2025 年 1 月 23 日

内閣府科学技術・イノベーション推進事務局
重要課題（社会システム基盤）担当　御中

「AI 戦略会議・AI 制度研究会中間とりまとめ（案）」に関する意見

AI 法研究会　政策提言部会有志*

（担当者）
阿部・井窪・片山法律事務所
AI 法研究会 政策提言部会 部会長
弁護士　柴山吉報

* 岡祐大、落合孝文、柿沼太一、春日舞、後藤大、近藤祥文、佐久間弘明、柴山吉報、鈴木淳哉、中崎尚、羽深宏樹、福冨友美、古川直裕、松本雄真、吉永京子ほか有志一同

「AI 戦略会議・AI 制度研究会 中間とりまとめ（案）」（以下「本とりまとめ」といいます。）について、以下の通り意見申し上げます。

Ⅰ はじめに

本コメントの作成主体である AI 法研究会政策提言部会有志は、AI に関する法や倫理を研究する任意団体である AI 法研究会において政策提言を行う政策提言部会所属のメンバーを中心にした、本とりまとめに対して提案がある上記研究会有志の集まりである。一度、有志各人においてコメントを検討のうえ、持ち寄り、議論をしたものであるが、個々のコメントは有志各人が作成したもの者であり、コメント間にみられる若干のニュアンスの違いは、上記のような作成経緯によるものである。

我々は、本とりまとめにおける「具体的な制度・施策の方向性」については、基本的に賛同する。すなわち、①既存法による対応を原則とするとの点は、個別具体的なリスクに着目し、AI か人の手かという手段ではなく、リスクや結果に着目した規制を行う（個別法アプローチ）という点で適切なものである。また、AI の技術進歩は早く、かつ AI の出力が予測しきれるものではないことから②政府司令塔を設立し、③重大インシデントに関する政府の調査権限を法律で定めることも適切である。④適正性を確保するための手法も、AI の個別事情により、適切な手法が異なることから、政府による調査権限を定めたうえで、サポートを行うものであり、法律で一定の手法の採用を義務付けるわけではないという点も、合理的なものである。⑤開発

者・提供者・利用者間の情報提供（透明性）については、「真に必要な範囲」に留めたうえで、政府による調査権限を定めるという方針であり、「真に必要な範囲」に留めるのであれば、適切なものといえる。

このように大きな点では、本とりまとめに賛同するものである。ただし、上記のような「具体的な制度・施策の方向性」に至る考え方や、比較的細部における考え方、本とりまとめが（専門的でないであろう読み手に与える）メッセージ性といった点について、提案がある。提案の詳細は、個別的なコメントをご覧いただきたいが、大きな点としては概要以下のとおりである。

① 政策の根拠の明確化

上記「具体的な制度・施策の方向性」が日本として最適な理由が分かりにくい。ある程度、知見のある者が読めばわかるが、EU やアメリカでの取り組みが「はじめに」で大きく取り扱われているため、「欧米が法規制を行うので、日本も遅れないように規制を検討する」ことが理由と、専門的でない読み手には読めてしまう。現に、本とりまとめに関する報道を見ても、欧米に追い付くというような基調が多く、誤解を生じさせている。さらに、欧州で AI 法が制定されたことは事実だが、アメリカでは AI を直接かつ包括的に規制する法律は連邦レベルでは存在しない。一部の議員による検討はなされているが、大きな動きとはなっていない。このような「世界は AI 規制に動いている」という誤解も、本とりまとめにより生じている可能性がある。

以上のことから、米国などの取り組みについて意味合いを詳しく説明することや、他国での取り組みはあくまで参考であることを分かりやすくし、あくまで日本の現状を考え最適な規制を提案するものだということを明確にすべきである。

② 意識調査の用い方

本とりまとめ 4 頁に記載されている意識調査から、日本において AI に対する不安の声が多く、諸外国と比べても開発・活用が進んでいないと判断し、AI の透明性・適切性確保が必要という結論を導くことは出来ない。

諸外国と比べて開発・活用が進んでいないのは、新しい技術に対する保守的な態度や、投資に対する否定的な態度などの別の要素が原因である。AI のリスクを理由に AI の開発・利用を行わないこともあるが、多くの場合は表面的な理由で、実際の理由は別である。

