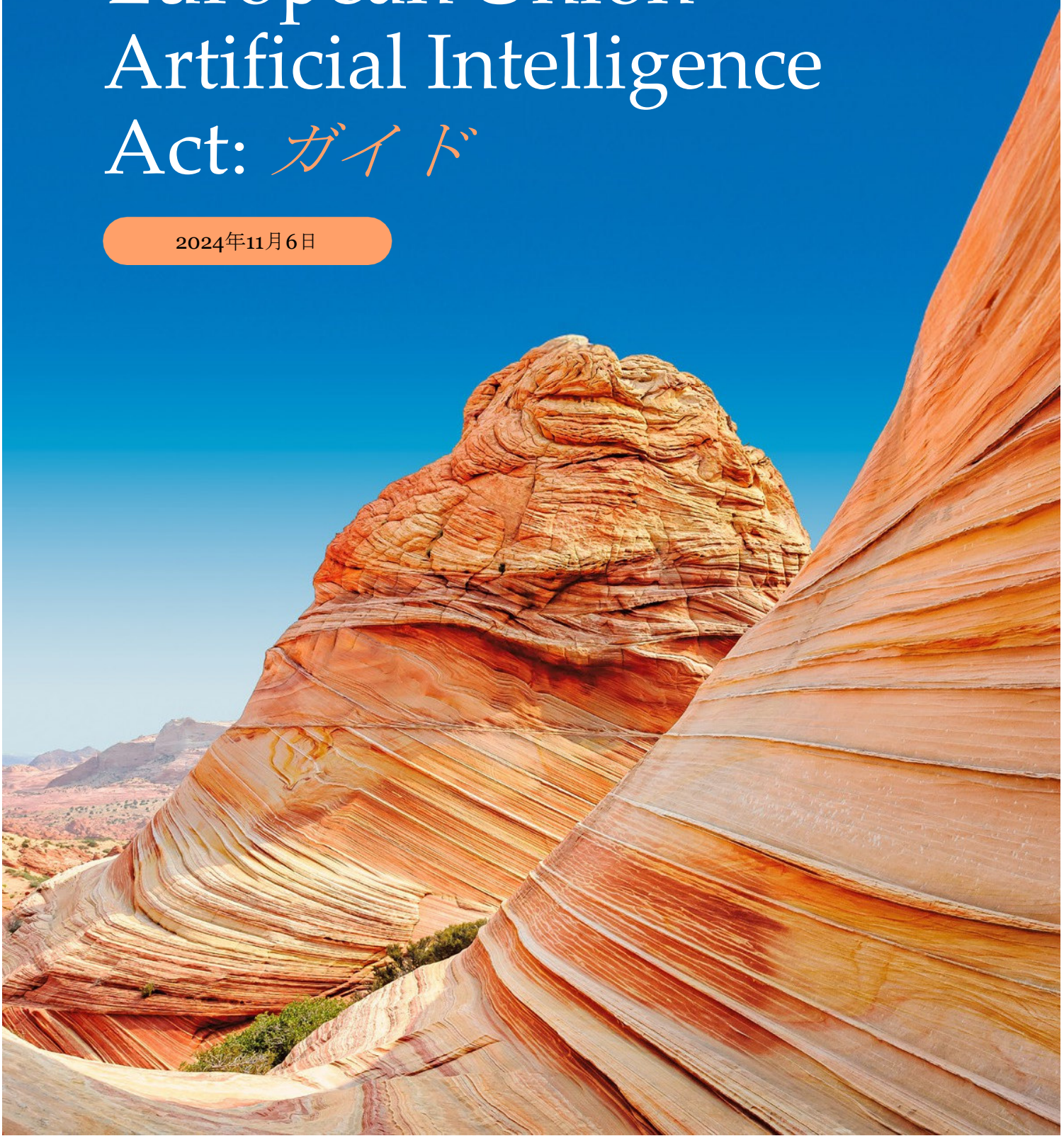
Bird & Bird

European Union Artificial Intelligence Act: *ガイド*

2024年11月6日



コンテンツ

概要、主要なコンセプト、タイムライン

概要

欧州連合（EU）は、人工知能（AI）規制のパイオニアとして、倫理と責任が担保されたAI開発を行うための積極的な取組みにより、世界的な基準を示している。実際に、GDPRが及ぼした影響力を彷彿とさせるような、新たなブリュッセル効果を目の当たりにすることになりそうだ。EUの包括的かつ予防的な枠組みは、透明性、アカウンタビリティ、人権を優先するものである。

AI Actは、EUの枠を超えて適用される。すなわち、同法の多くの条項が、プロバイダーの設立地または所在地がEU域内か第三国であるかを問わず適用される。同法は、AIシステムの導入に責任を負うプロバイダーや事業体に対し、EU域内において「システムにより生成されたアウトプットの使用が意図される (the output produced by the system is intended to be used)」場合に適用される。域外のサプライヤーは、AI Actの遵守を確保するため、EU域内で指定代理人を任命しなければならない。ただし、AI Actは、第三国の公的機関、EUとの警察・司法共助協定に基づく国際機関には適用されない。また、軍事防衛または国家安全保障の目的で市場に投入されるAIシステムにも適用がない。

この広範な適用範囲は、AIシステムとその使用に関する包括的な規制を確保することを目的としている。

本ガイドでは -

- 本章において、AI Act全体の概要、その主要なコンセプト、および同法の適用開始時期について説明する。
- 第2章では、AI Actの地理的適用範囲と実体的適用範囲について見ていく。
- 第3, 4, 5, 6章では、AI ActがAIのタイプごとに課す要件について説明する（禁止されたプラクティス、高リスクシステム、汎用目的AIおよびより高い透明性が求められるAI）。
- 第7章では、規制サンドボックスでAIをテストするためのAI Actの取決めについて説明する。
- 第8章では、ガバナンスと執行について確認する。
- 第9章では、AI Actの採択に続く数々の追加措置をまとめている。
- 最後に、第10章で、本ガイドの全寄稿者を紹介する。

リスク重視のアプローチ

EUのAI規制へのアプローチは、リスクベースの枠組みによっている点が特徴的である。この規制は、技術中立的な視点を採用し、AIシステムをそのリスクに基づき最小リスクから高リスクに分類している。このシステムにより、リスクの高いAIアプリケーション、特に基本的権利に重大な影響を与える可能性のあるアプリケーションは、禁止されるか、より厳しい要件と監視の対象とされている。

EUは、責任あるAIの開発と利用を促進することを重視している。AI Actは、データのセキュリティとユーザーのプライバシーに関する厳格な措置を義務付けており、AIシステムがこれらの点を最優先して設計・導入されることを確保している。これには、データの取扱いおよび保護の方法に関する厳格な要件が含まれ、ユーザーの個人情報の安全性が確保されている。

さらに、AI Actは、AIシステムに対する包括的なリスク評価を義務付けている。これらの評価は、AI技術に関連する潜在的なリスクの特定と軽減に役立ち、AIプロバイダーの透明性とアカウンタビリティを促進する。これらの評価を義務化することで、EUは、AI開発者がその技術の意味を十分に理解し、対処することを確保する。

この積極的なアプローチは、ユーザーの権利と福祉を保護することで、AI技術に対する市民の信頼を築くことを目的としている。データの安全性、プライバシー、リスクマネジメントを優先することで、EUは、安全かつ倫理的にAIの使用ができると、市民を安心させようとしているのである。責任ある開発を重視することで、AI技術のより広範な受容と統合が促進され、最終的には社会全体に利益をもたらす。AI Actは、AIシステムに関するルールを制定するだけでなく、その使用に関する倫理的枠組みを確立し、AIシステムが人々や他の事業者、環境、その他市民の生活の様々な側面に与える影響を、組織が考慮することを確保するために策定された。

AI Actの中心にある倫理

AI Actは、欧州委員会が2019年に発表した「信頼できるAIに関する倫理指針」（Ethical Guidelines on Trustworthy AI）を明確に基礎としている。これらのガイドラインは依然として拘束力を持たないが、その原則の多くはAI Actに直接組み込まれている。このアプローチの最たる例は、同法がその多くの条項において、欧州連合基本権憲章（Charter of Fundamental Rights of the European Union）に謳われている基本的権利に直接言及していることである。例えば、高リスクAIシステムとは、EU市民の健康、安全および基本的権利に重大な悪影響を及ぼすものをいうとされている。

AI Actの適切な適用には、多くの場合、基本的権利に対するリスクの分析が必要であり、これには法的問題と倫理的問題の両方が含まれる。したがって、AI Actには倫理が組み込まれていると言える。

ガバナンス

EUは、分散型の監督モデルを採用し、さまざまな国家当局との連携を推進している。AI Actは、欧州AI事務局（「AI事務局」）を独立した組織として設立した。同事務局は、EU全域におけるAIの専門知識における中央当局としての役割を果たすとともに、法的枠組みの実施において重要な役割を果たす。AI事務局は、信頼できるAIの開発を奨励し、国際協力を支援する。欧州AI委員会は、各加盟国につき1名の代表により構成され、EUデータ保護監督機関はオブザーバーとして参加する。

AI事務局は、国際的なアプローチを考慮しながら、ベストプラクティス規範の作成、見直し、採択を促進することを目的としている。これらの規範が現在の技術状況を反映し、多様な視点を取り入れることを確実にするため、AI事務局は、関連する国家当局と協力し、市民社会組織、利害関係者、科学的専門家を含む専門家と協議することが想定されている。

主要なコンセプト

AIシステム（第2章も参照）

> AI Actは、リスクを*「害悪が発生する確率とその害悪の重大性の組合わせ」*と定義している。

AI Actが*「人工知能（artificial intelligence）」*を定義しておらず、*「人工知能システム（artificial intelligence system）」*のみを定義していることは注目に値する。AIシステムの定義は、OECDのAIシステムの定義と意図的に合わせられている。この定義では、AIシステムに関する特定の技術や現在知られているアプローチには言及していない。AIの急速な進化に伴い、技術開発によってAI Actが時代遅れのものとなるのを防ぐためである。

この定義の重要な要素は、AIシステムの*「推論(infer)」*能力である。これにより、AIシステムと従来のソフトウェアを明確に区別することができる。コンピュータ・プログラムが、プログラマーによってあらかじめ定義されたルールに従って動作するのであれば、それはAIシステムではない。一方、あるシステムが、プログラムに提供されたインプットデータやデータセットに基づいて、プログラム自身がルールを作成できる技術を用いて構築されているのであれば、それはAIシステムである。

サプライチェーン全体の義務（第2章も参照）

AI Actは、システムの*「プロバイダー(provider)」*（*「輸入者(importer)」*も網羅）から始まり、*「販売者(distributor)」*、*「ディプロイヤー(deployer)」*を含むサプライチェーンのすべての参加者に適用される。大半の責任はプロバイダーにあり、次にディプロイヤーにある。

輸入者、販売者またはディプロイヤーは、その名前または商標をシステムに付した場合、高リスクAIシステムのプロバイダーになる可能性がある。また、AIシステムに大幅な変更を加えたり、AIシステムの意図された目的を変更したりすることにより、そのシステムが高リスクとなる場合には、高リスクシステムのプロバイダーとなる可能性がある。

AIシステムの分類に対するリスクアプローチ

> AI Actの大部分は、*「AIシステム」*に適用される。同法は*「AIシステム」*を、*「様々なレベルの自律性で動作するように設計された機械ベースのシステムであり、配備後に適応性を示す可能性があり、明示的もしくは黙示的な目的のために、受け取ったインプットから、物理的または仮想的な環境に影響を与えうるアウトプット（予測、コンテンツ、推奨もしくは決定など）を生成するもの」*と定義している。

AIシステムのリスクに基づく分類は、AI Actの基本的な側面であり、AIシステムが健康、安全、基本的権利に及ぼす潜在的な害悪に焦点を当てている。このアプローチでは、AIシステムを4つの異なるリスクレベルに分類している：

1. **許容できないリスク：**このような重大なリスクをもたらすAIシステムは容認できないため、禁止する。
2. **高リスク：**高リスクAIシステムは、厳しい規制要件の対象となる。
3. **限定的リスク：**このカテゴリーに属するAIシステムのリスクは限定的だが、特定の透明性の義務が課される。
4. **最小限のリスクまたはリスクゼロ：**リスクが最小限またはゼロのAIシステムには、AI Actに基づく規制は適用されない。

許容できないリスク：禁止されるプラクティス（第3章も参照）

AI Actには、禁止されるAIプラクティスのリストが含まれており、これらのプラクティスのいずれかを採用しているAIシステムを市場に投入する、そのサービスを開始する、これを使用することは禁止されていると理解すべきである。以下の事項が禁止されている。

- サブリミナル・テクニックや、故意に操作的または詐欺的な技術を用いて、実質的に行動を歪め、重大な害悪をもたらすこと。

- 個人や集団特有の特性による脆弱性を悪用し、重大な害悪をもたらすこと。
- 社会的採点システム、すなわち、社会的行動や個人的特徴に基づいて個人または集団を評価または分類し、有害または不利な扱いをすること。
- プロファイリングまたは個人的特徴のみに基づいて、犯罪を犯す可能性を評価すること。ただし、犯罪行為に関連する、客観的かつ検証可能な事実に基づく人物の評価を裏付けるために使用される場合を除く。
- インターネットまたはCCTVからのターゲティングされていないデータ収集に基づく顔認識データベース。
- 職場や教育機関において、感情を推論すること。ただし、医療上または安全上の理由がある場合を除く
- センシティブデータに基づいて個人を分類するバイオメトリック分類システム。ただし、法執行の分野で画像などの合法的に取得されたバイオメトリックデータセットをラベリングまたはフィルタリングする場合を除く。
- 法執行目的でなされる、公共の利用可能な空間におけるリアルタイムの遠隔生体認証システム。ただし、狭義に定義された特定の状況を除く。

AI Actには、これらの*「禁止された」*プラクティスを特定の状況で使用することを認める例外規定が含まれている。その好例がリアルタイムの生体認証で、同法では例外的な状況での使用を認めている。これらの例外の適用には、届出または事前承認が必要である。

高リスクAIシステム（第4章も参照）

高リスクAIシステムに関する広範な規制は、AI Actの主要部分を構成している。AIシステムは、EU域内の人々の健康、安全および基本的権利に重大かつ有害な影響を及ぼす場合、高リスクAIシステムとして認定される。高リスクAIシステムには2つのカテゴリーがあり、それぞれに異なる規制が適用される：

- 民間航空、車両保安、海洋機器、無線機器、玩具、リフト、圧力機器、医療機器、個人保護機器など、EU整合法令の対象となる製品または製品のセーフティ・コンポーネントとしての使用が予定されるAIシステム（AI Act付属書Iに列挙されている）。
- 教育、雇用、クレジットスコアリング、法執行、移民、遠隔生体認証システム、重要インフラのセーフティ・コンポーネントとして使用されるAIシステムなど、付属書IIIに列挙されているAIシステム。欧州委員会は、この付属書を修正することができる。

高リスクシステムの第一のカテゴリーには、EU整合法令とAI Actの両方が適用される。プロバイダーには、AI Actで要求される事項を、EU整合法令の下で要求される手続き（付属書Iのセクション Aに列挙されている）に統合する選択肢がある。さらに、付属書IのセクションBに記載されているEU整合法令の対象となる製品（航空機器など）に関するAIシステムについては、AI Actの一部の条項のみが適用される。

欧州委員会は、高リスクAIシステムの分類に関する実務的な支援を、2026年2月2日までに提供する。これには、高リスクAIシステムおよび高リスクでないAIシステムのユースケースの実例の包括的なリストを含む。

高リスクAIシステムの認定例外

付属書IIIに列挙された高リスクAIシステムが、意思決定の結果に重大な影響を与えないなど、自然人の健康、安全、基本的権利に重大な害悪を及ぼすリスクがない場合、高リスクAIシステムとしては扱われない。

このようなケースに該当するのは、AIシステムが以下の4つのいずれかを意図する場合に限られる。

- 狭い手続き上のタスクを実行すること。
- すでに完了した人間の活動の結果を改善すること。
- 意思決定のパターンや以前の意思決定のパターンからの逸脱を検出するものであり、かつ、人間による適切なレビューなしに、すでに完了した人間による評価に取って代わったり影響を与えたりするものではないこと。
- 付属書IIIに列挙されているユースケースの目的に関連するアセスメントの準備作業を行うこと。

ただし、AIシステムが自然人のプロファイリングを行う場合は、常に高リスクAIシステムとみなされ、上記の例外に該当することはない。

この例外は、高リスクAIシステムを市場に投入することに伴う義務やコストを回避できるため、実務上重要な役割を果たすと思われる。例えば、この認定例外を利用できるAIシステムの部分を切り出し、高リスクAIシステムの範囲を限定することも選択肢の一つである。

しかし、プロバイダーがこの例外を利用する場合でも、そのシステムの評価は文書化されなければならず、また、そのシステムを市場に投入したり、サービスを開始したりする前に、高リスクシステムのEUデータベースに登録しなければならない。

高リスクAIシステムに対する広範な義務

高リスクAIシステムのプロバイダーが満たさなければならない要件は厳しい。これらの要件には、特に、AIシステムの開発の各段階を文書化すること、トレーニングのための高品質データの使用に関する義務を満たすこと、ユーザーにシステムの性質と目的に関する完全な情報を提供すること、システムの正確性、堅牢性、サイバーセキュリティを確保することが含まれる。高リスクAIシステムは、EUデータベースに登録され、一般に公開される。

AIシステムのサプライチェーン全体の義務

AI Actは、高リスクシステムのライフサイクルを通じて、そのサプライチェーンに関わるすべての参加者に義務を課している。その責任は、プロバイダーだけでなく、輸入者、販売者およびディプロイヤーにも及ぶが、ほとんどの責任はプロバイダーとディプロイヤーにある。

輸入者および販売者の主な義務は、輸入または頒布される高リスクAIシステムがAI Actの要件を満たしていることを確認することである。さらに、輸入者、販売者またはディプロイヤーは、自己の名称や商標をシステムに付したり、重大な変更を加えたり、AIシステムの意図された目的を変更したりして、そのシステムが高リスクとなった場合、高リスクAIシステムのプロバイダーとなる可能性がある。

汎用目的AIモデル（第5章も参照）

AIモデルとAIシステムの区別は、AI Actの適用において極めて重要である。AIモデルは、AIシステムの不可欠な構成要素であるが、それだけではAIシステムとはならない。AIモデルがAIシステムとなるには、ユーザー・インターフェースなど他の構成要素を追加する必要がある。AI Actは、主に、モデルではなくAIシステムを規制対象としている。ただし、同法は、汎用目的AIモデルに関する規定を含んでいる。

AI Act は、すべての汎用目的AIモデルに関するルールと、システミック・リスクをもたらす汎用目的AIモデルに関する追加的なルールを定めている。これらは以下のような場合に適用される。

- 汎用目的AIモデルのプロバイダーが、自身のモデルを自身のAIシステムに統合し、市場で利用可能にし、またはサービスを開始する場合
- 汎用目的AIモデルのプロバイダーが、AIシステムのプロバイダーに自身のモデルのみを提供する場合。

この区別は、ある第一のプロバイダーの汎用目的AIモデルが、第二のプロバイダーの汎用目的AIシステムで使用され、それが第三のプロバイダーによって構築された、より特定の目的を持つ別のAIシステムに統合されるような場合に、特に重要になることがある。

透明性の義務（第6章も参照）

AI Actは、以下の4種類のAIシステムについて、透明性を確保する義務を課している。

- 自然人と直接対話するように設計されたAIシステム
- 汎用目的AIシステムを含む、合成音声、画像、動画、テキストコンテンツを生成するAIシステム
- 感情認識またはバイオメトリック分類システム
- ディープフェイクである画像、音声、映像を生成または操作するAIシステム

これらすべての場合において、AIシステムにおけるこれらの利用を、ユーザーに対して知らせなければならない。また、より詳細な義務も定められており、例えば、人工的に生成または操作されたものであることが識別できるように、アウトプットに機械可読な形でマークしなければならない。

複雑な監督・執行体制（第8章も参照）

AI Actは、執行を監督するため、複雑な複層的な構造を規定している。これには、加盟国レベルとEUレベルの主体が含まれる。各レベルには、認定機関や、第三者認証機関、適合性評価機関、欧州AI委員会、AI事務局、各国管轄当局、市場監視当局など、いくつかの種類の機関が存在する。

これらの当局は、コンプライアンスの管理をするだけでなく、行動規範の策定、AI規制サンドボックスの組織化、中小事業者やスタートアップへの支援提供などを通じて、市場をサポートする。

技術基準、実務規範、ガイドラインの役割（第7, 8, 9章も参照）

AI Act は、高リスクAIシステムのプロバイダーに欧州適合性（CE）マークの貼付を義務付けている。CEマークは、同法の要求事項に適合していることを示すものである。CEマークが発行されるためには、プロバイダーは整合化された技術基準を適用しなければならない。加えて、整合規格に適合する高リスクAIシステムまたは汎用目的AIモデルは、それらの規格が要件または義務をカバーしている限りにおいて、同法の要件に適合しているものと推定される。その結果、AI Actの比較的一般的な規定は、AI Act遵守の具体的な形を示す技術基準によって補完されることになる。したがって、CEマークと技術規格は、AI Actの実際の適用において非常に重要な役割を果たすことが期待される。

実践規範もまた、重要な役割を果たすだろう。実践規範が市場参加者により作成されない場合は、欧州委員会が実装法令の中で共通規則を定めることができる。また、欧州委員会は、実装法令を制定することで、実践規範を承認し、EU域内で一般的な効力を持たせることもできる。さらに、欧州委員会は、AI Actの実務的な運用に関するいくつかのガイドラインを作成する義務を負っている。

したがって、AI Actは、さらに多くの文書や法的行為から生じるより詳細な義務のための1つの枠組みに過ぎないとみることができる。

施行（第8章も参照）

AI Actは、違反に対する重い罰則を定めており、課される罰則は、違反の内容や関係するエンティティの規模によって異なる。高額な罰則が課される可能性のある行為には、以下のものが含まれる。

- 第5条に概説されている、禁止されているAIプラクティスに関するルールの不遵守。この場合、違反者には、最高3,500万ユーロまたは全世界における年間売上高の最高7%のいずれか高い方の制裁金が科される可能性がある。
- データ、データガバナンス、透明性に関するAIシステムの違反。最高2,000万ユーロまたは全世界における年間売上高の最高4%の制裁金が科される可能性がある。
- 第99条に定める規定（例：高リスクAIシステムに関するもの）の不遵守。最高1,500万ユーロまたは、違反者が事業者の場合、前会計年度の全世界における売上高の最高3%のいずれか高い方の制裁金が科される可能性がある。

これらの罰則は、AI Actの規制を遵守することの重要性を強調している。事業者は、これらの規制を十分に把握し、AIシステムが同法の要件を満たすようにすることが不可欠である。

タイムライン

AI Actは、段階的に適用される。また、特定の日以前に市場に投入されまたはサービスが開始されたAIシステムについては、経過措置が設けられている。同法は、2026年8月2日より前に市場に投入された、またはサービスが開始された高リスクAIシステムのすべてのオペレーターに適用されるが、これらのシステムが設計の大幅な変更の対象となる場合はこの限りではない（この場合、規定は全面的に適用される）。関連する適用開始日は以下のとおりである。

2024年7月12日	AI ActがEU官報に掲載され、特定の条項の適用開始日のトリガーとなる
2025年2月2日	禁止されるAIプラクティスの適用開始（第2章） AIリテラシー・ルールの適用開始（第4条）
2025年5月2日	汎用目的AIの実践規範の準備期限（第56条第9項）
2025年8月2日	国家当局の指定（第4節第3章） 汎用目的AI（GPAI）に関する義務（第5章） ガバナンス（EUおよび加盟国レベル）（第7章） 守秘義務と罰則（汎用目的AIに関するものを除く）（第7章）
2026年8月2日	AI Actのその他すべての規定の適用開始（後日適用開始される以下の場合を除く）
2027年8月2日	付属書Iに掲げられている高リスクカテゴリー 2025年8月2日より前に市場に投入された汎用目的AIモデル（第111条）
2030年8月2日	2026年8月2日より前に市場に投入され、またはサービスが開始した、公的機関での使用を目的とした高リスクAIシステム（以下に挙げるものを除く）（第111条）
2030年12月31日	2027年8月2日より前に市場に投入され、またはサービスが開始した、付属書Xに列挙された大規模ITシステムのコンポーネント（第111条）

実体的適用範囲および地理的適用範囲

ポイント

- AI Actは、AIシステム、汎用目的AIモデル、禁止されているAIプラクティスをカバーする。
- 義務は、プロバイダー、輸入者、販売者、製品製造者、指定代理人、ディプロイヤーの6種類の経済主体に課され得る。
- 高リスクAIシステムに関わるオペレーターは、重い義務を負う。また、特定のカテゴリーのAIシステムのプロバイダーやディプロイヤーも、透明性の義務の対象となる。
- 汎用目的AIモデルのプロバイダーも義務の対象となる。
- AI Actは、AIシステムまたは汎用目的AIモデルがEU市場に投入され、EU域内でサービスが開始され、EU域内に輸入され、またはEU域内で流通する場合に適用される。また、AIシステムが、EU域内に事業所を置く、またはEU域内にいるディプロイヤーにより使用される場合にも適用される。
- AI Actの適用範囲に含まれるAIシステムのプロバイダーやディプロイヤーは、2025年2月2日からAIリテラシー要件の対象となる。

