



AIに関わる製品安全・製造物責任の国際動向

～AI技術の台頭を受けた各国の動向～

中西 紀 Kaname Nakanishi

松本 英里子 Eriko Matsumoto

REUWサポート部門 リスクエンジニアリング部
賠償・労災グループ
コンサルタント
専門は製品安全・製造物責任

REUWサポート部門 リスクエンジニアリング部
賠償・労災グループ
主任コンサルタント
専門は製品安全・製造物責任

安藤 悟空 Goku Ando

REUWサポート部門 リスクエンジニアリング部
賠償・労災グループ
上級コンサルタント（チームリーダー）
専門は製品安全・製造物責任

概要

昨今のAI技術の開発や普及により、様々な製品にAI技術が搭載され、我々の生活や労働環境は大きな変化を迎えようとしている。

AI技術の普及が進む中、欧州連合（以下EU）は、各種製品の変化やそれを販売する事業者の性質の変化に対応するため、EU加盟各国に製造物責任法や製品安全規制の整備方針を示し、一般製品安全規則や改正製造物責任指令が発効された。また包括的なAI規制であるAI法の成立やAIによる損害の法的責任を定めたAI責任指令の検討が進められた。

一方で、EU以外の各国はAI技術に特化した製品安全、製造物責任法に関する法整備は発展途上であり、基準やガイドラインの提示にとどまり、具体的な対応に関しては各事業者に委ねられている。

本レポートでは、EUの動向をベースとしてAIに関わる製品安全・製造物責任の国際動向について、具体的な事例や関連法案などを交えながら紹介する。

本レポートは、当社が2025年7月末までに実施した周辺動向調査の結果を取りまとめたものである。AI分野は動向の変化が著しいため、記載内容は今後更新される可能性があることをご了承されたい。

目次

概要	1
1. EU の動向	3
1.1. GPSR、改正 PL 指令と AI の関連性	3
1.1.1. GPSR と AI の関連性	3
1.1.2. 改正 PL 指令と AI の関連性	3
1.2. 欧州 AI 法	4
1.2.1. 欧州 AI 法の概要	4
1.2.2. AI システムの定義	4
1.2.3. 禁止される AI 行為	5
1.2.4. リスクベースアプローチ	5
1.3. 欧州 AI 責任指令案	6
2. 英国の動向	7
2.1. 自動運転車両法 2024 の概要	7
3. 日本の動向	8
3.1. AI 事業者ガイドラインの概要	8
4. 米国の動向	11
4.1. 連邦政府の動向	11
4.1.1. NIST AI リスクマネジメントフレームワーク (NIST AI Risk Management Framework) の概要	11
4.1.2. AI の安全・セキュリティ・信頼性に関する行政命令 (Executive Order 14110) の概要	11
4.2. 州の動向	11
4.2.1. コロラド州 AI 法	12
5. 中国の動向	13
5.1. 生成 AI サービス管理暫定弁法の概要	13
5.2. 国家人工知能産業総合標準化体系構築ガイドライン (2024 年版) の概要	13
5.3. 「AI」に対する PL 責任の想定	13
6. AI によって生じた損害に対する司法判断および和解事例	14
6.1. 対話型 AI 自殺訴訟に関する司法判断	14
6.2. 自動運転タクシー交通事故に関する和解事例	14
おわりに	15
参考文献	16

1. EU の動向

EU では直接的ではないものの AI に対応した製品安全・製造物責任に関する法整備が進んでおり、GPSR や改正 PL 指令の発効によって AI 関連製品に関わる事業者などに対する責任が示されている。さらに、AI 法によって AI に関する包括的な定義、規制が定められ、より具体性を持った法整備も進められている。

1.1. GPSR、改正 PL 指令と AI の関連性

EU における消費者用製品の安全要件について包括的に規定した一般製品安全指令（General Product Safety Directive 以下 GPSD）が改正され、2024 年 12 月に一般製品安全規則（General Product Safety Regulation 以下 GPSR）¹として適用が開始されている。GPSD は「指令（Directive）」であり、EU 加盟各国はこの指令に基づき、各自で国内法を整備することとなっていた。一方で GPSR は「規則（Regulation）」であるため、すべての EU 加盟各国に直接適用され、国内法と同様の拘束力を持つ点が大きな特徴である。

この GPSR では、以下に示す製品の定義を拡大することや、安全性評価などを義務付けることで、AI に関する安全要件をカバーすることとなった。

表 1 AI に関する GPSR の内容²

内容	条文	概要
製品の定義	第 3 条	（AI を含む） IoT 製品やリモート更新可能なソフトウェアを製品として定義
安全性評価	第 6 条	『進化、学習、予測機能』を踏まえて安全評価をすることを要求

1.1.2. 改正 PL 指令と AI の関連性

EU の加盟各国における製造物責任（PL）法については、欧州委員会から出された製造物責任指令（以下 PL 指令）によって包括的に規定されている。加盟各国はこの PL 指令を基にそれぞれ自国向けに PL 法を整備することとなっている。欧州委員会は PL 指令についても技術の進歩や製品の変化に応じた改正を検討、2024 年 12 月には改正（Product Liability Directive 以下 改正 PL 指令³）が発効され、段階的に適用が開始されており、各国は 2026 年 12 月までに本指令を国内法として移行させる必要がある。