また、これらのアンケート対象者が適切な知識を持ったうえで回答しているのか疑問が残る。開発・活用が進んでいない日本では実際に AI を利用した人も少ないのだから、AI を十分に触ったことも漠然とした不安を抱いているだけという可能性もある。

③ 取り扱っている利益の偏り

本とりまとめで、取り扱っている AI のリスクや保護すべき利益が生成 AI に偏っている。本とりまとめが示す「具体的な制度・施策の方向性」は生成 AI 特有のものではなく、また AI の進歩は早く、生成 AI 以外の AI にも妥当するドキュメントとするためには、AI 一般を射程に置いた記載とすべきである。

④ 個別法アプローチの意義の明確化

本とりまとめは、個別法アプローチに立脚するものだと考えている。この点自体は、すでに述べた通り適切なものだが、この点が読み手によっては伝わりにくいこともあ

り、なぜ個別法アプローチなのか、個別法アプローチの意義をより明確化するべきである。

⑤　政府の人材調達

政府に司令塔を置くことや、調査権限を付与し情報収集することには賛成するが、これが適切に機能するには、当該司令塔なりに適切な人材が十分に存在することが前提となる。ここでは民間の人材の活用を含む形で広い意味での人材調達を述べている。このため、本とりまとめに、政府による人材調達について言及が不可欠だと考える。

なお、個別のコメントは以上の点に含まれない広範囲に及ぶものであり、以上の点だけがコメントの対象ではないことに注意されたい。

Ⅱ　具体的意見

1. 日本の法政策について（1頁総論）

EU域内ではアメリカと異なりAI産業が育っていないため、EUの政治的なアジェンダも踏まえて法律を作っている面もあるとの指摘がある。このように、各地域の法制度にはその地域の政治的アジェンダがあることを理解する必要がある。4頁目の意識調査は不安が全面に出ている結果となっているが、国の発展がない限り国民の保護は難しく、国としてどのようなプライオリティーをもってAIと向き合うか、政策をよく検討する必要がある。

また、AI活用人材の育成は重要であるが、博士レベルの人を育てるだけではなく、例えば日本が競争力を持っているエンタメコンテンツ生成でどうAIを使いこなすかといった教育も必須である。日本においては、著作権法において早い時期から機械学習を念頭に置いた規定を置く等の施策を行っているもののAI産業が育っていない現実があるため、そういった課題を踏まえた法制度の要否を検討すべきである。

2. リスクの記述について（2頁7行目以降）

ここでのリスクの記述が、不適切なコンテンツの作成・利用及び安全保障・セキュリティの内容に限定されており、中途半端な印象を与える。

AIのリスクは9頁に幅広に取り上げられており、また、公正競争も重要な政策アジェンダであるなど、その範囲は広い。

それらを全てに掲げることも困難だが、本とりまとめにおいて強調されている安全性（すなわち、医療機器・自動運転などに関する安全性（生命・身体の安全、狭義の安全性）のほか、プライバシー、知的財産権、環境等）について、もう少しバランスよく記述し、詳細は図3（9頁）を参照するなどの脚注を付すことはどうか。

3. CBRNの記載について（2頁9行目）

現状、CBRNの脅威がどの程度、テキスト生成AIで高まったのかについては疑問の余地がある。また、CBRNリスクのアセスメントには自衛隊による協力が不可欠であり、自衛隊の関与まで視野に入れていない現状ではCBRNは削除した方がよいのではないか。

4. AI Actの記載について（2頁13行目）

「AI Actは、４段階のリスクに応じたアプローチを採用し、」とあるのは、GPAI関係を考えると妥当ではないところがある。

「AI Actは、リスクを４段階に類型化し」に変更することが適切である。

5. SB942 の記載について（2 頁 30 行目）

(1) SB942 は Senate Bill、AB2013 は Assembly Bill で、法として成立する前の法案の名称番号であるため、正式名称を記載することが望ましい。

例：カリフォルニア AI 透明化法（California AI Transparency Act（SB942））、生成 AI トレーニングデータ透明化法（Generative Artificial Intelligence Training Data Transparency Act（AB2013））

