一般財団法人 日欧産業協力センター　レポート
欧州デジタル政策　EU Policy Insights

Vol.10　2024 年 5 月
「EU 人工知能法　（AI Act）- 採択・最終決定」

- 本資料は、当センターの公式見解を示すものではありません。
- 本レポートの内容は別途記載がない限り執筆時点で入手している情報に基づくものであり、その後の状況変化や追加政策発表により変わる場合があります。
- 本レポートへのご意見、取り上げて欲しいトピック等、お寄せください。
  eujp-info@eu-japan.or.jp

一般財団法人 日欧産業協力センター
〒108-0072　東京都港区白金 1-27-6　白金高輪ステーションビル 4 階
TEL: 03-6408-0281　FAX: 03-6408-0283
E-MAIL：eujp-info@eu-japan.or.jp

欧州デジタル政策 EU Policy Insights vol.10

「EU 人工知能法（AI Act）-採択・最終決定」

1. 概要

- EU 人工知能法（AI Act）は、EU の政策当局により最終決定され、AI システムを「禁止リスク」、「高リスク」、「限定リスク」、「最小リスク」の 4 段階に分類し、高リスクのシステムには厳格な要件を課すというリスクベースの枠組みを確立している。

- 特定の AI システムは禁止されており、その中には、操作技術、ソーシャルスコアリング、法執行のための遠隔生体認証、プロファイリング、性格的特徴のみに基づく予測的取り締まりなどが含まれる。

- リスクの高い AI システムの提供者(provider)や導入者(deployer)は、リスク管理、データガバナンス、技術文書作成、人的監督、正確性、堅牢性、サイバーセキュリティなどの厳しい義務を果たさなければならない。輸入業者、流通業者、サプライヤーもまた、特定の責任を負う。

- 汎用 AI（GPAI）モデルは、自動的に高リスクではないが、トレーニングやテストプロセスの詳細な文書化、著作権法の遵守、システミック・リスクを管理するための追加ステップが必要となる。汎用 AI が高リスクシステムとなった場合は、高リスク義務の完全遵守が求められる。

- 実施スケジュールは様々で、禁止 AI システムは 6 ヶ月以内、汎用 AI は 12 ヶ月以内、附属書 III の高リスク AI システムは 24 ヶ月以内、附属書 II の高リスクシステムは 36 ヶ月以内に尊寿されなければならない。実施規則は、法律発効後 9 ヶ月以内に制定されなければならない。

2. EU AI 法の概要

2024 年 3 月、欧州議会、同 5 月、EU 理事会は、欧州連合（EU）の人工知能法（AI 法）の最終案を成功裏に採決した。この法律は、欧州市場に投入される AI システムの提供者（provider）や導入者（deployer）向けの規則と義務に関する包括的な法律である。AI 法は、欧州連合（EU）全域における AI 技術の開発、展開、利用を管理することに特化した、この種のものとしては初の法的枠組みであり、特に注目される。

AI 法は、AI 技術の分類システムを導入し、AI 技術を 4 つの主要なリスクレベル、すなわち、①禁止リスク、②高リスク、③限定リスク、④最小リスクに分類している。この段階的アプローチは、様々な AI アプリケーションに関する潜在的リスクと規制監督を一致させる上で極めて重要である。高リスクに分類される AI システムについては、AI 法は厳格なコンプライアンス基準を義務付けている。これらのシステムは、インフラ管理、雇用・労務管理、法執行などの重要な分野で採用されることが多く、広範な安全性評価を受け、偏向やエラーを軽減する強固な対策を実証しなければならない。

逆に、最小リスクに分類される AI システムは、AI 対応ビデオゲームや電子メールスパムフィルターのようなアプリケーションを含み、規制上の制約に直面することはほとんどない。この区別は、AI アプリケーションの多様な意味合いを認識し、これらの違いに適切に対処するための規制枠組みを調整するものである。

AI システムの分類にとどまらず、AI 法は AI の倫理、プライバシー、データ・セキュリティに関するより広範な懸念にも対処している。同法は、EU 域内の AI 開発が基本的な権利と価値を維持することを保証することを目的としており、AI システムの透明性、説明責任、人間による監視を重視している。また、同法は、AI 技術の悪用や乱用の可能性を防止するという EU のコミットメントを反映し、有害性が高いと判断される特定の AI システムに対する具体的な禁止事項の概要も示している。