To doリスト

- [ ] 自社、自社と取引のある供給業者やクライアントが、AI Actの適用範囲に含まれるオペレーターに該当するかどうかを判断する。
- [ ] 自社または自社のサプライチェーンがAI Actの適用範囲に含まれる場合、AIシステムまたはAIモデルが1つ以上の規制対象カテゴリーに該当するかどうかを確認する。
- [ ] 自社がAI Actの適用範囲内にあるAIシステムのプロバイダーやディプロイヤーである場合、同法のAIリテラシー要件を遵守するための措置を講じていることを確認する。

実体的適用範囲

AI Actは主に、AIシステムの市場投入、サービス開始、および使用に関する調和のとれた規則を定めている。この法律は、「高リスク」AIシステムに広範な義務を課し、AIシステムに透明性の義務を設けている。また、AI Actは、特定のAIプラクティスを禁止し、EUにおける汎用目的AIモデルの供給を規制している。

AI Act はまた、市場監視・監督、ガバナンス、制裁金を含む執行に関するルールや、AIサンドボックスの運用など、特に中小事業者に焦点を当てたイノベーション支援策も定めている。さらに、次のとおり、新たに2つの機関が設立された：(i) 欧州AI委員会 - AI Actの一貫した効果的な適用を促進するため、欧州委員会およびEU加盟国への助言と支援を任務とする。(ii) AI事務局 - 欧州委員会内に設置され、AI Actの運用、信頼できるAIの開発と利用の促進、国際協力の促進を任務とする。

規制対象者：オペレーター

AI Actは、プロバイダー、ディプロイヤー、輸入者、販売者、製品製造者、指定代理人の6つのカテゴリーの者に義務を課している。*「オペレーター（operator）」*とは、これらすべての者を表すために用いられる。AIシステムや汎用目的AIモデルのプロバイダーは常に存在する。また他のオペレーターも存在するかどうかは、AIシステムや汎用目的AIモデルがどのように供給され、展開されるかによる。ほとんどのオペレーターは、AI Actの付属書Iで参照されているEUの製品に関する法令から転用された3つの重要な用語、*「利用可能にすること（making available）」*、*「市場に投入すること（placing on the market）」*、*「サービス（使用）を開始すること（putting into service）」*を参照して定義される。

> ***「利用可能にすること」***とは、商業活動の過程において、有償であるか無償であるかを問わず、EU市場での頒布または使用のために、AIシステムまたは汎用目的AIモデルを提供することをいう。
> ***「市場に投入すること」***とは、AIシステムまたは汎用目的AIモデルをEU市場で初めて利用可能にすることをいう。
> ***「サービス（使用）を開始すること」***とは、意図された目的のために、EU域内において、ディプロイヤーに直接、または自ら使用するために、AIシステムを提供することをいう。

*「使用（use）」*という用語はAI Actでは定義されていない。本質としては、*「使用」*という用語は、受け取ったインプットからどのようにアウトプットを生成するかを推論する、というAIシステムの主要な特徴を参照して認識されるだろう。

AI Actで規制されているオペレーターは以下の表のとおりである。

オペレーター		役割
AIシステムと汎用AIモデルの両方に関連	**プロバイダー（第3条第3号）**	有償・無償を問わず、AIシステムもしくは汎用AIモデルを開発する、またはAIシステムもしくは汎用AIモデルを開発させ、自己の名称もしくは商標の下に市場に投入しもしくはAIシステムのサービスを開始する。 *「市場に投入する」*の定義は、EU市場に言及しているが、AIシステムをEU市場に投入していなくても、AIシステムのアウトプットがEU域内で使用される場合には、AI Actで規制されるプロバイダーとみなされる可能性がある。下記*「地理的適用範囲」*を参照。 プロバイダーは、自然人または法人、公的機関、代理人、その他の団体である。EUの機関、団体、事務所、エージェンシーもAIシステムのプロバイダーとして活動することができる。 また、AIシステムが他のプロバイダーによってすでに市場に投入されている場合、またはEU域内でサービスを開始している場合、第25条第1項(a)～(c)に規定されるいずれかの措置を講じることにより、プロバイダーになり得る。下記*「高リスクAIシステム」*を参照。
	指定代理人（第3条第5号）	EU域外に設立されたプロバイダーによりそのプロバイダーの代理人として指名された、EU域内の自然人または法人。その役割には、AI Actが要求する書類を管轄当局が入手できるようにすること、および管轄当局と協力することが含まれる。第22条（高リスクAIシステム）および第54条（汎用目的AIモデル）を参照。
AIシステムのみに関連	**ディプロイヤー（第3条第4号）**	その権限の下でAIシステムを使用する者（私的または非専門的な活動の過程における使用を除く）。ディプロイヤーは、自然人または法人、公的機関、エージェンシー、その他の団体のいずれでもあり得る。EUの機関、団体、事務所、エージェンシーもAIシステムのディプロイヤーに該当し得る。
	輸入者（第3条第6号）	EU域内に設立されていない者の名称または商標が付されたAIシステムをEU市場に投入するEU域内に所在し、または設立された自然人または法人。
	販売者（第3条第7号）	プロバイダーまたは輸入者以外のサプライチェーンの自然人または法人で、AIシステムをEU市場で利用可能にする者。
	製品製造者（第25条第3項）	以下、特定の状況下では、製品製造者は、高リスクAIシステムの*「プロバイダー」*とみなされる： 製造しているのがAI Actの対象となる製品のセーフティ・コンポーネントであること（付属書Iのセクション A で言及されているEUの製品安全に関する法令の対象となること）、かつ、 製造者が、そのAIシステムをEU市場に投入するか、その製品とともに、自己の名称または商標の下でEU

域内でサービスを開始すること

*「製品製造者」*という用語は、AI Actでは定義されていないが、前文第87項は、これが付属書Iで参照されているEUの製品安全に関する法令に基づいて定義された*「製造者」*であることを明確にしている。

AI Actに基づく間接的義務

AI Actは、高リスクAIシステムのサプライヤーにコンポーネントを提供する供給業者に間接的な義務を課している。高リスクAIシステムで使用または統合されるツール、サービス、コンポーネントまたはプロセスを提供する者は、高リスクAIシステムのプロバイダーと書面による契約を締結し、プロバイダーがAI Actに基づく義務を遵守できるようにする必要がある（第25条第4項）。この義務は、そのようなツール、サービス、プロセス、またはコンポーネント（汎用目的AIモデルを除く）を、無償かつオープンソースのライセンスの下で一般に公開する第三者には適用されない。

AI Actにより認められた権利

個人に包括的な権利を提供するGDPRとは異なり、AI Actに基づく権利は限定的である。AI Actは、EU域内に所在し影響を受ける者に対してのみ、個別の意思決定について説明を受ける権利を付与している（第86条）。影響を受ける者とは、付属書IIIで特定された高リスクAIシステムのいずれかのアウトプットに基づく決定により、法的またはそれと同等の重大な影響を受ける者である。ここで使用されている文言は、GDPRの自動化された意思決定の規定（GDPR第22条）で使用されているものと類似しているが、2つの規定の範囲は同一ではない。

規制対象：AIシステム

AIシステムは、第3条第1号において次のように広く定義されている：*「様々なレベルの自律性で動作するように設計された機械ベースのシステムであり、配備後に適応性を示す可能性があり、明示的もしくは黙示的な目的のために、受け取ったインプットから、物理的または仮想的な環境に影響を与えうるアウトプット（予測、コンテンツ、推奨もしくは決定など）を生成するもの」*

この定義は、OECDのAI原則で使用されている定義と一致させることを意図している。AIシステムの主な特徴は、推論する能力、すなわち、インプットやデータからアウトプットを得たり、モデルやアルゴリズム、あるいはその両方を導き出したりする能力である。対して、従来のソフトウェアは、自然人によって定義されたルールのみに基づいてオペレーションを実行するものであり、従来のソフトウェアそのものだけではAIシステムとはみなされない。AIシステムが物理的に製品に統合されているか、統合されずに製品の機能を果たしているかにかかわらず、AIシステムは、単独で使用することも、製品のコンポーネントとして使用することもできる。

AI Actでは、AIシステムは以下のカテゴリーに分類される。

- 高リスクAIシステム
- 透明性リスクを伴うAIシステム
- 他のすべてのAIシステム

AIシステムは、禁止されているAIプラクティスの一部を構成することもある。これは、そのAIシステムの特定の機能やその使用方法によるものである。

高リスクAIシステム

AI Act第3章は、高リスクAIシステムを規制している。これらは、EU域内の人々の健康、安全、基本的権利に重大な害悪を及ぼす危険性のあるAIシステムである。AIシステムは以下の2つの方法で高リスクに分類される。

- 第6条第1項：AIシステムが、特定のEUの製品安全に関する法令（AI Act付属書Iに記載されたEU整合法令）により規制され、当該規制に基づいて第三者適合性評価機関による適合性評価手続の対象となる製

品のセーフティ・コンポーネントとして使用されるか、またはそれ自体がそのような製品を構成すること（例えば、医療診断目的に使用されるAIシステムは、それ自体が規制される医療機器となる）。

- 第6条第2項：AIシステムが、付属書IIIに規定された8つのカテゴリーのいずれかに該当すること。ただし、プロバイダーが、当該AIシステムが重大な害悪のリスクをもたらさないことを証明し、文書化できる場合を除く。

高リスクAIシステムに関する義務の大半は、プロバイダー（上記で説明したとおり、製品製造者も含まれる）に課される。一方、より限定的な義務は、ディプロイヤー、輸入者、販売者に課され、関連する場合には指定代理人に課せられている。

詳細は本ガイド第4章を参照。

透明性リスクのあるAIシステム

AI Actは、以下の者に対し、一定の透明性の義務を課している：

- 自然人と直接対話することを意図したAIシステムのプロバイダー（第50条第1項）
- 合成音声、画像、動画、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（第50条第2項）
- 感情認識システムまたはバイオメトリクス分類システムのディプロイヤー（第50条第3項）
- ディープフェイクを構成する画像、音声または映像コンテンツを生成または操作するAIシステムのディプロイヤー（第50条第4項）

詳細は本ガイド第6章を参照。

他のすべてのAIシステム

上記のカテゴリーに該当せず、禁止されているAIプラクティスに使用されないその他のすべての種類のAIシステムは、AI Actに基づく直接的な法的義務の対象とはならない。将来的には、このような広範なカテゴリーのAIシステムとその導入をした者を対象とした自主的な行動規範が作成される可能性がある（第95条）。プロバイダーおよびディプロイヤーは、これらの行動規範に従うかどうか選択することができる。

特定のカテゴリのAIシステムに関するルールは別として、AI Actに基づきAIシステムのプロバイダーまたはディプロイヤーとなる者は、その従業員およびAIシステムの運用・利用に関わるその他の者が、AIシステムの導入、その機会およびリスクに関して十分なレベルの知識、スキルおよび理解を有することを保証するためのAIリテラシー対策を講じることが義務付けられている（第4条）。この義務は、EUにおける信頼できるAIの開発、運用および利用を促進することを目的としている。しかし、この規定が自主的な行動規範に言及しており、AIリテラシー義務を遵守しなかった場合の制裁金が想定されていない点は注目に値する。

規制対象：禁止されるAIプラクティス

AI Actは、特定の禁止された機能を有する、または特定の禁止された目的に使用されることを意図するAIシステムの市場への投入、サービスの開始および使用を禁止している。例えば、インターネットやCCTVの映像から顔画像を無制限に収集して顔認識データベースを作成または拡張するAIシステムが該当する。これらの行為は、特に有害で濫用的であり、EUの価値観や基本的権利に反するとみなされる。禁止されるAIプラクティスは、AI Act第5条に列挙されているが、他のEU法（データ保護、非差別、消費者保護、競争法など）に違反するAIプラクティスの禁止には影響しない。

詳細は本ガイド第3章を参照。

規制対象：汎用目的AIモデル

> 汎用目的AIモデルは、第3条第63号で次のように定義されている：*「大規模な自己教師あり学習を用いて大量のデータで訓練される場合を含め、重要な汎用性を示し、（モデルが市場に投入される方法に関係なく、）広範で明確なタスクを適切に実行することができ、様々な川下のシステムまたはアプリケーションに統合することができるAIモデル。ただし、市場に投入される前の研究、開発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。」*

AI Actは*「AIモデル(AI model)」*の定義を定めていない。前文第97項は、AIモデルはAIシステムの不可欠な構成要素であるが、それ自体ではAIシステムを構成せず、AIシステムになるためには、ユーザー・インターフェースなどのさらなるコンポーネントが必要になると指摘している。汎用目的AIモデルの特徴については、前文第98項および第99項で詳しく説明されている。

AI Actは汎用目的AIモデルを規制し、システミック・リスクを伴う汎用目的AIモデルには追加義務を課している。このルールは、汎用目的AIモデルが市場に投入されると（ライブラリ、API、直接的なダウンロード、物理的なコピーなど、さまざまな方法で投入される）、そのモデルのプロバイダーに適用される。

汎用目的AIモデルに関するルールは、これらのモデルがAIシステムに統合される場合や、AIシステムの一部を構成する場合にも適用される。汎用目的AIモデルのプロバイダーが、自らのモデルを自らのAIシステムに統合し、市場で入手可能にしたり、サービスを開始したりする場合、そのモデルは市場に投入されたとみなされ、AIシステムに関する規定に加えて、汎用目的AIモデルに関する規定が適用される。第三者の汎用目的AIモデルを自身のAIシステムに統合する者は*「川下プロバイダー（downstream providers）」*とみなされ、AI Actの下で一定の権利が認められる。しかし、AI Actは、第三者の汎用目的AIモデルを微調整し、その微調整されたモデルを自身のAIシステムに統合する（あるいは、微調整された汎用目的AIモデルを市場に投入したり、サービスを開始する）プロバイダーは、その微調整に関してのみ、そのプロバイダーとみなされることを想定しているようである（前文第109項参照）。

詳細は本ガイド第5章を参照。

参照条文等

実体的適用範囲 第1条　前文第1-3, 6-8項

地理的適用範囲

AIシステムに関する規定

AI Actは、そのAIシステムの規定に関して、幅広い管轄を持つことを意図している。これらの規定は、AIシステムが、それ自体で、または付属書IのEUの製品安全に関する法令の対象となる製品の一部として、以下のいずれかに該当する場合に適用される。

- EU市場に投入され、EU域内でサービスが開始され、EU域内に輸入され、またはEU域内で頒布される場合
- EU域内に事業所を置く、またはEU域内に所在するディプロイヤーによって使用される場合

最初のポイントは、AIシステムのプロバイダーがどこで設立されているかに関係なく適用される点である。AI Actでは「*設立(establishment)*」の概念は定義されていない。GDPRなど他のEU法におけるこの用語の使用と同様に、広義に解釈されることが予想される。

これらのケースに加え、AIシステムの規定は、EU域外のAIシステムにより生成されたアウトプットがEU域内で使用される場合にも、適用される。

その場合、EU域外に設立され、または所在するプロバイダーおよびディプロイヤーもAI Actの適用範囲に含まれることになる。前文第22項は、このような場合、関連するAIシステムがEU域内の市場に投入されておらず、サービスを開始しておらず、または使用されていなくても、AI Actが適用されることを明確にしている。

禁止されるAIプラクティス

禁止されるAIプラクティスに関するAI Actの規定は、第5条に規定された関連するAIプラクティスのEU市場への投入、EU域内におけるサービス開始および使用に対して適用される。上述したように、*「市場に投入すること」*と*「サービスを開始すること」*の定義は、EU市場を参照している。AI Actは、禁止される*「使用」*が何を意味するのか、また、例えば、EU内でのAIシステムのアウトプットの単なる使用が対象となるのかどうかについては明示していない。

汎用目的AIモデル

AI Actにおける汎用目的AIモデルの規定は、汎用目的AIモデルのプロバイダーがEU域内でそれを市場に投入するか、EU域内でサービスを開始する場合に適用され、当該プロバイダーの所在地や設立地は問わない。

参照条文等

地理的適用範囲 第2条　前文第9, 11項

適用除外

一定の活動は、AI Actの適用範囲外である。AI Actは以下のものには適用されない：

- EU法の適用範囲外の分野（国家安全保障に関する活動など）。これは、国内法に基づいて免除される活動の実施を委託された事業体の種類に関係なく適用除外となるものである。欧州連合の機能に関する条約（TFEU, Treaty on the Functioning of the European Union）に規定されているように、EUの権限が非常に広範であることを考えると、この適用除外が実際に適用される範囲は非常に限定的なものになるだろう。

- 専ら軍事、防衛または国家安全保障の目的で、市場に投入され、サービスが開始され、もしくは使用されるAIシステム、またはそのアウトプットが上記目的のみでEU域内で使用されるAIシステム。AIシステムへの変更有無にかかわらず、また、そのような活動を行うエンティティの種類にもかかわらない。除外された目的（軍事、防衛または国家安全保障）と1つ以上の除外されない目的（民間目的や法執行など）の両方のために市場に投入され、またはサービスが開始されたAIシステムは、AI Actの対象となり、これらのシステムのプロバイダーは同法の遵守を確保する必要がある。

- EUまたはEU加盟国との法執行および司法協力のための国際協力または国際協定の枠組みにおいてAIシステムを使用する第三国の公的機関または国際機関。ただし、そのような第三国または国際機関が個人の基本的権利および自由を守るために十分な保護措置を提供することを条件とする。これらのアウトプットを利用する国家当局およびEUの機関、団体、事務所およびエージェンシーは、引き続きEU法に従う必要がある。

- 専ら科学研究・開発を目的として特別に開発されサービスが開始されたAIシステムおよびモデル（そのアウトプットを含む）。

- 市場に投入されまたはサービスが開始される前に行われる、AIシステムまたはモデルの研究、試験または開発（実環境でのテストを除く）。

- 純粋に私的かつ非専門的な活動の過程でAIシステムを使用する個人のディプロイヤー。これはGDPRの*「家庭内活動の適用除外(household exemption)」*に類似するが、AIシステムのプロバイダーは引き続きAI Actの対象となる。

- 無償およびオープンソースライセンスの下で公開されたAIシステム。ただし、高リスクAIシステムとして、禁止されたAIシステムとしてまたは同法の透明性の義務の対象となるシステムとして、市場に投入されたり、サービスが開始されたりする場合を除く。

他の規制枠組みとの関係

- RegulationであるAI Actは、国内法化を必要とせず、EU加盟国に直接適用される。EU加盟国は、AI Actによって明示的に認められない限り、AIシステムの開発、マーケティングおよび使用に制限を課すことができない。これが認められるのは限られた状況においてのみであり、例えば、EU加盟国は、禁止されたAIプラクティスを構成する遠隔生体認証システムの使用（第5条第5項）や、高リスクAIシステムを構成する事後遠隔生体認証システムの使用（第26条第10項）について、より制限的な法律を導入することができる。

- 高リスクAIシステムに関するAI Actの規定は、EU製品に関する新たな法的枠組みを中心に構築されている。これは、EU市場への製品の投入に関する規則を定めた立法パッケージであり、市場監視規則、適合性評価およびCEマークに関する規則を強化するものである。また、工業製品に関する共通の法的枠組みを、将来の法規制で使用するための措置のツールボックスという形で確立している。AI Actは、新法体系に規定されたこれらの手段が、AIシステムの文脈においてどのように適用されるべきかを規定している。

- これと並行して、AI ActはEU整合法令を補完するものでもある。これは一連のEUの製品安全に関する法令であり、これに基づいて特定のAIシステムが高リスクに分類される。

- AI Act上の義務は、GDPR、e-Privacy指令および法執行指令に基づく義務に追加して適用され、これらを損なうものではない。

禁止されるAIプラクティス

ポイント

- 第5条には、許容できないレベルのリスクをもたらすとみなされる8つの禁止事項がリストアップされている。
- これらの禁止は2025年2月2日に発効する。
- 禁止されるプラクティスは、以下の事項である。
  - サブリミナル的、操作的、または詐欺的な技術
  - 行動を著しく歪め、重大な害悪を及ぼす危険性のある、それぞれのケースにおけるグループの脆弱性を悪用する技術
  - 特定の使用事例における、ソーシャル・スコアリング
  - プロファイリングに基づく犯罪予測
  - 顔認識データベースのためのウェブやCCTVのスクレイピング
  - 職場や学校における感情の推論
  - 人種、政治的意見、労働組合員、宗教的・政治的信条、性生活、性的指向を推測するためのバイオメトリクス分類
  - 法執行を目的とした公共空間におけるリアルタイムの遠隔生体認証
- 禁止事項の多くには例外があり、ケースバイケースの分析が必要となる。
- 上記禁止のカテゴリーは最終的なものではなく、毎年再評価される。
- 違反した場合、最高3,500万ユーロまたは前会計年度の全世界の年間売上高の7%（いずれか高い方）の制裁金が科される。
- ここでの禁止は、オペレーターの別を問わず、その者の役割（プロバイダー、ディプロイヤー、販売者または輸入者など）に関係なく適用される。

To doリスト

- [ ] 使用しているAIシステムが禁止カテゴリーに該当していないか確認する。
- [ ] 禁止されるプラクティスのカテゴリーは随時更新される可能性があるため、アップデートを毎年確認する。
- [ ] 禁止に対する例外が適用されるかどうかを検討する。禁止される行為は絶対的なものではなく、例外があるものも多い。

禁止されるAIプラクティス

AI Actは、リスクベースアプローチを採用しているため、リスクのレベルに応じて異なる要件が適用される。本章では、禁止されている行為、すなわちEUの価値観に抵触し、自由、平等、プライバシーといった基本的権利に対する明白な脅威となる行為に焦点を当てる。禁止事項は、法律制定者が、透明性および倫理的懸念に対応し、人権の保護を保証しようとするものである。

禁止されるプラクティスは第5条に網羅的に列挙されており（さらに前文第28項から第45項で説明されている）、AIがEU域内で何ができ、何ができないかについて明確な枠組みを提供している。第5条の禁止事項は2025年2月2日から適用されるため、施行される最初の規定であり、その重要性が強調されている。

第5条の禁止プラクティスのリストは、網羅的なものであるが、最終的なものではない。欧州委員会は、年に1度、禁止プラクティスのリストの修正の必要性を評価し（第112条）、その結果を欧州議会および欧州理事会に提出することができる。そのため、禁止されるプラクティスのリストにはいずれ変更が加えられる可能性がある。

現在、禁止されているプラクティスは8つあり、人々の行動を実質的に歪めたり、民主主義社会で懸念を生じさせるプラクティスに焦点が当てられている。特に生体認証システムには注意が払われている。しかし、禁止事項の多くには詳細な例外があり、それぞれの行為はケースバイケースで検討されるべきである。

第5条第1項(a) サブリミナル的、操作的または詐欺的なテクニック

最初の禁止事項は、以下に該当する、サブリミナル的、操作的または詐欺的なテクニックを用いたAIシステムに関するものである。

- その技術が、個人または集団の行動を実質的に歪めることを目的とし、または実際にその効果を持つものであって、
- 十分な情報に基づいた意思決定を行う個人の能力を著しく損ない、かつ、
- 他の方法では行わなかったであろう意思決定を行わせ、重大な損害を引き起こすか、または引き起こす可能性が高いと合理的に考えられる場合。

前文第29項で明示されているテクニックには、人が知覚できない音声、画像、映像刺激などのサブリミナル的な構成要素の配置、または人の自律性、意思決定、自由な選択を破壊あるいは損なうその他の操作的または詐欺的なテクニックが含まれ、その方法は、そのようなテクニックに人が気づかないか、気づいていても欺かれたり、制御または抵抗できないような方法である。前文第29項にある、著しく有害な方法で人間の行動を実質的に歪める能力を持つマシーンブレインインターフェースへの言及は、コロラド州、カリフォルニア州、チリなど他の司法管轄区で現在議論されている、神経データを使用するツールに対する規制へのAI Actの試みかもしれない。

AIシステムが禁止されるためには、詐欺的なテクニックと引き起こされた重大な害悪との間に因果関係が必要となる。*「重大な(significant)」*害悪という閾値は立法過程で追加されたものであり、すべてのダークパターンがこの規定に該当するわけではないことを明確にしている。

この規定は解釈の余地があり、特に*「詐欺的(deceptive)」*という言葉についてはさらなる議論が必要だろう。

第5条第1項(b) 脆弱性の悪用

禁止されるAIプラクティスの第2のカテゴリーは、社会的弱者の保護を目的としている。年齢、障がいまたは特定の社会的・経済的状況による脆弱性の3つの類型である。

AIシステムが禁止されるのは、個人の行動を実質的に歪める目的または効果を持ち、誰かに重大な害悪をもたらしまたはもたらす可能性のある方法でそれを行う場合のみである。

AIシステムが、貧困にあえぐ人々を見つけ出し、その弱点を経済的に利用するために使用される場合、特定の社会的・経済的状況の悪用となる可能性がある。マーケティングや販売にAIシステムを使用する組織は、この要件に照らしてシステムをテストすることを確認すべきである。

