22-H006

パーソナル情報の利用のための
調査研究報告書

平成 23 年 3 月

財団法人日本情報処理開発協会

この事業は、競輪の補助金を受けて実施したものです。
http://ringring-keirin.jp

まえがき

本報告書は、財団法人日本情報処理開発協会が競輪の補助金を受けて実施した平成 22 年度「情報化推進に関する調査研究等補助事業「パーソナル情報の利用のための調査研究」の成果を取りまとめたものである。

通信技術の進歩やネットワークの進展、さらにはデバイス技術の高度化と各種端末の普及等により、世界中のあらゆるところで情報が生成、蓄積されており、個人の嗜好や行動といった情報（パーソナル情報）も同様に生成、蓄積されている。さらに、クラウド・コンピューティングを代表とする技術進展により、大量のデータを扱える土壌が整い、このような大量のパーソナル情報を有効活用し、パーソナライゼーションサービスを始めとした新たなサービスを展開することが盛んに検討されている。

一方で、このようなパーソナル情報から個人が特定されると、趣味趣向、財産や収入、行動パターンなど、他人には知られたくない個人のプライバシーに係る情報が流出する可能性がある。このため、パーソナル情報を活用するような新たなサービスを展開する際に大きな障壁となっている。

このような状況を鑑み、財団法人日本情報処理開発協会では、パーソナル情報認証スキーム検討委員会を設置し、「匿名情報の利活用に関する検討」、「視覚的に理解しやすい新オプトイン方式の検討」などについて取り組んだ。

本報告書は、上記に係る活動を中心に取りまとめたものである。本報告書が、パーソナル情報を利用したサービスを検討する企業・個人、パーソナル情報の利活用や安全性について研究を行う研究者に広く利用されることを希望する。その結果、議論が活性化され、情報産業の一層の発展に寄与することを願うものである。

最後に、パーソナル情報認証スキーム検討委員会の委員や調査にご協力いただいた方々に厚く御礼申し上げる。

平成 23 年 3 月

財団法人日本情報処理開発協会

パーソナル情報認証スキーム検討委員会　名簿

区分	氏名	所属
委員長	堀部　政男	一橋大学名誉教授
委員	岩田　修	NPO 法人個人情報保護有識者会議
委員	加藤　茂博	株式会社リクルート
委員	兼房　博司	凸版印刷株式会社
委員	狩野　昌央	エスト・メトリクス株式会社
委員	川上　正隆	株式会社電通
委員	小向　太郎	株式会社情報通信総合研究所
委員	佐久間　淳	筑波大学
委員	関　聡司	楽天株式会社
委員	中川　修	大日本印刷株式会社
委員	中村　洋一	茨城県立医療大学
委員	根来　龍之	早稲田大学
委員	牧野　二郎	牧野総合法律事務所
委員	松尾　正浩	株式会社三菱総合研究所
委員	村上　康二郎	東京工科大学

（順不同、敬称略）

目次

【サマリー】 1
1. はじめに 3
1.1 調査研究の背景 3
1.2 調査研究の目的 3
1.3 調査研究の方針 4
1.4 委員会活動 5
2. 調査事業について 7
2.1 調査の視点 7
2.2 調査項目 9
3. パーソナル情報の取扱いに関する国際動向 12
3.1 パーソナル情報の取扱いに関する各国の状況 12
3.2 各国のプライバシー・コミッショナー制度 15
3.3 各国のプライバシー関連法令 17
3.4 OECD、WPISP の検討状況 21
3.5 プライバシー・バイ・デザイン 35
3.6 まとめ 39
4. 匿名情報の利活用に関する調査検討 43
4.1 匿名情報の二次利用サービス事例 43
4.2 匿名情報の取扱いに関する認証スキーム事例 63
4.3 国内の個人情報ガイドラインと認証スキームの整合性分析 82
4.4 匿名化ツール事例にみる匿名性評価の指標 94
4.5 匿名情報を利活用するサービスモデルの検討 108
4.6 匿名情報利活用サービスに即した安全性およびトラストレベルの検討 148
4.7 匿名情報の利用を促進するための認証スキーム検討 179
5. 環境オプトインに関する調査検討 183
5.1 オプトイン、オプトアウトの文献調査 183
5.2 オプトインの先進的な事例の調査 188
5.3 新たに必要とされるオプトイン方式の定義 191
5.4 ユーザの受容性の調査 195
5.5 事業者の透明性確保の調査 196
5.6 新たなオプトイン方式（環境オプトイン）の成立要件の整理・分析 198
5.7 まとめ 209

【サマリー】

調査の背景と目的

近年、社会活動のあらゆる場面において大量の情報が「創出」、「蓄積」されている。その情報は、Web 上のデジタル情報にとどまらず、事業者内で作成されるデジタル情報、GPS を活用した位置情報・移動情報、デジタル TV 番組に関わる情報、個人の消費に関わる情報等、社会活動のあらゆる場面に及んでいる。また、パーソナル情報を収集した事業者が、自社の事業以外でこれを利用したり、他社への販売等を目的として流通させたりする、二次利用サービスについても一部検討が開始されている。

このような背景の中、産業界において行動履歴や視聴履歴のような情報を利用し、新しいサービスを創出しようとする機運が高まっている。他方、その具現化の過程において、「個人情報やパーソナル情報を加工し、非個人情報としてどのように扱うべきか」や「利用者に二次利用を行うことを受容してもらうために、何をすべきか」といった課題がある。

そこで、パーソナル情報を加工し非個人情報として利活用する際の「定量的な評価指標が組み立てられないか」、「認証などの制度的スキームが必要か否か」、およびパーソナル情報を収集する際に「視覚的に理解しやすいオプトインのような仕組みができないか」という三つの課題について、既存制度の拡充や必要な対策について具体化を検討、策定することを目的とした。

調査項目

パーソナル情報の利用を推進するための既存制度の拡充や必要な対策を検討するにあたり、事業者にとってのお墨付きとなる「匿名情報の保証」、匿名情報を利用する際の判断基準となる「評価基準の検討」、「効果的なオプトインの検討」という三つの視点を据えた。

まず、「匿名情報の保証」については、匿名情報の利活用に関し、各国の状況の調査を行い、匿名情報に関する安全性やトラストレベルを担保する認証機関を洗い出し、その詳細調査を実施して現状の動向を把握した。そして、これらの認証機関が利用するガイドラインや運用スキーム等について、国内の個人情報関連ガイドラインとの整合性について分析を行い、匿名情報の保証を行う認証スキームの在り方について検討した。

次に、「評価基準の検討」については、国内外の匿名情報の二次利用サービス事例の概要、取り扱うパーソナル情報の範囲、二次利用サービスの形態等を明らかにした。そして、国内外の匿名化関連ツールの匿名化手法と匿名化指標等を明らかにし、匿名情報利用における評価基準について検討した。

最後に、「効果的なオプトインの検討」については、現実空間での各種センサーやカメラによるデータ取得や、ICT サービスにおけるデータ取得の事例などを調査分析し、新たに必要とされるオプトイン方式を定義した。そして、新たなオプトイン方式が、ユーザに安心感を与え、信頼関係が成立するための課題を整理した。

匿名情報の保証

匿名情報を二次利用するサービスが創出される市場には、医療、金融、運輸、小売等が考えられるが、特に有望と考えられるのは、金融分野と小売分野である。

匿名情報の利用者は、パーソナル情報を匿名化して利活用したいと検討しているが、ユーザの信頼を得るために「匿名化したパーソナル情報の利用方法」や「匿名化の安全性」についての保証を必要としている。ガイドライン等で利活用のルールや指標を示すことで、情報流通が活発になり、市場が創出されると考えられる。

認証制度という面では、匿名情報の提供者は、元となる個人情報を保有しているため、P マークや ISMS を取得し、ユーザから信頼されていることが多いと考えられる。しかし、匿名情報の利用者が個人情報を保有していない事業者であるとき、情報利用者は適切な情報管理を実施していることについて第三者的な評価を受けていないと考えられる。そのような場合では、匿名情報の提供者が利用者のデータ管理能力について評価、承認しなければならないと考えられる。

評価基準の検討

匿名化したデータの評価については、匿名化評価ツールは運用される各国の法令等や利用ケースに影響されることが多く、匿名化評価指標に関する共通項は少ない。また、評価値については、経験に基づいて設定しており、定量的に明示することは難しい。

しかし、匿名化手法については、大域的再符号化や局所秘匿化など概ね共通していることが分かった。評価技術は、k-匿名性、l-多様性、t-近似性が広く認知されている。その中でも、k-匿名性は中心的な考え方であり、匿名化評価ツールでも採用されている。

匿名化手法については、標準的な規準を策定することができると考えられ、JIS 規格化や国際標準化を推進していくことが望ましいと考えられる。

環境オプトイン

技術の進展から各種センサーやカメラによるデータ取得など情報収集は実際に行われていることが分かった。また、デバイスからの情報収集については、オプトインは行っているものの、店舗等へ設置した機器による情報収集については、十分な告知が行われている状況ではないことが分かった。

一方、ユーザの受容性の面では、どのようなデータが取得されているのか分からないため不安感があり、特にセンシティブな商品や場所に関連する場合は抵抗感が高いことが分かった。

これらの結果を踏まえると、サービス業の進展や技術の高度化により各種センサーの利用はより進んでいくものと思われ、その場合に、来訪者に対して何らかの告知（環境オプトイン）は必要であると考えらえる。

1. はじめに

1.1 調査研究の背景

近年、社会活動のあらゆる場面において大量の情報が「創出」、「蓄積」されている。その情報は、Web 上のデジタル情報にとどまらず、事業者内で作成されるデジタル情報、GPS を活用した位置情報・移動情報、デジタル TV 番組に関わる情報、個人の消費に関わる情報等、社会活動のあらゆる場面に及んでいる。また、センサネットワークなどの発展によって、個人から発信される情報（パーソナル情報）が収集されており、個人の属性に着目したサービス（パーソナライゼーションサービス）が企業間連携の流れの中で拡大している。

また、パーソナル情報を収集した事業者が、自社の事業以外でこれを利用したり、他社への販売等を目的として流通させたりする、二次利用サービスについても一部検討が開始されている。特に医療分野においては、医療の効率化や研究等を目的として、各病院から収集した個々人の医療情報に匿名化等の処理を施したものが、研究者や政府機関において一部利用されている。また、我が国においても、平成 19 年度から平成 21 年度にかけて経済産業省が実施した情報大航海プロジェクト[1]において、パーソナル情報の利活用を想定し、制度的・技術的な検討を実施してきた。

パーソナル情報は散発的なものであり、それ自体は創造的行為ではないものが多く、事業者がそれを収集・編集・蓄積することによって価値を増幅させている。このようにパーソナル情報の利活用に関して検討が進められている一方、国内においては個人情報保護法等との関連から実際にビジネスを実施する例がほぼ無い[2]と言える。

そのような状況の中で、パーソナル情報に対して排他的権利（所有権など）を主張するのではなく、事業者と利用者の情報の非対称性のバランスを保ちつつ、個人の発する情報の経済価値を通じて社会価値を増幅させるための制度的枠組みを具現化することが喫緊の課題となっている。

1.2 調査研究の目的

当協会においても情報大航海プロジェクトに参画し検討を行ってきた。その活動から、産業界において行動履歴や視聴履歴のような情報を利用し、新しいサービスを創出しようとする機運が高まっていることが分かった。他方、その具現化の過程において、「個人情報やパーソナル情報を加工し、非個人情報としてどのように扱うべきか」や「利用者に二次利用を行うことを受容してもらうために、何をすべきか」といった課題があることも分かった。

前述のプロジェクトでは、集合匿名化という技術を用いてパーソナル情報を加工することを前提とし、そのような匿名情報を二次利用することについて定性的に判断するための「ガイドライン（案）」が策定された。また、その成果は、今年度設立された次世代パーソナルサービス推進コンソーシアム[3]の活動の中で、業界ガイドラインとして検討する動きが出ている。

---

[1] 平成 19 年度から 21 年度にかけて経済産業省が推進した、情報の種類に依らず大量の情報の中からユーザが求める情報を的確に検索・解析する共通技術（「知的情報アクセス技術」）の開発を目的としたプロジェクト

[2] 平成 22 年度は幾つか事例が出てきている。例えば、日経産業新聞 2010 年 8 月 16 日記事「サイト閲覧履歴、取引仲介」では、広告効果向上の支援を行うビジネスが報告されている。

[3] 個人に関する情報を利活用するための制度的・技術的な課題を検討するために、平成 21 年度に設立されたコンソーシアム

本事業では、これらの動きを受け、集合匿名化[4]されたパーソナル情報の「定量的な評価指標が組み立てられないか」、集合匿名化されたパーソナル情報を利活用する際の「認証などの制度的スキームが必要か否か」、パーソナル情報を収集する際に「視覚的に理解しやすいオプトインのような仕組みができないか」という三つの課題について、既存制度の拡充や必要な対策について具体化を検討、策定することを目的とする。

1.3 調査研究の方針

本調査研究では、情報大航海プロジェクトで検討された「パーソナル情報の利用」について課題となった点を中心に、個人情報保護およびプライバシー保護を行いつつパーソナル情報の高度な利用が促進されるような枠組みをまとめることを目標とする。

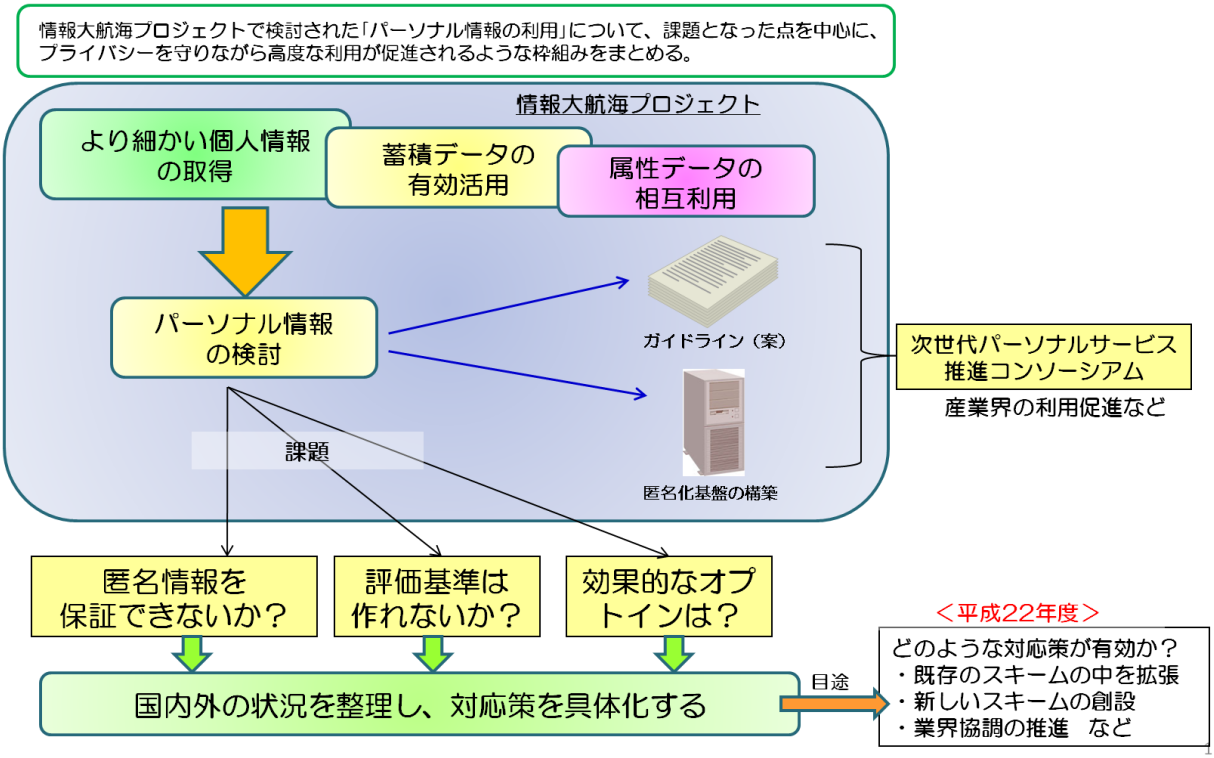

図 1-1　調査の概要

前述した「定量的な評価指標が組み立てられないか」、「認証などの制度的スキームが必要か否か」および「視覚的に理解しやすいオプトインのような仕組みができないか」という三つの課題に対し、それぞれ「匿名情報の保証」、「評価基準の検討」および「効果的なオプトインの検討」という調査の視点を設定し、国内外の状況を踏まえた対応策を具体化する。

[4] その個人の識別性を排除し、且つ一般化（抽象化）すること。（識別情報を加工（切り落とし、あいまい化など）し、開示リスクを考慮したアルゴリズムによって、グループ化すること）

表 1-1　調査の視点と実施項目

視点	実施項目	内容
匿名情報の保証	匿名情報を保証する仕組みについて検討する	1. 国内外の事例の調査 2. プロセスの分析 3. 我が国の各種制度との整合検討
評価基準の検討	匿名情報の定量的な評価軸の策定について検討する	1. ユースケースの収集と分析 2. サービス別、粒度別など分類の検討 3. 評価軸の策定
効果的なオプトインの検討	例えば、建物の入り口に目印を付けることで、その建物内でカメラや各種センサーにより行動履歴などを取得・利用することを理解させる仕組みについて検討する	1. 国内外の事例調査 2. オプトイン方式の骨子策定

「匿名情報の保証」については、Argus[5]（蘭）、CHEO[6]（加）など国内外の匿名情報を利用している事例を調査・分析し、匿名情報の利用においてどのように保証（安全性の担保の仕方、または安全性の担保が可能かの検討）しているかについて整理する。

「評価基準の検討」については、国内外の匿名情報流通における事例の調査・分析を基に、匿名情報の定量的な評価軸の策定について検討する。

「効果的なオプトインの検討」については、例えば建物等の入り口に目印を付けることで、その建物内ではカメラ映像や行動履歴などを利用することを理解させる仕組みについて検討する。本報告書では、このオプトイン方式のことを「環境オプトイン」と呼ぶこととする。

最後に、パーソナル情報の利用における課題への対応策を検討し取りまとめを行う。なお、対応策の検討にあたり、匿名情報利用のために認証スキームの検討結果から新しい認証制度が必要なのか、既存の認証制度の拡張で対応できるのか、または既存の認証制度を活用すれば対応できているのかを見極めることを主目的とする。また、活用促進にあたっては次世代パーソナルサービス推進コンソーシアム等の業界団体と協調しながら推進することとした。

1.4 委員会活動

本調査研究は、対象領域を俯瞰的・多面的に検討するため、異なる得意分野の有識者で構成されたパーソナル情報認証スキーム検討委員会を設置し、委員会での審議結果を参考に、事務局が取りまとめる形で報告書を作成した。ただし、本報告書の内容は、全てに渡って全委員の合意を得たものではなく、委員の意見を代表しているものでもない。文責は、あくまで事務局にある。

[5] オランダ統計局が採用している統計データ開示抑制を目的とした 2 つのソフトウェア・パッケージ
[6] Children's Hospital of Eastern Ontario

1.4.1 活動概要

パーソナル情報認証スキーム委員会は、有識者（15 名）、オブザーバ（7 名）、事務局（10 名）により構成され、4 回の委員会を開催した。

表 1-2　委員会一覧

開催	日程	議事内容
第 1 回	6 月 23 日	1.　開催要領 2.　今年度調査の全体像 3.　委託調査内容 ①「匿名情報流通に係る課題の調査」調査内容の提示 ②「匿名評価指標に関する調査」調査内容の検討 ③「環境オプトインに関する調査」調査内容の検討
第 2 回	8 月 23 日	1.　「匿名情報流通に係る課題の調査」の進め方 2.　「匿名情報流通に係る課題の調査」中間報告 ① 国内外のパーソナル情報の取扱いに関する認証スキーム調査 ②国内外のパーソナル情報の取扱いに関する認証スキームの詳細調査 3.　第 3 回委員会検討内容（案）
第 3 回	10 月 19 日	1.　「匿名情報流通に係る課題の調査」調査報告 2.　認証スキーム（案）策定に向けての検討報告
第 4 回	12 月 22 日	1.　匿名情報利活用に関する認証スキーム（案）検討 2.　環境オプトインのまとめ

2. 調査事業について

2.1 調査の視点

本調査事業における三つの視点ついて、詳細を以下に記す。

2.1.1 匿名情報の保証

パーソナライゼーションサービスでは、個人情報のみならず、多様なパーソナル情報を収集している。パーソナル情報を元の特定の個人を識別できない状態に集合匿名化を施した不可逆匿名情報（以下、“匿名情報”と呼ぶ）は、個人情報とは言えず二次利用が可能であると考えられる。しかし、情報提供者は匿名情報において自身のプライバシーが本当に守られているのか不安を感じている。匿名情報の利活用には、社会全体や利用者から個人を識別することなく、安全に利活用されているという信頼を得る必要がある。そのためには、匿名情報の安全性やトラストレベルを担保する認証（実施担保）が必要とされている。

しかしながら、世界各国を見ても匿名情報の二次利用についてその安全性やトラストレベルを担保する認証スキーム（以下、“匿名情報の認証スキーム”と呼ぶ）の事例は少ない。また、我が国においてもこのような制度的な仕組みは存在していない。

こういった状況を踏まえ、匿名情報の二次利用を検討する事業者にとっての後ろ盾となり、情報を提供する個人や情報を利用する事業者から信頼を得ることのできる実施担保の在り方について検討する。

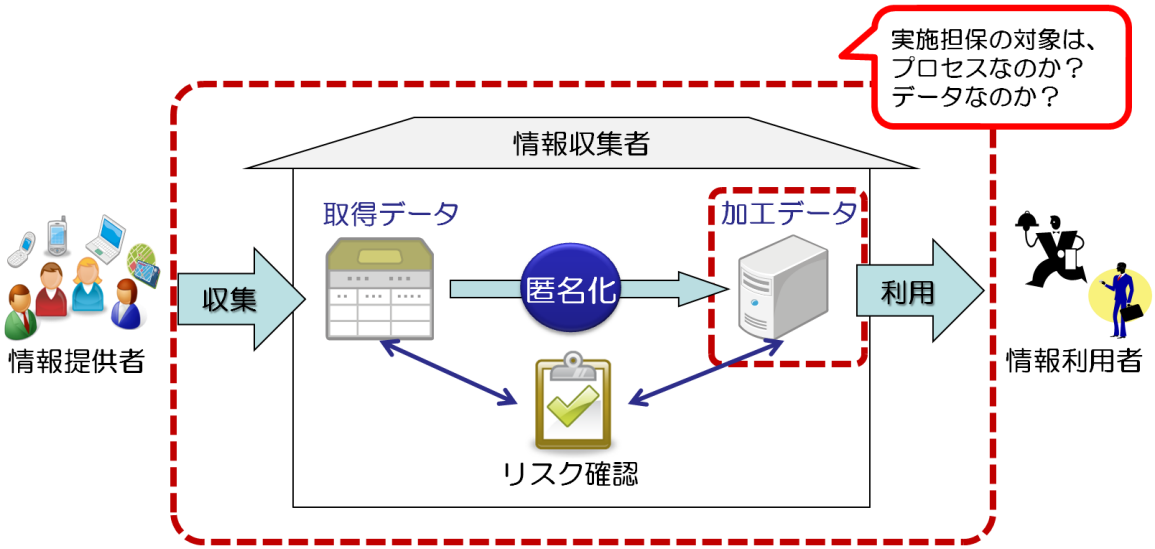

図 2-1　匿名情報保証の調査視点

2.1.2 評価基準の検討

我が国においては匿名化を行ったパーソナル情報を相互に流通させてビジネスを実施する例がほとんどない状況である。これは、実際にこれらのビジネスを実施している例をあまり知らないこと、匿名化技術についてその信頼性の指標等がよくわからないこと、ビジネスに関わった際

にどの程度の利益を得られるか不明確であること、などが挙げられる。

こうした状況を踏まえ、プライバシーを侵害する恐れがあるか否かを判断する匿名性の評価基準について検討する。

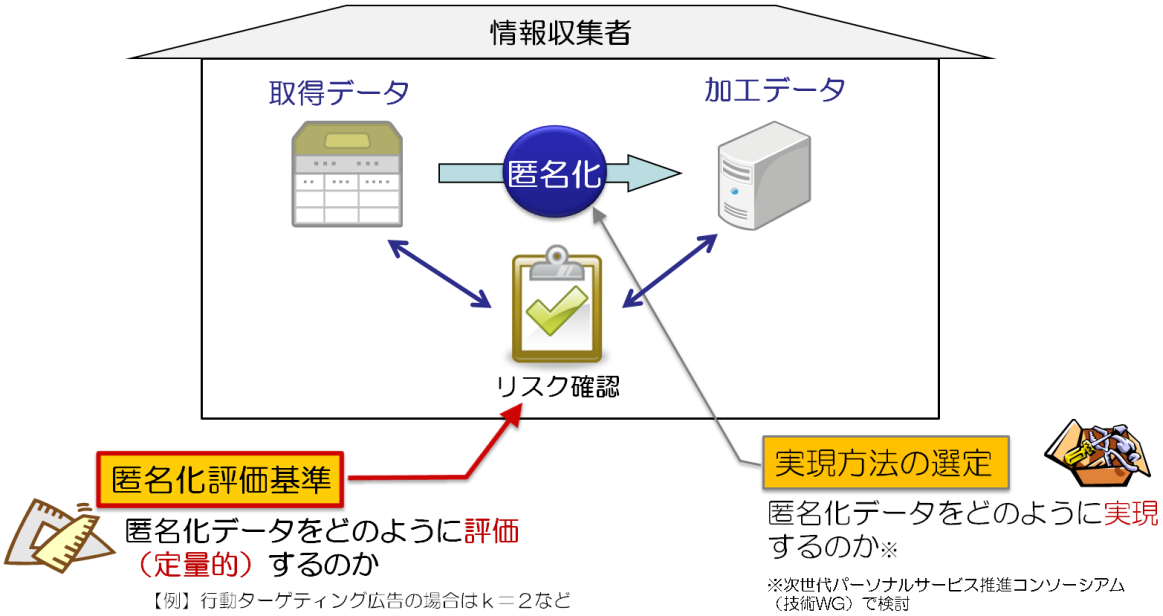

図 2-2　評価基準検討の調査視点

2.1.3 効果的なオプトインの検討

個人情報の利用については、事業者（情報収集者）と利用者（情報提供者）間でその利用に関する合意が必要であり主にオプトインによる合意確認で運用されている。また、事業者は、利用に関する約款の作成・メンテナンスや、約款の更なる告知の改善が行われている。一方、利用者は、専門家でない限り理解できない約款を読む場合は少なく、約款を読むこと無く利用の合意を行っている。この結果、事業者と利用者双方の信頼関係が十分ではなく、何かのきっかけによって訴訟にも至る不安定性もある。

また、IT の進展によって、各種センサー等を用いた狭域空間上での行動履歴や、購買履歴など本人を識別に至らないまでも、特定できる情報[7]の利用も始まっているが、何かのきっかけで個人が識別できる状態になった場合の対応の課題も指摘されている。

このような状況では、細かい約款を利用者に読んでもらう事は事業者にとって、大変負荷がかかることであり、利用者にとっても負荷のかかることである。

そこで、特定の環境において、誰もが「この事業者は、プライバシーに配慮して、安心安全にパーソナル情報をあつかっていること」が判る合意形成の概念（ここでは、“環境オプトイン”という）をまとめ、事業者と利用者の双方にとって信頼関係が確立、維持でき、両者の作業が訴訟リスクの低減に結びつく方法を検討する。

[7] 端末の識別 ID など、その情報単体で個人が識別できない情報では、第三者提供を含む二次利用が始まっている。

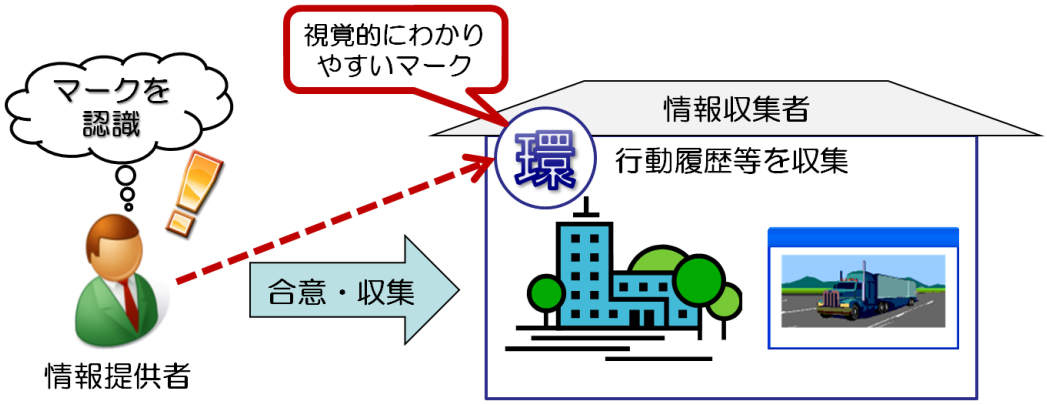

図 2-3　効果的なオプトイン検討の調査視点

2.2 調査項目

本調査事業における三つの視点に対し、設定した調査項目を以下に記す。

2.2.1 匿名情報流通に係る課題の調査

本調査では、匿名情報の利活用に関し、各国の状況の調査を行い、匿名情報に関する安全性やトラストレベルを担保する認証機関を洗い出し､その詳細調査を実施して現状の動向を把握する。そして、これらの認証機関が利用するガイドラインや運用スキーム等について、国内の個人情報関連ガイドラインとの整合性について分析を行う。また、我が国において匿名情報の認証機関を想定した場合に考えられる匿名情報の安全性およびトラストレベルについて、ケーススタディをベースに検討を行う。

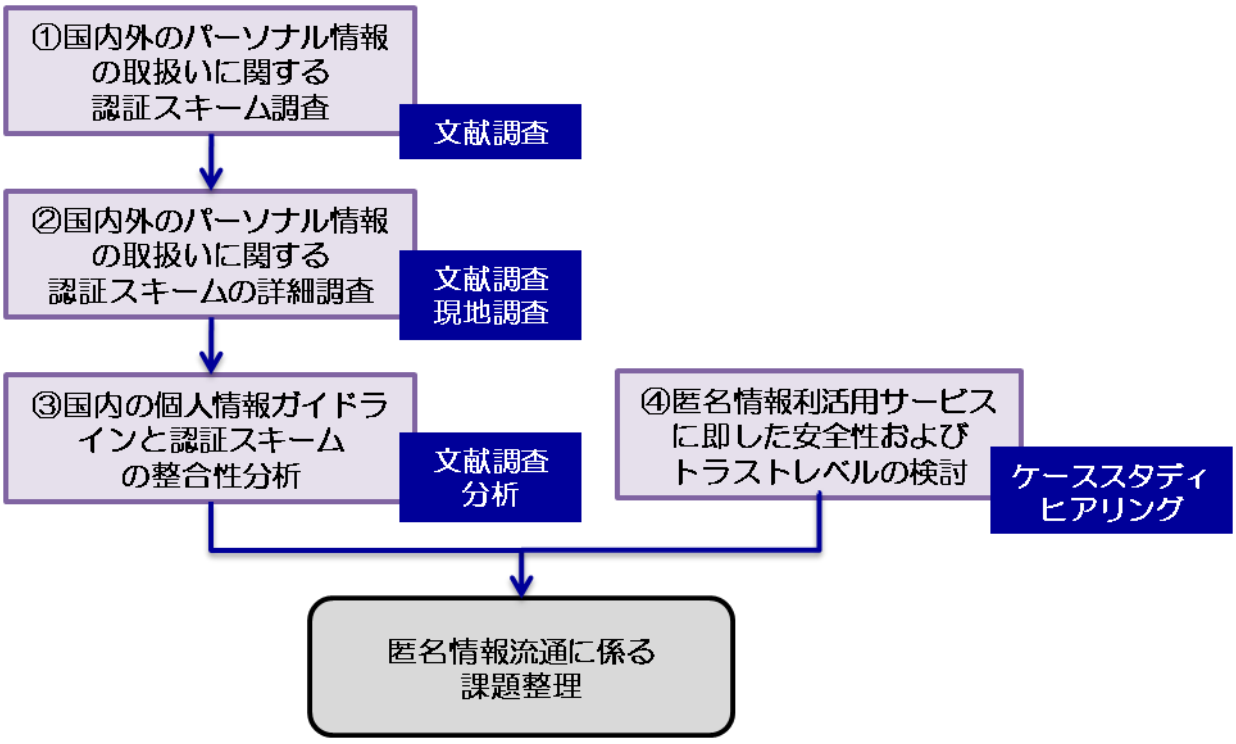

図 2-4　匿名情報流通に係る課題の調査方法

2.2.2 匿名評価指標に関する調査

本調査は三つのパートにより構成する（図 2-5 参照）。一つ目は、国内外の匿名情報の二次利用サービスの事例について、その概要、取扱うパーソナル情報の範囲、二次利用サービスの形態等を明らかにする。二つ目は、国内外の匿名化関連ツールに対して、その手法と匿名化指標等を明らかにする。三つ目は、匿名情報を利活用するサービスモデルを検討し、市場規模等の推計を行う。

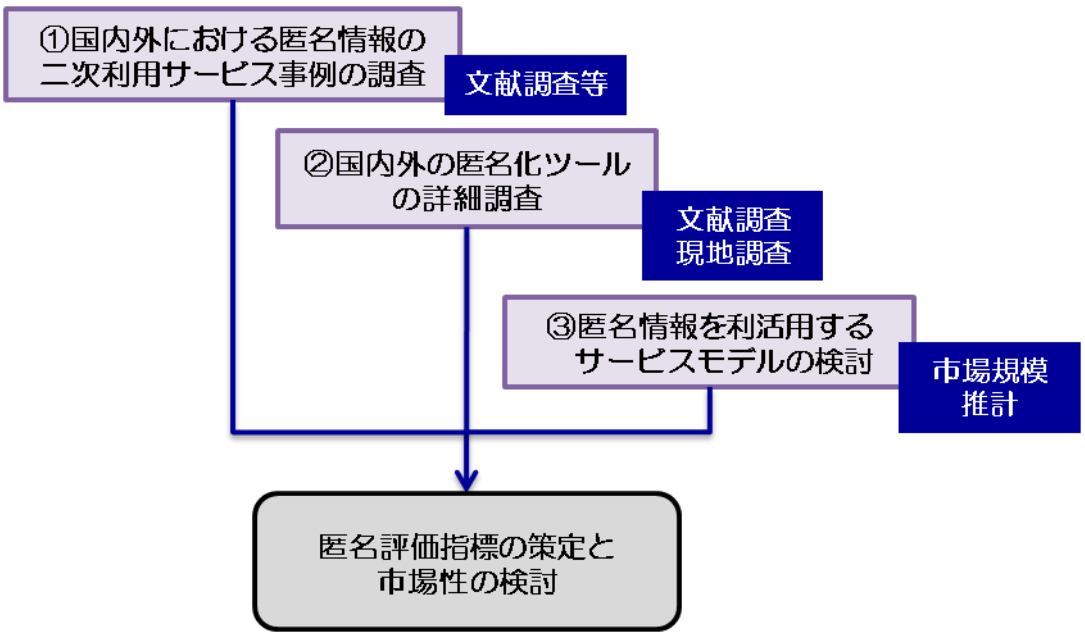

図 2-5　匿名評価指標に関する調査方法

2.2.3 環境オプトインに関する調査

本調査では、まず現状を整理するために、現実空間での各種センサーやカメラによるデータ取得や、ICT サービスにおけるデータ取得の事例など、①先進的な事例の調査を行う。また、この結果を用いて分析を行い、②新たに必要とされるオプトイン方式を定義する。ここで定義するオプトイン方式を、環境オプトインとする。そして、(A) ユーザの受容性の調査を行い、オプトインを実現する上での課題を整理する。特に、現実空間での各種センサーやカメラによるデータ取得に対するユーザの印象・安心感についてアンケートなども用いて調査する。また、(B) 事業者の透明性確保の調査を行い、事業者が必要とするパーソナル情報の項目についてヒアリング調査し、環境オプトインにおいて、ユーザに安心感を与え、信頼関係が成立するための課題を整理する。

以上の調査結果を踏まえて、現実空間での各種センサーやカメラによるデータ取得や ICT サービスにおけるデータ取得の際に、事業者と利用者の双方にとって信頼関係が確立し維持でき、両者の作業が訴訟リスクの低減に結びつく新たなオプトイン方式について要件をまとめる。

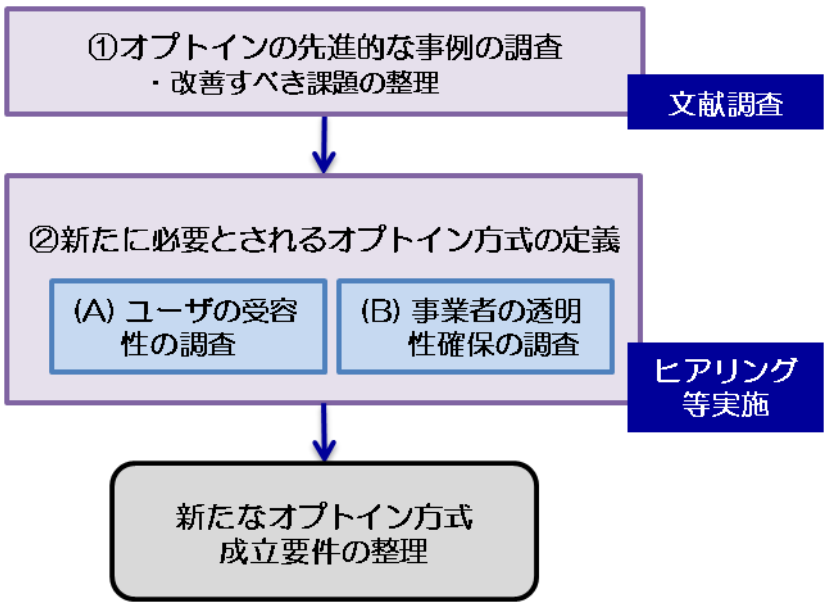

図 2-6　環境オプトインに関する調査方法

3. パーソナル情報の取扱いに関する国際動向

3.1 パーソナル情報の取扱いに関する各国の状況

本節では、パーソナル情報の取扱いに関して各国の状況を整理した。対象とする国は、パーソナル情報の利用が進んでいるカナダ、アメリカ、イギリス、オーストラリアとした。

3.1.1 カナダ

カナダでは、プライバシー関連の代表的な連邦法として、政府機関を対象とする Privacy Act、民間機関を対象とする Personal Information Protection and Electronic Document Act.(PIPEDA) があり、その実施状況を監督するプライバシー・コミッショナーとして Office of the Privacy Commissioner of Canada(OPC)[8]が設置されている。

医療分野では、オンタリオ州において Personal Health Information Protection Act. (PHIPA：個人医療情報保護法)[9]が制定されており、医療関連の研究者向けに医療個人情報の二次利用の認定を行うスキームが The Children's Hospital of Eastern Ontario(CHEO)[10]において実施されている（4.2.2 項参照)。

また、カナダ統計局のウェブサイト Statistic Canada において、いくつかのライセンス形態を提供し、ライセンス締結を結んだ業者に収集した統計データを提供するサービスを行っている。

金融分野における信用情報の取扱いについては、OPC が発行するガイドラインに基づき実施されることとなっている。

その他、The Canadian Institutes of Health Research(CIHR)、the Natural Sciences and Engineering Research Council(NSERC)、the Social Sciences and Humanities Research Council (SSHRC)の三機関で構成される Panel on Research Ethics (PRE)[11]より、調査対象に人間を含む研究倫理に関わるポリシーのガイダンスが提示されている。本ガイダンスの Article 10.3 の調査データには、個人の識別が可能な場合、そうでない場合の取扱いが記載されている。

3.1.2 アメリカ

Federal Trade Commissioner(FTC)[12]は、FTC Act.に基づき、民間で収集した個人情報をポリシーに違反して使用することを防止するとともに、Gramm-Leach-Billy ACT(GLBA)に基づき Financial Privacy のルール化を行っている。また、オンライン上での児童に関する情報の取扱いについて Children's Online Privacy Protection Act.(COPPA)も定めている。さらに、FTC では Fair Credit Report Act.(FCRA)に基づき、信用情報取扱機関(Consumer Reporting Agency：CRA)

---

[8] Office of the Privacy Commissioner of Canada
http://www.priv.gc.ca/index_e.cfm

[9] Personal Health Information Protection Act.(PHIPA)
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

[10] The Children's Hospital of Eastern Ontario(CHEO)
http://www.cheo.on.ca/

[11] Panel on Research Ethics
http://www.pre.ethics.gc.ca/eng/index/

[12] Federal Trade Commissioner (FTC)
http://www.ftc.gov/privacy/

向けのルールと規制を策定している。

Department of Justice(DOJ)の Chief Privacy and Civil Liberties Officer(CPCLO)の補佐を目的とする部局として、The Office of the Privacy and Civil Liberties(OPCL)[13]が設置されている。

米国の統計情報開示制御などを扱う Confidentiality and Data Access Committee(CDAC)[14]が、政府機関内の二次利用について SPW#22[15]に基づくチェックリストを公開している。

医療分野における個人の医療情報の取扱いについては、Health Insurance Portability and Accountability Act(HIPAA)に基づき、二次利用を行う場合には個人の特定ができないように De-Identification を行った上、実施することとなっている[16]。しかしながら、制度、ガイドラインとも標準が存在しないため、国の関与を望む声が上がっている。民間企業では、MedMining 社[17]が HIPAA よりも制約を強めた独自の運用を行い、製薬会社の研究用途に限定して販売している。MedMining 社は Honest Broker System という外部有識者を入れ透明性を高めている（4.2.3 項参照）。

金融分野では、収集した情報を利用し統計等を公表する事例がある。例えば、MasterCard 社の SpendingPulse[18]において、カードの利用状況から小売りの分析・予測レポートを発表している。また、Intuit 社の Mint.com ではオンライン家計簿情報から消費指標情報を作成するサービスを展開している。

その他、National Center for Supercomputing Applications(NCSA)では、各種ログファイルの匿名化を行う Framework for Log Anonymization and Information Management(FLAIM)というフレームワークを公開している[19]。また、Privacy Rulesets というユーザのプライバシープリファレンスを定義するドラフトが Center for Democracy and Technology(CDT)から出されており、W3C Privacy Workshop などで議論されている[20]。パーソナル情報の二次利用などについてもクリエイティブコモンズのように分かりやすい表示を推奨している。

3.1.3 イギリス

UK Ministry of Justice（司法省）がスポンサーである Information Commissioner Office (ICO)[21]が、The Data Protection Act.、The Freedom of Information Act.と関連の規制に基づき、Data Privacy に関する普及啓発、個別の問題解決、規制等を行っている。

---

[13] The Office of the Privacy and Civil Liberties
http://www.justice.gov/opcl/about-us.htm

[14] Confidentiality and Data Access Committee(CDAC)
http://www.fcsm.gov/committees/cdac/

[15] Statistical Policy Working Paper #22(SPW#22), Report on Statistical Disclosure Limitation Methodology
http://www.fcsm.gov/working-papers/spwp22.html

[16] HIPAA Privacy Rule and Its Impacts on Research
http://privacyruleandresearch.nih.gov/research_repositories.asp

[17] MedMining
http://www.medmining.com/

[18] MasterCard, SpendingPulse
http://www.mastercardadvisors.com/us/advisors/en/information_analytics/spendingpulse.html

[19] Framework for Log Anonymization and Information Management
http://flaim.ncsa.illinois.edu/

[20] W3C Privacy Workshop Day2 – 13 July 2010, Wrap-up discussion
http://www.w3.org/2010/07/13-privacy-minutes#item07

[21] Information Commissioner Office(ICO)
http://www.ico.gov.uk/

医療分野では、UK National The Health and Social Care Information Centre(NHS IC)において、医療情報の二次利用サービス Secondary Uses Service (SUS)[22]、および仮名化（匿名化）による医療データの二次利用を実現する Pseudonymisation Implementation Project(PIP)[23]を実施している。The Association of the British Pharmaceutical Industry(ABPI)[24]から ABPI Guidelines for the Secondary Use of Data for Medical Research Purposes[25]が発行されている。

社会科学系の調査データの集積・管理を行う Data Archives[26]では、これらの情報の二次利用サービスを展開しており、集積した調査データは必要に応じて匿名化処理が施される。

3.1.4 オーストラリア

オーストラリアでは、政府機関として Office of the Privacy Commissioner[27]を設置し、豪州におけるプライバシー関連の施策を統括している。

金融分野では、Credit Agency および Credit Provider が信用情報を取り扱う際に、Privacy Act. Part IIIA に示される基準に従うこととなっている。Privacy Act. Part IIIA では民間のクレジット会社が保有する信用情報は含まれないが、これらの企業は National Privacy Principles によって制限されることとなっている。

オーストラリアの統計局[28]では、Census データに関する任意の分析をオンライン上で実施可能な CDATA Online[29]サービスを提供している。また、Safe work Australia が各種統計データをオンラインで提供する On-line Statistical Database(NOSI)[30]を運用している。

また、オーストラリアでは、e-Health を推進している。医療情報 EHR の管理には Healthcare Identifier Service（2010 年 7 月 1 日稼働開始）を通して実施している。Healthcare Identifier Service は、Healthcare Identifier Act.に基づき実施されている[31]。

医学薬学研究に関する医療情報の取扱いについては、National Health and Medical Research Council(NHMRC)がガイドライン[32,33]を公開している。

---

[22] NHS IC Secondary Uses Service(SUS)
http://www.ic.nhs.uk/services/secondary-uses-service-sus

[23] NHS IC Pseudonymisation Implementation Project(PIP)
http://www.ic.nhs.uk/pseudonymisationworkshops
http://www.connectingforhealth.nhs.uk/systemsandservices/sus/delivery/pseudo

[24] The Association of the British Pharmaceutical Industry(ABPI)
http://www.abpi.org.uk/

[25] ABPI Guidelines for the Secondary Use of Data for Medical Research Purposes
http://www.abpi.org.uk/publications/pdfs/Guidelines_SecondaryUseData.pdf

[26] UK Data Archives
http://www.data-archive.ac.uk/

[27] Office of the Privacy Commissioner（豪）
http://www.privacy.gov.au/

[28] Australian Bureau of Statistics
http://www.abs.gov.au/

[29] CDATA Online
http://www.abs.gov.au/CDataOnline

[30] On-line Statistical Database (NOSI)
http://www.safeworkaustralia.gov.au/swa/AboutUs/Publications/DataandStatistics.htm
http://nosi.ascc.gov.au/

[31] Department of Health and Aging – Healthcare Identifier Service
http://www.health.gov.au/internet/main/publishing.nsf/Content/pacd-ehealth-consultation

[32] Guidelines under Section 95 of the Privacy Act 1988: privacy and medical research(March 2000)
http://www.privacy.gov.au/materials/types/download/8659/6503

[33] Guidelines under Section 95A of the Privacy Act 1988(December 2001)

3.2 各国のプライバシー・コミッショナー制度

本節では、3.1 節で概観した各国のプライバシー・コミッショナー制度について整理した。

3.2.1 Office of the Privacy Commissioner of Canada(OPC)（カナダ）

カナダ全州のプライバシー関連の問題を解決するために設置されたコミッショナーである。Privacy Act.および Personal Information Protection and Electronic Document Act.(PIPEDA)の遵守状況を監視し、問題発生時（苦情などが届けられた場合）には、仲裁・調停により問題解決をはかる。問題が解決しない場合には、証人喚問や証拠の提出等を求めることも可能な権限を有している。特に、民間向けのプライバシーに関する法令である PIPEDA に抵触した企業等に関しては提訴を行うこともある。

OPC では、プライバシー関連の問題を解決するほか、プライバシー関連の問題の調査およびその結果に関する公的機関および民間企業へのレポートの発行、Privacy Act.および PIPEDA に基づく監査、政府政策の Privacy Impact Assessment(PIA)のレビューと助言、個人のプライバシー権に関わる立法に関する分析と助言､ガイドライン発行等を含むプライバシーに関する普及啓発、プライバシー関連のトレンドの調査も実施している。

OPC では､プライバシーや個人情報に関しバランスある施策を実施するべく､オタワ大学教授、オタワ大学准教授、カナダ製造業者輸出業者連盟 CEO、ビクトリア大学教授、元最高裁判事などから構成される外部の助言委員会(External Advisory Committee)を設置し､ポリシーに関する助言等を受ける体制を構築している。

3.2.2 The Office of the Privacy and Civil Liberties(OPCL)（アメリカ）

Department of Justice(DOJ)の Chief Privacy and Civil Liberties Officer(CPCLO)の補佐を目的として設置された部局である。Privacy Act:1974 および E-Government Act:2002 とのコンプライアンスを含み、米国民のプライバシー保護および人権擁護に関わる調整等を実施する。具体的には、以下を実施する。

- プライバシーおよび市民的人権に関わる DOJ のポリシーの策定と改定
- 国際的なプライバシー関連事項の調査と政策（ポリシー）への反映
- 大統領および議会へのプライバシー関連の報告に関する監視・監督
- プライバシーおよび人権擁護に関連する DOJ の政策との調整
- プライバシーに関する定期報告書(Annual Privacy Report)を作成、公開

また、Privacy Impact Assessment(PIA)に関し、ガイダンスとテンプレートを作成・公開するとともに、DOJ の各部局が運営する情報システムの PIA を実施し、結果を公開している。

3.2.3 Information Commissioner's Office(ICO)（イギリス）

UK Ministry of Justice（司法省）がスポンサーである ICO が、The Data Protection Act.、The Freedom of Information Act.と関連の規制に基づき、Data Privacy に関する普及啓発、個別の問題解決、規制等を行う。Northern Ireland Office、Scotland Office、Wales Office の三つの

---

http://www.privacy.gov.au/materials/types/download/8660/6504

地方オフィスにより構成される。

ICO は、具体的には以下を実施する。

- 普及啓発活動
  - 個人および組織に関する問い合わせ
  - 組織向けの関連ガイダンスの作成
  - 個人の権利に関する情報提供
- 問題解決
  - Data Protection Act.および Freedom of Information Act.に関連する苦情等の解決
- 強制・規制
  - データコントローラの登録
  - Freedom of Information Act.に基づく情報公開の監視
  - 必要に応じて提訴
- Data Protection Act.および Freedom of Information Act.に関する影響の調査
- Data Protection Act.および Freedom of Information Act.に関するコンサルテーション

3.2.4 Office of the Privacy Commissioner(OPC)（オーストラリア）

Department of Prime Minister and Cabinet に設置されているが、独立に調整および政策助言を実施する独立機関である。Privacy Advisory Committee を有し、OPC への助言機能を保有している。Privacy and Freedom of Information Policy Branch と連携しながら、施策を実施する。

OPC では、Privacy Act:1988 に基づき、プライバシー関連の以下を実施する。

- 情報提供および助言提供
- 苦情等問題のハンドリング（調停等）
- 監査
- 普及啓発

OPC の Privacy Advisory Committee は、フリンダーズ大学教授、ニューサウスウェールズ大学准教授、ナショナル・オーストラリア銀行 Chief Privacy Officer、内閣 Privacy and FOI Policy Branch Assistant Secretary、オーストラリア連邦科学産業研究機構 予防医療国際研究フラグシップの Strategic Operations Director、タスマニア州反差別委員会委員の 6 名で構成され、幅広い視点から、プライバシーに関する方策上のアドバイスを行う。Privacy Advisory Committee は、OPC に対して以下の事項を実施する。

- プライバシーや個人情報保護に関する助言
- Privacy Commissioner によって遂行されるプロジェクトへの戦略的投入
- 個人のプライバシー保護の更なる促進のため、主要な利害関係者との協力関係を調整
- オーストラリアのコミュニティ、ビジネス、政府に対しプライバシーの価値を普及啓発
- 外部の利害関係者に対する説明責任のサポート

3.3 各国のプライバシー関連法令

本節では、3.1 節で概観した各国におけるプライバシー関連法令を整理した。

3.3.1 カナダ

(1) Privacy Act

政府機関で保有する個人に関わる情報（文書記録、ビデオ、コンピュータファイルを含む）に関して、情報提供者個人の保護と情報へのアクセスを目的とする。1982 年制定、1983 年施行。

特殊な場合を除き、個人情報を収集する際は個人にそのことを知らせなければならない。政府機関の管理下にある個人情報は、個人へ報告をしなければ収集した理由のためにしか使用できないし、公開することもできない。全てのカナダ住民、および永住者は政府機関の管理下にある自身の個人情報にアクセスする権利を持ち、情報が正確でない場合、変更を申請する権利をもつ。Privacy of Commissioner of Canada は「個人が自身の個人情報にアクセスできない」などの不満を受けた場合、調査することを法的に規定している。個人情報にアクセスすることを拒まれた個人は Office of the Privacy Commissioner of Canada(OPC)での手続きを経て証人喚問を行うことができる。OPC の活動を妨害した場合、$1,000 以下の罰金が科される場合がある。

例外として、公共の資料としての目的をもつ図書館や美術館の所蔵品、Canadian Broadcasting Corporation、the Queen’s Privy Council for Canada（カナダ枢密院）などが規定されている。

(2) Personal Information Protection and Electronic Document Act.(PIPEDA)

民間セクターにおける個人に関わる情報に関し、収集、利用と開示について規定することを目的とする。ただし、同等の法律をもつブリティッシュコロンビア州、ケベック州、アルバータ州、オンタリオ州は対象外である。2000 年制定。

個人情報の定義としては、個人を特定できる情報である。ただし、組織の従業員の名前、肩書、勤務先の住所や電話番号を除く。

PIPEDA 自体に法的拘束力はないが、OPC が調査をすることとなっている。OPC の勧告は必ず守られなくてはいけないわけではないが、申立人が訴えを起こす場合もある。

適用外となるのは、法的処置に関連した調査や緊急事態、Privacy Act が適用される政府機関、個人利用のために個人情報を使用する者、報道・芸術・文芸のみのために個人情報を使用する組織である。

(3) Personal Health Information Protection Act(PHIPA)

オンタリオ州における医療情報の収集、使用、公開について規定する。2004 年 11 月施行。

口頭、あるいは記述された形式で個人を特定できる情報を個人情報として規定し、その適用範囲は、オンタリオ州内の医療情報に従事する者、また医療組織外で個人医療情報を受け取る個人や組織であり、The Office of Information and Privacy Commissioner of Ontario (IPC)が監督を行う。法令が守られなかった場合、個人で$50,000 以下の罰金、個人以外で

$250,000 以下の罰金が科される場合がある。

適用外となるのは、the Quality of Care Information Protection Act, 2004 との整合性が取れない場合、法律によって個人情報の収集、使用、公開が必要とされる場合、研究目的の場合に医療個人情報の使用が認められるケースなどである。

(4) Personal Information Protection Act(PIPA)

ブリティッシュコロンビア州における個人の個人情報へのアクセスの権利や、ブリティッシュコロンビア州内の組織の情報収集、使用、公開について規定する。2003 年 10 月制定。

個人を特定できる情報を個人情報として規定し、従業員の個人情報を含む。その適用範囲は、ブリティッシュコロンビア州内の組織で、企業や非営利組織を含む。The Office of the Information and Privacy Commissioner for British Columbia(OIPC)が監督を行う。法令が守られなかった場合、個人で$10,000 以下の罰金、個人以外の者で$100,000 以下の罰金が科される場合がある。

適用外となるのは、報道・芸術・文芸が目的である場合、行政手続きに使用される場合、裁判所文書や起訴に関する文書に使用される場合などである。

3.3.2 アメリカ

(1) Privacy Act.

米国連邦政府機関によって維持管理される記録システムにおいて、収集、維持、利用、配布される識別可能な個人情報に関する法令である。情報提供者の明確な同意（書面）がない場合、例外を除いて、記録システムに記録された情報を開示することを禁じている。情報提供者個人の情報の閲覧および更新に関する手続きを各省庁に提供するように定めている。1974 年 12 月施行。The Office of the Privacy and Civil Liberties(OPCL)が所管する。

個人情報は、個人の氏名、ID 番号、シンボル、指紋・声紋・写真など個人を特定できるものが記された、学歴、金融取引、医療履歴、犯罪歴、職歴などを含むあらゆる情報である。

民事罰則と刑事処罰がある。組織が個人の情報を修正することを拒んだ場合、個人は民事裁判所にて訴えを起こすことができる。また、組織が故意に情報を公開した場合、$5,000 以下の罰金が科される。

Census Bureau と Bureau of Labor Statistics による統計目的、U.S. government agency 内での日常利用、「十分に歴史的、または U.S. government によって継続的に保護される価値があると認定された情報」の保存目的、法的措置の目的、アメリカ議会の調査目的、他の行政的目的など、12 の例外がある。

(2) E-Government Act.

連邦政府における電子政府サービスの運営と促進を向上させる目的で制定された。第 208 条では、全連邦政府機関において、識別可能な個人情報の収集・維持・配布を行う新規調達システムに対して、Privacy Impact Assessment(PIA)を実施することを求めている。PIA は、システムのライフサイクルを通したプライバシー保護を実現することを目的とし、識別可能な個人情報がどのように収集・蓄積・共有・管理されているかを分析する。2002 年 12 月制

定。

個人情報は、個人を特定できる情報とされ、法律の適用範囲は連邦政府機関である。

個人情報の公開が違法であると知りながら、情報を受け取る資格のない者に故意に情報を公開した場合、5 年以下の懲役、または$250,000 以下の罰金を科される場合がある。

書面による同意があれば、指定統計機関（商務省統計局、商務省経済分析局、労働省労働統計局）から他の指定統計機関へ個人を特定できる形で業務データを提供することは認められる。

(3) Gramm-Leach-Billy Act.(GLBA)

正式名称は The Financial Modernization Act である。1999 年成立。

Federal Trade Commissioner (FTC)が所管し、銀行、証券会社、保険会社といった典型的な金融機関だけでなく、様々な形態で金融商品および金融サービスを消費者に提供する企業に適用される。

ファイナンシャルプライバシールールおよびセーフガードルールにより構成される。ファイナンシャルプライバシールールは、法律が適用される機関が消費者に対して、収集する情報と共有に関してプライバシーに関する告知を行うこと、消費者は共有される情報を制限する権利をもつことを規定している。セーフガードルールは、法律の適用を受ける機関に対して、消費者個人の情報の守秘性および完全性を保護するセキュリティプラン策定の義務を規定する。

(4) Children’s Online Privacy Protection Act.(COPPA)

子供を持つ親に、自身の子供のどの情報がオンライン上で収集され、また、その情報がどのように使われているかのコントロール権を付与する法律である。1998 年成立。FTC が所管する。

この法律は、13 歳以下の子供から個人情報を収集する Web サイトや Web サービスのオペレーターに適用され、オペレーターは以下の義務を負う。

- サイト上のプライバシー・ポリシーに関するページを掲載し、個人情報を収集する全てのページからプライバシー・ポリシーにリンクすること
- 保護者に対してサイトにおける情報収集業務に関する告知を行い、子供から個人情報の収集を行う前に保護者から検証可能な同意を得ること
- 保護者に対して、子供の個人情報を第三者に開示してもよいか否かの選択肢を与えること
- 保護者に自身の子供の個人情報へのアクセス方法を提供し、子供の個人情報を削除する機会と、将来の個人情報の収集、または利用に関するオプトアウトを提供すること
- 子供が参加するゲーム、コンテストおよびその他の活動について、その活動に参加することに必要となる個人情報以上の情報を収集することを条件としないこと
- 子供から収集した個人情報の守秘性、完全性、セキュリティを維持すること

(5) Health Insurance Portability and Accountability Act(HIPAA)

医療情報の電子化の推進とそれに関係するプライバシー保護やセキュリティ確保について定めた法律である。医療情報は、個人の現在、過去、未来の身体的、精神的健康状態、個人に対するヘルスケアの提供とその医療費に関連する情報である。そして、医療情報は、口頭、あるいは書面に記載され、ヘルスケア提供者、医療保険、公共医療機関、雇用主、生命保険会社、学校や大学、ヘルスケア情報センターによって作られる、あるいは受け取られる。法律の適用範囲は、ヘルスケア提供者、健康保険、ヘルスケア情報センターである。法律の所管部署は、Office for Civil Rights(OCR)(U.S. Department of Health & Human Services)である。

法律が守られなかった場合、民事罰則として、一件につき$100～50,000 あるいはそれ以上の罰金が科される。ただし、一人に対する一年の罰金は$1,500,000 を超えない。また、刑事処分として、最低でも$50,000 以下の罰金、または一年以下の懲役が科される場合がある。

個人の許可なしで医療個人情報を使用できるケースがある。法律によって求められる場合、公共医療活動、裁判や行政の活動、法の施行、研究、必要な政府機能を目的とする場合、個人が死亡している場合などは適用を除外される。

3.3.3 イギリス

(1) The Data Protection Act.

自身に関する情報について、組織等の保有状況を知る権利、ならびに、これらの情報を適切に扱うことを確実にするルールを定める。認めがたい苦痛や損害が生じると認められる場合、個々人が、データコントローラに対してデータ処理を行わないように要求することができる権利も認めている。1998 年制定。Information Commissioner Office(ICO)が所管する。

個人情報は、生存する個人に関わる全ての情報である。その情報によって個人を特定できる場合、またその情報と、情報を操作するものが持っている、あるいは手に入れることのできるほかの情報によって個人を特定できる場合も含まれる。

個人情報について何らかの処理を実施する組織全てがその適用範囲となる。

故意に違反が行われた場合、または重大な損害につながる可能性を知っていた（あるいは知っているべきであった）場合、ICO は金銭的罰則を科す権利をもつ。

国家の安全、犯罪や課税、医療・教育・社会活動、報道・文学・芸術、研究・歴史・統計などの目的では、例外が認められる場合もある。

(2) The Freedom of Information Act.

公的機関が保有する情報を、特別な事由がある場合を除いて、取得することができる権利を定める情報公開に関する法律である。2005 年施行。

公的機関および公的企業がその対象となり、ICO が所管している。

ICO からの忠告等に従わなかった場合、高等法院に事案が報告され処理されることとなる。

セキュリティに関する問題を扱う情報、裁判所の記録に含まれる情報、上院や下院によって保持される情報で、その公開が公共の事柄の効果的な実施に損害をもたらす場合は、適用を除外されることもある。

3.3.4 オーストラリア

(1) Privacy Act.

