

# 「匿名加工情報」による ビッグデータビジネス活性化への期待と課題 マルチステークホルダー・プロセスによるルール作り



小林慎太郎

## CONTENTS

- I 「匿名加工情報」とは
- II 匿名加工情報が制度化される意義
- III 普及の鍵を握る事業者の自主的な取り組み
- IV 始まるマルチステークホルダー・プロセスによる民間自主ルール作り

## 要約

- 1 2015年9月3日に成立した個人情報保護法の改正の目玉として、本人同意なしにパーソナルデータを利活用できる制度「匿名加工情報」が新設される。個人情報を匿名加工処理し、かつ処理されたデータの取り扱いに対して、再識別禁止などの規律を課すことによって、本人同意がなくても、データを第三者提供することなどができる。
- 2 匿名加工情報が制度化される意義は大きい。従来は匿名処理しても、個人の再識別リスクが残存するために、第三者提供すると個人情報保護法に抵触する恐れがあった。これが立法によって、合法的に行うことができるようになる。改正法では名簿屋規制が導入され、従来以上に外部からの個人情報へのアクセスが制限されることになるため、匿名加工情報は、提供側、受領側双方にとって貴重である。
- 3 匿名加工情報の活用には、厳しい規律への対応が求められる一方で、加工処理のルールは、業界ごとの特性に応じて、業界団体などが音頭をとって定めることが可能となった。これは、官と民による新しい共同規制の仕組みである。このルール作りは、消費者代表などを含めた多様な主体による「マルチステークホルダー・プロセス」を通じて実施することが想定されている。
- 4 マルチステークホルダー・プロセスの実証研究は、既にさまざまな分野で着手されており、試行錯誤しながら、ルール作りの経験を積み重ねている。制度改正の機会をつかむに当たり、企業は業界団体に働きかけるなどして自らルール作りに取り組む必要がある。

## I 「匿名加工情報」とは

個人情報保護法が、施行後10年で初めて大きく改正される。2015年9月3日に成立した「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」（以下「改正法」）は、個人情報の保護強化とパーソナルデータの活用促進の両面から、ビジネスに大きな影響を及ぼす見込みである。

改正法による最大の目玉は、本人同意がなくてもパーソナルデータをさまざまな目的に利用したり、第三者提供したりすることができる「匿名加工情報」という制度の創設である。この匿名加工情報は、ビッグデータビジネスを促進する起爆剤となるものとして期待されている。

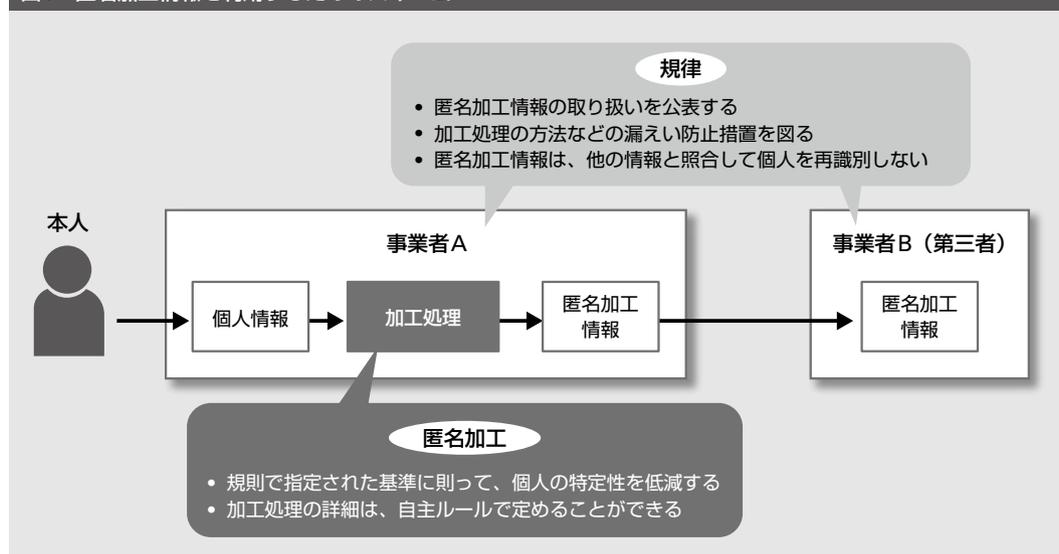
現行法では、個人情報を第三者へ提供するには、利用目的を特定して、本人から同意を取得することが原則である<sup>※1</sup>。同様に、個人情報の取得時に掲げていた利用目的の範囲を変更する場合も、本人から同意を取り直さなければならない。

しかし、ビッグデータビジネスのようなデータの二次利用までを、利用目的に含めてあらかじめ同意を取得しておくことは、利用目的の特定原則と矛盾する。また利用目的を変更するたびに本人から同意を取り直すことも、事業者、消費者、双方にとって負担が大きい。本人から同意を取得することは、ビッグデータ活用における大きなハードルとなっている。

そこで改正法では、利用目的の特定や第三者提供の制限といった個人情報の取り扱いに求められる義務の適用外となるよう、個人が特定できないようにデータを加工処理した「匿名加工情報」という新たなパーソナルデータの区分を設けたのである。この匿名加工情報の作成方法は、新設される個人情報保護委員会が、基準を定めることとされている。

ただし、匿名加工情報であっても、外部のデータとマッチングすることによって、特定の個人が再識別されるリスクは残存する。また匿名加工の方法が分かれば、個人情報に復元することも容易にでき得る。このため、改正法では、匿名加工情報を他の情報と照合し

