知財法務の勘所Q＆A（第52回）

激変するAI周辺のルール、EUのAI規制法案とは？

アンダーソン・毛利・友常 法律事務所 外国法共同事業
弁護士　**中崎　尚**

はじめに

2021年４月にAIをターゲットする世界で初めての包括的な規制枠組みとも言われる、AI規制法案がEUから公表されました。日本国内では法令レベルの規制の導入は、国内の状況に鑑みてふさわしくないとして見合わせられていますが、いわゆるソフトローとして、2021年７月に経済産業省から「AI原則実践のためのガバナンス・ガイドラインver. 1.0」が公表されています。本稿では、EUのAI規制法案を中心に、AI周辺をめぐるルールが激しく動きつつある直近の状況を紹介していきます。

Q1　最近、EUからAI規制法案が公表されたという記事を目にしたのですが、そもそもAI規制法案とはなんでしょうか。

A1　AI規制法案と呼ばれることの多い同法案は、正式名を「AIに関する整合的規則（AI法）の制定及び関連法令の改正に関する欧州議会及び理事会による規則案」（REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE（ARTIFICIAL INTELLIGENCE ACT）AND AMENDING CERTAIN UNION LEGISLATIVE ACTS）といいます[1]。名前にある通り、GDPR（一般データ保護規則）と同じく「指令」ではなく「規則」に位置づけられています。「指令」が加盟国の国内法制化を経ない限り、直接効力が生じないのに対して、「規則」は、それだけで直接に効力が生じ、国内法制化を経なくとも効力が生じることになり、日本法でいう「法律」に近いため、本稿ではわかりやすさを重視して「法案」と呼称します。

Q2　今回のAI規制法案の公表に至るまで、EUではどのような動きがありましたか。

A2　EUは、従前から、環境やロボットなど、新たに登場した、ルールが確立されていない分野において、世界に先駆けてルールを立ち上げようとする傾向があります。この

1　https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

傾向はAIの分野においても変わらず、活発な動きを見せてきました。

2018年４月には欧州委員会が、「AIに関する戦略方針」を発表、2019年４月には、専門家会議（AI HLEG）が、「AI倫理ガイドライン」を策定・公表しました。EUはさらに動きを加速させ、2020年２月には、AIのリスク対応とAI開発の推進の両面でEUが世界的な主導権を握るべきだとする「AI白書」と「AI・IoT・ロボットに関する安全・賠償責任レポート」を発表し、世界をリードしようとする姿勢を示しました。

この「AI白書」を具現化しようとするのが、今回、2021年４月に発表された「AI規制法案」を含む政策パッケージです。この政策パッケージには、他に以下のドキュメントが含まれています。

・「EUと加盟国間の協調計画」（Coordinated Plan on Artificial Intelligence 2021 Review）[2]
・機械製品に関する規制法案（Proposal for a Regulation of the European Parliament and of the Council on machinery products）[3]
・AIに対するEUアプローチのコミュニケーション
・Q&A

Q3 AI規制法案は何を目標としてつくられているのでしょうか。

A3 AI規制法案の冒頭「１．CONTEXT OF THE PROPOSAL」では、今回の法案公表に至るまでの詳細な経緯を紹介したうえで、立法目的を以下のように説明しています。まず、AIが社会に与える影響についての現状認識として、AIが人間の経済的・ 社会的活動に大きな利益をもたらす反面、使い方を誤れば生命・身体の安全や基本的人権に深刻な悪影響をあたえる危険性があると述べています。そしてこのような現状認識を前提として、EUにおけるAIに対する包括的・統一的な法的枠組みの構築を目標として、AI規制法案を提案したと説明されています。

Q4 AI規制法案の構成を教えてください。

A4 AI規制法案の構成は以下のようになっています。

・解説メモ（EXPLANATORY MEMORANDUM）
・本文：全85条から構成されており、その大部分はAIシステムのリスクに関連する条項です。AIシステムのリスクを４段階に分類し、段階ごとに規制を定めています。

（TITLE I）本法の対象範囲及び用語の定義（SCOPE AND DEFINITIONS）
（TITLE II）許容できないリスクをともなうため禁止されるAI実装（PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES）
（TITLE III）高リスクのAIシステム（HIGH-RISK AI SYSTEMS）
（TITLE IV）特定のAIシステムに求められる透明性確保義務（TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS）

