Global Guideline

Online Research

ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA

ESOMAR は社会・世論調査および市場調査の世界的機関で、市場調査の推進、発展および向上を目的とする主要機関です。www.esomar.org

グローバル・リサーチ・ビジネス・ネットワーク（GRBN）は、5 大陸における 38 の調査協会および 3,500 以上の調査機関を結ぶネットワークです。www.grbn.org

Official Translation Partner:
Language Connect

目次

1 イントロダクションおよび範囲

2011 年、ESOMAR は CASRO と共同で、「オンライン調査実施に関するガイドライン」をさらに、2015 年には ESOMAR／GRBN オンラインサンプルの質に関するガイドラインを発行した。調査者がオンライン調査をデザインおよび実施する際は、本ガイドラインだけでなく、「ESOMAR／GRBN オンラインサンプルの質に関するガイドライン」も参照することが推奨される。

この 10 年間で、オンライン調査に関する多くの技術的および方法論的な問題が明らかになる一方、テクノロジー、およびオンラインで収集可能なデジタルデータのタイプや多様性は常に発展しているため、職業的および倫理的ガイドラインには継続的な見直しと更新が必要である。

本「ESOMAR／GRBN オンライン調査に関するガイドライン」は、世界各国の現在の法的枠組みおよび規制環境において、市場、社会および世論調査の基本原則の一部をどのように適用するかをグローバルな視点から説明するものである。そのため、本文書では、既存の規制を列挙するのではなく、原則を説明している。本書の目的は、特に中小規模の調査機関の調査者が、新しいテクノロジーを使用してオンラインで調査を実施する際、法的、倫理的そして実務的な検討事項に対処することを支援することである。

本ガイドラインは、世界中の 60 を超える地域協会、または GRBN を構成する 38 の協会の各行動規範に採用されている ICC／ESOMAR 市場および社会調査における国際行動規範の熟読および理解に代わることを意図していない。むしろ、本ガイドラインは、オンライン調査におけるこれらの行動規範の基本的原則の解釈となるよう作成されている。

また、特定の国では基本原則の実施方法が異なる場合があるため、調査者は、データの収集および処理を計画する各国で定められるデータ保護および市場調査の自主規制要件を確認し、遵守することも重要である。本文書で提供するガイダンスは最低限の基準であり、特定の調査プロジェクトでは追加的な方策で補足する必要がある可能性がある。調査者は、自主規制要件を確実に遵守するため、調査を実施する国によっては、法的機関に問い合わせる必要があります。

調査者は消費者の懸念に対して敏感であり、市場調査の成功は一般の人たちの信頼に基づくことに注意していなければならない。調査者は、市場調査に対する一般の人たちの信頼を裏切るような行動および技術を使用してはならない。これには、調査デザイン、特に適切な質問デザイン、時間、参加者の負担に関して、適切な方法論的原則および実施事項の適用が含まれる。調査者は、また、調査と、ダイレクトマーケティングまたはターゲティング広告などの商業的行為の違いを常に明確にするよう努力しなければならない。調査手法を用いながらも純粋に調査のみを意図していない場合、調査者はそのような行動を、市場、社会または世論調査と説明してはならない。

本書では、必須要項を区別するため、「しなければならない」という表現が使用される。また、調査者が従う義務を負う原則または手続きを説明する際にも、「しなければならない」という表現が使用される。「すべきである」という表現は、実施について説明する際に使用される。この表現の使用は、調査者は、調査デザインに応じて異なる方法で、原則または手続きの実施を様々な方法で選択できることを示すことを意図している。

2 定義

アクティブなエージェント技術とは、バックグラウンドで、通常他のアクティビティを同時に実行している状態で、調査参加者の行動を把握する技術を意味する。これには次が含まれる。

訪問したウェブページ、完了したオンライン取引、記入したオンラインフォーム、広告のクリックスルー率またはインプレッション、オンラインでの購買、およびインターネットに接続するコンピューティングデバイスの GPS 情報など、調査参加者の実際のオンライン行動が把握できるトラッキングソフトウェア。このソフトウェアは、ハードディスクなどのデバイス上に保存されている調査参加者のメールおよびその他の書類から情報を把握することもできる。この技術の一部は、参加者が完全に知らず、オプトインの同意をしていない状態で、特にダウンロードまたはインストールまたはデータ収集が行われる場合、「スパイウェア」と分類されている。

調査参加の機会、調査コンテンツのダウンロードまたは調査質問について、調査参加者となる可能性のある者に警告を発することだけを目的として使用される、ユーザーのコンピューティングデバイス（コンピューター、タブレット、スマートフォンなど）にダウンロードされたソフトウェア。これは調査参加者によるインターネットのブラウズを追跡せず、全てのデータはユーザーが記入して直接提供する。

アクティブな調査とは、調査参加者との直接的なやり取り（対面、または電話、郵便、メール、ショートメール、その他の電子的方法を含むオンラインなどのその他のコミュニケーション方法を通じた、アンケート、フォーカスグループ、またはその他の調査方法）を通じたデータ収集を意味する。

ビジネス・トゥ・ビジネス調査（B2B）とは、企業、学校、非営利団体などの法的主体に関するデータ収集を意味する。

ビジネス・トゥ・コンシューマー調査（B2C）とは、個人または家庭から、あるいは関連するデータ収集を意味する。

クラウドコンピューティングとは、集中化されたデータ保存およびコンピューターサービスまたはリソースへのオンラインアクセスを可能にする一連のリモートサーバおよびコンピューターネットワークの配置を意味する。クラウドコンピューティングには、パブリック、プライベート、ハイブリッドの 3 種類の配置モデルが含まれる。

商業的行為とは、ダイレクトマーケティングやターゲット広告を含む、調査以外を目的とする全ての行動を意味する。

同意とは、回答者が、個人データの収集および処理に対して、自由意思で情報を基に与えた承諾を意味する。

クッキーとは、少量の情報を含むテキストファイルで、ユーザーがウェブサイトを閲覧すると、ユーザーのデバイスにダウンロードされる。その後ウェブサイトを閲覧するごとに、クッキーは元のウェブサイト、またはそのクッキーを認識する他のウェブサイトに読み込まれ送信される。

クッキーは、ウェブサイトがユーザーのデバイスを認識し、それによってユーザー体験をカスタム化することができるため有用である。これには、ユーザーの好みを記憶する機能などが含まれ、そのため通常ウェブサイトのナビゲーションをより効率的なものにする。調査者は、調査体験の向上、品質管理、検証を提供するため、調査への参加を可能または容易にするため、また、完了した調査またはその他の完了した行為のトラッキング、不正の検知および防止などの目的のため（ただしこれに限定されない）、クッキーを使用することがある。クッキーは、ブラウザの設定を通して拒否または削除することができる。

データ管理者とは、個人データの処理方法の決定に責任を担う個人または組織を意味する。例えば、調査依頼企業は顧客から受け取るデータの管理者である、調査パネルプロバイダー

はオンラインパネルメンバーから収集したデータの管理者である、調査企業はオムニバス調査の参加者から収集したデータのデータ管理者である。

データ処理者とは、データ管理者の依頼を受け、その指示のもとで、個人データの取得、記録、保持、または（分析を含む）作業を実施する者を意味する。上記に記した通り、調査企業はオムニバス調査のデータ管理者であると同時にデータ処理者になり得る。