図1 匿名加工情報を利用するためのスキーム



て個人を識別する行為を禁止するとともに、加工処理の方法などの漏えい防止措置を図る、さらに事業者は匿名加工情報を取り扱うことについて公表する、という匿名加工情報の取り扱いに当たって求められる「規律」を法定している。

このように、匿名加工情報は、技術と法制度の両面から、特定個人が識別されるリスクを十分に低減することで、個人情報の取り扱いに係る一連の制約から解放され、本人同意がなくても、目的外利用や第三者提供が可能となるのである（図1）。

このような匿名化技術と法定の規律を組み合わせた枠組みで、パーソナルデータの流通を促進しようとする方策は、米国などで検討されているものの、実際に立法措置を実現したのは世界初で、かなり野心的な取り組みといえよう。しかし、前例がないだけに、加工処理はどの程度であれば十分と判断できるのか、特定個人を識別する意図のない他の情報とのデータマッチングは認められるのか、など不明な点が多い。本稿の後段では、こうした疑問に対し、実証研究を通じて得た知見を紹介する。

## II 匿名加工情報が 制度化される意義

### 1 加工しても残存する「識別リスク」

現状においても、名前や生年月日を削除するなど、個人を特定できないように個人情報を加工処理してビジネスに利用している事業者は多数存在する。しかし、加工処理の方法や程度には明確な基準がなく、各事業者がそれぞれ独自に判断しているのが実情であり、

それが妥当な加工処理なのかどうかは曖昧な状況にある。

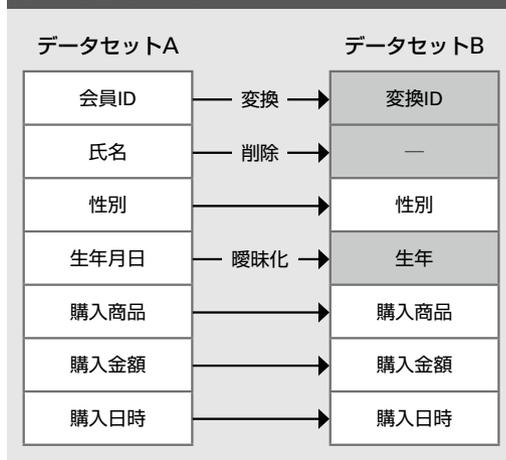
たとえば、購買履歴に関するデータセットAがあったとき、会員IDを他の番号に変換し、氏名は削除し、生年月日は生年に曖昧化するという加工処理を施すことで、データセットBにおける個人の特定性はかなり低減される（図2）。

しかし、会員IDと変換IDの対照表があれば、たちまちデータセットBにある個人を特定できてしまう。また、購入商品が珍しいものであったり、購入日時が限定的であったりすると、当該商品を購入した人物は限られるので、個人が特定されるリスクは高まる。さらに、データセットBを受け取った事業者が、自社で保有する顧客データベースと照合することで、個人を特定できる可能性もある。

これらの例からも分かるように、IDや氏名などを削除しただけでは、個人の特定リスクを排除することは難しい。「個人が特定できないように加工したパーソナルデータであっても、識別リスクが残存する限り、個人情報に求められる保護義務を免れることはできないのではないか」という論点は、パーソナルデータの利活用に対する非常に大きな阻害要因である。

匿名性を高めるには、「特定個人の識別につながる属性を削除する」「同じ属性を持つ人が複数いない場合はレコードを削除する」「ノイズを付加する」などのさらなる加工処理が必要となる。しかし、こうした処理はパーソナルデータの価値を損なうことになる上、手間もかかるため、事業者としてはなるべく簡便に抑えたいところである。

図2 加工処理の例



## 2 識別リスクの根底にある

### 「容易照合性」問題

この「識別リスク」問題の原因を突き詰めると、個人情報保護法における個人情報の定義に行き着く。

「個人情報」とは、生存する個人に関する情報であつて、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。）をいう。（個人情報保護法第2条第1項）

カッコ書きにある「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。」は「容易照合性」と呼ばれ、個人情報と非個人情報とを区別するための判断根拠として、重要な意味を持っている。その一方で、容易照合性の「容易」の判断には明確な基準がなく、どのような状態であれば、容易照合性が

ないといえるのかは、判然としていない。

先の例で見ると、ある事業者が、データセットAからデータセットBを作成し、データセットBを第三者に提供する場合、提供先の第三者はデータセットAへアクセスできないので、照合して個人を再識別することはできない。しかし、提供元の事業者はデータセットAも保持しているため、たとえアクセス制御がなされていたとしても、照合可能な環境はあるといえる。

また、提供先の事業者が、自社の顧客リストや外部の情報源から収集したデータと照合して、特定の個人を識別するリスクもある。SNSやスマートフォンが普及したことから、ネット上を流通するパーソナルデータは飛躍的に増大しており、外部のデータと突き合わせて個人が特定されるリスクが高まっている。

## 3 匿名加工情報は

### 容易照合性問題への答え

改正法で導入される匿名加工情報は、技術的に個人の特性を低減する手法の限界を踏まえ「識別を禁止する」「匿名加工情報の取り扱いを公表する」といった規律を組み合わせることで、容易照合性の問題を回避しようというものである。

従来は匿名処理したとしても、個人の容易照合性問題があるために、第三者提供すると個人情報保護法に抵触する恐れがあった。実際に、大手鉄道事業者が匿名処理したデータを販売しようとしたところ、個人情報の第三者提供に該当するのではないかという論争が巻き起こったことは記憶に新しい。