個人情報に関する収集、利用と開示、精度、安全な管理および情報提供者自身のアクセスを規定する。健康および医療情報はセンシティブデータとして分類し、特別な処置を求めることを規定する。1988 年制定。

真偽を問わず、個人の身元が明らかとなっている、または合理的に解明されうる、個人に関する情報や意見は全て個人情報とされる。州政府および北部地域の政府機関、および一部の民間セクターを除く政府機関および民間セクターがその適用対象となり、Office of the Privacy Commissioner(OPC)が所管している。

OPC からの質問に答えない場合、最高$2,000 の罰金、または 1 年の懲役が科される。

医療関連研究を目的とする場合、研究者が個人を特定できないように施せば、医療個人情報を扱うことを認められる場合がある。

3.4 OECD、WPISP の検討状況

本節では、パーソナル情報の取扱いに関して、OECD の検討状況を整理した。対象とする領域は、Committee on Information, Communications and Computer Policy（以下“ICCP”）の管轄下にある、Working Party on Information Security and Privacy（以下“WPISP”）における動向とした。

3.4.1 これまでの経緯

OECD が 1980 年に制定した「プライバシー・ガイドライン」は、我が国における個人情報保護法制をはじめ、先進国を中心とした諸外国の法制度および民間企業・団体の自主規制ルールの参照元として、今日に至るまで位置づけられている。一方で、制定から 30 年を経て、インターネットや移動体通信網の発達等、情報通信技術の高度化を踏まえた改訂の必要性が近年指摘されていた。こうした機運を受け、検討部会に位置づけられる WPISP では、個人情報・プライバシーに係る現状動向の把握や法制度のあり方について､ここ数年の間にわたって検討を重ねてきた。

特に契機となったのは、2009 年 6 月にポルトガル・リスボンで開催された大規模ワークショップ（Using Sensor-Based Networks to address Global Issues: Policy Opportunities and Challenges：センサベースネットワークの利活用に係る国際的課題：政策立案の可能性と挑戦）[34]である。このワークショップでは、センサネットワークをはじめとした情報発信・収集の多様化に伴う、経済・技術・制度などの議題が採り上げられ、当初は WPISP で行われていた議論をより具体化すべく、WPISP からのスピンオフという形で進められた。また開催前年に発生したいわゆる「リーマン・ショック」と称される経済危機を受け、経済開発に関するテーマも同時に議論する必要があるとの OECD 側の判断により、WPISP の上部組織である ICCP の主催という構成となり、同分野の事業展開等に関する議論と同時に、プライバシーやセキュリティに関する議論を行う場として位置づけられた。

[34] http://www.oecd.org/document/41/0,3343,en_2649_34223_42616233_1_1_1_1,00.html

このワークショップには、日本からも経済産業省・情報大航海プロジェクトが参加し、研究開発の成果として、モバイルや医療を応用分野とした大規模データの利活用に係る発表を行い、高い評価を得た。またその際に設定された他の議題も含めて、広義のプライバシー情報（註：日本の個人情報保護法で定義される個人情報を包摂する）の利活用と規制のあり方について、単に規制を強化するだけでなく、経済合理性の観点からも評価が必要であるとの見解が WPISP の中でも一般化した。

こうした経過を踏まえ、その後の WPISP 定例会合では、プライバシー情報のあり方について、規制と利活用の両面から検討が進められてきたが、そうした方向性を決定づけたのが、2010 年 10 月にイスラエル・エルサレムで開催された会議（Conference on the Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines：進化するプライバシー保護の役割＝プライバシー・ガイドライン制定から 30 年を迎えて）[35]と、同年 12 月にフランス・パリの OECD 本部で開催された WPISP と WPIE(Working Party on Information Economy)共催による会議（The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guideline：パーソナルデータとプライバシーの経済学＝ガイドライン制定から 30 周年を迎えて）[36]である。以下にその概要をまとめる。

3.4.2 エルサレム会議

(1) 概要とプログラム構成

OECD プライバシー・ガイドライン（いわゆる 8 原則を含むガイドライン）が制定されてから 30 周年にあたる 2010 年は、合計 3 回にわたって、それを記念する会議や講演が開催された。[37]そのうちイスラエル・エルサレムで 2010 年 10 月に開催された 2 回目の会議（Conference on the Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines：進化するプライバシー保護の役割＝プライバシー・ガイドライン制定から 30 年を迎えて、以下“エルサレム会議”）は、各国・地域のデータ保護機関のデータ保護プライバシー・コミッショナーにより、データ保護およびプライバシーに関する議論を行う目的で毎年開催される、いわゆる「プライバシー・コミッショナー会議」と連続する形で、各国のコミッショナーをはじめとしたプライバシー政策担当者や企業担当者を対象として開催された。

[35] http://www.oecd.org/document/44/0,3746,en_2649_34255_45780844_1_1_1_1,00.html
[36] http://www.oecd.org/document/22/0,3746,en_2649_34255_46565782_1_1_1_1,00.html
[37] http://www.oecd.org/document/35/0,3746,en_2649_34255_44488739_1_1_1_1,00.html

表 3-1　エルサレム会議　-プログラム構成-

	セッション名
1 日目 10/25（月） 18:00-20:00	オープニングセッション： （インターネットという）文脈におけるプライバシー・ガイドライン Opening Session: The Oecd Privacy Guidelines in Context
2 日目 10/26（火） 9:00-18:00	セッション 1： 人間による人間のデータ生成と共有 Data Creation and Sharing by Individuals about Individuals
	セッション 2： 集約と分析：個人プロファイルの構築 Aggregation and Analytics: Constructing an Individual　Profile
	セッション 3： 認知、理解、人間の意志決定 Awareness, Understanding, and Individual Decision-Making
	セッション 4： プライバシー保護技術の促進 Fostering Innovations in Privacy Protection
	セッション 5： 政策形成の考察 Implications for Policy Making
	クロージング

(2) オープニングセッション

1 日目は実質的なオープニングセッションで、全体のアジェンダ整理が行われた。具体的には、1）包括的なデジタル化された記憶（蓄積情報）がプライバシーのトレンドにどのような影響を及ぼすか、2）どのような（インターネット以外の）要素がプライバシー保護に影響を与えているか、3）プライバシー保護の視点を喚起するための考察として、どのようなプライバシー規律が提示されるべきか、それに向けたチャレンジにはどのようなものがあるか、といったアジェンダが提起された。

セッションには、以下のパネリストが参加した。

- アンドリュー・ワイコフ（OECD、科学技術産業担当ディレクター）
- ジェフリー・ローゼン（米国、ジョージ・ワシントン大学法学部教授）
- キャメロン・ケリー（米国商務省、ジェネラル・カウンセル）
- ヤンキ・マーガレット（アラジン・ナレッジ・システムズ社、創業者兼前 CEO）
- マリエ・シュロフ（ニュージーランド、プライバシー・コミッショナー）
- ジェニファー・ストッダート（カナダ、プライバシー・コミッショナー）

またセッションの最後には、イスラエルのネタニエフ首相が会場を訪れ、祝辞とプライバシー検討に関する短い講演を行った。

図 3-1　エルサレム会議・1 日目の様子

(3) 人間による人間のデータ生成と共有

2 日目の第 1 セッション「人間による人間のデータ生成と共有」では、30 年前の制定当時と現状の情報環境の差異を明らかにしながら、OECD プライバシー・ガイドラインが今後どのように変化していくべきか、といった趣旨のディスカッションが行われた。

具体的には、30 年前には情報の生成者は企業や政府等が中心だったものの、近年はインターネットにおける UGC や SNS の台頭などにより、個人が中心となったことを踏まえ、1）プライバシー情報の生成に係る現状のトレンド、2）企業や団体等が個人に係る情報の収拾や管理等に責任を持っている状態で、個人情報の保護やプライバシーの保護をどのように実現すべきか、3）個々人がプライバシーに対する気構えとして確証できるアプローチはどのようなものか、といった検討が行われた。

セッションには、以下のパネリストが参加した。

- ナターシャ・ピルク・ミューサー（スロベニア、情報コミッショナー）
- ジョシュア・カウフマン（米国、ハーバード大学、デザイン大学院）
- キャセイ・チャペル（ボーダフォン、グローバル・プライバシー・カウンセル）
- タイ・ミョン・チュン（韓国、成均館大学、情報通信工学部教授）
- エリザベス・デンハム（カナダ、ブリティッシュコロンビア州プライバシー・コミッショナー）
- ピーター・スワイア（オハイオ州立大学法学部教授）

(4) 集約と分析：個人プロファイルの構築

第 2 セッション「集約と分析：個人プロファイルの構築」では、インターネットやモバイル環境で、最終ユーザがあまり注意を払わない微細な個人情報も、その集積と分析によって個人プロファイルを構築可能な現状を示した上で、こうした状況とどのように向かい合うべきかを論じた。

具体的には、1）集約と分析の鍵となるトレンドや、組織がこうした情報を監視・生成で

きる実際の可能性、２）個人の断定と特定可能性に関わらず、どのようにその状態を定義するのが最適か、また技術がそれを可能にする時、どの時点でそれを明確化すべきか、３）こうした裁断された情報の集積がその範囲を広げる時、プライバシーという概念は成立するのか、といった議論が行われた。

セッションには、以下のパネリストが参加した。

- ダニエル・ワイツナー（米国、商務省国家通信情報局、アソシエイト・ポリシー・アドミニストレーター）
- オマー・テネ（イスラエル、イスラエル・法学マネジメント大学、シニア講師）
- アレキサンダー・ディクス（ドイツ、ベルリン州データ保護・情報の自由・コミッショナー）
- グス・ホサイン（プライバシー・インターナショナル、シニア・フェロー）
- ベッツィ・マシエロ（グーグル、ポリシー・マネージャー）
- リチャード・トーマス（情報ポリシー・リーダーシップ・センター、グローバル戦略アドバイザー）

(5) 認知、理解、人間の意志決定

第３セッション「認知、理解、人間の意志決定」では、データ利用の複雑化が進むにつれてプライバシー・ポリシーの表現が困難になり、最終ユーザのプライバシーに対する態度と実際の行動が対立・矛盾しかねない状況と、それを伝えるための方法・手段のそもそもの難しさを踏まえ、ユーザ個々人がどのように意志決定を行っているか、そしてそれを今後のプライバシー向上にどのようにつなげるかが議論された。

具体的には、１）人間は彼ら自身の情報がどのように使われ、またどのようなステップで保護されていると理解するのか、２）個々人は web サイトやマーケティング担当者が彼らのデータを使うことについて、費用便益の観点での評価をする動機があるのか、あるいはそれは可能なのか、３）情報の開示と保護の望ましいバランスを実現するには、市場原理、技術、政策立案のどれが、どのように有効か、といった議論が行われた。

セッションには、以下のパネリストが参加した。

- ペーター・ヒュスティンクス（欧州データ保護スーパーバイザー）
- アレッサンドロ・アクイスティ（米国、カーネギーメロン大学・ハインツカレッジ、助教授）
- アンナ・フィールダー（市民社会・情報社会アドバイザリー・カウンシル、シニアメンバー）
- モーゼル・トンプソン（米国、フェイスブック、アドバイザー）
- ビヨルン・エリク・トン（ノルウェー、データ保護調査部、ジェネラル・ディレクター）
- アラン・ウェスティン（米国、コロンビア大学法学部教授）

(6) プライバシー保護技術の促進

第 4 セッション「プライバシー保護技術の促進」では、アイデンティティや評判を管理するツール、リアルタイムの注意喚起、プライバシーダッシュボード（集中管理）、匿名ルーティング、プライバシーや嗜好性に関するデータの上書き等、インターネットおよび関連技術がもたらす新たなプライバシー保護技術の可能性を指摘し、1990 年代の PET(Privacy Enhanced Technologies)に比べてより進化した現状をどのように使いこなし、また促進していくかが議論された。

具体的には、1）技術イノベーションはユーザ個々人に、プライバシー情報へのアクセスと管理について、具体的にどのような容易性をもたらしたか、2）こうしたツールが普及する際のインセンティブと障害は何か、3）プライバシー保護のフレームワークにおいて、技術イノベーションの役割はどのようなものか、といった議論が行われた。

セッションには、以下のパネリストが参加した。

- ヨラム・ハコエン（イスラエル、情報・技術当局、法務責任者）
- ユリス・ポレネツキー（フューチャー・オブ・プライバシー・フォーラム、ディレクター）
- ダナー・ボイド（ハーバード・ベルクマン・センター、アシスタント研究員、マイクロソフト・リサーチ、シニア研究員）
- マリト・ハンセン（ドイツ、シュレスウィグ・ホルスタイン、プライバシー・情報副コミッショナー）
- デビッド・ホフマン（米国、インテル、セキュリティ・グローバル・プライバシー・ディレクター）
- クリスティン・ルネガー（ISOC、公共政策シニアマネージャ）

(7) 政策形成の考察

第 5 セッション「政策形成の考察」では、全体のまとめとして、人間のプライバシーを保護するための政策形成に係る幅広い考察が、OECD のみならず、APEC や欧州委員会、Global Privacy Enforcement Network 等の NGO 等の観点から、行われた。

具体的には、1）政策担当者はネット上の個々人の振る舞いやプライバシーに対する考え方から何を学んだか、2）プライバシー保護の役割が変わるなか、ビジネスや組織の役割はどのように変化するか、3）彼らの変化はプライバシー保護やプライバシー規律にどのような意味を与えるのか、等が議論された。

セッションには、以下のパネリストが参加した。

- アン・カーブラン（OECD、科学技術産業担当特別カウンセラー）
- ジョゼフ・アルハデフ（オラクル、CPO、OECD ICCP ビジネス・アドバイザリー委員会委員長）
- マリー・ヘレナ・ブランジェ（欧州委員会、法務部、データ保護部代表）
- 宮下紘（消費者庁、駿河台大学准教授）
- ヨルグ・ポラキエウィク（欧州議会、法改正部代表）

- マーク・ロテンベルグ（EPIC エグゼクティブ・ディレクター、市民社会・情報社会アドバイザリー・カウンシル、ステアリング・コミッティ・メンバー）
- デビッド・ウラデク（米国、FTC、消費者保護局、ディレクター）

(8) 全体の所感

エルサレム会議は、プライバシー・コミッショナー等、比較的高レベルの意志決定者を対象としていることもあり、詳細な個別論の検討というよりは、世界的なプライバシーを取り巻く動向の全体感の把握を重視しているように感じられた。その観点で、各セッションに共通していたのは、2009 年（マドリッド）や 2008 年（ストラスブール）でのプライバシー・コミッショナー会議等でも散見された、SNS 等の新しいネットサービスを「プライバシーの脅威」と見なす認識から、共存に向けた妥協点を探る動きへと、トレンドがシフトしているように感じられた。

実際、Facebook やグーグルに対する批判は一部には根強いものの、それを全否定するのではなく、それらを積極的に利用しているユーザのプライバシー意識はどのようなものか、またそういったユーザがどうすれば正確に現状把握ができるようになるのか、といった、現状を現実的に踏まえた上での議論に方向づけられることがほとんどであった。

その中で大きなトレンドとしてあげられるのは、１）透明性（トランスペアレンシー）の確保、２）プライバシー・バイ・デザインの推進、３）プライバシーと産業の協調、といったキーワードであった。特に２）については、プライバシーアセスメントの方法論、といった一般的な表現ではなく、「プライバシー・バイ・デザイン」と名指しで採り上げられることが極めて多かった。これは、欧州委員会での検討等で同フレームワークがすでに浸透しつつあること、また前述の通り北米などでは事業者にもフレームワークとして認められつつあること等が背景にあるものと考えられる。

また１）透明性の議論の延長で、プライバシーマークのような認証プログラムとそのアイコン化の必要性を説く参加者も少なくなかった。これは、プライバシーに関する技術やサービス、また人々の意識が複雑化する中で、プライバシー・ポリシーという条文ベースでは機能が破綻しかかっていること、また一方で一定のスタンダードが必要であろう、という認識に起因するものであった。なお、こうした発言について、会議では直接名指しはされなかったものの、コーヒーブレイク等で発言者に真意を確認すると、ほぼ例外なく JIPDEC のプライバシーマークを念頭に置いていることが分かった。

こうした中で、個人情報匿名化に関する議論は、全体の中で一つの手段として位置づけられて、それぞれのセッションで触れられていた。ただしそれは、体系的に定義された状態での議論ではなく、あくまで個人の特定（大規模データベースの統合による推定も含む）の可能性を回避するための手段として考慮する必要がある、という程度の位置づけであった。したがって、その技術的方法論や法的な確実性等に関する言及は特に行われなかったものの、概念的にその必要性が認められたという意味で、従来に比べより積極的に位置づけられるようになった、と考えられる。

3.4.3 パリ会議

(1) 概要とプログラム構成

2010 年 12 月にフランス・パリの OECD 本部で開催されたラウンドテーブル（The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guideline：パーソナルデータとプライバシーの経済学＝ガイドライン制定から 30 周年を迎えて、以下“パリ会議”）は、OECD プライバシー・ガイドライン制定 30 周年にあたる 2010 年に、合計 3 回にわたって開催された会議や講演の最終回となった。

今回のパリ会議は、OECD/WPISP の定例会合と連続する形で開催された。したがって参加者は、WPISP の活動に従来から関係している、各国政府代表や、ISOC 等の協力機関、学術団体、また民間企業等のプライバシー政策担当者等が対象となった。

表 3-2 パリ会議 -プログラム構成-

	セッション名
12/1（水） 9:30-18:00	セッション 1： 大量データと国際流通 Big Data and Global Flows
	セッション 2： オンラインサービス・金融サービスにおけるパーソナルデータの価値 Valuing Personal Data in Online and Financial Services
	セッション 3： 医療・健康セクターにおけるパーソナルデータの価値 Valuing Personal Data in the Health Sector
	セッション 4： プライバシー・ビジネス The Business of Privacy

(2) 大量データと国際流通

大量データと国際流通の加速について、原則としてそれを肯定する立場から、その現状と課題の整理が行われた。具体的には、1）大量データとその分析による活用が当然のものとなっているという現状認識の確認、2）グローバルなビジネスや経済全体を支えている中、人間はその鍵を握る関係者（提供者）となっていることへの理解の必要性、3）現代的な技術と計算機資源は、こうしたデータの問題を無害化し、大量データを前提とした意志決定を可能としているという事実の確認、4）一方で大量データそのもののリスクや、大量データ同士が連結された時の危険性への注意喚起、等が議論された。

セッションには、以下のパネリストが参加した。

- ジェフ・ジョナス（IBM チーフ・サイエンティスト、IBM エンティティ分析グループ）
- ケネス・クキエ（ザ・エコノミスト編集部、日本ビジネス・金融担当）
- ジョン・ボスウェル（SAS、最高法律責任者）
- マーク・ラトウシュ（シスコ、インターネットビジネスソリューション、ディレクター）

- ヴィクトル・メイヤー・ショーンバーガー（オックスフォード・インターネット研究所教授）
- 東條吉朗（経済産業省、情報処理振興課長）

この中で、オープニングプレゼンテーションを務めたジェフ・ジョナス氏(IBM)は、大量データはそれだけでは単なるデータの集合に過ぎず価値に乏しいが、それを解釈するための文脈（コンテキスト）が付与されることによって価値が顕在化すること、そして大量データの取得と利用が容易に可能となった現在、どうコンテキストを形成するかがむしろ重要となっていることを提起した。一方これに呼応する形で、ヴィクトル・メイヤー・ショーンバーガー氏（オックスフォード・インターネット研究所）は、大量データを価値化するコンテキストとしてメタデータの重要性を指摘し、その把握や形成が重要であることとの見解を示した。

一方、東條吉朗氏（経済産業省）は日本の取り組みとして、大量データの必要性が日本でも十分認識されていることと同時に個人情報／プライバシー法制との協調の難しさを指摘し、その課題解決の一案として日本では匿名化技術の開発を進めていること、またこうした技術的取り組みと Privacy by Design のコンセプトとは親和性があることを指摘した。

この東條氏からの指摘にはモデレータのケネス・クキエ氏（エコノミスト誌）から「非常に興味深い」との反応が得られ、その後の全体ディスカッションとして、誰がデータを制御するかという議論が非常に難しいものであることを踏まえた上で、規制当局の姿勢やユーザの信頼を得ることの必要性について議論が行われた。特に後者については、社会実験の重要性と、データ流出(data breach)の危険性への対策が必要である、と結論付けられた。

(3) オンラインサービス・金融サービスにおけるパーソナルデータの価値

大量データが自在に流通することで大きな価値が得られている代表的なセクターとして、オンラインサービス（Web サービス）と金融サービスを挙げ、その最新動向、課題、事業者の見解について整理が行われた。具体的には、１）当初取得されたのとは異なる領域でのデータ利用がすでに一般化しつつあるという現状認識の整理、２）その中でオンラインサービスと金融サービスがそうしたデータ利用を付加価値としており、消費者へも利益還元しているという事実の確認、３）一方でユーザがその流通の自由度に懸念を示しつつあるという課題提起、４）現状に対する事業者としてのスタンス、等が議論された。

セッションには、以下のパネリストが参加した。

- キャサリン・タッカー（米国、マサチューセッツ工科大学スローンスクール教授）
- ジェーン・ハミルトン（カナダ、インダストリー・カナダ、電子商取引政策）
- ベッツィ・マシエロ（米国、グーグル、ポリシー・マネージャー）
- ガブリエル・デ・モンテサス（スウェーデン、ハイメディアグループ、戦略・コーポレイトファイナンス担当上級副社長）
- マーティン・アブラムス（情報政策リーダーシップセンター、上級ディレクター）
- クリス・グラシオン（オーストラリア、ベダアドバンテージ、渉外担当）
- ジョンワ・チョン（韓国、国民銀行、CRM チームリーダー）

まず、オープニングプレゼンテーションを務めたキャサリン・タッカー氏（マサチューセッツ工科大学）から、プライバシー情報の利用は新しくてまだ規制されていない（あるいはやや無法な）領域であることを指摘し、その利用が爆発的に拡大していること、一方で利用そのもののみならず、そうした実態さえもよく分からないほどのスピードで利用が拡大していることへの懸念があることが示された。それに対し、ベッツィ・マシエロ氏（グーグル）は、データが世界を変えることをグーグルという企業が体現してきたことの事実と、未来は誰も予測できない以上、安易な規制は経済発展を阻害するという趣旨の指摘がなされた。

一方でガブリエル・デ・モンテサス氏（ハイメディアグループ）は、こうした大量データを利用するというアプローチは金融サービスに源流があること、それは古くは 1930 年代の sucker list（DM 規制）、あるいは 1960 年代のクレジットヒストリーの分析に端を発していること、そしてそれが資本市場のみならずローンのような一般向けの金融商品でもすでに前提となっていることを指摘した。こうした流れを受けて、クリス・グラシオン氏（ベダアドバンテージ）は、オンラインサービスと金融サービスのいずれにおいても、現在はもっとデータを利用したい段階であるとし、規制介入するタイミングではないと表明した。

(4) 医療・健康セクターにおけるパーソナルデータの価値

データ利用の革新が経済社会全体にとって好ましい影響を与える領域として、医療・健康セクターを採り上げ、このセクターの現状と課題について整理した。具体的な論点としては、1）医療・健康セクターにおけるデータ利用の新たな手法は、人々の生活の質的向上に資すること、2）これは経済的価値だけではなく広く社会全体における価値であること、3）さらにこうした取り組みは医療・健康セクターのイノベーションにもつながること、4）一方で重大なプライバシー情報であることから、その管理には厳重かつ慎重な配慮が必要であること、などが挙げられた。

セッションには、以下のパネリストが参加した。

- ピーター・デスモンド・シングルトン（英国、ロンドンカレッジ大学プリンシパル・リサーチ・フェロー、ケンブリッジ医療インフォマティクス・ディレクター）
- エリオット・マクスウェル（E-マクスウェル&アソシエイツ代表）
- アン・バー（サノフィアベンシス、研究開発データプライバシー副オフィサー）
- フレデリック・ディエルセン（オランダ、健康福祉スポーツ省、法律・政策シニアアドバイザー）
- ジェラルド・アビ・アード（OECD、雇用・労働・社会問題局、政策アナリスト）

まず、オープニングプレゼンテーションを務めたピーター・デスモンド・シングルトン氏（ロンドンカレッジ大学）は、医療・健康セクターが他のセクターと最も異なる点として、生産者と消費者という単純な構図ではなく、医師、保険業界、行政等が複雑に絡み合うことで成立するセクターであることを指摘し、こうしたプレイヤーの円滑な連携にはデータ利用と流通が不可欠であることを提起した。その上でアン・バー氏（サノフィアベンシス）は、こうした産業構造面でのデータ利用はもちろん、既往歴等の把握は治験など製剤開発や医療分野のイノベーションでも極めて重要であることを指摘した。

一方でジェラルド・アビ・アード氏(OECD)は、10 月に開催されたイスラエルでのシンポ

ジウムやプライバシー会議の議論を引用しつつ、一方で医療技術が極めて高度化した今日において、たとえば先天的な疾患の要因と推定される遺伝情報の把握のために、子供は親の遺伝情報を知る権利があるのか、あるいはこれが社会的に共有されるべきなのか、といった問題を提起した。あわせて、医療・健康セクターでのデータ利用に係る検討が、すでに極めて倫理的な側面を大きくしていることを指摘し、我々人間自身がその経済社会的利益をどのように計測し、価値を判断すべきか、という根源的議論が必要であることを提起した。

(5) プライバシー・ビジネス

近年のプライバシー動向の変化として、プライバシー保護の実践者とプロ化の拡大を挙げ、こうした動向を「プライバシー・ビジネス」として捉え、その市場拡大が始まっていることを提起するとともに、その最新動向を整理した。具体的には、1）プライバシー・プロフェッショナルの需要と実践者が拡大しているという事実の共有、2）こうした進展を支えるツールやサービスがプライバシーに関わる企業や個人への信頼や評判を形成しているというメカニズムの指摘、3）規制当局だけではなくこうした事業や市場がプライバシー保護をさらに向上させる可能性、等について検討を行った。

セッションには、以下のパネリストが参加した。

- アレッサンドロ・アクイスティ（米国、カーネギーメロン大学・ハインツカレッジ、助教授）
- デビッド・スミス（英国、情報副コミッショナー）
- J・トレバー・ヒューズ（IAPP エグゼクティブ・ディレクター）
- パオロ・バルボニ（欧州プライバシー協会）
- オーウェン・トリップ（レピュテーション・ディフェンダー、共同創設者兼 COO）
- アンドレアス・クリシュ（欧州デジタルライツ、代表）

まず、オープニングプレゼンテーションを務めたアレッサンドロ・アクイスティ氏（カーネギーメロン大学）が、プライバシー・ビジネス全体のニーズと動向を紹介し、データ漏洩等に対する保険の準備を高めるほどモラルハザードが生じやすい状況や、PET の有効性等について指摘した。続いて J・トレバー・ヒューズ氏（IAPP エグゼクティブ・ディレクター）がその活動を紹介するとともに、同団体が推進する Privacy Professionals をはじめとした、認証やトラストマークの役割や期待が拡大していることを指摘した。

一方、パオロ・バルボニ氏（欧州プライバシー協会）は、欧州委員会の Article29WP が発表した Opinion 3/2010 において、認証プログラムやシール（トレードマーク）の開発を推奨していること、また同委員会の COM(2010) 609 final[38]においても同様の推奨をしていることを例示し、規制当局においても検討が進んでいることを明らかにし、こうしたトラストマークの開発時期に来ていることを指摘した。またオーウェン・トリップ氏（レピュテーション・ディフェンダー）は、消費者保護の観点からもこうした認証ベースの監査システムが重要であるとの指摘がされた。さらに、アンドレアス・クリシュ氏（欧州デジタルライツ）は、こうしたプライバシー・ビジネスの台頭が企業のプライバシー意識の向上に資することを踏まえて肯定するとともに、個人レベルでの保護や救済には NGO/NPO によるアプローチ

[38] http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

が未だ有効であり、その役割も今後拡大するであろうと指摘した。

(6) 全体の所感

2010 年 10 月にイスラエルで開催されたシンポジウム(進化するプライバシー保護の役割)において、プライバシー情報の利活用を前提としたサービスの台頭を、従来のような「脅威」と捉えるのではなく、成長セクターの一つとして位置づけた上で社会との「協調」を目指すという認識の変化があった。今回のラウンドテーブルはそもそもが「パーソナルデータとプライバシーの経済学」と題されているように、同様の潮流はより具体的に明示されていたように思われた。

その中でも特質すべきは、1）大量データの利用がビジネスの礎であるという認識と課題の共有、2）医療分野でのデータ利用の必要性の確認、3）プライバシー・ビジネスにおいてトレードマークや認証の重要性が増しているとの指摘、が挙げられる。これらは今後の OECD でのプライバシーに係る検討においても重要な参照元となると考えられ、来年以降の WPISP における PWB2011-12（2011-2012 年の 2 カ年予算計画）の執行においてもこれらの要素が意識されるものと考えられる。

3.4.4 WPISP 定例会合

(1) 概要

第 29 回 WPISP(Working Party on Information Security and Privacy)定例会合が、2010 年 12 月 2 日～3 日にパリの OECD 本部にて開催された。今回は PWB2009-10（2009-2010 年の 2 カ年予算計画）の最終回となるため、全体としてはこの 2 年間の報告とまとめが多かった。

WPISP は、その名称の通り、情報セキュリティとプライバシーの両方を検討の対象としている。そのため、議題のいくつかは直接的にはプライバシーと関係のないものも含まれている。今回はプライバシーに係る検討について、主な論旨を以下の通り報告する。

図 3-2 WPISP の様子

(2) PWB2009-10 のレビューについて

全般に大きな問題はなく、30 周年のイベントも滞りなく進行することができた。また 2010 年 10 月のエルサレム会議や 12 月のパリ会議では、1）大量データが新たな事業機会となり、「ゲームのルール」が変わりつつあること、2）消費者の懸念が顕在化していること、という 2 点が明確になり、極めて興味深いものとなった、との指摘が議長からなされた。

一方で、プライシングモデルの議論が新たに必要（イスラエル)、また具体的な実験結果等を踏まえた検証が必要（ポルトガル)、等の意見があった。

(3) PWC2011-12 の全体像について

PWC2011-12 では、以下の論点が注目される（プライバシーに関係するもののみ抜粋)。

- パーソナルデータの経済学についてのポリシーレポートの編纂
- プライバシーの将来についての検討詳細化
- 規制当局の監視に係る協力をベースとした、知識経済(knowledge economy)のグローバルフォーラムへの参加
- トラストワークショップ向けの指標開発
- セキュリティとプライバシー・ポリシーのレビュー

また第 30 回 WPISP は 2011 年 6 月 9 日～10 日に実施することとなった。またその次は、2011 年 10 月 31 日～11 月 4 日の間、プライバシー・コミッショナー会議と背中合わせの日程とする形で、メキシコで WPISP が中心となったプライバシーに関するディスカッション・イベントを実施することを決めた。

一方、プライバシー・ガイドラインの改訂については、次回（第 30 回）を目途に対応方針を決めるものとする。その間、3 月前後に事務局とボランタリー・グループで、どのように取り扱うかをオンライン上で検討するものとする。

(4) プライバシー監視協力

PWB2011-12 としては、従来の方針を確認・踏襲しながら、以下の 4 点について OECD のサポートの下で具体化していく。

- コンタクトポイントの集約
- 支援仕様の募集
- 他のステイクホルダーへの助言
- 他のプライバシー団体との非公式なネットワークの構築促進：GPEN[39]、APEC-CPEA

また国内のフレームワークを国際協調につなげていけるように拡張するための支援を以下の通り行う。

- 国内フレームワークのレビュー
- 実効性を獲得するための体制構築
- 国際協調可能性の強化
- 他のステイクホルダーやオーソリティとの協力

[39] Global Privacy Enforcement Network　https://www.privacyenforcement.net/

(5) プライバシー・ガイドラインについて

プライバシー・ガイドラインの改定に向けて、現在ボランタリー・グループでの健闘を進めているが、以下の論点についての取り込みが引き続き必要と考えられる。

- システム開発とガイドラインの影響力の関係
- パーソナルデータの処理に関する昨今のトレンド
- 環境の進展に伴うプライバシーリスク
- 考察と挑戦
- プライバシーガバナンスの進化とイノベーション

こうした検討を、2011 年 3 月頃を目処にボランタリー・グループで一度取りまとめ、その後 2011 年 6 月の WPISP 定例会合で基本方針の了承にこぎつけたい。

(6) 欧州委員会のデータ保護指令の改定に係る検討状況について

協力団体の立場として、欧州委員会より、以下の狙いでデータ保護指令の改定に向けた検討が進められている旨が報告された。

- 欧州各国レベルでのデータ保護やプライバシー法を出し抜くような行為を防ぐ
- 他国でのデータ処理に係るリスクから守る
- 課題や困難を明確化する
- 個人(individuals)の自信を強化する

また以下の原則に基づいた法制度化を検討している。

- 委員会のアプローチ
- 委員会による助言・諮問
- 委員会が目指す方針
  - 個人の権利の強化
  - 市場内部の局面への適用強化
  - データ保護法制の一貫性の強化
  - データ保護の国際的な局面の明確化
- 個人の権利の強化
  - 透明性確保の原則
  - データ漏洩通知の義務化
  - データ保護に係る情報の伝達の明確化
  - データ保護に係る連絡の内実化
  - 欧州標準のフォーム統一
  - 最小収集原則
  - アクセス、修正、消去、ブロックに関する権利の明確化
  - 効果的な問題改善や罰則を求める権利の強化
  - 同意
  - 「忘れられる権利」の明確化
  - データの可搬性
  - 活動の可視化

この他、国際的なデータ移転のルールについて、妥当性やデータ保護に係る国際的な同意の際の基本的精神の観点から、明確化・単純化を進める。またこれらは、各国のデータ保護に係る組織、Article29WP 等と連携する。欧州委員会としては 2011 年中に新たに改正案を提示する予定である。

(7) 全体の所感

PWC2011-12 においては、イスラエルでのシンポジウムやパリでのラウンドテーブルの議論の基調であった「経済社会との協調」という方針を意識した検討が進むこと、一方でこうした前提に立った際の新たな課題について、ガイドラインに織り込んでいく方針であることがわかった。一方でその具体的な内容については少なくとも 2011 年いっぱいを要するであろうこと、また 2011 年 3 月のボランタリー・グループの検討と 6 月の WPISP での議論が重要なマイルストンとなることも概ね明らかになった。さらに、昨今のトラストマークに係る関心の高さを踏まえ、WPISP でも同様の検討を進めることが分かった。

我が国としては、これらの会合および 2011 年 10 月～11 月にメキシコで開催されるカンファレンスでの結果を把握すること、また WPISP での議論において OECD 日本政府代表部とも協調しながら、クラウドにおける大量データの安全な利用方法の一つとして匿名化の技術とそれを踏まえた認証プログラム等の必要性を、明確化する必要があるものと考えられる。

なお、欧州委員会のデータ保護指令改定に関しては、担当者の説明を聞く限りではかなり強く個人の権利強化を意識した内容となっている。このため、民間企業のみならず政府部門からも賛同を得られるかは若干不透明であり、2011 年中の提案となったとしても、そのままの内容や進行で検討が進むとは考えにくいと思われる。

3.5 プライバシー・バイ・デザイン

3.5.1 背景

近年、個人情報やプライバシーに係る国際的な検討において、「プライバシー・バイ・デザイン」という概念が台頭している。すでに欧州委員会や米国 FTC 等での検討において参照されるフレームワークとしての地位を占めつつあり、今後我が国の個人情報・プライバシーに係る検討においても重要度が高まる可能性がある。そこで本研究でもその概要について整理しておく。

まずプライバシー・バイ・デザインの定義だが、我が国では現時点でもまだ明確に定まった定義は、法学あるいは行政の領域においても存在せず、そのため対応する日本語もまだない。そのため概念の整理が必要となるが、まずその成立経緯から考えると、個人情報・プライバシーに係る領域では、1990 年代半ばから後半にかけて、カナダのオンタリオ州情報・プライバシー・コミッショナーのアン・カブキアン博士を中心に提唱されるようになったようである。当時は、要素技術開発の取り組みとしてプライバシー・エンハンシング・テクノロジー(PET:Privacy-Enhancing Technologies)が、またシステム構築のプライバシー評価手法としてプライバシー影響評価(PIA:Privacy Impact Assessment)が、それぞれ体系化されていった時期でもある。

一方で、PET はその実装および採用の困難さ、またプライバシー影響評価は、厳格に進めると情報システム構築の推進そのものに重大な影響を及ぼしかねない、といった状況が生まれ、より現実的なフレームワークの必要性が徐々に高まっていた。こうした背景を受け、特に情報システムの構築に際して、より現実的な合意形成のフレームワークが必要とされるようになった。プライバシー・バイ・デザインは、こうした要請を受けて、近年注目されるようになったものと思われる。

3.5.2 概要

カブキアン博士の発表した文献の記述を総合すると、プライバシー・バイ・デザインとは「個人情報を取り扱うシステムを構築するにあたって、最初からプライバシー保護策を講じておく」[40]ためのフレームワークであり、またこれをシステム設計の段階に応じてきめ細やかに推進することを求めているところに特徴が見られる。

具体的には、以下の原則によって定義されている。

- 回顧的でなく先見的、事後救済的でなく予防的
- デフォルト（予めシステムの前提としての）としてのプライバシー
- デザインはめ込み（予めシステムに標準設計されている）プライバシー
- 全機能性－ゼロサムではなくポジティブサム
- エンド・ツー・エンドにわたるセキュリティのライフサイクル保護
- 可視性および透明性
- ユーザ・プライバシーの尊重

こうした原則を踏まえ、1）構築段階に応じてステップ・バイ・ステップに対応し、2）必要に応じてステイクホルダー間でのコミュニケーションと協調を求め、3）情報システムの構築後も、運用段階で適宜チェックを行う、といった方針を情報システム開発に求めている。

3.5.3 適用動向

(1) 国際機関での取り組み

プライバシー・バイ・デザインの概念をフレームワークとして採用する動きは、2010 年頃より活発化している。

たとえば欧州委員会が検討を進めている「EU データ保護指令」の改正にあたっては、プライバシー・バイ・デザインの概念を参照し、広義のプライバシー情報を取り扱う情報システムはこの原則に基づいた開発プロセスを経ることを推奨しようとしている。

また、米国 FTC が 2010 年 12 月に発表した「変化の激しい時代における消費者のプライバシー保護に向けて」（原題：Protecting Consumer Privacy in an Era of Rapid Change）[41]と題されたスタッフレポートにおいて、事業者および政策立案者向けにフレームワークが提案されているが、このレポートが参照するフレームワークとしてプライバシー・バイ・デザインがレポートの冒頭で明確に位置づけられている。

---

[40] http://www.horibemasao.org/3.horibe3.pdf
[41] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

一方、OECD でも、2010 年 10 月に開催されたエルサレム会議と同日程で開催されたプライバシー・コミッショナー会議では、プライバシー・バイ・デザインに関する決議が行われた。具体的には、以下のような内容である。

- プライバシー・バイ・デザインを「基礎的なプライバシー保護の要素」として認識する
- プライバシー・バイ・デザインの原則が、企業・団体等の「標準的な運用形態」として採用されることを推進する
- 以下の点についてデータ保護・プライバシー・コミッショナーや事務局を招聘する
- プライバシー・バイ・デザインの幅広い普及・啓蒙
- プライバシー・バイ・デザインの原則をプライバシー・ポリシーや制度制定の原理として適用することの促進
- プライバシー・バイ・デザイン研究の積極的な推進
- 2011 年 1 月 28 日に実施される国際データ・プライバシー・デイへのアジェンダ追加の検討
- 2011 年に開催される第 33 回プライバシー・コミッショナー会議への適用事例やベスト・プラクティスの報告

(2) 具体的な適用事例：スマートグリッド

プライバシー・バイ・デザインの利活用事例として、カナダ・オンタリオ州におけるスマートグリッドの取り組みが上げられる。2010 年 10 月のエルサレム会議に先立つ形で、同州プライバシー・コミッショナーのアン・カブキアン氏が主催するプライベート・セミナー(Smart Grid Privacy 101: Privacy by Design in Action)が開催されたが、これによると同州におけるスマートグリッド事業の展開において、プライバシー・バイ・デザインが一定の役割を果たしているという。

具体的には、1）スマートグリッドのシステム開発時における開発段階に応じた最終消費者との協議、2）それを反映した上での運用ポリシーの策定、3）データの利用原則の確立、4）監視メカニズムの構築、4）行政を巻き込んだコミュニティ全体での同意（立法ではなくラフ・コンセンサス)、等を、プライバシー・バイ・デザインのフレームワークに沿って進めたという。

同セミナーでは、こうしたプロジェクトの実際の進め方等についてレクチャーや事業者からの報告があったほか、スマートグリッドへの取り組みを強化している IBM やグーグル等からプライバシー担当者（ポリシーカウンセル等）が講演し、両者の取り組みにおいてプライバシー・バイ・デザインを前提としたプライバシー情報管理の設計が進んでいることを発表した。会場には各国のプライバシー政策関係者のほか、インテルの法務担当者やジョージ・ワシントン大学の研究者等が集まり、各社の取り組みについて進捗状況や課題等について質疑が行われた。

同セミナー参加を通じて、プライバシー・バイ・デザインがすでに北米の大規模事業においてはプライバシーアセスメントの標準的なフレームワークとして見なされていることが分かった。コーヒーブレイクの際に参加者に率直な意見を求めても、異口同音に「注目され

ている重要なフレームワークであり、世界的に見ても事業に用いることのできる唯一の現実的なフレームワークではないか」との意見が多数であった。

図 3-3　会場の様子

3.5.4 今後の対応

プライバシー・バイ・デザインの適用領域について、カブキアン氏や他の参加者も指摘していたが、スマートグリッドや通信事業者のインフラなど、比較的大規模なシステムに適していることが分かった。これは、プライバシー・バイ・デザイン自体がそもそもそうした社会インフラに近い大規模システムでのプライバシー保護を念頭に作られたフレームワークであることに起因するが、実際の手続きや進め方のケーススタディを見ても、小規模システムへの適用では若干煩雑すぎる可能性があり、適用対象はある程度限定されるものと思われる。

またプライバシー・バイ・デザイン自体は狭義のプライバシー保護技術ではなく、そうした技術をシステムに導入することでプライバシー保護と利用を確立するための方法論である。その意味で、匿名化技術のような個別技術との親和性はあると考えられ、むしろそうした個別技術を適切に導入するための前処理としての共存が可能であると考えられる。

こうした論点について、プライベート・セミナー以外の機会でカブキアン氏と意見交換したところ、大変強い関心を示され、我が国の検討や技術開発の詳細状況について共有したいとの意向をいただいた。またプライバシー・バイ・デザインのプログラムと個人情報匿名化の取り組みの協調可能性について検討すべく、今後詳細に意見交換したいとのこちらからの申し出も快諾いただき、引き続き意見交換や面会の機会をいただけることとなった。

3.6 まとめ

3.6.1 匿名情報の認証スキームの先進的事例

カナダ CHEO、アメリカ MedMining にて、医療情報に関する匿名情報の二次利用の認証スキームが存在する。イギリス NHS において、医療情報の二次利用サービス Secondary Uses Service(SUS)が実施されており、その中で、仮名化方法を検討する Pseudonymisation Implementation Project (PIP)が実施されている。また、イギリス Data Archives では、社会科学系の調査で収集されたデータを管理するサービスを行っており、必要に応じて匿名化処理を実施している。

このような状況を鑑み、匿名情報の認証スキームの先進的事例として、CHEO、MedMining があげられる。MedMining は民間企業でありアクセスや情報収集について難航が予想されたことに対し、CHEO は様々な情報が公開されており、それらを調査した上での現地調査は有効性が高いと予想されたことから、CHEO について現地調査を実施することとした。

3.6.2 各国のプライバシー関連法律の比較

調査対象国のプライバシーおよび個人情報に関する法律の一覧を表 3-3 に示す。

表 3-3　各国のプライバシー／個人情報に関する法律一覧

	Personal Information Protection and Electronic Documents Act (PIPEDA)	Privacy Act.	Personal Health Information Protection Act (PHIPA)	Personal Information Protection Act (PIPA)	Privacy Act	E-Government Act	Health Insurance Portability and Accountability Act (HIPAA)	The Data Protection Act.	The Freedom of Information Act.	Privacy Act
国（地域）	カナダ	カナダ	カナダ／オンタリオ	カナダ／ブリティッシュコロンビア	アメリカ	アメリカ	アメリカ	イギリス	イギリス	オーストラリア
概要	個人に関わる情報に関し、収集、利用と開示について規定、2000 年制定、2001 年施行	個人に関わる情報に関して、情報提供者個人の保護と情報へのアクセスについて既定、1982 年制定、1983 年施行	オンタリオ州における医療情報の収集、使用、公開について規定、2003 年制定、2004 年施行	ブリティッシュコロンビア州における個人の個人情報へのアクセスの権利や、ブリティッシュコロンビア州内の組織の情報収集、使用、公開について規定、2003 年制定、2004 年施行	米国連邦政府機関によって維持管理される記録システムにおいて、収集、維持、利用、配布される識別可能な個人情報に関する法令、1974 年施行。 情報提供者の明確な同意（書面）がない場合、記録システムに記録された情報を開示することを禁じる。 情報提供者個人の情報の閲覧および更新に関する手続きを各省庁に提供するように定める。	電子政府サービスの運営と促進を向上させる目的で制定、2002 年制定、2003 年施行。第 208 条では、全連邦政府機関において、識別可能な個人情報の収集・維持・配布を行う新規調達システムに対する Privacy Impact Assessment(PIA)の実施を求める。	医療情報の電子化の推進とそれに関係するプライバシー保護やセキュリティ確保について規定、1996 年制定、2003 年施行	自身に関する情報について、組織等の保有状況を知る権利、ならびに、これらの情報を適切に扱うことを確実にするルールを規定、1998 年制定、2000 年施行	公的機関が保有する情報を、特別な事由がある場合を除いて、取得することができる権利を定める（情報公開）、2000 年制定、2005 年施行	個人情報に関する収集、利用と開示、精度、安全な管理および情報提供者自身のアクセスを規定、1988 年制定 健康および医療情報はセンシティブデータとして分類し、特別な処置を求めることを規定
個人情報の定義	個人を特定できる情報（ただし、組織の従業員の名前、肩書、勤務先の住所や電話番号を除く）	あらゆる形で記録された個人を特定できる情報	口頭、あるいは記述された形式で個人を特定できる情報	個人を特定できる情報 従業員の個人情報を含む	個人の氏名、ID 番号、シンボル、指紋・声紋・写真など個人を特定できるものが記された、学歴、金融取引、医療履歴、犯罪歴、職歴などを含むあらゆる情報	個人を特定できる情報	口頭、あるいは書面に記載され、以下を満たす情報。ヘルスケア提供者、健康保険、公共医療機関、雇用主、生命保険会社、学校や大学、ヘルスケア情報センターによって作られる、あるいは受け取られる、個人の現在、過去、未来の身体的、精神的健康状態、個人に対するヘルスケアの提供とその医療費に関連する情報	生存する個人を特定できる情報、あるいは他の情報を付加することで個人を特定できる情報	－	真偽を問わず、個人の身元が明らかとなる、または合理的に解明されうる、個人に関する情報や意見
適用範囲	民間セクター	政府機関	医療情報に従事する者、また医療組織外で個人医療情報を受け取る個人や組織	ブリティッシュコロンビア州内の組織（企業や非営利組織を含む）	連邦政府機関	連邦政府機関	ヘルスケア提供者、医療保険、ヘルスケア情報センター	個人情報に対して何らかの処理をする人や組織	公的機関および公的企業	政府機関および民間セクター
所管機関	Office of the Privacy Commissioner of Canada(OPC)	Office of the Privacy Commissioner of Canada(OPC)	The Office of Information and Privacy Commissioner of Ontario(IPC)	The Office of the Information and Privacy Commissioner for British Columbia (OIPC)	The Office of the Privacy and Civil Liberties(OPCL)	The Office of the Privacy and Civil Liberties(OPCL)	Office for Civil Rights(OCR)	Information Commissioner Office (ICO)	Information Commissioner Office (ICO)	Office of the Privacy Commissioner(OPC)
罰則	PIPEDA 自体に法的拘束力はないが、OPC が調査・勧告をする。OPC の勧告は必ず守られなくてはいけないわけではないが、申立人が訴えを起こす場合もある	個人情報にアクセスすることを拒まれた個人は OPC での手続きを経て証人喚問を行うことができる。 OPC の活動を妨害した場合、$1,000 以下の罰金が科される場合がある	法令が守られなかった場合、個人で$50,000 以下の罰金、個人以外で$250,000 以下の罰金が科される場合がある	法令が守られなかった場合、個人で＄10,000 以下の罰金、個人以外の者で$100,000 以下の罰金が科される場合がある	民事罰則と刑事処罰がある 組織が個人の情報を修正することを拒んだ場合、個人は民事裁判所にて訴えを起こすことができる。組織が故意に情報を公開した場合、$5,000 以下の罰金が科されることがある	個人情報の公開が違法であると知りながら、情報を受け取る資格のない者に故意に情報を公開した場合、5 年以下の懲役、または $250,000 以下の罰金を科される場合がある	法律が守られなかった場合、 民事罰則として、一件につき$100～50,000 あるいはそれ以上の罰金（ただし、1 人に対する 1 年の罰金は $1,500,000 を超えない）。 刑事処分として、最低でも$50,000 以下の罰金、または 1 年以下の懲役が科される場合がある	故意に違反が行われた場合、または重大な損害につながる可能性を知っていた（あるいは知っているべきであった）場合、 ICO により金銭的罰則を科される場合がある	ICO の勧告に従わなかった場合、高等法院（民事事件を扱う上級審）へ持ち込まれる	OPC からの質問に答えない場合、最高$2,000 の罰金、または 1 年の懲役を科される場合がある

	Personal Information Protection and Electronic Documents Act (PIPEDA)	Privacy Act.	Personal Health Information Protection Act (PHIPA)	Personal Information Protection Act (PIPA)	Privacy Act	E-Government Act	Health Insurance Portability and Accountability Act (HIPAA)	The Data Protection Act.	The Freedom of Information Act.	Privacy Act
例外	法的処置に関連した調査や緊急事態の場合 Privacy Act が適用される政府機関、個人利用のために個人情報を使用する者、報道・芸術・文芸のみのために個人情報を使用する組織　など	公共資料としての目的をもつ図書館や美術館の所蔵品、Canadian Broadcasting Corporation、the Queen's Privy Council for Canada（カナダ枢密院）　など	the Quality of Care Information Protection Act, 2004 との整合性が取れない場合、法律によって個人情報の収集・使用・公開が必要とされる場合、研究目的の場合などは、使用が認められることがある	報道・芸術・文芸が目的である場合、行政手続きに使用される場合、裁判所文書や起訴に関する文書に使用される場合　など	Census Bureau と Bureau of Labor Statistics による統計目的、法的措置の目的、アメリカ議会の調査目的、他の行政的目的など	書面による同意があれば、指定統計機関（商務省統計局、商務省経済分析局、労働省労働統計局）から他の指定統計機関へ個人を特定できる形で業務データを提供することは認められる	法律によって求められる場合、公共医療活動・裁判や行政の活動・法の施行・研究・必要な政府機能を目的とする場合、個人が死亡している場合　などは個人の許可なしで医療個人情報を使用できるケースがある	国家の安全、犯罪や課税、医療・教育・社会活動、報道・文学・芸術、研究・歴史・統計などの目的	セキュリティに関する問題を扱う情報、裁判所の記録に含まれる情報、上院や下院によって保持される情報で、その公開が公共の事柄の効果的な実施に損害をもたらす場合　など	医療関連研究を目的とする場合、研究者が個人を特定できないように施せば、医療個人情報を扱うことを認められる場合がある

3.6.3 プライバシー・コミッショナー制度に関する比較

調査対象国のプライバシー・コミッショナーに関する一覧を表 3-4 に示す。

米国を除いて独立機関、または独立に施策を実施できる機関が多い。権限範囲は異なるが、これらの機関は、プライバシーまたは個人情報関連の苦情およびその処理などを実施する権能を有している。

表 3-4　各国のプライバシー・コミッショナー制度一覧

	OPC（加）	OPCL（米）	ICO（英）	OPC（豪）
概要	Privacy Act および PIPEDA の順守状況を監視する権限を有するとともに、プライバシーに関わる調査研究、普及啓発を実施	Privacy Act:1974 および電子政府法とのコンプライアンスを含み、プライバシー保護および人権擁護に関わる調整等を実施	The Data Protection Act.、The Freedom of Information Act. と関連の規制に基づき、 Data Privacy に関する普及啓発、個別の問題解決、規制等を実施	Privacy Act:1988 に基づき、政府機関として豪州におけるプライバシー関連の施策を統括
所属	独立機関	司法省	独立機関	内閣（独立に活動）
助言機関	あり	特になし	特になし	あり
実施事項	・監査 ・調査 ・普及啓発 ・PIA レビュー ・立法の際の助言 ・プライバシーに関する調査結果レポート発行	・監査 ・調査 ・政策との調整 ・PIA ガイドライン ・ポリシー策定 ・プライバシーに関する定期報告書発行	・監査 ・調査 ・普及啓発 ・情報・助言提供 ・苦情処理 ・データコントローラの登録	・監査 ・普及啓発 ・情報・助言提供 ・苦情処理

4. 匿名情報の利活用に関する調査検討

4.1 匿名情報の二次利用サービス事例

本節では、国内外の匿名化したパーソナル情報の二次利用サービスの事例について、その概要、取り扱うパーソナル情報の範囲、二次利用サービスの形態等を明らかにした。

事例調査を通して整理する項目を下記に示す。

(1) 概要
(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）
(3) データの種類、形式、用途
(4) リスクに対する管理策・アセスメント結果
(5) 二次利用サービスの形態

4.1.1 CHEO

(URL: http://www.ehealthinformation.ca/)

(1) 概要

カナダの CHEO RI(Children's Hospital of Eastern Ontario Research Institute)による、健康に関する電子的な個人情報の取扱いに関するさまざまな研究を可能とする Web サイトである。

次の三つのツールを保有している。

(a) Privacy Analytics Re-identification Risk Assessment and De-identification Tool (PARAT)

CHEO 独自の匿名化技術を実現したスタンドアローンなツールである。再識別されるリスクを評価して、自動的に匿名化処理を行う。匿名化関係の文献などで著名なツールであるためツールの詳細については、4.4.1 項で詳細を述べる。

(b) Data Breach Analyzer and Dashboard

医学データのプライバシー侵害のリスクなどの傾向や広がりを分析し、そのリスクの型や侵害の方法を指定することにより分析結果を視覚化するツールである。

(c) Privacy and Confidentiality Knowledgebase

(http://www.ehealthinformation.ca/knowledgebase/)

匿名化の実践（29 件）、PARAT ツール（26 件）、他（6 件）の FAQ 的な入り口の知識ベースである。

以上のツールのほか、関連研究のレポートも多数参照できる。

(http://www.ehealthinformation.ca/ap0/tr.asp)

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、個人の健康・医療情報である。

ツールの利用例で示される対象とするデータは次の通りである。

- 個人とその家族の年齢に関する情報（生年月日など）
- 個人の身体的特徴値（身長、体重など）
- 個人のある時点での身体の状況を表す特性値（血圧など）
- 個人の病歴とある時点での診断結果
- 個人の医療診断に関わる生活習慣（喫煙習慣の有無、頻度など）

（CHEO が行うのはツールの提供であり、以上の情報を CHEO が保有するということではないことに注意する）

(3) データの種類、形式、用途

個人の健康･医療情報の再識別などのリスクを評価し、匿名化する技術に関する情報やそれを実現するツールを、医療情報管理者に提供する。

(4) リスクに対する管理策・アセスメント結果

匿名化ツール PARAT で実現している。詳細は、4.4.1 項参照のこと。

(5) 二次利用サービスの形態

医療情報の管理者向けの匿名化・リスク評価ツールと関連技術情報を提供する。ここで提供されたツール・技術を用いて、医療情報管理者がデータの再識別のリスクを評価したり、匿名化したデータを提供したりすることになる。

PARAT を利用している事例としては、CHEO の保有するデータの研究目的の二次利用、オンタリオ州の医療情報レジストリ（新生児と母親の健康情報、がん患者の情報など）および、IMS:Brogan 社が挙げられる。

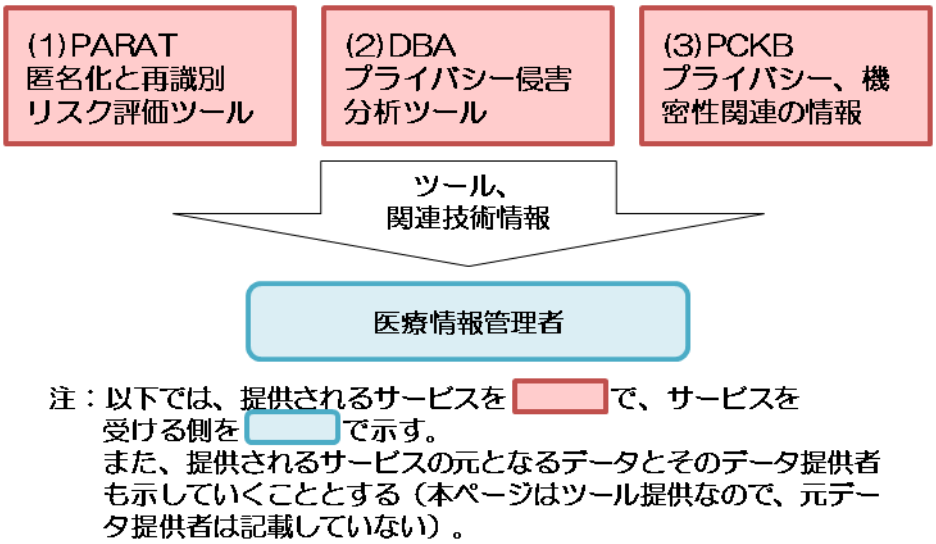

図 4-1　CHEO のサービス形態

4.1.2 MedMining

(URL: http://www.medmining.com/)

(1) 概要

米国 MedMining 社は、米国の HIPPA(Health information is protected by the Health Insurance Portability and Accountability Act)に基づいて非 ID 化された、多様な医療情報を保有し、次の 4 プロセスで、データを用いた解析結果とデータセットを販売している。

(a) Discover

顧客との徹底的なインタビューにより、顧客の研究に必要なデータを完全に理解する。その後顧客とフィージビリティースタディを実施する。

これにより、顧客が彼らの研究に関係する高度に独自なデータを見いだせることを保証する。

(b) Define

時間的な締切り、データ選択方針、データソースの複雑さ、データの構成要素、緊急性などを含むプロジェクトの定義を行う。結果、プロジェクト定義文書を含む MedMining 標準の契約書が提供される。

(c) Do

必要なデータソースからデータを抽出し、関連付けを行う。そのデータが、プロジェクト定義文書の全ての要求を満たすかをプログラムで判定する。さらに人手によるチェックも行う。

この MedMining による患者のプライバシーと情報セキュリティを守るプロセスは、Geisinger Health System's IRB, Privacy, and Information Security Offices により、承認されている。

結果、プロジェクト定義文書に示された通りの、完全なデータセットが提供される。

(d) Deliver

契約書に規定された期間内に、暗号化されパスワードにより守られた、最終データセットが提供される。

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、個人の健康・医療情報である。

保有情報の対象領域は、図 4-3 に示す。特徴として、以下があげられる。

- Patient Demographics（患者層）など、病院の経営に関わる病院全体に関わるデータがある
- Nephrology（腎臓学）など、医学領域で細分化されたデータを持つ

(3) データの種類、形式、用途

匿名化された個人健康・医療情報に加えて、医学研究者の医学の論文などを、病院、医療機関に提供する。

(4) リスクに対する管理策・アセスメント結果

匿名化技術に関する詳細な記述は公開情報にはない。

(5) 二次利用サービスの形態

病院、医療機関向けに、匿名化された患者の健康・医療情報からなる医療データセット、関連の医学論文、研究情報を提供する。さらに、データ解析を支援する。

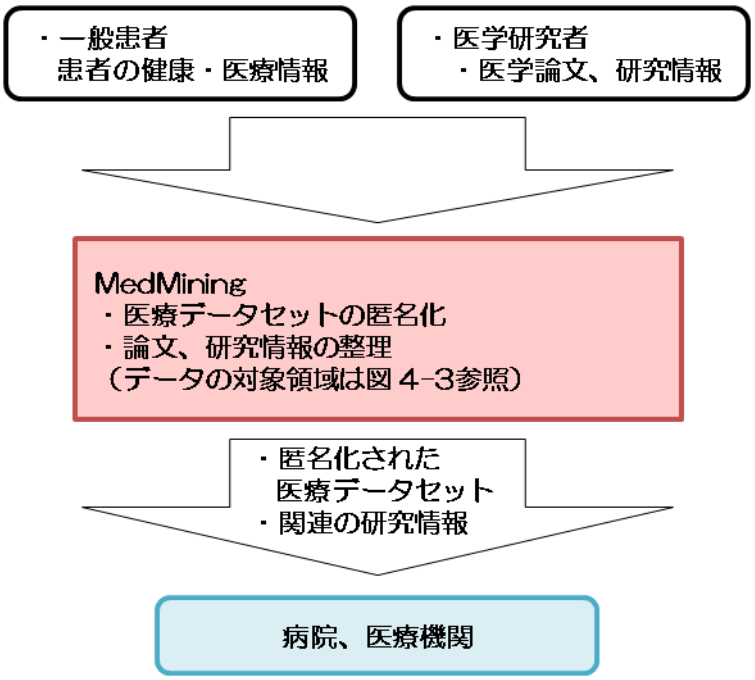

図 4-2 MedMining のサービス形態

□Core Data Elements ■Medication Data ■Encounter Data ■Cost Data ■Procedure Data ■Patient Demographics（患者層） ■Vital Data（血圧など） ■Laboratory Results ■Additional Core Data	□Speciality Data Elements ■Nephrology（腎臓学） ■Neurology（神経学） ■Obesity（肥満） ■Oncology（腫瘍学） ■Pulmonary（肺疾患） ■Rheumatology（リウマチ学） ■Women's Health ■Infectious Disease（伝染病） ■Gastroenterology（消化器病学） ■Diabetes（糖尿病） ■Cardiovascular（心臓血管） ■Allergy（アレルギー） ■Additional Special Data

図 4-3 MedMining の保有データ

4.1.3 SpendingPulse(MasterCard)

(URL:http://www.mastercardadvisors.com/us/advisors/en/information_analytics/spendingpulse.html)

(1) 概要

MasterCard 社による、カードの利用状況から、利用者の興味のある産業分野の消費活動（米国：小売全体と個別業種全体、英国：小売全体）を月単位、週単位でレポートし、利用者のビジネス上の意思決定、販売戦略を支援するサービスである。

MasterCard 社では、以下の項目からなる関連の統合的なサービスを行っており、SpendingPulse はこうしたサービスの一つである。

(a) Operational Data

顧客にとって効率的かつ、各種アプリケーションでの使用ができるような形で、顧客のビジネスに関連する一般消費者の購買データを提供する。ATM Location Services、Merchant Aggregation Services の二つのサービスが紹介されている。

(b) Comparative Information and Reporting

一般消費者の行動、産業、地理的な問題、マクロ経済学的、定量的なデータにより、使いやすく効率的な情報サービスを行っている。与えられる比較情報とソリューションのレポートにより、利用者は、ビジネスのパフォーマンスに関する深い分析が可能になり、ベンチマーキングのためのツールにより、ビジネスの強み、弱み、機会などについて、深い洞察を得ることができる。

SpendingPulse 以外に次の二つのサービスも行っている。

① Portfolio Analytics Performance Packs

顧客のトランザクションをベースにしたポートフォリオ分析により、顧客のビジネス全体のパフォーマンスと機会を計測する。

② Comparative Cardholder Dynamics

米国および欧州のカードホルダーの支払い情報から得られるデータの分析である。関連するトピックの研究も行う。

(c) Analytics and Models

データドリブンな傾向分析モデル、購買行動などによる一般消費者のクラスター分析など、上記の分析のもとになる、モデル化法が紹介されている。

(d) Applications and Tools

カードを消費者の好みにあうような直接カードアプリケーションにつながるようにすることでカード発行者を支援する Find-A-Card、カード保有者のキャンペーンの前、途中、後の行動を分析する Campaign Management、さまざまなポートフォリオ分析を可能にする Portfolio Diagnostic Engine などのツールを提供する。

(e) Information and Analytics Case Study

上記のサービスの事例が紹介されている。

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、特定の個人がカードを利用して、いつ、どこで、何を購入したかなどの個人の金融情報である。

(3) データの種類、形式、用途

小売業、航空業、アパレル、自動車部品、サービス、デパート、e コマース、電気製品、家具、服飾品、ホテル、宝石、高級品、レストラン、ハードウェア、ガソリンの個人消費データ（ATM 場所データ、小売店集約データ）を集約して、主として小売業者に提供する。

(4) リスクに対する管理策・アセスメント結果

加算された統計情報（業種毎の売り上げ合計など）のみを使用することで、特定の個人のカード使用状況などが特定されないようにして、パーソナル情報に関するリスクを回避する。

(5) 二次利用サービスの形態

個人のカードの利用状況と業種毎の売り上げなどの統計情報を収集し、小売業者向けに業種別売り上げのデータを提供することで、小売業者などが販売戦略の策定や関連の意思決定を行うことを支援する。

