

# プライバシー保護技術の事業活用に関する一考察

杉尾 信行<sup>1,a)</sup> 青野 博<sup>1</sup> 関野 公彦<sup>1</sup>

**概要：** パーソナルデータを含むビッグデータを利用する際のプライバシー保護を実現する技術は様々研究されており、一例として統計化、匿名化や秘密計算等が知られている。これらの手法はそれぞれ技術特性が異なり、それらの技術特性を理解した上で適切なプライバシー保護技術を選択し、適用する必要がある。本稿は、サービス事業者が事業を進める上で発生する様々なプライバシーの課題を明確化し、プライバシー保護技術の特性を踏まえた上で、どのような技術を適用することが適切か判断するフローを明らかにする事を目的とする。

## A Study on Business Utilization of Privacy Protection Technologies

NOBUYUKI SUGIO<sup>1,a)</sup> HIROSHI AONO<sup>1</sup> KIMIHIKO SEKINO<sup>1</sup>

### 1. はじめに

現在、ユーザのパーソナルデータを含むビッグデータを用いて様々なサービスが提供されている。ユーザに対してサービスを提供する事業者（以下、サービス事業者と記す）は、ユーザから取得したパーソナルデータを利用する際、取得時にユーザへ示した利用目的の範囲内で適切な利用を行う必要がある。パーソナルデータの利用に伴い、法令違反やプライバシーの侵害に対する事業リスクが増大しており、プライバシー保護の重要性が高まっている。

パーソナルデータを利用する際のプライバシー保護を実現する技術は様々研究されており、一例として統計化、匿名化、秘密計算等が知られている。これらの手法はそれぞれ技術特性が異なり、それらの技術特性を理解した上で適切なプライバシー保護技術を選択、適用する必要がある。

サービス事業者において、パーソナルデータを含むビッグデータを事業に活用する場合、法令違反やプライバシーの侵害に対するリスクが増大しているが、それらのリスクに対してどのようなプライバシー保護技術を用いれば良いか不明な点が多い。そこで本稿は、個別の要素技術の改良を

目的としたものではなく、サービス事業者が事業を進める上で発生する様々なプライバシーの課題を明確化し、プライバシー保護技術の特性を踏まえた上で、どのような技術を適用することが適当であるか判断するフローを明らかにする事を目的とする。

本稿の貢献を以下に示す。まず初めに、サービス事業者が事業を進める上で発生する様々なプライバシーの課題を明確にした。これにより、今後サービスを新たに開始するサービス事業者が事前にどのような課題が存在し得るのか把握する事が可能となる。また、課題に対し、どのようなプライバシー保護技術を適用することが適当であるか判断するフローを明らかにした。これにより、プライバシー保護技術の特性を踏まえて適切な技術を選択する事が可能となる。

最後に本稿の構成を示す。2節では、本稿で用いる用語の定義を行う。3節では、サービス事業者がパーソナルデータを含むビッグデータを事業に活用する際の課題について纏める。4節では、プライバシー保護技術とその特性について纏める。最後に、5節では、パーソナルデータを含むビッグデータを事業に活用する際に用いるプライバシー保護技術の判断フローを示すと共に、そのフローを用いた評価を行う。最後に6節にて、本稿のまとめと今後の課題について記載する。

<sup>1</sup> 株式会社 NTT ドコモ  
NTTDOCOMO, INC., 3-6 Hikarino-oka, Yokosuka, Kanagawa, 239-8536, Japan

<sup>a)</sup> sugio@nttdocomo.com

## 2. 用語定義

本稿で用いる用語を表1の通り定義する。

表1 用語一覧

| 用語       | 説明                                                                                                                             |
|----------|--------------------------------------------------------------------------------------------------------------------------------|
| ユーザ      | サービスを利用するデータ主体（本人）                                                                                                             |
| サービス事業者  | ユーザに対してサービスを提供する事業主体で、パーソナルデータを含むビッグデータを自社の事業に利用する主体<br>自社が保有するパーソナルデータを第三者に提供する主体を提供者とし、提供者から受領したパーソナルデータを自社の事業に活用する主体を受領者とする |
| 個人情報     | 生存する個人に関する情報で、特定の個人を識別できる情報                                                                                                    |
| パーソナルデータ | 特定の個人が識別できる情報の他に、個人に関するデータ項目を含む、幅広い情報                                                                                          |
| ビッグデータ   | パーソナルデータを含む事業に役立つ知見を導出するためのデータ                                                                                                 |
| 生情報      | 加工を施す前のパーソナルデータやビッグデータ                                                                                                         |
| 統計情報     | パーソナルデータやビッグデータをデータの集団と見なし、個々の要素の分布を調べ、その集団の傾向・性質などを数量的に統一的に明らかにした情報                                                           |
| 匿名加工情報   | 特定の個人を識別することができないようにパーソナルデータを加工して得られる個人に関する情報であって、当該個人情報情報を復元することができないようにしたもの                                                  |

## 3. 現状の課題

### 3.1 パーソナルデータを利用するサービス事業者の義務

パーソナルデータを利用する際の共通した基本原則として、OECD 8原則が知られている。表2にその要点を示す。詳細は文献[16]を参照のこと。

サービス事業者は、OECD 8原則や2017年5月30日に施行された（改正）個人情報保護法[6]に基づき、パーソナルデータ\*1を適切に取扱い、保護する必要がある。

