AI に関する暫定的な論点整理

2023 年 5 月２６日

AI 戦略会議

この暫定的な論点整理（以下、論点整理）は、最近の技術の急激な変化や 2023 年 G7 広島サミットなどを踏まえ、AI 戦略会議の構成員が有識者として 2023 年 5 月末の時点で、生成 AI を中心に AI に関する論点を整理したものである。

政府関係者の参考となることを期待するとともに、各界各層における議論に資することも期待している。

AI 戦略会議 構成員

江間有沙	東京大学未来ビジョン研究センター 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
北野宏明	株式会社ソニーリサーチ 代表取締役 CEO
佐渡島庸平	株式会社コルク 代表取締役社長
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
松尾　豊	東京大学大学院工学系研究科 教授【座長】
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 に関する暫定的な論点整理

目次

AI に関する暫定的な論点整理

1. はじめに

生成 AI の可能性

ある視覚障害を有する人がいる。その人には悩みごとがあった。こどもが小学校からもらってくる連絡プリントを読めず、内容を知るためだけに膨大な手間と時間がかかることだ。AI を勉強した若者のスタートアップが、その方の悩みに寄り添い、プリントの内容の要約を瞬時に生成できる AI ソフトをつくり、提供した。その人はこどもの学校からの連絡をすぐに把握し、気遣えるようになった。日常にあふれる情報へのアクセスを手にすることで、生活の質は向上していった。その人はこれからの AI の進化を楽しみにするようになったという。AI の力は、ひとつの家庭に幸せと安心、そして希望をもたらした。社会課題と真摯に向き合い、テクノロジーを活用することで、暮らしや社会は、大きく変わるのである。

現在、高度な対話型生成 AI[1]（以下、「生成 AI」と称する）の利用者が急増している。これにより、情報のアクセシビリティの向上、労働力不足解消から生産性向上まで、諸問題を解消できるのではとの期待もかかる。

たしかに生成 AI は、歴史の画期となる可能性を含んでいる。19 世紀に産業革命が起こって内燃機関の利活用が始まり、やがて日本では一家に一台以上の割合で自動車を所有するほどの「移動の自由」をもたらしたように。21 世紀初頭にはインターネットが普及しスマートフォンが生まれ、高性能なコンピュータを一人一台手にするようになり、世界中の人々が「情報の自由」を得て社会の様相がまったく変わったように。生成 AI もまた、変革の時代を呼び起こし、新しい自由を人に与えてくれそうな勢いと技術的背景がある。

AI の急速な進展を心配する人も多いだろう。私たち国民の多くは、「AI の難しいことはわからないけど、ついていけるのか」「世の中どうなってしまうのか」というのが実感かもしれない。また、具体的に生成 AI による変化で困難に直面している方も出てきている。こうした方にしっかりと寄り添い、国民の声に応え、懸念やリスクを低減する措置を同時に講じていくことも大変重要である。技術や成長の話をするばかりでなく、しっかりと懸念やリスクへの対応とのバランスを取りながら進めていく必要がある。

生成 AI と日本の親和性

[1] 画像を生成する拡散モデル（diffusion model）や自然言語を扱う大規模言語モデル(large language model: LLM)などを指す。従来から識別モデルに対して生成モデルという分類法があり、その生成の側面に注目した呼び方。

AI がもたらす新しい自由と変化はおそらく、産業革命やインターネット革命が生んだものよりずっと大きいものとなる。ただしそれが具体的にどのような形をとって人々の前に現れるか、正確に捉えられている人はまだ誰もいないのが現状である。

ここ 30 年来、成長の機会を逃し続けてきた感のある日本においても、変革の時代は大きなチャンスの到来である。ChatGPT の流行は、世界中が予想しない形で昨年 11 月末から始まり、AI の急速な進展が多くの人の共通認識となった。その後の急速な展開は、国や地域の別を問わず、企業組織の大小も関係なく、スピード感と技術力を頼りにして、だれもが競争に参画できる状況が生まれていることを示している。

もとよりテクノロジー関連における研究・技術水準は、極めて高い日本である。AI に関しても、ここ数年、ペースを上げて人材育成、研究開発、社会実装を進めてきた実績がある。自信を持って正面から堂々と競争に臨めば、充分に世界で活躍できる力はある。

日本にはさらなる強みもある。生成 AI はその利用において、どのような入力をするか創意工夫が必要であり、日本人に向いているという意見もある。ひとりひとりが創造的で、お互いに切磋琢磨しながら、きめこまやかなものを作り上げられる日本人は、その力を発揮して作り込んだ生成 AI サービスを、ユニークな国際的に競争力あるものとして生み出せる可能性がある。また、AI が人間に寄り添い、人間の暮らしを豊かにする光景は、私たち国民の多くが共有している。日本人に愛されてきたドラえもんや鉄腕アトムなど、ロボット・AI が人間と共生する像は、私たちがもつ無形の資産である。