---

2 https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review
3 https://ec.europa.eu/docsroom/documents/45508

（TITLE V） AIイノベーションの支援措置（MEASURES IN SUPPORT OF INNOVATION）
（TITLE VI）AIガバナンス（GOVERNANCE）
（TITLE VII）スタンドアロンで高リスクのAIデータベース（EU DATABASE FOR STAND-ALONE HIGH-RISK AI SYSTEMS）
（TITLE VIII）市場登場後のモニタリング、情報共有、市場調査（POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE）
（TITLE IX）行動規範（CODES OF CONDUCT）
（TITLE X）秘密保持及び罰則（CONFIDENTIALITY AND PENALTIES）
（TITLE XI）権限の委任及び委員会の手続き（DELEGATION OF POWER AND COMMITTEE PROCEDURE）
（TITLE XII）最終規程（FINAL PROVISIONS）

・附属書：附属書はIからIXまでが存在しており、本文に含めにくい詳細な情報が記載されています。たとえば、附属書III（Annex III）では、AIシステムのリスクの分類のうち、上から２番目の高リスクの事例を列挙しています。

（Annex I）第３条で参照されるAIの技術及びアプローチ（ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1）
（Annex II）調和が求められるEU法令のリスト（LIST OF UNION HARMONISATION LEGISLATION）
（Annex III）第６条第２項で参照される高リスクのAIシステム（HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6（2））
（Annex IV）第11条第１項で参照される技術文書（TECHNICAL DOCUMENTATION referred to in Article 11（1））
（Annex V）EU適合宣言（EU DECLARATION OF CONFORMITY）
（Annex VI）内部統制をベースとする適合性審査手続き（CONFORMITY ASSESSMENT PROCEDURE BASED ON INTERNAL CONTROL）
（Annex VII）品質管理審査及び技術文書審査の適合性（CONFORMITY BASED ON ASSESSMENT OF QUALITY MANAGEMENT SYSTEM AND ASSESSMENT OF TECHNICAL DOCUMENTATION）
（Annex VIII）第51条に沿った高リスクのAIシステムの登録において提出すべき情報（INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGH-RISK AI SYSTEMS IN ACCORDANCE WITH ARTICLE 51）
（Annex IX）自由・安全・正義の領域（域内での安全、権利と自由な移動を確保するために構築される諸政策　例：シェンゲン圏）における大規模ITシステムに関するEU法令（Union legislation on large-scale IT systems in the area of Freedom, Security and Justice）

Q5 AI規制法案の対象となるAIシステムとは何ですか。

A5 AI規制法案においては、AIシステムとは、附属書Iに列挙されている技術およびアプローチのいずれか１つ以上を用いて開発され、人間が定めた一定の目的のために、当該システムが相互作用する環境に影響をもたらすコンテンツ、予測、推奨または決定等のアウト

プットを生み出すソフトウェアを意味すると定義されています（本文第３条第１号）。この定義はかなり幅広に捉えられる可能性がある文言になっていますが、その趣旨として、解説メモでは、AIに関する急速な技術的進歩や市場の変化を考慮に入れ、できるだけ技術的に中立でかつ将来の情勢変化に耐えうるものにしようとする意図があると説明されています（解説メモ5.2.1）。

Q6 AI規制法案が適用されるのはどのような事業者でしょうか。

A6 AI規制法案においては、同法が適用されるのは、①EU域内でAIシステムを市場に投入するかまたはサービス提供する「プロバイダー（provider）」（当該プロバイダーがEU域内に拠点を有するか否かは問わないとされます）、②EU域内に所在するAIシステムの「ユーザー（user）」、③当該システムにより生み出された成果がEU域内で使用される場合の、第三国に所在するAIシステムの「プロバイダー」または「ユーザー」であると定められています（本文第２条第１項）。

ここでいう「プロバイダー」とは、「AIシステムを開発するか、自らの名でそれを市場に投入またはサービス提供する目的で開発されたAI システムを保有する主体」と定められており、AIビジネスに携わる事業者を広く含めています（本文第３条第２号）。「ユーザー」については「プライベートで個人的に利用する場合を除き、AIシステムを自らの権限のもとで利用する主体」と定められており（同条第４号）、いわゆるエンドユーザーを指すものではありません。

