

EUのAI法（AI規則）の概要

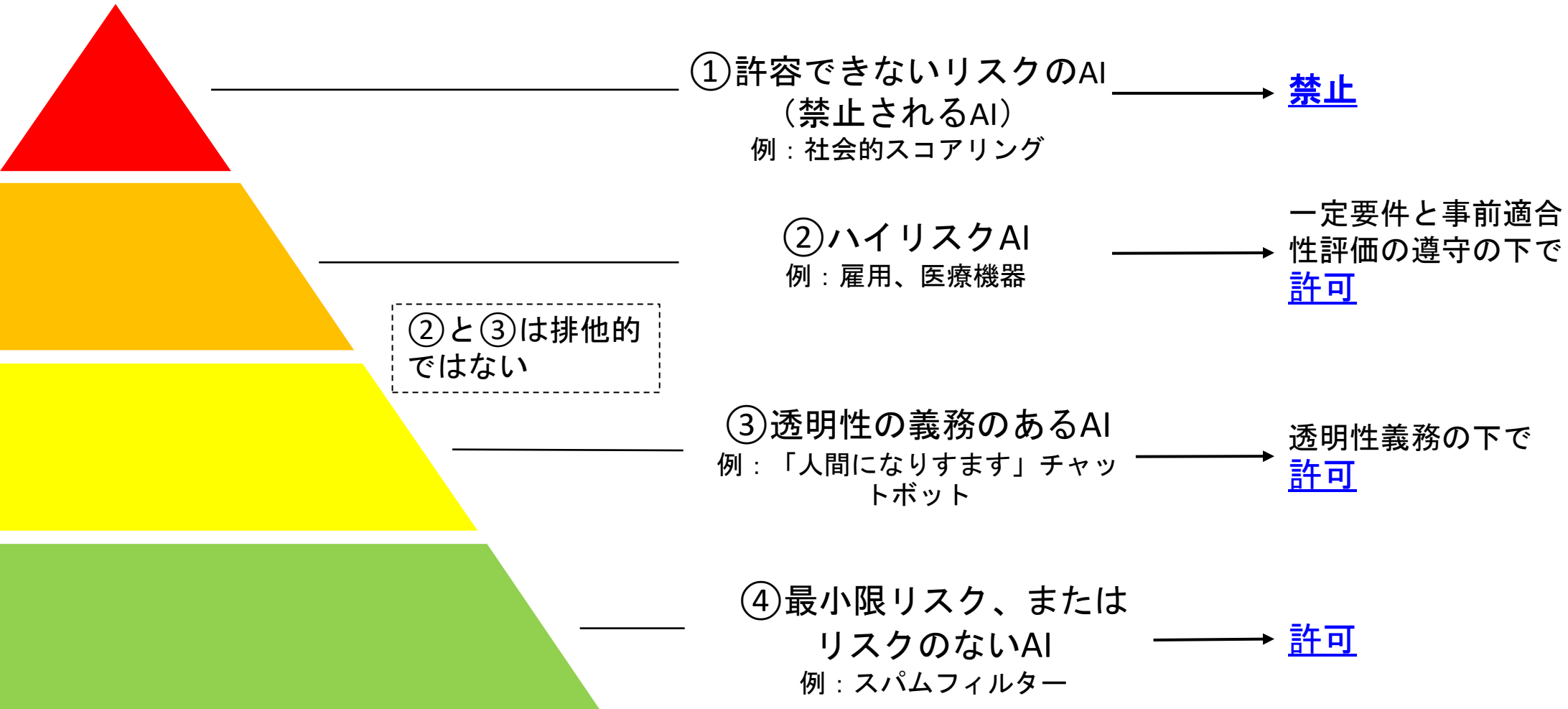
2024年 7月 12日

（株）国際社会経済研究所 小泉 雄介

- 2019年4月、欧州委員会のAIハイレベル専門家グループが「信頼できるAIのための倫理ガイドライン」を公表。
- 2020年2月、欧州委員会が「AIに関するホワイトペーパー：優越と信頼に向けた欧州アプローチ」を公表。立法措置を予告。
- 欧州委員会が2021年4月21日にAI法案（AI規則案）を提案・公表。
 - 「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」 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>)
- 上院にあたるEU理事会は2022年12月に合意案（general approach）を採択。下院にあたる欧州議会は2023年6月14日の総会で議会修正案を採択。 (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html)
- 欧州委員会・欧州議会・EU理事会による非公式な三者協議（trilogue）が2023年6月、7月、9月、10月、12月の5回行われ、2023年12月8～9日に欧州議会とEU理事会による暫定合意に達した。
- そののち、専門会合で合意テキストの詳細化が行われ、2024年3月13日に欧州議会総会で合意テキストが採択された。さらに法的・言語的な最終チェックが行われ、4月23日の欧州議会総会で最終テキストを採択 (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf)。 その後、EU理事会で2024年5月21日に採択されることでAI法（AI規則）の正式な制定となった。
- 2024年7月12日にEU官報で公表され (<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>)、その20日後に発効。
- AI法の全面適用（施行）は発効の2年後（2026年8月2日）だが、禁止AIについては6か月後（2025年2月2日）、汎用目的AIモデルについては12か月後（2025年8月2日）から適用（施行）となる。

AI法の特徴： リスクベースアプローチ

- AI法では、リスクベースアプローチ、すなわち（AIを一律に規制するのではなく）AI機器・サービスがもたらすリスクに応じて規制をかけるアプローチが取られている。欧州委員会によれば、ほとんどのAIシステムは④に相当。



※合意テキストでは、4階層のリスクベースアプローチは維持されながらも、別軸として「⑤汎用目的AIモデル」に対する規制（2段階）が追加された

- 「Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) 」
- 「人工知能に関する整合ルールを規定し、規則 (EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139 および (EU) 2019/2144、ならびに指令 2014/90/EU、(EU) 2016/797 および (EU) 2020/1828を修正する2024年6月13日の欧州議会および理事会の規則 (EU) 2024/1689 (AI法) 」

- 前文 (1) ～ (180)
- 条文
 - 第1章 一般規定 (General Provisions) : 第1条～4条
 - 第2章 禁止されるAI慣行 (Prohibited AI Practices) : 第5条
 - 第3章 ハイリスクAIシステム (High-risk AI Systems) : 第6条～49条
 - 第1節 ハイリスクAIシステムとしての分類 (Classification of AI Systems as High-risk)
 - 第2節 ハイリスクAIシステムに対する要件 (Requirements for High-risk AI Systems)
 - 第3節 ハイリスクAIシステムのプロバイダーとディプロイヤー、その他の当事者の義務 (Obligations of providers and deployers of high-risk AI systems and other parties)
 - 第4節 公認認証当局と公認認証機関 (Notifying Authorities and Notified Bodies)
 - 第5節 規格、適合性評価、証明書、登録 (Standards, Conformity Assessment, Certificates, Registration)
 - 第4章 特定のAIシステムのプロバイダーとディプロイヤーに対する透明性の義務 : 第50条
 - 第5章 汎用目的AIモデル (General-purpose AI Models) : 第51条～56条
 - 第1節 分類ルール (Classification rules)
 - 第2節 汎用目的AIモデルのプロバイダーの義務 (Obligations for providers of general-purpose AI models)
 - 第3節 システミックリスクのある汎用目的AIモデルのプロバイダーの義務 (Obligations of providers of general-purpose AI models with systemic risk)
 - 第4節 実践規範 (Codes of practice)

- 第6章 イノベーションを支援するための措置（Measures in Support of Innovation）：第57条～63条
- 第7章 ガバナンス（Governance）：第64条～70条
 - 第1節 EUレベルでのガバナンス（Governance at Union level）
 - 第2節 国内所轄機関（National Competent Authorities）
- 第8章 ハイリスクAIシステムに関するEUデータベース（EU database for high-risk AI systems）：第71条
- 第9章 市場流通後モニタリング、情報共有、市場監視（Post-market Monitoring, Information Sharing and Market Surveillance）：第72条～94条
 - 第1節 市場流通後モニタリング（Post-market monitoring）
 - 第2節 重大インシデントに関する情報の共有（Sharing of information on serious incidents）
 - 第3節 執行（Enforcement）
 - 第4節 救済（Remedies）
 - 第5節 汎用目的AIモデルのプロバイダーに対する監督、調査、執行およびモニタリング
- 第10章 行動規範とガイドライン（Codes of Conduct and Guidelines）：第95条～96条
- 第11章 権限の委任および委員会の手続（Delegation of Power and Committee Procedure）：第97条～98条
- 第12章 罰則（Penalties）：第99条～101条
- 第13章 最終規定（Final Provisions）：第102条～113条

• AI法の目的（第1条第1項）

- 本規則の目的は、EU域内市場の機能を改善し、人間中心で信頼できる人工知能（AI）の導入を促進すると同時に、EU域内での人工知能システム（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EU基本権憲章に謳われている）基本的権利の高レベルの保護を保証し、イノベーションを支援することである。

