Ⅰ－２－１　講演会　欧州・米国・中国のAI法規制動向について
---明確に後れを取った日本の現状

講師：渥美坂井法律事務所・外国法共同事業　パートナー弁護士
大阪大学招聘教授（社会技術共創研究センター）
三部　裕幸

開催日　　：2024年3月6日
開催場所　：JBMIA会議室（第4、第5会議室）＋Zoom開催
参加者　　：70名
記　　：坂津 務*

１．はじめに

2023年はEU AI規制法に関する動きが活発化し、アメリカや中国も独自にAI法整備を進めてきた。また、生成 AI が爆発的に社会に浸透し様々な問題が顕在化してきた年でもあり、AIを取りまく社会情勢が大きく変化を遂げてきている。

JBMIAの技術調査専門委員会に属しているAI関連対応検討WGより2023年7月に「AI倫理とAI規制の最新動向と AI 利活用のために考慮すべき注意点」を公開した。

（JBMIAホームページ2023年7月報告書）

https://www.jbmia.or.jp/whatsnew/detail.php?id=1653

その報告書では、三部弁護士が総務省の委託を受けて作成された「EUのAI規則案の概要」から多くを参考とさせていただいた。資料引用のご相談と合わせて、今回の講演会開催のご承諾を得て全2回に分けて講演していただくことになった。第1回目は、EU・アメリカ・中国のAI法規制動向について、第2回目は、AIに携わる企業が生き残るための4つのリスク対応策について4月4日にお話しいただいた。（2回目の講演内容については、Ⅰ－２－２を参照のこと。）

２．講演内容

2.1.　世界における日本のポジショニングと資源集中の必要性

AI 産業の方向性や法規制を考える前提となるのは世界の中で日本がどういうポジショニングにあるかという事である。それを知るために、Kaggle社が発表しているグローバルインデックス、および Tortoise Media社が発表しているグローバルAIインデックスのランキングをみてみると、日本は AI 産業では第三集団であることが明確にわかる。アメリカと中国がツートップであるが、EU全体で見ると第一集団となり、イギリス、カナダ、イスラエル、シンガポール、韓国が2 つの統計で共通して第二集団に位置している。日本はそれらの国々からかなり引き離されてしまっている。そうなると AI ガバナンスの着手検討という点でも日本は遅れてしまい、ビジネスの側でもこのままではガラパゴス化のリスクが高いということになってしまう。そうならないために、第一集団、第二集団を目指し、ガバナンスの点でも遅れを取り戻すことが重要になっ

* 技術調査専門委員会委員

てくる。

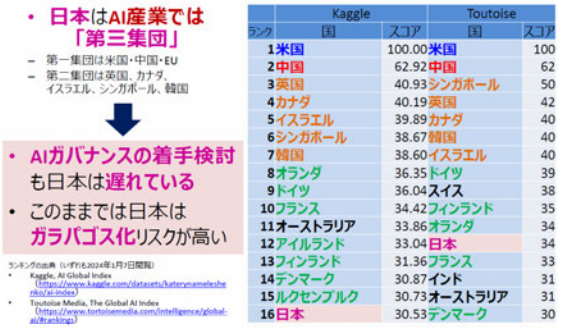

Fig. 1 AI 産業における日本のポジショニング

もう一つ重要なことは、アメリカと中国の AI 投資の規模はあまりにも巨大であり、日本が生成 AI を独自に基本開発しようとしても、アメリカや中国に絶対に勝てないということである。過去 10 年でアメリカは日本の 60～70 倍の投資をしてきている。中国は国家・省・民間連携で巨大な AI タウンを作っている。例えば、浙江省にある AI タウンでは 2019 年当時で東京ドーム 4 個分、現在では 6 個分の規模で、アリババ、バイドゥなどが主導でいろいろな企業や研究機関が集まってきている。しかも同じような AI タウンが中国の中に 10 個ほどあるらしい。これらを考えると、AI 産業ではアメリカ、中国と同じような巨額投資路線を採るのは現実的ではない。

Fig. 2 米中の AI 投資規模

では、AI 産業で日本が勝てないのかというとそうではない。私は 2016 年から AI 案件をサポートしてきているが、日本の AI 産業が得意とする領域も確実にある。特定分野×AI という一つの分野に特化した AI が多くしかも強い。画像・映像と AI は日本のお家芸みたいなものである。金融や医療・介護と AI は日本ならではの社会課題があるのでかなり検討が進められてきた。ゲームと AI は完全に日本が重視してきた分野で大・小企業において特化した AI 部隊がいる。災害対策と AI なども日本は非常に進んでいる領域である。大事なのは国・企業を挙げて第二集団、第一集団に格上げすべく資源を集中していくことである。生成 AI の基本開発を止める必要はないが、生成 AI を応用開発に結びつけて日本の強みを活かすということだ。