デバイス ID（デバイス認識番号）とは、スマートフォンまたは同様の携帯デバイスに関連する独特の番号である。このようなデバイスには、一般的に、異なる目的で使用される複数のデバイス ID がある。一部のデバイス ID は、Wi-Fi または Bluetooth のようなサービスを可能にするため、またはモバイル事業者のネットワークで操作する特定のデバイスを認識するために使用される。Apple の UDID または Android の Android ID などのその他のデバイス ID は、アプリ、デベロッパー、そしてその他の企業により、様々なモバイルサービスにおけるデバイスおよびそのユーザーの認識、追跡および分析のために使用される。

デジタルフィンガープリント（デバイスフィンガープリント、マシンフィンガープリントまたはブラウザフィンガープリントとも呼ばれる）は、コンピューティングデバイス（コンピューター、タブレット、スマートフォンなど）を識別する目的で収集した情報である。デジタルフィンガープリントは、クッキーが無効になっている場合でも、調査参加者またはデバイスを完全にまたは部分的に認識するために使用することができる。これは、一般的に、ウェブブラウザのコンフィグレーション情報を、取得可能なその他のコンピューティングデバイスのパラメータとともに使用する。この情報は、デジタルフィンガープリントを構成する 1 つの文字列に同化される。デジタルフィンガープリントは、調査以外のアプリケーションにも使用され、オンラインでの個人情報盗難およびクレジットカードの不正利用の防止に有用であることが証明されている。

一部の法管轄地域では、デジタルフィンガープリントを個人データをみなすこともあるため、同意の必要性を含み、個人データとして取り扱われなければならない。

デジタルフィンガープリントの構成要素は徐々に変化する可能性があり、デバイスに関連するデジタルフィンガープリントも同様に異なる場合があることに注意が重要である。

市場調査においては、デジタルフィンガープリントの代わりにデバイス ID という用語が使用される場合もある。ただし、デバイス ID には異なる意味がある（デバイス ID を参照）。

無料抽選とは、運によって賞品を配分するコンテストやくじで、参加者が当選するために、支払いをしたり登録以外の行為をする必要がないものを意味する。これは「くじ」と称されることがあるが、多くの法管轄地域では「くじ」は非常に特定された法律用語であり、調査機関などの民間団体には禁じられている場合が多い。

ジオロケーションとは、コンピューティングデバイス（コンピューター、タブレット、スマートフォンなど）のオブジェクトの実際の地理的な場所を意味する。また、ジオロケーションは位置評価の実行、または実際に評価された位置と称される場合もある。

報酬とは、調査参加を奨励するため参加者に提供されるすべての利益を意味する。

プライバシー保護法とは、国内法または規制、本文書に設定される原則に則った個人データの処理に効力を持つ法の施行を意味する。

ローカル共有オブジェクト（LSO）とは、（HTTP クッキーと類似していることから）一般に Flash クッキーと呼ばれ、Adobe Flash を使用するウェブサイトがユーザーのデバイスまたはコンピューターに保存する可能性のあるデータである。

市場調査とは、社会・世論調査を含み、見識を得たり、意思決定の根拠とするため、応用社会学、行動科学による統計的および分析的方法および手法を使用して、個人または組織に関する情報を体系的に収集し、解釈することを意味する。

オンライン調査とは、質問、調査デザイン、データ収集または分析の開発を含む市場調査プロセスの全ての段階で、補佐するためにコンピューターネットワーク、主にインターネットを使用することを意味する。

パラデータとは、調査データを収集するプロセスに関するデータを意味する。 その例には、調査が回答された日時、調査にかかった時間、調査内での参加者の移動が含まれる。

パッシブな調査とは、参加者の行為または行動を観察、測定または記録してデータを収集することを意味する。

個人データ（個人を特定できる情報、PII）とは、特定されたまたは特定可能な自然人に関連する全ての情報を意味する。身元の特定が可能な個人とは、特に身分証明番号、または身体的、生理学的、精神的、経済的、文化的または社会的特徴の言及により、直接的または間接的に特定が可能な個人である。一部の調査では、このようなデータ記録に、調査中に収集された写真、動画、録音、またはその他の個人データのため個人の特定が可能な状況が含まれる場合がある。

PII とは、個人を特定可能な情報を意味する。個人データを参照のこと。

プライベートクラウドとは、特定のデータセンターで調査者の機関専用の装置が割り当てられているクラウドコンピューティングの配置を意味する。

パブリッククラウドとは、サービスプロバイダーが、アプリケーションやストレージなどのリソースを、インターネット上で一般の人に対して使用可能とするようなクラウドコンピューティングの配置を意味する。

調査回答者とは、調査目的で、その個人データがアクティブまたはパッシブな方法で収集される個人を意味する。

調査者とは、顧客の組織に勤める者や、使用されるあらゆる下請業者を含み、市場調査プロジェクトを実施する、またはコンサルタントとして行動する個人または組織を意味する。

センシティブなデータとは、身元特定が可能な個人の人種的または種族的出自、健康または性生活、犯罪歴、政治的意見、宗教または哲学的信念、または労働組合のメンバーシップなどに関するすべての情報を意味する。法管轄地域により、他の情報もセンシティブであると定義されている場合がある。例えば、米国では、個人の健康に関する情報、収入またはその他の経済的情報、金融に関する識別情報、および政府が発行した、あるいは経済的に個人を特定可能である文書もセンシティブとみなされる。

ソーシャルメディア調査とは、ソーシャルメディアのデータが単独で、または他のソースからのデータと合わせて使用される調査を意味する。

スパイウェアとは、ユーザーが知らないうちにコンピュータを制御したり、個人または組織についての情報を収集し、そのような情報をユーザーの同意なく他の組織への送信することもあるソフトウェアを意味する。

委託契約とは、調査プロジェクトの一部の実施に関する責任を、アウトソースまたは国外を含む第三者組織または個人に移転することを意味する。

トラッキングピクセルとは、ウェブページまたはメールに組み込まれ、ユーザーにとってわかりにくい（通常目に見えない）オブジェクトである。トラッキングピクセルによって、ウェブページの運営者またはメールの送信者は、ユーザーがそのページまたはメールを見たか

どうかを判断することができる。メールのトラッキング、およびウェブアナリティクスのためのページタグがよく使用される。ウェブビーコン、トラッキングバグ、タグ、ページタグ、またはウェブバグと呼ばれることもある。

転送とは、データに関して、媒体の種類にかかわらず、1 つの組織から別の組織へのデータの開示、コミュニケーション、複製、または移動を意味する。これには、ネットワーク間の移動、物理的な移動、1 つのメディアまたはデバイスから他のメディアまたはデバイスへの転送、またはデータへのリモートアクセスが含まれるが、これに限定されるものではない。

個人データの国外への転送とは、データを収集した国以外の国からのデータへのアクセスを含め、何らかの方法で国境を越えた個人情報の移動を意味する。これには、データの収集および保存のためのクラウドテクノロジーの使用を含む場合がある。

