［論文］

LLM や生成 AI といった AI に対する規制や政策の動向とあり方の検討

小　林　　和　馬

〈目　次〉

1．イントロダクション

2023年、急速に利用が広がり社会経済への影響が大きいと予想されることからChatGPTを中心とした大規模言語モデル（LLM）と生成AIに対する規制やルール作りが急がれている。ChatGPTを中心としたAIはテキスト情報を扱う大規模言語モデル（LLM）として、人間が扱う言語（自然言語）を文字情報から学習し、学習した情報を確率論的に扱うことでAIが自然言語を扱うことを可能にした。

LLMの登場により、単に自然言語を扱うことが可能となり広く利用されるようになっただけでも影響が大きいことは想像できたが、これだけでなく、画像や映像、さらに音声を扱う生成AIが登場したことはその影響をLLMだけにとどめることなく、利用の可能性や多くが期待と不安を持つ「汎用AI」に向けた道筋となると考える人々が多く、大いに世間を賑わせた。

しかし、人々が期待と不安を持つ「汎用AI」の先にあるカーツワイルが主張した「シンギュラリティ」と呼ばれるAIが人間の知能を凌駕する特異点の到来については、その時点までに相当の距離があることは理解する必要がある。とはいえ、ある意味不完全とも言えるAIが人々の生活において幅広く活用される状況を作ったという点でLLMが果たした役割は大きく、隔世の感がある。

その隔世の感という意味で言えば、このChatGPTを中心としたLLMの登場からさらに利用拡大へと至ったことは、これまでにないパラダイムシフトを起こしたと考えている。それは、人間と機械の関係において、有史以来人間が使い方を工夫し、機械の調子を見ながら、時に機械の言葉（プログラム言語）を覚えて機械に動いてもらい、そして求める結果（出力）を得てきた。しかし、LLMの登場はその関係性を真逆にしたのだ。

つまり、「人間が機械に近づき、寄り添う」関係であったものが「機械が人間に近づき、寄り添う」関係となる。何をどうしたいのか、すべて機械が「言葉（自然言語）」で問いかけてくる。人間は求めるものを答えればよい。この関係性の変化はそれまでとは全く異なる世界観であり、革命的変化といえる。

本稿では、LLMや生成AIの特徴を捉えつつ、いち早く規制やルール作りに取り組んだEUや米国の政策立案の動向からLLMや生成AIにたいする政策立案のポイントを明らかにし、日本におけるLLMや生成AIに対する規制や政策といったルール作りのあり方について考察を行っていく。

2．LLMと生成AIの特徴

AIのモデルは「ニューラルネットワーク」という人間の脳の神経細胞の働きを模したものであるが、LLMを含むこのニューラルネットワークネットワークを用いたモデルは次にくる言葉をその可能性からウェイト付けし「確率論的に」選び出すものにすぎない。したがって、ニューラルネットワークによるモデルは本質的に誤った情報でも、大量にその情報が存在してしまうと「正しい」かのように判断し“知ったかぶり”をする「ハルシネーション」問題を引き起こしてしまう。すると「フェイクニュース」や「ヘイト」のように誤ったり偏ったりする情報がSNSを通じて価値観が似た仲間内だけで大量に流布されその偽情報の声を大きくしてしまう。この性質は「エコーチェンバー」と呼ばれ、社会に影響を与えるような大きな声となることで問題が深刻化する可能性もある。実際、すでに生成AIを用いた偽情報が氾濫を始めており、急速な勢いで偽情報が流布され始めている。

また同時に生成AIと呼ばれる画像、映像、さらに音楽といった多様な情報を文字（テキスト）情報から画像や映像、さらに音声と相互に生成可能となった。これは「マルチモーダル」と呼ばれ、AIが持つ可能性の幅を飛躍的に広げた。

3．政策的議論の経緯

AIに対する議論はこれまでも想定される影響の大きさから議論されることはあったが、2023年にChatGPTによる利用拡大とそれに伴い挙ってLLMを用いたサービスが一般提供を開始したことから急速に社会経済への影響が高まり、2023年5月に行われた広島サミットにより、取り急ぎLLMの影響を含めたAIへのルールや政策の策定に取り組んだ1年となった。

欧米諸国は早い段階からAIに対する方針について規制当局や担当部署での議論が行われ、米国では比較的早い段階でNAIRR報告書（2023）が提出されていた。こ

の中では、EUにおいては米国同様早い段階から議論に着手し、2022年段階で「」と言った形で議論が行われていた。

4．EUにおけるAIに対する政策的議論

EUにおける政策的議論は主にデジタル市場関連では「Shaping Europe's Digital Future」[1]として紹介され、「人々のための技術（Technology that work for people）」、「公正で競争的な経済（A fair and competitive economy）」、「開かれた、民主的で持続可能な社会（An open, democratic and sustainable society）」を掲げ政策により実現する社会像とし、2022年には議論や指令に基づき「デジタルマーケット法（Digital Market Act）」[2]をまとめ、制定した。

