知財法務の勘所Q＆A（第72回）

ChatGPT登場後のAI周辺のルール、世界各国の規制動向は？

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９月の記事において、EUのAI規則案を中心に、AI周辺をめぐるルールの動向を紹介しました。その後、2022年後半のChatGPTの登場でAIをめぐる情勢は大きく変わっており、国内外でAI規制に向けた動きがいよいよ本格化しています。AI規制の先端を走ってきたEUでは、AI規則案がいよいよ制定間近になっているほか、これを補完する法制として、AI責任指令案、製造物責任指令の改正案の準備が進められています。EUのほかにも、米国、英国、シンガポールでAI規制の議論が進められてきましたが、ChatGPTをはじめとする生成系AIへの規制の必要性が世界中で議論されるようになって以後、AI規制の導入に向けた潮流は世界各国で見られるようになっています。本稿では、生成系AI規制を含め、今まさに激しく動きつつある世界各国のAI規制の動向を紹介していきます。

Q1　そもそもEUのAI規則案とはなんでしょうか。

A1　いわゆる「AI規則案」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」に近いものとお考えください。

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

Q2 2021年の公表後、AI規則案をめぐって、EUではどのような動きがありましたか。

A2 2021年４月のAI規則案の公表後（「当初案」といいます）、パブリックコンサルテーションの手続きが実施され、300を超える意見がEUのみならず世界中の事業者・団体から寄せられました。

寄せられた意見を踏まえ、2021年11月29日付けのAI規則案の修正案が公開されました。同修正案では、当初案の理念は維持しつつも、国家安全保障、研究開発における汎用AIシステムを免除の対象とすること、保険におけるAIの使用は高リスクにあたることの説明、私的領域におけるソーシャルスコアリングの禁止の拡張等の重要な変更が加えられていました。

その後、2022年６月には、欧州理事会がAI規則案の進捗報告書を採択し、欧州議会内の消費者委員会（IMCO）と内務委員会（LIBE）の合同名義で全体的な修正案が提示されました。これらの修正案では定義の明確化、GDPRなど既存法令との調和等が求められました。

そして、2023年５月には、欧州議会の委員会審議において、生成系AIの登場を踏まえて、再び大幅修正されたAI規則案が賛成多数で採択されています（「議会案」といいます）。

さらに、AI規則案を補完するルールとして、欧州におけるAIシステムの提供・利用に関する法的責任に関する規律の基本ルールを定めるべく、2022年９月28日、AI責任指令案（Proposal for an Artificial Intelligence Liability Directive（AILD））及び製造物責任指令（Product Liability Directive(PLD))の改正案が公表されています。AI責任指令案及びPLD改正案に定める事項は、2023年６月から適用されるEUの集団訴訟指令（Representative Actions Directive）の対象となるため、関連サービスを提供する事業者にとって重要なルールになると考えられています。

Q3 AI規則の対象となるAIシステムとは何ですか。

A3 当初案においては、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、定義が広すぎるのではないかという批判があり、議論がなされていました。議会案では、再び定義の拡大が試みられ、「様々なレベルの自律性を持って動作するように設計され、明示的または暗黙的な目的のために、物理的または仮想的環境に影響を与える予測、推奨、決定などの出力を生成できる機械ベースのシステム」と定義されています。

Q4 AI規則が適用されるのはどのような事業者でしょうか。

A4 議会案においては、AI規則が適用されるのは、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。

ここでいう「プロバイダー」とは、「AIシステムを開発するか、自らの名または商標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。「ユーザー」については「プライベートで個人的に(non-professional)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、いわゆるエンドユーザーを指すものではありません。いずれも、自然人、法人、公的機関、代行機関、その他の団体が含まれます。

Q5 AI規則案は最終的にどうなりそうでしょうか。

A5 2023年５月の 欧州議会の委員会審議において、2000件以上の修正が加えられ、大幅に修正された議会案が賛成多数で採択されています。議会案においても、AIをリスクのレベルに応じて、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るという基本的な枠組みが維持されています。

委員会審議では、ChatGPTをはじめとする生成系AIの飛躍的進歩を受け、特に生成系AIに関する条項が付け加えられました。まず、生成系AIは、市場に投入される前に特有のルールに従わねばならないと定められています。また、違法コンテンツ対策や、著作権で保護されたデータがアルゴリズム開発に用いられた場合にはそれを公表することも定められています。これにより、著作権者は著作権料の支払いを求めることが可能となるとされています。

もう一つの大きな変更が、「高リスク」と見なされるAIの対象の拡大です。具体的には、健康、セキュリティ、基本的人権及び環境への影響が懸念されるAIに加え、有権者の投票行動に影響を与え得るAI、ユーザーが4500万人を超えるSNSのレコメンド機能に用いられるAIも含められることになりました。これらのAIは、より厳しい透明性及びガバナンス義務の下に置かれることになります。

