国立研究開発法人情報通信研究機構
高度通信・放送研究開発委託研究
における
パーソナルデータの取扱いに関するマニュアル

平成 29 年 6 月

国立研究開発法人情報通信研究機構
イノベーション推進部門
委託研究推進室

目　次

はじめに

国立研究開発法人情報通信研究機構（以下「機構」という。）では、**パーソナルデータの扱いについて、**機構内の各研究室等が主体となって行う研究開発だけではなく、**共同研究、委託研究、受託研究も含めた**マニュアルが策定されております。本マニュアルは、当該マニュアルをベースに高度通信・放送研究開発委託研究（以下「委託研究」という。）に関する部分について、抜粋、追加修正を一部加え、受託者向けに再構成したものです。

委託研究の受託者においては、本マニュアルを参照して委託研究を実施して下さい。

1.　本マニュアルの目的

ICT の発展及び普及により、現実世界に関する様々な情報を大量に取得することが可能になっています。その中で、ＰＣやスマートフォンを通じて取得される位置情報や購買履歴、カメラ等のセンサにより取得される顔認識情報などの個人に関する情報（いわゆるパーソナルデータ）についても利活用が期待されています。

一方、これらのパーソナルデータには個人のプライバシーに関する情報が含まれる場合があり、その取扱いを間違えると、そのデータの本人の権利侵害を引き起こし、ひいては社会的な非難にさらされることにもなりかねません。このような事態を招かないためにも、パーソナルデータの取扱うにあたっては、事前のアセスメントを行い、取扱い上のリスクを認識し、これらリスクへの対応策を講じておく必要があります。

本マニュアルは、委託研究におけるパーソナルデータを扱う研究開発の推進にあたり、プライバシーをはじめとする個人の権利利益の侵害や、それら侵害への懸念から生じる機構や受託者への社会的評価の毀損といったリスクを最小限のものとするため、委託研究におけるパーソナルデータの取扱いを説明したものです。

2. 背景

ICT の進展により、多様で膨大なデータの収集及び分析が可能となっており、これら「ビッグデータ」の利活用の機運が高まっています。機構においても、第 4 期中長期計画において、ビッグデータや IoT、人工知能等のＩＣＴ分野の技術についても積極的に取り組むこととなっています。

一方で、これには個人に関する情報（パーソナルデータ）が含まれることも多く、その利活用に対してはプライバシー侵害の懸念が指摘されており、実際に問題化する事例も発生しています。

従来は、個人情報保護法に基づいて個人情報（特定の個人を識別できる情報）を保護していればプライバシーの問題はあまり発生していませんでした。しかし、ICT の進歩により、必ずしも個人情報ではないと考えられる情報からプライバシーの侵害が発生するといった事態も起きています。

機構としては、パーソナルデータを取扱う研究開発を円滑に実施していくために、組織として適切にパーソナルデータを取り扱うための環境を整備していくことが必要となっています。特に、パーソナルデータの不適切な取扱いにより、データを提供する本人の権利を侵害することのリスクや、権利侵害の懸念から生じる社会的な批判等のリスクに対処することが重要となっています。

3.　パーソナルデータ等の定義と範囲

3.1.　パーソナルデータ、個人情報、プライバシー侵害の可能性がある情報

（１）概要

本マニュアルでは「パーソナルデータ」、「個人情報」、「プライバシー侵害の可能性のある情報」を区別しています。

「パーソナルデータ」、「個人情報」、「プライバシー侵害の可能性のある情報」は、次の（２）～（４）で説明しますが、それぞれに異なる概念です。

これら相互の関係を示すと図　3-1 のようになります。個人情報とプライバシー侵害の可能性のある情報は重複している部分もありますが、必ずしも一致しません。

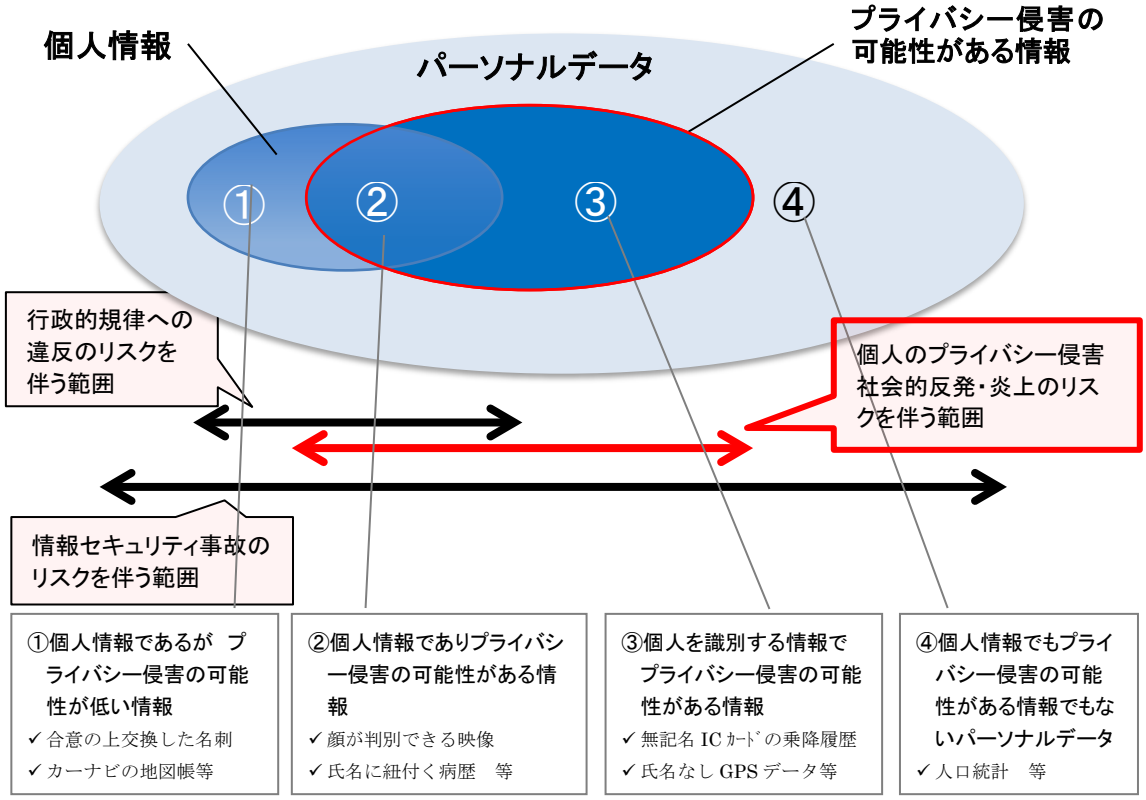

図 3-1　３つの情報の関係

（２）「パーソナルデータ」とは何か。

パーソナルデータとは法令上の用語ではなく、統一的な定義も存在しませんが、国における議論の中では、「個人の行動、状態等に関するデータ、従来の個人情報の定義では必ずしもとらえきれないものを含む」、「個人に関連するデータの総称」等とされています。次に示す個人情報よりも範囲が広く、個人に関する情報全般を指すことが多いです。

本マニュアルにおける定義及び具体例については、3.2 で説明します。

（３）「個人情報」とは何か

「個人情報」という言葉は、一般にもよく使われていますが、本マニュアルでは法律で定義された意味で用います。

個人情報保護法の改正案が平成 28 年 5 月に第 190 回国会で成立し、平成 29 年 5 月 30 日に全面施行されました。改正法では、個人情報の定義が以下のとおり明確化されています。

「生存する個人に関する情報であって、次の各号のいずれかに該当するもの。

一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。以下同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

二　個人識別符号が含まれるもの」　　（改正法第 2 条第 2 項）

また、改正法では、「要配慮個人情報」というカテゴリーが設けられました。要配慮個人情報とは、

「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」（改正法第２条第４項）

と定義されています。

その他、主な改正ポイントを付録にまとめています。

（４）「プライバシー侵害の可能性がある情報」とは何か

(ア)「プライバシー」とは何か

「プライバシー」は、法令上明文で定義されていませんが、判例において民法上保護される個人の権利利益として位置づけられており、プライバシーを侵害したと認められると民法上の責任を問われることになります。

判例等におけるプライバシーの定義は一様でありませんが、裁判所がプライバシー権を法的に保障された権利として初めて認めた「宴のあと事件」判決（東京地判昭和 39・9・28）では、

公開された内容が

(イ)私生活上の事実または私生活上の事実らしく受け取られるおそれのあることがらであること、

(ロ)一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められることがらであること、換言すれば一般人の感覚を基準として公開されることによって心理的な負担、不安を覚えるであろうと認められる

ことがらであること、

(ハ)一般の人々に未だ知られていないことがらであること

を必要とし、かつこのような公開によって当該私人が実際に不快、不安の念を覚えたことを必要とする、とされています。

(イ)「プライバシー侵害の可能性がある情報」とは何か

本マニュアルにおいて、「プライバシー侵害の可能性がある情報」は、**本人にとって他の人に知られることによってプライバシーが侵害されるような機微な内容を含む情報**が該当します。

