



EU AI 法：新規則がもたらす主な影響

本ニュースレターは、人工知能（AI）の規制に関する一連の記事の第一部です。本稿では、AI の利用その他の関連する問題に対応するための世界初の包括的な法的枠組みである EU AI 法の概要を紹介いたします。

I. はじめに：

欧州連合（EU）の人工知能法（「AI 法」）が 2024 年 8 月 1 日に発効しました。これは、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り、欧州内外で AI の信頼性を促進することを目的としています¹。AI 法は EU 指令ではなく EU 規則の形で採択されたため、EU 加盟国に直接適用されます。その目的を達成するため、AI 法は「リスクベースアプローチ」を採用し、AI の提供者と利用者には、特定されたリスクのさまざまなレベルに応じた要件と義務を定めています。AI 法の適用範囲が広範であることを考慮すると、EU 域内で AI システムを開発、創造、利用、またはそうしたサービスを提供する日本企業にとって、AI 法は重大な影響を及ぼす可能性があります。

II. AI 法の範囲 :

一般的な範囲 :

AI 法は、一般に「AI システム」に適用されます。「AI システム」とは、「様々なレベルの自律性で動作するように設計され、配備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をもって、物理的または仮想的な環境に影響を及ぼすことができる予測、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」と定義されています²。

AI 法は、以下のとおり AI エコシステム全体における複数の事業者を広くカバーしています³ :

- 提供者 (Provider) : 有償・無償を問わず、自社名や商標で AI システムを市場に出したり、サービスを開始したりすることを意図して AI システムを開発する者。
- 利用者 (Deployer) : 事業の一環として、自らの権限で AI システムを利用する者。
- 輸入者 (Importer) : EU 域内に所在または設立され、EU 域外に設立された自然人または法人または商標が付された AI システムを市場に投入する自然人または法人輸入者。
- 流通事業者 (Distributor) : AI システムを EU 市場で販売する者 (ただし、提供者や輸入者を除く)。

AI システムに加えて、AI 法は以下に説明する「汎用 AI モデル」 (GPAI モデル) も規制しています。

域外適用性 :

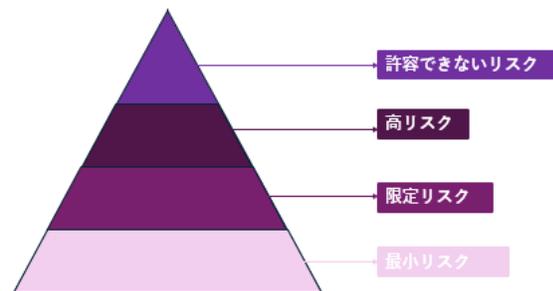
上記のように、AI 法は AI エコシステム全体の AI 事業者を広くカバーし、EU の地理的国境を越えて適用される可能性があるため、(GDPR と同様に) グローバルな適用範囲となる可能性があります。AI 法は、以下の 2 つの場合において第三国に設立された AI システムの提供者や利用者にも適用されます⁴。 :

- 提供者が、EU 域内において、AI システムを市場に投入したり、サービスを開始したり、汎用 AI モデルを市場に投入したりする場合。
- AI システムの提供者および利用者が、そのシステムによって生成されたアウトプットを EU 域内で利用する場合。

III. リスクベースのアプローチ：

AI 法は、AI システムを規制するためにリスクベースアプローチを導入しており、AI システムがもたらす健康、安全、基本的権利に対するリスクの度合いに応じて異なる要件と義務を課しています。AI システムは、リスクの度合いに応じて以下の 4 つに分類されます：

- 「許容できないリスク」の AI システム
- 「高リスク」の AI システム
- 「限定リスク」の AI システム
- 「最小リスク」の AI システム



AI システムの重要性を示すピラミッド
 欧州委員会のウェブサイトをもとに筆者にて作成
 (AI Act | *Shaping Europe's digital future* (europa.eu))

AI 法の大部分において、「高リスク」の AI システムのプロバイダーに課される義務が定められています。

(a) 「許容できないリスク」の AI システム：

AI 法は、EU 域内における「許容できないリスク」の AI システムの市場投入、サービス開始、利用を禁止しています。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を侵害する「許容できないレベルのリスク」をもたらす AI システムが含まれます⁵：