許容できないリスクを伴うAIについては、AIを用いて一定の行為を行うことが禁止されますが、一方、禁止される行為としては、一般市民に対する評価や公衆に対する監視のみならず、職場や教育現場及び移民管理の場面における感情認識技術の使用、公共の場における顔認識をはじめとするバイオメトリクス技術を利用した、リモートでの人物特定も含まれることとされました。また、警察によるAIを利用した犯罪予測や、顔認識技術向けデータベース構築のためのインターネット上での画像の大量収集も禁止することと定めています。

AI規則案については、さらにいくつかの審議が予定されており、発効が2023年後半にずれこむと予想されています。適用開始時期については、規定上、発効から２年後とされているため、適用開始は、早くとも2025年以降になる可能性が高いと予測されています。

Q6 製造物責任指令改正案ではどのようなルールが定められたのでしょうか。

A6 1985年に施行された現行の製造物責任指令においては、消費者が欠陥のある製造物により損害を被った場合の製造事業者などの民事責任を規定しているところ、デジタル化に十分対応できておらず、被害者の実効的な救済を妨げているとして改正の必要性が指摘され

てきたところです。

製造物責任指令改正案では、「製造物」にソフトウェアが含まれることとされたため、AIシステムも製造物責任の対象に含まれることになりました。すなわちAIシステムに欠陥があれば、システム開発者に対して、無過失責任を追求することができるようになります。欠陥の有無の判断に際して、設置後に継続学習できる能力やサイバーセキュリティー対応等に必要なソフトウェアのアップデートが加えられています。

製造物責任を負う事業者には、従来の製造事業者、EU域内の輸入事業者（製造事業者が域外で設立されている場合）などに加えて、認定代理人や、場合によっては、オンライン上のマーケットプレイスなどの販売事業者も含まれる点も注意が必要です。これは、越境EC、すなわち消費者がEU域外から製品を直接購入することが増えていることから、こうした消費者の効果的な救済をより容易にすることを目指したものと説明されています。被害者が域内の事業者を特定できない場合で、かつ販売事業者がこれらの事業者を特定しない場合、販売事業者が製造物責任を負うことになります。

また、より実効的な救済を確保するために、被害者は裁判所に対して製造事業者などに情報開示を請求することができることとされました。さらに、立証責任についても一定の緩和が図られています。まず、裁判所が技術的な複雑性などにより製品の欠陥や欠陥と損害の因果関係の立証が過度に困難であると判断した場合に、被害者が製品の欠陥や欠陥と損害の因果関係を完全に立証していない場合であっても、以下の立証をしていれば、裁判所は製品の欠陥や損害との因果関係、あるいはその両方が推定されなければならないというルールです。あくまで推定であり、みなしではないため、製造事業者には、反証が認められています。

・製品が損害の一因となっていること、かつ
・製品に欠陥があり、または製品の欠陥が損害のあり得べき原因となっている可能性があること

また、以下の要件のいずれかに該当する場合、製品に欠陥があることが推定されなければならない、というルールも設けられています（こちらも、推定であり、みなしではないため、反証可能です）。･被告が証拠開示命令に従わない。

・製品が所定の義務的安全性要件を遵守していないことが立証されている。
・製品の通常の使用時において、製品の明白な誤動作によって損害が発生したことが立証されている。

加えて、Q7で紹介するAI責任指令案と同様の因果関係の推定規定も導入されています。

Q7 AI責任指令案ではどのようなルールが定められたのでしょうか。

A7 製造物責任指令改正案はAIシステムも適用対象としているものの、AIシステムはその複雑性やブラックボックス問題により、その欠陥や因果関係を立証することが特に困難かつ高額であるという特有の問題状況が指摘されてきたところです。また、製造物責任指令改正案では、救済対象が、安全性が不十分であることから生じた損害に限定されるという限界があります。このため、AI責任指令案を新たに定め、より充実した被害者救済を図ることを目指すものとされています。

加えて、AI責任指令案においては、AIシステムの関与によって生じた損害に対する契約外の民事責任の特定の側面について統一的なルールを定めることで、EU域内の市場機能を向上させることも重要な目的であるとされています。

AI責任指令案が適用されるのは、AIシステムによって生じた損害に関する、契約外の事由による過失に基づく民事上の損害賠償請求であり、典型的には、不法行為責任などの各加盟国の国内法における過失を基礎とする責任などが想定されています。たとえば、AI技術を利用した採用活動においてしばしば指摘される差別的な取り扱いに伴う損害の賠償責任が考えられます。

証拠開示についてAI責任指令案では、高リスクのAIシステムにより損害が生じた疑いがある場合に、裁判所は、被害者の申立を受けて、当該システムの提供者等に対し、関連性のある証拠の開示･保全措置を講じるよう求めることができるとされました。もっとも、このような証拠の多くは企業秘密に該当することも多く、事業者側にも相応のリスクが発生する可能性があります。このため、裁判所が証拠の開示または保全を命令する場合、必要かつ相当な範囲に限定することが求められるとともに、開示･保全措置を実行するに際しては種皮性を保持するための措置を講じる必要があります。これらの開示･保全措置命令に従わなかった場合、被告の注意義務違反が推定されることになります（推定なので反証可能）。

