人道支援における
データ保護ハンドブック

共同編集者：CHRISTOPHER KUNER、MASSIMO MARELLI

第二版

REFERENCE

VUB BRUSSELS PRIVACY HUB

COMITÉ INTERNATIONAL GENÈVE ICRC

人道支援における
データ保護ハンドブック

共同編集者：CHRISTOPHER KUNER、MASSIMO MARELLI

第二版

目次

謝辞

このハンドブックは、ベルギー・ブリュッセルにあるブリュッセル自由大学（VUB）の学術研究センターであるブリュッセル・プライバシー・ハブ(BPH）と、スイス・ジュネーブにある赤十字国際委員会（ICRC）データ保護室の共同発刊によるものである。

同ハンドブックは、VUBのChristopher KunerとICRCのMassimo Marelliが共同編集した。

諮問委員会と起草チームの構成は以下の通りである。

- Christopher Kuner、Júlia Zomignani Barboza、Lina Jasmontaite（VUB）
- Massimo Marelli、Vincent Graf Narbel、Sarah Dwidar、Luca Bettoni、Pierre Apraxine and Romain Bircher（ICRC）
- Catherine Lennman（スイスデータ保護局）
- Claire-Agnes Marnier、Olivier Matter、Petra Candellier（欧州データ保護監督官）
- Alexander Beck（国連難民高等弁務官事務所）
- Christina Vasala Kokkinaki（国際移住機関）
- Lucie Laplante、James De France（国際赤十字・赤新月社連盟）
- Stuart Campo（国連人道問題調整事務所）
- Nathaniel Raymond（イェール大学）
- Alexandrine Pirlot de Corbion（プライバシー・インターナショナル）
- Marine Revel（個人情報保護局フランス語圏協会）
- Carmela Troncoso（スイス連邦工科大学ローザンヌ校）
- Mary Nunn（国境なき医師団）
- Awa Ndiaye、Anna Thiam（セネガルデータ保護局）

ICTリーガル・コンサルティング社（https://www.ictlegalconsulting.com/?lang=en）がクラウドセキュリティに関する資料を使用することを許可してくれたこと、およびトライラテラル・リサーチ社（http://trilateralresearch.com/）がデータ保護影響評価に関する資料を使用することを許可してくれたことに感謝の意を表する。

このハンドブックの章が第三者による特定の貢献に頼っている場合には、関連する章の脚注においても謝意を表している。

序文

Jean-Philippe Walter（欧州評議会、データ保護担当委員、ICRC情報保護独立管理委員会メンバー）

赤十字国際委員会（ICRC）とブリュッセル・プライバシー・ハブ（BPH）の非常に実り多い協力の成果である「人道支援におけるデータ保護ハンドブック」を紹介できることを喜ばしく思う。

個人データの保護は、受益者の生命、高潔さ・誠実さ（インテグリティ）、尊厳を守るために不可欠な部分であり、人道団体にとって根本的な重要事項である。

2015年、第37回データ保護・プライバシーコミッショナー国際会議において、プライバシーと国際的な人道支援に関する決議を採択した。決議の目的の一つは、データ保護に関する指針を策定するための協力を求める人道支援関係者の要求に応えることであった。作業部会が設置され、BPHとICRCが共同で運営する「人道支援活動におけるデータ保護」プロジェクトに参加した。このプロジェクトの目的は、データ保護法と人道支援の関係を調査し、新しい技術が人道支援分野におけるデータ保護に与える影響を理解し、適切な指針を策定することであった。

このプロジェクトでは、人道団体、データ保護当局、技術専門家を集めて一連のワークショップを開催し、データ分析、ドローン、生体認証、現金給付プログラム、クラウドベースのコンピューティング、メッセージアプリなど、人道支援の分野でますます重要になっているさまざまなトピックを取り上げた。

本ハンドブックはこのプロジェクトの成果の一つである。意識を高め、人道団体が個人データ保護基準を遵守できるよう支援するための有用なツールとなるだろう。また、特に新技術が用いられる場合の、人道支援における適切なデータ保護原則の解釈に関する具体的なガイダンスの必要性についても言及している。本ハンドブックが、人道支援アクター、データ保護当局、民間企業のいずれにとっても有益となることを確信している。本ハンドブックでは、データ保護法が個人データの収集や共有を禁止しているのではなく、個人のプライバシーの権利が尊重されるという認識と確信の中で個人データを利用できる枠組みを提供していることを明確に示している。

Jean-Philippe Walterは、元スイス連邦データ保護コミッショナー副委員長であり、個人データ保護局のフランス語圏協会会長および、データ保護・プライバシーコミッショナー国際会議（現在のグローバル・プライバシー・アセンブリ）のプライバシーと国際的な人道支援に関する決議に関するワーキンググループのコーディネーターでもある。

定義された用語と略語の用語集

匿名化には、個人データを含むデータセットが完全かつ不可逆的に匿名化され、識別された、もしくは識別可能な自然人に関連しないこと、またはデータ主体が識別されていない、もしくは識別できないことを保証するために使用できる技術が含まれる。

人工知能とは「人間の認知能力を機械によって再現することを目的とする一連の科学、理論および技術」を指す。[1]現在の形では、「過去に人間に任されていた複雑なタスクを機械に委ねる」[2]ことを技術開発者に許可することを目的としている。

バイオメトリクスまたは生体認証とは、個人の生物学的および行動学的特性に基づいて個人を自動的に認識することである。

ブロックチェーンとは、「本質的には、追加専用の分散型データベースで、コンセンサスアルゴリズムによって維持され、複数のノード（コンピュータ）に保持される。」[3]

現金給付プログラム、現金・バウチャー援助、現金ベースの介入、現金ベースの援助は、人道援助をバウチャーまたは現金の形で提供することを表現するための人道支援分野の用語である。

CERT – Computer Emergency Response Team（コンピュータ緊急対応チーム）

CISO – Chief Information Security Officer（最高情報セキュリティ責任者）

クラウドサービスとは、一般的には「共有の構成可能なコンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービスなど）の集積に、どこからでも、簡単に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続またはサービスプロバイダとのやり取りで速やかに割当てられ提供されるもの」を指す。[4]

同意とは、自由意思により、特定事項について、十分な情報に基づいて示されるデータ主体の意思であり、それによってデータ主体は、自身に関連する個人データが処理されることへ同意する。

CSIRT – Computer Security Incident Response Team（コンピュータセキュリティインシデント対応チーム）

CSO – Chief Security Officer（最高セキュリティ責任者）

CTO – Chief Technology Officer（最高技術責任者）

1 欧州評議会（CoE）、人工知能用語集：https://www.coe.int/en/web/artificial-intelligence/glossary
2 CoE、人工知能用語集
3 フィンク、ブロックチェーンとEUにおけるデータ保護、4（1）*European Data Protection Law Review*（2018年）、p17：https://doi.org/10.21552/edpl/2018/1/6
4 US NIST SP 800-145、NISTによるクラウドコンピューティングの定義（2011年9月）：http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Anonymization encompassesを参照

データ分析とは、膨大な量の多様な情報源（ビッグデータ）を組み合わせ、高度なアルゴリズムを用いて分析し、意思決定を行うことを指す。

データ侵害とは、個人データの不正な改変、複製、違法な破壊、偶発的な損失、不適切な開示、不当な転送、または改ざんを意味する。

データ管理者とは、個人データの処理の目的および手段を単独または共同で決定する者または組織を指す。

データ処理者とは、データ管理者に代わって個人データを処理する者または組織を指す。

データ保護影響評価またはDPIAとは、プロジェクト、方針、プログラム、その他のイニシアチブから生じる個人データのリスクを特定、診断、対処する評価を意味する。

データ主体とは、特に個人データを参照することにより、直接または間接的に識別される自然人（すなわち個人）を意味する。

デジタルアイデンティティとは、「電子的に取得および格納されたアイデンティティ属性情報の集合であり、特定のコンテキストの中で個人を独自に表し、電子取引に使用される」。[5]

DPOとは、本ハンドブックの文脈においては、人道団体内部のデータ保護室またはデータ保護担当者を意味する。

ドローンとは、遠隔操作または自律的に動作する小型の航空装置または非航空装置をいう。無人航空機（UAV）または遠隔操縦航空機システム（RPAS）として知られている。

追加処理は、データが収集された当初に元々特定されていた目的を超えた個人データの追加的処理を意味する。

健康データとは、個人の身体的または精神的健康に関するデータであって、その個人の健康状態に関する情報を明らかにするものをいう。

人道支援とは、人道上の緊急事態に対応して、援助、救済および保護活動のために公平に実施されるあらゆる活動を意味する。人道支援には、「人道援助」、「人道支援活動」、「保護」が含まれる。

人道上の緊急事態とは、通常広範囲にわたり、地域社会またはその他の大規模な人々の健康、安全、治安または福祉に重大な脅威をもたらす事象または一連の事象（とりわけ武力紛争または自然災害から生じるもの）をいう。

人道団体とは、その使命や任務に従い、人道上の緊急事態の際に、人々の苦痛を軽減する援助を提供し、および／または生命および健康を保護し、人間の尊厳を維持する団体をいう。

5 GSMA, World Bank Group, & Security Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, 2016, p. 11: https://www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/

IaaSはInfrastructure as a Service（サービスとしてのインフラ）の略。

国際的なデータ共有には、個人データが当初収集または処理された国または国際機関の外で、同一の人道団体内の異なる組織または第三者に対して、電子手段、インターネットまたはその他の手段を介して、個人データを移転する、またはアクセス可能にする全ての行為を含む。

国際機関とは、国際公法に基づき運営される機関およびその下部組織、または二国以上の間の協定により、若しくはその協定に基づいて設立されるその他の機関をいう。

Know Your Customer（KYC）はマネーロンダリングや汚職に関する規制や法律を遵守するために、企業が顧客の本人確認をできるプロセスをいう。[6]

機械学習とは、人工知能の一種の形態であり、特定の作業を完了する際に、機械で判読可能なデータ形式で経験を積んで、その性能を向上させるアルゴリズムの研究と定義することができる。

PaaS – Platform as a Service（サービスとしてのプラットフォーム）

個人データとは、識別されたまたは識別可能な自然人に関する情報をいう。

処理とは、自動化された手段によるか否かを問わず、個人データまたは個人データの組み合わせに対して実行される操作または操作の組み合わせを意味する。データの収集、記録、組織化、構造化、保管、適合または変更、検索、参照、使用、送信による開示、普及またはその他の方法で利用可能にする、調整、結合または削除など。

仮名化とは、匿名化とは異なり、追加情報を使用することなく特定のデータ主体に個人データを帰属させることができなくなるような個人データの処理をいう。ただし、そのような追加情報は別個に保管され、個人データが識別されたまたは識別可能な自然人に帰属させられないようにするための技術的および組織的な措置の対象となることを条件とする。

SaaS – Software as a Service（サービスとしてのソフトウェア）

機微データとは、開示された場合に、関係する個人に対する差別または抑圧をもたらす可能性のある個人データを意味する。一般的に、健康、人種または民族、宗教的／政治的／武装集団への所属、遺伝学的および生体認証データに関連するデータは機微データとみなされる。機微データの範囲の中でもデータの種類によって（例えば、異なる種類の生体認証データ）機微のレベルが異なるが、全ての機微データには強化された保護が必要である。人道団体が活動する具体的な状況と、ある種のデータ要素が差別を引き起こす可能性があることを考えると、人道支援における機微データのカテゴリーの明確なリストを作成することは意味がない。データ

6 PWC, Know Your Customer: *Quick Reference Guide*: http://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html

の機微性と適切な保護措置（例えば技術的・組織的なセキュリティ対策）は、ケースバイケースで考慮されなければならない。

SLA（サービスレベル合意書）とは、特に信頼性の高い情報通信サービスとインターネットサービスを提供するための、サービス提供者とクライアント間の正式な取り決めである。

被調査者とは、追跡調査が開始された、行方不明の人物のことである。

サブプロセッサとは、データ処理者の代わりに個人データを処理することに従事している個人または組織をいう。

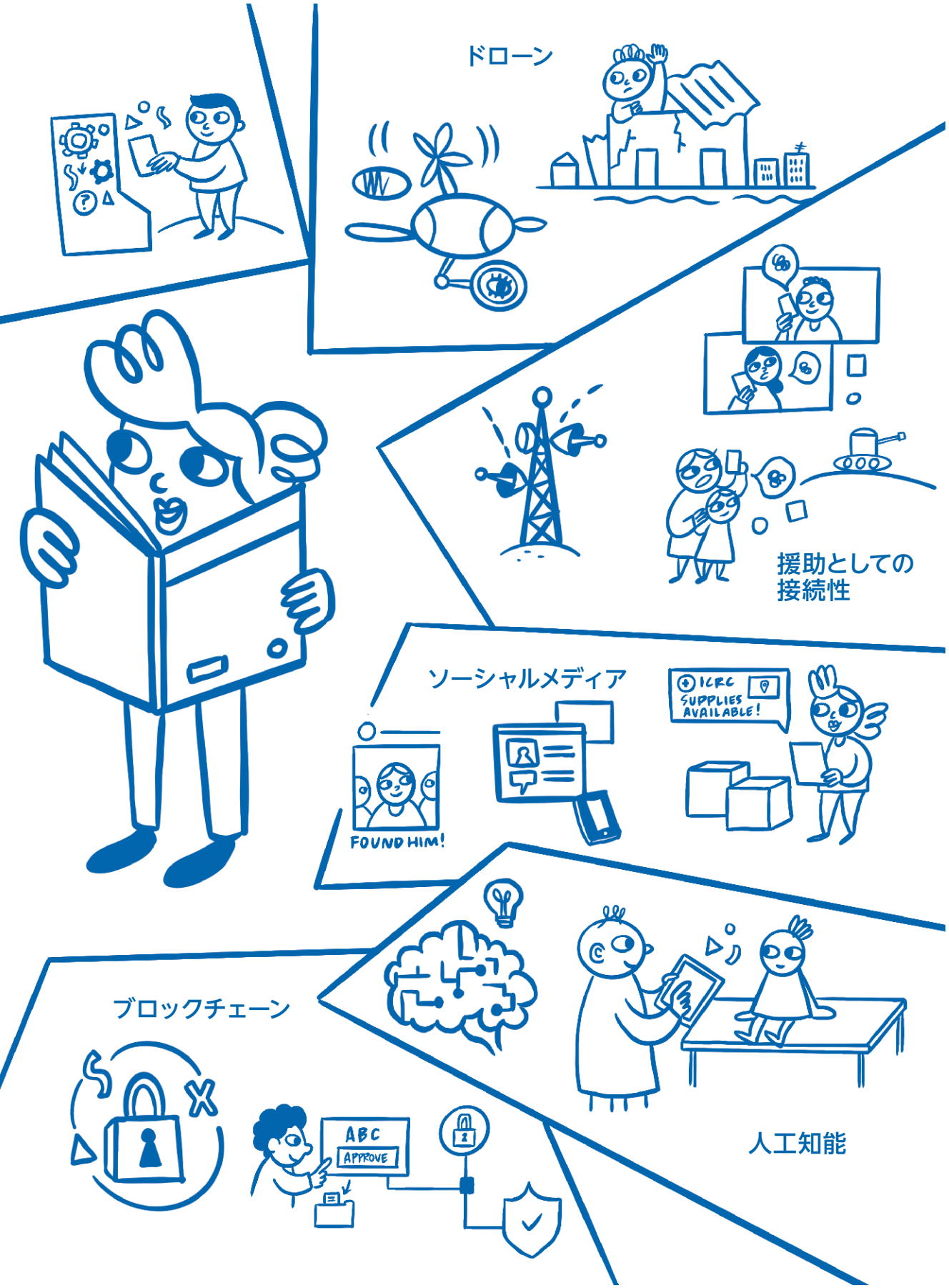
第三者とは、データ主体、データ管理者およびデータ処理者以外の自然人または法人、公的機関、代理人または、その他の団体をいう。

TLS（トランスポート・レイヤー・セキュリティ）は、インターネット接続の際にクライアントとサーバの間でプライバシーとデータ完全性を確保するための暗号化プロトコルのことである。

ICRC

VUB

BRUSSELS
PRIVACY
HUB


ドローン
援助としての
接続性
ソーシャルメディア
FOUND HIM!
ICRC
SUPPLIES
AVAILABLE!
ブロックチェーン
ABC
APPROVE
人工知能

第1章

はじめに

1.1 背景

各人の**個人データ**を保護することは、個人の生命、インテグリティ、尊厳を守るために不可欠である。これが、**個人データ**保護が**人道団体**にとって根本的に重要な理由である。

本ハンドブックは、**人道団体**がデータ保護原則をどのように適用すべきかを提案するにあたり、きわめて不安定な環境において、武力紛争、その他の暴力を伴う事態、自然災害、パンデミック、その他人道危機（これら全てを併せて「人道上の緊急事態」とする）による最も脆弱な被害者のための**人道支援**の中で確立されてきた、既存のガイドラインや作業手順、実践に基づき、作成されている。これらのガイドライン、手順および実践の中には、データ保護法が制定、発展する以前から存在しているものもあるが、全ては人間の尊厳の原則およびデータ保護法の根底にある保護の概念と同じ概念に基づいている。これらのガイドラインは、特に、「保護の任務のための専門的な基準」に設定されている。[7]

シリアのアル・バーブの町で、戦争で被害を受けた建物の前をオートバイが通り過ぎる様子（2017 年 3 月）

7 ICRC, *Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence*, 2nd ed., Geneva 2013: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights（参照：2020年3月）

近年新技術の開発により、インターネットで相互接続される世界において増え続ける**個人データ**を、より簡単かつ迅速に**処理**することが可能になった。これにより、個人の私的領域を侵害される可能性について、懸念が高まっている。これらの懸念に対応するため、世界中で規制の取り組みが進められている。

本ハンドブックは、ブリュッセル・プライバシー・ハブとICRCの**人道支援**におけるデータ保護プロジェクトの一環として出版されている。このプロジェクトは、ベルギーのブリュッセルにあるブリュッセル自由大学（VUB）の学術研究センターであるブリュッセル・プライバシー・ハブと、スイスのジュネーブにあるICRCデータ保護オフィスが共同で組織したものである。ハンドブックの内容は、2015～2016年にブリュッセルとジュネーブで開催された一連のワークショップにおいて作成された。ワークショップには、**人道団体**（人道支援専門家を含む）、データ保護当局、学術機関、非政府組織の代表者、研究者および特定のテーマに関するその他専門家が参加した。彼らは、特に新技術との関連において、**人道支援**の中でのデータ保護の適用における共通の関心事項について検討した。各種ワークショップの参加者は付録IIに記載されている。

1.2 目的

本ハンドブックは、2015年アムステルダムで開催されたデータ保護・プライバシーコミッショナー国際会議（ICDPPC）において採択された、プライバシーと国際的な**人道支援**に関する決議[8]に関連する議論をさらに進めることを目的としている。コンプライアンスを、適用可能な法的規範や、特定の組織が採用したデータ保護の規則、ポリシー、手順に置き換えることを意図したものではない。むしろ、本ハンドブックは、特に新しい技術が採用される場合に、**人道支援**の文脈におけるデータ保護原則の解釈について明確なガイダンスを提供することで、**人道団体**の意識を高め、人道援助活動を行う際、**個人データ**保護の基準に確実に準拠できるよう支援することを目指している。

本ハンドブックは、データ保護の原則および権利を人道支援の活動環境に取り入れるための支援を目的としている。ただし、一般的に**国際機関**と関連がある特権および免除の恩恵を受けていない**人道団体**に適用される場合には、データ保護に関する国内法の適用に関する助言を代替または提供するものではない。

8 データ保護・プライバシーコミッショナー国際会議、プライバシー及び国際的な人道支援に関する決議、オランダ・アムステルダム、2015年：https://edps.europa.eu/sites/edp/files/publication/15-10-27_resolution_privacy_humanitarian_action_en.pdf

個人データ保護の基準を遵守するためには、脆弱な個人の緊急かつ基本的なニーズに備え、人道支援の具体的な範囲および目的を考慮する必要がある。データ保護と**人道支援**は、相互に互換性があり、補完的であり、支援し合うものと見なされるべきである。したがって、データ保護が**人道団体**の活動を阻害しているとみなすべきではない。むしろ、彼らの活動に役立つはずである。同様に、データ保護の原則は、本質的な人道支援活動を妨げるような意味合いで解釈されるべきではなく、常に**人道支援**の究極の目的、すなわち人道上の緊急事態にさらされている被害者の生命、インテグリティ、尊厳の保護を促進するように解釈されるべきである。

本ハンドブックに含まれる提案やガイドラインは、特に以下の文書を含む、データ保護を扱う最も重要な国際文書に基づいている。

- 人道支援分野においてデータ保護原則を適用する際に特別の注意と柔軟性を求める人道的条項を含む*コンピュータ化された**個人データ**ファイルの規制に関するガイドライン*[9]を採択した、1990年12月14日の国連総会決議45/95[10]
- 国連**個人データ**の保護とプライバシーに関する原則。国連行政管理上級委員会（HLCM）により、第36回会合において2018年10月11日に採択[11]
- ***個人データ**・プライバシー保護に関する国際基準*（マドリード決議）。2009年マドリードで開催されたICDPPCで採択[12]
- *OECDプライバシーフレームワーク*（2013）[13]
- **個人データ**の自動処理に係る個人の保護に関する条約（欧州評議会条約第108）[14]、同条約を改正する議定書CETS第223号を含む（現在は条約第108号＋として知られている）[15]

9 国連総会、*コンピュータ化された個人データファイルの規制に関するガイドライン*、1990年12月14日：http://www.refworld.org/docid/3ddcafaac.html

10 国連総会決議45/95（1990年12月14日）、A/RES/45/95（1990年12月14日）

11 国連行政管理上級委員会（HLCM）、個人データの保護とプライバシーに関する国連原則、2018年12月18日：https://www.unsystem.org/personal-data-protection-and-privacy-principles

12 データ保護・プライバシーコミッショナー国際会議、*国際個人データ・プライバシー保護基準*：http://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf?mc_phishing_protection_id=28047-br1tehqdu81eaoar3q10

13 *OECDプライバシーフレームワーク*：https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

14 欧州評議会、個人データの自動処理に係る個人の保護に関する条約、1981年1月28日に署名開放、1985年10月1日に発効、ETS108：https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

15 欧州評議会、個人データの自動処理に係る個人の保護に関する条約を改正する議定書、2018年10月10日に署名開放、CETS 223：https://rm.coe.int/16808ac918

その他重要な基準も考慮されている。特に以下の基準がある。

- 近年の規制の進展。ただし、長年にわたる適用と新しい技術によって生じる課題に照らして、データ保護の概念と原則のさらなる進展が反映されている場合に限る（これには、条約第108号の改正及びEU一般データ保護規則2016/679（GDPR）[16]が含まれる。）。
- データ保護と大規模自然災害に関する決議[17]、2011年にメキシコシティでICDPPCにより採択
- プライバシー及び国際的な**人道支援**に関する決議[18]、2015年にアムステルダムでICDPPCにより採択
- ICRC *個人情報保護規則*（2015）[19]
- ICRC *保護の任務のための専門的な基準*（2013）[20]
- UNHCR、*UNHCR関係者個人情報保護方針*（2015）[21]
- *IOMデータ保護マニュアル*（2010）[22]

本ハンドブックは、**個人データ処理**のために推奨される最低基準を提供する。**人道団体**は、適切であると判断した場合、または国内、地域レベルでより厳しい法律の対象となる場合には、より厳格なデータ保護要件を規定することができる。

16 個人データの取扱いと関連する自然人の保護に関する、および、そのデータの自由な移動に関する、並びに、指令95/46/ECを廃止する欧州議会および理事会の2016年4月27日の規則（EU）2016/679（一般データ保護規則）、[2016] OJ L 119/1

17 データ保護・プライバシーコミッショナー国際会議、データ保護と大規模自然災害に関する決議：http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-Major-Natural-Disasters.pdf?mc_phishing_protection_id=28047-br1tehqdu81ea0ar3q10

18 データ保護・プライバシーコミッショナー国際会議、プライバシー及び国際的な人道支援に関する決議、オランダ・アムステルダム、2015年：http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf?mc_phishing_protection_id=28047-br1tehqdu81ea0ar3q10

19 ICRC、*個人情報保護規則*：https://www.icrc.org/en/who-we-are/the-governance/icrc-and-data-protection

20 ICRC, *Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence*, 2nd ed., Geneva, 2013）：https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

21 国連難民高等弁務官事務所（UNHCR）、*UNHCR関係者個人情報保護方針*（2015年5月）：https://www.refworld.org/docid/55643c1d4.html

22 国際移住機関（IOM）、*データ保護マニュアル*（2010）：https://publications.iom.int/books/iom-data-protection-manual

冒頭で、いくつかの重要な考慮事項を強調しておく必要がある。

- プライバシーの権利は、長い間、人権として世界的に認識されてきた[23]一方、**個人データ**保護の権利は、プライバシーの権利と密接に関連し、識別された、または識別可能な個人のデータの取扱い条件を定める、比較的新しい人権である。近年、100を超える明確なデータ保護法および規範が国および地域レベルで採用されている。[24] そして基本的権利としての**個人データ**保護は、世界中で広く受け入れられつつある。従って、**個人データ**保護基準の実装は、たとえ特定の**人道団体**が享受する特権および免責によってそれが法的義務でない場合であっても、その活動の主たる目的が個人の安全および尊厳のために働くことであることを考慮すると、全ての**人道団体**にとって優先事項であるべきである。
- 一部の**人道団体**は、特権および免責を享受し、国内法の適用を受けない**国際機関**である。それでもなお、多くの場合、プライバシー及びデータ保護規則の尊重は、他の事業体から**個人データ**を受け取るための必須条件である。
- **人道団体**が活動する緊急事態の例外的な状況は、データ保護に関して特別な課題を生み出している。したがって、人道支援の分野においてデータ保護原則を適用する際には、特別な注意と柔軟性が必要である。この必要性は、機密データの取扱いに関するより厳格な規則を含む上記の多くの国際文書および基準にも反映されている。[25]
- 故人の**個人データ**に関するデータ保護法に統一されたアプローチがないということは、**人道団体**がこの件に関して独自の方針を採用すべきであることを意味する（例えば、合理的な範囲内で、自然人の**個人データ**に適用される規則を故人に適用するなど）。管轄権からの免責を享受していない組織については、この問題は適用される法令によって規定される場合がある。
- 本ハンドブックの焦点は、**個人データ**の保護および法律のこの分野を人道支援に適用することにある。しかし、武力紛争やその他の暴力を伴う事態では、多くの脅威は個人的なものではなく集団的なものであり、村落、コミュニティ、特定の男女の集団が同じ脅威を共有している可能性がある。そのため**個人データ**の適切な管理のみに焦点を当てるのでは不十分な場合がある。場合によっては、**個人データ**以外のデータの**処理**が集団レベルで特定の脅威を引き起こすことがある。この点で、**人道支援**分野における多くのイニシアティブは、より一般的なデータ処理がコミュニティに及ぼす影響に焦点を当てており、例えば「人口統計学的に識別可能な情報」[26]、または「コミュニティ識別情報」と言及している。[27]

23 世界人権宣言第12条および市民的及び政治的権利に関する国際規約第17条を参照
24 国連貿易開発会議（UNCTAD）の報告書、*データ保護規制と国際データの流れ：貿易と発展への影響*（2016）：http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468を参照
25 セクション2.2: 基本的なデータ保護概念を参照
26 シグナルコード――危機下における情報への人権アプローチ：https://signalcode.org/を参照
27 人道データ共有プラットフォームの取り組み：https://data.humdata.org/about/termsを参照

- **人道団体**は、人道上の緊急事態における様々なカテゴリーの人々の個人データを処理する。例えば、受益者およびその活動に関与する連絡先データ、職員および物品・サービス提供者のデータ、さらには資金提供者のデータまでも含まれる。本ハンドブックでは、受益者の**個人データ**の取扱いに焦点を当てているが、他のカテゴリーの人々の**個人データ**の取扱いにも同様の考慮が適用される。

1.3 構成とアプローチ

本ハンドブックのPART Ⅰは一般的に、全ての種類の**個人データ処理**に適用される。PART Ⅱでは、特定のタイプのテクノロジーとデータ**処理**状況について取り上げており、関連するデータ保護の問題について、より具体的な議論も行う。PART Ⅱで概説されている特定の**処理**シナリオは、常にPART Ⅰを念頭に置いて読む必要がある。定義された用語は、このハンドブック全体で太字表記になっている。定義はハンドブックの冒頭にある用語集に含まれている。

1.4 ターゲットオーディエンス

このハンドブックは、所属する**人道団体**の人道援助のために**個人データ**の取扱いに携わる職員、特にデータ保護基準に関するアドバイスや適用を担当する職員を対象としている。また、人道支援やデータ保護に関与する、データ保護当局、民間企業などその他の団体、およびこれらの活動に関与するその他全ての人にとっても有用であることが示されるだろう。

第2章

データ保護の基本原則

2.1 はじめに

人道団体は、人道支援を実施するために、人道上の緊急事態の影響を受ける個人のデータを収集し処理する。人道団体は主に人道上の緊急事態下で、法の支配が完全にはなされていないかもしれない状況において活動している。そのような状況では、司法へのアクセスや国際人権の枠組みの尊重が仮に存在していても制限されるかもしれない。さらに、**個人データ**保護法は、未整備だったり存在しないか、完全には執行できない場合がある。

個人データ保護に関する各人の権利は絶対的な権利ではない。人間の尊厳の保護という全体的な目的との関連において考慮されるべきであり、比例性の原則に従って、他の基本的な権利および自由と衡量が図られるべきである。[28]

人道団体の活動は主に人道上の緊急事態において実施されるため、受益者および職員の**個人データ**の保護が彼らの安全、生命、活動を守るために必要とされる状況において展開されている。

J. Schneider/ICRC

コンゴ民主共和国、南キブ州ワールング。ICRC は 2016 年 12 月、避難民や地元の 1,750 世帯に食糧を提供した。

28 この文脈における比例性の原則は、国際人道法（IHL）の下での均衡性の原則と混同されるべきではない。ここで議論されている比例性の原則は、人道団体が、その任務を実行し、緊急時に活動する際に、データ保護および個人データへのアクセス権を制限する際にできる限り最小限の侵入的措置をとることを要求している。

したがって、**個人データ**保護と**人道支援**は相互補完的であり、互いに補強し合っている。しかし、様々な権利と自由の間のバランスをとる必要がある場合には、摩擦が生じることもある（例えば、表現および情報の自由とデータ保護の権利との間、または個人の自由および安全の権利とデータ保護の権利との間で生じる）。人権の枠組みは、ケースバイケースで様々な権利と自由のバランスをとることにより、すべての人権と基本的自由の尊重を確保することを目的としている。このアプローチは、しばしば、権利の目的論的解釈を必要とする。[29]すなわち、権利が果たす目的を優先させるものである。

例：
データ保護法は、**個人データ**の**処理**に関する基本情報を各個人に提供することを義務付けている。しかし、**人道上の緊急事態**においては、この権利と他の権利、特に影響を受けるすべての個人の権利とのバランスをとることが必要である。したがって、援助の分配を著しく妨害、遅延、阻止するような場合には、援助を受ける前にデータ収集の状況をすべての個人に知らせる必要はない。むしろ、関連する**人道団体**は、そのような情報を、より対象を絞らず個別化された方法で公示を用いるか、または、事後的に個別に提供することができる。

国際法の下で任務を与えられている**人道団体**の中には、その任務を遂行するために特定の作業手順に依存する必要があるものもある。国際法の下では、これらの任務は、**個人データ処理**において認められている原則および権利からの特例を正当化することができる。

例えば、データ保護の権利と、人道危機における関係者の歴史的・人道的説明責任を確保するという目的とのバランスを取ることが必要な場合がある。実際、人道上の緊急事態においては、**人道団体**が、将来の世代が歴史についての外部的な説明を保持し、被害者に発言権を与えることができる存在する唯一の外部組織である可能性がある。[30]さらに、**人道団体**からのデータは、武力紛争その他の暴力を伴う事態の被害者やその子孫を支援するためにも必要となる場合がある。例えば、被害者の身元および法的地位を文書化し、賠償請求を提出するなどである。特に人道上の緊急事態において他の記録がほとんど、または全く入手できないことを考慮すると、**人道団体**によるデータ保全は基本的に重要である。

29 1990年12月14日の国連総会決議45/95によって採択された、コンピュータ化された個人データファイルの規制のための国連ガイドラインの人道的条項に準ずる。

30 2007年11月15日、*ICRC WWI捕虜アーカイブがユネスコ世界記憶遺産に登録、以下を参照*
https://www.icrc.org/en/doc/resources/documents/feature/2007/ww1-feature-151107.htm

また**人道団体**にとって秘密保持が基本的に重要である可能性もある。不安定な環境の中での**人道支援**を継続するうえで、紛争当事者やその他の暴力を伴う事態に関与している人々による受け入れ、困窮している人々への接近、およびその職員の安全を確保するために欠かせない前提になる場合があるからである。これは、例えば、**データ主体**のアクセス権が行使される範囲に影響を与える可能性がある。[31]

以下のチェックリストは、本ハンドブックで詳細に説明されている、データが処理される目的に関連して、データ保護を扱う際に考慮すべき主要点を示したものである。

- **個人データ**が**処理**されているか。
- 処理されたデータによって個人が識別される可能性はあるか。
- **個人データ**とはみなされない情報であっても、保護する必要があるか。
- （該当する場合）地域のデータ保護およびプライバシーに関する法律に準拠しているか。
- どんな目的でデータが収集および処理されるか。目的に厳密に限定して**処理**されているか。その目的は、**データ主体**のプライバシーへの干渉を正当化するものであるか。
- **処理**の法的根拠は何か。データが公正かつ適法に処理されることをどのように保証するか。
- **個人データ**の**処理**は目的に比例しているか。同じ目的がより干渉度の小さい方法で達成できないか。
- **データ管理者**と**データ処理者**は誰か。両者はどのような関係か。
- データは正確で最新か。
- 可能な限り少ない量のデータが収集および処理されるか。
- **個人データ**はいつまで保管されるか。どのようにしてデータ**処理**の目的を達成するために必要な期間のみ保全されるのを確認するか。
- データを保護するための適切なセキュリティ対策が実施されているか。
- **個人データ**の**処理**に責任を負う担当者について、各個人に対して明確にされているか。
- **個人データ**がどのように**処理**され、誰と共有されるか、各個人に情報が提供されているか。
- **個人データ**の処理に関して、データ主体がその権利を主張できることを確保するための手続が整備されているか。

31 2007年11月15日、*ICRC WWI捕虜アーカイブがユネスコ世界記憶遺産*に登録 https://www.icrc.org/eng/resources/documents/feature/2007/ww1-feature-151107.htmを参照

- データを第三者と共有する必要はあるか。どのような状況の下で、個人データが第三者と共有され、または第三者がアクセスできるようになるのか。各個人はどのようにしてこのことを知らされるのか。
- **個人データ**が最初に収集または処理された国以外でアクセスできるようになるのか。そのための法的根拠は何か。
- プロジェクト、方針、プログラム、その他のイニシアチブから生じる**個人データ**のリスクを特定、審査、および対処するために**データ保護影響評価**が準備されているか。

2.2 基本的なデータ保護概念[32]

データ保護に関する法律および慣行においては、個人の権利を保護するため**データ主体の個人データの処理**を制限している。

処理とは、自動化された手段によるか否かを問わず、収集、記録、組織化、構造化、保管、適合または変更、検索、参照、使用、送信による開示、普及、またその他の利用可能化、調整、結合、または削除のような、**個人データ**または**個人データ**のセットに対して実行される操作または一連の操作を意味するものと解釈される。

個人データとは、識別された、または識別可能な自然人に関する情報をいう。**データ主体**とは、特に**個人データ**を参照することによって、直接的または間接的に識別できる自然人（すなわち個人）である。

データ保護法の中には、個人データの概念に**機微データ**というカテゴリーが追加されているものもある。本ハンドブックの目的上「**機微データ**」とは、開示された場合に個人に対する差別または抑圧をもたらす**個人データ**を意味する。一般的に、健康、人種や民族、宗教的/政治的/武装集団への所属、遺伝学的およびバイオメトリクスデータに関連するデータは機微データとみなされる。**機微データ**の範囲に含まれるデータの種類（例えば、異なるタイプのバイオメトリクスデータ）によって機微性のレベルが異なる場合があるが、すべての**機微データ**には強化された保護が必要である。**人道団体**が活動する特定の環境と、様々なデータ要素が差別を引き起こす可能性を考えると、**人道支援**のための**機微データ**の類型の最終的なリストを作成することは意味がない。例えば、状況によっては、リストに記載のある個人やその家族を迫害のリスクに晒すことがあれば、単なる名前のリストが**機微データ**となる。同様に、他の状況では、人道上の緊急事態に対応するために収集されたデータには、通常のデータ保護では機微データとみ

32 以下に定義される用語は、ハンドブックの冒頭の用語集にも示されている。

なされ、このようなデータの**処理**が原則として禁止されるようなデータを含んでいたとしても、地域の文化や特定の状況下では比較的無害である場合がある。したがって、データの機微性を考慮に入れて適切な**機微データ**保護（例えば技術的・組織的なセキュリティ対策）は、ケースバイケースで検討する必要がある。

個人データとはみなされないデータであっても、人道上の緊急事態においては、**処理**データは重大な危害を引き起こす可能性があることに留意することが重要である。したがって、**人道団体**は、特定の場合に個人にリスクが生じる場合には、本ハンドブックに記述されている保護を他の種類のデータにも適用する用意があるべきである。

例：
ある**人道団体**が、武器を用いた暴力の状況から逃れようとする人々の流れの中にいる個人の数を意図的ではないか明らかにし、これに関連する航空画像をオンラインで公開した。人々が避難する原因となっている暴力に関与した武装勢力の1人が、この情報を利用して避難民の居場所を突き止め、報復の対象とした。グループ内の個人の数および航空写真（解像度その他の要素によって個人の識別が可能であった場合）は、それ自体**個人データ**ではないが、特定の状況では非常に機微性が高くなる場合がある。この例では、**人道団体**はこのデータを保護するべきで、公開すべきでなかった。

また、**データ管理者**と**データ処理者**の違いを理解することも重要である。**データ管理者**は、**個人データ**の処理の目的や手段を、単独または共同で決定する個人や組織であり、**データ処理者**は、**データ管理者**に代わって**個人データ**を**処理**する個人や組織である。最後に、**第三者**とは、**データ主体**、**データ管理者**または**データ処理者**以外の、任意の自然人または法人、公的機関、代理人や団体である。

例：
ある国際**人道団体**は、**人道上の緊急事態**における個人の身元に関する情報を収集し、援助を提供している。そのためには、現地のNGOのサービスを利用して、元々**人道団体**が収集した身元情報を使用する必要がある。2つの組織はデータの使用を管理する契約に署名し、国際**人道団体**はNGOがデータをどのように使用するかを指示する権限を持ち、NGOは**人道団体**によって要求されているデータ保護措置を遵守することを約束する。NGOはまた、データが保存されているITシステムの定期的なメンテナンスを行うために、ITコンサルティング会社を雇っている。

上記の状況において、国際**人道団体**、NGOおよびITコンサルティング会社は、**データ主体**である各個人の**個人データ**を**処理**している。国際**人道団体**は**データ管理者**であり、NGOは**データ処理者**であり、ITコンサルティング会社は下位の処理者である。

2.3 集計化、仮名化、および匿名化されたデータセット

上述したように、集計データや統計データのような個人に関連しないデータ、または**データ主体**がもはや識別できないような方法で匿名化されたデータの取扱いは、本ハンドブックの範囲外である。

集計データが**個人データ**に由来し、特定の状況において関係者にリスクをもたらす可能性がある場合、そのようなデータの取扱い、共有、公表が個人の再識別につながらないことを確保することが重要である。[33]

個人データが集合体データセットや統計に使用される場合、**データ主体**からの特定の**同意**は必要ないが、**人道団体**は、そのようなデータ**処理**が別の正当な根拠を有することを保証すべきである。[34]また、個人またはグループを危害にさらしたり、彼らの保護を危うくしてはならない。

個人データの匿名化は、プライバシーに配慮した方法で、脆弱な個人の保護と支援のニーズを満たすのに役立つ。「**匿名化**」には、**個人データ**を匿名化するための技術を含む。データを匿名化する場合、**個人データ**を含むデータセットを完全かつ不可逆的に**匿名化**することが不可欠である。**匿名化**プロセスは、特に大規模データセットが広範囲の**個人データ**を含む場合は困難であり、個人の再識別に関して大きな危険度をもたらす可能性がある。[35]

33 英国の統計権威である*国家統計家のガイダンス：公式統計の機密性* https://www.statisticsauthority.gov.uk/archive/national-statistician/ns-reports--reviews-and-guidance/national-statistics-s-guidance/confidentiality-of-official-statistics.pdfを参照

34 第3章：個人データ処理の法的根拠を参照

35 英国個人情報保護監督機関発行*「匿名化：データ保護リスクの管理実施基準」*：https://ico.org.uk/media/1061/anonymisation-code.pdfを参照；併せて欧州連合第29条作業部会2014年5月による*「匿名化技術に関する意見書」*を参照：https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

「**仮名化**」は、**匿名化**と異なり、追加情報を使用しないと特定の**データ主体**に**個人データ**を帰属させることができなくなるような**個人データ**の取扱いを指す。ただし、かかる追加情報は別個に保管され、**個人データ**が識別されるか識別可能な自然人に帰属させられないことを確保するための技術的および組織的措置の対象となることが条件である。これには、データセット内のアナグラフィックな[36]データを数値で置き換えることが含まれる場合がある。名前の代わりに登録/識別番号を共有することは良い手段だが、**匿名化**とはいえない。

匿名データを共有または公表する前に、データセットに**個人データ**が含まれていないこと、および個人を再識別できないことを確認することが重要である。「再識別」とは、匿名化されたとされるデータを、データマッチング等の手法を用いて**個人データ**に変換する処理をいう。[37]再識別される可能性が高いと考えられる場合、その情報は**個人データ**とみなされ、本ハンドブックに定めるすべての原則とガイダンスに従うべきである。再識別のリスクを絶対的な確実性をもって評価することは非常に困難である。

集計データを共有または公開する前に、例えば、出身国、宗教、特定の脆弱性などのデータを対象者の地理的座標にマッピングすることによって、データセットが小規模でリスクの高いグループの実際の位置を明らかにしないようにすることが重要である。

2.4 準拠法および国際機関

人道支援には、**人道団体**、地方自治体、民間団体など多くの主体が関与している。**人道団体**に関しては、その活動を行う国の管轄下にある非政府組織（NGO）もあれば、国際法の下で諸国間の共同体から与えられた任務を完全に独立して遂行できる特権と免責が与えられている**国際機関**もある。

NGOに関する限り、適用可能なデータ保護法を決定するための規則は、多くの異なる事実の要素に依存する。このハンドブックは適用法の問題を扱っていない。この点に関する質問は、NGOの法務部門またはデータ保護室（**DPO**）に問い合わせる必要がある。[38]

36 https://en.wiktionary.org/wiki/anagraphic

37 「識別された」は必ずしも「名前がわかった」ことを意味しないことに注意すること。特定のデータと既知の個人との間に信頼性がある関係を確立することができれば十分である。

38 セクション1.2：目的参照

NGOに適用されるすべての法律に加えて、**個人データ処理**は、その内部のデータ保護ポリシーや規則、契約上の約束、およびその他関連する適用可能な規則によって管理されている。本ハンドブックに含まれる指針は、これらの規則および義務に関わらず常に適用されるべきである。このガイダンスは、周知のベスト・プラクティスと基準に基づいており、**国際機関**が**人道支援**のためのデータ保護ルールとポリシーを設計・解釈する際に、考慮に入れることが推奨される。

国際機関は、国際法の下で国際社会から与えられた任務を完全に独立して遂行することができ、かつ、活動する国の管轄に属しないことを確保する特権および免責を享受する。したがって、社内監視および自身のコンプライアンスシステムの実施を条件として、独自の規則に従って**個人データ**を処理することができる。この点において、独自の「管轄権」を構成する。**国際機関**のこの側面は、特に**国際的なデータ共有**に特有の意味合いを持っており、これについては第4章：国際的なデータ共有で詳細に論じる。

2.5 データ処理の原則

人道団体が実施する**個人データ処理**は、以下の原則に従うべきである。

2.5.1 公平性の原理と処理の適法性

個人データは、公正かつ適法に**処理**するべきである。第3章：個人データ処理の法的根拠に記載のとおり、**処理**の適法性を確保するためには、処理業務を行う上での法的根拠が必要である。公正な**処理**のもう一つの重要な要素は透明性である。

個人データの**処理**は、すべて関連する**データ主体**にとって透明性があるべきである。透明性の原則は、少なくとも**処理**に関する最小限の情報が、データ収集時に**データ主体**に提供されることである。ただし、現行の安全性や実務の状況、**処理**の緊急性があるかに依存する。**個人データ**の**処理**に関連する情報や通信は、容易にアクセスでき、理解しやすいものとすべきであり、必要に応じて翻訳を提供することを意味し、明瞭かつ平易な言語を使用すべきである。データ収集前または収集時に提供すべき情報提供の通知についてのより詳細な情報は、セクション2.10.2：情報通知に記載する。

2.5.2 目的制限の原則

人道団体は、データ収集時にデータの種類と処理される特定の目的を決定し、設定すべきである。特定の目的は、明確かつ正当であるべきである。特に、人道上の背景において関連する特定の目的には、例えば以下が含まれ得る。

- 生計を維持するため、被害にあった人々への人道援助やサービスの提供
- 人道上の緊急事態により離散した家族の再会
- 個々の違反行為の記録を含む、被害にあった人々の保護及び国際人権法/国際人道法（IHL）の尊重の構築
- 医療支援
- 国内制度への組み込みの確保（例えば難民のために）
- 例えば避難民や無国籍者への文書や法的地位/身元の提供
- 水と生計の保護

人道団体は、可能な限り透明性を保つために、緊急事態の状況下で可能な限り、意図されているすべての可能な目的、およびいかなる**追加処理**においても意図される可能性のある目的をデータ収集前に考慮し、特定するように注意を払うべきである。

2.5.3 比例原則

比例原則は、データ保護法の中核にある。これはデータ**処理**サイクル全体に適用可能であり、データ**処理**操作のさまざまな段階で適用されうる。**個人データ**の**処理**に関連する特定の行為や措置が、求められている目的に適切であるかどうかを考慮する必要がある（例えば、選択された正当な根拠は追求される目的に見合っているか。技術的および組織的措置が、**処理**に関連するリスクに見合うものか。）

人道団体によって取り扱われるデータは、それらが収集、処理される目的のために十分であり、関連性があり、かつ過度であってはならない。そのためには、特に（前もって決められた）目的を達成するために必要な**個人データ**のみを収集して追加処理した後、匿名化または消去するまでの保管期間を必要最小限にとどめることが必要である。[39]

39 セクション2.7：データ保全参照

比例原則は、**人道団体**が内部または組織間で実施する部門横断的なニーズ評価にとって特に重要である。これらの評価を実施する際、**人道団体**は目的を超える量のデータを収集しているリスクがある。例えば、後の段階で使用されるかわかっていない数百のデータフィールドを埋める調査を実施することなどである。このような状況では、受益者を支援するために、「知っておくと良いこと」と「知る必要があること」を区別できることが重要である。**人道団体**はまた、データの必要性と、収集されるデータが個人に及ぼす潜在的な被害や、「評価疲労」のリスクおよび支援を求めている人々の間に非現実的な期待を生じさせる可能性とを比較検討する必要がある。

収集するデータの量を制限することは、常に可能とは限らない。例えば、新たな**人道上の緊急事態**が発生した場合、データ収集時に人道上の必要性が十分に把握されていない可能性がある。したがって、この原則の適用は、**データ主体**の保護または他の者の権利および自由のために必要な場合、特例として限られた期間制限されることがある。

また、緊急事態によっては、収集時の目的が特に広い可能性もある。このような場合には、大量のデータの収集が必要と考えられる場合もあり、その後、状況によっては減らされる可能性もある。新たな**人道上の緊急事態**が発生した場合に、比例原則の柔軟な解釈が受け入れられるかどうかを検討する際には、以下の要因を考慮すべきである。

- 行動の緊急性
- 収集された**個人データ**の量と**人道支援**の目標の間の比例性
- 追加的な特定の目的が予見される場合、**データ主体**に対して追加的なデータを収集する際に（実務上またはセキュリティ上の制約により）起こり得る困難
- 対象となる**人道団体**の活動の目的
- 特定の目的を達成するために必要な**個人データ**の性質および範囲
- **データ主体**の期待
- 当該**個人データ**の機微性

例：
ある人道団体は、災害に脆弱な地域の人々の集団に人道支援を提供するために、**個人データ**を収集した。活動の最初の段階では、影響を受ける人々の具体的なニーズや、どのような支援やプログラムが直ちに、そしてさらにその先で必要になるかを決定することはできなかった（例えば、衛生施設の破壊は病気の蔓延のリスクを生む可能性がある）。したがって、当該**人道団体**は、影響を受ける人々のニーズを十分に評価し、対応プログラムを策定することを目的として、広範なデータ収集活動に従事した。緊急事態が収束した後、**人道支援**は必要であったが、衛生設備は病気の蔓延を防ぐのに間に合うよう復旧されたことが分かった。その結果、**人道団体**は、この特定の懸念に対処するために当初取得したデータを消去する必要があるかもしれない。

すべての場合において、収集されたデータを保持する必要性は、データ最小化の原則の適用を確保するために、定期的に見直されるべきである。

2.5.4 データ最小化の原則

データ最小化の原則は比例原則と密接に関連している。データ最小化は、データが収集された目的と用途を達成するために、最小限の個人データのみが処理されることを保証することを目的としている。データの最小化は、**個人データ処理**を必要最小限の量および範囲に制限することを要求する。**個人データ**は、当初の収集または適合する**追加処理**のために必要でなくなった場合は、消去されるべきである。また、**データ主体**が**処理**の**同意**を撤回した場合、または**処理**に正当に反対した場合にも、データは消去しなければならない。しかしながら、上記の状況においても、**個人データ**は、正当な歴史的、統計的若しくは科学的目的のために必要とされる場合、または**人道団体**が個人データを保持する適用可能な法的義務を負っている場合には、関連するリスクを考慮し、適切な保護措置を実施しつつ、保全することが許される。

データが収集された目的または適合する**追加処理**のためにもはや必要でないかどうかを判断するために、**人道団体**は以下を考慮すべきである。

- 指定された目的は達成されているか。
- そうでない場合でも、すべてのデータが必要か。指定された目的が達成されそうにないため、保全が意味をなさなくなっていないか。
- 不正確さが**個人データ**の品質に影響しているか。
- 更新や重要な変更によって、個人情報の記録が不要になっていないか。
- データは、正当な歴史的、統計的、または科学的目的のために必要か。関連リスクを考慮して保管を継続することは必要性に見合うものか。この保管には、適切なデータ保護措置が適用されているか。

- **データ主体**の状況は変化しているか、また、これらの新しい要因により、元の記録が古く無意味になっていないか。

2.5.5 データの質の原則

個人情報は、できる限り正確かつ最新のものでなければならない。不正確な**個人データ**は、遅滞なく消去または訂正されることを保証するために、あらゆる合理的な措置がとられるべきである。**人道団体**は、運用ガイドラインや手続に従い、収集された情報が信頼性があり、正確かつ最新であることを確認すべきである。

見直しの頻度を検討する際には、（i）実務上およびセキュリティ上の制約、（ii）**処理**の目的、および（iii）不正確なデータがもたらす潜在的影響を考慮に入れるべきである。潜在的に誤ったデータに基づいて人道的プログラムから個人を除外するなど、個人に不利益となりうる決定を下す可能性を最小限に抑えるために、あらゆる合理的な措置を講じるべきである。

2.6 特殊なデータ処理の状況

次に、より具体的な説明を必要とする一般的なデータ**処理**状況を以下に示す。

2.6.1 保健目的

健康データの不適切な取り扱い（開示を含む）は、関係者に重大な損害を与える可能性がある。したがって、**健康データ**は特に機微性が高いであると考えられるべきであり、そのようなデータを処理する際には特別な保証が実施されるべきである。これは**機微データ**にも適用される。**健康データ**もサイバー攻撃の標的になりつつある。人道的医療提供者は、WMA医の国際倫理綱領[40]に従ってデータを処理すべきである。これには特定の職業上の守秘義務が含まれている。

人道団体は、以下のような目的のために**健康データ**を処理することができる。

- 予防医学または職業医学、医学的診断、看護または治療の提供
- 医療サービスの管理
- **データ主体**に不可欠かつ救命的な医療援助を提供することを含め、命に係わる理由
- 公衆衛生（例えば、健康に対する深刻な脅威からの保護、または高水準の品質および安全性の確保とりわけ医薬品や医療機器の場合）

40 世界医師会、*医の国際倫理綱領*：https://www.wma.net/policies-post/wma-international-code-of-medical-ethics/

- 歴史的、統計的または科学的研究目的。例えば診断を改善し、類似したタイプの疾患を区別し、治療のための研究を準備するために、条件や保護措置を前提として設定された患者登録など

健康データは、他の**個人データ**とは別に保持されるべきである。そしてアクセス可能なのは、医療提供者や人道的な医療提供者によって特に委任された職員と研究職員のみであり、前者の場合、職員は、雇用、コンサルタントその他の契約によって保証される守秘義務の下で事前定義された**健康データ**管理目的のみのためにアクセス可能であるべきであり、後者の場合、研究職員は、雇用、コンサルタントまたは他の契約によって保証される守秘義務および他のデータ保護の保証の下で研究を行う職員であって、事前定義された研究目的のみのためにアクセス可能であるべきである。

保護または支援活動に従事する**人道団体**は、例えば、行方不明者（識別し追跡するために**健康データ**が必要とされる場合）の所在を突き止めたり、自由を奪われた個人の適切な処遇を提唱したり、特に脆弱な受益者層（栄養失調や特定の病気にかかっている人々）のニーズに対処する生計プログラムを確立するために必要な場合には、**健康データ**を処理することができる。[41]

南スーダン・ジョングレイ州。戦争による負傷者を医療チームが避難させた。

41 セクション2.6.3：追加処理参照

2.6.2 管理活動

人道団体は通常、雇用目的、キャリア管理、評価、ダイレクトマーケティング、およびその他の管理上の要件のために**個人データ**を**処理**する。これには、例えばフリートおよびセキュリティ管理のための車両のGPS追跡などの機微データ処理活動も含まれることがある。業務の状況によっては、職員の**個人データ**の取扱いは、例えば特定の人道支援が提供される地政学的状況により、特に取り扱いに留意する必要がある場合がある。このような場合には、こうしたデータの取扱いにおいて可能な範囲で追加的な保護措置が必要となる。

2.6.3 追加処理

人道団体は、**追加処理**が当初の目的に適合する場合は、収集時に当初指定された目的以外の目的のために**個人データ**を**処理**することができる。これには、**処理**が歴史的、統計的、科学的目的のために必要な場合を含む。

追加処理の目的がデータが最初に収集された目的に適合するか否かを確認するために、次の事項を考慮すべきである。

- 最初の目的と意図された追加的取扱いの目的の間の関連性
- データが収集された状況（今後の使用に関する**データ主体**の合理的な期待を含む）
- **個人データ**の性質
- 意図された**追加処理**が**データ主体**に与える影響
- 適切な保護措置
- そのような保護措置が**個人データ**の機密性と**データ主体**の匿名性をどれだけ保護できるか

データが収集される状況は、追加の使用に関して**データ主体**が合理的に期待していることも含めて重要な要因である。特に、**データ主体**がある目的のためにデータを提供する場合、付帯する人道活動も含まれることを一般的に理解しており、実際、可能な限りの人道的保護や援助まで拡大されることを期待している可能性がある。これは、人道的状況において特に重要である。なぜなら適合性についての理解が不適切に狭いと**データ主体**への人道的利益の提供を妨げる可能性があるからである。

したがって、**人道支援**に密接に関連する目的であって、当初の目的を考慮して予見できなかった追加的なリスクを伴わないものは、相互に適合する可能性が高く、これが確認された場合には、**人道団体**は、当該**個人データ**が当初収集された特定の目的を超えて、当該**個人データ**を合法的に**処理**することができる。この場合、**人道団体**は**人道支援**の枠組みの中で**追加処理**を実施することを前提とする。原則として、**人道支援**において、影響を受けた人々の治安や、生命、インテグリティ、健康、尊厳、安全などを保護するために必要かつ相応な場合には、追加処

理が許容されるべきである。これはケースバイケースの評価を必要とし、一律にみなすことはできない。

追加処理の目的が専ら**人道支援**に関連する場合であっても、**データ主体**に対するリスクが**追加処理**の利益を上回る場合、または**追加処理**が新たなリスクを伴う場合には、新たな目的のための処理は適合性があるとはみなされないことがある。この分析は事の状況に依存する。この結論に至る状況には、処理がその情報の関係者またはその家族の利益に反するリスク、特に、その生命、インテグリティ、尊厳、心理的、または物理的安全、自由、名誉を脅かすおそれのあるリスクが含まれる。これには、次のような結果が含まれる。

- 当局または第三者による嫌がらせ、または迫害
- 司法訴追
- 社会問題
- 深刻な心理的苦痛

追加処理が適合しないと考えられる状況の例としては、**個人データ**が手配者の追跡を支援するために必要な情報の一部として収集された場合が含まれる。関係当局が適用法令違反の可能性について調査を実施するために（例えば、民間人保護活動の観点から）、この情報をさらに処理することは、**追加処理**に適合しない場合がある。これは、意図された**追加処理**が**データ主体**に有害な影響をもたらす可能性と、適切な保護措置を提供することが困難と想定されることによるものである。

追加処理の意図された目的が、データが最初に収集された目的と両立しない場合には、別の法的根拠に基づいてそうすることが適切とみなされる場合を除き、そのデータはそれ以上の処理をしてはならない。この場合、適用される根拠に応じて追加の措置が必要となることがある。[42]

また、**個人データ**の**追加処理**が、法律上、職業上またはその他の拘束力のある守秘義務、または「害を及ぼさない」原則と抵触する場合には、適合性があるとみなされるべきではない。

データ集約および**匿名化**は、データの機微性を低下させる方法として使用することができ、補助的なケースのためのデータ使用を可能にする。

42 第3章：個人データ処理の法的根拠を参照

例：
人道支援活動中に食料と住居を提供するために収集されたデータは、避難民に対する医療サービスの提供を計画するためにも使用される。しかし、**人道団体**の次年度予算の必要性を計画するために、収集されたデータ（集約/匿名化されていない場合）を**処理**することは、**追加処理**に適合するとはみなされない。

2.7 データ保全

データはそのカテゴリーごとに、定められた期間（例：3か月、1年など）保存されるべきである。収集時にデータの保管期間を決定できない場合は、初期保全期間を設定する必要がある。最初の保全期間の後、データを消去すべきか、データが最初に収集された目的（あるいはさらに正当な目的）を満たすためにまだ必要かどうかについて評価を行うべきである。その場合、初期保全期間を一定期間更新する必要がある。

データが消去された場合、データのすべてのコピーも消去する必要がある。データが第三者と共有されている場合、**人道団体**は、そのような第三者もデータを消去することを確認するための合理的な措置をとるべきである。この考慮は、データを第三者と共有するかどうかについての最初の検討において考慮されるべきであり、いかなるデータ共有協定においても表明されるべきである。[43]

2.8 データセキュリティと処理のセキュリティ

2.8.1 はじめに

データセキュリティは、効果的なデータ保護システムの重要な要素である。**個人データ**は、個人データやその処理に使用される機器への不正なアクセスや使用を防止するなど、**個人データ**の適切なセキュリティを確保する方法で処理されるべきである。このことは、**人道団体**がしばしば活動する不安定な環境の場合にはさらに重要である。

個人データへのアクセス権を有する**データ管理者**の権限の下で行動する者は、本ハンドブックに説明されている適用可能な方針に従う方法以外で、そうしたデータを処理してはならない。

43 セクション2.12：データ共有と国際的なデータ共有および第4章：国際的なデータ共有を参照

セキュリティを維持するために、データ管理者は、**処理**にあたって特定のリスクを評価し、それらのリスクを軽減するための措置を実施すべきである。これらの措置は、保護される**個人データ**の性質および関連するリスクに関連して、適切なレベルのセキュリティを（利用可能な技術、現行の安全保障および後方支援の条件並びに実施の費用を考慮して）確保すべきである。これには、次のような措置が含まれる。

- スタッフ、パートナーの研修
- **個人データ**を含むデータベースへのアクセス権の管理
- データベースの物理的セキュリティ（入退室規制、水や温度による損害等）
- ITセキュリティ（パスワード保護、データの安全な転送、暗号化、定期的なバックアップなど）
- 裁量条項
- パートナーおよび第三者とのデータ共有契約
- **個人データ**の廃棄方法
- データ管理および保持に関する標準的な運用手順
- その他の適切な措置

これらの措置は、**個人データ**が技術的にも組織的にも安全に保持されること、また悪用、不正な改変、複製、改ざん、違法な破壊、偶発的な喪失、不適切な開示または不当な移転（集合的に、「**データ侵害**」）に対して、合理的かつ適切な措置によって保護されることを保証することを目的としている。データセキュリティ対策は、特に、以下を考慮すべきである：

- 操作の種類
- 評価されたデータ保護リスクのレベル
- 関連する**個人データ**の性質および機微性
- データの保存、転送、共有の形式
- 特定の**個人データ**の環境/場所
- 一般的な安全と物流の条件

個人データに適用される機微性の程度に適切なレベルのデータ保護を確保するために、また強化されたセキュリティを可能にする新しい技術の開発を検討するために、データセキュリティ対策は、定期的にレビューされ、改善されるべきである。

データ管理者は以下に責任がある。

- 情報セキュリティマネジメントシステムの構築。これには、国際的に認められた基準および危険度の評価に基づいて、データセキュリティポリシーを確立し、定期的に更新することが含まれる。ポリシーは、例えば、物理的セキュリティのガイドライン、ITセキュリティポリシー、Eメールセキュリティのガイドライン、IT機器の使用のガイドライン、情報の分類のためのガイドライン（すなわち、情報を公開情報、内部情報、機密情報、極秘情報に分類する）、危機管理計画、および文書破棄のガイドラインで構成されるべきである。

- データの機密性、完全性および可用性を保持するために、セキュリティポリシーに従って通信インフラおよびデータベースを開発する。
- **データ管理者**の情報システムで処理されるデータのセキュリティを保護するためのあらゆる適切な措置を講じる。
- **個人データ**を含むデータベースへのアクセス権の付与および管理（必要最小限のアクセス権を付与することを含む）。
- 認可された人員がシステムにアクセスできるようにする、施設のセキュリティ。
- データへのアクセスを許可された担当者が、セキュリティルールを十分に尊重する立場にあることを保証する。これには、データベースへのアクセスが許可される前に署名される雇用契約における関連する訓練、裁量の誓約および/または守秘義務条項が含まれる。
- 各データベースにアクセスできる担当者の登録簿を維持し、必要に応じて更新する（例えば、もはやアクセスを必要としない異なる責任を与えられた担当者）。
- 可能であれば、データベースにアクセスした担当者が処理したデータがデータベースに存在する限り、監査を実行する可能性も含めて、履歴ログを保持する。

担当者は、付与された処理権限の範囲内でデータを**処理**する必要がある。より高いアクセス権を有する担当者またはアクセス権の管理に責任を有する者は、守秘義務および非開示の追加的な契約上の義務の対象となることがある。

2.8.2 物理的セキュリティ

各**データ管理者**は、以下に責任がある。

- 特定された一般的なリスクに基づいて、適切なレベルの機密性、物理的な完全性、およびデータベース（物理ベースかITベースか）の可用性を確保するための手順、技術、および管理上のセキュリティコントロールを定義するセキュリティルールの策定
- セキュリティルールの周知と遵守の徹底
- データのセキュリティを確実に維持するための適切な制御メカニズムの開発
- 適切な電気および火災安全基準が保管場所に適用されることを確実にする
- 保管量が必要最小限に保たれるようにする

2.8.3 IT セキュリティ

データ管理者は、以下に責任がある。

- 危険度の評価に基づいて、使用される情報システムの機密性、完全性、可用性の適切なレベルを保証するため、手続上、技術上、管理上のコントロールを定義するセキュリティルールの策定
- データセキュリティを維持するための適切な制御メカニズムの開発
- 特に機微性の高い、または重要な**個人データ**が処理されている場合など、必要に応じた、IT 通信インフラストラクチャの一部、データベース、または特定の部門に特定のセキュリティルールの導入

個人データを含む社内外のすべての電子メール通信は、知る必要に応じて処理されるべきである。電子メール通信の受信者は、その役割上**個人データ**を必要としない個人に対する不必要な個人データの拡散を回避するために、慎重に選択されるべきである。**個人データ**の転送に、私的な電子メールアカウントを使用すべきではない。

サーバへのリモートアクセスおよび自宅のコンピュータの使用は、**データ管理者**の IT セキュリティポリシーに規定された基準に準拠する必要がある。運用上の理由から絶対に必要な場合を除き、**個人データ**を取得、交換、送信、または転送するためにインターネット接続やセキュリティで保護されていないワイヤレス接続を使用することは避けるべきである。

個人データを取り扱うスタッフは、**データ管理者**のサーバにリモート接続する際には十分な注意を払う必要がある。パスワードは常に保護され、定期的に変更され、「キーチェーン」機能による自動入力ができないようにする。[44]スタッフは、コンピュータシステムから適切にログオフしていること、および開いているブラウザが閉じていることを確認する必要がある。

困難な環境で作業する場合は、特に、ノートパソコン、スマートフォン、およびその他のポータブルメディア機器を保護することを特に考慮する必要がある。ポータブルメディア機器は、常に安全で安全な場所に保管する必要がある。

機密な個人データを含む文書は、ポータブルデバイスやリムーバブルデバイスに保管すべきではない。これが避けられない場合は、**個人データ**を適切なコンピュータシステムおよびデータベースアプリケーションにできる限り早く転送する必要がある。USB フラッシュドライブやメモリカードなどのフラッシュメモリを一時的に**個人データ**保管に使用する場合は、安全に保管し、電子記録を暗号化する必要がある。情報が適切に格納された後には、その情報がポータブルデバイスで不要になった場合、ポータブルデバイスまたはリムーバブルデバイス内の情報は、消去すべきである。

44 キーチェーンまたはパスワードマネージャーとは、ユーザーが複数のパスワードを一つのマスター・パスワードにまとめて管理できるようにするアプリケーションやハードウェアの機能である。

効果的な復旧メカニズムとバックアップ手順は、すべての電子記録を対象とすべきであり、関連する情報通信技術（ICT）担当官は、バックアップ手順が定期的に実行されることを確認すべきである。バックアップ手順の頻度は、**個人データ**の機微性と利用可能な技術リソースに応じて異なる。電子記録は自動化して、とりわけ定期的な停電、システム障害、災害などによってバックアップ手順が困難な状況でも容易に復旧できるようにする必要がある。

電子記録およびデータベースアプリケーションが必要とされなくなった場合、**データ管理者**は担当の情報通信担当官と調整し、それらの永久的な消去を確実にするべきである。

2.8.4 配慮義務および職員の行動

配慮義務は、個人情報セキュリティの主要要素である。これには以下が含まれる：

- 雇用/コンサルティング契約の一部として配慮および秘密保持契約や条項に署名するすべての担当者および外部コンサルタント。この要件は、担当者が**データ管理者**の指示に従ってのみデータを処理するという要件を伴う。
- 秘密保持条項に拘束されている外部**データ処理者**。この要件は、**データ処理者**が**データ管理者**の指示に従ってのみデータを処理するという要件を伴う。
- 情報の機密性に基づいた、情報分類ガイドラインの厳密な適用。
- **データ主体**の要請が適切に対処され、**データ主体**のファイルに安全かつ機密な方法で正確に記録されること、またそのような要請が第三者と共有されないことを保証すること。
- 機密情報源からのデータの収集と管理を担当する権限を与えられた担当者のみがアクセスできるようにすることで漏洩リスクを制限すること、該当する情報分類ガイドラインに従って、これらの担当者が該当する文書にアクセスできるのを保証すること。

担当者は、該当する情報分類のガイドラインに基づいて、自分が**処理**するデータに機密性のレベルを付与すること、および外部処理目的のために参照、送信、使用するデータの機密性に留意することに責任を負う。当初機密性のレベルを付与した担当者は、必要に応じて、自分がデータに付与した機密性のレベルをいつでも変更することができる。

2.8.5 緊急時対応計画

データ管理者は緊急時に、記録を保護、退避、または安全に破棄するための計画を立案し、実施する責任を負う。

2.8.6 破壊方法

個人データの保管が不要になったことが判明した場合は、すべての記録およびバックアップを安全に破棄するか、または匿名化する必要がある。廃棄の方法は、とりわけ次の要素に依存する。

- **個人データ**の性質と機微性
- フォーマットと保管媒体
- 電子記録と紙の記録の量

管理者は、**個人データ**廃棄の際に適切な破壊方法が使用されることを確実にするため、破壊の前に機密性評価を実施すべきである。この点に関して、次の三項はIOMデータ保護マニュアルの情報に基づいたものである。[45]

紙の記録は、シュレッダーや焼却など、将来の使用や再構築ができないような方法で破棄すべきである。紙の記録をデジタル記録に変換する必要があると判断された場合は、電子形式に正確に変換した後、紙の記録の保存が適用される国内法で要求されている場合や紙のコピーをアーカイブ目的で保存する必要がある場合を除き、紙の記録のすべての痕跡を破棄する必要がある。大量の紙記録の破棄は、専門企業に委託することができる。そのような状況において、**データ管理者**は、その監督下にあるすべての工程で、**個人データ**の機密性、廃棄記録の提出、廃棄証明が**データ処理者**の契約上の義務の一部を構成すること、および**データ処理者**がこれらの義務を遵守することを確認すべきである。

コンピュータ・システム上の削除機能は必ずしも完全な抹消を保証するものではないため、電子記録の破棄については、関連するICT担当者に問い合わせるべきである。指示に基づき、該当するICT担当者は、**個人データ**の痕跡がコンピュータシステムおよびその他のソフトウェアから完全に取り除かれていることを確認しなければならない。ディスクドライブとデータベースアプリケーションはパージする必要がある。また、特に**個人データ**の保管に使用されたCD、DVD、マイクロフィッシュ、ビデオテープ、オーディオテープなどのすべての書き換え可能なメディアは、再使用する前に削除する必要がある。リサイクル、粉砕、焼却など、電子記録を破壊する物理的手段は、厳格に監視されるべきである。

45 国際移住機関（IOM）、*データ保護マニュアル*、2010、pp.83–84：https://publications.iom.int/books/iom-data-protection-manual

データ管理者は、関連するすべてのサービス契約、覚書（MOU）、契約、書面による譲渡または**処理**契約に、特定の目的の達成後に**個人データ**を破棄するための保全期間が含まれていることを確認すべきである。第三者は、**個人データ**を**データ管理者**に返却し、許可された代理人および下請業者に開示された**個人データ**を含め、**個人データ**のすべてのコピーが破棄されたことを証明しなければならない。廃棄の時間と方法、および廃棄された記録の性質を示す廃棄記録は、維持管理され、プロジェクトや評価報告書に添付されるべきである。

2.8.7 その他の措置

データセキュリティには組織内部での適切な措置も必要である。これにはデータセキュリティ規則と、データ保護法で規定されている義務、または特権と免責が与えられている企業の内部規則によって規定されている義務（特に職員の守秘義務）を、すべての職員に定期的に内部普及することが含まれる。

各**データ管理者**は、セキュリティ業務を実施するために、データセキュリティ責任者の役割をその職員（おそらく管理者/IT担当者）の一人以上の者に割り当てるべきである。セキュリティ担当官は、特に以下を行うべきである。

- 適用されるセキュリティ手順と規則への遵守を保証する
- 必要に応じて、これらの手順を更新する
- 担当者のデータセキュリティに関する研修を実施する

2.9 説明責任の原則

説明責任の原則は、上記の原則に準拠するという**データ管理者**の責任と、データ管理者が準拠を確認するためにそれぞれの組織内で適切かつ相応な措置が取られたことを示す立場にあるという要件を前提としている。

これには、**人道団体**がデータ保護要件を満たすために強く推奨される次のような措置が含まれる。

- **個人データ処理**ポリシー（**処理**のセキュリティポリシーを含む）の策定
- データ**処理**アクティビティの内部記録の保持
- データ保護室など、適用されるデータ保護ルールの実施を監督する独立した機関を設立し、データ保護オフィサー（**DPO**）を任命する
- 全職員に対するデータ保護に係る研修プログラムの実施
- **データ保護影響評価**（DPIA）の実行[46]
- 法的に要求され、かつ「害を及ぼさない（Do No Harm）」という原則と相反しない場合には、所管官庁（データ保護当局を含む）に登録すること

46 第5章：データ保護影響評価（DPIAS）を参照

2.10 情報

透明性の原則に従い、**個人データ処理**に関する情報を**データ主体**に提供すべきである。原則として、この情報は**個人データ**が処理される前に提供されるべきだが、個人に緊急支援を提供する必要がある場合には、その限りではない場合がある。

データ主体は、口頭か文書により情報を提供されるべきである。これは、状況が許す限り透明性を保ち、可能であればデータ主体に直接行われるべきである。それが不可能な場合には、**人道団体**は、他の手段によって情報を提供することを検討すべきである。例えば、情報をオンラインで、又、容易にアクセスできる場所および形態（公共の場所、市場、礼拝所および/または機関の事務所）で表示されるチラシまたはポスター、無線通信、地域社会の代表者との議論において利用可能にすることなどである。**データ主体**は、実行可能な限り、自己のためにとられた措置に関連する**個人データ**の**処理**およびその後の結果について常に知らされるべきである。

提供される情報は、データが**データ主体**から直接収集されるか否かによって異なることがある。

2.10.1 データ主体から収集されたデータ

個人データは、以下の法的根拠に基づき、**データ主体**から直接収集することができる。[47]

- **データ主体**または他の者の重要な利益
- 公益
- 個別**同意**
- **人道団体**の正当な利益
- 法的または契約上の義務

上記の各ケースにおいて**データ主体**に提供されるべき情報のいくつかは、特定の状況に応じて異なる。この点での優先事項は、提供される情報が、データ保護の権利を効果的に行使するために十分なものでなければならないことである。[48]

47 第3章：個人データ処理の法的根拠を参照
48 セクション2.11：データ主体の権利を参照

2.10.2 情報通知

同意が法的根拠として使用される可能性がある特定の場合[49]データ主体は、データ**処理**のリスクと便益を十分に評価できる立場に置かれなければならない。そうでなければ、**同意**は有効とはみなされない可能性がある。

同意書を使用する場合、または**データ主体**が**処理**に異議を申し立てる権利やデータにアクセス、訂正および削除する権利を行使する場合、詳細な情報を提供する必要がある。**データ主体**は、いつでも**処理**に異議を申し立て、またはその**同意**を撤回することができることに留意することが重要である。**同意**が法的根拠である場合に提供される情報のタイプは次のとおりである。

- **データ管理者**のIDと連絡先の詳細
- **個人データ**の**処理**の具体的な目的並びに潜在的なリスクおよび便益の説明
- **データ管理者**が、収集時に最初に指定した目的以外の目的で**個人データ**を処理することができること。ただし上記の特定の目的と適合する場合に限り、その更なる適合した目的の提示
- **同意**をしたときはいつでもこれを撤回することができること
- **個人データ**を機密に取り扱うことができない場合がある状況
- **データ主体**の、**処理**に対する異議申立、**個人データ**へのアクセス、訂正および消去の権利。当該権利の行使の方法および行使の制限
- **データ管理者**が最初の収集時や**追加処理**の際の目的を達成するためにデータを転送する必要があるかもしれない第三国または**国際機関**
- **個人データ**が保管される期間、または少なくともそれを決定するための基準、および記録が正確で最新の状態に保たれることを保証するために取られるあらゆる措置
- データ収集国の当局等、**個人データ**を共有する可能性のある他の組織
- 自動**処理**に基づいて決定が行われる場合は、関連する論理回路に関する情報
- データ**処理**に関して**データ管理者**によって実施されるセキュリティ対策の提示

