

AI システムにおけるデータ利用の特性と 取扱い上の留意点

2020 年 6 月

田丸健三郎¹、満塩尚史¹、柳原尚史²、高木幸一³、
西村毅¹、梅谷晃宏¹、楠正憲¹、細川努¹

要旨

AI（便宜上、本書では、深層学習を含む機械学習を「AI」と表記する）の研究が進むとともに、AI の実社会への適用についても広く検討され始めています。一方で従来のルール、ロジックを基にしたアルゴリズム実装とは異なり、AI の推論過程を論理的に人が理解できる内容で説明することは現在の技術では困難と考えられています。加えて、学習に用いたデータの品質が AI の推論結果の品質に大きな影響を与え、データの偏り、不適切なアノテーションなどが誤った推論結果となって現れます。このような特性を踏まえ、政府情報システムにおいては、公平性、安全性、透明性およびセキュリティへの一層の配慮が重要です。

本書では AI を政府情報システムまたは政府が提供するサービス等で活用する際に、リスク度に応じて考慮すべき AI の学習データに関する透明性の確保、偏り（バイアス）の排除、データ加工の来歴保管の必要性、権利関係について AI を用いたシステムに求める検討事項および考え方を記述しています。

本ディスカッションペーパーは、政府 CIO 補佐官等の有識者による検討内容を取りまとめたもので、論点整理、意見・市場動向の情報収集を通じて、オープンで活発な議論を喚起し、結果として議論の練度の向上を目的としています。そのため、ディスカッションペーパーの内容や意見は、掲載時期の検討内容であり、執筆者個人に属しており、内閣官房 情報通信技術（IT）総合戦略室、政府の公式見解を示すものではありません。

¹ 政府 CIO 補佐官

² 株式会社 Ridge-i 代表取締役社長

³ 総務省情報通信政策研究所調査研究部主任研究官

改定履歴

改定年月日	改定箇所	改定内容
2020年2月10日		初版

目次

1	はじめに	4
1.1	背景と目的	4
1.2	説明可能な AI (Explainable AI)	5
1.3	用語	6
2	想定される課題	7
2.1	変わるシステム開発	7
2.2	知的財産から見た学習データと学習済みモデルの関係	7
2.3	データ来歴と安全性と責任	9
3	AI システムの学習データの取り扱いに関する留意点	11
3.1	保証レベルによるデータ要件	11
3.2	データの権利関係	12
3.3	政府が保有するデータを AI の学習データとして使用する際の留意点	13
4	参考情報	14

1 はじめに

1.1 背景と目的

日本を含む OECD 諸国は、人工知能(AI)に関する国際的な政策ガイドラインを正式に採択するなど、AI システム (本ペーパーでは、AI を使用したシステム、サービスを便宜上「AI システム」と記載します。) の健全、安全、公正かつ信頼に足るように構築する事で合意し、AI 活用における課題の検討を加速させています。特に AI 技術の進展により、これまで実質不可能であった膨大なデータを元にしたサービスの構築、提供が可能な段階にきています。ワンスオンリー⁴を実現する上で、申請者の属性情報および問い合わせを含む過去の様々な情報をもとに関連する手続きの案内、必要とされ得る情報の提供など、これまで困難であった最適化された行政サービスの実現が期待できます。しかしながら、信頼に足る AI システムを構築する為の技術的な検討は十分になされておらず、限られた AI 研究者、研究者コミュニティのみで検討が進められている状況です。

AI が組み込まれたシステムを用いるにあたり、従来のルール、ロジックによる仕組みと異なる AI 固有の特性を理解し、健全、安全、公正かつ信頼に足る政府情報システムとするために考慮すべき事項を明らかにする事が急務です。

AI 利活用の検討としては、平成 28 年 10 月に「AI ネットワーク社会推進会議」(総務省) が設置され、AI の便益の増進及びリスクの抑制のため、利活用において留意することが期待される事項が次の 10 の原則として整理が行われ、「AI 利活用ガイドライン⁵」にて解説がなされています。

