経済産業省 第九回 AI事業者ガイドライン検討会
議事要旨

令和 8 年 3 月 5 日(木)
16:00～18:00
オンライン会議

冒頭挨拶

- これまでに委員から寄せられた意見を踏まえ、事務局が更新案をまとめた。委員各位の忌憚ないご意見をいただきたい。
- 近年、AI ガバナンスおよび AI セーフティの重要性は国際的に増してきており、日本が積み重ねてきたソフトローを基盤とするアジャイルガバナンスは、透明性、説明責任とイノベーションの両立の観点から、世界的な注目を集めている。
- AI の国際的な議論の場において、AI ガバナンスが AI 利用の質を高め、信頼性を国際的に示す要であることを実感している。
- 今年度最終回となる本検討会においても、AI事業者ガイドラインをより良いものとするため、委員の皆様より忌憚のないご意見をいただきたい。

◆ 全体討議

■ AI 技術の動向の反映

- 本編第 2 部「C. 共通の指針」の「5)セキュリティ確保 – ①AI システム・サービスに影響するセキュリティ対策」は、「～その時点での技術水準に照らして合理的な対策を講じる」という表現に留まっている。AI には、人が関与せずに自動で処理を実行し続けるという特性があることも踏まえ、サンドボックス化等の具体的な対策にも言及できるとよい。
- フィジカル AI において、フェールセーフの設計に関する事項を追加するのも一案である。
- AI モデルが正規の開発によるものであることを確認する真正証明や、改ざんがないことを検証するベリフィケーションに関する事項も追加するとよいのではないか。
- AI エージェントと人間の責任分界に関する基本的な考え方が提示できるとよい。
- 人間が介在する仕組みを設けることでリスクに対応できる場合もあれば、リスクの低減に資さない場合や、逆に利便性が低下する場合等、AI の導入の意味がなくなることも考え得る。そのため、より具体的な議論が予定されている来年度においては、人が介在さえすればリスク対応をしたことになるという誤解を与えないようにするべく、人間の介在が必要なケース・不要なケースを解像度高く議論できるとよい。
- AI という言葉の持つイメージは多様化しており、今回 AI エージェントの概念が加わったことにより、これに伴うベネフィットとリスク、ユースケース、さらには人間との責任分界といった問題が一層複雑化し、質的にもこれまで議論してきたものとは異なる論点が出てきてもおかしくないと考える。特に、AI エージェントが複数のシステムと連携して一連のタスクを完遂するような場面を念頭に置くと、AI の開発

者・提供者・利用者の三者の間で、どの時点の判断について誰がコントロールを及ぼすことができたのかという制御可能性の考え方を、より精緻に議論していく余地があるのではないかと考える。

■ **AI によるリスクの追加・見直し**

- 差別的出力は、社会的リスクでもあり技術的リスクでもあることから、どちらにも分類できないというのが正確ではないかと考える。その他、リスクについても見方によって社会的リスクか技術的リスクか異なるものもあるため、リスク分類については次年度以降も検討が必要だと考える。
- ここ半年から数か月の間で最も注目を集めている AI は、コード生成 AI だと考えている。AI 事業者ガイドラインでも複数の箇所でコード生成 AI に関する記述があるが、それらを一つのセクションにまとめて記載するのも一案である。コード生成 AI は IT 業界全体に与えるインパクトが大きく、かつコード生成 AI には様々なリスクがあるため、次年度以降是非検討いただきたい。
- 労働者の失業・データや利益の集中といった政策的なリスクは重要ではありつつも、一事業者が対応できるものではないと思われるため、AI 事業者ガイドラインには記載しない方がよいのではないか。仮に記載するとしても、一事業者だけで対応可能なリスクと対応が難しいリスクについて記載の仕方を変えるなどの検討が必要であり、来年度には是非この点も論点として議論すべきであると考える。

■ **主体区分の整理**

- AI 提供者からの依頼を受けて、AI 開発者が RAG の開発を担うケースもあり得る。そのようなケースにおける考え方を脚注等に記載するということも考えられる。
- 開発者と提供者の区分やデータに関する考え方の箇所など、時代に合わせて詳細化されていてよい。