尚、2018年5月25日にEU一般データ保護規則（GDPR）[1]、[3]が施行された。EU加盟28カ国にアイスランド、リヒテンシュタイン、ノルウェーの3カ国を加えた31カ国に所在する個人に関する情報を取り扱うサービス事業者は、この規則に基づきパーソナルデータを適切に取扱い、保護する必要がある。本稿では議論の焦点を絞る為、EU一般データ保護規則（GDPR）は対象外とする。

\*1 本稿では、（改正）個人情報保護[6]で定義された個人情報を含むパーソナルデータを対象としている点に注意が必要である。

表2 OECD 8原則

| 原則        | 概要                                        |
|-----------|-------------------------------------------|
| 収集制限の原則   | データ主体（本人）に通知し、同意を得た上で適切にデータを収集する。         |
| データ内容の原則  | 個人データは、利用目的の範囲内で利用し、正確、完全及び最新の内容に保つ。      |
| 目的明確化の原則  | 個人データの収集し、利用する目的を明確にする。                   |
| 利用制限の原則   | 明確にした利用目的の範囲内でのみ、個人データを利用する。              |
| 安全保護措置の原則 | 個人データを不正アクセス、不正利用、改ざん又は漏えい等のリスクから安全に保護する。 |
| 公開の原則     | 個人データの利用目的や取扱い方針等、必要事項を明確に示す。             |
| 個人参加の原則   | データ主体（本人）が行う自分のデータに対する各種要求に対応する。          |
| 責任の原則     | データ管理者は、個人データの管理について責任を持つ。                |

### 3.2 事業を進める上で発生するプライバシーの課題

現在、多くのサービス事業者がパーソナルデータを含むビッグデータを事業に活用する為、ビッグデータの収集を行っている。しかしながら、（改正）個人情報保護法に対する法令違反やサービス提供後の風評被害（炎上リスク等）を考えると、パーソナルデータを含むビッグデータを事業に活用し難いという課題が存在する。

データライフサイクル（取得、利用、第三者提供、廃棄）毎にサービス事業者が担う OECD 8原則をマッピングしたものを図1に示す\*2。

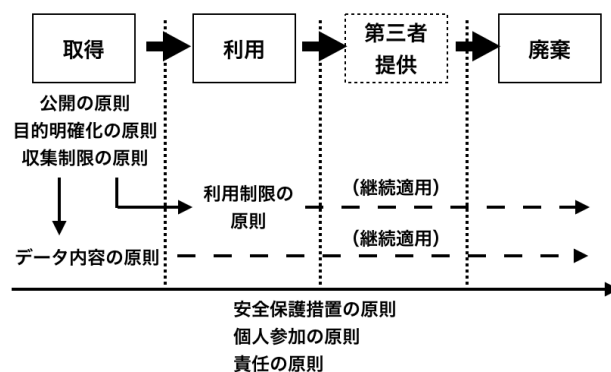


図1 データライフサイクルと OECD 8原則

前述の図を参考に、サービス事業者が事業を進める上で発生するプライバシーの課題を纏める。

【取得】 サービス事業者がパーソナルデータを含むビッグデータを事業に活用する場合、ビッグデータを分析した時

\*2 取得サイクルが無い場合としては、社内の他組織や他サービス等で取得済みのパーソナルデータを利用する場合や、他社から第三者提供にてパーソナルデータを受領した場合等が考えられる。

にどのような知見が得られるか不明であり、得られた知見に応じてビッグデータの利用目的が適宜変わる為、取得時に予め利用目的を特定することは困難である。本稿では、この課題を「(1) 利用目的の特定困難性」と呼ぶ事とする。

【利用】 利用目的の範囲内でパーソナルデータを含むビッグデータを事業に活用する場合は問題無いが、当初予定していた利用目的の範囲外でビッグデータを活用する為には、既に取得したパーソナルデータの利用目的を変更する必要がある。利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない((改正)個人情報保護法, 法第18条(第3項))。しかしながら、過度な通知はサービスの利便性低下に繋がる恐れがある。本稿では、この課題を「(2) 目的変更に関わる通知困難性」と呼ぶ事とする。

また、パーソナルデータを含むビッグデータを分析する際、自社のビッグデータだけでなく、他のサービス事業者が有するビッグデータを組み合わせて分析したい場合が存在する。第三者提供や共同利用が可能であれば問題無いが、センシティブでプライバシーの配慮が必要なパーソナルデータや、機密性が高いパーソナルデータを含むビッグデータを直接第三者提供や共同利用する事が困難な場合が存在する。本稿では、この課題を「(3) ビッグデータの共有困難性」と呼ぶ事とする。

【第三者提供】 パーソナルデータを第三者に提供する場合、(改正)個人情報保護法に基づく確認・記録義務がサービス事業者(パーソナルデータの提供者)と第三者(パーソナルデータの受領者)にそれぞれ発生する。しかしながら、パーソナルデータを受領する第三者において、受領するパーソナルデータの利用用途がマス・マーケティングの場合、特定の個人が識別できる情報は必要ない為、(改正)個人情報保護法に基づく確認・記録義務や安全管理措置を履行してパーソナルデータを提供・受領するのは提供者と受領者の双方にとって業務効率を低下させる要因となり得る。本稿では、この課題を「(4) 第三者提供に関わる業務効率困難性」と呼ぶ事とする。

