第２回　AI制度研究会　議事要旨

１.日　時　　令和６年８月23日（金）16:00～18:00

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	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セーフティー・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

宍戸　常寿	東京大学大学院法学政治学研究科 教授
國吉　啓介	株式会社ベネッセコーポレーションデータソリューション部 部長
吉岡　幹仁	神戸市企画調整局デジタル戦略部 部長
鳥澤健太郎	人工知能研究開発ネットワーク（AI JAPAN）／国立研究開発法人情報通信研究機構（NICT） フェロー
泰地真弘人	人工知能研究開発ネットワーク（AI JAPAN）／国立研究開発法人理化学研究所最先端研究プラットフォーム連携（TRIP）事業本部科学研究基盤モデル開発プログラム プログラムディレクター
辻井　潤一	人工知能研究開発ネットワーク（AI JAPAN）／国立研究開発法人産業技術総合研究所（AIST）情報・人間工学領域 フェロー
松尾　剛行	桃尾・松尾・難波法律事務所 弁護士

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	東京大学大学院法学政治学研究科 宍戸常寿教授 発表資料
資料２	株式会社ベネッセコーポレーション 発表資料
資料３	神戸市 発表資料
資料４	人工知能研究開発ネットワーク（AI JAPAN） 発表資料
資料５	桃尾・松尾・難波法律事務所 松尾剛行弁護士 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。

・ 今月２日、岸田総理、高市大臣ご出席の下、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、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いう指示があった。

・ 前回研究会の議論も踏まえ、本日を含めて３回にわたり、外部有識者の方からヒアリングを行い、AI制度の在り方について意見を頂く。

○ 東京大学の宍戸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のリスクに対してはハードローとソフトローの適切な組合せが必要。

・ AIに共通して顕在化するリスクを抽出してルールを定めることが必要。

・ 政府にはリスクへの規制をアジャイルに規律する司令塔体制が必要。

・ 研究開発の促進と規制のバランスをとり、AI利用の原則の確立と遵守を期待する。

・ 規制の内容以上に、規律を担う組織・体制が確立されることが大事。

（質疑応答）

□ 共同規制について、憲法学的な視点から何か気をつけるべき点はないか。また、偽情報・誤情報をプラットフォーム規制することについて、生成AIあるいはAIに関して議論されていることがあれば教えていただきたい。

■ 共同規制を行う場合は、法律に基本的な考え方、原則が明示され、具体的なやり方については事業者や、事業者と政府の間のガイドラインで定めるという、法律とガイドラインとの役割分担が大事。また、政府はある程度マイクロマネジメントを控えて、根本的に共同

規制の趣旨に反するような事業者の悪質な行為があった場合には法執行を行うという転換が求められる。プラットフォーム規制は、プラットフォーマーが偽情報・誤情報と思われるユーザーの投稿に対して、どのような対応をするのか方針を定めることが重要。生成AIによって生成された投稿などについて行うコンテンツモデレーションの明確化も必要。

□ 政府は利用者としての立場にもなることや、国レベルのルールと地方自治体が主体的につくるものがあり得ることについて、考えを教えていただきたい。

■ 国が行政サービスを提供する場合にAIを利用する際は、法の支配や人々の平等な取扱いに資するような使い方が求められる。国と地方の問題については、国と地方の間や地方毎の差異を積極的に許容すべき部分と、同じでないと困る部分の両方がある。

□ 学習教育の点について、EUのAI法では年齢に起因する脆弱性の悪用などに対しては特出しして規律されているが、日本においてはどういう点に特に注意を向けるべきと考えるか。

■ 若い世代に向けては、AIをうまく使いこなせるように、AIに振り回されない教育の在り方が求められる。一方で、若い世代は順応性が高いので技術についていけるが、大人や年長者は新しい技術についていけないことがあるので、社会の人々全体に対して新しい技術のリスクや、それを使うことの楽しさ等について生涯学習・生涯教育を行うことも必要。

○ 株式会社ベネッセコーポレーションの國吉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活用は事業活動に埋め込まれるため、事業特性に応じた既存法対応が重要。
・ 生成AIの技術の進化に則した基準やデファクトの整備が重要。
・ グローバルなサービス展開では、国際整合性と国際展開しやすい地域の拡大が重要。
・ 技術進化に伴うリスク拡大を踏まえて、社会実装やサービス価値向上では具体策が重要。

（質疑応答）

□ 新しい教育ツールを導入する際の効果の検証について、このAIに関する注意点や研究内容、公開状況、他国との連携状況について教えていただきたい。

■ 検証では出力をポイントとしている。社内の教育系のコミュニケーションに通じた者、情報教育の有識者、子供や保護者に出力物を評価してもらっており、多様な人に見ていただくことにこだわっている。ビジネス上の観点からは、自由研究を題材にしたことで夏休み

