiring processing information, etc.-related information concerning anonymously processed information that it received

・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。

・Collating anonymously processed information that it received with other information (*2) in order to identify a principal

【識別行為に当たらない取扱いの事例】

[Examples of Handling That are Not Deemed as an Act of Identifying]

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。

Example 1) To create statistical information by combining multiple sets of anonymously processed information

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。

Example 2) To carry out a statistical analysis of trends using anonymously processed information and other information that is not related to an individual (e.g. weather information, traffic information, trading volume of a financial instrument)

【識別行為に当たる取扱いの事例】

[Examples That Are Deemed as an Act of Identifying]

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。

Example 1) To sort out common descriptions in personal information at hand and anonymously processed information, and collate such descriptions with one another

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。

Example 2) To collate anonymously processed information produced at one's own initiative with the original personal information

（※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。

(*1) It is prohibited to collate anonymously processed information with other information for the purpose of identifying a principal of personal information from which said anonymously processed information was derived. Meanwhile, it is not prohibited to collate information that is handled as personal information, within the scope of purpose of utilization, with other information.

（※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。

(*2) The scope of "other information" is not limited. Any act of collating information containing personal information and anonymously processed information performed for the purpose of identifying a principal is prohibited. In addition, said prohibition applies regardless of technology or method used for collation.

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。

Regardless of whether an individual is identified or nor, the act of collating for the purpose of identification constitutes violation of these obligations.

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。

Therefore, for example, to collate anonymously processed information with other information to analyze the trend in a group or market does not constitute a violation of obligation, since such an act is not performed for the purpose of identifying an individual.

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。

For example, it is also possible to take history information, such as purchase information, which has similar basic attributes (age, residence area, etc.), from multiple anonymously processed information databases that have been provided by different business operators, and combine the said information in order to create more detailed statistical information.

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。

On the other hand, to link personal data contained in a personal information database that is internally held at a business operator and anonymously processed information contained in an anonymously processed information database that has been provided by a third party based on the similarity of basis attributes is generally considered to be conducted for the purpose of identification. This conclusion does not change even if the said linking was carried out by chance.

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

6.2 Collation Carried out for the Evaluation of a Processing Method and Determination of the Scope of Influence in Case of Re-Identification Incident, etc.

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]。

As stated in Section 3.2, the phrase "neither to be able to identify a specific individual nor to be able to restore the personal information" as used in relation to anonymously processed information is to be determined based on the ability of and method, etc. available to ordinary people and ordinary business operators. The said phrase is not intended to require the elimination of every technical possibility of identification or restoration.[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

[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。
"Report by the Technical Study Working Group" (December 2013) (Study Group on Personal Data), “Opinion 05/2014 on Anonymisation Techniques” (April 2014) (Article 29 Data Protection Working Party) and other documents also point out that there is no one-size-fit-all method for anonymization, that re-identification risks may change with technological progress, and that re-identification risks need to be monitored to evaluate and revise anonymization methods.

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。

Anonymously processed information is subject to the obligation concerning the prohibition of the act of identifying. In addition to this, Article 20, item (i) of the Enforcement Rules requires the clear definition of the authority and responsibility of a person handling processing method, etc.-related information, and item (iii) of the said Article requires control of access to processing method, etc.-related information by a person with no legitimate authority to handle the said information. Moreover, Article 36, paragraph (6) of the Act has a requirement to take necessary and appropriate action for the security control of anonymously processed information. Collation of information carried out by a person with legitimate authority to handle process information, etc.-related information for the purpose of evaluating or determining the scope of influence, which is conducted as part of security control action, is allowed as long as it is deemed necessary for the sake of security control action. Such act is not considered to constitute an act of identifying that is prohibited by Article 36, paragraph (5) of the Act.

6.3 匿名加工情報を加工したものの扱い

6.3 Handling of Information Produced by Processing Anonymously Processed Information

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。

Anonymously processed information that has been processed may be processed by a third party to which the said information was provided, by such means as adding information or deleting some categories of information.

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。

When information is added to anonymously processed information, anonymously processed information after the said addition of information should be handled as information identical to the original anonymously processed information, as it would retain information contained in the original anonymously processed information as it is.

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。

On the other hand, when information is deleted from the original anonymously processed information, it is appropriate to handle anonymously processed information after the said deletion of information as information identical to the original anonymously processed information, as long as the corresponding relationship between the information after the said deletion of information and the original anonymously processed information is clear, although this depends on the volume of information deleted.

6.4 意図せず特定個人を識別してしまった場合の扱い

6.4 Handling of Information with Which a Specific Individual Has Been Identified Accidentally

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。

Since obligations under Article 36, paragraph (5) and Article 38 of the Act only apply to the act of collating performed for the purpose of identification, a business operator would not be immediately punished for a violation of these obligations when it has accidentally identified a specific individual due to insufficient processing. However, the said business operator is required to make efforts not to identify another individual in the same way, and the said collated information is required to be handled properly as personal information.

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。

Moreover, if a specific individual has been identified in the course of usual business operation due to insufficient processing, it means that the requirements of anonymously processed information were not met and thus such information needs to be handled as personal information. In such case, a business operator that produces and itself handles anonymously processed information is required to properly handle such information as personal information after obtaining a principal's consent; otherwise, a business operator that has received information is required to delete the said information and discontinue the utilization of the said information.

7. 匿名加工情報のユースケースと加工例について

7. Use Cases and Processing Examples of Anonymously Processed Information

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。

Given the circumstances that various personal information handling business operators acquire and accumulate personal information, by producing anonymously processed information based on the processing standards prescribed by the Enforcement Rules, these business operators are able to use personal information for a new purpose that they did not intend when they acquired said personal information, and to provide said information to a third party. This Section will explain specific processing methods that accommodate matters and risks that need to be considered concerning each category of information, with possible use cases in mind. These methods were examined with reference to opinions from experts.

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。

Among the use cases explained in this Report, the use cases described in "7.1.2 Example of Purchase History 2 (Credit Card Usage Information)," "7.2.1 Example of Transportation History," and "7.3 Example of Power Consumption Data" were developed by the Secretariat of the Personal Information Protection Commission, with reference to the METI Manual. Note that all the use cases explained in this Report only cover the primary distribution of anonymously processed information produced, and do not cover the secondary distribution thereof.

7.1 購買履歴の事例

7.1 Example of Purchase History

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。

Purchase history information is acquired and accumulated in various forms by retail business operators which sell products to consumers, mail order business operators, credit card business operators which provide means of payment, point card management business operators, etc.

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。

Such purchase history information is expected to be used for advertisement, marketing, product development and various other purposes. The following is examples of possible use cases where retail business operators, credit card business operators, etc. produce anonymously processed information to use it for a purpose other than the original purpose or provide it to a third party.

7.1.1 購買履歴の事例１（ID-POS データ）

7.1.1 Example of Purchase History 1 (ID-POS Data)

１）ユースケース

1) Use Case

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。

In this use case, a retail business operator carries out anonymization processing on the purchase history (ID-POS data) it retains, and provides it (i.e. the annomymously processed purchase history information) to other business operators, by utilizing the framework of anonymously processed information. Said other business operators can utilize information on the basic attributes and purchase trends of consumers contained in the provided information for new product development, sales promotion activities, etc.

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

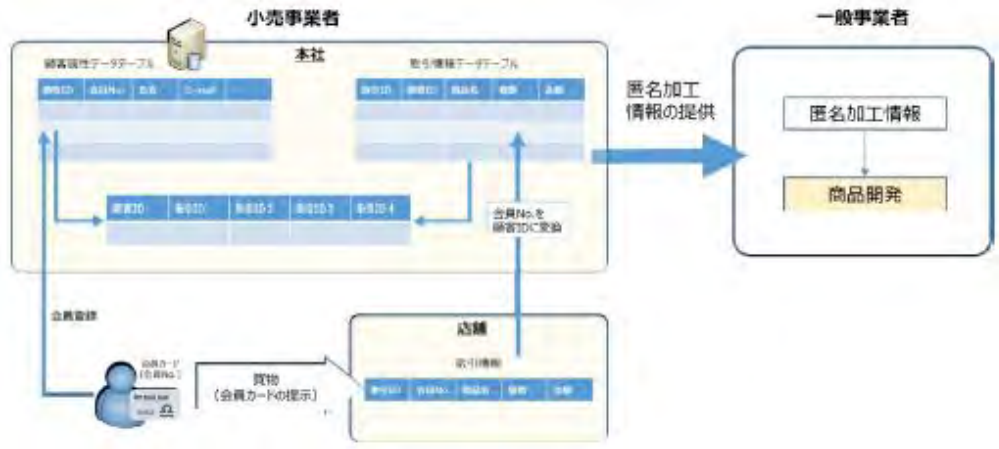
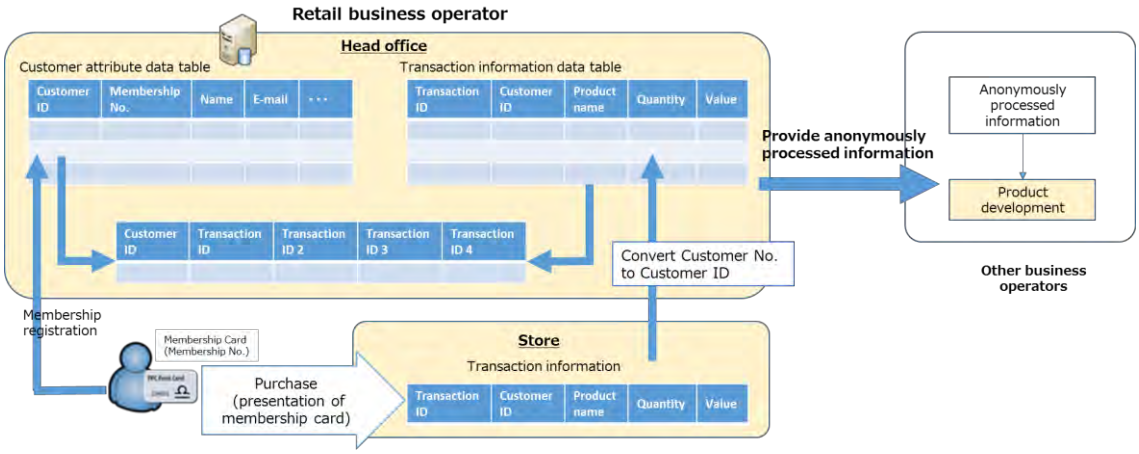


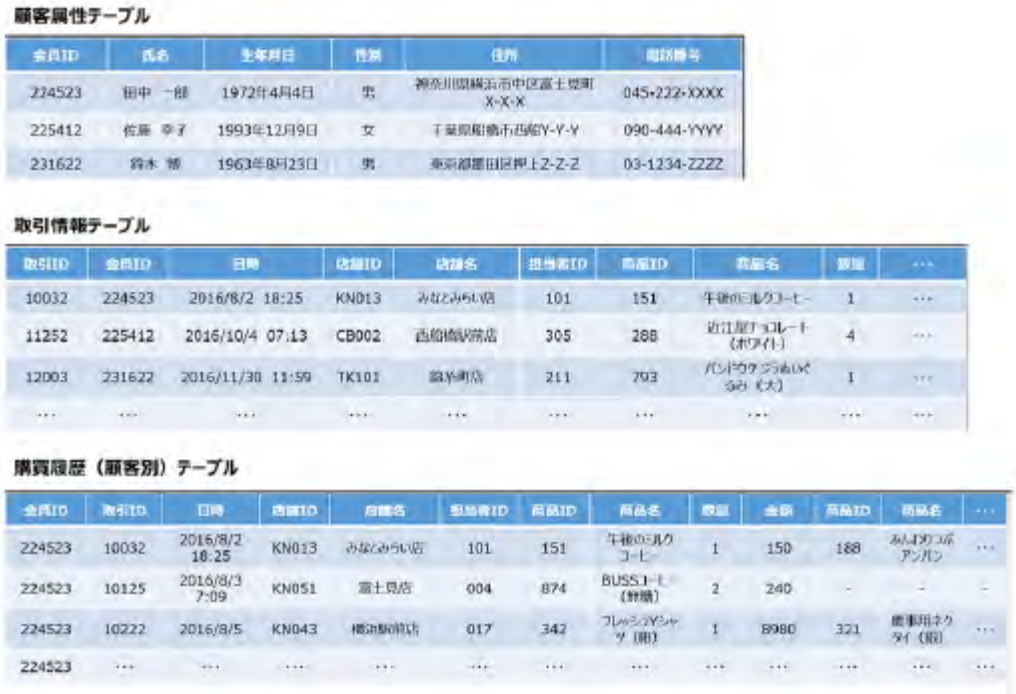
Figure 7-1 Concept of a use case where a retail business operator provides purchase history information it retains to a third party



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。

This use case is based on the data structure as shown in Figure 7-2, which is comprised of a customer attribute table, transaction information table, and purchase history table. The customer attribute table and transaction information table can be mutually linked using Membership IDs. By this means, a purchase history table that shows the purchase history of individual customers can be created.

