# EU AI規則の概要

2024年9月

欧州連合日本政府代表部

※英語の条文をもとに作成したものです。日本語訳は仮訳です。
※参照した条文はこちらです。
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
※網羅的なものではありません。

# EU AI規則（AI Act）とは

EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS**

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

○ 欧州委員会は、**2021年4月、AI規則案を公表**。共同立法機関（EU理事会及び欧州議会）による審議と交渉を経て、2024年5月成立。**2024年8月1日に施行**。

○ **2026年8月2日から本格適用**開始（施行6か月後、1年後、3年後に適用開始となる規定あり）。

○ 人間中心の信頼できる人工知能（AI）の導入を促進すること、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、環境保護等の基本的権利の高水準の保護を確保すること、イノベーションを支援することを目的としている。

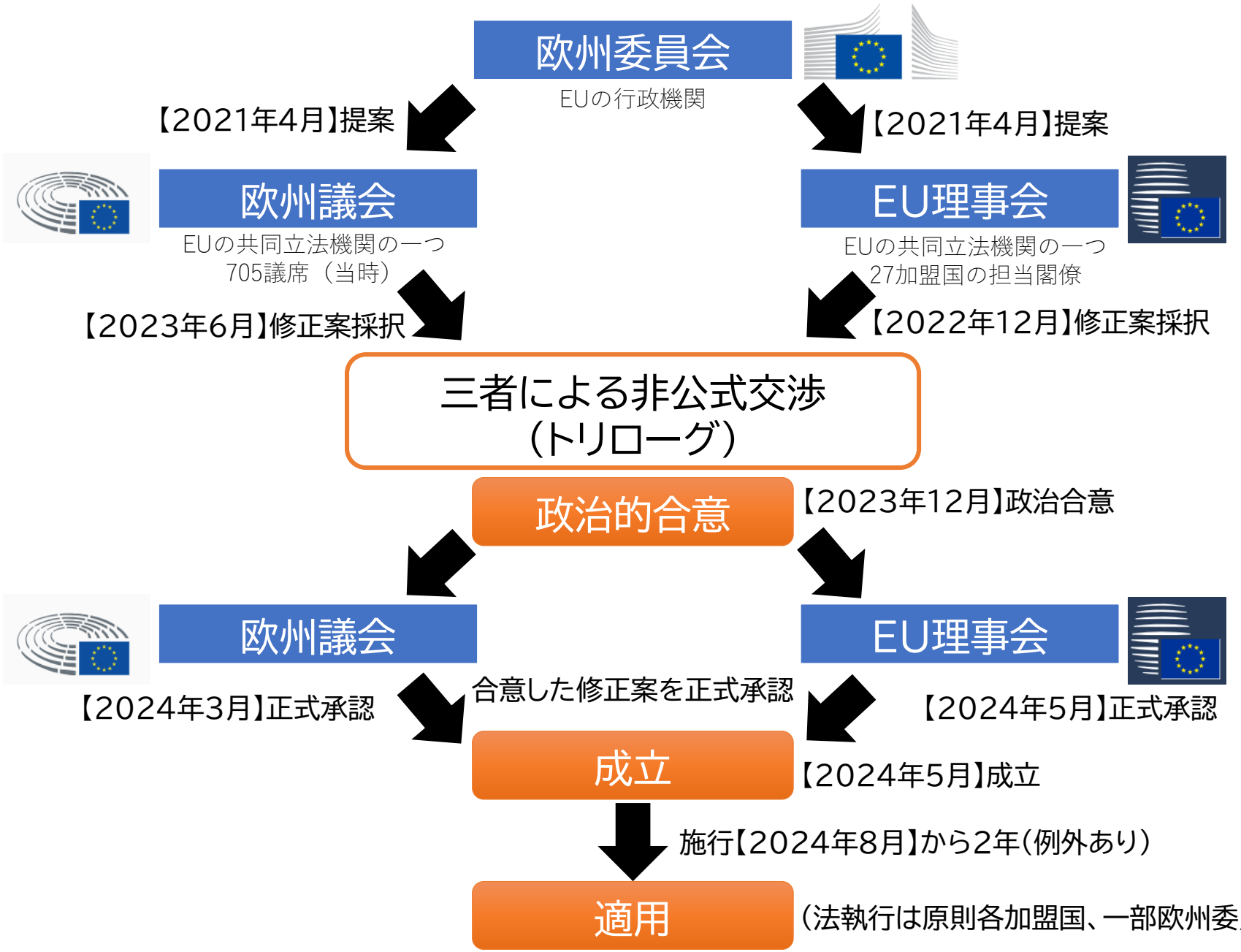
○ **リスクベースアプローチを採用**し、4つのリスクレベルを設け、**各々のリスクに応じた要件・規制を設定**するとともに、広範なタスクを学習・実行可能で他のAIシステムに統合可能な**汎用AIモデルに関する規律**を規定。提供者だけでなく導入者にかかる要件も存在。

○ EU域内にAIシステムを提供する**域外企業も適用対象**。

○ **違反の場合、最大で3,500万ユーロ又は年間世界売上高の7%の罰金**。

○ AIシステムの市場投入前に、革新的なAIシステムの**開発、試験、検証を実施できる環境として「AI規制サンドボックス」を提供する**。

# 審議経過


欧州委員会
EUの行政機関
【2021年4月】提案
【2021年4月】提案
欧州議会
EUの共同立法機関の一つ
705議席（当時）
EU理事会
EUの共同立法機関の一つ
27加盟国の担当閣僚
【2023年6月】修正案採択
【2022年12月】修正案採択
三者による非公式交渉
（トリローグ）
政治的合意
【2023年12月】政治合意
欧州議会
EU理事会
【2024年3月】正式承認
合意した修正案を正式承認
【2024年5月】正式承認
成立
【2024年5月】成立
施行【2024年8月】から2年（例外あり）
適用
（法執行は原則各加盟国、一部欧州委員会）

# 適用対象範囲①（第2条）

## 対象者

1. AIシステムをEU域内で市場に投入する又は稼働させる提供者（provider）。**設立場所がEU域内か第三国かは問わない**。
2. EU域内に所在するAIシステムの導入者（deployer）。
3. **アウトプットがEU域内で利用される**場合、**第三国に所在するAIシステムの提供者及び導入者。**
4. AIシステムの輸入者及び流通者。
5. 自らの名称又は商標の下に、製品とともにAIシステムを市場に投入する又は稼働させる製造者。
6. EU域内で設立されていない提供者の正規代理人。
7. EU域内に所在し影響を受ける者。

# 適用対象範囲②(第2条)

## 適用除外

1. **下記個別法**(Annex I Section Bに列挙)**の適用対象は、第6条第1項(ハイリスクAIシステムの定義)、第102条から第109条まで(関係法令のハネ改正)及び第112条(見直し規定)のみ適用**。
   a. 民間航空の安全性に関する規則 (Regulation (EC) 300/2008)
   b. 農林業用車両に関する規則 (Regulation (EU) No 167/2013)
   c. 二輪、三輪及び四輪車両に関する規則 (Regulation (EU) No 168/2013)
   d. 船舶用機器に関する指令 (Directive 2014/90/EU)
   e. 鉄道網の相互運用性に関する指令 (Directive (EU) 2016/797)
   f. 自動車及びその部品に関する規則 (Regulation (EU) 2018/858)
   g. 自動車の型式承認に関する規則 (Regulation (EU) 2019/2144)
   h. 民間航空分野の共通ルールに関する規則 (Regulation (EU) 2018/1139)
2. **軍事、防衛又は国家安全保障の目的のみ**のために市場に投入され、稼働され又は利用されるAIシステム。
3. 市場に投入され又は稼働されていないが、その**アウトプットが軍事、防衛又は国家安全保障の目的のみ**のために利用されるAIシステム。
4. 第三国の公的機関及び国際機関。ただし、当該機関がEU又はEU加盟国との法執行及び司法協力の国際協力又は協定の枠組みの下でAIシステムを利用する場合であって、当該第三国又は国際機関が個人の基本的権利及び自由の保護に関する適切な保護措置を提供するときに限る。
5. **科学研究開発の目的のみ**のために開発され稼働されるAIシステム及びAIモデル並びにそのアウトプット。
6. **市場投入又は稼働前**のAIシステム又はAIモデルに関する研究、テスト又は開発行為。
7. **純粋に個人的な非職業的活動**の過程でAIシステムを使用する自然人である導入者。
8. **フリー・オープンソース・ライセンス**でリリースされたAIシステム。ただし、ハイリスクAIシステム、禁止されるAIシステム(第5条)又は透明性義務(第50条)の対象となるAIシステムとして市場に投入され又は稼働される場合を除く。