日本は巨額投資の方向性ではなく既にある生成 AI を応用開発して自社の得意とする AI 領域と組み合わせ独自性のある AI を作り上げることに集中していくことが大事だと思っている。日本の諸課題を考えると地方創生や輸出振興とともに進めるのがよく、嘗て日本の産業が応用開発と輸出中心で経済発展を遂げてきたことと同様に、AI 産業において拡大的再現ができるのではないかと考える。

2.2. 世界先進西側諸国の AI 法整備の動向

2023 年後半に日本以外の西側先進諸国は AI 法規制において急進展を遂げている。アメリカは当局向けに大統領令を公表した。EU は領域内でほぼ AI 規制案に同意している。イギリスはアメリカに同調しながら EU とは距離を置きつつも極端に離れているとは言えない。カナダは EU の AI 規制案の類似型を提案している。

Fig. 3 AI 法規制における急進展

アメリカと EU は 2019 年ごろから AI 関連の重要リ

スクを列挙し詳細に分析して AI 法検討を進めてきた。しかし、日本は AI 利活用に伴うリスクの列挙・分析ができていないので、ガイドラインや業界団体ルールなど法的拘束力のないソフトローで柔らかく規制していくのがいいという先入観をもっていた。西側諸国が指向してきた方向とは違う方向に向かってしまった。

2.2.1. アメリカと EU の規制範囲

日本には、アメリカはソフトローを重視し、EU はハードローを重視しているという誤解をする言説が一部に見られた。しかし、実際に具体化してくると、アメリカの方が EU よりも規制範囲が広かった。EU は共同体なので横串を通したルールしか作れないのでアメリカが作る法律よりもシンプルになるが、アメリカの方が考えないといけない事項が多いというのがその理由である。ロシアや中国を念頭にいかに安全保障を達成すればよいのかという安全保障リスクは特に大きな課題であり、守ろうとする範囲が多くなっている。

2.2.2. EU の AI 規則案の目的と特徴

EU の AI 規則案の目的は AI リスクへの対処と、イノベーションの強化である。EU は人権重視のために規制を強化しようとしているという誤解があったが、自国の AI ビジネスの足枷になる規制を作るわけがなく、またアメリカの GAFA のようなビッグテックと組まないで AI ビジネスは成り立たない。実際の目的は、ビジネスとしてルールを統一することで単一市場を作りたいということ、個人情報の機械的処理によって差別・迫害が行われたという歴史的経緯を配慮した規制をつくるということ、その調和点を図っているのがこの法案となっている。

その規制の特徴は、リスクに応じて規制内容を変えるリスクベースアプローチである。

Fig.4 リスクベースアプローチ

許容できないリスクのある AI は禁止に、ハイリスクのある AI はハードローの規制、限定リスクのある AI は説明義務のみ、最小リスクの AI は規制なし、の 4 つに分類される。許容できないリスクは後で述べる 8 類型あって、歴史的経緯から絶対受け入れることができないタイプは禁止となっている。規制の中心はハイリスクのある AI に対するハードローによる規制であるが、安全に関わる AI、差別・偏見・迫害などにつながりやすい AI が対象となる。このハイリスクのある AI に関しては第二回目の講演にて詳しく説明する。

許容できないリスクのある AI についてかなり簡略化して列挙すると以下の 8 類型となり、最初の 4 つは原案が挙げていた類型の修正である。

●サブリミナルな手法や意図的な操作・詐欺的手法により、情報に基づく意思決定をできなくすること
●人やそのグループの年齢や障害、特定の社会的経済的状況に基づく脆弱性に付け込み行動を歪めること
●社会的スコアを利用し人やグループの不利益取扱いや不当・不釣り合いな取扱い
●法執行の目的による公にアクセスできる場所におけるリアルタイム生体識別

以下の 4 つは、原案公表後に新たに加えられた禁止類型である。

●人種、政治的意見、労働組合を推測するための生体分類システムを特定の目的のために使用する、宗教的哲学的信条、性生活、性的指向を推測すること
●人のプロファイリングや性格評価のみに基づきその人が罪を犯す危険性評価を行うこと
●ウェブや CCTV の映像から顔画像を無標的にスクレ

