「人工知能関連技術の研究開発及び活用の適正性確保に関する指針（案）」に対する意見書

意 見 書

令和 7 年 12 月 11 日

内閣府
科学技術・イノベーション推進事務局　人工知能政策推進室　宛て

〒105-0001 東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー5 階
一般社団法人新経済連盟　代表理事　三木谷浩史
TEL：050-5835-0770
E-mail：info@jane.or.jp
（連絡担当者：大室）

「人工知能関連技術の研究開発及び活用の適正性確保に関する指針（案）」に対する意見書に関し、別紙のとおり意見を提出します。

別紙様式

章・節	該当ページ	行番号	該当する記載	ご意見
1(2) 本指針における適正性確保の考え方	3	1-3	適正性確保に当たって、適正性についての一義的な定義や絶対的な水準を定めるものではなく、各主体が研究開発、活用するAIの特性、用途、目的や、自身の立場、社会的役割等を踏まえて自主的に取組を進めるという考え方	自主的に取組を進めるという考え方に賛同する。他方で、こうした考え方であれば、産業界との協働は不可欠。今回の意見募集は約1週間という短期間だが、任意の意見募集手続であるとしても、このような短期間で産業界の声を十分に把握することは困難。産業界の声をより広く反映できるよう、1 か月等の十分な意見募集期間等を設定頂くことを望む。さらに、今回の意見募集に先立ち、11/21-27 まで「指針骨子」のパブリックコメントが行われ、その結果概要が 12/5 に公表され、今回の意見募集が行われたと承知しているが、本来であれば前者の手続を経て「指針骨子」がどのように変更、具体化され、「指針（案）」に反映しているかが明らかとされる必要がある。加えて、脚注 13 等、具体的な記載がなく評価が難しい記載も散見され、このような点も含めて産業界から的確・適切に意見提出を行うことが困難。こうした事情を踏まえた適切な手続の実施を望む。
1(2) 本指針における適正性確保の考え方	P3	２５行目～２８行目	セキュリティ 不正な操作によるAIの意図しない動作や停止をはじめとするAIのセキュリティ上のリスクを低減させるよう、AIのセキュリティを適切に確保すること。	1(2)「セキュリティ」において、「不正な操作による AI の意図しない動作や停止をはじめとする AI のセキュリティ上のリスクを低減させるよう、最新のセキュリティ技術によって AI のセキュリティを適切に確保すること」等の文言に変更することを要望する。 【理由】 AI によって、大量の個人情報や機

章・節	該当ページ	行番号	該当する記載	ご意見
				密情報が取り扱われているが、サイバー攻撃は年々多様化・高度化してる。このような状況下では、機密性の高い情報が流出するリスクが高まるため、最新技術による高度なセキュリティ対策を指針においても言及することが重要。この点、EU AI Act 第 15 条では、AI システムに対する適切な堅牢性とサイバーセキュリティの確保が要求されており、HAIP を牽引し、AI ガバナンスの構築において国際協調を図る趣旨からも最新のセキュリティ対策への言及が必要。
1 (2) 本指針における適正性確保の考え方	P. 4	1-3	プライバシー 1 取り扱うデータの重要性等に応じてプライバシーを尊重し、適切に保護すること。	1(2)「プライバシー」において、「取り扱うデータの重要性等に応じて最新のプライバシー保護措置等の技術的手段によりプライバシーを適切に保護すること」等の文言に変更することを要望する。 【理由】 昨今、AI の急速な発展に伴い、プライバシー保護に関する懸念も出ています。AI の活用時は、大量の個人情報や機密情報等が処理されるため、当該情報の処理過程において技術的な保護措置を講ずる必要がある。この点、国際的には、プライバシー強化技術(PETs)が実用化されており、EU AI Act 第 10 条第5項(b)では、高リスク AI において、特別なカテゴリーの個人データには「最新のセキュリティ及びプライバシー保護措置」が求められてる。1(1)「本指針の位置付け」でも言及されているとおり、「広島 AI プロセス」を牽引し、AIガバナンスの構築において国際協調を図る趣旨から、最新

章・節	該当ページ	行番号	該当する記載	ご意見
				のプライバシー保護措置への言及が必要。
1(3) 適正性確保のための基本方針	P4	28	脚注 8 レッドチーム等の様々な手法を組み合わせて、多様な内部テスト手段や独立した外部テスト手段を採用することや、特定されたリスクや脆弱性に対処するための適切な措置を実施することが望ましい。	ここで触れられているリスクは P.4 にて分類される要素の中で「セキュリティ」を中心に記載されているように思料する。 個別リスクへの対策方法については脚注に記載するのではなく、本指針の中ではリスクベースでのアプローチにとどめ、固有のリスク事項への対策方法については別途まとめるなどをご検討いただくのが良い。
2 研究開発機関及び活用事業者が特に取り組むべき事項	P.6	2-4	AIを活用した製品、サービスの開発、提供をする活用事業者 10 は、その開発、提供したAIが多くの主体に影響を及ぼし得ることを踏まえ、国際的な規範、国際規格、各種ガイドライン等を活用しつつ、1(2)に示す適正性確保に必要となる主な要素に関して、特に以下の事項に取り組む。	本指針はAIガバナンスとリスクベースアプローチを基本方針とするが 、適正性確保を名目とする過度な規制や厳格なプロセス要求は萌芽的な研究開発を実質的に阻害する問題を含んでいる。AI 法が研究開発の推進も目的としていることを踏まえ、指針の運用においてはリスク管理とイノベーション促進のバランスが重要である。初期段階の探索的活動に対し、適度な失敗を許容する柔軟性を考慮いただき、長期的・破壊的なイノベーションを生む土壌も確保する旨を検討いただきたい。