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	バンドウイルカぬいぐるみ（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	みんなのコボアンパン	…
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	礼事用ネクタイ（銀）	…
224523	…	…	…	…	…	…	…	…	…	…	…	…

Figure 7-2 Layout of purchase history data (ID-POS data)

Customer attribute table

Membership ID	Name	Date of birth	Gender	Address	Telephone number
224523	Ichiro Tanaka	April 4, 1972	Male	X-X-X, Fujimi-cho, Naka-ku, Yokohama City, Kanagawa Prefecture	045-222-XXXX
225412	Sachiko Sato	December 9, 1993	Female	Y-Y-Y, Nishifuna, Funabashi City, Chiba Prefecture	090-444-YYYY
231622	Hiroshi Suzuki	August 23, 1963	Male	Z-Z-Z, Oshiage, Sumida-ku, Tokyo	03-1234-ZZZZ

Transaction information table

Transaction ID	Membership ID	Date and time	Store ID	Store name	Staff ID	Product ID	Product name	Quantity	…
10032	224523	2016/8/2 18:25	KN013	Minatomirai Store	101	151	Gogo no Milk Coffee	1	…
11252	225412	2016/10/4 07:13	CB002	Nishi-funabashi Ekimae Store	305	288	Ohmiya Chocolate (White)	4	…
12003	231622	2016/11/30 11:59	TK101	Kinshicho Store	211	793	Stuffed Bottlenose Dolphin (Large)	1	…
…	…	…	…	…	…	…	…	…	…

Purchase history (by customer) table

Membership ID	Transaction ID	Date and time	Store ID	Store name	Staff ID	Product ID	Product name	Quantity	Value	Product ID	Product name	…
224523	10032	2016/8/2 18:25	KN013	Minatomirai Store	101	151	Gogo no Milk Coffee	1	150	188	Funwari Tsubuan Bread	…
224523	10125	2016/8/3 7:09	KN051	Fujimi Store	004	874	BUSS Coffee (Sugar Free)	2	240	-	-	-
224523	10222	2016/8/5	KN043	Yokohama Ekimae Store	017	342	FRESH Shirt (Navy)	1	8980	321	Formal Tie (Silver)	…
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

2) Examination of Specific Processing Methods That Accommodate Matters and Risks That Need to Be Considered

① 含まれ得る情報の種類

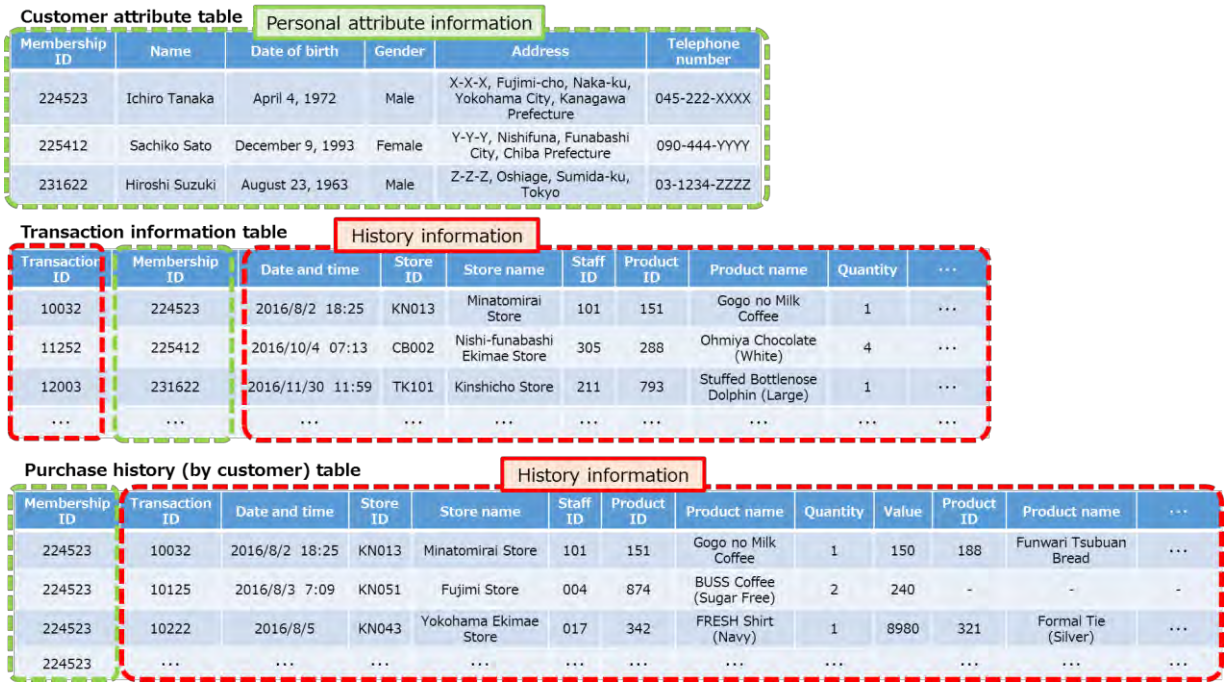
[i] Categories of Information Contained

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。

Categories of information that constitute the data tables shown in Figure 7-2 can be classified into personal attribute information and history information, as shown below.

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

Figure 7-3 Layout of purchase history data (ID-POS data)



② どのように加工すべきか

[ii] How the Information Should Be Processed

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。

Processing methods should be examined for each of personal attribute information and history information described above.

【個人属性情報】

[Personal attribute information]

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。

As for personal attribute information, processing methods are primarily examined on the aspects of Article 19, items (i) to (iv) of the Enforcement Rules. Personal attribute information in this use case includes a membership ID, name, date of birth, gender, address and telephone number.

＜会員ID＞

<Membership 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。

Membership IDs in this use case are assigned uniquely to individual customers. They are used for identifying each of customers and managing information relating to them, while they also function as codes to link the customer attribute table and the transaction information table. Therefore, these membership IDs fall under the scope of codes that link personal information and information obtained by having taken measures regarding the personal information, which is provided in Article 19, item (iii) of the Enforcement Rules. Accordingly, all of the membership IDs need to be deleted by replacing them with temporary IDs.

＜電話番号＞

<Telephone number>

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。

'Telephone number' is deemed as information that is likely to result in the identification of a specific individual, in light of the fact that it is information collected by many business operators and there is a risk of allowing access to a principal. Therefore, all telephone numbers need to be deleted. Note that it is possible to leave a part of a landline telephone number that indicates a geograpfical area, such as an area code and local number, to an extent that aligns with the information contained in generalized descriptions concerning address.

＜住所＞

<Address>

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）。

'Address' is deemed as information that is likely to result in the identification of a specific individual, in light of the fact that it is information collected by many business operators and there is a risk of allowing access to a principal. Meanwhile, information indicating the place of residence of customers is useful from the perspective of marketing, etc. Among descriptions comprising an address, information referring to a wide geographical area, such as prefecture name and city name, has little impact on an individual for a risk of identifying himself/hersel. Therefore, address information should be rounded (generalized) by deleting information indicating detailed areas.

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。

Although the rounding of information should be performed based on the size of dataset and level of processing of other information (for example, date of birth), it is encouraged to delete municipalities and more detailed address information, in principle. It is also possible to adopt different levels of rounding for the same dataset, according to the population.

＜生年月日＞

<Date of birth>

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。

At least, the date information contained in date of birth data should be deleted. However, the extent of deletion (such

as whether to replace date of birth with month and year of birth or generalize by age or to ten-year intervals) should be decided objectively based on the number of relevant people, as with the case of address information described above. For example, if the number of individuals born in a certain month of a certain year is small, the month data should be deleted. It is encouraged to consider the extent of generalization of date-of-birth information together with the processing of address information.
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。
Moreover, date of birth for which the number of living individuals is extremely low, such as date of birth of an extremely old individual, can constitute an idiosyncratic value under Article 19, item (iv) of the Enforcement Rules. In such a case, information concerning that date of birth should be deleted or age should be rounded to "100 years old and above" by top-coding.

＜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。
<Gender>
Gender information is not to be subject to processing in this use case, in light of the fact that there is a need to analyze the difference in purchase trends for men and women and that the level of identifiability has been reduced by rounding information concerning date of birth and address.

【履歴情報】
[Purchase history]
＜時刻情報及び店舗情報の取扱い＞
<Handling of time information and store information>
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。
Transaction information in this use case, which constitutes history information, contains detailed information on date and time of transaction and information on the store name. Basically, time information alone does not have an ability to identify an individual. However, since it is possible to roughly estimate a location based on a store name (e.g. "PPC Mart Kasumigaseki Store"), combination of time information and store information can lead to the identification of an individual, when collated with other datasets that contains location information and time information.

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。

Therefore, it is encouraged to generalize at least either time information or store information. Since it is considered that there is a need to use store name information as is, time information will be rounded in this use case. Time information should be rounded to the minute level, at least. If the risk of identification of an individual is high because of small number of customers, rounding to the half-hour level or one-hour level should be also considered.

＜商品の購買履歴（商品名、個数、金額）の取扱い＞

<Handling of product purchase history (product name, quantity and value)>

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。

Purchase information can include records on purchase of one-of-a-kind products, limited products, or extremely expensive products. Information on the purchase of rare products would entail a higher risk of identifying an individual, when combined with other information, such as the store name. Therefore, such information should be deleted or product names should be replaced with product categories.

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。

In addition, information on the purchase of an ordinary product can also constitute an idiosyncratic description, etc. if the quantity is extremely large. In such a case, such information should be processed by deleting quantity information or replacing quantity information with average purchase quantity of the product by microaggregation.

＜その他の情報の取扱い＞

<Handling of other information>

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。

In this use case, transaction IDs are assigned to individual transactions. Transaction information contains the staff ID

of the staff who handled individual transactions and product ID of the dealt product. Such information is to be deleted, since such information is considered to be useless for potential receivers for this use case and information that is considered as unnecessary in data utilization by a third party should be generally deleted to reduce the risks of unintended re-identification.

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。
Policies for the processing of each category of information in this use case described above can be summarized as follows.

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

Figure 7-4 Policies for processing in the use case of purchase history (ID-POS data)

項目 Category	想定されるリスク Potential risks	望ましい加工方法 Preferred processing method
①個人属性情報 [i] Personal attribute information		
会員ID Membership 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。 Functions as IDs for internal distributed management and can identify an individual	全部削除する、あるいは仮IDに置き換える[38]。（項目削除） Delete entirely or replace with temporary IDs[38] (deletion by category)
氏名 Name	単体で個人を特定できる。 This information alone can identify an individual.	全部削除する（項目削除） Delete entirely (deletion by category)
生年月日 Date of birth	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。 Can identify an individual when combined with residence area, gender, etc.	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） Replace with seven age groups (below 20 years old, 20s, 30s, 40s, 50s, 60s, 70 years old and above) (rounding).
電話番号	他の事業者でも収集している可能性が	全部削除する。（項目削除）

[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。
In this use case, temporary IDs are used as IDs to link the customer attribute table and purchase history table after anonymization. The same applies in other use cases. For details concerning replacement with temporary IDs, see Section 4.11 [Replacement with Temporary ID].

Telephone number	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。 Likely to have been collected by other business operators and can result in identification of an individual when collated with other information. Entails a risk of allowing access to a principal.	Delete entirely (deletion by category).
性別 Gender	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。 Can identify an individual when combined with date of birth and residence area.	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。 In this use case, identifiability is addressed by processing date of birth and address. Gender information is not to be processed from the viewpoint of its usefulness.
住所 Address	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。 Can identify an individual when combined with date of birth and gender. Entails a risk of allowing access to a principal.	市区郡単位より細かい情報を削除する。（丸め） Delete municipalities and more detailed address (rounding).
②履歴情報 [ii] History information		
利用日時 Date and time of purchase	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。 Can result in identification of an individual when combined with location information contained in another dataset.	秒単位の情報を削除し、分単位に置き換える。（丸め） Delete second information and replace with minute data (rounding).

店舗ID Store ID	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
店舗名 Store name	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。 Location of purchase can be estimated based on the store name. Can result in identification of an individual when linked with location information contained in other information.	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。 In this use case, identifiability is addressed by processing date and time of purchase. Store name information is not to be processed from the viewpoint of its usefulness.
取引ID Transaction ID	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
担当者ID Staff ID	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
商品ID Product ID	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
商品名 Product name	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。 Can result in identification of an individual when combined with information on purchase history and place of purchase concerning rare products, such as limited products and ultra high-end products.	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） Delete purchase history concerning rare products. Otherwise, replace with product categories (deletion of cells, rounding, generalization).

項目 **Category**	想定されるリスク **Potential risks**	望ましい加工方法 **Preferred processing method**
数量	特定の商品に関する大量の購入実績	特異な購入実績を示す数量については削除

Quantity	から、個人の特定につながる可能性がある。 A purchase record concerning a certain product in a massive quantity can result in identification of an individual.	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） Delete quantity data indicating an idiosyncratic purchase record or replace quantity data with an average value (deletion of cells, microaggregation).
金額 Value	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。 A payment record of an extremely high value can result in identification of an individual.	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） Delete payment data indicating an idiosyncratic purchase record or replace payment data with a description of price range, such as "XX yen or more" (deletion of cells, top-coding).

③ 加工後のデータのイメージ

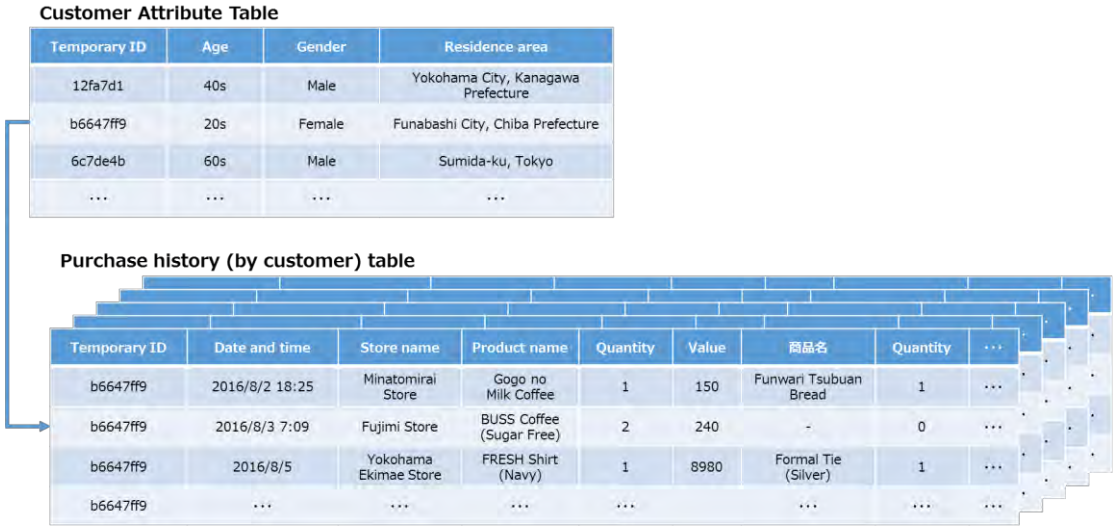
[iii] Processed Data

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。

Figure 7-5 shows data that has been processed based on the above approach.

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

Figure 7-5 Processed data in the use case of purchase history information (ID-POS data)



7.1.2 購買履歴の事例２（クレジットカード利用情報）

7.1.2 Example of Purchase History 2 (Credit Card Usage Information)

１）ユースケース

1) Use Case

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。

In this use case, a credit card business operator anonymizes credit card usage information that it retains, and provides processed information to other business operators, by utilizing the framework of anonymously processed information. Said other business operators can analyze relationships among annual income, job, and member stores, and utilize the results for marketing.

