2023 年 3 月
JDLA 事務局

「AI ガバナンスとその評価」研究会
（第Ⅲ期）第 6 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 6 回（2023 年 1 月 24 日開催）では、AI ガバナンスの実現に向けた「AI システム監査」をテーマに、関連する欧米の規制や標準化の動向等を踏まえながら、今後の AI 監査を考えるうえでの課題について、北村弘氏（CDLE AI リーガルグループ（日本電気））より話題提供いただいた。

2. 話題提供「AI システム監査の課題、および関連する最新動向」北村弘氏（CDLE AI リーガルグループ、日本電気株式会社）

AI システム監査に関連する最新動向

今後の AI システム監査や監査基準に影響するものとして、欧米における規制や標準化の動向をウォッチしていく必要がある。具体的に着目する動きに下記がある。（詳細は配布資料参照）

- 国際標準化：AI 監査の基になる AI システムのマネジメントシステム標準 ISO/IEC42001 の開発が急がれている。直接監査について規定する ISO/IEC42006（Information technology - Artificial intelligence - Requirements for bodies providing audit and certification of artificial intelligence management systems）の検討も進められている。また欧州の諮問研究機関である JRC（欧州委員会共同研究センター）が 2023 年 1 月 9 日に発行した報告書(AI Watch: Artificial Intelligence Standardisation Landscape Update(2023)[1])では、今後の標準化ニーズを満たすものとして、IEEE（米国電気電子学会）規格における要素を具体的に特定しており、特に IEEE P7001（現在は IEEE 7001 2021 という名称）は今後注目するべき関連情報源といえる。
- 米国 EU 貿易技術評議会(TTC)：欧州と米国が共同で取り組む動きも見られる。TTC は、信頼できる AI 及びリスク管理のための評価および測定ツールに関する共同のロードマップを示し(2022 年 12 月)、EU と米国協力のための手順を示している[2]

[1] https://publications.jrc.ec.europa.eu/repository/handle/JRC131155

[2] https://www.nist.gov/system/files/documents/2022/12/04/Joint_TTC_Roadmap_Dec2022_Final.pdf

・関連する決定や結論についてはまだ掴めていない が、欧州 AI 規制法案：欧州議会での 1 月時点の修正案の議論において、高リスク AI システムの利用者に対してヒューマンオーバーサイト(人による監視)の確保、AI 法遵守を保証するため基本的権利の影響評価などが必要になることが提案され、議論になっている。また欧州 AI 規制法案を前提とした、 欧州 PLD(製造物責任指令) の改正案において、ソフトウェアについても PLD の対象を拡大する方向で議論されている点も注目される。
・各国の動き：カナダにおける 42001 の実質的なテストランや、ドイツにおける AI Trust ラベルの構想など、各国でリードを得ようとする戦略的な動きが見られる。
・ニューヨーク市：自動雇用判断ツール（AEDT）に対してバイアス監査等を規定した法律が制定されており、この動きは今後全米に広がる可能性がある。

AI システム監査のあり方について

そもそも監査とは、自身では見えない組織のマネジメントシステムに対して、規制やガイドラインやチェックリスト等を鏡に見える化し、問題を発見するために行うものである。その基となる規制（社会システムとしてのルール）や組織のルールは、AI のように現在進行形で劇的に変化する技術に対しては、固定的な基礎の部分と、インシデント発生時の即時フィードバックシステムなどの変動部分の 2 つの組み合わせが必要になると考える。またシステム提供者のみに過度の責任を負わせるものではなく、サプライチェーンに沿った適切な説明責任の分岐点のバランスを取ることも重要である。個々の組織においては、目的志向でルール化が必要な部分の見極めを行うと同時に、社会的影響、安全、人命や人権に関わる部分には十分な注意を払う必要がある。また適正なルールか否かの判断が即座にできない場合に、継続的な見直しのフローを確保していくことが重要である。

AI システム監査に固有の課題

AI システム監査の固有の論点には、混在するステークホルダーにおいて、複雑・高度化する運用の責任分界点をどのように見極めるか（例えば、マルチエージェント化 AI について等の整理）、そもそも組織を対象とするか個別の AI システムを対象とするか、証跡の取り方はどうあるべきか、最適なナレッジマネジメントはどうあるべきか等、これまでのシステム監査と異なる様々な観点がある。また、日本がこれまで得意としてきた品質定義そのものが変わる可能性がある点にも、留意が必要である。

