

EU指令・米国の議論を踏まえた AIシステムの「製造物責任」

AIの誤解答や不適切提案による 損害の責任分担ルールの議論加速を

わが国では欧州連合（EU）のような包括的な事前規制がないまま、AI（人工知能）エージェントの顧客向け利用が急拡大している。そのためAIの誤判断による損害発生リスクが高まっているが、損害賠償責任の分担は契約解釈によるほかない。判例法国でないわが国では、法律で責任分担ルールを事前に明確化しておくことが、AIシステム導入の判断を容易にする。こうしたことから、AIシステムを製造物責任法の対象とすべきである。関連当事者が多く、サービスが継続学習により変化するAIの特色を踏まえた法改正の議論がまたれる。

瓜生・糸賀法律事務所
弁護士・弁理士

長野 聡



不明確な責任分担ルールで 対顧客AI利用が進む日本

わが国企業では人手不足の中で業務プロセスにAIシステムを組み込むAIエージェントが、企業内部事務の効率化だけでなく、顧客向けサービスに利用さ

れる例が著増している。他方でEUのような包括的な事前規制がなく、リスク管理は玉石混淆である。

そのため、AIエージェントに組み込まれたAIシステムが誤った事実提示（誤回答）や不適切な提案を行い、顧客または

第三者に損害を与える（以下、

事故）リスクが高まっている。

その責任は誰が負うのか、金融機関経営者からよく不安を聞く。

金融機関も含め企業のAIシステム利用を促進するためには、責任分担ルールが明確になっていくことが、ぜひとも必要であ

る。責任分担の明確化の方向性は

二つある。一つはEUの規制と同様の事前立法アプローチだ。

これは開発業者に行政上の事前規制を課して事故の頻度を抑制するとともに、製造物責任法をAIシステムにも拡大適用（ま

たは新規立法)し、AI開発業者や提供業者に「欠陥」を要件に厳格な責任(無過失責任)を課して消費者保護を図るものがある。

もう一つは米国で議論されているもので、イノベーションとのバランスを重視して事前規制を抑制し、製造物責任のAIシステムへの適用拡大も見送る。

他方で、事例・判例の蓄積を待ちつつ、懲罰的な損害賠償や損害保険の拡充により、消費者に対する事後補償を厚くする判例法アプローチである。

以下ではEU規制と米国での議論を比較して紹介しつつ、わが国製造物責任法の対象にAIシステムを含める法改正の在り方を検討する(図表)。

EUはAI責任指令撤回、製造物責任指令を改正

EUは2022年9月に、AIの誤判断に伴う損害賠償責任について過失責任を維持しつつ、AI開発業者や提供業者に対する証拠開示命令や因果関係の推定を含んだAI責任指令案を公表した。その後、これを時期尚

早として25年2月に撤回。一方、強力な行政上の事前規制を持つEU・AI指令の施行を踏まえ、消費者の予測可能性を高めるため、24年12月に製造物責任指令を改正した。

同指令は、過失を要せず欠陥のみを責任原因とする製造物責任(厳格責任)の対象に、AIシステムやそのアップデートを加えている。事前規制で事故を減らすとともに、事故により損害が生じれば消費者が賠償を受けやすくなる事前立法アプローチである。もつとも、消費者保護法の性格から被害者は消費者のみで、損害賠償の範囲も心身の損害に限られ、財産的損害は含まれていない。

注目すべきはAIが製造物と異なる点(推論過程の検証困難性、継続学習によるサービス自体の連続変化、複数主体のサービス提供への関与)を踏まえて、消費者保護を強化したことである。具体的には、AI開発業者や提供業者にはアップグレード後も責任を課し、また輸入者や販売者の責任も定めた。EU・AI指令を前提に、欠陥の推定

(安全基準不順守の場合等)、欠陥と損害の因果関係の推定規定を設け、証拠開示規定(金融機関による信用力評価等ハイリスクAIシステムに限る)も設けている。

AIシステムの事故時の責任分担に係る米国の議論

米国では1960年代以来、製造物責任(製造・設計・警告上の欠陥による厳格責任)は、消費者保護の見地から判例とリステートメント(注1)によって発展してきた。対象は動産から建築物、電気のほかソフトウェアにも拡大している。頒布や使用の状況が動産と十分類似している場合には、製造者は合理的に安全な態様で確実に作動させる義務があると解されている。

