経済産業省 第四回 AI事業者ガイドライン検討会
議事要旨

令和 6 年 12 月 20 日(金)
16:00～18:00
オンライン会議

冒頭挨拶

- 生成 AI という新しいテクノロジーを適切に社会や企業で使いこなしていくことは、特に人材不足の課題がある日本では不可欠と考えられる。
- 他方、新しいテクノロジーの導入にあたり、リスクとして利活用を躊躇する事態になりがちだが、日本の組織としてリスクを管理・低減させながら、しっかりと新技術を使いこなしていくことが重要である。
- 2024 年 4 月に AI 事業者ガイドラインを公表したが、常に状況は変わっている。年度内を目途に議論を重ね、同ガイドラインをより良いものにして、更新版を公表するべく、ご意見賜りたい。

◆ 議事(3) 全体討議

■ 観点1:AI ガバナンス・AI 安全性の充実

- **AI ガバナンスの手法**
  - 情報セキュリティガバナンス[1]の時と同様に、AI ガバナンスにおいてもベンチマークの策定が必要ではないか。
  - 公的機関が適切に AI ガバナンスを構築する必要があり、AI ガバナンスは調達により完結するのではなく、組織としてどのようにガバナンスに取り組み、どのように設計をするかが論点である。
  - 同ガイドラインは民間企業だけではなく、地方自治体も活用していると伺ったが、地方自治体等の「官」が利用する際に利用しづらいという声をしばしば聞く。アメリカ等では政府と民間でガイドラインを分けているので、日本も官公庁が行うべきガイドラインを別途で作成すべきではないか。特に AI プロキュアメント(調達)のほか、例えば採用においても公的機関の場合は公平性を担保する必要があるが、民間企業の場合は採用の自由があり、必ずしも採用は公平ではなかった部分もあるので、明確に分けるのが望ましい。⇒公的機関の AI ガバナンスについて、デジタル庁・総務省・経済産業省において、AI の政府調達利用ガイドラインの策定の検討を進めている。
  - 歴史的コンテンツを出力する際に、男女平等にしようとすると歴史的には適切でない画像となり得るように、ドメインごとに正しさの基準が異なるため、ドメインごとにテスト内容や公平性を担保することが重要となる。
- **リスク例の追加検討**
  - 近年 AI について米国では関心がフェイクニュースのみではなく、サイバーウィルスの生成や生物化学兵器の利用に移行している。日本で注視するべきか検討を

[1] https://www.meti.go.jp/policy/netsecurity/secgov-tools.html

する必要はあるものの、世界的には関心が高まっており、リスクとして記述するほうが良いのではないか。
- 個人が自身の LLM を構築する機会が増えている。今回は事業者が対象なものの、個人の利用者に対しても注意すべきところは課題としてあるのではないか。
- 開発者は技術を明らかにすること等の透明性が求められるものの、トレードオフの関係で、技術が明らかになるとハッキングができることにもなるので、どの程度の秘密を保つかも大事になる印象がある。そのバランスがガイドラインに含まれていると良いのではないか。

➢ **リスク分類・整理の方法**
- AI エージェントが注目される中、AI システムの複雑化により、どういう問題が起きているのか、リスクに対する検討が必要ではないか。
- 近年、LLM 自体（基盤）と LLM アプリケーションの論点が異なる点が顕著に表れており、課題を区別して検討することが望ましいのではないか。
- リスクを分類するのであれば、何のためのリスク分類かを考える必要があり、方針があるとよいのではないか。
- リスクの分類に関しても、事業者が対応すべきリスク等の取捨選択が必要ではないか。

■ **観点２：AI の契約に関する留意事項**

➢ **契約モデルや契約当事者の多様化**
- 生成 AI に関しては日本の事業者は主に提供者か利用者で、開発者は海外というケースが多く、日本の提供者と利用者だけが AI 事業者ガイドラインに準拠することになり、提供者が利用者と開発者の板挟みになることが起こり得る。提供者のリスクへの対処の仕方に丁寧に触れることが必要ではないか。

➢ **開発者・提供者・利用者の間における責任分界**
- 生成 AI において、開発者・提供者・利用者それぞれの責任分界として、誰がどう責任を負うかという基本的な考え方を示す必要があるのではないか。
- 開発者・提供者・利用者が責任を押しつけるのではなく、リスクと責任を切り分けていくことが肝要である。
- 誰が基本的に責任を持って対応していくのかが明確になればよく、例えば、開発者・提供者・利用者のそれぞれが契約の中で責任分担を決めていただくのがよいのではないか。

■ **観点３：事例の拡充**

➢ **コラム等の追加**
- AI 事業者ガイドラインがあることは知っているが、内容の詳細までは把握していないという大企業もあるので、ライトユーザー層に向けて分かりやすいユースケースを示すのが非常に有益ではないか。
- 事業者ごとの規模やリソースに対して、どのように対応（実施すべきこと）していくか、今後、長期的で充実すべき内容等が把握できると良いのではないか。

■ **観点４：その他**

➢ **AI 事業者ガイドラインの構成等**

- AI 事業者ガイドラインの利用促進に向け、ボリュームや UI 等の読者に対する工夫・配慮が必要ではないか。
- 本編・別添ともにボリュームが多いので、活用促進に向けては、それらに対する要約版が必要と考える。ウェブサイトではガイドラインの概要は公表されているが、現時点の概要に関して理念的なところは丁寧かつ詳細に書かれているものの、実務的に使うにはあまり具体的ではない印象がある。
- 大企業のみではなく、ライトユーザーやスタートアップ企業向けに対しては、どのように対応するべきかを検討することが必要ではないか。
- 過剰なガバナンスによるコストの肥大化やリスク分類については、現時点での設計だと毎年、ガイドラインの内容が増える総括的な設計になっているので、企業や導入者の取組難易度が上がってしまう懸念をしている。将来的には特に注力すべき基準が把握できる手法がリスク分類の中に含まれると使いやすくなると考える。
- リビングドキュメントの位置づけから、全体方針として今後どのように更新を行うのか検討が必要ではないか。

➢ **<u>他ガイドラインとの関係に関する考慮</u>**

- 産業技術総合研究所の機械学習品質マネジメントガイドラインとの連携や ISO/IEC42001 との関係等の考慮が必要ではないか。
- 欧米等の各国の制度動向も踏まえて、事業者は適切に対応しておくことが求められる。
- AI の品質に関する議論など、民間の現場の問題に対応できるとよい。

以上