イピングすることにより顔認識データベースを作成・拡張すること

●人の感情を推測すること

以上の合計 8 類型の禁止は 2024 年中に施行される見込みであり、法案の効力発生から 6 か月後に施行される。上記はかなり簡略化して記載したものであるので気をつける必要がある。関係のありそうな場合はご相談頂きたい。

守らないと摘発されるかという事に関しては、摘発される以前に、輸出する場合に輸入する側から遵守の確認を求められるのでそもそも受け入れてくれなくなるという事が起こる。早いタイミングで規制がかかってくることになる。

2.2.3. アメリカ AI 大統領令

この大統領令は、各種リスクに対処するために法的拘束力のあるハードローの整備を含む様々な方策を行政官庁に命令している。これらに対して、アメリカがハードロー寄りに行くのかと日本国内では驚かれたようだが、決して意外ではない。

この大統領令は最近考えられたものではなく、2019 年のトランプ政権から連邦議員が超党派で AI 法が必要だと考えて長期間にわたり検討してきており、バイデン政権だけの意向という事ではない。全米商工会議所においても AI 規制の必要性を発表しており同様の考えとなっている。したがって、2024 年秋の大統領選の結果によってこの大統領令の言っていることが根本的にひっくり返ることはないと考える。トランプ氏の発言に対しては、アメリカのマスコミや共和党議員および民主党議員の反応は薄く、もしトランプ氏が大統領になっても現大統領令を根本的に覆す AI 法案を考え出すことはできないと思われる。

	指導原則	策定・検討される内容の例
1	AIの安全性とセキュリティ	・AIの評価、リスクのテストなどのメカニズムづくり。特にデュアルユース基盤モデルのAIレッドチームテストと報告義務、外国の者とのAI取引の報告義務など ・最も差し迫った安全保障上のリスクに対処（バイオテクノロジー、サイバーセキュリティ、重要インフラなど） ・ラベリングとコンテンツ証明メカニズムの開発支援
2	イノベーションと競争の促進	・AI関連の教育訓練、研究開発等への投資 ・知的財産問題への取組 ・違法な談合の阻止、優越的企業の独占リスクへの対処 ・中小企業等の市場の支援
3	労働者の支援	・AIが生み出す雇用や産業へのアクセスと職業訓練・教育 ・労働者の権利侵害等のリスクへの対策（ベストプラクティスの公表） ・労働者、労働組合、教育者、使用者の意見の聴取
4	衡平性と市民の権利の推進	・AI開発・導入者に違法な差別や濫用をしない責任を課す（刑事手続や公的給付が念頭。人事採用や住宅取引でのAI利用ガイダンスも検討される）
5	消費者、患者、旅行者及び学生の保護	・AIの詐欺、偏見、差別、プライバシー侵害等からの保護措置（医療、金融、教育、住宅、法律、交通などの分野で重要）。特に消費者保護のためのDDや監視・説明義務等、医療・福祉サービスにおけるAIの監視措置など
6	プライバシーの保護	・プライバシーと機密性のリスクの軽減（特に、個人情報の収集・利用や個人に関する推論をリスクとして念頭に置いている） ・プライバシー強化技術（PETs）などの利用
7	連邦政府におけるAIの利用の促進	・AI人材を確保・登用、全従業員を訓練 ・テストやリスク管理の手法、AI出力に組み込む「透かし」の技術などの検討を勧告
8	米国の海外におけるリーダーシップの強化	・同盟国やパートナーと協力 ・競争する他国を含め責任あるAIの原則の推進に努力

Fig.5 アメリカ AI 大統領令における AI 規制範囲の広さ

この大統領令で一番重要なのは安全性とセキュリティに重きを置いている点である。例えば、核兵器や生物兵器の設計に使われる可能性のある基盤モデルや、海外から攻撃されるリスクのある基盤モデルなど、民間および軍事用途の双方に使用できるデュアルユース基盤モデル開発者に対する、安全性テストの結果報告義務や外国との AI 取引の報告義務などが含まれている。この大統領令は各行政官庁に向けた対応命令であり国民に向けた命令ではない。項目に応じて 30～540 日以内に対応する義務があるので、どんどん規制が出てくると思われる。法律化して義務付けられるものやベストプラクティスを作りなさいというものまであるので、アメリカも EU のリスクベースアプローチと同様にハードローとソフトローを分けて動いてきている。

