

EUのAI法（AI規則）改正の概要

2026年 9月 18日

（株）国際社会経済研究所 小泉 雄介

※本資料は「EUのAI法（AI規則）の概要」 <https://www.i-ise.com/jp/information/media/2024/240718.pdf> の改訂・追記版です。

※AI法（2024年5月制定）からの改正箇所は赤字で示しています。

目 次

- 1．主要国のAI規制政策の比較とAIリスク・対策の潮流
- 2．EUのAI法の制定および改正経緯と今後の予定
- 3．AI法の改正点
- 4．AI法の概要（改正点の反映版）
- 5．AI法のガイドライン・実践規範・整合規格
- 6．EUのクラウド・AI開発法案、サイバーセキュリティとAIに関する行動計画

1．主要国のAI規制政策の比較とAIリスク・対策の潮流

主要国のAI規制政策の比較

	米国 	EU 	英国 	中国 	日本 
AI所轄官庁	大統領府／商務省 等	欧州委員会通信総局	内閣府	国務院／国家インターネット情報弁公室 等	内閣府／総務省／経済産業省／デジタル庁
安全性機関	CAISI	AI Office	UK AISI	中国AI開発安全ネットワーク	J-AISI
主なAI事業者	OpenAI, Anthropic, Google, MS, Meta, xAI 等	Mistral AI(仏), Aleph Alpha(独), Black Forest Labs(独) 等	Google DeepMind 等	DeepSeek, Alibaba, Moonshot AI 等	SB, NTT, NEC, 富士通, PFN 等
AI規制法令 (ハードロー)	大統領令14409／州法 (CA, NY, IL等) ※連邦法案準備中	AI法	なし	生成AIサービス管理暫定弁法／AI生成成コンテンツ標示弁法／インターネット情報サービス深度合成管理規定／インターネット情報サービスアルゴリズム推薦管理規定／人工知能擬人化双方向サービス管理暫定弁法 等	AI推進法
AI規制ガイドライン (ソフトロー)	AIリスクマネジメントフレームワーク (AI RMF)	AI法ガイドライン・実践規範	AI白書の5原則／AIとデータ保護ガイダンス	AI安全ガバナンスフレームワーク2.0／AIアプリケーション倫理・安全ガイドライン 等	AI事業者ガイドライン
規制の重点	国家安全保障	製品安全性・人権保護	セキュリティ全般 (国家安全保障/安全性・人権保護)	社会秩序	イノベーションとリスク対応のバランス
規制の強弱	中国  (国家統制) EU  (事前規制) 米国  (事後規制) 日本  (バランス) 英国  (pro-innovation) 規制強 ←  → 規制弱				
ロードマップ	英国AI白書 (23/3) 米国バイデンAI大統領令 (23/10) HAIP国際指針 (23/10) 英国AIS設立/英国AIサミット (23/11) HAIP報告枠組み (25/2) 日本AI推進法の公布 (25/6) EU AI法実践規範 (25/7) 中国AI安全ガバナンスフレームワーク2.0 (25/9) 日本AI事業者ガイドライン(24/4) EU AI法の制定 (24/5) 米国AI連邦法立法勧告 (26/3) 米国トランプ大統領令14409 (26/6) Anthropic製品への米国輸出管理規制(26/6) EU AI法ハイリスクAI適用開始 日本AI推進法の改正 (?) 米国AI連邦法の制定 (?) CA/NY州AI規制州法(25/9,12) EU AI法改正案 (25/11) 2023年 2024年 2025年 2026年 2027年 2028年				

2021年4月:EU AI法案公表 2022年11月:ChatGPT無料公開 2024年6月:EU AI法制定 2026年4月:Claude Mythos限定公開

①従来からのAIリスク

(a) 身体や生命の安全へのリスク

- ・ 産業機械/自動運転車/医療機器等

(b) 基本的人権へのリスク

- ・ プライバシー/思想等の自由
- ・ プロファイリング/自動意思決定
- ・ 生体認識
- ・ FAT (公平性/アカウンタビリティ/透明性)

○AIリスク対策 (①従来リスク対策、EU AI法案時点)

- ・ リスクベースでのAIシステム分類
 - ・ 禁止AI慣行
 - ・ ハイリスクAI
 - ・ 透明性義務AI
- ・ 分類に応じたリスク対策 (下記はハイリスクAI)
 - ・ リスク管理システム構築
 - ・ データガバナンス実施
 - ・ 技術文書の作成
 - ・ トレーサビリティ確保
 - ・ 透明性と情報提供
 - ・ 人間による監督
 - ・ サイバーセキュリティ対策
 - ・ インシデント報告
 - ・ 適合性マーク貼付／第三者評価

②汎用目的AIによる新たなリスク
(主に個人へのリスク)

(a) 開発者に起因

- ・ 学習データでの個人情報/著作権侵害リスク
- ・ ハルシネーション
- ・ 青少年等の依存リスク

(b) 利用者に起因

- ・ 偽動画/ディープフェイク
- ・ 著作権侵害コンテンツ

○AIリスク対策 (EU AI法)

- ・ ①従来リスクへの対策
- +
- ・ ②汎用目的AIリスクへの対策
 - ・ 技術文書の作成
 - ・ 下流プロバイダーへの情報提供
 - ・ 著作権保護
 - ・ 学習データの透明性
- +
- ・ ③システミックリスクへの対策

③フロンティアAIによる新たなリスク
(社会全体へのリスク=システミックリスク)

(a) 攻撃者によるAI悪用リスク

- ・ サイバー攻撃
- ・ CBRN (化学/生物/放射線/核) 兵器
- ・ 人間の操作/民主主義への介入

(b) AI自体の誤動作リスク

- ・ 制御の喪失/ミスアライメント/AIの暴走

(c) その他の社会的リスク

- ・ 労働市場への影響
- ・ 人間の自律性の低下/AIへの依存

③システミックリスク対策 (EU AI法/米州法/国際AI安全性レポート)

- ・ システミックリスク管理策の文書化 (安全性・セキュリティフレームワーク)
- ・ システミックリスク評価と軽減
- ・ インシデント報告
- ・ モデルのサイバーセキュリティ対策
- ・ モデル概要レポート公開
- ・ 内部告発者保護 等

2. AI法の制定および改正経緯と今後の予定

- 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。
 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
- EU理事会は2022年12月に合意案（general approach）を採択。欧州議会は2023年6月14日の総会で議会修正案を採択。その後、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。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、AI Act）」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、その20日後（2024年8月1日）に発効。
 - 「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) (Text with EEA relevance)」
 - <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

AI法（AI規則）の発効後の経緯と今後の予定（1/2）

- 2025年2月2日、AI法の「第1章 一般規定」と「第2章（第5条）[禁止されるAI慣行](#)」が適用開始。
 - 欧州委員会は2025年2月4日、「AI法で規定された禁止AI慣行に関するガイドライン」を公表。
 - 欧州委員会は2025年2月6日、「AIシステムの定義に関するガイドライン」を公表。
- 2025年8月2日、AI法の「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9章第78条 機密保持」、「第11章 [罰則（「第101条 汎用目的AIモデルのプロバイダーに対する罰金」を除く）](#)」が適用開始。
 - 欧州委員会は2025年7月18日、「AI法で規定された汎用目的AIモデルの義務の範囲に関するガイドライン」を公表。
 - ステークホルダーにより2025年7月10日に「[汎用目的AIモデル実践規範](#)」が策定・公表。8月1日に欧州委員会が承認。
 - 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日までに義務を遵守](#)することが必要。
- 2025年11月19日、欧州委員会は「[AIに関するデジタル・オムニバス規則案](#)」を公表。[AI法の改正案](#)を含む。
 - 欧州議会とEU理事会はそれぞれ審議を行い、欧州議会は2026年3月26日に議会修正案（negotiating position）を、EU理事会は3月13日に理事会合意案（general approach）を採択。その後、欧州委員会も交えた三者協議を行い、5月7日に両者は修正案について暫定合意に至った。
 - AI法改正案は法的・言語的な修正後、6月16日に欧州議会総会で承認、[6月29日](#)にEU理事会で承認されたことにより、「[AIに関するデジタル・オムニバス規則](#)」の正式な制定となった。
 - その後、[2026年7月24日にEU官報に公表](#)され、その3日後（[7月27日](#)）に発効した。
 - 「Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) (Text with EEA relevance)」
 - <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>

