第3回　AI制度研究会　議事要旨

1．日　時　　令和６年９月10日（火）17:00～18:30

2．場　所　　中央合同庁舎８号館１階 講堂

3．出席者

○ AI 戦略会議　構成員

座　長	松尾　豊	東京大学大学院工学系研究科 教授
構成員	江間　有沙	東京大学国際高等研究所東京カレッジ 准教授
	岡田　淳	森・濱田松本法律事務所 弁護士
	佐渡島庸平	株式会社コルク 代表取締役社長

○ AI 制度研究会　構成員

座　長	松尾　豊	東京大学大学院工学系研究科 教授
座長代理	村上　明子	独立行政法人情報処理推進機構 AI セーフティ・インスティテュート 所長
構成員	生貝　直人	一橋大学大学院法学研究科 教授
	岡田隆太朗	一般社団法人日本ディープラーニング協会 専務理事
	岡本浩一郎	一般社団法人ソフトウェア協会 副会長／株式会社リアルソリューションズ 代表取締役社長
	柿沼　由佳	公益社団法人全国消費生活相談員協会消費者教育研究所 副所長
	工藤　郁子	大阪大学社会技術共創研究センター 特任准教授
	殿村　桂司	長島・大野・常松法律事務所 弁護士
	中尾　悠里	富士通株式会社富士通研究所人工知能研究所 プリンシパルリサーチャー
	永沼　美保	一般社団法人日本経済団体連合会デジタルエコノミー推進委員会 国際戦略ＷＧ 主査／日本電気株式会社 品質・エンジニ

アリング推進部門 主席プロフェッショナル

原山　優子　　東北大学 名誉教授／GPAI 東京専門家支援センター長

平野　晋　　中央大学国際情報学部 教授・学部長

福岡真之介　　西村あさひ法律事務所・外国法共同事業 弁護士

松原実穂子　　日本電信電話株式会社 チーフ・サイバーセキュリティ・ストラテジスト

○ ヒアリング対象者

古川　直裕　　株式会社ABEJA 弁護士

藤村　修平　　株式会社Preferred Networks 経営企画兼CEO/CER補佐

秦野　芳宏　　ヤマト運輸株式会社　執行役員（輸配送オペレーションシステム統括）

髙村　博紀　　一般社団法人情報処理学会ISO/IEC SC42WG1国内委員会 幹事

４.議　題　　AIのリスクと制度的対応について（ヒアリング）

５.資　料

資料１　　株式会社ABEJA 発表資料

資料２　　株式会社Preferred Networks 発表資料

資料３　　一般社団法人情報処理学会ISO/IEC SC42WG1国内委員会 発表資料

参考資料　　AI制度研究会 構成員名簿

６.議事要旨

○ ヒアリングに先立ち、松尾座長より以下の挨拶があった。

・ 先月２日、岸田総理、高市大臣御出席の下、ＡＩ戦略会議と合同で第１回研究会を開催した。構成員からは、生成ＡＩの登場によってリスクは大きく変わっている、ガイドラインはアジャイルでよいが守らない者もいる、国際整合性が必要、制度と技術の両面からＡＩの安全性を高めるべき、といった様々な意見を頂いた。