あるデータが「プライバシー侵害の可能性がある情報」かどうかは、上記判例等を踏まえながら、データごとに個別に判断する必要があります。

つまり、プライバシーは個々人の主観やデータの使われ方等にも依存することや、個人情報を匿名化した情報や統計処理した情報であっても他の情報との照合で特定の個人を識別することによりプライバシーを侵害する可能性があることから、「プライバシー侵害の可能性のある情報」であるか否かを（個人情報のように）データの外形のみで判断することは困難です。

（２）で述べた個人情報（特定の個人を識別できる情報）だからといって、必ずしもプライバシーが侵害されるわけではなく、プライバシー侵害のおそれのない個人情報もあります（例：合意の上で交換した名刺の情報)。逆に、個人情報でない(特定の個人を識別できない情報)だからといって、プライバシーが侵害されることがないわけではありません（例：交通用無記名ＩＣカードにおける乗降履歴)。このため、図 3-1 で示したように、個人情報とプライバシー侵害の可能性のある情報は、重複している部分もありますが、必ずしも一致しません。

ただし、改正独法等個人情報保護法で新たに定義された「要配慮個人情報」(前述（３）を参照）は、プライバシー侵害の可能性のある情報」に含まれるものと考えられます。

（５）「パーソナルデータ」、「個人情報」、「プライバシー侵害の可能性のある情報」を取り扱う場合のリスク

委託研究において、「パーソナルデータ」、「個人情報」、「プライバシー侵害の可能性のある情報」を取り扱うことには、それぞれリスクが存在します。想定されるリスクとしては、以下のものが考えられます。これらのリスクとパーソナルデータの関係は図 3-1 に示しています。

(ア)プライバシー侵害の可能性のある情報の取扱いにおいて、個人のプライバシーを侵害するリスク

（例：民法上の責任を負い、損害賠償等の義務が発生。）

(イ)個人情報の取扱いにおいて法令等に違反するリスク

（例：個人情報保護法、受託者組織での個人情報等管理規程などへの抵触、それに伴う官庁からの指導等。）

(ウ)プライバシー侵害への懸念から生じる社会的反発・炎上が発生するリスク

（例：パーソナルデータの取扱いに対して、個人の不安、気持ち悪さ等に起因してメディア等で批判の声が広がる等により、受託者や委託元である機構の社会的信用の毀損等が発生。法令を遵守していたとしても発生しうるものであり、昨今、市民の関心や要求が高まりから、リスクが増大。）

(エ)情報セキュリティ事故が発生するリスク

（例： 管理の不行届き等によるパーソナルデータの漏えい、滅失、毀損等）

3.2.本マニュアルの対象であるパーソナルデータを判断する観点と具体例

（１）本マニュアルの対象とするデータの範囲について

本マニュアルの適用対象となるデータの範囲は、**研究開発の対象として取得、利用・分析等を行うパーソナルデータ**です（研究開発を進める上で取得した他機関の研究者に関する個人情報等は除く）。「プライバシー侵害の可能性のある情報」や「個人情報」でなく、「パーソナルデータ」とした理由は以下のとおりです。

(ア)本マニュアルは、研究開発業務において、プライバシー侵害等を引き起こすおそれのあるデータについて、その取扱い方法を定めたものです。その観点からは、プライバシー侵害の可能性のある情報だけを対象にして扱えばよいと思うかもしれません。

(イ)しかし、前述したとおり、プライバシー侵害の可能性のある情報は類型化することは困難です。また、長期的にパーソナルデータを取得することによりそのデータ提供者の行動履歴や嗜好、さらには行動パターンまでわかる場合があります。この場合、データの取得者はデータ提供者との信頼関係が担保されていなければ、プライバシー侵害の可能性があると批判されるリスクがあります。さらに、個人情報を匿名化した情報であっても他の情報との照合により特定の個人を識別できた事例もあります。

(ウ)以上を踏まえ、受託者や委託元である機構のリスクを管理する観点から、対策を講じるデータの対象を個人情報やプライバシー侵害の可能性のある情報（前述したとおり、これを類型化することは困難。）だけではなく、より広い概念であるパーソナルデータ（個人に関する情報）とすることとしています。

（２）パーソナルデータか否かを判断する観点

ただし、（１）の記述だけでは判断に迷う場合もあると思いますので、以下で、パーソナルデータか否かを判断する観点を次に説明します。それでも迷う場合には、機構イノベーション推進部門委託研究推進室担当者までご連絡ください。

(ア)判断する観点

あるデータがパーソナルデータか否かの判断は、**「人についてのデータ」（人の行動に伴って記録されるデータや人そのもの（生体等）について記録されるデータ）であるか、又は「人が生成（記録）するデータ」（風景の写真、モノのことが書かれたＳＮＳ等）であるか、**という観点で行います。どちらの判断基準にも該当しないデータについては、パーソナルデータには当たらないと判断します。

(イ)パーソナルデータに該当しない例

パーソナルデータに該当しない例として以下を示します。

＜パーソナルデータに **該当しない** 例＞

- 気象レーダーが収集するデータ
- 電離層や太陽電波観測のデータ
- 水位計が記録する河川のデータ
- 部屋に設置されたＩｏＴ機器のＩＰアドレス、ＭＡＣアドレス

(ウ)パーソナルデータに該当する例

次に、パーソナルデータの具体例を以下に示します。なお、これらはあくまでも例であり、パーソナルデータはこれらに限定されるものではありません。

＜パーソナルデータに **該当する** 例＞

- カメラ・センサデータ（人物を撮影したもの）
  - ◆ カメラによる施設利用者の映像データ
  - ◆ ドローン搭載カメラから撮影された映像データ
  - ◆ ロボット制御目的で得られたカメラ・センサデータ
  - ◆ MRI/内視鏡/CT 等により得られた映像・画像データ
- 端末に関するデータ
  - ◆ 端末 ID（IP アドレス、MAC アドレス等）
  - ◆ アプリインストール ID
  - ◆ アプリ利用時刻
  - ◆ アプリへの入力情報（文章や図形）
- 位置データ
  - ◆ 携帯電話位置情報
  - ◆ 車プローブ情報
  - ◆ 住宅地図情報

    ※事業者が販売するものも含む。
- 生体データ

- ◆ 音声データ（スマートフォンによる音声収録）
- ◆ 音声データの書き起こしテキスト
- ◆ 指尖脈波データ
- ◆ 脳活動データ
- ◆ 人体の形状に関する測定データ
- ◆ 機械の遠隔操作時における人の行動計測データ
- ◆ カルテ・処方箋

・ 心理計測データ

- ◆ 知覚・認知に関する心理データ（アンケート等）
- ◆ 立体映像視聴における疲労感等の主観評価データ

・ データの分析により得られるデータ

- ◆ 特徴量情報（映像情報を処理して得られる個人識別に利用可能な情報など）
- ◆ 移動経路情報（個人が、いつ、どこを動いたかを表す情報）
- ◆ 音声認識結果
- ◆ 機械翻訳結果
- ◆ 心身リズムの推定結果

・ 被験者に関する情報

- ◆ 氏名、生年月日、出身地域、年代、性別、収録地域
- ◆ 施設・設備利用ログデータ

・ ＷＥＢ関係のデータ

- ◆ Web テキスト
- ◆ Web 音声データ（動画内の音声トラック含む）
- ◆ Web 画像データ
- ◆ Twitter へ投稿されたツイート情報
- ◆ Twitter アーカイブデータ
- ◆ 位置情報付き SNS

4.　パーソナルデータの取扱体制

4.1.　基本的な考え方

パーソナルデータのうち、プライバシー侵害の可能性のある情報や個人情報を不適切に取り扱う（例：本人の同意なく取得する、本人の同意なく第三者へ提供する）と、3.1（５）で示したように、プライバシー侵害、法令違反、機構に対する社会的な非難や批判といった事態を引き起こす可能性があります。一旦、そのような事態が発生すると、その解決には多くの労力と時間を要することになります。

そのため、本マニュアルによって、プライバシー侵害等の事態の発生を「予防」するとの考え方のもとで、パーソナルデータを取扱う体制を整備しています。つまり、パーソナルデータを利用する研究開発については、なるべく早い段階から、組織として把握し、プライバシー侵害等が発生しないような予防策を事前に講じていくこととしています。

なお、これらプライバシー保護のための体制・対策の検討に当たっては、プライバシー保護施策の世界的な標準になりつつある「プライバシー・バイ・デザイン」という考え方を参考にしました。

（参考）プライバシー・バイ・デザイン

プライバシー・バイ・デザイン(Privacy by Design)とは、1990 年代にカナダのアン・カブキアン博士が提唱した「システムやビジネスプロセスの設計段階からプライバシー対策を考慮し、企画から保守までのライフサイクル全体で一貫したプライバシー保護を行う」という概念です。この概念の導入・実施に当たっては、リスクを事前に評価し、リスクを低減化するための方策を講じることが重要と考えられています。