匿名加工情報の枠組みは、こうした匿名処理したデータの提供を合法的に行うことがで

きるようにするものである。また、改正法ではいわゆる「名簿屋」問題を封じるための厳しい規制が導入され、従来以上に外部の個人情報へのアクセスが制限されることになる。このため、匿名加工情報は、データ提供側、受領側双方にとって貴重なデータ流通手段となることが予想される。

また、匿名加工情報は利用目的の制限がないため、元の個人情報を取得した際に掲げていた目的とは別の目的で利用したい場合にも有効である。現状では、たとえ自社内であっても、個人情報である限り利用目的は制限され、漏えい防止のための安全管理措置も講じなければならない。しかし、一定の規律の下で匿名加工情報として取り扱えば、事業者はこうした制約から解放され、データをさまざまなビジネスへ適用できるようになる。

### Ⅲ 普及の鍵を握る事業者の自主的な取り組み

匿名加工情報を活用するためには、以下に示す改正法で規定された規律への対応が前提条件となる。

- 加工処理の方法は、個人情報保護委員会の規則に従う
- 個人情報保護委員会の規則を踏まえ、加工処理の方法などの漏えい防止措置を図る
- 匿名加工情報を取り扱うことを公表する
- 匿名加工情報は、他の情報と照合したりして個人を再識別しない

このうち、匿名加工情報を作成するための加工処理の方法や、加工処理の方法などの漏

えい防止措置は、新設される個人情報保護委員会が定める規則（以下「委員会規則」という）に従うこととされている。本稿執筆時点（2015年9月初）では、その内容は明らかになっていないが、すべての事業分野を包含するものとなるため、汎用性のある原則的な内容に留まることが予想される。

このため改正法では、事業分野ごとの特性に応じて、民間団体が自らルールを定めることのできる規定が設けられた。あくまでも委員会規則を踏まえることが条件となるが、民間が策定する自主ルールによるデータ活用の道が開かれたのである。なお民間自主ルールには、匿名加工情報の作成方法以外にも、個人情報の取り扱いに関するさまざまなルールを規定することができることとされている。

これは、改正法の基礎となった「パーソナルデータの利活用に関する制度改正大綱」（以下「大綱」）においてうたわれていた「民間主導による自主規制ルールの策定・遵守の枠組みの創設」に沿ったものであり、パーソナルデータの利活用促進とプライバシー保護の両立を意図している。

ところで一般に、民間自主ルールには、次のような構造的な問題が存在するため、実効性を担保することが難しいといわれている。

- 自主的にルールが作成されない
- 事業者がビジネスに都合のいいようにルールを作成する
- 自主規制に参加しない事業者が出る
- ルールの運用機関に中立性が欠けて、エンフォースメントが機能しづらい

こうした問題点を踏まえ、改正法では中立

的な機関によって、公正なルールが作成されて、きちんとした運用が担保される仕組みが考案された。以下では、民間自主ルールの策定・運用の手順を説明する。

## 1 認定個人情報保護団体を設立する

民間自主ルールを作成できるのは、公的に認定された「認定個人情報保護団体」である。現行の個人情報保護法においても認定個人情報保護団体は規定されており、2015年8月時点でさまざまな業界で41団体が認定されている<sup>注2</sup>。

現状の認定個人情報保護団体は、苦情の処理が主な役割であり、あまり目立たない存在である。しかし改正法により、民間自主ルールとなる「個人情報保護指針」を定めることができるようになり、一躍脚光を浴びることになった。

既に認定個人情報保護団体が設置されて機能している業界は、新たに設置する必要はない。しかし、いまだ認定個人情報保護団体のない業界において、民間自主ルールの枠組みを活用しようとするならば、まず、新たに団体を設立して認定を受けることから始めな

ればならない。

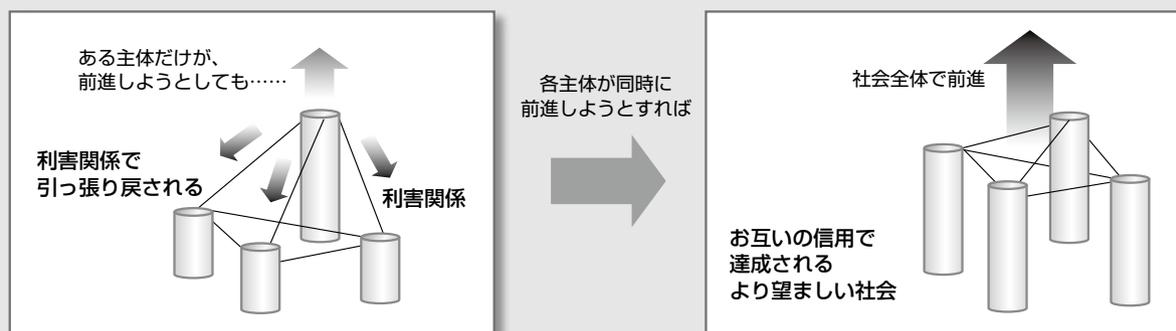
## 2 認定個人情報保護団体は、マルチステークホルダー・プロセスでルールを作成する

改正法では、認定個人情報保護団体は、「消費者の意見を代表する者その他の関係者の意見を聴いて」個人情報保護指針を作成するよう努めなければならないとされた（改正法53条第1項）。

