ESOMAR/GRBN GUIDELINE ON MOBILE RESEARCH (August 2017)

ESOMAR/GRBN モバイル調査 ガイドライン (2017 年 8 月)

目次

1 序文および適用範囲 3

1.1 適用範囲 3

2 用語の定義 5

3 対象者との関係性と責任 7

3.1 安全の確保 7

3.1.1 安全性 7

3.1.2 守秘義務と機微なデータ 7

3.1.3 費用 7

3.1.4 調査と非調査活動の区別 8

3.2 子どもおよび保護を要する人々 8

3.3 通知、誠実さ、同意、調査の自発性 8

3.3.1 データ取得の最小化と妥当な負荷 9

3.3.2 調査対象候補者への連絡方法 9

3.3.3 電話調査 9

3.3.4 インセンティブ 10

3.4 受動的データ収集 10

3.4.1 生体認証データ 11

3.4.2 写真および録画・録音 11

3.4.3 店内動線調査 11

3.5 ミステリーショッピング 12

3.6 二次データの使用 12

3.7 データ保護およびプライバシー 13
3.7.1 プライバシー保護通知 13
3.7.2 データの非特定化 14
3.7.3 デバイスのセキュリティ 14
3.7.4 静的 ID と動的 ID の使用 14
3.7.5 パラデータの使用および管理 15
3.7.6 国境を越えた転送 15
3.7.7 違反通知 15

3.8 クライアントとの個人データの共有 15
3.8.1 オブザーバー 15

4 クライアント：関係性と責任 **16**

4.1 二次契約 16

4.2 調査方法に関わる品質 16

4.3 透明性、誤りとエラーの訂正 17

5 一般市民：関係性と責任 **17**

5.1 公共の信頼性を維持 17

5.2 調査結果の公表 17

6 容認しがたい行為 **18**

1 INTRODUCTION AND SCOPE

1　序文および適用範囲

この ESOMAR / GRBN モバイルリサーチガイドラインは、リサーチャー（特に中小規模の調査機関の）がモバイル機器を使用して調査を行う際に、法的、倫理的および実践的に考慮すべき事項をサポートすることを目的としている。また、世界各国の現在の法的枠組みと規制環境の中で、市場・世論・社会調査の基本原則を適用する方法を説明する。そして、以前 ESOMAR と GRBN が 2012 年と 2014 年に個別に発表したガイドラインに取って代わるものとなる。これは現状の規制のカタログではなく、グローバルな原則の声明である。

本ガイドラインは、市場・世論・社会調査およびデータ分析に関する ICC / ESOMAR 国際綱領や、GRBN を構成する 45 カ国協会の個々の綱領を徹底的に読み込んで理解することを代用しようとするものではない。むしろこれは、どのような設定や形式であれ、個人を特定することが可能になるようなデータや情報を個々人が共有するリサーチの文脈において、これらの綱領の基本原則の解釈となることを意図している。

最後に、このガイドラインは、テクノロジーと政府による規制が進化し続けること、また、さまざまな国々で異なる法律や規制が存在する可能性があることを認識している。そのため、次の 3 つの重要な要求事項を満たすことを目指している：

1. 既存の法律の精神および字義と一致していること。
2. 業界の倫理的・専門的な原則を、我々の専門的な綱領に反映させること。
3. モバイル調査の現在および予期される将来の動向に対応するため、十分に幅広くかつ柔軟であること。

1.1 適用範囲

本ガイドラインでは、市場・世論・社会調査とデータ分析（以下、「調査」という）の目的のための、モバイル機器（携帯電話、タブレットなどのモバイルコンピューティングデバイス）による個人情報の収集と利用を取り扱う。また、例えばインターネットの一般的な使用、ソーシャルメディアネットワークへの投稿、さまざまな種類のメディアやオンラインショッピングの利用を含む、これらの機器によって可能となる多くの活動があることも認識している。これらのデータもまた、調査に使用される可能性がある。

これは、調査の目的で収集された一次データと、調査のために使用されたが、何らかの別の目的のために収集されたであろう二次データの両方を扱う際の、リサーチャーの責任について述べている。また、関連する業界の綱領、ガイドライン、調査が行われる行政区域において適用される法的要求事項に適合するために必要となる実践について記述している。

このガイドラインはまた、データ収集・実査準備・分析・保管および納品の際に、ある範囲の第三者機関が二次契約業者として関与する可能性があることを認識している。これらの第三者機関は、個人データの取扱いが含まれている場合にはリサーチャーと同じ義務を負う。

このガイドラインに記載されている実践の多くは（特に同意とプライバシー保護に関して）、オンライン調査に要求され

るものと同様である。リサーチャーは、多くの要求事項または推奨事項がより詳細に記載されている ESOMAR/GRBN オンラインリサーチガイドライン、オンラインサンプルクオリティについての ESOMAR/GRBN ガイドライン、ESOMAR のデータ保護に関するチェックリストを参照するように強く求められている。

この文書全体を通して、「must」という言葉は必須要件を特定するときに使用されている。我々は、リサーチャーが義務として従うべき原則や実践を記述する際に「must」と言う言葉を使用する。「should」という言葉は、履行することが推奨される際に使用されている。この用語の使用法は、リサーチャーが調査の設計に応じて、さまざまな方法で原則または実践を履行する選択を行う可能性があることを、認識することを意図している。