プライバシー・バイ・デザインでは、以下の７つ基本原則が提案されています。

- 事後的ではなく事前的：プライバシー侵害の救済策を考えるのではなく予防策を考える。
- デフォルト設定：デフォルト状態のシステムやビジネスでプライバシーが保護される。
- 設計に組み込まれるプライバシー：設計段階からシステムやビジネスにプライバシー対策が組み込まれている。
- ゼロサムではなくポジティブサム：セキュリティ対策等とプライバシー保護はトレードオフではなく、Win-Win の関係である。
- 最初から最後まで：データのライフサイクル全体でプライバシーが保護される。
- 可視性と透明性：プライバシー対策は全てのステークホルダーから可視的、透明である。
- 利用者のプライバシー尊重：システムやビジネスの設計者、管理者は、利用者のプライバシーを最大限に尊重する。

4.2.　パーソナルデータを取扱うための基本方針

パーソナルデータを取り扱う受託者が、共通に認識すべき事項を以下の［パーソナルデータを取扱うための基本方針］に示します。

透明性の確保
パーソナルデータの利用に関し、データの取得、管理、利用等について、データの提供者本人から同意を取得、あるいは通知又は容易に知りえる状態に置くこと

目的の明確化・必要最小限の取得
パーソナルデータの利用目的はできる限り明確化し、パーソナルデータの取得は当該目的実現のため最小限のものとすること

適正な手段による取得
パーソナルデータの取得は、適切な手段により行うこと

適切な取扱い（個人を特定する分析、第三者提供の禁止）
本人からの同意取得を行わずに個人を特定する分析や第三者へのパーソナルデータの提供を行わないこと

適切な安全管理措置
パーソナルデータの取扱いにあたっては、適切な安全管理措置をとること

5.　パーソナルデータの適切な取扱のための対策概要

5.1.　５つのプロセス

機構において、研究開発の対象としてパーソナルデータを取り扱う場合、研究開発の各段階（「計画」「事前準備」「研究・実証実験」「終了」）において必要なプライバシー保護のための対策として、**表 5-1 に挙げる５つのプロセスを実施します**。

プロセス①及び③において、委員会に所定の様式に記入したものを提出します。パーソナルデータ取扱研究開発業務審議委員会（以下「委員会」といいます。）は、提出された様式の内容に基づいて審査を行います。

※委員会は数か月に 1 回開催されるため、審査は、各段階の直前ではなく、早めに審査する必要がありますので、それに沿った対応が求められます。

各プロセスの詳細については、6 章以降に説明します。

表　5-1　プロセスの概要

プロセス番号	プロセス概要	説明	研究の段階
1	パーソナルデータを取扱う研究開発プロジェクトの把握と事前リスク評価	パーソナルデータを取扱う研究開発プロジェクトについて把握する。 委員会は、プライバシーリスクを事前評価し、研究開発を進めるにあたりプライバシー保護の観点から注意すべき点等についてまとめ、機構に提示する。	計画（予算が配分される前）
2	パーソナルデータを取扱う研究開発プロジェクトの契約時の措置	（委託研究相手先と機構が契約を締結する際に必要なプロセス） 委託先との間で事前にパーソナルデータの取扱を確認し、契約において適切な取扱いを担保する。	事前準備
3	パーソナルデータの取扱計画の決定	１で把握された研究開発プロジェクトにおいてパーソナルデータの具体的な取扱いの計画について決める。 委員会は、プライバシーリスクの評価を行い、プライバシー保護の観点から注意すべき点等についてまとめ、取扱責任者に提示する。	事前準備

4	パーソナルデータ取扱い時のプライバシー対策の実施	パーソナルデータの取得から破棄まで、それぞれの段階で適切な取扱いを行う。	研究・実証実験
5	パーソナルデータを取扱う研究開発プロジェクトに関するプレス発表時の措置	パーソナルデータを取扱う研究開発についてプレス発表する場合、一般市民に不安や不信を抱かせないように、わかりやすい説明を行う。	（研究・実証実験）終了

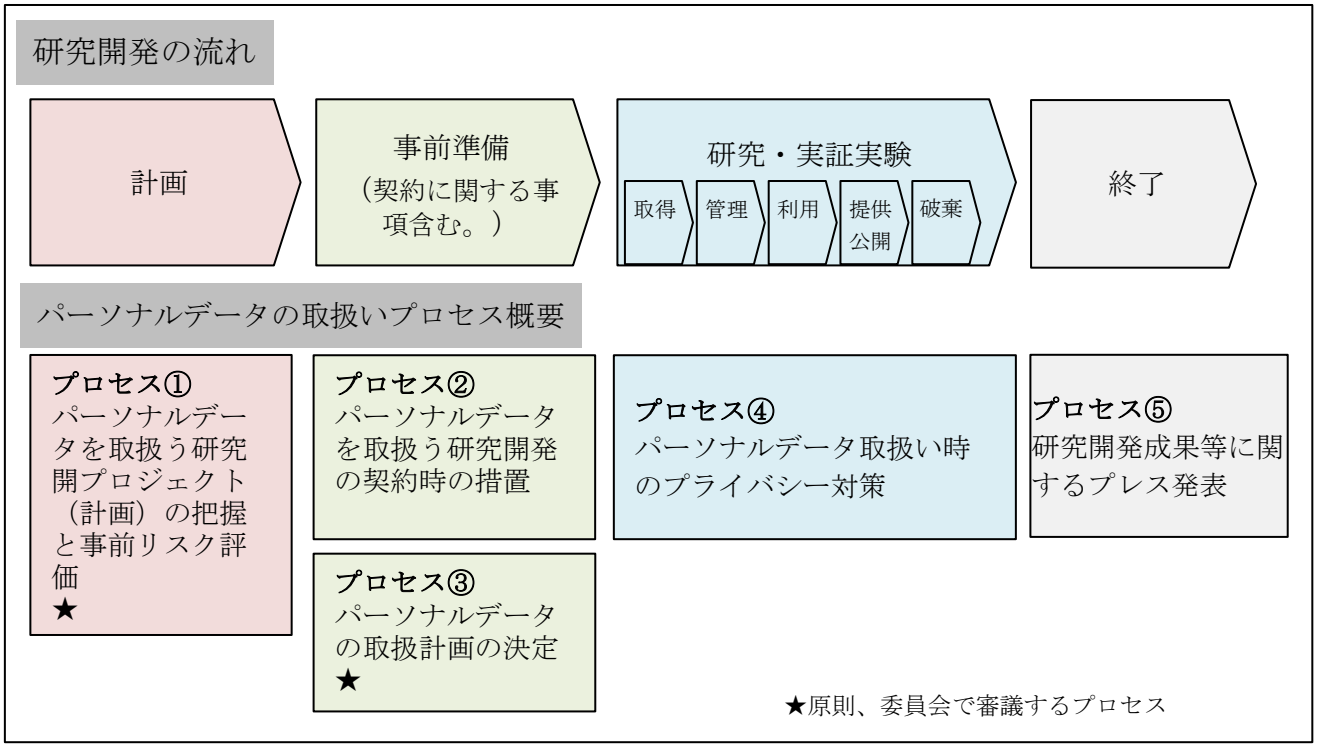

図 5-1　研究開発の段階及び実施するプロセス概要

5.2.　各プロセスを実施する順序

表 5-2 に基本的な流れを示します。

表 5-2　各プロセスの実施時期

研究形態	実施するプロセスの順	実施する時期	委員会での審議
委託研究	プロセス①	提案者からの応募資料を審査する時期。	要
	プロセス②	契約締結	不要※1
	プロセス③	受託者と契約を行った後、受託者がパーソナルデータの取得開始よりも前の段階	要
	プロセス④	委員会承認後、研究開発プロジェクトを実施している段階	不要※1
	プロセス⑤	研究開発プロジェクトに関する成果等のプレス発表を行う前の段階	不要※1

※1：委員会での審議が不要とされている場合でも、プロセスの過程でリスクが高いとされたものについては審議を要することがあります。

6. パーソナルデータを取扱う研究開発プロジェクト（計画）の把握と事前リスク評価（プロセス①）

6.1. 概要

委員会は、各研究開発プロジェクトのプライバシーリスクを事前に評価し、研究を進めるにあたってプライバシー保護の観点で注意すべき点等について助言します。

6.2. 実施時期

研究開発業務で取り扱うパーソナルデータの把握を行う時期は、下表に示すとおりとします。

表 6-1 パーソナルデータの把握を行う時期

研究の種類	把握する時期
委託研究	提案者からの応募資料を審査する時期。

6.3. 実施内容

（１）様式の提出

パーソナルデータを取り扱う予定の案件がある場合は、【様式１】「パーソナルデータ取扱チェックリスト（計画）」に必要事項を記載し、委員会あてに提出します。

様式 1「パーソナルデータ取扱チェックリスト（計画）」においては、研究開発の概要及びパーソナルデータ利用計画を記載します。記載時には以下の点に留意してください。

- 利用計画のチェック欄のうち〇と回答できない項目については、研究開発目的に照らし合わせて〇とできない理由を備考欄に記載してください。提出時点で未定の箇所があれば、未定と記載していただいても結構です。
- 様式右上に取扱責任者、取扱管理者の記入欄がありますので、確認を経たうえでそれぞれの氏名を記入してください。
- 委託研究（高度通信・放送研究開発委託研究）において、受託者がデータを所有する場合は、受託者が各組織内で責任者等を設置し、委託研究に係る事務管理責任者であるイノベーション推進部門委託研究推進室を通して必要書類を提出してください。なお、受託者との連絡窓口は、イノベーション推進部門委託研究推進室の担当者が行います。