【廃棄】 ビッグデータに含まれるパーソナルデータを廃棄する際、パーソナルデータが他のデータと組み合わせられている場合が存在する。この場合は、ビッグデータの中からパーソナルデータのみを抽出し、当該データのみ廃棄するという事が困難である。また、データの廃棄に関して適切な措置を施さなければ、パーソナルデータが記憶媒体に残留している場合がある。そして、廃棄した記憶媒体中の残留データから、パーソナルデータの漏洩に繋がる恐れがある。本稿では、この課題を「(5) 廃棄時のデータ抽出・消去困難性」と呼ぶ事とする。

## 4. プライバシー保護技術の概要と技術特性

本稿で対象とするプライバシー保護技術の概要と技術特性について説明する。尚、各技術の詳細は本稿では割愛する為、必要に応じて適宜参考文献を参照されたい。

### 4.1 統計化

統計は、広辞苑に拠ると『集団における個々の要素の分布を調べ、その集団の傾向・性質などを数量的に統一的に明らかにすること。また、その結果として得られた数値のこと』と説明している。

本稿では、パーソナルデータを含むビッグデータをデータの集団と捉え、その傾向・性質を数量的に統一的に明らかにする行為を統計化と呼ぶ。

### 4.2 匿名化

匿名化は、特定の個人を識別することができないようにパーソナルデータを加工し、当該個人情報を復元できないようにする事である。代表的な匿名化技法として、レコードの削除やトップ(ボトム)・コーディング等が知られている。詳細については文献[2], [10], [13]を参照されたい。

### 4.3 秘密計算

秘密計算は文献[11]に拠ると『個別の機関のデータを互いに共有することなく、その秘密性を保ったまま統計解析や機械学習などの計算を実行し、その結果のみを得るためのプライバシー保護技術』であると説明されている。

本稿では、複数のパーティが秘密情報を持ち寄り、自分の秘密情報を他者に知らせることなく、計算結果のみを得るマルチパーティ型秘密計算[15]を対象とする。

### 4.4 プライバシー保護技術の特性

本節では、統計化、匿名化、及び秘密計算が有する技術特性について纏める。

統計化と匿名化は、パーソナルデータを含むビッグデータの個人に関する情報を削減する事により、パーソナルデータを保護することが目的である。統計化と匿名化の違いを可視化したものを図2に示す。また、秘密計算はパーソナルデータを含むビッグデータに対して処理するプロセスの保護が目的である。統計化、匿名化と秘密計算の違いを可視化したものを図3に示す。

## 5. 提案手法と評価

本節では、前節のプライバシー保護技術の特性を踏まえて、サービス事業者が事業を進める上で発生する様々なプライバシー上の課題(1)～(5)に対し、どのようなプライバシー保護技術を適用することが適当であるかを判断するフローの提案と、そのフローを用いた評価を行う。

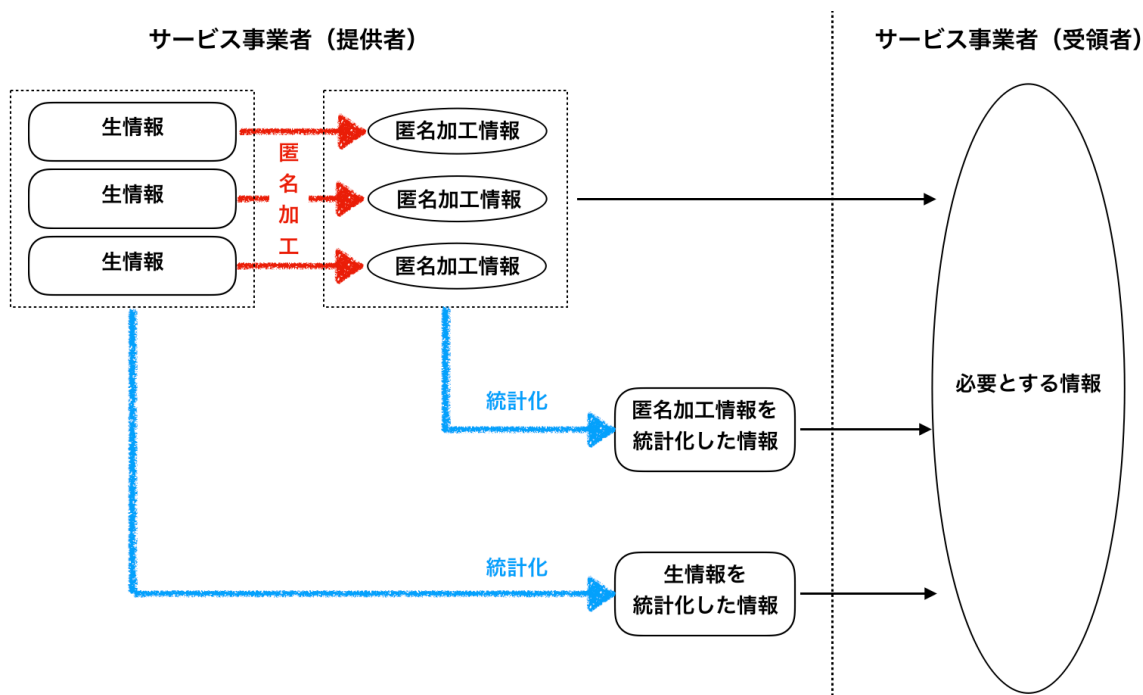
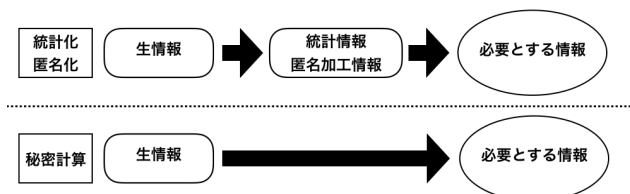


