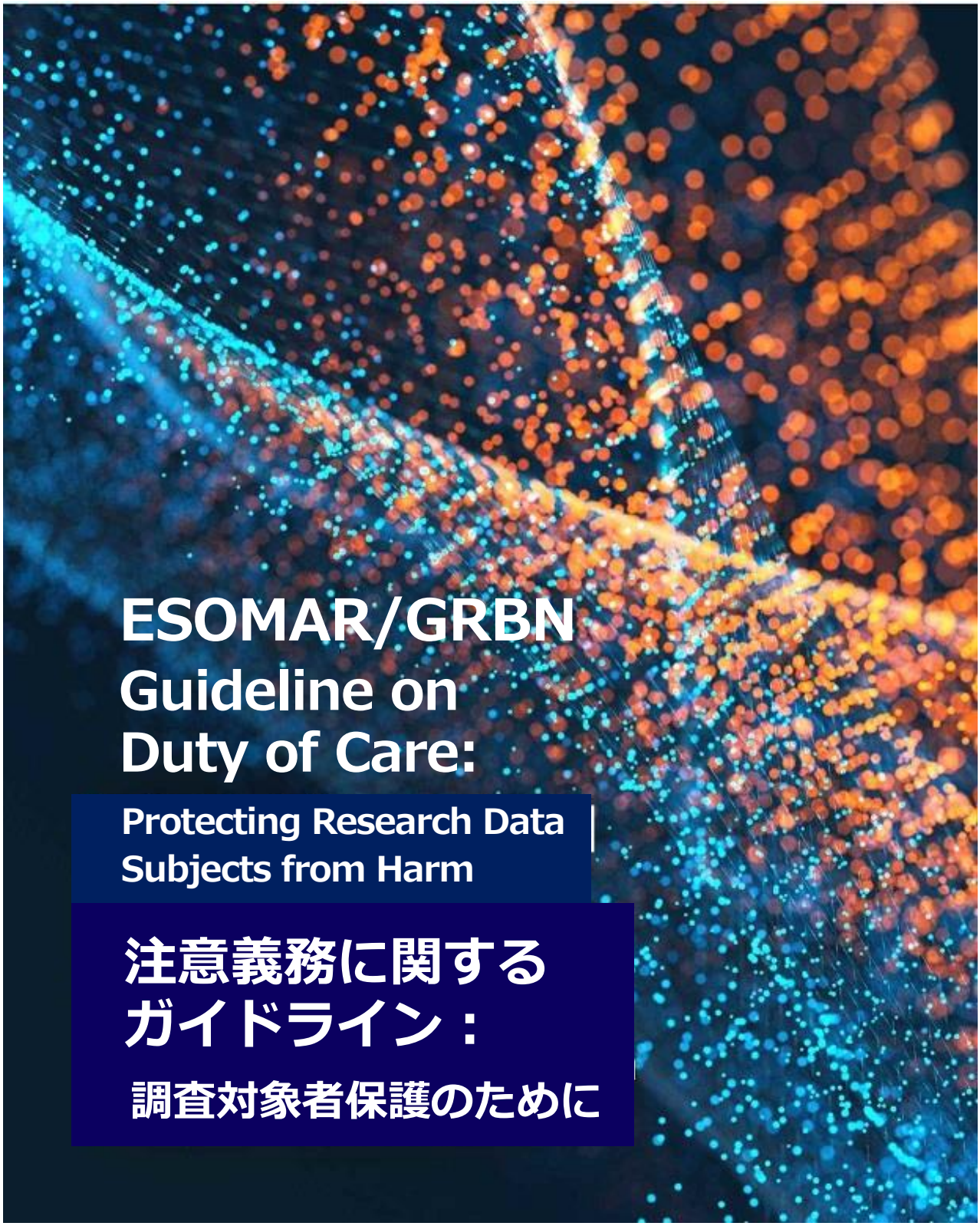
ESOMAR

GLOBAL RESEARCH BUSINESS NETWORK
APRC • EFAMRO • ARIA • AMRA



ESOMAR/GRBN Guideline on Duty of Care:

Protecting Research Data Subjects from Harm

注意義務に関するガイドライン：

調査対象者保護のために

JMRA

2021 年 9 月

目　次

1 はじめに

社会のあらゆる分野の意思決定者は、さまざまな構成員に利益をもたらす製品、サービス、及び政策を開発するために、自らが活動する環境を明確に理解する必要がある。市場・世論・社会調査及びデータ分析（以下「調査」）は、営利組織、政府、非営利組織、一般市民が証拠に基づいた意思決定を行うために必要なデータとインサイトを提供する。これには、多くの場合、大量の個人データの収集と処理が必要になる。そうすることにより、リサーチャーは、調査に参加した結果として、または調査の目的のために彼らのデータが使用された結果として、不利な処遇または危害を経験しないことを確実にし、個人データ及び個人のプライバシーを保護するために、データを収集及び処理する個人（以下「データ主体」）に対する注意義務を負う。

歴史的に、リサーチャーの主要な倫理的責任は、データ主体を自発的なダイレクト・マーケティングやその他の販売指向活動の害から保護することであった。最近では、あらゆる種類のデータが急増し、複数のソースからのデータをリンクして個々のデータ主体に関する豊富なプロファイルを作成できるようになったため、マーケティングや販売にとどまらず、医療サービスの提供、信用供与、刑事司法捜査、雇用に関する決定など、さまざまな分野でデータが新たに利用されるようになっている。このような利用は、データ主体のプライバシーを侵害するだけでなく、差別的である可能性もあり、一部の個人を他の個人よりも優遇し、不完全または偏った情報に基づいてそうする可能性もある。

