AI戦略会議（第11回）・AI制度研究会（第1回）

合同会議　議事要旨

1.日　時　　令和6年8月2日（金）10:15～10:55

2.場　所　　総理大臣官邸　2階大ホール

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
	川原圭博	東京大学大学院工学系研究科 教授
	田中邦裕	さくらインターネット株式会社 代表取締役社長
	山口真一	国際大学グローバル・コミュニケーション・センター 准教授

○ 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

○ 政府側参加者

岸田文雄	内閣総理大臣
高市早苗	科学技術政策担当大臣
松本剛明	総務大臣
石川昭政	デジタル副大臣
今枝宗一郎	文部科学副大臣
村井英樹	内閣官房副長官

他

４.議　題　　AI政策の現状と制度課題について

５.資料

資料１	AI 政策の現状と制度課題について
資料２	構成員提出資料
参考資料１	AI 戦略会議 構成員名簿
参考資料２	AI 制度研究会 構成員名簿

６.議事要旨

○ 議論に先立ち、高市科学技術政策担当大臣より以下の挨拶があった。

・ 本日はAI制度研究会の初回会合を、岸田総理にもご出席いただき、親会議であるAI戦略会議と合同で開催させていただく。
・ これまで、AI戦略会議の皆様には、発足からわずか二ヶ月で論点整理をまとめていただくなど、実にスピーディーに数多くのご助言をいただき、改めて感謝申し上げる。
・ AIはますます高性能化しており、競争力の強化、イノベーション促進と同時に、AIの安全性の確保、リスクへの対応はより一層重要になっている。
・ リスクへの対応は、技術と制度の両面で進める必要がある。AIのように変化が早く多様性が著しい分野では、制度的な対応は法律などのハードローと国際規格やガイドラインなどのソフトローの組合せが欧米では見られている。日本は、アジャイルにガイドラインで対応しているが、法制度の要否も含めて検討が必要になっている。
・ いくつかのアンケート調査では、日本も含む世界各国の国民の多くがAIに関して何らかの規制が必要だと答えている。
・ このような中、AI制度研究会の役割は非常に重要になってくる。構成員の皆様の忌憚のないご意見をよろしくお願い申し上げる。

○ 会議進行の関係上、松本総務大臣、斎藤経済産業大臣、石川デジタル副大臣、今枝文部科学副大臣の挨拶は書面にて机上配布となった。内容は以下のとおりである。

【松本総務大臣】
・ AI制度研究会における議論が開始されるに当たり、広島AIプロセスの成果等の国際的な動向や、幅広いステークホルダーのご意見も踏まえた多角的な検討が行われるよう期待するとともに、総務省としても積極的に議論に貢献してまいる。
・ まず、デジタル分野はボーダーレスであり、AIについても相互運用性が求められるとともに、国際的な協調が重要。
・ そのため、我が国は、昨年から広島AIプロセスを立ち上げ、国際的なルール形成を主導している。本年５月のOECD閣僚理事会では、岸田総理から「広島AIプロセス フレンズグループ」の立ち上げを発表いただいたが、多くの国から高い評価と幅広い支持を受け、現在、53の国・地域が参加している。賛同国の更なる拡大に向け、諸外国への働きかけを進めてまいる。