※条文の和訳は筆者による。和訳条文をそのまま掲載する場合は、グレー四角枠で囲う。下線は筆者加筆。以下同様。

• AI法が規定すること（対象事項）（第1条第2項）

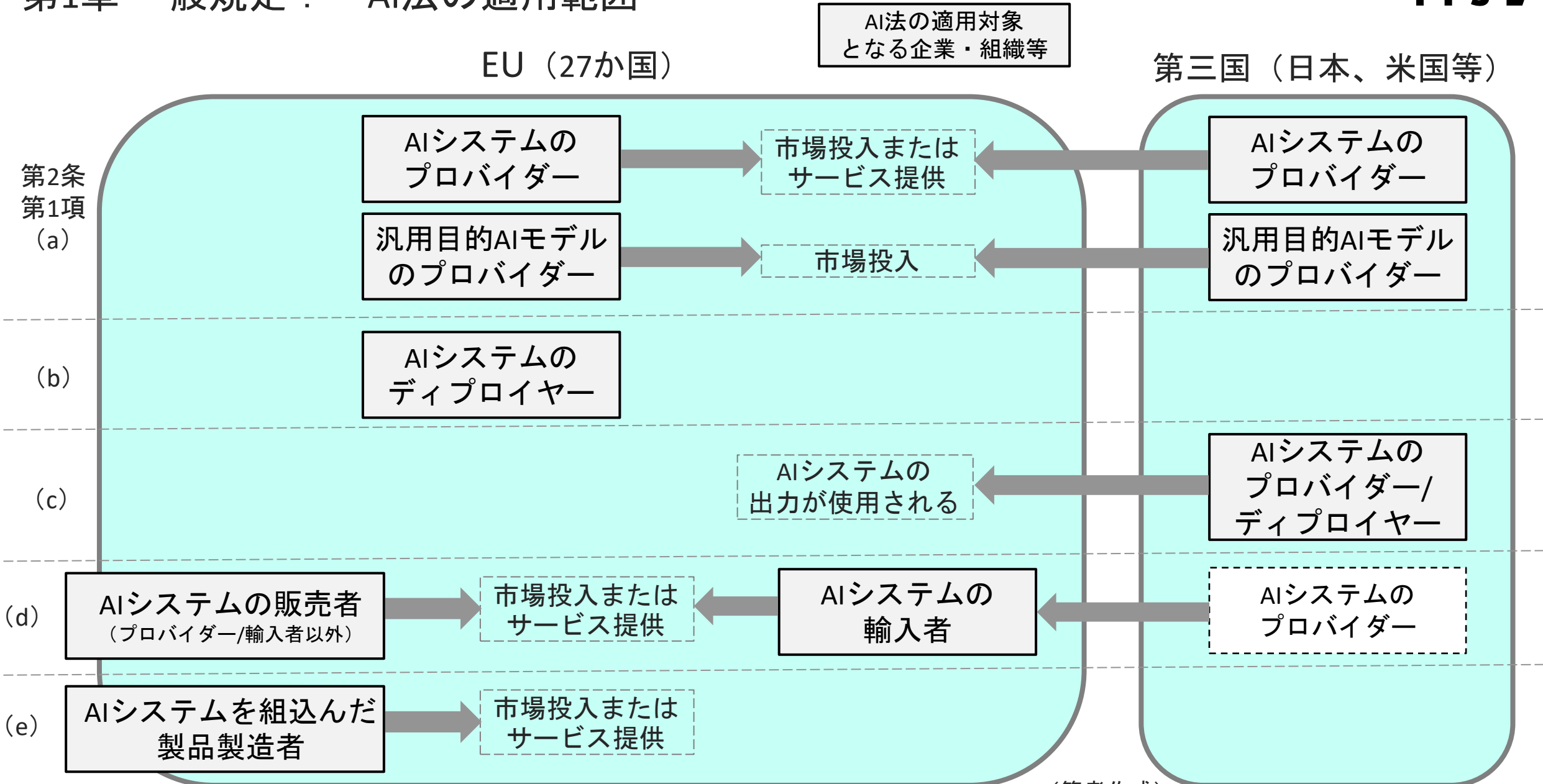
- (a) EU域内でのAIシステムの市場投入、サービス提供、および使用に関する整合ルール。
- (b) 特定のAI慣行の禁止。
- (c) ハイリスクAIシステムに対する特定の要件と、それらのオペレーターに対する義務。
- (d) 一定のAIシステムに関する整合的な透明性ルール。
- (e) 汎用目的AIモデルの市場投入に関する整合ルール。
- (f) 市場モニタリング、市場監視ガバナンス、および執行に関するルール。
- (g) 新興企業（start-ups）を含む中小企業に特に焦点を当てた、イノベーションを支援するための措置。

• AIシステムの定義

- 「AIシステム（AI system）」とは、様々なレベルの自律性で動作するように設計され、ディプロイメント後に適応性を示す可能性があり、明示的または暗黙的な目的のために、受け取った入力から、物理的またはバーチャルな環境に影響を与えうる出力（予測、コンテンツ、レコメンデーション、意思決定など）を生成する方法を推論するマシンベースのシステムを意味する。（第3条（1））
- 「汎用目的AIモデル（general-purpose AI model）」とは、当該モデルがどのように市場投入され、様々な下流システムやアプリケーションに組み込むかどうかに関係なく、AIモデルが大規模な自己教師あり学習を用いて大量のデータでトレーニングされる場合を含め、重要な汎用性を示し、広範囲にわたる個別のタスクを適切に実行できる AI モデルを意味する。ただし、市場にリリースされる前の研究、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。（第3条（63））

- AI法の適用範囲（第2条）→ EU域外のプロバイダー（開発・提供企業）やディプロイヤー（利用企業）も規制対象になりうる
 - （a）EU域内に拠点がある/位置するか第三国に拠点がある/位置するかに関係なく、EU域内でAIシステムの市場投入/サービス提供を行う、または汎用目的AIモデルの市場投入を行うプロバイダー。
 - （b）EU域内に拠点のある/位置するAIシステムのディプロイヤー。
 - （c）そのAIシステムによって生成された出力がEU域内で使用される場合、第三国に拠点のある/位置するプロバイダーとディプロイヤー。
 - （d）AI システムの輸入者および販売者。
 - （e）自社の製品とともに自社の名称/商標でAIシステムを市場投入/サービス提供を行う製品製造者。
 - （f）EU 域内に拠点のないプロバイダーの権限のある代理人。（g）EU 域内に位置する影響を受ける人々。
- AI法の適用対象外：軍事・防衛・国家安全保障の目的のみのAIシステム、科学研究開発の目的のみのAI、市場投入/サービス提供前のAI、個人的で非専門家的な活動の過程でAIシステムを使用する自然人としてのディプロイヤー（利用者）

第1章 一般規定： AI法の適用範囲



• 定義（第3条）

- （3）「[プロバイダー（provider）](#)」とは、AIシステムもしくは汎用目的AIモデルを開発し、または開発させ、有料または無料を問わず、自らの名前や商標でそれを市場投入したり当該AIシステムをサービス提供するような自然人もしくは法人、公的機関、部局、またはその他の組織を意味する。
- （4）「[ディプロイヤー（deployer）](#)」とは、個人的で非職業的なアクティビティの過程でAIシステムが使用される場合を除き、自らの権限でAIシステムを使用する自然人もしくは法人、公的機関、部局、またはその他の組織を意味する。
- （5）「権限のある代理人（authorised representative）」とは、AIシステムまたは汎用目的AIモデルのプロバイダーから、本規則で規定された義務と手続を実行するための書面による委任を受け、受諾した、EU域内に拠点のある自然人または法人を意味する。
- （6）「輸入者（importer）」とは、EU域外に拠点のある自然人または法人の名前や商標を付けたAIシステムを市場投入したりサービス提供するような、EU域内に拠点のある自然人または法人を意味する。
- （7）「販売者（distributor、頒布者）」とは、プロバイダーまたは輸入者以外の、その特性に影響を与えることなくAIシステムをEU域内市場で利用可能にするサプライチェーン内の自然人または法人を意味する。
- （8）「オペレーター（operator）」とは、プロバイダー、製品製造者、ディプロイヤー、権限のある代理人、輸入者、または販売者を意味する。
- （9）「[市場投入（placing on the market、上市）](#)」とは、EU市場で最初にAIシステムまたは汎用目的AIモデルを利用可能にすることを意味する。
- （10）「市場で利用可能にする（making available on the market）」とは、有料か無料かを問わず、商業活動の過程でEU市場で頒布または使用するためのAIシステムまたは汎用目的AIモデルの供給を意味する。
- （11）「[サービス提供（putting into service、サービス開始）](#)」とは、EU域内で、その意図された目的で、ディプロイヤーが最初に直接使用するための、または独自に使用するためのAIシステムの供給を意味する。

- 第4条 AIリテラシー（AI literacy）
 - AIシステムのプロバイダーおよびディプロイヤーは、彼らに代わってAIシステムの運用と使用を担当するスタッフおよびその他の人々の十分なレベルのAIリテラシーを、その人々の技術的知識、経験、教育、訓練、およびAIシステムが使用される状況を考慮し、またAIシステムが使用される個人またはグループを考慮して、最大限に保証するための措置を講じるものとする。

※第4条は第1章に含まれるため、AI法の発効から6か月後に適用開始となる。ただし、プロバイダーやディプロイヤーに対する制裁金は定められていない。

第2章 禁止されるAI慣行： ①禁止されるAIシステム

• 禁止されるAI慣行（第5条）

- (a) サブリミナル操作
- (b) 年齢、障害、社会的・経済的状况による脆弱性の悪用
- (c) ソーシャルスコアリング
- (d) プロファイリング等に基づく個人に対する予測的ポリシング
- (e) インターネットや監視カメラの映像から顔画像を無差別に（ターゲットを絞らずに）収集（スクレイピング）することで顔認識データベースを作成するシステム
- (f) 職場や教育機関における感情認識システム
 - ただし、医療または安全の理由の場合を除く（治療目的等）。
- (g) 生体データに基づき、個人の人種、政治的意見、労働組合への加入、宗教・思想上の信条、性生活・性的指向を推測する生体カテゴライゼーションシステム（属性推定システム）
- (h) 公的に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」リモート生体識別システムの使用
 - ただし、以下のいずれかの目的に厳密に必要な場合は除く。
 - (i) 行方不明者、誘拐・人身売買・性的搾取の被害者に対するターゲットを絞った搜索
 - (ii) 生命・身体的安全に対する特定・実質的・差し迫った脅威の防止、またはテロ攻撃の本物の現時点での/予見可能な脅威の防止
 - (iii) 特定の重大犯罪（テロ、人身売買、性的搾取、殺人、誘拐、強姦、武装強盗、犯罪組織への参加、環境犯罪など）の容疑者の位置特定または識別

禁止されるAIの8つのタイプのうち、
(e) ～ (h) の4つが生体データ
関連のシステム。

第2章 禁止されるAI慣行： ①禁止されるAIシステム

• 禁止されるAI慣行：第5条第1項の条文

- (a) 当人、他の人または人々のグループに重大な危害を引き起こしたり、引き起こす可能性の高い仕方で、情報に基づいた意思決定を行う能力を著しく損ない、それにより当人がそうでなければ行わなかったであろう意思決定を行わせることにより、個人または人々のグループの行動を実質的に歪める目的で、またはそのような効果を伴って、個人の意識を超えたサブリミナル技術、または意図的に操作的もしくは欺瞞的な技術を用いるAIシステムの市場投入、サービス提供、または使用。
- (b) 当人または他の人の重大な危害を引き起こしたり、合理的に引き起こす可能性の高い仕方で、当該グループに属する当人または個人の行動を実質的に歪める目的で、またはそのような効果を伴って、年齢、障害、または特定の社会的もしくは経済的状况による個人または特定グループの脆弱性を悪用するAIシステムの市場投入、サービス提供、または使用。
- (c) 個人の社会的行動または既知、推測もしくは予測された個人的特性もしくは性格特性に基づき、以下のいずれかまたは両者をもたらすようなソーシャルスコアを用いて、特定の期間にわたる自然人またはそのグループを評価または分類するための、公的機関による、または公的機関に代わってのAIシステムの市場投入、サービス提供、または使用。
 - (i) データが最初に生成または収集されたコンテキストとは関係のない社会的コンテキストにおける、特定の自然人またはそのグループ全体に対する不利益な、または望ましくない扱い。
 - (ii) その社会的行動またはその重大さに対して不当なまたは不釣り合いな、特定の自然人またはそのグループ全体に対する不利益な、または望ましくない扱い。
- (d) 自然人のプロファイリングのみに、またはその性格特性 (personality traits) や特性 (characteristics) の評価のみに基づいて、自然人が犯罪を行う可能性を評価または予測するために、自然人のリスク評価を行うAIシステムの市場投入、この特定目的のためのサービス提供、または使用。ただし、この禁止事項は、犯罪行為に直接関係する客観的かつ検証可能な事実にすでに基づいている、犯罪行為への自然人の関与に関する人間による評価をサポートするために使用されるAIシステムには適用されないものとする。