AI に対しての切実なニーズもある。ものづくり、金融、医療など大きな産業で、必ずしもデジタル技術をうまく利用できていなかった事業者も、AI を利用することで、一気に変革をとげられる可能性は大きい。そもそも労働人口が急減する日本においては、生産性を上げていくことは避けて通れない道であり、社会全体で AI を利用することの必要性は論を待たない。

いま戦略を検討することの重要性

盛り上がりを見せる生成 AI の技術は、まだ黎明期である。技術的な課題は多くあり、今後、こういった技術的課題が解決されるたびに大きな進展となって世の中に波及する。数年間のうちに技術が継続的に進展していくだろう。長らく停滞してきた日本は、AI の勃興とともに再び成長の機運が見えている。この芽を伸ばしていくため、いまこそ大胆な戦略が必要なのは間違いない。先行する二つの変革期における日本のふるまいを振り返れば、産業革命時には内燃機関という新しい技術をすみやかに吸収し、独自の改良を加え自動車産業を興して世界のトップランナーとなった。対してインターネット革命時には、戦略と決断の速さ、資本投下の物量で劣り、後塵を拝した。今回の AI 変革期はどうか。

生成 AI と日本の親和性を踏まえれば、十二分に競争できる状況にあるのではないか。ChatGPT の世界的流行などによりその利便性・重要性が日本の中でも一気に知れ渡ったこと、そして、オープンな技術開発も続いてきたために、地域や資本の別なく誰もが参入できることは日本には追い風だ。考えを尽く

し策を練れば、果実はついてくるのが現在のタイミングと言える。

AI は、安全保障、災害対策、温暖化対策等の地球規模の課題においても重要なツールであり、我が国は有志国とともに技術革新に取り組む必要がある。

生成 AI を進展させるにしても、足元でその利用に対する懸念も指摘されている。また、将来の展開は未だ誰にも分かっていない。一例を挙げれば、一つの大きなシステムで何を聞いても答えてくれるものが市場を支配するのか。それとも「医療系」「法律系」などと分野を縦割りに細分化し、部分特化した生成 AI が成立するのか。それによって様相は大きく変わる。

このように期待感と不透明感が交錯する今だからこそ、政府は、AI がもたらす社会変化に対して人々に安心感を与えると同時に、AI に関わる各プレーヤーができるだけ予見可能性をもってふるまえるようにすることが重要である。そして、様々な方面からのリスクに対応し、また、企業や研究者が存分に活動できるためのインフラを整備し、これら施策を適切に実現していくことによって、日本が成長へ向かう足取りを、確かなものとしていくことが重要である。

これまでの政策と論点整理との関係、論点整理の意義

政府においては、これまで「AI 戦略 2022[2]」や「人間中心の AI 社会原則[3]」などを定め、政府としての AI に対する基本戦略・基本理念を明らかにしてきた。しかしながら、生成 AI は、自然な文章のみならず画像や音声などの生成を著しく容易にするものであり、例えば人間の認知を欺瞞する情報を誰もが作成できるようになることや、その利用が世界中で爆発的に拡大していることから、従来の基本戦略・基本理念は維持しつつ、生成 AI の登場によって整理すべきリスクや論点をとりまとめることとした。

本論点整理は、第 1 回 AI 戦略会議における総理指示を踏まえ、同会議構成員が、幅広い課題に関して AI 戦略チーム（村井英樹総理大臣補佐官と関係省庁の実務者）のメンバー等と集中的な議論を行い、とりまとめたものである。

論点整理にあたっては、生成 AI の進展が国際的なものである点にも留意した。「我々が共有する民主的価値に沿った、信頼できる AI」が 2023 年 G7 広島サミットにおいて合意された共通のビジョンと目標である。これを実現するため、欧州はリスクレベルに応じて AI の使用を禁止・制限する法案を議会が検討し、米国では AI 開発者に情報開示等の何らかの責務を課そうという意見がある。しかしながら、欧米ともに、「現行法で対応できる場合はそれで対応すべき（不必要で過度な規制や監視はしない）」、「イノベーションを阻害しない」といった意見も聴かれ、各国ともに議論は一様ではない【別紙参照】。今般、

---

[2] 差し迫った危機への対処、社会実装の推進、「すべてに AI」を目指した着実な取組等によって構成される。

[3] 基本理念（人間の尊厳が尊重される社会、多様な背景を持つ人々が多様な幸せを追求できる社会、持続性ある社会）、AI 社会原則（人間中心の原則、教育・リテラシーの原則、プライバシー確保の原則、セキュリティ確保の原則、公正競争確保の原則、公平性・説明責任及び透明性の原則、イノベーションの原則）、AI 開発利用原則（開発者及び事業者において、基本理念及び AI 社会原則を踏まえた開発利用原則を定め、遵守すべき）等から構成される。

日本は、G7 議長国として国際的な議論に大きく貢献している。G7 首脳は、2023 年 5 月の広島サミットにおいて、議長を努める岸田内閣総理大臣主導のもと、G7 の価値に沿った AI のガバナンスの必要性を確認するとともに、特に生成 AI については「広島 AI プロセス」として担当閣僚のもとで速やかに議論させ、本年中に結果を報告させることとなった。我が国は今後も責任ある立場としてリードしていかなければならない。AI 戦略会議としても貢献していく考えである。

