経済産業省 第 6 回 AI事業者ガイドライン検討会
議事要旨

令和 7 年 3 月 17 日(月)
10:00～11:30
オンライン会議

冒頭挨拶

- 前回の第 5 回検討会で頂戴したご意見を踏まえた更新を行い、1.1 版の案としてお示しする。更新案の内容や次年度以降の更新に向けたご意見を頂戴したい。

◆ 議事(2) 全体討議

■ 更新案について

- 更新内容に関して非常に良い点としては、ガバナンスの論点や用語が、解釈が分からないことが多かったが、プラクティカルに更新して頂いているように思う。また、様々な企業の事例が別添として記述されているのも、非常に良いことと思う。必ずしも日本政府がお墨付きを与えるという意味ではないというところは注意しなければいけないが、このような形で様々な企業が体制を構築できると良い。
- 新規領域の AI エージェントや RAG 等に対しても、非常に柔軟な更新がされている。
- 非常に網羅的に更新されているため、今年度はこのままで進めていけば良いと思う。
- 現在の AI 利用時に生じるリスクでかつ、直接的に影響が出るものを網羅している。
- リスクの追加等は適切に更新がなされた印象である。
- 生成 AI の普及や RAG の導入等、世の中の動きに対応するとても有益な情報がアップデートされたと認識している。
- 情報の充実と整理が進んだ印象である。
- リスクを技術的リスクと社会的リスクに大別し、分類や事例を記載していただいたので非常に分かりやすい。
- コラムで具体的なケースを追加されており、スタートアップや自治体等のこれまでにないケースについて紹介ができており、具体的に踏み込んだ議論ができている点が非常に素晴らしいと思う。

■ 次年度以降の更新に関して

2-1. AI によるリスクの洗い出し・分類

- リスクに関する位置付けや定義を補記されているため良いが、1 つ 1 つ見ると、例えばトリアージにかかるリスク等はどれだけ日本企業やその担当者に関係があるか等、バランスを見直していただくと良いのではないか。
- AI が今後本格的に普及していった時に、必ずしも経済的な問題だけではなく、例えば教育や国際競争力などの様々な社会的影響が出てくるものと思われる。こうした影響に前もって備えておくことは難しいと思うが、中長期的なトレンドも含め、兆候を捉えて反映していくことが必要であるのではないか。
- リスク等を追加いただいたが、事業者や業種によってリスクは異なる。事業者が

自社の事業に沿って、どれだけのリスクがあるかを把握・特定し、取り組むことが大事になり、その意味ではガバナンスが重要になる。

- 生成 AI へのクローズアップがこの 1 年だけでもかなり進んだという所感がある。今まで生成 AI が社会実装に進むまでは、AI のリスクについて様々な抽象的なリスクを議論してきたけれども、かなり具体化し、顕在化してきたことを表す更新が多く、この辺りの意識はこれからも継続的に高めていかなければならないとともに、新たな更新においては、体系の見直しも考えていかなければいけないと考える。