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

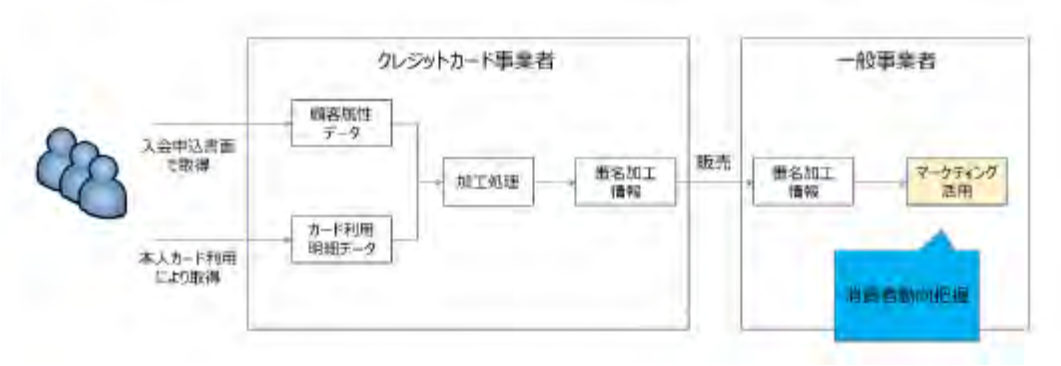
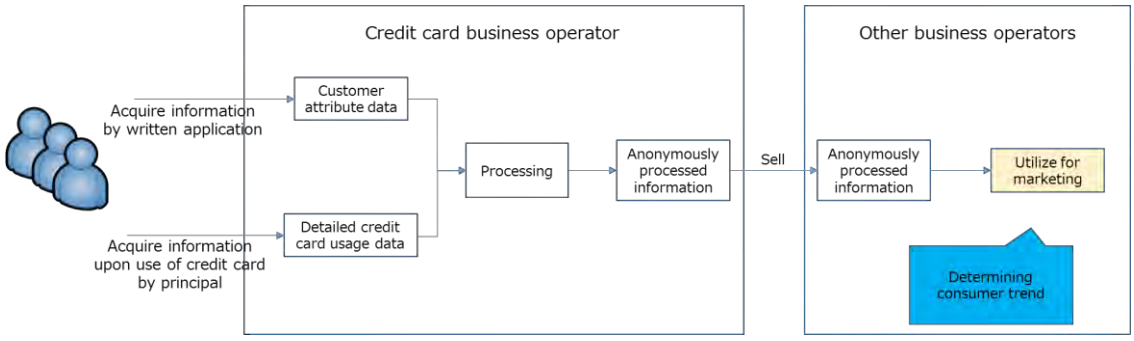


Figure 7-6 Use case where a credit card business operator provides card usage information it retains to a third party



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。

In this use case, the dataset that is subject to processing is comprised of two types of data: [i] customer attribute data; and [ii] detailed credit card usage data. These two kinds of data are mutually linked by cardholder IDs (numbers converted from credit card numbers).

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。

The customer attribute data contains information on customers' basic attribute, workplace, annual income and settlement financial institution. The detailed credit card usage data is comprised of information on date and time of credit card usage, member store, number of installments, and value of payment.

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

Figure 7-7 Sample layout of card usage data retained by a credit card business operator

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

2) Examination of Specific Processing Methods That Accommodate Matters and Risks That Need to Be Considered

① 含まれ得る情報の種類

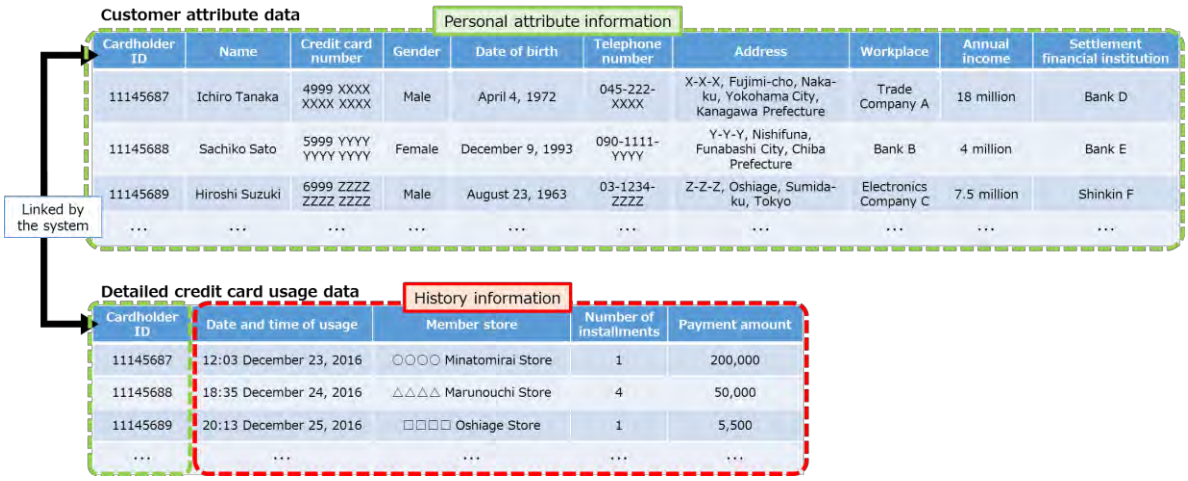
[i] Categories of Information That Can Be Contained

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。

Data shown in Figure 7-7 is categorized into personal attribute information and history information as below.

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

Figure 7-8 Layout of data contained in credit card usage information retained by a credit card business operator



② どのように加工すべきか

[ii] How the Information Should Be Processed

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。

In this use case, information that requires attention when handling is information on workplace and annual income, which is contained in personal attribute information, and information date of usage, member store, and value of payment, which is contained in the detailed credit card usage information that is history data.

【個人属性情報】

[Personal attribute information]

＜年収、勤務先＞

<Annual income and workplace>

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。

It is likely that risks of identification of an individual become higher when information on workplace is combined with address, for example. Furthermore, if information on annual income is added, it becomes possible to estimate job position, etc. Meanwhile, job category is information that is useful for marketing, etc. Therefore, information on workplace should be replaced with job category, rather than deleting the entire information.

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。

Since in this use case information on annual income is supposed to be provided to a third party along with information on workplace and address, information annual income should be rounded to a certain extent by replacing with annual income range. In addition, extremely high salary should be deleted or top-coded, since such data may fall under the scope of the measure provided in Article 19, item (iv) of the Enforcement Rules.

【履歴情報】

[History information]

＜カード利用明細データの取扱い＞

<Handling of detailed credit card usage data>

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。

Combination of date and time of usage, value of payment, and member store can result in the identification of an individual when combined with purchase history information held by another business operator. Since detailed credit card usage information is useful for marketing, etc., it should be generalized partially. Such generalization can be performed by replacing date of usage with month of usage and value of payment with payment value range.

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。

In addition, information concerning a member store at which the frequency of card usage is extremely low, extremely high payment value, and extremely high card usage frequency in a certain period should be processed by top-coding, etc., as such information can result in the identification of an individual due to its rarity.

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。

Policies for the processing of each category of information in this use case described above can be summarized as follows.

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

Figure 7-9 Examples of processing for the use case of purchase history (credit card usage history) information

項目 Category	想定されるリスク Potential risks	望ましい加工方法 Preferred processing method
① 個人属性情報 [i] Personal attribute information		
契約者ID Cardholder 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。 Converted from credit card numbers. Can identify an individual, if the conversion rules are decoded. Also used as IDs for internal distributed management at the business operator that produced anonymously processed information.	全部削除する、あるいは仮IDに置き換える。（項目削除） Delete entirely or replace with temporary IDs (deletion by category).
氏名 Name	単体で個人を特定できる。 This information alone can identify an individual.	全部削除する。（項目削除） Delete entirely (deletion by category).
クレジットカード番号 Credit card number	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） Delete entirely (deletion by category).

	Likely to have been collected by other business operators and can result in identification of an individual when collated with other information.	
性別 Gender	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。 Can identify an individual when combined with date of birth and address.	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。 In this use case, identifiability is addressed by processing information on date of birth and address. Gender information is not to be processed from the viewpoint of its usefulness.
生年月日 Date of birth	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。 Can identify an individual when combined with address and gender.	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） Replace with six age groups (below 30 years old, 30s, 40s, 50s, 60s, 70 years old and above) (rounding, top-coding).
電話番号 Telephone number	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。 Likely to have been collected by other business operators and can result in identification of an individual when collated with other information. Entails a risk of allowing access to a principal.	全部削除する。（項目削除） Delete entirely (deletion by category).
住所 Address	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。 Can identify an individual when combined	市区単位より細かい情報を削除する。（丸め） Delete information on municipalities and more detailed address information (rounding).

	with date of birth and gender. Entails a risk of allowing access to a principal.	
勤務先 Workplace	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。 Likely to have been collected by other business operators and can result in identification of an individual when collated with other information.	「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） Replace with job categories, such as "agriculture," "manufacturing," "retail," "financial service," etc.
年収 Annual income	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。 A person with extremely high income can be identified.	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） Replace with six income ranges (below 3 million yen, 3-6 million yen, 6-9 million yen, 9-12 million yen, 12-18 million yen, 18 million yen and above) (rounding, top-coding).
決済金融機関 Settlement financial institution	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
②履歴情報 [ii] History information		
利用日 Date of usage	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。 Can identify an individual when combined with member store and value of payment.	利用月単位に置き換える。（丸め） Replace with month of usage (rounding).
利用加盟店 Member store	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。 Can identify an individual if the frequency of credit card usage at the member store is low.	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） Delete information concerning member stores at which the frequency of credit card usage is extremely low (deletion of cells).

支払方法 Payment method	—	加工しない。 Not to be processed.
利用金額 Value of payment	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。 Extremely high payment value can identify an individual when combined with information on the member store at which the credit card was used.	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） Delete information on extremely high payment values. Delete information on cardholders whose payment values over a short term is high (deletion of cells, deletion of records).

③ 加工後のデータのイメージ

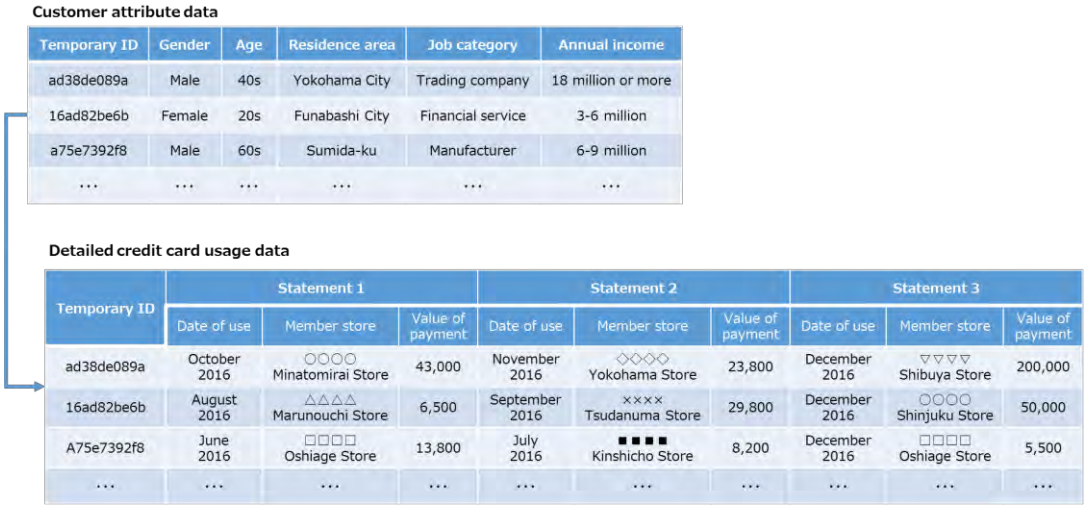
[iii] Processed Data

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。

Figure 7-10 shows data that has been processed based on the above approach.

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

Figure 7-10 Processed data in the use case of purchase history information (credit card usage history)



Customer attribute data

Temporary ID	Gender	Age	Residence area	Job category	Annual income
ad38de089a	Male	40s	Yokohama City	Trading company	18 million or more
16ad82be6b	Female	20s	Funabashi City	Financial service	3-6 million
a75e7392f8	Male	60s	Sumida-ku	Manufacturer	6-9 million
…	…	…	…	…	…

Detailed credit card usage data

Temporary ID	Statement 1			Statement 2			Statement 3		
	Date of use	Member store	Value of payment	Date of use	Member store	Value of payment	Date of use	Member store	Value of payment
ad38de089a	October 2016	○○○○ Minatomirai Store	43,000	November 2016	◇◇◇◇ Yokohama Store	23,800	December 2016	▽▽▽▽ Shibuya Store	200,000
16ad82be6b	August 2016	△△△△ Marunouchi Store	6,500	September 2016	×××× Tsudanuma Store	29,800	December 2016	○○○○ Shinjuku Store	50,000
A75e7392f8	June 2016	□□□□ Oshiage Store	13,800	July 2016	■■■■ Kinshicho Store	8,200	December 2016	□□□□ Oshiage Store	5,500
…	…	…	…	…	…	…	…	…	…

7.2 乗降履歴・移動履歴の事例

7.2 Examples of Transportation History Information and Movement History Information

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。

Due to the popularization of non-contact IC cards, railway companies (JR, private railways, metro, etc.) and bus companies have been promoting the acquisition and accumulation of transportation information. In addition, car navigation system manufacturers and automobile manufacturers have been promoting the accumulation and utilization of location information (movement history information) that can be obtained from GPS receivers on automobiles, as in-vehicle communication devices become popular.

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。

Such transportation history information and movement history information are expected to be used for various purposes, including traffic analysis for different areas and roads, analysis of commutation areas and commercial areas, regional development, advertisement, marketing, and product development. The following is examples of possible use cases where railway companies, bus companies, car navigation system manufacturers, automobile manufacturers, etc. produce anonymously processed information to use it for a purpose other than the original purpose and provide it to a third party.

7.2.1 乗降履歴の事例

7.2.1 Examples of Transportation History Information

１）ユースケース

1) Use Case

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。

In this use case, a railway company anonymizes transportation history information that it retains, and provides other business operators with anonymously processed information, by utilizing the framework of anonymously processed information. Said other business operators can utilize information on the basic attributes (age, gender, etc.) and transportation history of railway passengers contained in the provided information for commercial area analysis and development of strategies for targeted advertisement.