・ これを受け総理からは、イノベーション促進とリスク対応の両立、変化の速さへの対応、

国際的な相互運用性、政府による適切な調達、利用の４点を原則として検討を進めるようにと指示があった。

・ 先月23日に開催した第2回研究会では、外部有識者の方にヒアリングを行い、AI制度の在り方について御意見を頂いた。本日も、引き続きヒアリングを行う。

○ 株式会社ABEJAの古川様より発表と質疑応答があった。内容は以下のとおりである。
なお、質疑応答において、質問は「□」、回答は「■」とする

（発表）

・ AIのリスクはユースケースから離れて考えることはできない。現在日本でLLMの導入が進んでいるのは特定のユースケースを想定しているものであり、ユースケース毎のリスク管理が重要。AI規制ではなく、個別分野の個別規制、ソフトローと既存法の併用がベスト。
・ 日本では法規制がないと思われているが、個別法にAIの適用があることを明示できていないだけ。アメリカのようにガイダンスとして明文化することにも意味がある。
・ ユースケースごとのリスクを的確に把握する人材の育成とリスク検討実施例の公開が必要。
・ 技術に対する規制、つまりユースケースを離れた生成AI技術、汎用AI技術の規制についての議論も進んでいるが、これらは従前から存在する技術であり、あくまでユースケースの規制でよい。
・ 大型生成AIの規制も、イノベーションを阻害する。技術の発展が著しい中、規制の基準や内容、求められるものも定まっておらず、合意しようがない。ユースケースレベルの規制で事足りる。
・ アメリカで法規制が進んでいるというのは誤解がある。アメリカの専門家は法規制を行っているとは考えていない。州法による規制もあまり上手くいっていない。

（質疑応答）

□ 情報開示について、個別法で対応できる部分はあるが、汎用AIの開発者に一定の情報開示を課すこと、レッドチーミングなど安全性の確認方法を開示することなどは、一定の意味があると考えるか。

■ 情報開示の内容による。概して開示の意味のないものが多いと感じる。現実的な導入過程に即したものなど実効的な開示内容とすべき。レッドチーミングについては、生成AIの安全性というのが非常に広範であり、その評価方法も統一されていないため比較しようがない。一定の手法、データセットが決まらない中での情報開示は意味がない。

□ 意味のない開示義務は企業負担になるため、よく検討すべき。レッドチーミングは、国際的な基準への関与を深めると同時に、国内でも標準データセットを用意するなど、業界全体として安全性に対する準備をすべきと考えている。ぜひご参加頂ければと思う。

■ 国際的に統一する方向に動いているのは非常にありがたい。他方、レッドチーミングのノウハウはOpenAI等のビッグテックにあり、比較的小規模な企業で大企業と同様の実施は困難。中小企業でも実施可能な基準の策定を望む。

□ 日本の場合、下請け・孫請けも多くある中で、AIの技術を提供する業者、サービスを提供する業者などのうち誰に対して安全性の義務を課すのか、誰が責任をもつべきステークホルダーなのかも明らかにすべき。

□ ユースケースごとのリスク把握のための人材育成やリスク検討実施例公表については、政府主導ではなくて業界団体主導が望ましいという意味か。官民連携の在り方や政府がすべきことについて伺いたい。

■ 事例公開については、顧客企業との関係があるため、業界団体の要請があっても難しいため、政府の後押しがあると非常に説明しやすい。人材育成について具体の方法は分からないが、政府のレポートを出すなどしていただけたら、我々が情報を収集して知見を増やすことができるので、官民連携という形がよいと思う。

○ 株式会社Preferred Networksの藤村様より発表と質疑応答があった。内容は以下のとおりである。

（発表）

・ 当社ではAI技術のハードウェア応用にも注力しているため、特有のリスクとして、プラントの稼働停止、生命や身体への重大な損害などの物理的な側面に配慮している。

・ リスクへの対応は、ソフトローと既存の法制度での対処が適切。世界の動向はいろいろあるが、日本における立法事実があるのか検討すべき。

・ 日本は、コンプライアンス意識の高さを生かしながら国際的な競争力を高められる稀有な存在と考えている。開発企業はレピュテーションリスクに配慮して開発を行っており、またユーザー企業にとっても倫理に反するサービスを使うことは事業上のリスクであるため、倫理観に反するAIは自然と淘汰されていく。このような市場の論理が機能しない場合においてのみ法規制を行うべき。

