国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

# 委託研究におけるパーソナルデータの取り扱いについて

国立研究開発法人情報通信研究機構

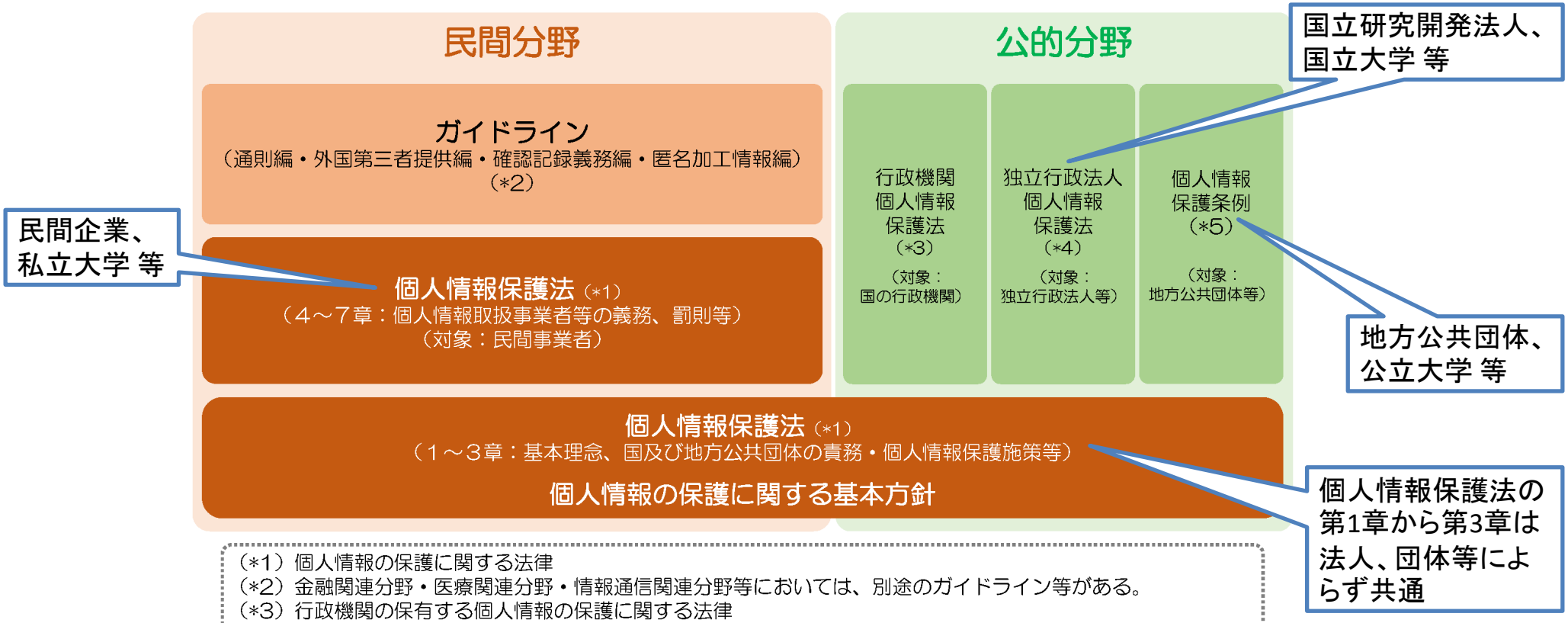
# はじめに

- 本文書の目的
  - 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（以下、「委託研究」という。）においてパーソナルデータを取り扱う研究開発を推進するにあたり、プライバシーをはじめとする個人の権利侵害や、それら侵害への懸念から生じるNICT及び受託者への社会的評価のき損といったリスクを最小限とすることを目的とし、委託研究におけるパーソナルデータの取り扱いについて説明する。
- パーソナルデータとは
  - 「パーソナルデータ」は、法令上の用語ではなく統一的な定義も存在しないが、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」等とされている。
  - 本文書では、個人情報の保護に関する法律（以下、「個人情報保護法」という。）第2条で規定される「個人情報」に加え、「プライバシー侵害の可能性がある情報」を含めてパーソナルデータの対象とする。
  - 「プライバシー」は、法令上明文で定義されていないが、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すると民法上の責任を問われ、損害賠償等の義務が発生する恐れがある。
- パーソナルデータ取扱研究開発業務審議委員会
  - 委託研究におけるパーソナルデータの適切な取り扱いのため、NICTの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」という。）において審議し、助言等を行う。

# 個人情報保護に関する法令の遵守

- 個人情報を取り扱う法人や団体等により、適用される個人情報保護関連法令が異なる。
- 各受託者が適用を受ける個人情報保護関連法令を遵守する必要がある。

## 個人情報保護に関する法律・ガイドラインの体系イメージ




（*1）個人情報の保護に関する法律
（*2）金融関連分野・医療関連分野・情報通信関連分野等においては、別途のガイドライン等がある。
（*3）行政機関の保有する個人情報の保護に関する法律
（*4）独立行政法人等の保有する個人情報の保護に関する法律
