

人道支援における データ保護ハンドブック

第3版



人道支援におけるデータ保護ハンドブック

このハンドブックは、個人データ保護に関する法律やそれが人道団体に及ぼす重要性について、包括的かつわかりやすい分析を提供する基礎的なテキストです。長年にわたる個人データ保護の原則に関する研究の成果をまとめ、最も脆弱な人々の権利と尊厳を守るために人道団体がいかにこの原則を用いることができるかを解説しています。新しい技術の急速な進化を反映し、人道支援の文脈における技術利用がもたらす影響について詳細な分析を提供しています。データ保護の重要性について認識を高め、人道団体が保有する個人データを、個人データ保護の原則と要件に準拠して責任ある方法で処理するための実践的な方法を提示しています。最新の調査研究と文脈に応じたアドバイスにより、人道分野の実務者および法曹、データ保護当局、ならびに人道分野および個人データ保護の分野の研究者にとって非常に重要なリソースとなることでしょう。本ハンドブックは、Cambridge Coreのオープンアクセスでも利用可能です。

編者のMassimo Marelliは、赤十字国際委員会 (ICRC) のデータ保護局長であり、マーストリヒト大学のプライバシー・サイバーセキュリティ欧州センターの諮問委員会メンバー兼客員研究員でもあります。

人道支援における データ保護ハンドブック

Massimo Marelli 編

第3版

このハンドブックは以下の機関に採用されています。



目次

- 寄稿者一覧 12
- 第3版の序文..... 17
- Christopher Kuner*
- 初版および第2版の序文..... 19
- Jean-Philippe Walter*
- 謝辞 21
- 定義された用語と略語の用語集 25
- 1. はじめに 35
 - 1.1 背景 36
 - 1.2 目的 36
 - 1.3 構成とアプローチ 41
 - 1.4 ターゲットオーディエンス 42
- PART I 人道支援におけるデータ保護の基本原則 45
- Massimo Marelli*
- 2. データ保護の基本原則..... 47
 - 2.1 はじめに..... 48
 - 2.2 基本的なデータ保護概念 51
 - 2.3 集計化、仮名化、および匿名化されたデータセット 53
 - 2.4 適用法および国際機関..... 56
 - 2.5 データ処理の原則..... 57
 - 2.5.1 公平性の原理と処理の適法性 57
 - 2.5.2 目的制限の原則 57
 - 2.5.3 均衡性の原則 60
 - 2.5.4 データ最小化の原則 62
 - 2.5.5 データの質の原則 63
 - 2.6 特殊なデータ処理の状況 64
 - 2.6.1 保健目的 64
 - 2.6.2 管理活動 65
 - 2.7 データ保全 65
 - 2.8 データセキュリティと処理のセキュリティ..... 66
 - 2.8.1 はじめに..... 66
 - 2.8.2 物理的セキュリティ 68
 - 2.8.3 IT セキュリティ..... 69
 - 2.8.4 配慮義務および職員の行動 70
 - 2.8.5 緊急時対応計画 71
 - 2.8.6 破壊方法 71
 - 2.8.7 その他の措置 73
 - 2.9 説明責任の原則..... 73
 - 2.10 情報 74

2.10.1	データ主体から収集されたデータ	74
2.10.2	情報通知	75
2.10.3	データ主体から収集されないデータ	76
2.11	データ主体の権利	77
2.11.1	はじめに	77
2.11.2	アクセス	78
2.11.3	訂正	79
2.11.4	削除権	80
2.11.5	異議申立権	81
2.12	データ共有と国際的なデータ共有	81
3.	個人データ処理の法的根拠	85
3.1	はじめに	86
3.2	同意	87
3.2.1	明確性	88
3.2.2	タイミング	89
3.2.3	有効性	89
3.2.4	脆弱性	89
3.2.5	子ども	90
3.2.6	通知	91
3.2.7	文書化	91
3.2.8	同意の保留 / 撤回	92
3.3	生命に関わる利益	92
3.4	公益という重要な根拠	94
3.5	正当な利益	95
3.6	契約の履行	96
3.7	法的義務の遵守	97
3.7.1	当局への個人データの開示	98
4.	国際的なデータ共有	101
4.1	はじめに	102
4.2	国際的なデータ共有のための基本ルール	104
4.3	国際的なデータ共有の法的根拠の提供	104
4.3.1	はじめに	104
4.3.2	国際的なデータ共有の法的根拠	105
4.4	個人にとってのリスク低減	105
4.4.1	適切な保護措置 / 契約条項	107
4.4.2	説明責任	108
4.5	データ管理者とデータ処理者の関係	109
5.	データ保護影響評価 (DPIAS)	111
5.1	はじめに*	112
5.2	DPIA プロセス	113
5.2.1	DPIAは必要か	114
5.2.2	DPIA チーム	114
5.2.3	個人データの処理の記述	114
5.2.4	利害関係者との協議	115
5.2.5	リスクの特定	116
5.2.6	リスクの評価	116

5.2.7	ソリューションの特定	118
5.2.8	勧告の提案	120
5.2.9	合意された勧告の実施	121
5.2.10	DPIAの専門家による審査および / または監査の実施	121
5.2.11	プロジェクトに変更がある場合は DPIAを更新	121

PART II 特定の処理の状況、テクノロジーおよびテクノロジー分野 123

6. データ保護のための設計 125

Carmela Troncoso et Wouter Lueks

6.1	はじめに	126
6.1.1	システムとは何か	128
6.2	ケーススタディ：プライバシー保護を重視した接触追跡アプリ	128
6.2.1	分散型のプライバシー保護を重視した接近追跡	130
6.3	目的制限による個人とその尊厳および権利の保護	132
6.3.1	目的の決定が重要である理由	134
6.3.2	目的の決定	138
6.3.3	目的制限の分析	140
6.4	データ最小化の役割	146
6.5	目的制限に対する課題	148

7. ドローン／無人航空機とリモートセンシング 151

Massimo Marelli

7.1	はじめに	152
7.2	データ保護基本原則の適用	156
7.2.1	個人データ処理の法的基盤	157
7.2.2	透明性 / 情報	160
7.2.3	目的制限と追加処理	161
7.2.4	データの最小化	161
7.2.5	データ保全	162
7.2.6	データセキュリティ	163
7.3	データ主体の権利	163
7.4	データ共有	165
7.5	国際的なデータ共有	166
7.6	データ管理者とデータ処理者の関係	167
7.7	データ保護影響評価	167

8. バイオメトリクス 171

Massimo Marelli

8.1	はじめに	172
8.2	データ保護基本原則の適用	175
8.2.1	個人データ処理の法的基盤	177
8.2.2	公正かつ適法な処理	180
8.2.3	目的制限と追加的処理	181
8.2.4	データの最小化	182
8.2.5	データ保全	183
8.2.6	データセキュリティ	184
8.2.7	本質的な「過剰性」	184
8.3	データ主体の権利	185

8.4	データ共有	185
8.5	国際的データ共有	186
8.6	データ管理者とデータ処理者の関係	186
8.7	データ保護影響評価	187
9. 現金およびバウチャー支援		191
<i>Massimo Marelli</i>		
9.1	はじめに	192
9.2	データ保護基本原則の適用	197
9.3	データ保護の基本原則	199
9.3.1	個人データ処理の法的根拠	199
9.3.2	目的制限と追加処理	201
9.3.3	データの最小化	203
9.3.4	データ保全	204
9.3.5	データセキュリティ	205
9.4	データ主体の権利	206
9.5	データ共有	206
9.6	国際的なデータ共有	208
9.7	データ管理者とデータ処理者の関係	208
9.8	データ保護影響評価	209
10. クラウドサービス		213
<i>Paolo Balboni</i>		
10.1	はじめに	214
10.2	データ管理者とデータ処理者の関係	218
10.3	クラウドにおける責任と説明責任	219
10.4	データ保護基本原則の適用	220
10.4.1	個人データ処理の法的根拠	220
10.4.2	公正かつ適法な処理	221
10.4.3	目的制限と追加的処理	222
10.4.4	透明性	222
10.4.5	データ保全	223
10.5	データセキュリティ	225
10.5.1	転送中データの保護	230
10.5.2	資産の保護	230
10.5.3	ユーザー間の分離	232
10.5.4	ガバナンス	233
10.5.5	オペレーショナルセキュリティ	233
10.5.6	人材	234
10.5.7	開発	234
10.5.8	サプライチェーン	234
10.5.9	ユーザー管理	235
10.5.10	アイデンティティと認証	235
10.5.11	外部インターフェース	235
10.5.12	サービス管理	236
10.5.13	監査	236
10.5.14	サービスの使用状況	236
10.6	データ主体の権利	237

10.7	国際的なデータ共有	237
10.8	データ保護影響評価	238
10.9	特権および免除とクラウド	238
10.9.1	法的措置	239
10.9.2	組織的措置	239
10.9.3	技術的措置	240
10.10	行動規範	240

11.0 クラウド、および政府によるアクセス..... 243

Andrea Raab-Gray

11.1	政府によるサービスプロバイダへの人道データ開示要求を可能にする法律について	246
11.1.1	国家安全保障を目的とした、政府によるサービスプロバイダへの人道データの開示強制を可能とする法的枠組み	247
11.1.2	刑事訴訟手続を目的とした、政府によるサービスプロバイダへのデータ開示強制の法的枠組み	252
11.2	人道支援およびその恩恵を受ける人々に対する強制的開示の影響	259
11.3	パブリッククラウドで処理される人道データの開示リスクの軽減	261
11.3.1	特権および免除の実効性の確保	262
11.3.2	国に対し、人道データを人道団体の任務とは異なる目的で使用またはしないことの重要性を認識させる	266

12. モバイルメッセージングアプリ..... 269

Lina Jasmontaite-Zaniewicz

12.1	はじめに	270
12.1.1	人道支援のためのモバイルメッセージングアプリ	272
12.2	データ保護基本原則の適用	275
12.2.1	モバイルメッセージングアプリを使用した個人データの処理	275
12.2.2	メッセージングアプリが収集し保管するデータの種類	277
12.2.3	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	281
12.2.4	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	285
12.2.5	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	288
12.3	個人データ処理の法的根拠	289
12.4	データ保全	290
12.5	データ主体の訂正および消去の権利	291
12.6	データの最小化	292
12.7	目的制限と追加処理	293
12.8	データの管理、分析および検証	294
12.9	データ保護バイデザイン	295
12.10	国際的なデータ共有	296

13. デジタルアイデンティティ..... 299

Vincent Graf Narbel

13.1	はじめに	300
13.1.1	認証、識別、照合：どうすれば自分の存在を証明できるのか	303
13.1.2	デジタルアイデンティティ	304
13.1.3	システム設計とガバナンス	305
13.1.4	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	308

13.1.4	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	310
13.2	データ保護影響評価	311
13.3	データ保護バイデザインおよびデータ保護バイデフォルト	312
13.4	データ管理者とデータ処理者の関係	313
13.5	データ主体の権利	314
13.5.1	アクセス権	315
13.5.2	訂正および削除の権利	316
13.6	データ保護基本原則の適用	317
13.6.1	個人データ処理の法的根拠	317
13.6.2	目的制限と追加的処理	318
13.6.3	均衡性	318
13.6.4	データの最小化	319
13.6.5	データ・セキュリティ	319
13.6.6	データ保全	320
13.7	国際的なデータ共有	321
14.	ソーシャルメディア	323
	<i>Júlia Zomignani Barboza と Lina Jasmontaite-Zaniewicz*</i>	
14.1	はじめに	324
14.1.1	人道支援分野におけるソーシャルメディア	324
14.1.2	ソーシャルメディアとデータ	327
14.2	データ保護影響評価	335
14.3	倫理的問題とその他の課題	337
14.4	データ管理者とデータ処理者の関係	340
14.5	データ保護基本原則	342
14.5.1	個人データ処理の法的根拠	342
14.5.2	情報	343
14.5.3	データ保全	344
14.5.4	データセキュリティ	346
14.6	国際的なデータ共有	346
15.	ブロックチェーン	349
	<i>Vincent Graf Narbel</i>	
15.1	はじめに	350
15.1.1	ブロックチェーンとは	350
15.1.2	ブロックチェーンのタイプ	354
15.1.3	ブロックチェーンの実務	357
15.1.4	人道支援における使用例	359
15.2	データ保護影響評価	361
15.3	データ保護バイデザインおよびデータ保護バイデフォルト	363
15.4	データ管理者とデータ処理者の関係	365
15.5	データ保護の基本原則	368
15.5.1	データの最小化	368
15.5.2	データ保全	368
15.5.3	均衡性	369
15.5.4	データセキュリティ	369
15.6	データ主体の権利	371
15.6.1	アクセス権	371

15.6.2	訂正する権利	372
15.6.3	削除権	373
15.6.4	データ主体の権利の制限	374
15.7	国際的なデータ共有	374
15.8	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	376

16. 援助としての接続性..... 383

Aaron Martin と John Warnes

16.1	はじめに	384
16.1.1	支援介入としての接続性の概要	385
16.1.2	運営の事情	387
16.1.3	複数のステークホルダーとのパートナーシップ	388
16.2	データ保護影響評価	391
16.3	データ管理者とデータ処理者の関係	393
16.4	データ保護の基本原則	394
16.4.1	個人データ処理の法的根拠	394
16.4.2	データセキュリティ	395
16.4.3	データ保全	397
16.4.4	情報	398
16.5	国際的なデータ共有	399

17. 人工知能..... 401

Alessandro Mantelero

17.1	はじめに	402
17.1.1	人工知能とは何か、どのように機能するか	402
17.1.2	人道支援分野における人工知能	408
17.1.3	人工知能を使用する際の課題とリスク	415
17.2	データ保護基本原則の適用	418
17.2.1	個人データ処理の法的根拠	419
17.2.2	目的制限と追加処理	423
17.2.3	公正かつ適法な処理	426
17.2.4	透明性	431
17.2.5	データの最小化	433
17.2.6	データ保全	435
17.2.7	データセキュリティ	436
17.3	データ主体の権利	438
17.3.1	自動化された意思決定に関する権利	438
17.4	データ管理者とデータ処理者の関係	441
17.4.1	説明責任	442
17.4.2	責任	442
17.5	国際的なデータ共有	444
17.6	データ保護影響評価と人権影響評価	446
17.6.1	人工知能に関する人権影響評価	448
17.6.2	人権影響評価：段階と手順	449
17.7	データ保護バイデザインとデータ保護バイデフォルト	454
17.8	倫理上の問題と課題	454

付録I：データ保護影響評価（DPIA）報告書のテンプレート	459
付録II：ワークショップ参加者	467

寄稿者一覧

Massimo Marelliは、赤十字国際委員会（ICRC）のデータ保護局長である。彼は、マーストリヒト大学のプライバシーおよびサイバーセキュリティ欧州センターの諮問委員会のメンバーおよび客員研究員であり、ブリュッセル自由大学のブリュッセル・プライバシー・ハブ諮問委員会のメンバーも務めている。彼はケンブリッジ大学ローターパクト国際法センターの客員研究員であり、欧州原子核研究機構（CERN）のメンバーも務める。ICRCのデータ保護局長に就任する前は、ICRCのデレゲートとして現場で活躍していた他、欧州連合一般裁判所の審判員や、またロンドンとブリュッセルで独占禁止法とEU法を専門とする個人事業弁護士を務めた。

Carmela Troncosoは、スイス連邦工科大学ローザンヌ校（EPFL）（スイス）の助教であり、そこでSPRING研究室の代表を務めている。彼女は、ビーゴ大学で電気通信工学の修士号（2006年）、ルーヴェン大学で工学博士号（2011年）を取得している。EPFLに加わる前はIMDEA Software Institute（スペイン）で2年間教員を務めていた。また、Gradientのセキュリティおよびプライバシーテクニカルリードを4年間務め、業界と緊密な関係を持ち、安全でプライバシーに配慮したソリューションを市場に提供した。COSICグループの博士研究員を務めた経験も持つ。彼女の研究はセキュリティとプライバシーにフォーカスしたものである。彼女の論文「Design and Analysis Methods for Privacy Technologies（プライバシーテクノロジーの設計と分析手法）」は、欧州情報学および数学セキュリティおよびトラストマネジメント研究コンソーシアムの最優秀博士論文賞を受賞している。また、プライバシーエンジニアリングに関する彼女の研究は2017年CNIL-INRIAプライバシー保護賞を受賞した。彼女は、セキュリティ（コンピュータセキュリティに関するACMカンファレンス、USENIXセキュリティシンポジウムなど）やプライバシー（プライバシー強化テクノロジー）の最も権威ある場で定期的に論文を発表している。

Wouter Lueksは、2022年末にドイツのザールブリュッケンにあるCISPAヘルムホルツ情報セキュリティセンターに入所し、教員を務めている。それ以前は、スイス、ローザンヌのEPFLの博士研究員を務めており、SPRING研

究室のCarmela Troncosoとは協力関係にあった。彼は、エンドツーエンドのプライバシーに配慮したシステムを設計することで現実世界の問題を解決することに興味を持っており、そのために、プライバシー、応用暗号学、システムを組み合わせた研究を行っている。彼が設計した、プライバシーに配慮した接触者追跡は世界の数百万台ものスマートフォンに導入されており、同じく彼が設計した安全な文書検索システムは、ある大規模組織に導入され、調査ジャーナリストのために役立てられている。

Paolo Balboni (PhD) は、マーストリヒト大学法学部内にあるプライバシーおよびサイバーセキュリティ欧州センター (ECPC) のプライバシー、サイバーセキュリティ、IT 契約法の教授を務めている。彼は欧州特許庁 (EPO) データ保護委員会の委員長を務め、EUMETSAT データ保護監督局のメンバーでもある。ICT、プライバシーおよびサイバーセキュリティ、知的財産を専門とする弁護士として、ミラノ法曹界で資格を取得しており、アムステルダム法曹界にも登録されている。国際法律事務所 ICT Legal Consulting (ICTLC) と、情報・データセキュリティを専門とする企業 ICT Cyber Consulting の創設パートナー。彼は、データプライバシーとデータ保護分野、電気通信、メディア、テクノロジー業種において、Legal 500 EMEA 2021で推奨弁護士にランクインしている。彼の主な研究内容は、企業の社会的責任としてのデータ保護である。これは、組織による責任ある経済目標の達成を支援すると同時に、公正なデータ中心社会の発展に積極的に寄与するために利用できるものである。教授はさらに、サイバーセキュリティとプライバシーに関する国家問題について複数の政府に助言を行っており、2018年にはスリナムのプライバシーおよびデータ保護法を起草した。

Andrea Raab-Gray は現在、オーストリア共和国連邦欧州国際問題省の法律顧問局で法律専門家として働いている。入省前は、ジュネーブとロンドンで ICRC の法律顧問を務めていた。彼女はまた、国際刑事法廷残余メカニズムや、ハーグに拠点を置く、性的およびジェンダーに基づく暴力と闘う非政府組織ジェンダー正義のための女性イニシアチブにおいては、セオドル・メロン判事と協力している。彼女はオックスフォード大学を優秀な成績で卒業。同大学の法学マギスター過程で学び、ウィーン大学で法学位を取得した。

その功績により、オックスフォード・グローバル・ジャスティス・インターンシップ基金や国際紛争解決におけるヴォルテラ・フィエッタ賞など、数多くの奨学金や賞を獲得した。

Lina Jasmontaite-Zaniewiczはブリュッセル自由大学の博士号取得候補生である。彼女はブリュッセル・プライバシー・ハブの寄稿フェローおよび教育コーディネーターであり、個人のプライバシー権やデータ保護権に関する新しい法律制定イニシアチブの法的影響などのトピックを研究している。彼女の博士課程の研究は主に、一般データ保護規則で予測される個人データ侵害通知義務に関するものである。彼女は、人権保護、新技術に関する規制（デジタルアイデンティティウォレットや人工知能（AI）など）、サイバーセキュリティに関するトピックについて論文を執筆している。

Vincent Graf Narbelは、民間企業で15年以上勤務した後（ソフトウェア開発者からソリューションアーキテクト、サービスマネージャーまでさまざまな役職を歴任）、2015年にICRCのICTイノベーション担当官として加わった。現在は、ICRCデータ保護室で戦略的技術顧問を務める。彼は、プライバシー、セキュリティ、倫理全般を専門とし、人道分野での新しいテクノロジーの導入に注力しており、人道支援におけるデータ保護作業シリーズ、特にバイオメトリクス、デジタルアイデンティティ、人工知能、ブロックチェーンの分野に積極的に参加した。また、これらの分野におけるいくつかの研究プロジェクトで共同リーダーを務めている。EPFL（スイス）で数学の修士号を取得。

Júlia Zomignani Barbozaは2012年にブラジルの大学で法学を修め、さまざまな法律の分野でインターンシップやボランティアの職を経験している。ジュネーブアカデミーで国際人道法と人権で法学修士号を取得。ジュネーブでは、人権非政府組織（NGO）Alkaramaで法律研究者として、またICRCでアソシエイトとして働く。ブリュッセル自由大学の前は、バンコクで亡命希望者や難民の法権利の擁護者として、またシドニーで亡命を扱う法務アシスタントとして働いていた。2018年10月にブリュッセル自由大学の博士号取得候補生となる。彼女の博士号研究は、ノン・ルフールマンの原則に違反せずに出身国に送還することができない移民（犯罪（容疑）者）の扱いに焦点を当

てたものである。同時に彼女は、移民、人道問題、データ保護をテーマとした複数の研究プロジェクトに貢献している。

Aaron Martinは、バージニア大学でメディア研究およびデータサイエンスの助教授を務めている。以前は、マーストリヒト大学で国際法および欧州法の助教授、ティルブルフ法・技術・社会研究所 (TILT) で博士研究員を務め、金融サービスセクターの、サイバーガバナンスとテクノロジー規制の分野で働いていた。また、欧州協力開発機構 (OECD)、欧州委員会、Vodafone グループの技術政策分野でも活躍。グローバルサイバーセキュリティキャパシティセンターのオックスフォードマーティンアソシエイトも務める。ロンドン・スクール・オブ・エコノミクス・アンド・ポリティカル・サイエンスで情報システムとイノベーションの博士号を取得している。

John Warnesは、国連難民高等弁務官事務所 (UNHCR) のイノベーションサービス内でデジタルインクルージョンプログラムの責任者を務めており、すべての難民と彼らを受け入れるコミュニティが、つながった社会に参加するという権利と選択を確保できるように、強力なパートナーシップを仲立ちし、解決策を進めることに重点を置いている。前職では、UNHCRの活動をサポートする、テクノロジーソリューションの設計と導入に従事しており、緊急時のコミュニティとのコミュニケーションや、難民の同組織とのつながりに関して取り組んできた。災害の影響を受けたコミュニティとのコミュニケーション (CDAC) ネットワークに協力し、コミュニティの関与と、影響を受けた人々への責任に関するセクター全体の問題を調査した経験も持つ。彼はまた、民間の電気通信会社での勤務実績、ベルリンのNGOトランスペアレンシーインターナショナルで透明性と説明責任の問題に取り組んだ実績も持っている。彼はバース大学で政治学の学士号を取得し、サウサンプトン大学でITおよび電気通信法の法学修士号を取得している。

Alessandro Manteleroは、トリノ工科大学の教壇に立つ、私法および、法律と技術の助教である。彼は、AI、データ保護、人権に関する欧州評議会の科学専門家 (人工知能に関する特別委員会 - CAHAI、条約108- 諮問委員会) であり、データ規制の専門家として、国連、EU 基本権庁、欧州委員会など、数々の国立・国際機関で働いてきた。ハーバード

大学バークマン・クライン・インターネットおよび社会センター、南京情報科学大学（NUIST）、オベルタ・デ・カタルーニャ大学、ムルシア大学などにも招かれており、2013年と2014年には、オックスフォード大学のオックスフォード・インターネット研究所のリサーチフェローとして、データ保護とビッグデータの研究に取り組んだ。Computer Law & Security Reviewの副編集長であり、European Data Protection Law Reviewの編集委員も務める。最新の著書は『Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI（データを超えて：AIにおける人権、倫理的および社会的影響の評価）』（T.M.C. Asser Press – Springer、2022年）。2022年には、欧州連合研究における卓越性が認められ、欧州委員会から、地中海デジタル社会と法律分野に関するジャン・モネ・チェアの称号を授与された。

第3版の序文

CHRISTOPHER KUNER

人道団体の活動には**個人データ**の処理が必要である。こうした団体は、迫害や自然災害に直面している人々を支援するため、可能な限り効果的かつ効率的に働く必要があるため、彼らの**個人データ**の処理を保護することは文字通り生きるか死ぬかの問題となる可能性がある。**データ処理**（特にオンラインで実行される処理）は、大きなメリットもあるものの、データ悪用の可能性やサイバーセキュリティの脅威などのリスクをももたらす。これが、人道団体が任務を果たすためにデータ保護が不可欠である理由であり、また、このことが関係者からますます期待されている理由でもある。

赤十字国際委員会（ICRC）とブリュッセル・プライバシー・ハブはすでに、人道支援におけるデータ保護に関するハンドブックを第2版まで共同出版しており、私はその共同編集者であることを誇りに思う。これらは、人道分野で活動する組織が業務にデータ保護を導入するためのガイダンスを提供するものである。しかし出版以後、データの悪用、セキュリティ侵害、不正な**データ処理**のリスクは増大し続け、**データ処理**を巡る新たな法的問題が浮かび上がり、それにしただがって人道団体の課題も増大し続けている。

そのため、ICRCのMassimo Marelliがこのハンドブックの第3版を編集したことを非常に喜ばしく思う。データ保護の導入における法的および実務的な複雑さが増大していることを考慮すると、この新版の編集は必要なことであるといえる。この版では、最初の2版では扱わなかった、リスク軽減、デジタル接触追跡、政府によるアクセスなどの追加トピックも取り上げている。また、関連する法的問題と人道団体が直面する実際的な課題についてもさらに詳しく説明している。

データ保護は、**データ処理**に対する脅威に対処するため、進化を続ける必要がある。このハンドブックの第3版は、人道団体が弱い立場にある人々のデータを保護し、その使命を果たすための重要なツールとなるだろう。

Christopher Kuner

ブリュッセル自由大学、ブリュッセル・プライバシー・ハブ 元共同ディレクター
ベルギー、ブリュッセル

人道支援におけるデータ保護ハンドブック初版および第2版の共同編集者

2022年2月

初版および第2版の序文

JEAN-PHILIPPE WALTER

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、欧州評議会のデータ保護コミッショナーであり、ICRCのデータ保護委員会のメンバーでもある。彼は、元スイス連邦データ保護副コミッショナーであり、フランス語圏個人データ保護当局協会会長および、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・アセンブリー）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。

謝辞

本ハンドブックの初版および第2版は、ベルギーのブリュッセルにあるブリュッセル自由大学の学術研究センター、ブリュッセル・プライバシー・ハブのChristopher Kuner教授と私が編集した共同出版物であり、本書はその第3版にあたる。

したがって何よりもまず、「人道支援におけるデータ保護」作業シリーズの共同招集者として、また、その結果として完成させることができた初版と第2版の共同編集者として、重要な役割と貢献を果たしてくださったChristopherに感謝の念を示したいと思う。長年にわたる彼の指導、知見、専門知識、助言は、ハンドブックの強固な基盤となり、この出版物の精神を導き続けている。

この第3版には、第2版の発行以来に明らかになった重要なニーズを満たす、新しい2つのガイダンスの章が含まれている。これらの新しい章のうち1番目の章では、Carmela TroncosoとWouter Lueksが、データ保護の設計に取り組む方法、および最初からデータ保護機能を組み込んでプログラムとシステムを設計する方法についてのガイダンスを提供する。この章は、PART IIで説明されるすべての技術分野に関連する極めて重要な部分である。2番目の新章では、Andrea Raab-Grayが、クラウドベースのツールを使用する人道団体が直面する課題と、収集したデータを排他的管理下に置き、人道目的のみに使用できるようにする方法について詳しく考察している。より具体的には、クラウドサービスプロバイダなどの**第三者**処理者を介した、政府による人道データへの「合法的な」アクセスが行われる可能性のあるソースを分析する方法についてのガイダンスを提供する。

他の既存の章についてはすべて、章の執筆に主にまたは大きく携わった著者が、最新の傾向、さらなる研究、分析を加え、最新の内容になるよう更新している。この版の本文は、原稿送信日である2022年12月10日時点で最新のものである。

したがって、この第3版の各章を監修してくださった共著者の方々、Carmela Troncoso、Wouter Lueks、Paolo Balboni、Andrea Raab-Gray、Lina Jasmontaite-Zaniewicz、Júlia Zomignani Barboza、Vincent Graf Narbel、Alessandro Mantelero、Aaron Martin、John Warnesにも感謝の念を示したいと思う。本版のハンドブックと、それに関連する多くの取り組みやプロジェクトで彼らと協力できたことは、大変光栄なことであった。

前版と同様、本版も、協議会、ワークショップ、インタビュー、パネルディスカッション、カンファレンスを通じて提供された知見から大きな恩恵を受けている。特に、学界の専門家、データ保護当局とプライバシー委員、人道活動家、寄付者、市民社会、民間セクターの人々など、広範で多彩なステークホルダーが集まった、2021年開催のDigitHariumワーキングシリーズ¹からはさまざまな知見がもたらされた。

また、以前の版と同様、作業中の原稿は諮問グループによって査読され、途中で多くの活発な議論が行われた。本版の諮問グループのメンバーは以下のとおりである。

- Christopher Kuner (元ブリュッセル自由大学)
- Cosimo Monda、Herke Kranenborg (マーストリヒト大学 欧州プライバシーおよびサイバーセキュリティセンター)
- Michèle Finck (テュービンゲン大学)
- Nathaniel Raymond (イエール大学)
- Carmela Troncoso (スイス連邦工科大学ローザンヌ校 (EPFL))
- Catherine Lennman (スイスデータ保護局、プライバシーと国際人道援助および国際開発に関するグローバル・プライバシー・アセンブリー作業部会)
- Claire-Agnes Marnier、Olivier Matter、Petra Candellier (欧州データ保護監督官)
- Marine Revel (フランス語圏個人データ保護当局協会)

1 ICRC, 'DigitHarium', ICRC, 2021, www.icrc.org/en/digitharium.

- Irina Conovali、Abtin Kronold（国連難民高等弁務官事務所（UNHCR））
- Christina Vasala Kokkinaki（元国際移住機関（IOM）、現国際電気通信連合（ITU））
- Lucie Laplante、James De France（国際赤十字・赤新月社連盟）
- Stuart Campo（元国連人道問題調整事務所（OCHA））
- Alexandrine Pirlot de Corbion（プライバシー・インターナショナル）
- Mary Nunn（元国境なき医師団（MSF）、紛争関連の性的暴力生存者のためのグローバル基金）
- Max Lamesch、Catherine Kayser（ルクセンブルク外務省）
- Gilles Cerutti、Jonas Belina（スイス連邦外務省）

この第3版の実現に貢献してくださったケンブリッジ大学出版局、特に Marianne Nield 氏、そしてこのハンドブックのプロジェクトを献身的かつ巧みにマネジメントしてくれた同僚の Silvia Pelucchi と Chloe Jensen にも深く感謝の念を伝えたい。

長年にわたり、人道支援におけるデータ保護の分野における私たちの取り組みは、ルクセンブルク外務省とスイス連邦外務省による大いなる支援のおかげで順調に続けられてきた。本ハンドブック第3版は、その具体的な成果の1つである。

デジタル変革において人道支援が直面する新たな傾向やジレンマを見つけ出し、予測し、対処するために必要な知識と知見を提供し続けている多くのすばらしいコミュニティの継続的な熱意と貢献に、私は非常に感謝している。第一に、人道支援実践者のコミュニティ、すなわち、赤十字国際委員会、各国赤十字・赤新月社、国際赤十字・赤新月社連盟、国連機関、人道支援現場の最前線で活動するその他の組織の献身的な職員たちだ。彼らは、人道危機にさらされた弱い立場にあるコミュニティのために新技術の恩恵を最大限に利用すると同時に、コミュニティの保護、尊厳、主体性を確保するという絶え間ない使命に取り組み、人道危機がもたらす異常な状況においてガイダンスが有意義で現実的なものであるよう、現場の状況に即した「リアリティチェック」を行ってくださった。第二に、データ保護監督当局と専門家のコミュニティは、

個人データの自動処理に係る条約、第108号（T-PD）に関するグローバル・プライバシー・アセンブリーおよび欧州評議会個人保護諮問委員会の枠組み内において、新しいテクノロジーやテクノロジー分野への主要なデータ保護ルールの適用に関するガイダンスの交換、考察、開発のための知見に満ちたスペースを提供してくださった。第三に、マーストリヒト大学の欧州プライバシーおよびサイバーセキュリティセンターとローザンヌ工科大学とチューリッヒ工科大学の学術コミュニティは、それぞれが法律とコンピューターサイエンスにおいて比類のない最先端の専門知識を持っており、学术界が提供できる、制約のない先進的な環境を提供してくださった。

以前の版に関連するクレジットと謝辞は、その場所に記載される。

Massimo Marelli

2022年11月、ジュネーブ

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。² 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」³ 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。」⁴

現金およびバウチャー支援とは、現金送金プログラム、現金ベースの介入、および現金ベースの援助を意味し、人道支援分野において、バウチャーまたは現金の形で人道的援助を提供することを表す用語である。

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）

² 欧州評議会（CoE）、*Glossary on Artificial Intelligence*（人工知能用語集）、Artificial Intelligence、2022年1月6日アクセス：www.coe.int/en/web/artificial-intelligence/glossary

³ 同上

⁴ Michèle Finck, “Blockchains and data protection in the European Union”, *European Data Protection Law Review*, Vol. 4, No. 1, 2018年, p.17: <https://doi.org/10.21552/edpl/2018/1/6>

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。⁵

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⁶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）

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。

⁵ Peter Mell と Timothy Grance、*The NIST Definition of Cloud Computing*、NIST Special Publication 800-145、米国立標準技術研究所（NIST）、アメリカ合衆国商務省、メリーランド州ゲイザースバーグ、2011年9月：<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

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、特定の文脈で個人を独自に表し、電子取引に使用される」。⁶

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。

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

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。

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。⁷

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。

⁷ PwC, *Know Your Customer: Quick Reference Guide*, 2016年1月: www.pwc.lu/en/anti-money-laundering/docs/pwc-kyc-qrg-final-interactive-2016.pdf

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。

再識別とは、データ照合または同様の技術を利用して、**匿名化**または**仮名化**されたとされるデータを**個人データ**に戻すプロセスを指す。**再識別**のリスクが合理的に考えられる場合、その情報は**個人データ**とみなされ、あらゆるデータ保護原則の対象となる。**再識別**のリスクを絶対的な確実性を持って評価することは非常に難しいとされる。

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、遺伝学の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。

クラウドサービス



現金給付
プログラム

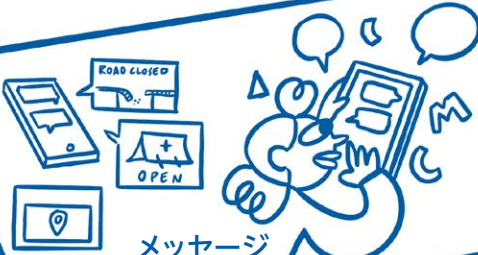
データ
分析



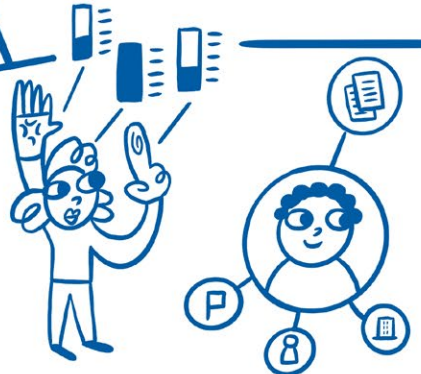
デジタル
アイデンティティ



メッセージ
アプリ

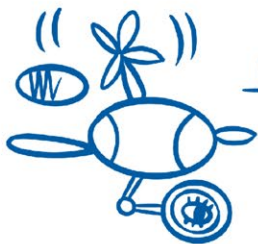


バイオメトリクス





ドローン



援助としての
接続性



ソーシャルメディア



① ICRC
SUPPLIES
AVAILABLE!



ブロックチェーン



人工知能

第1章

はじめに

MASSIMO MARELLI

1.1 背景

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。だが、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。

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。⁸

1.2 目的

本ハンドブックは、グローバル・プライバシー・アセンブリー（GPA）（旧データ保護・プライバシーコミッショナー国際会議（ICDPPC））によって開始され2015年アムステルダムで採択されたプライバシーと国際的な**人道支援**に関す

⁸ ICRC、*Professional Standards for Protection Work*（保護の任務のための専門的な基準）、第3版、ICRC、ジュネーブ、2018年：<https://shop.icrc.org/professional-standards-for-protection-work.html>

るICDPPC決議⁹に関連する議論をさらに進めることを目的としている。この議論は、2020年に採択された、国際開発援助、国際人道援助および危機管理における個人データ保護の役割に関するGPA決議¹⁰を通じて再開、継続された。そこでは、本ハンドブックの前版の作成と発行は人道支援に関わる主体とGPAとの間の協力の主な成果の1つであると、特に言及されている。

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は意図していない。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、**国際機関**に通常認められ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。

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、人道支援活動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、補助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、

9 データ保護・プライバシーコミッショナー国際会議、プライバシーと国際的な人道援助に関する決議、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、アムステルダム、2015年10月27日：<http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf>

10 グローバル・プライバシー・アセンブリー、国際開発援助、国際人道援助および危機管理における個人データ保護の役割に関する決議、第42回グローバル・プライバシー・アセンブリー非公開セッション、2020年10月：<https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-International-Aid-EN.pdf>

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¹¹を採択した、1990年12月14日の国連総会決議45/95。¹²
- 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¹³
- **個人データ・プライバシー保護**に関する国際基準（マドリッド決議）。2009年マドリッドで開催されたICDPPCで採択¹⁴
- OECDプライバシーガイドライン（2013）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（条約第108号）¹⁶、同条約を改正する議定書CETS第223号を含む（条約第108号+として知られている）¹⁷

11 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.htm>

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

13 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://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf.

14 データ保護・プライバシーコミッショナー国際会議、個人データおよびプライバシーの保護に関する国際基準、決議、マドリッド、2009年11月5日：<https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf>

15 OECDプライバシーガイドライン、OECD、2013年：www.oecd.org/digital/ieconomy/privacy-guidelines.htm

16 欧州評議会（CoE）、個人データの自動処理に関わる個人の保護に関する条約、欧州評議会条約（CETS）- 第108号、ストラスブール、1981年1月28日：www.coe.int/en/web/conventions/full-list

17 欧州評議会（CoE）、個人データの自動処理に関わる個人の保護に関する条約改正の議定書、欧州評議会条約（CETS）- 第223号、ストラスブール、2018年10月10日：<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）¹⁸が含まれる。）。
- データ保護と大規模自然災害に関する決議¹⁹、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²⁰、2015年にアムステルダムでICDPPCにより採択
- 国際開発援助、国際人道援助および危機管理における個人データ保護の役割に関する決議²¹
- ICRC、個人情報保護規則（2015年、2019年12月19日にICRC総会で更新および採択）²²
- ICRC保護の任務のための専門的な基準（2013）²³
- UNHCR、UNHCR関係者個人情報保護方針（2015）²⁴
- IOMデータ保護マニュアル（2010）²⁵

18 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

19 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、第33回データ保護・プライバシー・コミッショナー国際会議、メキシコシティ、2011年：<https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-Major-Natural-Disasters.pdf>

20 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、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、アムステルダム、2015年10月27日：<https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf>

21 グローバル・プライバシー・アセンブリー、国際開発援助における個人データ保護に関する決議、第42回グローバル・プライバシー・アセンブリー非公開セッション、2020年10月：<https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-International-Aid-EN.pdf>

22 ICRC、個人情報保護規則、出版物、ICRC、ジュネーブ、2015年：www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection

23 ICRC、ICRC保護の任務のための専門的な基準

24 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）：www.refworld.org/docid/55643cid4.html

25 国際移住機関（IOM）、IOMデータ保護マニュアル、ジュネーブ、2010年：<https://publications.iom.int/books/iom-data-protection-manual>

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。

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²⁶。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する比較的新しい人権であり、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ものである。近年、約150か国²⁷で**データ保護**または**プライバシー**関連の法律や規範が国および地域レベルで採用されており、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るようになってきている。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、**国際機関**の地位を持ち、特権および免除を享受しており、**個人データ保護**に関する国内法に従っていない。²⁸ 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。²⁹

²⁶ 世界人権宣言第12条および、市民的、政治的権利に関する国際規約第17条を参照。

²⁷ 国連貿易開発会議（UNCTAD）、「世界のデータ保護およびプライバシー関連法 | 登録」を参照。国連貿易開発会議、2022年1月6日アクセス：<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

²⁸ Massimo Marelli, “The law and practice of international organizations’ interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders”, Computer Law and Security Review, Vol. 50, 2023年, 105849: <https://doi.org/10.1016/j.clsr.2023.105849>.

²⁹ セクション2.2: 基本的なデータ保護概念を参照

- 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」³⁰または「コミュニティ識別情報」と言及している。³¹
- **人道団体**は、**人道上の緊急事態**において、影響を受ける人々や活動に関する連絡先データ、スタッフや物品 / サービスプロバイダーのデータ、さらに寄付者のデータなど、さまざまなカテゴリーの人々の**個人データ**を処理する。本ハンドブックの焦点は人道的プログラムの受益者の**個人データ**の**処理**であるが、他のカテゴリーの**個人データ**の取り扱いにも同様の考慮事項が適用される。

1.3 構成とアプローチ

このハンドブックのPART Iでは、人道上の緊急事態におけるあらゆるタイプの**個人データ**処理に広く適用され、人道上の緊急事態における**個人データ**の保護原則と要件について、詳細な分析を行う。PART IIでは、特定のタイプのテクノロジー、テクノロジー領域、および**データ**処理状況を扱い、関連

³⁰ “The Signal Code: A Rights Based Approach to Information during Crisis” を参照。The Signal Code、2022年1月6日アクセス：<https://signalcode.org>

³¹ Humanitarian Data Exchange Initiative、「利用規約」を参照。HDX、2022年1月6日アクセス：<https://data.humdata.org/faqs/terms>

するデータ保護の問題についてより具体的に説明していく。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

本ハンドブックは、人道活動のために**個人データ**の処理に携わる法律専門家および人道団体スタッフ、特にデータ保護基準についてのアドバイスと適用を担当する人を対象としている。また、データ保護当局、研究者、学者、**人道団体**とのパートナーシップを望む民間企業、こうした活動に関与するその他の人々など、**人道支援**やデータ保護に関わる関係者も対象となる。

PART I

人道支援における データ保護の 基本原則

MASSIMO MARELLI

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**個人データ**を収集し処理する。人道団体の主な活動現場である**人道上の緊急事態**下では、法の支配が完全にはなされていないかもしれない。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、均衡性の原則に従って、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。³²

人道団体の活動は主に**人道上の緊急事態**において行われるため、人道的な影響を受けている人々やスタッフの**個人データ**を保護することが、彼らの安全、生命、仕事を守るために必要となる状況であることがよくある。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。³³ すなわち、権利が果たす目的を優先させるものである。

³² この文脈における均衡性の原則は、国際人道法（IHL）の下での均衡原則と混同されるべきではない。ここで議論されている均衡性の原則は、**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侵入的でない措置をとることを要求している。

³³ 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。

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、特に人道的な影響を受けてい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、阻止してしまう場合には、援助の前にデータ収集の条件をすべての個人に知らせる必要はない。むしろ、援助に携わる**人道団体**は、そのような情報を、公示を用いてより対象を絞らず個別化しない方法で、または、事後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拠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、**人道上の緊急事態**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。³⁴ 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。

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団体の活動を受け入れてもらい、支援が必

³⁴ 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 www.icrc.org/en/doc/resources/documents/feature/2007/ww1-feature-151107.htm.

要な人々に寄り添い、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。³⁵

囲み内のチェックリストには、このハンドブックで詳細に説明している主要なポイントが記載されている。これらのポイントは、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る必要がある。

- **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**の処理は目的に均衡しているか。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。

³⁵ Els Debuf, “Tools to do the job: The ICRC’s legal status, privileges and immunities”, *International Review of the Red Cross*, Vol. 97, No. 897–898, 2015年, pp.319–44を参照: <https://doi.org/10.1017/S181638311500051X>

- **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。
- 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³⁶

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。

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

³⁶ 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。

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**の種類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、通常の方法では機微データとみなされ、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**以外の自然人、法人、公的機関、政府機関、またはその他の存在を指す。

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。このために、この団体は地元の非政府組織（NGO）のサービスを利用して援助の提供を支援するが、このNGOは、**人道団体**が最初に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**サブプロセッサ**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

先に述べたとおり、**データ主体**が識別できないように匿名化されたデータなど、個人と関係を持たないデータの**処理**についての議論は、このハンドブックの範囲外となる。

集計化されたデータが**個人データ**に由来しており、ある種の状況で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共有、公開などの処理を行うことが個人の**再識別**につながらないようにすることが重要である。³⁷

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。データの匿名化を行う場合、**個人データ**を含むデータセットが完全かつ**不可逆的に**匿名化されていること、つまり**再識別**が可能であるように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**に関してより大きなリスクをもたらす可能性がある。³⁸

「**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³⁹ 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。

個人データに**仮名化**を適用することで、**データ主体**が**再識別**される可能性を低くし、関係する**データ主体**のリスクを軽減できる。「**再識別**」という用語は、データ照合または同様の技術を使用して、匿名化または仮名化したとされるデータを**個人データ**に戻すプロセスをいう。⁴⁰ 仮名化は、管理者と処理者が

37 英国統計局、国家統計専門家のガイダンス：公式統計の機密保持 – GSS、2022年1月6日アクセス：<https://gss.civilservice.gov.uk/policy-store/national-statisticians-guidance-confidentiality-of-official-statistics>

38 英国情報コミッショナー事務局 (ICO)、匿名化：データ保護リスクの管理の実践規範、ICO、チェシャー州ウィルムズロー、2012年11月を参照：<https://ico.org.uk/media/1061/anonymisation-code.pdf>、匿名化技術に関するEU第29条作業部会意見 2014年5月も参照のこと：https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

39 “Anagraphic”、Wiktionary、2020年11月14日：<https://en.wiktionary.org/w/index.php?title=anagraphic&oldid=61117548>

40 「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。

データ保護の義務を果たすのにも役立つ。それにもかかわらず、すべての**仮名化技術**がそのままデータ保護要件を満たすわけではなく、あるケースでは**個人データ**を保護するために機能する**仮名化技術**が、別のケースでは十分に機能しない可能性がある。⁴¹

これらの手法を評価する際は、データ保護原則を慎重に適用する必要がある、リスク分析のツールは、適用されたリスク軽減手法が効果的かどうかを評価するために適したものでなければならない。目的の制限や保全などの原則は、既存の**仮名化**されたデータベースが新しいプロジェクトに再利用されたり、新しいプロジェクトに結合されたりするのを防ぐのに役立つため、ここでは特に重要である。さらに、データセットに機密性を追加することと、その有用性を低下させることの間には常にトレードオフが存在する。多くのプライバシー保護技術は、公開されるデータをかき回す（つまり、改変したり不明瞭にしたりする）ことによって機能し、その結果、その度合いによっては、共有や研究の目的のためにあまり役立たないデータとなる可能性がある。⁴²

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**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。一般的に、**個人データ**を保護する予防的措置が講じられていない場合、**再識別**が行われる可能性は大幅に高くなる。たとえば、ある事業体が人道的な影響を受けている人々に関する特定のデータセットを保持しており、**処理されたデータ**と組み合わせて、**データ主体**または**データ主体**が属するグループについての新しい情報を生成できる。

⁴¹ 参照：Athena BourkaおよびProkopios Drogkaris編、データの仮名化：高度な技術と使用例、欧州連合サイバーセキュリティ庁（ENISA）、2021年1月28日：<https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>

⁴² Gregory J. MatthewsとOfer Harel, “Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy”, *Statistics Surveys*, Vol. 5, 2011年1月1日, pp.1–29: <https://doi.org/10.1214/11-SS074>

たとえば、集計データを共有 / 公開する前に、出身国、宗教、脆弱性などのデータを関係者の地理的座標にマッピングするなどして、リスクにさらされている小規模なグループの実際の位置がデータセットから明らかにならないようにすることが重要である。

2.4 適用法および国際機関

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および免除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る。⁴³

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、特に国際法に基づき、完全に独立して、国際社会から課せられた任務を遂行できる特権および免除を享受しており、活動する国の管轄権の対象とはならない。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

⁴³ セクション1.2：目的を参照

ができる。この点において、独自の「管轄権」を構成する。⁴⁴ 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。

⁴⁴ 詳細については以下を参照：Massimo Marelli, “The law and practice of international organizations’ interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders”, Computer Law and Security Review, Vol. 50, 2023 年、105849：<https://doi.org/10.1016/j.clsr.2023.105849>

- 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
- 人道的な影響を受けている人々の保護、及び国際人権法 / 国際人道法（IHL）の尊重の構築（個々の違反行為の記録を含む）
- 医療支援
- 国内制度への包括支援（例えば難民に対する）
- 例えば避難民や無国籍者の法的地位 / 身元の文書化・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。

2.5.2.1 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**追加処理**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

データ主体が追加の使用に関し合理的に期待していることを含め、データが収集される状況は、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。なぜなら適合性を不適切に狭く解釈してしまうと、**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、人道的な影響を受けている人々の治安や、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均衡している場合には、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。この分析は事の実況に依存する。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**による嫌がらせや迫害
- 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**被調査者の追跡**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。⁴⁵

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。

データの集約と**匿名化**は、付随的ケースでのデータの使用を可能にするため、データの機密性を低下させる方法として用いられ、**追加処理**を適合とすることがある。

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。

2.5.3 均衡性の原則

均衡性の原則は、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

⁴⁵ 第3章：個人データ処理の法的根拠を参照

求される目的に均衡するか。技術的および組織的措置が、**処理**に関連するリスクに均衡するものか。)

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。⁴⁶

均衡性の原則は、**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。こうした状況では、人道的な影響を受ける人々の支援のため、「知っておくとよいこと」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、データの必要性和、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、均衡性の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**の目標の間の均衡性

⁴⁶ セクション2.7：データ保全を参照

- 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削除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全する必要性は、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均衡性の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

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**が個人データを保全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均衡するものか。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

個人データは、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。このことは、他の**機微データ**にも適用される。人道的医療提供者は、世界医師会（WMA）国際医療倫理規定⁴⁷に従ってデータを処理する必要がある。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、生命に関わる利益による理由
- 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）
- 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

⁴⁷ WMA – 世界医師会、国際医療倫理規定、2018年7月9日：www.wma.net/policies-post/wma-international-code-of-medical-ethics

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。⁴⁸

2.6.2 管理活動

人道団体は通常、雇用目的、キャリアマネジメント、評価、寄付金集め、マーケティング、その他の運営上の要件のために**個人データ**を処理する。場合によっては、保有車両やセキュリティ管理のための車両 GPS 追跡などの機密性の高い処理が含まれる場合もある。業務の状況によっては、職員の**個人データの処理**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**処理**において可能な範囲で追加的な保護措置が必要となる。

2.7 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）保全されるべきである。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。

データが削除された場合、データのすべてのコピーも削除する必要がある。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。この点は、

⁴⁸ セクション2.5.2.1 - 追加処理を参照。

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。⁴⁹

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。

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**の破壊方法

⁴⁹ 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

- データ管理および保全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、異なる責任を与えられもはやアクセスを必要としない担当者）。
- 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（物理的若しくはITベースの）データベース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。⁵⁰ 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。

⁵⁰ 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。

機密情報に分類される**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리카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。

