

Client Alert

15 April 2024

本アラートに関する
お問い合わせ先：



高瀬 健作
パートナー
03 6271 9752
Kensaku.Takase@bakermckenzie.com



達野 大輔
パートナー
03 6271 9479
Daisuke.Tatsuno@bakermckenzie.com



岡田 次弘
カウンセラー
03 6271 9541
Tsugihiko.Okada@bakermckenzie.com



菅 礼子
シニア・アソシエイト
03 6271 9696
Ayako.Suga@bakermckenzie.com

欧州議会が AI Act を採択：2 年後に完全適用 企業としての対応ポイントは

EUにおける「AI Act」が、2024年3月13日、欧州議会で採択された。AI Actは数か月以内に発効し、最初の実質的な規定内容の施行が2024年末までに行われる予定である。

AI Actは、AIのライフサイクル全体に適用されるものであり、これはAI技術の開発をする主体から導入をする主体に至るまでの広範な企業が適用の対象となることを意味する。各業界がその進展を注視してきた、このAI Actが最終的に承認された今、次に何が起こるのか、そして企業は、AI Actへの準拠を自社のAI戦略とガバナンスに組み込むために現時点でどのようなステップを実践すべきか、以下に示す。

なお、AI Actは、EU域内の主体だけでなく、EU域外に拠点を置きながらEU加盟国でAIビジネスを展開する主体にも適用されるため、多国籍企業の多くが同法の規定対象となる。日本企業も、この法律をめぐる動向を十分に注視する必要がある。

AI Actでは、公共の場での顔認証技術の使用といった、「容認されない」（したがって禁止される）利用形態、雇用関係におけるAIの使用といった、適合性評価やリスク管理の対象となる「高リスク」の利用形態、チャットボットのような「限定的リスク」の利用形態、情報要件や自主行動規範が適用される「最小リスク」の利用形態といった、用途ごとにAIを分類する、リスクベースのアプローチをとっている。現在大手ハイテク企業が開発している、幅広い明確なタスクを実行できる最先端のAIシステム、たとえばチャットGPTなどの「汎用的なAI」モデルも、この法律で規制されている。

今後のステップ

AI Actは、最終的な文書が公式発表されてから20日後に発効する。AI Actの内容は、AIシステムのリスクベースの分類に従い、以下のように段階的に施行されていく予定である。

- **発効から6か月後（おそらく2024年後半）**には、容認されないAIシステムについての禁止規定が発効する。これは、基本的権利の観点から許容できないリスクをもたらすとされる限定的事例を対象としている。禁止される事例の中には、サブリミナル技術の使用、人の脆弱性を悪用するシステム、バイオメトリクス分類、ソーシャルスコアリング、個人の行動を予測した取り締まり、一定の顔または感情認識技術の使用、および法律に基づく取り締まり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での遠隔バイオメトリクス識別システムが含まれる（一定の例外規定がある）。
- **発効から12か月後（おそらく2025年半ば）**には、汎用的なAIに関するガバナンスの義務が適用されるようになる。汎用的AIシステムは、市販



前の適合性評価を受ける必要がなく、一般的に高リスクシステムよりも企業側には負担が軽いものとなっている。ただし、技術文書の作成、著作権法を尊重するポリシー、学習データセットの内容の「十分に詳細な」要約の公開義務、AIが生成または操作したコンテンツであること表示するという要件が課される。システム上のリスクがあると判断された汎用 AI システムには追加の要件が課される。