（２）委員会による事前評価及び助言

委員会事務局は、提出された「パーソナルデータ取扱チェックリスト（計画）」をとりまとめます。委員会は、このとりまとめに基づいて、必要があれば問い合わせ等を行ったうえで、各研究開発プロジェクトのプライバシーリスクを事前評価し、注意すべき点

や計画の再考を求める必要があるかどうかについて委員会としての助言をとりまとめます。委員会で取りまとめられた助言は、提示されます。また、助言が付されなかった案件については、その旨を提示されます。

① 事前評価

事前評価については、この段階で具体的な研究計画が作成されているわけではないので、特にリスクが高い可能性のある研究開発がないかどうかを評価するため、次の２つのステップで行います。

- **事前評価のステップ１：取扱うパーソナルデータが、「プライバシー侵害の可能性のある情報」を含むか否か（機微な内容を含むか否か）を判別する。**

  「プライバシー侵害の可能性のある情報」又は「機微な内容を含む情報」とは、病歴、検診結果、収入や資産の状況、人の位置情報、交通機関の条項履歴など、人に知られたくないような情報を指します。一概には判断できないので、ケースバイケースで判断していくことになります。なお、改正独法等個人情報保護法で新たに定義された「要配慮個人情報」（3.1（３）参照）は、「プライバシー侵害の可能性のある情報」に含まれるものとします。

- **事前評価のステップ２：「プライバシー侵害の可能性のある情報」を取扱う研究開発のうち、表 6-2 における事前評価基準の少なくとも一つ該当しない項目があるものを、高リスク案件として重点的に扱う。**

② 委員会による助言

委員会は、事前評価においてリスクが高いとされた案件について、重点的な検討を行い、助言を行うものとします。ただし、リスクが低いとされた案件についても助言が附されることがあります。

表 6-2　プロセス①におけるプライバシーリスクに関する事前評価基準

データサイクルの別	評価基準
データ取得	・取得するデータ、取得方法、利用目的等について本人の同意を取得している。 （ただし、本人が自ら SNS やブログ等を通してインターネット上に発信した情報を取得する場合は除く）
データ管理	・本人の同意なく、データを予め特定した目的以外で利用することはない
データ利用	・本人の同意なく、個人の特定を行う分析や機微な内容を推定する分析は行わない
データ提供・公開	・第三者に対するデータの提供・公開の内容は、本人の同意を取得した範囲を超えておこなわない ・本人の同意なく、国外へのデータ移送は行わない

なお、委員会は、審議を重ねて知見が蓄積していく中で、事前評価基準を適宜見直すものとします。

（３）事前評価後の対応

当該研究開発プロジェクトの実施が決まった場合、委員会（事務局）の協力を得つつ、**委員会の助言内容を踏まえて、プロセス②以降を進めてください。**リスクが低いとされた案件についても、委員会からの助言が附されたものについては、プロセス②以降で考慮するようにしてください。

なお、当該プロセスで「プライバシー侵害の可能性のある情報」が含まれないと評価された研究開発プロジェクトはプロセス③以降のプロセスを省略可能とします。

プロセス①の流れを、図 6-1 に示します。

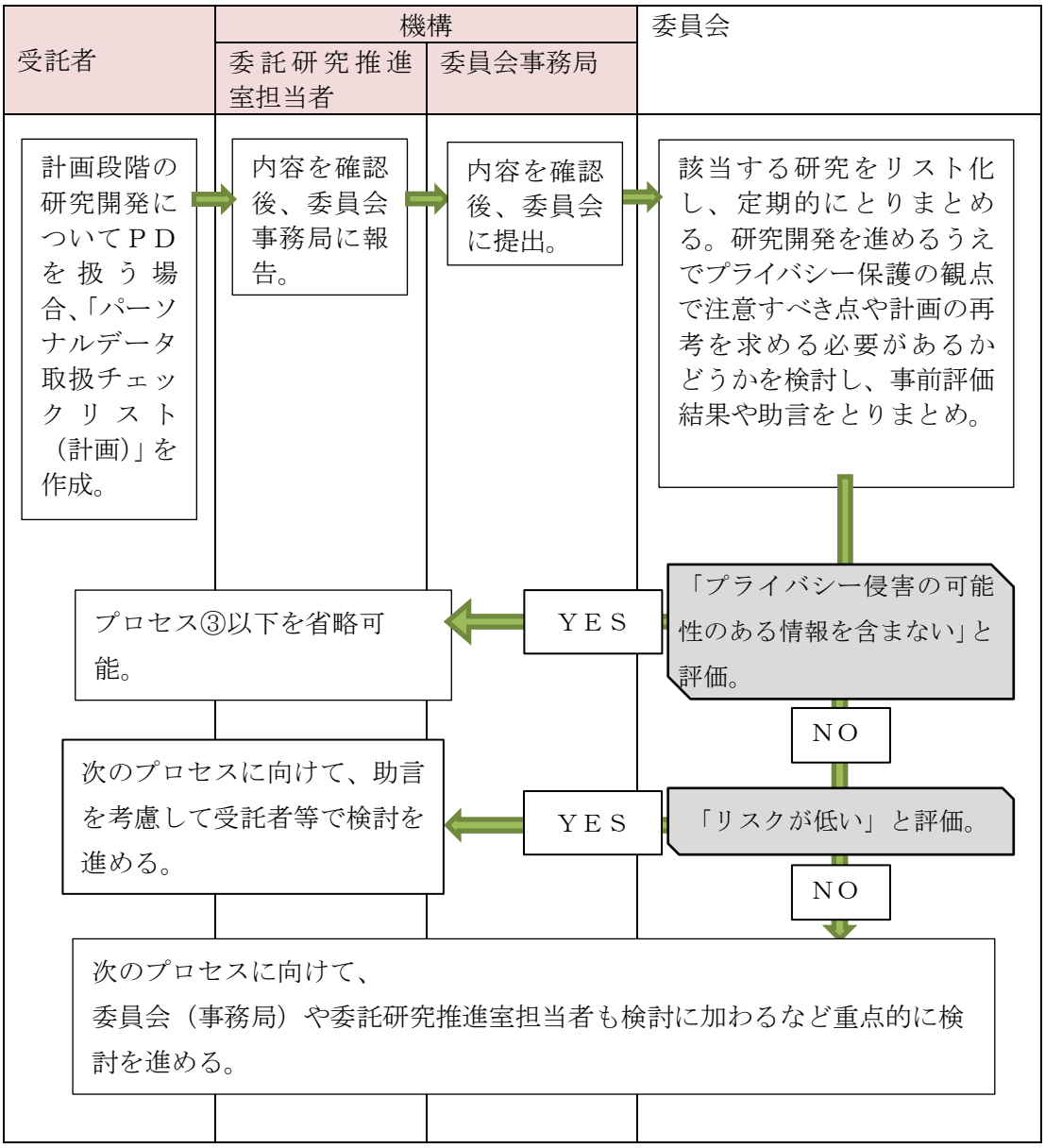

図 6-1　プロセス①の流れ

7.　パーソナルデータを取扱う研究開発プロジェクトの契約時の措置（プロセス②）

高度通信・放送研究開発委託研究においては、同委託研究の契約約款にて、平成 26 年 6 月に個人情報の善管注意義務に関する一般条項を設けました。

その後、平成 28 年度より機構内においてパーソナルデータの取り扱いに関する体制が構築され、具体的な運用が開始されたことを踏まえ、平成 29 年 5 月に一般条項をより具体的な条項に改正しました。

受託者は、委託研究の契約を締結する場合、約款に記載の内容を順守して頂く必要がありますので、契約締結前に事前によく確認頂くと共に、自身の研究開発において具体的にどのような措置が必要となるのかについても、検討して下さい。

委託契約約款抜粋

（パーソナルデータの取り扱い）

第５０条　乙は、委託業務の実施に当たり、自ら収集、作成、又は第三者から取得したパーソナルデータについては、善良な管理者の注意をもって取り扱わなければならない。

2　乙は、委託業務の実施に当たり、パーソナルデータを収集するときは適法かつ公正な手段により収集するものとし、パーソナルデータを第三者から取得するときはそのデータが適法かつ公正な手段により収集されていることを確認した上で取得することとする。