- 自然人の脆弱性の悪用、サブリミナル技術による操作や利用する AI システム；
- 公私にわたるソーシャルスコアリングを行う AI システム；

- 自然人のプロファイリング情報のみに基づいて犯罪リスクを評価・予測する AI システム；
- インターネットまたは監視カメラから無作為にスクレイピングした顔画像を用いて、顔認識データベースを作成する AI システム；
- 職場や教育機関において自然人の感情を推測するための AI システム；
- 自然人の生体測定分類または識別を行う AI システム。

(b) 「高リスク」の AI システム：

AI 法は、上市前の適合性評価の義務を含め、「高リスク」の AI システムに厳しい要件と義務を課しています。

AI 法は、「高リスク」の AI システムを健康、安全、環境または生産者の権利侵害に重大な危害を及ぼす可能性のある AI システムであると説明しています。「高リスク」の AI システムは、原則として以下のように規定されています：

- AI 法附属書 I の EU 整合法令法が適用される製品の安全措置として使用され⁶、当該法に基づく第三者による適合性評価を受ける必要がある AI システム⁷。
- AI 法の附属書 III に規定された 8 つの特定分野に該当する AI システム⁸：
 - 禁止されていない生体認証
 - 重要なインフラ
 - 教育及び職業訓練
 - 雇用、労働者管理、自営業へのアクセス
 - 必要不可欠な公共・民間サービスへのアクセスと享受
 - 法執行
 - 移民・亡命、国境管理
 - 司法の運営と民主的なプロセス

第二の категория（すなわち附属書 III の 8 分野）に該当する AI システムについては、一定の限定的に定められた例外が適用されますが、個人をプロファイリングする AI システムは常に高リスクとみなされ、厳格な要件の対象となります。

「高リスク」のAIシステムの提供者は、以下の厳しい義務を果たす必要があります⁹。：

- 「高リスク」のAIシステムに対する広範な要件が、AIシステムのライフサイクルを通じて満たされるようにする必要があります。そのような要件には以下が含まれます¹⁰。
 - リスク管理システム
 - データガバナンス
 - 記録管理
 - 透明性と利用者への情報提供
 - 人間による監視 可能性の確保
 - 正確性・安全性およびサイバーセキュリティの確保
- 品質管理システムの確立の確保
- すべての関連技術文書の管理
- 「高リスク」のAIシステムが自動生成したログの保管
- 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の採用
- 提供者がEU域外にいる場合は、EU域内に設立された認定代理人を連絡担当者として任命
- 「高リスク」のAIシステムがAI法第43条に基づく適合性評価手続を受けることの確保
- 欧州アクセシビリティ法の要件への準拠の確保
- 管轄当局への協力

また、利用者、輸入者、流通事業者といったその他の事業者も、AI法に定められた義務を果たさなければなりません。たとえば、利用者の義務には、以下¹¹が含まれます：

- 適切な技術的・組織的な措置の実施
- 適切な訓練と能力を備えた人間による監督の実施
- 使用説明書に基づいた「高リスク」のAIシステムの運用および監視の確保
- 「高リスク」のAIシステムの操作ログの少なくとも6ヶ月間の維持
- 「高リスク」の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、AIシステムの利用の通知

- 利用者が公的機関の場合、関連する登録要件に従う
- データ保護影響評価を実施する GDPR の義務の遵守
- 関係当局への協力

(c) 「限定リスク」の AI システム :

AI システムはユーザーと直接相互作用したり（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ります。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ります¹²。

「限定リスク」の AI システムに関連する透明性要件は、AI 法第 50 条に記載されています :

提供者の透明性要件 :

- 自然人と直接相互作用することを意図した AI システムは、個人が AI システムと相互作用していることを知らされるような方法で設計・開発されることを保証するものであること。
- 合成音声、画像、映像、テキストコンテンツを生成する際のシステムのアウトプットが、機械可読形式でマークされ、人為的に生成または操作されたものであることを検出できるようにすること。このような技術的解決策は、効果的で相互運用性があり、安全で信頼できるものでなければならない。

利用者の開示義務 :

- 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、システムの出力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こと。
- 公共の利害に関する事項を公衆に知らせる目的で公表された文章を作成またはその他の方法で修正する場合、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こと。

- 「高リスク」の AI システムとして認定される可能性がある感情認識や生体認識分類システムにさらされた個人に情報提供をすること。

(d) 「最小リスク」の AI システム：

上記のカテゴリーに該当しないその他の AI システムは「最小リスク」の AI システムであり、リスクが最小限またはゼロであるため規制の対象とはなりません（例：スパムフィルター）。「最小リスク」の AI システムは、さらなる制限や義務付けなしに導入することができますが、人間による監視、無差別、公平性といった一般原則に従うことが推奨されています¹³。

