

経済産業省 第6回 AI原則の実践の在り方に関する検討会
議事概要

令和4年12月5日(月)
13:00～15:00
オンライン開催

■ GPAI サミット 2022 報告に関する質疑応答

- ◆ AI 原則を考える上で、多様性は重要な観点であるが、GPAI サミット 2022 では、多様性に関する議論は行われたのか。
 - GPAI サミット 2022 では、多様性についても重要な観点として位置付けられており、ダイバーシティ & インクルージョンをテーマにしたセッションのほか、AI 分野で活躍する女性のランチセッションも開催されている。

■ 民間企業における AI ガバナンスの取組（NEC 様の事例）に対する質疑応答

- ◆ リスクの大小の判断に難しさがあるとのことだが、人権リスク、経営リスク等のうち、どのような観点での判断が難しいのか。
 - 社会全体の便益と人権課題をどのように両立できるのか、あるいは、そこに人権課題が残存している場合に本来想定していた AI の目的を達成する方向で舵を切ってよいのかという難しさがあり、また、その判断を企業自身がしてよいのかということについても非常に判断が難しいと感じている。AI の利用者と開発者側で社会的なリスク認識が共有されると、より良い形で AI が実装されていくと考えている。
- ◆ AI ガバナンスに関しては、プロジェクトの規模の大小ではなく、そこで取扱っているリスクの大小を判断し、問題を特定していく必要があるが、リスクの特定において社内で工夫されていることはあるか。
 - その点については、当社も取組を進めている段階であり、難しいと感じている。例えば、社内のリスクを管理する組織と現場では、AI 倫理に関する認識に差がある可能性を認識した上で、現場で機微な情報を扱う際には、基本的には専門性の高いリスク管理部門に相談するというルールを設けて対応している。

■ ISO/IEC JTC1/SC42 における検討状況に対する質疑応答

- ◆ 標準化に向けた検討などが進むにつれて、産業界でも AI ガバナンスに対する関心が高まっているが、AI スタートアップ企業の動きも活発化しているのか。
 - AI に関するサービスを提供するスタートアップ企業も、政府や国際標準の動向を注視し、自社のサービスがどうあるべきかを軌道修正しながら対応している。スタートアップ企業も、的確

な問題意識を有していると感じている。

■ AI ガバナンス・ガイドラインに関する今後の取組の方向性等について

- ◆ 今後、AI 利活用に関するリスクとその対応についてのベストプラクティスやユースケースを事例として収集・蓄積していくことが重要であり、これが取組を促進するためのインセンティブにもつながると考えられる。事例においては、立場が異なるステークホルダー間でも認識を共有しやすいように、ステークホルダー向けの説明や情報開示等がポイントになる。特に DataOps や MLOps に取り組む際に、企画や設計の段階で何をチェックし、誰を巻き込むべきなのかという点も重要である。
- ◆ 汎用的なガイドラインから、企業の現場部門が、自部門の事業に沿った具体的なリスクを想定することは難しい場合もあるため、事例とそこから抽出される教訓や知見のようなものが整理されることを期待したい。AI 利活用のリスクに関する“判例 100 選”があるとよい。
- ◆ AI ガバナンス・ガイドラインが公表された後も、必要な手続きやルールの明確化を求める声が非常に多い。その背景には、「手続きを遵守しなければどうなるのか」というイメージの可視化と共有が図られていないという課題がある。本ガイドラインの中で、遵守しなかった際の影響や結果を具体的に示すことができれば、負のリスクを回避できるというメリットを示せるのではないか。
- ◆ 現在の AI ガバナンス・ガイドラインでは、データに関するガバナンスについて、他の資料を参照する形となっているが、実務上、AI とデータは切り離せない関係にあるため、データに関するガバナンスをどのように位置づけるかという点については、さらなる検討が必要ではないか。
- ◆ AI 利活用に関するリスクには、セキュリティから公平性まで様々なものが存在し、取扱いが比較的簡単なものと、公平性のように非常に難しいものがある。取扱いが簡単なものについては、企業内でチェックリストを作成することも可能であるが、取扱いが難しいものに関しては、チェックリスト化することは難しいと考えられる。チェックリスト化が難しい場合は、ステークホルダー別のペインを洗い出すなどの分析を行うツールを作成することなども考えられるのではないか。
- ◆ AI 利活用のリスクに関して、企業側は人権リスクよりも経営リスクを重視する傾向があり、本来取り組むべき重要な人権リスクに対応できていないことも散見される。経済産業省がサプライチェーン上の人権のガイドラインを策定したこともあり、産業界での取組は急速に進展しているが、さらに取組を推進するために、今後、人権リスクの特定や評価に関するツールが提供できるとよい。
- ◆ 人権リスクは、企業にとってイメージが難しいリスクの一つであると感じているが、AI 利活用に伴うリスクには、法的責任が発生するリーガルリスクと、市場でネガティブなリアクションを受けるマーケティングリスクの2つがあると説明すれば、経営上も重要であることが伝わりやすい。
- ◆ 産総研では、「機械学習品質マネジメントガイドライン」の策定に取り組んでいるが、AI に関する技術について 100%完全に保証することは難しい中で、何か事故が起きた場合に「どこまで取り組んでいけば許されるのか」という基準が重要となる。このような品質基準については、本検討会とも連携しながら検討していけるとよい。

- ◆ 例えば個人情報保護の分野では、ガイドライン上で明示的に禁止されていないから問題ないと思って実施したことが社会的に許容されなかったという例もある。ガイドラインによって社会的に許容される水準が形成されるわけではなく、社会的に許容される水準が予め存在する中で、やってよいこととやってはいけないことの境界も存在するという点については、改めて認識しておくことが重要である。ガイドラインさえ順守していれば問題ないという風潮が生まれないような留意も必要である。
- ◆ AI 利活用に関する許容できないリスクをルール化した場合、リソースが不足しているスタートアップのような企業にとっては対応が非常に難しくなることを懸念している。少なくとも、スタートアップにとっては、現在の AI ガバナンス・ガイドラインのように、ソフトローとしてリスクの低減策を示す方法が良いと思われる。

以上