・ 一旦厳しめな規制を行い、社会受容を見て緩和するという手法も、国際的なAIの開発スピードを考えるとかなり厳しい。一度遅れると、キャッチアップは不可能。
・ AI事業者ガイドラインにもあるが、AIは多くの分野でメリットがあり横断的な規制は望ましくない。立法による対処も、過度に予防的であったり、逆に遅れたものになったりしてしまうのではないか。今は官民共同となって、ガイドラインに基づいた対応を行い、ベストプラクティスを作っていく段階。
・ モデルの規模に基づく法規制も適切ではない。モデルの規模より、データの品質が重視されるトレンドがある。フロンティアモデル規制はその主要な目的に安全保障があるが、安全保障に関する情報を外国企業が日本に提供することは現実的には考えられず、仮に日本で立法しても外国企業が法的責任を果たすことは期待できない。
・ 外国産モデルに依存すると安全保障面で様々なリスクが発生するため、国産LLMの利用を推進していただきたい。
・ 産業応用における物理的な安全性の確保を重視しており、高品質なデータによる学習、ログチェックによる監視、フィードバックの収集など、各産業分野における安全基準の遵守、取組先企業が求める安全基準への配慮などをして技術的対応を行っている。法的な取組としては用途制限、禁止事項の規定、規約に反するユーザーの調査等を行っている。
・ スタートアップとしては、過重な開示義務や報告義務を課せられるとコスト面から対応が困難。

（質疑応答）

□ 第三者認証によるモデル・利用データの安全性検証の有用性について議論があるが、事業を促進する、ビジネスにプラスになる制度は考えられるか。

■ 内部情報の守秘性が担保できるのであれば協力したい。ユーザーの安心感につながる制度であれば建設的な提案になる。しかし、対応コストが懸念されるため、その点を踏まえて設計して頂きたい。

□ 国産LLMの定義について、どのようなイメージを持たれているか。

■ 日本語データから開発を進めているところだが、そういった業者をサポートしていただければありがたい。また、国産LLMは日本の文化的な背景を生かせるところが強みで、政治・経済・教育などの場面において重要になると考えている。

□ 基本的な方向性として、既存の法律とソフトローの組み合わせは良い考えだと思うが、現

状の法規制の中で捕捉しきれない部分はどういったものがあるか。また、イノベーションの促進と国産の優遇に関して、一部矛盾しかねないところがあるが、この2つの観点に折り合いをつけられる良い案はあるか。

■ AIについて既存の法制度でフォローできないような具体例は特になく、社会問題にもなっていない認識。漏れ出てくるものについては、AIの関与の有無に関わらず悪質な行為と考えられるので、行為そのものを行為段階で規制すべき。また、イノベーションを促進する上では外国産ももちろん良いものだと思うが、例えば官公庁の調達規則に入れ込むなど限られた文脈において国産LLMの使用を促進することが考えられる。

□ 技術的な取組についてログチェックによる監視とはどのようなものか。人力で行うのか。

■ ユーザー企業に対して、我々がAIの効果的で適切な使い方を助言するという観点から、ログチェック機能について明示した上で行っている。自動化できていない部分も多いと思うが、そこに改良の余地はある。

□ 物理的な安全性の確保とはどのようなものか。生成AIはソフト的アプローチが多いので、物理的な取組は先進的だと感じた。また、物理的安全性については既存の法律でカバーできているのか。

■ 物理的な安全性確保については、応用する分野毎にガイドラインが異なり、分野横断的な安全基準を考えるのは難しい。各論的な話になるので、別の場で議論できればと思う。産業応用における安全性は詳細な法規制にはなじまないと考えているので、全く異なる文脈の話になると思う。

○ ヤマト運輸株式会社の秦野様より発表と質疑応答があった。内容は以下のとおりである。

（発表）

・ 物流業界では、安全性が特に重要。誤動作は生命に直結する。AIをルールでコントロールする点に課題意識がある。

・ 交通は公共・インフラであり、個別企業は一定の小さな関与しかできない。事業体ごとに特性があり、我々の場合は交通だが、各分野で公共・民間の役割・責務を明確化しなければならないと思う。