この条文は、民間自主ルールの作成にマルチステークホルダー・プロセスの考え方を取り入れた内容である。マルチステークホルダー・プロセスとは、内閣府の定義によると、「3者以上のステークホルダーが、対等な立場で参加・議論できる会議を通し、単体もしくは2者間では解決の難しい課題解決のために、合意形成などの意思疎通を図るプロセス」のことである<sup>注3</sup>。同プロセスを活用することで、さまざまな意見を反映することができ、社会が一体となって全体最適を追求していくことができると考えられている（図3）。

マルチステークホルダー・プロセスへの期待は大きい。しかし、プライバシー保護の分

図3 マルチステークホルダー・プロセスでは、全体最適を追求する



利害のある主体間においては、ある課題解決に対し、「他者がやらないから自分もできない」といって、誰も行動できなくなる硬直状態が起きてしまうことがあります。そこで、その課題に関する全てのステークホルダーが、「他者もやると信じて、自分も行動する」と考え、一歩ずつ踏み出すことで課題解決できるようになります。

出所) 内閣府「持続可能な未来のためのマルチステークホルダー・サイト」

野では、同プロセスの実践は緒に就いたばかりであり、どのようにすれば全体最適につながっていくことができるのか、今後時間をかけて試行錯誤していくことになる。次章において、先行的に取り組まれた事例について詳述する。

### 3 個人情報保護指針を、個人情報保護委員会へ届出する

認定個人情報保護団体は、個人情報保護指針を策定後、個人情報保護委員会へ届出する。その後、個人情報保護委員会は届出された内容を公表し、晴れて自主ルールが運用が開始される。認定個人情報保護団体は、傘下の事業者に対して、個人情報保護指針を遵守させるため、継続的に監視して必要な指導を行うことが求められる。また、個人情報保護委員会は、認定個人情報保護団体がきちんと機能するよう、指導していくことになる。

この民間自主ルールを活用するスキームは、官と民による共同規制の一形態といえる。民間の自主ルールの運用に、個人情報保護委員

会が影響力を保持することで、事業者を間接的に律することになるからである（図4）。この自主規制に参加する事業者は、個人情報保護指針で業界の特性を反映したパーソナルデータ活用のルールを適用することができ、当該ルールを遵守している限り、個人情報保護委員会から直接的に執行される懸念が減じられるので、ルール参加に対するインセンティブが高まるという効果もある。

## IV 始まるマルチステークホルダー・プロセスによる民間自主ルール作り

マルチステークホルダー・プロセスを通じたパーソナルデータ活用のための民間自主ルール作りは、諸外国を見渡しても、未だ試行錯誤している段階にある。改正法の成立を機に今後、我が国においてもさまざまなルール作りが行われていく見込みであるが、パーソナルデータ活用による産業振興を主導する経済産業省では、いち早くマルチステークホルダー・プロセスの実証研究に着手している。

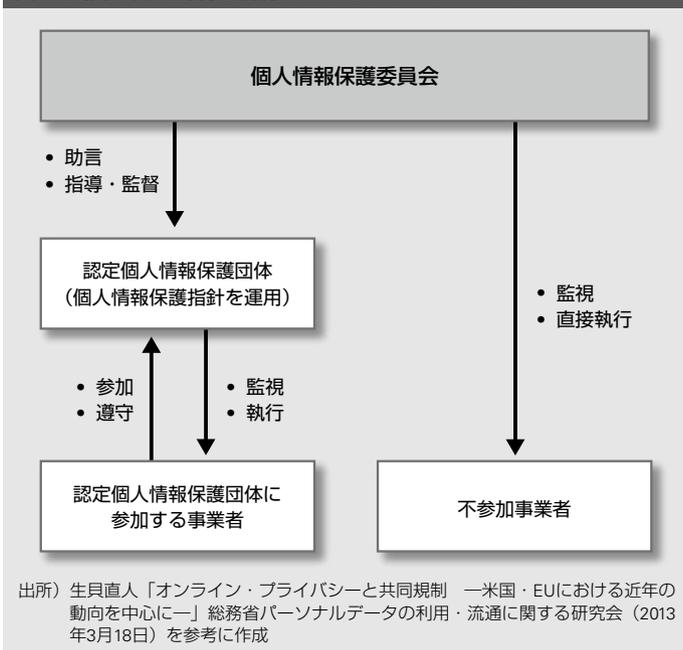
本章では、匿名加工情報の作成に係る先行研究の事例として、2014年度に野村総合研究所が経済産業省から委託を受けて実施した実証プロジェクトにおけるルール作りについて紹介する<sup>注4</sup>。

### 1 実証プロジェクトの概要

実証プロジェクトでは、クレジットカード業界における匿名加工情報の作成方法に関するルール作りを目的に、新たなデータ活用ビジネスを題材にして、主要なステークホルダーを集めた検討会を実施した（表1）。

検討会は、事業者、消費者代表、専門家

図4 民間の自主規制を機能させるためのスキームのイメージ



(法律、技術)を委員とし、政府機関をオブザーバーとした体制をとり、マルチステークホルダーによる構成とした。また事業者には、クレジットカード会社、加盟店、分析事業者を含め、クレジットカード業界としても、マルチステークホルダーとなるよう配慮した。

また、マルチステークホルダーで構成する検討会の諮問機関として、専門家(法律、技術)を中心としたアドバイザー会議を設置し、検討会で議論する題材を、専門的な見地から分析して助言する機能を有した位置づけとした(図5)。

## 2 ユースケースと主な議論

検討会に参加する事業者からの提案を受け、匿名加工情報を活用した具体的なユースケースを設定した。本稿では、そのユースケースの中から匿名加工情報の活用において重要な論点を包含する2つのケースを取り上げる。なおユースケースは、全て議論用の架空のものであり、実際に行われていないことに留意されたい。