（*5）個人情報保護条例の中には、公的分野における個人情報の取扱いに関する各種規定に加えて、事業者の一般的責務等に関する規定や、地方公共団体の施策への協力に関する規定等を設けているものもある。

出典：個人情報保護委員会 個人情報保護に関する法律・ガイドラインの体系イメージ
https://www.ppc.go.jp/personalinfo/legal/ に注記したもの

# パーソナルデータの適切な取り扱いのためのフロー

委託研究の段階に応じて以下のプロセス①～⑤を行う。プロセス①とプロセス③でそれぞれ委員会の審議を行う。各プロセスの詳細は9ページ～14ページに記述する。

## 計画

**プロセス①（研究計画時※）**

パーソナルデータを取り扱う委託研究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り扱う委託研究プロジェクトを把握し、リスク評価を行って、プライバシー保護の観点から注意すべき点等について留意事項等をまとめる。

**⇒様式1（チェックリスト）の提出**

## 事前準備
（契約に関する事項を含む。）

**プロセス②（委託契約時）**

パーソナルデータを取り扱う委託研究の契約時の措置

**プロセス③（委託契約後）**

パーソナルデータの取扱計画の決定

プロセス①で事前リスク評価を受けた委託研究プロジェクトの具体的な取扱計画のリスクを評価。

**⇒様式2（チェックリスト）の提出**

プロセス①でリスクが高いと評価された案件に限り、リスクを評価（第二次評価）し、対処策を提示する。

**⇒様式3（リスク分析・対策）の提出**

## 研究・実証実験

データサイクル

取得 → 管理 → 加工分析 → 提供公開 → 廃棄

**プロセス④**

パーソナルデータ取扱い時のプライバシー対策

パーソナルデータの取得から廃棄まで、それぞれの段階で適切な措置を講ずる。

## 終了

**プロセス⑤**

研究成果等に関する適切なプレス発表

研究開発成果を対外的に公表する場合、一般市民に不安や不信を抱かせないようにする。

※：プロセス①は研究公募に対する提案時に行うが、委託研究契約後に新たにパーソナルデータを取り扱う必要が生じた場合はその時点で行うものとする。

# 研究開発で取り扱われ得るパーソナルデータ

委託研究において下記に例示するパーソナルデータを取り扱う計画があれば、研究計画段階（公募時）にチェックシート（様式1）を提出し、委託契約締結後、パーソナルデータを取り扱う前にチェックシート（様式2、3）を提出する。合わせて2回の委員会審議を受ける必要がある。