この改正 PL 指令では、GPSR と同様、製品の定義が拡大され、これに伴う責任対象が明確化されることで、AI と PL とをより具体的に関連付けることとなった。

¹ EUR-Lex 「一般製品安全規則（GPSR）」

https://eur-lex.europa.eu/eli/reg/2023/988/oj/eng#pbl_1 (アクセス日：2025-7-22)

² 「一般製品安全規則（GPSR）」より当社にて作成

³ EUR-Lex 「改正 PL 指令」

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402853 (アクセス日：2025-7-22)

表 2 AI に関する改正 PL 指令の内容⁴

内容	条文	概要
製品の定義	第 4 条	(AI を含む) ソフトウェアや IoT 製品に紐づくソフトウェア、電気、ガスなどの無体物を製品として定義
責任の対象	第 8 条	(AI を含む) ソフトウェアなどが製品に組み込まれたり相互接続されることで、製品に欠陥を引き起こした場合、ソフトウェア製造業者も責任を負う
立証責任	第 10 条	<ul style="list-style-type: none"> ・製品の欠陥や事故との因果関係について、技術的または科学的な複雑さゆえに直接証明することが難しい場合でも、裁判所は状況に応じて、それらの存在を推定できるとされた。 ・裁判所は製品が強制的な安全要件に準拠しない（後述の AI 法を逸脱するなど）、製品の明らかな故障がある場合に、製品に欠陥があると推定することを可能とした
責任期間	第 17 条	原則上市後 10 年間であるが、製品に大幅な変更（アップグレードなど）があった場合は、変更があった日を起算日として 10 年間を責任期間とした

1.2. 欧州 AI 法

1.2.1. 欧州 AI 法の概要

欧州理事会および欧州議会は、人工知能 (AI) に関する包括的な法的枠組み（欧州 AI 法⁵）について、2024 年 2 月に加盟国の全会一致で可決し、3 月には欧州議会でも採択が決議された。2024 年 8 月には発効されており、段階的に適用が開始されていくことを想定している。この AI 法は、欧州域内の市場で使用される AI システムの安全性確保や基本的権利の保護など、共通の価値観形成を目的としたものとされている。

1.2.2. AI システムの定義

欧州 AI 法では、この規則の対象となる AI システムを以下のように定義している。

第 3 条 定義 (1)

「AI システムとは、運用中に適応性を示したり、また明示的または默示的な目的のために、受け取った入力から現実環境または仮想環境に影響を与える予測、推奨、決断などの出力を生成する方法を推測したりする、様々なレベルの自律性で動作する機械ベースのシステム」

AI 法では、AI システムの特長を「推論の能力 (capability to infer)」とし、それを実現する手法として機械学習 (machine learning)、ロジックベース(logic-based)、ナレッジベース(knowledge-based)のアプローチを挙げ、これらに基づいたシステムを「AI システム」として位置付けている⁶。

⁴ 「改正 PL 指令」より当社にて作成

⁵ EUR-Lex 「欧州 AI 法」

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> (アクセス日 : 2025-7-22)

⁶ 欧州 AI 法 前文(12)より

1.2.3. 禁止される AI 行為

AI 技術は、活用方法によっては人の行動に悪影響を与えること、自由な意思決定を阻害する可能性があり、この場合は重大な人権侵害となる恐れがあると言える。そのため AI 法では、実装が禁止される AI の特長についても以下のように定められている。

第5条 禁止されている AI 行為
<ul style="list-style-type: none"> サブリミナル技術⁷を用いて個人・集団の意思決定能力を損ない、行動を歪める可能性のあるもの 個人や特定のグループの特性や脆弱性（vulnerability）を活用し対象者やその他の人に危害を加える可能性のあるもの（年齢、障害、社会的または経済的事情による弱者の権利搾取） 社会的行動又は既知、推論若しくは予測される特性に基づき、一定期間にわたって個人や特定のグループを評価または分類するもの 直接的な事実に基づくものを除き、人の性格などの特性に基づいて犯罪行為の可能性を予測するものの インターネットや監視カメラから、対象人物を絞らずに画像を収集し、顔認識データベースを作成、拡張するもの 医療または安全上の理由を除き、職場や教育現場で人の感情を推測するもの 生体認証データに基づいて個人を分類し、人種、政治的意見、労働組合への加入、宗教的または哲学的信念、性生活、性的指向を推測または推論するもの

1.2.4. リスクベースアプローチ

AI 法では、対象となる AI システムで想定されるリスクに応じて、4つのリスクレベルを設定している。なかでも「容認不可リスク」、「高リスク」については、厳格な規制が課される。これらは禁止されないものの、適切な管理（リスク管理、データガバナンス等）や人間による監視、透明性やセキュリティの確保等、所定の要件を満たす必要がある。

表 3 リスクレベルとその概要⁸

リスクレベル	概要
許容不可リスク (Unacceptable Risk)	サブリミナル技術を用いたものや社会的弱者を搾取するもの、ソーシャルスコアリング、個人の犯罪リスク評価や予測、顔認識データベース作成・拡張のためのスクレイピング行為などは許容不可（Unacceptable）リスクとして禁止される。
高リスク (High risk)	特定の機器、製品に関するもの、また生体認証、重要インフラ、教育、雇用・労務管理、重要民間及び公共サービス、法執行、移民・国境管理、司法の運営などに関する AI システムが「ハイリスク」と分類される。