期間のみニーズのあるものとなり、期間限定で耐えられるサービス品質を考えてやればよいことがポイント。継続するサービスだとリスク対策の考慮点も増えてしまう。他国とは情報共有はしているが、一緒に取り組むまでは至っていない。

□ 子供の考えには想定外のものもあると思うが、免責についてはどう処理しているのか伺いたい。

■ サービスを始める前に保護者の方とお子様が一緒に学べる動画の学習サービスを提供した。情報教育と併せて提供するなど、保護者の方によく知っていただくことを免責のポイントに置いた。

□ リスク対応について、AI開発者と協力して検討したか、また検討の際にAI開発者から開示してほしかった情報等があれば教えていただきたい。

■ フィルタリングの技術やＬMMの本体の方で調整できることなどを聞いた上で、何を取り入れるか、組み合わせるかを考えるなど、開発者とは密なコミュニケーションを取りながら行った。

○ 神戸市の吉岡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）

・ 事前に完全な安全性担保は現実的ではなく、リスクが顕在化した際の対処の検討が重要。
・ 中小企業もAIに高い関心はあるが、AIの活用やリスク等が分からないというのが現状の声
・ 子供や高齢者のリテラシー向上には限界があり、啓発事業とは別で国民を守る施策が必要。
・ 安全性の担保が懸念であり、第三者評価や認証で担保できる仕組みがあれば活用が進む。
・ 開発者・提供者への義務や第三者認証機関による適合性評価は市単独では実施が困難。

（質疑応答）

□ 開発・提供者の情報提供が適切に得られるかどうかは、認証により担保されるものではないため、認証制度のみでは不十分ではないかと思うが、考えを教えていただきたい。

■ 企業からの情報提供について、求めるものを全て開示していただけるのであればありがたいが、それが企業のイノベーションを阻害する要因になるのかは判断しかねる。一方で、自治体職員にはAIに精通した技術者がいるわけではないので、細かなデータを開示されても正しく読み解けるかは難しい。専門家の方々が一定程度関与して認証という形で安全性を確認したとかの方が利用者としては使い勝手がいいと感じている。

□ 神戸市の条例の２条にAIの定義がされているが、どうやってこの定義が作られたか、参考にしたもの、実際これを適用するのに問題になった点があれば教えていただきたい。

■ 官民データ活用推進基本法などの定義を使っている。生成AIだけではなくその他も含む形。正直、非常に苦慮した。

○ 人工知能研究開発ネットワーク（AI JAPAN）の鳥澤様、泰地様、辻井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）

・ 強い規制があると、社会を守るつもりで作った生成AIが萎縮・弱体化する恐れがある。
・ 生成AIを使用するユーザーや目的に従って、安全性の検証・認証にレベルを設けるべき。
・ 正義を志向する生成AIで社会を守れる可能性があり、それらの阻害とならないような検討に期待する。
・ 科学研究と一般のAIガバナンスとは異なり、過度な研究への規制は発展の阻害となる。
・ 科学分野における公正な競争と発展という観点から、国際的な連携の下に規制を考えていく必要がある。
・ AIは人の認知に直接影響を与えることがあるため、利益優先の民間企業だけに任せておくことはできない。
・ マルチベンダーを前提とした、責任を明確化する法制度やシステム暴走への規制の検討が重要。

（質疑応答）

□ 「フレンドリーAI」という言葉に繋がると思われるが、正義を志向するAIの方向性を伺いたい。

■ 正義を志向するAIはコンセプトが固まっているわけではない。まずはアライメントをきっちりとやる。また、今のＬＬＭでも多少は出した情報に対して根拠を出すことはできるが、例えば信頼のおける情報による裏取りなど、徐々に制御に近づける仕組みが必要。

□ 正義を志向するAIを世の中に広げていく上で、法や制度に期待することがあれば教えていただきたい。

■ 正義を志向するAIがビジネスとして成立するのは厳しいかもしれないので、政府や政府から委託を受けた第三者機関などが社会に責任を持つという立場から、開発や運用を担保す

る必要があるのではないか。

□ 正義を志向する生成AIを生み出していく観点から、認証等の制度はあった方が良いか。また、認証のレベルを分けについて、具体的な考えもあれば伺いたい。

■ 政府や第三者機関が運用するものについては、その目的に照らしてビジネスベースのＬＬＭに課される制約は一部弱めることなどが必要。

□ AI for Scienceという観点より、サイエンスそのものの進め方すら変えてしまう可能性があるという議論もあるが、日本の立ち位置、感触を伺いたい。

■ AIモデルという観点からは欧米が進んでいる。モデルをつくるだけではなく、実験とデータの取得を含めたAIを使ったシステムづくり全体という観点からは、日本にも発展の可能性があり、今あるデータのみならず研究現場から出てくるデータをAI化するということも考えている。