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

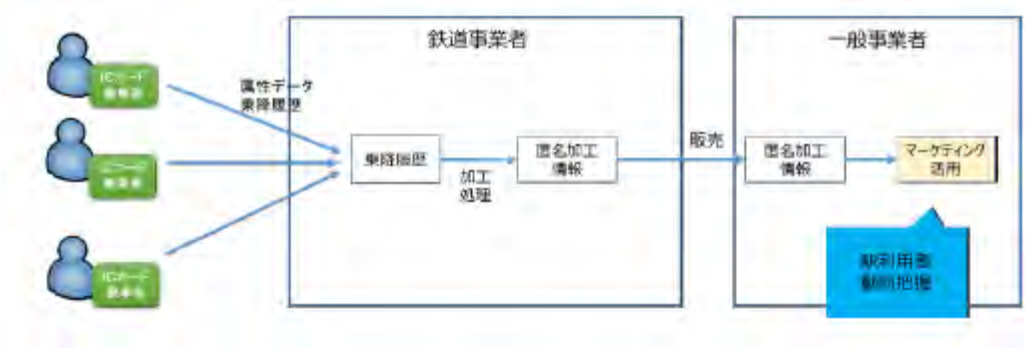
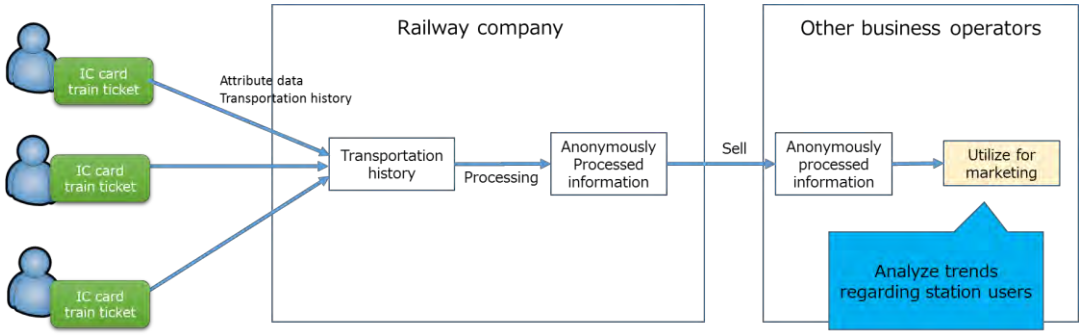


Figure 7-11 Use case where a railway company provides transportation history information it retains to a third party



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。

In this use case, the dataset that is subject to processing is comprised of two types of data: [i] customer attribute data;

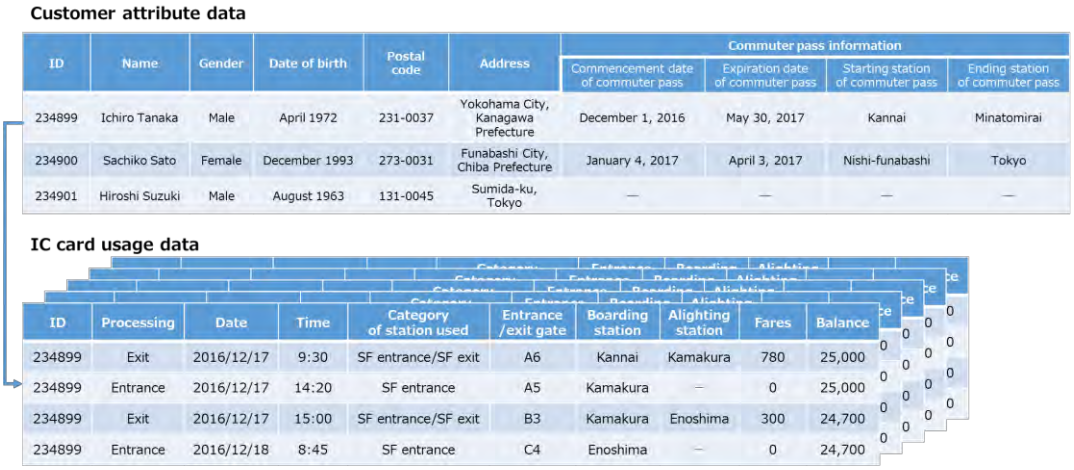
and [ii] IC card usage data. These two kinds of data are mutually linked by card IDs.

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。

The customer attribute data contains commuter pass information, which is comprised of the valid term (commencement date and expiration date) and valid area (starting station and ending station) of commuter passes. The IC card usage data is comprised of date and time of usage, stations at which the passenger got on and off the train, entrance/exit gates the passenger used, amount of transportation fees, and remaining balance on the IC card. In the IC card usage data, "SF entrance" means entrance into a station outside of the commuter pass area and "SF exit" means exit from a station outside of the commuter pass area.

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

Figure 7-12 Layout of data contained in boarding/alighting history information retained by a railway company



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

2) Examination of Specific Processing Methods That Accommodate Matters and Risks That Need to Be Considered

① 含まれ得る情報の種類

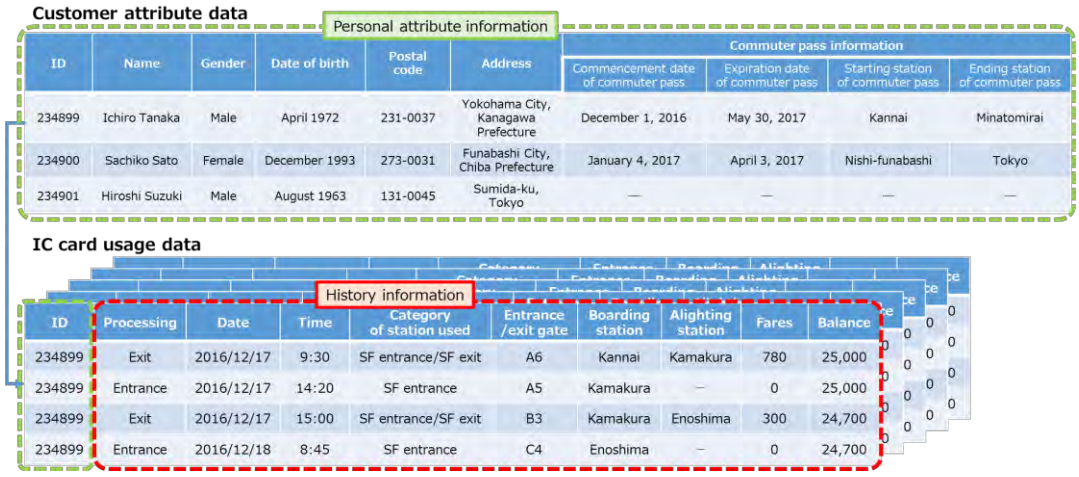
[i] Categories of Information That Can Be Contained

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。

Data shown in Figure 7-12 is categorized into personal attribute information and history information as below.

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

Figure 7-13 Layout of data contained in boarding/alighting history information retained by a railway company



② どのように加工すべきか

[ii] How the Information Should Be Processed

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。

In this use case, the handling of commuter pass information (valid period and area of a commuter pass), boarding and alighting station information, and time information requires extra care.

【個人属性情報】

[Personal attribute information]

＜定期券情報の取扱い＞

<Handling of commuter pass information>

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。

Commuter pass area information (starting station and ending station of a commuter pass) is useful for analyzing the relationship between the commuter pass area and trends concerning movement to a station outside of the commuter pass area (for example, transportation for shopping on holidays). This information is assumed to be used in this use case, too.

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。

Meanwhile, it is possible to determine the stations closest to an individual's home and workplace/school from

commuter pass area information. If the starting station or ending station is a station at which the number of passengers boarding or alighting with a commuter pass is small, commuter pass area information can lead to the identification of an individual. Therefore, it is encouraged to delete such information or replace such information with another station name, etc.

【履歴情報】

[History information]

＜入・出場駅及び時刻情報の取扱い＞

<Handling of boarding/alighting station information and time information>

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。

It is possible to estimate behavioral patterns of a principal (for example, commuting day, working hours, areas to which he/she travels to on weekends) from boarding/alighting station information and time information contained in daily boarding/alighting information.

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。

On the other hand, boarding/alighting information becomes more unique if the period of boarding/alighting history information contained in the dataset is longer. Since such uniqueness itself does not immediately result in the identification of an individual, it is desired to take certain measures.

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。

For example, the number of users per hour at the boarding station and alighting station at the time of use of the IC card should be examined. Then, information concerning stations or hours for which the number of users is small should be deleted. In addition, detailed entrance/exit time information should not contain the minute level information, and should be rounded to, half-hour level or hour level.

＜利用額・残額の取扱い＞

<Handling of fare and balance information>

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。

In this use case, information is assumed to be used for commercial area analysis. Since there is not much need for information concerning the recharging amount on an IC card and value of IC card payment, fare and balance information is to be deleted.

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。
Although it is possible to use fare and balance information for analyzing the status of IC card usage as electronic money, it should be noted that its relationship with the handling of commuter pass area information needs to be kept in mind, since commuter pass area and the existence of records of commuter pass usage can be determined based on a deviation of the value of payment or balance related to each entrance/exit history data.

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。
Policies for the processing of each category of information in this case described above can be summarized as follows.

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

Figure 7-14 Examples of processing for the use case of train boarding/alighting history data

項目 Category	想定されるリスク Potential risks	望ましい加工 Preferred processing
①個人属性情報 [i] Personal attribute information		
ID 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。 Used as internal management IDs to link the customer attribute data and IC card usage data.	全部削除する、あるいは仮IDに置き換える。（項目削除） Delete entirely or replace with temporary IDs (deletion by category).
氏名 Name	単体で個人を特定できる。 This information alone can identify an individual.	全部削除する。 （項目削除） Delete entirely (deletion by category).
性別 Gender	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。 Can result in identification of an individual when combined with address (residence area), date of birth, etc.	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。 In this use case, identifiability is addressed by processing information on date of birth and address. Gender information is not to be processed from the viewpoint of its usefulness.

生年月 Month and year of birth	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。 Can identify an individual when combined with address, gender, etc. Information concerning extremely old age can result in identification of an individual.	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） Replace with six age groups (below 30 years old, 30s, 40s, 50s, 60s, 70 years old and above) (rounding, top-coding).
郵便番号・住所 Postal code/address	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。 Can result in identification of an individual when combined with other information, such as gender and date of birth.	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） Not to be processed, since address information in this use case only contains municipality information. Postal codes are to be deleted, as they are considered as unnecessary (deletion by category).
定期券有効期間（開始日/終了日） Commuter pass valid period (commencement date/expiration date)	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	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） Delete entirely, since this information is considered to be unnecessary for the receiver in this use case (deletion by category).
定期券区間（発駅/着駅） Commuter pass area (starting station/ending station)	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。 Can be used for estimation of the closest	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） Delete information concerning stations which is not often used with a commuter

	stations to home, workplace, etc. Can result in identification of an individual when combined with other information.	pass. Otherwise, replace with another station name (deletion of cells/noise addition).
②履歴情報 [ii] History information		
処理名称　（出場/入場） Processing (exit/entrance)		加工しない。 Not to be processed
利用日時 （年月日・時間） Date and time of use (Date/time)	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。 Risk of identification of an individual when combined with boarding/alighting station information.	30分単位に置き換える。（丸め） Rounded to the half-hour level (rounding).
利用種別 Category of use	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
改札口 Entrance/exit gate	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
入場駅／出場駅 Boarding/alighting station	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。 Can result in identification of an individual, when combined with boarding/alighting station information, or due to hours of use.	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） Delete information for boarding/alighting stations for hours in which the number of users is small. Otherwise, replace with another station name (deletion of cells/noise addition).
利用額 Value of payment	定期券区間に関する情報を復元することができる。	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

	（提供先にとって不要な情報と想定） Can restore information concerning commuter pass area. (Considered to be unnecessary information for the receiver.)	る。（項目削除） Delete entirely, since this information is considered to be unnecessary for the receiver in this use case (deletion by category).
残額 Balance	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） Can restore information concerning commuter pass area. (Considered to be unnecessary information for the receiver.)	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） Delete entirely, since this information is considered to be unnecessary in this use case (deletion by category).

③ 加工後のデータのイメージ

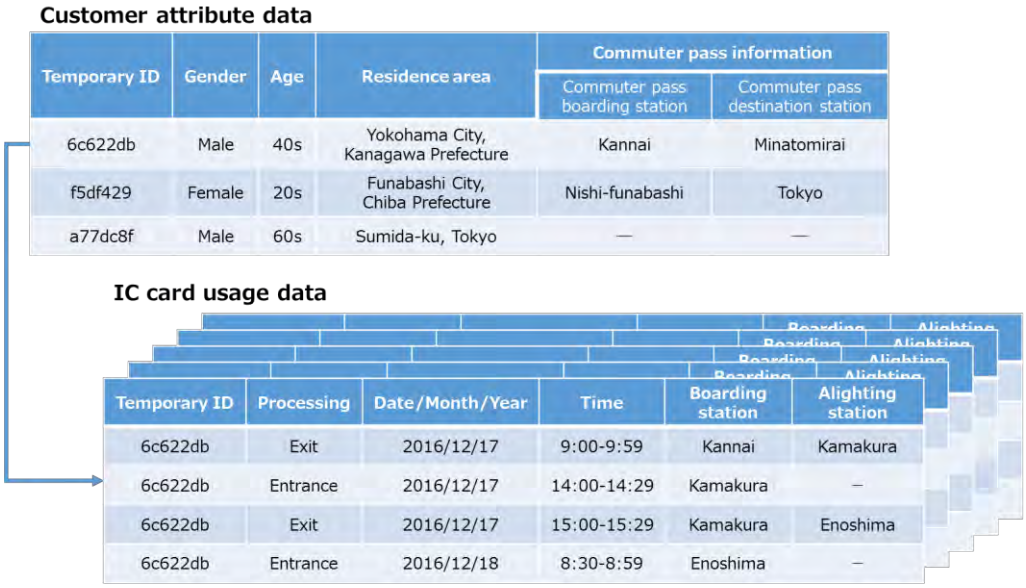
[iii] Processed Data

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。

Figure 7-15 shows data that has been processed based on the above approach.

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

Figure 7-15 Processed data in the use case of train boarding/alighting history data



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。

In the above use case, information is used for analyzing the movement of people based on train boarding/alighting history information. Other than that, there can be also a need for using such information for detailed analysis of the number of users at multiple entrance/exit gates at a particular station. Although more detailed time information is preferred in such a case, a set of boarding/alighting history information that indicates stations at which passengers got on and off the train is not always necessary. One of the ways to deal with such need is to leave detailed time information, and to replace entrance/exit history information at one of the stations, which is not the subject of analysis, with information on train lines used.

7.2.2 移動履歴の事例

7.2.2 Examples of Movement History Information

１）ユースケース

1) Use Case

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。

In this use case, an automobile company anonymizes movement history information that it retains, and provides processed information to another business operator (retailer), by utilizing the framework of anonymously processed information. Said another business operator can utilize automobiles' movement history information and basic attribute information (age, gender, etc.) concerning automobile owners for examining the product lineup at stores and developing new store establishment plans.