3 参加者：関係および責任

3.1 市場、社会および世論調査とその他のデータ収集活動との区別

調査者は、調査目的が、調査以外のオンライン活動と明確に区別されていることを確実にしなければならない。さらに、調査者は、市場調査以外のいかなる目的のためにも、収集した個人データの使用を許可してはならない。この区別を調査参加者に明確に伝えるために、調査者は、調査が調査以外の活動と明確に区別されるような方法で、調査を実施する調査サービスおよび組織または企業を提示しなければならない。

この要件は、いかなる個人データの収集も誤った意図を目的とせず、いかなる個人データも、各参加者から具体的な情報に基づいた同意が得られない限り、別の目的のために使用されないということを条件に、調査者が調査以外の活動に関与することを妨げるものではない。また、この要件は、市場調査およびその他の活動が明確に区別され、適用される法規制および国内の職業的行動規範に従って別々に実施される場合、組織がその両方を実行するという事実を促進する権利を、いかなる方法においても制限することはない。

3.2 通知、誠実、同意、および調査の任意的性質

調査者は、いかなる形態の個人データも、収集および処理前に調査参加者から情報に基づいた同意を得なければならず、収集を計画している情報、収集する目的、どのように保護されるか、誰とどのように共有されるかについて完全に平明でなければならない。情報は、明確、簡潔および目につきやすいべきである。これには、プライバシー保護方針におけるベストプラクティスの使用、アンケートおよびパネルサイト上でのプライバシー保護方針へのリンクの目につきやすい配置、そしてデータ収集およびデータ使用プロセスの全体におけるコミュニケーションが含まれるが、これに限定されない。参加者に誤解を与える、うそをつく、だます、または強要することがあってはならない。調査への参加は常に任意のものであり、参加者には、個人データが仮名化されていない限り、いかなる時点でも調査への参加の撤回および個人データの削除が許可されなければならない。

本ガイドラインは、一部の状況において、同意を得ることができないことも認識している。詳しい情報は、セクション 3.2.1 を参照のこと。

調査中のいずれかの時点で、調査計画に重大な変更がある場合（例えば、場所などパッシブなデータ収集が追加される、または調査使用者の顧客と身元特定可能なデータが共有される、など）、参加者が調査を続行するかどうかを情報に基づいて選択できるよう、その変更を通知しなければならない。アクセスパネルまたは調査コミュニティの場合、または調査が複数回にわたるデータ収集を含む、または数か月以上延長される場合、調査者は、データが収集されること、データ収集の理由および意図される使用について参加者に確認することで、定期的に新たに同意を得るべきである。 新たな同意を得るべき時期には、データ収集または

データ使用方法に関する重大な変更がある時、調査組織または所有者が変更される時、または適用される法規制が変更される時が含まれるが、これに限定されない。

最後に、調査者は、適用される法規制、国内の職業的行動規範をすべて遵守しなければならない。

3.2.1 パッシブデータ

新しいテクノロジーにより、データが収集される個人と直接やり取りせずに広範な個人データを収集できるようになっている。

その例には、ウェブブラウジングのデータ、ロイヤルティカードおよび店舗のスキャナー、接続されたデバイスからのジオロケーションのデータ、そしてある種のソーシャルメディアのデータが含まれるが、これに限定されない。モバイルテクノロジーは進化し続けているため、多くのこれらのデータソースはモバイルデバイスからもアクセス可能になっている。

調査者がパネルメンバーまたはモバイルアプリケーションからサイト間ブラウジングのデータを収集する場合、特定のデータ収集および収集のために使用する方法に関して参加者に詳細を説明し、データ収集に先立って明示的な同意を得なければならない。これは、特に、ジオロケーション、パッシブリスニング、そしてモバイルデバイスのオペレーティングシステムの測定に関する携帯アプリの場合、特に重要である。

個人データをウェブサイトまたはソーシャルメディアのサイトなど、公共のスペースで収集する場合、プラットフォームの利用規約で規定される通り、直接または明示的に同意を得なければならない。これは、プライバシーがあまり期待されていないと考えられるソーシャルメディア上の公開情報（著者名を含む）には適用されない。

CASRO および ESOMAR を含む一部の協会では、ソーシャルメディアに特化したガイドラインが設定されているため、詳細な情報を確認するべきである。これらが組み合わされた「ESOMAR／GRBN ソーシャルメディアに関すガイドライン」が現在作成中であり、2016 年初めに発行される予定である。

調査者が第三者のデータ収集サービスを使用する場合、データを合法的に得たことを確実にする責任は調査者にある。

各国で規制の実施行方法が異なる場合があるため、[1]調査者は、データの収集および処理を計画する各国で定められる国内および国際的データ保護規制および市場調査の自主規制要件を確認し、遵守しなければならない。

調査者が同意なく第三者にコメントを転送した場合、コメントのマスキングなどの手法を用いて匿名化されたデータのみを報告することを確実にしなければならない。

全ての調査プロジェクトの実施にあたり、調査企業は、調査企業への連絡方法を含め、データ収集およびプライバシー保護の実施方法に関して、明確でアクセス可能なプライバシー方針を提供しなければならない。

さらに、調査者は、データの取得方法にかかわらず、あらゆる個人データのプライバシーと安全性を守る義務を有する。これには、調査機関が第三者と共有する前にデータを匿名化する、データの受領者との間で個人の再特定を試みたり、データを調査以外の目的で使用しないことに同意する契約を締結する、などが含まれる。

[1] 多くの法管轄地域は、個人データ収集、処理、および共有に対する同意を要求している。一部の法管轄地域では、同意の確保が明らかに実行不可能であり、顧客に提供される分析が匿名化されたデータの形で行われる場合には、調査目的の例外が許可される場合がある。

3.2.2 センシティブなデータ

オンライン方法は他の方法と比較して侵入性の低いデータ収集方法であり、調査者は対面または電話でのインタビュー（インタビュー担当者の立会いのもと）よりもセンシティブなトピックを切り出しやすいが、調査者は、法的要件のため、または参加者に損害あるいは心理的苦痛を与えるリスクのため、センシティブな性質のトピックを参加者に問う際には、慎重に行わなければならない。

調査者は、調査でセンシティブな質問をする目的を説明し、参加者の明示的な同意を得て、データは匿名化され機密事項として処理され、各質問には「回答したくない」の選択肢があるか、あるいは回答したくないセンシティブな質問には回答しない他のオプションがあることに言及し、質問が必要なもので、調査との関連性が高く、明確であることを確実にしなければならない。調査デザインが原因でこれらが保護できない場合、参加者にその旨を通知し、明示的な同意を得なければならない。

一部の国では、該当する国家当局からセンシティブな個人データ収集に対する承認を得る必要がある場合がある。

3.3 損害を被らないことの確認

調査者は、オンライン調査参加者が調査プロジェクトへの参加によって、損害を被ったり不当な影響を受けないことを確実にするため、あらゆる妥当な注意を払わなければならない。これには、経済的、身体的または感情的ないかなる損害も含まれる。そのため、調査者は、調査の特定要件を注意深く検討し、国内の法的要件／制約および規制を調べ、調査が参加者に及ぼす現実的な影響を考慮するべきである。 あらゆる場合において、調査者は公正な取扱いの原則を適用しなければならない。これには次が含まれる。

