イノベーションを支える
データ倫理規範の形成

作成者：廣瀬太雅

データ倫理
――企業、公的機関、組織の為の原則とガイドライン

出典・凡例

本稿は、Tranberg, Pernille., Hasselbalch, G., Olsen, B.K. *et al.* (2018). *DATAETHICS – Principles and Guidelines for Companies, Authorities & Organisations*. DataEthics.eu. https://dataethics.eu/wp-content/uploads/Dataethics-uk.pdf の全訳である。

原語を付すために () を用いた。また、注はすべて訳者による注である。

目次

目次 1
第 1 章 序論 2
第 2 章　データ倫理の定義 3
第 3 章　データ倫理の原則 4
第 4 章　質問表 6
第 5 章　データ倫理に関する FAQ 11

本資料は，JST，RISTEX，JJPMJRX19B5 の支援を受けた研究成果の一部です。

第 1 章 序論

原文 pp. 5-6

独立系シンクタンク DataEthics.eu は、データ処理活動におけるデータ倫理の統合に役立つデータ倫理原則とガイドラインを開発した。ここでは、データ倫理に関する原則、詳細なアンケート、FAQ を紹介する。私たちは、データ倫理についても、すべて完成の前段階 (beta) であること、完璧なものはないことを認識している。重要なことは、私たちがプロセスを開始したことであり、私たちが取るすべてのステップでより良いものになるということである。

DataEhics.eu のリンク https://dataethics.eu/dataethics-principles-to-safeguard-autonomous-humans/ を明記している限り、原則とガイドラインは自由に複製することが可能である。

また、より多くの情報、ツール、インスピレーションは以下のリンク上で得られる：
www.dataethics.eu

万事うまくいくように

ペルニル・トランバーグ(Pernille Tranberg)
グリー・ハッセルバルチ(Gry Hasselbalch)
ビルギッテ・コフォッド・オルセン(Birgitte Kofod Olsen)
カトリーヌ・スーンドガード・バーン(Catrine Søndergaard Byrne)
2018 年 9 月

本資料は，JST，RISTEX，JJPMJRX19B5 の支援を受けた研究成果の一部です。

第 2 章　データ倫理の定義

（原文 pp. 7-8）

データ倫理は、データの責任ある持続可能な利活用に関するものである。それは、人と社会のために正しいことをすることだ。データプロセスは、まず、第一に人間に利益をもたらす持続可能なソリューションとして設計されなければならない。
データ倫理とは、人権と個人データ保護法の基礎となる原則と価値観を参照し、これを遵守することだ。それは、データ管理における誠実で真の透明性についての問題である。プライバシー・バイ・デザインやプライバシーを強化する製品やインフラを積極的に開発すること。誰かの個人情報を、自分が自分自身、または自分の子供の個人情報について求める扱い方でもって、扱うこと。データ倫理とは、単なる個人データ保護法の遵守を超えて、さらに一歩踏み込んだものである：したがって、すべてのデータ処理は、EU 一般データ保護規則（GDPR）、欧州連合基本権憲章、および欧州人権条約に定められた要件を最低限尊重する。

本資料は，JST，RISTEX，JJPMJRX19B5 の支援を受けた研究成果の一部です。

第 3 章　データ倫理の原則

（原文 pp. 9-12）

<中心的存在としての人間>

（原文 p. 9）

人間の利益は常に組織的、商業的な利益のよりも優先される。人はコンピュータのプロセスやソフトウェアの一部ではなく、共感性、自己決定力、予測不可能性、直観力、創造性を持ったユニークな存在であり、したがって、機械よりも高い地位を持っている。人間は中心にあり、データ処理の主な利益を得る。

<個人データ管理>

（原文 p. 10）

人間はデータを管理し、データによって権限を与えられなければならない。すべてのデータ処理において、個人の自己決定が優先されるべきであり、個人は自分について記録されたデータに積極的に関与しなければならない。個人は、データの利活用、データが処理される状況 (context)、およびデータがどのように利用されるかを、優先的にコントロールすることができる。