IV. 「汎用目的型 AI モデル」GPAI モデル：

AI 法は「汎用目的型 AI (GPAI) モデル」の利用を規制しています。「汎用目的型 AI (GPAI) 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、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プ活動に使用される AI モデルを除き、そのモデルが市場に投入される方法に関係なく、重要な汎用性を示し、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」と定義されています¹⁴。

GPAI モデルの利用は、「システムック・リスク」をもたらす GPAI モデル提供者に加重された義務を課す段階的アプローチによって規制されます。

GPAI モデルのすべての提供者は、以下の義務を果たさなければならないとされています¹⁵：

- モデルの技術文書を作成し、定期的に更新する；
- GPAI モデルをシステムに統合する予定の AI システムの提供者向けの文書を作成し、更新する；
- 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する；
- 学習に使用されたコンテンツの詳細なサマリーを一般に公開する；

無償かつオープンライセンスの GPAI モデルについては、GPAI モデルが「システムミック・リスク」を提示する場合を除き、無償かつオープンソースライセンスの下で一般に公開され、そのパラメータが公開されている GPAI モデルの提供者には、前者2つの義務のみが適用されます。

上記の義務に加え¹⁶、「システムミック・リスク」を有する GPAI モデルの提供者は、以下の追加的な義務を果たさなければならないとされています。このような「システムミック・リスク」は、そのトレーニングに使用される計算量の累計が 10^{25} FLOPs（フロップス（浮動小数点演算速度））を超える場合に認められます¹⁷：

- 標準化されたモデルの評価を行う；
- 潜在的な「システムミック・リスク」を評価し、軽減する；
- 重大インシデントと可能な是正措置の追跡と報告；
- 適切なレベルのサイバーセキュリティ保護を確保する。

「システムミック・リスク」を有する GPAI モデルの提供者は、整合化された基準が公表されるまで、準拠を実証するための実施基準に依拠することができます。かかる実施規範への準拠は、適合の推定につながります。AI オフィスは、GPAI モデル提供者、関連する各国所轄官庁に対し、EU レベルでの実施規範の作成に参加するよう要請することができます。

V. 新しい統治機構：

AI 法は、規制を適切に実施することを目的として、EU AI オフィス、独立専門家からなる科学委員会、AI 委員会、利害関係者のための諮問フォーラム¹⁸などの新たな管理機関を設立しています。

VI. 罰則：

この規則に従わない場合、罰則が適用されます。罰則額は、違反した義務の種類によって異なり、具体的には以下のように定められています¹⁹。：

ケース	罰金額
禁止されている AI 行為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
「高リスク」の AI システムまたは GPAI モデルの提供者、認定代理人、輸入者、販売業者、ユーザーまたはノーティファイド・ボディに課される義務の不履行	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
要請に対する回答として、不正確または誤解を招くような情報をノーティファイド・ボディまたは管轄当局に提供すること。	最高 750 万ユーロまたは全世界の年間総売上高の 1.5%のいずれか高い方の制裁金

上限額の罰金適用については例外があり、中小企業の場合、いずれか低い金額の罰金が科されます²⁰。

VII. AI 法適用のタイムライン：

EU の AI 法は、2024 年 8 月 1 日に EU 加盟 27 カ国すべてで発効されました。本規定は、以下のタイムテーブル²¹ に従って適用されます：

2024 年 8 月	EU の AI 法が発効
2025 年 2 月 2 日	一般規定と禁止されている AI 慣行
2025 年 8 月 2 日	汎用 AI モデルのガバナンス・ルールと義務
2026 年 8 月 2 日	AI システムへの EU AI 法の適用
2027 年 8 月 2 日	すべてのリスクカテゴリーに対する EU AI 法の適用

VIII. AI 法が日本企業に与える影響とは？

上記で説明したように、AI 法は EU の国境を越えて適用される可能性があり、そのような場合、同法第 22 条により、EU 域外に設立された「高リスク」の AI システムの提供者に対し、そのシステムを EU 市場で販売する前に、書面による委任により EU 域内に設立された認定代理人を任命するよう求められます。同法第 22 条は、EU 域外に設立された高リスクの AI システムの提供者に対し、EU 市場でそのシステムを利用可能にする前に、書面による委任により EU 域内に設立された認定代理人を任命することを義務付けています。EU 域内で AI システムを開発、作成、使用、またはそのようなサービスを提供する日本企業は、AI 法の導入がもたらす潜在的影響の評価を開始する必要があります。