処理に関する他の法的根拠の下では、リスク分析を実施する責任は**データ管理者**にあり、より基本的な情報を提供すれば十分である。**同意**以外の法的根拠の場合に提供すべき最低限の情報として、以下を推奨する。

- **データ管理者**のIDと連絡先の詳細
- **個人データ**の**処理**の具体的な目的
- **個人データ**の**処理**に関する問い合わせ先
- 特に、それが他の領域または管轄内の当局（例えば法執行当局）または団体と共有される場合には、当該データが共有される相手先

49 セクション3.2：同意を参照

個人が**同意**し、アクセス、異議、訂正、削除を実施する場合や、**データ主体**が追加情報を要求する場合の権利を行使できるようにするため必要な場合には、追加情報を提供しなければならない。[50]

一般的なセキュリティ上の制約および現場へのアクセスの困難さを含む実務上の制約のため、直ちに、または個人が所在する場所で、情報を提供することができない例外的な状況において、または**データ主体**から直接データが収集されていない場合、この情報は個人が容易にアクセスし理解できるような方法で、できるだけ早く利用可能にすべきである。[51]**人道団体**はまた、人道的な目的のために絶対に必要な場合を除き、この情報が適切に提供されるまで、受益者から広範なデータセットを収集することを控えるべきである。

2.10.3 データ主体から収集されないデータ

個人データが**データ主体**から取得されていない場合、データ収集に使用された法的根拠に応じて、上記第2.10.2項に規定された情報は、データが処理される特定の状況を考慮し、または、もし他の受領者への開示が想定される場合には、遅くともデータが最初に開示されるときに、実務上およびセキュリティ上の制約に従うことを条件として、データ取得後の合理的な期間内に、**データ主体**に提供されるべきである。この要件は、**データ主体**が既にその情報を持っている場合、または、それを提供することが不可能であるか不相応な努力を必要とする場合には適用されない。その場合には、上記2.10に概説した措置が考慮されるべきである。

例：
情報は、データを入手した後に提供されることがある。例えば、複数の被害者が関与する保護事例が文書化されており、その情報がそのうちの一人または第三の情報源からのみ収集される場合、あるいは、避難民のリストが援助の分配のために当局または他の組織から収集される場合である。

50 セクション2.10：情報およびセクション3.2：同意を参照
51 セクション2.10：情報を参照

2.11 データ主体の権利

2.11.1 はじめに

データ主体の権利の尊重は、データ保護の重要な要素である。ただし、これらの権利の行使には条件が付されており、以下のとおり制限される場合がある。

関連する**人道団体**の内部手続を用いて**DPO**に照会または苦情を申し立てるなど、個人がこれらの権利を行使することができるようにするべきである。ただし、**データ管理者**が管轄権から免除されている**国際機関**でない場合や適用法によっては、個人は、裁判所やデータ保護当局に請求する権利も有することがある。**国際機関**の場合、クレームはその機関の事件について独立した審査を担当する同等の機関に提出することができる。[52]

2.11.2 アクセス

データ主体が、**人道団体**に口頭または書面でアクセス申請をできるようにするべきである。**データ主体**は、自分の**個人データ**を検証し確認する機会を与えられるべきである。この権利の行使は、他者の権利および自由の保護のために必要な場合、または国際人道法や国際人権法の違反の嫌疑に関する文書化のために必要な場合には、制限することができる。

一般的情勢とそのセキュリティ上の制約を十分に考慮した上で、**データ主体**は、**個人データ**が処理されているかどうかを、**人道団体**から合理的な間隔で無償で確認を得る機会を与えられるべきである。そのような**個人データ**が処理されている場合、**データ主体**は、下記の別段の定めがある場合を除き、それらへのアクセスを得ることができるべきである。

人道団体の職員は、**データ主体**やその権限を与えられた代表者から十分な身元証明が提供されない限り、**データ主体**に関するいかなる情報も開示してはならない。

文書へのアクセスは、優先的な利益によってアクセス権が付与されないことが必要とされている場合には適用されない。したがって、公共の利益または他の者の利益が優先する場合、**人道団体**が**データ主体**のアクセス要求に応じることが制限される可能性がある。これは特に、他者の個人データを開示しない限りアクセスが提供できない場合に該当する。

52 国際刑事警察機構ファイル管理委員会：https://www.interpol.int/About-INTERPOL/Commission-for-the-Control-of-Files-CCF およびICRCデータ保護委員会：https://www.icrc.org/en/document/icrc-data-protection-independent-control-commission

ただし、当該文書または情報が、不相応の努力をすることなく、他者の**データ主体**への言及を削除するように配慮して編集できる場合、または開示に対する他者の**データ主体**の**同意**が、同じく不相応の努力をすることなく得られた場合を除く。

人道団体が**人道支援**の目的を追求する能力を危うくしたり、職員の安全にリスクをもたらすアクセスは、常に優先的な利益と解釈される。これは開示が**人道支援**に悪影響を与える可能性があるような、**人道団体**の内部文書の場合も同様である。このような場合、**人道団体**は、可能な範囲内で、また一般的な状況に従うことを条件として、優先する利益の性質を文書化するためにあらゆる努力を払うべきである。

このセクションに定める情報についての**データ主体**への連絡は、理解しやすい形で提供されるべきである。つまり、**人道団体**が**データ主体**に対して**処理**をより詳細に説明するか、または翻訳を提供しなければならない可能性がある。例えば、アクセス申請に応じて技術的な略語や医学用語を引用するだけでは、たとえそのような略語や用語しか保存されていなくても、通常は十分ではない。

コソボ　プリシュティナ
1999 年に終戦を迎えて以来の行方不明者の写真に添えられた生花 *

* 国連安全保障理事会決議1244

行方不明、意識不明、または死亡した**データ主体**の**個人データ**、または人道上や行政上の理由、または家族歴調査のために**データ主体**の家族がアクセスを求めている場合、個人データを家族または法定代理人に開示することが適切な場合がある。ここでも同様に、**人道団体**の職員は、要求者の身元に関する十分な証拠と、適切な場合には法定代理人/家族関係の証拠が提供され、かつ、人道団体の職員が申請の有効性を確立するための合理的な努力をしていない限り、いかなる情報も開示すべきではない。

2.11.3 訂正

データ主体はまた、**人道団体**が自身に関連する不正確な**個人データ**を訂正することを確保できなければならない。データが処理された目的を考慮して、**データ主体**は、例えば補足情報を提供することによって、不完全な**個人データ**を訂正することができるべきである。

これが単に事実データの訂正（例えば、名称の綴りの訂正、住所または電話番号の変更要求）を伴う場合、不正確さの証明は重要ではないかもしれない。しかしながら、そのような要請が**人道団体**の調査結果や記録（例えば、**データ主体**の法的身分証明、法的文書送達用の正しい居住地、またはデータ主体の人道的地位に関するより機微な情報若しくは**データ主体**に関する医療情報）に関連している場合、**データ管理者**は、申し立てられた不正確性の証拠を要求し、主張の信頼性を評価する必要があるかもしれない。そのような要求は、**データ主体**に不当な立証責任を負わせてはならず、**データ主体**がデータを訂正することを妨げるべきではない。加えて、**人道団体**の職員は、いかなる訂正も行う前に、**データ主体**やその権限を与えられた代理人からの十分な身元証明を要求すべきである。

2.11.4 削除権

データ主体は、以下の場合、**人道団体**のデータベースから自身の**個人データ**を削除することができるべきである。

- データの収集目的、**処理**や追加処理された目的に関連してデータが必要でなくなった場合
- **データ主体**が取扱いの**同意**を撤回し、それ以外に当該データの取扱いの根拠がない場合[53]
- **データ主体**が自己に関する**個人データ処理**について異議を述べることに成功した場合[54]
- **処理**が、適用されるデータ保護及びプライバシーに関する法律、規制およびポリシーに準拠していない場合

53 セクション3.2：同意を参照
54 セクション3.4：公益という重要な根拠およびセクション3.5：正当な利益を参照

この権利の行使は、以下のような場合には適切な保護に従うことを条件として、**データ主体**のリスクおよび利益を考慮しつつ、制限することができる。**データ主体**または他の者の権利および自由の保護のため、国際人道法または人権法の違反疑惑の文書化のため、公衆衛生の分野における公共の利益のため、該当する法的義務に準拠するため、法的請求権の確立、行使若しくは弁護のため、または正当な歴史上若しくは研究上の目的のために必要な場合である。これには、人類共通の遺産であるアーカイブを維持することへの利益が含まれる。さらに、**人道団体**の職員は、データ削除を実行する前に、**データ主体**が本人であることを確認できる身元証明を要求する必要がある。

例：
人道団体は、削除の要求が**第三者**からの圧力の下で行われており、削除が**データ主体**の保護や国際人道法または人権法の違反疑惑についての文書化を妨げることを疑っている。そのような場合、**人道団体**がデータの削除を拒否することは正当とみなされるだろう。

2.11.5 異議申立権

データ主体は、その特定の状況に関するやむを得ない正当な理由に基づき、いつでも、自己に関する**個人データ**の取扱いに異議を申し立てる権利を有する。

この権利の行使は、**人道団体**が**データ主体**の利益、権利および自由に優先する**処理**に対してやむを得ない正当な理由を有する場合には、必要に応じて制限することができる。そのような根拠には、例えば、**データ主体**や他者の権利および自由の保護、国際人道法または人権法違反疑惑の文書化、法的請求権の設定、行使若しくは弁護、または正当な歴史上若しくは研究上の目的を含むことがあり、適切な保護処置を講じ、かつ**データ主体**のリスクおよび利益を考慮しなければならない。このような場合、**人道団体**は以下を行うべきである。

- 組織の**DPO**に通知する（DPOがある場合）
- 可能であれば、この基準に基づいてデータを処理し続けるという**人道団体**の意図を**データ主体**に通知する
- 可能であれば、**DPO**または**国際機関**の場合は権限のある国家当局、裁判所若しくは同等の機関による**人道団体**の決定の再審査を要求する権利を**データ主体**に通知する

加えて、**人道団体**の職員は、異議を受け入れる前に、**データ主体**が本人であることを確認できる身元証明を要求すべきである。

2.12 データ共有と国際的なデータ共有

人道上の緊急事態においては、**人道団体**は、**データ処理者**および第三者（他国を拠点とする者を含む）または**国際機関**と**個人データ**を共有することが日常的に要求される。データ保護法は、特に国境または管轄区域を越えた移転の場合、第三者との**個人データ**の共有およびアクセスを制限している。また、多くのデータ保護法は、**国際的なデータ共有**を制限している。国際的なデータ共有とは、**個人データ**を最初に収集または処理した国以外の国や、**国際機関**の地位を享受していない同一**人道団体**内の異なる組織、または**第三者**に対して、電子的手段、インターネット、その他を介して個人データをアクセス可能にする行為である。[55]

データ共有にあたっては、本ハンドブックに記載されている全ての様々な条件に十分な考慮を払う必要がある。例えば、データ共有は**処理**の一形態であるため、それには法的根拠がなければならず、データが最初に収集またはさらに処理された特定の目的のためにのみ行うことができる。さらに、**データ主体**は、データ共有に関する権利を有し、それについての情報を与えられなければならない。**国際的なデータ共有**に関する条件については、第4章：国際的なデータ共有を参照のこと。

55 第4章：国際的なデータ共有を参照

第3章

個人データ処理の法的根拠

3.1 はじめに

第2章：データ保護の基本原則で概説したデータ処理の適法性の原則に基づき、**個人データ処理**業務を行うためには、正当な法的根拠が必要である。

人道支援において、**人道団体**は以下の法的根拠に基づいて**個人データ**を処理できる。

- **データ主体**または他の者の生命に関わる利益
- 公益
- **同意**
- 正当な利益
- 契約の履行
- 法的義務の遵守

人道団体が通常活動している緊急事態下では、有効な**同意**、特に十分な情報に基づく、自由意思による同意の基本的条件を満たすことは困難である。例えば、**個人データ**の**処理**に**同意**することが支援を受けるための前提条件となる場合が挙げられる。また、人事においても、**処理**に同意することが採用の条件となっている場合がある。

人道団体による処理は、生命に関わる利益または重要な公益の根拠に基づくことがよくある。[56] 例えば、国内法または国際法に基づく権限行使である。これには、次の条件を満たす必要がある。

- 生命に関わる利益については、情報**処理**を行わなければ、個人に身体的、倫理的な害悪が及ぶリスクがあると考えられる十分な要素があること。重要な公益の根拠については、特定の**処理**業務が、国内法、地域レベルの法的枠組または国際法の下で**人道団体**のために制定された権限の範囲内にあること、または**人道団体**が他の点では公共の利益に合致し、法律により定められた特定の任務または機能を遂行していることが明らかであること。
- **処理**業務の予定に関して明確な情報を個人に提供していること。
- 個人が発言権を持ち、異議申し立てする権利を行使できる立場にあることを保証していること。[57]どんな場合においても、できる限り早く、明確に、できればデータ収集の時点で、**処理**に異議を唱える機会を与えるべきである。**データ主体**が、**処理**に対する異議を正当化する十分な理由を提示する場合、および、いかなる法的根拠においても**処理**が必須でない場合（例：セクション3.3：生命に関わる利益、またはセクション3.4：公益という重要な根拠）、**データ主体**の個人データの処理を停止すべきである。

56 セクション3.3：生命に関わる利益、およびセクション3.4：公益という重要な根拠参照
57 第2章：データ保護の基本原則参照

適切な法的根拠に依拠することによって、人道団体が、個人、特定のグループ、または**人道団体**自体のための**個人データ**の収集、保管、または使用に関するリスクを評価する責任から**人道団体**免除されるわけではない。特に高いリスクを伴う場合、**人道団体**は、そもそもデータの収集および／または**処理**を控えることが適切でないかを検討すべきである。このようなリスクは、**人道団体**の経験からすぐに明らかになるかもしれないし、新しい技術ソリューションに内在する複雑なデータ・フローの中に隠されているかもしれない。したがって、**データ保護影響評価**（DPIA）を行うことは、関連する全てのリスクを確実に特定し、低減するための重要なツールである。[58]

3.2 同意

同意は、**個人データ処理**の最も一般的で、しばしば使用される法的根拠である。しかし、ほとんどの受益者の脆弱性と人道上の緊急事態の本質を考慮すると、多くの**人道団体**は、その**個人データ処理**の大部分について**同意**に頼ることはできない。特に、以下の場合には、他の法的根拠の選択が適切である。

- **データ主体**が、例えば**被調査者**であったり、意識不明であるなどの理由により、十分な情報に基づく、自由意思による**同意**ができる物理的立場にない。
- **人道団体**が、活動地域の一般的な治安やロジスティクスの状況によって、**データ主体**に情報を提供し、**同意**を得られる状況にない。
- **人道団体**が、実施すべき業務の規模からして、**データ主体**に情報を提供し、同意を得られる状況にない。例えば、(1) 多数の避難民への人道支援の配分リストを作成する場合や、(2) 国際人道法や人権法の規定に基づき、当局が**人道団体**に保護対象者のリストを提供する場合など。
- **データ主体**の**同意**が有効ではないと、人道団体の評価において判断される場合。例えば、**データ主体**が**同意**する時点で特に脆弱である場合（例えば、子ども、高齢者、障がい者）、または提供される特定の支援やそれに関連するデータ**処理**に代わるものがないなど、必要性や脆弱な状況のために現実的に**同意**を拒否する選択肢がない場合など。
- 複雑なデータの流通と、複数の管轄区域の**データ処理者**や再委託を受けた**データ処理者**など多数の関係者の関与を特徴とする、新しいテクノロジーが関係している場合。この場合、個人が**処理**業務のリスクと便益を十分に理解することが難しく、そのため**同意**することで必然的に伴う責任を負うことが困難になる。このような場合には、**人道団体**が**処理**のリスクと便益の評価においてより多くの責任を負う、他の法的根拠を選択することがより適切であろう。

58 第2章：データ保護の基本原則参照

なお、**同意**を得ることは、データ**処理**に関する情報（セクション2.10：情報）を提供することとは異なることに注意しなければならない。つまり、たとえ**同意**が得られない場合でも、異議申立、削除、アクセス、訂正の権利に関する情報を含む情報要件が適用される。

同意を有効なものにするには、以下の要件を満たす必要がある。

3.2.1 明確性

同意は、適切な方法で、十分な情報に基づき、自由意思によりなされるべきである。これは、**データ主体**が自らの**個人データ**の**処理**に対する同意を表明することを意味する。**同意**は、書面、または書面による**同意**が不可能な場合には口頭、もしくは**データ主体**（または、該当する場合は、その保護者）による他の明確な同意を確認できる行動によって行うことができる。

3.2.2 タイミング

同意は、データの収集時またはその後合理的に実行可能となった時点でなるべく速やかに得るべきである。

3.2.3 有効性

データ主体が、真に自由な選択ができない場合、不利益なく**同意**を拒否若しくは撤回することができない場合、または、**個人データ処理**の結果を理解するための十分な情報が与えられていない場合、**同意**は自由意思であると見なされるべきではない。

3.2.4 脆弱性

同意の有効性を検討する際は、**データ主体**の脆弱性を考慮すべきである。脆弱性の評価には、**データ主体**が属するグループの社会的、文化的、宗教的規範を理解し、各**データ主体**が自身の**個人データ**の所有者として個別に扱われることを保証することが含まれる。個人を尊重するということは、個人が自らの選択する際に自律的で、独立し、自由であるとみなされることを意味する。

脆弱性は状況によって異なる。この点に関し、以下の要因を考慮すべきである。[59]

- 識字能力、障害、年齢、健康状態、性別、性的指向などの**データ主体**の特徴
- 収容施設、再定住キャンプ、僻地などの**データ主体**の居場所
- 不慣れな環境、外国語や馴染みのない概念などの環境やその他の要因
- 例えば、少数民族や民族集団に属しているなど、**データ主体**の他者との関係における立場
- **データ主体**が属する家族、コミュニティまたはその他集団における社会的、文化的および宗教的規範
- 特に複雑な新しいテクノロジーが採用されている場合には、想定される**処理**業務の複雑さ

例：

ある**人道団体**が**人道上の緊急事態**の評価を実施する。その際には、適切な援助プログラムを構築するために、栄養、健康および保護の要素など、世帯の生計および特定の脆弱性に関する情報を含む潜在的な受益者に関するデータを収集する。これには、大量の**個人データ**の収集と**処理**が含まれる。人道団体は、収集されたデータが使用される目的についてインタビューを行う個人に通知すべきであるが、彼らの**同意**に基づいてデータを収集することは意味がない。なぜなら、彼らは極めて脆弱な立場にあり、提供された援助を受けることに伴う**処理**業務はなんであれ受け入れる以外になく、真の選択はできないため、データ収集に有効な**同意**を与える可能性が低いからである。他の法的根拠を識別し、想定される**処理**に異議を申し立てる選択肢を含む関連情報を提供すべきである。

3.2.5 子ども

子どもは**データ主体**の中でも特に脆弱なカテゴリーであり、子どもに影響を及ぼす全ての決定において、子どもの最善の利益が最優先事項である。子どもの考えや意見は常に尊重されるべきであるが、子どもが**処理**業務に伴うリスクと便益を十分に理解しているかどうかを確認し、子どもが異議を唱える権利を行使でき、また該当する場合には有効な**同意**を与えられるよう、特に注意を払うべきである。子どもの脆弱性の評価は、子どもの年齢と成熟度に左右される。

59 国際移住機関（IOM）、データ保護マニュアル（2010）、pp.45-48：https://publications.iom.int/books/iom-data-protection-manual

過去に軍隊や武装集団に加わった子どもたちのための CAJED* 移行・適応センターで、家族からのメッセージを受け取る子ども
コンゴ民主共和国・北キブ州

子どもに**同意**する法的能力がない場合は、親または法定代理人の**同意**が必要になることがある。次の要素を考慮する必要がある。

- 親または法的保護者に全ての情報を提供し、親または法定代理人の**同意**を示す署名を得ること
- **データ主体**に明確に情報が説明され、その主体の考えが考慮されていることを保証すること

3.2.6 通知

同意が**処理**の法的根拠として認められるには、事前に十分に説明されなければならない。これには、**データ主体**が、**処理**の状況、リスク、および利益を十分に納得し理解することができるように、専門用語を使わず簡単な言葉で説明を受けることが必要である。[60]

* CAJED（恵まれない若者と子どもたちのための協調行動）

60 セクション2.10：情報参照

3.2.7 文書化

処理が**データ主体**の**同意**に基づく場合、**データ主体**が**処理**に同意したことを証明できるように、その記録を残すことが重要である。記録は、署名若しくは**人道団体**の立会いのもとでのクロスマークを要求する、または口頭による**同意**の場合には、**人道団体**が**同意**を得た旨の書類を作成することにより、残すことができる。人道支援の世界では知られていないわけではないが、**同意**を確認するためだけに拇印を求めることは、生体認証データの収集になるため、非常に問題が多く、避けるべきである。生体認証データの収集に伴うリスクの分析については、第8章：バイオメトリクスを参照。

同意を使用する場合は、その使用の制限／条件、および**同意**を取得する具体的な目的を記録することが重要である。これらの詳細は、**人道団体**が対象となるデータを処理するために使用する全てのデータベースにも記録されるべきであり、また、その**処理**全体を通じてデータに添付されるべきである。

同意が記録されていない場合、または**同意**の記録が見つからない場合は、同意以外の法的根拠（例えば、生命に関わる利益、正当な利益、公共の利益）に基づいて処理できない限り、データをそれ以上処理（譲渡について**同意**の記録がない場合の**第三者**への譲渡を含む）すべきではない。

3.2.8 同意の保留 / 撤回

データ主体が明白に**同意**を保留する場合、**人道団体**および／または**第三者**機関によって提供されるかもしれない、または提供されないかもしれない支援に与える影響を含め、その保留がもたらす結果について助言されるべきである。ただし、**同意**がなかったために援助が提供されない場合は、**同意**は**処理**の法的根拠とはみなされないことに留意すること。[61]

データ主体は、**処理**に異議申し立てする権利と、データ**処理**のいかなる段階においても以前の**同意**を撤回する権利を有する。第三者からの圧力の下で**同意**が撤回されていると**人道団体**が疑う場合、**人道団体**は、生命に関わる利益が危険にさらされているなど別の根拠に基づいて、**データ主体**の**個人データ**の**処理**を継続する立場にある可能性が高い。（下記の3.3を参照）

61 セクション3.2：同意、四番目の箇条書き参照

3.3 生命に関わる利益

同意を有効な方法で得ることができない場合でも、それが**データ主体**または他の者の生命に関わる利益であると**人道団体**が判断する場合、すなわち、**データ主体**または他の者の生命、誠実性、健康、尊厳、安全にとって不可欠な利益を保護するためにデータ**処理**が必要な場合には、**個人データ**を処理してもよい。

人道団体の活動の本質および活動する緊急事態の状況を考慮すると、**人道団体**によるデータの処理は、以下の場合には、**データ主体**または他の者の生命に関わる利益を根拠としてもよい。

- **人道団体**が、**被調査者**のケースを扱っている
- **人道団体**が、遺体の身元確認および／または遺族の追跡調査について当局を支援しているこの場合、**個人データ**は、家族の生命に関わる利益のために処理される
- **人道団体**が、意識不明や**同意**を伝えることができない危険な状態にある個人を支援している
- **人道団体**が医療や医療支援を提供している
- 開示を含む情報**処理**が、**データ主体**またはその他の者の身体的および精神的インテグリティに対する差し迫った脅威に対する最も適切な対応である
- **処理**が、**人道上の緊急事態**の最中やその直後の個人やコミュニティの本質的なニーズを満たすために必要である

しかしながら、このような場合、**データ主体**ができる限り速やかに処理を認識し、**個人データ**が収集され**処理**される特定の目的を納得し理解するための十分な知識を有し、希望すれば**処理**に反対する立場にあることを、**人道団体**は可能な限り保証すべきである。なるべくなら、収集の時点での直接説明によって、これを行うことができる。また、例えば支援の際のポスター使用、グループ説明、または受益者が登録をする際や援助を受ける際に小冊子やウェブサイト上でさらなる情報を提供することでも、可能である。[62]

62 セクション2.5.1：公平性の原理と処理の適法性およびセクション2.10：情報参照

例：
ある**人道団体**は、自然災害の後、生命に関わる支援（例えば、食料、水、医療支援など）を提供するために、脆弱な個人から**個人データ**を収集する必要がある。彼らの**同意**を得る必要なしに、生命に関わる利益を法的根拠として、**個人データ**の収集の行うことができるかもしれない。しかしながら、人道団体は1）この法的根拠がそのような支援を提供するためにのみ使用されることを保証し、2）個人に反対する権利を与え、3）個人情報保護方針に従って収集されたデータを処理し、要望があれば**データ主体**がこの個人情報保護方針にアクセスできるようにすべきである。データ**処理**に関する全ての関連情報を提供すべきである。例えば、ポスター、グループ説明、または受益者の登録時や援助が行われる際に、小冊子やウェブサイト上でさらなる情報を利用できるようにする。

3.4 公益という重要な根拠

当該活動が国内法または国際法に基づいて確立された人道上の責務の一部である場合、または法律に規定された公共の利益のための活動である場合、公益という重要な根拠が生じる。例えば、ICRC、各国の赤十字社・赤新月社、国連難民高等弁務官事務所（UNHCR）、国連児童基金（UNICEF）、国連世界食糧計画（WFP）、国際移住機関（IOM）、その他の**人道団体**が、法律で規定された、公共の利益のための特定の業務や機能を遂行しており、これら業務を遂行するために**個人データ**の**処理**が必要である場合が挙げられる。[63]この場合の「必要である」という用語は、厳密に解釈されるべきである（すなわち、データ**処理**は関連する目的を達成するために単に便利なだけでなく、真に必要なものでなければならない[64]）。

この法的根拠が該当する可能性のある事例としては、全ての潜在的な受益者の**同意**を得ることが現実的でない状況、および**データ主体**または他の人々の生命、安全、尊厳およびインテグリティが危険にさらされているかどうかが明らかでない状況での援助の提供がある（危険にさらされていることが明らかな場合には、「生命に関わる利益」を**処理**のための最も適切な法的根拠とできる）。

この法的根拠が該当する可能性のある他のシナリオには、拘束されている**個人のデータ処理**があり、この種の活動が当該**人道団体**の任務の場合が挙げられる。これは例えば次の場合に起こり得る。**個人データ**の**処理**が武力紛争またはその他の暴力を伴う事態において自由を奪わ

63 例えば、国際的な武力紛争が発生した場合、ICRCは4つのジュネーヴ諸条約と第一追加議定書に基づいて活動する権限がある。ICRCは、非国際的な武力紛争における人道的介入の権利を有する。https://www.icrc.org/en/mandate-and-mission

64 セクション3.6：契約の履行を参照

れた人々に関する場合で、**人道団体**が自由を奪われた**データ主体**を訪問する立場にまだなく、そのため**同意**を得る立場にもなく、その後も、**データ主体**の脆弱性のために**同意**が有効な法的根拠とみなされない場合である。

リベリア・モンロビア中央刑務所に抑留される人々

これらの場合においても、可能であれば、**データ主体**が、自身の**個人データ**の処理についてできる限り速やかに認識し、個人データが収集され**処理**される特定の目的を納得し理解するための十分な知識を有し、かつ、希望する場合にはいつでも、**処理**に反対できる立場にあることを**人道団体**は保証すべきである。

3.5 正当な利益

個人データの処理が正当な利益となる場合、特に、任務に列挙されている特定の人道的活動を行うために必要な場合にも、**人道団体**は個人データを処理することができる。ただし、この利益が**データ主体**の基本的な権利および自由によって優先されないことを条件とする。これら全ての状況において、「必要な」という用語は、厳密に解釈されるべきである（すなわち、データ**処理**は関連する目的を達成するために単に便利なだけでなく、真に必要なものでなければならない[65]）。

65 セクション3.6：契約の履行を参照

正当な利益には、次のような状況が含まれる。

- 公益という重要な根拠が生じない場合で、**人道団体**の任務を効果的に遂行するためには、データ**処理**が必要である。
- データ**処理**が、情報システムおよび情報セキュリティを確保する上で必要である。[66]また、これらの情報システムから提供される、若しくはこれらの情報システムを介して利用できる関連サービスのセキュリティ、および、公的機関、コンピュータ緊急対応チーム（**CERT**）、コンピュータセキュリティインシデント対応チーム（**CSIRT**）、電子通信ネットワークとサービスのプロバイダ、並びにセキュリティ技術とサービスの提供者によって提供される関連サービスのセキュリティを確保するために必要である。これには、例えば、電子通信ネットワークへの不正アクセスおよび悪質なコード配信の防止や、「サービス妨害」攻撃やコンピュータと電子通信システムへの損害を阻止することが含まれる。
- データ**処理**が、詐欺や窃盗を防止し、立証し、阻止するために必要である。
- **個人データ**の**処理**が、**個人データ**の匿名化や仮名化のために必要である。[67]
- データ**処理**が、司法手続、行政手続または何らかの法定外手続であるか否かに関わらず、法的請求の確立、行使または抗弁のために必要である。

例：

人道団体は、ウイルス検出のためのITシステムのスキャンや、不正防止のための受益者の身元確認、元従業員が起こした訴訟での自らの弁護などの過程で**個人データ**を処理する。これらの**処理**活動は全て、組織の正当な利益に基づいて許可される。

66 情報セキュリティには、真正性、責任追跡性、否認防止および信頼性のような要素の他にも情報の機密性、完全性および可用性の維持が含まれる。ISO/IEC 17799:2005、情報技術 — セキュリティ技術 — 情報セキュリティ管理の実践規範：http://www.iso.org/iso/catalogue_detail?csnumber=39612参照

67 セクション2.3：集計化、仮名化、および匿名化されたデータセットを参照。仮名化とは、個人データを追加情報なしには特定のデータ主体に帰属できなくさせる処理をいう

3.6 契約の履行

データ主体が当事者である契約を履行するために**個人データ**処理が必要な場合、または契約を締結する前に**データ主体**の要望で措置を講じるために、**人道団体**はこの法的根拠に基づき、人道団体個人データを**処理**することができる。ここでも、用語「必要な」は厳密に解釈されるべきである（すなわち、データ処理は、単に便利なだけでなく、関連する目的を達成するために真に必要なものであるべきである）。

これは、一般的に、以下の目的のためのデータ**処理**に関して該当する。

- 採用を含む人事ファイルの管理
- 商品・サービスの供給者との関係の管理
- ドナーとの関係

例：

人道団体は、職員に対する雇用上の義務を果たすために、職員に関する人事ファイルを保管している。これは、職員に対する契約上の雇用義務を履行するために許容される。一方、同組織が、そのデータ**処理**を本社の所在地がある国の**第三者**に外部委託している場合には、データ**処理**を外部委託することは、必要性よりも利便性の観点から選択されたものであることから、外部委託先にデータベースへのアクセスを認めることは、外部委託先との契約の履行上必要なものとはみなされない。この場合、組織の正当な利益が適切な法的根拠となるかどうかを考慮すべきである。

3.7 法的義務の遵守

人道団体が対象とされる、または**人道団体**が従うべき法的義務を遵守するために必要な場合、人道団体はこの法的根拠に基づき、**個人データ**を処理することができる。例えば、雇用法の分野において、または、特権および免除の恩恵を受けていない組織が、実施可能な法的義務を遵守するために必要な場合が、これに該当する可能性がある。

例：
人道団体が活動している国では、職員への賃金支払いに関する情報を社会保障当局と税務当局に提供する法的義務がある。団体が国内管轄下にある場合、団体が対象とされる法的義務に基づいて許可される。

しかし、**人道団体**が活動している環境を考えると、法的義務をデータ処理の根拠とみなす場合には、以下の要因が考慮されるべきである。これらは、当局が法律の執行、諜報、またはその他の目的のために**個人データ**へのアクセスを要求する場合に特に関係する。

- データへのアクセスを必要とする国における法の支配と権力分立の存在
- 効果的な救済措置を受ける権利を含む人権の尊重
- アクセスを要求する当局が当事者を代表する可能性がある武力紛争または暴力の事態の存在
- データの性質、および差別または起訴につながる推測がデータから導き出されるか否か（例えば、必要な食べ物の名前や関連するデータが宗教や民族性を明らかにしないか、同性愛者が迫害されている国で**健康データ**が性的指向を明らかにしないか、あるいはデータを要求されている**データ主体**が死刑に科されないか）
- **人道団体**が特権および免除を享受していることで、義務が適用されない状況にないか

この点において、**人道団体**に適用される、データを開示する法的義務によって、**データ主体**を差別、迫害、社会的排斥、抑圧の危険にさらす可能性がないかを国際機関は考慮すべきであり、そのような可能性がある場合にはそもそもデータ収集を行わないことを検討すべきであるという点を、強調することも重要である。

第4章

国際的なデータ共有

4.1 はじめに

人道上の緊急事態には国境がない。そのため、必要とされる人道的な対応を提供するために、**人道団体**はたびたび国境を越えて他の組織とデータを共有する必要がある。従って、国家間で国境を越えた**個人データ**の効率的な流れを確保することは、**人道団体**の業務にとって不可欠である。さらに、人道的な対応における新技術の採用には、複数の**データ処理者**と再委託された処理者の関与が必要であるが、これら企業は、必ずと言っていいほど、**人道上の緊急事態**が発生する地域とは別の、様々な管轄区域に本拠地を置いている。例えば、**個人データ**を処理するために、**人道団体**によってクラウドベースのソリューションが人道団体使用される場合があり、その場合、データは人道団体が本部を置く地域のホストで保管されるが、サービスプロバイダは、いくつかの管轄区域で**データ処理者**および再委託された処理者として活動することがある。[68]

トルコ・ガジアンテップ州のシリア国境近くにあるニジップ難民キャンプ
（2016 年 11 月）

セクション2.4：準拠法および国際機関で触れたように、**人道団体**の中には、国際法の下で国際社会が認めた任務を完全に独立して遂行できるよう保障されるために、特権と免除を享受する**国際機関**もある。それに応じ、独自のルールに従い**個人データ**を処理するが、このルールは

68 第10章：クラウドサービスを参照

業務を行う地域に関係なく業務全体に適用され、また独自のコンプライアンスシステムによって管理、実施される。
従って、このような国際機関は独自の「管轄区」を設け、その中でデータを受け渡しするため、それらの下部組織については本章の範囲に含まれない。[69]

以下は、**人道団体**が国境を越えてデータを共有する必要があると考えられる組織のほんの一例である。

- 異なる国で活動する、同じ非政府組織（NGO）の事務所
- 他のNGO、**国際機関**、国連機関
- 政府当局
- **人道団体**に代わって**個人データ**を収集および／または**処理**する、サービスプロバイダ、コンサルタント、研究者などの**データ処理者**
- 学術機関および／または研究者
- 民間企業
- 博物館

国際的なデータ共有には、電子手段、インターネットその他を介して**個人データ**が収集若しくは処理された最初の国の外で、**個人データ**にアクセスできるようにする全ての行為が含まれる。個人データを新聞、インターネット、またはラジオ放送で公開することは、国境を越えてデータにアクセスできる場合、通常、データ共有とみなされる。

国際的なデータ共有には、**個人データ**が国境を越えて、または**国際機関**との間で移転、共有またはアクセスされることになるあらゆる行為が含まれる。したがって、**国際的なデータ共有**には、以下の状況のいずれかが含まれる可能性がある。

- **人道団体**が、別の管轄区域にある組織にデータを移転する。受取り側が、**処理**の手段と目的を決定する、新しい**データ管理者**である。
- **人道団体**が、他の管轄区域内にある組織にデータを移転するが、**処理**の手段と目的を決定するのは人道団体のままであり、受取り側は、共有機関の指示に従ってのみ**個人データ**を処理する。この場合、受取り側は**データ処理者**である。

どちらのシナリオにも、一度**個人データ**が共有されると、**人道団体**によってのみ**処理**された際に享受していた保護の一部または全部が失われるリスクがある。したがって、いずれのシナリオにおいても、意図しない保護の損失を避けるために、共有する側の組織によって全ての合理的な措置が確実に実施されることが重要である。

69 セクション2.4：準拠法および国際機関を参照

データ共有は処理業務であり、そのため前章で説明した全ての要件の対象となるということを忘れてはならない。[70]本章では、**人道団体**が**国際的なデータ共有**を実施する際には人道団体必ず考慮すべき、さらなる注意事項について説明する。

4.2 国際的なデータ共有のための基本ルール

国際的なデータ共有を保護の下で行うために、以下の全てのステップに従うべきである。

- データ共有に適用される全てのデータ保護規則やプライバシー要件[71]（該当する場合、現地の法律によるデータ保護やプライバシー要件の全てを含む）が、移転前に満たされている。
- 移転のための法的根拠が提示されなければならない。
- 移転が個人にとって容認できないリスク（例えば、差別や抑圧）をもたらすことがないかを判断するための評価が実施されるべきである。
- 移転を行おうとする組織は、**国際的なデータ共有**に関して**個人データ**の保護レベルを維持するために、受取り側が本ハンドブックに定めるデータ保護原則を確実に遵守するための適切な措置を講じたことを実証できなければならない（説明責任）。
- 当該個人は、移転の受取り側について通知されるべきである。移転は、データが移転される個人の合理的な期待と矛盾するものであってはならない。

4.3 国際的なデータ共有の法的根拠の提供

4.3.1 はじめに

上述したように、本ハンドブックは、データ保護の原則と権利を人道状況に取り入れ、尊重できるよう支援することを目的としている。ただし、**国際機関**が享受する特権や免除の恩恵を受けていない**人道団体**に適用される場合には、データ保護に関する国内法に代わるものではなく、また、助言するものでもない。したがって、本章に含まれる考慮事項は、特にこの**人道団体**に適用される限り、データを移転する国で適用される現地法の要件に追加されるものであることに留意すべきである。世界のあらゆる地域の数十の国が、**国際的なデータ共有**を規制するデータ保護法を制定しており、それらの法律を評価するために、**人道団体**は**DPO**、法務部門および／または現地の法律顧問と協議すべきである。

70 第2章：データ保護の基本原則、および第3章：個人データ処理の法的根拠を参照
71 第2章：データ保護の基本原則を参照

4.3.2 国際的なデータ共有の法的根拠

国際的なデータ共有は、次の場合に実施することができる

- 移転が**データ主体**やその他の者の生命に関わる利益である
- **人道団体**の責務に基づく、公益という重要な根拠のため
- **人道団体**が宣言する使命に基づく、**人道団体**の正当な利益のためであり、この利益が**データ主体**の権利や自由によって優先されず、かつ、人道団体が**個人データ**について適切な保護措置を提供している場合
- **データ主体**の**同意**を得ている
- **データ主体**との契約の履行のため

これらの法的根拠は、**個人データ処理**における適用と同様の方法で使用される。[72]また、**国際的なデータ共有**にはさらなるリスクが伴うことから、以下の「個人にとってのリスク低減」のセクションに記載されている要素についても十分に考慮する必要がある。

4.4 個人にとってのリスク低減

国際的なデータ共有を実施する際には、以下の要素が重要である。

- 国の管轄下にある組織や、データ保護の観点から十分であると公式に評価されている**国際機関**への移転の場合、リスクはより低くなる可能性がある。一般的に言えば、これは、データの受取り側が、独立監督機関、大量監視からの自由、個人の司法上救済へのアクセスなどの、高度な国際基準に沿ったデータ保護のための規制体制を有することが正式に判断された国にあることを意味する。しかし、国や地域の政府当局が正式な意味で十分な保護を提供していると認められた国はごく少数である。つまり、**人道団体**にとって、十分性の調査結果に頼ることは、ほとんどの状況において有用ではない。十分性は**国際的なデータ共有**の前提条件ではないが、考慮すべき要素である。
- 受取る側が適切なデータ保護を提供することを義務化する契約条項や、受取る側が**個人データ**保護に関する行動規範を遵守することを約束しているかどうかを確認する契約条項のように、これが論理的に実現可能な場合、**国際的なデータ共有**のために適切な保護措置が使用されるべきである。
- **人道団体**は、自らが関与する**国際的なデータ共有**について説明責任を負うべきである。

72 第3章：個人データ処理の法的根拠を参照

これら最後の2つの要素については、以下でより詳細に考察する。

例：
人道支援を行うあるNGOは、X国に本部があり、人道支援のサービスを提供する脆弱な個人に関する**個人データ**を含むファイルを、Y国の別のNGOに移転したいと考えている。これらのファイルは、Y国のNGOがアクセスできるように、安全なウェブベースのプラットフォームに置くことで利用可能になる。Y国は、十分な水準のデータ保護を提供していると、X国の公的機関によって正式に認定されている。ウェブベースのプラットフォーム上でファイルを利用可能にすることは、**国際的なデータ共有**に該当するが、下記のセクション4.4.1：十分な保護措置に規定されている追加の考慮事項に従うことを条件に、Y国に十分な水準の保護があることを根拠として移転を行うことができる。

4.4.1 適切な保護措置 / 契約条項

人道団体が**国際的なデータ共有**に伴うリスクの低減について決定する際に考慮すべき措置の一つは、受取る側が**個人データ**を保護するために適切な保護措置を講じることを保証することである。

実際には、そのような保護措置は、**人道団体**が自ら作成した、若しくは他の国際的に認められた情報源から適応させた、法的拘束力のある契約上の合意によって、講じさせる人道団体ことができる。この合意によって、人道団体とデータを移転される側は、**人道団体**に適用されるデータ保護基準に基づき、当該**個人データ**を保護することを約束する。

欧州委員会は、**データ管理者**からEU/EEA外に拠点を置く**データ管理者**や**データ処理者**への移転に関する標準的な契約条項を発した。[73]EUデータ保護法の対象となっている**人道団体**やこれらの条項の使用を希望している人道組織のためのものである。

リスク低減についての判断を行う際に考慮すべきもう一つの要素は、データ共有に関与する相手が、**個人データ処理**に関する事項を含む行動規範[74]を約束しているかどうか、そしてそのような行動規範が実際どの程度適用されているか、つまり拘束力や執行力があるのか否かという点である。

73 欧州委員会、個人データの第三国への移転のための標準契約条項：https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en を参照

74 たとえば、国際赤十字・赤新月社運動のデータ保護に関する離散家族の再会支援（Restoring Family Links）行動規範：https://www.icrc.org/en/document/rfl-code-conduct を参照

移転の法的根拠が存在し、リスク低減措置がとられている場合であっても、以下のような要因のために、**国際的なデータ共有**を実施することは適切でない場合がある。

- データの性質上、個人を危険にさらす可能性がある
- データを受取る側が十分な保護を受けることを保証できない可能性があると考える正当な理由がある
- データが送信される予定の国の状況により、データが保護される可能性が低い
- 組織の管轄権の免除による保護を根拠にデータが処理されているが、受取る側の組織がそのような免除を享受していない

例：
X国に事務所を有する**国際機関**である**人道団体**は、人道支援サービスを提供する脆弱な個人に関する**個人データ**を含むファイルを、同じ国のNGOに移転したいと考えている。その共有は**国際機関**からX国の管轄下にある機関への移転となるため、**国際的なデータ共有**とみなされる。**人道団体**はNGOとの間で標準的な契約条項に署名するが、武装集団がそのNGOの施設を攻撃するであろう重大なリスクがあり、過去にはそのNGOに送られたデータが失われたことがある。**人道団体**は、契約条項の署名にかかわらず、データを移転しないことを真剣に検討すべきである。

このようなリスクを特定し、適切に対処やリスク低減するために、DPIAが実施されるべきである。[75] 疑わしい場合は、**人道団体**の**DPO**に相談すべきである。

4.4.2 説明責任

移転を行おうとする**人道団体**が、**国際的なデータ共有**に関する基本的なデータ保護原則の遵守を保証するために、適切かつ相応な措置が講じられてきていることを実証できることが重要である。**人道団体**は、データが共有されている**データ主体**に対して説明責任を負う。これには、次のような方法がある。

- データ**処理**に関する内部記録の保管、特に、移転の記録や、該当する場合には、個人データの移転先との間で締結されたデータ移転契約書の写しの保管
- **DPO**の任命
- データセキュリティ指針を含む、**個人データ処理**指針の立案
- 移転に関するDPIAの実施と記録の保管
- 適用法令により義務づけされている場合は、所管当局（すなわちデータ保護当局）への移転の登録

75 第5章：データ保護影響評価（DPIAS）を参照

いかなる**国際的なデータ共有**についても、**個人データ**の第三者への伝達を保護するために適切な措置が取られるべきである。適用されるセキュリティのレベル[76]と伝達方法は、**個人データ**の性質と機微性、および関連するリスクに相応すべきである。また、取るべき予防措置をさらに特定するために、この要素をDPIAの一部として検討することが望ましい。

4.5 データ管理者とデータ処理者の関係

データ処理者が**データ管理者**によって雇用される場合、**データ処理者**が**データ管理者**が所在する国とは別の国に所在するか否かにかかわらず、両者の関係は、可能な限り、両者間で共有される**個人データ**の**処理**を保護するための拘束力のある合意によって管理されるべきである。

個人データの適切な保護が確保されるには、例えば以下のような多くの問題が、関連する契約文書において明確にされなければならないだろう。

- **データ処理者**の保全方針が許容可能なものかどうか（例えば、携帯電話事業者／金融機関は、国内のデータ保全要件の対象となる）
- **処理**の一部として**データ処理者**によって収集される追加のデータの種類（例えば、携帯電話事業者の位置情報、その他の電話のメタデータ）
- **データ処理者**による**個人データ**の**処理**が**データ管理者**の指示に従っているかどうか
- 契約処理終了後の**データ処理者**による**個人データ**の破棄方法

4.6 当局に対する個人データの開示

人道団体による**個人データ**の当局への開示および移転に関して、特に当局が紛争当事者またはその他の暴力的状況における行為者を代表する場合、問題が生じる可能性がある。このような開示は、中立的、公平かつ独立した**人道支援**にとって問題となることがある。**データ主体**の人道的状況に照らして、**データ主体**にとって開示が不利益を及ぼす場合や、そのような移転が組織の安全を脅かしたり、武力紛争や暴力の影響を受けた者や紛争当事者、またはその任務遂行に必要な情報への組織の今後のアクセスを危険にさらす場合に、特に当てはまる。

国際機関として特権および免除を享受する**人道団体**は、その特定の地位が確実に尊重されるようにすべきで、**データ主体**および**人道支援**の最善の利益のために必要でない限り、そのような要請に応じることを拒否すべきである。特権および免除を享受する**人道団体**が、そのような特権および免除を受けない**人道団体**にデータを移転する必要がある場合、受取り側がそのような要請に抗える立場にないかもしれないというリスクを考慮に入れるべきである。このリスクは、

76 セクション2.8：データセキュリティと処理のセキュリティを参照

2015年のデータ保護・プライバシーコミッショナー国際会議における、プライバシーと国際**人道支援**に関する決議[77]で特に認められている。

> *特権と免除を享受していない**人道団体**は、人道的目的のために収集したデータを他の目的（例えば、移民の流れの管理やテロとの闘い）に利用することを望む当局に提供するよう圧力を受けることがある。データの誤用のリスクは、避難民のデータ保護の権利に深刻な影響を与える可能性があり、また避難民の安全に、より広い意味では**人道支援**にも、支障をきたす可能性がある。*

77 データ保護・プライバシーコミッショナー国際会議、プライバシー及び国際人道支援に関する決議、アムステルダム、2015年。前掲。

第5章

データ保護影響評価（DPIAS）

5.1 はじめに

個人データの**処理**は、社会全体のリスクのみならず個人、グループおよび組織のリスクを増大させる可能性がある。**データ保護影響評価**（DPIA）の目的[78]は、**個人データ**、そして最終的には**データ主体**に対するプロジェクト、政策、プログラム、またはその他のイニシアチブから生じるリスクを特定し評価し対処することである。DPIAは、最終的にはデータ保護リスクの回避、最小化、移行または共有化に役立つ措置につながるべきである。ライフサイクルを通じて個人データの**処理**を必要とするプロジェクトまたはイニシアチブは、DPIAの実施を伴うべきである。プロジェクトが変更されたり、新たなリスクが生じて明らかになった場合には、DPIAを再度実施すべきである。

DPIAが適切な場合の例を次に示す。

- **人道団体**の事務所は、たびたび略奪されてきた。同団体は、現場のオフィスが紙のファイルを廃棄するか、本社に送付して、代わりにクラウドベースのストレージシステムに依存することを望んでいる。現場のオフィスでは、紙、CD、フラッシュ・ドライブを処分すべきか。
- 現地のNGOまたは当局が、国内での暴力のために離散した家族を再会させたいと**人道団体**に接近する。**人道団体**から国内の行方不明者に関するすべての情報の提供を受けることを望んでいる。情報を共有する必要があるか。もしそうなら、行方不明者を追跡するためには、どの程度の個人情報を共有すればいいのか。どのような条件の下で、個人情報は受入れ側の政府に開示されるべきか。
- 津波が何十もの沿岸の村を押し流した。数千人の行方不明者が報告されている。**人道団体**は、行方不明者の家族からどの程度の個人情報を収集すべきか。多いほうがいいか、少ないほうがいいか。開示された場合に個人に重大な損害を与える可能性のある健康または遺伝子データ、宗教的所属または政治的見解に関する情報を含めるべきか。
- **人道団体**は、行方不明の子どもたちだけが写っている写真をインターネットで公開すべきか。**人道団体**はポスターを作るべきか。それはどのような状況下ですべきか。

プライバシーまたはデータ保護のリスクによって悪影響を受ける可能性のあるユーザーと、それらのユーザーがどのように損害を受けるかを判断する上で、DPIAは重要な役割を果たすことができる。

78 著者らは、データ保護影響評価に関する資料の使用許可を許可してくださったTrilateral Researchに感謝の意を表する。

Schermbrucker/UNICEF

ラウイのチクワワ地区病院から地域の診療所に結果を伝えるために電話が使用される（2014 年）

本章は、**人道団体**のために、DPIAの実施方法とDPIA報告書に記載すべき内容に関する段階的な手引きである。付録Iには、DPIA報告書のテンプレートが含まれている。[79]DPIA報告書はDPIAプロセスの最終工程ではないが、その成功にとって非常に重要である。**人道団体**が、提案されたプロジェクトのプライバシーへの影響と、そのプロジェクトが**個人データ**を確実に保護するために何をしなければならないかを特定するのに、DPIA報告書は役立つ。また、**人道団体**が、プライバシーとデータ保護に対する利害関係者の権利を重要視し、プログラムに影響を受ける可能性のある人々やプログラムに関心を持つ人々の見解を求めることで彼らを安心させるのに役立つ。人道団体は、DPIA報告書、あるいは少なくともその要約を利害関係者が入手できるようにすることを検討すべきである。

79 付録I：データ保護影響評価（DPIA）報告書のテンプレートを参照

5.2 DPIA プロセス

このセクションでは、DPIAを実施するために必要なステップについて説明する。DPIAの実施にはさまざまなアプローチがある。以下のガイダンスは、様々なソースからのベストプラクティスを参考にしている。[80]

5.2.1 DPIA は必要か

個人データを収集、処理、保管、および/または他の組織に移転するいかなる組織も、DPIAの実施を検討すべきであり、その規模は組織がリスクをどの程度の重要度で評価するかによる。**人道団体**は、事前にすべてのデータ保護リスクを把握していない場合があり、その一部はDPIAの過程でのみ明らかになる可能性がある。**人道団体**は、リスクが非常に小さいとみなす可能性があり、そのためDPIAを行う根拠がないと見なされることがある。一部のリスクは、実在するが比較的小さいため、DPIAのプロセスと報告は相応に短いであろう。その他に非常に深刻なリスクもあり、**人道団体**は徹底したDPIAを実施したいと考えるだろう。万能なソリューションはない。

5.2.2 DPIA チーム

第2段階では、DPIAチームを特定し、TORを設定する。DPIAチームは、**人道団体**の**DPO**を含めるか、その見解を聞くべきである。実施されるDPIAの規模によっては、**人道団体**のIT、法務、業務、保護、政策、戦略計画、記録保管と情報管理、広報グループの専門家を入れることができる。DPIAを担当するチームは、**人道団体**の秘密保持に関する規則および行動規範のみならずデータ保護の要件にも精通している必要がある。計画されたプロジェクトに精通しているメンバーも含まれていることが重要である。TORの設定には、DPIAの期間、DPIAの範囲、協議する利害関係者、DPIA予算、および審査および/または監査に関してDPIA後に取られる措置の計画が含まれる。

80 David Wright、「*プライバシー影響評価の効率化*」、*The Information Society*（第29巻第5号2013）、pp.307-315.;NSWプライバシー・コミッショナー事務局、*ガイダンスNSWでのプライバシー影響評価*、2016年10月、シドニー、NSW、オーストラリア;ISO/IEC JTC 1/SC 27事務局。*情報技術 — セキュリティ技術 — プライバシー — 影響評価 —方法論*、ISO/IEC nth WD 29134:2017、2014年10月23日：https://www.iso.org/standard/62289.htmlを参照

5.2.3 個人データの処理の記述

DPIAチームは、評価対象のプログラムまたは活動の記載事項を作成すべきである。その記載事項には次の内容を含める必要がある。

- プロジェクトの目的
- プロジェクトの範囲
- 他のプロジェクトやプログラムとの繋がり
- プログラムまたは活動に責任を負うチーム
- 収集されるデータの種類の簡単な説明

データフローのマッピングは、いかなるDPIAにおいても重要なステップである。DPIAチームは、特定のプログラムや活動の情報フローをマッピングする際に、以下の質問を考慮すべきである。

- どのような種類の**個人データ**が、誰から、なぜ収集されているか。
- そのデータはどのように使用、保存、または移転されるか。
- **個人データ**にアクセスできるのは誰か。
- **個人データ**を保護するために、どのようなセキュリティ対策が講じられているか。
- そのデータはどのくらいの期間保持され、いつ消去されるか、データ保持の異なるレイヤーが特定されているか。
  これには、（1）X日までの機密データと見なされるデータの保存（2）そしてデータの長期保存のためのデータの名化、最後に（3）データの完全消去などの手順が含まれる。
- 機微情報を保護するために、データのクレンジングまたは**匿名化**が行われるか。

5.2.4 利害関係者との協議

DPIAを実施する上で利害関係者を特定することは重要である。利害関係者には、データ保護リスクに関心がある者、または影響を受けるすべての者が含まれる。利害関係者は、組織の内部および/または外部の者である。外部の利害関係者との協議の必要性と価値は、**人道団体**がリスクをどの程度深刻なものと考えるかにかかっている。**人道団体**にとって、利害関係者との協議は、考慮していなかったリスクやソリューションを特定する方法である。また、データ保護とプライバシーの問題に対する意識を高める方法でもある。利害関係者の意見は、DPIA報告書と勧告において考慮されるべきである。協議が効果的であるためには、利害関係者にプログラムに関する十分な情報を提供し、自らの見解を表明する機会を与えるべきである。利害関係者を関与させるにはさまざまな方法があるため、DPIAチームはプログラムや活動に応じて最適な方法を決定すべきである。

5.2.5 リスクの特定

リスクを特定する一つの方法は、プライバシー原則、それらの原則に対する脅威、脆弱性（脅威に対する感受性）、および脅威と脆弱性から生じるリスクを記載したスプレッドシートを作成することである。脆弱性のない脅威や脅威のない脆弱性はリスクではない。リスクは、脅威が脆弱性を不正利用する場合に生じる。

5.2.6 リスクの評価

データ保護リスク評価は、特定の事象の可能性または確率およびその結果（影響）を扱う。以下のステップの1つ以上を実行することにより、リスクを評価することができる。

- リスク、脅威、脆弱性を特定するために、内部および/または外部の利害関係者の意見を求めて協議する。
- 合意されたリスク基準に照らしてリスクを評価する。[81]
- 影響の可能性と重大性の観点からリスクを評価する。
- 必要性、適合性および比例性に照合して評価する。

5.2.7 ソリューションの特定

このステップには、プライバシーリスクを排除、回避、削減、または移行させるための戦略の策定が含まれる。これらの戦略には、技術的ソリューション、運用上および/または組織上のコントロールおよび/またはコミュニケーション戦略（例えば、意識を高めること）が含まれる。

5.2.8 勧告の提案

DPIAチームは、これまでのステップの結果に基づいて一連の勧告を作成すべきである。勧告には、一連のソリューション、組織レベルでの変更を含めることができ、さらに**人道団体**の全体的なデータ保護戦略、またはプログラムの全体的なデータ保護戦略に対する変更を含める場合もある。一連の勧告をDPIA報告書に含めるべきである。

5.2.9 合意された勧告の実施

DPIAチームは、DPIAの検討事項と調査結果に関する報告書を文書として作成すべきである。組織は定期的にDPIAを実施する必要があるため、DPIA報告書の長さと詳細度は大きく異なる。例えば、組織が調査目的で**個人データ**の公表を検討している場合、組織は、そのデータ保護影響分析の全ての詳細を反映した文書を作成すべきである。逆に、あるブランドのワープロソフ

81 危険度用語の定義については、ISO/Guide 73:2009（英語）*リスクマネジメント–用語：* https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

トから別のブランドのワープロソフトに切り替えるかどうかを決定しようとしている組織は、そのソフトが個人情報の処理に使われることを考えると、データ保護の問題を考慮すべきであるが、（ソフトウェアがクラウド環境で新しいデータフローを必要としない限り）詳細なDPIAは必要ないかもしれない。

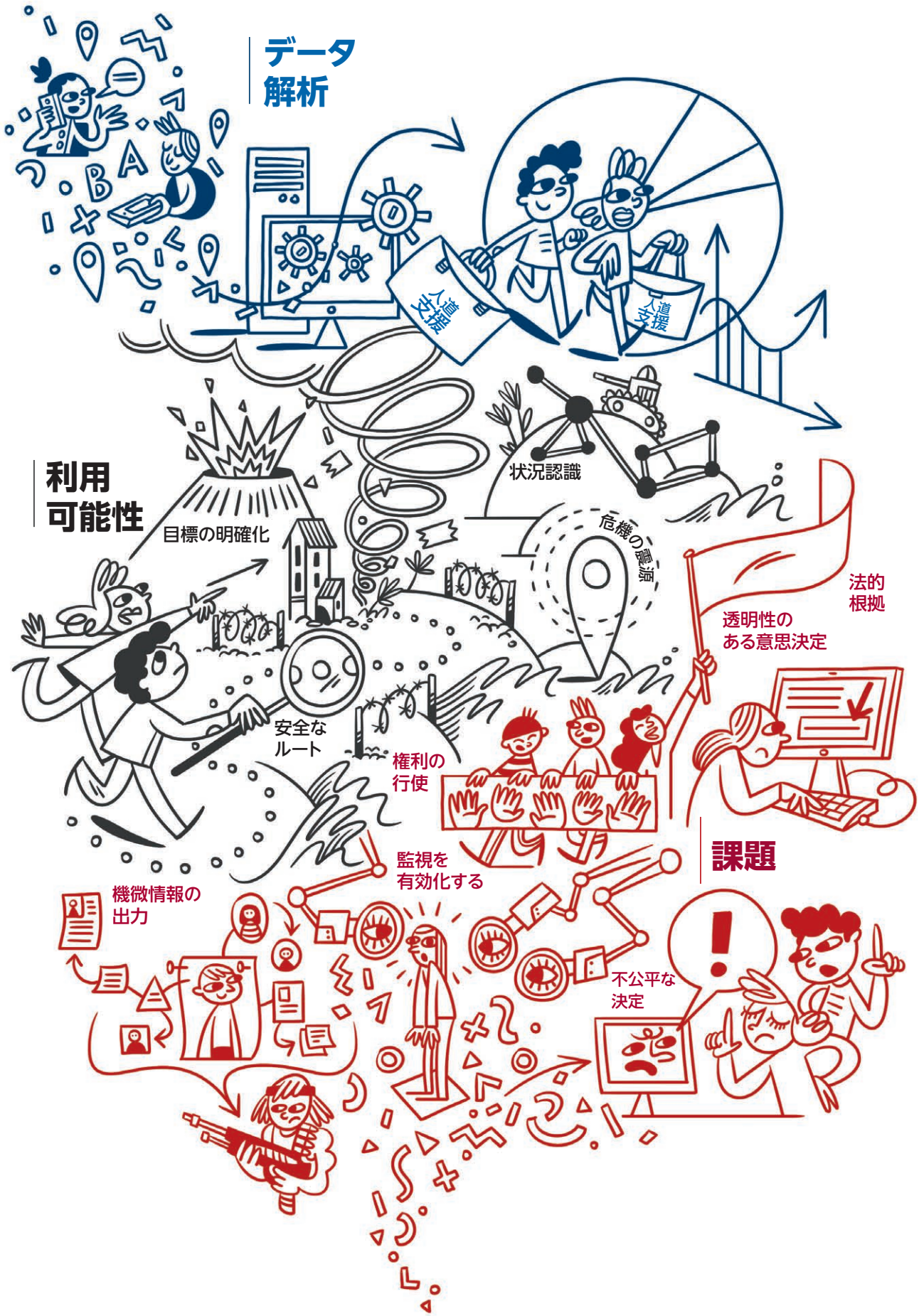
人道団体は、データ保護に関する決定事項を文書化し、実施することに加えて、そのデータ保護の意志決定の根底にある検討内容を理解することが、**データ主体**または公衆にとって有用であるかどうかを考慮すべきである。したがって、人道団体はその報告書（の全部または一部）を関連利害関係者と共有し、それによってデータ保護を重要視していることを示すことができる。DPIA報告書を共有することは、意識を高め、利害関係者からさらなる意見や提案を募る手段にもなるかもしれない。しかし、場合によっては、**人道団体**は、（例えば、物理的セキュリティ、活動の継続性、アクセスなどの理由で）機微情報が含まれているDPIA報告書の共有を拒否するかもしれない。そのような場合、**人道団体**は、DPIA報告書の要約または個人情報などが削除された編集版の共有を検討することができる。

5.2.10 DPIAの専門家による審査および/または監査の実施

人道団体は、組織のデータ保護担当官またはそのスタッフなどのデータ保護専門家が、DPIAの実施を審査または監査することを確実に保証すべきである。正確な監査のために、DPIA報告書には方法論セクションが含まれていなければならない。

5.2.11 プロジェクトに変更がある場合はDPIAを更新

DPIAの対象となる活動に重大な変更があった場合、あるいは新たなデータ保護リスクが生じた場合には、**人道団体**はDPIAを更新すべきである。


データ
解析
人道支援
人道支援
利用
可能性
目標の明確化
状況認識
危機の認識
法的
根拠
透明性の
ある意思決定
安全な
ルート
権利の
行使
課題
監視を
有効化する
機微情報の
出力
不公平な
決定

第6章

データ分析とビッグデータ

6.1 はじめに

人道支援は情報を元に決定されるため、**個人データ処理**による**データ分析**の実行には、**人道団体**にとって潜在的に大きな利点がある。[82]「**データ分析**」という用語は、多様な情報源から取得した非常に大量の情報（ビッグデータ）を組み合わせ、それらを分析し、高度なアルゴリズムを用いて十分な情報を得た上で意思決定する行為を意味する。ビッグデータは、大量のデータの収集と保存をサポートする技術力の向上だけでなく、データの価値を最大限に分析、理解、活用する可能性にも依存している（特に**データ分析**アプリケーションの使用による）。本章の趣旨に合わせ、「**データ分析**」と「ビッグデータ」という二つの用語は同義語として使用する。

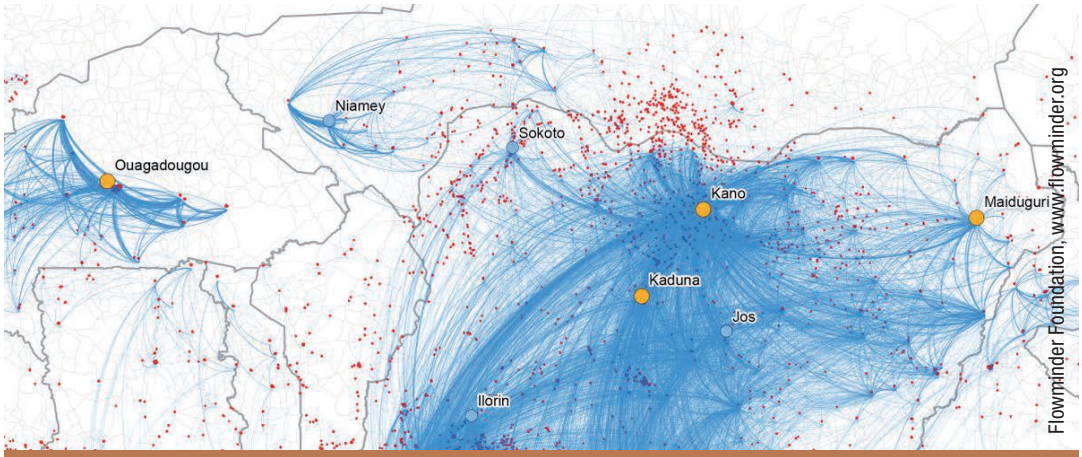
データ分析は、人道的活動に関連する潜在的な脅威の識別、備えの強化、困窮者または困窮者のカテゴリーの識別、あるいは伝染病、紛争、緊張関係および自然災害の潜在的な展開パターンの予測などの目的のために使用される。

データ分析によって、**人道団体**が実施する作業の効果を大幅に高めることが可能となる。具体的には、次のようなマッピングや識別が可能である。

- 紛争やその他の暴力的状況における被保護者を含む人道上の緊急事態における出来事のパターン
- 病気または自然災害の拡大、それによって起こりうる状況の展開を予測し、被害防止に備えること
- 危機の震源
- 安全なルート
- 個々の人道的な事案
- 人道的対応を必要とする可能性が高い脆弱な個人またはコミュニティ
- **人道上の緊急事態**で家族が離れ離れになった場合のマッチング

したがって、人道状況の**データ分析**に使用するアプリケーションには、広義の2つのカテゴリーが考えられる。第一に、一般的なパターンを認識するアプリケーション、第二に、**人道支援**に関連する個人または個人のグループを識別することを目的とするアプリケーションである。

82 国連人道問題調整事務所(OCHA)、*サイバー戦争時代の人道主義*（OCHA Policy and Studiesシリーズ、2014年）



西アフリカからの携帯電話データを使用して人口移動の地図を作成し、エボラウイルスがどのように広がるかを予測した

データ分析の使用は、誤解を招きやすい不正確な結果をもたらすとして、しばしば非難を引き起こしてきた。例えば、各事例に固有の特殊性を考慮に入れない恣意的で自動化された決定の正当化、デジタルフットプリントによるより効果的な監視を可能にするデータの生成、リバースエンジニアリングによる匿名性侵害の可能性と、その結果として**処理**の過程で含まれる個人の再識別につながる可能性である。ビッグデータのデータ保護への影響は、データ保護プライバシー・コミッショナー国際会議（International Conference of Privacy and Data Protection Commissioners）が2014年にモーリシャスで採択したビッグデータに関する決議で取り上げられている。[83]

データ分析に基本的なデータ保護の原則を適用する際にも、以下に関する懸念が生じる場合がある。例えば、1）**データ分析処理**が以前に予期されなかった目的のために**個人データ**を使用する限りにおける目的の明確化、2）**データ主体**に提供される情報が一般的に多くないことを考慮した透明性の要件、または3）適切な法的根拠として常に容易に識別できるとは限らない適法な**処理**の原則。[84]

本章の目的は、**データ分析**活動に従事している**人道団体**に指針を提供することである。データ保護の原則に従った**データ分析**の実行方法を説明するとともに、潜在的な課題を特定する。

83 International Conference of Data Protection and Privacy Commissioners, Resolution on Big Data, Fort Balaclava, Mauritius, 2014: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf?mc__phishing__protection__id=28047-br1tehqdu81ea0ar3q10

84 第2章：データ保護の基本原則を参照

この分析を始めるにあたり、データ保護に関連するいくつかの特性を明らかにする必要がある。

- *データソース*：まず、データの出所を特定することが重要である。**人道団体**が実施する**データ分析処理**の多くは、政府機関や公的記録、ソーシャル・メディア・ネットワーク、国勢調査データ、その他の公的に利用可能な人口動態調査など、公的に利用可能なデータに基づいている。その他の場合、**人道団体**は、電気通信やインフラ企業、インターネット・サービス、医療提供者、その他の商業組織などの民間企業と協力して、人道支援と災害対応を改善することができる。
- *緊急対応*：**データ分析**の成果は**人道団体**にとって確かな利益をもたらすが、必ずしも緊急事態下において使われるわけではなく、また関係者の重要な利益となるように活用されるとは限らない。例えば、事態が発生し対処された後、管理業務を支援するため、または今後の緊急事態への対応を改善するための戦略に貢献するために、**データ分析処理**が行われる場合がある。
- *精度*：データ分析に使用されるデータは必ずしも代表的で正確なものとは限らず、バイアスを含んでいる可能性があり、誤った結果につながる恐れがある。[85]匿名化されたデータや集約されたデータを利用することで、関係者のプライバシーへの侵害は小さくなるかもしれないが、精度に関するリスクが増大する可能性がある。
- *自動化された意思決定*：人間の介入や文脈的背景を伴わない**データ分析**は、誤った見解や決定につながることもある。[86]
- *他の目的のためのデータの再利用*：ビッグデータの利用でしばしば問題となるのは、**個人データ**が収集された目的以外の目的で利用できるかどうかという点ついてである。これは、データ保護法の下で問題となる。同法によって、一般的に**個人データ**は決められた目的のために収集され、そのような目的またはそれに準ずる目的のためにのみ処理され、関係する個人の**同意**またはその他の法的根拠なしに他の目的で再利用されないよう義務付けられているからである。
- *人道状況における**個人データ処理**によって生じるデータ出力の機微性*：ソーシャル・メディア・ネットワーク上のデータや一般に機微性が高いと考えられていないデータなど、ここで該当する状況以外では公開されているデータは、人道支援が必要な状況で**データ分析**の目的で処理されると、**機微データ**を生成する可能性があることを理解する必要がある。これは、痛みの軽減に関するデータを処理する際に、潜在的在的な被害者、暴力下の状況にある特定のグループに属する人々、または特定の病気を患っている人などへの差別または抑圧につながる個人のプロファイリングを可能にすることで起こりうる。このような場合、データの*平滑化*は、データ

85 UN Global Pulse, *Big Data for Development and Humanitarian Action: Towards Responsible Governance*, Privacy Advisory Group Report,（UNグローバルパルス、*開発と人道支援のためのビッグデータ：責任あるガバナンスに向けて*）p.12：http://unglobalpulse.org/sites/default/files/Big_Data_for_Development_and_Humanitarian_Action_Report_Final_0.pdf

86 同上、p.12年「データは通常、見解を正確に伝えるために代表的なものでなければならない。したがって、特定のデータセットまたはアルゴリズムにバイアスが含まれている可能性を考慮することが重要である。バイアスを回避するためには、データの質、正確性、およびデータ処理活動への人間の介入が極めて重要である。」

へのアクセスを許可しつつ、個人やグループのプライバシーを保護するために役立つ方法となり得る。[87]しかし、データは時間的・空間的に平滑化されるため、分析結果の明確さも損なわれることに留意が必要となる。

- **匿名化**：個人データの**匿名化**の有効性や、**データ分析**業務における**個人データ**の再識別の可能性については、人道的目的であるかその他の目的であるかにかかわらず、疑問が存在する場合がある。この場合も、データを*平滑化*し**匿名化**を補完することで、再識別を防ぐ別の保護層を提供できる。
- *規制の断片化*：多くの国がデータ保護法を制定し、多くの**人道団体**がすでにデータ保護指針とガイドラインを実施しているが、人道的危機の際にビッグデータが国境を越えて具体的にどのように規制されるかという問題は未解決のままである。[88]

データ分析が**人道支援**のために使われるとき、個人に対する影響は他の環境（例えば、商用環境で実行される**データ分析**）よりもはるかに深刻な場合があると認識することが重要である。例えば、分析されたデータが匿名化されている場合であっても、その結果は、個人のみならず、個人の集団に対しても深刻な悪影響を及ぼす可能性がある。**人道団体**は、公開するいかなるデータまたは**データ分析**から得た結果が、全体として集計されたものであっても保護対象とする人々に対して利用されるかどうかを検討すべきである。さらに、そのような潜在的に影響を受ける個人のグループは、必ずしも**データ主体**を含まない。多くの場合、目に見えない個体群は、データセットによって識別されたグループから切り離されることによって、突然可視化される。[89]したがって、脆弱な個人に対する**データ分析**の潜在的な影響の「大局」を常に念頭に置くことが重要である。

例：
人命の損失を避けることを目的とし、公共デモの発生地と流れを突き止めるためにソーシャル・メディア・ネットワーク上のツイートやその他の情報を抽出・分析し、当局に調査結果を公表することは、その後に同当局がそのような公共デモに参加した個人（あるいは参加しなかった個人）を識別するためにこれらの調査結果を使用することにつながり、識別された個人のグループに深刻な結果をもたらす可能性がある。

87 データの平滑化とは、データの重要パターンが目立つように、データセットからノイズを除去することである

88 UN Global Pulse, *Big Data for Development and Humanitarian Action: Towards Responsible Governance*, Privacy Advisory Group Report、（UNグローバルパルス、*開発と人道的行動のためのビッグデータ：責任あるガバナンスに向けて*）、前掲pp.7-9

89 同上、p.12

データ分析には、次のような**処理**シナリオが含まれる場合がある。

例1：公衆衛生従事者とコミュニケーションキャンペーンを支援するために、感情分析、トピック分類、ネットワーク分析を含む方法がどのように使用できるかを明らかにすることを目的とし、ソーシャルメディア、検索エンジンまたは電気通信サービス、ならびにニュースソースを介した公共コミュニケーションの抽出および分析

例2：通信信号または衛星データが緊急事態の対応管理をどのように支援できるかを実証するための、人道的な事案におけるインタラクティブなデータ可視化ツールの開発

例3：**人道団体**の市民報告プラットフォームに寄せられたメッセージの分析

例4：強制失踪のリスクのある個人を識別したり、行方不明者の所在を突き止めるための、ソーシャルメディア、携帯電話ネットワークのメタデータ、クレジットカードデータの分析

以下のデータセットが関連する可能性がある：

- パブリックデータセット（すなわち、政府が公表した公的記録または人々が意図的にニュース媒体またはソーシャルメディアを含むインターネット上において公表した情報のような、既に公に利用可能なデータセット）
- **人道団体**が保有するデータセット（例えば、配給受益者、患者、被保護者、行方不明者とその家族、国際人道法違反／人権侵害を報告している個人のリスト）
- 民間の第三者が保有するデータセット（例えば、集計または匿名化されているか否かを問わず、モバイル、電気通信、銀行および金融のプロバイダ、インターネット・サービス・プロバイダおよび金融取引データ、遠隔センサ・データ）
- **人道団体**、当局および／または企業（上記組織・団体を含む）のデータセットの組み合わせまたは全体

人道団体は、データ**処理**において以下の役割を果たすことができる。

- それぞれの組織内で保持されているデータの処理（**データコントローラ**として）
- **データ処理者**（すなわち、**人道団体**が保有するデータについて**データ分析**を行う営利団体）の採用
- **データ管理者**であり、データ管理者であり続ける営利団体に対して、人道目的のためにデータの分析を行い、**人道団体**に結論／分析結果を提供するよう要請すること。そのような結論は、対象全体の／匿名化されたデータ、または**人道支援**に関連する可能性のある個人を識別するデータのいずれかを含む可能性がある
- 共同**データ管理者**および／または**データ処理者**として、他の**人道団体**、公的機関および／または営利団体とデータセットを共有すること