<透明性>

（原文 p. 10）

データ処理活動と自動化された意思決定は、当該個人にとって理解可能でなければならない。それらは真に透明性があり、説明可能でなければならない。データ処理の目的と利益は、リスクを理解する、そして社会の人々への (social)、倫理的な、また社会への (societal)、影響を理解するという観点から、個人が明確に理解していなければならない。

<説明責任 (accountability)>

（原文 p. 11）

説明責任とは、組織が思慮深く、合理的かつ体系的に個人データを使用し、保護することである。説明責任はデータ処理のあらゆる側面に不可欠であり、個人のリスクを軽減し、社会的・倫理的な影響を軽減するための努力がなされている。持続可能な個人データ

本資料は，JST，RISTEX，JJPMJRX19B5 の支援を受けた研究成果の一部です。

処理は、組織全体に組み込まれており、短期、中期、長期的に倫理的な説明責任を保証する。組織の説明責任は、下請け業者や提携先のデータ処理にも適用されるべきである。

<公平性>

（原文 pp. 11-12）

民主的なデータ処理は、データシステムが維持、再生産、または創出する社会的な権力関係を意識した上で行われる。データを処理する際には、経済的、社会的、健康の状況などにより、自己決定と支配に悪影響を及ぼしたり、差別や烙印にさらす可能性のあるプロファイリングで特に傷つきやすい脆弱な人々 (vulnerable people) に特別な注意を払う必要がある。脆弱な人々に注意を払うことは、自己学習アルゴリズムの開発におけるバイアスを減らすために積極的に取り組むことにもつながる。

第 4 章　質問表

（原文 pp. 13-20）

以下の質問は、組織におけるデータ倫理のジレンマに対処するために、FAQ と組み合わせて使用することが可能である。例えば、データ倫理ガイドラインを作成するための基礎として、以下の質問についての議論を利用することができる。

<中心的存在としての人間>

（原文 pp. 13-14）

- 利用者（データの所有者ではない）からデータを借りているという事実に基づいてデータ処理を行っているか？
- 商業的利益や組織的利益よりも、利用者の権利が優先されることを確実にしているか？
- 組織だけでなく、主に利用者が利用者自分のデータから利益を得ることを確実にしているか？
- プライバシー・バイ・デザインの原則を使用しており、かつ、それを明確かつ透明性を持って説明できるか？

<個人のデータ管理>

（原文 pp. 14-15）

デバイス上での処理

- ユーザーのデータは、可能な限り、ユーザー自身のデバイスで直接処理されるようにしているか？
- サーバーやクラウドソリューションなど、ユーザー自身のデバイス以外でデータを処理する必要がある場合、収集したデータは、個人を特定できるものではないか？

プロファイリング

- プロファイリングを使用しているか？使用している場合、ユーザーがプロファイリングの基礎となる値、ルール、入力に影響を与え、決定することを許可しているか？

本資料は，JST，RISTEX，JJPMJRX19B5 の支援を受けた研究成果の一部です。

予測

- データを使って個人レベルの行動を予測するのか、それともパターンだけを予測するのか？

<透明性>

（原文 pp. 15-16）

データの保管

- あなたのデータはどこの国に保管されているか？
- ストレージ・ソリューション・プロバイダー[1]の本社はどこにあるか？
- データの転送はEU圏外の国を経由しているか？

人工知能

- -機械学習/人工知能を使用しているか？もしそうならば、アルゴリズム、つまり基準とパラメータを説明できるか？

行動デザイン

- ユーザーの行動に影響を与えるために個人データを使用しているか？
- 個人データの使用がユーザーの行動に影響を与える可能性がある場合、それが透明であることを保証しているか？
- 設計が依存症を起こさず、そして、その結果、その人の自己決定や権限付与に影響を与えることを保証しているか？

オープンソース[2]

- 他の人がそれを使用し、おそらくそれをさらに発展させることができるように、オープンソースのソフトウェアで動作するか？

<説明責任>

（原文 pp. 17-19）

[1] ストレージ・ソリューションとは膨大な電子情報の保管・管理などを、適切な機器・サービス・プログラムの組み合わせなどによって解決する方式のこと。
[2] 公開されたソースプログラムのこと。

匿名性

- 個人データをいつ匿名化するか？
- データのエンドツーエンド暗号化[3]を使用しているか？
- メタデータ[4]の使用を最小限に抑え、それがどのように行われるかを説明しているか？