3　乙は、甲の求めに応じ、パーソナルデータの取扱計画の決定、取扱時のプライバシー保護対策の実施、研究成果の公表等に先立ち必要な事項を甲に遅滞なく報告するものとし、甲は、プライバシー等の個人の権利利益の保護又は甲におけるリスクの顕在化の防止等のために必要と判断した場合は、その内容の変更や中止等の対策の実施を乙に求めることができ、乙はこの指示に従うものとする。

4　乙は、本委託業務を第２条の規定により第三者に再委託する場合、又は第三者に請負させる場合は、本条各項に定める内容と同様の措置を再受託者に求め、あわせて自らがすべての責任を負うものとする。

5　甲は、必要があると認めるときは、乙の事業の運営に支障が生ずるその他正当な理由がある場合を除き、甲の職員を乙の工場、研究施設その他の事業所（乙の再受託者の事業所を含む。）において、パーソナルデータの管理が適切に行われているか等について調査をさせ、乙に対して必要な指示をさせることができる。

6　乙は、パーソナルデータの漏えい、滅失、き損、その他本条に係る違反等の事実を認識した場合には、直ちに被害の拡大防止等のために必要な措置、本人（パーソナルデータによって識別される特定の個人）への連絡等を実施するとともに、甲に対して、当該事実が発生した旨、被害状況、被害の拡大防止等のために講じた措置等について直ちに報告しなければならない。また、甲から更なる指示を受けた場合には、その指示に従わなければならない。

8. パーソナルデータの取扱計画の決定（プロセス③）

8.1. 概要

パーソナルデータを用いた研究開発プロジェクトにおいて、パーソナルデータの取得開始よりも前に、機構として、このプロジェクトでのパーソナルデータの取扱いについての具体的な計画を決定します。

まず、受託者は、パーソナルデータの具体的な取扱い計画（案）を策定して、委員会（事務局）に提出します。次に、委員会は当該計画（案）を元に各研究開発プロジェクトのリスクを評価するとともに、対応策が十分かどうかを検討して、計画（案）を進めるにあたってプライバシー保護の観点で注意すべき点等について意見します。この意見を踏まえ、機構が計画を決定します。

8.2. 実施時期

取扱計画を決定する時期は、下表に示すとおりとします。

表 8-1 パーソナルデータの取扱計画を決定する時期

研究の種類	取扱計画を決定する時期
委託研究	受託者と契約を行った後、受託者がパーソナルデータの取得開始よりも前の段階

8.3. 実施内容

（１）受託者の対応

受託者は、パーソナルデータを取扱う研究開発プロジェクトについて、プロセス①での委員会の助言を踏まえて、パーソナルデータの具体的な取扱い計画（案）を策定します。

プロセス①で実施された事前評価で「プライバシー侵害の可能性のある情報」を含まないとされた案件については、プロセス③以降のプロセスを省略できるものとします。

具体的には、**表 8-1 に示す実施時期に、プロセス①での委員会の助言内容を踏まえつつ、【様式２】「パーソナルデータ取扱チェックリスト」を委員会に提出します。**（なお、様式２は様式１と同じ様式となっていますが、プロセス①から変更になった部分等については当該変更を反映したものとして提出してください。）

また、**プロセス①でリスクが高いと評価された案件については、様式２に加えて、リスク分析と対処策案を記載する【様式３】「パーソナルデータのリスク分析とリスク対策」についても作成し、委員会（事務局）に提出してください。**

（２）委員会での評価

委員会事務局は、提出された【様式２】及び【様式３】をとりまとめます。

委員会は、これらについて評価を行い、プライバシー保護の観点から注意すべき点等について意見をとりまとめ、提示します。なお、この際、委員会の審議においては、アドバイザーの参加が原則として必須となります。

（３）評価後の受託者の対応

委員会から提示された意見への対処方針をまとめ、委託研究推進室担当者を通して委員会に提出します。

委員会は、リスク評価とその対応策を検討する際、表 8-2 から表 8-7 の評価基準と対策例を参考に行うこととします。

表 8-2　プロセス③におけるリスク評価における評価基準

データサイクルの別	評価基準
データの取得時	【取得者が受託者である場合】 • 取扱うパーソナルデータに、プライバシー侵害の可能性のある情報（要配慮個人情報その他の機微な内容を含む情報）が含まれない • 取得するデータ、取得方法、利用目的等について本人から同意を取得している • 本人の同意（又は通知・公表）の手段及びその内容は本人に認識・理解しやすいものである • 本人からの要望を受けてデータ利用ならびに第三者提供を停止する手段（オプトアウト）を用意する 【取得者が受託者以外である場合】 • データの取得を受ける場合、適切な方法で取得されたデータであることを確認している。 • 受託者における取扱い内容は、データ取扱いに関する契約や約款等の内容を超えるものではない。
管理	• 本人の同意なく、データを予め特定した目的以外で利用することはない • パーソナルデータの移送時・保管時には、適切な暗号化処理等を行うセキュリティを担保する • 取扱うパーソナルデータにアクセスできる職員等は必要最小限とする • 海外研究機関・海外設置クラウド等、海外へ・海外からのデータ移送は行わない
利用	• 本人の同意なく、本人の特定を行う分析や機微な内容を推定する分析を行わない • 本人の同意なく、他の研究開発等において取得したデータとの突合処理は行わない • 利用の内容は同意（又は通知・公表）を行った範囲を超えない
提供・公開	【第三者に対するデータの提供・公開の予定がある場合】 • 第三者に対する提供又は公開の内容は、本人の同意を得た範囲を超えて行わない • 本人の同意なく、国外へのデータ移送は行わない

	• 第三者提供又は公開に当たり、データの利用目的や利用者、利用手続き等が明確化されている • データの提供先とは、プロファイル推定や個人の特定を禁止する契約等を結ぶ • 論文等の成果発表時、適切に匿名加工したデータ又は統計データを用いる
破棄	• データの利用期間・保有期間を設定し、本人にその内容の同意の取得（又は通知・公表）を行う。 • 利用期間・保有期間の終了後のデータの取り扱いに関する同意の取得（又は通知・公表）を行う。

下線部分は、プロセス①での事前評価基準に含まれる箇所。

主なリスク低減策案を以下の表 8-3 から表 8-7 に示します。

表 8-3　取得時のリスク評価基準に該当するケースと対策案

評価基準に該当するケース	リスク低減策（例）
取得するデータ、取得方法、利用目的等について本人からの同意を取得しない	①本人に対して改めて説明し、同意を得る。 ＜同意の取得が物理的に困難な場合＞ ②本人から同意を取得する以外の方法として、本人への通知もしくは利用目的の公表を行う。 ③本人が使用する機器や付帯する機器等の利用開始時に同意を得る手段を講ずる。 ④カメラ等を用いて個人を識別する写真や映像情報を取得する場合には、取得場所で利用目的を告知（公表）し、カメラ等により、写真や映像を取得されない回避通路等を用意する。
取扱うパーソナルデータに、プライバシー侵害の可能性のある情報（要配慮個人情報その他の機微な内容を含む情報）が含まれる	①機微な内容を含む情報を取得する必要があるのか再度検討する。 ②検討した上、取得が必要な場合には、研究の意義や目的等を説明し、本人の同意を得る。
パーソナルデータの提供を受ける場合、提供元が適法かつ公正な方法で、パーソナルデータの取得を行っているか不明である	①提供元が適正な方法でデータを取得したかどうかを確認する。（本人同意を取得したか、違法な方法で取得されていないか等） ②確認が得られない限り当該データは利用しないことを検討

表 8-4　管理に関するリスク評価基準に該当するケースと対策案

評価基準に該当するケース	リスク低減策（例）
本人の同意なく、取得したパーソナルデータをあらかじめ特定した目的以外の目的のために利用する	①追加したい利用目的と予め特定した目的の関連性を検討する。（予め特定した目的内と解釈できないかどうか。） ②再度、追加された利用目的の同意を本人から得る、あるいは通知又は公表する。
海外設置のクラウドを利用する。	パーソナルデータの管理体制や管理方法等が自国と同等であることを確認する。

表 8-5　利用におけるリスク評価基準に該当するケースと対策案

評価基準に該当するケース	リスク低減策（例）
利用の内容は本人同意（又は通知・公表）を行った範囲を超える	改めて当該利用について本人に十分に説明し同意を取る（あるいは通知又は公表する）。
本人の同意なく、個人を特定する分析や機微な内容を推定する分析を行う	①原則禁止。 ②必要性を再度検討し、必要な場合には本人から同意を得る。
他の研究開発等において取得したデータとの突合処理を行う	①取得時に本人に説明した目的に合致するかどうか確認する ②当初の目的には合致しない場合、改めて当該処理について十分に説明し同意を取る（あるいは通知又は公表する）。