- 適正利用の原則
- 適正学習の原則
- 連携の原則
- 安全の原則
- セキュリティの原則
- プライバシーの原則
- 尊厳・自立の原則
- 公平性の原則
- 透明性の原則

⁴ デジタル手続き法案の定める三つの原則のうちの一つ。一度提出した情報は、二度提出することを不要とする。

⁵ 令和元年 8 月 9 日に AI ネットワーク社会推進会議が取りまとめた「AI 利活用ガイドライン～AI 利活用のためのプラクティカルリファレンス～」

https://www.soumu.go.jp/main_content/000637097.pdf

- アカウンタビリティの原則

特に「透明性の原則」の論点の1つとして「行政機関が利用する際の透明性の確保」が掲げられており、以下の記載があります。

行政機関が利用する際の透明性の確保

行政機関が AI を利用する場合には、法の支配、行政の透明性確保、適正手続等の要請を踏まえ、AI を利活用する際の社会的文脈に応じ、AI の判断結果の説明可能性を確保することが期待されます。なお、説明可能性を向上させるため、例えば以下の方法などが考えられます。

[説明可能性を向上させるための方法の例]

- 行政機関が利用する AI のアルゴリズムの開発・設計プロセスに、様々な社会的少数派を包摂すること（コ・デザイン）
- 学習データの構成の考え方（学習データへの包摂・排除の考え方）、アルゴリズムの設計段階において行った政策的判断、AI を導入することによる社会的影響評価、AI に対する監査方法を説明すること
- AI の判断を説明する諸要素について、開発者や AI サービスプロバイダが不開示とする範囲を限定した形で開発者や AI サービスプロバイダと契約を締結すること

本ディスカッションペーパーは、これらの原則において重要な要素である、学習に用いるデータに対する考え方を示すものです。

1.2 説明可能な AI（Explainable AI）

AI の説明可能性は、「人が理解できる方法で過程・結果を説明できる」と解する事ができますが、主に、AI の推論過程と、学習に用いたデータに対する説明可能性に大別できます。

前者について、手法や類推による説明、可視化による説明、論理的（ルール、ロジックによる）説明など目的、対象により異なります。従来のシステムではルール、ロジックを基に実装されており、システムの動作結果と基にしたルール、ロジックとは一体の関係にあり、原理的に動作結果の説明可能性が担保されています。また、機械学習手法のうち、線形回帰、ロジスティック回帰、ディシジョンツリーなども、深層学習と比較して得られた過程の説明可能性は高いと言えます。

他方、ニューラルネットワークの階層が深い深層学習アルゴリズム（CNN、LSTM、Residual Network など）を用いて学習したモデルの多くは、説明可能性が低く、結果に至るまでのプロセスを人が理解できる方法で説明、証明することは現状難しいと言えます。この課題を解決し説明可能な AI（Explainable AI）を実現するために多くの研究者が様々な取り

組み⁶をおこなっていますが、早々の結果を期待できる状況にはありません。

本ディスカッションペーパーは、学習に用いたデータの説明可能性に注目し、有識者に協力を得つつ現時点で想定可能な AI 活用における技術的な課題を検討するとともに、考慮すべき事項について記述します。

なお、前述の「AI 利活用ガイドライン」では、「透明性の原則」の論点の 1 つとして「説明可能性の確保」が掲げられていますが、そのための総合的な対策として「消費者的利用者等のニーズ、意見等も踏まえつつ、説明が不足している部分を明確にし、どのような説明が必要か、開発者とも連携して解決策を模索する」との記載があり、『「必要とする説明の明確化」と開発者による『その説明に関する技術開発』が相互に繰り返され、当該技術が広く共有されることにより、説明可能性に関する課題の本質的な解決へとつなげることが期待できる。』としています。