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

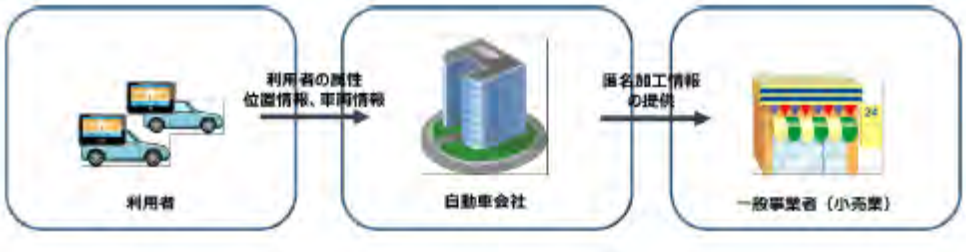
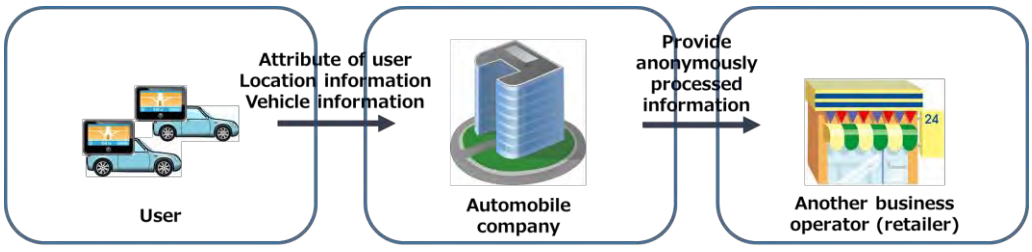


Figure 7-16 Use case where an automobile company provides movement history information it retains to a third party



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。

In this use case, the dataset that is subject to processing is comprised of two types of data: [i] customer attribute data; and [ii] probe data. These two kinds of data are mutually linked by IDs.

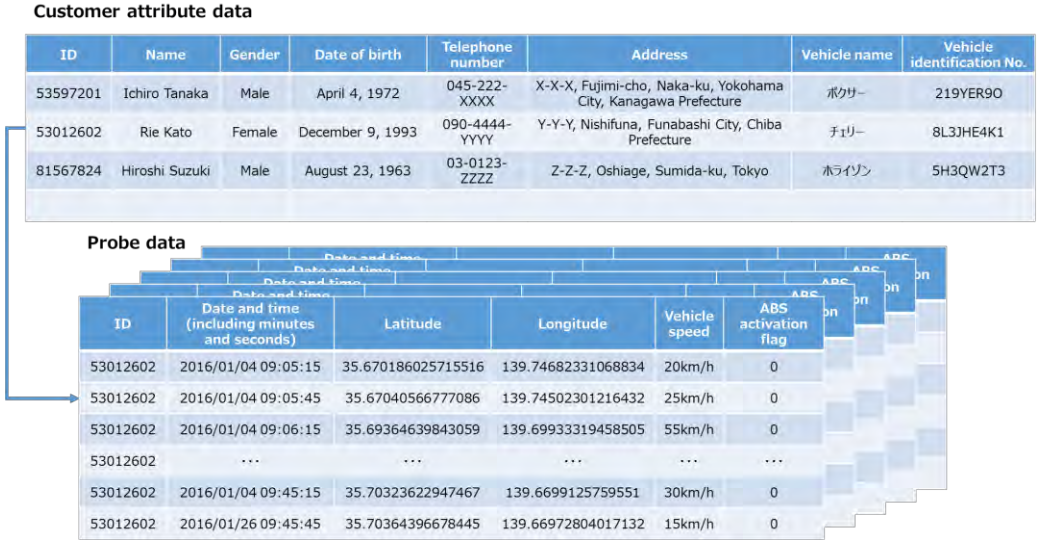
顧客属性データには、顧客の基本属性のほか、車種名と車両識別番号が含まれている。一方、プローブデータは、各車両の車載通信機により定期的に自動車メーカーのデータセンターに送信されて蓄積され

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。

The customer attribute data contains customers' basic attribute information, vehicle name, and vehicle identification number. On the other hand, the probe data is comprised of date and time information, location information (latitude and longitude), and vehicle information: namely vehicle speed and ABS[39] activation flag, which are obtained be in-vehicle communication device and sent regularly to the datacenter of the automobile manufacturer.

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

Figure 7-17 Sample layout of data contained in movement history information retained by an automobile company



[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

Figure 7-18 Movement history indicated by the probe data (latitude/longitude information)

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

2) Examination of Specific Processing Methods That Accommodate Matters and Risks That Need to Be Considered

① 含まれ得る情報の種類

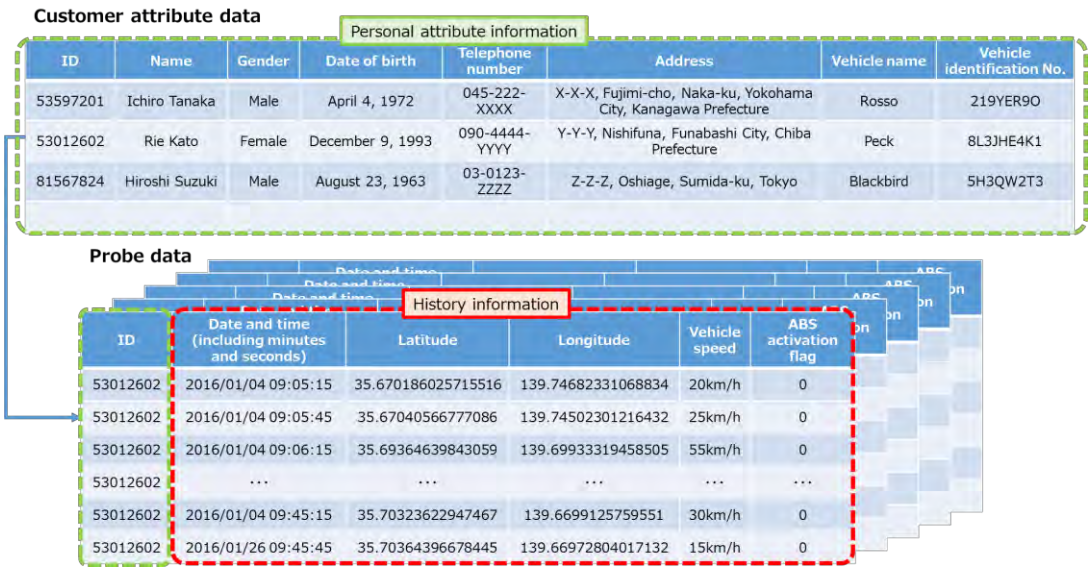
[i] Categories of Information That Can Be Contained

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。

Data shown in Figure 7-17 is categorized into personal attribute information and history information as below.

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

Figure 7-19 Sample layout of data contained in movement history information retained by an automobile company



② どのように加工すべきか

[ii] How the Information Should Be Processed

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。

In this use case, the handling of vehicle name information contained in the personal attribute information and location information (latitude/longitude information) contained in the history information requires extra care.

【個人属性情報】

[Personal attribute information]

＜車種情報の取扱い＞

<Handling of vehicle name information>

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。

The vehicle name information is useful in analyzing the styles of vehicle use. Meanwhile, such information can result in the identification of an individual when combined with other information, such as address (residence area). Therefore, it is encouraged to delete specific vehicle names and generalize to vehicle categories.

＜車両識別番号＞

<Vehicle identification number>

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。

A unique vehicle identification number is assigned to each vehicle for the purpose of identification. Although such information does not immediately result in the identification of an individual, it is possible that such information can lead to such an incident. Since in this use case such information is not useful for the receiver, it should be entirely deleted in order to avoid the risks of unintended re-identification.

【履歴情報】

[History information]

＜位置情報の取扱い＞

<Handling of location information>

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。

Consecutive data of location information linked with detailed time information allows for the estimation of the transportation route from one location to another. In addition, location information during the night, which is fixed at the same location for a while, indicates the location of home, while location information during the day, which is fixed at the same location for a while, indicates the location of workplace and/or school, etc.

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。

Therefore, a part of location information that can identify the location of home and/or workplace should be deleted from a dataset containing consecutive location information as described above. The following methods can be used to delete such location information.

・ 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。

・Delete location information in a certain scope, based on the home address.

・ 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。

・Delete information concerning a certain distance or time from movement history (from switching on to switching off of car ignition) from the starting point to the ending point.

・ 各移動履歴の始点・終点から数%の位置情報を削除する。

・Delete a certain percentage of location information from movement history from the starting point to the ending point.

＜車速情報の取扱い＞

<Handling of vehicle speed information>

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。

Vehicle speed information allows for the analysis of the road traffic situation. Traffic information is useful in developing retail store establishment plans. On the other hand, vehicle speed information can result in the restoration of deleted location information, since travel distance can be calculated when vehicle speed information is combined with time information. Therefore, vehicle speed information corresponding to the deleted location information needs to be deleted.

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。

Since in this use case detailed vehicle speed information is unnecessary for the receiver, it is advisable to be rounded to 10km intervals. In addition, it is also advisable that vehicle speed data of 50 km/h or more should be top-coded.

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。

Since this use case assumes that information is to be used for examining the product lineup at the business operator that receives the processed information and developing store establishment plans, etc., ABS activation information by road category is considered to be unnecessary. Therefore, it is also advisable for the ABS activation flag to be entirely deleted.

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。

Policies for the processing of each category of information in this case described above can be summarized as follows.

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

Figure 7-20 Examples of processing for the use case of vehicle movement history data

項目 **Category**	想定されるリスク **Potential risks**	望ましい加工 **Preferred processing**
①個人属性情報 [i] Personal attribute information		
ID 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。 Used as a code linking customer attribute data with movement history data.	全部削除する、あるいは仮IDに置き換える。（項目削除） Delete entirely or replace with temporary IDs (deletion by category).
氏名 Name	単体で個人を特定できる。 This information alone can identify an individual.	全部削除する。（項目削除） Delete entirely (deletion by category).
性別 Gender	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。 Can result in identification of an individual when combined with date of birth and address.	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。 In this use case, identifiability is addressed by processing information on date of birth and address. Gender information is not to be processed from the viewpoint of its usefulness.
生年月日 Date of birth	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。 Can result in identification of an individual when combined with address and gender.	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） Replace with six age groups (below 30 years old, 30s, 40s, 50s, 60s, 70 years old and above) (rounding, top-coding).
住所 Address	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） Delete information on municipalities and more detailed address information (rounding).

	Can result in identification of an individual when combined with date of birth and gender. Entails a risk of allowing access to a principal.	
車種 Vehicle name	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。 Can result in identification of an individual when combined with address and date of birth, etc.	「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） Replace with vehicle categories, such as "high-end car" and "compact car" (generalization).
車両識別番号 Vehicle identification number	（提供先にとって不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
②履歴情報 [ii] History information		
日時分秒 Date and time (including minutes and seconds)	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。 Combination of detailed time information and location information can result in identification of an individual.	秒を削除し、分単位に置き換える。（丸め） Delete second data and replace with minute data (rounding).
緯度・経度 Latitude/longitude	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。 Location of home, workplace, etc. can be identified based on location information during the night and day.	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） Delete latitude/longitude information concerning a certain distance from the location at which the vehicle stays for a certain period of time or longer. Otherwise, delete the latitude/longitude information for several minutes from the starting of running

		and for several minutes before the end of running.
道路種別 Road category	（提供先において不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).
車速 Vehicle speed	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。 Can restore deleted location information when combined with time information.	・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） ・Delete vehicle speed information in hours for which latitude/longitude information is deleted (deletion of cells). ・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） ・Replace with six vehicle speed ranges (below 10 km/h, 10km/h, 20km/h, 30km/h, 40km/h, 50km/h and above) (rounding).
ABS作動フラグ ABS activation flag	（提供先において不要な情報と想定） (Considered to be unnecessary information for the receiver.)	全部削除する。（項目削除） Delete entirely (deletion by category).

③ 加工後のデータのイメージ

[iii] Processed Data

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。

Figure 7-21 shows data that has been processed based on the above approach.

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

Figure 7-21 Processed data in the use case of vehicle movement history data

Customer attribute data

Temporary ID	Gender	Age	Vehicle type	Residence area
3e7ba68	Male	40s	Minivan	Yokohama City, Kanagawa Prefecture
10d393f8	Female	30s	Compact	Funabashi City, Chiba Prefecture
d416e64	Male	60s	Sedan	Sumida-ku, Tokyo
…	…	…	…	…

Probe data

Temporary ID	Date and time	Latitude	Longitude	Vehicle speed
10d393f8	2016/01/04/09	35.69364639843059	139.69933319458505	50km/h and above
10d393f8	2016/01/04/09	35.69467805968198	139.69868087166105	40km/h
10d393f8	2016/01/04/09	35.69782872486885	139.69727325020358	50km/h and above
10d393f8	…	…	…	…
10d393f8	2017/01/26/09	35.69746626454594	139.6710433899716	40km/h
10d393f8	2017/01/26/09	35.70244296802019	139.67199611244723	30km/h
10d393f8	2017/01/26/09	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）

Figure 7-22 Movement history indicated by the probe data (latitude/longitude information) (after processing)

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。

In the above use case, information is intended to be used for the development of retail store establishment plans and analysis of product lineup based on vehicle movement history information and basic attribute information of car owners. Said information can be also used for the examination of traffic accident reduction measures by local governments, as well as the examination of new insurance plans by insurance companies, through analysis of general trends in driving situation and surrounding situation.

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。

While such cases would require detailed information on vehicle speed, ABS activation and road category, the travel distance can become longer and location information may be unnecessary for certain areas. Therefore, policies for processing would be different from the above for such cases.

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。

This use case discussed the handling of vehicle movement history information. When handling movement history information of people obtained through smartphone apps, etc., consideration needs to be given to the difference in the movement and speed of transportation.

7.3 電力利用履歴の事例

7.3 Examples of Power Consumption History Information

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。

The Energy Basic Plan[41], which was approved by the Cabinet in April 2014, sets the goal of introducing a smart meters to every household in Japan by the early 2020s. It is expected that household power consumption history data will be obtained and accumulated by electricity companies, aggregators, HEMS servicers,[42] etc. through smart meters and networked distribution boards, etc.

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。

Such power consumption data is expected to be used for various purposes, including provision of specific advice on energy saving based on the power consumption pattern, monitoring of children and elderly people living alone, and marketing based on the estimation of life situation.[43] The following are examples of possible use cases where electricity companies, etc. produce anonymously processed information for use for a purpose other than the original purpose and provide it to a third party.

１）ユースケース

1) Use Case

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。

In this use case, a HEMS management business operator anonymizes power consumption information, and provides the processed information to another business operator, such as an electronics manufacturer, by utilizing the framework of anonymously processed information. Said another business operator can analyze life styles based

---

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

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

[42] Home Energy Management System.
Home Energy Management System.