また、AIに関連して損害賠償を求めようとすると、AIの出力と、AIシステムの提供者の過失との間の因果関係の立証が困難であるというハードルの高さが指摘されているところ、AI責任指令案では、損害が発生した際、特定の条件下において、AIシステムの出力（または出力できなかった事象）が、AIシステムの提供者の過失によって生じたと推定することが可能とされました。具体的には、以下の要件をすべて充足する場合、被告の過失とAIシステムによって生成された出力結果または出力結果が生成されなかったこととの間の因果関係が推定されることになります。

・注意義務違反からなる被告の過失の立証
・被告の過失が、AIシステムによって生成された出力結果または出力結果が生成されなかったことに影響を与えたことが合理的にあり得ること
・AIシステムによって生成された出力結果または出力結果が生成されなかったことに起因する損害の発生の立証

このうち「注意義務違反からなる被告の過失の立証」要件については、当該AIシステムが高リスクAIシステムである場合、被告の属性に応じて認められやすくなる場合があります。

加えて、「高リスクAIシステム」であるか否かによって、推定規定の適用可能な場面がことなってくるため、高リスクAIシステムを取り扱う事業者は、大きなリスクを事実上負うことになっています。

Q8 EU以外のAI規制の動向を教えてください。

A8

1．米国

2022年10月に米国科学技術政策局（OSTP）より「AI権利章典の青写真」が発表され、AIシステムの設計、使用、導入の際の指針となる５つの原則（①安全かつ有効なシステム、②アルゴリズムから生じる差別からの保護、③データのプライバシー、④告知と説明、⑤問題発生時の人間による代替、検討、対応）が提示されています。その後、ChatGPTの世界的なブレイクを踏まえ、2023年４月には、米国商務省が生成系AIついて安全性の保証を求め、リスク対

策の正式な意見公募を開始しており、米国政府の積極的な規制に向けた姿勢転換の兆しではないかとも言われており、要注目です。

なお、規制そのものではありませんが、2023年３月に、米国著作権局はAI生成コンテンツの著作権は認めない方針を発表しており、AI生成コンテンツの法的保護に関する世界の議論に大きな影響を与えています。

２．英国

英国政府からは、「AI規制政策文書」が2022年７月に発表され、AIの特性に合わせた分野横断的な原則に基づき、AI規制に向けた革新的なフレームワークを確立するよう提言が行われた。先行して2021年12月には、英国データ倫理・イノベーションセンター（CDEI）より、「効果的なAI保証エコシステムに向けたロードマップ」が発表され、効果的で成熟したAI保証エコシステム実現のための６つの優先分野（①AI保証の需要喚起、②AI保証の市場構築、③標準化、④専門機関の設置、⑤規制、⑥独立した調査研究）が提示されています。直近では、2023年３月に、英国政府からAI白書が発行されています。ここでは、AI業界に対し「責任ある使用」を求める一方で技術革新を阻害する「強引な法律」の導入は避ける旨の方針が示されています。

３．中国

2023年４月11日、国家サイバースペース管理局より、「生成型人工知能サービス管理弁法（意見募集案）」に関するパブリックコメントの募集案内の通知が行われています。同法案は全21条からなり、以下の内容を定めており、2023年中の施行が予定されています。

・生成系AIから生み出されるコンテンツには、反政府、テロリズム、差別、わいせつ、虚報等が含まれないようにする措置を講じること
・虚偽情報の生成を防止するための措置を講じること
・公衆にサービスを提供する前に、「世論属性や社会動員力を持つインターネット情報サービスのセキュリティ評価規定」に基づき、国家インターネット情報部門にセキュリティ評価を申告し、「インターネット情報サービスのアルゴリズム推奨管理規定」に基づき、アルゴリズムの申告等の手続を行うこと
・生成された写真や動画などのコンテンツには「インターネット情報サービス深層合成管理規定」に基づき、それと判別できるようマークを付すこと

従前の中国特有のインターネット規制を、生成系AIにも拡大する内容になっています。

４．韓国

2023年２月、韓国政府の文化観光体育部は、生成系AIの学習における著作権問題も含め、AI時代に対応する新たな著作権制度の在り方を検討すべく、「AI著作権法制度改善ワーキンググループ」を発足しました。同ワーキンググループでは、2023年９月まで、「AI学習データに使用される著作物の円滑な利用方法」「AI生成物の法的地位の問題と著作権制度での認定の可否」「AI技術の活用時に起きる著作権侵害とこれに対する責任規定」等が議論される予定です。

まとめ

AI規則案の実際の施行は早くても2025年と予想されていますが、加えて、今後のAIとりわけ生成系AIの発展状況によっては、より厳格な規制が、より広範な法域で導入されることが懸念されます。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るのは

間違いありません。

以　上