参加者にとって有害となる、または不快感を与えるような誤解を招く言明を避ける（例えば、調査内容、調査の予想所要時間、後日オンラインまたは他のインタビュー手法を用いた再インタビューが行われる可能性などに関する不正確な情報など）。

誤解を招くまたは未承認のデータ収集および処理を避ける（例えば、ユーザーがプライバシーを期待し、特定の行為に対する同意を求められることを期待するようなオンライン環境／モバイルデバイスで個人データを収集する非開示の自動システム、など）。

参加者が市場調査機関／調査者に尋ねる可能性のあるあらゆる問い合わせへの対応。

調査者は、調査結果から個人情報が突き止められたり、個人の身元が交差分析（演繹的開示）、小サンプル、またはその他の方法で推論できないことを確実にしなければならない。その例として、地理的データなどの補助的情報と、特定の調査参加者を特定できる能力を合わせたものが含まれる。

3.4 データ保護およびプライバシー

調査者は、個人データに関する世界的なデータ保護原則を遵守しなければならない。これらの原則には、収集され保持されるあらゆる個人情報は次の通りでなければならないとされている。

特定の調査目的のために収集し、この目的と相入れない方法では使用しない。

収集し、さらに処理する調査目的に関連して、十分かつ適切であり、過剰ではない。

可能な場合、回答データとは別に保存される。

情報の収集、さらに処理に必要な期間を超えて保存されることはない。

調査者は、全ての適用される国内法規制も遵守しなければならない。

3.4.1 プライバシー保護方針

プライバシー保護の法規制はすべて、一般的に、調査企業にウェブサイト上にプライバシー方針を掲載することを求めている。これらのプライバシー保護方針は、収集する個人情報、個人情報が使用、管理（保存およびアクセス）、共有される方法、第三者に開示することができる条件について調査参加者に知らせるものでなければならない。プライバシー保護方針は、詳細情報を得る方法および苦情を申し立てる方法についても説明しなければならない。また、全てのオンライン調査、該当するウェブサイト、および電子的コミュニケーションにおいて（一般的にリンクとして）も、プライバシー保護方針を参照できるようにしなければならない。

参加者は、データ収集に適用される法律についても知らされなければならない。複数の国でデータを収集する場合、調査者は調査を実施する国の法律を遵守しなければならない。参加者の居住国を知ることが可能である場合、調査者は、各法管轄地域で法規制に大きな違いがある場合があることを念頭に置いたうえで、その国の法規制に従わなければならない。

3.4.2 データのセキュリティ

調査者は、各データの喪失、不正アクセス、破壊、使用、修正または開示などのリスクから保護するためのセキュリティ・プロトコルを確実に整えなければならない。それに従い、調査者は厳格なデータセキュリティ方策を採用しなければならない。

調査者が必要な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べき様々な基準および枠組みが存在する。詳しい情報は、ISO 27001: 情報テクノロジー - セキュリティテクノロジー - 情報セキュリティマネジメントシステムまたは ESOMAR データ保護チェックリストを参照のこと。

3.4.3 違反通知

調査者は、違反通知およびプロトコル要件に関して適用される全ての法規制を遵守しなければならない。適用するべき法規制がない場合、調査者は、顧客、調査参加者、および下請業者など影響を受ける全ての当事者に対し、速やかにセキュリティまたはデータの違反について報告しなければならない。通知には、違反に関与したデータのタイプ、およびその違反の結果生じる可能性がある損害から保護するために個人が取るべき手段が含まれているべきである。

3.4.4 国境を越えた転送

個人データを収集した国から別の国へ転送する前に、調査者は、データ転送が合法であり、そ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あらゆる妥当な手段が取られていること確実にしなければならない。これは、データ収集サーバが別の国にある場合に適用される。この原則は、クラウドテクノロジーが使用され、クラウドサーバが別の国に置かれている場合にも適用される（セクション 7.7 を参照）。

3.5 メールおよびショートメールによる依頼

各国の国内法には、メールおよびショートメールの取扱い方法に違いがある場合がある。一部の国では、明示的な同意が得られていない場合、自動化されたシステムを使用したショートメールの送信は禁じられている。[2] 調査者は、参加者となる可能性のある者からメールア

[2] 通話および携帯電話のショートメール送信の際の自動化システムの使用に関する法規制は国によって異なるため、注意が必要である。調査目的の例外を認める法管轄地域がある一方、同意を必要とする法管轄地域もある。

ドレスや携帯電話番号を取得するために、いかなる口実も使用してはならない。これには、パブリックドメインの使用、個人が知らない状態でのテクノロジーまたは手法の使用、または調査以外の行動を装った収集が含まれる。

調査者は、調査参加の依頼、または秘密裡のデータ収集のため、未承認のメールまたはショートメールを使用してはならない。ここでの「未承認」とは、参加者がこのようなメールまたはショートメールの受信に同意していない、または合理的に予期していないことを意味する。

メールまたは SMS ショートメールで調査の連絡を受けた個人は、調査の連絡のメールまたはショートメールを受け取ることを合理的に予期していなければならない。次の状況が全て存在し、国内の法規制に基づき制限または禁止されていない場合、このような同意を想定することができる。

連絡を受ける個人と調査者、メールアドレスまたは携帯電話番号を提供する顧客、メールアドレスまたは携帯電話番号を提供するサンプルプロバイダーの間に以前から存在する実質的な関係が存在する（後者は、メールでの依頼またはショートメールによってそのように特定またはリンクされる）。

メールまたはショートメールで参加を依頼される者が、調査者またはサンプルプロバイダによるオンラインまたはモバイル調査に特にオプトインしている場合、またはメールまたはショートメールでのコミュニケーションからオプトアウトしていない、あるいは調査のために連絡してもよい顧客のリストが顧客から提供される場合。

調査参加者となる可能性のある者に対するメールおよびショートメールでの依頼が、サンプルプロバイダー、調査者または顧客、およびその個人との関係を明確に伝達またはリンクし、今後のメールまたはショートメールでの連絡を拒否する選択肢を明確に与えている。

メールサンプルまたは携帯電話番号のリストが、時宜を得た適切な方法で、以前その後のメールまたはショートメールでの連絡を拒否することを要求した全ての個人を除外している。

メールおよび携帯電話サンプルの参加者は、メールまたはショートメールによる未承認の依頼によって参加を求めれられなかった。

調査者は、次の点にも注意しなければならない。

顧客またはサンプルプロバイダーからメールリストまたは携帯電話リストを受け取る際、調査者は、顧客またはサンプルプロバイダーとともに、リストに掲載される個人がメールによる連絡またはショートメールを受け取ることを合理的に予期していることを確認しなければならない。

調査者は、参加者に依頼する際には、虚偽または誤解を招く返信用メールアドレス、またはその他の虚偽および誤解を招く情報を使用してはならない。

調査者は、参加者に対し、いかなる調査プロジェクトからもオプトアウトする機会を提供しなければならない。これは、参加者が盲検研究（調査依頼者がメールでの依頼またはショー

