EUのAI規制(AI法)

説明パンフレット

2025年5月12日

Araki International
IP&Law 荒木法律事務所

目次

1. AI法の概要

「AI法」とは

規則(EU)2024/1689(以下「AI法」という)は、人工知能(AI)に関する包括的な法的枠組みを世界で初めて定めた法律である。

「AI法」の目的とは

AI法の目的は以下のとおりである。

- EU域内市場の機能を向上する
- 人間中心で信頼できるAIの導入を促進する
- EUにおけるAIシステムの有害な影響に対して、健康、安全、民主主義、法の支配、環境保護など、憲章に謳われている基本的権利の高水準の保護を確保する
- イノベーションを支援する

2. AI法の適用範囲

規制対象となるAI

AI法はAIシステムに適用される。
AIシステムとは、「多様なレベルの自律性で動作するように設計され、デプロイ後に適応性を示す可能性があり、明示的または黙示的な目的のために、物理的または仮想的な環境に影響を及ぼし得る予測、コンテンツ、提案、または決定などのアウトプットを生成する方法を、受信したインプットから推測する機械ベースのシステム」と定義される。

AI法は、汎用目的AIモデルにも適用される。
汎用目的AIモデルとは、「大規模な自己教師を使用して大量のデータで学習されたAIモデルを含み、顕著な汎用性を示し、そのモデルが市場に投入される方法に関係なく広範囲の明確なタスクを適切に実行でき、様々な下流のシステムやアプリケーションに統合できるAIモデルであって、そのモデルが市場に投入される前に研究、開発またはプロトタイピング活動に使用されるAIモデルを除くもの」と定義される。

規制対象事業者

AI法は、AIのバリューチェーンにおける様々な事業者に対して適用される。
(a)EU域内においてAIシステムを市場に投入し、またはサービスを提供するプロバイダー、ならびに汎用目的AIモデルを市場に投入するプロバイダー(これらのプロバイダーがEU域内に設立されているか、EU域内に所在しているか、または第三国に所在しているかを問わない)
(b)EU域内に設立地または所在地があるAIシステムのデプロイヤー
(c)第三国に設立地または所在地があるAIシステムのプロバイダーまたはデプロイヤーであって、AIシステムにより生成されたアウトプットがEU域内で使用されるもの
(d)AIシステムの輸入業者および販売業者
(e)自社製品と共にまたは自らの名称または商標のもとでAIシステムを市場に投入し、またはサービス提供する製品メーカー
(f)EU域内に設立されていないプロバイダーの認定代理人

適用除外
AI法は、以下の場合等(これに限定されない)には適用されない。

- 軍事、防衛、国家安全保障の目的のみで市場に投入され、サービスを提供され、または変更の有無にかかわらず使用されるAIシステム。
- 適切なセーフガードが提供されている第三国の公的機関または国際機関によるAIシステムの利用。
- 科学的研究開発のみを目的として開発され、サービス提供されるAIシステムまたはAIモデル(そのアウトプットを含む)。
- AIシステムまたはAIモデルが市場に投入、またはサービス提供される前の研究、試験、開発活動(実環境でのテストはこの適用除外の対象とはならない)。
- 純粋に私的な非職業的活動の過程でAIシステムを使用する自然人。
- フリー・オープンソースライセンスのもとでリリースされたAIシステム(禁止AI、ハイリスクAIまたは限定リスクAIに該当するAIシステムとして市場に投入またはサービス提供された場合を除く)。