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、**個人データセキュリティ**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

個人データの保全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壊するか、または匿名化する必要がある。破壊方法は、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**消去のため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。⁵¹

⁵¹ 国際移住機関（IOM）、データ保護マニュアル、2010年、pp.83–84。

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した際は、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全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、破壊証明が**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・システム上の消去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、再使用する前に消去する必要がある。リサイクル、粉碎、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。

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。破棄の時間と方法、および破壊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、または特権および免除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均衡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、データ保護担当者（**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⁵²
- 管轄当局（データ保護当局を含む）への登録（法的な義務付けがあり、国際機関の独立性や「危害を加えない」原則と矛盾しない場合）

⁵² 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。⁵³

- **データ主体**または他の者の生命に関わる利益
- 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

⁵³ 第3章：個人データ処理の法的根拠を参照

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。⁵⁴

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、⁵⁵ 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、訂正および消去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
- 同意をした場合、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

⁵⁴ セクション2.11：データ主体の権利を参照

⁵⁵ セクション3.2：同意を参照

- 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

個人が**同意**し、アクセス、異議、訂正、消去を実施する場合や、**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。⁵⁶

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、すぐに、若しくはデータ主体となる人々が居る現場で、情報通知をすることができない例外的な状況下や、**データ主体**から直接データが収集されていない場合は、情報通知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行うべきである。⁵⁷ **人道団体**はまた、人道目的で絶対に必要な場合でない限り、情報を適切に提供するまで、人々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、上記セクション2.10.2：情報通知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

⁵⁶ セクション2.10：情報およびセクション3.2：同意を参照

⁵⁷ セクション2.10：情報を参照

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均衡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、上記セクション2.10：情報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。

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。⁵⁸

⁵⁸ 参照：ICRC、“The ICRC Data Protection Commission”、2016年1月22日：www.icrc.org/en/document/icrc-data-protection-independent-control-commission。“Commission for the Control of INTERPOL’s Files (CCF)”、2021年10月17日アクセス：www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF

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、合理的な間隔且つ無償で人道団体から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、データ主体やデータ主体に委任された代理人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。ただし、当該文書または情報が、不均衡な努力をすることなく、他者のデータ主体への言及を伏せ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、同じく不均衡な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。

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明と、適切な場合には法定代理人 / 家族関係の証明が提供されない場合、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場合には、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）であれば、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**や委任さ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**を消去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を取扱いの根拠がない場合⁵⁹
- 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⁶⁰
- 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

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、データ消去を実行する前に、**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**がデータの消去を拒否することは正当とみなされるだろう。

⁵⁹ セクション3.2：同意を参照

⁶⁰ 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

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、権利および自由により優先する**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、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**が最初に収集または処理された国の外、および、**国際機関**の地位を持たない、同一の**人道団体**内の別の事業体、または**第三者**に対して、電子的手段、インターネットなどを介して、**個人データ**へのアクセスを可能にするあらゆる行為を意味する。⁶¹

61 第4章：国際的なデータ共有を参照

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。

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。⁶² 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、**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**に関して明確な情報を個人に提供していること。

⁶² 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を参照

- 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。⁶³ 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。

適切な法的根拠に依拠することによって、**人道団体**が、**個人データ**の収集、保管、または使用による個人、特定のグループ、または**人道団体**自体へのリスクを評価する責任から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。⁶⁴

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。

⁶³ 第2章：データ保護の基本原則を参照

⁶⁴ 第2章：データ保護の基本原則を参照

- **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援助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。

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あ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は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。⁶⁵

- 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

65 国際移住機関（IOM）、データ保護マニュアル（2010）、pp.45-48

- 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。

子どもに**同意**する法的能力がない場合は、親または法的保護者の**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、親または法的保護者の**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必要がある。⁶⁶

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。

66 セクション2.10：情報を参照

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。⁶⁷

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。（下記のセクション3.3：生命に関わる利益を参照）

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

⁶⁷ セクション3.2：同意、四番目の箇条書き参照

- **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をし、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ができる。⁶⁸

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。

68 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：情報を参照

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、各国赤十字・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。⁶⁹ 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だけでなく、真に必要なものでなければならない⁷⁰）。

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可能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でない場合には、「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。

⁶⁹ 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。参照：ICRC、"The ICRC's Mandate and Mission"、ページ、赤十字国際委員会、ジュネーヴ、2014年8月6日：www.icrc.org/en/mandate-and-mission

⁷⁰ セクション3.6：契約の履行を参照

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だけでなく、真に必要なものでなければならない⁷¹）。

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。⁷² 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、

⁷¹ セクション3.6：契約の履行の例を参照

⁷² 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。国際標準化機構（ISO）、“ISO/IEC 17799:2005 | Information Technology – Security Techniques – Code of Practice for Information Security Management”を参照。ISO、ジュネーヴ、2005～2006年）：www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/96/39612.html。

「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。⁷³
- 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。
- データ処理が、団体の業務をより効果的かつ効率的に行うために必要である。

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。

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、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

⁷³ 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。

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。団体が国内法の適用を受ける場合、これは団体が従う法的義務に基づいて許容される。

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紛争当事者となりうる武力紛争または暴力の事態の存在
- データの性質、および差別または迫害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、名前や必要な食べ物に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、義務が実施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。

3.7.1 当局への個人データの開示

人道団体による当局への**個人データ**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、問題が発生する可能性がある。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。これは、開示が**データ主体**にとって不利益を及ぼす場合や、移転が**人道団体**の安全や、任務遂行に必要な、武力紛争や暴力の影響を受けた人々、紛争当事者、または情報への今後のアクセスを危険にさらしたりする場合に、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、2015年のプライバシーおよびデータ保護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で特に認められている。⁷⁴

「特権および免除を享受していない人道団体は、人道的目的で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。データの不正利用のリスクは、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、また避難民の安全だけでなく、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。」

この大きな懸念に対処するための具体的な措置として、2019年の第33回赤十字・赤新月国際会議は、離散家族の再会支援（RFL）と、個人データ保護を含むプライバシーの尊重に関する決議を発表しており、その中には次の内容が含まれている。⁷⁵

「各国および国際赤十字・赤新月運動は協力し、本運動の活動の人道的性質と適合しない目的で[…]、または本運動が支援する人々の信頼、またはRFLサービスの独立性、公平性、中立性を損なうような方法で、個人データが要求されたり使用されたりすることがないようにする。」

⁷⁴ データ保護・プライバシーコミッショナー国際会議、プライバシーおよび国際人道支援に関する決議。

⁷⁵ 赤十字・赤新月国際会議、*Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection*、決議、赤十字・赤新月国際会議、2019年12月、第11段落：https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf

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、異なる国家間を越境する**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**サブプロセッサ**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**サブプロセッサ**として活動することがある。⁷⁶

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、特権および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。⁷⁷したがって、それらは独自の「管轄区域」を構成し、その内部のデータフロー、たとえば本部と現場との間、または現場同士の間、および下部組織との間のデータフローは、この章の範囲内には含まれない。⁷⁸

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

⁷⁶ 第10章：クラウドサービスを参照

⁷⁷ Massimo Marelli, “The law and practice of international organizations? interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders”, *Computer Law and Security Review*, Vol. 50, 2023, 105849: <https://doi.org/10.1016/j.clsr.2023.105849>

⁷⁸ セクション2.4：準拠法および国際機関を参照

- 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または**国際機関**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。

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。⁷⁹ 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⁸⁰（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、受け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、移転の受け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。しかしながら、**国際機関**が享受する特権および免除の恩恵を受けない**人道団体**にデータ保護に関する国内法が適用される場合、本章はデータ保護に関する国内法に取って

⁷⁹ 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

⁸⁰ 第2章：データ保護の基本原則を参照

代わるものではなく、またそれに関する助言を提供するものでもない。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**はその**データ保護担当者（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。

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。⁸¹ 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、以下のセクション4.4：個人にとってのリスク低減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、データの受け取り側が、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

81 第3章：個人データ処理の法的根拠を参照

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。

- 受け取り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、受け取り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。

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 / 契約条項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**から欧州連合 / 欧州経済領域外に拠点を置く**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。⁸²これは、EUデータ保護法の適用を受ける、あるいはこれらの条項の利用を希望する**人道団体**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⁸³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の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。

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

⁸² 欧州委員会、“Standard Contractual Clauses for Data Transfers between EU and Non-EU Countries”、本文、欧州委員会 - 欧州委員会、2021年6月4日を参照：https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

⁸³ 以下の例を参照のこと。赤十字・赤新月国際会議、“Restoring Family Links Code of Conduct on Data Protection”、2016年1月18日：www.icrc.org/en/document/rfl-code-conduct

- 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、受け取り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。⁸⁴ 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、適切かつ均衡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

⁸⁴ 第5章：データ保護影響評価（DPIAS）を参照

- 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られている場合は、所管当局（すなわちデータ保護当局）への移転の登録

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⁸⁵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均衡すべきである。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

⁸⁵ 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

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、移行および／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破棄するか、本部に送付して、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または当局から、**人道団体**に対し、国内での暴力が原因で離散した家族を再会させたいと申し出があった。国内の行方不明者に関して人道団体が有しているすべての情報の提供を求められている。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共有すればいいのか。どのような条件の下で、個人情報開示されるべきか。
- 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。可能な限り多くの情報か、それとも制限を設ける必要があるか。それには、健康状態や遺伝データ、宗教や政治的見解に関する情報、あるいはその他の開示された場合に関係者に重大な害をもたらす可能性のある情報を含めるべきか。

* 著者は、データ保護影響評価に関する資料の使用を許可していただいたTrilarate Researchと、ご意見、フィードバックをいただいたAlessandro ManteleroおよびNahide Basriに感謝の念を示したいと思う。

- **人道団体**は、保護者のいない行方不明の子供の写真をインターネット上に公開すべきか。**人道団体**はこれらの写真を使ったポスターを作成すべきか。どのような状況で行うべきか。

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。

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1には、DPIA報告書のテンプレートが含まれている。⁸⁶ 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。

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している。⁸⁷

⁸⁶ 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

⁸⁷ David Wright, "Making Privacy Impact Assessment more effective", *The Information Society*, Vol. 29, No. 5, 2013年, pp.307-315: <https://doi.org/10.1080/01972243.2013.825687>。ニューサウスウェールズ州情報プライバシー委員会、ニューサウスウェールズ州におけるプライバシー影響評価ガイド、ニューサウスウェールズ州情報プライバシー委員会 2020年5月: www.ipc.nsw.gov.au/guide-privacy-impact-assessments-nsw。国際標準化機構 (ISO), "ISO/IEC 29134:2017 | Information Technology – Security Techniques – Guidelines for Privacy Impact Assessment", 2016年 – 2017年: www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/22/62289.html

5.2.1 DPIA は必要か

個人データを収集、処理、保管、および/または他の団体に転送する団体は、DPIAの実施を検討する必要がある。DPIAの規模については、団体が評価するリスクの重大度によって異なる。**人道団体**は、関連するデータ保護リスクすべてを事前に認識しているわけではなく、DPIAの過程でのみ明らかになるリスクもある。**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うる場合、**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スタッフ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。

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、保全、および／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全され、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匿名化、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、データには集約、**仮匿名化**、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、データ保護リスクから利益または影響を受ける者、処理者およびサブプロセッサとなる**可能性のある者が含まれる**。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和価値は、**人道団体**がリスクをどの程度深刻なものとす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なものとするため、利害関係者にはプログラムに関する十分な情報が提供され、見解を表明する機会が与えられるべきである。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

リスクを特定する方法のひとつとしては、プライバシーとデータ保護の原則、それらの原則に対する脅威、脆弱性（脅威に対する影響の受けやすさ）、および脅威と脆弱性から生じるリスクをリストアップしたスプレッドシートを作成することが挙げられる。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。⁸⁸
- 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、適合性および均衡性に照合して評価する。

予想されるリスクの重大度と可能性の評価：予防原則

影響の重大度の基準は、「リスクまたはリスクが現実化した場合の影響の大きさ」を指す。⁸⁹ その判断には、以下のようなさまざまな質問をすることが含まれるが、これらに限定されない：何人の人がリスクにさらされるのか。どのような種類のリスクが発生する可能性があるか（例：個人の生命、安全、尊厳、権利に対する脅威、差別、経済的損害、名誉に関する被害、個人がデータ保護の権利を行使できないリスク、個人がデータ保護の権利を行使できないリスク、第三者がデータにアクセスするリスクなど）。こうしたリスクがもたらされる可能

⁸⁸ リスク用語の定義については、国際標準化機構（ISO）、ISOガイド73:2009（英語）、リスク管理 - 語彙、2009年を参照：www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:vi:en

⁸⁹ 情報ポリシーリーダーシップ、GDPRに基づくリスク、高リスク、リスク評価およびデータ保護影響評価：CIPL GDPR 解釈および導入プロジェクト、2016年12月21日：www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

性のある人々の属性はどのようなものか（特に、これには弱い立場に置かれた人々、つまり特に害悪を受けやすいグループに属している人々が含まれるかどうか）。⁹⁰

武力紛争や暴力など、ある種の**人道上の緊急事態**では、リスクが現実のこととなった場合に特に深刻な影響を与える可能性があると想定し得ることに留意する必要がある。

潜在的なリスクの**可能性**とは、リスクが顕在化する可能性、および上記の分析で特定された、考え得る重大度でリスクが顕在化する可能性を指す。**人道上の緊急事態**においては、特に文書化されたインシデントが限られていることを考慮すると、リスクが顕在化する可能性を評価することはしばしば困難である。これは、リスクの顕在化を示す文書化された根拠が限られているか、まったく存在しないことが多いことを意味する。根拠が不足しているからといって、リスクが顕在化する可能性が低い、または特定された、考え得る重大度でリスクが顕在化する可能性が低いと解釈すべきではない。むしろ、重大な影響を与える可能性のあるリスクの特定は、根拠がなくその可能性を判断できないことと合わせて、それ自体が DPIA の一部として注意深い予防対策を行うに値する、高リスクの指標と考えるべきである。したがって、リスクが顕在化した場合の考え得る重大度、人道的コンテキストにおけるデータ**処理**活動の性質、状況、および目的は、可能性の基準はどのように解釈され適用されるかについての情報となるはずである。

この点に関して、DPIA の枠組みにおいて予防原則を考慮することが提案される。予防原則は、他分野（環境、健康、医薬品などの規制など）で一般的に使用されている原則であり、リスク管理における意思決定に情報を提供し⁹¹、「現象、製品、またはプロセスは、科学的かつ客観的な評価によって

⁹⁰ David Wright, “Making Privacy Impact Assessment more effective”, *The Information Society*, vol. 29, No. 5, 2013, p. 307–315 : <https://doi.org/10.1080/01972243.2013.825687>

⁹¹ 欧州委員会、予防原則に関する欧州委員会からの通知、以下で入手可能 : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A132042>.

特定された危険を持つ可能性がある」が、入手可能な根拠では「十分な確実性を持ってリスクを判断することはできない」場合には特に注意が必要であると呼びかけている。⁹² 仮定に基づいたすべてのリスクを詳細に検討する必要はないものの、予防原則では、「リスクの存在または程度に関して不確実性がある」状況に直面した場合、「リスクの現実と深刻度が完全に明らかになるまで待つことなく、保護措置を」講じるべきである、とされている。⁹³

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。次の例は、OCHAの人道データセンターによって提供されたもので、このテーマに関する研究に基づいたものである。⁹⁴

例：人道データ管理における統計開示の制御

世帯調査やニーズ評価、その他の形式のマイクロデータから得られるデータは、危機の影響を受ける人々のニーズや視点を判断するために重要である。このタイプのデータには、DPIAプロセスの一部として特定し、データが共有される前に軽減すべき固有のリスクも存在する。氏名、電話番号、その他の直接的な識別子がマイクロデータから削除された後であっても、場所や民族などのカギとなる変数の組み合わせによって、データセット内の個人を再識別したり、機密情報を開示したりすることが可能である場合がある。

⁹² 同上

⁹³ 欧州連合司法裁判所、1998年5月5日の裁判所判決。グレートブリテンおよび北アイルランド連合王国 対 欧州共同体委員会事件 事件C-180/96 ECLI:EU:C:1998:192

⁹⁴ OCHA 人道データセンター、“An Introduction to Disclosure Risk Assessment”, The Centre for Humanitarian Data（ブログ）を参照、2022年3月23日アクセス：<https://centre.humdata.org/learning-path/disclosure-risk-assessment-overview>

統計的開示制御 (SDC) とは、一連の統計的手法を指し、マイクロデータの安全な共有を促進するため、機密情報の**再識別**または開示のリスクを評価および軽減するために使用される。

SDC プロセスには3つのステップが含まれる。

- (1) **開示リスクの評価**: 開示リスクの評価を実施することにより、特定のデータセット内で個々の回答者について開示が発生する可能性を評価する。
- (2) **開示リスクの軽減**: 1つ以上の統計的開示管理手法を適用して、開示リスクを軽減する。
- (3) **情報ロスの定量化**: 情報ロスを定量化し、収集された本来の目的のために処理されたデータの有用性を評価する。

再識別のリスクの評価

SDC プロセスの最初のステップは、開示リスクの評価を実施することである。これは、開示が行われる可能性と、データ共有前に必要となる可能性のある緩和策のタイプを決定するのに役立つ。開示リスクを評価するには、**再識別**または機密情報の開示につながる可能性が最も高い間接識別子を選択し、統計的手法を使用してさまざまなリスク尺度の計算を行う必要がある。

人道に関するマイクロデータに含まれる一般的な重要な変数には、年齢、性別、民族、婚姻状況、宗教、収入、場所、その他の形式の地理的情報などがある。状況によっては、ほとんどすべての変数を間接識別子（キー変数と呼ばれる）と見なすことができる。そのため、キー変数を選択するには、データが生成された状況とデータ環境を理解する必要がある。

一般的なリスク尺度には、k- 匿名性、l- 多様性、個人および世界規模の開示リスクが含まれる。**人道団体**では、データを共有するためには、リスク対策ごとに到達すべき閾値を設定することが必要となる。

再識別のリスクの軽減

SDC プロセスの2番目のステップは、開示リスクを合意された閾値未満に軽減することである。開示リスクを軽減するには、主に2つの戦略がある。第1

は、非摂動的な方法によるもので、抑制またはデータの一般化によってデータの詳細を削減する。たとえば、年齢または収入などの連続的なキー変数は、年齢または収入区分に再コード化できる。データ値を精度の低い値に置き換えるこのプロセスは、データの分析力を維持しながら開示リスクを軽減できる効果的な方法となり得る。第2の方法は摂動的方法として知られるものである。真の値に関する不確実性を生み出すために、データ値を変更することで開示リスクを制限することを目的としている。これらの方法はデータ値を意図的に変更するため、慎重に行う必要がある。

情報ロスの定量化

SDCを行うことで、必ず何らかの情報ロスが発生する。場合によっては、情報ロスが大きくなり、データの有用性が失われてしまうこともある。情報ロスは、データの使用目的に応じて評価される必要がある。SDCプロセスの最終ステップでは、開示リスクの再評価を行い、SDC技術の適用によって開示リスクが許容可能なレベルにまで軽減されたかどうかを判断し、情報ロスが評価する。SDCプロセスの目標は、開示リスクを許容可能なレベルまで軽減しながら、ユーザーにとってのデータの有用性が最大化される最適なポイントを見つけることである。⁹⁵

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。

⁹⁵ 人道分野におけるSDCの詳細情報については、次のリソースを参照されたい。OCHA人道データセンター、“An Introduction to Disclosure Risk Assessment”。OCHA人道データセンター、“Statistical Disclosure Control”、人道データセンター（ブログ）、2022年3月23日アクセス：<https://centre.humdata.org/guidance-note-statistical-disclosure-control>。“Statistical Disclosure Control for Microdata: A Practice Guide for SdcMicro”、SDC実用ガイド文書、2022年3月23日アクセス：<https://sdcpractice.readthedocs.io/en/latest>

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 報告書の長さや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する。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を伏せたバージョン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 (DPO) 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

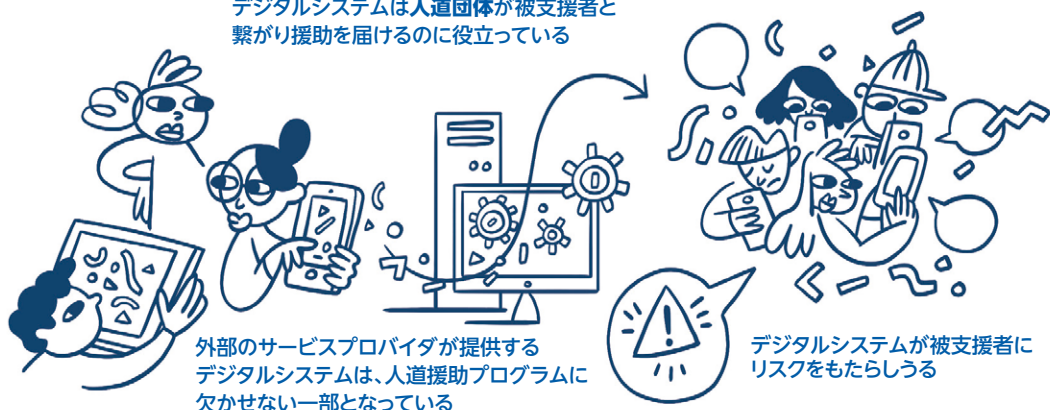
DPIA の対象となる活動に重大な変更があった場合、あるいは新たなデータ保護リスクが生じた場合には、人道団体は DPIA を更新すべきである。

PART II

特定の処理の状況、 テクノロジー およびテクノロジー 分野

データ保護 バイデザイン

デジタルシステムは人道団体が被支援者と
繋がり援助を届けるのに役立っている



課題

サードパーティのデジタルシステムは
様々な目的で不必要なデータを
収集・処理することがある



人道上の緊急事態においては、
規制順守だけでは人々へのリスクを
軽減できない。

リスク軽減

特定の目的を達成するためだけの
技術的設計が必要



システムを使って達成すべき
目的を厳密に特定する

第6章

データ保護のための 設計

CARMELA TRONCOSO、WOUTER LUEKS

6.1 はじめに

人道団体は、極めて困難な状況におかれた、最も弱い立場にある人々を支援する。効率性や説明責任の理由から、そしてできるだけ多くの人々を助けたいという思いから、**人道団体**はそのプログラムにおいて、デジタルテクノロジーへの依存度を高めている。多くの場合、弱い立場にある人々の生活と安全は、これらの組織が提供する支援に依存している。その結果として、彼ら個人には、支援を受け入れるかどうか、また支援を受けることを臨んだ場合にこれらのデジタルシステムに参加するかどうかについて、決定権が与えられることはほとんどない。デジタルシステムはデータ保護とプライバシーについてのリスクをもたらす。特に弱い立場にある人々にとって、これらのリスクは重大となる可能性がある。そのため人道支援組織には、彼ら個人の生活を短期的に守るだけでなく、データ保護、プライバシー権、支援する人々の尊厳を守る義務もある。

デジタルシステムのこの関連性は人道支援分野に限定されるものではない。これらのシステムは注目されるようになり、2010年代初頭、政策立案者や研究者は、デジタルシステムの設計における強固なプライバシー保護の確保を強く提唱するようになった。政策面では、プライバシー保護を重視した、敬意あるデジタルサービスのための法的基盤を確立することを目的とした規制の取り組みが行われた。⁹⁶ 研究面では、プライバシー保護を重視したシステム向けに膨大な数のプライバシー強化テクノロジーや構成要素も作成されており、電子投票や調査ジャーナリストのための文書検索、銃登録データベースなど、幅広い特定のユースケース向けのエンドツーエンドのプライバシー保護を重視

⁹⁶ たとえば、次のような取り組みがある。

EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (EU General Data Protection Regulation), [2016] OJ L119/1 (個人データの処理およびかかるデータの自由な移動に関する自然人の保護に関する2016年4月27日の欧州議会および欧州理事会のEU規則2016/679、および廃止される指令95/46/EC (EU一般データ保護規則)、[2016] OJ L119/1)

California Consumer Privacy Act (カリフォルニア州消費者プライバシー法)、2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST)

Ann Cavoukian, 「Privacy by Design: The 7 Foundational Principles (プライバシーバイデザイン: 7つの基本原則)」, Information and Privacy Commissioner of Ontario, 2011年1月: www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

したシステムが登場している。プライバシーに配慮したシステム設計のための具体的な戦略を明確にする取り組みも行われてきた。⁹⁷

こうした進歩にもかかわらず、強固なプライバシーとデータ保護を備えたシステムを設計・立案するプロセスは、依然として困難なことである。主な理由の1つは、技術的成果であるプライバシー保護という特性を、データ保護の規制、方針、原則に当てはめることは、多くの場合、難しいことにある。

通常、人道支援組織は独自のシステムを設計することではなく、その代わりにサービスプロバイダーに要求事項を提出する。その結果、彼らは適切な質問をし、より良い分析を要求することで、提供されたソリューションを評価する必要がある。この章は、デジタルシステムがもたらすプライバシーとデータ保護について考える手法を読者に提供することを目的としている。我々は、強固なプライバシー保護を実現する設計を行うために使用できるプライバシーエンジニアリング手法を通じてこれを行う。我々が提示するプライバシーエンジニアリングの原則に準拠したシステムは、設計によって、データの最小化を実現し、収集されるデータの使用目的を制限することを可能とする。我々がこうしたデータ保護原則を守るためのテクニカルな手段を提供することで、このメソッドに従って設計されたシステムは、個人、そしてその尊厳、権利を強固に保護することができる。

より具体的に言うならば、この章では、システムの目的を決定する方法についてのガイダンスを提供し、目的の制限を設けることで、システム設計者がいかにして強固なプライバシーとデータ保護を備えたシステムを作成できるかを示していく。最後に、本章では、システムを分析する方法に関する具体的なガイダンスを提供している。この分析により、システムが目的の制限を守るためのテクニカルな手段を備え、データ使用ポリシーによって達成できる保護を超えて、ユーザーに強固な保護を提供できるかどうかを判断することができる。

また、本章で紹介する方法とテクノロジーは、データの最小化、目的の制限、およびデータ保護に含まれるデータセキュリティといったニーズに対応している

⁹⁷ Jaap-Henk Hoepman, 「Privacy design strategies (Extended abstract) (プライバシー設計戦略 (詳細要約))」、*IFIP Advances in Information and Communication Technology*, No. 428, 2014年1月1日, pp.446-459

ことに注意されたい。ただし、説明責任など、他のデータ保護要件には対応していない。しかし、本章で紹介する設計原則により、**人道団体**は、あらゆるデータ保護要件を満たすために追加されるメカニズムが、個人やその権利の技術を活用した保護にとって有害であるか否かを評価できるようになるであろう。

6.1.1 システムとは何か

本章では頻繁に「システム」について言及される。我々はシステムを「1つ以上の所定の目的を達成するために組織された相互作用する要素の組み合わせ」と定義する。⁹⁸ システムとはつまり、ある目的を達成するために必要なすべての部分（または要素）を指す。この定義に従うなら、システムは中央サーバーだけではなく、より多くの部分で構成されることとなる。通常、システムには少なくともユーザー用デバイスが含まれる。

6.2 ケーススタディ：プライバシー保護を重視した接触追跡アプリ

本章では、大規模な導入に成功した、プライバシー保護を重視したシステムである、モバイルアプリベースの接触追跡システムを例として使用する。これによってアプリケーションの目的から出発し、テクノロジーを使用して目的の制限を守ることが、強固なプライバシーの確保にどのようにつながるかを説明したい。

新型コロナウイルス感染症のパンデミックの初期に、感染拡大を止めるための公衆衛生対策として、接触追跡アプリが導入された。接触追跡の目的は、新型コロナウイルス感染者の濃厚接触者を特定し、新型コロナウイルス陽性者に近づくことでウイルスにさらされた可能性が高い接触者が、自分自身が

⁹⁸ Joint Task Force Interagency Working Group, *Security and Privacy Controls for Information Systems and Organizations*（合同タスクフォース省庁間ワーキンググループ、情報システムおよび組織のセキュリティとプライバシーの管理）、NIST Special Publication 800-53, National Institute of Standards and Technology, 2020年9月: <https://doi.org/10.6028/NIST.SP.800-53r5>

感染症に罹った場合に備えて、病気の蔓延を避けるために自主隔離などの行動を取れるようにすることにある。

効果を高めるためには、接触者追跡はタイムリーに行われ、できるだけ多くの接触者に連絡する必要がある。従来、追跡は人の手で行われていた。しかし、人力による接触追跡は、訓練を受けた人員に依存するため、新型コロナウイルス感染症などの病気が広く蔓延した場合、規模を拡大することができない。そのうえ、マンパワーによる接触追跡には時間がかかる。追跡者が発端患者、つまり病気に感染した人に聴き取りを行う必要があるためである。追跡者は発端患者の連絡先を特定し、1人ずつ連絡を取っていく必要がある。さらに、空中に浮遊する病原体を扱う場合、接触者が発端患者にとって知らない人（バスの乗客やスーパーのレジで並んでいる人々など）である可能性があるため、発端患者はすべての接触者を特定できないことも考えられる。

新型コロナウイルス感染症のパンデミックの最初の数か月、人力による接触者追跡には限界があったため、いくつかのデジタルソリューションが提案された。本章では、Bluetoothテクノロジーを使用したソリューションを見ていく。これは、人と人との距離を測定し、新型コロナウイルス感染者と接近した事実を元に、感染リスクをユーザーに自動的に通知するソリューションである。こうしたデジタルシステムは、発端患者や連絡すべき人物との手作業によるやり取りに依存する必要がないため、拡張性が向上する。また、ある人が誰と接触したかということを知ったり、連絡先情報を手に入れたりする必要がないため、より使いやすい。同時に、これらのデジタルソリューションの効果は本質的に、接触追跡アプリも使用する濃厚接触者の発見することのみに限定される。

接触追跡アプリは、機密情報を含む個人データを漏洩させてしまう可能性がある。この種の情報は、個人や集団のプロファイリング、操作、制御に悪用されてきた過去を持つ。⁹⁹ したがって、プライバシー保護を重視した接触追

⁹⁹ 参照例：Balthasar StaehelinとCécile Aptel、「COVID-19 and Contact Tracing: A Call for Digital Diligence（新型コロナウイルス感染症と接触者追跡：デジタルディリジェンスの呼びかけ）」、Humanitarian Law & Policy Blog（ブログ）、2020年5月13日：<https://blogs.icrc.org/law-and-policy/2020/05/13/covid-19-contact-tracing-digital-diligence>

跡アプリは、こうした機微データが利用できないように作成されており、感染の危険性のユーザーへの通知以外の目的で悪用することはできない。

次のセクションでは、プライバシー保護を重視した接触追跡アプリケーションの設計について説明する。こうしたアプリケーションに精通している読者は、セクション6.3 - 「目的制限による個人とその尊厳および権利の保護」に進んでいただきたい。

6.2.1 分散型のプライバシー保護を重視した接近追跡

本章では、分散型のプライバシー保護を重視した接近追跡（DP3T）プロトコルに基づく、プライバシー保護を重視した接触追跡アプリケーションの例を使用する。¹⁰⁰ このプロトコルにより、強固な保護を実現できる分散型のシステムの作成が可能となる。ユーザー間の社会的な交流に関する情報などといった機微データは、中央のエンティティではなくユーザーのデバイスに保存・処理される。スマートフォンはローカルで曝露スコアを計算し、新型コロナウイルス陽性ユーザーへの曝露が非常に高い場合、ユーザーに通知を行う。一部のデータはサーバー経由で交換されるが、それ自体にはユーザーに関する機密情報は含まれておらず、悪用されることはない。

デジタル接触追跡システムのすべてのユーザーは、自分のスマートフォンにアプリをインストールしている。あらかじめ決められた間隔（約15分）で、アプリは新しい乱数を生成する。アプリは、Bluetooth Low Energy (BLE) ビーコンを介して乱数をブロードキャストする。その近くにあるスマートフォンは、受信した乱数を、「見た番号リスト」に記録する。近くにあるデバイスは送信されたBluetoothビーコンを高強度で受信するが、遠くにあるデバイスは低強度で受信するか、まったく受信しない。低強度のビーコンは、デバイスが感染のリスクがあるほど近くでないことを示すために、記録されない。

ユーザーが検査で陽性と判断された場合、保健当局はこのユーザーに、感染期間中に本人のデバイスから送信された乱数を中央サーバーにアップロー

¹⁰⁰ Carmela Troncoso 他、「Decentralized privacy-preserving proximity tracing（分散型のプライバシー保護を重視した接近追跡）」、ArXiv: 2005.12273 [Cs]、2020年5月25日：<http://arxiv.org/abs/2005.12273>

ドすることを許可する。中央サーバーは、新型コロナウイルス感染症の陽性ユーザーが送信したすべての乱数のリストを定期的に公開する。システム内のすべてのデバイスはこのリストをダウンロードし、デバイス内の（物理的に近くにいた人々を示す）「見た番号リスト」のエントリーが、ダウンロードした乱数のリスト（感染した人々が載っている）に含まれているかどうかをローカルで確認する。この2つのリストの中に重複する番号があれば、ユーザーが発端患者の近くにいたこと、新型コロナウイルスにさらされた可能性があることを示すことになる。この接触（接近の長さや相対的な信号強度によって決定される）が閾値を超えると、スマートフォンはユーザーに通知を行う。

このシステムにおいては、ユーザーのデバイスから出る情報はほとんどない。中央サーバーは、新型コロナウイルス感染症の陽性ユーザーから送信された乱数のみを受信する。この番号はユーザーのデバイスによってランダムに生成されるもので、ユーザーの身元や場所とは関係を持たない上、ユーザーが会った人の数や会う頻度、時間の長さとも無関係である。ただし、陽性ユーザーの乱数が公開されると、多くの場所でBluetoothビーコン（つまり、乱数）を受信できる攻撃者にとって、このユーザーの追跡や特定が容易になる可能性がある。¹⁰¹ 要約すると、サーバーには、ユーザーに損害を与えるために悪用される可能性のある情報はほとんど保持されていない。

先程の「所定の目的を達成するために組織された要素の組み合わせ」というシステムの定義に戻ると、DP3Tシステム内のユーザーのスマートフォンは中央サーバーと連携して、新型コロナウイルスにさらされたユーザーに通知するという目的を達成する。したがって、スマートフォンと中央サーバーの両方がこのシステムの一部となっている。また実際のところ、公衆衛生当局は、検査で陽性反応を示したユーザーによるアップロードをデジタル的に承認する必要があるため、公衆衛生当局（または少なくとも公衆衛生当局が運営するサーバー）も接触追跡システムの一部となる。

101 The DP-3T Project, *Decentralized Privacy-Preserving Proximity Tracing: Overview of Data Protection and Security* (DP-3Tプロジェクト、分散型のプライバシー保護を重視した接近追跡：データ保護とセキュリティの概要)、GitHub、2020年：<https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf>

6.3 目的制限による個人とその尊厳および権利の保護

強固なデータ保護、プライバシーを実現するシステムの設計と分析を導く、方法論と原則がいくつか存在する。本章では、**設計による目的制限**の確保に基づいた方法論を使用する。デジタルシステム設計の際にさまざまなテクニックを慎重に用いることにより、データ保護原則を守ることについて説明していく。この方法論は比較的使いやすく、強固なプライバシー確保を可能とするシステムを実現し、またプライバシーに配慮した設計の限界をも自ずと示すものである。

読者は、データ保護要件としての目的制限について熟知しているかもしれない。この要件は、データが特定の目的のために収集されるものとし、別の目的で使用されることを禁止するものである。従来目的の制限は、プロセスと手順を通じて実現されてきた。ただし、本章では、テクニカルな意味での「目的の制限」について述べていく。

「技術を活用した目的の制限」を備えたシステムは、その技術を活用した設計を通じて、システム全体が所定の目的にのみ使用されることを約束する。こうしたシステムでは、所定目的の範囲内である場合にのみ、敵対的なエンティティがデータにアクセスすることができる。

結果として、技術を活用した目的の制限を達成するように設計されたシステムは、システム内でどのデータがどのように収集・処理されるかによって生じる可能性のある害悪を最小限に抑える。目的制限のあるシステムでは、システムの目的以外でデータを使用することができない。したがって、ユーザーは、システム内の他の行為者が適切な行動を取ること、またはデータ保護ポリシーに違反しないことを信頼する必要はない。他の行為者が意図的に危害を加えようとした場合でも、こうした危害からは保護されるしくみが整っている。

従来のアプローチ



プライバシーに配慮したアプローチ

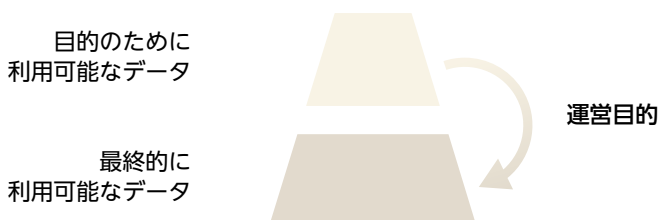


図6.1. 目的の制限からスタートした結果として（ユーザーが信頼していないエンティティで）一元的に収集されるデータの量は、コンプライアンス遵守のメカニズムに従ってデータを最小限に抑えた場合よりも、大幅に少なくなる。

テクニカルという観点から考えると、目的の制限は、ユーザーには制御することができず、したがって信頼されることはないエンティティによって収集されるデータの量に大きな影響をおよぼす。図6.1の上の図は、デジタルシステムを構築するときに収集するデータを決定するときに最もよく使用されるアプローチを示している。通常、設計者は（これらのデータが将来役立つという考えをもって）できるだけ多くのデータを収集するシステムを作成しようとすることから始める。次に、法規制への準拠（主にデータ保護への準拠、またはストレージや処理能力などといった運用上の制約）により、最終的に収集されるデータ量は制限される（図 6.1 – 一元的に収集されるデータを参照）。

対照的に、設計者がシステムの目的に基づいてデータ収集を考える場合、その目的を果たすために必要なデータのみの収集・処理を行うシステムであることが出発点となる。それ以上のデータを収集すると、目的の制限に違反することとなる。場合によっては、運用上の制約により、追加データの収集・処

理を行わなければならない場合もある。ただしそれでも、収集されるデータの量は、規制遵守のみを考慮した場合に許容される量よりも大幅に少なくなる。

このセクションのポイントとして、設計による目的制限のメカニズムを利用してシステムを評価する方法に注目してみる。これには2つの重要なステップが含まれる。第一に、評価者はシステムの目的を確立する必要がある。第二に、評価者は確立された目的を考慮して、技術を活用した目的の制限をシステムが備えているかどうかを評価しなければならない。

6.3.1 目的の決定が重要である理由

プライバシー保護を重視したシステムを設計するための最初のステップは、システムの目的を決定することである。システムを導入する目的を、本質的な目的にまで絞り込むことが重要である。目的が広すぎたり不明確であったりすると、目的を厳密に制限した、個人の権利と尊厳を強固に保護するシステムを設計することが非常に困難になったり、不可能になったりするだろう。

広すぎる目的はプライバシーにとって有害であり、データの保護が制限されてしまう。広すぎる目的や不明確な目的が有害である理由を知るには、接触追跡アプリについて考えていただきたい。その目的が、「発端患者の連絡先に通知を送る」という狭いものではなく、「接触者の追跡を実行する」というより広いものであると仮定してみよう。この後者の目的は非常に広範におよぶものであるため、疫学調査、過去にさかのぼった追跡（発端患者ではなく感染源を特定する）、通知された患者の監視、感染者の隔離の監視の強化など、人力の接触者追跡プロセスに関わるすべてのステップを実行するものと理解されるかもしれない。このような広範な目的を達成するには、ユーザーの身元、連絡先情報、住所などを含むあらゆる種類のデータを公衆衛生当局が利用できるようにする必要があるだろう。そしてこれらのデータは、後に悪用される可能性がある。しかし、システムの唯一の定められた目的が、発端患者の連絡先に通知することであるならば、これらのデータはいずれも中央サーバーで利用できるようにする必要はない。

また、目的がより狭いものであったとしても、さらなるデータを強制的に利用可能にすることにより、害悪が発生する可能性がある。たとえば、ドイツの Luca 接触追跡システムの目的は、陽性者が訪れた場所へ行った人々の名前と電話番号を公衆衛生当局に提供することであった。このような情報を利用可能とすることにより、たとえそのデータが特定の条件下でのみ他者が利用可能なものであったとしても、データ保護に準拠した設計の、目的を制限する能力は重大な影響を受ける。システムは信頼できるものである必要があるものの、その信頼は侵害される可能性がある。ドイツ警察は、何らかの保護措置が講じられていたにもかかわらず、Luca システムを使用して訪問者情報にアクセスを行った。¹⁰²

プライバシー保護を重視したシステムを、複数の目的に合わせて設計するのは困難である。複数の目的を定義すると、目的制限を行ったとしても、システムが実現できるプライバシーの確保能力が低下するおそれがある。商用アプリケーションにおける一般的な例としては、システムが非常に具体的な目的を持っているか（モバイル懐中電灯アプリなど）、非常に広範な目的を持っているか（金融資産を管理するアプリなど）に関わらず、データの一元収集を促進する目的に「カスタマーエクスペリエンスの改善」を含めていることが見て取れる。このような「改善」目的が現れると、一元的に収集・利用されるデータ量が大幅に増加する可能性がある。それは、アプリケーションに関連するデータ（懐中電灯が点灯していた時間など）から、厳密にはアプリケーションに関するものではないが、カスタマーエクスペリエンスに関わるデータ（アプリを開いたときの携帯電話のバッテリー状態、そのアプリと同時に実行されているアプリ数など）にまでおよぶ。

こうした目的により追加データを一元的に利用できるようにしてしまうと、プライバシーの保護が困難になる。一つひとつのデータ間の関連性や相関関係は、特にそれらのデータが人やその行動に直接またはデバイスを介して関係している場合、これらのデータに基づいて行うことができる推測や予測、将来利用できること

¹⁰² Rachel Pannett, 「German police used a tracing app to scout crime witnesses. Some fear that' s fuel for covid conspiracists (ドイツ警察は追跡アプリを、犯罪目撃者を探すために使用した。新型コロナ陰謀論者を刺激することを懸念する声も。)」, ワシントン・ポスト, 2022年1月13日: www.washingtonpost.com/world/2022/01/13/german-covid-contact-tracing-app-luca

の量を予測することは非常に困難になる。さまざまな種類のデータからどのような推論を行うことができるかを決めることの難しさは、堅牢な匿名化メカニズムを探る際に遭遇する問題、つまり「次元の呪い」と似通っている。¹⁰³ 実際、予測できない方法で関連付けられるデータフィールドが多すぎるため、匿名化アルゴリズムの設計者は考えるすべての仮名化された識別子を特定することはできない。したがって、データの有用性を損なわずに、堅牢な匿名化メカニズムを設計することはほぼ不可能となる。

複数の目的を持つことは、システムの設計におけるプライバシーの保護方法にも制約を与える。たとえば、接触追跡アプリは通知のみを目的としていたために、他に使い道のないランダムな識別子のみをサーバー経由で交換するという設計が可能になった。さらなる目的（強制隔離や疫学調査など）があれば、おそらく設計者はより多くのデータを一元的に利用できるようにする必要があっただろう。そうすると、データを1つの目的のみに使用するよう制限することがはるかに難しくなる。たとえば、強制隔離には通常、位置情報、または少なくとも、ユーザーが自宅にいるかどうかの情報が必要となる。そして疫学的な監視には、感染の連鎖を明らかにする必要があり、そのためには人間関係を明らかにしなければならない。

システムに課せられた複数の目的が本質的にプライバシーに関する脆弱性を生じさせない場合でも、実用的な目的制限システムを作成するのは難しいだろう。特に、これらのシステムは実際の運用のために最適化するため、目的制限を備えたソリューションを構築することは困難である。たとえば、準同型暗号化に基づくプライバシー保護を備えた医療分析システムが十分に

103 Arvind Narayanan および Vitaly Shmatikov, 「Myths and fallacies of 'personally identifiable information' (『個人特定可能』の神話と誤謬)」、Communications of the ACM, Vol. 53, No. 6, 2010 年 6 月 1 日, pp.24–26 : <https://doi.org/10.1145/1743546.1743558>。Theresa Stadler および Carmela Troncoso, 「Why the search for a privacy-preserving data sharing mechanism is failing (プライバシー保護を重視したデータ共有メカニズムの探索はなぜ失敗するのか)」、Nature Computational Science, Vol. 4, 2022年4月21日, pp.208–210 : <https://doi.org/10.1038/s43588-022-00236-x>

その性能を発揮するには、非常に慎重なドメイン固有の最適化が必要である。¹⁰⁴このようなシステムを、新しい制約に対応するために困難な最適化プロセスを繰り返すことなく、さまざまな目的に使用することは困難である。

忍び寄る、目的という誘惑。一旦システムまたはインフラが構築されると、既存のコンポーネントを活用するために、目的を追加したくなる誘惑にかられる。たとえば、接触追跡アプリケーションのエコシステムでは、疫学的監視から隔離の実施、通知を受けたユーザーのデータ収集など、多くの拡張機能が提案された。最終的に、これらは導入されることはなかったが、他のものは導入されたものもあった。2020年後半、研究者らは、新型コロナウイルス感染症が飛沫によって接近者に広がるだけでなく、換気の悪い部屋でのエアロゾルによっても広がることを発見した。多くの国がその後、既存の接近ベースのシステムに加えて、屋内の共有スペースの訪問者に接触追跡を適用するチェックインソリューションを採用した。この機能が追加されるとすぐ、バーやレストランの最大収容人数についての規制の監視と実施にも、システムを使用する必要があるという提案がなされた。ただし、目的を追加することで、ユーザーのデバイスと中央サーバーの間でより多くの情報が交換されることになり、目的制限の実現がはるかに困難になる。

人道団体が行う人道支援活動においても、同様の要望と圧力が起こることが予想される。援助の二重取りを防ぐために構築されたシステムは、リソース配分を最適化するための機会とみなすことができる。また、受益者の認証の目的で構築されたシステムは、リソースの使用状況を監視する機会として考えることができる。これらの目的は完全に正当であり、望ましくすらあるが、それらすべてを同時にひとつのシステムに含めようとする、強固なプライバシー保証を確保し、テクノロジーによって目的制限を守るシステムを設計することが不可能になる可能性があることを理解することが大切である。システムを構築できる可能性はあるものの、プライバシーとデータ保護は、ポリシーと規制によ

¹⁰⁴ David Froelicher 他、「Truly privacy-preserving federated analytics for precision medicine with multiparty homomorphic encryption (マルチパーティ準同型暗号化使用の、真にプライバシーを保護する精密医療向け統合分析)」、*Nature Communications*、Vol. 12、No. 1、2021年10月11日、5910: <https://www.nature.com/articles/s41467-021-25972-y>

る保護のみに頼ることになりかねない。システムが導入される環境によっては、このような保護では十分ではない場合がある。

6.3.2 目的の決定

システムの目的を定義することは、簡単な作業とはいえない。一般的に、目的が狭いほど、システムを設計するための技術的手段を見つけるのが容易になる。したがって、目的制限を確実にを行い、個人とその尊厳、権利を強固に保護することができる。通常、目的を決定するには、関係者との話し合いが必要である。こうした話し合いでは、多くの目的が候補として挙げられてくるだろう。問題を解決する手段としてのテクノロジーの力がしばしば過大評価されるためである。

その時点で、これらの目的を分離し、システムが対処すべき根本的な問題は何かを特定することが大切である。また、他の問題に対処したり、システムまたはシステムを委託している組織の効率を向上させたりすることができる、さらなる望ましい機能は何かも考えてみる必要がある。目的を分離した後、設計者は、目的を制限し、悪用につながる情報漏洩を回避しつつ、どの目的を採用するかを決定する必要がある。このステップで設計者は、たとえば、この目的は信頼できない当事者が機微データを利用することを可能にしてしまう、といった具合に、システムの目的自体がリスクを誘発することに気付くだろう。

設計や導入の選択によってリスクが発生することもある。これはプライバシー保護を重視した設計ではよくあることである。図6.2を参照されたい。設計者は、目的に内在するリスクのみを考えて設計を行うかもしれないが、最終的には設計に対するリスクはわずかに多くなる可能性がある。多くの場合これは、こうしたリスクを完全に軽減するシステムを構築する方法を知らないか、構築方法は知っているが、システムを十分に効率的にすることができないために起こる。この時点で、進むべき道は2つある。1つは、リスクが大きすぎるためシステムを構築しない決定を下すこと。もう1つは、個人の権利と尊厳に対する害が目的によってもたらされる益よりも大きく、ポリシー以外では制御できないことを受け入れてでもシステムを構築することである（図6.1を参照）。



図6.2. 実用的で展開可能なシステムには、目的のみによって生み出されるリスクよりも多少高いリスクが伴う可能性がある。

プライバシー保護を重視したアプリの例は、内在するリスクと導入によって起こるリスクの両方を示している。まず、発端患者の連絡先に通知を行うという目的に内在するリスクを考えてみる。ユーザーが通知を受け取ると、その通知をトリガーした発端患者が特定される可能性があり（たとえば、報告された接触が行われた日に一緒にいたのは1人だけだったなど）、医療情報も知ることができる。この漏洩はシステムの機能に内在するものであり、システムは、ユーザーが適切な措置を講じられるように、ユーザーに通知を行わなければならない。次に、導入によって起こるリスクを考えてみる。サーバーは陽性ユーザーからのアップロードのみを受け取る。したがって、サーバーまたは通信の観測者は、新型コロナウイルス感染症陽性ユーザーの仮名化された識別子（IPアドレスなど）を決定することができる。この場合、仮名化された識別子の処理は、システムがその目的を達成するために厳密に必要とされるよりも多くのデータが処理されることをも意味する（図6.1を参照）。

システムの目的を制限することで、プライバシーエンジニアリングを最大限に行うことができる（そして、制限しないことにより、ソリューションがプライバシー保護を行えず、個人に害悪をおよぼすリスクが発生する可能性がある）。ただしこの決定は、組織の効率やコストに影響をおよぼすことがある。設計によって目的制限を採用するには、目的ごとに、1つ以上のプライバシー保護を重視したシステムを構築する必要があるだろう。どのオプションが最適であるかを判断することは、利用可能なリソースや、システムが展開される条件によって異なるため、本章の目的ではない。代わりに本章は、リスクと利益の分析を

実施するためのガイダンスを提供することを目的としている。**人道団体**が、データ保護とその他の運用上の制約との間のトレードオフについての情報を得て、意思決定を行えるようにするためである。

6.3.3 目的制限の分析

システムの目的決定後の次のステップは、システムの技術が、システムの目的的制限を実現できるかどうかを評価することである。これは簡単なプロセスではない。というのも、システムが、利害関係者が定めた目的以外に使用できないかどうかを判断するのは難しいことであるためだ。

この複雑なプロセスに取り組むには、次の2段階のアプローチを使用すると良いだろう。第一に、システム内で生成、保存、処理されるデータすべてを（こうした作業がどこで行われるかに関わらず）分析して、個人の権利と尊厳に害悪をもたらす可能性のあるシステム内のプライバシーリスクを特定するとともに、システム全体によって引き起こされる可能性のある危険性を探る。次に、特定されたリスクごとに、そのリスクがシステムの目的そのものに内在するものであるかどうか（その場合は何もする必要はない。上記を参照）、またはシステムに技術を活用したプライバシー保護措置を追加することによってこのリスクが軽減されるかどうかを判断する。

先に述べたように、**人道団体**は通常、独自のシステムを設計しないため、本章ではシステムの設計についての言及を意図的に除外している。¹⁰⁵

6.3.3.1 潜在的リスクの特定

リスクは明らかなものではないため、潜在的リスクを特定するプロセスは複雑である。**人道団体**は、ボトムアップとトップダウンを組み合わせたアプローチをとることができる。ボトムアップアプローチは、システム内で処理された利用可能なすべてのデータを調べることから始める。リスクは、データが直接的、間接的にアクセス可能になった場合に、誰が被害を受ける可能性があるかに

