March,21 2025

NEW "AI ACT" REGULATING ARTIFICIAL INTELLIGENCE IN THE EU ENTERED INTO FORCE ON 1 AUGUST 2024

*Over the past several years, the European Union has been discussing the introduction of a regulation for AI. Since the first bill was presented in April 2021, various discussions and negotiations have taken place to introduce the regulation, and as a result, the AI Act ("**AI Act**") was published in the Official Journal of the EU on July 12, 2024 and entered into force on August 1, 2024 ((EU) 2024/1689).*

The AI Act is of great interest because it is the first comprehensive AI framework in the world and other countries may refer to its regulatory framework in the future. Additionally, the AI Act is a framework that many businesses should be aware of because of the wide range of businesses to which it applies, its direct application to extraterritorial companies that provide AI systems within the EU, and the severe penalties it imposes for violations.

1. The Purpose of the regulation

The AI Act aims to improve the functioning of the internal market, promote the uptake of human-centric and trustworthy artificial intelligence (AI), and support innovation. At the same time, the AI Act also seeks to ensure a high level of protection of health, safety, and fundamental rights enshrined in the Charter (such as democracy, the rule of law and environmental protection) against the harmful effects of AI systems. (Art. 1).

In general, while most AI systems pose no noteworthy risks and are rather beneficial in helping to solve various social problems, some AI systems are considered to have potentially undesirable consequences for people.

The AI Act was introduced as a result of the belief that existing laws were not sufficient protection against such risks. Against this backdrop, the AI Act took a risk-based approach, and was designed to avoid imposing unnecessary restrictions on the promotion of the use of AI.

2. Scope of Application

- **Material Scope: AI Systems and GPAI Models**

The AI Act applies to **AI systems**, defined as "a machine-based system designed to operate with varying levels of autonomy

2025 年 3 月 21 日

EU における AI を規制する新たな「AI 規則」が 2024 年 8 月 1 日に発効しました

EU では、ここ数年にかけて、AI に対する規制の導入について議論を行ってきました。最初の法案が 2021 年 4 月に発表されて以降、規制の導入に向けて様々な議論や交渉が行われた結果、「AI Act」（以下「AI 規則」といいます。）は 2024 年 7 月 12 日に EU 官報に掲載され、2024 月 8 月 1 日に発効しました（(EU) 2024/1689）。

AI 規則は、世界初の包括的な AI 規制であり、今後、他国もその規制枠組みを参考にする可能性があるため、大変注目されます。加えて、AI 規則は、規制の対象になる事業者が広範であること、EU 域内に AI システムを提供する域外企業に対しても直接適用があることや、高額な制裁金が定められていることから、多くの事業者にとって注意すべき規制となっています。

1. 規則の目的

AI 規則は、EU 域内市場の機能を向上させ、人間中心の信頼できる人工知能（AI）の導入を促進し、それと同時に、EU 域内における AI システムの有害な影響に対して、健康、安全や、民主主義・法の支配・環境保護を含む基本的人権の高いレベルの保護を確保し、イノベーションを支援することを目的としています（第 1 条）。

一般論として、ほとんどの AI システムは、特筆すべきリスクはなく、むしろ様々な社会課題の解決に貢献する有益な存在ですが、一部の AI システムは、人々にとって望ましくない結果をもたらすおそれがあると考えられています。

そのようなリスクに対して、既存の法律だけでは保護が十分ではないと考えられた結果、AI 規則が導入されるに至りました。このような考え方を背景に、AI 規則は、リスクベースのアプローチをとり、AI の利用促進に対して、必要以上の規制を行わないよう配慮されています。

2. 適用範囲

- **実体的適用範囲：AI システム・汎用 AI モデル**

AI 規則の第一の適用対象は **AI システム**であり、「様々

and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (Art. 3(1)).

The AI Act applies to all AI systems except for specific sectors and activities, such as for military and national security use (Art. 2.3), law enforcement and judicial cooperation use (Art. 2.4), research, scientific and development use (Art. 2.6), personal and non-commercial use (Art. 2.10), and free and open-source use (Art. 2.12, with some exceptions.).

The AI Act also applies to **general-purpose AI ("GPAI")** models, being defined as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market" (Art. 3(63)).

Additionally, **GPAI system** is defined as an AI system which is based on a GPAI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems (Art. 3(66)).