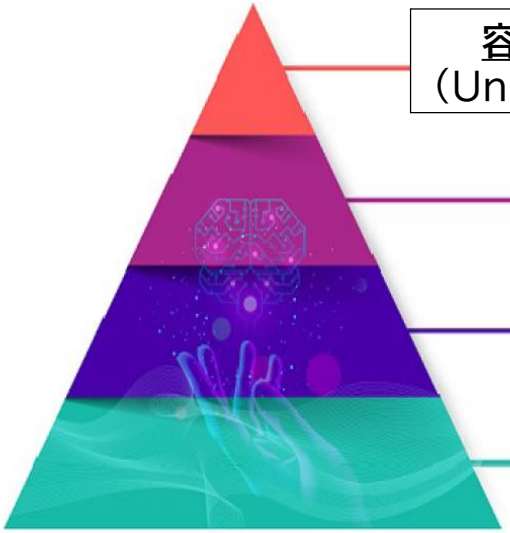
# 定義（第3条）

| 用語 | 定義 |
| --- | --- |
| AIシステム<br>（AI System） | 様々なレベルの自律性で動作するように設計され、導入後に順応性を示す可能性のある、機械ベースのシステムであって、明示的又は暗黙的な目的のために、物理的又は仮想的な環境に影響を与え得る予測、コンテンツ、推奨又は決定等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論するもの。 |
| 汎用AIモデル<br>（general-purpose AI model） | AIモデルが大規模に大量のデータで自己教師あり学習される場合を含め、大きな汎用性を示し、モデルが市場に投入される方法に関係なく広範で異なるタスクを有能に実行することができ、様々な川下のシステム又はアプリケーションに統合することができるAIモデル。ただし、市場に投入される前の研究、開発、プロトタイピング活動に使用されるAIモデルを除く。 |
| 汎用AIシステム<br>（general-purpose AI system） | 汎用AIモデルをベースとしたAIシステムであって、直接使用する場合及び他のAIシステムに統合される場合の両方において、様々な目的に対応する能力を有するAIシステム。 |
| 提供者<br>（provider） | AIシステム若しくは汎用AIモデルを開発する、又はAIシステム若しくは汎用AIモデルを開発させ、有償・無償を問わず、自己の名称若しくは商標の下に市場に投入又は稼働させる自然人又は法人、公的機関、代理店その他の団体。 |
| 導入者<br>（deployer） | 自らの権限の下でAIシステムを利用する自然人又は法人、公的機関、代理店その他の団体。ただし、AIシステムが個人的な非職業的活動の過程で利用される場合を除く。 |
| 川下提供者<br>（downstream provider） | AIモデルを統合したAIシステム（汎用AIシステムを含む）の提供者。そのAIモデルが自社で提供され垂直統合されたものであるか、契約関係に基づき他の事業者から提供されたものであるかを問わない。 |
| 本来の用途<br>（intended purpose） | 使用説明書、販売促進資料及び技術文書において提供者により提供される情報に明記されている、具体的な使用状況及び使用条件を含む、提供者によって意図されたAIシステムの用途。 |

# リスクベースアプローチ

○ AI規則では、**リスクベースアプローチを採用**し、4つのリスクレベルを設け、各々のリスクに応じた規制を規定。それに加え、汎用AIに関する規制あり。

## リスクベースアプローチ



（欧州委員会HP等の資料から一部加工）

| | |
|---|---|
| **容認できないリスク**（Unacceptable Risk） | ➢ サブリミナル技術、ソーシャルスコアリング、職場又は教育機関での感情推測システム、公共空間における法執行目的でのリアルタイム遠隔生体認証システム　等<br>➢ **原則禁止** |
| **ハイリスク**（High Risk） | ➢ 機械、医療機器、生体認証、重要インフラ、教育、雇用、法執行、移民管理　等<br>➢ **プロバイダー、輸入者、販売業者、導入者それぞれに対して、リスク管理、データガバナンス、技術文書の作成、人的監視措置、適合性評価手続、ログ保存など厳格な規制** |
| **限定的なリスク**（Limited Risk） | ➢ 生成AI、自然人とやり取りするAI、感情認識システム　等<br>➢ **AIにより生成されたコンテンツである旨のマーキングやAI使用の告知など限定的な透明性義務** |
| **最小限のリスク**（Minimal Risk） | ➢ 上記以外<br>➢ **自由に利用可能（自主的な行動規範の推奨あり）** |

## 汎用AIモデル提供者に対する義務

| 汎用AIモデル一般 | システミックリスクを有する汎用AIモデル |
|---|---|
| ➢ 技術文書の作成及び更新<br>➢ 汎用AIモデルをAIシステムに統合する提供者向けの情報・文書の作成、更新及び提供<br>➢ 著作権法を遵守するためのポリシーの実行<br>➢ 汎用AIモデルの学習に使用したコンテンツに関する十分に詳細な要約の作成及び公開<br>➢ 域内代理人の指名 | （左記に加えて）<br>➢ モデル評価の実施<br>➢ EUレベルでのシステミックリスクの評価及び軽減<br>➢ 深刻なインシデント及びそれに対する是正措置のAIオフィスへの報告<br>➢ 適切なレベルのサイバーセキュリティ保護 |

# AIリテラシー（第4条）

- AIシステムの**提供者及び導入者は**、技術的知識、経験、教育及び訓練並びにAIシステムが使用される文脈を考慮し、かつ、AIシステムが使用される対象者又は対象者のグループを考慮した上で、最善の範囲で、職員及びその職員に代わってAIシステムの操作及び使用を担当する者の**十分なレベルのAIリテラシーを確保するための措置を講じなければならない。**

# 禁止されるAIシステム①(第5条)

## 1. サブリミナル技術を使用するAIシステム

十分な情報に基づいた意思決定を行う能力を著しく損なうことにより人の行動を著しく歪める目的又は効果を有する、人の意識を超えたサブリミナル技術又は意図的に操作的若しくは欺瞞的な技術を導入するAIシステムの上市、稼働又は利用。

## 2. 人の脆弱性を悪用するAIシステム

人に重大な損害を与えるか又は与える可能性が合理的に高い方法で人の行動を著しく歪める目的又は効果を有する、年齢、障害又は特定の社会的若しくは経済的状況に起因する自然人又は特定の集団の脆弱性を悪用するAIシステムの上市、稼働又は利用。

## 3. ソーシャルスコアリング

社会的行動又は既知、推論若しくは予測される個人的若しくは人格的特徴に基づき一定期間にわたり自然人又は集団の評価又は分類を行うための AI システムであって、以下のいずれかにつながるソーシャルスコアを伴うものの上市、稼働又は利用。

（1）データが当初生成又は収集された文脈とは無関係な社会的文脈での特定の自然人又は集団に対する不利益又は不利な扱い。

（2）特定の自然人または集団に対する、その社会的行動又はその重大性に照らして不当又は不釣り合いな不利益又は不利な扱い。

## 4. 犯罪予測

自然人のプロファイリング又はその人格的特徴及び特性の評価のみに基づいて自然人が犯罪を犯すリスクを評価又は予測するために自然人のリスク評価を行うためのAIシステムの上市、この特定の目的のための稼働又は利用。ただし、この禁止は、犯罪活動に直接関連する客観的かつ検証可能な事実に基づいている、犯罪活動への人の関与に関する人間による評価を支援するために使用されるAIシステムには適用されない。

## 5. 顔画像のスクレイピング

インターネットや監視カメラ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又は拡張するAIシステムの上市、この特定の目的のための稼働又は利用。

## 6. 職場及び教育機関での感情推測AIシステム

職場及び教育機関での自然人の感情を推測するためのAIシステムの上市、この特定の目的のための稼働又は利用。ただし、医療上又は安全上の理由で利用することが意図されている場合を除く。

## 7. 生体分類システム

人種、政治的意見、労働組合への加盟、宗教的又は哲学的信条、性生活又は性的指向を推測または推論するために、生体データに基づいて自然人を分類する生体分類システムの上市、この特定の目的のための稼働又は利用。ただし、この禁止は、合法的に取得された画像などの生体データセットの生体データに基づくラベリング若しくはフィルタリング又は法執行の分野における生体データの分類を対象としない。

# 禁止されるAIシステム②(第5条)

**8. <u>公衆がアクセス可能な空間における法執行目的でのリアルタイム遠隔生体認証システムの利用。</u>ただし、<u>以下の目的のために厳密に必要な場合は除く。</u>**

(1) 誘拐、人身売買若しくは性的搾取の被害者の的を絞った捜索又は行方不明者の捜索。
(2)自然人の生命若しくは身体の安全に対する具体的、実質的かつ差し迫った脅威又は真正かつ現在若しくは真正かつ予見可能なテロ攻撃の脅威の防止。
(3)Annex IIに言及され、かつ、当該加盟国において少なくとも4年の拘禁刑又は拘禁命令により処罰される犯罪について、犯罪捜査、訴追又は刑事罰の執行の目的で、容疑者の所在を突き止め又は特定すること。
※利用に当たっては、一定の緊急事態を除き、司法機関又は独立した行政機関による事前許可が必要。

＜Annex IIに列挙されている犯罪リスト＞

- テロリズム
- 人身売買
- 児童の性的搾取、児童ポルノ
- 麻薬又は向精神薬の不正取引
- 武器、軍需品、爆発物の不法取引
- 殺人、重傷傷害
- 人間の臓器又は組織の不正取引
- 核物質又は放射性物質の不法取引
- 誘拐、不法な拘束又は人質取り
- 国際刑事裁判所の管轄下にある犯罪
- 航空機又は船舶の不法な拿捕
- 強姦
- 環境犯罪
- 組織的又は武装した強盗
- サボタージュ
- 上記の犯罪に関与する犯罪組織への参加

# ハイリスクAI①（第6条、Annex I及びIII）

○ ハイリスクAIには2つのカテゴリが存在。それぞれAnnex IとAnnex IIIに関連。

## ハイリスクAI（第1カテゴリ）

■ 以下の条件の**両方を満たす**AIシステム。

（1）AIシステムが、**Annex Iに記載されている法令の対象となっている製品の安全部品**として使用されることを意図しているか、またはそれ自体が製品であること。