また被害者が法人の場合は適用対象外であるものの、製造物責任と実質は大差ない運用がされている。すなわち通常のネグリジェンス(過失責任)でも、裁判所は過失をリスク対効用テストで判断し、設計や警告が不合理に危険か否か判断している。しかし第2次ドナルド・トラ

ンプ政権は、支配的なAI開発業者が米国に所在することを踏まえて、イノベーションを阻害しかねない製造物責任のAIシステムへの適用拡大や、連邦レベルでの包括的な事前規制には消極的である。もつとも米国では事故時には、懲罰的賠償・成功型弁護士報酬・証拠開示制度(ディスクバリー)を背景に、毎年5万~10万件もの製造物責任訴訟が起こされている(日本では毎年平均10万件)。それを受けて、個別契約・判例による解決(合理的に安全な回答を提供するのに十分な学習経験や推論の鍛錬をシステム提供者に求める)や、損害保険拡大、AI開発業者等への一部事前規制の強化の組み合わせによって対処する方向性が議論されてきた。厳格責任が保険コストを大幅に増加させ、消費者や利用者の負担増となることが、むしろ警戒されている。

事故時の責任分担ルールを明確化することは、これまでの製造物責任法形成と同様に、個別解決を積み重ねて消費者保護立法がようやく議論される判例法

〔図表〕

欧米日の製造物責任法の比較とAIシステムへの適用範囲拡張の論点

		消費者保護法			不法行為法特則		
項目	EU製造物責任指令(旧EUPLD)	EU製造物責任指令(新EUPLD)(2024年12月発効(下線部について拡大))	EU・AI責任指令案(AILD) ※推論ブラックボックスに対応(証拠開示命令、推定規定)、25年2月撤回	米国：製造物責任第3次リステートメント	日本：製造物責任法(太字は欧米より広い) ※根拠は危険責任、報償責任、信頼責任	わが国法制の論点	
①行為主体	物・サービス	欠陥ある製造物(動産、AI含まず)	+ソフトウェア、オンラインAI、アップグレード等関連サービス	AIシステムによる出力またはそのエラー	欠陥ある製造物(動産、AI含まず)、判例はソフトウェアにも責任を認めるものがある	欠陥ある製造物(動産、AI含まず) ※旧EUPLDと同じ	AIシステムへの適用範囲拡張
	過失・欠陥	無過失責任、欠陥責任	無過失責任、欠陥を総合事情勘案(製造者の管理を離れた時点、供用後の継続的な学習能力、サイバーセキュリティーを含む製品安全基準、最終使用者の期待等)	契約外の過失責任	無過失責任、欠陥責任	無過失責任、欠陥責任 ※旧EUPLDと同じ	AIシステムの特徴に沿った考慮要素の拡大・例示
	賠償請求対象	生産者	製造者、EU内への物流代行業者、販売者(特定できない場合)	(規定なし、EU法一般による)	生産者	製造業者等 ※旧EUPLDと同じ	AI開発業者・提供者(物流代行、販売者を含む)への拡張
②被害主体(賠償請求権者)		自然人 ※日本法より狭い	自然人、法人、 <u>集団訴訟適格団体</u>	自然人、クラスアクション	他人(個人、法人) ※旧EUPDLより広い	—	
③損害賠償の範囲	死亡、障害、財物損傷	+データ消失や改竄 ※日本法より狭い	死亡、傷害、財物損傷+財産損害(AI判断による不利益等)+精神的損害(プライバシー侵害等)	死亡、傷害、財物損傷(財産損害は不法行為法の過失責任による)	生命身体、財産損害(含む精神的損害、逸失利益) ※旧EUPLD、AILDより広い	— (現行でも相当因果関係の範囲内)	
④推定規定	なし	欠陥の推定(安全基準不順守の場合ほか)、欠陥と損害の因果関係推定	AIに起因する全損害と過失との因果関係推定、ハイリスクAI(信用力評価など)システム提供者や使用者(含む記録保持義務者)への証拠開示命令(違反すると過失推定、評価根拠事実の認定義務)	欠陥の推定(安全基準不順守の場合ほか)	なし ※旧EUPLDと同じ	AIシステムの特徴に沿った証拠開示命令、推定規定の追加	
抗弁	開発危険	開発危険の抗弁限定(製造者管理下期間に限定)	—	開発危険(判例で制限)	開発危険 ※旧EUPLDと同じ	抗弁の限定を設けるか	
行使期間(出訴期間)		3年	—	2~3年(州法による)	3年 ※旧EUPLDと同じ	—	
⑤他制度		強力な行政規制、少ない訴訟、懲罰的賠償なし、訴訟保険も少ない		多い訴訟、懲罰的賠償、弁護士成果報酬、訴訟保険	EUと同じ	行政規制は現時点では弱い、他はEUと同じ	