2 DEFINTIONS

2　用語の定義

本ガイドラインの目的に沿って、以下の各用語はそれぞれ特定の意味を持つように定義する：

Access panel アクセスパネル	将来、選ばれた場合にデータ収集に協力することを表明した潜在的な調査回答者のデータベースを指す。
Children 子ども	親または責任ある大人から、調査に参加する許諾を必ず取得しなければならない個人を指す。 子どもの年齢の定義は（国によって）大きく異なり、各国の法律および自主規制によって定められている。国による定義がない場合、子どもは 12 歳以下、13 歳から 17 歳は「若者」と定義される。
Client クライアント	市場調査プロジェクトを依頼、委託または申し込む、個人または組織を指す。
Consent 同意	ある個人（調査協力者）による、個人情報の収集と処理に対して自由意思に基づいて通知された合意を指す。
Data subject 調査対象者（データ主体）	その個人データが調査に使用される、あらゆる個人を指す。
Device ID デバイス ID	携帯電話などのモバイル機器に関連付けられた固有の番号を指す。デバイス ID は、ハードウェアのシリアル番号とは区別される。“デバイス ID”という用語は、調査上ではしばしば"デジタル指紋"という意味で使用される。
Deductive disclosure 演繹的情報開示	クロス分析や、小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）との組み合わせを通じて、対象者（個人）を識別するように推定することを指す。
Digital fingerprinting デジタル指紋	マシンやデバイスの指紋を生成するために使用できる、調査参加者のデバイス（コンピュータ、携帯電話、タブレットなど）に関する設定データ一式を指す。このようなシステムでは、「マシンの指紋」が個々のデバイス、または潜在的に個々のユーザアカウントに関連付けられたデバイスユーザの設定と特性を、ユニークに識別するものと仮定している。
Facial coding フェイシャルコーディング	広告や新商品のコンセプトなどの様々な刺激に対する応答から感情的な反応を推測するために、個人の顔の筋肉の動きをコード化する手法を指す。これは、デジタル画像内の特定の個人を識別することを目的とした、顔認識とは異なる。
Geolocation 地理的位置情報	コンピュータ、携帯電話、タブレットなどのデバイスの地理的な位置情報を指す。
GPS (global positioning system) 全地球測位システム	4 つ以上の GPS 衛星によって遮られることのない視線を確保し、あらゆる気象条件下で、地球上またはその近くのどこでも、位置情報と時間情報を提供してくれる衛星ナビゲーションシステムを指す。
Harm 危害、（単に）害	有形および物的損害（身体的傷害または財政的損失など）、無形または倫理的損害（風評や営業妨害など）、または特定の個人にターゲットを絞った迷惑なマーケティングメッセージを含む、個人生活への過度な干渉を指す。
IoT（Internet of Things) アイ・オー・ティー （モノのインターネット）	エレクトロニクス・ソフトウェア・センサー・駆動装置およびネットワーク接続機能が埋め込まれた、物理的なデバイス・車・建物およびその他のアイテムのネットワークを指し、それらの物体が（相互に）データを収集・交換することを可能にすること。
Mobile device モバイル機器	一般的にタッチ入力可能なディスプレイまたはミニチュアキーボードを持つ、小型・軽量で持ち運びできるコンピューティング機器（携帯電話、タブレットなど）を指す。
Mobile phone 携帯電話	無線回線を通じて広い地理的な範囲を移動しながら電話をかけたり受信したりできる機器を指す。

Mystery shopping ミステリーショッピング	顧客または将来の顧客として行動し、顧客サービスプロセスを観察・体験・測定するために訓練されたデータ収集者を使用することを指し、事前に決められた一連のタスクを実行し、サービス品質のベンチマークに対する行動を評価するか、または競合他社が提供する情報を収集すること。
Non-research activity 非調査活動	ある個人の態度、意見または行動を変更させる意図で、個人データを収集または分析したその個人に対して直接的に働きかけることを指す。
Paradata パラデータ	データ収集期間中の対象者の振る舞いを含む、データが収集されたプロセスに関するデータを指す。
Passive data collection 受動的データ収集	ある個人の行動や振る舞いを観察、測定または記録することによって、個人データを収集することを指す。
Personal data 個人データ (個人識別情報または PII とも呼ばれる)	ある個人を識別するために使用できる、自然人（以下、「対象者」という）に関するあらゆる情報を指す。例えば、直接的な識別子（氏名、特定の地理的位置情報、電話番号、画像、音声またはビデオ録画など）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・文化的または社会的な特性を参照することによって可能となる。デバイス ID とデジタル指紋も、一部の行政区域では個人データとみなされる。
Primary data 一次データ	調査の目的でリサーチャーが個人から、または個人について収集したデータを指す。
Privacy notice プライバシーに関する告知 （プライバシポリシーとも呼ばれる）	ある組織が、ある個人の個人情報を収集・使用・開示および管理する方法を説明する、組織のプライバシー保護に関する取り組みの要約を公表したものを指す。
Research 調査	すべての形態の市場・世論・社会調査およ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を指す。それは、商品やサービスの供給者、政府、非営利組織および一般市民によってインサイトを生み出し、意思決定を支援するために、社会学・行動科学およびデータサイエンスが適用された、統計的な分析手法および技術を使用する。
Researcher リサーチャー	調査を実行するか、またはコンサルタントとして行動するあらゆる個人または組織を指し、クライアントの組織内で働いている者や、使用される二次契約者を含む。
Secondary data 二次データ	別の目的のために収集され、その後調査で使用されることになったデータを指す。
Sensitive data 機微なデータ	識別可能な個人の人種や民族、健康や性生活、犯罪記録、政治信条、宗教的または哲学的信念に関するあらゆる情報を指す。行政区域が異なると、機微として定義される追加情報（所在地や財務情報など）があり得る。
SMS (Short Message Service) ショートメッセージサービス	固定回線または携帯電話機器間での短いテキストメッセージの交換を可能にする標準化された通信プロトコルを使用して、電話、ウェブまたはモバイル通信システムの構成要素としてのテキストメッセージングサービスを指す。
Social media data ソーシャルメディアデータ	ユーザーがソーシャルメディアに参加することで、または参加している間に、生成または共有する情報（コメントや写真など）を指す。
Wearables ウェアラブル（機器）	人間が介在せずにデータの収集や交換を可能にする、服の下、上または一部として着用される電子デバイス（センサー）を指す。
Web browsing history ウェブブラウジング履歴	あるユーザーが最近訪れたウェブページのリストと、ページタイトルや訪問時刻などの関連データを指し、ウェブブラウザのソフトウェアによって一定期間記録されるもの。

3 DATA SUBJECTS: RELATIONSHIPS AND RESPONSBILITIES

3　対象者との関係性と責任

3.1　安全の確保

リサーチャーは、データが調査に使用された結果として対象者が被害を受けることが決してないように、すべての妥当な予防策を講じなければならない。そのために、リサーチャーは調査の具体的な要求事項（現地の法的要件/制限、規制、風習等）や、調査活動が対象者に与え得る実際の影響について注意深く考慮しなければならない。いかなる場合でも、リサーチャーは対象者が容認でき、安全で公平なことのみを質問しなければならない。