第2章 禁止されるAI慣行： ①禁止されるAIシステム

• 禁止されるAI慣行：第5条第1項の条文（続き）

- (e) インターネットや監視カメラ（CCTV）の映像から顔画像を無差別に収集（untargeted scraping）することで顔認識データベースを作成または拡張するAIシステムの市場投入、この特定目的でのサービス提供、または使用。
- (f) 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AIシステムの市場投入、この特定目的でのサービス提供、または使用。ただし、当該AIシステムの使用が医療または安全の理由での導入または市場導入を意図している場合を除く。
- (g) 当人の人種、政治的意見、労働組合への加入、宗教上もしくは思想上の信条、性生活、または性的指向を推論（deduce）または推測（infer）するために、当人の生体データに基づき、個々の自然人をカテゴライズする生体カテゴライゼーションシステムの市場投入、この特定目的でのサービス提供、または使用。ただし、この禁止事項には、法執行分野における、画像などの合法的に取得された生体データセットの生体データに基づくラベル付けもしくはフィルタリング、または生体データの Kategorization は含まれない。
- (h) 公的にアクセス可能な空間における法執行の目的での「リアルタイム」リモート生体識別システムの使用。ただし、そのような使用が以下の目的の1つに厳密に必要な場合を除く。
 - (i) 行方不明の人々の搜索、および誘拐、人身売買、または人間の性的搾取の特定の犯罪被害者に対するターゲット化された搜索。
 - (ii) 自然人の生命または身体的安全に対する特定の、実質的かつ差し迫った脅威の防止、またはテロリスト攻撃の本物の現時点での（genuine and present）脅威もしくは本物の予見可能な（genuine and foreseeable）脅威の防止。
 - (iii) Annex II で言及され、当該加盟国において国内法によって少なくとも43年間の拘禁刑または拘禁命令により罰することができる犯罪に対する刑事捜査、訴追、または刑事罰の執行を目的とした、犯罪容疑者の検出、位置特定または識別、または起訴。
- 第1段落の (h) は、法執行以外の目的での生体データの処理に関して、規則 (EU) 2016/679（GDPR）の第9条に影響を与えるものではない。

(1) 製品安全性に関する既存のEU整合法令で規制された製品の安全コンポーネント（第6条第1項、Annex I）

(→身体等の安全にかかわるもの)

- Annex Iで挙げられた製品のうち、EU整合法令に従い、第三者適合性評価の対象となるもの。
- Annex I セクションA 新たな法的フレームワーク（NLF）に基づくEU整合法令のリスト

機械に関する指令2006/42/EC	玩具の安全性に関する指令2009/48/EC
レジャー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2013/53/EU	昇降機および安全コンポーネントに関連する加盟国の法律の整合に関する指令2014/33/EU
潜在的な爆発性雰囲気での使用を目的とした機器および保護システムに関連する加盟国の法律の整合に関する指令2014/34/EU	無線機器の域内市場での利用可能化および指令1999/5/ECの廃止に関連する加盟国の法律の整合に関する指令2014/53/EU
圧力機器の域内市場での利用可能化に関連する加盟国の法律の整合に関する指令2014/68/EU	ケーブルウェイの設置に関する規則（EU）2016/424
個人用保護具に関する規則（EU）2016/425	ガス燃料を燃焼する機器に関する規則（EU）2016/426
医療機器に関する規則（EU）2017/745	体外診断用医療機器に関する規則（EU）2017/746

- Annex I セクションB その他のEU整合法令（オールドアプローチ法令）→第112条（評価と見直し）のみ適用

民間航空のセキュリティの分野における共通ルールに関する規則（EC）No 300/2008	二輪車等の認可と市場監視に関する規則（EU）No 168/2013
農林業用車両の認可と市場監視に関する規則（EU）No 167/2013	船用機器に関する指令2014/90/EU
鉄道システムの相互運用性に関する指令（EU）2016/797	自動車とトレーラーの認可と市場監視に関する規則（EU）2018/858
自動車の型式認可要件に関する規則（EU）2019/2144	民間航空分野における共通ルールと欧州連合航空安全庁の設置に関する規則（EU）2018/1139

(2) 以下の分野におけるAIシステム（第6条第2項、Annex III）

(→基本的人権等にもたらされるリスクが高いとして、AI法で新たに名指しされたもの)

1. バイオメトリクス（EU法または国内法で使用が許可された範囲内で）

2. 重要インフラ

3. 教育と職業訓練

4. 雇用、従業員管理、自営業者へのアクセス

5. 重要な民間サービス、公共サービス、公的給付金へのアクセスおよび享受

6. 法執行（EU法または国内法で使用が許可された範囲内で）

7. 移住、亡命、国境管理（EU法または国内法で使用が許可された範囲内で）

8. 司法手続および民主的手続の管理

第3章 ハイリスクAIシステム： ②ハイリスクAIシステムの分類

• Annex III 第6条第2項で言及されたハイリスクAIシステム

- 1. バイオメトリクス（Biometrics）（関連するEU法または国内法で使用が許可されている場合）：
 - （a）[リモート生体識別システム](#)。これには、特定の自然人が本人であると主張する者であることを確認することを唯一の目的とする生体検証（biometric verification）に使用することを目的としたAIシステムは含まれないものとする。
 - （b）センシティブな、または保護されている属性または特性の推測に基づき、これらの属性または特性による[生体カテゴライゼーション](#)に使用することを目的としたAIシステム。
 - （c）[感情認識](#)に使用することを目的としたAIシステム。
- 2. 重要インフラ（Critical infrastructure）：重要デジタルインフラ・道路交通の管理と運用、または水・ガス・暖房・電気の供給における安全コンポーネントとして使用することを目的としたAIシステム。
- 3. 教育と職業訓練（Education and vocational training）：
 - （a）あらゆるレベルの[教育機関および職業訓練機関へのアクセスもしくは入学を決定](#)したり、自然人をアサインする目的で使用されることを目的としたAIシステム。
 - （b）[学習成果を評価](#)するために使用することを目的としたAIシステム。これには、あらゆるレベルの教育機関および職業訓練機関における自然人の学習プロセスを導くためにその成果が使用される場合が含まれる。
 - （c）あらゆるレベルの教育機関および職業訓練機関の文脈で、またはその内部で、個人が受ける、またはアクセスできる[適切な教育レベルを評価](#)する目的で使用されることを目的としたAIシステム。
 - （d）あらゆるレベルの教育機関および職業訓練機関の文脈で、またはその内部で、[試験中の学生の禁止行為をモニタリング](#)および検出するために使用することを目的としたAIシステム。
- 4. 雇用、従業員管理、自営業者へのアクセス（Employment, workers management and access to self-employment）：
 - （a）[自然人の採用または選定](#)、特にターゲット化された[求人広告](#)の掲載、応募者の分析およびフィルタリング、および候補者の評価に使用することを目的としたAIシステム。
 - （b）仕事関連の関係の条件、[昇進／仕事関連の契約関係の終了](#)に影響を与える意思決定、個人の行動もしくは個人的特性・特徴に基づく[業務の割り当て](#)、またはそのような契約関係における[個人のパフォーマンスと行動のモニタリングや評価](#)に使用することを目的としたAIシステム。

- 5. 重要な民間サービス、重要な公共サービス、重要な公的給付金へのアクセスおよび享受：
 - (a) 公的機関によって、または公的機関に代わって、自然人が重要な公的支援の給付金およびサービス（ヘルスケアサービスを含む）を受ける資格を評価し、またそのような給付金およびサービスを許可、削減、取り消し、または再請求するために使用することを目的としたAIシステム。
 - (b) 個人の信用度を評価したり、個人の信用スコアを作成するために使用することを目的としたAIシステム。ただし、金融詐欺を検出する目的で使用されるAIシステムを除く。
 - (c) 生命保険および健康保険において自然人に関するリスク評価および保険料設定に使用することを目的としたAIシステム。
 - (d) 自然人による緊急通報を評価および分類することを目的としたAIシステム、または警察、消防士、および医療救護、ならびに緊急ヘルスケア患者トリアージシステムを含め、緊急時の初期対応サービスを派遣、または派遣の優先順位を決定するために使用されることを目的としたAIシステム。
- 6. 法執行（Law enforcement）（関連するEU法または国内法で使用が許可されている場合）：
 - (a) 自然人が刑事犯罪の被害者となるリスクを評価するために、法執行機関によって、もしくは彼らに代わって、または法執行機関の支援においてEUの機関、組織、事務局、部局によって、もしくは彼らに代わって使用されることを目的としたAIシステム。
 - (b) 法執行機関によって、もしくは彼らに代わって、または法執行機関の支援においてEUの機関、組織、事務局、部局によって、ポリグラフまたは同様のツールとして使用されることを目的としたAIシステム。
 - (c) 刑事犯罪の捜査または起訴の過程で証拠の信頼性を評価するために法執行機関によって、もしくは彼らに代わって、または法執行機関の支援においてEUの機関、組織、事務局、部局によって使用されることを目的としたAIシステム。
 - (d) 指令（EU）2016/680（法執行指令）の第3条（4）で言及されているような自然人のプロファイリングのみに基づくことなく自然人が犯罪または再犯罪を行うリスクを評価するために、または自然人やグループの人格特性・性格や過去の犯罪行動を評価するために、法執行機関によって、もしくは彼らに代わって、または法執行機関の支援においてEUの機関、組織、事務局、部局によって使用されることを目的としたAIシステム。
 - (e) 刑事犯罪の検出、捜査または起訴の過程で、指令（EU）2016/680（法執行指令）の第3条（4）で言及されているような自然人のプロファイリングのために、法執行機関によって、もしくは彼らに代わって、または法執行機関の支援においてEUの機関、組織、事務局、部局によって使用することを目的としたAIシステム。