・また、本年７月、AIに関する国際的な官民連携組織であるGPAI（AIに関するグローバル・パートナーシップ ）東京専門家支援センターを設立した。本日ご参加いただいている原山優子センター長のリーダーシップの下、生成AIのリスク対策に関する技術実証等のプロジェクトを支援し、官民の国際連携を推進してまいる。
・さらに、国立研究開発法人情報通信研究機構（NICT）による質の高い日本語による学習用言語データの整備・提供により、我が国のLLM開発力の強化等に取り組んでまいる。
・これまで培ってきた多言語翻訳技術も活かし、グローバルサウスをはじめとする諸外国との国際連携にも貢献してまいる。
・加えて、経済産業省と連携して本年４月に策定・公表したAI事業者ガイドラインを活用して、今後もOECDやGPAI等と緊密に連携し、AIに関する国際的なルール作りと連携を牽引してまいる。
・次に、AIに密接に関連する課題として、プラットフォーム上の情報流通に係る対応も重要。とりわけ、インターネット上の偽・誤情報の拡散が深刻化する中、先の通常国会にて成立した情報流通プラットフォーム対処法は、大規模なプラットフォーム事業者に対して削除対応の迅速化と運用状況の透明化を求めるものであり、生成AIによって生成された偽・誤情報へも効果が期待される。施行前であっても、早期に本法に準じた対応を行うよう、必要に応じて、プラットフォーム事業者に対して、求めてまいりたい。
・さらに、偽・誤情報を含む情報流通の健全性確保の在り方については、有識者会議で議論・検討を進めていただいており、今後、提言がとりまとめられれば、その内容を踏まえ、生成AIコンテンツの判別等に対する技術的な対応や制度的な対応を含めて、総合的な対策を進めてまいる。
・世界で最もAIを開発・活用しやすい安全・安心な環境を構築するためには、チャンスの拡大とリスクの抑制の両面からの検討が重要。総務省としても、AI制度研究会における議論を踏まえ、関連する制度的な対応も含め、更なる対応を検討するとともに、安全・安心なAIの開発・利用環境作りをしっかりと支えてまいる。

【齋藤経済産業大臣】
・幅広い産業を所管する当省として、AIのポテンシャルを最大限に引き出し、高い競争力を持つサービスの創出を促進することで、我が国を「AIを持てる国」に育て上げ、世界に貢

献していきたい。

・ このためにも、便益とリスクの双方をもたらすAIに対して、「イノベーションの促進」と「規律」のバランス確保を重視して政策を進める。

・ イノベーションの促進に向けては、引き続き、AI開発の基盤となる計算資源を官民で整備するとともに、「GENIAC(ジーニアック)」プロジェクトも通じて、データの利活用を進め、国内における生成AIの開発を加速させていく。

・ また、生成AIの時代にあっては人材こそが鍵。AIの利用促進に向け、求められるスキルの提示や学習機会の拡大など、厚生労働省とも連携して人材育成を強化していく。

・ 一方で、規律の確保に向けては、総務省とともに、４月にAI事業者ガイドラインを発表したところ。まずはこの普及・促進を通じて、あらゆる事業者がリスクに応じてAIを使いこなせるよう後押ししていく。こうした中、政府が率先して実践することが重要であり、デジタル庁と協力しながら、政府におけるAIの調達・利用の在り方について議論を進めていく。

・ 加えて、AIセーフティ・インスティテュート（AISI）を中心に、AI安全性評価の議論も進展している。AISIが、米英をはじめとする国際的なパートナーと連携しながら、相互運用可能な安全性評価手法を策定できるよう、全力で支援していく。

・ 変化の激しいAIについては不断に対応策を検討していくことが重要。これまでの取組を着実に進めながらも、我が国におけるAI環境の整備に向けて、AI制度の検討に、当省として積極的に貢献していく。

【石川デジタル副大臣】

・ デジタル庁では、関係府省庁等と連携して、行政における生成AIの適切な利活用に向けた検証を実施し、ユースケースを発掘するとともにリスク、調達等に係る様々な知見を獲得した。これを基に、今年５月には、行政業務等で生成AIを利活用する場合の想定されうるリスクとその対応策等をガイドブック※として取りまとめるなど、行政における生成AIの適切な利活用に向けた情報発信を行っている。

※テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）

・ また、総務省・経済産業省から「AI事業者ガイドライン（第1.0版）」が公表されたことや、行政における生成AIの利用状況等を踏まえ、本年秋頃を目標として、関係省庁における生成AIの業務利用に関する申し合わせである「ChatGPT等の生成AIの業務利用に関する申合せ

（第2版）」の改定に向けた準備を進めている。

・ 併せて、経済産業省等とも協力し、AIの政府調達において留意すべきリスクや求められる品質確保について整理を進めているところ。

・ 今後のAI制度の検討に当たっても、デジタル庁として、技術面や実務・運用上の観点から、引き続き、貢献してまいりたい。

【今枝文部科学副大臣】

・ 生成AIを含むAIの様々なリスクを抑え、安全・安心な環境を確保しつつ、イノベーションを加速させることが重要である。

・ 文部科学省においては、６月に閣議決定された統合イノベーション戦略2024において、「AI分野の競争力強化と安全・安心の確保」が強化方策の一つとして示されたことを踏まえ、