¹⁰⁵ 目的が特定された後でプライバシー保護を重視した設計を行う方法の詳細については、次を参照されたい。Seda GürsesとCarmela TroncosoおよびClaudia Diaz, “Engineering privacy by design reloaded (再考されたプライバシーバイデザインのエンジニアリング)”, Amsterdam Privacy Conference, 2015: <http://carmelatroncoso.com/papers/Gurses-APC15.pdf>

基づき、導き出す必要がある。リスクを特定するには、データがユーザーのデバイスのみで処理されるか、中央サーバー間で分散されるか、単一の中央サーバーで利用できるかなどといった、具体的な運用の詳細は無視すべきである。

ボトムアップアプローチでは一部のリスクを特定できないことがあるため、トップダウンアプローチと組み合わせる必要がある。このアプローチは、システム導入による潜在的な害悪を特定することから始め、そこからリスクを引き出していく。被害を受ける可能性があるのは誰かを考えるときは、被害の対象には個人のユーザーだけでなく、グループやコミュニティも含まれることを覚えておくことが大切である。こうしたグループやコミュニティは、個々のメンバーへの害悪は許容できるものと考えられる場合でも、全体として大きな影響を受ける可能性がある。実際、この害悪は、システムに参加していない場合でも発生する場合がある。

データからリスクへ。本章で説明しているデジタル接触追跡システムの例は、データに基づいたボトムアップアプローチの一例としても使うことができる。接触追跡システムで処理されるデータは、暴露リスクの計算を可能にするために、社会的なやり取りデータ（たとえば、誰が誰と、いつ、どのくらいの時間会ったかなど）を反映する必要がある。したがって、デジタル接触追跡システムには、社会的接触情報漏洩のリスクがある。さらに、このシステムから位置データ漏洩のリスクがあり（その結果、システムが追跡インフラとなるリスクもあり）、またユーザーの身元情報漏洩の危険性もある。実際、デジタル接触追跡ソリューションから位置データが明らかになることがある。ドイツの Luca アプリは、感染した人がいた場所の訪問者を追跡することに重点を置いていた。警察は、Luca アプリに保存されている接触追跡情報を利用して、特定の場所の訪問者の連絡先データを要求し、入手した。¹⁰⁶ デジタル接触追跡システムは、陽性者が誰であるか、誰が陽性者と接触した可能性があるのかなどといった医療データの処理も行う。したがって、デジタル接触追跡システム

106 Rachel Pannett, 「German police used a tracing app to scout crime witnesses. Some fear that' s fuel for covid conspiracists (ドイツ警察は追跡アプリを、犯罪目撃者を探すために使用した。新型コロナ陰謀論者を刺激することを懸念する声も。)」, ワシントン・ポスト, 2022年1月13日: www.washingtonpost.com/world/2022/01/13/german-covid-contact-tracing-app-luca

から、誰が陽性となったか、誰がウイルスに曝されたのかなど、秘密にされるべき健康情報が漏洩する危険性がある。

リスクは、個人とは関連しないデータにおよぶ場合もある。たとえば、感染した個人が行った場所の訪問者の追跡に焦点を当てたLucaなどの接触追跡ソリューションでは、システムが場所を追跡する必要があるため、場所に関するデータが漏洩する危険性もある。システムがバーやレストランなどにのみ使用されている場合、リスクは低いと考えられるが（こうした場所はおそらくすでに公開されているため）、そうはいかない場所も存在する。こうしたシステムがより広範囲に展開されると、位置に関するデータが漏洩することのリスクが確実に浮かび上がってくる。実際、オーストラリアの同様のシステムのデータベースから情報漏洩が発生した際に、防衛施設や家庭内暴力保護施設の場所が明らかになってしまった。¹⁰⁷

害悪からリスクへ。これまで述べたリスクは主に個人データ（社会的接触、位置データ、健康状態）に関連するものであった。ただし、リスクは人々のグループに関わる場合もありえる。これらのリスクを特定するために、**人道団体**はトップダウンのアプローチを適用すると良いだろう。接触者追跡アプリに関しては、市民社会団体は、偏見を生み出すという害悪を見出している。それは、さまざまな形のリスクとして現れる可能性がある。第一に、このシステムが医療データのヒートマップ作成に使用されるリスクがある。こうしたヒートマップが作成されることにより、たとえば、移民者が多く住む地域で新型コロナウイルスの感染者や接触者の発生率が高いことが判明した場合などに、特定の場所や地域に不名誉な烙印が押されることになりかねない。同様に、発端患者に関する人口統計情報が漏洩するリスクもある。これは、たとえば、特定の病気の有病率が同性愛者の男性の間で高いことが判明した場合、特定のマイノリティに対する偏見を生み出す結果となりえる。

¹⁰⁷ Jonathan Kearsley と Clair Weaver, 「Sensitive business addresses among 500,000 published in COVID data breach（新型コロナウイルスのデータ侵害で、機密性の高い施設を含む50万件の住所が漏洩）」、Sydney Morning Herald、2022年2月14日：www.smh.com.au/politics/federal/sensitive-business-addresses-among-500-000-published-in-covid-data-breach-20220214-p59wal.html

最後に、プライバシーなどの人権は、データの秘密を保持したり、開示を最小限に抑えたりすることに必ずしも関連しているわけではない。代わりに、移動の自由などの権利に関連付けることができる。こうしたリスクを引き出すには、システムが何に使用されるのか、または使用される可能性があるのかを熟考することが肝要である。たとえば、接触追跡アプリから通知を受けることにより、ユーザーは自己隔離を行うことになる。これは重大な移動制限である。このようなメカニズムが悪用される可能性があり、市民のコントロールというリスクにつながる可能性がある。

6.3.3.2 リスクの存在の評価

リスクが特定されれば、**人道団体**はそれを利用して新しいシステムの設計を推進したり¹⁰⁸、既存のシステムの設計を評価したりすることができる。本章では、後者のプロセスについて説明し、リスクの軽減を、技術を活用した目的制限の実施へと結び付けていく。

システムの技術的設計がすべてのリスクを軽減するかどうかを評価することは、専門的な技術知識を必要とする困難なプロセスである。**人道団体**は、この知識を持ち合わせていないかもしれない。したがって、**人道団体**はリスクを特定し（前のセクションを参照）、特定されたリスクを、提案されたシステムがどのように、そしてなぜ軽減するのかを判断するために、サポートを求める必要がある。これは、システムの設計者にリスクへの対応法王について説明を求めるか、テクノロジーの外部評価を実施できる、プライバシー攻撃の開発と展開に関する知識を持った専門家（学者など）に問い合わせることで実行できる。

プライバシー保護を重視した接触追跡システムに、目的制限が設けられているのはなぜか。接触追跡アプリに関する、既に述べたリスクを思い出していただきたい。社会的接触情報の漏洩リスクについては、社会的接触に関

¹⁰⁸ 以下の例を参照されたい。

Seda GürsesとCarmela TroncosoおよびClaudia Diaz, “Engineering privacy by design reloaded（再考されたプライバシーバイデザインのエンジニアリング）”, *Amsterdam Privacy Conference*, 2015: <http://carmelatronicoso.com/papers/Gurses-APC15.pdf>
Jaap-Henk Hoepman, “Privacy design strategies (Extended abstract)（プライバシー設計戦略（詳細要約））”, *IFIP Advances in Information and Communication Technology*, No. 428, 2014年1月1日, pp. 446–459

連するすべての情報（受信した乱数のリスト）はそれぞれのユーザーのデバイスにのみ保存され、デバイスから外部に流出することはない。したがって、この設計により、このリスクは軽減される。

位置情報漏洩のリスクについては、アプリは位置情報を一切収集しない。したがって、システム内には漏洩または悪用される位置データは存在しない。ただし、データ保護リスクすべてが直接的に顕在化するとは限らない。デバイスが、Bluetoothビーコンで乱数をブロードキャストすることを思い出していただきたい。システムの外部に傍受インフラが存在する場合、乱数はユーザーの追跡に利用される可能性がある。スマートフォンが作り出す乱数は15分ごとに入れ替わるため、陰性のユーザーを追跡することはできない。

同時に、DP3T設計では、陽性ユーザーの追跡リスクを完全になくすことはできない。既に述べたように、陽性のユーザーがブロードキャストしたすべての乱数をサーバーにアップロードすることで、他のデバイスで曝露量の計算を行うことができるようになる。性能の最適化により、同じ日に同じ陽性ユーザーによってブロードキャストされたすべての乱数は相互にリンクされる。これにより、Bluetoothの通信範囲内であれば、陽性ユーザーを追跡することが可能になる。ここでは、展開可能なシステムを設計する必要があるため、リスクが増大することに注意されたい（図6.2も参照のこと）。

機密の医療データに関しては、ユーザーが曝露されたかどうかをスマートフォンがローカルで判断し、通知が行われる。この通知に関するデータが他者に伝達されることはない。これにより、個人の曝露に関するデータもグループの曝露に関するデータ（ヒートマップ）も漏洩することはない。既に述べたように、通知を行う接触追跡システムでは、陽性ユーザーを特定できる可能性がある。この設計にもそれが当てはまる。

最後に、分散型設計により、誤って通知をトリガーすることが困難になるため、市民のコントロールの可能性を抑えることができる。スマートフォンが、(1) 乱数を受信し、それが近隣のデバイスからのものであると解釈し、(2) この乱数が、サーバーからダウンロードされた陽性者の番号リストの中にあつたときに、通知を表示することはすでに説明した。誤った通知をトリガーするには、攻撃者が

Bluetoothを介して乱数を送信できるほどターゲットに近づき、サーバーをだましてアップロードを受け入れさせる必要がある。どちらも厳密に言えば不可能なことではないが、この攻撃を実行するのは、大きな規模では、困難であると考えられる。

いくつかの残留リスクが残っているとしても、システム内のデータを使用することで、これらのリスクはいずれも現実化することはない。システムはその設計において、目的が通知のみであることを保証することができる。

目的制限を設けていない接触者追跡システム。 反対の例として、通知を目的としているが、目的制限を設けていない、別の接触追跡システム、ドイツで提案されたNeedToKnow (NTK) システムについて見てみることにする。¹⁰⁹ 分散型設計と同様に、NTKがインストールされたデバイスでは、番号が交換され、ローカルに保存される。ただしNTKでは、(1) これらの番号はランダムではなく、サーバーはすべてのユーザーの送信番号を知っており、(2) 陽性ユーザーは、自分が受信した番号のリストをアップロードする。サーバーは番号と人を結び付けることができるため、こうしたシステムはユーザーの追跡に利用される可能性がある。たとえば、法執行当局は容疑者の番号のリストを要求し、Bluetooth受信器を使用してその容疑者を追跡することができる。実際、シンガポール¹¹⁰でもドイツ¹¹¹でも、人を追跡するために接触者追跡システムが実際に使用された。

109 Pan-European Privacy-Preserving Proximity Tracing (汎ヨーロッパ・プライバシー保護接近追跡) (PEPP-PT)、*High Level Overview*, 2022年: <https://github.com/pepp-pt/pepp-pt-documentation/blob/8ba05287c349318a03837fe374fd949e60d4eaf8/PEPP-PT-high-level-overview.pdf>

110 Mia Sato, 「Singapore's police now have access to contact tracing data (現在シンガポール警察は、接触追跡データにアクセス可能)」, *MIT Technology Review*, 2021年1月5日: www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid

111 Rachel Pannett, 「German police used a tracing app to scout crime witnesses. Some fear that's fuel for covid conspiracists (ドイツ警察は追跡アプリを、犯罪目撃者を探すために使用した。それが新型コロナ陰謀論者を刺激することを懸念する声も。)」, *ワシントン・ポスト*, 2022年1月13日: www.washingtonpost.com/world/2022/01/13/german-covid-contact-tracing-app-luca

さらに、陽性ユーザーは受信した番号のリストをサーバーにアップロードし、サーバーは数字を個人と関連付けることができるため、サーバーは陽性ユーザーの社会的な交流を知ることができる。最後に、システムはどのユーザーが陽性であり、どのユーザーに通知されたかを知ることができる。

この分析を考慮すると、システム内で作成・収集されたデータは、ユーザーへの通知以外の目的にも使用できることは明らかである。したがって、このシステムは技術を活用した目的の制限を行っていないと言える。

6.4 データ最小化の役割

規制のフレームワークや研究者は、プライバシーやデータ保護の実践の指針となる多くの原則を提案してきた。設計によって行われるプライバシーとデータ保護の保証を判断するために使用される重要な原則の1つが、データ最小化原則である。¹¹² データ管理者は、所定の目的のためにデータが必要な場合にのみ、データ収集を行うことが求められる。これらのデータは、その目的を達成するために必要な期間のみ保全されるべきである。この原則は技術文献にも反映されている。¹¹³

データの最小化は間違いなく、プライバシー保護を重視した設計の必要条件である。システム運用に不必要なデータを収集せず、不要になったデータを削除することで、システム利用者のプライバシーリスクを軽減する。たとえば、アグリゲーションやプライバシー保護暗号の使用によって、保存される情報の量を削減することで、ユーザーのプライバシーが侵害される可能性が減り、彼らの権利や尊厳が脅かされるリスクも減らすことができる。

¹¹² セクション2.5.4：データ最小化の原則を参照

¹¹³ Hoepman は、プライバシーに配慮した設計を作成するための重要なテクニックの1つとしてデータの最小化について述べており、Gürsesらは、プライバシーに配慮した設計を作成するには、データの最小化という観点から考える必要があると主張している。

Jaap-Henk Hoepman, "Privacy design strategies (Extended abstract) (プライバシー設計戦略(詳細要約))", IFIP Advances in Information and Communication Technology, No. 428, 2014年1月1日, pp. 446-459

Seda GürsesとCarmela TroncosoおよびClaudia Diaz, "Engineering privacy by design reloaded (再考されたプライバシーバイデザインのエンジニアリング)", Amsterdam Privacy Conference, 2015: <http://carmelatronicoso.com/papers/Gurses-APC15.pdf>

ただし、データ最小化の原則を適用してシステムが実現する保護レベルを評価するのは必ずしも簡単なことではない。アプリがとある連絡先に関する詳細情報を中央サーバーに送信する、(プライベートではない) 連絡先追跡システムを例に考えてみよう。サーバーは受信したデータを使用して感染者の接触者を特定し、通知する。この場合、サーバーには機密性の高い社会的交流に関するデータが保存される。サーバーでのデータ収集と処理を最小限に抑えるため、プライバシーに配慮した設計により、アプリはローカルに保存されたやり取りの記録に基づいて、ユーザーのデバイス上でローカルに、ユーザーのウイルスへの曝露を計算することができる。

しかし、データの最小化がすぐに不十分になる可能性がある。驚くべきことに、ユーザーのデバイスやサーバーを含むプライバシーに配慮したシステム全体を調べると、データの最小化は行われていないことが分かる。システムとして見ると、集中型システムと分散型システムの両方が連絡先データの収集、処理、保存を行っている。違いは、これらのデータが保存される場所にある。集中型システムにおいては、データのほとんどが中央サーバーに保存されるが、プライバシー保護を重視したシステムにおいては、ユーザーのデバイスとサーバー全体に分散して保存される。

その結果、データ最小化原則を適用しても、アナリストはこれら2つの設計を区別することはできない。たとえそれらが明らかに異なるプライバシーとデータ保護に関する特性を持っていたとしてもである。設計による目的制限アプローチでは、この問題は発生しない。さらに、設計によって目的制限を設けたシステムは、データの最小化をも、設計によって実現する。ユーザーの制御がおよばないエンティティでは、目的によって明示的に許可されているデータのみが利用できる。さらに多くのデータが利用可能な場合、これらのデータは他の目的に使用される可能性があるため、目的制限に違反することとなる。

6.5 目的制限に対する課題

前セクションでは、目的の制限の原則とデータの最小化の原則について述べた。そしてこれらが、強固なプライバシー保護と、権利および尊厳の保全を実現するシステムの設計と評価のための指針として使用できることを示した。本セクションでは、設計者の目的制限の実現を妨げる可能性のある設計に関する側面について説明していく。これは即ち、評価者がシステムによって実現される保護レベルを理解するために、求めるべきものでもある。

- **要件の不足または要件の進化。**現在のソフトウェア開発サイクルにおいては、システムの要件は設計プロセスの開始時に完全に具体化されていることはない。代わりに、デザイナーはアジャイルな方法でそれらを拡張し、修正する。これは開発と展開の観点からは非常に望ましいものの、こうした開発手法を使用すると、システムが実現できるプライバシー保証が大幅に制限される。要件が明確でない場合、目的を特定し、目的の制限を念頭に置いて設計を特定することは困難である。目的に柔軟性を持たせなければならない場合、強固なプライバシー、さらには個人の権利と尊厳の保護を保証するために設計者ができることはほとんどない。
- **第三者サービスへの依存。**現在のソフトウェアの2番目の特徴は、設計者と開発者がシステム内のすべてのモジュールをプログラムしないことにある。彼らは他者によってプログラムされ、実行されたツール、ライブラリ、サービスに依存している。これにより開発がスピードアップし、低コストで優れた性能の高品質の専用モジュールが利用できる。ただし、これらの要素を使用することで、目的を制限したシステムの適用が妨げられる。これらの**第三者**の要素は、それらのインターフェイスを介して、アプリケーションが使用できるデータやフォーマットを制限する。これにより、設計者が使用できるプライバシーを重視したテクノロジーの数が制限される。ほとんどが**第三者**サービスの要件と互換性がないためである。
- **すべてのシステムレイヤーがデータ保護において役割を果たす。**人道団体は、プライバシー保護に関して、その目的は何か、どんなデータが必要か、データはどこに保存・処理されるかなど、アプリケーションの観点から考えることが多い。実際には、アプリケーションのデータは、システム内に存在

する全体的な（メタ）データのごく一部であり、これらが**データ主体**の権利と自由の侵害につながる可能性がある。この意味において、プライバシーを最も弱いリンクプロパティと考えることが重要である。すべてのレイヤーで保護が確保されるか、ユーザーの保護は最も弱いレイヤーによって提供される保護に限定される。

たとえば、接触追跡システムのリスクの1つは、攻撃者がどのユーザーが陽性かを知ることである（セクション6.2.1 - 分散型のプライバシー保護を重視した接近追跡を参照）。ここで最も弱いリンクは、アプリケーション（陽性者をサーバー以外のすべての人から見えなくする）ではなく、ネットワークレイヤーである。陽性ユーザーのみが中央サーバーにデータをアップロードすることを思い出していただきたい。したがって、ネットワークを監視している者は、このネットワークトラフィックの存在のみに基づいて、ユーザーが陽性であると結論付けることができる。つまり、展開されたシステムは、このようなネットワーク攻撃者に対する対策を使用する必要がある。¹¹⁴

- **技術的に実行可能なもの。**最も強固な目的制限を実現するために、使用するテクノロジーを決定することは困難である。多くの場合、最も強固な制限を実現するシステムには、接触アプリの場合のように、非主流の技術の使用、または新しいテクノロジーの開発が必要である。**人道団体**はこのような知識は持っておらず、多くの場合、委託を受けた製品開発者も持っていないかもしれない。評価と同様、**人道団体**は学術機関と提携して、利用可能な技術と設計に関する知識を得ると良いだろう。これらの設計が財務上または運用上、実行可能でない場合でも、どのような状況が理想的であるかということについての知識は、システムが望ましいものかどうかについて団体がより良い決定を下す上で、役立つであろう。

¹¹⁴ セクション5.2.5: リスクの特定 を参照

ドローン

利用可能性

搜索救助活動

緊急事態地域の把握

従来の
支援活動の
補完

課題

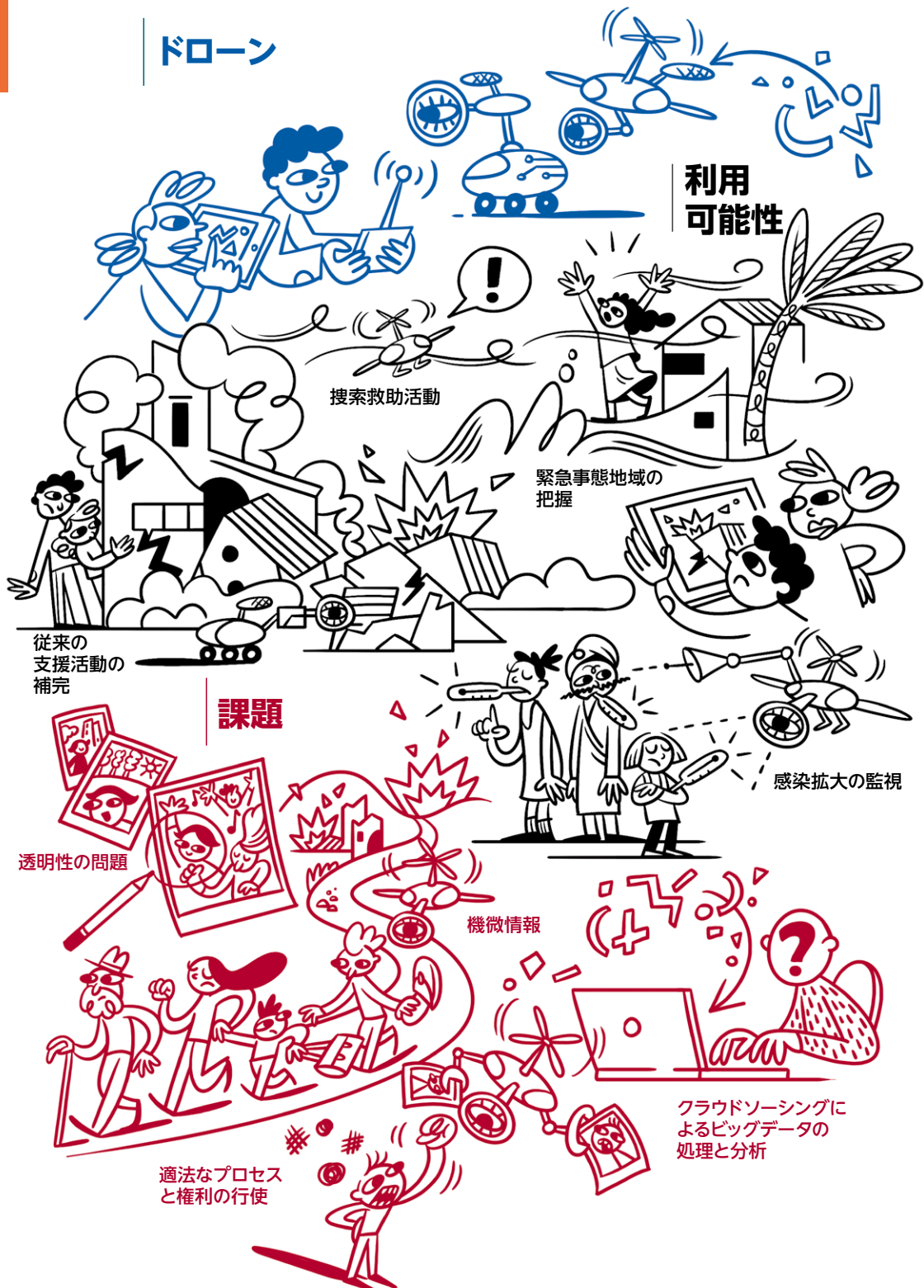
感染拡大の監視

透明性の問題

機微情報

適法なプロセス
と権利の行使

クラウドソーシングに
よるビッグデータの
処理と分析



第7章

ドローン／ 無人航空機と リモートセンシング

MASSIMO MARELLI

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。

- 搜索救助
- 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。」¹¹⁵ 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。¹¹⁶

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。¹¹⁷ 安全性の問題そのもの（例えば、稼働中の事故により、

¹¹⁵ Joint Legislative Committee on Emergency Management and the Senate Committee on Judiciary, *Drones and Emergencies: Are We Putting Public Safety at Risk?*、公聴会、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.10 : https://sjud.senate.ca.gov/sites/sjud.senate.ca.gov/files/background_paper_-_drones_and_emergencies.pdf

¹¹⁶ アメリカ赤十字社、*Drones for Disaster Response and Relief Operations*、2015年4月 : www.issue4lab.org/resources/21683/21683.pdf

¹¹⁷ Florian Delafoi, *Le drono, l' allié ambigu des humanitaires*, *Le Temps*, 2016年4月11日 : <https://www.letemps.ch/monde/2016/04/11/drone-allie-ambigu-humanitaires>
ICTworks, “What Do Tanzanians Think About Drones? Now We know ”, ICTworks (ブログ)、2016年2月22日 : <https://www.ictworks.org/what-do-tanzanians-think-about-drones-now-we-know/>

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。

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。¹¹⁸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

¹¹⁸ Article 29 Data Protection Working Party, *Opinion 01/2015 on Privacy and Data Protection Issues Relating to the Utilisation of Drones*, 欧州委員会、2016年11月23日、p.7: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602

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。¹¹⁹

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。¹²⁰
- （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。¹²¹
- 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

¹¹⁹ 同上、p.14

¹²⁰ Storyhunter, “Storyhunter Guide to Commercial Drone Regulations around the World”, Medium (ブログ)、2018年4月3日: <https://blog.storyhunter.com/storyhunter-guide-to-commercial-drone-regulations-around-the-world-5795c31165d9>

¹²¹ 第17章：人工知能を参照

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。¹²²

- 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、特定の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考慮すべきである。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。

¹²² 例えば、“Guidelines”、Humanitarian UAV Code of Conduct（ブログ）、2017年12月6日：<https://uavcode.org/further-guidance>

“Humanitarian UAV Guidelines on Data Protection（データ保護に関する人道的UAVガイドライン）”、“Humanitarian UAV Guidelines on Data Protection”（ブログ）、2017年12月6日：<https://uavcode.org/further-guidance/131-2>を参照

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。¹²³

- データ主体または他の者の生命に関わる利益
- 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
- 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、窮地にあり人道援助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。

「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、

¹²³ 第3章：個人データ処理の法的根拠を参照

データ保護法の下で、有効な法的根拠として使用するには、個人から同意を得る必要がある。

例：

自治体の長や関係する国の当局は、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**するかもしれないが、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**または他の者の生命に関わる利益になる可能性があるとして**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（セクション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**の生命に関わる利益になるとみなされることがある。¹²⁴

人道団体による**ドローン**の使用は、**データ主体**または他の者の生命に関わる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。

¹²⁴ 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

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。

例：

人道団体による搜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）の生命に関わる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**の生命に関わる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、公共の利益または生命に関わる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。

- 搜索救助
- 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和均衡性について厳密な評価が行われるべきである。¹²⁵ 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、均衡する技術

¹²⁵ 第2章：データ保護の基本原則を参照

を選択し、バイデザインかつバイデフォルトのデータ保護・プライバシーの措置を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**されるべきである
- 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削除または匿名化されるべきである。保存と削除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削除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削除すべきである。**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）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。

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。¹²⁶ 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。¹²⁷

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、情報通知キャンペーン、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、

¹²⁶ 第2章：データ保護の基本原則を参照

¹²⁷ セクション2.11：データ主体の権利を参照

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。

ドローンの場合、個人が調査地域を避けることができない可能性、そして**ドローン**センサーによるデータ収集に気づかない可能性さえあるため困難な場合があるものの、**データ主体**は**処理**を拒否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、データの訂正と消去が可能になる。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。¹²⁸

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¹²⁹
- 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

¹²⁸ 第4章：国際的なデータ共有を参照

¹²⁹ 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

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¹³⁰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データ保護影響評価を実施することは、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。¹³⁰

¹³⁰ 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



課題



第8章

バイオメトリクス

MASSIMO MARELLI*

* 情報とご意見をいただいた、Vincent Graf Narbel氏およびJustinas Sukaitis氏に感謝の意を表する。

8.1 はじめに

国際標準化機構（ISO）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。¹³¹ 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、データ保護・プライバシー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。¹³²

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

¹³¹ 国際標準化機構（ISO）、ISO/IEC 2382-37:2022 情報技術用語、語彙パート37：バイオメトリクス、2022年3月：<https://www.iso.org/standard/73514.html>を参照

¹³² 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9月16日：https://edps.europa.eu/sites/default/files/publication/05-09-16_resolution_biometrics_en.pdfを参照

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。¹³³

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。¹³⁴ 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。¹³⁵ 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。同時に、第三者は、ハッキングなどの不正な手段によってバイオメトリクスデータにアクセスすることに興味を持っている可能性がある。

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。¹³⁶

技術開発の現状では、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。

¹³³ 以下の例を参照されたい。Hugo Slim, “Eye Scan Therefore I am: The Individualization of Humanitarian Aid”, European University Institute (ブログ)、2015 年3月15日: <https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid/>、Paul Currión, “Eyes Wide Shut: The challenge of humanitarian biometrics”, *The New Humanitarian* (旧 IRIN News)、オンライン版、sec. Solutions and Innovations | Opinions: IRIN, 2015 年8月26日: www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics

¹³⁴ Gus Hosein と Carly Nyst, *Aiding surveillance*, Privacy International, 2013年11月1日、p.16: <http://privacyinternational.org/report/841/aiding-surveillance>.

¹³⁵ 同書、p.33-36

¹³⁶ 第9章: 現金およびバウチャー支援を参照

- 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（前項の結果として）
- 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

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人々の場合の指紋の判読不能）
- バイオメトリクス情報は固有のものであり変更できないため、データ漏洩が発生した場合、その影響を受ける人々は、バイオメトリクス情報の合成という手段を通じて、個人情報の盗難にさらされる可能性がある
- 最新のバイオメトリクスシステムのハードウェアおよびソフトウェアのモジュールは、ソリューションプロバイダー間で互換性がないため、**人道団体**がひとつのベンダーに固定されてしまう可能性がある
- バイオメトリクスデータには、認証や識別目的に絶対的に必要な情報よりも多くの個人に関する情報が含まれているため（健康に関する情報など）、**バイオメトリクス**は本質的に過剰な情報である

- 倫理的問題（文化的感受性、影響を受けた人々の認知および/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。¹³⁷

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。¹³⁸

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。¹³⁹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。

¹³⁷ 以下の例を参照されたい。Massimo MarelliとBen Hayes, “Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy”, Humanitarian Law & Policy Blog（ブログ）、2019年10月18日：<https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy>

¹³⁸ 2016年4月27日欧州議会及び閣僚理事会のEU規則2016/679、第4条（14）

¹³⁹ 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、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。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。¹⁴⁰

¹⁴⁰ 例えば：Patrick Tucker, “How Facial Recognition Might Stop the Next Brussels”, Defense One, 2016 年 3 月 22 日：<http://www.defenseone.com/technology/2016/03/how-facial-recognition-might-stop-next-brussels/126883/> を参照

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。

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。¹⁴¹

- データ主体または他の者の生命に関わる利益
- 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、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**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、

¹⁴¹ 第3章：個人データ処理の法的根拠を参照

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せられる場合）
- 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で不可逆的な性質により、**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
- 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、個人やその家族が生き残るために人道援助に依存している場合、または個人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、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者の生命に関わる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**もしくは他の者の生命に関わる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

の者の生命に関わる利益そのものが、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る。

さらに、その人物の生命に関わる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**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、関係する個人の生命に関わる利益に應えるものではない。

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、その個人の生命に関わる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。

この分野の最後の考察事項は、**人道上の緊急事態**の影響を受ける人々に明確かつ一義的なアイデンティティを確立する上でのバイオメトリクスデータの本質的価値と、これが人々の尊厳の回復や強化、およびデータに対する権利の保護において果たし得る役割に関するものである。この観点から考慮すると、**データ主体**としての個人の生命に関わる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、関係者の**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、生命に関わる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/または生命に関わる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OMETRICS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、人道援助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OMETRICS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OMETRICS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、第三者がデータに不正アクセスしたり、人道団体に対して、こうした機微データを提供したり人道以外の目的で使用するよう圧力をかけたりする可能性があるという確実なリスクがある場合に特に重要である。

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。¹⁴² 「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OMETRICS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。

¹⁴² 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

8.2.3 目的制限と追加的处理

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、人道援助の配布、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

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、¹⁴³ 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。

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、これらの目的に均衡している必要がある。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。特に、バイオメ

¹⁴³ セクション8.2.3：目的制限と追加的処理を参照

トリクスの生データが処理され、認証または識別の目的でさらに使用するために保存する準備が整い次第、中間または元の生のバイオメトリクスデータはすべて削除する必要がある。

同様に、収集されるバイオメトリクスのデータセットは、目的に均衡する範囲内に限定されるべきである（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、均衡とはみなされないことがある）。

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。

最後に、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：

ある人を特定し、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均衡であり、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**追加処理**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、¹⁴⁴ データ処理の目的および手段を決定した、十分かつ均衡な安全対策が**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。

8.2.7 本質的な「過剰性」

バイオメトリクス情報の機微性の背後にある理由の1つは、この情報は本質的に、過剰な**処理**を引き起こす性質を持っているという事実である。バイオメトリクスシステムとバイオメトリクス情報には、データとそのデータの元となる個人との間の本質的なつながりが含まれている。現在の最先端のバイオメトリクス技術では、バイオメトリクスデータが処理される際に、認証や、ほとんどの場合識別の目的で厳密に必要とされる情報よりも多くの個人情報の処理が行われてしまっている。データにより、個人の健康、性別、民族性、その他の個人情報が明らかにされる場合がある。¹⁴⁵

リスクが完全に緩和されることは決してないかもしれないものの、**人道団体**は、バイオメトリクスデータのセキュリティをより引き上げるか、組織のニーズや、影響を受ける人々やコミュニティに対するメリットがこの本質的なリスクを上回るかどうかを再評価しなければならない。

¹⁴⁴ 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/>

¹⁴⁵ Daniel HartungとChristoph Busch, “Why Vein Recognition Needs Privacy Protection”, IEEE Press, 2009年, pp. 1090–1095: <https://doi.org/10.1109/IIH-MSP.2009.132>.
Justinas Sukaitis, “Building a Path towards Responsible Use of Biometrics”, thesis, EPFL, Lausanne, 2021年: <https://infoscience.epfl.ch/record/285077>.
Stelvio Cimato 他, “Privacy in biometrics”, Nikolaos V. Boulgouris, Konstantinos N. Plataniotis and Evangelia Micheli-Tzanakou (共編), *Biometrics: Theory, Methods, and Applications* 所収, Wiley-IEEE Press, Hoboken, NJ, 2010年, p. 633–654.

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、第三者が生体認証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。これは、例えば、再定住を促進するために、難民のバイオメトリクスデータを関係国と共有する場合に当てはまる。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。

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。¹⁴⁶ **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、¹⁴⁷ 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。**

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。

¹⁴⁶ セクション8.2.1：個人データ処理の法的基盤を参照

¹⁴⁷ セクション8.7：データ保護影響評価を参照

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
保全

データ
共有

互換性のない
追加使用

第9章

現金および バウチャー支援

MASSIMO MARELLI

9.1 はじめに

現金およびバウチャー支援¹⁴⁸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のセットである。**現金およびバウチャー支援**、現金給付プログラム、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、すなわちバウチャーと現金の両方、および全ての種類の物理的・デジタル的なデリバリーメカニズムを包含すると理解される。¹⁴⁹

送金は、人道的な影響を受けている人々の選択と彼らが直面するトレードオフへの尊重を最大化する支援である。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、または人道的な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**現金およびバウチャー支援**が採用され続けている。¹⁵⁰

デジタル的に提供される現金支援にはさまざまな形式（デジタル的に使用したり現金に変換したりすることができる、金銭的価値を持つ電子的なキャッシュ（モバイルマネー、プリペイドカード、銀行振込など）があり、そのすべてが制限なく使用される。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）

¹⁴⁸ 第2版では「現金給付プログラム」という用語を用いていたが、最近の人道支援分野でより広範に用いられている「現金およびバウチャー支援」を使用することとした。

¹⁴⁹ キャッシュラーニングパートナーシップ（CaLP）のCash Transfers Glossaryを参照。2022年1月20日アクセス：www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/calp-glossary_of_cash_transfer_programme_terminology.pdf.

¹⁵⁰ 人道的現金給付に関するハイレベルパネル、“Doing Cash Differently: How Cash Transfers Can Transform Humanitarian Aid”、グローバル開発センター、ロンドン、2015年9月14日、11：www.cgdev.org/publication/doing-cash-differently-how-cash-transfers-can-transform-humanitarian-aid

人に送られ、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。¹⁵¹ 紙のバウチャーの他に、現金が使われることもある。

現金およびバウチャー支援を通じて提供される人道援助の有効性と適切性は状況によって異なることが広く認識されている（人々が特定の状況において、必要な物品を入手できるかなど）。¹⁵² **現金およびバウチャー支援**については懸念（現地市場のインフレなど）も提起されているものの、「現物での代替手段と比較してコストパフォーマンスが良い」ことを裏付けるエビデンスがある。¹⁵³

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。¹⁵⁴

- 危機の影響を受けている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、人道援助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援助の説明責任の向上
- 限られた予算のさらに有効な活用に向けた人道援助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援助の支持の増大
- 人道対応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

¹⁵¹ 欧州委員会、人道的ニーズに対応するための多目的現金ベース支援に関する10の共通原則、2015年3月：http://ec.europa.eu/echo/files/policies/sectoral/concept_paper_common_top_line_principles_en.pdf; 欧州委員会、人道的危機における現金およびバウチャーの使用。DG ECHO 資金調達ガイドライン、2013年3月11日：https://ec.europa.eu/echo/files/policies/sectoral/ECHO_Cash_Vouchers_Guidelines.pdf

¹⁵² Paul Harvey and Sarah Bailey, Cash transfer programming and the humanitarian system, Background Note for the High Level Panel on Humanitarian Cash Transfers, Overseas Development Institute, ロンドン、2015年3月：<https://odi.org/sites/odi.org/en/publications/cash-transfer-programming-and-the-humanitarian-system>

¹⁵³ 同上

¹⁵⁴ 人道的現金給付に関するハイレベルパネル、現金給付方法の変更、p.8

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、**現金およびバウチャー支援**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援助に反対する場合、あるいは関連市場がインフレのリスクにある場合など）。¹⁵⁵ 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、より広範な人道援助プログラムの一部である。¹⁵⁶

現金およびバウチャー支援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的・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。**現金およびバウチャー支援**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、**現金およびバウチャー支援**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。¹⁵⁷

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。

¹⁵⁵ 同上

¹⁵⁶ 同上

¹⁵⁷ ICRC と Privacy International, The Humanitarian Metadata Problem: *Doing No Harm in the Digital Era*, “Chapter 6: Cash Transfer Programmes”, 2018 年 10 月: www.icrc.org/en/download/file/85089/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

モバイルマネーのデータが他の当事者に届く仕組み

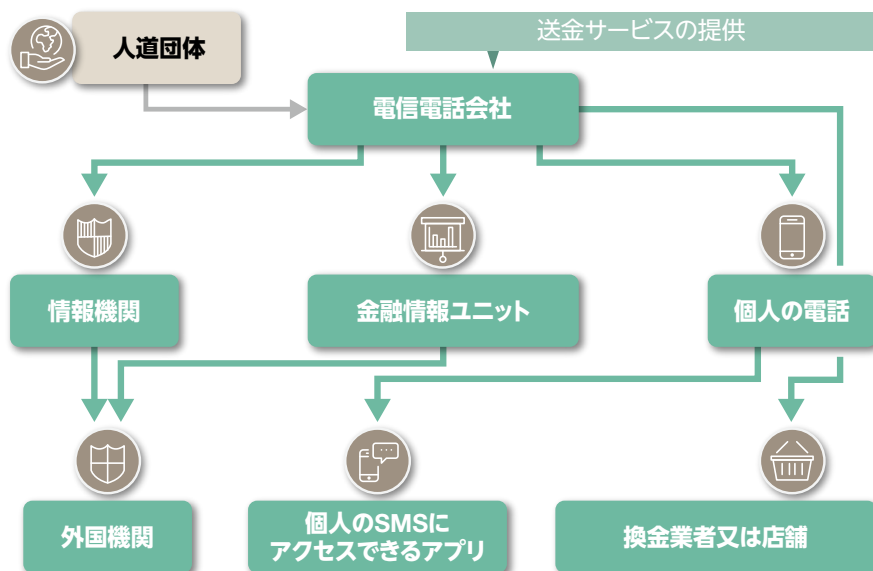
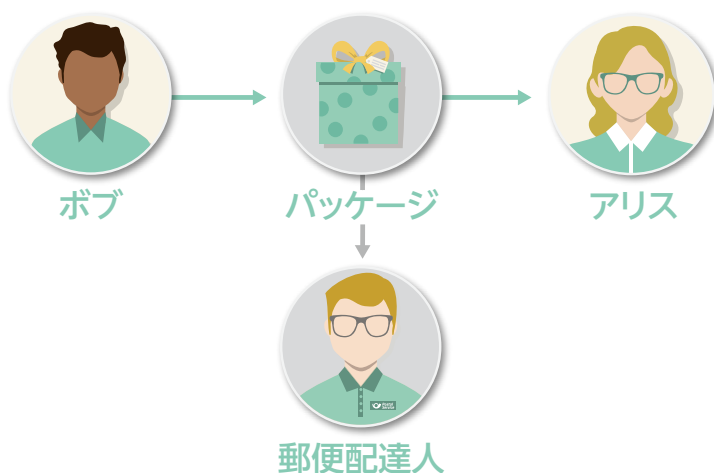


図9.1. ICRCとPrivacy International, The Humanitarian Metadata Problem: Doing No Harm in the Digital Era, Chapter 6: Cash Transfer Programmes, 2018年10月, p.73

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、人道的な影響を受けている人々をリスクにさらす可能性がある。¹⁵⁸ 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。

¹⁵⁸ これについてのより詳細な考察については、Jo Burton “‘Doing no harm’ in the Digital Age: What the digitalization of cash means for humanitarian action”, International Review of the Red Cross, Vol. 102, No. 913, 2020年4月, pp.43-73を参照: <https://doi.org/10.1017/S1816383120000491>。「目に見えなかった人々が目に見えるようになる」ことの長所と短所は、デジタル化された支援とデジタルアイデンティティを議題にしたDigitHarium Monthで議論された。ICRC、「DigitHarium Month #2: デジタル化された支援、社会的保護、および人道データに関する懸念」、赤十字国際委員会、2021年3月9日: www.icrc.org/en/digitharium/digitharium-month-2。ICRC、「DigitHarium Month #9: デジタルアイデンティティと人道支援」。赤十字国際委員会、2022年2月18日: www.icrc.org/en/digitharium/digitharium-month-9。

異なるタイプのデータ及びメタデータ



**郵便配達人は以下の点を考えて
パッケージの中身を推測できる**

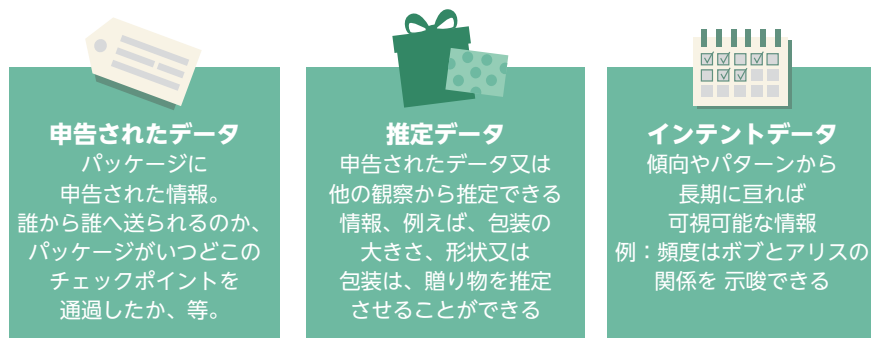


図9.2. ICRCとPrivacy International, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, Chapter 2: Processing data and metadata, 2018年10月, p.33.

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、現金およびバウチャー支援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。¹⁵⁹

¹⁵⁹ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, pp.68–69

9.2 データ保護基本原則の適用

現金およびバウチャー支援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、現金およびバウチャー支援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。現金およびバウチャー支援は、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 (KYC)¹⁶⁰、SIMカード登録¹⁶¹、その他の対象となる義務を遵守するために、人道的な影響を受けている人々からのデータ収集を求められる可能性がある。現金およびバウチャー支援のために収集された個人データは、他の種類の人道援助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。¹⁶² 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、すなわち現金およびバウチャー支援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、保全には、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。¹⁶³ 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

¹⁶⁰ 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。

¹⁶¹ Kevin P. Donovan と 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: <https://doi.org/10.5210/fm.v19i2.4351>を参照

¹⁶² CaLP, "Protecting beneficiary privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes", 2020年, p. 4: www.calpnetwork.org/wp-content/uploads/2020/01/calpbeneficiary-privacy-web.pdf.

¹⁶³ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, pp.73-75

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。

援助を提供するために**現金およびバウチャー支援**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。¹⁶⁴

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、**現金およびバウチャー支援**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、人道的な影響を受けている人々の一部（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」¹⁶⁵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。¹⁶⁶

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**。¹⁶⁷

¹⁶⁴ セクション6.1：データ保護のための設計～はじめにを参照

¹⁶⁵ 定義された用語と略語の用語集を参照

¹⁶⁶ 第17章：人工知能、特にセクション17.1.2：人道分野における人工知能を参照

¹⁶⁷ セクション9.5：データ共有を参照

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。¹⁶⁸

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。

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の者の生命に関わる利益
- 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

現金および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¹⁶⁹。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¹⁷⁰。人道的な影響を受けている人々への支援の前提条件として個人情報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

¹⁶⁸ 第2章：データ保護の基本原則を参照

¹⁶⁹ セクション3.2：同意を参照

¹⁷⁰ ICRC と Privacy International, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, “Chapter 6: Cash Transfer Programmes”, 2018年10月, p.21

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べきである。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。¹⁷¹

- **現金およびバウチャー支援**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。
- 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**現金およびバウチャー支援**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

¹⁷¹ CaLP, “Protecting beneficiary privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes”, 2020 年、p. 14 : www.calpnetwork.org/wp-content/uploads/2020/01/calpbeneficiary-privacy-web.pdf.

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**または他の者の生命に関わる利益が、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**が得られず生命に関わる利益も適用されない場合には、**現金およびバウチャー支援**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。¹⁷² 具体的な目的は明確かつ正当なものであるべきであり、**現金およびバウチャー支援**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。

¹⁷² セクション9.3.1: 個人データ処理の法的根拠を参照

- 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全、信用力判定のための受益者のプロファイリング等。¹⁷³ 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。

- 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。

追加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。

¹⁷³ ICRC と Privacy International、*The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*、"Chapter 6: Cash Transfer Programmes"、2018年10月

現金およびバウチャー支援の場合、**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、これらの目的に均衡する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、**現金およびバウチャー支援**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。

現金および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**現金およびバウチャー支援**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。

現金およびバウチャー支援を使用するプログラムで考えられる**人道団体**の選択肢のひとつは、個人が特定された後、可能であれば、固有の識別子（受領者は最終受益者を特定できない）と分配される現金の金額をサービスプロバイダ（銀行やモバイルネットワーク事業者など）にのみ転送することである。これにより、個人へのリスクを限定することができる。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、データを他のソースと関連付けて再識別を可能にする場合には特に、現在の**仮名化**（または不完全な**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。¹⁷⁴

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、これらの理由で保全されるデータは、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。

¹⁷⁴ Larry Hardesty, “How Hard Is It to ‘de-anonymize’ cellphone data?”, MIT News | Massachusetts Institute of Technology (ブログ)、2013年3月27日: <https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>。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も参照。

9.3.5 データセキュリティ

現金およびバウチャー支援において収集、処理された**個人データ**の悪用の可能性を避けるために、適切かつ均衡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。¹⁷⁵

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、**現金およびバウチャー支援**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、通知され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。

¹⁷⁵ 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

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。

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。

現金および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

現金およびバウチャー支援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**が情報を収集したときと矛盾する、提供された情報の保全義務
- 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、**現金およびバウチャー支援**に関して非常に重要である。この点に関し、**現金およびバウチャー支援**については、セクション10.9：特権および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およびバウチャー支援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、現金およびバウチャー支援に関与する全ての機関と、(i) 国内および国際的に、主要なパートナーが誰であるか、(ii) 現金およびバウチャー支援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。¹⁷⁶

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および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。

¹⁷⁶ ICRCとPrivacy International, “The Humanitarian Metadata Problem”, 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。現金およびバウチャー支援は、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。

現金およびバウチャー支援のためのテンプレートDPIAは、キャッシュラーニングパートナーシップ（CaLP）が開発している。¹⁷⁷

¹⁷⁷ CaLP, “Protecting beneficiary privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes”, 2020 年、p. 18 : www.calpnetwork.org/wp-content/uploads/2020/01/calpbeneficiary-privacy-web.pdf.