■ 2-2. AI の契約に関する留意事項

- （契約に関して、委員からのご意見等はなし）

■ 2-3. 生成 AI に関する記載の追加

- 別添の P.100-101 では、RAG に関して追記はされているものの、生成 AI と従来型 AI が区別されていないため、次年度以降の議論の中で、生成 AI と従来型でどう対応していくべきかを分けて考えることを議論してもよい。
- 近時の流れとして、2025 年から AI エージェント、そして Deep Research がある。特に Deep Research は非常に便利なもので、急速に広まると予想されるため、若干触れた方が良いのではないか。AI エージェントについては、責任論の問題があり、Deep Research については著作権やシミュレーションの問題がある。一方で、経済の活性化や業務効率化を図っていく上では非常に重要なものであり、状況を勘案しつつ、動きを取り込んでいくことが重要ではないか。
- 実際に人間中心的な AI 開発をしようとすると、本編 1)人間中心の②「AI による意思決定・感情の操作等への留意」における「人間の意志決定、認知等、感情を不当に操作することを目的とした・・・AIシステム・サービスの開発・提供・利用を行わない」との記載が、実際のプロジェクトでは問題ないか否かで議論が分かれることが多かったため、具体例がより増えるか、考え方が示されると良い。この記載は、マインドコントロールやナショナリズムを煽ることを NG とするための条項だと思うが、実際のプロジェクトの場合、カスタマーサポートで怒っている顧客を宥める AI や Slack の中の AI bot で社員のやる気を引き出すこと、子供に対して勉強するように仕向けていくことや、AI に頼って答えだけ聞かないようにしつつ、英語を大好きにすること等が、操作や洗脳にあたってしまうのではないか。あるいは普通の手法の中で利用されている、リバタリアン・パターナリズムも、AI 事業者ガイドラインの中では厳密に言うと先導したり、仕向けたりするような AI に含まれてしまう。
- 偽・誤情報による混乱、金銭的被害、フィルターバブルやエコーチェンバーによる考え方の偏りなどは、現在、消費者問題として顕在化している。こうした背景があるため、事業者には是非隅々まで共有いただき学習していただきたい。事業者の中にも様々な業態があり、事業規模も大きく異なるため、大企業や業界団体については問題ないが、小規模事業者や業界団体がないケースについては、どのように隅々まで届けることができるのかが非常に大きな課題と考えている。

■ 2-4. AI ガバナンスに関する事例の充実

- もともと、今回法的拘束力がないソフトローのアプローチを進めたことは、AI の技術がそれほど発達していない中で、最初から罰則ありの法令にしてしまうと企業のイノベーションが進まないことを懸念したことがある。また、我が国の企業文化

を見ても、ソフトローの場合でも取り組むことが多いことを考えてそのようにしたが、非倫理的な AI 開発や利活用があれば今後、法制化しなければならなくなる。事業者は、是非 AI 事業者ガイドラインに則って組織内の AI ガバナンスの構築をしていただきたい。特に今後政府の AI の調達においても AI 事業者ガイドラインに則って開発していることが基準になってくるのではないか。

今後の課題としては、日本においてはまだ AI を活用している例が少ないため、政府が率先して AI を使っていくことが国際競争力を高めていくのではないか。AI モデルを作るには、まずデータ作成準備から行う必要があるため、デジタル化も今後も進めていくということが重要になる。

- 海外のモデル、特にオープンモデルを利用することが非常に多くなってきているなか、海外のモデルがどのように学習・制御がされているかが把握できない場合がある。海外の AI 開発ガバナンスに関する機関と連携し、海外との歩調を揃えていくことが大事であるが、どうしても歩調を完全に揃えることは難しい国や地域のモデルを実際に利用する場合に、どういった事例が問題になるかをまとめ、使う際の指針を作っていくことが必要ではないか。
- 企業の経営に関わる 1 人として、経営者の積極的な関心と関与が、企業における AI の活用と、その付加価値を高めていく鍵になると強く感じている。特に経営層における AI ガバナンスの取組が重要である。今回の更新でも事例の追加がなされたが、更に事例が充実されていくことが重要なのではないか。現在コラムで掲載されている事例は非常に大きな企業の取組が中心になっている。今後は、大企業ではない規模であって、AI 開発をしていない、活用が中心である多くの企業の後押しを、AI 事業者ガイドラインを通じて行うことが非常に重要になる。そのためにも、様々な規模の企業の取組事例、あるいはガイドラインの活用事例を充実して情報発信をしていくとよいのではないか。
- ユースケースの拡充等は今後の課題としてあり得ると思いつつ、どこまで本検討会で取り組むのか、またどのような内容を民間で、より具体的に議論していくことかを検討すべきではないか。