⁷ 人間の意識では自覚できないレベルでの刺激を通じて、無意識に影響を与えることを目的とした技術や手法

⁸ 欧州委員会「AI 法・リスクベースのアプローチ」より当社にて作成
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (アクセス日: 2025-7-22)

1.3. 欧州 AI 責任指令案

欧州 AI 責任指令案⁹は 2022 年に提案されたものであり、AI 法が、AI システムの要件を規定しているのに対して、AI システムに起因する法的責任を定めようとするものであった。これは GPSR や各製品個別の規則・指令がそれぞれの製品での満たすべき要件を規定し、製造物責任に基づく企業の法的責任については、PL 指令で規定（することを各国に求める）されているのと同じ構図と言える。

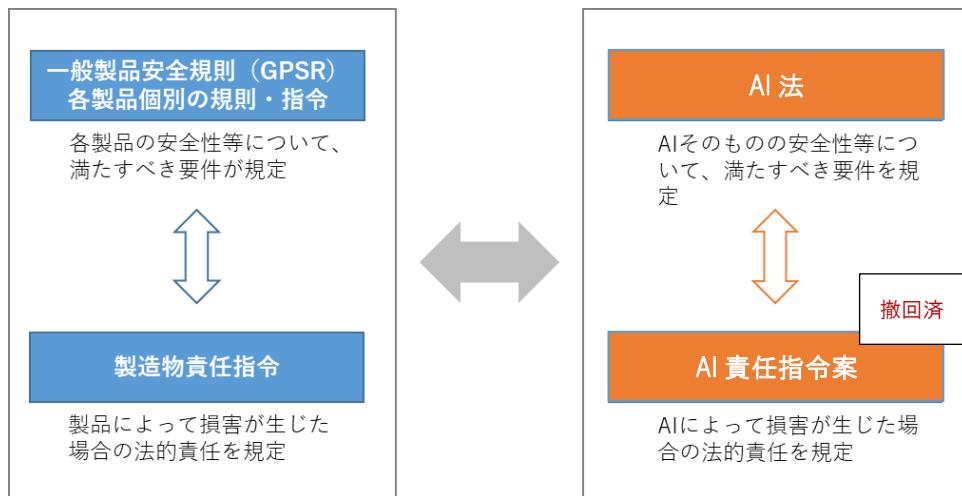


図 1 欧州 AI 法と AI 責任指令案の関係性¹⁰

なお、本指令案については、AI に関する規制緩和が進む世界的情勢を考慮し、さらなる複雑化を推し進める要因になるとして 2025 年に撤回されている。

撤回とはなったが、欧州ではどのような発想があったかの参考となると考え、この AI 責任指令案の特長を以下にまとめる。

表 4 AI 責任指令案の特長¹¹

条文	概要
第 2 条	<ul style="list-style-type: none"> 冒頭に、「一貫性を確保するため『AI 法 (AI Act)』に従う」と記載 被害を受けた当事者だけでなく、各国法に従う範囲で、複数の被害者に関して代理人を立て、損害賠償を提起することも可能とされている。 <p>→これは AI システムによる損害について、集団訴訟が提起できることを示唆している。</p>
第 3 条	<ul style="list-style-type: none"> 損害を引き起こした高リスク AI システムについては、証拠開示を命じることができる。 <p>→AI 技術には企業秘密も多く、事業者の開示拒否を見越した規程と考えられる。</p>
第 4 条	<ul style="list-style-type: none"> AI の不備によって損害を被った場合に、事業者等に賠償請求するための要件となる過失の立証について規定されている。 <p>→請求者にとって、AI システムの不備や、損害との因果関係等を立証するのは困難である。このため本案では、因果関係や過失の存在について「推定 (presumption)」できるとされている。</p>

⁹ EUR-Lex 「欧州 AI 責任指令案」

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496> (アクセス日: 2025-7-22)

¹⁰ 「欧州 AI 責任指令案」より当社にて作成

¹¹ 「欧州 AI 責任指令案」より当社にて作成

2. 英国の動向

英国においては AI に特化した製品安全・製造物責任 (PL) に関する新たな法律や条文は制定されていない。2020 年に EU を離脱したため、上述の EU の規制に関しても対象外となる。英国独自の動向としては、自動運転技術について規定した自動運転車両法 2024¹²の制定があげられる。

2.1. 自動運転車両法 2024 の概要

自動運転車両法 2024 においては、自動運転車両に関する責任主体に関して細かな規定がされ、安全基準や自動運転に関するマーケティングに関しても規定がされることになった。

本法においては、自動運転機能を持つ車両の使用者は、自動運転機能作動中に生じた交通違反行為（信号違反、一時停止などを含む）に関して責任は問われないことが定められている。一方で、運転方法以外で生じる使用者の責任（シートベルトの着用確認や駐車違反、通行料支払い、自動車保険への加入¹³など）は使用者が負うものとされ、いつでも自動運転から手動制御に切り替えることができる状態（無免許、携帯電話の使用、睡眠はあってはならない）であることが求められる。例外として、運転者を一切不要とする自動運転車両に関してはこれらの責任は求められない（当該サービス利用者も責任を負わない）。

車両の使用者に責任が問われない場合、その責を負うのは認可自動運転主体（ASDE : Authorised Self-Driving Entity）¹⁴となる。このほか、認可自動運転主体は自身が主管する自動運転機能について安全かつ合法に動作するよう措置を講じる責務を常に負うこととなる。