- **発効から 24 か月後（おそらく 2026 年後半）**には、AI Act が全面的に適用開始される。市販前の適合性評価、品質およびリスク管理システム、市販後のモニタリングなど、高リスクの AI システムに適用されるすべての義務が適用されるようになります。AI Act は、高リスクの AI システムに該当する事例が詳細なリストとして規定されているが、これは将来の発展を反映して修正される可能性があるほか、EU 委員会による実践的なガイダンスや事例が補足される予定である。
- **発効から 36 か月後（おそらく 2027 年後半）**に、既に第三者機関による適合性評価が義務付けられている製品にも AI Act が適用されるようになる。AI Act では、AI それ自体が製品となるものと、AI が製品の安全性に関する部品として使用されることを意図している AI システムについて、若干異なるアプローチをとっている。後者に関しては、EU で上市される製品に第三者適合性評価を受けることがすでに義務付けられている。このカテゴリの製品の具体例は、医療機器から玩具に至るまで、多岐にわたる。この既存の分野別の規制についての当局は、引き続き、これらの製品に対して AI Act を施行する権限を有しており、これらの製品の適合義務は 1 年延長されることになる。
- **すでに市販されている AI システム**には、遵守のための追加の期間が設けられている。このカテゴリの AI システムは、その設計が大幅に変更された場合のみ、同法の規制対象となる。すでに市場に出回っている汎用 AI システムの場合には、さらに 2 年間の猶予期間が与えられることになる。

上記の動きと並行して、EU 委員会と加盟国は、同法の施行のため、以下のような枠組みを整備することになっている。

- **関連の監督当局の特定、設置、人員の配置**

EU 加盟国のガバナンス機関を支援し、GPAI モデルの規則を施行する目的で、EU AI 事務局が設立された。加盟国は、禁止されているシステムの禁止と、高リスクの AI システムに適用される義務を執行するために、各国の監督当局を指定することが求められる。既存の EU 製品安全法で規制されている、航空分野から医療機器に至るまでの幅広い分野については、規制執行の責任は既存の各分野の規制当局が負うことになるが、これらの規制当局は、AI Act における新たな規制のための適切な技術的専門知識を確保する必要がある。

- **罰則の設定**

AI Act は、加盟国に罰則やその他の強制措置を定める権限を与えており、その上限は（違反した義務に応じて）全世界の年間総売上高の 7%または 3,500 万ユーロまでとなっている。これらは、同法の発効後まもなく決定される必要がある。



- **AI Act の遵守に関するガイダンスの提供**

AI Act は、欧州委員会に対し、発効後 18 か月以内に実質的な実施に関するガイドラインを作成するよう求めている。加盟国の監督当局もまた、AI Act に基づく規制上の期待に関するガイダンスを作成する必要がある。

企業のとるべき対策

事業者は、自社の AI システムが EU の AI 法の対象となるかどうか、また、自社の AI システムがどのリスクカテゴリーに分類されるかを判断する評価を行う必要がある。

もちろん、AI Act への準拠は、AI ガバナンス・プログラムの一部に過ぎない。AI Act は EU 初の包括的な AI に関する法律として注目されている一方、各国でも AI 関連の取り組みが多数あり、各国規制当局も既存の法律のもとでの AI に関するデータプライバシー、消費者保護、差別に関する規制へのコンプライアンスを検討している。

これを踏まえ、事業者は以下のことを行っておくべきと考えられる。

- 自社組織内、そしてサプライチェーンにおける AI の開発・利用を監査すること。
- AI の原則を踏まえた「超えてはならない線」を決定すること。AI Act で定められているパラメータもそうだが、法律を超える倫理的配慮が含まれる可能性が高くなっている。
- 組織レベルおよび製品のライフサイクルレベルの両方において、AI Act の要件を満たすことをはじめとした、AI に関するリスクを評価し、コントロールを強化すること。
- 関連する AI リスクについて、責任部署と内部のガバナンスチームを特定しておくこと。
- (i) AI の調達、(ii) AI を使用して作成される可能性のある第三者のサービス、製品、成果物の調達の両方に関連する、既存のベンダーのデューデリジェンスプロセスを再検討すること。
- 既存の契約ひな形について、AI リスクを軽減するために必要な見直しを行うこと。
- AI 及び AI に関連する法律、ガイダンス及び基準の世界的な展開を継続的に監視し、会社の AI ガバナンスの枠組みが更新されるようにすること。