今回の論点整理は、いま考えられるリスクと AI の開発・提供・利用に当たっての必要な環境整備を中心に構成されている。単に課題を羅列したものではなく、基本的な考え方や進め方などを可能な限り提案しており、政府関係者の参考となることを期待するとともに、AI の利用が民間サービスや個人に爆発的に広がっていくことも想定し、幅広い各界各層におけるさらなる議論に資することも期待している。なにぶんこの分野は出てきたばかりであり、有識者にせよ政府にせよ、誰かが他より何かを知っている状態ではない。ならばせめて私たちは、いま考えられるリスクへの対応と開発等に必要なインフラの整備をどうしたらいいか、それを意識し議論するようにしてきた。我々の会議の仕事のすべては、せっかく土壌から顔を出した芽を、皆で大切に大きく育てていく、そのために費やされる。

香川県三豊市は先般、大学の研究室と協同してゴミ出し AI システムを開発した。細分化されたゴミ分別ルールを覚え込ませた AI に、ゴミ捨てのガイド役になってもらおうというものだ。各国語対応なので、海外からの労働者が多い三豊市では有効な住民サービスとして活用が期待される。「ゴミの分別に悩まない」とは生活内のごく小さい不便の解消に過ぎないが、AI が生み出す新しい社会と暮らしとは、こうしたささやかな創意工夫の積み重ねだ。ささやかな創意工夫で利用者が増え、その声がまた次の創意工夫を生む。こうした改善のサイクルを楽しんでいるうちに、いつの間にかレベルが高くなった AI が国内の生産性を底上げする。AI サービスは、国内に留まっていた産業をグローバルに展開させる。

小さい「こまやかさ」を集積し、大きい「豊かさ」を生み出す。そんな道のりを今後日本が歩んでいくことに、今回の論点整理が寄与できればと願う。

2. 基本的な考え方

国際的なルール構築に向けた主導的役割の発揮

AI には国境はなく、国際的な流通が容易であり世界中に影響を及ぼし得る。そのため、特に、リスクへの対応は、一つの国や地域だけが対応すればよいという問題ではなく、国際協力、国際協調が必要である。また、国際的に人間中心の観点が重視されているとともに、Responsible Deployment（責任ある展開）という概念が広がってきている。こうした国際的に共通の大きな考え方・ルールとの整合性や、各国のルールの詳細な差異を確認しながら相互運用性を確保していくことが必要である。政府は有識者の協力も得て、OECD、G7、GPAI、ISO 等における議論に貢献すべきである。今回の G7 で合意された「広島 AI プロセス」は、国際協調の大きな一歩であり、我が国としても引き続き議論をリードしていかなけ

ればならない。

その際、例えば日本は災害が多いこともあり、AI を用いた防災や被災者支援に関する知見や、プラットフォーム化された AI システムがダウンした場合などの緊急事態対応に関する知見で世界をリードできる可能性がある。また、ものづくりと AI、コンテンツや食文化と AI、物理や化学等の基礎科学と AI など、日本の強みを活かした分野との融合でも世界をリードできる可能性がある。

また、日本では大規模な生成 AI の開発事例が少ないが、研究水準が高い分野もあり、また、米中を除けば技術水準は概ね諸外国と大きな差はない。人材の育成も近年は進んできている。様々な利害得失も渦巻く中で、公正中立で倫理観の高い日本の研究者・技術者が国際的協調の議論に貢献できる可能性は高い。

リスクへの対応と利用

生成 AI の開発・提供・利用を促進するためにも、生成 AI に関する懸念やリスクへの適切な対処を行うべきである。いわば、「ガードレール」の設置が必要となる。生成 AI に関する懸念・リスクや対応の方向性を、AI 開発者・AI を活用したサービス提供者・企業や個人などの AI サービス利用者ごとに整理することが、開発・提供・利用を後押しすることとなる。

まず、AI 開発者・サービス提供者に対して、既存の法令・ガイドラインの遵守を促すことが重要である。その上で、既存の法令・ガイドラインで対処できない場合は、政府をはじめ関係者は必要な対応を検討すべきである。その際、過度な規制を避けつつ、ビジネスの予見可能性を高める観点・変化を前提とした柔軟性を持たせる観点の双方を踏まえる必要がある。また、ハード・ローとソフト・ローの二者択一の議論に陥ることなく、さらに、新技術が起こす問題に対しては新技術で対応するという発想も必要である。これまでの技術の歴史においても、例えば、ブラウザに関しては有害コンテンツフィルタリング、メールソフトに関しては迷惑メール対策ソフト、自動車に関しては安全運転支援技術など、新技術によるリスクに対して新技術で対応してきたことは珍しくない。例えば、AI による不適切な生成物を削除する AI や、コンテンツの信頼度を出元によって付与する仕組みなど、新たな技術の開発・普及が期待される。