本稿では、AI 法の適用範囲（どのような AI システムが適用範囲に含まれるか）、適用範囲に含まれる AI システムの提供者（provider）や導入者(deployer)の義務、そして最後に AI 法の実施（企業が AI 法を遵守するためのスケジュール）について詳しく解説する。

3. AI 法の範囲

AI 法は、人工知能に関わる主体を注意深く区別し、「提供者(provider)」と「導入者(deplore)」のいずれかに特定する包括的な法的構造を確立している。提供者は AI システムを開発する者であるのに対し、導入者はこれらのシステムを実用的な場面で実装する個人または組織である。この区別は極めて重要であり、責任の所在を明確にし、同法の規制を遵守することを保証するものである。

AI 法では、「AI システム」は、機械技術に基づき、様々な程度で自律的に機能するように設計され、配備後に適応できるシステムとして広義に定義される。これらのシステムは、明示的または暗黙的な目的によって導かれ、入力データを処理して、物理的または仮想的な環境に影響を与えることができる予測、内容、推奨、または決定のような出力を生成する。AI システムの定義は、OECD の定義と広く類似している。

図表 1：ソフトウェアと AI を区別する AI システムの定義の主な要素

ソフトウェアで区別されるEUのAI法で定義されているAIシステムとは?	機械ベースのシステム
	様々なレベルの自律性で動作するように設計されている。
	導入後に適応性を示す可能性がある。
	明示的または暗黙的な目的のために設計されたもの。
	受け取った入力から、予測、コンテンツ、推奨、決定などの出力を生成する方法を推測する。
	物理的または仮想的な環境に影響を与えることができる。

冒頭で述べたように、AI 法は AI システムに対するリスクベースの分類アプローチである。高リスクの AI システムとは、安全性や基本的人権に重大な影響を与える可能性があるもので、厳しい規制の対象となる。これらのシステムは通常、医療、運輸、教育、法執行など、重要とみなされる分野で使用され、その導入には厳格な安全性評価、卓越したデータ品質、包括的な文書化が必要となる。

3.1 禁止される AI システム

AI 法は、特定の AI システムが欧州市場で運用されることを禁止している。禁止されている AI システムには以下が含まれる：

図表 2 : EU で禁止される AI システムの詳細な説明

操作	搾取	社会的スコアリング	生体認証による分類	予測的取り締まり	映像の非標的スクレイピング	感情認識
身体的・精神的危害を与える可能性のある人の行動を歪めるサブリミナル技術	年齢、障害、社会経済的状況に起因する特定集団の脆弱性を利用し、危害を及ぼす可能性のある行動を歪曲する。	社会的行動に基づいて人を評価し、不利益な扱いをすること： - データ収集の背景と無関係 - 不当 - 不釣り合い	人種、政治的意見、労働組合への加入、宗教的信条、性的指向を推測するために、自然、人を個別に分類すること。	プロファイリングや性格的特徴に基づき、犯罪を犯すリスクを評価または予測するために自然、人を評価すること。	インターネットやCCTV映像から顔画像を無制限にスクレイピングし、顔認識データベースを作成または拡大すること。	職場や教育機関において、医療上または安全上の理由がない限り、感情を推測すること。