## 1. 被験者等の個人に関する情報
- 氏名、生年月日、年代
- 性別、出身地域、データ収録地域

## 2. 個人の特定につながる識別子
- マイナンバー、保険証、免許証等のID
- スマートフォン、ICカード等のID

## 3. 個人の特定につながる生体情報
- 画像・映像
  （顔、指紋、虹彩、体形、風貌等の特徴量）
- 音声（声紋等の特徴量）

## 4. 個人の特定につながる位置情報
- 住所（自宅、職場、学校等）
- 施設・設備利用ログデータ
- スマートフォンの位置（GPS、基地局情報）
- 車の位置（画像、映像、GPS、車両番号）
- 端末のアドレス（IP address、MAC address）

## 4. 個人の健康状態に関わる情報
- 病歴（カルテ・処方箋）
- 生体計測・分析（MRI/内視鏡/CT等）
- 心理計測・分析（知覚、認知、行動）

## 5. 個人の性質や行動に関わる情報
- アプリ、SNS、Web等への入力内容、時刻
- アプリインストールID
- 位置情報を分析して得た移動経路

## 6. その他、プライバシーに関わる情報
- 人種、国籍、宗教、思想、信条
- 職業、所得、資格、学歴、家族構成

# パーソナルデータ（PD）の取り扱いルール（１）

- 取り扱うパーソナルデータを必要最小限とする
  - 委託研究に必要なPD※1の種類や対象者を絞り込む。
  - 各PDの利用目的を具体的に特定※2し明確化する。
- 本人の同意を得る
  - 取得するPDの利用目的等※3について、本人にわかりやすく明示して同意を得る。
  - 本人が未成年者や高齢者等でPDの取り扱いに関する判断が難しい場合は、保護者等に説明して同意を得る。
  - 要配慮個人情報（個人情報保護法第2条第3号）は、あらかじめ本人の同意を得ずに取得してはならない。（受託者が適用を受ける個人情報保護関連法令により規定が異なるが、原則として本人の同意を必須とする。）
  - もし、個別に本人の同意を得られない場合は、取得するPDの利用目的等※3を本人が容易に認識できる形で通知※4又は公表※5する。
  - 公共空間の撮影において不特定の人、車両、家屋等が映り込む場合、前項の通知又は公表を行うとともに、委託研究において不要なPDの削除等の対策を行う。
  - 参考文献：カメラ画像利活用ガイドブックver2.0（https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000040.html）

※1：パーソナルデータを「PD」と略記。
※2：詳細は15ページに示す。
※3：詳細は16ページに示す。
※4：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る。
※5：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、受託者のウェブへの掲載（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る。

# パーソナルデータ（PD）の取り扱いルール（2）

- 本人からの要望を受け付ける
  - 本人から同意内容の変更やPDの利用停止等の要望を受け付ける窓口を設け、要望に対し適切に対応する。
- 利用目的以外の目的で利用しない
  - あらかじめ特定した利用目的以外の目的でPDを利用してはならない。
  - PDの利用目的を変更する場合は、あらためて本人の同意を得る。
- 個人の特定や機微な内容の推定をしない
  - 個人情報やプライバシーに該当しないデータであっても、他のデータと突合すると個人の特定や機微な内容の推定ができる場合がある。本人の同意なくこれらの分析を行わない。
- 外国との間でデータを移転する場合は関係各国の法令を遵守する
  - PDを外国機関（又は外国人）から取得、逆に外国機関へ提供する場合は、関係各国の法令を遵守する。
    - 特に欧州一般データ保護規則（GDPR）において、PDの処理や移転に厳しい制約があることに留意する。
  - 外国のクラウドサービスを利用する際は適用される法令、規約等においてPDが日本と同等に保護されることを確認する。