### ケース1：ダイレクトメール送付先の抽出条件設定への適用

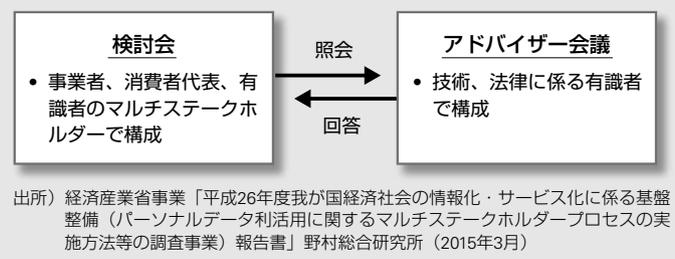
カード会社が、加盟店に対して提供しているダイレクトメール(DM)サービス<sup>注5)</sup>において、匿名加工情報を活用して、DMを送付する消費者を絞り込み、DMの効果を向上させることを目的としたケース。具体的なデータ授受の手順は次の通り。

- ①カード会社は、自社のデータベースから、匿名加工情報に加工された会員データリスト(匿名会員リスト)を作成する
- ②カード会社は、加盟店に対して匿名会員

表1 匿名加工情報の作成に係る実証プロジェクトの概要

| 目的   | 匿名加工情報の作成方法のルール作り   |
|--|---|
| 主催者  | 経済産業省   |
| 事務局  | 野村総合研究所   |
| 業界   | クレジットカード業界  |
| マルチステークホルダー・プロセス(検討会)・参加者の構成   | <ul style="list-style-type: none"> <li>・クレジットカード会社(4社)</li> <li>・加盟店事業者(1社)</li> <li>・データ分析事業者(1社)</li> <li>・消費者代表(2人)</li> <li>・法律専門家(2人)</li> <li>・技術専門家(1人)</li> <li>・政府機関(内閣官房、特定個人情報保護委員会、消費者庁、経済産業省)</li> </ul> |
| アドバイザー会議・参加者の構成  | <ul style="list-style-type: none"> <li>・法律専門家(2人)</li> <li>・技術専門家(4人)</li> <li>・事業者(1人)</li> </ul>  |
| 実施期間   | 2015年1月～3月  |
| <small>出所) 経済産業省事業「平成26年度我が国経済社会の情報化・サービス化に係る基盤整備(パーソナルデータ活用に関するマルチステークホルダープロセスの実施方法等の調査事業)報告書」野村総合研究所(2015年3月)を基に作成</small> |   |

図5 検討会とアドバイザー会議の関係



リストを提供する

- ③加盟店は、匿名会員リストを分析し、DMを送付したい見込み客層の抽出条件(性別、年代、居住地域、年間利用金額、会員種別)を考案する。なお分析時に、自社の顧客リストと突き合わせることは匿名加工情報の規律として禁じられる
- ④加盟店は、カード会社に対して考案した抽出条件を伝える
- ⑤カード会社は、加盟店が指定した抽出条件に基づき、実際にDMを送付する会員を抽出してDMを送付する

表2 アドバイザー会議からの助言（ケース1）

| 全体の評価      | 認められる（条件付）   |
|------------|--|
| 脅威分析       | ①識別：→リスクあり<br>②属性推定：→なし<br>③本人アクセス：→あり   |
| 技術面        | <ul style="list-style-type: none"> <li>カード会社から加盟店に提供している情報が、匿名加工情報なのであれば、「匿名加工情報の規律」（他の情報と照合禁止など）に従うこと</li> <li>カード会社から加盟店に提供している情報が、匿名加工情報でないのであれば、十分な匿名化（例：1,000&gt;k-匿名性<sup>注6</sup>）が必要（ただし、加盟店は提供後に匿名加工情報として自由に活用することが可能）</li> <li>どのタイミング（毎回、毎週、毎月）でk-匿名性を保証するのか</li> </ul> |
| 法制度面       | <ul style="list-style-type: none"> <li>カード会社から加盟店への情報提供は、「委託」なのか、「第三者提供」なのか要確認</li> <li>仮名化（k=1）で提供する場合、規律が正しく機能するために、カード会社が加盟店に対してどのような行為規範を設けるか</li> </ul>   |
| 備考（確認事項など） | <ul style="list-style-type: none"> <li>売上日と売上金額から該当する会員を一意に絞りきることができるか確認</li> <li>「住所」は特定の個人を識別できる記述なので、その一部にする必要があるか確認</li> <li>「DM抽出条件」はどのように指定するのか。（仮IDで、郵便番号と利用金額で、など）</li> </ul>  |

出所）経済産業省事業「平成26年度我が国経済社会の情報化・サービス化に係る基盤整備（パーソナルデータ活用に関するマルチステークホルダープロセスの実施方法等の調査事業）報告書」野村総合研究所（2015年3月）を基に作成

まずアドバイザー会議において、技術面、法制度面の両方からプライバシーリスクを検討し、リスクを軽減するための方策について助言をとりまとめた（表2）。全体評価は、条件付きながら認められるというものであった。

アドバイザー会議からの助言を受け、検討会では、事業者、消費者代表、専門家（法律、技術）、政府機関が、それぞれの立場か

ら意見を述べ、事務局においてケース1における消費者メリットとプライバシーリスクについてとりまとめた（表3）。

### ケース2：ダイレクトメール送付先の個別リスト抽出への適用

ケース1と同様に、カード会社が加盟店に対して提供しているDMサービスに、匿名加工情報を活用するものであり、DMを送付する消費者を、匿名会員リストから直接指定して、DMの効果を向上させることを目的としたケースである。具体的なデータ授受の手順は次の通り（図6）。