（2）AIシステムを安全部品とする製品又は製品としてのAIシステム自体が、**Annex Iに掲げる法令に基づく第三者による適合性評価義務の対象**であること。

### Annex I Section A

1. 機械指令（Directive 2006/42/EC）
2. 玩具の安全性指令（Directive 2009/48/EC）
3. レジャー用・個人用船舶指令（Directive 2013/53/EU）
4. エレベーター及びその部品に関する指令（Directive 2014/33/EU）
5. 爆発性環境下での保護システムに関する指令（Directive 2014/34/EU）
6. 無線機器指令（Directive 2014/53/EU）
7. 圧力機器指令（Directive 2014/68/EU）
8. ロープウェイ設備規則（Regulation (EU) 2016/424）
9. 個人用保護器具規則（Regulation (EU) 2016/425）
10. ガス燃料機器規則（Regulation (EU) 2016/426）
11. 医療機器規則（Regulation (EU) 2017/745）
12. 体外診断用医療機器規則（Regulation (EU) 2017/746）

※Annex II Section Bは、第112条（見直し規定）等のみが適用される製品に関する法令を列挙（P3参照）。

# ハイリスクAI② （第6条、Annex I及びIII）

## ハイリスクAI（第2カテゴリ）

| | |
|---|---|
| 原則 | **Annex III**に記載されているAIシステム。 |
| 例外 | ただし、意思決定の結果に重大な影響を与えないことを含め、**自然人の健康、安全又は基本的権利に危害を及ぼす重大なリスクをもたらさない場合、ハイリスクとはみなされない。以下のいずれか**を満たす場合はこの例外に該当する。<br>（a）AIシステムが**限られた手続的タスク**を実行することを意図したものであること。<br>（b）AIシステムが以前に**完了した人間の活動の結果を改善する**ことを意図したものであること。<br>（c）AIシステムが、**意思決定のパターン又は**以前の意思決定のパターンからの**逸脱を検出する**ことを意図しており、人間による適切なレビューなしに以前に完了した人間の評価に取って代わる又は影響を与えることを意図していないこと。<br>（d）AIシステムが、Annex IIIに掲げ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たものであること。 |
| 例外の例外 | ただし、Annex IIIに記載されているAIシステムは、**自然人のプロファイリングを行う場合、常にハイリスク**とみなされるものとする。 |

- AIシステムがAnnex IIIに列挙されているがハイリスクではないと考える提供者は、市場投入又は稼働前にその評価を文書化し、当局の要求に応じて当該文書を提出する。ただし、当該AIシステムの登録は必要。
- 欧州委員会は、ハイリスク・非ハイリスクの具体例の包括的なリストを伴うガイドラインを策定する（施行から18か月以内）。
- 上記（a）～（d）のリストは、欧州委員会が委任法令により追加・削除可能。

# ハイリスクAI③（第6条、Annex I及びIII ）

## Annex III

※欧州委員会が委任法令で追加・修正・削除可能。

### 1. 生体認証

（1）遠隔生体認証システム（1対1認証（verification）は含まない）、（2）機微な特徴や属性に基づく生体分類、（3）感情認識

### 2. 重要インフラ

重要デジタルインフラ、道路交通、水、ガス、暖房及び電力の供給の管理・運営における安全部品

### 3. 教育・職業訓練

（1）教育機関及び職業訓練機関へのアクセス又は割当て決定、（2）学習結果の評価、（3）個人が受ける教育レベルの評価、（4）テスト中の禁止行為のモニター・検知

### 4. 雇用、労働者管理及び自営業へのアクセス

（1）採用・選考（特に職業広告、求職申込みの分析、候補者の評価）、（2）雇用関係の条件、昇進、雇用契約関係の終了、タスク割り当て及びパフォーマンス評価に影響を与える決定

### 5. 必須の民間・公共サービスへのアクセス

（1）公的支援給付及びサービスへの自然人の適格性の評価、付与、減額、取消し又は再請求、（2）クレジットスコア（金融詐欺検知目的の場合を除く）、（3）生命保険・健康保険におけるリスク評価・価格決定、（4）緊急通報の評価・分類、緊急時初動対応サービス（警察、消防士、医療、緊急患者トリアージシステム等）の派遣又はその優先順位付け

### 6. 法執行

（1）自然人が犯罪被害者になるリスクの評価、（2）ポリグラフ、（3）犯罪捜査・訴追過程での証拠の信頼性評価、（4）プロファイリングのみに基づかない自然人の犯罪・再犯リスクの評価又は性格特性若しくは過去の犯罪行動の評価、（5）犯罪認知・捜査・訴追過程でのプロファイリング

### 7. 移民、亡命、国境管理

（1）ポリグラフ、（2）入国者の安全保障上のリスク、不正移民のリスク又は健康上のリスクなどの評価、（3）亡命、査証及び滞在許可申請並びに関連する苦情の審査、（4）自然人の検知・認識・特定（旅行書類真正性の検証を除く）

### 8. 司法及び民主的プロセスの運営

（1）司法当局による事実と法律の調査・解釈及び法律の適用の支援並びに紛争解決手続における同様の用途、（2）選挙若しくは住民投票の結果又は投票行動に影響を与えること（選挙キャンペーンの組織運営等を除く）

# ハイリスクAIシステム提供者の義務①（第16条～第25条、第48条～第51条、第62条）

1. ハイリスクAIシステムが**本法の要件（次ページ以降参照）に準拠していることを確保**すること。
2. ハイリスクAIシステム、そのパッケージ又は付属文書に、その**名称、登録商号又は登録商標及び住所**を表示すること。
3. **品質管理システム**を策定・文書化すること。以下の内容を含める。

| | | | |
|---|---|---|---|
| 1 | 適合性評価手順の遵守及びハイリスクAIシステムの修正管理手順を含む、規制遵守のための戦略 | 7 | 市販後モニタリングシステムの設定、実施及び維持 |
| 2 | 設計、設計管理、設計検証、開発、品質管理、品質保証に使用される技術、手順及び体系的措置 | 8 | 重大インシデントの報告に関する手順 |
| 3 | 開発前、開発中、開発後に実施すべき審査、試験、検証手順、それらの実施頻度 | 9 | 当局、顧客その他の利害関係者とのコミュニケーションの取扱い |
| 4 | 適用される規格を含む技術仕様 | 10 | 関連文書及び情報の記録保持のためのシステム及び手順 |
| 5 | データ管理のためのシステム及び手順 | 11 | 供給確保に関する措置を含む資源管理 |
| 6 | リスク管理システム | 12 | 各項目の管理者その他の職員の責任を定めた説明責任の枠組み |

4. 以下の**文書を、市場への投入又は稼働後10年間、当局に利用可能**とすること。
   ・技術文書　　・品質管理システム関連文書　　・適合性評価機関に承認された変更に関する文書
   ・適合性評価機関から発出された文書　　・EU適合性宣言
5. 自己の管理下にある場合、自動的に生成する**ログを保管**すること。
   ・保存期間は、本来の用途と適用される法的義務に照らして適切な期間だが、**最低6ヶ月間**。
6. 上市前に関連する**適合性評価手続を受ける**こと。
7. **EU適合性宣言の作成**及び**CEマークの貼付。**
8. **EUデータベースへの登録**（提供者とAIシステムの両方）。

# ハイリスクAIシステム提供者の義務②（第16条～第25条、第48条～第51条、第62条）

9. ハイリスクAIシステムが本法の要件に適合していない場合、**必要な是正措置（リコール含む）を講じる**こと。
10. ハイリスクAIシステムが自然人の**健康、安全又は基本的人権に対するリスク**を生じさせていることを認識した場合、直ちに原因を調査し、法令不遵守の性質及び講じた是正措置について**当局及び適合性評価機関に通知する**こと。
11. 当局からの要請に応じ、**本法の要件遵守の証明、情報・文書の提出、保管ログへのアクセスの提供**。
12. **アクセシビリティに関するEU指令**（指令2016/2102及び指令2019/882）の遵守。
13. **域内正規代理人の設置**。代理人には以下のタスクを行う権限を付与すること。
    - ・EU適合性宣言及び技術文書が作成されていること及び適切な適合性評価手続が実施されていることの確認。
    - ・市場への投入又は稼働後10年間、提供者の連絡先並びにEU適合性宣言、技術文書及び適合性証明書のコピーを当局に利用可能とすること。
    - ・当局に対する本法の要件遵守の証明、情報・文書の提出、保管ログへのアクセスの提供。
    - ・その他当局の行動への協力。
    - ・EUデータベースへの登録又は登録内容の正確性の確保。

# ハイリスクAIシステムが満たすべき要件① (第8条～第15条)

| 要件 | 内容 |
|---|---|
| リスク管理システム | ■ **リスク管理システムを確立・実施・文書化・維持すること**。<br>■ リスク管理システムとは、以下で構成される、**AIシステムのライフサイクル全体を通して反復継続的に実施**されるプロセスでなければならない。<br>**i.** **健康、安全又は基本的人権に対する既知及び予見可能なリスクの特定及び分析**<br>ii. 本来の用途に従って使用され又は**合理的に予見可能な誤用が行われた際に出現し得るリスクの推定及び評価**<br>iii. 市販後モニタリングに基づくリスク評価<br>iv. 上記i.で特定されたリスクに対処するための適切かつ的を絞った**リスク管理措置の採用**<br>■ **リスク管理措置**:**残留リスクが許容可能と判断されるものでなければならない**。措置の特定に当たっては以下を確保する。**残留リスクは、利用者に要伝達**。<br>➢ 適切な設計及び開発により、可能な限りリスクを排除又は低減<br>➢ 排除できないリスクに関して、適切な軽減及び管理手段を実施<br>➢ 導入者に対する適切な情報及びトレーニングの提供<br>■ **テスト**:適切なリスク管理措置を特定するため、**開発中、遅くとも上市前にテストを実施。** |
| データガバナンス | **以下の品質基準を満たす学習・検証・テスト用データセットに基づいて開発**すること。<br>➢ 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。<br>➢ 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**。<br>➢ 本来の用途のために必要な範囲において、AIシステムの利用が意図されている特定の地理的、文脈的、行動的又は機能的設定に特有の特性又は要素を考慮する。<br>※ 使用されることが意図される特定の地理的、文脈的、行動的又は機能的設定を反映したデータに基づいて学習及びテストされたハイリスクAIシステムは、本要件に適合するものと推定される。 |