リサーチャーはまた、対象者に提供されるソフトウェアについて十分にテストを行い、プライバシー保護に関する合意事項を遵守しなければならず、対象者の携帯機器への干渉やダメージを与えてはならない。より詳細には、セクション 6「許容できない方法」を参照のこと。

3.1.1　安全性

リサーチャーが調査対象候補者の携帯電話に電話を掛ける際、対象者が何かに集中しているか、固定電話にかける場合には通常起こりえない状況にいる可能性がある。これには、車の運転中、機械の操作中、公共スペースを歩行中などが含まれる。リサーチャーは、対象者が法的に安全で、電話に出ることができる状況にあるかどうかを確認することが望ましい。もしも確認が得られない場合には、別の機会にまた電話することの許可を得て、通話を終了することが望まれる。

モバイル調査手法の一部には、対象者に特定の場所へ移動してもらうか、特定の役割を演じることでデータ収集者として行動することを依頼するものがある。そのような場合、リサーチャーは対象者を危険にさらしたり、法律を破ったり、他者のプライバシーを侵害したりすることがないように注意をしなければならない。例えば、運転中にモバイル機器で文字を書きこむことや、写真撮影や録音が禁止されている場所（例えば、政府庁舎、銀行、学校、空港の保安区域、プライベートな空間や区域、カメラの使用禁止と掲示されている店舗等）での撮影について警告することなどが含まれる。

3.1.2　守秘義務と機微なデータ

リサーチャーは、調査対象候補者が何らかの活動に集中しているか、他人に通話の内容を聞かれるかもしれない状況で連絡を取ることがある。この場合、リサーチャーは、対象者の話が他人に聞かれ、個人情報や行動が不注意によって開示され、またはその状況の結果として回答が変化する可能性を踏まえて、調査内容の性質を考慮しなければならない。適切な場合には、機密性が損なわれないように、通話を別の時間または場所に再設定することが望ましい。

リサーチャーはまた、対象者に危害や苦痛を与える恐れがある機微な性質の調査トピックスのためにアプローチする場合には、注意して取り組まなくてはならない。一部の国々では、機微なデータを収集するためには関連する当局からの許可が必要となる場合がある。

3.1.3　費用

他の多くの調査手法とは異なり、対象者がモバイル機器を利用した調査に参加する際にはその結果として、データのダウンロード、オンラインアクセス、テキストメッセージの送付、契約しているデータ量の超過、ローミング料金、ボイスメールの検索、通常の電話の使用等で発生した費用など、対象者側にコストが発生する可能性がある。リサーチャーは、対象者

の承認なしに費用を払わなくて済むように調査を設計することが望ましい。もしそれが不可能ならば、リサーチャーは補償を用意しなければならない。それらの補償は、現金、モバイルマネー、無料通話時間や他の形式の価値であっても良い。

3.1.4 調査と非調査活動の区別

リサーチャーは、調査目的が非調査活動とはっきりと区別されるようにしなければならない。さらに、調査目的のために収集した個人情報が、対象者の事前の同意なしに、他の目的のために使用されることを許可してはならない。この要求事項は、リサーチャーが非調査活動に関与することを妨げるものではなく、調査以外の目的で個人データが収集され、その目的が対象者に明示的に伝えられ、それを含む調査活動と合理的に区別され、非調査目的のためのデータ使用の同意がデータ収集の事前に得られている場合に適用される。

3.2 子どもおよび保護を要する人々

子どもや保護を要する人々に調査を行うときは、リサーチャーは、親の許諾が要求されるのか、または文化的な繊細さが特定の取扱いを要求するのかを判断するために、国内法およびそのデータが収集される行政区域の自主規制規範を調べなければならない。潜在的な調査対象者に電話で連絡する時には、対象者が子どもであることが明らかな場合、その子どもに調査への参加を依頼するための親または責任ある大人の許可を得ることなしに、リサーチャーはインタビューを続行してはならない。また、その個人に判断能力がない場合、一部の行政区域では、リサーチャーが別の方法を使って調査に参加する機会を提供することを求められる場合がある。

リサーチャーは、子どもの写真撮影や録音時に特に注意を払う必要がある。許可を得ることができない場合、子どもの画像はモザイクをかけるか削除されなければならない。

ほとんどのモバイルオペレーティングシステムには、（有効になっていれば）アプリをインストールする前に、事前に親の同意を要請することを可能にする機能が備わっている。リサーチャーは、調査に使用するアプリを開発または開発委託する時に、これらの設定を使用することが望ましい。

3.3 通知、誠実さ、同意、調査の自発性

リサーチャーは、以下の内容について明解にし、あらゆる形式の個人データを収集する前に対象者から同意を得なければならない：

- （調査機関の）身元；
- 収集を予定している情報；
- 情報を収集する全般的な目的；
- データ収集の方法；
- 対象者が調査の参加に要する予想時間；
- データの保護方法；そして、
- 誰とデータを共有し、どのような形式で共有するか。

この情報は、明確、簡潔かつ目立つようにすることが望ましい。「3.7.1 プライバシー保護通知」も参照のこと。さらに、上記の情報のいずれかが変更された場合、対象者にあらためて同意をとる必要がある。対象者に誤解を与えたり、嘘をついたり、騙したり、強要するようなことがあってはならない。調査への参加は常に自発的なものであり、対象者はいつでも

参加を取りやめ、個人データを削除させることが許されなければならない。

最後に、リサーチャーは、関連するすべての法律、規則、現地の専門的な行動規範を遵守しなければならない。

3.3.1 データ取得の最小化と妥当な負荷

リサーチャーは、個人データの収集または処理を、リサーチに関連する項目に制限しなければならない。また、対象者に与えられたタスク（例えば、アンケート、日記やディスカッションフォーラム）が、モバイル機器に適した形式で、かつ適切な長さで提示されるようにすることが望ましい。