本法に先んじて自動運転および電気自動車両法 2018¹⁵が施行され、自動運転によって生じた交通違反や事故における保険会社の役割、立ち位置、支払保険金の求償権についても規定されている。そのため、実際に自動運転が関与する損害等が発生した際には第一に保険会社がその賠償責任を負い、自動運転機能の提供者に対して求償するといった流れが考えられる。

¹² 英国政府「自動運転車両法 2024」

<https://www.legislation.gov.uk/ukpga/2024/10/contents> (アクセス日: 2025-7-22)

¹³ 英国では自動車保険加入は任意ではなく義務となっており、違反した場合は刑事罰が科される。

英国政府「英国道路交通法 1988」 143 条より <https://www.legislation.gov.uk/ukpga/1988/52/contents> (アクセス日: 2025-7-22)

¹⁴ 自動運転車両法 2024 において、自動運転システムを公道で使用可能とするために認可された法人（または実体）

¹⁵ 英国政府「自動運転および電気自動車両法 2018」

<https://www.legislation.gov.uk/ukpga/2018/18/contents> (アクセス日: 2025-7-22)

3. 日本の動向

日本においては AI に特化した製品安全・製造物責任 (PL) に関する新たな法律や条文は制定されておらず、検討段階にある。現在は経済産業省が発行する「AI 事業者ガイドライン」¹⁶にて AI 関連事業者への、AI 開発・提供・利用にあたって必要な取組についての基本的な考え方を示し、事業者側の自主的な取り組みを推進するにとどまっている。

しかし、同ガイドラインでは、AI の性能の限界や不確実性を前提に、開発・提供者にはアルゴリズムの透明性、バグ・誤作動への対処、説明責任、利用者への注意喚起などが求められており、PL 法の「設計上の欠陥」「警告表示の欠陥」に対応しうる観点が含まれている。直接的な賠償責任を示したものではないものの、企業責任の判断の一助になり得る内容となっている。

3.1. AI 事業者ガイドラインの概要

AI 事業者ガイドラインにおいては、開発者、提供者、利用者に分けて基本的指針が、高度な AI システム開発者には追加指針が示されている。以下に各事業者の定義を示す。

表 5 AI 事業者ガイドラインにおける各事業者の定義¹⁷

各事業者	定義
AI 開発者	AI システムを（研究）開発する事業者。AI モデル・アルゴリズムの開発、データ収集、前処理、AI モデル学習及び検証、AI モデルのシステム基盤、入出力機能等を含む AI システムを構築する役割を担う者と定義。
AI 提供者	AI システムをアプリケーション、製品、既存のシステム、ビジネスプロセス等に組み込んだサービスとして利用者に提供する事業者。AI システム検証、他システムとの連携実装、AI システム・サービスの提供、運用サポート、AI サービスの運用自体を担う者と定義。
AI 利用者	事業活動において、AI システム・サービスを利用する事業者であり、AI 提供者とともに AI システムを運用する役割を担う。また、AI の活用において業務外利用者に何らかの影響が考えられる場合、当該者に対する AI による意図しない不利益の回避、便益最大化の実現に努める役割を担う者と定義されている。

本ガイドには、製品安全・製造物責任 (PL) に関する直接的な指針は示されていない。一方で、企業の賠償責任を考える際に関連しそうな内容が明記されている。以下に、各事業者における製品安全・製造物責任 (PL) に関する指針を示す。

¹⁶ 経済産業省 「AI 事業者ガイドライン（第 1.1 版）」

https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html (アクセス日: 2025-7-22)

¹⁷ 「AI 事業者ガイドライン（第 1.1 版）」はじめに より当社にて作成

表 6 各主体共通の製品安全・製造物責任 (PL) に関する指針¹⁸

指針	内容
人間の生命・身体・財産、精神及び環境への配慮	<p>AI システム・サービスの出力の正確性を含め、要求に対して十分に動作していること</p> <ul style="list-style-type: none"> ● パフォーマンスレベルを維持し、著しく誤った判断を発生させないようにすること ● AI の活用・意図しない動作によって生じうる権利侵害の可能性等に対し、定期的かつ客観的なモニタリング・対処も含めて人間による制御可能性を確保すること ● 適切なリスク分析を実施し、リスクへの対策（回避、低減、移転又は容認）を講じること ● 危害を及ぼす可能性がある場合は、措置方法を事前整理し、利用者等に情報提供すること ● 関連するステークホルダーが講すべき措置及び利用規則を明記すること ● AI システム・サービスの安全性を損なう事態が生じた場合の対処体制を整備すること
適正利用	<ul style="list-style-type: none"> ● 本来の目的を逸脱した利用により危害が発生しないよう、開発・提供・利用を行うこと ● AI システム・サービスの生成物については、その精巧さにより誤解、偏見、知的財産権の侵害等の可能性があるため、利用に際し人の判断を介在させる等の対策を講じること