これらのシナリオは、次のように表すことができる。

	人道団体が保有するデータ	**第三者（当局 / 法人）の保有データ**
人道団体がデータ管理者	**人道団体**は独自に分析を実行または外部の**データ処理者**にサービスを依頼してもよい	外部パートナーが**人道団体**にデータを提供して処理
第三者がデータ管理コントローラ	**人道団体**が外部パートナーにデータを提供して処理	**人道団体**の要請により、外部パートナーがデータを処理

人道団体と**第三者**は、同時に**データ管理者**と**データ処理者**の二つの役割を担う可能性に留意する必要がある。例えば、データは、**第三者**の組織によって保有され、**人道団体**の要請により**第三者**の組織によって処理され、その後**人道団体**によって他の利害関係者と共有されることがある。

6.2 データ保護基本原則の適用

データ分析のための**個人データ**の**処理**は、個人データ保護に関する重要な課題を提示している。このデータ処理が、収集された目的以外の目的のために**処理**される大規模データセットを使用する場合には、目的の制限、データの最小化、収集目的の実行に必要な期間のみのデータ保持など、データ保護の基本的概念に違反するおそれがある。本質的に、データ分析はオープンで制限のない**処理**環境を得意とする一方、**個人データ**保護は、制限され、明確に定義された**個人データ処理**を好む。このため、データ保護を**データ分析**に革新的に適用する必要がある。[90]

データ保護の基本原則は、**データ分析処理**を行う際に尊重されるべきベースラインを構成する。第2章：データ保護の基本原則で述べたとおり、**データ分析**を行う際に尊重されるべきデータ保護基本原則には、**処理**の公正性・適法性の原則、透明性の原則、目的制限の原則、データ最小化の原則、データの質の原則が含まれている。これらの原則のいくつかは**データ分析**の目的に適合するが、疑問や衝突を引き起こすものもあり、その結果、これらの原則を実際に適用する際には、**人道団体**が特別な注意を払わなければならない。

90 European Data Protection Supervisor（EDPS）, Opinion 7/2015, *Meeting the challenges of big data*, 2015年11月19日, p. 4: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

他の**人道団体**は、本章の議論を補完するビッグデータの取扱いに関する原則を策定している。[91]

本章のデータ保護に関する説明は、第1部で詳述した原則に基づいている。第1部では、この原則についてさらに詳しく考察している。

人道**データ分析**における最も重要な課題のひとつは、分析作業が、**人道団体**または第三者が異なる目的のために収集した既存のデータセット上で実行される可能性が最も高いということである。したがって、重要な問題は、想定される分析が収集の本来の目的に適合するかどうかを判断することである。適合すると判断された場合は、分析作業は既存の法的根拠に基づいて実行できる。そうでない場合は、その後の**処理**のための新しい法的根拠を見つける必要がある。

6.2.1 目的制限および追加処理

第2章：データ保護の基本原則で述べたように、**人道団体**は、データを収集する際に、データが処理される特定の目的を決定し、明示しなければならない。具体的な目的は、明確かつ正当なものであるべきであり、離散家族の再会、拘束されている個人の保護、法医学の活動、水と住居の保護など、あらゆるものを含むことができる。理想的には、想定される分析の目的は、データ収集の開始時に特定されるべきである。

追加処理に関しては、最初の処理に用いられた法的根拠にかかわらず、**人道団体**は、**追加処理**が歴史的、統計的または科学的目的のために必要な場合を含め、追加**処理**がそれらの目的に適合する場合には、収集時に最初に指定された目的以外の目的のために**個人データ**を処理することができる。[92]

データ分析の**処理**業務では、最初に収集された目的以外の目的でのデータ処理が必要になることがよくある。しかし、**データ分析**の目的は、最初の**個人データ**収集時にはほとんど予測できない。

分析操作が、データが最初に収集された目的に適合する**追加処理**とみなされるかどうかを確認するには、次の要因に注意する必要がある。

---

91 See United Nations Global Pulse, Privacy and Data Protection Principles: http://www.unglobalpulse.org/privacy-and-data-protection-principles; Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data, January 2017: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a

92 セクション2.6.3：追加処理を参照

- データが収集された目的と意図された**追加処理**の目的との間の関連
- **個人データ**が収集された状況、特に、**データ主体**と**データ管理者**との関係および**データ主体**のぐられる予想
- **個人データ**の性質
- **データ主体**に対する意図された**追加処理**の考えられる結果
- 適切な保護措置の存在

上記の要因を考慮する際、データ処理の人道的目的を念頭に置くべきである。一般的に、人道的目的は互いに適合する可能性が高い。データセットの使用における人道的価値のために、**第三者**のデータが当初収集された目的を超える目的のために処理される場合、**データ主体**が以下に詳細を説明するような新たなリスクや害にさらされない限り、データは適合性のある**追加処理**として人道的目的のために使用される場合がある。新たなリスクが生じる場合、または**データ主体**に対するリスクがその後の**処理**の利益を上回る場合には、人道的目的のためであっても、新たな**処理**の適合性は認めない。適合性は、事例の状況によって異なる。また、**処理**が、情報が関係する者またはその家族の利益を潜在的に害する場合、特に、その処理がそれらの者の生命、誠実性、尊厳、心理的もしくは身体的安全、自由またはそれらの者の評判を脅かすリスクが存在する場合には、更なる**処理**の適合性は認めない。これには、次のような結果が含まれる。

- 当局または第三者による嫌がらせまたは迫害
- 司法訴追
- 社会的・私的問題
- 自由の制限
- 心理的苦痛

例1：人道団体が、事故に対処している間に収集したデータセットがある。例えば、その後の人道上の緊急事態において援助を分配するために、避難のパターンを理解し、援助を事前に配備するために、収集後の段階でそのデータセットを使用することができる。

例2：電気通信事業者がそのサービスを加入者に提供する過程で収集したデータセットは、**人道団体**による**データ分析処理**において、加入者の**同意**なしには使用することができない。ただし、そのような個人（加入者）が病気の潜在的な保有者としてプロファイルされ、その結果、当局によって移動が制限される可能性がある場合に限る。このような場合、**人道団体**とその相手方である**第三者**機関は、データ集約のような緩和措置が、特定されたリスクの排除に十分効果があるかどうかを検討すべきである。

6.2.2 個人データ処理の法的根拠

分析の目的が処理の本来の目的と適合しないと考えられる場合には、分析のための新たな法的根拠を探すべきである。**データ分析**の使用において、**人道団体**は、以下の根拠のひとつ以上に基づいて**個人データ**を**処理**することができる。[93]

- **データ主体**または他の者の極めて重要な利益
- 特に国内法または国際法に基づく機関の権限に基づく公共の利益
- **同意**
- 機関の正当な利益
- 契約の履行
- 法的義務の遵守

同意の使用は、既に収集され、既存のデータセットに編成されている**個人データ**に対して行われる**データ分析**にとって問題となる。さらに、**データ主体**が**データ分析**のリスクと利点を十分に理解しているかどうかを確認することは、データ収集時には難しいかもしれない。**処理**作業が複雑であることと、データ収集時の段階ではそれらが意味することが完全には明確でない可能性があるからである。

人道団体への支援を目的としてソーシャル・メディア・ネットワークや携帯電話事業者によって提供される**データ分析**は、場合によっては**同意**に基づくものである。これは、当該ソーシャルメディアプラットフォームまたは携帯電話の事業者が、関連情報と**同意**要求と共にポップアップウィンドウまたはテキストメッセージによって意図された**処理**を**データ主体**に通知することができる場合である。しかし、このシナリオでは、個人の一部が**同意**を保留するならば、分析の正確性とその結果としての結論への影響を考慮する必要がある。

同意が確実かつ適切に通知されるように、提供される情報は、データ保護影響評価（DPIA）の結果（完了していれば）を考慮に入れるべきである[94]また、その情報は、経験から学ぶアプローチにおいて、データ利用の効果および**データ主体**への潜在的な影響をシミュレートするインターフェースを通じて提供されるかもしれない。[95]**データ処理者**は、**データ主体**が**同意**を撤回し、当初の目的と適合しないデータ**処理**に対応するための、容易でユーザーフレンドリーな技術的方法を提供すべきである。[96]

93 第3章：個人データ処理の法的根拠を参照
94 セクション6.7：データ保護影響評価を参照
95 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data*, January 2017, op. cit
96 同上

収集時に十分な情報が**データ主体**に提供され、**追加処理**の目的が適合している場合であっても、**同意**の妥当性を評価することが重要である。
この評価では、**データ主体**のリテラシーのレベルおよび**データ主体**のデータ**処理**のために**データ主体**が受けるリスクと損害を考慮すべきである。[97]

データを提供する個人または**データ主体**から**同意**を得ることができない場合であっても、それが**データ主体**または他の者の極めて重要な利益であることが立証される場合、すなわち、**データ主体**または他の者もしくは集団の生命、完全性、健康、尊厳もしくは安全に不可欠な利益を保護するためにデータ**処理**が必要である場合には、**個人データ**を処理することができる。さらに、公共の利益、団体・機関の正当な利益、法的義務を伴う契約またはコンプライアンスの履行などの追加的な法的根拠が、データ**処理**の根拠となりうる。

武力紛争その他の暴力的状況下で、**人道団体**の緊急活動を行う際の法的根拠としての極めて重要な利益の使用に関しては、**人道団体**によるデータ**処理**が**データ主体**またはその他の者の極めて重大な利益になると推定される事例がいくつか存在する（例えば、対象者の場合にデータが処理される時、または関係者の身体的および精神的インテグリティに対する差し迫った脅威がある時）。しかし、例えば管理上の目的のように、データ**処理**が緊急事態以外の状況で行われる場合には、死活的な利益の条件が満たされないことがある。

例：
データ分析が行政運営の目的または純粋な研究目的で行われる場合、極めて重要な利益の法的根拠は適用されない。

人道団体は、公共の利益の重要な根拠について、**個人データ処理**の適法な根拠としての使用が想定される分析作業と十分かつ密接に関連している状態がいつ引き起こされるのかを慎重に評価すべきである。**人道支援**を実施する権限が国内法、地域法または国際法に定められており、**同意**が得られておらず、法的根拠として極めて重要な利益をもたらすような緊急事態が存在しない場合には、公益的アプローチが**データ分析処理**の適切な法的根拠を構成する可能性がある。

人道団体は、**個人データ処理**の法的根拠としての公共の利益は、国内法または国際法の下での機関の権限に固有のものであるため、移転できないことを認識すべきである。第三者が機関に代わって**データ分析処理**を行うことができる条件（もしあれば）や、**国際的なデータ共有**に適用される条件については別途検討する必要がある。

97 国連開発計画(UNDP)、UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*：http://www.unglobalpulse.org/privacy/tools

人道団体はまた、**個人データ**が正当な利益になる場合には、**データ主体**の基本的権利および自由がその利益に優先されない限り、個人データを処理することができる。そのような正当な利益には、団体の活動をより効果的かつ効率的にするために必要な処理を含む場合があり、人道上の緊急事態を予測して援助や職員の事前配備を可能にするための後方支援の円滑化が含まれる。このような洞察はデータ分析から得ることができる。管理目的の**データ分析処理**もこのカテゴリに分類されることがある。

例：
人道団体は各地域の潜在的な従業員のデータベースを構築するために、従業員のデータの**データ分析処理**を行うことができる。

正当な利益は、処理の目的が人道的内容に限られる場合には、**人道団体**を手助けするために**データ分析**の実施を厭わない営利団体によって使用されることもある。

6.2.3 公正かつ適法な処理

公正かつ合法的であるためには、**処理**は法的根拠を必要とする。セクション2.5：データ処理の原則に詳述する。

データ分析は客観性ではなく潜在的な相関関係を扱うため、標本抽出、代表性、人口推計に関する懸念を含め、**処理**の公正性について多くの問題を提起する。研究者は、サンプルデータの代表性を理解するように注意し、広範で代表的なデータセットの使用を試み、潜在的なバイアスを報告すべきである。さらに、政策立案者は、意志決定時にこれらのバイアスについて説明すべきである。政策立案に使用される場合、不正確なデータや調査結果の誤った解釈に基づく分析は、有害かつ/または不公正な政策立案につながる可能性があり。また、**データ主体**は、潜在的に偏った、自動化された決定や一般化の影響を受ける可能性がある。

加えて、データ保護法における公正性要件は、一般的に、情報の提供、透明性およびデータ**処理**の影響に焦点を当てている。**データ分析**では、**処理**の複雑さと有意なリスク分析の実行の難しさを考えると、方法論（可能な場合はアルゴリズムを含む）についての透明性が非常に重要であり、そのため**データ主体**の情報に関する権利を超えて、アプローチの厳しさを独立して評価することができる。[98]透明性が個々のレベルでデータの機微性と矛盾する場合、あるいは**処理**の透明性が悪意のある行為者によるデータ処理システムのゲーミフィケーションを助長し、それによって**処理**の透明性を偏向する可能性がある場合には、透明性に関する意思決定過程で注意が必要である。

98 セクション6.3：データ主体の権利およびセクション6.5：国際的なデータ共有を参照

公平性の原則は、再識別のリスク評価は非識別化の前に実施されるべきであり、可能な場合には、**データ主体**または関連する利害関係者に評価の結果が通知されるべきであることを意味する。再識別の可能性が高い場合は、分析を実行しないか、方法論を調整するかを決定する必要がある。このような**データ分析**の状況を適切に評価するには、DPIAの実施が必要である。[99]

また、**データ分析**に関わるすべての従業員、請負業者またはその他の関係者が、データ保護リスクおよび倫理的調査手順について学ぶための訓練を受け、これらのリスクを軽減するための措置が取られることも重要である。

6.2.4 データの最小化

人道団体によって処理されるデータは、それらの収集・処理目的に対して適切かつ妥当であるべきである。具体的には、データ収集が過度に行われないようにし、匿名化またはアーカイブ化されるまでのデータの保存期間を必要最小限に制限することを意味する。収集および**処理**される**個人データ**の量は、理想的には、データ収集、データ**処理**または適合する**追加処理**の特定の目的を満たすために必要なもの、または他の法的根拠に基づいて正当化されるものに限定されるべきである。

一方、通常の**データ分析**では、最適な結果を得るために、かなりの期間を対象とした、できるだけ多くの情報を含む大規模なデータセットが必要になる。これは、上述したデータ最小化原則、つまり、**人道団体**によって収集されたデータセットの内容を収集時の分析目的に対して絶対的に最小に保つことを要求するこの原則に反する。したがって、データ収集の目的が可能な限り具体的に規定されており、元のプロジェクトのニーズを超えてデータを保持する場合は、目的が適合する**追加処理**によって正当化されることが重要である。

また、アーカイブに保管されたまたは匿名化されたデータセットも**データ分析**作業で使用することができるが、それらの使用は技術的および法的な課題を提起する。前者については、アーカイビングの制限によって処理能力が妨げられる可能性があるが、後者については、**処理**の結果が他の方法で非識別化された個人を再識別できないように特に注意する必要がある。匿名化または集計されたデータを**処理**する際の**データ分析**の出力の正確性についても質問する必要がある。したがって、**匿名化**または集計の方法およびレベルは、再識別のリスクを最小限に抑え、データが信頼できる結果を達成するために適切な品質と有用性を維持するように慎重に選択されるべきである。

99 セクション6.7：データ保護影響評価を参照

データ管理者および**データ処理者**（該当する場合）は、冗長データおよび限界データの存在を最小限にするために、データ分析の設計を慎重に検討すべきである。[100]

個人データは、収集された目的のために必要な一定の期間のみ保持されるべきである。初期保存期間の後、データを消去すべきかまたは目的を達成するためにより長期間保存すべきかについて評価を行うべきである。**データ分析**作業の可能性については、関連する保持ポリシーまたは情報通知で詳細に説明する必要がある。収集時に**データ分析**の**処理**が計画されている場合は、これを最初の情報通知に含める必要がある。また、想定される保存期間は、分析作業の実行に必要な時間をカバーする必要がある。

「適合する**追加処理**」のように、既存のデータセットに対してこの処理を実行する場合、[101]この**処理**は、初期収集の目的で許可されたデータ保全期間内に実行されるべきである。収集時に保全ポリシーで更新が考慮されている場合、初期保全期間の更新が行われ、「適合する**追加処理**」として分析を実施できる。

処理が既存のデータセット上で行われ、その**データ分析**の目的が初期収集の目的に適合しないとみなされる場合、**処理**のための新しい法的根拠を見つけ、保全期間を含む分析作業を説明した特定の情報通知の作成が必要である。

6.2.5 データセキュリティ

データ分析業務における情報保護に必要なセキュリティ対策の適切性を検討する際には、相互に関連があり、既存のデータセットを分析できる**処理**のアウトプットが、初期データセットよりも機微性の高いデータを生成する可能性があることを考慮する必要がある。個人やグループのプロファイリングを含むアウトプットは、悪意ある者の手に渡った場合、対象となる個人に有害であることが判明する可能性がある。

この場合、**データ分析**を行う**人道団体**は、アウトプットを保護するために、関連するリスクに十分で適切な安全対策を実施すべきである。[102]さらに、セキュリティの脅威に対する認識を高め、**データ侵害**を回避するためには、データセキュリティおよびデータプライバシーに関する定期的なトレーニングが不可欠である。

100 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data*、（2017年1月）前掲

101 セクション2.6.3：追加処理を参照

102 セクション6.2.5：データセキュリティおよびセクション2.8：データセキュリティと処理のセキュリティを参照

6.3 データ主体の権利

データ主体の権利については、セクション2.11：データ主体の権利に記載されている。情報受領、アクセス、訂正、削除、異議申立に対する権利は、効果的なデータ保護指針の重要な要素と考えられている。しかし、**データ分析**のための**個人データ**の**処理**には大きな課題がある。

データ主体者が情報を得る権利を行使すること（透明性の原則にも関連は、セクション6.2.：データ保護基本原則の適用参照）は、特に既存のデータセットで**処理**が行われている場合は、**処理**に関する詳細な情報を関係者に直接提供できない場合があるため、**データ分析**ではより困難である。したがって、例えば、関連する組織のウェブサイト、**データ主体**がおそらく使用する他のインターネットプラットフォーム、または他のマスコミュニケーション手段（新聞、リーフレット、ポスターなど）を使用することによって、情報提供の代替手段を探求することが重要である。**データ主体**への情報提供が困難または不可能であることが判明した場合、国内または国際的な情報リソース（単一事業者のウェブサイトよりも見つけやすい）の作成が提案されている。またグループ代表者への情報提供についても調査することが望ましい。

人道的**データ分析**に従事する組織には、**個人データ処理**の実践と内部データ保護ポリシーに苦情手続を組み込むことが推奨されている。これらの手順により、データの訂正と削除が可能になる。しかしながら、一定の個人的権利の行使は、**処理**の法的根拠により制限される可能性があることを認識すべきである。例えば、個人によるオプトアウトの要請は、上記の公共の利益という法的根拠に基づいて行われる**処理**の場合には遵守されないことがある。

人道団体は、人間の介入なしに人道支援プログラムに害を及ぼしたり、プログラムから排除されたりする可能性のある個人について、自動化された決定が行われないようにする必要がある。実際には、個人に悪影響を及ぼす可能性のある**データ分析**の結果に基づいて決定を下す場合、人間が常に最終的な意思決定者であるべきであることを意味する。

例：
援助が分配される場合、**データ分析**のアウトプットに基づいて、特定の地域または人々のグループを優先する（これらの地域や集団から取り残された人々に不利益をもたらす）決定は、常に人間によるクロスチェックと検証を受けるべきである。

6.4 データ共有

データ分析処理は、**データ分析**の実行前にデータ・セットが異なる**データ管理者**に属する場合、その完了後に結果および発見を第三者と共有できる場合の双方において、**データ処理者**または第三者とのデータ共有を含むことができる。したがって、**個人データ**と集計データまたは匿名データの両方が含まれる場合がある。データを共有する相手は、新しい**データ管理者**または**データ処理者**である場合がある。このデータ共有には、**処理**内容または**人道団体**の拠点に応じて、国境を越えたデータ、または**国際機関**によって若しくは国際機関との間で共有されるデータが含まれる。「共有」には、データが積極的に第三者に移転される状況だけでなく、第三者がデータにアクセスできるようになる状況も含まれることに留意することが重要である。国際要素を含むデータ共有および**データ管理者/データ処理者**の関係は、以下でより詳細に説明する。

6.5 国際的なデータ共有

データ分析は、異なる国に所在するさまざまな関係者との、日常的な**個人データ**の**国際的データ共有**を伴う。これには、上記のようなシナリオが含まれる場合がある。これらのシナリオの概要は次のとおりである。

- **データ処理者**、すなわち営利団体を雇用する**人道団体**が、当該**人道団体**が保有するデータに関する**個人データ**の実際の処理を行う。
- **人道団体**が、このデータのデータ管理者であり、今後も**データ管理者**のままである営利団体に対し、人道目的のために当該データの分析を実施し、**人道団体**に結論／調査結果を提供するよう要請する。このような結論には、集約／匿名化されたデータ、あるいは人道団体に関連する可能性のある個人を識別するデータが含まれる可能性がある。
- **人道団体**、公的機関および/または営利団体間でデータセットを共有する（共同**データ管理者/データ処理者**）。
- **人道団体**による処理のための人道団体への実際の共有（またはデータの転送）。

データ保護法は**国際的なデータ共有**を制限しているため、上述のように、**人道団体**は、**データ分析**が実施される際に国際的なデータ共有の法的根拠を提供するメカニズムを整備すべきである。[103]**データ分析**の複雑さ、データ主体が十分な情報を得られ、上記の権利を十分に行使できる状態にあることを確保することの難しさ、および**データ分析**が**データ主体**に及ぼす可能性のある広範囲な影響を考慮すると、**データ分析**のための**国際的なデータ共有**に先立ってDPIAを実施することが不可欠である。[104]実際DPIAはデータ共有に関連して考えられるリスクを識

103 セクション6.2.2：個人データ処理の法的根拠を参照
104 セクション6.7：データ保護影響評価を参照

別するための最も適切なツールであり、利用可能な最も適切なリスク軽減手段である（例えば、契約条項、行動規範、または実際にデータ共有を控えること）。[105]

さらに、**人道団体**が**データ分析**を実施または支援するためにサービス提供者を雇用する場合、これらの企業がデータを使用する目的について理解を深めるべきである。具体的には、自分自身のデータの分析を提供したり、**人道団体**のデータを**処理**したりする企業は、顧客に対する理解を向上させたり、さらなる顧客プロファイリングを行うために、商業目的でデータ処理の結果を利用するインセンティブを持つ可能性がある。したがって、これらの企業とのいかなる契約上の取決めにおいても、**処理**の目的が専ら人道的なものであり、かつ、その目的を維持しなければならないこと、およびサービス提供者が人道的な**処理**を商業活動から分離しておくことを完全に明確にすることが非常に重要である。サービス提供者がこの条件を尊重できるか否かについて疑義が生じた場合、**人道団体**は、処理に関与することを控えるべきである。これは、**人道支援**のための**処理**以外の処理は、**データ主体**に重大な影響を与える可能性があるためである。例えば、**人道支援**の潜在的受益者のカテゴリーを識別する分析結果は、信用供与の拒否、高い保険料、汚名、差別、あるいは迫害といった結果に誘導する場合がある。

人道団体は、暴力や紛争が発生した場合には、当事者が**データ分析**の結果にアクセスし利用することで、**データ主体**の安全性や**人道支援**の中立性を損なうような利益を得ようとする可能性があるというリスクにも注意を払うべきである。したがって、アウトプットが潜在的にセンシティブである場合には、**人道団体**がデータプロバイダに結果を開示せずに**データ分析**を機関内で実施するシナリオを考慮することが重要である。

6.6 データ管理者とデータ処理者の関係

データ分析を行う場合、**データ管理者**と**データ処理者**の役割が明確でないことが多い。したがって、どの関係者がデータ**処理**の目的と手段を実際に明らかにし（つまり**データ管理者**）、どの関係者が**データ管理者**から指示を受けるだけなのか（つまり**データ処理者**）を決定することが重要である。また、複数の団体が共同**データ管理者**と見なされる可能性もある。

105 第4章：国際的なデータ共有およびセクション4.4：個人にとってのリスク低減を参照

例1：データセットを共有し、自機関のリソースを使用して**データ分析**を実施する**人道団体**は、データ共同管理者とみなすことができる。

例2：データセットを共有しているが民間のサービス提供者に**データ分析**を委託している**人道団体**で、そのサービス提供者は調査結果を転送し自身の使用のための記録を保持しない場合は、データ共同管理者とみなされ、サービス提供者は**データ処理者**とみなされる。

データ分析作業に先立って行われるDPIAは、**処理**に関与するさまざまな関係者の役割を明確にするための適切な手段となり得る。

役割が明確に定義され、対応するタスクが割り当てられたら、データ**処理**関係者間で締結する必要がある関連契約を確定することが必要である。**人道団体**および/または国境および/または第三機関（民間または国家）の全てにわたるデータ収集または**国際的なデータ共有**は、一般的に契約条項によって対応されるべきであり、これは以下の理由から重要となり得る。

- さまざまな関係者間で役割を明確に割り当て、特に、**データ管理者**または**データ処理者**（または両方）としての役割を果たすのかについて通知する必要がある。
- それらには、各当事者が対象となるデータ保護義務の概要を含めるべきである。これには、国境を越えて移転される**個人データ**を保護するために当事者がとるべき措置を含める必要がある。
- データセキュリティ、当局からデータへのアクセスについて要請があった場合の対応（相手方当事者に対する異議または通知）、**データ侵害**への対処手順、**データ処理者**のデータ**処理**終了時におけるデータの返却／廃棄、および職員の研修を対象とする義務を含めるべきである。
- また、許可なくデータへのアクセスがあった場合には、関連する**人道団体**に通知するよう求めるべきである。

6.7 データ保護影響評価

データ保護影響評価（DPIA）は、適用可能なデータ保護規制と潜在的リスクのすべての側面を確実に対象とするための、プロジェクト設計時の重要なツールである。[106]DPIAは現在、多くの管轄や一部の**人道団体**で義務付けられている。しかし、リスクが明確でない新技術の場合は、実施はより困難である。**処理**の詳細と規格を明確にすることとは別に、DPIAは処理がもたらすリスクと軽減措置に焦点を当てるべきである。

106 第5章：データ保護影響評価（DPIAS）を参照

したがって、DPIAは**データ分析**作業の前に行う必要がある。特に重要なのは、国連のグローバルパルス・イノベーションリスク評価ツール（Global Pulse Data Innovation Risk Assessment Tool）のような、**人道支援**における**データ分析**のリスク評価のために特別に開発されたリスク評価ツールである。[107]

データ分析DPIAで対処すべきリスクには以下のものがある。

- 分析の目的がパターンを特定することである場合、**人道支援**に関連する個人の再識別
- 国際人道法または国際人権法違反の被疑者のデータが処理される場合における、人道支援活動の実行可能性および安全に対するリスク
- **人道団体**が当局または企業に特定のパターンまたはカテゴリーの関心を有する個人について要請する場合、そのような第三者が差別を行なったり、もしくは**人道支援**の中立性に不利益な影響を与えることに関心を持つおそれ
- **人道団体**が行う**データ分析**の結果で**第三者**がアクセスできるものが、営利目的の第三者および／または当局によって無関係な目的のために利用されるおそれがあるというリスク
- 暴力や紛争の状況にある当事者が、他の利害関係者に対して有利になるために**データ分析**のアウトプットにアクセスし利用する可能性があり、それによって**データ主体**の安全性と**人道支援**の中立性が損われるリスク
- 自身のデータを分析する、あるいは**人道団体**のデータを処理する営利目的のプロバイダーが、彼らの現在または潜在的な顧客への理解を深めるため、あるいは更なる顧客プロファイリングのために、商業目的で**処理**の結果を利用するという動機を持つ可能性があるというリスク[108]

データ分析のためのDPIAは、リスクから生じる得る損害の可能性、大きさおよび重大性を考慮に入れる。そのようなリスクと損害は、**データ分析**から予想される利益に対して、比例性の原則を考慮して評価されるべきである。[109]

具体的なリスク軽減措置には、以下のものが含まれる。

- 技術的手段としての**匿名化**
- 関係者の再識別の可能性を防ぐための法的および契約上の義務[110]

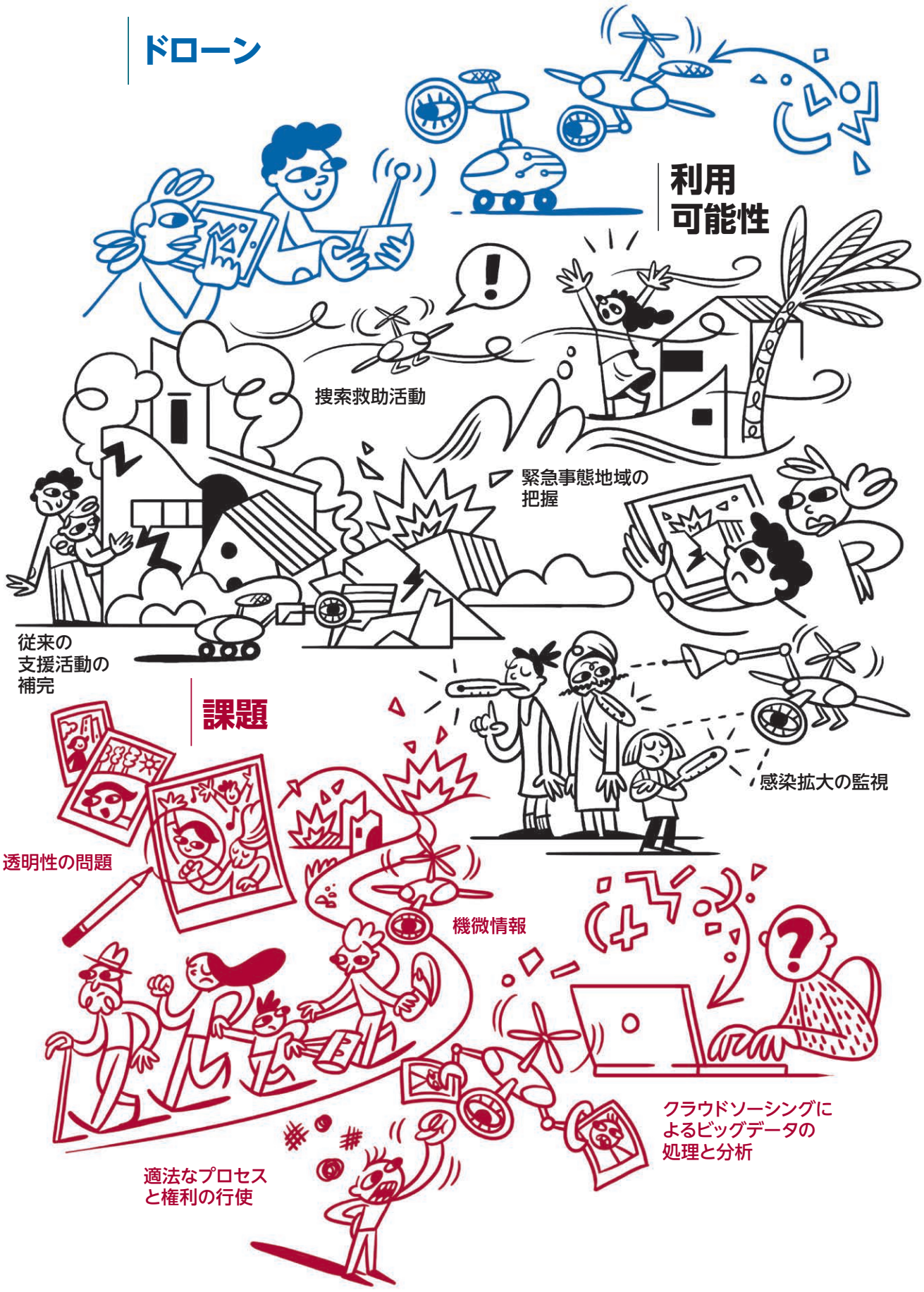
107 国連開発計画(UNDP)、UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*：https://www.unglobalpulse.org/privacy/tools

108 セクション2.3：集計化、仮名化、および匿名化されたデータセットを参照

109 国連開発計画(UNDP)、UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*：http://www.unglobalpulse.org/privacy/tools

110 Consultative Committee of the Convention for the Protection of Individuals with Automatic Processing of Personal Data (T-PD)、*Guidelines on the protection of personal data in a world of big data* (T-PD)、（2017年1月）前掲

ドローン


利用
可能性
捜索救助活動
緊急事態地域の
把握
従来の
支援活動の
補完
課題
感染拡大の監視
透明性の問題
機微情報
クラウドソーシングに
よるビッグデータの
処理と分析
適法なプロセス
と権利の行使

第7章

ドローン／無人航空機とリモートセンシング

7.1 はじめに

ドローンは将来有望で強力な新技術であり、状況把握、自然災害や人災への対応、救出活動を**人道団体**が改善するのに役立つ可能性がある。これらは、業務をより効率的、効果的、迅速かつ安全にすることにより、従来の有人支援を補完することができる。**ドローン**が正しく配備されれば、**人道支援**に重大な影響を及ぼす可能性がある。

ドローンは、遠隔操作されるか、または自律的に作動する小型の空中無人機または非空中無人機である。無人航空機（UAV）または遠隔操縦航空機システム（RPAS）とも呼ばれる。何に使用されるかに応じて、ドローンは多くの場合、カメラ、マイクロフォン、センサーやGPS装置を備えており、全てまたはいずれかが、**個人データ処理**を実行することが可能になる。

データ保護の観点から、**ドローン**の使用に関して様々な懸念が提起されている。しかし、**ドローン**の場合、この早い段階で明確にすることが重要なのは、注目されるのはドローンの利用そのものではなく、高解像度カメラやマイクロフォン、赤外線画像装置、無線通信を傍受する装置など、搭載されているさまざまな技術である。なぜならそれらの技術がデータ収集や**処理**に使用されるからである。この点に関して、本章で取り上げる考察は、衛星の使用にも、また、より一般的にはリモートセンシングにも適用できる。

本章では、**ドローン**の使用によって生じるデータ保護の問題のみに絞って取り上げる。他の問題や法律の分野も関連するかもしれないが、対象としない。例えば、航空管制にかかわる問題、飛行許可証、機器安全証明書などについては言及しない。

一般的に言って、今日の無人機の最も一般的な人道的使用は、状況把握を高めるための観測とデータ収集である。以下は、**ドローン**が人道支援の場で利用される、あるいは利用される可能性のある適用例の一覧である。

- 捜索救助
- 行方不明者の所在確認
- 航空画像の収集/状況認識/危機後の評価（例えば、送電線やインフラの状況調査、負傷者、家屋の破壊、死亡した家畜の数の把握など）
- 熱センサーを使った病気の広がりの監視
- 緊急住宅地域の把握
- ビデオや写真の提供によるリアルタイムの情報と状況の監視、即ち概況の提供
- 不発弾（UXO）の位置特定
- 自然災害や紛争地の地図作成
- **人道上の緊急事態**発生によって避難した人々の所在確認と追跡
- 遠隔地への医薬品などの救援物資の輸送
- メッシュネットワークの設立/信号の中継による通信ネットワークの復旧

災害の状況では「無人機は、さまざまな活用用途が考えられるが、例えば瓦礫の中から生存者を探し出したり、損傷したインフラの構造解析を行ったり、必要な物資や機材を届けたり、負傷者を避難させたり、火災の消火を助けたりすることができるため、救済作業者により良い状況認識を提供するために使用される可能性がある。」[111]**ドローン**はまた、**人道支援**の提供者にとって安全ではないと考えられる地域（例えば、放射能に汚染された場所や山火事の場所）の空中データを提供できる。[112]

しかし、**ドローン**は緊急事態に対応する際の直接的・間接的な情報源として非常に貴重なものではあるものの、どのような特定の場面で使用される前にも批判的評価を行わなければならない。ドローンの使用には重大なリスクが含まれることがある。[113]安全性の問題そのもの（例えば、稼働中の事故により、身体的な損傷や死亡を引き起こす可能性）は別としても、紛争が生じている場面で**ドローン**がスパイしたり、介入したりしていると受け取られるかもしれないので、運用者や**人道団体**の職員の安全を著しく損なう可能性があり、また地元の人々が自分たちのために無人機の使用に同意したと紛争当事者に見なされて、危険にさらされる可能性がある。

例：

人道団体は、地理的に広い地域にわたる航空画像の作成にドローンを使用することについて、自治体の長の承認を得ているかもしれない。しかし、**ドローン**の稼働中に、上記の地理的領域の特定の場所で行われている違法行為を偶然撮影し、その結果、その証拠を提供することがある。違法な活動を行っているグループは、ドローンが上空を飛んでいることを知って、承認を与えた自治体の長を見つけて懲らしめ、収集された証拠を破壊するために**人道団体**の運営者を探すかもしれない。

111 Joint Oversight Hearing by the Joint Legislative Committee on Emergency Management and the Senate Committee on Judiciary, *Drones and Emergencies: Are We Putting Public Safety at Risk?*、バックグラウンドペーパー、カリフォルニア州上院、2015年、p.2：https://sjud.senate.ca.gov/sites/sjud.senate.ca.gov/files/background_paper_-_drones_and_emergencies.pdf

112 アメリカ赤十字社およびその他、Drones for Disaster Response and Relief Operations、2015年4月、p.4：http://www.issuelab.org/resources/21683/21683.pdf

113 Delafoi F, Le drono, l' allie ambigu des humanitaires, Le Temps, 2016年4月11日：https://www.letemps.ch/monde/2016/04/11/drone-allie-ambigu-humanitaires
Think About Drones? Now We know, ICT Works、2016年2月22日：http://www.ictworks.org/2016/02/22/what-do-tanzanians-think-about-drones-now-we-know/

上述したように、**個人データ**保護の権利の潜在的な侵害についての懸念は、**ドローン**の使用によってではなく、**個人データ**を処理することができる搭載機器によって引き起こされる。**ドローン**に埋め込まれた、またはドローンに接続された情報技術は、さまざまなデータ**処理**および操作（例えば、データ収集、記録、整理、保管および収集されたデータセットの組合せ）を実行できる。通常、無人機によって収集されるデータには、ビデオ録画や、「識別された、または識別可能な自然人に関連する画像（個人、家屋、車両、ナンバープレートなどの画像）、音声、位置情報データその他の電磁的信号」が含まれる。[114]データの質によっては、個人を直接または間接的に特定することが可能である。これは、人間のオペレータによって、または自動的に、例えば、顔認識プログラム/アルゴリズムから画像をキャプチャすることによって、スキャンによってスマートフォンを探し出してそれを使用して個人を特定することによって、またはパスポート中の無線周波数識別（RFID）チップを使用することによって行うことができる。[115]

ドローン利用に対する**人道団体**のデータ保護対応を評価する際には、以下の要素が関連する可能性がある。

- **ドローン**の基本的な部分に埋め込まれている固有の識別子に基づいて、空中ドローンを特定の飛行と紐づけることが技術的に可能である。
- 多くの国では、**ドローン**の飛行許可と国当局が発行するリモートパイロットの免許が必要である。[116]
- （様々なレベルの分析と質の）画像データが、**ドローン**が収集する最も一般的な種類のデータである。
- 飛行高度および画像の捕捉角度もまた、捕捉された画像が直接的または間接的に個人を識別する可能性に重大な影響を及ぼす。
- 技術は急速に進歩し、現在の**ドローン**は非常に詳細な画像を撮影することができるが、ほとんどは個人の顔を撮影することはできない。識別できるようにするには、画像を他のデータセットに接続する必要がある。顔の識別が不可能な場合、位置および他のタイプのデータを使用することによって識別が可能であり得る。この文脈では、メタデータ（他のデータに関する情報を提供するデータ）の使用が重要である。
- 収集されたデータがどこに保存され、どのような種類の処理が実行されるかを確立することが重要である。この点で、**ドローン**と**データ分析**の間には相関関係がある。[117]

114 Article 29 Working Party, *Opinion 01/2015, on Privacy and Data Protection Issues relating to Utilization of Drones*, p.7：https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602

115 同上、p.14

116 Storyhunter Guide to Commercial Drone Regulations Around the World：World: https://blog.storyhunter.com/storyhunter-guide-to-commercial-drone-regulations-around-the-world

117 第6章：データ分析とビッグデータを参照

- 標準規格やその他の**ドローン**利用の仕様に関する多くの国際的なイニシアチブが現在進行中であり、中では特に人道目的のドローンについて検討されている。**人道団体**は、これらのイニシアチブの進展に注意を払い、その調査結果を業務に適用することが推奨される。[118]
- **人道団体**はドローンの運用を専門家に外注することが多いため、データ保護の問題が生じる（**データ管理者 / データ処理者**の関係、データへのアクセスなど）。
- ドローン関連の**個人データ処理**には国境を越えた移動が含まれることが多く、これにはデータ保護法に基づく法的根拠が必要となる。

しかし、これらの技術の変化のペースを考えると、上記の知見の多くは近い将来に大きく変化する可能性があることは注目に値する。

人道団体はまた、無人機の使用によって個人の識別が不可能な場合であっても、その使用が個人および共同体の生命、自由および尊厳に実質的な影響を与える可能性があることを認識すべきである。したがって**人道団体**は、**ドローン**で収集されたデータを、記録された個人がすぐには特定できない場合でも、保護するように対策するべきである。

例：
ドローンを使って避難した人々の流れを追跡するデータに悪意のある第三者がアクセスした場合、個人を識別することができなくても、脆弱な人々が危険に晒される可能性がある。

7.2 データ保護基本原則の適用

この章のデータ保護に関する説明は、第I部で詳述した原則に基づいており、さらに詳しく考察する。

7.2.1 個人データ処理の法的基盤

人道団体は、以下の法的根拠の一つ以上を用いて、無人機によって収集された**個人データ**を処理することができる。[119]

- **データ主体**または他の者の重要な利益
- 公共の利益、特に国内法または国際法の下で組織に与えられている権能から生じる場合
- **同意**
- 組織の正当な利益

118 例えば、*人道的UAV行動規範＆ガイドライン*：http://uaviators.org/docsを参照
119 第3章：個人データ処理の法的根拠を参照

- 契約の履行
- 法的義務の遵守

適法に**同意**を得ることは、**ドローン**を使って**人道団体**が行う仕事では実際には現実的でない可能性が高い。

例えば、個人が調査対象地域に出入りする自由がない場合、同意は「個人が自発的に与えた」ものにはならない。

これは、**同意**が、**人道団体**による無人機操作の文脈における**個人データ処理**の適法な根拠としては、一般的に非現実的であることを意味する。**ドローン**は、コミュニティへのアクセスが部分的であるか、まったくない場合に使用されるのがほとんどである。たとえそのようなアクセスが提供されたとしても、ドローン関連の**処理**によって影響を受ける可能性のあるすべての人々から**同意**を得ることはほとんど不可能であろう。加えて、**ドローン**が使用される状況によっては、窮地にあり人道支援を必要とする人々からの**同意**が自発的とみなされるかどうか疑問である。

ドローンは、ほとんどの場合、人々にアクセスすることが難しい、またはできない状況で使用される。アクセス可能であっても、ドローンに関連した処理の影響を受ける可能性のある全ての人の同意を得ることはほとんど不可能である。

「コミュニティの**同意**」あるいは「当局の**同意**」を手に入れるという考えは、**人道支援**における無人機の使用についても、個人の**同意**に代わる妥当な選択肢として示唆されている。これには、例えば、脆弱な個人のグループの代表者からのみ**同意**を得ることが含まれ、個人自身からは得られない。ただし、データ保護法の下では、**同意**は個人によって提供されなければならない。

例：
自治体の長や関係する国当局は、難民キャンプの地図を作成するために**人道団体**が**ドローン**を使用することに同意することができるが、その地域にいる人々はその**ドローン**のことを知らないかもしれないし、**個人データ**を**ドローン**によって収集されることを望まないかもしれない。

該当する個人から**同意**を得ることができない場合でも、**個人データ**は、それが**データ主体**または他の者の極めて重要な利益になる可能性があると**人道団体**が立証する場合、または他の法的根拠が適用される場合（7.2.1の記載のとおり）、人道団体によって引き続き処理されることができる。換言すれば、**個人データ**は、**データ主体**の、または他の人の生命、インテグリティ、健康、尊厳、またはセキュリティにとって不可欠な利害を保護するために処理が必要な場合には、処理が可能である。

第3章：個人データ処理の法的根拠で既に述べたように、**人道団体**の活動の性質およびその活動が緊急事態下で行われていることを考慮すると、状況によっては、人道的目的のために必要なデータの**処理**が**データ主体**の極めて重要な利益になるとみなされることがある。[120]

人道団体による**ドローン**の使用は、**データ主体**または他の人の極めて重要な利益の保護のために実際に必要であるかどうかを決定するために、ケースバイケースで評価されるべきである。生命、インテグリティ、セキュリティなどの優先的な私的利益の保護に対して**ドローン**が貢献できることは、証明されなければならない。あるいは、少なくとも、緊急事態の種類と規模や、**ドローン**の使用によってのみ改善することができる緊急事態に関する情報の不足に関する懸念を考慮した場合、貢献できることの可能性が高くなければならない。したがって、この法的根拠が存在するかどうかを決定するために厳格な基準が適用されるべきである。

120 2016年4月27日欧州議会及び閣僚理事会のEU規則2016/679、前掲書、前文第46項を参照

例：
人道団体による捜索救助活動における無人機の使用は、**データ主体**（すなわち、行方不明の人物）の極めて重要な利益を保護することになるため、この法的根拠の下で適格となる可能性が高い。

特定の緊急事態が存在しない場合、**人道団体**による地図作成作業での**ドローン**の使用は、この法的根拠のもとでは適切ではない可能性が高い。なぜなら、地図作成される地域で居住または移動している**データ主体**の重要な利益と直接的な関連がないからである。

人道団体は、公共の利益という重要な根拠が生じ、**ドローン**によって収集された**個人データ**を**処理**するための法的根拠として使用される場合には、慎重な評価を行うことが重要である。例えば、当該活動が国内法または国際法の下で確立された人道的権能の重要な一部である場合は、通常、対象となる（ICRC、IFRC、各国の赤十字・赤新月社、UNHCR、UNICEF、WFP、IOMなど）。

人道団体はまた、**ドローン**によって収集された**個人データ**が正当な利益になる場合には、その利益より**データ主体**の基本的権利および自由が優先しない限り、これを処理することができる。団体の正当な利益は、その使命を推進または支援するために**個人データ処理**が必要な場合に確立される。しかし、公共の利益または重要な利益が確立されない場合、特に**個人データ**捕捉の対象となる可能性のある個人に情報を提供することができなかったり、その個人がデータ保護の権利を効果的に行使できなかったりする場合には、**データ主体**の権利および自由が機関の正当な利益より優先されない状況を想定することは困難であると主張することができる。

例：
ある**人道団体**は、行動の成功を示すためにドローンを使い、例えばプロモーションビデオ用の映像を収集することができる。これは、正当な利益の法的根拠に該当する可能性があるが、ビデオに登場する個人の権利および自由の侵害の可能性について慎重に検討する必要がある。この点で、**データ主体**がどの程度情報を与えられ、どの程度その権利を効果的に行使できる（異議を申し立てる権利を含む）かどうかが重要な要因になる。

7.2.2 透明性 / 情報

透明性の原則は、少なくとも処理に関する最低限の情報が**データ主体**に提供されることを必要としている。さらに、**処理**に関する情報および通信は、容易にアクセスでき、理解しやすく、明確かつ平易な言葉で表現されるべきである。明らかに実用的な理由から、**ドローン**の場合、これらの要件を満たすことは困難である。情報のタイミングも重要であり、非緊急時には、ドローンの飛行前および飛行中に行うことが理想的である。共同体の指導者や当局の関与、または想定されている**データ主体**を対象としたメディアキャンペーン（例えば、ラジオ、新聞、公共エリアのポスター）の利用は、透明性に関する義務の履行に役立つ。

例：
透明性と情報に関する義務を果たすために、**ドローン**を利用する**人道団体**は、ドローンにマークやサインを付けたり、ウェブサイトを維持したり、ソーシャルメディア上で関連情報を提供する、利用可能なローカル通信チャネル（例えばラジオ、テレビ、新聞）を利用する、共同体の指導者と討論する、などができる。

7.2.3 目的制限と追加処理

個人データが収集される特定の目的は、明確かつ適合でなければならない。**人道団体**は、次のような目的のために**ドローン**を使用することができる。

- 捜索救助
- 行方不明者の所在確認
- 航空画像の収集、状況認識、危機後の評価（例えば、援助を必要とする避難民の所在確認、送電線やインフラの状況調査、負傷者数、破壊家屋や死亡した家畜の数の把握など）
- 熱センサーを使った病気の広がりの監視
- 抗議行動における群衆シミュレーション
- 緊急住宅地域の把握
- ビデオや写真の提供によるリアルタイムの情報と状況の監視、即ち概況の提供
- 自然災害や紛争地域の地図作成
- 不発弾の位置特定（UXO）
- **人道上の緊急事態**により避難した人々の所在確認と追跡
- 遠隔地への医薬品等の救援物資の輸送
- メッシュネットワークの構築、または信号の中継による通信ネットワークの復旧

また、第2章：データ保護の基本原則において、**人道団体**は、処理に用いられる法的根拠にかかわらず、その**追加処理**が当初の目的と両立する場合には、収集時に指定された目的以外の目的のために**個人データ**を**処理**することができることが規定されている。

7.2.4 データの最小化

個人データは、収集された目的に照らして適切で、関連性があり、かつ過度でない場合に限り、処理されるものとする。したがって、処理されたデータの必要性と比例性について厳密な評価が行われるべきである。[121]さらに、**ドローン**が人道的目的で使用される場合、データ最小化の原則は、適切な技術を選択し、データ保護とプライバシーの措置を意図的かつデフォルトで採用することによって尊重されるべきである。

例えば、**人道団体**は以下の選択肢を検討することができる。

- サービスおよび製品のプライバシー設定では、デフォルトで不要な**個人データ**の収集および/または**追加処理**を回避する必要がある
- **匿名化**技術を実施すべきである
- 顔/人間は自動的に（またはより脆弱な立場にある特定のカテゴリだけが）ブラー処理される
- 飛行高度または画像の撮影角度は、個人を直接特定できる画像を撮影する可能性を最小限にするために増加されるべきである

7.2.5 データ保全

ドローンによって処理された**個人データ**は、**処理**の目的に必要な期間を超えて長期間保管してはならない。すなわち、収集されたデータは、収集された目的が達成された時点で消去または匿名化されるべきである。保存と消去のスケジュールを採用することも推奨に値する。**ドローン**に搭載され、またはドローンに遠隔的に接続されるデータ収集装置は、データを保全する必要がある場合には収集される**個人データ**の保存期間を定めて設定することができ、その結果、もはや不要になった**個人データ**は定められたスケジュールに従って自動的に消去できるように設計されるべきである。

例：

人道団体が事件に対応するために**ドローン**によって収集したデータは、原則として、事件が首尾よく処理された場合には消去すべきである。**人道団体**がこの情報をアーカイブすることを望む場合（例えば活動記録の維持のために）、人道団体は、データの完全性とセキュリティを保護し、いかなる不正アクセスも防止するための適切な措置を講じるべきである。

121 第2章：データ保護の基本原則を参照

7.2.6 データセキュリティ

ドローンを運用する**人道団体**は、関連するリスクに適切な安全対策を実施すべきである。[122]**ドローン**に関しては、搭載されているデータベースや一時記憶装置の暗号化や、必要に応じてドローンと基地間の移動中のデータのエンドツーエンドの暗号化などが考えられる。

7.3 データ主体の権利

データ主体の権利は、既に第2章：データ保護の基本原則に記述されている。以下は、**人道団体**の**ドローン**利用に関する**データ主体**の権利についてのさらなる言及である。[123]

情報に対する権利に関する限り、ドローン関連**処理**にさらされる**データ主体**は、以下を提供されるべきである。

- ドローンの**データ管理者**とその代表者の身元
- **処理**の目的
- 収集した個人情報の類型
- データの受信者または受信者の類型
- データ主体に関するデータにアクセス権があることと、それらを特定し訂正する権利があること
- 現実的に可能である場合には、異議申立の権利があること

しかし実際には、**ドローン**を利用して**個人データ**を収集するに、上記の線に沿った情報を**データ主体**に提供することは、**人道団体**にとって実際には困難な場合がある。しかし、ケースバイケースで決定する様々な選択肢には、情報キャンペーン、公告、その他の類似した方法があると考えられる。ドローン事業者は、自らのウェブサイトや専用プラットフォームで情報を公開し、実施された様々な事業や今後実施される事業について対象者に知らせるべきである。遠隔地の場合や、対象者がインターネットにアクセスできる可能性が低い場合には、新聞、ちらし、ポスターに情報を掲載したり、手紙やラジオ放送で情報を提供したりすることができる。

データ主体への情報提供が実際に困難または不可能な場合、より広い地理的領域をカバーする可能性のあるドローンアプリケーションに関しては、個人が特定の**ドローン**に関連するミッションおよび運用者を特定できるようにするために、国内または国際的な情報リソース（単独事業者のウェブサイトよりも追跡しやすい）の作成が提案されている。

122 第2章：データ保護の基本原則を参照
123 セクション2.11：データ主体の権利を参照

個人が調査対象地域を避けることができない可能性があるため、**ドローン**の場合には難しいかもしれないが、**データ主体**は**処理**からオプトアウトする権利も持つべきである。さらに、**人道団体**は、**個人データ処理**慣行および内部データ保護方針において苦情手続きを実施することが強く奨励されている。これらの手順により、データの訂正と削除が可能になる。しかし、データ**処理**には、すべての個人の権利の行使を認めない法的根拠が存在する可能性があることを認識すべきである。（例えば、個人によるオプトアウトの要請は、上記の公共の利益という法的根拠に基づいて行われる処理の場合には、遵守されない可能性がある。）

最後に、情報にアクセスする権利に関する限り、あるデータ**主体**によるアクセスが他のデータ**主体**の**個人データ**を暴露したり、悪意のあるデータ**主体**が脆弱な個人（特定可能かどうかにかかわらず）に危害をもたらす行動をとったりするリスクを軽減するために、アクセスを制限すべきである。

データ**主体**の**個人データ**を含む航空画像または映像のみへのアクセスを制限することは、その性質上、他の多くの個人の**個人データ**を含む可能性があり、実用的かつ有意義に編集される可能性が極めて低いため、特に困難である。

例：
ドローンによって収集された航空写真の場合、データ**主体**によるアクセス権の行使には、申請者に関連しない他の顔や**個人データ**のブラー処理が必要となる場合があり、異議申立の権利には、同一の写真上にある申請者の**個人データ**を識別できないようにする措置が含まれるが、写真自体またはその写真上に写っている他の個人の**個人データ**の破壊は含まれない。

7.4 データ共有

人道団体間、あるいは人道団体と第三者との間で個人情報が交換される状況は、データ保護に関して特定して対応する必要がある。**ドローン**によって収集された情報は、収集の時点で共有することも、後の段階で共有することもできる。**人道団体**は、ドローン関連の作業をデータ**処理者**にアウトソーシングすることができる。上記のいずれかに、**個人データ**が国境を越えて共有されることが含まれる場合には、**国際的なデータ共有**に関連する問題にも対応する必要がある。[124]

124 第4章：国際的なデータ共有を参照

このような場合は、次の点を考慮することが重要である。

- 保護に関する該当**人道団体**の役割[125]
- 交換される画像またはその他の情報に個人情報が含まれるべきかどうか、または収集された画像の分析および評価の結論および所見のみを共有するだけで十分かどうか（未加工のデータ交換なし）
- 非自主的な、または偶発的なデータ共有（例えば、イメージがデバイスに保存され、デバイスが捕獲された場合）、または航空画像フィードが安全で暗号化されていない方法で送信された場合は、その影響を該当**人道団体**は考慮すべきである

クラウドソーシングは、**ドローン**によって収集された大規模なデータセットを**処理**および分析する一般的な方法である。その重要性は、航空画像や映像がしばしば巨大であり、これらすべての資料を見直すことが**人道団体**自身にとって不可能であるという事実に由来する。ますます一般的になってきている手法は、画像をオンラインで公開し、ボランティアを審査に招待して、例えば送電線の遮断、家屋の破壊、被災者や家畜を探してもらうことである。しかし、これは深刻な悪影響をもたらす可能性がある（例えば、悪意のある可能性のある第三者によるオンライン資料へのアクセスを可能にすること）。したがって、次のことを確認することが重要である。

- 画像にアクセスしているボランティアたちは、**人道団体**によって身元調査され訓練を受けている
- ボランティアは、裁量と守秘義務を網羅した条項を含む**処理**契約にコミットする
- その資料は、公開されていない。公開されなくとも調査されたボランティアのグループを越えて共有されない
- ボランティアはデータ**処理**の目的を理解するために適切な支援を受ける
- ボランティアの**処理**は適切に記録される

7.5 国際的なデータ共有

データ保護法は国際的な**データ共有**を制限しているため、**人道団体**は、第4章：国際的なデータ共有で議論されているように、**ドローン**が使用される際に、**国際的なデータ共有**のための法的根拠を提供するメカニズムを持つべきである。**人道団体**は、**国際的なデータ共有**を実施する前に、適用可能な法律の下で、かつ、自らの内部方針に沿った法的根拠があるかどうかを検討すべきである。そのような国際データ共有に先立ってDPIAを実施することは、そのような**処理**の合法性をさらに強化することができる。[126]

125 セクション7.6：データ管理者とデータ処理者の関係を参照
126 セクション7.7：データ保護影響評価を参照

7.6 データ管理者とデータ処理者の関係

ドローンを操作するときや、ドローンが収集したデータを**処理**するときに、**データ管理者**と**データ処理者**の役割が不明になることがある。前述したように、ドローン関連の**処理**では外注も頻繁に行われている。したがって、実際にデータ**処理**の目的と手段を決定する当事者（**データ管理者**）と、単に**データ管理者**から指示を受ける当事者（**データ処理者**）がだれになるかを決定することが重要である。また、複数の当事者が共同**データ管理者**と見なされる可能性もある。

例：
独自の目的のために職員に**ドローン**を運用させる**人道団体**は、そのような**処理**のための（唯一の）**データ管理者**である。

ドローンの運用を専門企業にアウトソーシングしている**人道団体**は、専門企業がドローンの操縦のみを任務としている場合、そのような**処理**のための（唯一の）**データ管理者**である。専門企業がこの運用の**データ処理者**になる。

ドローンを使用し、関連するすべての運用作業を収集されたデータへのアクセス権を持たない企業に外注することを希望する2つの人道団体は、共同の**データ管理者**となる。企業は、この運用の**データ処理者**となる。

7.7 データ保護影響評価

第5章：データ保護影響評価（DPIAS）で説明したように、DPIAは、データ保護規制と適用可能なリスクのすべての側面に確実に対応するためにプロジェクト設計時に使用する重要なツールである。DPIAは、**処理**の詳細と仕様を明確にすることとは別に、活動によってもたらされるリスクとその緩和措置に焦点を当てるべきである。この点で、ドローン運用の前にDPIAを作成することが重要である。

人道活動を阻害することを避けるために、**ドローン**を使用するためのDPIAのテンプレートを事前に開発すべきである。これらのテンプレートは、本章で概説されている特定のリスクと考慮事項に対応しており、容易かつ迅速に完成して実施できるものであるべきである。

バイオメトリクス


機微性のレベル
利用可能例
本人であることを証明する他の手段を用いずに個人を識別する
個人を効率的に特定
課題
データの最小化
データの信頼性
技術的な問題
不可逆性
同意取得が困難
人道的目的倫理的問題

第8章

バイオメトリクス

8.1 はじめに

国際標準化機構は、生体認証あるいは**バイオメトリクス**を「生物学的および行動特性に基づく個人の自動認識」と定義している。[127]したがって、**バイオメトリクス**は、指紋、虹彩スキャン、または人の歩き方などの行動特性を含むことができる測定可能で一意的な人間を表す特徴である。

バイオメトリクスデータの使用がデータ保護に及ぼす影響は、特にパスポート、IDカード、および渡航文書におけるバイオメトリクスデータの使用に関して、プライバシーデータ保護コミッショナー国際会議が2005年にスイスのモントルーで採択した『**バイオメトリクス**に関する決議』の中で強調されている。[128]

生体認証は、個人を効率的に識別し、人道援助の不正および/または誤用を防止することができる利点から、世界各地の人道団体が識別システムの一部として導入している。たしかに、非デジタルな代替手段となる紙ベースの識別メカニズム（身分証明書、配給カード、リストバンドなど）は、容易に紛失したり偽造されたりする可能性があり、照合するために相当な資源を必要とし、（その結果、重複と非効率性の可能性があり、）ほとんどの場合、自動**処理**ができないなどの制約がある。特定の状況において、これらの欠点は、（しばしば検証の追加手段として）生体認証システムの使用によって克服され得ることが示唆されている。バイオメトリクスデータは偽造がより困難であり、デジタル的に生成され保存されることで、現場での人道援助の効率的な管理を容易にし、**データ分析**や他のタイプの高度なデータ**処理**操作にも使用することができる。さらに、個人の特徴に焦点を当てることにより、**バイオメトリクス**は、それを適切に証明する他の手段を持たない個人の身元を確認することができる。これは避難民の場合によく見られることであり、個人の身元と尊厳を**人道支援**の中心に据えることができる。[129]

127 ISO/IEC 2382-37:2017 情報技術—用語，語彙—パート37：バイオメトリクス https://www.iso.org/standard/66693.html を参照

128 データ保護・プライバシーコミッショナー国際会議、パスポートおよびIDカード等におけるバイオメトリクスの利用に関する決議、スイス・モントルー、2005年：http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Biometrics-in-passports-identity-cards-and-travel-documents.pdf?mc_phishing_protection_id=28047-br1tehqdu81eaoar3q10を参照

129 Hugo Slim, *Eye Scan Therefore I am: The Individualization of Humanitarian Aid, European University Institute Blog*、2015 年：https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid/、Paul Currion,Eyes Wide Shut: The challenge of humanitarian biometrics, IRIN, 2015 年：http://www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics 等を参照

しかし、これらの約束は**バイオメトリクス**識別システムの実際の展開では必ずしも満たされていない。**バイオメトリクス**を実施するいくつかのプロジェクトは、関連するシステムの信頼性に関してかなりの問題に直面していると報告されている。[130]個人の指紋が常に読み取り可能であるとは限らないという事実などにみられる本質的な制約は、プロジェクト実施の際のさらなる困難となる。倫理的な問題も、例えば、国の識別システムにおけるバイオメトリクスデータの使用や、一部の国におけるそのようなシステムの歴史的背景にある問題によっても生じる可能性がある。[131]さらに、国の法執行と国家安全保障の目的のためのバイオメトリクスデータへの関心から、**人道団体**は、人道活動を超える目的のために国や地域の当局とのデータ共有がますます強いられる環境に置かれるかもしれない。バイオメトリクスデータが関心を集めていることは、第三者による不正アクセス、すなわちハッキングの多大なリスクに直面していることを意味する。

人道団体は、現金やバウチャーを通じて提供される援助を含め、人道援助の分配のために登録しなければならない避難民に関するデータの収集と管理のような**処理**作業にバイオメトリクス技術を使用することができる。[132]

現在のところ、上記**処理**に用いられる技術は、主に、自動指紋認識システム（指紋は収集されるバイオメトリックデータの主要な形態）および虹彩スキャンを含む。しかし、以下のようなバイオメトリクスデータの他の形態も考えられる。

- 手掌静脈認識
- 音声認識
- 顔認識
- 行動特性

人道団体によるバイオメトリクス技術の利用の利点には、以下のものが含まれる。

- 正確な個人識別
- 不正腐敗との戦い
- ドナーの支持と計画の信頼性の向上（上記の点の結果として）
- 識別データのデジタル**処理**による効率化
- 個人の物理的保護の効率化/失踪リスクの最小化
- 個人の身元と尊厳を**人道支援**の中心に据えること
- 個人の自由な移動の権利を高めること
- 第三国への個人の再定住の促進
- 銀行口座の取得を可能にすること

130 Gus Hosein と Carly Nyst、*Aiding surveillance: An exploration of development and humanitary aid initiative is enabling surveillance in development countries*、IDRC/UKaid、2014年、p.16

131 同書、p.19

132 第9章：現金給付プログラムを参照

しかし、多くのリスクと課題も同様に提起されている。

- データ（誤一致のリスクを含む）および/またはシステムの信頼性および精度 – 生体認証システムの品質は、最終的には、使用される検知装置の品質および提供される生体認証の品質に左右される
- 内在する技術的課題（例えば、指紋が摩耗している受益者の場合の指紋の判読不能）
- 生体認証情報は固有のものであり変更できない
- 倫理的問題（文化的感受性、受益者の認知および/または監視に関する懸念）
- 機能の目的外への拡張（非人道的目的を含む、当初指定された目的以外のために同一のシステムが使用される）
- 各国当局や地域当局（ドナーを含む）が**人道団体**が収集したバイオメトリクスデータを入手しようとして圧力をかける可能性があり、その場合、厳密な人道目的以外の目的（例えば、法執行機関、治安、国境管理または移民動向の監視）に使用されるリスクがある

したがって、**人道団体**がバイオメトリクスデータの利用の必要性を慎重に分析・検討し、理想的にはバイオメトリクスデータの利用に関する公共政策を通じて、データ保護の要件に適合する方法でバイオメトリクスデータをどのような意図で利用するかを明確かつ透明性を持って規定することが非常に重要である。[133]

8.2 データ保護基本原則の適用

バイオメトリクス技術の使用は、重大なデータ保護上の問題を提起する。生体認証情報は個人データとみなされるため、データ保護法制の対象となる。例えば、EUの一般データ保護規則（GDPR）はバイオメトリクスデータを明確に規制しており、「自然人の身体的、生理的または行動的特性に関連する特定の技術的**処理**から生じる**個人データ**であって、顔画像または指紋データのような当該自然人の固有の識別を可能にし、または確認するもの。」と定義している。[134] 多くの法制度において、生体認証情報は、「**機微データ**」とみなされる。[135]したがって、この種のデータの処理には特別に詳細な要件が適用され、これらの要件が満たされない場合には**処理**の適法性に直接影響する。

133 例えば、ICRCによる生体情報の取扱いに関する方針等について、https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/を参照

134 2016年4月27日欧州議会及び閣僚理事会のEU規則2016/679、前掲書、第4条（14）

135 例えば、EUでは、バイオメトリクスデータは個人データの特別なカテゴリとみなされる：2016年4月27日欧州議会及び閣僚理事会のEU規則2016/679、前掲書、第9条

このような高いレベルの保護は、生体認証情報の次のような特別な特徴によって正当化される。

- 固有であり変更できないため、なりすましのリスクが増大する。および
- 技術の発展によって**処理**が予測不可能な方法で影響を及ぼす可能性がある。なぜなら、現在収集されている個人のバイオメトリクスデータの種類によっては、将来的に個人に関するより多くの情報（例えば、網膜に関する情報によって遺伝子、人種、健康状態、年齢）が明らかになる可能性がある。

したがって、本ハンドブックの根底にある基本的な前提として、**人道支援**においては、特別な保護を必要とする**個人データ**の明確な分類を確立することは(ある緊急事態の状況では機微性の低いデータでも別の緊急事態の状況では機微性が高い場合があるため）不可能であるとする一方で、バイオメトリクスデータは、状況や事情にかかわらず、特別な保護を必要とするという前提がある。このため、データ保護影響評価（DPIA）は**バイオメトリクス**を使用する前に必ず実施すべきである。

DPIAを実施する際、**人道団体**は、異なる種類のバイオメトリクスデータが異なるレベルの「機微性」を有する可能性があるという事実を考慮に入れるべきである。バイオメトリクスデータの機微性は、上に述べた理由によりいくつかのカテゴリで高い場合でも、他のカテゴリと比べると高かったり低かったりすることがある。例えば、指紋は、非意図的に(例えば、手作業を伴う重労働で)、あるいは意図的に、摩耗したり削除されたりすることがあり、その結果、このタイプのデータは、他よりも機微性が低くなる。一方、虹彩スキャンは、個人の識別だけでなく非常に機微性の高い情報の抽出を可能にする可能性がある。さらに、ある種のバイオメトリクスデータは、手のひら静脈認識のように、**データ主体**の直接の参加によってのみ収集および読み取りが可能であり、したがって、この種のデータは他のデータよりも機微性が低い。虹彩情報のような他のカテゴリのバイオメトリクスデータは、離れたところから読み取ることができるので、特に機微性が高い。[136]

したがって、上記の個人情報**処理**に関する法律が適用されない場合であっても、バイオメトリクスデータの**処理**には特別なリスクがあり、より一層の注意が必要である。したがって、**個人データ処理**は事前審査が必要であり、この事前審査は、後述するように、実施前、実施中、実施後に特定の保護措置（例えばセキュリティ対策の強化）を講じる必要があるかどうか、または、潜在的なリスクを考慮してバイオメトリクスデータを使用すべきであるかどうかを決定するために行われる。

136 例えば：*How Facial Recognition Might Stop the Next Brussels*、2016年3月22日、http://www.defenseone.com/technology/2016/03/how-facial-recognition-might-stop-next-brussels/126883/を参照

本章のデータ保護に関する分析は、第一部で提示した原則に基づいており、第一部ではこの原則について詳述している。

8.2.1 個人データ処理の法的基盤

人道団体は、以下の法的根拠の一つまたは複数を用いて**個人データ**を処理することができる。[137]

- **データ主体**または他の人の極めて重要な利益
- 公共の利益
- **同意**
- 組織の正当な利益
- 契約の履行
- 法的義務の遵守

第3章個人データ処理の法的根拠で述べたように、**同意**は**個人データ処理**を行うための望ましい法的根拠であるが、人道支援を必要とする状況においては、**同意**の有効性を証明することは困難である可能性がある。しかしながら、バイオメトリクスデータは**機微データ**とみなされるため、**データ管理者**は個人の**同意**を得るべきである。加えて、生体認証情報は関係する個人から直接収集されるのであり、データ収集と**処理**の他の方法とは対照的に、**人道団体**がバイオメトリクスデータを使用するための**同意**を得ることは一般的に可能であろう。しかし、第3章：個人データ処理の法的根拠でも示される次のような理由で、バイオメトリクスデータ処理のための明確で、自由意思に基づき、十分に情報を得た上での文書による**同意**を取得することは、常に可能であるとは限らない；

- 意識のない患者の場合のように、それを提供する個人の身体的な障がい（例えば、患者の医療ファイルのロックを解除するためにバイオメトリクスデータが必要で、他の正当な権限と組み合わされる場合）
- 救命援助を提供することが優先される緊急事態の最初の段階で、十分なカウンセリングを確保するための時間とスタッフが不足する場合
- 個人の脆弱性および/または同意を提供する法的能力の欠如
- データの高度に技術的な性質および不可逆性により、**同意**するときに理解または熟慮することが困難なリスクに個人がさらされる可能性がある場合。特に、**同意**の時点では予測できなかった新たなリスクをもたらすような形で科学技術が発展する可能性（例えば、個人の虹彩のスキャンから遺伝情報にアクセスできるようになる）を指す

137 第3章：個人データ処理の法的根拠を参照

ヨルダン・アンマンにあるカイロ・アンマン銀行の支店でシリア難民が彼女の虹彩をスキャンし、毎月の現金支援にアクセスしている

- 援助や保護を受けるための代替的な方法について現実的な選択肢がない場合（例えば、あなたやあなたの家族が生き残るために人道援助に依存している場合、またはあなたが現在いる国に合法的に滞在するために登録する必要がある場合には、あなたがバイオメトリクスデータの収集を拒否する機会は極めて限られる）

個人すなわち**データ主体**から有効な**同意**を得ることができない場合でも、実質的な公共の利益のために必要であること、または、データ主体若しくは他の人に極めて重要な利益のために必要であること、すなわち**データ主体**若しくは他の人の生命、インテグリティ、健康、尊厳、安全を保護するためにデータ**処理**が必要であることを立証できる場合、**個人データ**は当該**人道団体**によって引き続き処理されることができる。

場合によっては、**人道団体**の業務の性質および武力紛争その他の暴力を伴う事態における緊急事態が、人道団体による**個人データ**の**処理**が**データ主体**もしくは他の人の極めて重要な利益になるとの推定につながる（例えば、対象者の心身のインテグリティに対する差し迫った脅威の場合）。

困難な状況においては、**バイオメトリクス**が個人を効果的に特定できることから、**人道団体**が対象者の**同意**を得ることができない場合、**データ主体**または他の人の極めて重要な利益そのものが、関連する**処理**の妥当な代替的な法的根拠となる可能性があると主張することもできよう。

さらに、受益者の極めて重要な利益を促進することが、生体認証システムの使用を正当化すると主張できる状況も想像することができる。例えば、**人道支援**のために利用可能なリソースが限られており、援助が他の個人グループに不正に過剰供給されているために、一部の潜在的受益者が必要不可欠な支援を受けられない場合、生体認証システムは正確な資源配分と不正防止を促進することができる。その一方、バイオメトリクスデータは援助の分配のために必須ではないと主張することもできる。バイオメトリクスデータの利用は、どちらかというと**人道団体**が効率的かつ効果的な方法で業務を遂行する必要性に応じたものであり、資金の重複配付や浪費を避けるものであり、関係する個人の極めて重要な利益に応えるものではない。

さらに、バイオメトリクスデータのライフサイクルを明らかにすることが重要である。これらのデータが個人の生涯を通じて使用されることを意図しているならば、その個人の極めて重要な利益を法的根拠として適用できない可能性が高いので、代わりに**同意**を得るべきである。

この分野で最終的に考慮しなければならないのは、人道上の緊急事態によって影響を受けた人々の明確で一義的な身元の確立を可能にするバイオメトリクスデータの本質的な価値、およびそれが、個人の権利の行使を可能にすることを含め、個人の尊厳を回復および/または強化する役割を果たす可能性についてである。この観点から考慮すると、**データ主体**としての個人の極めて重要な利益が問題の焦点になる可能性がある。

場合によっては、公共の利益という重要な理由が、バイオメトリクスデータを**処理**するための法的根拠として使用されることがある。例えば、問題となっている活動が国内法または国際法で定められた人道的任務の一部である場合は、通常、そうである。該当する場合として、受益者の**同意**を得ることができない場合の援助の分配が含まれる。**データ主体**または他の人々の生命、安全、尊厳およびインテグリティが危険にさらされている場合には、極めて重要な利益が最も適切な法的根拠となり得ることに留意することが重要である。

人道支援を遂行する権能が国内法、地域法または国際法の中で確立されており、上述の事例のように**同意**および/または極めて重要な利益が適用できない場合には、公共の利益と言う点が、バイオメトリクスデータ**処理**のための適切な法的根拠と認められうる。

人道団体はまた、**個人データ**の処理が団体の正当な利益となる場合には、当該利益が**データ主体**の基本的な権利および自由によって優先されない限り、処理することができる。このような正当な利益には、人道支援の提供の効率性を高めることや、コスト削減と重複および詐欺のリスク削減のために必要な処理を含むことができる。しかしながら、バイオメトリクスデータが潜在的にかなり立ち入った目的のために使用され得ることを考慮し、またバイオメトリクスデータには上記で強調した特徴があることから、**データ主体**の権利および自由よりも、上記に述べた正当な利益が必ず優先するということは疑問視されうる。**データ管理者**の正当な利益が法的根拠として使用される前に、**データ主体**の基本的権利および自由に対するリスクおよび起こり得る干渉

の慎重な分析が、関連するDPIAに含まれなければならない。これは、第三者がデータへの無許可アクセスを得る可能性があるリスクが想定される場合、または第三者に機関がこの高度な**機微データ**を提供するよう圧力をかけ、人道的な目的以外に使用される可能性がある場合には特に重要である。

8.2.2 公正かつ適法な処理

個人情報保護法制の下では、**個人データ**を適法かつ公正に取り扱う必要がある。[138]「**処理**の適法性」とは、適切な法的根拠の特定をいう。公正性の要件は、一般に、情報の提供およびデータの使用に関連する。バイオメトリクスデータ**処理**に関与する人道団体は、これらの原則が**処理**の全段階で適用される必要があることに留意すべきである。