Q7 AI規制法案は日本企業にも適用があるのでしょうか。

A7 GDPRがEU域外の事業者に正面からGDPRを域外適用するルールを定め、世界中の事業者に衝撃を与え、どの法域の事業者もGDPR対策を迫られる状況に陥ったのは記憶に新しいところですが、AI規制法案においても域外適用に関するルールが正面から定められています。Q６でも説明しましたように、EU域外の事業者であっても、EU域内でAIシステムを市場に投入するかまたはサービス提供している場合や、当該システムにより生み出された成果がEU域内で使用される場合には、「プロバイダー」（前者及び後者）または「ユーザー」（後者のみ）に該当する可能性が生じ、日本企業にも適用される可能性は否定できません。

Q8 AI規制法案の定めるリスク分類とはどのようなものですか。

A8 AI規制法案では、リスクの観点からAIを、①許容できないリスクを伴うAI、②高リスクを伴うAI、③透明性確保義務を伴うAI、④極小リスクを伴う（あるいはゼロリスクの）AIの４カテゴリに分類しており、それぞれに対して異なる規制を設けています。とりわけ、②高リスクを伴うAIについては、全85条のうち、第６条から第51条までが割り当てられており、多くの義務が詳細に定められています。

① 許容できないリスクを伴うAI：利用禁止
② 高リスクを伴うAI：利用可能だが、要件と事前の適合性審査の準拠が必須条件。
③ 透明性確保義務を伴うAI：透明性確保義務を果たせば、利用可能。

④　極小リスクを伴う（あるいはゼロリスクの）AI：利用に制限なし。

Q9　許容できないリスクを伴うAIとはどのようなものですか。

A9　AI規制法案では、許容できないリスクを伴うAIとして、以下のAIシステムを市場に投入、サービス提供または使用する行為は原則として禁止されています（本文第５条第１項(a)ないし(d)）。

①　サブリミナル技術を用いて人の無意識に働きかけて当該人物の行動を歪め、当該人物や他の人物に肉体的または精神的な害をもたらす（またはそのおそれのある）AIシステム

②　児童や肉体、精神に障害のある人などの脆弱性につけ込んで、当該人物の行動を歪め、当該人物や他の人に肉体的または精神的な害をもたらす（またはそのおそれのある））AI システム

③　自然人の信用性を一定期間にわたってその人の社会的行動や性格に基づいて評価または分類するために公的機関やその代理機関が、用いるAIシステムであって、以下の事象につながるようなソーシャルスコアリングを伴うもの

㈠　分析対象のデータが元来生成、収集された文脈とは関係のない社会的な文脈において、特定の自然人や当該人物の属するグループ全体を不利益に扱うこと

㈡　特定の自然人や当該人物の属するグループ全体を、当該人物の社会的行動やその重大性からは正当化できない、あるいは不釣り合いな態様で不利益に扱うこと

Q10　高リスクのAIシステムとはどのようなものを指しますか。

A10　AI規制法案では、人間の健康・安全や基本的人権に重大なリスクをもたらしかねないAIを「高リスクAI」に分類し、その適切な管理・運用を目的とした一定の要件を充足することを求めるとともに、プロバイダーその他の事業者に対し、かかる要件充足性を担保するための厳格かつ広範な義務を課しています。 AI規制法案が、高リスクを伴うAIとして分類しているのは、以下のAIシステムです。

①　附属書IIに列挙される既存のEU法令の規制

対象である製品（機械、玩具、レジャークラフト、昇降機、爆発性のある大気中で使用される装置、無線機器、圧力機器、ケーブルウェイ、個人用保護具、ガス燃料機器、医療機器等）の安全性コンポーネントとして使用されることを意図されるかまたはかかる製品そのものであるAIシステムのうち、かかる製品が当該各EU法令に基づき第三者適合性審査の対象となるもの（第６条第１項）。

