AIガバナンスの動向

三部 裕幸 ●弁護士・ニューヨーク州弁護士／大阪大学 招聘教授（社会技術共創研究センター）

世界中でAI法制度に向けた動きが急進展している。日本でもAI基本法案が検討されているが、以前から議論はソフトロー偏重だ。企業は、AI開発・利活用の「4つのリスク」への自主対策が不可欠だ。

2023年後半から、世界中でAI法制度に向けた動きが急進展した。米欧の動きの一部は、それ以前からの検討に基づいている。これと比べ、日本の議論の中心は法的拘束力のないガイドラインや業界ごとの規範など「ソフトロー」となりがちで、あまりにも偏っていた。さらに、検討されているAI基本法案が成立しても、企業は現行法に違反するリスクを含むAI開発・利活用の「4つのリスク」への自主的な対策が欠かせない。

以下では、まず海外と日本の動きの概略を記載した上で、現時点での状況をベースとしたAIガバナンスにおける留意点を述べたい。なお、本稿の情報は網羅的なものではなく（関係する情報のごく一部にすぎない）、また、分かりやすさを重視し本稿全体で厳密な書き方をしていないので、ご了承いただきたい。

■海外と日本の動きの概略

世界で最も早く包括的なAI法を成立させたEUから順に、米国、中国、そして日本の動き、また補足的に国際機関の動きの概略を述べる。

●EU：AI法のリスクベース・アプローチ

AI法の成立は2024年5月であり、同年8月に発効した。個別の条文の施行時期は段階的に設定されており（後述）、その一部は本書発行時に、既に施行されている。

【AI法の目的、適用範囲、制裁金】

AI法の目的は、AIビジネスの促進とリスク対策であると言える。27の加盟国から成るEUで法律がバラバラでは、EU域内でAIビジネスがしづらい。そのため「デジタル単一市場」をつくってビジネスを促進することは、EUの長年の政策である。一方で、人権・健康・安全・民主主義・法の支配などへのリスクに応じた対策を講じている[1]。

AI法は、EUにAI商品やサービスを提供する日本企業にも適用がある。AIそのものをEUに届けなくても、AIによる分析結果を届ければ適用される。違反に対する制裁金の金額も大きい[2]。そのため、EUと関わりを持つ日本企業の対策は必須である。

【リスクベース・アプローチ】

AI規則案のポイントは、リスクベース・アプローチである。AIシステムのリスクを4つに分類し、リスクに応じた対応を取るというものである。その概要と施行時期は資料3-1-5の通りであるが、ハードロー（法的拘束力のあるルール）とソフトローを併用している点に特徴がある。

資料3-1-5　AI規則案のリスクベース・アプローチの概要

リスク	該当するAIシステム（例）	措置		施行時期
許容できないリスク	・子どもや障害者などの脆弱性につけこみ不利に扱うAI ・国が国民に社会スコア付けして不利に扱うAI ・逮捕・起訴を目的とした公共の場でのリアルタイム顔識別など	禁止		2025年2月2日
ハイリスク	・安全に関わるAI（医療機器、機械、船舶など） ・主に差別・偏見・迫害などにつながりやすいAI（人の生体識別・分類、雇用・入学の決定、貸し付けの決定、犯罪・再犯予測に使われるAIなど、一定の類型）	ハードローの規制 （ただし極端な規制を課そうとはしていない）		安全に関わるAIについては 2027年8月2日 それ以外は 2026年8月2日
ローリスク	・チャットボットやディープフェイクなど	透明性の確保義務	行動規範が推奨される	2026年8月2日
最小リスク	・上記以外のAIシステム	規制なし		

※施行時期に関する細かな点は省略した。

出所：筆者

このリスクベース・アプローチの中心はハイリスクのAIシステムであり、法的拘束力のあるハードローの規制が課される。具体的には、AIシステムの提供者がリスク管理システムの導入やデータガバナンス、記録の保持、人間の監視など7項目の要求事項を守れているかどうかを評価する義務（適合性評価の義務）などが課される。