- ①カード会社は、自社のデータベースから、匿名加工情報に加工された会員データリスト（匿名会員リスト「データA」）を作成。この際、データAからは会員IDは削除し、代わりに会員IDと照合可能な仮IDを付与している
- ②カード会社は、加盟店（百貨店X）に対して、データAを提供する

表3 消費者メリットとプライバシーリスク（ケース1）

| 消費者メリット   | プライバシーリスク   |
|---|---|
| <ul style="list-style-type: none"> <li>顧客の属性や購買履歴に基づいて、顧客が関心を持ちそうな商品・サービスの案内に関するDMが届く</li> <li>・カタログ</li> <li>・割引クーポン</li> <li>顧客にとって意味のないDMの届く確率が減る</li> <li>加盟店における品揃えが、顧客ニーズに沿ったものになる</li> </ul> | <p>（個人の特定、識別リスク）</p> <ul style="list-style-type: none"> <li>加盟店に提供される「加盟店利用会員属性分析リスト」から、特定の個人が識別されるリスクがある</li> <li>・小さい加盟店の場合、顧客が少ないので、リストの対象が誰であるか分かる</li> <li>・高額商品の購入者や決済金額の大きい人などの該当者が少ない場合、リストの対象が誰であるか分かる</li> </ul> <p>（個人の属性が増えるリスク）</p> <ul style="list-style-type: none"> <li>カード会社の顧客DBに、DM送付した対象者であることを示す記録が付加される</li> </ul> <p>（本人へのアクセスに伴うリスク）</p> <ul style="list-style-type: none"> <li>DMが届く</li> <li>・クレジットカード会社からDMが届く理由・背景を理解していない場合は、不安に感じる</li> </ul> |

出所）経済産業省事業「平成26年度我が国経済社会の情報化・サービス化に係る基盤整備（パーソナルデータ活用に関するマルチステークホルダープロセスの実施方法等の調査事業）報告書」野村総合研究所（2015年3月）

- ③百貨店Xは、データAを分析し、DMを送付したい見込み客の仮IDを特定する
- ④百貨店Xは、カード会社に対して見込み客の仮ID（データA'）を伝える
- ⑤カード会社は、百貨店Xが指定した仮IDを会員IDと照合して、実際にDMを送付する会員を抽出して送付する
- ⑥～⑦は省略

ケース2に対するアドバイザー会議からの助言は、基本的にケース1と同様であった。しかし、検討会の場で議論している際に、⑤の行為は、匿名加工情報取り扱いの規律として禁じている「他の情報との照合による個人の識別」に該当するのではないか、という指摘がなされた。

理屈は次の通りである。百貨店Xはカード会社からデータAを受領するためには、匿名加工情報の規律を守らなくてはならない「匿名加工情報取扱事業者」となる必要がある。

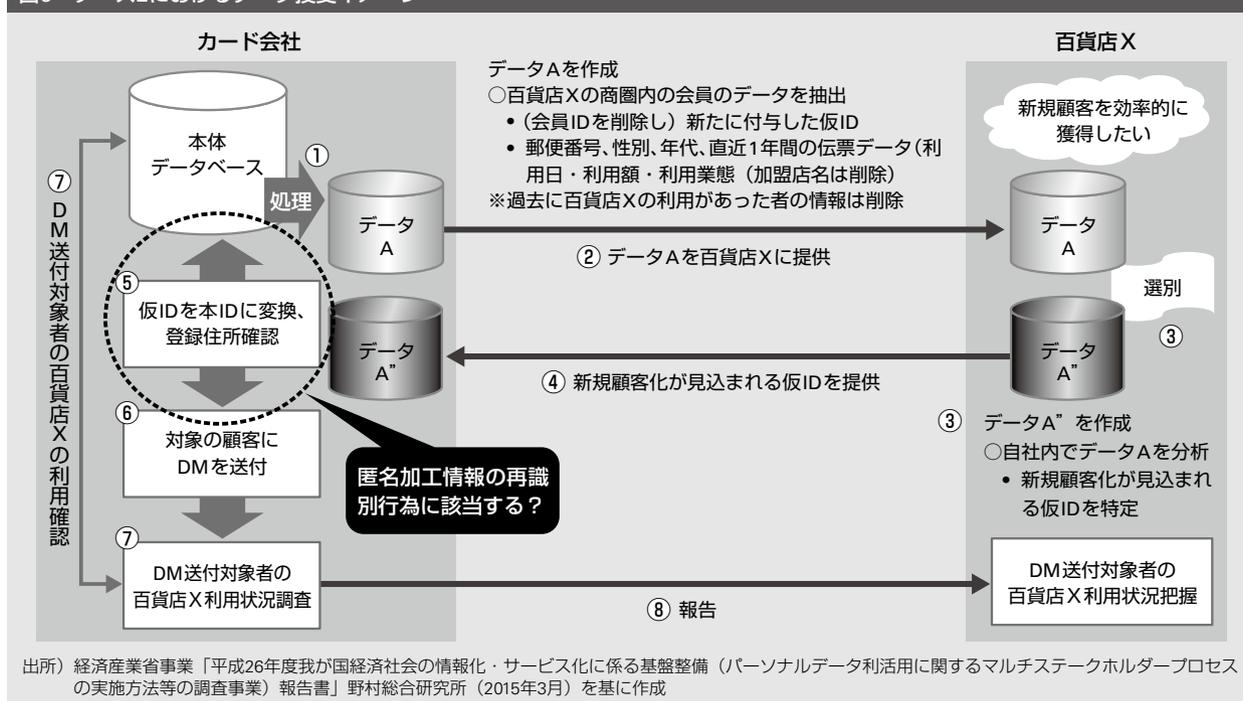
すると、百貨店Xがカード会社に仮IDを伝える行為が、カード会社への匿名加工情報の提供に該当するため、カード会社には、仮IDの扱いについて「他の情報との照合による個人の識別をしてはならない」という規律が課せられることになるというわけである。