[43] 経産省マニュアル P.15。
METI Manual, P.15

on the family structure and use status of home appliances and use the results for new product development and advertisement strategy for existing products.

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

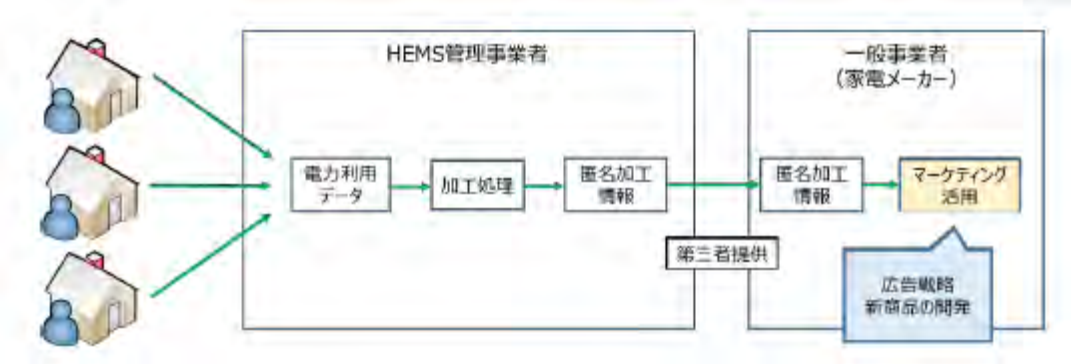
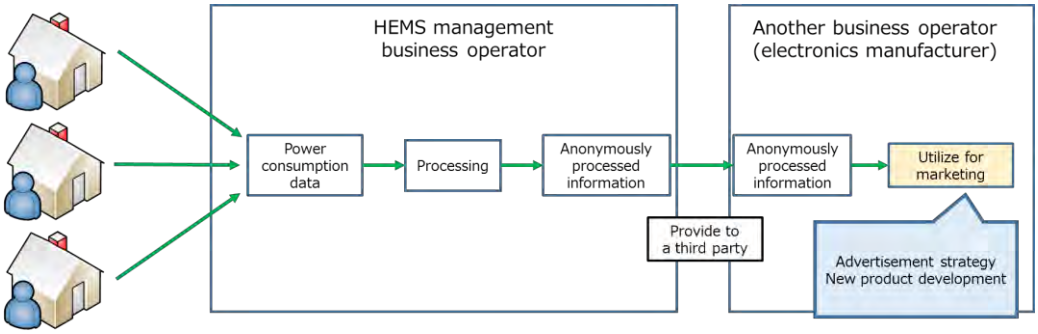


Figure 7-23 Use case where a HEMS management business operator provides power consumption history information it retains to a third party

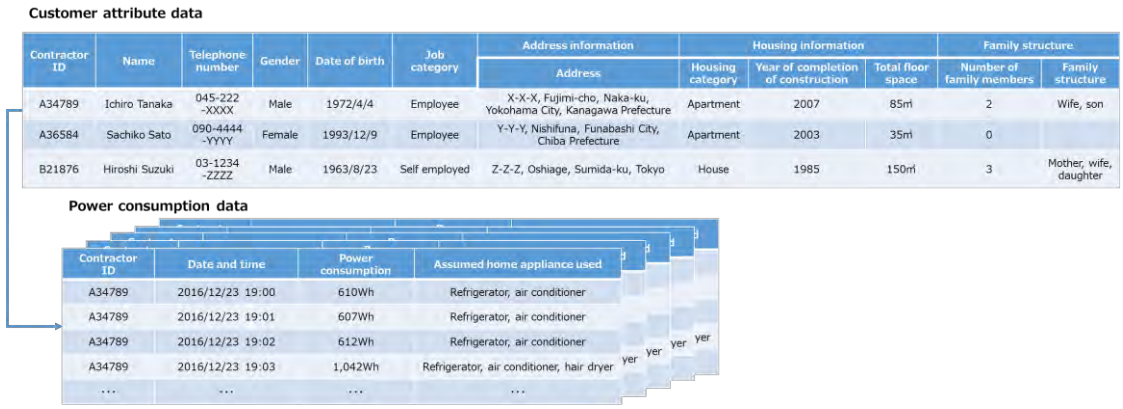


本ユースケースにおいて加工対象となるデータセットは、①顧客属性データ及び②電力利用データの２種類からなり、いずれも契約者IDによってリンクされている。電力利用データのうち、推定使用家電については、各家庭の配電盤に設置されるエネルギー計測ユニットで計測される電流量の変化に基づいて、稼働中の家電の種類を推定している。

In this use case, the dataset that is subject to processing is comprised of two types of date: [i] customer attribute data; and [ii] power consumption data. These two kinds of data are mutually linked by subscriber IDs. Among power consumption data, assumed home appliance used refers to a kind of home appliance being used, which is assumed based on changes in the amount of current measured by an energy measurement unit installed in the distribution board at each household.

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

Figure 7-24 Layout of data contained in power consumption history information retained by a HEMS management business operator



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

2) Examination of Specific Processing Methods That Accommodate Matters and Risks That Need to Be Considered

① 含まれ得る情報の種類

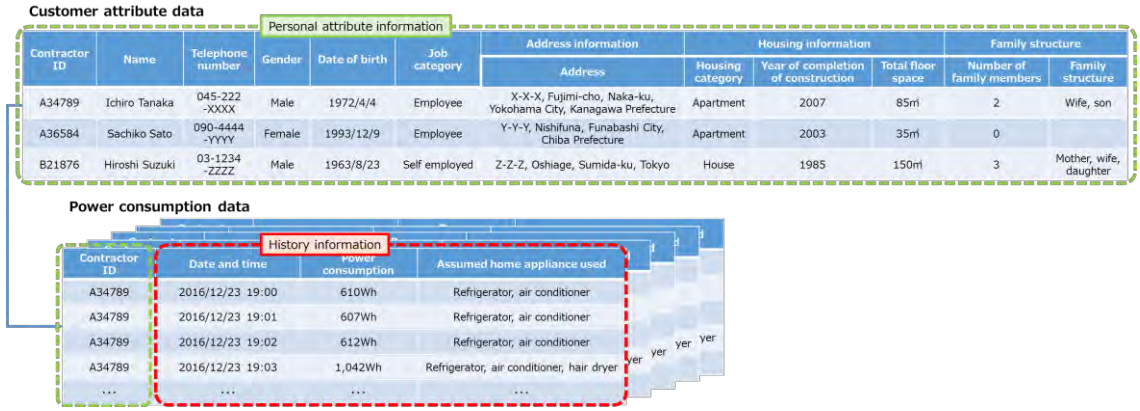
[i] Categories of Information That Can Be Contained

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。

Data shown in Figure 7-24 is categorized into personal attribute information and history information as described in Figure 7-25.

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

Figure 7-25 Sample layout of data contained in power consumption history information retained by a HEMS management business operator



② どのように加工すべきか

[ii] How the Information Should Be Processed

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。

In this use case, the original customer attribute data contains housing information and family information. In addition, the history information allows for the determination of detailed power consumption data and asumption of home appliance being used based on changes in power consumption. Such information not only may result in the identification of an individual, but also entails a risk that information related to privacy, such as life patterns, can be estimated based on such information. Information should be processed with these issues in mind.

【個人属性情報】

[Personal attribute information]

＜住居情報の取扱い＞

<Handling of housing information>

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。

The housing information in this use case is comprised of housing category (house/apartment), year of completion of construction, and total floor space. Some housing information services, etc. provide such information concerning rental properties and condominium apartments on the Internet. Therefore, since such information can be readily accessed by the public and can result in the identification of a specific individual, the information needs to be partially deleted or rounded. In particular, year of completion of construction and floor space should be rounded, as the combination of these two types of information entails a high identification risk.

＜家族情報の取扱い＞

<Handling of family information>

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。

The family information is comprised of the number of family members and family structure. The data held by the HEMS management business operator contains information on the basic attribute information of the residents (representatives), address and housing information. The combination of these types of information and family information can lead to the identification of an individual.

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。

Therefore, the processing of family information should be considered, such as replacement with brackets, taking into account the level of processing of basic attribute information, address and housing information.

【履歴情報】

[History information]

＜電力利用量の取扱い＞

<Handling of power consumption information>

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。

It is possible to estimate family structure and life patterns, such as waking time and bed time and presence and absence at home, based on changes in power consumption. Although the results of such estimation do not immediately result in the identification of a specific individual, information that contain particularly outstanding changes in power consumption (such as waking time and bed time being idiosyncratic when compared with other people contained in the dataset) should be processed. Possible processing methods include deletion of records and deletion of data in the part where outstanding difference is observed.

＜推定使用家電＞

<Assumed home appliance used>

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。

In addition to power consumption data, use status of each home appliance used is assumed based on the current waveform in this use case. While it is considered to be difficult to identify a specific individual based on the use status of home appliances, outstanding difference from other people in relation to power consumption and use status of home appliances may result in the identification of an individual due to the idiosyncrasy of life style, etc. that can be assumed based on such information. In such case, it is advisable to delete such information itself.

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。

Policies for the processing of each category of information in this case described above can be summarized as follows.

図表7-26 電力利用履歴のユースケースにおける加工例

Figure 7-26 Examples of processing for the use case of power consumption history information

項目 **Category**	想定されるリスク **Potential risks**	望ましい加工 **Preferred processing**
①個人属性情報 [i] Personal attribute information		
契約者ID Contractor 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	全部削除する、あるいは仮IDに置き換える。（項目削除） Delete entirely or replace with

	ある。 Functions as IDs for internal distributed management and can result in identification of an individual.	temporary IDs (deletion by category).
氏名 Name	単体で個人を特定できる。 This information alone can identify an individual.	全部削除する。 （項目削除） Delete entirely (deletion by category).
電話番号 Telephone number	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。 This information is closely related to the principal and is likely to have been collected by other business operators, as well.	全部削除する。 （項目削除） Delete entirely (deletion by category).
性別 Gender	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。 Can result in identification of an individual when combined with address (residence area), date of birth, etc.	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。 In this use case, identifiability is addressed by processing information on date of birth and address. Gender information is not to be processed from the viewpoint of its usefulness.
生年月日 Date of birth	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。 Can result in identification of an	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） Replace with six age groups (below 30 years old, 30s, 40s, 50s, 60s, 70 years old and above) (rounding,

	individual when combined with address, gender, etc. Information concerning extremely old age can result in identification of an individual.	top-coding).
職種 Job category	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。 Rare job categories may result in identification of an individual when combined with other information, including address.	少ない職種については、「その他」等に置き換える。（丸め） Replace rare job categories with such descriptions as "others" (rounding).
住所 Address	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。 Entails a risk of identification when combined with date of birth and gender. Entails a risk of allowing access to a principal.	市区単位より細かい情報を削除する。（丸め） Delete information on municipalities and more detailed address information (rounding).
住居（竣工年） Housing (year of completion of construction)	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。 Address can be identified when combined with residence area and floor area.	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） Convert to age of housing and replace with five ranges (below 5 years, 5-10 years, 10-15 years, 15-20 years, 20 years and above) (rounding).
住居（床面積） Housing (floor space)	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。 Can result in identification of	4区分（20㎡未満/20～40㎡/40～80㎡/80㎡以上）に置き換える。（丸め） Replace with four ranges (smaller

	address when combined with residence area and age of the housing.	than 20 m^2, 20-40 m^2, 40-80 m^2, 80 m^2 and above).
家族人数 Number of family members	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。 Information on families whose number of members is large may increase the risk of identification of an individual.	4区分（1人/2人/3人/4人以上）に置き換える。（丸め） Replaced with four groups (one/two/three/four or more) (rounding).
家族構成 Family structure	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。 Can result in identification of an individual when combined with other information, such as number of family members and address.	4区分（独居、夫婦のみ、親子、その他）に置き換える。（丸め） Replace with four groups (living alone, couple only, parents and children, others) (rounding).
②履歴情報 [ii] History information		
日時 Date and time	—	本ケースでは加工しない。 Not to be processed in this case
電力利用量 Power consumption	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。 Combination of idiosyncratic power consumption and other information can result in identification of an individual.	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） Delete information on extremely large power consumption (deletion of records/deletion of cells).
推定使用家電 Assumed home appliance used	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。 Can result in identification of an individual, if an idiosyncratic life	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） Delete information that is remarkably different from others (deletion of records).

style, etc. can be determined from the combination of this information and power consumption information.

③ 加工後のデータのイメージ

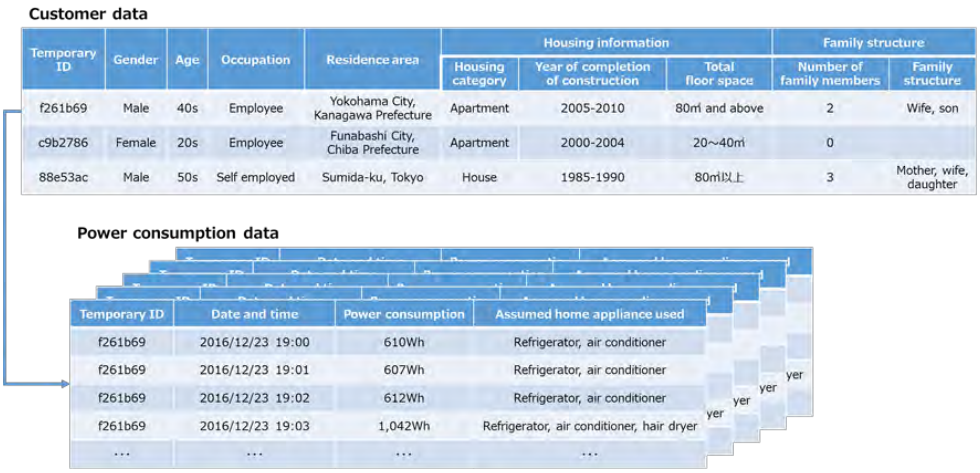
[iii] Processed Data

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。

Figure 7-27 shows data that has been processed based on the above approach.

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

Figure 7-27 Processed data in the use case of power consumption history information



おわりに

Conclusion

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。

Various data that can be used as useful big data is being accumulated in many fields in the private sector. Among such data, those which have been linked and accumulated as personal data in combination with customer information, etc. are highly reliable, accurate and useful. On the other hand, such information is often deemed as personal information by the private sector (personal information handling business operators) from the legal perspective. As business operators refrain from providing information to a third party from a legal perspective and avoid privacy-related risks for their customers, approaches for desired information utilization are not shared, which adds to the issue of "barriers to utilization."