8.2.3 目的制限と追加的処理

第2章データ保護の基本原則で述べたように、**人道団体**は、**個人データ**の収集時に、データが処理される特定の目的を決定し、設定すべきである。具体的な目的は、明示的かつ正当なものであるべきであり、人道支援の提供、離散家族の再会、拘束された個人の保護、医療支援の提供、法医学の活動などの人道的目的を含むことができる。

処理の目的は、収集時に個人に明確に伝達される必要がある。生体認証情報は個人を識別するために使用されるので、**処理**の目的は、本人確認の当初の目的（例えば、本人確認そのもの、現物給付や現金支払いを通じた援助の支出）に基づくべきである。

個人データの**追加処理**は、その当初の目的と両立する場合には、収集時に最初に指定された目的以外の目的のために処理することができる。これには、その処理が歴史的、統計的または科学的目的のために必要な場合を含む。**追加処理**が最初にデータを収集した目的に適合するかどうかを確認するために、以下の要因に注意を払うべきである。

- データが収集された目的と意図された追加処理の目的との間の関連
- **追加処理**がどの程度人道的な性質のものであるか
- **個人データ**が収集された状況、特に**データ主体**と**データ管理者**との関係
- **個人データ**の性質
- **データ主体**にとっての**追加処理**の潜在的な結果またはリスク
- 適切な保護措置の存在
- データが今後どのように利用されるかに関する**データ主体**の合理的な期待

138 セクション2.5.1：公平性の原理と処理の適法性とセクション8.2.2：公正かつ適法な処理を参照

例：
生体認証システムが**人道団体**による援助分配のために配備され、関係する個人がこれに同意した場合でも、参加者が追加の目的に同意しない限り、参加者のデータを相互参照の目的で**人道団体**のドナーに伝送するために同じシステムを使用することはできない。

上記の要因を考慮する際には、追加**処理**の目的の人道的側面が特に考慮されるべきである。

上述したように、[139]より広い意味での「人道的目的」にあたる目的は、さらなる**追加処理**活動と両立する可能性が高い。しかし、新たなリスクが関与している場合や、対象者のリスクが**追加処理**の利益を上回る場合には、この限りではない。評価は、事案の状況次第であり、特に、対象者の生命、インテグリティ、尊厳、心理的または物理的な安全、自由または評判を脅かすリスクがその**処理**によって生じる場合には、その情報が関係する者またはその家族の重大な利益に反するおそれのあるあらゆる**処理**のリスクの分析を含む。

同様に、非人道的目的のための**追加処理**（例えば、法執行や国家安全保障、セキュリティチェック、移民の流れの管理、難民申請など）は、**人道団体**によって行われる最初の取扱いと両立しないものとみなされるべきである。同様に、人道目的と解釈されるかもしれないが、移住管理や難民申請、当局による身元確認など、個人にとって新たなリスクを伴う目的は、適合性のある**追加処理**とはみなされない。

139 セクション8.2.3：目的制限と追加的処理を参照

8.2.4 データの最小化

処理される**個人データ**は、それらが収集される目的のために十分でありかつ関連性があるべきである。特に、収集されるデータが過剰ではなく、データが保存される期間が必要最小限に制限されることを保証することを意味する。収集および処理される**個人データ**の量は、理想的には、データ収集およびデータ**処理**または両立する**追加処理**の特定の目的を満たすために必要なものに限定されるべきである。

識別目的で収集される生体認証情報は、これらの目的相応である必要がある。これは、個人の識別に必要なだけの生体認証情報だけが収集され、処理される必要があることを意味する。識別に関係のない「過剰な」情報は収集すべきではなく、収集した場合には消去すべきである。同様に、収集されるバイオメトリクスのデータセットの範囲は、目的相応（例えば、顔画像または虹彩スキャンの収集は、写真および指紋がすでに識別目的で使用されている場合には、相応であるとはみなされないことがある）に限定されるべきである。

生体認証システム内で収集されたデータの区分化（すなわち、必要な範囲に限定してアクセスが提供される）は、**人道団体**がデータ最小化要件に取り組むための有意義な方法を提供することができる。

また、バイオメトリクスデータの収集を含むプログラムを設計する場合、**人道団体**はデータ最小化原則に沿って、特定の**人道支援**のための識別の目的を達成するために最小限のバイオメトリクス識別子を収集するべきである。

例：
受益者を特定し、不正行為や複製を避けることが目的である場合は、バイオメトリクスデータの1つの情報源（例えば1つの指紋）の収集を以て十分な場合があり、1つ以上の指紋や虹彩の組み合わせの収集は不相応であり、データ最小化原則に違反しているとも考えられる。

8.2.5 データ保全

生体認証情報にはセキュリティ上の課題がある。これは、その処理の完了後の消去または破棄、あるいは、消去または破棄の条件または適用されるべきその他の選択肢（例えば、識別解除またはアクセス制限）を記述した慎重に構成されたデータ保全指針のいずれかによって対応できる。したがって、**追加処理**のためのデータ保全は、その追加的取扱いが明確に定義され、データが当初収集された目的のために必要とされた保存期間内に必要な場合を除いて避けるべきである。**人道団体**は、収集したデータの種類と将来の利用可能性に基づいて、独自の内部データ保全指針を策定する必要がある。

8.2.6 データセキュリティ

生体認証情報の機微性に加え、無許可のアクセスが認められた場合やその他の方法でアクセスされた場合の悪用の可能性を考慮すると、[140]データ**処理**の目的および手段を決定した、十分かつ相応の安全対策が**人道団体**によって（すなわち**データ管理者**によって）実施されることが不可欠である。例えば、情報の暗号化や区分化は、**人道団体**にとって実行可能な解決策となる。

8.3 データ主体の権利

第2章データ保護の基本原則に記載されている**データ主体**の権利には、情報、アクセス、訂正、消去および異議申立の権利が含まれる。

情報に対する権利に関しては、バイオメトリクスデータの場合のように、関係する個人から直接データを収集する場合には、**データ管理者**が**処理**の詳細について対象者に十分な情報を提供することが、他の場合よりもしやすい場合が多い。**同意**に基づいてデータが**処理**される場合、それに伴う重大な追加的リスクを考慮すると、提供される情報のレベルは高くなる。これには、**バイオメトリクス**プロジェクトの実施に必要な**処理**の一部として、第三者がバイオメトリクスデータにアクセスした場合に起こりうる影響に関する情報を含めるべきである。第三者による追加的なアクセスは、当初は想定することができず、また、起こり得る結果も想定することができない。これには、例えば住居移転処理のために移転先と共有する場合などが該当する。このシナリオは、収集の時点では想定されていないが、最初の登録/生体認証情報登録後に個別の**同意**収集が必要になる。

140 Sarah Soliman、*Tracking Refugees With Biometrics: More Questions Than Answers*, War on the Rocks Blog、2016年3月9日：https://warontherocks.com/2016/03/tracking-refugees-with-biometrics-more-questions-than-answers/

バイオメトリクスが使用される場合には、アクセス、異議申立、消去および訂正の権利を促進するための十分なインフラが整備されるべきである。この点に関して、内部のデータ保護方針の中に苦情手続を定義し、**個人データ**処理の実務の中でそれらを実施することが望ましい。

8.4 データ共有

生体認証**処理**には、以下のシナリオにおける第三者とのデータ共有が含まれることがある。

- **人道団体**がデータの収集と処理に必要な生体認証技術を提供するために、外部の**データ処理者**を採用する場合。この場合、**データ管理者**と**データ処理者**の関係が確立される。
- **人道団体**が第三者にデータを転送した結果、その第三者が新しい**データ管理者**となる場合。
- 受入国の当局が、自国領土内で一括して、または特定の個人について収集したバイオメトリクスデータの写しを要請または要求する場合。

そのような共有を行う前に、データ保護要件を考慮することが重要であり、「共有」には、データが積極的に第三者に移転される状況のみならず、データが他者からアクセス可能とされる状況も含まれることに留意する必要がある。**バイオメトリクス**データの機密性を考慮して、データ共有を行う前には特に注意を払う必要がある。

8.5 国際的データ共有

生体認証情報の**処理**には、異なる**人道団体**間の**国際的なデータ共有**や、**人道団体**と民間または公共部門の第三者間の**国際的なデータ共有**の場合のように、異なる国に所在する様々な当事者との**個人データ**の共有が含まれることがある。

データ保護法は、**国際的なデータ共有**を制限しており、上述のように、**バイオメトリクス**が使用される場合には、**人道団体**は、**国際的なデータ共有**の法的根拠を提供するためのメカニズムを持つべきである。[141] **人道団体**は、**国際的なデータ共有**を実施する前に、国際的なデータ共有に適用される法の下での法的根拠があるかどうか、また自身の内部方針の下で法的根拠があるかどうかを検討すべきである。国際的なデータ共有に先立ってDPIAを実施することは、[142]データ保護の観点から、そのような**処理**の適法性をさらに強化することができる。

141 セクション8.2.1：個人データ処理の法的基盤を参照
142 セクション8.7：データ保護影響評価を参照

8.6 データ管理者とデータ処理者の関係

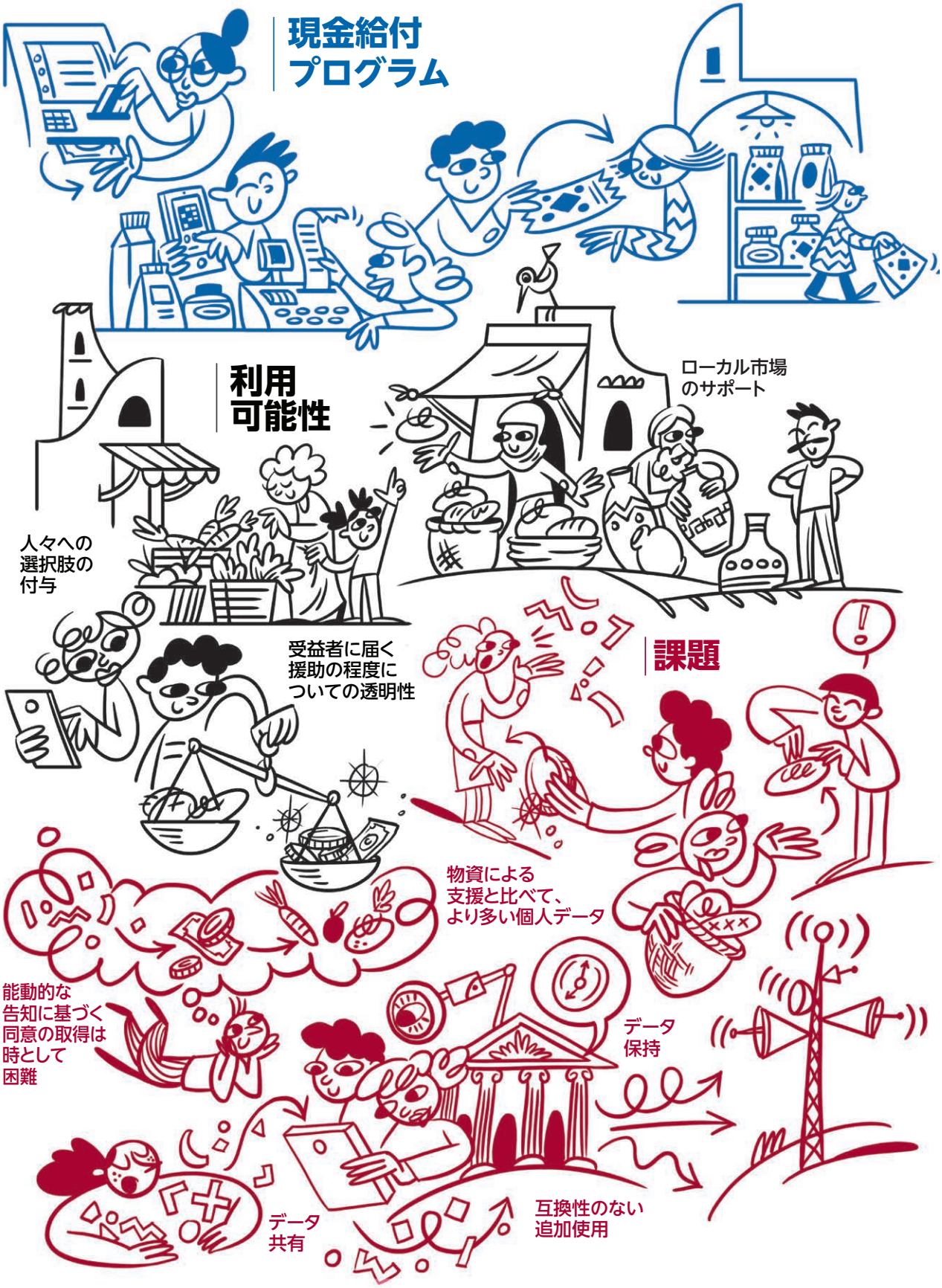
人道団体による生体認証システムの展開には、現場でのプロジェクト実施のために現地のオペレーターに作業をアウトソーシングすることが含まれる。これらの高度に洗練された技術は、専門技術プロバイダのサポートを必要とする。**人道団体**はまた、相互に協力して、生体認証情報のデータベースを共有することもある（上記を参照）。国家当局（例えば法執行機関）は、**人道団体**に対し、その期間が保有する生体認証情報（例えば、人々が移住したり強制的に立ち退きさせられたりした場合）に一括または特定の個人についてアクセスするために圧力をかけることもある。

上記を考慮すると、どの当事者が実際にデータ処理の目的と手段を決定し（すなわち**データ管理者**として）、どの当事者が単に**データ管理者**から指示を受け取るだけか（すなわち**データ処理者**として）を定義することが重要である。役割が明確に定義され、それに対応する任務が割り当てられた場合、**人道団体**間、および/または国境を跨いだ場合、および/または民間または公共部門の第三者との**国際的なデータ共有**は、当事者の責任を定めた適切な契約条項が締結された場合にのみ、実施されるべきである。また、採用されている**データ処理者**が、セキュリティおよびデータ区分に関する要件を完全に遵守できる状態にあるかどうかも慎重に確認する必要がある。これはバイオメトリクス技術にとって特に重要で、複数の**データ管理者**から外部委託された作業を**データ処理者**が管理する場合、および、その場合の**データ管理者**が**人道団体**と当局の両方を含む場合、データセットが適切に区分されない可能性があるリスクを注意深く評価する必要がある。**バイオメトリクス**データの**処理**に先立って作成されたDPIAは、**処理**に関与する様々な当事者の役割を明確にするための適切な手段となり得る。

8.7 データ保護影響評価

DPIAは、データ保護規制のあらゆる側面と、上記で強調した特定のリスクに確実に対応するための、プロジェクト設計時の重要なツールである。

人道団体が生体認証情報を処理する際には、DPIAを実施することが不可欠である。DPIAは取扱いの詳細と仕様を明確にし、潜在的なリスクと可能な緩和措置を強調し、バイオメトリクスデータを収集すべきかどうか、収集する場合にはどのような保護措置を講じるべきかを決定すべきである。DPIAは**バイオメトリクス処理**の実行前に実施されるべきであることに留意することが重要である。


現金給付
プログラム
利用
可能性
ローカル市場
のサポート
人々への
選択肢の
付与
受益者に届く
援助の程度に
ついての透明性
課題
物資による
支援と比べて、
より多い個人データ
能動的な
告知に基づく
同意の取得は
時として
困難
データ
保持
データ
共有
互換性のない
追加使用

第9章

現金給付プログラム

9.1 はじめに

現金給付プログラムは、人道上の緊急事態における生存と回復のプロセスを支援する有望なツールである。**現金給付プログラム**、現金・バウチャー（引換券）支援、現金ベースの介入、現金ベースの支援という用語は、同義に使用することができ、全ての種類の現金給付プログラム、すなわちバウチャーと現金の両方、および全ての種類のデリバリーメカニズムを包含すると理解される。[143]

送金は受益者の選択と彼らが直面するトレードオフに対する尊重は最大限に活かす支援である。人道支援の世界では、特定のサプライヤーからの特定の製品やサービスと交換しなければならないバウチャーから、ある種の要件を満たす受益者を条件とした送金、または人道上の緊急事態の影響を受けている人々が必要とする全てのものに使える無制限かつ無条件の送金に至るまで、いくつかの異なる種類の現金・バウチャー支援が採用され続けている。[144]

電子的現金支援には様々な形態がある。例えば、電子マネーは、受益者に送られる価額であり、現金化または無制限での使用が可能である（例えば、モバイルマネー、プリペイドカード、銀行振込）。また、電子バウチャーは（スマートカードや携帯電話を使って）受益者に送られ、支出制限を設けて認定販売業者と認められた物品を交換することができる。[145]紙のバウチャーの他に、現金が使われることもある。

現金で提供される人道支援の有効性と適切性は、状況に左右されることは広く認識されている（例えば、個人は特定の状況下で必要な物品を手に入れることができるだろうか）。[146]**現金給付プログラム**についての懸念（例えば国内市場のインフレ）もあるが、現金・バウチャー支援を「現物の代替品と比較して、値段相応の価値がある」と裏付ける証拠もある。[147]

143 Key Cash Transfer Terminology、Cash Transfers Glossaryの図表を参照：https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/092017_cash_transfer_programming_terminology_glosssary.pdf

144 Center for Global Development, Doing cash differently: How cash transfers can transform humanitarian cash transfers、Report of the High Level Panel on Humanitarian Cash Transfers、（2015 年 9 月）、p.11：https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf

145 European Commission, *10 common principles for multi-purpose cash-based assistance to respond the humanitarian needs*（欧州委員会、人道的ニーズに対応する多目的キャッシュベースの支援に関する10の共通原則、2015年3月）：https://ec.europa.eu/echo/files/policies/sectoral/concept_paper_common_top_line_principles_en.pdf、DG ECHOファンディング・ガイドライン、人道的危機における現金とバウチャーの使用、2013年3月：https://ec.europa.eu/echo/files/policies/sectoral/ECHO_Cash_Vouchers_Guidelines.pdf

146 Paul Harvey and Sarah Bailey、*Cash transfer programming and the humanitarian system*、*Background Note for the High Level Panel on Humanitarian Cash Transfers*、2015 年 3 月：https://odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9592.pdf

147 同上

調査の結果、必要に応じて、制限なしで、可能な限り電子決済として提供される人道的送金の利用を増やすことには、次のような利点があることが示されている。[148]

- 危機の影響を受けた人々への選択肢の提供と、彼ら自身による生活の自己管理レベルの向上
- 人々が必要としているものと人道的システムの整合性の向上
- 対象となる人々に実際にどれだけの援助が届いているかを示すことによる、人道支援の透明性の向上と不正行為の防止
- 被災者とドナー国の納税者の双方に対する人道支援の説明責任の向上
- 限られた予算のさらに有効な活用に向けた人道支援のコスト削減の可能性
- 現地の市場、雇用、生産者の所得への支援
- 地元住民からの人道支援の支持の増大
- 人道支援のスピードと柔軟性の向上
- 人々を決済システムと結びつけることによる金融包摂を拡大

しかし、多くの困難と課題も存在する。一部の人道上の緊急事態においては、現金・バウチャー支援の利用は、最適な解決策ではない場合がある（例えば、必要な物資やサービスが入手できない場合、地元当局がこの種の人道支援に反対する場合、あるいは関連市場がインフレのリスクにある場合など）。[149]現金給付はプログラムの目的を達成するための単なる手段であり、多くの場合、保護、衛生または保健サービスを提供する措置を含む、より広範な人道支援プログラムの一部である。[150]**現金給付プログラム**を機能させるために、**人道団体**は各人の**個人データ**を処理する必要がある。これには、多くの場合、個人または集団の社会経済的状態および脆弱性に関するデータが含まれる。これは、特に関連する複雑なデータフローを踏まえると、受益者の**個人データ**の収集および取り扱いに関するプライバシー関連の固有の脅威やリスクをもたらす。**現金給付プログラム**のためにデジタル技術を使用する場合、**人道団体**以外の第三者（例えば、国内外の移動体通信のネットワークプロバイダ、金融機関、金融情報機関）の関与がしばしば必要となる。これは、**現金給付プログラム**によって収集されたデータと生成されたメタデータについて、人道団体が制御を失うことを意味する。

これらのデータは、**人道目的**以外の目的（例えば、潜在顧客のプロファイルを作成するため）に使用することができる。また、法的義務を遵守するためや、パートナーシップ契約の下で、外部当事者と共有することもできる。[151]

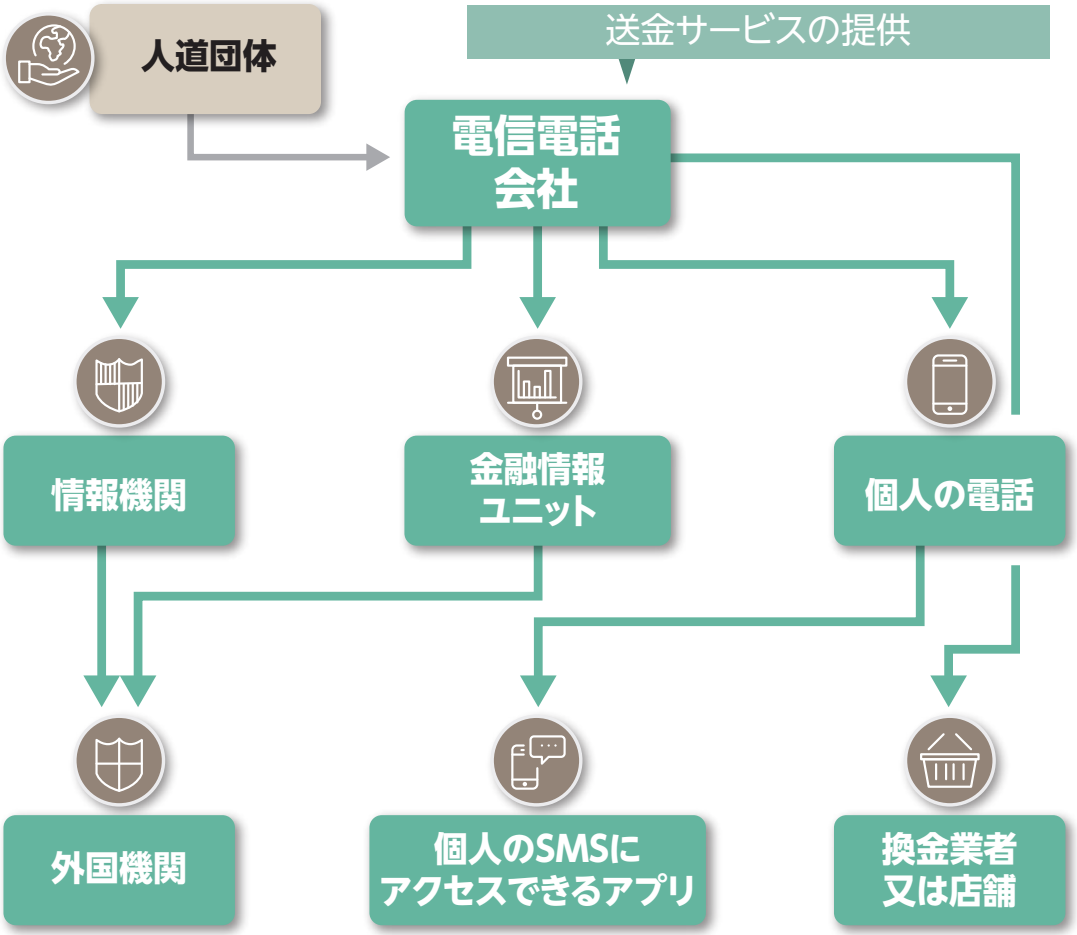
148 ODI and Center for Global Development、*Doing cash differently: How cash transfers can transform humanitarian aid*、Report of the High Level Panel on Humanitarian Cash Transfers、（2015年9月）、p.8：https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf

149 同上、p.11

150 同上、p.11

151 ICRC and Privacy International、“Chapter 6: Cash Transfer Programmes”、The Humanitarian Metadata Problem: *Doing No Harm in the Digital Era*、2018年10月

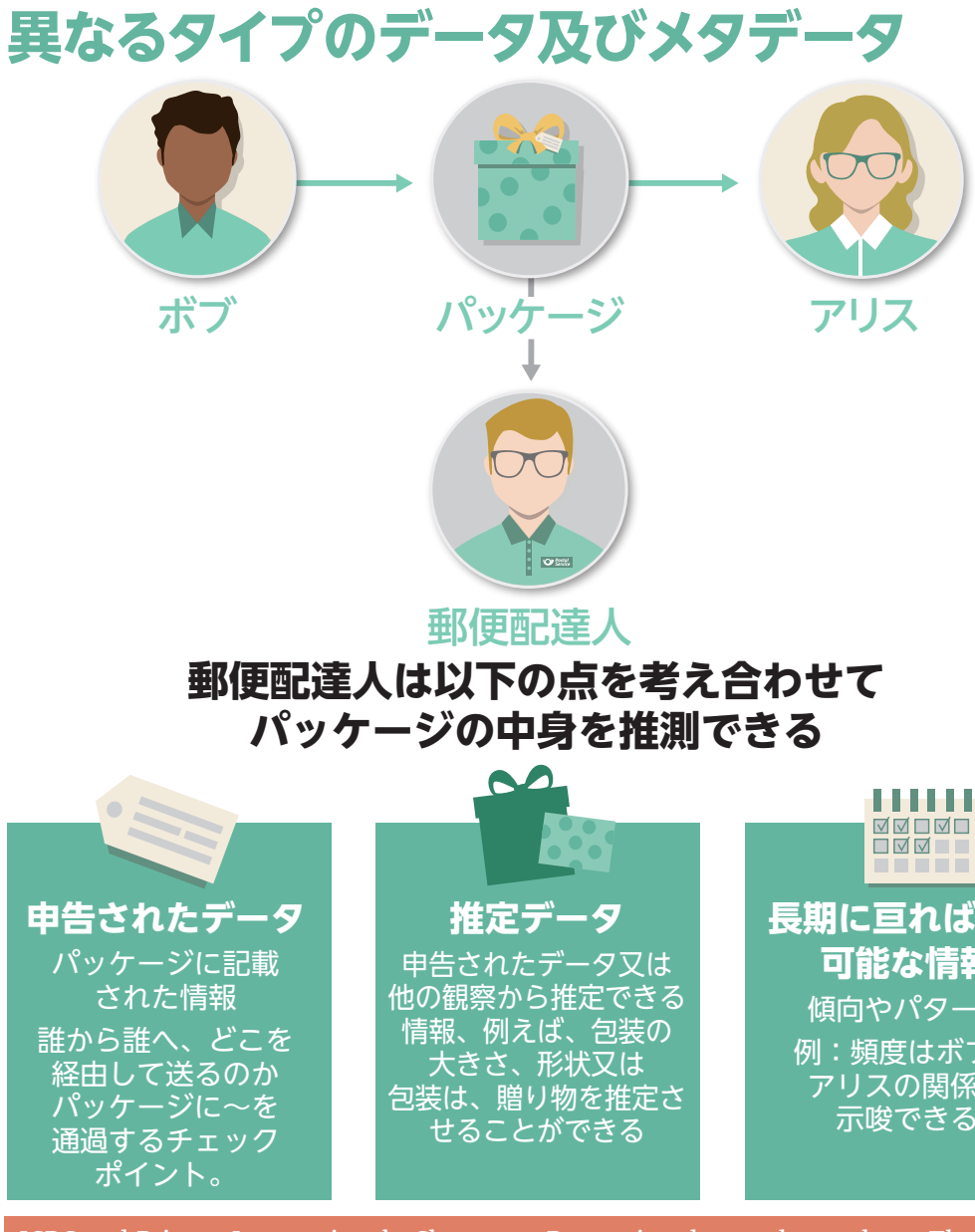
モバイルマネーのデータが他の当事者に届く仕組み



ICRC and Privacy International、Chapter 6: Cash Transfer Programmes、*The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018 年 10 月、p.73

さらに、ICRCとPrivacy Internationalが共同で行った調査では、意図的に収集および処理されたデータだけでなく、1つ1つの相互作用によってメタデータ（データに関するデータ）が生成されることが強調されている。このメタデータは、システムまたはサービスとの相互作用の必然的な結果である。

最後に、デジタル技術と接続性の利用の増加によって、以前は「目に見えなかった」人々が金融機関の「目に見える」ようになっている一方で、これらのデジタルアイデンティティと足跡は、以前のプログラムでは見落とされていた人々の取り込みを助けることができる。しかし、この新たな可視性には、受益者をリスクにさらす可能性がある。彼らが人道団体からの支援を求めているという事実だけで、特定のグループとの関係が明らかになり、差別にさらされる可能性がある。



ICRC and Privacy International、Chapter 2: *Processing data and metadata*、*The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018 年 10 月、p.33

つまり、デジタルの関与によって生じる必然的な可視性は、人道的な状況において脅威をもたらす可能性がある。デジタルの可視性とプロファイリングは、現金給付プログラムの本来の目的に反する金融差別のための手段になり得る。[152]

152 ICRC and Privacy International、"Section 6.1: CTP and financial inclusion: benefits and challenges"、in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月、pp.68-69

9.2 データ保護基本原則の適用

現金給付プログラムのための受益者の**個人データ**の収集および取り扱いに関連する固有のプライバシー関連の脅威およびリスクは、不十分な組織的および技術的なデータセキュリティ対策から生じる可能性がある。**人道団体**はまた、**現金給付プログラム**によって直接的または間接的に生成されたデータの長期的影響を考慮すべきである。**現金給付プログラム**は、銀行や通信事業者などの既存のサービスやシステムを利用しているため、**人道団体**は、Know Your Customer[153]、SIMカード登録[154]、その他の対象となる義務を遵守するために、受益者からのデータ収集を求められる可能性がある。**現金給付プログラム**のために収集された**個人データ**は、他の種類の人道支援には不要だった可能性のある様々なデータセットを含む場合がある。[155]これらのデータは資金援助の分配のため、民間団体と共有される。

さらに、収集されたデータだけでなく、生成されたデータ、すなわち**現金給付プログラム**の実際の仕組みから生成されたメタデータについても、慎重に考慮する必要がある。このようなデータの収集、共有、保持には、さまざまな法律上および規制による義務が適用される。例えば、モバイルマネーの場合、これには送信者と受信者の電話番号、金融取引の日付と時刻、取引ID、取引の場所と金額規模、取引が行われた店舗、およびいずれかの当事者に関係するエージェントなどのデータが含まれる。そのようなデータは、ユーザーのプロファイリング、標的化、モニタリングに使用可能な他の情報や機密情報を推測するために使用できる。[156]したがって、**人道団体**は、受益者の行動、活動、所属、その他の特徴に関する情報を推測するために、データをどのように利用できるかを認識しなければならない。受益者について推測することは、プログラムが終了後もしばらく可能である。

153 Know Your Customer (KYC) は、マネーロンダリング及び腐敗の防止に関する規制と法律を遵守するために、企業が顧客の身元を確認するプロセスを指す。PwC、*Anti-Money Laundering: Know Your Customer Quick Reference Guide and Global AML Resource Map*、PricewaterhouseCoopers、2016年：2016, https://www.pwc.com/gx/en/industries/financial-services/publications/financial-crime-guide-tool-and-global-financial-crime-resource-m.htmlを参照

154 Kevin P. Donovan and Aaron K. Martin, "The rise of African SIM registration: The emerging dynamics of regulatory change", *First Monday*、19巻2号（2014年1月26日）セクション4：http://firstmonday.org/ojs/index.php/fm/article/view/4351を参照

155 Cash Learning Partnership、*Protecting Beneficiary Privacy*、*Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*、p.4：http://reliefweb.int/sites/reliefweb.int/files/resources/calp-beneficiary-privacy-web.pdf

156 ICRC and Privacy International、"Chapter 6: Cash Transfer Programmes" in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月、pp.73-75

援助を提供するために**現金給付プログラム**を選択する**人道団体**の数が増加していることから、この種の支援を配布するために必要な**個人データ処理**の影響（例えば、金銭的援助を受けている個人は差別の対象となるか、など）とリスクを軽減するための措置を考慮する緊急の必要性がある。[157]

データ保護の問題は、現金支援プログラム活動中にデータが**データ管理者**またはデータ処理者によって収集、保存、相互照合されるという事実から生じる。多くの場合、**現金給付プログラム**で収集されるデータは、社会経済的要因と脆弱性に関連している。このデータは支援の対象を特定するために使用される。対象となるのは、影響を受ける人々の一部（ニーズ評価調査のため）、または最終的に現金給付を受けない人々を含む可能性のある幅広いグループである。全ての受益者について、プロセス中に収集される**個人データ**には通常、以下が含まれる：名、姓、携帯電話番号、「KYC」[158]データ、位置情報／その他の電話メタデータおよび**バイオメトリクス**。**人道団体**は、支援の対象を定める目的で社会経済的要因や脆弱性に関するデータを収集することもある。このデータは、一旦収集され格納されると、他の目的のための**処理**および／または**データ分析**またはデータマイニングのような他の種類のデータ**処理**を可能にする場合がある。[159]

現金とバウチャーによる支援を利用する**人道団体**とパートナー組織の間のデータの流れが複雑であることも、データ保護の問題を引き起こしている。これは、以下のデータ共有のセクションで扱う。[160]

9.3 データ保護の基本原則

データ保護の基本原則は、あらゆる種類の**個人データ処理**に従事する際に尊重されるべき基準を構成する。これらには、**処理**の公平性と適法性の原則、透明性の原則、目的制限の原則、データ最小化の原則、データの質の原則が含まれる。[161]

この章のデータ保護に関する説明は、第一部で詳述した原則に基づいている。第一部では、この原則についてさらに詳しく分析している。

157 同上、p.4
158 グロッサリーとPWC、Know Your Customer: *Quick Reference Guide*: http://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html を参照
159 第6章：データ分析とビッグデータを参照
160 セクション9.5：データ共有を参照
161 第2章：データ保護の基本原則を参照

9.3.1 個人データ処理の法的根拠

人道団体は、以下の法的根拠の1つ以上を使用して**個人データ**を処理することができる。

- **データ主体**または他者の極めて重大な利益
- 公共の利益、特に国内法または国際法に基づく当該機関の権限に基づくもの
- **同意**
- 人道団体の正当な利益
- 契約の履行
- 法的義務の遵守

現金・バウチャー支援を用いたプログラムの受益者から、有効な告知に基づいた**同意**を取得することが困難な場合がある[162]。受益者がデータ**処理**のリスクと便益を十分に理解するために提供される必要がある情報の量と複雑さのためである。さらに、単にサービスを利用するだけで、ユーザーの意見なしに必然的にメタデータが生成される[163]。受益者への支援の前提条件として個人情報を収集する他の場合と同様、代替的な援助の提供方法がない限り、援助を必要とする個人にとっては、**同意**を与えるか否かは実際には選択ではなく、したがって、**同意**は有効とはみなされない可能性がある、と論ずることもできる。

同意が不可能な場合は、以下に示す別の法的根拠を用いることができる。受益者は少なくとも、提供されるプログラムの性質、**処理**の法的根拠、どのようなデータが収集されているか、誰により、どのような理由で収集されるのか、データの提供が強制的か任意か、データの出所、データの保存期間、関与している**データ処理者**、他のデータ共有者、およびこれらの関係者の権利（データを是正する権利を含む）について、個別または集合的に知らされるべきである。

人道団体は以下の点を守るべきである。[164]

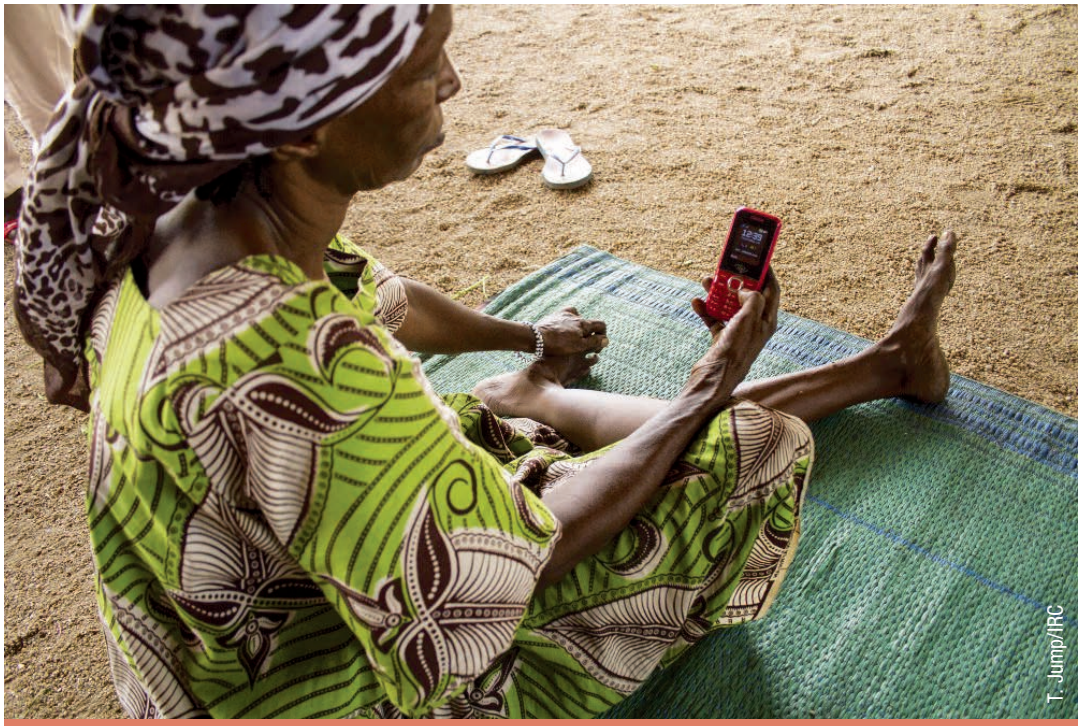
- 現金・バウチャー支援を利用する場合には、受益者の**個人データ**の利用に関する能動的かつ十分な説明をした上での**同意**を得ることを目指すこと。
- それを得ることが非現実的であるか、ここに記載されている他の理由で有効な**同意**を取得することができない場合にのみ、能動的かつ十分な説明をした上での**同意**に代わるものを使用すること。能動的かつ十分な説明をした上での**同意**を求めない正当な理由には、緊急性がある場合や、配布の状況によって「能動的かつ十分な説明をした上での**同意**」が意味をなさない場合が含まれる。

---

162 セクション3.2：同意を参照

163 ICRC and Privacy International、“Chapter 6: Cash Transfer Programmes” in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月、p.21

164 Cash Learning Partnership、*Protecting Beneficiary Privacy*、*Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*、前掲書、p.13



カメルーンの最北部で、女性が無条件の現金送金を受け取るために電話で相談している

- 可能であれば、有効な**同意**が提供されることを確保するか、データフローに不安を感じている個人および/または現金・バウチャー支援の使用に関係する利害関係者のための代替支援方法を提供すること。
- 公表されている情報であることを考慮して知りうる限り最大限の範囲で、**人道団体**が利用しているサービスやシステムの第三者によって生成、収集、処理される可能性のあるデータやメタデータについて受益者に知らせること（銀行向けKYC、通信事業者向けSIMカード登録など）。

災害と緊急事態下での現金ベースのオペレーションの潜在的有効性と、（例えば現物支援と比較した場合）事前に適切に準備されていれば展開が迅速であることも考慮すると、**人道団体**が個人の**同意**を得ることができない場合、**データ主体**または他の者の極めて重大な利益が、関連する**処理**の妥当な代替的な法的根拠を構成することがある。しかし、常にこの法的根拠に基づき、また、本ハンドブックの別の箇所で述べられているように、その使用は慎重に考慮されるべきである。

公共の利益は、上述の事例のように、**人道支援**を実施する権限が国内法、地域法、国際法で確立されており、**同意**が得られなくても重大な利益が誘発されない場合には、現金・バウチャー支援の利用におけるデータ**処理**への適切な法的根拠となりうる。

人道団体はまた、**個人データ**が当該団体の正当な利益なる場合には、その利益が**データ主体**の基本的な権利および自由により優先されない限り、個人データを処理することができる。そのような正当な利益には、人道援助の実施をより効果的かつ効率的にすること、援助の不正や重複を防止することが含まれる。

9.3.2 目的制限と追加処理

データ収集時に、関係する**人道団体**は、データが処理される特定の目的を決定および設定しなければならない。[165]具体的な目的は明確かつ正当なものであるべきであり、**現金給付プログラム**の場合には、被災者が必要な商品やサービスにアクセスできるようにするための支援の提供を含むべきである。

処理の目的を明確にし、収集時に個人に伝達する必要がある。

個人データは、**追加処理**が収集時に最初に指定された目的以外の目的と両立する場合には、それらの目的のためであっても**処理**することができる。これには、その取扱いが歴史的統計的または科学的目的のために必要な場合を含む。**追加処理**が最初にデータを収集した目的に適合するかどうかを確認するために、以下の要因に注意を払う必要がある。

- データが最初に収集された目的と意図された**追加処理**の目的との間の関連
- **個人データ**が収集された状況、特に**データ主体**と**データ管理者**の関係、**データ処理者**との関係
- **個人データ**の性質
- **データ主体**に対する意図された**追加処理**の予想される結果
- 適切な保護措置の存在
- データのさらなる利用可能性に関する**データ主体**の合理的な期待

上記を評価する際には、データ**処理**の人道的目的を特に考慮すべきである。

営利目的の処理者（金融機関やモバイル通信事業者など）による、または営利目的の処理者が関心を寄せる可能性のある**処理**に係る追加的な目的も考慮されるべきである。これには次のようなものが含まれる可能性がある：受益者リストと指定人物リストの照合、法律の執行のためのメタデータの保持、信用力判定のための受益者のプロファイリング等。[166]営利目的のデータ処理者が、想定される専ら人道的目的以外の目的のために**個人データ**を処理する義務を負った場合、またはそのような目的以外の目的のために個人データを処理する立場にあった場合には、次のような結果が生じるであろう。

165 セクション9.3.1：個人データ処理の法的根拠を参照

166 ICRC and Privacy International、“Chapter 6: Cash Transfer Programmes” in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月

- 問題の主体が実際は**データ管理者**ではなく**データ処理者**であり、**処理**の手段と目的を決定しているのではないかと疑問視される。
- **追加処理**は、当初の収集目的と両立しない可能性があり、新たな法的根拠を必要とする可能性がある。新たな法的根拠が見つかるかもしれないが（指定された人物に報告する法的義務の遵守など）、**人道団体**は、これが**人道支援**の中立、公平かつ独立した性質と両立するかどうかを慎重に検討すべきである。

追処理契約の契約条項は、**データ処理者**による**追加処理**を可能な限り制限すべきである。

現金給付プログラムの場合、**人道団体**は、自らが使用しているサービスおよびシステムのデータ処理者によって処理されるデータおよびメタデータを認識すべきである。これらは、契約条項によって規制する必要がある分野を識別するために、DPIAに含めるべきである。

例：
人道団体による現金またはバウチャー支援を行うために設置されたシステムであって、関係する個人がその目的に同意した場合、相互参照の目的で参加者のデータを**人道団体**のドナーに伝達するために同じシステムを使用することはできない。

同様に、金融機関は、**人道団体**から支援を受けた後を含め、受益者の信用力判定や金融サービスとの適格性を評価するために収集したデータを使用することはできない。

9.3.3 データの最小化

資金援助業務のために収集される情報は、これらの目的に見合ったものにする必要がある。すなわち、個人を識別するために必要な**個人データ**のみを収集して処理し、識別目的に関係のない「過剰な」情報は収集しないものとし、収集してしまった場合は消去しなければならない。

現金・バウチャー支援を利用する際には多くの種類のデータが収集されることを考えると、データの最小化要件を満たす方法としてデータの区分化が推奨され、データへのアクセスは必要に応じて提供される。さらに、営利団体による**追加処理**に対して契約上の規定を設けることができる。

データ最小化原理の適用を評価する際に、信用取引メタデータおよびモバイルネットワーク・メタデータのような、**データ処理者**による現金給付プログラムの一部として生成されたデータを考慮することも重要である。

現金・バウチャー支援を利用するプログラムで考えられる選択肢の一つは、**人道団体**が実行可能であれば一意の識別子（受信主体が最終受益者を識別できないもの）と現金の額を営利サービス提供者（銀行やモバイルネットワーク事業者等）に転送し、関係する個人に対するリスクを制限することである。しかしながら、このようなプログラムは、金融機関、電気通信事業者およびその他の関連組織によって提供される厳格なシステムに依存するため、これらのアプローチの限界を考慮することが重要である。同様に、特に再識別を可能にするためにデータを他の情報源と関連付けることができる場合、現在の**匿名化**技術の限界と再識別の影響を認識することが重要である。[167]

9.3.4 データ保全

人道団体は、受益者データが収集された特定の目的を達成するために必要とされる期間を超えて（人道団体か**第三者**である**データ処理者**かに関わらず）保持されないようにすることが推奨される。ただし、保全が反復分配に役立つ可能性がある場合はこの限りではない。プログラムを終了した受益者の**個人データ**は、該当人道団体、その**データ処理者**、およびデータにアクセスした全ての第三者によって消去されるべきである。**人道団体**は、可能な限り、民間サービス提供者によるデータ消去を検証すべきである。プログラムの終了時に保持する必要があると考えられる情報は、将来のプログラム、監査または報告目的、モニタリング、評価など、正当な目的があるデータに関連する場合にのみ保持すべきである。理想的には、これが意味を持つ範囲で、これらの理由で保持されるデータは、集約および/または匿名化されるべきである。

データ保全を検討する際、**人道団体**は、金融機関、クレジットカード会社、移動体通信事業者など、一部のデータ処理業者に対して国内法によって適用される可能性のある保全義務についても考慮する必要がある。これらは、プログラムのDPIAとプライバシーポリシーに含まれるべきである。

167 Larry Hardesty、"How Hard Is It to 'de-anonymize' cellphone data?" MIT News、2013年3月27日：https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data

9.3.5 データセキュリティ

現金給付プログラムにおいて収集、処理された**個人データ**の悪用の可能性を避けるために、適切かつ適合したセキュリティ対策が実施されることが不可欠である。**人道団体**は、受益者データの収集、使用、移転の各段階について、適切な技術的および運用上のセキュリティ基準を満たすことが推奨され、受益者**個人データ**を紛失、盗難、破損または破壊から保護するためのプロセスが整備されるべきである。これには、バックアップシステムおよびセキュリティ侵害に対応し、不正なアクセス、開示または喪失を防止するための効果的な手段が含まれる。[168]

人道団体は、受益者から取得する個人データについて、自己使用、第三者が開始または実施する現金またはバウチャーを使用するプログラム毎に、「デザインによる」**個人データ**保護も望ましい。つまり、現金・バウチャー支援の実施に使用するプロセスとメカニズムに、プライバシー保護を組み込むべきだ、ということである。情報の暗号化または区分化は、このニーズを満たす実行可能なソリューションである。

人道団体は、データ処理の契約をする前に、潜在的な**データ処理者**と、そのシステム、サービス、インフラに依存している他の第三者がとりうる措置について、知ろうとするための措置を講じなければならない。保存時あるいは転送時の**個人データ**、ならびに処理のために依拠されるインフラストラクチャは、データの違法または無許可のアクセス、使用および開示、ならびにデータの損失、破壊または損害などのリスクに対するセキュリティ保護措置によって保護されるべきである。デュー・ディリジェンスおよびDPIAの一環として、**人道団体**は、**データ処理者**および他の第三者が経験した既知のセキュリティインシデントについて、そのシステム、サービスおよびインフラに依存していること、並びに、保存中および転送中のデータのセキュリティおよび整合性を確保するためにその後どのような措置を講じたか、および依存しているインフラについて、知っているべきである。

データの保存と**国際的なデータ共有**の可能性も考慮する必要がある。例えば、難民については、出身国に支店または保管施設を有する地域銀行を利用することに伴う深刻なデータ保護リスクが存在する可能性がある。そのデータを各国当局から要請されることがあるからである。

外部**データ処理者**を選択する場合、彼らが保証できるセキュリティ対策が重要な要素となる。

168 セクション2.8：データセキュリティと処理のセキュリティを参照

9.4 データ主体の権利

情報に対する権利は、提供されるプログラムの性質、どのような情報が誰によって、なぜ収集されているか、どの**データ処理者**が関与しているかについて、受益者が個別または集合的に知らされることを確実にすることによって尊重されるべきである。**人道団体**は、収集して処理をする**個人データ**の使用用途について、透明性を保つべきである。彼らは、より詳細な情報を望む受益者に、想定される完全なデータフローとデータ保全を説明するプライバシー通知を提供すべきである。

現金・バウチャー支援を利用するプログラムについて、アクセス、異議申立、消去および訂正の権利を促進するために、適切な基盤および資源が整備されるべきである。この点に関して、苦情手続を**個人データ処理**の実務及び機関内部のデータ保護方針に組み込むことが望ましい。

9.5 データ共有

現金給付プログラムのための**個人データ**処理には、データセットが異なる**データ管理者**または**データ処理者**（例えば、現金支援プログラムシステムを実施している**人道団体**が、現場のオペレーターに、現場での個人識別を外注する場合）によって収集および処理されている場合には、**データ処理者**および第三者とのデータ共有を含むことができる。データを共有する前に、データ保護要件を考慮することが重要であり、「共有」には、データが積極的に第三者に移転される状況のみならず、データが他者からアクセス可能となる状況（例えば、受益者の個人情報を含むデータベースの共有）も含まれることに留意すること。

人道団体は、自らに代わってデータを収集してくれるパートナー機関や、そのようなプログラムの実施に関与する民間組織（金融機関や移動体通信事業者など）に頼ることができる。これらのその他の組織は、第三者（規制当局を含む）とデータを共有するためのさまざまな法的要件および組織的要件の対象となっている場合がある。これらの要件には、次のものが含まれる。

- 支援を提供する目的で厳密に必要とされる以上の**個人データ**の収集を要求するKYC義務
- 紛争や暴力の状況に関与している可能性のある団体を含む、地域当局によって設置された特定人物のリストとKYCの情報を照合する義務。このプロセスは、公的機関によって監視される可能性があり、報告義務を伴うことがある。その結果、包括性（すなわち、一致が見つかったことに基づいて受益者を援助プログラムから除外することができるか）に関する問題が生じ、**人道支援**の中立性と独立性が損なわれる。
- モバイル通信事業者が関与している場合は、プロセスの一部として、位置情報や電話機個体識別番号、その他のモバイルネットワークのメタデータなどの追加データの収集
- SIMカード登録の要件
- **人道団体**が収集時に提供した情報と矛盾する保存義務

- 信用力判定や広告用の個人のプロファイリングなど、追加的な営利目的
- 国内法によって課される追加の義務

特権および免除はまた、**現金給付プログラム**に関して非常に重要である。この点に関し、**現金給付プログラム**については、セクション10.9：特権・免除とクラウドを考慮する必要がある。

9.6 国際的なデータ共有

データ保護法は**国際的なデータ共有**を制限しているので、**人道団体**は、第4章：国際的なデータ共有で議論されているように、その法的根拠を**現金給付プログラム**において提供するメカニズムを持つべきである。**人道団体**は、**国際的なデータ共有**を実施する前に、それが適用法の下で法的根拠を有しているかどうか、また、国際的なデータ共有自体の内部方針があるかどうかを検討すべきである。

金融サービスは、**人道団体**がコントロールできないような形で相互に密接に関連している。データが国境の内外を移動する方法は、この相互接続性、ならびに国内法、規制および慣行の影響を受ける。このような理由から、**人道団体**は、**現金給付プログラム**に関与する全ての機関と、(i)国内的および国際的に、主要なパートナーが誰であるか、(ii)**現金給付プログラム**のデータを情報交換の枠外に保持することができるかどうか、について議論しなければならない。[169]

9.7 データ管理者とデータ処理者の関係

人道団体による現金・バウチャー支援の利用には、プロジェクト実施のために現地または国際的な営利サービス提供者が関与することがある。**人道団体**相互間でも、これらの活動を通じて収集された情報のデータベースを共有するために協力することができる。したがって、どの当事者が実際にデータ**処理**の目的と手段を決定するか（すなわち**データ管理者**として）どちらが**データ管理者**から指示を受け取るだけか（すなわち、**データ処理者**として）を決定することが重要である。また、複数の当事者がデータ共同管理者と見なされる可能性もある。役割が明確に定義され、対応する任務が割り当てられている場合、**人道団体**および／または国境および／または第三の（民間または国家）機関の間でのデータ共有は、一般に、適切な契約上の取り決めによってカバーされるべきである。

169 ICRC and Privacy International、"Chapter 6: Cash Transfer Programmes" in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月、p.79

個人データは、国際法の下で特権および免除の恩恵を受ける**人道団体**のシステムに保管されている間は保護されるかもしれないが、それらの特権および免除を享受していない**データ処理者**に転送された場合には、同じデータであってもそのような保護を失う可能性があることに留意すべきである。さらに、**データ処理者**は、当地の法律により、政府機関とデータを共有することを義務付けられている場合がある。また、データの送信元である**人道団体**に、政府当局とのデータ共有について通知しないよう義務付けられている場合もある。

9.8 データ保護影響評価

データ保護影響評価（DPIA）は、現金とバウチャーを使用する各プログラムに合わせて作成する必要がある。**現金給付プログラム**は、組織ごとに異なるだけでなく、組織内でも異なる場合がある。各プログラムは、DPIAの対象となるべき個別のデータ保護活動を構成する。DPIAは以下の点で**人道団体**を助けることができる。(a) 個人、特にデータフローから生じる個人および関係する利害関係者に対するプライバシーリスクを識別する場合。(b) 組織におけるプライバシーおよびデータ保護に関するコンプライアンスの責任を識別する場合。(c) 組織の評判を保護し、プログラムに対する一般市民の信頼を高める場合。(d) **人道支援**の中立性に妥協しないことを確保する場合。

人道団体には、自らの組織内で内部的に、または外部の他者との間で外部的に開始または実施する各プログラムについて、受益者データの流れを分析、文書化および理解し、関連するリスクを識別し、リスク緩和策を講じることが推奨される。多くの場合、商用サービスプロバイダに関連する特定の問題や、KYC規制、各国当局への強制報告、**国際的なデータ共有**、潜在的なクラウドストレージに関連する特定の問題については、具体的に評価し、現金とバウチャーによる支援を利用するメリットと比較検討する必要がある。

現金給付プログラムのためのテンプレートDPIAは、Cash Learning Partnershipが開発している。[170]

170 Cash Learning Partnership、Protecting Beneficiary Privacy、*Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*、前掲書、p. 18


クラウド
サービス
短期間で強力な
処理能力を発揮
データを
安全かつ
確実にホスト
利用
可能性
迅速な
拡張性
課題
場所の
柔軟性
クラウド
サービス
全体における
限られた制御力
機微情報の
傍受
必要な時に
全てのバック
アップを
消去できると
いう保証
クラウド
ソリューション
プロバイダ
による
アクセスの
可能性
政府による
アクセスの可能性
監査の実施

第10章

クラウドサービス

10.1 はじめに

最も広く使用されている「クラウドコンピューティング」の定義は、アメリカ国立標準技術研究所（NIST）が発行した定義である。[171]それによると、「クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスフプロバイダとのやりとりで速やかに割当てられ提供されるものである」。NISTの文書では、**SaaS**（Software as a Service／サービスとしてのソフトウェア）、**PaaS**（Platform as a Service／サービスとしてのプラットフォーム）、**IaaS**（Infrastructure as a Service／サービスとしてのインフラストラクチャ）という三つのサービスモデル、並びにパブリッククラウド、プライベートクラウド、コミュニティクラウド、ハイブリッドクラウド環境という4つの実装モデルが定義されている。[172]ただし、常に新しいモデルが開発されていることに留意する必要がある。

クラウドコンピューティングは、大量のデータの作成と**処理**、および、新しいサービスやアプリケーションの作成を容易かつ迅速にする。また、その展開も加速させている。人道支援は情報によって促進されるため、この新しい代替的なデータ処理概念は**人道団体**にとって有用なツールとなっている。そのメリットには、短時間で膨大な処理能力にアクセスできること、データの場所や流れが固定されず柔軟であること、コスト削減などがある。[173]

しかし、**クラウドサービス**は、プライバシーとデータ保護にリスクと課題ももたらしている。これらは一般的に二つの主なカテゴリーに分類される。第一に、データ制御の欠如、第二に、**処理**操作自体に関する透明性の欠如である。**人道支援**にとって特に重大なリスクは次の通りである。

- 保護されていない場所からのサービスの利用
- 機微情報の傍受
- 認証の脆弱性
- 例えばハッカーによって、クラウドサービスプロバイダからデータが盗まれる可能性
- 政府や法執行機関によるアクセスの可能性

171 US NIST SP 800-145、NISTによるクラウドコンピューティングの定義、2011年9月：http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

172 欧州データ保護監督官（EDPS）、欧州委員会の「欧州におけるクラウドコンピューティングの潜在力の解放」の公表に関するEDPSの2012年11月16日付オピニオン、p.4：https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

173 ダラ・シュナイデルヤンスとコリー・オズボラト、人道支援ロジスティクスにおけるクラウドコンピューティングの実証的検討、ワーキングペーパー：http://www.cba.uri.edu/research/brownbag/spring2013/documents/DaraS2013329paper.pdf

クラウドコンピューティングがデータ保護に与える影響は、データ保護・プライバシーコミッショナー国際会議が2012年にウルグアイで採択した、クラウドコンピューティングに関する決議[174]で注目を集めた。

さらに、国際法の下で特権と免除を享受している**人道団体**は、**個人データ**処理を第三者のクラウドサービスプロバイダに外部委託することによって、その特権と免除を失い、データを危険に晒す可能性があることを認識すべきである。クラウド環境における特権および免除の潜在的な影響の詳細については、以下のセクション10.9：特権・免除とクラウドで説明する。

クラウドサービスのモデルには、主に次の3つのタイプがある。[175]

- サービスとしてのインフラストラクチャ（**IaaS**）：**IaaS**クラウドは、クラウドシステムを構築するためのコンピューティングリソースを提供するサービスである。クラウドのカスタマーは、ハードウェア自体を購入するのではなく、必要な容量に応じてクラウドプロバイダーのハードウェアへのアクセス権を購入する。
- サービスとしてのプラットフォーム（**PaaS**）：**PaaS**クラウドは、コンピューティングプラットフォームを提供するサービスであり、カスタマーはプラットフォーム上でアプリケーションを開発できる。開発したアプリケーションはそのプラットフォーム上や、別のインスタンス上でも実行できる。プラットフォームは**IaaS**クラウド上でホストされる場合もある。
- サービスとしてのソフトウェア（**SaaS**）：**SaaS**クラウドとは、クラウド利用者がウェブブラウザまたはその他のソフトウェアを通じてアクセスできる、完成したソフトウェアアプリケーションを提供するサービスである。この方法でソフトウェアにアクセスする場合、クライアントの機械にソフトウェアをインストールする必要がなくなる、または少なくなり、多様なデバイスをサポートするサービスが可能になる。ソフトウェアは、クラウドプラットフォームまたはクラウドインフラストラクチャ上でホストされる場合もある。

クラウドインフラストラクチャにも様々な種類がある。プライベートクラウドは、内部あるいは**第三者**によって管理されているかに拘わらず、単一の組織で使用され、内部または外部でホストされる。パブリッククラウドでは、サービスは一般に公開されたネットワークを介して提供される。ハイブリッドクラウドは、二つ以上の別々のクラウドを組み合わせたクラウドであり、複数の実装モデルのメリットを提供する。

これらのモデルにはそれぞれ長所と短所がある。パブリッククラウドは情報がオフサイトバックアップされ、インターネット経由でどこからでも利用できるため、アクセスしやすい。また、サーバー容量を即座に拡張できるため、コスト削減になり得る。さらに、セキュリティおよびパフォーマンスのアップデートと改善が定期的に行われる。一方、パブリッククラウドはインターネット接続に依

174 http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Cloud-Computing.pdf?mc_phishing_protection_id=28047-br1tehqdu81ea0ar3q10を参照

175 情報コミッショナーオフィス、*クラウドコンピューティングの利用におけるガイダンス*、2012年、pp.5-6：https://ico.org.uk/for-the-public/online/cloud-computing/

存しているため、データの制御を失う危険性がある。というのは、元の管轄エリアから別の管轄エリアへの未知、不正なデータ転送、データの誤った消去、サービス終了後のデータ保持、ハッキング、およびセキュリティ攻撃の危険性があるためである。データが特定の時点で、パブリッククラウドのどこに保存されたのかを特定することは困難であり、管理されていないバックアップが多数存在するため、そのデータの消去はほとんど不可能である。更に、プライバシーおよび秘密保持上の懸念も多くある。例えば、データ**処理**が様々な法規制の適用対象となる結果、強制的に権限なくデータの提供を義務付けられたり、当局による管轄権を行使される可能性がある。

プライベート／内部クラウドでは、データは組織の内部ネットワーク内で保管されるため、一般からはアクセスできない。より管理された環境で、限られたユーザー数による利用となるため、第三者への情報開示のリスクが減る。プライベートクラウドは、パブリッククラウドと同様の便宜性、拡張性、柔軟性を備えている。ただし、その欠点は、コスト面や、最新のパフォーマンスとセキュリティのアップグレード、改善が得られないという点である。

ハイブリッドクラウドでは、保存する情報の分類に応じて、組織がどのオプションを使用するかを選択できる。通常、機微性の低い情報はパブリッククラウドに送信されるが、機微性の高い情報はプライベートクラウドまたは内部のクラウドに保存される。このモデルは、コスト削減、拡張性、セキュリティ、パフォーマンスのアップグレード、改善を実現するが、データ制御を失う可能性や不正なデータ開示という点ではパブリッククラウドと同じリスクを伴う。

10.2 クラウドにおける責任と説明責任

クラウドクライアントとプロバイダーの関係は、**データ管理者**と**データ処理者**の関係と等しい。[176]しかし、例外的に、クラウドプロバイダーが**データ管理者**の役割も担う場合がある。その場合には、クラウドプロバイダーはデータ**処理**に対して（共同で）全責任を負い、データ保護に関する全ての法的義務を遵守しなければならない。クラウドクライアント（**人道団体**）は、**データ管理者**として、データ保護法に基づく法的義務を遵守する責任がある。さらに、クラウドクライアントは、データ保護法に準拠するクラウドプロバイダーを選択する責任を負う。

説明責任の概念は、データ保護法の下で**データ管理者**と**データ処理者**が負うコンプライアンスの直接的な義務を表している。これは、適切なデータ保護方針の適用と通知の実施を通して、自らのデータ**処理**活動が法的要件に適合していることを確実にし、証明できなければならないことを意味する。

176 セクション10.7：データ管理者とデータ処理者との関係を参照

例：

人道団体がクラウドプロバイダーとの間で、クラウド内で**個人データ**を保管する契約を締結する場合、**人道団体**は、クラウドプロバイダーが犯したあらゆるデータ保護違反に関し、**データ主体**に対して責任を負う。従って、人道団体は、**個人データ**をクラウドに保存する前に以下の措置を講じることが不可欠である。

- **個人データ**のクラウドへの保存についてDPIAを実施し、その結果、個人データ保護に過度なリスクが発生することが判明した場合には、そのプロジェクトを中止にする備えをする
- クラウドサービスプロバイダが相当の注意を払ってデータ保護に真剣に取り組むことを保証するため、クラウドサービスプロバイダに対してデューディリジェンスを実施する
- データ保護についてプロバイダーと隠し立てなく話し合い、プロバイダーがデータ保護の義務を果たす準備ができ、義務を果たせそうかどうかを評価する
- 署名の前にプロバイダーとの契約を注意深く審査し、適切なデータ保護の文言が含まれていることを確認する
- 特権と免除を享受している**人道団体**、そのような特権と免除がクラウドソリューションの設計に適切に組み込まれ、尊重されるようになっているかを確認する

10.3 データ保護基本原則の適用

全てのデータ保護原則が**クラウドサービス**にも適用されるが、ここでは特に関連性の高い、いくつかの問題に焦点を当てる。

この章のデータ保護に関する説明は、第一部で詳述した原則に基づいている。第一部では、この原則について更に詳しく説明している。

10.3.1 個人データ処理の法的根拠

人道団体は、クラウドプロバイダーと契約する前に次の法的根拠のいずれかが存在することを明確にする必要がある。[177]

- **データ主体**または他の者の生命に関わる利益
- 特に、国内法または国際法で規定された機関の権限に則った、公共の利益
- **同意**
- 人道団体の正当な利益
- 契約の履行
- 法的義務の遵守

177 第3章：個人データ処理の法的根拠を参照

個人の生命に関わる利益が個人データを収集するための十分な法的根拠にはなっても、そのデータをクラウドに置く場合には別の法的根拠がなければならない。

これに関して、**人道団体**による個人データの初期の**処理**と、クラウド上での**個人データ**の**処理**とを区別することが重要である。**人道団体**は第一に**個人データ**を収集して**処理**するための法的根拠を持たなければならない。これは、第3章：個人データ処理の法的根拠で言及した、いずれの法的根拠でもよい。加えて、クラウド上での**処理**に関しては別の法的根拠が必要となる。個々の具体的な状況または人道的活動における法的根拠、およびそれを「追加的な」法的根拠として、またはそれを組み合わせた形でクラウドに適用できるかどうかについては、ケースバイケースで評価を行うべきである。

例：
ある**人道団体**は、個人の生命に関わる利益であるという根拠に基づき、脆弱な個人から**個人データ**を収集している。人道支援サービスをより効率的に提供するために、プライベートクラウドにデータを保管したいという目的のもと、この人道団体はクラウドサービスプロバイダを利用している。個人の生命に関わる利益が**個人データ**を収集するための十分な法的根拠にはなるが、データ収集とは別にデータをクラウド上に置くための法的根拠も存在しなければならない。人道支援サービスはクラウドにデータを置かなくても実施できるため、生命に関わる利益がクラウド上にデータを置くための十分な法的根拠になるとは言い切れない。むしろ、クラウド上に置く目的は、人道援助をより効率的に提供するためである。従って、クラウドプロバイダーを利用するための法的根拠となり得るのは、**人道団体**の正当な利益、および、それがデータを処理される**データ主体**の基本的な権利によって優先されないことである。この主張は、プライベートクラウドを使用する場合、より強いものとなる。この法的根拠を確認するためにDPIAを実施すべきである。

10.3.2 公正かつ適法な処理

個人データは適法かつ公正に**処理**されなければならない。適法処理とは、適切な法的根拠を特定できることであり[178]、また、公正な処理のためには、情報の提供およびデータの利用に関連して一般的に求められる広範な原則に則る必要がある。**クラウドサービス**を利用する**人道団体**は、これらの原則が**処理**の全ての段階（収集、**処理**、保管）で適用されることに留意すべきである。

10.3.3 目的制限と追加的処理

人道団体は**個人データ処理**の具体的な目的を決定し、説明する義務がある。即ち**処理**の目的を明確にし、収集時に個人に伝達しなければならない。

人道的な目的によっては**追加処理**業務を正当化できる広範な法的根拠が成立する。しかし、関係する個人のリスクが**追加処理**による利益を上回る場合、その両立は見出されない。これは個々のケースによる。例えば、データ**処理**が、その情報に関係する者あるいはその家族の重大な利益に相反する恐れがある場合、特に、データ**処理**によってその者の生命、インテグリティ、尊厳、精神的または身体的な安全、自由、評判を脅かす恐れのあるリスクが存在する場合は、追加的取扱いの正当性と個人のリスクは両立し得ない。

クラウドコンピューティング環境では、クラウドクライアントは、**データ主体**から**個人データ**を収集する前に、データ**処理**の目的を決定する責任を負い、その目的を**データ主体**に通知しなければ

178 セクション10.3.1：個人データ処理の法的根拠を参照

ならない。クラウドクライアントは本来の目的と異なる目的のために**個人データ**を処理してはならないという禁止規定に基づき、クラウドサービスプロバイダは、**個人データ**（およびその**処理**）を未知のクラウドデータセンターに自動送信するよう一方的に決定したり、手配することはできない。さらに、クラウドサービスプロバイダは、自社の目的（例えば、マーケティングや、プロファイリング、他の目的で研究を実施すること）のために**個人データ**を利用することはできない。

また、クラウドプロバイダーおよびそのサブコントラクタも本来の目的に反する**追加処理**を行うことは禁止されている。クラウドを利用する場合の一般的なケースでは、多くのサブコントラクタが容易に関与している。**追加処理**のリスクを緩和するため、クラウドプロバイダとクラウドクライアントとの間の契約には技術的および組織的な措置を含めるべきであり、クラウドプロバイダまたはそのサブコントラクタの従業員によって行われる**個人データ**に関する処理作業のログ記録や監査を行うことを保証をすべきである。

10.3.4 透明性

透明性は、公正かつ正当な**個人データ処理**の一側面であり、**データ主体**への情報提供にも密接に関連する。クラウドクライアントは、**個人データ**、あるいは自身に関連するデータを収集される**データ主体**に対して、詳細な情報を提供する義務を負う。これには、クラウドクライアントの身元、アドレス、および、**処理**の目的の他、公正な処理を保証するために追加的情報を必要とする場合に限り、情報の受領者または**データ処理者**を含むデータ受領者のカテゴリーに係る情報、そして、データ主体の権利についての情報を含む。

また、クラウドクライアント、クラウドプロバイダー、（もしあれば）サブコントラクタの関係においても透明性が保証されなければならない。クラウドクライアントは、関連する全ての問題についてクラウドプロバイダーがクライアントに通知した場合にのみ、クラウド上の個人データ処理の合法性を評価することができる。クラウドプロバイダーとの契約を検討している**データ管理者**は、プロバイダーとの契約条件を注意深く精査し、データ保護の観点からそれらを評価すべきである。

クラウドコンピューティングにおける透明性のもう一つの側面は、クラウドクライアントが直接契約関係にある再委託者についてだけでなく、各クラウドサービスの提供に関与する全ての再委託者について知らされなくてはならないということである。また、**個人データ**が処理される全てのデータセンターの場所についても知らされなくてはならない。

10.3.5 データ保全

人道団体は、明確且つ正当な、文書化された理由がない限りにおいて、（人道団体または**データ処理者**においても）**個人データ**を必要以上に長期間保持しないよう保証した方が良い。理由がない場合には、機関および関連する**第三者**が保有するデータは破棄されるべきである。デー

タ**処理**の完了後にデータを破棄すること、または、データ保管方針を綿密に作成することが推奨される。**個人データ**収集の目的が達成されたら、第三者がそのデータを保持することに**同意**を得ていない限り、データにアクセスした機関および第三者の双方が**個人データ**を消去しなくてはならない。

データは、正当な**処理**目的がある場合にのみ、**クラウドサービス**に保全されるべきである。この場合の正当な目的には、将来のプログラムの可能性、モニタリングおよび評価が含まれる。他方で、研究目的のためには匿名化または集計されたデータとしての保持が適切である。データ最小化の原則に従い、必要最小限のデータのみを保全すべきである。

不要になった**個人データ**が直ちに削除されることを保証する責任はクラウドクライアントにある。データの削除は、クラウドコンピューティングの契約期間中だけでなく、契約終了の際にも極めて重要な問題である。これはサブコントラクタが替わったり撤退した場合にも該当する。そのような場合、クラウドクライアントは、クラウドサービスプロバイダに対し、データ破棄の証明書、或いはデータが新しいクラウドサービスプロバイダに転送されたことを確認できる証明書を請求できる。

データ削除の原則は、そのデータがハードドライブや、その他の記憶媒体（例：バックアップテープ）に保存されているかに拘わらず、**個人データ**に適用される。**個人データ**は、様々な場所の異なったサーバーに同時に保管される場合があるため、全てのインスタンスを復元できないように確実に削除する必要がある。（以前のバージョン、一時ファイル、更にはフラグメントも消去しなければならない。）

個人データを安全に削除するには、記憶媒体を破壊または消磁するか、保存された個人データを効果的に消去しなければならない。承認された仕様に従って、**個人データ**を複数回上書きする特別なソフトウェアツールを使用する必要がある。クラウドクライアントは、クラウドプロバイダーが上記の意味で安全な削除を保証すること、および、クラウドプロバイダーとクライアントとの間の契約に**個人データ**削除に関する明確な規定が含まれていることを確認すべきである。クラウドプロバイダーとサブコントラクタとの間の契約についても同様である。

10.4 データセキュリティ

データセキュリティ対策には、法的、技術的、組織的なものがある。法的措置には契約上の取り決めだけでなく、**データ保護影響評価**（DPIA）も含まれる。**クラウドサービス**契約において下記の段階を考慮に入れた全体的な視点から見る必要がある。

- クラウドコンピューティングを利用する判断の評価（DPIAと経営陣による「利用する／利用しない」かの決定）

- 契約を検討しているクラウドサービスプロバイダに対しての法的および技術的な観点を考慮したデューディリジェンスを含む、クラウドサービスの調達プロセス
- 契約（適切な契約条件を得ること）
- サービスの実施、維持および停止

包括的なデータ保護戦略が推奨され、契約締結前、締結中、締結後の全ての段階においてデータ保護の問題に注意を払うべきである。そのためには、**SLA（サービスレベル合意書）**、一般的な（データ保護に限らない）条項（適用対象となる法制、契約の変更、管轄、責任、補償など）、および「クラウド内外の並行」の一般原則（例えば、クラウドまたは非クラウド処理のデータ保持期間が同じであること）を含む契約フレームワークの総合的な評価を行う必要がある。**人道団体**がクラウドコンピューティングサービスの契約を決定する際には、想定される処理を管理する技術的なセキュリティと組織的な措置に対して十分な保証を提供できるクラウドプロバイダーを選択し、その措置を確実に遵守させるべきである。更に、**データ管理者**と**データ処理者**との関係の規定に法的拘束力を持たせるため、クラウドサービスプロバイダとの書面による契約を結ぶ必要がある。契約では、少なくとも、**データ処理者**は**データ管理者**の指示に従うこと、そして、**データ処理者**は適用されるデータ保護法に従って**個人データ**を適切に保護するための技術的および組織的措置を実施することを規定しなければならない。

法的安定性を確実にするため、**人道団体**と**データ処理者**との間の契約には、以下の中核的なデータ保護条項も含めるべきである。

- データセンターの所在地、再委託先の身元と所在地、および、処理の性質の事後的な変更に関する情報の提供。この処理の性質には、クラウドプロバイダーが提供するクラウドサービスの対象と期間、クラウドプロバイダーによる**個人データ**処理の範囲、方法、目的、および処理する**個人データ**の種類も含まれるべきである。
- クラウドクライアントがプロバイダーに与える指示の詳細。特に、適用される**SLA（サービスレベル合意書）**や、それに違反した場合の罰則。（コンプライアンスに違反した場合のプロバイダーに対する損害賠償請求、またはその他の訴訟能力）
- クラウドクライアントのデータに影響を及ぼす**データ侵害**が発生した場合に、クラウドプロバイダーがその旨をクラウドクライアントに通知する責任を明確にする。セキュリティに関する事故は必ずしも**データ侵害**に該当しないことに注意する。
- 明記された特定の目的のためにのみ**個人データ**を処理し、契約終了時にデータを消去するという義務の承認。サービスが終了した際のデータ返還または破棄についての契約条件を明確にしなければならない。更に、クラウドクライアントの要求に応じて**個人データ**が安全に削除されることを保証しなければならない。
- プライベートクラウドがクラウドクライアントの管理範囲外にある場合は、**人道団体**のデータが別のサーバーに保管されていることを確認する。