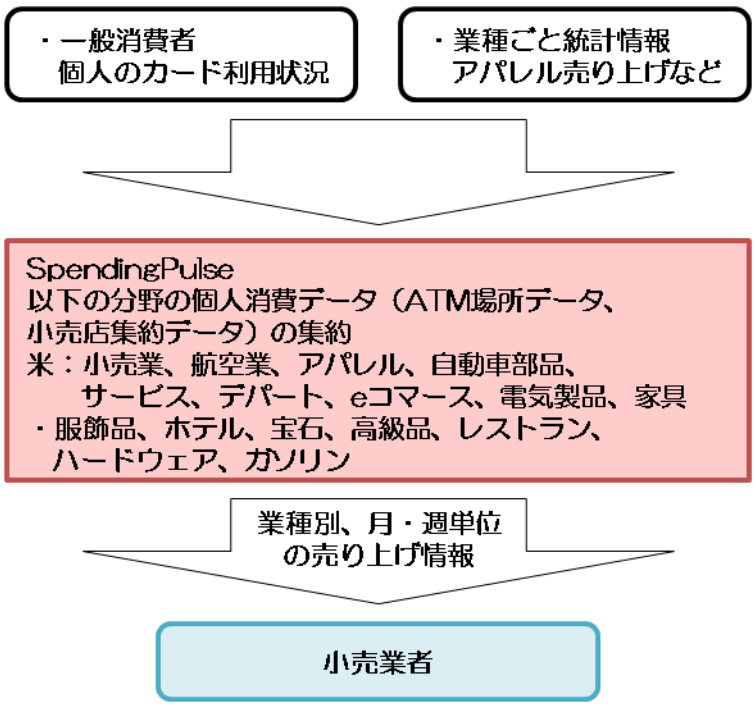

図 4-4 SpendingPulse(MasterCard)のサービス形態

4.1.4 Mint.com

(URL: http://www.mint.com/)

(1) 概要

利用者がオンラインで、自身の収入、支出、投資などの情報を入力し、システムはその情報を管理して、視覚化して表示するなどの機能を持つ「オンライン家計簿システム」である。利用者は、これらシステムが提供する機能を利用できるメリットのほか、以下の利点などがある。

- システム利用者のコミュニティと専門家のアドバイスを受けられる
- 各種のスタイルの投資システム(Folio Investing、SMART 401K、MarketRiders)を割引などで利用できる

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、個人の家計簿情報である。個人レベルの金銭的な収入、支出、投資などの情報が時系列的に並べられたものである。

(3) データの種類、形式、用途

オンラインで入力された個人の家計簿情報を整理、分析した結果を利用者本人に提供する。

(4) リスクに対する管理策・アセスメント結果

リスクに対する管理策は次の通りである。

- 最初から、利用者の個人情報に結び付く ID 情報をシステム登録しない
- 利用者から受けた情報は、銀行レベルのデータセキュリティ管理(VeriSign Secured、TRUSTe、HACKER SAFE(SCAN ALERT)、RSA)を行う
- READ ONLY（このシステムを使って実際のお金を動かすことは出来ない）なシステムとしているため、他者から不正利用されて金銭が動くようなリスクからも開放されている

(5) 二次利用サービスの形態

一般消費者向けの、オンライン収入支出管理、投資などに関する支援サービスである。利用者がオンラインで入力した家計簿情報を整理、分析するシステムサービスである。さらにシステム利用者のコミュニティおよび金融の専門家からアドバイスを受けられることが利用の動機となる。情報提供者とサービス利用者が同じことが、二次利用サービスの形態としての特徴となっており、ID 情報を元から登録しないことなどでリスクが軽減される。

匿名情報を販売するというモデルについても Bloomberg 社が報道して、話題になったが、現時点で実際に販売されたという事実は確認できていない。消費者の消費傾向の変化などの指標となるため、プライベートエクイティなどが興味を持つと考えられている[42]。

[42] Mint.com May Begin Selling Access to Anonymous Consumer Data - Bloomberg
http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aWJnLqF0Y8zs

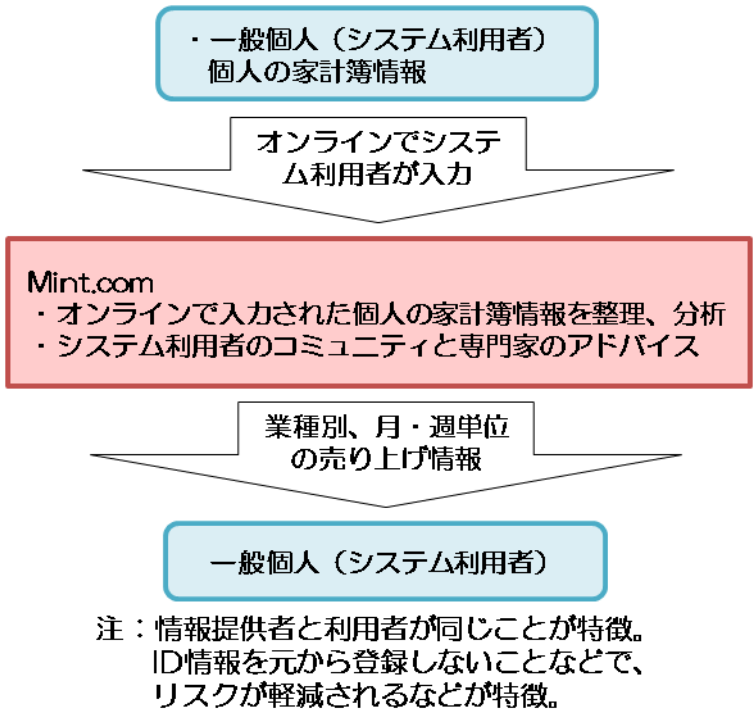

図 4-5　Mint.com のサービス形態

4.1.5 neuGRID

（URL: http://www.neugrid.eu/pagine/home.php）

(1) 概要

The European neuroscience community によるプロジェクトで、大量の脳のイメージ画像を収集し、コンピュータによる解析が可能な形でアーカイブすることで、進行性の脳疾患に関する研究を支援することを目的とする。

グリッドベースのイメージ情報のインフラ構築に必要な技術主体のプロジェクトであり、匿名化やデータ保護の記述は少ない。ここでは、上記 URL に保持されたデータ保護関連論文が若干あるので、以下で紹介する。

(a) D2.1 Review document on data protection(legal and procedural issues)

欧州 28 ヶ国のデータ保護の状況とグリッド、インフラを使用した欧州のプロジェクトの紹介。各国の関連の取り組みが表形式で示されており、関連の動向を概観できる。また、紹介されるプロジェクトは、SHARE、ACGT、ARTEMIS、@neurIST、HEALTH-E-CHILD、LHP の六つである。

(b) D2.2 Rules for commercial exploitation of data

医学データの商用利用に関するルールを検討するレポートである。検討においては、生物由来物質（バイオエタノールなど）の商用利用からのアナロジーを行っている。生物由来物質の商用利用については、現在、欧州の法的、倫理的フレームワークの改定が行われており、関連のガイドラインの提案も行われている。

(c) D2.3 PROTOCOL FOR ENSURING DATA PROTECTION/SAFETY IN neuGRID

neuGRID におけるデータ保護のプロトコルを解説したレポートである。このプロトコルは、欧州のプライバシーとデータ保護の改定版に基づいている。neuGRID におけるデータ保護のプロトコルの要点は次の通りである。

- 本人識別される可能性のあるデータは、個人情報として取り扱う
- 慎重に扱うべきデータ（センシティブデータ）を扱う際には、特にインフォームド・コンセントが必要
- 科学的な研究でデータの二次利用をする際、データ主体への通知義務がないのは、次の条件を満たす場合のみである
  - ➢ データの利用が、もともとの目的と矛盾しないこと
  - ➢ データが完全に匿名化されていること

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、一般患者の脳イメージ画像を中心とする医療情報である。

(3) データの種類、形式、用途

上記の一般患者の医療情報に加え、関連する研究に関する情報を保持する。医療研究者の研究のために提供する。

(4) リスクに対する管理策・アセスメント結果

匿名化指標の観点からは、特記事項はない。

(5) 二次利用サービスの形態

医療研究者向けの、脳のイメージ画像と医学研究者の研究情報のデータセットを提供する。

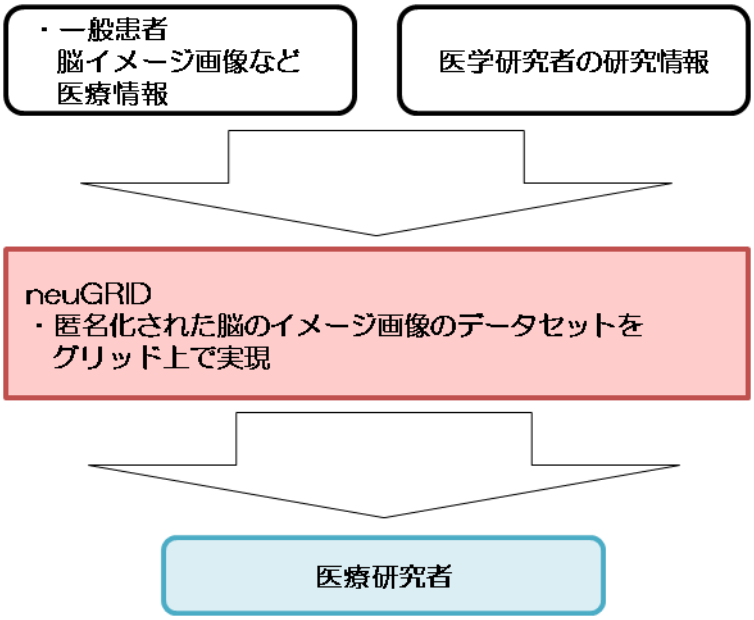

図 4-6 neuGRID のサービス形態

4.1.6 ACGT

(URL:http://eu-acgt.org/en/news/newsletters/spring-2009/single-article/archive/2009/march/article/center-for-data-protection-cdp-1.html)

(1) 概要

ACGT(Advancing Clinico Genomic Trials On Cancer)では、個人データの保護を検討するセンター、Center for Data Protection(CDP)を設置している。法的な見地からは、ACGT プロジェクトは EC の医学データのセキュリティとプライバシーに関するポリシーを補強するものでなくてはならない。また、ACGT プロジェクトのデータ保護フレームワークは、European Data Protection Regulations のカバー範囲を広げることを助けて、匿名情報の取扱いを可能にするデータ保護アーキテクチャを構築することが、主な目的となっている。

複数の病院で遺伝子情報が集められ、匿名化された後で、ACGT のインフラに蓄えられ、多くの研究者がそれを使って研究を行う。

匿名化には、Custodix Anonymisation Tool(CAT)を利用する（4.4.4 項参照）。

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、一般患者の遺伝子情報である。

(3) データの種類、形式、用途

上記の一般患者の遺伝子情報を匿名化したデータセットを保持し、関連する医学研究者の研究情報とともに、医療研究者に提供する。

(4) リスクに対する管理策・アセスメント結果

匿名化処理は、Custodix Anonymisation Tool(CAT)（4.4.4 項参照）を使用している。データ提供者、アクセス権限のある研究者が望んだときのみに再識別が可能になる枠組みを提供している。

(5) 二次利用サービスの形態

研究者向けの、遺伝子情報のデータセットと関連する医学の研究情報を提供する。

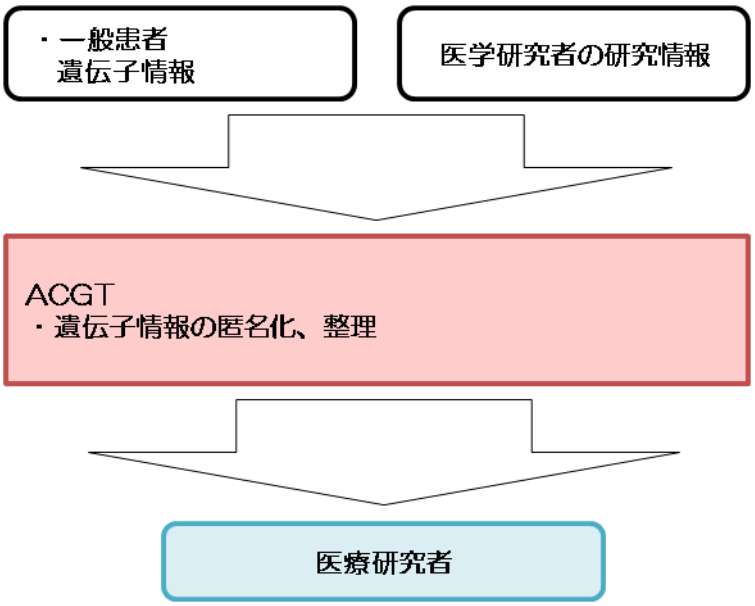

図 4-7　ACGT のサービス形態

4.1.7 ESSnet

(URL: http://neon.vb.cbs.nl/casc/)

(1) 概要

欧州の統計的開示抑制に関わる複数のプロジェクトの共通ホームページである。この協力は、The 4th Framework SDC-project(1996-1998)に始まり、the 5th Framework CASC project(2000-2003)、the CENEX project(2006)を経て、ESSnet(2008-2009)に至っている。

このプロジェクトの主な目的は、統計的開示抑制(Statistical Disclosure Control: SDC)を行うツールの適用をより容易にすることにある。このプロジェクトの現在のタスクは次の通りである。

- Task 1. Dissemination of CENEX results
- Task 2. Making SDC-tools better usable by NSIs
- Task 3. Output checking
- Task 4. Communication; Web and FAQ
- Task 5. Improvement of software for micro data
- Task 6. Improvement of software for tabular data
- Task 7. Synthetic data files
- Task 8. Analysis of problems on linked tables

上記 URL から直接リンクが張られているプロジェクトツールなどを表 4-1 にまとめる。

表 4-1　プロジェクトツール一覧

プロジェクト、ツール名称	概要
CENEX	すでに終了したプロジェクト。現在は、以下が入手可能。1)関連するレポート、2)ハンドブック、3)μ-ARGUS、T-ARGUS の最新版、CENEX-Conference のプロシーディング。
CASC	統計的な機密保持に関わる実践的なツールを開発するプロジェクト。マイクロデータの公開のコントロール法の検討と、テーブルデータの取扱法の検討に大きく分かれている。
μ-ARGUS	代表的な匿名化ツール。「4.4.3　μ-Argus」で詳細に述べる。
τ-ARGUS	テーブル型のデータを統計的に保護するためのツール。CASC プロジェクトで構築された。
Testsets	上記ツールで使用できるサンプルデータ。

以上のほかに、FAQ、Glossary、Handbook/Case Studies、Links、Papers、Papers、Books のページがあり、いずれのページも関連した豊富な情報が保持されている。

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

個別サービスの他の調査対象とは異なるが、匿名化の方法論・ツールなどの包括的な方法論を保持している。ARGUS の管理も行っている。「4.4.3　μ-Argus」も参照のこと。

(3) データの種類、形式、用途

包括的なサービスのため、「データの種類、形式、用途」についての特記事項はない。

(4) リスクに対する管理策・アセスメント結果

包括的なサービスのため、匿名化処理についての特記事項はない。

(5) 二次利用サービスの形態

統計データ管理者向けの、欧州の統計データコントロールに関わる複数のプロジェクトの共通ホームページであり、複数のプロジェクトで構築された技術、ツールの情報提供を行う。

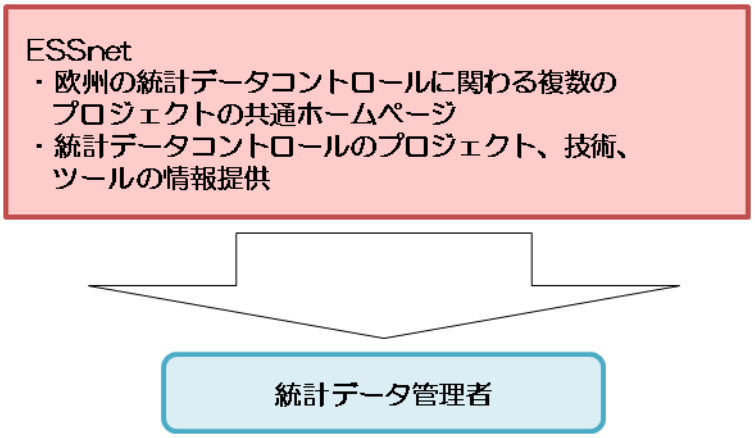

図 4-8　ESSnet のサービス形態

4.1.8 CDATA Online

(URL: http://www.abs.gov.au/CDataOnline)

(1) 概要

豪州の人口調査結果などの統計データと地図データを公開し、利用者はオンラインで分析、加工して、カスタマイズできるシステムである。政府機関の統計データの取扱いとして、注目すべきサービスである。

豊富なデータ項目が閲覧可能であり、図 4-9 に示すような各トピックにまとめられている。

Age and Population Distribution	Indigenous Education and Training
Ancestry	Indigenous Housing
Birthplace	Indigenous Labour
Carers	Indigenous Language and Culture
Childcare	Indigenous Population Size and
Children	Distribution
Citizenship	Internet and Computer Usage
Cultural and Language Diversity	Labour Force Participation
Dwellings	Language
Educational Attainment	Living Arrangements
Employment	Marriage Partnering Separation and
Employment by Industry	Divorce
Family Formation and Dissolution	Migrants
Fertility and Fertility Intentions	Migration Internal
Home Ownership	Migration International
Hours Worked	Motor Vehicles
Household Characteristics	Occupation
Housing Costs	Population Size and Growth
Housing Rental	Religion
Income Personal Family and Household	School Education
	Transport Access and Usage
	Type of Internet Connection
	Unpaid Housework
	Voluntary Work

図 4-9 CDATA Online の保有データのトピックス

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、個人の住居情報など、人口調査項目である。詳細な情報の分類などは図 4-10 の通りである。

(3) データの種類、形式、用途

上記の個人の住居情報など、人口調査項目に加えて、地域境界線などの地理情報を保持し、両者を組み合わせた分析、視覚化を可能とする。

例えば、ある地域の居住者の年齢層の分布などを分析し、地図上に結果を表示するなどの処理を行うことができる。

(4) リスクに対する管理策・アセスメント結果

利用者がアクセスできるのは、ある地域で集約されたデータである。個人のレベルまでは

たどれない。他、オリジナルデータに関しては、税務局など他の政府機関にすら出さない、本システムを他システムと統合しないなど、厳しい基準で管理する記述が多く見られる。

(5) 二次利用サービスの形態

一般利用者向けの、人口調査結果データと地図データを提供する。さらに、利用者がそのデータを利用した分析を可能とする環境を提供する。

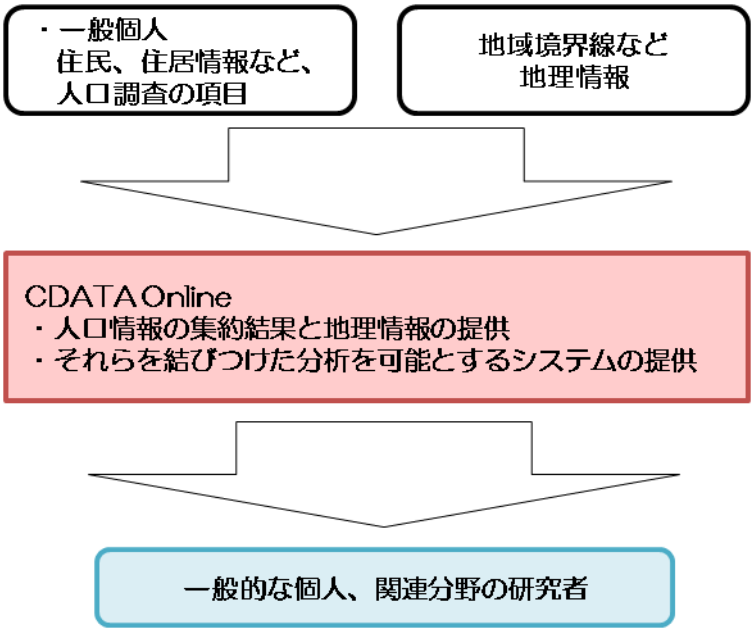

図 4-10 CDATA Online のサービス形態

4.1.9 On-line Statistical DataBase(NOSI)

(URL: http://nosi.ascc.gov.au/)

(1) 概要

豪州の労働に関する健康と安全、労働の賃金の調整を役目とする Safe Work Australia の公開 DB である。

the National Data Set for Compensation-based Statistics(NDS)から抽出した労働の安全に関する統計データのオンライン検索が可能である。

データは次の項目に分けて保持されている。

(a) Number of Claims

1 週間以上、仕事を休むことになった就労不能に対する補償の申し立てに関わるデータである。

(b) Incidence Rate

労働中の負傷、発病などの発生率で、労働者 1000 人に対する申し立ての件数で表す。中でも死亡にまで至った例は、特例として別にも取り扱われることになる。また、産業分

野毎の数値はないという断り書きがある。このようにデータの種別により、その公開の仕方、範囲が考慮されている。

(c) Frequency Rate

労働中の負傷、発病などの時間当たり頻度である。百万時間当たりの、労働中の負傷、発病件数で表す。中でも死亡にまで至った例は、特例として別にも取り扱われることになる。また、産業分野毎の数値はないという断り書きがある。このようにデータの種別により、その公開の仕方、範囲が考慮されている。

(d) Median Time Lost From Work

（労働中の負傷、発病などにより）失われた労働時間の統計データである。

(e) Median Total Compensation Payments

（労働中の負傷、発病などにより）支払われた保証金の統計データである。

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、個人から得られた労働の安全に関する情報である。

次の内容の DB を保持している。

- Number of Claims
- Incidence Rate
- Frequency Rate
- Median Time Lost From Work
- Median Total Compensation Payments

(3) データの種類、形式、用途

上記の個人から得られた労働の安全に関する情報に加えて、関連の研究論文を提供する。

(4) リスクに対する管理策・アセスメント結果

匿名化に関する特記事項はない。

(5) 二次利用サービスの形態

労働に関する健康と安全、労働の賃金の調整を目的とした DB を公開して、一般労働者、労働関係研究者に情報提供を行う。

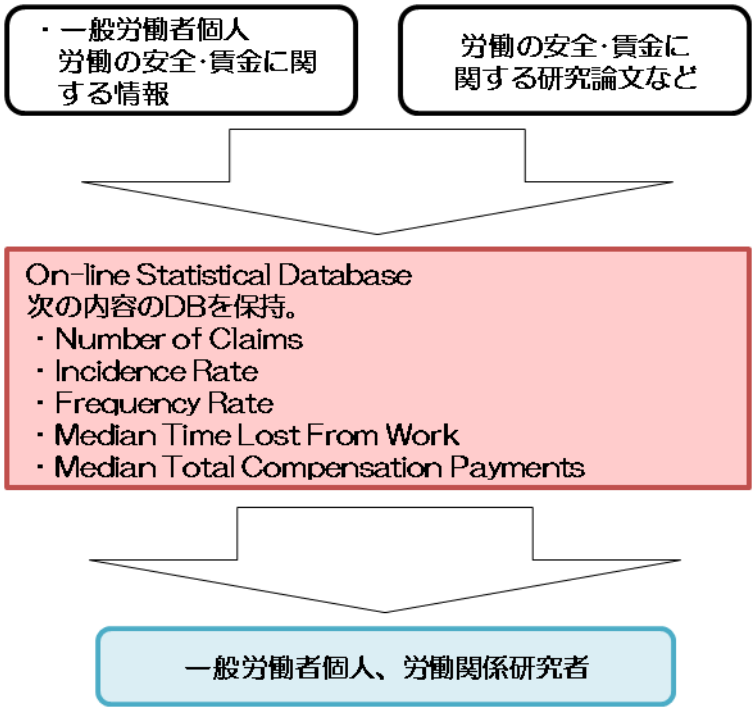

図 4-11　NOSI のサービス形態

4.1.10 NHS Secondary Uses Service

(URL: http://www.ic.nhs.uk/services/secondary-uses-service-sus)

(1) 概要

NHS 情報センター(The Health and Social Care Information Centre)は、最前線の意思決定者のために、英国の健康と社会医療に関する情報提供を行う。医療機関で収集した医療関連情報を集約し、提供する。具体的に取り扱う情報は、次の通りである。

(1)Audits and performance
Ambulance, National clinical audits, Complaints, The Quality and Outcomes Framework
(2)Health and lifestyles
Alcohol, Contraception, Diabetes, Diet, Drug misuse, Immunization, NHS stop smoking services, Obesity, Physical activity, Smoking
(3)Hospital care
Accident and emergency, Cancer, Coronary heart disease, Critical care, Hospital activity (HESOnline), Maternity, Outpatients, Patient Reported Outcome Measures (PROMs)
(4)Mental health
Mental Health Act, NHS specialist mental health services, Mental Health Surveys
(5)Population, geography and international
Vital Statistics, Digital Mapping, International Statistics collections for the UK, Populations data and managing the Population Statistics Database (PSD), Primary Care Mortality Database (PCMD), Geographies and NHS organizational changes, Neighborhood statistics, GP Registered Populations, Public health
(6)Primary care
Pharmacies, Prescriptions, General practice, Dentistry, Eye care
(7)Screening
Breast screening, cervical screening
(8)Social care
Adult social care information, Career support, Learning disability, Older people, Disability, Children's social care, User surveys
(9)Workforce
NHS staff numbers, NHS staff earnings, NHS staff turnover, NHS and GP vacancies, Sickness absence

図 4-12 NHS が保持するデータ

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

取り扱うパーソナル情報の範囲は、一般患者の医療関係情報である（図 4-12 参照）。

(3) データの種類、形式、用途

匿名化された一般患者の医療関係情報に加えて、関連する医学研究者の研究情報を、病院、社会医療関係者向けに提供する。

(4) リスクに対する管理策・アセスメント結果

匿名化処理に関する特記事項はない。

(5) 二次利用サービスの形態

病院、社会医療関係者向け、医療機関で収集した図 4-13 の領域の医療関連情報を集約し、公開している。

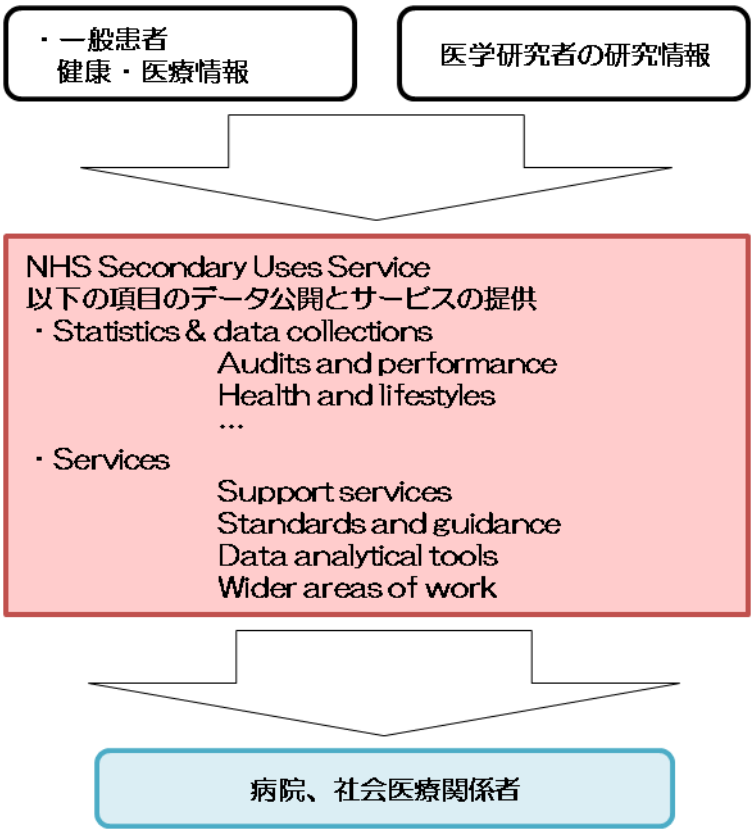

図 4-13　NHS Secondary Uses Service のサービス形態

4.1.11 Data Archives

（URL: http://www.data-archive.ac.uk/）

(1) 概要

英国で最大の社会、経済領域のデータセットである。2 大テーマは以下の通りである。

- 健康
- 犯罪と社会の制御

研究と教育のための 5,000 以上の社会的データへのアクセスに経済で高範囲のデータを含む。

利用者がデータを預けることができる。取り扱うデータは次の通りである。

(1)Economics

Consumer behaviour; Economic conditions and indicators; Economic systems and development; Income, property and investment

(2)Education

General; Higher and further; Literacy; Primary, pre-primary and secondary; Research; School leaving; Teaching profession

(3)Employment and labour

General; Industrial relations; Retirement; Training; Unemployment

(4)Environment, conservation and land use

Energy and fuel; Environmental and conservation issues; Land use and planning; Natural landscapes; New town studies; Plant and animal distribution

(5)Health

Accidents and injuries; Childbearing, family planning and abortion; Drug abuse, alcohol and smoking; General; Health services and medical care; Mental health; Nutrition; Physical fitness and exercise; Specific diseases and medical conditions

(6)History

Administrative history; Agricultural and rural history; Cultural history; Ecclesiastical and religious history; Economic history; Education history; Gender history; Historical geography; Historiography; Imperial and colonial history; Intellectual history; International and diplomatic history; Legal history; Local history; Medical history; Military, naval and maritime history; Political history; Population history; Science and technology history; Social history; Transport history; Urban history

(7)Housing

(8)Industry and management

Agriculture, forestry and rural industry; Industrial/commercial location; Management and organisation; Trade, industry and markets

(9)Law, crime and legal systems

Crime and law enforcement; Legislation and legal systems

(10)Media, communication and language

Information technology; Language and linguistics; Mass media

図 4-14 Data Archives が取り扱うデータの分類

(11)Politics

Conflict, security and peace; Election and campaign studies; Election returns; Government and political systems; International politics and organisations; Political behaviour and attitudes

(12)Population, vital statistics and censuses

Migration; Morbidity and mortality; Population censuses; Population studies; Vital statistics

(13)Psychology

(14)Reference and instructional resources

Computer and simulation programs; Reference sources; Teaching packages and test datasets

(15)Regular opinion polls

(16)Science and technology

(17)Society and culture

Community and urban studies; Leisure, tourism and sport; Race relations; Religion and values; Rural life; Social attitudes and behaviour; Social indicators and quality of life; Time use

(18)Social stratification and groupings

Child development and child rearing; Elderly; Elites and leadership; Equality and inequality; Ethnic minorities; Family life and marriage; Gender roles; Social and occupational mobility; Youth

(19)Social welfare policy and systems

Charities, voluntary organisations and voluntary work; General; Use and provision of specific social services

(20)Travel and transport

図 4-15 Data Archives が取り扱うデータの分類(続き)

(2) 取り扱うパーソナル情報の範囲（医療情報、統計情報など）

社会学研究の一次データに含まれるもので多様なパーソナル情報が考えられる。

具体的には、図 4-14 の分野情報から、個人の経済的活動に関する情報、個人の教育に関する情報、個人の健康に関する情報などが含まれることが考えられる。

(3) データの種類、形式、用途

図 4-14、図 4-15 に示した通りの分野のデータを取り扱う。一般利用者・関連分野研究者に提供する。

(4) リスクに対する管理策・アセスメント結果

匿名化手法をガイドとして紹介している。データ預け入れ者が、そこでのガイドも参考にして匿名化することを想定していると考えられる。

(5) 二次利用サービスの形態

一般利用者・関連分野研究者向け、「健康」と「犯罪と社会の制御」を 2 大テーマとする英国で最大の社会、経済領域のデータセットを提供する。

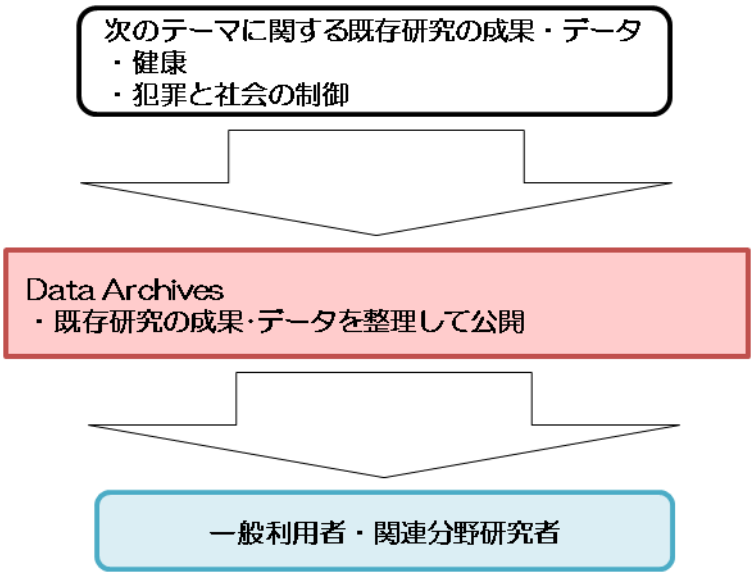

図 4-16　Data Archives のサービス形態

4.1.12 まとめ

事例調査を通して、匿名化指標に基づいて匿名化されたパーソナル情報を用いたサービスの事例は非常に少ないことを確認した。

医療分野においては、匿名化されたパーソナル情報を提供するサービスが実施されている。その他の分野では、統計情報として提供するケースが多いことを確認した。

匿名化されたパーソナル情報の提供サービスでは、その多くが研究者向けに実施されている。

4.2 匿名情報の取扱いに関する認証スキーム事例

4.2.1 詳細調査の目的と方法

詳細調査では､3.6.1 項で挙げた国内外のパーソナル情報の取扱いに関する認証スキームの先進的事例について、匿名化・認証プロセスの実態を明らかにした。

詳細調査の対象は、海外 2 件(The Children's Hospital of Eastern Ontario(CHEO)、MedMining)と国内 1 件（統計センター）である。特に、CHEO と統計センターについては現地ヒアリング調査を実施した。また、CHEO の監督機関であるオンタリオ州プライバシー・コミッショナー(IPC)にも訪問し CHEO との関係などについてヒアリング調査を実施した。

はじめに、詳細調査を通して整理する項目を表 4-2 に示す。

表 4-2 の項目『パーソナル情報の収集』は、パーソナル情報を収集する際の手続きに関わる事項であり、収集するデータの種類と、収集に際して利用目的を明示しているか、同意を得ているかを確認する。

同様に『匿名化』は、パーソナル情報の二次利用に際して、匿名化を実施しているかどうか、実施している場合、手法は何を選択しているのか、個別パラメータの設定はどのようにしているかを確認する。

『匿名化プロセス審査』では、匿名化されたデータの利用申請に対する審査の詳細を確認する。実際に審査を実施しているかどうか、実施している場合、審査プロセスの概要はどうなっているのか、データの管理方法はどのようになっているのかを確認する。

『匿名化評価』では、匿名化を実施する際の基準について確認する。実際にどういう条件を満たせば匿名化されたと認めるのか、どのように評価するのかについて確認する。

『認証対象』では、匿名情報の利用に対する認証の対象を確認する。機関・組織が対象の場合、その機関・組織は十分に安全な匿名情報を作ることができるため、匿名情報を流通させて良い、という扱いになる。同様に、ツールが対象の場合、認証を受けたツールを用いて匿名化すれば匿名情報を流通させて良い、という扱いになる。また、データが対象の場合、ある基準を満たして匿名化されたデータであると認められたデータについては流通させて良い、という扱いになる。

表 4-2　詳細調査の調査対象項目

匿名化・認証プロセス	
パーソナル情報の収集	収集するデータの種類（取り扱うデータの範囲）
	利用目的の明示の有無
	ユーザの同意の有無
匿名化	匿名化の有無
	手法の詳細
	個別パラメータの設定等
匿名データ利用に対する審査	審査の有無
	審査プロセス（概略）
	データの管理方法等
匿名化評価	匿名化評価基準の有無
	評価基準
	評価方法
認証対象（機関・組織／ツール／データ）	匿名情報の利用に対する認証の対象

4.2.2 The Children's Hospital of Eastern Ontario(CHEO)

(1) 組織概要

The Children's Hospital of Eastern Ontario(CHEO)は、カナダ・オンタリオ州・オタワにある、小児医療と研究を行う機関である。1974 年に開院し、スタッフ数 4,500 名程度（2008-2009 年）とされる。University of Ottawa Health Sciences Centre と提携している。

また、匿名化の専門家が所属している CHEO Research Institute(CHEO RI)は、CHEO 付設の研究機関であり、1984 年に設立された。University of Ottawa Teaching Hospitals と提携している。CHEO 内外での共同研究などを実施しており、後述の研究倫理委員会(Research Ethics Board)も CHEO RI 内に存在している。以下では CHEO と CHEO RI を総称して CHEO と記載する。

(2) 匿名化・認証プロセス

CHEO における、匿名化・認証プロセスを図 4-17 に示す。図は、匿名情報の利用を申請して、実際に匿名情報が提供されるまでの手順を簡略に示している。特徴としては、データアクセス委員会のリスク査定による申請からデータ提供までの期間を短縮した点にある。以下ではこの手順を説明する（表 4-3 参照）。

まず、申請者は、利用申請を CHEO のデータ利用窓口に出す。利用申請には、研究プロジェクトの情報、研究目的、利用したいデータに関する情報などを所定のフォームに記入した文書を添える。この窓口の実体は、データアクセス委員会(DAC)である。DAC という名称は、CHEO 以外の病院組織でも一般的に使われる名称であるが、CHEO の場合、DAC の運用実態が他の組織とは大きく異なる。一般に、DAC は多数の委員により構成される委員会であり、必要に応じて会合を開き、データ利用申請などについて、審議をする。その結果、日程調整や申請の許可・不許可の議論に時間を要する。CHEO の場合は、名称だけは混乱を避けるため他の組織とそろえているが、実際には 3 名の職員がツールを使って持ち回りで申請に対応している（図 4-17①）。

次に、DAC は、リスク査定を PARAT というツールを用いて実行する。このツールでは、ISO/IEC 27002（企業などの組織における情報セキュリティマネジメントシステムの仕様を定めた規格）などに基づくチェックリストを申請に対してチェックし、リスクを定量的に算出する（図 4-17②）。リスク査定の詳細は 4.2.2(3)項に別途記載する。

リスクを算出した結果、CHEO にとって許容できるリスクであれば、次の段階に進めるが、実態としては、申請時には常にリスクが大きすぎて調整が必要になる。DAC は、申請者に対してデータ共有協定の項目や、データの匿名化の項目毎の強弱について協議をし、合意に至る。この際、リスクが許容できる範囲であるという証明書、データ共有協定、契約書も作成する（図 4-17③）。

なお、申請者は必要に応じて科学レビュー委員会からも承認を得る必要があるが、この委員会の実態は研究ファンドであることが多い（図 4-17④）。

最終的な意志決定は、研究倫理委員会(REB)の判断に委ねられるが、その際に DAC からリスク査定の結果、リスクは許容範囲であるという証明書やデータ共有協定が添付される。これらの情報を基にして、REB では申請に対する判断をする（図 4-17⑤）。

REB での許可を得た後、DAC はデータベース管理者に依頼して、匿名情報を作成し、申請者に暗号化して送付する（図 4-17⑥⑦）。

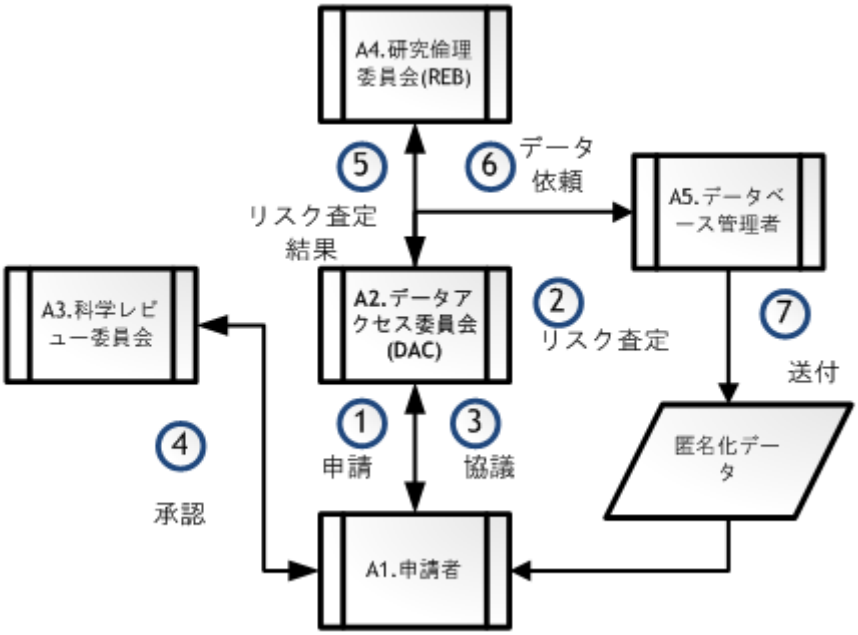

図 4-17　CHEO における匿名情報利用認証のプロセス

表 4-3　CHEO における匿名情報利用認証のプロセスの説明

番号	説明	関連文書
1	申請者(A1)が CHEO のデータアクセス委員会(DAC, A2)に申請をする。	・データリクエストフォーム
2	DAC がリスク査定を実施する。	―
3	リスク査定結果を基に、申請者と匿名情報の精度やデータ共有協定について協議する。	・データ共有協定 ・契約書
4	（必要に応じて）科学レビュー委員会(A3)から承認を受ける。	―
5	DAC から研究倫理委員会(REB, A4)に対してリスク査定結果などを通知する。	・リスク証明書
6	REB で承認された場合、データベース管理者(A5)に匿名情報の作成を依頼する。	―
7	データベース管理者から匿名情報を申請者に送付する。	―

CHEO の匿名化・認証プロセスについて、表 4-4 に整理した。

収集するパーソナル情報は、CHEO で作成されるレセプト（診療報酬明細書）などが該当する。オンタリオ州の PHIPA では、匿名化された個人情報を法の適用外としているが、CHEO では匿名情報の流通を利用申請者にとどめるよう、契約で抑制している。データの匿名化には、局所秘匿化(Local Suppression)[43]と大域的再符号化(Global recoding)[44]を使用している。

[43] セルデータの削除

匿名化の度合いはリスク査定の結果に依存するが、通常 k-匿名性(k-anonymity)の k の値は 5 以上としている。

匿名情報利用の認証手順は上述の通りである。

CHEO の匿名化・認証プロセスの特徴は、データアクセス委員会にある。名称は他の同等の機能を有する機関と揃えているが、実態は 3 名の職員が持ち回りで利用申請のリスク査定をしている。リスク査定をツールで定量的に行うことで、従前のデータアクセス委員会での審議の長期化などを回避している。

表 4-4　CHEO の匿名化・認証プロセスの整理

匿名化・認証プロセス		内容
パーソナル情報の収集	収集するデータの種類（取り扱うデータの範囲）	Personal Health Information（CHEO にて作成される医療情報）
	利用目的の明示の有無	有 CHEO のウェブサイト[45]に Privacy Policy の記載がある。ケアの提供、治療の対価、研究と統計データ作成のため、などの項目を明記している。
	ユーザの同意の有無	有（ただし、匿名化されれば Personal Information ではないという立場をとる）
匿名化	匿名化の有無	有
	手法の詳細	局所秘匿化と大域的再符号化（k-匿名性）。準識別子、リスクしきい値（検察、ジャーナリスト、マーケティングによる攻撃を想定）を指定し、リスク分析をした上で匿名化を実施。
	個別パラメータの設定等	研究者がチェックリストで利用したいデータフィールドを提出する。データアクセス委員会(DAC)と研究者の間でリスク査定を経て決定される。
匿名データ利用に対する審査	審査の有無	有
	審査プロセス（概略）	1. 申請者(A1)が CHEO のデータアクセス委員会(DAC, A2)に申請をする。 2. DAC がリスク査定を実施する。 3. リスク査定結果を基に、申請者と匿名情報の精度やデータ共有協定について協議する。 4. （必要に応じて）科学レビュー委員会(A3)から承認を受ける。

44 集合匿名化の手法の一つである一般化のうち、テーブル全体のデータを一般化階層の上位の値に書き換える匿名化の手法。

45 http://www.cheo.on.ca/en/PrivacyandConfidentiality?mid=ctl00_LeftMenu_ctl00_TheMenu-menuItem009

匿名化・認証プロセス		内容
		5. DAC から研究倫理委員会(REB, A4)に対してリスク査定結果などを通知する。 6. REB で承認された場合、データベース管理者(A5)に匿名情報の作成を依頼する。 7. データベース管理者から匿名情報を申請者に送付する。
	データの管理方法等	データの匿名化、リスク査定はデータベース管理者の管理下で実行する。
匿名化評価	匿名化評価基準の有無	有
	評価基準	ID 開示リスク（k の値と連動）、データ共有契約
	評価方法	PrivacyAnalytics Tool（リスク査定ツール）を用いたリスク分析、データを共有する組織が病院外かどうかなど。
認証対象（機関・組織／ツール／データ）		データ

(3) リスク査定

図 4-17②に記したデータアクセス委員会におけるリスク査定について記載する。

CHEO のリスク査定の概念は、図 4-18 を用いて説明される。中央に Risk Exposure（組織として取れるリスク）があり、四つの項目が作用している。

- Re-identification Probability（ID 開示の確率）
- Mitigating Controls（軽減制御）
- Motives & Capacity（ID 開示のモチベーションと能力）
- Invasion-of-Privacy（プライバシーの侵害）

前者 2 項目は、CHEO 側が制御できる項目であるが、後者 2 項目はデータ申請者に依存する項目である。

CHEO 側が制御できる 2 項目について、ID 開示の確率は提供するデータの匿名化度合いを制御することにより調整できる。軽減制御は、申請者にデータの管理について厳重に実施するよう契約ベースで強制することにより調整できる。

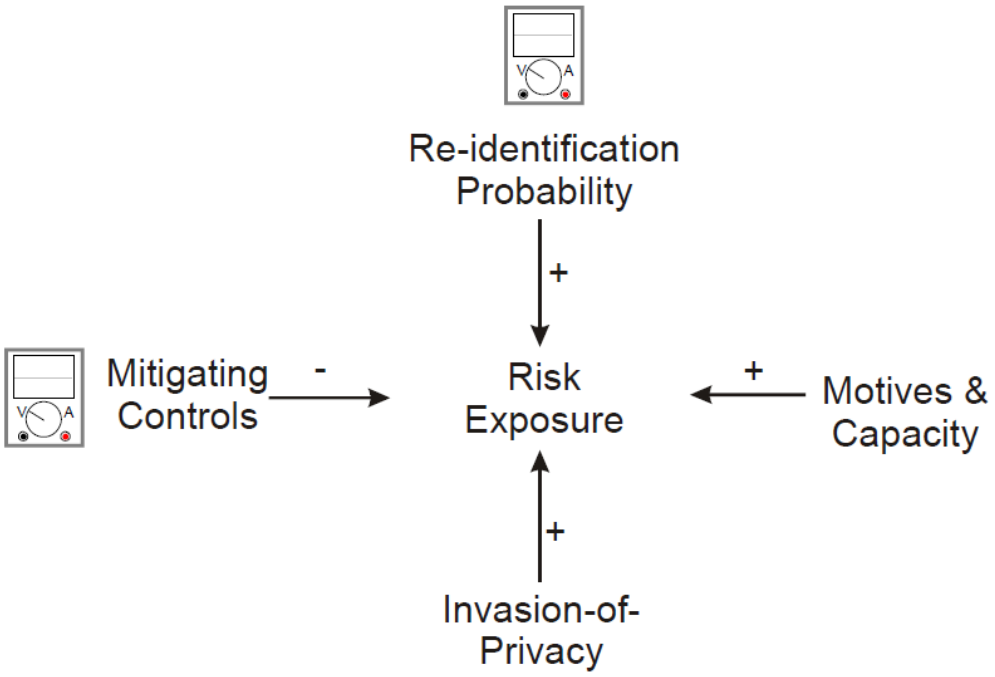

図 4-18　CHEO のリスク査定の概念図（出典：El Emam K: De-identifying health data for secondary use: A framework. Ottawa: CHEO Research Institute; 2008.）

表 4-5　CHEO 運用のリスク査定で用いる審査項目[46]

審査項目
■軽減制御
認証されたスタッフのみがデータにアクセスできるようにする
データ共有協定を締結している、またはこれから締結する
秘密保持契約をスタッフと外部協力者に対して結んでいる
個人を特定できないデータ、および集合データのみ公開する
長期保有の際には外部監査を受ける
保有期間を過ぎたデータは廃棄される
データは国内でのみ処理、保持、アクセスできる
第三者への開示と共有をしない
情報システムに対する脅威、およびリスク脆弱性の監査を実施する
プライバシー、機密性、セキュリティに関して組織的な管理フレームワークをもつ
データ保持、管理、アクセスに関して、組織的なポリシーを持つ
プライバシーとセキュリティポリシーが監視され、効力を持つ

[46] 出典：EMAM, K., DANKAR, F., VAILLANCOURT, R., ROFFEY, T., LYSYK, M.. Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records. The Canadian Journal of Hospital Pharmacy, North America, 62, jul. 2009. Available at: http://journals.sfu.ca/cshp/index.php/cjhp/article/view/812.に基づき三菱総合研究所が作成

審査項目
関係者に対するプライバシー、機密保持、セキュリティのトレーニングを強制的に適宜実施している
プライバシー、機密、セキュリティの違反時の罰則がある
プライバシーオフィサーやデータ管理委員会が任命されている
プライバシー違反時のプロトコルがある
プライバシー監査が内部・外部ともある
情報システムに適切な認証を掛けている
データに適切な認証をかけている
データへのリモートアクセスに対し、特別な保護機構を導入している
ウィルスチェックを実施している
利用記録をシステムによりモニタリングしている
データを電子的に送付する際には、暗号プロトコルが使われる
開示データを含むコンピュータやファイルは厳重に施錠管理された場所に置かれる
スタッフには、写真付きの ID、または磁気カードが与えられる
訪問者をスクリーニング、管理する
アラームシステムが設置されている
パーソナル情報が保存される場所の数は最小限にとどめ、あらかじめ特定されている
センシティブデータを保持する場所では一般の人が入れないようにする
定常的な敷地内の監視が実施されている
物理的なセキュリティ対策がなされている
プライバシー担当者のコンタクト情報が提示されている
従業員管理担当者のコンタクト情報が提示されている
組織の透明性と、情報公開の仕組みが整っている
苦情窓口をもっている
REB のような独立した権威がデータの二次利用に関わる提案を承認している
内外の監査、モニタリング機構が導入されている
独立諮問機関、または管理委員会が監視する
■プライバシーの侵害
データの詳細度、データのセンシティブさ、などからプライバシー侵害の影響を測る
■モチベーションと能力
申請者にとって匿名情報を再 ID 化するモチベーションとその能力を測る

CHEO では、リスクの判断を Privacy Analytics Risk Assessment Tool(PARAT)という Privacy Analytics[47]社のツールを用いて実施している。ツールの利用手順は次の通りである。

まず、申請者が要求しているデータセットの中から準識別子を指定する。これは、個人を間接的に識別しうる情報を指す。

次に、許容できるリスクのしきい値を設定する。これは、上述のチェックリストへの回答により導出される。導出のアルゴリズムは Privacy Analytics 社の経験則に基づく。

しきい値を設定した後で、リスク分析を PARAT が実施する。ここでのリスク分析には、想定される三種類の攻撃者モデルが用いられる点に特徴がある。三種類の攻撃者モデルとは、Prosecutor（検察）、Journalist（ジャーナリスト）、Marketer（マーケッター）である。それぞれの特徴を図 4-19 に記載する。個人に対する攻撃のリスクが大きいのは Prosecutor であるが、例えば攻撃者が隣人などの場合が該当する。

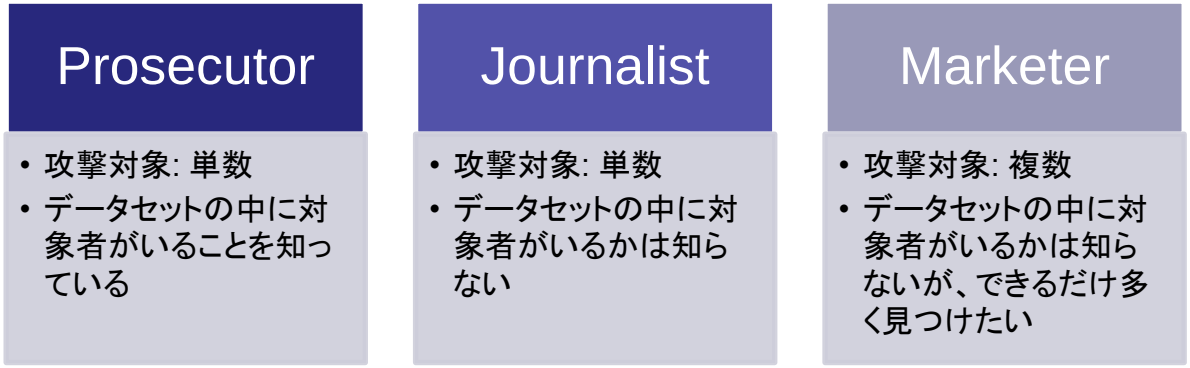

図 4-19　三種類の攻撃者モデル

リスク分析の結果、設定したしきい値内にリスクの定量値が収まればデータをそのまま提供できるが、多くの場合リスクがしきい値を超えるため、データの匿名化処理が必要となる（図 4-21 参照）。

PARAT における匿名化は、大域的再符号化（データの一般化）と局所秘匿化（特異なデータレコードの削除）により実現されている。特に、大域的再符号化に関しては、全域最適匿名化を高速に実行するアルゴリズムを実装している[48]。なお、大域的再符号化におけるデータの一般化の例としては、図 4-20 の入院期間が挙げられる。例えば、準識別子として、居住地域と入院期間を指定した場合、仮に地区 A 在住の人で入院期間が 50 日だった人が一人しかいない場合、”5weeks”、”2month”と適切な k の値を満たすまで全レコードの入院期間を一般化する。

[47] http://www.privacyanalytics.ca/ CEO は CHEO の El Emam 博士

[48] Khaled El Emam, Fida Kamal Dankar, Romeo Issa, Elizabeth Jonker, Daniel Amyot, Elise Cogo, Jean-Pierre Corriveau, Mark Walker, Sadrul Chowdhury, Regis Vaillancourt, Tyson Roffey, Jim Bottomley, A Globally Optimal k-Anonymity Method for the De-Identification of Health Data, Journal of the American Medical Informatics Association, Volume 16, Issue 5, September-October 2009, Pages 670-682, ISSN 1067-5027, DOI: 10.1197/jamia.M3144.
(http://www.sciencedirect.com/science/article/B7CPS-4X5J6WG-C/2/0f6bb93202b116b49d7aab4891f8d8df)

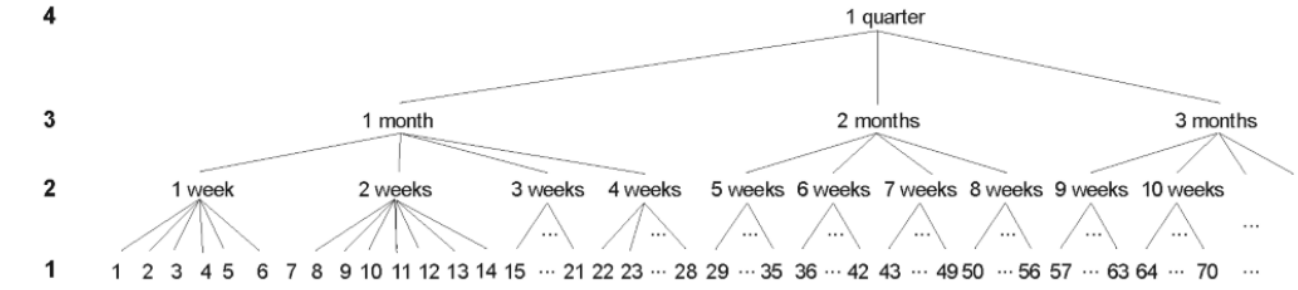

図 4-20　匿名化一般化階層の例（入院期間）

（出典：EMAM, K., DANKAR, F., VAILLANCOURT, R., ROFFEY, T., LYSYK, M.. Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records. The Canadian Journal of Hospital Pharmacy, North America, 62, jul. 2009. Available at: http://journals.sfu.ca/cshp/index.php/cjhp/article/view/812.）

匿名化した後のリスクについても PARAT により算出され、可視化される（図 4-22 参照）。これにより、許容範囲内にリスクが収まれば、データの匿名化処理と、データの提供を行う。

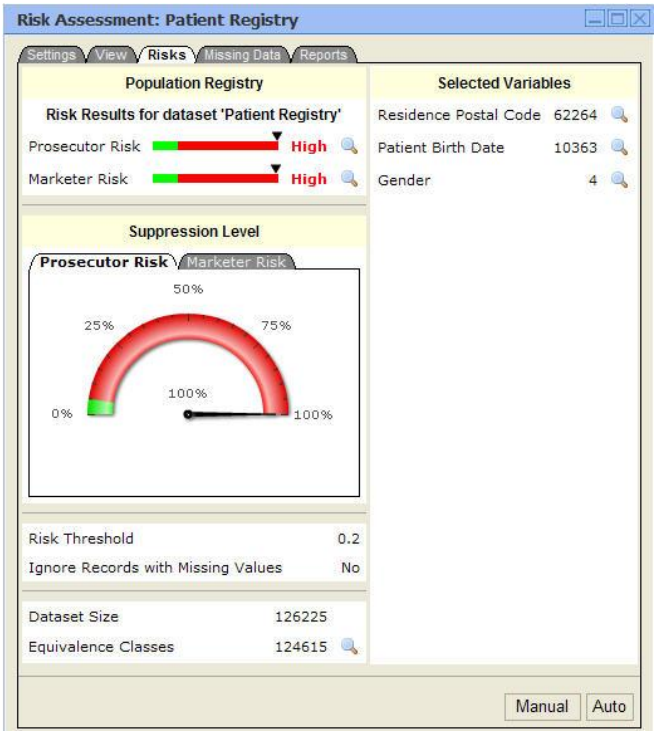

図 4-21　PARAT によるリスク分析イメージ（匿名化前）

（出典：CHEO RI & uOttawa, www.ehealthinformation.ca）

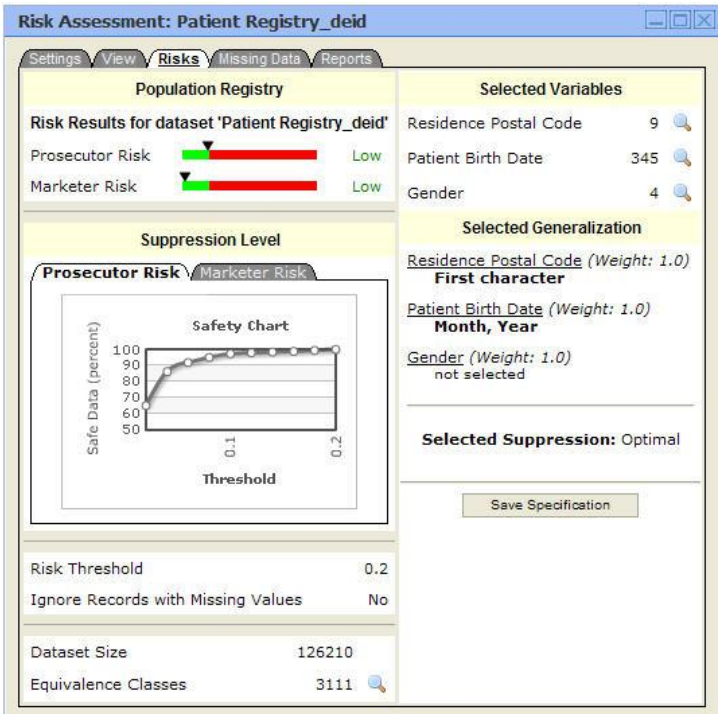

図 4-22　PARAT によるリスク分析イメージ（匿名化後）

（出典：CHEO RI & uOttawa, www.ehealthinformation.ca）

PARAT によるデータの流れを整理すると図 4-23 のようになる。PARAT は、リスク査定レポートとリスクが所与のしきい値の範囲内であることを示す証明書を発行するほか、匿名化処理の設定ファイルも出力し、匿名化処理と連動して動作する。

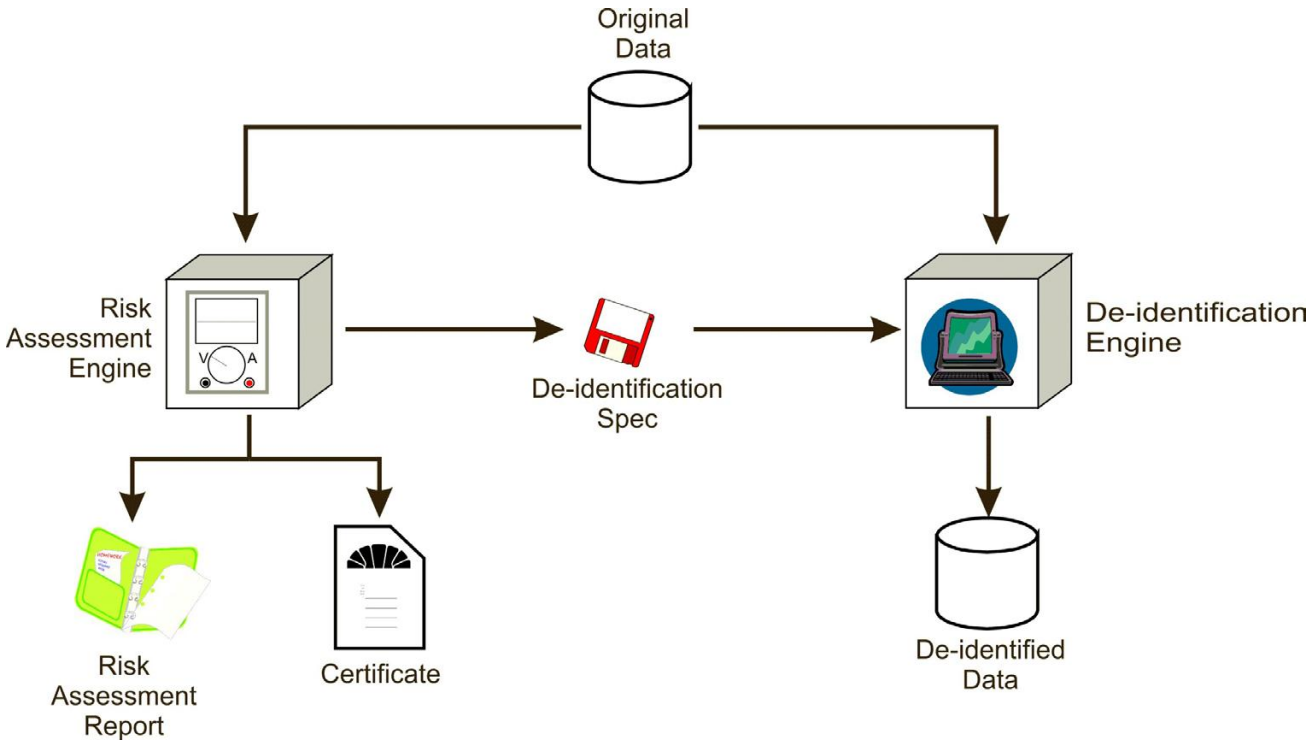

図 4-23　PARAT に関係するデータの流れ（出典：PARAT Brochure, Privacy Analytics, 2010）

(4) ヒアリング結果の要点

以下では、CHEO の実地調査で判明した、CHEO における匿名情報提供の認証の背景、プロセス、運用状況について整理する。

表 4-6 CHEO の実地調査結果

背景の要点	
ニーズ駆動で始められた匿名情報の提供	匿名情報の提供を始めたのは、データベースのサイズが大きくなり、利用ニーズが増えたためであり、匿名化は唯一の実践的、合法的な手段であった
	オンタリオ州の個人医療情報保護法(PHIPA)の制定と直接は関係ない。
born という匿名情報提供インフラが 2009 年より構築	オンタリオ州全域の新生児と母親のレジストリ。毎年 125,000 件の登録がある。
	匿名情報の提供をしている。CHEO のプロセスを原型とし、El Emam 博士が参画している。
北米の匿名情報提供の判断はリスクベースが中心	リスクを定量化し、判断は Chief Privacy Officer などが行うという方式が主流になりつつある。
データ提供の判断が 1 週間で済むようになった	Privacy Analytics Risk Assessment Tool(PARAT)ツールによる、リスクの定量化の主要な効果といえる。
	以前は数ヶ月から半年かかっていた。
認証プロセスの要点	
匿名情報の提供の認証をリスク査定ベースで行い、ツールにより高速化することが特徴	匿名情報を利用申請者に提供するかどうかの判断は、他機関と同様、研究倫理委員会が行う。
	研究倫理委員会の判断材料となる定量的なリスク査定をツールにより実施し、判断を高速化する点において、CHEO は先進的である。
リスク査定をチェックリストを用いて多角的に行う	申請者による申請情報(Mitigating Controls) ISO/IEC 27002（情報セキュリティ管理）より作成された項目。 申請者の組織における、情報セキュリティ、秘密保持などについて。
	査定情報(Motives and Capacity、Invasion of Privacy) 申請者から見たデータの価値や、データ流失時の被害の大きさなどについて。
リスク査定ツールによる査定結果を見ながら、匿名化のレベルを協議する。	どこかの段階で折り合いを付ける。過去に一度だけ、匿名化のレベルに満足せずに、CHEO のセキュリティルームに来て研究をした事例がある。