# ハイリスクAIシステムが満たすべき要件②（第8条～第15条）

| 要件 | 内容 |
|---|---|
| **技術文書** | **技術文書を上市前に作成し、最新に維持**すること。<br>➢ ハイリスクAIシステムが満たすべき要件を満たしていることを証明し、当局及び適合性評価機関が要件遵守の評価を行うために必要な情報を提供するような文書。<br>➢ 少なくとも**Annex IVの内容**を含む。<br>➢ ハイリスクAI第1カテゴリ（他法令の規制対象）の場合、当該**他法令で求められている内容を含む単一の技術文書**とする。 |
| **記録保存** | システムの耐用期間を通じて**自動でログを記録する機能**を備えること。 |
| **透明性及び導入者への情報提供** | ■ 導入者がAIシステムの**アウトプットを解釈して適切に利用できるよう、透明性を確保すること**。<br>■ 導入者に関連し、アクセス可能で理解可能な、**簡潔、完全、正確かつ明確な情報が含まれる使用説明書を添付すること**。具体的には以下の情報を含める。<br>➢ **提供者の身元及び連絡先**<br>➢ **AIシステムの特徴、能力及び性能の限界**<br>・本来の用途<br>・正確性、堅牢性及びサイバーセキュリティのレベル<br>・健康及び安全又は基本的権利に対するリスクにつながる可能性がある状況<br>・データセットに関する情報など<br>➢ 初回適合性評価時点から予定されていた性能の変更<br>➢ **人的監視措置**<br>➢ **必要な計算・ハードウェア資源、想定寿命**及び適切な機能を確保するために必要な**保守・ケア措置** |

# ハイリスクAIシステムが満たすべき要件③（第8条～第15条）

| 要件 | 内容 |
| --- | --- |
| 人的監視措置 | ■ **適切な人間・機械間インターフェース**を含め、AIシステムが使用されている期間中、**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。<br>■ 人間による監視措置は、**AIシステムのリスク、自律性のレベル及び使用の状況に見合ったもの**でなければならず、**次のいずれか又は両方**を通じて確保する。<br>➢ 上市前又は稼働前に、**提供者が特定しAIシステムに組み込む措置**。<br>➢ AIシステムの上市前又は稼働前に**提供者が特定した措置**であって、**導入者が実施**することが適切なもの。<br>■ ハイリスクAIシステムは、**監視業務要員が以下を行うことを可能とする**態様で導入者に提供されなければならない。<br>➢ **異常、機能不全及び予想外の性能の兆候を検知し対処する**目的で、AIシステムの能力及び限界を十分に理解し、その動作を適切に監視すること。<br>➢ AIシステムによって生成されるアウトプットに自動的に依存し又は過度に依存する傾向（**「自動化バイアス」）の可能性について認識すること。**<br>➢ AIシステムの**アウトプットを正しく解釈すること。**<br>➢ 特定の状況において、**AIシステムを使用しないこと、又はAIシステムの出力を無視、上書き若しくは反転させる**ことを決定すること。<br>➢ AIシステムの動作に介入すること又は**「停止」ボタン**若しくは類似の手順でシステムを中断し、安全な状態で停止させること。 |

# ハイリスクAIシステムが満たすべき要件④（第8条～第15条）

| 要件 | 内容 |
|---|---|
| **正確性、堅牢性、サイバーセキュリティー**<br><br>※サイバーセキュリティ法に基づく認証スキーム（が今後できた場合）の下で認証を受けたハイリスクAIシステムは、本条に定めるサイバーセキュリティ要件に適合するものと推定される。 | ■ **適切なレベルの正確性、堅牢性、サイバーセキュリティを達成し、ライフサイクルを通じて一貫した性能を発揮する**ように設計・開発すること。<br>■ 欧州委員会は、利害関係者及び計量・ベンチマーク当局などの組織と協力して、ベンチマークや計測方法の開発を奨励しなければならない。<br>■ AIシステムの**正確性レベル及び関連する指標は、添付の使用説明書に明記する**。<br>■ 発生する可能性のある**エラー、障害又は不整合に関して強靭**でなければならない。<br>■ 堅牢性は、**バックアップ又はフェイルセーフプランを含む技術的な冗長性ソリューション**によって達成することができる。<br>■ **上市後又は稼働後も学習を続けるAIシステム**は、偏ったアウトプットが将来の運用のためのインプットに影響を及ぼす可能性（「**フィードバックループ**」）**を可能な限り除去又は低減する**ように、かつ、フィードバックループが**適切な緩和措置によって適切に対処される**ように、開発されなければならない。<br>■ ハイリスクAIシステムは、**システムの脆弱性を悪用**することによってその用途、アウトプット、性能を変更しようとする第三者による試みに対して**強靭でなければならない**。<br>■ AI特有の脆弱性に対処するための技術的解決策には、必要に応じて、**以下の攻撃を防止、検知、対応、解決及び制御するための措置**を含まなければならない。<br>i. 学習データセットを操作しようとする攻撃（「**データポイズニング**」）<br>ii. 学習に使用される学習済みコンポーネントを操作しようとする攻撃（「**モデルポイズニング**」）<br>iii. AIモデルに誤りを犯させるように設計されたインプット（「**敵対的事例**」又は「**モデル回避**」）<br>**iv. 機密性攻撃**<br>**v. モデルの欠陥** |

# ハイリスクAIシステムの適合性評価手続（第40条～第44条）

**【前提】**
- 本法が定める要件をカバーする**欧州標準に適合しているハイリスクAIシステム及び汎用AIモデルは、本法が定める要件に適合していると推定**される。
- 欧州標準の不存在等の場合、欧州委員会は共通仕様を策定可能。本法が定める要件をカバーする**共通仕様に適合しているハイリスクAIシステム及び汎用AIモデルは、本法が定める要件に適合していると推定**される。

| 対象AIシステム | 適合性評価手続 |
|---|---|
| **生体認証**（遠隔生体認証システム、機微な特徴や属性に基づく生体分類、感情認識） | ■ 欧州標準又は共通仕様を**適用している**場合　→　以下の**いずれか**。<br>・Annex VIに基づく**自己評価**<br>・Annex VIIに基づく**適合性評価機関による第三者認証**<br>■ 欧州標準も共通仕様も**適用していない**場合（不存在の場合も含む）<br>→　Annex VIIに基づく**適合性評価機関による第三者認証**。 |
| **ハイリスクAI（第1カテゴリ）**（他の法令の対象） | ■ **当該他の法令の規定に従って実施** |
| **その他** | ■ Annex VIに基づく**自己評価**<br>**※欧州委員会が委任法令で第三者認証必須に変更することが可能。** |

※ハイリスクAIシステムが**大幅に変更された場合は、新たな適合性評価手続の実施**が必要。

※上市後又は稼働後も学習を続けるハイリスクAIシステムについて、最初の適合性評価の時点で提供者が事前に決定していた変更であって技術文書に含まれるものは、「大幅な変更」とはならない。（＝**これ以外の場合は、学習の結果大幅な変更があった場合も、新たな適合性評価手続の実施が必要**。）

※適合証明書の**有効期間は①第1カテゴリ**（他の法令の対象）については**最長5年、②第2カテゴリ**（Annex III）については**最長4年**。更新には適合性評価手続と同様の再査定が必要。

# 市販後モニタリングシステム(第72条)

- ハイリスクAIシステム提供者は、市販後モニタリングシステムを確立・文書化しなければならない。
- ハイリスクAIシステムの性能について、その耐用期間を通じて、**導入者から提供される又は他の情報源を通じて収集される関連データを積極的かつ体系的に収集、文書化、分析**する。
- 提供者が、**AIシステムが本法の定める要件に継続的に適合していることを評価**するためのもの。

＜関連規定＞

- 市販後モニタリングシステムは、**市販後モニタリング計画**に基づいて実施。市販後モニタリング計画は、**技術文書の一部**を構成。
- **欧州委員会は、市販後モニタリング計画のテンプレート及び盛り込まれるべき要素を定める実施法令を、本規則施行後18か月以内に策定**。
- 第1カテゴリのハイリスクAIシステム(他の法令の対象)で、当該他の法令に基づき既に市販後モニタリングシステム・市販後モニタリング計画が策定済みのものについては、当該システム・計画に本規則に基づく市販後モニタリングの要素を統合する。