同時に、あらゆる部門の組織によるデータ取得、処理、分析、提供のための最新技術の利用が継続的に拡大していることは、データ主体にとって新たな一連のリスクを生み出している。これには、個人データの不正な開示や、外部の個人または組織によるデータ侵害が含まれる。

データ主体のプライバシーと福祉を保護するという私たち専門職の責任を果たすには、調査業務を委託または実施する組織と個人が、所有する個人データを偶発的またはその他の不正な開示から保護するためのプロセス、ツール、標準、及び技術の適切かつ効果的なインフラストラクチャを提供することが必要である。そのような開示が行われた場合、データ主体及び規制当局に対して最終的に責任を負うことを認識しなければならない。

2 目的と対象範囲

本ガイドラインの目的は、調査に参加するか、または調査の目的のためにデータが処理されるデータ主体のプライバシーと福祉を保護する責任について、リサーチャー及びクライアントに代わって調査を行う者のために助言することである。また、調査を委託した者が自らの責任を十分に認識し、確立された倫理的・法的要求事項の下で何が可能で何が不可能かについて、期待値を設定するためのガイダンスを提供することを意図している。

このガイドラインは、主として（クライアント組織内の人を含む）リサーチャーや、主にデータ分析を専門とするその他の人々を対象としているが、調査のための個人データの収集や処理に関与する個人や組織にも幅広く適用される。

ここに記載されている要求事項及びベストプラクティスは、特定の国または地域の法的要求事項を反映するものではない。むしろ、ICC/ESOMAR の市場・世論・社会調査及びデータ分析に関する国際規範、既存の ESOMAR/GRBN のガイダンス文書、世界各国の協会の綱領とガイドライン類を補完するように設計されている。したがって、本ガイドラインを単独で参照すべきではない。

この ESOMAR/GRBN の指針は、国内法に優先するものではない。国際プロジェクトに責任を負うリサーチャーは、本ガイドラインの規定を最低限の要求事項とし、法律または国が合意した基準に定められたその他の責任をすべて果たすべきである。これは法的助言ではなく、そのように信頼されるべきではな

い。リサーチャーの責任は、調査に影響を与える可能性のあるいかなる法律にも遅れずについていくことと、関係者全員がその要求事項を認識し、それに従うことに同意することである。

この文書では、必須の要求事項を特定するために「must」という語が使用されている。リサーチャーが守らなければならない原則や実践を表すときに、「しなければならない」という言葉を用いる。
「should」という言葉は、推奨事項を説明するときに使用される。この用法は、リサーチャーが調査の設計に応じて異なる方法で原理または調査活動を実施する際に、選択ができることを伝えるように意図されている。

3 用語の定義

本文書の目的上、これらの用語は以下の特定の意味を持つ。

API（アプリケーション・プログラミング・インターフェース）
コンピュータ・プログラムが他のプログラムまたはコンポーネントと通信する際の基準となり、また、内部または外部でのアクセス/データ交換をサポートできる一連の定義。

Automated decision-making system（自動化意思決定システム）
人間が介入することなく反復的な運営面の決定を行う、定められたルールに基づいて稼働するシステム。

Children（子供）
調査に参加しようとする個人は、親、法定後見人、または責任ある大人から許可を得なければならない。子供の年齢の定義は国によって大きく異なり、各国内法及び自主規制規範によって定められている。国による定義がない場合、子供は 12 歳以下、「若者」は 13 歳から 17 歳と定義されている。
（日本語版注記：日本では JMRA 綱領で「中学生以下」と定義している）。

Client（クライアント）
調査プロジェクトの全部または一部を依頼、委託、または申し込む個人または組織。

Consent（同意）
個人データの収集及び処理に対して、本人の自由意思に基づいて与えられ、かつ、明確に示された合意。

Data analytics（データ分析）
調査目的のために、隠れたパターン、未知の相関関係、傾向、好み、及び他の有用な情報を明らかにするために、データセットを調べるプロセスを意味する。

Data provenance（データの出所）
１つ１つのデータの起源と、それがデータベース間を移動する場合に追跡すること。

Data subject（データ主体）
その個人データが調査に使用されるすべての個人。

Deductive disclosure（演繹的特定）
クロス分析、少量サンプル、または他のデータ（クライアントの記録や公的機関の二次データなど）との組み合わせによって、あるデータ主体を推論的に特定すること。

Harm（危害）
有形的及び物質的な損害（身体的な傷害や金銭的損失など）、無形的または道徳的な損害（評判または信用の失墜など）、または私的な生活への過度の侵害を意味し、求められていない個人を標的としたマーケティング・メッセージを含む。

Non-research activity（非調査活動）
個人データが収集または分析された個人に対して、その個人の態度、意見または行動を変える目的で直接的な行動をとること。

Passive data（受動的データ）
個人の行動または態度を観察、測定または記録することにより、個人データを収集すること。

Personal data（個人データ：時には個人を特定できる情報、または PII と呼ばれる）
例えば、直接的な識別子（名前、特定の地理的位置、電話番号、画像、音声、ビデオ録画など）を参照することによって、または間接的に個人の身体的、生理学的、精神的、経済的、文化的若しくは社会的特徴を参照することによって、個人を特定するために使用することができる自然人に関するあらゆる情報。

Primary data（一次データ）
調査の目的のためにデータ主体から、またはデータ主体についてリサーチャーが収集したデータ。

Privacy（プライバシー）
個人が他からの侵害や干渉から自由であり、自分自身に関する情報を制御、編集、管理及び削除する能力を有し、そのような情報をどのように、どの程度他人に伝達するかを決定する能力を有することを前提とする個人の権利。

Privacy Impact Assessment（プライバシー影響評価：時に PIA または DPIA と呼ばれる）
データ主体のプライバシーリスクを特定し、軽減するプロセス。