注意する必要のある特定の法管轄地域の一つは米国である。米国では、電話消費者保護法（TCPA）により、通話およびショートメール送信のため自動化システムを使って携帯電話に連絡するためには、同意が必要とされる。

トメールに記載またはリンクされていないが、インタビュー中または後に参加者に開示する）のサンプルソースリストからの削除を求めた場合にも適用される。

調査者は、ショートメールと類似した特徴および機能を持つ通知のために、モバイルアプリケーション（携帯アプリ）などその他のメッセージテクノロジーを使用する際には、本セクションの該当する要件を遵守しなければならない。

調査者は、調査参加者から受領する個人情報のアクセスおよび使用に同意する、または制限を設けるメールおよびその他の文書の複製または記録を残すことはグッドプラクティスである。[3]

3.6 報酬

くじ、および無料の抽選に関する規則と、報酬に関する次の規則を合わせて読むべきである。

オンライン調査プロジェクトへの参加を奨励するために報酬が提供される際、調査者は、参加者が次のことについて明確に知らされていることを確実にしなければならない。

報酬を管理する者

報酬の内容

参加者が報酬を受け取る時期

付随条件（例えば、特定のタスクの完了、または（オンラインのパネル調査とともに）品質管理の確認に合格する、など

調査者は、報酬が相応であり、わいろとならない、またはわいろとみられることがないことを確認しなければならない。報酬は、回答者および調査の性質に対し適切なものでなければならない。例えば、オンライン調査が運転の習慣に関するものである場合、報酬としてアルコール飲料を提供することは適切ではない。

調査者は、報酬の管理のために収集したデータを、データベース構築など、他の目的で使用しないことを確実にしなければならない。調査者は、報酬プロセスの一環として収集した参加者の身元を特定できる詳細を、顧客（顧客サイドの調査部門で実施される場合、社内顧客を含む）またはその他のいかなる第三者に対しても、参加者の明示的な許可なく転送してはならない。

調査者は、報酬に関する国内法規制を知らなければならない。例えば一部の国では、

参加者が報酬から利益を得るために代金の支払いを必要とするような報酬または割引料金を顧客が提供する場合（例えば、参加者が利益を得るためには差額を支払う必要がある製品およびサービスの価格割引など）、このような行為はダイレクトマーケティングの範疇になるため、オンライン調査では禁じられている（顧客から提供された報酬および割引は、顧客への販売促進の一形態とみなされるため）。

[3] これは、EU（欧州連合）加盟国すべて、アルゼンチン、オーストラリア、カナダ、ニュージーランド、および米国（米国－EU 間セーフハーバープログラムに参加する調査者のみ）を含む国々では、法的要件となっている。

報酬は特定の性質のものでなければならない（金銭以外のもの、など）。

国境を越えた、複数の国においてオンライン調査プロジェクトを実施する際には、報酬適用のプロセスは、関係する全ての国で適用される全ての法律を遵守しなければならない。

3.6.1 くじおよび無料抽選

くじおよび無料抽選は、オンライン調査の報酬として特に人気がある。これらを使用する際、調査者は、国によって異なる適用される法規制、必要とされる詳細な知識をもたずこの方法を用いることの重大なリスクを理解していなければならない。例えば、一部の国では、

参加者が無料抽選またはくじに登録するために、オンライン調査プロジェクトへの参加に同意する以外に何らかの行為をする必要があってはならない。これには、特に個人が不相応な量のデータを提供する場合、調査プロジェクトの一部である調査の質問への回答、調査の完了を要求しないことが含まれる。それは、参加者が「金額に応じてデータを譲渡している」とみなされる場合があるからである。このような場合、参加者への支払いの要件と同じようにみなされ、法規制に従った有料のくじとみなされる。

抽選に登録する前に、比較的簡単なある程度の知識を要求する質問（「アメリカの大統領は誰か？」など）をするなど、参加者を分類するため、無料抽選／くじの登録にある形態のスキルが求められる場合がある。

調査活動またはプロジェクトを完了しなくても、参加者は無料抽選またはくじへの登録を除外されない。

参加者が無料抽選／くじの規定に設定される基準を明らかに満たさない場合を除いて（無料抽選またはくじを担当する社員の家族の抽選への参加を制限する、など）、調査者は無料抽選／くじを撤回してはならない。

調査者は、同意を求める時点で無料抽選 / くじに関連する全ての情報が、参加者に明確に伝えられていることを確実にしなければならない。具体的な要件は国によって異なるが、次の情報が含まれる。

登録最終日

賞品の性質

いずれかの賞品の代わりに現金を受け取ることができるか

当選者に結果を通知する方法と時期

当選者と結果を発表する方法と時期

参加資格および失格となる基準

別の登録方法

全ての規則は、参加者が容易に理解し、誤解を生じさせないよう、明確で明白なものではければならない。これには、当選確率、賞品の価値などが含まれる。さらに、

このような規則は、非合理的または不当に制限するものであってはならない。

調査者は、参加者全員またはほぼ全員に提供される贈答品と、当選者に提供される賞品を明確に区別しなければならない。

調査者は、全ての無料抽選 / くじに別の無料登録方法があること、そしてどの登録方法でも当選確率は平等であることを確実にしなければならない。

調査者は、無料抽選 / くじの当選者が、偶然の法則を確実に公正に適用する方法で選ばれることを確実にしなければならない。当選者の決定プロセスは、明確な監査証跡で裏付けられなければならず、いかなる抽選も独立したものでなければならない。一部の国では、抽選が行われる際、参加者に平等な機会が与えられていることを確実にするため、独立した立ち合い人が必要となる場合がある。

最後に、調査者は、顧客に代わって実施する無料抽選／くじに対する顧客の責任または潜在的な責任について、顧客が周知していることを確実にしなければならない。調査者は、このような責任を軽減するため、顧客のアプローチ方法について話し合うべきである（第三者および免責規定を含める、など）。

調査者は、この種の行為を実施する前に、各国の協会のガイドラインを常に確認しなければならない。

4 顧客：関係および責任

4.1 委託

調査者は、調査のいずれかの部分が調査者が所属する組織以外の組織に委託される場合、調査開始前に顧客にその旨を知らせなければならない。要求に応じて、顧客にその委託組織の身元を明かさなければならない。

サンプルソーシングに使用する委託業者の身元が専有情報だと合法的にみなされる場合、サンプルプロバイダは下記を提供しなければならない。

使用するサンプルソースのタイプの説明、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割合の推定値。

調査者は、委託業者と共有する個人データは、委託業務の遂行に必要なものに限定されること、委託業者はデータ保護のため、必要なデータセキュリティ手順を定めていること、そしてデータ保護に対する委託業者の責任が明確に文書化され同意されていることを確実にすることも求められている。

4.2 個人データの保護

調査者は、調査参加者の身元が顧客に開示されないことを確実にしなければならない。適用されるプライバシー保護法または規制がより厳格な要件を規定していない限り、調査者は、次の条件においてのみ、調査参加者の身元を特定できる個人情報を顧客に伝えることができる。