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
全体に対する
限られた
コントロール

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

政府による
アクセスの可能性

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

監査の実施

第10章

クラウドサービス

PAOLO BALBONI

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。¹⁷⁸ 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。¹⁷⁹ 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。人道援助は情報を活用することで進められるため、クラウドコンピューティングサービスとそれに関連するデータ**処理**パラダイムは、**人道団体**にとって役立つツールと言えるだろう。それらのメリットには、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。¹⁸⁰

¹⁷⁸ Peter Mell と Timothy Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, National Institute of Standards and Technology, US Department of Commerce, メリーランド州 Gaithersburg, 2011年9月: <https://www.nist.gov/publications/nist-definition-cloud-computing>

¹⁷⁹ 欧州データ保護監督官（EDPS）, “Opinion of the European Data Protection Supervisor on the Commission’s Communication on ‘Unleashing the Potential of Cloud Computing in Europe’（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の意見）”, ブリュッセル, 2012年11月16日, p.4: https://edps.europa.eu/sites/default/files/publication/12-11-16_cloud_computing_en_o.pdf

¹⁸⁰ Dara G. Schniederjans と Koray Ozpolat と Yuwen Chen, “Humanitarian supply chain use of cloud computing”, *Supply Chain Management: An International Journal*, 2016年8月8日: <https://doi.org/10.1108/SCM-01-2016-0024>を参照

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¹⁸¹
- 効果的コントロールがおよばない下請け業者による長いデータ**処理**チェーン
- クラウドプロバイダやその下請け業者による、本来とは異なった目的で行われる追加**処理**
- クラウドプロバイダやその下請け業者による期間を延長したデータ保全
- 許可を得ていない（国際的）**データ共有**。

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で注目を集めた。¹⁸²

さらに、国際法の下で特権および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、その特権および免除を失い、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：特権および免除とクラウドで説明する。

¹⁸¹ 法執行機関によるクラウドへのアクセスについては、第11章：クラウドおよびガバメントアクセスを参照。さらに詳細な考慮事項については、例えば、Paolo BalboniとEnrico Pelino, “Law enforcement agencies’ activities in the cloud environment: A European legal perspective”, *Information & Communications Technology Law*, Vol. 22, No. 2, 2013年, pp.165-190を参照。

¹⁸² データ保護・プライバシーコミッショナー国際会議、クラウドコンピューティングに関する決議、（第34回データ保護・プライバシーコミッショナー国際会議、プンタ・デル・エステ / カネロネス、ウルグアイ、2012年10月26日）を参照：<http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Cloud-Computing.pdf>

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。¹⁸³

- 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クラウドサービスである。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。コミュニティクラウドは、共通の関心や懸念、要件（セキュリティ、コンプライアンス要件、管轄権、特権および免除など）を共有する多くの組織が共同で利用できる**クラウドサービス**である。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、

¹⁸³ 英国情報コミッショナーオフィス（ICO）、クラウドコンピューティングの使用に関するガイダンス、1.1版、2012年10月2日、pp.5-6 : <https://ico.org.uk/media2/migrated/1042330/cloud-computing-guidance-for-organisations.pdf>

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全、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。

コミュニティクラウドは、内部または**第三者**によって管理され、内部または外部でホストされる。したがって、その長所と短所は、どのように管理されるかによって異なってくる。興味深いことに、共通の関心、懸念、要件を共有する組織は協力することで、クラウドプロバイダに対してより多くの交渉力を持つことができ、同様の目的に適したカスタマイズされたサービスレベル合意（SLA）を達成することができる。¹⁸⁴

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

¹⁸⁴ クラウド契約の交渉については、以下を参照。Paolo Balboni “Managing legal compliance risk in the cloud and negotiating personal data protection requirements with vendors”, Cloud Computing Security: Foundations and Challenges, CRC Press、アビンドン、英国、2016年、pp.267-276

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 データ管理者とデータ処理者の関係

セクション 4.5 データ管理者とデータ処理者の関係で説明したように、個人データをクラウドに置く**人道団体**と、契約しているクラウドプロバイダとの関係は、一般的に言えば、**データ管理者とデータ処理者の関係**である。ただし、実際には、これらの役割をカテゴライズするのは見た目よりも難しい場合がある。というのも、これはクラウドプロバイダがどの程度の裁量権を持っているかに依存するものであり、その裁量権はプロバイダとクライアントの間の契約によって定義する必要があるものであるためである。重要なことは、こうした不確かさが**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使用について可能な限り透明性を確保し、クラウドプロバイダがデータ主体に不利益を与えないようにしなければならない。

人道団体によるクラウドサービスの使用には通常、クラウドプロバイダによる**サブプロセッサ**の雇用が伴う。プロバイダとの契約には、**データ管理者（人道団体）**が与えた許可に基づいてのみ、**サブプロセッサ**を使用できることを明記する必要がある。**データ処理者（クラウドプロバイダ）**は、この点に関する変更が生じた場合は**データ管理者**に通知する明確な義務を負う必要があり、**データ管理者**はこうした変更により異議を唱えるか、契約を終了するかを選択肢を保持する。

10.3 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の関係は、**データ管理者**と**データ処理者**の関係と等しい。¹⁸⁵しかし、例外的に、クラウドプロバイダが**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。

例：

人道団体がクラウドプロバイダとの間で、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／セキュリティ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と隠し立てなく話し合い、プロバイダ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

¹⁸⁵ セクション10.2：データ管理者とデータ処理者との関係を参照

- 特権および免除を享受している**人道団体**、そのような特権および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くかを確認する

10.4 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。

10.4.1 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。¹⁸⁶

- 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

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。クラウドプロバイダが処理者としての役割を果たす場合、同じ法的根拠がクラウドでの**処理**にも適用される（**処理**の手段とみなされる）。ただし、クラウドプ

¹⁸⁶ 第3章：個人データ処理の法的根拠を参照

ロバイダが管理者としての役割を果たすその他の場合では、クラウドプロバイダとのデータ共有のための別の法的根拠を見つける必要がある。いずれのケースでも**人道団体**は、DPIAを実行することで、**人道団体**による排他的なデータ「管轄」管理が失われる可能性を含めた、個人に起こり得るリスクを特定し、それを適切に軽減する必要がある。

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は、**個人データ**を収集し、クラウドに保存することの十分な法的根拠となる（プロバイダは**人道団体**のために処理者としての役割を果たす）が、関連するDPIAが実施され、個人に対するリスクが十分に緩和されている必要がある。

10.4.2 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¹⁸⁷、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。これらのデータ保護の基本原則への準拠を確保するために**人道団体**が実施すべき基本的な第一の行動は**クラウドサービス**使用前にDPIAを実行することであり、第二の行動はサービス提供中に監査を行い、クラウド環境における継続的な適合性をモニタリングすることである。

¹⁸⁷ セクション10.4.1：個人データ処理の法的根拠を参照

10.4.3 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。典型的なクラウド環境では、多数のサブコントラクトが関与することがよくあるため、同様のことがクラウドサービスプロバイダのサブコントラクトにも当てはまることは指摘に値するだろう。**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ト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。

10.4.4 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、(もしあれば) サブコントラクター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との契約を検討している**データ管理者**は、プロバイダ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进行评估すべきである。

クラウドコンピューティングにおける透明性を確保するためのもうひとつの側面は、クラウドクライアントは、直接の契約関係にあるものだけでなく、それぞれの**クラウドサービス**の提供に関わるすべてのサブプロバイダ、そして**個人データ**が処理されるすべてのデータセンターの場所について通知を受ける必要があるという事実である。というのも、これらの要素は国際的なデータ共有のトリガーとなる可能性があるためである(セクション10.7: 国際的なデータ共有を参照)。

10.4.5 データ保全

人道団体は、明確で正当な、文書化された理由がない限り、**個人データ**が収集された目的の達成に必要な期間を超えて(団体または**データ処理者**によって) 保持されないようにすることが推奨される。こうした理由がない場合、団体および関連する**第三者**が保持するデータを破棄する必要がある。**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場合、データ保全のための関連する法的根拠に依存できない限り、団体およびデータにアクセスした**第三者**の両者は**個人データ**を削除する必要がある。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**が直ちに消去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。データの消去は、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。こうした場合、クラウドクライアントは、**クラウドサービスプロバイダ**が発行する破棄証明書、またはデータが新しい**クラウドサービスプロバイダ**に転送されたことを証明する適切な証拠を要求することができる。¹⁸⁸

データ消去の原則は、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消去する必要がある。（以前のバージョン、一時ファイル、更にはフラグメントも削除しなければならない。）

個人データを安全に消去するには、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**を効果的に削除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が上記の意味で安全な消去を保証すること、および、クラウドプロバイダとクライアントとの間の契約に**個人データ**消去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。

188 クラウドでのデータ削除方法の例としては、最初にデータベース、ストレージ、バックアップシステムからの削除を行い、そのうえで対象データの削除を確実なものにするため、データの上書き（例：データを0と1で上書きする）または暗号化シュレッディング（つまり、データの暗号化と暗号キーの破壊）を行うというやり方がある。こうした作業を実施した後は、データの処理方法と削除方法に関する管理文書や関連するアクティビティログなどといった削除のエビデンスを提供できる。注意点としては、データが削除されたことを100%保証することは非常に難しいことが挙げられる。たとえば、これを確実に行うには、クラウドクライアントはデータをクラウドに保存する前に強力なキーで暗号化し、キーを決して失くさないようにしなければならない。そして削除が完了したらキーを削除する。暗号化サービスプロバイダはキーとデータの両方に一度にアクセスすることがないため、これにより、100%に近い完全削除が可能となる（暗号化アルゴリズムによって異なる）。

10.5 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ューリジェンスを含む、**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¹⁸⁹

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全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

¹⁸⁹ クラウドサービスの導入については、たとえば Paolo Balboni 他、Procure Secure: A Guide to Monitoring of Security Service Levels in Cloud Contracts, European Union Agency for Cybersecurity、アッティキ、ギリシャ、2012年を参照：www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts.

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削除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**が安全に消去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、削除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）から得られる委任に基づいてのみ**サブプロセッサ**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、**サブプロセッサ**はクラウドプロバイダと同じ契約義務の対象となる。）特に、クラウドプロバイダ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。
- プロバイダの内部組織やそのデータ処理の契約が（**サブプロセッサ**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。¹⁹⁰

- **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

¹⁹⁰ 出典：第29条データ保護作業部会、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.

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がバックアップ回線、冗長ストレージ、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、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。¹⁹¹
- **移植性**：異なるクラウドプロバイダ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に移行することを決定した場合、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るはずである。

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。

¹⁹¹ セクション10.6：データ主体の権利を参照

10.5.1 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）¹⁹² 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）¹⁹³、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。

10.5.2 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。

10.5.2.1 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

¹⁹² 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：“API”、ウィキペディア、2022年1月13日アクセス：<https://en.wikipedia.org/w/index.php?title=API&oldid=1065488861>

¹⁹³ 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：“Virtual Private Network”、ウィキペディア、2022年1月16日アクセス：https://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=1065922505.

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。特権および免除を享受する**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および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。

10.5.2.2 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。

10.5.2.3 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。

10.5.2.4 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、削除、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、データを消去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。

10.5.2.5 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。

10.5.2.6 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。

10.5.3 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を評価する場合、そのクラウドプロバイダ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。

10.5.4 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。

10.5.5 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ない。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。主要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

10.5.6 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。

10.5.7 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。

10.5.8 サプライチェーン

クラウドプロバイダは、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。プロバイダは、**第三者**のサプライヤ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が機関にとって受け入れられない**第三者**のサプライヤを利用することを防止する契約を締結すべきである。

サプライチェーンに関するさらなる懸念としては、非人道的性質を持つ組織とサプライチェーンを共有するという選択が、安全に対して中立、公平かつ独

立した人道的アプローチをとる人道団体の能力にどのような悪影響をおよぼす可能性があるかということが挙げられる。¹⁹⁴

10.5.9 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確実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、団体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。

10.5.10 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、団体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。

10.5.11 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。

¹⁹⁴ Massimo Marelli, "The SolarWinds hack: Lessons for international humanitarian organizations", *International Review of the Red Cross*, Vol. 104, No. 919, 2022年3月28日, pp.1267-1284: <https://doi.org/10.1017/S1816383122000194>

10.5.12 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。

10.5.13 監査

サービスプロバイダは、独立した監査結果を利用できるようにするか、クラウドクライアントによる直接監査または信頼できる**第三者**への評価の依頼を行えるようにする必要がある。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。監査は、**クラウドサービス**の性質と目的に応じた適切な頻度で定期的に行われなければならない。この件に関するベストプラクティスは（これは認証および証明の監査で一般に認められているルールでもあるが）、これらの監査を少なくとも年に1回設定し、大幅な変更または監査の対象に関連する変更があった場合には追加の臨時監査を実行することである。

10.5.14 サービスの使用状況

団体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、その他クラウドと団体の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いといけない。

10.6 データ主体の権利

データ主体の権利（アクセス、訂正、消去、異議申し立てなど）は当然ながら、クラウドでの処理にも適用される。¹⁹⁵ 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の間の契約においては、クラウドプロバイダがデータ主体の権利の行使を容易に行えること、この協力がどのように提供されるかについての具体的な規定が含まれること、サブプロバイダとの関係においても、これらの権利の同様の行使が確実に保護されるようにすることが要求される必要がある。

10.7 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との如何なる契約においても、プロバイダ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の実行に先立って、関係するデータ主体の権利と自由に共有がおよぼす影響に特に注意を払って DPIA¹⁹⁶ を実行すること（データ転送影響評価など）で、かかる処理のデータ保護の観点からの合法性をさらに強化し、また該当する場合、人道団体の特権および免除を維持することに貢献する可能性がある。

¹⁹⁵ セクション2.11：データ主体の権利を参照

¹⁹⁶ セクション10.8：データ保護影響評価を参照

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。¹⁹⁷ 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。

10.9 特権および免除とクラウド

上記の考慮事項に加えて、特権および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および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および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。この問題は、クラウドにおける「データ主権」、つまり、クラウドやクラウドプロバイダがある国の法律の対象となるデータに適用される管轄管理権限または法的権限と密接に関係している。¹⁹⁸

人道団体は、その特権および免除がクラウド環境で適切に保護され、データに対する「主権」を守るため、次に提案する法的、組織的、および技術的措置を導入することを検討する必要がある。¹⁹⁹

¹⁹⁷ 第5章：データ保護影響評価（DPIAS）を参照

¹⁹⁸ Marelli, “The SolarWinds hack”, 特に “‘Data sovereignty’ and ‘digital sovereignty’: Tools for protecting humanitarian principles in cyberspace” のセクションを参照

¹⁹⁹ Massimo Marelli, “Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation”, *International Review of the Red Cross*, Vol. 102, No. 913, 2020年4月, pp. 367–387: <https://doi.org/10.1017/S1816383121000151>

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、団体の特権および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**サブプロセッサ**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**サブプロセッサ**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サブプロセッサ**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**サブプロセッサ**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。

10.10 行動規範

最後に、2021年に欧州データ保護会議（EDPB）は、EU一般データ保護規則（GDPR）の第40条に沿って**クラウドサービス**にGDPRを適用するための2つの行動規範を採択しており、²⁰⁰ 現在3つ目の行動規範が欧州監督当局によって評価中である²⁰¹ことは言及しておく価値があるだろう。GDPRの対象となる**人道団体**の場合、特定のサービスが該当の行動規範のいずれかに基づいて承認されているかどうかを確認することが推奨される。行動規範の遵守は、良い出発点として考えられなければならない。**人道団体**は実際、

²⁰⁰ Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the “EU Data Protection Code of Conduct for Cloud Service Providers” submitted by Scope Europe: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf

Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE): https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202117_cispecode_en_0.pdf

²⁰¹ Cloud Security Alliance (CSA), “CSA Code of Conduct for GDPR Compliance”, CSA, 2022年5月9日アクセス: <https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct>

その特有の問題と要件を考慮すると、この章で示したすべての事柄を具体的かつ注意深く検討する必要がある。

パブリッククラウドで処理されるデータへの 政府によるアクセス

国家安全
保障

刑事訴訟
手続

データ開示を可能とする
法制度の増加

課題

政府はサービス
プロバイダへ
直接開示を要求
できる

人道団体は
開示命令に
気づかない

人道データの
強制的開示による
人道団体の信頼の低下

リスク軽減

クラウドで
処理すべき
データの検討

人道団体の特権および
免除の有効性の実現確保

人道データの使用を控えることの
重要性について各国へ意識喚起

第11章

クラウド、および 政府によるアクセス

ANDREA RAAB-GRAY*

* 免責事項：本寄稿で述べられた意見や見解は著者自身のものであり、必ずしもオーストリア共和国欧州
および国際問題連邦省の意見や見解を表すものではない。

世界中の国々で、国家の安全保障のため、および／または刑事訴訟手続での使用を目的として、顧客によって作成された、または顧客に関連するさまざまな種類のデータを開示するよう、政府がサービスプロバイダに要求することを認める国内法が制定されている。こうした法律の根拠としてしばしば引用されるのが、クラウドコンピューティングなどのデジタルテクノロジーが違法な目的で使用されることが増加している、というものである。²⁰² しかし、これらの法律の多くは、その副作用として、パブリッククラウド環境で処理された**人道団体**の活動に関するデータの開示を政府が命じることをも可能にしている。このようなデータには、団体内やパートナーとの通信、団体の活動から恩恵を受けている人々との通信内容などを含め、**人道団体**が生成、収集、または他者と交換するデータが含まれ得る。多くの場合、開示の対象となるデータには、メタデータ、位置データ、トラフィックデータなども含まれる。つまり、通信の内容だけでなく、通信の受信者や通話時間などに関するデータなども含まれる。²⁰³ 本章では、簡潔に表現するため、こうした内容、メタ、位置、トラフィックデータをまとめて「**人道データ**」と呼ぶこととする。

人道データと国家との関連性に関しては、**人道団体**がしばしば中立、公平かつ独立した方法でその任務を遂行していることを理解することが重要である。こうした団体のいくつかは、武力紛争やその他の危機に対するすべての当事者と対話をしながら、援助活動を行っている。これには、国家の法的枠組みにおいて「テロリスト」として指定される非国家主体および個人が含まれる可能性がある。国際人道法は、公平な活動を行う**人道団体**に主導権を与えることを容認しており、実際にこれを承認している。この権利には、公平な**人道団体**が、国際的および非国際的な武力紛争の当事者に対して、反テロリズムや制裁体制下でその紛争がどのような特徴を持っているかに関わりなく、人

²⁰² 以下の例を参照されたい。米国司法省、*Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act*（世界中の公衆の安全、プライバシー、法の支配の促進：クラウド法の目的と影響）、白書、米国司法省、ワシントンDC、2019年4月：www.justice.gov/dag/page/file/1153436/download

²⁰³ **人道団体**にとってのメタデータの重要性についての詳細は、ICRCおよびPrivacy International、*The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*、2018年10月、chap. 6：www.icrc.org/en/download/file/85089/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdfを参照のこと。

道的活動を提供できることが含まれている。²⁰⁴ したがって、**人道データ**は、テロ対策や刑事訴訟手続きの目的で、政府の関心をひくものとなる可能性がある。

したがって**人道団体**は、テクノロジー、特に**クラウドサービス**を選択する際、政府が**人道データ**を処理するプロバイダを含むサービスプロバイダにデータの開示を要求することを認める法律が引き起こす、法的および実務上の影響を考慮しなければならない。本章は、**人道団体**が考慮すべき以下の内容を伝えることを目的としている。セクション11.1は、それが主目的の法律ではないにせよ、国家安全保障および/または刑事訴訟手続の目的で、政府がサービスプロバイダに**人道データ**の開示を請求することを認める法律について述べる。セクション11.2では、**人道団体**が、団体の活動から利益を受ける人々と団体の運営に与える影響を評価する際に考慮すべき基準について概説する。最後にセクション11.3では、**人道団体**が、パブリッククラウド環境で**人道データ**を処理することを選択した場合に、**人道データ**の開示リスクを軽減するために講じることができる法的手段についてのガイダンスを提供していく。²⁰⁵

204 1949年のジュネーブ条約の共通条項3および共通条項9/9/9/10を参照。これについてのさらなる情報は、以下を参照のこと。Tristan Ferraro「International humanitarian law, principled humanitarian action, counterterrorism and sanctions: Some perspectives on selected issues (国際人道法、原則に基づいた人道的行動、反テロリズムと制裁: 選択された問題に関するいくつかの視点)」、*International Review of the Red Cross*, Vol. 103, No. 916/917, 2021年, pp.109–155

205 本章では、法的根拠に基づかないソッキングなどの「不正アクセス」については扱わない。不正アクセスは、クラウドに特有の問題ではなく、法的対応とサイバーセキュリティ対応の両方に関して、より広範な疑問を提起するためである。例として、以下を参照していただきたい。Massimo Marelli「Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation (人道主義者をハッキング: デジタル変革における国際的人道団体のためのサイバー境界の定義およびサイバーセキュリティ戦略の開発)」、*International Review of the Red Cross*, Vol. 102, No. 913, 2020年4月, pp.367–387: <https://doi.org/10.1017/S1816383121000151>。
同様に、本章では、いわゆる「クラウド抽出」、デバイスやアプリケーションの製造業者がデータバックアップのために通常使用する、**第三者**のサーバーに保存されているユーザデータのフォレンジック分析については説明しない。法的機関にますます利用されるようになっているこの新しいトレンドは、**人道団体**に対して、本章で説明する法律と同様の懸念を引き起こす。詳細については、以下を参照されたい。Privacy International「Cloud Extraction (クラウド抽出)」、Privacy International, 2022年5月9日: <https://privacyinternational.org/learn/cloud-extraction>。Privacy International「Are UK Police Accessing Your Cloud Apps? (英国警察があなたのクラウドアプリにアクセスしている?)」、Privacy International, 2020年4月1日: <http://privacyinternational.org/report/3551/are-uk-police-accessing-your-cloud-app>。Privacy International「Secret Tech Lets Governments Collect Masses of Data from Your Apps (秘密情報技術により、政府はアプリから一括のデータを収集可能)」、Privacy International, 2020年1月6日: <http://privacyinternational.org/node/3323>

11.1 政府によるサービスプロバイダへの 人道データ開示要求を可能にする法律に ついて

人道団体は、使用するテクノロジーを選択する際、そして次に挙げる内容に当てはまる場合、国家安全保障および/または刑事訴訟手続の目的で、政府がサービスプロバイダに人道データの開示を強制できる法律について、考慮する必要がある。

- パブリッククラウド環境で処理するかどうか、またどのようなデータを処理するかを検討している
- クラウドサービスプロバイダを選んでいる

本章で話題にしている法律自体は、クラウドサービスを含むデジタルテクノロジーの違法目的での使用が増加していることによって推進されたものであり²⁰⁶、特に人道データをターゲットにすることを目的としてはいない。ただし、こうした法律は、人道データを対象から除外するものでもない。実際これらの法律には、通常、人道データを明示的に除外する「人道的免除条項」は含まれていない。逆に、以下に示す通り、サービスプロバイダによるデータ開示を要求する権限を政府に与える法的要件が、人道データに直接適用されることがよくある。

サービスプロバイダへの人道データの開示要請は、人道団体自体に向けたデータ開示要請とは異なる。人道団体自体がこうした要請を受け取った場合は、その任務と方針を考え合わせて、要請にいかに対応するかを評価できる立場にある。開示要請に応じないことを決定した場合、開示に異議を唱えるため、国内法に定められた救済手段に訴えることができる。さらに、人道団体は、国内法や国際法に基づいて享受できる特権および免除を利用できる場合がある（「セクション11.3 - パブリッククラウド環境で処理される人道データの開示リスクの軽減」も参照のこと）。これは、データがホストされている場所がプ

²⁰⁶ 例は以下のとおりである。欧州委員会「Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters（刑事事件における電子的証拠の欧州作成および保存命令に関する、欧州議会および評議会の規制に関する提案）」、COM/2018/225 final、2018年4月17日：<https://eur-lex.europa.eu/legal-content/EN/TEXT/?uri=COM:2018:225:FIN>

プライベートクラウド環境か、パブリッククラウド環境かは無関係である。しかしプロバイダが国家当局から開示要請を受けた場合、**人道団体**はプロバイダが要請にどのように対応するか、たとえば、プロバイダが開示要請を**人道団体**に通知するか否か（法的に許可されている場合）、そしてその要請に対抗するために抗弁を行うかどうか、に依存することとなる。²⁰⁷

この章では、米国、英国、欧州連合の関連する法律の実例を取り上げていく。ただし、その他の国でも、国家安全保障や刑事訴訟の目的で、サービスプロバイダに顧客データ（**人道団体**のデータを含む可能性がある）の開示を強制できる法律を制定していることに注意が必要である。²⁰⁸

11.1.1 国家安全保障を目的とした、政府によるサービスプロバイダへの人道データの開示強制を可能とする法的枠組み

世界には、国家安全保障を目的とし、管轄下のサービスプロバイダへのデータ開示強制という法的手段を政府に与える法律を採択している国がある。したがって、**人道団体**は、こうした国の管轄下にあるクラウドサービスプロバイダーを選択することにより、データが国家安全保障の目的で開示される可能性があることを認識しなければならない。

²⁰⁷ クラウド環境で処理されるデータの保護に関する特権および免除の有効性を確保するために**人道団体**がとるべき法的措置については、「セクション10.9 – 特権および免除およびクラウド」も参照されたい。

²⁰⁸ 例として、オーストラリア議会の2020年改正電気通信法（国際製造令）法案（2020年）を参照していただきたい：<https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fr6511%22>

欧州データ保護会議（EDPB）、「Government Access to Data in Third Countries（第三国のデータへの政府アクセス）」、EDPS/2019/02-13、2021年11月：https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_o.pdfも参照のこと

こうした法律のよく知られた例として、世界貿易センタービルへの攻撃に対応して2001年10月に制定された米国愛国者法がある。²⁰⁹ 同法により、米国政府は米国の人的管轄権²¹⁰の下にあるサービスプロバイダに対し、データ開示を要求することができる。したがって、**人道団体**が米国のサービスプロバイダのサービスを利用すると、そのデータは愛国者法の適用範囲内に含まれる可能性があり、同法に基づく開示要求に対して対抗することができなくなる可能性がある。

クラウドサービスの使用を検討している**人道団体**が特に関心を持っているのは、外国情報監視法（FISA）に基づいて行われた命令、そして国家安全保障書簡に関する愛国者法の制度であろう。²¹¹ FISAに基づき、米国政府には次の権限が与えられている。

- 国際テロ、対スパイ活動、または外国諜報活動に「関連する」とみなされる場合に、クラウドサービスプロバイダなどの**第三者**に対し、記録またはその他の「有形物」の提出を要求する秘密裁判所命令を入手する²¹²

209 具体的には、テロ犯罪捜査を進めるために、同法は既存の法律を改正し、テロ捜査のためツールの監視の適用を拡大し、その範囲をも拡大した。これと愛国者法についてより一般的な情報については、以下を参照されたい。米国司法省、「The USA PATRIOT Act: Preserving Life and Liberty（米国愛国者法：生命と自由の保護）」、日付不明：www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

アメリカ自由人権協会、「Surveillance under the USA/PATRIOT Act（米国愛国者法下の監視）」、日付不明：www.aclu.org/other/surveillance-under-usapatriot-act。Greenberg Traurig LLP、「Schrems II – U.S. Legislation（シュレムスII – 米国立法）」、Memorandum、2022年2月12日：<https://slmmicrosoftrij.nl/wp-content/uploads/2022/02>

210 例としては、以下を参照のこと。Daniel LevinとJacqueline L. Chung、「Patriot Act Subpoenas: Reinvigorated and Reaching across Borders（よみがえり、国境を越えて届く、愛国者法の召喚状）」、White & Case LLP、日付不明：www.whitecase.com/insight-alert/patriot-act-subpoenas-reinvigorated-and-reaching-across-borders

211 FISA命令の要求数は比較的少ないが、国家安全保障書簡はより頻繁に使用されている。2020年の統計については、以下を参照されたい。Joseph Gaeta、「Letter to Nancy Pelosi（ナンシー・ペロシへの書簡）」、2021年4月30日：www.justice.gov/nsd/nsd-foia-library/2020_fisa/download

212 Brennan Center for Justice、「Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs（それをして、彼らは許されるのか？選択された政府監視プログラムの内訳）」、2022年11月27日にアクセス：www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf

こちらも参照のこと。「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001（テロを阻止し妨げるために必要な適切なツールを提供することによって、アメリカを団結させ強化する（米国愛国者法）2001年法）」、Pub.L. No. 107-56、§ 215（2001年）：www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf 合衆国法典第50編第1804条(a)項(6)号(B)

- 例えば、独立裁判所であるFISA裁判所の許可を得て、米国の人的管轄下にあるクラウドサービスプロバイダに対し、特定の種類の外国諜報情報を取得する目的で、米国外に所在する非米国人の通信データを開示することを要求する命令を発行する²¹³
- FISA裁判所は、少なくともいくつかの状況において、第702条に基づき、メタデータと通信内容の収集を許可してきた。²¹⁴ 第702条は、転送中データと保存中データの両方に適用される。²¹⁵

国家安全保障書簡により、連邦捜査局（FBI）長官およびFBI高官は、たとえばクラウドサービスプロバイダーに対し、国際テロまたは秘密諜報活動から保護するための、認可を受けた調査に関する、加入者情報や料金請求記録情報、電子通信取引記録の開示を要求することができる。²¹⁶ つまり、国家安全保障書簡は、通信内容に関するデータを取得するためには使用できない。

しかし実際、**人道データ**は上記の目的に「関連する」可能性がある。たとえば、**人道団体**は、公平かつ中立的に任務を果たすために、「テロリスト」と指定されているグループと対話したり、こうしたグループの支配下にある人々に人道援助を行ったりすることもある。**人道団体**がこの対話に関するデータをパブリッククラウド環境で処理することを選択した場合、これらのデータは愛国者法に基づいて開示の対象となる可能性がある。

²¹³ 以下を参照のこと。「An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information（外国諜報情報取得を目的とした電子監視を認可する法律）」、Pub. L. No. 95-511, § 702 (1978年): www.congress.gov/bill/110th-congress/house-bill/6304 ニューヨーク大学のブレナン司法センターによると、この条項は、Google、Facebook、Skype、Appleを含む米国のインターネット企業大手9社が処理するデータへのアクセスを容易にするコンピューターネットワーク、PRISMの法的な正当化のためにも引用されている。Brennan Center for Justice、「Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs（それをして、彼らは許されるのか? 選択された政府監視プログラムの内訳）」

²¹⁴ Stephen I. Vladeck、「Expert opinion on the current state of U.S. surveillance law and authorities（米国監視法と当局の現状に関する専門家の意見）」、*Conference of Independent Data Protection Supervisors of the Federal Government and the Länder*（連邦政府および国の独立データ保護監督者会議）、2021年2月: www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf

²¹⁵ 同上 3

²¹⁶ 合衆国法典第18編第2709条

ヨーロッパでは、欧州司法裁判所（CJEU）の判例が、特に政府によるアクセスを目的とした、トラフィックデータと位置データの保全をサービスプロバイダに要求するEU加盟国の権限の輪郭を描くうえで有益である。CJEUの判例は特にクラウドコンピューティングに関するものではないが、著者は、この判例が目下の議論に関連していると考える。この判例により、欧州における国家安全保障上の問題と権利のバランスをとるための一般的なアプローチについて、結論を導き出すことができる。したがって、上述の基準がクラウドのコンテキストにおいても同様に適用される可能性を排除することはできない。

Watson および Privacy International の訴訟では、CJEU は、他の法律の中でも特に、英国の法律を検討する必要があった。同国の法律では、当局がサービスプロバイダに対して、メタデータの保全とアクセス許可を要求することができた。²¹⁷ どちらの訴訟でも、裁判所は、あらゆる電子的通信手段に関連するすべての加入者のすべてのトラフィックおよび位置データの一般的かつ区別のない保全と当局への開示を規定する国内法は、EU法と両立しないと判示した。²¹⁸ しかし、裁判所は「特定の状況、たとえば国家安全保障、国家防衛、公共の安全上の利益がテロ活動によって脅かされている場合、特定のケースでそのデータがテロ活動との闘いに効果的に利用できる可能性があると考えられる客観的な証拠があれば、他人のデータへのアクセスも許可される場合がある」とも述べている。²¹⁹ したがって、裁判所によって定められた基準自体は**人道データ**を対象とするものではないものの、除外するものでもない。逆に、**人道団体**がその任務を果たすために非国家主体と対話を行う場合、こうした対話に関する位置およびトラフィックデータは実際に「テロ活動」との闘いに役立つとみなされる可能性がある。

²¹⁷ 併合訴訟 -203/15およびC-698/15 (*Tele 2 Sverige and Watson*)、判決（大法廷）、2016年12月21日。訴訟C-623/17 (*Privacy International*)、判決（大法廷）、2020年10月6日。例えば、*Privacy International* の件では、CJEUは、当局からサービスプロバイダに対して行われた、英国の2000年の捜査権限規制法（RIPA）および英国の1984年の電気通信法に基づく、国家安全保障を目的とした一括の通信の開示命令に、どの要件が適用されるかを判断することを求められた。データ保全については、2020年10月6日の併合訴訟C-511/18、C-512/18、C-520/18 (*La Quadrature du Net and ors*) も参照のこと

²¹⁸ *Watson*、112項。*Privacy International*、81項

²¹⁹ *Watson*、119項。こちらも参照のこと。*Privacy International*、78項

さらに、**人道団体**は、自分のデータが探されていることに気づいていない可能性もある。たとえば、愛国者法に基づき、米国政府当局は不開示義務を課すことができ、これによりサービスプロバイダが、**人道団体**を含む顧客である第三者に、国家安全保障書簡やFISA命令について通知することは禁止される。²²⁰

最後に、人道データをパブリッククラウド環境で処理することを選択する場合、**人道団体**は安全保障当局による傍受に起因するリスクも考慮する必要がある。社会に大きな影響をおよぼしたBig Brother Watch訴訟において、欧州人権裁判所はとりわけ、国家安全保障を目的とした、安全保障当局による内容データ、通信データの大量傍受を認めた2000年の英国捜査権限規制法（RIPA）に基づいて発せられた許可と、欧州人権条約第8条との適合性を検討した。²²¹ 裁判所はその際、大量傍受の根拠、適用される手続、制限と安全保障に関する法律の明確化の必要性を強調した。²²² 裁判所はまた、通信の内容だけでなく、通信データとメタデータの収集や処理にも、同様の保護措置を適用すべきであるとの考えを述べた。²²³ 重要なのは、裁判所が**人道データ**を、大量傍受の範囲から除外する基準を定義していないことである。²²⁴ 英国のRIPAは、英国の2016年調査権限法に置き換えられた。こ

²²⁰ 合衆国法典第50編第1861条（d）項、合衆国法典第18編第2709条（c）項

²²¹ Big Brother Watchら対英国、訴訟番号：58170/13、62322/14および24960/15、大法廷、判決、2021年5月25日。同様の訴訟については、Centrum för rättvisa対スウェーデン、訴訟番号35252/08、大法廷、判決2021年5月25日を参照のこと。

²²² Big Brother Watch、361項判決の他部分の概要については、以下を参照のこと。Marko Milanovic、「The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum För Rättvisa（大衆監視の大規模な常態化：Big Brother WatchとCentrum För Rättvisa裁判における、欧州人権裁判所大法廷判決」、EJIL（ヨーロッパ国際法雑誌）：Talk!（ブログ）、2021年5月26日：www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa

Big Brother Watch裁判は特に、国家当局にデータを提供するサービスプロバイダの義務とは関係がないものだが、裁判所が国家安全保障上の利益に対してどれほどの恭順を見せてきたかを示す上で極めて重要である。

²²³ Big Brother Watch、342、363–364項

²²⁴ 最終的に、裁判所は、RIPAの一括傍受体制は、条約424–427項に基づくプライバシー義務に違反していると認定した。一部の人権団体はこの判決を画期的な勝利と称賛したが、他の評論家は、この判決が大規模監視と一括傍受を常態化させているとして批判し、裁判所がこれらの仕組みを欧州評議会加盟国の安全にとって「価値ある」、「極めて重要」なものとみなしていることを強調している。さまざまな立場について詳細を説明しているMarko Milanovic「The Grand Normalization of Mass Surveillance（大衆監視の大規模な常態化）」を参照されたい。

の法律では、**人道データ**を明示的に除外することなく、特に国家安全保障の利益のために必要である場合、通信の「内容」や「二次データ」に対する一括傍受許可も認められており、二次データには、個人、人物の位置、出来事を特定するために使用できるデータが含まれる。²²⁵

Big Brother Watch訴訟も、特にクラウドコンピューティングに関するものではないが、著者は、CJEUの判例に関して上述したのと同様の理由から、この訴訟が関連するものと考えている。

11.1.2 刑事訴訟手続を目的とした、政府によるサービスプロバイダーへのデータ開示強制の法的枠組み

こうした法律の最もよく知られた例の1つが、米国クラウド法である。クラウド法の最初の部分では、以下のことが明示されている。²²⁶

²²⁵ 2016年捜査権限法の第136条以降を参照。この点に関しては、以下の訴訟に注意したい。*Privacy International* 対捜査権限法廷訴訟、[2021] EWHC 27 (Admin)、2021年1月8日。*Privacy International*は、この訴訟において、英国高等裁判所が諜報活動法第5条に基づく判決を下したと説明している。同条項は、安全保障および諜報機関が、非特定の令状（別名一般令状としても知られる）によって、広範囲におよぶハッキングおよび財産干渉権限を行使することを許可しない。テーマ別令状は一般的な令状で、「犯罪組織の構成員が使用するすべての携帯電話」など、構成員の名前や所在地を特定せずに、財産、人、または行為の種類全体を対象とする。*Privacy International*、「Q&A: PI Case – UK High Court Judgment on General Warrants and Government Hacking Explained (Q&A: *Privacy International* 訴訟 – 一般令状と政府のハッキングに関する英国高等裁判所判決の説明)」、*Privacy International*、2021年1月8日：<http://privacyinternational.org/long-read/4361/qa-pi-case-uk-high-court-judgment-general-warrants-and-government-hacking-explained>。この判決がIPAの解釈に影響を与えるかどうかは今後の展開を待つことになる。

²²⁶ 詳細については、以下も参照のこと。米国司法省、*Promoting Public Safety, Privacy, and the Rule of Law around the World*（世界中の公共安全、プライバシー、法の支配の推進）。Vladeck、「Expert opinion on the current state of U.S. surveillance law and authorities（米国監視法と当局の現状に関する専門家の意見）」、13。Greenberg Traurig LLP、「Schrems II – U.S. Legislation（シュレムスII – 米国立法）」、2022年2月12日。スイス連邦司法省、「Bericht zum US CLOUD Act（米国クラウド法レポート）」、2021年9月17日：www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html

- 米国当局は、米国の人的管轄下にあるサービスプロバイダーが「所有、保管、または管理」している内容データおよびトラフィックデータの開示を、以下の条件において、強制することができる。²²⁷
- 特定の刑事手続の目的で²²⁸
- データの所在地には関連しない²²⁹

クラウド法のこの最初の部分には、**人道データ**を適用範囲から免除するような内容は何もない。また、クラウド法内にこうしたデータを暗黙的に免除する他の制限も存在しない。

したがって、**人道団体**が**人道データ**を処理するために米国の人的管轄下にあるサービスプロバイダを選択した場合、これらのデータは、米国のサービス

²²⁷ 米国司法省、*Promoting Public Safety, Privacy, and the Rule of Law around the World* (世界中の公共の安全、プライバシー、法の支配の推進)、8。注目に値するのは、司法省が次のように勧告していることである。クラウド法の命令は補助的な措置であるべきであり、「任務遂行上問題がなく、捜査に支障をきたさないものであれば、検察官は企業から直接データを入手すべきである。したがって、プロバイダからデータを求める前に、検察官は捜査官と協力し、企業とプロバイダのどちらが求めているデータの情報源としてより良いかを判断する必要がある」:17

²²⁸ 合衆国法典第18編第2703条 (b) を参照のこと。

²²⁹ 法的議論は、クラウド法が主権行為の不適切な治外法権を引き起こしたかどうかという問題に焦点を当てた。以下の例を参照されたい。Johannes ThumfartおよびPaul De Hert, 「Both the US' s Cloud Act and Europe' s GDPR Move Far Beyond Geography, but Will Not Solve Transatlantic Jurisdictional Conflicts (米国のクラウド法とヨーロッパの一般データ保護規則は地理を超えたものだが、大西洋を越えた管轄権の衝突は解決しないだろう)」, Just Security, 2018 年 6 月 4 日: www.justsecurity.org/57346/uss-cloud-act-europes-gdpr-move-geography-solve-transatlantic-jurisdictional-conflicts

すべてはMicrosoftの訴訟から始まった。2013年12月、連邦法執行官はMicrosoftにすべてのEメールおよびその顧客のアカウントに関するその他の情報の開示を求める令状を発行する許可を得た。(米国最高裁判所、*米国対Microsoft社*, 584 U.S. (2018年), p.1) Microsoftは、アカウントの電子メールの内容がアイルランドにあるMicrosoftのデータセンターのみに保存されている、つまり米国の手の届かない場所にあると主張し、令状の抑え込みに動いた。(同上、p.2) このようなわけで、米国の裁判所が直面した問題は、データが米国外の場所にあった場合、令状の執行に障害となり、米国の法を不適切に域外適用していることになるかどうかということであった。Microsoftと米国政府はさまざまな裁判でこの問題について争ったが、裁判所の見解は異なった。判事はMicrosoftの申し立てを却下したが、控訴院は、Microsoftに件の電子通信の開示を要求することは令状の法的根拠となった米国の法を不適切な域外適用となるとの考えを示した。(Microsoft社によって管理、維持されている特定のEメールアカウントを検索するための令状に関して、829 F.3d 197, 205, 222 (CA2 2016)) 最終的に、この問題は米国最高裁判所に持ち込まれたが、この再審理は退けられた。というのも、米国クラウド法が発効し、データが外国にある場合でも米国当局が米国のサービスプロバイダーに開示を要求できるようにしたため、問題は解決されたのだった。(米国最高裁判所、*米国対Microsoft社*, pp.2-3)

プロバイダが**人道データ**の「保管、所有、管理」を行っている限り、米国当局によるデータ開示要求に対抗できなくなる可能性がある。この法律は「保管、所有、管理」の概念を定義しておらず、本稿執筆時点では、当局と裁判所がクラウド法のコンテキストにおいてこれらの語をどのように解釈するかはまだわかっていない。

これに加え、米国政府は、サービスプロバイダに対し、特定の状況下において機密保持義務を課すことができる。²³⁰ これは、サービスプロバイダが、データ開示要求の存在をその**人道団体**に通知することが禁止されることがあることを意味する。

（簡略化した）例

人道団体（HO）は、中立かつ公平にその使命を果たし、人道的な影響を受けている人々とのつながりを確保し、人道援助を提供するために、グループGおよびそのリーダーLとの対話を維持している。グループGは、関連法に基づき、「テロリスト」としてリストされている。HOは、この対話の内容をパブリッククラウド環境に保存している。**クラウドサービス**は、ニューヨーク（米国）に設立されたサービスプロバイダSPによって提供されるものである。データの保存先はヨーロッパである。

米国当局は米国クラウド法に基づき、Lに対する特定の刑事手続の目的で、こうしたデータを開示することをSPに対し、法的に義務付ける権限を持つことができる。SPがHOにこの要求について通知することは禁止される可能性がある。阻止のための法と、特権および免除の影響については、後述の「セクション11.3 - パブリッククラウドで処理される人道データの開示リスクの軽減」を参照していただきたい。

人道団体は、米国のサービスプロバイダを選択すると、刑事手続の目的で、他国がそのサービスプロバイダに対して、人道支援の内容データやトラフィックデータの開示を要求できる可能性があることにも留意しなければならない。

²³⁰ 合衆国法典第18編第2703条（b）、第2705条

これは、クラウド法の第2部により、米国政府が他国といわゆる行政協定を締結する権限が与えられるためである。これにより、テロなどの重大犯罪の防止、発見、捜査、起訴を目的として、一方の締約国が他方の締約国に（その逆も同様）、その管轄下にあるサービスプロバイダに対して、特定の内容データやトラフィックデータの開示要求をすることが認められる。²³¹ クラウド法のこの第2部には、**人道データ**を適用範囲から除外する記述は何もない。この最たる例は、クラウド法の第2部および英国の犯罪（国外データ提出命令）法に基づいて締結された英国と米国の協定である。²³²

クラウド法の第2部に相当する英国の法律は、2019年2月に国王の裁可を得た犯罪（国外データ提出命令）法である。この法律は²³³

- 英国の法執行機関²³⁴が、治外法権を有する裁判官からの裁判所命令（「国外データ提出命令」）を申請できるようにする。
- 英国外で運営または拠点を置いているものの、求められているデータを国内で「所有または管理している」サービスプロバイダから電子データを直接取得する。
- 犯罪捜査および起訴対象の犯罪またはテロ捜査の訴追を目的とする。
- サービスプロバイダが事業を行う国との指定された国際協力協定がすでに結ばれている場合。

人道データをこの法の適用範囲から明示的に免除するものは何もないが、国外データ提出命令を通じて取得できるデータには、一部の**人道団体**に関連

²³¹ 合衆国法典第18編第2523条(b)(4)(D)(i)条開示命令は意図的に米国人を対象にしてはならない。この用語は、「米国民、永住権を合法的に認められた外国人、相当数の構成員が米国民または永住権を合法的に認められた外国人である非法人団体、または米国で設立された法人」と定義される。合衆国法典第18編第2523(a)(2)

²³² Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime（アメリカ合衆国政府、およびグレートブリテンおよび北アイルランド連合王国政府間の重大犯罪対策を目的とした電子データアクセスに関する協定）、2019年10月3日：www.justice.gov/dag/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern-ireland

²³³ 犯罪（国外データ提出命令）法、第1項、2項および4項

²³⁴ これらには、とりわけ、巡査、検察官、および国務大尽が制定した規則で指定されたその他の人物が含まれる。犯罪（国外データ提出命令）法、第2項

する可能性のある例外が1つある。電子データとは、電子的に保存されたデータを意味し、パブリッククラウド環境でホストされている内容データおよび通信データが含まれる。²³⁵ ただし、クライアントと弁護士の間の特定の通信や、機密情報である個人の記録など、法的特権の対象となる情報は、国外データ提出命令を使用して取得することはできない。²³⁶ 機密情報である個人の記録には、健康データや、個人の福祉を目的としてボランティア団体が個人に提供する、または提供する予定のカウンセリングまたは援助に関するデータ（特にその記録が、個人に対して守秘義務を生じさせる状況で作成された場合）が含まれる。²³⁷ この後者の免除には、非常にまれなケースではあるが、**人道団体**が実施する**人道支援**に関連する一部のデータが含まれる場合がある。しかしこの法律は、その適用範囲から、**人道支援**に関するデータを明確に除外していない。

国外データ提出命令に基づいて開示を要求できるのは、これらの手続または捜査にとって実質的な価値があると考えられる電子データのみである。²³⁸ 上述の通り、**人道団体**は、公平かつ中立的に任務を果たすために、「テロリスト」と指定されているグループと対話したり、こうしたグループの支配下にある人々に人道援助を行ったりすることもある。そのため、団体がその対話に関する情報をクラウド環境に保存している可能性があり、こうした情報が実際にテロ捜査において「重大な価値」を持つ可能性があることを排除することはできない。

クラウド法第2部および犯罪（国外データ提出命令）法の前提である米国と英国の協定には、**人道データ**に対する明示的な免除は含まれていない。したがって、協定に含まれる制限のいずれかが適用されない限り、こうしたデータは原則としてサービスプロバイダに要求することもできる。

²³⁵ 犯罪（国外データ提出命令）法、第3項(2)

²³⁶ 犯罪（国外データ提出命令）法、第3項(3)

²³⁷ 犯罪（国外データ提出命令）法、第3項(7)、および第3項(8)

²³⁸ 犯罪（国外データ提出命令）法、第4項(5)

（簡略化した）事例1

人道団体（HO）は、中立かつ公平にその使命を果たし、人道的な影響を受けている人々とのつながりを確保し、人道援助を提供するために、グループGおよびそのリーダーLとの対話を維持している。グループGは、関連法に基づき、「テロリスト」としてリストされている。HOは、この対話の内容をパブリッククラウド環境に保存している。**クラウドサービス**は、ニューヨーク（米国）に設立されたサービスプロバイダー（SP）によって提供されるものである。

米国/英国間の協定に基づき、英国当局は正式に承認された裁判所命令を提示することにより、SPに対し「テロ捜査」の目的でHOのデータの開示を要求することができる。協定の対象範囲から除外されない限り、SPは求められた情報を英国当局に提供しなければならない。米国当局によるアクセスについては、上記の例を参照していただきたい。

（簡略化した）事例2

人道団体（HO）は、中立かつ公平にその使命を果たし、人道的な影響を受けている人々とのつながりを確保し、人道援助を提供するために、グループGおよびそのリーダーLとの対話を維持している。グループGは、関連法に基づき、「テロリスト」としてリストされている。HOは、この対話の内容をパブリッククラウド環境に保存している。**クラウドサービス**は、英国に設立されたサービスプロバイダー（SP UK）によって提供されるものである。

米国/英国間の協定に基づき、米国当局は正式に承認された令状をSP UKに提示することにより、SP UKに対し「テロ捜査」の目的で**人道団体**のデータの開示を要求することができる。協定の対象範囲から除外されない限り、SP UKは求められた情報を米国当局に提供しなければならない。

公に知られている限り、本稿の執筆時点で英国 / 米国協定と同様に締結された唯一の協定は、米国とオーストラリアの間の協定である。²³⁹

人道団体は、EUがクラウド法や犯罪（国外データ提出命令）法と同様の法律、すなわち電子証拠規制（2026年8月18日完全適用開始予定）を採択したことに注意する必要がある。この規制により、あるEU加盟国に置かれた法執行当局（LEAs）は、他のEU加盟国に拠点もしくは法的代表者を置く特定のカテゴリのサービスプロバイダ（ユーザが通信やデータ保存をすることを可能にする電子通信サービスプロバイダ、ドメイン名・IP登録サービスプロバイダ、情報社会サービスプロバイダを指す）に対し、ある種のデータの開示または保存について法的拘束力のある要請を発することができる。²⁴⁰

より広範な欧州レベルにおいて、**人道団体**は、欧州評議会の閣僚委員会が条約の第二追加議定書を採択したことに注目すべきであろう。その内容は、協力の強化と電子証拠の開示に関するものである。この議定書は、サイバー犯罪に関する協力と、犯罪捜査や訴訟手続を目的とした、あらゆる犯罪の電子的証拠の収集を、より効率的な相互支援や、その他の形の管轄当局の協力、ひいては緊急時協力、管轄当局とサービスプロバイダおよび関連情報を所有または管理するその他の団体との間の直接協力などのためのツールを通じて、さらに強化することを目的としている。²⁴¹

この目的達成のため、議定書はたとえば、締約国は他の締約国領域内にあるサービスプロバイダに直接命令を出し、締結国の特定の犯罪捜査または

²³⁹ Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime（アメリカ合衆国政府とオーストラリア間の重大犯罪対策を目的とした電子データアクセスに関する協定）、2021年12月15日：www.justice.gov/dag/cloud-act-agreement-between-governments-us-and-australia

その他のリソースについては、司法省のクラウド法リソースを参照されたい。次の場所から入手可能である。クラウド法リソース（justice.gov）

²⁴⁰ Lisa Peets と Marty Hansen と Paul Maynard, “The EU E-Evidence Package Is Published in the Official Journal,” Inside Global Tech, 2023年8月23日：www.insideglobaltech.com/2023/08/23/the-eu-e-evidence-package-is-published-in-the-official-journal/

²⁴¹ 議定書の前文。

刑事手続に必要な、そのサービスプロバイダが所有、管理する特定の加入者の情報の開示を要求することができることを予見している。²⁴²

11.2 人道支援およびその恩恵を受ける人々に対する強制的開示の影響

前の章で説明した法律が**人道団体**に何らかの課題をもたらすかどうかを検討する際には、**人道データ**の開示が次のことにおよぼす影響を考慮すべきである。

- **人道団体**の活動から恩恵を得ている人
- **人道団体**の活動

人道支援の恩恵を受ける人々への影響に関しては、**人道団体**が提供しているサービスと人道団体が個人から収集するデータの種類によって、大きく異なる。

例

人道団体は、その任務を果たすために、性暴力の被害者に医療サービスを提供し、彼らの医療データや性暴力の被害状況に関する情報を入手することがある。**人道団体**は、この情報をパブリッククラウド環境に保存する。国家は、特定の状況における性暴力犯罪についての捜査を行う際に、領域的、人的、または普遍的管轄権に基づいて、この被害者に関するデータの入手を求める場合がある。

刑事手続を目的とした、医療データや性暴力の状況に関するデータの強制的開示は、被害者自身に害をおよぼす可能性がある。第一に、この情報を当局に提供するかどうかを被害者自身が決定する主体性が奪われる。第二に、多くのコミュニティでは依然として、性暴力を受けた者は偏見の目で見られる。もし性被害者であることが知られれば、コミュニティから排斥されるかもしれない。したがって、被害者データの強制的開示とその後の法的手続での使用は、被害者が直面している害をさらに悪化させる可能性がある。

²⁴² 議定書の第7条(1)を参照のこと。

強制的開示が**人道団体**の運営に与える影響は、その任務と活動方法によって異なる。一部の**人道団体**は定期的に政府と連絡し合い、例えば個人が権利や法的地位を得られるようにするため、個人の利益になる情報を政府に渡している。対照的に、極秘に活動しており、国家、個人、その他の関係者との対話の内容を、政府には共有しない**人道団体**もある。これは、信頼を構築し、武力紛争の影響を受けた地域、その他の形の暴力にさらされた地域にアクセスするために、必要不可欠な活動手段であるためである。一部の団体のこうした活動方法は、国際社会によって承認され、実際に保護されており、さまざまな被害を受けた人々が、不可欠な人道サービスを受けることができるようにするための前提条件と考えられている。²⁴³ 上述した法律の難しさは、当局がサービスプロバイダに**人道団体**のデータの開示を直接要求できることにあることを、**人道団体**は心に留めておくべきである。直接要求できるため、通常、**人道団体**と法執行機関との関係性の違いを考慮する余地が残されておらず、**人道団体**の明確な任務と実践の特殊性が移動の際に失われる危険があり、それが団体自身、そして最終的には団体が支援している人々に損害を与える可能性がある。

そのうえ**人道団体**は、強制的開示が団体運営におよぼす影響を考慮する際に、**人道データ**が提供された目的以外の目的で使用される可能性があるという事実が、利害関係者が団体に対して抱く信頼にどのような影響を与えるかについても考える必要がある。²⁴⁴

- **人道支援**の恩恵を受けている人々は、自分のデータが通知された目的のみに使用され、中立かつ公平で、独立した方法でのみ処理されるという確約が得られなければ、**人道団体**との関わりを望まないだろう。その結果、

²⁴³ 「The ICRC' s privilege of non-disclosure of confidential information (ICRCの機密情報非開示の特権)」、*International Review of the Red Cross*, Vol. 97, No. 897–898 (2015年6月), pp. 433–444 <https://doi.org/10.1017/S1816383115000533>.