域外適用

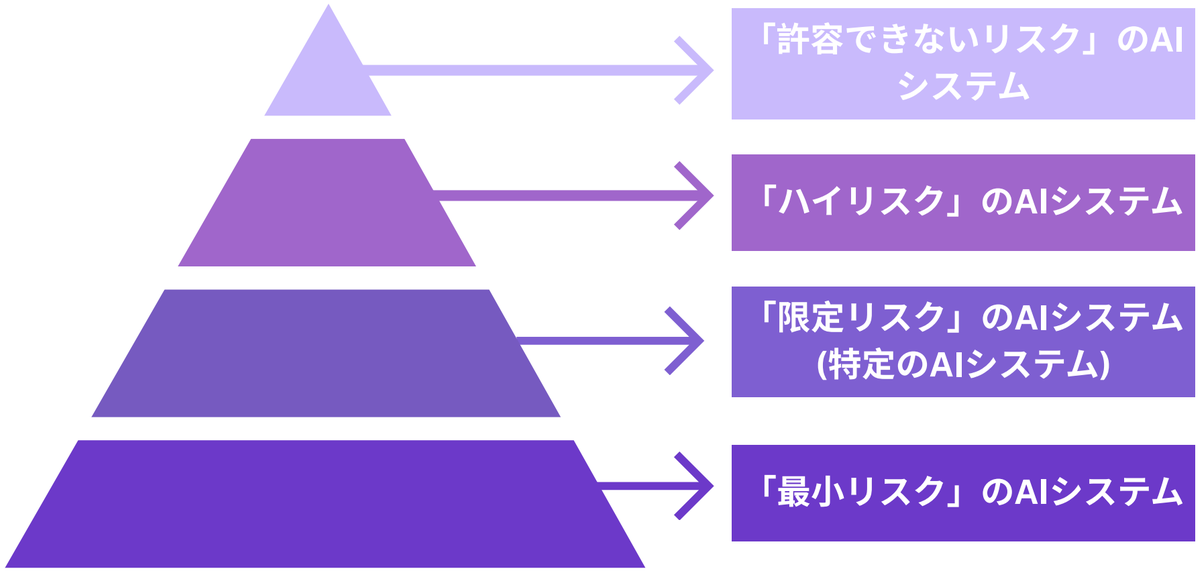
AI法は以下の場合に域外適用される。

- AI法は、設立地または所在地に関係なく、EU域内においてAIシステムを市場に投入、またはサービスを提供するプロバイダー、汎用目的AIモデルを市場に投入するプロバイダーに適用される。
- AI法はまた、AIシステムによって生成されたアウトプットがEU域内で使用され、第三国に設立または所在するAIシステムのプロバイダーおよびデプロイヤーにも適用される。

AI法を域外適用するための重要な仕組みは、「認定代理人」という概念である。EU域内の認定代理人は、EU域外に設立されたハイリスクAIシステムまたは汎用目的AIモデルのプロバイダーが、当該AIシステムまたは汎用目的AIモデルをEU域内市場で販売する前に、書面による委任状により任命され、当該委任状に規定された業務を遂行しなければならない。

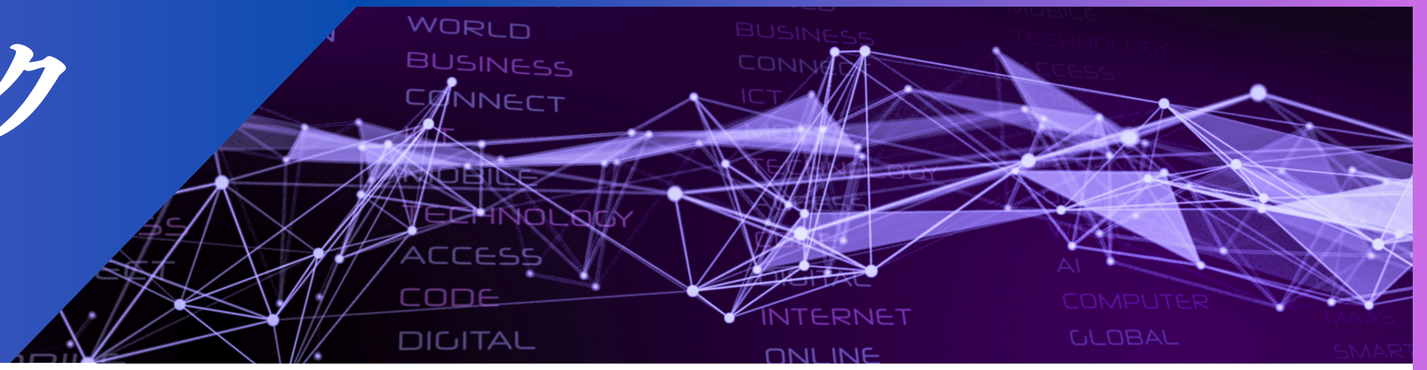
3. リスクベースアプローチ

AIシステムに対して比例的かつ効果的な拘束力あるルールを導入するため、AI法はリスクの度合いに応じてAIシステムを規制する、リスクベースのアプローチを導入している。このアプローチでは、AIシステムが生み出しうるリスクの強度と範囲に合わせて、ルールの種類と内容を調整する必要がある。



✱ 注：AIシステムの中には、ハイリスク・カテゴリーと限定リスク・カテゴリーの両方に該当するものがあり、対象企業は関連するすべての要件を満たさなければならない。そのため、「限定リスク」に代えて「特定のAIシステム」と呼ばれることもある。

許容できないリスクのAIシステム



禁止されているAIシステムとは

AI法は、EU域内で禁止されているAIの市場投入、サービス提供、使用を禁止している。このカテゴリーには、いくつかの例外を除き、以下のようなEUの価値観や基本的権利に許容できないリスクをもたらすAIシステムが含まれる。