表 7 AI 開発者における製品安全・製造物責任 (PL) に関する指針¹⁹

指針	内容
人間の生命・身体・財産、精神及び環境に配慮した開発	<p>ステークホルダーに危害を及ぼすことがないよう、以下の事項を検討すること</p> <ul style="list-style-type: none"> ● 予想される利用条件下だけでなく、予期しない環境での利用にも耐えうる性能の要求 ● リスク（運動するロボットの制御不能、不適切な出力等）を最小限に抑える方法の要求
適正利用に資する開発	<ul style="list-style-type: none"> ● 開発時に想定していない AI の提供・利用により危害が発生することを避けるため、安全に利用可能な AI の使い方について明確な方針・ガイダンスを設定すること ● 事前学習済の AI モデルに対する事後学習を行う場合に、学習済 AI モデルを適切に選択すること（商用利用可能か、事前学習データ、学習・実行に必要なスペック等）
検証可能性の確保	AI の予測性能及び出力の品質が、活用開始後に大きく変動する可能性を踏まえ、事後検証のための作業記録を保存しつつ、その品質の維持・向上を行うこと
最新動向への留意	AI システムに対する攻撃のリスクに対応するため、開発の各工程での留意点を確認すること
関連するステークホルダーへの情報提供	<p>自らの開発する AI システムについて、例えば以下の事項を適時かつ適切に関連するステークホルダーに（AI 提供者を通じて行う場合を含む）情報を提供すること</p> <ul style="list-style-type: none"> ● AI システムの技術的特性、安全性確保の仕組み、利用の結果生じる可能性のある予見可能なリスク及びその緩和策等の安全性に関する情報 ● 開発時に想定していない AI の提供・利用により危害が発生することを避けるための AI 開発者が意図する利用範囲 Etc...

¹⁸ 「AI 事業者ガイドライン（第 1.1 版）」第 2 部 AI により目指すべき社会及び各主体が取り組む事項 2) 安全性 より当社にて作成¹⁹ 「AI 事業者ガイドライン（第 1.1 版）」第 3 部 AI 開発者に関する事項 2) 安全性 より当社にて作成

表 8 AI 提供者における製品安全・製造物責任 (PL) に関する指針²⁰

指針	内容
人間や環境に配慮したリスク対策	AI 利用者などに危害を及ぼすことがないよう、予想される利用条件下でのパフォーマンスだけでなく、様々な状況下で AI システムがパフォーマンスレベルを維持できるようにし、リスク（連動するロボットの制御不能、不適切な出力等）を最小限に抑える方法を検討すること
適正利用に資する提供	<ul style="list-style-type: none"> ● AI システム・サービスの利用上の留意点を正しく定めること ● AI 開発者が設定した範囲で AI を活用すること ● 提供時点で AI システム・サービスの正確性・学習データの最新性等を担保すること ● 適切な目的で AI システム・サービスが利用されているかを定期検証すること Etc...
脆弱性への対応	AI システム・サービスに対する攻撃手法も数多く生まれているため、最新のリスク及びそれに対応するために提供の各工程で気を付けるべき点の動向を確認する。また、脆弱性に対応することを検討すること
関連するステークホルダーへの情報提供	<p>提供する AI システム・サービスについて、例えば以下の事項を平易かつアクセスしやすい形で、適時かつ適切に情報を提供すること</p> <ul style="list-style-type: none"> ● AI を利用しているという事実、活用している範囲、適切/不適切な使用方法等 ● 提供する AI システム・サービスの技術的特性、利用によりもたらす結果より生じる可能性のある予見可能なリスク及びその緩和策等の安全性に関する情報 ● AI システム・サービスの動作状況情報、不具合原因・対応状況、インシデント事例等

表 9 AI 利用者における製品安全・製造物責任 (PL) に関する指針²¹

指針	内容
安全を考慮した適正利用	<ul style="list-style-type: none"> ● AI 提供者が定めた利用上の留意点を遵守して、AI 提供者が設計において想定した範囲内で AI システム・サービスを利用できるようにすること ● 正確性・必要な場合には最新性等が担保されたデータの入力を行うこと ● AI の出力について精度やリスクを理解し、リスク要因を確認した上で利用すること

²⁰ 「AI 事業者ガイドライン（第 1.1 版）」第 4 部 AI 提供者に関する事項 より当社にて作成²¹ 「AI 事業者ガイドライン（第 1.1 版）」第 5 部 AI 利用者に関する事項 より当社にて作成

4. 米国の動向

米国においては、連邦政府として、AI に特化した製品安全・製造物責任 (PL) に関する新たな法律や条文は制定されていない。そもそも AI に関する法案の多くが未成立であり、現在は、行政命令、フレームワークを用いて AI の安全と責任の指標を示すにとどまっている。また、政権交代の影響もあり、規制を強化するのではなく、規制緩和によって技術発展を促すという動きがみられる。

州単位で見ても AI に特化した製品安全・製造物責任 (PL) に関する新たな法律や条文は制定されていない。一方でディープフェイク²²や AI を用いた欺瞞行為に関しては、州独自の法案が成立・施行されるなどの動きがみられる。

4.1. 連邦政府の動向

4.1.1. NIST AI リスクマネジメントフレームワーク (NIST AI Risk Management Framework) の概要

NIST AI リスクマネジメントフレームワーク²³は、2023 年に米国商務省の国立標準技術研究所 (NIST) によって発表され、AI システムの設計、開発、展開、使用において、リスクを管理し、信頼性の高い責任ある AI の発展と使用を促進することを目的としている。