1.3 用語

本ディスカッションペーパーでは、AI、機械学習(Machine Learning)、深層学習(ディープラーニング・Deep Learning)、インファレンス(推論)、アノテーション等の用語を使用しています。これらの用語が広く一般的に使用されるようになるにつれて、より広い意味を持つ傾向にあり、また用語の使用者、使用場所により定義も様々です。本ディスカッションペーパーでは、便宜上これらの用語を下記の通り定義しますが、これは学術もしくは通念上の標準的な考え方を示すものではありません。

- AI - 人工知能、Artificial Intelligence (AI) という言葉が様々な場面で頻繁に使用される今日において、AI の定義は不定であり、その意味するところは使用者、使用場所により異なります。その為、分野問わず合意できる定義として説明することは非常に困難です。本ディスカッションペーパーでは、ルール、ロジックによる実装ではなく、データの特徴を学習することにより、従来の実装を代替できるだけでなく、これまで精度向上が困難であった分野で実用的な品質の実現を可能にした仕組みを AI としています。代表的な仕組みとしては、機械学習、深層学習があります。
- 機械学習 - 機械学習は、データの集合から、そのデータに内在するロジック、ルール、分類など、人間では容易に見出す事の出来ない傾向(パターン)を学習してモデル化し、目的変数への適合可能性の評価、特徴量間の傾向を算出する仕組みです。
- 深層学習 - 深層学習(ディープラーニング)は、ニューラルネットワークを多層に構成した DNN (Deep Neural Network) を中心とする機械学習手法の一つです。深層学習により、画像、自然言語など、従来の機械学習手法では難易度の高かった問題に対して高い精度を得られるようになり、様々なシステムへの活用が加速しています。今日 AI と称する多くの仕組みは、この深層学習の技術を用いたものです。
- アノテーション、ラベリング - 機械学習には、大まかに教師あり学習、教師なし学習

⁶ 代表的な取組の 1 つに米国の国防高等研究計画局 (DARPA) が進める Explainable AI (XAI) がある。

および強化学習があります。教師あり学習の場合、学習するデータに対して正解となる情報が必要となります。アノテーション、ラベリングは、データに対して正解情報を付加する作業を指します。（例：画像全体もしくは特定の箇所に対して、人・車など対象物の名前を紐づける。）

- データクレンジング – 機械学習の分析、学習に用いるデータの誤り、欠損等を修正し、機械学習アルゴリズムが使用可能な状態にする作業です。既に整えられている場合を除き、対象データを確認の結果、大幅な修正を要する場合が少なくありません。データに部分欠損がある場合には、関連する箇所の削除もしくは他の値（中央値、最小値、最大値など）を目的や用途に応じて充てます。画像の場合、ノイズの除去、輝度平均化など画像統計量の正規化、対象物のサイズの調整、不要なデータの除外など、クレンジング作業は多岐に及びます。また、今日では AI 活用における倫理、公平性、安全性およびセキュリティの点より、学習データの偏り無くして平準化する作業、不正、不適切なデータを取り除く作業をデータクレンジングに含める場合もあります。

2 想定される課題

2.1 変わるシステム開発

機械学習技術の進歩に加えて GPGPU などによる計算処理の高度化、クラウドサービスによる計算リソースの低価格化、インターネットや IoT による大規模データへの容易なアクセスにより、これまでのルール、ロジックに基づくアルゴリズム実装からデータを活用した機械学習による実装へとシステム開発手法が大きく変化してきています。この開発手法の変化（進化）により、対象とする問題によっては大きく開発コストの低減が実現されています。加えて、従来ルール、ロジックでは対応できなかった領域で機械学習による自動化、システム化の実現、IT 活用が急速に拡大しています。AI ではデータの再取得、学習および推論モデルの更新を自動化する事が可能であり、変化する環境に合わせたシステムの更新を柔軟に行える特性を持ちます。一方で AI は学習に用いたデータに深く依存するため、自動化されたシステムの更新においては先に述べた公平性、安全性等が維持されていることを保証する仕組みについても同時に考える必要があります。AI が持つ特性への適切な理解と配慮の元に、その活用を円滑に進めるための環境整備が求められています。