重大な害悪という概念は、サブリミナル的な技術と社会的弱者の搾取の両方に共通する。立法過程において、その害悪が身体的または心理的なものでなければならないという要件は削除された。害悪の概念については幅広いアプローチが意図されているようだが、前文第29項では依然として、金銭的利益と並んで、身体的・心理的健康に対する重要な悪影響が例示されている。また、同前文では、害悪は時間の経過とともに蓄積される可能性があるとしている。

この禁止は、合法的な医療行為（同意の上で行われる精神疾患の心理的治療など）に影響を及ぼすことを意図したものではない。前文第29項はまた、広告やその他のいくつかの商行為が本質的にナッジに依存していることを黙示に認めており、特に広告の分野において、一般的で合法的な商行為を禁止する意図はないと述べている。

第5条第1項(c) ソーシャル・スコアリング

第3の禁止事項は、いわゆるソーシャルスコアリング、すなわち、社会的行動や、既知の個人的特徴、推論される個人的特徴、または予測される個人的特徴に基づいて、個人または集団を一定期間分類することに関するものである。ソーシャル・スコアリングが禁止されるのは、次の2つのケースである：

- データの利用が、データが当初生成された文脈とは無関係な社会的文脈における不利な取扱いにつながる場合
- 個人または集団がとった社会的行動やその重大性に対して、不当または不釣合いな不利な取扱いを個人または集団が受けることになる場合

ソーシャル・スコアリングは、世界のいくつかの政府で使われている。オランダ政府は、リスクスコアリングのアルゴリズムの欠陥により、個人の特徴や行動に基づいた謂れのない福祉手当の不正受給を摘発したことで、2021年に退陣した。このケースでのアルゴリズムは、マイノリティや経済状況に基づいて人々を対象としていた。ソーシャル・スコアリングについて考えるとき、政府が真っ先に思い浮かぶ例かもしれないが、この規定はより広く、すべてのソーシャル・スコアリング・システムを包含している。多くのアルゴリズムは本質的に行動スコアに依存している。しかし、AI Actが禁止しているのは、不利な扱いをもたらすスコアリングシステムだけである。この重要な制限は、ソーシャルスコアリングの結果を対象とし、不当な結果や個人または集団の差別を防止するものである。

第5条第1項(d) 犯罪リスク評価のためのプロファイリング

第4の禁止事項は、プロファイリングや人物の性格的特徴、特性の評価のみに基づいて、人物が犯罪を犯す可能性を評価または予測するAIシステムを市場に投入したり、サービスを開始したり、使用したりすることである。ただし、犯罪行為に直接関連する客観的かつ検証可能な事実に基づく、犯罪行為に関与する人物についての人間評価を支援するために使用されるAIシステム（すなわち、事実に基づいて人間の意思決定を補完するもので、人間の意思決定に取って代わるものではない、検知ツール）については例外である。この禁止は、映画『マイノリティ・リポート』で描かれているように、人々が（まだ）犯してもいない犯罪に対して有罪として扱われるというシナリオを避けることを目的としている。これは、欧州連合基本権憲章（Charter of Fundamental Rights）第1条に定められた人間の尊厳と結びついている。

第5条第1項(e) 顔認識データベース

第5の禁止事項は、インターネットやCCTV映像から顔画像を無制限にスクレイピングし、顔認識データベースを作成または拡張するために、AIシステムを市場に投入したり、特定の目的の

ためにサービスを開始したり、使用したりすることである。前文第43項は、このような行為が集団監視の感覚を助長し、プライバシーの権利を含む基本的権利の重大な侵害につながりうると考えている。これは、クリアビューAIに対する管轄当局の調査に対応したものであるかもしれない。

第5条第1項(f) 職業と教育における感情の推測

第6の禁止行為は、職場や学校において、感情を推測するためにAIシステムを市場に投入したり、特定の目的のためにサービスを開始したり、使用したりすることである。ただし、治療用システムなど、安全上または医療上の理由がある場合を除く。

前文第18項では、喜び、悲しみ、怒りなどの感情または意図を区別している。前文第18項は、この概念には、痛みや疲労などの身体的状態は含まれないと説明している（したがって、事故防止のためにプロのパイロットや運転手の疲労状態を検知するシステムは影響を受けない）。また、しかめっ面や笑顔のようなすぐにわかる表情や、手、腕、頭の動きのようなジェスチャー、声の大きさや囁き声のような人の声の特徴の検出も含まれない。

> AI Actには*「感情認識システム」*という用語が定義されており、これは*「生体認証情報に基づいて自然人の感情または意図を識別または推論することを目的とするAIシステム」*を意味する。

不思議なことに、第5条第1項(f)にはこの用語は使われておらず、感情を推測するためのAIシステムのあらゆる使用に言及している（すなわち、これがバイオメトリクスデータに由来するものでなければならないという要件はない）。しかし、前文第44項は、第5条は定義された感情認識システムに適用されることを意図しているようである。これが正しければ、非バイオメトリクス感情認識システム（例えばテキストベース）は禁止されていないことになる。同法は、バイオメトリック感情認識システムの不正確さと、力の不均衡が存在する環境（職場や学校など）におけるその侵入的な性質を、そのような環境における禁止の理由として言及している。しかし、同法は、非バイオメトリクス感情認識システムを、バイオメトリクスシステムよりも侵入性が低い、あるいは精度が高いとみなす理由を説明していない。

第5条第1項(g) バイオメトリック分類

第7の禁止事項は、GDPRに基づく特定の（すべてではない）特別なカテゴリーデータ、すなわち人種、政治的意見、労働組合員、宗教的または政治的信条、性生活または性的指向を推測または推論するために、個人の生体データに基づいて個人を分類するバイオメトリック分類システムを使用することである。

GDPRの特別なカテゴリーデータのうち、禁止事項の対象となっていないのは、民族的出自、健康状態、遺伝データの推論である。しかし、そのような種類のデータを推論することは、付属書IIIの高リスクカテゴリーに該当する可能性が高い。さらに、この禁止は、合法的に取得された生体データセットのラベリングもしくはフィルタリング、または法執行機関による生体データの分類（例えば、法執行機関による容疑者捜索のための髪の色や目の色による画像の分類）を対象としていない。しかし、前文第54項は、GDPRに基づく機微属性または特別のカテゴリーデータに従った生体認証分類に使用されることを意図したAIシステムは、AI Actで禁止されていない限り、高リスクに分類されるべきであると示唆しているため、バイオメトリクス分類を使用するこのようなラベリングおよびフィルタリングシステムが高リスクカテゴリーに該当するかどうかは不明である。

前文第16項は、客観的な技術的理由により主要サービスなしにはその機能を使用することができず、かつ、AI Actの適用を回避するためのメカニズムではない場合（例えば、小売のtry before you buyフィルターやソーシャルメディアのフィルター）、バイオメトリクス分類システムには、別の商業サービスとリンクしている純粋に付随的な機能は含まれないことを明確にしている。

第5条第1項(h) 公共空間におけるリアルタイム遠隔生体認証

最後の第8の禁止事項は、法執行を目的とした、公共のアクセス可能な空間におけるリアルタイムの遠隔生体認証システム（「RBI」）の使用である。RBIシステムとは、本人の関与なしに、通常は遠隔で、生体データを参照データベースに含まれるものと比較することにより、自

然人を識別することを目的とするAIシステムである。リアルタイムシステムには、比較短時間の遅延があるものが含まれる。検証に使用される（すなわち、サービスや機器にアクセスするため、または施設へのセキュリティ・アクセスを有するために、当該人物が本人であることを確認するために使用される）バイオメトリック・システムは、RBIとは区別されるため、この禁止の対象とはならない（前文第15項）。

AI Actは、厳密に必要な限られた状況（以下に列挙するいずれかのもの）において、加盟国が法執行目的のためにRBIの使用を許可することを認めている（しかし、義務付けてはいない）。

- 拉致、人身売買、性的搾取の特定の被害者を対象とした捜索や、行方不明者の捜索
- 生命もしくは身体の安全に対する具体的、実質的かつ差し迫った脅威、またはテロ攻撃に対する真正かつ現在または予見可能な脅威の防止
- 重大な犯罪（付属書IIで言及されているもので、当該加盟国において4年以上の実刑判決により処罰され得るもの）に関する、容疑者の所在の確認または身元の特定、捜査の実施、起訴または刑事罰の執行

適用除外は、特別に対象とされた個人の身元を確認するために使用されるRBIのみを許可するものである。加えて、RBIの使用は、状況の性質、特にシステムが使用されなかった場合に生じる害悪の重大性、蓋然性および規模を、関係者の権利および自由に対する影響に照らして考慮すべきである。さらに、使用に対する保護には、基本的権利評価を完了することの要求、第49条に沿ったEUデータベースへのシステムの登録、司法当局または行政当局による各使用ケースの事前承認（緊急措置の対象）が含まれる。さらに、一般にアクセス可能な空間におけるRBIの使用は、関連する市場監視当局および各国のデータ保護当局に通知されなければならない。その後、各国当局は欧州委員会に報告しなければならず、欧州委員会は、これらの規定に従って、RBIの使用状況に関する年次の加盟国報告書を作成する。

禁止の適用対象となるのは誰か？

第2章で述べたように、AI Actは、AIシステムに関わるさまざまな関係者を区別し、AIモデルまたはシステムとの関係における役割に基づいて特定の責任を負わせている。これより、AI技術の開発と実施に最も影響力のある者が、最高の基準を遵守することが確保される。

しかし、禁止されるプラクティスに関するルールは、オペレーターの別を問わない。言い換えれば、特定の役割（すなわち、禁止行為に関するAIシステムの提供、開発、配備、流通または使用に関与しているか否か）に関係なく、普遍的に適用される。

この広範な適用は、基本的権利を侵害する可能性のあるプラクティスや受け入れがたいリスクをもたらすプラクティスを阻止するための同法の厳しい姿勢を強調するものであり、また、有害なAI技術とのあらゆる種類の相互作用をカバーする規制への包括的なアプローチを強調するものである。

執行と制裁金

ある行為が禁止されている場合、当該AIシステムはEU域内では使用できない。また、違反があった場合、管轄当局は、違反者の前会計年度の全世界における年間総売上高の7%または3,500万ユーロのいずれか高い方を上限とする制裁金を科すことができる。

各国の市場監視当局は、禁止されているAIシステムに関するAI Actの規定の遵守を確保する責任を負う。各国の市場監視当局は、毎年、欧州委員会に対し、その年に発生した禁止されている手法の使用と、当該当局がとった対策について報告する。

参照条文等

サブリミナル的、操作的、詐欺的なテクニック	第5条第1項(a)	前文第28, 29項
脆弱性の悪用	第5条第1項(b)	前文第28, 29項
ソーシャル・スコアリング	第5条第1項(c)	前文第31項
犯罪リスク評価のためのプロファイリング	第5条第1項(d)	前文第42項
顔認識データベース	第5条第1項(e)	前文第43項
職業と教育における感情の推論	第5条第1項(f)	前文第44-45項
バイオメトリック分類	第5条第1項(g)	前文第30項
公共空間におけるリアルタイム遠隔生体認証	第5条第1項(h)	前文第32-41項

その他の有用なリソース

- 信頼できるAIのための倫理ガイドライン：AIに関するハイレベル専門家グループ（2019年）
  (ETHICS GUIDELINES FOR TRUSTWORTHY AI: High-Level Expert Group on Artificial Intelligence (2019))
- ビデオ機器を通じた個人データの処理に関するEDPBガイドライン
  (EDPB Guidelines on Processing Personal Data Through Video Devices)
- 法執行分野における顔認識技術の使用に関するEDPBガイドライン
  (EDPB Guidelines on Use of Facial Recognition Technology In The Area of Law Enforcement)
- 自動意思決定とプロファイリングに関するEDPBガイドライン
  (EDPB Guidelines on Automated Decision Making and Profiling)
- AI法案に関するEDPB-EDPS共同意見書
  (EDPB-EDPS Joint Opinion On The Proposal For The Artificial Intelligence Act)
- ソーシャルメディアにおける詐欺的デザインパターンに関するEDPBガイドライン
  (EDPB guidelines on Deceptive Design Patterns in Social Media)
- フィンランド市場当局によるダークパターンに関するガイドライン
  (Guidelines on dark patterns from the Finnish Market Authority)

高リスク AIシステム

ポイント

- AIシステムが*「高リスク(high-risk)」*のスコープに含まれるのは、以下いずれかの使用が意図されている場合である。
  - 付属書Iの対象となる法令に従って第三者適合性評価を受けなければならない製品または製品のセーフティ・コンポーネント
  - 付属書IIIに列挙されたいずれかを目的とするもの
- 高リスクAIシステムのプロバイダー、ディプロイヤー、輸入者、販売者、プロバイダーへの供給者は、AI Act上の義務を負う。市場参加者は、複数の役割を並行して担うことがあり、複数の義務を同時に遵守することが求められる。
- 高リスクAIシステムのプロバイダーは、コンプライアンス上の負担が最も重く、システムの市場投入やサービス開始の前に適合性評価を実施する必要がある。
- 高リスクAIシステムのプロバイダーに変更されることがあり得る（例えば、システムに自己の名称や商標を付す、大幅な変更を加える、元のプロバイダーの意図とは異なる目的でシステムを使用する、といったことにより、高リスクAIシステムのプロバイダーとなる）。

To do リスト

- [ ] AIシステムが、第6条（あわせて付属書Iおよび付属書III）に定められている高リスクの範囲に含まれるかどうかを判断する。
- [ ] バリューチェーンにおける自身の役割（プロバイダー、ディプロイヤー、輸入者、販売者または第三者提供者）を決定し、対応する義務を確認する。

高リスクAIシステムとしての分類

AI Actの主要部分は、高リスクAIシステムを規制するものである。同システムは、EU域内の人々の健康、安全、基本的権利に重大な有害な影響を及ぼす可能性のあるAIシステムである。高リスクAIシステムには主に2つのカテゴリーがある：

(a) 製品またはシステムのセーフティコンポーネントとして使用されることが意図されているシステム、またはそれ自体が製品またはシステムであり、付属書Iに記載されているEU整合法令の適用範囲に含まれるシステムで、各法令に従って第三者適合性評価を受ける必要があるもの、および

(b) AI Actの付属書IIIに規定されたユースケースの範囲に意図された目的が含まれるシステム。

カテゴリーA：付属書Iシステム

最初のカテゴリー(a)については、付属書Iに列挙されている製品の安全に関する法令が以下のカテゴリーをカバーしている：

- 機械類
- 玩具
- レジャーボートおよびパーソナルウォータークラフト
- リフト／エレベーター
- 爆発性雰囲気のための装置と保護システム
- 無線通信設備
- 圧力装置
- 空中ケーブル工事
- 個人用保護具
- ガス燃料を燃焼する機器、医療機器
- 体外診断用医療機器
- 民間航空機
- 二輪または三輪の車両
- 農業・林業用車両
- 舶用機器
- 鉄道システム
- 自動車とそのトレーラー
- 無人航空機

付属書Iの法令は、上記のカテゴリーを対象としているが、関連製品を対象とすることもあることに留意する必要がある。例えば、機械類規則は、機械だけでなく、吊り上げ用付属品や取り外し可能な機械式伝達装置も対象としている。また、ロボット工学の中核的規制でもあり、AI Actとその高リスク要件が大いに関連する、AI導入のもう一つの着実な成長分野でもある。

セーフティ・コンポーネントは、その故障や誤動作が人や財産の健康や安全を脅かすような場合に、製品の安全機能を果たすものである。セーフティ・コンポーネントについては、付属書I中の該当する製品安全に関する法令に従って、AIシステムがその法令に従って第三者適合性評価を受ける必要があるかどうかを確認する必要がある。例えば、欧州医療機器規則では、クラスIIa以上の医療機器は第三者適合性評価の対象となる。AIシステムがそのような医療機器のセーフティ・コンポーネントとして適格である場合、またはAIシステム自体がそのような医療機器を構成する場合、AI Actに基づく高リスクAIシステムとなる。

付属書Iの対象となる法令の中では、「*高リスク (high-risk)*」や「*中リスク (medium-risk)*」といった用語も使われている。しかし、これらの分類はAI Actにおける高リスクの分類とは別個のものである。例えば、適用されうる製品安全に関する法令の下で、製品が*「中リスク」*に分類される場合であっても、その製品が第三者適合性評価を受けなければならない場合、その製品のセーフティ・コンポーネントであるAIシステム、あるいはそれ自体がそのような製品を構成するAIシステムは、AI Actの下では高リスクとなる。

カテゴリーB：付属書IIIシステム

高リスクシステムの独立のリストには現在、以下のものが含まれている：

- **バイオメトリクス**：個人の遠隔生体認証、バイオメトリクス分類、および/または感情認識
- **重要インフラの管理・運営**：重要なデジタルインフラ（インターネットエクスチェンジ、DNSサービス、TLDレジストリ、クラウドコンピューティングサービス、データセンター、コンテンツデリバリーネットワーク、トラストサービスプロバイダー、電子通信ネットワークまたはサービスなど）の管理・運営、または水、ガス、暖房または電気の供給に関連して、物理的完全性または個人と財産の健康と安全を直接保護すること
- **教育および職業訓練**：教育および職業訓練における意思決定（学生または学生志願者の選抜、評価、査定、監視など）
- **採用および人事**：採用および人事における意思決定（従業員および／またはその他の労働者および／または応募者の選考、評価、査定、昇進、解雇、業務配分、モニタリングなど）
- **必要不可欠なサービス**：公的扶助給付（医療サービス、社会保障手当、障がい者手当など）の受給資格に対する（継続的な）評価、個人の信用度の評価、またはクレジットスコアの確立（金融詐欺の検出を除く）、生命保険および医療保険の場合の個人に関するリスク評価および価格設定、緊急通報の評価および分類、または緊急第一応答サービス（警察、消防、医療救助など）の派遣または派遣の優先順位付けに関する決定、および緊急医療患者のトリアージ
- **犯罪分析**：法執行当局による／法執行当局に代わって／法執行当局を支援するための以下の事項の評価：(i)個人が被害者または犯罪者（再犯を含む）になるリスク、(ii)個人の性格および特徴、(iii)個人または集団の過去の犯罪行動、または(iv)刑事犯罪の摘発、捜査、訴追の過程における個人のプロファイリング
- **証拠収集と評価**：刑事犯罪の捜査や起訴における、もしくは亡命、ビザ、滞在許可申請における、または関連する苦情申立てに対する、証拠の信頼性の評価。法執行当局または移民、亡命、もしくは国境管理を実施する当局による／そうした当局に代わって／そうした当局を支援するための、ポリグラフまたは類似のツールの使用
- **移民識別、移民リスクおよび移民申請評価**：移民、亡命または国境管理における個人の検出、認識または識別（旅券の照合は除く）。EU域内に入国しようとする、または入国した個人がもたらすリスク（安全保障リスク、非正規移民のリスク、健康リスクなど）の評価ならびに亡命、ビザ、滞在許可申請および関連する苦情申立ての審査
- **司法行政**：司法当局または裁判外紛争解決機関が事実と法律を調査・解釈し、法律を事実に適用することの支援
- **民主主義プロセス**：選挙や国民投票の結果または個人の投票行動に影響を与えること

なお、欧州委員会は、付属書IIIを改正することができる（第7条）。

> 意図された目的は、第3条第12号で次のように定義されている：*「使用説明書、販売促進資料、説明書、および技術文書においてプロバイダーが提供する情報に明記されている、具体的な使用状況および使用条件を含む、プロバイダーによって意図されたAIシステムの用法」*

例外：高リスクとはならないもの

第6条第3項は、意図された目的が付属書IIIの範囲に含まれ、（この規定がなければ）高リスクとなるAIシステムであっても、自然人の健康、安全または基本的権利に重大な害悪を及ぼす危険性がなければ、高リスクとはみなされないと定めている。条文では4つの基準が挙げられている。これらの基準の1つ以上が満たされる場合、適用除外として依拠することができる（第6条第3項および前文第53項）：

- AIシステムが、狭い手続き上のタスクを実行することを意図している場合
  - 例：非構造化データを構造化データに変換するシステムや、文書の重複を検出する

システム

- AIシステムが、すでに完了した人間の活動の結果を改善することを目的としている場合
  - 例：すでに作成された文書であって、使用される専門的なトーンやアカデミックなスタイルを改善するシステム
- AIシステムが、意思決定のパターンや以前の意思決定のパターンからの逸脱を検出することを意図しており、人間による適切なレビューなしに、すでに完了した人間の評価に取って代わったり影響を与えたりすることを意図していない場合
  - 例：教師が適用した評定を、その教師の既存の評定パターンと比較して、矛盾や異常をチェックするシステム
- AIシステムが、付属書IIIに列挙されているユースケースの目的に関連するアセスメントの準備作業を行うことを意図している場合
  - 例：文書を翻訳するシステム

これらの例外は、AIシステムが、Regulation (EU) 2016/679（GDPR）第4条第4号、Directive (EU) 2016/680（データ保護施行指令）第3条第4項またはRegulation (EU) 2018/1725（EU機関のデータ保護）第3条第5号（前文第53項）の意味における自然人のプロファイリングを含む場合には、適用されない。

これらの例外を利用しようとする事業者は、そのシステムが高リスクであるかどうかを証明する責任を負うことに留意すべきである。第6条第3項に基づく評価は、システムが市場に投入され、またはサービスが開始される前に文書化されなければならず、かつ、システムの登録がなされなければならない（第49条第2項および第6条第4項）。このようなシステムのプロバイダーは、要請があれば、この文書を各国の管轄当局に提出しなければならない。

欧州委員会は、AIシステムの高リスクおよび非高リスクのユースケースの包括的なリストを含む、第6条の実践的な実施に関するガイドラインを提供する（第6条第5項）。欧州委員会はまた、第6条第3項の基準を追加または修正する委任法令を採択することもできる。ガイドラインは、AI Actが発効した後6ヶ月以内に公表される予定である。

高リスクAIシステムのプロバイダーの義務

AI Actは、第3章第2, 3, 4節において、高リスクAIシステムのプロバイダーとディプロイヤーに対する義務の詳細なリストを以下のに定めている：

高リスクAIシステムに関するプロバイダーの義務	
第 2 節の要件	第 2 節（下記参照）の要件の遵守を確保すること。
プロバイダーの名称および連絡先	システムに（不可能な場合はパッケージまたは付属文書に）、プロバイダーの名称またはそのブランド名と連絡先を明記すること。

品質マネジメントシステム	第 17 条に準拠した品質マネジメントシステムを有すること。 （第 17 条には、方針、手順、指示を通じて文書化されるべきシステムの側面の詳細なリストが示されている。）
ドキュメンテーション	第 18 条で言及されている文書を保管すること。文書には以下が含まれる： • 技術文書（第 11 条） • 品質マネジメントシステムに関する文書（第 17 条） • 該当する場合、第三者認証機関により承認された変更に関する文書 • 該当する場合、認定機関が発行した決定書およびその他の文書 • EU 適合宣言書（第 47 条）
過去ログ	システムが自己の管理下にある場合は、システムによって自動的に生成されるログを保管すること（第 19 条）。 このようなログは、高リスク AI システムの意図された目的に適した期間保存されなければならない。その期間は少なくとも 6 ヶ月間以上でなければならない（個人データ保護の規定に別段の定めがある場合を除く）。
適合性評価	市場投入またはサービス開始前に、システムが第 43 条の適合性評価手続きを受けることを確保すること（下記参照）。
適合宣言	EU 適合宣言書を作成すること（第 47 条）。 下記参照
CE マーク	CE マークを高リスク AI システムに貼付すること（貼付できない場合は、パッケージまたは添付文書に貼付する）。 CE マークにより、高リスク AI システムが AI Act 第 48 条に適合していることが確認される。 下記参照。
登録義務	EU データベースへの登録義務（第 49 条第 1 項）を遵守すること。 下記参照。
是正措置／情報提供	システムが AI Act に適合していない場合、必要な是正措置を講じる、または回収、無効化もしくはリコールを行うこと。 システムが安全性または個人の基本的権利にリスクをもたらす場合、管轄の市場監視当局に通知すること。該当する場合には、そのシステムの認証書を発行した第三者認証機関にも通知する（第 79 条）。

適合性の証明	加盟国の管轄当局から合理的な要請があった場合、必要なすべての情報および文書を提出し、第 2 節（上記参照）に定める要求事項へのシステムの適合性を証明すること。 管轄当局との協力に関する義務は、第 21 条でより詳細に規定されている。 なお、加盟国の管轄当局と共有されるいかなる情報も、機密として扱われる
アクセシビリティ要件	高リスク AI システムが、アクセシビリティ要件に準拠していることを確認する： • （公共機関のウェブサイトおよびモバイルアプリケーションのアクセシビリティに関する）Directive (EU) 2016/2102 • （製品およびサービスのアクセシビリティ要件に関する）Directive (EU) 2019/882

高リスクAIシステムのプロバイダーに関する整合規格と適合性評価手続き

整合規格

整合規格はEU官報に掲載される。AIシステムがこれらの規格に適合している場合、そのAIシステムは、第3章第2節（第40条第1項）の高リスクAIシステムの要件に適合していると推定される。