具体的には、以下のような対応が考えられます²²。：

- AI 法に記載されているカテゴリーに従って、使用されている AI システムの種類を特定し、カタログ化する；
- EU の AI 法の適用範囲が広いことを考慮し、事業者による AI システムの利用が同法の適用範囲に含まれるかどうかを評価する；
- 社内外の AI システムがもたらす具体的なリスクを理解し、役割（提供者、利用者など）と使用する AI システムとの関連で満たすべき要件を理解する；
- ギャップ分析を実施し、コンプライアンス違反の領域を特定する；
- AI アプリケーションの意味について従業員を教育・訓練する；
- EU の AI 法の要件に正しく対応するため、関係者とコミュニケーションを図る；

最後に、AI 法は AI システムのリスクと展開に特に対処することを意図していますが²³、GDPR、消費者保護、知的財産権法など、企業が考慮する必要のある他の多くの規制の枠組みがあることに留意が必要です。したがって、AI 法を具体的に遵守する一方で、企業は既存の法的枠組みの下での他の義務を忘れてはならないことを理解することが重要です²⁴。

¹ Article 1 of the AI Act

² Article 3 (1) of the AI Act

³ [The EU AI Act Is Here: 10 Key Takeaways for Business and Legal Leaders – Publications \(morganlewis.com\)](#) (last visited on September 5, 2024)

⁴ Article 2, para. 1, items a) and c) of the AI Act

⁵ Article 5 of the AI Act

⁶ Article 6, para. 1, item a) of the AI Act

⁷ Article 6, para. 1, item b) and Recital 50 of the AI Act

⁸ Article 6, para. 2 of the AI Act

⁹ Articles 16-21 of the AI Act

¹⁰ Articles 8-15 of the AI Act

¹¹ Article 26 of the AI Act

¹² [ey-eu-ai-act-political-agreement-overview-february-2024.pdf](#) (last visited on September 5, 2024)

¹³ <https://www.trail-ml.com/blog/eu-ai-act-how-risk-is-classified> (last visited on September 5, 2024)

¹⁴ Article 3 (63) of the AI Act

¹⁵ Article 53, para. 1 of the AI Act

¹⁶ Article 55, para. 1 of the AI Act

¹⁷ Article 51, para. 2 of the AI Act

¹⁸ https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/?trk=public_post_comment-text (last visited on September 5, 2024)

¹⁹ Article 99 of the AI Act

²⁰ Article 99, para. 6 of the AI Act

²¹ [Long awaited EU AI Act becomes law after publication in the EU's Official Journal | White & Case LLP \(whitecase.com\)](#) (last visited on September 5, 2024)

²² [EU Artificial Intelligence Act - 10 essential EU AI Act questions businesses need to know \(kpmg.com\)](#) (last visited on September 5, 2024)

²³ Article 3 of the AI Act

²⁴ <https://www.linklaters.com/en/insights/blogs/digilinks/2024/may/eu---the-ai-act-reaches-the-finish-line---10-key-points> (last visited on September 5, 2024)

コンタクト



荒木 昭子

(Akiko Araki)

カリフォルニア州弁護士、弁護士、弁理士

akiko.araki@arakiplaw.com

CV: <https://arakiplaw.com/our-people/araki/>



ラウラ・コロンビーニ

(Laura Colombini)

パラリーガル

laura.colombini@arakiplaw.com

CV: <https://arakiplaw.com/our-people/colombini/>

[荒木法律事務所について]

荒木法律事務所 (Araki International IP&Law) は、2021年にグローバル・ファーム及び日本の国内ファーム等で10年以上の経験を有する弁護士によって創設された法律事務所です。特に、知的財産分野のクロス・ボーダーのライセンスや国際的な紛争解決の分野に力を入れています。その他、国際取引・紛争解決、データ・プライバシー、IT・情報通信、規制対応・コンプライアンス等、幅広い領域において企業をサポートいたします。

本ニュースレターは、当事務所のクライアントの皆様、当事務所所属弁護士と名刺交換させていただいた皆様、及び、当事務所が主催又は後援するイベントにご参加いただいた皆様宛てに、一般的な情報提供を目的としてご案内しております。本レターが法的アドバイスを構成するものではないことにご留意ください。配信を希望される場合、その他お問合せにつきましては、お手数ですがメールでご連絡ください。