# パーソナルデータ（PD）の取り扱いルール（３）

- PDの管理
  - PDの目的外利用、漏えい、滅失、き損等を防ぐため、PD取扱者の指導・監督、アクセス権の管理を適切に行う。
  - 情報漏えいリスクを低減するため、PDの保存、通信にあたっては暗号化等の対策を行う。
  - PDの処理結果を本人へ伝達する等、本人を特定する必要がある場合はPDを仮名化し、仮名とPDとの対照表を厳重に管理する。
    - （注）仮名化された情報だけでは本人を特定できないが、対照表を用いれば本人を特定できるため、対照表の管理が重要となる。
  - PDの処理において本人を特定する必要がない場合は、PDを匿名化する。
    - (注)匿名化すると、元のPDに復元する手段はなく、本人を特定できなくなることに留意する。
  - 暗号化、仮名化、匿名化はそれぞれ意味が異なるので、チェックリスト等において、適切に使い分けて記述する。
- PDの破棄
  - あらかじめ定めた保持期間終了後直ちに、漏えいを防ぐ安全確実な方法でPDを破棄する。
  - なお、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。

# パーソナルデータ（PD）の取り扱いルール（４）

- PDを取り扱う委託研究に対する苦情・批判に関する対処
  - 委託研究におけるPD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は速やかに委託研究推進室に報告する。
  - エスカレーションすべき事案の判断基準（目安）を以下に示す。事案によるが、原則として、どれかひとつでも該当すれば事案が発生したと判断する。
    - 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
    - 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
    - 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もしくは機構に告訴があった場合
    - 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

# プロセス① 研究計画段階※

- パーソナルデータ取扱チェックリスト（様式1）の提出
  - パーソナルデータを取り扱う計画をしている提案者は、「パーソナルデータ取扱チェックリスト」の左上で「研究計画中（委員会にて様式1で審議する段階。プロセス1）」を選択し（上に「様式1」と表示されます）、必要事項を記載し、委託研究推進室に提出してください。委託研究推進室の担当者から委員会事務局に審議を依頼します。
  - 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。
    - 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てください。
- 委員会審議結果の通知
  - 委員会は、提出された様式1及び提案書に基づきプライバシーリスクの評価・助言を行います。
  - 委託研究推進室は、その結果を研究公募で採択された提案者に提示します。
  - 受託者は、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。
  - なお、当該プロセスで「プライバシー侵害の可能性がある情報」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は研究公募に対する提案時に行うが、委託研究契約後に新たにパーソナルデータを取り扱う必要が生じた場合はその時点で行うものとする。この場合は上記の提案者を受託者に読み替える。

# プロセス② 契約段階

- 委託研究契約におけるパーソナルデータの取り扱いに関する規定
  - 受託者がパーソナルデータを取り扱う研究開発を実施する場合、委託元である機構には研究開発の管理責任があるため、受託者との契約を通じて、受託者がパーソナルデータの適切な取扱いを行うことを確保します。
  - 具体的には、受託者は機構との委託研究契約において、委託契約約款　第50条（パーソナルデータの取扱い）を遵守してください。
    ① 受託者の責任に関する事項
    ② パーソナルデータの第三者への提供の制限又は条件に関する事項
    ③ 受託者でのパーソナルデータの管理・運営等についての調査に関する事項
    ④ パーソナルデータの漏えい等の事案の発生時における対応に関する事項

# プロセス③ パーソナルデータの取扱計画の決定

- パーソナルデータ取扱チェックリスト（様式2）の提出
  - 受託者は、委託研究契約締結後、パーソナルデータの取得を開始する前に、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計画（案）を策定し、「パーソナルデータ取扱チェックリスト」の左上で「研究実施前（委員会にて様式2を審議する段階。プロセス3）」を選択し（上に「様式2」と表示されます）、必要事項を記載して、委託研究推進室に提出してください。
  - 「様式2」は、プロセス①で記載した情報が表示されますが、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させて提出してください。またリスク評価１のコメントを『委員会からの「パーソナルデータ取扱研究開発に対するリスク評価結果」への回答』欄に転記し、回答を書いてください。
- パーソナルデータのリスク分析・対策（様式3）の提出
  - 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・対策」※を作成し、提出してください。
    (※様式に指定はありませんが、参考の様式はあります。)
- 委員会審議結果の通知
  - 委員会は、提出された様式2及び3に基づきプライバシーリスクの評価・助言を行います。
  - 委託研究推進室は、その結果を受託者に提示します。
  - 受託者は、委員会の助言内容を踏まえて、プロセス④以降を進めてください。