技術開発者にとって重要な事の一つは、イノベーションと競争の促進のところで、知的財産問題への取組が盛り込まれており、例えば AI と著作権の問題や独占禁止法の観点でどのような動きがあるかを見ておかないといけない。また、消費者保護の為のデューデリジェンスや監視、説明義務等、医療・福祉サービスにおける AI の監視措置など、個別分野に特化したことも検討しようとしているので、関係のある企業は重要視しないといけない。さらに、プライバシー保護の観点でプライバシー強化技術を導入しようとしている。個々の情報の身元を明らかにせずに検討・分析ができるので、プライバシー情報の漏洩リスクを低減し、組織の壁を超えたデータ利活用を可能にするというメリットの反面、どこまでのことを認めてもらえるのか、

またどういう対策を組まないといけないのかという事が重要になってくる。

2.2.4. 中国の AI ハードロー

中国は着々とハードローの施行・導入を進めている。インターネット情報サービスのリコメンドや深層合成や声の合成をする技術などについては国の統制下に置かれる。世論に影響を与えるなど一定の AI に対しては完全に管理し言論統制したいということだと思われる。また、反スパイ法の改正により、データや分析に関しても規定対象が伸びてきているので、場合によっては出国できないという状況になりかねない。生成 AI の基本開発に対しては開発自体の内容に介入し出している。社会主義体制の転覆をそそのかすような生成 AI や他の民族意識を称揚する生成 AI は認められない。

2.3. 間違った言説による日本のソフトロー選択

2.3.1. 誤解をベースにした言説

「アメリカは自由な AI ビジネスのためにソフトロー重視の立場をとり、EU はがちがちの複雑なハードローを志向する。いずれ世界はビジネスのためにソフトローになるので日本は EU に追随してはならない。」と言っている人が日本には多かった。ところがアメリカ大統領令によってこの言説が完全に間違った言説だったという事が明らかになった。アメリカも EU もそれぞれハードローの部分とソフトローの部分で規制対応しようとしていた。

2.3.2. 守ろうとするものの違い

アメリカ、EU、イギリス、カナダは民主主義的価値観を守ろうとしている。人権、健康、安全、民主主義、法の支配の 5 つ、企業、国家自体を合わせれば 7 つを守りたいというのが西側共通の価値観である。日本はごく一部の AI 開発者の心情を守ろうとした。規制化されるとよくないという先入観があったので、ソフトローの方向に向かった。アメリカ、EU、イギリス、カナダとは対立したいわけではないけど日本が勝手に孤立してしまっている。

中国は国家ではなく国家体制を守ろうとしている。法規制が中心となるので、西側諸国とは対立関係になる。日本だけが AI 法規制がないので、隙を突いた AI 攻撃の対象となりやすい。

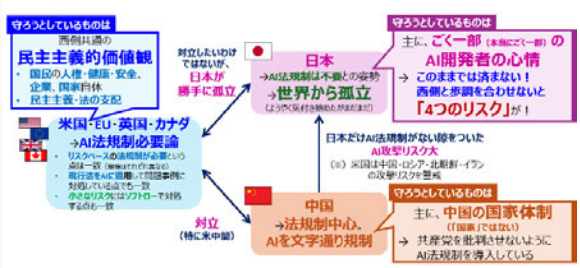

Fig.6 米欧中日の守ろうとするもの

次回の講演では、これらの対応策について話す予定である。

3．おわりに

アメリカ、EU、中国、の AI 法規制の最新動向とそれに対する日本の現状を解説していただいた。多面的で幅広い情報収集とそれらの情報を読み解く洞察力で大局的な関係性や細部の具体的事項など、大変に興味深いお話しで 1 時間の講演時間が短く感じた。

アメリカと EU はどちらもハードローとソフトローを使い分けて両立させているが、日本だけ自ら後れを取った形になっていて、どうやって追いつくかを考えないといけない。追いつけていない現状において 4 つのリスクに直面するとの事であり、2 回目の講演会でその対応策についてお話しいただいた。

AI 法規制に関しては、2023 年後半から急進展を迎えている。ビジネス機器業界も無関係ではいられない状況の中で、世界の動きと日本の対策について今後も注目していく必要があると考えている。

講演会には会員各社の方が多数参加され、講演終了後の質疑応答、講演会前後のディスカッションでも多くの質問や意見があり、講演内容への関心の高さが伺えた。

最後に、三部様にはお忙しい中、時間を割いていただき、分かりやすい講演を行っていただいた。この場を借りて御礼申し上げる。

2023 年度「ビジネス機器関連技術調査報告書」“Ⅰ－２－１”部

発行　2024 年 6 月
一般社団法人 ビジネス機械･情報システム産業協会（JBMIA）
技術委員会 技術調査専門委員会
〒108-0073　東京都港区三田三丁目 4 番 10 号 リーラヒジリザカ 7 階
電話　03-6809-5010（代表） / FAX　03-3451-1770