なレベルの自律性をもって動作するように設計された、実装後に適応性を示すことがある、明示的または黙示的な目的のために、物理的またはバーチャルな環境に影響を与える予測・コンテンツ・レコメンデーション・決定などのアウトプットを生成する方法を受け取っ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(第 3 条 1 号)。

AI 規則は、軍事・国家安全保障のための利用（第 2 条 3 項）、法執行・司法協力のための利用（第 2 条 4 項）、研究・科学・開発のための利用（第 2 条 6 項）、個人的・非商用目的の利用（第 2 条 10 項）、無償かつオープンソースライセンスで提供される AI システム（第 2 条 12 項。ただし例外あり。）など特定の分野や活動を除き、すべての AI システムに適用されます。

また、AI 規則は**汎用 AI モデル**と呼ばれる AI モデルにも適用されます。汎用 AI モデルは、大要、「著しい汎用性を示し、市場投入される態様にかかわらず、広範囲の個別タスクを適切に実行することができ、様々な下流システムまたはアプリケーションに統合可能な AI モデル(大量のデータを用いた大規模な自己教師あり学習によりトレーニングされた AI モデルを含む)（市場投入前の研究、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）」と定義されています（第 3 条 63 号）。

また、汎用 AI モデルに基づく AI システムであり、直接利用することも、他の AI システムに統合することも可能な、多様な目的に対応できる AI システムのことを、**汎用 AI システム**と定義されています（第 3 条 66 号）。

● Personal Scope of Application: Operator

Under the AI Act, the entity subject to regulation is referred to as an **operator** (Art. 3(8)). An operator mainly consists of the following categories:

Provider	a natural or legal person, public authority, agency or other body that develops an AI system or a GPAI model or that has an AI system or a GPAI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge (Art. 3(3));
Product Manufacturer	a person who is placing on the market or putting into service an AI system together with its product and under its own name or trademark(Art. 2.1(e));
Deployer	a natural or legal person, public authority,

● 義務を負う主体―「事業者」

AI 規則において、規制の対象となる主体は総称して**事業者**と呼ばれます（第 3 条 8 号）。事業者は、主に以下のカテゴリーから構成されています。

提供者	AI システムもしくは汎用 AI モデルを開発する、または AI システムもしくは汎用 AI モデルを開発させ、有償・無償を問わず、自己の名称もしくは商標を用いて市場に流通させる、もしくはサービスを展開する自然人もしくは法人、公的機関、代理店、その他の団体（第 3 条 3 号）
製造業者	AI システムを、その製品とともに、自己の名称または商標の下で市場に流通させ、または使用させようとする者（第 2 条 1 項(e)）。

	agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity (Art. 3(4));
Importer	a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country (Art. 3(6));
Distributor	a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market (Art. 3(7)).

- **Geographic Scope of Application: In and Outside EU**

The AI Act is applicable to AI systems and GPAI models placed on the EU market, AI systems put into service in the EU, AI systems used in the EU, and AI systems whose produced output is used (or is intended to be used) in the EU (Art. 2).

Please note that providers of AI systems and GPAI models fall within the scope of the AI Act, independently of their place of establishment (Recitals 21 and 22, Art. 2.1). Furthermore, even if the AI system itself is not placed on the EU market, put into service, or used within the EU, if the output of an AI system is used (or is intended to be used) in the EU, relevant providers and deployers of AI systems, even if established in a third country, are subject to the AI Act (Art. 2.1).

Therefore, even a Japanese company that does not have an office in the EU may be subject to regulation as a provider if it is recognized as placing systems incorporating AI on the EU market, and even if its AI system is not placed on the EU market, it may be subject to regulation as a provider or implementer if the output of the AI system is used, or is intended to be used, in the EU.

3. General Obligations for AI Systems: A Risk-Based Approach

The AI Act categorizes AI systems depending upon the level of risks resulting from their functions into four categories and subjects each category of AI systems to different regimes, meaning that each operator of an AI system has different

導入者	AI システムを権限に基づいて使用する（個人的な非専門的活動の過程で使用される場合は除く）自然人または法人、公的機関、代理店、その他の団体（第 3 条 4 号）
輸入業者	EU 域外の自然人または法人の名称または商標が付された AI システムを市場投入する、EU 域内の自然人または法人（第 3 条 6 号）
販売業者	提供者または輸入業者以外のサプライチェーン上の自然人または法人で、AI システムを EU 市場で入手できるようにする者（第 3 条 7 号）

- **地理的適用範囲 ― EU 域内及び EU 域外**

AI 規則は、EU 市場に投入された AI システム・汎用 AI モデル、EU 域内でサービスを開始した AI システム、EU 域内で使用される AI システム、及びそのアウトプットが EU 域内で使用される（又は使用が意図される）AI システムに適用されます（第 2 条）。