整合規格は実務上、非常に重要な意味を持つ。伝統的な製品安全に関する法令の下では、*「製造者(manufacturer)」*は、通常、製品安全に関する法令の要求事項への準拠を証明するために、それに従っている。これはAI Actでも同様である。

欧州委員会は、第40条第2項に基づき、標準化団体CENおよびCELENECに対し、2025年4月30日までに第3章第2節の要求事項をカバーする整合規格を起草するよう要請する標準化要請書（草案）を発行した。

適合性評価手続き

第43条に基づく高リスクAIシステムの適合性評価手続きは、プロバイダーに対し、第3章第2節（以下に概要を示す）の高リスクAIシステムに関する要件の遵守を証明することを求めている。

付属書III 高リスクAIシステム

AI Actは、適合性評価について2つの主要な手続きを概説している。付属書IIIの高リスクAIシステム（付属書IIIの第2項から第8項に記載されたシステム）のプロバイダーの大半は、第三者認証機関を介さずに、付属書VIに規定された内部管理手続きに従わなければならない。付属書III（バイオメトリクス）の第1項に列挙された高リスクAIシステムのプロバイダーで、第40条および第41 条で言及されている整合規格または共通規格を適用している者も、十分な内部管理手続きに従わなければならない。しかし、これを実施していない高リスクのバイオメトリクス・システムのプロバイダーに対しては、第三者認証機関の関与が求められる。

付属書I 高リスクAIシステム

高リスクAIシステムが付属書Iのセクション Aに列挙されたEU整合法令に該当する場合、これらの法令に基づく適合性評価手続きが適用される。第3章第2節の高リスクAIシステムの要件はこの評価に統合され、付属書VIIの特定の規定も適用される。これらの法令に基づく第三者認証機関は、一貫した監視を確保するため、AI Act の特定の要件を遵守しなければならない。

重大な変更に対する新たな適合性評価

高リスクAIシステムに重大な変更を加える場合、新たな適合性評価が必要となる。しかし、システムがあらかじめ定めたトレーニングプロセスの一部をなす変更は、重大な変更とはみなされない。

高リスクAIシステムの要件

高リスクAIシステムに対する要求事項（第8条から第15条に焦点を当てる）	
要求事項の遵守（第 8 条）	第 8 条は、高リスク AI システムは、意図された用途と技術の状況を考慮し、そのライフサイクルを通じて、技術的・組織的要件（第 9 条から第 15 条）を満たさなければならないことを強調している。人間に影響を与える要件に優先順位をつけることが極めて重要であり、適切なトレードオフが見いだせない場合は、AI システムを導入すべきではない。

リスク管理（第 9 条）	第 9 条は、プロバイダーに対し、リスク管理システムの確立を求めている。これは、予見可能なリスクを特定、分析、軽減するための継続的なプロセスであり、リスク軽減措置の設計、コントロールの実施、ユーザー情報やトレーニングの提供を含む。取られた措置は文書化され、高リスクの AI システムは適切な段階でテストされ、一貫した性能を確保しなければならない。
データガバナンス（第 10 条）	堅牢なデータガバナンスは、高リスク AI システムの技術的・組織的要件の重要な要素である。システムの適切な機能と安全性を確保するためには、高品質で、代表的で、可能な限りエラーのない、完全なトレーニング、検証、試験のためのデータセットが必要である。プロバイダーはまた、禁止された差別につながる可能性のあるデータセットの偏りを軽減するための措置を講じなければならない。データの完全性を検証し、AI Act のデータガバナンス要件を遵守していることを証明するために、認証された第三者サービスを採用することができる。
技術文書と記録の保持（第 11 条および第 12 条）	第 11 条と第 12 条では、システムのライフサイクルを通じて、詳細な技術文書と記録保管ログが必要である。プロバイダーは配備前にこれを準備し、定期的に更新しなければならない。これは、システムの特性、アルゴリズム、データ、トレーニング、テスト、検証、リスク管理など、システムのあらゆる側面をカバーするものでなければならない。高リスク AI システムは、トレーサビリティを提供し、潜在的なリスクや必要な修正を特定するために、使用ログも自動的に記録する必要がある。
透明性と情報提供（第 13 条）	第 13 条は、高リスク AI システムのディプロイヤーに対する明確で包括的な指示を提供するよう義務付けている。これらの指示は、ディプロイヤーがシステムのアウトプットを正しく理解し、使用することを可能にするものでなければならない。システムの意思決定は理解可能なものでなければならず、その出所、特徴、制限、目的、正確性、危険性、能力、監督、保守、期待される存続期間に関する詳細が提供されなければならない。すべての文書は、予定されるディプロイヤーのニーズと知識レベルに合わせて作成されなければならない。
人間による監督（第 14 条）	人間による監督の措置は、健康、安全および権利に対するリスクを防止または最小化しなければならない。これらの措置は、システムのリスクと自律性のレベルに見合ったものでなければならない。また、人間であるオペレーターは、必要に応じてシステムをオーバーライドできなければならない。 監督機能は、以下のような方法で実現できる： • 内蔵されたシステム制約と人間であるオペレーターへの応答性 • ディプロイヤーが十分な情報を得た上で自律的な意思決定を行えるよう、ディプロイヤー向けにプロバイダーが定めた対策 • 監督アプローチには、アプリケーションのリスクに応じて、ヒューマンインザループ、ヒューマンオンザループ、ヒューマンインコマンドが含まれる

正確性、堅牢性、サイバーセキュリティ（第 15 条）	第 15 条では、高リスク AI システムは、適切な精度、堅牢性およびサイバーセキュリティレベルを達成しなければならないと定めている。精度の対策には予測誤差の最小化が含まれ、堅牢性の対策はシステムがエラーや矛盾に対処できることを保証する。最後に、サイバーセキュリティ対策は、無許可のシステム改変から保護するものでなければならない。この場合、EU サイバーレジリエンス法の対象となる関連 AI システムについては、EU サイバーレジリエンス法を通じてコンプライアンスを証明することができる。

高リスクAIシステムのディプロイヤーの義務

AI Actは、高リスクAIシステムのディプロイヤーに対する義務を定めている（第26条）。

技術的・組織的対策

ディプロイヤーは、システムに付随する使用説明書に従ってシステムを確実に使用するために、適切な技術的・組織的措置を講じなければならない。

人間による監督

ディプロイヤーは、必要な能力および権限を持ち、訓練を受け、必要なサポートを受けられる自然人に、人間による監督の役割を割り当てなければならない。

インプットデータ

ディプロイヤーがインプットデータを管理する場合、ディプロイヤーはインプットデータに関連性があり、十分に代表的であることを確保しなければならない。言い換えれば、この原則は、インプットデータの質に関するディプロイヤーの責任を表明するものである。

高リスクAIシステムの監視

ディプロイヤーは、使用説明書に基づいて高リスクAIシステムの動作を監視しなければならない。

ディプロイヤーは、市販後の活動に関する第72条に従って、プロバイダーへの通知を実施しなければならない。ディプロイヤーは、第79条第1項に従いリスクを特定した場合、直ちにプロバイダー、次いで輸入者または販売者および関連する市場監視当局に通知し、そのシステムの使用を一時停止する。重大なインシデントが確認された場合、ディプロイヤーはまた、その事態を直ちにプロバイダー、次いで輸入者または販売者および関連する市場監視当局に通知しなければならない。

過去ログ

高リスクAIシステムのディプロイヤーは、そのログが自己の管理下にある場合、高リスクAIシステムによって自動的に生成されたログを、高リスクAIシステムの意図された目的に適した期間、保管しなければならない。この期間は、適用されるEU法または国内法、特に個人データの保護に関する法律に別段の定めがない限り、少なくとも6ヶ月間である。

労働者の代表への情報提供

ディプロイヤーが使用者である場合、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対し、高リスクAIシステムの使用対象となることを通知しなければならない。

ディプロイヤーが公的機関の場合

高リスクAIシステムのディプロイヤーが公的機関、またはEUの機関、団体、事務局、またはエージェンシーである場合、第49条に基づきEUデータベースへの登録義務を遵守しなければならない。

データ保護影響評価

高リスクAIシステムのディプロイヤーが、Regulation (EU) 2016/679（GDPR）第35条またはDirective (EU) 2016/680（データ保護施行指令）第27条に基づきデータ保護影響評価を実施する必要がある場合、AI Act第13条に基づきプロバイダーが提供する情報を利用しなければならない。

犯罪捜査 – 事後遠隔生体認証のための高リスクAIシステム

Directive (EU) 2016/680を損なうことなく、犯罪を犯したと疑われる者または有罪判決を受けた者を対象とした捜査の枠組みにおいて、事後遠隔生体認証のための高リスクAIシステムの導入を希望する者は、事前、または不当な遅延なく、遅くとも48時間以内に、司法当局または行政当局にこの使用の認可を請求しなければならない。

高リスクAIシステムの基本的権利影響評価

第6条第2項にいう高リスクAIシステム（AI Act付属書IIIに詳述されている高リスクAIシステム）を配備する前に、ディプロイヤーが、

i. 公法が適用される団体、または

ii. 公共サービスを提供する民間団体である場合であって、これら(i), (ii)いずれの場合にも

iii. 高リスクAIシステムの使用を、

   a. 自然人の信用度を評価し、クレジットスコアを設定するため（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）に使用する意図を有し、かつ、

   b. 生命保険および医療保険の場合には自然人に関するリスク評価および価格設定のために使用する意図を有している場合、ディプロイヤーは、システムの使用が基本的権利に与える影響を評価しなければならない（FRIA）。ただし、重要インフラに関連する高リスクAIシステムについては例外がある。

評価内容は以下のとおり：

- 高リスクAIシステムがその意図された目的に沿って使用されるプロセスに関する、ディプロイヤーによる説明
- 各高リスクAIシステムの使用が予定される期間と頻度の説明
- 特定の状況において、その使用によって影響を受ける可能性のある自然人および集団のカテゴリー
- 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、上記に従って特定された自然人または集団のカテゴリーに影響を及ぼす可能性のある具体的な害悪のリスク
- 使用説明書に従った、人間による監督措置の実施に関する記述
- これらのリスクが顕在化した場合に取るべき措置（内部統治および苦情処理のメカニズムを含む）

高リスクAIシステムに関連する他の当事者の義務

AI Actにおける高リスクシステムに関する義務の大半は、プロバイダーとディプロイヤーに向けられたものである。ただし、その他の関係者（すなわち、高リスクAIシステムの輸入者および販売者、および高リスクAIシステムで使用または統合されるあらゆるシステム、ツール、サービス、コンポーネント、またはプロセスのサプライヤー）には、限定的な義務が課せられる。サプライヤーによるサービスの例としては、モデル（再）トレーニング、試験および評価、ソフトウェアへの統合などがある（前文第88項）。義務は、関連製品またはサービスを自由かつオープンソースのライセンスで提供するサプライヤーには適用されない（第25条第4項）。さらに、AIシステムの当初のプロバイダー以外の当事者が、AI Actによって高リスクAIシステムのプロバイダーとしての役割を割り当てられる可能性もある。

輸入者、販売者、サプライヤーの義務

第23, 24, 25条は、輸入者、販売者およびサプライヤーの義務を定めている：

輸入業者（第 23 条）	販売者（第 24 条）	サプライヤー（第 25 条）
検証：システムを市場に投入する前に、プロバイダーが真正に以下を実施しているかどうかを検証する： • 適合性評価手続きの実施 • 技術文書の作成 • CE マークの貼付および EU 適合宣言書の添付 • 指定代理人の指名	**検証**：システムを市場に出す前に、以下を検証する： • CE マークが表示されていること • EU 適合宣言書および使用説明書のコピーが添付されていること • プロバイダーおよび輸入者が、該当する場合、それぞれの義務を遵守していること	**サポートの提供**：書面による合意により、高リスク AI システムのプロバイダーがその義務を完全に遵守できるようにするために、必要な情報、能力、技術的アクセス、および一般に認められた最新技術に基づくその他の援助を特定する。 AI 事務局／委員会はまた、高リスク AI システムのプロバイダーとその第三者サプライヤーとの間で、自主的なモデル契約条件を策定し、推奨することができる（第 25 条第 4 項および前文第 90 項）。
リスクフラグ：システムが人の健康、安全、または基本的権利に対するリスク[1]を提示する場合、プロバイダー、指定代理人、および市場監視当局に通知する。	**リスクフラグ**：システムが第 2 節に規定された要求事項に適合していないと販売者が考える、または考える理由がある場合、システムが適合するまで、システムを利用可能にしないこと。また、システムが人の健康、安全、または基本的権利にリスクをもたらす場合、直ちにシステムのプロバイダーまたは輸入者および管轄当局に通知し、特に違反の詳細と講じられた是正措置について報告すること。	
注意点：保管・輸送条件が、第 2 節の要件への準拠を危うくしないことを確認する。	**注意点**：保管・輸送条件が、第 2 節の要件への準拠を危うくしないことを確認する。	
当局への協力：合理的な要請があった場合、システムの適合性を証明するために、技術文書を含む必要なすべての情報／文書を管轄当局に提供し、かつ当該システムに関連して当局が取るあらゆる措置に協力する。	**当局への協力**：合理的な要請があった場合、システムの適合性を証明するために、上記における義務に関するすべての必要な情報／文書を管轄当局に提供し、当該システムに関連して当局が取るあらゆる措置に協力する。	

記録の保存：システムの市場投入／サービス開始後 10 年間は、第三者認証機関が発行した認証書（第三者適合性評価の場合）、使用説明書および EU 適合宣言書の写しを保存する。

連絡先の詳細：システム、その包装または添付文書に、輸入者に連絡するための名称、登録商標または登録商号、住所を記載する。

是正措置：販売者がシステムを第 2 節に定める要求事項に適合していないと考える、またはそう考える理由がある場合、システムを適合させるために必要な是正措置を講じる、または、システムを回収もしくはリコールすること、またはプロバイダー、輸入者もしくは関連するオペレーターが是正措置を適宜講じることを確実にする。

x

---

1. ここでいうリスクとは *「意図された目的との関連において、または当該製品の通常のもしくは合理的に予測可能な使用条件下において、使用期間および該当する場合にはサービスの開始、設置および保守の要件を含め、合理的かつ許容可能と考えられる程度を超える程度に、人の健康および安全全般、健康および安全（...）に悪影響を及ぼす可能性を有すること」*（Regulation (EU) 2019/1020（市場サーベイランス規則）第3条第19号と併せてAI Act第79条第1項）。

他者の（高リスク）AIシステムのプロバイダーになること

第25条第1項は、たとえその者がもともとAIシステムのプロバイダーでなかったとしても、以下いずれかに該当する場合、その者が高リスクAIシステムのプロバイダーとみなされると定めている：

- すでに市場に投入され、サービスが開始されている高リスクAIシステムに、自身の名称や商標を付けていること
- 既存の高リスクAIシステムを、高リスクのまま維持するような方法で[2]、重大な変更を加えること
- もともと高リスクでないAIシステムの目的を変更し、高リスクにすること

これら3つの状況のいずれかが発生した場合、元のプロバイダーはもはや（新規または新たに使用される）AIシステムのプロバイダーとはみなされない。このようなプロバイダーの役割の切替えにつながる可能性がある、実際に実務上よく起こる状況としては、第6条（および付属書IおよびIII）に規定されている高リスクのカテゴリーに入る方法で、ディプロイヤーが汎用目的AIシステムを配備することが挙げられる。そのような場合、ある者が高リスクの方法で汎用目的AIシステムを配備した場合、配備したディプロイヤーはプロバイダーの責任を引き受けることになる。

新たなプロバイダーは、高リスクAIシステムのプロバイダーの義務をすべて引き受ける。元のプロバイダーは、新たなプロバイダーと密接に協力し、必要な情報を提供し、システムをAI Actに適合させるために合理的に期待される技術的アクセスその他のサポートを提供する義務を負う（第25条第2項）。ただし、元のプロバイダーが、AIシステムを高リスクAIシステムに変更しないことを*「明確に指定(clearly specified)」*していた場合（第25条第2項）、または適用される契約において高リスクの目的での配備を禁止するなど*「高リスクAIシステムへの変更を明示的に除外していた(expressly excluded the change of the AI system into a high-risk AI system)」*（前文第86項）場合には、元のプロバイダーはこれを行う義務を負わない。高リスク目的での配備が禁止されていない場合、協力義務は適用されるが、知的財産権、業務上の機密情報、営業秘密を遵守し保護する必要性を損なうものではない（第25条第5項）。そのため、元のプロバイダーは、自らの知的財産権や営業秘密を損なう程度にまで協力する必要はない（前文第88項）。

欧州委員会は、今後、この第25条で言及されている要件と義務の適用に関するガイドラインを提供する（第96条第1項(a)）。

---

2. 「重大な変更」とは、第3条第23号において、*「市場に投入後またはサービス開始後のAIシステムの変更であって、プロバイダーが実施した最初の適合性評価において予見または計画されておらず、その結果、AIシステムの第3章第2節に規定された要件への適合性が影響を受けるか、またはAIシステムが評価された意図された目的の変更をもたらすもの」*と定義されている。欧州委員会は、実質的な変更に関する規定の実務的な実施について、さらなるガイドラインを提供する予定である（第96条第1項(c)）。また、前文第84項では、欧州医療機器規則など、新法規制の枠組みに基づく特定のEU整合法令で定められた規定も引き続き適用されるべきであると定めている。例えば、欧州医療機器規則第16条第2項は、特定の変更は、適用される要求事項への適合に影響を及ぼす可能性のある機器の変更であってはならないと定めており、これらの規定は、欧州医療機器規則上の医療機器である高リスクAIシステムにも引き続き適用されるべきである。

参照条文等

高リスクシステムの範囲	第6条、付属書I, III	前文第43-63項
高リスクAIシステムのプロバイダーに対する要件	第8条-第22条、第43条、第47-49条	前文第64-83, 123-128, 147, 131項
高リスクAIシステムのディプロイヤーに対する要件	第26, 27条	前文第91-96項
高リスクAIシステムの輸入者に対する要件	第23条	前文第83項
高リスクAIシステムの販売者に対する要件	第24条	前文第83項
高リスクAIシステムの販売者に対する要件	第25条	前文第83-90項
高リスクAIシステムに関する第三者サプライヤーに対する要件	第40, 41条	前文第121項
適合性評価手続き	第28条	前文第149項

汎用目的AIモデル

ポイント

- 汎用目的AIモデルは、処理できるタスクの汎用性が非常に高い汎用AIコンポーネントであり、特に近時の生成AIモデルを包含している。
- 汎用目的AIモデルの微調整や修正が、新たな汎用目的AIモデルを生み出す可能性がある。
- 汎用目的AIモデルのプロバイダーは、AI事務局や管轄当局に対してだけでなく、自身のAIシステムを汎用目的AIモデルと統合しようとするAIシステムのプロバイダーに対しても、多くの透明性の義務を負う。
- システミック・リスクをもたらす汎用目的AIモデル、すなわちこれまでで最も多用途で強力なモデルには、評価、透明性、セキュリティ、リスク評価、インシデント管理についてより高い義務が設定されている。システミック・リスクを伴う汎用目的AIモデルの分類手順は、汎用目的AIモデルのプロバイダーにとって重要な分野となるはずである。
- 実践規範の策定と公表は、汎用目的AIモデルのプロバイダーが、その義務を遵守するために実施すべき具体的な技術的・組織的措置を特定するのに役立つだろう。
- 汎用目的AIモデルに関する規定は2025年8月2日から適用される。

To doリスト

- [ ] 汎用目的AIモデル、汎用目的AIシステム、AIシステム、および高リスクAIシステムの概念 - およびこれらの相互関係 - に慣れ親しむこと。この理解は、自身がどのシステムを使用または販売しているかを評価し、十分な情報に基づいた法的評価を行う上で極めて重要である。
- [ ] 汎用目的AIモデルのプロバイダー向け：徹底したガバナンスの見直しを行い、コンプライアンスを確保するために必要な調整を行うこと。 - 汎用目的AIモデルのプロバイダーに対する義務は、AI Actの中で最も厳しいものの一つである。
- [ ] 汎用目的AIモデルのプロバイダー向け：包括的かつ法的な知的財産の評価を実施すること。汎用目的AIモデルに関する規制は、特に著作権のポリシーや様々なトレーニングデータについての義務など、知的財産権法制と大きく絡んでいる。
- [ ] 汎用目的AIモデルのプロバイダー向け：*「システミック・リスク(systemic risk)」*の閾値は、委任法令を通じて将来にわたり調整される可能性があるため、継続的かつ注意深く監視すること。
- [ ] 汎用目的AIモデルのプロバイダー向け：汎用目的AIモデルのプロバイダーが実務上義務をどのように遵守するかについての、具体的かつ技術的な詳細を含む実践規範の策定・公表を注視すること。当事務所のニュースレター「Connected」に登録し、最新の動向をご確認ください！！

汎用目的AIモデルの背景と関連性

AI Actの立法過程で最も目立った議論のひとつは、汎用目的AIの規制をめぐるものだった。AI Actの最初の草案（2021年4月の欧州委員会の提案）は、各AIシステムは特定の目的のために作られ、その目的は特定のリスクの可能性と関連づけられるという理解に基づいていた。この分類では、幅広いユースケースに適用できるよう、幅広いデータで訓練された基盤モデルは念頭になかった。こうしたAIモデルは、同法の最初の草案にあった、リスクベースのスキームには当てはまらなかった。このようなモデルの特定の能力と危険性を考慮した新しいカテゴリーを含めるために、分類を拡大する必要があった。2023年夏、*「基盤モデル(foundation model)」*（後に汎用目的AIと改称）が当時の同法草案に追加された。

AI Actの汎用目的AIモデルの規制に関する章は、主に2つの理由から重要な意味を持つ：

- 第一に、ビジネス環境において現在最も魅力的な新たな機会を開きつつあるAIのサブセットであり、事業者のユースケースの大部分を包含する生成AIを取り上げている。
- 第二に、AI Actに基づく汎用目的AIの要件は、高リスクAIシステムの要件と並んで、同法の中で最も厳しいものであり、ビジネスへの導入には、最大限の注意が必要である。

この重要性は、すべての要求事項がディプロイヤーではなく、プロバイダーだけに向けられたものであるという事実によって、いくらか弱められているに過ぎない。

用語および汎用目的AIのバリューチェーン

汎用目的AIモデルと汎用目的AIシステム

第3条第63号は、汎用目的AIモデルの特徴を概説し、様々なタスクに対応できる汎用性と能力を強調している。

前文第98項は、2つの重要な指標を強調している。

1. 少なくとも10億のパラメータを持つ
2. 自己教師（self-supervision）を使って大量のデータで学習される

これらのモデルは、多様な川下のシステムやアプリケーションに統合して機能する能力によって区別される。一般的に、汎用目的AIモデルは、大量のデータセットを用いて大規模な学習を行い、多くの場合、大規模な自己教師のような手法を利用する。前文第99項は、さらに、LLMや拡散モデルのような大規模な生成AIモデルが、汎用目的AIモデルの典型例であると規定している。

前文第97項は、汎用目的AIモデルはAIシステムの重要な構成要素ではあるが、AIシステムそのものではないことを明確にしている。汎用目的AIモデルを完全に運用可能なAIシステムに変換するには、ユーザー・インターフェースなどの追加要素が必要である。汎用目的AIシステムとは、汎用目的AIモデルの上に構築されたAIシステムであり、様々なタスクに対する汎用性を維持するものである（第3条第66号および前文第100項）。例を挙げて説明すると、翻訳のみを行うシステムは、汎用目的AIシステムとして認められない可能性が高い。

汎用目的AIシステムと高リスクAIシステム

前文第85項は、汎用目的AIシステムは、その汎用性から、高リスクAIシステムとして、あるいはその中のコンポーネントとして機能する可能性があることを強調している。汎用目的AIシステムのプロバイダーは、AI Actの遵守を確保し、AIのバリューチェーンに沿って公平に責任を分配するために、高リスクAIシステムのプロバイダーと緊密に協力しなければならない（高リスクシステムについては第4章を参照）。

汎用目的AIモデルの修正と微調整

特定のタスクに対してより良いパフォーマンスを達成するために、新しい専門化されたトレーニングデータセットをモデルに供給する形で汎用目的AIモデルを修正または微調整することは、汎用目的AIシステムに変換させることにはならない。すなわち、インターフェイスを持たない抽象的なモデルのままである。その代わりに、このようなアクションは、修正または微調整された汎用目的AIモデルを作り出す。前文第97項と前文第109項は、汎用目的AIモデルを修正または微調整するプロバイダーは、技術文書や使用したトレーニングデータの概要を提供するなど、変更点のみに関連する限定的な義務を負うと規定している。