(2) SB1047 は Veto で不成立になったことも、過剰規制への懸念という文脈で追加することが考えられる。

文案：「他方で、包括的な AI 規制を目指した SB1047 はイノベーションの阻害を懸念した州知事の拒否権が発動され成立しなかった。」

6. 我が国の取り組みの記載について（2 頁 31 行目）

我が国での取り組みが「広島 AI プロセス」から始まったような書きぶりだが、2016 年に G7 の議長国として提唱した「AI の研究開発に関する 8 原則」からそれが OECD の AI Principles にも寄与した点、総務省の旧ガイドライン（AI 開発ガイドラインと AI 利用者ガイドライン）、経済産業省の「AI 原則実践のためのガバナンス・ガイドライン」、内閣府の「AI 社会原則」の簡単な歴史も記載したほうがよい。記載しないと日本が 2016 年から既に取り組んできたにもかかわらず、米国と EU に遅れて対応したかのように世界に誤解を与えてしまい、もったいない。そのため、日本が以前から取り組んできたこと、G7、G20、OECD 等でリーダーシップをとってきたことをアピールすべきである（欧米の諸国は少なくともそれぞれアピールしており、日本はアピールが足りない）。

7. 諸外国の動向について（2 頁全体）

諸外国の動向について、バイデン政権下での動向に基づいて整理がなされているが、トランプ政権となった後に、大統領令の撤回等がなされる可能性がある。

本取りまとめ自体は政権移行後に最終的にとりまとめされるところ、パブコメ募集期間後にトランプ政権での初期的な対応があった場合には、その点についても背景事情の整理において記述される必要がある。

また、欧州と米国いずれについても同様の方向を見ているかのような記述となっているが、AI の一般法を制定し、運用していく方針の強さも圧倒的に異なる中であり、十分に精査した背景の整理が必要である。

8. AI に関する意識調査の結果の記載について（3 頁 14 行目）

(1) 日本での調査結果が無知や十分な情報（AI について何も規制していないというわけではなく、後述にもある既存の法令で対応できるものが多いほか、既存の法律も改正をしている現状）を周知されていない結果に基づくものである可能性があることが気になる。77%の人が「AI には規制が必要」と考えているから規制すべきというのは少々、乱暴な議論である。

(2) AI に関するリスクのみの記述になっているところ、AI の受容性に関する文化的背景を踏まえた場合、JIPDEC の調査
（https://www.jipdec.or.jp/news/pressrelease/20240418.html）でも現れているように、リスク・不安感だけでなく、期待感も強いことはファクトであり、不安一辺倒

ではないことを留意した記述が必要である。JIPDEC の調査内容も注記において指摘するのが望ましい。

9. 欧米を中心とする各国の AI に関する法制度の議論や検討の記載について（3 頁 18 行目）

(1)　欧米をはじめとする各国で AI 規制の議論や検討が進んでいるわけではない。EU だけである。アメリカをここに含めるべきではない。また、各国といっても韓国、ブラジル、カナダ程度であり、ごく少数である。あたかも多くの国が立法規制を検討しているかを記載すべきではない。そのため、「欧米を中心とする各国においては」を、「EU 加盟国など、いくつかの国では」に変更することが望ましい。

(2)　「欧米を中心とする各国においては AI に関する法制度の議論や検討が進んでいる」とあるが、明確に AI の包括的規制をしているのは EU だけである。米国の州や自治体レベルではあるものの、連邦レベルではそのような方向にはない（またトランプ次期政権ではさらに規制なしになると予測されている）。イスラエルは分野別に法規制をしているが、日本もその意味では分野別には既存の法の充当や法律の改正等はしており、日本が何もしていないという誤解を与えかねない。また、9 頁の表とも矛盾する。既存の法律で不足な点は何か、何に対応できていないか、AI 特有の性質への対応ができていない箇所は何かを精査すべきである。

10. 安全保障についての記載について（3 頁 27 行目）

安全保障についてのみ明確にスコープ外とされているが、実際には環境・公正競争・仕事の代替といった項目もスコープ外となっており、また、プライバシーや著作権の各論についても踏み込んでいるものではない。むしろ、本とりまとめは一般的なアプローチを記述したものであって、上記のような各論は全て別途検討されるべきであるという書き方にしてはどうか。