(a)人の意識を超えたサブリミナル技術や、意図的に操作的または欺瞞的なテクニックを駆使して、人の行動を歪める目的または効果を持ち、その結果重大な危害を与え、または与える可能性が合理的に高いAIシステム
(b)年齢、障害、特定の社会的・経済的状況に起因する脆弱性を悪用して、人の行動を歪める目的または効果を持ち、その結果重大な危害を与え、また与える可能性が合理的に高いAIシステム
(c)自然人または人々の集団を、その社会的行動または個人的もしくは性格的特徴に基づいて評価または分類し、無関係な社会的状況における不利益もしくは不利な扱い、または不当もしくは不均衡な扱いにつながるAIシステム
(d)プロファイリングや人格的特徴・特性の評価を通じて、人が犯罪を犯す危険性を評価または予測するAIシステム（犯罪行為に直接関連する客観的かつ検証可能な事実に基づき人が犯罪行為に関与しているかどうかを評価する人間の判断をサポートする場合を除く）
(e)CCTVの映像から顔画像を無差別に収集し、顔認識データベースを作成または拡張するために作られたAIシステム
(f)職場や教育機関において、人の感情を推測するAIシステム（医療や安全上の理由を除く）
(g)生体認証に基づいて人を分類したり、人種、政治的意見、労働組合員、宗教的・哲学的信条、性生活、性的指向を推測したりするAIシステム（法執行の分野、合法的に取得された生体認証データセットのラベリング、フィルタリングを除く）
(h)法執行を目的とした、公共のアクセス可能な空間におけるリアルタイムの遠隔生体認証のためのAIシステム（特定の被害者の捜索、テロ攻撃を含む特定の脅威の防止、または特定の犯罪の被疑者の捜索のために必要な場合を除く）

施行スケジュール

AI法は、**2025年2月2日**以降、EU域内で、許容できないリスクのAIシステムの市場投入、サービス提供、または使用を禁止する。

ハイリスクAIシステム

ハイリスクAIシステムとは

AI法は、以下のAIシステムをハイリスクに分類している。

(a) 製品の安全コンポーネントとして使用されることが意図されたAIシステム、またはAIシステム自体が付属書Ⅰに記載されたEU整合法令の対象となる製品であり、当該EU整合法令に従って第三者適合性評価を受ける必要があるもの

(b) AI法の付属書IIIに規定されている以下の8つの特定分野にデプロイされたAIシステム

- 生体認証、
- 重要なインフラ
- 教育および職業訓練
- 雇用・労働者管理・自営業へのアクセス
- 必要不可欠な民間および公的サービスや便益へのアクセスと享受
- 法の執行
- 移民・亡命・国境管理
- 司法行政と民主主義のプロセス

付属書Iに記載されている法律とは

付属書Iのセクション A

- 機械に関する指令
- 玩具の安全性に関する指令
- レクリエーショナル・クラフトとパーソナル・ウォータークラフトに関する指令
- リフトおよびリフト用安全部品に関する指令
- 爆発の危険性のある環境での使用を目的とした機器および保護システムに関する指令
- 無線機器に関する指令
- 圧力機器に関する指令
- 索道敷設に関する規制
- 個人用保護具に関する規制
- ガス燃料を燃焼する機器に関する規制
- 医療機器に関する規制
- 体外診断用医療機器に関する規制

付属書Iのセクション B

- 民間航空保安分野における共通ルールに関する規則
- 二輪車・三輪車・四輪車の認可と市場監視に関する規則
- 農林業用車両の認可および市場監視に関する規則
- 舶用機器に関する指令
- EU域内の鉄道システムの相互運用性に関する指令
- 自動車とそのトレーラーおよび当該自動車向けのシステム・部品・個別の技術ユニットの承認と市場監視に関する規則
- 自動車およびそのトレーラー並びに当該自動車を対象とするシステム・部品および個別技術ユニットの型式承認要件に関する規則
- 民間航空分野における共通規則および欧州連合航空安全機関の設立に関する規則

一方、これらの分野で使用されるAIシステムであっても、健康、安全、基本的権利に重大な危害を及ぼす危険性がなく、以下の条件のいずれかを満たす場合には、ハイリスクとはみなされない。

- 限定的な手続き上のタスクを実行するためのもの
- 既に完了した人間の活動の結果を改善することを目的としているもの
- 意思決定のパターンや、以前の意思決定のパターンからの逸脱を検出することを意図したものであり、人間による適切なレビューなしに、既に完了した人間による評価に取って代わるものでも、影響を与えるものでもないもの
- 付属書IIIに記載されているユースケースの目的に関連する評価の準備作業を行うことを意図しているもの

もっとも、付属書IIIに列挙された分野のいずれかに使用されるAIシステムが、自然人のプロファイリングを行う場合には、常にハイリスクとみなされる。付属書IIIで言及されるAIシステムがハイリスクではないと考えるプロバイダーは、当該システムを市場に投入またはサービス提供する前に、その評価を文書化しなければならない。当該プロバイダーは、AI法に基づく登録義務の対象となり、国内所轄当局の要求に応じて、評価文書を提供しなければならない。