モバイル機器によっては画面のサイズがより小さいため、指示、質問または書式が明確で読みやすく、簡潔であるようにするための特別な注意が払われなければならない。これには、デバイス間でフォーマットを最適化するとともに、アンケートが長すぎたり複雑すぎたりする場合に、特定のデバイスを除外することが含まれる。これらは、「モバイルファースト」、「デバイスに依存しない」、「画面サイズに合わせたデザイン」などの用語と一緒によく言及される。

リサーチは進化を続けており、最近の実証データによれば、モバイル調査の対象者は、電話調査や対面によるフォーカスグループなどの他の手法よりも、リサーチャーとのやりとりをより短くしてほしいと希望していることを示している。

調査では固定電話によるよりもオンラインで対象者をつなぎとめることがより困難であることが示されており、同様の注意が、携帯電話を介してインタビュアーが管理するアンケートを設計する際にも適用される。

3.3.2 調査対象候補者への連絡方法

モバイル技術とコミュニケーション手法は急速に成長し、法的な枠組みの整備もまだ進化中である。そのような規制は、電話、電子メール、テキストメッセージのいずれか、またはモバイル機器を介して調査対象候補者に連絡を取る際に、リサーチャーに間接的な影響を及ぼし、法的責任を生じさせると解釈される可能性がある。例えば一部の国々では、明示的な同意が得られない限り、テキストメッセージを送信するために自動化されたシステムを使用することが禁止されている。

リサーチャーは、調査対象候補者の電子メールアドレスや携帯電話番号を入手する際、いかなるごまかしも使用してはならない。これには、公的な Web サイトの使用や、個人が知覚できないテクノロジーや技法の使用、または調査ではない何らかの活動を装って個人情報を集めることなどが含まれる。最後に、携帯電話の番号に電話をかける際には、発信者の番号を表示する設定にすることが望ましい（意図的に非通知設定にしてはならない）。

リサーチャーは、調査への参加を求める電子メールやテキストメッセージ[1]を受け取ることを期待している人だけが含まれていることを、サンプル提供者（サンプル供給業者かクライアントかに関わらず）に確認しなければならない。

ESOMAR / GRBN Online Research Guideline の Section 3.5 に、許容される実務の詳細な説明がある。

3.3.3 電話調査

携帯電話に電話をかける際、リサーチャーは、調査ではない商業目的での迷惑な電話が法的に規制されていることを認識していなければならず、固定電話と同様に携帯電話についても、既存の調査専用「連絡不可リスト」があれば、調べて適用することが不可欠である。

また一部の国々では、あらゆるタイプの迷惑電話を許容する通話時間帯を指定する法律や基準があり、携帯電話によるアンケートについても同様に対応することが望ましい。リサーチャーは、連絡しようとしている相手が異なるタイムゾーンにいる可能性があることを予測し、都合のよい時間帯、場所や状況を確認しておくべきである。そのような要求事項がない

[1] モバイルのアプリ通知など、その他のメッセージング技術についてもテキストメッセージと同様の性格と機能を持つ。

場合には、リサーチャーは固定電話向け調査と同じ通話時間帯を守ることが望ましい。B to B 領域の調査では、許容される時間帯は暗黙のうちに、そのビジネスに関係する通常の営業時間内となる。携帯電話へのテキストメッセージの送信についても調査参加者がメッセージを「正常な時間」以外に受信することを避けるために、同様の注意を払うことが望まれる。

一部の国々では、予測ダイヤル発信システムを含む、オートコールやその他の自動ダイヤル発信装置の使用を制限している。その他の国では、そのような装置の使用は、事前に対象者が（例えば、アクセスパネルのメンバーとして）自動ダイヤル発信装置による電話を受けるという明示的な同意を与えている場合にのみ、許可される。ただし、自動ダイヤル発信が許可され、使用される場合であっても、すぐに対応できるインタビュアーがいない場合の、無応答電話や無言電話については許容されない。

3.3.4 インセンティブ

モバイル調査への参加を促すインセンティブが提供されている場合、リサーチャーは対象者に次のことについて明確な情報を提供しなければならない：

- インセンティブは何か；
- 誰がそれを管理するのか；
- いつ対象者がそれを受け取るのか；そして、
- 何らかの条件がついているかどうか（例えば、ある特定のタスクの完了、受動的調査データへのアクセス、品質管理チェックのクリア、コミュニティのアクティブなメンバーとして要求される最低限の時間を満たした場合など）。

リサーチャーは、クライアントから提供されるインセンティブ（クライアントの商品や、クライアントのロゴが付いている商品）の使用については、一部の行政区域ではマーケティング（販促）活動と見なされる場合があるため、十分に考慮することが望ましい。

懸賞やくじ引きなどの使用を含む、インセンティブに関する詳細な説明については、ESOMAR / GRBN Online Research Guideline の Section 3.6 を参照のこと。

3.4 受動的データ収集

モバイルのアプリは、対象者と直接のやり取りをすることなく、幅広い個人データを収集することができる。例としては、ウェブの閲覧・使用履歴、アプリ使用の統計値、ロイヤリティカードのデータ、地理的位置情報、ソーシャルメディアのデータ、ウェアラブル機器や IoT から取得したデータ、モバイル機器[2]から取得または生成されたデータ等があげられる。

加えて、オンライントラッキングのような特定の技術は、受動的データ収集の一形態として調査に有効なアプリケーションをもたらした。典型的には以下のようなものが含まれる：

- オンラインサンプルの精度の向上；
- 不正の防止；または、
- オンラインの視聴率測定、コンテンツ測定および広告テストを含むが、これらに限定されない調査用のアプリ。

[2] ある対象者が使用している機器の種類を受動的に検出することは可能だが、アプリや調査のパフォーマンスを最適化することが目的である限りにおいては、これは個人データとはみなされない。

このような、および同様の状況下で、リサーチャーは 3.3 項に記載された同意を取得するために、すべての合理的な努力を払わなければならない。同意を得ることができない（あるウェブサイトのトラフィックを測定するような）場合、リサーチャーはデータを収集するために法的に許容される根拠を持たなければならず、運用上可能な限り早く、個人を識別し得る特性を削除または不明瞭化しなければならない（データの匿名化については 3.7.2 を参照）。