調査参加者が明示的に同意している。

調査のみを目的としている。

その情報を提供する直接的な結果として、マーケティングまたは販売行動を参加者に対して実施することはない。

さらに、上記条件が満たされない限り、顧客が参加者の身元特定を試みない旨、調査者は顧客から書面で保証を得ることが重要である。

4.3 平明さ、不当表示および誤りの訂正

全ての調査プロジェクトは、正確、平明、そして客観的に報告され文書化されなければならない。納品後に誤りが発見された場合は、直ちに顧客に知らせたうえで、迅速に訂正しなければならない。

報告要件に関する詳しい情報は、本文書の後半「セクション 6－方法の質」を参照のこと。

5 一般大衆：関係および責任

5.1 社会的信頼の維持

調査者は、サンプルプロバイダまたは顧客から提供されたサンプルに、調査への参加を依頼するメールまたはショートメールを受け取ることを予期している個人のみが含まれていることを確認する必要がある。モバイルアプリケーション（携帯アプリ）などその他のメッセージテクノロジーを使用した通知には、ショートメールと類似した特徴および機能がある。詳しい情報は、セクション 3.5 を参照のこと。

5.2 結果の公表

顧客が調査プロジェクトの結果の公表を予定している場合、顧客および調査者の両者は、発表する結果が誤解を生じないことを確実にする責任を負う。そのため、顧客には、結果を公表する形式および内容について調査者と相談することが強く奨励される。

調査者は、要求された場合、公表された結果の有効性を評価するために必要な技術的情報を利用できる準備も整えておかなければならない。これには、研究の背景に関連する情報、サンプルソース、データ収集方法、使用した質問の言葉遣い、使用された重み付け、および出版物に報告された表またはその他の分析のアウトプットが含まれる。

調査者は、データで十分に裏付けされている場合を除いて、市場調査プロジェクトの結論の配布時に自身の名を関連させることを許可してはならない。

6 方法の質

オンライン調査の使用者が、結果となるデータが目的に適うものであると納得する場合、調査者は、データによって裏付けられない結論が導かれる可能性のある方法の限界を含め、調査の実施方法についてこれらの使用者に適切な情報を提供可能にしなければならない。この情報には、次が含まれる。

サンプルのサイズ、ソースおよび管理

サンプルのデザインおよび選定

データの収集方法

適用された可能性のあるデータクリーニング、重み付け、またはフィールド後調整

インターネット普及率の低い国でオンライン調査を実施する場合、調査結果が研究対象者の意見を代表することを確実にするためにとられた措置

次に挙げるのは、最低限の要件である。詳しい情報は、ESOMAR／GRBN オンラインサンプルの質に関するガイドライン を参照のこと。

6.1 サンプルのソースおよび管理

オンラインサンプルのソースの主なカテゴリーは、下記の通りである。

オンラインパネル：サンプルプロバイダは、サンプルを生成するパネルを開発している。

リバーまたは動的に生成されるサンプル：インターネット上のトラフィックソース

リストサンプル：顧客リスト、業界団体の会員、特定の学校の学生、など

それぞれの場合において、サンプルプロバイダーは、サンプルの依頼方法およびサンプリングフレームの説明、そしてサンプルが調査対象層をどの程度代表しているかに関する情報を、調査者に対して提供可能にする準備を整えなければならない（例えば、サンプルが「NatRep」の場合、サンプルに使用される「NatRep」の正確な定義、サンプルにおいて代表性に欠ける可能性のある人口統計学的、地理的またはその他のグループを提供しなければならない）。さらに、調査者は、潜在的な非回答バイアスの評価を可能にするため、完了率および未完了率、そして適切な場合、回答率（リストサンプルの場合など）を報告すべきである。

サンプルプロバイダは、提供された回答の質および収集されたデータを確認するために使用した手順に関する情報を、閲覧可能にする準備もしなければならない。これには次が含まれる。

サンプルソース検証のためにとられた措置

パネル、コミュニティまたはリストの参加者となる可能性のある「初期の」者に使用された手順

クリーニングおよび更新の手順

個人の調査参加実績のモニタリング、または満足化または不正を最小限に抑えるための品質管理、およびそのような行為が特定された場合にとられる措置

参加者のサポート手順

報酬の管理方法

新しいソースのサンプリングフレームへの統合の有無とその方法

プロジェクトを追跡するためサンプルの一貫性を最大限に高めるために整えられているすべての手順

6.2 サンプルの選定およびデザイン

完了した調査が、調査対象層および調査デザインの目標を確実に代表するため、調査者は、サンプルソースのブレンディング、サンプルルーティング技術の使用、参加者に提供される報酬を含め、サンプル選定の際に使用されたあらゆるクオータまたはターゲティングの選定を文書化しなければならない。

6.3 データ収集

調査者は、調査使用者に対して、データ収集方法に関する適切な情報も共有しなければならない。アンケートが使用された場合、この情報には次を含むべきである。

アンケートの所要時間の中間値または平均値

全質問およびフィルターまたは回答者への指示の言葉遣い

データ収集の開始日と終了日

アンケートが、スマートフォンまたはタブレットを使用する参加者に対応するようにデザインされているか、デザインされていない場合、このような個人はサンプルから除外されるかどうか、または使用するデバイスに最適化されていない調査に参加するのかどうか

ソフトウェアのダウンロード、またはセンシティブな情報または個人データの共有など、特別なタスクを実施する必要性

6.4 データクリーニングおよび重み付け

調査者は、データのクリーニング方法、完了したインタビューがデータから削除されているかどうか、その場合の理由、重み付けまたはその他の調整に関する情報を文書化しなければならない。代入法が使用される場合、どの変数にどの程度代入されたか、および使用した代入方法を明確にする必要がある。

7 追加ガイダンス

7.1 子供からのデータ収集

子供からのデータ収集には、その子供の親または法的保護者から許可を得る必要がある。このような許可を必要とせずにデータを収集できる年齢を規定する規則は、国により大きく異なる。調査者は、親による許可が必要な場合、または文化的に繊細な事柄のため特定の取り扱いが必要な場合を判断するため、データが収集される国の国内法および自主規制の行動規範を調べなければならない。

回答者になる可能性のある者に最初に連絡する際、その者が子供であると思われる妥当な理由がある場合、調査者はその者の年齢を尋ねた後でその他の個人データについて質問しなければならない。回答された年齢が、その国で子供として定義されている年齢を下回る場合、適切な許可が得られるまでそれ以上の個人データの提供を促してはならない。調査者は、その子供に対し、許可を求めることができるよう、親または保護者の連絡先情報の提供を求めてもよい。

許可を求める際、調査者は、親または保護者が情報に基づいて子供の参加を決定できるように、調査プロジェクトの性質について十分な情報を提供しなければならない。これには次が含まれる。

調査を実施する調査者／組織の名称と連絡先情報

子供から収集するデータの性質

データの使用方法についての説明

子供に参加を依頼する理由、および予想されるメリットまたは影響についての説明

同意を与え確認する手順についての説明

同意を確認するため、親または責任を負う大人の連絡先住所または電話番号の提供の依頼

調査者は、責任を負う大人の身元、および子供との関係についても記録すべきである。

親が子供の調査参加に同意した後、調査に回答する子供の身元の匿名性を維持することと、必要に応じて、調査への回答を手助けするよう備えることを、親に伝えるべきである。

調査トピック（若年層の参加者または保護者を混乱させる可能性のあるセンシティブなトピックなどの重要な要素を含む）、および調査アンケートのデザイン（年齢、理解力など子供のそれぞれの特徴に合わせ、親／責任を負う大人、および子供の両方に、特定の質問への回答は必須ではないことを知らせる／言及する、など）に関して、特別な配慮をしなければならない。