表 8-6　提供・公開のリスク評価基準に該当するケースと対策案

評価基準に該当するケース	リスク低減策（例）
本人が同意した範囲を超えて、第三者に対する提供・公開を行う	①再度、本人から同意を得る、又は通知する ②（①が難しい場合には、）パーソナルデータを統計化などの手法で匿名加工処理したうえで実施する。
本人の同意なく、国外へのデータ移送を行う	①本人から海外の機関への提供について同意を得る。 ②提供先機関のパーソナルデータの管理体制や管理方法等が自国と同等であることを確認する。
データを第三者に提供又は公開する場合、各データの利用目的、利用形態、利用方法（利用手続きを含む）等が明確でない。	提供・公開に当たっての事前に各データの利用目的、利用形態、利用方法（利用手続きを含む）等を規定する。
データの提供先とは、プロファイル推定や個人の特定を禁止する契約等を結んでいない	データの提供先と取扱いについて協議し、適宜契約等を結ぶ

表 8-7　廃棄のリスク評価基準に該当するケースと対策案

評価基準に該当するケース	リスク低減策（例）
データの利用期間・保持期間を設定しない、かつ本人から同意も取得しない	①データ利用目的にかんがみて定められないか検討する ②データ取得前までにデータの保管期間を定めることが難しい場合には、その旨をあらかじめ同意書等に記載する。

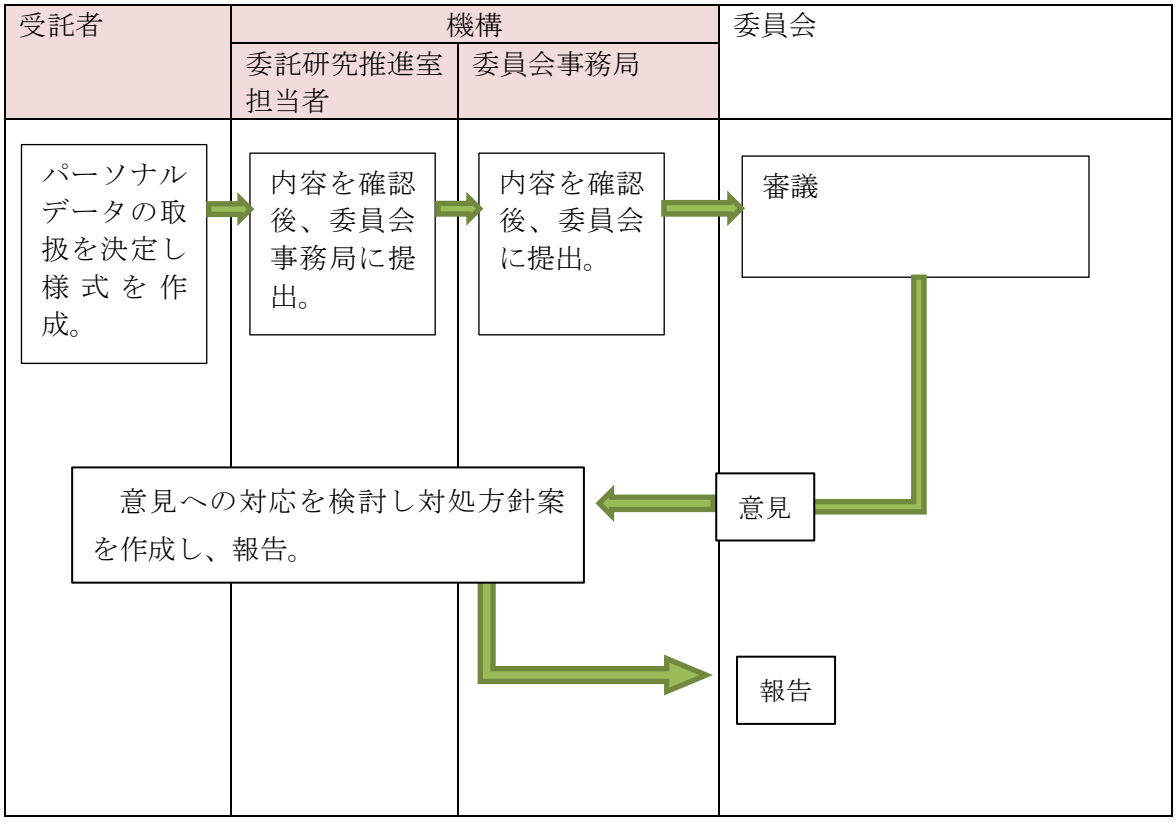

図 8-1　プロセス③の流れ

9.　パーソナルデータの取扱いの運用（プロセス④）

受託者は、プロセス③までの作業を踏まえ、研究開発や実証実験を開始します。その際には、パーソナルデータの取得、管理、利用、提供・公開、破棄というデータのライフサイクルのそれぞれの段階において、9.1以下に示す取扱いルールに従うものとします。

委員会は、研究開発プロジェクトが「パーソナルデータ取扱チェックリスト」及び「パーソナルデータのリスク分析とリスク対策」のとおりに実施されているかどうかを定期的に確認します。該当する案件数が多い場合には、プロセス①でリスクが高いと判断されたものから優先的に実施します。

なお、プロセス③までの作業を経た後に、データの追加や変更等、データを利用する研究分担者の追加、提供先の拡大などパーソナルデータの取扱計画を変更する場合には、事前に「パーソナルデータ取扱チェックリスト」を再度委員会に提出してください。提出の内容に応じて委員会で再度審議を実施します。

なお、プロセス①で実施された事前評価で「プライバシー侵害の可能性のある情報」を含まないとされた案件については、プロセス③以降のプロセスを省略できるものとします。

9.1.　**データ取得時のルール**

パーソナルデータを取得する際には、その利用目的をできる限り具体的に特定し、その目的の達成に必要な最小限度を取得することを原則とします。本人に対して利用目的、利用方法、安全管理及び提供範囲についてわかりやすく説明するとともに、事前に取得の同意を得る（それが物理的に困難な場合には本人への通知または公表を行う）必要があります。

9.1.1.　パーソナルデータを受託者が取得する場合

（1）データ取得時のルール

① 取得については、原則として事前に本人の同意を得るものとする。本人の同意を得ることが物理的に困難である場合には、本人に対して通知又は公表するものとする。

② 要配慮個人情報等の機微性の高い情報は原則として取得しない。研究開発の観点から取得する必要がある場合には書面による同意を得る。

③ 取得に当たっては、取得データの内容と目的、取得方法等（下記ア～コ）について本人にわかりやすく説明する。なお、本人が未成年者である場合など、同意したことによる影響について判断できない可能性等がある場合には、保護者・親権者等に対してもわかりやすく説明を行うとともに、その同意を取得するようにしてください。

（ア）データの種類・内容、取得方法

（イ）データの利用目的・利用方法

※　利用目的の記述については、後述する「（4）パーソナルデータの利用目的の記述のしかた」に従ってください。

（ウ）研究分担者が取得データを利用する場合はその旨も含める。

（エ）データを第三者に提供する場合はその旨も含める。当該提供先とパーソナルデータの取扱いに関する契約がある場合はその旨を記載するとよい。

（オ）データを海外の第三者に提供する場合はその旨を含める。

（カ）データを公開、もしくは匿名加工、統計処理等したデータを論文等で公開する場合はその旨も含める。

（キ）データの安全管理措置

（ク）データの保管期間・破棄方法

- データの保管期間は、利用目的にかんがみ適切な期間を定める。
- 現時点で未定だが将来の研究に用いられる可能性がある等、データ取得前までにデータの保管期間を定めることが難しい場合には、その旨をあらかじめ同意書等に記載する。
- 研究活動における不正行為への対応等に関し、委託契約約款において、委託研究における研究資料の保存期間は当該研究に係る論文等を発表してから原則として10年間としている。なお、論文等の発表を予定しない研究資料の保存期間については、想定した成果が得られない、又は研究開発を中止する等により将来にわたり論文等の発表を行わないこととなった場合には、データを削除することが適当。

（ケ）パーソナルデータの取得の中止（オプトアウト）の可否、可能である場合の方法

（コ）問い合わせ先

④データを外部機関やインターネットを介して取得する場合、適切な暗号処理等を行うなどセキュリティを担保する

（2）同意の取得方法

本人から同意を取得する方法として、書面による確認のほか、ウェブ画面上のボタンのクリック、スマートフォンアプリでの承認ボタンのクリック等が考えられます。

同意書文例を以下に示します。

同意書（文例）

私は，本研究開発（●●：実施期間●年●月●日～●年●月●日）のもとで実施される「●●の実証実験」への参加を承諾します．参加の承諾にあたり，以下の内容について理解し同意します．