図 2 統計化と匿名化の違い



(注釈) 秘密計算は生情報を暗号化した後、複数のパーティに暗号化した断片情報を分散し、断片情報を元に統計処理を行う事で、生情報を第三者に開示せずに統計分析が可能となる [15].

図 3 統計化、匿名化と秘密計算の違い

## 5.1 判断フロー

判断フローを図4に示す。図4において、点線の左半分はパーソナルデータを含むビッグデータを保持するサービス事業者（提供者）であり、点線の右半分はパーソナルデータ等の情報を受領するサービス事業者（受領者）を示す。以下、判断フローについて説明する。

- 「利用目的を特定可能か？」  
パーソナルデータを含むビッグデータの利用目的が特定可能であるか判断する。ビッグデータを分析した時にどのような知見が得られるか不明であり、得られた知見に応じてビッグデータの利用目的が適宜変わる為、利用目的を特定する事が困難な場合がある。
- 「利用目的を変更するか？」  
パーソナルデータを含むビッグデータの利用目的を変

更するか判断する。（改正）個人情報保護法では『個人情報取扱事業者は、利用目的を変更する場合には、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て行ってはならない。（法第15条第2項）』とある為、パーソナルデータ取得後に当初の利用目的から変更する場合は、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ることはできない。

- 「第三者提供を行うか？」  
ユーザから集めたパーソナルデータを含むビッグデータを第三者に提供するかどうか判断する。第三者提供を行う場合は、（改正）個人情報保護法に則った対応（ユーザの同意や第三者提供時の確認・記録義務など）が必要となる。
- 「生情報が必要か？」  
サービス事業者がパーソナルデータを含むビッグデータを事業へ活用する際に、ユーザから集めた生のデータが必要かどうか判断する。個人を特定する必要があるダイレクト・マーケティング等では、ユーザから取得した氏名、年齢、性別、住所などは重要な情報の為、生情報のまま保存、活用する必要がある。事業活用の内容（ビッグデータの活用の用途）によっては、必ずしも生情報を必要とする訳ではない為、適切に判断することが重要である。
- 「匿名加工情報が必要か？」  
サービス事業者がパーソナルデータを含むビッグデー