Profiling（プロファイリング）
調査以外の目的でデータ主体に直接的な働きかけを行うために、データ主体の業務上のパフォーマンス、経済状況、健康状態、個人の嗜好、関心、信頼性、所在地、行動を分析または予測する目的で、個人データを収集及び処理すること。

Research（リサーチ：すべての形態の市場・世論・社会調査及びデータ分析を含む）
個人や組織に関する情報の体系的な収集と解釈。社会科学、行動科学、データ科学を応用した統計的・分析的方法と技術を用いて、インサイトを生み出し、企業、政府、非営利団体、一般市民による意思決定を支援する。

Researcher（リサーチャー）
調査に関するコンサルタントとして活動する個人または組織。クライアントの組織及び使用される二次契約業者で働く者を含む。

Secondary data（二次データ）
すでに収集され、別の情報ソースから入手可能なデータ。

Segmentation（セグメンテーション）
広範な対象母集団を、共通のニーズ、関心、優先事項を持っているか、持っていると思われる個人または組織のサブセットまたはグループに分割し、それらを相互作用するための戦略を設計し実行することを目的とした分析技術。セグメンテーションはプロファイリングとは異なり、個々のデータ主体ではなく、共通の特徴を持つ明確に定義された人々のグループに焦点を当てている。

Sensitive data（機微なデータ）（国によっては「特殊カテゴリーデータ」とも呼ばれる）
個人や組織のプライバシーまたはセキュリティを保護するために、現地の法律で許可されていないアクセスから可能な限り高いレベルで保護することが要求されている特定の種類の個人データであり、処理前にデータ主体からの追加の明示的な許可が必要になる場合がある。機微なデータの指定は行政区域によって異なり、データ主体の人種または民族的出自、健康記録、生体情報及び遺伝子データ、性的指向または性的習慣、犯罪記録、政治的見解、労働組合への加入、宗教的または哲学的信念などを含むが、これらに限

定されない。また、所在地、財務情報、規制薬物またはアルコールの使用などの違法行為など、その他の種類のデータ（必ずしも法的に定義されているわけではない）を含む。

Vulnerable individuals（保護を要する人々）
認知障害またはコミュニケーション障害を有する人を含め、自発的かつ得られた情報に基づく意思決定を行う能力が限られている人々。

Web scraping（ウェブスクレーピング）（時にクローリングまたはスパイダーとも呼ばれる）
Web サイトからデータを抽出するためのソフトウェアを使用すること。

4 主要な原則

市場・世論・社会調査及びデータ分析の長い歴史を通して、リサーチャーは、個人データがいつ、どのように収集され、使用されるかを決定する固有の権利が個々のデータ主体にあることを認識してきた。この目的のために、調査は 3 つの最も重要な原則によって統治されてきた。

1. 調査の目的のためにデータ主体から個人データを収集する場合、リサーチャーは、収集する予定の情報、それが収集される目的、それが誰と共有される可能性があるか、どのような形式であるかについて透明性を確保しなければならない。
2. リサーチャーは、調査に使用される個人データが不正なアクセスまたは使用から保護され、データ主体の同意なしには開示されないことを確実にしなければならない。
3. リサーチャーは、常に倫理的に行動し、適用されるすべての法律及び規制を遵守し、データ主体に危害を及ぼしたり、調査の評判を傷つけたりするようなことをしてはならない。

これらの原則[1] は、私たちがデータを依存している一般市民と、より良い決定を下して長期的に成功することを支援するために私たちを雇ったクライアントの信頼の基盤を形成する。これらの原則は、私たちの長い歴史の中でいつでもそうであったように、今日においても重要である。

5 調査活動と非調査活動

端的に言えば、リサーチャーや調査を委託する人々が直面する本質的な課題は、最初にデータ主体の同意を取得することなく、調査の目的のために収集され処理されたデータが、調査以外の目的に使用されないようにすることである。この区別は、学問的な問題以上のものである。多くの国は、調査の社会的・経済的価値を認識しており、その規制の枠組みは、目的が調査である場合には、より柔軟性を許容している。次に例を示す。

- データ主体となる可能性のある人物に調査への参加機会を提供する、未承諾な連絡先に対する制限の緩和；
- データ保存期間の延長（例：アーカイブ）；
- 子供や若者を調査に参加させる際の負担の少ない要求事項；
- 「機微」な情報と定義される可能性のあるデータの収集または使用に関する制限の緩和；

[1] 経済協力開発機構 (OECD) も同様のプライバシー原則を支持しており、世界中の多くの既存及び新興のプライバシー及びデータ保護法に反映されたプライバシー・フレームワークを構成している。詳細は、OECD Privacy Framework を参照。

- 調査と互換性のある目的として定義するなどして、データ主体の同意を必要とせずに、調査のために二次データを再利用する自由度を高めること。

調査活動と非調査活動とを区別する際に誠実で正直でないことは、明確で独立した目的としての調査の長期的な持続可能性に不可欠な社会的信用と規制上の便益を失うリスクがある。

調査と非調査との重要な違いは、調査の目的は統計的・社会科学的分析とインサイトの提供に限定されていることである。その目的は、個人データを作成したり、特定のデータ主体に対して働きかけを行うための根拠を提供したりすることではない。リサーチャーは、より大きなグループの代表者としての場合を除いて、個々のデータ主体の特定には関心がない[2]。個人情報の収集・処理者の身元は開示されず、厳重に保護されている。

その他の活動は、人々に連絡を取り、質問をし、データを記録し、分析するという点で、調査と表現されることもあれば、少なくとも調査に類似しているように思われる。また、他の情報ソースやデータセットからデータを収集することで、既存のデータを強化することもできる。データがどのように使用されるか（データを収集する目的）によって、その活動が調査であるかその他であるかが決まる。データが収集または処理される個人に対して直接働きかけを行うことを目的としている場合、その個人の意見、態度、行動を変えたり、他の個人的な方法で影響を与えるかどうかにかかわらず、その目的は調査とはみなされない。