②　附属書IIIに列挙される８分野におけるスタンドアロンAIシステム（同条２項）。

附属書IIIに記載されている８分野

ⅰ）自然人の生体識別及び分類；リアルタイムで行うか否かを問わず、遠隔地からの生体識別を行うために使用されるAl

ⅱ）重要インフラの管理及び運営：道路交通や水、ガス、暖房及び電気の供給の管理、運営における安全性コンポーネントとして使用されるAl

iii）致育及び職業訓練：自然人の教育・職業訓練に対するアクセス・割当ての決定、学生や入学試験受験者を評価するために使用されるAl
iv）雇用、労働者管理、自営業へのアクセス：職への応募者の評価・選別、昇進・解雇の決定、業務の分配、被雇用者のパフォーマンスや態度を監視・評価するために使用されるAl
v）エッセンシャルな民間・公共サービスへのアクセス：自然人が、公共サービス等を受給できる資格の有無の審査、自然人の信用力の評価、消防士や救急隊員等の発動やその優先順位の決定にあたって使用されるAl
vi）法執行：自然人が犯罪行為や再犯に及ぶリスクや犯罪の被害者となるリスクの評価、嘘の発見や自然人の心理状態の特定、ディープフェイクの発見、刑事捜査や訴追の過程での証拠の信用力の評価、特定の自然人の来歴に基づいた犯罪発生の予測、自然人やグループの人格的特徴や過去の犯罪的行動の評価、ある複雑・大規模な一群のデータの中から未知のパターンや隠れた関係性を発見するための犯罪分析に用いられるAl
vii）移民、亡命、国境管理：嘘の発見や自然人の心理状態の特定、テロや不法移民、公衆衛生の観点からのリスクの評価、旅券等の書面の真正の確認のために使用されるAl、所轄機関が亡命、ビザ、居住許可の申請等を審査するのを援助するAl
viii）司法行政及び民主主義プロセス：司法機関が事実や法の調査、解釈を行い、法を具体的事実に当てはめるのをサポートするために使用されるAl

この８分野のうち、実務上影響する範囲が大きいと考えられるのは、iii）及びiv）です。ここに分類されるAIはリスクにやや幅があることから、一律の規制を課すのが望ましいかは今後も議論されると予想されています。

Q11 高リスクを伴うAlシステムに求められる要件とは何ですか。

A11 高リスクを伴うAlシステムに求められる要件としては、以下が定められています（本文第８条ないし第15条）。

① リスク管理システムの構築（本文第９条）：高リスクAIに関して、「リスク管理システム」が作成、実施、文書化、保存される必要があります。このリスク管理システムについて、市場流通後のモニタリングから収集されたデータの分析に基づく他の潜在的リスクの分析等、一定の定められた要素を含める必要があります。
② データガバナンス（本文第10条）：データの学習を含む技術を使用する高リスクAIシステムは、所定の品質基準を満たすトレーニング、検証、テストデータセットに基づいて開発される必要があります。
③ 技術的内容に関する情報の記述（本文第11条）：高リスクAIについて、市場への投入・サービス提供に先立ち、当該AIがAI規制法案に定める要件を充足していることを示す、附属書IV に記載される事項を含む技術文書が作成され、かつ適宜アップデートされる必要があります。
④ 記録保持（トレーサビリティ）（本文第12条）：高リスクAIは、その動作中に自動でログを保存する機能を備える必要があるとともに、当該ログは、AIの使用目的に照らして適切な態様で、そのライフサイクルを通じて追跡可能である必要があります。
⑤ ユーザーに対する情報提供、透明性の確保（本文第13条）：高リスクAIについては、その

透明性確保のため、ユーザー向けの使用マニュアルを用意する必要があります。

⑥　人力による監視（本文第14条）：高リスクAIについては、適切にインターフェイスを設けるなどして、その使用中に自然人が監視できるように設計・開発されている必要があります。

⑦　AIの正確性、強固性、サイバーセキュリティの確保（本文第15条）：高リスクAIについては、適切な正確性、強固性及びサイバーセキュリティのレベルを達成するように設計、開発されている必要があります。