• サブリミナル技術、または意図的に操作または欺瞞的な技術を使用して行動を実質的に歪め、重大な危害をもたらす AI システム。

•特定の特性に起因する個人またはグループの脆弱性を悪用し、重大な危害をもたらす AI システム。

• 法執行の分野で合法的に取得された生体認証データセットのラベル付けまたはフィルタリングを除き、機密情報に基づいて個人を個別に分類する生体認証分類システム。

• ソーシャルスコアリングシステム。

• 法執行を目的とした公衆におけるリアルタイムの遠隔生体認証システム。

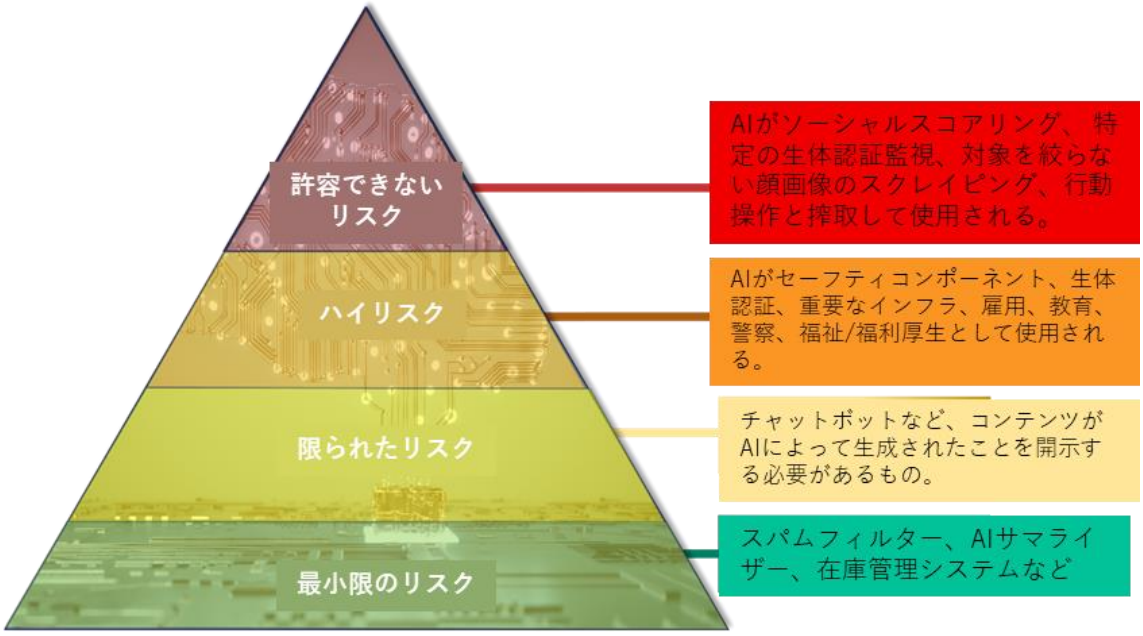
• 犯罪に関連する客観的で検証可能な事実に基づく人間の評価を支持する場合を除き、プロファイリングまたは性格特性のみに基づく予測的な取り締まり。

• ターゲットを絞らないスクレイピングに基づく顔認識データベース。

• 医療や安全上の理由を除き、職場や教育機関で感情を推測する。

3.2 高リスク AI システム

図表 3：AI 法 AI システムのリスクに基づくアプローチ。なお、分類された AI システムの一部には適用除外や除外項目がある（例：リアルタイムの生体認証）。



AI 法は、いくつかの基準に基づいて AI システムを「高リスク」に分類している。これらの基準には、AI システム自体がすでに特定の EU 規制の対象となっている製品の一種であるかどうか、AI システムが規制対象製品の安全コンポーネントとして機能するかどうか、または AI 法に規定されている「高リスク」AI システムの記述に合致するかどうかが含まれる。

1. 製品としての AI システム：AI システムが EU 調和法（AI 法の付属書に記載）の対象となる製品であり、同法に基づく第三者適合性評価が必要な場合、その AI システムは「高リスク」とみなされる。
2. 安全部品としての AI システム：第三者適合性評価を必要とする EU 調和法に該当する製品の安全部品として使用される AI システムも「高リスク」に分類される。

3. 記述された高リスク AI システム： AI 法の附属書にある「高リスク」カテゴリーの具体的な記述に合致する AI システムは、そのように分類される。これらのカテゴリーは、バイオメトリクス、重要インフラ、教育、雇用、エッセンシャルサービスへのアクセス、法執行、移民、司法・民主主義プロセスの管理などの分野で利用される AI システムを広く包含する。

3.3 適用除外とプロファイリングに関する考慮

AI システムが「高リスク」の分類に該当しない場合もある。軍事、防衛、国家安全保障の目的にのみ使用される AI システムや、科学的研究開発のために特別に開発・使用される AI システムなどである。さらに、AI システムが定義された「高リスク」基準外の役割を果たし、個人の健康、安全、基本的人権に重大な影響を与えない場合は、適用除外となる可能性がある。