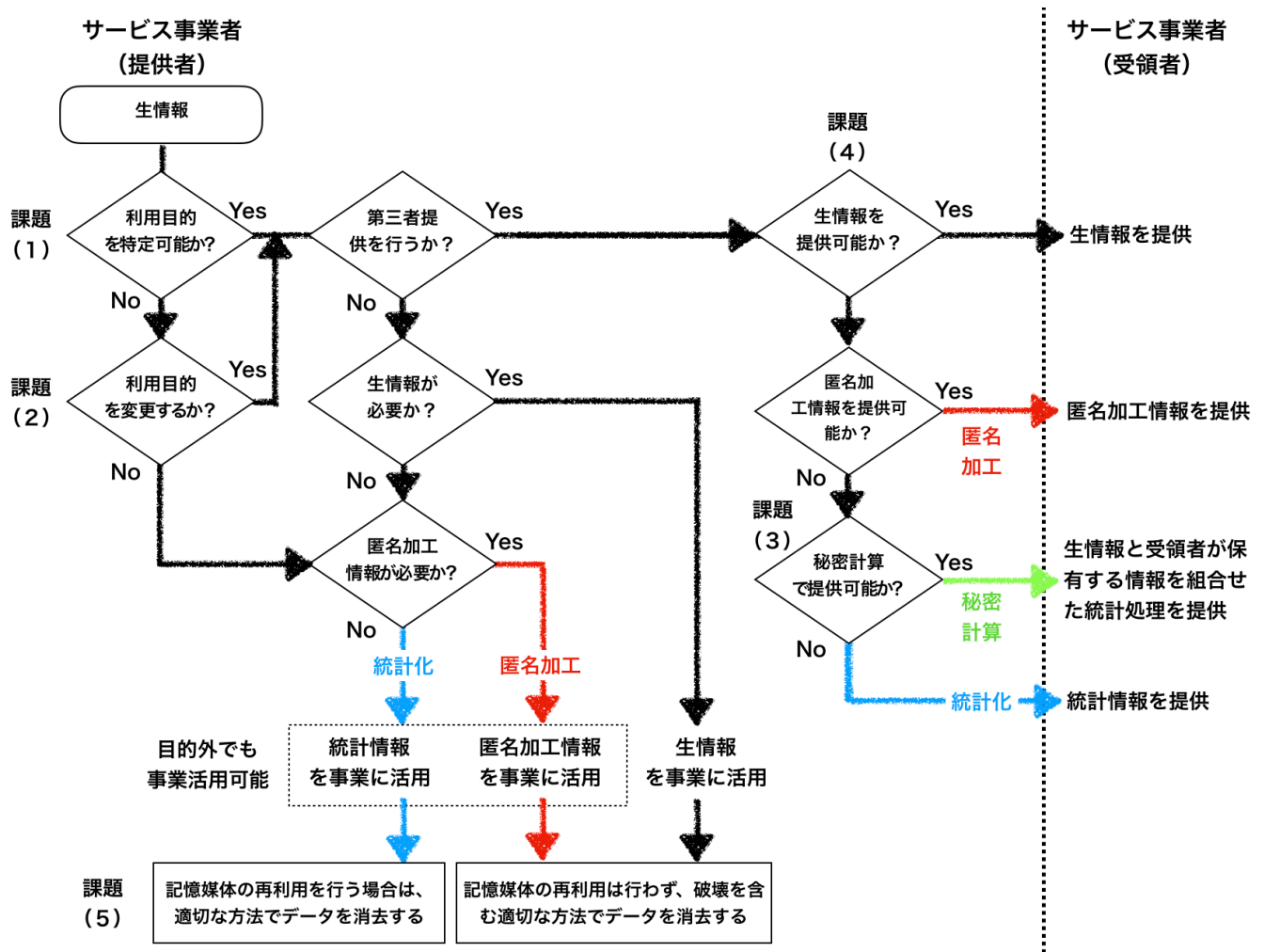


図 4 判断フロー

タを事業へ活用する際に、ユーザから集めた生情報は必要無いが、匿名化したデータが必要かどうか判断する。マーケティングの分析で、ユーザの特定までは不要であるが、属性（年齢や性別）に基づいた購入商品の分析などを行う場合には、匿名加工情報が必要になる。また、事業活用の内容によっては統計情報で十分な場合も有る為、適切に判断することが重要である。

- 「生情報を提供可能か？」

第三者提供を行う際、ユーザから取得したパーソナルデータを含むビッグデータを生情報のまま提供可能か判断する。あるサービスで集めたユーザのパーソナルデータを第三者提供する事が予め分かっている場合などが該当する。尚、個人データの第三者提供を行う場合、(改正) 個人情報に則った対応(ユーザの同意や第三者提供時の確認・記録義務など、オプトアウトによる第三者提供も含む)が必要となる為、第三者提供先が必要とする情報が生情報でなければならないのかを事前に判断することが望ましい。

- 「匿名加工情報を提供可能か？」

第三者にパーソナルデータを含むビッグデータを生情報のままで提供する事が難しい場合、生情報を匿名加工情報に加工し、提供可能か判断する。自社の事業活用時と同じく、第三者が必要とする情報が匿名加工情報で実現可能な場合は、生情報を匿名加工情報に加工し、提供する事が望ましい。尚、匿名加工情報を作成、提供する場合も、(改正)個人情報保護法に則った対応が必要である。

- 「秘密計算で提供可能か？」

秘密計算を用いることで、そのパーソナルデータを含むビッグデータの秘密性を保ったまま第三者のデータと合わせて統計解析や機械学習などの計算を実行し、その結果のみを得る事が出来る。センシティブでプライバシーの配慮が必要なパーソナルデータや、機密性が高いパーソナルデータを含むビッグデータを生情報や匿名加工情報として第三者に提供出来ない場合は、秘密計算を用いた統計分析を行う事が出来るか検討する事が望ましい。尚、本稿で対象とする秘密計算は、複数のパーティが秘密情報を持ち寄り、自分の秘密情

報を他者に知らせることなく、計算結果のみを得るマルチパーティ型秘密計算 [15] である。秘密計算は計算結果を得る過程を保護する技術であり、計算結果から元の秘密情報に関する情報が漏洩する出力プライバシーの対策については、別の技術を用いる必要がある。

## 5.2 評価

図 4 に示す判断フローを用いた評価を行う。以下に課題 (1) ～ (5) を再掲する。

- (1) 利用目的の特定困難性
- (2) 目的変更に関わる通知困難性
- (3) ビッグデータの共有困難性
- (4) 第三者提供に関わる業務効率困難性
- (5) 廃棄時のデータ抽出・消去困難性

### 5.2.1 準備

本紙では、図 4 の判断フローを用いた場合の稼働を見積もる事で評価を行うこととする。全体の稼働は、データライフサイクル (取得, 利用, 第三者提供, 廃棄) の各フローで発生する稼働の総和で示すものとする。各フローで発生する稼働は下記の様に設定する。

【取得】 サービス事業者が取得するパーソナルデータの利用目的を特定 (設計) するのに必要な稼働を  $w_1$  とする。

【利用】 パーソナルデータを含むビッグデータを事業に活用する場合、ビッグデータを分析した時にどのような知見が得られるか不明であり、得られた知見に応じてビッグデータの利用目的が変わる場合がある。ユーザへの利用目的変更通知に必要な稼働に関して、利用目的を変更しない場合は  $w_2$ 、一つのサービスに関する利用目的を変更する場合は  $w_3$ 、二つ以上のサービスに関する利用目的を変更する場合は  $w_4$  とする。また、パーソナルデータを含むビッグデータの活用に必要な稼働に関して、統計情報の場合は  $w_5$ 、匿名加工情報の場合は  $w_6$ 、生情報の場合は  $w_7$  とする。