- 7. 移住、亡命、国境管理（Migration, asylum and border control management）（関連するEU法または国内法で使用が許可されている場合）：
 - （a）所轄の公的機関によって、もしくは彼らに代わって、またはEUの機関、組織、事務局、部局によって、[ポリグラフや同様のツール](#)として使用されることを目的としたAIシステム。
 - （b）所轄の公的機関によって、もしくは彼らに代わって、またはEUの機関、組織、事務局、部局によって、加盟国の領土に入国することを意図する、または入国した自然人によってもたらされる[セキュリティリスク、不法移民のリスク、健康リスクを含むリスクを評価](#)するために使用されることを目的としたAIシステム。
 - （c）所轄の公的機関によって、もしくは彼らに代わって、またはEUの機関、組織、事務局、部局によって、[亡命、ビザ、居住許可の申請](#)を、また関連する苦情を、それらのステータスを申請する自然人の資格の観点から審査することの支援のために使用されることを目的としたAIシステム。
 - （d）所轄の公的機関によって、もしくは彼らに代わって、またはEUの機関、組織、事務局、部局によって、渡航文書の検証を除き、[自然人の検出、認識、または識別](#)のために、移住、亡命、または国境管理の文脈で使用されることを目的としたAIシステム。
- 8. 司法手続および民主的手続の管理（Administration of justice and democratic processes）：
 - （a）司法当局によって、または彼らに代わって、事実と法律を調査および解釈し、[法律を具体的な一連の事実に適用](#)することの支援のために使用されることを目的としたAIシステム、または裁判外の紛争解決において同様な仕方で使用されることを目的としたAIシステム。
 - （b）[選挙もしくは国民投票の結果](#)、または[選挙もしくは国民投票における自然人の投票行動に影響](#)を与えるために使用することを目的としたAIシステム。これには、管理上またはロジスティック上の観点から政治キャンペーンを組織、最適化、または構築するために使用されるツールなど、自然人が直接さらされない出力を行うAIシステムは含まれない。

- 「ハイリスクAIシステム」としてAnnex IIIにリスト化されたAIシステムは、例外として「それが自然人の健康、安全、または基本的権利に危害を及ぼす重大なリスクを提示しない場合、ハイリスクとはみなされない」（第6条第3項）。具体的には、以下のいずれかの場合。
 - (a) 当該AIシステムが、狭い手続上のタスクの実行を目的としている。
 - (b) 当該AIシステムが、以前に完了した人間の活動結果の改善を目的としている。
 - (c) 当該AIシステムが、意思決定パターンの検出または以前の意思決定パターンからの逸脱の検出を目的としており、人間による適切なレビューなしに、以前に完了した人間による評価を置き換えたり影響を与えたりすることを目的としていない。
 - (d) 当該AIシステムが、Annex IIIにリスト化されたユースケースの目的に関連する評価の準備タスクを実行することを目的としている。
 - ただし上記にかかわらず、Annex IIIにリスト化されたAIシステムは、自然人のプロファイリングを実行する場合、常にハイリスクであるとみなされる。
- Annex IIIにリスト化されたAIシステムがハイリスクか否かの評価は、プロバイダー自身の実施。プロバイダーはハイリスクでないと評価した場合も、その評価を文書化するとともに、当該AIシステムをEUデータベースに登録しなければならない。（第6条第4項）

第3章 ハイリスクAIシステム： ②ハイリスクAIシステムの要件

- ハイリスクAIシステムには以下の要件が課せられる。

リスク管理システム (第9条)	健康・安全・基本的権利に提示しうるリスクの特定・分析・評価、リスク管理措置の特定・採用。
データおよびデータガバナンス (第10条)	学習データ・検証データ・テストデータにおけるバイアスの検出・防止・軽減、これらのデータの関連性・代表性・正確性の保証、当該システムが使用される地理的・文脈的・行動的・機能的な条件の考慮。 - バイアスの検出および修正を保証するために厳密に必要な範囲で、プロバイダーは自然人の基本的権利および自由に対する適切な保護措置に服することにより、例外的に、特別なカテゴリーの個人データを処理することができる。(第10条第5項)
技術文書 (第11条)	当該システムが要件を遵守していることの評価に必要な全ての情報を記載し、国内所轄機関および公認認証機関に提供。
記録保管 (第12条)	- 当該システムのライフタイムに渡ってイベントの自動記録(ログ)を可能にする。 「リモート生体識別システム」には追加要件あり。
透明性とディプロイヤーへの情報提供 (第13条)	透明性：ディプロイヤーが当該システムの出力を解釈し、適切に使用できるように、その動作が十分に透明であることを保証する仕方で設計および開発する。適切な透明性のタイプと程度は、プロバイダーおよびディプロイヤーの義務の遵守を達成する観点から、保証する。 情報提供：ディプロイヤー向け使用説明書に、当該システムの特性・能力・制限（意図された目的、正確性・堅牢性・セキュリティのレベル、健康・安全・基本的権利へのリスク等）、人間による監督措置などを含める。
人間による監督 (第14条)	- プロバイダーによって当該システムに組込まれる監督措置 and/or ディプロイヤーによって実施される監督措置の保証。 - 監督者がシステムの動作をモニターし、自動化バイアスを自覚し、出力を正しく解釈し、システムの不使用を決定したり出力をオーバーライドでき、システムの動作に介入したり安全に停止できるようにする。(第14条第4項) 「リモート生体識別システム」には追加要件あり。
正確性、堅牢性、サイバーセキュリティ(第15条)	- 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する。 - データポイズニング、モデルポイズニング、敵対的サンプル等の攻撃に対処する。

- ハイリスクAIシステムのプロバイダーの義務は以下。（第16条）
 - (a) ハイリスクAIシステムが、[第2節（第8条～15条）で規定されている要件を遵守](#)していることを保証する。
 - (b) ハイリスクAIシステムに、またはそれが不可能な場合はそのパッケージまたは付属文書に、該当する場合にはその名前、登録商標名または登録商標、連絡先住所を表示する。
 - (c) 第17条を遵守した[品質管理システムを導入](#)する。
 - (d) 第18条で言及されている[文書を保管](#)する。
 - (e) 管理下にある場合、第19条で言及されているように、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。
 - (f) ハイリスクAIシステムの市場投入前またはサービス提供前に、第43条で言及されているように、関連する[適合性評価手続を実施](#)していることを保証する。
 - (g) 第47条に従って[EU適合性宣言書を作成](#)する。
 - (h) 第48条に従って、本規則への適合性を示す[CEマーク](#)をハイリスクAIシステムに貼付するか、それが不可能な場合はそのパッケージまたは付属文書に貼付する。
 - (i) 第49条第1項に記載されている[登録義務](#)を遵守する。
 - (j) 第20条に従って必要な[是正措置](#)を講じ、要求された情報を提供する。。
 - (k) 加盟国の[国内所轄機関の合理的な要求に応じて](#)、ハイリスクAIシステムが第2節で規定されている要件に適合していることを実証する。
 - (l) ハイリスクAIシステムが指令 (EU) 2016/2102 および指令 (EU) 2019/882 に準拠した[アクセシビリティ要件](#)を遵守していることを保証する。

第3章 ハイリスクAIシステム： ②ハイリスクAIのプロバイダーの権限のある代理人 I I S E

- 第22条 ハイリスクAIシステムのプロバイダーの権限のある代理人
 - 1. EU域外に拠点のあるプロバイダーは、EU市場でハイリスクAIシステムを利用可能にする前に、書面による委任（mandate）により、EU域内に拠点のある、権限のある代理人を指名するものとする。
 - 2. プロバイダーは、その権限のある代理人がプロバイダーから受け取った委任に指定された職務を実行できるようにするものとする。
 - 3. 権限のある代理人は、プロバイダーから受け取った委任で指定された職務を実行するものとする。また、要求に応じて、国内所轄機関が示すEU機関の公式言語のいずれかで市場監視機関に委任のコピーを提供するものとする。本規則の目的上、この委任は、権限のある代理人が以下の職務を実行する権限を与えるものとする。
 - (a) 第11条で言及されたEU適合性宣言書および技術文書が作成されていること、およびプロバイダーによって適切な適合性評価手続が実行されていることを検証する。
 - (b) 権限のある代理人を指名したプロバイダーの連絡先詳細、EU適合性宣言書のコピー、技術文書、および該当する場合は公認認証機関が発行した証明書を、国内所轄機関または第74条第10項で言及されている国内当局が、ハイリスクAIシステムが市場投入またはサービス提供されてから10年間、自由に使用できるように保管する。
 - (c) 合理的な要求に応じて、第2節で規定されている要件へのハイリスクAIシステムの適合性を実証するために必要なすべての情報と文書を、本項(b)で言及されたものを含め、国内所轄機関に提供する。これには、プロバイダーがログを管理している範囲で、第12条第1項に言及されたハイリスクAIシステムによって自動生成されたログへのアクセスが含まれる。
 - (d) ハイリスクAIシステムに関連して所轄機関が講じる措置について、合理的な要求に応じて、特にハイリスクAIシステムが提示するリスクを低下および軽減するために、当該機関に協力する。
 - (e) 該当する場合、第49条第1項に記載されている登録義務を遵守するか、登録がプロバイダー自身によって行われる場合は、Annex VIII のセクションAに記載されている情報が正しいことを確認する。
- この委任により、権限のある代理人は、プロバイダーに加えて、またはプロバイダーに代わって、本規則の遵守の保証に関連するすべてのイシューについて、所轄機関によって対処される権限が与えられるものとする。
- 4. 権限のある代理人は、プロバイダーが本規則に基づく義務に反して行動しているとみなした場合、またはそう考える理由がある場合、委任を終了するものとする。このような場合、当該代理人はまた、代理人が所在するまたは拠点のある加盟国の市場監視機関、および、該当する場合には関連する公認認証機関に、委任の終了およびその理由を直ちに情報提供するものとする。