3.4.1 生体認証データ

受動的データや行動データの収集はまた、対象者との直接的なやり取り含むことがある。例えばフェイシャルコーディングでは、対象者がアンケートまたは同様のタスクを完了する時に、彼または彼女の顔のデータを記録する。アイトラッキングでも、バーチャルリアリティのヘッドセットや他のウェアラブル機器が同様に使用される。これらのすべてにおいて個人データの収集を伴い、場合によっては、適用される現地の法律および業界の行動規範を遵守することをチェックするためのプロセスが要求されるような、一部の行政区域内で機微な情報に分類され得るデータが含まれることがある。

3.4.2 写真および録画・録音

写真・ビデオ・音声録音も個人データとみなされるため、収集・利用・保管の際にはそのように扱われなければならない。それらは、対象者が使用される特定の目的について知らされ、事前に同意を与えた場合にのみ、クライアントに共有することができる。（モザイク処理や音声変換技術等によって）潜在的な個人識別情報が削除されている場合、それはもはや個人データとはみなされず、「個人を特定しようとしない」旨の合意を得たクライアントに対して共有することができる。

リサーチャーは、調査対象者（またはデータ収集者として行動する可能性がある人）に対して、個人や公共の場所の監視に従事させるような指示をしてはならない。対象者には、特定の限られたタスク（例えば、同意を得た友人とのやり取り、または対象物やディスプレイの撮影など）が与えられるべきであり、その場にいあわせた同意の取れていない人々の個人データが取りこまれてしまうような、特定エリアの監視は含まれない。ある場所で観察調査の記録が行われる場合、そのエリアで観察が行われていることを明確でわかりやすく記した標識を、調査を実施しているリサーチャーまたは調査機関の詳細な連絡先と合わせて設置することが望ましく、個人の画像はモザイク処理するか可能な限りすみやかに削除しなければならない。カメラは、観察対象のエリアのみを撮影するように配置されることが望まれる。

3.4.3 店内動線調査

対象者（買い物客）の店内動線調査も受動的データ収集の一形態であり、買い物行動としての個人の店内での移動の様子が記録される。具体的な収集方法は、大きく以下の 2 つのカテゴリーに分けられる。

ひとつ目のカテゴリーは、対象者に依頼をして、店内での移動状況を追跡し、記録するためのハードウエア（ビーコンなど）と同期する機器を持ち運ぶか、アプリをダウンロードしてもらうことである。このアプローチでは、規格要求事項の通知と同意が適用される。（「3.3 通知、誠実さ、同意、調査の自発性」を参照）。

ふたつ目のカテゴリーは、対象者には彼らが店内にいる間、観察され、行動データが収集されていることを明示的には伝えない場合である。このようなケースでは、リサーチャーは以下のことを確実にしなければならない：

- 店内での撮影とデータ収集が、現地の法律で許されていること；
- 店内での行動が記録されている旨をわかりやすく記した標識が設置されていること；そして、
- 個人を識別し得る要素は、運用上可能な限りすみやかに削除または不明瞭化されること。

3.5 ミステリーショッピング

ミステリーショッピングの調査対象者（通常は従業員）は、一般的に観察されていることには気づいていない。リサーチャーは、個人のプライバシーが尊重されることを確実にし、ミステリーショッピングの対象となった調査対象者が、その結果としてどのような形であれ、不利益や被害を被ったりすることが無いように注意を払わなければならない。彼らの個人データは保護されなければならず、（一般的に雇用契約の一部として）対象者からの許諾が得られていない限り、写真や録音をクライアントに共有することはできない。

ミステリーショッピングは、買い物行動の特徴と購入意思決定への影響に対する対象者の反応を把握するために設計された、瞬時のデータ収集とは異なる。それは、対象者の同意のもとで実施されるエスノグラフィーの一形態である。

3.6 二次データの使用

今日のようなデジタル時代では、日々の商取引や事業活動に付随する結果として、データ量が増え続けている。例えば、モバイルサービス業者はしばしば、顧客や、顧客のモバイル端末の使用に関する広範な情報を収集している。携帯電話には、誰が誰に電話したかのみならず、誰がどこにいたか（地理的位置情報）や、どのウェブサイトを訪問していたか、どの基地局に接続していたかなどのデータが記録されている。また、個々のアプリの利用履歴やソーシャルメディアへの投稿といったデータまで記録されている。

これらの、および他の同様のデータは、リサーチャーに、人々の行動の理解を拡大する新たな機会を与えてくれる（理解するのに大いに役立つ）。リサーチャーは、従来型の手法を使用してこれらのタイプのデータの一部を収集する調査プロジェクトを設計することがあるが、その多くは再利用可能な二次データとして既に存在している可能性がある。

これらのデータを使用する前に、リサーチャーはまず以下のことを確認しなければならない：

- その使用計画は、データ収集の前に対象者が合意した条件内で合法的に許可されるものであり、当初のデータ収集時に提示されたプライバシー保護通知から特に外れるものではないこと；
- そのデータは、対象者を欺いたり、曖昧な方法を通じてではなく、合理的に識別可能で、対象者が予想可能な、法律で課された制限に違反して収集されたものではないこと；
- 対象者が、そのデータが例えば調査のような他の目的に使用されるかもしれないという、合理的な予想を感じていたこと；
- 他の目的のためにデータを使用しない（でほしい）という、対象者からのあらゆる要請が尊重されること；そして、
- そのデータを提供する組織が、データを共有する法的権利を持っていること。

リサーチャーはまた、そのデータの更なる処理が演繹的な情報の開示につながって、対象者に危害を及ぼすリスクをもたらす可能性があるかどうかを検討しなければならない。そのようなリスクが存在する場合、リサーチャーはそうした危害のリスクを軽減させるための、安全対策を講じなければならない。これには、個々の対象者の身元が事前の同意無しに開示または公開されないようにすることが含まれるが、それに限らず、調査のために使用されているデータが、その直接的な結果として非調査活動に利用されないということも含まれる。

3.7 データ保護およびプライバシー

リサーチャーは、個人データに関する普遍的なデータ保護原則[3]を遵守しなければならない。これらの原則では、収集または使用されるあらゆる個人データは、次の通りでなければならない：