# 市場監視当局への報告義務(第73条)

- ハイリスクAIシステム提供者は、**重大インシデントが発生した場合**、当該インシデントが発生した**加盟国の市場監視当局に報告しなければならない**。

**「重大インシデント」(serious incident)の定義:**
以下のいずれかに直接的又は間接的につながるAIシステムのインシデント又は誤動作をいう。
(a) 人の死亡、または人の健康への重大な危害
(b) 重要インフラの管理または運用の重大かつ不可逆的な中断
(c) 基本的権利の保護を目的とする連邦法に基づく義務の侵害
(d) 財産または環境に対する重大な損害

| 分類 | 報告期限 |
|---|---|
| **原則** | 提供者がAIシステムと重大インシデントとの間の**因果関係又はその合理的な蓋然性を立証した後直ちに**、かつ、いかなる場合においても、提供者又は導入者が重大インシデントを**認識した後15日以内** |
| **広範な侵害インシデント(b)** | 提供者又は導入者が当該インシデントを**認識した後直ちに、遅くとも2日以内** |
| **人が死亡** | 提供者又は導入者が、ハイリスクAIシステムと重大な事故との**因果関係を立証した後又はその疑いが生じた後直ちに、**ただし、**遅くとも提供者又は導入者が重大インシデントを知った日から10日以内** |

- まず不完全な最初の報告書を提出し、その後完全な報告書を提出することが可能。
- 報告後、提供者は、遅滞なく、当該重大インシデント及び当該AIシステムに関連して**必要な調査(インシデントのリスク評価と是正措置を含む)を行わなければならない**。
- 欧州委員会は、本規則施行後12か月以内に、本報告義務に関するガイダンスを策定する。
- 市場監視当局は、報告の受領後7日以内に適切な措置を講じる。

# ハイリスクAIシステム輸入者及び販売業者の義務（第23条、第24条）

## 輸入者の義務

1. ハイリスクAIシステムを市場に投入する前に、**以下を確認しなければならない**。
   ・提供者が適切な**適合性評価手続**を実施していること。
   ・提供者が**技術文書**を作成していること。
   ・**CEマーク、EU適合性宣言及び使用説明書**が添付されていること。
   ・提供者の**域内代理人**が指名されていること。
2. ハイリスクAIシステムが**本規則に適合していない、偽造されている、又は偽造文書が添付されていると考える十分な理由がある場合、当該AIシステムを市場に出してはならない**。
3. **輸入者の名称、登録商号又は登録商標及び連絡可能な住所**を表示しなければならない。
4. ハイリスクAIシステムの上市後又は稼働後**10年間、適合性証明書、使用説明書及びEU適合性宣言のコピーを保管**しなければならない。

## 販売業者の義務

1. ハイリスクAIシステムを市販する前に、**以下を確認しなければならない**。
   ・**CEマーク、EU適合性宣言及び使用説明書**が添付されていること。
   ・**提供者が名称等の表示義務及び品質管理システム策定義務を遵守していること。**
   ・**輸入者が名称等の表示義務を遵守している**こと。
2. ハイリスクAIシステムが**本規則に適合していないと考える場合、当該システムを市販してはならない**。
3. 市販したハイリスクAI システムが本規則に適合していないと考える販売業者は、**必要な是正措置を講じ、撤回し、若しくはリコールし、又は提供者、輸入者若しくは関係事業者が是正措置を講じることを確保しなければならない。**

# ハイリスクAIシステム導入者の義務（第26条）

1. **使用説明書に従って使用する**ことを確保するための技術的及び組織的措置を講じること。
2. 必要な能力、訓練、権限、必要な支援を有する自然人に**人的監視をアサイン**すること。
3. **AIシステムの本来の用途に照らしてインプットデータの関連性と十分な代表性を確保**すること。
4. 使用説明書に沿ってAIシステムの**動作を監視**すること。
5. AIシステムが**健康、安全又は基本的人権に関するリスクをもたらす可能性**があると考える理由がある場合、**提供者又は販売業者及び市場監視当局に通知し、当該AIシステムの使用を停止**すること。
6. **重大なインシデント**を発見した場合には、その旨を**まず提供者、次いで輸入者又は販売業者及び市場監視当局に通知する**こと。
7. 自動的に生成する**ログを保管**すること。
   ・保存期間は本体の用途に照らして適切な期間、**少なくとも6か月間**。
8. **職場でハイリスク AI システムを稼働又は使用する前に**、雇用者である導入者は、ハイリスク AI システムの使用の対象となることを、**労働者代表及び影響を受ける労働者に通知**すること。
9. 導入者が公的機関の場合のみ：事前登録義務あり。
10. 犯罪の容疑者又は有罪判決を受けた者に的を絞った捜索を行う枠組みの下で、ハイリスク事後遠隔生体認証AIシステムの導入者のみ：事前又は遅くとも事後48時間以内に遅滞なく、司法当局又はその決定が拘束力を有し司法に服する行政当局の許可を求めること。
11. **自然人に関する意思決定を行う又は意思決定を支援するハイリスクAI第2カテゴリ（Annex III）**の導入者のみ：ハイリスクAIシステムの使用の対象であることを当該**自然人に通知する**こと。

# 基本的権利影響評価(第27条)

- **Annex III記載のハイリスクAIシステムの導入者**は、導入前に、当該AIシステムの利用が生み出す可能性のある**基本的権利への影響を評価しなければならない。**
  **ただし、以下のハイリスクAIシステムや導入者は除く。**

| | | | |
|---|---|---|---|
| 1 | 重要インフラで使用されるハイリスクAIシステム | 4 | クレジットスコア評価 |
| 2 | 公法に準拠する組織 | 5 | 生命保険・健康保険におけるリスク評価・価格決定 |
| 3 | 公共サービスを提供する民間団体 | | |

- **基本的権利影響評価は以下で構成される。**

| | | | |
|---|---|---|---|
| 1 | ハイリスクAIシステムがその**本来の用途に沿って使用される導入者のプロセス**の説明 | 4 | 3で特定されたカテゴリーに影響を及ぼすと見込まれる**具体的な危害のリスク**。提供者により提供される情報を考慮する。 |
| 2 | ハイリスクAIシステムが使用される**期間と頻度**の説明 | 5 | 使用説明書に沿った**人的監視措置**の実施の説明 |
| 3 | 特定の文脈での使用によって**影響を受ける可能性のある自然人および集団のカテゴリー** | 6 | これらの**リスクが顕在化した場合に講じる措置**(内部ガバナンスや苦情メカニズムを含む) |

- 影響評価は、ハイリスクAIシステムの**最初の導入に適用**される。**類似のケースでは、実施済みの評価に依拠することが可能**。使用中に上記要素に変更があった又は最新でなくなったと考える場合、導入者は情報をアップデートしなければならない。
- 基本的権利影響評価を実施後、**市場監視当局にその結果を通知**しなければならない。
- AIオフィスは質問票のテンプレートを作成する。

# AIバリューチェーンにおける責任(第25条)

## 「提供者」とみなされるケース

- **販売業者、輸入者、導入者又はその他の第三者であっても、以下のいずれかに該当する場合、ハイリスクAIシステムの「提供者」とみなされ、提供者の義務が適用される。**この場合、当初当該AIシステムを上市又は稼働させた提供者は提供者ではなくなる。
  - i. 上市済み又は稼働済みのハイリスクAIシステムに**自己の名称や商標を付す**場合。ただし、義務を他の方法で割り当てる契約には影響しない。
  - ii. 上市済み又は稼働済みのハイリスクAIシステムに**大幅な変更を加える**場合。
  - iii. 上市済み又は稼働済みで**ハイリスクAIシステムと分類されていないAIシステム(汎用AIシステムを含む)がハイリスクAIシステムとなる**ような方法で当該AIシステムの**本来の用途を変更する**場合。
- この場合、**当初の提供者は新たな提供者が本規則を遵守するために必要な協力及び情報を提供しなければならない**。ただし、**最初の提供者がAIシステムをハイリスクAIシステムに変更してはならないことを明確に規定している場合はこの限りではない**。
- **第1カテゴリのハイリスクAI(他法令の対象)であって製品の安全コンポーネント**であるものについては、**以下のいずれかの場合、製品の製造業者**(manufacturer)**がハイリスクAIシステムの提供者とみなされる**。
  - i. ハイリスクAIシステムが**製造業者の名称又は商標の下で市場に投入**される場合。
  - ii. ハイリスクAIシステムが、市場投入後、**製造業者の名称又は商標の下で稼働**される場合。

## 提供者とサプライヤーの協力

- **ハイリスクAIシステムの提供者**とハイリスクAIシステムにおいて使用され又は統合される**AIシステム、ツール、サービス、コンポーネント又はプロセスを提供する第三者**は、ハイリスクAIシステムの提供者が本規則に定める義務を完全に遵守することができるよう、**必要な情報、能力、技術的アクセス及びその他の支援を書面による合意により規定する**ものとする。
  - ➢ ただし、**無償かつオープンソースのライセンス**に基づき、ツール、サービス、プロセス又はコンポーネント(**汎用AIモデルを除く**)を**一般に公開する第三者は適用除外**。
  - ➢ AIオフィスは**モデル契約条項**を開発・推奨する。