しかし、極端な規制を課そうとするものではない。すなわち、要求事項の多くは人間が従来ビジネスでやってきたことをAIビジネスに適合させたものにすぎない。さらに、適合性評価は原則として自己評価で足り、第三者評価が必要な例外は安全に関するAIなどに限られる。しかも、提供者が依拠できるハイリスクAIの整合規格や共通仕様が定められた場合、それに依拠すれば要求事項を守っていると推定される[3]。なお、提供者だけでなくデプロイヤー[4]などにも一定の義務がある。

ローリスクのAIシステムにおいては、AIであることをユーザーに示すといった透明性の義務があるのみであり、最小リスクのAIシステムと併せて行動規範が推奨されている。ただし、許容できないリスクのあるAIシステムの禁止の施行時期（2025年2月2日）が早いことは盲点になりやすいと思われるため、注意が必要である。

【その他の義務の例】

以上のほか、汎用AIの提供者にも一定の義務が課される（施行時期は2025年8月2日）。また、AIシステムの提供者やデプロイヤーには、従業員などのAIリテラシーを確保する義務が生じる（施行時期は2025年2月2日）。これらの施行時期も早いので注意が必要である。

【AI法の影響と他の法令との関連】

EUのAI法は、EU域外の国々の政策にも影響し、かつEUの他の法令と関わっている点でも重要である。

まず、EU域外の国々の政策に影響し得る。実際、2024年12月には韓国がAI基本法を成立させており、世界で2番目にAIの包括的な法制度を制定した国と評されている。影響力の高いAIに関する義務が加重されている点や過料の規定がある点などで、EUのAI法と共通しているとの評価がある。

また、EUの他の法令と関わっている点でも重要である。例えば、2024年12月に発効したEUの新たな製造物責任指令では、AI法におけるAIシステムの提供者は製造者として取り扱われ、同指令（に基づき制定されるEU加盟国の法律）上の義務を負う。また、EUのGDPR（一般データ保護規則）やデータに関するEUの法令とも関わる。

●米国：ハードローとソフトローの組み合わせ

米国については、ソフトロー重視で自由にAIビジネスをさせる国であるという誤解が一部にある。しかし、ソフトロー一辺倒では全くなく、ハードローとソフトローの組み合わせが志向されてきた。本稿では、そのうちハードローの面に着眼して、現行法をAIに適用する動き、新たな法制度を作る動き、そして2023年10月の大統領令の概略を述べる。

【現行法をAIに適用する動き】

既に、連邦や州などによって、現行法がAIに適用されている。特に、連邦政府機関ないし行政委員会が、どの法律をどのように適用するかの方針をウェブサイトや報告書などで公表している点は重要である。例えば、連邦取引委員会（FTC）が2021年、FTC法などの法律違反となるケースとして、企業が人種・性別などのバイアスのあるAIを利用したり、AIの問題を顧客や消費者に伝えなかったりしたことなどを例示し、その後も公表を行っていることが挙げられる。取り締まりの実例もある。

拘束力のないソフトローを定める際にも、現行法を意識し、現行法と関連付けたものとなっているケースが見られる。例えば、食品医薬品局（FDA）が2025年1月に公表したガイダンス案などである。

米国の現行法は日本の政策にも影響を及ぼしている。例えば、米国は2022年10月に、AIに使われる半導体やその製造に必要な装置・技術の中国への輸出を制約しつつ、日本とオランダにもこの動きに対する同調を求めており、日本は2023年にこれに応じている。