ゼロ知識

- ゼロ知識[5]を設計原理にしているか？

データの販売

- データを第三者に販売しているか？
- 個人を特定できるデータとして販売しているか？
- 集計されたレベルのパターンとしてデータを販売しているか？
- データを販売する場合、それが完全に匿名化された情報であり、個人ではなくパターンのみを記述したものであることを確認しているか？

データの共有

- 第三者のクッキーを使用しているか？
- これにはSoMe（ソーシャルメディア）のクッキーとSoMeのログインが含まれるか？
- Googleアナリティクスや同様の追跡ツールなどを使用しているか？
- 第三者のクッキーを使用している場合、ユーザーはクッキーの使用がユーザーに関するデータを第三者と共有することにつながることを十分に認識しており、それに同意しているか？

[3] エンドツーエンド暗号化とは通信を行う末端の二者のみが通信の暗号化と復号を行い、途中経路上の第三者が介入できないようにする方式のこと。

[4] メタデータとはあるデータそのものではなく、そのデータを表す属性や関連する情報を記述したデータのこと。

[5] ゼロ知識とは、ある人が，秘密の知識（パスワードなど）を所持していることをもって，本人であることを他の人に示したいが，この秘密自体は誰にも開示しなくてよい認証方式のことである。

データの付加

- ソーシャルメディアデータ、購入したデータ、ウェブスクレイピング[6]などの外部データなどをデータに付加しているか？
- この付加は、ユーザーに応じて、あるいはユーザーと協力して行われているか？

組織的固定化

- データの倫理的管理を担当する個人または部署があるか？
- データ倫理を伴う作業が組織にどのように組み込まれているか？
- データ倫理ガイドラインが尊重されていることをどのように確認しているか？

外部の管理

- データの処理は、独立した第三者による監査を受けることができるか？
- 下請業者や提携先にデータ倫理を要求し、管理しているか？

<公平性>

（原文 pp. 19-20）

公開されたプラットフォーム[7]

- 公開されたプラットフォームでユーザーとの対話を行っているか？
- プラットフォームを利用するためのガイドラインがあるか？
- 機密性の高い個人データを削除するために、プラットフォームを調整しているか？
- サービスが子供に提供されている場合、親の同意を確保しているか？

データの再利用

- データはアルゴリズムの開発や訓練に使われているか？
- データの利用が差別につながらないことを保証しているか？
- データの利用が個人の脆弱性を露呈しないことを保証しているか？

[6] ウェブスクレイピングとは、ウェブサイトから情報を抽出するコンピューターソフトウェア技術のこと。

[7] IT 用語では、プラットフォームとはソフトウェアをうごかすための基盤のことを言い、具体例を挙げると、アプリケーションにとってのプラットフォームは OS である。

人工知能

- 人工知能/機械学習の利用が個人の利益になるようにし、個人に物理的、心理的、社会的、金銭的な害を与えないようにしているか？

第 5 章　データ倫理に関する FAQ

（原文 pp. 21-38）

データ倫理に関するよくある質問をアルファベット順にまとめた。

当事者の参加 (Active Party)

当事者の参加とはどういうことか？

医師が患者の日誌にあなたについて何かを書いたり、教師があなたの子供について何かを記録したり、親としてのあなたについて何かを記録したりしていて、彼らが問題のニュアンスを考慮していないとあなたが考えている場合、あなたはあなたのデータにアクセスできる誰もが見ることができる追加の情報を投稿することができる。または保険会社は、あなたのデータに基づいて彼らが到達した結論についてコメントするためのアクセス権を与える。

匿名化

倫理的に責任のある匿名化 (anonymization) とは？

偽名化 (pseudonymization) とは、ある情報が関係する個人を直接見ることができないことを意味するが、個人の身元を確認する機会はある。匿名化はその一歩先を行くものである。誰も個人の身元を再現することはできない。個人データの匿名化と同様に、偽名化においても、これを文書化し、第三者が内部の装置を検査し、その事実を検証し、場合によっては証明することが重要である。現在、このサービスを提供している外部の第三者は多くはないが、重要な一歩となるであろう。“外部の管理”を参照のこと。