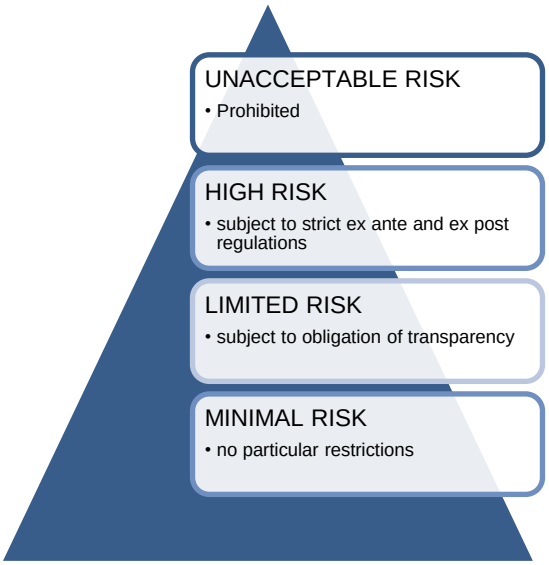
ここで、留意いただくべき点は、AI システム及び汎用 AI モデルの提供者は、その設立地とは無関係に、AI 規則の適用があるということです（前文 21 及び 22、第 2 条 1 項）。また、AI システムそのものが EU 市場に流通したり、稼働したり、使用されたりしていなくても、AI システムのアウトプットが EU 域内で使用される（又は使用が意図される）場合、関連する AI システムの提供者や導入者は、その設立地とは無関係に、AI 規則の対象となります（第 2 条 1 項）。

したがって、EU 域内に拠点を有しない日本法人であっても、AI を組み込んだシステムを EU 向けに市場投入していると認められる場合は提供者として規制対象になる可能性がありますし、EU 向けに市場投入またはサービス提供を行っていないとしても、自らが提供しまたは導入した AI システムについて、そのアウトプットが EU 域内で利用される場合（または利用が意図される場合）は、提供者または導入者として適用対象になる可能性があります。

3. AI システムの一般的義務：リスクに基づくアプローチ

AI 規則は、AI システムを、その機能から生じるリスクの大小に応じて以下の 4 つに分類し、カテゴリーごとに異なる規制の対象としています。すなわち、AI 事業者の義務の内容は、該当するカテゴリーに応じて、異なるもの

obligations based upon the applicable category.



According to this description, it would seem that AI systems are exclusively classified into one of the four risk categories as below, but this is actually not an accurate description; "Limited-Risk AI Systems" are defined from a different perspective than "High-Risk AI Systems," and some AI systems may fall into both categories (See Art. 50.6).

- **Prohibited AI Systems (Unacceptable Risk)**

In order to deal with AI that poses unacceptable risks, the AI Act prohibits the placing on the market, the putting into service, or the use of the following types of AI systems (Art. 5.1):

- Subliminal techniques

An AI system that deploys subliminal techniques beyond a person's consciousness, or purposefully manipulative or deceptive techniques, to cause significant harm.

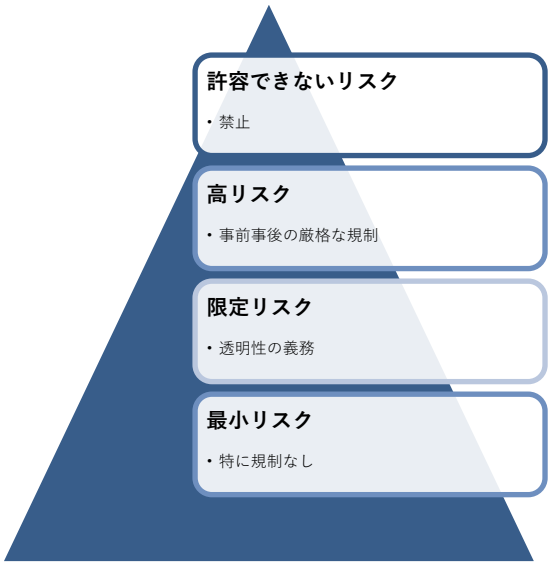
- Exploitation of vulnerabilities of persons

An AI system that exploits any of the vulnerabilities of a natural person due to such person's age, disability or a specific social or economic situation, by materially distorting the behavior of that person or in a manner that causes significant harm.

- Social scoring

An AI system for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behavior or known, inferred or predicted

となります。



この説明によれば、AI システムは以下の 4 つのリスクのいずれかに排他的に分類されるように思われますが、実はこれは正確な説明ではなく、「限定リスクの AI システム」は、「高リスクの AI システム」とは別の観点から定義されており、その両方に該当する AI システムもあり得る（第 50 条 6 項参照）ことに注意が必要です。

- **禁止される AI システム（許容できないリスク）**

許容できないリスクをもたらす AI に対処するため、AI 規則は、以下の種類の AI システムの市場投入、サービス開始、または利用を禁止しています（第 5 条 1 項）。

- サブリミナル技術

サブリミナル技術や操作的・欺瞞的な技術を用いて人の行動を歪め、人が通常は行わないような、重大な損害をもたらす決定を行わせる AI システム

- 人の脆弱性を悪用

年齢、障害又は社会的・経済的な苦境に起因する自然人の脆弱性を悪用し、重大な損害をもたらすような態様で人の行動を変容させる AI システム

- ソーシャルスコアリング

自然人または集団の社会的行動や性格的特徴等に基づいてソーシャルスコアリングを行うものであって、スコアリングの元データが収集された文脈と無関係な文脈での不利益な取扱い又は不当若しくは過度に不利益な取扱いをもたらす AI システム

personal or personality characteristics, with the social score leading to: (i) detrimental or unfavorable treatment in social contexts that are unrelated to the contexts in which the data was originally generated or collected; and/or (ii) detrimental or unfavorable treatment.