Q12 高リスクAIシステムに関わるプロバイダーはどのような義務を負いますか。

A12 プロバイダーは以下の義務を負うものとされています。

①　高リスクAIが充足すべき要件（Q11参照）を満たすようにすること

②「品質管理システム」を設けること

③　高リスクAIの「技術文書」（Q11参照）を作成すること

④　高リスクAIにより自動的に出力されたログを保存すること

⑤　高リスクAIシステムを市場投入またはサービス提供するのに先立ち、適合性審査を実施すること

⑥　EUデータベースに高リスクAIを登録すること

⑦　高リスクAIが要件を充足しない場合にその是正措置を講じること

⑧　各加盟国当局等に要件不充足及び是正措置を知らせること

⑨　CEマークを高リスクAIシステムに貼付すること

⑩　各国の求めに応じて高リスクAIシステムの要件充足性を証明すること

⑪　AIシステムの市場投入またはサービス提供開始後10年間、技術文書、品質管理に関する文書その他の文書を保存すること

⑫　市場流通後のモニタリングシステムを設け、文書化すること

⑬　市場流通後の高リスクAIシステムについて発生した深刻なインシデントや不具合を、関連する加盟国の市場監視当局に報告すること

Q13 高リスクAIシステムに関わる輸入業者はどのような義務を負いますか。

A13 輸入業者は以下の義務を負うものとされています。

①　高リスクAIを市場に投入する前に、適合性審査の実施状況、プロバイダーによる技術文書の作成状況、必要なCEマークが貼付されかつ使用マニュアル等を伴っていること等を確認すること

②　AIが、AI規制法案に適合しないと考えまたはそう考える理由がある場合には、適合性を満たすようになるまで当のAIを市場に投入しないこと

③　自らの商号・商標及び所在地をAI自体または包装等に記載すること

④　保管または運搬中の条件によってAIがAI規制法案に定める要件を充足しないことにならないようにすること

⑤　各国当局からの要請に応じて、AIの要件適合性に関するすべての必要な情報及び文書を

提供すること

Q14 高リスクを伴うAIを取り扱う販売業者はどのような義務を負いますか。

A14 販売業者は、以下の各義務を負うことが定められています。

① 高リスクAIを流通させる前に、CEマークの貼付状況、使用マニュアル等を伴っていること、プロバイダー及び輸入業者によるAI規制法案に定める義務の履行状況を確認すること

② AIがAI規制法案に適合しないと考えまたはそう考える理由が、ある場合には、適合性を満たすようになるまでそのAIを流通させないこと

③ 保管または運搬中の条件によってAIがAI規制法案に定める要件を充足しないのを避けること

④ 市場にすでに流通させたAIが、AI規制法案に適合しないと考えまたはそう考える理由がある場合には、当該AIが要件に適合するようにするか、市場からの引き上げやリコールを行うといった是正措置を自ら講じるか、プロバイダー、販売業者その他に適切な是正措置を講じるようにさせること

⑤ 各国当局からの要請に応じて、AIの要件適合性に関するすべての必要な情報及び文書を提供すること

Q15 違反した場合、GDPRのような制裁はありますか。

A15 AI規制法案では、GDPR類似の、非常に厳しい制裁金が定められています。 その上限は、以下の通りです。

① AI規制法案第５条に定める特定のAIの使用禁止義務及び第10条に定めるデータガバナンスに関する義務違反：3000万ユーロ以下の制裁金、または違反者が企業の場合は 直近の会計年度における全世界の年間売上総額の６％の金額のうち、いずれか高額のほう（本文第71条第３項）

② AI規制法案のその他の要件及び義務を遵守しない場合：2000万ユーロ以下の制裁金、または違反者が企業の場合は直近の会計年度における世界全体における年間売上総額の４ ％の金額のうちずれか高額のほう（同条第４項）

③ 外部審査機関及び各国関連当局に対して不正確、不完全または誤解を招くような情報を提供した場合：1000万ユーロ以下の制裁金、または違反者が企業の場合は直近の会計年度における世界全体における年間売上総額の２ ％の金額のうちいずれか高額のほう（同条第５項）

まとめ

AI規制法案は冒頭で紹介した正式名の通り、現時点ではあくまで提案にとどまるものです。今後は欧州議会及び理事会における数年間の立法手続に服することになるため、現在の文言から大きな変更を伴う修正が行われる可能性も否定できません。他方で、日本はソフトローを選択し

ましたが、今後世界各国で展開されるであろうAI規制の議論の出発点の一つになる可能性があり、その影響を軽視できるものではありません。EUにおける議論の進展と同時に、世界各国の議論状況に注意を払う必要があります。