本フレームワークにおいても、製品安全・製造物責任に特化した明確な指標などは示されておらず、広範なリスクに対するリスク管理のプロセスなどが規定されている。大枠は従来のリスク管理プロセスを採用しており、AI 独自が有するリスク（学習データへの依存性、従来ソフトウェアを超える複雑性、社会への影響度など）を組み合わせた構成となっている。

4.1.2. AI の安全・セキュリティ・信頼性に関する行政命令 (Executive Order 14110) の概要

AI の安全・セキュリティ・信頼性に関する行政命令 (Executive Order 14110)²⁴は 2023 年に発令されたものであり、AI の安全とセキュリティに関する基準確立、国民のプライバシー保護、公平性と市民権の推進、消費者と労働者の擁護、イノベーションと競争の促進、米国のリーダーシップの推進などを 8 つの原則を示していた。

しかし本大統領令は 2025 年の政権交代に際し、撤廃された。新たに規制緩和、イノベーション、開発促進などに重きを置いた大統領令が発令されている。

4.2. 州の動向

州単位で見ると、多くの州が州独自の AI 関連法案を検討しており、法案提出の段階まで進んでいる（多くはディープフェイクや著作権侵害など個別の AI の問題点に関して制定されている）。この中でもコロラド州は、全米初の包括的な AI 法としてコロラド州 AI 法²⁵を制定、2026 年 2 月に施行を予定している。

²² AI 技術を用いて生成された偽の画像や映像、音声、またはそれらを生成する技術

²³ 米国国立標準技術研究所 (NIST) 「NIST AI リスクマネジメントフレームワーク」
<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf> (アクセス日 : 2025-7-22)

²⁴ 連邦官報「AI の安全・セキュリティ・信頼性に関する行政命令 (Executive Order 14110)」
<https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>
(アクセス日 : 2025-7-22)

²⁵ 米国コロラド州「コロラド州 AI 法」
https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf (アクセス日 : 2025-7-22)

4.2.1. コロラド州 AI 法

コロラド州 AI 法は 2024 年に制定され、2026 年から施行予定の州法である。AI による差別や既知または予見可能なリスクから消費者を保護することを事業者に義務付ける法律となっている。

コロラド州 AI 法では AI 関連の製品安全・製造物責任に特化した明確なルールは示されていない。しかしながら本法への違反は、不公平取引慣行に該当するとされ、違反が確認された場合は法的措置をとることが可能であることが定められている。具体的には下記内容が事業者の責任として示されている。

表 10 コロラド州 AI 法における事業者の責任²⁶

責任種別	内容
リスクへの合理的注意	AI 開発者または提供者は AI システムに対して、アルゴリズムによる差別から消費者を保護するために既知または予見可能なリスクについて合理的注意を払う必要がある。AI 提供者はリスク管理ポリシーの設定と影響評価を行わなければならない。
利用者への通知義務	AI システムによる重要な意思決定（医療判断、融資判断など）が行われる場合は、消費者に対してその事実を平易な言葉で通知する必要がある。
利用者への説明責任	利用者に悪影響を及ぼす決定が下された場合、提供者はその決定に至った主な理由や、その際に使用されたデータの種類、出所などを説明しなければならない。また、利用者に対して自己の個人データを訂正する機会を提供したり、決定に対する異議申し立ての機会を提供する必要がある。

本法においては事業者側の免責事項が設定されており、AI システムが法に準拠していないことを発見・改善した場合や前述の NIST AI リスクマネジメントフレームワークのほか、公共性の高いフレームワーク、他の優先法令に準拠していた場合は、法的措置に対して抗弁が認められるとされている。²⁷

²⁶ 「コロラド州 AI 法」第 6-1-1702 条 開発者の責任、第 6-1-1703 条 使用者の責任 より当社にて作成

²⁷ 「コロラド州 AI 法」第 6-1-1705 条 その他の法的義務の遵守 より当社にて作成

5. 中国の動向

中国においては AI に特化した製品安全・製造物責任に関する法整備は未整備の状態であり、生成 AI サービス管理暫定弁法や国家標準の制定などによる広範なリスクに対する安全性確保を図っている。

5.1. 生成 AI サービス管理暫定弁法の概要

生成 AI サービス管理暫定弁法²⁸は 2023 年に発行され、中国国内の AI サービスに関する管理の暫定措置について定めている。冒頭記載の通り、本法には製品安全、製造物責任に関する具体的なルール等は定められておらず、国家安全保障やサイバーリスク、知的財産権などに関するルールが主に定められている。一方で、未成年ユーザーの使用依存防止や生成された画像、ビデオなどのコンテンツに関してはマークをつけることを定めるなど、EU を除く他国と比べてやや具体的なルールが定められている。

また、違反した場合には是正措置が求められること、是正措置が不可または拒否された場合、サービス停止、法的処罰が下されること、事業者の行為が犯罪に資する行為となった場合は刑事責任にも問われる旨も定められている。

5.2. 国家人工知能産業総合標準化体系構築ガイドライン（2024年版）の概要

中国においては AI に関する国家または業界標準に関するガイドライン（国家人工知能産業総合標準化体系構築ガイドライン（2024年版））²⁹を発表している。文書の中で、中国は 2026 年までに 50 以上の国家または業界標準を策定することを提案している。

