

Client Alert

15 December 2023

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

暫定合意された EU の AI Act、実務上の影響は？

12月8日金曜日深夜、EU議会、欧州理事会、欧州委員会は、3日間にわたる広範な最終討議を経て、欧州におけるAIの開発と利用を包括的に規制するEU AI Act（以下「AI Act」）の暫定合意を発表した。このAI Actがどのように施行されるかについての詳細はまだ明らかにされていないものの、EUにおけるAIの利用を包括的に規制するものであり、今後、EU以外においても同様の規制に向けた動きを加速させる可能性もある。

AI Actは、今後、議会と理事会の双方による正式な採択を経れば、正式にEUにおいて発効することになり、一部の例外を除き、発効から2年後に施行される。

経緯

AI Actは、2021年に欧州委員会がAIに関する規則を提案したのを皮切りに制定に向けた検討が進められてきたが、2023年になってAIの大規模な言語モデルへの関心が爆発的に高まったことを受け、議論が加速していた。

AI Actが欧州におけるイノベーションを阻害するとの懸念を表明している団体や企業もあるが、立法者は、AI Actの内容によって、イノベーションの実現と責任ある技術の促進のバランスがとられると考えている。

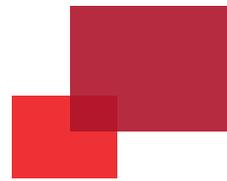
適用範囲

成立した暫定合意では、EU AI Actが、「EU法の範囲外では」適用されないとしているが、実際のところは、EU域内に所在する企業であるか否かにかかわらずAI Actの対象となりうる。但し研究開発のためだけに使用されるAIシステムや、私的な理由でAIを使用する場合には、AI Actは適用されない。

規制の概要

AI Actは、AI製品の規制について、リスクベースのアプローチをとっており、当該AI技術が属するリスクのカテゴリーごとに異なる義務を課している。たとえば、「許容できない」レベルの危険性をもたらす技術は禁止され、「高リスク」の技術には厳しい制限が課される。禁止される技術には、生体情報による識別認証システムや、予測捜査システム、感情認識システムといったシステムがある。インターネットや防犯カメラからの顔画像を大量に収集する行為は禁止され、ディープフェイクのような操作された画像を作成するために使用されるAIは、その画像がAIによって生成されたものであることを明示しなければならない。

詳細はまだ明らかにされていないが、EUは、ChatGPTに代表されるような汎用AIモデルに対しては透明性要件を課し、より広範な影響を及ぼす強力なAIモデルに対してはより厳格な要件を課す、という二段階のアプローチをとることを合意している。最先端のAIモデルについては、その規制を監督するために、欧州委員会内にAI専門のオフィスが設置される予定である。



AI Actに基づく義務として、AIを提供・導入しようとする場合、透明性と安全性の観点からの制約を特に受けることになる。また、健康、安全、人権、民主主義等を保護するために高リスクに分類されるAIを提供する場合、設計やテストといった段階から、危険性の評価とその軽減措置、EUのデータベースへのモデルの登録といった保護措置を実施しなければならない。高リスクのAIシステムのユーザーも、一定の公共団体についてはEUのデータベースに登録しなければならないこととなる。

制裁

AI Actで禁止される行為を行った場合、最高3,500万ユーロ、または企業の年間世界売上高の7%の罰則が科されうる。それ以外の義務違反には1,500万ユーロまたは売上高の3%、誤った情報の提供には750万ユーロまたは売上高の1.5%の罰則が科されうる。中小企業やスタートアップに対する行政罰については、その規模に応じた上限が規定されている。

事業者への影響

このAI Actに関する合意の成立を踏まえ、日本企業としては、自社のAIシステムがAI Act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、といった分析を進めることが求められる。但し、AI Actの遵守は、AI開発におけるガバナンスの一部に過ぎず、欧州以外の法域におけるAI関連の規範へのほか、データプライバシー、消費者保護、差別に関する規制など、既存の法律の枠組みにおけるAIに対する規制などへの準拠も必要であることには留意を要する。

企業としては、以下のような事項に対して、対策を講じておくべきである。

- 自社の組織内、および製品のサプライチェーンにおけるAIの開発および利用についての確認・監査を行うこと
- AIの活用に関する社内の基礎的なルールの作成をしておくこと。これにあたっては、AI Actをはじめとした法規範のほか、倫理的な観点からの考慮も必要となる。
- 企業全体およびサービスや製品ごとに、AIに関する既存のリスクの洗い出しとその対策の見直し・強化を行っておくこと
- AIに関するリスクや責任を負うこととなる部署を特定し、内部ガバナンスのためのチームを組織すること
- AI自体の調達のほか、AI（特に生成系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や物の調達について、AIリスクの観点からの、サプライヤーに対するデューデリジェンスを行うこと
- AIに関するリスク軽減という観点から、既存の契約テンプレートの見直しを行うこと
- AIに関連する法律、ガイダンス、基準についての継続的なモニタリングと、その進展に応じたAIガバナンスの枠組みの更新を行うこと