以下については、親または責任を負う大人からの事前の許可を必要としない。

データ収集および許可の依頼を通知することだけを目的とする子供または親のメールアドレスの収集

スクリーニングおよび除外を目的とする子供の年齢の収集このスクリーニングにより子供がインタビュー参加基準を満たしていると判断される場合、調査を継続するため、スクリーニング後に親または責任を負う大人から許可を得なければならない。

7.2 オンラインでの身元確認およびトラッキングのテクノロジー

オンライントラッキングなど、オンラインのマーケティング活動に使用されるいくつかのテクノロジーは、調査において有効である。調査におけるこのようなテクノロジーの使用は、一般的に次を含むパッシブなデータ収集の一形態である。

オンラインサンプルの完全性の改善

不正防止

オンライン視聴者測定、コンテンツ測定および広告効果テストを含む（が、これに限定されない）調査応用これらおよび同様の場合、参加者の同意が必要となる。

7.2.1 特定のテクノロジーと調査における使用要件

これには次が含まれる。

クッキー

ローカル共有オブジェクト（Flash クッキーとも称される）

トラッキングピクセル

デジタルフィンガープリントおよびデバイス ID

これらのテクノロジーの一部は、オンライン行動ターゲティングなどのマーケティング活動にも使用されるため、その使用については、回答者が知らないうちにその個人のオンライン活動がモニタリングされる可能性を憂慮する立法者、規制当局、またプライバシー保護団体による精査を受けている。

できる限り、個人データを収集、使用、報告する方法に対する同意を得なければならない。これは、調査者が調査参加者のデバイスにソフトウェアのダウンロードを依頼する際、特に重要である。参加者の明示的な同意を得て、アクティブなエージェントのみを使用することができる。

直接的な同意またはその他の既存の同意（利用規約など）がそれ以外を許可しない場合、

データは集計された形でのみ報告または共有しなければならず、データの受領者との間で、データの受領者が個人の再特定を試みないことに同意する契約を締結しなければならない（セクション 4.2 参照）。

個人データを（顧客を含む）いかなる第三者とも決して共有してはならない。

データが不要になった場合、データを匿名化しなければならず、匿名化が不可能な場合は、データは受容されるベストプラクティスを使用して安全に保管しなければならない。

オンラインのトラッキングおよび身元特定のテクノロジーが調査に使用される際、調査目的のみで使用されなければならず、すべてに優先される市場調査の原則を適用しなければならない（詳しい情報は、セクション 3.1 を参照）。さらに、調査者は、適用される法規制、国内の職業的行動規範すべてを遵守しなければならない。

7.3 モバイル調査

一般に、モバイル市場調査は、本ガイドラインで取り扱うオンライン調査とは異なる方法とみなされる。ESOMAR および GRBN は、いずれもモバイルを特別に取り扱うガイドラインを発行している。

ただし、オンライン調査の依頼を受ける大半の参加者は、スマートフォンまたはタブレットなどのモバイルデバイスを使用して回答することを選択している。その結果、調査者は、オンライン調査をデザインする際、スマートフォンの制約（画面サイズやダウンロードの速度など）を考慮すべきである。

7.4 ソーシャルメディア調査

近年のソーシャルメディアの進歩により、数百万人が自分についての情報を新しい方法で世界中で共有している。インターネット上で自分のコンテンツを発信する消費者というコンセプトは当たり前になり、調査者が情報を観察、やりとり、収集する新たな機会が生まれている。コミュニティパネル、市場調査オンラインコミュニティ、クラウドソーシング、コ・クリエーション、ネットノグラフィ、ブログマイニング、および Web スクレーピングなど、ソーシャルメディアを駆使するための多くの手法がすでに開発されている。また、インターネットが進化し続けるのに伴い、将来さらに多くが進化を続ける可能性が高い。

調査者は、対面、メールおよび電話での調査を規定する基本的な倫理的および職業的原則を遵守しなければならない。

ソーシャルメディアのデータには、個人を特定可能な情報が含まれていることが多い。この分野で多くの規制が作成されたのは、一般にアクセスが可能なオンラインプラットフォームでの個人による多数の人とのコミュニケーションを可能にする前である。プライバシーおよびデータ保護法の改正はまだ策定中の状態であり、広く受け入れられるようになった慣行の変化に遅れをとっている場合が多い。

それにもかかわらず、調査者は、調査が計画されている法管轄地域で制定されている地方の法規制または業界の行動規範を調べなければならない。詳しい情報は、セクション 3.2.1 を参照のこと。

7.5 個人データの新しい形態

調査者は、写真、音声、動画は個人データであり、そのように取り扱われなければならないことを、認識しなければならない。デジタル画像に個人の顔が鮮明に写り、その個人の身元を特定できる場合、その画像は個人データとみなされる。それに従い、調査プロジェクトの一環として収集、処理および保存される全ての写真、動画および音声を個人データとして取

り扱い、保護しなければならない。それらは、参加者が同意した場合、調査目的の遂行だけを目的として顧客または調査使用者とのみ共有することができる。個人の特定ができないよう適切に匿名化された情報（ピクセル化または音声変換テクノロジーを使う、など）は、顧客または調査使用者の顧客と共有することができる。

詳しい情報は、ESOMAR データ保護チェックリストを参照のこと。

7.6 ビジネス・トゥ・ビジネス調査

多くの調査プロジェクトでは、企業、学校、非営利組織からデータを収集している。このような調査には、収益、社員数、セクター、地域など、組織に関する情報の収集が伴う場合が多い。

あらゆる場合において、参加組織は報告における身元開示に対して、他の調査形式において個人に与えられるものと同等の水準の保護を受ける権利がある。

多くの国のデータ保護法は、個人の役職名および職場の連絡先情報を個人データとみなしていることに注意が必要である。一部のデータ保護法では、その要件をさらに自然人および法的主体（個人と法人など）にまで拡大している。ただし、法人には調査参加者などのデータにアクセスする法的権利はない。

7.7 クラウドストレージ

個人データのクラウドへの保存は、慎重に決定すべきである。調査者は、クラウドストレージのサービスプロバイダーのセキュリティ管理および標準利用規約を検討し、プロバイダー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ない。例えば、調査者は、実行中（クラウドへ／からの転送）および保存中（クラウドプロバイダのサーバに保存）に個人データを暗号化すべきである。

調査者はまた、クラウドストレージが国境を越えた転送であるかどうかを判断するため、個人データが保存される具体的な場所についても検討しなければならない。個人データが別の法管轄地域に転送される場合、転送元と転送先の両法管轄地域におけるデータ保護要件を満たす方法で転送されなければならない。そのため、調査者は、適切な手配を決定するため、該当する国の法規制すべてを検討し、理解しなければならない。