5.3. 「AI」に対する PL 責任の想定

中国においては、PL 責任に関連する法律として、民法（1202 条～1207 条）、製品品質法、消費者権益保護法が存在しているが、現状の「製品」の定義においては、ソフトウェアや AI に対して何も言及していない。そのため、AI 関連製品に PL 責任が及ぶか否かについては、個別具体的な状況に応じた法解釈がなされることとなる。

たとえば、AI がハードウェアに組み込まれ、自動運転車やスマート家電の制御に用いられている場合、その AI は製品の一部とみなされ、ハードウェア全体として「製品」性を認められる可能性が高い。一方、クラウドベースの生成 AI や純粋なソフトウェアとして提供される AI については、現在の法制度上、「製品」としての法的位置づけが曖昧であり、PL 責任ではなく契約責任や一般不法行為責任の枠組みで処理される可能性が高い。

また、AI 固有の特徴である自律性や予測困難性は、設計や警告の欠陥の認定を難しくする要因となる。しかし中国は、消費者保護を重視する傾向が近年強く、被害者救済の観点から、製造者やサービス提供者に対して広く説明責任や注意義務を課す判断がなされる可能性がある。今後、AI の振る舞いに対する責任論が PL 領域にも波及する可能性もあり、立法や司法判断の動向が注目される。

²⁸ 生成 AI サービス管理暫定弁法

https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (アクセス日: 2025-7-22)

²⁹ 国家人工知能産業総合標準化体系構築ガイドライン（2024年版）

https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (アクセス日: 2025-7-22)

6. AI によって生じた損害に対する司法判断および和解事例³⁰

AI に対応した製品安全・製造物責任に関する法整備が検討される中、すでに市場には AI 搭載製品、サービスが普及しつつある。件数はわずかながらも AI が原因と思われる事故、損害は発生しており、それに対する訴訟が提起され、判決も下されている。また、訴訟には至らないものの、和解にて早期解決を図ったケースもある。以下に 2 事例紹介するが、いずれも米国の事例である。米国では、判例法主義（過去判例をもとに判決を下すという考え方）がとられていることもあるが、現在の法体系でも解決は可能であることがうかがえる。

6.1. 対話型 AI 自殺訴訟に関する司法判断

2023 年には米国フロリダ州では対話型 AI を使用し、精神的被害を負った少年が自殺してしまった事故を発端とした訴訟が提起されている。本訴訟では対話型 AI サービスの提供者とその関係会社が被告として提起された。

被告側は、AI によって出力されたメッセージについては合衆国憲法第一条に規定される表現の自由に該当するものであるとして、対話型 AI より出力されたメッセージに製造物責任の法理は適用されないという反論を行ったが、判事は大規模言語モデルから出力されたメッセージを表現として認めるることはし難いとの判断を示し、当該対話型 AI を「サービス」ではなく「製品」として判断した。

従来、ゲームや SNS プラットフォームといった無体物から発する情報などにから生じた危害などについては、前述の表現の自由により免責とされ、被告側も類似の判例を用いて反論を行ったが、当該対話型 AI は「表現」をいう「サービス」ではなく「製品」として解釈されることとなった。

本訴訟は現在も係争中であるため、最終的な判決は定かでは無いが、AI によって生じた危害に対する賠償責任を製造物責任として認めた事実は今後の AI 関連訴訟に大きな影響を与えると考えられる。

6.2. 自動運転タクシー交通事故に関する和解事例

2024 年には米国カリフォルニア州では自動運転タクシーが歩行者に衝突し、長距離にわたってひきずるといった事故が発生した。

詳細な情報は現時点で得られていないが、本件事故は和解により早期に解決されることとなった。この和解後リコールが実施され、最終的に事業者は事業を終了するまでに至ったため、仮に訴訟となっていた場合、事業者側は非常に不利な立ち位置であったことがうかがえる。

AI 製品という見方よりは、ソフトウェア組み込み型製品に関する事例とみるのが正しいとも考えられるが、AI ソフトウェアが下した判断に対する責任を、最終的にはサービス提供者が負ったという点で、今後の自動運転関連訴訟等に大きなインパクトを与える事例であったと考えられる。

³⁰ SOMPO リスクマネジメント「PL・リコールクラブ」米国ウェイクリーニュースより
<https://plclub.sompo-re.co.jp/PLClub/> (アクセス日: 2025-7-22)

おわりに

本レポートでは、近年加速するデジタル化や AI 技術の導入に伴い、法的枠組みも変革が求められる中、世界に先駆けて立法手続きを推し進める欧州の状況をはじめ、各国の状況を紹介した。欧州を除く各国の法整備はいまだ検討段階にあり、欧州でも AI に特化した責任指令に関しては、複雑化を推し進める要因になるとして撤回された。各国で立法手続きが進まない状況は、いまだ発展途上の AI に対し、規制を高めることが自国の AI の発展、イノベーションの障壁になってしまうことを考慮しての対応であることも一つの理由であると考えられる。また、「6. AI によって生じた損害に対する司法判断および和解事例」にあるようにすでに現在の法体系で対応可能であれば、新たに立法する必要がないとの見方もある。

一方で AI の進化は目覚ましく、AI 技術が導入されることで製品の機能が大きく変化、設計段階では想定しえないリスクが生じる可能性がある。そのため、技術革新などが起こった場合は、従来とは違ったスピード感での規制強化や法整備が進む可能性が高い。