- Individual predictive policing

An AI system for making risk assessments of natural persons in order to assess or predict the risk of such persons committing a criminal offense, based solely on the profiling of a person or assessing their personality traits and characteristics.

- Scraping for facial images

An AI system that creates or expands facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.

- Emotion recognition in the workplace and educational institutions

An AI system to infer emotions of a natural person in the areas of workplace and educational institutions.

- Biometric categorization

A biometric categorization system that individually categorizes natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation.

- Real-time remote ID systems for law enforcement

A real-time remote biometric identification system in publicly accessible spaces for the purposes of law enforcement (however, there are exceptions under certain conditions for searches relating to specific victims and missing persons, preventing terrorism, etc.).

- 犯罪予測

自然人のプロファイリング情報又はその人格的特徴及び特性の評価のみに基づいて、その者の犯罪リスクを評価又は予測する AI システム

- 顔画像のスクレイピング

インターネットや監視カメラから無作為にスクレイピングすることにより、顔認識データベースを作成する AI システム

- 職場・教育機関での感情推測

職場および教育機関の分野において、自然人の感情を推測するための AI システム

- 生体測定分類システム

自然人をその生体データに基づいて分類し、その者の人種、政治的意見、労働組合への加入状況、宗教的又は哲学的信念、性生活又は性的指向を推測または推論するための AI システム

- 法執行目的でのリアルタイム遠隔生体認証

公共空間において法執行を目的として利用する場合における、リアルタイムでの遠隔生体識別のための AI システム（※ただし、犯罪被害者・行方不明者の捜索やテロ防止等については、一定の要件の下で許容される例外あり）

- **High-Risk AI Systems**

High-risk AI systems refer to:

- An AI system that is a product, or used as a safety component of a product, which is covered by particular EU legislation (the "EU-level harmonized legislation" listed in Annex I) such as radios, toys or medical devices, and required to undergo a third-party conformity assessment (Art. 6.1); or
- An AI system operating in eight sensitive areas, such as biometrics, critical infrastructure, education and vocational training, employment workers' management and access to self-employment, essential private and public services, law enforcement, migration, asylum and

- **高リスク AI システム**

高リスク AI システムとは、以下のいずれかに該当するものを指します。

- 特定の EU 規制（「EU 整合法令」。付属書Ⅰに列挙される。）でカバーされる製品（ラジオ、玩具、医療機器等）である AI システムや、そのような製品の安全装置である AI システムであって、当該法令に基づき第三者による適合性評価が必要とされているもの（第 6 条 1 項）
- 付属書Ⅲに列挙される AI システム（生体認証、重要インフラ、教育・職業訓練、雇用・労働者管理、必須の民間・公共サービスへのアクセス、法執行、移住・亡命・国境管理、司法及び民主的プロセスの運営に関する AI システム）（第 6 条 2

border control management, and administration of justice and democratic processes (Annex 3) (Art. 6.2).

AI systems that fall under the category of high-risk AI systems are generally required to contain the following features:

- Updated management system to assess and reduce risks (Art. 9)

The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating, including the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights and the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse.

- Implementation of data training, testing and data governance (Art. 10)

Data sets used in developing high-risk AI systems shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system, and shall be relevant, sufficiently representative, to the greatest extent possible, free of errors and complete in view of the intended purpose.

- Updated technical documentation demonstrating compliance with the AI Act which can be provided to competent authorities (Art. 11)

The technical documentation to demonstrate that the high-risk AI system complies with the requirements shall be drawn up before such system is placed on the market or put into service and shall be kept up to date.

- Recordkeeping and automated logs (Art. 12)

High-risk AI systems shall technically allow for the automatic recording of events over the lifetime of the system to ensure a level of traceability of the functioning of the high-risk AI system that is appropriate to the intended purpose of the system.

- Transparency and instructions for use for deployers (Art. 13)

High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret the system's output and use it appropriately. Specifically, it is required to provide instructions for use that include the identity and the contact details of the provider, the characteristics, capabilities and limitations of performance of the high-risk AI system, etc.