# 透明性義務（限定的なリスク、汎用AIモデル）①（第50条）

| 対象AIシステム | 対象者 | 義務 |
|---|---|---|
| **自然人と直接やり取りするAIシステム** | 提供者 | ■ **自然人がAIシステムとやり取りしていることを認識できるように設計・開発**すること。<br>※使用の状況や文脈を考慮し、合理的に十分な知識を持ち、観察力と思慮深さを備えた自然人から見て**明らかな場合を除く**。 |
| **合成音声、画像、動画又はテキストコンテンツを生成するAIシステム**（汎用AIシステムを含む） | 提供者 | ■ AIシステムの**アウトプットが人為的に生成又は操作されたものであると機械可読形式でマークされ検知可能**であることを確保すること。<br>■ 技術的に可能な限り、その技術的ソリューションが**効果的で、相互運用性があり、堅牢で信頼できるもの**であることを確保するすること。<br>※以下のAIシステムには**適用されない**。<br>➢ 標準的な編集のための補助機能を実行する場合。<br>➢ 導入者によって提供された入力データ若しくはそのセマンティクスを実質的に変更しない場合。<br>➢ 犯罪の検知、防止、捜査若しくは訴追のために法律で認められている場合。 |
| **感情認識システム・生体分類システム** | 導入者 | ■ **対象者にそのシステムの運用について通知する**こと。<br>※第三者の権利と自由のための適切な保護措置が講じられている場合、犯罪の検知、防止、捜査のために法律で認められているものには**適用されない**。 |

# 透明性義務（限定的なリスク、汎用AIモデル）②（第50条）

| 対象AIシステム | 対象者 | 義務 |
|---|---|---|
| ディープフェイク生成AIシステム | 導入者 | ■ コンテンツが人為的に生成又は操作されたものであることを開示すること。<br>➢ コンテンツが明らかに芸術的、創作的、風刺的、フィクション的又は類似の作品又は番組の一部を形成する場合、作品の表示又は享受を妨げない適切な方法で、そのような生成又は操作されたコンテンツの存在を開示することのみで足りる。<br>※犯罪の検知、防止、捜査若しくは訴追のために法律で認められている場合には適用されない。 |
| 公共の関心事について公衆に知らせる目的で公表されるテキストを生成または操作するAIシステム | 導入者 | ■ 当該テキストが人為的に生成又は操作されたものであることを開示すること。<br>※以下の場合には適用されない。<br>➢ 犯罪の検知、防止、捜査若しくは訴追のために法律で認められている場合。<br>➢ AIが生成したコンテンツが、人によるレビュー又は編集管理のプロセスを経ており、自然人又は法人がコンテンツの公表について編集責任を有する場合。 |

■ 開示される情報は、遅くとも最初のやり取りの時点で、明確かつ区別可能な方法で、当事者に提供されなければならない。

■ AIオフィスは、人為的に生成又は操作されたコンテンツの検知及びラベリングに関する義務の効果的な実施を促進するため、EUレベルでの実践規範の作成を奨励し、促進する。

# 汎用AIモデルの提供者の義務（第53条、第54条）

1. **学習及びテストの過程並びに評価結果を含むモデルの技術文書を作成し、最新の状態に維持する**こと。少なくとも**Annex XI規定の情報**を含む。AIオフィス及び加盟国当局からの要請に応じて提供する。
2. 汎用AIモデルを組み込むことを意図する**AIシステムの提供者に対して、情報及び文書を作成し、最新の状態に保ち、利用可能にする**こと。ただし、知的財産権、業務上の機密情報又は営業秘密を遵守し保護する必要性を損なうものではない。**情報及び文書は以下の両方を満たす**ものでなければならない。
   ・AIシステムの**提供者が、汎用AIモデルの能力と限界を十分に理解し、本規則に基づく義務を遵守できるようにする**こと。
   ・少なくとも**Annex XII規定の要素**を含むこと。
3. EU域外国の提供者のみ：**域内代理人を指名**すること。

| | |
|---|---|
| 例外 | **上記1.～3.の義務**は、モデルへのアクセス、使用、修正及び配布を認める**無償のオープンソースライセンスの下でリリースされ、重み、モデル構造に関する情報及びモデルの使用に関する情報を含むパラメータが一般に公開されているAIモデル**の提供者には**適用されない**。 |
| 例外の例外 | ただし、この例外は、**システミック・リスクを有する汎用AIモデルには適用されない**。 |

4. **著作権及び関連する権利に関するEU法を遵守**し、特に、デジタル単一市場著作権指令（2019/790）第4条第3項に従って表明された権利の留保（**テキストマイニング及びデータマイニングに対する権利制限への留保）を特定し、最先端技術を含めて遵守するためのポリシーを導入する**こと。
5. AIオフィスが提供するテンプレートに従って、**汎用AIモデルの学習に使用したコンテンツに関する十分に詳細な要約を作成し、一般に公開する**こと。

- 本法が定める要件をカバーする**欧州標準に適合している汎用AIモデルは、本法が定める要件に適合していると推定**される。
- 欧州標準策定までの間、提供者は、**義務の遵守を証明するために実践規範**（code of practice）**に依拠する**ことができる。

# システミックリスクを有する汎用AIモデル（第51条、第52条）

## システミックリスクを有する汎用AIモデルとは

- **以下のいずれかの条件**を満たす汎用AIモデルは**システミックリスクを有する汎用AIモデル**として分類される。
  - i. 指標やベンチマークを含む適切な技術的ツールや方法論に基づいて評価された**高い影響力**（high impact capabilities）**を有する**こと。
    ※学習に使用された**累積計算量を浮動小数点演算（FLOP）で計測した値が10^25より大きい場合、「高い影響力」を有すると推定**される。
  - ii. 職権で又は科学パネルからの適格な警告に従い、欧州委員会の決定に基づき、**Annex XIIIに定める基準**に照らして、**上記i.と同等の能力又は影響を有する**こと。
- 欧州委員会は、上記規定の閾値を修正するための委任法令並びにベンチマーク及び指標を補足するための委任法令を策定する。

## 指定手続

- **汎用AIモデルが「高い影響力」の条件を満たす場合、提供者は**、当該要件が満たされた後又は満たされることが判明した後、**遅滞なく、遅くとも2週間以内に欧州委員会に届け出なければならない**。汎用AIモデルがシステミックリスクを有していることを知った欧州委員会が当該モデルを指定することも可能。
  - 提供者は、その届出とともに、その汎用AIモデルが、その特性により、**システミックリスクを呈さず、したがってシステミックリスクを有する汎用AIモデルとして分類されるべきではないことを実証するための十分な裏付けのある論拠を提示することができる**。
- 欧州委員会は、**Annex XIIIに定める基準に基づいて、職権で又は科学パネルからの適格な警告に基づき、汎用AIモデルをシステミックリスクを有するものとして指定**することができる。
  - 指定から**6か月以上経過後**、提供者は、欧州委員会に対し、指定決定以降に生じた客観的かつ詳細で新たな理由を添えて、汎用AIモデルがシステミックリスクを有するかどうかの**再評価を要請可能**。
- 欧州委員会は、**システミックリスクを有する汎用AIモデルのリストが公表・更新**されることを確保する。

# システミックリスクを有する汎用AIモデルの提供者の義務（第55条、第56条）

## システミックリスクを有する汎用AIモデルの提供者の義務

汎用AIモデルの提供者の義務に**加えて以下の義務が適用**される。

1. システミックリスクの特定と軽減を目的としたモデルの敵対的テストの実施と文書化を含む、最新技術を反映した標準化されたプロトコルとツールに従って、**モデル評価(model evaluation)を実施する**こと。
2. システミックリスクを有する汎用AIモデルの開発、市場投入、使用から生じる可能性のある**EUレベルのシステミックリスクを、その発生源を含め、評価・軽減する**。
3. AIオフィス及び加盟国当局に対し、**重大インシデント及びそれに対処するための可能な是正措置に関する関連情報を、遅滞なく記録、文書化し、報告する**こと。
4. システミックリスクを有する汎用AIモデルとその物理インフラに対する**適切なレベルのサイバーセキュリティ保護を確保する**。

（参考）汎用AIモデル提供者の義務一覧

| 汎用AIモデル一般 | システミックリスクを有する汎用AIモデル |
|---|---|
| ➢ 技術文書の作成及び更新<br>➢ 汎用AIモデルをAIシステムに統合する提供者向けの情報・文書の作成、更新及び提供<br>➢ 著作権法を遵守するためのポリシーの実行<br>➢ 汎用AIモデルの学習に使用したコンテンツに関する十分に詳細な要約の作成及び公開<br>➢ 域内代理人の指名 | （左記に加えて）<br>➢ モデル評価の実施<br>➢ EUレベルでのシステミックリスクの評価及び軽減<br>➢ 深刻なインシデント及びそれに対する是正措置のAIオフィスへの報告<br>➢ 適切なレベルのサイバーセキュリティ保護 |

# 汎用AIモデルに関する実践規範（第56条）

- **AIオフィスは**、国際的なアプローチを考慮しつつ、本規則の適切な適用に寄与するため、EUレベルでの**実践規範（codes of practice）の作成を奨励し、促進する**。実践規範は、少なくとも**汎用AIモデル関連の義務をカバーし、以下を含める**。
  - i. 汎用AIモデル提供者が作成すべき**技術文書及びAIシステム提供者向け情報**を、市場及び技術の発展に照らして**常に最新のものとするための手段**。
  - ii. **学習に使用されたコンテンツに関する要約の詳細さの適切なレベル**。
  - iii. その発生源を含め、EUレベルでの**システミックリスクの種類と性質**の特定。
  - iv. EUレベルの**システミックリスクの評価及び管理のための措置、手続及び形式**（その文書化を含む）。
- **AIオフィスは、全ての汎用AIモデル提供者及び関連する加盟国当局に対し、実践規範の作成に参加するよう要請する**ことができる。市民社会組織、産業界、学界並びに川下提供者や独立専門家などの他の関連利害関係者は、このプロセスを支援することができる。
- AIオフィスは、**実践規範への参加者が、コミットメントの実施、講じられた措置及びその結果について、KPIに対する測定結果も含め、AIオフィスに定期的に報告する**ことを確保することを目指す。KPI及び報告のコミットメントは、参加者間の規模及び能力の違いを反映する。
- **AIオフィス及び欧州AI委員会は、**参加者による実践規範の目的の達成及び本規則の適切な適用への貢献を**定期的に監視及び評価する**。
- **欧州委員会は、実施法令の形で、実践規範を承認**し、それを域内で一般的に有効とすることができる。
- **AIオフィスは、全ての汎用AIモデル提供者に対し、実践規範を遵守するよう求める**ことができる。
- **実践規範は、遅くとも本規則施行日から9か月までに作成されなければならない**。もし12か月以内に実践規範が完成しない場合又はAIオフィスが適切でないと断した場合、欧州委員会は、実施法令の形で、汎用AIモデル関連の義務の実施に関する共通のルールを定めることができる。