人工知能（AI）

AI を管理するにはどうすればいいか？

それは、人間の管理を確実にすることである。デンマーク工科大学の応用数学・コンピュータサイエンス学科は、いくつかの細かい「安全な AI（以下、セーフ AI とする）」の原則を策定した。

- セーフ AI は安全である：テストと検証に合格し、組織的な攻撃や専門家の攻撃に対して堅牢である
- セーフ AI は自意識をもつ：自分の役割や不確実性を理解し、例えば行動を拒否することができる

本資料は，JST，RISTEX，JJPMJRX19B5 の支援を受けた研究成果の一部です。

- セーフ AI は秘密を守ることができる：設計により (by design) プライバシー保護とプライバシーは、内蔵されている
- セーフ AI はよく定義された価値観を持っている: 固定観念、偏見が取り除かれ、感情を理解する
- セーフ AI は人と上手く付き合える：社会的な関係性を理解し、ユーザーの知識やスキルを理解する
- 安全な AI は力を理解している：データと関連する行動の背景とその結果を理解している
- 安全な AI は文書化されている：透明性があり、隠し立てをせず、説明する権利を提供している
- 安全な AI はオープンソースである: メソッド、コード、テスト結果は誰でも利用できる。

出典：ラース・カイ・ハンセン教授、DTU コンピュート

行動デザイン

データ倫理の観点から見た行動デザインとは？

ユーザーの行動に影響を与えるための個人データの使用は、ユーザーのコントロールが中心ではない場合には操作的なものになる可能性があるが、そのデザインは主に依存性を生み出したり、サービスの利用やユーザー数を増やしたり、あるいは単に売上を上げるために開発されているものである。行動デザインは透明でなければならず、かつ差別的な効果や中毒性を持たないことを目的とすべきである。個人に権限を与え、自己決定を維持できるようにしなければならない。

バイアス

設計におけるバイアスとはなにか？

バイアスとは、内蔵された偏見や負の固定観念のことである。バイアスは、自己学習アルゴリズムを開発するために使用される過去のデータである訓練データに発生することがある。また、バイアスは、例えば母集団で識別するような方法で人を分類し、ラベリングすることができるアルゴリズムの設計にも発生することがある。バイアスは、特に、データの手作業での並び換えやクリーンアップによって低減することができる。また、アルゴリズムが説明され、解釈され、監査に開放されていることを確認することによっても、バイアスは減少させることができる。例えば、自己学習アルゴリズムによって判定された最初の美人コンテストの優勝者は、事実上すべて白人であった、というのもアルゴリズムは主

に白人の画像で訓練されていたからである。バイアスは、他の人種の画像が多く含まれていない訓練データにあった。

説明責任

説明責任とは何か？

アルゴリズムは、個人が理解できるように説明されなければならない。アルゴリズムは、データ処理に関する基本的な情報を提供するだけでなく、文書化されていなければならず、例えば信用格付け、保険料、社会的利益の配分などに関する決定の基準やパラメータを含め、アルゴリズムの決定がどのように行われたかを説明することができなければならない。

データアクティベーション

データアクティベーションとは何か？

GDPR は、個人が自分のデータをコントロールする権利と、ユーザーの要求に応じてデータを簡単に転送できる「ポータビリティ」（移植可能性とも）の権利を与えている。しかし、長期的には個人のデータ管理だけでは十分ではなく、個人は自分のデータを有効化し、財政や健康、日常生活を豊かにするために活用する権限を与えられることがますます必要になっている。これは、個人が自分のデータを有効化できるような新しいサービスを提供する企業や機関にとっても有益なものとなるでしょう。

データの付加

ウェブスクレイピングとは何か、倫理的に責任を負うことができるか？

ソーシャルメディアの公開セクションを含むウェブサイトからのウェブスクレイピングでデータを付加することは可能か？しかし、データが公開されているにもかかわらず、倫理的な意味合いがあるため、論争になっている。したがって、ウェブスクレイピングがユーザーの要求に応じたもので、かつユーザーのインフォームドコンセントで行われることを忘れないようにすること。