このように、たとえカード会社が百貨店Xから受け取るデータの提供元が自社であったとしても、法令上は、一律に匿名加工情報の規律が課せられることになり、このケースは法令に抵触する可能性のあることが判明した。ただし検討会の場では、こうしたケースにまで、匿名加工情報の規律が課せられることに対して疑問を唱える声があった。

### 3 プライバシーリスクの考え方と匿名加工方法に関する留意点

アドバイザー会議では、ケース1の匿名加工の方法についてデータセットのイメージ（図7）をもとに検討を進め、プライバシー

図6 ケース2におけるデータ授受イメージ



出所) 経済産業省事業「平成26年度我が国経済社会の情報化・サービス化に係る基盤整備(パーソナルデータ利活用に関するマルチステークホルダープロセスの実施方法等の調査事業)報告書」野村総合研究所(2015年3月)を基に作成

リスクの考え方（脅威分析）（表4）を整理し、その上で、匿名加工方法に関する留意点（案）（表5）をとりまとめた。

以上述べた通り、実証プロジェクトでは、先ず専門家によるアドバイザー会議においてケースを分析し、「助言」として検討会へフィードバックした。次に、検討会では、助言を踏まえ、消費者のメリットとプライバシーリスクの両面について議論した。三番目に、検討会の議論を踏まえ、アドバイザー会議において匿名加工方法に関する留意点（案）を整理し、最後に再び検討会において、アドバイザー会議から呈された同案について討議して賛否を諮った。

このように検討の場を、マルチステークホルダーによる検討会と、専門家によるアドバイザー会議との二つに分け、相互に議論の到達点をフィードバックし合うことで、ユースケー

スについて理解を深めつつ、意見集約を図っていったのである。回を重ねる毎に論点が明確になり、議論もより深いものとなった。

とりわけ、アドバイザー会議が、有効に機能していたことが実証プロジェクトでは重要であった。アドバイザー会議が、技術と法律の論点を先行して整理することによって、検討会では、消費者のメリットとプライバシーリスク、そしてビジネスニーズの議論に集中することができた。また意見集約に当たって、アドバイザー会議が原案を作成して提示したことによって、検討会において賛否を諮ることができた。

本稿で紹介した実証プロジェクトはあくまでも実証研究であり、作成したルール（案）も極めて限定的なユースケースを対象としたものであるが、法改正を先取りして、未知の領域に挑戦した意義は大きい。実証プロジェ

図7 データセットのイメージ（ケース1）

|                | ID    | 氏名   | 性別  | 年齢         | 住所                     | 職業  | カード種別  | 加盟店           | 利用履歴   | 年間利用額      |
|----------------|-------|------|-----|------------|------------------------|-----|--------|---------------|--|------------|
| カード会社ローデータ     | 10001 | 野村○郎 | 男   | 28         | 埼玉県さいたま市<br>○○町1-6-5   | 会社員 | 一般     | 三越<br>新宿店     | 18,000円（2014年1月3日）<br>9,000円（2014年1月9日）        | 241,056円   |
|                | 10002 | 佐藤○郎 | 男   | 58         | 東京都練馬区<br>○○町5-8-13    | 公務員 | ゴールド   | 高島屋<br>新宿店    | 160,000円（2014年1月2日）<br>120,000円（2014年1月25日）    | 669,600円   |
|                | 10003 | 山田○子 | 女   | 42         | 神奈川県横浜市<br>港北区○○町9-3-1 | 自営業 | 一般     | 高島屋<br>二子玉川店  | 300,000円（2013年12月23日）<br>260,000円（2013年12月25日） | 4,320,000円 |
|                | 10004 | 曾我○子 | 女   | 37         | 栃木県さくら市<br>○○1210      | 会社員 | 一般     | ユニクロ<br>池袋店   | 9,200円（2013年12月20日）<br>9,200円（2014年1月20日）      | 107,784円   |
|                | 10005 | 大田○郎 | 男   | 66         | 山梨県甲府市<br>○○3-5        | 無職  | プラチナ   | ユニクロ<br>新宿西口店 | 50,000円（2014年1月2日）<br>30,000円（2014年1月3日）       | 108,000円   |
| ...            | ...   | ...  | ... | ...        | ...                    | ... | ...    | ...           | ...  |            |
| カード会社ローデータ匿名加工 |       | 仮名化  | 男   | 20代        | 埼玉県さいたま市               | 会社員 | 一般     | 百貨店           | 18,000円（2014年1月3日）<br>9,000円（2014年1月9日）        | ～50万円      |
|                |       | 仮名化  | 男   | 50代        | 東京都練馬区                 | 公務員 | ゴールド   | 百貨店           | 160,000円（2014年1月2日）<br>120,000円（2014年1月25日）    | 50～100万円   |
|                |       | 仮名化  | 女   | 40代        | 神奈川県横浜市                | 自営業 | 一般     | 百貨店           | 300,000円（2013年12月23日）<br>260,000円（2013年12月25日） | 400～450万円  |
|                |       | 仮名化  | 女   | 30代        | 栃木県さくら市                | 会社員 | 一般     | 衣料店           | 9,200円（2013年12月20日）<br>9,200円（2014年1月20日）      | ～50万円      |
|                |       | 仮名化  | 男   | 60代        | 山梨県甲府市                 | 無職  | プラチナ   | 衣料店           | 50,000円（2014年1月2日）<br>30,000円（2014年1月3日）       | ～50万円      |
|                |       | ...  | ... | 加工部分（k-匿名） | ...                    | ... | 加工（粒度） | 非加工（制限）       | ...  |            |