- 第25条 AIバリューチェーンに沿った責任（Responsibilities along the AI value chain）
- 1. 販売者、輸入者、ディプロイヤー、またはその他の第三者は、本規則の目的上、以下のいずれかの状況下ではハイリスクAIシステムのプロバイダーとみなされ、第16条の下でのプロバイダーの義務に従うものとする。
 - （a）その義務が別の方法で割り当てられることを規定する契約上の取決めに損なうことなく、すでに市場投入されたり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前または商標を掲載する場合。
 - （b）すでに市場投入されたり、サービス提供されているハイリスク AI システムに実質的な変更を加え、かつ変更後も第6条の下でハイリスク AI システムに該当する場合。
 - （c）ハイリスクとして分類されておらず、既に市場投入またはサービス提供されている AI システム（汎用目的AIシステムを含む）の意図された目的を、当該AIシステムが第6条の下で ハイリスクAIシステムになるような仕方に変更する場合。
- 2. 第1項で言及された状況が発生した場合、最初に当該AIシステムを市場投入またはサービス提供したプロバイダーは、本規則の目的上、もはや当該AIシステムのプロバイダーとはみなされなくなるものとする。その最初のプロバイダーは、新しいプロバイダーと緊密に協力し、必要な情報を利用可能にし、特にハイリスクAIシステムの適合性評価の遵守に関して、本規則に定められた義務の履行に必要な、合理的に予想される技術的アクセスおよびその他の支援を提供するものとする。本項は、最初のプロバイダーが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示しており、そのため文書を提供する義務が発生しない場合には適用されない。
- 3. Annex IのセクションAにリスト化されているEU整合法令の対象となる製品の安全コンポーネントであるハイリスクAIシステムであって、以下のいずれかの状況の場合、製品製造者はハイリスクAIシステムのプロバイダーとみなされ、第16条に基づく義務の対象となるものとする。
 - （a）ハイリスクAIシステムが製品製造者の名前または商標の下で当該製品と共に市場投入される。
 - （b）当該製品が市場投入された後、ハイリスクAIシステムが製品製造者の名前または商標の下でサービス提供される。
- 4. ハイリスクAIシステムのプロバイダーと、ハイリスクAIシステムで使用または組み込まれる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、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本規則に定められた義務を完全に遵守できるようにするために、一般的に認められている最先端技術に基づいて、必要な情報、能力、技術的アクセス、およびその他の支援を指定するものとする。本項は、無償かつオープンなライセンスに基づいて、汎用目的AIモデル以外の公開ツール、サービス、プロセス、またはコンポーネントにアクセスできるようにする第三者には適用されないものとする。（第4項第2段落および第5項は略）

- ハイリスクAIシステムのディプロイヤーの義務は以下。（第26条）
 - ハイリスクAIシステムに添付された使用説明書に従ってシステムを使用することを保証するために、適切な技術的措置および組織的措置を講じる。
 - 人間による監督を、必要な能力、訓練、権限を有し、必要なサポートを有する自然人に割り当てる。
 - ディプロイヤーが入力データを管理している範囲内で、ハイリスクAIシステムの意図された目的に照らして、入力データが適切かつ十分に代表的であることを保証する。
 - 使用説明書に基づいて、ハイリスクAIシステムの動作をモニターする。該当する場合には第72条（市場流通後モニタリング）に従ってプロバイダーに情報提供する。
 - 使用説明書に従った使用が、当該システムに健康・安全・基本的権利に対するリスクを提示する恐れがあると考えられる理由がある場合、プロバイダーまたは販売者および関連する市場監視機関に情報提供し、システムの使用を一時停止する。
 - 重大インシデントを特定した場合は直ちに、まずプロバイダーに、そして輸入者または販売者および関連する市場監視機関に情報提供する。
 - ハイリスクAIシステムによって自動生成されたログを、当該ログが管理下にある範囲で、適切な期間、少なくとも6か月間保管する。ただし、適用されるEU法または国内法に別段の定めがある場合を除く。
 - 職場でハイリスクAIシステムを使用する前に、雇用主であるディプロイヤーは、労働者の代表および影響を受ける労働者に、ハイリスクAIシステムの使用の対象となることを情報提供する。
 - 公的機関やEUの機関等であるディプロイヤーは、第49条で言及されている登録義務を遵守する。

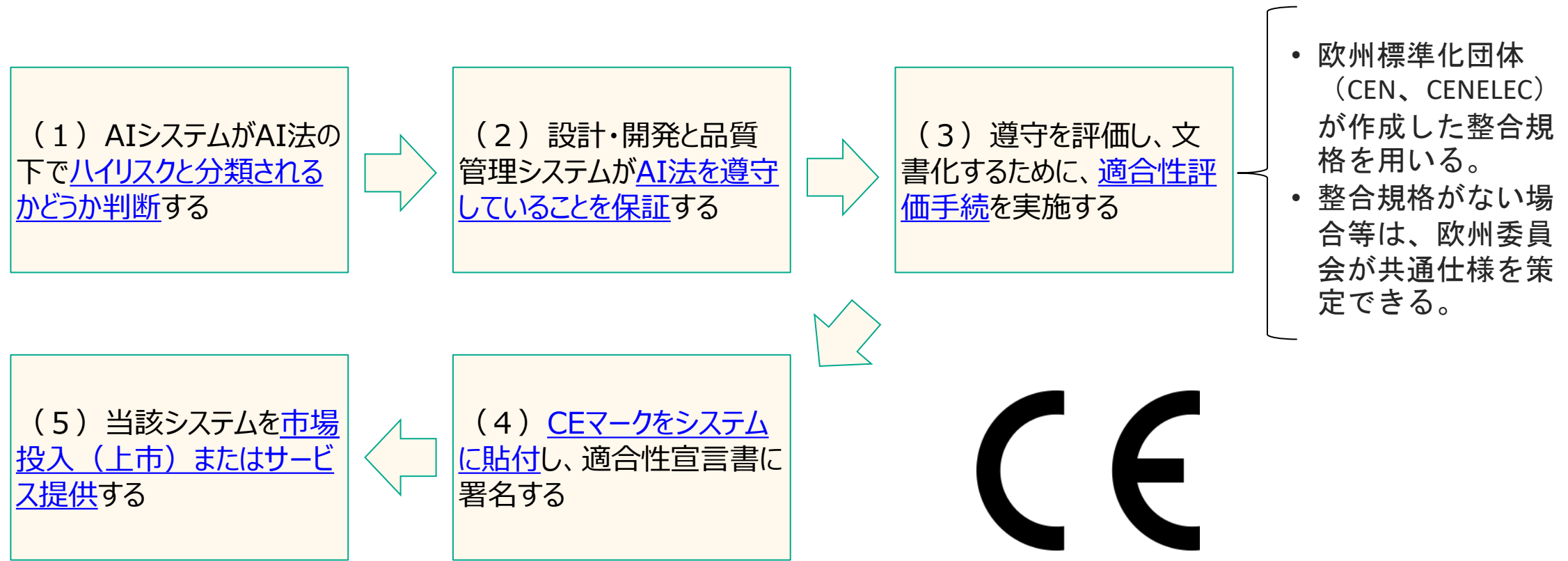
- 第27条 ハイリスク AI システムの基本的人権影響評価
- 1. 第6条第2項で言及されたハイリスクAIシステムをディプロイする前に、Annex IIIの第2項にリスト化された領域での使用を目的としたハイリスクAIシステムを除き、公法によって規律される団体であるディプロイヤー、または公共サービスを提供する民間団体であるディプロイヤー、およびAnnex IIIの第5項 (b) および (c) で言及されているハイリスクAIシステムのディプロイヤーは、当該システムの使用によって生じる可能性のある基本的権利への影響に関する評価を実行するものとする。この目的のために、ディプロイヤーは以下から構成される評価を実行するものとする。
 - (a) ハイリスクAIシステムが意図された目的に沿って使用されるディプロイヤーのプロセスの説明。
 - (b) 各ハイリスクAIシステムが使用される予定の期間と頻度の説明。
 - (c) 特定の状況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グループのカテゴリー。
 - (d) 第13条に従ってプロバイダーから提供された情報を考慮した、本項の (c) に従って特定された自然人またはグループのカテゴリーに影響を与える可能性がある具体的な危害のリスク。
 - (e) 使用説明書に従った、人間による監督措置の実施の説明。
 - (f) 内部ガバナンスおよび苦情処理メカニズムの取り決めを含む、それらのリスクが現実化した場合に講じる措置。
- 2. 第1項に定められた義務は、ハイリスクAIシステムの最初の使用に適用される。同様のケースにおいて、ディプロイヤーは、以前に実施された基本的人権影響評価、またはプロバイダーが実施した既存の影響評価に依存することができる。ハイリスクAIシステムの使用中に、第1項にリスト化された要素のいずれかが変更された、または最新ではなくなったとディプロイヤーが判断した場合、ディプロイヤーは情報を更新するために必要な措置を講じるものとする。
- 3. 本条第1項で言及された評価が実施されたら、ディプロイヤーはその結果を市場監視機関に通知し、通知の一部として本条第5項で言及されている記入済みテンプレートを提出するものとする。第46条第1項で言及されているケースの場合、ディプロイヤーはこの通知義務を免除されうる。
- 4. 本条に定められた義務のいずれかが、規則 (EU) 2016/679 (GDPR) 第35条または指令 (EU) 2016/680 (法執行指令) 第27条に従って実施されるデータ保護影響評価を通じてすでに履行されている場合、本条第1項で言及された基本的人権影響評価はそのデータ保護影響評価を補完するものとする。
- 5. AIオフィスはディプロイヤーが本条に基づく義務を簡略化して遵守できるよう、自動化ツールを含め質問票のテンプレートを開発するものとする。

- 欧州委員会は、ハイリスクAIシステム等の整合規格の標準化要求を欧州標準化団体に発行する。（第40条）
 - EU官報にレファレンスが公開されている整合規格に適合しているハイリスクAIシステム（または汎用目的AIモデル）は、当該規格が要件/義務をカバーする範囲で、AI法で規定されたハイリスクAIシステムの要件（または汎用目的AIモデル/システムミックリスク汎用目的AIモデルの義務）に適合していると推定される。（第1項）
 - 欧州委員会は、不当な遅滞なく、ハイリスクAIシステムの要件（または汎用目的AIモデル/システムミックリスク汎用目的AIモデルの義務）を対象とする標準化要求を、欧州標準化団体（CENやCENELEC）に発行する。（第2項）
 - この標準化要求に基づき作成される整合規格は、Annex I にリスト化された既存のEU整合法令の対象となる製品分野で開発された整合規格との一貫性を含め、明確で一貫性のあるものでなければならない。（第2項）
- 欧州標準化団体が要求に合った整合規格を作成しない場合、欧州委員会は自ら共通仕様を定めることができる。（第41条）
 - 欧州委員会は、欧州標準化団体に整合規格の作成を要求したが、その要求が標準化団体のいずれにも受け入れられない/整合規格が期限内に提出されない等の理由でEU官報に整合規格へのレファレンスが掲載されない場合、ハイリスクAIシステムの要件（または汎用目的AIモデル/システムミックリスク汎用目的AIモデルの義務）について共通仕様を定めることができる。（第1条）
 - この共通仕様に適合しているハイリスクAIシステム（または汎用目的AIモデル）は、当該共通仕様が要件/義務をカバーする範囲で、AI法で規定されたハイリスクAIシステムの要件（または汎用目的AIモデル/システムミックリスク汎用目的AIモデルの義務）に適合していると推定される。（第3項）