リスク査定ツールは、証明書（リスクは許容範囲）、データ共有協定、契約書のひな形を出力する。	リスク査定の際に調査した内容と連動した文書のひな形を出力する。
運用状況の要点	
件数	born の場合は年に 15-20 件と予測。その他の関係するレジストリでは申請が 1 日に 2-3 件あるものも存在する。
	非認可になったことは無い。申請者の要望に答えられるよう調整していく。
主要な利用者	研究者と公的医療機関が大部分を占める。
	Brogan 社は例外的に多い。
体制	匿名化のリスク査定は、通常業務の範囲内で El Emam 博士ら 3 名が、持ち回りで担当している。
再配布	再配布は契約で認めないようにしている。なお、研究成果のデータを公開する場合、リスク査定のしきい値が厳しくなる。その結果、データの匿名化度合いは高くなる。
海外展開	カナダやアメリカなど、契約の強制力があるところでは機能するが、インドなど強制力の弱い地域での扱いが今後の懸案となっている。リスク査定の項目に含めることを検討している。

(5) プライバシー・コミッショナー － IPC

CHEO はカナダのオンタリオ州に存在するため、オンタリオ州のプライバシー・コミッショナー(IPC)の監督下にある。CHEO は IPC から見ると”Data Custodian”（データ管理者）という立場になる。実際に両者の関係についてヒアリング調査を実施した結果を以下に記す。

CHEO の El Emam 博士は、匿名情報の提供を始めるに当たり、データの匿名化について IPC でプレゼンテーションを実施している。ただし、その後 IPC は CHEO への定期的な監査を実施してはいない。他の機関と同様に、違反があればレビューを実施するという立場を取っている。

オンタリオ州では、Canadian Institute for Health Information や Cancer care in Ontario といった公的医療機関も行政や研究のためにデータを二次利用できるようにしている。IPC では、こうした他のデータ管理者にも PARAT を使うように指導しているとのことである。

なお、オンタリオ州 IPC のコミッショナーである Cavoukian 博士は CHEO の El Emam 博士と医療分野の Privacy by Design(PbD)に関する共著もある[49]。PbD は、概念的なフレームワークで、IT、ビジネス、インフラを設計する段階でプライバシーを組み込んでおくという思想を持つ[50]。この PbD の基本原理に Positive-Sum という項目がある。これはプライバ

[49] IPC - Office of the Information and Privacy Commissioner/Ontario | Whats New Summary http://www.ipc.on.ca/english/About-Us/Whats-New/Whats-New-Summary/?id=145

[50] PbD には、スマートグリッド、クラウド、バイオメトリクスなど、新しい分野における適用報告が多く公開されているほか、EU や米国でも採用が進められている。例えば、EU のデータ保護指令は古くなっており、レ

シーを設計時の要件として組み込むことにより、他のセキュリティなどの要件を犠牲にするわけではない、という考え方である。CHEO の匿名化の場合、プライバシーと匿名情報の品質との双方を獲得することができている例として扱われている。

(6) クライアント – Brogan

CHEO の匿名情報の主要な利用者は、研究者と公的医療機関であり、両者で 8 割を占める。ただし、Brogan 社は民間からの利用としては例外的に多いと CHEO、IPC 双方で言及されていた。

Brogan 社は、レセプト（診療報酬明細書）などの非 ID 化したデータを集めて分析したレポートを医薬開発会社に販売している。主要な顧客は、国際的な製薬会社、民間の処方薬保険業者、カナダの州政府とされている。Brogan 社の商品は以下の通りである[51]。

- Rx Dynamics
  - 月次の総合的な分析統計レポート。一日の平均服用量や複合薬の使用割合など医薬品の使用についてのデータならびに関連のビジネスデータを提供
  - 州（オンタリオ州）のデータ、または国・地域レベル（カナダ東部、ケベック、オンタリオ、西部諸州）の民間のデータを提供
- PharmaStat
  - 公的および民間のドラッグプラン（薬剤費給付プラン）で支払われた薬品毎の売上データを提供するオンラインアプリケーション
  - 請求額、請求件数、およびカナダで販売されている全医薬品の販売数などを把握できる
- Rx Ticker
  - 民間のドラッグプランの市場シェアについて、週単位の統計レポートを提供するインターネットアプリケーション
  - カナダの最新の医薬品販売実績を提供。患者全体および新規患者集団の国および地域シェア（カナダ東部、ケベック、オンタリオ、西部諸州）も把握できる
- iMAM
  - フォーミュラリー（補償対象の医薬品を掲載する優先選択薬剤リスト）の詳しい分析情報を提供するインターネットアプリケーション
  - 1990 年以降のカナダ 10 州のフォーミュラリー等について、医薬品、機器、栄養製品のリスト掲載状況およびその基準などが把握できる
- GPM
  - 薬局処方薬の売上についての月次レポート。各地域より報告され、全国をカバーしている

ビュープロセスを進めているが、European Data Protection Supervisor(EDPS)の Peter HUSTINX 氏は、レビュープロセスには PbD をフレームワークとして使うべきだと言及している。米国でも連邦取引委員会(Federal Trade Commission)のチェアである Jon Liebowitz 氏もプライバシー保護規制の見直しには PbD アプローチに従うとしている。

[51]出典：Brogan Inc. サイト http://www.broganinc.com/english/products/index.html

- 本レポートには、処方薬売上の予測・実績や市場シェア、薬局医薬品の売上高等が掲載されている

なお、Brogan 社は 1989 年に設立された企業だが、2010 年 6 月に IMS Health Canada と合併し、IMS Brogan という IMS の 1 ユニットになっている。その 4 ヶ月前の 2010 年 2 月に、IMS Health Canada の親会社である IMS Health はプライベートエクイティの TPG Capital, L.P.と CPP Investment Board に買収されている。カナダにおいて匿名医療情報の二次利用のマーケットが注目されていると言える。

4.2.3 MedMining

(1) 組織概要

MedMining 社はアメリカ・ペンシルバニア州の Geisinger Health System の出資するベンチャー企業であり、2006 年に設立された。Electronic Medical Record(EMR)から ID を除いて、製薬、バイオテクノロジー、医療器具関係の企業に販売している。Geisinger の三つの病院、40 の外来診療所、二つの研究所のデータがデータセットの基である。

MedMining 社では、個人の属性や、特定の病気のデータに加え、費用（入院時の実費、支払いなど）などのデータも提供している。

(2) 匿名化・認証プロセス

MedMining社における匿名化･認証プロセスの概略を図 4-24に､主な手順の説明を表 4-7にそれぞれ示す。申請者は、製薬会社・バイオテクノロジー企業が多いとされ、研究用途に限定しての提供とされる。MedMining 社内外に監督機関を設けており、社内については内部監査員（社内の法務部と社外の弁護士)、社外については、Honest Broker System という社外の HIPAA､個人医療情報､研究に精通した専門家からなる第三者機関により審査される。Honest Broker System の管理をする主体は、MedMining の出資元の Geisinger 社のプライバシー部門である。

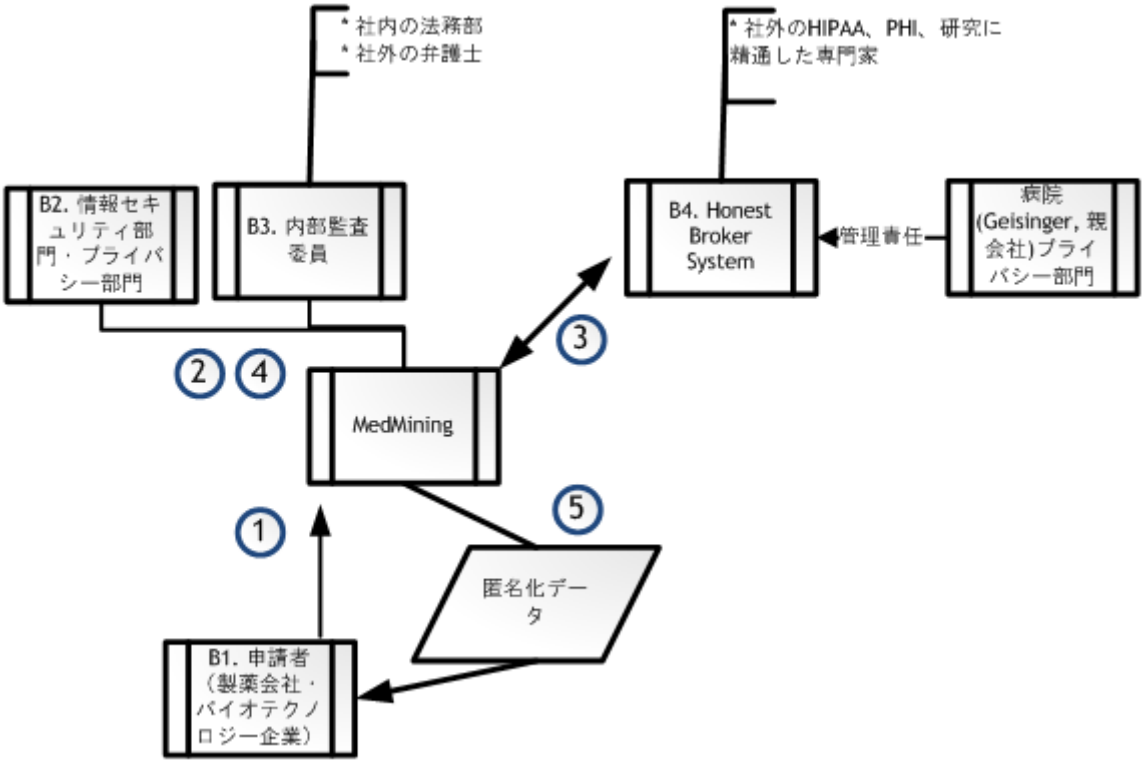

図 4-24　MedMining 社における匿名化・認証プロセスの概要

表 4-7　MedMining 社における匿名化・認証プロセスの概要の説明

番号	説明
1	申請者(B1)が MedMining 社に申請をする。
2	MedMining 社の情報セキュリティ部門・プライバシー部門(B2)と内部監査委員会(B3)の確認を受ける。
3	社外諮問機関である Honest Broker System(B4)に確認を受ける。
4	MedMining 社のプライバシー部門の確認を受ける。
5	匿名情報を申請者に送付する。

MedMining 社における匿名化・認証プロセスについて表 4-8 に整理した。出資元の Geisinger 系の医療機関において収集した医療情報を匿名情報の基データとして利用する。匿名化自体は、HIPAA（3.3.2(5)参照）に準拠して非 ID 化を実施している。匿名化プロセスの特徴としては、Honest Broker System という外部有識者による審査機関を設けていたことがある。ただし、匿名化の手法やプロセスにおける具体的な情報のやり取りについては公開されていない。

表 4-8　MedMining 社における匿名化・認証プロセス

匿名化・認証プロセス		内容
パーソナル情報の収集	収集するデータの種類（取り扱うデータの範囲）	Electronic health record-based(EHR)data
	利用目的の明示の有無	Geisinger 系の医療機関において明示されていると推測
	ユーザの同意の有無	Geisinger 系の医療機関において明示されていると推測
匿名化	匿名化の有無	有
	手法の詳細	HIPAA に準拠したセーフハーバー方式の非 ID 化手法
	個別パラメータの設定等	不明
匿名データ利用に対する審査	審査の有無	有 Honest Broker System による審査がある。この組織は HIPAA、PHI、研究などに詳しい外部の有識者から構成される
	審査プロセス（概略）	MedMining 社内の Internal Review Board と Information Security Office と Privacy Office による審査のち、Honest Broker System による審査が行われる
	データの管理方法等	Privacy Office がデータの授受のタイミングでレビューを行う
匿名化評価	匿名化評価基準の有無	有
	評価基準	HIPAA 準拠の非 ID 化がなされているかどうか
	評価方法	不明
認証対象（機関・組織／ツール／データ）		データ

4.2.4 統計センター

(1) 組織概要

独立行政法人統計センターは、国勢調査や消費者物価指数などの国の基本となる統計の作成（製表）を主要な業務とする総務省所管の独立行政法人であり、平成 15 年 4 月に発足した。平成 21 年度から新統計法が全面施行され、公的統計の体系的整備、統計データの有効活用の推進等に取り組んでいる。匿名情報の提供サービス[52]もその一環で実施されている。

(2) 匿名化・認証プロセス

統計センターにおける匿名化・認証プロセスは表 4-9 の通りである。パーソナル情報の収

[52] http://www.nstac.go.jp/services/anonymity.html

集や匿名情報の提供が統計法に基づくという点で、データの収集時の手続きが CHEO や MedMining の事例とは異なる。また、統計センターでは匿名データ利用申出について、統計センター内部の審査会により処理している。審査会には統計データ高度利用推進室に所属する職員全員（7 名、2010 年 9 月）が参加している。匿名情報の作成は、各府省が「匿名データの作成・提供に係るガイドライン[53]」にしたがって実施する。

表 4-9　統計センターにおける匿名化・認証プロセス

匿名化・認証プロセス		内容
パーソナル情報の収集	収集するデータの種類（取り扱うデータの範囲）	統計調査毎に異なる。 例えば『全国消費実態調査[54]』の場合、家計の収支および貯蓄・負債、耐久消費財、住宅・宅地などの家計資産。
	利用目的の明示の有無	調査の段階では、一次利用目的についてのみ明示している。 ただし、統計法（平成 19 年法律第 53 号）第三十六条により、『行政機関の長又は届出独立行政法人等は、学術研究の発展に資すると認める場合その他の総務省令で定める場合には、総務省令で定めるところにより、一般からの求めに応じ、前条第一項の規定により作成した匿名データを提供することができる。[55]』と認められている。
	ユーザの同意の有無	－（統計法に基づく）
匿名化	匿名化の有無	有
	手法の詳細	各府省により決定
	個別パラメータの設定等	各府省により決定
匿名データ利用に対する審査	審査の有無	有
	審査プロセス（概略）	「匿名データの作成・提供に係るガイドライン」の基準に基づき申出内容の審査を行っている。 ・ 利用相談から始まり、利用要件に合致するかを判断している。この段階を仮申出と呼んでおり、利用要件の説明を丁寧に行っている。 ・ センター内に「利用目的審査会」を設置し、申出の諾否の審査を行っている。 ・ 利用目的審査会には、統計データ高度利用推進室に所属する職員全員が参加している。

53 http://www.stat.go.jp/index/seido/houki.htm
54 http://www.stat.go.jp/data/zensho/2009/index.htm
55 http://www.stat.go.jp/index/seido/houbun2n.htm

匿名化・認証プロセス		内容
	データの管理方法等	匿名データの管理や匿名データの複製に当たっては、「調査票情報等の管理に関するガイドライン」（平成 21 年 2 月 6 日総務省政策統括官（統計基準担当）決定）、統計センターが定める「情報セキュリティポリシー」等の内部規則に基づき実施している。
匿名化評価	匿名化評価基準の有無	各府省により決定
	評価基準	各府省により決定 「匿名データの作成・提供に係るガイドライン」では以下のように言及されている。 『調査票情報の特性は統計調査ごとに異なることから、各統計調査について一律に匿名化の基準を設定することは困難である。 このため、提供機関は、匿名化する統計調査ごとにその特性を勘案し、一橋大学における匿名標本データの試行的提供の事例および諸外国の統計機関における同様の提供の事例等を参考に匿名化の基準となる値、例えば、最小値が 2 件以下とならない等を定める。 なお、個人・世帯を対象とする統計調査の匿名化について、一橋大学で行われた試行的な取組で用いた基準は別紙 3 「匿名化処理の目安」のとおり。』
	評価方法	各府省により決定 なお、基幹統計調査に係る匿名データを作成しようとするときは、あらかじめ、統計委員会の意見を聞かなければならない。
認証対象（機関・組織／ツール／データ）		各府省により匿名化されたデータ

(3) ヒアリング結果の要点

ヒアリング結果の要点のうち、表 4-9 以外の情報を以下に記す。

統計センターにおける匿名データ提供サービス運営の実態は、昨年度のサービス開始から、広報や提供メニューの拡大に力を入れて堅調に利用者数を増やしているという状況である。具体的な利用者像、利用件数、利用目的は次の通りである。

- 利用者は大学関係者が八割を占めている。残りの二割の利用者は大学関係者以外の個人、財団法人や企業等である
- 平成 21 年 4 月に匿名データの提供サービスを開始し、平成 21 年度は 20 件の提供実績がある。今年度(平成 22 年度)は 9 月末現在で 25 件、仮申出中は 5 件である
- 学術研究目的が主であるが、高等教育目的もある。

また、今後の運営に関する話題として、以下のご回答を頂いた。

- 昨年度から開始したサービスで、利用者のほとんどの方が利用期間中のため、利用後の満足度については、まだ把握できていないが、匿名データを提供した段階の意見では、匿名化しすぎているという声もあった。例えば、地域区分を二区分にしているが、都道府県別にしてほしい、年齢は 5 歳刻みだが、各歳でほしい、といった要望もあった
- データの匿名化レベルは、サービスを開始したばかりということもあり、匿名化の度合いは比較的強いものと考えている。ただし、これは今後変わっていく可能性がある

匿名データの利用状況等に関する実地検査に赴くこととしているが、今年度、具体的にどの利用者を対象とするかはこれから検討をする。

4.2.5 まとめ

詳細調査を通して、現時点ではパーソナル情報を匿名化したデータの自由な流通は公にはなされていないことを確認した。例えば CHEO では契約で利用申請者の利用にとどめており、第三者提供を認めていない。また、北米ではリスクベースの匿名化を採用する流れになっているということも確認した。匿名化は、利用者の所属組織のセキュリティポリシー、利用目的、データの種類など、多角的なリスク分析を経て実施されている。

4.3 国内の個人情報ガイドラインと認証スキームの整合性分析

4.3.1 分析の目的と方法

(1) 分析の目的

本整合性分析の目的は、海外の先進的な匿名情報の認証スキームのガイドラインや運用状況等と国内の個人情報保護ガイドラインとの比較分析を行い、課題を洗い出すことである。

(2) 分析の方法

代表的な海外の先進事例であるカナダの CHEO の運用方法について現地調査結果ならびに公表されている文書等から、国内の個人情報保護ガイドラインとの対応関係を整理した。特に、国内ガイドラインとの不整合部分を把握するために、以下の分類を行った。以下、CHEO の運用を PHIPA とあわせて CHEO/PHIPA と記載する。

a. 国内ガイドラインに記載されている項目で、CHEO/PHIPA に対応項目がある項目
b. 国内ガイドラインに記載されている項目で、CHEO/PHIPA に対応項目が無い項目
c. 国内ガイドラインに記載されていない項目で、CHEO/PHIPA に含まれる項目

a については、大枠で整合が取れていると判断する。厳密な解釈までは本調査で実施しない。**b** については、CHEO/PHIPA に含まれない項目である。**c** については、CHEO/PHIPA にのみ含まれる項目であり、先進的な匿名情報の認証スキームと国内ガイドラインの不整合を表す。そのため、本分析では **c** を特定することに重きを置く。

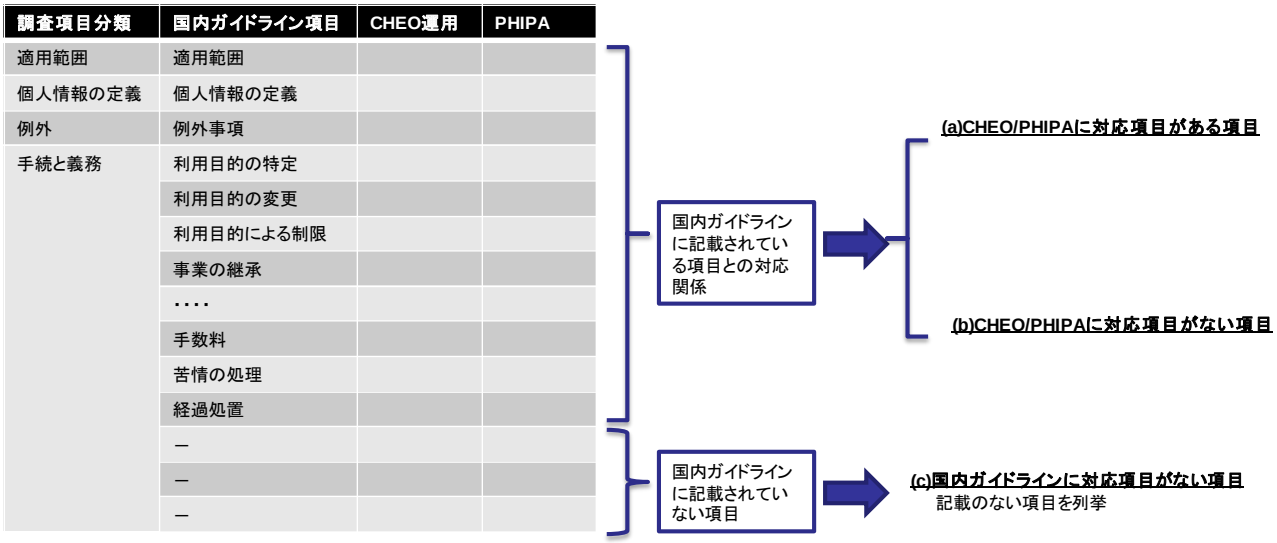

図 4-25　分析の方法

(3) 調査範囲

調査範囲に関し、CHEO の運用に関わる文書と国内の個人情報保護ガイドラインそれぞれについて以下の通りとした。

CHEO/PHIPA については、リスク査定の際に使われる審査項目[56]と、PHIPA とする。前者は、認証を与える際に CHEO が組織として考慮している情報であり、後者は、CHEO の所在地であるオンタリオ州により考慮されている情報であることから CHEO における運用の前提といえる。なお、分析の結果得られる **b** の項目はカナダの連邦法の Privacy Act（3.3.1(1)参照）に含まれる可能性はあるが、本調査の主要な目的は、CHEO/PHIPA での先進的な取り組みに対して現行の国内ガイドラインの課題を整理することであるため、分析は CHEO/PHIPA の範囲にとどめた。

国内の個人情報保護ガイドラインについては、表 4-10 に示す国内の個人情報の保護に関する法律についてのガイドラインを調査範囲の候補とした。この中で、汎用性の高さと CHEO の事例との対応を考えて、『1.個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成２１年１０月９日厚生労働省・経済産業省告示第２号)』と『4.医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン』を調査範囲とした。また、医療研究分野の各指針（表 4-10 11-14）については、『1.個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成２１年１０月９日厚生労働省・経済産業省告示第２号)』と『4.医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン』で整合性の取れていない項目を中心に整理した。

[56] BioMed Central | Additional Files | A method for managing re-identification risk from small geographic areas in Canada
<http://www.biomedcentral.com/1472-6947/10/18/additional/>

表 4-10　国内の個人情報の保護に関する法律についてのガイドライン

	ガイドライン名	分野	発行者	URL
1	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成２１年１０月９日厚生労働省・経済産業省告示第２号）	経済産業	厚生労働省・経済産業省	http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf
2	経済産業分野のうち信用分野における個人情報保護ガイドライン	信用分野	経済産業省	http://www.meti.go.jp/policy/it_policy/privacy/091009guideline.pdf
3	経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン	個人遺伝情報を用いた事業分野	経済産業省	http://www.meti.go.jp/press/20041217010/041217iden.pdf
4	医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン	医療・介護	厚生労働省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf
5	医療情報システムの安全管理に関するガイドライン	医療・介護	厚生労働省	http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html
6	健康保険組合等における個人情報の適切な取扱のためのガイドライン	医療・介護	厚生労働省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161227kenpo.pdf
7	国民健康保険組合における個人情報の適切な取扱のためのガイドライン	医療・介護	厚生労働省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170401kokuho.pdf
8	福祉部関係事業者における個人情報の適正な取扱のためのガイドライン	福祉	厚生労働省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161130fukusi.pdf
9	金融分野における個人情報保護に関するガイドライン	金融	金融庁	http://www.fsa.go.jp/common/law/kj-hogo/01.pdf
10	ヒトゲノム・遺伝子解析研究に関する倫理指針	医療研究	文部科学省・厚生労働省・経済産業省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161228genomu.pdf
11	疫学研究に関する倫理指針	医療研究	文部科学省・厚生労働省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161228ekigaku.pdf

	ガイドライン名	分野	発行者	URL
12	遺伝子治療臨床研究に関する指針	医療研究	文部科学省・厚生労働省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161228idennsi.pdf
13	臨床研究に関する倫理指針	医療研究	厚生労働省	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161228rinsyou.pdf
14	ヒト幹細胞を用いる臨床研究に関する指針	医療研究	厚生労働省	http://www.mhlw.go.jp/bunya/kenkou/iryousaisei01/pdf/01.pdf

4.3.2 分析の対象

CHEO の運用項目のうち、リスク査定に使われる審査項目の情報を整理する。

CHEO におけるリスク査定では、三つの観点で審査項目が用意されている。すなわち、軽減制御(Mitigating Controls)、プライバシー侵害(Invasion of Privacy)、モチベーションと能力(Motives and Capacity)である。『軽減制御』に関しては、申請者の所属する組織について、ISO/IEC 27002（情報セキュリティ管理）などを参考にして作成された審査項目であり、申請者の組織における情報セキュリティ、秘密保持などについて確認をしている。項目数も 25 件程度あり、ガイドラインとの比較分析は主にこの軽減制御の項目となる。残りの『プライバシー侵害』と『モチベーションと能力』については、データ流失時の被害の大きさや匿名情報利用申請者にとっての再 ID 化したデータの価値などについて、CHEO 側で定性的に分析を行う。

表 4-11 に審査項目を列挙する。これらの審査項目、および PHIPA、とガイドラインとの整合性を 4.3.4 項、4.3.5 項で分析する。

表 4-11 CHEO 運用のリスク査定で用いる審査項目（再掲）

審査項目
■軽減制御
認証されたスタッフのみがデータにアクセスできるようにする
データ共有協定を締結している、またはこれから締結する
秘密保持契約をスタッフと外部協力者に対して結んでいる
個人を特定できないデータ、および集合データのみ公開する
長期保有の際には外部監査を受ける
保有期間を過ぎたデータは廃棄される
データは国内でのみ処理、保持、アクセスできる
第三者への開示と共有をしない
情報システムに対する脅威、およびリスク脆弱性の監査を実施する
プライバシー、機密性、セキュリティに関して組織的な管理フレームワークをもつ
データ保持、管理、アクセスに関して、組織的なポリシーを持つ

審査項目
プライバシーとセキュリティポリシーが監視され、効力を持つ
関係者に対するプライバシー、機密保持、セキュリティのトレーニングを強制的に適宜実施している
プライバシー、機密、セキュリティの違反時の罰則がある
プライバシーオフィサーやデータ管理委員会が任命されている
プライバシー違反時のプロトコルがある
プライバシー監査が内部・外部ともある
情報システムに適切な認証を掛けている
データに適切な認証をかけている
データへのリモートアクセスに対し、特別な保護機構を導入している
ウィルスチェックを実施している
利用記録をシステムによりモニタリングしている
データを電子的に送付する際には、暗号プロトコルが使われる
開示データを含むコンピュータやファイルは厳重に施錠管理された場所に置かれる
スタッフには、写真付きの ID、または磁気カードが与えられる
訪問者をスクリーニング、管理する
アラームシステムが設置されている
パーソナル情報が保存される場所の数は最小限にとどめ、あらかじめ特定されている
センシティブデータを保持する場所では一般の人が入れないようにする
定常的な敷地内の監視が実施されている
物理的なセキュリティ対策がなされている
プライバシー担当者のコンタクト情報が提示されている
従業員管理担当者のコンタクト情報が提示されている
組織の透明性と、情報公開の仕組みが整っている
苦情窓口をもっている
REB のような独立した権威がデータの二次利用に関わる提案を承認している
内外の監査、モニタリング機構が導入されている
独立諮問機関、または管理委員会が監視する
■プライバシーの侵害
データの詳細度、データのセンシティブさ、などからプライバシー侵害の影響を測る
■モチベーションと能力
申請者にとって匿名情報を再 ID 化するモチベーションとその能力を測る

4.3.3 分析の作業手順

図 4-26 に具体的な整合性分析作業イメージを示す。表の見出し行に CHEO/PHIPA の項目を記載し、表の見出し列にはガイドライン項目を記載している。CHEO/PHIPA とガイドライン項目の細目との間に同等の記述がある場合 **a** に分類する。見出し列の項目で同等の記述が無い場合 **b** に分類する。見出し行の項目で同等の記述が無い場合、**c** とする。

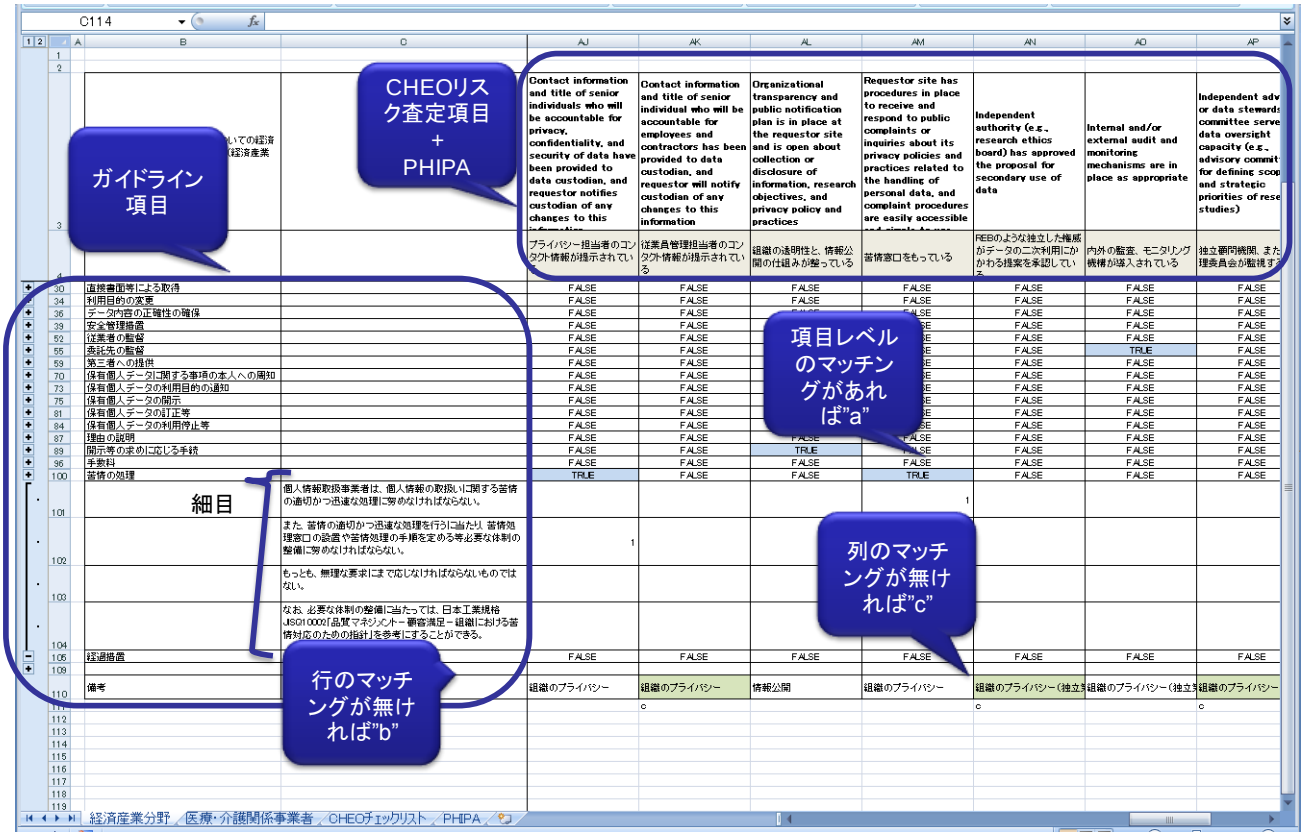

図 4-26　分析の具体的な作業イメージ

4.3.4 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」との比較

CHEO 運用のリスク査定で用いる審査項目（28 件）と「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(23 件)の比較を実施した結果は次の通りである。

a. 19 件 - ガイドラインに記載されている項目で、CHEO/PHIPA に対応項目がある項目
b. 4 件 - ガイドラインに記載されている項目で、CHEO/PHIPA に対応項目が無い項目
c. 9 件 - ガイドラインに記載されていない項目で、CHEO/PHIPA に含まれる項目

特に、今回の分析で重視する **c** の項目のうち、主要な項目を表 4-12 に示す。

表 4-12　CHEO/PHIPA に含まれ国内ガイドラインに記載されていない主要な項目

項目	CHEO / PHIPA	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（経済産業分野ガイドライン）
匿名情報の扱い	（匿名情報利用者は）「個人を特定[57]できないデータの公開、および集合データの開示のみ行う」	（引用）【個人情報に該当しない事例】（事例３）特定の個人を識別することができない統計情報 →「統計情報」の具体的な基準については言及せず。これは CHEO/PHIPA も同様だが、リスク査定により運用でカバーしている。
独立第三者機関による審査・監視	（匿名情報利用者の研究を）「研究倫理委員会のような独立した権威がデータの二次利用に関わる提案を承認している」 （匿名情報利用者を）「独立諮問機関、または管理委員会が監視する」	ー
データの越境について	（匿名情報利用者は）「データを国内でのみ処理、保持、アクセスできる」	（引用）【第三者提供とされる事例】（事例４）外国の会社に国内に居住している個人の個人データを提供する場合 →第三者提供の事例としては触れられている。
プライバシーリスク影響範囲の具体的な分析	リスク分析の項目がデータ利用申請時のチェック項目として具体的に示されている ・ 流出時の想定被害 ➢ データの性質（精度、センシティブさなど） ・ 流出の可能性 ➢ データ利用者の性質（再 ID 化のモチベーション、再 ID 化をする能力）	（引用）委託先の監督（法第２２条関連）取扱いを委託する個人データの内容を踏まえ、本人の個人データが漏えい、滅失またはき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質および個人データの取扱状況等に起因するリスクに応じた、必要かつ適切な措置を講じるものとする。 →具体的なリスク分析については言及せず。

[57] Personal Health Information Protection Act (PHIPA, Ontario) “Identifying information” means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

b の項目には「利用目的の変更」、「適性取得」、「保有個人データの利用停止等」、「経過措置」が該当した。

「利用目的の変更[58]」については、匿名情報を提供する CHEO の場合、申請者の利用目的の変更は研究のため、基本的には該当しない。

「適性取得」については、CHEO のデータ取得経路が明確であり、不正な入手には該当しない。

「保有個人データの利用停止等」について、リスク査定と PHIPA には存在しない項目であったが、内部の運用文書には存在する項目と考えられる。

「経過措置」に関しては、法律施行前のデータの扱いについて触れたものであり、カナダの CHEO には該当しない。

4.3.5 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」との比較

CHEO 運用のリスク査定で用いる審査項目（28 件）と「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（10 件）の整合性を分析した結果を以下に示す。

a. 13 件 - ガイドラインに記載されている項目で、CHEO/PHIPA に対応項目がある項目
b. 0 件 - ガイドラインに記載されている項目で、CHEO/PHIPA に対応項目が無い項目
c. 15 件 - ガイドラインに記載されていない項目で、CHEO/PHIPA に含まれる項目

表 4-12 に示した項目が同様に、主要な整合性の無い項目として挙げられる。**c** の項目は件数としては増えているが、実際には経済分野におけるガイドラインから大きな差異は認められない。**c** の項目が増加した理由に、匿名情報利用者の所属する組織のセキュリティポリシーに関する項目（例：写真付き ID/磁気カードの使用、アラートシステムの運用）について具体的に明記されていないことが挙げられる。しかし、これらの項目は、ガイドライン中の『安全管理措置、従業者の監督および委託先の監督（法第２０条～第２２条)』に暗黙的には含まれていると考えられる。

4.3.6 医療研究分野の倫理指針と非整合項目の比較

医療研究分野についても以下の指針が出されている。本節では、4.3.4 項、4.3.5 項で整合性の取れなかった項目である匿名化、第三者機関、海外との研究について整理した。

---

58 「利用目的の変更」特定した利用目的は、社会通念上、本人が想定することが困難でないと認められる範囲内で変更することは可能である。変更された利用目的は、本人に通知するか、または公表しなければならない。本人が想定することが困難であると認められる変更を行う場合は、法第１６条に従って本人の同意を得なければならない。利用目的で示した個人情報を取り扱う事業の範囲を超えての変更は、あらかじめ本人の同意なく行うことはできない。
「適性取得」個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはならない。
「保有個人データの利用停止等」個人情報取扱事業者は、本人から、手続違反の理由により保有個人データの利用の停止等※２が求められた場合には、原則として、当該措置を行わなければならない。なお、利用の停止等を行った場合には、遅滞なく、その旨を本人に通知しなければならない（「電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。)。
（出典：個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン，経済産業省，2004）

- ヒトゲノム・遺伝子解析研究に関する倫理指針（平成１６年１２月２８日告示改定）
- 疫学研究に関する倫理指針（平成１６年１２月２８日告示改定）
- 遺伝子治療臨床研究に関する指針（平成１６年１２月２８日告示改定）
- 臨床研究に関する倫理指針（平成１６年１２月２８日告示改定）
- ヒト幹細胞を用いる臨床研究に関する指針（平成１８年７月３日告示）

(1) 匿名化

『ヒトゲノム・遺伝子解析研究に関する倫理指針』、『疫学研究に関する倫理指針』、『ヒト幹細胞を用いる臨床研究に関する指針』に関しては、匿名情報の定義と扱いが記載されている。また、外部機関への提供に際しての匿名情報の扱いの記載も前者の二指針には研究目的に限り存在する。

『遺伝子治療臨床研究に関する指針』、『臨床研究に関する倫理指針』など、臨床研究ではインフォームド・コンセントを取り、第三者提供などを許容する立場を取っていると考えられる。

表 4-13 医療研究分野の指針 - 匿名化

指針	匿名情報の扱い	外部機関への提供に際しての匿名情報の扱い
ヒトゲノム・遺伝子解析研究に関する倫理指針	個人情報を連結不可能匿名化した情報は、個人情報に該当しない。個人情報を連結可能匿名化した情報は、研究を行う機関において、当該個人情報に係る個人と当該情報とを連結し得るよう新たに付された符号または番号等の対応表を保有していない場合は、個人情報に該当しない。	試料等の提供が行われる機関の長は、試料等を外部の機関に提供する際には、原則として試料等を匿名化しなければならない。 また、試料等の提供が行われる機関内のヒトゲノム・遺伝子解析研究を行う研究部門（以下「試料等の提供が行われる機関における研究部門」と いう。）に試料等を提供する際にも、原則として匿名化しなければならない。 ただし、次に掲げる要件のすべてを満たしている場合には匿名化せずに試料等を提供することができる。 ア提供者または代諾者等が、匿名化を行わずに外部の機関または試料等の提供が行われる機関における研究部門に提供することに同意していること。 イ倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において、匿名化を行わずに、外部の機関または試料等の提供が行われる機関における研究部門に提供することが認められていること。

指針	匿名情報の扱い	外部機関への提供に際しての匿名情報の扱い
疫学研究に関する倫理指針	ただし、次のいずれかに該当する疫学研究は、この指針の対象としない。 資料として既に連結不可能匿名化されている情報のみを用いる研究	既存資料等の提供を行う者は、所属機関外の者に研究に用いるための資料を提供する場合には、資料提供時までに研究対象者から資料の提供に係る同意を受け、および当該同意に関する記録を作成することを原則とする。ただし、当該同意を受けることができない場合には、次のいずれかに該当するときに限り、資料を所属機関外の者に提供することができる。 ① 当該資料が匿名化されていること。(連結不可能匿名化または連結可能匿名化であって対応表を有していない場合)
遺伝子治療臨床研究に関する指針	―	―
臨床研究に関する倫理指針	―	―
ヒト幹細胞を用いる臨床研究に関する指針	被験者等に関する個人情報については、連結可能匿名化（必要な場合に個人を識別できるように、その個人と新たに付された符号または番号の対応表を残す方法による匿名化をいう。）を行った上で取り扱うものとする。	―

(2) 研究倫理委員会

独立第三者機関による審査については、各指針とも見受けられないが、研究倫理委員会に相当する機関は各指針とも存在する。特に、『ヒトゲノム・遺伝子解析研究に関する倫理指針』、『疫学研究に関する倫理指針』については、外部機関への提供に際して倫理審査委員の許可がある場合、匿名化の必要がなくなる。

他の三つの臨床研究の指針については、4.3.6(1)の通り、外部機関への提供に際して匿名化する義務が無いことと連動しており、倫理審査委員が特別な許可を出す必要は無い。そのため、特に記載は無いと考えられる。

表 4-14　医療研究分野の指針 - 審査委員会

指針	研究倫理委員会相当の委員会	外部機関への提供に際しての役割
ヒトゲノム・遺伝子解析研究に関する倫理指針	倫理審査委員会	試料等の提供が行われる機関の長は、試料等を外部の機関に提供する際には、原則として試料等を匿名化しなければならない。 次に掲げる要件のすべてを満たしている場合には匿名化せずに試料等を提供することができる。 イ倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において、匿名化を行わずに、外部の機関または試料等の提供が行われる機関における研究部門に提供することが認められていること。
疫学研究に関する倫理指針	倫理審査委員会	既存資料等の提供を行う者は、所属機関外の者に研究に用いるための資料を提供する場合には、資料提供時までに研究対象者から資料の提供に係る同意を受け、および当該同意に関する記録を作成することを原則とする。ただし、当該同意を受けることができない場合には、次のいずれかに該当するときに限り、資料を所属機関外の者に提供することができる。 ① 当該資料が匿名化されていること。(連結不可能匿名化または連結可能匿名化であって対応表を有していない場合) ② 当該資料が①の匿名化に該当しない場合において、以下の要件を満たしていることについて倫理審査委員会の承認を得て、研究を行う機関の長の許可を受けていること。
遺伝子治療臨床研究に関する指針	審査委員会	―
臨床研究に関する倫理指針	倫理審査委員会	―
ヒト幹細胞を用いる臨床研究に関する指針	倫理審査委員会	―

(3) データの越境

データの越境については、海外の共同研究を条件付で許可するという形で、『遺伝子治療臨床研究に関する指針を除く指針』で認められている。ただし、海外の外部機関へのデータ提供について明示された指針は存在していない。

表 4-15　医療研究分野の指針 - データ越境

指針	海外との共同研究	海外の外部機関への提供
ヒトゲノム・遺伝子解析研究に関する倫理指針	可	―
疫学研究に関する倫理指針	可	―
遺伝子治療臨床研究に関する指針	―	―
臨床研究に関する倫理指針	可	―
ヒト幹細胞を用いる臨床研究に関する指針	可	―

4.3.7 まとめ

本整合性分析を通して明らかにした匿名情報の流通に係る課題は次の通りである。

- 匿名情報の流通に際し、国内の個人情報ガイドラインでは明示的に扱われていない項目の検討が必要である
  - 匿名情報の定義、ガイドラインでの扱いの明確化
  - 独立第三者機関による審査・監視
  - （匿名情報に関する）データの越境問題
- 匿名情報の流通に際し、国内のガイドラインにリスク分析手法の詳細化が必要である
  - 匿名情報の品質と連動することが想定されるため、リスクを考慮する方法、基準などの明確化・詳細化が必要

匿名情報の定義、ガイドラインでの扱いの明確化については、匿名情報を『匿名』と認める基準が明記されていないことに不整合の原因があると考えられる。仮に、匿名情報を定義し、匿名情報が個人情報保護法の対象外となった際にも、ガイドラインとして提供者・利用者双方による扱い方について明示する必要がある。

独立第三者機関による審査・監視については、不整合を埋めるためにはプライバシー・コミッショナーの設置か、それに類する機関が必要である。

データの越境問題については、個人情報保護の国際的に整合する必要性が訴えられていることと同様に、匿名情報についても検討が必要である。

リスク分析手法については、北米でリスク分析に基づく匿名情報の利活用が進められていることもあり、匿名情報の流通や利活用を実現する上では、具体的なリスク分析についてもガイドラインとして記述する必要があると考えられる。

4.4 匿名化ツール事例にみる匿名性評価の指標

本節は、国内外の匿名化ツールの事例を調査し、匿名性評価のための指標および匿名性が妥当だといえる基準となる値について整理した結果を記載する。

4.4.1 Privacy Analytics Risk Assessment Tool(PARAT)

(URL: http://www.privacyanalytics.ca/)

(1) 概要

PARAT は、カナダ・Privacy Analytics 社の匿名化ツールであり CHEO（4.1.1 項参照）など、カナダ・オンタリオ州を中心に利用されている。同社の設立者は CHEO の Khaled El Emam 博士である。PARAT には、個人医療情報を匿名化して提供する際のリスク査定機能と、実際に匿名化する機能が備わっている。リスク査定に実運用を考慮し、ISO27002（組織における情報セキュリティマネジメントシステムの仕様）に準ずる項目や k-匿名性の指標と連動させるために経験則を組み込んでおり、ツールとしての成熟度は高い。現在はスタンドアローンツールとしての提供形態を取っているが､近い将来 Web ツールとして提供をする予定とされている。これは、リスク査定をする際に、審査対象の研究者と確認をしながらリスク査定を実施するためである。PARAT には、相手によって匿名化の度合いを変える時に、いかに納得感を持たせるかという問題意識の下で作成しているため、対話的なリスク査定機能が充実している。

(2) 匿名化手法

次の手順により、データの匿名化を行う。PARAT では GUI が提供されており、各段階の設定や結果の確認は GUI を通して行う。

(a) 再 ID 化リスクの許容できるしきい値の査定

データを提供するリスクのしきい値に関する査定項目は三種類に大別される。

1. 利用申請者の組織のセキュリティ・プライバシー保護状況などについて
2. 再 ID 化のモチベーションと能力について
3. プライバシー事故が起きた場合の影響の大きさについて

1 の項目は、ISO27002（組織における情報セキュリティマネジメントシステムの仕様）に準じたチェックリストを、利用申請者と共に確認をする形で査定する。

2 の項目は、再 ID 化をする経済的な価値や、必要な解析能力の有無をチェックリストの項目に対して確認をする。（図 4-27 参照）

3 の項目は、データの詳細度、データのセンシティブさ等からプライバシー侵害の影響を測る項目である。

上記 1-3 の結果、リスクのしきい値(0.05～0.33)を決定する（図 4-28 参照）。

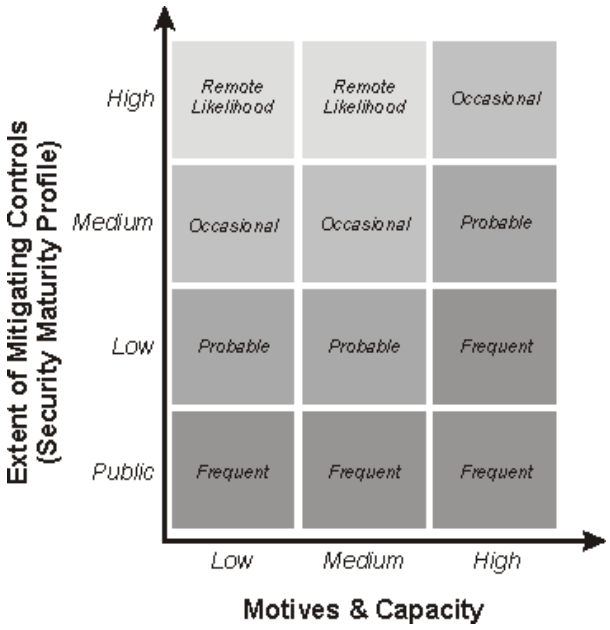

図 4-27　リスク査定（前半）（出典: PARAT, Privacy Analytics, www.privacyanalytics.ca, 2010）

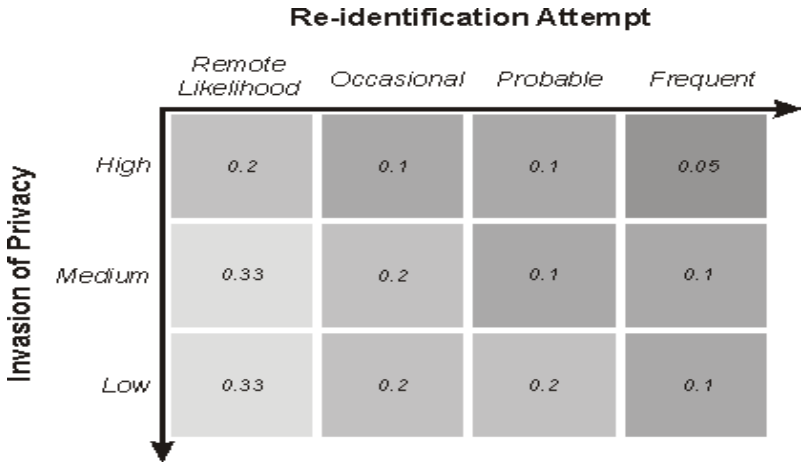

図 4-28　リスク査定（後半）（出典: PARAT, Privacy Analytics, www.privacyanalytics.ca, 2010）

(b)　リスク査定

リスク査定に用いる変数には、準識別子、再 ID 化リスクのしきい値、サンプリングの度合い、が含まれる（図 4-29 参照）。

準識別子は、間接的に個人を識別しうる属性データである。PARAT では、自動的に準識別子を判別する機構も備えている。これは、属性の名前では無く、データの中身を走査し判定している（図 4-29-①）。

再 ID 化リスクのしきい値は、データ管理者が、研究者に匿名情報を提供することにより負うことになるリスクの取り得る値であり、上記(a)で査定した結果得られる値である（図 4-29-②）。

サンプリングの度合いは、匿名化するデータセット全体のうち、どの割合のデータを匿名化するかを指定する（図 4-29-③）。

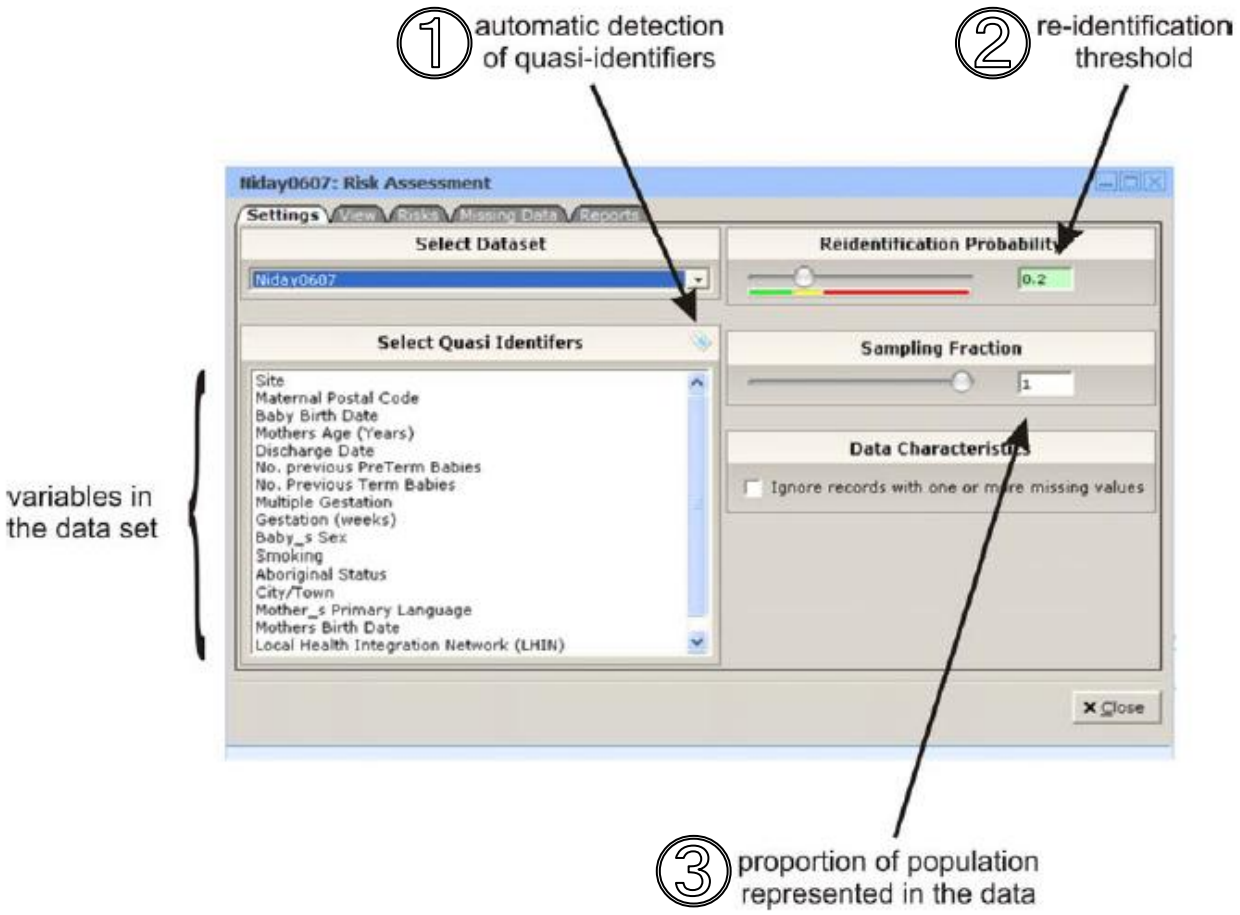

図 4-29　PARAT – 準識別子の特定画面

（出典: PARAT, Privacy Analytics, www.privacyanalytics.ca, 2010、数字は三菱総合研究所が追加）

(c)　リスク査定の実行

PARAT は三つのタイプの攻撃者のモデルを扱う。攻撃者とは、再 ID 化攻撃を実施する第三者であり、Prosecutor（検察）、Journalist（ジャーナリスト）、Marketer（マーケッター）という三タイプのリスク値を計算する。攻撃者モデルは、データの性質など場合によって使い分ける。

図 4-31 は、検察とマーケッターの攻撃者モデルを想定した際のリスクである。しきい値を上回っているため、このままのデータ提供はリスクが高いので避けるべきという結果である。なお、検察のリスクでは、個々のエントリの再 ID 化リスクのうち最大値であり、マーケッターリスクは再 ID 化リスクの平均値である。

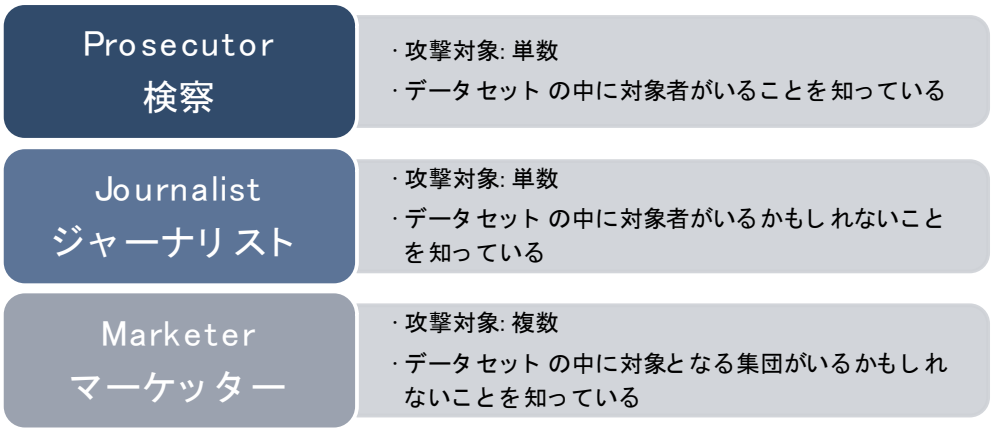

図 4-30　攻撃者モデル

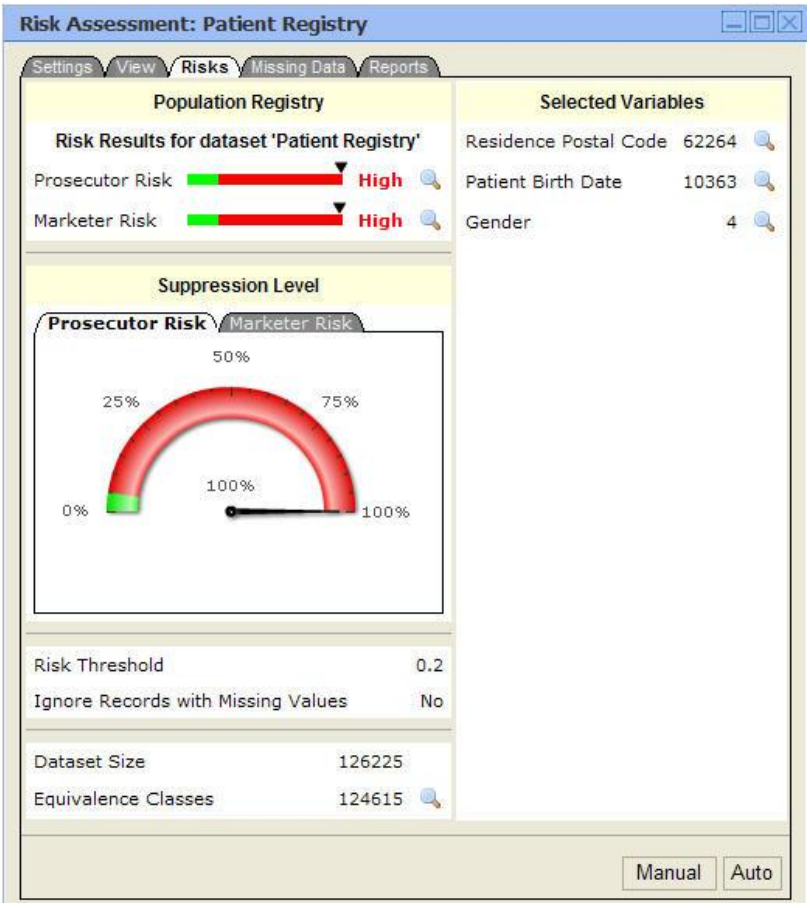

図 4-31　リスク査定(出典: PARAT brochure, Privacy Analytics, www.privacyanalytics.ca, 2010)

(d)　匿名化の実行

PARAT では、大域的再符号化と局所秘匿化による匿名化を実施することで、リスクをしきい値以下に抑える。匿名化の際には、利用者の希望により、重要な項目の一般化を相対的に緩和するなどの重み付けができるようになっている。

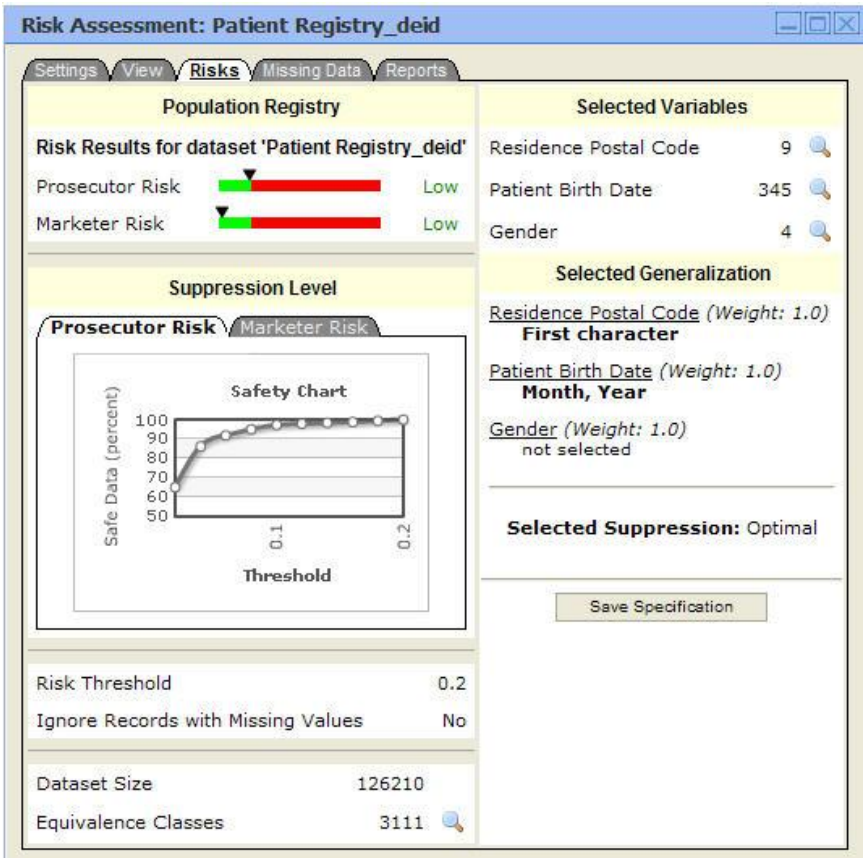

図 4-32　リスク査定（匿名化後）（出典：PARAT brochure, Privacy Analytics, www.privacyanalytics.ca, 2010）

(3) 評価値

リスクのしきい値は 0.05～0.33 であり、これは k-匿名性の k の値と連動している。例えば 0.05 の場合は k=20 で匿名化され、0.33 の場合は k=3 で匿名化される。ただし、実際の運用では慣行上 k=5 以上の匿名化を実施している。

4.4.2 Cornell Anonymization Toolkit(CAT)

（URL: http://sourceforge.net/projects/anony-toolkit/）

(1) 概要

Cornell Anonymization Toolkit(CAT)は、コーネル大（米国）の Cornell Database Group[59]の研究者らが、k-匿名性、l-多様性(l-diversity)、t-近似性(t-closeness)といった匿名化の指標を一般の人からも使いやすいように GUI で対話的に使えるようにしたツールである。SourceForge.net でソースコードも公開されている。

ツール自体のドキュメントは、国際会議のデモセッションで発表された文章[60]程度しか公開されていないが、SourceForge.net でデモ用のデータを付けた状態でデモアプリケーションとして公開されている。

[59] http://www.cs.cornell.edu/bigreddata/privacy/
[60] Xiaokui Xiao, Guozhang Wang, Johannes Gehrke: Interactive anonymization of sensitive data. SIGMOD Conference 2009: 1051-1054

(2) 匿名化手法

(a) 匿名化処理に必要なデータの用意

匿名化処理に必要な下記三種類のデータを用意する。

- 個別のレコードデータ(MicroData)
- レコードの属性値の定義(MetaData)
- レコードの属性値に関する一般化階層構造（HierarchiesData、属性毎に作成）

MicroData
```
1  48  1  1  10  83
2  66  2  1   6  14
3  51  1  1  11  50
・・・
```

MetaData
```
5  300000

127  0  0  Age
0  126

2  0  1  Gender
1  Male
2  Female

9  0  1  Race
1  White
・・・
9  Three or more major races

18  0  1  Education
00  Not applicable
01  No school completed
・・・
17  Doctorate degree

100  0  1  Income
0  0k-1k
・・・
99  99k-100k
```

HierarchiesData(Age)
```
4  // Number of Levels in the Hierarchy, excluding the leaf level
21  // Number of nodes in the first level
0  4  0-4
5  9  5-9
・・・
100  126  100+
10  // Number of nodes in the second level
0  14  0-14
15  24  15-24
・・・
95  126  95+
4 // Number of nodes in the third level
0  24  0-24
・・・
65  126  65+
1 // Number of nodes in the fourth level
0  126  0-126
```

図 4-33 Cornell Anonymization Toolkit(CAT)の初期データの例

(b) 匿名化処理

匿名化処理には、一般化を実施している。具体的には Incognito アルゴリズム[61]を実装している。

k-匿名性に加え、l-多様性、t-近似性に関するパラメータも設定できる。処理の際には、匿名化、結果の確認、匿名化のパラメータを変更、という手順を反復し、最終的に希望の匿名情報を得ることを想定している。

CAT は、リスク分析機能も具備しており、想定される攻撃者の持つ知識を選択し、再 ID 化のリスクを分析して、個々のレコードに対する再 ID 化リスクを利用者に提示する。

[61] Kristen LeFevre, David DeWitt, and Raghu Ramakrishnan.
Incognito: Efficient Full-Domain K-Anonymity.
In ACM SIGMOD International Conference on Management of Data, June 2005