【第三者提供】 パーソナルデータを含むビッグデータの第三者提供に必要な稼働に関して、前述の活用時と同様に統計情報の場合は  $w_5$ 、匿名加工情報の場合は  $w_6$ 、生情報の場合は  $w_7$  とする。また、秘密計算を用いる場合は  $w_8$  とする。

【廃棄】 パーソナルデータを含むビッグデータの廃棄に関して、ビッグデータの中からパーソナルデータを抽出せず、記憶媒体を再利用する場合は  $w_9$ 、パーソナルデータを抽出し、当該データを削除した上で適切な方法 (消磁や破壊等) を用いて記憶媒体の廃棄を行う場合は  $w_{10}$  とする。

図 4 の判断フローに関し、稼働  $w_i$  ( $i = 1, 2, \dots, 10$ ) に置き換えたものを図 5 に示す。円で囲まれた記号  $w_i$  は各処理で発生する稼働を示す。図 5 を用いることにより、パーソナルデータの取得, 利用, 第三者提供, そして廃棄までの

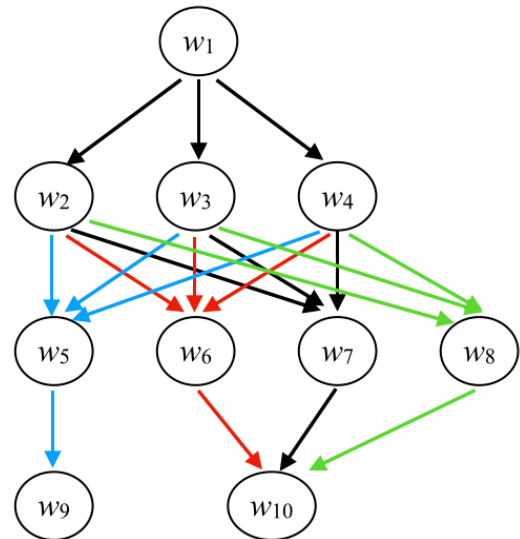


図 5 データライフサイクルに必要な稼働

一連の流れで必要な稼働を  $w_i$  の総和で示すことができる。

### 5.2.2 稼働を用いた評価

図 5 を用いた一例を以下に示す。サービスで取得するパーソナルデータを利用目的を変更することなく、統計情報で利用し、データ廃棄を行う場合の総稼働  $W$  は、

$$W = w_1 + w_2 + w_5 + w_9$$

と見積もることができる。その他の場合も同様である。

稼働  $w_i$  ( $i = 1, 2, \dots, 10$ ) に数値を代入した一例を図 6 に示す。

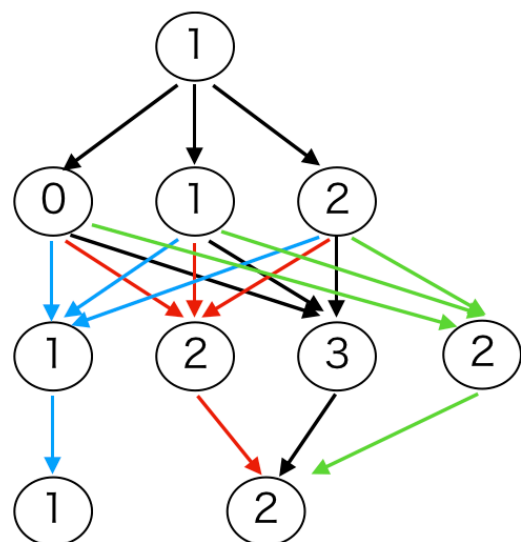


図 6 稼働を用いた評価の一例

図 6 から、パーソナルデータを含むビッグデータを生情報のまま自社事業に活用する場合、最大で



$$W = 1 + 2 + 3 + 2 = 8$$

の稼働が想定される。その為、生情報のまま事業活用する場合は、利用目的を変更することなく、当該サービスに関わる事業に活用することが効率的である。この場合、当該サービスによるパーソナルデータの取得からデータ廃棄までに必要な全体の稼働は、

$$W = 1 + 0 + 3 + 2 = 6$$

と見積もることができ、最大2の稼働削減が可能となる。また、互いに利用目的が異なる複数のサービスから取得したパーソナルデータの集合をビッグデータとして自社事業に活用する場合は、統計情報、又は匿名加工情報に変換することで全体の稼働を削減しつつ、データ活用が可能である。この場合、 $n$  個 ( $n = 1, 2, \dots$ ) の互いに利用目的が異なるサービスのパーソナルデータを取得し、利用目的を変更せずに統計情報として利用後、不要になった時点でデータ廃棄する際に必要な全体の稼働は、

$$W = n \times (1 + 0 + 1 + 1) = 3n$$

と見積もることができる。また、上記例で利用目的を変更せずに匿名加工情報として利用後、不要になった時点でデータ廃棄する際に必要な全体の稼働は、

$$W = n \times (1 + 0 + 2 + 2) = 5n$$

と見積もることができる。互いに利用目的が異なる複数のサービスから得られたパーソナルデータを含むビッグデータを生情報のまま自社事業に活用する場合、最大で  $W = 8n$  の稼働が想定される為、まずは統計情報や匿名加工情報に変換したデータで要件を満たせるか検討し、全体の稼働を削減しつつ、データを活用する事が望ましい。