具体的には、「なお、」以下の文章を、「本とりまとめは、AI 制度の在り方に関する一般的なアプローチを記述したものであって、具体的な政策分野（安全保障・プライバシー・知的財産・公正競争・環境等）における AI の活用及びリスクガバナンスについては、関係省庁を中心に別途検討を進めることが必要である。」とすることが考えられる

11. 汎用型 AI の記載について（5 頁 7 行目）

生成 AI を一般的に汎用的というのは無理がある。日本で導入が進んでいるのは、自社に特化した生成 AI であり、これは汎用的と言えない。汎用的といえるのは基盤モデルであるため、「生成 AI」を「基盤モデルたる生成 AI」に変更することが望ましい。

12. 地理的な要因等の記載について（6 頁 20 行目）

「地理的な要因等からコンプライアンスの協力を得られにくい国外事業者に対しても制度の実効性」との点について、そもそもクラウド環境等において整備されたサービスの関係では、そもそも現場での指図・指示ができるか否かというより、その協力要請について、それを拒絶し得ないようなインセンティブ又はディスインセンティブが設定されているかが重要である。AI の文脈においても、地理的要因を国内外の差異の主たる論拠とされるようであれば、本当に対処すべき課題を見失うおそれがある。この点は、制裁制度や、執行協力その他の制度的な問題により、日本の制度を無視することもリスク管理の観点で

合理的な場合があることを是正する必要がある、という論点であることに留意すべきである。

そのため、「地理的な要因等から」を「法制の差異や制度的な要因等から」へ修正することが望ましい。

13. 国際整合性の記載について（7 頁 26 行目）

「国際整合性の確保や安全性評価や認証の実施」が重要であることは異論はないものの、既に EU では独自の整合規格が検討され、カルフォルニア州でも透明性に関する法律が成立し、中国も生成 AI について独自の法律が存在しており、整合性、評価手法の統一をいつまでも待っていては、国としての競争力が更に低下するため、この記載が現実的か否か疑問である。

14. 規制を伴わない法令の記載について（8 頁 29 行目）

「規制を伴わない法令」の趣旨が不明確であるため、「制裁を伴わない法令」「基本方針のみを定めた法令」など、より分かりやすい表現に修正することが望ましい。

15.「AI のもたらし得るリスクの例に関する整理」（図 3）について（9 頁図 3）

(1) 「AI のもたらし得るリスクの例に関する整理」についてより具体的にすべきである。例えば、「主要法令等」は「関連する主要法令」または「適用可能な主要法令」とする等の修正が考えられる。また、タイトル自体は、「AI のもたらし得るリスクの具体例と現行法上適用可能な法令」等とするなど、関係性を明確化すべきである。

(2) 「AI の開発・利用の過程でのプライバシー侵害・個人情報保護違反」の項目について、個人情報保護委員会における中間整理では、同意無しでの利用が公益に資する可能性を議論するものであり、リスクに対処するというよりは、広く研究開発推進の観点を持って特例の整備をしようとするものと理解できるため、かかる方向性を踏まえて記載を修正すべきである。

(3) 「ディープフェイク（AI で合成した肖像・声等の悪用）」の項目について、ディープフェイクや偽・誤情報に関しては、発信者情報開示との関係でプロバイダ責任制限法も関係するのではないか。

(4) 「人間と AI の負の相互作用」については、「AI への過度な依存」といった表現も考えられる。

(5) 「人間と AI の負の相互作用」や「人間と AI の負の相互作用」や「AGI が制御不能になる懸念」について、何らの法制度が関係しないとされている点は事実認識に誤りがある。ハルシネーションにおいて、民法（不法行為、契約）と記載されている項目と同様に一般的な法理の適用がある。自動運転において 3 省の SWG で議論がされたように、仮に従来のサービス提供主体のような者が関与しない場合に、開発者に直接責任追及をできるような環境があるか、もしくはその考え方を修正するか、さらに注意義務としてどのような内容を開発者ないしサービス提供者に求めるか、少なくとも何らかの行政等での報告書や裁判例が出るまで不明確であるというにすぎないので、その点の誤解が生じないようにする必要がある。

(6) 図 3 に記載のないリスクの例として、AI からの個人情報の出力といったものも考えられる。

(7)　図3について、データセットへの広範なアクセス権限、AI技術・人材の囲い込み、莫大な資金が不当に集中されることを防ぐための独禁法、競争法の観点を追記してはどうか。