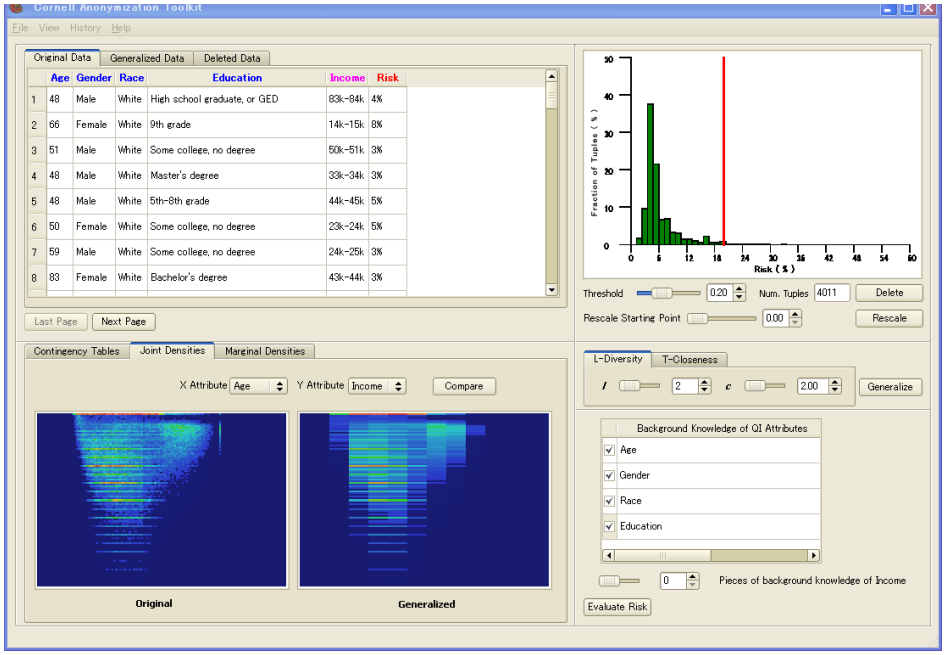

図 4-34 CAT - 実行イメージ(出典 Cornell Anonymization Toolkit Ver1.0.0, Cornell University)

(3) 評価値

k-匿名性、l-多様性、t-近似性の値を指定して評価するが、具体的な値の指定は利用者に委ねられている。

4.4.3 μ-Argus

(1) 概要

オランダ統計局(CBS)を中心に、EU のファンド[62]で開発されてきた統計的開示抑制のためのツールであり、リスク評価、匿名化の機能を有する。

(2) 匿名化手法

μ-Argus は統計的開示抑制を目的とした匿名化に関する機能を有する。オランダ統計局における運用に際しては、大域的再符号化と局所秘匿化の組み合わせを主として利用する。

- Global recoding
- Local suppression
- Top and bottom coding
- The Post RAndomisation Method(PRAM)
- Numerical Micro Aggregation
- Multivariate fixed-size microaggregation
- Numerical Rank Swapping

[62] CASC(5th FP)、CENEX、ESSNet(Eurostat) は FY2009 まで。FY2010 も別途 Eurostat の予算を確保している。

(3) 評価値

指標については、利用者が設定することを前提としている。特に、統計的開示抑制に詳しい人が利用することを想定している。

オランダ統計局での運用に際しては、例えば匿名化の対象となるデータに 20 の準識別子がある場合、三つの変数の全ての組み合わせの出現頻度を基準とする。一般に、母集団の中で出現回数が 100 以上あればマイクロデータとして提供を許可するとしている。

(4) 現地ヒアリング

オランダ統計局にて、Argus の開発者、Anco Hundepool 氏と Peter-Paul de Wolf 氏から μ-Argus の匿名化についてヒアリングした要点を表 4-16 に示す。なお、表 4-16 ではオランダ統計局の略称 CBS を用いる。

表 4-16 μ-Argus ヒアリング要点

大項目	中項目	内容
1.導入の経緯		● Argus を開発するに至った経緯は、法律や規制への準拠と言うよりも、研究結果をツールに落とすという使命の方が強かった。 ● オランダにはプライバシーに関する一般法がある。 ● EU データ保護指令は、統計データ開示について、”How”を指定しているわけではない。
2.匿名化の詳細	匿名化手法	● 大域的再符号化と局所秘匿化の組み合わせが中心である。双方の度合いについては、目的による。
	匿名化評価指標	● K-匿名性は計算量の関係で使っていない。 ● （国勢調査がオランダではできなくなっており、統計は母集団のサンプリングを行い、そこから全数推計を行っているためでは無いかと推測される） ● 準識別子（説明変数、個人特定可能変数）三つの組み合わせに対して、頻度表を作成し、母集団に対して 100 件を目安にしている。この作業を自動化するために Argus を利用する。
	評価値（しきい値）	● コンテキストとサンプリングによるが、マイクロデータの場合、3 変数の全ての組み合わせについて、母集団に対して 100 件を目安にしている。 ● パブリックユースファイルの場合、全ての二つの変数の組み合わせについて、母集団に対して 10,000 件を目安にしている。 ● 匿名化の度合いは、誰がリクエストをするかによらない。どのようにして渡されるかによって変わる。契約を締結した授受、CBS ネットワーク内での利用、パブリックユースファイルによって変わる。

大項目	中項目	内容
3.匿名化の運用実態	稼働状況	● Argus が CBS 内で使われている頻度は不明である。 ● マイクロデータファイルを公開する時には、CBS 内で必ずμ-Argus のチェックを通す。ただし、実際に Argus を利用しているのはごく限られた職員だけである。Argus を利用する処理は一部の職員に集約されている。 ● インターネットに公開するテーブルデータを作成するときは、τ-Argus のチェックを原則として通す。必ずしも全ての統計に対してマイクロデータを作成する訳ではないので、τ-Argus の方が使用頻度は高くなる。
	関係する法律、文書	● オランダ統計法 ● CBS 内でルールを記述したドキュメントはオランダ語で書かれている。 ● 厳密なルールは公開されるべきではないという立場をとっている。一般的なルールは公開できるが、パラメータなどについては公開してしまうと開示リスクを高めることになってしまう。
	データ提供について	● 匿名マイクロデータの提供サービスを実施している。 ● 契約ベースでの授受、オンサイト（CBS 内、リモート）利用、パブリックユースファイルとしての公開、という提供形態がある。
	組織間の連携	● EU で統計開示制御を真剣に取り組んでいる国は少ない。イタリア、ドイツ、英国、北欧諸国など、ESSNet に参加しているところが中心であり、いつも同じ面々になっている。 ● 日本の統計局からも数年前にメールはもらった。技術的には問題ない。どの国でもダウンロードして使えるはず。
4.今後の展望		● Eurostat（EU 統計機関）の予算を 1 年分獲得した。1 年間様子を見て、継続となる予定である。 ● リスクベースアプローチについて促進することが目的の一つである。 ● Glossary:Continuing vocational training survey(CVTS), http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Glossary:Continuing_vocational_training_survey_(CVTS)という統計データが対象となる予定である。 ● もうひとつの目的は Argus をオープンソースソフトウェアにすることである。 ● 新しい汎用的なオープンパッケージでのアーキテクチャにする。R パッケージの作者も新プロジェクトのメンバーになる。一つの大きなパッケージになることが想定されている。 ● ただし、μ-Argus と τ-Argus は異なる方向に進化していく可能性が高い。

4.4.4 Custodix Anonymisation Tool(CAT)

(1) 概要

Custodix Anonymisation Tool (CAT)は、ベルギー・Custodix 社の作成した匿名化ツールである。同社は、主にヘルスケア業界で、プライバシーを保護したデータ管理のワンストップサービスを提供している。ゲント大学から学内ベンチャーとして起業した背景もあり、ACGT(Advanced Clinico-Genomic Trials)や TAS3(Trusted Architecture for Securely Shared Services)といった EU の研究プロジェクト(FP5-7)にも参画している。

また、製薬大手との契約でも使われるほか、2010 年度中に、英国 NHS から受注予定のプロジェクトでも利用される予定である。

(2) 匿名化手法

仮名化、暗号化、項目の削除が提供される。CAT の機能自体は、異なる情報源の EHR データを統合する部分が主な機能であり、その際に必要に応じて匿名化をするという位置づけである。匿名化手法には一般化などを含まないが、これは医療研究では、個人の時系列のデータを扱うため、ある時点の情報で匿名化をしてしまうとニーズを満たせなくなってしまうためである。

(3) 評価値

弁護士団と Custodix 社（信頼できる第三者機関）と利用者の間の交渉で仮名化、暗号化、項目の削除の適用方針を決める。

リスク審査はツール(PANDA - Privacy ANalyser for DAtabases)を作成しているが、既に存在するデータにしか適用できないため、実際には利用してしない。そのため、リスク査定は手動で実施しており、目的、攻撃者モデルなどからリスクを算出している。リスク査定の特徴は、攻撃者にとっての金銭的なメリットを重視している点にある。例えば、匿名化するデータを他に廉価で入手することができるかどうかをリスク査定項目に含めている。

(4) 現地ヒアリング

Custodix 社 COO の Brecht Claerhout 氏から CAT の匿名化についてヒアリングした要点を表 4-17 に示す。

表 4-17 CAT ヒアリング要点

大項目	中項目	内容
1.導入の経緯		● Custodix Anonymisation Tool(CAT)を作ったそもそもの動機は、医療研究用のデータを作成する際にカスタム、アドホックな非 ID 化が多かったためである。 ● 時間がかかり、無駄が多いため、汎用ツールを作るに至った。 ● また、データ保護指令の実装が各国で異なるため、非常に煩雑な確認が必要となることもあり、Custodix 社のようにノウハウを持ってワンストップサービスを提供するところにニーズがある。

大項目	中項目	内容
2.匿名化の詳細	匿名化手法	● 仮名化、暗号化、項目の削除が中心である。 ● 一般化は実施していない。これは、医療研究に対するデータ提供の難しさによる。 ● 統計的開示制御とニーズが異なり、アグリゲートしたデータでは無く、個人のデータが要求される。これは、医療研究が、しばしば個人の時系列データを使うためである。 ● リスク審査はツール(PANDA)をコンセプトレベルで作成しているが、実際には利用してしない。匿名化処理の設定はマニュアルで実施している。 ● CAT ツールはμ-Argus とは違い、各所で異なるフォーマットデータの統一をすることに主眼を置いている。
	匿名化評価指標	● 弁護士、信頼できる 3rd パーティ（=Custodix 社）、クライアント（利用者）の協議により決まる。 ● 『ネゴシエーションというグレーゾーン』という認識もしている。 ● FP6 の ACGT（ポストゲノム研究）の時は主にドイツの弁護士団であった。
	評価値（しきい値）	● 『法律にはしきい値が載っていない』という認識をしている。
3.匿名化の運用実態	マーケット	● 英国 Sapior 社、IBM などと過去にコンペになっている。 ● ただ、医療研究向けのマーケットはそれほど大きいわけではない。 ● 顧客としては、政府と研究（産・学）が中心である。
	関係する法律、文書	● 基本はデータ保護指令を実装した各国内法
	契約形態	● ツール単体の販売(CAT)よりは、インフラサービス(CATS)に重点を置いている。 ● Custodix 社からのデータの第三者提供はない。あくまでデータを流通させるインフラを用意するビジネスを実施している。
	組織間の連携	● Center for Data Protection(CDP)という NPO を設立し、医療研究における匿名情報利用の法的、技術的なデファクト基準の提供と適正利用の監視を目指している。
4.今後の展望	● 英国 NHS から、異なる拠点の EHR データ統合（匿名化）サービスの案件をコンペで受注している。	

4.4.5 まとめ

本節で調査した四種類のツールの特徴を下記、および表 4-18 にまとめる。

- PARAT は、カナダの医療研究分野を中心に利用されている。リスク査定に情報セキュリティマネジメントシステムの仕様(ISO27002)に準ずる項目や経験則を組み込むなど、実運用を考慮しており、ツールとしての成熟度は非常に高い。また、カナダ・オンタリオ州を中心にプライバシー・コミッショナーからも理解を得ているツールである。
- Cornell Anonymization Toolkit(CAT)は、米国コーネル大の研究者がオープンソースとして匿名化に関する近年の研究成果を実装したツールである。k-匿名性、l-多様性などの匿名化の指標を一般の人でも使えるよう GUI に工夫をしている。また、オープンソースソフトウェアとして公開されている。アカデミアの成果を広く伝えるという目的で作成されているため、匿名化の指標に関しては十分に実装されているといえる。
- μ-Argus は、EU 諸国の統計局が共同で開発した統計的開示抑制(Statistic Disclosure Control)で利用される高機能なツールである。利用には統計的開示抑制の知識を前提としている。オランダ統計局を中心に EU の統計局で利用されている。
- Custodix Anonymisation Tool(CAT)は、ベルギーの企業の提供するツールであり、医療研究データの保護などに利用されている。運用時には弁護士団との協議によりしきい値が決められる。Custodix 社の顧客が個人医療データを利用する際に、インフラ構築の一部として利用され、監査への対応も考慮されている。ツール単体の機能としてはシンプルだが、個人医療情報を EU データ保護指令の下で利用するためのサービス提供の実績は十分にあると考えられる。

表 4-18 の見出し行に含まれる「実装された機能」は、匿名化の度合いを判定するための『リスク査定』機能、単純な仮名化や ID の切り落としではなく『集合匿名化』をする機能、利用者が匿名化の度合いを決定する際に、シミュレーションした値を GUI で確認しながら決定できる『対話的 UI』機能、の実装状況を三段階（○：十分に提供されている、△：簡単な機能が提供されている、×：提供されていない）で文献・ヒアリングの情報に基づき評価した。

また、「実装された指標」については、k-匿名性、l-多様性、t-近似性という広く認知された指標の実装がされているかどうかを評価した。

表 4-18　ツールの特徴

名称	管理者（国）	概要	適用領域	実装された機能			実装された指標		
				リスク査定	集合匿名化	対話的UI	k-匿名性	l-多様性	t-近似性
PARAT (Privacy Analytics Risk Assessment Tool)	CHEO/Privacy Analytics（カナダ）	Privacy Analytics 社の匿名化ツール。同社の CEO は CHEO の Khaled El Emam 博士。	医療研究	○	○	○	○	×	×
Cornell Anonymization Toolkit(CAT[Cornell])	Cornell University（米国）	匿名情報の開示をインタラクティブに行うツール。SourceForge.net でソースコードも公開されている。	汎用	△	○	△	○	○	○
μ-Argus	Statistics Netherlands（オランダ・EU）	マイクロデータの匿名化のために EU 統計局などで主に使われるソフトウェア。ESSNet プロジェクトなどで作成。	統計的開示	×	△	△	×	×	×
Custodix Anonymisation Tool (CAT[Custodix])	Custodix（ベルギー）	eHealth のデータ保護に使われる。ACGT などの研究プロジェクトなどで使われる。	医療研究	×	△	△	×	×	×

表 4-19 には、実装されている機能に対して、運用時の利用のされ方を整理している。特徴を以下に示す。

- PARAT は、PARAT の提供する査定支援機能を用いたリスク査定を実施し、その結果に基づき匿名化を実施する。その際には、k-匿名性を指標として用いている。通常 k の値は 5 以上とされているが、本調査時点でのツールの仕様では最低でも k の値は 3 以上となっている。また、データ提供時に際しては契約を締結する。
- CAT[Cornell]は、k-匿名性、l-多様性、t-近似性の各指標を利用者が自由に選択して利用できるが、実際に運用されている事例は公開されていない。
- μ-Argus は、オランダ統計局において、準識別子の任意の三つの組み合わせの母集団における出現頻度を指標として利用されている。統計データのマイクロデータを提供する場合、母集団に対して 100 以上の頻度があることを条件としている。また、利用時には研究者と所属組織の双方に対しての契約を締結する。

CAT[Custodix]は、単純匿名化、仮名化といった機能のみを提供しているが、指標は不定である。弁護士団、Custodix 社、顧客（製薬研究）の間での合議の下、仮名化などの処理内容が決定される。

表 4-19　ツールの指標

調査対象（ツール名）	運用時に使われる指標	運用時における指標の扱い（基準等）
PARAT (Privacy Analytics Risk Assessment Tool)	k-匿名性	k≧3（リスク査定結果による）とする。
Cornell Anonymization Toolkit(CAT[Cornell])	不定（k-匿名性、l-多様性、t-近似性を利用者が選択する）	利用者がリスク査定の結果を勘案しつつ設定する。リスク査定の機能はツールに含まれており、攻撃者の前提知識を指定する。
μ-Argus	準識別子の任意の三つの組み合わせの母集団における出現頻度	母集団に対して 100 以上とする（オランダ統計局において、マイクロデータを契約して提供する場合）。
Custodix Anonymisation Tool (CAT[Custodix])	不定	弁護士団、Custodix 社（信頼できる第三者機関）、顧客（製薬研究）の間での合議の下、仮名化や局所秘匿化などの処理内容が決定される。

詳細調査を通じて、匿名性を評価する指標は運用される各国の法令等に影響されることが多く、匿名化評価指標に関しての共通項は少ないことを確認した。k-匿名性、l-多様性、t-近似性という広く認知された指標の中でも、k-匿名性は中心的な考え方となっている。

匿名化評価指標の評価値については、各国の法令に遵守しつつ、利用者との協議および運用者の経験値により決定された運用がなされており、標準的な基準を定めることは難しいことが分かった。

4.5 匿名情報を利活用するサービスモデルの検討

4.5.1 背景と目的

(1) 調査の背景

集合匿名化（以下、匿名化）技術はパーソナル情報の流通を促し、既存のビジネスの効率化や新たなビジネスを創出する契機を提供し得る技術である。しかし、これまでのところ集合匿名化を用いたビジネスの事例はほとんどなく、むしろ医療分野を中心とした研究目的での利用が主である（4.1 節参照）。

匿名情報の流通およびそれによる新たなビジネスの創出や既存ビジネスの効率化が進まない原因として、以下が考えられる。

- 匿名情報の提供、または利用事例がなく、効果が不明確である
- 匿名情報を利用したサービスの具体例が乏しく、イメージが難しい
- 匿名情報を利用するサービスを実施した場合の収益面について可能性が不明確であり、ビジネスとして収益を得られるか分からない

今後、社会の情報化を推進し、新たなビジネスの創出や既存ビジネスの効率化を推し進めるためには、上記の要因について検討を行い、匿名情報の流通を促進することが求められる。

(2) 調査の目的

上述の三つの原因を解決するために、本項では以下を目的とする。

- 匿名情報を利用するサービスモデルの多様性を明らかにすること
- 匿名情報を利用するサービスモデルの市場規模について明らかにすること
- 今後有望と考えられる匿名情報を利用するビジネスモデルについて、詳細に検討すること

(3) 調査方法

調査ステップを図 4-35 に示す。

まず、匿名情報を利用するサービスのモデルについて、ブレインストーミング等により、複数の例を抽出する。同時に、匿名化を必要とするサービスの条件を検討し、その条件を基にして抽出した各サービス例をスクリーニングする。

次に、スクリーニングにより割り出された匿名情報を利用するサービスについて、それぞれ市場規模を推計し、各推計値を足し合わせることで匿名情報を利用するサービス全体の市場規模を推計する。

最後に、今後有望と考えられる匿名情報のサービスモデルについて、詳細化を行う。

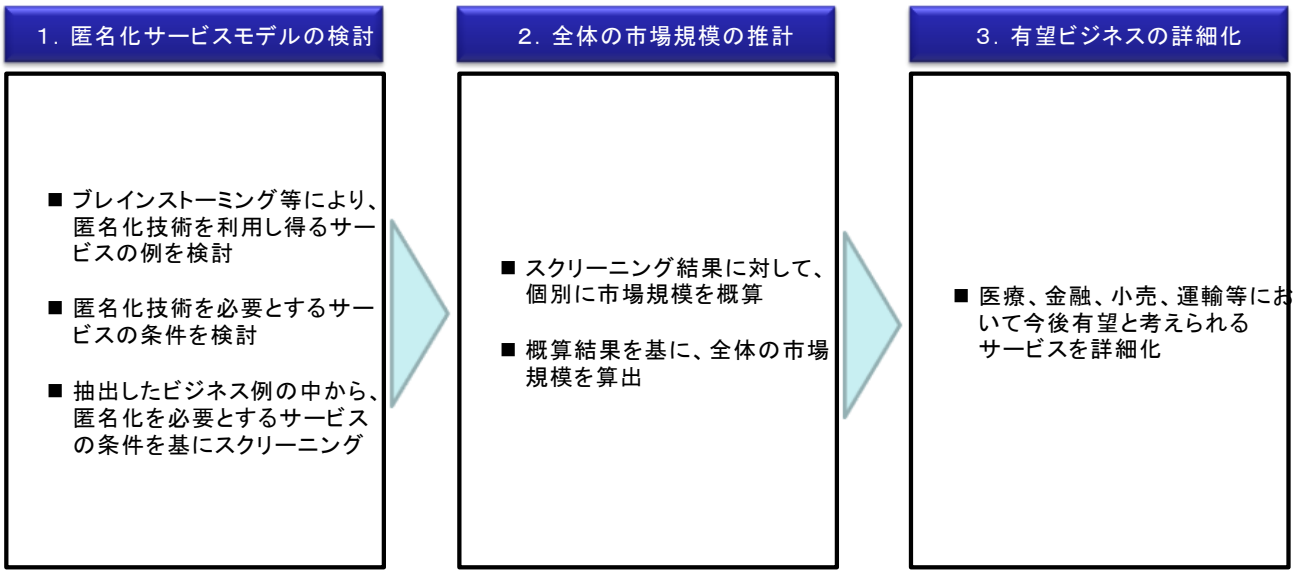

図 4-35 調査方法

4.5.2 匿名化サービスモデルの検討

匿名情報を利用するサービスについて、複数の例を抽出する。また、匿名化が必要でかつビジネスとして成立し得る条件について検討を行い、抽出したサービス例をスクリーニングする。

(1) 匿名情報利用サービスの条件

匿名情報を利用するサービスは、匿名化すべきデータを扱っている必要がある（条件 A）。匿名化すべきデータとは、例えば、個人の病歴や通院歴などの医療情報をはじめとするセンシティブデータを扱っている場合が挙げられる（条件 A-1）。センシティブデータを扱っていない場合でも、情報を提供した個人（以下、情報提供者）を特定しやすい場合には、プライバシー等の観点から匿名化を必要とする（条件 A-2）。例えば、データセットを統計的な観点からみて偏りが大きく、希少なデータがある場合には、そのデータから個人を特定される可能性があるため、匿名化を必要とする（条件 A-2-a）。また、データセットのフォーマットに依存し、一つのレコードを定義する属性が多い場合には、個々のレコードがユニークになる可能性が高くなるため、情報提供者個人の特定が行われる可能性が高まる（条件 A-2-b）。また、属性としては一つであるが、行動履歴などの履歴データも、その系列が長くなるほど、情報提供者個人を特定しやすくなると考えられる（条件 A-2-c）。

一方で、匿名化がサービスの阻害要因となるようなサービスは、サービスそのものの実施が困難となるため、匿名情報利用サービスには向かない（条件 B）。サービスを行うために、複数の情報源（以下、情報収集者）から個別に匿名情報の購入等を行い、それらに対して名寄せなどによって結合する必要があるサービスが挙げられる（条件 B-1）。また、匿名化はデータ（セット）に対してノイズを付加する操作であるという側面を持っている。このため、匿名化によって、サービスに必要となるデータ分析の結果への影響が大きくなるような場合には、匿名情報を利用するサービスには向かないだろう（条件 B-2）。このようなケースとしては、分析モデルが精緻で複雑で精度の高い分析結果を必要とする場合（条件 B-2-a）や、

誤差の影響が分析結果を大きく左右するような分析を要するようなサービスの場合（条件 B-2-b）が、挙げられる。

上記について整理した結果を、図 4-36 に示す。ここで匿名化を要するデータを扱っており（条件 A が成り立つ場合)、かつ、匿名化によりサービスへの影響が少ないと考えられる場合（条件 B の否定が成り立つ場合）が、匿名情報利用サービスの条件といえる。

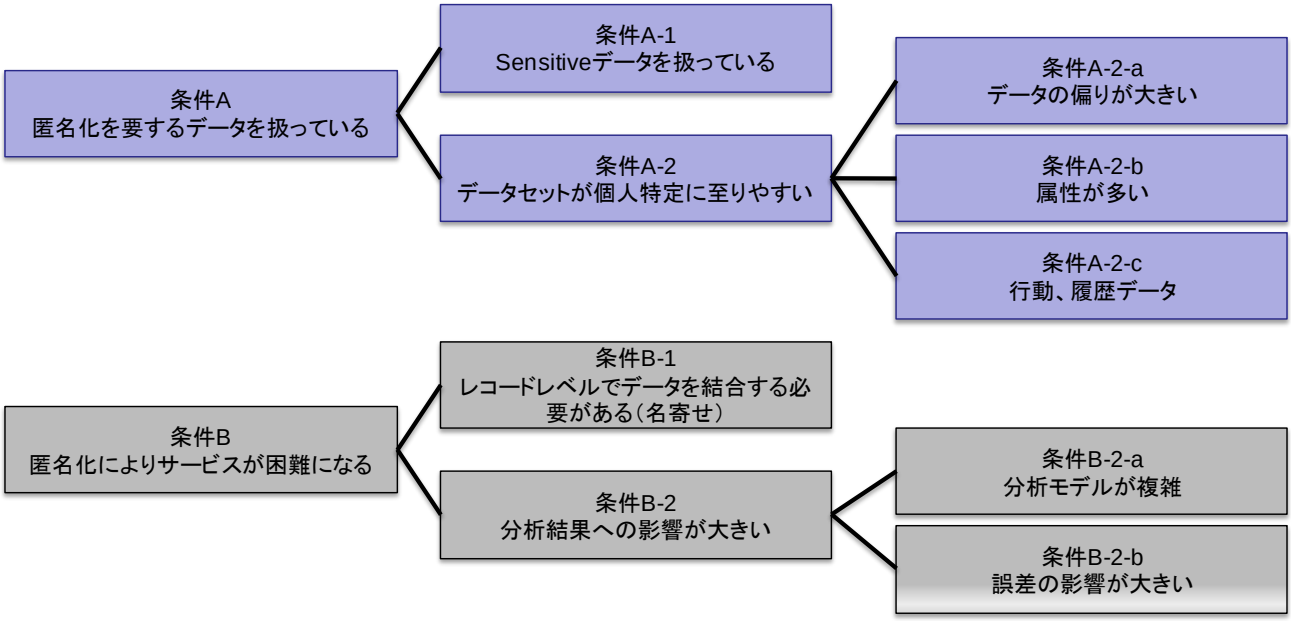

図 4-36　匿名情報利用サービスの条件

(2) 匿名化を要するサービス例

「図 4-36　匿名情報利用サービスの条件」に匿名情報利用サービスの例を示す。条件 A および条件 B は図 4-36 に示したものであり、条件 A が○、条件 B が×のサービスが匿名情報利用サービスとしてスクリーニングされたものである。

表 4-20　匿名情報利用サービス例一覧

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
1	医療	疾病情報等の保護により、患者の医療情報が断続的になっており、効果的な治療や分析ができていない	患者から収集した医療情報を分析することで疫学研究を行うこと	レセプト 電子カルテ	患者	病院（医師）	病院（医師）	○	×
2	医療	医療画像は病院が保管するものであり、医療界全体で有効に活用されていないデータ量を増やすことで医療の発展に役立てる	正常画像との比較による疾病のスクリーニング	医療画像	病院（医師）	病院（医師）	病院（医師） 患者	○	○
3	医療	疾病情報等の保護により、患者の医療情報が断続的になっており、効果的な治療や分析ができていない	病気にかかりやすい人、アレルギー等の要因分析	疾病履歴 生活履歴	病院（医師）	病院（医師） 学術関係者	学術関係者	○	○
4	医療	疾病は遺伝を起因とするものも多く、家族の疾病履歴情報を用いて、有効な疾病予測、診断を行うことが待ち望まれている	家族の疾病履歴と生活行動から疾病予測	疾病履歴(家族) 生活行動 履歴	患者	病院（医師） 学術関係者	病院（医師） 学術関係者	○	○
5	医療	普段からの健康管理気運が高まっている中、気象情報を含めた位置情報に関連した健康への影響を与える要素を把握したいというニーズがある	気象情報等の組合せによる健康管理支援	位置情報 経路情報 バイタル	気象関連会社、組合 一般家庭	病院（医師） 健康保険組合	病院（医師） 健康保険組合	○	×

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
6	医療	普段からの健康管理気運が高まっている中、食事情報を把握することでより健全な生活習慣を外から管理することが望まれている	食事や購入物と合わせて、疾病の履歴を勘案して、健康管理を行うこと	食事情報 購入履歴 疾病履歴	一般家庭 病院（医師） 患者	病院（医師） 健康保険組合	病院（医師） 健康保険組合	○	×
7	医療	遺伝情報から自身が将来にかかりやすい病気等を予測するビジネスが、アメリカをはじめとして、活発になってきている	遺伝子レベルにおいて、今後予測される病気を知る。また、その情報から、的確な診療を行う	ゲノム情報	一般利用者	医療関係機関	医療関係機関	○	○
8	安全	スマートメータなど、家庭にあるセンサー情報を利用して、より住みやすいコミュニティを作ることに注目が集まっている	家電製品のセンサー情報と個人の位置情報とを連携し、犯罪等の異常判定を実施	家庭内センサー 位置情報	一般利用者	警備保障会社	警備保障会社	○	×
9	安全	凶悪犯罪数が増加する中、犯罪から身を守る手段として防犯マップという概念が普及しつつある	犯罪発生情報や被害状況、場所、時間帯の情報を利用し、防犯マップとして公開する	犯罪発生データ	警察	警察	警察 一般市民	○	○

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
10	安全	子供が犯罪に巻き込まれることが増えてきており、保護者は安全な社会を望んでいる	子ども等の経路情報に基づき、普段の行動範囲からの逸脱を判定し、保護者等に警告を行う	生活地理情報 位置情報 犯罪データ	一般利用者 （子供）	警備保障会社 通信会社	警備保障会社 通信会社 子どもを持つ保護者	○	×
11	金融	不払いや貸し倒れ等のリスクが増大する経済において、より信用リスクをヘッジできるデータが求められている	複数の信用情報を統合し、信用リスクを分析、ヘッジすること	信用情報 支払履歴	金融関連機関	金融関連機関	金融関連機関	○	○
12	金融	生命保険において、損害率に関するより正確な情報を獲得することで、より顧客にあった商品開発をしたいというニーズがある	金融機関との取引履歴と各社支払の情報を統合し、今後の支払リスクを分析すること	生命保険の加入者情報	生命保険会社 保険加入者	生命保険会社	生命保険会社	○	○
13	金融	損害保険において、損害率に関するより正確な情報を獲得することで、より顧客にあった商品開発をしたいというニーズがある	複数の生命保険会社が保有するデータを統合し、保険料策定のための基礎データやマーケティングとして使用	損害保険の加入者情報	生命保険会社 保険加入者 損害保険会社	損害保険会社	損害保険会社	○	○

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
14	金融	オンラインショッピングとは異なり、実世界における一般消費者の商品購入履歴は情報が保護されており、有効に活用されていない。小売業者としては、より効果的に消費者へ自社商品を売りたいと考えている	クレジットカードや金融商品の利用履歴、小売店での購入履歴を統合することで、消費者の生活パターン、資金状況、生活必需品等を予測し、適切なタイミングで金融商品等のリコメンデーションを実施	金融商品 購入履歴 カード利用 履歴 小売店での 購入履歴	金融関連 機関 消費者	金融関連 機関 カード会 社 小売業者	カード会 社 小売業者	○	○
15	金融	個人の生活レベルの情報は対外的に使用されることはなく、それを統合したマクロな情報として扱われる傾向にある。しかしながら、ミクロな情報を匿名化して用いることにより、より正確な経済状況を把握することが望まれている	信用情報と個人の生活レベル等の情報を統合し、個人の消費活動や金融商品利用状況等に関する統計分析を行うことで、将来的な金融商品等の開発に利用	信用情報 収入状況 生活レベル	金融関連 機関	金融機関 保険業 学術関係 者	金融機関 保険業 学術研究 経済統計	○	×
16	金融	証券会社をはじめとした、機関投資家により公平なトレーディング環境が壊されているという意識が個人投資家に根ざしている	株や債券のトレーディング情報を匿名化し、一般投資家に知らせることでより公平かつ有用なトレーディング環境を整える	投資家 株売買情報	投資家 金融機関	投資家 金融機関	投資家 金融機関	○	×

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
17	運輸	ハイテク機器である自動車とのコミュニケーションは今活発に研究開発されている分野である。技術開発とともに、自動車利用者に配信する適切な情報が何かということが現在模索されている	自動車の走行状況、環境情報、およびドライバーの状況を統合して事故／危険の予測し、ドライバーに警告を行う。また、事故や渋滞の原因を探る	プローブデータ 個人の状況に関する情報（画像等）	自動車利用者 道路管理関係者	警察 自動車利用者 メーカー 学術関係者	警察 都市計画 自動車利用者 メーカー 学術関係者	○	○
18	運輸	デジタルになっていく社会の中で、タクシーはアナログなサービス体系を保つビジネスであり、より効率的に利用者や利益を獲得する手段が模索されている	潜在顧客の行動パターンや利用交通手段等の情報を基に、地域計画に基づく特定事業計画を策定	行動履歴情報	一般利用者	通信キャリア	タクシー会社	○	×
19	運輸	デジタルになっていく社会の中で、タクシーはアナログなサービス体系を保つビジネスであり、より効率的に利用者や利益を獲得する手段が模索されている	潜在顧客が集中する地域を割り出し、配車情報等に利用	行動履歴情報	一般利用者	通信キャリア	タクシー会社	○	×
20	運輸	ガソリン高など、運輸業界の風当たりは強く、費用を抑えた運輸活動が望まれている	移動パターンにあわせて、最適な交通手段を薦める	行動履歴情報 利用交通手段履歴	運輸業界全般 一般利用者	運輸業界全般	運輸業界全般	○	×

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
21	運輸	ハイテク機器である自動車とのコミュニケーションは今活発に研究開発されている分野である。技術開発とともに、自動車利用者に配信する適切な情報が何かということが現在模索されている	ETC 情報を用いて、高速利用状況をデータでより正確に把握、渋滞緩和に役立てる	ETC 情報	一般利用者 道路公団	道路公団	一般利用者	○	×
22	小売	小売店において、顧客のデータをより正確に知ることは、商売の生命線であり、競合他社との優位性を見つけることにお金を投資することに積極的な傾向にある	他社の顧客データベースと結合することで、自社の顧客の位置づけを明確化する	顧客データベース（サービス利用履歴）	消費者 小売店	小売店 マーケティング関連会社	サービス小売店 マーケティング関連会社	○	○
23	小売	個人のサービス利用情報は、断続的に保管されており、効率的に使用されていない。匿名化することにより、情報を統合し、有効利用することが待ち望まれている	過去のサービス利用履歴から個人の趣味・興味を特定し、位置情報を基に、個人の嗜好にあった店舗・商品を勧める	サービス利用履歴 位置情報	消費者 サービス小売店 通信企業	サービス小売店 通信企業	サービス小売店 通信企業	○	×

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
24	小売	小売店の競争が激化しており、効率的に消費者に商品を売りたいという背景がある	購入履歴、支払履歴等において、特定エリア等における潜在顧客を割り出すと共に、潜在顧客の移動パターン等を捉え店舗のスクラップアンドビルドを行う	行動履歴 購入履歴 支払履歴	消費者 カード会社	小売（コンビニ等）	小売（コンビニ等）	○	○
25	小売	小売店の競争が激化しており、効率的に消費者に商品を売りたいという背景がある	店舗周辺の顧客の行動パターンと購買傾向を分析し、自店舗における販売商品・価格などの戦略を策定する	行動履歴 購入履歴 支払履歴	消費者 カード会社	小売店 マーケティング関連会社	小売店 マーケティング関連会社	○	×
26	小売	小売店の競争が激化しており、効率的に消費者に商品を売りたいという背景がある	経路情報と属性情報から、店舗周辺を通過する潜在顧客の傾向を割り出し、その傾向にマッチした商品およびサービスを展開する	属性情報 経路情報	消費者	小売店 マーケティング関連会社	小売店 マーケティング関連会社	○	×
27	小売	通販やインターネットショップなどの仮想店舗の販売情報と実店舗の販売情報が共有されていない	仮想店舗で収集した販売情報を、リアル店舗を展開する小売業に販売し、小売業はその情報を基に商品陳列戦略を検討する	販売情報	一般利用者	インターネットショップ インターネットモール 通信販売業者	（リアル店舗を展開する）小売業	○	×

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件A	条件B
28	小売	通販やインターネットショップなどの仮想店舗の販売情報と実店舗の販売情報が共有されていない	リアル店舗の販売情報(POS)情報を、仮想店舗を運営する小売業者に販売する。仮想店舗を運営する小売業者は、その情報を基に、商品在庫の調整および仕入れを検討する	販売情報 経路情報含む	一般利用者	（リアル店舗を展開する）小売業	インターネットショップ インターネットモール 通信販売業者	○	×
29	小売	PASMO や Suica、Edy をはじめとして電子決済手段が増える一方、そのデータを有効活用できずにいる	電子決済が行われた金額や消費者嗜好を把握することで、効果的なマーケティングを行う	電子決済情報	一般利用者 電子決済関連会社	電子決済関連会社	メーカー 小売店 マーケティング会社	○	×
30	サービス	通信利用情報が有効的にマーケティングに使われていない現状があり、通信会社は有効に使いたいと考えている	通信会社等のグループ企業において、個人の支払履歴等を統合し、設備投資や商品開発をはじめとする戦略策定	通信サービス利用履歴 位置情報	加入者 通信会社	通信会社関連企業	通信企業関連グループ企業 企業連携	○	○
31	サービス	SNS などソーシャルネットワークが Web 上で盛り上がっているが、実世界への効率的な利用がまだ行われていない	ネット情報から、個人ネットワークをグルーピングして、個人の「コネクション」を把握。 就職活動や営業活動等に利用	個人ネットワーク	一般人	学術関係者 マーケティング会社	学術関係者 マーケティング会社	○	○

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件A	条件B
32	サービス	テレビや出版が広告で伸び悩むなか、いかに広告を効率よく消費者に提示するかが問題となっている	位置情報に合わせた特定地域に対する広告を行う。繁華街などでは、特定地域に入ったものに広告を提供する	位置情報	一般利用者	サービス小売店 通信企業	サービス小売店 通信企業 一般利用者	○	×
33	サービス	Web 上には、個人情報など情報が煩雑に置かれている。その情報は断片的に Web 上に存在するため有効に活用されていない	ブログ上で語られる趣味・嗜好等のプロフィール情報と購入履歴を組み合わせ、より有用なマーケティング情報とすること	プロフィール情報 購入情報 ブログ情報	消費者	オンラインショップ マーケティング会社	オンラインショップ マーケティング会社	○	○
34	サービス	twitter や SNS など情報伝達方法が刻一刻と変わっていく社会において、次のトレンドを把握して、学術や経済において有効活用したいというニーズがある	通話履歴やメール履歴から、コミュニケーションモデルを構築する社会的情報伝達に関する研究を展開	コミュニケーション履歴	通信会社 ユーザ	学術関係者	学術関係者	○	○
35	サービス	人口の少ない日本において、主婦をはじめとして、労働力を有効活用するビジネスが求められている	個人間委託業務。個人が業者や企業にクリーニングなどの雑務や家事を委託するのではなく、匿名の個人に委託する	位置情報 行動履歴情報	一般利用者	サービス	一般利用者 サービス	○	△

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	利用情報	情報提供者	情報収集者	情報利用者	条件 A	条件 B
36	サービス	アンケートは個人情報が多く含まれ、特定目的にしか使用できないように制限されている。しかしながら、同一人物が行ったアンケートを統合することできれば、現在見えてない有意義なマーケティングデータをとることができると考えられている	複数アンケートとの統合を行うことで、より有意義なアンケート、統計を行う	アンケート情報	一般人	アンケート会社 学術関係者	アンケート会社 学術関係者	○	○
37	サービス	正確なテレビの視聴率や雑誌の購読に関する実態を把握することができていない	iPhone、iPad など個人が所有する情報端末を通して、雑誌や動画コンテンツに関する視聴情報を収集し、正確な実態を把握し、これをコンテンツ制作上の戦略策定に用いる	コンテンツのアクセス情報 性別、年代	一般利用者	キャリア	コンテンツ作成者	○	×

4.5.3 匿名情報の市場規模（推計）

上述のスクリーニングにより、匿名情報利用サービスとして選定されたサービスに対して、個々の市場規模を算出し、各分野および全体の匿名情報の市場規模を推計する。

(1) 個別の匿名情報利用サービスの市場規模

上述の個別サービスの市場規模について、表 4-21 に示す。

表 4-21　個別の匿名情報利用サービスの市場規模

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	サービス 市場規模
1	医療	疾病情報等の保護により、患者の医療情報が断続的になっており、効果的な治療や分析ができていない	患者から収集した医療情報を分析することで疫学研究を行うこと	約 300 億円
3	医療	疾病情報等の保護により、患者の医療情報が断続的になっており、効果的な治療や分析ができていない	病気にかかりやすい人、アレルギー等の要因分析	約 950 億円
4	医療	疾病は遺伝を起因とするものも多く、家族の疾病履歴情報を用いて、有効な疾病予測、診断を行うことが待ち望まれている	家族の疾病履歴と生活行動から疾病予測	
5	医療	普段からの健康管理気運が高まっている中、気象情報を含めた位置情報に関連した健康への影響を与える要素を把握したいというニーズがある	気象情報等の組合せによる健康管理支援	約 15 億円
7	医療	遺伝情報から自身が将来にかかりやすい病気等を予測するビジネスが、アメリカをはじめとして、活発になってきている	遺伝子レベルにおいて、今後予測される病気を知る。また、その情報から、的確な診療を行う	130～180 億円
8	安全	スマートメータなど、家庭にあるセンサー情報を利用して、より住みやすいコミュニティを作ることに注目が集まっている	家電製品のセンサー情報と個人の位置情報とを連携し、犯罪等の異常判定を実施	約 80 億円
10	安全	子供が犯罪に巻き込まれることが増えてきており、保護者は安全な社会を望んでいる	子ども等の経路情報に基づき、普段の行動範囲からの逸脱を判定し、保護者等に警告を行う	約 120 億円

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	サービス 市場規模
11	金融	不払いや貸し倒れ等のリスクが増大する経済において、より信用リスクをヘッジできるデータが求められている	複数の信用情報を統合し、信用リスクを分析、ヘッジすること	約 2,000 億円
12	金融	生命保険において、損害率に関するより正確な情報を獲得することで、より顧客にあった商品開発をしたいというニーズがある	金融機関との取引履歴と各社支払の情報を統合し、今後の支払リスクを分析すること	約 455 億円
14	金融	オンラインショッピングとは異なり、実世界における一般消費者の商品購入履歴は情報が保護されており、有効に活用されていない。小売業者としては、より効果的に消費者へ自社商品を売りたいと考えている	クレジットカードや金融商品の利用履歴、小売店での購入履歴を統合することで、消費者の生活パターン、資金状況、生活必需品等を予測し、適切なタイミングで金融商品等のリコメンデーションを実施	約 680 億円
16	金融	証券会社をはじめとした、機関投資家により公平なトレーディング環境が壊されているという意識が個人投資家に根ざしている	株や債券のトレーディング情報を匿名化し、一般投資家に知らせることでより公平かつ有用なトレーディング環境を整える	約 1,770 億円
18	運輸	デジタルになっていく社会の中で、タクシーはアナログなサービス体系を保つビジネスであり、より効率的に利用者や利益を獲得する手段が模索されている	潜在顧客の行動パターンや利用交通手段等の情報を基に、地域計画に基づく特定事業計画を策定	640 億円
19	運輸	デジタルになっていく社会の中で、タクシーはアナログなサービス体系を保つビジネスであり、より効率的に利用者や利益を獲得する手段が模索されている	潜在顧客が集中する地域を割り出し、配車情報等に利用	
20	運輸	ガソリン高など、運輸業界の風当たりは強く、費用を抑えた運輸活動が望まれている	移動パターンにあわせて、最適な交通手段を薦める	約 600 億円

No.	分野	背景・ニーズ	匿名情報利用 サービス概要	サービス 市場規模
21	運輸	ハイテク機器である自動車とのコミュニケーションは今活発に研究開発されている分野である。技術開発とともに、自動車利用者に配信する適切な情報が何かということが現在模索されている	ETC 情報を用いて、高速利用状況をデータでより正確に把握、渋滞緩和に役立てる	
25	小売	小売店の競争が激化しており、効率的に消費者に商品を売りたいという背景がある	店舗周辺の顧客の行動パターンと購買傾向を分析し、自店舗における販売商品・価格などの戦略を策定する	約 1,350 億円
26	小売	小売店の競争が激化しており、効率的に消費者に商品を売りたいという背景がある	経路情報と属性情報から、店舗周辺を通過する潜在顧客の傾向を割り出し、その傾向にマッチした商品およびサービスを展開する	
27	小売	通販やインターネットショップなどの仮想店舗の販売情報と実店舗の販売情報が共有されていない	仮想店舗で収集した販売情報を、リアル店舗を展開する小売業に販売し、小売業はその情報を基に商品陳列戦略を検討する	約 480 億円
28	小売	通販やインターネットショップなどの仮想店舗の販売情報と実店舗の販売情報が共有されていない	リアル店舗の販売情報(POS)情報を、仮想店舗を運営する小売業者に販売する。仮想店舗を運営する小売業者は、その情報を基に、商品在庫の調整および仕入れを検討する	約 1,210 億円
29	小売	PASMO や Suica、Edy をはじめとして電子決済手段が増える一方、そのデータを有効活用できずにいる	電子決済が行われた金額や消費者嗜好を把握することで、効果的なマーケティングを行う	約 25 億円
31	サービス	SNS などソーシャルネットワークが Web 上で盛り上がっているが、実世界への効率的な利用がまだ行われていない	ネット情報から、個人ネットワークをグルーピングして、個人の「コネクション」を把握。 就職活動や営業活動等に利用	280 億円
32	サービス	テレビや出版が広告で伸び悩むなか、いかに広告を効率よく消費者に提示するかが問題となっている	位置情報に合わせた特定地域に対する広告を行う。繁華街などでは、特定地域に入ったものに広告を提供する	500 億円

(2) 各分野の市場規模と全体の市場規模

上述の個別サービスの推計結果を集計した結果を表 4-22 に示す。

全体では約 11,635 億円規模と推計され、金融分野（約 4,905 億円）、小売分野（約 3,065 億円）の市場規模が特に大きい。

表 4-22 匿名パーソナル情報の市場規模（推計）

分野	匿名情報の市場推計額
(1) 医療	約 1,445 億円
(2) 安全	約 200 億円
(3) 金融	約 4,905 億円
(4) 運輸	約 1,240 億円
(5) 小売	約 3,065 億円
(6) サービス	約 780 億円
全体	**約 11,635 億円**

4.5.4 有望ビジネスの詳細化

(1) 医療分野

(a) 医療情報を活用した有効治療サービス

① サービスの背景

医療機関では電子化が推進され、カルテやレセプトといった患者の医療情報の蓄積が進んでいる。しかし、そもそも診療情報はプライバシー上の観点からセンシティブな情報として扱うべきものであることもあるが、診療関連情報の所有者はだれであるかなどの問題から、患者の医療情報が個別病院のみで管理されやすいという現状がある。一方で、ひとりの患者が複数の病院や診療所などを利用する傾向があり、ひとりの患者の医療情報が複数の機関に分散して管理されているという現状がある。このような状況の下、一人の患者の情報が複数の医療機関で断続的に管理され、有効に活用されていないという問題がある。

② サービス内容

個別の病院等で管理されている電子カルテやレセプト情報を収集し、それを匿名化して病院等に販売等を行うことで、診断等の精度向上や新たな治療法の開発に役立てる。

情報収集者は各病院から電子カルテやレセプトなどの情報を収集する。収集後、名寄せ等を実施したのち、匿名化処理を施して匿名化診療情報として、病院等に販売する。匿名化診療情報は複数の患者の疾病歴や処方薬などの情報が含まれる。匿名化診療情報を購入した病院（に所属する医師）は、自身の研究により新たな治療法を開発したり、日々の診断に役立てたりすることにより、病院サービスの充実をはかる。

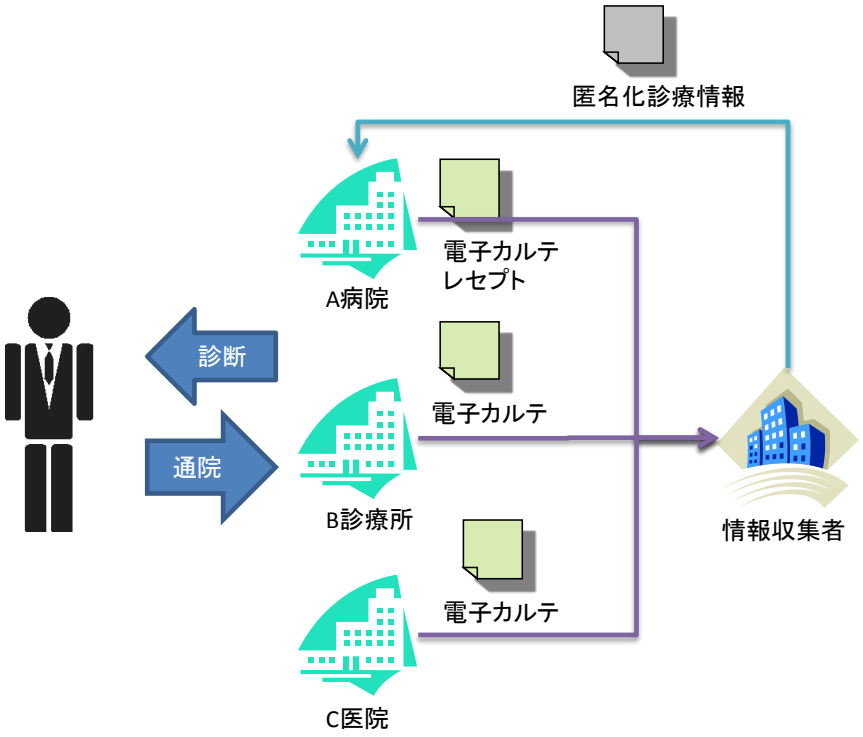

図 4-37　医療情報を活用した有効治療サービス

③　匿名化により解決する問題

匿名化技術を用いることにより、統合管理された医療情報を有効活用できる。その結果、医療サービスの向上を実現できる。

④　市場規模

我が国の年間患者数を概算し、その結果とレコード一件当たりの情報価値を乗じて市場規模を算出した。年間の患者数は、「2008 年厚生省統計情報」[63]を基に、人口×平均通院数（月、年代）×12 ヶ月で概算した。その結果は統計を元にしたものとの誤差も 0.12%であり、信頼のおけるものであると考えられる。レコード一件当たりの情報価値は、就職活動等で学生に告知を送付する際の料金を参考とし、100 円とした。

[63] 2008 年厚生省統計情報　http://www.mhlw.go.jp/toukei/saikin/hw/kanja/08/

表 4-23　年間患者数（概算）

	人口（百万人）	入院・通院回数（月）	年間患者数(百万人)
0 歳～9 歳	13.5	2.5	405
10 歳～19 歳	13.5	1.0	162
20 歳～29 歳	15	1.0	180
30 歳～39 歳	15	2.0	360
40 歳～49 歳	15	2.0	360
50 歳～59 歳	15	2.0	360
60 歳～80 歳	33	3.0	1,188
総計	**120**		**3,015**

上記においては、日本の総人口を 120（百万人）、平均寿命 80 歳、少子化関連因子 0.9 と設定する。また、入院・通院回数による年間患者数については、厚生省 2008 年統計を元に、信頼性について検証を行う。一日当たり患者数が 8.25（百万人）であり、推定年間患者数と比較すると 0.12%の誤差であり、数値の妥当性が証明される。これに、一次利用で用いられる医療匿名情報の利用価値を掛けることで、市場規模を推定することとする。この市場規模推定方法を用いると、本サービスの市場規模は、301,500（百万円）と推定される。

(2) 安全分野

(a) 家電センサーを用いた防犯サービス

① サービスの背景

防犯に関する意識は高い。携帯電話、スマートメータなど、家庭内のネットワークに接続する機器にセンサーの搭載が進んできており、これらの情報を用いて防犯サービスの効率化、高度化、低価格化を進めることが望まれている。

② サービス内容

家庭に設置されている家電等に内蔵されるセンサー情報と、携帯電話に搭載される GPS 等から取得できる位置情報から、強盗犯等の犯罪者の家庭への侵入を検知するサービスである。

セキュリティサービス提供会社は、各家庭と契約を締結した上で、家庭内にある家電等のセンサー情報と家族構成員が保有する携帯電話の位置情報を収集する。収集した家族構成員の位置情報と家電センサー等の情報から、「家族構成員が誰もいないはずなのに、冷蔵庫の扉があいている」などの異常を検出する。このような条件は、セキュリティサービス提供会社が保有するデータベースに蓄積され、更新される。データベースに蓄積・更新するこれらのルールは匿名化して管理するとともに、複数の事業所等で蓄積しているデータを匿名化して集約し、ルールの更新を行う。

ある契約家庭において異常を検知した場合には、警備員を急行させる、世帯構成員の携帯電話にメール等で連絡を入れるなどの防犯サービスを提供する。

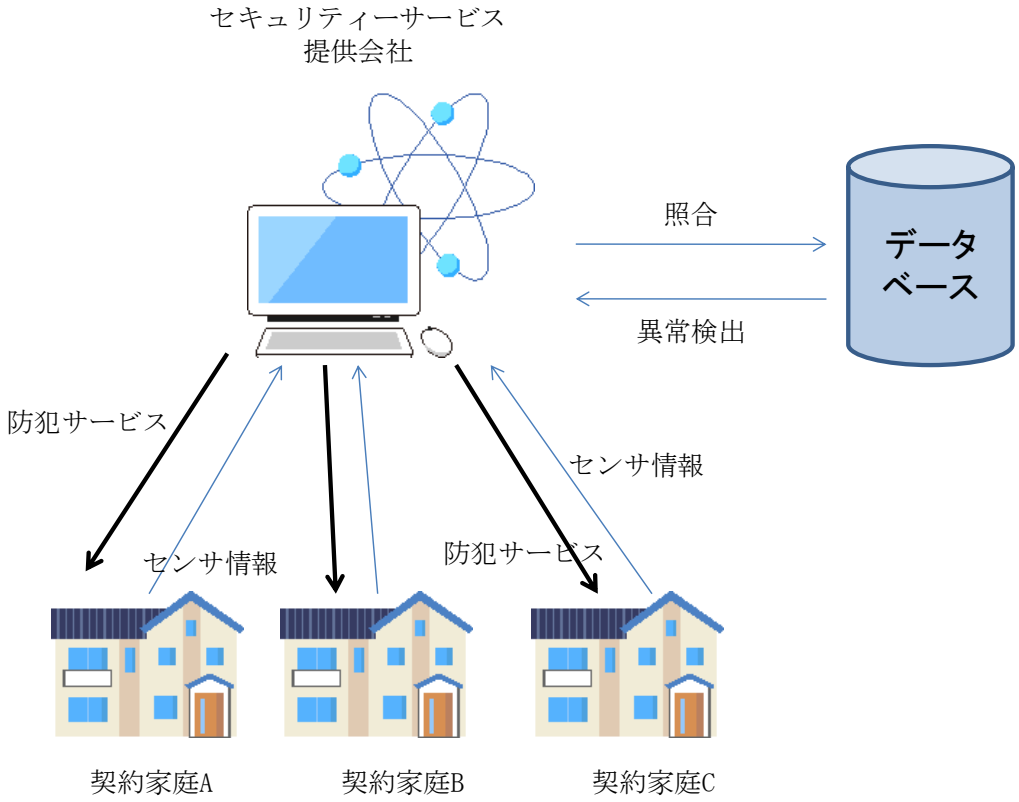

図 4-38　家電センサーを用いた防犯サービス（フロー図）

③　匿名化により解決する問題

家族構成員の位置情報と家電センサーの反応状況を蓄積するため、家庭における家族構成員の行動がセキュリティサービス提供会社に漏れ得る。したがって、家族のプライバシーの観点から、匿名化技術を適用することでこの問題を解決できる。

また、世帯構成員間においても、同様の問題が存在する。例えば、親が不在時の子供の行動などを把握したいというニーズは潜在的に存在する。一方で、子供は親が不在のときに自由に行動したいという、相反するニーズをもっている。匿名化を用いない場合、親はセキュリティサービス提供会社と連携することにより、もしくは、セキュリティサービス会社が親にこの情報を提供することにより、親は子供に対して圧倒的に優位な立場となり、子供のプライバシーは侵害される。これに対して、子供は携帯電話の電源を切り、位置情報を提供しないなどにより、自身のプライバシーを自分で守る行動に出かねない。

このような観点から、匿名化により、個々人と位置情報および家電センサーのリンクを切り離すことがサービスを成立させるための一要件となると考えられる。

④　市場規模

富士経済 2008 年予測の防犯機器・サービス市場規模と月額サービス料から、防犯サービスの利用者数を算定する。本サービスを提供することで増える利用人数割合を楽観ベースと悲観ベースで仮定する。

防犯機器・サービス市場規模は 2010 年度で 883 億円と推計されている[64]。サービスの月額利用料金は、防犯大手企業の料金例[65]を参考に、設置機器（買取）376,500 円を機器耐用年数 5 年[66]に年間月数 12 ヶ月を乗じた値（つまり、60 ヶ月）で除した結果に、月額利用料金 4,500 円を加えたものとして計算した。その結果、月額利用料金は 10,755 円となる（表 4-24 参照）。

本サービスを導入することにより、防犯機器・サービス市場規模が 10%増大するシナリオを楽観ベースシナリオ、5%増大する場合を悲観ベースシナリオとする。楽観ベースでは 8,830 百万円、悲観ベースでは 4,415 百万円と推計される。

表 4-24　各種パラメータ

防犯機器・ サービス市場規模：	883 億円
機器耐久年数：	5 年
月額料金：	10,755 円 (月額サービス料に加えて、機器料金を耐久年数で割った料金)
楽観ベース：	10.0% (大手防犯会社がヒットサービスを導入した時の利用者増加率を参考)
悲観ベース：	5.0%

(3) 金融分野

(a) 匿名化トレーディング情報活用サービス

① サービスの背景

インターネットの普及により、手軽に株式、債券、外貨などの金融商品を取引できる環境が整い、個人投資家の市場における存在感が増している。他方で、銀行、証券会社、ファンドをはじめとする大規模資本を有する機関投資家、個人では知りえない情報を基に取引を行うことが可能であるなど、個人投資家との間の情報の非対称性が存在する。例えば、銀行などでは、自行における多数の顧客の注文状況などを把握し、これを基に投資判断を行うことが可能であり、また、プロの間の情報のやり取りなどから投資判断を行うことも可能であるが、個人投資家がこれらの情報にアクセスすることはほとんど不可能である。

このように、取引環境の整備が進んだとはいえ、個人投資家とプロの投資家との間には、純然たる情報格差があり、個人投資家は投資活動を行う上で不利な環境に立たされ

64 全日本伝説資材卸業協同組合連合会、住宅用セキュリティ・防犯監視カメラシステム特集 http://www.jeda.or.jp/news/news_65.html

65 セコムホームセキュリティ　一戸建て｜プラン・料金例 http://www.secom.co.jp/homesecurity/plan/kodate/detail01.html

66 耐用年数については、器具および備品の耐用年数表（http://www.k3.dion.ne.jp/~afujico/zeigaku/taiyounen/be0108.htm）から「その他の事務機器」を参考に 5 年とした。

ているといえる。このため、プロの投資家と個人投資家との間の情報格差を埋めるためのサービスが求められている。

② サービス内容

証券会社が収集可能な、個人投資家や機関投資家の取引情報を匿名化して共有し、これを各社で分析してサービスとして、自社に口座を持つ個人投資家に提供するサービスである。

証券会社は、自社のインターネット取引サービス等や機関投資家などの取引情報を随時蓄積している。この情報をある一定間隔毎に匿名化して、予めアライアンスなどを締結している他社の証券会社と共有する。証券会社は、他社から収集した情報を基に分析した結果を個人投資家に（Web 上の）サービスとして提供する。例えば、直近一時間のある商品（例えば、株や外貨）の取引状況（売り、買いの残高）などをグラフ形式で提供することなどがあげられる。

料金は取引手数料などに上乗せして徴収することが考えられるが、会員向けの無料サービスとして提供することにより、会員数を伸ばし取引量を増やすことで収益を拡大することもできると考えられる。

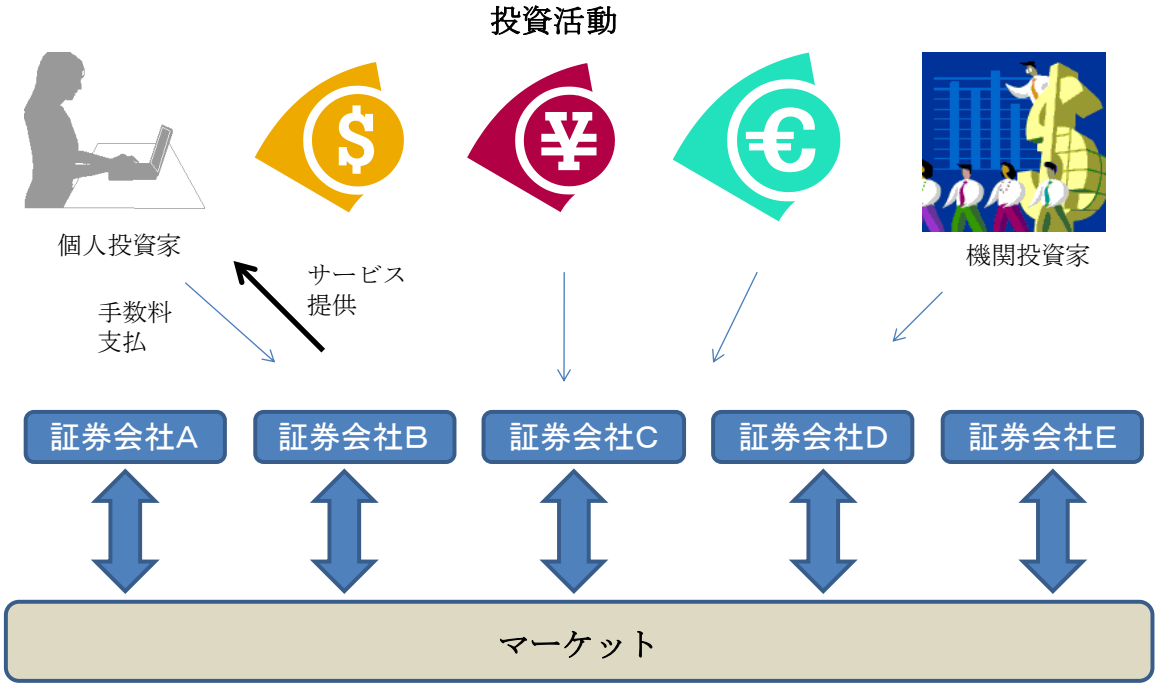

図 4-39 匿名化トレーディング情報活用サービス（フロー図）

③ 匿名化により解決する問題

本サービスは、プロの投資家と個人投資家との情報格差を少なからず埋めることができ、個人投資家にとっては有用なサービスになりえると考えられる。一方で、投資家は自身の取引情報を隠したいと考えるだろう。特に、機関投資家など、大規模資本を有する投資家がどのように動いているかは、市場への影響もあり（自身にとっていい場合も悪い場合もある）、慎重になることが想定される。また、個人投資家においても、取引量

や取引金額の多い個人投資家は、自身の資産や経済力が漏れ、その結果、不当な勧誘を受けるなどの被害を受ける可能性がある。

したがって、匿名化を施すことにより、投資家に関する情報を秘匿し、純粋に取引量だけを用いたサービスを構築することができる。つまり、本サービスにおいて、匿名化はサービスを構成するための重要なファクターといえる。

④ 市場規模

2010 年 10 月時点での、ネット証券の口座数上位 5 社をリストアップ[67]し、口座数を元に売買代金を加重平均する。これは、取引数は口座数に比例するという仮定に基づいている。

表 4-25 ネット証券会社　口座数上位 5 社

証券会社名	口座数
SBI 証券	2,138,603
マネックス証券	1,285,403
楽天証券	1,031,529
カブドットコム証券	717,366
松井証券	801,668