しかし、本ガイドラインでは、リサーチャーが非調査活動に従事する場合があることを認識している。その際には、データ主体に対して、その目的、データがどのように使用されるかについて、その使用のための同意を獲得し、その活動を調査とは表現しないことを明確にしなければならない。

6 プライバシー影響度評価

冒頭で述べたように、調査には通常、個人データの収集が含まれ、直接的にはデータ主体から、間接的には二次的なデータソースから収集される。すべての場合において、関係者には、データが収集または処理されるデータ主体のプライバシーを侵害しないことを保証する責任がある。プライバシー影響評価（PIA）は、組織が調査を設計する際に、リサーチャーに要求する有用なツールである。

6.1 PIA とは何か？

PIA はリスク管理ツールであり、データ主体に対する潜在的なプライバシーリスクと、調査組織に対する潜在的な法令遵守リスクを特定する。簡単に言えば、PIA は調査プロジェクトのライフサイクルを通じて、データ主体の個人データとプライバシーに対するリスクを体系的に特定し、軽減するプロセスである。

PIA の設計は、組織のビジネスと内部プロセスによって異なる。評価は個々のプロジェクトレベルで実施され、プロジェクトの計画段階で実施され、個人データの計画的な使用を対象とすることが望ましい。各評価の記録は維持されることが望まれ、プロジェクトが進展し、元の設計に重要な変更が加えられたときに更新される[3]。

[2] 例外の 1 つは、品質保証のための個人データの使用である。

[3] PIA に関する特に有用な議論については、ICO 出版の「プライバシー影響評価の実施：行動規範」を参照。

6.2　どのような状況の時に PIA を求めるか？

ベストプラクティスとしては、個人データの収集または使用を含むすべてのプロジェクトに対して PIA が必要であろう。それが現実的でない場合には、リサーチャーはプライバシーに関する懸念が高まっていることを示す、PIA を必要とする特定のプロジェクトの特徴を考慮する必要がある。次のリストは単なる例であり、すべてを網羅するものではない。

- 大規模なデータ処理、特にデータ項目数、データ主体の数、予定されている保存期間、地理的範囲；
- 一致または結合されたデータセットの使用；
- 継続的かつ体系的なモニタリングを伴うデータ収集；
- 機微なデータの収集または処理（特別なカテゴリーのデータ、財務情報または有罪判決や犯罪に関するデータも含む）；
- 評価または採点を含むデータ処理；
- 二次契約業者への個人データの委託処理；
- 新しい技術や方法論の使用；
- 子供や保護を要する人々に関するデータの収集・処理；

  国境を越えたデータ転送。

6.3　PIA プロセスのステップ

PIA には通常、以下の 4 つのステップまたは段階がある。

6.3.1　組織内の計画された情報の流れを図示する

データを取得する目的と、データの収集、処理、保護、及び保持方法をできる限り詳細に説明する。個々の組織は、これらの分野で類似した業務を行っていることが多いが、組織の構造や、二次契約業者を通さずに内部で行う業務、処理されるデータの種類、顧客に提供されるインサイトを生成するために使用される統計的・分析的手法によっても、かなりのバラツキがある。組織外の人々（二次契約業者や顧客など）とデータを共有する計画がある場合は、特に注意を払う（収集時にデータ主体が合理的に予測できない方法でデータを利用すること、及び調査の目的を達成するために必要ではないが計画されていた処理段階など）。

6.3.2　潜在的なリスクとその重大性・発生可能性の特定

この段階でリサーチャーは、そのプロジェクトがデータ主体のプライバシーにどのような影響を与える可能性があるかを体系的に検討する。この段階では、データが収集または処理される国で適用されるすべての法的要求事項にプロジェクト計画が適合していることを確認することも同様に重要である。

包括的なリストというわけではないが、調査から発生する可能性があるリスクには明らかなカテゴリーがいくつかある。これには次のようなものが含まれるが、これらに限定されない。

- 個人データを利用して個々のデータ主体に直接働きかけることを含む、非調査活動；
- 調査活動と非調査活動との区別が不十分であるため、さらにデータ主体を、ダイレクト・マーケティングを含む直接的な働きかけにさらすこと；
- 過剰または不適切な情報の収集（機微な情報を含む）；
- 過度に長期にわたるデータ保存方法；

- 収集時にデータ主体に開示されていない目的でのデータの利用；
- ごまかしによって、またはデータ主体の知識なしに収集されたデータの使用；
- 顧客に個人情報を提供することを含む、同意を得ない第三者への開示；
- データ主体のコメントや引用を広告目的で利用すること；及び
- 不適切な組織内のプロセスや第三者のデータ処理者のプロセスなど、データ漏えいにつながる可能性のある、効果的でない情報セキュリティ慣行。

これらのうち、リストの最初に挙げられた「個人データを利用して個々のデータ主体に直接働きかけること」は、以前から大きな懸念事項となっていた。この問題に対処するため、リサーチャーは、厳格な同意のプロセスに頼るようになっている。このプロセスでは、さまざまな条件の中でも、データ収集の目的、データがどのように使用されるかの説明、データが共有されるかどうか、共有される場合にはどのような形式で誰と共有されるかを指定する。