章・節	該当ページ	行番号	該当する記載	ご意見
2 研究開発機関及び活用事業者が特に取り組むべき事項	P.6	2-4	AIを活用した製品、サービスの開発、提供をする活用事業者 10 は、その開発、提供したAIが多くの主体に影響を及ぼし得ることを踏まえ、国際的な規範、国際規格、各種ガイドライン等を活用しつつ、1(2)に示す適正性確保に必要となる主な要素に関して、特に以下の事項に取り組む。	開発者と提供者に課される内容は分けるのが現実的ではないか。開発事業者はある程度大手で体力があると想定されるところ、提供事業者は中小やベンチャーレベルの企業も多数あると想定され、かつ当該事業者でコントロールできる範囲が限定的であることから、提供事業者に課される内容は軽減し活発な利活用へ誘導する方が便益の最大化に繋がるのではないか。
2(2) ステークホルダーとの信頼関係の構築に向けた透明性の確保	P.6	19	脚注 13 「内閣府ウェブサイト参照（国内外のＡＩに関する規範、ガイドライン等を示す予定）」	脚注 13 「内閣府ウェブサイト参照（国内外のAIに関する規範、ガイドライン等を示す予定）」とあるが、具体的な記載がなされていない脚注については、評価することは難しい。

章・節	該当ページ	行番号	該当する記載	ご意見
2(3) 適正性確保のための基本方針	P7	6行目～14行目	(3) 十分な安全性の確保 AIを悪用したサイバー攻撃や詐欺をはじめとする各種犯罪、違法行為が行われる 7 リスクを特定・評価し、適切な対策を講じる。 また、ハルシネーションや偏見・差別の助長、偽・誤情報等（ディープフェイク技術によるフェイク動画、性的加工画像等）の拡散等につながるAIによる不適切な出力の抑制、AIの意図しない動作や誤作動の防止をするため、最新の技術と知見を駆使して、解決、改善に向けて取り組む。特に、AIで生成された偽・誤情報等の拡散 12 が深刻なリスクとなっていることを踏まえ、AIの生成物であることが判断できる技術（電子透かし、API 等）の開発に努め、必要に応じて実装する。	2(3)「十分な安全性の確保」において、「最新のセキュリティ技術と知見を駆使して、解決、改善に向けて取り組む」旨の内容を盛り込むことを要望する。 【理由】 AI によって、大量の個人情報や機密情報が取り扱われているが、サイバー攻撃は年々多様化・高度化してる。このような状況下では、機密性の高い情報が流出するリスクが高まるため、最新技術による高度なセキュリティ対策を指針においても言及することが重要。この点、EU AI Act 第 15 条では、AI システムに対する適切な堅牢性とサイバーセキュリティの確保が要求されており、HAIP を牽引し、AI ガバナンスの構築において国際協調を図る趣旨からも最新のセキュリティ対策への言及が必要。
2(3) 十分な安全性の確保	P7	12-14	「特に、AIで生成された偽・誤情報等の拡散が深刻なリスクとなっていることを踏まえ、AIの生成物であることが判断できる技術（電子透かし、API 等）の開発に努め、必要に応じて実装する。」	事業者が画像生成サービスを提供する際には、電子透かしの実装をすることを求める記載が追記されているが、この記載を短期間のパブコメにて行うべきかは、議論の余地があると考える。
2(5) AIのイノベーションの基盤となるデータ	P7～P8	P.7 21行目～P 8 5行目	(5) ＡＩのイノベーションの基盤となるデータの重要性を踏まえたステークホルダーへの配慮 ＡＩのイノベーションに	2(5)「AI のイノベーションの基盤となるデータの重要性を踏まえたステークホルダーへの配慮」において、「データ保有者が安心してデータを提供できるプライバシー及びセキュリティ