データの共有

第三者のクッキーを使用することが非倫理的なのはどのような場合か？

企業や組織が子供やその他の弱い立場にあると考えられる人々を相手にしている場合、識別可能な機密データを第三者と共有する目的で、ウェブサイト上で第三者のクッキーを使用することは倫理的ではない。健康データや政治的意見や所属、性的志向や宗教的志向、その他の機密データを持っている場合は、ウェブサイト上で第三者のクッキーを許可することも倫理的ではない。また、公共部門が（SoMe クッキーを含めた）第三者のクッキー

を介して市民の行動に関するデータを共有することも非倫理的である。ポップアップではっきりと同意しているにもかかわらず、データ共有を理解し、暗に示されていると捉えている消費者や市民はほとんどいない。合法かもしれないが、ほとんどの人は不安を感じさせ、また度を越していると考えており、非倫理的と考えなければならない。

データの保管

データの保管が倫理的に問題となるのはどのような場合か？

EU 圏外の国にデータを保管することは合法かもしれないが、合法だからといって倫理的だとは限らない。例えば、デジタル独裁やデータ独占を実践・容認している国に拠点を置く企業とデータを保管することが倫理的に正当化されるかどうかは議論の対象となりうる。私たちは正当化されるとは思わない。しかし、常にデータをコントロールできる自社のサーバーや、EU/EEA に登録されたオフィスを持つクラウドプロバイダーにデータを保存することは、データの倫理的な扱いと考えることができる。

収益化

データ処理で金を得ることは可能か？勿論、個人のコントロールが中心にある限り、金を得ることができる。金銭的な利益は、プライバシーの権利、自己決定権、差別を受けない、もしくは烙印を押されない権利などの人権に優先することは決してできない。これは、例えば「プライバシー・バイ・デザイン」によって達成することができる。

エンドツーエンドの暗号化

暗号化とは何か？

一つは、誰も通信中にデータを傍受できないように通信を暗号化することで、もう一つは、送信者と受信者以外はコンテンツを見ることができず、通信が行われるプラットフォームを所有している会社でさえも見ることができないエンドツーエンドの暗号化である。

外部の管理

なぜ独立監査なのか？

少なくとも将来的には、データ処理が外部の独立した監査人によるレビューと検証に耐えうるものであることが重要である。環境、児童労働、IT セキュリティと同様に、ますます多くのユーザーは、企業の言っていることが実際に行うことであることを知る必要がある。今日では、ISO や EuroPriSe のような検証や認証のための信頼できる制度はほとんど存在していない。しかし、GDPR を受けて、EU が決定的なヨーロッパのプライバシー認証制度を発表したように、今後より多くの認証制度が生まれることは間違いない。

メタデータ

メタデータとは？

メタデータとは、データに関するデータ、またはデータセットやサービスに関する情報を提供することができるデータの叙述の一種である。例えば、誰が、誰に、いつ、メールを送ったかというデータがあるかもしれないが、このメタデータはメールの内容については何も示していない。メタデータが個人情報であるかどうか、すなわちメタデータに基づいて個人を特定できるかどうかについては、これまでも議論があった。しかし、メタデータがプロファイリングだけでなく、行動や興味の範囲、習慣などをマッピングするための強力なツールであることは間違いない。データ倫理的に問題となるのは、メタデータの利用について、利用者を特定して知らせるかどうか、利用者がメタデータにアクセスして見識を得られるかどうか、ということだ。

デバイス上での処理

デバイス上での処理とは？

個人データを自社のサーバーやクラウドに収集・保存するのではなく、ユーザーのデバイス上で直接データを処理することができる。Apple は Siri、安全なスイスのメッセージングアプリ Wire、安全なドイツのブラウザ Cliqz、でデバイス上での処理を行っている。サーバー上でデータを処理する必要がある場合は、データを特定できないようにして、匿名で収集する必要がある。

オープンソース

なぜオープンソースは良いことなのか？

オープンソースとは、アプリケーションのソースコードが自由に利用可能で、他社がシステムを改善、テスト、デバッグ、セキュリティの確保ができることを意味する。これは無料という意味ではないが、多くの場合は安価であり、サプライヤーから独立して開発することができる。その結果、透明性が生じる。ユーザーや第三者は、製品に何が含まれているかを正確に知ることができる。