2.2 知的財産から見た学習データと学習済みモデルの関係

これまでデータ活用の多くはシステムの内部に組み込まれて使用されるものではなく、データに現れる様々な事象の可視化、分析、またこれらをもとにした将来予測の為の指標など、システムの外で使用されてきました。企業の売上分析、マーケティング分析などでは天候、SNS など様々な外部データが使用されています。また、製造現場においても人がデータを分析し、結果をもとに次のアクションを決定するなど用いられてきましたが、いずれもシステムの外部での活用（消費型データ活用）であり、使用とともにデータはその役割を

終えます。一方で、昨今急速に活用が進む AI（深層学習、強化学習など）で学習に用いるデータセットは、学習結果（推論モデル）へと形を変えてシステム内部に組み込まれ、再利用可能なものとして永続し、そして、オリジナルデータには無い新たな付加価値を与えて流通しつづけます。

機械学習がデータに与える付加価値は、商流、適用されるエンドサービスにより異なり、アルゴリズム特許などの技術特許に似た特性を持っていると言えます。技術特許の場合、商流、適用される最終製品の種類、価格、数量などによりライセンス価格を含むライセンス契約の内容が異なります。また、対象である特許が技術（発明）であるのに対し、機械学習に用いる学習用データは、形を変え AI として流通もしくはサービスとして提供されます。しかし、これまでのデータ流通の取引は、消費型データ利用を前提としており、データが形を変えて推論モデルとして永続し、再利用され、新たな価値創出する要素となることを想定していません。

このように、機械学習に用いる学習データに求められる保証、説明責任などは新たな課題を含んでおり、また新たなデータに対する付加価値の創造プロセスを持ち、権利の契約モデル⁷に至ってはその複雑さから整備に至っていない状況です。このような背景から、参照できる契約モデルがなく、現在 AI 研究者、知的財産・個人情報 の専門家団体⁸により AI を前提としたデータ流通促進の為の検討が進められています。

商流とライセンス（技術特許の例）

技術特許のライセンス契約および価格は、特許を適用する製品のカテゴリ、想定出荷台数、単価などにより異なり、一般的には商流のヒアリング、交渉を経て確定します。その中でも商流に関係する契約条件は非常に複雑なものとなり、技術特許のライセンス契約の場合、多くライセンス提供されている一部の技術特許を除きその多くが個別に協議、合意された内容となるのが一般的です。特に技術を適用する対象が最終製品ではなく、部品などの中間製品である場合、契約内容および価格は非常に複雑な交渉を経て合意されます。

機械学習に外部データを用いる場合、学習済みモデルの適用対象、流通先などの考慮したデータ取引が求められます。加えて、政府が保有するデータが民間企業の機械学習モデルに使用され、流通する場合などを想定し保証の範囲、権利関係など十分に配慮することが求め

⁷ 経済産業省は、民間事業者等が、データの利用等に関する契約や AI 技術を利用するソフトウェアの開発・利用に関する契約を締結する際の参考として、契約上の主な課題や論点、契約条項例、条項作成時の考慮要素等を整理した「AI・データの利用に関する契約ガイドライン」(<https://www.meti.go.jp/press/2018/06/20180615001/20180615001.html>)を作成し公開している。推論モデルが副次的な価値を持つケース、技術特許に近い特性持つことについては考慮していない。

⁸ 国内では、一般社団法人 AI データ活用コンソーシアム (<https://aidata.or.jp>) が、AI の学習用としてデータ使用することを想定したデータ流通の促進、AI 研究の加速のための調査研究、データ流通基盤の構築を行っている。