4. 高リスク AI システムに対する規制義務

高リスク AI システムの提供者および導入者は、規制上の義務を負う。これらの義務には、AI システムのライフサイクル全体を通じたリスク管理の確保、データセットの品質と関連性を確保するためのデータガバナンスの維持、コンプライアンスを証明するための技術文書の作成などが含まれる。また、これらのシステムは、効果的な記録管理のために設計され、人間による監視を可能にし、正確性、堅牢性、サイバーセキュリティの基準を満たさなければならない。

図表 4 ：上の表は、高リスク AI システムのプロバイダーと導入者の義務

リスク管理システム：提供者は、AIシステムのライフサイクルを通じてリスクを特定、評価、軽減するための強固なシステムを導入しなければならない。	ライフサイクルを通じて継続的かつ反復的なプロセス： - 既知のリスク及び合理的に予見可能なリスクを特定し、分析する。 - 適切なリスク管理手段を採用する（全体的な関連残留リスクは "許容可能 "でなければならない）。 - 合理的に予見可能な使用と誤用及び配備の状況を考慮しなければならない。リスクマネジメントシステムは、実環境でのテストを含むことができ、内部リスクマネジメントプロセスと組み合わせることができる。
データガバナンス： AIシステムで使用されるデータの品質、代表性、セキュリティは、例えばバイアスを避けるために維持されなければならない。	データセットのトレーニング、バリデーション、テストは以下のことが必要である： - 適切であること。 - 十分に代表的であること。 - 可能な限り誤りがなく、意図された目的に照らして完全であること。 - 導入の背景を考慮すること。 バイアスの検出と修正のために、（適切な保護措置を講じた上で）特別なカテゴリーの個人データを例外的に処理することができる。
人的監視：AIの意思決定に人間が介入し、テクノロジーが管理下に置かれ、説明責任を果たすことを可能にする仕組みが必要である。	AIシステムは、導入者が（可能な限り適切かつ適切に）以下のことを行えるようにしなければならない： - 停止ボタンによってAIの機能を中断させる。 - AIの出力を無視、上書き、または逆行させる。 すべての監視手段は、以下のものでなければならない： - リスクレベル、自律性レベル、およびコンテキストの使用に比例すること。 - 技術的に可能であれば、提供者によって組み込まれること。 - 提供者によって特定され、導入者によって実装されること。
技術的文書化： 法の遵守を証明するために、詳細な文書化が必要である。	文書は以下のものでなければならない： - 明確かつ包括的であること。 - AI法附属書IVに記載されている最低限の要素を含むこと。 - 10年間保存されなければならない。
記録の保存：AI提供者と導入者は、AIシステムの確実な記録を保持しなければならない。 AIシステムのライフタイムにわたるイベント（ログ）の自動記録は技術的に可能でなければならない。 - ログは、提供者と導入社によって少なくとも6ヶ月間保存されなければならない。	記録の保存：AI提供者と導入者は、AIシステムの確実な記録を保持しなければならない。 AIシステムのライフタイムにわたるイベント（ログ）の自動記録は技術的に可能でなければならない。 - ログは、提供者と導入社によって少なくとも6ヶ月間保存されなければならない。 トレーサビリティを確保するために、特に重要なのは、以下に関連するイベントの記録を可能にすることである： - リスク及び／又は大幅な変更につながる状況を特定すること。 - 市販後モニタリングの促進。 - 導入中の業務のモニタリング。
透明性と使用説明書： 導入者は、AIシステムがどのように機能するか、またその限界について、明確で利用しやすい情報を提供されるべきであり、これによって理解と信頼が強化される。	AIシステムは導入者がAIアウトプットを適切に解釈し使用できるように設計されなければならない。 使用のインストラクションは以下を含まねばならない。 - 提供者とその代表者の情報 - AIシステムの特徴、能力及び限界 - 人的監視手段 - リソースとメンテナンスの必要性：AIライフサイクルを通しての頻度を含む。

また、高リスク AI システムの輸入業者、流通業者、サプライヤーも、特に登録、品質管理、モニタリング、事故報告などの面で責任がある。

5. 汎用 AI

欧州連合の AI 法は、汎用 AI（GPAI）モデルに関する具体的なガイドラインを導入している。汎用 GPAI の規定は、チャットボットや AI 画像生成テクノロジーなどの生成 AI システムに最も影響を与える。高リスクの AI システムとは異なり、汎用 GPAI モデルは、それ自体が高リスクとはみなされず、同法に基づく AI システムともみなされない。汎用 GPAI モデルは、その汎用性と様々なタスクを実行する能力を特徴とし、多くの場合、大規模なデータセットと自己監視を使用して開発される。しかし、これらのモデルは、まだ研究、開発、試作段階にある AI 技術を除外している。