１．私は本実験のパーソナルデータの取り扱いの内容（別紙に記載）に関して同意します．

２．本実験により得られる研究成果は，実験実施責任者（後述）に帰属することに同意します．

３．参加者の権利（別紙記載） について理解しました．

４．実験参加にあたり費用負担・謝礼が生じないことを理解しました．

私は，上記の内容について理解し同意した上で，本実験に参加します．

署名：

実験参加者：

年　　月　　日：

実験実施責任者：　××大学　××研究所　××研究室

〇〇株式会社〇〇部門

電話：　　Email：

実験の概要：

皆様には，●●の技術を利用した●●の体験をして頂きます．貸し出す端末を利用し，展示会場のどこに皆様が訪れたかの**位置情報**（半径●程度の精度)を分析して，●●をします．更に，皆様からご提供頂く**属性情報**（年齢・性別・趣味）を合わせて分析して，●●の情報を貸出しの端末に表示します。

パーソナルデータの取扱い：

本実験で取得するデータは以下の通りです。

- 別紙に記載の皆様の**連絡先**（氏名，電話番号）
- 皆様がどの展示に皆様が訪れたかの**位置情報**（半径●メートルの精度）
- 皆様からご提供頂く**属性情報**（年齢・性別・趣味）

連絡先については，皆様に端末を貸し出すため，身元確認する目的のみで使用します。実験に参加している間，紙で保管し，参加終了後に皆様に返却します．**位置情報**と**属性情報**のデータついては以下のように取り扱います．

- データの用途の範囲を本実験のみに限定する．
- 第三者へのデータの提供は行わない．ただし、個人が特定できない統計情報として学会発表等の場で公表する可能性がある
- データは実験を実施する○○株式会社及び研究分担者の××大学××研究室の関係メンバしかアクセスできないようアクセス制限を行う
- 個人が特定できない匿名データに変換して本実験で利用する
- 皆様からの要望があった場合は，要請に基づいてデータの利用停止を行う．
- 本実験による成果を学会に発表した後 10 年間はデータを適切に管理し、その後適切な方法で破棄する

実験参加者の権利:

1. 実験の内容について，疑問な点があればいつでも実験を実施する実験実施責任者に質問ができる．
2. 実験参加中のいつの時点でも，参加を取りやめることができ，実験実施責任者に通知し理由を告げることなく直ちに参加を取りやめることができる．
3. 実験の実施中，あるいは実施後であっても，私の申し出により本実験で取得された私に関するパーソナルデータの利用停止ができる。
4. 実験への参加を取り消すことで、何らのペナルティも生じない。

参加者の管理情報

利用者番号:

(パーソナルデータの利用停止申請の際に必要になります)

参加者の連絡先

(端末を貸し出すため, 身元確認する目的のみ使用します)

・氏名:

・電話番号

3）通知・公表について

パーソナルデータを取得する際、本人の同意を得ることが物理的に困難である場合には、本人に通知又は公表することにより取得することができるものとします。

ただし、その際は、パーソナルデータを取得すること、利用目的、利用方法、安全管理及び提供範囲等について、本人が容易に認識できる形で通知又は公表を行うよう、特に注意してください。

(注)「通知」「公表」の意味

「通知」とは、本人に直接知らせることをいい、例としては、面談において利用目的等を記載した文書を渡して口頭で説明すること、当該文書を電子メール、ファックス等により送信すること等が考えられます。

また、「公表」とは、国民一般その他不特定多数の人々が知ることができるように発表することをいい、例としては、機構のウェブへの掲載（画面中のトップページから１回程度の操作で到達できる場所への掲載)、実験場所での掲示、パンフレットの配布等が考えられます。

（4）パーソナルデータの利用目的の記述のしかた

（1）での述べたとおり、本人からパーソナルデータを取得するに当たっては、本人にパーソナルデータの利用目的を示す必要があります。その際は、以下に従うようにしてください。

- 本人の同意を取得する際等には、パーソナルデータの利用目的をできるだけ特定して明示する。
- その際、利用目的は、「○○技術の研究開発のために利用する」、「○○メカニズムの解明に関する研究のために利用する」、「○○実証実験において、○○を行うために利用する」等、利用の範囲に応じて記載する。
- 単に「○○（受託者組織名称）の研究開発に利用する」と記載するのみでは、本

人に対する説明としては不十分である。

- 今回の研究だけでなく、将来にわたっても当該データの利用が見込まれるときは、将来どのような研究開発に利用する予定かを考慮して適切に記述する。下表に記述例を示す。
- 将来の研究のために用いられる可能性があるが、本人から同意を受ける時点では具体的に特定できない場合には、想定される内容を同意書等に記載することが望ましい。

利用目的の記述（例）
• 脳情報通信技術の研究開発のために利用します。 • 音声認識・翻訳技術の研究開発のために利用します。 • 人間の脳における情報の意味表現や情報の意識化過程に関する脳科学的研究のために利用します。 • 多感覚情報の認知・脳メカニズムの解明に関する研究のために利用します。 • 実証実験（○年○月～同年○月）で利用された●●アプリの利用履歴を把握するため、当該アプリをダウンロードする利用情報通信端末のＭＡＣアドレスを取得します。

9.1.2.　パーソナルデータを間接的に取得する場合等

パーソナルデータの提供を受ける場合でも、取得元により適切に取得されたものであることを確認してください。

① 取得元となる、研究分担者において本人への同意、通知又は公表が適切に行われているかを担当者に確認する。

② ①の確認が得られない限り、当該データを利用しない。

なお、インターネット上で本人が自発的に公にしているパーソナルデータを取得する場合については今後必要に応じて検討していきます。

9.2.　データ管理時のルール

保管しているパーソナルデータは、同意等を取得した利用目的以外に利用することのないように管理をしてください。また、パーソナルデータデータの漏えい等は防止しなくてはなりませんので、必要な安全管理のための措置等を講じてください。

① 本人の同意なく、取得したパーソナルデータをあらかじめ特定した目的以外の目的のために利用しない。

② データにアクセスできる職員等を必要最小限に設定する。
③ データの移送時・保管時には適切な暗号化処理等を行うなどセキュリティを担保する。
④ オプトアウトにより、本人からデータの削除要求があった場合に迅速に対応できるよう、データの保守性を高めるよう努める。
⑤ 海外研究機関・海外設置クラウド等、海外へデータ移送を行う場合には、パーソナルデータの管理体制や方法等が十分かどうかを確認する。
⑥ 海外研究機関・海外設置クラウド等、海外からデータ移送を行う場合には、各国のパーソナルデータに関するルールを確認する。特に欧州諸国から日本へのパーソナルデータの移送については、注意すること。

9.3. データ利用時のルール

研究開発の過程において個人を特定して本人へのフィードバックを行うケースや他のデータとの突合処理を行うケースが考えられるが、いずれもプライバシー保護の観点から、本人への同意をするようにしてください。

① 本人の同意なく、個人の特定を行う分析や機微な内容を推定する分析を行わない。
② 本人の同意なく、他の研究開発等において取得したデータとの突合処理は行わない。
③ 利用の内容は本人の同意（又は通知・公表）を得た範囲を超えない。
④ 分析結果等を本人へフィードバックする場合は、不快を与えないように説明責任を果たす。本人からの苦情窓口を設ける。

9.4. データの提供・公開時のルール

パーソナルデータを提供、公開する場合には、データの取得元である本人の提供、公開について同意した範囲内で行うと共に、必要に応じて提供先や公開先での利用制限などを明確にする必要があります。

① データの提供・公開は、本人の同意を取得した範囲を超えて行わない。
② 本人の同意なく、国外へのデータ提供は行わない。提供先機関のパーソナルデータの管理体制や管理方法等が自国と同等であるかどうかを確認する。
③ 取得時に、本人から同意が得られない場合、第三者に提供・公開するデータは、統計処理などプライバシーを侵害しないように加工処理を施した情報に限る。
④ データの提供・公開に当たり、データの利用目的や利用者、利用手続き等を定める。
⑤ データの提供先に個人を特定する分析や、機微な内容を推定する分析を禁止する契約等を結ぶ（ただし、本人から同意を得ている場合はこの限りではない。）

⑥　論文等の成果発表時、適切に匿名加工したデータもしくは統計データを用いる。

9.5.　データ破棄時のルール

①　予め定めたデータの保管期間終了後、直ちにデータの破棄を行う。

②　情報機器内のデータを破棄するには、データ消去ツールでデータを確実に削除し、データ削除のログデータを取得しておく。

③　データを蓄積したサーバを破棄する場合は、ハードディスクを物理的に破棄し、ディスク内のデータを破壊したうえで、サーバ破棄を破棄業者に依頼する。破棄業者は信頼できる業者を選択し、秘密保持契約を締結する。

10.　研究成果等に関するプレス発表（プロセス⑤）

10.1.　概要

パーソナルデータに関する実証実験や研究成果等をプレス発表する場合、パーソナルデータの提供者や市民に不安や不信を抱かせないよう十分な説明を行う必要があります。

10.2　実施内容

機構では、次に説明する記載の観点から発表原稿案について確認し、不備があれば受託者に修正の指示を行います。また、委員会事務局は、当該研究内容が委員会で了承されたものかどうかを過去の審議結果から確認を行います。