(注) EUPLD=EU Product Liability Directive、AILD=EU AI Liability Directive

(出所) 各種資料をもとに筆者作成。

アプローチといえる。損害保険会社は、AIシステムの残存期間全体をカバーする補償を消費者に提供するためには政府の保険料補助が必要だと主張するとみられる。

結局、EUでも米国でも、AIシステムの関係者が多いなか（開発業者、提供者、利用者）、アップデートによる継続利用を踏まえて、責任の担い手を増やしつつ対応することとなる。事前規制が厳しければ、事故は少なく、事故時には消費者に限り責任追求しやすくする（補償額は不法行為一般と同じ）のがEU型。または事前規制が緩く、事故や間接被害（注2）は頻繁に起こり得るが、事故時には莫大な賠償と保険カバーが求められるのが米国型。これが2大潮流だといえる。

日本の議論の現状と製造物責任法改正の論点

わが国の製造物責任法（以下、法）は、被害者に法人を含み、損害賠償請求範囲も不法行為として同一で広いなど、消費者保護よりも不法行為の特則の性格を持

つ点でユニークなものとなつていく。無過失でも欠陥（注3）ある場合に責任を問う点は欧米と同じである。

現行法の対象は製造物に限定され、AIシステムは対象となっていない。また、現時点で法改正の議論が政府でなされているとの情報はない。昨年9月に施行された「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）では、行政上の事前規制を具体的には何ら定めていない。同年12月に閣議決定した「人工知能基本計画」（AI計画）でも「AI利活用における事故や損害が発生した場合の民事責任の所在や範囲について在り方を検討する」と記載されているのみで、行政内部での検討段階にある。

こうしたなか実務では、企業内データおよびカスタマイズされたAIを業務に組み込むAIエージェントの導入が拡大している。これは大規模汎用AIを指している米国AI企業よりも、個別の課題解決を得意とする金融機関をはじめ日本企業やわが国AIベンチャーがリード

している。EUのような包括事前規制もない中で、AIの誤判断による事故が起こりやすい状況で、事故時の責任分担は個別契約の解釈によるほかない状況だ（注4）。今後、AIの活用を推進するのであれば、責任分担ルールを明確化する制度的な手当てが必要と考える。

前提として、米国のような懲罰的賠償・成功型弁護士報酬・証拠開示制度がなく、損害保険のリスクテイクにも限界がある下では、まず事故を抑えるための包括的事前規制（学習データや推論ロジックの記録保持、適切な警告、ハイリスクAIの特定等）を設ける必要がある。また、事故時に消費者等を保護するための法改正が求められる。論点は、以下のとおりである（注5）。

① AI開発者・提供者・利用者が継続的に顧客向けサービス提供に関与する特色を踏まえた責任分担
② 消費者保護を越え一般不法行為と同じ条項（被害者に法人を含み、賠償範囲に財産的損害を含む）の維持

③ 欠陥の存在や欠陥と損害との因果関係の推定規定導入

AIシステムの誤回答や不適切提案への対応方法

まず、AIの判断の是非を人がチェックして顧客に提供する場合には、その人の注意義務違反（契約違反、不法行為）を問えばよい。そこで、以下では人がAIの判断に関与しない場合を想定する。

AIシステムは、事実に対する誤回答をする場合と、不適切な提案（医療AIの不適切なアドバイスや提案で心身の不調を来す場合など）をする場合がある。

前者の誤回答は、学習情報や推論ロジックの不適切さから起こる。こうした誤りは欠陥に相当し、データ投入や推論構築に注意義務違反があることから、違反ある責任者を特定すべきである。