近年では AI 自体も多様化し、様々な企業が独自の AI を開発、競争も激化している。IoT 製品のように今後、技術の発展に伴い各企業が独自に開発する AI が一般化し、それを搭載した製品の普及もさらに進むと予想される。AI 利用サービスや AI 搭載製品における設計や要件定義、デザインレビューの際にには、各国の法整備の状況を踏まえたうえで、リスク評価と対策を行っていく必要があると考える。

当社では、今回紹介した欧州規制の状況をはじめ、各種製品安全に関するレポート情報などを配信するサービス「PL・リコールクラブ」を提供している。定期的かつ体系的に外部情報を収集でき、自社製品に係るリスクも的確かつ迅速に把握するとともに、具体的な対策のヒントを得ることが可能である。このような情報を活用して、最新の情報を入手することで、適切な対策を講じていくことが重要と考える。

参考文献

- ・ EUR-Lex Web ページ
<https://eur-lex.europa.eu/homepage.html> (アクセス日 : 2025-7-22)
- ・ 日本貿易振興機構 (ジェトロ)
「EU、デジタル化や循環型経済に対応の製造物責任指令案で政治合意」
<https://www.jetro.go.jp/biznews/2023/12/b81f2a24a2559216.html> (アクセス日 : 2025/7/22)
「欧州委、デジタル化や AI に対応した製造物責任指令の改正案を発表」
<https://www.jetro.go.jp/biznews/2022/09/4fae1d6d98b70072.html> (アクセス日 : 2025-7-22)
- ・ 経済産業省「経済産業省委託事業 営業秘密に関する欧米の法制度調査」
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/outreach_r3_europeandunitedstates.pdf
(アクセス日 : 2025-7-22)
- ・ EU 日本政府代表部「EU AI 法案の最新動向」
<https://www.eu.emb-japan.go.jp/files/100551012.pdf> (アクセス日 : 2025-7-22)
- ・ SOMPO インスティチュート・プラス
「EU、約 40 年ぶりに PL 指令を全面改正—デジタル・AI 時代の製品特性に対応し、企業の製造物責任を拡大—」
https://www.sompo-ri.co.jp/topics_plus/20241230-15616/ (アクセス日 : 2025-7-22)
- ・ EUR-Lex 「一般製品安全規則 (GPSR)」
https://eur-lex.europa.eu/eli/reg/2023/988/oj/eng#pbl_1 (アクセス日 : 2025-7-22)
- ・ EUR-Lex 「改正 PL 指令」
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402853 (アクセス日 : 2025-7-22)
- ・ EUR-Lex 「欧州 AI 法」
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> (アクセス日 : 2025-7-22)
- ・ 欧州委員会「AI 法-リスクベースのアプローチ」より
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (アクセス日 : 2025-7-22)
- ・ EUR-Lex 「欧州 AI 責任指令案」
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496> (アクセス日 : 2025-7-22)
- ・ 米国国立標準技術研究所 (NIST) 「NIST AI リスクマネジメントフレームワーク」
<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf> (アクセス日 : 2025-7-22)
- ・ 連邦官報「AI の安全・セキュリティ・信頼性に関する行政命令 (Executive Order 14110)」
<https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence> (アクセス日 : 2025-7-22)
- ・ 米国コロラド州「コロラド州 AI 法」
https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf (アクセス日 : 2025-7-22)
- ・ 英国政府「自動運転車両法 2024」
<https://www.legislation.gov.uk/ukpga/2024/10/contents> (アクセス日 : 2025-7-22)
- ・ 英国政府「英国道路交通法 1988」
<https://www.legislation.gov.uk/1988/52/contents> (アクセス日 : 2025-7-22)
- ・ 英国政府「自動運転および電気自動車法 2018」
<https://www.legislation.gov.uk/ukpga/2018/18/contents> (アクセス日 : 2025-7-22)
- ・ 経済産業省「AI 事業者ガイドライン」
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html (アクセス日 : 2025-7-22)
- ・ 中国政府「生成 AI サービス管理暫定弁法」
https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (アクセス日 : 2025-7-22)
- ・ 中国政府「国家人工知能産業総合標準化体系構築ガイドライン (2024 年版)」
https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (アクセス日 : 2025-7-22)
- ・ SOMPO リスクマネジメント「PL・リコールクラブ」米国ウェーブクリーニュース
<https://plclub.sompo-rc.co.jp/PLClub/> (アクセス日 : 2025-7-22)

執筆者紹介

中西 紀 Kaname Nakanishi

REUW サポート部門 リスクエンジニアリング部
賠償・労災グループ
コンサルタント
専門は製品安全・製造物責任

安藤 悟空 Goku Ando

REUW サポート部門 リスクエンジニアリング部
賠償・労災グループ
上級コンサルタント（チームリーダー）
専門は製品安全・製造物責任

松本 英里子 Eriko Matsumoto

REUW サポート部門 リスクエンジニアリング部
賠償・労災グループ
主任コンサルタント
専門は製品安全・製造物責任

SOMPO リスクマネジメントについて

SOMPO リスクマネジメント株式会社は、損害保険ジャパン株式会社を中心とする SOMPO ホールディングスのグループ会社です。「リスクマネジメント事業」「サイバーセキュリティ事業」を展開し、全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、サイバー攻撃対策などのソリューション・サービスを提供しています。

本レポートに関するお問い合わせ先

SOMPO リスクマネジメント株式会社
営業企画部 広報担当
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL : 03-3349-3500