組織的固定化

データ倫理の組織的固定化とは？

データ倫理は「一人でできる仕事」ではない。製品開発、イノベーション、マーケティングから戦略的開発に至るまで、すべてをカバーする幅広いアプローチである。したがって、データ倫理のアプローチは、最高幹部から全面的に推進され、従業員の間で価値あるものとして考えられるべきだ。それは様々な方法で実行される。例えば、アップルのプライバシーの専門家は最初からすべての製品開発チームに関与し、フランスのアクサ（保険

会社）には独立した専門家による諮問委員会があり、年に 2 回パリで会合を開き、データ倫理のジレンマについて議論している。

予測

データに基づく予測は倫理的に可能なのか？例えば、個別化された医療や治療で個人の予測を行うことは許容されるかもしれない。データ倫理の問題は、個人が見識を持ち、異議を唱えたり、断ったり、受け入れるか否かなどを選択する力を持っているかどうかに関係する。

プライバシー・バイ・デザイン

プライバシー・バイ・デザインとは何か？

プライバシー・バイ・デザイン（PbD）とは、サービスの設定がデフォルトでプライベートなものになっており、プライバシーを出発点として設計・開発されていることを意味する。最初の PbD の原則は、1990 年代にカナダの元情報・プライバシー委員であったアン・カブーキアン博士により開発され、その後も進化を続けてきた。

PbD をビジネス哲学、つまり、設計および技術開発から人材開発、CSR およびマーケティングに至るまで、企業が開始するさまざまな革新的なビジネスプロセスのための出発点がプライバシーである、デジタルビジネス開発への革新的なアプローチとして捉えることもできる。

このようにして、PbD の原則は、データ駆動型のパブリック・バイ・デフォルト（プライバシー・バイ・デザインの対義語）型の企業への代替物を確立するための一般的な指針となる。

プロファイリング

プロファイリングとは何か？

プロファイリングとは仕事、経済的状況、健康状態などその人に関するある種の個人的な側面を、予測を立てるために分析する自動的なデータ処理のことである。プロファイリングは、個人データ処理の中で最も甚だしい形態であり、データ倫理上の課題であるので、プロファイリングの法的根拠があるかどうか先ず確かめる必要がある。倫理的なデータプロファイリングは常に個人の利益のために開発され、個人はプロファイリングで使用される価値観、ルール、インプットに影響を与え、決定する機会を持つ。

データの販売

倫理的に責任を持って第三者にデータを販売することはできるか？

明確に同意を得ている場合を除き、データを第三者に販売することは違法である。
例えば、デンマーク人の大多数は、組織がデータを第三者に販売していると考えている。必ずしもそうではないかもしれないが、何を当然と思っているのかを説明することは重要である。市民のグループ内の傾向に基づく完全匿名化された情報の場合には、倫理的責任を持って第三者にデータを販売することができる。

透明性

透明性とは？
例えば、規制機関が裁判所の命令で企業のデータへのアクセスを要求した回数を共有する透明性報告書だけでは不十分である。透明性とは、自社の組織内での個人データの処理についても同様である。
透明性は、同意のための基本的な法的要件や、洞察や異議申し立ての可能性よりも一歩進んだものである。データシステムとプロセスは、個人の信頼を支え、個人に対して自分のデータ処理に異議を唱える実際の機会を与えられるように設計される。個人は、権利を失うことなくデータ処理に異議を唱えることができなければならない。

脆弱さ

データ処理に特に脆弱なのは誰か？
難民、身体障害者、精神疾患を持つ人、社会的に不利な立場にある人、失業者、受刑者など、特に脆弱な人々については、より多くのデータが収集されることが多い。例えば、デンマークの公的給付金の徴収、分配、管理を担当する機関である Udbetaling Danmark は、受給者、そのつれあい、世帯、つれあいと思われる人、に関する多くの情報を収集している。

ゼロ知識

ゼロ知識主義とは何か？
GDPR では、目的の為に必要な以上に長くデータを保存してはいけないとしている。法規制を超えて、必要な期日までにデータを削除することを選択することができるので、特に機密性の高いデータを保有することで不必要にリスクを負うことはない。これには、自動削除という方法もあるが、そもそもデータにアクセスしないという方法もある。