パーソナルデータを第三者に提供する場合、図6から生情報をそのまま提供するには最大8の稼働が想定される。この場合、受領者も（改正）個人情報保護法の確認・記録義務が発生する為、事業活用に必要な最小限のデータ授受であることが望ましい。予め受領者が必要とするデータ特性を明らかにすることにより、要件を満たす様に統計情報や匿名加工情報に変換し、第三者提供を行うことで、全体の稼働を削減しつつ、データ活用が可能である。また、受領者が必要とするデータ特性が明らかで無い場合、必要最小限の観点から、統計情報、匿名加工情報、生情報の順に段階的に提供した方が望ましいと思われる<sup>\*3</sup>。

### 5.3 考察

本稿では、パーソナルデータを含むビッグデータの事業

<sup>\*3</sup> 必要最小限の観点から統計情報、匿名加工情報、生情報の順に段階的に第三者へ提供する場合、生情報の第三者提供に関して、ユーザへの通知と同意取得に関わる義務が発生することに注意が必要である。

活用に関し、「稼働見積による評価」、「ユーザの同意に基づく生情報の活用」、及び「データ活用時に必要な情報の粒度」の3点について考察する。

#### 5.3.1 稼働見積による評価

図5にて、判断フローを稼働  $w_i$ , ( $i = 1, 2, \dots, 10$ ) で置き換え、データライフサイクル（取得、利用、第三者提供、廃棄）に必要な稼働を  $w_i$  の総和で示した。パーソナルデータを含むビッグデータの活用に関する稼働はデータライフサイクルの中でも特に重要であり、それらを以下に再掲する。

- $w_5$ : 統計情報（を事業に活用する場合）
- $w_6$ : 匿名加工情報（同上）
- $w_7$ : 生情報（同上）

本稿では、上記の稼働  $w_i$ , ( $i = 5, 6, 7$ ) の数値例をそれぞれ ( $w_5, w_6, w_7$ ) = (1, 2, 3) とした（図6参照）。この根拠を以下に示す。統計情報は匿名加工情報や生情報から個人に関する情報を削除した情報である為、統計情報を取得・管理・運用する稼働  $w_5$  は、匿名加工情報や生情報を事業に活用する為の稼働  $w_6, w_7$  よりも小さいと判断した。また、匿名加工情報と生情報を事業に活用する為の稼働  $w_6$  と  $w_7$  の大小比較について、両者は（改正）個人情報保護上の履行義務が発生する為、一概に稼働の大小比較を関係する事は難しいが、匿名加工情報は生情報から特定の個人を識別することができないように情報を削除した情報である為、匿名加工情報を取得・管理・運用する稼働  $w_6$  は生情報の事業活用に必要な稼働  $w_7$  よりも小さいと判断した。以上から、本稿では稼働  $w_5, w_6, w_7$  の大小関係を  $w_5 < w_6 < w_7$  とした。

しかしながら、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パーソナルデータ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（表1参照）である為、生情報を事前に取得済みであると考え、稼働  $w_6, w_7$  の大小関係は  $w_6 \geq w_7$  と考えることもできる。従って、パーソナルデータを含むビッグデータの事業活用で必要となる稼働の見積り精度の向上は今後も継続的に検討が必要である。

#### 5.3.2 ユーザの同意に基づくパーソナルデータの活用

ユーザの同意に基づき取得したパーソナルデータを含むビッグデータを様々な目的で自社事業に活用できるならば、サービス事業者において生情報の取得・利用・廃棄に関わる稼働はかかるが、データ活用の観点からは望ましいと思われる。しかしながら、データ取得時にユーザに提示し、ユーザの同意を得た利用目的を超える範囲でパーソナルデータを活用する事は目的外利用に該当する為、その様なデータの活用は（改正）個人情報保護法により禁じられている。その為、生情報のまま事業活用を行う場合、サービス毎に利用目的を明記し、ユーザの同意を得た上で取得したパーソナルデータをその目的の範囲内で、当該サービ

スに関わる事業に活用することとなる。ユーザへ提供するサービス数が少ない場合は、サービス毎に得られたパーソナルデータを利用目的の範囲内で活用すれば良いが、サービス数が多くなるにつれて様々な種類のパーソナルデータがサービス事業者を集まる為、得られたパーソナルデータを含むビッグデータとして事業に活用する事がサービス事業者にとって重要になってくる。パーソナルデータを含むビッグデータはサービス事業者の競争力の源泉となる為、サービス毎に明記した利用目的の範囲で生情報を事業に活用しつつ、ユーザの同意を得た利用目的を超える範囲は生情報を匿名加工情報や統計情報に加工した上でデータを事業に活用する事が、サービス事業者の観点からは望ましいと思われる。なお、データ活用時の炎上リスクを低減させる為、ユーザの同意を得た利用目的を超える範囲でデータの事業活用を行う場合には、可能な範囲内で予めユーザに対して通知、及びユーザの同意を得ておく事が望ましいと思われる。