□ システムの暴走とは、一つのAIが暴走するというのではなく、マルチベンダーや社会システムにおいてAIが大きくなる中で社会的なリスクが高まるという理解でよいか。

■ 超知能的あるいは社会機能的なものの暴走と、マルチベンダーの複雑でヘテロジニアスなAIシステムというのが社会の中に入っていったときの暴走は別。ブラックボックス性が高い複数のシステムがトータルとして社会システムを支えるときに、ある種の誤りが起こったときに暴走し、コントロールできなくなるという危険性の方が大きい。

□ 現社会では情報収拾に感度がよくトラブルに遭わない人がいる反面、トラブルに遭いやすい人もいる。ＡＩによる人間のリスクについて、今までとは全く異なるものなのか。また、今後リテラシーを育む際に誰でも同量のリテラシーを育む必要があるのか、今までトラブルに遭いやすかった人に重点的に行ったほうがよいのか教えて頂きたい。

■ 正義の定義が人によって変わるため、人間社会の持っている分断状況がAI世界の中に入ってきて、それが更に強化され社会の分断がより進むことが危険。人間の認知バイアスをAI側が補正してくれるという力はあると思うが、心理性を何も吟味されていないAIの情報に対する批判的な能力を持つということを、全ての人に対して教育していく必要がある。特定のバイアスが強い人だけの問題ではない。

○ 桃尾・松尾・難波法律事務所の松尾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）

・ 中国は推進と規制をバランスよく打ち出しており、弊害を最小化しながら推進している。
・ 既存の法制度がAI技術の推進の障害に成り得る場合は、解釈の明確化・制度変更も検討すべき。
・ 中国では価格差別から規制対象ができたように、日本も問題等を把握した上で検討すべき。
・ 日本は共同規制等の選択肢を踏まえ、民間ができないところを国がすべき。

（質疑応答）

□ 様々なアルゴリズムの届出がかなりの件数で実施されているが、それを可能にするペナルティーや文化のような要因はあるのか。

■ ペナルティーについては、既にネットワーク安全法、データ安全法、個人情報保護法等に関する大きな枠組みがあるため、既存の法令に紐づけていることが良く見られる。刑事処罰ができない場合、主管部門・管轄部門の警告や内容を変更する勧告などが行われ、変更命令の無視や量が重い場合は関係するサービスを停止するように命じるといった書き方である。

□ ３法全てに域外適用があるのか把握できていないが、中国から見て海外企業が届出等にどれぐらい応じているのか。

■ グレートウォールがあり、海外企業のサービス提供がリスクをもたらすなら、サービスを切断することによる解決が可能である。そこで、海外企業のサイトへのアクセスが増え、問題が発生した場合にアクセスを遮断することが多い。少なくとも域外適用対象の海外企業が続々と届出等をしているような状況ではないという理解。

□ 生成AIサービス利用暫定弁法について、ここで言う生成AIとはどのように中国の中で定義をしていて、パラメーター数とかユーザー数などの定量的な基準はあるのか。

■ 中国の生成AIの定義は、基本的にはテキスト、画像、音声、動画等のコンテンツを生成する能力を有するモデル及び関連技術を指すと書かれており、パラメーターの基準などは記載されておらず、かなり広い範囲が対象となる。スライドに期待したとおり、国内企業を中心に届出数がかなり多かった。これは、パラメーター数などの基準を明確に区切らずに広く網をかけたというところが大きいと感じる。

□ 世界の国際議論において中国は民間の中ではメインプレーヤーになっているが、規制の体制や考え方についてどれだけ世界に対して影響を及ぼそうとしているのか感触を伺いたい。

■ 中国は独自の動きをしているという部分はあるが、AIに関する考え方に関して親和的なところを見つけたら協調していくとうスタンス。ルールメイキングも他国とは違う点もあるが、十分に国際的な動きを進めている。例えば、中国はフランスと人工知能と国際ガバナンスに関する共同声明を２０２４年５月に発表している。