# AI規制サンドボックス①(第57条～第59条)

## AI規制サンドボックスとは

- AIシステムの市場投入・稼働前の限られた期間、革新的なAIシステムの**開発、学習、試験、検証を容易にする管理された環境を提供する**もの。
- **EU加盟国の当局により、各国に少なくとも一つ設置**(他の加盟国と共同設置も可。また、EU機関向けには欧州データ保護監督機関(EDPS)により設置)。本規則の施行日から**24か月以内に運用を開始**する。
- サンドボックス内では、本規則及び関連法に関する**当局による指導を受け、サンドボックス内での活動結果に関する報告書を当局から受領可能**。また、法定の条件を満たせば、**他の利用目的のために収集した個人データを、革新的なAIシステム開発・試験目的に利用可能**。

## 当局の役割

- **当局は**、特に基本的権利、安全衛生、試験、リスク軽減措置並びに本規則の義務及び要件、関連する他のEU法及び国内法との関連におけるそれらの有効性に対するリスクを特定することを目的として、**AI規制サンドボックス内で指導、監督及び支援を提供**する。AIシステムが**個人データの処理を伴う場合、加盟国は、データ保護当局の関与を確保する**。
- 当局は、参加者に対し、規制上の期待並びに本規則に定める要件及び義務の履行方法に関するガイダンスを提供する。提供者の要請に応じて、**当局は、①サンドボックスで成功裏に実施された活動の証明書と②サンドボックスにおいて実施された活動、関連する結果及び学習成果を詳述した終了報告書を提供する。参加者は、適合性評価手続又は関連する市場監視活動を通じて本規則に準拠していることを証明するために、これらの文書を使用することができる。**
- AIオフィスは**AI規制サンドボックスのリストを公表**・更新する。欧州委員会は、関係者がAI規制サンドボックスとやり取りできるよう、**全ての関連情報を含む単一の専用インターフェースを開発**する。
- **当局は毎年1回、年次報告書**をAIオフィスに提出し、公表する。

# AI規制サンドボックス②(第57条～第59条)

## 参加者の責任

- AIシステムの**開発及び試験中に特定された、健康、安全、基本的権利に対する重大なリスクには、適切な軽減策を講じる**。当局は、軽減策が不可能な場合に一時的又は恒久的に試験プロセス又はサンドボックスへの参加を停止する権限を有する。
- 参加者は、サンドボックス内で行われた実験の結果、**第三者に与えた損害について責任を負う**。ただし、**提供予定者が具体的な計画及び参加条件を遵守し、当局の指導に誠実に従っていた場合、本規則の違反に対して当局が制裁金を課すことはない**。また、他のEU法及び国内法を管轄する当局が、サンドボックス内のAIシステムの監督に積極的に関与し、遵守のためのガイダンスを提供していた場合、当該法に関して制裁金が課されることはない。

## 細則

- **欧州委員会は、AI規制のサンドボックスの設置、開発、実施、運用、監督に関する詳細な取決めを規定する実施法令を採択する**。実施法令は、**以下の論点に関する共通原則を含む**ものとする。
  - i. AI規制サンドボックスへの**参加資格と選考基準**
  - ii. サンドボックス計画及び終了報告書を含む、AI規制サンドボックスの**申請、参加、監視、退出及び終了の手順**
  - iii. 参加者に適用される**規約**
- 上記実施法令は、**選考基準が透明かつ公正**であること、**申請から3か月以内に当局の決**定が行われること、中**小企業とスタートアップについては無料**とすること、中小企業やスタートアップにとってもわかりやすいシンプルな手続とすること等の要件を満たすものとする。

# AI規制サンドボックス③(第57条～第59条)

## 個人データの目的外利用

■ AI規制サンドボックスでは、**以下の条件を全て満たす場合、他の目的で合法的に収集された個人データを、サンドボックス内で特定のAIシステムを開発、学習、テストする目的で処理することができる**。

**【対象：以下のいずれかの分野で、大きな公共の利益の保護のために開発されるAIシステム】**

| | | | |
|---|---|---|---|
| 1 | 疾病の発見、診断、予防、管理、治療、医療システムの改善を含む公共の安全と公衆衛生 | 4 | 交通システム、モビリティ、重要インフラ及びネットワークの安全性と強靭性 |
| 2 | 高水準の環境保護と質の向上、生物多様性の保護、汚染からの保護、グリーン移行措置、気候変動の緩和と適応対策 | 5 | 行政及び公共サービスの効率性と質 |
| 3 | エネルギー持続可能性 | | |

i. 処理されるデータが、**ハイリスクAIシステムに対する本規則の要件に準拠するために必要**であり、**匿名化データ、合成データ又はその他の非個人データでは効果的に満たすことができない**こと。
ii. データ主体の権利と自由に対する高いリスクがサンドボックス実験中に発生する可能性があるかどうかを特定するための**効果的な監視メカニズム**、及びそれらのリスクを速やかに軽減し、必要に応じて処理を停止する**対応メカニズム**が存在すること。
iii. 個人データが、提供予定者の管理下で、**機能的に分離され、隔離され、保護されたデータ処理環境**にあり、**権限を与えられた者のみがこれらのデータにアクセス**できること。
iv. 個人データの共有はEUデータ保護法に従って行うこと。**サンドボックス内で作成された個人データは、サンドボックス外で共有することはできない**。
v. 個人データの処理が、**データ主体に影響を及ぼす措置や決定をもたらすものではなく**、EUデータ保護法に規定された権利の適用に影響を及ぼすものでもないこと。
vi. 個人データが、**適切な技術的及び組織的手段によって保護**され、サンドボックスへの参加が終了する又は個人データの保持期間が終了した時点で**削除される**こと。
vii. 個人データの処理に関する**ログをサンドボックスへの参加期間中保存**すること。
viii. AIシステムの学習、試験及び検証の**プロセス及び背景理論に関する完全かつ詳細な説明**が、試験結果とともに技術文書の一部として保管されること。
ix. サンドボックスで開発された**AIプロジェクト、その目的、期待される結果の簡単な概要が、当局のウェブサイトで公表**されること。

# 中小企業・スタートアップ支援措置（第62条）

## 加盟国が講じる措置

- 参加資格と選考基準を満たす限りにおいて、EU域内に登録されたオフィスや支社を有する中小企業（スタートアップを含む）に対し、**AI規制サンドボックスへの優先的なアクセスを提供する**。
- 中小企業（スタートアップ、導入者、地方公共団体を含む）のニーズに合わせて、**本規則の適用に関する具体的な啓発・研修活動を実施する** 。
- 中小企業（スタートアップ、導入者、その他のイノベーター、地方公共団体を含む）とのコミュニケーションのために、既存の専用チャネルを活用し又は新たなチャネルを確立し、**本規則の実施に関する助言の提供及び問合せ対応を行う。**
- **標準化開発プロセスへの中小企業及びその他の利害関係者の参加を促進する。**

## AIオフィスが講じる措置

- 本規則でカバーされている分野に関する**標準テンプレートを提供する**。
- EU域内の全事業者向けに本規則に関連した使いやすい情報を提供する**単一の情報プラットフォームを開発・維持する**。
- 本規則の義務について認識を高めるため、適切な**コミュニケーションキャンペーンを実施する**。
- **AIシステムに関連する公共調達手続のベストプラクティス**の収れんを評価・促進する。

## その他

- **適合性評価の手数料**を設定する際には、中小企業（スタートアップを含む）の利益及びニーズを考慮し、その手数料を**企業規模、市場規模及びその他の関連指標に比例して減額**しなければならない。

# ガバナンス（第64条～第70条）

## 欧州委員会

**AIオフィス**

助言・支援

事務局機能

諮問

## 欧州AI委員会

（EAIB：European Artificial Intelligence Board）

**市場監視SG**
（市場監視当局）

**適合性評価SG**
（適合性評価機関指定当局）

**・本法の適用・執行（汎用AIモデルのみ）**
**・下位法令・ガイドラインの策定**

助言

### 科学パネル
（Scientific Panel of Independent Experts）

・AI分野の最新の科学的知見を有する、AIシステム提供者から独立した専門家で構成
・汎用AIに係る本規則の執行に関してAIオフィスに助言・支援
・要請に応じて加盟国の執行活動への協力

### アドバイザリーフォーラム
（Advisory Forum）

・欧州委・EAIBへの専門的知見の提供・助言
・産業界、スタートアップ、中小企業、市民団体及びアカデミアで構成
・欧州基本権機関、ENISA、CEN / CENELEC、ETSIも参加

| | |
|---|---|
| 構成 | ・加盟国当局（うち1国が議長）<br>・オブザーバ：EDPS<br>・事務局：AIオフィス（投票権なし） |
| 主な業務 | ・加盟国当局間の調整、統一的な行政執行への貢献、執行に関する助言・支援<br>・技術的・規制的専門性やベストプラクティスの収集・共有<br>・意見・勧告（行動規範、実践規範、ガイドライン、本規則の見直し、欧州標準、共通仕様等関連）<br>・国際関係に関する欧州委への助言 |