■ **特定単語の整理・見直し**

- AI の定義について、現ガイドライン本編には AI の確立された定義が存在しない旨が記載されており、それ自体は事実であるが、AI 法では AI 関連技術が定義されている。法律に規定されている内容を適切に記載すべきとの方針であれば、法律の定義に即して何らかの形で追記することも一案ではないか。

■ **ユーザビリティの改善**

- 活用の手引きの中で、AI 事業者ガイドラインに技術的な記載があることに簡単に触れられているものの、どのような内容が記載されているのかまで要約して記載してはどうか。
- 研修や動画といった形での展開も良いかと思うが、そうした展開の中でも技術的なフィージビリティについて十分に意識すべきであると考えている。今後ユースケースを追加するのであれば、技術的な実現可能性の観点を意識してユースケースの選定を検討いただけるとよい。

- 企業の現場で働いている AI プロダクトの担当者においては、活用の手引きを読んだとしても何をしてよいのか・どう解釈すればよいのかが分からず、まだアクションに落とせるレベルではないのではないかという印象を受けている。
- そのため、特定のユースケースにおいて、AI 事業者ガイドラインの内容をウォークスルーできるような内容を提示することが望ましい。例えば、実際に AI 事業者ガイドラインを使った場合のロールプレイのようなものを例として想定している。ただしその場合は、当該内容を全てそのまま踏襲すればよいという訳ではないという前提を置く必要があると考えている。
- 来年度は、企業の現場で AI プロダクトの管理や開発の実務を担っている方々の意見や経験を活用の手引きに反映できるとよい。
- 活用の手引きの「AI システムとは」にて AI システムの「output」に図示されている AI のユースケースが古いのではないか。現在図示されている異常検知・需要予測といったユースケースは、機械学習モデルのユースケースであり、昨今想起されやすい AI システムのユースケースとしては、第一にコーディングの自動化が、次にバックオフィス業務の自動化が挙げられる。自動運転も想起されやすいユースケースに含まれるであろう。図示されているユースケースは、現在活用が進んでいるユースケースのひとつの要素に過ぎない。図示するユースケースを細かい粒度で捉えすぎているのではないか。
- リスクやガバナンスに関する議論が本検討会でも盛んに行われている一方、AI の活用や導入が進んでいない企業が非常に多い印象を受けている。来年度以降になるかもしれないが、このような企業における AI の活用や導入をどうすれば加速できるか、という視点での議論を増やすべきではないか。新技術の導入に向けた検証方法や新技術の業務への組み込みの考え方など、攻めの観点を踏まえたガイドラインも今後必要となると考えている。
- AI 開発者・AI 提供者よりも AI 利用者の方が層が厚い一方、AI 利用者にとって AI 事業者ガイドラインは難易度的にもボリューム的にもハードルが高いドキュメントになっている。また、AI 利用者と AI 開発者・AI 提供者ではリテラシーも大きく違う。そのため、AI 利用者向けのガイドラインは、AI 開発者・AI 提供者向けのものとは括りを変えて議論をするのがよいのではないか。一例を挙げると、活用の手引きは AI 利用者の目線に合わせるという側面が強いような印象を受けている。AI 利用者向けの文書であることを明示したうえで、AI 利用者に合わせた書き方をするとよいのではないか。
- 普及・展開の取組について、実際の効果測定を行っていくことが非常に重要であると考える。また、これまで本ガイドラインの解説動画やセミナー動画といったものが政府公式としては作成されていなかったように見受けられる。現在、あらゆる分野においてビデオ・オン・デマンド形式での研修や e ラーニング教材の活用が広がっており、民間部門における取組事例も多く見られるところ、来年度においてはそうした形での展開についてもご検討いただいてはどうか。
- 活用の手引きにおいても AI ガバナンスの構築に関する事業者の適切な取組と、個人の利用との関係について記載すると良いのではないか。現在、個人による AI の利用も非常に広がっている中で、事業者が基本理念や原則に基づいた適切な取組を行うことが、個人の適切な利用にもつながるという点を考慮し、初めて AI を導入する方にとっても、今後取組を進めるにあたっての基本的な考え方や姿勢