- 特定の目的のために収集され、その目的と両立しない方法では使用されない；
- それが収集され、またはさらに処理される目的との関係において、適切で、関連性があり、過度ではないこと；
- 対象者を欺いたり、曖昧な方法を通じてではなく、合理的に識別可能で、対象者が予想可能な、法律で課された制限に違反して収集されたものではないこと；
- 対象者に危害を及ぼす結果になりそうな方法では使用されないこと（そのような危害を防ぐための措置を取ることを含む）；
- 損失、不正アクセス、破壊、（不正な）使用、改ざん、開示などのリスクから保護されていること；そして、
- 情報が収集され、さらに処理される目的のために、必要な期間を超えて保存されないこと。

必要とされるデータセキュリティ基準および方針を策定するために使用する、リサーチャーのための様々な基準と枠組みが存在する。詳細については、ISO 27001: 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム（ISO 27001:Information technology – Security techniques – Information security management systems – Requirements）、または ESOMAR データ保護チェックリスト（ESOMAR Data Protection Checklist）を参照のこと。

リサーチャーは、個人データをクラウド環境に保管することの意思決定については慎重に検討しなければならない。クラウドストレージサービス事業者のセキュリティ管理および標準利用規約を評価し、事業者の管理が十分でない場合には補完的な管理を実施する準備を整えなければならい。詳細は、ESOMAR/GRBN オンラインリサーチガイドライン（ESOMAR/GRBN Online Research Guideline）の 7.7 項、ESOMAR データ保護チェックリスト（ESOMAR Data Protection Checklist）、クラウドコンピューティングサービスの実用ガイド（The Practical Guide to Cloud Computing）を参照のこと。

3.7.1 プライバシー保護通知

一般的にプライバシー保護法と関連規制は、調査機関が調査対象者に対してプライバシー保護通知を提供することを要求している。モバイル機器の画面サイズの制約のため、リサーチャーはプライバシー保護通知の階層化（レイヤー方式）を検討することが望ましい。これは通常、組織の身元や個人データが使用される方法などの基本的な情報を含む短い通知文と、より長い通知文を合わせて構成されている。

調査対象者は、彼らの同意を表明するために、短い通知だけに基づく十分な情報を得られなければならず、氏名・年齢・意見などといった明白な種類の収集データよりも、むしろ音声や画像、地理的位置情報、データの二次利用、データの共有、データの保持期間などの、明確ではないデータ活用や使用方法について強調することが望ましい。

短い通知文には、より詳細な説明が記載された次のページへ飛ぶリンクを含むことが望ましく、デスクトップのパソコンから閲覧されるように設計された画面をスクロールせずに、すべての情報を容易に見られるようにすることが望ましい。

プライバシー保護通知には、データ収集に適用される法律について記載しなければならない。複数の国でデータを収集する場合、リサーチャーは調査が実施される国々の法律を遵守しなければならない。調査対象者の居住国を知ることが可能である場合、リサーチャーは、各行政区域間で法規制に大きな違いがあり得ることを念頭に置きつつ、その国の法的

[3] 例として、「OECD プライバシー原則」を参照のこと。

要求事項に従わなければならない。

3.7.2 データの非特定化

リサーチャーは、個人データの流出を防ぐために、クライアントや他のデータ使用者と共有するあらゆるデータが、十分に非特定化されることを確実にしなければならない。非特定化技法には様々なものがあり、それぞれが個人データの流出対策または追加的なセキュリティ対策のために様々なレベルの防御策を提供している。それらは、直接的な識別子の削除、間接的な識別子（演繹的な情報開示を可能にし得る項目）の削除、およびデータ変換（例えばハッシュ化、暗号化、集合化など）を含む、広範なデータ加工をカバーする。

仮名化は、データ処理期間中や、マッチングや妥当性確認などの目的で元データを復元する必要があるかも知れない場合に、非特定化のために特によく使用される手法である。それは一般的に、調査データから個人データを分離し、各ファイルに異なる ID を与え、必要に応じて元データを復元するために使用できる２つの ID にリンクする第三のファイルを生成する。リンクファイルへのアクセス権は、わずかな人数にのみ制限される。リサーチャーはデータ取得後、できる限り速やかに仮名化することが強く推奨されている。

匿名化には、個人データが削除または変更され、演繹的な情報特定手法によっても個々の対象者の再識別がもはや不可能になるような、様々な技法が含まれる。例として、個人情報に繋がるデータ項目の削除や暗号化、写真やビデオの顔を隠すための画像のぼかし加工、ノイズの挿入、集計された統計値としての結果のみを報告すること、などが挙げられる。

3.7.3 デバイスのセキュリティ

調査対象者のモバイル機器内に保存されている個人データは、その機器が盗まれたり他の人に使用された場合、他人が利用できる可能性がある。例として、その機器にインストールされている調査用または非調査用のデータ収集アプリに保存されているデータ、エスノグラフィーやその他の調査活動の間に撮影された写真、個人データを含む調査データを送受信するために使用されてきた SMS、電子メールまたはその他のメッセージサービスなどが挙げられる。

ウェアラブルやその他の IoT 機器からデータを収集する場合、リサーチャーはデバイス間でデータが転送される前に、すべてのデータが暗号化されることを確実にしなければならない。

調査対象者は、これらのリスクを認識させられなければならず、またリサーチャーは個人データを保護するための施策を実施しなければならない。例としては、データの暗号化（格納中のデータ、伝送中のデータの暗号化を含む）、パスワードによるデバイスの保護、調査対象者に対して調査終了時にすべての個人情報を削除する方法を指示し、その他の安全対策やコントロール方法を提供することなどが挙げられる。

3.7.4 静的 ID と動的 ID の使用

調査のクライアントおよびサンプル供給者は、時折、アドホック調査と経年的調査の両方において、調査対象者の管理や割当を支援するために、対象者の固定的な識別子（静的 ID）を使用している。この技法は、各調査対象者に関する情報の統合に役立ち、ある経年的調査の中で対象者を特定すること、または調査除外期間を守ることを確実にするための有用なアプローチとなっている。