  ・ 生成AIモデルの透明性・信頼性の確保に向けた研究開発

  ・ 世界に先駆けた科学研究向けAI基盤モデルの開発・共用

等を引き続き推進することに加えて、革新的なAIロボットの研究開発等を推進してまいる。

・ また、先月には検討会を立ち上げ、学校現場における生成AIの利活用に関するガイドラインの改訂を見据えた議論を開始したところ。

・ 文部科学省としては、AIに関する様々な研究開発やその成果の社会実装の推進を通じて安全・安心なAIの利活用によるイノベーションの促進に貢献するとともに、学校現場におけるAIの利活用に向けた取組を進めてまいる。

○ 続いて、松尾座長より、AI制度の現状と制度課題について研究会の構成員の皆様を中心にご意見いただきたいとの説明があり、各構成員から順次、以下の意見が述べられた。

・ 生成AI以前のAIのリスクの焦点は、製品の安全性と個人情報のプロファイリングの問題であったが、生成AI以降は、違法情報や偽・誤情報の生成など情報環境全体に問題の領域が拡大。また、制度を具体化していく上で、①AIの種類や用途、影響力の大小に合わせたリスクベースの仕組み、②AIのイノベーションと安全性を両立するためのソフトローとハードロー両面からの官民の共同規制、③国際的な整合性が重要。

・ AIは素晴らしい可能性を秘めている一方で、高度なAIが何の制約もなく反社会的な勢力に利用されれば、大きな害をなすことも想像できる。AIの積極的活用による日本経済の発展を目指しつつも、最小限であれ歯止めをかけるべきところには歯止めをかけるメリハリのある議論を望む。

・ AIを用いたSNS広告の投資詐欺や、偽サイトと気づかずに商品を購入した相談が多数寄せられている。消費者はAIを使ったサービスに対する期待度は高い反面、偽・誤情報による混乱の懸念がある。AIのアルゴリズムやモデルの透明性が高まれば、消費者はAIの判断を信頼し安全に利用できる。情報の真偽を峻別できる技術開発や、詐欺的なものに対する法的規制や救済手段が必要。

・ 現時点においては新法による規制は謙抑的であるべき。AI モデルの開発者に対して、リスク管理体制等に関する定期的な報告や重大インシデント発生時の報告を求め、国は責任をもって継続的にモニタリングする共同規制の枠組みが一案。AI 提供者と AI 利用者は、個別法や業法・規制法、製品・サービスに関する規格、AI 事業者ガイドラインによる規律に委ねる。ただし、国際的な枠組みとの整合性も踏まえた継続的な見直しや、事業者がインセンティブを感じられる認証制度を作ることも重要。

・ AIにより就職活動中の大学生が選別・評価される話をよく耳にする。AIが公平な判断を下していない、予測が正しいというエビデンスに欠けるという問題があり、アメリカでは州法レベルで規制立法が進んでいる。欧州も、AI法が雇用分野をハイリスクに分類して様々な規制をかけている。日本でもAIの利活用が盛んになっており、現在の実定法を遵守しているのか、ガイドラインをコンプライアンスしているのか心配。

・ 日本は広島AIプロセスなど国際的なAIのルール作りに主導的な役割を果たし、国内においてもAI事業者ガイドラインの作成など積極的な取り組みをしており、世界の中でもAIの開発や利活用がしやすい環境。現状でも改善すべき点はあり、AIの技術は常に進化するので、それに対応したルール整備が必要。また、AIのルール整備は国の将来を見据えた長期的な視点が必要。規制はインセンティブや活力を阻害してしまう面があるため、単なる規制だ