を明確にした上で取り組むことが必要であり、有益であると考える。可能であれば対応をお願いしたい。

- これまでに提示した活用の手引きに関するコメントは、適切な形で盛り込んでいただけたと思っている。本手引きの公表により、AI 事業者ガイドラインの理解および実務での活用が促進されることに期待する。
- 現在、企業においても統合報告書等の公開資料を動画形式にして YouTube 上で配信することにより理解の促進を図る動きが進んでいる。本ガイドラインについても同様の対応を行うことで、より一層の活用促進と理解の深化が期待できるのではないかと考えるので、次年度以降、そうした対応についてもご検討いただきたい。
- AI 開発者・AI 提供者であれば AI 事業者ガイドラインを読めるが、分量があまりに多いため一般の方やビジネスマンが読むことは難しいと考えている。企業では、AI 関連のガイドラインの内容のパワーポイント等を用いた資料により従業員向けに説明する場合があるが、そのような資料を参考にするとよいのではないか。他、東京都「文章生成 AI 利活用ガイドライン」や東京商工会議所「中小企業のための『生成 AI』活用入門ガイド」なども参考になると考えている。

■ **AI ガバナンスに関する動向の反映**

- ISO 42001 や ISO 42006 等はマネジメントレイヤー向けのドキュメントであるが、それらと AI 事業者ガイドラインとの整合性に関する質問を受ける機会が多い。また、ISO 42001 については、実際に運用することが難しく、かつ AI 事業者ガイドラインに比べて記載がより抽象的であるという印象を受けている。ISO 42001 との整合や ISO 42001 の運用に関する、開発者に向けた示唆を AI 事業者ガイドラインに記載できるとよいのではないか。来年度の検討でも差し障りない。
- 別添 7C（ワークシート）では、「ワークシート_高度な AI システムに関係する事業者」が、「ワークシート_全ての AI 関係者向けの広島プロセス国際指針」に差し替わっていると理解している。同シートにて、「高度な AI システムを開発する組織向けの広島プロセス国際行動規範」（以下、行動規範）の表記と若干のずれが見られる箇所がある。シート上の記載を、行動規範に合わせることを検討いただきたい。
- プリンシプル・コードの内容について、現在も様々な方面で議論がなされている。来年度以降はプリンシプル・コードも念頭に議論することとなると思われるが、プリンシプル・コードを踏まえた議論をする場合、プリンシプル・コードをどのように AI 事業者ガイドラインへ反映するかを考えるのではなく、独立した文書として AI 事業者ガイドラインを位置づけたうえで、必要な対応を検討するのがよいのではないか。
- 昨年から今年にかけての大きな変化は AI 法が成立・施行されたことであるが、本編「はじめに」における AI 法の施行に関する記述はやや唐突な印象がある。できれば、AI 法が成立し、同法第 13 条に基づき指針を策定することとなっており、内閣府の指針とともに AI 事業者ガイドラインが中核的な役割を担っていることを明記し、その上で本ガイドラインを読んでいただきたい旨を記載するのがよいのではないか。
- 本編「はじめに」における AI 法と AI 事業者ガイドラインとの関係に関する記載は、重要な論点であると考える。AI 法第 13 条に基づく指針においては、本ガイドライ

ンが明示的に言及されているわけではないものの、事業者が取り組むべき事項として、国際的な規範・規格及び各種ガイドライン等を活用する旨が記載されている。各種ガイドラインについては、ウェブサイト等に我が国で策定されたガイドラインとして掲載されることが想定されるところ、間接的ではあり、また罰則を伴う強制的なものではないにせよ、本ガイドラインがある種の法的な裏付けを得たとも言い得る状況にある。書きぶりについては種々の調整が必要であろうが、できる範囲で現状を記載するのが望ましいと考える。