られます。

2.3 データ来歴と安全性と責任

全ての製造物には責任が伴います。製造物責任法（PL 法）は、製造物を使用して生ずる結果に対して製品サプライチェーンにおける各事業者が責任を負う法律です。従来のシステム開発では、問題が生じた際の現実的な原因究明方法として、プログラム（コード）の解析が行われます。一方で、AI の学習済みモデルを従来のルール、ロジックによるアルゴリズム実装と同様に分析、説明することについては様々な研究がなされていますが、既に述べたように人間による推論過程の解釈は困難です。このような背景から、AI 品質を担保する上で重要な要素です。学習に用いるデータセットの説明可能性を担保する方法が現実的と考えられます。

一般に学習に用いるデータセットの品質に関わる要素として次に挙げる 4 つがあります。

1. データソース

データがいつどこで誰によってどのように取得されたのか、そして取得時点での加工の有無を特定できることは、データの確からしさを明らかにする際に重要です。センサーが高度化するなか、センサーから取得したデータが RAW データ（オリジナルのデータ）か、処理されたデータなのかの判別はより困難になってきています。センサーが出力するデータは必ずしも RAW データとは限らず、データが内蔵する仕組みにより一次処理されている場合があります。デバイスによる一次処理の有無および使用されている技術は必ずしも明示されていません。また、一次処理に AI を用いている場合もあり、その場合はその AI がどのようなデータを用いて学習されたのかも検討材料に入り、複雑さが増しています。

2. アノテーション、ラベリングの定義・検証

データアノテーションとは、収集したデータに人が意味を持たせるラベル付けの作業を指します。例えば、音声データの場合、データの指定時間への文章（スクリプト）の紐づけ（start sec, length, script）、画像データであれば、画像の指定エリアへのラベル付け（x, y, width, height, label）[bounding box の場合]などです。ラベル付けの基準（アノテーションポリシー）は、AI システムが担う責任範囲を保証する上でも、特に重要です。例えば、人物検出を行う場合に、足のみが写った人を解析対象とするか、全身がすべてみえる場合対象とするか、などの詳細をアノテーションポリシーで定めることにより、AI が精度保証すべき対象物・シーンが特定されます。

3. データクレンジング

データの正規化、不正データ・ノイズの除去など、モデルの精度を向上させるためのデータ処理に加えて、過失もしくは恣意的に改変されたデータがアノテーションプロセスに混在する可能性を排除することも指します。例として、画像認識に使用する AI の学習データでナイフをペン、線路を横断歩道と、悪意ある作業者が意図的に不正なアノテーションをするケースを想定します。このようなデータを AI が学習した場合、その

AI システムは問題のある結果を引き起こす可能性があります。(後者の例だと、線路を歩行可能の場所と AI が出力してしまいます。)このようなリスクを低減するためには、適切なアノテーションポリシーを定めるだけでなく、作業者を含む作業記録の監視、アノテーション済データの検証を行う必要があります、データクレンジング行程および作業履歴などの管理の基準が明確である事が重要です。

4. データドメイン、バイアス

品質向上のためには通常多くの学習データを確保することが重要ですが、学習データの偏りは AI の品質、出力の偏りとなって現れる事が多いです。例として、人物検出の画像認識 AI において、日中の画像でのみ学習した場合は夜間では全く機能しません。このように学習データが想定用途を適切にカバーされているかを検証する必要があります。また、AI システムに公平性⁹が求められる用途では、収集するデータの量のみならず均一性が重要となります。例として、自治体が市民へのサービス提供の為のシステムに AI を用いる場合、学習に使用するデータにおける人種、年齢、地域、性別また注目する対象データに偏りが無いよう配慮することは重要です。近年少ないデータで AI の高い品質を得るための研究が進められていますが、少ないデータになると偏りの影響がより顕著になるリスクがあります。