次に、AI 利用者に対しては、利用にあたってのリスクを示すとともに、AI に対するリテラシー向上を促す取組を講ずるべきである。

また、上記のリスクとは性格を異にするが、今回の検討に際しては、生成 AI を利用しないことによるリスクについても留意した。まず、開発段階での一定の関与がなければ、AI が有する技術的リスクの把握が困難になるおそれがある。また、我が国の AI 開発者・サービス提供者が競争力をもたなければ、現在４兆円とも言われているデジタル赤字がさらに拡大する懸念や AI サービスの供給途絶リスクもある。さらには、AI の企業・個人による利用が進まなければ、我が国の生産性が他国に比して低迷するおそれがある。

多様な関係者を巻き込んだ迅速かつ柔軟な対応

AI は、その影響が広範におよぶことから、AI 開発者・AI を活用したサービス提供者・企業や個人などの AI サービス利用者など多様な関係者を巻き込んだ対応が必要であり、政府においては、従来の所管・ステークホルダーにとらわれない、より能動的な対応が求められる。また、AI を巡る技術・社会の変化に対応する観点から、リスク毎の緊急性・重要性に応じた対応が必要である。緊急性・重要性の高い課題に対しては、迅速に対応しつつ、予想外の事態も想定した柔軟な対応をとるべきである。また、中長期的な課題に対しては、技術・社会の変化を機敏に捉えた対応が求められる。また、「広島 AI プロセス」などの検討スケジュールも念頭に、国際的な議論の動向も踏まえることも重要である。

3. 主な論点の整理

今回の論点整理の主旨の一つは政府への提案である。政府の役割としては、AI の最適な利用に向けて、リスク対応に関する政策の実施が大きいと考えられる。リスク対応は、困難に直面する方への対応という意味でも重要であるが、AI を開発・提供する方が存分に活動できる環境を整える意味でも重要である。このため、まずリスク対応に関して論点を整理する。その後、AI の最適な利用、AI 開発力について整理する。

3-1　リスクへの対応

リスク対応の基本的方針

これまでも、AI が包含するリスクについては、様々な議論が行われてきた。例えば、日本では、「人間中心の AI 社会原則会議」の中で、もっともらしい嘘の流布などにより社会の安定性を損なうリスク、画像生成・音声合成などにより巧妙な詐欺や政治の混乱を生むリスク、AI を使える人・使えない人といった利用者間の能力差などが議論されてきた。実際に、米国では国防総省周辺での爆発の偽画像が拡散されて株価に影響が出るなど、今般の生成 AI の登場により、そのリスクはより切迫したものとなり、また、AI を取り巻く環境も大きく変化してきた。そうした変化を踏まえ、本論点整理では、より詳細かつ具体的にリスクを列挙し、対応の方向性を示すことで、関係者に必要な対応を促すものである。

特に生成 AI の登場を踏まえたリスクに関しては、国際協調、リスクへの対応と利用、多様な関係者を巻き込んだ迅速かつ柔軟な対応といった基本的な考え方を踏まえ、リスクへの対応に関する論点を整理した。その際、まずは AI 開発者・サービス提供者・利用者等が自らリスクを評価し、ガバナンス機能を発揮すること（法制度・ガイドライン等の遵守や技術による対応）が重要であるとともに、必要に応じ、政府を含む多様な関係者によるリスク対応の枠組みを検討・実施することが求められる。そうした中で、既に表面化しつつあるリスクのうち、既存の法制度やガイドライン・体制を前提に対処できるものはその周知徹底など早急に対応し、既存の法制度等では十分に対応できない可能性があるものについては諸外国における検討なども参考に対応を検討すべきである。また、将来生じ得るリスクについては、技術開発や事業展開のスピードが急速であることを踏まえ、専門家も交え、国際的な議論に積極的に参画しつ

つ、そのリスク把握に随時努める必要がある。

なお、国民の生命、自由、財産、基本的人権等を保護する観点から、リスクの全体像を可能な限り正確に把握することが重要であり、この論点整理では、現時点で考えられるリスクを幅広く記載している。

透明性と信頼性

リスクへの対応を考える際に、まず AI の透明性と信頼性を確保することが重要である。AI がどのようなデータを学習しているのか、学習データをどのように作成しているのか、どのような手法で回答を作成しているのかなどについて、AI の透明性を高めることにより、使用目的に対して適切な AI を選択することができるほか、問題が生じた場合の対処が容易となる。あるいは、AI が誤った回答をしていないか、AI との対話によって機密情報が漏洩しないかなど、AI の信頼性に関する懸念もある。これらは、生成 AI が登場する前から議論されていたが、自然な対話を可能とする生成 AI の登場によって課題や懸念は拡大したと考えられる。

このため、まずは AI 開発者・サービス提供者には、現行法令やガイドラインに則り、積極的な情報開示を求めたい。政府は、主要な AI 開発者・サービス提供者に対して、透明性・信頼性の確保を直接働きかけることも検討すべきではないか。また、生成 AI の普及を踏まえ、既存のガイドライン[4]に関して、必要な改訂などを検討する必要がある。その際、諸外国における検討とも協調し、第三者認証制度や監査制度等も参考とすべきである。さらに、例えば、AI による不適切な回答を削除するソフトウェア、AI によって生成された画像・映像・テキストか否かを判定するソフトウェア等、顕在化したリスクを低減するような技術の研究開発・普及を奨励することも望ましい。