ハイリスクAIシステムの要件

ハイリスクAIシステムが満たすべき要件（以下「ハイリスクAIシステムの要件」という。）は以下のとおりである。

- リスク管理システム
- データガバナンス
- 技術文書
- 記録管理
- 透明性とデプロイヤーへの情報提供
- 人的な監視
- 正確性、堅牢性、サイバーセキュリティ

ハイリスク AIシステム

各対象事業者の義務

(a)プロバイダー

ハイリスクAIシステムのプロバイダーは、以下の各点を含む厳しい義務を履行しなければならない。

- ハイリスクAIシステムの広範な要件が満たされていることを確認する
- 品質管理システムを確立する
- すべての関連技術文書を管理する
- ハイリスクAIシステムによって自動生成されたログを保管する
- AIシステムの継続的な適合性を確保するための是正措置を採用する
- プロバイダーがEU域外に設立されている場合は、AIシステムをEU市場で利用可能にする前に、EU域内に設立された認定代理人を、書面による委任によって任命する
- ハイリスクのAIシステムが、市場に投入またはサービス提供前に、適合性評価手続を受けることを保証する
- アクセシビリティ要件に準拠していることを確認する
- 管轄当局の合理的な要請に対して協力し、ハイリスクAIシステムが要求事項に適合していることを証明する
- 登録義務を遵守する
- プロバイダーの名称、登録商標または商標、連絡先を明記する
- ハイリスクAIシステムのパッケージまたは付属文書にCEマーキングを貼付する
- EU適合宣言書を作成する

(b)デプロイヤー

ハイリスクAIシステムのデプロイヤーは、以下の各点を含む義務を履行しなければならない。

- システムを使用説明書に従って確実に使用するために、適切な技術的・組織的対策を実施する
- 必要な権限、トレーニング、能力および必要なサポートを備えた人間に人的監督を任せる
- 使用説明書に基づくハイリスクAIシステムの運用を確保・監視し、関連データの収集、文書化、分析について事業者に通知する
- 使用説明書に従ったハイリスクAIシステムの使用が、健康、安全、または人々の基本的権利に対するリスクをもたらす可能性がある場合、プロバイダーまたは販売業者および関連する市場監視当局に通知し、そのシステムの使用を一時停止する
- 重大な事故が発生した場合は、プロバイダー、輸入業者または販売業者、および関連する市場監視当局に報告する
- ハイリスクAIシステムによって自動的に生成される操作ログを少なくとも6ヶ月間保持する
- ハイリスクAIシステムから得られた結果によって影響を受ける可能性のある個人（従業員など）に、当該AIシステムの使用の対象になることについて知らせる
- デプロイヤーが公的機関、連邦機関、団体、事務所、機関である場合は、関連する登録要件に従う
- GDPRの義務を遵守し、プロバイダーが提供する指示書を使用してデータ保護影響評価を実施する
- 自然人に関する意思決定を行う、または意思決定を支援する、付属書IIIで言及されているハイリスクAIシステムのいずれかのAIシステムによって影響を受ける可能性のある個人に、当該システムの使用の対象になることについて知らせる
- 関係当局に協力する

(c)輸入業者

ハイリスクAIシステムの輸入業者は、以下の各点を含む義務を履行しなければならない。

- AIシステムを市場に投入する前に、プロバイダーに課された義務の遵守を検証する
- リスクがある場合、関連するAI事業者に通知する
- AIシステムおよびその包装または添付文書に、輸入者名、登録商号または商標および住所を表示する
- AIシステムが輸入業者の責任下にある間、AIシステムがAI法に準拠していることを確認する
- 関連書類をAIシステムを市場に投入またはサービス提供してから10年間保管する
- 所轄官庁の要請に応じて情報や書類を提供する
- 関係当局に協力する

(d)販売業者

ハイリスクAIシステムの販売業者は、以下の各点を含む義務を履行しなければならない。

- AIシステムを市場で入手可能にする前に、プロバイダーと輸入業者に課された義務の遵守を確認する
- AIシステムが販売業者の責任下にある間、AIシステムがAI法に準拠していることを確認する
- 関連するAI事業者に報告し、不適合やリスクがある場合は是正措置を実施するか、またはプロバイダー、輸入業者もしくは関連する事業者が是正措置を実施することを確保する
- 所轄官庁の要請に応じて情報や文書を提供する
- 関係当局に協力する

(e)認定代理人

ハイリスクAIシステムの認定代理人は、以下の各点を含む義務を履行しなければならない。

- 要請があれば、市場監視当局に委任状の写しを提出する
- プロバイダーが受領した委任事項で指定されたタスクを実行する（当該委任事項は、認定代理人が以下のタスクを実行できるようにするものでなければならない）