²⁴⁴ こちらについては以下の例を参照のこと。国際赤十字・赤新月運動代表評議会、決議12: 人道データの保護、2022年6月23日: https://rcrcconference.org/app/uploads/2022/06/CD22-R12-Safeguarding-Humanitarian-Data_23-June-2022_FINAL_EN.pdf
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、プライバシーおよび国際人道活動に関する決議、2015年10月27日、説明文の5節。
第33回赤十字・赤新月国際会議、決議4、2019年12月、p.8およびop 8。

生活や生計を改善できる重要な人道サービスや援助を受けられなくなる可能性がある。

- 同じことが国家にも当てはまる。**人道団体**が国内で収集したり、国家から受け取ったりするデータが他国に転送されるリスクがあると考えた場合、国家はその団体に関わることに消極的になる可能性がある。それどころか、団体がサービスを提供しようとしている人々へアクセスすることすら許可しなくなるかもしれない。国家もまた、これらのデータが、中立かつ公平に独立した方法で扱われることを期待している。
- さらに、支援を必要とする人々に差別なく援助を提供する**人道団体**は、非国家武装集団と関与する可能性もある。時として、これには一部の国が「テロリスト」として指定したグループが含まれる場合がある。しかし、こうしたグループや個人とのやり取りがなければ、**人道団体**は被害を受けた人々に不可欠な人道的サービスを提供できない場合がある。こうした非国家武装集団が、**人道団体**が自集団と交わした対話の内容を直接的、間接的に政府に共有するよう強制される可能性があるというリスクを認識した場合、これは団体が中立であるという認識に影響を与える可能性がある。したがってこうした集団は、**人道団体**に関わることを望まなくなる可能性があり、その管理下にある人々に対する重要な人道サービスの実施を妨げることになる可能性がある。

11.3 パブリッククラウドで処理される人道データの開示リスクの軽減

これまでのセクションでは、**人道団体**にとって不可欠なことは、人道データをパブリッククラウド環境で処理するかどうかについて、情報に基づいた決定を下すことであることを示してきた。「セクション 11.1 – 政府によるサービスプロバイダへの人道データ開示要求を可能にする法律について」では、法律および協定に基づく開示の可能性について、「セクション 11.2 – 人道支援およびその恩恵を受ける人々に対する強制的開示の影響」では、こうした強制的開示が人道活動、そしてそれを享受する人々におよぼす影響について考えてきた。

人道団体がパブリッククラウド環境で人道データを処理することを選択した場合、データ開示リスクを軽減するために、次の措置を講じることを検討すべきである。

団体が享受できる特権および免除の実効性を確保する

国に対し、人道データを任務とは異なる目的で使用または要請しないことの重要性を認識させる

これらの対策は、「第10章：クラウドサービス」で説明した技術的、法的、組織的な方策」に加えて提案するものである。とはいえ、人道団体は暗号化に特に注意を払うべきであることを強調しておく。暗号化自体には、データ開示のリスクを軽減することはできないが、開示されたデータは判読できなくなるため、使用をより困難にすることができる可能性はある。²⁴⁵ これは、クラウド法など、復号化されたデータを提供する義務を含まない法的フレームワークのコンテキストで、特に意味を持つ。²⁴⁶

11.3.1 特権および免除の実効性の確保

人道団体の中には、二国間もしくは多国間条約、または国内法に基づいた特権および免除を享受している団体もある。これらは、団体が自らの任務を独立的かつ効果的に実行するためのツールとなる。人道団体に与えられた

²⁴⁵ その他の技術的方策については、以下を参照のこと。欧州データ保護委員会（EDPB）、*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*（個人データのEUレベルの保護への準拠を確保するための、転送ツールを補足する措置に関する推奨事項 01/2020）、2021年6月18日、付録2：https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

²⁴⁶ 米国司法省、*Promoting Public Safety, Privacy, and the Rule of Law around the World*（世界中の公共の安全、プライバシー、法の支配の推進）、18

特権および免除は、クラウド環境で処理されるデータにも適用されるため、原則としてデータの強制的開示を防ぐことができる。²⁴⁷

アーカイブの不可侵性は特に重要である。国連のコンテキストでは、アーカイブは、組織に属する、組織によって保持または使用されるデータとインフラストラクチャを含むものとして解釈されてきた。不可侵性とは、とりわけ、国家がデータを押収するなどの方法で、データを含むアーカイブに干渉できないことを意味する。²⁴⁸ さらに、団体およびそのスタッフの管轄権の免除により、強制的開示の要請を拒否できる可能性がある。

ただし、クラウドに限った法律の機能は、特権および免除の効果的な適用に障害をもたらす。

第一に、普遍的に特権および免除を享受していない**人道団体**もある。こうした団体にとって、特権および免除によって強制的開示を防止できるかどうかは、データ開示を求める国が団体に与えた特権および免除の利用可能性と範囲によって異なってくる。こうした特権および免除が慣習国際法の一部でない限り、それらを与えた国家でのみ有効となる。それらは第三国に対していかなる義務も定めていない。したがって、特権および免除の地理的範囲に合わせたサービスプロバイダおよびデータ処理地点を選択することが、これらの団体にとって最も重要である。

特にサービスプロバイダの選択について考慮する際、**人道団体**は、自団体に特権および免除を与えている国家、および / または効果的なブロッキング規

²⁴⁷ 欧州データ保護監督者 (EDPS)、*Guidelines on the use of cloud computing services by the European institutions and bodies* (欧州の機関および団体によるクラウドコンピューティングサービスの使用に関するガイドライン)、2018年3月16日: https://edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

米国国務省の見解も同様に、文書が国の代理人または請負業者として活動する**第三者**の手に渡ったとしても、特権および免除による保護を維持できるものとしている。: エストニア経済通信省とマイクロソフト社、*Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government*, 日付不明: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVMcb>

²⁴⁸ G. L. Burci, "Inviolability of archives (アーカイブの不可侵性)", in *The Conventions on the Privileges and Immunities of the United Nations and Its Specialized Agencies: A Commentary* (国連およびその専門機関の特権および免除に関する条約: 解説)、Oxford University Press, Oxford, 2016年、8–10項

則を制定している国家の管轄下にあるサービスプロバイダのみを選択したいと考えるかもしれない。ブロッキング規則とは、国内法の対象者による、特定の外国法に基づく要件または禁止事項の遵守を禁止する国内法として定義できる。²⁴⁹ こうしたブロッキング規則の一例として、スイス刑法第271条がある。これにより、「(i) 外国のために行われる公的機関に留保された行為を、(ii) スイスの領土内で、(iii) 法的権利および/または連邦省および警察から特別に得た許可なしに、故意に行動する意図をもって実行する」ことは犯罪とされる。²⁵⁰ そのため状況によっては、スイスのブロッキング規則によって、スイスのサービスプロバイダがスイス領土内のデータに無許可でアクセスする外国当局を支援する行為が禁止される可能性がある。²⁵¹

人道団体は、サービスプロバイダを選択する際に、英国/米国協定などの二国間協定にも留意すべきである。これは、**人道団体**が特権および免除を享受できない国が、協定のもう一方の締約国の管轄下にあるサービスプロバイダ内のデータの開示を要求できる可能性があるためである。

さらに、**クラウドサービス**の特徴を定義付けるとすれば、内容データやメタデータ、トラフィックデータ、位置データにアクセスする**サブプロセッサ**が頻繁に使用されることが挙げられる。このような状況を背景に、**人道団体**は**サブプロセッサ**を選択または受け入れる際に、上述と同様の事項を考慮する必要がある。

第二に、「セクション 11.1 – 政府によるサービスプロバイダへの人道データ開示要求を可能にする法律について」で検討した、法律および判例に基づく

²⁴⁹ 欧州委員会によるブロッキング規則の定義については、以下を参照のこと。欧州委員会、「Extraterritoriality (Blocking Statute) (治外法権 (ブロッキング規則))」、日付不明: https://finance.ec.europa.eu/eu-and-world/open-strategic-autonomy/extraterritoriality-blocking-statute_en

²⁵⁰ Valentine BagnoudとDeborah HondiusとSandrine Giroud、「Swiss Blocking Statute: Update on Do's and Don'ts under the Threat of Criminal Sanctions (スイスのブロッキング規則: 刑事制裁の脅威下ですべきこと、してはいけないことの最新情報)」、LALIVE (ブログ)、2019年12月3日: www.lalive.law/swiss-blocking-statute-update-on-dos-and-donts-under-the-threat-of-criminal-sanctions

²⁵¹ これについては、以下を参照のこと。David Rosenthal、「US CLOUD Act: Why It Should Not Prevent Cloud Projects (米国クラウド法: クラウドプロジェクトを阻止すべきではないのはなぜか)」、VISCHER、2020年8月2日: www.vischer.com/en/knowledge/blog/us-cloud-act-why-it-should-not-prevent-cloud-projects-38580

要請により、当局は、当局に直接情報を開示するよう、**人道団体**ではなくサービスプロバイダに要求することができる。そのため、**人道団体**自体には、特権および免除に頼る機会が得られない可能性がある。この状況をさらに悪化させているのは、一部の法律によって当局がサービスプロバイダに秘密保持命令を課すことが許可されているという事実である。これによってサービスプロバイダは、情報を取得されるエンティティに、開示要請の存在を通知することを禁じられる。その結果として、**人道団体**は、自分のデータが探されていることに気づいていない可能性さえある。

そのため、**人道団体**がパブリッククラウド環境で**人道データ**を処理することを決定した場合、自らの特権および免除の効果を守るため、次の手段を講じることを検討すべきである。

- クラウドサービスプロバイダ、**サブプロセッサ**、およびデータ保管場所を選択する際には、関連する法律や国家間協定（英国 / 米国協定など）を考慮すること
- パブリッククラウドベースのサービスを提供するサービスプロバイダなどのテクノロジープロバイダとの契約において、サービスプロバイダが、要請された場合、求められたデータが特権および免除の対象となる可能性があるという事実をプロバイダが少なくとも当局に通知すべきであると交渉すること²⁵²

包括性を目的として特に特権および免除を受けていない**人道団体**は、もちろん、国内法に定めのある救済策や異議申立に訴えることもできる。こうした措置の利用可能性と範囲は国によって異なるため、**人道団体**は関連法律を理解しておく必要がある。

²⁵² 「セクション10.9 – 特権および免除とクラウド」も参照のこと。

11.3.2 国に対し、人道データを人道団体の任務とは異なる目的で使用またはしないことの重要性を認識させる

人道データの開示要請に対抗する力を高めるために、人道団体はまず国に対し、その任務と運営形態に従って、その業務にそぐわない目的で人道データを使用したり要請したりすることを控えることの重要性を認識させることを考えるとよいだろう。この目的を達成するために、人道団体は、たとえば以下のようなことを主張することができる。

- 関連する法律および国際協定の範囲から人道データを除外する
- または、団体の任務や運営形式にそぐわない目的で人道データを使用または要請しないという法的拘束力のある約束を、国から得る²⁵³

²⁵³ 例えば、赤十字・赤新月運動を念頭に置き、2022年の国際赤十字・赤新月運動代表評議会は、「第33回国際会議にて、各国と運動に対し、人道データの要求と使用は、運動の活動の人道的性質とそぐわない目的で行われてはならず、運動規約の第2条に従い、人道サービスを受ける人々の信頼、あるいはサービスの独立性、公平性、中立性を損なわないような方法で行わなければならないということが強く要請されたことを強調している」。2022年代表評議会、決議12、https://rcrcconference.org/app/uploads/2022/06/CD22-R12-Safeguarding-Humanitarian-Data_23-June-2022_FINAL_EN.pdfを参照。

モバイル メッセージング アプリ

利用可能性



課題

メッセージング
アプリから
集まった情報を
人道団体が
どのように処理
するか、明確な
ガイダンスが必要



第12章

モバイル メッセージング アプリ

LINA JASMONTAITE-ZANIEWICZ*

*本章は次の著作に基づいている。ICRCとThe Engine Room と Block Party, *Humanitarian Futures for Messaging Apps*, 2017年1月: <https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html>

12.1 はじめに

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ている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**にとって魅力的なツールである。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、**個人データ保護**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。

モバイルメッセージングアプリは優れた機能を提供するものの、その使用には、データ保護の問題や虚偽情報など、重大な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。**人道団体**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。このアプローチに包括的なリスク分析が欠けているならば、説明責任、適切性、「害をおよぼさない」、デューデリジェンスなどの**人道団体の基本原則に反することになる**。²⁵⁴ 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

²⁵⁴ これらの原則の運用例については、ICRC、*Accountability to Affected People Institutional Framework*、2019年1月を参照：www.icrc.org/en/publication/accountability-affected-people-institutional-framework

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。²⁵⁵

「デジタル近接」、すなわち、受益者がいる場所に**人道団体**が物理的にもデジタル的にも存在しようとする必要があることから、**人道上の緊急事態**の際に、**人道団体**はWhatsApp、Facebook Messenger、Snapchat、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。これらの独自のクロスプラットフォームを確立しているサービスプロバイダーは通常、**人道団体**のニーズに合わせてアプリケーションをカスタマイズすることに積極的ではない。同時に、あまり多くの人に利用されてい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、団体が支援しようとしている人々を排除してしまう可能性がある。したがって、特定の場所にどのようなコミュニケーション・チャンネルが存在するだけでなく、影響を受ける個人がどのコミュニケーション・チャンネルを信頼しているか、そして使用することができるかを知ることが不可欠となる。²⁵⁶

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。このことと、**個人データ**の**追加処理**の可能性を考慮すると、メッセージングアプリケーションの使用目的や収集されたデータの共有先の数を制限することは実際には困難であると考えることが重要である（例えば、人々は、チャンネルが公衆衛生情報を共有するために設計されているにもかかわらず、意見

²⁵⁵ Article 29 Data Protection Working Party, *Opinion 02/2013 on Apps on Smart Devices* (WP 202), 2013 年 2 月 27 日: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

²⁵⁶ ICRC, *Accountability to Affected People Institutional Framework*, 2019年1月, p. 5

の提供や機微性の高い個人情報の報告のためにチャンネルを使用しようとする可能性がある)。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、ユーザーが既に提供したデータを破棄または削除することができる、と**人道団体**は自信を持って述べるできない場合がある。

モバイルメッセージングアプリは、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において、モバイルメッセージングアプリは、一方向の「放送」用チャンネルとして機能することができる（人道支援物資の到着時間や場所、地域の診療所の営業時間の変更、または人々の移動や避難のための安全なルートなど）。ただし、メッセージングアプリは双方向のコミュニケーション機能を備えた設計になっているため、受益者との一方向のコミュニケーションに特化して使用されるようにするのは困難である。双方向コミュニケーションによって、危機の影響を受けた人々にははるかに高いリスクを負うことが多く（より多くの**個人データ**が転送される可能性がある）、予想に反した**長期的な管理/持続可能性の問題**をも引き起こすことがあることを強調しておく必要があるだろう。

12.1.1 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ング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。²⁵⁷

- モバイルメッセージングアプリは、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。

²⁵⁷ ICRC と The Engine Room と Block Party, *Humanitarian Futures for Messaging Apps*

- モバイルメッセージングアプリでは、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ングアプリ同士では、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ング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。²⁵⁸
 - すでにメッセージング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
 - 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
 - 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

モバイルメッセージングアプリの使用は、危機の影響を受けた人々に利益をもたらすことができる。こうしたコミュニケーションツールは、コミュニティの関与と受け入れを強化し、より調整された、人間を中心とした、責任ある効果的な

²⁵⁸ 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、同上を参照

対応へとつなぐことができる可能性を持つ。²⁵⁹ ただし、人々がどのアプリを使用しているか、またその使用方法に関する、高品質で細分化されたデータはほとんど存在しない。²⁶⁰ ヨーロッパに移住しようとする人々に関しては、デジタル通信技術が以下の目的で使用されていることが明らかになっている。²⁶¹

- 目的地の国に関するデータ（法的情報を含む）の検索
- 密入国業者またはブローカーとの接触の開始
- 移住ルートに関する最新情報の入手、特に噂の検証の試み
- 移動中の安全および救助サービスへのアクセス

確かに、人道的コンテキストから人々がメッセージングアプリを使用する理由はさまざまであろう。そしてそれは基本的なコミュニケーションから、記録された残虐行為の共有の可能性まで多岐にわたる。

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。

- モバイル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。

259 OCHA, “From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action – World | ReliefWeb”, 国際連合人道問題調整事務所 (OCHA)、政策部、ニューヨーク、2021年4月19日: <https://reliefweb.int/report/world/digital-promise-frontline-practice-new-and-emerging-technologies-humanitarian-action>

260 ICRC と The Engine Room と Block Party, *Humanitarian Futures for Messaging Apps*, p.32

261 Bram Frouws と Melissa Phillips と Ashraf Hassan と Mirjam Twigt, “Getting to Europe the WhatsApp Way: The use of ICT in contemporary mixed migration flows to Europe”, SSRN Scholarly Paper, Social Science Research Network, ニューヨーク州ロチェスター、2016年6月1日: <https://papers.ssrn.com/abstract=2862592>。John Warnes, *Update: 10 CwC Challenges in the New Face of the European Refugee Crisis*, UNHCR, 2016 年: www.unhcr.org/innovation/update-10-cwc-challenges-new-face-european-refugee-crisis

12.2 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。

12.2.1 モバイルメッセージング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、言い換えれば受益者は、そのようなアプリケーションを既にダウンロードおよびインストールしており、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ングアプリを通じて受益者と連絡を取ることで、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になるかもしれない。したがって、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、彼らのアプリ利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、メッセージング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。

12.2.1.1 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²⁶²

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。

²⁶² Maria XynouとChris Walker, “Why We Still Recommend Signal over WhatsApp … Even Though They Both Use End-to-End Encryption”, Security in a Box, 2016年5月23日: <https://securityinabox.org/my/blog/why-we-still-recommend-signal-over-whatapp/>

「特権および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。データの不適切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。」²⁶³

12.2.2 メッセージング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。²⁶⁴

- 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、Meta 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。
- 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。
- 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

²⁶³ データ保護・プライバシー・コミッショナー国際会議、Resolution on Privacy and International Humanitarian Action、37th International Conference of Data Protection and Privacy Commissioners、Amsterdam、2015年10月17日：<http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf>.

²⁶⁴ ICRC と Privacy International、*The Humanitarian Metadata Problem*、p.50

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、オプション機能としてのみ含まれているものもあることを留意すべきである (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)。²⁶⁵

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。²⁶⁶ 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)。²⁶⁷ 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

²⁶⁵ Lucy Handley, "Sheryl Sandberg: WhatsApp Metadata Informs Governments about Terrorism in Spite of Encryption", Yahoo! Finance, 2017 年 7 月 31 日: <https://finance.yahoo.com/news/sheryl-sandberg-whatsapp-metadata-informs-112540721.html>

²⁶⁶ 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

²⁶⁷ Micah Lee, "Battle of the Secure Messaging Apps: How Signal Beats WhatsApp", The Intercept, 2016 年 6 月 22 日: <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>

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。²⁶⁸ 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全されると述べているが、データが保全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（トール）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、²⁶⁹ 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、²⁷⁰ 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。

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。

²⁶⁸ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, p.60

²⁶⁹ たとえば、OrbotはTorの秘匿サービスを利用している: “Orbot: Proxy with Tor”, Guardian Project, 2022年1月20日アクセス: <https://guardianproject.info/apps/org.torproject.android>
Joseph Cox, “‘Ricochet,’ the Messenger That Beats Metadata, Passes Security Audit”, Vice, 2016年2月17日: <https://www.vice.com/en/article/ricochet-encrypted-messenger-tackles-metadata-problem-head-on/>

²⁷⁰ Signal Messenger, “Grand Jury Subpoena for Signal User Data, Eastern District of Virginia”, Signal Messenger, 2016 年 10 月 4 日: <https://signal.org/bigbrother/eastern-virginia-grand-jury>.

例：

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か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。²⁷¹

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。²⁷² Twilioは、いくつかのメッセージングアプリ企業と提携している**第三者プロバイダー**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。²⁷³

²⁷¹ 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>

²⁷² たとえば、GDPR 第65条(1)(a)に基づくWhatsApp Irelandに関するアイルランド監督当局の決定草案に関して生じた紛争に関するEDPBの拘束力のある決定1/2021では、WhatsAppの法的根拠通知における「その他のビジネスサービス」への言及は、特定の正当な利益との関係を示すものでも、WhatsApp IEが言及するビジネスやパートナーを特定するものでもないため、不明確であると指摘した（第63項）。参照：欧州データ保護会議（EDPB）、GDPR 第65条(1)(a)に基づくWhatsApp Irelandに関するアイルランド監督当局の決定草案に関して生じた紛争に関する拘束力のある決定1/2021。2021年7月28日: https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf.

²⁷³ Twilio, “Transparency Reporting”, Twilio, 2022年1月20日アクセス: www.twilio.com/legal/transparencyを参照

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。

12.2.3 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企業（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企業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。²⁷⁴
- 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

²⁷⁴ 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。Masashi Crete-Nishihataら、“Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications”, The Citizen Lab, 2013 年 11 月 14 日: <https://citizenlab.ca/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/> Jon Russell, “Thailand’s Government Claims It Can Monitor The Country’s 30M Line Users”, TechCrunch (ブログ), 2014 年 12 月 23 日: <https://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/>

タにアクセスできる。²⁷⁵ 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、電話に直接ではなくクラウドに保存されたデータ、または存在またはアクセスが確認できないデータ、つまり削除されたデータにアクセスするものもある。²⁷⁶

- 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²⁷⁷、リモートでその電話や保存されたデー

²⁷⁵ ICRCとPrivacy International、*The Humanitarian Metadata Problem*、セクション5.3

²⁷⁶ 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:Privacy International、“Mobile Phone Extraction” (Neighbourhood Watched: How policing surveillance technology impacts your rights)、2019年2月:<https://privacyinternational.org/sites/default/files/2019-02/Explainers-MPE.pdf>.

²⁷⁷ Frederic Jacobs、“How Russia Works on Intercepting Messaging Apps”、bellingcat、2016年4月30日:<https://www.bellingcat.com/news/2016/04/30/russia-telegram-hack>
thaddeus t grugq、“Operational Telegram”、Medium、2016年7月5日:<https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a>

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。²⁷⁸

- **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。²⁷⁹ これを考慮した、「自己破壊」または「消滅」メッセージを許可するメッセージングアプリは、短期間または事前に定められた期間後に自動的に破壊され、送信されたメッセージを追跡できなくなる。これは危機にさらされた人々にとってより安全な選択肢を提供するものである。
- **メッセージングアプリ企業は、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。²⁸⁰ 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

²⁷⁸ たとえば、“Malware Posing As Human Rights Organizations and Commercial Software targeting Iranians, Foreign Policy Institutions and Middle Eastern Countries”, Iran Threats: Documenting Iranian State Sponsored Hacking, 2016年9月1日: <https://iranthreats.github.io/resources/human-rights-impersonation-malware> Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, Amnesty International, 2021年7月18日: www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus を参照

²⁷⁹ Danny O' Brien, “Your Apps, Please? China Shows How Surveillance Leads to Intimidation and Software Censorship”, Electronic Frontier Foundation, 2016年1月8日: www.eff.org/deeplinks/2016/01/china-shows-how-backdoors-lead-software-censorship

XynouとWalker, “Why We Still Recommend Signal over WhatsApp … Even Though They Both Use End-to-End Encryption”

²⁸⁰ Patrick Howell O' Neill, “Russian Bill Requires Encryption Backdoors in All Messenger Apps”, Daily Dot, 2016年6月20日: www.dailydot.com/debug/encryption-backdoor-russia-fsb

拒否したことを公に述べている。²⁸¹ 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。²⁸²

- **グループが公開に設定されている**（つまり、招待されなくても誰でも参加できる）場合、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。²⁸³
- **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。**²⁸⁴ 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。²⁸⁵

²⁸¹ Jon Russell, “Apple Won’t Create Universal iPhone ‘Back Door’ to Aid FBI”, TechCrunch (ブログ)、2016 年 2 月 17 日: <https://social.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”, PCMag UK、2014 年 1 月 8 日: <https://uk.pcmag.com/opinion/11141/what-its-like-when-the-fbi-asks-you-to-backdoor-your-software>

²⁸² 以下参照: Privacy International, “Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages”, 2019年5月29日: <http://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages>

²⁸³ V. Wadhwa, “WhatsApp Public Groups Can Leave User Data Vulnerable to Scraping”, VentureBeat (ブログ)、2018年4月3日: <https://venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/>

²⁸⁴ 今日の公衆交換電話網（PSTN、すなわち全国的、地域的または地方で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る。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ている。詳細については、ICRCとPrivacy International、*The Humanitarian Metadata Problem*、セクション5

²⁸⁵ vijay, “How To Hack Facebook Using SS7 Flaw”, TechWorm (ブログ)、2016年6月16日: www.techworm.net/2016/06/hack-facebook-using-ss7-flaw.html

John Leyden, “SS7 Spookery on the Cheap Allows Hackers to Impersonate Mobile Chat Subscribers”, The Register、2016年5月10日: https://www.theregister.com/2016/05/10/ss7_mobile_chat_hack/

12.2.4 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。

12.2.4.1 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、他者がアクセスできる情報は少なくなる。

12.2.4.2 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企業のサーバーから削除されれば、ユーザープライバシーはより良く保護される。Telegram、WhatsApp、Viber、Signalなどのアプリ企業は、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削除すると述べている。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全しており、データを消去するまでの最大時間を明示していない。

12.2.4.3 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、企業がコンテンツデータを保全している場合でも、暗号化された形式であるため当該企業または**第三者**には判読できない。暗号化はメッセージングアプリ企業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。²⁸⁶

²⁸⁶ “Secure Messaging Apps Comparison | Privacy Matters”、2022年4月8日アクセス：
www.securemessagingapps.com

12.2.4.4 データのユーザー所有権

メッセージング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 사용할 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。

12.2.4.5 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）。²⁸⁷ 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。

12.2.4.6 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。²⁸⁸

12.2.4.7 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企業は、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。対象となるアプリ企業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

²⁸⁷ Jeremy Seth Davis, “Telegram Metadata Allows for ‘Stalking Anyone’”, SC Media, 2015年11月30日, Online edition, sec. Security News: www.scmagazine.com/news/security-news/telegram-metadata-allows-for-stalking-anyone

²⁸⁸ 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?”, Mashable, 2013年3月4日: <https://mashable.com/archive/wickr>

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、Microsoft²⁸⁹とMeta²⁹⁰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、Signal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。²⁹¹

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。²⁹²

12.2.4.8 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**第三者**（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者）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企業に明確に確認するよう努めるべきである。

²⁸⁹ Microsoft、*Law Enforcement Requests Report*、Microsoft Corporate Social Responsibility、2022年2月21日アクセス：www.microsoft.com/en-us/corporate-responsibility/lerr

²⁹⁰ Meta、“Government Requests for User Data | Transparency Center”、Meta、2022年2月15日アクセス：<https://transparency.facebook.com/government-data-requests>

²⁹¹ Signal Messenger、“Government Requests”、Signal Messenger、2022年2月21日アクセス：<https://signal.org/bigbrother>

²⁹² さらなる研究のための有用な情報源は、Electronic Frontier Foundation、“Digital Citizen”、Electronic Frontier Foundation、2019年11月4日：www.eff.org/digital-citizen Privacy International、“We Demand Change and Litigate | Advocacy”、Privacy International、2022年2月21日アクセス：<https://privacyinternational.org/advocacy> Global Voices Advox、“Defending Free Speech Online”、Global Voices Advox、2022年2月21日アクセス：<https://advox.globalvoices.org> Electronic Frontier Foundation、“Deeplinks Blog”、Electronic Frontier Foundation、2022年2月21日アクセス：www.eff.org/deeplinks

12.2.4.9 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12.2.3: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）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。²⁹³

12.2.5 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ある。

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。

- グループやチャン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なすればよいか。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。

²⁹³ ICRC と Privacy International, *The Humanitarian Metadata Problem*, 2018 年 10 月, pp.61-62

- 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、どのような目的で保存されるかを、当事者がどのように知ることができるか。
- 技術的経験が十分でない人を含め、人々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。

12.3 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。²⁹⁴

- **データ主体**または他の者の生命に関わる利益
- 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**、生命に関わる利益、または公共の利益に基づいている。個人がすでにメッセージングアプリを使用して**人道団体**と通信している場合、または自分の電話番号を提供している場合、その個人は使用するメッセージングアプリのプライバシーポリシーに同意したものとみなされる。ただしこの同意を、

²⁹⁴ 第3章：個人データ処理の法的根拠を参照

人道団体による**個人データの処理**の法的根拠と混同してはならない。**人道団体**が取得する同意には通知が必要であり、本ハンドブックで説明しているように、収集されたデータの目的、保全、またはさらなる共有に関して、関連性・透明性があり、明確でわかりやすい情報を**人道団体**が提供することが重要である。²⁹⁵

人道上の緊急事態に関するメッセージは、**データ主体**の生命に関わる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。情報の品質、アクセスしやすさ、わかりやすさは、**処理**に関する通知の内容と同様に重要である。²⁹⁶

12.4 データ保全

人道団体は、情報通知及びデータ保護ポリシーに、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**（メッセージングアプリ企業）によって保存されており、さらにそれらデータの一部は、アプリを機能させるサービスプロバイダかアプリ企業の親会社といった他者と共有されている（Meta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、アプリ提供者や関係する**第三者**によって保全され、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。

²⁹⁵ 第2章：データ保護の基本原則を参照

²⁹⁶ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*（規制2016/679に基づく透明性に関するガイドライン）（WP260 Rev.01）、2018年4月11日、第4項：<https://ec.europa.eu/newsroom/article29/redirection/document/51025>

欧州データ保護会議（EDPB）、GDPR第65条(1)(a)第51項に基づくWhatsApp Irelandに関するアイルランド監督当局の決定草案に関して生じた紛争に関する拘束力のある決定1/2021。

人道団体はまた、情報の交換または「チャット」自体に関する保全ポリシーを持ち、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。

12.5 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。こうしたポリシーは、簡潔で透明性がありわかりやすく、アクセスしやすいものであり、明確で平易な言葉で書かれている必要がある。²⁹⁷

人々には、これらのポリシーは特定のアプリのデータ保護ポリシーとは異なるものであることを知らせ、関連するデータ管理者にアプローチできるようにする必要がある。データ主体の権利を行使しようとする個人は、権利の行使を考えているのが人道団体の通信チャンネル内なのか、またはアプリの範囲内なのかに応じて、異なる手順に従う必要がある。

メッセージングアプリから抽出した個人データの人道団体による消去または修正は問題なく行えるかもしれないが、メッセージングアプリから、ユーザーが既に送信したデータを破棄または削除できるとは言いきれない。これには複数の関係者（そのすべてが保持しているデータについて透明性を持っているわけではない）との交渉が必要になる可能性があるためである。このことについては、人道団体のデータ保護ポリシーにも明記しておくことが推奨される。

²⁹⁷ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*（規制2016/679に基づく透明性に関するガイドライン）（WP260 Rev.01）、2018年4月11日、第7項

12.6 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団体は送信する情報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。²⁹⁸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べきである。

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の声財団（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。²⁹⁹

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。若者の間での普及度合を考慮しWhatsApp（利用46人）と Messenger（利用476人）が手段に選ばれた。アフリカの声財団は、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、社会的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。

²⁹⁸ Patrick Gage Kelleyら、"A conundrum of permissions: installing applications on an Android smartphone", *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, Springer, Berlin/Heidelberg, 2012 年, pp.68-79: https://link.springer.com/chapter/10.1007/978-3-642-34638-5_6

²⁹⁹ Africa's Voices Foundation, "Youth Priorities for 2016 Municipal Elections in South Africa (Livity Africa)", Africa's Voices Foundation (ブログ), 2016年: www.africasvoices.org/case-studies/youth-priorities-for-2016-municipal-elections-in-south-africa-livity-africa

しかし、アフリカの声財団は、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することを目指したが、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もとめたため、問題があったと感じた。今後はプライバシーのリスクが事前に十分に理解されていない場合は、同様のプロジェクトは行わないことにした。」

先に示したように、**人道団体**は一定の間隔（たとえば必要なデータが抽出された後など）でチャットを削除することについて明確なポリシーを持つことも検討すべきである。

12.7 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、団体は**データ処理**の目的を明確に規定すべきである。

これは、そのようなソリューションが提供する使用上の柔軟性とコミュニケーションの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、一般的な人道支援活動および保護目的の範疇で十分だと考えられる。

繰り返すが、モバイルメッセージングアプリケーションによる**処理**は**人道団体**の制御の範囲を超えたものであるため、**人道団体**のデータ保護ポリシーでは、

こうしたアプリが独自のデータ保護ポリシーに従ってさまざまな目的でデータを処理する可能性があるという事実についても、明確に言及する必要がある。

12.8 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。より多くの人々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、収集したデータを管理、分析および検証する能力を組織が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、分析するための効果的なワークフローを作成する際に困難が生じるかもしれない。メッセージングアプリで使用されるシステムは、**人道団体**がもともと使用している情報管理システムやデータベースと必ずしも相互運用できるわけではない。多くの場合、**人道団体**は個々のメッセージを手作業でスプレッドシートに転記することになる。これが、データを分析して効果的な意思決定を行うための唯一の方法であろう。

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ンネルで問題となっており、³⁰⁰ 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、メッセージング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。一部のメッセージングアプリ（WhatsApp など）は、検証および事実確認プ

300 The Engine Room, “Verification of Social Media: The Case of UNHCR on Twitter”, Responsible Data (ブログ), 2016 年: <https://responsibledata.io/rd-reflection-stories/social-media-verification>

ロセスを支援する機能を開発した。³⁰¹ 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。³⁰²

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。

12.9 データ保護バイデザイン

人道団体は、メッセージングアプリを利用したコミュニケーション・チャンネルをスタートさせる前に、人道活動の基本原則に加え、³⁰³ アプリが適切な技術的、組織的措置を備えているか、そしてデータ保護のコア原則（適法性、公平性と透明性、目的の制限、データの最小化など）をふまえて設計されているかどうかを検討する必要がある。

人道団体がメッセージングアプリを開発する場合は、データ保護バイデザイン・バイデフォルトの原則を導入することを考えなければならない。これには、一連の技術的ソリューションと組織的措置の両方を活用した、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。データ保存に使用されるクライアント／サーバーアーキテクチャも、データ保護バイデザインの原則を実効すべきである。設計およびデフォルトによるデータ保護についての詳細は、第6章：データ保護のための設計を参照されたい。

³⁰¹ Mark Sweney, “WhatsApp launches factcheck feature aimed at viral messages”, *The Guardian*, 2020年8月4日、電子版、sec. Digital Media: www.theguardian.com/technology/2020/aug/04/whatsapp-launches-factcheck-feature-aimed-at-viral-messages

³⁰² 以下の例を参照されたい。Craig Silverman (ed), *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, 初版、European Journalism Centre, マーストリヒト, 2014年: <http://verificationhandbook.com>
AAVV, *DatNav: New Guide to Navigate and Integrate Digital Data in Human Rights Research*, Guide, The Engine Room; Benetech; Amnesty International, 2016年6月: www.theengineerroom.org/datnav-digital-data-in-human-rights-research
First Draft News Partner Network, “Mission Statement”, 初版, 2022年2月22日アクセス: <https://firstdraftnews.org/about>

³⁰³ ICRC, *Accountability to Affected People Institutional Framework*, 2019年1月

人道団体が独自のアプリやプラットフォームを開発することを決定する場合、留意すべき考慮事項がいくつかある。まず、団体は状況、ニーズ、地域コミュニティのコミュニケーション・チャンネル（その社会でどのようなメッセージングアプリが広く使われているのか、新しいアプリがその補完または代替のものとしてどのように機能するのかなど）を理解する必要がある。³⁰⁴ 次に、団体の受益者に新しいアプリの使用を促すことは難しい可能性がある。おそらく地元のコミュニティは、新しいアプリよりも確立されたコミュニケーションプラットフォーム（メッセージングアプリ）を好むことが多いだろう。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。³⁰⁵

12.10 国際的なデータ共有

また、一部のサービスは交差したり、関連する事業体や運営手段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、別々であると思われるべきではないし、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はMetaが所有しており、同社はFacebookも所有している）。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。³⁰⁶

³⁰⁴ 同上

³⁰⁵ ICRCとPrivacy International、*The Humanitarian Metadata Problem*、2018年10月、セクション5.4

³⁰⁶ 同上、セクション4.1

デジタル アイデンティティ

電子的に
取得された
アイデンティティ
属性の集積

デジタルアイデンティティによる
さまざまな解決策

利用可能性

援助の分配を
容易にする

セクター間で
横断的に使用

ケアの継続

課題

法的根拠

危害のリスク

データ
保護

目標、目的、
ステークホルダーの定義

第13章

デジタル アイデンティティ

VINCENT GRAF NARBEL*

* この章への貢献に対し、Aiden Slavin氏（ID2020）、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。

13.1 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。³⁰⁷ 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。³⁰⁸ 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。³⁰⁹ 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³¹⁰ 人々に法的アイデンティティ³¹¹（デジタル形式の場合もある）を

³⁰⁷ 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

³⁰⁸ 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>

³⁰⁹ Strategy & Research team, “Identity in a Digital Age: Infrastructure for Inclusive Development（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（米国国際開発庁）、2017年、p.1: https://uploads-ssl.webflow.com/5a0ad2cbd65a2f0001be3903/5baf8a923a685e04cdd721a6_USAID%20-%20Identity%20in%20a%20Digital%20Age.pdf

³¹⁰ 本章を通じて、「法的アイデンティティ」という表現は、国連の運用上の定義に従う。すなわち、「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。」“UN Legal Identity Agenda”, UN Stats, 2022年3月10日アクセス：<https://unstats.un.org/legal-identity-agenda/>

³¹¹ Strategy & Research team, “Identity in a Digital Age: Infrastructure for Inclusive Development（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）”, p.1: https://uploads-ssl.webflow.com/5a0ad2cbd65a2f0001be3903/5baf8a923a685e04cdd721a6_USAID%20-%20Identity%20in%20a%20Digital%20Age.pdf

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。この移行により、アイデンティティツールの機能の大幅な変化が起こり、データ保護とプライバシーのリスクの完全な再評価が必要となってくる。

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。

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。³¹² 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。³¹³ 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13.1に示す。

³¹² 世界銀行グループ、GSMA and Secure Identity Alliance、“Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation”, Mobile for Development, GSMA, ワシントンD.C., 2016年7月26日: www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation

³¹³ Jonathan Donner, “The Difference between Digital Identity, Identification, and ID”, Medium (ブログ), 2018年12月19日: <https://medium.com/caribou-digital/the-difference-between-digital-identity-identification-and-id-41580bbb7563>

表 13.1

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。	文脈依存的、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。	通常、政府ベースで作成される、国の人々全体をカバーする法的アイデンティティ。 ³¹⁴ 社会保障番号、出生証明書、またはAadhaar番号（インドで使われる、バイオメトリクスおよび人口統計データに基づいて個人を識別する12桁の番号）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） ³¹⁵	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。

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、さまざまな法的枠組みにより、アイデンティティ・システムの設計には大きな制

³¹⁴ Strategy & Research team, “Identity in a Digital Age: Infrastructure for Inclusive Development（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）”, p.12: https://uploads-ssl.webflow.com/5a0ad2cbd65a2f0001be3903/5baf8a923a685e04cdd721a6_USAID%20-%20Identity%20in%20a%20Digital%20Age.pdf

³¹⁵ 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。

約や要件が課される。データ保護原則を守りつつ、これらの要件に準拠することが不可欠である。

13.1.1 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（例えば、援助の分配に役立てるため）に必要な属性のみ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。

13.1.2 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**だけを持たせる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でもできるシステムを必要とする場合がある。これは、ある人物を正式に特定するために法的身分証明書（または基本的アイデンティティ）が必要になる点を除き、前のケースと非常に似ている。

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、人道的な影響を受けている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全する必要があるかどうかについても決定すべきである。

13.1.3 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。³¹⁶ 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。

以下の意思決定系統図は、アイデンティティ・システムを導入の判断を行う際に、**人道団体**が答える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。照合する必要がある場合、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全する必要があるか。

316 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、以下を参照。

“DIF – Decentralized Identity Foundation”、2022 年 2 月 22 日 ア ク セ ス : <https://identity.foundation>

“Decentralized Identifiers (DIDs) v1.0”、World Wide Web Consortium、2022 年 2 月 22 日アクセス : <https://w3c.github.io/did-core>

世界経済フォーラム、*Trustworthy Verification of Digital Identities*、白書、Inclusive Deployment of Blockchain for Supply Chains (World Economic Forum (WEF)、2019 年 4 月 : www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf

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、個人情報的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。

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**：³¹⁷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**：³¹⁸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。³¹⁹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。

³¹⁷ 第8章：バイオメトリクスを参照

³¹⁸ 第15章：ブロックチェーンを参照

³¹⁹ Ana Beduschi ら、*Building Digital Identities: The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for New Digital Identity Systems*, Open Research Exeter, University of Exeter & Coalition, 2017年、pp.15–16、p.26：https://ore.exeter.ac.uk/articles/report/Building_Digital_Identities_The_Challenges_Risks_and_Opportunities_of_Collecting_Behavioural_Attributes_for_new_Digital_Identity_Systems_/29734124?file=56753750

- **データ分析**³²⁰ 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。³²¹ 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。³²²

13.1.4 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。ただし状況によっては、こうした識別システムが受益者のアイデンティティの証明、つまり基礎的アイデンティティとして受け入れられることがある（シナリオ4参照）。しかし、人道プログラムの中には、識別を必要とせずに、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証明するために認証を行うだけでよいものもある。

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、団体の各部署は、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

³²⁰ データ分析の利用に関する課題については第17章：人工知能を参照

³²¹ Beduschi ら、*Building Digital Identities*、2017 年、p.8：https://ore.exeter.ac.uk/articles/report/Building_Digital_Identities_The_Challenges_Risks_and_Opportunities_of_Collecting_Behavioural_Attributes_for_new_Digital_Identity_Systems_/29734124?file=56753750

³²² 例えば、Facebook のシャドウアカウント。Russell Brandom、"Shadow profiles are the biggest flaw in Facebook's privacy defense", *The Verge*、2018 年 4 月11 日：www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacyを参照

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ある、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活動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³²³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。³²⁴ 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。

³²³ 「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。

³²⁴ 欧州データ保護監督官（EDPS）、*Opinion 8/2017: EDPS Opinion on the Proposal for a Regulation Establishing a Single Digital Gateway and the 'Once-Only' Principle*（意見 8/2017：単一のデジタル・ゲートウェイと「一度だけ」の原則を制定する規則の提言についてのEDPS意見）、意見、EDPS、ブリュッセル、2017年8月1日：https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en.pdfを参照

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、基本的な身分証明書の役目を果たし、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。

13.1.4 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

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さまざまな取り組みが進められている。

これらの取り組みは、自分が誰であることを証明できない人々は、自分の権利を主張したり、公共サービスにアクセスしたり、年齢、国籍、状況、その他のアイデンティティや地位の属性³²⁵に基づく給付金や受給資格を請求したりすることが困難であるという事実を端を発している。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

³²⁵ Guglielmo Verdirame と Barbara E. Harrell-Bond、*Rights in Exile: Janus-Faced Humanitarianism*、Berghahn Books、ニューヨーク、2005年、pp.59-63: <https://www.berghahnbooks.com/title/VerdirameRights>.