5. AI の精度検証方法

AI が想定する利用目的を満たしているかの検証方法は、利用目的、データソース、アノテーションポリシーに深く依存し、学習データとは別途用意した検証データを用いて Confusion Matrix などにより客観的に評価します。様々な精度検証方法がありますが、精度保証にあたって重要な点は、検証データが実際に起こりうるケースをどの程度検証したか、その際の精度がどれくらいであったかを透明性高く履歴を残すことです。学習・検証時に実利用時に起こりうる全てのケースに対応したデータを網羅することは現実的に厳しいですが、公共性の高いシステムに AI を用いるためには、可能な限り十分な量と種類のデータで検証したこと、および不測のケースへの対策案を適切に講じている点について説明可能性が求められます。

このように、AI システムの品質は、学習アルゴリズムやチューニングだけでなく学習に用いるデータの品質、確からしさなど、来歴の把握と透明性の確保が重要です。適切なアノテーション作業とクレンジングを通して、不適切なデータが混入するリスクを可能な限り避けるとともに、万が一 AI の出力で不測の結果が発生した場合にも、早急に該当の不適切なデータを特定し、作業履歴を遡及する仕組みが必要です。

特に、公共性が高く、説明性が求められる政府における AI システムの活用においては、AI

⁹ 「公平性」には集団公平性・個人公平性など複数の基準があることに留意する必要があります。

システムの用途に応じたリスク評価、AI システムに求められる保証レベルに応じた学習データの評価および管理の仕組みが求められます。

3 AI システムの学習データの取り扱いに関する留意点

AI システムの用途に応じて、使用するデータの来歴、品質に求められる要件は異なります。AI システムの品質により使用者に不利益が生ずる可能性がある場合は、AI システムに求められる保証レベルに応じて AI の学習に使用するデータの来歴、所謂データの取得、アノテーション、クレンジングなどそれぞれの品質だけでなく、作業者を含む履歴の適正管理を考慮しなくてはなりません。AI システムの欠陥に起因する問題が生じた際の原因究明、説明責任の点からも学習に用いたデータの来歴情報は重要です。

3.1 保証レベルによるデータ要件

既に示したように AI システムを適用する対象、用途および想定されるリスクに応じて学習に用いるデータの来歴および品質に求められる要件は異なります。本ディスカッションペーパーでは、AI システムを使用することによるリスクレベルに応じて学習データに求められる要件を次（表 1 - システムに求められる保証レベルとデータ要件）に示します。レベル 3 については、今後の検討により分化する事が想定されることから分けて記載しています。

表 1 - システムに求められる保証レベルとデータ要件

保証レベル	レベル 1	レベル 2	レベル 3-1	レベル 3-2
データ要件	AI を使用することによる影響が想定可能、且つ使用者に限定され許容可能である。	AI を使用することによる影響が想定可能であり、補償もしくは回復可能である。	AI を使用することにより倫理、公平性に問題が生ずる場合がある。	AI を使用することにより身体、社会権に影響を及ぼす可能性がある、若しくは補償、回復が困難である。
データソース	データの取得元、取得方法、取得方法が説明可能であること。	データの取得元、取得方法、取得方法が説明可能であること。	データの取得元、取得方法、取得方法を特定可能であり、説明可能であること。	データの取得元、取得方法、取得方法を特定可能であり、説明可能であること。

アノテーション、ラベリングの定義・検証	特定要件を設けない	アノテーションの仕様、作業者、評価者、評価方法が説明可能であること。	アノテーションの仕様、作業者、評価者、使用したツールなどが特定可能であり、説明可能であること。	アノテーションの仕様、作業者、評価者、使用したツールなどが特定可能であり、説明可能であること。
データクレンジング	特定要件を設けない	クレンジングの仕様、作業者、評価者、評価方法が説明可能であること。	クレンジングの仕様、作業者、評価者、評価方法、使用したツールなどが特定可能であり、説明可能であること。	クレンジングの仕様、作業者、評価者、評価方法、使用したツールなどが特定可能であり、説明可能であること。
データドメイン、バイアス	特定要件を設けない	データの分布が評価されており、説明可能であること。	データの分布が評価されており、評価方法、評価基準が示されていること。	データの分布が評価されており、評価方法、評価基準が示されていること。
AI の精度検証方法	使用者との合意に基づく	使用者との合意に基づく	精度検証に利用したデータと方式、および不測のケースへの対策が説明可能であること。	精度検証に利用したデータと方式、および不測のケースへの対策が説明可能であること。