汎用目的AIモデルのプロバイダーの義務

汎用目的AIモデルを市場に投入する、あるいは自身のAIシステムと統合して市場に投入しもしくはサービスを開始するプロバイダーは、以下の義務を負う。

a. AI事務局および管轄当局が利用できるようにするために、モデルの説明およびその開発プロセス（トレーニング、試験および検証を含む）に関する情報（第53条第1項(a)）を含む最新の技術文書を作成し、維持すること。

b. 川下のAIシステムプロバイダー（すなわち、自らのAIシステムを汎用目的AIモデルと統合することを望む者）がモデルの特性を理解し、自らの義務を遵守できるように、一定の情報および文書を準備し、最新の状態に維持し、利用できるようにすること（第53条第1項(b)）。最低限必要な情報のリストは付属書XIIに記載されている。プロバイダーは、共有する情報と、事業上の機密情報や営業秘密を保護する必要性とのバランスをとることが認められている。

c. デジタル単一市場における著作権および関連する権利に関するDirective (EU) 2019/790の第4条第3項に規定されているテキストマイニングおよびデータマイニングのオプトアウトの権利を考慮し、著作権および関連する権利に関するRegulation (EU)の第53条第1項目(c)を遵守するためのポリシーを確立すること（AI Actは、ポリシーで対処しなければならないその他の事項を規定していない）。

d. モデルのトレーニングに使用したデータに関する包括的なサマリーを作成し、公にすること（第53条第1項(d)）。AI事務局がこの目的のためのひな形を提供することになっている。前文第107項が説明するように、概要は、例えば、使用された主なデータコレクション、データベース、データアーカイブを列挙することにより、利害関係者が権利を行使できるようにすべきである。

e. 関係当局がAI Actに基づき付与された権限を行使する際に協力すること（第53条第3項）

f. プロバイダーがEU域外に設立されている場合、EU域内の指定代理人を指名すること（第54条第1項）

プロバイダーが汎用目的AIモデルを無償のオープンソースライセンスの下でリリースし、関連情報を一般に公開する場合、その汎用目的AIモデルがシステミック・リスクをもたらすと認定されない限り、上記a,bおよびfに列挙された要件を満たす必要はない（第53条第2項および第54条第6項）。

システミック・リスクを伴う汎用目的AIモデル

資格基準

AI Actは、*「システミック・リスク」*、例えば、重大事故、重要セクターの混乱、公衆衛生および安全、公共および経済の安全保障ならびに民主主義プロセスに対する深刻な影響、虚偽または差別的なコンテンツの流布などに関する合理的に予見可能な悪影響をもたらす汎用目的AIモデルに対して、特定のより重い義務を導入している（前文第110項）。

AI Act第51条第1項によれば、汎用目的AIモデルは、以下2つの条件のいずれかを満たす場合、システミック・リスクを有する汎用AIモデルとして分類される：(a)技術的なツールや方法論に基

づいて*「高い影響能力(high impact capabilities)」*を有すると評価された場合、または、(b)付属書XIIIに規定された基準を考慮し、(a)に規定されたものと同等の能力または影響力を有すると欧州委員会が指定した場合。これらの基準には、特に、モデルのパラメータ数、データセットの質または規模、学習に使用する計算量、欧州市場へのモデルの影響、EUでの登録ユーザー数などが含まれる。

さらに、10の25乗以上の浮動小数点の演算、すなわち大規模な計算能力で学習されたモデルは、*「影響の大きい能力」*を持つと推定される（第51条第2項）。このガイドの時点では、この閾値を満たす大規模言語モデルはほんの一握りである。

AI Act第52条は、分類手続きを定めている。最も注目すべきは、システミック・リスクの分類条件を満たす汎用目的AIモデルのプロバイダーは、その要件を満たした後、あるいは満たすであろうことが判明した後、遅滞なく、遅くとも2週間以内に、欧州委員会に通知しなければならないという点である。プロバイダーは、要件を満たしているにもかかわらず、自身のモデルがシステミック・リスクをもたらさないことを証明するための論拠を示すことができる。欧州委員会がそのような主張を却下した場合、当該モデルはシステミック・リスクをもたらすものとみなされる。プロバイダーからの*「合理的な要請(reasoned request)」*があった場合、欧州委員会は分類の再評価を決定することができる（第52条第5項）。

システミック・リスクを伴う汎用目的AIモデルのリストは、欧州委員会により公表され、更新される（第52条第6項）。

システミック・リスクを伴う汎用目的AIモデルのプロバイダーに対する義務

すべての汎用目的AIモデルのプロバイダーに適用される一般的な要件に加えて、AI Actは、システミック・リスクを伴う汎用目的AIモデルのプロバイダーに対して、さらに強化された義務を課している（第53条第1項および第55条第1項）。これらの義務は、モデルが市場に投入される前からそのライフサイクル全体を通じて適用され、以下の事項に関連する：

- モデルの評価
- システミック・リスクの評価と低減
- インシデント管理と報告
- サイバーセキュリティ保護レベルの向上
- 拡張された技術文書

透明性

ポイント

AI Actは、AIシステムをリスクレベル別に分類し、リスクの高いカテゴリーについては高い透明性を求める。高リスクAIシステムについては、市場に投入される前、またはサービスが開始される前に透明性が求められる。高リスクAIシステムに対する透明性要件の詳細については、本ガイド第4章を参照のこと。

さらに、AI Actは、特定の種類の商品について、第50条に基づく透明性の要件を義務付けており、プロバイダーまたはディプロイヤーのいずれかによって、適切な情報が個人に提供されることを要求している：

- ディスクレーマー：個人に直接作用することを意図したAIシステムのプロバイダーは、個人がAIシステムと接している事実を個人に知らされるように、AIシステムを設計・開発する必要がある。
- マーキング要件：AIシステムのプロバイダーは、AIが生成したコンテンツ（音声、画像、動画、テキスト）を、人間が生成したコンテンツと区別する方法でマークを表示しなければならない。
- ディープフェイクのマーキング：AIが生成したコンテンツ（画像、音声、動画）のうち、実在の人物に似ており、本物と誤解させる可能性のあるものにはラベルを付す必要がある。
- 感情認識システム／バイオメトリクス分類システム：AIシステムのディプロイヤーは、これらのシステムの動作を個人に認識させるべきである。

AI Act上の透明性の義務は、EUの他の規制の枠組みと連携している。特に、GDPRの透明性要件とAI Actの透明性要件には重なる部分があるが、後者はより技術的な性質を持っている。

To doリスト

プロバイダー向け

- [ ] マーキングの実装：AIが生成したコンテンツが機械可読な形でマークされるようにすること。
- [ ] ディスクレーマーの導入：個人と直接対話することを意図したAIシステムに、適切なディスクレーマーが追加されるようにすること。

ディプロイヤー向け

- [ ] ディープフェイク：明確かつ区別可能な方法で「ディープフェイク」と表示し、人為的に作成または操作されたものであることを明らかにすること。
- [ ] 感情認識システム／バイオメトリック分類システム：そのようなシステムが稼働していることを個人に認識させること。

一般的な透明性の義務

AI Actは、AIシステムの利用における透明性の重要性を認めている。個人がAIシステムの設計と利用を理解できるようにすべきであり、事業者や公的機関による決定にはアカウンタビリティがあるべきである。透明性はまた、AIシステムに対する社会の信頼を生み出し、その責任ある展開を確保するためにも不可欠である。

さらに透明性は、より広範な「AIリテラシー」の概念を強化し、AIの機会とリスク、そしてAIが引き起こす可能性のある害悪についての認識を深める。このような認識は、特に以下のような人々の間で育まれる必要がある：

- AIに関わる個人：AIの文脈における個人の権利について理解を深める
- ディプロイヤー：十分な情報を得た上でAIシステムを配備することができるようにする

プロバイダーには、また、特定の状況によってはディプロイヤーにも、独自の透明性の要件がある。AI Actは、AIシステムをリスクレベル別に分類しており、リスクの高いカテゴリーほど透明性への要求が高まる。

特定のタイプの製品に関する透明性要件は、以下のとおり。

プロバイダーの義務：

チャットボット（第50条第1項）

AI Act第50条第1項では、AIシステムのプロバイダーは、個人に直接作用することを意図したそのようなシステムが、当該個人がAIシステムと接していることを知らされるように設計・開発されることを確保する必要があると定めている。

- **対象読者**：この義務を実施する場合、プロバイダーは、ディスクレーマーが表示される対象読者を、意図された対象読者だけでなく、より広い潜在的な対象読者とすべきである。年齢や障がいのために社会的弱者に属する個人の特性は、AIシステムがそれらの集団との交信も意図している限りにおいて、考慮されるべきである。意図された、あるいは潜在的な対象読者は、アクセシビリティの検討に大きな影響を与える。
- **形式**：実務上、個人がAIシステムと接しているという明確な情報を提供する限り、プロバイダーはさまざまな形式（アバター、アイコン、インターフェースなど）で免責条項をデザインすることができる。

適用除外

- **明白である場合**：AIシステムの使用状況や文脈を考慮した場合、合理的で十分な知識を持ち、観察力があり、慎重な個人にとって、AIシステムと接していることが明白である場合、そのシステムはこの透明性要件から免除される。
- **合法的使用**：犯罪行為の検知、防止、捜査または訴追のために使用することが法律で認められているAIシステムで、第三者の権利と自由に対する適切な保護措置が講じられているものもまた、一般市民が犯罪行為を通報するためのシステムでない限り、これらの透明性要件から除外される。

AIが生成したコンテンツのマーキング（第50条第2項）

AI Act第50条第2項は、汎用目的AIシステムを含む、AIシステムのプロバイダーに対し、音声、画像、動画、テキストなどの合成コンテンツに適切なマーキングを行うことを義務付けている。前文第133項はその根拠を次のように説明する - AI技術の進歩に伴い、AIが生成する合成コンテンツは人間が生成したコンテンツと区別がつかなくなりつつあり、誤情報、操作、詐欺、なりすましおよび消費者を欺くリスクが高まっている。

マーキングの義務

- **マーキング**：AIシステムのプロバイダーのみが、AIが生成したコンテンツにマークを付けることを求められる。この要件は、コンテンツのディプロイヤーやその他のユーザーには適用されない。
- **フォーマット**：アウトプットは、人為的に生成または操作されたものであることを示すために、機械可読な形でマークされなければならない。
- **技術基準**：マーキングは、効果的で、相互運用可能で、しっかりとしたもので、信頼できるものでなければならない。プロバイダーは、コンテンツの種類、導入コスト、現在の技術標準を考慮する必要がある。

マーキング方法：

- **透かし**：目に見える透かしは、基本的な編集ツールで簡単に実装・削除できるが、目に見えない透かしは、検出と削除のための専用ソフトウェアが必要である。
- **メタデータ**：ファイルの作成と出所に関する情報を提供するが、ファイル編集ツールで簡単に変更したり削除したりできる。
- **アルゴリズムのフィンガープリント**：AIモデルは、生成したコンテンツに独特の痕跡や変則を残す。例えば、AIが生成した画像にはテクスチャやパターンにわずかな歪みがあるかもしれないし、AIが作成した音声ファイルには不自然な間やトーンのずれがあるかもしれない。
- **暗号署名**：コンテンツの真正性を検証する暗号ハッシュなど、暗号的手法で埋め込まれたデジタル署名。データのわずかな変更でも異なるハッシュが生成されるため、改ざんを簡単に検証できる。

AIが生成したコンテンツを管理・検出するためのツールや取組みは数多く存在する。アルゴリズムパターンや埋め込まれたメタデータを分析するディープフェイク検出ソフトウェアを使用するプラットフォームもあれば、メタデータや暗号ハッシュを利用してコンテンツの出所を認証するプラットフォームもある。例えば、プラットフォームは、音声分析ツールを使って合成音声を検出したり、ブロックチェーン技術を採用してデジタルアートの出所や改変を追跡したりすることができるかもしれない。

適用除外

- **編集支援**：主に定型的な編集作業の支援を提供する、または元のインプットデータに大きな変更を加えないAIシステムは、マーキング義務の対象外となる。
- **合法的使用**：犯罪行為の検知、防止、捜査または起訴に使用することが認められたAIシステムも、マーキング義務の対象外となる。

ディプロイヤーの義務：

感情認識／バイオメトリクス分類システム（第50条第3項）

AI Act第50条第3項では、ディプロイヤーに対する具体的な透明性要件を定めている。

- **感情認識システム**：自然人の生体データ、例えば顔の表情などの非言語的なサインに基づいて、自然人の感情や意図を特定または推論する目的で使用されるAIシステム。

または

- **バイオメトリクス分類システム**：生体データに基づいて自然人を特定のカテゴリーに割り当てる目的で使用されるAIシステム。このような特定のカテゴリーは、例えば、性別、年齢、髪の色、目の色、タトゥー、個人的特徴、民族的出自、個人的嗜好、興味などの側面に関連することがある。

感情認識システムやバイオメトリクス分類システムの使用禁止の詳細については、本ガイド第4章を参照のこと。

これらのシステムが許可される場合、ディプロイヤーはシステムの使用について、そのシステムにさらされる自然人に通知しなければならない。特に、生体データを処理することで、感情や意図を特定・推論したり、特定のカテゴリーに分類したりすることができるAIシステムにさらされる場合は、個人に通知されるべきである。

適用除外

- **合法的使用**：第三者の権利および自由に対する適切な保護措置の対象となる犯罪行為の検知、防止または捜査のために使用することが許可され、EU法に準拠するAIシステムは、これらの要件から免除される。

- **付随的使用のバイオメトリクス分類システム**：他の商業サービスに付随して使用され、客観的な技術的理由により厳密に必要とされるAIシステムは、これらの要件から免除される。

現時点では、提供すべき情報の範囲に関する明確なガイドラインはない。ディプロイヤーは、これらのシステムを使用する場合、処理の法的根拠に関する要件とは別に、適用されるGDPR、Regulation (EU) 2018/1725およびDirective (EU) 2016/680に従って個人データを処理する。つまり、これらの規制は、管理者として行動するディプロイヤーに対しても、別の透明性の義務を課す。このような場合であっても、GDPR第13条および第14条で義務付けられているとおり、個人はデータの処理について通知を受ける必要がある。自動化された処理に関しては、管理者は意思決定の背後にある論理を説明することが求められる。AIシステムの場合、これは説明可能性の声明（組織がAIを使用する理由、AIがどのように開発されたか、AIがどのように運用され使用されているかなどについての非技術的な説明を提供する文書）の一部として提供される可能性がある。

ディープフェイク（第50条第4項）

AI Act第50条第4項は、*「ディープフェイク(Deepfakes)」*と呼ばれるコンテンツについて、具体的なラベリング要件を定めている。これらの義務は、AIシステムがコンテンツの生成や操作に使用される際の透明性を確保するために極めて重要である。

ディープフェイクの定義（第3条第60号）

ディプロイヤーが以下のコンテンツを生成する場合、ディープフェイクに該当する：

- 画像、音声または動画を生成または操作するものであって、

- そうしたコンテンツが、実在の人物、物、場所、実体または出来事に著しく類似しており、かつ

- そのコンテンツが本物または真実であると誤解させる可能性があるもの。

ディープフェイクの例：

- 従業員を騙して大金を振り込ませるために会社幹部を装う、ディープフェイクのビデオ

- AIが生成した政治家が有権者に選挙日程を誤解させる、ロボコール音声

- 政治家になりすましソーシャルメディア上で世論を操作する、ディープフェイクの動画広告

- 著名人になりすますディープフェイク技術を使った、偽のZoomインタビュー

- 視聴者を欺くために捏造した報道を伝える、デジタルアバター

ラベリング要件

AI Actは、AIシステムによって生成または操作されるコンテンツは、人為的に作成または操作されたものであること明らかにするために、明確かつ区別できるように表示されなければならないことを義務付けている。この要件は、透明性を確保し、そのようなコンテンツによって一般大衆が惑わされるのを防ぐことを目的としている。現在のところ、コンテンツにどのようなラベルを付けるべきかについての明確なガイドラインはない。この問題は、将来、行動規範で扱われる可能性が高い。

コンテンツが人工的なものであることを示すために、透かし、メタデータ識別子、フィンガープリントなどの手法を用いるべきである（前文第133項参照）。このようなラベルは、視聴する者が容易に、即座に、そして常に目にすることができるようにすることが極めて重要である。例えば、動画の場合、プリロール・ラベルや永続的な透かしを使用することで、これらの要件を効果的に満たすことができる。

適用除外

AI Act第50条第4項により、ラベリング要件の一定の緩和と例外がある：

- 芸術的、創造的、風刺的、フィクション、またはそれらに類似する作品については、透明性の要件がより緩和される。このような作品の例としては、AIが生成した映画やパロデ

ィ、デジタルアートの展示、AIが生成したミュージックビデオなどがある。このような場合、視聴者の体験を妨げない形でAIの関与を開示する義務がある。これは、さりげない透かし、短い音声によるディスクレーマー、あるいはデジタルプラットフォーム上の説明文の注記によって達成されうる。

- AIが生成したコンテンツにラベルを付ける義務は、AIシステムの使用が犯罪の検知、防止、捜査または起訴の目的で法的に許可されている場合には適用されない。

- AIが生成したコンテンツが人によるレビューや編集管理を受けており、自然人または法人が出版物の編集責任を有している場合、ラベリング要件は適用されない可能性がある。つまり、AIが生成したコンテンツを人間が確認・承認し、その正確性と完全性を確保した場合、厳しいラベリング要件は緩和される可能性がある。この例外は、AIが生成したコンテンツの品質と信頼性を維持する上での人間の監視の役割を認めるものである。

高リスクAIシステムに関する透明性の義務

第50条第6項では、ここで概略を説明している透明性の義務が他の規制要件と並行して機能すると説明されている。それらの要件は、第3章に規定された義務や、EU法または国内法に基づく他の透明性要件に取って代わるものでも、それを軽減するものでもない。

詳細は本ガイド第4章を参照のこと。

タイミングおよび形式

第50条の透明性の義務を果たすために必要な情報はすべて、以下の形で個人に提供されなければならない：

- 明確かつ区別できるような方法で、

- 遅くとも、AIシステムとの最初の交信または接触が始まるまでに、

- 適用されるアクセシビリティ要件に準拠した形で。

アクセシビリティ要件とは、障がい者を含む多様な聴衆が情報にアクセスできることを意味する。実際には、状況によっては、ディスクレーマーや他のマーキングは、文字だけでなく、聴覚的、（音声付き）映像の形でも表示されなければならない。

もうひとつ考慮すべき点は、明確で十分な、しかし圧倒されることのない量の情報が提供されるべきであるということである。

加盟国レベルでの透明性の義務および実践規範

AI Act第50条第1項から第4項に概説される透明性の義務は、同条第6項によれば、他の規制要件と共存するように設計されている。これらは、第3章に規定された要件や、EU法または国内法に基づくその他の透明性義務に取って代わるものでも、軽減するものでもない。

AI事務局は、AI Act第50条第1項から第4項に基づく透明性確保義務のEUレベルでの効果的な実施を支援するため、第50条第7項に基づき、実践規範の策定を推進・促進する責任を負っている。これらの規範は、AIによって生成されたコンテンツの検出とラベリングの方法を明確にし、バリューチェーン全体の協力を強化し、人間が作成したコンテンツとAIが作成したコンテンツを公衆が明確に区別できるようにする（前文第135項）。

他の規制枠組みとの関係

- AI Act第50条第2項から第4項に基づく表示義務は、超大規模オンラインプラットフォーム（VLOP）と検索エンジン（VLOS）がディープフェイクの拡散に関連するリスクを特定し、軽減するためのデジタルサービス法（Digital Service Act; DSA）の要件をサポートする（DSA第33条等）。AIのプロバイダーがVLOPやVLOSから独立している場合、これらの表示により、プラットフォームはAIが生成したコンテンツをより効率的に認識すること

ができる。逆に、VLOPまたはVLOSがAIのプロバイダーでもある場合、そのDSA上の義務はAI Actによってさらに詳細化され、強化される。

- ディープフェイクに関する透明性ルールは、誤解を招く広告に関する欧州ガイドライン（不公正商行為指令（Unfair Commercial Practices Directive）参照）およびディープフェイクに関する国内刑事規定と相関する。

- AI Actの透明性の義務は、Regulation (EU) 2016/679に基づく透明性を支え、補完するものでもある。ただし、GDPRの透明性要件は、AIライフサイクルのあらゆる異なる段階（AI技術の開発、テスト、導入時など）でAI技術を使用する際に個人データが処理される場合に適用され、管理者に適用される。AIツールの開発者やプロバイダーが常にそのような役割を果たすとは限らない。その場合でも、AIツールの開発者やプロバイダーには、管理者が義務を果たせるよう、特定の情報を管理者に提供する義務が生じる可能性がある。

AI規制サンドボックス

ポイント

- AI Actは、プロバイダーが革新的なAIシステムを市場に投入する前に、一定期間テストを実施するための管理された環境を提供する*「AI規制サンドボックス(AI regulatory sandboxes)」*の設置を可能にしている。
- この制度は、AIのプロバイダー（またはプロバイダーになる可能性のある事業者）が、規制当局の監督下で、新しく革新的な製品を実験的に開発することを奨励する。中小事業者やスタートアップによる制度参加を促すことを目的とした特別なインセンティブも用意されている。
- 各加盟国は、2026年8月2日までに少なくとも1つのAI規制サンドボックスを設置しなければならないが、他の加盟国と協力して行うことも認められている。
- 欧州委員会は、AI規制サンドボックスの設置、運用、監督に関する詳細な取決めを定める実装法令を採択する予定である。
- AI Actはまた、参加者を保護するための一定の条件のもと、規制当局のサンドボックスの内外におけるAIシステムの*「実環境(real-world)」*テストについて定める。
- AI規制サンドボックスと実環境テストに関する制度は、EU全体で調和されることが意図されている。しかし、加盟国レベルでアプローチが異なる可能性があり、プロバイダーによる*「フォーラム・ショッピング(forum shopping)」*が行われる可能性がある。

To doリスト

- [ ] AI規制サンドボックスおよび実環境テストへの参加は任意である。AIのプロバイダーは、サンドボックスや実環境テストを利用する場合、AI Actの関連規定をよく理解し、欧州委員会がいずれ指定するAI規制サンドボックスの詳細な取決めを含め、これらのトピックに関する今後の発表やガイダンスに注意すべきである。
- [ ] AI製品／サービスのテストを実施する国をどこにするか、検討する必要がある。AI Actは調和の取れた制度を確立することを意図しているが、一部の加盟国が他の加盟国よりも自身にとってより適切である可能性がある。
- [ ] AI規制サンドボックスに参加することを決めた場合、サンドボックス計画を作成し、関連する加盟国の管轄当局が提供するガイドラインと監督に従う必要がある。また、実環境テストを実施する場合には、テスト計画を作成し、関連する市場監視当局の承認を得る必要がある。
- [ ] AI規制サンドボックスのプロセスを成功裡に完了した場合、関連する加盟国の管轄当局から終了報告書を取得するべきである。これは、AI製品／サービスの適合性評価プロセスを加速するために有用となるだろう。

AI規制サンドボックス

AI Actは、革新的なAIシステムが市場に出回ったり、その他の形で実用化されたりする前に、一定期間テストを実施するための管理された環境を提供する*「規制サンドボックス(regulatory sandboxes)」*の設置を可能にしている。AI規制サンドボックス制度の目的は以下のとおり：

- 革新的なAIシステムがAI Actに準拠していることを確認しながら、AIのイノベーションを促進すること。
- イノベーターにとっての法的確実性を高めること。
- AIの利用がもたらす機会、リスク、影響に関する各国管轄当局の理解を深めること。
- 協働とベストプラクティスの共有を支援すること。
- 中小事業者やスタートアップへの障壁を取り除くことを含め、市場へのアクセスを加速すること。

AI Actにおける規制のサンドボックスとは？

AI Actは、*「AI規制サンドボックス」*を次のように定義している：
「管轄当局が設定する管理された枠組みであり、AIシステムのプロバイダーまたはプロバイダーとなる可能性のある者に、管轄当局の監督下で、限定された期間、サンドボックス計画に従って、革新的なAIシステムを現実の状況下で開発、トレーニング、検証、テストする機会を提供するもの」

AI規制サンドボックスは、物理的、デジタル、またはハイブリッドの形態で設置することができ、物理的製品だけでなくデジタル製品にも対応することができる。

加盟国に対するAI規制サンドボックス設置義務

AI規制サンドボックスを設置する義務は、加盟国とその国の管轄当局にある（詳細は第8章参照）。各加盟国は、2026年8月2日までに少なくとも1つのAI規制サンドボックスを設置しなければならない。ただし、加盟国は、(i)加盟国レベルで1つ以上のAI規制サンドボックスを設置する、(ii)1つ以上の他の加盟国の国家管轄当局と共同でサンドボックスを設置する、(iii)既存のサンドボックスに参加する、のいずれかを選択することができる。

AI規制サンドボックスを設置する各国管轄当局は、適切な場合には他の関連する各国管轄当局と協力すべきであり、AIエコシステム内の他の当事者も巻き込むことができる。また、EUデータ保護監督機関は、EUの機関、団体、事務所およびエージェンシーのためにAI規制サンドボックスを設置することができる。

予定されているサンドボックスおよび既存のサンドボックスのリストは、AI事務局が一般に公開する。また、欧州委員会は、AI規制サンドボックスに関する関連情報を含む単一のインターフェースを開発し、利害関係者が以下を行えるようにする予定である：

- AI規制サンドボックスと相互作用すること。
- 各国の管轄当局に問い合わせを行うこと。
- 革新的なAI製品、サービス、ビジネスモデルの適合性について、拘束力のないガイダンスを求めること。