汎用 GPAI モデルの提供者は、AI 法に基づき一定の責任を負う。汎用 GPAI モデルの提供者は、そのモデルのトレーニングやテストの過程と結果について、詳細な技術文書を作成しなければならない。さらに、汎用 GPAI モデルを他の AI システムに統合する可能性のある人々に対して、理解とコンプライアンスを促進するための明確な情報を提供することが求められる。

さらに、提供者は著作権法を遵守し、モデルのトレーニングに使用したデータの包括的な概要を共有しなければならない。汎用 GPAI モデルがフリーでオープンなライセンスの下で公開されている場合、そのモデルがシステミックなものと見なされない限り、提供者の責任は著作権ポリシーの管理とトレーニングデータの開示に絞られる。

汎用 GPAI モデルにおけるシステミックリスクとは、そのトレーニングに使用される計算能力が相当なものであることを意味し、提供者は追加的な措置を講じる必要がある。提供者は、モデルの能力を評価し、文書化し、リスクを特定するために敵対的テストを実施し、重大なインシデントを追跡し、関連する EU 当局に報告し、高いサイバーセキュリティ基準を確保しなければならない。コンプライアンスは、承認された実践規範を遵守することで証明することができ、その規範に従えば、AI 法の要件に適合していることを意味する。

これらのモデルから開発された汎用 GPAI システムについては、出来上がったシステムが高リスクに分類された場合、高リスクの AI システムに対する義務のすべてに従うことになる。これには、徹底した文書化の維持、著作権の尊重、訓練過程の透明性などが含まれる。

AI 法はまた、人と直接対話したり、合成コンテンツを生成したり、感情を認識したり、バイオメトリクスを分類したり、ディープフェイクを作成したりする AI システムについて、ユーザーに情報を提供することを義務付けている。場合によっては、このようなコンテンツは、人工的に生成または操作されたものであることを示すために、明確にラベル付けされなければならない。

ただし、法執行や芸術的、風刺的、創造的な目的で使用される AI システムについては、AI 法に除外規定が設けられている。これらの適用除外は、AI 利用における透明性と説明責任という全体的な目的を維持しつつ、特定の文脈における柔軟性の必要性を認めている。

6. バイオメトリクス AI システム

AI 法は、生体認証システムの使用にも特に注意を払っている。AI 法は、特定のバイオメトリクス識別システムを禁止するか、高リスクに分類している。

AI 法は、バイオメトリクス識別の利用を特定の状況において高リスクに分類する一連の措置を制定し、それによって、これらの技術を導入する者に高水準のコンプライアンスを要求している。これには法執行機関だけでなく、業務にバイオメトリクス・データを使用する可能性のある民間団体も含まれる。AI 法は、特に法執行機関による公共空間での無差別なライブの生体認証を禁止しているが、そのような導入が必要な場合には、厳格な監視と説明責任措置の対象となる狭い例外を設けている。

AI 法はさらに、顔画像の無秩序なスクレイピングを禁止し、適切な承認なしにデータベースを作成したり拡大したりすることを禁止している。

AI 法はまた、特に法執行機関による生体認証の使用に関して、包括的な報告と監視の仕組みを導入する。このようなメカニズムは、これらの技術の社会的影響を評価し、EU の基本的権利との整合性を確保するためのものである。国家当局には、バイオメトリクス識別システムの使用を監視・分析し、AI 法の規定への適合を確保し、公的説明責任を促進する任務が課せられている。

7. AI 法の施行

AI 法の実施スケジュールは、AI 法発行後 6 ヶ月から 36 ヶ月の期間をかけて、様々なカテゴリーの AI システムについて段階的に導入するように構成されている。実施スケジュールの概要は以下の通り：