懸念されるリスクの具体例と対応

①　機密情報の漏洩や個人情報の不適正な利用のリスク

AI との対話によって利用者の機密情報の漏洩や、個人情報の不適正な利用やプライバシーに関するリスクが指摘されている。

自己の情報のコントロールを重視する傾向にある欧州では、例えば、一般にアクセス可能な空間における顔識別等の遠隔生体認証に関する関心も高く、利用禁止を求める議論がある。

個人情報の不適正な利用やプライバシーの問題については、例えば、利用者が認識しない中で生成 AI が利用者との対話情報を蓄積し、利用者の趣向やその変化等の情報を推定して広告配信等の目的で利用するなどのリスクが考えられる。文章で対話する生成 AI の場合、利用者が何に関心を持っているのかなどの情報が、単語だけを入力するキーワード検索等よりも AI サービス提供者側からわかりやすく、リス

[4] 総務省「AI 利活用ガイドライン」（AI サービス等を他者に提供する者（AI サービスプロバイダー）、業として AI システム等を利用する者（ビジネス利用者）向け）、経済産業省「AI 原則実践のためのガバナンス・ガイドライン」（AI システムの開発・運用等に関わる事業者向け）など。

クが高まる懸念もある。また、個人の経歴や趣味等の情報はインターネット上で閲覧できる場合があり、AI がインターネット上の情報のみで学習したとしても、個人の情報が含まれる可能性がある。そのため、AI が特定の個人について、個人情報を探索・収集・分析したり（不適切なプロファイリング）、個人に関する不適切な情報を出力する可能性もある。

この問題に関しては、AI 開発者・サービス提供者はデータの取扱いなどを開示し、透明性、信頼性を高める努力が必要である。カメラ画像に関しては、生成 AI を念頭に策定されたものではないが、「カメラ画像利活用ガイドブック（経済産業省・総務省）」の活用も期待される。一方で、その AI 開発者・サービス提供者がそれを厳格に遵守しているか否かの確認は、実態的には難しいのではないかという論点もあり、生成 AI のような先端技術の可能性とリスクを踏まえた情報の取扱いについて、対応の在り方を検討すべきではないか。

なお、AI サービス提供者の信頼性の確認は一義的には利用者が行うものであるが、政府も利用の当事者であり、生成 AI サービス提供者や利用者のデータの取扱いなどを確認する必要がある。

②犯罪の巧妙化・容易化につながるリスク

生成 AI によって、従来の犯罪がより巧妙かつ容易になるリスクがある。例えば、生成 AI によって低コストで作成された精緻な画像・音声や巧妙な文章が、オレオレ詐欺等に利用される可能性がある。また、生成 AI を通じて得た武器、大麻や覚醒剤、麻薬の製造法等の情報が犯罪につながる可能性がある。検索エンジンで有害な情報が検索できてしまう場合と類似するが、一般人がより手軽に聞き出せてしまうこと、削除が従来と比べて容易ではないことなどが異なる。今後、技術の進展とともに、さらに巧妙な犯罪が出てくることも予想される。

このようなケースに関しては、現時点では、刑法（246 条 詐欺罪、246 条の 2 電子計算機使用詐欺罪）、不正アクセス禁止法（4 条 識別符号の不正取得）、武器等製造法、大麻取締法等の法制度等と執行体制により、対処されるものと考えられる。その上で、現行の法制度・ガイドライン、体制で不足する場合には、諸外国における同種の問題への対処方法なども参考に、対応を検討すべきではないか。

また、AI が詐欺・武器製造などに利用されないよう、AI による不適切な回答を抑制するソフトウェアの開発・普及、そのための生成 AI の制御方法の開発、それにつながる生成 AI の現象解明などの研究を奨励することも望ましい。

③ 偽情報等が社会を不安定化・混乱させるリスク

生成 AI によって、本物と見分けがつかないような情報を誰でも作ることができるようになり、悪意をもった人が簡単に偽情報を作ることができるようになった。すなわち、AI は偽情報による工作を「民主化」したとも言える。そのため、AI が生成した偽情報・誤情報・偏向情報が、民主主義に不当に介入するなど、社会を不安定化・混乱させるリスクが高まっている。

例えば、他国においては、生成 AI が生成した偽画像や、AI が生成した偽プロフィールを使った SNS

アカウント、AI が生成した偽投稿などによる生成 AI が生成した偽の画像と大量の偽 SNS アカウントを使った世論操作などが既に確認されている。我が国においても、選挙や特定の政党のイメージに不当な影響を与えたり、マスメディアが誤情報を事実であるかのように報じてしまうリスクが高まっている。