2010 年 4-9 月期の上位 5 社の売買代金を合算したものを計算し、2 倍したものを通年として換算する。

表 4-26　売買代金（単位：兆円）

証券会社名	4-9 月期	通年
SBI 証券	15.6	31.3
マネックス証券	9.4	18.8
楽天証券	7.5	15.1
カブドットコム証券	5.2	10.5
松井証券	5.9	11.7
合計	**43.7**	**87.4**

[67] SBI 証券
http://www.secom.co.jp/homesecurity/plan/kodate/detail01.html
マネックス証券
http://www.monexgroup.jp/jp/ir_library/account_volume_monthly/index
楽天証券
https://www.rakuten-sec.co.jp/web/company/disclosure/business/fy2010.html
カブドットコム証券
http://kabu.com/company/disclosure/order.asp
松井証券
http://www.matsui.co.jp/company/press/ir.html

一口座当たりの年間平均売買代金を計算すると、14.6（百万円）であり、一日平均売買代金は、40,079（円）と計算される。

毎日のトレード約定数の平均をシナリオ毎に以下のように定める。

- Aシナリオ：毎日平均 1 トレード
- Bシナリオ：毎日平均 2 トレード
- Cシナリオ；毎日平均 3 トレード

シナリオ毎に、約定した売買代金の一回平均を算出する。

表 4-27　A,B,C シナリオ毎　売買代金

	売買代金／回　（円）
毎日 1 トレード	40,079
毎日 2 トレード	20,039
毎日 3 トレード	13,360

各社の約定手数料と比較する（手数料は 2010 年 11 月現在のものを使用）。

表 4-28　SBI 証券　手数料一覧[68]

取扱商品	1 注文の約定代金	手数料（税込）
現物	～10 万円	145 円
	～20 万円	194 円
	～50 万円	358 円
	～100 万円	639 円
	～150 万円	764 円
	～3,000 万円	1,209 円
	3,000 万円超	1,277 円

表 4-29　マネックス証券　手数料一覧[69]

約定金額	手数料	
	成行	指値
～100 万円	1,050 円	1,575 円
～200 万円	2,100 円	3,150 円

[68] SBI 証券　手数料一覧
https://www.sbisec.co.jp/ETGate/?_ControlID=WPLETmgR001Control&_DataStoreID=DSWPLETmgR001Control&burl=search_home&cat1=home&cat2=price&dir=price%2F&file=home_price.html&getFlg=on

[69] マネックス証券　手数料一覧
http://www.monex.co.jp/ServiceInformation/00000000/guest/G900/srv/srv05.htm

表 4-30　楽天証券　手数料一覧[70]

約定代金	手数料
10 万円まで	145 円／1 回
20 万円まで	194 円／1 回
50 万円まで	358 円／1 回
100 万円まで	639 円／1 回
150 万円まで	764 円／1 回
3,000 万円まで	1,209 円／1 回
3,000 万円超	1,277 円／1 回

表 4-31　カブドットコム証券　手数料一覧[71]

約定金額	インターネット			電話			
				自動音声応答		オペレーター	
	取引所取引		kabu.com PTS	取引所取引		取引所取引	
	成行	指値	成行／指値	成行	指値	成行	指値
2 万円以下	105 円	630 円	378 円	210 円	735 円	2,205 円	2,730 円
20 万円以下	500 円	1,025 円		605 円	1,130 円	2,600 円	3,125 円
100 万円以下	1,050 円	1,575 円		1,155 円	1,680 円	3,150 円	3,675 円
1,000 万円以下	1,890 円	2,415 円		1,995 円	2,520 円	3,990 円	4,515 円
1,000 万円超	1,000 万円を超える部分に対して、100 万円ごとに 42 円加算						

表 4-32　松井証券　手数料一覧[72]

1 日の約定代金合計金額	手数料（税込）
10 万円まで	21 円
30 万円まで	315 円
50 万円まで	525 円
100 万円まで	1,050 円
200 万円まで	2,100 円
100 万円増えるごとに 1,050 円加算	
1 億円超	105,000 円（上限）

[70] 楽天証券　手数料一覧
https://www.rakuten-sec.co.jp/web/domestic/stock/commission.html#skip-01
[71] カブドットコム証券　手数料一覧
http://kabu.com/cost/
[72] 松井証券　手数料一覧
http://www.matsui.co.jp/service/fee/list.html

シナリオ毎に、口座数と手数料から手数料収入（/日）を計算する。

表 4-33　A シナリオ手数料、手数料収入（単位：円）

A シナリオ

	手数料	手数料収入
SBI 証券	145	310,097,435
マネックス証券	1,050	1,349,673,150
楽天証券	145	149,571,705
カブドットコム証券	500	358,683,000
松井証券	21	16,835,028

表 4-34　B シナリオ手数料、手数料収入（単位：円）

B シナリオ

	手数料	手数料収入
SBI 証券	145	620,194,870
マネックス証券	1,050	2,699,346,300
楽天証券	145	299,143,410
カブドットコム証券	500	717,366,000
松井証券	21	33,670,056

表 4-35　C シナリオ手数料、手数料収入（単位：円）

C シナリオ

	手数料	手数料収入
SBI 証券	145	930,292,305
マネックス証券	1,050	4,049,019,450
楽天証券	145	448,715,115
カブドットコム証券	105	225,970,290
松井証券	21	50,505,084

サービスによって、新顧客が増えると仮定した上で、純粋なサービスによる手数料の割増について計算する。また、サービスの形態としては、有料情報とするのではなく、全顧客に提供することにより、手数料が上乗せされるサービスを想定している。

表 4-36　シナリオ—手数料割増、口座純増加数

	手数料割増	口座増加数
悲観 1	5%	1%
悲観 2	5%	3%
中立 1	10%	1%
中立 2	10%	3%
楽観 1	20%	1%
楽観 2	20%	3%

表 4-37　シナリオ毎手数料収入(/日)

	A シナリオ	B シナリオ	C シナリオ
悲観 1	2,317,044,367	4,634,088,734	6,049,624,630
悲観 2	2,362,926,434	4,725,852,868	6,169,419,177
中立 1	2,427,379,813	4,854,759,627	6,337,701,993
中立 2	2,475,446,740	4,950,893,481	6,436,201,042
楽観 1	2,648,050,705	5,296,101,411	6,913,856,720
楽観 2	2,700,487,353	5,400,974,706	7,050,764,774

表 4-38　シナリオ毎純増手数料収入(/日)

	A シナリオ	B シナリオ	C シナリオ
悲観 1	132,184,049	264,368,098	345,122,386
悲観 2	178,066,116	356,132,232	464,916,933
中立 1	242,519,495	485,038,991	633,199,749
中立 2	290,586,422	581,172,845	758,698,798
楽観 1	463,190,387	926,380,775	1,209,354,476
楽観 2	515,627,035	1,031,254,070	1,346,262,530

表 4-39　シナリオ毎純増手数料収入(/年)

	A シナリオ	B シナリオ	C シナリオ
悲観 1	48,247,177,972	96,494,355,944	125,969,670,803
悲観 2	64,994,132,310	129,988,264,619	169,694,680,503
中立 1	88,519,615,784	177,039,231,568	231,117,908,416
中立 2	106,064,044,137	212,128,088,275	276,925,061,435
楽観 1	169,064,491,407	338,128,982,814	441,414,383,641
楽観 2	188,203,867,793	376,407,735,585	491,385,823,298

本市場規模推定においては、B-中立 1 シナリオを記載している（各上位 5 社が新サービスを提供した後の口座数の推移等を基にしている）。

以上より、約 1,770 億円規模の市場があると推定される。

(4) 運輸分野

(a) タクシー運行の最適化サービス

① サービスの背景

タクシー業界では、その供給量が過剰な状態の地域が存在し、サービス等の劣化、事業収益の減退、法令等の遵守状況の悪化、労働環境の劣悪化等を引き起こし、社会問題化している。これを受けて、国土交通省は、「特定地域における一般乗用旅客自動車運送事業の適正化および活性化に関する特別措置法」[73]を制定した。特定事業者として認定されたタクシー事業者は、特定事業計画を策定し、国土交通大臣の認定を受け、事業の質の向上に努めることが求められる。

このようにタクシー業界においては、タクシー事業の再構築が求められている。

② サービス内容

携帯電話等の端末に搭載されている位置情報から、顧客等が集まっており、乗車を期待できる可能性を割り出し、タクシーの配車等を行い、事業の最適化をはかるサービスである。

通信キャリア等が収集している携帯電話所有者の位置情報を集積し、匿名化してタクシー事業者に販売する。タクシー事業者はその情報を基に、顧客が高い確率で乗車してくれそうな有望地域にタクシーを配車する。

図 4-40 タクシー運行の最適化サービス（フロー図）

[73] 特定地域における一般乗用旅客自動車運送事業の適正化および活性化に関する特別措置法（タクシー適正化・活性化法案）について
http://www.mlit.go.jp/report/press/jidosha03_hh_000037.html

③　匿名化により解決する問題

経路や位置などの情報から、「誰」が「どこ」にいるか判明すると、犯罪等を誘発する場合がある。例えば、「女性」が夜「人通りの少ない道」や「街灯がない道」にいることが判明する場合などが想定される。また、本来は知られたくない「住所」などが割り出される可能性もある。

このように、匿名化を適用しないで本サービスを実施した場合には、プライバシー上の問題だけでなく、犯罪等を誘発する可能性を有しているといえる。

したがって、匿名化により、「誰」と「どこ」のリンクを切り離すことが、このサービスを成立するに当たり、重要なファクターであると考えられる。

④　市場規模

本サービスの市場規模の推定では、以下の式を用いることとする。

■市場規模　＝　タクシーの台数　×　客単価の上昇分

■客単価の上昇分　＝　一人当たりの単価　×　上昇割合

なお、本サービスの提供により、タクシー業界全体の市場が増大するという仮定の下に、推計を進める。また、一台当たりの一人輸送人員単価が 30 円増大すると仮定する。

まず、日本におけるタクシー台数、輸送人員、営業収入を統計資料[74]から表 4-40 に示す。

表 4-40　日本のタクシー台数、輸送人員、営業収入の合計

日本のタクシー台数	271,327 台
輸送人員	213,700 万人
営業収入	20,729 億円

表 4-40 を基に、平均客単価を計算する。その過程も含めて表 4-41 に示す。

表 4-41　タクシー一台あたりの平均客単価（概算）

項	計算式	値（平均値）
タクシー一台あたりの平均収益	営業収入÷日本のタクシー台数	7,639,859　円/台
タクシー一台あたりの平均輸送人員	輸送人員÷日本のタクシー台数	7876.105　人/台
タクシー一台あたりの平均客単価	タクシー一台あたりの平均収益÷タクシー一台あたりの平均輸送人員	970.0047　円

74 日本のタクシー台数：　全国ハイヤー・タクシー連合会　「全国の事業者数及び車両数の推移」
http://www.taxi-japan.or.jp/pdf/toukei_chousa/jigyousya_syaryou_suii.pdf
輸送人員：　全国ハイヤー・タクシー連合会　「輸送人員の推移」
http://www.taxi-japan.or.jp/pdf/toukei_chousa/yusoujinin.pdf
営業収入：　全国ハイヤー・タクシー連合会　「営業収入の推移」
http://www.taxi-japan.or.jp/pdf/toukei_chousa/eigyousyuunyuu_suii.pdf

本サービスを用いることにより、客単価が 30 円上昇すると仮定し、タクシー一台あたりの収益が 3.0%増加すると想定すると、本サービスを採用することにより、営業収益×3.0%=641.1 億円の市場規模が想定できる。

(b)　運送業者への最適経路情報提供サービス

①　サービスの背景

ガソリン高など、運輸業界の風当たりは強く、費用を抑えた運輸活動が望まれている。特に、トラック運送事業においては、総経費の約 20%が燃料費で占められるため、燃料の管理が急務である。また、トラックなどは、アナログに燃料を管理している業者が多く、本サービスを利用することで、燃料費削減を含め、業者の経営判断を容易にすることができると考えられる。

②　サービス内容

ETC 情報を用いて、高速利用状況をデータでより正確に把握し、渋滞緩和に役立てるサービスである。また、移動パターンにあわせて、最適な交通手段を薦めるサービスである。本サービスでは、最初のステップとして、主にトラックや特殊用途車向けに経路情報を提供することで、燃料費の管理や削減に寄与し、サービス料を得るビジネスモデルとする。また、経路情報や行動履歴がとりやすい高速道路を主な情報収集場所とする（ETC による高速道路への入出情報等）。

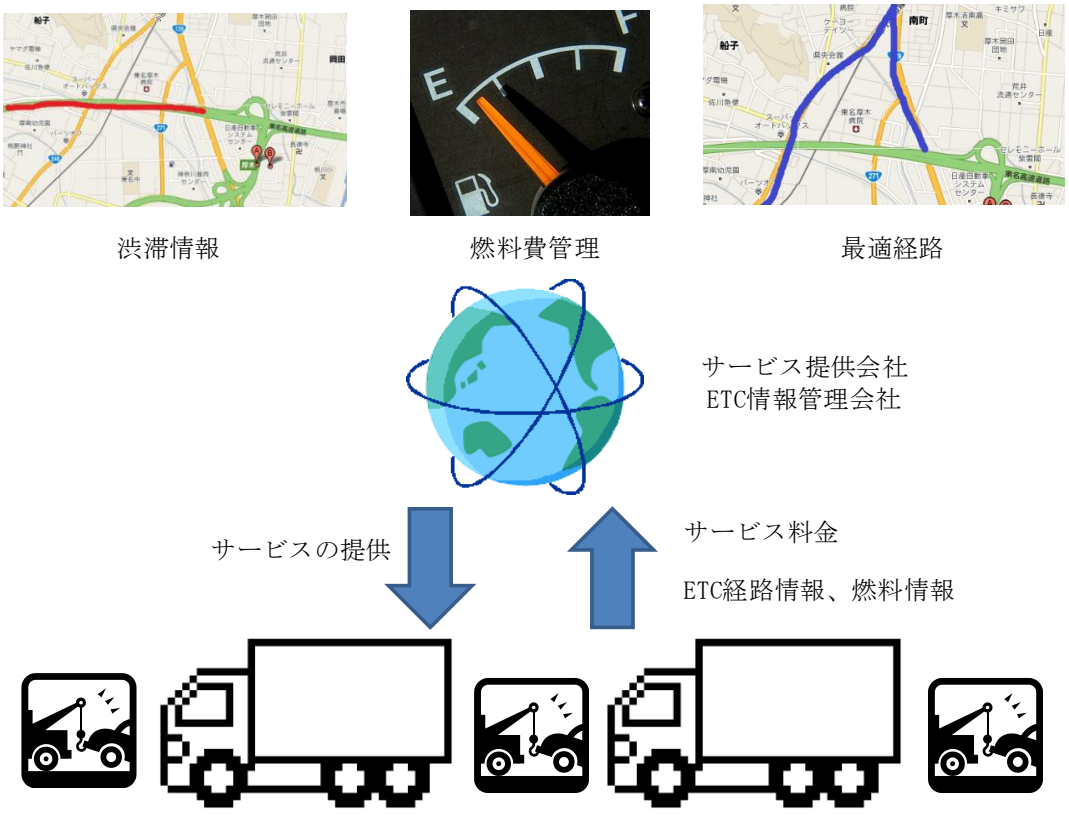

図 4-41　運送業者への最適経路情報提供サービス（フロー図）

③　匿名化により解決する問題

ETC による高速道路への入出情報は、サービスを利用する運送業者から取得される情報だけではなく、他の一般の利用者の情報を含む ETC 情報である必要がある。一般の利用者の ETC 情報にはどの車両がどこで入出したかが分かる情報が含まれており、一般利用者の情報は秘匿する必要がある。

④　市場規模

算出方法として、高速道路 ETC 利用台数（トラック＋特殊）×一台あたりの燃料削減額、を用いて推定する。一台あたりの燃料削減額は、一台あたりの燃料費×削減割合とする。

統計データ[75]を用いて、高速道路で ETC を利用した自動車の年間台数を計算する。年間の高速道路 ETC 利用台数は、5,771,992（千台）である。

表 4-42　高速道路別　自動車 ETC 利用台数（千台/日）

	H21.10	H21.11	H21.12	H22.1	H22.2	H22.3	H22.4	H22.5	H22.6	H22.7	H22.8	H22.9
東日本高速道路	2,474	2,437	2,346	2,192	2,250	2,407	2,472	2,575	2,541	2,906	3,098	2,873
中日本高速道路	1,708	1,753	1,648	1,531	1,575	1,665	1,732	1,727	1,702	1,972	2,149	1,981
西日本高速道路	2,320	2,388	2,305	2,132	2,187	2,360	2,490	2,548	2,415	2,967	3,274	3,029
NEXCO系小計	6,502	6,578	6,299	5,855	6,011	6,432	6,693	6,849	6,658	7,845	8,521	7,883
首都高速道路(株)	1,132	1,128	1,135	1,039	1,084	1,135	1,117	1,075	1,126	1,162	1,170	1,150
阪神高速道路(株)	886	870	881	804	833	876	870	846	858	896	923	897
本四高速道路(株)	38	40	38	38	35	45	51	62	43	49	65	51
合計	**15,060**	**15,194**	**14,652**	**13,591**	**13,975**	**14,920**	**15,425**	**15,682**	**15,343**	**17,797**	**19,200**	**17,864**

次に、高速道路 ETC 利用台数における、トラックと特殊用途車の台数を推計する。上記の表 4-42 から通年での ETC 利用台数を算出の上、文献76の 2009 年度分のデータから乗用車、トラック、バス、その他の割合を算出して、積を取ることで推計する。

[75] 独立行政法人　日本高速道路保有・債務返済機構　高速道路機構 WEB
各月の交通量　過去分のデータ（各月一覧表）http://www.jehdra.go.jp/pdf/kotu/k999.pdf

[76] 株式会社　潤滑通信社、自動車保有台数推移（各年末現在）
http://www.juntsu.co.jp/jouhou/toukei/toukei14.html

表 4-43　2009 年度自動車保有台数内訳（台）

	乗用車	トラック	バス	その他
普通車	16,688,645	2,319,612	108,760	
小型四輪車	23,919,554	3,952,534		
軽四輪車	17,412,189	9,288,679		
小型車			119,637	
特殊用途車				1,515,691
計	**58,020,388**	**15,560,825**	**228,397**	**1,515,691**
割合	**77.0%**	**20.7%**	**0.3%**	**2.0%**

表 4-44　高速道路　ETC 利用台数内訳　推計

（千台）

自家用車	4,445,959
トラック	1,192,388
バス	17,501
特殊	116,144

トラック年間燃料費を国土交通省の統計データ[77]を元に推計する。軽油年間平均料金は、東京 2010 年 10 月のデータを採用する。

表 4-45　トラック年間年消費推計

	燃料費（兆円）	軽油年間平均料金（円）
2003 年	1.00	64.0
2010 年	1.80	115.2

トラック、特殊用途車の年間燃料費を台数ベースで計算する。年間燃料費は 1.98 兆円である。

シナリオ毎に燃料費の削減幅を計算し、市場規模を推計する。

表 4-46　シナリオ毎削減額

	削減割合	削減額
悲観シナリオ	0.5%	9,877
中立シナリオ	1.5%	29,630
楽観シナリオ	3.0%	59,260

77 2003 年国土交通省　燃料費データ　ニュース情報
http://www.47news.jp/CN/200711/CN2007112101000524.html
国土交通省　「中小トラック事業者構造改善支援事業」応募要領
http://www.mlit.go.jp/jidosha/sesaku/environment/cng/h20h/index2.htm

中立シナリオの場合の一台当たりの年間削減額は、29,630 百万円と計算される。記載した市場規模は、中立シナリオを用いることとする。約 300 億円規模の市場があると推定される。

(5) 小売分野

(a) 仮想店舗の購入履歴活用サービス

① サービスの背景

通販やインターネットショップなどの仮想店舗の販売情報と実店舗の販売情報が共有されていない。このため、実店舗を運営する事業者は、仮想店舗における商品の売れ行きや、年代・性別などでセグメントした商品販売トレンドなどを仮想店舗が独自に分析し、自社の戦略立案に役立てることができない現状がある。仮想店舗の販売情報を仮想店舗が利用できる環境になった場合、実店舗を運営する事業者は、これらの販売情報を基に、仕入れや商品在庫の調整、販売戦略の立案に利用することができる。

② サービス内容

仮想店舗の販売情報を、実店舗を運営する事業者に販売する。実店舗を運営する小売業者は、その情報を基に、商品在庫の調整および仕入れを検討する。

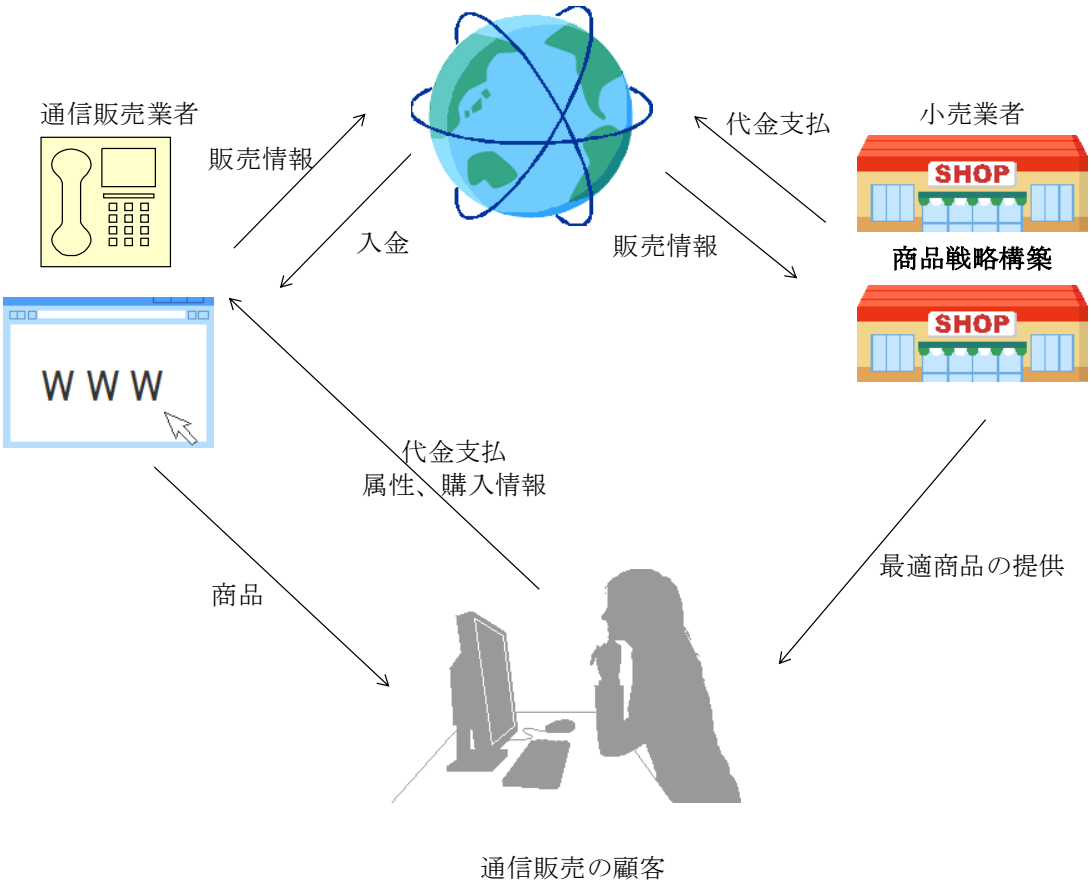

図 4-42 仮想店舗の購入履歴活用サービス（フロー図）

③　匿名化により解決する問題

仮想店舗の販売履歴は、情報提供者である個々人の消費者から提供される。他人に知られたくない商品を購入していることや、高額な商品を購入していることなどの事実と、その事実を有する個人とのリンクが判明する可能性があることは、消費者にとって望ましくない。したがって、購入した物品と購入者との対応関係を匿名化により、秘匿する必要がある。

④　市場規模

本サービスでは、ネットを含む通信販売における購買履歴データが、実店舗を運営する事業者への販売商品となる。このため、日本において、一年間に通信販売事業者が蓄積し得る購買履歴データの総量に対して、一件当たりの情報量の積を取ることで市場規模を算出することとする。ここで一件のデータとは、一回の通信販売利用時の購入品目であると仮定する。

まず、通販の利用状況について、経済産業省の調査[78]をもとに年間利用回数、年間利用額を計算する。同調査では、直近三ヶ月の利用回数であるため、これを四倍したものを通年での利用回数とする（表 4-47 参照）。

表 4-47　ネットを含む通信販売における年間平均利用回数（男女別）

	直近 3 ヶ月		通年	
	男性	女性	男性	女性
ネットショッピング	5.61	5.81	22.44	23.24
テレビショッピング	1.55	1.7	6.2	6.8
カタログ通販	2	2.35	8	9.4

表 4-47 の各セルに対して、男女別の日本の人口[79]（表 4-48 参照）を掛け合わせたものが、おおよそ通信販売事業者全体で蓄積可能な購買履歴データとなる（表 4-49 参照）。

表 4-48　日本の人口　男女別

（万人）

男	女
6,203	6,534

78 「消費者の購買に関するニーズの動向調査」の結果発表について
～リーマンショック以降の日本の消費者の実像～（METI/経済産業省）
http://www.meti.go.jp/press/20100421002/20100421002.html

79 統計局　人口推計
http://www.stat.go.jp/data/jinsui/pdf/201010.pdf

表 4-49　日本における通年での通信販売利用件数（推計）

	男性	女性	計
ネットショッピング	1,391,953,200	1,518,501,600	2,910,454,800
テレビショッピング	384,586,000	444,312,000	828,898,000
カタログ通販	496,240,000	614,196,000	1,110,436,000
総件数（推計）			**4,849,788,800**

日本における通年での通信販売利用件数（＝レコード件数）に対して、一件当たりの情報量を 10 円と仮定[80]し、掛け合わせると、およそ 480 億円規模の市場があると推計できる。

(b)　実店舗の販売情報活用サービス

①　サービスの背景

通販やインターネットショップなどの仮想店舗の販売情報と実店舗の販売情報が共有されていない。このため、仮想店舗を運営する事業者は、実店舗における商品の売れ行きや、年代・性別などでセグメントした商品販売トレンドなどを仮想店舗が独自に分析し、自社の戦略立案に役立てることができない現状がある。実店舗の販売情報を仮想店舗が利用できる環境になった場合、仮想店舗を運営する事業者は、これらの販売情報を基に、仕入れや商品在庫の調整、販売戦略の立案に利用することができる。

②　サービス内容

リアル店舗の販売情報(POS)情報を、仮想店舗を運営する小売業者に販売する。仮想店舗を運営する小売業者は、その情報を基に、商品在庫の調整および仕入れを検討する。経路情報など POS システムで取りうる匿名顧客情報を扱うこととする。また、小売業自身も統合した情報を有効活用できるようなサービスとする。

[80] 情報料金は、男性ネット通販の 1 回平均購入単価の 0.1%と設定する

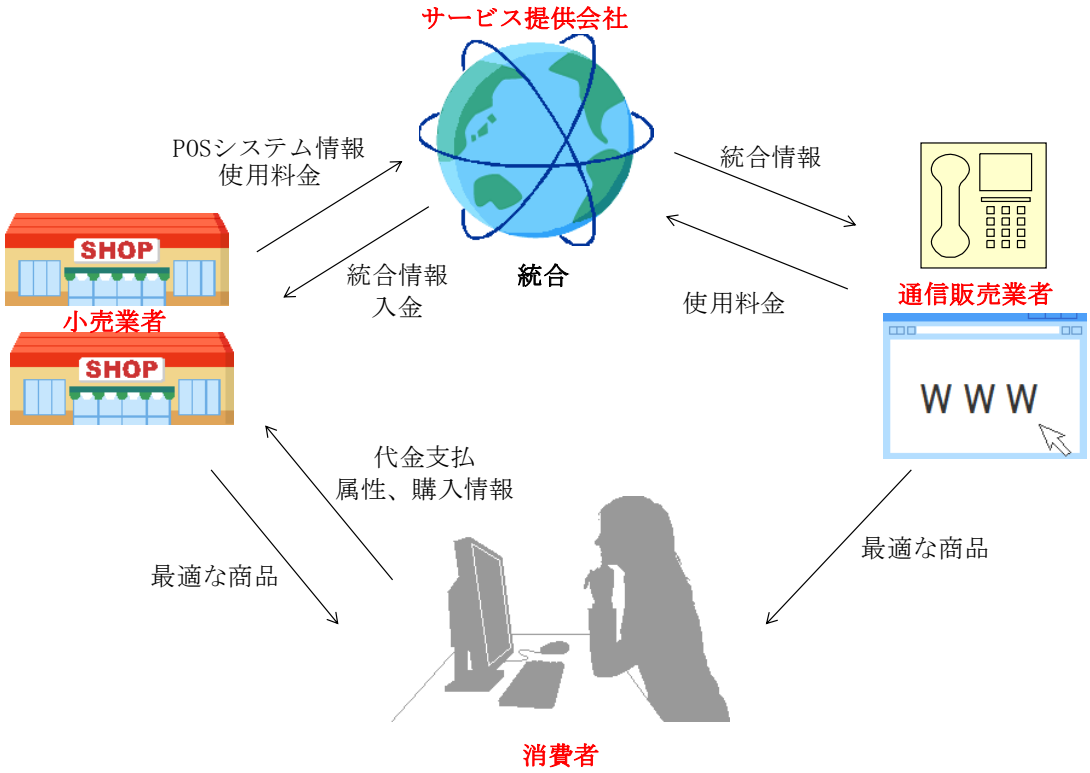

図 4-43　実店舗の販売情報活用サービス（フロー図）

③　匿名化により解決する問題

実店舗の販売履歴は、情報提供者である個々人の消費者から提供される。当然ながら、他人に知られたくない商品を購入していることや、高額な商品を購入していることなどの事実と、その事実を有する個人とのリンクが判明する可能性があることは、消費者にとって望ましくない。したがって、購入した物品と購入者との対応関係を匿名化により、秘匿する必要がある。

④　市場規模

小売店年間販売額として経済産業省の商業データ[81]から、小売店年間販売額は 135（兆円）である。

日本の総人口 12,737（万人）で年間販売額を割ることで、国民一人当たりの小売店の商品購入額が算出される。平均年間消費額は 1,060（千円）である。国民の小売店での一日の購入回数を、人口割合で加重平均して、算出すると、年間購入回数は 2.45 回となる。

[81] 経済産業省「平成１６年商業統計表業態別統計編」平成 14 年　小売業年間商品販売額

表 4-50　年代別小売店での想定購入回数（/日）

（回数）

年代	男子	女子
0	0.0	0.0
10	3.0	3.0
20	3.5	3.5
30	3.0	3.5
40	3.0	3.5
50	2.5	3.0
60 超	1.5	2.0

表 4-51　年代別人口推計(2010 年度 10 月時点)

（万人）

年代	男子	女子
0	561	534
10	612	583
20	722	689
30	910	885
40	841	830
50	809	818
60 超	1,746	2,196

平均年間消費額を一日当たりの購入回数と日数で割ることで算出される。一回当たりの購入金額は 1,183（円）となる。

情報料金は、一回当たりの購入金額の 0.1%と設定する。一情報料を 1.30（円）と設定し、小売店の POS システム導入割合を 90%と仮定すると、市場規模は、121,500（百万円）と推計される。約 1,210 億円規模の市場があると推定される。

(6) サービス分野

(a)　情報端末におけるコンテンツアクセス集計サービス

①　サービスの背景

これまでメディアの中心は、テレビ、新聞、雑誌が主なものであった。これらのメディアにおいても、視聴率や販売部数などを集計することにより、ある程度の精度でコンテンツへのアクセスを把握することができ、広告料などに反映されてきた。しかしながら、これらメディアにおけるコンテンツへのアクセス状況は、複数の人が同じ番組を見ている、同じ雑誌や新聞を回し読みしているなどの状況を正確に分離することが難しいという問題があった。

近年、iPhone、iPad に代表されるポータブルな情報端末の普及により、動画、雑誌などのデジタルコンテンツへのアクセス環境が向上するとともに、これらの端末は基本的には一人で利用するものであることから、既存メディアにない精度の高いコンテンツアクセス状況の把握が可能となりつつある。

② サービス内容

iPhone、iPad など個人が所有する情報端末を通して、雑誌や動画コンテンツに関する視聴情報を収集して、コンテンツ作成会社等に販売し、コンテンツ作成会社はこれを分析することで事業戦略やコンテンツ作成のための基礎データとして用いる。

図 4-44 情報端末におけるコンテンツアクセス集計サービス（フロー図）

③ 匿名化により解決する問題

ポータブルな情報端末は、上述の通り、個人での利用がほぼ前提となる。したがって、「どのコンテンツ」に「誰が」アクセスしたかが容易に収集できる。これらのリンクが判明すると、「誰が」「どのようなものに」興味があるかまで判明する。この情報を基にダイレクトメール等によるマーケティングを行うことも可能であるが、一方で、情報提供者である個人はダイレクトメールなどを好まない傾向があり、ダイレクトメールが増大すると情報提供者がサービスに参加しなくなる可能性が高まる。

したがって、匿名化により、「誰が」と「どのコンテンツ」というリンクを切り離すことが、本サービスの成立条件の一つとなると考えられる。

④　市場規模

本サービスで想定するポータブルな情報端末として、携帯電話、ネットブック、ブロードバンドネットワークに接続した PC（以下、ブロードバンド）とする。

携帯電話の契約数[82]、ネットブック（iPad）の販売台数[83]、ブロードバンド契約数[84]から、それぞれにおいて本サービスに協力するユーザ数を設定し、市場規模を求める。

表 4-52　携帯電話契約数

2010 年 11 月末

純増数	累計
497,700	116,399,500

表 4-53　iPad 販売台数各国比較

		Est. iPad Shipments (000s)			
Country	Launch Date	Q3/F10	Q4/F10	Q1/F11	CY10
US	3-Apr-10	1,855	1,094	1,701	4,651
Australia	28-May-10	37	58	81	176
Canada	28-May-10	58	91	128	277
France	28-May-10	171	270	364	805
Germany	28-May-10	66	105	131	302
Italy	28-May-10	46	73	91	211
Japan	28-May-10	101	159	215	476
Spain	28-May-10	27	43	54	124
Switzerland	28-May-10	13	20	25	59
UK	28-May-10	124	196	265	585
Austria	Jul-10		19	24	44
Belgium	Jul-10		16	20	36
Hong Kong	Jul-10		32	40	73
Ireland	Jul-10		13	16	29
Luxembourg	Jul-10		3	4	7
Mexico	Jul-10		11	14	25
Netherlands	Jul-10		10	12	22
New Zealand	Jul-10		19	24	44
Singapore	Jul-10		16	20	36
Other Countries	N/A			150	150
Total iPad Shipments		**2,500**	**2,250**	**3,381**	**8,130**

Source: RBC Capital Markets

[82] 社団法人　電気通信事業者協会　携帯電話契約台数
http://www.tca.or.jp/database/2010/11/

[83] RBC Capital Markets
http://blog.sohaya.com/2010/05/21/apples-ipad-believed-to-be-outselling-macs-in-the-us/

[84] 総務省　ブロードバンドサービスの契約数等（平成 20 年 12 月末）
http://www.soumu.go.jp/menu_news/s-news/090318_1.html

表 4-54　ブロードバンドサービス契約件数

	ブロードバンドサービス合計	FTTH	DSL	CATV	FWA
平成 20 年 12 月末	30,107,327 (100%)※2	14,417,207 (48%)	11,594,082 (39%)	4,083,072 (14%)	12,966 (0.04%)
＜参考＞同年 9 月末	29,755,467※3 (100%)	13,756,294 (46%)	11,966,838 (40%)	4,019,497 (14%)	12,838 (0.04%)
差（純増数）	351,860	660,913	▲372,756	63,575	128

「表 4-55　シナリオ別ユーザ数」のように、携帯電話、ネットブック、PC（ブロードバンド利用者数を代用）毎の契約数、販売台数、利用者数を用いて、各シナリオにおいて、コンテンツ追跡サービスに協力するユーザ割合を設定する。

表 4-55　シナリオ別ユーザ数

単位（千）

		加入割合			ユーザ数（重複あり）		
		悲観	中立	楽観	悲観	中立	楽観
携帯電話数	116,400	0.3%	0.5%	1.0%	349	582	1,164
ネットブック(ipad)	476	1.0%	1.5%	2.0%	5	7	10
ブロードバンド	60,215	0.5%	1.0%	1.5%	301	602	903
合　計					**655**	**1,191**	**2,077**

月額情報利用価値を 100 円と想定すると（カルテ情報と同様に設定）、年間で 1,200 円になり、それを中立シナリオのユーザ数に乗算すると、約 14 億円程度になると想定される。

4.5.5 まとめ

匿名情報を利活用するサービスを洗い出し、各サービスの市場規模を合算して市場規模を算出した。特に有望と考えられるのは、金融分野と小売分野である（図 4-35 参照）。また、特に有望と考えられる個別サービスについて詳細化を行った。

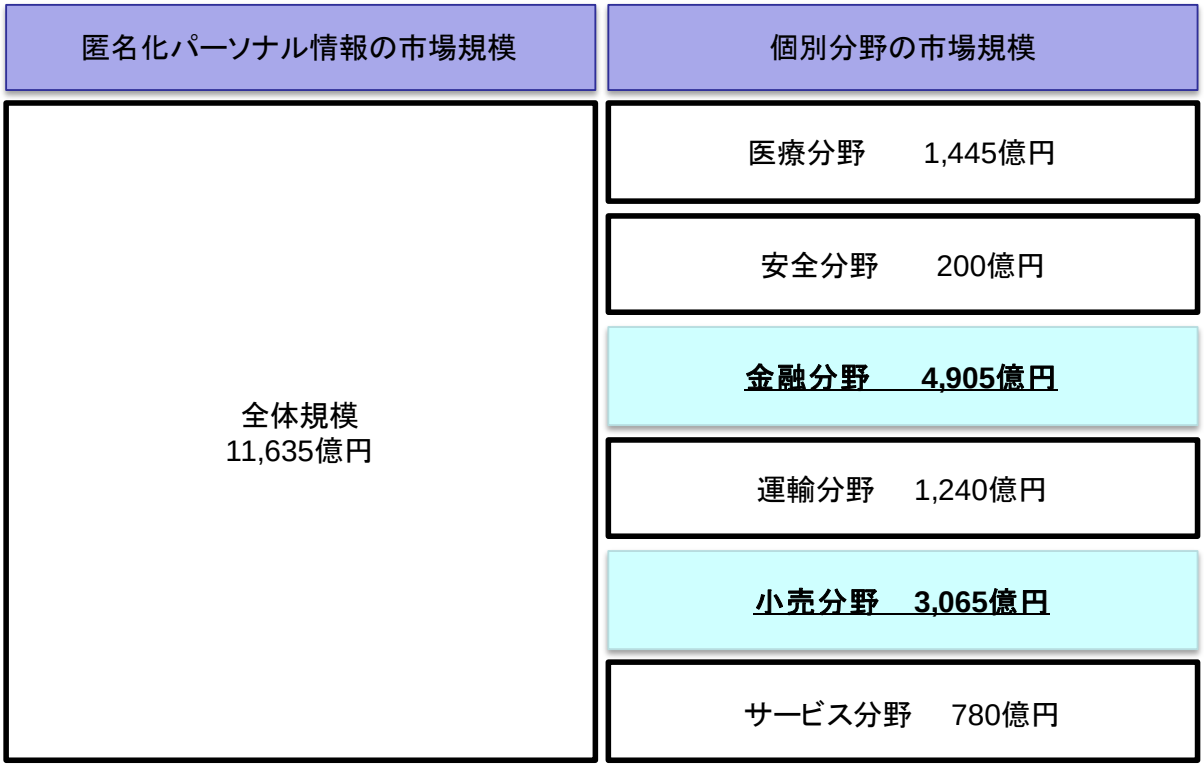

図 4-45　匿名情報の市場規模（推計：概算）

4.6 匿名情報利活用サービスに即した安全性およびトラストレベルの検討

4.6.1 検討方法

(1) 調査の目的

パーソナル情報の流通、二次利用の促進を考えた場合、パーソナル情報を提供する側からみると、提供した情報から自身が特定され、不利益を被ったり、プライバシーの侵害を受けたりすることに危惧を感じると考えられる。他方、パーソナル情報の収集を行う企業等の事業者や、これを二次利用する利用者の視点に立った場合、パーソナル情報を提供する側からの信頼を得られないのであれば、そもそものパーソナル情報の収集が立ち行かず、匿名情報を用いてのサービスの事業自体が成り立たない。

これらの問題を解決する一つの方策として、パーソナル情報を取扱う事業者や利用者に対する信頼性（トラスト）を公平に評価するとともに、パーソナル情報の性質によって求められる安全性を評価し事業者や利用者に提供するような、信頼のおける第三者が実施する匿名情報の認証スキームを構築するアプローチが考えられる。

このような匿名情報の認証スキームを考える場合、事業者や利用者のトラストをどのように評価するか、また、匿名情報に求められる安全性要件とは何か、など、様々な問題が存在する。

そこで、本調査では匿名情報の認証スキームに関して、情報収集者および情報利用者に関するトラストと匿名情報の安全性要件について検討を行う。そして、医療、統計、金融等の分野におけるケーススタディを行うとともに、有識者にヒアリングを行い、匿名情報の認証スキームの構築に向けて課題を抽出・整理することを目的とする。

(2) 調査方法

本パートの調査方法を図 4-46 に示す。

本調査では、情報収集者および情報利用者に求められるトラストレベルについて、汎用的な視点からその設計内容を検討する。また、パーソナル情報の性質に基づき、異なると考えられる匿名化の安全性要件について検討し、トラストレベルと安全性レベルの関係性について議論する。これらの結果を基に医療、統計、金融、小売、運輸等の各分野から一つ、匿名情報を利用するビジネスモデルを想定し、ケーススタディを実施する。また、検討経過ならびにケーススタディの結果をもって有識者にヒアリングを行う。最後に、ケーススタディならびに有識者ヒアリングの結果を受けて、匿名情報の認証スキームに関して抽出された課題を整理する。

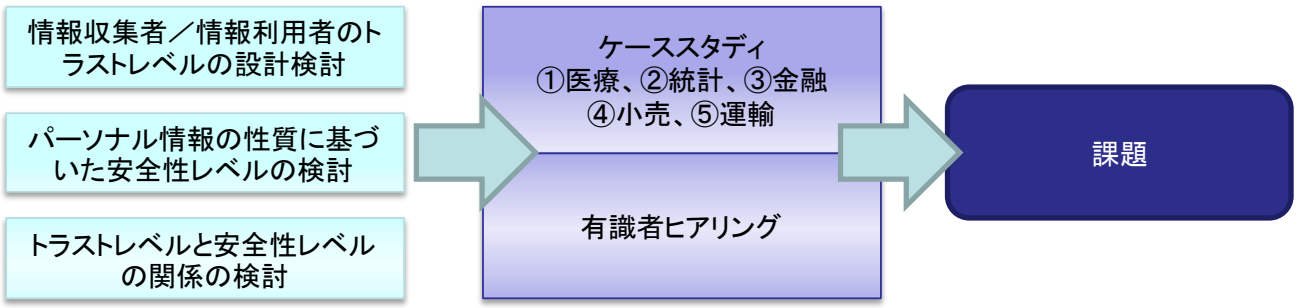

図 4-46　検討方法のフロー図

(3) 検討の前提

本調査の検討は、「パーソナル情報の利用ガイドライン（案）<利用の在り方に関する提言>」[85]に従い実施することとする。

(a) パーソナル情報の二次利用を考えた場合の基本的なプレイヤー

パーソナル情報の流通を踏まえた場合の基本的なプレイヤーを図 4-47 に示す。

情報提供者は情報収集者に自身のパーソナル情報を提供する。情報収集者は、事前に情報提供者に対して、「明示ルール」を提示した上で、複数の情報提供者からパーソナル情報を収集する。収集したパーソナル情報は、情報収集者が「加工ルール」に基づき、匿名化

[85] 情報大航海プロジェクト パーソナル情報検討チーム、“パーソナル情報の利用ガイドライン（案）<利用の在り方に関する提言>”、平成 22 年 3 月
http://www.meti.go.jp/policy/it_policy/daikoukai/igvp/index/h22_report/sub/05.pdf

等の加工を行う。情報利用者と情報収集者は、情報収集者が提供する匿名情報の利用に関する取り決めである「利用ルール」について合意を行い、情報利用者は情報提供者から匿名情報を購入する等により提供を受け、「利用ルール」に基づき利用する。

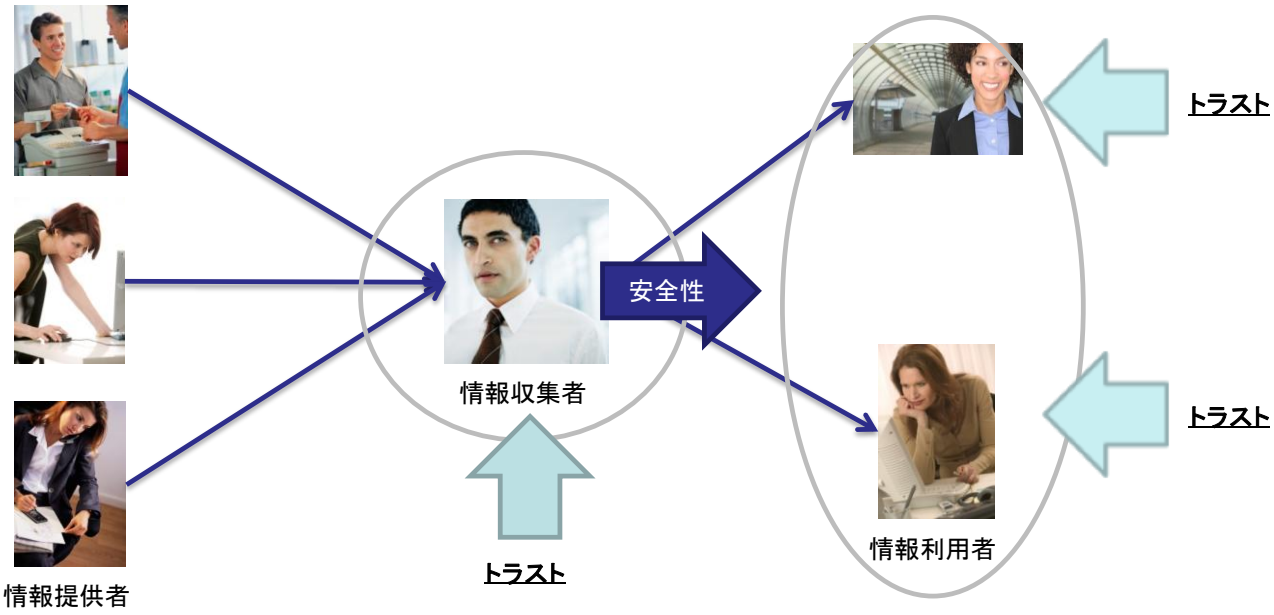

図 4-47　パーソナル情報の二次利用を考えた場合の基本的なプレイヤー

(b)　加工処理に用いる集合匿名化について

情報収集者が情報利用者にパーソナル情報を渡す際には、集合匿名化（以下、匿名化）を用いることで、個々の情報提供者の特定が困難になるようにすることを前提とする。匿名化は、個々の情報提供者のパーソナル情報を集積した上で、指定したいくつかの準識別子において、少なくともｋ個以上のレコードが同じ値になるように操作する。値の操作方法として、あいまい化、切り落としなどの方法を用いる。情報収集者は、加工ルールに基づき、パーソナル情報のデータセットに対して匿名化処理を行う。

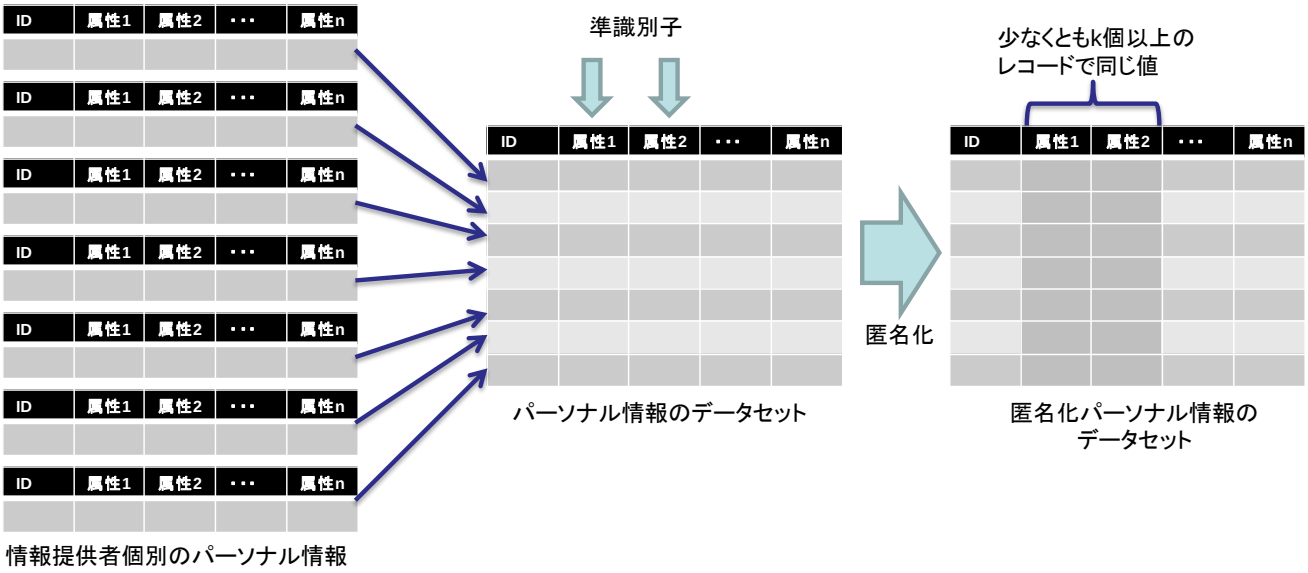

図 4-48　集合匿名化のフロー図

(c)　トラストと安全性について

上述図 4-47 に示すプレイヤーを想定する場合、情報提供者は信頼のおけない情報収集者よりも信頼のおける情報収集者に対しては比較的安心して、自身のパーソナル情報を提供できるだろう。一方、情報収集者は、信頼のおけない情報利用者に対してよりも信頼のおける情報利用者に対しての方が、比較的安心して自身が収集したパーソナル情報を提供することができるだろう。したがって、本報告書では、「情報収集者または情報利用者の信頼性」をトラストと考える。

一方で、情報提供者と情報収集者、および、情報収集者と情報利用者の間で信頼性が成り立っていても、匿名化処理等を行った匿名情報から情報提供者個人が特定され得る場合、内部犯行者が利用ルールに基づかない匿名情報の利用や個人の特定、情報利用者の倒産等による匿名情報の流出による、不特定の第三者の利用や個人の特定等が想定される。したがって、本報告書では「匿名情報から個人を特定することの困難さ」を安全性と考える。

4.6.2 トラストレベルについて

情報収集者のトラストを考える場合、不特定多数の情報提供者からみた個々の情報収集者に関する信頼性は情報提供者毎に異なり、また、情報提供者が情報収集者を知らない場合、情報収集者に対する信頼性は低くなる傾向があるだろう。同様に、匿名情報の販売等を考える場合、ある情報収集者は、既に取引等をよく行っており相互信頼が構築されている情報利用者だけでなく、不特定多数の情報利用者との間で利用ルールの合意を行い、匿名情報の提供や販売を行うことが想定されるため、匿名情報の利用を希望する未知の情報利用者に関する情報収集者の信頼性は低くなると想定される。

そこで、信頼のおける外部の評価者が情報収集者または情報利用者のトラストを評価し、評価結果を公表または個別に提供することができれば、情報利用者が知らない情報収集者にも安心して自身のパーソナル情報を提供することが可能となり、同様に、情報収集者が知らない情報利用

者に対しても安心して匿名情報を提供・販売することができるだろう。

このような信頼のおける外部の評価者を想定する場合、評価者は個別の情報収集者または情報利用者を公平に評価することが求められる。この場合の公平とは、評価者の恣意性が個々の被評価者の評価結果に反映されることがなく客観性を有しており、同じような被評価者に対しては同様の評価結果が得られることである。もし、評価者が、同じような被評価者に対して異なる評価結果を出すとすると、これまでの評価結果や評価者自体に対する信頼性が揺らぎ、ひいてはパーソナル情報の流通自体を阻害するか、もしくは、無秩序な流通が行われるようになるだろう。

評価者が行う評価に対する信頼性を保持するための一つの方法として、決められた手順を策定し､その手順にしたがって評価を行う方法が考えられる｡評価手順が決められているのであれば、異なる二つの評価者で､ほぼ同じ特性を有している場合は､同様の結果が得られるだろう｡もし、その評価方法も公開するのであれば、評価者が出した評価結果に対して、評価者でない者（情報提供者、情報収集者、情報利用者、もしくはそれ以外のものでもよい）が、被評価者に関する情報を基に、公開されている評価方法に基づき検証を行うことができるため、望ましいと考えられる。

さて、情報収集者および情報利用者に関するトラストの評価方法にはさまざまな方法が考えられる。この評価方法は匿名情報の流通を支える基盤となる。したがって、被評価者に対しては、匿名情報の不正な利用、流通を行うようなリスクが低いほど、高い評価結果を得られるような評価手順が望ましいだろう。

以降では、上述図 4-47 に示したプレイヤーを基に、そのリスク分析に基づくトラストの評価方法の例を示し、この例に基づいて被評価者のトラストレベルを決定する方法を示す。

(1) リスク分析に基づくトラストの評価方法の例

パーソナル情報の適切な流通は、以下の手順で行われるものとする。

パーソナル情報の適切な流通に関する手順

1. 情報収集者は、情報利用者に対して、収集するパーソナル情報の明示ルールを示す。
2. 情報提供者は、提示された明示ルールを読んで、自身のパーソナル情報の提供に関する判断を行う。
3. 情報収集者は、複数の情報提供者から収集した情報を集約して保管する。
4. パーソナル情報の利用を望む情報利用者と情報提供者は､その利用方法に関する利用ルール（契約）を締結する。
5. 情報収集者は、情報利用者が求めるパーソナル情報のデータセットに対して、加工ルールに基づき、匿名化処理を施し、情報利用者に渡す。
6. 情報利用者は､情報収集者から提供された匿名情報を､利用ルールに基づき、利用する。

図 4-49　パーソナル情報の適切な流通に関する手順

このモデルに基づく場合、情報収集者に起因するものとして、情報提供者に提示した明示ルールから逸脱して利用ルールに合意しない第三者へ、収集したパーソナル情報を流通させたり、加工ルールに従わないでパーソナル情報の匿名化処理を行ったりするなどのリスクが考えられる。また、情報利用者に起因するものとして、合意した利用ルールに従わないで利用を行うケースや、利用ルールに記載されている範囲を逸脱して第三者に匿名情報を渡すなどのリスクが考えられる（図 4-50 参照）。

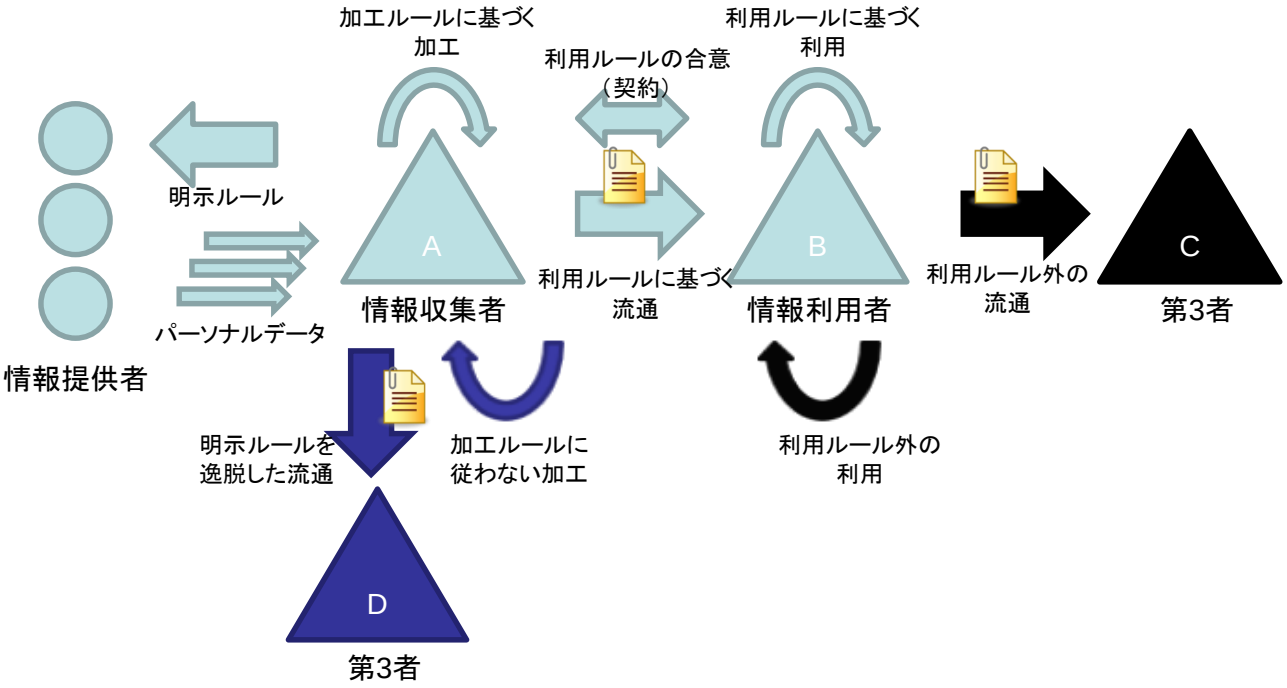

図 4-50　パーソナル情報の流通におけるリスク

これらのリスクについて、細分化し、それぞれ想定される影響と原因を取りまとめたものを、表 4-56、表 4-57 に示す。

表 4-56　情報収集者に起因するリスクの詳細化

大項目	中項目	小項目（具体的事例）	想定される影響	原因
明示ルールを逸脱した流通	利用ルールの合意を伴わない流通	■ 契約等行わずに匿名情報を第三者（情報利用者）に渡す	■ 第三者が、個人の特定、目的外利用を行う ■ 当該個人にダイレクトメール等が送付される ■ 情報提供者の情報収集者に対する信頼性が低下する	■ 情報収集者に、不適切な資本関係者／取引関係者が存在する
		■ 情報収集者に属する従業員が、故意／過失により、第三者に匿名情報を渡す	■ 第三者が、個人の特定、目的外利用を行う ■ 当該個人にダイレクトメール等が送付される ■ 情報提供者の情報収集者に対する信頼性が低下する	■ 情報セキュリティ対策、管理体制が不十分である ■ 社員教育、社員環境、雇用条件が不十分である
加工ルールに基づかない加工	安全性レベルの低い匿名化を行う	■ 適切でない加工ルールを利用し続ける	■ 情報利用者が、個人の特定、目的外利用を行う ■ 当該個人にダイレクトメール等が送付される ■ 情報提供者の情報収集者に対する信頼性が低下する	■ 加工ルールの更新コストが、情報収集者にとって過大である ■ システムの更新のコストが、情報収集者にとって過大である
		■ 従業員が、故意／過失により、加工ルールに従わない	■ 情報利用者が、個人の特定、目的外利用を行う ■ 当該個人にダイレクトメール等が送付される ■ 情報提供者の情報収集者に対する信頼性が低下する	■ 社員教育、社員環境、雇用条件が不十分である ■ 加工ルールを明文化していない ■ 加工ルールを定めていない ■ 匿名情報作成に関するチェック体制がない
	匿名化を行わない	■ 加工ルールを規定していない	■ 情報利用者が、個人の特定、目的外利用を行う ■ 当該個人にダイレクトメール等が送付される ■ 情報提供者の情報収集者に対する信頼性が低下する	■ 加工ルールの策定コストが、情報収集者にとって過大である ■ システムの構築コストが、情報収集者にとって過大である
		■ 従業員が、過失により加工ルールに従わない	■ 情報利用者が、個人の特定、目的外利用を行う ■ 当該個人にダイレクトメール等が送付される ■ 情報提供者の情報収集者に対する信頼性が低下する	■ 社員教育、社員環境、雇用条件が不十分である ■ 加工ルールを明文化していない ■ 加工ルールを定めていない ■ 匿名情報作成に関するチェック体制がない

表 4-57　情報利用者に起因するリスクの詳細化

大項目	中項目	小項目（具体的事例）	想定される影響	原因
利用ルール外の利用	個人の特定	■情報提供者が、匿名情報から個人を特定し、当該個人のプライバシー情報を知る	■当該個人にダイレクトメール等が送付される ■情報提供者の情報収集者に対する信頼性が低下する	■加工ルールが適切でない ■技術の進歩等により適切でなくなった加工ルールで匿名化されたデータであった ■情報利用者が特定個人に関するサイド情報を有している
		■情報提供者内の従業員が、匿名情報から個人を特定し、当該個人のプライバシー情報を得る	■従業員が、当該個人のプライバシーを公表する ■従業員が、当該個人のプライバシー情報を基に脅迫等、犯罪に利用する	■情報セキュリティ対策、管理体制が不十分である ■社員教育、社員環境、雇用条件が不十分である
	目的外利用	■匿名情報を契約範囲外の目的に利用し、情報提供者が新たな事業等を行う	■情報利用者が、情報収集者が想定しない利益を得る ■情報提供者の情報収集者に対する信頼性が低下する	■情報利用者の財務基盤が健全でない
		■情報提供者内の従業員が、自身の目的のために利用する	■当該従業員が犯罪等に利用する	■情報セキュリティ対策、管理体制が不十分である ■社員教育、社員環境、雇用条件が不十分である
利用ルール外の流通	故意の流失	■情報提供者が、第三者に匿名情報を渡す	■第三者が、個人の特定、目的外利用を行う ■当該個人にダイレクトメール等が送付される ■情報提供者の情報収集者に対する信頼性が低下する	■情報利用者に、不適切な資本関係者／取引関係者が存在する
		■情報提供者内の従業員が、第三者に匿名情報を渡す	■第三者が、個人の特定、目的外利用を行う ■当該個人にダイレクトメール等が送付される ■情報提供者の情報収集者に対する信頼性が低下する	■情報セキュリティ対策、管理体制が不十分である ■社員教育、社員環境、雇用条件が不十分である
	意図しない流出	■匿名情報を管理する情報システムが攻撃によりハッキングされ、第三者に匿名情報が渡る	■第三者が、個人の特定、目的外利用を行う ■当該個人にダイレクトメール等が送付される ■情報提供者の情報収集者に対する信頼性が低下する	■情報セキュリティ対策、管理体制が不十分である

大項目	中項目	小項目（具体的事例）	想定される影響	原因
		■情報提供者内の従業員の過失により、匿名情報が流出し、第三者に匿名情報が渡る	■第三者が、個人の特定、目的外利用を行う ■当該個人にダイレクトメール等が送付される ■情報提供者の情報収集者に対する信頼性が低下する	■情報セキュリティ対策、管理体制が不十分である ■社員教育、社員環境、雇用条件が不十分である
		■情報提供者が破綻し、匿名情報が流出する	■第三者が、個人の特定、目的外利用を行う ■当該個人にダイレクトメール等が送付される	■情報利用者の事業の永続性がない ■情報利用者の財務基盤が健全でない

これらのリスク分析の詳細化の結果から、個別のリスクの原因に関して、その性質毎に近しいと考えられるものを取り纏めたものを図 4-51 に示す。

内部の管理体制や社員教育にリスクの原因があるような場合には、内部の管理プロセスをPマーク[86]やISMSの取得状況によりチェックすることができる。システム投資等に係る原因については、システム投資に耐えうる資本や将来的な事業計画などによりチェックできるだろう。加工ルールの適切性に関する原因を有しているかどうかをチェックするには、明文化された加工ルールがあること、また、その加工ルールを適切に更新している等のPDCAサイクルの運用状況、実施状況、ならびに加工ルールの内容を基に判断する。情報収集者ならびに情報利用者に不適切な資本関係者や取引関係者がいないかなどは、資本関係者や取引先のリストを被評価者から提示を受けることで、確認することができる。