- クラウドプロバイダーが遵守しなければならないセキュリティ対策の規定。これは、処理によって予想されるリスクと、保護されるべきデータの性質に応じて決まる。
- クラウドプロバイダーとデータにアクセスできる従業員の双方を拘束する機密保持条項。認証された者のみがデータにアクセスできる。
- **データ主体**が自身のデータへアクセスする、または訂正、消去する権利を行使できるよう促進する上で、クライアントをサポートするというプロバイダー側の義務。
- クラウドクライアントの（該当する場合）特権および免除を尊重する上でのクラウドプロバイダー側の義務。
- 一般的には**データ管理者**（クラウドクライアント）から得られる、**同意**に基づいてのみ再委託先に委託できるという趣旨の条項。これは、**データ処理者**は再委託先の委託に関し、全ての変更予定について**データ管理者**に通知するという明確な義務に基づく条項であり、同時に、**データ管理者**はそのような変更に対して常に異議を唱えることや、契約を終了することが可能である。クラウドプロバイダーには、委託する全ての再委託先を明示するという明確な義務がある。クラウドプロバイダーと再委託先との間の契約は、クラウドクライアントとクラウドプロバイダーとの間の契約規定を反映したものでなければならない。（つまり、再委託先はクラウドプロバイダーと同じ契約義務の対象となる。）特に、クラウドプロバイダーと全ての再委託先は、クラウドクライアントからの指示に基づいてのみ行動することが保証されなければならない。こうした責任の連鎖は契約書に明確に示されるべきである。
- クラウドクライアントが契約期間中および契約終了時に監査を実施することへの合意。契約では、クラウドプロバイダーや再委託先が実施する**個人データ**に関する処理作業のログ記録および監査について規定しなければならない。
- プロバイダーの内部組織やそのデータ処理の契約が（再委託先によるものも含めて）国内法および国際法の要件と基準に準拠していることを保証するためのプロバイダー側の一般義務。

以下は、データセキュリティの技術的な側面に関して、**人道団体**が留意すべき重要な考慮事項である。[179]

- **可用性：**可用性を提供するということは、**個人データ**へのタイムリーで信頼性の高いアクセスを保証することを意味する。クラウドの可用性は、クライアントとプロバイダーとの間のネットワーク接続が事故により失われたり、（分散型）サービス妨害（DoS）攻撃などの悪意のある行為によってサーバーのパフォーマンスが低下したりすることで脅かされることがある。その他の可用性に関するリスクとしては、ネットワークやクラウド処理、データストレージシステムの双方で起こる事故によるハードウェア障害、電源障害、その他のインフラストラクチャの問題などがある。従って、**データ管理者**は、クラウドプロバイダーがバックアップ回線、冗長ストレージ、

179 出典：第29条作業部会、*クラウドコンピューティングに関する意見*05/2012、WP196、2012年7月1日、pp.14-17：https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

効果的なデータバックアップメカニズムなど、通信障害の危険性に対処するための適切な手段を用いていることを確認すべきである。

- **完全性**：完全性とは、データの**処理**、保管、転送の際に、事故または悪意により、改変されてはならない、データ品質の維持を意味する。ITシステムでは、完全性とはシステム上で処理されている**個人データ**が変更されていない状態を指す。**個人データ**の変更は、メッセージ認証コード、署名、暗号学的ハッシュ関数などの暗号認証メカニズムによって検知できる。そして、クラウド内のITシステムの完全性への干渉は、不正侵入検知／防止システム（IDS/IPS）によって検知、または防ぐことができる。これらのセキュリティツールはクラウドが通常作動するオープンネットワーク環境にとって特に重要である。
- **機密性**：クラウド環境では暗号化が正しく適用されれば**個人データ**の機密性に大いに役立つが、個人データが不可逆的に匿名化されるということではない。これは、クラウドクライアントが責任を持つ**個人データ**に、正しい鍵を持った認証者のみがアクセスできることを保証するための単なるツールである。**個人データ**の暗号化は全ての「転送中データ」に使用すべきであり、可能な場合は「保存データ」にも使用するべきである。これは、**データ管理者**が**機微データ**を転送する場合に特に当てはまる。クラウドプロバイダーとクライアント間、および、データセンター間の通信も暗号化する必要がある。データを保護するための技術的手段として暗号化を選択する場合、鍵の安全性を保証することも重要である。機密性の確保を目的とした更なる技術的手段には、承認メカニズムや強力な認証（例：2段階認証）がある。契約条項においてもクラウドクライアント、クラウドプロバイダー、および、再委託先の従業員に守秘義務を課すべきである。
- **アイソレーション（目的制限）**：アイソレーションとは目的制限の原則のことをいう。クラウドのインフラストラクチャでは、ストレージ、メモリ、ネットワークなどのリソースが多数のユーザー間で共有される。これはデータ開示や不正な**追加処理**といった新たなリスクを生み出す。アイソレーションは、この問題に対処し、データが本来の目的を超えて使用されないようにすると共に、機密性と完全性を維持することを目的とする。アイソレーションは**個人データ**にアクセスできる権利や権限を適切に管理することによって機能し、また定期的に見直されなくてはならない。法外な特権を与えた権限の行使は避けるべきである。（例えば、ユーザーであれ管理者であれ、クラウド全体へのアクセスを承認されるべきではない）。より一般的には、管理者とユーザーは正当な目的のために必要な情報にのみアクセスできる（最小特権の原理）。
- **介入可能性**：**データ主体**は、以下に述べるように、アクセス、訂正、削除、遮断、異議申立の権利を有する。[180]
- **移植性**：異なるクラウドプロバイダー間の相互運用性とポータビリティを促進するため、クラウドプロバイダーが標準的なデータフォーマットとサービスインターフェースを使用することは非常に重要である。クラウドクライアントが別のクラウドプロバイダーに移行することを決定した場合、

180 セクション10.5：データ主体の権利を参照

相互運用性がなければ、クライアントの（個人）データを新しいクラウドプロバイダーに移行することが困難または不可能になる。この状態を「ベンダーロックイン」という。クラウドクライアントは、クラウドサービスを発注する前に、プロバイダーがデータとサービスのポータビリティを保証しているかどうか、またどのように保証しているかを確認する必要がある。また、データの移植性は、**データ主体**が処理中のデータのコピーを、一般的に使用される構造化された電子フォーマットで、**データ管理者**から取得できる状態を指す。この権利を行使するためには、一旦データが移行されると、元のシステムにはトレースが残らないようにすることが重要である。技術的には、データの安全な削除の検証を可能にすべきである。

以下は、クラウドにデータを移行する際に**人道団体**が考慮すべきITセキュリティの原則である。[181]

10.4.1 転送中データの保護

データ移行の際、盗聴や改ざんから適切に保護されなければならない。これは、組織の構内やクラウドアプリケーション間の接続だけでなく、サービス内のデータパスや、アプリケーションとその他のサービス間の接続（API）[182]にも関係する。一般的な解決策は、ネットワークレベルのトラフィック暗号化（VPN）[183]、トランスポート・レイヤー・セキュリティ（**TLS**）、またはアプリケーションレベルの暗号化を使用してネットワークトラフィックを暗号化することである。暗号化のための秘密鍵の管理と同様、正しいプロトコルの選択や暗号化の実行のために十分な注意を払わなければならない。状況によっては専用の光ファイバ接続を使用することも可能であり、これは便宜性が高い。

10.4.2 資産の保護

クラウド環境での資産の保護は、オンサイトでの資産の保護とは方法が異なる。従って、クラウドソリューションを評価する際には、いくつかの特定の点を考慮する必要がある。

181 ICTリーガル・コンサルティング社がクラウドセキュリティに関する資料の使用を許可してくれたことに感謝の意を表する。出典：英国国家サイバーセキュリティセンター、クラウドセキュリティガイダンス：クラウドセキュリティ原則の実施、2018年11月17日：https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

182 API（アプリケーション・プログラミング・インターフェース）とはアプリケーションソフトウェアを構築するための一連のサブルーチンの定義、プロトコル、ツールのことである：software: https://en.wikipedia.org/wiki/Application_programming_interface

183 VPN（仮想プライベートネットワーク）とはインターネットなどのパブリックネットワーク上に構築されたプライベートネットワークのことである。ユーザーは、自分のコンピューティングデバイスがプライベートネットワークに直接接続されているかのように、共有ネットワークまたはパブリック・ネットワークを介してデータを送受信できる。VPN（仮想プライベートネットワーク）とはインターネットなどのパブリックネットワーク上に構築されたプライベートネットワークのことである。ユーザーは、自分のコンピューティングデバイスがプライベートネットワークに直接接続されているかのように、共有ネットワークまたはパブリック・ネットワークを介してデータを送受信できる。https://en.wikipedia.org/wiki/Virtual_private_network

10.4.2.1 物理的な場所

どの法律が適用されるか把握するためだけでなく、電力やネットワークの遮断、敵対するグループや組織による行動、また、その他の各国特有の脅威など、具体的な脅威の可能性を特定するために、データストレージの物理的な場所を知ることが重要である。従って、データセンターの物理的な場所に関する詳細な情報を入手し、機関の知らないうちに異なる場所にあるデータセンター間でデータ通信が行われる可能性があることを認識しておくことが重要である。

特権と免除を享受する**人道団体**にとっては、データセンターを設置している国がその特権と免除を尊重する法的義務を持ち、それらを実際に尊重していることが知られている国であることも必要不可欠である。

10.4.2.2 データセンターのセキュリティ

クラウドサービス契約では、データセンターの物理的なセキュリティはサービスプロバイダによって完全に管理される。そのため、データやアプリケーションが保管される場所のセキュリティについて明確に理解しておくことが重要である。これは、データセンターが取得した証明書（もしあれば）、および／またはクラウドサービスプロバイダと人道団体との関係の基礎となる契約上の義務を検証することで理解できる。保証されるセキュリティレベルは、アプリケーションがクラウドでホストされるために必要なセキュリティレベルと一致しなければならない。物理的な監査によって有用な情報を得られるが、大抵のクラウド環境では監査が実現する可能性は低い。

10.4.2.3 保存データのセキュリティ

保存データのセキュリティレベルは、必要なサービスの種類やサービスプロバイダとの契約によって異なる。ただし、データが共有の記録媒体に保存されると想定することが妥当であるため、関係する**第三者**認証と共に、保護レベルとその達成方法についてのサービスプロバイダによる明確な文書が必要である。しかし、保存データについて、少なくともほとんどの**機微データ**については、クラウドプロバイダーのセキュリティだけに依存するのではなく、暗号化などの保護層を追加することが推奨される。

10.4.2.4 データのサニタイズ

クラウド環境の特徴は、リソースの提供、消去、移行が頻繁に行われることである。換言すれば、共有インフラストラクチャの様々な部分にデータやアプリケーションを容易に移行できるということを意味する。他のカスタマーのアプリケーションが**人道団体**が以前使用していたものと同じハードウェアで実行される可能性が高いため、クラウドが正しく管理されていないとデータが開示される危険性がある。更に、データはクラウドインフラストラクチャ内に無期限に保存され得る。この脅威を制御するために対策を取る必要がある。そのためには専用のリソースを使用するか、データを削除またはサニタイズするためにどんな対策がとられているかをプロバイダーに確認しなければならない。サービスプロバイダの対策とは別に、暗号化を使用することで保護層の追加もできる。

10.4.2.5 機器の廃棄

機器の廃棄は前述の点と密接に関連しており、ハードウェアの解体時や廃棄時にデータや情報が残っていたり開示されたりする可能性がないという強い確証が必要である。クラウドプロバイダーは、この要件が満たされていることを保証するか、または他の手段（暗号化）を採用しなければならない。

10.4.2.6 可用性

クラウドサービスでは、必要なレベルの可用性が提供されなければならない。この点で**SLA（サービスレベル合意書）**は最も重要である。また、SLAは損害賠償責任の観点からも検討される必要がある。公開されている情報の検証が推奨され、提供されるサービスの実際の信頼性を確認するのに役立つ。

10.4.3 ユーザー間の分離

クラウド環境では、サービスプロバイダがユーザーの分離を保証する責任を負う。しかし、クラウドプロバイダーを評価する場合、そのクラウドプロバイダーと関連技術が広く知られていない場合は尚更、利用されている技術を評価し、どのように分離が保証されているかを理解するために有用な情報を収集することが重要になる。分離には幾つか影響を受ける要因があり、サービスモデル、実装モデル（パブリッククラウド若しくはプライベートクラウド）といったモデルの違いや、その他の要因が挙げられる。分離手段の有効性を評価するためにペネトレーションテストは役に立つが、限定的ではある。すなわち、試験が実施される特定の期間にのみ有効であり、既知の問題についての兆候しか得られない。また、過去のインシデントやプロバイダーによる管理のバックグラウンドのチェックが非常に有用である。

10.4.4 ガバナンス

サービスプロバイダは適切なセキュリティのガバナンスフレームワークを持つ必要がある。このフレームワークが全てのセキュリティ上の取り組みの管理や統制の基盤となり、また脅威の変化やテクノロジーの発展を管理するための基盤にもなる。そして、クラウドプロバイダーは、クラウドのセキュリティを担当するC*レベルの管理者（例：**CSO**、**CISO**、**CTO**）に通常義務付けられる必要な要件を有していることを証明しなければならない。また、適切に実施されるセキュリティガバナンスのフレームワークを持っていること、通常のリスク・財務管理にセキュリティやセキュリティリスクが含まれていること、規制および法的要件に準拠していることも証明しなければならない。こうした広く認められている基準への適合性を評価すべきである。

10.4.5 オペレーショナルセキュリティ

クラウド提供サービスは厳格なセキュリティ要件に従って運用されなければならず、標準的なオペレーション手順にセキュリティの事柄が組み込まれている必要がある。主な要件は下記の通りである。

- 環境設定および変更の管理：本番環境の内容およびそれに関連した変更の管理、必要なテストの実施、変更前に適切な承認を得る
- 脆弱性の管理：サービスやインフラストラクチャで発生する可能性のあるセキュリティ問題の評価、特定および修正
- モニタリング：サービスのセキュリティを損なう危険性のある異常や攻撃、不正アクションの検出
- インシデント管理：インシデントが発生した場合、サービスプロバイダは問題を軽減、制御、正しく修正するための適切な措置を講じることで問題に対処しなければならない。これにはカスタマーや法執行機関への連絡および報告が含まれる

10.4.6 人材

クラウドサービスプロバイダは、サービス管理を担当する人材の信頼性を評価するための手段を講じなければならない。特権を持つ役割や機微性の高い役割を担う人員については、適切なバックグラウンドチェックとスクリーニングを実施すべきである。オペレーターは訓練を受けることで自らの責任を理解、認識しなければならない。

10.4.7 開発

サービスプロバイダは通常、インフラストラクチャの大部分を開発している。開発中に脅威を確実に評価できるよう、ベストプラクティスと業界標準を用いる必要がある。安全な設計、コーディング、テストおよび導入のためのガイドラインを設けなくてはならない。

10.4.8 サプライチェーン

クラウドプロバイダーは、多くの場合、**第三者**の製品やサービスを利用して自らの提供するサービスを統合、管理している。サプライチェーンの弱点はクラウドサービスとアプリケーション全体のセキュリティを脅かすことになる。プロバイダーは、第三者の供給者がどのようにスクリーニングされているかを次の点で明らかにしなければならない。サービスと製品の受け入れプロセス、セキュリティリスクの管理方法、サービスプロバイダのセキュリティ態勢の検証方法、スペアパーツ、アップデート、その他の変更の検証方法。このプロセスは、**クラウドサービス**が階層化され、チェーンの下位にある他のサービスプロバイダに依存している場合には、さらに重要度を増す。可能であれば、供給者の検証を実施するか、若しくはクラウドプロバイダーが機関にとって受け入れられない**第三者**供給者を利用することを防止する契約を締結すべきである。

10.4.9 ユーザー管理

提供されるサービスによっては、承認プロセスの一部がクラウドプロバイダーによって管理されることもあり得る。管理インターフェースへの安全なアクセスを確保するために、このプロセスを評価して、ベストプラクティス、規制、機関のニーズに沿っているかを検証する必要がある。管理インターフェースは、従来のデータセンター内で実行される物理的なアクションとある程度同等とみなすことができるアクションのパフォーマンスは許可する。従って、そのようなアクションは慎重に監視されなければならない。権限や特権を適切に管理できるよう、権限は詳細に設定する必要がある。

10.4.10 アイデンティティと認証

ユーザー管理と同様に、サービスインターフェースへのアクセスは厳密に保護する必要がある。認証および承認プロセスの実施は、組織のセキュリティニーズに適合するように評価されるべきである。様々なアプローチの例として、二段階認証、**TLS**クライアント証明書認証の使用、シングルサインオンシステムなどがある。採用される方法は、セキュリティの発展と脅威の高度化に伴って常に最新のものでなければならない。

10.4.11 外部インターフェース

管理インターフェースが露出されると、悪意のあるエンティティが利用できる攻撃範囲が増加する。従って、この脅威に対して管理インターフェースのセキュリティを評価する必要がある。プライベートネットワークや、プライベートインターフェースにアクセスするための同等の手段といった解決策の可用性を評価すべきである。

10.4.12 サービス管理

管理システムは攻撃者にとって非常に価値が高いため、慎重に構造を実装し、管理を実施する必要がある。従って、管理システムの管理法や手順の説明はサービスプロバイダのセキュリティ態勢を評価するのに役立つ。

10.4.13 監査

サービスプロバイダは独立した監査の結果を公開するか、または機関からの独立した評価や監査の求めに応じなくてはならない。サービスに関する監査データ（パフォーマンス、ダウンタイム、セキュリティインシデントなど）も検査のために公開すべきである。

10.4.14 サービスの使用状況

組織はインターフェースや、データ送受信、ユーザーの承認プロセス、管理、ワークロード、その他クラウドと組織活動の総体としてみなされるサービスに影響を与える事柄など、クラウドサービスとの間で発生する相互作用を明確に理解しなければならない。クラウドソリューションを利用する前に、データフローや、プロセス、構造の詳細な評価をする必要がある。適切な手順が考案、実施され、職員も訓練されている必要がある。また、クラウドソリューションや使用法、機関との関係、その他、クラウドソリューションの正しい使用や管理に係る情報について、必要な知識がオペレーターに提供されていなければならない。

10.5 データ主体の権利

データ主体は、クラウドで処理された**個人データ**に関しても、アクセス、訂正、削除、異議申立てをする権利を有する。[184] **人道団体**は、再委託先がデータを事後処理する場合であっても、クラウドプロバイダーが技術的および組織的にこれらの要件を侵害しないことを検証する必要がある。クライアントとプロバイダーとの間の契約において、**データ主体**による権利行使の促進をクラウドプロバイダーに求めるべきであり、これらの権利行使がいかなる再委託先との関係においても確実に保証されるようにしなければならない。

10.6 国際的なデータ共有

クラウドサービスには、その性質上、各国の様々な関係者との**個人データ**の国際的な共有が含まれる。データ保護法は**国際的なデータ共有**を規制している。従って、**人道団体**は、**クラウドサービス**の使用に対して適用される法律がある場合はその法律に準拠していること、また、団体内の方針にも準じていることを保証すべきである。これは例えば、クラウドプロバイダーとの如何なる契約においても、プロバイダーが**国際的なデータ共有**に関する法的要件をどのように遵守しているかを示すべきであることを意味する（例えば、その事業体や再委託先との間の契約条項の適用などを通じて）。**国際的なデータ共有**に先立ったDPIAの実施[185]によって、データ保護の観点からデータ**処理**の合法性を更に強化することができる。

184 セクション2.11：データ主体の権利を参照
185 セクション10.8：データ保護影響評価を参照

10.7 データ管理者とデータ処理者の関係

上記セクション4.5[186]で記述したように、**個人データ**をクラウドに置く**人道団体**と、そのために契約しているクラウドプロバイダーとの関係は、**データ管理者**と**データ処理者**との関係に等しいと一般的には言えるだろう。しかし実際には、それぞれの役割を分類することは、クラウドプロバイダーがどの程度の裁量権を持っているかに依るため、一見するほど容易ではなく、プロバイダーとクライアントとの間の合意において定義するべきである。重要なのは、これらの不確実性が**データ主体**の権利に影響を与えてはならないということである。つまり、**人道団体**は**クラウドサービス**の利用について可能な限り透明性を保つべきであり、クラウドプロバイダーが**データ主体**に不利益をもたらすことを許すべきではない。

人道団体による**クラウドサービス**の利用では、クラウドプロバイダーが再委託処理者を採用することが一般的である。プロバイダーとの契約では、**データ管理者**（**人道団体**）からの**同意**に基づいてのみ再委託処理者を採用できることを明記しなければならない。**データ処理者**（クラウドプロバイダー）は、再委託処理者に関する変更を**データ管理者**に通知する義務を有しており、**データ管理者**はその変更に異議を唱える、または契約を終了する選択肢を保持している。

10.8 データ保護影響評価

データ保護影響評価（DPIA）は、プロジェクト企画時に、データ保護規制や想定できるリスクの全側面を確実に評価する重要なツールである。**クラウドサービス**の利用に関心がある場合には、クラウドコンピューティングに合わせた特定のDPIAを実施することが不可欠である。[187]DPIAでは**処理**の詳細と規定を明確にし、それによってもたらされるリスクと緩和措置に焦点を当てなくてはならない。これに関して重要な留意点は、**クラウドサービス**を利用する前にDPIAを実施すべきであるということである。

186 セクション4.5：データ管理者とデータ処理者の関係を参照
187 第5章：データ保護影響評価（DPIAS）を参照

10.9 特権・免除とクラウド

上記の考慮事項に加えて、特権と免除を享受する**人道団体**は、特定の法的、技術的、組織的措置を取らない限り、クラウドに置かれたデータが自らの特権と免除による保護を危うくする可能性があることも考慮すべきである。人道上の緊急事態においては特にこの考慮が重要であり、特に紛争やその他の暴力を伴う事態において**人道団体**の特権と免除が脆弱な個人の**個人データ**を保護するための第一線となり得るからである。

人道団体は、その特権と免除がクラウド環境において十分に保護されることを保証するため、以下に示す法的、組織的、技術的措置の実施を検討すべきである。

10.9.1 法的措置

- 外部の**データ処理者**がデータをホスト、処理して良いのは、該当の団体のデータがどこで誰によって保持されているかに拘わらず、ファイル、アーカイブ、文書のやり取り、通信の不可侵性を承認し、あらゆる形式の法的手続を免除する地位協定によって、団体の特権と免除が正式に認められている管轄区内においてのみに限定するべきである。この法的保護は、理想的には、そのような特権および免除が一貫して尊重されてきた実績によって裏付けられるべきである。
- **データ処理者**および再委託先は、データへのアクセスを求める当局に対し、要請の該当データが**人道団体**の特権および免除の対象となっていることを通知するという契約上の義務を有している。また、非公式、行政上のまたは法的手続を問わず、当局からのアクセスの要請を拒否し、代わりに当局の要請を**人道団体**に通知する義務、非公式、行政上のまたは法的手続を問わず、当局からデータへのアクセスの要請があること、その当局の身元、および要請の状況を直ちに人道団体に通知する義務、非公式、行政上の、または法的手続を問わず、当局から要請を受けたデータに関して**人道団体**の特権および免除を主張するため、**人道団体**が手続の一環として必要となる情報や証拠文書を**人道団体**に提供することで、人道団体を支援する義務も有している。

10.9.2 組織的措置

- **人道団体**のデータは個別のサーバーに保存されるべきであり、そのデータは**データ処理者**および再委託処理者の他のクライアントのデータから隔離するべきである。
- **人道団体**のデータをホストするサーバーには機関の標章を明確に表示し、サーバーには「法的な特権に守られた情報」を示すマークを付けるべきである。
- 可能であれば、**人道団体**のデータをホストするサーバーは、**データ処理者**と**人道団体**の両者の承認によってのみデータアクセスが可能とするべきである。

- **データ処理者**および再委託処理者の職員は、人道団体が持つデータの特権について適切に理解すべきであり、また、第三者によるアクセス要求の場合に取るべき手順を身に付けておかなくてはならない。

10.9.3 技術的措置

- クラウド環境でホストされるデータは暗号化されるべきであり、**人道団体**のみがその暗号鍵を保有すべきである。
- 利用を想定しているクラウドソリューションが**SaaS**であり、**データ処理者**および**サブプロセッサ**が提供されるサービスを管理する必要がある場合、その**データ処理者**と再委託処理者が、保護されていない（暗号化されていない）データに一切アクセスすることなく、クラウドシステムにアクセスして管理やアップデート、バグの修正、ユーザーのサポートを行うことを保証する契約が必要になる。


モバイル
メッセージング
アプリ
利用可能性
効率的な
調整
遠隔地又は
アクセスできない
場所にいる
人々との
即時通信
多数の個人に
向けた
ブロードキャスト
コンテンツ
課題
メッセージング
アプリから
集まった情報の
処理に関し、
人道団体による
明確なガイダンスが
必要
処理する
データの種類に
関する認識不足
メタデータへは
第三者による
アクセスと分析が
可能であり、
それらの第三者に
よって脆弱な個人に
不利益となる形で
利用される可能性

第11章

モバイル
メッセージングアプリ

11.1 はじめに [188]

人道団体は日常業務において、公式（例えばラジオやテレビ）、非公式、および直接的な情報交換手段を含む複数のコミュニケーション手段に依存している。与えられた状況で最も適切なコミュニケーション・チャンネルを使用するため、**人道団体**は、危機の影響を受ける特定社会の文化的背景とニーズ、そしてコミュニケーション手段を理解しなければならない。

メッセージングアプリは、危機や紛争の影響を受けた人々との即時コミュニケーションを可能にし、内部のタスクや行動を効率的に調整するのに役立つので、**人道団体**にとって魅力的ツールである。この種の技術は**人道支援**の有効性と効率性を高め、遠隔地やアクセス困難な場所にいる人々に手を差し伸べることができる。しかし、メッセージングアプリは、個人情報保護に関するリスクを十分に考慮せずに採用されることも多い。

イタリアのコモにあるサンジョバンニ駅近くの仮設キャンプにある一時的な Wi-Fi スポットで携帯電話を充電する難民たち（2016 年 8 月）

188 本章は、ICRCによる*Humanitarian Futures for Messaging Apps*, The Engine Room and Block Party、2017年1月：https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html に基づいている。

モバイルメッセージングアプリは、優れた機能にもかかわらず、その使用には重大なデータ保護リスクを伴う可能性がある。実際、**人道団体**は、リスク分析や長期間の持続可能性と管理を考慮した正式な手続を踏まずに、場当たり的に使用することがある。それらの機関の差し迫った情報とコミュニケーションのニーズに焦点が当てられているからである。このアプローチにリスク分析が含まれない限りは、説明責任、適切性、無害性、デュー・ディリジェンスといった**人道団体**の指針に反することになる。他の通信手段と同様に、メッセージングアプリの採用には、その利点とリスクを慎重に考慮する必要がある。分析に含める問題点の多くは特定の状況の個別条件による。例えば**個人データ**に関して、政治的暴力状況下にあるセキュリティ上の懸念は、自然災害におけるセキュリティ上の懸念とは大きく異なる可能性がある。

携帯電話やその他のスマートデバイスにインストールされたモバイルメッセージングアプリは、**個人データ**保護の権利を侵害する可能性がある。これは、アプリがユーザー間のデータ交換だけでなく、大量のデータ（メタデータ、位置データ、連絡先など）を処理、集約、生成する可能性を提供するからである。一部のデータ保護規制当局は、**個人データ**保護に対するリスクは、以下の要因が組み合わさって生じると考えている。（1）ユーザーがスマートデバイス上で実際に**処理**するデータの種類についての認識欠如、（2）ユーザーの**同意**の欠如、（3）セキュリティ対策の不備、（4）**追加処理**の可能性。[189]

「デジタル近接」の必要性（すなわち、受益者の所在について、**人道団体**が物理的に確認しようとするのと同様、デジタル的にも確認を目指している状態）に従い、**人道上の緊急事態**の際に、**人道団体**はWhatsApp、Facebook Messenger、スナップチャット、Viber、Telegram、LINEなど、特定の社会で普及しているモバイルメッセージングアプリを利用する傾向がある。同時に、あまり一般的ではないコミュニケーションプラットフォームを導入すると、**人道団体**が支援しようとしている人々が対象から排除される可能性が出てくる。

モバイルメッセージングアプリの採用は、**個人データ**を含む収集データの**追加処理**につながる可能性もある。モバイルメッセージングアプリはオンラインで情報を収集することで、利用可能なデータを分析する新しい方法を提供するかもしれない。つまり、モバイルメッセージングアプリを通じて収集されたデータとメタデータは、新しい方法で情報を三角測量するのに役立つ可能性がある。

個人データの**追加処理**では、メッセージングアプリを使用する目的と、収集したデータを共有する関係者を考慮することが重要である。**人道団体**は、複数の関係者との複数の交渉を必要とすることがあるため、提供されたデータをユーザーが破棄または削除できると自信を持って述べることができない場合がある。

189 Article 29 Data Protection Working Party, Opinion 02/2013 on smart devices（WP 202, 2013年2月27日）を参照

モバイルメッセージアプリは、主に個人や小人数グループのプライベートなコミュニケーションのために設計された。この種の機能は、**人道団体**が基本的なカウンセリングを提供したり、進行中の紛争または特定のニーズについて受益者から情報を得る場合に利用が可能である。これらのアプリは、**人道支援**において、多数の個人の連絡先やフォロワーにコンテンツを「放送」するためにも使用することができる。特に、ユーザー数が非常に多い状況では、モバイルメッセージングアプリは一方通行の放送チャンネルとして機能可能である（例えば、人道支援物資の配布時間や場所、または地元の診療所の営業時間変更のお知らせなど）。

11.1.1 人道支援のためのモバイルメッセージングアプリ

メッセージングアプリは、ユーザーが携帯電話やその他のスマートポータブルデバイスを使用して情報を送受信できるようにするソフトウェアプログラムである。アプリの使い易さが人気、大衆の支持、継続的に増加する需要に大きな影響を与えてきた。モバイルメッセージアプリを使ったコミュニケーションと、携帯電話ネットワークを使ったコミュニケーションには、大きく次の三つの違いがある。[190]

- モバイルメッセージアプリは、Wi-Fiインターネット接続またはモバイルデータ接続を使用してデータを送受信しており、従来の電話網で送信されるSMSメッセージとは異なる。
- モバイルメッセージアプリでは、SMSやそのマルチメディア対応の後継機能であるMMSを使用した場合よりも、さらに様々な種類のデータを送受信できる。モバイルメッセージアプリ同士では、徐々に相違点よりも類似点の方が多くなり、音声通話やテキストメッセージに加えて、写真、イメージ、（場合により）ドキュメントファイル、ボイスメールと同様の機能を持つ音声録音、携帯電話のGPSセンサーに基づく位置確認データ、ライブビデオコール（一部のアプリ）、emoji（絵文字：感情または特定の物体の絵文字表現）など各種の情報も送受信できるようになった。
- モバイルメッセージアプリはエンドツーエンドで暗号化されたコンテンツを送信できる。ただし、大量の暗号化されていないメタデータを生成して保持する場合もある。

そして**人道団体**は、以下のような理由からモバイルメッセージングアプリを採用している。[191]

- すでにメッセージアプリを使用している人々（スタッフまたは受益者）を対象とするため
- 通信コストの削減
- 移動中の人々（スタッフか受益者に関わらず）との信頼できる接触を維持するため、また、他の通信手段が利用できない環境にいる人々とのコミュニケーションを可能にするため
- 通信速度を上げるため

190 ICRC、The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps*、2017 年 1 月、https://shop.icrc.org/humanitarian-futures-for-messaging-apps-print-en.html

191 人道支援にモバイルメッセージングアプリを導入する理由の詳細については、*Humanitarian Futures for Messaging Apps*、ICRC、The Engine Room and Block Party、2017年1月、前掲書を参照

- 既存の通信方法と比較してデジタル通信の安全性を向上させるため（そのようなアプリがコンテンツのエンドツーエンドでの暗号化を提供する場合）
- アクセス困難な地域、遠隔地またはアクセス不可能な地域での情報収集や発信を容易にするため
- データ収集の迅速化や効率化のため
- オフィス間の調整を改善するため

上記の考察に基づき、データ保護の観点から、二つの区別すべき個別の分析分野が挙げられる。

- メッセージングアプリ自身による**個人データ処理**
- モバイルメッセージングアプリを通じて収集された**個人データ**で**人道団体**により**処理**されたもの

次に、これらについて説明する。

11.2 データ保護基本原則の適用

この章のデータ保護に関する説明は、第Ⅰ部で詳述した原則に基づいている。

11.2.1 モバイルメッセージアプリを使用した個人データの処理

メッセージングアプリを通じて人道上の緊急事態にある個人と連絡を取るには、大抵の場合、**人道団体**は大半の人が既に使用しているアプリケーションをインストールし、それを使用する必要がある。ほとんどの場合、個人の受益者はそのようなアプリケーションをダウンロードおよびインストールし、その際にデータ保護条件に同意している。

人道団体は、モバイルメッセージアプリを通じて受益者と連絡を取ることにより、直接的であれ間接的であれ、そのような連絡手段は安全であり、受益者に危害が生じる可能性はないことを示すことができる。したがって、個人受益者が使用開始時にアプリ・プロバイダに与えた**同意**にかかわらず、**人道団体**がアプリ利用の影響に関する明確な分析を行い、彼らのアプリ使用によって予期せぬ悪影響が生じないようにすることが重要である。DPIAを用いてこれを行い、以下の事項を考慮することが推奨される。DPIAの成果として、特定の種類のデータのみが特定のアプリを通じて収集または伝達されること、または特定のアプリは特定の状況においてのみ使用され、それ以外では使用されないことである。特に人気の高いアプリを使用することが人道団体にとって不適切である場合、**人道団体**は、より安全な他のアプリを使い連絡を取る意図を個人に通知する、という目的のみでそのアプリを使用することもある。評価を実施する際に、メッセージアプリが頻繁に機能を開発、変更していることに留意することも重要である。またアプリが提供する機能が無期限に利用可能であるという保証はなく、特に暗号化が法律で制限されている国では、ユーザーが最新のソフトウェアを入手しているという保証もない。同様に、データの

使用、セキュリティ、およびプライバシーに関する企業のポリシーや声明は、事後的に改訂される可能性もある。**人道団体**は、基盤となるコードの技術的な詳細にはアクセスできないことも多く、変更がユーザーのセキュリティやプライバシーにどのような影響を与えるかを包括的に評価できない場合がある。情報の管理と処理に第三者のプロバイダーを使用する場合も、**人道団体**はこれらのリスクへの対処を準備する必要がある。アプリケーションの機能を変更するには、DPIAの改訂が必要になる場合がある。

アプリを通じた受益者との一方向あるいは双方向のコミュニケーションの違いもまた大切である。後者はしばしばはるかに高いリスク（より多くの個人情報が転送される可能性）を伴い、予想に反する長期的な管理/持続可能性の問題を提起するからである。

11.2.1.1 潜在的な脅威

データ保護とプライバシーに関する懸念は、**人道団体**の業務のあらゆる分野で発生するため、これらの組織では、メッセージングアプリの導入を検討する際に特定のリスクを評価すべきである。最も懸念されるのは、想定外の第三者が、**人道団体**が収集したデータに対し、人道的活動の中立、公平、独立に反する目的でアクセスする可能性である（例えば、地方当局、法執行当局、様々な利害関係者によって動かされるグループ、民間団体等によるアクセス）。

これらの第三者には、次のものが含まれる

- 難民の出身国に存在する団体（武装集団および当局を含む）であって、危害を与えまたは標的とする目的で集団または個人を識別する意図があるもの
- 移住政策や安全保障上の利害を持つ団体で、移住の傾向や流れを把握し予測する意図があるもの
- 国家安全保障のための監視に関与する団体
- **人道団体**や支援者に対し暴力的な攻撃や敵対的意図をもつ団体
- 特定の集団の行動プロファイリングを実施する意図を持つ営利団体[192]

この分野の懸念は、データ保護・プライバシー・コミッショナー国際会議による2015年の「プライバシーと国際的な**人道支援**に関する決議」において以下の通り認知され支持されている。

192 Maria Xynou and Chris Walker、*Why we still recommend Signal over WhatsApp*、2016 年 5 月 23 日: https://securityinabox.org/en/blog/2016-05-23/why-we-still-recommend-signal-over-whatsapp-even-though-they-both-use-end-to-end-encryption

「特権や免除を与えられていない**人道団体**は、人道的目的のために収集したデータを、他の目的（例えば移民動向の管理やテロとの闘い）に利用するために当局に提供するよう圧力を受けることがある。データの不適当な使用によるリスクとして、避難民のデータ保護権に深刻な影響を与える可能性があり、避難民の安全と、より一般的な**人道支援**に害をもたらす可能性がある。」[193]

11.2.2 メッセージアプリが収集し保管するデータの種類

モバイルメッセージングと暗号化の世界には、主にSignal Protocol、MTProto、iMessageという三つのプロトコルが存在する。[194]

1. Signal Protocol（以前はAxolotlおよびTextSecureとして知られていた）はOpen Whisper Systemsの Signal Messenger、Facebookの WhatsApp、Facebook Messenger（秘密の会話で）、Google Allo（シークレットモードで）、Skype（2018年半ばからプライベートな会話で）、Viber（独自の修正版）で使用されている。
2. MTProtoはTelegram（シークレットモードで）によって開発され、使用されている。
3. iMessageプロトコルはAppleによって開発され、iMessageで使用されている。

これらのメッセージング・プロトコルはそれぞれ、異なる種類のデータを生成および処理し、また、メッセージコンテンツおよびメタデータを異なるレベルで保護する。

メッセージコンテンツ：一部の主要なメッセージングアプリ企業は、アプリにはエンドツーエンドの暗号化を提供しており、メッセージの内容を解読または読み取ることができないと述べているが、Facebook Messengerのように一般的に広く使用されているアプリは全てのメッセージコンテンツを自社のサーバーに保管している。エンドツーエンドの暗号化を提供するアプリの中には、オプトイン機能としてのみ含まれているものもあることは留意すべきである（Telegram、LINE、Facebook Messengerなど）。つまり、設定でこの機能を有効にする必要があることをユーザーが認識していない限り、全てのメッセージデータが暗号化されずに送信される可能性がある。Telegramのようなボットとの通信は、ほとんどエンドツーエンドで暗号化されていない。コンテンツは保護されていても、メタデータには同じ種類の保護機能が備わっていない可能性に注意することが重要である（後述の「メタデータ」を参照）。[195]

193 International Conference of Data Protection and Privacy Commissioners、Adopted Resolutions、Resolution on Privacy and International Humanitarian Action, 2015、前掲

194 ICRC and Privacy International、“Chapter 6: Cash Transfer Programmes”、The Humanitarian Metadata Problem: *Doing No Harm in the Digital Era*、2018年10月、p. 50

195 Lucy Handley、“Sheryl Sandberg: WhatsApp metadata informs governments about terrorism in spite of encryption”、CNBC、2017年7月31日、Lucy Handley、“Sheryl Sandberg: WhatsApp metadata informs governments about terrorism in spite of encryption”、CNBC、2017年7月31日、https://finance.yahoo.com/news/sheryl-sandberg-whatsapp-metadata-informs-112540721.html

ユーザー情報：アプリにサインアップすると、ユーザーは自分の情報（ほとんどのアプリの場合は電話番号にはじまり、WeChatやFacebook Messengerのようなアプリの場合は画像、フルネーム、メールアドレスまで）を提出するよう求められる。世界中の多くの国でSIMカード登録が強制されているが、これらの国では電話番号を提出しなければならないため、個人が匿名でメッセージングアプリを利用することは事実上できない。中南米の一部地域では、携帯電話番号の登録が必要である。[196]多くのアプリは、サインアップ時にユーザーの電話番号連絡先リストに自動的にアクセスして、既にアプリをインストールしている連絡先を探し出す。場合によっては、アプリがこのデータを個別に保存することもある（例えば2016年6月、WhatsAppは連絡先リストの情報を保存していることを認めた）。[197]ユーザーが属するグループの詳細も保存される場合がある。

メタデータ：サービス規約に基づき、アプリケーションは、アプリケーション内からアクセスするサイトや情報など、様々な量のメタデータを収集する。メッセージから取得できるメタデータの例には次のようなものがある。IMEI/IMSI（デバイスおよびSIM識別子）、送信者の電話番号、受信者の電話番号、メッセージサイズ、位置データ、時刻データ、IPアドレス、ハードウェアモデル、およびWebブラウザ情報。[198]多くのアプリ会社は、そのようなデータはサーバー上に保持されると述べているが、データが保持される時間の長さや、メタデータが暗号化されるかどうか、どのように暗号化されるかについてはほとんど明らかにしていない（エンドツーエンドの暗号化を実施したと主張するアプリでも例外ではない）。
メッセージングアプリの中には、PC向けに、Tor（トーア）匿名通信システム（匿名ブラウジングを可能にするソフトウェア）を使用しユーザーのメタデータを隠すことができる機能を提供するものもあるが、[199]現在利用可能な主要なメッセージングアプリ上ではこのオプションは選択できない。一方で、Signalのようなプライバシーを意識したアプリは、[200]収集するメタデータをできるだけ少なくすることを目的としている。

196 GSMA、*Mandatory registration of prepaid SIM card: Addressing challenges through best practice*、2016年4月：www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Mandatory-SIM-Registration.pdf

197 Micah Lee, *Battle of the secure messaging apps: How Signal beats WhatsApp*、The Intercept、2016年6月22日、6: https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/

198 ICRC and Privacy International、"Chapter 6: Cash Transfer Programmes" in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月、p.60

199 以下は全てTorの秘匿サービスを利用している（匿名通信を可能にするように設計されたソフトウェア）、Guardian Project, What is *Orbot*? https://guardianproject.info/apps/orbot/、Security in a Box, *Guide to Orbot* https://securityinabox.org/en/guide/orbot/android、*Tor Project, Tor Messenger Beta: Chat over Tor, Easily*、2015年10月29日：https://blog.torproject.org/tor-messenger-beta-chat-over-tor-easily/；Joseph Cox、'Ricochet', *the Messenger That Beats Metadata, Passes Security Audit*、2016年2月17日：http://motherboard.vice.com/read/ricochet-encrypted-messenger-tackles-metadata-problem-head-on

200 Signal, *Grand jury subpoena for Signal user data*, Eastern District of Virginia、2016年10月4日、https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/

推測されるデータ：コンテンツのエンドツーエンドの暗号化を使用しても、メッセージングに関するメタデータから多くの情報が推測できる。
ベルギーにあるMITとCatholique de Louvain大学の研究者らは、欧州の小国において150万人の携帯電話ユーザーのデータを15カ月にわたって分析し、わずか4つの参照点を使って、空間的、時間的解像度がかなり低い中でも95%のユーザーを一意に識別できることを発見した。つまり、百万人以上の「匿名化」されたデータセットから、一人の人物の完全な位置情報を抽出するには、その人物が携帯電話の伝達物から数百ヤード以内に、ある時は一時間、あるいは年に四回程度位置するだけでよい。もしTwitterの投稿の中にその人の位置の特定情報が含まれていれば、数件の投稿内容だけでおそらく必要な全ての情報が提供されているだろう。[201]

第三者プロバイダーと共有するデータ：メッセージングアプリ会社は、アプリの動作を可能にするサービスを提供する他の会社とユーザーの個人情報を共有する、としばしば述べている。しかし、どの企業と提携しているのか、どのようなサービスを提供しているのか、どのようなデータにアクセスしているのか、どのようにデータが処理および保存されているのかについてはほとんど言及していない。Twilioは、いくつかのメッセージングアプリ会社と提携しているサードパーティープロバイダーであるが、制限付きで透明性に関する報告を提供している。その報告によると、2015年上半期では46件だった国際機関からのデータ要求が2016年上半期では376件となった。[202]

ユーザーが自分のスマートフォンにアプリをインストールした証拠：当局は、個人のデバイスにアクセスすることで、そのユーザーが特定のメッセージングアプリをインストールしたという物理的な証拠を見つけることができる。また、他の方法でアクセスすることも可能である。例えば、ほとんどの場合、ユーザーはアプリをダウンロードするためにスマートフォンにメールアドレスを関連付ける必要があり、アプリと他のオンラインアクティビティの間に追跡可能なリンクを作成することとなる。

201 L. Hardesty、"How hard is it to 'de-anonymize' cellphone data?" , MIT News、2013年3月27日、https://newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data

202 Twilio, *Transparency Policy*：https://www.twilio.com/en-us/legal/transparencyを参照

11.2.3 どのようにして他者がメッセージングアプリに共有されているデータにアクセスできるか

他者は様々な手段で、メッセージングアプリから送信されたデータにアクセスする可能性がある。

- メッセージングアプリ会社（またはアプリユーザーの個人情報にアクセスする第三者プロバイダー）が、そのサーバー上に保存しているメッセージコンテンツまたはメタデータについて、そのようなデータが保存されている管轄地域の当局からの開示要求に応じる。
- 他者がメッセージングアプリ会社のサーバーに保存されているメッセージコンテンツやメタデータに違法または秘密裏にアクセスを行ったり（ハッキング）、両者の間を行き来しながらその情報にアクセスしたりする（「中間者攻撃」として知られている）。例えば、トロント大学のCitizen Labが2013年後半に行ったテストでは、メッセージングアプリLINEは、Wi-Fi経由で送信されるコンテンツは暗号化されていたが、3G経由で送信されるコンテンツを暗号化していなかった。[203]
- デバイス（例えば携帯電話やコンピュータ）が押収された場合、フォレンジックツールを使用して、ユーザーが消去したコンテンツやデータなどのメタデータにアクセスできる。[204]抽出ツールを使用すると、次のようなデータをダウンロードできる。
  - 連絡先
  - 通話データ（誰に、いつ、どのくらいの時間通話したか）
  - テキストメッセージ
  - 保存されたファイル（写真、ビデオ、オーディオファイル、文書など）
  - アプリデータ（使用しているアプリケーションとそのアプリケーションに保存されているデータ）
  - 位置情報
  - Wi-Fiネットワーク接続（職場や訪れた場所など、Wi-Fiに接続した場所が特定できるもの）

携帯電話抽出ツールの中には、携帯電話に直接ではなく、クラウドに保存されたデータ、または、存在を知らない、あるいはアクセスできないデータにアクセスするものもある（つまり、消去されたデータ）。[205]

---

203 3Gネットワークはデフォルトで暗号化されているが、ネットワーク・プロバイダのレベルでのみ行われる。つまり、インターネット・サービス・プロバイダ（ISP）や電気通信事業者は、これらのプロバイダーを通じて送信される情報を復号化できる。Citizen Lab、*Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications*、2013年11月：https://citizenlab.ca/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/、*Thailand's Government Claims It Can Monitor The Country's 30M Line Users*：https://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/

204 ICRC and Privacy International、"Section 5.3 Other Metadata" in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月

205 Mobile Phone Extraction、Privacy InternationalとLibertyが共同キャンペーン"Neighbourhood Watched: How policing surveillance technology impacts your rights"の一環として作成した解説書https://privacyinternational.org/neighbourhood-watchedから入手可能

- 他者がその他の秘密の方法でメッセージングアプリのコンテンツにアクセスする。これには、ユーザーがアプリにサインアップするときに送信されるSMSログインコードに、従来のモバイル電話ネットワークのトラフィックをリダイレクトすることでアクセスする方法や[206]、リモートでその電話や保存されたデータにアクセスできるようにするマルウェア（悪意のあるソフトウェア）を自分の電話にインストールするようユーザーを誘導することなどが含まれる。[207]
- 個人が自分のデバイスを手渡すことを強制される。エンドツーエンドの暗号化は、ユーザーのデバイス上ではなく、転送中のデータのみを暗号化するものである。ユーザーにロック解除を強制する方法などで、ユーザーのメッセージングアプリのアカウントにアクセスできるようになれば、メッセージの内容やデバイスにインストールされているアプリ詳細にアクセスが可能となるだろう。一部の国の当局は、WhatsAppのようなアプリをインストールするだけで破壊的行為の範疇になると考えている。[208]Signal、Telegram、スナップチャットはいずれも「自動消滅メッセージ」を提供しており、これらのサービスは送信者および受信者の携帯電話に一定期間保存された後、自動的に消去される。
- メッセージングアプリ会社は、そのコードに秘密の機能（「バックドア」として知られている）を組み込むことで、当局がアプリ上で送信されたコンテンツやデータに直接アクセスすることを許可している。例えば、WhatsApp、Telegram、Viberを例に挙げると、コードにバックドアを導入していないメッセージングアプリ企業に罰金を科すと脅している国もあるという。[209]他の企業は、政府機関からのバックドア機能組み込み要請を拒否したことを公に述べている。[210]諜報機関が暗号化されたコンテンツにアクセスできるようにしようとする試みは継続している。[211]

206 Frederic Jacobs、*How Russia Works on Intercepting Messaging Apps*、2016 年 4 月 30 日、https://privacyinternational.org/neighbourhood-watched、Operational Telegram、2015 年 11 月 18 日：https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a#.f1vg48cl1

207 例えば、Iran Threats、*Malware posing as human rights organizations targeting Iranians, foreign policy institutions and Middle Eastern countries*、2016年9月1日：https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a#.f1vg48cl1を参照

208 Electronic Frontier Foundation、*Your Apps, Please? China Shows How Surveillance Leads to Intimidation and Software Censorship*、2016 年 1 月 https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a#.f1vg48cl1、Maria Xynou and Chris Walker、*Why we still recommend Signal over WhatsApp*、2016 年 5 月 23 日：https://securityinabox.org/en/blog/2016-05-23/why-we-still-recommend-signal-over-whatsapp-even-though-they-both-use-end-to-end-encry

209 Patrick Howell O' Neill、*Russian bill requires encryption backdoors in all messenger apps*、2016年6月20日：http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb/

210 Jon Russell、*Tim Cook Says Apple Won' t Create Universal iPhone Backdoor For FBI*、2016 年 2 月 17 日、https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/、Max Eddy、*What It's Like When the FBI Asks You To Backdoor Your Software*、2014 年 1 月 8 日：http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software

211 以下参照：Privacy International、*Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages*、2019年5月29日、https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages

- グループが公開（つまり、招待されなくても誰でも参加できる）に設定されている場合はデータにアクセスが可能である。また、WhatsAppなどのメッセージグループでは、全てのメンバーが、他のメンバーの名前、電話番号、送信したメッセージを抽出できる。[212]
- メッセージングアプリで使用されている保護機能も、基本的な通信プロトコルであるSS7の不具合によって危険にさらされる。[213]これらの不具合により、個人が電話番号を偽装し、メッセージングアプリ上に重複アカウントを作成することにより、本来のユーザーに知られることなく、この番号宛ての全てのメッセージを送受信できるようになる。[214]

11.2.4 メッセージングアプリのプライバシーとセキュリティに関する機能

人道的状況における情報交換のためにメッセージングアプリを選ぶ際には、以下の関連機能に留意する。

11.2.4.1 匿名可 /ID 認証不要

ユーザーがメッセージングアプリを介して匿名でやり取りできるようにすることで、ユーザープライバシーを保護が向上する。一方で、実名、電子メールアドレス、認証済みIDの使用の要求は、個人が監視され標的にされる危険度を増加させる。アプリを利用するためにユーザーが提供する個人情報が少なければ、他のユーザーがアクセスできる情報は少なくなる。

11.2.4.2 メッセージコンテンツの非保存

メッセージの内容がユーザーのデバイスに配信され、読まれた後にアプリ会社のサーバーから消去されれば、ユーザープライバシーはより良く保護される。Telegram、WhatsApp、Viber、Signalなどのアプリ会社は、彼らが日常的にメッセージを保存しているわけではなく、対象の受信者に配信された直後にサーバーからメッセージを消去すると述べている。ただし、Skypeなどの企業では、ユーザーがメッセージを読んだ後もメッセージの内容をサーバーに保持しており、データを消去するまでの最大時間を明示していない。

---

212 V. Wadhwa、“WhatsApp Public Groups Can Leave User Data Vulnerable to Scraping”、VentureBeat、2018 年 4 月 3 日、https://venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/

213 今日の公衆交換電話網（PSTN、すなわち全国的、地域的または地域的に運用されている回線交換電話網の合計）は、信号システムNo.7（「SS 7」）と呼ばれる信号システムを使用しています。SS 7はモバイルテレフォニーの基盤でもあり、コール、SMS、その他のモバイルサービスのルーティングに使用されます。詳細については、ICRC and Privacy International、” Section 5: Telecommunications and messaging” , in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018を参照

214 Vijay、“How To Hack WhatsApp Using SS7 Flaw”、TechWorm (blog)、2016 年 6 月 2 日、https:/www.techworm.net/2016/06/how-to-hack-whatsapp-using-ss7-flaw.html、John Leyden、「SS 7の安価なスプークリーにより、ハッカーはモバイルチャットの利用者になりすますことができる」、The Register、2016年5月10日、電子版、sec. c. Security, https://www.theregister.com/2016/05/10/ss7_mobile_chat_hack/

11.2.4.3 エンドツーエンドの暗号化

エンドツーエンドの暗号化は、**人道団体**とその受益者との間の通信を、政府や敵対者などの第三者が傍受することを制限する。この場合、会社がコンテンツデータを保持している場合でも、暗号化された形式であるため当該会社または**第三者**には判読できない。暗号化はメッセージアプリ会社が開示を余儀なくされるデータの種類と量を制限する。理想的には、一対一チャットとグループチャットの両方に暗号化をデフォルト設定する必要がある。特定のアプリが提供するセキュリティレベルを評価するオンラインリソースも存在する。[215]

11.2.4.4 データのユーザー所有権

メッセージアプリのユーザーは、メッセージの内容だけでなく、個人を識別できるデータの適法な所有者と見なされる必要がある。そうすることで、メッセージングアプリ企業は、ユーザーの明確な**同意**なしに、このようなデータを商業その他の目的で使用することができなくなる。この問題は一部の国の国内法で扱われており、メッセージングアプリの利用規約にも含まれている可能性がある。

11.2.4.5 メタデータ保全が不要または最小限

メッセージアプリがサーバーに保全するメタデータが少なければ少ないほど、政府へのデータ開示を余儀なくされたり、営利目的に販売したりする分も少なくなる。SignalやTelegramといったメッセージングアプリは、ユーザーのメタデータを一切保全していないと主張している（Telegramの主張には異論があるが）。[216]一方、大部分の主要アプリは、連絡先番号、アプリ上のアクティビティのログ、および位置情報を収集していると述べている。

11.2.4.6 メッセージアプリのコードがオープンソース

メッセージアプリを支えるコードがオープンソースであれば、アプリを個別に精査でき、セキュリティ上の脅威やバックドアなどの隠れた監視機能に対する脆弱性がないことを確認できる。理想的なのは、アプリがコードベース全体を公開することである – SignalやWireは完全にオープンソースだが、Telegram、Threemaなど一部のコードのみを公開している。[217]

---

215 Electronic Frontier Foundation、Secure Messaging Scorecard：https://www.eff.org/pages/secure-messaging-scorecard

216 Jeremy Seth Davis、*Telegram metadata allows for 'stalking anyone'*、2015 年 7 月 30 日：https://www.scmagazine.com/news/telegram-metadata-allows-for-stalking-anyone

217 このトピックの詳細については、Lorenzo Franceschi - Bicchierai、Wickr：*Can the Snapchat for Grown-Ups Save You From Spies?* 2013年3月4日：https://mashable.com/archive/wickr#3EwYsDKZ5kqhを参照

11.2.4.7 企業が法執行機関からの開示請求を審査する

メッセージングアプリを作成している会社は、法執行機関からのユーザーデータの要求に対して厳格に審査し、抑制的に対応することが重要である。対象となるアプリ会社自身の行為に関する情報について、どの管轄当局からどのような要請を受け、どのような種類の情報を提供したかの詳細を、定期的に更新される透明性に関する報告書として公表することが理想的である。このハンドブックを執筆している時点では、Microsoft[218]とFacebook[219]が、受け取った要請の数と法執行機関に渡すデータの量について詳述した定期的なレポートを発行している。また、Open Whisper Systems（Signalの会社）は、少数の要請についてのより詳細な情報を提供している。[220]

さらに、メッセージングアプリを提供する企業の所在地が、政府が広範な監視権限を持っている国なのか、あるいは監視に対する法的制限を定期的に無視した国なのかを考慮することも重要である。[221]

11.2.4.8 第三者との限定的な個人データの共有

メッセージングアプリは、サービス提供を促進するために、一部のデータをサードパーティ（大半はデータ**処理**に何らかの技術的な役割を果たしている先）と共有する必要があるが、**個人データ**は共有しない、あるいは個人データの共有が本当に必要な場合でも最小限の匿名化データのみを共有するに留めることが重要である。人道団体は、サービスの技術的な運用に必要なデータ以外のデータを第三者と共有しないメッセージングアプリを選択すべきであり、そのことを事前にアプリ会社に明確に確認するよう努めるべきである。

11.2.4.9 デバイスのオペレーティングシステム、ソフトウェア、または特定のセキュリティパッチによるアクセスの制限

新しいバージョンの携帯電話OSには、例えばアプリがデバイス上の他の場所のデータにアクセスできないようにするセキュリティ機能も追加されている。また、ユーザーが個々のアクセス許可を付与するか、フルデバイス暗号化を有効にするかを選択することもできる。しかし、これらの新しい機器やOSは、**人道団体**が活動している地域ではあまり使われていないだろう。すなわち、現状では第三者が上述の様々な手段（セクション11.2.3）を使用して、メッセージングアプリを通して生成されたメタデータだけでなく、共有されたデータにもアクセスできる可能性があることを意味する。[222]

---

218 Microsoft、Law Enforcement Requests Report：https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

219 Facebook、Government Requests to Facebook：https://govtrequests.facebook.com/about/

220 Open Whisper Systems、Government Requests：https://whispersystems.org/bigbrother

221 さらなる研究のための有用な情報源は、https://www.digcit.org/、https://privacyinternational.org/advocacy、https://advox.globalvoices.org/、https://www.eff.org/deeplinks

222 ICRC and Privacy International、"Chapter 4.3: Other metadata" in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月、pp.61-62

11.2.5 モバイルメッセージングアプリで収集された個人データの処理

受益者がモバイルメッセージングアプリを通じて**人道団体**とのコミュニケーションを行う場合、**人道団体**としては、情報を収集した後に他のプラットフォーム上で保存し、集約し、その提供された情報を分析する必要がでてくる。

この**処理**が、本ハンドブックのパートIに記載されているデータ保護原則に沿って行われることが重要である。以下では、モバイルメッセージングアプリを通じてデータを収集することに特化したいくつかの原則について考察する。

人道支援が必要な状況で地域社会とコミュニケーションを取るには、常に次のような複雑な問題について話し合う必要がある。

- グループやチャネルに詳細を追加するには、個人が**人道団体**に「許可」を与える必要があるか。
- 個人がコンテンツの受信を拒否するにはどのようすればよいか。このような手順は最初に彼らに明らかにされているか。
- **個人データ**が誰と共有されているかを、どのようにして知ることができるか。
- 特定の**人道団体**の権限外の支援要請について、他の人道援助機関と共有される場合、明確なデータ共有手順が確立されているか。
- データがどのくらいの期間保存されどのような目的で使用されるかを、当事者が知ることができるか。
- 技術的経験が十分でない人を含めて、地域社会が理解しやすい方法でこれらの問題を伝えるにはどうすればよいか。

メッセージングアプリを使うことで、これらの問題に新たな複雑さが加わる。

人道団体のDPIAには、様々なプロトコルの詳細、および各プロトコルがコンテンツとメタデータをどの程度保護しているかを含めるべきである。
そうすることで、受益者のプロフィールだけでなく、与えられた目的（すなわち、機密情報の共有）にどのオプションが最適か、またそれが使用される法的政治的背景も評価することができる。

11.3 個人データ処理の法的根拠

人道団体は、モバイルメッセージングアプリを通じて収集した**個人データ**を、以下の法的根拠のひとつ以上に基づき処理することができる。[223]

- **データ主体**またはそれ以外の人の重要な利益
- 国内法または国際法による人道団体の権限に基づく公共の利益
- **同意**
- 組織の正当な利益
- 契約の履行
- 法的側面からのコンプライアンス

ほとんどの場合、モバイルメッセージングアプリを通じて収集された**個人データ**の**処理**は、**同意**、重大利益、または公共の利益に基づいている。もし個人が既にメッセージアプリで**人道団体**と連絡を取っているか、もしくは電話番号を伝えているならば、メッセージを受信するための**同意**と仮定することができる。しかし、このハンドブックの関連セクションで議論しているように、**人道団体**は、収集したデータの目的、保持または更なる共有等の関連情報を対象となる個人に提供し**同意**を得なくてはならない。[224]

人道上の緊急事態に関するメッセージは、**データ主体**の重大利益の範囲内にあるか、または公共の利益にあると仮定することができる。これらの法的根拠でも個人へ情報提供が求められるが、使用されるメッセージングアプリを介して関連の情報通知へのリンクを送信することで対応できる。

11.4 データ保全

人道団体は、情報通知及び保護ポリシーに、収集したデータを保持する期間を明記する必要がある。

ほとんどのメッセージングアプリでは、入力されたデータの一部が第三者（メッセージアプリ会社）によって保存されており、そのデータの内の一部がアプリを機能させるサービスプロバイダーかアプリ会者の親会社などの他の関係者と共有されている（FacebookやWhatsAppと同様）。したがって、**人道団体**は、アプリを通じて提供されたデータは、アプリ提供会社や関係する第三者によって保持され、アプリ提供者の責任下で彼らのデータ保護ポリシーによって管理されていることを情報通知の際に指摘すべきである。

223 第3章：個人データ処理の法的根拠を参照
224 第2章：データ保護の基本原則を参照

人道団体はまた、情報の交換または「チャット」自体に関する保存ポリシーを持ち、データの最小化を確実にするため定期的にチャット履歴を消去することを考慮すべきである。

11.5 データ主体の訂正および消去の権利

本ハンドブックの第一章に述べられている通り、**人道団体**は、データ保護ポリシーにおいて**データ主体**の権利の効果的な実行を促進するためのメカニズムを提供し、それについて**データ主体**に知らせる必要がある。

人道団体がメッセージングアプリから抽出するデータに関しては問題ではないかもしれないが、メッセージングアプリ側は、複数の関係者（全員が保持するデータについての透明性を有している訳ではない）との交渉を要することもあるため、ユーザーによる自己のデータの破棄を許可することを明言することは難しいかもしれない。この要因についてもデータ保護ポリシーへの明記が推奨される。

11.6 データの最小化

人道団体によるモバイルメッセージングアプリ経由のデータ収集の管理が限定的であることを考えると、メッセージングアプリを使用する機関は送信する情報量を最小限に抑えることを目指すべきである。米国を対象とした学術研究では、メッセージングアプリユーザーは、アプリの導入とアプリ上にデータを共有することによるプライバシー上の影響をあまり認識していないことが示された。[225]したがって、**人道団体**は危機の影響下にある個人に対し、人道援助を提供するために必要な**個人データ**のみを共有してくれるように伝えることを提案する。

225 Kelley P.G., Consolvo S., Cranor L.F., Jung J., Sadeh N., Watherall D. (2012) *A Conundrum of Permissions: Installing Applications on an Android Smartphone*、Blyth J., Dietrich S., Camp L.J.（編）、Financial Cryptography and Data Security。FC 2012。Lecture Notes in Computer Science、vol 7398。Springer, Berlin, Heidelberg：http://dx.doi.org/10.1007%2F978-3-642-34638-5_6

例：
2016年8月の南アフリカ共和国の地方選挙に先立ち、非営利団体のアフリカ・ボイス財団（Africa’s Voices Foundation）は、若者にとって重要な問題を明らかにし、彼らに投票を促すためのキャンペーン「投票は力となる」の影響を評価するため、リビティ・アフリカ（Livity Africa）と提携した。[226]

評価のために、若者へのオンライン調査（電子メール、WhatsAppやFacebook Messenger、ソーシャルメディアサイトへの投稿による）を行った。若者の間で普及を考慮しWhatsApp（利用46人）とMessenger（利用476人）が手段に選ばれた。AfricaのVoices Foundationは、WhatsAppグループを利用することで価値のある会話のフィードバックが促進されると評価した。インパクト・コミュニケーション・オフィサー（Impact and Communications Officer）のレインボー・ウィルコックス（Rainbow Wilcox）氏は、「WhatsApp経由の収集データは豊富で信頼でき、社会文化的な信念と行動に関する洞察を提供している」と述べた。

しかし、アフリカ・ボイスは、Facebook MessengerとWhatsAppの両方の使用時にプライバシーについて懸念を抱いた。「インフォームド・コンセントを実施しデータを安全に保存したが、これらのプラットフォームでデータがどのように使用されるのかを制御することはできない。」と、リサーチ・イノベーションの責任者（Head of Research and Innovation）、クラウディア・アブロー・ロペス（Claudia Abreu Lopes）氏は語った。「投票態度や人口統計などの個人情報を求めたため、問題があったと感じた。今後はプライバシーのリスクが十分に理解されていない場合は、同様のプロジェクトは開始しないことにした。」

上記のように、**人道団体**は、必要なデータが抽出された後は、定期的なチャットの消去について、明確な方針の策定を検討することが望ましい。

11.7 目的制限と追加処理

ほとんどの場合、モバイルメッセージングアプリを通じて収集されたデータは、**人道団体**により他のプラットフォーム上で抽出され、分析される。**データ主体**に伝達される**人道団体**のデータ保護ポリシーの一環として、これらの機関はデータ**処理**の目的を明確に規定すべきである。

226 Africa’s Voices, Case Study: Livity South Africa：http://www.africasvoices.org/case-studies/livity- south-africa/

これは、そのような解決策によるやり取りの柔軟性と即時性を考慮するとかなり困難になり得る。どのようなチャットにおいても**データ主体**によって多くの問題が提起され、それぞれの問題は一つまたは複数のフォローアップ措置を必要とするからである。このことを念頭に置き、かつ人道目的の適合性を考慮して、一般的な人道支援および保護目的の範疇で十分だと考えられる。

繰り返しになるが、モバイルメッセージングアプリによる**処理**は**人道団体**の管理外であるため、**人道団体**のデータ保護ポリシーでは、それぞれのアプリが独自のデータ保護ポリシーに従い、異なる目的のためにデータを処理する可能性があるという事実にも言及する必要がある。

11.8 データの管理、分析および検証

人道支援でメッセージングアプリを通じて処理されたデータを利用することは簡単ではない。多くの人がより大量のデータを収集し、組織と共有できるようになってきたが、これは同時に、組織が収集したデータを管理、分析および検証する能力を確保する必要があることを意味する。

受信した情報を管理、分析するためのワークフローを作成する際に困難が生じることもある。メッセージングアプリで使用されるシステムは、既存の情報管理システムやデータベースと相互運用できないことがある。それゆえ、個々のメッセージをスプレッドシートに手作業で書き写すことが、**人道団体**が効果的な意思決定を行うためにデータ分析する唯一の方法であることも多い。

また、メッセージングアプリを通じて受信した情報の検証に関しても課題が生じる。これは多くのオンラインチャネルで問題となっており、[227]情報の送信速度、メッセージの量、データタイプの範囲などの要因で、メッセージアプリからのコンテンツの検証はより困難になっている。報道機関と人権擁護活動家は、この問題のリソースと指針作成のために協力して努力を続け対応しようとしてきた。これらのリソースの中には人道団体の役に立つものもあるだろう。[228]

人道団体は、アプリを通じて収集された**個人データ**が管理、分析または検証された後、**追加処理**を行う。従って、**人道団体**は**個人データ**の**追加処理**が、データ収集された当初の目的と両立することを確認する必要がある。

227 The Engine Room, *Verification of social media: The case of UNHCR on Twitter*：https://responsibledata.io/reflection-stories/social-media-verification/

228 例えば、Craig Silverman（ed）、*The Verification Handbook, European Journalism Centre*、http://verificationhandbook.com/、DatNav：*New Guide to Navigate and integrate digital data in human rights research*, The Engine Room, Benetech, and, Amnesty International, 2016 年、https://www.theengineroom.org/datnav-digital-data-in-human-rights-research/ First Draft News Partner Network、https://firstdraftnews.org/about/を参照

11.9 データ保護バイ・デザイン

もし**人道団体**がメッセージアプリを開発しようとするなら、データ保護の原則を設計段階で組み込むことを考慮すべきである。これは、技術的な解決策と組織的な対策の両面で、プライバシーに配慮したシステムとサービスの開発が必要となることを意味する。**データ保護影響評価**（DPIA）は、実際にデータ保護の原則を実装できているかを評価する方法である。データ保存に使用されるクライアント／サーバアーキテクチャも、データ保護バイ・デザインの原則を実施すべきである。

独自のアプリやプラットフォームを開発する際に、**人道団体**が心に留めておくべき事項がいくつかある。第一に、人道団体の受益者間でアプリ利用を促進することは簡単ではない。第二に、アプリのメンテナンスとセキュリティには継続的なコストがかかる。全てのソフトウェアは、開発されたあと、新しい脆弱性の出現のたびに更新が必要となる。**人道団体**は、そのようなアプリやプラットフォームを開発・維持するためスキルや専門知識を組織内に持てるかどうかを検討する必要がある。[229]

11.10 国際的なデータ共有

また、一部のサービスは交差したり、関連する事業体や操作方法の点で重複している場合があることも**認識**することが重要である。実際にソーシャルメディアネットワークとメッセージングアプリのデータ処理活動は、別々であると見るべきではないし、そのように見ることは不可能である。多くの場合、メッセージングアプリはソーシャルメディアネットワークに直接リンクしているか（例：Facebook Messenger）、または同じビジネスグループに所有されているために間接的にリンクしている（例：WhatsAppの所有者はFacebook）。この場合、これらのサービスは様々な目的でデータを共有できる。[230]

229 ICRC and Privacy International、“Chapter 5.4：Outsourcing, contracting, and using third parties,” in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月

230 ICRC and Privacy International、“Section 4.1: Messaging apps and social media” in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、2018年10月

デジタル アイデンティティ

利用可能性

課題

第12章

デジタル アイデンティティ[231]

231 この章への貢献に対し、Aiden Slavin氏（ID 2020）、Giulio Coppi氏（ノルウェー難民評議会）、Tom Fisher氏（プライバシーインターナショナル）、Robert Riemann氏（欧州データ保護監督官）に感謝の意を表する。

12.1 はじめに

全ての人間はアイデンティティを持っている。アイデンティティに対する権利は、議論の余地がなく、国際宣言および国際条約において認められている。[232]しかし、人間全員が自分のアイデンティティを証明する方法を持っているわけではない。この点では、誰もがアイデンティティツールを通じて自分が誰であるかを証明する手段を持つべきである。[233]そのようなツールが取るべき形態については依然として議論がある。しかし、書類、カード、トークン、モバイル・アプリなど、その形式が何であれ、それを作成し、管理する必要がある。**人道団体**の責務は、その活動の枠組みを定めることであり、この章で述べるように、デジタルアイデンティティに関しては特に重大である。

多くの場合、**人道団体**は、プログラム上の目標（例えば、援助が意図された個人に確実に提供されるように設定された受益者管理システム）を促進するため、アイデンティティ管理システムを使用する必要がある。[234]一部の機関は、単なるプログラム上の目標のサポートにとどまらず、実際問題として、本人確認書類を持っていないために「目に見えず、無視され、取り残された存在」となり得る[235]人々に法的アイデンティティ[236]（デジタル形式の場合もある）を提供する、アイデンティティ管理システムの開発を目的とした取り組みに関与している。しかし、時には、当初はプログラム上の目標をサポートするために設計され導入された識別ツールが、時間の経過とともに、より広範な使用（法的アイデンティティを証明するためなど）に移行することがある。

このような背景から、本章では、受益者のために**デジタルアイデンティティ**管理システムを設定することのデータ保護上の意味について分析する。本章の議論では、とりわけ、**人道団体**がそのようなシステムを使用してどのようにしてデータを収集し保管するのか、また、参加者、利用者および／または受益者に関する情報をどのように管理するかという点を取り上げる。

232 例えば、世界人権宣言第6条および国連子どもの権利条約第7条参照

233 持続可能な開発目標（SDG target)16.9を参照：2030年までに全ての者について出生登録を含む法的身分証明を提供すること: https://sustainabledevelopment.un.org/sdg16

234 USAID（米国国際開発庁）、デジタル時代におけるアイデンティティ：インクルーシブな開発のためのインフラストラクチャ、USAID、2017 年、p.1: https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

235 本章を通じて、「法的アイデンティティ」という表現は、「法的アイデンティティは、個人のアイデンティティの基本的特徴として定義される。例えば、出生の発生後に、権限のある民事登録当局による証明書の登録・発行によって与えられる氏名、性別、出生場所および生年月日である。出生登録がない場合は、法的アイデンティティは、法的に認められた確認当局によって与えられることがある。この制度は、出生から死亡までの法的アイデンティティへの総合的アプローチを確保するために、市民登録制度とリンクされるべきである。法的アイデンティティは、死亡の登録時に民事登録当局が死亡証明書を発行することによって消滅する。難民の場合、加盟国は主に法的な身分証明書を発行する責任がある。難民に対する法的な身分証明書の発行は、国際的に承認され、委任された当局によって管理されることもある。」という国連の運用上の定義に従ったものである：https://unstats.un.org/legal-identity-agenda/

236 USAID（米国国際開発庁）、2017年、p.1

用語	目的	代表的な特徴	例
機能的アイデンティティ	特定のサービス（機能）が参加者を認証できるようにする。	文脈上 情報の重複	全ての個人は、複数の機能的アイデンティティを持つことができる。これらのアイデンティティには、学生 ID、有権者 ID、または食品配給プログラム ID など国境を跨ぐものもある。
基本的アイデンティティ（法的アイデンティティ）	特定のサービスを指定することなく、公共財としての法的アイデンティティを広範な人々に提供する。個人が自己証明することを可能にする。 このようなアイデンティティの発行者は、信頼できる発行元と見なされ、アイデンティティの権威ある発行元とも呼ばれる。	他のユーザーが参照できる法的アイデンティティを生成する。与えられた範囲内では、各人はそのようなアイデンティティを 1 つだけ持つことができる。ただし、同じ人物が複数の法的アイデンティティ（例えば複数の国が発行したパスポート）を持っている場合もある。	典型的に政府ベースで、国の全人口を対象とする。[237] 例えば、社会保障番号、出生証明書または Aadhaar 番号（インドにおいて、生体情報と人口統計データに基づいて個人を一意に識別する 12 桁の数字）など。
概念上のアイデンティティ（個人的アイデンティティ）[238]	特定の社会構造の中で、他者との関係において個人のアイデンティティを定義し、その個人が自分自身をどのように見ているか、また、周囲の社会からどのように認識されているかを決定する。	無形で、変化に富み、主に個人的および社会的認識によって定義される。	定義のための属性（民族性、セクシュアリティ、宗教、政治的志向など）。これに基づいて、個人は自分自身を定義し、社会の他者によって定義される。

議論を始めるにあたって、「**デジタルアイデンティティ**」という用語に関しては、普遍的に受け入れられている定義は存在しないことに注意すべきである。しかし、デジタルアイデンティティは「特定の文脈内の個人を一意に記述し、電子取引に使用される、電子的に取得および保管されたアイデンティティ属性の集積」で構成されるということで一般的に合意されている。[239]しかし、多面的な概念として、**デジタルアイデンティティ**は、識別、機能的アイデンティティ、基本的アイデンティティ、および個人的アイデンティティのような多くの他の重要概念と関連付けることができる。[240] これらの用語は本章全体を通して使用されているため、それぞれの簡単な説明を上記の表に示す。

237 USAID、2017年、p.12

238 概念上のアイデンティティはアイデンティティ・システムの対象とはならないため、この章では取り上げない。

239 World Bank Group、GSMA and Secure Identity Alliance、Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation、World Bank Group、GSMA and Secure Identity Alliance、2016 年、p.11：https://www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/

240 J. Donner、"The difference between digital identity, identification, and ID: Caribou Digital's style guide for talking about identity in a digital age"、2018年12月19日：https://medium.com/caribou-digital/the-difference-between-digital-identity-identification-and-id-41580bbb7563

