AI活用と規制の綱引き

◆EUがAI規制法の適用時期を延期

欧州委員会は2025年11月19日、段階的に適用が進められるEUのAI規制法（AI Act）について、自動車や医療機器、公的インフラなどに使われる高リスクのAIに関する規則の適用時期を26年8月から最大16ヵ月（27年12月まで）遅らせる方針を発表した。24年に包括的なAI規制を法制化したEUだが、厳しい規制が技術革新を阻害すると反発する欧米のIT大手企業や米国政府に配慮した形だ。

この数年で生成AIなどが劇的に進化し、仕事や生活のあらゆる場面で活用されている。同時に、ハルシネーションやバイアス、誤作動、判断過程のブラックボックス化、個人情報や機密情報流出、知的財産権侵害、悪用など、さまざまなリスクや課題が存在する。各国がAIの研究開発にしのぎを削る一方で、こうしたリスクに対応するため、規制や法制度の整備が進められている。

AIに関するリスク例　（出所：総務省・経済産業省「AI事業者ガイドライン1.1別添　概要」）

大分類	中分類	リスク例
技術的リスク（＝主にAIシステム特有のもの）	学習及び入力段階のリスク	データ汚染攻撃等のAIシステムへの攻撃
	出力段階のリスク	バイアスのある出力、差別的出力、一貫性のない出力等
		ハルシネーション等による誤った出力
	事後対応段階のリスク	ブラックボックス化、判断に関する説明の不足
社会的リスク（＝既存のリスクがAIにおいても発生又はAIによって増幅するもの）	倫理・法に関するリスク	個人情報の不適切な取扱い
		生命等に関わる事故の発生
		トリアージにおける差別
		過度な依存
		悪用
	経済活動に関するリスク	知的財産権等の侵害
		金銭的損失
		機密情報の流出
		労働者の失業
		データや利益の集中
		資格等の侵害
	情報空間に関するリスク	偽・誤情報等の流通・拡散
		民主主義への悪影響
		フィルターバブル及びエコーチェンバー現象
		多様性・包摂性の喪失
		バイアス等の再生成
	環境に関するリスク	エネルギー使用量及び環境の負荷

筆者注　「トリアージにおける差別」：医療現場などで患者の優先順位付け（トリアージ）を行う際に、AIのアルゴリズムや学習データのバイアス（過去の受診傾向の偏りなど）により、判断に不適切な偏りや不公平が生じること。
「フィルターバブル」：アルゴリズムがユーザの過去の検索履歴などに基づいてユーザの関心ある情報のみを選別すること。
「エコーチェンバー」：限られたコミュニティ内で同じような意見が繰り返し共有されることで、それを正しいと過信すること。

◆米国は州独自規制にトランプ政権が懸念、中国は政府の強力な管理と開発促進

先行するEUでは21年にAI規制法案が発表され、24年5月に成立した。リスク度

により、許容できないリスク（禁止）／高リスク／限定的なリスク／最小リスクに分類し、程度に応じ罰則付きの規制を定めた。人権侵害に関わるなどのAIの禁止は25年2月に適用開始されており、高リスクAIは透明性やデータ品質、監査などの厳しい要件が26年8月から適用の予定だったが、前述の通り延期となる。

米国は、23年10月のバイデン政権時の大統領令で、AIの安全性・公平性確保などの方針が示されたが、包括的な連邦法制は存在せず、カリフォルニア州などが州独自のAI規制を制定している。トランプ政権は、AIの規制よりも技術開発促進をより重視する姿勢を示している。25年11月18日、トランプ大統領は、州による過度な規制が技術発展を阻害する恐れがあるとし、連邦統一の基準を整備するよう議会に求めた。ただし、基準の内容には言及していない。

中国は、22年の「インターネット情報サービスアルゴリズム推薦管理規定」、23年の「生成AIサービス管理暫行弁法」、25年9月の「AI生成合成内容標識弁法」など、AI関連法令を整備するとともに、AIに関する国家標準の制定も進めている。AIを国家戦略技術と位置づけ、政府が強力に管理・規制を行うと同時に、国際競争力を確保するための技術開発を推進する戦略と思われる。

韓国では24年12月、EUに続き世界で2例目の包括的なAI基本法が成立し、26年1月から施行される。AI事業者の義務と責任などを定め、罰則規定も含まれる。

◆日本はソフトローで自主的取り組み促す、企業はリスク対応体制整備が必要

日本では24年4月、経済産業省と総務省が「AI事業者ガイドライン1.0」を策定し（25年3月に1.1へ改定）、安全性・透明性・公平性・プライバシー保護など、AI開発者・提供者・利用者のリスク管理に関わる基本的考え方と指針を示した。

25年9月には、AIに特化した初めての法律「人工知能関連技術の研究開発及び活用の推進に関する法律」（AI法）が施行された。国が指針整備、情報収集や事業者への指導を行い、AI活用に伴うリスクへの対応を図りながら、AIの研究開発と活用を推進することを目的とする。罰則規定のない「ソフトロー」である。

日本では今のところ、EUや韓国のように罰則を設けて強制するのでなく、自主的な取り組みに委ねられる部分が大きい。AI開発・提供事業者だけでなく、利用企業もAIの利点とリスクを正しく理解し、リスクガバナンス体制の整備やリテラシー向上を図り、適切にAIを活用することが必要だ。　【本間克治】