・ 人口減少や2024年問題は他国に先駆けた課題解決の機会ともとらえられるが、役割分担が明確化出来ていない現状では、スピード感が出ない。

・ 職場環境の整備や未来の働き方の在り方について、一定の解をだす必要がある。その上で

AIをどう活用していくか考える必要がある。

・ 当社では、業務量計画において予測数量を導出する過程でAIを用いている。予測が外れた際の補完業務も一緒にデザインしている。

・ LLMや生成AIに関しては、国産のものを利用したいという思いもあるが、海外勢との圧倒的な差を考えると、何か策がないかと考えている。

・ AIを産業の活性化の柱として考えるのか、サポートとして考えるのかによってアプローチが異なるかと思う。

（質疑応答）

□ 事業推進の上では、現行の法規制の中での手当ては可能だと考えられるのか、難しい部分があるのか伺いたい。

■ 一般的な法でできることには限界があるため、業界に応じた論点が必要だと認識している。交通の分野では今は自由に事業として活用できないところがある。業界の特徴と業法で組み立て直す必要がある。

□ 公共と民間の役割の明確化について、公共側に担ってほしい部分は何か。また、AI の規制を設けるとしたら、納得できる範囲や事業としての影響範囲を伺いたい。

■ 規制がかかりすぎること自体がリスクだと思われる。今後の状況が見通せない中、制約がかかると制約内でしかデザインが出来ないのは問題。規制については、（個人の意見として）国力をつけるための規制なら、利益の観点からは手放しでは喜べないが、積極的に関与していきたい。

□ 個別の領域で更にAIを使いやすくするために、現行法で足りない部分を整備していく必要があるという意図か。

■ 然り。

○ 一般社団法人情報処理学会の髙村様より発表と質疑応答があった。内容は以下のとおりである。

（発表）

・ AIの国際標準はISO/IECのJoint Technical Committee 1のSC42が中心的に行っている。WGは5つあり、他の委員会との共同委員会もあり、ウィーン協定の下、CEN/CENELECから依頼され共同開発している国際規格などもある。

・ 67のプロジェクトのうち、日本が3割弱程度を主導している。
・ ISO/IECにおけるAIの国際規格は、基本的な用語、AIシステムのフレームワーク、機械学習、適合性評価、機能安全とAIシステムについてのものなどがある。いくつかの国際規格のJISの作成も進んでいる。
・ ガバナンス、マネジメントシステムの規格についても国際規格ISO/IEC 42001が2023年12月に発行されており、そのJIS原案作成をしているところ。適合性評価に関しては、High level frameworkを規定するマネジメントシステムだけでなく、製品（プロセス、サービス等を含む）に対する適合性評価についての提案が出ており、今後の動向に注目したい。
・ EUのAI Actでは義務要件を規定しているが、欧州委員会がCEN/CENELECに整合規格を依頼するプロセス、体制が存在する。日本においては、事業者ガイドラインは存在するものの、法律と国際規格が連動できているとは言えないので、CEN/CENELEC相当の機関が必要かなどの議論をすべきである。
・ 企業は利益を上げるためにビジネスを行っているが、法律があれば遵守する。法律制定と標準化が整合・連動することにより、企業の競争力強化につながるのであればすべきであると考える。

（質疑応答）

□ 企業の標準化担当の活動が社内でなかなか認められないとのご指摘があったが、そうした活動が経営層や社外で認知され、支持されるようになるためにはどのような政府からの支援が必要か。

■ 国際会議の時差、海外現地での交渉といった働き方への配慮が必要。また、国際的な役職や特許など知財に絡む標準化活動に直接関与されていない場合でも精力的に活動している方もいるが、企業内において、そのような活動を評価されにくい部分があると聞いているので、そういった方の活動も評価できる仕組みがあればよいと思う。

□ CEN/CENELEC相当の機関が必要かという議論に関して、標準化にかかる組織の必要性のみを指摘されているのか、法制度とAIに係る標準の関係性の設計も含めて検討していく必要があるということを指摘されているのか。

■ 欧州では制度があると国際標準が関連するという形で連携が取れている。他方、日本では民間主導で規格策定がされるが、AIに係る制度と規格を紐づける必要があるのか、また、標準を使った制度設計や体制作りにまで議論を展開させた方が良いのでは。