監督

協力

参加

助言・支援

## EU加盟国当局

（対EU機関の当局は欧州データ保護監督機関（EDPS））

**・本法の適用・執行（汎用AIモデルを除く）**
・適合性証明機関と市場監視当局（本規則施行後12か月以内に指名・公表）

監督

## 事業者

# 執行①（第74条、第75条、第79条、第82条、第85条、第86条）

## 市場監視

- 市場監視規則（Regulation (EU) 2019/1020）をAIシステムにも適用。
  ・EU域内代理人の設置義務、市場監視当局への協力義務等。
  ・市場監視当局へ**資料・情報提出命令、立入検査、是正措置命令（リコール含む）等の権限**を付与。
- **AIシステムが汎用AIモデルに基づいており、当該モデルと当該システムが同一の提供者によって開発されている場合**、当該AIシステムを監視及び監督する**権限はAIオフィスが有する**。
- 市場監視当局は、**AIシステムがリスクをもたらしていると考える十分な理由を有する場合**、当該AIシステムについて、本規則の**要件及び義務の遵守に関する評価を実施しなければならない**。
- AIシステムが本規則の**要件及び義務を遵守していない**と認められる場合、市場監視当局は、関係事業者に対し、当局が定める期間内、**遅くとも15営業日以内**又は関連法令が定める期間内のいずれか短い期間内に、遵守するために全ての適切な**是正措置をとる**こと、当該AIシステムを市場から**撤去する**こと又はAIシステムを**リコールする**ことを遅滞なく要求しなければならない。
- 事業者が期間内に**適切な是正措置を講じない場合、市場監視当局は、あらゆる適切な暫定措置を講じなければならない**。当局は、遅滞なく、当該措置を欧州委員会及び他の加盟国に通知する。
- 市場監視当局は、ハイリスクAIシステムが**本規則を遵守しているにもかかわらず、人の健康、安全、基本的権利又はその他の公益保護の側面に対するリスクをもたらしている**と認める場合、関係事業者に対し、当該リスクをもたらさないことを確保するための**適切な措置を講じるよう求める**。

# 執行②（第74条、第75条、第79条、第82条、第85条、第86条）

## 当局によるアクセス

- 市場監視当局は、API等を通じて、提供者が使用する学習、検証及び試験の**データセットへの完全なアクセス**を認められる。
- ハイリスクAIシステムの本規則が定める要件への適合性を評価するために必要であり、試験又は監査手続並びに提供者から提供されたデータ及び文書に基づく検証を実施し尽くした又は不十分であることが判明した場合、市場監視当局は、当該システムの**ソースコードへのアクセス**を認められる。
- 市場監視当局が汎用AIモデルに関連する特定の情報にアクセスできないためにハイリスクAIシステムに関する調査を完了できない場合、当該当局は、**AIオフィスに関連する情報へのアクセスを要求可能**。

## 苦情申立て等

- **本規則違反**があったと考える根拠を有する自然人又は法人は、関連する**市場監視当局に苦情を提出することができる。**
- その者の健康、安全又は基本的権利に悪影響を及ぼすと考えられる法的効果を生じさせる又は同様にその者に重大な影響を及ぼす**第2カテゴリのハイリスクAIシステム（Annex III）（重要インフラを除く）からのアウトプットに基づき導入者によって下された決定の対象となる者は**、導入者から、**意思決定手続におけるAIシステムの役割及び下された決定の主な要素に関する明確かつ意味のある説明を受ける権利を有する**。

# 執行③（第88条～第94条）

## 汎用AIモデル提供者の監督

- **欧州委員会は、汎用AIモデルに関する規定を監督し執行する独占的権限を有する**。欧州委員会は、この業務の実施を**AIオフィスに委ねる**ものとする。
- AIオフィスは、**実践規範の遵守を含め**、汎用AIモデルの提供者による**本規則の効果的な実施及び遵守を監視するために必要な措置をとる**ことができる。
- **川下提供者は、本規則の違反を主張する苦情を申し立てる権利を有する**。
- **科学パネル**は、ある汎用AIモデルが**①EUレベルで具体的に特定可能なリスクをもたらす**こと又は**②システミックリスクを有する汎用モデルの要件を満たす**ことを疑う理由がある場合、**AIオフィスに適格通報(qualified alert)を提供する**ことができる。
- 適格通報を受け取った欧州委員会は、AIオフィスを通じて、また、欧州AI委員会に通知した後、当該事項を評価する目的で本規則に規定する権限を行使することができる。講じる措置は欧州AI委員会に通知する。
- 欧州委員会は、汎用AIモデル提供者に対し、**必要な文書・情報の提供を要求することができる**。また、科学パネルから正当な根拠のある要請があった場合、欧州委員会は、**科学パネルの任務の遂行に必要かつ適切な場合には、汎用AIモデルの提供者に対して情報提供を要求することができる**。
- AIオフィスは、欧州AI委員会に諮問後、以下の目的で**汎用AIモデルの評価を実施する**ことができる。この評価を欧州委員会に代わって実施する**独立した専門家を任命可能**。
  - i. 収集された情報が不十分である場合に、**提供者が義務を遵守しているかを評価**するため。
  - ii. 科学パネルからの適格警告に基づき、**EUレベルでのシステミックリスクを調査**するため。
- 上記評価のため、欧州委員会は、**汎用AIモデル（ソースコードを含む）へのアクセスを要求可能**。
- **汎用AIモデル提供者又はその代理人は、要求された情報を提供しなければならない**。
- 欧州委員会は、汎用AIモデル提供者に対し、**義務を遵守するための措置の実施、リスク軽減措置の実施、市販の制限、撤回、リコールを要求することができる**。

# 罰則（第99条、第101条）

## 原則

■ **本規則が定める上限の範囲内で加盟国が定める。**

| 違反内容 | 罰則の上限 |
|---|---|
| **利用禁止AI**規定への違反 | **3,500万ユーロ又は全世界年間売上高の7%のいずれか高い方** |
| **その他の規定への違反** | **1,500万ユーロ又は全世界年間売上高の3%のいずれか高い方** |
| 当局又は適合性認証機関への**不正確、不完全又はミスリーディングな情報の提供** | **750万ユーロ又は全世界年間売上高の1%のいずれか高い方** |

**※スタートアップを含む中小企業**については、それぞれ上記のうち**低い方が上限**。

## 汎用AIモデル提供者への罰則

■ **以下のいずれかの場合、欧州委員会が1,500万ユーロ又は全世界年間売上高の3%のいずれか高い方を科す。**

i. **本規則に違反**した場合

ii. **文書・情報提供要求に応じなかった場合**又は**不正確、不完全若しくはミスリーディングな情報を提供した場合**

iii. **措置要求に応じなかった場合**

iv. **モデルへのアクセスを欧州委員会に提供しなかった場合**

# 行動規範（第95条）

## 行動規範（Code of Conduct）

- AIオフィス及び加盟国は、**ハイリスクAIシステム以外のAIシステムに、ハイリスクAIシステムが満たすべき要件の一部又は全部を自主的に適用する**ことを促進することを意図した、関連するガバナンス機構を含む**行動規範（codes of conduct）の作成を奨励及び促進する**。
- 行動規範に含むべき要素は、例えば、**環境の持続可能性への影響の評価・軽減**、**AIリテラシーの促進**、**AIシステムの包摂的かつ多様な設計の促進**、**脆弱な個人又は集団への悪影響の評価・防止**を含む。
- 行動規範は、AIシステムの個々の**提供者若しくは導入者又はそれらを代表する組織によって、市民団体やアカデミアを含む利害関係者の関与を得ながら作成**される。行動規範は、関連するシステムの本来の用途の類似性を考慮して、1つ又は複数のAIシステムを対象とすることができる。

# 施行日（第111条、第113条）

■ 施行（2024年8月1日）から以下の期間経過後にそれぞれ適用開始。

| 期間 | 適用開始規定 |
|---|---|
| **6か月**（2025年2月2日） | ・適用対象範囲<br>・定義<br>・AIリテラシー<br>**・禁止されるAI** |
| **12か月**（2025年8月2日） | ・適合性評価機関<br>**・汎用AIモデル**<br>・ガバナンス<br>・罰則（汎用AIモデルの罰則は除く） |
| **24か月**（2026年8月2日） | **・その他の規定**<br>**・これ以前に上市され又は稼働されたAIシステムは、その後設計上の大幅な変更があった場合のみ適用。**ただし、公的機関による使用が意図されているハイリスクAIシステムの提供者及び導入者は、施行から6年以内に本規則の要件及び義務を遵守するために必要な措置を講じる。 |
| **36か月**（2027年8月2日） | **・第1カテゴリのハイリスクAIシステム（他法令の対象）**<br>**・本規則の施行日から12ヶ月以内に上市された汎用AIモデルの提供者が本規則に定める義務を遵守するために必要な措置を講じる。** |
| 2030年12月31日 | ・Annex Xに列挙された法律により設置された大規模ITシステムの構成要素であって、本規則の施行日から36ヶ月以内に上市され又は稼働されたAIシステムの本規則の遵守（禁止されるAIは除く） |