日本型生成AI規制の可能性

生成AIの急速な進歩に伴い、生成AIがもたらすリスクへの懸念も高まっている。各国で生成AIのリスクを抑制するための規制の導入が議論されている。入口の自由度を高め、出口の品質に注目する日本型生成AI規制の枠組みは生成AIのイノベーションを阻害せず、健全な発展を促す取り組みとして注目されつつある。

進む生成AI規制とモデルからみた規制の枠組み

生成AIの急速な機能進化が続いている。一方で生成AIがもたらすリスクへの警戒感も高まっており、各国では生成AIの健全な発展に向けた規制を検討している[1)]。

ここでは生成AI規制を、生成AIのモデルに応じた形で分類してみたい。

生成AIは「開発・学習段階」「調整済みモデル構築段階」「生成・利用段階」の大きく3つの段階に分類できる。

開発・学習段階とは、大量のテキストデータや画像データなどの学習データを収集し、それらのデータを元に大量の計算資源を投入して学習済みモデルを構築する段階である。

そして、構築された学習済みモデルに対して、回答の精度を高めるために様々なチューニング（調整）を行い、より自然で精度の高い回答が得られるようにしたものが調整済みモデル構築段階である。

そして、実際に利用者が質問や作業指示を行い、その結果として調整済みモデルがテキストデータや画像などのアウトプットを生み出す段階が生成・利用段階となる。

そして生成AI規制はそれぞれの段階で論点が異なっている。

開発・学習段階では、利用されるデータが論点となる。大きくは著作権で保護されたコンテンツの利用に関する問題と、個人情報を含むプライバシー情報の取り扱いなどが課題となる。また学習するデータの中にバイアスや誤りを含む「低品質の学習データ」が含まれていないかという点も論点に挙げられている。

調整済みモデル構築段階では、そのモデルが倫理的に問題のあるバイアスを含んでいないか、誤ったアウトプットを不用意に生成してしまわないか、開発者の想定外の挙動を取ってしまわないかといった点が焦点となる。

そして生成・利用段階では（調整済みモデル段階と重複するが）、生成されたアウトプットに倫理的に問題がないか、誤った情報（加えてディープフェイク）を生み出すリスクはないか、さらに生成されたアウトプットが著作権を侵害していないか（もしくは生成AIのアウトプットに著作権はあるのか[2)]）といった点が論点となる。

注意すべき点として、これらの規制はすべての生成AIに一律に適用されるわけではなく、その生成AIが利活用される用途のリスクに応じて規制の強弱が変化する点である。いわゆるリスクベースアプローチが生成AI規制の枠組みに含まれている。

EU、米国の生成AI規制の特徴

<EU>

EUは2023年6月、生成AIを含む包括的なAIの規制案である「AI法案」を欧州議会の本会議において賛成多数で採択し、2026年の施行を予定している。

EUのAI法案の特徴は、域内における人権や自由の確保が最優先であり、技術は人間中心であるべきとの基本理念に立脚していること、リスクベースアプローチを採用していること、他の欧州規制（GDPRなど）と同様、域外企業が提供するAIも対象となることが挙げられる。

AI法案では、開発・学習段階の学習データはGDPRに準拠することが求められ、多様な学習データの確保にかなりの制約が課せられることが予想される。また一定以上のリスクが予想される調整済みモデルはEUへの登

NOTE

1) 2023年5月、広島でのG7サミットにおいて、生成AIの開発者や利用企業に広く適用される生成AIの活用や規制に向けた共通のルール作りが提案された。「広島AIプロセス」では、AIのリスク評価、リスクベースアプローチ、情報公開、セキュリティ対策、個人情報や著作権の保護といった取り組みを開発者や利用企業に要求している。
2) 多くの国では生成AIのアウトプットそのものに著作権を認めない方針が多いが、中国では一部の生成物に著作権を認める判決を出して注目されている。「AIルール、急ぐ中国　声の権利や著作権認定、各国に影響も」日本経済新聞 (2024/7/22)。https://www.nikkei.com/article/DGKKZO82222200R20C24A7TCJ000/
3) 「AI大手、規制警戒で"EU離れ"　メタもマルチモーダルAI提供見送りへ」ASCII.jp (2024/7/19)。https://ascii.jp/elem/000/004/210/4210899/
4) 「米国の「AIマンハッタン計画」追従は危険」JBpress (2024/7/23)。https://jbpress.ismedia.jp/articles/-/82183
5) 「AIを開発するために必要なデータが急速に枯渇、たった1年で高品質データの4分の1が使用不可に」GIGAZINE (2024/7/23)。https://gigazine.net/news/20240723-ai-data-restrictions/

録が求められる。加えて生成・利用段階も含めて品質管理プロセスの整備が義務付けられる。

このAI法案は生成AIにかなり厳しい規制を課すものであり、特に域外の事業者にとってハードルが高い。実際、米Appleは6月にプラバシー保護規制への懸念から一部AI機能のEU域内での提供を取りやめ、米Metaは7月にEU域内でのマルチモーダルモデルのAI投入を見送ると発表した[3]。AIのEU離れが懸念されている。

＜アメリカ＞

アメリカは2023年10月、「人工知能の安全・安心・信頼できる開発と利用に関する大統領令（以下、大統領令）」を公表した。大統領令では、生成AIの開発・学習段階のテストに、基準を設け、企業などにはそのテスト結果や重要な情報を連邦政府と共有することを求めている。また、国家安全保障などに重大なリスクをもたらすAIの開発をする企業にはその開発過程を政府に通知するよう求められる。

大統領令はあくまで行政としての措置であり、新たな規制の立法措置などは含まれていない。その意味では、EUのAI法案と比較してよりイノベーション促進に軸足をおいた規制の枠組みといえる。

一方で、共和党はこの大統領令の撤回を求めており、さらにトランプ候補の支持者が「AIマンハッタン計画」と呼ばれる新たな大統領令の草案を作成しているという報道もある[4]。AI規制の先行きは不透明だ。

日本型生成AI規制の可能性

日本では現時点では包括的な生成AIの規制の枠組みは存在しない。ただ各国の生成AI規制を受けて国内での生成AI規制の議論が開始されている。検討されている枠組みはおおよそ広島AIプロセス[1]に則ったものであり、リスクベースアプローチや事業者との情報連携、課徴金などが論点として挙がっている。

一方、日本の生成AIの現行の規制の最大の特徴は、入口の開発・学習段階での著作物の取り扱いである。日本の著作権法は「情報解析のための権利制限」規定（情報解析規定）が盛り込まれており、情報解析の目的であれば著作権のある著作物を大量に利用することを原則自由としている。この規定により、日本の著作権法の適用範囲内ではSNS上のデータや学術論文、記事データなどを網羅的に解析対象とすることが可能となっている。この情報解析規定により、日本では入口を緩くし、より有用な学習済みモデルの構築を促すことが可能になる。

良質な学習データの確保が生成AIの競争力を左右する。しかし、ここのところデータ所有者はAI開発者が自由に自分たちのデータを利用することに対して反発を強めている[5]。一方、日本ではAI開発者は著作権侵害を気にせずに学習データを収集できる優位性を持っている。この優位性を活かす政策の促進を期待したい。当然ながら生成・利用段階での著作権侵害には厳しく対処するための制度・体制作りを同時に進めることも必要なのはいうまでもない。

Writer's Profile

柏木 亮二 Ryoji Kashiwagi
金融デジタルビジネスリサーチ部
エキスパート研究員
専門はIT事業戦略分析
focus@nri.co.jp