けではなく、AIの開発や利活用を後押しする制度も検討したい。

・サイバー攻撃者は、生成AIを使い、機械のスピードで攻撃を始めている。日本でもサイバー攻撃のリスクは顕在化しており、今年5月、生成AIを使い、ITのバックグラウンドを持たない若者がランサムウェアを作った容疑で逮捕された。また、米セキュリティ企業「ラドウェア」によると、生成AIを使えば脆弱性を見つける時間を90%短縮できる。IBMは今まで訓練用のなりすましメールを16時間かけて作っていたが、生成AIなら5分で作成可能だ。一方、守る側は人材不足が叫ばれ、ガートナーは2025年までにサイバーセキュリティ人材の半数が離職すると予想している。ゲームチェンジャーとなり得る技術だからこそ、生成AIやAIを活用して、人材の負担を減らし、防御能力を革新すべきだ。

・①基本原理の確保：法の支配や基本的人権の尊重など基本原理を現行制度で確保できているか、リスクが高く早急な手当てが必要なものがあるか。②国際的な相互運用性：各国で立法が相次いでおり、それらの制度の違いを前提としつつ、連携できる仕組みを整えることで実効性を持たせる。③AIの進展と規律密度のバランス：技術や市場の変化にある程度耐えられるように、政省令に加えて技術標準や規格などに委ねることや、数年ごとに見直す規定を置くなどのアジャイル・ガバナンスの導入。という3つの視点から検討したい。

・様々な専門家やユーザーが入って技術の運用を見守る「ヒューマンオーバーサイト」や、AIと人がチームとなって仕事をする「ヒューマンマシンチーミング」は、マルチステークホルダーによるAIのガバナンスを実現するために重要な概念。今回の議論においても、規制と技術発展のバランスを保ちつつ、人間とAIがどのように協調し共存していけるかという観点でヒューマンオーバーサイトやヒューマンマシンチーミングの議論が必須。

・あらゆる分野でAIのメリットを享受できる「AI-Poweredな社会」を実現する観点から、開発者、提供者、利用者など各主体が適切に利益を享受するためのルール形成と連動して、信頼できる高品質AIの開発・活用を戦略的に進めていくことが重要。また、AIの制度設計については、AIガバナンスの担保や法的課題への対応はもとより、AIの活用が人々の生活に与える影響についても広範に検討する必要がある。AI制度に関する相互運用性を確保す

る観点は非常に重要であり、国際的なルールの確立に関してもわが国がメインプレイヤーとして主体的に関与していくことが重要。

・ 初めの一歩として、守るべき価値が何かの確認が必要。ヨーロッパの場合は、人権、民主主義、法の支配が列挙されるが、それを日本も準じて行うのか、日本独特の価値を提唱するのか。また、他国・他地域で策定される様々な制度との整合性が喫緊の課題。中でも欧州評議会のAI国際条約は、現在、署名に向けたプロセスの準備が整っており、日本はどうするか議論すべき。また、公共調達も含めた政府のAI利活用に関するガイドラインもこれから議論すべき。

○ 続いて、松尾座長より、AI制度研究会座長および親会のAI戦略会議座長として、次の発言があった。

【松尾座長】

・ 昨年来、生成AIの急速な進化・普及に即応して、岸田政権は最善手を打ち続けており、大変素晴らしい。広島AIプロセスなど大きな実績をあげてきた。周回遅れだった生成AIの開発も、日本語性能で米国製品を凌ぐものが出てくるなど、追い上げが始まっている。
・ 今後も各分野で、AI利活用と開発力の強化を引き続き、強力に進める必要がある。そのためにも、技術と制度の両面からAIの安全性を高めることが重要であり、このAI制度研究会の立ち上げも、時宜を得た対応と思う。
・ 本日の合同会議に当たり、AI戦略会議の構成員からも、予め意見を預かっている。それを簡単に紹介すると、「世界的な制度議論を踏まえて、日本の実情に合った、国際的にも調和のとれた制度の期待」、「ソフトローの良いところは活かしながら、将来のリスクや有事にも実効性ある対応が取れ、モニタリングできる規律など、スモールスタートでもよいので、手遅れとならない制度的手当てが必要」、「AIの利用推進と同時に開発力も獲得して日本の国力を強化していくべき」など、今後の研究会での検討への様々な期待や意見があった。
・ 私としては、こういった議論が非常に早いタイミングでスタートできること自体すばらしいと思っている。AIの最先端の技術をこのように早いタイミングで日本が動けてきたことはこれまでにないと思う。一方で、AIの技術進展は非常に早いため、リスクへの対応とイ