これらの異なるタイプのアイデンティティの観点から、**人道団体**は、受益者からの機能的アイデンティティと基本的アイデンティティのどちらを必要とするかを最初から明確にすることが重要である。なぜなら、この選択は、アイデンティティ・システムの設計および関連する管理プロセス（例えば、第三者との提携、他の既存システムへのリンクなど）に影響を及ぼすからである。多くの場合、法的な制約がアイデンティティ・システムの設計に関する決定を左右する。

12.1.1 認証、識別、照合：どうすれば自分の存在を証明できるのか

人道団体は常に誰かの法的アイデンティティを知る必要があるとは限らない。これは、たとえば、交流の目的が援助の提供である場合に当てはまる。したがって、**人道団体**は、**デジタルアイデンティティ**・システムを開発する前に、特定の人道プログラムのために受益者からどのような情報が必要かを識別する必要がある。ここで、認証、識別、照合の間には重要な区別がある。

識別は、「あなたは誰か」という質問に答える。しかし、アイデンティティ管理システムを設置する際、その組織は「援助や保護を提供するために、その人から何を知る必要があるか」という別の質問から始める必要がある。その人が誰であるかを知ることが重要となることもあるからだ。例えば、保護者のいない未成年者を両親と再会させる場合、両親であると主張している人々が本当の両親であることを確認することが重要である。しかし、多くの場合、おそらくほとんどの場合は、特定の基準を満たしているか、または、特定の属性（例えば、特定のワクチン接種を受けるために、十二歳未満であることを証明することができる属性）を持っているために、その人がサービスにアクセスする資格があるかを知るだけで十分である。これは認証とも呼ばれ、自分が何者であるかを証明することができる。

人道団体が認証のみを必要とする場合でも、アイデンティティ管理システムに受益者を登録する際には、照合プロセスを実施すべきである。したがって、照合とは、誰かのアイデンティティを確認する（身分証明書の名前を確認するなど）こと、または、そのアイデンティティ属性の一部を確認する（コミュニティのリーダーに、その人物が支援を受けるコミュニティの一員であることを確認するなど）ことである。援助が確実に被災者に届けられるようにするために単純な認証システムが用いられる場合、登録時の照合は、援助を受ける資格がある人々が登録された人々であることを確実にするのに役立っている。ただし、援助サービスによっては照合を全く必要としない場合もあることに留意する必要がある。例えば、**人道団体**が、誰でも登録できるオンライン・プラットフォーム上で情報を利用可能にする場合などがこれに該当する。

人道団体が受益者を登録する際には、受益者に関するデータの一部を収集し、アイデンティティ管理システムに保存する必要がある。以下で明らかになるように、記録する必要がある属性とその目的を決定することは、データ保護の観点から重要な決定事項である。特に、活動の目的を達成するために必要な属性のみ（例えば、援助の提供）を収集すべきである。例えば、ほとんどの場合、おそらく組織は、登録された個人が未成年者であることが確認されたという事

実を記録するために身分証明書のコピーを保管する必要はないであろう。加入した受益者は、証明、カード、PINコードやモバイル機器でアクセスや管理が可能なデジタル証明書など、身元に関する記録の一部を受け取ることができる。受取人は既に対象サービスにアクセスする権利があることを証明しているため、引き渡し時点でさらなる照合を行う必要はない。

12.1.2 デジタルアイデンティティ

デジタルアイデンティティは、デジタル的に保存される一連の属性であり、特定の文脈（前述のアイデンティティの種類：機能的、基本的、概念的）参照において個人を一意的に記述する。場合によっては、個人が複数、場合によっては数百のデジタルアイデンティティを持つことがあり、それぞれが機能的アイデンティティとしての役割を果たす。このタイプのシステムは、受益者が法的アイデンティティを証明しなくても、ユーザ名とパスワードのアクセスモデルまたはトークンシステムと同様の方法で、サービス、支援または保護にアクセスすることを可能にする。

しかし、他の場合には、組織はある個人を高い確信を持って別の個人と区別し、各個人に対して一つの**デジタルアイデンティティ**だけを持つ必要があるかもしれない。このようなシナリオでは、アイデンティティ・システムは、**デジタルアイデンティティ**を物理的な人物にリンクできるようにすべきである。ここでの目的は、例えば人道団体が個人に向けられた援助を提供している場合（医療など）、個人を区別しやすくすることである。しかし、そのようなリンクが必要な場合でも、諸団体は受益者から法的な身分証明書を取得する必要はないかもしれない。例えば、提示された名前が法的アイデンティティと一致することを確認する（例えば、出生証明書やその他の身分証明書と照合する）必要なしに、名前だけで登録することができるかもしれない。

最後に、**人道団体**が、個人の法的アイデンティティを確認し照合することもできるシステムを必要とする場合がある。これは前述のケースと非常に似ているが、問題の人物を正式に識別するために法的な身分証明書が必要になる点が異なる。

要約すると、**人道団体**が**デジタルアイデンティティ**管理システムを設置する際に従うべき主な手順は次のとおりである。

- 第一に、特定の人道的プログラムを実施するために、影響を受けた人々について知るべきことを決定する。これにより、識別が必要かどうか、または認証だけで十分かどうかが判断される。データ保護の観点からは、可能な限り後者を選択することが推奨される。
- 第二に、人道団体は、プログラムのニーズに基づいて、機能的アイデンティティと基本的アイデンティティのどちらを必要とするかを決定する。ただし、基本的アイデンティティを確立し管理する権限を有するのは一握りの**人道団体**だけであり、特定の目的のためにのみ適用されることに留意する。

- 第三に、人道団体は登録段階で提供された情報を照合確認するための照合プロセスを設計する。選択されたアイデンティティ・システムによっては、特定の形式、デュー・デリジェンス、または正式な法的文書を必要としない。人道団体は、照合段階で評価された情報を保持する必要があるかどうかについても決定すべきである。

12.1.3 システム設計とガバナンス

人道団体は、その目的（認証・識別・照合）を理解した後、**デジタルアイデンティティ**・システムがその意図された目的を達成するためにどのように設計され、どのように管理されるかを決定する必要がある。**人道団体**（または他の団体）は、システムを中央で管理することもできるし、複数の主体に分散して管理することもできる。[241]現在の取り組みの中には、誰がいつ自分のアイデンティティ証明書にアクセスできるかを決定することで、個人が自分のアイデンティティ・システムを管理できるようにすることを目的としているものもある。この意味で、ガバナンス構造は、データが収容される場所によって影響を受けることがある。たとえば、複数の関係者が同じシステムにアクセスする場合は、共有プラットフォームが必要となる。同様に、個人に管理を移そうとする場合には、個人が自分のデバイス上で自分の認証情報を保管したり、自分で選んだサービス・プロバイダを利用したりできるようにすることも考えられる。

次の意思決定の系統図は、**人道団体**がアイデンティティ・システムを導入するかどうかを決定する際に、回答すべき質問と考慮すべき要素をまとめたものである。

1. アイデンティティ・システムのタイプ
   - 認証だけに頼ることができるか、または本当に受益者を識別する必要があるか。
   - 機能的アイデンティティや基本的アイデンティティの生成を目指しているか。（基本的アイデンティティを生み出す権限を持っているのは一部の組織だけだということを忘れないこと。）
   - 登録時に情報を照合する必要があるか。照合する必要がない場合、照合なしのシステムは受け入れられるか。照合する必要がある場合、照合には正式な法的身分証明書（または、照合可能なより単純なフォーム）が必要か。照合プロセスで評価された情報を保持する必要があるか。

2. 設計の選択肢
   - どのような情報を、誰が、どこで保管する必要があるか。
   - 特定の属性（人道的プログラムの対象となる資格があるかどうかを決定するための国籍）を照合することは、その情報をアイデンティティ・システムに保管する必要があるという意味

241 分散型アーキテクチャーと統合されたアイデンティティ・システムの違いは、文献で詳細に説明されている。これは重要なポイントだが、この章の範囲を超えているため、ここでは説明しない。分散型アイデンティティの詳細については、Digital Identity Foundationの資料(https://identity.foundation/)、World Wide Web Consortium (https://w3c-ccg.github.io/did-spec/)、およびWorld Economic Forumの資料(http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf)を参照

ではないことに留意すべきである。このシステムでは、それ以上の詳細なしで、個人が必要な属性を持っていることを確認することができる。

- 場合によっては、最初から照合の必要がないこともある。例えば、個人情報を一切開示することなく自由にアカウントを作成することができる場合や、一般的にアクセス可能なデジタル・サービスや、避難者用の場所での個人の存在確認だけで援助にアクセスする権利が与えられる場合（例えば、情報を収集せずにカードが配布される場合）に当てはまる。
- データをどのように制御および管理するか。誰がどのような情報に、どの時点で、どのような目的でアクセスする必要があるか。

12.1.4 人道支援分野におけるデジタルアイデンティティ：可能性のあるシナリオ

以下の四つのシナリオは、人道セクターにおけるさまざまな**デジタルアイデンティティ**・システム間の相互作用を明らかにする。

シナリオ1：人道団体が、登録された援助受益者にアイデンティティ証明書（例えば、登録カードや書類）を発行する。このシナリオでは、受益者（**データ主体**）は、支援を受けることを可能とする機能的アイデンティティを使用するだろう。しかし、場合によっては、そのようなアイデンティティ・システムは、受益者が誰であるかの証明、すなわち、基本的アイデンティティ（シナリオ4を参照）として受け入れられる可能性がある。しかし、人道プログラムの中には、本人確認を必要とせずに、特定の援助サービスに適法にアクセスする権利があることを認証するためだけに、本人確認を行うものもある。

シナリオ2：人道団体が受益者に複数のサービスを提供する。これらのサービスを提供するために、機関の各部署は、受益者から収集されたデータのうち、特定の部分にアクセスできる必要がある。例えば、現物給付援助を提供するために、担当部署は受益者に関連する援助分配記録にアクセスする必要があるかもしれない。一方、別の部署は経過観察を提供するために医療記録にアクセスする必要が、三番目のユニットは家族のつながりを回復するために個人に関する情報を必要とする場合があるかもしれない。

シナリオ3：複数の**人道団体**が、統合されたアイデンティティ・システムを通じて受益者に複数のサービスを提供する。アイデンティティを共有するこのような方法では、各機関がサービスの提供に必要かつ関連するデータにアクセスできる。このシナリオでは、認証と識別の両方が必要になる。関係するさまざまな機関や団体間の相互運用性は、このシステムが人道支援の単独のゲートウェイとして機能し、有益であることを証明することができるだろう。これは、**人道支援**において「一

度だけ」の原則[242]を適用し、オンライン・プラットフォームおよび／またはさまざまな**人道団体**の間の情報・文書の交換（自動または要請による）を介して、受益者に直接、物理的またはデジタルサービスの提供を容易にすることを必要とする。[243]しかし、そのような解決策を選択する際には、さまざまな要素を考慮する必要がある。例えば、適用可能なガバナンスの枠組みを識別し、システムに関与する者（データ管理者と**データ処理者**）の役割が明確であるようにすべきである。データへのアクセスを適切に分離することは技術的に困難な場合があるため、統合された商用ソリューションで**データ侵害**が発生することは珍しくない。同様に、統合されたシステムでは、団体同士の複雑な関係によって、データが収集された目的のためだけに使用されることを保証することが困難になる場合がある。加えて、このような複雑なシステムは、必要なデジタルリテラシーのスキルを持っていない一定の集団を、事実上排除する原因となり得る。

シナリオ4：状況によっては、**人道団体**は受益者に対し、機能的な身分証明書、例えば人道的影響を受けている人々がサービスにアクセスできるようにする登録カードを発行することがある。これらは最終的に、基本的なアイデンティティ文書の役目を果たし、それらを受け入れる当局または金融機関に対するアイデンティティの証明として機能する可能性がある。

例：
難民の大量流入を受け入れているヨルダンとエジプトでは、モバイルSIM登録と**Know Your Customer**（**KYC**）の要件を満たすために、地元当局は有効なパスポートまたはヨルダン内務省の難民・亡命希望者用サービスカードのような政府発行の身分証明書を要求している。国連難民高等弁務官事務所（United Nations High Commissioner for Refugees：UNHCR）は、当該機関が発行する身分証明書が亡命希望者や難民が所持する唯一の身分証明書である可能性を考慮し、これも認めるべきだと主張している。

12.1.5 基本的アイデンティティとしてのデジタルアイデンティティ

現在、さまざまな取り組みが進められており、身分証明書を持たない人々のための基本的アイデンティティの形式として役立つ**デジタルアイデンティティ**・システムの開発を目指している。

242 「一度だけの原則」は、個人が当局に個人情報を一度だけ提供し、その後は、個人の要求により、または、その同意を得て、政府部局は、情報を再度収集する代わりに、公務の遂行のために情報を交換することができることを意味する。

243 欧州データ保護監督官（EDPS）、*意見 8/2017：EDPS単一のデジタル・ゲートウェーと「一度だけ」の原則を制定する規則の提言についての意見*、EDPS、2017年8月1日：https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en.pdfを参照

これらの取り組みは、自分が誰であるかを証明できない人々は、自分の権利を主張し、公共サービスにアクセスし、年齢、国籍、状況、その他のアイデンティティや地位の属性[244]に基づく給付金や受給資格を請求することが困難であるという事実に端を発している。IDの証明は多くのサービスにアクセスするための前提条件となっているので、アイデンティティの乖離は政治的、社会的および経済的生活への参加に対する大きな障壁である。例えば、民間のサービス提供者は、法的要件に準拠するため、またはデューデリジェンス手続き（KYC、詐欺・なりすまし防止、取引リスクとコスト削減など）の一環として、アイデンティティの証明を要求することが多い。**デジタルアイデンティティ**・システムは、身分証明書を必要としていながら、それを持っていない人々を支援する1つの方法かもしれない。しかし、前述したように、この種の基本的なシステムを開発し、展開する権限を持っている**人道団体**はほとんどなく、したがって正当な根拠を有していない。

重要なのは、**デジタルアイデンティティ**・プログラムが特定の技術やシステムに限定されないことである。このようなプログラムは、多くの技術のうちの1つ、または解決策の組み合わせを用いて設計することができる。**デジタルアイデンティティ**にしばしば関連するテクノロジーは、次のとおり。

- **バイオメトリクス**：[245]人道分野における**デジタルアイデンティティ**制度への受益者の登録には、指紋や虹彩スキャンなどの生体認証の利用を含めることができる。
- **ブロックチェーン**：[246]**ブロックチェーン**は、デジタル技術やインフラへのアクセスが制限されている個人が自分の身元を証明可能な手段の一つである。[247]しかし、その有用性に期待はできるものの、**ブロックチェーン**技術に伴う課題は真剣に検討する必要がある。
- **データ分析**：[248]デジタルアイデンティティは、公式の証明書を使用せずに、デジタル行動属性（「アルゴリズムアイデンティティ」とも呼ばれる）から作成することができる。ここでは、個人のオンライン活動（ソーシャルメディアの利用、閲覧履歴、オンライン購入、通話履歴など）を使用して、そのアイデンティティを検証できる。[249]プロファイル・ベースのアイデンティティ・システムの可能性はまだ完全には実現されていないが、このアプローチではデータ保護に関する懸念が生じる。[250]

244 G. Verdirame et *al.*、*Rights in Exile: Janus-Faced Humanitarianism*、Berghahn Books、ニューヨーク、2005年、pp.59–63

245 第8章：バイオメトリクスを参照

246 第14章：ブロックチェーンを参照

247 A. Beduschi et al.、*Building Digital Identities: The challenges, risks and opportunities of collecting g behavioural attributes for new digital identity systems*、University of Exeter and Coelition、2017年、pp.15–16、p.26：https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Buiding_Digital_Identities_with_Behavioural_Attributes.pdf

248 データ分析の利用に関する課題については、第6章：データ分析とビッグデータを参照

249 A.Beduschi et al.、2017年、p.8

250 例えば、Facebookのシャドウアカウント。R. Brandom、“Shadow profiles are the biggest flaw in Facebook’s privacy defense”、2018年4月11日：https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacyを参照

12.2 データ保護影響評価

データ保護影響評価（Data Protection Impact Assessment：DPIA）には、データの取扱いを伴うプロジェクト、方針、プログラムまたはその他の取り組みの**データ主体**およびその**個人データ**に対する影響の識別、評価、対処が含まれる。DPIAは、最終的には、個人の権利と自由に対するリスクを最小限に抑え、そのライフサイクルを通じてプロジェクトまたは取り組みに沿った対策に結び付くべきである。**デジタルアイデンティティ**・システムが関与する大規模な**処理**、および同システムの使用によって生じる**データ主体**への他の潜在的なリスクと損害を考慮し、**人道団体**はシステムおよびプログラムの実施前および実施中にDPIAを実施すべきである。さらに、DPIAの過程では、データ保護要件の遵守だけでなく、システムがさまざまな基本的権利に与える潜在的な悪影響、およびデータ**処理**の倫理的、社会的影響も分析すべきである。[251]

複数の人道目的（当初から識別されていないものもある）のためにアイデンティティ・システムを利用することは、いわゆる「ファンクション・クリープ」を引き起こす恐れがある。これは、**人道団体**が、意図的か否かを問わず、当初予測されなかった目的のためにアイデンティティ・システムを使用し、受益者のデータを悪用する場合に起こる。さらに、人権を尊重しない政府や非国家武装集団は、敵や敵対者を識別したり、民族性、政治的見解、国籍、その他の特徴に基づいて特定の集団を標的にしたり、プロファイルを作成したりするために、アイデンティティ・システムやその他のシステムにアクセスすることができる。この情報は、さまざまな方法でこれらの個人やグループをコントロールし、差別し、危害を加えるために利用することができる。例えば、必要不可欠なサービスや援助から彼らを除外したり、彼らの自由や公正な裁判を受ける権利を剥奪したり、残虐行為を行うなど（例えば、ルワンダの大量虐殺やナチス・ドイツの迫害では、身元確認とプロファイリングが重要な役割を果たした）がその例である。

12.3 データ保護バイ・デザインおよび初期設定によるデータ保護

データ保護バイ・デザインおよび初期設定によるデータ保護は、**個人データ**を**処理**するアプリケーションのライフサイクルを通じて重要な役割を果たす実践である。[252]それは、最初から重要なデータ保護原則を含み、**データ主体**に可能な限り最大限のデータ保護を提供するような方法で、

251 A. Mantelero、"AI and Big Data: A blueprint for a human rights, social and ethical impact assessment"、*Computer Law & Security Review*、Vol.24、Issue 4、2018 年 8 月、pp.754–772、p.755：https://doi.org/10.1016/j.clsr.2018.05.017

252 L. Jasmontaite et al.、" Data Protection by Design and by Default: Framing Guiding principles into Legal Obligations in the GDPR"、*European Data Protection Law Review*、Vol.4、Issue 2、2018年：https://edpl.lexxion.eu/article/EDPL/2018/2/0

処理操作、プログラム、解決策の設計を含む。この意味で重要なデータ保護の原則は次のとおりである。

- 適法性・公正性・透明性
- 目的制限
- データ最小化
- 正確性
- 保管制限（保全制限）
- 完全性と機密性（セキュリティ）
- 説明責任

したがって、**人道団体**は、アイデンティティ・システムを設計する際には、まずニーズを考慮し、次にアイデンティティ・システムが識別された問題を解決するために必要かつ相応であるかどうかを検討することから始めるべきである。機関がアイデンティティ・システムが必要であると判断した場合、その機関のニーズに最も適合し、特定の状況に適したシステムのタイプを慎重に検討する必要がある。以下の第6項で説明するように、このプロセスに従うことで、機関はデータ最小化と比例性の原則を適用することができる。

また、データ保護バイデザインにより、人道団体は、**データ主体**が権利（下記の第5項を参照）を行使することが可能かつ容易になるような方法でシステムを構築する必要がある。例えば、**デジタルアイデンティティ**・システムでは、**データ主体**は初期設定によって、情報通知、各人のアイデンティティに関連付けられた全ての情報、および誰が何の目的でそのデータにアクセスしたかを詳述するログにアクセスできるようにするべきである。

12.4 データ管理者とデータ処理者の関係

デジタルアイデンティティ・システムは、**人道団体**、政府、および、銀行、決済システムプロバイダ、ITネットワークプロバイダ、バイオメトリクス企業などの商業組織を含む、広範な組織や団体に関与することができる。その結果、当事者のうち誰をデータ管理者および**データ処理者**として扱うべきかを特定することは困難である。同様に、責任と義務の境界が当事者間のどこにあるのかを判断するのは難しい。この問題に対処するために、**デジタルアイデンティティ**・システムは、利害関係者が誰であり、彼らがどのような責任と義務を持ち、各自がどのようなデータカテゴリとフローをどのような目的で使用しているかを明確にするように設計されなければならない。**人道団体**が識別プログラムの手段と目的を決定する場合、その機関は**データ管理者**として行動し、したがって、プログラムから生じる可能性のある違反、誤用、その他の種類の損害に対して潜在的に責任を負う。共同管理者が設置される場合、または**データ処理者**が**データ管理者**の代

理としてのみ**個人データ**を処理する場合、書面による合意で当事者間に責任を割り当てることがベスト・プラクティス（最善の慣行）である。

12.5 データ主体の権利

データ主体によって制御される**デジタルアイデンティティ**・システムの開発の可能性は、現在、さまざまな取り組みを通じて調査されている。このようなシステムは、個人が中央の保管場所に頼ることなく、自分のデバイス上で保管されたアイデンティティデータにアクセスできるようにすることにより、また、必要な時に必要な人に認証情報を提供することにより、管理を個人に移行することを目的としている。[253]前述したように、これは、例えば、受益者が彼ら自身のデバイスまたは彼らが選択する別の記憶媒体上に彼らの個人情報を保管し、それを人道的対応に関与する団体や組織といつ共有するかを決定することができるシステムを構築することによって達成することができる。機能的または基本的アイデンティティの取り組みの中には、個人が自分の**個人データ**を自分のデバイスで保管できるようにし、必要に応じて他の人と共有することにより、データの管理を個人に移行することを目的としているものもある。しかし、実際に管理の移行が起こるかどうかについては、依然として議論が続いている。このような取り組みを進めるにあたっては、個人が自らの権利や個人情報を個人の機器に保存することのリスクを認識し、十分安全に利用できるようにすることが重要である。

例：
「ID 2020アライアンス」は、いわゆる「良い」デジタルアイデンティティの開発に影響を及ぼすために設立された。このデジタルアイデンティティでは、個人が自分のアイデンティティを完全に管理し、どのデータを誰と共有するかを決定できる。アライアンスによると、「現在、ほとんどの**個人データ**はサイロに保存されている。サイロ化されたデータ数が多いほど、管理が及ばなくなる。」。この問題を解決するために、アライアンスは、個人が「**個人データ**がどのように収集、使用、共有されるかを含め、自分のデジタルアイデンティティを管理しなければならない」と提案している。[254]

このような取り組みはまだ一般的ではないが、**人道団体**が受益者に対し自身のアイデンティティ証明書に関連する全ての情報にアクセスするためのログインと、該当する場合は、当該機関が作成した個人プロファイルを提供することによって、自らのデータに対するより多くのコントロールと

253 M. Pisa and M. Juden、*Blockchain and Economic Development: Hype vs. Reality*、Center for Global Development, Washington, D.C.、2017 年、p.25：https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf

254 ID 2020ウェブサイトからの全ての引用：https://id2020.org

アクセスを提供することができる。この解決策が実際に機能するかどうか、またこれによってデータの管理が真に個人に移行するかどうかを判断するために、この解決策に関連する潜在的なメリットとリスクを十分に調査する必要がある。しかし、理論的には、このようなシステムは、第三者がデータにアクセスした場合や、データ**処理**の活動が開始された場合はいつでも、それらを受益者に自動的に通知することができる。また、同意書がデータ**処理**の法的根拠となっている場合には、受益者が同意書を更新し、データ処理についての最新情報を受け取ることができるようにすることも可能である。より多くの管理を行うことで、受益者はオンライン・プロファイルやプラットフォームを通じて、**データ主体**としての権利を直接行使することができる。受益者がデジタル情報に通じていない場合、または必要な技術を利用できない場合、**人道団体**は、受益者が**個人データ**に関して権利を行使するための代替法を提供しなければならない。

12.5.1 アクセス権

受益者は、自分のデータの**処理**に関する情報および処理中のデータへのアクセスを要請する権利を有する。[255]この権利は特定の状況では制限される可能性があるが、**人道団体**は、データ管理者として、受益者の**個人データ**が処理されているかどうかを受益者に通知し、処理されている場合は該当データへのアクセスを許可することによって、そのような要請に応えるべきである。しかし実際には、アクセス許可の要請がデジタル手段（**デジタルアイデンティティ**の場合には最も可能性の高いシナリオ）によってなされる場合、情報へのアクセスを要請している人がそれを受け取る権利を有する個人であることを照合するのは困難である可能性がある。そのため、この権利は**デジタルアイデンティティ**・プログラムにおいて実施することは困難であるかもしれない。これは広範囲のデジタル・システムに当てはまる問題であるが、**デジタルアイデンティティ**の場合にも等しく考慮されなければならない。したがって、**人道団体**は、**デジタルアイデンティティ**・システムの設計を決定する前にも、またそれを実施するかどうかを決定する際にも、**データ主体**の権利が尊重されるように措置を講じるべきである。

デジタルアイデンティティ・プログラムにおける**データ主体**の権利を尊重することに対するもう一つの課題は、同じ組織内の別の部署が同じ**データ主体**について異なる情報を保持している可能性があるという事実から生じる。その結果として、受益者の要請に応えるために、こうした情報を編集することは難しいかもしれない。受益者は、しばしば、組織が保有する彼らに関する全てのデータではなく、特定の分野のデータや特定のプログラムに関連するデータへのアクセスのみを要請するため、不必要な努力を伴うことさえある。したがって、人道団体は、要請の詳細を理解し、余分な努力を避けるために、こうした問題について**データ主体**と話し合うべきである。**人道団体**は、このような課題を**デジタルアイデンティティ**・システムの設計段階で考慮に入れ、

255 セクション2.11.2：アクセスを参照

この種の問題を予測し、それを防ぐ方法を考案すべきである。上記のようなログイン・ベースのアクセス・システムは、受益者がいつでも自分のプロファイルにアクセスし、自分について保持されている情報と、それが使用されている目的を確認できるようにするものである。

12.5.2 訂正および削除の権利

受益者は、自身に関する誤ったデータを訂正し、特定の状況においては、そのデータを消去できるべきである。例えば、自分のアカウントにログインすることで、（上記のように）これを直接行うことができる。受益者が自らのデータを管理できない場合、その権利を行使することは、とりわけ、データの修正または消去を要求する者のアイデンティティを評価し確認する場合に、やはり困難である。この問題に対処するために、**人道団体**は、最小化原則に準拠し、不必要な**個人データ**を収集しない照合システムを実施する必要がある。ここでも、受益者が自分のアカウントにログインすることは、この目的を達成する一つの方法である。

12.6 データ保護基本原則の適用

このセクションでは、***デジタルアイデンティティ***・システムを扱う際に発生する可能性があるデータ保護問題の概要を説明するが、全ての事例において、使用される技術と、想定されるプログラムの目的を達成するために必要な識別の種類を考慮して、詳細に、かつその是非について検討すべきである。要件は各プログラムで異なる。同様に、テクノロジーが異なれば、データ保護の意味合いも異なる可能性がある。

12.6.1 個人データ処理の法的根拠

人道団体は、受益者のアイデンティティを確定または検証するために、**個人データ**を**処理**する必要がある。これらの処理操作は、一つまたは複数の法的根拠に基づいて実行することができる。例えばシナリオ2および3では、**人道団体**は、医療記録の**処理**に対する重大な関心や、家族のつながりを回復するための**個人データ**の**処理**に対する**同意**など、個々の処理活動に対する個別の法的根拠を識別しなければならない。

同意の問題については、援助を受ける受益者がそれを有効にする立場にないかもしれないことを認識することが重要である。[256]**同意**とは、**データ主体**がその**個人データ**の取扱いに同意することを、自由意思により、特定的に、状況の説明を受けた上で示すことである。同様に、**人道団体**は、公的身分証明書を提供するプログラムの法的根拠として公共の利益を使用するかもしれないが、**同意**を得られない場合、受益者の不信感を招く可能性がある。受益者は、**個**

256 セクション3.2：同意を参照

人データの**処理**に関して発言権がないため、自分の権利が制限されていると感じるかもしれない。これは、対象となるデータが個人の生活の本質的な部分であるアイデンティティに関連している場合に特に当てはまる。

12.6.2 目的制限と追加的処理

個人データは、特定され、明示的かつ正当な目的のために収集されるべきであり、**追加処理**は、当初の目的と両立する場合にのみ行われるべきである。[257]この点で、特定の人道支援プログラムの下で**デジタルアイデンティティ**証明書を提供するために**データ主体**から収集された**個人データ**（例えば、受益者のアイデンティティを確定する目的のもの）を、別のプログラム（例えば、援助またはサービスを提供するもの）の下で追加的に取り扱えるかどうかを検討することが重要である。**人道団体**は、目的制限の原則を適用する際に、以下の要素を考慮すべきである。[258]

- 当初の目的とその後の目的の両立性
- 個人と管理者の関係を含む、データが収集される状況
- データの性質
- 受益者への潜在的な影響
- 関連する保護手段（暗号化や**仮名化**などのデータセキュリティ対策を含む）

デジタルアイデンティティ・システムには複数の用途があり、それぞれに目的があるため、人道団体は特定の**処理**操作の全ての目的を明確に指定する必要がある。これらの目的が変更されたり、後に明確化された場合には、その機関は**データ主体**に対して更なる通知を行う必要がある。

12.6.3 比例性

比例性の原則は、特定のデータ**処理**目的を達成するために、立ち入る度合いが最小限のデータ**処理**手段を使用することを要求する。援助の提供のような人道活動の中には、受益者が給付を受ける権利を有することのみの証明を要求するもの（すなわち認証）もあれば、基本的（または「公的」）アイデンティティを要求するもの（すなわち照合）もあることは、記憶に値する。このため、**人道団体**は、データ管理者として、どの活動が識別を必要とし、どの活動が必要としないかを考慮すべきである。受益者の法的アイデンティティはそもそも人道団体によって収集または保管されることはないため、データ**処理**を受益者のサービスへのアクセス権を認証することに限定することで、偶然または意図せずにデータを転用したり、不必要な情報を収集したりすることを回避できる。認証または識別が必要な場合、人道団体は必要なデータの量と種類についても考慮する必要がある。たとえば、生体認証用データを使用する場合は、できるだけ最小限のデータポイント（例えば、10個の指紋の代わりに1つの指紋）を処理すべきである。

257 第2章：データ保護の基本原則を参照
258 EDPS、2017年、pp.9–10

12.6.4 データの最小化

人道団体は、データ処理の目的を達成するために必要な最小限のデータのみを収集し、処理すべきである。そのため、**個人データ**を**処理**する識別システムを導入する前に、受益者からどのような情報が必要かを十分に理解しておく必要がある。資格の証明だけで十分であると機関が判断した場合（認証）、どのような方法であってもアイデンティティ情報を収集または処理すべきではない。

12.6.5 データ・セキュリティ

シナリオ3で想定されているような**デジタルアイデンティティ**・システムは、受益者が自分のデバイス上に自身の**個人データ**を保存することを可能にする。同じことが、アイデンティティ証明書を持たない人々にアイデンティティ証明を提供するために計画された取り組みにも当てはまる。このような場合、悪意のある個人または組織は、理論上、デバイスのセキュリティを侵害できる場合にのみ、この情報にアクセスできる。しかし、受益者が身体的に強要されて自分のデバイスを引き渡す可能性もある。

シナリオ1とシナリオ2で言及されているような他のケースでは、**人道団体**は、**デジタルアイデンティティ**・プログラムの一部として、自身のデータベース内に**個人データ**を保管することができる。これらのデータベースは、悪意のある個人や組織のターゲットになる可能性がある。したがって、**人道団体**は、**デジタルアイデンティティ**・システムがシステム内のデータの機密性、可用性、完全性を確実に維持し、その際にデータを誤用、データ侵害、障害から適切に保護しなければならない。[259]さらに、特定の種類の**個人データ**の機微性は、一般に非常に高いレベルのセキュリティを必要とする。秘密分散共有（「秘密分散」とも呼ばれる）システムなどの暗号化技術は、セキュリティの強化に役立つ。このようなシステムでは、データが暗号化され、キーが複数の当事者間で断片化される。その後、これらの当事者は連携してデータを復号する必要があるため（例えば、シナリオ3で想定されているような異なる**人道団体**）、単一障害点を回避できる。この構成では、特定の数のフラグメント（その数はシステムによって異なる）を消去するとデータが使用できなくなるため、必要に応じてキーを簡単に破棄できる。

アイデンティティ・プログラムを実施する際、**人道団体**は、パートナーが採用する安全対策も考慮すべきである。例えば、受益者の情報が他の機関や組織と共有される場合、それらの組織はデータを保護し、データ侵害の有害な結果を回避するための適切なセキュリティ対策を講じていなければならない。

259 USAID、2017年、p.25

12.6.6 データ保全

個人データは所定の期間保全されるべきであり、その期間はデータ**処理**の目的のために必要な期間を超えてはならない。データ**処理**の主な目的が、食料、住居および医療の形態の基本的な人道支援を提供することである場合、**個人データ**は、その支援の提供のために必要な期間のみ保全されるべきである。しかし、アイデンティティ証明書を持たない受給者にある種のアイデンティティ証明書を提供しようとするデジタル身元確認プログラムの場合、状況はより複雑である。なぜなら、受給者は、生涯にわたって自分のアイデンティティ（身分証明書に代わるもの、または身分証明書として機能するもの）を使い続けたいだけでなく、時間の経過とともにその地位や状況を更新したいと考える可能性があるからである。ここで、適切なデータ保存期間を決定することは困難である。しかしながら、**人道団体**は、データが収集されている当初の目的と整合性のある保存期間を最初に提示すべきである。この期間が終了したら、この種のプログラムに関与する機関は、データの保持を継続する必要があるかどうかを判断するために、定期的な評価を実施すべきである。もう1つの選択肢は、受益者によって彼らのデータが保持できるかどうかを決定できるようにすることである。

12.7 国際的なデータ共有

技術的な解決策と選択された設計によっては、***デジタルアイデンティティ***・システムで処理されたデータは、国境を越えて日常的に出回る可能性がある。例えば、上記シナリオ3では、複数の組織が情報を共有したり、受益者が同時に複数の組織とデータを共有したりする場合がある。**国際的なデータ共有**はデータ保護への懸念を引き起こす。[260]一部の国・地域では保護措置が認められているが（契約条項の使用など）、***デジタルアイデンティティ***・プログラムを実施している人道団体は、システムが異なる場所の複数の当事者を関与させる可能性があるため、実際にはこれらの措置の実施に苦慮する場合がある。原則として、**人道団体**は、個人情報の第三者への移転（およびその後の転送）が個人の権利保護の水準を低下させないことを確実にするために、あらゆる手段を講じることが推奨される。**人道団体**は、自らが行う全てのデータ転送について責任を負うため、想定されるシナリオにおいてデータが他の組織と違法に共有された場合には責任を負う。しかし、受益者の**同意**は、場合によっては、組織がデータを移転するための適切な法的根拠となる可能性がある。しかし、上記のとおり、援助を受けた受益者が常に有効な**同意**を与えることができるかどうかは疑問である。[261]そのような場合、異なる法的根拠を識別しなければならない。

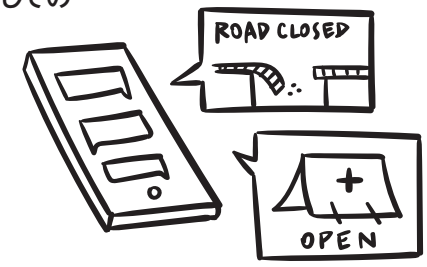
260 第4章：国際的なデータ共有を参照
261 セクション3.2：同意を参照

ソーシャルメディア

利用可能性

災害
緊急時
対応

援助としての
情報



保健情報と
アドバイス

行方不明者の
特定

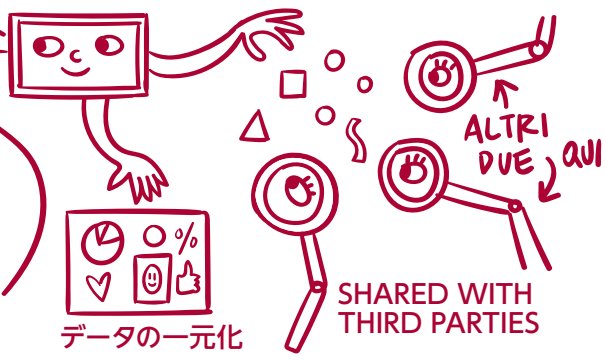
対応体制の準備

復旧に向けた
取り組み

フィードバックの
収集

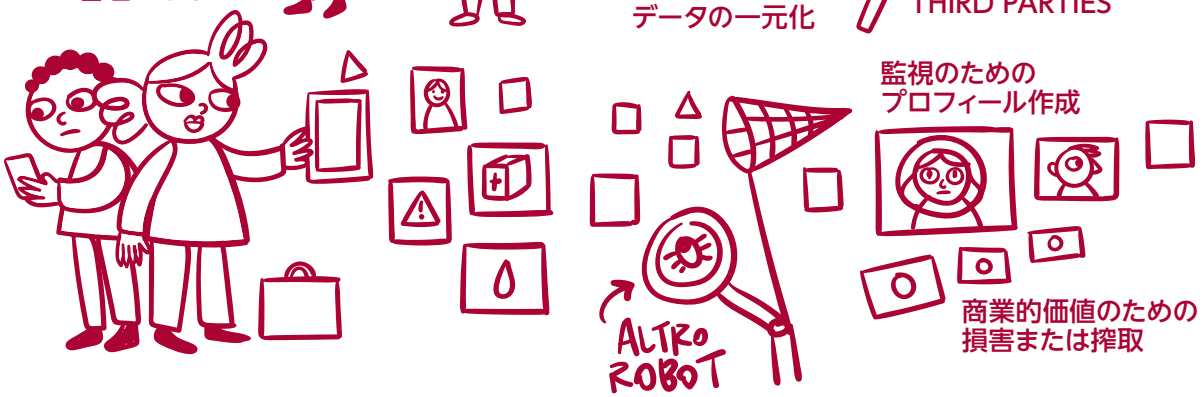
CHALLENGES

個人データが
管理できない



データの一元化

SHARED WITH
THIRD PARTIES



監視のための
プロフィール作成

商業的価値のための
損害または搾取

第13章

ソーシャルメディア[262, 263]

262 本章では、人道団体が受益者とコミュニケーションを取り、関与するためにソーシャルメディアを利用することに焦点を当てる。ソーシャルメディアを活用した危機の把握や人道対応の改善に関する情報については、第6章：データ分析とビッグデータを参照されたい。メッセージアプリについては、第11章：モバイルメッセージングアプリを参照

263 この章への貢献に対し、Nicolas de Bouville氏（Facebook）、Camila Graham Wood氏、Antonella Napolitano氏、Ed Geraghty氏（プライバシーインターナショナル）に感謝の意を表する。

13.1 はじめに

13.1.1 人道支援分野におけるソーシャルメディア

人道団体は、ソーシャルメディアを通じて様々な方法で受益者と交流している。例えば、緊急時には、ソーシャルメディアを使って人々に安全な場所や支援物資の提供について知らせることができる。又、ソーシャルメディアを利用して認知度を高めたり（移住の枠組みの中で生じる人道的ニーズへの対応など）、緊急時に受益者同士が情報を共有したり、医療や健康に関する情報を提供したりすることもある。

このような方法で受益者と関わることは多くのリスクを伴う。個人が**人道団体**による公共または民間のソーシャルメディアの投稿を閲覧したり返信したりする場合、あるいはそのような団体が主催する公共または民間のグループに参加する場合、彼らは当該プラットフォームと多種多様なデータを共有する。**人道団体**も受益者も、自分たちがデータとメタデータ（他のデータについて記述し、情報を与える一連のデータ）の両方を生成していることを必ずしも十分に認識していないまま、ソーシャルメディア上で互いに関わり合っている可能性がある。[264]そうしたデータやメタデータは、ソーシャルメディア・プラットフォームによって収集され、受益者のアイデンティティの主要な側面、ネットワーク、見解や意見、嗜好や所属といった特質を決定する個人のプロフィールを作成するために使用される。上記と同様に、組織と受益者はそのようなデータ**処理**の結果とリスクを認識していないかもしれない。

個人は私的な会話のような方法で非公式に**人道団体**と関わっているが、ソーシャルメディア・プラットフォームは、その設計と運用方法により、第三者が個人同士の交流を監視し、収集し、保持し、分析できるかもしれないことを意味する。これらの第三者には、ソーシャルメディアのプロバイダだけでなく、オープンソースの情報技術とソーシャルメディアの高度な監視ツールを使用する企業団体、法執行機関、移民および国境当局、および政府も含まれる。ソーシャルメディア上で共有されている画像を含むデータは、画像や顔の認識から感情の認識[265]に至るまで、しばしば不透明なアルゴリズムや**機械学習**を使用するなど、さまざまな方法で分析されている。[266]この種のプロファイリングは、ソーシャルメディアによる交流やソーシャルメディアの利用を通して個人がどのように露出されるかに関する不透明さを増している。このようなプロファイリングに基づいて決定がなされると、個人に重大な影響がもたらされる可能性がある。なぜなら、この不透明

264 メタデータの詳細については、次を参照：ICRC and Privacy International、*The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、Privacy International and ICRC、2018 年：https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf

265 例えば、F. M. Plaza-del-Arco et al.、" Improved emotion recognition in Spanish social media through incorporation of lexical knowledge"、2019年9月27日：https://www.sciencedirect.com/science/article/pii/S0167739X1931163Xを参照

266 第16章：人工知能と機械学習を参照

性は、例えば、意思決定のプロセスや結果に影響を与えたり、それを決定したりする誤った仮定に異議を唱えることをできなくするなど、データと司法制度への不平等なアクセスから生じる追加的なリスクをもたらすからである。

ソーシャルメディアは**人道団体**がサービスを提供するのに役立つが、これらのプラットフォームを使用すると、機関は生成および共有されるデータを制御できなくなり、中長期的なリスクをもたらす可能性がある。こうしたリスクは、明確な手順とリスク・アセスメント（後述の**データ保護影響評価**に関するセクション2を参照）を通じて評価されなければならない。

人道団体が受益者と関わるためにソーシャルメディアを利用した事例を以下に示す。[267]

- **災害と緊急事態の緩和、準備体制、対応、復旧に貢献することにより危機管理を容易にすること：**バングラデシュでは、国家調整プラットフォームの創設により、**人道団体**は政府と連携して、災害の準備段階を促進するために、緊急時に、理解しやすい防災メッセージをソーシャルメディアで配信することができた。
- **援助物資輸送の質の向上：**シリアでは、治安状況により食糧配給間隔が長期化し、2016年に赤十字国際委員会（ICRC）が食糧パックで提供される食糧の容量を倍増した。受益者はFacebookのICRCの公式ページで共有された短い動画でこの変更を知らされた。コメント機能を通じて、受益者は動画に返信し、自分たちのニーズを説明する機会も得られた（例えば、輸送中に中の食品が損傷しないように、より良い段ボール箱を要求するなど）。ICRCはコメントに回答し、要求を満たすために何をしていたのか、又なぜできなかったのかについて説明した。
- **サービスの効率化：**ケニア赤十字社（KRCS）はソーシャルメディア・プラットフォームを積極的に監視し、交通事故の情報を収集して救急車を現地に派遣している。このことを知っているケニア人は、ソーシャルメディアを通じてKRCSに道路交通事故を頻繁に通知している。
- **「援助としての情報」と健康増進：**MSFをはじめとするNGOは、ソーシャルメディアを利用して受益者に保健情報やアドバイスを提供している。

ソーシャルメディア・プラットフォームは幅広い機会を提供するが、それらを利用することは受益者にリスクをもたらし、**人道団体**に重大な責任問題を提起する可能性もある。本章では、中核的なデータ保護の問題に取り組む前に、ソーシャルメディア上でどのようにデータが生成されるかについて論じる。

267 T. Lüge、*How to Use Social Media to Better Engage People Affected by Crises: A brief guide for those media using social media in humanitarian organizations*、ICRC, IFRC and UN-OCHA、2017年：https://www.icrc.org/en/document/social-media-to-engage-with-affected-peopleより抜粋

13.1.2 ソーシャルメディアとデータ

13.1.2.1 ソーシャルメディア上でどのようなデータがどのように生成されるか

ソーシャルメディア・プラットフォームは、メタデータ、ユーザーの居住地、画像、連絡先、「いいね!」、注目や興味を表す要素などを含む、大量のデータをユーザーから受け取り、取り込み、生成し、処理して、さまざまな目的に利用する。ユーザーが具体的に自分のデータについて問い合わせても、どのようなデータが作成されているのか、プラットフォームや他の第三者がどのようにこれらのデータにアクセスし、プロファイリングやその他の目的に使用しているのかについては、ほとんど透明性がない。

ソーシャルメディア・プラットフォームによって収集されるデータの中には、個人から直接収集されるもの（これは「宣言データ」として知られている）がある。その類には、アカウントにサインアップしたときに収集されるデータ（名前またはユーザー名、場合によっては身分証明書のコピー、電話番号、電子メールアドレス、および実際の住所）や、プロフィールに写真やコメントを投稿したときに収集されるデータなどがある。[268]

ソーシャルメディア・プラットフォームは、ユーザー自身が直接提供していないが、宣言されたデータから推定される追加データである、いわゆる「推定データ」も処理する。ここで、宣言されたデータには、ユーザーが直接提供したデータと、他のアプリやプラットフォームからのユーザーに関するデータの両方が含まれている。ユーザーがアプリを開いたり、そのサービスにアクセスしたりすると、**同意**を得る前であっても、ソーシャルメディア・プラットフォームに**個人データ**が自動的に転送されることがある。[269]例えば、オンライン店舗が、ユーザーが店舗のウェブサイトにアクセスしたことをソーシャルメディア・プラットフォームに通知し、プラットフォームがターゲット広告を提供するためにユーザーの買い物の好みを使用できる場合がこれに当たる。

ソーシャルメディア・プラットフォームは通常、異なる情報源から得たデータを組み合わせ、**データ分析**を適用して、[270]ユーザーの活動と行動を監視するユーザープロフィールを作成する。[271]例えば、プロバイダはある人の友人が誰であるかをソーシャルメディア上の連絡と交流の頻度から推定することができる。[272]ユーザーの習慣的な行動と振る舞いを理解することで、プラットフォームは対象を絞ったサービスとパーソナライズされたコンテンツをユーザーに提供することができる。[273]

---

268 ICRC and Privacy International、2018年、p.34

269 Privacy International、“Investigating Apps interactions with Facebook on Android”、2019 年：https://privacyinternational.org/appdata

270 第6章：データ分析とビッグデータを参照

271 EU第29条作業部会、*規則2016/679（wp 251 rev.01）の目的における自動化された個別意志決定及びプロファイリングに関するガイドライン*、2018年、p.12

272 ICRC and Privacy International、2018年、p.35

273 ターゲット広告の詳細については、Privacy International、「AdTech」、https://privacyinternational.org/topics/adtechを参照してください

ある人のデジタル行動特性、すなわちオンライン活動、からプロフィールの形でアイデンティティを構築することが可能であることを示す証拠がある。[274]その結果、ある人のデジタル上の痕跡は、その人に知られずに、デジタルプロフィールを作成するために使用することさえでき、[275]そして、その人の性別、性的志向、宗教、居住地、人間関係および予期される行動を含むその人に関する情報を推定することができる。[276]このタイプのプロフィールは、ターゲット広告に使用されるが、過去には政治キャンペーンや予測的警察活動にも使用されたこともある。[277]これは、受益者がソーシャルメディア上で人道団体と関わることを奨励する**人道団体**は、この種のターゲット戦法に加担しているかもしれないことを意味する。

収集可能なデータの例：

Facebookは収集したデータを、ユーザーが提供するデータ、他のユーザーがそのユーザーについて提供するデータ、ユーザーのネットワークと接続に関するデータ、支払い情報とデバイス情報、広告主、アプリ開発者、発行者などのパートナーからの情報など、さまざまなカテゴリーに分類している。[278]各カテゴリには、プラットフォームが収集する次のようなデータの長いリストがある。

ユーザーがアカウントにサインアップしたとき、コンテンツを作成または共有したとき、および他のユーザーとメッセージをやり取りしたときを含む、当社製品の使用時にユーザーが提供するコミュニケーションおよびその他の情報。これには、写真の撮影場所やファイルが作成された日付など、（メタデータのような）ユーザーが提供するコンテンツに関する情報を含めることができる。[279]

このリストには、「ウィンドウが前面に表示されているか背面に表示されているか、マウスの動きなど、デバイス上で実行される操作と行動に関する情報」[280]、ブルートゥース信号、近隣のWi-Fiアクセスポイント、ビーコン、携帯電話基地局に関する情報も含まれている。

274 A. Beduschi et al.、" Building Digital Identities: The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for new Digital Identity Systems"、*Open Research Exeter*、2017年、p.8：https://ore.exeter.ac.uk/repository/handle/10871/28297

275 例えば、Facebookのシャドウアカウントhttps://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacyを参照

276 ICRC and Privacy International、2018年、p.90

277 例えば、A. Meijer and M. Wessels、" Predictive Policing: Review of Benefits and Drawbacks"、*International Journal of Public Administration*、Vol.42、Issue 12、2019 年、pp.1031–1039、DOI: 10.1080/01900692.2019.1575664参照。予測的な警察活動は法執行活動の一部と考えられている。

278 Facebookデータポリシー：https://www.facebook.com/full_data_use_policy

279 Facebookデータポリシー

280 Facebookデータポリシー

一方、Twitterは、ユーザーの基本情報（宣言された名前、ユーザー名、電子メールアドレスなど）、プロフィール情報、連絡先情報、公開情報（ツイートやツイートによって生成される時間や場所などのメタデータ）に関するデータを収集する。[281]

13.1.2.2 どのようなデータを第三者と共有できるか

一部のソーシャルメディア・プラットフォームは、特定のプロフィールを持つ個人のターゲット広告を実施するなどの目的で、収集した情報を他のサービスプロバイダと共有する場合がある。ソーシャルメディア・プラットフォームの急激な成長に伴い、個人情報にアクセスできる人や広告会社の数が近年大幅に増加しており、個人が異なる方法で追跡される可能性が高まっている。さらに、ソーシャルメディア・プラットフォームはパートナーシップ契約を通じて他の関係者や組織からデータを受け取り、これらの追加データは広告を含む様々な目的のためにユーザープロフィールをさらに発展させるために使用される。

ソーシャルメディア・データの共有方法の例：

Facebookは、同ネットワークのユーザーおよび非ユーザーから収集した集計情報を、他のFacebook企業（Instagram、WhatsApp、Messengerを含む）および第三者のパートナー企業と共有する。又、ユーザーは自分のFacebook上の保存データを、Facebookを利用している、あるいはFacebookと統合されている第三者のアプリ、ウェブサイト、その他のサービスと共有することができる。[282]これは、ユーザーが（知っているかどうかにかかわらず）友達リストのように自分以外の情報を含むデータを共有する場合があることを意味する。結果として、「ユーザーがプロフィールを『ロック』しても、ユーザーのデータは友達の1人が利用する第三者のアプリによって収集することができる」。[283]

Facebookは又、広告主がユーザープロフィールから恩恵を受けるためのさまざまなオプションを提供している。例えば、広告主は登録した顧客のメールや電話番号のリストをアップロードし、マーケティング目的でターゲット広告を実施するために、Facebookにターゲットとなる顧客のソーシャルメディア・プロフィールを見つけるよう依頼することができる（「カスタムオーディエンス」として知られている）。[284]これにより、広告主はFacebookから提供される集約された情報の恩恵を受ける一方で、ソーシャルメディア・プラットフォームは広告主からもデータを収集する。企業は又、広告の範囲を広げたり、特定の場所、人口統計、性別に焦点を当てたり、さらには自社のウェブサイトにピクセルを追加したりするために、既存の顧客に類似したプロフィールを見つ

281 ICRC and Privacy International、2018年、p.96
282 Facebookデータポリシー
283 ICRC and Privacy International、2018年、p.96
284 Facebook,「顧客リストのカスタム対象者について」：https://www.facebook.com/business/help/341425252616329

けるようFacebookに求めることがある。[285]これにより、Facebookユーザーが自社のウェブサイトを訪問すると、ユーザーのFacebookページに同社の広告を表示させることができる。[286]しかし、2019年12月以降、Facebookはユーザーが二要素認証にサインアップする際に入力した電話番号を「知り合いかも」（友達紹介）[287]に使用することを許可しなくなった。

この企業慣行の変更は、プラットフォームと第三者間のデータ共有の影響に対する認識の高まりを反映している。これはさらに、新しい「Facebook外のアクティビティ」ツールによって実証されている。[288]これにより、ユーザーは第三者が入手した情報を自分のFacebookプロフィールから分離することができる。

一方、Twitterは、ユーザーが**処理**アクティビティの多くからオプトアウトできるようにしている。ただし、デフォルトでは、ユーザーが特に指定しない限り、プラットフォーム上で共有および発表されるものは全て公開となる。実実上、Twitterは：
ユーザーの公開情報（プロフィール情報、公開ツイート、フォロワーなど）を広範囲のユーザー、サービスおよび組織に共有または開示することを許可されている。Twitterはさらに、これらのデータから、ユーザーにとって興味のあるトピックを推定する権利を維持する。[289]

13.1.2.3 どのようなデータを法執行機関と政府は入手できるのか

国内法では、公的機関が法執行の目的のため、個人を識別したり、オンライン活動に関する情報を入手したりできるように、ソーシャルメディア・プラットフォームに対して**個人データ**の保存を必要と定める場合がある。[290]全てではないが一部の法域では、そのような情報にアクセスするために令状が必要となる場合がある。

政府のアクセス要請に関する情報は、特に司法手続のある法域では、一部公開されているかもしれないが、透明性レポートを公表しているソーシャルメディア企業はごくわずかである。[291]

285 Facebook pixelはFacebook分析ツールで、企業がその有効性を測定し、企業のウェブサイトを訪問した際に人々が取る行動を理解することで、広告のターゲットを絞り込むことができるようにしている。「Facebook Pixelについて」：https://www.facebook.com/business/help/742478679120153?helpref=page_contentを参照

286 B. V. Alsenoy et al., *From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms*、ベルギープライバシー委員会、2015、pp.55–64

287 K. Paul、" Facebook separates security tool from friend suggestions, citing privacy overhaul"、Reuters、2019年12月19日：https://www.reuters.com/article/us-facebook-privacy-idUSKBN1YN26Q

288 Facebook、"Now You Can See and Control the Data That Apps and Websites Share with Facebook"、2019年8月20日：https://about.fb.com/news/2019/08/off-facebook-activity/

289 ICRC and Privacy International、2018年、p.97

290 ICRC and Privacy International、2018年、p.34

291 Facebook、" Government Requests for User Data"、2018 年：https://transparency.twitter.com/en.html
Twitter、"Twitter Transparency Report"、2018年：https://transparency.twitter.com/en.html

プラットフォーム自体が提供するツール（いわゆる「ファイアホース」）を含む様々なツールを使用して、法執行機関やその他の第三者は、オープンソース・インテリジェンス（OSINT）、すなわち公に入手可能なデータから収集されたインテリジェンスを通じて、ソーシャルメディアに直接アクセスすることができる。又、ソーシャルメディア・インテリジェンス（SOCMINT）を利用することもできる。これは、ソーシャルメディア・プラットフォーム上の公開情報と個人情報の両方を収集・監視するものである。[292]これらの行為は多くの法域で規制されておらず、そのような監視が適法であるかどうか法律が不明瞭な場合が多い。さらなる侵入技術により、デバイス[293]上に物理的に保存されている、またはクラウドベースのアプリケーション[294]内にあるデータおよび情報も抽出することが可能となる。SOCMINTと同様に、携帯電話およびクラウド上の抽出技術は、透明性がほとんどなく、多くの法域で規制されていない。実際には、ソーシャルメディアの保存はクラウドベースであることが多いため、こうした方法で取得できる**個人データ**の量は非常に多い。

13.2 データ保護影響評価

人道団体は、ソーシャルメディアプラットフォームがどのように機能し、どのようにデータを生成し処理するかを完全にコントロールすることはできない。しかし、そのようなプラットフォームを使用するかどうか、どのように使用するか、そしてどのような目的で使用するかを決定する前に、受益者と交流するためにソーシャルメディアを使用することの影響を理解するために、リスク評価を実施することは可能であり、又実施するべきである。

人道団体は、受益者がすでに登録し、プラットフォームの条件に同意しているか、またはその他の方法で同意していることを期待して、ソーシャルメディアを利用する。このような期待があっても、機関は**データ保護影響評価**（DPIA）を実施する義務を免れることはない。[295]DPIAの目的は、ソーシャルメディアの利用が受益者にどのような影響を与えるかを明らかにし、潜在的なリスクを軽減するために組織が取ることのできる措置を明らかにすることである。特に、DPIAはデータ保護のリスクを検討するだけでなく、特定の状況でのソーシャルメディアの利用が、人権侵害を引き起こすのか、そうでなくとも問題となっている個人に害を与えるのかを評価すべきである。これらのリスクと潜在的な便益とを比較検討すべきである。

292 Privacy International、“Social Media Intelligence”：https://privacyinternational.org/explainer/55/social-media-intelligence

293 例えば、Privacy International、“Push This Button For Evidence: Digital Forensics”：https://privacyinternational.org/explainer/3022/push-button-evidence-digital-forensics と Privacy International、“Can the police limit what they extract from your phone?” 2019 年 11 月 14 日：https://privacyinternational.org/node/3281を参照

294 Privacy International、「クラウド抽出技術：政府機関がアプリから大量のデータを収集できる秘密の技術」、2020 年 1 月 7 日：https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data

295 第5章：データ保護影響評価（DPIAS）を参照

強調しておきたいのは、ユーザーがアカウントにサインアップする際に生成し提供するコンテンツは別として、ユーザーのソーシャルメディアの利用は大量のデータやメタデータを生成するが、プラットフォームはそれらを積極的に公表しないことである。そのため、ユーザーはこれらのデータが生成および処理されていることに気づかない場合がある。[296]たとえば、ユーザーが「いいね!」ボタンをクリックしたり、他のWebサイトに転送されるリンクをクリックしたりするだけで、メタデータが生成される。

近年、多くの政府が、大量のソーシャルメディアデータやメタデータにアクセスし、それらを利用するとともに、そうしたデータのパターンを特定し、個人やグループのプロフィールを作成するのに役立つ強力な分析ツールを利用している。[297]したがって、DPIAは単にデータ保護要件が遵守されているかどうかを分析することにとどまってはならない。又、特定のアプリケーションやプラットフォームの利用が、様々な基本的権利や**人道団体**によるデータ**処理**の倫理的・社会的意味合いに、どのようにプラスまたはマイナスの影響を与えるかについても検討すべきである。[298]

メタデータの**処理**には大きなリスクが伴う。たとえば、2014年には、米国家安全保障局（NSA）の元長官が、メタデータから取得した情報に基づいて人を殺害することを決定することもあると述べている。[299]フィンテック企業や広告会社も、このようなデータを利用するために多くの技術を採用している。[300]だからこそ、**人道団体**は、DPIAを実施し、そのソーシャルメディア利用戦略を策定する際に、ソーシャルメディアを利用する際の人道以外の目的と影響を考慮に入れることが重要である。

同様に、DPIAは、ソーシャルメディアプロバイダのビジネスモデルがユーザーデータの収益化に依存しているという事実を考慮すべきである（例として、広告ターゲティング）。これは、このようなプラットフォームを通じて人道目的のために収集されたデータは、商業目的の搾取行為や監視に対して脆弱である可能性があることを意味する。

人道団体は又、ソーシャルメディアが受益者とコミュニケーションをとるための最も安全で信頼できる方法であるかどうかを評価すべきである。例えば、緊急時には、政府は恐怖やデマの拡散を避けるためにソーシャルメディアをシャットダウンすることができる。[301]これは、**人道団体**が他のコミュニケーション手段を考慮する必要があることを意味する。

296 ICRC and Privacy International、2018年、p.17
297 ICRC and Privacy International、2018年、p.29
298 A. Mantelero “AI and Big Data: A blueprint for a human rights, social and ethical impact assessment” *Computer Law & Security Review*、Vol. 34、Issue 4、2018 年、pp.754–772：https://doi.org/10.1016/j.clsr.2018.05.017
299 ICRC and Privacy International、2018、p.22
300 ICRC and Privacy International、2018、pp.23–24
301 例えば、J. Wakefield、“Sri Lanka attacks: The ban on social media”、BBC、2019年4月23日：https://www.bbc.com/news/technology-48022530を参照

13.3 倫理的問題とその他の課題

人道団体にとって、ソーシャルメディアのプラットフォームを業務に含めることは、倫理的な問題を必然的に引き起こす。なぜなら、同団体は第三者のプライバシーやデータ保護ポリシーを制御できないからである。これらのプラットフォームの多くは、ユーザーのデータを利用し収益を上げることに依存しており、[302]これらのデータは、宣言されたデータと推定されたデータの両方であり、個人の性的志向、宗教、政治的意見、民族性などの機密情報を明らかにすることができる。[303] **人道団体**は、ソーシャルメディア上で受益者と関わることにより、こうした推定がなされるデータとメタデータの生成に貢献することになる。[304]

同様に、ソーシャルメディアプラットフォームは、ユーザーの**同意**を常に要求することなく、契約条件、プライバシーポリシー、**処理**アクティビティを常時変更している。さらに、ユーザーはプラットフォームが宣言したデータを処理することは理解しているかもしれないが、プラットフォームがそのようなデータから何を推定するのか、さらに重要なことに、他のソース（オンライン活動、他のユーザー、第三者など）から取得した情報や、プラットフォームの設計および運営方法によって設計段階かつデフォルトで生成されたデータから何を推定するのかについて、透明性がないかもしれない。[305] 次の例に示すように、収集された情報、および最終的にはこのデータに基づいて行われた決定は、ユーザーの生活に深刻な悪影響を及ぼす可能性がある。

ソーシャルメディア上のデータは、融資を要請しているユーザーの信頼性を評価したり、既に融資を受けているユーザーを監視したりするためにますます利用されるようになっている。こうした評価は、人々を「信頼・信用できる借り手」または「信用できないリスクの高い借り手」のいずれかに分類する指標の選択に基づいている。[306]

ソーシャルメディア・プラットフォーム上で受益者がデータを共有することに伴うリスクとは別に、**人道団体**は自らが共有するコンテンツにも留意しなければならない。受益者が写っている公開された写真や動画などの一部のコンテンツは、企業によるプロファイリングやターゲット広告から、迫害、脅迫、恐喝、差別、個人情報窃盗や、自分自身のデータ管理ができなくなることに至るまで、対象となっている個人に悪影響を及ぼす可能性がある。

---

302 例えば、Privacy International、“Guess what? Facebook still tracks you on Android apps (even if you don’t have a Facebook account)”、2019年3月5日：https://privacyinternational.org/blog/2758/appdata-updateとPrivacy International, How *Apps on Android Share Data with Facebook–Report*、Privacy International、2018年：https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report

303 ICRC and Privacy International、2018 年、pp.89–90：https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report

304 ICRC and Privacy International、2018、p.91

305 ICRC and Privacy International、2018、p.102

306 ICRC and Privacy International、2018 年、p.106。Privacy International、“Fintech”：https://privacyinternational.org/topics/fintechも参照

又、人道団体は、ソーシャルメディアが必ずしも対象となるオーディエンスに到達するための最も有用かつ効果的な方法ではないことを覚えておくべきである。ソーシャルメディアの利用は農村部や遠隔地では部分的にしか可能でないことが多く、対象となる人々の全てが平等にテクノロジーを利用できるわけではない。同様に、一部の状況では、ほとんどのソーシャルメディアユーザーが男性であるため、女性の健康のための取り組みのためにプラットフォームを利用することは効果的ではないであろう。

13.4 データ管理者とデータ処理者の関係

人道団体がコミュニケーションの目的でソーシャルメディアを利用する場合、受益者の個人**データ**の**処理**に関する団体の役割は、必ずしも明確ではない。例えば、ソーシャルメディア・プラットフォーム上に団体のページやプロフィールを設立する場合、プラットフォームの契約条件によっては、プロバイダはそのページを通じてより多くのデータを処理したり、広告目的でユーザーをプロファイリングしたりすることもできる。ここで、団体は、ほぼ間違いなくプラットフォームとの共同管理者とみなされる可能性があり、したがって**処理**の責任の一部を負う。しかし、団体がプラットフォームを利用して、受益者自身が作成したページ、プロフィール、またはグループを通じて受益者と対話するだけでは、団体の役割と責任の範囲を確定することはより困難である。

共同管理者の例：
2018年、欧州連合の司法裁判所（CJEU）は、C-210/16事件において、Facebookページの管理者は、Facebookがファンページを通じて収集および処理した**個人データ**に関連するデータ管理者であるとの判決を下した（ファンページとは、企業や組織がFacebookプラットフォーム上に作成した組織的なページで、Facebookユーザーとコミュニケーションをとり、彼らの仕事に関するコンテンツを共有するためのものである）。[307]ファンページはFacebookプラットフォーム上でホストされているため、Facebookは、プラットフォームのFacebookアカウントを持っているかどうかに関係なく、ファンページにアクセスしたり、ファンページと対話したりするユーザーに関する情報を収集する。Facebookはこの情報を使ってファンページの訪問者に関する統計を作成し、ページの管理者と共有する。

307 Court of Justice of the European Union (CJEU)、Case 210/16、Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH、Judgement ECLI:EU:C:2018:3885、2018年6月

裁判所によると、そのようなページの管理者（つまり、ページを作成および管理する組織）はデータ管理者である。なぜなら、ファンページを作成することは「Facebookに、ファンページを訪れた人がFacebookアカウントを持っているかどうかにかかわらず、その人のコンピュータやその他のデバイスにクッキーを置くことができる機会を与える」からである（第35項）。さらに、管理者がページの訪問者に関する統計から利益を得るためにFacebookによって収集される特定のパラメータを指定する場合、管理者はデータ**処理**の手段と目的の決定に参加していると見なされる。

この裁定は欧州連合の規制の文脈に関したもので、Facebookにのみ関係しているが、EUのデータ保護法の影響は、このように管理に関する広義の定義が（物議を醸してはいるが）他の領域でも採用される可能性があることを意味する。そのような場合、使用するソーシャルメディア・プラットフォームによる団体ページに関連した**個人データ**の**処理**に関して、**人道団体**がデータ管理者とみなされる可能性がある。実務上、団体のページを通じて収集された**個人データ**をソーシャルメディア・プラットフォームが人道的目的以外のために処理する場合、対象団体がそのような**処理**について責任を負う可能性があることを意味する。

したがって、**人道団体**は、利用するソーシャルメディア・プラットフォームのビジネスモデル、プライバシーポリシー、およびセキュリティプロトコルを完全に理解するために、できる限りのことをしなければならない。なぜなら、プラットフォームや他の第三者による誤用の責任を負う可能性があるからである。データ保護、人権、人道原則を遵守しているかどうかについて疑問がある場合、団体は必ずより安全なコミュニケーションの選択肢を選択するべきである。

13.5 データ保護基本原則

13.5.1 個人データ処理の法的根拠

人道団体は、ソーシャルメディア・プラットフォームがどのように運用され、データが**処理**されるかを制御することはできないが、それでも、ソーシャルメディアを通じて要求したり、受け取ったりするデータ処理の法的根拠を決定すべきである。例えば、**人道団体**は、広報キャンペーンにおいて受益者の画像を使用することがある。同意書に依拠する場合、個人は同意書を撤回できなければならない。しかし、いったん画像や動画がオンラインで公開されると、団体はそのコピーや複製を制御できなくなる可能性があり、受益者が同意書を撤回した場合、団体はコンテンツを完全に削除できない可能性がある。

人道団体は、各**処理**アクティビティの法的根拠を明確にしなければならない。[308]団体はしばしば同じソーシャルメディアのページやプロフィールを、人道支援活動やキャンペーンおよび資金調達のために使用しており、実際にはそれぞれの目的を区別することが困難になる可能性がある。このような場合、**処理**アクティビティの各項目の目的を考慮し、然るべく文書化することが重要である。[309]

13.5.2 情報

個人には、**データ管理者**によって、自分のデータの取扱いに関する明確かつ適時な情報が与えられるべきであり、[310]どのようなデータが収集されるか（例えばサービスを提供するために）、サービスの利用によってどのようなデータが生成されるか、収集の目的は何か、および誰が自分の**個人データ**にアクセス、共有および/または使用できるかが説明されるべきである。この情報により、**データ主体**は、特定のサービスを利用するかどうかについて十分な情報を得た上で決定を下し、自らの権利を行使する方法を理解することができる。しかし、**人道団体**がソーシャルメディアを通じて受益者と交流する場合、データは主にプラットフォーム自身を通じて直接生成・処理されるため、**人道団体**は上記の行動をほとんどコントロールできない。それにもかかわらず、組織は可能な限り関連情報を提供する責任を負うべきである。

繰り返しになるが、プラットフォームは定期的にプライバシーポリシーとデータ保護ポリシーを変更および更新するため、どのようなデータが生成および処理されているかについてユーザーが理解すること（すなわち、データがどのように使用され、誰と共有されるか）が非常に困難になっている。[311]したがって、ソーシャルメディアを利用することがもたらすリスクを理解することは**人道団体**にとって困難であり、団体がどのような情報を**データ主体**に提供すべきかも不明瞭である。**人道団体**は、少なくとも受益者に対し、自らが責任を負う**処理**業務について情報を提供することが望ましい。例えば、なぜソーシャルメディアを通じて情報を伝達するのか、受益者が団体と共有する情報がどのように使用され、どのような目的で使用されるのかを説明するべきである。

人道団体は、ソーシャルメディア・プラットフォームが収集したデータをどのように扱うかについてはコントロールできないが、ソーシャルメディアに関連するリスクと受益者が自分のデータを保護するためにどのような行動を取るべきかを説明するために、オンラインの意識向上キャンペーンを実施した団体もいくつかある。例えばメキシコでは、UNHCRはエルジャガーのページを使って受益者と連絡を取っている。同機関は、Facebookを利用することに伴うリスクと、そのリスクを最小限に抑える方法について受益者に警告する動画を作成し、そのページで共有した。[312]

308 第3章：個人データ処理の法的根拠を参照
309 第3章：個人データ処理の法的根拠を参照
310 セクション2.10：情報を参照
311 ICRC and Privacy International、2018年、p.17
312 キャンペーンビデオ（スペイン語）はこちらを参照：https://www.facebook.com/ConfiaEnElJaguar/videos/874221649451680/

このようなキャンペーンは、受益者がソーシャルメディア上で生成したデータにアクセスする可能性のある団体や組織の繋がり、そしてこれらのプラットフォームを通じて害が生じる危険性を理解するのに役立つ。しかし、現在のプラットフォームに代わるものを見つけられなければ、ソーシャルメディアのデータとプライバシーポリシーについて受益者に知らせても役に立たないかもしれない。代わりに、**人道団体**は受益者に、例えば、団体のグループに参加したり、ソーシャルメディア上の団体のページをフォローしたりしたときに経験する可能性のある最もあり得るリスクについて知らせることに焦点を当てるべきである。又、そのようなコミュニティのメンバーシップが他人に見られたり、何らかの形で悪用されたりする可能性を説明することにも焦点を当てるべきである。

これは特に重要である。なぜなら、データ保護の問題は別として、ソーシャルメディアの利用は、脆弱な人々やグループの監視や、その結果として悪意のある者による識別（および所在地特定の可能性）などの他のリスクをもたらすからである。

13.5.3 データ保全

データ保全の原則に従って、データは処理された目的のために必要な一定期間保全されるべきである。この期間には、3ヶ月、1年、危機がある期間、その他の期間がある。[313]なお、データの収集時に保全期間が確定できない場合には、最初の期間の終了時に見直しを実施する。

人道団体がソーシャルメディアを通じて受益者と交流する場合、プラットフォーム自体がデータを収集し、保全する。したがって、保全期間はプラットフォームによって異なる。

Facebookのデータ保全ポリシーの例：
Facebookのデータポリシーでは、サービスを提供する必要がなくなるまで、またはアカウントが消去されるまでデータを保持することが規定されているが、アカウントが消去された後もプラットフォームが一部のデータを保全しているという証拠がある。[314]ポリシーではさらに次のように説明されている。これは、データの性質、データが収集および処理される理由、関連する法的または運用上の保全ニーズなどに応じて、ケースバイケースで決定されます。例えば、Facebookで何かを検索すると、ユーザーの検索履歴内からいつでもそのクエリにアクセスして消去できますが、その検索のログは6か月後に消去されます。アカウント確認のために政府発行の身分証明書のコピーを提出された場合、提出から30日後にそのコピーを消去します。[315]

313 セクション2.7：データ保全を参照
314 A. Picchi, "OK, you' ve deleted Facebook, but is your data still out there?" CBS News 2018 年 3 月 23 日: https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/
315 Facebookデータポリシー

一部のソーシャルメディア・プラットフォームは、データまたは情報を第三者と共有する場合がある。これらの関係者は、異なるデータ保全ルールを設定している場合もある。ソーシャルメディアのユーザーがこれらのサービスを利用するために利用規約に同意しなければならないという事実は、第三者の保全ポリシーを受け入れることについて疑問を提起する。したがって、**人道団体**は、こうしたポリシーを分析し、受益者または団体自体にリスクをもたらすかどうかを評価し、意図した目的のためにそのプラットフォームを利用することが団体にとって適切であるかどうかについて、十分な情報に基づいた決定を行うべきである。

又、**人道団体**は、ソーシャルメディアの相互作用、グループ、ページを通じて受益者から収集するデータの保存期間やポリシーを設定する責任を負う。人道団体は、これらの期間またはポリシー、あるいはその両方を団体のスタッフと受益者の双方に説明すべきである。

13.5.4 データセキュリティ

人道団体は、プラットフォームのビジネスモデル、ポリシー、利用規約、より広範なエコシステム、およびプラットフォームが処理するデータを保護するために取るあらゆるセキュリティ対策を考慮して、DPIA（上記のセクション2参照）を実施すべきである。プラットフォームはこの情報をオープンに共有していないかもしれないが、過去のデータ侵害やプラットフォームの対応、その他の既知の脆弱性を分析することを有効な出発点とすることができる。又、プラットフォームがユーザーのデータをどのように処理し、データが安全に保持されていることを保証するためにどのような手段を講じているかを理解することも重要である。

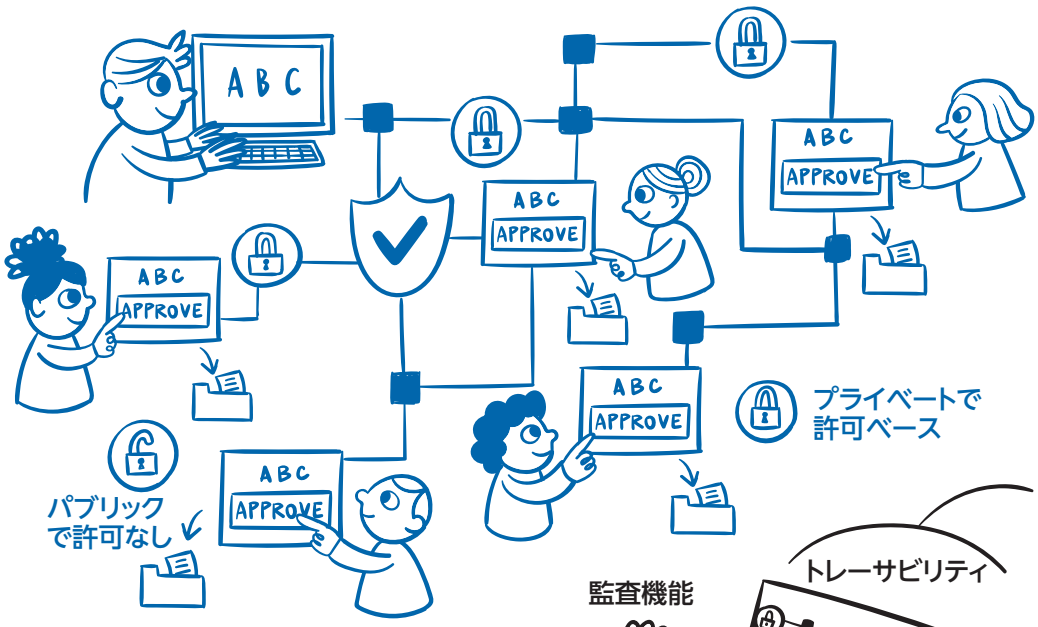
内部的には、**人道団体**は、受益者から収集したデータを保護するために、ログインと強力なパスワードによりデータを保護すること、必要な場合のみアクセスを許可すること、およびデータを正しく扱うために職員を訓練することなど、適切な措置を確実に講じることが望ましい。