このようなケースに関しては、現時点では、刑法（233 条 信用毀損・偽計業務妨害、234 条 威力業務妨害、230 条 名誉毀損）等の法制度等と執行体制により、対処されるものと考えられる。その上で、現行の法制度・ガイドライン、体制で不足する場合には、諸外国における同種の問題への対処方法なども参考に、対応を検討すべきではないか。

また、AI によって生成されたコンテンツか否かを判定するソフトウェア等の開発（ディープ・フェイクを検知する技術の開発）・普及や、ディープ・フェイクが流通しない仕組みの開発、そのための研究を奨励することも望ましい。なお、具体例は列記しないものの特筆すべき点として、AI がジェンダー、人種、地域等の観点から偏った文章や画像を生成していないかといった公平性の論点は、国際的に注目されており、注視が必要である。

④ サイバー攻撃が巧妙化するリスク

生成 AI に限った問題ではないが、AI の高度化によって、サイバー攻撃が AI を用いて巧妙化し、防御しにくくなるリスクが指摘されている。サイバー攻撃には、AI を用いた攻撃とは別に、AI をターゲットとした新手の攻撃も指摘されている。

例えば、チェックツールで検知しにくい攻撃メールの作成などが増加するリスクが考えられる。生成 AI と様々なツールを組み合わせることで、生成 AI が個人・企業を対象にしたサイバー攻撃のプランを作成する、人間になりすまして攻撃するなど、従来よりも高度な攻撃が可能になるかもしれない。AI をターゲットとした攻撃の場合、むしろ AI が弱点となる可能性も指摘されている。

政府は、AI がサイバー攻撃に使われる事例の類型等について情報を収集し、必要に応じ周知するなどの対策を検討すべきではないか。また、AI を用いてセキュリティ対策を向上させることも必要ではないか。

⑤ 教育現場における生成 AI の扱い

教育現場では、例えば、生成 AI が宿題に使われ適切な評価が損なわれる、また作文やレポートに生成 AI を使うことで生徒・児童の創造力等が低下する懸念があるなどの喫緊の問題がある。その反面、例えば、生徒の理解度にあわせて教え方を調整する、評価テストを簡易に生成し学習効果をきめ細かく確認する、AI との対話的な教育方法を導入するなど、生成 AI をうまく活用した教育を進めていくことで、AI の利用により教育効果が上がり、教員の負担も軽減できる可能性もある。教育現場で生成 AI をどう扱うかは国民的な関心事である。

文科省においては、早急に論点を整理し、夏前にガイドライン策定を目指すこととしている。加えて、AI リテラシー教育が重要であり、現在の教育を検証し、必要に応じ、教育項目の追加などの措置を講じ

るべきである。

⑥ 著作権侵害のリスク

生成 AI がオリジナルに類似した著作物を生成するなどの懸念がある。生成 AI の普及によって個々の権利者にとって著作権侵害事案が大量に発生し、紛争解決対応も困難となるおそれもある。一方で、生成 AI を利用して映像制作を効率化する例もある。クリエーターの権利の守り方、使い方は重要な論点である。

政府は、まずは現行の著作権法制度を丁寧に周知すべきである。今後、専門家も交えて、AI 生成物が著作物として認められる場合、その利用が著作権侵害に当たる場合や著作物を学習用データとして利用することが不当に権利者の利益を害する場合の考え方などの論点を整理し、必要な対応を検討すべきである。

⑦ AI によって失業者が増えるリスク

AI が人間の作業を代替する可能性は、失業リスクとも考えられる。

例えば、従来も点検、審査、調査など様々な業務（一定の基準や手法に基づき行う業務など）で AI の利用拡大によって失業者が増える可能性が指摘されてきたが、生成 AI の登場によって、文書作成、画像制作など、より広い分野・職種で（創作・創造的な業務においても）失業者が増えるのではないかという懸念がある。生成 AI の活用は、これまで参入障壁の高かった専門職にも及ぶ可能性があるとする指摘もある。

政府は、AI が雇用に与える影響に関する各種の調査研究等の情報を収集し、必要に応じて対応を検討すべきである。また、業務がなくなった場合にも新たな働き方ができるよう、リスキリングや人材流動化を、政府全体の動きともあわせて AI の文脈においても検討していくべきである。

3-2　AI の利用

デジタル社会実現に向けた AI 利用の意義

デジタル社会の実現に向けて、行政・企業・教育・医療機関等において、データやデジタル技術の活用や DX の促進に向けた取組が進められている。生成 AI を含む AI には、デジタル化・デジタル技術の活用を加速させ、我が国全体の生産性向上のみならず、様々な社会課題解決に資する可能性がある。また、データ形式の変換を得意とする生成 AI は、医療や介護、行政、教育、金融、製造等のデータ連携基盤の整備に貢献することも期待でき、国内のみならずアジアを始めとする海外市場へのサービス展開の可能性も秘めている。