ノベーション促進のバランスを取ることが重要。今が正に重要なタイミングだと思っており、ここでどのようなルールを作っていくのか、議論によってはよりよい社会あるいは国際的な競争力にうまく結びついていく可能性があり、非常に重要な議論の場だと思う。秋の中間取りまとめに向け、座長として貢献していきたい。

○ 最後に、岸田内閣総理大臣より締め括りの挨拶として、以下の発言があった。

【岸田内閣総理大臣】

本日は、熱心な御議論を頂き、誠にありがとうございました。

ただ今、松尾座長から大変心強いコメントを頂きました。日本政府として、昨年来、スピード感を持って、国際的なルールメーキング、国内事業者向けガイドラインの策定、そしてAIセーフティ・インスティテュートの創設や国際的なネットワーク作りなど、リスクへの対応を進めてきました。

私自身がお会いする他国の首脳やAI企業の経営トップから、頻繁に、「広島AIプロセス」について言及がなされるようになっています。「広島AIプロセス」で合意された国際的な指針等は、先進的なAIシステムに関する世界初の指針です。賛同国は50を超え、G7を超えて着実に世界に広がっており、信頼できるAIの実現に大いに貢献することとなります。

一方、国内におけるリスク対応も重要です。AIの安全性の確保が、AIの利活用促進、開発力強化のためにも不可欠です。我が国では、広範なAI関連事業者を対象とするガイドラインによって、柔軟かつ迅速に対応していますが、法制度の要否も含む制度の在り方の議論は、今日が、事実上のキックオフとなります。

これまで国際的なルールメーキングをリードしてきた我が国が、どのような制度を創りあげるか、世界が注目しています。

本日の皆さんの御意見も踏まえ、制度の在り方を議論するに当たって、次の４点が基本原則だと考えています。

１つ目は、リスク対応とイノベーション促進の両立です。ガイドラインをベースとしつつ、リスクの大きさに応じて対策を講じ、AIの安全性を確保する必要があります。

２点目は、技術・ビジネスの変化の速さに対応できる柔軟な制度の設計です。

３点目は、国際的な相互運用性、国際的な指針への準拠です。

４点目は、政府によるAIの適正な調達と利用です。政府の取組は、他への波及効果も大きいので、しっかりと検討を進めていきたいと思っています。

AIは、使われ方も多種多様で、技術革新のスピードも速いことから、先の予測も難しいですが、お集まりの専門家の皆さんの知見も集約し、世界をリードするような議論を進めていきたいと思っております。

本日は、誠にありがとうございました。

〇本会議終了後、構成員のみで、AI 政策の現状と制度課題について以下のような議論があった。

・これまでの日本のソフトローを中心としたAIリスク対応の良いところは活かして、イノベーションを阻害しないような形で十分配慮しつつも、現時点で想定し切れないリスクが将来顕在化する可能性を想定して、有事の際には実効性のある対応を取れるよう、また、海外事業者に対しても適切なモニタリングを行えるような法的規律の要否・程度について、多様な意見を集約して方向性を決めていくことが重要である。スモールスタートでもいいので、将来の技術や社会の急速な変化への対応が手遅れにならないように、法的な裏付けとしてのフレキシブルな土台となる制度的な手当てをしておく必要がないか、という観点を念頭に置くことで、より生産性の高い、かつ解像度の高い議論に繋がることを期待している。

・実際に国として、計算リソースの確保・利用促進・基盤モデルへの支援などがこの１年で積極的に実施されたのは非常にすばらしいと思う。これからは基盤だけでなく、その上で開発する人をいかに支援するかが政府にとって重要だと思う。

・利活用とリスクのバランスを考えていくことも重要であり、国際的な情勢や技術の発展が早い状況で互いに連携が必要な部分、独自で検討が必要な部分など切り分けしながら考えることは大事と思っており、その辺のバランス感覚が非常に求められる。