この流れの中で、AI自体に対する法制度の議論は2020年に規制と投資によりAIの利用促進を支援する目的で「AI白書」[3]としてまとめ、AIによる社会的影響について考察を行うことでAIを戦略的に用いて全体として人間中心、倫理的、かつ持続可能な社会を基本的人権に基づいて構築することを確認した。そして、2021年規制の枠組みがの中で「EU regulatory framework on artificial intelligence」[4]として提案され、枠組みの中で特に今後規制手段だけでなく予算や影響への評価を行い継続的に多面的なAIによる影響に対応していくとした。このAIに関する動きも踏まえ、2022年にデジタル分野の市場に対しての規制として前述のデジタルマーケット法として成立したのである。したがって、2023年はLLMや生成AIによるAIへのルール作りとして、デジタルマーケット法でプラットフォームを提供するビッグテックを「ゲートキーパー」として指定した上での規制による市場形成という方向性の延長線から、ChatGPTを提供しているOpenAIやマイクロソフトといったLLMの事業者についても議論が続いていると考えることができる。

また、2022年には「AI Liability Directive」[5]と称したAIに関する指令を出し、AIシステムの利用等により契約を伴わない形で負うことになる市民の責任について統一した要件を示した。これにより、AIシステムにより生じた損害についての責任の範囲、損害の定義、証拠の公開、さらに欠陥との関連性の推定など、損害や責任の評価を行う上での指針を示した。

2023年4月、ChatGPTの利用拡大に伴ってデータ保護委員会が作業部会を設置し、LLMの学習や学習による出力に際して個人情報の漏洩がないかどうかを確認し対処する方針を示したと読売新聞（2023）などメディアで報じられた。こうした議論も含めて、同時期にデジタルマーケット法の導入に際しての詳細な手続きについても定められ、起こりうる問題に対して具体的な手続き上の対処方法を明確化した。

EUの政策的議論は、これまでのデジタルプラットフォームとそれを提供するビッグテック企業への監視・評価を想定した法的な枠組みで取り組んできた。その中で2023年ChatGPTの利用拡大からの急速な変化が起こったことから、LLMや生成AIによるAIシステムとしてのサービス提供は、これまでのデジタルサービスプラットフォームの提供と同様の監視と評価するものとなっている。特にAIへの懸念に対する議論として、今後のAIの発展を踏まえた国家や社会像というレベルで、社会経済が人間中心でかつ基本的人権を前提として構築されることを確認するものとなっている。

5．米国における政策的議論

米国における政策的議論はAIに関しては2020年に米国議会下院において法案を「National AI Initiative Act」[6]としてAIに対する政策的議論の足がかりとした。これを受け、2021年6月にはホワイトハウス科学技術政策局（OSTP）とアメリカ国立科学財団（NSF）によりAIについて議論するタスクフォース「National Artificial Intelligence Research Resource (NIRR) Task Force」を

1）EU（2020a）参照。
2）EU（2022a）参照。
3）EU（2020b）参照。
4）EU（2021）参照。
5）EU（2022b）参照。
6）House of Representatives（2020）参照。

設置し[7]、AIに関する動向や問題点に特化して分析を行っている。

そして2023年1月、NIRRはAIに関するレポート[8]を発表し、NIRRがAIの研究開発を推進し、多分野にわたる利用者がデータや学習資源に触れられるようにし、AIの問題点を主張する考えや分野とコラボレーションすることが容易となるようにすることを目的としている。また、レポートの中で将来の信頼できるAIに向けた支援として、人材育成を行うべく様々な資源を提供しアイディアを交流させる「触媒」になるとしている。したがって、NIRRはその目的として、①イノベーションを刺激し、②才能の多様性が増し、③可能性を広げ、そして④信頼できるAIに発展させる、とした4つの目的を持つとした。

また、OSTPはAIによる懸念や脅威を想定した「Blueprint for an AI Bill of Rights」[9]を示し、AIの影響から守られる5つの事項；非効率や安全ではない自動化システムの被害からの保護、アルゴリズムやシステムによる差別からの保護、データのプライバシーの保護、通知と説明の担保、オプトアウトや解決策の検討や代替は「権利」であるとした。