章・節	該当ページ	行番号	該当する記載	ご意見
の重要性を踏まえたステークホルダーへの配慮			は、質の高いデータを確保し、それらを適正に活用することが重要である。これを踏まえ、質の高いデータが充実し、信頼できるＡＩが開発、提供されることにより、新たな創作活動等が促進されるという好循環を実現するため、ＡＩを開発、提供する事業者は、データの利用状況に応じて、知的財産等のデータ保有者等のステークホルダーと、データの適正な活用の在り方等について継続的なコミュニケーションを図る。また、特に、社会的影響力の大きいＡＩを開発、提供する事業者は、知的財産等のデータ保有者等に対する利益還元のエコシステムや安心して創作活動ができる環境の構築に向けた方策の検討、実施に努める。	基盤の整備に努める」旨の内容を盛り込むことを要望する。 【理由】 本指針案では、データ保有者等との継続的なコミュニケーションやデータ保有者等への利益還元のエコシステム構築等、データ保有者等への配慮について言及されてるが、質の高いデータの確保と適正な活用を実現するためには、データ保有者が安心してデータを提供できる技術的基盤の整備が不可欠。 さらに、日本が HAIP を主導する立場として、データ活用における技術的プライバシー保護措置の重要性を指針に盛り込むことは、国際的なリーダーシップの発揮にもつながる。
2(2) ステークホルダーとの信頼関係の構築に向けた透明性の確保	P7	26	脚注 18 「学習データの開示が求められた際はその必要性を判断して適切に対応する」	学習データの開示を受け付けることは消費者保護の観点から理解できるが、事業者が開示を求められた際の手続きについて脚注で触れることは、本文にある「合理的な範囲で説明可能性を確保する」の意図を狭める記述と見受けられる。
3 国及び地方公共団体が特に取り組むべき事	P9	2-7	国は、1(2)に示す適正性確保に必要となる主な要素に関して、特に以下の事項に取り組む。	指針2（5）は AI のイノベーション基盤として質の高いデータの適正な活用を重視すると指摘（P.7）。AI のエンドユーザーである国民・事業者にとっても、国民・事業者の自己デー

章・節	該当ページ	行番号	該当する記載	ご意見
項			地方公共団体は、1⑵に示す適正性確保に必要となる主な要素に関して、置かれた環境や課題が多様であることを踏まえ、地域の実情に応じて、特に以下の事項に配慮しつつ、必要な対応を行う。 なお、AIを開発、提供する際は、2に示す事項についても取り組む。	タ活用により個別化されたサービスや検証を受けることは極めて重要。政府は医療・金融などの自己データを適切に連携し、AI サービスにインプットする仕組みを整備すべきであり、これは AI の適正利用と国民の権利保護に不可欠。既に「データ利活用制度の在り方に関する基本方針」（令和7年6月デジタル行財政改革会議決定）で、公共性の高い重要分野でのデータ連携・相互運用性確保が謳われている（P.3）。これを受け、本指針「3」に「国民や事業者が自己に最適化された AI 活用を可能にするための自己データ取得環境等の整備」といった項目を追加し、政府の責任で API 等による安全かつマシンフレンドリーな自己データの収集・連携環境整備などを推進することを記載すべき。
3 （3） AI ガバナンスの在り方の検討	10	1-6	また、様々な局面におけるAI導入の障壁を低減するため、AIを活用する際に想定・発生し得る課題に対して、その責任の所在等に関する解釈適用上の論点及び考え方を整理するとともに、判例等を踏まえ可能な限り解釈を明確化するよう努める。 さらに、AIは国境を越えて展開されるため、国内だけでなく、国際的なガバナンスが不可欠であり、相互運用性の確保にも配慮しつつ、AIガバナンスの構築を主導する。	国や地方公共団体に取り組んでいただきたい事項として、解釈の明確化だけでなく AI 利活用に即し既存法令や条例の見直しの検討も必要ではないか。これは古い法律がイノベーションの障壁にならないようにすべきということと、利便性が先行した結果（特に海外勢の）AI エージェントなどが無法地帯で動作する事態を予防すべき、という 2 つの要素を含む。

章・節	該当ページ	行番号	該当する記載	ご意見
3(2) 社会全体におけるAIリテラシーの向上	9	15-23	国及び地方公共団体は、国及び地方公共団体の職員はもちろんのこと、全ての主体が、倫理、法令、人権、安全等に関する課題を理解し、責任ある利用者としての自覚をもって行動できるように、社会全体におけるAIリテラシーの向上を図ることが求められる。 このため、常にAIの最新の技術動向や活用実態を把握し、リスク及びその対応策を検討して、ステークホルダーの自主的な取組を促すための考え方を提示する。また、事業者、国民等におけるAIの研究開発・活用における適正性確保に向けて、生成AIの基本的な使い方や注意点を学べるコンテンツの提供、社会人向けの生成AIスキル・知見の習得支援等、教育・ガイダンスを積極的に推進する。	偽・誤情報等だけでなく、外国の組織・個人や政党など、特定の勢力や個人による世論・価値観の誘導、洗脳のほか、SEO のような AI 最適を実現する手法に注意をする必要があると思われる。それらに対して、どのように向き合い、正しい情報を得るのか、といったことを学ぶ教育が子どもから大人まで、必要になる。 特に公教育の消費者教育等において、AI 教育、情報リテラシーの教育を実施しておくことは、わが国の平和と安定、民主主義の維持においても不可欠。AIを抜きにしても、国民がなりすまし、フェイクニュースに踊らされているのが現状であり、そこに AI が加われば、より世論の誘導灯のリスクが高まることになりかねない。

以上