・技術に対して規制をかける話を議論する場合、FLOPsの値や特定の事業者・特定の部分だけの規制、あるいは促進したりということを決める場合は技術の定義を踏まえて、慎重に行かなければいけない。規制対象者という面では、国内外を踏まえて誰を規制するか、利用者の方に注目すべきなのか等も重要な論点だと思うので、その辺りも検討を進めていきたい。人の人生に重要な意思決定にAIを使うことに対する言及があったが、透明性と説明可能性に関してはAIのブラックボックス性に鑑みて技術的に可能な部分と不可能な部分がある。開発者や利用者の説明責任の議論の対象について、生成AIより前のAI技術も対象になるか生成AIのみが対象になるかは特に注意深く検討した方が良いと思う。

・公共調達というのはハードローでもソフトローでもない中央に位置するところで、かつ政府

自身のことであり、一つ取り組みやすい分野である。また、顔認証・顔認識関係のAIと公共調達に関しては活発な議論がされているが、生成AIなどは議論が低調な部分もあると感じている。その点、だからこそ切り込むべきポイントでもあると思うため、是非検討事項に入れて頂きたい。

・リスクのレイヤーごとに具体的に話をした方が具体性を持った指針が出せると考えている。また、リスクの種類やいろいろな角度の具体性もあるため、最初はそこを整理してから踏み込んだ議論をした方が具体な話になると思う。既存の法律や新しい法律、AIに特化せずに考えた方がいい法律がある可能性があるため、AIの特別な法律で抑えるべきかは一つの論点となる。AIの安全性に関する認証については、他の認証されている分野と進化のスピードが圧倒的に違うため、もし認証制度を設けた場合に保証できる期間の短さや国際整合性などの問題点が出てくる。実現性のある執行制度を考えるべき。

・今の既存の法律を遵守しているのかの点検やガイドラインを遵守しているかの確認等によって浮かび上がってきた不遵守に対しては、当然法執行等々をお願いしたい。不十分なところがあれば、監督の各省庁が一番その分野は詳しいため、立法論やガイドラインなどの俎上にのせていくことやその各分野で今の法執行で問題ないか、今後のあるべき姿を検討していただきたい。また、機械によって人を評価するというのは、人間の尊厳に反するという強い意見もヨーロッパを中心にあり、正確性をどのように担保しているのかが議論になる。人を評価する、特に人の人生に関わるようなことは尋常ではない為、透明性や説明責任の確保等の手間を掛けることが必要だと思う。AIの採用活動については動きが活発な点が多々見られるため、オーバーサイト、エビデンスに基づいて実際に遵守しているのかを見る必要がある。また、認証というのは事前の話だが、事後的に確認することも大事だと認識している。なお、採用活動におけるAI利活用のように、AIがヒトを評価する問題は、単なるプライバシーや個人情報保護法上の問題にとどまらない。AI利活用の不正確性や不透明性といった、個人情報保護法の射程を超えたAI特有の問題が含まれているので、AI特有な制度上の検討と対策が必要である。

・しかるべき機関からの監査も必要に応じて受ける義務を設けるのかなどの中間的手段を丁寧に見ていくことが重要。AI制度の考え方をより具体化し、どの範囲をハード・ソフトに切り分けまたは組合せをするかなどを考えていくのが、一つの枠組みになる。リスクや影響が大き

いAIとしては、①精巧な出力が可能で、何かあったときの影響も大きい高性能な汎用生成AIシステムと、②悪質な目的をもって作られるAIシステムが考えられる。また、生成AI以降の偽・誤情報、違法情報、場合によっては国家安全保障にも影響を与えるようなものの生成と流通をどう抑止するかなど、ハードローで押さえるべき点を特定できる作業が重要と考える。違法情報も対象となるが、偽・誤情報の問題をAIの文脈で考えるとしたら、それを流通するプラットフォーム側での対策をどう考えるかがポイントとなる。

・規制的なものは最小限の方が良く、基本的には利活用の方を中心に考えていくべきだというスタンスであるが、LAWSなどAIを活用した兵器などはそれなりの規制は必要ではないかと考える。偽情報や詐欺については必ずしもAI固有の問題ではないと考えており、AIを活用しなくても偽情報は作成可能であるため、こういった問題を全てAIの観点で必ずしも規制する必要はない。一方でAIによって容易になる事は事実であるため、バランスの取れた議論が必要である。