16. 法令による規制の記載について（10頁10行目）

「法令とガイドライン等のソフトローを適切に組み合わせ、基本的には、事業者の自主性を尊重し、法令による規制は事業者の自主的な努力による対応が期待できないものに限定して対応していくべきである」との記載は具体的な行為義務の整備に関する考え方としては合理的である。一方で、個別具体のリスク対策等はともかく、一般的な改善を目指すための取り組みに対する実効性が十分でない場合には、自主的な取り組みにおいて、インセンティブ又はディスインセンティブを設定するための、根拠となる法令の整備が必要となることもあることに着目も必要である。そのため、「法令による規制」を「法令による行為規制」と修正するのが望ましい。

17. 法令の枠組の記載について（10頁14行目）

我が国の法令においては、むしろ文言解釈の幅が必ずしも広くなされない場合がある。単に既存の法令の枠組みを活かすだけであれば、利用を制限・抑止する結果になる場合があることに留意すべきである。前提となる我が国の法制の認識として、新しい技術を当然に利用できるような技術中立性を意識した法整備は必ずしも十分に進んでおらず、デジタル技術一般の採用も遅れた状況を直視するべきである。そのため、「既存の個別の法令の存在する領域においては、AI が各領域で様々な用途で利用され始めており、権利利益の保護の必要性が生じる場面も AI の用途に応じて異なることから、まずは当該法令の枠組みを活用しつつ対応すべきである。」との箇所であるが、「当該法令の枠組みを活用しつつ、AIの適切な利用を推進するような見直しも進めつつ対応するべきである」と修正するのが望ましい。

18. 線引きの記載について（10頁20行目）

「何が規制の対象となり、事業者の活動はどこまで許容されているのかといった線引きを明確化すること」とあるが、法律によってそのような点を明確に線引きすることは困難である。そのため、（規制の対象等について）「線引きを明確化すること」ではなく、「事業者の予見可能性を可能な限り確保する」といった現実的な表現に改めるべきである。

19. 規制の記載について（10頁21行目）

「その際、政府と事業者との役割分担を意識した上で、何が規制の対象となり、事業者の活動はどこまで許容されているのかといった線引きを明確化することが重要である。」という点について、あらかじめ規制を行うことが重要であるとの誤解が生じないようにすることが重要である。既存の法令において、解釈が曖昧であり禁止をしている趣旨とも捉える事業者がいるような規制領域において、解釈の明確化を行うことは本項目で議論しているような方向性での意味合いがあるものの、一方で、単に新たに規制を設定することになるような趣旨の明確化は新たな取組の振興との関係では阻害的効果があることに留意が必要である。

20. スタートアップ企業の記載について（10 頁 25 行目）

「スタートアップ企業も含め、どのような規模の事業者であっても対応可能なものとなるよう」との点について、基本的な方針としては理解できるものの、どのような規模の事業者もと記載した場合に 1-2 名程度の事業者でも対応できる規制を整備することまで意図するとすれば、政策的なツールを予め絞りすぎることにはならないか。規制対象について適切な検討を行ったうえで、「スタートアップ企業も含め、様々な事業者が合理的に対応可能なものとなるよう」と修正するのが望ましい。

21. 基盤サービス等の記載について（11 頁 5 行目）

「国民生活や経済活動の基盤となるインフラやサービス等（以下「基盤サービス等」という。）や製品安全に関する AI」の指し示す範囲が不明である。サイバーセキュリティ、経済安保、その他複数の規制、政策の関係でこのような基盤サービス等に類似するような重要性のあるサービス等は特定されている例があるが、どの範囲を指し示そうとするか不明確である。このような基盤サービス等に関して「各業所管府省庁により既存法等を中心とした対応がなされる」とされているが、一般的には重要インフラ等は個別規制が存在する範囲の一部であり、理解に誤りがあると思われる。基盤サービス等の想定内容を記載するとともに、基盤サービス等に限らず、既存の政策、規制と関係がある内容で AI を利用しようとする場合には、所管府省庁が既に対応を行ってきていることを示すべきである。