第3章 ハイリスクAIシステム： ②ハイリスクAIシステムのCE適合性マーク **I I S E**

○ハイリスクAIシステムのCE適合性マーク（第48条）

- CEマークは、ある製品が当該製品を規制するEU法令の要件を遵守していることを示す。
ハイリスクAIシステムにCEマークを貼付するために、プロバイダーは次の手順を実施する。



出典：欧州委員会資料を和訳、加筆

○ 各ハイリスクAIシステムのプロバイダーに求められる適合性評価は以下。（第43条）

• Annex IのセクションA：

- プロバイダーは、各EU整合法令の下で必要とされる第三者適合性評価に従う。（第43条第3項）
- 各EU整合法令に基づく公認認証機関は、AI法第31条の要件を満たす場合、適合性評価を行うことができる。
- 各EU整合法令により製品製造者が第三者適合性評価からオプトアウト可能な場合は、当該製造者がAI法の要件をカバーする整合規格（または共通仕様）を適用している場合に限り、オプトアウトを行うことができる。

• （Annex IのセクションB： 第112条（評価と見直し） 以外はAI法の対象外）

• Annex IIIの第1項（バイオメトリクス）：

- 整合規格（または共通仕様）を適用する場合、プロバイダーは以下の適合性評価手続のいずれかを選択する。（第43条第1項）
 - （a）内部統制に基づく適合性評価手続。
 - （b）公認認証機関による第三者適合性評価手続。
- 整合規格（または共通仕様）を適用しない/できない場合、プロバイダーは公認認証機関による第三者適合性評価手続に従う。

• Annex IIIの第2項～第8項：

- プロバイダーは、内部統制に基づく適合性評価手続に従う。（第43条第2項）
- 欧州委員会はAnnex IIIの第2項～第8項のハイリスクAIシステムを第三者適合性評価手続に従わせるために第43条2項を修正することができる。その場合、公認認証機関の十分な能力とリソースの可用性を考慮に入れる。（第43条第6項）

・ 特定AIシステムのプロバイダーとディプロイヤーに対する透明性の義務（第50条）

プロバイダーの義務

- ・ プロバイダーは、AIシステムと直接的にやり取りをしている人々に、それが明白でない限り、その旨を情報提供するような設計と開発を保証する。（チャットボットなど）（第1項）
 - ・ ただし、刑事犯罪を検出・防止・捜査・訴追するために法律で承認されたAIシステムを除く。
- ・ 汎用目的AIシステムを含め、合成音声・画像・ビデオ・テキストコンテンツを生成するAIシステムのプロバイダーは、当該システムのアウトプットがAIで生成または加工されたものであることが分かるように、機械可読な形式でマーク付けされることを保証する。（いわゆる電子透かし）（第2項）
 - ・ ただし、当該AIシステムが標準的な編集のための支援機能を実行する場合、ディプロイヤーによって提供される入力データやそのセマンティクスを実質的に変えない場合、または刑事犯罪を検出・防止・捜査・訴追するために法律で承認されている場合は除く。

ディプロイヤーの義務

- ・ 感情認識システムや生体カテゴライゼーションシステムのディプロイヤーは、それらのシステムの対象となる人々に、その旨を情報提供する。（第3項）
 - ・ ただし、刑事犯罪を検出・防止・捜査・訴追するために法律で許可されている場合を除く。
- ・ ディープフェイクに該当する画像・音声・ビデオコンテンツを生成または加工するAIシステムのディプロイヤーは、それらのコンテンツがAIで生成または加工されたものであることを開示する。（第4項第1段落）
 - ・ ただし、刑事犯罪を検出・防止・捜査・訴追するために法律によって使用が承認されている場合は除く。また、当該コンテンツが明らかに芸術的・創造的・風刺的・フィクション的・類似的な作品/プログラムの一部を形成している場合、上記の透明性義務は、当該作品の表示/享受を妨げない適切な方法での開示に限定される。
- ・ 公益に関する事項を公衆に知らせることを目的として公開されるテキスト（ニュース記事等）を生成または加工するAIシステムのディプロイヤーは、それらのテキストがAIで生成または加工されたものであることを開示する。（第4項第2段落）
 - ・ ただし、刑事犯罪を検出・防止・捜査・訴追するために法律によって使用が承認されている場合は除く。また、AIで生成されたコンテンツが人間によるレビューもしくは編集管理のプロセスを受けており、自然人もしくは法人がコンテンツの公開の編集責任を負っている場合も除く。

- 汎用目的AIモデルのプロバイダーには、以下の義務が課される。（第53条第1項）
 - (a) 学習およびテストのプロセスと評価の結果を含む当該モデルの技術文書を作成し、最新の状態に保つ。これには、要求に応じてAIオフィスおよび国内所轄機関に提供する目的で、少なくともAnnex XIに規定されている情報を含める。
 - (b) 汎用目的AIモデルを自らのAIシステムに組み込むことを意図するAIシステムの下流プロバイダーに対して、以下のような情報と文書を作成し、最新の状態に保ち、利用可能とする。
 - (i) AIシステムのプロバイダーが当該モデルの能力と制限を十分に理解し、本規則に基づく義務を遵守できるようにする。
 - (ii) 少なくとも、Annex XIIIに規定されている要素を含む。
 - (c) 著作権および関連する権利に関するEU法を遵守し、特に指令 (EU) 2019/790（著作権指令）の第4条第3項に基づいて表明された権利の留保を、最先端の技術を用いる等により、特定し遵守する方針を導入するための方針を導入する。
 - (d) AIオフィスが提供するテンプレートに従って、汎用目的AIモデルの学習に使用されるコンテンツについての十分に詳細な概要を作成し、公開する。
- 上記 (a) および (b) の義務は、無料のオープンソースライセンスの下でリリースされており、重みなどのパラメータ、モデルアーキテクチャに関する情報、モデルの使用法に関する情報が公開されているAIモデルのプロバイダーには適用されない。ただし、この例外はシステミックリスクのある汎用目的AIモデルには適用されない。（第53条第2項）
- 汎用目的AIモデルのプロバイダーは、整合規格が発行されるまで、義務の遵守を実証するために、実践規範に依拠できる。欧州整合規格を遵守すると、その規格が義務をカバーする範囲で、プロバイダーに適合性の推定が認められる。承認された実践規範に準拠していない、または欧州整合規格を遵守していないプロバイダーは、欧州委員会による評価のために、遵守の十分な代替手段を実証しなければならない。（第53条第4項）

第5章 汎用目的AIモデル： ⑤ システミックリスクのある汎用目的AIモデル I I S E

- システミックリスクのある汎用目的AIモデルとしての分類（第51条）
 - 汎用目的AIモデルは、以下のいずれかの条件を満たす場合、システミックリスクのある汎用目的AIモデルとして分類される。（第1項）
 - （a）当該汎用目的AIモデルが、指標およびベンチマークを含め、適切な技術ツールおよび方法論に基づいて評価された、ハイインパクトな能力を備えている。
 - （b）職権による、または科学パネルからの適格な警告を受けた欧州委員会の決定に基づき、当該汎用目的AIモデルが、Annex XIIIに定められた基準を考慮して、（a）に規定されたものと同等の能力または影響を有する。
 - 汎用目的AIモデルは、浮動小数点演算（FLOP）で測定された、学習に用いられた累積計算量が10の25乗を超える場合、上記（a）に従ってハイインパクトな能力を備えていると推定される。（第2項）
- ハイインパクトな能力、システミックリスクの定義
 - 「ハイインパクトな能力（high-impact capabilities）」とは、最先端の汎用目的AIモデルが記録している能力と同等またはそれを超える能力を意味する。（第3条（64））
 - 「システミックリスク（systemic risk）」とは、汎用目的AIモデルのハイインパクトな能力に特有のリスクであって、そのリーチによって、または公衆衛生、安全、治安、基本的権利、もしくは社会全体に対する実際もしくは合理的に予見可能な悪影響によって、EU市場に重大な影響を与え、かつバリューチェーン全体に大規模に伝播しうるものを意味する。（第3条（65））

第5章 汎用目的AIモデル： ⑤ システミックリスクのある汎用目的AIモデル I I S E

・ システミックリスクのある汎用目的AIモデルの指定基準（Annex XIII）

- 汎用目的AIモデルが第51条第1項 (a) に規定されたものと同等の能力または影響を有するかどうかを判断するために、欧州委員会は以下の基準を考慮するものとする。
- (a) モデルのパラメータの数。
- (b) データセットの品質またはサイズ。たとえばトークンを通じて測定されるもの。
- (c) モデルの学習に使用される計算量。浮動小数点演算で測定されるもの、または学習の推定コスト、学習に必要な推定時間、もしくは学習の推定エネルギー消費などの他の変数の組合せによって示されるもの。
- (d) モデルの入力と出力のモダリティ（テキストからテキスト（大規模言語モデル）、テキストから画像、マルチモダリティ、各モダリティのハイインパクトな能力を決定するための最新のしきい値など）、および特定の種類の入力と出力（生物学的配列など）。
- (e) モデルの能力のベンチマークと評価。これには、追加の学習を必要としないタスクの数、新たな異なるタスクを学習する適応性、自律性と拡張性のレベル、アクセスできるツールの考慮が含まれる。
- (f) そのリーチによりEU域内市場にハイインパクトを与えるかどうか。これは、EU域内に拠点のある10,000以上の登録されたビジネスユーザーが利用できるようになった場合に推定されるものとする。
- (g) 登録されたエンドユーザーの数。

・ システミックリスクのある汎用目的AIモデルの手続（第52条）

- プロバイダーは、汎用目的AIモデルが第51条第1項（a）の条件を満たす場合、遅滞なく（その要件が満たされた後、または要件が満たされると知ってから2週間以内に）欧州委員会に通知する。その通知には、関連要件が満たされていることを証明するために必要な情報を含める。（第1項）
 - ただし、上記（a）の条件を満たす汎用目的AIモデルのプロバイダーは、例外的に、当該モデルがその特有の特性によりシステミックリスクを示さないため、システミックリスクのある汎用目的AIモデルとして分類されるべきではないことを証明するために、欧州委員会に通知とともに、十分に実証された主張を提示できる。（第2項）
- 欧州委員会は、通知されていない、システミックリスクを示す汎用目的AIモデルを認識した場合、それをシステミックリスクのあるモデルとして指定できる。（第1項）
 - 欧州委員会は、職権により、または科学パネルからの適格な警告に従って、Annex XIIIに定められた基準に基づいて、汎用目的AIモデルをシステミックリスクを示すものとして指定できる。（第4項）
- 欧州委員会はシステミックリスクのある汎用目的AIモデルのリストを公開・維持する。（第6項）