6.3.3　特定されたリスクを軽減するソリューションの開発と評価

これは、特定されたプライバシーリスクに対処し、適用可能なすべての倫理的及び法的要求事項の遵守を確実にするために、組織が取らなければならない行動を特定するポイントである。ESOMAR の「データ保護チェックリスト」、または各国協会のデータ保護ガイダンスは、ソリューション開発のための推奨資料である。 データプライバシーに関する規制を日常的な用語に変換し、組織がグローバルなデータ保護の枠組みの中で責任を果たすための指針となる。また、組織のプライバシー保護対策におけるギャップを特定することにも役立つ。

このステップを費用対効果分析と表現するのは妥当かもしれないが、組織は、データ主体のプライバシーを保護する義務を果たさないと、評判が損なわれるだけでなく、多額の罰金や訴訟につながる可能性があることを認識する必要がある。そのために重要なことは、情報源にかかわらず、調査プロジェクトや個人データの取り扱いに関わるすべてのスタッフが、組織のプライバシー保護プログラムを認識し、訓練を受けることを確実にすることである。

6.3.4　リスク軽減ソリューションを組織のプロセスと計画に統合する

最終段階は、他の類似したプロジェクトと同様に、計画されたプロジェクトのために使用されるプロセスへのソリューションの実装である。

6.4　いくつかの具体的な懸念事項

調査これまで、その歴史を通じて、プライバシー保護の保証を厳格な同意のプロセスで管理する一次データの収集に頼ってきた。この 10 年ほどの間に、新しい技術の組み合わせ、収集されるデータ量の劇的な増加、そして調査と非調査目的の両方のための、そのデータのますます革新的な使用は、調査の組織に、データ主体の権利を保護するための従来のプロセスを再考することを促してきた。いくつかの具体的な懸念事項が浮上し、調査業界と規制当局の双方が解決策を模索し始めている。完全なリストではないが、以下のようなものである。

6.4.1　受動的なデータ収集

受動的データの収集は、広く使用されている調査のアプローチであり、オンライン視聴率の測定、店舗内の行動追跡、広告テスト、ブランド、製品、選挙の候補者などに関する態度や意見が含まれるが、これらに限定されない。一般的な収集手法には、行動追跡ソフトウェアや、Web サイトの所有者が提供する API の使用などがある。

このようなデータを収集する場合、リサーチャーは同意を得るためにあらゆる合理的な努力を払い、個人データの使用を調査やその他の正当な調査目的に限定しなければならない。データ主体から直接同意を得ることができない場合（ウェブサイトへのトラフィックを測定する場合など）、リサーチャーはデータを収集するための法的に許容される根拠を持たなければならず、かつ運用上可能な限り速やかに識別可能な特徴を削除または不明瞭にしなければならない。さらに、たとえ間接的であっても、同意を得ることができないことを補うための努力がなされていることを示すために、適切なプラットフォームを使用して、そのようなデータ収集と利用の実践に関する顕著な情報を利用可能にしなければならない。これは、調査業界や専門家団体が主導する最近の産業イニシアチブに参加することによって達成できる。これらは、データ主体に合わせて間接的かつ顕著な情報を提供したり、オプトアウトの仕組みを提供するために使用することができる。

Web スクレーピングを使用してこのようなデータを収集する前に、リサーチャーはサイトの利用規約を調べる必要がある。これは、多くの場合、著作権や知的財産権を保護するためにスクレーピングを禁止しているためである。

6.4.2 二次データの利用

リサーチャーも非リサーチャーも、既存のデータ（公開と非公開の両方）を取得して使用し、一次データの収集を強化または置換することにますます注目している。一次データ収集の場合と同様に、調査と非調査の主な違いは、調査が自らを統計・社会科学、行動分析、インサイトの提供に限定していることである。リサーチャーは、データのさらなる処理が、直接的にも間接的にも、例えば演繹的特定を通じてデータ主体のプライバシーを危険にさらすことのないように、調査を設計しなければならない。組織は、事前の同意なしには、個々のデータ主体の身元が識別または明らかにされないようにし（直接的に、または他のデータと組み合わせることによって）、データ主体が特定される可能性を低下させるためにデータの細分性を低下させる措置を用い、調査のために使用されたデータの直接的な結果として、非調査活動がそれらに向けられないようにしなければならない。

6.4.3 機械学習とその他の AI アプリケーション

過去 10 年ほどの間に、リサーチャーらは分析技術を拡張し、行動の結果を予測したり、非構造化データの分析操作などを自動化するアプリケーションを構築する機械学習技術を組み込んだ。こうした業務の大多数は、大量の個人データを含む大規模なデータベースに依存している。伝統的なデータ保護の原則は、そうしたデータを保護するのに適してはいるが、通常、実際のモデルの保護には含まれていない。しかし、これらのモデルでは、それらを訓練するために使用された個人データや、モデルが製造中に処理したデータ主体の個人データを開示するようにリバースエンジニアリングすることができる。このような侵害に対する防御技術はまだ開発途上である。さらなる議論については、FPF の報告書「警告のサイン：機械学習の時代におけるプライバシーとセキュリティの未来」と、ICO 出版の「ビッグデータ、人工知能、機械学習、データ保護」を参照。リサーチャーは、データ保護インフラストラクチャを開発する際に、このようなタイプの潜在的な開示リスクを警戒し、確実に防御するようにしなければならない

6.4.4 セグメンテーションとプロファイリング

多くの場合、調査において個人データがどのように使用されるかについて、調査以外との違いは、セグメンテーションとプロファイリングの違いとして表すことができる。セグメンテーションは、共通のニーズ、関心、及び優先順位を持つ人々のグループを定義するために使用できる特性のクラスタを識別する分析技法である。その焦点は、個々のデータ主体ではなく、共通の特徴を持つ、明確に定義された人々のグループにある。最も重要なことは、その研究に使用されたサンプルがクライアントから提供されたものであっても、データ主体の個人データはクライアントとは共有されないことである。セグメンテーションは、合法的な調査活動である。