22. 「民主的行政責任」について（11 頁 21 行目）

「民主的行政責任」という言葉が耳慣れず、また、広島 AI プロセス等でも使用されている形跡が見られない。たとえば、2024 年の G7 イタリア閣僚宣言（https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document07_en.pdf）では、"rule of law, due process, democracy, human rights"という表現が使われており、そちらに寄せた方が良いのではないか。具体的には、「民主的行政責任」を「民主主義及び人権」に改めることが考えられる。

23. 条約名の記載について（12 頁 9 行目）

「人工知能 （AI）と人権、民主主義及び法の支配に関する欧州評議会枠組条約」 （仮称）とあるところ、あたかも英文の条約名自体が仮称であるかのような印象を受ける。実際には和訳名が仮称であるとの趣旨と思われるが、誤解を招くので記載を修正すべきである。そのため、（仮称）を脚注に落とし込むべきである。

24. ISO の活動の記載について（12 頁 28 行目）

ISO の活動として、2023 年 12 月 18 日に国際規格「AI マネジメントシステム（ISO/IEC 42001）」として発行されたことを脚注等において指摘することが望ましい。

25. 政府の司令塔機能を強化の記載について（13 頁 13 行目）

「研究開発から経済社会における活用までの一体的な施策を推進する政府の司令塔機能を強化すべきである。」について、例えば、新保史生「AI 規正論」総務省 学術雑誌『情報通信政策研究』 第 7 巻第 1 号では、 「民間部門とともに公的部門による AI の利用についても監督を行うための組織として、国家行政組織法第三条に基づくいわゆる三条機関（委員会）として、「AI 規正委員会（仮称）」の設置を提案」している。

26. 司令塔機能の強化の記載について（13 頁 16 行目）

「司令塔機能の強化に際しては、広く関係府省庁が参加する政策推進体制を整備する必要がある。」との箇所については、そもそも司令塔機能が政府にあることは広い意味での役割分担として適切であるが、具体的な技術、事業の知識が政府には欠ける。その中で、省庁間協議の実質しかない本部を設置しても、実効的なマルチステークホルダーの議論を喚起するための戦略的機能の発揮は困難であり、民間の力の活用も十分に論じられるべきである。

また、関係行政機関に協力を求めることを記載しているが、不十分である。法令上の記載としては関係行政機関への協力要請が記載しやすいことはわかるが、どのように民間の協力を得られるようにしていくか、十分に議論し、当初の仕組みの整備の時点から組み込むことが重要である。努力義務等の方法も含めて、既に民間に協力を求めるような基本法等もあり、それが実運用されている事例などを参照していくべきではないか。

27. 透明性及び適正性の確保の記載について（13 頁 26 行目）

「研究開発」段階から透明性の確保が必要であると読めるが、開発した AI をリリースする時点で初めて利用者に対するリスク対応が必要になるため、およそ研究開発一般について透明性及び適正性の確保を求める必要はない。また、研究開発段階ではあえて「リスクの高い AI」を研究することもあり得、このような研究への萎縮効果を生じさせるべきではないこと、及び研究開発の内容は企業の機密にも関わることであることからすると、およそ研究開発一般について透明性及び適正性の確保を求めるべきではない。そのため、「研究開発から活用までのライフサイクル」という表現を、「開発した AI の公開から活用までのサイクル」等に変更し、研究開発についての記載を削除すべきである。

28. 開発時点の記載について（14 頁 3 行目）

利用者は、テスト導入等の方法でリスクを判定することができる。実際のところ、開発者によるシステムカードなどの形での情報開示よりも、テスト導入などの方法の方が、はるかに実際の環境でのリスク評価ができる。このため、あくまで「開発時点での」リスクについて言及しているものと理解する。そのため、「「開発段階に関する」リスクに対応するにあたっては、このようなリスクに係る必要な情報を関係者に適切に共有しなければ、誤った認識で AI システムを提供者が利用者に提供し、あるいは利用者が不適正に AI サービスを利用し、リスクが顕在化する可能性がある。」に変更すべきである。