1. EU適合宣言書に関するプロバイダーに課された義務(p.12参照)および技術文書に関するプロバイダーの義務(p.9参照)の遵守を検証する
2. ハイリスクAIシステムが市場に投入またはサービス提供されてから10年間、関連文書を保管する
3. ハイリスクAIシステムがハイリスクAIシステムの要件に適合していることを証明するために必要なすべての情報および文書を、管轄当局の合理的要請に基づき提供する（当該ログがプロバイダーの管理下にある限り、ハイリスクAIシステムにより自動的に生成されるログへのアクセスを含む）
4. ハイリスクAIシステムに関連してとられる措置、特にハイリスクAIシステムによってもたらされるリスクを低減・軽減するためにとられる措置について、管轄当局の合理的要請に対して協力する
5. 登録義務を遵守する、または、登録がプロバイダー自身によって行われる場合は、提供される情報が正確であることを確認する

- プロバイダーがAI法に基づく義務に違反する行為をしていると判断、または判断する理由がある場合、委任を終了する。委任の終了およびその理由は、関連市場監視当局および関連する通知機関（該当する場合）に通知されるものとする。

(f)AIバリューチェーンにおける責任

以下の場合、販売業者、輸入業者、デプロイヤー、またはその他の第三者は、ハイリスクAIシステムのプロバイダーとみなされる。

- すでに市場に投入されている、またはすでにサービス提供されているハイリスクAIシステムに、自社の名称や商標を付した場合
- すでに市場に投入されている、またはすでにサービス提供されているハイリスクAIシステムに大幅な変更を加える場合
- すでに市場に投入されている、またはすでにサービス提供されているAIシステムの目的を変更し、ハイリスクAIシステムとした場合

上記のいずれかが発生した場合、最初にAIシステムを市場に投入しまたはそのサービスを提供したプロバイダーは、もはやAIシステムのプロバイダーとはみなされない。最初のプロバイダーは、新しいプロバイダーがAI法に基づく義務（特にハイリスクAIシステムの適合性評価）を遵守できるように、必要な情報を提供し、必要な技術的アクセスおよび支援を提供しなければならない。ただし、最初のプロバイダーが、そのAIシステムをハイリスクAIシステムに変更しないことと明確に指定している場合は、この限りではない。もっとも、知的財産権、業務上の機密情報、企業秘密を遵守し保護する必要性を損なうものではない。

ハイリスクAIシステムのプロバイダーおよびハイリスクAIシステムにおいて使用または統合されるAIシステム、ツール、サービス、コンポーネントまたはプロセスを提供する第三者は、以下の各点を履行しなければならない。

- 書面による合意により、ハイリスクAIシステムのプロバイダーがAI法に定める義務を完全に遵守するために必要な情報、能力、技術的アクセスおよびその他の支援を特定する。ただし、第三者が、汎用目的AIモデル以外のツール、サービス、プロセスまたはコンポーネントを、フリー・オープンソースライセンスの下で一般に公開する場合は、この限りではない。
- AIオフィスは、ハイリスクAIシステムのプロバイダーと、ハイリスクAIシステムに使用される、または組み込まれるツール、サービス、コンポーネント、またはプロセスを供給する第三者との間の契約について、自主的なモデル条項を策定し、推奨することができる。

ハイリスクAIシステム

整合規格と共通仕様

整合規格と共通仕様は、AI法を遵守するにあたり、重要な役割を果たす。

- 整合規格（harmonized standard）または共通仕様（common specification）に準拠するハイリスクAIシステムは、整合規格と共通仕様がハイリスクAIシステムの要件や義務をカバーしている限りにおいて、ハイリスクAIシステムの要件（p.8を参照）に適合していると推定される。
- 2023年5月22日、欧州委員会は、欧州標準化委員会（CEN）と欧州電気標準化委員会（CENELEC）に対して要請を行った。この要請に基づいて、CENとCENELECは整合規格の開発を進めている。

しかし、AI法の要件を満たす整合規格がない場合、欧州委員会は、代わりに、ハイリスクAIシステムの要件に関する共通仕様を定める実施法令を採択することができる。

適合性評価と整合規格

適合性評価とその実施方法

適合性評価とは、ハイリスクAIシステムの要件が満たされているかどうかを実証するプロセスである。
プロバイダーは、ハイリスクAIシステムを市場に投入したり、サービス提供したりする前に、適合性評価手続を受けなければならない。ただし、特定の免除措置が適用される場合はこの限りではない。
適合性評価には、(a)プロバイダーが行う自主評価である内部統制に基づく評価と、(b)届出機関が関与する第三者評価の2種類がある。前者の内部統制に基づく評価とは、第三者である届出機関が関与することなく、確立された品質マネジメントシステムが規制に適合していることを検証し、技術文書に含まれる情報を調査して、AIシステムがハイリスクAIシステムの要件に適合していることを評価し、AIシステムの設計及び開発プロセス並びに市販後のモニタリングの評価を実施して、技術文書との整合性を確保する手続である。