13.6 国際的なデータ共有

ソーシャルメディア・プラットフォームを通じて処理されたデータは、日常的に国境を越えて流れ、アクセスされるため、**個人データ**保護の懸念が生じている。認められた契約メカニズムは存在するが、特にソーシャルメディア・プラットフォームはしばしば**人道団体**の制御範囲外にあるため、効果的な契約の履行は困難である。とはいえ、機関側は、できる限りのことをしてプロバイダが必要なデータ転送の仕組みを実装していることを保証しなければならない。[316]適切で的を絞ったリスク分析は、管轄権の選択と法の選択がソーシャルメディアガバナンスに明確に埋め込まれていない限り不可能なため、適用可能な法律と管轄権の決定が又課題となる場合もある。

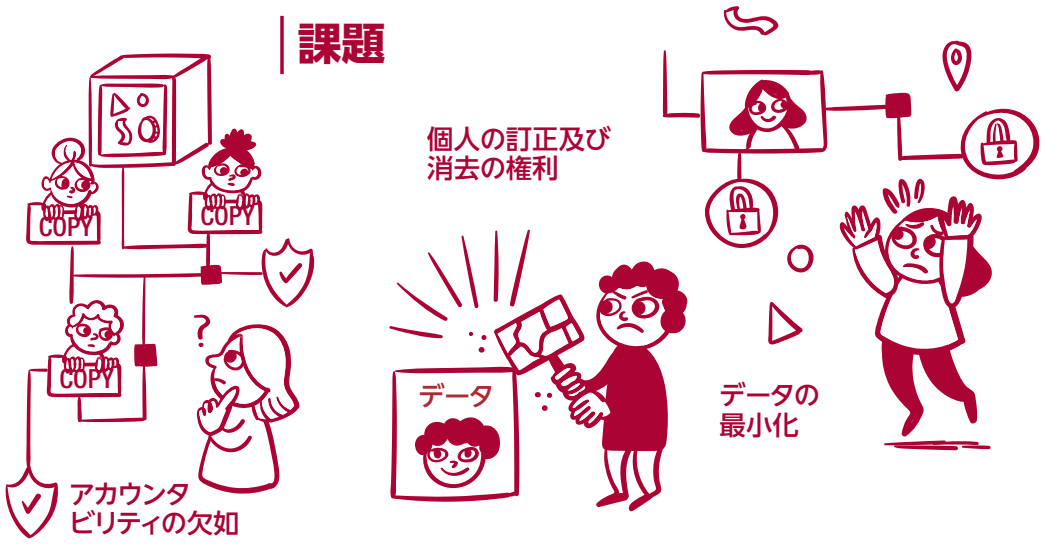
316 第4章：国際的なデータ共有を参照

ブロックチェーン



利用可能性

課題



第14章

ブロックチェーン[317]

317 この章への貢献に対し、Robert Riemann氏（欧州データ保護監督官）、Giulio Coppi氏（ノルウェー難民評議会）、Bryan Ford氏（スイス連邦工科大学ローザンヌ校）に感謝の意を表する。

14.1 はじめに

近年、「**ブロックチェーン**」が流行語となっており、人道団体を含む様々な組織がこの技術の利用を模索している。**ブロックチェーン**は、例えば金融取引やサプライチェーンの追跡などに関わる人道支援プログラムの効率性を改善できると主張されている。[318]又、ブロックチェーンは情報の完全性において透明性と信頼性を高めることもできると示唆されている。[319]しかし、このような改善の達成は、多くの現実的な課題とデータ保護の課題により相殺される可能性がある。これらについて、予想されるメリットとリスクとともに以下で説明する。

本章では、**ブロックチェーン**の技術、主な関係者、およびそのさまざまなアーキテクチャについて、簡略化してわかりやすく説明する（セクション1.1からセクション1.3）。**ブロックチェーン**は複雑な技術であるため、この説明は決して網羅的なものではない。セクション2からセクション7で説明するデータ保護分析を補完するものに過ぎない。[320]

14.1.1 ブロックチェーンとは

ブロックチェーンは「本質的には、コンセンサスアルゴリズムによって維持され、複数のノード（コンピュータ）に格納されるアペンド専用の分散データベース」である。[321]この定義には、以下により詳細に説明する多数の複雑な技術的要素が含まれる。基本的に、**ブロックチェーン**・テクノロジーは、データベース内にデータを保管する特別な方法である。したがって、**個人データ**を含むいかなるタイプのデータでも**ブロックチェーン**に格納することができる。**ブロックチェーン**では、各データがチェーンのように繋がって順次格納される（これが「アペンド専用」と呼ばれる理由である）。[322]これは、データをブロック単位でグループ化し、追加する新しいブロックにその前のブロックを指す暗号ポインタ（参照またはリンク）を付加することによって行われる。

ブロックチェーンの設計は、セキュリティを高めたいという（広義の）願望に導かれている。特に、上述したように、**ブロックチェーン**技術はデータベースの完全性の透明性と信頼性を高めることを目的としている。**ブロックチェーン**は「分散型」であり、しばしば「非集中型」である。これ

318 V. Ko and A. Verity、*Blockchain for the Humanitarian Sector: Future Opportunities*、UN-OCHA、2016年、pp.12–14：https://reliefweb.int/sites/reliefweb.int/files/resources/BlockChain%20for%20the%20Humanitarian%20Sector%20-%20Future%20Opportunities%20-%20November%202016.pdf

319 Ko and Verity、2016、p.8

320 ブロックチェーン技術のより詳細な定義および説明については、J.Bacon *et al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers"、25 Rich. J.L. & Tech.、No.1, 2018年：https://jolt.richmond.edu/Blockchain-demystified-a-technical-and-legal-introduction-to-distributed-and-centralised-ledgers/を参照

321 M. Finck, "Blockchains and Data Protection in the European Union"、*European Data Protection Law Review*、Vol.4、Issue 1、2018年、p.17：https://doi.org/10.21552/edpl/2018/1/6

322 この特性が元帳とも呼ばれる理由であることに注意を要する：元帳はアペンド専用モードで（伝統的に貨幣的な）取引を格納する帳簿である

らは2つの異なる概念だが、共通の特徴を備えている。つまり、処理対象のデータが一元的に管理および保管されていないことを示している。ここで、「分散型」とは、データベースの複数のコピーが異なるコンピュータに格納されていることを意味し、「非集中型」とは、どのデータを台帳に追加するかを決定する権威と権限が単一の主体または個人によって保持されているのではなく、協働しなければならない多数のエンティティまたは個人の間で共有されていることを意味する。本章では、これらのエンティティまたは個人を「検証者」（**ブロックチェーン**に格納されるデータを一緒に検証する役割）と呼ぶ。通常、検証者の数が多いほど、合意に達するために従うべきルールが複雑になる。これらのルールは「コンセンサスプロトコル」（詳細については後述のセクション1.2を参照）に反映される。

ブロックチェーンのコピーを保持するコンピューターは、（巨大なネットワーク内にあるノードを表しているため）「ノード」と呼ばれる。ノードはパッシブ（**ブロックチェーン**の最新版を保管しているだけ）またはアクティブである。アクティブ・ノードは検証者でもあり、データの「マイニング」をしている（すなわち、データの新規挿入の妥当性を確認するためのコンセンサスプロトコルに参加している）と言われる。検証者は、類似的に「採掘者（マイナー）」と呼ばれることがある。

「ユーザー」とは、**ブロックチェーン**に情報を追加することを希望する当事者である（そのため、**ブロックチェーン**上で検証および記録する必要のあるデータを作成する）。

情報の一片は、検証されて初めて**ブロックチェーン**に挿入される。このため、悪意のある第三者が**ブロックチェーン**にデータを追加することは非常に困難である。データは、まず検証者によって受け入れられなければ追加されないからだ。

さらに、**ブロックチェーン**内の情報のブロックはタイムスタンプされ、上述のように、前のブロックへの暗号リンク（ポインタまたは参照）を含む。つまり、悪意のある者が特定のブロックに含まれるデータの変更に成功した場合でも、次のブロックも（そこに含まれている暗号ポインタの変更のために）変更する必要があり、同様に、チェーンの最後まで続く全ての後続ブロックも変更しなければならない。全ての検証者が同意する必要が組み込まれた**ブロックチェーン**の分散化設計では、このような変更が気付かれないで実行される可能性はないだろう。**ブロックチェーン**で情報を変更することは（全く不可能ではないものの）実際上、非常に難しいので、**ブロックチェーン**はしばしば変更不能台帳と呼ばれる。[323]

ブロックチェーンに追加された情報は、ユーザーの公開鍵（ユーザー名のような、データソースの偽名デジタル署名）によってデジタル署名される。[324]公開鍵だけでは、それに関係する人の身元を明らかにすることはできないが、特定の個人（情報を追加したユーザー）にリンクされて

323 Finck、2018年、p.19
324 Finck、2018年、p.19

いるため、偽名化された**個人データ**とみなされる。公開鍵を追跡すると、例えば、個人のIPアドレスに行き着いたりして、そこから個人が識別されることにもにつながりかねない。[325]**ブロックチェーン**はほぼ変更不能なため、台帳が存在する限り、公開鍵が**ブロックチェーン**内に残る可能性がある。

ブロックチェーン技術の上記の特徴のいくつかは、**人道団体**にとって有利であり得る。例えば、分散化されたアーキテクチャにはシステムの単一障害点や単一侵害点がないので、セキュリティが潜在的に強化される。**ブロックチェーン**全体を侵害しようとする攻撃者は、複数のリンクを侵害しなければならないからだ。この構造により、データの変更不能性がほぼ常に保証されるとみなされるため、システムの完全性が向上する。

情報にはタイムスタンプが押されており、変更不能に近いという事実、および責任が共有されているという事実に照らして、[326]**ブロックチェーン**は次の場合に最も価値があると主張されている。

- 複雑な事柄の所有権を長期的に追跡するために使用される場合
- 複数のグループまたは関係者が関係する場合
- 十分に確立された、または効果的な中央当局（信頼できる第三者とも呼ばれる）が存在しない場合
- 関係するグループや関係者が協力して取り組む必要がある場合
- トランザクションの記録または証明が必要である場合

これらの例は、**ブロックチェーン**技術の主なメリットの1つが、単一障害点または侵害点に対する耐性であることを示している。この耐性は、**ブロックチェーン**に新しいデータを追加するために複数のノードを連携させる必要がある、元帳の分散設計に起因している。又、元帳全体が複数のノードにコピーされるため、元帳の情報を変更することが困難となり、1つのノードが不正侵入されてもデータを他で利用可能にすることが可能となり、完全性が高まる。

完全性のレベルに問題がない場合（すなわち、特定のプログラムに関与する当事者間に十分な信頼があり、十分なレベルの監査能力がある場合）、または単に他の現行の技術が十分な程度の完全性と可用性を提供する場合は、**ブロックチェーン**技術はほとんど必要ないことに注意することが重要である。このような場合、たとえば、中央データベースを使用した従来型のソリューションの方が、より効率的、迅速、低コストで導入でき、データ保護の観点から全体的により適切であることが判明する場合がある。

325 Finck、2018年、pp.24–25
326 Ko and Verity、2016年、p.9

14.1.2 ブロックチェーンのタイプ

ブロックチェーンは、システム設計の選択に応じて、さまざまな方法で構築できる。たとえば、**ブロックチェーン**を公開するかどうかは一つの重要な決定事項である。**ブロックチェーン**の各タイプの定義について、広く合意されているものはないが、次の定義がより一般的に使用されている。

ブロックチェーン	**許可不要型： 誰でも検証者になれる （ノードまたはマイナー）**	**許可型： 検証者（ノードまたはマイナー）は、管理機関によって事前に定義および承認されている**
パブリック： 誰でも、**ブロックチェーン**に格納されたデータにアクセス（「参照」または「読み取り」）し、トランザクションを追加できる。	**ブロックチェーン**は公開されているので、誰でもブロックチェーン上のトランザクションを読み取り、新しいトランザクションの検証者としてコンセンサスプロトコルに参加できる。ただし、元帳に追加されるデータは暗号化されている可能性があるため、暗号化解除キーがないと解読してその内容を読み取ることができないことに注意。しかし、公開鍵とタイムスタンプは全てのユーザーに表示される。 このタイプの**ブロックチェーン**（無許可の）はビットコインで使われている。	**ブロックチェーン**は（公開されているため）誰でもそこに格納されたトランザクションを読むことができるが、事前に定義された関係者だけが検証者となり、新しい挿入を検証するためのコンセンサスプロトコルに参加することができる。 このような**ブロックチェーン**は、例えば、サプライチェーンの透明性を向上させるのに役立つ可能性がある。というのは、商品の取扱いに関与する者のみが元帳の変更を認可され（検証者として）、一般の人々は取引をチェックすることができるからである。
プライベート： 承認されたユーザーのみが、**ブロックチェーン**上のデータにアクセスできる。	理論上は、このタイプの**ブロックチェーン**では、事前に定義された関係者だけがブロックチェーンに格納されたデータにアクセスでき、新しい挿入の検証は誰でも参加できる。しかし実際には、検証者が元帳全体のコピーを保管できるので、このとおりに実施するのは難しいだろう。従って、検証者が元帳上の情報にアクセスできないようなプラットフォームは考えにくい。	**ブロックチェーン**に格納されているデータにアクセス（「読み取り」）できるのは事前定義されたユーザのみであり、新しい挿入の検証に参加できるのは事前定義された検証者（必ずしも同じユーザーではない）のみである。

システム設計者は、**ブロックチェーン**内で誰が「読む」または「書く」ことができるかを選択するだけでなく、検証をどのように行うかも決定しなければならない。**ブロックチェーン**の検証プロセスは、当事者間の信頼関係を分担する一連の事前に定義される規則からなる合意メカニズム（またはコンセンサスプロトコル）によって規制される。これらの規則により、中央当局（または信頼

できる第三者）なしでデータを変更不能な形で保持できるため、元帳の完全性が保持される。[327] 換言すれば、合意メカニズムは新しい情報が**ブロックチェーン**内の当事者によってどのように検証されるかを定義し、その検証によって有効であるとみなされた情報は、元帳に追加される。

コンセンサスプロトコルにはさまざまなタイプがある。例えば、プルーフ・オブ・ワーク・プロトコルを使用する**ブロックチェーン**では、検証者は、かなりの**処理**能力と電力を必要とする強力な演算手法を使用して複雑な計算問題を解くことによってトランザクションを検証する権利を獲得する必要がある。[328]一方、プルーフ・オブ・ステーク・プロトコルでは、関係者は単純な議決権を持ち、議決権の重みは、**ブロックチェーン**に係るそれぞれの利害によって異なる場合がある。

ブロックチェーンを開発する際に行わなければならないさまざまな選択のいくつかを説明するために、システムを企業のように考えることが有用である。企業は通常、取締役会を開く。取締役の選出方法や、誰に投票権や決定権があるかを規定する規則が必要である。一つの選択肢は、誰が取締役会に参加し、誰が取締役会から辞任するかを、非公開グループに決定させることである（許可の必要な**ブロックチェーン**に似ている）。もう一つの可能性は、会社の「株」を十分な数買っていれば、誰でも取締役会の席に座れるようにすることだ（プルーフ・オブ・ステーク・**ブロックチェーン**）。第3の選択肢は、過去10分間、作業に十分なエネルギーを費やしたことを証明できれば、誰でも取締役会の席に座れるようにすることである。これは参入に対する便宜的な障壁である（プルーフ・オブ・ワークの**ブロックチェーン**）。

14.1.3 ブロックチェーンの実務

学者と実務者は、ブロックチェーン技術を使用することの利点と課題を次のように提示している。[329]

利点：

- 信頼できる第三者（中央当局）が共有レコードの完全性を維持する必要がない。**ブロックチェーン**に挿入されたトランザクションは、参加者によってコンセンサスメカニズムを通じて検証される。ただし、この利点の有効性は、**ブロックチェーン**の使用方法によって異なる。
- 信頼できる第三者を排除することで、コストを削減できる。例えば、**ブロックチェーン**は、取引当事者間の直接の国境を越えた現金給付をサポートし、手数料を請求することが多い銀行や他の金融機関の必要性をなくすことができる。

327 W. Al-Saqaf and N. Seidler、"Blockchain technology for social impact: opportunities and challenges ahead"、*Journal of Cyber Policy*、Vol. 2、Issue 3、2017年、p. 2：https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1400084

328 M.Pisa and M.Juden, *Blockchain and Economic Development: Hype vs. Reality*、Center for Global Development, Washington, D.C.、2017、p.8：https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf

329 詳細については、Finck、2018年、Bacon *et al.*, 2017年を参照。

- **ブロックチェーン**は監査証跡として機能する。これは、データが保管および接続される方法が、デジタル・トークンに関連付けられた物理的資産の出所と移動を容易に追跡できるためである。[330]
- より多くの当事者が元帳にアクセスできるため、特にパブリック・**ブロックチェーン**では、透明性が向上する。しかし、プライベート・**ブロックチェーン**では、このメリットが減少したり、場合によっては存在しないことがある。
- **ブロックチェーン**は、オペレーションのレジリエンスを提供し、単一障害点や侵害点とは無縁なので、完全性と可用性を向上させる。[331]

課題：

- **ブロックチェーン**ソリューションごとに適切なガバナンス構造を決定する必要がある。
- **ブロックチェーン**は「信頼無用」と考えられているが、システムには信頼されなければならない関係者が存在する。その中には、コードの開発者や、**ブロックチェーン**やデータを格納できる**クラウドサービス**とやりとりするアプリケーションを作成する設計者も含まれる。
- **ブロックチェーン**を使用すると、悪意のある者による攻撃に晒される可能性のあるアクセスポイントの数が増加し、セキュリティリスクが発生する。さらに、合意メカニズムも様々だ。例えば、あまり例は多くないが、51%の検証者がトランザクションを承認した場合には、トランザクションを有効なものとして受け入れる合意メカニズムもある。その場合、もし検証者の集団がノードの51%をコントロールできるようになれば、彼らだけで共同で元帳を管理できるようになる。
- この技術はインターネット接続に依存している。
- プルーフ・オブ・ワークプロトコルを使用する**ブロックチェーン**など、一部のブロックチェーンは、代替技術よりもはるかに多くの電力を消費する。[332]
- 個人は、情報通知を通じて**個人データ**の取扱いについて通知されなければならず、又、**個人データ**に関する権利（削除、訂正および**同意**の撤回等）を行使できなければならない。
- プライベートの許可型**ブロックチェーン**は、限られた数の参加者しか関与しないため、一部の種類の人道的プログラム（**現金給付プログラム**など）にはより適切であろう。しかし、これは場合によっては、信頼できる当事者の再導入とそれに伴った透明性の低下につながる可能性がある。
- 法的管轄区域毎に異なるデータ保護要件に対する適合性が懸念事項となる（下記参照）。
- **ブロックチェーン**技術は、多くの状況で透明性の向上に役立つが、いわゆる「不良データ」を引き起こす根本的な問題を解決するものではない。つまり、信頼性の低いレコードが**ブロックチェーン**に格納されると、そのレコードの信頼性は低いままであり、システムの潜在的なメリットが発揮できなくなる。[333]

---

330 Pisa and Juden、2017年、p.9

331 ただし、本技術の他の特徴が、攻撃を受けやすくしている可能性がある（以下の課題、およびデータセキュリティに関するセクション5.4を参照）

332 Bacon ***et al.***、2018年、p.15

333 Pisa and Juden、2017年、p.49

ブロックチェーンのこれらの利点と課題は、その使用に大きな影響を与えてきた。**ブロックチェーン**は、暗号資産などの資産の所有や保管、またはその責任を記録する取引履歴を管理するために頻繁に使用されている。又、タイムスタンプを公証したり、サプライチェーン、デジタル資格情報、その他の文書にタイムスタンプを付与するためにも、又、契約の条件を強制するためにも使用されている（スマート・コントラクトの利用を通じて）。[334]

14.1.4 人道支援における使用例

人道団体は、**ブロックチェーン**の応用の可能性を模索し始め、この技術を使ったパイロット・プロジェクトを開始した。[335]**ブロックチェーン**技術がそのような場合にもたらすメリットとリスクについて入手可能な情報はほとんどないが、**人道団体**の間では以下のような利用法がいくつか提案されている。[336]

- **現金給付プログラム（Cash Transfer Programming：CTP）：**[337] **ブロックチェーン**は、安全で構造化されたトランザクション記録管理システムにより、CTPの効率を向上させることができる。その結果、透明性が向上し、システムに格納されたデータが改ざんされていないことが多重に保証される。CTPに対する**ブロックチェーン**技術の適用は、**人道団体**がデジタル現金支払いをより安く、より効率的で追跡可能にし、複数の組織間で相互運用可能にすることを可能にする。さらに、**ブロックチェーン**技術は、運用上の耐障害性を提供し、単一障害点や侵害点がないと言われているため、取引をより安全にすることができる（**ブロックチェーン**とセキュリティの詳細については、後述のセクション5.4参照）。
- **ロジスティクスの最適化とトラッキング：**人道支援のサプライチェーンは非常に複雑で動的であり、適切に監視することが困難である。**ブロックチェーン**技術は、これらの業務に透明性を導入する方法となることが考えられる。例えば、医薬品の供給の場合、供給品が倉庫を出た時点、原産国から輸送された時点、目的国に到着した時点、**人道団体**の地方支部によって受け取られた時点、目的病院に到着した時点を示す、ほぼ変更不能のタイムスタンプ付きの記録が**ブロックチェーン**に含まれる場合がある。パブリック・**ブロックチェーン**は、一般に公開される元帳を提供するため、人道物資の出所、使用、目的地を追跡する透明なデータ・プラットフォームとして機能することができる。

---

334 スマート・コントラクトは本章で扱わないブロックチェーンの機能である。スマート・コントラクトの詳細については、M. Finck、“Smart Contracts as a Form of Solely Automated Processing Under the GDPR”、*Max Planck Institute for Innovation & Competition Research Paper No. 19-01*、2019年：https://ssrn.com/abstract=3311370またはhttp://dx.doi.org/10.2139/ssrn.3311370を参照

335 人道セクターにおけるブロックチェーンの使用に関する詳細については、G.Coppi and L.Fast、*Blockchain and distributed ledger technologies in the humanitarian sector*、HPG Comissioned Report、2019年：https://www.odi.org/sites/odi.org.uk/files/resource-documents/12605.pdfを参照。

336 Ko and Verityから抜粋した例、2016年

337 例えば、国際赤十字・赤新月社連盟（IFRC）、*Learning Review: Blockchain Open Loop Cash Transfer Pilot Project*、IFRC、2018：https://www.alnap.org/help-library/blockchain-open-loop-cash-transfer-pilot-projectを参照

- **寄付提供者の資金調達の追跡：**ピアツーピア追跡と寄付の監視は、従来の「中間業者」[338]（または信頼できる第三者）を排除した財務モデルの規模拡大を可能にするかもしれない。[339] このようなモデルは、国際的な人道支援の資金調達に関連する取引コストを削減し、一般市民からのものを含む寄付の追跡を改善することができる。しかし、**ブロックチェーン**の技術は、匿名で寄付をすることにも使うことができる。これは寄付者の身元確認を義務付けるなどと、資金調達ポリシーが厳格化されるので**人道団体**にとって課題となる場合がある。
- **紛争における共通の状況認識の強化：**ホワイトフラグ議定書[340]（ICRCが協力した内容）は、紛争に関与する全ての当事者に中立的なコミュニケーション手段を提供することを目的としている。ホワイトフラグは、緊急事態、局地的な危険性、地雷、人口移動、その他の問題に関するリアルタイムの情報を、悪意ある者によって改変されていないことを知った上で共有できるメッセージングシステムを実現することを目的としている。この構成では、参加者は互いに信頼する必要はない。しかし、この情報が公開されると、民間人の居場所を突き止め、攻撃に際して区別と均衡性を評価するのに役立つかもしれない一方で、特定された集団を標的にすることにも利用できてしまう。

例：

ブロックチェーン・オープン・ループ現金給付パイロット・プロジェクト341では、IFRCとケニア赤十字社は、干ばつの被害を受けた世帯の受益者に対して行われた現金ベースの給付を記録するためにブロックチェーンを使用した。このパイロットの構想は、CTPにおける**ブロックチェーン**の利用と付加価値を調査することであり、給付そのものは地域の移動体通信プロバイダと情報管理会社との従来のパートナーシップを通じて、**ブロックチェーン**から独立して行われた。しかし、プライベートで許可型の**ブロックチェーン**を使用することで、取引をほぼ変更不能かつ分散的に記録することが可能になり、それによって当事者間の透明性が増し（当時者のみが**ブロックチェーン**へのアクセスが許可されたため）、監査証跡が作成され（レコードは改ざんされないことが保証されたため）、記録のセキュリティが強化された（単一障害点や侵害点がないため）。

このプロジェクトでは、2つの重要な課題が発生した。第一に、誤って支払いを要求し、取引を組み戻す必要が生じた場合など、レコードの変更が困難だったことである。第二に、受益者は**同意**がなければ援助を受けることができなかったため、そのような**同意**が自由に提供され、かつ、十分な情報が告知されていたかには疑問があった。[342]

338 Ko and Verity、2016年、p.13
339 Finck、2018年、p.18
340 プロジェクトホームページ：https://www.whiteflagprotocol.net
341 国際赤十字・赤新月社連盟（IFRC）、*Learning Review: Blockchain Open Loop Cash Transfer Pilot Project*, IFRC, 2018年：https://www.alnap.org/help-library/blockchain-open-loop-cash-transfer-pilot-project
342 セクション3.2：同意参照

14.2 データ保護影響評価

人道的プログラムにおける**ブロックチェーン**の使用は、必ずしも他の状況では起こらない多くのデータ保護の課題をもたらす可能性がある。これが、**ブロックチェーン**・システムの導入を決定する前に**データ保護影響評価**（DPIA）を実施することが重要である主な理由の一つである。DPIAは、そのようなシステムを配備することが必要かつ相応であるかどうかを特定するのに役立つ。人道団体が**ブロックチェーン**・システムの導入を決定した場合、DPIAは、**ブロックチェーン**の使用に関連するリスクと課題を特定し、対処し、軽減するのにも役立つ。DPIA実施のためのテンプレートや資料はたくさんあるが[343]、今のところ、人道支援における**ブロックチェーン**に特化して作成されたものはない。従って、人道団体は既存のDPIAモデルを適応させるか、**ブロックチェーン**固有のモデルを作成する必要がある。[344]

DPIAは、**個人データ**の**処理**に関する一般的な質問と、特定の種類の技術（この例では、**ブロックチェーン**）の使用に関する質問の両方をカバーする体系的かつ適応的なプロセスである。本章の別のところで論じたように、**ブロックチェーン**は**人道団体**にとって利点と課題の両方を提示している。メリットがあるとされているにもかかわらず、ほとんどの場合、実際に改善が認められた例は記録されていない。したがって、DPIAの過程で、**人道団体**は**ブロックチェーン**の利用に伴うメリット、課題、リスクを明確に特定し、他の技術と比較すべきである。このアプローチは新しいものではないが、**ブロックチェーン**のような新しいテクノロジーにとっては特に重要である。

ブロックチェーンにはさまざまな形態があるため、DPIAは個々の利用に合わせたガバナンスと設計も考慮して検討しなければならない。利用可能な用途の多様性と**ブロックチェーン**の技術的複雑性のために、**人道団体**は、**ブロックチェーン**技術を実施するかどうか、実施する場合はどのような保護を実施すべきかを決定するのに役立つ意思決定の枠組みを開発することも考えられる。一部の学者は、**ブロックチェーン**を実施するための一般的な意思決定フレームワークを提案している。[345]しかし、これらの汎用テンプレートは、**ブロックチェーン**が人道的活動セクターで提起しているデータ保護に関する懸念を考慮に入れていない。このため、代替の、**ブロックチェーン**固有の意思決定枠組みを本章附録に示す。

DPIAの実施は、**ブロックチェーン**を使用するための適切な法的根拠を特定するためにも不可欠である。DPIAプロセスは、特定の種類の**ブロックチェーン**（すなわち、与えられた状況で

343 例えば、フランスデータ保護局（CNIL）、“Guidelines on DPIA”、2017年10月18日：https://www.cnil.fr/en/guidelines-dpia、情報コミッショナー事務局（ICO）、***Sample DPIA template***、2018年：https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx?mc_phishing_protection_id=28047-br1tehqdu81eaoar3q10を参照

344 DPIAモデルとその設計の詳細については、第5章を参照

345 K. Wüst and A. Gervais、***Do you need a Blockchain?***、Crypto Valley Conference on Blockchain Technology（CVCBT）、2018年で発表された論文：https://eprint.iacr.org/2017/375.pdf

想定されるもの）が**データ主体**の権利への影響及びデータ保護の原則の適用に与える影響を考慮すべきである。この評価に基づき、**人道団体**は、潜在的なリスクを最小限に抑えるための最善の解決策を選択することができる。

DPIAは、データ**処理**の比例性という観点から、**ブロックチェーン**がもたらす影響を明確に示すべきである。この評価に基づいて、**人道団体**は、受益者への危険度を少なくしてそのニーズを満たすことができる、従来のデータベースのような、ブロックチェーンよりも各方面に影響を与えない手段がないかどうかを判断する立場にある。

DPIAプロセスは、システムの技術設計を評価するだけでなく、以下のセクション3からセクション7に詳述する問題と原則も考慮すべきである。

14.3 データ保護バイ・デザインおよび初期設定におけるデータ保護

データ保護バイ・デザインおよび初期設定におけるデータ保護には、最初から主要なデータ保護原則を実施し、**データ主体**に可能な限り最大限のデータ保護を提供する方法で、**処理**作業、プログラム、またはソリューションを設計することが含まれる。この意味で重要なデータ保護の原則は次のとおりである。

- 適法性・公正性・透明性
- 目的制限
- データ最小化
- 正確さ
- ストレージの制限（限定保有）
- 完全性と機密性（セキュリティ）
- 説明責任
- **データ主体**の権利の設計支援

これらの原則の一般的な説明については、第2章を参照。これらの原則のいくつかは、以下のセクションで状況に照らし合わせて説明する。

この段階では、さまざまな種類の**ブロックチェーン**を考慮することが重要である。データ保護の原則に準拠したモデルを設計する場合は、全ての選択肢を考慮する必要があるからだ。

プライベートで許可型の**ブロックチェーン**（定義についてはセクション1.2を参照）は、**ブロックチェーン**内の情報を検証する権限と誰が元帳上のデータにアクセスできるユーザーかを定義する権限を、一つまたは複数の関係者に与えるため、最大の制限が課せられるタイプである。そのため、

データ保護原則と互換性のある方法でプライベートで許可型の**ブロックチェーン**を設計する方が、簡単かもしれない。[346]しかし、参加者の権利を制限することは、場合によっては、「信頼できる当事者」を再導入することとなり、又、潜在的に単一障害点または侵害点を再導入することにもつながり、ブロックチェーン技術の目的そのものを損なうおそれがある。

パブリックな**ブロックチェーン**は、常に、**個人データ**を保管しないように設計される必要がある（これは、プライベートな元帳であっても、常に好ましい選択肢である）。**個人データ**は、「チェーン外」（すなわち元帳の外側）に保存することもできる。ここで、公開台帳には、特定の文書や情報が別の場所（例えば**人道団体**のサーバーに）に保管されていることを確認するための暗号ポインタが含まれているにすぎなく、[347]データ自体は**ブロックチェーン**に保持されていない。しかし、この設計であっても、**ブロックチェーン**に含まれる個人が所有する公開鍵は**個人データ**であることを覚えておくことが重要である。暗号化ポインタも**個人データ**に該当するかどうかは、議論の余地がある。[348]

14.4 データ管理者とデータ処理者の関係

ブロックチェーンには、分散元帳として、広範囲の団体や主体が関与する場合がある。したがって、どの当事者を**データ管理者**および**データ処理者**として扱うべきかを確認することが困難になる。説明のために、それぞれの役割を以下に示す。

- **データ管理者**は、**処理**の手段および目的を決定する。彼らは**個人データ**の取扱いについて説明責任を負い、**データ主体**の権利を行使する責任を負う。データ管理者はデータ保護の原則を遵守し、アクセス、訂正、削除に関する権利を行使する個人の要求に対応する必要がある。**ブロックチェーン**内に複数のデータ管理者がいる場合、または**データ管理者**たりうる新規ユーザーが**ブロックチェーン**に参加していると考えられる場合、それぞれの責任は、書面による合意書に記載されるべきである。
- **データ処理者**は、データ管理者の指示に従い、データセキュリティを確保する責任を負う。又、データ管理者に対し、データを処理するためにどの手段が使用されているか、およびデータの完全性、機密性および可用性に関して生じる可能性のある問題または苦情についても知らせるべきである。

346 M. Finck, ***Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?***、STUDY: Panel for the Future of Science and Technology、European Parliamentary Research Service (EPRS)、2019 年、p.1：https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445EN.pdf

347 暗号化ポインタ（ハッシュポインタとも呼ばれる）は、任意の入力（メッセージや文書）を固定長の文字と数字の組み合わせに一方向で数学的に変換するもの（出力）。特定の入力がハッシュされるたびに出力は同じになるが、入力にわずかな変更（例：カンマの追加または削除）を加えると、まったく異なるハッシュ（Pisa and Juden、2017年）が生成される。したがって、ブロックチェーンにハッシュポインタを追加すると、ドキュメントが格納されていることを確認できる。これは、ドキュメントを再度ハッシュすると、元帳に含まれているポインタと同じポインタが生成されるためである。

348 Finck、2019年、p.30

各**ブロックチェーン**・アーキテクチャは、（セクション1.2に記載の通り）元帳を操作する様々な主体が果たす役割を決定する際に、それぞれ異なる意味合いを有することがある。重要なことは、**データ管理者**の識別にあたって、**処理**の目的を決定することが処理の手段を選択することよりも重要な要素であることである。このことを念頭に置き、**ブロックチェーン**の主要な関係者を見て、次のような構成を検討することができる。

- 許可型の**ブロックチェーン**では、中心的な当事者（または仲介者）が**データ管理者**（たとえば、「書き込み」権限を付与するシステム・オペレータ）となり、従ってノードが適格な**データ処理者**になると位置づけることが可能である。
- 許可型でない**ブロックチェーン**では、ネットワークはすべてのノードによって分散的に運用されるため、中心的な仲介者は存在しない。ここでは全てのノードがチェーンに参加してその目的を追求するかどうかを自律的に決定できるため、潜在的に**データ管理者**として適格である可能性がある。[349]しかし、この結論は全面的に同意されているものではない。
- ノードが**ブロックチェーン**・ネットワークに参加することは**処理**の目的を決定することに等しいと考えられるため、ノードは**データ管理者**であると主張する人もいる。[350]ノードは**データ管理者**ではないという主張もある。[351]又、暗号化されたデータのみを参照するノードもあり、それらは元帳の変更が許可されてないソフトウェアプログラムを実行することにも注意する必要がある。そのようなノードは、**個人データ**を含むどのデータが処理されているかを「見る」ことができず、データに変更を加えることもできず、したがって、**データ管理者**のデータ保護義務を遵守することができない。
- 一方、ユーザー（**ブロックチェーン**の使用を決定する組織や個人）は、**処理**の目的（すなわち、特定の情報を**ブロックチェーン**に記録すること）を明確に決定するので、状況によっては**データ管理者**として適格である。[352]しかも、ユーザーは、**ブロックチェーン**の特定のバージョンを選択するときに、処理方法を選択する。しかし、この解釈は全ての種類の**ブロックチェーン**に適用されるわけではない。パブリックで許可ベースでない**ブロックチェーン**の場合には該当する場合があるものの、プライベートで許可ベースの**ブロックチェーン**では、複数の組織の共同体によって設立される可能性が高く、その場合、共同体が共同**データ管理者**として適格である。

349 Finck、2018年、pp.26–27
350 Finck、2018年、p.26
351 J.Bacon ***et al.***, ***Blockchain Demystified***、Queen Mary School of Law Legal Studies Research Paper No.268/2017, 2017, pp.64-65: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218
352 Bacon ***et al.***、2017年、p.64

フランス共和国データ保護当局（CNIL）は、この問題に関するガイダンスの提供を試みている。CNILによると：[353]

- 「書き込み」権限を持つブロックチェーン参加者は、入力したデータが専門的な活動に関連している場合、**データ管理者**と見なされる。
- **ブロックチェーン**にデータを「書き込む」法人は、**データ管理者**とみなされる。
- **ブロックチェーン**にデータを追加せず、（コンセンサスプロトコルに参加することによって）データの信憑性のみを検証するマイナー（またはノード）は、**処理**の手段と目的を定義しないため、データ管理者ではない。代わりに、データ管理者の指示に従って動作する**データ処理者**と見なすことができる。
- 一方、**ブロックチェーン**ユーザーは2つのタイプに分けられる。
  - 商業的または専門的な目的で**ブロックチェーン**を使用するユーザーは、**データ管理者**として適格である。
  - 個人的な目的で元帳を使用するユーザーは、ほとんどのデータ保護法の範囲外にある純粋に個人的な活動とみなされるため、**データ管理者**として適格ではない。

この問題に関する様々な解釈とガイダンスを考慮すると、**ブロックチェーン**技術を使用しようとする**人道団体**は、選択されたソリューションのガバナンスに**データ管理者**と**データ処理者**の概念が組み込まれていることを保証しなければならない。彼らは又、可能な限り明確に、各処理業務内の各当事者の責任を決定しなければならない。特定の状況において、データ管理者がその義務（特に**データ主体**の権利行使を可能にすること）を果たすことが不可能である可能性があることが明らかになった場合、**ブロックチェーン**の使用はデータ保護原則と両立しない可能性が高いため、代替的な解決策を探すべきである。

14.5 データ保護の基本原則

上で説明したように、**ブロックチェーン**の使用をデータ保護の基本原則と調和させることは、困難な場合がある。実際には、この2つの間の互換性は、各**ブロックチェーン**ソリューションのアーキテクチャおよび設計に依存する。このセクションでは一般的なガイダンスを提供するが、データ保護の原則との互換性を評価する際には、各適用事案の具体的な特徴を考慮する必要がある。

353 CNIL、*BLOCKCHAIN: Solutions for a responsible use of the blockchain in context of personal data*、CNIL、2018年：https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

14.5.1 データの最小化

その性質上、分散された元帳は、処理の趣旨と目的を達成するための最小量の**個人データ**を処理すべきであると宣言されているデータ最小化の原則に反するように思われる。[354]
これは主に、**ブロックチェーン**内のデータが永続的に格納される可能性があり、および元帳全体のコピーが多数のデバイス上の複数のノードに格納されているためである。ただし、回避策がある場合もある。**個人データ**を**ブロックチェーン**外に保管して、元帳は、異なる場所に保管されているデータへの暗号化ポインタのみを保持することができる。この場合、データが元帳に永続的に格納されたり、全てのノードで共有されたりすることはない。データを保管する個人または組織は、データを完全に管理できるため、元帳自体を変更することなく、データ最小化の原則をデータのオフチェーン**処理**に適用できる。暗号化ポインタが**個人データ**にも該当するかどうかは、まだ議論の余地がある。[355]

14.5.2 データ保全

ブロックチェーンが変更不能の分散型台帳であると主張されているという事実も、データ保全の原則に対する問題を提起している。[356]**ブロックチェーン**に格納されたデータは、複数のコンピュータ上で特定できない期間保持される。したがって、最善の解決策は、**ブロックチェーン**上に**個人データ**を保管しないことである。公開台帳のような種類の**ブロックチェーン**には誰でもアクセス（または読み取り）できるため、例えば、**個人データ**などは公開台帳に格納してはならない。特に、民族性や健康記録など、特に機微性の高い**個人データ**は、**ブロックチェーン**に決して格納してはいけない。

14.5.3 比例性

相応性は、データ保護のコアとなる原則である。一般に、**個人データ**の**処理**に関連する特定の行為または措置が、その追求する目的に適切であるかどうかを検討する必要がある。比例性は、選択肢を設定し、**データ主体**の権利に関して最も影響の少ないものを選択する考え方である。**ブロックチェーン**の複雑さは、特定の形態が妥当かどうかを判断することを困難にする場合がある。

データ最小化とデータ保全の原則と同様に、パブリックで許可型ではない**ブロックチェーン**における相応性の懸念に対処する一つの方法は、**個人データ**をチェーンの外で保管することである。しかし、オフチェーンデータベースを追加するということは、データを保存するクラウドサービスプロバイダのような信頼できる第三者を再導入することを意味する。これは、そもそも**ブロックチェー**

354 例えば、EUの一般データ保護規則（GDPR）第5条第1項(c)および（e）に基づき、個人データは「その個人データが取扱われる目的との関係において、十分であり、関連性があり、かつ、必要のあるものに限定されなければならない」、および「その個人データが取扱われる目的のために必要な期間だけ、データ主体の識別を許容する方式が維持 されるべきである」。
355 Finck、2019年、p.30
356 セクション2.7：データ保全参照

ンを使うことがもたらすメリットを否定することかもしれない。しかし、**ブロックチェーン**の特性が想定された目的を達成するために不可欠である場合（例えば、既存のソリューションの完全性、透明性、可用性を改善する要請がある場合）、およびその目的が集中データベースモデルで達成できない場合（例えば、当事者同士が互いに信頼し合っていないため）には、相応性の条件が満たされる可能性がある。しかし、**データ主体**に対するリスクは、追求される目的と比較して不釣り合いに高いものであってはならない。

14.5.4 データセキュリティ

データセキュリティは、効果的なデータ保護システムの重要な側面である。[357]セキュリティは、多くの場合、次の3つの主要な原則に関連している。

- **機密性**：許可された者のみがデータにアクセスできること
- **完全性**：許可されていない第三者がデータを変更できないこと、およびデータが失われたり、破壊されたり、破損したりしてはならない
- **可用性**：**必要な時にデータが**（権限のある当事者によって）使用可能であること

ブロックチェーンには、これら3つの側面のセキュリティに関して、長所と短所の両方の要素がある。次に、これらの詳細について説明する。

機密性の問題に関して言えば、**ブロックチェーン**の分散性には、その性質上、あるデータが複製され、広く分散される潜在性がある。これにより、アクセスポイントと脆弱性が増加する。さらに、**ブロックチェーン**・システムが複雑な暗号化およびハッシュ化技術を使用している場合でも、量子コンピューティングの進歩により、復号鍵を使用せずに情報を復号できる可能性もある。将来、暗号化によってデータの安全性と匿名性が保証されなくなった場合、パブリックな**ブロックチェーン**に格納されている全ての**個人データ**が漏洩する可能性がある。又、ほとんどの場合、**ブロックチェーン**に格納されているデータは消去できないため、損傷は不可逆となる可能性がある。これは、**ブロックチェーン**自体での**個人データ**保管が推奨されないもう一つの理由である。

完全性に関しては、**ブロックチェーン**技術の変更不能性とコンセンサスプロトコルの使用は、一元化されたデータベースよりもセキュリティ上のメリットを提供するが、その理由は少なからず「一元化されたサーバーに機密データを保管することはハッキングを試みる犯罪者にとって『ハニーポット』となり、単一障害点となる」ことにある。[358]しかし、**ブロックチェーン**では、単一障害点や侵害点はなく、攻撃者がコンセンサスプロトコルを制御するのに十分な数のノードを制御できるようにならない限り、システムが侵害されることはほとんどない。

357 セクション2.8：データセキュリティと処理のセキュリティ参照
358 Pisa and Juden、2017年、p.6

可用性の問題に関しても、**ブロックチェーン**は複数のコンピュータに同時に格納される分散元帳から構成されるため、有益である。

単一障害点や侵害点に対する耐性は、**ブロックチェーン**のセキュリティに関連する主な付加価値であるとよく言われる。これが組織にとって必須でない場合は、従来の非**ブロックチェーン**・テクノロジーの方が効率的で高速で安価で、適している可能性がある。
例えば、分散型台帳における暗号化されたデータの保護を強化すると言われている秘密共有技術は、伝統的なデータベースでも使用することができ、**ブロックチェーン**に限って使われる技術ではない。このテクノロジーは、完全性と可用性が重要な要素で、参加者が互いに信頼し合っていない場合に付加価値をもたらす。

14.6 データ主体の権利

データ主体は、自らの**個人データ**の管理を可能にする一定の権利を有する。しかし、以下に説明するように、**ブロックチェーン**上でこれらの権利を実行することは、技術的に非常に困難または不可能である可能性がある。

14.6.1 アクセス権

個人は、自分の**個人データ**が**データ管理者**によって処理されているかどうかを知り、当該**個人データ**のコピーを取得する権利を有する。[359]したがって、人道活動セクターでは、**個人データ**が**ブロックチェーン**に格納される場合、**人道団体**は常に元帳の完全なコピーを保持するノードとして参加する必要がある。これにより、データベース全体が常に利用可能であることを保証し、どのデータが**ブロックチェーン**に格納されているかを受益者に通知できる。

一方、**個人データ**がチェーン外に保存されている場合、元帳にはチェーン外データへのポインタのみが含まれる。そのような場合、最もありそうなシナリオは、人道団体が自らデータを保管し、法的要件に沿って**データ主体**の要請に回答できるようにすることである。

359 セクション2.11：データ主体の権利参照

14.6.2 訂正する権利

データ主体は、自らに関する不正確なデータを修正させる権利を有する。[360]しかし、**ブロックチェーン**では、一旦元帳に加えられたデータを変更することは、不可能ではないものの技術的に非常に困難であるため（「変更不能」という用語の所以）、これは問題となり得る[361]。

個人データがチェーン上に保管されている場合、この権利を維持するための一つの方法は、以前のデータにアクセスできないようにしながら（たとえば、不正なデータにアクセスするために必要な復号化キーを消去するなどして）、新しく修正されたデータを、補足説明としてチェーンに追加することである。しかし、この解決策についての合意は学者と実務者の間ではまだない。

場合によっては、古いデータを修正する必要があることを示す新しいトランザクションを挿入することもできる。ただし、これらの選択肢の問題は、元のデータを修正するのではなく、チェーンにデータを追加するだけであることである。これが訂正として受け入れられるかどうかは不明である。

これらの制限を考慮すると、これらの課題に対処する最良の方法は、**個人データ**をオフチェーンに保管することであり、そうすれば元帳自体を変更することなく訂正することができる。この選択肢を使用すると、前述の**ブロックチェーン**の完全性と可用性の利点が大幅に低下することに注意を要する。言い換えれば、完全性と可用性も**個人データ**にとって重要である場合、**ブロックチェーン**・ベースのソリューションは推奨されない。

14.6.3 削除権

ブロックチェーンのほぼ変更不能な性質は、概念的に削除の権利と対立している。[362]この問題に対処するためのさまざまな選択肢が提案されている。前述したように、1つの選択肢は、データがチェーン上に存在していても、チェーン上のデータにアクセスできないようにすることである。これは、例えば、該当する暗号化データの解読に必要な復号鍵を消去することによって達成することができる。しかし、一部の学者や実務者は、該当する**個人データ**は暗号化されているが、（削除権が示唆するように）消去されておらず、単にアクセス不能にされているだけなので、このアプローチは不満足であると主張する。これは、暗号解読技術（上記のデータセキュリティに関する説明を参照）の進歩を考慮すると問題になるかもしれない。

---

360 セクション2.11：データ主体の権利参照

361 D.Conte de Leon ***et al.***、“Blockchain: properties and misconceptions”、***Asia Pacific Journal of Innovation and Entrepreneurship***、Vol.11、No.3、2017 年：https://www.researchgate.net/publication/321811785_Blockchain_properties_and_misconceptions また、DAOのハッキングを修正するためのEthereumハードフォークの例：https://blog.ethereum.org/2016/07/20/hard-fork-completed/

362 Finck、2018年、p.30

チェーン外に保管された**個人データ**は、分散された元帳自体を変更することなくデータ保護要件に沿って修正および消去することができるので、これがこの点に関しても好ましい選択肢になる。

例：
人道団体が**現金給付プログラム**（CTP）に**ブロックチェーン**を使用する場合、**ブロックチェーン**上に「ウォレット（電子財布）」を持つよう受益者に要求する可能性が高い。ウォレットは、公開鍵とほとんど同じように機能する。つまり、それ自体では受益者を識別しないユーザ名と同じようなものである。しかし、人道団体はおそらく、全てのウォレットを特定の受益者に一対一でリンクするオフチェーンのデータベースや受益者管理システムを維持するだろう。

現金が受益者に送金されるたびに、どのウォレットにいつ、いくらが送金されたかを指定するトランザクションが**ブロックチェーン**に追加される。トランザクションは、コンセンサスプロトコルによって検証されると、**ブロックチェーン**に変更不能な形で格納される。受益者が自分のデータを削除することを要請しても、技術的には（公開鍵と同様に**個人データ**となる）ウォレットをチェーンから消去することはできない。この場合の一つの選択肢は、個人を、ウォレットが個人に関連付けられている唯一の場所であるオフチェーンのデータベースまたは管理システムから削除することである。個人プロファイルが削除されれば、ただちに再識別ができなくなる。

14.6.4 データ主体の権利の制限

前述のアクセス、削除および訂正に関する説明は、**ブロックチェーン**・テクノロジーを使用する際にデータ保護の権利を行使することがいかに困難であるかを示している。パブリックで許可ベースでない**ブロックチェーン**を**データ主体**の権利と両立させることはほぼできないため、唯一の解決策は**個人データ**をオフチェーンに保管することだと思われる。しかし、これらの権利は絶対的なものではなく、したがって制限することができる。**データ管理者**は、**データ主体**がその権利を行使することを要求する場合、利用可能な技術および実施の費用を考慮に入れることが許されている。しかし、重要なことは、これらの制限は例外的な場合にのみ許容されるという点である。[363]本ハンドブックの第2章では、**データ主体**の権利が制限される状況を説明し、例示している。合法的な**処理**でデータ主体の権利が必然的に減少する特定の使用事例において、「データ保護に準拠している」**ブロックチェーン**というものがあり得るかどうかについては疑問が残る。特定の権利を制限することが正当であると判断された場合でも、他の全てのデータ保護原則（データの最小化、必要性、相応性、セキュリティなど）は依然として適用される。

363 セクション2.11：データ主体の権利参照

14.7 国際的なデータ共有

ブロックチェーン・アプリケーションで処理されたデータは、日常的に国境を越えて転送されている。特に、誰もがどこからでも参加できる可能性のある、パブリックで許可型でないアーキテクチャではそうである。このことは、データが国際的に共有されている場合の**ブロックチェーン**・アプリケーションにおけるデータ保護について問題を提起する。[364]契約条項やその他の認識されたメカニズムは存在するものの、そのような措置は、**ブロックチェーン**においては、実際的ではないと言える。

適用される法律と管轄を決定することも難題になる可能性がある。本ハンドブックの第4章で予測されているように、適切で的を絞ったリスク分析は、（チェーンに参加できる人々の地理的な位置を制限するプライベートで許可型の**ブロックチェーン**のように）管轄の選択と法の選択が明確に**ブロックチェーン**・ガバナンスに組み込まれていない限り、不可能である。

一部の種類の**ブロックチェーン**では、国際送金が問題になる可能性がある。暗号資産ビットコインで使われているような無制限のパブリックで許可ベースの**ブロックチェーン**がその例であるが、そこでは、誰がシステムに参加して元帳のコピーを保存するかを制御する中央当事者がない。一方、プライベートで許可ベースのものや他のアーキテクチャでは、より強力な制御が可能なので、したがって、そのようなリスクを軽減するのに役立つ。したがって、例えばデータ保護保証を（**ブロックチェーン**・アーキテクチャにハード・コーディングするなどの方法で）組み込むことによって、**ブロックチェーン**・ガバナンスを通じて送金問題の対策を試みることが可能である。

データ管理者は又、データが他の関係者と共有されたり第三国に転送されたりした場合に、**データ主体**に通知する必要がある。これは、限られた例外はあるものの、一般的には、パブリックで許可ベースでない**ブロックチェーン**では不可能である。なぜなら、世界中の誰もがシステムに参加し、元帳のコピーを保管することが可能だからである。しかし、許可ベースの**ブロックチェーン**では、**データ管理者**はより広範囲にわたった制御が可能なため、この要件を遵守することが可能であろう。

付録：人道支援活動におけるブロックチェーンのための意思決定の枠組み

以下の意思決定の枠組みは、人道活動のために**ブロックチェーン**を実装するプロセスのにおいて**人道団体**のガイダンスとなることを意図している。

364 第4章：国際的なデータ共有参照

ステップ 1：
この手順は、新しいテクノロジーの導入に共通であり、**ブロックチェーン**だけに適用されるものではない。最初の情報収集と範囲設定の準備作業で構成されており、次の質問に答えるものである。

- **ブロックチェーン**のソリューションはどのような問題に対処するためのものか
- ブロックチェーンのソリューションはどのプログラムに適用されるのか、又そのプログラムのニーズは何か
- **ブロックチェーン**・システムは、現在直面している問題に対処するために利用可能なテクノロジーの中で、最も侵襲性が低く、リスク回避性が高く、制御可能なものか
- **ブロックチェーン**はどのような場面で機能するか
- ブロックチェーンはどこで機能するか（1つの国または地域で、世界中で）
- ステークホルダーは誰になるか（受益者、地方当局、金融パートナー、移動体通信の事業者、その他の**人道団体**など）
- このテクノロジーの目的は何か（内部効率の向上、ポジショニングの改善、既存のプログラムの拡大、寄付者の要求事項への対応、リスクの管理など）
- 現在のガバナンス体制とIT能力はどのようなものか、現在の体制と能力の下で、技術を導入し、関連するリスクを管理することができるか
- ブロックチェーンの技術が地域の情報エコシステムにどのように貢献するかが明確になっているか

ステップ 2：
ブロックチェーンの技術が実施される特定の状況において、上述のように技術に関連する利点と課題を考慮しつつ、ブロックチェーン・ベースのシステムが人道的プログラムやその他のイニシアティブの目的を達成するために必要かどうかを決定する。人道団体は、そのニーズが何であるか、**ブロックチェーン**がそれらのニーズを満たすかどうか、データ主体がシステムを通じてどのような体験をするか、**データ主体**の権利がどのように尊重されるか、**データ主体**とその権利をよりよく保護する別のシステムによって同じニーズを満たすことができるかどうかを理解するよう努めるべきである。次のような問いかけをするべきだろう。

- トランザクションや行為の順序は重要か
- 信頼できる中央当局は存在するか
- データを保管する必要はあるか
- ガバナンス/ITサポートチームの賛同はあるか
- 人道団体のシステムが地域の情報エコシステムにどのように貢献するかを理解しているか

ステップ 3：
人道団体が目標を達成するには**ブロックチェーン**のソリューションだけしかないと判断した場合は、どの種類の**ブロックチェーン**のソリューションが最適か、または必要かを判断する必要がある。次のような質問をすべきだろう。

- 貢献者は複数いるか
- 「常時オンライン」の信頼できる第三者（TTP）を利用できるか
- 全ての貢献者は既知の存在か
- 全ての貢献者は信頼されているか
- 公的な検証能力が必要か

ステップ 4：
DPO、ITサポート、および同僚と相談する。

- 指導を求める。
- 他人の経験を生かす。たとえば、同じようなシステムを開発している同僚や、使用する予定の既製のソリューションを使用している同僚に相談し、**ブロックチェーン**の専門家にアドバイスを求めよう。

ステップ 5：
個人データ処理の影響を特定し評価するためにDPIAを実施する。DPIAには次のような質問を含める必要がある。

- 適用法律は何になるか、全ての利害関係者に適用されるか
- どのような種類の**個人データ**が処理されるか、**ブロックチェーン**に格納されるトランザクションに必要な種類のデータはどれか
- **処理**は公正、適法かつ透明であるか
- **ブロックチェーン**自体に**個人データ**を保管することに代わる方法は何か、オフチェーンの保管は可能か
- **データ主体**はその権利を完全に行使できるか、そうでない場合、課されている制限は適法かつ相応なものか
- **ブロックチェーン**のガバナンスを決定する権限を持つのは誰か
- プラットフォームはどのように運営されるか
- 誰がプラットフォームを変更でき、どのような状況で元帳のエントリを更新できるか
- 選択された技術がもたらすリスクは何か、それぞれのリスクはどのように対応され、緩和されるのだろうか
- 個人はどのようにして権利を行使できるのか

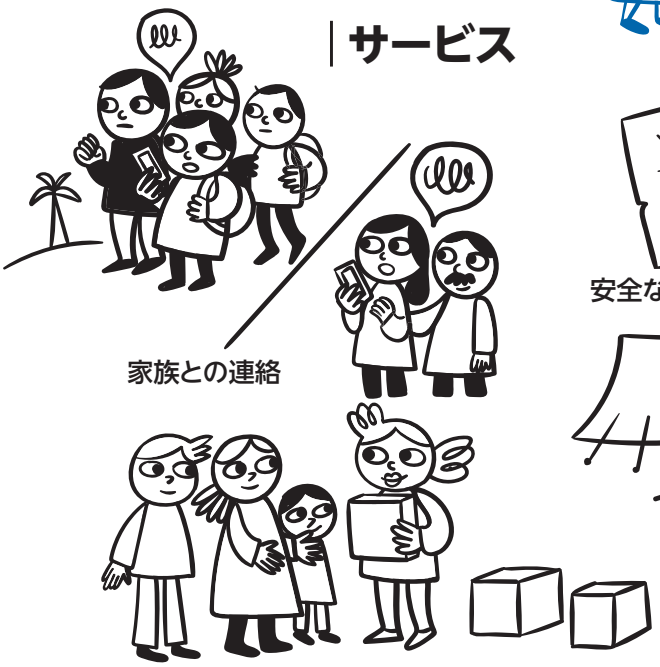
ステップ 6：

データ保護バイ・デザインおよび初期設定におけるデータ保護の原則を実装する。

- 両原則には、以下の事項 – 利用可能な技術、実施費用、**処理**の性質、範囲および文脈、**処理**の目的、**処理**によってもたらされる（さまざまな可能性と重大度の）自然人の権利および自由に対するリスク – を考慮し、継続的監視並びに技術的および組織的措置の見直しが必要になる。使用される技術または収集されるデータの種類に上記事項に関連する変更がある場合は、常に新たなDPIAが実施されるべきである。
- 意図的に提供するデータ保護では、次のような要素を考慮する。
  - データ保護原則の遵守（適法性、公平性と透明性、目的制限、データ最小化、正確性、保管制限、完全性、機密性）
  - **データ主体**の権利（例：通知、アクセス、削除、訂正）
  - その他のデータ保護義務（例：説明責任とセキュリティ）
- 既定で提供するデータ保護には、次のような要因を考慮する必要がある。
  - 処理する**個人データ**の種類とカテゴリ
  - 処理される**個人データ**の量
  - 処理目的
  - 保管期間
  - アクセス

利用可能性

サービス



課題

第15章

援助としての接続性[365]

365 この章への貢献に対し、Robert Riemann氏（欧州データ保護監督官）とJohn Warnes氏（UNHCR）、Antonella Napolitano氏、Ed Geraghty氏（プライバシー・インターナショナル）に感謝の意を表する。

15.1 はじめに

緊急時に接続性を維持することにより、受益者が離散した家族と連絡を取り合い、安全な避難ルートを計画し、避難所を見つけ、**人道団体**と関わり、人道支援やその他のサービスにアクセスするのを支援することができる。しかし、災害後には、接続性[366]をもたらす電気通信ネットワークが機能を停止するのはよくあることで、被災者の依存度が増している通信経路を奪うことにつながっている。観測では、受益者は接続性をかなり重視している様子が見られる。例えば、2016年にギリシャで移民を支援している援助団体職員は、受益者が食料や水よりも先に、インターネットへのアクセスを要求することが多かったと報告している。[367]**人道団体**は接続性の重要性を認識し、それに応じて一連のプログラムを策定した。

援助としての接続性と援助のための接続性を区別することが重要である。後者は、援助従事者が自らの仕事を遂行できるように援助従事者に接続性を提供することを指す。一方、前者は、緊急時や長期にわたる危機の際に、被災者に接続性を提供し、援助の一つの形態として関連サービスを提供することを指す。

この章では、援助としての接続性から生じるデータ保護の問題に、コミュニティと個人という2つの異なるレベルから焦点を当てる。コミュニティ・レベルでは、人道組織は通常、ホットスポットを設置したり、コミュニティ・センターにおいて接続性を提供したりしている。このような場合、機関は通常、ユーザ間で共有される「パイプ」（つまり、接続性を提供するために必要なケーブルやファイバー・バンドルなどの物理的インフラ）を管理する。個人レベルでは、**人道団体**は人々が接続性を提供するプロバイダと取引を行うのを支援することができるが、個人が自らの接続性へのアクセスに対してより大きな責任を負うことになる。[368]この2つのレベルの違いは、**人道団体**のデータ保護責任にも影響を及ぼす。

15.1.1 支援介入としての接続性の概要

さまざまなイニシアチブや組織が、緊急時に接続性を提供したり、接続が困難な地域に対処しようと取り組んでいる。次に例を示す。

- **NetHope**[369]は、緊急時のさまざまな環境に応じた接続ソリューションを提供している。USAIDと協力して、同組織は中東、アフリカ（ボツワナ、ガーナ、ケニア、リベリア、ナイジェ

366 本章で「接続性」とは、モバイル機器およびインターネット接続へのアクセスをいう。

367 L. Taylor、”Internet Is As Important As Food And Water To Refugees In Greece: Aid Groups”、ハフポスト、2016年7月22日：https://www.huffpost.com/entry/internet-is-as-important-as-food-and-water-to-refugees-in-greece_n_57928a22e4b02d5d5ed1ac5b

368 例えばUNHCRの難民のためのコネクティビティイニシアチブ、コネクションズ、2019年を参照

369 https://nethope.org

リア、ザンビア）、アジア（カンボジア・インドネシア）、カリブ海諸国（ジャマイカ）の農村部にブロードバンドインターネットを提供している。

- **緊急通信クラスター（ETC）**は、人道危機の際に共用の通信サービスを提供するために協力する組織のグローバルネットワークである。ETCは、機関間常設委員会（IASC）によって指定されている11のクラスターの一つである。[370]
- UNHCRの**難民のためのコネクティビティ**イニシアチブは、国内制度へのインクルージョンを重視する権利に基づくアプローチをとり、避難民や受け入れコミュニティが接続性にアクセスできるよう支援するものである。
- 民間セクターのイニシアチブ：
- **Loon**[371]は、当初はGoogleが主導したイニシアチブで、既存のネットワークでカバーされていない地域にインターネットアクセスをもたらすために電波塔の重要な構成要素を入れた気球を配備することによって、人々をつなぐ取り組みである。プロジェクトの目的は、モバイルネットワーク事業者と提携し、4Gワイヤレスブロードバンド（またはLTE）の到達範囲を拡大することである。
- **Facebook Connectivity**[372]は、世界中に無料のインターネットアクセスを提供することを目的としたFree Basicsや、成層圏通信プラットフォーム（HAPS）接続システムと衛星技術の利用を促進し、遠隔地への接続を低コストで実現するHigh Altitude Connectivityなど、多くのイニシアチブにも関わっている。
- **CISCO Tactical Operations**（TacOp）[373]は、多様なテクノロジーとネットワーク機器を配備して、災害後に**人道団体**と受益者の双方に無料の通信ネットワークを提供している。例えば、2015年にネパールで発生したマグニチュード8.1の地震の際には、Cisco TacOpは現場に72時間以内に到着して通信を再開した。

15.1.2 運営の事情

援助としての接続性プログラムを開始する際には、危機とは複雑な状況であり、影響を受ける状況や人々はそれぞれの危機によって異なるということを覚えておくことが重要である。同様に、接続性プログラムも状況によって異なってくる。将来の自然災害や緊急事態に備えて既存ネットワークのレジリエンスを高めることに重点が置かれるプログラムもあれば、これまでアクセスのなかった地域に接続性を確立することに焦点が当てられるプログラムもある。実際の手はずは必然的に異なるが、支援機関はどのような種類のプログラムを実施しているかにかかわらず、いくつかの共通要素を考慮する必要がある。一つ目は、その機関が何をできるか、何をできないかを決定

370 https://www.etcluster.org/
371 https://loon.com
372 https://connectivity.fb.com
373 https://www.cisco.com/c/m/en_us/never-better/csr.html

する、規制の状況である。二つ目は、その地域で現在接続性を提供している営利および非営利組織である。実際、**人道団体**は、接続ネットワークの一部または全部を通じて民間企業と関わることが多く、そのようなパートナーシップがますます一般的になるにつれて、両セクターの組織は相互に協力する方法についてガイドラインを策定してきた。[374]

他の主体とのパートナーシップ（下記のセクション1.3を参照）を検討する場合、**人道団体**は常にそのようなパートナーシップのリスクを評価することが推奨される。そのための方法のひとつとして、少なくとも部分的なものとして、**データ保護影響評価**（DPIA）がある。これは、データ保護の問題（下記のセクション2を参照）を超えて、パートナーシップが被災者に害を及ぼさないことを確認するための作業である。

15.1.3 複数のステークホルダーとパートナーシップ

人道団体は、接続性プログラムを単独で実施するために必要な専門知識、技術、設備を持たない場合がある。つまり、目標を達成するためには、1者もしくは複数の接続性または技術を提供するプロバイダと提携する必要がある。これには、非営利団体、民間企業（通信事業者や技術系企業など）、および緊急時に接続ソリューションを提供するNGOが含まれる。

他の関係当事者を検討するだけでなく、接続性の提供が階層化されたプロセスであることを理解することも重要である。前述したように、コミュニティと個人という2つの異なるレベルがある。個人レベルでは、接続事業者が個人から直接データを収集する可能性があるため、受益者は自らの接続に対してより大きな責任を負う。

一旦接続が確立されると、例えば電話契約の上で作動するソーシャルメディアサービス、お財布携帯またはモバイル・マネーなど、追加の（いわゆる「オーバー・ザ・トップ」）サービスが利用できるようになる。これらのサービス提供者の中には、援助を受ける受益者に直接製品を販売する者もいる。ここで、受益者は技術的には消費者として行動しているが、実際には平均的な消費者よりも脆弱である。また、インフラのプロバイダや、**人道団体**やサービスプロバイダに接続性をもたらすためのバックホールに関わる者（帯域幅プロバイダなど）のように、接続性プログラムに関与するあまり目に見えない関係者もいる。プロバイダはネットワーク保護の追加レイヤーとしてディープ・パケット・インスペクション（DPI）[375]も追加できる。DPIには、ウイルスやマルウェアなどの不要なパケット（インターネットを介して発信元から宛先に送信されるデータの単位）のフィルタリングが含まれる。しかし、重要なのは、DPIによって特定のパケットを含むコンテンツの発

374 例えば、GSMアソシエーション（GSMA）、「人道接続性憲章」：https://www.gsma.com/mobilefordevelopment/mobile-for-humanitarian-innovation/humanitarian-connectivity-charterを参照

375 ディープ・パケット・インスペクションの詳細については、Tech Target – Search Networking、「ディープ・パケット・インスペクション（DPI）」：https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPIを参照

信元または受信先を識別できることである。つまり、DPIはモニタリングや監視の目的にも使用できるということである。

バックホール、パイプ、オーバー・ザ・トップ、ラストマイル接続など、接続性プログラムのさまざまなレイヤーでオペレーションするこれらの全ての組織および主体が、ユーザのデータを収集したり、ユーザのデータにアクセスできる。これは、追加のデータとメタデータが接続の全てのレイヤーで生成および**処理**されるためである。異なる主体によるこの処理は、技術的に必要である。なぜなら、ある場所から別の場所へメッセージを送るためには、通常、複数の主体がその送信元と宛先を知る必要があるからである。[376]これらのメタデータ（接続エンドポイント、「いいね！」、訪問など）には、接続ネットワークに関わる一部または全ての主体がアクセスできる可能性があり、これら主体は受益者と**人道団体**の両方が想定することが困難な方法で、人道的緊急事態および関係する個人に関する知識を抽出できる可能性がある。[377]

受益者から直接データを収集する接続事業者の例：
国内のモバイルネットワーク事業者は、通常、請求目的で次の情報にアクセスできる。SIMカードや端末固有の識別情報（IMSIおよびIMEI番号）、通話やメッセージなどのトランザクションの時間と場所、SIMカードの登録時に取得したデータである。[378]SIMカードの登録時に取得されるデータは、国や購入したSIMカードの種類（プリペイドまたは後払い）によって大きく異なる。それにもかかわらず、全ての種類のカードについて登録を強制する傾向が一般的にあり、利用者は、IDのコピー、国民識別番号、生年月日などの**個人データ**を提供することが求められる[379]。場合によっては、国民IDデータベースと照合されたり（インド・パキスタン）、指紋や写真を撮らされたりすることもある（例えばナイジェリア）。[380]調査[381]によると多くの場合、難民やその他の強制的に移住させられた人々は、標準的な合法的手段でSIMカードを入手することが難しく、その代わりに公式および非公式の代替策に頼っており、データの流通に関する多くの課題を提示している。

376 赤十字国際委員会（ICRC）およびプライバシー・インターナショナル、The Humanitarian Metadata Problem: “Doing no Harm” in the Digital Era、Privacy International and ICRC、2018年、pp.22–23：https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf

377 ICRC and Privacy International, 2018年、p.23

378 ICRC and Privacy International, 2018年、p.71

379 K.P. Donovan and A.K. Martin、“The rise of African SIM Registration: The emerging dynamics of regulatory change”、First Monday、Vol.19、No.2、2014年：http://firstmonday.org/ojs/index.php/fm/article/view/4351、Breyer v. Germany事件（適用第50001/12号）の欧州人権裁判所（ECHR）判決（2020年1月30日）も参照

380 GSMA、Mandatory registration of prepaid SIM cards: Addressing challenges through best practice、GSMA Public Policy、2016年：https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

381 UNHCR、“Displaced and Disconnected”、2019年：https://www.unhcr.org/innovation/displaced-and-disconnected/

この文脈では、**人道団体**は接続ネットワーク全体を管理することはできず、したがって、個人のデータやメタデータが悪用されないように保護することを保証することはできない。**人道団体**とそのパートナーが、被害を受けるコミュニティの接続性を改善するために積極的な役割を果たす場合には、このような管理の欠如から生じるリスクを、**データ保護影響評価**（下記セクション2を参照）を通じて評価すべきである。対処法として、**人道団体**の中には、被災者にデジタルセキュリティに関する情報とガイダンスを提供しているところもある。[382]しかし、リスクがあまりにも大きいことが判明した場合には、**人道団体**は接続性を提供しないことを選択せざるを得ないこともある。

15.2 データ保護影響評価

データ保護影響評価（DPIA）[383]は、プロジェクト、政策、プログラム、その他のイニシアチブに関連して**個人データ**を**処理**することで、**データ主体**にもたらされるリスクを特定、評価、対処するために実施される。最終的には、データ保護リスクの回避、最小化、移転または共有を促進する措置につなげるべきである。**個人データ**の**処理**を含む技術プログラムを開始する前に、**人道団体**は、パートナーによる受益者データの違法な使用や政府によるネットワークへの干渉など、起こり得る結果を評価するためにDPIAを実施すべきである。

接続性プログラムのためのパートナーシップを結ぶ前に、**人道団体**は、受益者のデータがどのように処理されるかを完全に理解するため、潜在的なパートナーとそのプライバシーポリシー、および彼らに適用される法的義務を評価すべきである。接続性の様相、関係者、および提供するサービスの全体像が明確になったら、機関は、標準ガイドライン、または必要なサービスを説明する要件（技術要件やプライバシー要件など）を作成することができる。これにより、各機関はパートナーと連携し、緊急時における連携から合意までの時間を短縮できる。

また、人道分野においては、受益者が特に脆弱であり、被害のリスクが高いことを忘れてはならない。これらの理由から、DPIAでは**データ主体**の他の基本的権利を十分に考慮すべきである。[384]**人道団体**は、人道原則に従って活動しているので、接続性プログラムを設定する際には、データと関わらない権利を含めて、特定のグループまたはコミュニティの全てのメンバーの権利と自由を考慮することも適切であろう。DPIAは例えば、ネットワークへの不平等なアクセスに関わる問

382 データセキュリティの詳細については、セクション2.8：データセキュリティと処理のセキュリティを参照

383 第5章：データ保護影響評価（DPIAS）を参照

384 EU第29条作業部会、*データ保護影響評価（DPIA）、および処理がEU規則2016/679の目的に照らして「高度のリスクをもたらす可能性」があるかを決定するためのガイドライン*（wp 248 rev.01）、2017年：http://ec.europa.eu/newsroom/document.cfm?doc_id=47711、およびR. Gellert、*"Understanding the notion of risk in the General D ata Protection Regulation"*、Computer Law & Security Review、Vol.43、Issue 2、2018 年：https://doi.org/10.1016/j.clsr.2017.12.003を参照

題[385]や、デジタル情報に精通していない特定のグループが排除される可能性の問題についても評価することができる。また、人道団体と協力しているパートナーの中には、データの金銭化に基づくビジネスモデルを有しているものがあり、人道主義の原則と相容れない可能性があることを考慮することも重要である。また民間部門の中には、パートナーシップを組むことが評判リスクを生むために、機関がパートナーシップを組むことを望まないものもいる。接続性プログラムによって解決できることよりも、引き起こす問題の方が多い可能性をDPIAが示している場合には、関与しないことを決定することが適切であろう。

15.3 データ管理者とデータ処理者の関係

データ管理者は、**個人データ**の**処理**の目的および手段を単独または他者と共同で決定する個人または組織である。一方、**データ処理者**は、**データ管理者**に代わって**個人データ**を処理する個人または組織である。これらの概念については、第2章で詳しく定義、説明している。

人道団体が接続性プログラムを設定し、運営する場合、**人道団体**は、それぞれのプログラムにおける役割や他のパートナーの役割に応じて、**データ管理者**または**データ処理者**となる。この区別は、データ**処理**の責任を割り当てる上で重要である。

データは接続性プログラムの様々なレイヤーで収集されるため、データフローをレイヤーごとにマッピングし、データを収集する者、収集の目的、データ保全の期間、およびデータを共有される相手を確認することが重要である。このマッピングを行うことで、データの処理方法を決定する上で、人道団体を含む各当事者がどのような役割を果たしているのかを特定することができ、またそれによって各当事者が**データ管理者**、**データ処理者**のどちらとして機能しているのかを特定することができる。

人道団体がプログラムの最終目的（接続性の確立など）を決定し、それを実施するために特定のパートナー（手段）を選択する場合、**人道団体**は**データ管理者**となる。これは、機関が、自らの権利[386]を行使しようとする**データ主体**からの要請に応じることを含め、一連の義務を負っていることを意味する。時には人道団体と他セクターのパートナーが共同でプログラムの目的と手段を決定し、共同で**データ管理者**となることがある。このような場合、共同管理者は、**データ主体**の要求への対応を含め、それぞれの責任範囲を定め、書面により合意しなければならない。