### 5.3.3 データ活用時に必要な情報の粒度

サービス事業者において、パーソナルデータを含むビッグデータは競争力の源泉であるが、事業活用上必要の無い範囲のパーソナルデータまで取得する事は、サービス事業者にとって余計な管理・運用コストを発生させる要因となり、経済的合理性に反する為、望ましく無い。従って、サービス事業者はサービスを通じて取得するパーソナルデータは必要とする情報の範囲に留める事が望ましい。例えば、個人へのダイレクトマーケティング等を想定しない場合には、個人を特定・識別可能な情報は仮名化等を行う事で個人に関する情報を削減する事が安全管理上は好ましいと思われる。更に、分析対象とする地域（エリア）に属する人の統計分析を想定する場合には、サービスを通じて取得したパーソナルデータを統計情報に加工後、直ちにパーソナルデータを削除してしまう運用も安全管理上は望ましいと思われる。しかしながら、一度パーソナルデータを含むビッグデータを匿名加工情報や統計情報に加工し、個人に関する情報を削減した場合は、元のパーソナルデータに復元する事は出来ない<sup>\*4</sup>為、サービス事業者は可能な限り、事業活用に必要とする情報の粒度を明らかにする事に稼働を費やす事が望ましいと思われる。尚、本稿では、事業活用に必要な情報の粒度を見極める為に必要な稼働は考慮していない為、今後の課題とする。

## 6. まとめと今後の課題

本稿では、サービス事業者が事業を進める上で直面する様々なプライバシー上の課題を明らかにした。また、それらの課題に対してどのようなプライバシー保護技術を適用することが適切であるかを検討する判断フローを新たに提

案した。

今後は、サービス事業者内で本稿で提案した判断フローを活用し、フィードバックに基づき本手法の改良を行うと共に、パーソナルデータの事業活用で必要となる稼働の見積り精度の向上を行う予定である。

## 参考文献

- [1] General Data Protection Regulation, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [2] Khaled El Eman, Luk Arbuckle 著, 木村 映善, 魔 狸 監訳, 「データ匿名化手法」, オライリージャパン, 2015
- [3] 一般財団法人日本情報経済社会推進協会 (JIPDEC), 「EU 一般データ保護規則 (仮訳) について」, <https://www.jipdec.or.jp/library/archives/gdpr.html>
- [4] 小栗 秀暢, 黒政 敦史, 松井 くにお, 「匿名加工・再識別コンテストを通じた情報流通プラットフォームの検討」, 第72回コンピュータセキュリティ研究会, No.34, 2016
- [5] 菊池 浩明, 山口 高康, 濱田 浩気, 山岡 裕司, 小栗 秀暢, 佐久間 淳, 「匿名加工・再識別コンテスト Ice & Fire の設計」, コンピュータセキュリティシンポジウム 2015 論文集, 2015(3), pp.363-370, 2015
- [6] 個人情報の保護に関する法律 (平成 15 年法律第 57 号)
- [7] 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 (通則編)」, 2016 年 11 月 改正版 <https://www.ppc.go.jp/files/pdf/guidelines01.pdf>
- [8] 個人情報保護委員会, 「個人情報の保護に関する法律についてのガイドライン (外国にある第三者への提供編)」, 2016 年 11 月 改正版 <https://www.ppc.go.jp/files/pdf/guidelines02.pdf>
- [9] 個人情報保護委員会, 「個人情報の保護に関する法律についてのガイドライン (第三者提供時の確認・記録義務編)」, 2016 年 11 月 改正版 <https://www.ppc.go.jp/files/pdf/guidelines03.pdf>
- [10] 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 (匿名加工情報編)」, 2016 年 11 月 改正版 <https://www.ppc.go.jp/files/pdf/guidelines04.pdf>
- [11] 佐久間 淳 著, 「データ解析におけるプライバシー保護」, 講談社, 2016
- [12] 鈴木 良介 著, 「ビックデータビジネスの時代」, 翔泳社, 2011
- [13] 高橋 克己, 「匿名化技術の概要」, <https://www.dekko.or.jp/kenkyukai/data/4th/20160612.Doc2.pdf>
- [14] 藤村 明子, 間形 文彦, 千田 浩司, 諸橋 玄武, 高橋 克己, 「新たな個人情報保護法における匿名加工情報の基準に関する一考察」, コンピュータセキュリティシンポジウム 2015 論文集, pp.1143-1150, 2015
- [15] 千田 浩司, 五十嵐 大, 宮田 輝子, 瀧口 浩義, 桐淵 直人, 「高密度データも安全に二次利用可能な「秘密計算技術」」, <http://www.ntt.co.jp/journal/1403/files/jn201403067.pdf>
- [16] 堀部 政男, 新保 史生, JIPDEC (野村 至) (仮訳), 「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告 (2013)」, 一般財団法人日本情報経済社会推進協会 (JIPDEC), <https://www.jipdec.or.jp/library/archives/u71kba0000002fym-att/01.pdf>

<sup>\*4</sup> (改正) 個人情報保護法では、匿名加工情報から元の個人データを特定する再識別行為は禁止されている。