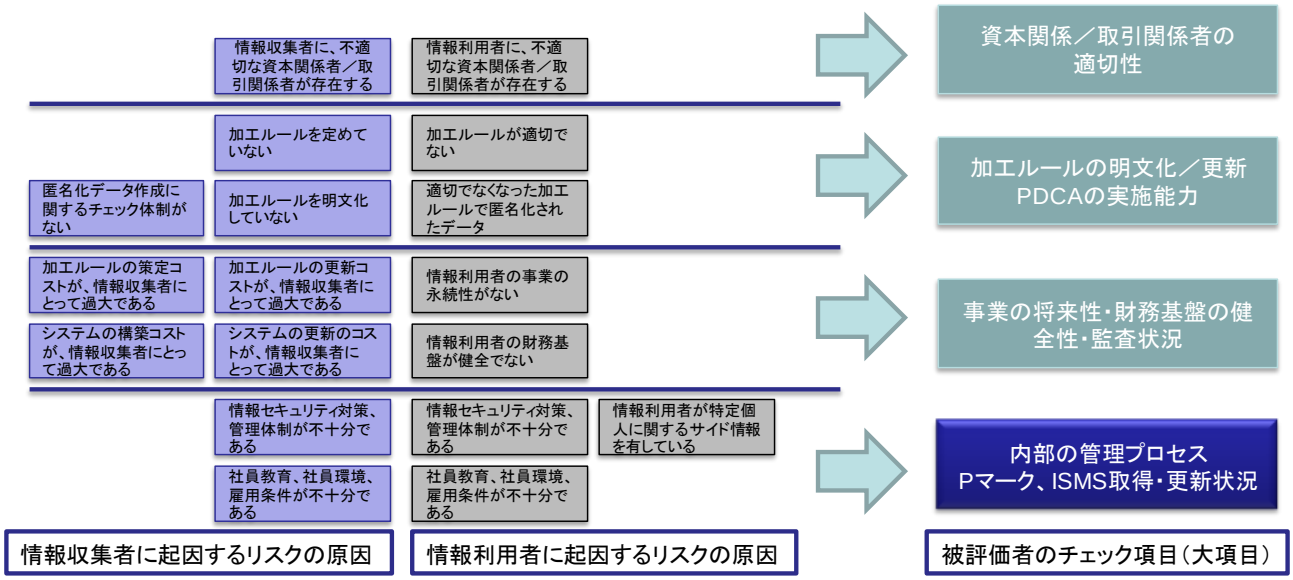

図 4-51　トラストのチェック項目（案）

(2) トラストレベルの評価について

上述(1)に示したトラストのチェック項目を基に、トラストレベルの算出手順を考える。トラストレベルの算出方法については、様々な方向性が考えられる。しかし、情報管理に関する内部プロセスが構築されており、適切に運用されていることは、パーソナル情報を取扱う上で必須の項目であり、もしPマークやISMS等の認定を受けていないのであれば機微な情報を含み得るパーソナル情報または匿名情報が適切に管理されていない可能性を有すると考えられる。そこで、本報告書では、この項目を必須項目と捉え、もしPマークやISMS等を取得していない場合には評価の対象外とし、その他の「事業の将来性・財務基盤の健全性・

[86] プライバシーマーク制度とは、『プライバシーマーク制度は、日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度』（出典: プライバシーマーク制度 - 概要と目的 http://privacymark.jp/privacy_mark/about/outline_and_purpose.html）

監査状況」、「加工ルールの明文化／更新等 PDCA の実施能力」、および、「資本関係／取引関係者の適切性」については加点評価として、各項目につき 1 ～10 の点数で評価を行い、それを積算することでトラストレベルを評価する方法を提示する（図 4-52 参照）。なお、この評価方法を用いて情報利用者を評価する場合には、「加工ルールの明文化／更新・PDCA 実施能力」については除外して考えるものとする。

分類	大項目	チェック項目	評価内容	評価値
必須項目	内部の管理プロセス	Pマーク、ISMS取得・更新状況	当該資格を保有	○／×
評価項目	事業の将来性・財務基盤の健全性・監査状況	財務の健全性	財務諸表の監査	1～10
		システム投資に関する財務能力	情報投資計画	1～10
		内部統制等に関わる財務体制	内部管理支出計画	1～10
		事業の将来性・永続性	事業計画	1～10
		対外的評価	外部の格付け総合評価	1～10
	加工ルールの明文化/更新・PDCA実施能力	加工ルールの明文化	加工ルールの確認	1～10
		加工ルールに関するPDCA体制	PDCA体制の確認	1～10
		匿名化データの検査体制	検査体制の確認	1～10
	資本関係・取引関係の適切性	資本関係者の妥当性	主要な資本関係者の確認	1～10
		取引関係者の妥当性	主要取引先確認	1～10

×の場合は、認定対象から除外

加点評価

	トラストレベル
90以上	AAA
80～89	AA
70～79	A
60～69	BBB
50～59	BB
40～49	B
30～39	CCC
20～29	CC
19以下	C

図 4-52　トラストレベルの評価方法の例

ここで示した方法は一例である。更なる検討や目的の明確化、他の状況を鑑み、各評価項目の適切な重みづけや、合計得点に関するトラストレベルの割り付けなど、適宜検討する必要がある。

4.6.3 パーソナル情報の安全性について

(1) パーソナル情報の性質と求められる安全性について

情報収集者が収集するパーソナル情報は、収集する情報の属性毎に扱いが異なると考えられる。文献 85 では、定義の観点および一意性の観点から、基本情報、変化情報①、変化情報②、行動情報の四つに分類している。また、医療データや犯罪歴など、そもそもその情報自体がプライバシー上、機微な情報として取扱うものがある（センシティブデータ）。そこで、まずセンシティブデータか否かで分類することを考える。センシティブデータを含むようなパーソナル情報のデータセットは、それ自体で高い安全性レベルが求められる。

次に、パーソナル情報のデータセットに個人特定が行われやすいデータレコードが存在するか否か、個人が特定された場合に想定被害が大きいか否かで分類することを考える。個人特定の行い易さは情報収集者がパーソナル情報を収集する母集団とサンプリング結果により異なり、あるパーソナル情報のデータセットでは、他のどのレコードとも共通点が少ないようなレコードは個人の特定が行い易いと考えられる。想定被害については、どのような属性をもつ情報を収集しているかによって異なるため、個別に判断する必要がある。

個人特定が行い易いデータレコードが存在し、かつ、個人特定が行われた場合に想定被害が大きいと考えられる場合には、センシティブデータと同じ扱いをする方が望ましいだろう。また、個人特定が行い易いデータレコードが存在するが、想定被害が小さいと想定される（例えば文献 85 に示される基本情報②）場合には、センシティブデータほど厳重な安全性は必要ないだろうが、個人特定されるリスクが存在するため、適切なレベルの匿名化処理が必要であると考えられる。他方、個人特定しやすいデータが含まれないデータセットにおいて、想定被害が小さい場合にはそれほど過大な匿名化を行う必要はないだろう。また、個人特定しやすいデータレコードが含まれないデータセットにおいて、想定被害が大きいと考えられる場合には、個人特定が比較的困難であると考えられるが、万が一特定された場合の被害が想定されるため適切なレベルの匿名化や管理が必要だろう。

以上取りまとめると、図 4-53 のようになる。本報告書では安全性レベルをⅠ～Ⅲの三段階に分けることとした。

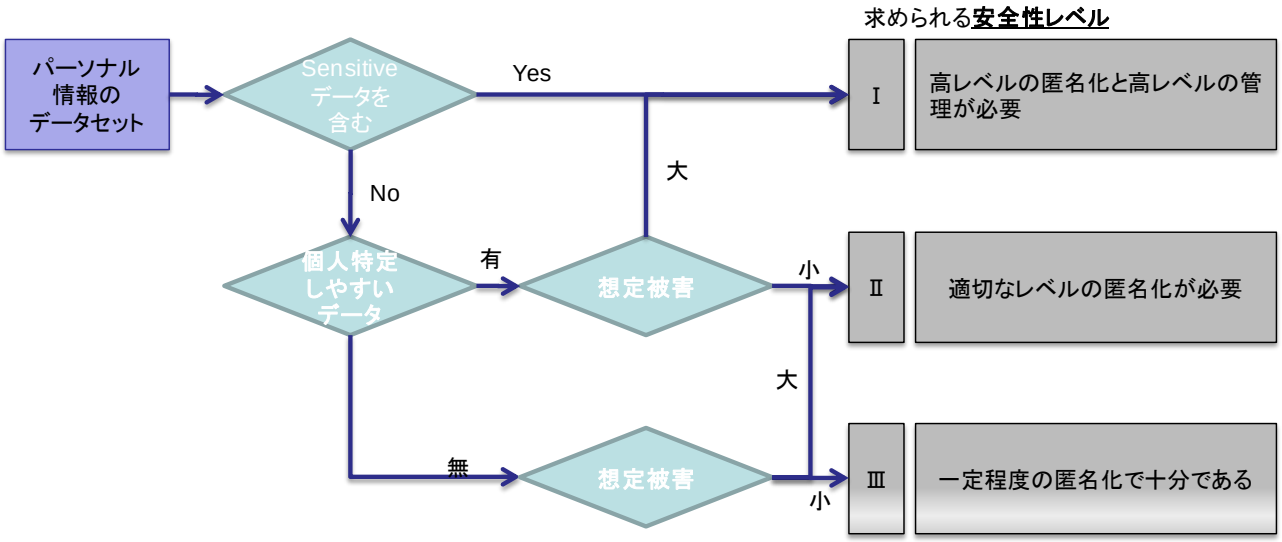

図 4-53　パーソナル情報の性質毎に求められる安全性レベル

(2) トラストレベルと安全性レベルの関係について

上述(1)に示したパーソナル情報の安全性レベルにおいて、医療情報などのセンシティブデータが含まれるパーソナル情報のデータセットや、個人の特定が行い易いパーソナル情報のレコードが含まれており個人特定時の影響が大きいと想定されるパーソナル情報のデータセットの場合、高いレベルの匿名化だけでなく、その管理においても厳重さが求められるため、パーソナル情報を扱う情報収集者および情報利用者においては高いトラストレベルが必要とされる。

この点をどのように実装するかについては、いろいろな考え方があるが、本報告書では最もシンプルな例を、表 4-58 に示す。この例では、高いトラストレベル（AAA、AA、A）を有する情報収集者および情報利用者は、必要とされる安全性が高い（安全性レベルⅠ）のパーソナル情報を取扱うことができるが、中程度のトラストレベル（BBB、BB、B）では個別に扱えるか否かの判断を行うようになっている。また、トラストレベルの低い（CCC、CC、

C）情報収集者および情報利用者においては、安全性レベルが高い（安全性レベルⅠ）または中程度（安全性レベルⅡ）のパーソナル情報を扱うことはできない。

表 4-58　トラストレベルと安全性レベルの関係（案）

			安全性		
			Ⅰ	Ⅱ	Ⅲ
トラストレベル	A ランク	AAA	○	○	○
		AA	○	○	○
		A	△	○	○
	B ランク	BBB	△	△	○
		BB	×	△	○
		B	×	△	○
	C ランク	CCC	×	×	○
		CC	×	×	△
		C	×	×	△

○：取扱可　△：個別判断が必要　×：取扱不可

4.6.4 ケーススタディ

上述 4.6.2、4.6.3 で検討したトラストレベルと安全性レベルを基にして、医療、統計、金融、小売、運輸の各カテゴリにて、パーソナル情報を利活用する具体的なサービスを想定し、ケーススタディを行う。具体的なケースに基づき、情報収集者および情報利用者に求められるトラストレベル、匿名化手法の安全性を検討する。具体的にケーススタディで取り上げる各分野のサービス内容を表 4-59 に示す。

表 4-59　各ケーススタディで取り上げるサービス内容

	分類	収集する情報	サービス内容	利用者
①	医療	レセプト 電子カルテ	**薬剤マーケティング** 実際の病状と投薬の履歴から、薬の有効性を検証し、マーケティングに利用する	薬剤メーカー
②	統計	アンケート調査の個票セット	**アンケートデータの再利用** 過去に実施したアンケートの個票を再利用し、ニーズに合った独自の分析を行う	アンケート会社
③	金融	保険の加入者に関する情報	**保険商品設計** 複数の生命保険会社が保有するデータを統合し、料金策定のための基礎データやマーケティングとして活用する	保険会社
④	小売	行動履歴	**店舗出店戦略策定** 携帯電話等に付属した GPS により測位される潜在顧客の経路情報から店舗のスクラップアンドビルドを行う	小売 （コンビニ等）
⑤	運輸	行動履歴情報	**配車管理** 携帯電話等に付属した GPS により測位される位置情報を基に、潜在顧客が集中する地域を割り出し、配車等に利用する	タクシー会社

各ケーススタディでは、以下の手順に基づき実施する。

ケーススタディの方法

1. ビジネスモデルの例

パーソナル情報を用いるビジネスモデルについて、パーソナル情報のフローやお金のフローを検討する。また、ビジネスモデルにおいて流通するパーソナル情報の属性について検討を行い、例示する。

2. 情報提供者の個人特定の可能性

検討したビジネスモデルで流通するパーソナル情報の属性について、可能であれば公表されている統計等の情報から、個々の情報提供者が特定される可能性を検討する。適切な統計等の情報がない場合には、定性的な分析により、個々の情報提供者が特定される可能性を検討する。

3. 個人特定時の影響

ビジネスモデル毎に、匿名情報から個々の情報提供者が特定された場合の影響は異なると考えられる。その影響について分析を行う。

4. 情報収集者／情報利用者のトラストレベル

上述 1～3 の分析結果を基に、情報収集者および情報利用者に求められるトラストレベルを、表 4-58 を基に検討する。

5. 匿名情報に求められる安全性レベル

上述 1～3 の分析結果を基に、匿名情報に求められる安全性レベルを表 4-58 を基に検討する。

図 4-54　ケーススススタディの方法

(1) ケーススタディ①：薬剤マーケティング（医療）

(a) ビジネスモデルの例

ここでは、電子カルテやレセプト等の情報を患者のパーソナル情報として集積し、製薬メーカー等がその分析を行うことで、新薬の開発やマーケティングを行い、収益を得るビジネスを考える。

医療機関に代表される情報収集者は、診察を行った患者の情報を電子カルテ等に記載している。また、診療報酬明細書などのレセプトも近年電子化が進んでおり、蓄積されている。これらの情報を情報収集者は収集し、患者毎に成形しなおしパーソナル情報のセットとして蓄積する。さらに情報収集者は、このパーソナル情報に対して匿名化等の加工処理を施し、利用ルールに合意した製薬メーカー等の情報利用者へ販売する。製薬メーカー等の情報利用者は、入手した匿名情報に基づいて分析を行い、新薬開発やマーケティングに用いる。

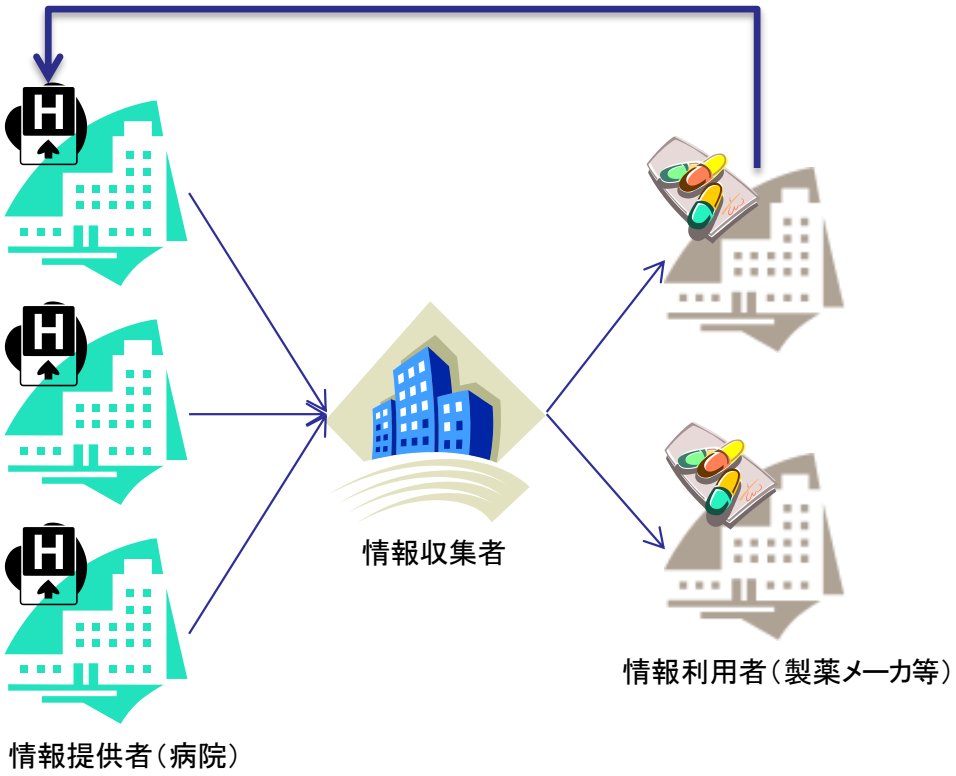

図 4-55　ケーススタディ①：薬剤マーケティングにおけるデータフロー

製薬メーカー等の情報利用者は、新薬の開発や薬のマーケティングに用いるため、情報収集者が再構成するパーソナル情報には、病気やけがの情報（傷病名）、処方した薬の情報、年齢、性別の情報に加えて、薬の効き具合などの所見に係る情報が含まれている必要がある。したがって、収集するパーソナル情報のデータセットは、表 4-60 のようになると考えられる。

表 4-60　ケーススタディ①：薬剤マーケティングのデータセットの構成

ID	診療日	傷病名	所見	投薬	性別	年齢

(b)　情報提供者の個人特定の可能性

情報提供者が特定される可能性は、収集したパーソナル情報のデータセット内の分布において、数の少ない（割合の少ない）特異な情報ほど個人特定に結びつきやすいと考えられる。

このビジネスにおいて、情報収集者が収集して再構成したパーソナル情報（表 4-60 参照）には、傷病名が含まれているとしている。我が国における傷病名の分布は厚生労働省

が発行する医療動態実態調査から知ることができる。ここでは、医療給付実態調査（平成20年度）[87]の「第３表　疾病分類別、診療種類別、制度別、件数、日数（回数)、点数（金額)」から、各傷病の件数が全体件数に占める割合を算出した結果を表 4-61 に示す。医療給付実態調査では、診療月から三ヶ月以内に審査決定された平成 20 年 4 月診療分から平成 21 年 3 月診療分の診療報酬明細書および調剤報酬明細書（以下、“レセプト”という。）を集計対象としている。傷病分類数は 121、総数 534,915,693 件に対して、傷病毎に最低 0 件、最大 64,584,568 件となっていた。

本分析結果では、121 分類中 120 分類が 5%以下であり、高血圧疾患のみ約 12%であり、ほぼ全ての傷病が、発生頻度の非常に少なく、傷病名と病院名、性別、年齢と結びつくことで、個人特定に結びつく可能性があるといえる。

表 4-61　我が国における傷病毎の分布（一部抜粋）

傷病名	件数	割合（%）
重症急性呼吸器症候群[SARS]	45	0.00001%
感染症および寄生虫の続発･後遺症	135,668	0.02536%
知的障害＜精神遅滞＞	302,141	0.05648%
妊娠および胎児発育に関連する障害	359,058	0.06712%
主として性的伝播様式をとる感染症	403,707	0.07547%
精神作用物質使用による精神および行動の障害	478,729	0.08950%
悪性リンパ腫	530,852	0.09924%
自律神経系の障害	621,324	0.11615%
メニエール病	630,894	0.11794%
子宮の悪性新生物	711,921	0.13309%
その他の男性生殖器の疾患	764,228	0.14287%
その他の先天奇形，変形および染色体異常	1,189,063	0.22229%
その他の感染症および寄生虫症	1,207,100	0.22566%
痔核	1,495,890	0.27965%
その他の精神および行動の障害	1,910,951	0.35724%
結腸の悪性新生物	1,959,836	0.36638%
胃の悪性新生物	2,385,407	0.44594%
気分(感情)障害(躁うつ病を含む)	7,879,905	1.47311%
症状，徴候および異常臨床所見・異常検査所見で他に分類されないもの	10,871,929	2.03246%

[87] 厚生労働省、平成２０年度医療給付実態調査
http://www.mhlw.go.jp/bunya/iryouhoken/database/zenpan/iryoukyufu/h20.html

(c) 個人特定時の影響

病名と個人が特定された場合、様々な差別が想定される。例えば、稀な感染症に感染している情報提供者が特定されると、たとえ感染の可能性が低いとしても、感染等を危惧する周囲の人から避けられることが考えられる。その他、悪性新生物（がん）にかかっていることが判明することで、所属する会社から解雇や自主退社に追い込まれる事態も想定される。

(d) 情報収集者／情報利用者のパーソナル情報のトラストレベル

このケーススタディで検討したパーソナル情報のデータセットには、傷病名の属性を含んでいるため、センシティブデータである。したがって、トラストレベルの高い AAA または AA クラスの情報収集者または情報利用者である必要があるだろう。

(e) 収集するパーソナル情報に求められる安全性レベル

このケーススタディで検討したパーソナル情報のデータセットには、傷病名の属性を含んでいるため、センシティブデータである。したがって、求められる安全性は最も高い安全性レベル I が必要であると考えられる。

(f) まとめ

以上、「ケーススタディ①：薬剤マーケティング（医療）」の結果をまとめると、表 4-62 のようになる。

表 4-62 ケーススタディ①：薬剤マーケティング まとめ

1．ビジネスモデルの例	情報収集者は各情報提供者（医療機関等）から電子カルテやレセプト等のパーソナル情報を収集し、蓄積・加工 情報利用者（薬剤メーカー等）は、事業者からデータを購入し、個々の薬剤の販売量や効能などを分析 情報利用者（薬剤メーカー等）は分析結果をもとに、病院等に薬剤のマーケティングを実施
2．情報提供者の個人特定の可能性	発症頻度が低い疾病、死亡率が高い疾病、精神疾患、性病 （厚生労働省　平成 20 年度医療給付実態調査）
3．個人特定時の影響	疾病に関する差別
4．収集者／利用者のトラストレベル	トラストレベル AAA、AA が必要である ※医療情報であり、センシティブデータを扱う
5．匿名化の安全性レベル	安全性レベル I が求められる

(2) ケーススタディ②：アンケート調査結果の再利用（社会調査）

(a) ビジネスモデルの例

Web 等を通して、様々なアンケート調査が実施されている。これらのアンケートは、他のアンケート結果を集計した統計等を参考とすることもあるが、基本的にはアンケート調査を行うたびに設計が行われることが一般的である。アンケート調査を行うには通常、それなりの金額がかかり、中小企業や大学などが単独で行うことは難しい。また、アンケート調査を単独で行えるほどの資金力を有する企業であっても、一回のアンケート調査で行う分析の精度を高めたいというニーズは、潜在的に存在していると考えられる。そこで、アンケート調査会社等の情報収集者が、過去のアンケート調査で回収した個票を表形式に整理した上で、匿名化を行い、企業や大学へ販売するビジネスを考える（図 4-56 参照）。

調査実施事業者である情報収集者は、アンケート回答者である情報提供者にポイントまたは景品等の対価を与える代わりにアンケート調査に協力してもらいアンケートの個票を回収する。情報収集者は、回収したアンケート個票を表形式などに成形し、一つのファイルとして保管する。企業や大学といった情報利用者は、情報収集者が持つ過去のアンケートから、自身のニーズに合うものを選択し、情報収集者に提供の依頼を行う。情報収集者は、情報利用者から指定されたアンケート結果を表形式にして保管したファイルに対し、匿名化等の加工を施し、代金と引き換えに情報利用者に渡す。

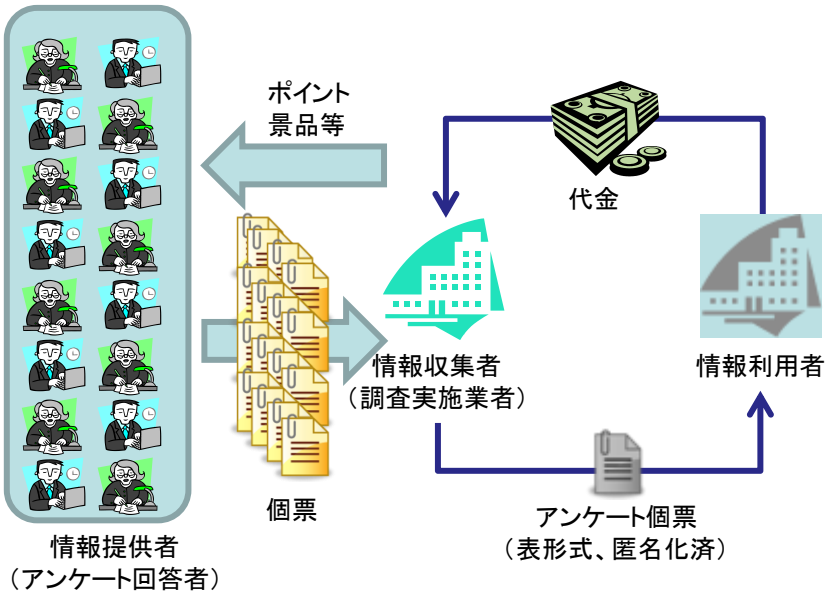

図 4-56 ケーススタディ②：アンケート調査結果の再利用 フロー

通常、アンケート毎に収集するデータの内容は異なる。一般的に、アンケートは、年齢、性別、居住地などの基本属性を問う質問と、アンケートの目的に合わせて設計された質問の回答部分に分けることができるケースが多い。したがって、このモデルでは、アンケート毎に異なるデータセットが作成され、そのデータ形式は図 4-57 のようになる。

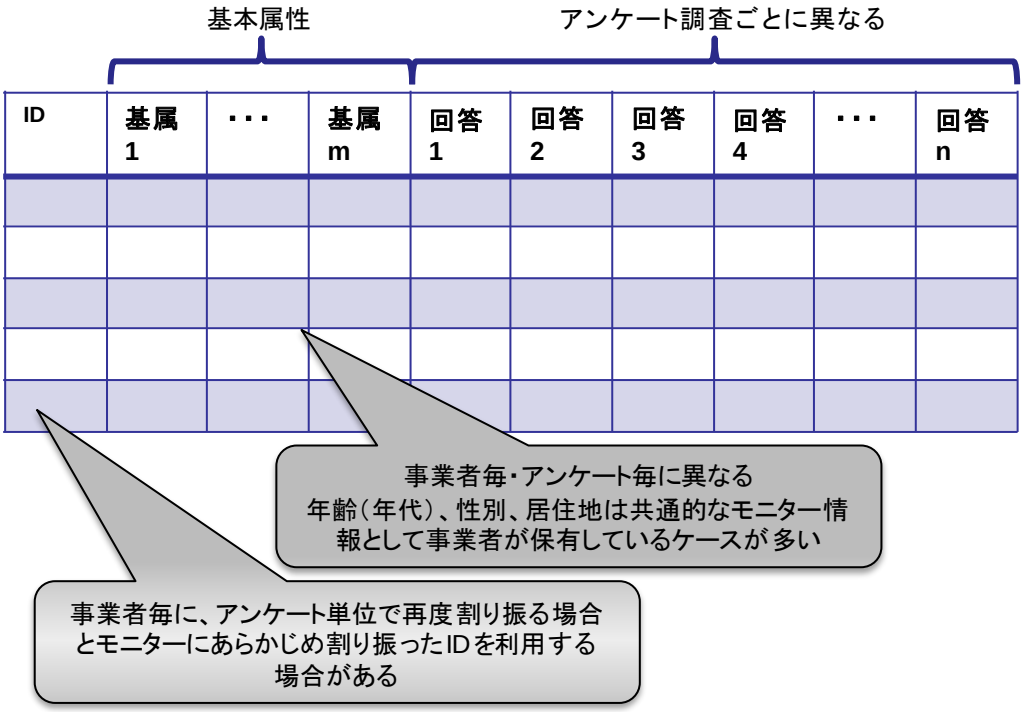

図 4-57　ケーススタディ②：アンケート調査結果の再利用　データセットの形式

(b)　情報提供者の個人特定の可能性

アンケートでは、年齢、性別、居住地などの基本属性に関する質問と、アンケートの目的に合わせて設定した質問の回答部分に分けられるケースが多い（図 4-57 参照）。

アンケート調査において、個人が特定されやすいようなサンプルは、他のどのサンプルとも一致する項目が少ないサンプルであると考えられる。各調査のサンプリングをランダムサンプリングと仮定する場合、基本属性などにおいて発生確率が低いサンプルが、他のどのサンプルとも一致する項目が少ないサンプルとなる可能性が高いと考えられる。例えば、人口の少ない県や市に在住する人が、アンケートに回答した場合には、同じ県や市に在住する人が同じアンケートに回答している可能性は低くなると考えられる。また年齢、性別などとも組み合わせると、同じ県や市に在住していて、同じ性別、同じ年齢（層）に属するサンプルが、同じアンケートで抽出される可能性はさらに低くなるだろう。そこで、年齢、性別、居住地などの基本属性について、日本の人口分布と年齢分布、性別の分布を基に、発生頻度の少ないサンプルが含まれるセグメントについて推計を行うことにより、情報提供者の個人特定の可能性を見積もることとする。

居住地（都道府県レベル、市区レベル）、年齢層（10 歳刻み、0～9、10～19、20～29、30～39、40～49、50～59、60～69、70～79、80～89、90～99、100 以上）、性別（男、女）で構成されるセグメント分けについて考える。各セグメントにおいて、日本の人口に占める割合が少ないセグメントほど、各アンケート調査で抽出されるサンプルとなる可能性が低くなり、個人特定の可能性が高くなると考えられる。総務省統計局が発行する「平

成 20 年度　日本の統計 2010 第 2 章 人口、世帯」[88]の統計をもとに、各セグメントの分布を推計する。推計方法は、日本の人口における年齢層毎の分布を「2-4 年齢各歳別人口」から、10 歳刻みで、男女別の構成比を算出する（年代×性別セグメント）。これを、「2-2 都道府県別人口と人口増減率」、および、「都市別人口（平成 21 年）」の集計値に乗じて、アンケート母集団における居住地、年代、性別の各セグメントの構成比として、推計値とする。

このアンケート母集団における各セグメントの構成比の推計値を基に、人口に占める割合が 0.05%以下、0.01%以下、0.005%以下、0.001%以下、0.0005%以下、0.0001%以下、0.00005%以下、0.00001%以下のセグメントを数え上げた結果を、表 4-63 に示す。この結果をみると、都道府県レベルで集計したデータは 60 歳以上が発生頻度の少ないサンプルとなる可能性がある。また、市区レベルで集計したデータでは、全ての層で発生頻度の少ないサンプルが発生する可能性があるといえる。

表 4-63　居住地×年代×性別のセグメント別の日本の人口に占める割合が少ないセグメントの数

総人口に占める割合	人口（基準値推計）×1000 人	総人口に占める割合以下のセグメント数 都道府県別		総人口に占める割合以下のセグメント数 市区別	
		全ての年代	59 歳以下	全ての年代	59 歳以下
0.05%以下	63.8445	544	141	31639	17176
0.01%以下	12.7689	223	0	26557	13481
0.005%以下	6.38445	183	0	20226	9017
0.001%以下	1.27689	123	0	6403	340
0.0005%以下	0.638445	106	0	4925	65
0.0001%以下	0.127689	35	0	3200	36
0.00005%以下	0.0638445	16	0	2719	36
0.00001%以下	0.0127689	0	0	1324	36

(c)　個人特定時の影響

情報提供者の個人が特定された場合、アンケート毎に設定される設問の回答により、得られる情報が異なるため、基本的には各アンケートの内容により異なると考えられる。「よく見るテレビ」や「好きなスポーツ」などのような、一般的な設問に関する回答結果であれば、さほど問題となる場合は少ないとも考えられるが、個人のプライバシーの観点からは望ましくないと考える場合もあり得る。また、「年収」や「総資産」などの設問がある場合、個人が特定されることにより、その人の年収や総資産が判明することになる。このように、個人特定時の影響は、アンケート調査において設定された設問により異なるため、個別に判断する必要があると考えられる。

[88] 総務省統計局「平成 20 年度　日本の統計 2010 第 2 章 人口、世帯
http://www.stat.go.jp/data/nihon/02.htm

(d)　情報収集者／情報利用者のトラストレベル

個人特定時の影響がアンケート調査毎に異なることから、基本的にはこれに準じて、情報収集者および情報利用者のトラストレベルは異なるといえる。しかしながら、情報収集者は、頻繁に様々なアンケートを実施しているとすると、個人特定時の影響が高いと考えられるアンケートを実施するケースもあり得るだろう。したがって、情報収集者には高いトラストレベル（表 4-58 における AAA、AA、A 相当）が必要であり、情報利用者については、選択されたアンケート毎に個別に判断する必要があるだろう。

(e)　安全性レベルの要件

匿名化の処理に求められる安全性レベルは、個人特定時の影響がアンケートの内容毎に異なることから、個別に判断を行う必要がある。

(f)　まとめ

以上、「ケーススタディ②：アンケート調査結果の再利用（社会調査）」の結果をまとめると、表 4-64 のようになる。

表 4-64　ケーススタディ②：アンケート調査結果の再利用　まとめ

1．ビジネスモデルの例	情報収集者（調査実施業者）は Web アンケート調査等を実施し、個票の収集・集計を行う 情報収集者は、情報利用者が必要とするアンケートについて、個票を取りまとめた表を匿名化して、代金と引き換えにユーザに渡す 情報利用者は、匿名化された表（と調査票）を基に、自由な分析を行う
2．情報提供者の個人特定の可能性	都道府県レベルで集計したデータは 60 歳以上が発生頻度の少ないサンプルとなる可能性がある 市区レベルで集計したデータは、全ての層で発生頻度の少ないサンプルが発生する可能性がある
3．個人特定時の影響	影響の有無はアンケートの実施内容毎に判断する必要がある
4．収集者／利用者のトラストレベル	情報収集者には高いトラストレベル（AAA、AA、A 相当）が必要である 情報利用者のトラストレベルは、アンケート内容毎に判断が必要である
5．匿名化の安全性レベル	アンケート内容毎に判断が必要である

(3) ケーススタディ③：保険商品設計（金融）

(a) ビジネスモデルの例

保険商品は実に多様である。保険商品を購入する人のニーズに応じて、フレキシブルに組み合わせることができる。保険会社では、顧客獲得のために低価格で保証の大きな商品を設計するとともに、適切な利益を上げられるように保険商品設計を行っている。顧客のニーズや状況を適切なタイミングで捉え、保険商品の設計に役立てることは保険会社のニーズとして存在すると考えられる。

ここで、複数の保険会社から個々の顧客に関する情報を収集し、分析を行い、情報を提供した保険会社に対して分析結果を提供するビジネスを考える。

情報収集者である保険会社は、情報提供者である保険商品購入者から、顧客の病歴や年齢、喫煙の有無などのヒアリングを行ったり、場合によっては医師の診断書などを入手するなどして、顧客のニーズとリスク、顧客が希望する支払金額の上限などを基に保険商品の組み合わせを提示したりする。情報提供者である顧客は、提示された選択肢の中から自分の判断により、保険商品の購入を決め、保険に加入する。情報収集者である保険会社はこれまでに集めた個々の情報提供者に関する情報と、選択された保険商品、支払額、支払総額などを逐一記録し、保管する。情報収集者は、この保管している顧客の情報のデータセットを、匿名化等の加工処理により個人の識別が困難なようにして、情報利用者である分析会社に渡す。情報利用者は、匿名化されたデータセットを、複数の保険会社から集め、統合し、全体の動向や傾向などを分析し、レポートとして保険会社にフィードバックするとともに代金を徴収する（図 4-58 参照）。

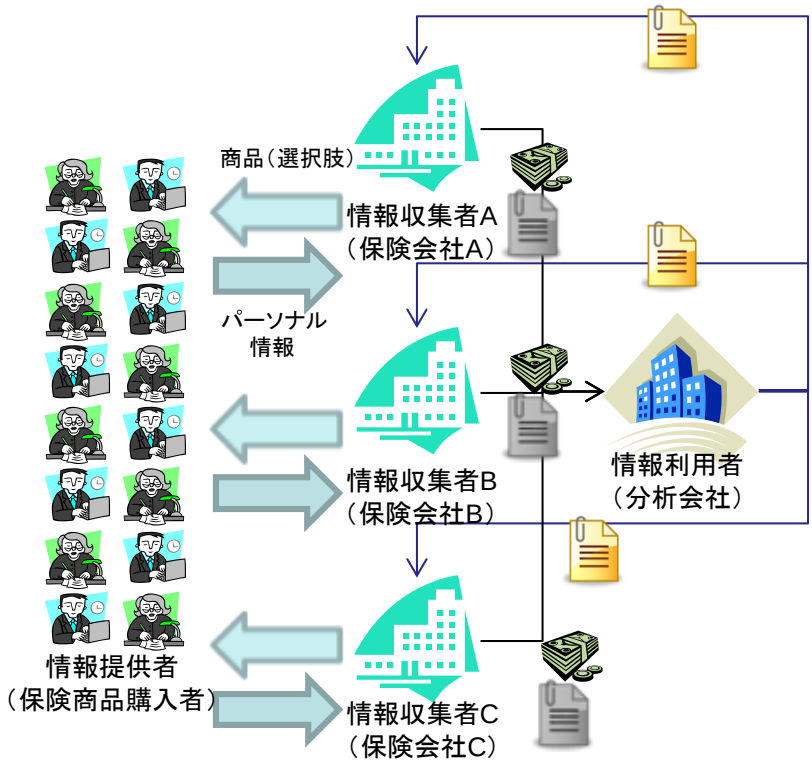

図 4-58 ケーススタディ③：保険商品設計 フロー

情報収集者が収集する情報提供者である保険購入者の情報は、情報収集者毎に異なると考えられる。したがって、情報収集者と情報利用者は、分析に必要となり、かつ異なる情報収集者間でも共通に収集できる情報の属性を取り決める必要がある。例えば、表 4-65 のような属性について、情報収集者から情報利用者に提供することが考えられる。

表 4-65　ケーススタディ③：保険商品設計におけるデータセットの例

ID	年齢	性別	住所	喫煙	病歴	商品	商品説明	オプション	オプション説明	年数	支払額	総額

(b)　情報提供者の個人特定の可能性

上記表 4-65 に示したデータフォーマットを仮定する場合、個人特定の可能性は、年齢、性別、住所の属性が存在するため、ケーススタディ②の場合（上記(2)参照）と同様である。

(c)　個人特定時の影響

上記表 4-65 に示したデータフォーマットには「病歴」が含まれる。病歴はセンシティブデータであり、個人が特定された場合、病歴が判明することで差別等を受ける可能性がある。また、「支払額」が含まれるため高額保険商品を購入していることや、「総額」が含まれるため、資産などの裕福さが推定され得る。これにより、個人が特定された場合、詐欺などの犯罪の対象となる可能性がある。

(d)　情報収集者／情報利用者のトラストレベル

「病歴」はセンシティブデータであり、「支払額」、「総額」は取扱いが機微な情報であることから、情報収集者および情報利用者に求められるトラストレベルは、表 4-58 における AAA、AA 等である。

(e)　安全性レベルの要件

「病歴」はセンシティブデータであり、「支払額」、「総額」は取扱いが機微な情報であることから、情報収集者および情報利用者に求められる安全性には安全性レベル I が求められる。

(f)　まとめ

以上、「ケーススタディ③：保険商品設計（金融）」の結果をまとめると、表 4-66 のようになる。

表 4-66　ケーススタディ③：保険商品設計　まとめ

1．ビジネスモデルの例	各保険会社は自身が保有する顧客データを匿名化して、事業者に渡す 分析会社は、匿名化された顧客データを複数の保険会社から収集し、統合（名寄せをせずに単純に連結）した上で、分析し、レポートを作成する 分析会社はレポートを保険会社に販売する（会員制などの形態もあり得る）	
2．情報提供者の個人特定の可能性	性別×住所×年齢×疾病歴	性別×住所×年齢×高額保険商品
3．個人特定時の影響	病気による差別	窃盗、詐欺等の犯罪の対象
4．収集者／利用者のトラストレベル	トラストレベル AAA、AA が必要である ※センシティブデータを扱う	
5．匿名化の安全性レベル	安全性レベル I が必要である	

(4) ケーススタディ④：店舗出店戦略策定（小売）

(a)　ビジネスモデルの例

東京などの都市圏では、一つの地域にたくさんのコンビニエンスストアがあり、非常に便利である。一方で、コンビニエンスストア等を展開する小売企業では、競合他社が同じ地域内に出店を行うことにより、一つの地域からあげられる収益が分割されるという問題をもっている。したがって、他社の出店状況や顧客の入店状況、地域住民の動線などを分析し、より客数が望める場所に出店するとともに、今後も客数が望めない店舗を閉鎖するなどのスクラップアンドビルドに関するニーズが存在すると考えられる。

ここでは、携帯電話に付属する GPS から収集される位置情報を通信事業者が収集し、これを匿名化して、小売企業に販売、小売企業は動線分析を行うことで、店舗のスクラップアンドビルドを実施するというモデルを考える（図 4-59 参照）。

情報提供者である地域住民またはある地域に流入する人は、自身が保有する携帯電話に付属する GPS によって、情報収集者である通信事業者に自分の位置情報を一定間隔で送信する。情報収集者は、この位置情報を集積し匿名化等の加工処理を施し、情報利用者である小売企業に販売する。情報利用者は、この位置情報が集積されたデータを基に、潜在顧客の動線を分析したり、多店舗や競合他社の店舗などへの情報提供者の流入状況を分析したりして、店舗の出店、閉店に関する計画を策定する。

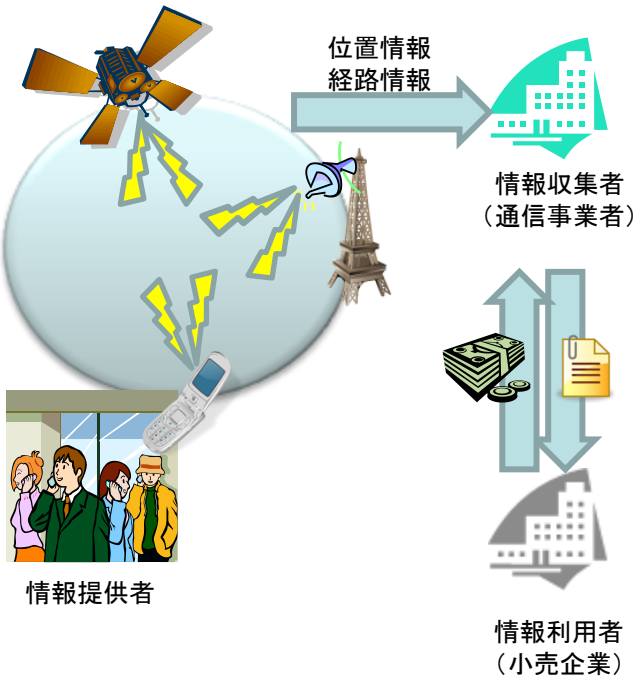

図 4-59　ケーススタディ④：店舗出店戦略策定　フロー

このモデルでは、情報収集者である通信事業者は、情報提供者が所持している携帯電話の GPS 機能により、位置情報を収集する。GPS では、携帯電話の緯度、経度を収集できる。位置情報を収集したタイミングの日付、時刻も記録し、同一の携帯電話において割り当てた ID により、一貫性をもたせることで、動線解析を行うことが可能となる（表 4-67 参照）。

表 4-67　ケーススタディ④：店舗出店戦略策定データフォーマット

ID	日付	時刻	緯度	経度

(b)　情報提供者の個人特定の可能性

同一の携帯電話の GPS により収集された位置は同じ ID で管理され、同一の ID で時系列に並べなおした位置の列は、経路情報となる。経路情報が全く同じとなるケースは、同一の情報提供者が複数の携帯電話を保有している場合など、非常に限られている。このため、経路情報はそれぞれの情報提供者でほとんど唯一となることが想定され、ある情報提供者が頻繁に通る経路などを知る人や、情報提供者が所属する会社所在地や通っている学校を知る人が、経路情報から個人を特定できる可能性がある。

(c) 個人特定時の影響

経路情報から情報提供者個人を特定された場合、その情報提供者の住所や頻繁に訪れる場所、通勤や通学の経路、また、それらの時間帯まで知られる。したがって、特に女性の場合に想定される、ストーカー等の犯罪が危惧される。

(d) 収集者／利用者のトラストレベル

経路情報は情報提供者個人の特定がしやすいデータであると考えられる。したがって、表 4-58 における高いトラストレベル（AAA、AA）などが求められる。

(e) 安全性レベルの要件

経路情報は情報提供者個人の特定がしやすいデータであると考えられる。また、個人特定時の影響も、特に女性の場合、被害が発生するとその影響は大きい。したがって、安全性レベル I が求められる。

(f) まとめ

以上、「ケーススタディ④：店舗出店戦略策定（小売）」の結果をまとめると、表 4-68 のようになる。

表 4-68 ケーススタディ④：店舗出店戦略策定 まとめ

1．ビジネスモデルの例	情報収集者（通信事業者）は携帯電話利用者の位置情報を収集して、データを情報利用者（小売企業）に販売 情報利用者（小売企業）は、経路情報（単一端末の位置の履歴）を基に、ある区域内の動線を解析 情報利用者（小売企業）は、動線の解析結果を基に、店舗のスクラップアンドビルドを実施
2．情報提供者の個人特定の可能性	経路情報であり、唯一となるデータが存在する可能性が高い
3．個人特定時の影響	住所の特定、通勤経路等の頻繁に通る道などの特定によりもたらされる犯罪の誘発
4．収集者／利用者のトラストレベル	トラストレベル AAA、AA、A が必要である ※経路情報を扱い、個人特定の可能性がある
5．匿名化の安全性レベル	安全性レベル I が必要である

(5) ケーススタディ⑤：タクシー配車管理（運輸）

(a) ビジネスモデルの例

タクシー事業者は、個々のタクシードライバーに対して、顧客等の求めに応じて、無線を通じて配車を行っている。また、個々のタクシードライバーは、駅などの人が集まるポイントで客待ちをしたり、個々のタクシードライバーが保有する、よくお客さんを乗せられるポイントに関するノウハウなどに従い、地域を巡回したりする。

もし、潜在顧客がいると考えられるポイントや時間帯などをタクシー事業者が知ることができたなら、配車するタクシーの数やポイントを管理することにより、より高い収益を上げられる可能性が増すだろう。

ここでは、携帯電話の GPS 機能により、収集できる潜在顧客の位置情報を基に、タクシー事業者が分析を行い、人通りの多い場所や道や時間帯を割り出し、タクシーの配車に用いることを考える。

情報提供者は携帯電話を所持しており、GPS により情報収集者である通信事業者に一定間隔で自分の位置を知らせる。ここでの位置は緯度、経度である。情報収集者は、位置情報が送られてきた時間とともに、これを記録する。そして、この時刻と位置情報が集積されたデータセットに対して、匿名化処理を施して、情報利用者であるタクシー事業者に販売する。タクシー事業者は、人がたくさん集まっている場所と時間帯などを分析し、自社の管理下にあるタクシーの配車に用いる。

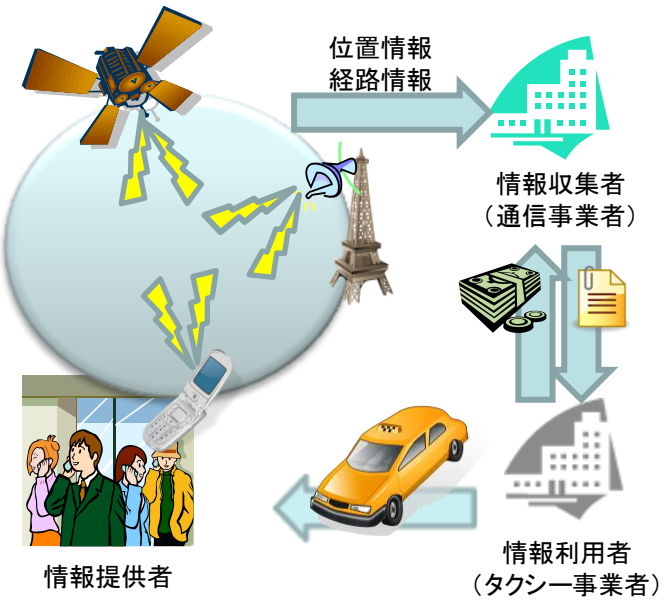

図 4-60 ケーススタディ⑤：タクシー配車管理 フロー

このモデルでケーススタディ④と同様に、情報収集者である通信事業者は、情報提供者が所持している携帯電話の GPS 機能により、位置情報を収集する。GPS では、携帯電話の緯度、経度を収集できる。位置情報を収集したタイミングの日付、時刻も記録し、同一の携帯電話において割り当てた ID により、一貫性をもたせることで、動線解析を行うことが可能となる（表 4-69 参照）。

表 4-69　ケーススタディ⑤：タクシー配車管理データフォーマット

ID	日付	時刻	緯度	経度

(b)　情報提供者の個人特定の可能性

同一の携帯電話の GPS により収集された位置は同じ ID で管理され、同一の ID で時系列に並べなおした位置の列は、経路情報となる。経路情報が全く同じとなるケースは、同一の情報提供者が複数の携帯電話を保有している場合など、非常に限られている。このため、経路情報はそれぞれの情報提供者でほとんど唯一となることが想定され、ある情報提供者が頻繁に通る経路などを知る人や、情報提供者が所属する会社所在地や通っている学校を知る人が、経路情報から個人を特定できる可能性がある。

(c)　個人特定時の影響

経路情報から情報提供者個人を特定された場合、その情報提供者の住所や頻繁に訪れる場所、通勤や通学の経路、また、それらの時間帯まで知られる。したがって、特に女性の場合に想定される、ストーカー等の犯罪が危惧される。

(d)　収集者／利用者のトラストレベル

経路情報は情報提供者個人の特定がしやすいデータであると考えられる。したがって、表 4-58 における高いトラストレベル（AAA、AA）などが求められる。

(e)　安全性レベルの要件

経路情報は情報提供者個人の特定がしやすいデータであると考えられる。また、個人特定時の影響も、特に女性の場合、被害が発生するとその影響は大きい。したがって、安全性レベル I が求められる。

(f)　まとめ

以上、「ケーススタディ⑤：タクシー配車管理（運輸）」の結果をまとめると、表 4-70 のようになる。

表 4-70　ケーススタディ⑤：タクシー配車管理　まとめ

1．ビジネスモデルの例	情報収集者（通信事業者）は、情報提供者の携帯電話の位置情報を収集する 情報利用者（タクシー事業者）は、情報収集者（通信事業者）から、単位時間当たりで最新の携帯電話の位置情報を購入する 情報利用者（タクシー事業者）は、購入した位置情報から人口の密集地帯、時間帯などを分析し、タクシーの配車戦略に利用する
2．情報提供者の個人特定の可能性	経路情報であり、唯一となるデータが存在する可能性が高い
3．個人特定時の影響	住所の特定、通勤経路等の頻繁に通る道などの特定による犯罪の誘発
4．収集者／利用者のトラストレベル	トラストレベル AAA、AA、A が必要である ※経路情報を扱い、個人特定の可能性がある
5．匿名化の安全性レベル	安全性レベル I が必要である

(6) ケーススタディのまとめ

上記のケーススタディの結果をまとめると、表 4-71 のようになる。この結果から、これまで検討してきた汎用的なトラストレベルの評価方法、および、安全性レベルの評価方法では、どれも高いレベルのトラストレベルが必要であり、統計を除いて、高い安全性が必要となることが分かる。

表 4-71　ケーススタディのまとめ

分野	サービス概要	収集データ	データセットの性質	トラストレベル	安全性レベル
医療	**薬剤マーケティング** 実際の病状と投薬の履歴から、薬の有効性を検証し、マーケティングに利用する	診療日、性別、年齢、傷病名、所見、投薬剤など	センシティブデータを含む（傷病名、投薬剤）	高いトラストレベル（AAA、AA）	高い安全性（I）
統計	**アンケートデータの再利用** 過去に実施したアンケートの個票を再利用する	個別アンケート結果（表）	基本的に性別、年齢、所在地が含まれる	収集者には高いトラストレベル（AAA、AA、A）利用者はアンケート内容毎に判断	アンケート内容毎に判断

分野	サービス概要	収集データ	データセットの性質	トラストレベル	安全性レベル
金融	**保険商品設計** 複数の生命保険会社が保有するデータを統合し、商品設計のための基礎データとして利用する	年齢、性別、住所、病歴、喫煙の有無、購入商品、オプション、加入年数、支払額、総額　など	センシティブデータを含む（病歴）	高いトラストレベル（AAA、AA）	高い安全性（Ⅰ）
小売	**店舗出店戦略策定** 携帯電話の GPS で測位される経路情報から店舗のスクラップアンドビルドを行う	経路情報（時刻、緯度、経度の系列）	経路情報（個別経路は唯一になる可能性が高い）	高いトラストレベル（AAA、AA、A）	高い安全性（Ⅰ）
運輸	**配車管理** 携帯電話の GPS で測位される位置情報を基に、潜在顧客が集中する地域を割り出し、配車等に利用する	位置情報（時刻、緯度、経度）	位置情報の蓄積により経路情報となる（個別経路は唯一になる可能性が高い）	高いトラストレベル（AAA、AA、A）	高い安全性（Ⅰ）

4.6.5 有識者ヒアリング

上述 4.6.1 から 4.6.4 までの検討結果をもって、有識者にヒアリング調査を行い、内容や課題に関するご意見を頂戴した。ご協力いただいた有識者は、情報セキュリティ分野およびデータマイニングの分野の専門家である。主なご意見を以下にまとめる。

ヒアリング調査にて頂いた主なご意見

- ■ガイドライン（案）を基にトラストを検討した場合、「明示ルール」、「加工ルール」、「利用ルール」が重要である。特に記載内容が決まっていない部分は今後検討が必要である。
- ■基本的なコンセプトとして、ルールで厳しく縛るような方法よりも、最低限の部分だけ担保してパーソナル情報を流せるような仕組みを考えてほしい。
- ■原則としてある仕組みに従わないと情報を流せないというものは好ましくない。
- ■業界毎の自主規制的なものを育てるような仕組みが望ましい。
- ■業界毎の事情やニーズが異なるので、業界横断的な仕組みや制度を構築するよりも、匿名情報でも利用したいというニーズがある分野をベースに検討を行った方が、簡単で適切なものを構築できる可能性がある。
- ■ケーススタディを深掘りしながら、匿名情報に関するニーズがある分野を明確にし、その分野の事情に合致した認証スキームを検討した方がよい。

図 4-61　ヒアリング調査の主な意見

4.6.6 まとめ

以上、ケーススタディの結果ならびに有識者ヒアリングの結果から、匿名情報の認証スキームを構築するに当たり、以下の課題があることが判明した。

分野横断的な認証スキームよりも、特定分野の認証スキームを検討すべきある

- 汎用的な認証スキームを構成すると制度自体が重く、認証を受ける者にとって厳しいものとなる
- 分野やサービスごとに異なる事情があることから、匿名化パーソナル情報へのニーズが深い分野・サービスに絞って検討を進めた方がよい

明示、加工、利用の各ルールに記載する最低限の事項を検討する必要がある

- これまでのところ明示、加工、利用の各ルールについては検討がまだ十分なレベルには至っていない
- 必要以上の事項をルールとして定めると、各プレイヤにとって重い仕組みとなり、情報の流通を妨げ得る
- 必要最小限の事項をガイドラインとして取りまとめるなどの方向で検討を進めるべきである

制度の在り方について、流通を促進するような仕組みを検討する必要がある

- 認証スキーム構築における本来の趣旨は、パーソナル情報を安心して、かつ、便利に利用するための仕組みを検討し、構築していくことである
- 制度として厳しく規制するようなアプローチでは、本来の趣旨に反することになりかねない

図 4-62　認証スキーム構築の課題

4.7 匿名情報の利用を促進するための認証スキーム検討

安全に匿名化したパーソナル情報を利用するための認証スキームに関して、「パーソナル情報認証スキーム委員会」にて検討を行った。

4.7.1 匿名情報の二次利用を行う市場について

匿名情報を利活用するサービスを洗い出し、各サービスの市場規模を合算して市場規模を算出した。サービスが創出される市場には、医療、金融、運輸、小売等が考えられるが、特に有望と考えられるのは、金融分野と小売分野である（4.5.5 項参照）。

医療分野においては、匿名化したパーソナル情報を医療研究向けに提供するサービスが実施されているが、健康志向が高まる中、匿名化したパーソナル情報をヘルスケアに利用する等新たなサービスを創出する動きが出てきている。

医療分野だけでなく、情報利用者はパーソナル情報を匿名化して利活用したいと検討しているが、ユーザの信頼を得るために「匿名化したパーソナル情報の利用方法」や「匿名化の安全性」についての保証を必要としている。ガイドライン等で利活用のルールや指標を示すことで、情報流通が活発になり、市場が創出されると考えられる。

4.7.2 匿名情報の利用に関するガイドラインについて

経済産業省では、平成 22 年 11 月から匿名情報の安全な利用についてのガイドラインを検討している。匿名化した情報であっても、その匿名化の粒度を細かくしようとすると、個人情報保護法上の「個人情報」にあたる可能性がある。また、当該情報を第三者提供した場合にはプライバシーとの関係で問題が生じる可能性が高い。

したがって、個人情報を匿名化する際の方法に加え、匿名化された情報を安全に利用するためのガイドラインの検討をしている。

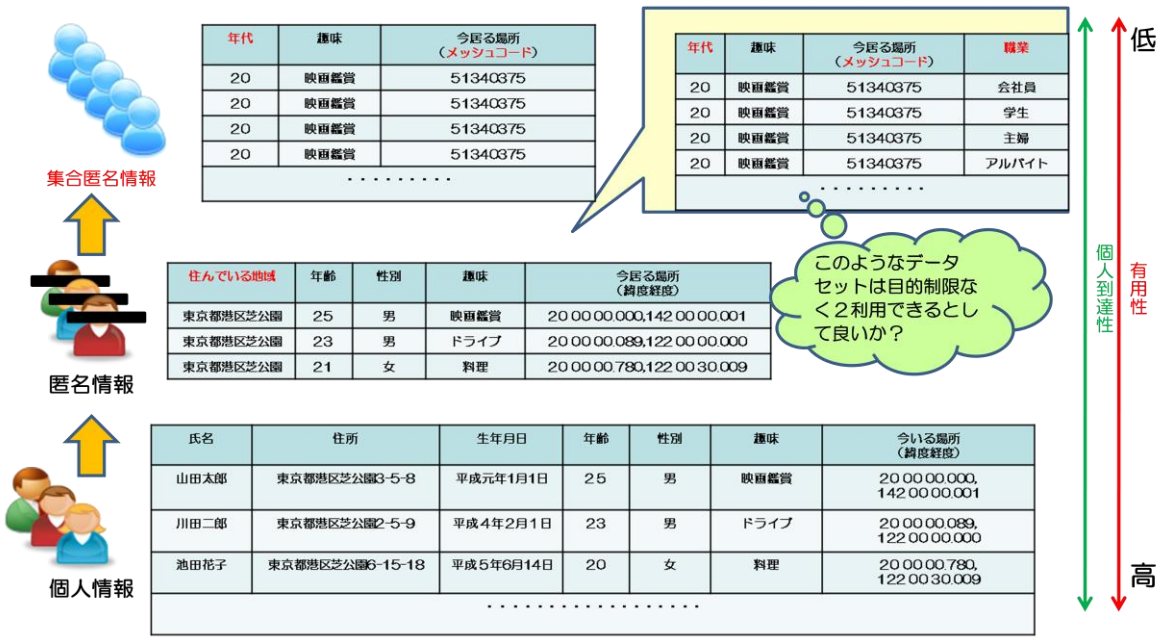

図 4-63　匿名情報の作成

また、次世代パーソナルサービス推進コンソーシアムでは、産業界での匿名化したパーソナル情報の利活用について検討している。コンソーシアムの活動体制として、制度検討 WG、技術検討 WG およびサービス検討 WG により構成される。その中でも制度検討 WG では、匿名化したパーソナル情報の利活用についての産業界からのガイドライン策定を検討している。

これらのガイドラインが策定され匿名情報の利活用についてのルールを明示されることにより、匿名情報の利用および流通が進み、匿名情報を利用するサービスの市場が台頭してくると考えられる。

4.7.3 匿名情報関連の制度検討事項

「匿名情報の利活用の安全性」を保証するには、「情報提供者および情報利用者の評価」および「匿名化したデータの評価」を実施し認定する制度が必要になってくると考えられる。図 4-64 は、匿名情報の利活用における情報提供者および情報利用者の行うプロセスを、本調査結果から整理したものである。

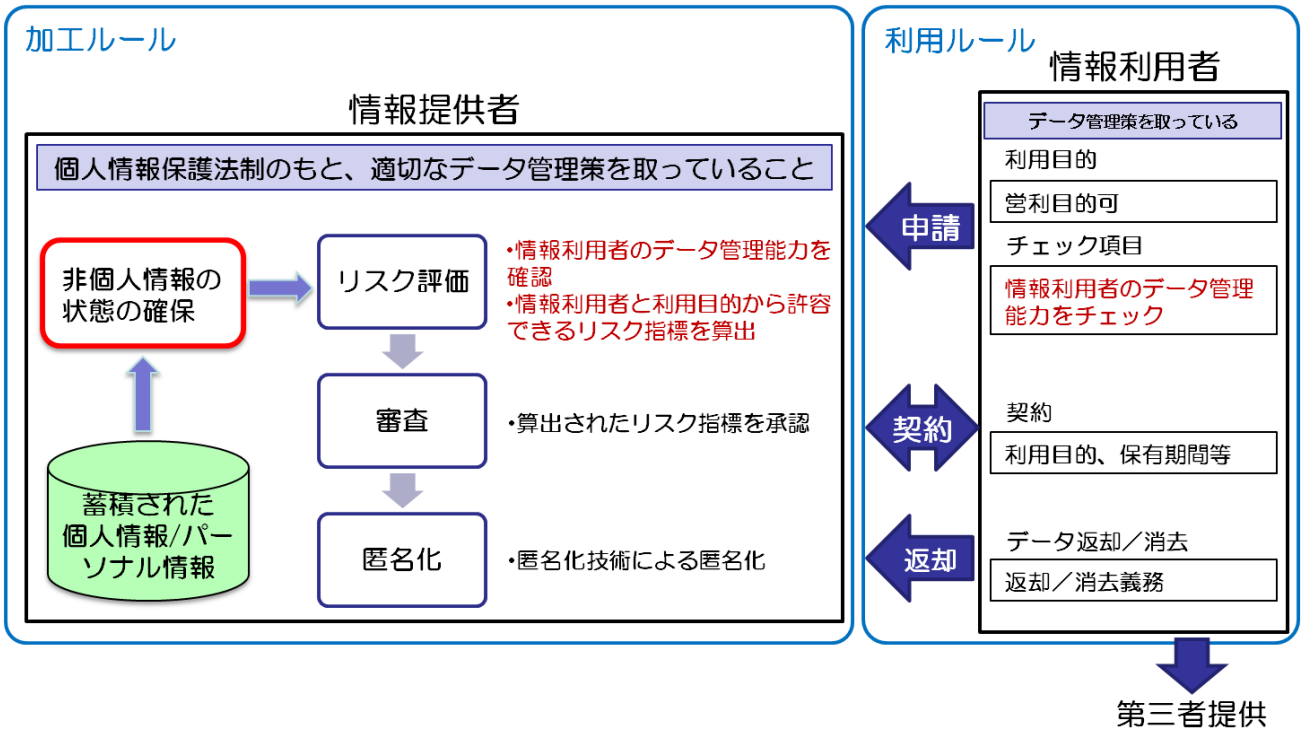

図 4-64　匿名情報の利活用におけるプロセス

情報提供者は、個人情報を保有しているため、P マークや ISMS を取得し、ユーザから信頼されていることが多いと考えられる。しかし、情報利用者が個人情報を保有していない事業者であるとき、情報利用者は適切な情報管理を実施していることについて第三者的な評価を受けていないと考えられる。そのような場合では、情報提供者が情報利用者のデータ管理能力について評価しなければならない。

