

**「AI ガバナンスとその評価」研究会
(第Ⅲ期) 第5回
開催報告**

1. はじめに

日本ディープラーニング協会では、人工知能（以下 AI）や Deep Learning（以下 DL）に関連する国内外の政策動向についての知見を深め、議論する場としてテーマごとに研究会を設置している。本研究会「AI ガバナンスとその評価」は多様なアクターによる管理・評価の体制の在り方を「ガバナンス」と定義し、信頼される AI 構築へ向けた AI ガバナンスの在り方をテーマとして、2020年7月から活動を継続し、今年は三期目となる。

第Ⅲ期第5回（2022年12月19日開催）では、AI ガバナンスの実現に向けた「海外の事例」をテーマに、特に米国における AI ガバナンスをめぐる動向について、平田泰一氏（Robust Intelligence Inc.）より話題提供いただいた。

2. 話題提供「米国企業における AI ガバナンスと品質管理」平田泰一氏（Robust Intelligence Inc.）

米国における AI ガバナンスをめぐる動向

AI 利用の急速な拡大に伴い、導入時におけるリスクが年々顕著になってきている（差別的予測やドリフトの発生、モデルの不正挙動、敵対的入力等）。これらは従来のソフトウェアに見られなかった新たな課題である。実際に AI 先進国の欧米では、企業価値を毀損するような大きなインシデントが発生し出している（住宅価格予測 AI にコロナ禍による大きなドリフトが発生し、誤った購入判断を行うことで巨額の損失が発生した(米国: Zillow)、資産を共有し、住所などの与信審査 AI の代表的な特徴量に違いが無いにもかかわらず、夫妻という性差によって与信額に 20 倍の差がつき当局から調査の依頼が入った(Apple Card)、等）。

こうした大規模なインシデントを受けて米国では、各省庁機関が業界に向けて、ガバナンスやリスクマネジメントの文脈で様々な法規制が整備されつつある。またそれらを受けて、ニューヨーク市やワシントン DC、カリフォルニア等の各州において、より具体的な法規制を進める動きがある。

また企業側に目を向けると、米国の大手企業では、AI の社会的責任を果たすための組織を構築し、その分野の専門人材を採用する動きが活発になっている。

企業による具体的な対応の事例（公平性への対応やモデルリスク管理の事例）

これら法規制の動きを受けた対応の事例として 2 つ挙げる。まずニューヨーク市による Artificial Intelligence Hiring Bias Law（採用 AI を使用する企業に年次のバイアス監

査実施を義務付、求人欄への監査結果の公表、採用 AI モデル使用の告知。2023 年春頃施行予定) の制定を受けて、ニューヨーク州に本社のある大手人材サービス会社等では、既に対応を進めている。使用している採用関連の AI モデルについて、バイアス監査で対象となる人種のみならず性別や居住区等の観点も追加し、積極的に公平性に関する検証・監査対応を実施している。

また、モデルリスク管理に関しては特に金融機関がその強化を進めているが、実現に向けては実務上の課題も多い。ある Fintech 企業の例では、コンプライアンス部門がモデル・リスクガイドラインに準拠してルールを作っても、回答するデータサイエンス部門が示す数学的な根拠を理解できずに、一線・二線が機能しなかった。その際の解決策として、Robust Intelligence のモデルカードという「AI モデルの通知簿」を運用に取り入れ、視覚的で要点をまとめた品質評価レポートに変更した。これにより、モデルカード上で必要な項目を管理し、その情報を介して各部門がコミュニケーションすることで適切なガバナンス体制を構築することができた。コンプライアンス実務側と DS 部門が共通言語を持たないことはガバナンス推進上の大きな課題といえるが、モデルカードを用いた運用手法は、部門横断的な施策の施行が求められるモデルリスク管理において、有用なツールの一つといえる。

日本における AI ガバナンスの在り方について

上記にみられるように、欧米では AI ガバナンスを喫緊の課題と捉え、リスク管理体制の構築を進めており、その意識は年々高まっている印象がある。

一方日本の企業については、AI の本格運用に至っていないケースが未だに多い。さらにデータサイエンティストに説明や報告などの「AI のおもり作業」に大きな管理作業負担を発生させているといった状況等が見られる。AI 導入検討の場合では、過度に保守的に AI 活用を捉える文化が、コア業務での AI 活用に踏み切れず、リスクの少ない業務でしか AI を使わないことで、本格的な AI 導入にブレーキをかけてしまっているといったことも感じている。

このような日本の現状をガバナンスの視点から考えると、「AI で何をどこまでやってもいいのか」を示す AI ガバナンスが未整備であることが、AI 導入の検討が進まない一つの要因ともいえるだろう。今後 AI ガバナンスを考える際は、「守り」の視点だけでなく「攻め」の視点でも捉えることが、日本企業の今後の AI 活用の推進に重要だと考える。