□ 国際標準と法律の整合という点について、機械規則のように個別法とも整合すべきという観点もあるが、AIの一般的な包括法との整合か、個別法との整合かについてはどう考えるか。

■ 実際には、機械規則などでは事業者が整合規格から選ぶことになる。ヨーロッパでは、横断的な規格を作った上で、事業者が柔軟に適合するものを選ぶ方式になっている。

□ CEN/CENELECについて、AI actを受けて行動するのではなく、立法の動きと並行しながら標準化のプロセスを進める調整役のようなところに注目しているが、日本で必要となる機能について具体的に聞きたい。

■ EUは、AIに限った話ではなく機械規則や医療規則についても、法律と標準化という大きなフレームワークでとらえている。日本の場合、普段から法令と整合規格との関係性の明確なグランドデザインが必要。EUは参加国が多いこともあって、民主的に議論を進め、トップダウンで行う文化がある。

□ 国際規格の策定への貢献度が下がると、日本のビジネスにどのような影響があるか。

■ 国力的な観点で国際標準の活動は重要。ガラパゴス的な規制は国際的に貿易障壁にならないようにしなければならない。日本は規格に関して中立的に関与するだけではなく、戦略的に規格をどう使っていくか、ビジネスや今後の戦略について国として議論を進めるべきかと思う。

□ AIの産業が発展途上で、技術的にも見通せない中、標準化はどういった考えで進められているのか。方向性はあるか。

■ 個社で参加されている方も含めて中立的である。変な標準が作られるのを防ぐことと、日本に突出した技術があれば国際的に有利な規格を作り国益を確保することの、守りのための標準化と攻めの標準化の2側面が要点。

□ 国際標準化活動は重要。例えば、日本で特に発展していた燃料電池については、中国主導で標準化が進んでしまった。標準を制する者が製品の競争力や評価を制する。法律と規格の関係は微妙なところはあるが、WTO上の協定に即して、国際標準があればそれを意識するようになっている。AI製品の認証については、ISOで検討が進んでおり、手遅れになる可能性はある。世界的に標準ができてしまうとそっちに引っ張られてしまうか。また、国際標準に基づく認証制度がスタートするのはいつ頃と考えるか。

■ 42001のマネジメントシステムの規格自体は既にできている。おそらく年内には42006の規

格が発行されるので、認証機関の設置が認められ、国際認証のスキームがスタートするだろう。日本ではJISができて国内で認定機関、認証機関が出てきてからとなると時間がかかるが、遅れをとる形にはならないようにしたい。

□ 日本は中立的であるのに対して、海外の方は標準化に当たっては綱引きをしているのかと思うが、標準化の会議等の様子はどうか。

■ 規格提案に対し、総会の場では強い対立となる場面もあったが、結果的に総会外での調整で話を収めることがあった。タフな交渉力が求められる場面もあるが、EU内は距離的にも近いので、密にコミュニケーションを取って民主的に進めているという感じがある。

○ 本日のヒアリング全体を通して、各構成員よりコメントがあった。内容は以下のとおりである。

・ AI 制度のアプローチとして、ハードローかソフトローか、個別法か AI 法か、という論点があるが、個別法ベース＋ソフトローという話が納得感がある。
・ 個別の法規制による対処では、AI ができることが広がって（増えて）しまうため、何らかの手当が必要。また、人が運転しない自動運転等、現状の法規制が想定していないものを、どう手当てしていくかが課題。
・ 事業者や国際標準化の現場から重要な点を聞けた。特に、透明化・情報開示に関して、開示する意味のない情報が指定されているとの指摘は、真剣に検討する必要がある。
・ 個別法と AI 法は二者択一ではなくて、個別法で対処すべきものはそれで対応すべきだが、それで足りるのかが論点。
・ 誰を規制するのが効率的かとの観点から、開発者に情報を出させた上で利用者がリスクを判断するというような、役割分担も視点として必要。
・ ビジネスを後押しするための制度として認証を検討することは有意義。
・ 利用者と開発者の責任の分担と、その中でいかに予防原則的な考えを入れていくのかが論点。
・ 国際相互運用性について、アメリカは報告義務、欧州は規制という中で、日本としてどうするのか考える必要がある。