CHEO では、ISO/IEC27002（情報セキュリティ管理）などに基づいて、データの管理の仕方やスケジューリング方法、管理者の有無という点をチェックし、リスクを算出している。また、統計センターでは、情報利用者のデータ管理について審査している。（4.2 節参照）

このことから、情報提供者が情報利用者のデータ管理能力について評価する際、情報利用者が ISO/IEC27002 取得相当の管理体制があることを評価すれば良いと考えられる。

一方、匿名化したデータの評価については、匿名化評価ツールは運用される各国の法令等や利用ケースに影響されることが多く、匿名化評価指標に関する共通項は少ない。また、評価値については、経験に基づいて設定しており、定量的に明示することは難しい。（4.4 節参照）

しかし、匿名化手法については、大域的再符号化や局所秘匿化など概ね共通していることが分かった。評価技術は、k-匿名性、l-多様性、t-近似性が広く認知されている。その中でも、k-匿名性は中心的な考え方であり、匿名化評価ツールでも採用されている。

匿名化手法については、標準的な規準を策定することができると考えられ、JIS 規格化や国際標準化を推進していくことが望ましいと考えられる。

4.7.4 まとめ

本調査によって、現状では匿名化されたパーソナル情報を用いたサービスの事例は非常に少ないことが分かった。匿名化したパーソナル情報を利用するための認証スキームについては、匿名情報を利用するサービス事例が少ない中で認証制度を先行して策定するのではなく、産業界において匿名情報の利用が進み、匿名情報を利活用するサービスの運用における課題が明確になった時点で策定されることが望ましい。まずは、4.7.2 項で検討されているガイドラインから「セーフハーバー」が明示され、「情報提供者／情報利用者の評価」と「匿名化したデータの評価」の方法を提示することで、市場が創出されることが重要である。

5. 環境オプトインに関する調査検討

5.1 オプトイン、オプトアウトの文献調査

本節には、環境オプトインを定義する上で参考とするオプトインおよびオプトアウトの事例に関する調査結果を記載する。5.1.1 項にオプトイン、オプトアウトの概念を、5.1.2 項に主な事例を、5.1.3 項に課題に関する調査結果を示す。

5.1.1 オプトイン、オプトアウトの概念

オプトインおよびオプトアウトの概念を示す。オプトインとオプトアウトは、共に個人情報の収集・利用と選択（承諾）に関する方法を表す用語である。オプトインとは、企業などの団体や個人が個人情報[89]を収集、利用または、第三者への提供を行う場合に、個人情報の主体者である本人への承諾を事前に得ることを意味する。また、個人情報の主体者である本人への承諾を事前に得ずに、事後に利用制限や破棄などを示せることを意味する。例えば、行動ターゲティング広告の経済効果と利用者保護に関する調査報告書[90]による説明では、オプトインを「利用者の同意を得た場合に行動ターゲティング広告の表示を行う。同意を得られない場合には広告の表示を行わない。」、オプトアウトを「利用者が行動ターゲティング広告を拒否する手段を提供する。拒否しない限り表示を行う」と記述している。

■オプトイン　・・・　事前に本人へ承諾を得てサービス等を提供すること

■オプトアウト・・・　事前に本人へ承諾を得ないでサービス等を提供し、サービス提供後に本人が拒否的な行為・意見を示せること

図 5-1　オプトイン、オプトアウトの定義

5.1.2 オプトイン、オプトアウトの主な事例

本節では、オプトインおよびオプトアウトの一般的な事例と環境オプトインを定義する上で参考となる関連する事例について示す。環境オプトインに関連する事例は、センサーを用いた情報取得に関連するセンサネットワーク[91]と特定の環境において情報収集しレコメンドサービスを行う行動ターゲティング広告（文献 90 参照）である。

---

89 個人情報とは、生存する個人の情報であって、特定の個人を識別できる情報(氏名、生年月日等)を指す。これには、他の情報と容易に照合することができることによって特定の個人を識別することができる情報(学生名簿等と照合することで個人を特定できるような学籍番号等)も含まれる。 個人情報の保護に関する法律(2 条 1 項)

90 行動ターゲティング広告の経済効果と利用者保護に関する調査研究 報告書,総務省, 情報通信政策研究所, 平成 22 年 3 月
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2009/2009-I-16.pdf

91 センサネットワークは、センサーをネットワークすることで一つのシステムとして動作する

(1) 一般的なオプトイン、オプトアウトの事例

オプトインおよびオプトアウトの事例として、最も多いものは、電子メールを利用した広告等であり、一般的には、メールマーケティング等と言われるサービスである。個人情報を利用する企業、または個人情報を利用してサービス提供する事業者は、個人情報の主体者である本人に自らの個人情報や属性、電子メールアドレスを登録させ、電子メールによる広告を受けることをサービス開始よりも前に許諾させる。この方式がオプトインである。

また、このメールマーケティングの事例におけるオプトアウトは、広告メールの末尾に、広告送信を断ることや登録した個人情報の破棄などをサービス開始後に求めることができる場合として説明されることが多い。

しかし、2008 年 6 月に成立した「改正特定商取引法」には、ネット通販事業者（ネットショップ）等や電子メール広告受託事業者に関係する規制があり、現在ではオプトインに義務付けられている。この改正では電子メール広告を送信する前にあらかじめ消費者（個人情報主体者）に対して請求や承諾を得ることが義務付けられているため、請求や承諾を得ていない電子メール広告の送信は原則禁止されている（この規制は、オプトイン規制等とも呼ばれている)。

一般的には、この規制によってオプトインが義務付けられているため、現在ではオプトインによる運用の事例に比べ、オプトアウトによる運用の事例は極端に少ない。なお、オプトイン／オプトアウトの概念を説明する上で、用いられるオプトアウトの事例は、以下の 2 点がある。

■住宅地図業者・・・	具体的には、調査対象の表札や郵便受けを調査し、その結果に基づき住宅地図を作成し、不特定多数へ販売（不特定多数への第三者提供[92]）する場合。
■データベース事業者・・・	具体的には、ダイレクトメール用の名簿等を作成し、販売（上記同様、不特定多数への第三者提供）する場合。

図 5-2　オプトアウトの事例

上記に示した事例の通り、オプトアウト事例では、名簿や電話帳等のように個人情報を第三者提供することが目的の場合には、本人の同意を受けずに第三者提供を行い、本人の求めがあった場合に後から第三者提供を停止する方法である。

[92] 第三者提供の手段または方法の事例として、１)書籍として出版、２)インターネットに掲載、３)プリントアウトして交付等 が想定されている。

(2) 一般的でない同意取得方法の事例

一般的ではない同意取得方法の事例の調査として、センサネットワーク[93] [94]、行動ターゲティング広告（文献 90 参照）における事例調査の結果を報告する。行動ターゲティング広告およびセンサネットワークにおいて、ユーザへの告知や同意を得るオプトイン、利用を制限するオプトアウトの対応は、各業種・サービス毎に異なり、ユーザは、どのような情報を取得し、利用されているのかを理解できない状況であることが分かった。

表 5-1　行動ターゲティング広告、センサネットワークの事例

		業種・サービス	取得デバイス	取得情報	オプトイン	オプトアウト
B1	行動ターゲティング広告	クーポン配信	GPS(携帯)	位置情報	○	○
B2		空輸(チケット購入)	PC	入力文字等	×	×
B3		SNS[95]	PC	入力文字等	※1	×
B4		フィードリーダー	PC	入力文字等	×	×
B5		電子市場	携帯、PC	入力文字等	※1	×
S1	センサネットワーク	SNS	GPS(携帯)	位置情報	○	※1、※2
S2		共通ポイントカード	IC カード	識別子	○	○
S3		交通 IC カード、共通ポイントカード	IC カード	識別子	○	○
S4		防犯・警備	カメラ	動画	×	×
S5		防犯・警備	赤外線センサー	人の存在(熱)	×	×
S6		イベント管理	RFID タグ	識別子	○／×	－

※　1：プライバシー・ポリシーを掲載しているのみで、情報取得の合意については明確な意思表示を得ていない。

※　2：同社の別サービスに対する登録ユーザは、プライバシー・ポリシーを掲載しているのみ。

93 センサネットワーク活用調査報告, センサネットワーク活用調査報告, 平成 20 年 3 月
http://www.jipdec.or.jp/archives/ecom/results/h19seika/h19results-10.pdf

94 センサネットワークを活用した情報システムに関する調査・開発報告書, 財団法人ニューメディア開発協会, 平成１８年３月
http://www.nmda.or.jp/keirin/h17houkoku/h17sensor.pdf

95 ソーシャル・ネットワーク・サービス

5.1.3 オプトイン、オプトアウトの課題について

前項の調査結果から、オプトインおよびオプトアウトの課題を整理する。事業者とユーザの間には情報の非対称性が存在する。情報の非対称性を埋めるために、オプトインを行うことで事前同意を得て情報取得を実施するのが現状である。一方、現状の一般的な約款は専門家でないと理解できない内容であり、ユーザが内容を熟読した上で同意を得るという行為が難しい。この結果として、既存のサービス事業者では、形骸化したユーザ同意を得る、またはユーザ同意を得ないことによる訴訟リスクをサービス事業者が抱える可能性がある。また、新たなサービスを行う事業者においては、さらにユーザの同意を得ることが難しく、新たなサービスの創生の阻害になる可能性がある。これらを踏まえて検討した課題事項を示す。

(1) 個人情報にあたらない取得情報時の告知

以下に個人情報にあたらない情報（個人を特定できない情報）の取得に関する課題を示す。

(a) 事業者のポリシーが不明

オプトインおよびオプトアウトは、個人を特定できる情報に関する議論であり、個人を特定できない情報については、事業者が情報取得の際に注意すべき点、情報取得の際にどのような告知を行うことが求められるのか？また取得し利用する情報をどのように管理すべきか？について不明確であると考えられる。

(b) 情報取得の告知

センサネットワークにおけるカメラ等を例とした場合、個人を特定できない情報取得であっても何も告知せず、ユーザにカメラを向け撮影する行為はユーザが受容できないと考えられるのが一般的である。このように特定のセンサーやデバイスについては、ユーザの受容性が変化することが考えられるため、情報取得するセンサーやデバイスの特性を踏まえた検討が必要であると考えられる。以上のことから、どのようなセンサーやデバイスを用いて、どのような情報を取得しているのかを告知する必要があると考えられる。

(c) 情報利用の告知

行動ターゲティング広告事例の通り、どのような情報を利用しているのかを告知せずに、サービス提供を行う場合は、ユーザが受容できない可能性も考えられる。また、個人を特定できない情報として利用する場合では、どのような方法で個人を特定できない情報に変換（加工）されているのかも告知する必要がある。以上のことから、どのような情報を利用してサービス提供しているのかを告知する必要があると考えられる。

(2) 健全な産業およびサービスの発展

現状では、いわゆるオプトイン規制によって、ネット通販事業者や電子メール広告受託事業者等では、個人情報の利用および取扱いについては、オプトインによる事前承認を得る必要がある。この場合、個人情報の利用および取扱いについては、ユーザにとって既存の（または、認知されている）魅力的なサービスでない限り、オプトインによる事前承認を得ることは難しく、新しいサービスについては事前承認を得ることが困難な場合も懸念され、新しい産業やサービスの健全な発展が阻害される恐れがある。

(3) 訴訟リスク

専門家でないと理解できない内容の約款では、ユーザが内容を熟読した上で同意を得るという行為が難しく、訴訟に関するリスクを事業者が抱えている可能性がある。消費者庁の集団的消費者被害救済制度研究会[96]では、下表に示す通りオプトイン、オプトアウトに関する訴訟リスクに対する長所・短所等が検討されている。一方、これらの訴訟リスクは取得する情報およびその利用範囲や管理等を専門家でなくとも理解できる簡易的な内容で事前に告知することで軽減できる可能性があり、これらを抜本的に改善する告知方法について検討する必要があると考えられる。

表 5-2　オプトイン、オプトアウトの長所・短所の例[97]

オプトイン型	長所	● これまでの我が国の訴訟手続と親和性が高いのではないか ● 既存法制度との整合性がとりやすいのではないか ● 個別訴訟に比して、個々の消費者の訴訟に関する負担（証拠収集の労力、弁護士費用など）の軽減が図れるのではないか
	短所	● オプトインの時期を訴訟係属中に限ると、訴訟の回数がわからないので、個々の消費者がオプトインをためらうことが多くなり、手続に積極的に関与する必要のないオプトアウト型に比して、救済される消費者が少なくなるのではないか ● オプトインが必要であるので、個々の請求額が少ないほど利用されにくくなるのではないか
オプトアウト型	長所	● オプトインが不要であるので、手続に積極的に関与しない多数の消費者に判決効を及ぼすことができ、広く消費者を救済するという目的に合致するのではないか ● 個々の消費者の訴訟に関する負担（弁護士費用など）の軽減が図れるのではないか（オプトイン型に比して多くの消費者に判決効を及ぼすことになり、より多くの消費者が判決で利益を得ることが有り得る。また、それらの消費者に訴訟に関する負担を分担させることができれば、個々の消費者の訴訟に関する負担は軽減され得るのではないか。）
	短所	● 訴訟の当事者および参加した者に対して、その訴訟の判決効が及ぶことを前提とするこれまでの我が国の訴訟手続とは異なる点が多い ● オプトアウトの権利を保障するため、訴訟係属を通知する必要があるが、通知の費用が膨大になり得るため、現実に訴訟を起こすことが困難になるおそれがあるのではないか ● 訴訟が濫用され、事業者の活動に萎縮効果をもたらすおそれがあるのではないか

96 第５回集団的消費者被害救済制度研究会,配布資料 2, 集団的消費者被害救済制度研究会 http://www.caa.go.jp/planning/pdf/100219-2.pdf

97 消費者庁の集団的消費者被害救済制度研究会の資料から本調査に関連する事項について、みずほ情報総研が任意に抜粋した内容である。

5.2 オプトインの先進的な事例の調査

5.2.1 事例調査

本項は、オプトインに関連する先進的な事例について調査した結果を記載する。

(1) センシング Web に関する実証実験

京都大学の美濃教授らが実施した研究および実証実験に関する公開情報調査およびヒアリング調査の結果を以下に示す。以下の情報は公開情報[98] [99]に基づく。

(a) 研究概要について

研究の概要について、表 5-3 に示す。

表 5-3 研究概要

研究名称	センサー情報の社会利用のためのコンテンツ化
研究期間	平成 19 年度～21 年度
研究課題	USN[100]がごく近い将来に社会全体に普及し、世界各地に様々な用途の USN が多数設置されている状況が出現するという予想の下に、その次の段階として、USN から得られるセンサー情報を Web のように誰もが自由に利用できる仕組みを実現することを目指す。
研究目的	実世界に分散配置された様々なセンサーから得られるセンサー情報と、人口分布、気候分布、土地用途分布、生態系分布などの広域環境情報とを有機的に統合利用すると共に、これに基づいて利用者からの要求に応じてコンテンツを動的・適時的に提示する実世界ポータルを構築すること。
研究内容	①プライバシー情報管理技術 ②センサー情報コンテンツ化技術 ③観測型実世界コンテンツ提示技術

(b) 実証実験の概要について

実証実験の概要について、表 5-4 に示す。

98 センサー情報の社会利用のためのコンテンツ化, 京都大学学術情報メディアセンター, 美濃導彦, 2009 年 12 月 1 日
http://www.renkei.jst.go.jp/infor/21/21_2_1.pdf

99 センサー情報の社会利用のためのコンテンツ化, 美濃導彦
http://scfdb.tokyo.jst.go.jp/pdf/20071620/2007/200716202007pp.pdf

100 ユビキタスセンサネットワーク

表 5-4　実証実験概要

実証実験の目的	・動くシステムを作って実証実験の実施 ・実証実験を進めるための施策 ・実証実験の場所として新風館（京都、烏丸御池）を選定
場所	商業施設：新風館（烏丸三条）
期間	2009 年 7 月～12 月
実施内容	・継続的なデータ処理技術開発 ・三回のイベント実施 ・メディア等への情報発信
情報取得センサー	カメラ、RFID タグリーダ、赤外線センサー、 無線 LAN アクセスポイント、気象センサー
統計データの蓄積	入館した客の人数（性別、年齢） ・客の滞在時間の統計 ・客の移動軌跡
アンケートの目的	・プライバシー意識の調査 ・プライバシー対処技術の有効性評価 ・SWeb[101]サービスの受容度調査
アンケート回収件数	117 件

① 匿名化処理（変身カメラ）について

実証実験では、撮影した人物像を即時に棒状の記号に置き換えることで、個人を特定できない情報（匿名情報）として蓄積する。棒状の記号は、棒の長さによってある程度の身長を表し、匿名化しつつもある一定の属性情報を含んでいる。この処理について下図に示す。

[101] センシング Web

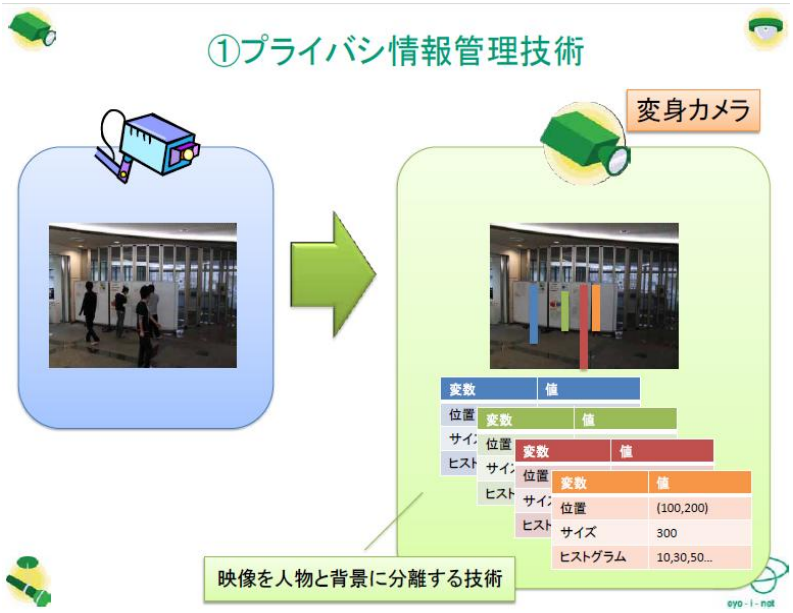

図 5-3　変身カメラの概要：撮影(左)を棒状の記号に置き換える(右)処理[102]

② アンケート結果について

上記匿名化処理を踏まえ、情報取得（捕捉）される主体（ユーザとする）の受容性に関する主なアンケート結果が示されている。

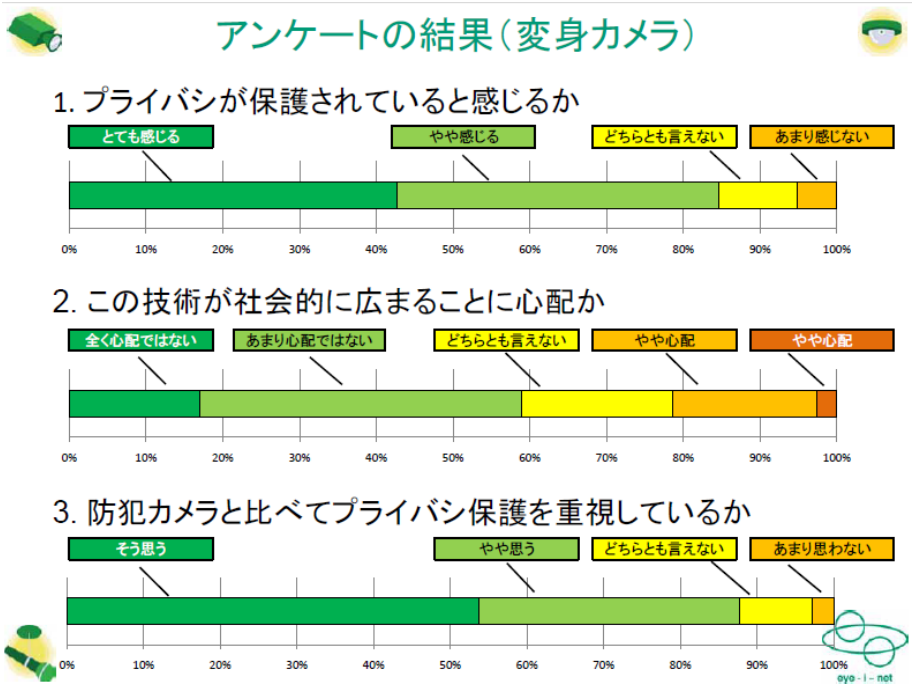

図 5-4　変身カメラに関するアンケート結果

[102] センサー情報の社会利用のためのコンテンツ化, http://www.renkei.jst.go.jp/infor/21/21_2_1.pdf

(c)　ヒアリング結果について

実証実験に関するヒアリング結果について、表 5-5 に示す。

表 5-5　実証実験に関するヒアリング結果

実証実験の環境	駅や公道等、往来が激しい場合は、実証実験による情報取得の告知義務が果たせないため、特定の環境内（商業施設）で実施した。
実証実験のセンサーに関する受容	各々のセンサー利用について個別のクレーム／問合せはなかったが、カメラを見ただけで監視カメラと理解される傾向もあった。
実証実験の告知方法	・ 環境内に立て看板で実証実験を実施していることを告知した。 ・ 必要に応じて実証実験内の説明ルームで実証実験を説明する体制を整えた。
実証実験のアンケート/クレーム/オプトアウト	・ イベント趣旨、各センサーの利用方法、匿名化処理方法の説明を行った。 ・ クレーム発生時は、施設内の説明ルームで対応する予定であったが、クレーム事例は 0 件であった。 ・ オプトアウトの申入れ事例も 0 件であった。

(d)　本調査を終えて見えてきた課題

①　ガイドラインおよびポリシー等の必要性

ユーザが感じる「分からない」ことへの不安感として、①センサーの設置場所が明示されない、②収集データの使用目的が明示されない、③情報の利用者が限定されない等、プライバシー意識への配慮が示されている（文献 98 参照）。これらをユーザに対して告知する有効な手段を検討する必要があるのではないか。

②　告知可能な環境に限定する必要性

現実空間での各種センサー、カメラによるデータ取得や ICT サービスにおけるデータ取得ではユーザに対して告知を行う必要があるのではないか、そのため、実施する環境は特定の管理者が管理する施設とし、告知を確認せずに通り過ぎる可能性のある道路などは、想定環境から除外した方がよいのではないか。

5.3 新たに必要とされるオプトイン方式の定義

5.3.1 環境オプトインの定義

本節では、環境オプトインの定義について、5.3.1(1)に概念を、5.3.1(2)に想定するプレイヤーを、5.3.1(3)に想定する環境を、5.3.1(4)想定するセンサーの種類およびユーザの選択手段を、5.3.1(5)に想定する告知ケースを示す。

(1) 環境オプトインの概念および手段

環境オプトインとは、パーソナル情報の利用について合意する、または合意しないという二者択一ではなく、特定の環境における暗黙の同意（または同意擬制）による利用可能を実

現する概念およびその手段とする。

例えば、「環境オプトイン方式（センシング Web プロジェクトの今後の方向性）」[103]では、環境オプトインの提案として、①環境への接近という視点[104]、②対等性、透明性、選択性（拒否権）の保証、③判例の基準を尊重する、④事後の判断基準（判例の基準）と環境設計基準（事前判断）の区別がないとサービス実施できない。と述べられている。

上記概念および手段の想定する具体的に取扱う情報を個人情報に該当しない情報として考慮した場合は、個人情報に対する管理、利用の制限よりも軽減することが可能であること。また、防犯対策や災害対策などを利用目的とした場合は、さらに一般的な情報利用の制限よりも軽減する可能性があることが考えられる。

(2) 想定するプレイヤー

環境オプトインの具体的なイメージとしては、個人が情報を収集されることを知りながら、あえてその環境下に自主的に入るのであれば、その情報補足に同意したと考え、補足した情報を匿名化（個人を識別できない状態）し、利用していると考えられる。また、本調査では、環境オプトインとして、特定の団体等で情報を取得（捕捉）することで自社のサービスに使用することやサービス自体の効率化などを実施することを想定している。そのため、環境オプトインで想定するプレイヤーは、情報を取得（捕捉）し、その情報を利用、管理しつつサービス提供する主体者である事業者と、情報を取得（捕捉）される主体者およびサービス利用者であるユーザとする。

(3) 想定する環境

環境オプトインは特定の環境において取得、利用される情報であり、情報取得する環境の広さに対してユーザの受容性が大きく異なる可能性がある。例えば、特定のイベント会場などでは、情報取得についても受容されるが、イベント会場を出てからも引き続き情報取得することで、広範囲な環境における移動情報（移動履歴等）を取得する場合は、受容できないことも考えられる。本調査では、特定の施設や商業店舗内における情報取得であること、また情報取得の告知が可能である場合に検討を限定するため、企業を含む団体等で管理者が存在する特定の環境であり、一般道等、公共的な施設や区間は含まないこととする。

また、特定の環境において、個人を特定できない情報として取得、利用する場合であっても、広範囲な環境において取得される場合は、取得される情報に関する環境の単位が広く、抽象化度が高い場合も想定できる。逆に環境が広くなく、取得、利用する情報に対する環境の単位が狭い場合は、抽象化度合が低くなる可能性もある。[105]

以上のことから、環境オプトインで取得、利用する情報については、二つの軸を考慮する。個人特定の軸として、個人を特定できる情報と個人を特定できない情報とする。もう一つは、

---

[103] 環境オプトイン方式の提案(センシング Web プロジェクトの今後の方向性), 牧野総合法律事務所弁護士法人, 弁護士牧野二郎, 2010 年 3 月 1 日
http://www.murase.m.is.nagoya-u.ac.jp/fm-kenkyukai/event/FM20100303-makino.pdf

[104] 公害訴訟等においては、危険を知りながら、そして避けることができたのに、あえて避けずに接近した場合には「危険接近の法理」「免責の法理」「減額の法理」「ニューサンスへの接近」といった理論で過失相殺的にバランスを取る主張が行われてきた, 2010 年 3 月 1 日, 牧野二郎

[105] 例えば、HIPAA では、特定区間の住居者が 2 万人以下の場合には情報を規制するプライバシールールが規定されている。

取得する環境の広さの軸として、広範囲な環境で抽象度の高い情報と広範囲な環境ではなく抽象度の低い情報に大別する。

具体的例を図 5-5 に示す。

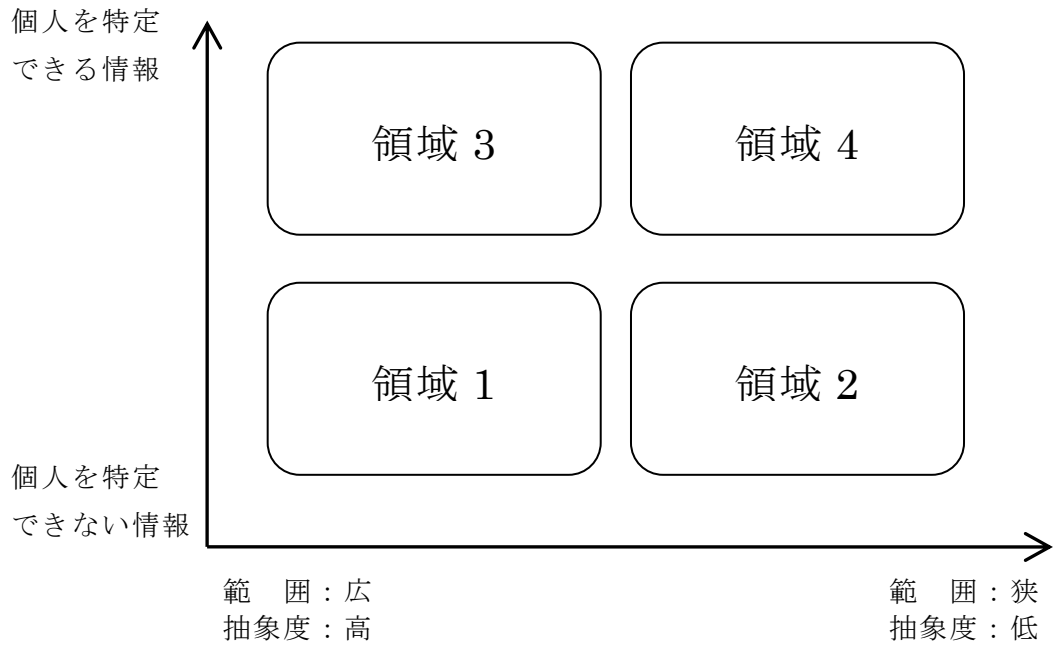

図 5-5　取得情報と環境の抽象度に関する概要図

領域 1 は、個人情報を特定できない情報を広い環境（環境における抽象度の高い）情報として取得、利用することであり、商業施設において特定時間内に何人存在したかを取得することを想定する。

領域 2 は、個人情報を特定できない情報を狭い環境（環境における抽象度の低い）情報として取得、利用することであり、店舗内の特定商品の売場付近に、どの程度滞在したかを取得することを想定する。

領域 3 は、個人情報を特定できる情報を広い環境（環境における抽象度の高い）情報として取得、利用することであり、商業施設において特定時間内に誰が存在したかを取得することを想定する。

領域 4 は、個人情報を特定できる情報を狭い環境（環境における抽象度の低い）情報として取得、利用することであり、店舗内の特定商品の売場付近に、誰がどの程度滞在したかを取得することを想定する。

個人を特定できる情報（領域 3、4）よりも個人を特定できない情報（領域 1、2）が、個人を特定できない情報であるため、受容し易いと考えられる。また、環境の抽象度が低い方（領域 2、4）よりも環境の抽象度が高い方（領域 1、3）が特定のセンシティブな商品に関連しない（結び付かない）上納であるため受容し易いと考えられる。

(4) 想定するセンサーおよび選択手段

環境オプトインを検討する上で、特定の環境における情報取得方法や種類および、取得（捕捉）する情報に対する可否の選択手段を明確にする必要がある。各々のセンサーおよびデバイスが情報取得する際に想定するユーザ選択の手段を表 5-6 に示す。

表 5-6　想定する情報取得の方法

No	センサー/デバイス	情報取得の可否選択		備考
		可	否	
1	カメラ	特定環境に入る等	特定環境から出る等	補足する情報は映像（静止画、動画、自分や同伴者等）を想定
2	RFID タグ/IC カード	センシング可能領域にデバイスを入れる等	センシング可能領域からデバイスを出す。またはシールド材で包む等	帯同しているデバイスが存在（タグ No）していることを取得することを想定
3	赤外線センサー	特定環境に入る等	特定環境から出る等	帯同しているセンサーが存在していることを取得することを想定
4	無線 LAN	センシング可能領域にデバイスを入れる等	センシング可能領域からデバイスを出す。または電源を切る等	所持している無線 LAN デバイス（IP、MAC 等）が存在していることを取得することを想定
5	消費電力	消費電力測定可能な接続端末に機器を接続する等	消費電力測定可能な接続端末に機器を接続しない。または電源を切る等	所持している機器の消費電力の測定値を取得することを想定（スマートグリッド等）

(5) 想定する告知ケース

ユーザに対する告知が、事前にできるケースと、事前にできないケースが存在する。事前告知可能なケースとは、ユーザが特定環境に入る前に、事前に情報取得する旨を示す手段がある場合であり、例えば、展示会等で事前登録時に情報取得する旨を示すことである。一方、事前告知可能でないケースとは、事前にユーザを特定し、特定したユーザに対して告知することが困難な場合であり、例えば、特定施設内を通過する人数計測などである。事前告知可能なケースであれば、事業者が事前告知を実施することできる。

また、事前に告知することが困難であるケースでは、事前告知を行いたいが、どのような手段でどのような内容を告知すればよいかが明確ではない。

以上のことから、本調査では、事前に告知することが困難であるケースを中心に検討することとし、事前告知可能なケースは検討外とすることとした。

5.4 ユーザの受容性の調査

オプトインに関する受容性の変化の事実と変化要因を確認するため、情報取得の対象となるユーザに対してヒアリング調査を行った。ヒアリング調査方法、調査結果について、以下に示す。

5.4.1 ヒアリング調査方法について

ユーザに対して実施したヒアリング調査の目的、対象および仮説を以下に示す。

表 5-7　ユーザヒアリングの概要

ヒアリングの目的	オプトインに関する受容性の変化の事実と変化要因の確認を目的とする。主な受容性変化項目を以下に示す。 ・ 個人特定/個人非特定に関する受容性および変化 ・ センサー/デバイスと告知の有無に関する受容性の変化 ・ 環境特性（抽象度の高低）に関する受容性の変化 ・ 告知方法、告知内容に関する受容性の変化
ヒアリングの対象	関連する研究実績および実務者を対象とする。主な対象研究、実務を以下に示す。 ・ 個人情報保護の研究および実務 ・ プライバシーマークの研究および実務 ・ その他プライバシー関連の研究および実務 ・ 著作権、肖像権関連の研究および実務
ヒアリングにおける仮説	・ 受容できない情報取得方法において情報取得および利用方法を告知することで受容性は向上する ・ 受容できない情報取得方法において告知方法を改善することで受容性は向上する

5.4.2 告知の有無によるユーザ受容性の調査結果

上記で示した各センサーおよびデバイスでの情報取得については、実機がユーザに確認できる状態で設置されているかおよび、告知の有無によって、ユーザの受容性が大きく変化することが考えられる。特に最新のセンサーやデバイスについては、小型化が進み、特定の環境において情報を取得される場合でも実機を容易に確認できない場合も存在する。これら実機の認識と告知の有無の関係が、ユーザの受容性にどのように影響するかをヒアリングによって確認した結果を下表に示す。ユーザが実機を確認できる場合は、実機有無の欄に“有”、実機を確認できない場合は“無”と示す。また、情報取得と告知内容については、ユーザが受容する項目については告知有無の欄に“○”、場合によって受容する場合は“△”、受容できない項目については“×”で示す。

表 5-8　想定する情報取得と告知の有無に関する受容性の結果

No	センサー/デバイス	実機有無	告知有無	
			有	無
1	カメラ（匿名化機能付）	有	○	×
		無	○	×
2	RFID タグ/IC カード	有	△	×
		無	×	×
3	赤外線センサー	有	○	×
		無	○	×
4	無線 LAN	有	×	×
		無	×	×
5	消費電力	有	○	×
		無	○	×

ヒアリングの結果では、無線 LAN デバイスのように、個人を特定できる（所持しているデバイスの固有の識別子を特定できる）場合は受容できない。また、告知を行わない場合の情報取得は受容できない結果である。一方、受容できる場合は、個人を特定できない情報取得で且つ、告知を実施している場合である。ただし、RFID タグおよび IC カードについては、場合により異なる。例えば、展示会やイベントにおいて事前に自らが登録した情報と関連付けられた RFID タグおよび IC カードを所持することによって情報を取得することが告知されているのであれば受容できるが、RFID タグおよび IC カードによる情報取得をユーザが確認できない状態で情報取得する場合は、受容できないという結果である。

取得する情報と環境特性に関する受容性の変化については、上記の通り、個人を特定できない情報（5.3.1(3)で示した領域 1、2）であれば、告知内容と方法を改善することで受容できる結果となっている。また、個人を特定できる情報（5.3.1(3)で示した領域 3、4）については、センシティブな商品や場所と関連しない情報取得（領域 3）が、センシティブな商品や場所と関連する可能性のある情報取得（領域 4）に比べ、受容しやすい傾向にある結果となっている。

5.5 事業者の透明性確保の調査

5.5.1 事業者ヒアリング調査

オプトインが必要とされるサービス、実証実験の内容と今後取得を考える情報を確認するため、事業者に対してヒアリングを行った。ヒアリング調査方法、調査結果について、以下に示す。

(1) ヒアリング調査方法について

事業者に対して実施したヒアリング調査の目的、対象および仮説を以下に示す。

表 5-9　事業者ヒアリングの概要

ヒアリングの目的	オプトインが必要とされるサービス、実証実験の内容と今後取得を考える情報の確認を目的とする。
ヒアリングの対象	特定環境において情報取得し、利用・管理する事業者および実証実験関連者を対象とする。
ヒアリングにおける仮説	・ 個人を特定できる情報の取得、利用については、個人情報保護法およびプライバシーマークを遵守する告知を実施している。 ・ 個人を特定できない情報の取得、利用については、告知を実施していないケースも存在する。 ・ ユーザからのクレームおよび問合せなどで大きな問題に発展する事案は発生していない。

(2) ヒアリング調査結果

環境オプトインに関連する事業者および実証実験者に対してヒアリングを行った結果、特定環境における情報取得の状況として以下のような結果が得られた。下表の通り、取得情報については、全ての事例で「個人が特定できない情報」として利用され、今後、個人を特定できる取得情報の追加は望まない結果である。この理由としては、個人を特定できる情報（個人情報）の取得や利用については、管理コストおよび告知に関する作業のコストが膨大になる可能性があり、想定するサービスとの比較において見合わないとの判断である。

また、情報取得する環境は、限定した環境において情報取得が行われているが、事例 4 においては、現在、さらに広範囲な環境に対する実証実験が開始されている。なお、事例 4 は一部の内容が実証実験に基づく内容であり、事例 5 は全て実証実験の内容である。

表 5-10　事業者ヒアリング結果の概要

事例 No	業種	取得デバイス	取得情報	追加取得したい個人情報	情報利用	取得環境	告知・承諾
1	情報通信業	カメラ	静止画、動画から推定した性別や年代、視認時間	なし	レコメンデーション、共通ポイントサービス、デジタルサイネージ	特定の施設内	事前に規約を示し承諾を得る
2	放送通信業	カメラ、マイク	イベント参加者および視聴者の映り込み（音声、動画）	なし	イベント等の放送および録画情報の出版（書籍、DVD 等）	イベント会場およびイベント会場の周辺	イベント会場内での告知
3	スポーツ・レジャー施設	カメラ、マイク	スポーツ観戦者およびイベント参加者の映り込み（音声、動画）	なし	イベント等の放送および録画情報の出版（書籍、DVD 等）	イベント会場およびイベント会場の周辺	なし

事例No	業種	取得デバイス	取得情報	追加取得したい個人情報	情報利用	取得環境	告知・承諾
4	鉄道・不動産業	GPS、交通 IC カード、ハウスカード	メールアドレス、移動情報、閲覧情報、利用サービス、購入情報	なし	ライフログ関連サービス、共通ポイントサービス（一部実証実験を含む）	特定の店舗・施設内	事前に規約を示し承諾を得る
5	広告業	カメラ、測定専用機器	総人数、通過人数、顔数および顔から推定した性別や年代、視認時間	なし	デジタルサイネージおよび効果測定に関する実証実験	駅、各種商業施設	基本的には取得環境で告知

さらに、告知・承諾については、事例 3 を除いて事前承諾、または取得環境における告知のいずれかが実施されている。

事例 3 については、個別にユーザに対して受容性を確認した結果、いわゆる個人情報保護法の制定前からスポーツ観戦時にスポーツ観戦者の姿が撮影、放映されることは知られている事実であり、個人情報の保護に関する法律（第五十条）[106]が存在すること。また、スポーツ中継や臨場感を伝える目的で撮影され、スポーツ観戦者を必要に撮影していないこと等を理由として、受容できるという結果である。なお、全ての事例について取得情報の取扱いおよび告知・承諾に関するユーザからの問合せやクレームは発生していないことが分かった。

5.6 新たなオプトイン方式（環境オプトイン）の成立要件の整理・分析

5.6.1 ヒアリング結果の分析

環境オプトインにおいて事業者とユーザの信頼関係を成立させる要件について検討した結果を以下に整理する。環境オプトインにおいて信頼関係を成立させるためには、情報取得の事実およびその方法や取得する情報など、情報の取得と利用に関する告知を向上させること。また、情報取得や利用を行う事業者がどのような管理を実施し、信頼性があるかを示すことが必要になると考えられる[107]。以下に具体的な三つのポイントについて示す。

(1) ガイドラインについて

環境オプトインを用いて情報取得を行う事業者は、情報取得を行う場合に、どのような利用制限を行い、取得した情報を管理するかの指針を求めている。また、事業者がどのような情報を取得・利用・管理するかをユーザへ告知することで、ユーザは情報の取得・利用の範囲が理解でき、その管理手法や体制も明らかになることから、安心することによって、双方の信頼関係を成立させることが可能になることが考えられる。

---

106 第五十条　個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部または一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。
一　放送機関、新聞社、通信社その他の報道機関(報道を業として行う個人を含む。)　報道の用に供する目的
２　前項第一号に規定する「報道」とは、不特定かつ多数の者に対して客観的事実を事実として知らせること(これに基づいて意見または見解を述べることを含む。)をいう。

107 個人情報をベースとしたパーソナライゼーションサービス利用の消費者選好に関する研究，高崎晴夫(KDDI 総研)，小野智弘(KDDI 研究所)，土生由希子(KDDI 研究所)，酒巻隆治(KDDI 総研)，電子情報通信学会，
http://www.jotsugakkai.or.jp/doc/taikai2010/A-1%20Takasaki.pdf

(2) マークについて

環境オプトインでは、特定の環境において様々なセンサーやデバイスによって情報取得するため、その環境において理解し易い方法でユーザに告知する必要がある。この方法としてマークによる告知が考えられ、マークによる告知を行うことで信頼性を向上させることが可能になると考えられる。

(3) 認定制度について

環境オプトインを利用する事業者が、本当に規定した管理策や、取得、利用の範囲を正しく守っているのかを示すためには、自らが保証するよりも第三者が確認し保証する方がより信頼性を向上させることができると考えられる。

5.6.2 環境オプトインのガイドラインについて

本項では、環境オプトインに対するガイドラインに関するヒアリング結果および検討結果を記載する。

(1) ガイドラインの必要性に関するヒアリング結果

以下に、ガイドラインの必要性に関して実施したヒアリングの結果を報告する。まず、ポリシーを Web 等による公開の必要性については、事業者は、関連する部分へのリンクを示すことで、管理策や管理体制を理解してもらう必要を感じていることが得られた。ユーザからは、公開ポリシー等へのリンクはあった方が安心感を増す（さらに安心できる）というコメントが得られた。

また、ガイドラインの必要性については、事業者では、一様に必要と感じている結果となった。現状では、本調査に関係するガイドラインが存在しないために、何をどの程度管理すべきなのか？が明確ではなく、ビジネスや事業化についても阻害される恐れがあるというコメントもあった。これらのコメントから、早急にガイドラインの策定を検討した方が望ましい状況であることが得られた。ユーザは、ガイドラインは一様に必要であるというコメントであった。このコメントの背景としては、事業者と異なるモチベーションであり、様々なガイドラインやポリシーが存在しても、理解し難いため、統一した記述が望ましいことから、ガイドラインで最低限必要と思われる告知、管理内容を簡潔にまとめて欲しい。という要求であった。具体的な内容については、以下に主なコメントの抜粋を示す。

表 5-11　ガイドラインに関するヒアリング結果の概要

	事業者	ユーザ
ポリシー公開の必要性	・公開する必要があると感じている。 ・撮影（捕捉）した情報や、行動履歴などは、個人を特定できない情報として利用しているため、現状の公開ポリシーに追記するという方針は馴染まないと考えている（また、本件では、以降も個人を特定できる情報を利用することは考えていないため、公開ポリシーに追記することはないと考えている）。	・掲載していた方が安心する。 ・いろいろなポリシーが乱立すると理解できないので、統一フォーマットにして欲しい（ガイドラインで示すべきだと思う）。
ガイドラインの必要性	・ガイドラインの必要性は感じている。 ・ガイドラインがないと、実証実験もできないので、ビジネス化・事業化できない。 ・取得したい情報や、その利用は事業者によって様々だと思うため、統一ガイドラインが必要であるか疑問である。	・統一していた方が、理解し易いので、あったほうがよい。
ガイドラインに何を求めるか	・管理コストを考えると、簡易的である方が望ましい。 ・FTC の行動履歴捕捉に関する自主規制原則が、理解し易いので、この差分を考えると、簡単に作成できるのではないか。	・個人を特定できない情報であれば、少なくともプライバシーマークよりも簡易化され、理解し易くするべきだと思う。 ・個人を特定できない情報であれば、保存期間は明記しなくてもいい（捕捉の仕方だけ気になる）。 ・理解し易くないと見ないと思うので、第三者提供の有無を簡潔に示すことや、現状の公開ポリシーとの差分を明確に示すなど。

(2) ガイドラインで規定すべき内容の整理

環境オプトインを実現する上で、必要と考えられるガイドラインについて検討した結果を報告する。ガイドラインの検討については、事業者視点のヒアリングにおいて、一部の企業の社内検討では FTC[108]の行動ターゲティング広告における自主規制原則[109] [110]の内容を参

108 FTC：Federal Trade Commission(米国連邦取引委員会)

109 Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles, Federal Trade Commission,
http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

110 FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising, February 2009, Federal Trade Commission,

考に検討を進めているという事例が存在した。そのため、ガイドラインの検討については、まず、FTC の自主規制原則の内容を環境オプトインに適用した場合について検討する。以下に、FTC の自主規制原則を示す。

①透明性とユーザによるコントロール

・ 行動ターゲティング広告のために情報を収集する事業者は、これらのサービス活動およびサービスの受入／拒否についてユーザが決定するのに役立つ情報をユーザに開示しなえればならない。

②情報に対する合理的セキュリティの確保とデータ保持の制限

・ 行動ターゲティングデータを不正者が入手することがないよう、合理的なセキュリティ対策を提供し、データの保存を正当なビジネスおよび法執行に関して必要な期間内に限定しなければならない。

③既存のプライバシー関連の制約に関して重要な変更に対する能動的かつ明示の同意

・ 事業者が行動ターゲティングデータについて、収集時点で事業者が規約した内容について実質的に異なる方法で使用する場合は、事前に能動的かつ明示の同意をユーザから取得しなければいけない。

④行動ターゲティング広告のためのセンシティブなデータの使用に対する能動的かつ明示の合意（または禁止）

・ 例えば子供や健康および、金融などに関連するセンシティブなデータを事業者が行動ターゲティング広告に利用する場合には、消費者から能動的かつ明示の同意を取得しなければならない。

○追加

・ ターゲティングデータを行動ターゲティング広告以外の目的で使用する可能性については追跡情報を求める。また、そうした二次的利用が懸念を示し、より高度な保護が必要となるか否かについての情報を必要とする。

図 5-6　FTC 産業界による自主規制原則

本調査において実施した事業者へのヒアリング結果では、環境オプトインで想定している情報の利用目的は、広告サービスの精度向上および、人の行動、流量確認など統計データとしての限定的な利用であって、その他の二次的な利用は想定されていない。

また、FTC の「行動ターゲティング広告における自主規制原則」を受け、JIAA[111]が「行動ターゲッティング広告ガイドライン」を策定している。このガイドラインでは、14 項目を示している。詳細な検討を行う上で、JIAA のガイドラインを参考に検討を進める。14 項目について以下に示す。

http://www.ftc.gov/os/2007/12/P859900stmt.pdf

[111] インターネット広告推進協議会

① 取得の事実
② 対象情報を取得する事業者の氏名または名称
③ 取得される情報の項目
④ 取得方法
⑤ 第三者提供の事実
⑥ 提供を受ける者の範囲
⑦ 提供される情報の項目
⑧ 利用目的
⑨ 保存期間
⑩ 利用者関与の手段
⑪ 個人を特定できない情報の利用である旨の明示
⑫ 個人情報取り扱いに関するポリシー（もしくはそこへのリンク）
⑬ 参画企業でのガイドライン遵守の明示
⑭ 各社がそれぞれに留意・配慮している領域

図 5-7 JIAA 行動ターゲティング広告ガイドライン

また、関連する認定制度としては、個人情報保護に関するコンプライアンス・プログラムの要求事項である JISQ15001:2006 が存在し、3.4.2.4 項に「本人から直接書面によって取得する場合の措置」が示されている。

本調査では、JIAA の「行動ターゲティング広告ガイドライン」の項目についてヒアリングの結果（事業者およびユーザを含む）から要／不要を検討し、これらの結果について、JISQ15001:2006 の 3.4.2.4 項に対する充足を確認した。ヒアリング結果と主に JISQ15001:2006 の充足・比較を行うことで、JISQ15001:2006 の認定取得企業は、環境オプトインを実施する上で、何を規定、告知すべきかを示すことが可能となる。JISQ15001:2006 の 3.4.2.4 項を以下に示す。

a) 事業者の氏名または名称
b) 個人情報保護管理者(若しくはその代理人)の氏名または職名，所属および連絡先
c) 利用目的
d) 個人情報を第三者に提供することが予定される場合の事項
　d1) 第三者に提供する目的
　d2) 提供する個人情報の項目
　d3) 提供の手段または方法
　d4) 当該情報の提供を受ける者または提供を受ける者の組織の種類，および属性
　d5) 個人情報の取扱いに関する契約がある場合はその旨
e) 個人情報の取扱いの委託を行うことが予定される場合には，その旨
f) 3.4.4.4～3.4.4.7[112] に該当する場合には，その求めに応じる旨および問合せ窓口
g) 本人が個人情報を与えることの任意性および当該情報を与えなかった場合に本人に生じる結果
h) 本人が容易に認識できない方法によって個人情報を取得する場合には，その旨

図 5-8　JISQ15001:2006：3.4.2.4 項

以下に「行動ターゲティング広告ガイドライン」および JISQ15001:2006 の「3.4.2.4 項」の比較とそれらの項目に対するヒアリング結果から考察した結果を示す。前項で示した通り、環境オプトインで想定している情報は、個人を特定できない情報であり、第三者提供は想定されていないため、下表ではヒアリング結果欄に「任意」と示す。また、ポリシー、ガイドライン、留意・配慮している領域など、事業者が任意に告知すべきと考える内容についてもヒアリング結果欄に「任意」と示す。

表 5-12　ガイドラインで規定すべき事項の検討結果

行動ターゲティング広告ガイドライン(JIAA)の項目	JISQ15001:2006 の 3.4.2.4 項目	ヒアリング結果	
		ガイドライン（ポリシー等として公開）	マーク（現場での告知）
① 取得の事実	本 3.4.2.4 項により規定	必要	必要
② 事業者の氏名または名称	a) 事業者の氏名または名称	必要	必要
—	b) 個人情報保護管理者	任意	
③ 取得される情報の項目	d3) 提供の手段または方法	必要	必要
④ 取得方法		必要	必要

[112] 3.4.4.4(開示対象個人情報の利用目的の通知)、3.4.4.5(開示対象個人情報の開示)、3.4.4.6(開示対象個人情報の訂正、追加または削除)、3.4.4.7(開示対象個人情報の利用または提供の拒否権)

行動ターゲティング広告ガイドライン(JIAA)の項目	JISQ15001:2006 の 3.4.2.4 項目	ヒアリング結果	
		ガイドライン（ポリシー等として公開）	マーク（現場での告知）
⑤ 第三者提供の事実	e) 個人情報の取扱いの委託を行うこと	任意	
⑥ 提供を受ける者の範囲	d4)当該情報の提供を受ける者	任意	
⑦ 提供される情報の項目	d2) 提供する個人情報の項目	任意	
⑧ 利用目的	c) 利用目的	必要	任意
	d1) 第三者に提供する目的	任意	
	d5) 個人情報の取扱いに関する契約	任意	
⑨ 保存期間	3.4.3 適正管理により規定	任意	
⑩ 利用者関与の手段	g) 本人が個人情報を与えることの任意性および当該情報を与えなかった場合に本人に生じる結果	必要	不要
⑪ 個人を特定できない情報の利用	h) 本人が容易に認識できない方法によって個人情報を取得	必要	必要
⑫ 個人情報に関するポリシー	3.4.3.2 安全管理措置により規定	任意	不要
⑬ ガイドライン遵守の明示	上記同様	必要	任意
⑭ 留意・配慮している領域	f) 3.4.4.4～3.4.4.7 に該当する場合	任意	不要

ユーザ視点のヒアリング結果において、⑪個人を特定できない情報として利用するのであれば、保存期間の告知を求めるという意見はなかった。上表のヒアリング結果欄に「必要」と示した 8 項目については、少なくともガイドラインとして規定する必要があり、各々の項目を公開ポリシーなど Web で告知することが求められていることが分かった。

5.6.3 環境オプトインのマークについて

本項では、環境オプトインのマークに関するヒアリング結果および検討結果を記載する。

(1) 環境オプトインのマークに関するヒアリング結果ついて

環境オプトインのマークの必要性に関して実施したヒアリングの結果を以下に示す。

事業者の主なコメントとしては、情報取得する環境において告知することで説明責任を果たすこと。また、クレームの事前回避策として、情報を取得していることを告知した方がよいと考えている。一方、デジタルサイネージ等では、宣伝効果を正しく測定する目的で、効

果測定をしている事実自体を意識させることがない配慮も必要というコメントもあった。

ユーザの主なコメントとしては、何も告知されず情報を取得（捕捉）されるのは納得できない。というコメントが多くあった。一方、スポーツ観戦時に撮影された画像が放送される場合など、既に情報取得と利用が理解されている場合は、あえて告知する必要を感じないというコメントもあった。具体的な内容については、以下に主なコメントの抜粋を示す。

表 5-13　マークに関するヒアリング結果の概要

	事業者	ユーザ
情報取得する環境での告知	・問合せやクレームを回避するために必要だと感じている。 ・宣伝効果の測定結果の正しさを求める場合は、捕捉していることを告知しないという考え方もある。	・記載されないと納得できない。 ・カメラが小型化して存在がわからない場合も撮っていることは告知すべきだ。 ・いわゆる個人情報保護法に比べ、歴史的に古い「スポーツ観戦」による映り込みの事実については理解しているので告知していなくともよいと思う。 ・個人を特定できない情報であれば、少なくとも情報を取得していることと、個人を特定できない情報として扱うことを示せば受容できる場合が多いと考える。
マークの必要性	・安価に取得できる認定マークであれば、信頼性を向上させるために検討したい。 ・安全な施設運用や移動手段の連携においては、人の流動・流量情報の取得は必要である。このような利用目的に見合うマークも必要である。	・あった方が理解し易いし、安心する。 ・マークを貼る位置にも配慮が必要（普段は見ない天井等ではなく高い確率で見える出入り口のドア等に張る必要がある）。 ・個人を特定できる情報を取得する場合は、マークで示しても、いわゆるデフォルト・オプトインと解釈できるので賛成できない。

(2) マークで示すべき要件の整理

環境オプトインを実現する上で、必要と考えられるマークについて検討した結果を以下に示す。マークの検討については、マーク自体に盛り込むべき事項を検討した結果を示す。また、マークの検討については、告知すべき事項を図や画像として直感的に示すことが必要である項目と、マークに文字を記載することが望ましい項目がある。下表において、図や画像で示すことが必要である項目は、ヒアリング結果を踏まえ検討した結果欄に、「マークに図として記載する」と表し、マークに文字を記載することが望ましい項目は、「マークに文字

を記載する」と表す。なお、①取得の事実については、今後、検討するマーク自体の認知度が向上すれば、マーク自体を示すことで理解されることを考え、「マーク自体で示す」と記載している。また、マークで示すべき要件の整理には、前項のガイドラインの検討と同様にヒアリング結果を反映し、環境オプトインで想定している情報は個人を特定できない情報であり、第三者提供を想定していないことを前提とする。

表 5-14　マークで規定・告知すべき事項の結果

行動ターゲティング広告ガイドライン(JIAA)の項目	ヒアリング結果を踏まえ検討した結果(マークによる現場での告知)
① 取得の事実	マーク自体で示す。
② 事業者の氏名または名称	マークに文字を記載する。
③ 取得される情報の項目	マークに図として記載する。
④ 取得方法	マークに図として記載する。
⑤ 第三者提供の事実	（任意：存在する場合はガイドラインに示す）
⑥ 提供を受ける者の範囲	（任意：存在する場合はガイドラインに示す）
⑦ 提供される情報の項目	（任意：存在する場合はガイドラインに示す）
⑧ 利用目的	（任意）
⑨ 保存期間	（任意：存在する場合はガイドラインに示す）
⑩ 利用者関与の手段	（任意）
⑪ 個人を特定できない情報の利用	マークに図として記載する。
⑫ 個人情報に関するポリシー	（任意：存在する場合はガイドラインに示す）
⑬ガイドライン遵守の明示	適用するガイドライン、第三者認定制度などがあれば、マークに図案として示す。
⑭留意・配慮している領域	（任意：存在する場合はガイドラインに示す）

上記の告知すべき項目について、以下に例示を示す。①取得の事実については、マーク自体で事実を示し、②事業者の氏名または名称は直接明記し、③取得される情報の項目、④取得方法は例示では、カメラによる取得であることを示している。

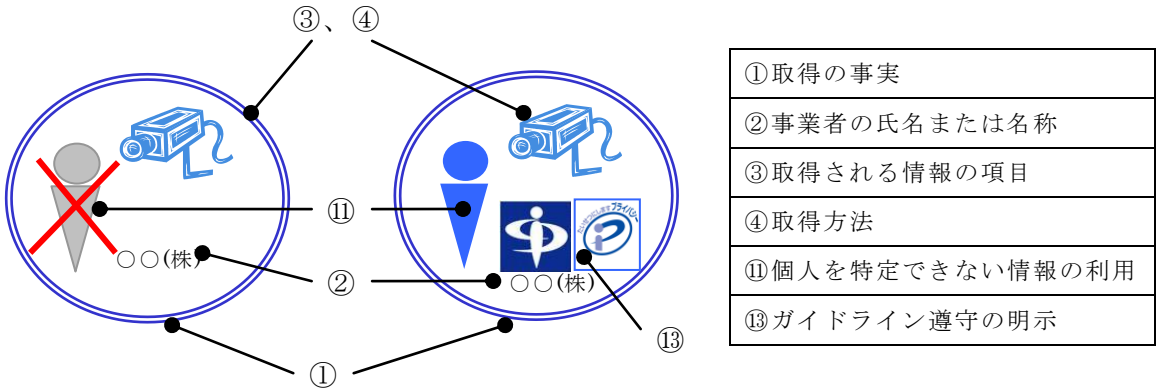

図 5-9　マークによる告知事例

また、⑪個人を特定できない情報の利用では、マーク案（左側）では個人を特定できない情報として取得することを表し、マーク案（右側）では個人を特定できる情報として取得することを表した例示である。また、事業者がプライバシーマーク付与事業者である場合は、マーク案（右側）で示した通り、⑬ガイドライン遵守の明示として認定取得マークを含める。なお、⑧利用目的および⑩利用者関与の手段の図案については、さらに検討を行う必要がある。

5.6.4 環境オプトインに対する第三者認定制度について

本項では、環境オプトインに対する第三者認定制度に関するヒアリング結果および検討結果を記載する。

(1) 第三者認証制度の必要性に関するヒアリング結果ついて

第三者認証制度の必要性に関する事業者へのヒアリングによると、第三者認証制度については、安価であれば運用を検討するという意見が多かった。また、情報取得および管理主体が匿名化処理を行っていることをユーザに告知している場合でも、実際の施工者および SIer などが不正なカメラの取り付けやシステムを不正に操作し、匿名化処理の迂回を行っている可能性もあり、正しく匿名化処理されていることを情報管理主体がユーザに証明することが望ましいと考えると、システム上および技術的に不正がないことも安価に認証する制度が必要という回答も得られた。

一方、ユーザへのヒアリングによると、第三者が認証することで安心感が増すためよいという回答が多かった。また、安心感を増すと同時に、認定取得の証をマークとして明示することで、視覚的にも理解し易くなることが期待できる。ただし、マークを明示する場合は、直感的に理解し易いマークである必要があるという回答があった。

個人の特定が可能な情報である場合は、個人情報の取得となるため、プライバシーマーク付与事業者と同程度の管理策が求められる。この場合は、プライバシーマーク付与事業者であれば管理策を追加する必要はないという回答が多い。さらに、個人を特定できない情報である場合は、プライバシーマーク付与事業者よりも簡易的な管理策でもよいという回答もあった。

なお、認定マークを策定する際には、類似のマークによる誤解を与えないための対策（商標登録等）も必要という指摘もあった。

具体的な内容については、以下に主なヒアリングの回答の抜粋を示す。

表 5-15　第三者認定制度に関するヒアリング結果の概要

	事業者	ユーザ
確認・認証スキームや制度について	・安価であれば運用を検討する。 ・不正なカメラやシステムではないことを検査するスキームは欲しい（本当に匿名化処理しているのか？というのは、メーカーではわからず、SIer などの不正を見抜けない。そのため、不正なカメラでないことを証明したい）。 ・単純なルールでないと利用されない。 ・説明責任を果たすという観点から、ガイドライン、マーク、認定制度はセットで考えるべきである。	・第三者が確認する制度はあった方が安心する。 ・ガイドラインやポリシー系の確認と機器・システムの確認という二段階になると思う。 ・プライバシーマーク付与事業者であれば利用目的を公表するだけで追加認定は不要と思える。

(2) 第三者認証制度の検討課題ついて

環境オプトインを実現する上で、検討すべき第三者制度としては、情報管理系のマネジメントシステムに関する第三者認定制度と、IT システム系の第三者認定制度がある。双方の第三者認定制度の実現可能性については、主に、認定取得コストの軽減が重要であり、認定取得金額および期間等を如何に削減できるかが、普及のための課題であると考えられる。

この認定取得コストの削減方法については、情報管理系のマネジメントシステムでは、環境オプトインで告知、管理する項目において親和性があるプライバシーマーク(JISQ15001:2006)を流用することも考えられる。プライバシーマークの流用については、前述のガイドライン検討で示した通り、管理、告知する項目は重複した部分が多いため、企業内の管理体制については、「プライバシーマーク付与事業者」に対しては簡易的な確認のみとすること等が考えられる。

また、IT システム系の第三者認定制度については、JISEC(ISO/IEC 15408)が想定される。JISEC[113]とは、「IT セキュリティ評価および認証制度(JISEC:Japan Information Security Evaluation and Certification Scheme)」であり、IT 関連製品のセキュリティ機能の適切性・確実性を、セキュリティ評価基準の国際標準である ISO/IEC15408 に基づいて第三者（評価機関）が評価し、その評価結果を認証機関が認証する、わが国の制度である。しかし、JISEC の評価コストは、本調査で想定している評価コストよりも高くなる可能性があるため、一部のスキームを流用し、確認するポイントを適切に絞る方法などを考え、確認作業を低減しつつ確実に確認できる実施方法を検討する必要がある、例えば、開発資料の確認や想定されるアーキテクチャ等を示すことで、評価・確認する項目を少なくさせる方法である。

113 情報処理推進機構： IT セキュリティ評価および認証制度(JISEC),
http://www.ipa.go.jp/security/jisec/scheme/index.html

5.7 まとめ

本調査により、技術の進展から各種センサーやカメラによるデータ取得など情報収集は実際に行われていることが分かった。また、デバイスからの情報収集については、オプトインは行っているものの、店舗等へ設置した機器による情報収集については、十分な告知が行われている状況ではないことが分かった。

一方、ユーザの受容性の面では、どのようなデータが取得されているのか分からないため不安感があり、特にセンシティブな商品や場所に関連する場合は抵抗感が高いことが分かった。

これらの結果を踏まえると、サービス業の進展や技術の高度化により各種センサーの利用はより進んでいくものと考えられ、その場合に、来訪者に対して何らかの告知（環境オプトイン）は必要であると考えらえる。

本調査では環境オプトインの成立要件として、「ガイドライン」、「マーク」、「第三者認証」について整理したが、環境オプトインの具体化に向けて以下に挙げるポイントの検討が引き続き必要であろう。

- ユーザへの告知内容と方法
  - 取得の目的、方法、データの様態について示すべきか
  - 明示方法は、Web だけで良いのか
- 感覚で理解できるマーク
  - 業界の合意による目印で良いか
  - 第三者の認証に基づく目印が良いか
- 各種センサーやカメラのデータ取得に対するオプトアウト
  - オプトアウト申請時点で、個人が特定されてしまうのではないか
  - どの様にデータを消去すべきか。管理方法はどうすべきか
- 国際連携の検討
  - トラストマークをはじめ、国際的に議論が高まっている

これらのポイントを踏まえ、より具体的な検討がなされ、実証実験等によりその効果が示していくことが重要であると考える。

禁　無　断　転　載

平成２３年３月発行

発行所　財団法人　日本情報処理開発協会

東京都港区芝公園３－５－８
機械振興会館内
ＴＥＬ（３４３６）７５００

印刷所　株式会社　サンワ

東京都千代田区飯田橋２－１１－８
ＴＥＬ（３２６５）１８１６

22-H006