そして2023年10月、バイデン大統領は大統領行政命令[10]を発令し、OSTPを含むNIRR（2023）としての議論をベースに、大きく8つの視点から保護する内容を明示し詳細に説明した。それらの中で特筆すべき点は、OSTPの議論からの追加的論点として、生物学的情報の保護、労働者の保護、AIについて世界を先導すること、政府による責任ある効率的なAIの利用を宣言するなど多岐にわたり、市民としてや消費者として人々の多様な権利を守るとしている点である。さらに、この命令では遺伝子情報など生物学的情報やAI技術の軍事転用などにも言及している点は2023年5月に広島で行われたG7サミットの世界的なAIに対する「広島AIプロセス」の議論と共通した点も世界に先んじて政策へ反映させていることも重要な点である。

6．日本の現状とAIに対する政策の検討

日本における政策的議論は規制や政策が取り急ぎ議論され、ここ数ヶ月で矢継ぎ早に公表されている。これは現時点ですでに偽情報が氾濫し始めていることから、緊急性のある対応として議論がなされていることが分かる。日本は政策の方向性として2023年5月に日本で開催されたG7サミットにおいて問題を提起し、国際的な枠組みで対策や政策を検討した。そして、10月には「広島AIプロセスに関するG7首脳声明」として世界的な議論としてのAIに対する規制や政策の方向性を示したことで世界と歩調を合わせて政策的議論ができる環境を作ったと言える。

しかし、日本のAIに対する政策的議論において注目しなければならないのは、日本において米国であればGoogleやマイクロソフトなどGAFAMと呼ばれ、中国であればバイドゥ、アリババ、テンセントといったデジタルプラットフォームを通じたデジタルサービスを提供するテクノロジー企業、つまりビッグテックが存在しない。このことはAIで世界を牽引すると考える場合致命的問題である。日本は常にAIにより世界を構築する当事者になれず、常に利用者の立場でしか議論に参加できない。

一方で日本のデジタル政策である「デジタル田園都市構想」は、デジタル政策の前身であるIT・ICT政策の時代から一貫して、世界一のIT国家やデジタル国家を標榜している。この点を見るに日本の政策立案者は日本が置かれている現状を認識しているのかと疑念がわく。

とはいえ、ChatGPTを中心としたLLMや生成AIによる急速な普及と発展は、そのスケジュール感あるいはスピード感という点で影響がいかに広大かつ甚大になるのかを示すものであり、日本は置かれている状況とAIの影響の大きさやスピード感にどのように対処するのか、AIの影響をどのように経済の活力に変えていこうとしているのか、速やかに具体的な方策を示す必要がある。

7）Whitehouse（2021）参照。
8）NIRR（2023）参照。
9）Whitehouse（2023a）参照。
10）White house（2023b）参照。

結論

本稿ではChatGPTを中心としたLLMや生成AIの特徴を捉えつつ、規制やルール作りに取り組んだEUや米国の政策立案の動向を踏まえ政策立案のポイントを明らかにした。さらに、日本におけるLLMや生成AIに対する規制や政策といったルール作りのあり方について考察を行った。LLMや生成AIを踏まえたAIに対する政策的議論は始まったばかりである。とはいえ本稿議論を通じ、日本においてデジタルプラットフォームを提供するビッグテックと呼べる企業が不在であることは政策的議論をする上で欧米の議論と同じ土俵で議論して良いのか大いに疑問である。したがって、日本のAI政策は、ICT同様、デジタルサービスの利活用としてそのあり方を政策として考えた方が良いと考える。むしろ高度に利活用する国として国家を発展させ、国民を高度にAIの利活用ができる人材に育成し、その上でAIの開発へと向かう企業や人材を数多く創出するというのが本来の日本の成長シナリオではないかと考える。

〈参考文献〉

EU (2020a) *Shaping Europe's Digital Future*, https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf.>

EU (2020b) *AI White Paper*, https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

EU (2021) *Proposal for a Regulation laying down harmonised rules on artificial intelligence*, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_ 1 &format=PDF.

EU (2022a) *REGULATION (EU) 2022/1925*, https://eur-lex.europa.eu/eli/reg/2022/1925.

EU (2022b) *AI Liability Directive*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX% 3 A52022PC0496.

NIRR (2023) *Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem*, https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf.

Whitehouse (2021) *The Biden Administration Launches the National Artificial Intelligence Research Resource Task Force*, https://www.whitehouse.gov/ostp/news-updates/2021/06/10/the-biden-administration-launches-the-national-artificial-intelligence-research-resource-task-force/.

Whitehouse (2023a) *Blueprint for an AI Bill of Rights*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

Whitehouse (2023b) *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

読売新聞（2023）「ＥＵが「チャットＧＰＴ」への対応協議、データ保護委が作業部会設置へ」、https://www.yomiuri.co.jp/economy/20230414-OYT 1 T50112/