- 付属書IIIポイント1に記載されているハイリスクAIシステム
  - 原則として、AIシステムのプロバイダーは、整合規格または共通仕様を適用する場合、(a)内部統制または(b)第三者評価のいずれかに基づいて適合性評価を実施することができる。
  - ただし、整合規格が存在しないか、制限付きで発行されているか、またはプロバイダーが整合規格を適用していない場合、あるいは共通仕様が利用できないか、またはプロバイダーが共通仕様を適用していない場合には、プロバイダーは第三者評価に基づいて適合性評価を実施しなければならない。
- 付属書IIIポイント2から8に記載されているハイリスクAIシステム
  - AIシステムのプロバイダーは、内部統制に基づく適合性評価手続に従わなければならない。
- 付属書Ⅰセクション Aに記載されているEU整合法令の対象となるハイリスクAIシステム
  - プロバイダーは、これらの法令に基づき要求される関連する適合性評価手続に従わなければならない。

さらに、既に適合性評価手続の対象となっているハイリスクAIシステムは、システムに大幅な変更があった場合、新たに適合性評価手続を受けなければならない。ただし、市場に投入された後、またはサービス提供が開始された後も引き続き学習するハイリスクAIシステムの場合、最初の適合性評価の時点でプロバイダーが事前に決定したものについての変更、およびハイリスクAIシステムの要件に継続的に準拠することを確保するために採用された技術的ソリューションに関連する情報の一部についての変更は、大幅な変更に該当しない。

ハイリスクAIシステム

適用スケジュール

ハイリスクAIシステムに関する適用スケジュールは以下の通りである。

(a) 2026年2月：ハイリスクのAIシステムに関する実践的なガイドラインが提供される。

(b) 2026年8月：AIシステムに対するAI法の適用開始。ただし、製品の安全コンポーネントとして使用されるAIシステムおよび付属書Iに記載されたEU整合法令に従って第三者適合性評価を受ける必要があるハイリスクAIシステムは除く。

(c) 2027年8月：すべてのリスクカテゴリーに対するAI法の適用開始。

適合性評価と整合規格

適合性評価終了後、プロバイダーは何をすべきか？

1.証明書またはEU適合宣言書

ハイリスクAIシステムの要件に適合していると評価され、適合性評価手続きが終了した場合、ハイリスクAIシステムのプロバイダーは、EU適合宣言書を発行しなければならない。プロバイダーは、EU適合宣言書を適宜最新の状態に保つ必要がある。

2.CEマーキング

CEマークに関しては、規則(EC) No 765/2008第30条に規定される一般原則が適用される。ハイリスクAIシステムはAI法への適合を示すCEマークを貼付する必要がある。

3.登録

さらに、EUのデータベースへの登録が必要となる場合がある。

-付属書IIIに記載されたハイリスクAIシステム（付属書IIIポイント2に記載されたハイリスクAIシステムを除く）を市場に投入またはサービス提供する前に、プロバイダーまたは認定代理人は、EUのデータベースに、自身およびそのAIシステムを登録しなければならない。

限定リスクAIシステム

限定リスクAIシステムとは

AIシステムは、ユーザーと直接やり取りし（チャットボットなど）、「ディープフェイク」を構成する映像や音声のコンテンツの生成や操作に関わることがある。
このような利用は、限定的なリスクをもたらすことがあるため、透明性と開示義務の対象となる。

適用スケジュール

透明性義務は2026年8月2日から適用される。

義務

限定リスクAIシステムに適用される透明性義務は、以下のとおりである。

(a)プロバイダーの義務

- 自然人と直接やり取りすることを意図したAIシステムは、個人がAIシステムとやり取りしていることについて知らされるような方法で設計・開発されていることを保証する。
- 合成音声、画像、映像、テキストコンテンツを生成するAIシステムは、システムのアウトプットが、機械で読み取れる形式で表示され、人工的に生成または操作されたものとして検出できるようにする。このような技術的解決策は、効果的で相互運用性があり、確実で信頼できるものでなければならない。

(b)デプロイヤーの義務

- ディープフェイクを構成する画像、音声または映像コンテンツを作成または編集する際に、システムのアウトプットが人為的に生成または操作されたものであることを開示する。
- 公共の利益に関する事項を公衆に知らせる目的で公表されたテキストを作成または修正する場合、システムのアウトプットが人為的に生成または操作されたものであることを公表する。
- ハイリスクAIシステムとみなされる可能性のある、感情認識システムまたは生体認証分類システムにさらされる個人に対し通知する。個人データはGDPR、EUDPRおよび捜査機関データ保護指令の規定に基づいて処理する。