- 国際標準化も含め、企業のイニシアティブ争いは国際の場では熾烈。リスクは特に業種によって違うため、セクター毎、ユースケース毎にリスクの優先度をカテゴライズすることが必要。
- 事業者の意見としては、個別法をユースケースごとに考えて、ソフトローが望ましいというのが概ねの意見という印象を受けた。
- 国際標準をどう活かしていくかについては規制とは別枠で考える必要があるのでは。一方で、国際標準に基づく認証はAIの信頼性確立のために重要であり、戦略的に考える必要がある。
- AIに関わる制度の在り方を考える上で、標準と一体化した制度の枠組みを議論していくことが重要。一方で、平等や人間の尊厳に関わる点について既存の標準プロセスに委ねるだけでなく、行動規範を具体化することが必要。
- 開発者と利用者との責任分担・コスト負担について考えることが重要、併せて、スタートアップのような開発者に対する公的支援の在り方についても考える必要がある。
- AI実装の担い手である事業者がAIを利活用できる状況を確保するためには、既存制度を使っていくことが重要。
- 国際規格の教育の観点について、規範等で必要とされる知識を示すことも必要と考えられる。
- 規制を議論する前に事実関係の把握の必要性がある。どのように把握し、その結果をどう生かせるのか疑問に思う。
- 整備されたガイドラインに基づいて官民協働でベストプラクティスを作っていく際には、ステークホルダーとして最終利用者も含むべき。
- 人的不足をAIで補うには、安全性の観点から規制が必要。公共事業はセキュリティの確保も必要。
- 事業者はソフトローを望む声が多かったと感じたが、ソフト・ハードの線引きをもう少し議論すべき。
- AI規制については、法規制が企業を縛るという意味ではなく、守るという観点からの議論も必要ではないか。

- アクターに応じて、想定するリスクや規制に対する意見が異なることを再認識し、全体像を共有することが必須だと感じた。ポテンシャルとして存在しうる社会的責任の捉え方も共有できるところがないか探るべき。
- CEN/CENELIC では様々なレイヤーが重層的に議論に参加しており、現状の技術に関して幅広い議論をした上で標準化に落とし込んでいる。日本もこういったアプローチが必要である。
- アメリカの大統領令では、教育や労働の分野における AI 利用については担当官庁が法執行するように明確に指図している。日本でも、現行法を AI にも適用すべきと明確に指図すべき。
- レピュテーションリスクが重要というのは理解するが、重要な部分にはハードロー、既存法による法執行も時として必要と思う。
- ビジネスリスク、リーガルリスク、レピュテーションリスクについてお話を伺ってきた中で、教育という観点も新たに出てきた。日本の AI に関する教育の現状やどのような人材教育が不足しているのかについても、雇用側から話を伺う機会があればよいと思う。
- ソフトローや既存の法律でカバーできる点は分野によって異なるため、アメリカが個別の対処を監督官庁に任せているように、全体の議論をベースとして、個別の対処は、AI のセクター毎に所管先に振り分ける方が良いと考える。
- 情報開示の議論でもあった通り、実効性のある規制を考える必要がある。
- 標準を制する者は産業を制する。日本は直ぐに効果が出ないものに対する評価が低い。人材育成を含め、長期的な目線に立って戦略を考えるべき。
- 産業の視点では合理的な判断がしやすいため、大枠として方向性が見えてきたと思う。他方、一般の方や国際的な視点からはどうなのかという部分を、次回以降議論していければと思う。
- 規制は難しい論点が多くあり、基準を作ると規制強化に見えるが基準が明確な方が安心してビジネスができるという意見もあれば、そもそも報告義務は規制ではないというような意見もある。言葉遣い一つとっても受け取り方が異なるため、そういった点も配慮しながら検討を進めていきたい。

以上