【新たなAI法制度を作る動き】

民間のAIビジネスに影響する新たな法制度を作る動きも、連邦・州・自治体のレベルで見られる。動きが活発なのは州のレベルである。例えば、カリフォルニア州のプライバシー法制（CCPAおよびCPRA）やイリノイ州の生体情報プライバシー法（BIPA）など、多くのプライバシー法制が州において整備・提案されている。2024年5月には、コロラド州が消費者をAIによる差別等から守ることを主眼とした総合的な法制度を可決成立させた。同年9月には、カリフォルニア州がAI生成コンテンツの透明性やAI学習データに関する2つの州法を可決成立させた。

自治体レベルでも動きがある。例えばニューヨークは、雇用主による採用の場面におけるAI利用を規制する法律を施行済みである。

ChatGPTの登場以後、連邦議会の動きも急激に活発化しており、超党派での公聴会等が開かれAIに関する法案も多く提出されている。

【バイデン政権の大統領令と、第2次トランプ政権の方針】

これらの動きの中で2023年10月30日、バイデン政権の大統領令が公表された。この大統領令は、AIの安全性とセキュリティ、イノベーションと競争の促進、労働者の支援など8つの指導原則に基づき、各原則に対応した内容を行政官庁に命令するものである。実際、新たな法制度づくり、現行法の適用、ソフトローの整備などが命令されており、これまで各行政官庁はその命令に対応し

て施策を講じてきた。また、EUのAI法で対処されているリスクに加え、安全保障へのリスクも明確に意識されている。

だが、大統領選に勝利したドナルド・トランプ氏は、バイデン政権の大統領令を大統領就任初日（2025年1月20日）に覆した。しかし、当該大統領令に基づき行政官庁が既に行った施策まで完全に覆すのか、それとも表紙と名前だけを覆し、実質的にはバイデン政権の大統領令の内容で引き継げるものは引き継ぐことにするのかは、本稿執筆時点では不明である[5]。

●中国：ハードローによる規制重視

中国は近年、AIに関しハードローによる規制を採用する姿勢を明確化した。そのような中国のハードローは、一面では、西側諸国に類似したAI法制度となっており、例えば自動運転の普及策（事故時の責任分担を含む）を法律や条例で定める、プライバシーや知的財産権の保護を新法に含めるなどしている。しかし他面では、中国特有の事情に基づく規制が導入されている。例として次のものがある。

まず、インターネット情報サービスにおける2つの管理規定により、アルゴリズムによるリコメンド、ディープフェイクや声の合成といった深層合成を規制している。中でも、「世論属性」や「社会動員能力」などがある影響力の大きいリコメンドや深層合成を行う企業は事前に届け出をしなければならず、AI開発段階からさまざまな管理を受ける。

次に、生成型AIサービス管理暫定弁法は、イノベーションへの配慮を漂わせつつも、生成AIサービスの提供と利用が「社会主義の核心の価値観を堅持」するものでなければならないと規定し、国家権力の転覆や社会主義体制の打倒の煽動、国の安全保障や利益を損なうこと、国家の分裂の煽動などのコンテンツの生成を禁止している。

さらに、反スパイ法（スパイ防止法）が近時改正され、AIとの関係でも適用されやすくなった。

これらに共通する特徴は、中国の国家レジーム維持を目的とした規制であるという点である。「中国では自由にビジネスができる」という幻想を抱くと足をすくわれることがあり得ることになる。

●日本：ソフトロー偏重

対して日本では、ソフトロー偏重で議論が進められることが多かった。その論旨は「ルールベースの規制がイノベーションを阻害し得るなどとして法律の検討を極力行わない」というもので、各国とは出発点と方向性が異なる。すなわち、各国はリスクの洗い出し・分析から出発し、ハードローとソフトローで対策を講じてきた。その際、ハードローについては、新法の制定のみならず、現行法をAIに適合させるための対策や解釈の明示なども行われてきた。一方、日本では「規制はイノベーションを阻害する」という前提を置くところから出発し、リスクの洗い出しや分析に関心がなく、はなからソフトロー志向であるという点に特徴がある。