プロファイリング（行動ターゲティングとも呼ばれる）は、ダイレクト・マーケティングのような非調査目的のために個人としての個人に向けた直接的で、個別化された行動をとるためにそのデータを使用することを意図し、個々のデータ主体に関する個人データの収集に焦点を当てる。一般的には、自動化された意思決定システム（次のセクションを参照）の文脈で使用される。データは調査に利用されるかもしれないが、そのような調査は主要な目的ではない。主な目的は、個人データを使用して、調査目的以外で個人をターゲットにすることである。したがって、プロファイリングは調査ではない。

6.4.5　自動化された意思決定システム

過去 10 年間、あらゆる種類のデジタルデータの爆発的な増加に伴い、消費者データを広範な目的のために収集し分析する新しいサービスが登場した。その目的の一部は調査向けだが、大部分はそうではない。その中でも重要なのは、自動化された意思決定システム、すなわち、個々のデータ主体のプロファイルを使用して、人間の介入なしに管理上の意思決定を行うルールベースのシステムの開発である。これらの決定は、個々のデータ主体のプライバシーと福祉に対するさまざまなレベルの影響を伴及ぼす広範な活動を対象としており、その一部は明らかに差別的である。これらは、大きく 4 つのカテゴリーに分類できる。

- 機会損失（例えば、雇用、保険・その他の給付へのアクセス、住宅、教育）；
- 経済的損失（例えば、信用供与、商品やサービスの価格設定、選択の幅の狭まり）；
- 社会的損害（例えば、感情的圧力、公共の恥、選択的広告）；及び
- 自由の喪失（例えば、監視の強化、投獄）[4]。

その結果、調査では、個人データの収集、使用、及び処理について、特にオンラインの手法を使用して行動データを収集する場合には、能動的または受動的な手段にかかわらず、より広範な議論が行われるようになった。現在、一部には「調査」という言葉を使って、マーケティングや販売目的だけでなく、経済的幸福、健康、雇用機会などに影響を与える可能性のある幅広い決定を自動化するために、個人のプロファイルを作成するデータ駆動型の業界を指す人もいる。この曖昧な境界線は、データ分析と非調査活動の区別を継続的に実証する際にリサーチャーが直面する困難を浮き彫りにしている。

多くの場合、個々のデータ主体への影響の重大性という観点から、各国の規制の枠組みによって、このデータの使用方法が規定されることがある。ただし、組織は、収集または処理する個人データが、データ主体のプライバシー及び福祉に直接影響を与える目的で使用されることを許可してはならない。

明確な 1 つの例外は、リサーチャーが運用効率を高め、データ品質を維持するために自動化システムを使用することである。これには、サンプルの選択、インタビュアーの作業負荷の管理（コールスケジューリング、自由回答質問のコーディング、データ準備、自動レポート生成など）が含まれるが、これらに限定されない。このような状況では、個々のデータ主体への影響は重要な懸念事項ではない。

6.5　リスク軽減ソリューションを組織のプロセスと計画に統合する

最後のステップは、プライバシー影響評価によって特定されたリスク緩和策を実施することである。各ソリューションは、組織の構造とそれが実行する業務のタイプに照らして評価され、それが特定のプロジェクトのために実施されるべきか、または組織のすべての調査活動のための標準運用手順とすべきかを判断することが望ましい。前述のように、ESOMAR「データ保護チェックリスト」は推奨されるリソースの１つである。その他には、各国の協会やデータ保護規制当局が作成した DPIA ガイダンスが含まれる。

[4] 詳細については、Future of Privacy Forum(2017)、「アルゴリズムによる不公平性：自動化意思決定の弊害の解明」を参照。

7 特定の種類の調査に関連するプライバシーリスク

組織は、従業員が有効な調査の慣行と、（個々のデータ主体に対して直接働きかけを行うことを含む）調査目的以外でのデータ収集及び取扱い活動とを、確実に区別できるようにしなければならない。このセクションでは、多くの一般的な調査手法について説明する。これらの手法はすべて、個々のデータ主体が完全に保護され、識別・開示されないようにするために有効である。

7.1 世論調査

世論調査は、ある時点での選挙などの政治的話題についての世論を把握するために行われる。彼らは、一般市民全体または特定のサブグループの代表的なサンプルについて報告する。

しかし、商品を販売したり、資金を調達したり、候補者や課題を宣伝したりするための活動を、世論調査やそれに類する調査と偽ることがある。データ主体は合法的な調査質問と思われるものを尋ねられ、お金を寄付したり、商品を購入したり、政治的なメーリングリストに自らの名前を追加したりするように求められる。「サギング」（調査を装った販売行為）、「フラギング」（調査を装った募金活動）、調査を装ったキャンペーンは調査ではなく、協力を求める際にリサーチャーがそのような表現をしてはならない。

7.2 調査データベースの充実とデータ統合

クライアントの組織は、彼らの顧客の調査が主な目的であり、さらなる調査のためのより広範な基盤を構築する調査活動を通じて収集した個人データを用いて、彼らの顧客データベースを充実させようとすることがある。分析目的でデータベースを拡張することだけが目的であれば、これは正当な調査である。

しかし、個々のデータ主体に対して直接的な働きかけを行うためにデータを利用しようとするのであれば、それは調査ではなく、リサーチャーはそのような提示をしてはならない。

7.3 視聴率調査

視聴率調査は、広告を含むメディアコンテンツに触れた聴衆の規模に関する集計された統計値をクライアントに提供する。これは、メディア所有者や広告主が広告スペースの価値を判断することを可能にし、特にラジオ、テレビ、インターネットなどの幅広いサービスや情報の提供を支える基本的な機能である。