項）

高リスクの AI システムに該当する AI システムは、大要、以下のシステム要件を備えることが求められます。

- リスク管理システムの確立・実施・文書化・維持（第 9 条）

このリスク管理システムは、AI システムのライフサイクル全体を通じて反復継続的に実施されるプロセスでなければならず、定期的なレビューとアップデートが要求されます。また、健康・安全・基本的権利にもたらす可能性のある既知のリスクや合理的に予見可能なリスクを特定・分析することや、意図された目的や合理的に予見可能な誤用が行われる状況下において想定されるリスクについて分析することが必要です。

- データガバナンス（第 10 条）

高リスクの AI システムを開発するにあたって使用するデータセットは、本来の用途に照らして、適切なデータガバナンス及び管理プラクティスに服するものであること、また、本来の用途に照らして、関連性があり、十分に代表的で、可能な限り誤りがなく完全なものであることが要求されます。

- 技術文書の作成・維持（第 11 条）

AI システムがこれらのシステム要件を充足していることを示す技術文書を市場投入前に作成し、常に最新の状態を維持することが要求されます。

- 記録（第 12 条）

AI システムの適切な作動のトレーサビリティを確保するために、システムのライフタイムを通じて自動でログを記録する機能を備えることが要求されます。

- 透明性・情報提供（第 13 条）

導入者が AI システムの出力を解釈し、適切に利用できるように、透明性を確保することが必要です。具体的には、提供者に関する情報の身元・連絡先、AI システムの特徴・能力・性能の限界等の所定の事項について記載した使用説明書を提供することが要求されます。

- 人的監視装置（第 14 条）

AI システムの使用期間中、人間が効果的に監督できるような方法で設計・開発することが要求されます。

- 正確性・堅牢性・サイバーセキュリティの確保（第 15 条）

AI システムのライフサイクルを通じて、一貫して、適切

- Enabling of human oversight (Art. 14)

High-risk AI systems shall be designed and developed in such a way that they can be effectively overseen by natural persons during the period in which they are in use.

- Warranty of technical robustness, accuracy, and cybersecurity (Art. 15)

High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

In addition to the above system requirements, operators involved in high-risk AI systems are subject to different obligations depending on their position, i.e., Art. 16 to 21 apply to providers, Art. 23 applies to importers, Art. 24 applies to distributors, Art. 26 applies to deployers, respectively.

Only after compliance with the relevant requirements has been documented and proper notice submitted/registered by the operator to the relevant authorities in a Member State through a conformity assessment procedure (Art. 43) and execution of an EU declaration of conformity (Art. 47), will a certificate of conformity valid for a maximum of 5 years be issued (Art. 44), and the market or the service launch of the relevant high-risk AI system on the EU market be permitted (Art. 16).

- **Limited-Risk AI Systems**

Certain types of AI systems are subject to transparency obligations depending on the type.

- AI systems intended to interact directly with natural persons (ex., chatbots)

Providers shall ensure that AI systems are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system (Art 50.1).

- AI systems generating synthetic audio, image, video or text content (ex., AI image generator)

Providers shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated (Art 50.2). Deployers of an AI system that generates or manipulates image, audio or video constituting a deep fake, shall disclose that the content has been artificially generated or manipulated (Art 50.4).

- Emotion recognition system or Biometric categorization

なレベルでの正確性・堅牢性・サイバーセキュリティが達成されるように、設計・開発することが要求されます。AI システムの正確性の水準や、関連する正確性の指標は、使用説明書において明記される必要があります。

以上のシステム要件に加え、高リスク AI システムに関与する事業者は、それぞれの立場に応じて異なる義務の対象となります。すなわち、提供者には第 16 条から第 21 条の規定が、輸入者には第 23 条の規定が、販売業者には第 24 条の規定が、導入者には第 26 条の規定がそれぞれ適用されます。

関連する要求事項への適合が文書化され、事業者が適合性評価手続き（第 43 条）を通じて加盟国の関連当局に適切な通知・登録を提出した後にのみ、最長 5 年間有効な適合証明書が発行され（第 44 条）、EU 市場での高リスク AI システムの市場投入又はサービス開始が許可されます（第 16 条）。

- **限定リスク AI システム**

いくつかの種類の AI システムは、透明性の義務の対象となります。

- 自然人と直接やり取りすることを意図した AI システム（例：チャットボット）

提供者は、当該自然人に、AI システムと相互作用していることが通知されるように、その AI システムを設計・開発しなければなりません（第 50 条 1 項）。

- 人工音声、画像、動画、テキストなどのコンテンツを生成する AI システム（例：画像生成 AI）

提供者は、当該コンテンツが人工的に生成・操作されたものであることが検出できるようなマークがなされるようにしなければなりません（第 50 条 2 項）。また、ディープフェイクを構成する画像、音声、動画コンテンツを生成・操作する AI システムの導入者は、そのコンテンツが人為的に生成・操作されたものであることを開示

system

Deployers of an emotion recognition system or a biometric categorization system shall inform the natural persons exposed thereto of the operation of the system (Art 50.3).