最小リスクのAIシステム

最小リスクAIシステムとは

最小リスクに分類されるAIシステムは、先に述べた3つのカテゴリーに属さないものである。

義務

最小リスクのAIシステムは、制限や義務付けなしに導入することができるが、AI法は、ハイリスクAIシステムの要件である透明性、人間による監視、正確性などの要件のすべてまたは一部について自主的な遵守を求めている。

汎用目的AIモデル

汎用目的AIモデルとは

AI法は、汎用目的AIモデルについても規制対象としている。汎用目的AIモデルとは、「大規模な自己監視を使用して大量のデータで学習されたAIモデルを含み、顕著な汎用性を示し、そのモデルが市場に投入される方法に関係なく広範囲の明確なタスクを適切に実行でき、様々な下流のシステムやアプリケーションに統合できるAIモデルであって、そのモデルが市場に投入される前に研究、開発またはプロトタイピング活動に使用されるAIモデルを除くもの」と定義されている。

さらに、汎用目的AIモデルが以下の条件のいずれかを満たす場合、システミック・リスクをもたらすものとして分類される。
(a) 指標やベンチマークを含む適切な技術ツールや方法論に基づき評価された、高い影響力を有するもの。特に、そのトレーニングに使用される計算量の累計が10の25乗FLOPs（フロップス（浮動小数点演算速度））を超える場合には、高い影響力を有すると推定される。
(b) 委員会の職権による決定、または科学パネルからの適格な警告に基づき、AI法付属書XIIIに記載された基準に照らし、(a)と同等の能力または影響力を持っているもの。

義務

汎用目的モデルの使用は、「システミック・リスクをもたらす汎用目的AIモデルのプロバイダーに、加重された義務を課す」という段階的アプローチで規制される。

汎用目的AIモデルの全てのプロバイダーは、以下の義務を果たさなければならない。

- 汎用目的AIモデルの技術文書を作成し、定期的に更新する。
- 汎用目的AIモデルをシステムに統合することを計画しているAIシステムのプロバイダーが、汎用目的AIモデルの能力と限界を理解し、AI法に基づく義務を遵守することができるように、情報と文書を準備し、最新の状態に保ち、利用可能にする。
- EU著作権法および関連する権利を遵守するための方針を確立し、著作権物の権利保有者による留保を遵守する。
- 汎用目的AIモデルに使用されたトレーニングデータの十分詳細な要約を作成し、一般に公開する。

フリー・オープンソースライセンスの下で一般にアクセス可能であり、パラメータが一般に公開されている汎用目的AIモデルのプロバイダーには、システミック・リスクをもたらすものでない限り、後半2つの義務のみが適用される。
上記の義務に加え、システミック・リスクを有する汎用目的AIモデルのプロバイダーは、以下の義務を果たさなければならない

- 標準化されたモデルの評価を行う。
- 起こりうるシステミック・リスクを評価し、軽減する。
- 文書を記録し、重大インシデントと取り得る是正措置をAIオフィスに報告する。
- 適切なレベルのサイバーセキュリティ保護とモデルの物理的インフラを確保する。

行動規範

システミック・リスクの有無に関係なく、汎用目的AIモデルのプロバイダーは、整合規格または共通仕様が公表されるまで、AI法準拠を証明するために行動規範(code of practice)に依拠することができる。AIオフィスは、汎用目的AIモデルのプロバイダーおよび関連する各国管轄当局所轄官庁に対し、EUレベルでの行動規範の作成に参加するよう要請することができる。

適用スケジュール

汎用目的AIモデルに関する規定は2025年8月2日から適用される。

4. イノベーション支援策

AI規制サンドボックス

「AI規制サンドボックス」とは、管轄当局が設定する管理された枠組みであって、AIシステムのプロバイダーまたは潜在的プロバイダーが、規制当局の監督の下、サンドボックス計画に従って、一定期間、革新的なAIシステムを開発、トレーニング、検証、テストする機会を、適切な場合には実世界の条件下で提供するものをいう。
2026年8月2日までに、各加盟国で少なくとも1つのAI規制のサンドボックスを稼働させる。

サンドボックス外の実環境でのハイリスクAIシステムのテスト

実環境におけるテストとは、信頼性が高く確実なデータを収集し、AIシステムが本規則の要件に適合していることを評価し検証することを目的として、実験室またはその他の模擬環境以外の実環境において、AIシステムをその意図する目的のために一時的に試験することを意味し、AI法の意味における、AIシステムを市場に投入またはサービスを提供することを意味するものではない。
AI規制サンドボックス外の実環境におけるハイリスクAIシステムのテストは、禁止AIの規制を損なうことなく、規制および実環境テスト計画に従って、付属書IIIに記載されているハイリスクAIシステムのプロバイダーまたはプロバイダー候補が実施することができる。