出所）経済産業省事業「平成26年度我が国経済社会の情報化・サービス化に係る基盤整備（パーソナルデータ利活用に関するマルチステークホルダープロセスの実施方法等の調査事業）報告書」野村総合研究所（2015年3月）

表4 プライバシーリスクの考え方（脅威分析）

データの第三者提供によるプライバシーリスクとして、「本人へアクセスされるリスク」と「不安感（気持ち悪さ）」の2種類に分けられる。後者は個人差があるため、前者についてのみリスクを評価した

**【性別、年齢、住所、職業、カード種別】**

- 組み合わせることで特定の個人を識別する可能性がある属性（性別、年齢、住所、職業、カード種別）は、k-匿名化<sup>注7</sup>または適切な加工処理をして、個人の特定性を低減する必要がある

**【加盟店】**

- 加盟店に関する情報（例：○○スーパー△△店）は加盟店の位置に関する情報を必然的に含むものである。位置に関する情報は、地図や住所録などと容易に照合できるため、本人へアクセスされるリスクがある。たとえば、利用頻度の高いコンビニは、自宅や職場などの推定につながる。このため、他の属性情報よりも、加工に当たって配慮が必要である

**【利用金額、年間利用額】**

- 外れ値を除くこと以外は、特に加工処理をしなくてもよい。たとえば、千円単位などに処理しなくてよい。位置情報などは異なり、照合対象のデータを外部から観察するのが困難なため<sup>\*</sup>、特定個人が識別されるリスクは高くない  
※照合表（匿名加工なしの元の表）が漏えいするとたちまち識別される。従って、適切な安全管理措置が必要
- 利用履歴の日時については、安全なレベルまで匿名加工すべき。①数年にわたる長期間の履歴の利用は脅威②履歴の期間が長いほど識別されやすくなる③短期間に集中して利用した場合識別されやすくなる

表5 匿名加工方法に関する留意点（案）<sup>注8</sup>

- 氏名は削除し、仮名化する（逆変換不能なIDを振る）
- 属性（性別、年齢、住所、職業、カード種別、加盟店）は、組み合わせることで特定の個人が識別される可能性があるため、次のいずれかの方法で加工処理をする。
  - ▶方法1：k-匿名化の加工処理をする。このときkの値は、データの特性に鑑みて設定する
  - ▶方法2：カテゴライズ化、曖昧化を行って、特定性の低減に寄与する妥当な加工処理をする
- 特に、加盟店については、住所や職場などのエリアが推定されないような配慮をする。
- 利用金額、年間利用額はトップコーディング、ボトムコーディングを行って、特異な値（外れ値）を除外する
- 利用履歴は、①利用期限を定める②履歴の期間の上限を決める、③履歴の回数の上限を決める、などを行い、制限を超えたものは削除したりIDを変えたりして、特定個人識別リスクを低減する

**（前提条件）**

- オリジナルのデータ、対照テーブルは、照合されないように適切な安全管理措置をとる
- 本事例においては、仮名化処理だけでは決して匿名加工情報に該当しない

クトでとりまとめられた知見は、今後さまざまな主体によるルール作りにおいて活用されることが期待される。

**注**

- 1 あらかじめ特定した目的の範囲内であれば、オプトアウト方式によって、第三者へ提供することは認められている
- 2 消費者庁ウェブサイト（<http://www.caa.go.jp/planning/kojin/ninteidantai.html>）による
- 3 内閣府「持続可能な未来のためのマルチステークホルダー・サイト」の定義による。<http://www5.cao.go.jp/npc/sustainability/concept/definition.html>
- 4 経済産業省事業「平成26年度我が国経済社会の情報化・サービス化に係る基盤整備（パーソナルデータ利活用に関するマルチステークホルダープロセスの実施方法等の調査事業）報告書」野村総合研究所（2015年3月）[http://www.meti.go.jp/meti\\_lib/report/2015fy/000296.pdf](http://www.meti.go.jp/meti_lib/report/2015fy/000296.pdf)

- 5 加盟店の販売促進を支援する、郵便や電子メールを使ったダイレクトメール受託サービス。クレジットカード会社の保有する会員データから加盟店の見込み客層を抽出することができる
- 6 「k-匿名性」とは、単独では個人を識別できないが、複数を組み合わせることで個人を高い確率で識別することが可能な属性（たとえば性別、年齢、居住地、職業など）について、どの属性値の組み合わせでも、対象とするデータ中に必ずk件以上存在する状態のこと
- 7 人口密度の高い地域や年齢層などにより、カテゴリーの大きさが変わるため、一様の加工は困難
- 8 必ずしも検討会委員全員の賛同が得られたものではないことに留意して参照されたい

**著者**

小林慎太郎（こばやししんたろう）  
 ICT・メディア産業コンサルティング部兼未来創発センター上級コンサルタント  
 専門はICT公共政策・経営