しなければなりません（第 50 条 4 項）。

- 感情認識システムまたは生体認証分類システム

導入者は、対象となる自然人に、当該システムが動作していることについて、情報提供する必要があります（第 50 条 3 項）。

- **Minimal or No-Risk AI Systems**

This is not a specific named category. No obligations are stipulated in the AI Act but concerned AI operators are encouraged to voluntarily adopt codes of conduct, including governance mechanisms, objectives and performance indicators (Recital 165, Art. 95).

- **最低リスク又はノーリスク AI システム**

これは、特定の名称のカテゴリーではなく、AI 規則には具体的な義務は規定されていませんが、関係する AI 事業者は、ガバナンスの仕組み、目的、成果指標を含む行動規範を自主的に採択することが奨励されています（前文 165、第 95 条）。

4. Specific Duties for GPAI Models

Independently of the risk-based categorization of AI systems above, the AI Act introduces specific duties for the GPAI models.

- **Duties of GPAI model Providers**

GPAI model providers are subject to specific obligations relating to transparency consisting of the following: (a) create, update and save technical documentation of the GPAI model and provide it to the AI system providers, or to the AI Office or competent national authorities upon request; (b) implement a policy to comply with EU copyright law; and (c) provide a summary of information about the relevant GPAI models for the public (Art. 53.1).

- **Duties regarding GPAI Model Posing a Systemic Risk**

The AI Act applies additional restrictions to GPAI models that are considered to have "systemic risk". This "systemic risk" is defined as a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society, that can be propagated at scale across the value chain (Art. 3(65))。

More concretely, a GPAI model is classified as a GPAI model with systemic risk based on its high technical capabilities, and it shall be presumed to be a GPAI model with systemic risk if the cumulative amount of computation used for its training is greater than a certain threshold (Art. 51).

In addition to the requirements outlined above for GPAI model providers, providers of GPAI models with systemic risk shall notify the European Commission if they become aware that a GPAI model does or will qualify as one with systemic risk

4. 汎用 AI モデル用の個別な義務

上記のリスクベースの AI のカテゴリーとは別に、AI 規則では、汎用 AI モデルに関連する事業者に対する義務が課せられています。

- **汎用 AI モデルの提供者の義務**

汎用 AI モデルの提供者には、透明性に関する次の義務が課せられます ― (a)汎用 AI モデルの技術文書を作成・更新・保管し、AI システムの提供者や、AI 事務局や加盟国の関連当局（要請がある場合）に提供すること、(b) EU の著作権指令を遵守する方針を実施すること、(c)関連する汎用 AI モデルに関する情報の概要を一般に公開すること（第 53 条 1 項）。

- **システミックリスクのある汎用 AI モデル**

AI 規則では、汎用 AI モデルのうち「システミックリスク」があるとされるモデルについて、追加的な規制が適用されます。この「システミックリスク」とは、汎用 AI モデルの影響力の大きさに特有のリスクであり、その影響範囲の広さ、または公衆衛生・安全・治安・基本権・社会全体に対する実際の、もしくは合理的に予見可能な悪影響により、EU 市場に重大な影響を及ぼし、それがバリューチェーン全体にわたって大規模に伝播する可能性があるリスク」と定義されています（第 3 条 65 号）。

具体的には、システミックリスクのある汎用 AI モデルかどうかは、モデルの有する技術的能力から判断されますが、学習に使用された累積の計算量の所定の閾値を超える汎用 AI モデルは、システミックリスクがあるものと推定されます（第 51 条）。

without delay, or within two weeks (Art. 52), perform model evaluation to identify and mitigate systemic risk, assess and mitigate such systemic risk, track and report serious incidents to the AI Office and the competent national authorities, and ensure an adequate level of cybersecurity protection for the relevant GPAI model posing a systemic risk (Art. 55).

5. Institutional Structure and Competent Authorities

- **The AI Office**

The AI Act establishes the **AI Office**, an EU-level regulatory agency within the European Commission (Art. 64).

Established in February 2024, the AI Office is globally tasked with coherent application of the AI Act. It specifically develops better tools and guidance to identify and classify GPAI models (Art. 75) and High-Risk AI (Art. 27), facilitates compliance by AI operators as regards AI requirements notably by issuing template documents, sandboxes (Art. 57) and codes of practice (Art. 56), and monitors, supervises, and enforces the AI Act requirements by investigating violations and taking corrective action (Art. 89 to 93).

- **The Artificial Intelligence Board**

The European Artificial Intelligence Board is composed of representatives from Member States. It advises and assists the European Commission and Member States in order to facilitate the consistent and effective application of the AI Act (Art. 65).

- **National Competent Authorities**

National authorities will supervise and enforce the AI Act's national application and implementation. Each Member State must establish or designate at least one notifying authority (responsible for conformity assessment bodies and their monitoring) and one market surveillance authority (responsible for ex-post monitoring) by 2 August 2025 (Art. 70).