- システミックリスクのある汎用目的モデルのプロバイダーには、（前述の汎用目的AIモデルのプロバイダーの義務に加えて）以下の義務も課される（第55条第1項）。
 - （a）システミックリスクの特定と軽減を目的とした当該モデルの敵対的テストの実施と文書化を含め、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を実行する。
 - （b）システミックリスクのある汎用目的AIモデルの開発、市場投入、または使用に起因する可能性のあるシステミックリスクを、その発生源を含めてEUレベルで評価し、軽減する。
 - （c）重大インシデントとそれらに対処するための是正措置に関する関連情報を追跡し、文書化し、不当な遅滞なくAIオフィス、および必要に応じて国内所轄機関に報告する。
 - （d）システミックリスクのある汎用目的AIモデルおよび当該モデルの物理インフラストラクチャに対して十分なレベルのサイバーセキュリティ保護を保証する。
- システミックリスクのある汎用目的AIモデルのプロバイダーは、整合規格が発行されるまで、上記の義務の遵守を実証するために、実践規範（codes of practice）に依拠できる。欧州整合規格を遵守すると、その規格が義務をカバーする範囲で、プロバイダーに適合性の推定が認められる。承認された実践規範に準拠していない、または欧州整合規格を遵守していないシステミックリスクのある汎用目的AIモデルのプロバイダーは、欧州委員会による評価のために、遵守の十分な代替手段を実証しなければならない。（第55条第2項）

- 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て、AI法の適切な適用に貢献するために、EUレベルでの実践規範の策定を奨励し、促進する。（第1項）
 - AIオフィスと欧州AI会議は、実践規範が少なくとも第53条と第55条に規定された義務をカバーすることの保証を目指す。これには以下の 이슈が含まれる。（第2項）
 - (a) 第53条第1項（a）および（b）で言及された情報が、市場および技術の発展を考慮して最新の状態に保たれることを保証する手段。
 - (b) 学習に使用されるコンテンツに関する概要の十分に詳細なレベル。
 - (c) 必要に応じて、その発生源を含む、EUレベルでのシステミックリスクの種類と性質の特定。
 - (d) EUレベルでのシステミックリスクの評価と管理のための措置、手続、および様式（それらの文書化を含む）。それらは、リスクの重大度と確率を考慮し、AIバリューチェーンに沿ってそのようなリスクが出現し現実化する仕方の観点からそれらのリスクに取り組む際の具体的な課題を考慮して、当該リスクに比例したものであるものとする。
 - AIオフィスは、汎用目的AIモデルのすべてのプロバイダーおよび関連する国内所轄機関に、実践規範の策定に参加するよう招待できる。市民社会組織、産業界、学界、および下流プロバイダーや独立した専門家などのその他の関連する利害関係者がこのプロセスをサポートすることができる。（第3項）
 - 欧州委員会は、実施法令によって実践規範を承認し、実践規範にEU域内での一般的な有効性を与えることができる。（第6項）
 - AIオフィスは、汎用目的AIモデルのすべてのプロバイダーに対し、実践規範に準拠するよう呼びかけることができる。（第7項）
 - 実践規範は、遅くとも2025年5月2日までに準備されるものとする。2025年8月2日までに実践規範を完成できない場合、またはAIオフィスによる評価の結果、実践規範が十分でないと判断した場合、欧州委員会は、本条第2項に規定された 이슈を含め、第53条および第55条に規定された義務を履行するための共通ルールを実施法令により規定できる。（第9項）

- AI法の適切な運用については、基本的にEU加盟国の[国内所轄機関](#)（national competent authority：市場監視機関等）が[プロバイダー等のオペレーターの監督](#)を行う。加盟国間で齟齬が生じた場合や、加盟国間で情報共有等が必要な場合には、[EUレベルで対処](#)する。ただし、[汎用目的AIモデル](#)に関しては、[欧州委員会/AIオフィスが監督](#)を行う。
- 欧州委員会
 - 市場や技術の発展等に合わせて[AI法の条文を修正](#)したり、詳細ルールを定めるための[委任法令](#)を採択する権限を持つ。
 - AI法を適用する上での様々な[詳細ルール](#)（共通仕様、共通ルール等）を定める[実施法令](#)を採択する権限を持つ。
 - ハイリスクAIシステムの分類手順・ユースケースや、その他AI法の実施に関する[ガイドライン](#)を作成する。（第6条第5項、第96条）
- AIオフィス（欧州人工知能オフィス）

- 「AIオフィス（AI Office）」とは、2024年1月24日の欧州委員会決定により設立された欧州人工知能オフィスによって実行される[AIシステムおよびAIガバナンスの実装、モニタリング、監督](#)に貢献する欧州委員会の機能を意味する。本規則におけるAIオフィスへの言及は、欧州委員会への言及として解釈されるものとする。（第3条（47））
 - 欧州委員会は、AIオフィスを通じてAI分野におけるEUの専門知識と能力を開発するものとする。（第64条第1項）
- 欧州AI会議（European Artificial Intelligence Board）
 - [各加盟国から各1人の代表者](#)によって構成される。[欧州データ保護監察官（EDPS）](#)はオブザーバーとして参加する。[AIオフィス](#)も欧州AI会議の会合に参加するが、議決権は持たない。AIオフィスは欧州AI会議の事務局となる。（第65条）
 - 欧州AI会議はAI法の一貫した効果的な適用を促進するために、[欧州委員会と加盟国に助言し、支援](#)する。この目的のために、国内所轄機関間の調整、市場監視機関の共同活動の支援、専門知識・ベストプラクティスの共有、汎用目的AIモデルに関するルール実施のアドバイス等を行う。（第66条）
- 諮問フォーラム（Advisory forum）
 - 欧州委員会は産業界、中小企業、市民社会、学界等からAI分野で専門知識を有する関係者を諮問フォーラムのメンバーとして指名する。諮問フォーラムは、欧州AI会議および欧州委員会に技術的専門知識を提供し、助言を行う。（第67条）
- 独立した専門家から成る科学パネル（Scientific panel of independent experts）
 - 欧州委員会が選出した、AI分野での最新の科学的・技術的専門知識を有し、プロバイダーからの独立性が確保された専門家で構成される。汎用目的AIモデルに対するAI法の実施（システミックリスクの警告）等についてAIオフィスを支援する。（第68条）

- 第72条 プロバイダーによるハイリスクAIシステムの市場流通後モニタリングと市場流通後モニタリング計画
 - 1. プロバイダーは、当該AI技術の性質とハイリスクAIシステムのリスクに比例した仕方で、市場流通後モニタリングシステムを作成し、文書化するものとする。
 - 2. 市場流通後モニタリングシステムは、ディプロイヤーから提供されうる、または他のソースから収集されうる、ハイリスクAIシステムのライフタイムに渡るパフォーマンスに関する関連データを積極的かつ体系的に収集、文書化、分析し、プロバイダーが第3章第2節で規定されている要件の継続的遵守を評価できるようにするものとする。関連する場合、市場流通後モニタリングには、他のAIシステムとの相互作用の分析が含まれるものとする。この義務は、法執行機関であるディプロイヤーのセンシティブ業務データには適用されないものとする。
 - 3. 市場流通後モニタリングシステムは、市場流通後モニタリング計画に基づくものとする。市場流通後モニタリング計画は、Annex IVで言及されている技術文書の一部であるものとする。欧州委員会は、市場流通後モニタリング計画のテンプレートと当該計画に含まれる要素のリストを策定する詳細な規定を定めた実施法令を2026年2月2日までに採択するものとする。その実施法令は、第98条第2項で言及されている審査手続に従って採択されるものとする。
 - 4. Annex IのセクションAで言及されている法令の対象となるハイリスクAIシステムについて、当該法令の下で市場流通後モニタリングシステムと計画がすでに確立されている場合、それが同等な保護レベルを達成するならば、一貫性を確保し、重複を避け、追加の負担を最小限に抑えるために、プロバイダーは本条第1項、第2項および第3項に記載されている要素を第3項で言及されたテンプレートを用いて、必要に応じて、当該法令の下での既存のモニタリングシステムと計画に統合する選択肢を有するものとする。

第1段落は、EU金融サービス法に基づく内部ガバナンス、取決めまたはプロセスに関する要件の対象となる金融機関によって市場投入またはサービス提供される、Annex IIIの第5項で言及されているハイリスクAIシステムにも適用されるものとする。

- 重大インシデントの報告（第73条）
 - EUに市場投入された[ハイリスクAIシステムのプロバイダーは、重大インシデントを、当該インシデントが発生した加盟国の市場監視機関に報告](#)する。（第1項）

- 「重大インシデント（serious incident）」とは、直接的または間接的に以下のいずれかにつながるAIシステムのインシデントまたは誤動作を意味する。（第3条（49））
 - （a）人の死亡、または人の健康への重大な危害。
 - （b）重要なインフラストラクチャの管理と運用の深刻で不可逆的な混乱。
 - （c）基本的権利を保護することを目的としたEU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危害。
 - 重大インシデントの報告は、プロバイダーがAIシステムと当該重大インシデントの間の因果関係を確認した直後に、またはそのような関係の合理的な可能性を確認した直後に、いずれにしてもプロバイダーまたは（該当する場合）ディプロイヤーが重大インシデントに[気づいた時から15日以内](#)になされるものとする。この報告期間は、重大インシデントの重大度を考慮する。（第2項）
 - ただし、[広範な侵害または第3条\(49\)\(b\)の重大インシデント](#)が発生した場合には、報告は直ちに、プロバイダーまたは（該当する場合）ディプロイヤーがインシデントに[気づいた時から2日以内](#)に提供されるものとする。（第3項）
 - また、[人が死亡](#)した場合には、プロバイダーまたはディプロイヤーがAIシステムと重大インシデントの間の因果関係を確認した直後に、またはその疑いが生じた直後に、プロバイダーまたは（該当する場合）ディプロイヤーが重大インシデントに[気づいた時から10日以内](#)に報告が提供されるものとする。（第4項）
 - タイムリーな報告を保証するために必要な場合、プロバイダーまたは（該当する場合）ディプロイヤーは、[不完全な最初の報告](#)（速報）を提出し、その後に[完全な報告](#)（確報）を提出することができる。（第5項）
 - プロバイダーは、重大インシデントの報告後、遅滞なく、重大インシデントおよび当該AIシステムに関して必要な調査を実施する。これには、当該インシデントの[リスク評価と是正措置](#)を含める。（第6項）