3. 研究会参加者からの主なコメント

話題提供に続いて、Robust Intelligence の Co-Founder である大柴行人氏も加わり、ディスカッションを行った。主な質疑やディスカッションの内容を以下に示す。

➤ コンプライアンス対応について横断的な機能の担い手について

- ✓ 各種法規制やガイドラインへの対応をすべて個社毎のマネジメントプロセスの中で対応するには無理があり、共通項目等を示せる部分については、企業横断的な役割の存在が必要なのではないかと考える（NIST では守秘義務に問題ないところはプレイブックやデータベースを作ろうとしている）
- ✓ 米国におけるサイバーセキュリティや情報セキュリティ分野（SOC2、ISO27001、NIPPA 等への対応）のトレンドをみると、個々の現場のエンジニアで対応が難しい部分について独立して担おうとするスタートアップ企業（e.g. Vanta、Drata）が出てきている。今後 AI 分野でもこの動きと同様に、専門ベンダーが担うことが予想される。
- ✓ このような専門企業は、技術的なチェックのみならず、監査やリーガル面を担えるチャンネルを持っており、それらを必要とする企業との橋渡しをする役割を担っている。このビジネスモデルは、プラットフォーマーとは一線を画するものだといえ、今後テクニカルな部分についてはプラットフォーマーが担う（例えばデータの自動削除など）ことは考えられても、最終的な規制やガイドラインとの兼ね合いの部分についてコーディネートする機能として、エコシステムの中で共存していくことになるだろう。

➤ AI ガバナンスに必要な組織内の推進力とモチベーション

- ✓ 米国では、ビジネス自体の AI サービス依存度が高まっているということもあり、技術投資とともに AI ガバナンスへの投資も増えているのだと思われるが、日本では投資対効果の説明が難しいといった点で、推進上の難しさがある。
- ✓ 経営層がその重要性を認識し、トップダウンで推進することが重要である。そうすることで、部門レベルの短期的な ROI に論点が集約され、推進できないというありがちな課題を解決できる可能性が高い。米国の NYC の法規制対応の事例では、まず理事レベルで対応の必要性が言われて、それが CEO からチーフデータオフィサーへ指示され、AI 倫理委員会が構成されることによって社内活動として定着するといった流れが見られた。AI に直接かかわらない高いレベルからの賛同を得ていることが強い推進力になっている。
- ✓ 米国では、予算がリスク管理部門やセキュリティ部門で組まれることも多い。AI ガバナンスの ROI の議論は、IT セキュリティ部門の方が、DS 部門よりも慣れている。
- ✓ ガバナンスを組織論やポリシー論だけでなく、現場のデータサイエンスチームが担っているモデルの性能維持や UX 向上の側面まで対策が落ちていくことを示す必要がある。そうすることで上層部の長期的目線、ガバナンス的な ROI 議論、そしてデータサイエンスチーム目線の KPI といった、関係各所からの訴求に応じる形でガバナンスの推進が実現できる。

➤ 外部的な専門要素と内部知見の融合について

- ✓ 米国では、AI ガバナンス推進人材の雇用もあるが、社内との関係各所への説得に苦労

するケースも散見される。外部とのブリッジ的な人材と、社内に精通している人材の二党体制のようなチームだとうまく機能するのかもしれない。

- ✓ ガバナンスのモデルへの適用を考えると、一度に全モデルを対象とするのは無理があり、まずはハイリスクなモデルを一つ対象にするといったことは米国でもよく取られる方法である。そのうえで全社的に展開するとき、どのような順序で横展開するかについては、組織や業務に精通した内部人材が重要な役割を果たす。

➤ **国・政府や、または大学・業界団体等に期待される役割や支援**

- ✓ 欧米と比較しても個々の企業が AI 導入に慎重な傾向のある日本において、政府によるガイドラインは、AI 推進を後押しする「攻めのガバナンス」としての役割も大きいと考える。例えば、ドメインや使い方について明確でない部分（公平性等）があるとしたとき、ガイドラインがその項目を扱うことで、ここさえ守ればよいというガードレール的な情報提供となり、企業における導入を後押しすることにもつながるのではないか。
- ✓ 大学機関や JDLA のような業界団体が担う役割として、人材育成の領域は大きい。AI ガバナンスの重要性を育成プログラムや検定の中で取り上げることで意識を醸成することが、産業全体として必要なキャリアパスや人材流動の方向性を示すことにつながる。
- ✓ 業界として政府に働きかけをするための企業の調整役やまとめ役としての機能もありうる。またその前段として、企業のガバナンス事例やインシデント事例を収集して示していくような活動も期待される。

以上

<(第Ⅲ期)第5回開催概要>

日時：12月19日(月) 11:00-12:00 (Zoom 開催)

内容：

・「米国企業における AI ガバナンスと品質管理」平田泰一氏 (Robust Intelligence Inc.)

・質疑・ディスカッション