- **Other AI Act Stakeholders**

AI systems providers downstream will have the right to submit complaints to the relevant market surveillance authority and receive explanations (Art. 89). More widely, any natural or legal person having grounds to believe that there has been an infringement of the AI Act may submit complaints to the relevant market surveillance authority (Art. 85).

汎用 AI モデルの提供者に関する上記の要求に加え、システミックリスクのある汎用 AI モデルの提供者は、汎用 AI モデルがシステミックリスクを有するものであること（またその見込みであること）を認識した場合、遅滞なく、又は 2 週間以内に欧州委員会に通知し（第 52 条）、システミックリスクを特定・軽減するためのモデル評価を実施し、当該システミックリスクを評価・軽減し、重大な事故を追跡し、AI 事務局及び所管の加盟国の関連当局に報告し、関連するシステミックのある汎用 AI モデルについて適切なレベルのサイバーセキュリティを確保しなければなりません（第 55 条）。

5. 組織構造と権限機関

- **AI 事務局**

AI 規則は、欧州委員会内に EU レベルの規制機関である **AI 事務局**を設置しています（第 64 条）。

2024 年 2 月に設立された AI 事務局は、AI 規則の首尾一貫した適用を任務としています。具体的には、汎用 AI モデル（第 75 条）及び高リスク AI（第 27 条）を特定・分類するためのツールや指針の開発・改善や、特にテンプレート、サンドボックス（第 57 条）及び実務指針（第 56 条）を発行することにより、AI 事業者による AI 規則の遵守を促し、違反行為を調査し是正措置を講じることにより AI 規則の要件を監視、監督、かつ執行しています（第 89 条から第 93 条）。

- **欧州 AI 委員会**

欧州 AI 委員会は加盟国の代表で構成されており、AI 規則の一貫した効果的な適用を促進するため、欧州委員会及び加盟国に助言を与え、支援しています（第 65 条）。

- **加盟国の関連当局**

各加盟国の関連当局は、AI 規則の国内適用と実施を監督・執行します。具体的に各加盟国は、2025 年 8 月 2 日までに、少なくとも 1 つの届出機関（適合性評価機関及びその監視を担当）及び 1 つの市場監視機関（事後監視を担当）を設置又は指定しなければなりません。(第 70 条）。

- **その他の AI 規則関係者**

下流の AI システム提供者は、関連する市場監視当局に苦情を提出し、説明を受ける権利を有しています（第 89 条）。また、AI 規則に違反があったと信じるに足る根拠を持つ自然人又は法人は、関連する市場監視当局に異議

6. Sanctions

Non-compliance with EU AI Act rules on prohibited AI systems can result in monetary fines of up to EUR 35 million or 7% of worldwide annual turnover, whichever is higher. In contrast, the AI Act sets lower penalties for violations of high-risk AI systems provisions or limited-risk AI systems (3% or EUR 15 million), as well as for providing false information to authorities (1% or EUR 7.5 million) (Art. 99).

The AI Act also imposes separate penalties for providers of GPAI models who violate the Act; specifically, maximum fines of 3% of worldwide annual turnover or EUR 15 million, whichever is higher (Art. 101.1).

7. Timeline of Application

The AI Act entered into force on 1 August 2024, and individual provisions are enforceable in phases. Provisions for prohibited AI systems have been effective and subject to fines from 2 February 2025. Most of its provisions will be fully enforceable (including provisions on high-risk and main limited-risk AI systems) as of 2 August 2026 (Art. 113). The provisions for GPAI model including governance and notification will apply from 2 August 2025, and the remaining obligations will apply from 2 August 2027.

Because the obligations under the AI Act are mostly stipulated in the form of results and general obligations rather than examples of application, implementation guidelines by the European Commission (Art. 96) and delegated acts by the AI Office will follow, such as codes of practice for GPAI models providers, which are expected by May 2025 (Art. 56).

As Japanese companies are within the scope of application of the AI Act, they will need to prepare for compliance without waiting for full enforcement of all provisions, because compliance will require taking time-consuming steps, and also because once the guidelines and delegated acts are adopted, effective enforcement and imposition of sanctions are expected to be swift, with non-compliance also posing risks in terms of reputation loss.

8. Conclusions and Key Advice for Japanese Companies

In light of the enactment of the AI Act in the EU, some key

を提出することができます（第 85 条）。

6. 制裁

禁止される AI システムに関する EU の AI 規則の条項に違反した場合、最高 3,500 万ユーロ又は全世界の年間売上高の 7%のいずれか高い金額の課徴金の対象となります。高リスク AI システムや、限定リスク AI システムに関する条項の違反（3%又は 1,500 万ユーロ）、及び当局への虚偽情報提供（1%又は 750 万ユーロ）に関しては、より低い額の課徴金が設定されています（第 99 条）。

また、汎用 AI モデルの提供者がその義務に違反した場合は、全世界の年間売上高の 3%又は 1,500 万ユーロのいずれか高い金額の課徴金の対象となります（第 101 条第 1 項）。