監査には再現性（誰が監査をしても結果が変わらない）が必要であることを踏まえると、AI システムの監査で求められるのは、学習をどのように評価するか、であり、学習で結果が変わることと誤動作で結果が変わることを識別できる必要がある。この視点で体系的に過不足のない監査を実現させるには、まだ課題が多いと認識している。

3. 研究会参加者からの主なコメント

主な質疑やディスカッションの内容を以下に示す。

- **参加型のルール形成の実際について**
  - ✓ 欧米での規制の検討に民間企業がどのように参加しているかは見えづらい。米国でも、GAFAM 以外の中小企業等の参加はいまだ課題だと認識している。スペインのサンドボックスの取り組みもまだ大手企業が主に動かしている段階で、第 2 段階で裾野を広げることになるとみている。
  - ✓ 欧州の規制法案では、中小企業や NPO とのコミュニケーションも今後デザインしていくような方向性が見られる。
  - ✓ 生成系 AI の広がりなどもあり、ユーザ側やコミュニティの使う責任という意味でも、エンドユースでの使われ方やフィードバックがますます重要になってくる。利害関係者とのコミュニケーションをどのようにデザインするかが重要になってくる。

- **AI 監査の導入へ向けたステップについて**
  - ✓ ISO/IEC42001 のテストランについて言うと、テストランが回せるある程度の規模があることは必要で、その規模の企業を産業界に偏らずに対象にしていくことになろう。
  - ✓ 例えばドイツではインダストリー4.0 の枠組みで戦略的に強化したいビジネスモデルを踏まえ、そのようなところから導入をテストするといったことも考えられる。
  - ✓ GAFAM のサービスを使っているユーザ企業がテック化して、影響力を持つようになっている事例も多くみられる。それらが監査のテストケースにもなっていく可能性がある。
  - ✓ 前述のように、従来日本が得意としてきた品質定義そのものが変わる可能性がある。最新動向をキャッチアップして、議論していく必要がある。

- **日本におけるルール作りの方向性について**
  - ✓ 日本には明確なルールが存在しなくても常識としてやらないといった、グレーゾーンへの対応が得意なように思える。AI システムは変化が激しく、全部をルール化してドキュメンテーションを必須とすると動かない。
  - ✓ 欧州は完全にハードローでいく方針。米国は、リスクマネジメントはソフトローであると位置付けつつも、人や社会をプロテクトするギャップを埋めるために、既存のハードローをベースにして不足部分をソフトローで補おうとしている面も見受けられる。
  - ✓ 日本はソフトローの方向性ではあるが、中央省庁が出すガイドラインをハードロー的に真面目に守ってしまう面がある。例えソフトローでも、イノベイションの阻害要因にならないような留意が重要になる。

- **必要なマネジメントや監査の体制について**
  - ✓ これから AI システムを導入する企業についても、必要な監査体制や要求事項が、AI

導入の障壁にならないようにする必要がある。

- ✓ 既存のガバナンスやマネジメント体制と 2 重管理にならないようにする必要がある。かつ守りのガバナンスと、イノベイションを促進する攻めのガバナンスの視点で、現場の負荷を最小にしながら監査の生産性を最大化し、過不足なく、適切な監査をしていく必要がある

➢ **AI ガバナンスに必要な人材について**

- ✓ 客観的に監査できる人材をどのように育成・確保できるのか、本当に必要な人材が十分集まるのかという懸念がある。
- ✓ AI 教育はエンジニア領域にとかく目が行きやすいが、従来型のハードウェア、ソフトウェアの勉強をしても追いつかない。システムオブシステムズ（SoS）や AI エコシステムの体系的かつ俯瞰的な学びと、それを組織に実装するマネジメントシステムの知識と AI 監査のスキルもさらに必要である。この部分の人材育成は日本の大きな課題の一つだと考えている。

以上

＜(第Ⅲ期)第 6 回開催概要＞
日時：1 月 24 日(火) 15:00-16:00 （Zoom 開催）
内容：
・「AI システム監査の課題、および関連する最新動向」北村弘氏（CDLE AI リーガルグループ、日本電気株式会社）
・質疑・ディスカッション