誰がAI規制サンドボックスに参加できるのか？

サンドボックス制度は、AIシステムのプロバイダー（またはプロバイダーになる可能性のある事業者）を対象としているが、ディプロイヤーやその他の関連する第三者と提携して申請を提出することもできる。

中小事業者やスタートアップの参加を奨励するための特定の規定が存在する。この規定には、以下のものが含まれる：

- 中小事業者やスタートアップによるサンドボックスへのアクセスは、通常、無料とすべきこと。
- EU域内に登録事務所または支店を持つ中小事業者およびスタートアップに対する優先的アクセス。
- 中小事業者やスタートアップがAI Actの実施に関するガイダンスやその他の付加価値サービスにアクセスできるようにすべきこと。

責任

AI規制のサンドボックスに参加するプロバイダーおよびプロバイダーとなる可能性のある者（中小事業者やスタートアップを含む）は、サンドボックス内で行われたテストの結果、第三者に与えた損害について責任を負う。ただし、以下の場合、制裁金はプロバイダーとなる可能性のある者には課されない：

- 該当するサンドボックス計画と参加条件を遵守しており、かつ、
- 国の管轄当局が示すガイダンスに（誠実に）従った場合

サンドボックス制度の実施

EU全域での断片化を避けるため、欧州委員会は、AI規制サンドボックスの設置、運用、監督に関する、以下の共通原則を含む詳細な取決めを定める実装法令を採択する予定である：

- 参加資格と選考基準
- サンドボックスの申請、参加、監視、退出、終了の手続き
- 参加者に適用される条件

これらの実装法令は、AI規制サンドボックスが以下のようなものになることを確保することを意図している：

- 公正で透明性のある資格基準を満たしたプロバイダーであれば、誰でも参加できること。
- 広く平等なアクセスを可能にし、参加需要に対応すること。
- 精度、堅牢性、サイバーセキュリティなどの規制学習に関連するAIシステムの側面をテストし説明するためのツール・インフラの開発や、基本的権利や社会全体に対するリスクを軽減するための措置の発展を促進すること。
- AIエコシステム内の関連するアクター（例えば、第三者認証機関や標準化団体、テスト・実験施設、リサーチ・実験ラボ、欧州デジタルイノベーションハブ）の関与を促進し、また、AI規制サンドボックスへの参加がEU全域で一律に認められる（また、同じ法的効果を持つ）ようにすること。

各国管轄当局の義務

各国の管轄当局は、次のことを行わなければならない：

- サンドボックス制度がAI Actの要件に準拠するよう十分なリソースを割り当てること。
- AI Actの要件を満たす方法について、サンドボックス参加者にガイダンスを提供すること。
- サンドボックスで実施された活動、結果、学習成果を詳述した終了報告書を参加者に提供し、後に適合性評価プロセスまたは関連する市場監視活動を通じてAI Actの遵守を証明するために使用できるようにすること。
- ベストプラクティス、インシデント、得られた知見を含む年次報告書を、AI事務局と欧州AI委員会（詳細は第8章参照）に提出すること。

各国の管轄当局は、基本的権利や健康・安全に対する重大なリスクに対処する必要がある場合、サンドボックス内で実施される活動を一時

停止または終了する能力を含め、サンドボックス活動に関する監督権限を保持する。

サンドボックス内での個人データの処理

他の目的のために合法的に収集された個人データは、AI Actに規定された様々な条件を遵守することを前提に（関連する処理活動が許可されるためには、そのすべてが満たされなければならない）、AI規制サンドボックスで使用することができる。主な条件には以下が含まれる：

- サンドボックスに導入されるAIシステムは、重要な公共の利益（公衆衛生、エネルギーの持続可能性、重要インフラの安全性など）を守ることを目的としていなければならない。
- 個人データの利用は必要なものでなければならず、匿名化されたデータや合成データで代替することはできない。
- 個人データは分離され保護された環境で取り扱われ、適切な技術的および組織的措置に従わなければならない。
- AIシステムのトレーニング、テスト、検証の過程と根拠に関する記述を、テスト結果とともに保持しなければならない。

AIシステムの実環境でのテスト

AI Actはまた、一定の条件のもとで、*「実環境(real-world conditions)」*でのAIシステムのテストも可能にしている。

AI Actは、*「実環境テスト(testing in real-world conditions)」*を以下のように定義している：
「実験室やその他の模擬環境以外の実環境の下で、AIシステムをその意図する目的のために一時的に実施する試験で、信頼性が高く健全なデータを収集し、AIシステムが［AI Actの］要件に適合していることを評価・検証することを目的とするもの」

このような実環境テストは、AI Actの関連要件が遵守されている限り、当該AIシステムの市場投入やサービス開始には該当しない（詳細は第2章参照）。

AI Actは主に、AI規制サンドボックスの外で実施される、高リスクAIシステムの実環境テストにフォーカスしている。しかし、同法は、国の管轄当局の監督の下、（高リスクか否かにかかわらない）AIシステムが、AI規制サンドボックスの枠内で実環境テストの対象となる可能性も想定している。

どちらのシナリオでも、実環境テストは、AI Actに定められた様々な条件（テストが許可されるためには、そのすべてが満たされなければならないが、サンドボックス内でテストが実施される場合は、より柔軟性がある）に従わなければならない。主な条件は以下を含む：

- 提案されている実環境テストが、関連する市場監視当局によって承認され、高リスクAIシステムのEUデータベースに登録されていること。
- 試験を実施するプロバイダーが、EUで設立されていること（またはEUにおける法定代理人を任命していること）。
- テストが最大6ヶ月間まで（6ヶ月間延長され得る）に限定されていること（ただし、サンドボックス環境での実環境テストの場合はこの要件は免除され得る）。
- 実環境テストの参加者が適切に保護されていること - インフォームド・コンセントがなされていること、悪影響が可逆的（あるいは軽微）であること、いつでも参加を撤回できること。
- 市場監視当局が、実環境テストの実施について抜打ち検査を行うことができること。

プロバイダーおよびプロバイダーとなる可能性のある者は、実環境テストの過程で生じたいかなる損害に対しても責任を負う。

サンドボックスや実環境テストへの参加に関して、*「フォーラム・ショッピング」*のリスクはあるか？

AI Actは、EU全域でAI規制のサンドボックスや実環境テストに関する制度を調和させることを目指しているが、業界の人々や利害関係者は、

間違いなくその発展を注視し、業界に最も優しいアプローチ（サンドボックスや実環境テストへの参加に関連する責任がどのように決定されるか、など）をとっていると思われる法域のサンドボックスや実環境テストに参加することを選択するだろう。

執行とガバナンス

ポイント

- AI Actは、市販後のモニタリング、報告、情報共有プロセスを導入している。
- ほとんどの義務は、高リスクAIシステムを提供するプロバイダーに課せられ、そのプロバイダーは、市販後のモニタリングシステムと重大インシデントを報告するための手順を導入しなければならない。
- 重大インシデントの報告義務は、ディプロイヤーにも適用されることがある。
- インシデント発生直後の報告が求められることがある。
- インシデントが発生した加盟国の市場監視当局に報告する必要があるため、複数の当局への報告が必要となる場合がある。
- 執行には多方面のアプローチがある。
  - EUデータ保護監督機関は、EUの機関等に対する指揮を行う。
  - 欧州委員会は、汎用目的AIモデルのプロバイダーへの対応を行う。
  - その他については、各加盟国の管轄当局が対応する責任を負う。
- 制裁は、違反のあった規定の重大性に応じて段階的に行われる。
- 影響を受けた人は、個別の意思決定について説明を受ける権利を有する。

To doリスト

☑ 高リスクAIシステムのプロバイダーは、以下を行うべきである：

- 2026年2月2日までに採択される欧州委員会の市販後モニタリング計画のテンプレートを注視する。
- 市販後モニタリング計画を作成し、実施する。
- すでに既存の市販後モニタリング義務の対象となっている場合、または規制対象の金融サービスのプロバイダーである場合は、AI Act上の義務をこれらのシステムに統合できるかどうかを検討する。

☑ 高リスクAIシステムのプロバイダーは、以下を行うべきである：

- すでに他の同等の義務を負っているかどうかを検討し、もしそうであれば、二重の報告義務があるかどうかを確認する。
- 品質マネジメントシステムに重大インシデント報告手順が含まれていることを確認する。
- これらの手順が、重大インシデントの性質（死亡、健康への重大な危害、基本的権利の侵害など）およびインシデントが広範囲に及んでいるかを確認するものであることを確保する。
- 報告先を明確にする。

☑ リスクの高いシステムのディプロイヤーは、次のことを行うべきである：

- 必要に応じて報告できるよう、スタンバイ手順を策定する。

To doリスト

- [ ] プロバイダーおよびディベロッパーは、以下を行うべきである：
  - 2025年8月2日までに予定されている欧州委員会のガイダンスを確認する。
  - ガイダンスは再評価が行われる予定であるため、検討を継続する。
- [ ] 高リスクでないAIシステムのオペレーターは、以下を行うべきである：
  - 既存の製品安全に関する法令をすべて遵守していることを確認する。
- [ ] 汎用目的AIモデルのプロバイダーは、以下を行うべきである：
  - 欧州委員会による執行のアレンジに関する実装法令を注視し、それに関する協議への対応を検討する。
- [ ] AIのバリューチェーンに含まれるすべての組織は、以下を行うべきである：
  - 加盟国レベルで採択された執行に関するルールを注視し、協議への対応を検討する。
  - AIシステムがリスクをもたらすと考える十分な理由がある場合、市場監視当局と協力することが求められていることに留意する。
  - トレーニング、検証、テスト用データセットおよびソースコードの開示が必要となる可能性があることに留意する。
- [ ] 高リスクAIシステムのディプロイヤーは、以下を行うべきである：
  - AIの意思決定プロセスについて、明確かつ意味のある説明ができるようにする。

概要

AI Actは、AIシステムの事前要件と事後監視・執行の両方の実施と監督を規定するガバナンスの枠組みを概説している。前者については前章までで述べた。後者については、ガバナンス構造の説明とともに本章の主題とする。

執行体制は、製品の安全性に対するリスクと、基本的権利に対するリスクという2種類のリスクに対処する。前者について、AI Actは、既存の製品の安全に関する法制を基礎としており、そのほとんどが各国の市場監視当局によって執行される。基本的権利に対するリスクが特定された場合、市場監視当局は、関連する国の公的機関または基本的権利の保護団体に通知し、全面的に協力しなければならない。

AI Actのリスクベースアプローチに従い、様々なリスクを持つAIシステムに適用される異なる規制から成る多層的な執行構造が定められている。高リスクAIシステムについて、AI Actは、第一に市販後のモニタリング義務、第二に重大インシデントの報告義務を定めている。重大インシデントの報告義務については、ディプロイヤーにも適用される場合があるため、ディプロイヤーも認識しておく必要がある。

市場監視当局は、オペレーターに対し、AIシステムがリスクをもたらさないことを保証するためにあらゆる適切な措置を講じるよう求めることができ、必要に応じて、製品やAIシステムの市場からの撤退を要求することができる。また、AI Actの条項が遵守されない場合、極めて高額な制裁金を課すこともできる。

汎用目的AIモデルについては、欧州委員会がAI Act上の義務を監督・執行する独占的権限を有する。

AI Actは、ガバナンス構造として、EUレベル（AI事務局、欧州AI委員会、諮問フォーラム、科学パネル）と加盟国レベル（届出当局、市場監視当局）の双方に新たな機関組織を設置することを定めており、それぞれの役割と権限を概説している。AI Actの効果的な実施と執行のために、これらの機関の連携が鍵となる。

本章で扱うトピックは以下のとおりである：

- 市販後の義務
- 市場監視当局
- 執行手続き
- 基本的権利を保護する当局
- 汎用目的AIモデル
- 罰則
- 第三者に対する救済措置
- ガバナンス

市販後の義務

高リスクAIシステムの市販後モニタリングシステム

AIシステムには適応する能力があり、市場への投入後も学習を続けるため、市場投入後もパフォーマンスのモニタリングを継続することが重要である。前文第155項では、市場投入後のモニタリングシステムの目的は、高リスクAIシステムのプロバイダーが、システムのコンプライアンスと改善を継続的に確保するため、システムの利用による経験を考慮できるようにすることであると説明されている。

高リスクAIシステムのプロバイダーは、システムを市場に投入する前に作成する技術文書に、市販後モニタリング計画を含めなければならない（第72条第3項および第11条第1項）。この計画は、2026年2月2日までに採択される欧州委員会のテンプレートに沿ったものでなければならない。市販後の義務は、是正／予防措置を直ちに実施する必要性を特定するものでなければならない（第3条第25号）。

第72条は、市販後モニタリングシステム（およびシステムに関する文書）は、AI技術の性質とシステムのリスクに見合ったものでなければならないと定めている。このシステムは、プロバイダーが継続的なコンプライアンスを評価できるよう、AIシステムの耐用期間を通じて、関連データを積極的かつ体系的に収集、文書化、分析するものでなければならない。データは、デ

ィプロイヤーから提供されることもあれば、その他の者から提供されることもある（ただし、法執行当局であるディプロイヤーによる機微な運用データは除外される）。関連する場合、システムは、デバイスやソフトウェアを含む他のAIシステムとの相互作用の分析も含むべきである。

すでに市販後モニタリングシステムを導入している特定の種類の高リスクAIシステムのプロバイダーは、同等の保護レベルを満たしているのであれば、AI Actに基づく義務を既存のシステムに統合することができる。これは、付属書IのセクションAに記載されているEU整合法令の対象となる高リスクAIシステムの場合である（すなわち、特定の機械、玩具、医療機器など）。また、内部ガバナンス、アレンジメント、またはプロセスに関して、EUの金融サービスに関する法令上の要件の対象となる金融機関が、附属書IIIの第5項（具体的には、信用度の評価、または生命・医療保険に関するリスク評価と価格設定）に記載された高リスクAIシステムを市場に投入する場合も同様である（第72条第4項）。

高リスクAIシステムに関する重大インシデント情報の報告

高リスクAIシステムのプロバイダーは、*「重大インシデント(serious incidents)」*を報告しなければならず、プロバイダーの品質管理システムには、これに関する手順が含まれていなければならない（第17条第1項(i)）。通常、高リスクAIシステムのディプロイヤーは、重大インシデントをプロバイダーに報告しなければならない。しかし、ディプロイヤーがプロバイダーに連絡できない場合には、第73条の重大インシデント報告義務がディプロイヤーに直接適用される（第26条第5項）。従って、ディプロイヤーもこれらの規定に留意すべきである。欧州委員会は、2025年8月2日までに、インシデント報告に関するプロバイダー向けのガイダンスを発表することになっており、これは定期的に見直されることになっている。

重大インシデントは、第3条第49号で定義されており、AIシステムの事故や誤作動のうち、直接的または間接的に以下を及ぼすものを意味する：

- 死亡、または人の健康への重大な危害
- 重要インフラの管理・運営に深刻かつ不可逆的な混乱をもたらす
- 基本的権利を保護するEU法に違反する
- 財産や環境に重大な損害を与える

重大インシデントは、以下に定める期限内に報告されなければならない。必要であれば、プロバイダーまたはディプロイヤーは、まず最初の報告書を提出し、それを後に完成させることもできる（第73条第5項）。

状況	期限
広範囲に及ぶ違反、または 重要インフラに関わる重大インシデント	直ちに （重大インシデントを認識してから 2 日以内）
人の死亡	重大インシデントを認識してから 10 日以内、 または 重大インシデントと AI システムとの間の因果関係が確認され、または疑われた直後（10 日よりも早い場合）
その他の状況（すなわち、健康への重大な危害、基本的権利の侵害、財産や環境への重大な損害が発生した場合。ただし、これらが広範囲に及んでいる場合を除く。）	重大インシデントを認識してから 15 日以内、 または AI システムと重大インシデントとの間の因果関係またはその合理的な可能性をプロバイダーが確認した直後

報告後、プロバイダーは、リスク評価および是正措置を含む、必要な調査を速やかに実施しなければならない。プロバイダーは、後のインシデント原因の評価に影響を与えるような形でのAIシステムの変更を、管轄当局に報告する前に行ってはならない。

重大インシデントの報告は、インシデントが発生した加盟国の市場監視当局に行わなければならない（第73条第1項）。そのため、重大インシデントが複数の加盟国に影響を及ぼす場合、または複数のセクターに影響を及ぼすため加盟国内に複数の市場監視当局が存在する場合には、複数の報告が求められる。

市場監視当局は、通知を受け取ってから7日以内に適切な措置（製品の回収やリコールを含む）を講じなければならず、また、重大なインシデントが発生した場合には、措置を講じたか否かにかかわらず、直ちに欧州委員会に通知しなければならない（第73条第8, 11項）。

高リスクでないAIシステム

高リスクでない製品に関連するAIシステムは、それにもかかわらず、市場への投入時またはサービス開始時に安全である必要がある。一般製品の安全に関するEU規則（Regulation (EU) 2023/988）および製品の市場監視とコンプライアンスに関するEU規則（Regulation (EU) 2019/1020）は、AI Actが適用されるすべてのAIシステムに適用されるが、これら2つの規則は、高リスクでない製品に関するセーフティネットを提供している（前文第166項および第74条第1項）。

Regulation (EU) 2019/1020は、製品に第3条第19号（下記の定義参照）のリスクがあると信じるに足る理由がある場合に、すべてのオペレーターが関連市場監視当局に通知することを義務付けている。AI Actは、第3条第19号のリスクのリストに、人々の基本的権利に対するリスクを追加した（第79条第1項）。

> *「リスクを伴う製品(product presenting a risk)」*とは、意図された目的との関連で、または当該製品の通常のもしくは合理的に予見可能な使用条件（使用期間、該当する場合、使用開始、設置および保守の要件を含む）の下で、合理的かつ許容可能な範囲を超えて、人々の健康および安全、職場における健康および安全、消費者の保護、環境、公共の安全、および適用されるEU整合法令によって保護されるその他の公共の利益に悪影響を及ぼす可能性を有する製品を意味する。

市場監視当局

AI Actの執行においては、ローカルでの対応が必要になることが多いため、加盟国が重要な役割を果たす。加盟国は、それぞれ少なくとも1つの市場監視当局を指定しなければならず、当局が複数指定された場合は、これらの当局のうち1つが、市民向けならびに加盟国およびEUレベルの他の関連当局向けの一元的窓口として設定されなければならない。加盟国は欧州委員会に一元的窓口を通知し、欧州委員会はそのリストを一般に公開する（前文第153項および第70条第1, 2項）。加盟国は、2025年8月2日までにこれらの規定を遵守しなければならない（第113条(b)）。

どのような主体が市場監視当局に指定されるのか？

加盟国は、この点について一定の裁量を有しており、AI Actの施行に特化した新たな機関を設置するか、付属書Iのセクション Aに列挙されたEU整合法令またはEU Actで規制される金融機関や信用機関を規制する既存機関の枠組みの中にAI Actの要件を統合することができる（第74条第3, 6, 7項）。ただし、バイオメトリクス、法執行、移民、亡命、国境管理、司法行政の分野における高リスクAIシステムについては、加盟国は、Regulation (EU) 2016/679により設立された国内データ保護局、またはDirective (EU) 2016/680に基づき指定された監督当局のいずれかを指定しなければならない（第74条第8項）。

AIシステムが、付属書Iのセクション Aに列挙さ

れたEU整合法令の適用をすでに受けている製品に関するものであり、かつ、当該法令が、AI Actと同等のレベルの保護を確保し、AI Actと同一の目的を有する手続をすでに規定している場合には、第79条から第83条に定める国内レベルの実施手続に代えて、分野別の手続が適用されるものとする（下記「執行手続き」を参照）。

この場合、プロバイダーに重大インシデントにかかる二重の報告は要求されず、プロバイダーは当該他の法律に基づいて報告する（第73条第9項および同条第10項）。これらの例外は、具体的には以下の場合に適用される：

- 付属書IIIに掲げる種類の高リスクAIシステムで、プロバイダーが、AI Actに規定されたものと同等の報告義務を定めるEU法の適用を受けるもの。ここでの同等性は、例えば、AI Actに基づく義務と同等と評価し得る独立のインシデント報告義務を含むサイバーセキュリティ規制の対象となる重要インフラに認められる可能性がある。ただし、他のEU法に基づく報告義務がAI Actに基づく報告義務と同等とみなされるかどうかが明らかでないケースもある。

- 医療機器に関するRegulation (EU) 2017/745および体外診断用医療機器に関するRegulation (EU) 2017/746の対象となる、機器の安全コンポーネントである、または機器そのものである高リスクAIシステム。これらの規則は報告義務を定めており、(a)患者、使用者またはその他の人の死亡、(b)患者、使用者またはその他の人の健康状態の一時的または恒久的な深刻な悪化、(c)公衆衛生上の深刻な脅威を伴う重大インシデントが発生した場合、管轄当局に報告しなければならないとされている。

しかし、いずれの場合も、インシデントが基本的権利の侵害に関連するものであれば、AI Actに基づき届け出なければならず、関連する市場監視当局は、国内の基本権当局に通知しなければならない。

EUの機関、エージェンシー、事務局、団体（司法的立場で行動する欧州司法裁判所を除く）が使用するAIシステムについては、EUデータ保護監督機関が市場監視当局となる（第74条第9項）。

市場監視当局の権限

市場監視当局は、AI Actで認められたさらなる権限に加え、Regulation (EU) 2019/1020で定められたすべての広範な執行権限を有する。例として以下の権限がある：

- オペレーターに関連書類、データ、コンプライアンスに関する情報を開示させる。AI Act上、高リスクAIシステムのプロバイダーはさらに以下の開示を強制される可能性がある：

  – 高リスクAIシステムの開発のために使用された学習、検証および試験用データセット。適切な場合、セキュリティセーフガードを講じた上で、アプリケーション・プログラミング・インターフェース（API）または遠隔アクセスを可能にするその他の関連する技術的手段・ツールを通じての開示を含む（第74条第12項）。

  – プロバイダーから提供されたデータおよび文書に基づく試験または監査手続きおよび検証が尽くされた場合または不十分であると証明された場合で、高リスクAIシステムの第3章第2節に規定された要件への適合性を評価するために必要な場合には、ソースコード（第74条第13項）。

- 抜打ちの立入検査とテスト購入（第74条第5項）。

- 調査の実施（高リスクAIシステムが2つ以上の加盟国にまたがって深刻なリスクをもたらすことが判明した場合、欧州委員会と協力して実施される）（第74条第11項）。

- 形式的な不遵守（第83条）およびリスク排除（第79条から第82条）の観点で、不遵守を終了させるために適切な行動をとることのオペレーターへの要求。

- オペレーターが是正措置を講じない場合、または違反が継続する場合、回収およびリコールを含む適切な措置を講じること（第73条第8項、第97条から第83条）。

- 罰則を課すこと（第99条から第101条）。

また、市場監視当局は、実環境での試験がAI Actに準拠していることを保証しなければならない（第7章参照）。当局は、プロバイダーまたはディプロイヤーに対し、試験の修正、中止または終了を要求する権限を有する（第76条第3項）。

機密情報の取扱い

市場監視当局が入手したいかなる情報または文書も、第78条に定める守秘義務に従って取り扱われるものとする。第78条の規定はまた、欧州委員会、基本的権利を保護する当局、AI Actの適用に関与する自然人および法人にも適用される。これらの者は、機密情報および営業秘密を保護するだけでなく、知的財産権およびソースコードの権利、公共および国家安全保障上の利益、ならびに国家機密を保護する形で、その任務を遂行しなければならない。

これらの規定は、2025年8月2日から適用される。

執行手続き

すでに述べたように、以下の手続きは、AI Actと同等レベルの保護を提供し、同じ目的を持つ調和法令がすでに存在する場合には適用されない。

リスクをもたらすAIシステム（第79条、第81条）

市場監視当局は、AIシステムがリスク（上記の定義参照）をもたらすと考える十分な理由がある場合、AIシステムがAI Actに準拠しているかどうかの評価を実施しなければならない。

適合しない場合、市場監視当局は、不当に遅延することなく関連するオペレーターに通知し、AIシステムを適合させるためのあらゆる適切な是正措置をとるか、AIシステムを市場から回収またはリコールするよう要求しなければならない。市場監視当局は、遵守するための期限を明示しなければならないが、15営業日を超えてはならない。

オペレーターが指定された期間内に適切な是正措置を講じない場合、市場監視当局は、当該AIシステムがその国内市場で入手可能になることもしくはサービス提供されることを禁止・制限し、または当該市場からの製品もしくはスタンドアロンAIシステムの回収もしくはリコールを行うためのあらゆる適切な暫定措置を講じなければならない。市場監視当局は、その決定の根拠をオペレーターに通知しなければならない。

不遵守が自国の領域に限定されない場合、市場監視当局は、欧州委員会および他の加盟国に対し、不当な遅滞なく、評価の結果、オペレーターに求めた措置、およびオペレーターが遵守しなかった場合に講じた暫定措置について、通知しなければならない。