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。

Accredited organizations have promoted the development of personal information protection policies and business operators' voluntary efforts based on these policies. It is hoped that they will include production methods for anonymously processed information in said policies, in accordance with the Act after the amendment.

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。

This Report was compiled with such awareness as stated above. It is intended to help accredited organizations, trade associations, etc. shaping provisions concerning production methods for anonymously processed information as they formulate policies and industries' voluntary rules, etc. This Report is also intended to provide reference for business operators that they can directly refer to when the produce anonymously processed information.

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。
In addition to personal information protection policies and industry's voluntary standards, etc., it would be also useful if accredited organizations, trade associations, etc. could collect and communicate good examples that specifically show types of information that need to be processed and proper processing methods for these types of information, while publishing and sharing best practices of efforts at accredited organizations and trade associations across industries. It is hoped that such efforts will be promoted under collaboration among relevant entities.

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。
The anonymously processed information system aims to provide useful personal data in the private sector to a third party and to allow for the utilization of such data for a purpose other than the original purpose. As relevant entities cooperate with each other in promoting their efforts and use of this system is promoted broadly in the private sector in an appropriate manner, it is hoped that the safe distribution of personal data is promoted and new technologies and services are created, while maintaining the confidence of consumers and service users.

【参考資料】

[Reference]

I. 匿名加工情報に関連する法令の規定

I. Provisions of Laws Related to Anonymously Processed Information

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）

I-1 Act on the Protection of Personal Information (Act No. 57 of 2003; as of the time when the Amendment Act fully entered into force) (excerpt)

（定義）

(Definition)

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。

Article 2 (1) "Personal information" in this Act means that information relating to a living individual which falls under any of each following item:

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。）

(i) those containing a name, date of birth, or other descriptions etc. (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other forms that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph, item (ii)); the same shall apply in Article 18, paragraph (2)); hereinafter the same) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual)

二 個人識別符号が含まれるもの

(ii) those containing an individual identification code

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。

(2) An "individual identification code" in this Act means those prescribed by cabinet order which are any character, letter, number, symbol or other codes falling under any of each following item.

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

(i) those able to identify a specific individual that are a character, letter, number, symbol or other codes into

which a bodily partial feature of the specific individual has been converted in order to be provided for use by computers

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

(ii) those character, letter, number, symbol or other codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or, stated or recoded for the said user or purchaser, or recipient of issuance

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。

(5) A "personal information handling business operator" in this Act means a person providing a personal information database etc. for use in business; however, excluding a person set forth in the following;

一 国の機関

(i) a central government organization;

二 地方公共団体

(ii) a local government;

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。）

(iii) an incorporated administrative agency etc. (meaning an independent administrative agency etc. prescribed in Article 2, paragraph (1) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003); hereinafter the same);

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。）

(iv) a local incorporated administrative agency (meaning a local incorporated administrative agency prescribed in Article 2, paragraph (1) of the Local Incorporated Administrative Agencies Act (Act No. 118 of 2003); hereinafter the same);

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。

(8) A "principal" in relation to personal information in this Act means a specific individual identifiable by personal information.

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。

(9)　"Anonymously processed information" in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

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。）。

(i)　personal information falling under paragraph (1), item (i); Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

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。）。

(ii)　personal information falling under paragraph (1), item (ii); Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes)

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。

(10)　An "anonymously processed information handling business operator" in this Act means a person who provides for use in business a collective body of information comprising anonymously processed information which has been systematically organized so as to be able to search using a computer for specific anonymously processed information or similar others prescribed by cabinet order as systematically organized so as to be able to search easily for specific anonymously processed information (referred to as an "anonymously processed information database etc." in Article 36, paragraph (1)). However, a person set forth in each item of paragraph (5) is excluded.

（匿名加工情報の作成等）

(Production etc. of Anonymously Processed Information)

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。

Article 36　(1)　A personal information handling business operator shall, when producing anonymously processed information (limited to those constituting anonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production.

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。

(2)　A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of information relating to those descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

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。

(3)　A personal information handling business operator, when having produced anonymously processed information, shall, pursuant to rules of the Personal Information Protection Commission, disclose to the public the categories of information relating to an individual contained in the anonymously processed information.

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。

(4)　A personal information handling business operator, when having produced anonymously processed information and providing the anonymously processed information to a third party, shall, pursuant to rules of the Personal Information Protection Commission, in advance disclose to the public the categories of information concerning an individual contained in anonymously processed information to be provided to a third party and its providing method, and state to the third party explicitly to the effect that the information being provided is anonymously processed information.

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。

(5)　A personal information handling business operator shall, when having produced anonymously processed

information and making itself handle the anonymously processed information, not collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the said anonymously processed information.

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。

(6)　A personal information handling business operator shall, when having produced anonymously processed information, strive to take itself necessary and appropriate action for the security control of the anonymously processed information and necessary action for ensuring the proper handling of the anonymously processed information such as dealing with a complaint about the handling, including producing, of the said anonymously processed information, and strive to disclose to the public the contents of such action taken.

（匿名加工情報の提供）

(Provision of Anonymously Processed Information)

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。

Article 37　An anonymously processed information handling business operator, when providing anonymously processed information (excluding those which it produced itself by processing personal information; hereinafter the same in this Section) to a third party, shall, pursuant to rules of the Personal Information Protection Commission, in advance disclose to the public the categories of personal information contained in anonymously processed information to be provided to a third party and state to the third party explicitly to the effect that the provided information is anonymously processed information.

（識別行為の禁止）

(Prohibition against the Act of Identifying)

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。

Article 38　An anonymously processed information handling business operator, shall, in handling anonymously processed information, neither acquire information relating to those descriptions etc. or individual identification

codes deleted from the personal information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1), nor collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the anonymously processed information.

（安全管理措置等）

(Security Control Action etc.)

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。

Article 39　An anonymously processed information handling business operator shall strive to take itself necessary and appropriate action for the security control of anonymously processed information and necessary action to ensure the proper handling of anonymously processed information such as dealing with a complaint about the handling of anonymously processed information, and shall strive to disclose to the public the contents of such action taken.

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）

I-2 Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; as of the time when the Amendment Act fully entered into force) (excerpt)

（匿名加工情報データベース等）

(Anonymously Processed Information Database etc.)

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。

Article 6　Those prescribed by cabinet order under Article 2, paragraph (10) of the Act mean a collective body of information including a table of contents, index or similar others to facilitate search of information that has been systemically organized by arranging anonymously processed information contained in the database etc. according to a certain rule that enables specified anonymously processed information to be readily searched for.

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）

I-3 Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of 2016) (excerpt)

（匿名加工情報の作成の方法に関する基準）

(Standards in the methods of producing anonymously processed information)

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。

Article 19　Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (1) of the Act shall be as follows.

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。）。

(i)　deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the whole or part of descriptions etc.)

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。）。

(ii)　deleting all individual identification codes contained in personal information (including replacing such codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes)

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。）。

(iii)　deleting those codes (limited to those codes linking mutually plural information being actually handled by a personal information handling business operator) which link personal information and information obtained by having taken measures against the personal information (including replacing the said codes with those other codes which cannot link the said personal information and information obtained by having taken measures against the said personal information using a method with no regularity that can restore the said codes)

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。）。

(iv)　deleting idiosyncratic descriptions etc. (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the idiosyncratic descriptions etc.)

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。

(v)　besides action set forth in each preceding item, taking appropriate action based on the results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information

（加工方法等情報に係る安全管理措置の基準）

(Standards in the security control action concerning processing method etc. related information)

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。

Article 20　Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (2) of the Act shall be as follows.

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。

(i)　defining clearly the authority and responsibility of a person handling anonymously processed information (information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1) (limited to those which can restore the personal information by use of such relating information); the same applies hereinafter in this Article).

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。

(ii)　establishing rules and procedures on the handling of processing method etc. related information, handling appropriately processing method etc. related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement

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。

(iii)　taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc. related information from handling the processing method etc. related information

（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）

(Public disclosure by a personal information handling business operator when producing anonymously processed information)

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。

Article 21　(1)　Public disclosure pursuant to the provisions of Article 36, paragraph (3) of the Act shall, without delay after anonymously processed information has been produced, be made by utilizing the Internet or other appropriate method.

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。

(2)　In cases where a personal information handling business operator entrusted by another personal information handling business operator has produced anonymously processed information, the said other personal information handling business operator shall disclose the categories of information relating to an individual contained in the anonymously processed information by a method prescribed in the preceding paragraph. In such cases, it shall be deemed that the public disclosure of the said categories has been made by the said entrusted personal information handling business operator.

（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）

(Public Disclosure etc. by a personal information handling business operator when providing anonymously processed information to a third party)

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。

Article 22　(1)　Public disclosure pursuant to the provisions of Article 36, paragraph (4) of the Act shall be made by utilizing the Internet or other appropriate method.

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。

(2)　An explicit statement pursuant to the provisions of Article 36, paragraph (4) of the Act shall be given by sending an e-mail, delivering a written document or employing other appropriate method.

（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）

(Public Disclosure etc. by an Anonymously Processed Information Handling Business Operator when Providing Anonymously Processed Information to a Third Party)

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。

Article 23　(1)　The provisions of the preceding Article, paragraph (1) shall apply mutatis mutandis to public disclosure pursuant to the provisions of Article 37 of the Act.

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。

(2)　The provisions of the preceding Article, paragraph (2) shall apply mutatis mutandis to an explicit statement pursuant to the provisions of Article 37 of the Act.

II. パーソナルデータの匿名加工を巡る海外の動向

II. Trends Concerning the Anonymization of Personal Data Overseas

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。

Below, reports, etc. from other countries, which focus on anonymization[44] among other trends concerning legislation and discussions regarding personal data and privacy.

II-1 米国における動向

II-1 Trends in the United States

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。

The Unites States does not have any comprehensive law on personal data. Instead, laws regulating the handling of personal data are provided for each field. Such field-specific laws include HIPPA[45] and COPPA.[46]

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。

The FTC,[47] which monitors and supervises unfair and deceptive acts and practices in commercial activities, issued a report on personal data anonymization titled "Protecting Consumer Privacy in an Era of Rapid Change"[48] (FTC Staff Report) in 2012. This report refers to the "de-identification" of personal information. In addition, the NIST[49] also issued a report on anonymization of personal data titled "De-identification of Personal Information"[50] (NIST

---

44 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。
Some of the reports, etc. appearing in Chapter II use the term "anonymization" and others use the term "de-identification." In this report, the term that is used in the relevant report is used.

45 Health Insurance Portability and Accountability Act.
Health Insurance Portability and Accountability Act.

46 Children's Online Privacy Protection Rule.
Children's Online Privacy Protection Rule.

47 Federal Trade Commission.
Federal Trade Commission.

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

49 National Institute of Standards and Technologies.
National Institute of Standards and Technologies.

50 http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf
http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

Report) in October 2015.
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。
In addition, guidelines that focus on the medical field as stated above were issued under the title of " Guidance Regarding Methods of De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act."[51]

II-1-1 FTC スタッフレポート (2012 年 3 月)

II-1-1 FTC Staff Report (March 2012)

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。
The FTC Staff Report encourages business operators to act in accordance with the practices shown in the report, and provides recommendations for the formulation of privacy policies, from the three perspectives of [i] privacy by design, [ii] simplification of consumer choice, and [iii] transparency of data practices.
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。
The framework proposed in the report covers data that can be reasonably linked to a specific consumer. If a business operator has taken the following three measures, the data is deemed as data that "cannot be reasonably linked to" a specific consumer and thus does not fall under the scope of the framework.
[i] To carry out de-identification in a reasonable manner
[ii] To publicly commit to refraining from re-identifying de-identified data
[iii] When providing de-identified data to a third party, to prohibit the act of re-identification by said third party under a contract
The above are also called FTC's three requirements.
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条で禁止され

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

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。

If a business operator has violated the second requirement, the FTC can seek injunction against said violating act and claim civil fines as such violating act constitutes an "unfair or deceptive act" prohibited under Section 5 of the Federal Trade Commission Act.

II-1-2 NIST レポート（2015 年 10 月）

II-1-2 NIST Report (October 2015)

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。

The NIST Report provides an overview of terms and issues to be considered in relation to the de-identification of personal information for government organizations, advocacy groups, researchers, etc. Specifically, it explains data sharing models, approaches for de-identification and major de-identification methods, evaluation of field-based de-identification, estimation of re-identification risk, etc. However, the NIST Report also clearly states that it does not make recommendations regarding the appropriateness of de-identification or specific de-identification algorithms.

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。

The report states that de-identification should be carried out by processing direct identifiers and quasi-identifiers in personal data in the following manner.

（１） 直接識別子

(1) Direct identifiers

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。

Direct identifiers include names, social security numbers, and email addresses. Direct identifiers need to be removed or replaced with random values, etc.

（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）

(2) Quasi-identifiers (in an example of an article by Sweeney, date of birth, telephone number, and sex fall under the category of quasi-identifiers)

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。

Since quasi-identifiers are important for analyses that are to be performed later and they also affect the usefulness of a dataset, the report states that the processing of quasi-identifiers should be carried out with careful consideration to balance the risk of re-identification with the utility gained by their inclusion. Processing methods for quasi-identifiers include suppression, generalization, perturbation, swapping, sub-sampling. The report also covers 11 de-identification steps proposed by Emam and Malin.

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。

Subsequently, the first draft of "De-Identifying Government Datasets" (NIST SP800-188) was issued in August 2016, and the second draft was issued in December 2016. As expressed in the title, this document provides guidelines for de-identification of personal data held by the Federal Government. Based on the NIST Report, this document provides more specific approaches to the governance and management of de-identification (determination of goals, estimation of risks, education, etc.) and technical steps for de-identification.

II-1-3 HIPAA ガイドライン（2012 年 11 月）

II-1-3 HIPAA Guidelines (November 2012)

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。

For entities covered by the HIPAA (health care providers, health care clearinghouses, health plans) these Guidelines explain how they can fulfill the de-identification requirements for health information, which are prescribed the HIPAA Privacy Rules, in the form of Q&A.

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。

The HIPAA Privacy Rules clearly provides that de-identified data becomes outside of the scope of legal regulation. The following two items are listed as standards for de-identification.

（１） 専門家による判定（Expert Determination）

(1) 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

A person with knowledge of statistical and scientific principles and methods for rendering information not individually identifiable submits a document to the effect that he/she determined that the re-identification risk is very small.

（２） セーフハーバー（Safe Harbor）

(2) 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

18 identifiers, including names, geographic subdivisions, and telephone numbers are removed and the covered entity does not have actual knowledge to identify an individual.