7. 適用時期

AI 規則は 2024 年 8 月 1 日に発効し、個々の規定は段階的に執行可能となります。禁止される AI システムに関する規定は、2025 年 2 月 2 日に正式に適用され、課徴金の対象となりました。2026 年 8 月 2 日にはそのほとんどの規定（高リスク及び主な限定リスク AI システムの規定を含む）が完全に執行可能となります（第 113 条）。ガバナンスや届出を含む汎用 AI モデルに関する規定は 2025 年 8 月 2 日から、また残りの義務は 2027 年 8 月 2 日から適用されます。

AI 規則に基づく義務は、そのほとんどが適用例ではなく、結果や一般的な義務という形で規定されているため、欧州委員会によるガイドライン（第 96 条）や 2025 年 5 月までに予定されている汎用 AI モデル提供者のための実務指針を含む AI 事務局による委任規則が引き続き提供されることになります（第 56 条）。

日本企業にも AI 規則は適用される可能性があり、AI 規則遵守のための準備は時間を要するものです。そして、ガイドラインや委任規則が採択されれば、レピュテーションの低下といったリスクにとどまらず、執行や制裁の発動が実際に、かつ迅速に行われることが予想されるため、全ての条項が完全に施行されるのを待つことなく、速やかに AI 規則遵守のための準備に着手すべきです。

8. 結論と日本企業への主なアドバイス

recommendations for Japanese companies are as follows:

- Conduct internal assessments of whether the company has/may have AI systems or models (including GPAI models) in use, in development or about to be procured.
- Confirm whether the company is a deployer, provider or another type of AI operator under the AI Act.
- Assess the risks associated with company systems and categorize the relevant AI system or AI model based on their risks via AI-related mapping.
- Compare the AI Act requirements with existing internal AI-related policies and governance already in place and improve the latter to fill any gaps in non-compliance.
- Externally implement the relevant AI Act requirements in the company's supply chain and customer policies (by amending or drafting terms, policies, contracts, and other documents).
- Stay up to date with respect to the European Commission's future guidelines etc.

Compliance by Japanese companies with the AI Act is especially urgent, as outside the EU, the AI Act may become the standard for other national AI-related regulations. Indeed, some jurisdictions outside the EU, such as the U.S. State of Colorado and Canada have announced a desire to possibly replicate it.

Finally, as AI systems and AI models have widespread yet differentiated usages depending on the relevant business sectors, it might be useful to analyze the topical impact of the AI Act on some specific sectors.

If you have any questions regarding the contents of this newsletter, please do not hesitate to contact the authors.

KITAHAMA PARTNERS

Jiri Mestecky (Partner)
JMestecky@kitahama.or.jp

Ryosuke Naka (Partner)
RNaka@kitahama.or.jp

Minami Hosoi (Associate)
MHosoi@kitahama.or.jp

Claude Kaneda (Associate)
Ckaneda@kitahama.or.jp

EU における AI 規則の制定を踏まえ、日本企業におかれましては以下の事項を実施することをご提言させていただきます。

- 使用中、開発中、又は調達しようとしている AI システム又は AI モデル（汎用 AI モデルを含む）がある（又は可能性がある）場合、社内評価を実施する。
- 自社が AI 規則上の導入者、提供者、その他の事業者のいずれに該当するかを確認する。
- 会社のシステムに関連するリスクを評価し、AI マッピングによってリスクに基づき、各カテゴリーに関連する AI システム及び AI モデルを分類する。
- AI 規則の要件と既存の社内 AI ポリシー及びガバナンスを比較し、不足がある場合は改善する。
- 会社のサプライチェーンや顧客方針において、関連する AI 規則の要件を外部的に実施する（規約、方針、契約等を作成または修正する）。
- 欧州委員会の今後のガイドライン等に関して常に最新情報を入手する。

AI 規則は、EU 域内にとどまらず、各国が今後定める AI 規制のスタンダードとして参照される可能性があります。実際、コロラド州やカナダなど、EU 域外のいくつかの法域は、AI 規則を参照する可能性があるとの意向をすでに表明しています。そういった観点からも、日本企業による AI 規則への対応は特に急ぐべきだといえます。

最後に、AI システム及び AI モデルは広範でありながら事業分野によって具体的な使用方法には違いがあり、AI 規則が特定の事業分野に与える影響を分析することも興味深いといえます。

本ニュースレターの内容に関するご質問等がございましたら以下の著者までお気軽にお問合せ下さい。

弁護士法人北浜法律事務所

ジェリー・メステッキー（パートナー）
JMestecky@kitahama.or.jp

中 亮介（パートナー）
RNaka@kitahama.or.jp

細井 南見（アソシエイト）
MHosoi@kitahama.or.jp

金田 蔵人（アソシエイト）
Ckaneda@kitahama.or.jp