- 来年度以降、AI 法の精神と本ガイドラインとの関係性の整理が様々な形で進められていくことが望ましい。これは法的な関係性の論理的な整理という観点もあるが、今後、例えば AI 事業者ガイドラインの 2.0 版のようなものがあり得るとすれば、一つの考え方として、AI 法に基づく指針と本ガイドラインとの内容に関する対応関係の整理といったことも視野に入ってくるであろう。我が国において現在形成されつつあるハードローとソフトローの関わりの全体像の中で、本ガイドラインの意義が来年度あたりにより一層明確化されていくことが望ましいと考える。
- AI 法と AI 事業者ガイドラインとの関係性について、AI 事業者ガイドラインを活用する方々がより具体的に理解できるよう整理していくべきではないかと考える。
- 「Blueprint for an AI Bill of Rights」はトランプ政権によって有効でなくなったと認識している。別添 9 への掲載是非について検討いただければ。
- 「Artificial Intelligence Risk Management Framework (AI RMF 1.0)」とあわせて、「NIST AI RMF Playbook」も別添 9 に掲載してもよいのではないか。
- 別添 9 に ISO を追加してはどうか。別添 9 のタイトルは「海外ガイドライン等の参照先」となっており、『等』という文言が含まれているため、追加に問題はないと考えている。
- 「Artificial Intelligence Act」とあわせて、「The General-Purpose AI Code of Practice」(以下、行動規範)も別添 9 に掲載してもよいのではないか。ただし、行動規範は汎用 AI という非常に限られた AI に適用されるものだが、別添 9 へ掲載されることで、行動規範が全ての AI に適用されるという誤解を与えてしまう可能性もある。この可能性が懸念される場合は、掲載を見送ることも一案である。
- 「AI 利活用における民事責任の解釈適用に関する手引き(案)」(以下、民事責任の解釈適用手引き)に対するパブコメの募集が 2026 年 2 月に開始された。AI 事業者ガイドラインでフィジカル AI を取り上げることも踏まえ、民事責任の解釈適用手引きに触れてもよいのではないか。民事責任の解釈適用手引きの最終版の公開時期が未定であるなどの事情も鑑み、今年度中の検討が難しい場合は、次年度以降の検討でも差し障りない。
- AISI から公開された「Chief AI Officer (CAIO) ガイドブック(案)」・「CAIO 設置・AI ガバナンス実務マニュアル(案)」でも AI ガバナンスについて言及がされていると理解している。これらの文書を AI 事業者ガイドラインで参照してもよいのではないか。

■ その他

- 「はじめに」の記述について、ガイドライン策定から 2 年が経過し状況が大きく変化していることを踏まえ、今回でなくとも次回の更新以降で、過去の経緯は参考資料に移すなどしてはどうか。そして今回が 2 回目の更新となること等を明示し、継

続的にバージョンアップしているというストーリーを強調する書きぶりにリバイスしてはどうか。

- 変更点の明示について、昨年度は見え消し版を公表していたと承知しているが、新たに AI 事業者ガイドラインを読む方も多い一方で、既に読んでいる方も多いことから、今回の更新でどのような方針での更新がなされたのかが分かるような資料を併せて公表してはどうか。
- AI 品質マネジメントイニシアティブにて、企業間の受発注の合意をする際に AI 事業者ガイドラインをどのように使えばよいかを企業の方々と討議したことがあったものの、明確な結論は出なかった。他の委員からの御意見にもあるように、事業者の参考となるような記載が必要と考える。
- ステークホルダーとの関係について、現在の記載では、透明性、アカウンタビリティ、社会的受容といった表現が見受けられるが、やや範囲が狭いのではないかと感じた。より積極的にステークホルダーとの関係を記載してはどうか。例えば、基本理念や原則に基づく取組を通じて、社会全体における AI 活用の信頼性向上や AI 活用の拡大がもたらす社会的便益といった観点を積極的に記載することが必要ではないかと考える。
- 事業者の適切な取組と個人の利用との関係について、現在、個人による AI の利用も非常に広がっている中で、事業者が基本理念や原則に基づいた適切な取組を行うことが、個人の適切な利用にもつながるという点を記載してはどうか。ガイドラインの中にはステークホルダーへのフォローアップ、ステークホルダーへの情報提供といった項目も設けられているので、そうした観点からの追記が望ましいと考える。
- 本編及び別添に対する更新内容の公表の仕方についてである。他の委員からも同様のご指摘があったが、今回加えられた更新内容は、AI の技術動向、AI ガバナンスに関する国内外の最新動向、事業者の取組の進展など、押さえるべき環境変化を踏まえ、ガイドラインとしての考え方をさらに深め、あるいは見直しを行ったものであり、どのような点が更新されたかという情報は活用する方々にとって非常に重要であると考える。どのような環境変化に対してどのような考え方でガイドラインが更新されたかというポイントを簡潔に整理し、公表してはどうか。今回の公表と同時には難しいかもしれないが、ぜひご検討いただきたい。

以上