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。

13.2 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。³²⁶

複数の人道目的（そのうちのいくつかは必ずしも当初から識別されているとは限らない）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、当初予見しなかった目的のためにアイデンティティ・シ

³²⁶ Alessandro Mantelero, “AI and Big Data: A blueprint for a human rights, social and ethical impact assessment”, *Computer Law & Security Review*, Vol. 34, No. 4, 2018 年 8 月, p.755: www.sciencedirect.com/science/article/pii/S0267364918302012?via%3Dihub

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、プロフィー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し得る。こうした情報は、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。

13.3 データ保護バイデザインおよびデータ保護バイデフォルト

データ保護バイデザインおよびデータ保護バイデフォルトは、**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**。³²⁷ 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、**処理操作**、プログラム、ソリューションの設計を行うことを含む（第6章：データ保護のための設計を参照）。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

³²⁷ Lina Jasmontaite ら、"Data Protection by design and by default: Framing guiding principles into legal obligations in the GDPR", *European Data Protection Law Review*, Vol. 4, No. 2, 2018年, pp.168–189: <https://doi.org/10.2152/edpl/2018/2/7>

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均衡してい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。以下のセクション13.6：データ保護基本原則の適用で説明するように、このプロセスに従うことで、機関はデータ最小化と均衡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（下記のセクション13.5：データ主体の権利を参照）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。

13.4 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し得る。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のがベスト・プラクティス（最善の慣行）である。

13.5 データ主体の権利

データ主体によって管理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。³²⁸ 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：

「ID2020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**（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）の開発に影響を及ぼすために設立された。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。³²⁹

³²⁸ Michael Pisa と Matt Juden、*Blockchain and Economic Development: Hype vs. Reality*、CGD Policy Paper、世界開発センター、ワシントンD.C.、2017年7月、p.25：https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_o.pdf

³²⁹ ID2020ウェブサイトからの全ての引用：<https://id2020.org>

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、当該団体が作成した個人プロフィー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**が**処理**の法的根拠となっている場合には、受益者が**同意**を更新し、**デ処理**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。より多くのコントロールをもって、受益者はオンライン・プロフィー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。

13.5.1 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。³³⁰ 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、この権利を**デジタルアイデンティティ**・プログラムにおいて行使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、

330 セクション2.11.2：アクセスを参照

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、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ィールにアクセスし、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。

13.5.2 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、そのデータを削除できるべきである。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削除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装する必要がある。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。

13.6 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。

13.6.1 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立または照合するために、**個人データ**を処理する必要がある。これらの**処理**業務は、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**という生命に関わる権利や、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らないかもしれないことを認識することが重要である。³³¹ **同意**とは、**データ主体**がその**個人データ**の**処理**に同意することを、自由意思により、特定の、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。

³³¹ セクション3.2: 同意を参照

13.6.2 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。³³² この点で、特定の人道援助プログラムの下で**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立する目的のもの）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。³³³

- 当初の目的とその後の追加目的の両立性
- 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**処理業務**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、その団体は**データ主体**に対して更なる通知を行う必要がある。

13.6.3 均衡性

均衡性の原則は、特定の**処理目的**を達成するために、立ち入る度合いが最小限の**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

³³² 第2章：データ保護の基本原則を参照

³³³ 欧州データ保護監督官（EDPS）、*Opinion 8/2017: EDPS Opinion on the Proposal for a Regulation Establishing a Single Digital Gateway and the 'Once-Only' Principle*, pp.9–10

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であろうから、**処理**を受益者のサービスへのアクセス権を認証するために限定することで、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も、人道団体は必要なデータの量と種類について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。

13.6.4 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。

13.6.5 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、身分証明書を持たない人々にアイデンティティ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、これら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。³³⁴ 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（例えば、シナリオ3で想定されているのは複数の**人道団体**）は連携してデータを復号する必要があるため、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）を削除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。

13.6.6 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援助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、身分証明書を持たない受益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**デジタルアイデンティティ・プログラム**の場合、状況はより複雑である。なぜなら、受益者は、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、適切なデータ保全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全期間を最初に提示すべきである。この期間が終了したら、

³³⁴ Strategy & Research team, “Identity in a Digital Age”, p.25: https://uploads-ssl.webflow.com/5a0ad2cbd65a2f0001be3903/5baf8a923a685e04cdd721a6_USAID%20-%20Identity%20in%20a%20Digital%20Age.pdf

この種のプログラムに関与する機関は、データの保前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。

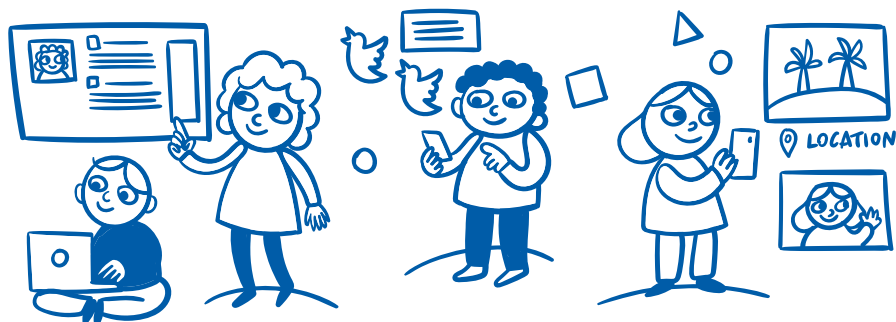
13.7 国際的なデータ共有

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。³³⁵ 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、個人データの第三者への移転（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。³³⁶ 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。

³³⁵ 第4章：国際的なデータ共有を参照

³³⁶ 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



CHALLENGES



第14章

ソーシャルメディア

**JÚLIA ZOMIGNANI BARBOZA と
LINA JASMONTAITE-ZANIEWICZ***

*この章への貢献に対し、Nicolas de Bouville 氏 (Facebook)、John Warnes 氏 (UNHCR)、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。

14.1 はじめに³³⁷

14.1.1 人道支援分野におけるソーシャルメディア

人道団体は業務の中で、支援を必要としている人々への支援、そしてキャンペーンや募金活動の両方の目的で、ソーシャルメディアをよく使用する。この章では前者の使用例にフォーカスするが、通常、使用されるソーシャルメディアの「プロフィール」は両方の目的において同じであるため、また完全に個別の分析は不可能であるため、後者についても言及することがある。

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。³³⁸ 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

³³⁷ この章では、**人道団体**が危機の影響を受けているコミュニティと通信し、関与する目的でソーシャルメディアを使用することに着目していく。危機を特定し、人道的な対応をより良いものにするためのソーシャルメディアの使用についての情報は第17章：人工知能を、メッセージングアプリについては第12章：モバイルメッセージングアプリを参照されたい。

³³⁸ メタデータの 詳細 については、次を 参照：ICRC および Privacy International, The Humanitarian Metadata Problem: “Doing No Harm” in the Digital Era, 2018 年 10 月：www.icrc.org/en/download/file/85089/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

用される。上記と同様に、団体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、³³⁹ 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³⁴⁰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。³⁴¹ 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、生成および共有されるデータを団体がコントロールすることはできなくなり、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（後述のセクション15.2: データ保護影響評価を参照）を通じて評価されなければならない。

³³⁹ 以下の例を参照されたい。Lina Jasmontaite-ZaniewiczとJúlia Zomignani Barboza, “Disproportionate surveillance: Technology-assisted and automated decisions in asylum applications in the EU?”, *International Journal of Refugee Law*, Vol. 33, No. 1, 2021 年 10 月 27 日, pp.89–110: <https://www.icrc.org/en/document/social-media-to-engage-with-affected-people>

³⁴⁰ 以下の例を参照されたい。Flor Miriam Plaza-del-Arcoら, “Improved emotion recognition in Spanish social media through incorporation of lexical knowledge”, *Future Generation Computer Systems*, No. 110, 2020 年 9 月 1 日, pp.1000–1008: <https://doi.org/10.1016/j.future.2019.09.034>

³⁴¹ 第17章: 人工知能を参照

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。³⁴²

- **災害と緊急事態の、緩和・準備・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モニタリングし、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**：国境なき医師団（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。
- **誤情報との戦い**：新型コロナウイルス感染症パンデミックの初期に、国際移住機関（IOM）は、TikTokが、外国人排斥や偏見や差別へとつながる可能性のある、パンデミックに関する誤った情報（移民が危機の原因であるという虚偽など）と戦う強力なツールであると指摘した。³⁴³

³⁴² 最初の4つの例は、Timo Lüge, “How to Use Social Media to Engage with People Affected by Crisis”, ニュースリリース、ICRC, IFRC, UN OCHA, 2017年9月：www.icrc.org/en/document/social-media-to-engage-with-affected-peopleより抜粋

³⁴³ 国際移住機関（IOM-UN Migration）, “Humanitarians on TikTok”, Medium, 2020年5月15日：<https://medium.com/digital-diplomacy/humanitarians-on-tiktok-246651af74d>

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。

14.1.2 ソーシャルメディアとデータ

14.1.2.1 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。このような大規模な**処理**が行われているにもかかわらず、どのようなデータが作成されているか、プラットフォームや他の**第三者**がプロファイリングなどの目的でこれらのデータにどのようにアクセスして使用しているかについては、透明性がほとんどない場合が多い。

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「申告されたデータ」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。³⁴⁴

さらに、申告されたデータには、ユーザーが直接提供したデータだけでなく、ユーザーに関する、他のアプリやプラットフォームから得られたデータも含まれる場合があり、³⁴⁵ ユーザーがアプリを開いたりサービスにアクセスしたりすると、同

³⁴⁴ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, 2018年10月, p.34

³⁴⁵ 欧州データ保護会議は、ソーシャルメディアユーザーのターゲティングに関するガイドラインの中で、この種のデータを「観察データ」と呼んでいる。欧州データ保護会議 (EDPB)、*Guidelines 8/2020 on the targeting of social media users*, 2021年4月13日, p.13: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

意を得る前であっても、**個人データ**がソーシャルメディア・プラットフォームに自動送信されることがある。³⁴⁶ 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、ユーザー自身が直接提供していないが、申告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。この点において、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、³⁴⁷ 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。³⁴⁸ 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。³⁴⁹ 同様に、ソーシャルメディア・プラットフォームは、「個人のウェブ閲覧行動やネットワーク接続に基づき、その人が特定の活動や製品に興味を持っている可能性が高いと推測する可能性がある」。³⁵⁰ 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。³⁵¹

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。³⁵² 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

³⁴⁶ Privacy International, “Investigating Apps Interactions with Facebook on Android”, 2019年3月: <https://privacyinternational.org/appdata>

³⁴⁷ 第17章: 人工知能を参照

³⁴⁸ Article 29 Data Protection Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 Rev.01)*、ガイドライン（個人データの処理に係る個人の保護に関する作業部会、2018年8月22日）、p.12: <https://ec.europa.eu/newsroom/article29/items/612053>

³⁴⁹ ICRC と Privacy International, *The Humanitarian Metadata Problem*、2018年10月、p.35

³⁵⁰ 欧州データ保護会議（EDPB）、*Guidelines 8/2020*、p.14

³⁵¹ ターゲット広告の詳細については、Privacy International, “AdTech”、2022年2月15日アクセス: <https://privacyinternational.org/learn/adtech> を参照

³⁵² Beduschi ら, “Building Digital Identities”, p.8: https://ore.exeter.ac.uk/articles/report/Building_Digital_Identities_The_Challenges_Risks_and_Opportunities_of_Collecting_Behavioural_Attributes_for_new_Digital_Identity_Systems_/29734124?file=56753750

ファイルを作成するために使用することさえでき、³⁵³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。³⁵⁴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。³⁵⁵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。さらに、**人道団体**は、人道活動、そしてキャンペーンや募金活動の両方の目的で、同じソーシャルメディアページやプロフィールを頻繁に使用するため、他の活動でもそのようなターゲティングから恩恵を受けると同時に、データとユーザープロフィールの生成に貢献する可能性がある。

収集可能なデータの例：

Facebookは収集したデータを、3つのカテゴリに分類する。ユーザーが作成したり提供したりしたデータ、デバイス情報、パートナーからの情報である。³⁵⁶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。³⁵⁷」

³⁵³ 例えば、Facebook のシャドウアカウント。Brandom, “Facebook Has a Shadow Profile for You” を参照

³⁵⁴ ICRC と Privacy International, *The Humanitarian Metadata Problem*, 2018 年 10 月, p.90

³⁵⁵ 以下の例を参照されたい。Albert Meijer と Martijn Wessels, “Predictive policing: Review of benefits and drawbacks”, *International Journal of Public Administration*, Vol. 42, No. 12, 2019 年 9 月 10 日, pp.1031-1039: <https://doi.org/10.1080/01900692.2019.1575664>。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。

³⁵⁶ Facebook, “Data Policy”, Facebook, 2022 年 2 月 15 日 アクセス: www.facebook.com/about/privacy

³⁵⁷ 同上

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」³⁵⁸、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。

TikTokも同様に、収集したデータを、ユーザーが提供する情報、自動的に収集される情報、他のソースからの情報の3つのカテゴリに分類する。³⁵⁹ 自動的に収集される情報には、推測情報が含まれており、プラットフォームはそれについて次のように説明している。

当社は、お客様に関して保有している情報に基づいて、お客様の属性（年齢層や性別など）と興味事項を推測します。当社は推測を利用し、たとえば、当社プラットフォームの安全な運営、コンテンツの管理、許可されている場合には、お客様の興味に基づきパーソナライズされた広告の提供などを行います。

一方、X (旧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。³⁶⁰

14.1.2.2 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

³⁵⁸ 同上

³⁵⁹ TikTok, “Privacy Policy”, TikTok, 2022 年 2 月 15 日: www.tiktok.com/legal/privacy-policy-eea?lang=en

³⁶⁰ ICRC と Privacy International, The Humanitarian Metadata Problem, 2018 年 10 月, p.96

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 Meta 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。³⁶¹ 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」。³⁶²

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）。³⁶³ 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は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ける

³⁶¹ Facebook、「Data Policy」：www.facebook.com/about/privacy

³⁶² ICRC と Privacy International、*The Humanitarian Metadata Problem*、2018 年 10 月、p.96

³⁶³ Facebook、「About Customer List Custom Audiences」、Facebook Business Help Center、2022 年 2 月 15 日アクセス：www.facebook.com/business/help/341425252616329

ようFacebookに求めることがある。³⁶⁴ 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。³⁶⁵ 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）³⁶⁶ 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。³⁶⁷ 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。³⁶⁸ 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。同様にAppleは、最近のバージョンのモバイルオペレーティングシステムで、モバイルユーザーによるこうした行動の透明性と制御を高めること

³⁶⁴ 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, “About MetaPixel”, Facebook Business Help Center, 2022年2月15日アクセス：www.facebook.com/business/help/742478679120153を参照

³⁶⁵ Brendan Van Alsenoy ら, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook’s Revised Policies and Terms*, Belgian Privacy Commission, 2015年, pp.55-64

³⁶⁶ Katie Paul, “Facebook Separates Security Tool from Friend Suggestions, Citing Privacy Overhaul”, Reuters, 2019年12月19日, sec. Internet News: www.reuters.com/article/us-facebook-privacy-idUSKBN1YN26Q

³⁶⁷ プラットフォームはまた、2020年に、人種や民族に関連するターゲットオーディエンスのカテゴリの一部を、悪用を防ぐために削除した。ただし、プラットフォームが人種カテゴリの代理ともみなされるカテゴリを依然として使用しているという事実疑問を抱く向きもある。Meta, “Simplifying Targeting Categories”, Meta for Business, 2020年8月11日: www.facebook.com/business/news/update-to-facebook-ads-targeting-categoriesを参照。

Jon Keegan, “Facebook Got Rid of Racial Ad Categories. Or Did It?”, The Markup, 2021年7月9日: <https://themarkup.org/citizen-browser/2021/07/09/facebook-got-rid-of-racial-ad-categories-or-did-it>も参照

³⁶⁸ Erin EganとDavid Baser, “Now You Can See and Control the Data That Apps and Websites Share With Facebook”, Meta (ブログ), 2019年8月20日: <https://about.fb.com/news/2019/08/off-facebook-activity>

を目的とし、ソーシャルメディアアプリケーションなどのモバイルアプリ間の追跡オプションを制限している。³⁶⁹

広告に関して、TikTokはFacebookと同様の方法でパートナーからデータの共有・受信を行う。プラットフォームのプライバシーポリシーには次のように書かれている。

広告主と測定・データパートナーは、広告用のモバイル識別子、ハッシュ化された電子メールアドレス、ウェブサイトやアプリでユーザーが行ったアクションについてのイベント情報などの情報を当社と共有します。当社の広告主やその他のパートナーの一部は、当社のTikTok広告主ツール（TikTok Pixelなど）を統合することで、当社がそのウェブサイトやアプリから同様の情報を直接収集できるようにしているところもあります。

一方、X（旧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。事実上、X（旧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。³⁷⁰」

³⁶⁹ Apple, “User Privacy and Data Use – App Store”, Apple Developer, 2022年2月15日アクセス: <https://developer.apple.com/app-store/user-privacy-and-data-use>. “How the Apple iOS 14 Release May Affect Your Ads and Reporting”, Facebook Business Help Center, 2022年2月15日アクセス: www.facebook.com/business/help/331612538028890

³⁷⁰ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, 2018年10月, p.97

14.1.2.3 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。³⁷¹ 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。これに関して、いくつかのソーシャルメディア企業は、政府のアクセス要求についての情報を含む透明性レポートを公開している。³⁷²

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。³⁷³ 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³⁷⁴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³⁷⁵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

³⁷¹ 同上、p.34

³⁷² Meta, “Government Requests for User Data | Transparency Center”. Twitter, “Twitter Transparency Center”, Twitter, 2022年2月15日 アクセス:<https://transparency.twitter.com/en.html>, TikTok, “Reports”, TikTok, 2022年2月15日アクセス:www.tiktok.com/transparency/en-us/reports

³⁷³ Privacy International, “Social Media Intelligence”, Privacy International, 2017年10月23日:<http://privacyinternational.org/explainer/55/social-media-intelligence>

³⁷⁴ 以下の例を参照されたい。Privacy International, “Push This Button For Evidence: Digital Forensics”, Privacy International, 2019年6月24日:<http://privacyinternational.org/explainer/3022/push-button-evidence-digital-forensics>. Privacy International, “Can the Police Limit What They Extract from Your Phone?”, Privacy International, 2019年11月14日:<http://privacyinternational.org/node/3281>

³⁷⁵ Privacy International, “Cloud Extraction Technology: The Secret Tech That Lets Government Agencies Collect Masses of Data from Your Apps”, Privacy International, 2020年1月7日:<http://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data>.

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。

14.2 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ができ、かつ実施するべきである。

人道団体は、受益者がすでに登録しているか、プラットフォームの利用条件に同意していることが期待される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、団体が**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。³⁷⁶ 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。

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ということである。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。³⁷⁷ たとえば、ユーザーが「いいね!」

³⁷⁶ 第5章：データ保護影響評価（DPIAS）を参照

³⁷⁷ ICRCとPrivacy International、*The Humanitarian Metadata Problem*、2018年10月、p.17

ボタンをクリックしたり、他のウェブサイトへ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ァイ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。³⁷⁸ 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。³⁷⁹ これは、プログラムを実施する前に**人道団体**が行っている他の形式の影響評価をDPIAに置き換えるべきであるという意味ではない。ただし、**個人データの処理**から生じる影響を、データ保護以外の分野の関係者も巻き込み、総合的な方法で考慮する必要がある。

これは、**個人データ**、特にメタデータの**処理**には重大なリスクが伴う可能性があるためである。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であると述べている。³⁸⁰ 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。³⁸¹ 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

³⁷⁸ 同上、p.29

³⁷⁹ Alessandro 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, pp. 754–772: <https://doi.org/10.1016/j.clsr.2018.05.017>

³⁸⁰ ICRC と Privacy International, *The Humanitarian Metadata Problem*, 2018年10月、p.22

³⁸¹ 同上、p.23–24

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。たとえば、人道団体への物理的なアクセスが難しい場所では、ソーシャルメディアは、団体と受益者の間の効果的なコミュニケーション手段を提供できる場合がある。³⁸²しかし、緊急時には、恐怖やデマの拡散を避けるために政府がソーシャルメディアをシャットダウンすることがあり得る。³⁸³これは、人道団体が他のコミュニケーション手段を検討する必要があることを意味する。

14.3 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、³⁸⁴これらのデータは、申告されたデータと推定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。³⁸⁵ 実際、ソーシャルメディア・プラットフォームだけでなく、他の事業体も、

³⁸² 人道活動の地平に影響をおよぼしている現在の技術的变化に適応するために、ICRCは物理的接触に代わる手段のひとつとして、ソーシャルメディアやその他の関連手段を提案してきた。こうしたコミュニケーションやその他の活動を責任を持って管理する方法に関するICRCのガイドラインは、以下で見ることができる：ICRC, *Accountability to Affected People Institutional Framework*, Publication, ICRC, ジュネーヴ, 2019年2月15日：www.icrc.org/en/publication/accountability-affected-people-institutional-framework

³⁸³ 以下の例を参照されたい。Jane Wakefield, “Sri Lanka Attacks: The Ban on Social Media”, *BBC News*, 2019年4月23日, Online edition, sec. Technology: www.bbc.com/news/technology-48022530

³⁸⁴ 以下の例を参照されたい。Privacy International, “Guess What? Facebook Still Tracks You on Android Apps (Even If You Don’t Have a Facebook Account)”, Privacy International, 2020年10月7日: <http://privacyinternational.org/blog/2758/appdata-update>
Privacy International, “How Apps on Android Share Data with Facebook – Report”, Privacy International, 2018年12月29日: <http://privacyinternational.org/report/2647>

³⁸⁵ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, 2018年10月, pp.89-90

こうしたプラットフォームから公開されている情報に基づいて同様の推定を行うことができる。その一例が2022年の事件である。あるNGOが、所有者の**個人データ**を匿名化することなく、3,300件超のTwitterアカウントの政治的プロフィールを作成した研究を発表したとして、ベルギーとフランスのデータ保護当局より制裁措置を受けている。³⁸⁶ **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。³⁸⁷ さらに、これらの推論は、ソーシャルメディアのユーザーをターゲットにしたり、区別したりするために利用されるだけでなく、ユーザーを操作するためにも使用される可能性があることに注意する必要がある。これについては、

「ターゲティングメカニズムは、定義上、個人の行動や選択に影響をおよぼすために利用される。それは、消費者としての商品購入の決定に関しても、市民生活を送る個人としての政治的決定に関しても、影響をおよぼす。また、ある種のターゲティングアプローチによって、個人の自主性や自由が損なわれることさえ起こりえる（たとえば、ある種の脆弱性、個人の価値観、または懸念事項を悪用したり強調したりするように設計された、個別化されたメッセージを送信するなど）。³⁸⁸」

また、ソーシャルメディア・プラットフォームは、利用規約、プライバシーポリシー、**データ処理**活動方法を非常に頻繁に変更しており、その変更には必ずしもユーザーの**同意**が求められるものでもないことを考慮することも重要である。さらに、ユーザーは、プラットフォームが申告され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

³⁸⁶ Autorité belge de Protection des Données, *Décision quand au fond 13/2022* du 27 janvier 2022, 2022年1月27日

³⁸⁷ ICRC と Privacy International, *The Humanitarian Metadata Problem*, 2018年10月, p.91

³⁸⁸ 欧州データ保護会議（EDPB）、*Guidelines 8/2020*, p.7

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。³⁸⁹

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。³⁹⁰」

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。

また、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。

³⁸⁹ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, 2018年10月, p.102

³⁹⁰ 同上, p.106. Privacy International, “Fintech”, Privacy International, 2022年2月21日
アクセス: <https://privacyinternational.org/learn/fintech>も参照。

14.4 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）。³⁹¹ 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、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。

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

³⁹¹ 欧州連合司法裁判所（CJEU）、第210/16事件、Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH、判決ECLI:EU:C:2018:3885、2018年6月

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**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則した、Facebookのみに関わるものだが、³⁹² 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のページに関連した**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、ソーシャルメディア・プラットフォームが、団体のページを通じて収集された**個人データ**を人道的目的以外のために処理する場合、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。ただし、場合によっては、**人道団体**が特定の人々とコミュニケーションを取るために、他に選択肢がない場合もある。これは、その人々が特定のソーシャルメディア・プラットフォームを主に使用しており、他のコミュニケーション手段の使用が進まない可能性があるためである。しかし、選択肢の制限に関係なく、**人道団**

³⁹² 欧州データ保護会議は、ソーシャルメディアユーザーをターゲットにする活動における共同管理は、こうしたサービスを提供するすべてのソーシャルメディア・プラットフォームに適用されると解釈した。複数のターゲティング活動における共同管理者の役割と責任に関する分析については、以下を参照されたい。欧州データ保護会議（EDPB）、*Guidelines 8/2020*

体はこうしたツールの使用から生じる可能性のあるリスクを軽減するためにできることはすべて行う必要がある。

14.5 データ保護基本原則

14.5.1 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**されるかをコントロール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求めたり受け取ったりするデータを**処理**することの法的根拠を決定すべきである。

その結果、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。³⁹³ 前述のように、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³⁹⁴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。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。同意に依拠する場合、個人は同意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再使用を制御できなくなる可能性があり、受益者が同意を撤回した場合、団体はコンテンツを完全に削除できない可能性がある。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。³⁹⁵

³⁹³ 第3章：個人データ処理の法的根拠を参照

³⁹⁴ 例えば、2019年にIFRCは、気候変動対策を促進するためのグローバルなフラッグシップキャンペーンを推進する上での主要なツールとして、組織のTikTokアカウントを使用することを選択した。Dante Licona と Melis M. Figanmeşe, “We Were the First Global Humanitarian Organization to Partner with TikTok”, Medium, 2019年10月22日: <https://medium.com/digital-diplomacy/we-were-the-first-global-humanitarian-organization-to-partner-with-tiktok-ea16b280d51>を参照

³⁹⁵ 第3章：個人データ処理の法的根拠を参照

14.5.2 情報

個人には、**データ管理者**によって、自分のデータの**処理**に関する明確かつ適時な情報が与えられるべきであり、³⁹⁶ 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**は上記の行為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。³⁹⁷ 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El Jaguarのページを使って受益者と連絡

³⁹⁶ セクション2.10：情報を参照

³⁹⁷ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, 2018年10月、p.17

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。³⁹⁸

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、受益者が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および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し得る、最も起こ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。

14.5.3 データ保全

データ保全の原則に従って、データは処理される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、危機が発生している間、等がある。³⁹⁹ 収集の時点で保全期間を決定できない場合は、最初に定められた期間の終了時に見直しを行う必要がある。

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。

³⁹⁸ キャンペーンビデオ（スペイン語）はこちらを参照：El Jaguar, “Privacidad En Facebook”, Facebook, 2018年10月27日：www.facebook.com/ConfiaEnElJaguar/videos/874221649451680

³⁹⁹ セクション2.7：データ保全を参照

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全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持しているという証拠がある。⁴⁰⁰ 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か月後に削除されます。アカウント確認の目的で政府発行の身分証明書のコピーを提出した場合、別途の定めがない限り、審査後30日後にそのコピーは削除されます。⁴⁰¹」

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。

また、**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全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。

⁴⁰⁰ Aimee Picchi, “OK, You’ ve Deleted Facebook, but Is Your Data Still out There?”, CBS News, 2018年3月23日、Online edition、sec. Moneywatch : www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there

⁴⁰¹ Facebook, “Data Policy” : www.facebook.com/about/privacy

14.5.4 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14.2：データ保護影響評価参照）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。

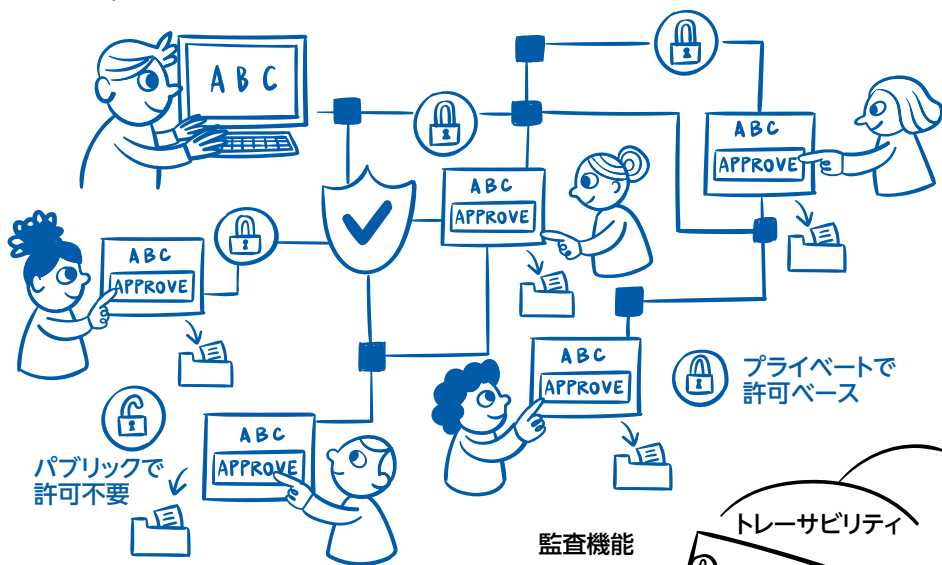
内部的には、**人道団体**は、受益者から収集したデータを保護するために、ログインと強力なパスワードによりデータを保護すること、必要な場合のみアクセスを許可すること、およびデータを正しく扱うために職員を訓練することなど、適切な措置を確実に講じることが望ましい。

14.6 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、団体側は、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。⁴⁰² 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課題となる場合もある。

⁴⁰² 第4章：国際的なデータ共有を参照

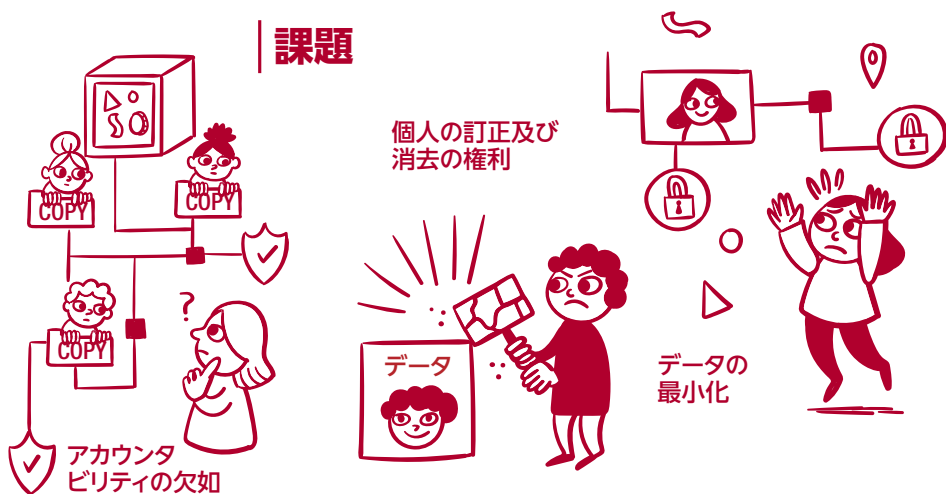
ブロックチェーン



利用可能性



課題



第15章

ブロックチェーン

VINCENT GRAF NARBEL*

* 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。

15.1 はじめに

近年、「**ブロックチェーン**」が流行語となっており、人道分野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プログラムの効率性を改善できると主張されている。⁴⁰³ 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。⁴⁰⁴ 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15.1.1からセクション15.1.3）。**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15.2からセクション15.7で説明するデータ保護分析を補完するものに過ぎない。⁴⁰⁵

15.1.1 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。⁴⁰⁶ 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**技術は、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

⁴⁰³ Vanesse Ko と Andrej Verity, *Blockchain for the Humanitarian Sector– Future Opportunities*, DH Network, UN-OCHA, 2016 年 11 月, pp.12–14 : <https://reliefweb.int/sites/reliefweb.int/files/resources/BlockChain%20for%20the%20Humanitarian%20Sector%20-%20Future%20Opportunities%20-%20November%202016.pdf>

⁴⁰⁴ 同上, p.8.

⁴⁰⁵ 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ら, “Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers”, *Richmond Journal of Law and Technology* (ブログ), 2018 年 11 月 6 日 : <https://jolt.richmond.edu/blockchain-demystified-a-technical-and-legal-introduction-to-distributed-and-centralised-ledgers>を参照

⁴⁰⁶ Michèle Finck, “Blockchains and Data Protection in the European Union”, *European Data Protection Law Review*, vol. 4, no 1, 2018 年 : <https://doi.org/10.21552/edpl/2018/1/6>

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）。⁴⁰⁷ 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15.1.2 **ブロックチェーン**のタイプを参照）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。

⁴⁰⁷ 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

「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）変更する必要がある、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ずに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。⁴⁰⁸

情報が**ブロックチェーン**に追加されると、トランザクションを保護するために、公開鍵と秘密鍵を含むメカニズムが使用される。**ブロックチェーン**のユーザーは、こうした鍵のペアを1つ以上所有する。公開鍵、または公開鍵から導き出された値は、**ブロックチェーン**上のユーザーのアドレスとして機能する。これは公知のものであり、追加された情報の発信元と宛先を検証するために使用される。⁴⁰⁹ **ブロックチェーン**アドレス自体は、関係している個人のアイデンティティを明らかにするものではないものの、ひとりの特定の個人（情報の追加や受信をするユーザー）に関連付けられているため、仮名化された**個人データ**であるとみなされる。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つながりかねない。⁴¹⁰ **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。

⁴⁰⁸ Finck, “Blockchains and data protection in the European Union”, p.19.

⁴⁰⁹ 同上

⁴¹⁰ 同上、pp.24-25

ブロックチェーン・ベースのトランザクションにおける調査やコンプライアンスのニーズに対応するプラットフォームを提供することに特化した、ブロックチェーン分析サービスを提供している企業がある。さまざまなブロックチェーン・ネットワークからデータを収集、分析、解釈するためのブロックチェーンインテリジェンスを提供する。こうした企業のプラットフォームにより、ブロックチェーン活動に関わるトランザクション、アドレス、エンティティの識別と監視が可能となる。こうした調査は、企業や規制当局がマネーロンダリング防止（AML）要件を遵守するために役立つ。別の使用方法としては、暗号通貨を使用した違法活動と戦う法執行機関の支援が挙げられる。これらの調査は、ブロックチェーンの公開アドレスをユーザーの再識別のために使用できるため、可能となる。より高レベルの匿名性を実現するために、Monero プロトコルや ZCash プロトコルなど、新しい設計がいくつか提案されている。これらにはそれぞれ制限があり、人道団体はそれらの制限とバランスを取りながら慎重に利用する必要がある。ブロックチェーン・ベースのソリューションを導入する場合には、プライバシーをさらに高める必要性にも留意しなければならない。

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、⁴¹¹ 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

⁴¹¹ Ko and Verity, *BlockChain for the Humanitarian Sector*, p.9

- 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關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均衡であることが判明する場合がある。

考慮すべきもう1つの要素は、終了基準である。多くの場合、**人道支援**は一時的なものとして計画されている。たとえば、現金およびバウチャー支援プログラムで**ブロックチェーン**を使用する場合、プログラムを終了し、**個人データ**を破棄し、受益者のアカウントを閉鎖するプロセスは、**ブロックチェーン**が持つ分散的で不変の性質ゆえに、より複雑なものとなるだろう。

15.1.2 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。

表 15.1

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 （許可不要型の）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。⁴¹² 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。⁴¹³ 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**）。

⁴¹² Walid Al-Saqaf と Nicolas Seidler, “Blockchain technology for social impact: Opportunities and challenges ahead”, *Journal of Cyber Policy*, Vol. 2, No. 3, 2017 年9月2日, pp. 338–354: <https://doi.org/10.1080/23738871.2017.1400084>

⁴¹³ Pisa と Juden, *Blockchain and Economic Development: Hype vs. Reality*, CGD Policy Paper, 世界開発センター, ワシントンD.C., 2017 年7月, p.8: https://www.cgdev.org/sites/default/files/blockchain-and-economicdevelopment-hype-vs-reality_0.pdf

15.1.3 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。⁴¹⁴

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ることができる。
- **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。⁴¹⁵
- 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。⁴¹⁶

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、

⁴¹⁴ 詳細については、Finck, “Blockchains and data protection in the European Union”。Baconら, “Blockchain Demystified”, を参照。

⁴¹⁵ PisaとJuden, *Blockchain and Economic Development*, p.9

⁴¹⁶ 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、およびセクション15.5.4データセキュリティを参照）

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。⁴¹⁷
- 個人は、情報通知を通じて**個人データの処理**について通知されなければならない。又、**個人データ**に関する権利（消去、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（**現金およびバウチャー支援**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。
- 法的管轄区域ごと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。⁴¹⁸

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

⁴¹⁷ Baconら、"Blockchain Demystified"、p.15

⁴¹⁸ PisaとJuden、*Blockchain and Economic Development*、p.49

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）。⁴¹⁹

15.1.4 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。⁴²⁰ 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。⁴²¹

現金およびバウチャー支援 (Cash and Voucher Assistance, CVA) ⁴²²: 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、CVA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。CVA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15.5.4：データセキュリティ参照）。

ロジスティクスの最適化とトラッキング: 人道援助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、

⁴¹⁹ 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、Michèle Finck, *Smart Contracts as a Form of Solely Automated Processing Under the GDPR*, SSRN Scholarly Paper, Social Science Research Network, ニューヨーク州ロチェスター, 2019 年1月8日: <https://papers.ssrn.com/abstract=3311370>を参照

⁴²⁰ 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、Larissa Fast と Giulio Coppi, *Blockchain and Distributed Ledger Technologies in the Humanitarian Sector*, Humanitarian Policy Group Report, ODI, ロンドン, 2019 年 2 月: <https://odi.org/en/publications/blockchain-and-distributed-ledger-technologies-in-the-humanitarian-sector>

⁴²¹ KoとVerity, *BlockChain for the Humanitarian Sector* から例示している。

⁴²² 以下の例を参照されたい。IFRC, *Blockchain Open Loop Cash Transfer Pilot Project*, ALNAP, 2018年9月1日: <https://alnapp.org/help-library/resources/blockchain-open-loop-cash-transfer-pilot-project/>を参照

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。

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」⁴²³（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。⁴²⁴ 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**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ているようなより厳格な資金調達ポリシーを有している**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⁴²⁵（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、民間人の所在を把握し、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。

⁴²³ KoとVerity、*BlockChain for the Humanitarian Sector*、p.13

⁴²⁴ Finck、"Blockchains and data protection in the European Union"、p.18

⁴²⁵ "WhiteflagProtocol"、アクセス2022年3月16日：www.whiteflagprotocol.org.

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⁴²⁶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、CVA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携帯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、誤って支払いを依頼し、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。⁴²⁷

15.2 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均衡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

⁴²⁶ IFRC、Blockchain Open Loop Cash Transfer Pilot Project、<https://alnap.org/help-library/resources/blockchain-open-loop-cash-transfer-pilot-project/>

⁴²⁷ セクション3.2：同意参照

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⁴²⁸、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。⁴²⁹

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。⁴³⁰ 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付録に示す。

⁴²⁸ 以下の例を参照されたい。フランスデータ保護局（CNIL）、*Guidelines on DPIA*、2017 年 10 月 18 日：www.cnil.fr/en/guidelines-dpia。英国の情報コミッショナー事務局（ICO）、*Sample DPIA Template*、2018 年 6 月 22 日：<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/>を参照

⁴²⁹ DPIA モデルとその設計の詳細については、第 5 章：データ保護影響評価（DPIAs）を参照

⁴³⁰ Karl Wust と Arthur Gervais, "Do you need a Blockchain?", IEEE、2018 年、pp.45-54: <https://doi.org/10.1109/CVCBT.2018.00011>.

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プロセスでは、特定の種類の**ブロックチェーン**（すなわち、所与の状況下で想定されるもの）が**データ主体**の権利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**の均衡性という観点から**ブロックチェーン**がもたらす影響を**人道団体**に明確に示すはずである。この評価に基づいて、団体は、より少ないリスクで受益者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れるだろう。

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15.3からセクション15.7に詳述する問題と原則も考慮すべきである。

15.3 データ保護バイデザインおよび データ保護バイデフォルト

データ保護バイデザインおよびデータ保護バイデフォルトには、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、**処理業務**、プログラム、またはソリューションを設計することができる（第6章：データ保護のための設計を参照）。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（限定保全）
- 完全性と機密性（セキュリティ）
- 説明責任
- 設計による**データ主体**の権利の支援

これらの原則の一般的な説明については、第2章：データ保護の基本原則を参照。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15.1.2：ブロックチェーンの種類を参照）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。⁴³¹ 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、公開元帳には、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トが含まれているにすぎなく、⁴³² データ自体は**ブロックチェーン**に保持され

⁴³¹ Michèle 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、欧州議会調査局（EPRS）、2019年：[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)

⁴³² 暗号化ポイント（ハッシュポイントとも呼ばれる）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方向で数学的に変換するもの（出力）。特定の入力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が生成される（PisaとJuden, *Blockchain and Economic Development*）。したがって、**ブロックチェーン**にハッシュポイントを追加すると、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トと同じポイントが生成されるためである。

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。暗号化ポイントも**個人データ**に該当するかどうかは、議論の余地がある。⁴³³

15.4 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**処理**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。

各**ブロックチェーン・アーキテクチャ**は、（セクション15.1.2：ブロックチェーンのタイプに記載の通り）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）

⁴³³ Finck, *Blockchain and the General Data Protection Regulation*, p.30

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。

- 許可不要型**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。⁴³⁴ 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。⁴³⁵ ノードは**データ管理者**ではないという主張もある。⁴³⁶ また、暗号化されたデータのみを参照し、元帳の変更はできないソフトウェアプログラムを実行するノードがい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。⁴³⁷ しかし、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。パブリックで許可不要型**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型の**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。

⁴³⁴ Finck, “Blockchains and data protection in the European Union”, pp.26–27

⁴³⁵ 同上, p.26

⁴³⁶ Baconら, “Blockchain Demystified”, pp.64–65

⁴³⁷ 同上, p.64

フランス共和国データ保護局（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⁴³⁸

- 「書き込み」権限を持つブロックチェーン参加者は、彼らの入力する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**とみなされる。
- **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。

⁴³⁸ フランスデータ保護局（CNIL）、BLOCKCHAIN: Solutions for a Responsible Use of the Blockchain in Context of Personal Data、2018 年 9 月: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

15.5 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。

15.5.1 データの最小化

分散された元帳は、その性質上、**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**を処理すべきだというデータ最小化の原則に反するように思われる。⁴³⁹

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、かつ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。⁴⁴⁰

15.5.2 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。⁴⁴¹ **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

⁴³⁹ 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「その個人データが処理さ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「その個人データが処理さ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」。

⁴⁴⁰ Finck, *Blockchain and the General Data Protection Regulation*, p.30

⁴⁴¹ セクション2.7：データ保全参照

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。パブリックな元帳のような種類の**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**などはパブリックな元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。

15.5.3 均衡性

均衡性は、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。均衡性は、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、特定の実装が均衡である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、パブリックで許可不要型**ブロックチェーン**における均衡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約化された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、均衡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均衡に高いものであってはならない。

15.5.4 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。⁴⁴²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。

⁴⁴² 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

- **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。また、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削除できないため、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。⁴⁴³ 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。

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。

⁴⁴³ PisaとJuden、*Blockchain and Economic Development*、p.6

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**技術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さ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。この技術は、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。

15.6 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。

15.6.1 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。⁴⁴⁴ 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**へのポイントのみが含まれる。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。

⁴⁴⁴ セクション2.11：データ主体の権利参照

15.6.2 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。⁴⁴⁵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⁴⁴⁶。

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、不正確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。

⁴⁴⁵ 同上

⁴⁴⁶ Daniel Conte de Leon ら、“Blockchain: Properties and misconceptions”, *Asia Pacific Journal of Innovation and Entrepreneurship*, Vol. 11, No.3, 2017 年 12 月 4 日, pp.286–300: <https://www.emerald.com/insight/content/doi/10.1108/APJIE-12-2017-034/full/html>

また、DAO ハックを修正するための Ethereum ハードフォークの例: <https://blog.ethereum.org/2016/07/20/hard-fork-completed>

15.6.3 削除権

ブロックチェーンのほぼ変更不能な性質は、概念的に消去の権利と対立している。⁴⁴⁷ 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削除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、（消去権が示唆するように）削除されておらず、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（セクション15.5.4：データセキュリティを参照）の進歩を考慮すると問題になるかもしれない。

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削除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：

現金及びバウチャー支援（CVA）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消去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削除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

⁴⁴⁷ Finck, “Blockchains and data protection in the European Union”, p.30

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。個人プロフィールが削除されれば、ただちに再識別ができなくなる。

15.6.4 データ主体の権利の制限

前述のアクセス、消去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。パブリックで許可不要型の**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**をチェーン外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。⁴⁴⁸ 第2章：データ保護の基本原則では、**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、均衡性、セキュリティなど）は依然として適用される。

15.7 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、パブリックで許可不要型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

⁴⁴⁸ セクション2.11：データ主体の権利参照

タ保護について問題を提起する。⁴⁴⁹ 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地を決定することも難題になる可能性がある。第4章：国際的なデータ共有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不要型の**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いない。一方、プライベートで許可型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、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事が可能である。

データ管理者はまた、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、パブリックで許可不要型の**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、許可型の**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のため、この要件を遵守することが可能であろう。

⁴⁴⁹ 第4章：国際的なデータ共有参照

15.8 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、**人道支援**のために**ブロックチェーン**を実装するプロセスにおいて**人道団体**のガイダンスとなることを意図している。

ステップ 1：

この手順は、新しい技術を導入する際に共通するものであり、**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技術の中で、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、携帯通信事業者、その他の**人道団体**など）
- この技術の目的は何か（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。

- ステータスを保存する必要があるか?これは、システムがアクションの実行だけでなく、システムのステータスと条件の保存が必要かどうかということを意味する。
- 貢献者は複数いるか。貢献者は、システムにデータを直接書き込むことができる者を意味する。すべてのユーザーが業者のウェブサイトを通じてデータベースにアクセスする従来のEコマースにおいては、ユーザーは業者の制御なしにデータベースにアクセスできないため、業者が唯一の貢献者となる。**ブロックチェーン**の場合、考慮すべき役割がいくつかあることに注意されたい。
- 「常時オンライン」の信頼できる**第三者** (TTP) を利用できるか。TTPとは、通常はトランザクションを検証するために、特定の機能を一元的に実行するエンティティを指す。
- 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。公的な検証能力と、監査または透明性報告書の発行を混同してはならない。ここでは、データの証明可能な検証能力(数学的な意味で)を持つことを意味する。⁴⁵⁰

⁴⁵⁰ WüstとGervais, “Do you need a Blockchain?”, IEEE, 2018年

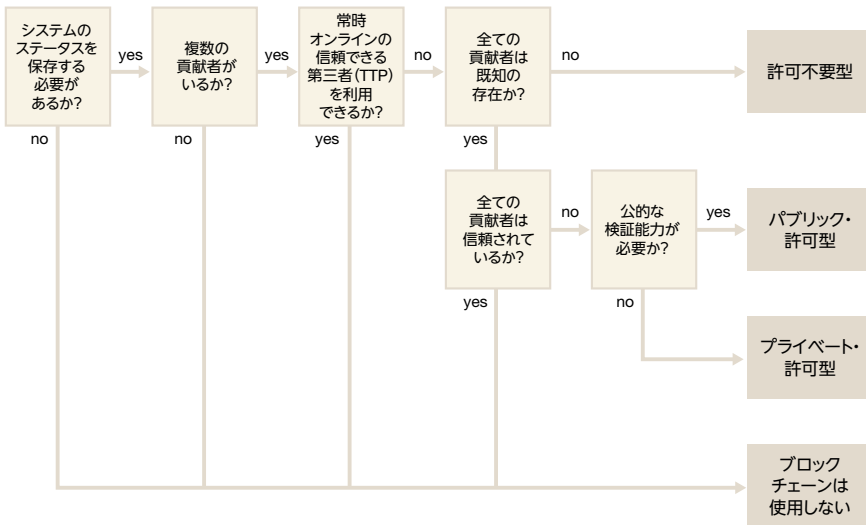


図15.1 意思決定の系統図。

WüstおよびGervaisの“Do you need a Blockchain?”, IEEE、2018年から応用。

ステップ 4：

DPO、IT サポート、および同僚と相談する。

- ガイダンスを求める。
- 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る。

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。

- 適用法は何か、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均衡するものか

- **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データ保護バイデフォルトの原則を実装する。

- 両原則には、以下の事項 – 利用可能な技術、実装費用、**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自然人の権利および自由に対する（さまざまな可能性と重大度の）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

上記の枠組みは下図のように要約される。情報収集の段階で、ブロックチェーンよりも他のシステムの方が適当であると結論付けた場合は、ステップ1以降には進まない。

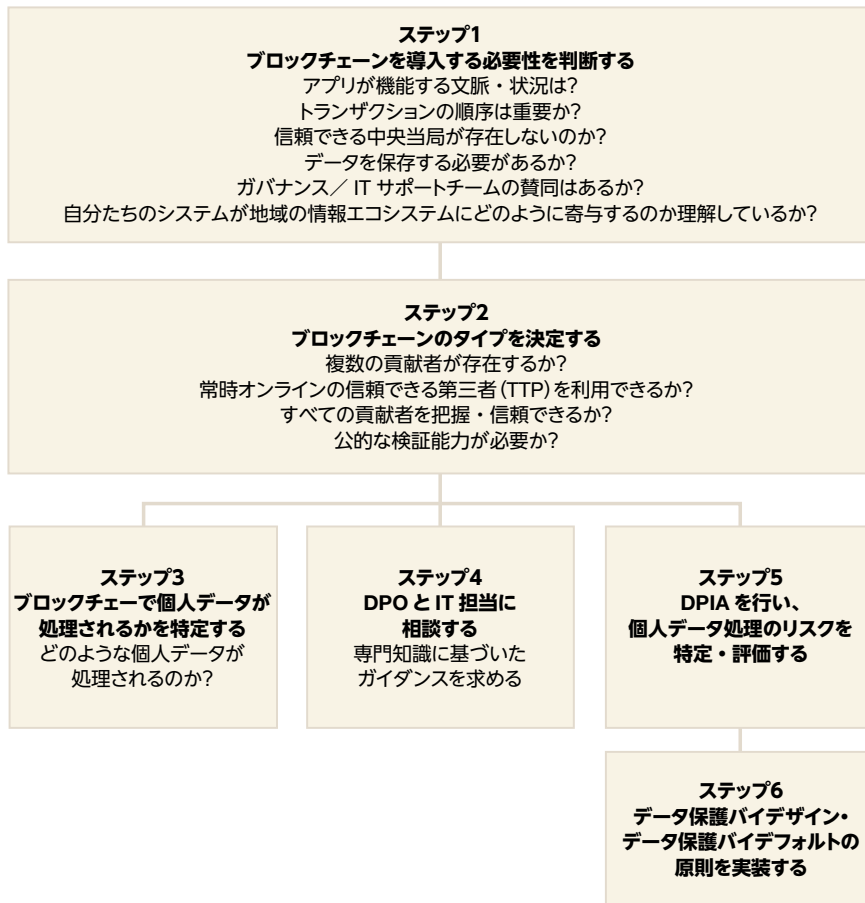


図15.2 人道支援のためのブロックチェーン・ベースのソリューション。WüstおよびGervais, “Do you need a Blockchain?”, IEEE, 2018年から応用。

援助としての接続性



利用可能性



課題



第16章

援助としての接続性

AARON MARTIN と JOHN WARNES*

* この章への貢献に対し、Robert Riemann 氏（欧州データ保護監督官）、Antonella Napolitano 氏と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。

16.1 はじめに

緊急時に接続性を維持することにより、人道的な影響を受けている人々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⁴⁵¹をもたらす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。同様の状況は、ネットワークが被害を受ける紛争環境や、その他の人道的危機環境（緊急事態前であっても接続性レベルが低かった場合など）でも発生する。

ただし、危機の影響を受けたコミュニティは接続性に非常に重きを置くものである。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。⁴⁵² **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⁴⁵³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、**人道団体**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、団体は通常、ユーザ間で共

⁴⁵¹ 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。

⁴⁵² Lin Taylor, "Internet Is As Important As Food And Water To Refugees In Greece", ハフポスト、2016年7月22日: www.huffpost.com/entry/internet-is-as-important-as-food-and-water-to-refugees-in-greece_n_57928a22e4b02d5d5ed1ac5b

⁴⁵³ 区別とその意味合いの詳しい説明は、こちらを参照されたい。ICRC, "DigitHarium | Month #5: Connectivity as Aid, for Aid, Denial", International Committee of the Red Cross、ジュネーブ、2021年7月9日: www.icrc.org/en/digitharium/digitharium-month-5

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。⁴⁵⁴ 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。

16.1.1 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。ごく最近、国連システム内では、援助行為としての接続性の調整と提供の強化・体系化のための具体的な取り組みが行われている。特に**事務総長のデジタル協力のためのロードマップ**は、すべてのステークホルダーを結集して、より安全でより公平なデジタル世界を実現することを目的とした取り組みである。このイニシアチブのカギとなる柱の1つは、「世界的な接続性」であり、2030年までにユニバーサルな接続性を達成することを目的としている。この柱の行動5は、人道的危機状況にフォーカスしたものである。⁴⁵⁵

援助としての接続性を提供するための運用上の取り組みには、次のものが含まれるが、これらに限定されるものではない。

- **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。⁴⁵⁶
- UNHCRのイノベーションサービスの**デジタルイノベーションプログラム**は、国家制度への包含を重視した権利ベースのアプローチを採用し、やむなくして難民となった人々と受け入れ先のコミュニティのための接続性ソリューションを導入する活動に取り組んでいる。難民への対応を調整する上での

⁴⁵⁴ 以下の例を参考されたい。UNHCR Innovation, “Connectivity for Refugees”, UNHCR Innovation（ブログ）、2019年：www.unhcr.org/innovation/connectivity-for-refugees

⁴⁵⁵ 国際連合、“Secretary-General’s Roadmap for Digital Cooperation（事務総長の『デジタル協力のためのロードマップ』”、United Nations、2020年6月：www.un.org/en/content/digital-cooperation-roadmap

⁴⁵⁶ “Emergency Telecommunications Cluster (ETC)”, 2022年4月1日アクセス：www.etcluster.org

UNHCRの必須の役割の中には、難民が直面する接続性の問題の調整が含まれる場合もある。

- UNHCR、ITU、GSMA、ルクセンブルク政府の支援を受けて新たに設立された、**難民のための接続性**に関するイニシアチブは、多くのステークホルダーを巻き込み、国家と民間企業のより深い協力を促進することにより、2030年までに2,000万人の難民とその受け入れ先の接続性を促進することを目指している。
- **GIGA**は、「すべての学校をインターネットに、すべての青年を情報、機会、選択肢につなげる」ことを目的として、国際電気通信連合とユニセフによって設立されたプログラムである。⁴⁵⁷
- **NetHope**⁴⁵⁸やそのメンバー⁴⁵⁹、**Télécoms Sans Frontières**⁴⁶⁰や、その他多くの**NGO**が、さまざまな緊急事態への備えや対応の場面で接続性ソリューションを提供している。

危機に見舞われた人々に提供される商用接続サービス（携帯電話など）以外の、民間セクターの取り組みも注目に値する。

- **CISCO Crisis Response (TacOps)**⁴⁶¹ 373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 Crisis Responseは現場に72時間以内に到着して通信を再開した。

⁴⁵⁷ UNICEF と ITU、"Giga – Connect Every School to the Internet"、Giga Initiative、2022年4月1日：<https://gigaconnect.org>

⁴⁵⁸ NetHope, Inc.、"Homepage"、NetHope、2021年10月18日：<https://nethope.org>

⁴⁵⁹ NetHope, Inc.、"Our Members"、NetHope、2021年11月2日：<https://nethope.org/who-we-are/>

⁴⁶⁰ Télécoms Sans Frontières (TSF)、"Home"、Télécoms Sans Frontières – ONG téléphonie humanitaire | Telecoms Sans Frontieres – NGO in Humanitarian calling、2022年4月1日：www.tsfi.org/en

⁴⁶¹ Cisco、"Incident Response – Connecting Communities in Crisis"、Cisco、2022年4月1日：www.cisco.com/c/en/us/about/csr/impact/cisco-crisis-response/incident-response.html

- 多くの場合、衛星企業⁴⁶²は企業の社会的責任（CSR）プログラムを運営しており、そのテクノロジーを活用して、人道団体と協力し合い、人道的観点から、危機に見舞われたコミュニティの接続性確保に貢献している。
- **Meta Connectivity**⁴⁶³は、2022年12月に閉鎖される以前は、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た。
- **Loon**⁴⁶⁴（現在は閉鎖）はAlphabet Inc. がリードしたイニシアチブで、携帯電話基地局に必要な設備を搭載した気球を展開することで、既存のネットワークがカバーしていないエリアにいる人々にインターネットアクセスを提供するというものであった。

16.1.2 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、影響を受けてい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

⁴⁶² Michael Oduor, “Boosting Self Reliance among Refugees through Satellite Connectivity”, Africanews, 2021 年 5 月 28 日: www.africanews.com/2021/05/28/boosting-self-reliance-among-refugees-through-satellite-connectivity.
^{SES}, “SES Is Enabling Disaster Response and Connecting Affected Communities”, Bloomberg.com, 2017 年 3 月 22 日: www.bloomberg.com/press-releases/2017-03-22/ses-is-enabling-disaster-response-and-connecting-affected-communities. “Intelsat Customer UNHCR Wins Changing Lives Award at AfricaCom 2017”, Intelsat (ブログ), 2017年11月16日: www.intelsat.com/newsroom/intelsat-customer-unhcr-wins-changing-lives-award-at-africom-2017

⁴⁶³ Meta, “Meta Connectivity”, accessed 1 April 2022年4月1日アクセス: www.facebook.com/connectivity

⁴⁶⁴ “Loon”, X, the moonshot factory, 2022 年 4 月 1 日 ア ク セ ス : <https://x.company/projects/loon>

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。一つ目は規制の状況である。これにより、組織およびサービスのユーザー（危機の影響を受けたコミュニティなど）にできること、できないことが明らかになる。

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 경우가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。⁴⁶⁵

他の団体との協力を検討する場合（セクション16.1.3：複数のステークホルダーとのパートナーシップを参照）、**人道団体**には常にその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、少なくとも部分的にでも、**データ保護影響評価**（DPIA）を利用することが挙げられる。これは、中核となる**データ保護**の問題以外のことも検討できるように設計することが可能で（セクション16.2：データ保護影響評価を参照）、これによってパートナーシップを、「害悪を与えない」原則に徹するものとし、合理的に可能な限りリスクを最小限に抑えることができる。

16.1.3 複数のステークホルダーとのパートナーシップ

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。

⁴⁶⁵ 以下の例を参照されたい。GSMA, "Humanitarian Connectivity Charter（人道接続性憲章）", Mobile for Development（ブログ）、2022年4月1日アクセス：www.gsma.com/mobilefordevelopment/mobile-for-humanitarian-innovation/humanitarian-connectivity-charter