一部のサンプル供給者は、個々の対象者の身元情報を保護するために動的 ID（都度変化する ID)を好む。

リサーチャーは、それぞれのタイプの ID の使用を慎重に検討し、対象者のプライバシー保護と具体的な調査の中で生

じる品質に関する懸念事項とをバランスさせることが望ましい。

3.7.5 パラデータの使用および管理

リサーチャーは、後続の調査および分析において、データ収集プロセスに関するそれらのデータの収集、使用および転送を指導、制限および保護するための、サンプル供給者とクライアントとの間で相互に交わされた法的合意がある場合でなければ、パラデータを使用してはならない。一部の行政区域では、パラデータは機微なデータとみなされている。

3.7.6 国境を越えた転送

個人データが収集した国から別の国へ転送される前に、リサーチャーはそのデータ転送が合法であり、それらのデータのプライバシーとセキュリティを確保するためにすべての合理的な手順が取られていることを確実にしなければならない。これは、データ収集サーバが調査対象者とは異なる国にある場合に適用される。また、クラウド技術が異なる国でのデータ保管に使用される場合にも適用される。

リサーチャーは、データ転送を容易にするために、転送の代替手段が存在するかも知れないことに留意しつつ、このような国境を越える転送を規定する情報ソースと、転送先の国で適用されるプライバシー保護法や規制について理解しなければならない。

3.7.7 違反通知

リサーチャーは、データが収集されている国の違反通知や手順の要求事項に関して、関連するすべての法律および規制を遵守しなければならない。リサーチャーは、セキュリティまたはデータの違反が生じた場合には、最初に関係当局に報告しなければならず、続けて（不合理な遅延なく）クライアント、調査対象者、二次契約者を含む、影響を受けるすべての当事者に対して報告をしなければならない。その通知には、違反が生じたデータの種類の説明と、その違反の結果によって生じる可能性がある損害から調査対象者を守るために、彼らが取るべきあらゆる手順が含まれることが望ましい。

3.8 クライアントとの個人データの共有

適用されるプライバシー保護法または規則がより高い要求事項を規定していない限り、リサーチャーが調査目的以外にも使用し得る個人データを収集する予定がある場合には、調査対象者に対してデータ収集前にそのことを明確にし、非調査目的に対する同意を得なければならない。

リサーチャーは、調査対象者個人を識別できる情報をクライアントに共有してはならない。共有する場合には必ず、対象者がそのことに同意し、その情報がどのように使用されるか、具体的な目的についての合意を得なければならない。

また、匿名化されたデータセットをクライアントに提供する場合であっても、リサーチャーはクライアントから、それを使用して対象者個人を再識別化する意図はないという書面による保証を取得しなければならない。ただし、これは上記の条件を満たした場合には適用されない。

3.8.1 オブザーバー

一部の調査方法では、ビデオやクライアントのダッシュボードを通じ、リアルタイムで、または少し遅れて、データ収集の状

況を観察することにより、個人データにアクセスできる人々が参加することがある。例として、リサーチャーではない顧客チームのメンバーや、広告代理店などクライアントの二次契約者が挙げられる。そのような場合には、リサーチャーは以下の同意や合意を取得しなければならない：

- データの収集中または収集後に、調査対象者がそのような人々（関係者を含む）に観察されることについての同意；そして、
- すべてのクライアントおよび他の観察者からの、調査対象者の個人データを開示しないこと、または同意なしに調査目的以外の方法では使用しないことの正式な合意。

4 CLIENTS: RELATIONSHIPS AND RESPONSBILITIES

4　クライアント：関係性と責任

4.1　二次契約

リサーチャーは、業務の一部がリサーチャーの所属組織外に委託される場合には、業務を開始する前に、クライアントに知らせることが望ましい。要請を受けた場合、クライアントにはそのような二次契約者の身元を伝えなければならない。

サンプルの調達に使用される二次契約者の身元が、合法的に独占的な情報であるとみなされる場合、そのサンプル供給者は以下の情報を提供しなければならない：

- 使用されるサンプル情報源のタイプの説明；そして、
- パネルソースおよび非パネルソースから予想される、サンプルの使用割合の見積り。

リサーチャーはまた、二次契約者と共有するあらゆる個人データが、二次契約された業務を実行するために必要なものだけに限定されるようにする必要がある。二次契約者はデータを保護するために必要なデータセキュリティ手順を講じていること。そして、データ保護に対する二次契約者の責任が明確に文書化され、合意されていること。

4.2　調査方法に関わる品質

モバイル調査のユーザーが、調査結果データが目的に合致しているという確信を持っている場合、リサーチャーは、調査方法の限界によって結論がデータによって支持されないかもしれないことを含め、結果の妥当性を評価できるように、調査がどのように実施されたかについて、クライアントに適切な情報を提供しなければならない。この情報には、以下の点が含まれることが望ましい：

- サンプルの大きさ、情報源（ソース）、管理状況；
- サンプル設計と抽出方法；

- データ収集の方法；
- 適用された可能性がある、あらゆるデータクリーニング、ウエイト付けまたはフィールド終了後の調整；そして、
- モバイルの普及率が 100% 未満の場合に、調査結果が目標母集団を代表することを確実にするために取られた手順。

これらの各分野における具体的な要求事項は、『ESOMAR/GRBN Guideline on Online Sample Quality』と、『ESOMAR/GRBN Online Research Guideline』 の第 6 章に記載されている。

4.3 透明性、誤りとエラーの訂正

すべての調査プロジェクトは、正確、透明かつ客観的に報告され、文書化されなければならない。納品後に誤り（エラー）が発見された場合には、クライアントに直ちに通知し、速やかに訂正を行わなければならない。

5 THE GENELAE PUBLIC: RELATIONSHIPS AND RESPONSBILITIES

5 一般市民：関係性と責任

5.1 公共の信頼性を維持

リサーチャーは、正直かつ誠実で客観的であり、適切な科学的調査の原則、方法、および技術に従って調査が行われることを確実にしなければならない。リサーチャーは、常に倫理的に行動しなければならず、市場・世論・社会調査及びデータ分析の評判を損なう恐れのある行為を決して行ってはならない。ICC/ESOMAR と GRRBN Code の基本原則に常に注意を払い、公共の信頼を損なう可能性のある活動や行為を避けなければならない。

5.2 調査結果の公表

クライアントが調査結果を公表しようとする場合のリサーチャーの責任については、ESOMAR/GRBN Online Research Guideline の 5.2 項を参照のこと。