こうした観点を踏まえ、AI を利用した行政・企業・教育・医療機関等における取組を官民で加速していくことが期待される。

AI 利用を加速するための取組（連携基盤構築・人材育成・事業環境整備）

AI 利用を加速するためには、データを学習して作り上げる AI の前提であるデータ連携基盤の構築が極めて重要である。その際、官民様々なところから取得されるデータを、信頼性を前提としながら連携させていくことが必要となる。我が国は、これまでも、高い信頼性を確保しつつ、オープンなデータのやりとりを図る国際的な仕組みを作るため、「DFFT」（Data Free Flow with Trust）構想を主導してきており、生成 AI において、DFFT 構想の具体化を進めるべきである。

また、デジタル人材の育成・確保も重要である。学びの指針となるデジタルスキル標準など、様々な人材育成策が掲げられてきたが、AI、特に生成 AI の登場を踏まえた必要な見直しを早期に検討すべきである。

また、スタートアップ創出に向けた事業環境整備も重要である。生成 AI は事業が作りやすいことから、海外では、すでに多くのスタートアップが設立されている。我が国においても、適切なアクセラレーションや投資が鍵となる。

政府機関における生成 AI の利用

政府機関では、生成 AI の利用によって機密情報漏洩などのリスクがある一方で、様々な事務作業や事務手続きの効率化、問い合わせ対応の高度化を含み、働き方の改革や国民サービスの向上につながる可能性があり、生成 AI の典型的な活用例のひとつとなることが想定される。したがって、民間や地方を含めた様々な主体による生成 AI の利用に向けて、政府機関が率先してその可能性を追求することは重要である。

そのために、中央省庁は改めて意思統一を行うとともに、知見を集積することとした。独法等にも同様の取組を依頼した。自治体に対しては中央省庁の取組を周知した。また、AI 戦略チームでは、代表的な生成 AI 開発者・サービス提供者のデータの取扱い、海外政府の対応を確認中である。さらに、生成 AI の活用を通じた行政運営の効率化・行政サービスの質の向上に向けて、複数の省庁が公開情報を用いた試験的な取組を進めている。加えて、内閣人事局・デジタル庁が共同して、中央省庁における働き方改革促進のための生成 AI 活用ワークショップを開催するほか、中央省庁職員を対象としたアイデアソンや概念検証（PoC）を行うこととしている。こうした取組が政府機関一体となって進められることが期待される。

幅広い世代における生成 AI の扱い

生成 AI は、生活者の利便性を向上させ、利益をもたらすが、生成 AI を活用できるかどうかに左右される。若年層はもとより、生成 AI の恩恵は広く国民が享受できることが重要であり、幅広い世代が生成 AI を賢く使いこなすことのできるスキル・リテラシーを身に付けることが重要である。

このため、上記の教育現場向けのガイドライン策定の取組と連携して、幅広い世代で生成 AI を賢く使うためのリテラシー習得のためのコンテンツを開発する。

3-3　AI 開発力

開発力強化に向けた基本的考え方

AI は技術革新のスピードが速く予見可能性の低さを有するがゆえに、AI の開発にタイムリーに関与しないことは、最先端の技術情報にアクセスする機会を失うこととなり、それ自体がより大きなリスクを生む。さらに言えば、AI の研究成果が AI 以外の分野の研究開発の加速に寄与することもほぼ確実である。このため、いま生成 AI によって世界の変革がもたらされようとしている中、可及的速やかに生成 AI に関する基盤的な研究力・開発力を国内に醸成することが重要である。AI の進化を促す知識基盤研究は、将来に渡った革新的なイノベーションの創出にも貢献するものである。

政府が AI の開発支援を行う際は、AI 開発におけるインフラとも言うべき、計算資源とデータの整備・拡充を行うことが最も重要である。一方で、生成 AI 自体の開発は、スピード感を持って行うことが重要であり、政府の動きがボトルネックにならないよう、民間の活力を十分に活用すべきである。なお、政府による AI 開発の支援先には、透明性・信頼性の確保やその説明など、リスク対応に関する一層の責任を求めることが必要である。

計算資源

生成 AI の開発には、高速・大容量の GPU 等の計算資源が必要となる。計算資源の確保は、競争力に直結する。足下では、国内の開発需要に比して、計算資源の供給量は圧倒的に不足している。諸外国に劣後しないためには、政府が十分に計算資源に対する支援を行うべきである。世界で計算資源の獲得競争が生じており、政府も関与しつつ、可及的速やかに計算資源の整備・拡充が必要である。

計算資源を確保したとしても、次に電力調達が大きな課題となる。地方のデータセンターの活用を含め、再生可能エネルギー等の電力を有効活用する方策の検討が必要である。同時に、鍵を握る省エネ半導体等の開発を促し、早期に社会実装すべきである。

データ

生成 AI の開発には、大量かつ良質なデータが必要である。著作権等に留意しつつ、公的機関が保有するデータについて、我が国の民間企業・アカデミア等に対し開発用にアクセス可能となる仕組みを構築すべきである。また、前述のデジタル化関連施策の加速と連携しつつ、AI 利用に大きな期待があるものの課題を抱える分野のデータを整備し、その分野に変革をもたらす AI 開発を促進すべきである。