AI法（AI規則）の発効後の経緯と今後の予定（2/2）

- 2026年8月2日、AI法の「第4章（第50条）[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9章 市場流通後モニタリング、情報共有、市場監視（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](#)を含む）」「第11章第101条 [汎用目的AIモデルのプロバイダーに対する罰金](#)」などが適用開始。
 - 欧州委員会は2026年7月10日、「AI法第50条の下での特定AIに対する透明性義務の実施に関するガイドライン」を公表。
 - ステークホルダーにより2026年6月10日に「AI生成コンテンツの透明性に関する実践規範」が策定・公表。
 - 2026年8月2日より前に市場投入された生成AIシステムのプロバイダーは、[2026年12月2日までに（第50条の透明性義務のうち）第50条第2項を遵守することが必要。](#)
- 2026年12月2日、AI法の「第2章（第5条）禁止されるAI慣行」の[追加条項（\(ba\)と\(bb\)）](#)が適用開始。
- 2026年8月2日までに、加盟国は国内にAI規制サンドボックスを設置して運用開始。
- 2027年12月2日、AI法の「第3章 ハイリスクAIシステム」第1節～第3節が適用開始（[Annex IIIに基づくハイリスクAIシステム](#)）。
- 2028年8月2日、AI法の「第3章 ハイリスクAIシステム」第1節～第3節が適用開始（[Annex Iに基づくハイリスクAIシステム](#)）。
 - [上記の適用開始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（Annex IおよびIII）](#)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。
 - 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、本規則の要件と義務を遵守するために必要な措置を講じる。
 - 欧州委員会は2026年5月19日、「AI法第6条の下でのハイリスクAIシステムの分類に関するガイドライン案」を公表、6月23日までパブコメ実施。
- 2030年12月31日までに、Annex Xにリスト化された法令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AIシステムは、AI法を遵守する。

EUのAI法の章・節	適用開始日
第1章（一般規定）	2025年2月2日
<u>第2章（禁止されるAI慣行）</u>	<u>2025年2月2日</u>
第5条第1項第1段落（ba）（bb）、第1a項、第1b項	2026年12月2日
<u>第3章（ハイリスクAIシステム）</u> 第1節（ハイリスクAIシステムとしての分類） 第2節（ハイリスクAIシステムに対する要件） 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）	<u>2027年12月2日（Annex III関連）</u> <u>2028年8月2日（Annex I関連）</u>
第6条第5項（ハイリスクAIシステムのガイドライン）	2026年2月2日
第4節（公認認証当局と公認認証機関）	2025年8月2日
第5節（規格、適合性評価、証明書、登録）	2026年8月2日
<u>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）</u>	<u>2026年8月2日</u> （既存プロバイダーは第50条第2項については2026年12月2日）
<u>第5章（汎用目的AIモデル）</u>	<u>2025年8月2日</u>
第6章（イノベーションを支援するための措置）	2026年8月2日
第7章（ガバナンス）	2025年8月2日
第8章（ハイリスクAIシステムに関するEUデータベース）	<u>2026年8月2日</u>
<u>第9章（市場流通後モニタリング、情報共有、市場監視）</u>	
第78条（機密保持）	2025年8月2日
第10章（行動規範とガイドライン）	2026年8月2日
第11章（権限の委任および委員会の手続）	
<u>第12章（罰則）</u>	<u>2025年8月2日</u>
第101条（汎用目的AIモデルのプロバイダーに対する罰金）	2026年8月2日
第13章（最終規定）	2026年8月2日

- 欧州委員会は第7次簡素化オムニバス・パッケージとして、2025年11月19日に「[デジタル・パッケージ](#)」を公表。
 - https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718
 - [簡素化オムニバス・パッケージ](#)（Simplification Omnibus packages）とは、[ドラギ報告書](#)（2024年9月）の提言（行き過ぎた規制はEUの競争力を阻害する）を行動計画化した「[競争力コンパス](#)」（2025年1月）において予告されていたもの。欧州委員会は競争力コンパスにおいて、[企業の法令遵守コストを減らすために企業の報告負担およびその他の法令遵守負担を中小企業（SME）で35%、全企業で25%削減し、5年の任期終了までに375億ユーロの経常コストを削減する](#)という目標を立て、そのために2025年2月から一連の簡素化オムニバス・パッケージを開始。
- デジタル・パッケージは、簡素化の取り組みによって企業のコンプライアンスを緩和することを目的としており、[2029年までに法令遵守コストを最大50億ユーロ削減](#)すると見込んでいる。さらに、欧州ビジネスウォレットにより、企業は毎年さらに1500億ユーロを節約できる可能性。
- デジタル・パッケージは以下で構成。
 - デジタル法令の簡素化に関する規則案（[デジタル・オムニバス規則案](#)）
 - AIの整合ルール実施の簡素化に関する規則案（[AIに関するデジタル・オムニバス規則案](#)）
 - [欧州ビジネスウォレット規則案](#)
 - [データ連合戦略](#)（Data Union Strategy）：AIのためのデータの解放
 - データ法のモデル契約と標準契約条項の勧告案

- 欧州委員会はデジタル・パッケージの一部として、「[AIの整合ルール実施の簡素化に関する規則案（AIに関するデジタル・オムニバス規則案）](#)」を2025年11月19日に公表。
 - <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal>
- 以下から構成される。
 - [AI法の改正](#)
 - ハイリスクAIシステムの適用開始日の変更
 - 中小企業（SME、従業員250名未満）向けの特例を中堅中小企業（SMC、従業員750名未満）に拡大
 - AI規制サンドボックス関連
 - バイアス検出・軽減のためのセンシティブ個人データ処理条項の明確化
 - 適合性評価関連
 - その他、手続きの簡素化 等
 - 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の改正
 - （規則案には無かったが、正式制定されたAIデジタル・オムニバス規則では[機械規則の改正](#)が追加された）

3 . AI法の改正点

AI法の主な改正点（1/5）

○ 禁止AI関連

- [禁止されるAI慣行](#)に「本人同意のない性的な画像・ビデオ等の生成」と「児童ポルノの生成」を追加：
 - 2026年12月2日から適用開始。（第5条第1項(ba)(bb)、第113条第3項）

○ ハイリスクAIシステム関連

- [ハイリスクAIシステムの適用開始日の変更](#)：
 - 既存条文ではハイリスクAIシステムに関する規定の適用開始日は2026年8月2日（Annex III関連）または2027年8月2日（Annex I 関連）であったが、ハイリスクAIシステムの規定遵守を支援する措置（[整合規格、共通仕様、欧州委員会ガイドライン](#)）が未発行な状況を踏まえ、[適用開始日を2027年12月2日（Annex III関連）または2028年8月2日（Annex I関連）](#)に先送り。（第113条第3項）
- [機械規則（EU）2023/1230](#)をAnnex IのセクションAからセクションBに移動（[AI法の直接適用から除外](#)）：
 - 機械規則とAI法の両方を適用すると重複が生じる恐れがあり、[AI搭載機械（AI-enabled machinery）の規制枠組みを簡素化](#)するため（AIデジタル・オムニバス前文(42)）。
 - そのためには、機械規則に、AI法と同等の保護レベルの、[ハイリスクAIシステムに対する健康・安全要件](#)（AI法の第3章第2節、第17条、第19条、第72条、第73条に相当）を追加することが必要。そのため、機械規則の改正により、[欧州委員会に機械規則のAnnex III（機械または関連製品の設計および製造に関する必須の健康・安全要件）を改正する委任法令](#)の採択権限が付与された。当該委任法令は2028年8月2日までに適用開始。
 - AI搭載機械の製品製造者は、機械規則に従ったハイリスクAI関連の整合規格や共通仕様が採択されるまでは、AI法第40条・第41条に従って採択された整合規格や共通仕様に依拠して、機械規則Annex IIIのハイリスクAIシステムの健康・安全要件に適合させることが可能。

○ ハイリスクAIシステム関連（続き）

- Annex IのセクションAのハイリスクAIについて、[分野別整合法令におけるAI要件と調整](#)するメカニズムを追加：
 - Annex IのセクションA（医療機器・玩具・エレベーターなど）の分野における[整合法令がAI法と同等以上のAI要件・義務を持つ場合](#)、実施法令（2027年8月2日までに採択）によって、第9条～第15条および第17条～第25条までに定める個々の要件・義務の適用を個別に制限可能。（第2条第13項）
 - また、ハイリスクAIシステムのプロバイダーがAI法の要件と分野別整合法令の要件を遵守する際に、法令遵守負担を最小限に抑えられるように、欧州委員会はAI法の「第8条 要件の遵守」第2項、「第9条 リスク管理システム」第10項、「第17条 品質管理システム」第3項のガイドラインを2027年8月1日までに策定・公表。（第96条第1項(g)）
- バイアス検出・軽減のためのセンシティブ個人データ処理条項の適用範囲拡大：
 - 「バイアス検出・軽減のためのセンシティブ個人データ処理」はもともとハイリスクAIシステムのプロバイダーにのみ例外措置として認められていたが（第10条第5項）、これをハイリスクAIシステムのディプロイヤーや、ハイリスク以外のAIシステム・AIモデルのプロバイダーやディプロイヤーにも拡大（第4a条に移動）。

○ 適合性評価関連

- ハイリスクAIと分野別整合法令の共同遵守を支援する整合規格等の開発を追加：
 - AI法のハイリスクAIの要件と、Annex Iの分野別整合法令に定められた関連要件を同時に遵守する必要があるプロバイダーを支援するために、欧州委員会は、不当な遅滞なく、欧州標準化機関に対し、整合規格を含む標準化デリバラブルを開発するよう要求する義務が追加された。

○ 適合性評価関連（続き）

- ハイリスクAIシステムがCRAの関連要件を満たす場合、AI法第15条のサイバーセキュリティ要件に適合：
 - ハイリスクAIシステムがサイバーレジリエンス法（CRA）の適用範囲に該当し、かつCRA第12条（ハイリスクAIシステム）第1項に規定する条件を満たす場合、当該システムはAI法「第15条 正確性、堅牢性、サイバーセキュリティ」に定めるサイバーセキュリティ要件に適合するものとみなされる。
- Annex I（セクションA）とAnnex IIIの両方に該当するハイリスクAIシステム：
 - ハイリスクAIシステムが、Annex IのセクションAにリスト化されたEU整合法令の対象であり、かつAnnex IIIにリスト化されたカテゴリーのいずれかにも該当する場合、当該システムのプロバイダーは、[Annex IのセクションAにリスト化された整合法令に従って要求される適合性評価手続](#)に従う。

○ 透明性義務AIシステム関連

- 透明性の義務のあるAIシステムの移行期間規定の追加：
 - 「[透明性の義務のあるAIシステム](#)」（第50条）の適用開始日は変わっていないが（2026年8月2日）、この適用開始日より前にEU域内に市場投入された生成AIシステム（汎用目的AIシステムを含む）のプロバイダーは[2026年12月2日までに](#)第50条第2項（AIシステムの出力を機械可読形式でマークし、人工的に生成または加工されたものとして検出可能とする義務）を遵守するために必要な措置を講じるとの移行期間規定が追加。（第111条第4項）

○ 汎用目的AIモデル関連

- 汎用目的AIモデルとAIシステムが同一のプロバイダーによって開発されている場合のAIオフィスの監督権限範囲を明確化：
 - 汎用目的AIモデルに基づくAIシステムであって、当該モデルとシステムが同一のプロバイダー（または当該プロバイダーと同一の事業体に属するプロバイダー）によって開発されたものは（各加盟国の国内所轄機関ではなく）AIオフィスが排他的な監督および執行権限を有するが、以下のAIシステムは除く。（第75条第1項）
 - Annex Iの整合法令の対象となる製品に関連するAIシステム
 - Annex III第2項（重要インフラ）に規定するAIシステム
 - 法執行機関、国境管理機関、金融機関（ただし当該AIシステムが第74条6項に該当する場合に限る）が提供するAIシステム
 - 司法の運営に関しAnnex III第8項に規定するAIシステム
 - デジタルサービス法（DSA）に基づき指定された超大規模オンラインプラットフォームや超大規模オンライン検索エンジンを構成するAIシステム（またはそれらに組み込まれたAIシステム）についても、AIオフィスが排他的な監督および執行権限を有する。（第75条第1項）
 - AIオフィスは、上記のAIシステムのうち、ハイリスクに分類され、かつ第43条に基づき第三者による適合性評価の対象となるものについて、市場投入又はサービス提供が行われる前に、その適合性評価およびテストを行う責任を負う。欧州委員会は、当該評価やテストの実施を、AI法に基づき指定された公認認証機関に委託する。（第75条第1e項）

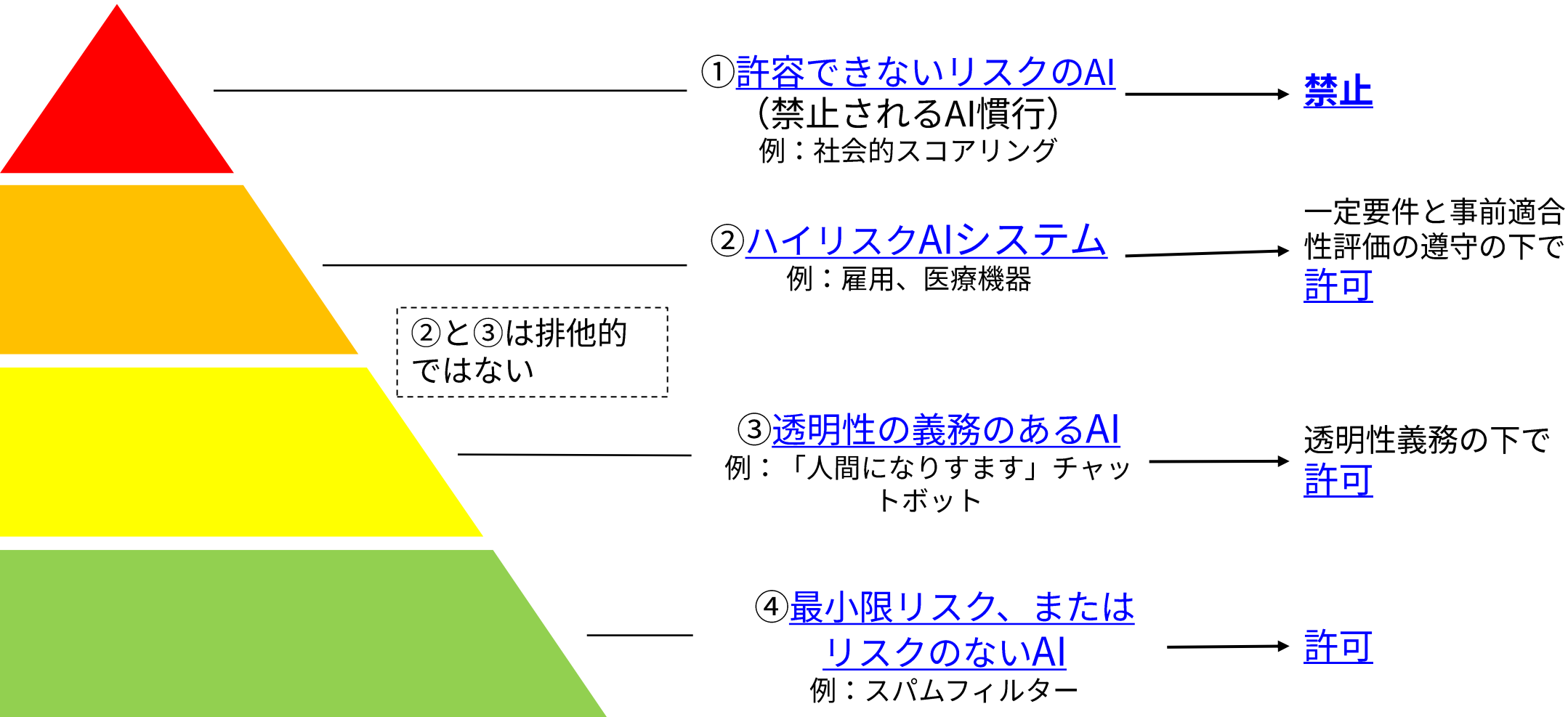
○ その他

- 中小企業（SME、従業員250名未満）向けの特例を[中堅中小企業（SMC、従業員750名未満）に拡大](#)：
 - 技術文書の簡素化（第11条）
 - AI規制サンドボックスへの優先アクセス（第57条）
 - 行動規範での考慮（第95条）
 - 各加盟国における罰則での考慮・制裁金の減額（第99条）
 - 品質管理システム（第17条）
 - 国内所轄機関のガイダンスおよび助言（第70条）
 - ガイドラインでの考慮（第96条）
- プロバイダーおよびディプロイヤーの[AIリテラシー関連義務を緩和](#)：
 - 「AIシステムのプロバイダーおよびディプロイヤーのAIリテラシーに関する義務」（第4条）において、従業員等の十分なレベルのAIリテラシーを保証するという義務を、AIリテラシー向上の支援義務に緩和。
- AI規制サンドボックス関連：
 - 各加盟国の国内所管機関によるAI規制サンドボックスの設置期限を2026年8月2日から2027年8月2日に延期。（第57条第1項）
 - 「第60a条 Annex IのセクションBにリスト化されたEU整合法令の対象となるハイリスクAIシステムの、AI規制サンドボックス外の現実世界条件下でのテスト」を追加。
- その他、手続きの簡素化：
 - 「[汎用目的AIモデルの実践規範](#)」（第56条6項）および「透明性の義務のあるAIシステムの実践規範」（第50条7項）について、実施法令を制定する欧州委員会の権限を削除。

4．AI法の概要（改正点の反映版）

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。



※法案では左記の4階層だったが、審議過程で別軸として「⑤汎用目的AIモデル」および「⑥システミックリスクのある汎用目的AIモデル」に対する規制が追加された

○ 前文 (1) ～ (180)

○ 条文

- 第1章 一般規定 (General Provisions) : 第1条～4a条 (4a条追加)
- 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(60a条追加)
- 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 (75a条～75d条追加)
 - 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
- Annex I～XIV (XIV追加)

• 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システムに関する統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) **中堅中小企業（SMCs）**、および新興企業（start-ups）を含む中小企業（SMEs）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。

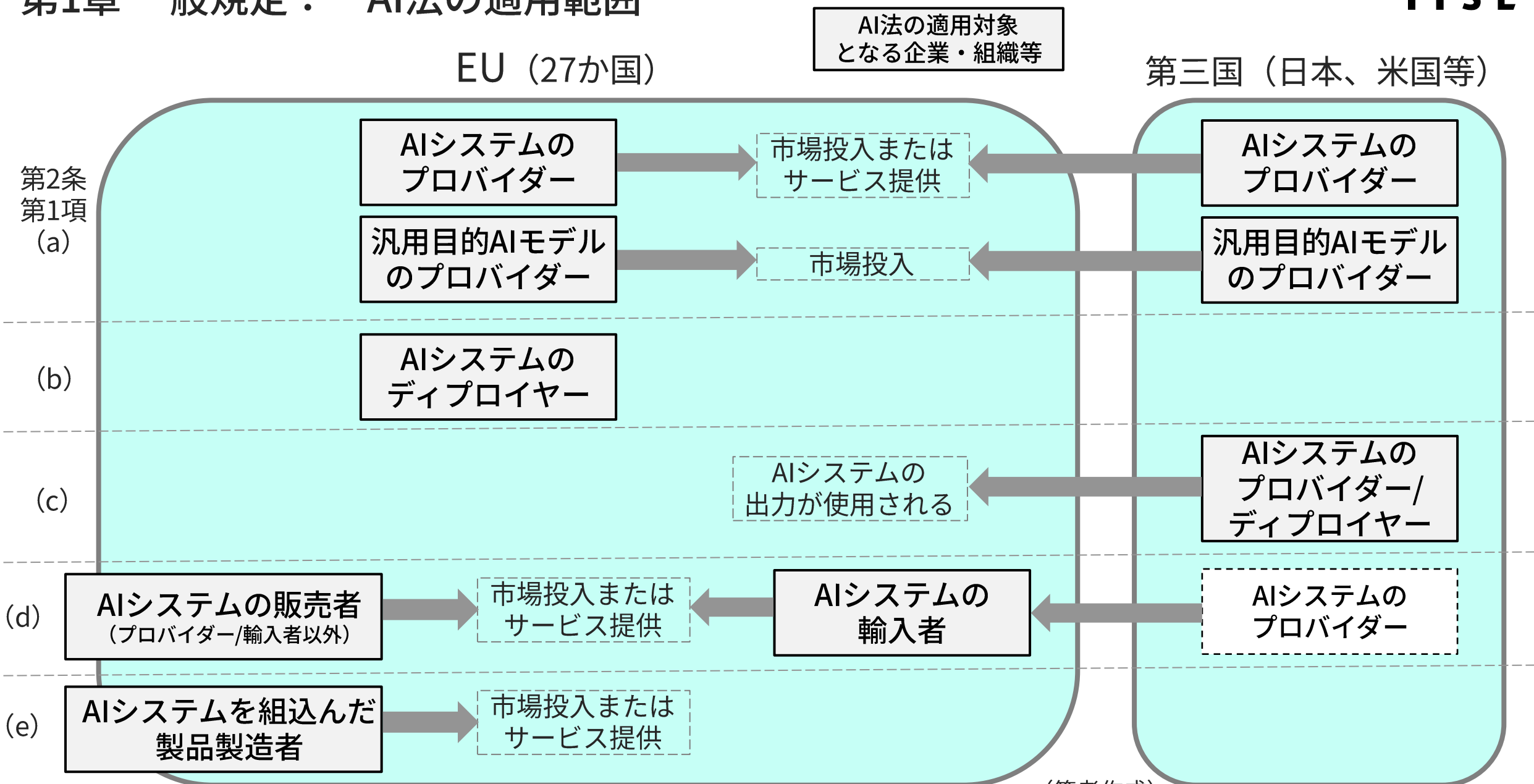
- ※中堅中小企業（SMCs）：中小企業（≒従業員数250名未満）に該当せず、従業員数が750名未満で、年間売上高が1億5000万ユーロ以下、または貸借対照表の総資産が1億2900万ユーロ以下の企業。欧州委員会によればEU域内に約38000社。

• 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



(筆者作成)

・ 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)
- 1. 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AIリテラシー向上を支援するための措置を、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、講じるものとする。この義務は、プロバイダーまたはディプロイヤーが個人の特定のレベルのAIリテラシーを保証することを要求するものではない。
- (第2項および第3項は略)

※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慣行

• 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
- (ba) 本人同意のない性的な画像・ビデオ等の生成
- (bb) 児童ポルノの生成
- (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10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。

• 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。
- (ba) 識別可能な自然人の親密な部分、または性的に露骨な活動に従事する識別可能な自然人のリアルな画像、ビデオ、音声、または類似の素材を、その生成または加工についてその自然人が、自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、明示的な同意を得ずに生成または加工するAIシステムの市場投入、サービス提供、または使用。
- (bb) 指令2011/93/EU第2条(c)項（児童ポルノ）および(e)項（児童のポルノ的パフォーマンス）に規定する素材またはパフォーマンスを生成または加工するAIシステムの市場投入、サービス提供、または使用。ただし、国内法に基づき「権利なし」の抗弁が適用される場合を除く。
- (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。

• 禁止されるAI慣行：第5条第1項の条文（続き）

- (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。
- (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カテゴライズは含まれない。
- (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。

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

(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りうるもの。
- 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6条1項、第60a条、および第102条から第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
機械規則 (EU) 2023/1230	

(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

- 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。（第2節、第8条）

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。（ハイリスクAIシステムのディプロイヤーや、ハイリスク以外のAIシステムのプロバイダー/ディプロイヤーも処理可能とするために、第10条第5項から第4a項に移動）
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、当該所轄機関に協力する。
 - (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を損なうことなく、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。

特に、第2段落に定める義務には、同段落に規定する目的に関連する場合には、以下の事項が含まれるものとする。

- (a) 第16条に規定された要件への適合性を評価するのに十分な技術文書を利用可能にすること。
- (b) 新しいプロバイダーに対し、既知の制限事項や障害モードについて情報提供すること。
- (c) 新しいプロバイダーに対し、テストや検証を含む、対象を絞った技術的アクセスを提供すること。

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、そのため新しいプロバイダーとの協力義務や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。（第4項および第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。

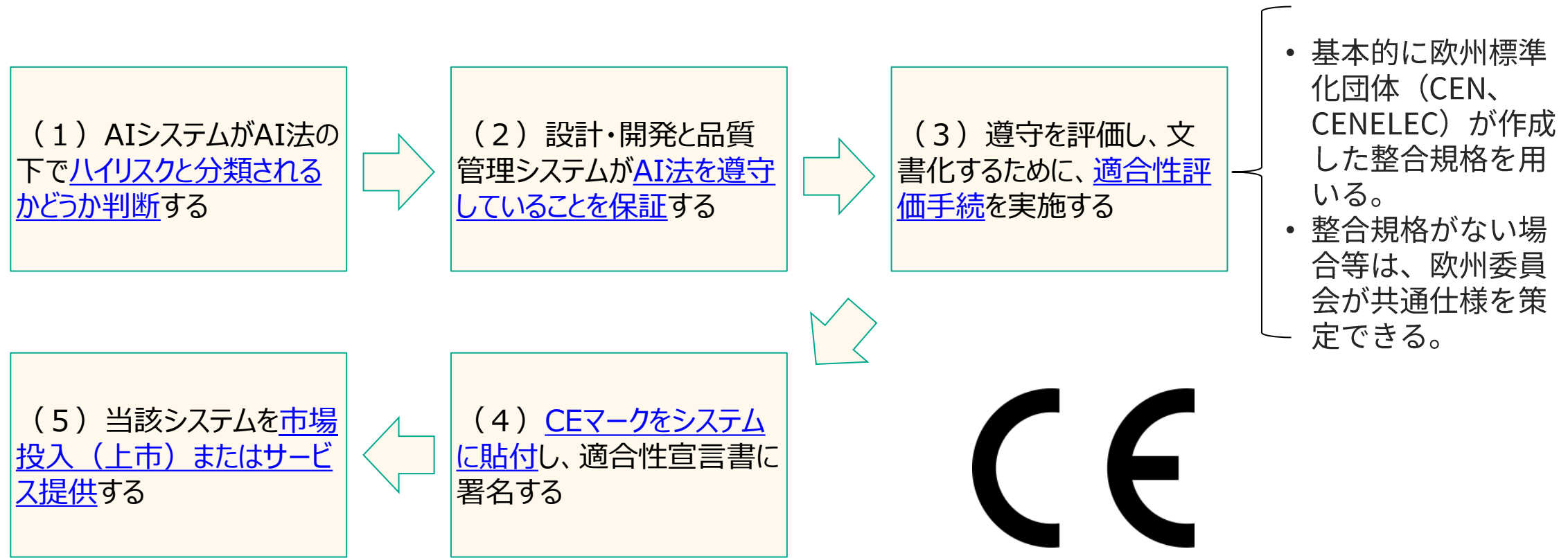
- 第27条 ハイリスク AI システムの基本的人権影響評価
 - 1. 第6条第2項で言及されたハイリスクAIシステムをディプロイする前に、Annex IIIの第2項にリスト化された領域での使用を目的としたハイリスクAIシステムを除き、公法によって規律される団体であるディプロイヤー、または公共サービスを提供する民間団体であるディプロイヤー、およびAnnex IIIの第5項 (b) および (c) で言及されているハイリスクAIシステムのディプロイヤーは、当該システムの使用によって生じる可能性のある基本的権利への影響に関する評価を実行するものとする。この目的のために、ディプロイヤーは以下から構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、**ディプロイヤーは、本条第1項で言及された基本的人権影響評価を実施する際に、参照先にそのデータ保護影響評価の関連セクションを含めるか、またはそのデータ保護影響評価の関連部分を基本的人権影響評価に含めることができる。**
 - 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。**このテンプレートは、該当する場合、ディプロイヤーが第4項に従って参照先にデータ保護影響評価の関連セクションを含めたり、データ保護影響評価の関連部分を基本的人権影響評価に含めたりできるようにするものとする。**

- 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/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義務と、Annex I のEU整合法令に定められた関連要件および義務への共同遵守を促進するため、必要に応じて整合規格を含む、標準化デリバブルを開発するよう欧州標準化機関に要求する。（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整合法令に基づく公認認証機関は、2028年1月28日までに、AI法の下での指定を申請する。
- 各EU整合法令により製品製造者に第三者が関与しない適合性評価に依拠できるオプションが提供されている場合は、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、そのようなオプションを利用することができる。

• （Annex IのセクションB：第6条1項、第60a条、および第102条から第112条以外はAI法の適用対象外）

• 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）

• Annex IのセクションA、かつAnnex IIIのいずれかにも該当する場合：

- プロバイダーは、Annex IのセクションAのEU整合法令の下で要求される適合性評価手続に従う。（第43条第3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 XII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： ⑥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： ⑥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）

第5章 汎用目的AIモデル： ⑥システミックリスク汎用目的AIモデルのプロバイダーの義務 I I S E

- 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）

第5章 汎用目的AIモデル： ⑤⑥汎用目的AIの実践規範（Codes of practice） I I S E

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）

- 国内所轄機関（第70条）
 - 加盟国は、少なくとも1つの公認認証機関および少なくとも1つの市場監視機関を国内所管機関として設置または指定する。（第1項）
 - 加盟国は、公認認証機関および市場監視機関の名称、それらの機関の職務、その後の変更について、欧州委員会に連絡する。加盟国は、国内所管機関および単一連絡窓口への連絡方法に関する情報を、2025年8月2日までに電子通信手段により公開する。加盟国は、本規則の単一連絡窓口として機能する市場監視機関を指定し、当該窓口の名称を欧州委員会に通知する。欧州委員会は、単一連絡窓口のリストを公開する。（第2項）

※各加盟国の単一連絡窓口（国内所轄機関）のリスト（2026年9月時点） <https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act>

Austria	未定	France	Directorate General for Competition Policy, Consumer Affairs and Fraud Control	Malta	Malta Digital Innovation Authority (MDIA)
Belgium	未定	Germany	Federal Network Agency	Netherlands	Dutch Authority for Digital Infrastructure
Bulgaria	未定	Greece	Hellenic Data Protection Authority	Poland	Commission for the Development and Security of Artificial Intelligence
Croatia	未定	Hungary	未定	Portugal	National Regulatory Authority for Communications
Cyprus	Commissioner of Communications	Ireland	AI Office of Ireland	Romania	National Authority for Management and Regulation in Communications of Romania
Czech Republic	Czech Telecommunication Office	Italy	National Cybersecurity Agency	Slovakia	未定
Denmark	Agency for Digital Government	Latvia	Consumer Rights Protection Centre	Slovenia	Agency for Communication Networks and Services of the Republic of Slovenia
Estonia	Consumer Protection and Technical Regulatory Authority	Lithuania	Communications Regulatory Authority of the Republic of Lithuania	Spain	Spanish Artificial Intelligence Surveillance Agenc
Finland	Transport and Communications Agency	Luxembourg	National Commission for Data Protection	Sweden	The Swedish Post and Telecom Authority

- 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、**欧州AI会議の意見を最大限に考慮した上で、市場流通後モニタリング計画に関するガイダンス**（テンプレートを含む）を**2027年9月2日**までに採択するものとする。
 - 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9章 市場流通後モニタリング・情報共有・市場監視：AIシステムの市場監視と管理 I I S E

- AIシステムの市場監視と管理、および相互支援（第75条）
 - AIオフィスは、以下のAIシステムに関して、本規則に基づく義務の監督および執行について排他的な職務権限を有するものとする。（第1項）
 - (a) 汎用目的AIモデルに基づくAIシステムであって、当該モデルとシステムが同一のプロバイダー、または当該プロバイダーと同一の事業体（undertaking）に属するプロバイダーによって開発されたもの。ただし、以下を除く。
 - (i) Annex Iにリスト化されたEU整合法令の対象となる製品に関連するAIシステム
 - (ii) Annex III第2項（重要インフラ）に規定するAIシステム
 - (iii) 法執行機関、国境管理機関及び金融機関（ただし当該AIシステムが第74条6項に該当する場合に限る）が提供するAIシステム
 - (iv) 司法の運営に関し、Annex III第8項に規定するAIシステム
 - (b) 規則(EU) 2022/2065（DSA）に基づき指定された超大規模オンラインプラットフォームもしくは超大規模オンライン検索エンジンを構成するAIシステム、またはそれらに組み込まれたAIシステム
 - 上記の排他的職務権限は、当該システムのプロバイダーに適用される。当該システムのディプロイヤーに対しては、当該ディプロイヤーがプロバイダーでもある場合、またはプロバイダーと同一の事業体の一部を構成する場合に限り、適用される。
 - 第1項に基づきAIオフィスの所轄に服するハイリスクAIシステムのプロバイダーは、重大なインシデントをAIオフィスに報告する。AIオフィスは、当該プロバイダーまたはその法的代理人が所在する加盟国の市場監視機関に対し、関連情報を速やかに伝達する。（第1a項）
 - AIシステムを市場で利用可能にすることもしくはサービス提供することを禁止もしくは制限する効果をもたらす決定、または当該市場から当該AIシステムを撤退もしくはリコールする決定を行う前に、AIオフィスは、当該決定を行う意図がある旨を、当該市場を所轄する市場監視機関に不当な遅滞なく通知する。（第1d項）
 - AIオフィスは、第1項に言及されるAIシステムのうち、ハイリスクに分類され、かつ第43条に基づき第三者適合性評価の対象となるものについて、市場投入またはサービス提供が行われる前に、その適合性評価およびテストを行う責任を負う。欧州委員会は、当該テストまたは評価の実施を、本規則の下で指定された公認認証機関に委託し、当該公認認証機関は欧州委員会に代わって行動する。（第1e項）

第9章 市場流通後モニタリング・情報共有・市場監視：リスクを提示するAIシステム I I S E

- リスクを提示するAIシステムへの国レベルの対応手続（第79条）
 - 加盟国の市場監視機関は、AIシステムが人の健康や安全または基本的権利に対するリスクを提示すると考える十分な理由がある場合、本規則で規定されたすべての要件と義務の遵守に関して、当該AIシステムの評価を実施する。脆弱なグループにリスクを提示するAIシステムには特に注意が払われるものとする。基本的権利の保護に対するリスクが特定された場合、市場監視機関は、基本的権利を保護する国内公的機関にも情報提供し、全面的に協力する。関連するオペレーターは、必要に応じて、それらの機関と協力する。（第2項）
 - 市場監視機関が、当該評価の過程で、AIシステムが本規則で規定された要件と義務を遵守していないことを発見した場合、不当な遅滞なく、関連するオペレーターに、市場監視機関が設定する期間内に、いずれにしても15営業日以内に、または関連するEU整合法令で規定された期間内に、当該AIシステムを遵守させたり、市場から撤退させたり、リコールしたりするためのあらゆる適切な是正措置を講じるように要求する。（第2項）
 - 市場監視機関は、非遵守が自国の領土に限定されていないと判断した場合、欧州委員会および他の加盟国に、不当な遅滞なく、当該評価の結果およびオペレーターに取るように要求した措置を情報提供する。（第3項）
 - オペレーターは、EU市場で利用可能なすべての当該AIシステムに関して、すべての適切な是正措置が講じられていることを保証する。（第4項）
 - AIシステムのオペレーターが第2項の期間内に適切な是正措置を講じない場合、市場監視機関は、AIシステムが国内市場で利用可能になる、またはサービス提供されることを禁止または制限したり、国内市場から当該製品または当該スタンドアロンAIシステムを撤退させたり、リコールしたりするためのすべての適切な暫定措置を講じる。市場監視機関は、欧州委員会および他の加盟国に不当な遅滞なくこれらの措置を通知する。（第5項）
 - 第5項で言及された通知には、入手可能なすべての詳細、特に非遵守AIシステムの特定に必要な情報、当該AIシステムの起源とサプライチェーン、疑われている非遵守とリスクの性質、講じられた国内措置の性質と期間、関連するオペレーターによって提起された議論を含める。特に、市場監視機関は、非遵守が以下の1つ以上によるものかどうかを示す。（第6項）
 - (a) 第5条のAI慣行の禁止の非遵守
 - (b) ハイリスクAIシステムが第3章第2節で規定された要件を満たしていないこと
 - (c) 適合性の推定を与える第40条および第41条の整合規格または共通仕様における不十分な点
 - (d) 第50条の非遵守

第9章 市場流通後モニタリング・情報共有・市場監視： 救済（Remedies） I I S E

- 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。

- 欧州委員会は、[汎用目的AIモデルのプロバイダーの義務の監督と執行を行う排他的権限](#)を有する。（第88条第1項）
 - 欧州委員会はこれらの職務の実施をAIオフィスに委託する。
- AIオフィスは汎用目的AIモデルのプロバイダーによるAI法の効果的な実施と遵守（実践規範への準拠を含む）をモニタリングするために必要な措置を講じることができる。（第89条第1項）
- 科学パネルは、以下を疑う理由がある場合には、AIオフィスに適格な警告を提供できる。（第90条第1項）
 - (a) ある汎用目的AIモデルが、EUレベルで具体的で特定可能なリスクを提示する。または、
 - (b) ある汎用目的AIモデルが第51条（システミックリスクのある汎用AIモデルとしての分類）で言及された条件を満たす。
- 欧州委員会は、汎用目的AIモデルのプロバイダーに対して、第53条および第55条に従って[プロバイダーが作成した文書](#)や、プロバイダーのAI法の遵守を評価する目的で[必要な追加情報の提供を要求](#)できる。（第91条第1項）
 - 情報要求には、法的根拠と要求の目的を記載し、どのような情報が必要であることを特定し、情報を提供する期間を設定し、不正確、不完全または誤解を招く情報を提供した場合の[第101条に規定された罰金](#)を示すものとする。（第91条第4項）
- AIオフィスは、欧州AI会議に相談した後、以下のために、[汎用目的AIモデルの評価を実施](#)できる。（第92条第1項）
 - (a) 第91条に従って収集された情報が不十分な場合、AI法に基づく義務に対するプロバイダーの遵守を評価する。または、
 - (b) 特に第90条第1項(a)に基づく科学パネルからの適格な警告を受けて、システミックリスク汎用目的AIモデルの[EUレベルでのシステミックリスクを調査](#)する。
 - 欧州委員会は、科学パネルからの専門家を含め、欧州委員会に[代わって評価を実施する独立した専門家の指名](#)を決定できる。（第92条第2項）
 - 評価のため、欧州委員会はAPIその他の適切な技術的手段・ツール（ソースコード含む）を介して、[当該モデルへのアクセスを要求](#)できる。（第3項）
 - アクセス要求には、法的根拠、要求の目的および理由を記載し、アクセスを提供するまでの期間を設定し、アクセスを提供しなかった場合の[第101条に規定された罰金](#)を示すものとする。（第92条第4項）
- 欧州委員会は必要かつ適切な場合、[プロバイダーに以下を要求](#)できる。（第93条第1項）
 - (a) 第53条および第54条（第55条の間違い？）に定められた[義務を遵守するために適切な措置を講じる](#)こと。
 - (b) 第92条に従い実施された評価により、EUレベルでのシステミックリスクの深刻かつ実証された懸念が生じた場合に、[軽減措置を実施](#)すること。
 - (c) 当該モデルを[EU市場で利用可能にすることを制限したり、撤退またはリコール](#)すること。

- 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、**および中堅中小企業**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、第26条（ディプロイヤーの義務）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。
 - (g) 本規則の要件およびAnnex I のセクションAのEU整合法令の要件を遵守するに当たり、整合性の確保、重複の回避、追加的負担の最小化を図ることを目的として、補完性と比例性の原則に従い、第8条第2項、第9条第10項、第17条第3項を実際に実施するためのガイドライン。2027年8月1日までに公表。
 - 欧州委員会は、ガイドラインを発行する際、欧州AI会議を関与させるとともに、新興企業を含む中小企業、中堅中小企業、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 <u>AI慣行の禁止</u> を遵守しない場合。	<u>3500万ユーロ以下</u> 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 <u>世界全体における売上総額の7%以下</u> 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 (da) 第25条第2項、第4項に基づくプロバイダーおよびオペレーターの義務 (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	<u>1500万ユーロ以下</u> 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 <u>世界全体における売上総額の3%以下</u> 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 <u>不正確、不完全、または誤解を招く情報を提供</u> した場合。	<u>750万ユーロ以下</u> 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 <u>世界全体における売上総額の1.5%以下</u> 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、および中堅中小企業の場合。	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（中堅中小企業の場合は禁止AI慣行については除く）

• 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、適用開始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。
 - 2026年8月2日より前に市場投入された、合成音声・画像・動画・テキストのコンテンツを生成するAIシステム（汎用目的AIシステムを含む）のプロバイダーは、2026年12月2日までに第50条第2項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。ただし第5条第1項第1段落(ba)および(bb)、ならびに第5条第1a項および第1b項は、2026年12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3章第1節（ハイリスクAIシステムの分類ルール）、第2節（ハイリスクAIシステムに対する要件）、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）は、第6条第5項を除き、以下から適用される。
 - (i) 第6条第2項およびAnnex IIIに基づきハイリスクに分類されるAIシステムについては、2027年12月2日。
 - (ii) 第6条第1項およびAnnex IIに基づきハイリスクに分類されるAIシステムについては、2028年8月2日。
 - 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。

5 . AI法のガイドライン・実践規範・整合規格

- 「AI法で規定された禁止AI慣行に関するガイドライン」（2025年2月4日）
 - <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>
 - AI法は第96条第1項で、欧州委員会はAI法の実際の実施に関する一連のガイドラインの作成を義務付けている。この規定を受け、また2025年2月2日からの禁止AI慣行に関連した規定の適用開始に先立ち、欧州委員会AIオフィスは、約1か月間のパブコメを経て、同ガイドラインを公表。
 - ガイドラインには拘束力はなく、権威のある法解釈は欧州連合司法裁判所（CJEU）のみによって最終的に示されうるが、禁止事項に対する欧州委員会の法解釈を示すもの。EU加盟国の国内所轄機関やプロバイダー、ディプロイヤーといったステークホルダーがAI法の要件を理解して遵守できるように、法的な説明と実用的な事例を提供。
 - AI法の第5条1項で挙げられた禁止AI慣行の8類型ごとに条文の詳しい解説と適用事例の紹介がなされている。
- 「AIシステムの定義に関するガイドライン」（2025年2月6日）
 - <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>
 - AIシステムの定義（第3条(1)）を、「マシンベースのシステム」「様々なレベルの自律性で動作するように設計されていること」「ディプロイメント後に適応性を示す可能性があること」「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出力を生成する方法を推論する」「予測、コンテンツ、レコメンデーション、意思決定など」「物理的またはバーチャルな環境に影響を与えうる」の7つの要素に分解し、それぞれについて欧州委員会の法解釈を提示。
- 「AI法で規定された汎用目的AIモデルの義務の範囲に関するガイドライン」（2025年7月18日）
 - <https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act>
 - AIモデルが「汎用目的AIモデル」とみなされる条件（累積学習計算量が10の23乗FLOPを超え、かつ言語生成、テキストから画像生成、またはテキストから動画生成が可能なモデル）など、明確な技術的基準を提示。
 - （汎用目的AIモデルのプロバイダー以外では）AIモデルに大幅な変更を加える者のみが汎用目的AIモデルプロバイダーの義務を遵守する必要があると、軽微な変更を加える者は汎用目的AIモデルプロバイダーの義務遵守の必要がないことを明確化。
 - 透明性とイノベーションを促進するために、オープンソースAIモデルのプロバイダーがどのような条件下で特定の義務を免除されるかを明確化。

- 「[汎用目的AIモデル（GPAIモデル）の実践規範（Code of Practice）](#)」（2025年7月10日公表）
 - <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>
 - 最終版は作業グループによる作成が遅延していたが、2025年7月10日に欧州委員会に提出され公表。欧州委員会は8月1日、GPAIモデル関連条項の適用開始日（8/2）の前日に、実施法令による十分性決定を通じて実践規範の最終版を承認。同日、欧州AI会議も最終版を承認。
 - 実践規範は「[透明性](#)」「[著作権](#)」「[安全性とセキュリティ](#)」の3つの章から構成。
 - 「透明性」と「著作権」の章は、GPAIモデルのプロバイダー全般向けのものであり、AI法第53条の義務（[技術文書の作成](#)、[下流プロバイダーへの情報提供](#)、[著作権法の遵守](#)、[学習データ詳細概要の公表](#)）の遵守を証明する方法を記載。
 - 「安全性とセキュリティ」の章は「システミックリスクのあるGPAIモデル」のプロバイダー向けのものであり、AI法第55条の義務（[\(a\)敵対的テスト・文書化含むモデル評価](#)、[\(b\)システミックリスクの評価と軽減](#)、[\(c\)重大インシデントの報告](#)、[\(d\)モデルとインフラのサイバーセキュリティ](#)）の遵守を証明する方法を記載。
 - システミックリスクの4類型として「化学・生物・放射線・核（CBRN）」「制御の喪失」「サイバー攻撃」「有害な操作」を提示。
 - 「EUのAI法の汎用目的AIモデル実践規範について」<https://www.i-ise.com/jp/information/media/2025/251118.pdf>も参照のこと。
 - GPAIモデルのプロバイダーは[実践規範に自発的に署名](#)し、自発的に準拠することにより、AI法への遵守を証明することができる。実践規範に準拠しないGPAI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証明しなければならない。
 - 実践規範に署名した企業は[Anthropic](#)、[Amazon](#)、[Google](#)、[IBM](#)、[Microsoft](#)、[Mistral AI](#)、[OpenAI](#)など21社（2025年8月1日時点では26社だった）。Metaは署名しておらず、xAIは「安全性とセキュリティ」のみに署名。中国企業も署名していない。また[日本企業で署名した企業はない](#)。

- 「汎用目的AIモデル（GPAIモデル）の実践規範」における指定システミックリスクの4類型

指定システミックリスク	説明
1. <u>化学・生物・放射線・核</u> (Chemical, biological, radiological and nuclear)	<u>化学・生物・放射線・核（CBRN）の攻撃または事故を可能にする</u> ことによるリスク。これには、関連する兵器や素材の設計・開発・取得・リリース・配布・使用において、悪意のある行為者の参入障壁を大幅に低下させること、または達成される潜在的な影響を大幅に増大させることが含まれる。
2. <u>制御の喪失</u> (Loss of control)	<u>モデルを確実に指揮したり、変更したり、シャットダウンしたりする能力を人間が喪失する</u> ことによるリスク。そのようなリスクは、人間の意図または価値観との <u>ミスアライメント</u> 、自己推論、 <u>自己複製</u> 、自己改善、 <u>欺瞞</u> 、 <u>目標変更への抵抗</u> 、力を得ようとする行動（power-seeking behaviour）、AIモデルやAIシステムの <u>自律的作成・改善</u> から生じうる。
3. <u>サイバー攻撃</u> (Cyber offence)	重要システム（重要インフラなど）を含む、 <u>大規模で高度なサイバー攻撃を可能にする</u> ことによるリスク。これには、脆弱性の自動発見、エクスプロイト生成、運用上の使用、攻撃の規模拡大などを通じた攻撃的なサイバー作戦で、悪意のある行為者の参入障壁を大幅に低下させること、または達成される潜在的な影響を大幅に増大させることが含まれる。
4. <u>有害な操作</u> (Harmful manipulation)	<u>大規模な集団や重要な意思決定者を標的にすることで、説得・欺瞞・個人的ターゲティングを通じて、人間の行動や信念の戦略的な歪曲を可能にする</u> ことによるリスク。これには、特に複数ターンのやり取りを通じて、個人がそのような影響に気づいていない、あるいは合理的に検知できない場合に、説得・欺瞞・個人的ターゲティングを行う能力を大幅に強化することが含まれる。このような能力は、保護対象の特性に基づく搾取を含め、民主的なプロセスや基本的権利を損なう可能性がある。

- 「AI法第50条の下での特定AIに対する透明性義務の実施に関するガイドライン」（2026年7月10日）
 - <https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems>
 - AI法第50条（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義務）に基づき、[プロバイダー](#)は、人々がAIシステムとやり取りする際にその旨を情報提供し（第50条第1項）、AIによって生成・加工されたコンテンツを検出できるように機械可読なマークを追加しなければならない（第50条第2項）。
 - また[ディプロイヤー](#)は、人々がディープフェイク（第50条第4項）、公益に関するAI生成の出版物（第50条4項）、感情認識システム・生体カテゴライゼーションシステム（第50条第3項）に触れる場合に、その旨を情報提供しなければならない。
 - [これらの義務は2026年8月2日からプロバイダーとディプロイヤーに適用](#)される（2026年8月2日より前に市場投入したプロバイダーには2026年12月2日から）。ガイドラインは義務の範囲を明確化することで、プロバイダーとディプロイヤーの遵守を支援。
- 「AI生成コンテンツの透明性に関する実践規範」（2026年6月10日）
 - <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>
 - ガイドラインと並行して、ガイドラインを補完する実践規範が欧州委員会AIオフィスの指名した専門家たちにより作成された。
 - AI生成コンテンツの機械可読なマークと検出（第50条第2項）、ディープフェイクおよびAI生成出版物のラベル付け（第50条第4項）に関するもの。プロバイダーとディプロイヤーがこれらの義務の遵守を証明するための[自主的ツール](#)。
 - 最初の署名者リストに掲載されるためには、プロバイダーやディプロイヤーは2026年7月27日までに記入済みのフォームを提出する必要がある。この期日までに[実践規範に署名した企業は約190社](#)であり、セクション1（プロバイダー）が82社、セクション2（ディプロイヤー）が152社であった。日本企業は含まれていない模様である。

- 「[AI法第6条の下でのハイリスクAIシステムの分類に関するガイドライン案](#)」（2026年5月19日）
 - <https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems>
 - 同年6月23日までパブコメ実施。
 - 同ガイドラインは、AI法第6条（ハイリスクAIシステムの分類ルール）の統一的な適用と効果的な執行を促進するため、AIシステムのプロバイダーおよびディプロイヤー、また加盟国の市場監視機関が、[AIシステムをハイリスクに分類すべきか否かを評価することを支援](#)。
 - ハイリスクAIの分類に関連する特定の概念に関する欧州委員会の解釈を示しており、AI法第6条5項に基づき、[ハイリスクとして分類すべきAIシステムと分類すべきでないAIシステムの実例](#)を記載。本ガイドラインにリスト化された例は、あらゆる分野とユースケースをカバーするように努めているが網羅的ではなく、更新されうる。
 - [法的拘束力はないが、欧州委員会の解釈を反映しており、執行の指針](#)となる。今後、ハイリスクAIシステムの義務の遵守を促進するための他のガイドラインによっても補完される予定。
 - 以下の3部から成る。主要部は「AI法の第6条第2項とAnnex IIIに従ったハイリスク分類」。
 - 一般原則
 - AI法の第6条第1項とAnnex Iに従ったハイリスク分類
 - AI法の第6条第2項とAnnex IIIに従ったハイリスク分類
 - 正式版の公表時期は未定。

- 前頁のハイリスクAIシステム分類ガイドライン案において、Annex I 関連の製品において「[安全コンポーネント](#)」とみなされるAIシステムの例示は以下。
 - プロバイダーによって当該AIシステムが[製品の安全機能を果たすことが意図されている](#)場合。（第45項）

機械	ロボットセル（産業用ロボットや周辺機器をユニットとしてパッケージ化した自動化システム）内での人間の存在を検知し、負傷を防止する目的で安全停止または速度低下を作動させる、AIベースのコンピュータビジョンシステム。
ATEX（爆発の可能性のある気体）機器	ガス濃度をモニターし、シャットダウンを指示することを意図したAIシステム。
圧力機器	圧力の暴走を予測し、安全アクセサリと連動したシャットダウンの作動など、保護措置を講じることを意図したAIシステム。
鉄道の相互運用性	速度制限をモニターし、衝突や脱線を防止することを意図した列車内のAIシステム。

- 製品の安全機能を果たすことが意図されていなくても、[その故障や誤動作が人や財産の健康・安全を危険に晒しうる](#)場合。（第46項）

昇降機（エレベーター）	ドアの閉鎖タイミングや障害物検知を管理するAIシステム。プロバイダーによる当該システムの意図された目的は効率的なエレベーターの運用かもしれないが、システムの誤動作は負傷を引き起こし、それによって人の健康・安全を危険に晒す可能性がある。
車両	車線支援用AIシステム。プロバイダーによる当該システムの意図された目的はUXの向上かもしれないが、システムの誤動作により予期せぬ操縦が行われ衝突に至った場合、負傷を引き起こし、それによって人や財産の健康・安全を危険に晒す可能性がある。
農業	化学物質を散布する農地エリアを特定するAIシステム。プロバイダーによる当該システムの意図された目的は化学物質使用の最適化かもしれないが、近隣に人間がいることを適切に考慮しない場合、人の健康・安全を危険に晒す可能性がある。

- 欧州委員会は2025年6月、欧州標準化団体（欧州標準化委員会（CEN）と欧州電気標準化委員会（CENELEC））に対して、[以下に関する整合規格](#)を開発するように要求（M/613）。https://ec.europa.eu/growth/tools-databases/enorm/mandate/613_en。これは2023年5月の標準化要求（M/593）（CEN/CENELECのdraft期限が2025年4月だった）の修正版。
 - リスク管理システム（第9条関連）
 - データセットのガバナンスと品質（第10条関連）
 - ログ能力を通じた記録保管（第12条関連）
 - 透明性と情報提供（第13条関連）
 - 人間による監督（第14条関連）
 - 正確性の仕様（第15条関連）
 - 堅牢性の仕様（第15条関連）
 - サイバーセキュリティの仕様（第15条関連）
 - 品質管理システム（市場流通後モニタリングプロセスを含む）（第17条関連）
 - 適合性評価（第43条関連）
- CENとCENELECは2026年7月22日、AI法の実施を支援するために開発された初の整合規格である[EN 18286「人工知能：EUのAI法規制目的のための品質管理システム」](#)を発行。
 - 欧州委員会は2026年後半に、当該整合規格に関するレファレンスをEU官報に掲載する予定（<https://www.cencenelec.eu/news-events/news/2026/newsletter/ots-75-anec/>）。EU官報に掲載されると、整合規格に基づく適合性の推定が適用される。
 - ISO/IEC 42001「情報技術—人工知能—マネジメントシステム」（2023年12月発行）との関係については、「両規格は補完的な関係にあり、組織はISO/IEC 42001をベースにAI管理体制の土台を作り、その土台の上に、EN 18286を用いてAI法特有の要件への対応を上乗せするという使い方をすることができる」（<https://webdesk.jsa.or.jp/common/W10K0620?id=1740>）。

6. クラウド・AI開発法案、サイバーセキュリティとAIに関する行動計画

- 欧州委員会は2026年6月3日、欧州技術主権パッケージの一環として「[クラウド・AI開発法案（CADA）](#)」を公表。
 - <https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act>
 - 欧州委員会通信総局の法案責任者の1人は5月、同法案は[EUが技術植民地のような状態に陥り、自国の製品を開発できなくなることを避けることが目的](#)と述べている。<https://www.politico.eu/article/cloud-law-will-stop-europe-becoming-technological-colony-commission-official-says/>
- CADAはクラウドとAIにおけるEUのリーダーシップを強化する「[AI Continent Action Plan](#)」（AI大陸行動計画）の中核部分。[今後5～7年間で欧州のデータセンター容量を3倍](#)に増加し、AI普及促進のために「Apply AI戦略」の役割を強化。
- AIへの需要が高まり続ける中、データセンター・クラウド・コンピューティング容量の供給需要に対応できる必要。現状では[長期にわたる許認可手続き](#)、[エネルギー・土地・資金への限られたアクセス](#)などが、欧州におけるデジタルインフラの拡張を困難に。さらに、[EU域外のクラウドサービスプロバイダーへの過度の依存](#)は、欧州のデジタル自律性とレジリエンスにとって重大なリスクに。
- CADAはこれらの課題に対処するために、持続可能なクラウドとデータセンターの導入をより容易かつ迅速に行えるようにし、欧州の技術主権を強化し、重要なデジタルインフラにおける戦略的依存度を低減。また、重要分野におけるクラウドとAIの展開を加速させると共に、[EUのパートナーに対して市場を開放](#)し続ける。
- 以下の3領域に焦点。
 1. 研究・開発・イノベーション： 次世代の最先端かつ持続可能なクラウドとAI技術の展開に向けた取組みを支援
 2. 容量： EU全域でデータセンターの展開環境を加速させ、公共部門の重要な機能を強化する施設に重点
 3. 自律性： クラウドとAIの主権を評価するEU共通の主権フレームワークの導入と、公共部門における導入メカニズムの導入

○CADAの3領域

1. 研究・開発・イノベーション	- 次世代の最先端クラウドおよびAI技術の開発を支援。特に、フロンティアAI、産業AI、フィジカルAIの分野に注力。 - これらの目標を達成するために、将来の研究開発・イノベーション活動を推進する「グランド・チャレンジ」を導入する。 - 加盟国における国家クラウド・AI戦略、および「AI経験・加速センター」を通じて、戦略的な産業部門および公共部門におけるクラウドとAIの導入を保証。
2. 容量 (Capacity)	- 今後5～7年以内に、EUのデータセンター容量を少なくとも3倍に増加。 - データセンターの許認可および展開を簡素化・迅速化。 - エネルギー・土地・水・資金といった重要な資源へのアクセスを改善。 - AI、クラウドサービス、データ集約型アプリケーションをサポートするために十分なコンピューティング容量を確保。
3. 自律性 (Autonomy)	- クラウドおよびAIの主権を評価するための、EU共通の主権フレームワーク（sovereignty framework）を導入。 - 重要分野におけるクラウドとAIの導入を加速させると同時に、市場の大部分をEUのパートナーに開放し続ける。 - クラウドとAIにおけるEUの付加価値を促進し、EUベースのイノベーションとサプライチェーン・レジリエンスへの貢献を奨励。 - 公共機関が共同購買力を活用できるよう、EUレベルで共通の調達枠組みを確立。 - レジリエンスを強化するために、オープンソースソリューションを促進。

○クラウド・AI主権の定義（主権フレームワーク）

- CADAは、4つの保証レベルから成るクラウド・AI主権を定義し、公共機関は自らのリスク評価に基づいてこれらの基準を利用。クラウドサービスプロバイダーは、監査の後、加盟国からこのフレームワークの下で認定を受ける。
 - レベル1： EU域内に位置するインフラにおいてデータが処理され、保存される。
 - レベル2： プロバイダーは第三国からの独立性と自社のソフトウェアサプライチェーンの透明性を証明しなければならない。
 - レベル3： プロバイダーはEU域内で所有およびEU域内からコントロールされていなければならない、従業員の国籍などの追加基準も満たさなければならない。欧州委員会は第三国のプロバイダーを認定することが可能。
 - レベル4： プロバイダーは自社のソフトウェアサプライチェーンを完全に透明性をもってコントロールし、第三国からの干渉を受けない。

- 欧州委員会は2026年7月7日、「[サイバーセキュリティとAIに関する行動計画](#)」を公表。[Mythos Preview](#)の問題を受け、サイバーセキュリティにおける[高度なAIモデルのリスクに対処](#)するための体系的な対応策を定めたもの。

https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1544、<https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence>

○ Piller1：欧州のサイバーセキュリティのために、フロンティアAIを安全でアクセス・展開可能なものにする

1. [AI法に基づく監督・執行](#)： AI法に基づき、汎用目的AIモデルは、EU市場に投入される前に評価され、リスク軽減策が検討される必要。
 - AI法では、汎用目的AIモデルに対する義務は2025年8月2日から適用開始済みだが、それらのプロバイダーに対する罰金のみは2026年8月2日から適用開始。
2. [AI評価能力の強化](#)： サイバーセキュリティ分野を対象としたEU域内のAI評価能力の構築に向けた公募を開始し、2027年の運用開始を目指す。AIの能力とリスクに関する第三者評価能力を強化することで、AIオフィスの規制機能に貢献。
3. [フロンティアAIへのアクセスの確保](#)： 欧州サイバーセキュリティ機関（ENISA）と協力して、サイバーセキュリティのための高度なAI能力への構造化されたアクセスに関する欧州の青写真を策定し、企業や組織がAI事業者からアクセス許可を得るためのEUとしての基準を示す。
4. ENISAと欧州委員会の共同研究センターはシミュレーション環境の利用を含め、[サイバーセキュリティの観点からAIをテストするための安全なプラットフォームを構築](#)する。これにより、金融・エネルギー・医療・運輸・行政分野等に対してAIの安全利用に関するノウハウを提供。

○ Piller2：AI時代に向けたEUのサイバー・エコシステムの整備

- 企業や組織における脆弱性への対応と重要インフラの保護、およびサイバーエコシステムにおける関係者間の連携を、ENISAが支援。

○ Piller3：サイバー分野における欧州のAI能力の拡大

- 欧州市場の規模拡大を促進するため、AI活用型サイバーセキュリティ・ソリューションのコンテスト「EUグランドチャレンジ」を開始。
- その他、[G7、国連、UK AISI主導のINAMES](#)（旧AISII国際ネットワーク）、[各国政府、フロンティアAI事業者、NATOとの連携](#)を促進・強化。

- 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、AI規制/AI倫理、海外政策動向調査
- 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
 - 2023年～ 日本セキュリティ・マネジメント学会 代議員(2025年～ 執行理事／編集部会長)
- 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
- 主な論文等
 - 「米欧政府のAI安全性へのコミットメントと国際AI安全性レポート：日本はAI安全面でプレゼンスを発揮できるのか」(IISE調査研究レポート、2026年6月)
 - 「EUのデジタル・オムニバス規則案におけるGDPR改正とAI開発の促進」(IISE調査研究レポート、2025年12月)
 - 「AIが意識を持つと社会はどうなるのか：リスクと対策」(IISE調査研究レポート、2025年5月)
 - 「AI倫理原則の規範倫理学的根拠の探求」(日本セキュリティ・マネジメント学会誌2024年度第3号)
 - 「EUのAI法(AI規則)の概要」(JEITA個人データ保護専門委員会講演資料、2024年7月)
 - 「『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)

I I S E