6 UNACCEPTABLE PRACTICES

6　容認しがたい行為

リサーチャーは、以下のようなソフトウェアやアプリケーションを使用、またはインストールをしてはならない：

- 十分にテストがなされていないもの；
- 対象者の同意なしに、調査の実施に必要な範囲を超えて、モバイル機器の設定を変更するもの；
- OSと競合する原因となるか、インストールされている他のソフトウェアが不安定化または予期せぬ動作をする原因となるもの；
- 勝手にダウンロードされるか、またはアンインストールが困難な、他のソフトウェア内に隠されているもの；
- 正当な広告調査のために必要なものを除き、広告コンテンツを配信するもの；
- 対象者への通知、およびオプトアウトの機会を提供することなしに、収集したデータを変更するもの；
- 具体的な同意を得ずに、デバイスのバッテリーに異常に高い負荷をかけるもの；
- 対象者の同意なく発生し、リサーチャーによって補償されない費用を対象者に負担させるもの；
- 対象者の同意なしに、地理的位置情報追跡ソフトウェアを使用するもの；
- 暗号化されていない個人データを送信するもの；
- 対象者への通知や同意の取得なしに、身元の識別および追跡技術の性質を変更するもの；
- アップグレードに関連するプライバシー保護慣行の変更を、対象者に通知できなくするもの；
- 対象者の同意なしに、非調査目的でアプリ提供者によって使用される可能性のある個人データを収集するもの；そして、
- 調査目的の一部であり、かつ同意が得られている情報を除き、モバイル機器や携帯電話から情報を抽出するもの。

調査が完了し次第、不要になったあらゆるアプリが無効化されなければならない。調査対象者には、彼らのデバイスからアプリを安全に削除する方法について通知し、指示を与えなければならない。

モバイル調査ガイドライン：訳語に関する注記

原則として、以下の訳語を採用している（例外もあり）。

No.	用　語	本ガイドラインでの主な訳語	備考／一般的な訳語
1	research	調査	調査（一般）、研究
2	researcher	リサーチャー	
3	research provider/company	調査機関	調査会社
4	sample provider/supplier	サンプル提供者/供給者	
5	survey	アンケート	（実査を伴う）調査
6	must	～しなければならない	（ISO 用語では shall になる）
7	should	～することが望ましい	
8	may	～する可能性がある、し得る	～かも知れない
9	can	～できる、し得る	
10	and/or	（単に）または	および/または
11	requirements	要求事項	要件
12	require	要求する	
13	request	要請する	
14	ensure	～することを確実にする	～を確保する、保証する
15	sensitive data	機微なデータ	機密データ
16	local	現地の	地方の
17	jurisdiction	行政区域	管轄区域
18	data subject	調査対象者（or 単に対象者）	データ主体
19	potential data subject	調査対象候補者	潜在的なデータ主体
20	participant	調査参加者（or 単に参加者）	参加者、出席者
21	mobile devices	モバイル機器	
22	mobile phone (or mobile)	携帯電話	
23	unsolicited calls	迷惑電話	求められていない電話
24	in the context of	～の文脈（の中）で	
25	to comply with	～を遵守する、～に準拠する	
26	vulnerable individuals	保護を要する人々	脆弱な人々
27	subcontractor	二次契約者	下請業者、外注先
28	geolocation	地理的位置情報	位置情報
29	permission	許諾、許可	
30	client	クライアント	（調査機関からみた顧客）

No.	用　語	本ガイドラインでの主な訳語	備考／一般的な訳語
31	customer	顧客	（クライアントからみた顧客）
32	consider	考慮する、検討する	
33	privacy notice	プライバシー保護通知	
34	de-identification	非特定化	（仮名化や匿名化を含む）
35	pseudonymisation	仮名化	（管理者による復元が可能）
36	anonymisation	匿名化	（もはや復元は不可能）
37	disclosure	開示、流出、漏洩	
38	validation	妥当性確認（特定ISO用語）	検証
39	general public	一般市民、一般公衆	
40	practice	実践、行為、慣行	（練習なども）

その他注意事項：

1　原則として、ISO ルールにのっとって整理・監訳している。
世界的な共通認識が形成できるように、できるだけ原文に忠実な翻訳を心がけている。
（バックトランスレーションした時に、原文にできる限り近い表現になっているように）
"must"（～しなければならない)、"should"（～することが望ましい）は、この表現が必須
（注： ISO の本規格では、「～しなければならない」は "shall" で統一される）
「である」調で統一している。
2　翻訳文の意味が通じにくいところは、往々にして原文もあいまいな表現であることが多いので
このような場合には、わかりやすい意訳を試みている。
3　最終的には、委員会としての判断でより理解しやすい表現に変更しているところがある。

JMRA　インターネット調査品質委員会　構成表

(翻訳)

	氏名	所属
管掌理事	五十嵐　幹	(株)クロス・マーケティング
担当理事	佐々木　徹	(株)マクロミル
委員長	村上　智章	(株)マクロミル
委員	岸田　典子	(株)クロス・マーケティング
委員	高山　佳子	(株)インテージ
委員	大野　聖二	GMO リサーチ(株)
委員	工藤　公久	GMO リサーチ(株)
委員	中村　真一	(株)マクロミル
委員	出口　敬子	楽天リサーチ(株)
委員	松島　貴史	楽天リサーチ(株)
委員	二瓶　哲也	(株)インテージ
委員	馬來　稔	(株)クロス・マーケティング
委員	加藤　宏	(株)インテージ
委員	鹿戸　隆史	イプソス(株)
委員	三橋　章人	(株)インテージ
委員	笹田　幸典	(株)日本リサーチセンター
委員	田中　悟史	(株)ビデオリサーチ
委員	磯部　直樹	(株)マーシュ
委員	山川　知	(株)東京サーベイ・リサーチ
委員	金澤　宣明	(株)日経リサーチ
委員	星野　洋子	(株)サイズ
事務局長	中路　達也	(一社)日本マーケティング・リサーチ協会
事務局	上杉　公志	(一社)日本マーケティング・リサーチ協会
事務局	岡　愛	(一社)日本マーケティング・リサーチ協会

(監修)

委員長	一ノ瀬　裕幸	JMRA　ISO/TC225 国内委員会