ただし、報告されるセグメントが非常に詳細かつ細分化されているため、特定のデータ主体をターゲットにして個々の要求事項に合わせたコンテンツを作成できる場合、これはプロファイリングであり、したがって調査ではない。リサーチャーは、調査プロジェクトの一環として収集されたそのようなデータが、クライアントに提供される前に可能な限り匿名化されるよう、必要な注意を払わなければならない。

7.4 ミステリーショッピング

ミステリーショッピングは、クライアントの組織が広告、ブランディング、商品やサービスの上市を通じて顧客に毎日約束していることが、実際に顧客への提供時点で満たされているかどうかを判断するのに役立つ。 約束の例としては、具体的な価格やプロモーション、知識があり親切なスタッフ、清潔で歓迎的な店舗、迅速な電話サービス、簡単で直感的なオンラインショッピングなどがある。これらの約束は、現場の第一線のスタッフ、コールセンター、チャットラインによって提供されることになっている。ミステリーショッピングは、顧客に与えられた約束の遵守を測定する。

ミステリーショッピングという一般的な名目の下で、2 つの非常に異なるタイプの調査が行われるかもしれない。第 1 のタイプでは、収集されたすべての個人データは機密に保持され、クライアントとは共有されず、調査目的でのみ使用される。第 2 は、クライアントが個人データを機密として扱わず、科学的調査以外の目的（例えば、個人の業績向上やボーナス制度の運用）のために、データ主体に個別にアプローチするために使用される。個人データを調査以外の目的で利用する後者のケースは、調査とはみなされな

い。リサーチャーは、調査の設計と実行を通して、提案書の段階からこの区別を監視するよう注意しなければならない。

7.5　ソーシャルメディア調査

ほとんどフィルターをかけられていないソーシャルメディアユーザーの投稿は、公共部門であれ民間部門であれ、企業や組織が関心を持つさまざまな問題に関するインサイトの情報源として、ますます有益なものとなっている。社会の推進力やトレンドを早い段階で理解することで、ステークホルダーは早期かつタイムリーな行動を取ることができる。

しかし、そのデータの多くは、直接的または間接的にデータ主体を識別するために使用することができ、したがって非調査目的に使用することができるという点で、個人データである。営利目的のメッセージをターゲットにしたり、プロモーション目的で個別の投稿を引用したりできるように、個々のデータ主体を識別することが目的である場合、これは調査ではなく、リサーチャーはそのように説明してはならない。

7.6　オンラインコミュニティ

オンラインコミュニティは、ブランドがさまざまなトピックにわたって顧客やその他の利害関係者のグループと継続的に対話することを可能にする手段として、ますます普及してきている。これにより、新製品のデザイン、新サービス、広告、及び長期にわたる満足度を高めることができる。

オンラインコミュニティの多くは調査に焦点を当てているが、コミュニティーは、ブランドの支持者、つまりブランドを仲間に宣伝するブランド大使を意図的に作成するためにも使用できる。通常、ブランド・アドボカシー（支援）・コミュニティーは、調査のためだけのコミュニティーよりもはるかに規模が大きく、パネルメンバーがそのブランドを宣伝するための行動を起こすことを目的としている。したがって、アドボカシー・パネルは調査のものではなく、リコミュニティーコミュニティのメンバーや彼らのクライアントに対して、アドボカシー・パネルをそのように提示してはならない。

7.7　カスタマー・エクスペリエンス調査

顧客体験調査は、代表的なサンプルデータを収集して分析し、ブランド/製品または体験に対する満足度と維持のダイナミクスを理解することを目指している。顧客体験調査の広範な出現は、調査活動と非調査活動の区別を維持する上で新たな課題をもたらした。これらのプロジェクトには、次の 2 つの目的があることがますます一般的になっている。

1. 満足度と維持のダイナミクスを理解するための代表的なサンプルデータの収集と分析。
2. サービスの回復、販売促進、または製品の提供に関するフォローアップのために、クライアントに個人データを提供すること。

第一の例には明確な調査目的があるが、第二の例にはない。潜在的な例外には、データ主体の健康または安全がリスクにさらされている場合、または法律で要求されているその他の状況にある場合が含まれる。詳細については次のセクション 8 の状況を参照。

8　情状酌量

極めてまれではあるが、調査以外の目的で個人データを共有することが必要かつ許容されるであろう場合がある。

8.1　個々のデータ主体の健康と安全の保護

まれな状況として、リサーチャーが、個々のデータ主体の安全及び福祉に対する脅威を認識し、第三者への通知が必要になると思われる場合がある。例えば、重篤な病気やけが、自殺の疑い、ガスや電気器具などの家庭用機器の誤作動などの報告が含まれる。このような場合、リサーチャーは最初に、第三者に知らせてもよいかを含む、データ主体の同意を取得しようとしなければならない。データ主体が意識を失っているか、または応答できない場合、リサーチャーは、調査を監督する責任者と協議の上、適切な第三者に通知することができる。データ主体が同意を拒否する場合、リサーチャーはその拒否の事実を文書化し、データ主体の希望に従わなければならない。

8.2　やむを得ぬ公共の利益

また、社会全体の健康と安全に貢献する可能性がある場合、データ主体の同意なしに政府機関とデータ主体の個人データを共有することが、まれにあり得る。最近の例としては、COVID-19 のパンデミックの広がりを示すために個人の位置情報を利用したり、ソーシャル・ディスタンス（社会的距離の確保）行動をモニタリングしたりすることが挙げられる。このような要請に従う前に、リサーチャーは以下を確認しなければならない。

- 脅威は正当であり、公共の利益にかなう。
- 要請機関は、このデータの使用目的が関連するデータ保護当局によって承認されたことの証拠を提供することができる。
- 要請機関は、データは特定の目的のためにのみ使用され、他の機関や民間部門の組織とは共有されないと規定している。
- 両当事者が合意した共有条件を明記した契約が締結されている。