このため、① AI開発者・提供者・利用者を広く責任対象とすべきであるほか、② 財産的損害も、現行法と異にする理由はなく賠償範囲とすべきである。

また、特にAIシステムを信頼した消費者保護の観点からは、③欠陥の存在や欠陥と損害との因果関係の推定規定は、少なくとも対消費者には導入すべきである。

他方、AIシステムが不適切な提案をすることは、AIの内在的限界ともいえる。AIはそもそも不変の真理を回答しているのでなく、過去データの平均から見て、聞かれていた条件に最も合う(尤度の高い)回答を出しているためである。

AIも人間同様に、前提条件や推論ロジックの能力的な限界から判断を誤ることがあり得る。正解が一意でない提案をAIに求める場合には、プロの人間の知恵が関与すべきである(それがプロの存在意義である)。人を介さないAIエージェントの利用者は、AIの提案が必ずしも真実やベストでないことを甘受すべきではないか。

この場合のAIの欠陥は、その業界で平均的な人が関与した判断による回答よりも不適切な程度の回答を示したか否かで判断すべきである(注6)。その判

断の際には、①明らかな推論ロジックの誤りはAI開発者や提供者の責任、②学習や参照、インプット情報の不十分性は提供者や利用者の責任となろう。利用者が人を介さない提案を自ら求めている以上、③推定規定まで設けることは不要と思われる。もつとも、いわゆるハイリスクAIの人を介さない誤判断(自動運転車や医療薬品事故)については、事情が異なる。ハイリスクAIは、EU法にいう「人の健康、安全、基本的人権」に重大な影響をもたらしているものである。

この場合、まず利用者が、AIによる案(最適ルート等)の提示に人の判断を介することを求める選択肢がなく、AIの判断を信頼せざるを得ない。また、危険度も高く、開発者や提供者の報償も大きい。こうしたことから、事実上の結果責任を確保するために推定規定を置くことが考えられる。

* * *

本稿では欧米と比較するかたちでAI利用に伴う損害分担ルールについて不法行為法上の論

点と私見を述べた。消費者保護の見地からは、事前規制が守られない場合には損害額が不明でも最低の賠償責任を負う米国の例も検討すべきであろう。特に情報の塊であってAIと親和性が高い金融分野での利用が拡がる場合には、個人情報保護法と同様に特則ルールを先行して検討することも考えられるのではないか。今後、関係者の議論を期待したい。

(注1) 米国において法の分野ごとに各州の判例動向を分析し整理した上で、およその平均値と目されるところに従って法の現状を条文形式で記述し、コメントと注釈を付したものである。

2 日本生命保険の米国子会社は今年3月、弁護士資格を持たない生成AIのチャットGPTが顧客に法的アドバイスをした(非弁行為)ことで損害を受けたとして、開発元のオープンAIに対して損害賠償請求訴訟を起した。

3 「欠陥」とは、製造物に關するさまざまな事情を総合的に考慮して、「製造物が通常有すべき安全性を欠いていること」をいう。安全性に関わらないような単なる品質上の不具合は、

これに該当しない。

4 この点、経済産業省は、契約責任を問うための契約の解釈指針について「AI利活用における民事責任の解釈適用に関する手引き(第1.0版)」を公表した(2026年4月)。

5 ほかにも消費者保護の観点からの開発の抑制、クラスアクション導入、時効期間、情報セキュリティの欠陥性(アンソロピックのクロード・ミュトスの問題)、BPR(Business Process Reengineering)などの論点があるが、割愛する。

6 逆に、自動運転に係る最適ルート判断における「トロッコ問題」など人の判断基準の合意形成が難しい問題について、人が関与しないAIの判断には、平均的な人の注意義務を基準にして責任を問えない。トロッコ問題は、多数の生命を守るため少数の生命を犠牲にしてよいかという問題で、ドイツではその選択を禁じる規制がある。

ながの さとし

86年日本銀行入行。18年弁護士登録。20年弁理士登録。訳注書に『現代語訳 銀行業務改善集 語』(近代セールス社)。