・生成AIによりフィッシングメールを簡単に作れるようになったが、AIだけの話ではないという論点はありつつも、他方でAIによって簡単にできるという話があるため、文章を作る生成AIを全部規制するとなると、対象としては広過ぎるという印象。音声や画像については、オレオレ詐欺に子供そっくりの声で掛けてくる詐欺は広がると思うが、例えば肖像権や個人情報などで対応できる可能性があるため、既存法も含めた慎重な検討が必要。AIはデュアルユースであり、アメリカでは安全保障やサイバーセキュリティ、モニタリングを迂回するようなAIが限定的に対象とされている認識である。安全保障やサイバーセキュリティに何らかの対策が必要と思われるため、現実的な落としどころになると考えている。また、日本は法制度としてAI開発などの面で良い環境にある。もしも、アメリカよりも厳しい規制にすると、日本で開発するメリットがなくなり、AIの開発面としては良くない状況になる。AGIのような何がリスクか予想できないものに関しては、法律のテクニックとしては見直し条項や時限立法という法律のやり方がある。例えば個人情報保護法は3年ごとの見直し条項が入っており、その時々で必要なものだけ必要な限度で適切なルールを作っていくことが重要。仮に規制をする場合、事業者ごとかモデルごとに規制するのかという論点がある。

・民主主義国家以外、例えば中国とかロシアとかの国々でどういう制度でAIが進められているのか、あるいはそういった国々でどれだけすぐれたAI技術が既に生まれているのか確認する必要がある。配布資料を拝見すると、欧米諸国におけるAI関連の動きがまとめられている。しかし、欧米以外の国々でもどのような制度や技術があるのか情報収集すべきではないか。

・ハードローによる規律は、少なくとも今の時点では謙抑的であるべきと思っており、日本の競争力に与える影響は非常に大きいと認識している。リスクがあるなら規制をした方が良いことではあるが、それによる副次的なマイナスの効果がどれぐらい大きいのかきちんと踏まえた上で規律を考えていくべき。汎用的なAIの開発者に対しては様々なリスクを検証させて、透明性を確保させることが必要だと思う。海外事業者にAI事業者ガイドランの説明をしたとき、ソフトローなのでペナルティは特にないと説明すると別の話題に意識が移る。メジャーなプレーヤーはソフトローでも遵守しているが、日本としてハードローなどの強制力を持って情報を出させるという観点も重要。また、真面目な企業ではソフトローでも努力して遵守しているが、頑張り損をしないような制度、枠組みを作った方が良いと考えている。例えば、第三者認証や補助金などを制度化して、一定のことを遵守していることに対しては認証を与えるなど。

・AIシステムのライフサイクルで、開発者・事業者・利用者を含めた全体の形で、どの部分にどのような体系の枠組みが必要かという議論も重要である。また、法制度としてある種の例外を作るのか作らないか、通常はディフェンスに関しては例外というのが各国のやり方だが、その辺のアプローチをどうするのか検討する余地がある。更にはハードロー/ソフトローのどちらに対しても、正しく執行されるかを確認する必要があり、オーバーサイトのストラクチャーを作るのかなど、政府も含めた議論が必要であり、ガイドラインがあれば大丈夫というロジックで進めてしまうと、喫緊のところでまた見直す必要になることを懸念している。

・どんな人でもチャレンジできる状況になっているのは、非常に良い事だと思うため、そこがより促進されるような形で、かつ、これがリスクだと明確に分かることがAIに手をつける人にとって大事だと考える。

・利用者はどういう視点で考えて利用していくかを見極められる力など、事業者だけではなく

利用者側の検討が必要。また、リスクを回避をするのは事業者や国・機関だけではなく、当然利用者も考える必要がある。

・仮に各国それぞれで認証制度が整備され、それぞれの認証のレベル感や方向性が異なると事業者の負担は増加するため、国際的な相互運用性を踏まえて慎重に進める必要があると思う。また、責任という面でAIの場合は開発者・提供者が引渡しの後にどこまで責任を被るかという議論が今後出てくると考えており、日本でもこの議論について一つのトピックとして入れた方が良い。

・いろんな意見で一度はその分野で精査されていることがこのように一堂に議論されたことは非常に価値の高いことだと思っており、この話の内容の粗筋自体が誰の目にも見える形で情報共有されることが極めて重要だと思う。

以上