プロバイダーとデプロイヤー、特にスタートアップ企業を含む中小企業に対する措置

- 中小企業はAI規制サンドボックスへの優先的アクセスが可能となる。
- 加盟国は、中小企業向けの専用チャネルを利用または設置し、AI法の適用に関する特定の意識向上および研修活動を組織し、全体として標準化開発プロセスへの中小企業の参加を促進する。
- 適合性評価の料金を設定する際には、スタートアップ企業を含む中小企業プロバイダーの特定の利益とニーズを考慮しなければならない。

5. 新しいガバナンス体制

連合レベル

- **AIオフィス**

AIシステムや汎用目的AIモデルの実施、監視、監督する、AIガバナンスに貢献する欧州委員会の機能である。

- **欧州AI委員会**

AI法の一貫した効果的な適用を促進するため、欧州委員会および加盟国に助言および支援を行うものである。

- **アドバイザリー・フォーラム**

欧州委員会と欧州AI委員会の双方に助言を与える技術的専門知識を提供し、AI法に基づく両者の業務に貢献するために設立される。

- **独立専門家科学パネル**

各加盟国のAI法に基づく執行活動を支援する。

加盟国レベル

各加盟国は、少なくとも1つの通知当局および1つの市場監視当局を設置または指定するものとし、これらの当局は、その活動および業務の客観性を保護し、AI法の適用および実施を確保するために、独立、公平かつ偏見なくその権限を行使する。所轄官庁および単一の連絡窓口への連絡方法に関する情報は、2025年8月2日までに公開されなければならない。

6. 罰則

AI法に違反した場合、罰金が適用される。その金額は、違反した義務の種類によって異なる。

＊ 最高額罰金の例外として、中小企業の場合は下記各項目の金額のうち低い方の金額が適用される。

ケース	罰則
禁止されるAIシステムに関する規則の不遵守	最高3,500万ユーロまたは全世界の年間総売上高の7％のいずれか高い方の制裁金
• プロバイダーおよびデプロイヤーに対する透明性義務違反 • ハイリスクAIシステムのプロバイダー、デプロイヤー、輸入業者、販売業者、認定代理人に課される義務違反 • 届出機関に課される要件と義務違反	最高1,500万ユーロまたは全世界の年間総売上高の3％のいずれか高い方の制裁金
不正確、不完全または誤解を招くような情報を届出機関または管轄当局所轄官庁の要請に対して提供	最高750万ユーロまたは全世界の年間総売上高の1％のいずれか高い方の制裁金

＊ 生成AIモデルのプロバイダーが、故意または過失によりAI法の関連規定に違反した場合、欧州委員会は、最高1,500万ユーロまたは全世界の年間総売上高の3％のいずれか高い方の制裁金を課すことができる。

7. AI法の適用スケジュール

1

2024年8月1日

AI法が発効

2

2025年2月2日

一般規定と禁止AIに関する規定適用

3

2025年5月2日

汎用目的AIモデルのための行動規範の準備期限

5

2025年8月2日

- 届出機関および届出団体、ガバナンス、汎用目的AIモデル、罰則、秘密保持に関する規定適用
- 行動規範がまとまらない場合、またはAI事務局が適切でないと判断した場合、欧州委員会は共通規則を定めることが可能

6

2026年2月2日

欧州委員会は、ハイリスクAIシステムに関する要件の実際的な実施に関するガイドラインを提供

2026年8月2日

- 製品の安全コンポーネントとして使用されるAIシステムおよび付属書Iに記載されたハイリスクAIシステムに関する対応義務を除くAIシステムに対するAI法の適用
- 上記はこの日以前に市場に投入/サービス提供されたハイリスクAIシステム（付属書Xに列挙されている法令により設置された大規模ITシステムの構成要素であるAIシステムであって、2027年8月2日より前に市場に投入されたものを除く）の事業者に適用。ただし、この日以降に設計が大幅に変更されるシステムにのみ適用。

7

2027年8月2日

- 全リスクカテゴリーに対する規定適用
- 2025年8月2日以前に市場に投入された汎用目的AIモデルのプロバイダーは、この日までにAI法に定められた義務を遵守するために必要な措置を講じる必要あり

8

2030年12月31日

付属書Xに列挙されている法令により設置された大規模ITシステムの構成要素であるAIシステムであって、2027年8月2日より前に市場に投入/サービスを提供したものは、この日までにAI法に定められた義務を遵守するために必要な措置を講じる必要あり

Araki International IP&Law 荒木法律事務所

バレン明子
パラリーガル

荒木 昭子
代表弁護士
弁護士(日本)
米国弁護士(カリフォルニア州)

杉村 領
外部顧問

www.arakiplaw.com　info@arakiplaw.com　+81.3.6810.2102

〒100-0005 東京都千代田区丸の内3丁目3-1 新東京ビル2階254区