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、例えばモバイルサービス契約の上で作動するソーシャルメディアサービス、携帯財布またはモバイル・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、援助を受ける人道的な影響を受けている人々に直接製品を販売する者もいる。ここで、人道的な影響を受けている人々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可視化されにくい関係者もいる。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）⁴⁶⁶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、ユーザーのデータを収集したり、ユーザー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

466 ディープ・パケット・インスペクションの詳細については、Rahul AwatiとJessica Scarpati, “What Is Deep Packet Inspection (DPI)?”, Tech Target – Search Networking（ブログ）、2021年9月:www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPIを参照

主体がその送信元と宛先を知る必要があるからである。⁴⁶⁷ 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。⁴⁶⁸

人道的な影響を受けている人々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。⁴⁶⁹ 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⁴⁷⁰。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）。⁴⁷¹ 調査⁴⁷²によると、ほとんどの場合、難民やその他の移住を余儀なくされた人々は、標準的な法的手段でSIMカードを入手するのに苦勞しており、そのために公式/非公式の回避策に頼っている。そのことがこうした人々にさらなるリスクをもたらし、**人道団体**にとっては、関連するデータフローをマッピングする上での課題となっている。

この文脈では、**人道団体**は接続ネットワーク全体をコントロールすることはできず、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

⁴⁶⁷ ICRC と Privacy International, *The Humanitarian Metadata Problem*, 2018 年 10 月, pp.22-23

⁴⁶⁸ 同上, p.23

⁴⁶⁹ 同上, p.71

⁴⁷⁰ Donovan と Martin, “The rise of African SIM registration”. 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

⁴⁷¹ GSMA, “Mandatory Registration of Prepaid SIM Cards”

⁴⁷² UNHCR Innovation, “Displaced and Disconnected”, UNHCR Innovation（ブログ）、2019 年：www.unhcr.org/innovation/displaced-and-disconnected

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、人道的な影響を受けてい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、このようなコントロールの欠如から生じるリスクを、**データ保護影響評価**（セクション16.2：データ保護影響評価（DPIAS）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、人道的な影響を受けている人々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。⁴⁷³ **データ保護影響評価**によってリスクが高いことが判明した場合、**人道団体**は接続性を提供しないことを選択することもできるが、コミュニティがオープンな市場や闇の市場を通じて代替の選択肢を得ようとした場合、さらに大きなリスクを引き起こす可能性がある。**人道団体**は、こうしたリスクを総合的に考慮し、接続性エコシステムのリスクを最小限に抑える適切な措置を講じなければならない。

16.2 データ保護影響評価

データ保護影響評価（DPIA）⁴⁷⁴は、プロジェクト、ポリシー、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。

人道団体は、接続性に関するプログラムのパートナーシップを結ぶ前に、パートナー候補とそのデータ保護ポリシー、課せられる法的義務や、保有する特権および免除を評価し、対象となる人々のデータを、パートナー候補がどのように処理するかを完全に理解する必要がある。場合によっては、接続性を提供するために必要なインフラストラクチャやローカルの資産の所有権がなければ、データフローを完全に理解し制御することが非常に困難になることがある。

⁴⁷³ 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

⁴⁷⁴ 第5章：データ保護影響評価（DPIAs）を参照

機関が接続性の状況、関係者、提供するサービスの明確な全体像を収集できる場合、技術仕様やデータ保護の要件など、必要とされるサービスを説明する標準ガイドラインや要件を起草できる立場にあると言えるだろう。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、人道的な影響を受けている人々が特に脆弱であり、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。⁴⁷⁵ **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。他の適切なリスク評価枠組みの適用と並行して、DPIAの設計を工夫することで、たとえば、ネットワークへの不平等なアクセス⁴⁷⁶や、デジタルに精通していない人々が排除される可能性についての問題を特定できるようにすることもできる。

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、人権デューデイルジェンスプロセスの結果が不適當であること、それによって生じる可能性のある風評リス

⁴⁷⁵ EU Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679* (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)、2017年10月。

Raphaël Gellert, “Understanding the notion of risk in the General Data Protection Regulation”, *Computer Law & Security Review*, Vol. 34, No. 2, 2018 年 4 月 1 日, pp.279–288: <https://doi.org/10.1016/J.CLSR.2017.12.003>参照

⁴⁷⁶ 例えば、若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・マナーの利用率は33% 低い。」出典:GSMA, *Connected Women: The Gender Analysis & Identification Toolkit. Estimating subscriber gender using machine learning* (コネクテッド・ウイメン: 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: www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/08/GSMA-Gender-Analysis-and-Identification-Report-August-2018.pdf

クを理由に、民間セクターのパートナーとの協力を見送ることを考慮する必要もあり得る。接続性プログラムが、適切に軽減できないような問題を引き起こす可能性があることがDPIAによって判明した場合、プログラムの中止を決定することが適切である場合もある。

16.3 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：データ保護の基本原則で詳しく定義、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さまざまな段階で収集されるため、データ提供者から取得できる、または利用可能な情報に基づいて、各段階のデータフローの可能な限りのマッピングを行い、誰がどのようなデータを収集しているか、データの保全期間はどれくらいか、誰と共有されるかを特定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、団体が、自らの権利⁴⁷⁷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

⁴⁷⁷ セクション2.11：データ主体の権利を参照

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**からの要請への対応を含め、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。

16.4 データ保護の基本原則

16.4.1 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、第3章：個人データ処理の法的根拠に挙げており、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**とサービスプロバイダは、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**：これは、接続へのアクセスを容易にするという特定の権限を持つ組織、またはこうした権限を持つ組織の指示に従って作業を行う**データ処理者**の選択肢となり得る。⁴⁷⁸
- **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団体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、団体が追求

⁴⁷⁸ 第3章：個人データ処理の法的根拠を参照

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。⁴⁷⁹

契約の履行：適用される契約法規に基づいて、危機の影響を受けているコミュニティに、商業ベースで接続サービスを提供する民間企業は、**データ処理**の法的根拠として、契約の履行を用いる場合がある。⁴⁸⁰

- **法的義務**：一部の法管轄地では、接続サービスを利用するためにユーザー登録が必要な場合がある。この場合、登録のためにユーザーのデータを**処理**する法的根拠は、法的義務の遵守となる。⁴⁸¹

16.4.2 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。こうした事業者には、事業展開する国の電気通信規制に応じて、通信ネットワークを保護し、送信されるデータの安全性を保つために、技術的および組織的なセキュリティ対策の導入が求められる。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。⁴⁸²

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。⁴⁸³ 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

⁴⁷⁹ セクション3.5：正当な利益を参照

⁴⁸⁰ セクション3.6：契約の履行を参照

⁴⁸¹ セクション3.7：法的義務の遵守を参照

⁴⁸² 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

⁴⁸³ ICRCとPrivacy International, *The Humanitarian Metadata Problem*, 2018年10月、p.25

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。⁴⁸⁴ 同様の法律がベルギー、スイス⁴⁸⁵、オーストリアで可決された。⁴⁸⁶ 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。⁴⁸⁷ 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、その任務およびステータスにもよるが、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

⁴⁸⁴ 同上、p.62

⁴⁸⁵ Secrétariat d'État aux migrations, "Mise en œuvre de la révision de la loi sur l'asile (LAsi): accélération des procédures d'asile", 政府機関ウェブサイト、スイス連邦、2018年5月12日: www.sem.admin.ch/sem/fr/home/sem/rechtsetzung/aend-asylg-neustruktur.html

⁴⁸⁶ ICRC et Privacy International, *The Humanitarian Metadata Problem*, 2018年10月。オーストリア国会議事堂, "Fremdenrechtsänderungsgesetz 2018 – FrÄG 2018", 政府機関ウェブサイト, 2018年6月13日: www.parlament.gv.at/gegenstand/XXVI/I/189も参照

⁴⁸⁷ 例えば, Bruce Schneier, "China Isn't the Only Problem with 5G", *Foreign Policy* (ブログ), 2020年1月10日: <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance> を参照

タが保健当局と共有される場合のように、人道的な影響を受けている人々の利益になりうる。**人道団体**は、そのような協力の取り決めについて人道的な影響を受けている人々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、可能であれば、パートナーとセキュリティ対策について交渉を行い、組織の管理外にある部分も含め、接続性チェーン全体にわたる、最高レベルのセキュリティを確保すべきである。

データ保全 16.4.3

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全してはならない。⁴⁸⁸ これは、**個人データ**が不要になった時点で、常に削除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。

データ主体との接続サービス契約の履行において要求される保持以外にも、モバイルネットワーク事業者は、国内法で指定された期間、ユーザに関するデータを保全する義務がある。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全しないで済む。

⁴⁸⁸ セクション2.7：データ保全を参照

16.4.4 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に連絡す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。⁴⁸⁹

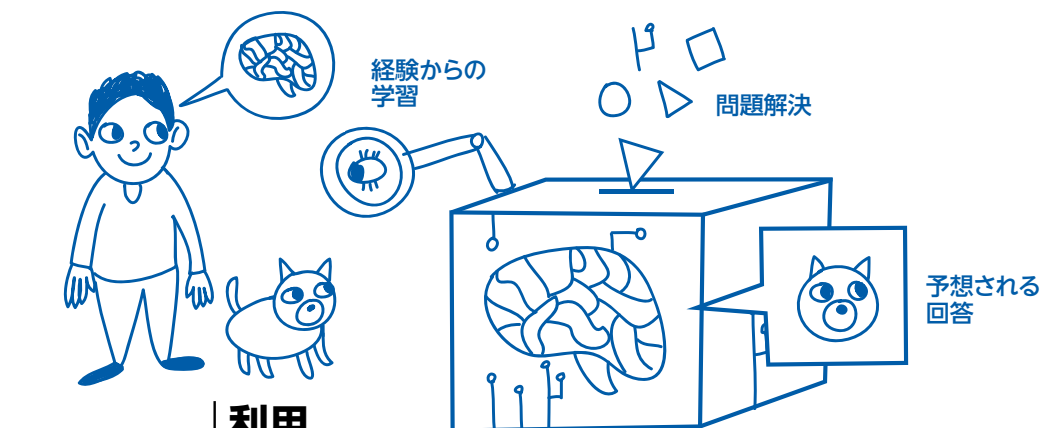
⁴⁸⁹ El Jaguar, “Privacidad En Facebook” を参照。このキャンペーンビデオでは、ソーシャルメディアにおけるプライバシーとプロフィールの安全性に関するヒントを提供している。

16.5 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。それでも、団体はプロバイダが必要なデータ転送の取り決めに確実に履行するよう、デューデリジェンスを行う必要がある。⁴⁹⁰

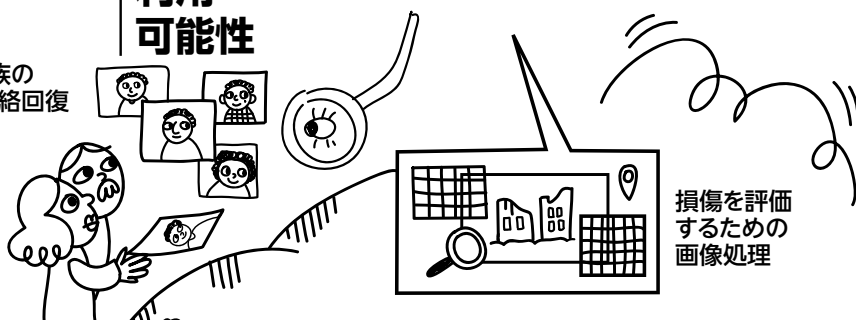
⁴⁹⁰ 第4章：国際的なデータ共有を参照

人工知能



利用可能性

離散家族の
再会・連絡回復



援助を必要と
している人々の
カテゴリーの識別



課題



人口知能主導の
分析に基づく決定



結論の理解



第17章

人工智能

ALESSANDRO MANTELERO

17.1 はじめに*

本章では、人道支援分野における**人工知能**システムの使用に関連するデータ保護の課題について検討する。特に関連性が高いのは、**データ処理**における重要な要素（大規模データセットの利用など）および、特に意思決定プロセスに関わるような**処理**という目的である。続くセクションでは、まず問題となる技術について基本的な説明を行い、次に関連するデータ保護上の課題を特定した上で、そのいくつかに対処する方法について**人道団体**にガイダンスを提供する。

17.1.1 人工知能とは何か、どのように機能するか

人工知能という用語に対して、普遍的に受け入れられている単一の定義はないが、一般的には「人間の認知能力を機械で再現することを目的とした一連の科学、理論および技術」⁴⁹¹と理解されている。そして現行の形態では、技術開発者が「これまで人間に委ねられていた複雑なタスクを機械に任せる」⁴⁹²ことを可能にすることを目指している。

人工知能という文脈において、**機械学習（ML）**とは、意思決定プロセスにおける個人データの利用に関して特に関連性の高い処理方法の一つである。**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入力を受けながら、ある課題について時間をかけてより良く完了させる一連のアルゴリズムと定義することができる。⁴⁹³ **機械学習**のアルゴリズムは、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ることで、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

* 本章は、本ハンドブック第二版の、ビッグデータとAIのそれぞれに関する2つの章に基づいて、改訂したものである。これらの章の内容は、2019年にブリュッセル自由大学（VUB）のブリュッセル・プライバシー・ハブと赤十字国際委員会が主催した「人道支援における人工知能および機械学習ならびにデータ保護に関するワークショップ」において、執筆者からの寄稿により開発されたセミナーから発展したものである。

⁴⁹¹ 欧州評議会（CoE）、*Glossary on Artificial Intelligence*、Artificial Intelligence: www.coe.int/en/web/artificial-intelligence/glossary

⁴⁹² 同上

⁴⁹³ Tom M. Mitchell、*Machine Learning*、McGraw-Hill Series in Computer Science、McGraw-Hill、ニューヨーク、1997年、p.2

あまり依存しない人工知能技術もある⁴⁹⁴が、近年では機械学習が人工知能への投資の大部分を占めていることから、本章で述べる考察の主な参照となっている。

あらゆる形態の人工知能には、共通の特徴がある。つまり人工知能とは、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だということである。さまざまな人工知能技術が存在するが、機械学習に依存するものについては、以下のようにいくつかの共通する重要な要素に要約することができる。

1. ある調査分野（例えば、人物の認識や分類のための人物画像）において、特定のパターンまたは類似性（トレーニングデータ）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。
2. 人工知能は、トレーニングデータセットに存在する関連する特徴に従ってデータの分類や集約を行うことにより、これらのパターンを特定する。
3. この処理によって、新しいデータが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。これらのパターンは、使用されるデータ（例えば、グループの移動パターンを検出するためのモバイル地理位置データ）に関連する予測や分類をサポートする。⁴⁹⁵

人工知能の使用例を理解するためには、機械学習に対する3つのアプローチを区別することが重要である。

- **教師あり学習**：トレーニングデータは、それぞれのデータに「クラス」を割り当てることでラベルが付けられる。例えば、動物の画像に「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（以前に見たことのない）画像を、学習したクラスのいずれか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、広さ、建築年に基づいて家を評価するなど、異なるパラメータ（または特徴）に基づいて

⁴⁹⁴ 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。

⁴⁹⁵ ノルウェー王国データ保護機関、*Artificial Intelligence and Privacy*、ノルウェー王国データ保護機関、オスロ、2018年1月、p.7: www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

値を予測するためにも使用できる。どちらの場合も、モデルの目的は、データを正しいクラスに適切に区分するか、正しい値を評価することにある。このプロセスにおいて、データのラベル付けは重要なステップであり、データセットと分析の目的に基づいて、現場の専門家が主要な関連要素を特定する必要がある。

- **教師なし学習**：ラベルはシステムに入力されず、**人工知能**は学習データセットから自律的に検出した類似性やパターンに基づいてデータをグループ分けする。この場合、分類は学習プロセス中に**人工知能**によって行われ、**機械学習**プロセスによって作成されたクラス以外にクラスが追加されることはない。
- **強化学習**：このアプローチでは、トレーニングデータをほとんど必要とせず、その代わりに、「飴と鞭」の方法に依存する。「システムが、設計者が望んでいることを達成したとき、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を達成したときに、「報酬」のシグナルが与えられる。システムが何か間違ったことをしたとき（求める結果に向かって効率的に進めなかったとき）は、報酬は全く与えられない。⁴⁹⁶

上記のいずれかの方法に基づいて、⁴⁹⁷ 静的モデルと動的モデルを作成することができる。静的モデルは時間が経過しても変化することはない、トレーニングデータセットを利用して開発されたモデルを常に適用する。このため、開発者はモデルをより適切に制御することができるが、採用されたソリューションが時間の経過とともに改善されることはない。一方、動的モデルは、改善や変更を目的として新しいデータを利用することができるため、一種の継続的学習ができることが特徴である（スパムフィルターシステムなど）。このため、モデ

⁴⁹⁶ 同上、p.18。

⁴⁹⁷ 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しているわけではない。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、Larry Hardesty, “Explained: Neural Networks”, MIT News | Massachusetts Institute of Technology（ブログ）、2017年4月14日：<https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414>
Future of Privacy Forum, *he Privacy Expert’s Guide to Artificial Intelligence and Machine Learning*, Future of Privacy Forum, ワシントンDC、2018年10月：https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdfを参照

ルの開発に関する制御をすることができず、出力や期待される動作において、予期せぬ重大な影響をもたらす場合がある。⁴⁹⁸

これらの人工知能技術のほとんどは、性質上、大規模なデータセットに依存している。大規模なデータセットは、人工知能が適用される主な理由であり、人工知能が機能するための本質的な要素であるためである。大量のデータ、例えば、国家レベルで作成された移民に関するデータから共通のパターンを見つけることは、人間の専門家には難しい場合がある。同時に、人工知能システムが使用するコンピュータや、統計的および数学的ツールは、外れ値やその他の「ノイズ」や攪乱を最小限に抑えた大規模なデータセットに適用された場合に限り、適切に機能する。

このような技術的背景から、さまざまな情報源から生み出されるデータの利用可能性が高まり、センサー、IT機器やサービス、コンピューティング・パワーにかかるコストが低下したことにより、社会のデータ化が進み、その結果、人道支援をはじめとするあらゆる分野の人間活動において、人工知能の利用や大規模なデータセットの分析が可能になった。⁴⁹⁹ 21世紀初頭、いわゆるビッグデータと人工知能に基づくデータ分析が登場したのに伴い、社会分析へのアプローチにも変化が生じた。大規模な数学的アルゴリズムや、高度なコンピュータベースのツール（例えば、ニューラルネットワーク）を使って、多種多様な情報源から得られた非常に多くの情報を組み合わせ、分析することで、さらなる情報を抽出し、情報に基づいた意思決定を行うことが初めて可能になった。

⁴⁹⁸ マイクロソフトのTayチャットボット問題などを参照：James Vincent, “Twitter Taught Microsoft’s AI Chatbot to Be a Racist Asshole in Less than a Day”, The Verge, 2016年3月24日：www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

⁴⁹⁹ 国連人道問題調整事務所（OCHA）、*Humanitarianism in the Age of Cyber-Warfare*, OCHA Policy and Studies series, 2014年：<https://www.unocha.org/publications/report/world/humanitarianism-age-cyber-warfare-towards-principled-and-secure-use-information>を参照

しかしながら、**人工知能**を社会分析に利用することで、いくつかの疑問と「アルゴリズムによる幻想」⁵⁰⁰ のリスクが生じる。それと同様に、データ収集を実施する方法、**人工知能**モデルの設計、使用されるトレーニングデータセットおよびこのプロセスにおける潜在的なエラーやバイアスは、**人工知能**によってサポートされる**人道支援**ツールで用いられる、人間の活動や人間関係およびプロファイルの表現に影響を及ぼす。

「**人工知能**」という言葉は、自然知能と人工知能とが似ていることを示唆しているが、実はそうではない。**人工知能**は、データ駆動型の、数学的な情報処理形態に過ぎず、思考したり、概念を精緻化したり、因果関係の理論を構築したりすることはできない。**人工知能**は、非常に多くのデータを選別して、新しい情報や相関関係について推論するために、経路認識のようなアプローチを取っているのに過ぎない。したがって、データへの依存性と経路への依存性は、こうしたシステムの長所であると同時に短所でもある。そしてまた、**人工知能**ベースのソリューションは、連続的に適用されることを目的として設計されていることから、設計に問題があった場合、同じ、または類似した状況にある多数の人に影響を及ぼすことになる。

最後に、信じられないほどに大規模なデータセットと複雑な**人工知能**システムを使用することを考えると、人間の監督による、意思決定に対する保護の役割は、不可能ではない場合もあるが、非常に困難で時間のかかるものとなる可能性がある。

分野に特化した応用という点では、**人工知能**と大規模なデータセットは、**人道支援**に関連する潜在的な脅威の識別、備えの強化、支援を必要とする個人またはそのような個人のカテゴリーの識別、ならびに伝染病、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に利用される場合がある。データ駆動型テクノロジーは、**人道団体**が実施する作業の

⁵⁰⁰ 社会におけるデータ分析の利用については、Alessandro Mantelero, “Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection”, *Computer Law & Security Review*, Vol. 32, No. 2, 2016 年 4 月 1 日, pp.238–255: www.sciencedirect.com/science/article/abs/pii/S0267364916300280?via%3Dihub も参照

効果を大幅に高めることができる。具体的には、次のようなマッピングや識別である。

- 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、およびそれによって起こりうる状況の展開の予測と被害防止の準備
- 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**によって離散した家族のマッチング

人道支援における人工知能ベースのソリューションのアプリケーションには、大きく分けて2つのカテゴリーが考えられる。

- 一般的なパターンを認識し、傾向を予測するアプリケーション
- **人道支援**に関連する個人またはそのような個人のグループを識別することを目的としたアプリケーション

このような状況において、大量のデータを収集し、個人情報に基づくデータ集約型アプリケーションを使用することは、いくつかのリスクを伴う。誤解を招くような不正確な結果や判断につながる可能性があるだけでなく、正確なデータ保護を目的として設計されていないことによる、侵略的で比例的に不均衡な**人工知能**システムの開発、匿名化が不十分なデータセットに含まれる個人を**再識別**することができる重大な弱点によって影響を受けるソリューションの採用、**データ侵害**やその他のサイバーセキュリティ攻撃につながる可能性もあると思われる。⁵⁰¹

⁵⁰¹ Massimo Marelli, “Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation”, *International Review of the Red Cross*, Vol. 102, No. 913, 2020年4月, p.367: <https://doi.org/10.1017/S1816383121000151>

17.1.2 人道支援分野における人工知能

近年、利用可能なデータが増大し、**処理能力**が向上したことにより、日常生活における**人工知能**用途の数が大幅に増加している。これは例えば、バーチャルデジタルアシスタント、デバイスのロック解除や建物への出入り許可する生体認証システム、スマートシティの交通管理、オンラインプラットフォーム上でのコンテンツモデレーションをはじめとする、オンラインやオフラインの製品やサービスのその他多くの機能などである。また**人工知能**は、医療診断、画像認識、株式市場予測など、従来人間が行っていたさまざまな作業にも応用することができる。

人道支援分野への応用に関して、**人工知能**は、大規模なデータセットを収集、処理、分析し、意思決定プロセスに情報を提供するための推論や予測を抽出する能力により、人道活動の効率と効果を高めるための貴重な選択肢となる。このことは、以下に詳述する使用事例を見れば明らかである。

- **世論を読む**：ウガンダでは、国連のグローバルパルス・プログラムにおいて「音声認識技術と翻訳ツールを使用してラジオの内容をテキストに変換し、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」⁵⁰²の試験的な使用が行われた。Pulse Lab Kampalaが開発したこのツールは、さまざまな人口集団、特に農村部の人々の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は、こうした傾向から、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することができるようになり、開発プログラムを実施する際に考慮されるようになるという理論的根拠がある。
- **行方不明の子どもたちの特定と発見**：インドの「行方不明および脆弱児童全国追跡システム」が、新しい顔認識システムの試験運用開始から4日以内に、3,000人近くの行方不明の子どもを特定したことが報告されて

⁵⁰² UN Global Pulse、'Using machine learning to analyse radio talk in Uganda'
2017: <https://unsdg.un.org/sites/default/files/Using-machine-learning-radio-content-uganda.pdf>

いる。⁵⁰³ このシステムは、児童養護施設や孤児院で暮らす児童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 プログラム⁵⁰⁴ は、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アを募集した。これは、破壊された建物を識別することを目的とするもので、民間人に対する組織的な攻撃を示す可能性がある。将来的には、このデータを使って機械学習ツールをトレーニングし、画像を分析することで、処理の高速化と能力向上を実現することができると思われる。
- **疾病の予防と診断**：1990年代以降、人工知能は癌、多発性硬化症、膵臓疾患、糖尿病など、さまざまな種類の疾患の診断に使われてきた。⁵⁰⁵ 最近ではマイクロソフトが、病原体を発症前に検出する Project Premonition を開発した。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、蚊の分布について予測を立てて、対象となる種を捕獲する。そして捕獲した蚊については、機械学習技術によって、咬んだ動物から媒介される可能性のある病原体を探す。⁵⁰⁶

人工知能をベースとしたプロジェクトを扱う場合、この文脈において、データ保護の基本原則⁵⁰⁷を適用する際にも懸念が生じる場合がある。人工知能に基づくプロファイリングや、隠されたナッジングの実践は、データ主体が自己の情報を管理するという概念に基づく選択の自由という考え方に対して問いか

⁵⁰³ Anthony Cuthbertson, “Indian police trace 3,000 missing children in just four days using facial recognition technology”, *The Independent*, 2018年4月24日: www.independent.co.uk/tech/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html を参照。

また、PTI, “Delhi: facial recognition system helps trace 3,000 missing children in 4 days”, *The Times of India*, 2018年4月22日: <https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms> も参照。

⁵⁰⁴ アムネスティ・インターナショナル, “Amnesty Decoders | Join Decode Surveillance NYC”, アムネスティ・インターナショナル, 2022年3月17日閲覧: <https://decoders.amnesty.org>

⁵⁰⁵ Heather M. Roff, “Advancing Human Security through Artificial Intelligence”, Chatham House – International Affairs Think Tank, 2017年5月11日, p.5: www.chathamhouse.org/2017/05/advancing-human-security-through-artificial-intelligence

⁵⁰⁶ Microsoft, “Microsoft Premonition”, Microsoft Research (ブログ), 2022年3月21日閲覧: www.microsoft.com/en-us/research/project/project-premonition を参照

⁵⁰⁷ 第2章：データ保護の基本原則を参照

けるものであり、**人工知能**アルゴリズムが広範にわたり、複雑で、不明瞭であることが原因となって、真の意味でのインフォームド・コンセントを得て、透明性の要件を満たす機会を妨げている。ビッグデータや**機械学習の人工知能**アルゴリズムは、有用な結果を生み出すために大量のデータに依存していることから、もう一つの重要な原則であるデータの最小化に対しても、同様の課題が関連してくる。⁵⁰⁸

人工知能と大規模な**データ処理**に関連する具体的な問題を検討する前に、データ保護に関連するいくつかの特性を、この分析の冒頭で明らかにしておく。

- **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**人工知能**ベースの**データ処理**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、その他の公開されている人口統計や人口調査などの情報などの一般に入手可能なデータに基づいている。また**人道団体**は、人道対応や災害対応を向上させるために、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する場合もある。
- **緊急対応**：**人工知能**に基づく**データ処理**の成果は、**人道団体**に対して重要な利益をもたらす可能性がある。しかし、緊急事態が継続している場合や、関係する人々の生命に関わる利益に対処する場合に、使用されるとは限らない。例えば、**人道団体**が活動する例外的な「異常」事態は、予測**機械学習**アルゴリズムの限界となる場合がある。緊急事態ではない時に開発されたデータ駆動型分析による過去のデータセットやモデルは、

⁵⁰⁸ 欧州評議会 (CoE)、*Guidelines on Artificial Intelligence and data protection / T-PD(2019)01*、Guideline (Strasbourg: Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)、2019年1月25日)：<https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

欧州評議会 (CoE)、*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data / T-PD(2017)01* (Strasbourg: Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)、2017年1月23日)：<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?docuementId=09000016806ebe7a>を参照。

また、Alessandro Mantelero、Beyond Data Human Rights, Ethical and Social Impact Assessment in AI、1st ed.、*Information Technology and Law Series*、Springer、ハーグ、2022年、第1章も参照

緊急事態という極めて変化しやすい状況から生じた異常値に対応しきれない場合があるかもしれない。したがって、**人道データ**から独自に導き出された**人工知能**について検討することが重要である。なぜならこれらのモデルは、緊急時に学習した情報を統合することで、管理業務を支援し、今後の緊急事態への対応を改善する戦略に貢献するものだからである。

- **精度：人工知能**はデータ駆動型であることを考えると、トレーニングに使用されるデータの質は、モデルの開発と性能の両方に大きく影響する。したがって、人工知能モデルのトレーニングと実行に使用されるデータが、代表的な正確なものであり、バイアスが含まれていないことを確認することは極めて重要である。⁵⁰⁹
- **自動化された意思決定**：緊急事態において、自動化はタイムリーな対応を促進することができるが、誤った洞察や決定を防ぐために、複雑な背景を十分に理解する能力など、人間の介入や監視の欠如に伴うリスクに注意することが重要である。
- **他の目的のためのデータの再利用**：大規模なデータセットが利用可能になると、収集されたデータを収集時の目的以外に使用することで問題が生じることが多い。これは、**データ保護法**の下で問題となる。同法によって一般に、個人データは特定の目的のために収集され、そのような目的またはそれに適合す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に再利用されないように義務付けられている（セクション17.2.1：個人データ処理の法的根拠を参照）。
- **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、モビリティ・データ、携帯電話接続によって生成されたデータなどの公開されているデータは、一般的には機微性の高いデータではないと考えられているが、さまざまな状況にお

⁵⁰⁹ UN Global Pulseとライデン大学、“Big Data for Development and Humanitarian Action: Towards Responsible Governance”、（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）Global Pulse Privacy Advisory Group Meetings 2015–2016、2016年12月：www.unglobalpulse.org/document/big-data-for-development-and-humanitarian-action-towards-responsible-governanceを参照。

Mireille Hildebrandt, “The issue of bias: The framing powers of machine learning”, *Machine We Trust: Perspectives on Dependable AI*, ed. Marcello Pelillo and Teresa Scantamburlo, The MIT Press、マサチューセッツ州ケンブリッジ、2021年、pp.44–59：<https://dx.doi.org/10.2139/ssrn.3497597>も参照

いて、また主に人道的状況において、**機微データ**を生成する可能性があることを理解することが重要である。これは、機微性の高くないデータを**処理**する際に、例えば、潜在的な被害者、暴力下という状況にある特定の集団に属する人々、または特定の病気を患っている人々などに対する差別や抑圧の対象となり得る個人のプロファイリングが可能になる場合に起こり得る。このような場合、差分プライバシー⁵¹⁰のような特定のコンピューティング技術は、データへのアクセスを許可しながらも個人や集団のプライバシーを保護する貴重な方法となる。⁵¹¹

- **匿名化**：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、**人工知能**を使用した作業においては、**個人データの匿名化**の有効性および**再識別**の可能性については疑問が生じる場合がある。この場合も合成データ⁵¹²などのプライバシーを向上させる技術によって、**匿名化**の試みを補完し、より高い保護を提供し、**再識別**を防止することができる。⁵¹³
- **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、データや**人工知能**ベースの**データ処理**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。⁵¹⁴

⁵¹⁰ Cynthia Dwork, “Differential Privacy”, in Henk C. A. van Tilborg and Sushil Jajodia (eds), *Encyclopedia of Cryptography and Security*, Springer US, マサチューセッツ州ボストン、2011年、pp.338–40 : https://doi.org/10.1007/978-1-4419-5906-5_752

⁵¹¹ 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。

⁵¹² 合成データとは、アルゴリズムによって生成された情報であり、実世界のデータではないが、数学的または統計的に実世界のデータを反映したものである。欧州データ保護監督官（EDPS）、“IPEN Webinar 2021 – ‘Synthetic Data: What Use Cases as a Privacy Enhancing Technology?’”, EDPS, 2021年6月16日 : <https://edps.europa.eu/data-protection/our-work/ipen> を参照

⁵¹³ Prokopios Drogkaris と Monika Adamczyk (eds.), *Data Protection Engineering – From Theory to Practice*, European Union Agency for Cybersecurity (ENISA), 2022年1月27日 : www.enisa.europa.eu/publications/data-protection-engineering.

⁵¹⁴ UN Global Pulseとライデン大学、*Big Data for Development and Humanitarian Action*（開発と人道支援のためのビッグデータ）、p.7–9を参照。

Júlia Zomignani BarbozaとLina Jasmontaitė-ZaniewiczおよびLaurence Diver, “Aid and AI: The challenge of reconciling humanitarian principles and data protection”, in *Privacy and Identity Management. Data for Better Living: AI and Privacy*, IFIP International Summer School on Privacy and Identity Management, Springer, Cham, 2020年、pp.161–176 : https://doi.org/10.1007/978-3-030-42504-3_11も参照

人工知能が人道支援に使用される場合、個人に対する影響は他の状況よりもはるかに深刻になる可能性がある」と強調することが重要である。したがって、人道団体は、データ集約型の人工知能システムを用いて公開するデータや提供する情報が、たとえ集計された形であっても、保護対象とする人々に対して利用される可能性があるかどうかを考慮すべきである。さらに、「目に見えない個体群」に関する情報は、関連するさまざまな集団のデータを使って間接的に抽出される可能性があるため、マイノリティに対する差別や行動という点で潜在的な意味を持ち、特に紛争の場合には問題となる。したがって、保護体制の低下や脆弱性の増大によって特徴付けられる状況においては、データ集約型の人工知能システムを使用することの潜在的な意味という「大局」を常に念頭に置いておくことが重要である。

例

当局が、人命の損失を避けることを目的として公共デモの発生地や流れを特定するために、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資料の抽出・分析に基づいて公開または公表された調査結果を利用する場合が考えられる。しかし、同じ調査結果が同じ当局によって、そのような公共デモに参加した（あるいは参加しなかった）個人を識別するために使用される可能性があり、識別された個人のグループに対して深刻な結果をもたらす可能性がある。

人工知能には、以下のような処理シナリオが含まれる場合がある。

例1: ソーシャルメディア、検索エンジン、電気通信サービス、および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。これは、公衆衛生従事者や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手法をどのように使用できるかを示すのに役立つ。

例2：人道的な事案発生時のインタラクティブなデータ可視化ツールの開発。これは、通信信号や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のに役立つ。

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：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、クレジットカードのデータの分析。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たことを目的とする。

人工知能が利用する可能性のある大規模データセットに注目すると、以下のようことが関連する可能性がある。

- **アクセス可能なデータセット：**すなわち、政府が公表した公文書や、人々が意図的に、ソーシャルメディアを含むメディアやインターネット上で公開した情報など、既に一般に入手可能なデータセットのこと。
- **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、国際人道法や人権侵害を報告する個人のリスト。
- **個人の第三者によって保有されるデータセット：**例えば、集計化や仮名化されているかどうかに関わらず、携帯電話、通信、インターネットサービス、銀行や金融プロバイダー、金融取引データ、遠隔センサーデータなど。
- **人道団体、当局および/または企業体（上記組織や団体を含む）のデータセットの組み合わせまたはその全体。**

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。

- **データ管理者または共同管理者（他の人道団体、公的機関および/または営利団体と共同で処理の目的および手段を決定する場合）として、それぞれの組織の目的のために保有するデータを処理する。**
- **団体に代わってデータ処理を行い、データ処理者として機能する第三者（例えば、人道団体が保有するデータに関する予測分析や団体の目的のために人工知能を使用する営利団体など）を雇用する。**

- **データ管理者**であり、かつ**データ管理者**であり続ける営利団体に対して、人道的目的のためにデータ分析を実施し、**人道団体**に結論や所見を提供することを要求する。このような結論は、集計化や仮名化されたデータ、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に関連する場合がある。

17.1.3 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。データ保護の問題以外にも、⁵¹⁵ 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、行方不明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。

人工知能は、人道的影響を受ける人々にも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るが、ソリューションが正確な識別を行わない場合、本来であればプログラムに参加する資格を有していたはずの人々が、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。⁵¹⁶

⁵¹⁵ Anne Meuwese, “Regulating algorithmic decision-making one case at the time: A note on the Dutch ‘SyRI’ judgment”, *European Review of Digital Administration & Law*, Vol. 1, No. 1, 2020年, pp.209–211も参照

⁵¹⁶ Tom Willis, “Sweden: Rogue Algorithm Stops Welfare Payments for up to 70,000 Unemployed”, AlgorithmWatch, 2019年2月25日: <https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments>

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入手することになるため、アルゴリズムによって予期せぬ結果や不合理な結果が生じるリスクが高いこのことはまた、既製の**人工知能**モデルを選択する際、例えば、元々は何らかの目的のために使用されていたモデルが、異なる文脈や目的⁵¹⁷のために再利用される場合、あるいは異なる母集団からの過去のデータに基づいてトレーニングを行なったモデルを使用する場合に、文脈から逸脱するリスクが浮かび上がってくる⁵¹⁸。

さらに、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的企業が、これらの団体をターゲットにする可能性があり、データに含まれ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り得る。

バイアスは**人工知能**の有効性に別のリスクをもたらすが、特に特定の人道的文脈においては、意図した目標に適合したデータセットの使用が重要である。他の多くの技術と同様に、**人工知能**にも「ゴミを入れたら、ゴミが出てくる (garbage in, garbage out)」⁵¹⁹の概念が適用され、適合しない、不正確である、または関係のないデータを使用すると、ソリューションの精度に影響を及ぼす可能性がある。**人道団体**にとっては、既製のアルゴリズムが人道支援の文脈に適合することは極めて稀であるため、特に問題となる。例

⁵¹⁷ Robyn Caplanら、"Algorithmic Accountability: A Primer", Data & Society, 2018年4月18日、p.7: <https://datasociety.net/library/algorithmic-accountability-a-primer> を参照。PredPolアルゴリズムの事例を引用している。このアルゴリズムは、元々地震を予測するために設計されたものだが、後に犯罪のホットスポットを識別し、警察を配置するために使用された。

⁵¹⁸ 欧州評議会 (CoE)、Guidelines on Artificial Intelligence and data protection / T-PD(2019)01を参照。

欧州評議会 (CoE)、Artificial Intelligence and Data Protection: Challenges and Possible Remedies / T-PD(2018)09Rev、人工知能に関するレポート(Strasbourg: Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 2019年1月25日): <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>も参照。

⁵¹⁹ 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、「ゴミを入れば、ゴミが出てくる」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。

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、トレーニングデータセットは、マッチング機能の精度を最大化するために、身体的特徴の人種的差異を確実に統合できるように十分に広範にわたるものでなければならない。

人工知能を使った**個人データ**の処理も、個人データ保護に関する重要な課題をもたらす。収集以外の目的で大規模なデータセットを**処理**する場合、目的の制限、データの最小化、データの保持（すなわち、データ収集の目的を果たすために必要な期間だけデータを保持する）など、データ保護の基本的概念に違反する恐れがある。⁵²⁰ 本質的に、大規模なデータ分析はオープンで制限のない**処理環境**を得意とするのに対して、**個人データ**保護は制限され、明確に定義された**処理**が好ましい。したがって、データ保護はこれらの技術に対して、革新的な方法で適用される必要がある。⁵²¹

人工知能に基づく**データ処理**を行う際には、データ保護の基本原則を尊重しなければならない。この原則には、(i) 処理の公正性と適法性の原則、(ii) 透明性の原則、(iii) 目的制限の原則、(iv) データの最小化の原則、(v) データの質の原則が含まれる。これらの原則の中には、**人工知能適用**の性質に適合するものもあるが、疑問や矛盾を引き起こすものもある。⁵²² したがっ

⁵²⁰ 第2章：データ保護の基本原則を参照。欧州評議会（CoE）、*Artificial Intelligence and Data Protection: Challenges and Possible Remedies* | T-PD(2018)09Revも参照

⁵²¹ 欧州評議会（CoE）、*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* | T-PD(2017)01

Alessandro Mantelero, “Regulating Big Data: The guidelines of the Council of Europe in the context of the European Data Protection Framework”, *Computer Law & Security Review*, Vol. 33, No. 5, 2017 年 10 月, pp.584–602: www.sciencedirect.com/science/article/abs/pii/S02673664917301644?via%3Dihub

UN Global Pulse, *Guidance note on Big Data for achievement of the 2030 Agenda*, 2019 年 8 月 19 日: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

European Data Protection Supervisor (EDPS), *Opinion 7/2015: Meeting the Challenges of Big Data*, Opinion, EDPS, ブリュッセル, 2015年11月19日, p.4: https://edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_enを参照

⁵²² Alessandro Mantelero, *Beyond Data Human Rights, Ethical and Social Impact Assessment in AI*, 1st ed., *Information Technology and Law Series*, Springer, ハーグ, 2022, 第1章も参照

て、**人道団体**は、これらの原則を実際に適用する際には特に注意しなければならない。⁵²³

17.2 データ保護基本原則の適用

人工知能を統合または使用するソリューションは、適切に機能するために、個人および非個人を問わず、大量のデータを処理する。この点で、これらのアプリケーションが非個人情報または匿名化データから、**個人データ**を推論し得る点を考慮することは極めて重要である。これは、**人工知能**のソリューションが、「非個人データを識別可能にするかもしれないデータのリンクやパターンを認識する」ことができるようになってきているからである。⁵²⁴ つまり**人工知能**は、例えばセンサーやスマートデバイスが提供するデータを**再識別**することもできるのである。

したがって、**再識別**のリスク評価を実施し、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この結果を知らせることが望ましい。**再識別**の可能性が高い場合は、分析を実施しないか、または分析方法を調整することが望ましい。

このような理由から、データ保護義務に関する「出口戦略」として**匿名化**を使用することは必ずしも有効ではない。さらに、匿名のデータまたは匿名化されたデータは、**処理中**に処理能力が妨げられる可能性があるため、技術的な課題が生じることもある。

さらに、匿名化または集計されたデータを**処理**する際の**人工知能**の出力精度について評価することが望ましい。したがって、**匿名化**または集計の方法とレベルは、**再識別**のリスクを最小化するだけでなく、信頼できる結果を得る

⁵²³ 本章のデータ保護に関する議論は、第I部で示された原則に基づき、より詳細に検討するためのものである。

⁵²⁴ Centre for Information Policy Leadership, *Artificial Intelligence and Data Protection in Tension*, Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, 2018 年 10 月 10 日, p.11: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf

ために適切な品質レベルをデータが確実に維持できるよう、慎重に選択することが望ましい。

17.2.1 個人データ処理の法的根拠

人工知能主導による処理業務を実施する際、人道団体は、以下の法的根拠の1つ以上に基づいて実施する場合がある。⁵²⁵

- 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に基づく機関の権限に基づく公益
- データ主体のインフォームド・コンセント
- 組織の正当な利益
- 契約の履行
- 法的義務の遵守

しかし、人工知能アプリケーションとそれに関連するデータ処理の特殊性によって、この従来の枠組みにいくつかの課題が生じている。主にデータ処理に対する個人の同意と収集されたデータの二次利用である（すなわち、大規模なデータセットが必要とされる人工知能ではしばしば見られるように、元々は特定の目的のために収集されたデータが、別の目的のために再利用されること）。

文献でも指摘されているように、法的根拠としてのデータ主体の同意の有効性は、長くて技術的なデータ処理通知、社会的および技術的なロックイン、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によって損なわれている。⁵²⁶ このような動きは、データ主体が既に権力格差やその他の状況的要因により実効性のある自己決定が妨げられている人道支援の場面において、さらに深刻である。

⁵²⁵ 第3章：個人データ処理の法的根拠を参照

⁵²⁶ より広範にわたる分析と考察については、Alessandro Mantelero, “The future of consumer data protection in the E.U. Re-thinking the ‘notice and consent’ paradigm in the new era of predictive analytics”, Computer Law & Security Review, Vol. 30, No. 6, 2014年12月1日, pp.643–660: <https://doi.org/10.1016/j.clsr.2014.09.004>を参照。

さらに、**人工知能**に基づくプロファイリングや隠されたナッジングといった慣行は、契約上の合意に基づく選択の自由という考え方や、個人情報に対する**データ主体**のコントロールという考え方の両方にとっての課題となる。最後に、**人工知能**のアルゴリズムは複雑で不明瞭なことが多いため、真にインフォームド・コンセントを得ることが困難になっている。。

法学者は、透明性、⁵²⁷ リスク評価、⁵²⁸ 広範な同意⁵²⁹ や動的な同意⁵³⁰ などのより柔軟な**同意**形態の役割を強調することで、これらの問題に対処してきた。これらの解決策はいずれも、個人の**同意**に影響を及ぼす問題を解決するものではないが、特定の文脈においては、単独であっても、組み合わせであっても、自己決定を強化する可能性がある。

⁵²⁷ 例えば、Lilian Edwards and Michael Veale, “Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for”, *Duke Law & Technology Review*, 16, 2018 2017, pp. 18–84

Andrew Selbst と Julia Powles, “‘Meaningful information’ and the right to explanation”, *International Data Privacy Law*, Vol. 7, No. 4, 2017 年 12 月 19 日, pp.233–242: doi.org/10.1093/idpl/ixp022: <https://proceedings.mlr.press/v81/selbst18a.html>

Sandra WachterとBrent MittelstadtとLuciano Floridi, “Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation”, *International Data Privacy Law*, Vol. 7, No. 2, 2017 年 5 月 1 日, pp. 76–99: <https://doi.org/10.1093/idpl/ixp005>.