暫定措置は、加盟国の市場監視当局および欧州委員会のいずれからも3ヶ月以内（第5条で言及されている禁止事項の不遵守の場合は30日以内に短縮）に異議が出なかった場合、正当なものとみなされる。ただし、異議が出た場合には、欧州委員会は、市場監視当局およびオペレーターと協議し、6ヶ月以内（第5条に該当する場合は60日以内）に、暫定措置が正当であるかどうかを決定する。正当である場合、すべての加盟国は、当該AIシステムに関して、市場からの回収を要求するなど、適切な制限措置を講じることを確保しなければならない。正当であるとされなかった場合、暫定措置は撤回される。

これらの規定は、聴聞を受ける権利を含むRegulation (EU) 2019/1020の第18条に定めるオペレーターの手続き上の権利を損なうものではない。

プロバイダーが高リスクでないと分類したAIシステム（第80条）

市場監視当局は、第6条第3項によりプロバイダーが高リスクでないと分類したAIシステムが実は高リスクであると考える十分な理由がある場合、評価を実施しなければならない。

従うべき手続きは上記のとおりだが、第80条では特に、関連するプロバイダーに制裁金を科すことができると定める。

第80条の適用を監視する権限を行使する際、市場監視当局は、高リスクAIシステムのEUデータベースに保存されている情報を考慮することができる（下記「EUレベルでのガバナンス：欧州委員会の役割」を参照）。

リスクをもたらす適合AIシステム（第82条）

市場監視当局は、高リスクAIシステムがAI Actを遵守しているものの、人の健康もしくは安全、基本的権利、またはその他の公益保護の側面にリスクをもたらしていると判断した場合、該当するオペレーターに対し、そのようなリスクをなくすようあらゆる適切な措置を講じるよう求めるものとする。

形式上の不履行（第83条）

市場監視当局が、例えばCEマークが本来貼付されるべき場所に貼付されていない、指定代理人が任命されていない、技術文書が入手できないなどの事実を発見した場合、当該プロバイダーに対し、所定期間内に是正するよう求めるものとする。

不遵守が続く場合、市場監視当局は、高リスクAIシステムの市販を制限もしくは禁止する、または遅滞なく市場からの回収もしくはリコールを確保するための適切かつ相応の措置を講じなければならない。

基本的権利を保護する当局

市場監視当局を特定することに加え、各加盟国は、2024年11月2日までに、付属書IIIで言及されている高リスクAIシステムの使用に関して、差別を受けない権利を含む基本的権利を保護するEU法上の義務を監督・執行する公的機関または団体を特定し、欧州委員会に通知しなければならない。

市場監視当局が基本的権利に対するリスクを特定した場合、同権利の保護を監督する関連の国家公的機関に通知しなければならない。

これらの機関は、その任務を効果的に遂行するためにAI Actに基づき作成または維持されている文書へのアクセスが必要な場合、当該文書の提出を要求し、アクセスする権限を有する。また、関連する期間は、加盟国の市場監視当局に対して、かかる要求について通知し、文書が不十分であることが判明した場合には、技術的手段を用いて高リスクAIシステムのテストを実施するよう要請することができる（第77条）。

汎用目的AIモデル

欧州委員会は、汎用目的AIモデルのプロバイダーに対する義務を監督・執行する唯一の機関である。その所以は、EUレベルでの集中的な専門知識と相乗効果の恩恵に与るためである（第88条）。しかし、実際には、AI事務局（下記「ガバナンス」を参照）が、欧州委員会の組織的権限および加盟国―欧州連合間の権限分担に影響を与えないことを条件に、汎用目的AIモデルに関するAI Actの効果的な実施を監視するために必要なすべての措置を実施する。

AI事務局は、自身の監視活動の結果を踏まえ、あるいは市場監視当局からの要請を受けて、独自のイニシアティブで汎用目的AIモデルのプロバイダーによる規制違反の可能性を調査することができる。

同局は、モデルと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、汎用目的AIモデルに基づくAIシステムに対して、市場監視当局としての権限を有する。

汎用目的AIシステムが、ディプロイヤーにより少なくとも1つの高リスクの目的で使用され得るものであるときには、市場監視当局は、同システムがAI Actに準拠していないと判断した場合、AI事務局と協力してコンプライアンス評価を実施しなければならない。

市場監視当局は、自身でその情報にアクセスできない場合（かつ、その結果、高リスクAIシステムに関する調査を完遂できない場合）、AI事務局に対して汎用目的AIモデルに関する情報の提供を要請することができる（第75条）。

罰則

自然人もしくは法人、公的機関、またはEUもしくは加盟国の機関の別にかかわらず、AI Actを遵守しない者は、制裁を受ける可能性がある。AI Actの罰則規定は、GDPRの罰則規定（最高2,000万ユーロまたは全世界年間売上高の4%）をも上回る。制裁金の上限は、立法過程を通じて見直されたが、最終的には3,500万ユーロまたは全世界年間売上高の7%に設定された。

制裁金は、各国当局、EUデータ保護監督機関、または欧州委員会が課すことができる。EUデータ保護監督機関は、EUの機関、エージェンシー、団体に制裁金を課すことができる。欧州委員会は、汎用目的AIモデルのプロバイダーに制裁金を課すことができる。各国当局は、その他のオペレーターに対して制裁金を課すことができる。

AI Actは、以下のように罰則を段階的に設けている。

違反の根拠	EU機関	その他のすべての主体
	EUデータ保護監督機関による罰則	各国当局が課す罰則（GPAIモデルの場合には、欧州委員会が課す）
		制裁対象者が事業者である場合、罰則の上限は、%ベースまたは金額ベースの値のいずれか高い方となる。 中小事業者の場合、いずれか低い方が上限となる。 その他の制裁対象者については、指定された金額ベースの値が上限となる。
第三者認証機関または各国管轄当局に対し、不正確、不完全、または誤解を招く情報を提供	≤€750,000 （第100条第3項）	≤前年の全世界年間売上高の1% または ≤€7,500,000 （第99条第5項）
高リスクAIシステムに関する義務違反		≤前年の全世界年間売上高の3% または ≤€15,000,000 （高リスクAIシステムについて、第99条第4項、汎用目的AIモデルについて、第101条第1項）
汎用目的AIモデルのプロバイダーに関する義務違反		
禁止されるAIプラクティスに関する義務違反	≤€1,500,000 （第100条第2項）	≤前年の全世界年間売上高の7% または ≤€35,000,000 （第99条第3項）

興味深いことに、第4条のAIリテラシー義務を遵守しなかった場合の罰則は用意されていないようである。

国家当局による罰則および制裁金

効果的、比例的、かつ抑止的な制裁措置を定めることは、加盟国の責任である。これらの措置には、金銭的および非金銭的な措置や警告が含まれる。これらの措置は、適用開始日までに欧州委員会に通知されなければならない（第99条第1 ,2項）。

罰則は、ケースバイケースで課される。管轄の国家当局は、違反の性質、重大性、継続性、その結果、およびプロバイダーの規模を考慮して、特定のケースにおけるすべての関連する状況を考慮すべきである（第99条第7項）。

加盟国レベルでの執行は、効果的な司法救済を含む、適切な手続き上の保護措置の対象となる必要がある。

EUの機関、団体、事務所、エージェンシーに対する制裁金

EUデータ保護監督機関は、EUの機関、エージェンシーおよび団体に制裁金を課す権限を有する。制裁金に関する決定を下す前に、EUデータ保護監督機関は、予備的な調査結果を対象機関に伝え、意見聴取の機会を与えなければならない。制裁金は、対象機関の効果的な運営に影響を及ぼすものではあってはならず、制裁金賦課により徴収された資金は、EUの一般予算に組み込まれる。

汎用目的AIモデルのプロバイダーに対する制裁金

欧州委員会は、汎用目的AIモデルのプロバイダーによる違反に対して制裁金を課すことができる（第101条）。2025年8月2日から適用される第12章の罰則および制裁金に関する他の規定とは異なり、第101条は2026年8月2日まで適用されない。

欧州委員会は、手続きに関するアレンジメントや手続き上の保護措置の詳細を盛り込んだ実装法令を公表する予定である。

欧州委員会は、固定額または定期的に発生する制裁金の支払いを課す場合、違反の性質、重大性、継続性、ならびに比例原則および妥当性の原則を十分に考慮すべきである。制裁金に関する決定を採択する前に、欧州委員会は、その予備的な見解を汎用目的AIモデルのプロバイダーに通知し、意見聴取の機会を与えるべきである。制裁金の賦課は、欧州司法裁判所における司法審査を含む、適切な手続き上の保護措置の対象となる必要がある。欧州司法裁判所は、課された罰金の取消し、減額または増額をすることができる。

第三者に対する救済措置

市場監視当局への苦情申立て（第85条）

EU法および加盟国の法令はすでに、AIシステムの使用によって権利と自由が悪影響を受ける自然人および法人に対して、いくつかの効果的な救済手段を提供している。それにもかかわらず、AI Actは新たな苦情処理メカニズムを導入した。同法は、自然人・法人を問わず、同法違反があったと信じるに足る根拠がある場合、管轄の市場監視当局に苦情を申し立てることができると定めている。

比較：GDPRの下では、データ主体は、自身に関する個人データの処理がGDPR上の権利に違反していると考える場合、違反の疑いについて監督当局に苦情を申し立てる権利を有する。

対照的に、AI Actに基づく苦情は、苦情申立人の権利侵害だけでなく、同法全体の遵守に関わることもある。さらに、GDPRの下では、救済措置はデータ主体のみが申し立てることができるが、AI Actの下では、法人も苦情を申し立てることができる。

個人の意思決定に関する説明を受ける権利（第86条）

AI Act上、影響を受ける者は、高リスクAIシステム（重要インフラシステムを除く）による決定について、ディプロイヤーから*「明確かつ意味のある(clear and meaningful)」*説明を受ける権利を有する。この説明は、使用された意思決定手順と、AIシステムによる決定の主な要素を明確にしなければならない（第86条）。

この権利は以下の場合に行使できる：

- ディプロイヤーの決定が、主に高リスクAIシステムのアウトプットに基づいている場合。
- その決定が、影響を受ける者に対し、法的な効果、または類似の重大な効果を及ぼし、その者の健康、安全、または基本的権利に悪影響を及ぼす場合。

比較：AI Actに基づく説明を受ける権利は、自動化された意思決定プロセスに関するGDPRに基づく管理者の義務（GDPR第22条）と整合する。GDPRの下、管理者は、データ主体に対し、処理のロジックおよび処理結果の重要性に関する意味のある情報を提供しなければならない。

AI Act第86条は、GDPRに基づくデータ主体の説明を受ける権利を補完するものである。同法は、意思決定におけるAIシステムの役割を説明することをディプロイヤーに対して要求している点で、AIにより特化している。さらに、AI Actは、この権利を、法人を含むすべての影響を受ける者に付与している。AI Act上同条を執行する権限を有する当局がどこであるかにかかわらず、個人データの処理を伴う自動的な意思決定に関しては、GDPR上の各国データ保護当局は、依然として管理者の情報提供義務を執行する権限を有する当局である。

内部告発者の保護（第87条）

AI Act違反の通報には、EU法違反を通報する者の保護に関するDirective (EU) 2019/1937が適用される。

川下プロバイダーの苦情申立て（第89条）

AI Actに基づき、川下のプロバイダー（汎用目的AIシステムのディプロイヤー）は、同法に定められたルールに違反する可能性について苦情を申し立てることができる。

苦情は、AI事務局に対して申し立てることができ、十分な根拠のあるものでなければならず、少なくとも以下を含む必要がある：

- 苦情の対象となった汎用目的AIモデルのプロバイダーの詳細とその連絡先
- 違反した条項および関連する事実の説明
- 違反があったと申立人が考える理由
- 申立てをする川下のプロバイダーが関連性があると考えるその他の情報（適切な場合、自らのイニシアティブで収集した情報を含む）

川下のプロバイダーによるこのような苦情申立ては、AI事務局がAI Actの執行を効果的に監督することを可能にする。

ガバナンス

ガバナンス構造は、AI Actの適用を調整・支援するために定められている。その目的は、EUレベルと加盟国レベルの両方で執行能力を構築し、利害関係者間の関係を調和させ、信頼できる建設的な協力を確保することである。

EUレベルでのガバナンス：欧州委員会の役割

欧州委員会は、AI Actによって、委任法令の策定と実施、ガイドラインの策定と公表、基準とベストプラクティスの設定、同法を効果的に実施するための拘束力のある決定など、多くのタスクを課せられている。実際には、これらの任務は、欧州委員会を支援する役割を担うAI事務局（通信ネットワーク・コンテンツ・技術総局の行政機構の一部）が遂行する。

欧州委員会が加盟国と協力して行わなければならない業務のひとつが、AI Act第8章に定められている。欧州委員会は、第6条第2項で言及されている高リスクAIシステムおよび第6条第3項に従って高リスクとはみなされないAIシステムに関するEUデータベースを構築し、維持しなければならない。データベースには以下が含まれる：

- プロバイダーまたは指定代理人がEUデータベースに入力した、付属書VIIIのセクションAおよびBに掲げられるデータ
- 公的機関、エージェンシー、団体であるディプロイヤー、またはこれらの機関の代理として行動するディプロイヤーがEUデータベースに入力した、付属書VIIIのセクションCに掲げられるデータ

これらのデータは一般に公開される（法執行、移民、亡命、国境管理分野のAIシステムに関するデータを除く）。

AI Actによって設立された超国家機関

AI 事務局の役割	アクション
AI 事務局は、2024 年 1 月 24 日の欧州委員会の決定（C/2024/1459）によって設立された。 AI 事務局の機能は、汎用目的 AI モデルを含む AI モデルの進歩を監督すること、科学界と交流すること、調査やテスト、法執行において重要な役割を果たすこと、そしてグローバルな使命を担うことである（決定書 5）。 AI 事務局は、独立した専門家に評価を代行させることができる。 AI 事務局は、潜在的な利益相反を管理・防止するためのシステムと手続きを確立し、AI 分野における EU の専門知識と能力を進展させなければならない。 AI 事務局は、汎用目的 AI システムの監視と管理の役割を担っている（第 75 条）。	監視と実施：汎用目的 AI モデルのプロバイダーに対する義務の遵守と実施を監視する。 調査：汎用目的 AI モデルのプロバイダーへの文書・情報提出要求、評価・対策要請による違反調査。 リスク管理：リスク軽減や（システミック・リスクが確認された場合、）市場での利用制限や回収、リコールを含む、適切な措置を要請する。 調整と支援：各国当局による AI 規制サンドボックスの設置を支援し、協働と情報共有を促進し、行動規範の作成を奨励・促進する。市場監視当局と欧州委員会の共同調査を調整する。 助言：行動規範、実践規範、ガイドラインに関して、欧州委員会および欧州 AI 委員会に勧告や意見書を提出する。

欧州 AI 委員会の役割	アクション
欧州 AI 委員会は、各加盟国の代表で構成され、AI Act の一貫した効果的な適用について欧州委員会と加盟国に助言し、支援することを任務としている。さらに、欧州 AI 委員会は、ガイドラインと勧告を発行する（第 65 条および第 66 条）。 代表は、3 年の任期で任命され、任期更新は 1 度のみ。代表は、AI に関する専門知識を持ち、国内レベルの調整を促進する権限を持つ公的機関の個人であることが想定される。欧州 AI 委員会の議長は、代表のうちの 1 人が務める。	調整と協力：各国の管轄当局と EU の機関、団体、事務所、エージェンシーおよび関連する EU の専門家グループとネットワークの間の調整、協力を促す。 専門知識の共有：技術や規制に関する専門知識、ベストプラクティス、ガイダンス文書を収集し、共有する。 助言と勧告：特に汎用目的 AI モデルに関するルールの施行に関して、AI Act の実施に関する助言を提供し、（欧州委員会の要請に応じて、または自らの主導で）勧告や意見書を発行する。

欧州 AI 委員会の役割	アクション
欧州 AI 委員会は、2 つの専門常設サブグループを設置しなければならない： 認定機関のための常設サブグループは、第三者認証機関に関連する問題についての協力および情報交換のためのプラットフォームを提供する。 市場監視のための常設サブグループは、AI Act の事務協力グループ（ADCO）として機能する。	調和：管理実務を標準化し、共通基準の開発と共通理解の促進を実施する。 AI に関する市民の理解：AI がもたらす便益およびリスクや、AI に関するセーフガード、権利および義務に関する、リテラシー、市民の理解の向上に努める。 国際協力：AI に関する国際問題に関して欧州委員会に助言を与え、加盟国以外の第三国の管轄当局および国際機関と協力する。

欧州 AI 委員会は、特定の問題を検討する目的で、適宜、その他の常設または臨時のサブグループを設置することができる。

EU データ保護監督機関および AI 事務局は、欧州 AI 委員会の会合にオブザーバーとして出席する。その他の国および EU の当局、機関、専門家または諮問フォーラムの代表者は、ケースバイケースで出席を要請される。

諮問フォーラムの役割	アクション
諮問フォーラムは、AI Act の実施と適用に関して利害関係者の関与を確保するため、設立された（第 67 条）。 メンバーは欧州委員会によって任命され、産業界、スタートアップ、中小事業者、市民社会、AI 分野の専門知識を有する学術界など、利害関係者のバランスを勘案して選出される。 メンバーの任期は 2 年で、最長 4 年延長され得る。メンバーの中から 2 名の共同議長を選出する。議長の任期は 2 年で、任期更新は 1 度のみ。 基本権庁（FRA）、欧州ネットワーク・情報セキュリティ機関（ENISA）、欧州標準化委員会（CEN）、欧州電気標準化委員会（CENELEC）、欧州電気通信標準化機構（ETSI）は、諮問フォーラムの常任メンバーとなる。 諮問フォーラムは、特定の問題を検討するために、必要に応じて常設または臨時のサブグループを設置することができる。 諮問フォーラムは少なくとも年 2 回会合を開き、専門家やその他の利害関係者を会議に招くことができる。	助言と技術的専門知識：欧州 AI 委員会および欧州委員会に助言を提供する。要請に応じて意見、勧告、文書の作成を行う。 相談：欧州委員会は、第 41 条で言及されている標準化要求の作成または共通仕様の起草の際、諮問フォーラムと協議しなければならない。 年次報告書：年次活動報告書を作成・発行する。

独立専門家科学パネルの役割	アクション
科学パネルは、欧州委員会の執行活動を支援するにあたり、科学界を取りまとめるために設立された（第 68 条）。 専門家は、AI に関する科学的または技術的な専門知識に基づいて欧州委員会により選出される。 専門家の人数は、欧州委員会が欧州 AI 委員会と協議の上、必要な専門知識、ジェンダー間の公平性や地理的な代表構成に基づいて決定する。	汎用目的の AI モデルやシステムに関して、AI 事務局による執行をサポートする： • システミック・リスクの可能性について、AI 事務局に警告する。 • 能力を評価するためのツールや方法論を開発する。 • システミック・リスクを含む分類について助言する。 • ツールやテンプレートの開発に貢献する。

科学パネルの任務遂行に必要な情報を提供するため、パネルが欧州委員会に対し、欧州委員会がプロバイダーから文書や情報を取得するよう要請できる仕組みを設けるべきである。

実装法令は、科学パネルとそのメンバーがどのようにアラートを発し、AI 事務局に支援を要請するかを定める。

- 市場監視当局を支援する：市場監視当局の要請に応じて実施。クロスボーダーでの市場監視活動を含む。
- 第 81 条に基づき、EU のセーフガード手続きを支援する。

要求に応じて、加盟国の執行活動を支援する：

- 加盟国は、科学パネルが提供する助言と支援に対して手数料を支払うことを求められる場合がある。
- 第 68 条第 1 項で言及されている実装法令は、手数料と回収可能な費用を規定する。

加盟国レベルのガバナンス：国家管轄当局

AI Actの適用と執行において、加盟国は極めて重要な役割を果たす。EU内および加盟国間での効果的な適用、調和、協働を確保するため、各加盟国は少なくとも1つの認定機関と1つの市場監視当局を指定しなければならない。両者が合わせて国内管轄当局となる。EUの機関、エージェンシー、事務所、団体が使用するAIシステムについては、EUデータ保護監督機関が管轄当局となる。

認定機関の役割	アクション
認定機関は、適合性評価機関の枠組みを確立し、適用する責任を負う（第 28 条）。 認定機関は、基本的人権保護の監督を含め、情報技術、AI、法律などの分野で必要な専門知識を持つ適任の人材を十分な数確保しなければならない。 認定機関は、適合性評価機関との利害の対立を避け、その活動の客観性および公平性を確保しなければならない。特に、適合性評価機関を認定する旨の決定は、適合性評価機関を評価した者が行ってはならない。	手続きの確立と実行：適合性評価機関の評価、指定、認定および監視のために必要な手順を確立し、実施する。これらの手続きは、他の加盟国の認定機関と協力して策定する。 助言と指導：欧州 AI 委員会および欧州委員会からのインプットを考慮し、（また、該当する場合には）他の EU 法上の各国の管轄当局と協議し、AI Act の執行に関するガイダンスおよび助言を提供する。 活動およびサービスに関する制限： • 適合性評価機関が行ういかなる活動もオファーまたは提供してはならない。 • ビジネスまたは競争ベースでコンサルタントサービスを提供してはならない。

市場監視当局の役割	アクション
Regulation (EU) 2019/1020 に従った市場監視と製品のコンプライアンスに関する活動・措置の実施の責任を担う。 各加盟国は、市場監視当局の 1 つを、市民向けならびに加盟国および EU レベルの他の関連当局向けの一元的窓口として指定する。 EU データ保護監督機関は、AI Act に関する EU の機関、エージェンシー、団体に対する市場監視当局として機能する。 法執行、移民、亡命、国境管理、司法、民主主義プロセスに使用されるバイオメトリクスにおける高リスク AI システムの市場監視当局は、強力な調査権限と是正権限を持つべきである。これには、すべての個人データとその任務に必要な情報へのアクセスが含まれる。 加盟国は、市場監視当局と他の関連国家当局との間の調整を促進しなければならない。	市場監視当局のタスクと責務の多くは上記のとおりであるが、それに加えて市場監視当局には以下のタスクと責務が課せられている： • 高リスク AI システムの認可：加盟国は、公共の安全、健康、環境、重要なインフラといった例外的な理由から、適合性評価が行われるまでの間、一時的に特定の高リスク AI システムの市場投入や自国内での稼働を許可することができる（第 46 条）。 • 年次報告：欧州委員会および各国競争当局に対し、監視活動および禁止されたプラクティスについて、(i)競争法の潜在的な適用可能性が確認された情報、(ii)禁止されたプラクティスの実施、(iii)これらのプラクティスに関して取られた措置、を含む報告を行う。 • 助言と指導：欧州 AI 委員会および欧州委員会からのインプットを考慮し、（また、該当する場合には）他の EU 法上の各国の管轄当局と協議し、AI Act の執行に関するガイダンスおよび助言を提供する。

参照条文等

ガバナンス：第7章	前文第148-154, 163,179項
EUデータベース：第8章	前文第131項
執行：第9, 12章	前文第162-164, 168-172項

AI Act：今後の展望

ポイント

- AI Actは、2024年8月1日に発効。
- ほとんどの条項は、2026年8月2日から適用されることになっている。その他の条項は、発効日から6ヶ月から36ヶ月かけて段階的に適用されることになっている。
- 欧州委員会は、委任法令および実装法令、ガイドライン、行動規範、基準を策定する。これらのイニシアチブは、AI Actに関連する実践的な指針、倫理原則、技術仕様を提供することを目的としており、同法の効果的な実施を確保することを目的としている。
- 2024年7月、欧州委員会はまた、AI責任指令案（AI Liability Directive）の更新版を、欧州議会および欧州理事会の双方に送付し、検討を求めた。
- Bird & BirdのAI分野のエキスパートは、AI法に関して見込まれる今後のイニシアチブを注視し、さまざまなプロセスや要求への対応をサポートする。

To doリスト

- [ ] AIシステムを取り扱うすべての関係者は、本章で概説する立法上または非立法上のイニシアチブの展開を、能動的に監視すべきである。

AI Act: 今後の展望

本章では、AI Actの適用時期と、同規則の下で見込まれる今後の取組みについて概観する。EUの諸機関は、AI Actは、技術の進歩に合わせて、二次立法やその他のイニシアティブによって継続的に補足される*「生きた規制(living regulation)」*の新しい形態であると考えている。今後数ヶ月の間に、AI Actは様々な委任法令や実装法令、ガイダンス文書、行動規範、実践規範、標準化要請の採択を想定している。これらの取組みは、同規則の効果的な実施を確保することを目的として、同法に関する実践的な指針、倫理原則、技術仕様を提供することを目的としている。

これらの文書に定められた要件は、AI Actの効果的な実施と、その義務を遵守する関係者に求められる能力を大きく左右する。

したがって、AIシステムを取り扱うすべての関係者は、本章で述べる欧州委員会の立法上および非立法上のイニシアチブの策定作業を能動的に監視することが推奨される。

Bird & BirdのRegulatory and Public Affairsチームは、AI Actに関して見込まれる今後のイニシアチブを注視し、さまざまなプロセスや要求への対応をサポートする。

AI Act の適用時期

2024年7月12日のEU官報[1]への掲載後、AI Actは2024年8月1日に発効した。

主な適用時期は以下のとおり。

2024年7月12日	AI ActがEU官報に掲載され、特定の条項の適用開始日のトリガーとなる
2025年2月2日	禁止されるAIプラクティスの適用開始（第2章） AIリテラシー・ルールの適用開始（第4条）
2025年5月2日	汎用目的AIの実践規範の準備期限（第56条第9項）
2025年8月2日	国家当局の指定（第4節第3章） 汎用目的AI（GPAI）に関する義務（第5章） ガバナンス（EUおよび加盟国レベル）（第7章） 守秘義務と罰則（汎用目的AIに関するものを除く）（第7章）
2026年8月2日	AI Actのその他すべての規定の適用開始（後日適用開始される以下の場合を除く）
2027年8月2日	付属書Iに掲げられている高リスクカテゴリー 2025年8月2日より前に市場に投入された汎用目的AIモデル（第111条）
2030年8月2日	2026年8月2日より前に市場に投入され、またはサービスが開始した、公的機関での使用を目的とした高リスクAIシステム（以下に挙げるものを除く）（第111条）
2030年12月31日	2027年8月2日より前に市場に投入され、またはサービスが開始した、付属書Xに列挙された大規模ITシステムのコンポーネント（第111条）

1. 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, OJ L, 2024/1689, 12.7.2024.