■ <u>2-5. AI ガバナンスの動向等の反映</u>

- AI 法案が国会に提出されており、可決されると AI 事業者ガイドラインはどのような位置づけとなるのか。
- 2 月 28 日に閣議決定された「人工知能関連技術の研究開発及び活用の推進に関する法律案（AI 法案）」と AI 事業者ガイドラインとの関係は明確にした方が良いのではないか。具体的には、AI 法案の 13 条に、「国は、人工知能関連技術の研究開発及び活用の適正な実施を図るため、国際的な規範の趣旨に即した指針の整備その他の必要な施策を講ずるものとする。」と明記されているが、条文を読むと 13 条に基づいて AI 事業者ガイドラインができているようにも思える。少なくとも国は、AI に関するガイドラインを作ると自ら義務を負っている法律になっている一方、AI 法案はまだ国会に提出されたばかりで成立していないため、現時点での入れ込みは難しいのかもしれない。AI 事業者ガイドラインが、AI 法案に基づいて作られているとすれば、同ガイドラインの根拠やポジションを明確にし、存在意義やバックグラウンドを持っていることを明示するには非常に役に立つのではないか。単なるガイドラインではなく、何らかの法的な根拠に基づいて作られているものであるということであれば、事業者も真剣に取り上げてくれるのではないか。

- AI 法案と AI 事業者ガイドラインとの関係を意識することが良いというご意見があったが、法体系の中での AI 事業者ガイドラインの位置付けをしっかり意識していく必要があるのではないか。特に、今後生成 AI の利活用が進んでいくことが予想されると、アプリケーションの提供者の役割は、これからより大きくなると予想している。AI 事業者ガイドラインでは特に提供者の概念の見直しは今回行われていないが、今後の議論の中で、現在の提供者の概念が、現実の社会の影響を反映したものになっているかどうか、見直す必要があるのではないか。ガバナンス体系上の提供者の立ち位置や提供者中心の整理について考えていく必要がある。また、現状 AI に対する具体的な規制は各業法の内容に委ねているという理解がある。一方で、利用者観点では、AI に対する具体的な規制のわかりづらさが否めないという感触を持っている。各業法の AI に対する規制に関する見取り図のような役割を AI 事業者ガイドラインが果たしていくと良いのではないか。
- AI 法案と AI 事業者ガイドラインの関係性については、今後、主要なイシューとして本検討会等でも議論していける機会ができると非常に良い。また、AI 戦略会議・AI 制度研究会の中間取りまとめの中で、様々なリスクに日本のどの現行法が直接関わりうるかの詳細な表が作成されている。表自体も大変有用であり、これからおそらく個別法の中で利用に関わる法改正や新しい立法が進んでいくため、整理の表を継承し、整理していく可能性も十分あると感じている。
- 様々なリスクを整理していく中で、国際的なハードローの制度整備が続いていく状況を適切に整理し、位置付けていくことを誰がやっていくかは、継続的に考える価値がある。EU の COP 等の動きや、例えば 2024 年 9 月に十数本の AI 関連法を成立させ、2025 年から徐々に施行させているカリフォルニアをはじめとした手法、特に政権交代後アメリカの立法は更に進むと思われる。例えば、学習データの概要を適切に開示できる前提で作っておくことや、AI から生成されたコンテンツが適切に識別できるような技術的仕組みを作っておかないと海外展開ができない状況に徐々になりつつある。数日前に中国でも新しい自主コンテンツ識別についての法規範が公表されている。自身の知る限りでは、今までプライバシーやデータ保護に関しては DFFT の文脈もあり、海外進出リスクに関する法制の情報を日本政府も極めて丁寧にこれまで事業者向けに紹介しているものの、ヨーロッパ法や州法についての情報のアップデートをしっかりしている政府機関は日本には今のところ存在していない。日本で取り組む場合に、AI 事業者ガイドラインの一部に位置づけるということも考え始めても良いのではないか。
- 今後 AI 事業者ガイドラインをどういった位置付けとしていくかは次の課題としてあり得る。サスティナビリティは比較的新しいトピックであるものの、先進的な企業が取り組みを始め、投資家からも非常に重視され、スチュワードシップコードやコーポレートガバナンスコードに組み込まれて、より取組が広がっていったという流れがある。現在、AI ガバナンスにおいては先進的な企業が取組を始め、助言会社がガバナンスについて言及する等、投資家も非常に重視し始めている段階であり、今後同様の流れが加速するとなると、AI 法案との関係としてソフトローの中で本ガイドラインをどう位置付けていくかという課題もある。
- 今後、事業者としても日本の法律やガイドラインに準拠しつつ、海外の規定にも適用できる相互運用可能な体制の参考とできるように、クロスウォークで違い等を明らかにしていくのがよいのではないか。