3.2 データの権利関係

先に示したように AI の学習に用いるデータは、これまでのデータ利用と異なり学習に用いたデータは形を変え学習済みモデルに永続します。また、学習済みモデルは、ソリューション、サービスに組み込まれ新たな価値を持つことから、次にしめす（表 2 - 政府が保有するデータと求められる手続き）新たな権利関係の整理がなされることが求められます。

表 1 - 政府が保有するデータと求められる手続き

	AI の使用範囲		
	AI の最終使用者が政府内に限定され、特定可能である	AI を政府内で共有、流通し、最終使用者が複数に及ぶ	AI を政府内および外部に共有、流通し、使用者が複数に及ぶ
学習データ（クレンジング、アノテーションを含む）に求められる手続き	AI の学習に使用したデータの権利関係が整理されており、且つ AI 固有の特性 ¹⁰ を考慮した契約手続きが行われていること。	AI の学習に使用したデータの権利関係が整理されており、且つ AI 固有の特性および適正な利用範囲を含む契約手続きが行われていること。	AI の学習に使用したデータの権利関係が整理されており、且つ来歴保証レベルに応じた管理がなされ、AI 固有の特性を前提とした契約等の適正な手続きが行われていること。

3.3 政府が保有するデータを AI の学習データとして使用する際の留意点

AI の品質は従来のルール、ロジックによる実装と異なり様々な要素を考慮しなくてはなりません。例えば、画像認識では学習に用いた画像および画像のアノテーションデータの偏りが AI 品質の偏りとして現れます。自然言語においても同様であり、学習に用いる自然言語データを収集した地域、対象とした年齢などの偏りが、言語認識、音声認識の品質の偏りとなって現れます。

一方で、AI システムの用途に関わらず高い品質、偏りの無いデータを求める事は、AI システムのコストを押し上げ、バランスの取れた持続可能なシステム構築の妨げとなります。目的、用途、適応対象などを考慮し、満たすべき AI システムの品質に応じて必要とするデータの品質を明らかにする事が重要となります。特に AI システムの品質により利用者に不利益が生ずる可能性がある場合は、AI システムに求められる保証レベルに応じて学習に使用するデータの来歴、所謂データの取得、クレンジング、アノテーションの仕様および作業者を含む履歴が適正に管理されていることが求められます。加えて、透明性、公平性、安全性およびセキュリティを考慮したデータの評価を行いそれぞれの基準、評価手法およびその結果が明らかにされている事が求められます。

AI システムの品質以外にも、知的財産および学習に用いるデータ取得における契約などについても注意が必要です。特にデータが AI の学習に用いられる事で、データが AI の学習済みモデルとして形を変え流通し、その過程により価値を変える技術特許に似た特性を持つことへの理解が必要です。政府が保有するデータを公開して外部の AI ベンダーが利活

¹⁰ AI 固有の特性については、「2.2 知的財産から見た学習データと学習済みモデルの関係」で説明するデータの永続性および永続することによる考慮事項を指している。

用する場合においても、本ディスカッションペーパーで提言した内容を示し、データが適正に利用されるよう努めることが重要です。

4 参考情報

- (1) Explainable Artificial Intelligence (XAI)
<https://www.darpa.mil/attachments/DARPA-BAA-16-53.pdf>
- (2) 一般社団法人 AI データ活用コンソーシアム
<https://aidata.or.jp/>
- (3) 総務省 AI ネットワーク社会推進会議 「AI 利活用ガイドライン」
https://www.soumu.go.jp/main_content/000637097.pdf