# プロセス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

- 委託研究におけるパーソナルデータの適切な取り扱い
  - 受託者は委託研究において、委員会審議による助言結果とパーソナルデータ取り扱いルール（5ページ～8ページ）に従い、パーソナルデータを取り扱うものとします。
  - なお、プロセス③以降に、新たなパーソナルデータの追加や変更、提供先の変更等、パーソナルデータの取扱計画を変更する場合は、事前に「パーソナルデータ取扱チェックリスト（様式2）」を再度、委託研究推進室に提出してください。提出内容に応じて委員会で再度審議を実施します。
- 本人からの同意の取得について
  - 本人からの同意を取得する際に明示して説明すべき事項を16ページ、同意書の例を17ページにそれぞれ示します。

# プロセス⑤ 研究開発プロジェクトに関するプレス発表時の措置（1）

- パーソナルデータを用いる委託研究の実施や成果等をプレス発表する場合
  - パーソナルデータを用いる実験実施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本人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。
  - 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の担当者に提出するようお願いしています。プロセス①や③の過程でリスクが高いと判定されたものについては、原稿の修正やプレス発表の中止を依頼する場合があります。
- プレス発表原稿の事前確認
  - 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。

# プロセス⑤ 研究開発プロジェクトに関するプレス発表時の措置（2）

- プレス発表原稿の事前確認（つづき）

## ④ パーソナルデータの提供の有無及び提供先

- パーソナルデータの第三者への提供の有無と、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

- 利用者が受託者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持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（委託研究約款）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

- 発表内容に関する問合せ先：メールアドレス、電話番号など
- 問合せ事項により異なる場合は、それぞれの問合せ先

# パーソナルデータの利用目的の特定

- パーソナルデータの利用目的の特定
  - 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してください。
  - その際、利用目的は、「〇〇技術の研究開発のために利用する」、「〇〇メカニズムの解明に関する研究のために利用する」、「〇〇実証実験において、〇〇を行うために利用する」等、利用の範囲に応じて記載してください。
  - 単に「〇〇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す。
  - 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載してください。
  - 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です。
  - 利用目的の記載例
    - 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（〇年〇月～同年〇月）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。

# パーソナルデータの利用目的等の明示すべき事項

- 本人の同意を取得する際等に明示すべき事項

1. データの種類・内容、取得方法
2. データの利用目的・利用方法
   - 利用目的の記述については、前ページの「パーソナルデータの利用目的の特定」に従ってください。
3. 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てください。
4. データを第三者に提供する場合はその旨も含めてください。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してください。
5. データを海外の第三者に提供する場合はその旨を含めてください。
6. 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てください。
7. データの安全管理措置を記載してください。
8. データの保持期間・破棄方法を含めてください。
   - データの保持期間は、利用目的にかんがみ適切な期間を定めてください。
   - 現時点で未定だが将来の研究に用いる可能性がある等、データ取得前までにデータの保持期間を定めることが難しい場合には、その旨を予め同意書等に記載してください。
   - 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年間としています。
   - 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触れてはいません。例えば、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です。
9. パーソナルデータの取得・利用の中止（オプトアウト）の可否。可の場合は方法を記載してください。
10. 問い合わせ先を記載してください。

# 同意書の文例

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：**

電話:　　Email:

**実験の概要**：

皆様には、●●の技術を利用した●●の体験をしていただきます。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とおりです。

- 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○○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、要望に基づいてデータの利用を停止する。
- ○○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、申し出により本実験で取得された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に使用します)