日本は2023年のG7において議長国として「広島AIプロセス」を提唱し、翌2024年のOECDでは49の国・地域が参加する「広島AIプロセス・フレンズグループ」が立ち上がるなどの成果があった。しかし、国内でAIに関わりを持つハードローの検討が行われた事項は限られ、ソフトローとして総務省・経済産業省の「AI事業者ガイドライン」などが公表された[6]にとどまる。

そのような中、AI戦略会議・AI制度研究会の中間とりまとめ案が2024年12月に示された。同案では「政府に対しては、本とりまとめを踏まえ、AIの研究開発・実装が最もしやすい、他国のモデ

ルとなるようなAIに係る法制度を含む制度整備を速やかに実施していくことを期待する」と述べられている。その要旨は、①AIの開発・利活用に規制をかけたくない、②事業者は既存の法令を守れ、というものである。しかし、①悪意ある者の攻撃リスクを野放しにしかねない、②日本の既存の法令こそがAIビジネスを阻害する事態が往々にしてあるのに対策が立てられていない、という問題がある。さらに、各AI大国よりも圧倒的に遅れて法制度に着手したのに「他国は日本の法制度をモデルとしろ」と述べるのは非現実的である。

なお、本稿執筆時点では、国会提出に向けて準備が進められているAI基本法案の内容が不明であるため、ここではその内容を紹介することができない。

●国際機関の動き

以上に加え、OECD、GPAI（Global Partnership on AI）、ユネスコなどの国際機関にも動きが見られる。また、欧州評議会[7]は、2024年にいわゆるAI条約を採択した。

■現時点でのAIガバナンスにおける留意点――4つのリスクを踏まえた企業の自主対策

日本ではソフトロー偏重のため具体的なAIビジネスの実例で何をすればよいのかが分かりにくいという批判がある上、AIを想定せずに制定された現行法こそがAIビジネスの障害になっている点が多くのケースで意識されにくくなってしまっている。

このような状況では、企業が自ら個別のAIビジネスのリスク分析をして自主対策を講ずることが不可欠である。その際に分析すべきリスクは、次の「4つのリスク」である。

①悪意ある者から攻撃を受けるリスク
②何が許され許されないかの羅針盤がないリスク
③現行法が障害となるリスク
④海外とAIルールが異なることから輸出入・投資・M&Aの障害となるリスク

このうち③については、日本のソフトロー偏重論に惑わされず、個別のAIビジネスに適用される現行法（外国法を含む）を特定した上で、違反しないように対策を講じる必要がある。

その際、日本の現行法対策のみならず、EUのAI法が適用されたと仮定した場合に守らなければならない事項、さらに、必要に応じて米国の連邦・州の規制を守れるようにする（べく今からできる対策を講じておく）のが現実的な方策であろう。これらへの対策が講じられていれば、実際にAIビジネスを行う国において今後制定・改正される法令に対応するためにAIビジネスを大きく後戻りさせなければならないリスクや、そのためのコスト・負担を小さくできるだろう。

1. 特に、ナチスなどの歴史的経緯から、差別や迫害、監視社会、不当なレッテル貼りなどのリスクへの対策が強く講じられている。
2. 最大で3500万ユーロ（約60億円）、または全世界売上高の7％のうち、より高い金額が上限。
3. 整合規格や共通仕様は、ハイリスクAIに関する施行期日を目指して整備されていくとみられる。
4. デプロイヤーをどのように訳すかは訳者によって異なっているが、おおむねAIシステムを利用する者と理解しておけばよい。
5. 米国内では、当該行政官庁の施策の一部をトランプ政権が引き継ぐのではないかという見方を複数のメディアが既に報じている。実際、2025年1月23日のトランプ政権の大統領令によれば、覆されるのは同大統領令に示された方針と矛盾し得る施策である。
6. 2024年4月。改訂版である1.01版は同年11月。
7. 欧州評議会は、EUの機関ではない。

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2025年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp