ChatGPT

EU AI法（AI Act）に関する包括的調査レポート

法的影響：AI Actの法的枠組み・定義・義務・罰則

リスクベースの法的枠組み: EUのAI法（AI Act）は、AIシステムをリスクに応じて4つのカテゴリーに分類し、それぞれ異なる規制を設ける包括的な法制度です [1]。**「許容できないリスク」**(Unacceptable Risk)に分類されるAIシステムは、人間の尊厳や基本的人権を著しく侵害する恐れがあるものとして**使用が禁止**されます（例：政府による社会的スコアリング、個人の行動を歪める操作的技術、法執行機関による公共空間での無差別のリアルタイム遠隔バイオメトリクス識別など） [2] [3]。**「高リスク」**に分類されるAIシステムは、**厳格な要件**を満たした上で利用が許可される領域で、**人々の健康・安全・基本権に深刻なリスクをもたらす可能性**のあるものです [4]。具体例として、インフラや医療機器の安全性制御AI、教育や雇用（履歴書の自動選別等）へのAI利用、金融サービスの信用評価AI、司法・法執行領域のAI（犯罪リスク評価等）などが Annex III に列挙され高リスクとみなされます [5] [6]。**「限定的リスク」**(Limited Risk)のAIシステムは、リスクは小さいものの**透明性義務**が課され、人がAIと相互作用していることを通知するなど信頼性確保の措置が求められます [7]。例えば、チャットボットなど人がAIと対話する場合は「これはAIです」と明示することや、生成AIによるコンテンツ（ディープフェイクや公共情報に関する文章など）にはその旨の表示を付けることが義務付けられます [8]。**「最小リスク」**(Minimal or No Risk)のAIシステム（多くのゲームAIやスパムフィルタ等）は現時点では追加規制の対象外です [9]。

定義の明確化: AI Actでは「AIシステム」を広く定義し、機械学習や統計手法、論理に基づく手法など**様々な技術を含むソフトウェアシステム**を対象としています [10]。定義上、ある程度の**自律性**を持ち、デプロイ後に適応的な振る舞いを示しうるシステムで、与えられた目標に対して予測・推論・意思決定・コンテンツ生成などを行うものがAIシステムに該当します [10]。また**「汎用目的AI」**(General-Purpose AI)も定義されており、幅広いタスクに利用可能で他のサービスにも組み込まれる**基盤モデル**（Large Language Modelなど）を指します [11]。このように定義を広くとることで、今後登場する新たなAI技術もカバーしようとしています。

高リスクAIへの具体的義務: 高リスクAIシステムを提供・開発する企業や組織には、製品を市場投入する前に以下のような**具体的な法的義務**が課されます [12]：

- **リスクマネジメント:** システムごとの**リスク評価と軽減策**を実施し、潜在的な危険を特定・低減 [13]。特に人権侵害や安全上のリスクについて継続的に分析する体制が必要です。
- **データガバナンス:** 学習データや訓練データに関する**高品質・適切性の確保**。偏りや差別的結果を生まないようデータセットを検証し、不備があれば是正する義務があります [13]。
- **技術文書の作成:** システムの仕様・目的・アルゴリズムの説明など**詳細な技術文書と記録**を整備し、当局が要求した際に提供できるようにします [14]。システムの設計意図やテスト結果、リスク分析の内容を網羅した文書が求められます。
- **透明性と情報提供:** 利用者や導入者 (deployer) に対し、AIシステムの性質・目的やそのAIが生成したアウトプットの意味合い等、**適切な情報提供**を行う義務があります [15]。例えば、AIが下した判断の根拠を説明できるように準備するなどが該当します。
- **人的監督: 適切な人的監視(ヒューマン・オーバーサイト)** を確保する措置も必要です [15]。具体的には、AIの判断を人間が検証・介入できる仕組み（例：重要な決定には人間の最終承認を要件とする等）を設けることが期待されます。
- **堅牢性・安全性:** システムの**堅牢性、サイバーセキュリティ及び精度**を高い水準で担保すること [16]。外部からの不正アクセス耐性や、予期せぬ入力に対する挙動の安定性、一定の精度要件を満たすことなどが含まれます。

その他の関係者の義務: 高リスクAIをEU市場に投入する際には、単に開発者（提供者）だけでなく、**輸入業者**や**流通業者**、**下流ユーザー**にも一定の義務が課されます [17]。例えば、輸入業者・販売業者は適合宣言やCEマーキング等の規制順守を確認する義務、導入して使用する事業者（デプロイヤー）は適切な監視や不具合報告を行う義務などがあります（AI Act第16〜26条）。また**一般用途AIモデル**(GPAI)についても後述のとおり独自の義務規定（第52〜55条）が設けられました。

罰則規定: AI ActにはGDPRを参考にした**重い制裁金**の規定があります。禁止された用途（上記「許容できないリスク」のAI、AI Act第5条違反）を提供・使用した場合、**最大3,500万ユーロまたは世界年間売上高の7%**の行政罰金が科され得ます [18]。高リスクAIに関する要件やその他の義務（第5条以外の義務）に違反した場合は**最大1,500万ユーロまたは売上高の3%**まで、それ以外にも当局への虚偽・不備の情報提供等の違反には**最大750万ユーロまたは売上高の1%**までの罰金が規定されています [19] [20]。違反企業の規模や悪質性等に応じて罰金額は調整され、中小企業については上限金額または率の**低い方**が適用される考慮もされています [21]。各加盟国の監督当局が違反を調査し、是正勧告や制裁を科す仕組みで、科された罰金や処分は毎年欧州委員会へ報告されます [22] [23]。このような高額の罰則規定は、AI Actの遵守を企業に強く促すとともに、**グローバル企業にとってもEU市場での非遵守は重大な財務リスク**となることを意味します [24]。

スケジュール詳細：段階的な施行スケジュール

法律の発効と全体的な適用開始: EUのAI法は**2024年8月1日**に欧州連合官報で公布・発効しました [25]。しかし発効時点では企業への直接的な義務は生じず、**2年間の移行期間**を経て**2026年8月2日**から本格的に適用が開始されます [25]。この2年間で各種準備措置や段階的施行が行われる計画です。以下、重要なマイルストーンを時系列で示します [26] [27]。

- **2024年8月1日: AI Act発効**。法的には効力を持ち始めますが、この時点では義務の適用はなく、各国は監督当局の指定準備など実施段階へ移行 [28]。
- **2025年2月2日: 禁止事項とAIリテラシー教育義務の適用開始** [29]。この日から、AI Act第5条で定める**禁止AIシステム**（許容不可リスクの項で列挙されたもの）の提供・使用が違法となり、また**AIリテラシー向上**（市民や労働者へのAIに関する教育啓発）に関する加盟国の義務が発動します [29]。
- **2025年5月2日: コードオブプラクティス（実務規範）の策定期限** [30]。AI Act第56条(9)に基づき、欧州委員会が主導する**自主的な行動規範**（後述の汎用AIコード）等がこの日までに準備されることになっていました [30]。
- **2025年8月2日: 段階的施行の主要な開始日**。この日から以下の規定群が適用となります [31] [32]：
- **汎用目的AIモデル（GPAI）に関する義務**（第52〜55条）が**適用開始**。 [33] [34] すなわち、大規模言語モデル等の提供者に対する透明性確保・著作権順守・（該当する場合）安全対策義務が法的に要求されます。これに合わせ、**「汎用AIコードオブプラクティス」**（後述）が発効しました。
- **AIガバナンス体制**の稼働：加盟各国はこの日までに国内の**監督当局および通知機関**を指定し公開する義務があり [35]、**欧州AI委員会（AI Board）**や**欧州AI事務所（AI Office）**といった枠組みの活動が開始します [36]。またAI Actの**罰則規定**（前述の行政罰金の条項）もこの日から適用され、各国は**罰則の国内ルールを整備**して欧州委に通知する必要があります [37]。
- **認証機関（ノーティファイドボディ）制度**の開始：高リスクAIの適合性評価を行う第三者認証機関に関する規定もこの日から適用されます [38]。これにより、AIシステムの認証プロセス構築が本格化します。
- **2026年2月2日: 高リスクAIに関するガイドライン**の策定期限 [39]。AI Act第6条（高リスク分類基準）および第72条（事後モニタリング計画）に関し、欧州委員会が**実施指針（ガイドライン）**を策定・公表する期限です [40]。これによって企業が高リスクAI要件を実務的に実装する際の手引きが示される見込みです。
- **2026年8月2日: AI法の本格施行（一般適用開始）** [41]。移行期間満了に伴い、**AI Actの大部分の規定がこの日から全面的に施行**されます [42]。高リスクAIシステムに関する要求事項（リスク管理や技術文書、適合宣言等）もこの日までに遵守が必要となり、違反は制裁対象となります [43]。なお、適用開始時点ですでに市場投入済みの**既存の高リスクAIシステム**については、この日以降に設計上の重大

な変更を行う場合にはAI Act準拠への更新が求められます [44] 。また加盟各国は**少なくとも1つのAIレギュラトリーサンドボックス**（規制実験空間）を設置・運用開始する義務があります [45] 。

- **2027年8月2日: 特定分野への猶予期限**。一部の規定は上記よりさらに長い経過措置が認められており、例えば**既存の特定製品（おもちゃ、医療機器、車両等）の中に組み込まれたAIシステム**で高リスクに該当するものは**2027年8月2日まで**適合猶予があります [46] [47] 。また**2025年8月2日より前に市場投入された汎用AIモデル**についても、この日までにAI Actの義務に合致するよう**2年間の移行措置**が設けられています [48] [49] 。つまり既存の基盤モデル提供者は2027年までに透明性や安全性の措置を講じ直す必要があります。
- **2030年12月31日:** Annex Xにリストされた**大規模ITシステム（役所の大型情報システム等）**に組み込まれたAIシステムで、2027年8月前から運用されているものについては**2030年末**までの長期猶予が与えられています [50] 。

以上のように、AI Actは2024年〜2026年にかけて段階的に適用範囲を広げ、2026年以降は**全面施行**、さらに一部例外措置を経て2030年頃まで完全浸透を目指すスケジュールです。特に**2025年8月**と**2026年8月**が重要な節目となっており、企業はこれら期限に合わせてコンプライアンス計画を立てる必要があります。

汎用AIコード・オブ・プラクティス: 上記スケジュールに関連し、**「汎用目的AIコード・オブ・プラクティス」**（General-Purpose AI Code of Practice）という業界の自主規範が2025年8月に公開・適用されました [51] 。これはAI Actにおける汎用AI提供者の義務（透明性、著作権順守、安全管理等）を具体化した**任意参加のガイドライン**であり、OpenAIやGoogleなど主要企業を含む多数のAI企業が署名・参加しています [52] [53] 。このコードは**透明性**（モデルの説明と文書化） [54] 、**著作権**（学習データにおける知的財産権尊重） [55] 、**安全・セキュリティ**（高度な基盤モデルにおけるリスク管理） [56] の3章からなり、企業が法の発効前から自主的に遵守できるよう実務的な指針を提供しています。EU委員会はこの自主規範を**AI Act本格施行までの橋渡し**と位置づけており、2025年8月以降はこのコードへの署名企業リストを公開しつつ、**必要に応じて法的拘束力のある実施法**により汎用AI義務の詳細を定める用意も整えています。

ビジネスへの影響：産業界へのインパクト、コストと機会

AI Actは幅広い業種のビジネスに影響を与えると予想されます。特に**AI技術を扱う企業**や、AIを活用する**各産業分野（SaaSサービス、医療、金融など）**において、**コンプライアンス対応コスト**や**事業機会の変化**が生じるでしょう。以下、主な業界別の影響を概観します。

- **AI開発企業・SaaSプロバイダ:** AIアルゴリズムや基盤モデルを開発・提供する企業、および自社のクラウドサービスにAI機能を組み込むSaaS企業にとって、AI Actは**設計・開発プロセスの高度な見直し**を迫ります。**高リスクに該当するAI**（例：人事評価や医療診断機能を持つSaaS）はリリース前に大幅なテストと文書化が必要となり、その分**開発コストが増大**します [57] 。中小のスタートアップにとっては**遵守負担**が相対的に重くなり、新規参入のハードルになる懸念があります。一方で、いち早く規制を織り込んだ「**倫理的AI**」を提供することは**競争優位**になり得ます。EU市場でビジネスを行う以上、**透明性や説明可能性**を高めたAIモデルを提供しなければ信用を失うため、企業は説明可能なAI（Explainable AI）への投資や、バイアス低減の取り組みを強化する動きが見られます [58] 。大手クラウド企業も顧客企業のコンプライアンス需要に応じ、AIサービスに関する**コンプライアンス支援機能**（例えばモデルカードの提供や監査ログ機能など）を拡充する可能性があります。

- **医療分野:** 医療・ライフサイエンス領域ではAIの活用が進んでおり、画像診断AIや患者データ分析AI、手術ロボットのAI制御など多岐にわたります。この分野のAIはしばしば**人的生命・健康に直接影響**するため**高リスクAI**に該当します [59] 。医療機器に組み込むAIは従来からCE認証等が必要でしたが、AI Act施行により**追加の適合評価**や**当局への登録**（高リスクAIはEUデータベースへの登録義務があります）などが必要になり、**製品開発サイクルが長期化**する可能性があります。またアルゴリズムの**透明性要求**により、医療AIの提供企業は医師や患者に対し**AIが提示する診断結果の根拠**を説明できるようにしなければなりません。これはブラックボックス型のディープラーニングに対する説明手法の開発

を促進するでしょう。医療データは個人情報でもあるため、AI Actと併せてGDPR等の他法令との複合遵守も課題です [60]。もっとも、規制に適合した医療AIは安全性・信頼性が保証された製品として市場で評価され、**患者や医療従事者の信頼向上**につながるという**機会**もあります。

- **金融分野:** 金融業界では与信（クレジットスコアリング）や不正検知、資産運用アドバイスなどにAIが活用されています。これらは個人の機会や経済的権利に重大な影響を与え得るため**高リスクAI**と分類され、偏りのないモデル構築や人による判断介入など**厳格な管理**が必要になります [61] [62]。例えば融資審査AIについては**アルゴリズムのバイアス評価**を行い、人種や性別による差別がないか継続監査する体制が求められます [63]。また、顧客に対して「この審査にはAIを用いています」と通知したり、説明を求められれば理由を開示する義務も発生します。金融機関にとってはこれら対応に**コンプライアンスコスト**が増す一方、AI Act準拠を果たすことで**顧客からの信頼**を得て差別的取扱い等のリスク低減につながります。規制を順守しないAIモデルの利用は各国の金融当局からも問題視されるため、結果的に**グローバルな金融グループ全体でAIガバナンスを強化**する動きが必要になるでしょう [64] [24]。

この他、**人事労務（HR）領域**もAI Actの影響が大きい分野です。履歴書の自動スクリーニングや従業員のモニタリングAIは高リスクに分類され、企業が知らずに使っている場合でも**そのAIのせいで不当な差別や不利益を生じさせれば企業に責任**が及ぶ可能性があります [65] [66]。このため人事部門では導入するAIツールのアルゴリズムを精査し、公平性を監督することが求められます。また**マーケティング**や**小売**の分野でも、チャットボットやレコメンドエンジンへの透明性義務が生じるため、顧客対応におけるAI活用のルール策定が必要になります。

総じて、AI Actは**「信頼あるAI」**をビジネスに組み込むことを強制し、短期的にはコスト増や事業戦略の見直しを迫りますが、中長期的には**AIの品質向上とユーザーからの信頼獲得**を通じて市場拡大につなげるチャンスともなりえます。企業にとって重要なのは、受動的に規制遵守するだけでなく、**コンプライアンスを競争力強化とイノベーション推進に結びつける戦略**を描くことです。

技術的要件：汎用AIモデルと高リスクAIへの技術的・倫理的・透明性要件

高リスクAIシステムの技術要件: 高リスクに分類されるAIを扱う企業は、前述のようなリスク管理プロセスやデータガバナンス以外にも、システム設計において**具体的な技術上の要件**を満たす必要があります [67]。例えば以下のようなポイントが技術要件として挙げられます。

- **精度・ロバスト性の確保:** 高リスクAIは**十分な精度**を達成し、環境や入力の変動に対して**ロバスト（頑健）**であることが求められます [16]。これは、誤検知や誤分類が人命や権利に関わる領域であるため、統計的な性能指標（正答率やエラー率など）が一定基準以上であることや、外れ値や悪意ある入力に対しても安定して動作する設計が必要という意味です。
- **セキュリティ対策:** システムがサイバー攻撃によって不正に操作されたり、トレーニングデータへのデータポイズニング等で性能を劣化させられたりしないよう、**サイバーセキュリティ対策**も技術要件の一部です [16]。モデルの堅牢性テストや、推論結果の改ざん検知、対策手順の文書化などが含まれます。
- **人が理解できる説明可能性:** 高リスクAIには**説明可能性**(Explainability)も強く求められます [58]。すなわち「なぜそのような結果や判断に至ったのか」を人間の担当者や監督官庁に説明できるよう、モデルの決定プロセスを追跡・説明する機能が望まれます。具体的には、モデルの重要変数の可視化や、意思決定ルールを説明するアルゴリズム的手法（例：決定木への近似）などが奨励されます。これは必ずしもAI Act本文に明示的規定があるわけではありませんが、**透明性義務**や**人的監督義務**を果たす上で**技術的な実装**として不可欠となる部分です。

汎用目的AIモデルへの要件: 近年発展した大規模言語モデル等の**汎用目的AI**(General-Purpose AI, GPAI)についても、AI Actでは**専用の章（第V章）で規定**が設けられています [38]。汎用AIモデルはそれ自体は特定用途に限定されないためリスク分類が難しい面がありますが、AI Actでは**「透明性」と「著作権配慮」**をキーワードに、提供者への以下のような要件を定めました [33]。

- **モデル情報の開示・透明性:** 汎用AIモデルの提供者は、自らのモデルを他者が組み込んで利用する際に備え、**モデルの仕様や用途、制限事項に関する情報**を文書化して公開する義務があります [51] [68]。具体的には、モデルの基本機能や意図された用途、訓練に使われたデータの概要、既知の限界や偏向性などをまとめた**「モデルカード」**等のドキュメントを提供しなければなりません。EU委員会はこのために**「公開用訓練データ概要テンプレート」**も提示しており、主要なデータソースのドメイン名やデータ取得元、データ前処理の方法等を一覧できるよう標準化しています [69]。この透明性要件により、下流の開発者やユーザーがその基盤モデルの特性を理解し、適切にリスクを管理できるようにします。
- **著作権と法令順守:** 基盤モデルの提供者には、モデルが**他者の著作物を無断で学習データに利用していないか**、生成コンテンツが著作権侵害にならないかに配慮する**ポリシー策定義務**も課されました [55]。例えば、ウェブ上から収集したデータで学習する場合でも、EUのデジタル著作権指令等に照らして適法に行われる必要があります。コード・オブ・プラクティスの「著作権」章では、モデル提供者が**著作権法順守のための社内ポリシー**を策定・実施することや、権利者からの申し立てに対応する仕組みを提案しています [70]。
- **高性能モデルへのリスク対策:** 特に**極めて高い能力を持つ基盤モデル**や**広範に普及したモデル**は、社会に与える影響も大きいため**「システミックリスクを伴う汎用AIモデル」**として追加の管理が求められます [71] [56]。AI Act第55条では、そうしたモデルの提供者に対し**リスクアセスメントと軽減策の実施**（高リスクAIと同等のリスク管理義務）や**安全性検証**を義務付けています [72] [71]。例えば大規模言語モデルがデマの拡散や模倣攻撃に使われるリスクがある場合、事前にフィルタリングや安全対策を講じ、その結果を当局に示す必要があるでしょう。

限定的リスクAIの要件: 「限定的リスク」に分類されるAIシステムについても、技術的・倫理的観点から**最低限の透明性要件**が規定されています [7]。具体的には、ディープフェイク（AIによる合成音声・画像等）やチャットボットなど、人間がAIから生成された情報を**人の産物と誤認する恐れ**があるケースで、**そのAI起源を明示する義務**です [8]。例えばソーシャルメディア上でAI生成の画像を用いる場合は透かしや注記で「AI生成」とわかるようにし、公衆に情報発信する文章をAIが自動生成したならその旨を表示します [73]。また、ユーザーが対話している相手が人間でなくAIである場合（チャットボット応対など）は、その事実を通知しなければなりません [7]。これら措置により、ユーザーがAIか人間かを認識した上で対応や判断ができるようにし、AIによる欺瞞や誤解を防ぐことが狙いです。

以上のように、AI Actは**AIシステムのライフサイクル全般**にわたり、設計・開発段階から運用・利用段階まで技術的な注意義務を網羅しています。倫理的原則（公平・説明責任・プライバシー保護など）を具体化する形での技術要件が盛り込まれており、AI開発者はこれを踏まえて**「倫理設計(ethical by design)」**を行うことが求められるでしょう。

遵守戦略：企業がAI Actに準拠するための方法と支援策

企業の遵守へのアプローチ: AI Actへの適合は、多くの企業にとって初めて直面する包括的なAI規制対応となります。以下のような**ステップ・戦略**を取ることが推奨されています [74] [75]。

1. **社内AIシステムの棚卸し（AIマッピング）:** まず自社が利用・提供している全てのAI機能やシステムを洗い出し、それぞれが**AI Actの対象となるか**、なればどのリスク区分に当たるかを分類します [76] [77]。AI Act上の「AIシステム」に該当するか判断が難しいケースもあるため、法務や技術の専門家と協力してグレーゾーンを整理することが重要です。また自社だけでなく**取引先や下請けのAI活用状況**も確認し、サプライチェーン全体でのAI利用実態を把握します [78]。

2. **リスク分類と要求事項の特定:** 洗い出したAIシステムを**リスクレベル別に分類**し、それぞれに適用される義務（高リスクなら技術文書や適合評価が必要、限定的リスクなら表示義務のみ等）を整理します[77]。高リスクに該当する場合は**外部の適合性評価**（認証）が要るか否かも確認します。必要に応じてこの段階で専門のコンサルタントや認証機関と連携し、具体的な適合手順を検討するのも有効です[79]。

3. **AIガバナンス体制の強化:** 社内に**AIガバナンスの仕組み**を構築します[80]。具体的には、法務・コンプライアンス部門だけでなく、AI開発部門やIT部門、業務部門など**横断的なチーム**を編成し、AI Act対応の統括役割を担わせます[81]。社内ポリシーとしてAIの開発・利用指針を策定し（例えば「AI倫理ガイドライン」）、**AIの設計・デプロイ・運用時に遵守すべき手順**を定めます[82]。さらに取締役会レベルでもAIリスクを監督する役割者を置き、**経営陣の責任範囲**にAIガバナンスを組み込みます[83]。

4. **既存コンプライアンスとの統合:**　新たなAIポリシーや体制は、既存の情報セキュリティ・個人情報保護・製品安全等のコンプライアンス制度と**統合的に運用**される必要があります[84]。例えば、AIに関する内部監査チェックリストを既存の内部統制プロセスに追加したり、AIリスク評価をプロダクト開発の既存ゲートプロセスに組み込む等、**社内ルールの整合性**を図ります。これにより効率的かつ漏れのない遵守が可能になります。

5. **トレーニングと文化醸成:**　現場の開発者や製品担当者、営業・マーケティングなど関係者に対し、**AI Actの要点や倫理的AIの重要性について教育**します[85]。具体例を交え、自社のどのプロジェクトが高リスク相当か、何に注意すべきかを周知することで、単なる法務チェックに留まらず**組織全体で倫理的AI開発文化**を醸成します。

6. **専門家との連携と最新情報の追跡:** 自社内にノウハウがない部分は**外部の専門家**（AI倫理コンサルタントや法律事務所等）から助言を得ます[86]。またAI　Actは今後運用面で解釈ガイダンスが更新されたり、他国規制とも相互作用するため、**最新動向をウォッチ**し続けることが重要です[75]。欧州委員会や各国当局から出されるQ&A、ガイドラインを定期的に確認し、必要に応じて**業界団体のセミナーや情報共有の場**に参加します。

EUや業界からの支援ツール:　欧州委員会および業界団体も、企業の遵守を支援するため様々なリソースを提供しています。

- **EU委員会のガイドライン:**　2025年7月には、**「汎用AIモデル提供者の義務の範囲に関するガイドライン」**が公開され、GPAI提供者が誰でどこまで遵守すべきか明確化が図られました[87]。また**禁止AIの解釈指針**や**高リスク判断の具体例**についても委員会やAI委員会から随時ガイダンスが出されています[88]。

- **コード・オブ・プラクティス（実務規範）:** 前述の**汎用AIコード**は自主的とはいえ**実質的なコンプライアンスツール**として機能します[89]。署名企業はこのコードのモデル文書フォームを活用して透明性情報を整理でき、また安全管理のベストプラクティスを共有できます[54][90]。他にも**「AI　Pact」**と称される自主宣言プログラムがあり、EUは企業に早期参加を呼びかけています[91]（AI　Act施行前に自主的にAI倫理原則を受け入れる誓約で、後の規制対応に役立てる狙い）。

- **チェックリスト・自己診断ツール:** 民間ベースで、例えばFuture of Life Instituteが提供する**「AI Act コンプライアンス・チェッカー」**[92]や、中小企業向けガイド[93]など、質問に答えることで自社システムの該当規制や必要措置を教えてくれるオンラインツールがあります。これらは非公式ながら実務的な第一歩として参考になります。

- **規制サンドボックス:** 各加盟国に設置される**AI規制サンドボックス**では、企業が新規AIソリューションを**当局の監督下でテスト**し、規制適合を試行できる場が提供されます [94]。これにより革新的AIの開発者も委縮せず実験が可能になり、当局から助言を受けつつ改善できます。

- **標準化と認証支援:** EUはAI Actに対応する**技術標準**の策定を欧州標準化機関(CEN/CENELEC等)に依頼しており、2025年以降順次**ハーモナイズドスタンダード**が公表される見込みです。企業はこれら標準に従うことで効率的に「**推定適合**」を主張でき、適合評価も簡易になるメリットがあります。また認証機関やコンサル会社からは**適合性評価に向けたテンプレート**や**リスク管理フレームワーク**の提供も始まっています。

このように多角的なサポートを活用しつつ、企業は**能動的かつ計画的にAI Act順守体制を整備**することが求められます。単なるコストではなく、自社のAIの信頼性を高め差別化する投資と捉えて戦略的に対応することが重要です。

他地域との比較：米国・中国・日本のAI規制との相違点

EUのAI Actは世界で初めての包括的なAI法として注目されており、**他の主要地域**（米国、中国、日本）もそれぞれ異なるアプローチでAIガバナンスに取り組んでいます。それぞれの特徴とEU規制との比較を以下にまとめます。

アメリカ合衆国（米国）

米国には現時点でEUのAI Actに相当する**単一の包括的AI法**は存在しません。連邦政府は主に既存の法律（差別禁止法、消費者保護法、製品安全規制など）や業界ガイドラインを援用してAIを間接的に規制している状況です [95]。例えば、自動車の自動運転AIは自動車安全基準で、医療AIはFDA（食品医薬品局）の医療機器規制でカバーするといった**セクター別規制**が中心です。またAI倫理に関する政府指針として、2022年に**「AI権利章典（Blueprint for an AI Bill of Rights）」**がホワイトハウスから発表されましたが、これは**法的拘束力のない指針**に留まっています。

もっとも近年、生成AIの台頭などを受け**規制強化の機運**も高まっています。2023年10月にはバイデン政権が**AIに関する大統領令**を発し、**高性能AIモデルの事前リスク検証**や**連邦政府調達時の要件**など包括的な施策を打ち出しました。またNIST（米国標準技術局）は**「AIリスクマネジメントフレームワーク」**を策定し、自主的なベストプラクティスとして推奨しています。連邦議会でもAI法制化の議論が進みつつあり、将来的には**連邦AI安全法**のような立法が検討されています [95]。しかしEUのように明確なリスク分類や罰則を定めた法律はまだなく、**業界の自己規制と技術標準**への委ねが大きい状況です。GoogleやOpenAIなど主要企業もEUに倣い自主的な**AI安全プログラム**を発表したり、政府との協力覚書に署名する動きがあります。アメリカは**イノベーション促進を重視**しており、規制においても「柔軟でプロビジョン（原則）ベース」なアプローチを取る傾向があります [96]。EUと比較すると規制の厳しさは控えめですが、今後はEU規制の影響で**グローバル企業が自発的にEU基準を世界標準にする**可能性もあり、米国企業も事実上対応を求められる場面が増えるでしょう。

中華人民共和国（中国）

中国はAI規制において**EUとは異なるアプローチ**を取っています。**単一の包括法ではなく**、分野ごとの行政規則やガイドラインによってAIを統制する戦略です [97]。例えば、2022年には「**アルゴリズム推薦サービス管理規定**」が制定され、ニュースフィードやリコメンデーションアルゴリズムの提供者に対し登録制や内容管理義務を課しました。また**ディープフェイク規制**や**自動運転ガイドライン**など、個別領域ごとに細かな規則が次々と発表されています。特筆すべきは**生成AIに対する規制強化**で、2023年8月には「**生成式AIサービス暫定管理办法**」が施行され、ChatGPTのような生成AIを提供する企業に対し**セキュリティ評価の事前実施**や**生成コンテンツの検閲・違法内容フィルタ**、ユーザーの実名登録制等を義務付けました [98]。つまり中国では**政治**

的・社会的影響の大きいAI（世論形成や社会動員に関わるもの）に特に厳しい規制を敷いているのが特徴です [99] [100]。例えばチャットボットや推薦AIが**「社会の安定を脅かす」**と判断される場合、当局の強権的介入もありえます。

リスク評価の枠組みもEUとは異なり、中国にはEUのような明確な高リスクカテゴリー分類はありません [101]。その代わり、**違法・有害なAI利用は禁止**する一方で、それ以外のAIについては行政当局が個別ケースで判断する形を取っています。EUが人権や倫理を重視するのに対し、中国は**国家安全や社会秩序**への影響を最重視している点で哲学が異なります [102] [103]。またEUでは独立の監督機関による執行ですが、中国では公安や網信弁公室など**政府当局が直接監督・強制**する仕組みです。企業にとっては、EU以上に**運用上の裁量が大きい規制環境**と言え、ケースによっては事前に非公開の当局審査を受けたり、企業内に共産党セルを設け監督を受け入れる必要もあります。

このように中国のAI規制は**統制色が強く、セキュリティ・検閲寄り**ですが、一方でAI産業振興も国家戦略に掲げており、限定的な**サンドボックス**や**技術標準化**の推進も行われています。将来的に包括的なAI法律が制定される可能性も指摘されていますが [104]、現時点では**「規則+標準+試行」**の多層的アプローチが取られています。

日本

日本はEUとは対照的に、これまで**「ガイドライン中心のソフトロー」**でAIガバナンスを進めてきました。しかし最近になって**初のAIに関する包括法**が成立し、独自路線ながら規制と振興のバランスを模索しています。