- 第85条 市場監視機関に異議を申し立てる権利（Right to lodge a complaint with a market surveillance authority）
 - 他の行政的または司法的救済を損なうことなく、本規則の規定の侵害があったとみなす根拠のある自然人または法人は、関連する市場監視機関に異議を提出することができる。
 - 規則 (EU) 2019/1020（製品の市場監視とコンプライアンスに関する規則）に従い、かかる苦情は市場監視活動を実施する目的で考慮され、市場監視機関がそのために確立した専用手続に従って取り扱われるものとする。
- 第86条 個人に対する意思決定について説明を受ける権利（Right to explanation of individual decision-making）
 - 1. Annex III（第2項を除く）にリスト化されているハイリスクAIシステムからの出力に基づいてディプロイヤーが下す決定であって、当該人物に自分の健康、安全もしくは基本的権利に悪影響を与えると考えられる仕方では法的効果を生み出すか、または同様の重大な影響を及ぼす決定の対象となる、影響を受ける人物は、意思決定手続における当該AIシステムの役割と下された決定の主要素について、ディプロイヤーから明確で意味のある説明を得る権利を有するものとする。
 - 2. 第1項は、EU法またはEU法を遵守する国内法に基づき、同項の下での義務の例外または制限が適用されるAIシステムの使用には適用されないものとする。
 - 3. 本条は、第1項で言及された権利がEU法で別途規定されていない範囲にのみ適用されるものとする。
- 第87条 違反の報告と報告者の保護（Reporting of infringements and protection of reporting persons）
 - 指令 (EU) 2019/1937（EU法違反の報告者の保護に関する指令）は、本規則の違反の報告およびそのような違反を報告した者の保護に適用されるものとする。

- 特定要件の自主的適用のための行動規範（第95条）
 - AIオフィスと加盟国は、第3章第2節で規定された要件（ハイリスクAIシステムの要件）の一部または全部について、ハイリスク以外のAIシステムに自主的に適用することの促進を目的とした行動規範の作成を、推奨および促進する。（第1項）
 - AIオフィスと欧州AI会議は、以下のような特定要件について、すべてのAIシステムに自主的に適用すること（ディプロイヤーによるものを含む）を促進することを目的とした行動規範の作成を、推奨および促進する。（第2項）
 - （a）EUの「信頼できるAIに関する倫理ガイドライン」に規定されている該当する要素。
 - （b）AIシステムが環境の持続可能性に与える影響を評価し、最小限に抑える。これには、エネルギー効率の高いプログラミングや、AIの効率的な設計・学習・使用のための技術も含まれる。
 - （c）AIリテラシー、特にAIの開発・運用・使用に携わる人々のリテラシーを促進する。
 - （d）包括的で多様な開発チームの設立やそのプロセスへの利害関係者の参加の促進などを通じて、AIシステムの包括的で多様な設計を促進する。
 - （e）障害者のアクセシビリティやジェンダー平等など、脆弱な人々またはグループに対するAIシステムの悪影響を評価し、防止する。
 - 行動規範は、市民社会組織や学会など関心あるステークホルダーやその代表組織の関与を含め、AIシステムの個々のプロバイダーもしくはディプロイヤー、もしくはそれらを代表する組織、またはその両者が作成できる。行動規範は、当該システムの意図された目的の類似性を考慮に入れて、1つまたは複数のAIシステムを対象とすることができる。（第3項）
 - AIオフィスと加盟国は、行動規範の作成を推奨および促進する際に、新興企業を含む中小企業の特定の利益とニーズを考慮に入れる。（第4項）

- 本規則の実施に関する欧州委員会のガイドライン（第96条）
 - 欧州委員会は、本規則の実際の実施、特に以下に関するガイドラインを作成する。（第1項）
 - (a) 第8条～第15条、第25条で言及された要件と義務の適用 【②ハイリスクAIシステム】
 - (b) 第5条で言及された禁止慣行 【①禁止AIシステム】
 - (c) 実質的な変更に関連する規定の実際の実施 【②ハイリスクAIシステム】
 - (d) 第50条に定められた透明性義務の実際の実施 【③透明性の義務のあるAIシステム】
 - (e) 本規則とAnnex I にリスト化されたEU整合法令、およびその他の関連するEU法との関係に関する詳細情報（執行の一貫性を含む） 【②ハイリスクAIシステム】
 - (f) 第3条（1）に規定されたAIシステムの定義の適用。
 - 欧州委員会は、ガイドラインを発行する際、新興企業を含む中小企業、地方公共団体、および本規則によって最も影響を受ける可能性が高い分野のニーズに特に注意を払う。（第1項）
 - ガイドラインは、一般に認知されているAIに関する最先端技術、第40条・第41条にいう整合規格と共通仕様、EU整合法令に基づき定められた整合規格や技術仕様を適切に考慮する。（第1項）
 - 欧州委員会は、加盟国やAIオフィスの要求に応じて、または自らの主導で、必要な場合にはガイドラインを更新する。（第2項）

・ 禁止AI・ハイリスクAI・透明性の義務のあるAIに関連した罰則（第99条）

違反事由	制裁金額（加盟国がルールを決め、違反者に科す）
第5条（禁止されるAI慣行）で規定されたAI慣行の禁止を遵守しない場合。	3500万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の7%以下の金額、もしくはいずれか高額の方の制裁金（administrative fines）
以下を遵守しない場合。 (a) 第16条に基づくプロバイダーの義務 (b) 第22条に基づく権限のある代理人の義務 (c) 第23条に基づく輸入者の義務 (d) 第24条に基づく販売者の義務 (e) 第26条に基づくディプロイヤーの義務 (f) 第31条、第33条第1項、第3項、第4項、または第34条に基づく公認認証機関の要件および義務 (g) 第50条に基づくプロバイダーおよびディプロイヤーに対する透明性義務	1500万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の3%以下の金額、もしくはいずれか高額の方の制裁金
要求への回答において公認認証機関および国内所轄機関に不正確、不完全、または誤解を招く情報を提供した場合。	750万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の1.5%以下の金額、もしくはいずれか高額の方の制裁金
新興企業を含む中小企業の場合。	制裁金は、上記で示されたパーセントまたは金額のいずれか低額の方を上限とする

（筆者作成）

• 汎用目的AIモデルのプロバイダーに対する罰金（第101条）

違反事由	罰金額（欧州委員会が違反者に科す）
汎用目的AIモデルのプロバイダーが故意または過失で以下のことを行ったと欧州委員会が判断した場合。 （a）本規則の関連規定に違反した。 （b）第91条に基づく文書または情報の要求に従わなかった、または不正確、不完全もしくは誤解を招く情報を提供した。 （c）第93条に基づいて要求された措置に従わなかった。 （d）第92条に基づく評価を実施する目的で、汎用目的AIモデルまたはシステミックリスクのある汎用目的AIモデルへのアクセスを欧州委員会に提供しなかった。	直前の会計年度における 世界全体における売上総額の3% または 1500万ユーロ のいずれか高額の方を超えない罰金（fines）

（筆者作成）

- 既に市場投入またはサービス提供されているAIシステムと既に市場投入されている汎用目的AIモデル（第111条）
 - Annex Xにリスト化された法令（シェンゲン情報システム、ビザ情報システム等）によって構築された大規模ITシステムのコンポーネントであるAIシステムであって、2027年8月2日より前に市場投入またはサービス提供されたものは、2030年12月31日までにAI法を遵守する。（第1項）
 - 上記のシステム以外の[ハイリスクAIシステム](#)であって、[2026年8月2日より前に市場投入](#)またはサービス提供されたハイリスクAIシステムのオペレーターには、[その日以降それらのシステムの設計または意図された目的に重大な変更が加えられる場合に限り、AI法が適用](#)されるものとする。いずれにしても、公的機関による使用を目的としたハイリスクAIシステムのプロバイダーおよびディプロイヤーは、2030年8月2日までに、AI法の要件と義務を遵守するために必要な措置を講じる。
 - 2025年8月2日より前に市場投入された[汎用目的AIモデルのプロバイダー](#)は、2027年8月2日までに本規則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。
- 発効と適用（第113条）
 - AI法は、EU官報上で公示された翌日から20日目の日に発効する。
 - AI法は、[2026年8月2日から適用](#)される。ただし、
 - (a) 第1章（一般規定）と第2章（[禁止されるAI慣行](#)）は、[2025年2月2日から適用](#)される。
 - (b) 第3章第4節（公認認証当局と公認認証機関）、第5章（[汎用目的AIモデル](#)）、第7章（ガバナンス）、第12章（罰則）、および第78条（機密保持）は、第101条（汎用目的AIモデルのプロバイダーに対する罰金）を除き、[2025年8月2日から適用](#)される。
 - (c) 第6条第1項（[Annex I 関連のハイリスクAIシステム](#)）および本規則の対応する義務は、[2027年8月2日から適用](#)される。
 - AI法は、その全部について拘束力があり、すべての加盟国において直接適用される。

- 小泉 雄介 （株）国際社会経済研究所 主幹研究員 yusuke-koizumi@nec.com
- 専門領域：
 - プライバシー/個人情報保護、国民ID/マイナンバー制度、海外政策動向調査、途上国市場調査
- 略歴：
 - 1998年 （株）NEC総研入社 ・ 2008年7月 日本電気（株）に出向
 - 2010年7月 （株）国際社会経済研究所（旧NEC総研）に復帰
 - 2012年～ 電子情報技術産業協会（JEITA）個人データ保護専門委員会客員
- 主な著書
 - 『国民ID 導入に向けた取り組み』（共著、NTT出版、2009年）
 - 『[現代人のプライバシー](#)』（共著、NEC総研、2005年）
 - 『経営戦略としての個人情報保護と対策』（共著、工業調査会、2002年） 等
- 主な論文
 - 「[『国民IDの原則』の素描：選択の自由を手放さないために](#)」（日本セキュリティ・マネジメント学会誌2023年度第2号）
 - 「[感情認識の倫理的側面：データ化される個人の終着点](#)」（同学会誌2022年度第2号）
 - 「[中央銀行デジタル通貨における個人情報保護と日本での発行モデル](#)」（同学会誌2021年度第2号）
 - 「[AI社会における「自由」と「安全」のトレードオフ：顔認識技術のケーススタディ](#)」（同学会誌2020年度第2号）
 - 「[『快適で安全』な監視社会—個人の自由が保障されなくていいのか](#)」（岩波『世界』2019年6月号）等

I I S E