2024年8月1日から2027年8月2日の間に、欧州委員会は同法を実施するためのさまざまな文書を採択する予定である。これらには、委任法令および実装法令、ガイダンス文書、行動規範、実践規範、標準化要請が含まれる。一部の例外を除き、欧州委員会がこれらのイニシアチブを発表する期限は特に定められていない。ただし、欧州委員会は、各規定の適用時期に先駆けて関連する文書を採択することを目指すものと思われる。

委任法令

いくつかの条項は、欧州委員会が採択する委任法令の対象となり、義務や運用の明確化がされる。

第97条は、2024年8月1日から5年間、欧州委員会に委任法令を採択する権限を与えている。欧州委員会は、期間終了の9カ月前にこの委任について報告しなければならない。この期間は、終了の3カ月前までに欧州議会または欧州理事会が反対しない限り、自動的にさらに5年間延長され、その後も同様である。

前述のとおり、このような委任法令の採択期限は特に定められていない。しかし、AI Actの関連規定の適用開始に先立って採択されることが予想される（第113条参照）。

第97条第4項に従い、欧州委員会は、委任法令を採択する前の準備作業中に、パブリックコンサルテーションを実施しなければならず、また、関連する専門家グループ（加盟国の専門家で構成）とも協議を行わなければならない。

欧州委員会は、採択後、欧州議会と欧州理事会に対して同時に通知しなければならない。委任法令は、欧州議会と欧州理事会のいずれもが通知から3ヶ月以内（必要であれば、さらに3ヶ月延長され得る）に異議を申し立てない場合にのみ発効する。欧州議会または欧州理事会はこの権限をいつでも放棄することができるが、既存の委任法令の効力には影響しない。欧州委員会は、2016年4月13日付けのより良い立法に関する機関間協定（Interinstitutional Agreement of 13 April 2016 on Better Law-Making）の原則に従い、欧州議会と欧州理事会が加盟国の専門家と同時にすべての文書を受け取れるようにしなければならない。また、欧州議会と欧州理事会の専門家が、委任法令の作成を行う欧州委員会の専門家グループの会合に体系的にアクセスできるようにしなければならない。

AI Actは、欧州委員会が必要と考える場合に、以下の委任法令が採択されることを見込んでいる：

- **第6条第6, 7項**：付属書IIIに該当すべきでない、または第6条第3項の条件に該当すべきでないAIシステムが存在するという具体的かつ信頼できる証拠がある場合に、同項に新たな条件を追加し、または同項の条件を修正もしくは削除する。
- **第7条第1, 3項**：高リスクAIシステムのユースケースを追加、修正、削除することにより、付属書IIIを改正する。
- **第11条第3項**：技術文書がシステムの適合性を評価するために必要なすべての情報を提供することを確保するため、技術の進歩に照らし、必要に応じて付属書IVを改正する。

2. Inter-institutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making, OJ L 123, 12.5.2016.

- **第43条第5項**：技術の進歩に合わせて、付属書VIおよびVIIを更新する。
- **第45条第6項**：付属書IIIの第2項から第8項で言及されている高リスクAIシステムを第三者適合性評価の対象とするため、第43条第1, 2項を改正する。
- **第47条第5項**：技術の進歩により必要となる要素を導入するため、付属書に定めるEU適合宣言の内容を更新することにより、付属書Vを改正する。
- **第51条第3項**：第51条第1, 2項に記載されたシステミック・リスクのある汎用目的AIモデルの閾値を修正し、これらの閾値が最新技術を反映するため必要な場合には、アルゴリズムの改善やハードウェアの効率向上などの技術進展に応じてベンチマークや指標を補足する。
- **第52条第4項**：システミック・リスクのある汎用目的AIモデルの基準を規定または更新することにより、付属書XIIIを改正する。
- **第53条第5項**：付属書XIへの準拠促進を目的に、比較可能で検証可能な文書化を可能にする観点から、詳細な測定および計算方法を定める。
- **第53条第6項**：進化し続ける技術に照らして、付属書XIおよびXIIを改正する。

実装法令

AI Act第98条第2項は、欧州委員会に対し、Regulation (EU) 182/20113に従って実装法令を採択する権限を与えている。実装法令は、必要な場合に、特定の法令を実施するための統一的な条件を整備することを目的としている。実装法令の起草に関して、欧州委員会は、加盟国の専門家で構成される*「コミトロジー(Comitology)」*委員会の支援を受ける。

委任法令におけるのと同様、実装法令の採択時期は条文に明記されていない（2026年2月2日までとされる第72条3項の実装法令を除く）。そのため、AI Actの関連規定の適用開始の前に、関連する実装法令が採択されるものと考えられる（上記および第113条参照）。

AI Actは、欧州委員会が必要と考える場合に、以下の実装法令が採択されることを見込んでいる：

- **第37条第2項**：加盟国が必要な是正措置を講じない場合、第三者認証機関の指定を停止、制限または撤回する。
- **第41条第1, 4, 6項**：第67条で言及されている*「諮問フォーラム(Advisory Forum)」*と協議の上、第5章第2, 3節に規定された高リスクAIシステムの要件または汎用目的AIモデルについての義務に関する共通仕様を策定する。整合規格への言及がEU官報に掲載され、それが本第3章第2節に規定されたものと同じ要求事項をカバーする場合、欧州委員会は、第41条第1項に基づく実装法令を廃止するものとする。実装法令の共通仕様が第3章第2節に規定された要求事項を完全に満たしていないと加盟国が考える場合、欧州委員会は、その情報を評価し、適切であれば、第41条第1項に基づく実装法令を改正しなければならない。
- **第50条第7項**：第56条第6項に定める手続きに従い、人工的に生成された、または操作されたコンテンツの検出と表示に関する義務の効果的な実施を促進するための実践規範を承認する。実践規範が適切でない場合、欧州委員会は、第50条の特定のAIシステムのプロバイダーおよびディプロイヤーが負う透明性の義務の実施に関する共通ルールを定める実装法令を採択することができる。

3. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011.

- **第56条第6項**：汎用目的AIモデルに関する実践規範を承認し、EU域内一般に効力を及ぼす。2025年8月2日までに実践規範を最終決定できない場合、または実践規範が不十分であるとAI事務局が判断した場合、欧州委員会は、実装法令により、第53条および第55条に定める義務（第56条第2項に定める事項を含む）の実施に関する共通ルールを定めることができる。

- **第58条第1項**：AI規制サンドボックスの設置、発展、実施、運用、監督に関する詳細な取決めを定める。

- **第60条第1項**：高リスクAIシステムのプロバイダーのための実環境テスト計画の詳細な要素を規定する。

- **第68条第1項**：AI Actの執行をサポートすることを目的とした、独立した専門家による*「科学パネル（scientific panel）」*の設置に関する規定を設ける。

- **第72条第3項**：2026年2月2日までに、高リスクAIシステムのプロバイダーに対する市販後モニタリング計画のひな形と、計画に含めるべき要素のリストを定める詳細な規定を定めた実装法令を公表する。

- **第92条第6項**：独立した専門家を関与させるための詳細な取決めおよびその選定手続きを含む、汎用目的AIモデル評価のAI事務局に関する詳細な取決めおよび条件を定める。

- **第101条第6項**：汎用目的AIモデルのプロバイダーに課される可能性のある制裁金を勘案し、手続きに関する詳細な取決めと手続き上のセーフガードを定める。

委員会ガイドライン

*「委員会ガイドライン(Commission Guidelines)」*は、AI Actの特定の条項がどのように適用されるべきかについて、実務的かつ非公式なガイダンスを提供するために、委員会によって作成される説明文書である。

AI Actは、以下の委員会ガイドラインの採択を見込んでいる：

- **第6条第5項**：欧州AI委員会に諮った上で、2026年2月2日までに、高リスクと高リスクでないAIシステムのユースケースの例の包括的なリストを含む、第6条の実務運用について明記する。

- **第63条第1項**：小規模事業者のニーズを考慮し、保護レベルや高リスクのAIシステムに関する要求事項の遵守の必要性に影響を与えることなく、簡易な方法で遵守することができる品質マネジメントシステムの要素を定める（このガイドラインの策定期限は設定されていない）。

- **第73条第7項**：重大インシデントの報告義務の遵守を促進する。このガイダンスは2025年8月2日までに採択されなければならず、欧州委員会により定期的に評価される。

- **第96条**：AI Actの実務上の運用について定める。このガイドラインの策定期限は定められていない。しかし、関連規定は2026年8月2日から適用される。欧州委員会は、特に以下に関するガイドラインを作成することになっている：

  – 第8条から第15条および第25条に定める要件と義務の適用

  – 第5条に定める禁止されるプラクティス

  – 重大な変更に関する規定の実務的な運用

  – 第50条に規定された透明性の義務の実務的な運用

  – 付属書Iに掲げられているEU整合法令およびその他関連するEU法の、AI Actとの関係性に関する詳細な情報（執行における一貫性に関する情報を含む）

  – 第3条第1号にあるAIシステムの定義の適用

行動規範と実践規範

行動規範

行動規範とは、一定の条件下におけるAIの開発と活用に関する倫理的な指針と原則を定めた自主的な性質の文書である。また、AI Act上の特定の義務を自主的に遵守するために、組織内でのAIポリシーの策定を促進することも意図されている。

AI Actは、以下の行動規範の採択を求めている：

- **前文第20項および第4条**：AIの開発、運用、利用に携わる人々のAIリテラシーを向上させるための自主行動規範。
  - AIリテラシーを向上させるための自主行動規範の策定期限は定められていないが、第4条のAIリテラシーに関する関連規定は2025年2月2日から適用される。
- **前文第165項および第95条**：高リスクのAIシステムに適用される義務的要件の一部または全部の自主的な適用を促進することを意図した行動規範。これらは、システムが意図する目的および関連するリスクの低さに照らして適用され、利用可能な技術的解決策およびモデルカードやデータカードなどの業界のベストプラクティスを考慮に入れる：
  - 自主的な行動規範の実効性を確保するためには、同規範は、明確な目標とその達成度を測る重要達成度指標に基づくべきである。
  - 適宜、事業者や市民社会組織、学界、研究機関、労働組合、消費者保護団体などの関連する利害関係者の参加を得て、包括的な方法で策定されるべきである。
  - 高リスクAIシステムに適用される義務的要件の一部または全部の自主的な適用を促進することを意図した自主行動規範の策定期限は定められていないが、第95条に含まれる関連規定は、2026年2月2日から適用される。欧州委員会は、2028年8月2日までに、また、その後3年ごとに、そうした自主行動規範の影響と有効性を評価する。

実践規範

実践規範は、AI Act上の特定の義務を適切に遵守するための中心的なツールである。特に、ある実践規範は、汎用目的AIモデルおよびシステミック・リスクを伴う汎用目的AIモデルのプロバイダーに対する同法上のルールの詳細を定める。別の実践規範は、人工的に生成された、または操作されたコンテンツの検出とラベリングに焦点を当てる。組織は、関連する義務の遵守を証明する際、実践規範に依拠することができ、これは*「適合性の推定(presumption of conformity)」*として知られている。

具体的には、AI Actは、欧州委員会のAI事務局に対し、すべての利害関係者とともに以下の実践規範の策定を促進するよう求めている：

- **第50条第7項**：人工的に生成され、または操作されたコンテンツの検出と表示に関する第50条第2, 4項の義務の効果的な実施を促進するための、EUレベルでの実践規範。欧州委員会は、これらの実践規範を承認するための実装法令を採択することができる。第50条第2, 4項の義務の効果的な実施を促進するための自主的な実践規範の策定期限は定められていないが、第50条に含まれる関連規定は2026年2月2日から適用される。
- **第56条第1, 3項**：2025年5月2日までに、汎用目的AIモデルに関する実践規範を制定する。これらは、関連する国の管轄当局との協力や、市民社会組織やその他の関連する利害関係者、専門家との適宜の協議を通して、国際的なアプローチや多様な観点を勘案する。これには、AI Actに基づき設置される独立専門家の*「科学パネル」*も含まれる。

欧州委員会は、2028年8月2日までに、また、その後3年ごとに、自主的な実践規範の影響と有効性を評価しなければならない。

2024年7月30日、AI事務局は、汎用目的AIに関する最初の実践規範の作成への参加意思表明の募集を開始した。関心のある当事者は、2024年8月25日まで参加希望を表明することができた。欧州委員会によると、同規範は、AI Actが2024年8月1日に発効してから9ヶ月後の2025年4月までに、双方向のプロセスを経てドラフトされる。実践規範は、汎用目的AIモデルに対するAI Act上のルールの適切な適用を促進する。

欧州委員会は、第56条第6項に従い、実践規範を承認し、実装法令によってEU域内一般に効力

を及ぼすことができる。実践規範が不十分であると判断された場合、欧州委員会は、関連する義務の履行に関する共通ルールを定める。

加えて、AI事務局は、2024年7月30日、特に汎用目的AIモデルのトレーニングに使用する内容の要約のひな形とそれに付随するガイダンスに関する、AI Actに基づく信頼できる汎用目的AIモデルについてのコンサルテーションを開始した。回答期限は2024年9月10日であった。

規格

初期の標準化作業

AI Actをサポートする欧州規格の起草プロセスは同法が採択される前から始まっており、人工知能に関する調和の取れたルールを定める規則の提案は、2023年5月22日、欧州委員会実施決定C(2023)3215として採択された。

この実施決定は、欧州標準化委員会（CEN）および欧州電気標準化委員会（CENELEC）に対し、2025年4月30日までにAIに関する以下の新しい欧州規格または欧州標準化成果物を起草するよう要請した：

- AIシステムのリスク管理システムに関する欧州規格または欧州標準化成果物
- AIシステム構築のために使用されるデータセットのガバナンスと品質に関する欧州規格または欧州標準化成果物
- AIシステムによるログ機能による記録保持に関する欧州規格または欧州標準化成果物
- AIシステムのユーザーに対する透明性および情報提供に関する欧州規格または欧州標準化成果物
- AIシステムの人間による監視に関する欧州規格または欧州標準化成果物
- AIシステムの精度仕様に関する欧州規格または欧州標準化成果物
- AIシステムの堅牢性仕様に関する欧州規格または欧州標準化成果物
- AIシステムのサイバーセキュリティ仕様に関する欧州規格または欧州標準化成果物
- 市販後モニタリングのプロセスを含む、AIシステムプロバイダーの品質管理システムに関する欧州規格または欧州標準化成果物
- AIシステムの適合性評価に関する欧州規格または欧州標準化成果物

このCENおよびCENELECへの標準化要請は、欧州委員会の「欧州標準化のための年次連合作業プログラム」2022のアクション項目(63)に従い、AIシステムの安全性と信頼性を確保することを目的として行われた。

これらの規格のドラフトのために、CENとCENELECは、*「CEN-CENELEC JTC 21 Artificial Intelligence」*と称する合同専門委員会を設立した。CENとCENELECはまた、情報通信分野における独立した非営利の標準化団体である欧州電気通信標準化機構（ETSI）とも、草案作成について協働している。

AI Act標準化要請

AI Act第40条第2項は、欧州委員会に対し、同規則の発効後、過度な遅滞なく、EUにおけるAI規格の調和に関する標準化要請を提示するよう求めている：

- AI Act第3章第2節に規定されているすべての要件
- AI Act第5章第2, 3節に規定された義務をカバーする標準化要請（該当する場合）

これらの要請は、欧州委員会実施決定C(2023)3215に含まれる要請を修正するものである。これは、2024年2月に発表された欧州委員会の2024年標準化作業プログラムでも予定されていた。実際、同作業計画のアクション項目（15）では、*「AIに関するEUの政策を支援するための標準化要請の改訂(revision of the standardisation request in support of Union policy on artificial intelligence)」*を求めており、AI Actの最終的な文言を踏まえた欧州委員会決定の改訂を求めている。

AI Act第40条第2項によれば、標準化要請は、AIシステムの資源パフォーマンス改善のための報告および文書化プロセスに関する成果物も求めるべきとされている。このような要請には、高リスクAIシステムのライフサイクルにおけるエネルギーやその他の資源の消費量削減や、汎用目的AIモデルのエネルギー効率の高い開発などが含まれる。欧州委員会は、欧州AI委員会およ

びAI Actに基づき設立された諮問フォーラムを含む利害関係者と協議した上で、要望書を作成する必要がある。

さらに、欧州委員会は、関連する標準化団体に標準化要請を出す際に、標準が明確で一貫性がなければならないことを明記すべきとされる。この前提条件には、付属書Iに列挙されている既存のEU整合法令の対象となる製品についての、さまざまな分野で作成された規格が含まれる。これらの規格は、高リスクAIシステムまたは汎用目的AIモデル（EU域内市場に投入され、または同市場でサービスが開始されたもの）が、AI Actに定められた関連する要件または義務を満たすことを保証することを目的としている。

2028年8月2日までに、またその後4年ごとに、欧州委員会は、汎用目的AIモデルのエネルギー効率の高い開発に関する標準化成果物の策定に関する進捗状況をレビューする報告書を提出しなければならない。これに関連して、欧州委員会は、拘束力のあるものも含め、さらなる対策や措置の必要性を評価することも求められる。報告書は、欧州議会および欧州理事会に提出され、公表される。

責任

欧州委員会、AI Actに沿った提案に修正

最後に、2024年7月末、契約関係にない当事者間の民事責任に関するルールをAIに適用させる提案（AI責任指令(AILD)）の更新版を、欧州委員会が欧州議会と欧州理事会の双方に送付したことは注目に値する。この提案は、2022年9月に欧州委員会が初めて議題に上げたもので、基本的権利の尊重と安全性に焦点を当てた一連の規則を通じて、AIの特定の使用によって生じるリスクに対処することを目的としている。今回の変更は、AI責任指令案を、完成したAI Actと整合させるためのものである。

注目すべきは、新たな提案では第4条が改正され、AIシステムを導入する事業者の潜在的責任が強化されたことである。これらのディプロイヤーは、*「AIシステムの運用を監視せず、適切な場合には（その）使用を停止しなかった(did not monitor the operation of the AI system or, where appropriate, suspend [its] use)」*場合、または*「十分に代表的な(sufficiently representative)」*インプットデータを使用しなかった場合に生じた損害について、責任が推定される。

この件の欧州議会筆頭起草者であるドイツ・キリスト教民主主義の欧州議会議員Axel Voss氏は、以前、欧州議会リサーチサービスに対し、AI Actの採択を見据えてもなおAILDが必要かどうかを評価するための「代替影響評価」の実施を要請していた。提案されているAI責任指令の先行きは依然不透明だが、縮小された形で進行する可能性もある。

AIガイドの寄稿者

当事務所は、テクノロジー分野において市場をリードする法律事務所であり、12の法域においてLegal 500のAI部門（この種の法律事務所としては欧州初のランクイン）およびTMT（情報通信）部門でTier 1にランクされ、また、Chambersのグローバル複数法域TMT部門でBand 1にランクされています。このような法律事務所として、当事務所は、AI技術の開発と導入に関わる技術的な複雑さを深く理解したサポートを提供できる点で、他の事務所と一線を画しています。このような専門知識により、当事務所は、この分野独特の言語を理解し、また、開発者やビジネスチームと効果的に協力し、案件・相談開始の当初から適切な対話をすることが出来ます。当事務所のグローバルなAIグループは、**120人以上**のエキスパートで構成され、変革的なテクノロジーと法律・規制が交差する事項のほぼすべてをカバーしています。前例のない知的財産訴訟の取扱いや複雑な規制変更への対応サポートから、効果的なガバナンスの枠組みの導入や画期的なビジネス・契約上のアレンジの作り込みまで、幅広く対応します。

AI Actや本ガイドに関するご質問は、下記の寄稿者、またはBird & Birdの貴社御担当者までご連絡ください。また、最新のAIに関するアップデートについては、当事務所のAI Hubでもご覧いただけます。

Belgium

Benoit Van Asbroeck
Partner
+3222826067
benoit.van.asbroeck@twobirds.com

Paolo Sasdelli
Regulatory and Public Affairs Advisor
+3222826076
paolo.sasdelli@twobirds.com

Finland

Tobias Bräutigam
Partner
+358962266758
tobias.brautigam@twobirds.com

France

Anne-Sophie Lampe
Partner
+33142686333
anne-sophie.lampe@twobirds.com

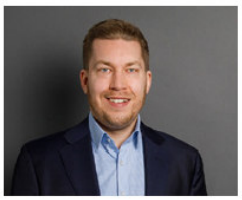
Cathie-Rosalie Joly
Partner
+33142686742
cathie-rosalie.joly@twobirds.com

Cen Zhang
Senior Associate
+33142686000
cen.zhang@twobirds.com

Germany

Delphine Frye
Senior Associate
+33142686054
delphine.frye@twobirds.com

Dr. Miriam Ballhausen
Partner
+4940460636000
miriam.ballhausen@twobirds.com



Dr. Nils Lölfing
Counsel
+4921120056000
nils.loelfing@twobirds.com

Oliver Belitz
Counsel

+4969742226000
oliver.belitz@twobirds.com

Dr. Simon Hembt
Senior Associate

+4969742226000
simon.hembt@twobirds.com

Ireland

Francine Cunningham
Regulatory and Public Affairs Director

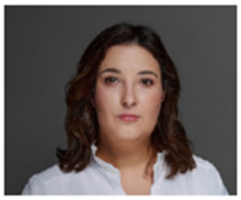
+3222826056
francine.cunningham
@twobirds.com

Italy

Gian Marco Rinaldi
Counsel

+390230356071
gianmarco.rinaldi@twobirds.com

Poland



Aleksandra Cywinska
Senior Associate

+48225837875
aleksandra.cywinska@twobirds.com

Aleksandra Mizerska
Lawyer

+48225837900
aleksandra.mizerska@twobirds.com

Andrzej Stelmachowski
Associate

+48225837977
andrzej.stelmachowski
@twobirds.com

Izabela Kowalczuk-Pakula
Partner

+48225837932
izabela.kowalczuk-pakula@
twobirds.com

Dr. Maria Jurek
Senior Associate

+48225837839
maria.jurek@twobirds.com

Marta Kwiatkowska-Cylke
Counsel

+48225837964
marta.kwiatkowska-cylke@
twobirds.com

Pawel Lipski
Partner

+48225837991
pawel.lipski@twobirds.com

Tomasz Zalewski
Partner

+48225837946
tomasz.zalewski@twobirds.com

Spain

Joaquín Muñoz
Partner

+34917906007
joaquin.munoz@twobirds.com

The Netherlands

Feyo Sickinghe
Of Counsel

+31703538904
feyo.sickinghe@twobirds.com

Shima Abbady
Senior Associate

+31703538984
shima.abbady@twobirds.com

United Kingdom

Alex Jameson
Senior Associate

+442078507139
alex.jameson@twobirds.com

Ian Edwards
Partner

+442079056377
ian.edwards@twobirds.com

Katerina Tassi
Senior Associate

+442074156066
katerina.tassi@twobirds.com

Katharine Stephens
Partner

+442074156104
katharine.stephens@
twobirds.com

Liz McAuliffe
Associate

+442074156787
liz.mcauliffe@twobirds.com

Nora Santalu
Associate

+442079826513
nora.santalu@twobirds.com

Ruth Boardman
Partner

+442074156018
ruth.boardman@twobirds.com

Toby Bond
Partner

+442074156718
toby.bond@twobirds.com

Will Bryson
Senior Associate

+442074156746
will.bryson@twobirds.com

twobirds.com

Bird & Bird

アブダビ • アムステルダム • 北京 • ブラチスラバ • ブリュッセル • ブダペスト • カサブランカ • コペンハーゲン • ドバイ • ダブリン • デュッセルドルフ • フランクフルト • ハーグ • ハンブルク • ヘルシンキ • 香港 • ロンドン • リヨン • マドリード • ミラノ • ミュンヘン • パリ • プラハ • ローマ • サンフランシスコ • 上海 • 深セン • シンガポール • ストックホルム • シドニー • 東京 • ワルシャワ