図表 5 ：AI 法実施スケジュール

禁止AIシステム	AI法で禁止される、容認できないと判断されるAIの実施。	AI法発効後6ヶ月
汎用AI（GPAI）	GPAIシステムの提供者は、AI法のGPAIに関する規定を遵守しなければならない。	AI法の発効から12ヶ月後
Annex IIIに基づく高リスクAIシステム	AI法のAnnex IIIに規定される高リスクカテゴリーに該当するAIシステム。	AI法発効から24ヶ月後
Annex IIに基づく高リスクのAIシステム	Annex IIの対象となる高リスクのAIシステムで、通常、製品の安全部品として使用されるAIシステムを含む。	AI法発効後36ヶ月
実施規則	実施規則は、AI法の発効から9カ月後に制定されなければならない。これらの規則は、AIシステムの提供者が採用できるベストプラクティスとコンプライアンス基準のガイドラインとなる。	AI法発効から9ヶ月後

8. 違反に対する罰則

AI 法は、規定の不遵守に対する明確な罰則と行政罰を定めており、最も重大な罰則は、禁止 AI システムの配布に対する不遵守である（第 5 条）。

8.1 AI 禁止行為に対する罰則

禁止されている AI 行為（第 5 条）に違反した場合、最も厳しい罰則が課される。罰金額は、最高 3,500 万ユーロ、または違反者の全世界における前会計年度の年間総売上高の 7%のいずれか高い方となる。

8.2 高リスク AI システム規定の不遵守に対する罰則

高リスク AI システムのオペレーター、正規代理人、輸入業者、流通業者、導入者に関する規定違反、または透明性保持義務に関する規定に違反した場合、最高 1,500 万ユーロ、または前会計年度の全世界における年間総売上高の 3%のいずれか高い方の罰金を課される可能性がある。

8.3 不正確または誤解を招く情報の提供に対する罰則

規制機関や各国当局に対し、不正確、不完全、または誤解を招くような情報を提供することも罰則の対象となる。この種の違反には、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罰金が課される。

8.4 罰則に関するその他の考慮事項

AI 法は、特に中小企業（SMEs）や新興企業について、違反企業の規模や性質を考慮する必要性を認めている。これらの企業に対する罰金は、侵害の重大性、違反者の市場シェア、当局との協力の度合いなど、様々な要因によって低くなる可能性がある。

以下は、AI 法の違反に対する罰則体系をまとめた表である：

図表 6 ：AI 法に基づく主要な規定の不遵守および違反に対する罰則

違反カテゴリー	罰則
違反カテゴリー 罰則	禁止されるAI慣行 3500万ユーロまたは全世界の年間売上高の7%まで
事業者関連規定の不遵守	最高1,500万ユーロまたは全世界の年間売上高の3%まで
不正確または誤解を招く情報の提供	最高750万ユーロまたは全世界の年間売上高の1%まで

9. 日本企業への意味合い

EU AI 法の発効後は、AI システムの提供者、AI システムの導入者、AI システムのユーザーはすべて、それぞれの規定に従う必要がある。 注意すべき最も重要な要素は、AI 法はヨーロッパに拠点を置く企業だけでなく、所在地に関係なく、ヨーロッパで AI システムを導入するすべての企業に影響を与えるということである。

したがって、EU の AI 法は、EU 市場内または EU 市場向けに AI システムを開発、導入、または使用する日本企業に影響を与える。

企業はまず、自社が AI システムの開発者、導入者、提供者のいずれに分類されるかを特定する必要がある。 次に、この内部識別に続いて、ヨーロッパで開発、導入、または提供するすべての AI システムの計画を立てる必要がある。 このマッピングは重要な要素である。なぜなら、そうすることで、企業はどの AI システムが禁止、高リスク、限定リスク、または最小リスクに分類されるかをよりよく理解できるようになるから。 これにより、企業が自らの義務を認識するための遵守点となる。

主なソース

European Parliament adopted AI Act text (13th March 2024).

European Commission Press Release on adoption of the EUs AI Act (09th December 2023)

AI Act provisional agreement: 5662/24 (26th January 2024).

OECD definition adaption of AI Systems (29th November 2023).

European Council Press Release on provisional agreement on AI Act (09th December 2023).

European Council defining of AI and position on AI Act.

European Commission original AI Act text [outdated – for reference only] (23rd April 2021).

Shaping Europe's digital future - European Commission publication on AI.

European Commission Factsheet on AI Act.

European Commission Q&A on AI Act.

以上