そのためには、すでに整備したデータへのアクセスの提供、また今後開発に用いることのできる日本語を中心とするデータの整備・拡充を国立の研究所が中心となって、進めるべきである。日本語のデータを揃えることは、生成 AI の性能に直結し、今後の日本の競争力に影響する可能性がある。

従来型ではない開発促進策

特に生成 AI の技術革新のスピードや予見可能性の低さを踏まえると、従来の政府による開発促進策で

は対応が難しい。市場原理を最大限尊重し、迅速、柔軟かつ集約的にプレーヤーの取組を加速するような支援を政府としても行っていくことが期待される。その際には、開発に関わる組織が、まずはしっかりと最先端をキャッチアップし、その中で技術を磨き、高度な開発能力を持つ人材を育成し、最終的には国際的な競争力につながるような支援を行う必要がある。

また、技術の公開を通じて新たな技術革新が生み出される可能性を踏まえ、計算資源やデータのほか、オープンに利用可能な基盤技術等を提供する環境を整備し、世界からトップ人材が集まり切磋琢磨できる研究・人材育成環境の構築や産学官の基盤開発力の強化を進めていくことが期待される。

3-4　その他

その他の論点

例えば、安全保障関係においても AI の利用が重要ではないかという論点があるが、情報管理上の必要性に応じて、専門部署による議論に委ねるなど、柔軟に対応すべきである。

また、現状では生成 AI に大きな注目が集まっているが、生成 AI ではない従来型の AI との適材適所による使い分けも念頭に置かれるべきである。

政府の体制

政府の司令塔、政策検討体制の強化が必要ではないかとの論点があり、政府は、AI 戦略会議（有識者）、AI 戦略チーム（村井補佐官＋関係省庁の実務者級）を軸に、各省協力しながら政策を立案・推進していく必要がある。

今後の検討

AI 戦略会議は、幅広い知見を有する有識者によって構成されており、2023 年 G7 広島サミットで合意された「広島 AI プロセス」に対しても貢献していく。

AI の急速な進歩は、ここ数年で止まるものではない。今後、長期間に渡って技術進歩が続き、それによって産業・社会への影響が継続する。技術進歩等により、上記以外の新たな論点、想定外の事態が生じた場合の対応が必要である。

なお、政府が本論点整理を踏まえた政策を実現するに際しては、広く国民や事業者からの意見を聴くことが重要である。

別紙

各国の議論の動向

米国	・ＡＩ分野における米国のリーダーシップを促進する「米国ＡＩイニシアチブ」に沿って政策推進。ＡＩに対する過度な規制を制限する米国 AI 規制原則案を公開。 ・連邦取引委員会、司法省、消費者金融保護局、雇用機会均等委員会が連名で、ＡＩが違法な偏見や差別を生む可能性を指摘する声明を発表。 ・本年５月にハリス副大統領が有力 AI 企業と直接面談し、ＡＩの潜在的な危険から社会を守るよう要請。同時にＡＩシステムの公開評価を実施する方針を表明。
英国	・本年３月に言語系生成 AI へのサイバーセキュリティの観点からの留意点を発表。 ・イノベーション担当省庁が AI に関するイノベーションを容易にする観点から本年３月にホワイトペーパーを公表（個人情報保護当局も基本的に支持を表明）。 ・競争・市場庁が、競争と消費者保護の観点からのレビュー開始を本年５月に公表。
EU	・欧州委員会が 2021 年に発表したＡＩ法案は、安全保障目的のＡＩや、悪用の可能性がある AI に規制がかかる可能性があるとした。これに対し、欧州理事会（ＥＵ加盟国による意思決定機関）が 2022 年にイノベーションを重視した修正案を発表。2023 年５月には、欧州議会（直接選挙により選出された議員からなる EU の立法府）の委員会にて当初案よりも規制を強化すべきとの修正案を議決。
イタリア	・GDPR（個人情報保護法に相当）違反の恐れがあるとして、本年３月に個人情報保護当局が ChatGPT の国内利用の一時停止を命令（その後、一時停止命令は解除）。一方、同国の副首相はこの一時停止命令は過剰であると批判。
ドイツ	・個人情報保護当局が調査を開始。危険な開発を抑制する必要があるなどの発言がある中、各閣僚からは、適切な活用をすべきとの発言が相次ぐ。本年５月には、言語系生成 AI を適切に使うための情報提供なども行っている。
フランス	・個人情報保護当局やデジタル化の担当閣僚などから雇用に与える影響への強い懸念が表明されるなど、全般的にネガティブな反応。
中国	・本年４月に、生成 AI に対し、その生成コンテンツが社会主義的な価値観に沿うべきことや、サービス提供前に当局の審査を求める「生成式 AI サービス管理規則案」について、パブリックコメントを開始。
コミュニティ	・米国の NPO「Future of LIFE Institute」は本年３月に、リスクが管理可能と確信できる場合にのみ開発すべき、GPT-4 よりも強力な AI の学習を６か月停止すべきなどとする公開書簡を公表、著名な AI 研究者も署名。