8.3　医薬品調査における有害事象報告

医薬品調査では、しばしば、調査の過程において医薬品、セラピー、その他の医薬品に対する副作用を報告するために、データ主体に関する個人データを報告することが要求される（「有害事象報告」と呼ばれることもある）。これらの要求事項は通常、クライアントの組織に課せられた法的要求事項を反映しており、行政区域によって異なる傾向がある。リサーチャーは、適用されるすべての法律及び規制に準拠するように調査を設計しなければならない。多くの市場調査団体では、法的要求事項とプライバシー保護の指針を明記したガイドラインを作成しており、リサーチャーはこの分野で働く際にそれらを参照することが強く奨励されている。そのような団体には、EPHMRA, BHBIA, Intellus Worldwide などがある。

9　プライバシーとは無関係な有害性

最後に、プライバシーには関係しないが、それでもプロジェクトの企画段階で考慮されなければならない、データ主体の福祉に対するリスクがある。調査を実施する組織は、従業員にこれらのリスクを認識させ、調査がそうしたリスクから保護されるように設計されていることを確実にしなければならない。

9.1　人身事故のリスク

リサーチャーは、調査に参加した結果として、データ主体が負傷する可能性があることを認識し、それを防止しなければならない。例えば、電話調査を実施する場合、インタビュアーは、データ主体が調査に参加することで、身体的危害を受ける可能性のある活動や環境にさらされている（自動車の運転、機械の操作、公共の場での歩行など）潜在的な対象者にコンタクトする場合がある。第 2 の例は、データ主体がアレルゲン、タバコ、アルコールを含む製品など、身体的危害を引き起こす製品にさらされる可能性のある

製品テスト試験である。リサーチャーは、企画段階で、これらのリスク及び同様のリスクを考慮し、プロジェクト担当者に、このような状況が発生した場合の対処法を明確に指示しなければならない。

9.2 健康と福祉

調査のいくつかの形態では、データ主体との密接で個人的な対面を必要とする。このような設定の場合、リサーチャーは、CLT やグループインタビュー用施設を含む、個別面接会場個人面接で病気の伝染を防ぐために必要なすべての予防策を講じなければならない。潜在的なリスクは、ふつうの風邪から死に至る可能性のある病気まで多岐にわたり、感染症の重症度と感染の可能性に合わせて予防策の規模を調整することが望ましい。データ主体が感染している可能性のあるいかなる状況においても、リサーチャーは、面接の延期を含め、疾患の伝染を防止するために必要なあらゆる措置を講じなければならない。インタビュアー及びデータ主体と接触する可能性のある支援スタッフには、疾病があってはならない。施設は、必要に応じて消毒剤の使用を含め、頻繁に清掃しなければならない。調査が実施されている国では、地域の保健当局と業界団体が適切な予防措置に関する最良の情報源である。

9.3 感情的な苦痛

リサーチャーは、調査の内容が機微なものである場合、またはデータが収集される状況がデータ主体を動揺させたり混乱させる可能性がある場合には、特別な注意を払わなければならない。

9.4 法的な危険性

データ主体は、特定の場所に移動したり、特定のタスクを実行したりすることによって、データ収集者として行動するように求められることがある。例えば、禁止されている場所（政府庁舎、銀行、学校、空港の保安区域、私有地またはカメラ等の使用を禁止する掲示がなされている店舗等の区域）で写真を撮ったり、録音したりすることである。その他のリスクには、違法行為への参加または記録、違法薬物の使用、ウェブサイトのコンテンツの違法ダウンロードなどがある。いずれの場合も、リサーチャーはデータ主体がそのようなリスクについて完全に知らされていることを確実にし、それらの法的危険性にさらす可能性のある依頼を行わないようにしなければならない。

9.5 データ主体が所有する電子機器の損傷

調査では、コンピュータやモバイル機器への依存度が高まっており、ソフトウェアの誤動作、クラッシュ、他のアプリケーションとの干渉などにより、データ主体のコンピュータやモバイル機器のパフォーマンスが損なわれる可能性がある。リサーチャーは事前に、実装されているすべてのアプリケーションとシステムが中間フィールドの更新を含めて完全にテストされていること、及びデータ主体によって報告されたすべての誤動作に対応し、適切に対処するためのプロセスが導入されていることを確実にしなければならない。

9.6 財務的な損失

データ主体は、調査に参加することで、補償されない費用を負担してはならない。例としては、CLT 会場への往復の交通費や、モバイル調査におけるテキストメッセージやデータダウンロードのための追加の携帯電話料金などがある。

10 参考資料

ESOMAR「データ保護チェックリスト」

ESOMAR/GRBN「調査のための二次データを処理する際のガイドライン」（近日公開予定）

Future of Privacy Forum, Unfairness by Algorithm: Distilling the Harms of Automated Decisions-Making

ICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics

ICO, Conducting Privacy Impact Assessments: Code of Practice

OECD「プライバシー・フレームワーク」

11 プロジェクトチーム

Reg Baker, North American Regional Ambassador, ESOMAR

Debrah Harding, Managing Director and Finance Director, Market Research Society

Joke Ruwen-Stuursma, Professional Standards Executive, ESOMAR

ドラフトに有益なコメントを寄せてくれた多くの人々に感謝する。

Pepe Aldudo, ANEIMO

Jeremy Brodsky, Gutcheck

Gerrit Burghardt, Searchlight Pharma

Jackie Lorch, Dynata

Adam Phillips, Real Research

Ashlin Quirk, Dynata

John Tabone, CRIC

＜日本語版作成＞

一般社団法人　日本マーケティング・リサーチ協会