⁵²⁸ 欧州評議会 (CoE), Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data | T-PD(2017)01

Alessandro Mantelero, “Regulating Big Data.:The guidelines of the Council of Europe in the Context of the European Data Protection Framework”, *Computer Law & Security Review*, Vol. 33, No. 5, 2017 年 10 月: www.sciencedirect.com/science/article/abs/pii/S0267364917301644?via%3Dihub

UN Global Pulse, Guidance note on Big Data for achievement of the 2030 Agenda, 2019 年 8 月 19 日: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

European Data Protection Supervisor (EDPS), Opinion 7/2015: Meeting the Challenges of Big Data, EDPS, ブリュッセル, 2015年11月19日: www.edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_enを参照

⁵²⁹ Mark Sheehan, “Can broad consent be informed consent?”, *Public Health Ethics*, Vol. 4, No. 3, 2011年11月1日, pp.226–235: <https://doi.org/10.1093/phe/phr020>

⁵³⁰ Jane Kaye ら, “Dynamic consent: A patient interface for twenty-first century research networks”, *European Journal of Human Genetics*, Vol. 23, No. 2, 2015 年2月, pp.141–146: <https://doi.org/10.1038/ejhg.2014.71>

このような理論的枠組みや規制手段に関してまだ解決されていない重大な問題があるのにもかかわらず、**同意は人道団体が収集したデータを処理する正当な根拠となりうるだけでなく、第三者が収集したデータを異なる目的のために再利用する正当な根拠ともなりうる。**この意味において、**人道団体を支援するためにソーシャル・メディア・ネットワークや携帯電話事業者が提供するデータ分析は一例である。**これは場合によっては**同意**に基づくことも可能である。このような場合、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事業者は、関連情報を記載した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**について**データ主体**に通知し、**同意**を要求することができる。

データ主体が同意をする前に十分な情報を受け取ることができるようにするため、そうした情報には（実施された場合）DPIA の結果⁵³¹を含めるべきであり、経験学習型アプローチとして、データ使用の効果と**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介して提供することもできる。⁵³² **データ管理者は、データ主体に対して、同意を撤回し、当初の目的にそぐわないデータ処理に対処するための、簡単にユーザーフレンドリーな技術的手段を提供することが望ましい。**⁵³³

データ収集時に**データ主体**に対して適切な情報を提供し、**追加処理**の目的が合致している場合であっても、**同意の有効性**について評価を行うことは重要である。この評価においては、**データ主体**のリテラシーのレベル、データを**処理**することの**データ主体**に対するリスクおよび損害についても考慮することが望ましい。⁵³⁴

データ主体の同意がなくても、データ主体またはその他の人の生命に関わる利益、すなわち、データ主体またはその他の人もしくは集団の生命、インテグリティ、健康、尊厳および安全に関する不可欠な利益を保護するためにデー

⁵³¹ セクション17.6：データ保護影響評価および人権影響評価を参照

⁵³² 欧州評議会（CoE）、*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* | T-PD(2017)01

⁵³³ 同上

⁵³⁴ UN Global Pulse、Risks, Harms and Benefits Assessment Tool、2020年更新：<https://www.unglobalpulse.org/document/risks-harms-and-benefits-assessment-tool/>

タ処理が必要な場合に、**個人データ**を処理することができる。さらに、公共の利益、団体の正当な利益、契約の履行または法的義務の遵守などの法的根拠も、**データ処理**の根拠となり得る。

武力紛争およびその他の暴力状況における**人道団体**の緊急支援活動の法的根拠として生命に関わる利益を用いることに関して、**人道団体**による**データ処理**が**データ主体**または他の者の生命に関わる利益のために行われると推定される場合がいくつかある（例えば、**被調査者**であるときに**データ処理**が行われる場合、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場合など）。ただし、管理目的など緊急事態でない場合に**データ処理**が行われる場合は、生命に関わる利益の条件を満たさないことがある。

人道団体は、**個人データ処理**の法的根拠として使用するために、想定される**人工知能**ベースの活動と十分に密接に関連する重要な公共の利益の存在について慎重に検討することが望ましい。公益は、**人道支援**を実行する権限が国内法、地域法、または国際法において確立されているが、**同意**が得られておらず、また生命に関わる利益を法的根拠として想起するような緊急事態も存在しない場合には、**データ処理**の適切な法的根拠となり得る。

人道団体は、**個人データ処理**の法的根拠としての公益は、国内法または国際法の下での当該団体の職務権限に固有のものであるため、移転不可能であることに留意することが望ましい。**人工知能**の使用を含む**データ分析**を、**第三者**が当該**人道団体**に代わって行うことができる場合、または**国際的なデータ共有**に適用される条件（もしあれば）については、別途検討する必要がある。

人道団体はまた、**個人データ**が正当な利益となる場合に、**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において、**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**によって得ることができる。管理目的の**人工知能**の使用もこのカテゴリに分類される場合がある。

17.2.2 目的制限と追加処理

人工知能を人道的な目的に使用する際に特に重要な課題の一つは、人工知能が、人道団体または第三者によって別の目的で収集された既存のデータセット上で実行される可能性が非常に高いということである。したがって重要なことは、想定される分析が本来の収集目的に適合しているかどうかを判断することである。適合しているのであれば、人工知能の運用は既存の法的根拠の下で実施することができる。そうではない場合は、追加処理のための新たな法的根拠を見つけなければならない。

さらに、人工知能に目的制限の原則⁵³⁵を適用することは難しいかもしれない。それは、これらのテクノロジーは、当初予定されていなかった方法でデータを処理する能力を持っており、その性質上、予期しない、未知の新しいパターンや推論を識別するために使用されるからである。

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」について、その人物からそれ以上の情報を得ずに分析を行なったところ、ソリューションによって「性的指向、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、非常に機微性の高いさまざまな個人属性を自動的かつ正確に予測する」ことができた。⁵³⁶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コーカサス系アメリカ人の間では95%、民主党と共和党の間では85%」を正しく識別している。⁵³⁷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このような推論を独自に引き出し、

⁵³⁵ セクション2.5.2：目的制限の原則を参照

⁵³⁶ Michal KosinskiとDavid StillwellおよびThore Graepel, “Private traits and attributes are predictable from digital records of human behavior”, Proceedings of the National Academy of Sciences, Vol. 110, No. 15, 2013年3月11日, p.1: <https://doi.org/10.1073/pnas.1218772110>

⁵³⁷ 同上

開発者の意図ではない場合であっても、個人に関する機微情報を明らかにすることがある。

第2章：データ保護の基本原則でも述べているとおり、データを収集する際に**人道団体**は、データを処理する具体的な目的を決定し、明示しなければならない。そして具体的な目的は、明示的かつ合法的なものであることが望ましく、離散家族の再会、拘束されている個人の保護、法医学活動、水や住居の保護など、あらゆるものが含まれる場合がある。計画されている分析の目的は、データ収集の開始時に特定することが望ましく、新たに目的を追加する場合には、適合する目的と法的根拠という点でデータ保護要件と一致していなければならない。

人工知能は、ビッグデータ⁵³⁸と同様に、目的制限原則の適用に際しての課題となる。一方では、分析により、データ収集時に**データ処理**の具体的な目的を特定することが困難であり、もう一方では、**機械学習アルゴリズム**（その目的は必然的に特定される）は、これらの目的がどのように達成されるかについて、予測も説明もしない場合がある。いずれの場合も、**データ処理**の目的と方法に関する透明性は限定的なままになる可能性がある。

さらに、使用されるデータセットと、潜在的な望ましくない結果に関しても、目的制限の原則を考慮することが望ましい。ソリューションが、定義された目的とは相容れない方法で**個人データを処理**する可能性がある場合、または、望ましくない情報の開示や予測を行うことが予見される場合、トレーニングデータセットの選択とモデル開発の際に、これらの要素を考慮することが望ましい。

このような大規模なデータ集約型アプリケーションでは、データを最初に収集した時の目的以外の目的でデータを処理する**処理操作**を実施することが一般的である。したがって、このようなデータの二次利用の場合、**人道団体**は、追加処理が、歴史的、統計的または科学的な目的のために必要な場合を

⁵³⁸ ノルウェー王国データ保護機関、Artificial Intelligence and Privacy、ノルウェー王国データ保護機関、オスロ、2018年1月：www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf も参照

含め、データ収集時に当初指定された目的に適合しているかどうかを評価することができる。⁵³⁹

これらの処理が、データを最初に収集した目的と適合する**追加処理**と見なすことができるかどうかを判断するためには、以下の要素を考慮すべきである。

- 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性
- **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**の期待
- **個人データ**の性質
- 意図された**追加処理**が**データ主体**にもたらす可能性のある結果
- 適切な保護措置の存在

これらの要因に基づき、場合によっては、異なる人道的目的が相互に関連し両立すると見なされる可能性がある。両立性は、個々のケース状況によって異なり、新たなリスクが生じる場合、または、**データ主体**にとってのリスクが、**追加処理**による利益を上回る場合には、**追加処理**は両立しない。また、**追加処理**によって**データ主体**やその家族の利益を損う可能性がある場合、特にその**処理**が**データ主体**またはその家族の生命、インテグリティ、尊厳、心理的または身体的安全、自由またはその者の評判を脅かすリスクがある場合にも、**追加処理**は両立しない。これには、当局やまたは**第三者**による嫌がらせや迫害、司法訴追、社会的・私的問題、自由の制限、心理的苦痛などの結果が含まれる。

また、EUのGDPRのようなデータ保護規制の中には、個人データの二次利用を制限しているながら、人道的目的を含む公益を目的とした特別な適用除外を採用しているものもある。**第三者データ**が、データセットの使用における人道的価値により、最初に収集された時の目的から外れる目的で処理される場合、人道的目的によって**データ主体**が新たなリスクや危害にさらされないようにすることが望ましい。

⁵³⁹ サブセクション2.5.2.1: 追加処理を参照

例1：人道団体が、事案への対処中に収集したデータセット。例えば、援助物資を配布する目的で、その後の段階で、**人道上の緊急事態**における、避難の 패턴の理解、援助物資の事前配布を目的として使用する場合

例2：電気通信事業者が加入者に対してサービスを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、当該個人が潜在的な疾病保有者としてプロファイリングされ、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、当該加入者の同意なしに使用してはならない。このような場合、**人道団体**およびその相手方の**第三者**は、特定されたリスクを排除するために、データ集約などの緩和措置が十分効果を発揮するかどうかについて検討することが望ましい。

17.2.3 公正かつ適法な処理

- **個人データ処理**を行う場合には常にそうであるように、**個人データ**が**人工知能ソリューション**内でまたはそのトレーニングの一部として処理される場合、合法的な処理には、**処理が実施されるための正当な法的根拠**が必要となる。第3章：個人データ処理の法的根拠では、異なる法的根拠を概説し、**人道支援**における法的根拠として**同意**を用いることの限界を指摘している。**同意**の使用に対する制限、特に**同意**を撤回する可能性は、**人工知能ソリューション**の開発と改善にも関連している。⁵⁴⁰

人道団体が**人工知能**ベースの**ソリューション**を開発する場合、明確に定義された目的を達成するため、アルゴリズムのトレーニングに**個人データを処理**する適切な法的根拠を特定すべきである。システムがトレーニングされた後は、意図された目的を達成するため、新しい**個人データの処理**に対する法的根拠も定義すべきである。最後に、動的モデルの場合には、**人道団体**はモデルを改善するための**データ処理**の法的根拠も特定する必要がある。

テクノロジー企業が開発した既成の**ソリューション**を含む動的モデルでは、開発および適用中にシステムに入力されたすべてのデータが、その改善に使用

⁵⁴⁰ セクション17.2.1：個人データの処理の法的根拠も参照

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**の使用にさらなる課題をもたらす可能性がある。受益者は特定の人道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、人工知能のソリューションの開発に使用されることは想定しないかもしれないからである。⁵⁴¹ このような場合、特定された**処理**の法的根拠が**同意**であるならば、**データ主体**に対し、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、またどのように使用されるのかについて、わかりやすく説明すべきである。また、ソリューションによる**再識別**や、悪意のある攻撃時にデータがアクセスされる可能性があるという事実など、潜在的なリスクについても情報の提供が必要となる。

上記に照らして、**同意**は、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。援助や救命サービスの提供については、生命に関わる利益⁵⁴²または公共の利益⁵⁴³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の場合はそうはみなされないこともある。**人工知能**ソリューションの改善が選択した法的根拠の下で許容さ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。

公平性の原則⁵⁴⁴によって、すべての処理活動が**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ぐための措置を講じることが求められる。⁵⁴⁵ **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。⁵⁴⁶

⁵⁴¹ Future of Privacy Forum, 'The Privacy Expert's Guide to Artificial Intelligence and Machine Learning', Future of Privacy Forum, ワシントンDC、2018年10月、p.8: https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

⁵⁴² セクション3.3: 生命に関わる利益を参照

⁵⁴³ セクション3.4: 公益という重要な根拠を参照

⁵⁴⁴ セクション2.5.1: 公平性の原理と処理の適法性を参照

⁵⁴⁵ ノルウェー王国データ保護機関、Artificial Intelligence and Privacy、ノルウェー王国データ保護機関、オスロ、2018年1月、p. 16: www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

⁵⁴⁶ Sandra Wachter と Brent Mittelstadt および Chris Russell, "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI", Computer Law & Security Review, Vol. 41, 2021年、105567.

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、刑事事件における再犯率を予測する**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ほぼ2倍であると誤って評価した。⁵⁴⁷

差別的偏向のリスク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潜在的、隠されたものを含む偏見、**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。⁵⁴⁸

人工知能ソリューションにおける偏向は、バイアスのかかったデータセットをトレーニング用のデータとして使用すること、社会における構造的な偏見、または各データセットのどの機能により多くの価値を割り当てるかを開発者が決定することにより生じる可能性がある。さらに、社会に歴史的偏向がある場合、**人工知能**をトレーニングするための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。もしくは、データセットを「クリーニング」または正規化するか、偏向のない合成データなどの代替手段を採用する必要がある。

より一般的には、偏向を防ぐために、モデルは関連性があり正確なデータを用いてトレーニングされなければならない、また、どの特徴を重視すべきかを学習する必要もある。恣意的な差別の恐れがある場合には、人種的・民族的出自、政治的見解、宗教的および哲学的信念、性的指向、またはその他

⁵⁴⁷ Julia Angwin ら、“Machine Bias”, ProPublica, 2016 年 5 月 23 日 : <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

⁵⁴⁸ 欧州評議会 (CoE)、Guidelines on Artificial Intelligence and data protection | T-PD(2019)01、Guideline (Strasbourg: Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)、2019 年 1 月 25 日)、p.2: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

の差別の根拠となり得るいかなる情報については、**処理**しない、もしくは差別につながるような形で重視されないように保護するべきである。⁵⁴⁹

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、選択され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トレーニング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となる。偏向を回避するために、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**は開発者と協力して、取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可能であり、適合するようにすることが重要である。

しかし、**人工知能**モデルがそのような種類のデータを重視すべきではないという事実は、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の排除を意味するものではない。システムは、人種や性別などの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 (Proxies)」と呼ば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習できる。⁵⁵⁰ さらに、主な差別的特徴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：

前述した米国の予測ソリューションを考察した別の研究では、明らかな偏向があるにもかかわらず、約70%のケースでアルゴリズムが正確な再犯予測を行ったことが判明した。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（またはその他の排除

⁵⁴⁹ ノルウェー王国データ保護機関、Artificial Intelligence and Privacy、ノルウェー王国データ保護機関、オスロ、2018年1月、p. 16：www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

⁵⁵⁰ Centre for Information Policy Leadership、Artificial Intelligence and Data Protection in Tension、Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice、2018年10月10日、p.14：www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf

された要素)の代用を作成しないモデルを見つけるという課題」が浮き彫りになっている。⁵⁵¹

このため、トレーニングデータセットを選択する際には、**人工知能開発者は、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たとしても、使用される個人データの品質、性質、および出所を評価し、文脈から切り離されたデータを使用して文脈から切り離されたモデルを作成することによる、個人やグループに対する潜在的なリスクを考慮する必要がある。**⁵⁵² 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** (セクション17.2: データ保護基本原則の適用参照) に、「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。⁵⁵³ こ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。

また、**人工知能**は考えられ得る相関関係を扱うため、データの選択、表現、母集団推定推計に関する懸念が生じる。研究者は、使用されるデータの表現を理解し、潜在的な偏向を報告するように気をつける必要がある。さらに、不正確で偏向したデータは有害で不公平な政策決定につながる可能性があるため、政策立案者は潜在的な偏向を認識し、決定を下す際にはそれらを考慮する必要がある。

⁵⁵¹ Future of Privacy Forum, 'The Privacy Expert' s Guide to Artificial Intelligence and Machine Learning, Future of Privacy Forum, ワシントンDC, 2018年10月, p.15: https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

⁵⁵² 欧州評議会 (CoE)、Guidelines on Artificial Intelligence and data protection | T-PD(2019)01, Guideline (Strasbourg: Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 2019 年 1 月 25 日) p.2: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

⁵⁵³ Article 29 Data Protection Working Party, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 Rev.01), Guideline (Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 2018年8月22日): <https://ec.europa.eu/newsroom/article29/items/612053>

最後に、データ処理に関与するすべての従業員、請負業者、またはその他の関係者に、これらのリスクとその軽減のために取るべき手順についての教育的なトレーニングへの受講を義務付けるといふ、公平性の手続き的要素を特定することも可能である。

17.2.4 透明性

公平性と並んで、透明性はデータ保護のもう一つの重要な側面である。この原則によれば、**個人データの処理**は関連する**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、⁵⁵⁴ データが収集される際には、**個人データの処理**に関する重要な情報を**データ主体**は受け取る必要がある。⁵⁵⁵

透明性はデータ保護における公平性要件の適用にも貢献している。**処理**の複雑さを考慮すると、方法論（可能な場合はアルゴリズムを含む）についての透明性は非常に重要で、アプローチの厳密性を（**データ主体**の情報に関する権利を超えて⁵⁵⁶）独立して評価することができ、意味のあるリスク分析を実行するための主要な要件である。

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困難な可能性があるため、**人工知能**に対しては、透明性は適用が難しい原則となるかもしれない。⁵⁵⁷ さらに、多くの**機械学習**モデルには多層ネットワークが含まれており、その出力は内部プロセスの結果であり、データ科学者やソリューション設計者自身であっても、再現または数学的に理解できない場合がある。⁵⁵⁸ この多層構造は一般的に「ブラックボックス」として知られているが、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到達したのかについて理解できなくなる可能性があるからである。つまり、

⁵⁵⁴ セクション2.5.1: 公平性の原理と処理の適法性を参照

⁵⁵⁵ セクション2.10: 情報を参照

⁵⁵⁶ セクション17.3: データ主体の権利、およびセクション 17.5: 国際的なデータ共有参照

⁵⁵⁷ ノルウェー王国データ保護機関、Artificial Intelligence and Privacy、ノルウェー王国データ保護機関、オスロ、2018年1月、p. 19: www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

⁵⁵⁸ Future of Privacy Forum、The Privacy Expert's Guide to Artificial Intelligence and Machine Learning、Future of Privacy Forum、ワシントンDC、2018年10月、p.17: https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

これらのアプリケーションの機能の背後にある理由は、ほとんどの場合、人間にとって透明性がなく、理解できないものである。したがって、処理の公平性と質を評価することは困難である。

人工知能アプリケーションにおける透明性の課題に対して提案された一つの解決策は、ソリューションの背後にある論理を説明するというものである。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ということである。「解釈可能性」として知られるこのアプローチは、入力における変化が出力に与える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すべての論理を説明する必要はない。しかし、ブラックボックスの場合には、解釈可能性の達成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。他のアプローチは選択的開示または契約戦略に基づいているが、それらにもある程度の制約があるか、一般化することは困難である。⁵⁵⁹

人道団体はまた、特に意思決定の支援のために**人工知能**ソリューションを使用する場合、「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。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**に説明できる必要がある。

最後に、透明性が個人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**の透明性が悪意ある行為者による**データ処理**システムの回避を助長することで**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において注意が必要である。

⁵⁵⁹ Andrew D. Selbst および Solon Barocas, “The intuitive appeal of explainable machines”, Fordham Law Review, Vol. 87, No. 3, 2019年、2018年, pp. 1085–1140
も参照

17.2.5 データの最小化

データ最小化の原則は、**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。⁵⁶⁰ しかし、**人工知能**を使用する場合、その機能に**大規模な処理**が必要になることが多く、また、データセット内の新しいパターンや相関関係を探索することで、利用されるデータの範囲を制限することが困難になる可能性がある。⁵⁶¹ さらに、結果における潜在的な偏向を減らすために、適度に大規模で代表的なデータセットを使用して、そのようなソリューションをトレーニングすることも必要である。⁵⁶²

人工知能とデータ最小化の間のこのような緊張関係にもかかわらず、異なるニーズのバランスを取るために、さまざまなソリューションが可能である。これらについては、潜在的な制限とともに以下に説明する。

- 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、適切に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すべての統計的側面の特性と比例関係を反映している」。⁵⁶³ これは非常に有望なソリューションではあるが、⁵⁶⁴ それでも出発点として実際のデータが必要である。また、データ科学者によ

⁵⁶⁰ セクション2.5.4：データ最小化の原則参照

⁵⁶¹ Centre for Information Policy Leadership, Artificial Intelligence and Data Protection in Tension, Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, 2018年10月10日, p.14: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf

⁵⁶² 同上, p.13

⁵⁶³ Future of Privacy Forum, 'The Privacy Expert's Guide to Artificial Intelligence and Machine Learning', Future of Privacy Forum, ワシントンDC, 2018年10月, p.8: https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

⁵⁶⁴ 欧州評議会 (CoE), Artificial Intelligence and Data Protection: Challenges and Possible Remedies | T-PD(2018)09Rev

るより多くの専門知識も必要であり、複製プロセスに起因するいくつかの制限や、多くの変数や複雑な状況を考慮した場合の精度の確保に困難が生じる可能性がある。

- 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、望ましい結果が得られるまでソリューションを再度テストすることができる。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、この原則は大規模な**処理**が禁止されることを意味するものではなく、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ことを意味している。さらに、前述のように、すべての**人工知能**ソリューションが、精度を高め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であれば、ほとんどデータを用いずに**トレーニング**することができる。

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うちに、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。

最後に、**人工知能**は大規模なデータセットを必要とすることがよくある。しかし、**人道団体**によって収集されたデータセットの内容を**処理**の目的に必要な最小限に保ち、データ**処理**の目的を可能な限り具体的に定義することにより、データ戦略を慎重に設計することが常に重要である。**データ管理者**および**データ**

処理者（該当する場合）は、冗長データや限界データの存在を最小限に抑えるために、データ分析の設計を慎重に検討すべきである。⁵⁶⁵

17.2.6 データ保全

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全されるべきである。⁵⁶⁶ 初期保全期間の後、データを削除すべきかまたは目的を達成するためにより長期間保全すべきかについて、評価を行う必要がある。「適合する**追加処理**」⁵⁶⁷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、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、初期保全期間を更新し、「適合する**追加処理**」として分析を実施できる。

ただし、**人工知能**の文脈では、パフォーマンスシステムを監視し、⁵⁶⁸予期しない偏向を防ぐためにデータが使用される場合、データ保全期間を長くすることが正当化される可能性がある。例えば、モデルが偏向を示している場合、潜在的な偏向の原因を調査するために、トレーニングデータセットが利用できると役立つ場合がある。**データ管理者**は、不正確さのリスクを軽減するために、保全期間中のデータが常に更新された状態であるようにしなくてはならない。⁵⁶⁹

人工知能は人道支援分野でさまざま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、2年間のような初期保全期間を監査目的のために検討し、設定

⁵⁶⁵ 欧州評議会 (CoE)、Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data | T-PD(2017)01

⁵⁶⁶ セクション2.7：データ保全参照

⁵⁶⁷ サブセクション2.5.2.1：追加処理参照

⁵⁶⁸ Centre for Information Policy Leadership、Artificial Intelligence and Data Protection in Tension、Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice、2018 年 10 月 10 日、p.15: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf

⁵⁶⁹ Article 29 Data Protection Working Party、Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 Rev.01)、Guideline (Working Party on the Protection of Individuals with regard to the Processing of Personal Data、2018 年 8 月 22 日)、p.12: <https://ec.europa.eu/newsroom/article29/items/612053>

すべきである。この初期期間を過ぎてもなおデータが必要な場合には、**人道団体**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。

17.2.7 データセキュリティ

データセキュリティ⁵⁷⁰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、次の三つのカテゴリー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**：モデルの効用を低下させようとする攻撃
- **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しようとする攻撃

特にモデルの反転を見ると、いくつかのシステムはトレーニング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トレーニングで使用された場合、悪意のある者は、システムに何度もクエリ（Query）を実行し、入力画像を少しずつ修正しながら、その人物がトレーニングセットの一部であるとわかるのに十分な精度で顔を再構築する可能性がある。⁵⁷¹

⁵⁷⁰ 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

⁵⁷¹ Matt Fredrikson と Somesh Jha および Thomas Ristenpart, “Model inversion attacks that exploit confidence information and basic countermeasures”, in CCS’ 15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM、デンバー、コロラド州、2015年、pp.1322–1333: <https://doi.org/10.1145/2810103.2813677>

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、時には誤った分類や予測をするような有害な結果につながることもある。

これらのすべての要因は、**人工知能**が使用される状況において、不十分なデータセキュリティが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な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る。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段階にあるが、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るものの、すでに一般的になっている。差分プライバシーの使用も⁵⁷² **人工知能**ソリューションをトレーニングする際に検討されるべきである。

最後に、**人工知能**ベースのソリューション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、既存のデータセットを分析できる**処理**のアウトプットのほうが、個人やグループのプロファイリングを含む初期データセットよりも機微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。また、そのようなアウトプットが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、**人道団体**はアウトプットを保護するために、関連するリスクに適切な安全対策を実施すべきである。⁵⁷³ 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研修が不可欠である。

⁵⁷² 「差分プライバシーアルゴリズムは、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すべてノイズが多く、不正確になり、プライバシーを侵害することがはるかに困難である（実行可能であれば）」。Aaruran Elamurugaiyan, "A Brief Introduction to Differential Privacy" Medium, 2018 年 8 月 31 日: <https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b>

⁵⁷³ セクション17.2.7: 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参照

17.3 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。⁵⁷⁴ **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、個人が権利を行使できることを保証する手続とシステムを整備すべきである。同時に、本ハンドブックのセクション2.11：**データ主体**の権利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では制限される場合がある。

17.3.1 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思決定、すなわち「人間の関与なしの技術的手段による決定」⁵⁷⁵が法的効果をもたらす場合または同様に対象の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。

例：

もっぱら自動化された意思決定の例としては、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、オンラインの与信取引申請に対する自動拒否、人間の介入なしのオンライン採用の実践などがある。⁵⁷⁶

この権利の背後にある理論的根拠は、「アルゴリズムによる偏向への懸念。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、**人工知能**システムが不正確または不公正だった場合

⁵⁷⁴ セクション2.11：データ主体の権利参照

⁵⁷⁵ Article 29 Data Protection Working Party, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 Rev.01), Guideline (Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 2018 年 8 月 22 日), p.8: <https://ec.europa.eu/newsroom/article29/items/612053>

⁵⁷⁶ 同上

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。⁵⁷⁷ 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」ことを意味する。⁵⁷⁸ **人道支援**において、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が、**人工知能**ソリューションによって決定されたとしたら、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してもらう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確実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。⁵⁷⁹ これは特に重要である。なぜなら、意思決定を行う者は、数学的アルゴリズムが間違いがないとされることを根拠に、**人工知能**によるソリューションの提案に盲目的に依存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。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。⁵⁸⁰

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（上記のセクション17.2.4：透明性を参照）。意思決定者は常に、すべ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

⁵⁷⁷ Centre for Information Policy Leadership, Artificial Intelligence and Data Protection in Tension, Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, 2018 年 10 月 10 日, p.16: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te...pdf

⁵⁷⁸ Tom Willis, "Sweden: Rogue Algorithm Stops Welfare Payments for up to 70,000 Unemployed", AlgorithmWatch, 2019 年 2 月 25 日: <https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments>

⁵⁷⁹ Article 29 Data Protection Working Party, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 Rev.01), Guideline (Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 2018 年 8 月 22 日), p.21: <https://ec.europa.eu/newsroom/article29/items/612053>

⁵⁸⁰ 欧州評議会 (CoE), Artificial Intelligence and Data Protection: Challenges and Possible Remedies | T-PD(2018)09Rev

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。

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、意思決定が「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。⁵⁸¹ したがって、**人道団体**は、受益者が意思決定への人間の介入を要請する権利を有していた場合、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。⁵⁸² また、データ処理に対して意義を唱えることができる必要がある。

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、アクセス、修正、削除、異議申立に対する権利は、効果的なデータ保護方針の重要な要素と考えられている。しかし、**個人データの人工機能**ベースの**処理**には大きな課題がある。

データ主体者が自動化された意思決定に関する情報を得る権利を行使すること（透明性の原則にも関連している。セクション17.2.2：目的制限と**追加処理**を参照）は、そのようなシステムの複雑さとその運営方法を考慮すると、**人工知能**の文脈ではより困難である。したがって、**人工知能**の透明性の代替手段を探求し、最も影響力のあるシステムの主要な機能と特性を記述した公

⁵⁸¹ Article 29 Data Protection Working Party, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 Rev.01), Guideline (Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 2018年8月22日), p.27: <https://ec.europa.eu/newsroom/article29/items/612053>

⁵⁸² 同上、p.25

的記録簿の作成など、情報提供の新しい形態を検討することが重要である。影響を受ける可能性のあるグループの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。

人工知能の人道的利用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。これらの手続により、データの訂正と削除が可能になる。しかしながら、個人による一定の権利の行使は、**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、個人に害を及ぼしたり人道支援プログラムから排除されたりする可能性のある自動化された決定が個人について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人工知能のアウトプット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：

援助物資が配布される際、人工知能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。

17.4 データ管理者とデータ処理者の関係

人工知能ソリューションでは、目的と手段の定義に関連して**データ処理**を制御および監督する権限という概念を中心とした、**データ管理者**と**データ処理者**の役割に関する従来の区別があいまいになることが多い。これは主に、人工知能ソリューションの場合、プロバイダがサービスの構成と人工知能アーキテクチャに関する重要な特権を保持しているという事実によるものである。

17.4.1 説明責任

説明責任と責任義務を適切に配分するには、どの組織が実際に**データ管理者**として機能し、個人情報の管理とデータ処理の目的と手段を管理する一般的な権限を保持し、どの組織が**データ管理者**に代わって**データ処理者**となり、**個人データを処理**するかを慎重に決定することが重要である。また、複数の団体が**データ処理**の目的と手段を共同で決定し、共同**データ管理者**と見なされる可能性もある。

例1: データセットを共有し、自組織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、共同**データ管理者**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、商用サービスプロバイダに**データ分析**を委託している**人道団体**で、そのサービスプロバイダが調査結果を転送し、自身の使用のための記録を保持しない場合は、その**人道団体**は共同**データ管理者**とみなされ、サービスプロバイダは**データ処理者**とみなされる。

データ管理者と**データ処理者**は、異なる役割とそれぞれの権限範囲に応じて、**データ処理**に関して自らが採用する決定に対して説明責任を負う。しかし、上述したように、**人工知能**はブラックボックス効果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均衡の取れた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なくなくてはならない。⁵⁸³

17.4.2 責任

自動意思決定（上記を参照）は、責任の所在をめぐる特有の問題を提起する。例えば、医療では、特定の種類の癌などの病気の診断や、X線画像を解析する場合、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、

⁵⁸³ セクション2.9：説明責任の原則参照

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。⁵⁸⁴ この例のような状況では、診断に対する責任の所在が不明確になる場合がある。⁵⁸⁵ このバランスをとるために、**人道団体**は、製造物責任の考え方をアルゴリズムにまで適用することで開発企業に全責任を負わせようとする可能性がある（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）。倫理的観点からは、**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すことも重要である。

別のシナリオでは、**人工知能**システムのパフォーマンスは、不十分なスキャン技術の使用により画像ベースの診断に偏りが生じる地理的領域など、特定の文脈で利用可能なデータの品質の低さに大きく影響される可能性がある。したがって、このような場合、**人道団体**は潜在的な責任を回避するためにデータの品質を慎重に評価しなくてはならない。

データ管理計画や**DPIA**などの特定の手段の中には、**処理**に関与するさまざまな関係者の役割をより明確にできるものもある。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）のすべ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る。これらの契約は重要であり、次の理由から責任管理において主要な役割を果たすことが可能である。

- 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**、**データ処理者**または**共同管理者**のいずれの役割を果たすのかについて通知する必要がある。

⁵⁸⁴ Victor DemiauxとYacine Si Abdallah, “Comment permettre à l’ homme de garder la main? Les enjeux éthiques des algorithmes et de l’ intelligence artificielle”, フランスデータ保護局 (CNIL)、パリ、2017年12月、p.27: www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

⁵⁸⁵ 同上

- 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。

17.5 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、国際的なサービスプロバイダの存在とクラウドコンピューティングサービスの使用により、国境を越えることが頻繁にある。これは、国際的な国境を超えるデータフローに関する規定と慣行の適用につながる。⁵⁸⁶ この点において、適用される法律と管轄区域に注意を払う必要がある。

国際的なデータ共有にはいくつかのシナリオが含まれる可能性がある。

- **個人データ**は、**人道団体（データ管理者）**によって、営利団体またはその他の**人道団体**である**第三者（データ処理者）**に転送され、**人道団体**の代理としてクラウドコンピューティング・サービスプロバイダなどにより処理される。
- **個人データ**は、**人道団体**、公的機関、および／または営利団体（**共同データ管理者**）の間で共有される（共同行動におけるパートナーシップなど）。
- **個人データ**は、独自の目的のため、そのような情報を自律的に処理する他の**人道団体**、公的機関、および／または営利団体（**データ管理者**）に転送される。

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**を実施する際に**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。⁵⁸⁷ **国際的なデータ共有**の前に、移転先国の現地規制を考慮して潜在的なデータ転送リスクを評価し、**データ主体**に適切に通知することが不可欠である。潜在的なリスクのが存在する場合、契約レベル（例：契約条項、行動規範）と技術レベル（例：データ暗号化、強力な仮名化）の両方で、適切な緩和策を講じることが可能である。リスクが高く、緩和策によってもリスクを軽減できない場合は、データ共有を控えるという決定を下すべきである。⁵⁸⁸

多くの場合、**国際的なデータ共有**は第三者によるサービスの利用に関係するため、**人道団体**が**人工知能**サービスプロバイダーを採用する場合には、国境を越えたデータ転送に関するすべての関連情報を収集する必要がある。**人工知能**ソリューションを提供する企業には、**人道団体**のデータ処理の結果を利用および悪用するインセンティブがある場合もある（商業目的、プロファイリングなど）。したがって、これらの企業とのいかなる契約上の取り決めにおいても、**処理**の目的がもつば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、およびサービスプロバイダが人道的な**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。

サービスプロバイダがこの条件を尊重できるか、または尊重する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**に深刻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、高額な保険料、汚名、差別、あるいは迫害といった結果を招く場合がある。

人道団体は、暴力や紛争が発生した場合には、紛争当事者が**人工知能**に基づく分析結果にアクセスし利用することで優位性を得ようとし、それが**データ主体**の安全性や**人道支援**の中立性を損なう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**は**第三者**のソリューションに頼ることなく、独自の**人工知能**アプリケーションの開発を検討することが重要である。

⁵⁸⁷ セクション17.2.1：個人データ処理の法的根拠参照

⁵⁸⁸ 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参照

17.6 データ保護影響評価と人権影響評価

人工知能の利用は個人に重大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導入する決定を下す前に、**データ保護影響評価（Data Protection Impact Assessment：DPIA）**を実施すべきである。

DPIAには、データ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**に対する影響の識別、評価、対処が含まれる。⁵⁸⁹ 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、**個人データの処理**を含むプロジェクトまたは取り組みをプロジェクトライフサイクル全体を通して実施すべきである。

人工知能の利用における透明性の限界を考慮すると、公開されている**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促進に寄与する可能性がある。

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。⁵⁹⁰ **DPIA**は現在、多くの管轄区域や一部の人道団体で義務付けられている。

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。**DPIA**の最も関連性の高いモデルによれば、これらのリスクはプライバシーの権利とデータ保護に限定されず、自然人の権利と自由に対するリスクも含まれるべきである。⁵⁹¹ バイデザインアプローチとデータ処理関連のリスクの最小化に合わせて、**DPIA**は人工知能に基づいた作業の前に行い、データ処理作業または文脈的な要素に変更がある場合は更新する必要がある。

⁵⁸⁹ 第5章：データ保護影響評価（DPIAs）参照

⁵⁹⁰ 第5章：データ保護影響評価（DPIAs）参照

⁵⁹¹ 人道支援におけるリスクを評価するために特別に開発された評価ツールについては、以下を参照。UN Global Pulse, Risks, Harms and Benefits Assessment Tool, 2020年更新: <https://www.unglobalpulse.org/document/risks-harms-and-benefits-assessment-tool/>

DPIAでは、特定のデータ処理作業に応じて、**処理**されたデータの性質、**人工知能**アプリケーションを使用して抽出された推論、**処理**が実行される文脈などの、いくつかのリスクが考慮される。いくつかの例として、**第三者**が利用可能な状態にした匿名化されたデータまたは仮名化・集計結果が使用される場合、**人道支援**に関連する個人の**再識別**のリスク、または**人道団体**が実施した**人工知能**に基づく分析結果が、商業的な第三者および／または当局によって無関係の目的に悪用されるリスクが挙げられる。

人権保護に関するより広範な文脈で考慮されるべきリスクのさらなる例としては、以下が挙げられる。

- **データ主体**を差別や有害な結果にさらし、**人道支援**の中立性に悪影響を与える可能性がある当局または企業が、**人道団体**に対して特定のカテゴリーの個人に関する特定のパターンまたは情報について要請すること
- 暴力または紛争の状況にある当事者が、他の利害関係者に対して優位性を得るために**人工知能**ベースの分析結果にアクセスし利用することで、**データ主体**の安全と**人道支援**の中立性を損なうこと

最後に、**人道支援**における**人工知能**サービスプロバイダの役割を考慮すると、**DPIA**は、営利目的のプロバイダが、既存顧客または潜在的顧客への理解を深めるため、あるいはさらなる顧客プロファイリングのためなど、商業目的で**処理結果**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も考慮すべきである。⁵⁹²

DPIAで特定されたリスクに関して、この評価では、**データ主体**に対する潜在的な悪影響の可能性と重大度が考慮され、競合する権利と自由および法律で認められた正当な利益も評価される。この潜在的な影響の分析に基づいて、ソリューションの設計を含む特定の緩和策が採用される。これには、匿名化技術、プライバシーを強化する技術的手段、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などが含まれる。⁵⁹³

⁵⁹² 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参照

⁵⁹³ 欧州評議会 (CoE)、Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data | T-PD(2017)01

DPIA は国内法および国際法⁵⁹⁴の下で必須の要件となっているが、評価方法は主に、データ処理、タスクの割り当て、データ品質、およびデータセキュリティに重点を置いた限定的な観点を採用しており、**人工知能**アプリケーション、その多様性、複雑さによって潜在的に影響を受けるすべての人権を適切に考慮していない。しかし、国連人権高等弁務官が指摘しているように、⁵⁹⁵潜在的な悪影響に対抗するための包括的なバイデザインアプローチを用いて、**人工知能**の開発、展開、使用に人権を組み込むという、より広い視点を採用する必要がある。

17.6.1 人工知能に関する人権影響評価

このように、人権影響評価 (HRIA) は、代替設計オプション間の比較を容易にして、製品・サービスをそのライフサイクルを通して常に把握し、リスク評価と緩和ソリューションの設計に基づき反復的なアプローチを使用することで、新たな**人工知能**ソリューションの設計において最初から**人工知能**の開発者とユーザーを導くことができる。これらの理由から、HRIAは国際および地域レベルでの将来の**人工知能**規制の礎石となると考えられている。⁵⁹⁶

ただし、**人工知能**の影響に対処する場合、従来のHRIAの方法論を直接適用することはできず、**人工知能**に特有の性質を考慮して文脈化する必要がある。**人工知能**の文脈に関連してHRIAに導入された最も関連性のある

⁵⁹⁴ 欧州評議会 (CoE)、Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data、条約、Council of Europe Treaty Series (CETS) – No. 223、ストラスブール、2018年10月10日、段落10: <https://rm.coe.int/16808ac918>

⁵⁹⁵ 国連人権高等弁務官事務所 (OHCHR)、A/HRC/48/31: The Right to Privacy in the Digital Age、国連人権高等弁務官報告書、UN Doc、OHCHR、2021年9月15日、www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high.

⁵⁹⁶ 欧州評議会 (CoE) (Ad Hoc Committee on Artificial Intelligence (CAHAI)) “5th Meeting, Strasbourg, 5–7 July 2021: Abridged Meeting Report and List of Decisions, 2021年7月7日、CAHAI(2021)10: www.coe.int/en/web/artificial-intelligence/cahai-1 European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021年4月21日、COM/2021 206 final

二つの変更は、実行される評価の事前の性質と、定量化可能なリスク閾値へのより大きな重点である。前者に関しては、従来のHRIAの特徴である是正方針を中心とした事後評価とは対照的に、**人工知能**プロジェクトの設計と開発においてHRIAが果たそうとしている指導的役割により、事前のアプローチが求められている。

リスク閾値への焦点に関しては、これは**人工知能**に関する規制上の議論で浮上している要件と一致している。そこでは、さまざまなリスクレベルの定義が**人工知能**の製品およびサービスの受容性において重要であり、**人工知能**メーカー、プロバイダおよびユーザーの義務に直接影響を与える。したがって、**人工知能**の設計ガイダンスと法的遵守の両面において、リスクの範囲という観点からの評価の定量的な側面が必要となる。

ビジネス部門における自主的かつ政策に基づいた従来のHRIAの実践と異なり、HRIAが法的手段となると、それはもはやよりよいビジネス政策を提案するための単なる勧告の情報源ではなくなる。今後の**人工知能**規制では、リスクの評価と管理、および所定のリスク閾値（例：高リスク）に関連したコンプライアンス違反に対する特定の法的義務と制裁が課される可能性が高い。

17.6.2 人権影響評価：段階と手順

これらの重要な違いは評価方法論に影響を与えるが、評価手順の主な構成要素は同じであり、**DPIA** 枠組みの各段階、つまり、(i) 計画と範囲設定の段階および (ii) データ収集と分析の段階に類似している。

最初の段階では、HRIAの対象の定義を扱い、製品／サービスの主な特徴とそれが置かれる文脈を特定する。この段階で考慮すべき主な領域は三つある：(i) 製品・サービスの種類に関する説明と分析、(ii) 人権状況の分析、(iii) 関連する利害関係者の特定。

第2段階では、人権への影響を評価するため、関連する実証的証拠に焦点を当てる。ほとんどの場合、評価は測定可能な変数に基づいていないため、権利と自由への影響は必然的に専門家の評価の結果となり、専門家の意見は判例、文献、法的枠組みの知識に依存している。これが意味するところは、

予想される影響を正確に測定することはできず、提供できるのはリスクの範囲に関する評価のみであるというものである。

リスク評価手順に沿って、リスクの特定、可能性 (L)、重大度 (S) という三つの重要な要素を考慮する必要がある。一つ目に関しては、人権と自由に重点を置くことで、影響を受ける可能性のあるカテゴリーがすでに定義されており、ケース固有の分析により、使用される技術とその目的に応じて、具体的に影響を受けるカテゴリーが特定される。これは権利に基づいたモデルであるため、リスクは、物質的損害に関係なく、不法な制限や制約という観点から、権利と自由に対する侵害に関するものとする。

特定されたリスクの予想される影響は、平均的な位置付けのリスクを回避するために、4段階のスケール（低、中、高、非常に高）を使用して、予想される結果の可能性と重大度の両方を考慮することによって評価される。

可能性は、悪影響の確率とエクスポージャーの組み合わせである（表17.3）。前者は、特定のリスクの悪影響が発生する確率（表17.1）に関係し、後者はリスクにさらされる潜在的な人数（表17.2）に関係している。これらの変数はどちらも文脈に応じて評価する必要があり、関連する利害関係者の参加が役に立つ。

表 17.1 確率

低	偏見のリスクは低い、または非常に低い	1
中	リスクが発生する可能性がある	2
高	リスクが発生する可能性が高い	3
非常に高	リスクが発生する可能性が非常に高い	4

表 17.2 エクスポージャー

低	特定された権利保有者人口のうち、影響を受ける可能性がある人はほとんどいない、またはごくわずかである	1
中	特定された人口の一部が影響を受ける可能性がある	2
高	特定された人口の大部分が影響を受ける可能性がある	3
非常に高	特定された人口のほぼ全員が影響を受ける可能性がある	4

表 17.3 可能性の表 (L)

		確率			
		1	2	3	4
エクスポージャー	1	1	2	3	4
	2	2	3	5	9
	3	3	5	9	12
	4	4	7	12	15
可能性					
低					
中					
高					
非常に高					

予想される結果の深刻さ（表17.6）は、権利と自由の行使における侵害の重大さ（重大さ、表17.4）と、それを克服し悪影響を回復させるための取り組み（取り組み、表17.5）を考慮することによって推定される。

表 17.4 偏見の重大度

	偏見の重大度	
低	影響を受ける個人やグループは、権利や自由を行使する際に軽微な偏見にのみ直面する可能性がある	1
中	影響を受ける個人やグループは、権利や自由を行使する際に重大な偏見に直面する可能性がある	2
高	影響を受ける個人やグループは深刻な偏見に直面する可能性がある	3
非常に高	影響を受けた個人やグループは、深刻な、あるいは取り返しのつかない偏見に遭遇する可能性がある	4

表 17.5 偏見を克服し悪影響を逆転させるための取組み

	取組み	
低	受けた偏見は問題なく克服できる（例：情報修正に費やした時間、煩わしさ、イライラなど）	1
中	受けた偏見は、いくつかの困難（例：追加費用、恐怖、理解の欠如、ストレス、軽度の身体的疾患など）にもかかわらず、克服することができる	2
高	受けた偏見は、深刻な困難（経済的損失、物的損害、健康状態の悪化など）を伴いながらも、克服することができる	3
非常に高	受けた偏見は克服できない場合がある（例：長期にわたる精神的または身体的疾患、死など）	4

表 17.6 重大度に関する表 (S)

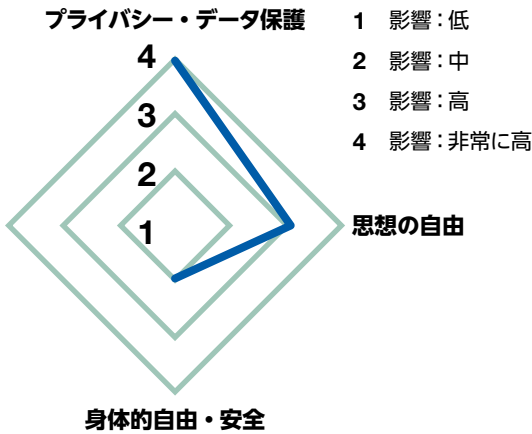
		重大度			
		1	2	3	4
取組み	1	1	2	4	6
	2	2	3	5	8
	3	3	5	8	10
	4	5	8	10	12
重大度					
低					1
中					2
高					3
非常に高					4

L 値とS 値を考慮した上で、全体的な影響は表（表 17.7）を使用して決定される。この表では、最も明るい色から最も暗い色で色分けし、全体的な影響度合いの最低から最高を表している。考慮されるすべての権利と自由について潜在的な悪影響が評価された後、全体的な影響を表す放射状グラフ（グラフ17.1）を使用して、予想される悪影響を軽減するために製品・サービスの特性を変更する際の介入の優先順位を決定できる。法的な観点からリスクを除外できる要因（例：影響を与える特定の機能に必須の性質）を考慮すべきである。

表 17.7 全体的なリスクの影響に関する表

		重大度 [影響を受けた権利／自由]			
		低	中	高	非常に高
可能性	低				
	中				
	高				
	非常に高				

グラフ 17.1. 放射状グラフ（影響）の例



予測されるリスクに対して適切な緩和策を最初に採用した後、残留リスクのレベルとその許容度に応じてさらなる評価を実施可能である。

17.7 データ保護バイデザインとデータ保護バイデフォルト

データ保護バイデザインとデータ保護バイデフォルトには、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（第6章：データ保護のための設計参照）。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、公平性、透明性
- 目的制限
- データ最小化
- 正確性
- 保全期間制限（限定保全）
- 完全性と機密性（セキュリティ）
- 説明責任

バイデザインアプローチは、**データ処理**に関する影響評価の具体的な実装も表している。通常、影響評価で特定された潜在的なリスクに対処する主な方法は、特定の緩和策の採用またはシステム設計の変更である。

データ保護バイデザインの観点から採用される対策は必然的に文脈固有のものとなるが、合成データ、**仮名化**、**匿名化**（可能な場合）、暗号化技術などのソリューションがバイデザインアプローチの構成要素となることが多い。

17.8 倫理上の問題と課題

技術が進化するスピードを考えると、法律は概して社会の大きな変化に遅れをとっている。そのため、**人工知能**のソリューションに関連する倫理的問題の中には、まだ既存の法律で対応されていないものが存在する可能性が高い。さらに、法的規定には反映されていないが、データ集約型**人工知能**システムの利用とその社会的受容性に対する特定のコミュニティのアプローチを定義する際に関連する、社会的および倫理的な問題と価値観の領域がある。

人工知能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、データ保護法およ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。ただし、重要なことは、**人道団体**はデータ処理の倫理的および社会的影響に対する潜在的な悪影響も考慮すべきだということである。⁵⁹⁷ システムの分析に関するトピックの詳細については、セクション6.3.3：目的制限の分析を参照のこと。

人工知能ツールには、差別的な偏向の可能性やシステム精度の欠如など、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方法で入手したデータを使用してシステムをトレーニングすることがある。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る場合に懸念される。

従来のデータ保護にとどまらず、より広範な関心、倫理基準および権利（無差別の権利など）を対象とするリスク評価⁵⁹⁸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、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。そのため、倫理的価値の評価は、データ保護法への遵守のみを評価するよりも、複雑で文脈に依存し、包括的なものになる。

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）⁵⁹⁹や、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 Data Protection and Privacy Commissioners：ICDPPC）の「AIにおける倫理及びデータ保護についての宣言」（Declaration on Ethics and Data Protection in

⁵⁹⁷ Alessandro Mantelero, Beyond Data Human Rights, Ethical and Social Impact Assessment in AI, 1st ed., Information Technology and Law Series, Springer, ハーグ、2022

⁵⁹⁸ 同上、第2章

⁵⁹⁹ Future of Life Institute, “Asilomar AI Principles” : <https://futureoflife.org/ai-principles>

Artificial Intelligence) などが挙げられる。⁶⁰⁰ 学者による**人工知能**に関連する倫理研究も行われており⁶⁰¹、一部の多国籍企業は独自の倫理原則を策定している。⁶⁰²

ただし、社会的評価と同様、倫理的評価はデータ保護および人権影響評価よりも複雑である。後者が明確に定義されたベンチマークを参照するのに対し、倫理的枠組みには、基礎となる価値観に関するさまざまな理論的投入やガイドラインの急増が含まれており、場合によっては「倫理洗浄」または企業価値観の反映によって部分的に影響を受けている。

したがって、専門家は、既存の倫理的および社会的価値観に照らして**人工知能**ソリューションを検出、文脈化、評価する上で重要な役割を果たす。専門家は、人権評価の場合よりもはるかに、関連するコミュニティの価値観を把握する際に決定的な役割を果たしている。これは、その価値観が文脈固有の性質を持ち、多くの場合、価値観をよりよく理解するためには権利所有者や利害関係者との積極的な対話が必要であるためである。

人工知能が与え得る影響を考慮し、**人工知能**に関連する分野では、開発者が権利に基づいた社会志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倫理委員会への関心が高まっている。⁶⁰³ そのような委員会の

600 データ保護プライバシー・コミッショナー国際会議、「AIにおける倫理及びデータ保護についての宣言」、第40回データ保護プライバシー・コミッショナー国際会議（40th International Conference of Data Protection and Privacy Commissioners）、ブリュッセル、ベルギー、2018年10月23日：http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

601 例えば、近年注目を集めている、公平性、説明責任、透明性に関するACM会議（<https://fatconference.org>）を参照

602 Marcello Ienca と Effy Vayena, “AI ethics guidelines: European and global perspectives”, Towards Regulation of AI Systems: Global Perspectives on the Development of a Legal Framework on Artificial Intelligence Systems Based on the Council of Europe’s Standards on Human Rights, Democracy and the Rule of Law, Isaac Ben Israel ら、欧州評議会（CoE）、2020年、pp.38–60：<https://edoc.coe.int/en/artificial-intelligence/9656-towards-regulation-of-ai-systems.html>
Thilo Hagendorff, “The ethics of AI ethics: An evaluation of guidelines”, Minds and Machines, Vol. 30, No. 1, 2020 年、pp.457–461: <https://doi.org/10.1007/s11023-020-09526-7>

603 欧州評議会（CoE）、Artificial Intelligence and Data Protection: Challenges and Possible Remedies | T-PD(2018)09Rev, p.16

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、領域固有の知識も不可欠である。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。

法的・倫理的基準への遵守を確実にするために、**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、次の三つの質問に答える必要がある。
 1. 実際には何をすればいいのか
 2. 何が法律で認められているのか
 3. 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
 - 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
 - この技術は、リスクの低い他の技術と比較してどのように機能するか

この点で、倫理的評価は、特に提案された**人工知能**ソリューションの受け入れ可能性に関して、**人工知能**ソリューションの設計にも影響を与える。この評価では、**人工知能**の製品・サービス自体を検証するだけでなく、特定されたニーズを満たすためのより幅広い代替可能性を検討し、必ずしも**人工知能**に基づかないソリューションも考慮する。

そのため、(**人工知能**を使わない) ゼロオプションも常に念頭におく必要がある。これは、**人工知能**の使用は合法だが倫理的には受け入れられないという場合に、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、このような不快感や不信感によって、テクノロジーを導入しないという決定が正当化される可能性がある。

付録 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 プロセスの序文と概要

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で採用された方法論（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の必要性和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説明

評価される活動の説明には、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、および、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¹ 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、**データ処理**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。

1 国際標準化機構（ISO）、“ISO/IEC 29100:2011 | Information Technology – Security Techniques – Privacy Framework”、2017年：www.iso.org/standard/45123.html

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**が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。

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、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したあと後に公表されたり、機微な情報を含む部分は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。

付録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。

- Barclays (バークレイズ)
- 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)
- Canadian Red Cross (カナダ赤十字社)
- Cash Learning (キャッシュラーニング)
- Council of Europe (欧州評議会)
- Council of the EU (欧州連合理事会)
- Dalberg Data Insights (ダルバーク・データ・インサイト)
- EFTA Surveillance Authority (欧州自由貿易連合監督局)
- Engine Room (エンジンルーム)
- European Commission, DG ECHO (欧州委員会 ECHO 総局)
- European Commission, DG Justice (欧州委員会 司法総局)
- European Data Protection Supervisor (欧州データ保護監督官)
- European UAV-Drones Area (欧州 UAV ドローン地域)
- Facebook (フェイスブック)
- Fairphone (フェアフォン)
- French Data Protection Authority (フランス共和国データ保護機関)
- 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)
- Government of Luxembourg (ルクセンブルク政府)
- GSMA (GSM アソシエーション)
- Harvard Humanitarian Initiative (ハーバード大学人道イニシアチブ)
- Human Rights Watch (ヒューマン・ライツ・ウォッチ)
- ID2020
- International Committee of the Red Cross (赤十字国際委員会)

- International Federation of the Red Cross and Red Crescent Societies（国際赤十字・赤新月社連盟）
- International Organization for Migration（国際移住機関）
- ITU（国際電気通信連合）
- KU Leuven（ルーヴェン・カトリック大学）
- MasterCard（マスターカード）
- Médecins Sans Frontières（国境なき医師団）
- Mercy Corps（マーシー・コープス）
- Microsoft（マイクロソフト）
- MIT（マサチューセッツ工科大学）
- Netherlands Red Cross（オランダ赤十字社）
- Norwegian Red Cross（ノルウェー赤十字社）
- Orange Business Services（オレンジビジネスサービス）
- Oxford University（オックスフォード大学）
- Politecnico di Torino（トリノ工科大学）
- Privacy International（プライバシーインターナショナル）
- Queen Mary University of London（クイーン・メアリー（ロンドン大学））
- 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：プライバシーバイデザイン卓越センター）
- Sensometrix（センソメトリクス）
- SES（欧州衛星社）
- Spanish Data Protection Agency（スペイン王国データ保護機関）
- Swiss Data Protection Authority（スイスデータ保護局）
- Swiss Federal Institute of Technology in Lausanne（スイス連邦工科大学ローザンヌ校）
- UN Global Pulse（国連グローバル・パルス）
- UN Office of the Special Rapporteur on the Right to Privacy（国連プライバシーの権利特別報告者事務所）
- United Nations High Commissioner for Refugees（国連難民高等弁務官事務所）

- United Nations Office for the Coordination of Humanitarian Affairs（国連人道問題調整事務所）
- University of Geneva（ジュネーブ大学）
- USAID（米国国際開発庁）
- VIVES University College（ヴィベス大学カレッジ）
- Vrije Universiteit Brussel（ブリュッセル自由大学）
- World Food Programme（国連世界食糧計画）
- World Vision International（ワールド・ビジョン・インターナショナル）
- Yale University（イェール大学）

おわりに

本書は、Massimo Marelli の編集により、赤十字国際委員会 (ICRC) が発刊した「Handbook on Data Protection in Humanitarian Action : Third Edition」を日本語に翻訳したものです。

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

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。

🌐 jp.icrc.org

📘 facebook.com/ICRC.jp

✂️ x.com/ICRC_jp

📷 instagram.com/icrc



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

shop.icrc.org

© ICRC、2025年12月

ISBN 978-2-940396-96-2