- AI 事業者ガイドラインと AI 法案との関係については、可決成立後、どのような形で表現するか明確にするべきではないか。

■ 2-6. 特定単語の整理・見直し

- AI 事業者ガイドラインに記載されている様々な企業の事例は有益であるものの、必ずしも日本政府がお墨付きを与えるという意味ではないというところは注意しなければならないが、このような形で様々な企業が体制を敷いていけると良いと考える。今後の課題としては、AI 事業者ガイドラインに記載の具体的なユースケースや AI サービス等の例の解像度を上げ、具体的なサービスにおける見本となるようなガバナンスのプラクティスを参考事例として拡充できると良い。
  また、もう 1 つの課題はガバナンスに関する要望が非常に整理されてきたからこそ、キャッチアップが難しいとは認識しているものの、新たに出てくるような技術の用語を含めて整理していく必要があると考える。例えば AI の学習という言葉 1 つをとっても、それが機械学習を指すのか、いわゆるプロントエンジニアリング等を含める文脈内学習（In-Context Learning）を指すのか等、全く AI モデルに与える影響が異なるところでも誤解されていることが一般的には多く見受けられる。

■ 2-7. その他

- 本編_P.8 の脚注 8 において英国の AI 安全性機関（AI Safety Institute）」の設置計画発表について記載があるが、2025 年 2 月に英国 AISI の名前が「AI Safety Institute」から「AI Security Institute」となったため、更新が必要であると認識している。
- AI 事業者ガイドラインについて、今後 1 年ごとに公表すると思うが、進め方として毎年 3 月または 4 月に公開するパターンでいくのか、それとも、やはり AI 分野はマルチステークホルダープロセスが言われており、同プロセスを活用したやり方で、さらに取組を進めていくのかということも今後の検討課題になる。また、AI 事業者ガイドラインを使う立場としては、1.0 版から 1.1 版への更新はあまり変わっていないと感じるのではないか。確かに中身を見ていると本編は少なくとも注意書きが追記されている程度であまり変わっていないという見方もあるが、今後は令和 6 年度の見直しではなく、「2024 年度版」「2025 年度版」とした方が理解しやすいのではないか。今後どのように更新し、最新版を提示し、更新を行うかは試行錯誤をしながら考えていかなければならないと考える。
- 政府に、事業者が AI 事業者ガイドラインの趣旨に沿った形で取り組んでいるかという調査は適宜行っていただきたいと思う。AI の社会的影響は大きいため、消費者個人の不利益等がないかも含めて AI 事業者ガイドラインの内容は適宜見直されると良い。教育については、AI が事業者の競争力を高めるという点もあるが、社会への影響力も非常に大きいため、事業者内や政府においても教育を進めていただきたい。また、消費者個人は、AI 事業者ガイドラインの対象ではないが、消費者個人への教育についても大事であり、例えば、消費者個人に対して影響力を及ぼすという面と、消費者個人をエンパワーメントするという面がある。
- AI 事業者ガイドラインは、より多くの企業で繰り返し活用されてこそ意味が大きくなるので、今回 AI 事業者ガイドラインがアップデートされたことを積極的に様々な場所や機会で情報発信していくことが大事である。また、継続して AI 事業者ガイドラインがどのように活用されているか、どういった要望があるか等を調査し、吸い

上げ、今後の方針に生かしていくことが非常に大切であると考える。

- AI 事業者ガイドラインの利用状況の調査やフィードバックは非常に重要かと思う。また、今後は毎年更新していく進め方で問題ないかといった点も含めて検討が必要ではないかと考える。対外発信については組織体制等の問題もあると思うため、その辺りは是非ご検討いただきたい。

■ 本日の議論を踏まえたガイドライン（案）更新のご一任、及び今後のスケジュール

- 本日のご指摘の点等に係るガイドラインの更新については、総務省側の有識者会合の議長および座長および経済産業省側の座長に一任とさせていただく。

（特段の異議なく賛同）

- ガイドラインへの必要な反映を行った上で、総務省側の有識者会合の議長および座長および経済産業省側の座長に一任のもと、政府の手続きを 踏まえ、3 月下旬から 4 月上旬頃に AI 事業者ガイドライン第 1.1 版を公開する予定

以上