調査者は、パブリッククラウドよりもプライベートクラウドに個人データを置くかどうかを、真剣に検討すべきである。プライベートクラウドの場合、専用の装置が調査者の企業に割り当てられており、調査者は個人データが置かれる場所を常に知ることができる。

反対に、パブリッククラウドは、データが 2 つ以上のデータセンター、または 2 つ以上の国または大陸に保存される結果になる場合があり、そのため、データ保護法に定められる適用要件、およびデータ管理者との間で締結している個人データの保存場所を指定する契約の両方の遵守に関する問題が生じる可能性がある（詳しい情報は、ESOMAR データ保護チェックリストを参照のこと）。

最後に、調査者は、サイバー賠償責任保険の加入も検討することが望ましい。セキュリティ違反が生じ、個人データが危険にさらされた場合、多くのクラウドストレージサービスプロバイダが提供する補償は十分ではない。これは、影響を受けた個人が損害を受ける結果となる重大なプライバシー侵害により、調査者の企業が経済的損害および損失の大きなリスクを受けることを意味している。

7.8 匿名化と仮名化

調査者のデータ保護に関する主な責任は、顧客または一般の人に対して開示する前のデータの匿名化である。匿名化とは、データを個人が特定ができない形態にするため、個人を特定する情報の削除または変更のいずれかを含む保護措置の 1 つである。その例には、特定の個人の特定を不可能にするため、画像をぼやかして顔を隠したり、集計された統計として結果を報告することが含まれる。

仮名化には、ID 番号などの固有の識別子の使用やハッシュアルゴリズムなどにより、データセット内で個人特定が依然として可能である方法で個人データを変更する一方、確認の目的で個人データを分離して保持することが含まれる。

このような手法を採用する際、調査者は、このようなデータの匿名化／仮名化に関する法的基準を満たすために、どの要素を削除すべきかを判断するため、国内法および自主規制の行動規範を調べるべきである。

7.9 スタティック ID とダイナミック ID の使用

従来、調査参加者のスタティックな識別子（スタティック ID）は、経年的研究およびアドホック研究の両方の特定の研究において、調査参加者の管理および割当に役立つよう、調査顧客およびサンプルプロバイダによって使用されてきた。この手法は、各参加者についての情報の統合に役立ち、単一の経年的研究における一意の参加者と調査研究の除外期間への遵守を確実にする有用なアプローチとなっている。品質管理・監督除外期間およびサンプル選定を改善し、研究に適する個々の調査参加者を正確に特定できることに加え、一部の調査者はデータ分析を容易にするためスタティック ID の使用も要求している。

ダイナミック ID（使用ごとに変化する ID）の使用は、一部のサンプルサプライヤーにより、個々のメンバーの身元の安全確保、悪質な顧客が調査参加者のデータならびにインタビューセッションで参加者から収集したその他のデータ（パラデータ）を使用して見識を深めるために、あるいは参加者の実際の身元を特定しようとすることを防止または削減する方法として奨励されている。

調査者は、各タイプの ID の使用、および特定の研究におけるプライバシーおよび調査品質に関する懸念のバランスを慎重に検討すべきである。全ての関係者（調査参加者、サンプルサプライヤー、調査者、エンドクライアント）の間の合意により設定された契約上の制限内で研究により生成した情報の収集および使用の管理に対し、法的および契約上の条項を適用すべきである。

7.10 パラデータの使用および管理

その後の調査プロセスにおいてこれらのデータの収集、使用および第三者への転送の指針となり、制限および保護するためにサンプルプロバイダーと顧客の間で交わされた法的合意に従って、パラデータを使用することが推奨される。

7.11 容認されない行為

下記は、厳密に禁じられている、または防止すべき容認されない調査者の行為のリストである。調査者が次の行為のいずれかをする場合、スパイウェアを使用しているとみなされる。

参加者の同意を得ずにソフトウェアをダウンロードする。

収集する情報のタイプ、およびその情報の使用方法について、完全、明確、簡潔そして平明な通知および開示をすることなくソフトウェアをダウンロードする。

参加者のオプトインに関する同意を得ずにキーロガーを使用する。

調査の実施に必要な範囲を超えて参加者のコンピューターの設定を変更するソフトウェアをインストールする。

スパイウェア対策ソフト、ウイルス対策ソフト、またはスパム対策ソフトを無効にする、または参加者のコンピューターまたはデバイスをハイジャックするソフトウェアをインストールする。

ソフトウェアが主要オペレーティングシステムに障害を発生させないこと、および他のインストール済みソフトウェアが不規則にまたは予期しない方法で作動しないことを確実にするためのあらゆる努力を怠る。

ダウンロードされる可能性がある、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ソフトウェア、または広告テスト目的のソフトウェアを除き、広告コンテンツを発信するソフトウェアをインストールする。

ユーザーに通知せず、参加者がオプトアウトする機会を与えずに、ソフトウェアの更新をインストールする。

ユーザーに通知せずに身元特定およびトラッキングのテクノロジーの性質を変更する。

ソフトウェアの更新に関連するプライバシーの取扱い変更について、ユーザーに通知しない。

参加者のメールのコンテンツをトラッキングする。

参加者のブラウザがプライベートモードに設定されている場合、オプトインの同意を得ずにトラッキング行為をする。

参加者がリンク先の安全性を保つよう設定されているサイト（SSL サイトなど）にいる場合、オプトインの同意を得ずに個人データを収集する。

8 参考文献

- ESOMAR データ保護チェックリスト
- ESOMAR / GRBN オンラインサンプルの質に関するガイドライン
- Global Research Business Network
- ICC / ESOMAR 市場および社会調査における国際行動規範
- ISO 20252:2012（市場・世論・社会調査）
- ISO 26362:2009（市場、世論及び社会調査におけるアクセスパネル）
- ISO 27001（情報セキュリティ）

9 プロジェクトチーム

- レグ・ベーカー（Reg Baker）、共同主催者、ESOMAR 職業基準委員会コンサルタント、Marketing Research Institute International
- ピーター・ミラ（Peter Milla）、共同主催者、CASRO 技術コンサルタント、Peter Milla Consulting
- マリオ・カレガロ（Mario Callegaro）、調査研究シニアサイエンティスト、Google
- メラニー・コートライト（Melanie Courtright）、エグゼクティブ・ヴァイス・プレジデント（グローバル・クライアント・サービス）、Research Now
- ブライアン・ファイン（Brian Fine）、会長、Quality Online Research
- フィリップ・ギルバール（Phillipe Guilbert）、ジェネラルディレクター、Toluna
- デブラ・ハーディング（Debrah Harding）、マネージングディレクター、Market Research Society
- キャシー・ジョー（Kathy Joe）、ディレクター（国際基準およびパブリックアフェアー）、ESOMAR
- ジャッキー・ローチ（Jackie Lorch）、ヴァイス・プレジデント（グローバルナレッジマネジメント）、SSI
- ブルーノ・パロ（Bruno Paro）、マネージングディレクター、Netquest
- エフライン・リベイロ（Efrain Ribeiro）、最高調査責任者、Lightspeed Research
- アリーナ・サーバニカ（Alina Serbanica）、シニア・ヴァイス・プレジデント（インタラクティブ・サービス）、Ipsos