29. 適正性の記載について（14 頁 14 行目）

適正性については、既に AISI でも意識されていると思われ、また偽・誤情報の関係でのコンテンツモデレーションでも利用がされているような、コンプライアンスやスクリーニングに関する自動化に関する考察がされていくことが極めて重要である。実際には、多くのデータや AI による判断をすべて人間の手で行っていくことは現実的ではなくなるのであり、人間の関与により是正できる機会の確保も重要である一方で、AI の開発・利用の中にコンプライアンスの自動化に即した取り組みを入れていくことが重要である。この意味ではセーフティ・バイ・デザインないしコンプライアンス・バイ・デザインのような観点を持って、適正化について、様々な主体が合理的に取り組めるように検討を進めることが重要ではないか。

30. 透明性の確保を含む適正性の記載について（14 頁 20 行目）

「透明性の確保を含む適正性」とあるが、本節では透明性と適正性が並列に論じられてきているので、この箇所だけ包含関係で説明するのは違和感を覚える。そのため、「透明性及び適正性」に修正すべきである。

31. 国内外の組織が実践する安全性評価と認証に関する戦略的な促進の記載について（15 頁 1 行目）

「② 国内外の組織が実践する安全性評価と認証に関する戦略的な促進」を達成するためには、新保史生「AI 規正論」『情報通信政策研究』 第 7 巻第 1 号において「日本版 AI システム適合性評価制度」構築に向けて必要な検討事項や構成要素が示されていることから参照すべきである。なお、2024 年 8 月 23 日第 2 回 AI 制度研究会の松尾剛行弁護士の資料（https://www8.cao.go.jp/cstp/ai/ai_kenkyu/2kai/shiryou5.pdf）p.29 にも同論文が参照されている。

32. リスク評価の記載について（15 頁 6 行目）

「組織内外の専門家チームや評価用のツールなどを使って、基本的には自らリスク評価を行い」との箇所について、実際のリスク評価や専門家起用のコストも考慮して制度や推奨事項の整理がなされていくべきである。例えば AISI 等がツールを開発し、それにより社会コストを低減させようとする仕組みは評価できる。一方で、ISMAP などもそうであるが、日本においては過度に細かい要件と、高額な監査費用を要求する、我が国独自の仕組みが整備され、国際的な相互運用性も失われる事案が少なくない。このような観点で、費用対効果や、既に本文において考慮する方針が示されている、各国との相互運用性の確保を意識して議論がなされるべきである。この際に、規制や認証の枠組みを単に最も規制が厳しい国・地域等に合わせることは、最終的に国内事業者の競争力強化に繋がらないことは留意するべきである。

33. 安全性の記載について（15 頁 17 行目）

AI 時代における自動運転車の社会的ルールの在り方検討サブワーキンググループでは、民事・刑事責任とも関連して、道路交通法のデジタル化や保安基準の整備、事故調査制度などを議論しており、海外にも紹介する本報告書においては、言及をすることが重要である。脚注に上記会議のとりまとめリンクを追記することが望ましい。

34. 政府による情報収集の記載について（15 頁 31 行目）

(1)　国による情報収集は望ましいところである。しかし、いくら情報を収集してもそれを適切に分析できる人材が十分に存在しないと無意味である。このような政府の人材の確保・育成に触れるべきである。

(2)　重大インシデントに関する情報収集は各省庁が行うべきで、省庁間でも AI インシデント情報を共有する体制が必要。省庁横断的な AI インシデント情報共有体制として、日本では例えば内閣サイバーセキュリティセンター（NISC）の機能を拡大することも考えられる。（参考：Jason D. Schloetzer, Kyoko Yoshinaga, Algorithmic Hiring Systems: Implications and Recommendations for Organisations and Policymakers, YSEC 2023- Law and the Governance of Artificial Intelligence, Springer, 2024, p.239、古川直裕・吉永京子「責任ある AI とルール」（KINZAI、2024 年）p.275-277）

35. AI の利用の記載について（16 頁 6 行目）

「AI の利用に起因する重大な事故が実際に生じてしまった場合、政府としては、その発生又は拡大の防止を図るとともに、AI を開発・提供する事業者による再発防止策等について注意喚起を行っていく必要がある」との点については、そもそも AI 利用に関する具体的に求められる対応が明確ではない。その中で個別事業者に後付で注意喚起をしていった場合に、AI 利用に関する強い抑制的効果が生じる可能性がある。この点、最小限、どのような目的での事故情報共有等の制度であるか趣旨を明確にし、またその対象となる権利・利益の保護を念頭にしたものかを明らかにすることは最低限必要である。そのうえで、実際の注意喚起に当たっても、一方的に政府が公表することが適切か、例えば繰り返し同様の事象を起こしており改善が見込まれない場合や、対話に応じないような場合を念頭に置くなど、運用におけるインセンティブ設計にも着目した議論が重要である。