385 例えば、幼い子どもや高齢者は、コンピュータリテラシーの欠如によって、接続性プログラムや接続性を必要とするアクセスサービスから恩恵を受けることができないことがある。また、「低・中所得国では、女性の携帯電話所有率は男性より10%低く、より革新的なサービスの利用率はかなり低い。例えば、低・中所得国の女性のモバイル・インターネット利用率は、男性よりも26%低く、またモバイル・マネーの利用率は33%低い。」出典：GSMA、コネクテッド・ウィメン：性別の分析と特定ツールキット—機械学習を用いた利用者性別の推定、GSMA、2018年、p.6：https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/GSMA-Gender-Analysis-and-Identification-Report-GAIT-August-2018.pdf

386 セクション2.11：データ主体の権利を参照

15.4 データ保護の基本原則

15.4.1 個人データ処理の法的根拠

接続性を提供するサービスにアクセスするために**個人データ**が必要な場合、またはその過程で個人データが生成される場合、これらのデータの**処理**のための適切な法的根拠が必要である。このような法的根拠は、本ハンドブックの第3章に挙げており、人道的状況における法的根拠としての**同意**の利用に関連する課題についても説明している。人道的状況においては、**同意**は、自由意思によるものとならない場合がある。特定のサービス（この場合、接続性）を受けるために同意する以外に方法がない場合、受益者が**同意**を強いられていると感じる可能性があるためである。さらに、援助としての接続性を取り巻く複雑さにより、デジタルリテラシーのレベルが低い**データ主体**は**処理**の全ての側面を理解することができない可能性があるため、十分な情報に基づく同意に頼ることも困難な場合がある。そこで、**人道団体**とサービス提供者は、データ収集とデータ**処理**のために、以下に挙げるような別の法的根拠を求めるべきである。

- **公共の利益：**機関が接続性を確立するための特定の権限を持つ場合、これは一つの選択肢になり得る。[387]
- **人道団体の正当な利益：**接続性を確立、または再確立することが機関の使命に沿っている場合、またそうすることで受益者が他の不可欠なサービスにアクセスできるようになり、人道対応に必要な調整を改善できる場合に、この法的根拠を考慮することができる。しかし、この根拠は、機関が追求する利益および**処理**により得られると想定される利益が、当該個人の権利および自由によって優先されない場合にのみ適用される。[388]
- **法的義務：**一部の管轄区域では、接続サービスを利用するためにユーザ登録が必要な場合がある。この場合、登録のためにユーザのデータを処理する法的根拠は、法的義務の遵守となる。[389]

15.4.2 データセキュリティ

モバイルネットワーク事業者は、重要な接続インフラの提供者として重要な役割を果たしている。例えば、緊急事態では、救急車や他の医療提供者と連絡が取れることは、効果的な事故対応に不可欠である。これらの事業者は、通信ネットワークを保護し、取り扱うデータの安全を保持するために、技術的および組織的なセキュリティ対策を実施する必要がある。これらの措置には、リスクの程度に応じて、暗号化および収集されたデータの機密性、完全性および可用性を確保する他の技術的方法、並びに**処理**システムおよびサービスの全体的なレジリエンスなどがある。[390]

---

387 第3章：個人データ処理の法的根拠を参照
388 セクション3.5：正当な利益を参照
389 セクション3.7：法的義務の遵守を参照
390 データセキュリティの詳細については、セクション2.8：データセキュリティと処理のセキュリティを参照

ただし、個々のデバイスに保存されているメタデータの中には、暗号化されておらず、別のセキュリティ対策が必要なものもある。[391]新しいセキュリティ技術の発展を考慮し、個々の**個人データ処理**に伴うリスクの程度に合わせた適切なレベルのデータ保護およびセキュリティを確保するために、**人道団体**および個人は可能な限り、日常的に自らがとる措置を見直し、更新すべきである。一部の団体や組織は、商業的なターゲティングや開拓、調査など、人道以外の目的のために接続性プログラムで生成されたデータやメタデータにアクセスすることに関心を持つ場合があることに留意しておくことが重要である。

例：
ドイツとデンマークは、当局が亡命希望者のスマートフォンの詳細な鑑識分析を行うことを認める法律を可決した。端末から抽出されたデータとメタデータを「難民申請書に記載された申請内容を確認したり、身元、経歴、経路などに関する新たな情報を入手したりする」ために使用可能とした。[392]同様の法律がベルギーで可決され、オーストリアで提案された。[393]実際には、このような法律は、接続性プログラムを通じて得られたデータが、たとえ合法であっても、**人道団体**が遵守する原則にそぐわない目的のために使用される可能性があることを意味する。

現在の調査方法は非常に洗練されており、ネットワークユーザに関するかなりの量のデータおよびメタデータを得ることができる。[394]メタデータは個人が共有することを同意していない情報を推測し、行動を予測するために使用できるので、これは特に懸念すべき事項である。このことは人道支援の過程で得られたデータが、最終的には紛争の際に非常に貴重な情報として利用される可能性があることを意味する。

場合によって**人道団体**は、その任務にもよるが、特定の接続性プログラムに関して、国内または外国の政府当局と協力する必要がある。この種の協力は、医療援助や公衆衛生の提供を促進するために医療データが保健当局と共有される場合のように、受益者の利益になりうる。**人道団体**は、そのような協力の取り決めについて受益者に対して透明性を保つべきであり、そのデータが国内外の当局と共有されることを明確にすべきである。

人道団体は、団体の管理下にない部分も含め、接続ネットワーク全体を通じて最高レベルのセキュリティを確保するために、パートナーとセキュリティ対策について交渉すべきである。

391 ICRC and Privacy International、2018年、p.25
392 ICRC and Privacy International、2018年、p.62
393 ICRC and Privacy International、2018年、p.62
394 例えば、B. Schneier、"China Isn't the Only Problem With 5G"、Foreign Policy、2020年1月10日：https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/ を参照

15.4.3 データ保全

個人データは、収集された目的を達成するため、または適用される法的義務を遵守するために必要な期間を超えて保管してはならない。[395]これは、**個人データ**が不要になった時点で、常に消去または匿名化されるべきであることを意味する。しかし、接続性プログラムでは、様々なパートナーが、データを保全する期間を含むデータの処理方法に影響を与える可能性のある、異なる役割、方針、およびニーズを持つ場合がある。繰り返しになるが、最初に、各関係者の責任とデータ保全ポリシーを記載した契約書を作成することが重要である。これにより、**人道団体**は、特定の時点で各パートナーがどのようなデータを保持し、どこにデータが保存されているかを完全に把握できるようになる。

モバイルネットワーク事業者は、しばしば国内法で規定された期間、利用者に関するデータを保持しなければならない。このような要件は、たとえば、犯罪が発生した場合に法執行機関がデータにアクセスできるようにすることを目的としている。したがって、**人道団体**は、どのデータがプログラムの展開に実際に必要かを分析し、可能な限り不要なデータの収集を避けるべきである。最小限のデータのみ収集すれば、最小限のデータしか保持しないで済む。

15.4.4 情報

接続性プログラムにおいて、**データ主体**は、自身に関わるどのようなデータが、どのような目的で、どのような手段で収集されているかについて、明確かつ平易な言葉で知らされるべきである。これは、メタデータが生成されたときや収集されたデータが推定されたデータであるとき（データ主体によって明示的に与えられたデータまたは他の観察から推論できる情報）のように、**データ主体**にとってデータが収集されていることが明らかでない場合に特に重要である。個人はまた、権利を行使するために誰と連絡を取ることができるかを知らされるべきである。この情報によって、各個人は特定のサービスを利用するかどうかについて十分な情報を得た上で決定を下すことができ、権利を行使したい場合にどのように進めるかを理解することができる。

透明性と完全な情報開示のために、**人道団体**はプログラムに関与する第三者、その第三者がどのような活動に責任を持つか、またどのように連絡を取るかについて、**データ主体**に知らせることが推奨される。また、接続サービスを受けて利用すること、および接続性プログラム全般に関連する、実際および潜在的なマイナスの影響とリスクについても情報を提供されるべきである。El Jaguarキャンペーンに関連するプライバシーリスクを個人に知らせるUNHCRの例は、参考になるモデルである。[396]

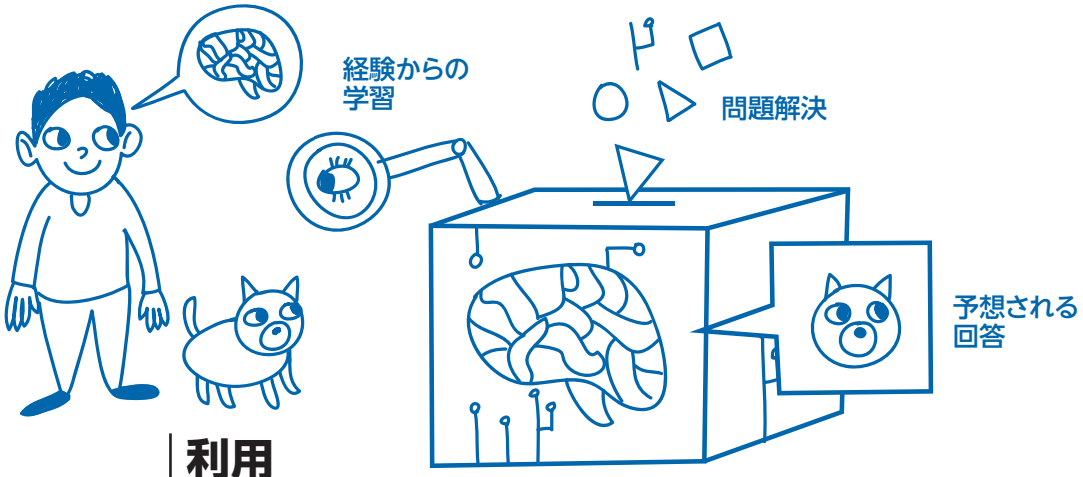
395 セクション2.7：データ保全を参照
396 https://www.facebook.com/ConfiaEnElJaguar/videos/874221649451680を参照。このキャンペーンビデオでは、ソーシャルメディアにおけるプライバシーとプロフィールの安全性に関するヒントを提供している。

15.5 国際的なデータ共有

オンラインで処理されたデータは、国境を越えて日常的に流れている。このことが接続性プログラムに関連して**個人データ**保護の懸念を引き起こす。契約条項の使用のような、認められた法的メカニズムは存在するが、特に接続性に係るソリューションはしばしば彼らの管理外にあるため、**人道団体**がそれらを効果的に実施することは困難である。とはいえ機関は、プロバイダが必要なデータ移転の取り決めを確実に実行するために、できる限りのことをすべきである。[397]

397 第4章：国際的なデータ共有を参照

人工知能



利用可能性

課題

第16章

人工知能と機械学習[398]

398 この章への貢献に対し、Alessandro Mantelero氏（トリノ工科大学）に感謝の意を表する。

16.1 はじめに

この章では、人道支援の分野における**人工知能**と**機械学習**システムの利用に関連するデータ保護の課題について検討する。これらの課題の中には、大いに議論されてきた自動化された意思決定の話題に関連するものが含まれる一方で、その他にはそのようなシステムがしばしば**個人データ**を含む大量のデータ利用に依存しているという事実から生じるものもある。以降のセクションでは、まず問題となっている技術の基本的な説明を行い、次に関連するデータ保護の課題を識別し、これらの課題のいくつかに対処する方法について**人道団体**向けのガイダンスを提供する。

16.1.1 人工知能と機械学習

人工知能という用語には、一般的に受け入れられている定義はないが、一般的には「(a) 人間の認知能力を機械によって再現することを目的とする一連の科学、理論および技術」と理解されている。[399]現在の形式では、テクノロジー開発者が「以前は人間に委任されていた複雑なタスクを機械に委任すること」ができるようにすることを目的としている。[400]

機械学習は、**人工知能**の特定の形態であり、機械で判読可能なデータの形で経験を積みながら、ある課題を時間をかけてより良く完了させるアルゴリズムの研究と定義することができる。[401]アルゴリズムは、解決しようとしている問題に相当するより多くのデータを受け取り、そのようなデータから「学習」する。しかし、様々な方法で「学習」するため、データにあまり依存しない**人工知能**技術もある。[402]

学習方法に関係なく、人工知能の全ての形式は共通の特徴を持っている。それらは、機械が特定の課題を完了するための一連の指示ではなく、その課題を完了するための戦略や解決法を生成するための一連の指示である。以下のモデルで示す。

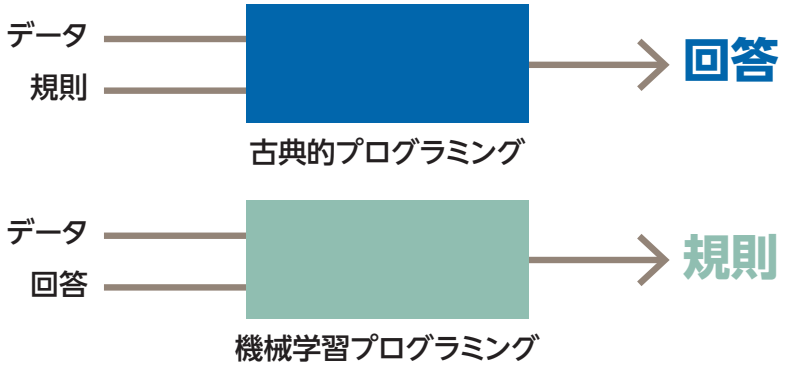
機械学習は**人工知能**の一形態であり、近年では、**人工知能**への投資の大部分を占めている。これらの理由から、この章を通して使用する「**人工知能**」という用語は、**人工知能**ソリューションと**機械学習**ソリューションの両方を意味することとする。特定の技術に関連する点については、その都度明確に説明する。

399 欧州評議会 (CoE)、人工知能のグロッサリー:https://www.coe.int/en/web/artificial-intelligence/glossary?mc_phishing_protection_id=28047-brbqhtidu81d093fnuog

400 CoE、人工知能のグロッサリー

401 T. Mitchell、Machine Learning、McGraw-Hill、ニューヨーク、1997年、p.2

402 これらの方法の例は、ベイジアンネットワークおよびルールエンジンを含む。ただし、これらの方法については、この章で扱わない



出典：F. Chollet、*Deep Learning with Python*、*Manning Publications*、2017年

16.1.2 人工知能と機械学習はどのように機能するのか

人工知能には様々な技術が存在し、**個人データ**を処理するものとしないものがある。一方で、ほとんどのソリューション、特に**機械学習**を使用するソリューションは、次のように機能する。

- 特定のパターンまたは類似性（訓練データ）を含むことが期待される選択されたデータが、システムに提示される。
- **人工知能**技術は、パターンを識別し、これらのパターンまたは類似性の分類および新しいデータの予測に関連する特徴を決定する。
- 予測もしくは分類するために「新しいデータがモデルによって処理されるときに現れるパターンを認識できるモデルが生成される。」[403]

ほとんどの種類の**人工知能**は大量のデータを供給されることに依存しているが、機能するために限られた量のデータのみを必要とする種類もある。本章のセクション3で説明するデータ保護の最も重要な意味を理解するには、**人工知能**ソリューションが「学習」する様々な方法を理解することが必要である。

- **教師あり学習（Supervised learning）**：このモデルでは、トレーニング・データに（分析者は各サンプルデータに「クラス」を割り当てる）というラベルが付けられる。例えば、動物のサンプルイメージに「dog（犬）」、「cat（猫）」、「parrot（おうむ）」などのラベルを付けて、システムに入力する。
- 一般的に、最終的な目的は、アルゴリズムが新しい（見えない）画像を学習した種類の一つに分類できるようにすることである。このタイプの学習は、例えば、部屋の数、サイズおよび/または建設年に基づく家の評価など、異なるパラメータ（または機能）に基づいて値を

403 ノルウェー王国のデータ保護機関、*Artificial intelligence and privacy*、2018年、p.7：https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

予測するために使用することもできる。どちらの場合も、原則は、データを正しい分野に適切に区分する、もしくは、正しい値を評価する、最適な数学関数を決定することである。

- **教師なし学習：**この場合、ラベルはシステムに入力されない。このアルゴリズムの目的は、データセット内の類似点やパターンを検出し、ラベル（またはクラス）自体を作成することである。データを「クラスター」に編成するために、様々な方法が適用される。正解も不正解もない。
- **強化学習：**このアプローチには、トレーニングデータはほとんど、または全く必要ない。その代わりに、「システムには、設計者が望むことを達成したときの「報酬」シグナル、または設計者が記述した結果に向けてプロセスを進めるステップが与えられる。システムが何か間違ったことをしても（求める結果に効率的に進めない）、それは報われない」という報酬と処罰の方法に依存している[404]

上記のいずれかの方法によってソリューションがトレーニングされると、[405]新しくて、見えないデータを分析および／または予測するために使用されるモデルを作成する。**人工知能**によって生成されるモデルには、静的モデルと動的モデルがある。静的モデルは時間が経過しても変化せず、トレーニングデータで開発されたモデルを常に適用する。これにより、開発者はモデルを完全に制御できるようになるが、時間の経過とともにソリューションが洗練されなくなる。一方、ダイナミックモデルは、入力データの変更に合わせ、出力を調整する。[406]

ほとんどの**人工知能**ソリューションは、それらを通過するデータ（トレーニング中、または動的モデルでは展開中も含め）から学習するため、その結果として得られるモデルは、それらを開発および／または改善するために使用されたデータの一部を保持する。これは、場合によっては、システムを攻撃して制御に成功した悪意のある当事者がトレーニングデータ（または、動的モデルでソリューションを展開する際に使用されるデータ）にアクセスできることを意味する。**人工知能**ソリューションに対する攻撃の可能性についての詳細は、以下のデータセキュリティに関する議論（3.5項）を参照。

404 ノルウェー王国のデータ保護機関、2018年、p.18

405 この章では、人工知能の学習方法として考えられる全ての方法について説明するわけではない。ここに記載されていない方式（ニューラルネットワーク等）の詳細については：L. Hardesty、“Explained: Neural networks”、MIT News、2017年4月14日：https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414、およびFuture of Privacy Forum, ***The Privacy Expert's Guide to Artificial Intelligence and Machine Learning***, 2018年：https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdfを参照

406 詳細については、ノルウェー王国のデータ保護機関、2018年、p.10を参照

16.1.3 人道支援の分野における人工知能

近年における利用可能なデータと**処理**能力の増大は、日常生活での**人工知能**の活用数を大きく増加させた。[407]**人工知能**は、例えば、音声起動式デジタルアシスタント、電話のロック解除や建物へのアクセスを可能にする生体認証システム、交通ルート決定のアプリケーション、オンラインプラットフォーム上での購入または閲覧の推奨、およびオンラインツール、サービスおよびスマートデバイスの他の多くの機能に存在する。この技術はまた、医療診断、画像認識、株式市場予測およびゲームを含む非常に多様な作業に適用することができる。

また、**人工知能**は、人道支援やそれに関連する活動、あるいはそれと同様の機能を持つ活動を促進し、より効果的かつ効率的なものにすることができる。いくつかの既存および潜在的な活用の詳細を次に示します。

- **世論を読む：**ウガンダでは、国連のグローバルパルス・プログラムで「音声認識技術と、ラジオコンテンツをテキストに変換する翻訳ツールを使用し、公共ラジオ放送を機械で読めるようにするツールキット」の試験的な使用が行われた。[408]このツールはパルスバボ・カンパラ（Pulse Lab Kampala）によって開発されたもので、様々な人口集団、特に農村部における傾向を識別することを目的としている。このイニシアティブの背景にある理論的根拠は、こうした傾向によって、政府や開発パートナーが国の開発ニーズに関する世論をよりよく理解できるようになり、それが開発プログラムの実施時に考慮されるようになるということである。
- **行方不明の子どもたちの特定と発見：**インドの行方不明児・脆弱な子どもたちのための国家追跡システムが、新しい顔認識システムの試行を開始してから4日以内に、3,000人近くの行方不明の子どもたちを特定したと報告されている。[409]このシステムは、児童養護施設や孤児院に住む子どもたちの写真と行方不明者の顔を照合するものである。
- **民間人への攻撃と人権侵害の追跡：**アムネスティ・インターナショナルのDecode the Difference project[410]では、民間人に対する組織的な攻撃を示す可能性がある破壊された建物を識別することを目的とし、異なる時期の同一の場所の画像を比較するためのボランティ

407 Centre for Information Policy Leadership、First Report：***Artificial Intelligence and Data Protection in Tension***、2018年、p.4：https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdfを参照

408 UN Global Pulse, "Making Ugandan Community Radio Machine-readable Using Speech Recognition Technology"、2016年：2016: https://www.unglobalpulse.org/projects/radio-mining-ugandaを参照

409 A. Cuthbertson、"Indian police trace 3,000 missing children in just four days using facial recognition technology"、The Independent、2018年4月24日：https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html、The Times of India、"Delhi: Facial recognition system helps trace 3,000 missing children in 4 days"、2018年4月22日：http://timesofindia.indiatimes.com/articleshow/63870129.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppstを参照。システムの公式サイト：https://trackthemissingchild.gov.in/trackchild/index.php/index.php

410 アムネスティ・インターナショナル、" Amnesty Decoders"、https://decoders.amnesty.org/

アを募集した。将来的には、画像を分析する**機械学習**ツールを訓練するためにデータを使用し、それによって処理を高速化し、容量を増加させることが可能となる。

- **疾病の予防と診断**：「1990年代以降、AI（**人工知能**）は、癌、多発性硬化症、膵臓疾患および糖尿病などの様々なタイプの疾患を診断するために使用されてきた。」[411]最近では、マイクロソフトの「Project Premonition」が、病原体が急激な増加を起こす前に検出するために開発された。このプロジェクトでは、ロボットを配備し、ある地域に蚊がいるかどうかを監視し、蚊の分布を予測して、対象となる種を捕獲する。**機械学習**技術によって、捕獲した蚊については、咬んだ動物から得た可能性のある病原体を持つ個体を探す。[412]

16.1.4 人工知能を使用する際の課題とリスク

人工知能の活用には、その可能性にもかかわらず、課題とリスクがある。データ保護の問題（下記の3項を参照）以外にも、前述の全ての使用例で、実装上の実用的な課題が示されている。例えば、行方不明者を識別するために使用される**人工知能**ベースの画像認識ソフトウェアは、あまりにも多くの偽陽性を提供する可能性がある。こうした誤った一致は、ケースワーカーの間に混乱を生み出すだけでなく、対象者の家族に誤った希望を与える可能性もある。他のシステムでは、より正確であっても、正しい一致を見逃してしまう可能性がある（偽陰性として知られている）。偽陰性は商業的利用ではあまり問題にならないかもしれないが、人道的分野では壊滅的な結果をもたらす可能性がある。親との接触を失った子どもを誤って識別してしまうと、家族全体に害が及ぶ可能性がある。

上記の議論が強調しているように、**人工知能**は受益者にリスクをもたらす可能性がある。例えば、もし**人工知能**が特定の人道支援プログラムのための適切な対象集団を識別するために使われ、ソリューションが正確な識別を行わない場合、そうでなければプログラムに参加する資格を有していた人々が除外される可能性がある。スウェーデンでは、何千人もの失業者が、**人工知能**を利用した政府システムによって誤って給付を拒否された。[413]

ほとんどの**人道団体**は、独自のモデルを開発するのではなく、既製のソリューションを獲得するため、アルゴリズムが予期せぬ、または不合理な結果をもたらす可能性のあるリスクが存在する。同様に、ソリューションの切り替えにはコストがかかる可能性があるため、業者の固定化はリスク要因となる。また、主に人道団体が保有する大規模データセットへのアクセスとその活用に関心を持つ商業

411 H. M. Roff "Advancing Human Security through Artificial Intelligence"、Chatham House、2017年、p.5：https://www.chathamhouse.org/archive/advancing-human-security-through-artificial-intelligence

412 Microsoft、"Microsoft Premonition"：https://www.microsoft.com/en-us/research/project/project-premonition/

413 T. Wills "Sweden: Rogue algorithm stops welfare payments for up to 70,000 unemployed"、Algorithm Watch、2019年2月25日：https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments/

ベンチャーが、これらの機関をターゲットにする可能性があり、時にはデータが関係する個人やコミュニティにとって大きなリスクとなることもある。

バイアスは、特に特定の人道的状況において、**人工知能**の有効性に上記とは別のリスクを突きつけている（下記3.2.2項を参照）。ほとんどの（全てではない）ソリューションは大量のデータに対してトレーニングされるため、目的に合ったデータセットを選択することが重要である。このソリューションを使用して個人または特定のコミュニティのパターンを識別したり、予測を行ったりする場合、トレーニングデータセットには**個人データ**を含める必要がある。

他の多くの技術と同様に、「ゴミを入れたら、ゴミが出てくる（garbage in, garbage out）」の考え方[414]は**人工知能**にも適用され、適合しない、不正確な、または無関係なデータを使用することは、ソリューションの精度に影響を与える可能性がある。既製のアルゴリズムが**人道団体**の文脈に適合することは非常にまれであるため、これは**人道団体**にとって**特**に難しい問題である。例えば、**人道団体**が行方不明者の発見を支援するために顔認識ソフトウェアを開発したい場合、訓練データセットは、マッチング機能の精度を最大化するために、身体的特徴の人種差が確実に統合されるように、十分に広範である必要がある。

16.2 データ保護影響評価

データ保護影響評価（DPIA）は、データの**処理**を伴うプロジェクト、方針、プログラムまたはその他の取り組みの**データ主体**およびその個人データに対する影響を特定、評価し、対処することを含む。[415]最終的には、データ**処理**作業に関連するリスクを回避、最小化、移転または共有する措置につながるべきである。DPIAは継続的なプロセスであり、ライフサイクル全般における個人データの**処理**を含むプロジェクトまたは取り組みに従うべきである。**人工知能**（以下のセクション3.2.3でより詳細に説明されているように）の利用における透明性の限界を考えると、DPIAは受益者の**人工知能**ソリューションの受け入れと、人道団体による利用の増加を促進する可能性がある。**人工知能**の利用は個人に大きなデータ保護リスクをもたらす可能性があるため、人道団体はそのようなソリューションを実施する決定を下す前にDPIAを実施すべきである。第8節で後述するように、DPIAを実施する際には、**人工知能**の倫理的意義も考慮されるべきである。

414 コンピューティングの無料オンライン辞書（http://foldoc.org）、によると、ガーベッジイン、ガーベッジアウトの概念は、「コンピューターは人間と違って、無意味な入力データを疑いなく処理し、無意味な出力を生成する」という事実に関連している。「欠陥のある、不完全または不正確なデータによる人間意志決定の障害」という意味でも用いられる。

415 第5章：データ保護影響評価（DPIAS）を参照

16.3 データ保護基本原則の適用

前述したように、ほとんどの**人工知能**ソリューションは、適切に機能するために、大量のデータ（個人データと非個人データの両方）を処理する必要がある。しかし、**人工知能**ソリューションがいつ**個人データ**を処理し、その結果としてデータ保護の原則がいつ適用されるかを知ることは困難な場合がある。これは、**人工知能**ソリューションの能力がますます高まり、「データの連携、あるいは、非個人データを識別できるようなデータのパターンを認識すること」ができるからである。[416]これは、場合によっては、**人工知能**ソリューションが、仮名化されたデータ再識別できることを意味する。すなわち、「例えば、携帯電話、車、その他の機器のセンサーから収集されるデータの種類とそれへの要求」を拡大することで、また、「収集したデータを処理するためのますます高度な計算能力」を提供することによっても再識別できるようになり、よって、個人を確実に識別するための組み合わせの機会が提供されることを意味している。[417]**個人データ**を処理する他のシステムと同様に、データ保護原則の適用（または不適用）およびその方法を決定する際には、ソリューションのアーキテクチャ、およびソリューションが使用される文脈を十分に考慮する必要がある。

16.3.1 目的制限と追加的処理

人工知能および**機械学習**のソリューションへの目的制限原則[418]の適用は、これらの技術が当初計画されていなかった方法でデータを処理する能力を有し、従って、当初意図されたものとは異なる目的を達成する可能性があるため、難易度が高い。これは主に**機械学習**の本質的な性質によるものであり、分析されたデータセット内の様々な相関関係をテストして明らかにすることである。その結果、これらのソリューションでは、データの機能から新しいことを容易に推測できる。

416 Centre for Information Policy Leadership、2018年、p.11
417 Centre for Information Policy Leadership、2018年、p.11
418 セクション2.5.2：目的制限の原則を参照

例：
2012年、研究者らは、**人工知能**アルゴリズムがある人のFacebook上の「いいね」を分析したところ（その人物からはそれ以上お情報は得ずに）、ソリューションによって「性的嗜好、民族性、宗教的および政治的見解、性格指向、知性、幸福さ、依存性物質の使用、親の別居、年齢、性別など、非常に機密性の高い様々な個人属性を自動的かつ正確に予測する」ことができた。[419]より具体的には、そのソリューションは、「同性愛者と異性愛者の間では88%、アフリカ系アメリカ人と白人アメリカ人の間では95%、民主党と共和党の間では85%」を正しく識別した。[420]この特定のケースでは、そのソリューションは、これらの相関関係を作るように求められていた。しかし、**人工知能**ソリューションがそのような推論を独自に引き出し、開発者の意図ではない場合でも、個人に関する機微情報を明らかにすることがある。

目的制限の原則によって、組織が**個人データ**の取扱いについて明確に定義された目標を決定し、そのような目標を達成するために必要な手段と情報を考慮することが求められる。しかし、**人工知能**の場合は、そのソリューションが望ましくない結果をもたらすかどうかについても考慮する必要がある。ソリューションが、定義された目的と両立しない方法で**個人データ**を**処理**する可能性がある、または望ましくない情報を明らかにしたり、予測を行ったりすることが想定される場合は、ソリューションの開発時や、トレーニングデータセットの選択時に、これらの要因を考慮する必要がある。最終的な目的は、望ましくない結果や不要な形の**追加処理**を防ぐことです。

16.3.2 公正かつ適法な処理

16.3.2.1 適法性

個人データが**人工知能**ソリューション内でまたはその訓練の一部として処理される場合は、**処理**が行われるための正当な法的根拠が要求される。**人工知能**システムの複雑さを考慮すると、適切な法的根拠の発見と正当化は特に困難である。第3章では、異なる法的根拠を概説し、**人道支援**の法的根拠として**同意**を用いることの限界を指摘する。これらの困難に加えて、**同意**の利用に対する制限、特に同意の撤回の可能性もまた、**人工知能**ソリューションの開発と改善に関連している。**人工知能**における**同意**が十分に情報に基づいている、あるいは自由に与えられているとはみなされない理由には、「長期的かつ技術的なデータ処理通知、社会的および

419 M. Kosinskia, D.Stillwella and T. Graepel、"Private traits and attributes are predictable from digital records of human behavior"、PNAS、Vol. 110、No. 15、2013 年、p.1：https://www.pnas.org/content/pnas/early/2013/03/06/1218772110.full.pdf

420 Kosinskia, Stillwella and Graepel、2013年、p.1

技術的な囲い込み、不明瞭なインターフェース設計、データ主体側の認識不足」などが含まれる。[421]

この章の冒頭で説明したように、**人工知能**によって生成されるモデルは静的であっても動的であってもかまわない。この二種類のモデルは、データ保護に異なる影響を及ぼす可能性がある。静的モデルはシステムに割り当てられた作業を実行するためにのみ**個人データ**を**処理**する一方、動的モデルは目的の出力に到達するためにデータを処理するが、より正確な結果を提供するためにシステムの改良も行う。これは、各モデルのデータ処理の目的と法的根拠が異なることを意味する。

例えば、**人道団体**が動的モデルを選択する場合、明確に定義された目的を達成するために、アルゴリズムを訓練するための**個人データ処理**を行う適切な法的根拠を識別すべきである。システムが訓練された後、意図された目的を満たすために、新しい**個人データ**の**処理**に対する法的根拠も定義されるべきである。最後に、人道団体は、動的モデルを改善するためのデータ処理の法的根拠も識別する必要がある。

テクノロジー企業が開発した既製のソリューションを含む動的モデルでは、開発中にシステムに入力された全てのデータと適用がその改善に使用されることを覚えておくことが重要である。このことは、**同意**の使用にさらなる挑戦をもたらす場合がある。[422]受益者は、特定の人道的目的のために自分の**個人データ**が**処理**されることには同意するかもしれないが、**人工知能**ソリューションの開発のために使用されることを想定しない可能性があるからだ。このような場合、特定された処理の法的根拠が**同意**である場合には、**データ主体**に対し、彼らのデータが要請される理由、そのデータが何のために使用されるのか、およびそのデータがどのようにソリューションに影響を与えるのかについて、分かりやすく説明する必要がある。また、ソリューションによる再識別（3.1項で述べたように）や、攻撃中にデータにアクセスされる可能性があるという事実（冒頭で述べたように）など、潜在的なリスクについても情報の提供が必要となる。これにより、人道団体は**データ主体**から十分な情報に基づく**同意**を得ることができる。

上記に照らして、**同意**は、必ずしも人道分野における**人工知能**の利用のための適切な法的根拠であるとは限らない。援助または人命救助サービスの提供は、生命に関わる利益[423]または公共の利益[424]は、**個人データ**の**処理**を正当化する適法な法的根拠とみなすことができるが、**人工知能**ソリューションの開発は、場合によってはそうはみなされない。**人工知能**ソリューション

421 A. Mantelero、A.、*Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, 欧州評議会（CoE）、2019年、p.7：https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6
422 Future of Privacy Forum、2018年、p.8
423 セクション3.3：生命に関わる利益を参照
424 セクション3.4：公益という重要な根拠を参照

の改善が選択された法的根拠に基づいて受け入れられるかどうかを決定するには、人道団体は、ソリューションの改善のための**追加処理**が、**個人データ**を収集した当初の目的と適合するかどうかを検討すべきである。

16.3.2.2 公正対偏見

公正の原則[425]によって、全てのデータ**処理**活動が**データ主体**の利益を尊重し、**データ管理者**が個人に対する恣意的な差別を防止するための措置を講じることが求められる。[426] **人工知能**における差別的偏向の問題は広く認識され議論されている。

例：
よく知られている例では、有罪判決を受けた犯罪者に保釈を認めるかどうかに対する裁判官の判断を助けるために、刑事事件の再犯率を予測する**人工知能**ソリューションが米国で開発された。このソリューションは、黒人の被告の再犯率は白人の被告の再犯率のほぼ2倍であると誤って評価した。[427]

リスクにおける差別的な偏向を最小限に抑えるため、**人工知能**の開発者には「ヒューマンライツ・バイ・デザインのアプローチを採用し、意図的でないものや隠されたものを含む潜在的なバイアス、**データ主体**の人権や基本的自由に対する差別やその他の悪影響のリスクを回避する」ことが推奨されている。[428]

人工知能ソリューションにおける偏向は、トレーニング・データとしてバイアスのかかったデータセットを使用すること、社会における体系的なバイアス、または開発者が各データセット内でより多くの価値を割り当てる機能を決定することに起因する可能性がある。さらに、社会に歴史的偏向があるとき、ソリューションの訓練のために偏向がないデータを見つけることは困難であるかもしれない。ここで、このソリューションは、データセットに含まれる体系的偏向を単に強化するだけとなる場合もある。したがって、モデルは関連性のある正確なデータを用いて訓練されなければならず、また、どの特徴を強調すべきかを学習しなければならず、その結果、データに存在する可能性のある差別的な側面に過度の重みを与えてはならない。恣意的な差別に関するリスクがある場合には、人種的または民族的出自、政治的見解、宗教的および哲学的信念、性的

425 セクション2.5.1：公平性の原理と処理の適法性を参照
426 ノルウェー王国データ保護機関、2018年、p.16
427 J. Angwin et al. “Machine Bias”、ProPublica、2016 年 5 月 23 日：https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
428 CoE、Guidelines on artificial intelligence and data protection、2019 年、p.2：https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

指向に関連する情報、またはその他の差別の根拠となり得るいかなる情報も、過度に強調されないよう処理しないようにするべき、もしくは保護されるべきである。[429]

しかし、**人工知能**のモデルがそのような種類のデータを強調すべきでないという事実は、データセットからそれらのデータを抑制することが、必ずしも偏向のリスクを排除することを意味するわけではない。システムは人種や性別のような他の特徴を相互に関連づけることができ、モデルは、この文脈では「代理人」として知られる、これらの相関する特徴に基づいて偏向を受けることを学ぶことができる。[430]さらに、主な識別機能がデータセットから削除されているため、偏向の検出と訂正がより困難になる可能性がある。

例：
前述の米国の予測的ソリューションを調べた別の研究では、ほぼ70%のケースで、偏向が明確であるにもかかわらず、アルゴリズムは正しい再犯予測をしたことがわかった。しかし、この第二の研究では、人種はデータセットに含まれておらず、「貧困、失業、社会的疎外など、人種（またはその他の除去された要因）の代用とならないモデルを見つけることが課題」が強調されている。[431]

このため、訓練データセットを選択する際には、独立した**データ管理者**、**データ処理者**、または**人道団体**との共同管理者のいずれであっても、**人工知能**開発者は、使用される**個人データ**の質、性質、および出所を評価し、文脈から切り離されたモデルを作成するために文脈から切り離されたデータを使用することによる、個人およびグループに対する潜在的リスクを考慮する必要がある。[432]これを達成する一つの方法は、**データ管理者**が継続的DPIAプロセスに（本章第2節参照）、「偏向の有無を確認するために処理するデータセットを頻繁に評価する」および「相関関係への過度の依存を含め、偏見につながる要素に対処する方法を開発する」を含めることである。[433]2章で論じたように、そのような措置を取らないことは、法的および倫理的な意味合いを持つ。

429 ノルウェー王国データ保護機関、2018年、p.16
430 Centre for Information Policy Leadership、2018年、p.14
431 Future of Privacy Forum, 2018, p.15
432 CoE, 2019, p.2
433 EU第29条作業部会、*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01)、2018年、p.28：https://ec.europa.eu/newsroom/article29/items/612053

16.3.2.3 透明性

公正さと並んで、透明性はデータ保護のもう一つの重要な側面である。この原則に従えば、個人データの**処理**は**データ主体**にとって透明性のあるものでなければならず、[434]彼らのデータが収集される際には、**個人データ**の**処理**に関して少なくとも最低限の情報は受け取るべきである。[435]しかし、これらのソリューションは高度な技術に基づいており、平易な言葉での説明や理解が難しい可能性があるため、**人工知能**に関しては透明性を適用することが難しい原則となる場合がある。[436]さらに、多くの**機械学習**モデルは、出力がデータ科学者やソリューション設計者自身によっても複製または数学的に理解できない内部プロセスの結果である多層ネットワークを含む。[437]この多層構造は、ソリューションを使用する人がどのように特定の結論または予測に達したのかを理解できなくする可能性があるため（例えば、処理の過程でどの昨日により重みが割り当てられたか、など）、一般的に「ブラックボックス」として知られている。つまり、**人工知能**の複雑さのために、重量の選択の背後にある論理は、ほとんどの場合、人間にとって透明性がない、または理解できるものではない。したがって、機能の選択が包括的であるかどうか、およびその重み付けが妥当であるかどうかを断言することは困難である。

人工知能の適用における透明性の課題に対して提案された一つの答えは、ソリューションの背後にある論理回路を説明するということである。すなわち「入力データのタイプと予想される出力に関する情報を提供する、変数とその重みを説明する、または分析アーキテクチャに光を当てる」ことである。[438]「解釈可能性」として知られるこのアプローチは、入力における変化の出力への因果関係を理解することに焦点を当てており、必ずしもその複数の層を通して機械の全ての論理を説明する必要はない。しかしながら、ブラックボックスの場合には、解釈可能性を達成することは困難なことが多く、**データ主体**に対し、未知および不確実な領域について透明性を保つことが重要である。

16.3.3 データの最小化

データの最小化原則は、人道団体が**個人データ**の**処理**について、**処理**の目的を達成するために必要な最小限の量および範囲に制限することを求めるものである。[439]**人工知能**を使用する場合、何が必要なのかを事前に知ることが困難になる場合がある。[440]これらのソリューションはそれら自体で機能やパターンを認識するため、特定の作業を完了するために必要なデータとその量を理解することが困難になるからである。従って、**機械学習**のような技術は、有用な結果を生成

434 セクション2.5.1：公平性の原理と処理の適法性を参照
435 セクション2.10：情報を参照
436 ノルウェー王国データ保護機関、2018年、p.19
437 Future of Privacy Forum、2018、p.17
438 Mantelero、2019、p.12
439 セクション2.5.4：データ最小化の原則を参照
440 Centre for Information Policy Leadership、2018年、p.14

するために大量のデータを必要とするので、ある特定範囲までの最小化のみが可能である。[441] さらに、そのようなソリューションは、適切に大規模で代表的なデータセットを使用してトレーニングする必要があり、そうでなければ偏った結果が生じる可能性がある。[442]

人工知能とデータ最小化の間のこの明白な矛盾にもかかわらず、様々な緩和手段が存在する。以下に、潜在的な制限事項とともに、これらの緩和手段を記載する。

- 使用する情報の量や性質を制限するなど、データを通じた個人の識別を困難にする技術を採用する。このアプローチは、機能するために大量のデータを必要とする特定の**人工知能**ソリューションには適さない場合がある。さらに、データを識別しにくいものにすること自体は、データの最小化原則の尊重を保証するものではない。
- 「合成データ」をトレーニングデータとして使用する。合成データは「人工的なデータセットであり、『現実に存在する』個人に関する実際のデータは含まれないが、元のデータセットの全ての統計的側面の特性と比例関係を反映している」。[443]しかし、この手法は、合成データが実データの元の一連のデータ（合成データが、ソリューションによって分析される社会や状況を反映して正確な結果を生成できるようにするために必要）から導出されるため、課題も提起する。このように、合成データセットを使用する場合にも再識別のリスクが存在する。
- 期待される結果を達成するために必要と考えられる最小限のデータを収集し、ソリューションがどのように機能するかを確認するためにソリューションをテストするという段階的なアプローチを採用する。テスト後、必要に応じてさらにデータを追加し、目的の結果が得られるまでソリューションを再度テストできる。このアプローチでは、不要なデータの**処理**が削減され、ソリューションが最小限のデータセットで確実にトレーニングされる一方、再識別が困難になる。

人工知能におけるデータの最小化に関連する課題にもかかわらず、この原理は大規模な**処理**が禁止されることを意味するのではなく、むしろ適切なセキュリティとリスク軽減措置を必要とするより高いリスクをもたらす。さらに、前述したように、全ての**人工知能**ソリューションが、正確であるために大量のデータを必要とするわけではない。例えば、強化学習に基づくものは、ほとんどまたは全くデータを用いずに訓練することができる。

441 Mantelero、2019、p.8
442 Centre for Information Policy Leadership、2018年、p.13
443 Future of Privacy Forum、2018年、p.8

16.3.4 データ保全

個人データは、所定の期間保全されるべきであり、その期間はデータ**処理**という目的のために必要な期間を超えてはならない。[444]ただし、**個人データ**を一定期間後に消去すると、システムの動作を可能にするトレーニング、展開、監視のためには使用できなくなる。[445]例えば、モデルに偏向と表示されている場合、正しく重み付けされていない機能がどれなのかを理解するために使用可能なデータがあり、より正確な結果を提供するためのソリューションを保持することは、役に立つだろう。**人工知能**ソリューションでは貯蔵のデータをより長期間保持できるという利点があるが、**データ管理者**は、**個人データ**を必要以上に保持しないことを保証し、ソリューションのリスクの不正確さを低減するために、保全期間を通じてデータが確実に更新されるように対策を講じる必要がある。[446]**人工知能**は人道支援の分野で様々な用途が考えられるため、それぞれのプログラムにおいて、特定の保全期間を考慮すべきである。この点に関し、**人道団体**は、監査における2年間のような、初期保全期間を考慮し、設定すべきである。この初期期間を過ぎてもデータが必要な場合、組織は保全ニーズに基づいて定期的に評価を行い、保全期間を変更する法的根拠を検討する必要がある。また、**データ主体**が収集時点で同意した期間を超えてデータが保全される場合には、彼らから追加の**同意**を求める必要がある。

16.3.5 データセキュリティ

データセキュリティ[447]は、**人工知能**ソリューションを実施する上で、特に人道分野では不可欠な要素である。**人道団体**は、これらの技術がもたらすリスクに留意し、それらを使用する際には最高レベルのデータセキュリティを実施しなければならない。悪意のある者による攻撃は、通常、次の3つのカテゴリのいずれかに分類される。

- **モデル反転攻撃**：システムのモデルを反転させることにより、トレーニング・データに関する情報を明らかにしようとする攻撃
- **中毒攻撃**：モデルの効用を減らそうとするもの
- **バックドア攻撃**：ソリューションへの不正アクセスを試み、トレーニング後に修正すること

特にモデルの反転を見ると、いくつかのシステムは訓練でのデータセットを記憶していることが示されている。例えば、ある人物の顔が顔認識システムの訓練で使用された場合、悪意のある当事者は、その人物が訓練セットの一部であることを理解するのに十分な精度で顔を再構成す

444 セクション2.7：データ保全を参照
445 Centre for Information Policy Leadership、2018年、p.15
446 EU第29条作業部会、2018年、p.12
447 セクション2.8：データセキュリティと処理のセキュリティを参照

るために、入力画像をゆっくりと変更しながら、その人物の顔を何度もシステムに問い合わせることができる。[448]

別のタイプの意図的な攻撃は、結果の質を低下させるためにデータにノイズを加えることを含んでおり、時には間違った分類や予測をするような無用な結果につながることさえある。

これらの全ての要因は、不十分なデータセキュリティが、**人工知能**の使用において脆弱な個人に重大なリスクをもたらす可能性があることを意味する。これらのリスクを考慮すると、不正アクセスから効果的に保護する強力で安全なシステムを構築することが重要である。この点で役に立つ方法の中には、**仮名化**と暗号化技術があります。暗号化されたデータに関するモデルをトレーニングする技術はまだ初期の段階にありますが、暗号化された入力を受け取り、暗号化された出力を生成する静的モデルは、それ自体に制約はありますが、すでに一般的になっている。差分プライバシーの使用も[449]**人工知能**ソリューションを訓練する際に考慮されるべきである。

16.4 データ主体の権利

データ管理者は、データ**処理**の手段および目的を決定し、**データ主体**がその権利を確実に行使できるようにする責任を負う。[450]**人工知能**は、**データ管理者**がこれらの義務を遵守することをより困難にするかもしれないが、一定の目的を達成する手段としてそのようなソリューションを選択することは、**データ管理者**の責任を免除するものではない。したがって、**人道団体**は、個人が確実に権利を行使できるように手続きとシステムを整備すべきであり、また、データ保護・バイ・デザインとデータ保護・バイ・デフォルト（下記の7項を参照）の原則も採用すべきである。同時に、本ハンドブックのセクション2.11で議論されているように、これらの権利の行使は特定の状況において制限される場合がある。

448 M. Fredrikson, S. Jha and T. Ristenpart、"Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures"（2015 年 ）CCS '15 ***Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security***、pp. 1322–1333：https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf

449 「差分プライベートアルゴリズムは、補助情報を使用する適応攻撃に耐性がある。これらのアルゴリズムは、ランダムなノイズをミックスに組み込むことに依存しているので、敵が受け取るものは全てノイズが多く、不正確になり、プライバシーを侵害することははるかに困難です。（実行可能であれば）」。A. Elamurugaiyan、「差別的プライバシーの簡単な紹介 」、Medium、2018 年 8 月 31 日：https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b

450 セクション2.11：データ主体の権利を参照

16.4.1 通知を受ける権利

他の技術と同様に、**人工知能**が適用される場合、**データ主体**は、**データ管理者**の身元と連絡先の詳細、管理者への連絡方法、データ**処理**の目的と法的根拠、処理中の**個人データ**の種類、**データ主体**としての権利（特にアクセス権）、および処理に関連する保護措置について通知を受けるべきである。[451]さらに、**データ主体**は、**人工知能**の使用、想定される**処理**に対するその重要性、および**処理**に関連するリスク、規則および保護措置について情報提供されるべきである。[452]

16.4.2 削除権

人道団体が**人工知能**ソリューションを使用する際には、データ削除の権利を十分に考慮する必要がある。[453]**データ主体**からデータ消去の要請があったものの、該当するデータが特定のソリューションを訓練するために使用されていた場合、たとえデータが消去可能であっても、そのソリューションは消去要請のあったデータに基づくものである。つまり、人道団体がデータセットからデータを消去しても、ソリューションには消去されたデータの特定の特徴は残ったままになる場合がある（ソリューションを作成する際にそれらの特徴が解析され、データセット内の他の特徴と比較されたため）。これは、上述したように、モデル反転攻撃によって元のデータが明らかになる場合に問題となることがある。

この場合、ソリューションを変更せずにデータセット自体を消去することが、削除の権利に対する制限を構成するかどうか、また、そうであれば、そのような制限が状況において正当化されるかどうかを考慮することが重要である。削除に関する課題が何であれ、「個人の意見や各人の自己発展に影響を及ぼす技術に基づくデータ処理に関しては、異議を申し立てる権利が確保されるべきである。」[454]重要なことは、本ハンドブックのセクション2.11で議論されているように、この権利を制限する正当な理由が存在する場合もあるということである。

16.4.3 自動化された意思決定に関する権利

データ主体は、もっぱら自動化された意志決定、すなわち「人間の関与なしの技術的手段による決定」が[455]法的効果をもたらす場合、または同様に当該個人に重大な影響を及ぼす場合、対象とならない権利を有する。

451 セクション2.10：情報を参照
452 ノルウェー王国データ保護機関、2018年、p.19
453 セクション2.11.4：削除権を参照
454 CoE、2019年、p.2
455 CoE、2019年、p.8

例：
もっぱら自動化された意志決定の例としては、スピードカメラからの証拠だけに基づいて課されるスピード違反の罰金、オンライン信用適用の自動拒否、人間の介入なしのオンライン採用の実践などがある。[456]

この権利の背後にある理論的根拠「は、アルゴリズム的な偏向への懸念による。つまり、不正確または不完全なデータに基づいた、もっぱら自動化された決定に関する不安、また、アルゴリズムが間違っていたり不公正だったりした場合には、個人が補償を受ける必要性と決定に異議を唱える能力」である。[457]こうした懸念は、前述のスウェーデンの給付金制度のような例によって正当化される。この場合、不正なソリューションは、「何千人もの失業者が誤って給付を拒否された[458]」ことを意味する。

人道支援において、**人工知能**ソリューションが、誰が支援を受け、誰が支援プログラムの対象人口に含まれるかについて決定する場合、同様の問題が生じる可能性がある。受益者は、自分に影響を及ぼす決定を人間に監督させる権利を常に有するべきである。

「人間の関与とみなされるためには、管理者は、決定に対する監督が単なる形式的な意思表示ではなく、意味のあるものであることを明確にしなければならない」ということに注意する必要がある[459]これは特に重要になる。なぜなら、意思決定を行う者は、数学的アルゴリズムが失敗しないとされていることを根拠に、**人工知能**によるソリューションの示唆に盲目的に依拠する可能性があるからである。したがって、個々の人間の意思決定者の存在だけでは十分ではない。[460]意思決定者は、機械の決定や提案に反論する能力を持たなければならない。

同様に、意思決定者は、システムがどのようにして特定の決定または提案に到達したのかを完全には理解していない可能性があり、したがって、それが誤って行われたかどうかの評価が困難になる可能性がある（上記の3.2.3の透明性を参照）。意思決定者は常に、全ての事実と情報をゼロから調査し、**人工知能**ソリューションの決定を考慮することなく、独立した決定を下すことができる必要がある。しかし、**人工知能**ソリューションは、同じ状況にいる人よりもはるかに多くの情報を処理できるため、これは必ずしも簡単ではない。このような場合には、この分野の専門家や技術開発者を含む学際的なチームを立ち上げることも一つの選択肢だろう。

456 CoE、2019年、p.8
457 Centre for Information Policy Leadership、2018年、p.16
458 Wills、2019年
459 EU第29条作業部会、2018年、p.21
460 Montelero、2019年、p.11

技術の高い正確性を考えると、専門知識のレベルに関係なく、個人が**人工知能**の自動化された決定に異議を唱えることをためらう可能性がある。したがって、考慮すべき別の問題は、決定の審査が「決定を変更できる適切な権限と能力を持つ人によって行われる」ように、人的介入をどのように調整するかである[461]したがって、人道団体は、受益者が意思決定への人間介入の権利を有していたなら、自動化された意思決定の対象となることを受け入れられるかどうかを考慮する必要がある。ここでは、そもそもこの技術を使用すること自体が問題になるかもしれない。

いずれにしても、受益者は、**人工知能**ソリューションの背後にある論理、処理の重要性、および受益者に想定される結果を含め、対象となるあらゆる自動化された意思決定について情報の提供を受けることが不可欠である。[462]また、データ**処理**に対して異議を申し立てる必要がある。

16.5 データ管理者とデータ処理者の関係

16.5.1 説明責任

上述したように、**人工知能**はブラックボックス効果（4.2.3項参照）のために開発者が完全に理解できない形で進化することがある。これにより、**データ管理者**の説明責任と責任の原則に関する疑問が生じる可能性がある。これらの原則を実施するために、**データ管理者**は、データ保護要件を遵守し、それぞれのデータ**処理**作業において適切かつ相応の技術的および組織的措置を講じたことを証明できる立場にある必要がある。[463]

16.5.2 責任

自動意思決定（上記を参照）は、責任をめぐる特定の問題を提起する。例えば、医療では、特定の種類のがんなどの病気を診断したり、X線画像を分析したりする場合、機械の方が人間よりも正確だと考えられることが多い。このため、医師は機械の助言に従わざるを得ないと感じることがある。[464]ここでは、診断の責任者が誰なのか、つまり、機械自体（それが法人と見なされるべきだと仮定する）なのか、開発者なのか、医師なのかが不明な場合がある。[465]同様の状況は、**人道団体**が緊急事態において医療サービスを提供する場合にも起こり得る。例えば、伝染病の発生中に誰かが誤診された場合である。これに対抗するために、人道団体は製造物責任の論理をアルゴリズムにまで拡張しようとする可能性があり、それによって開発会

461 EU第29条作業部会、2018年、p.27
462 EU第29条作業部会、2018年、p.25
463 セクション2.9：説明責任の原則を参照
464 フランス共和国データ保護機関（CNIL）、“Comment permettre à l’homme de garder la main? Les enjeux éthiques des algorithmes et de l’intelligence artificielle”、2017年、p.27：https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
465 CNIL、2017年、p.27

社に責任の全責任を負わせることになる[466]（しかし、実際に交渉をするのは非常に難しいかもしれない）。倫理的観点から、**人道団体**がそのような技術の使用を選択する際に自らの責任を理解し、それに応じて受益者に対して説明責任を果たすことも重要である。

16.6 国際的なデータ共有

人工知能ソリューションで処理される**個人データ**やその他の種類のデータは、国境を越えて日常的に流れるだろう。これにより、データが国際的に共有される場合の**人工知能**の適用におけるデータ保護についての問題が発生する。[467]認知された法的メカニズムは存在するが、**人工知能**の文脈では、ほとんど実用的ではないかもしれない。

適用される法律と管轄の決定も難しい課題となる可能性がある。管轄権の選択と法律の選択が**人工知能**のガバナンスに明確に組み込まれていない限り、移転に必要な適切で的を絞ったリスク分析は不可能である。このハンドブックのセクション4.2に記述されている原則は、**人工知能**の文脈における**国際的なデータ共有**に関する、人道団体へのより詳細なガイダンスを提供している。データ共有の説明責任は、**人道団体**が**国際的なデータ共有**を含む活動を行う際に考慮すべき重要な原則である。

16.7 データ保護・バイ・デザインと初期設定におけるデータ保護

データ保護・バイ・デザインと初期設定におけるデータ保護には、最初から主要なデータ保護原則を実施し、**データ主体**に最大限のデータ保護を提供する方法で、**処理**作業、プログラム、またはソリューションを設計することが含まれる。この意味で重要なデータ保護の原則は次のとおりである。

- 適法性・公正性・透明性
- 目的制限
- データ最小化
- 正確さ
- 保存の制限（限定保有）
- 完全性と機密性（セキュリティ）
- 説明責任

466 Mantelero、2019年、p.17
467 第4章：国際的なデータ共有を参照

これらの原則の一般的な説明については、このハンドブックの第2章を参照のこと。またこの内のいくつかについては、上記の3項に記載がある。

人工知能の特定の特性は、前述の3項で説明したように、データ保護準拠ソリューションの実装において困難な課題となる可能性がある。最初からこれらの課題やリスクに対処する方法でソリューションを構築することは、それらを回避または軽減できる最も効果的な方法の1つになり得る。例えば、ほとんどの人工知能技術は、大量のデータを処理して、関連する特徴を比較検討し、パターンを識別し、モデルを訓練して改善する方法を学習する。**人工知能**が正常に機能するためには詳細なデータセットが必要になることがよくあるため、このようなデータはほとんど匿名化されていない。

しかし、データセットに追加される特徴がユニークであればあるほど、モデルが当初に意図したよりも多くの推論を行う（3.1項参照）か、システムが意図的な攻撃を受ける（3.5項参照）かのいずれかの理由で、データが関係する人物を識別する可能性が高くなる。最終的には、**人工知能**技術を使用するかどうかの決定には、常に**人工知能**技術の潜在的な利益と**データ主体**に対する潜在的なリスクとを比較検討することが含まれる。

合成データ（上記参照）は、再識別の可能なソリューションとしてしばしば提案される。しかし、合成データは実際のデータの元のデータセットから導出されるため、元のデータセットから多数の固有な特徴が残っている場合、再識別問題は依然として発生する可能性があるため万全ではない。モデルから受益者を再識別する可能性は、人道部門には特に関連性がある。人道部門では、悪意のある個人や組織が、脆弱な人々やグループを標的にしたり、傷つけたりすることを目的として、**人道団体**が収集したデータの入手を望む場合がある。また、**仮名化**、**匿名化**（可能な限り）および暗号化技術は、**データ主体**の再識別を回避し、身元の保護に役立つ場合がある。[468]暗号化と化仮名を組み合わせたり、合成データを使用したりすることで、保護層をさらに増やすことができる。これは、システムにアクセスする攻撃者は、復号化キーなしで取得した情報を「読み取る」ことができないためである。

トレーニングデータは、**人工知能**ソリューションの目的にも適合している必要がある。つまり、選択したデータは作業に関連している必要があり、不正確なデータや破損したデータを識別して訓練用のデータセットから削除するには、定期的な確認と更新が必要になる。偏向（3.2.2項参照）を回避するために、新しいデータを追加することもある。したがって、人道団体が開発者と協力して、彼らが獲得または開発したソリューションが、特定の文脈における組織のニーズに確実に適用され、適合するようにすることが重要である。

468 ノルウェー王国データ保護機関、2018年、p.18

人道団体はまた、特に意思決定を支援するために**人工知能**ソリューションを使用しようとする場合、「説明可能性」の問題について開発者と協力する必要があるだろう。彼らは、ソリューションがどのように機能するのか、どのようなリスクが発生するのか、**人工知能**システムがどのように結果に到達するのか、人間の意思決定者が必要に応じ決定や提案を確認できるように、どのような取り決めが準備されているのかについて、**データ主体**に説明できるべきである。

結論として、**人工知能**ソリューションの導入を選択する際、**人道団体**は、開発または調達プロセスの不可欠な部分として、データ保護・バイ・デザインに投資することが推奨される。これは、データ保護原則への準拠を確保するための最も効果的な方法である可能性が高い。

16.8 倫理上の問題と課題

技術が進化しているスピードと、法律が概して社会の大きな変化に遅れをとっていることを考えると、**人工知能**のソリューションに関連する倫理的な問題の中には、まだ既存の法律で対応されていないものがおそらく含まれている。このようなソリューションを開発または使用する場合、**人道団体**は当然ながら、データ保護法及びデータ保護・バイ・デザインの原則に準拠しているかどうかを考慮する必要がある。しかし、重要なことであるが、人道団体は、**データ主体**の様々な基本的権利に対する潜在的な悪影響、およびデータ**処理**の倫理的および社会的影響についても考慮すべきである。[469]

人工知能ツールには、差別的な偏向の可能性、責任の確立の困難さ、システム精度、およびプライバシー侵害の可能性など、多くのリスクが存在する。また、一部の開発者は、違法にまたは非倫理的な方法で入手したデータを使用していたシステムを訓練することがある。例えば、ユーザーが**人工知能**の訓練にデータを使用することに同意した場合にのみ、プラットフォームやサービスへのアクセスを許可するという方法である。このことは、特にそのようなプラットフォームやサービスのユーザーが脆弱なグループのメンバーであり、サービスにアクセスするために、企業が処理をするデータについて透明性を確保せずに同意する必要がある場合に懸念される。**人工知能**の倫理的な展開は、使用されたデータが一般に認められている人権基準に従って収集され、特定の個人および／またはグループの識別子が仮名化されていることを常に保証することを伴うだろう。

従来のデータ保護にとどまらず、より広範な関心、倫理基準及び権利（無差別の権利など）を対象とするリスク評価[470]は非常に重要である。社会的利益と倫理は法律よりも範囲が広く、

469 A. Mantelero、"Artificial Intelligence and Big Data: A blueprint for a human rights, social and ethical impact assessment"、Computer Law & Security Review、Vol. 34、Issue 4、2018 年、p.755：https://doi.org/10.1016/j.clsr.2018.05.017

470 Mantelero、2019年、p.13

人道団体は政治的、文化的なニュアンスを含むより広い文脈的背景を考慮する必要がある。このため、データ保護法だけでコンプライアンスを評価するよりも、倫理的価値を評価する方が複雑で、文脈依存しており、包括的である。

これまで、**人工知能**の開発に適用される倫理的原則を定義しようとする多くの試みがなされてきた。例としては、アシロマAI原則（Asilomar AI Principles）[471]、データ保護プライバシーコミッショナー国際会議での**人工知能**における倫理及びデータ保護についての宣言（International Conference of Data Protection and Privacy Commissioners' Declaration on Ethics and Data Protection in Artificial Intelligence）などがある。[472]学者は**人工知能**に関連する倫理問題の研究も行っており[473]、一部の多国籍企業は独自の倫理原則を策定している。現在のところ、これらのイニシアチブ全体の調和は見られず、ガイドラインの基準も統一されていないが、透明性、公正性、説明責任（上記3項参照）など、倫理と法律の両方にまたがる原則は、共通の基盤を提供しているようである。

人工知能が与え得る影響を考えると、「AI（**人工知能**）の世界で、倫理委員会への関心が高まっている」。[474]彼らは「開発者が権利ベースで社会指向のアルゴリズムを設計する上で貴重な支援を提供できる」からである。[475]そのような委員会の構成に関しては、「社会的な問題が重要な場合、法的、倫理的、社会学的な専門知識だけでなく、領域特化型の知識も不可欠である」。[476]したがって、**人道団体**は、**人工知能**ソリューションを展開する際に、このような問題への対処を支援する倫理委員会の設立を検討することができる。

コンプライアンスに法的・倫理的基準を保証するために、**人道団体**は以下の二つのステップを考慮すべきである。

- まず、DPIAの過程で次の3つの質問に答える必要がある。
  - 実際には何をすればいいのか
  - 何が法律で認められているのか
  - 技術的に可能なことは何か
- 第二に、新しい技術を採用する際には、人道団体が直面している問題と、**人工知能**がその問題の解決に役立つかどうかを、以下の質問をして検討する必要がある
  - どのような問題が**人工知能**で解決できるか

471 Future of Life Institute、"Asilomar AI Principles"：https://futureoflife.org/ai-principles/

472 データ保護・プライバシーコミッショナー国際会議、「人工知能における倫理及びデータ保護についての宣言」：http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf?mc_phishing_protection_id=28047-br1tehqdu81ea0ar3q10

473 例えば、近年脚光を浴びているACMの公正性、説明責任、透明性に関する会議(https://fatconference.org)、を参照

474 Mantelero、2019年、p.15

475 Mantelero、2019年、p.15

476 Mantelero、2019年、p.15

- どのような問題が解決できないか
- どのような問題が発生しているか
- このテクノロジーは、リスクの低い他のテクノロジーと比較してどのように機能するか

ゼロオプション（**人工知能**を使っていない）も常に念頭に置く必要がある。これは、**人工知能**の使用が合法だが倫理的には受け入れられない場合、特に関連性がある。例えば、人道団体が選択したソリューションが、プログラムの意図された対象となる受益者に十分に受け入れられない場合、この不快感や不信感は、技術を導入しないという決定を正当化できる可能性がある。

付属書Ⅰ

データ保護影響評価（DPIA）報告書のテンプレート

表紙

- 「アクティビティ名」に対するデータ保護の影響評価（DPIA）
- 担当者、役職、Eメールアドレス
- 日付

エグゼクティブサマリー

DPIAが20ページを超える場合は、エグゼクティブサマリーを収録する。エグゼクティブサマリーには、DPIAが実施された理由、誰のために、誰によって実施されたのか詳細を記載する。エグゼクティブサマリーには、主な調査結果と主な推奨事項を含める必要がある。

DPIA プロセスの紹介と概要

序文は、DPIAの範囲、いつ、なぜ、誰のために、誰によって実施されたかを概説する。評価された活動に関する情報を提供し、DPIAで採用された方法（例えば、利害関係者を関与させるために選ばれた方法）を紹介する。

閾値評価

このセクションでは、DPIAの必要性とDPIAの規模を決定するために人道団体が取り組んだ問題を列挙する。

評価される活動またはプロジェクトの記述

評価される活動の記述には、誰がその活動を実施しているか、およびいつ実施されるかを記載する。アクティビティの影響を受けるユーザー、あるいは、アクティビティに関心を持つ、またはアクティビティの影響を受ける可能性のあるユーザーを述べる必要がある。評価対象の活動の説明では、その活動が人道団体の他のサービスまたは活動とどのように適合するかについての文脈情報を提供すべきである。

情報フロー

このセクションでは、（少なくとも）に以下について詳しく説明する。

- 収集するデータのタイプ
- 機微情報を収集するかどうか
- データの収集方法
- データがどのような目的で使用されるか
- データの保存やバックアップの方法と場所
- 個人データへのアクセス権を持つユーザー
- 個人データの開示の有無
- 機微性の高い個人データの開示の有無
- データが他の組織や国に転送されるかどうか

法令・規制・規範・ガイドラインの遵守

DPIA報告書は、活動が遵守しているまたは遵守すべき法律、規制、行動規範及びガイドラインを識別する必要がある。グローバルなレベルでは、国際標準化機構（International Organization for Standardization: ISO）のISO/IEC 29100:2011規格に列挙されているプライバシー原則[477]がDPIAの参考資料として有用である。さらにDPIA報告書は人道団体の秘密保持に関する規則と行動規範の遵守状況、人道団体によるコンプライアンスの監視方法を記載すべきである。

ステークホルダー分析

報告書では、データの取扱いに関心を持ち、または影響を受ける主要な利害関係者は誰か、またDPIAまたは人道団体がどのようにしてこのリストを導き出したかを識別すべきである。

データ保護の影響（リスク）

本項では、関連する法律及び人道団体の秘密保持に関する規則および行動規範に規定されている主要なプライバシー原則に関連して識別されるプライバシーリスクについて詳述する。

リスクアセスメント

報告書の本項には、リスクがどのように評価されたのか、および実施したリスク評価の結果の詳細を含める。

組織の問題

DPIA報告書には、データ保護に関連する意思決定に上級管理職がどのように関与しているかを記述したセクションが必要である。これには、データ処理活動によって直接的または間接的に影響を受ける組織上の問題を識別する議論を含めるべきである。例えば、データ処理には、説明責任を確保するための組織的なメカニズムを整備することが必要であること、すなわち、上級管理者には、プログラムが人道団体やその利害関係者に悪影響を及ぼさないようにする責任があることが明らかになるかもしれない。

DPIAの過程で、人道団体はプライバシーや倫理問題に関する従業員の意識を高めるためにより多くの時間を費やす必要があり、人道団体は組織内でデータ保護を主流化する必要があることがDPIAチームの目に明らかになるかもしれない。報告書では、データ保護に対する従業員の意識を高めるために人道団体が現在何を行っているか、またどのようにしてそれを改善できるかについて記載すべきである。

報告書には、人道団体がデータ保護違反などのデータ保護インシデントをどのように識別、調査、対応するか、人道団体インシデントの影響を受ける当事者への通知方法をどのように決定したか、どのようにインシデントから学ぼうと努めているかを記述すべきである。

477 https://www.iso.org/standard/45123.html

このセクションでは、人道団体が、個人情報へのアクセスや収集した情報の訂正・修正の要請にどのように対応するか、また、データが誰に転送されるか、また、人道団体転送を行う前に、人道団体が主張するどのような保護措置が取られているかについても説明する必要がある。

協議の結果

報告書では、人道団体が利害関係者と協議し、潜在的なデータ保護の影響について意見やアイデアを収集するためにどのような努力をしたか、データ処理によって（肯定的および／または否定的に）どのような影響を受ける可能性があるか、負の影響をどのように緩和、回避、最小化、排除、移転、受け入れられるかを明記すべきである。

DPIAチームは、採用した協議手法（アンケート、インタビュー、フォーカスグループ、ワークショップなど）、実施時期、協議の結果、異なる手法を用いた場合に意見の相違が確認されたかどうかを明記する。

DPIAは、誰が相談を受けたか、行方不明者の家族を含む利害関係者に人道団体がどのような情報資料を提供したかを記載すべきである。

DPIAは、協議によって新たな知見が得られたかどうか、また情報処理活動の設計において利害関係者の見解および考えを考慮に入れるために人道団体が行った努力について記載する。

推奨事項

DPIAチームは、データ保護リスクを回避、最小化、移転、共有するための推奨事項を定める必要がある。リスクの中には取る価値があるものもあり、その場合、DPIAはその理由を述べるべきである。DPIAは誰がリスクを負うか明確にしなくてはならない（つまり、それは人道団体または利害関係者なのか、もしくはその他の人たちなのか）。DPIAはまた、その勧告を実施するためにどのような作業がさらに必要か、あるいは望ましいかを明確にすべきである（例えば、DPIAは勧告の中で独立した第三者による監視の必要性について言及する）。

DPIAは、DPIA報告書を公表するかどうかについても勧告を行うべきである。DPIAまたはその一部を公表することが適切でない状況があるかもしれない。例えば、守秘義務やセキュリティ上の理由がある状況である。多くの場合、報告書はどこかで編集され、公表されたり、機密扱いの付録に含まれたりする。もしくは、人道団体はDPIA報告書の要約を提供しても良い。

付属書Ⅱ

ワークショップ参加者

全てのワークショップは、ブリュッセルプライバシーハブと赤十字国際委員会（International Committee of the Red Cross: ICRC）が共催し、以下の団体の代表者が参加した。

- バークレイズ（Barclays）
- Belgian Privacy Commission（ベルギープライバシーコミッション）
- Biometrics Institute（バイオメトリクスインスティテュート）
- Brussels Privacy Hub（ブリュッセルプライバシーハブ）
- カナダ赤十字社（Canadian Red Cross）
- Cash Learning（キャッシュラーニング）
- 欧州評議会(Council of Europe)
- 欧州連合理事会(Council of the EU)
- Dalberg Data Insights（ダルバーグ・データ・インサイツ）
- EFTA監視機関（EFTA Surveillance Authority）
- Engine Room（エンジンルーム）
- 欧州委員会 ECHO総局（European Commission, DG ECHO）
- 欧州委員会 司法総局（European Commission, DG Justice）
- 欧州データ保護監督官（European Data Protection Supervisor）
- European UAV-Drones Area（欧州UAVドローン地域）
- Facebook（フェイスブック）
- フェアフォン（Fairphone）
- French-speaking Association of Personal Data Protection Authorities（フレンチスピーキング・アソシエーション・オブ・パーソナルデータプロテクション・オーソリティ）
- フランス共和国データ保護機関（French Data Protection Authority）
- ルクセンブルク政府（Government of Luxembourg）
- GSMA（ジーエスエムエー）
- ハーバード大学人道支援イニシアチブ（Harvard Humanitarian Initiative）
- ヒューマン・ライツ・ウォッチ（Human Rights Watch）
- ID 2020
- 赤十字国際委員会(International Committee of the Red Cross)
- 国際赤十字・赤新月社連盟（International Federation of the Red Cross and Red Crescent Societies）
- 国際移住機関（International Organization for Migration）
- ITU
- KU Leuven（KUルーベン）
- マスターカード（MasterCard）
- 国境なき医師団（Médecins Sans Frontières）
- Mercy Corps（マーシー・コープス）

- マイクロソフト（Microsoft）
- MIT
- オランダ赤十字社（Netherlands Red Cross）
- ノルウェー赤十字社（Norwegian Red Cross）
- オレンジビジネスサービス（Orange Business Services）
- オックスフォード大学（Oxford University）
- トリノ工科大学（Politecnico di Torino）
- プライバシーインターナショナル（Privacy International）
- クイーン・メアリー（ロンドン大学）（Queen Mary University of London）
- Royal Military Academy Belgium（ベルギー王立陸軍士官学校）
- Ryerson University-Privacy by Design Centre of Excellence（ライアソン大学：デザインセンター・オブ・エクセレンスによるプライバシー）
- センソメトリクス（Sensometrix）
- SES
- スペイン王国データ保護機関（Spanish Data Protection Agency）
- スイスデータ保護局（Swiss Data Protection Authority）
- スイス連邦工科大学ローザンヌ校（Swiss Federal Institute of Technology in Lausanne）
- 国連グローバル・パルス（UN Global Pulse）
- 国連プライバシー権特別報告者事務所（UN Office of the Special Rapporteur on the Right to Privacy）
- 国連難民高等弁務官事務所（United Nations High Commissioner for Refugees）
- 国連人道問題調整事務所（United Nations Office for the Coordination of Humanitarian Affairs）
- ジュネーブ大学（University of Geneva）
- 米国国際開発庁（USAID）
- VIVES University College（ヴィベス大学カレッジ）
- ブリュッセル自由大学（Vrije Universiteit Brussel）
- 国連世界食糧計画（World Food Programme）
- ワールド・ビジョン・インターナショナル（World Vision International）
- イェール大学（Yale University）

おわりに

本書は、Christopher Kuner、Massimo Marelliの共編者により、ブリュッセル・プライバシー・ハブ (BPH)と赤十字国際委員会(ICRC) が発刊した「Handbook on Data Protection in Humanitarian Action : Second Edition」を日本語に翻訳したものです。

日本語版の発行にあたり、以下の方々に改めて謝意を表します。

- 日本語版編集作業に携わっていただいた日本赤十字社語学奉仕団の芦村和男氏、天野八重子氏、佐藤有氏、柴田ひさ氏、清水靖子氏、田貝征之氏、中久保慎一氏、箱守友子氏、松宮会里氏
- 日本語版を技術的見地から監修いただいた日本電気株式会社 (NEC) 久木田信哉氏、坂本静生氏、寺田亜紀子氏

最後に、日本語版を監訳していただいた中央大学教授の宮下紘氏に、心よりの感謝を申し上げます。

なお、原版（英語）については、以下のサイトからPDF版が無料でダウンロードできます。
https://www.icrc.org/en/data-protection-humanitarian-action-handbook

日本語版発行者
赤十字国際委員会（ICRC）駐日代表部

日本語版監訳
宮下紘／中央大学総合政策学部 教授

日本語版編集人
冨田麻美子／赤十字国際委員会（ICRC）駐日代表部　企画調整官

赤十字国際委員会(ICRC)は、公平で中立、かつ独立した組織で、武力紛争およびその他暴力の伴う事態によって犠牲を強いられる人々の生命と尊厳を保護し、必要な援助を提供することをその人道的使命としています。ICRCは、国際人道法および世界共通の人道の諸原則を普及させ、また強化することによって人々に苦しみが及ばないよう尽力しています。

ICRC

facebook.com/ICRC.jp
twitter.com/ICRC_jp　　instagram.com/icrc

赤十字国際委員会（ICRC）駐日代表部
〒107-0052
東京都港区赤坂1-11-36
レジデンスバイカウンテス#320
jp.icrc.org

ISBN 978-2-940396-92-4