2023年までは、日本政府は経済産業省による「**AI開発ガイドライン**」(2019)やその後継の「AI社会実装原則（企業向けガイドライン）」（2021年初版、2022年・2023年更新）など、**民間が自主的に遵守する原則**の提示に留めていました [105]。これらはOECDのAI原則に基づき、公平性・透明性・安全性などを掲げつつも法的拘束力はありませんでした。しかし**2024年**に入り、生成AIの普及や各国の規制強化を受けて日本でも議論が加速。**2025年5月**、日本初のAI法となる「**人工知能（AI）関連技術の研究開発及び利用の促進に関する法律**」（略称：AI促進法）が成立しました [106] [107]。この法律はわずか7ページ程度の簡潔なもので、EUのような詳細規制ではなく**国家戦略方針を定めるフレームワーク法**です [108]。AI促進法は**「AIの研究開発・利用を促進しつつ、その成果を経済社会に貢献させる」**ことを目的とし、政府に**AI戦略本部（内閣に設置）**の設立や**AI基本計画の策定**を義務付けています [109]。一方、民間企業（法文上は「AI事業者」）に対しては**努力義務**として「事業効率向上のため積極的にAIを活用すること」 [110] や「国の示す指針に従うよう努めること」など緩やかな規定のみで、**違反に対する罰則や直接規制はありません** [111]。強いて言えば、政府が調査や助言を行う権限があり、協力しない企業名を公表するといった措置が検討されていますが、法律上は明記されていません [112] [113]。

このように日本のAI促進法は**規制と言うより産業振興策**に近いものですが、同法附則や政府方針には**特定の有害なAI利用に対する将来的規制の可能性**も示唆されています [114]。現に、2024年には「AIによる差別的なコンテンツ生成やフェイク拡散への対策」を含む論点整理が政府検討会から出されており、場合によっては個別法による対応もありえます。また、日本政府はG7議長国として**「広島AIプロセス」**を主導し、**Hiroshima AI Guiding Principles**（先進的AIの開発原則）を世界に提唱するなど、国際協調によるルール作りにも力を入れています [115]。これは、単独で厳格規制を敷くより**各国での原則共有と自主的取組を促す**日本の基本姿勢を示すものです。

総じて日本のアプローチは、**「まずはAIを社会に取り入れ、メリットを享受しつつ、問題があれば段階的に規制する」**という**漸進的かつイノベーション重視**の姿勢と言えます [116] [117]。EUのように事前に包括規制を作るのではなく、業界との対話や社会実験を重ねながらガバナンスを進めており、この**「レギュラトリーサンドボックス的」**なアプローチは欧米とも異なる特徴となっています。

以上、EUのAI Actについてその内容と影響、そして他地域との比較を包括的に検討しました。EU AI Actは**人間中心かつ信頼できるAI**の実現を目指すものであり、その動向は各国のAI政策にも大きな影響を与えています。企業はこの規制を単なる制約と捉えるのではなく、**倫理と信頼を基盤としたAIイノベーションの機会**と捉えて積極的に対応していくことが求められるでしょう。

25 2 等

---

1 24 26 27 32 41 43 47 49 50 57 58 61 62 63 64 65 66 74 75 81 83 85 86 How the EU AI Act is Impacting Your Industry and Key Dates - Sheffield Haworth
https://www.sheffieldhaworth.com/how-the-eu-ai-act-is-impacting-your-industry-and-key-dates/

2 3 106 108 109 112 116 117 Japan’s AI Promotion Bill and How It Differs from the EU AI Act
https://ediscoverytoday.com/2025/05/30/japans-ai-promotion-bill-and-how-it-differs-from-the-eu-ai-act-artificial-intelligence-trends/

4 5 6 7 8 9 12 13 14 15 16 25 33 34 46 59 67 68 69 73 87 89 AI Act | Shaping Europe’s digital future
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

10 11 60 97 98 99 100 101 102 103 104 Preparing for compliance: Key differences between EU, Chinese AI regulations | IAPP
https://iapp.org/news/a/preparing-for-compliance-key-differences-between-eu-chinese-ai-regulations

17 18 19 20 21 22 23 Article 99: Penalties | EU Artificial Intelligence Act
https://artificialintelligenceact.eu/article/99/

28 29 30 31 35 36 37 38 39 40 42 44 45 48 93 94 Implementation Timeline | EU Artificial Intelligence Act
https://artificialintelligenceact.eu/implementation-timeline/

51 52 53 54 55 56 70 71 72 90 The General-Purpose AI Code of Practice | Shaping Europe’s digital future
https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

76 77 78 79 80 82 84 91 The Impact of the new EU AI Act on the Healthcare Sector – Part II Practical Guidance – What Businesses need to do
https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2024/04/impact-of-the-new-eu-ai-act-on-the-healthcare-sector-part2.html

88 European Commission Guidelines on Prohibited AI Practices under ...
https://www.insideprivacy.com/artificial-intelligence/european-commission-guidelines-on-prohibited-ai-practices-under-the-eu-artificial-intelligence-act/

92 EU AI Act Compliance Checker | EU Artificial Intelligence Act
https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/

95 96 105 107 110 111 113 114 115 AI Watch: Global regulatory tracker - Japan | White & Case LLP
https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-japan