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。

The HIPAA Guidelines consist of three parts. Following explanation on provisions of the HIPAA Privacy Rules related to de-identification, Q&A are given for individual de-identification criteria (expert determination and safe harbor). Q&A concerning expert determination is explained with illustrations of identification risk estimation methods and approaches used by experts. Q&A on safe harbor provides explanation on detailed matters, such as information that needs to be removed and information that is allowed to be maintained.

II-2 欧州における動向

II-2 Trends in Europe

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。

Section (26) of the preamble of EU Data Protection Directive clearly states that the regulation does not apply to data rendered anonymous in such a way that the data is no longer identifiable. Statements to the same effect are also seen in the GDPR[52] that is scheduled to enter into force in 2018.

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

[52] General Data Protection Regulation.
General Data Protection Regulation.

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”[53]がある。

Documents related to the anonymization of personal data include an opinion by the Article 29 Data Protection Working Party [54] titled "Opinion 05/2014 on Anonymisation Techniques" [55] and a report by ICO titled "Anonymisation: managing data protection risk code of practice."[56]

II-2-1 第 29 条作業部会によるオピニオン（2014 年 4 月）

II-2-1 Opinion by the Article 29 Data Protection Working Party (April 2014)

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。

This Opinion states that whether an individual can be identified is to be determined, taking into account all the means likely reasonably to be used. In light of the fact that technologies are constantly evolving, the Opinion does not require information to be non-identifiable in any setting. Instead, it required companies to anonymize information to a reasonable level based on a good balance between anonymization effort and costs.

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。

This Opinion also analyzes the effects and limitations of existing anonymization methods. Each method is evaluated from the viewpoint of robustness based on the following three criteria: [i] is it still possible to single out an individual, [ii] is it still possible to link records relating to an individual, and [iii] can information be inferred concerning an individual?

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）。

Each method was evaluated as follows (this evaluation estimates the existence of risks and does not analyze whether anonymity is secured).

---

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

54 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）。
Article 29 Data Protection Working Party is a working party on the protection of individuals with regard to the processing of personal data, set up under Article 29 of the EU Data Protection Directive, which has advisory status (Article 29, paragraph (1)). It examines any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures (Article 30, paragraph (1)).

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

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

Figure II-1 Advantages and disadvantages of anonymization methods

加工手法 Processing method	シングルアウト・リスク Single out risk	連結リスク Linkage risk	推定リスク Inference risk
仮名化 Pseudonymisation	あり Yes	あり Yes	あり Yes
ノイズ付加 Noise addition	あり Yes	低い Low risk	低い Low risk
置換え（スワップ） Permutation (swapping)	あり Yes	あり Yes	低い Low risk
集約化/ｋ-匿名化 Aggregation/k-anonymity	なし No	あり Yes	あり Yes
ℓ-多様化 l-diversity	なし No	あり Yes	低い Low risk
差分プライバシー Differential privacy	低い Low risk	低い Low risk	低い Low risk
ハッシュ化/トークン化 Hashing/t-closeness	あり Yes	あり Yes	低い Low risk

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。

The Opinion concludes as follows: "each [anonymization] technique has its advantages and disadvantages. In most cases it is not possible to give minimum recommendations for parameters to use as each dataset needs to be considered on a case-by-case basis." It recommends the following practices as general ideas, while also referring to contextual elements and technical elements.

・ 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

・Data controllers should not rely on the “release and forget” approach. Data controllers should identify new risks and re-evaluate the residual risks regularly, and assess whether the controls for identified risks suffice and adjust accordingly.

・ 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。

・As part of such residual risks, data controllers should take into account the identification potential of the non-anonymized portion of a dataset.

II-2-2 英国 ICO レポート（2012 年 11 月）

II-2-2 U.K. ICO Report (November 2012)

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。

As practical guidelines for anonymization of personal data in the United Kingdom, this report explains the meaning and advantages of anonymization, estimation of re-identification risk, governance, etc. This report is in the same position as the FTC Report and this Report in that they are all published by the secretariat. The ICO Report also shows the anonymization process as follows.

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

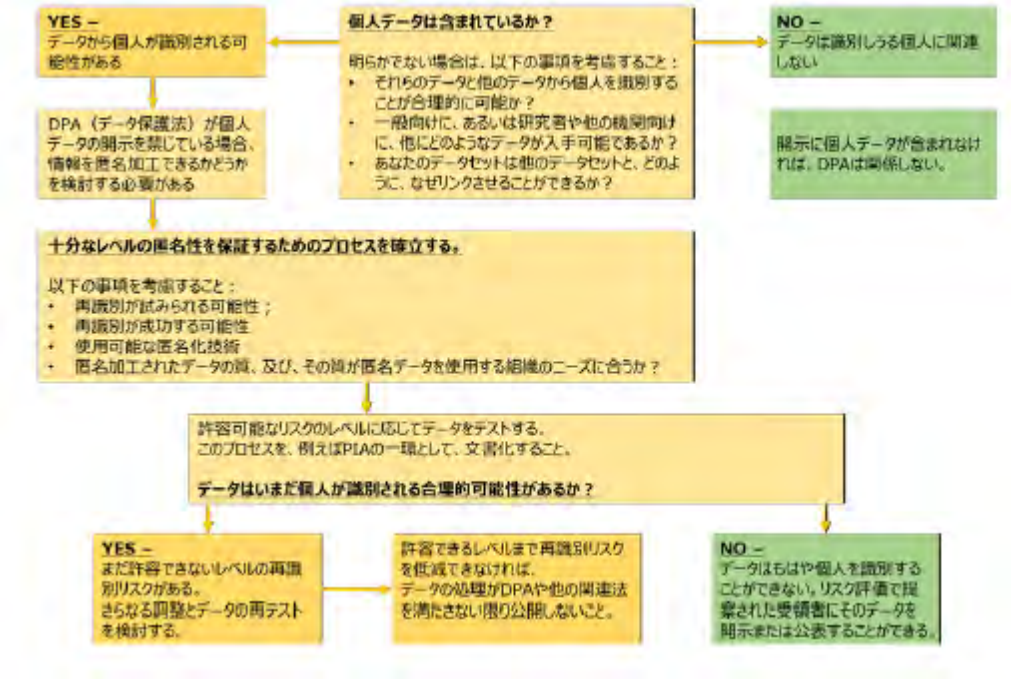
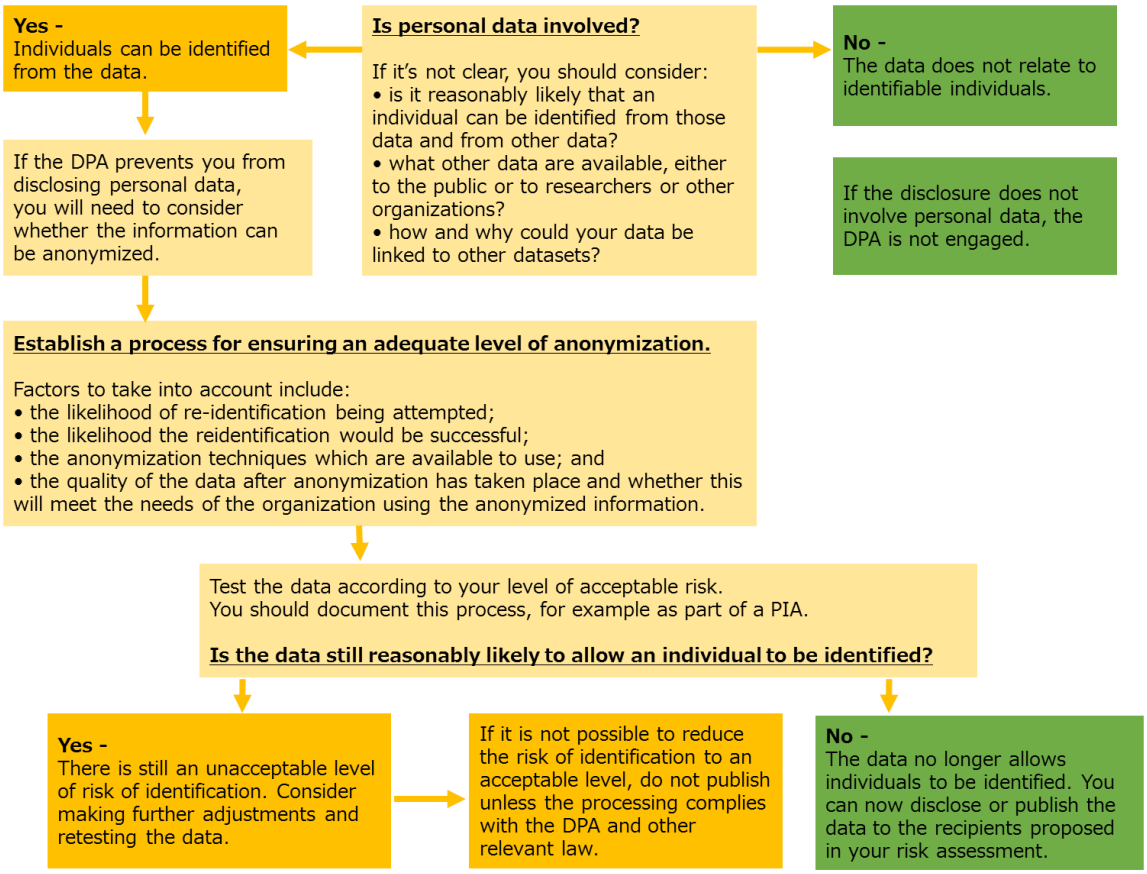


Figure II-2 Deciding when and how to release anonymized data



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。

In addition, Annexes contain case study on anonymization and explanation of anonymization methods.

II-3 その他の動向

II-3 Trends in Other Regions

II-3-1 オーストラリア

II-3-1 Australia

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。

In Australia, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 provides APP[57] that commonly apply to the private sector and public sector. One of these principles is "anonymity and pseudonymity" (APP2).

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。

APP2 provides that "individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter." Anonymization is provided as an option that individuals can request to business operators. However, it is also provided that said option is not required to be provided if anonymization or pseudonymization is impracticable.

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。

In addition, the Office of the Australian Information Commissioner published a report titled "Privacy business resource 4: De-identification of data and information" in April 2014.

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。

The report states that "personal information is ‘de-identified’ if the information is no longer about an identifiable individual or an individual who is reasonably identifiable." It also states that whether information has been effectively de-identified can be determined based on the cost, difficulty, practicality and likelihood of re-identification. The following two steps are listed as an anonymization method:

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

[57] Australian Privacy Principles.

[i] removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and

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

[ii] removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

II-3-2 韓国

II-3-2 South Korea

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。

In South Korea, six agencies[58] jointly published guidelines[59] on de-identification in June 2016, in light of the importance of data utilization in line with the development of information technologies.

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。

In these Guidelines, de-identification is explained in four phases, namely [i] ex ante review, [ii] de-identification, [iii] evaluation of the adequacy of processing, and [iv] follow-up management for preventing re-identification.

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。

Attribute information subject to de-identification include attribute of an individual (sex, age, address, religion, taste, etc.), physical characteristics (blood type, weight, eye color, medical records, etc.), credit information (tax payment, credit rating, income level, etc.), background information (name of school, major, work experience, place of work, etc.), information relating to electronic media (cookie, log-in time and date, access log, GPS data, etc.), and family information (information concerning spouse and children, legal representative, etc.)

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。

---

[58] 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。
Office for Government Policy Coordination, Ministry of the Interior, Korea Communications Commission, Financial Services Commission, Ministry of Science, ICT and Future Planning, and Ministry of Health and Welfare

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

The adequacy of processing is to be evaluated by external experts using k-anonymity and l-diversity.

II-3-3 国際規格

II-3-3 International Standards

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]。

The establishment of international standards is also promoted in relation to the protection of personal information and privacy. Major examples of such standards are "ISO/IEC 29100 Privacy Framework" and "ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." The standardization of anonymization is discussed in relation to "ISO/IEC 20889 Privacy enhancing data de-identification techniques" (ISO/IEC 20889).[60]

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。

ISO/IEC 20889 refers to de-identification of data as part of PET.[61] Specifically, it aims to define terms concerning de-identification, categorize de-identification methods according to their characteristics, and clarify the applicability of reduction of re-identification risk, as it is necessary to choose a de-identification method that suits the situation to effectively address re-identification risks.

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。

ISO/IEC 20889 "Privacy Framework," which has already been established as international standards, provides definition of the terms "anonymization" and "anonymous data" as follows.

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

---

[60] 2017 年 1 月時点で、委員会原案（Committee Draft）まで進んでいる。
A Committee Draft has already been formulated as of January 2017.

[61] Privacy enhancing techniques.
Privacy enhancing techniques.

III. 参考文献

III. Bibliography

【 報告書等 】

[Reports, etc.]

- 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

- Technical Study Working Group, Study Group on Personal Data, "Report by the Technical Study Working Group" (December 2013)

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

- Technical Study Working Group, Study Group on Personal Data, "Report by the Technical Study Working Group: Examination of 'Quasi-Personal Information (Tentative Name)' and 'Data with Reduced Identifiability (Tentative Name)' from Technical Perspectives" (May 2014)

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

- Expert Panel on the External Provision of Suica Data "Interim Report on the External Provision of Suica Data" (February 2014)

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

Expert Panel on the External Provision of Suica Data "Report on the External Provision of Suica Data" (October 2015)

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

- Study Group on Handling of Location Information in Emergencies and Similar Acute Situations, Ministry of Internal Affairs and Communications "Location Information Privacy Report: Balanced Realization of Appropriate

Protection of Privacy and Social Use of Location Information" (July 2014)
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
Ministry of Economy, Trade and Industry, "Reference Material to Help Business Operators Consider Methods for Producing Anonymously Processed Information (Anonymously Processed Information Production Manual)" (August 2016)

- 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

- Technical Study Working Group on Anonymously Processed Information, National Institute of Informatics, "Report on the Proper Processing of Anonymously Processed Information (Dated February 21, 2017)" (February 2017)

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 】

[Standards]

- 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 】

[Articles]

- 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 】

[Books]

- 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）
- Compiled by Kazuhisa Uryu, "Ichimon Itto 2015 Amendment to the Act on the Protection of Personal Information" (Shoji Houmu, December 2015)
- Hiroshi Nakagawa "Introduction to the Protection of privacy" (Keiso Shobo, February 2016)

- Jun Sakuma, “Protection of Privacy in Data Analysis” Kodansya, August 2016)
- Khaled El Emam & Luk Arbuckle (translated into Japanese by Takashi Sasai), "Anonymizing Health Data" (O'Reilly Japan, May 2015)