なお、プロセス①から⑤までの過程でリスクが軽減されていると考えられることから基本的には、プレス発表について委員会での審議は不要とします。ただし、プロセス①や③の過程でリスクが高いとされたものについては、プレス発表についても審議事項とすべきかどうかを委員会で審議します。

委託研究においては、プレス発表の１か月前に原稿を委託研究推進室担当に提出するようお願いしております。プロセス①や③の過程でリスクが高いとされたものについては、原稿の修正やプレス発表そのものが中止となる場合があります。

10.3　**発表原稿案に関する確認内容**

パーソナルデータを利用する研究開発に関するプレス発表原稿については、下のような観点で説明が行われているか確認します。

① 研究開発成果や実証実験の実施（公開するアプリケーション等を含む。）の概要
- 研究開発や実証実験の公益性や、公開するアプリケーションの利用者に与えるメリットを記載しているか
- 研究成果を達成するために、パーソナルデータが必要になる理由を記載しているか

② 取得するパーソナルデータと取得の方法
- 研究開発の過程で取得するパーソナルデータの項目とその取得方法について、可能な限り細分化し、具体的に記載しているか

③ パーソナルデータの利用目的・利用方法
- 取得するパーソナルデータの利用目的を具体的に記載しているか
- パーソナルデータの利用目的や利用方法は、取得するパーソナルデータの項目と対応して記載しているか

- パーソナルデータを当該研究開発でどのように利用するか（匿名加工に含まれない加工や分析の方法等）について説明しているか
- 特に利用者にとって分かりにくいものを明確に記載しているか

④　パーソナルデータの提供の有無及び提供先

・パーソナルデータを第三者への提供が有るかの有無と提供先を明確に記載しているか

・提供先でのデータの利用範囲についても記載しているか

・研究分担者等とデータの共有、提供を行う場合には、相手先研究機関名と相手先研究機関での利用方法を説明しているか

⑤　利用者によるパーソナルデータの提供の停止・訂正の可否及びその方法

・利用者が機構によるパーソナルデータの取得の中止又は利用の停止が可能であるかを記載しているか

・上記が可能である場合には取得の中止方法又は利用の停止方法を記載しているか

⑥　データの管理方法（保存期間、破棄 ）

・パーソナルデータおよび加工したデータの保管期間と破棄方法について記載しているか

⑦　プライバシー保護のための措置

・パーソナルデータのプライバシー保護のために技術面（匿名化技術、安全管理体制等）及び運用面（研究分担者との契約、機構内ガバナンス）の両面から措置を講じていることを記載しているか

⑧　問合せ先

11.　パーソナルデータを取り扱う研究開発に対する苦情・批判に関する対処

11.1.　常設の対応窓口の設置

委員会事務局は、本人からの苦情及び相談を受け付け、適切、かつ、迅速な対応を以下のように行います。

（1）　委員会事務局は、苦情及び相談の受付のため、常設の対応窓口を設置し、窓口責任者を置きます。

（2）　窓口責任者は、上記対応窓口で受け付けた苦情及び相談内容を書面に記録し、回答案を作成します。苦情及び相談内容が特定の研究開発のパーソナルデータの取扱いに関するものであれば、当該研究開発の取扱責任者等と連携して対処します。

（3）　窓口責任者は、対応内容案について委員会幹事の承認を得たうえで、本人に回答します。

（4）　窓口責任者は、本人への回答内容とその結果を書面に明記し、委員会幹事及びパーソナルデータ取扱責任者に報告します。

11.2.　エスカレーション対応

機構の委託研究におけるパーソナルデータの取扱いについて、プライバシー保護の観点に基づく外部からの批判が発生した場合、当該事実を知った受託者は、速やかに委託研究推進室担当までご報告願います。

エスカレーションすべき事案の判断基準（目安）を以下に示します。事案によりますが、原則として、どれか一つに当てはまれば事案が発生したと判断します。

- プライバシー侵害であるとデータ提供本人や関係者から苦情が申告された場合
- 特定の研究開発について、マスコミ報道で批判的な記事が週に1回以上あった場合
- 特定の研究開発について、ネット掲示板やＳＮＳで批判的な内容の投稿が週に10回以上あった場合
- プライバシー侵害を受けた被害者から受託者や機構に告訴があった場合
- 特定の研究開発について、問い合わせ窓口への苦情や問い合わせが週に10回以上あった場合

付録．個人情報保護法の主な改正ポイントについて

① 利活用促進の観点

（ア）「個人情報」明確化（第２条第１項、第２項）

従来の定義「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」に「個人識別符号が含まれるもの」が追加されました。「個人識別符号」には、特定の個人の身体的特徴を変換したもの（例：顔認識データ）と個人がサービスを利用したり商品を購入したりする際に割り当てられ又は個人に発行される書類に付される符号の２つの類型があり、具体的には今後政令で定めるものとされています。

なお、法改正に関する国の議論（パーソナルデータに関する検討会）では、遺伝子データ、顔認識データ、指紋データ、虹彩等生体認証に関わるデータ、個人番号、運転免許証番号、旅券番号、各種保険証の番号、携帯電話番号、ＩＰアドレス、メールアドレスや会員ＩＤまで広く検討が行われましたが明確な指針が示されたとは言えず、政令を注視していく必要があります。

＜参考＞諸外国の「個人情報」について

ＥＵでは、データ保護指令の解釈上、遺伝子データ、社会保障番号、携帯電話番号、クレジットカード番号、メールアドレス、ＩＰアドレス等が該当するものとされています。

また、米国では、平成27年２月に同国大統領府が公表した「消費者プライバシー権利章典法案」においては、指紋等の生体識別子、社会保障番号、携帯電話番号、メールアドレス、クレジットカード番号、ＩＰアドレス等が例示されています。

（イ）匿名加工情報（第２条第９項、第10項、第36条～第39項）

個人情報を加工して、特定の個人を識別できなくする等し、個人の権利利益侵害がその取扱いによって生じないようにしたものを「匿名加工情報」として新たに類型化し、一律の取り扱い規律の下、本人の同意の関与なく自由な流通・利活用を認めることや、利用目的の変更要件を緩和することとしています。

具体的な規律としては、匿名加工情報を作成するにあたっては個人情報保護委員会（個人情報保護上の権限を集約し、一元的な監視・監督を行う機関として独立性の高い委員会として設置された委員会。）が定める基準を順守すること、加工方法等復

元につながる情報の漏えい防止のための安全管理措置、作成した匿名加工情報に含まれる項目の公表、作成の元となった個人情報に係る本人を識別するための行為の禁止等が設けられています。

なお、匿名加工情報に関する安全管理措置（改正法第 36 条 6 項）については、事業者の過度な負担とならないよう努力義務とされています。

（ウ）利用目的の制限の緩和（第 15 条第 2 項）

個人情報は取り扱うにあたってできる限り利用目的を特定しなければいけないとされています。これは本人に対して透明性を確保し、本人自らが権利利益侵害の防止に必要な対応を図ることができる、というところにあります。従来法では、利用目的の変更が認められる範囲は、「変更前の利用目的と相当の関連性を有すると合理的に認められる範囲」とされ、未限定な目的変更は認められませんでした。改正法では「相当の」が削除され、変更できる利用目的の範囲を、本人が予期し得る限度で拡大することとし、利用目的を特定される趣旨を損なわないようにしつつ、事業者の機動的な目的変更を可能となることを目指しています。ただし、「関連性を有すると合理的に認められる範囲」について、その詳細や具体例はいまだ明確化されていません。

② 保護を強化する観点の改正概要

（ア）要配慮個人情報（第 2 条第 3 項）

人種、信条、病歴など差別・偏見につながり得るような性質の情報が含まれる個人情報を「要配慮個人情報」として類型化し、事前に本人の同意を得て取得することを原則義務化し、本人の同意を得ない第三者提供を禁止しています。

（イ）オプトアウト手続きの厳格化（第 23 条第 2 項～第 4 項）

個人情報保護法は、個人データの第三者提供について原則として本人の同意を得ることを求めています。例外的な場合として、法令に基づく場合や人の生命、身体又は財産の保護に必要で同意取得が困難な場合等、単一の個人情報取扱事業者と同視できるものとして委託先への提供、合併に伴う提供、グループによる共同利用があり、これらについて同意は不要とされています。

これらに加えて、従来法ではビジネスを念頭に、あらかじめ①第三者提供を利用目的とすること、②適用される個人データの項目、③提供方法、④本人の求めに応じて提供停止すること、⑤求めを受け付ける方法を本人へ通知し、又は本人が容易に知り得る状態におくことで、事前の本人同意なく提供することができました（以下「オプトアウト手続」という。）。例としては住宅地図を作成する事業者等があげられます。

改正法では、オプトアウト手続きを行う事業者に個人情報保護委員会に対して上記の①から⑤の事項を届け出させることとし、個人情報保護委員会が届出の内容を委員

会のＷＥＢサイトで公表することされました。これにより、オプトアウト手続による第三者提供を行う個人情報取扱事業者を把握し得る機会が広く提供され、当該手続きの実効性が高まることとなります。