○ 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。

・ 神戸市の事例を踏まえて、利用者側でのリスクアセスメントが難しい場合、第三者評価や認証の仕組みが重要。自主的な認証制度の構築・運用は簡単ではない。制度的なインセンティブを考える必要がある。
・ 宍戸先生と同じ考えで、透明性に加えて、特にAI提供に伴うAI提供者が自らリスクを特定・評価し対処することや、システミック・リスク対応のための規制が必要。
・ 神戸市の事例から、AI 提供者・利用者は恐る恐る使用していると思う。進めやすい枠組みがあるとよい。
・ 教育が大事との話を踏まえて、社会全体で活用する環境を整えることが大事。
・ 認証制度に対する期待感及びやってほしくないことも含めて御示唆を頂いた。法律には基本的な原則と考え方を書き込まなくてはいけないということを考えるべき。
・ 既に実践・応用している皆様のお話、そして中国の動向は学ぶべき点が多かった。
・ 規制をかけ過ぎるのはよくないという話があったが、そこは同じ理解。
・ 第三者・信頼できる人の認証でないと利用できないという話は、正に生の利用者の声。利用を促進する規制を意識する必要がある。データを出させることと認証制度を組み合わせて、利用者目線で制度を作ることが重要。
・ 行政における AI 利用の原則の確立と遵守という提言と、一方で、専門的なことは外部認証を頼るべきとの話があり、行政が当事者になる場合にどのような規制にするのかが重要
・ 利用目的に従って安全性の検証・認証にレベルを設けるべきとの話に大いに賛成。AIの公平性の研究をする上でも機微情報を取らないと公平性が損なわれる場合がある。
・ 論点整理の視点では、地方自治体、国レベル、プライベートセクター・ビッグセクターの論点をうまく整理した形で議論を進めたい。
・ 技術的な課題には、技術的に回答を出すというスタンスは重要。その実現のためには法的な専門家と技術的な専門家など、社会と技術の様々な人々が一緒に議論することが大事。

- 神戸市と宍戸先生の話から、透明性と説明責任の問題が気になった。政府調達によってAIを政府機関や地方公共団体等が利活用する際には、例えば何らかの審査等においてAIの予測や決定等を利活用して不利益処分を下した場合等においては、理由の開示等の適正手続が要求され、説明責任が求められる。その説明責任を果たすための、AIサービスを提供している民間ベンダへの情報開示強制には、立法もしくは解釈の検討が必要になるかもしれない。また日本が理事会勧告に向けて主導してきた「OECD AI原則」の中の、OECD原則1.3条では不利益なAI処分への異議申し立て規定があり、分かり易い説明責任が求められている。
- 法制度ということを考えた場合、実際に導入している神戸市あるいは中国の話は参考になった。神戸市の今後の条例や課題とその解決等の動向には注目していきたい。
- 利用者の立場での話から、かなり注意しながら慎重に進めていることが印象に残った。何をどこまで許容されるのかという予見性を与えるという意味で、一定の枠組みは有益。
- AIに完全無欠を求めるというのはかなり無理がある。AIは１人の人間よりも圧倒的に大きな影響を持ち得るので、AIが完璧なものではないことの教育も重要。
- 消費者法や裁判例などの情報をAIに与えて、法規制に抵触しないすれすれを攻めてくる悪質事業者が増えてくることを懸念。
- 認知バイアスの悪用に対するリテラシーの向上が重要。一方でそれには時間がかかり、子供や高齢者への啓発には限界があることが示されたが、これに対してどのように行えばよいのか分析が必要。
- AIを用いたダイナミックプライシングは、消費者が不公平感や不信感を抱く可能性もあることから、表示と説明責任が必要。
- 技術とその規制にはバランスが重要。①技術には技術で対抗していくこと②国際的な共通基準の自主的な活用とその表明③ある程度の規定・規制に従った事業の発展が必要。
- 国レベルのリテラシー、教育現場、ユーザーとしての自治体の話は非常に勉強になった。
- 日本に様々な国籍の方が住むようになった今、日本で使うAIの入出力情報は日本語だけではない。日本語とそれ以外の言語での認知バイアスや出力情報のリスクについても議論をする必要がある。また、言語に関係なく、データポイズニングのリスクに対するセキュリティについても考えていかなければならない。
- 政府の役割として、規制のレベルと国と地方の役割をマトリックスで考える必要がある。

・ 認証については、認証だけでできないことはガイドラインとの組合せが重要。また透明性とのバランス、グローバルとの関係も重要。
・ 安全性に関して、開発者、提供者、利用者の役割も考えながら、ガードレールのつくり方を考える必要がある。その際、「正義感というのは一つではない」という話が非常にポイントになる。国民が納得するように、ガードレールに多様性を持たせ、ガイドラインを柔軟にしていくことを考えていかなくてはいけない。
・ 短時間で様々な視点から説明していただき、密度が濃く、本当にすばらしい内容であった。今後も何回かヒアリングしてくことで相当な点から議論が進むと思う。

以上