36. 「この調査や情報発信は事業者の協力なしでは成り立たないため・・・」との記載について（16 頁 14 行目）

「この調査や情報発信は事業者の協力なしでは成り立たないため・・・法制度による対応が適当である。」との点について、関係者の範囲も明確ではなく、どのような主体のどのような協力を求めるか不明確である。情報の収集にあたり、個人情報保護法や不正競争防止法など法令レベルでの整合性確保もさることながら、真に競争環境に悪影響を及ぼす情報を政府が早期公開等を行わないよう手当が必要である。

実際の AI 開発・利用に関わる国外も含めたプラットフォームへの情報の蓄積が進んでいるが、協力を求めても、法令上の要請を定めただけという我が国の協力要請依頼には、事業者によっては十分に応じない可能性があることも留意が必要である。本頁に限らず、民間事業者という場合に、ベンチャー企業等の小規模事業者の合理的かつ実効性のある協力を求められるようにする観点の反面で、超大規模国際事業者への対応も重要課題となることに十分に留意されたい。

37. 政府調達の基準の記載について（16 頁 22 行目）

政府調達の基準に AI リスクの概念を導入することは望ましい。この部分の記述自体には賛同するが、政府の調達先が下請企業などにも、合理的な範囲で AI リスクへの対応を求めることによるトリクルダウン的な AI リスク対応の広がりにも言及することが望ましい。近しいものとしては、下請け・孫請けにも求める暴力団排除など。

38. 政府等による利用の記載について（17 頁 9 行目）

記載内容自体に異存はない。民間の AI 利用を促進したければ、まず政府から利用を活発に行うべきであるという、隗より始めよという点を追加し、政府の AI 利用をより強く推奨すべきである。

39. 各自治体の先進的な取組 の記載について（17 頁 17 行目）

注釈 11 について、港区では AI による沢山の事例があるため、港区情報政策課に問い合わせるとよい。（参考：古川直裕・吉永京子「責任ある AI とルール」（一般社団法人金融財政事情研究会、2024 年）p. 177, 188）

40. 機密性 2 情報の記載について（17 頁 24 行目）

「機密性 2 情報」という用語は一般になじみがないため、括弧または注釈等において説明することが望ましい。注釈に、「組織内では開示・提供が可能だが、第三者には開示・提供ができない情報」と記載することなどが考えられる。

41. システミック・リスクの記載について（18 頁 6 行目）

2 頁の AI Act のシステミック・リスクと同じ用語であるが、両者の意味が異なっている。AI Act の用語法が一般的ではないことは理解しているが、変更できないもののため、こちらのシステミック・リスクを関連システムに波及するリスクのような「こなれた」日本語にするべきである。

42. 「現時点においては…検討すべきである。」との記載について（18 頁 9 行目）

「現時点においては…検討すべきである。」は当然のことであるが、むしろこれが冒頭でも強調されるべきである。全体を読むと、諸外国が法制度対応しているから日本でもしなくては、というトーンが強すぎて、主体性を感じない。

43. 「諸外国においては、AI に関する制度整備が進められているなか」との記載について（18 頁 23 行目）

「諸外国においては、AI に関する制度整備が進められているなか」と書くと、主体性が感じられない。諸外国がやっているから我が国でもというのはよくなく、日本で対応できていないリスクがあればそれに対応すべきである。よって、既存法の精査が必要である。ここでは、例えば、「諸外国においては。AI に関する制度整備が進められているなか」を削除する。

44. 適正手続きの記載について（19 頁 6 行目）

「適正手続き」を「適正手続」としたほうがよいか。

45. 英訳について（全体）

今後、英訳は速やかに、諸外国からもすぐに認知してもらえるように公表していただきたい。また、いつまでも「仮訳」(tentative)としないほうがよい。（諸外国からよく「tentative ということで確定していないのではないか」という指摘を受けるため。）

以上