

AIエージェント利用者に求められるAIガバナンス

——「AI利活用における民事責任の解釈適用に関する手引き」から読み解く法的リスク低減の視点

PwC弁護士法人
パートナー代表 **北村 導人**
PwC弁護士法人
パートナー **山田 裕貴**

PwC弁護士法人
弁護士 **黒瀧 海詩**
PwC弁護士法人
弁護士 **高松 礼奈**

PwCコンサルティング合同会社
トラストコンサルティング事業部
パートナー **橋本 哲哉**

はじめに

近時、複雑な業務プロセスの自動化・効率化を目的として、AIエージェントなどの高度なAIシステムの活用が進みつつあります。AIエージェントは、総務省および経済産業省が公表する「AI事業者ガイドライン（第1.2版）」^{※1}（以下、「AI事業者ガイドライン」）本編11ページにて、「特定の目標を達成するために、環境を感知し自律的に行動するAIシステム」と定義されているとおり、人間による個別の入力や指示を前提とせず、環境を感知し、一定の範囲で自律的に処理を進める点に特徴があります。こうしたAIのうち、人がその判断に依拠しながら用いることが予定されているもの（依拠／代替型AI）については、人の判断や行動を前提としてきた従来の不法行為責任^{※2}判断の枠組みでは捉えられないリスクをどのようにコントロールするかが重要な課題となります。

この課題に対する基礎的な考え方を提示するものとして、経済産業省は、2026年4月9日、「AI利活用における民事責任の解釈適用に関する手引き」[第1.0版]^{※3}（以下、「本手引き」）を公表しました。本手引きは、AIを用いたサービスやシステムが事故に寄与した基本的な想定事例を題材に、主として不法

行為法などの観点から、AI利活用の場面における解釈適用上の論点および考え方を整理し、現行法がどのように適用され得るかの方向性を示すものです。本手引きでは、AIエージェント利用者が、不法行為に基づく損害賠償責任リスクを低減するために講じるべき措置について一定の示唆が提示されており、AIエージェントの利活用を検討中の事業者であれば把握しておくべき資料と言えます。

本稿では、本手引きを踏まえ、依拠／代替型AIに該当するAIエージェントを利用する事業者の責任判断の枠組み、そして、不法行為責任リスクを低減するためのAIガバナンス構築のポイントを概説します。

なお、文中の意見は筆者らの私見であり、PwC弁護士法人およびPwCコンサルティング合同会社ならびに所属部門の正式見解ではないことをお断りします。

1 依拠／代替型AIに該当するAIエージェント

本手引きは、AIの利活用に関する各当事者の責任判断にあたり、AIの利用形態を以下の2類型に整理して検討する手法を提示しています。

- **補助／支援型AI**：AI利用者の判断の補助ないし支援としてのみ用いられ、最終的に人の判断や行動を介在させることが予定されている類型
- **依拠／代替型AI**：人の判断や行動の全部または一部を代替する前提で提供され、AIの判断に依拠しながら用いることが予定されている類型

※1 総務省のウェブサイト「AI事業者ガイドライン」掲載ページ（https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html）および経済産業省のウェブサイト「AI事業者ガイドライン」（https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20260331_report.html）参照。

※2 故意または過失によって他人の権利または法律上保護される利益を侵害した場合、それによって生じた被害者の損害について、賠償する法的責任（不法行為に基づく損害賠償責任）が生じます（民法第709条）。

※3 経済産業省のウェブサイト「AI利活用における民事責任の解釈適用に関する手引き」を公表しました」（<https://www.meti.go.jp/press/2026/04/2026040901/20260409001.html>）参照。

AIエージェントであればただちに依拠／代替型AIに該当するというものではなく、依拠／代替型AIに該当するかは、人による判断や行動を介在させるだけでは実現困難な効用が見込まれること（必要性）と、AIが一定の精度や安全性を備えていること（精度および安全性）の2つの要件で判断するとされています。

例えば、カスタマーサポート業務を自律対応するAIエージェントが、休日・深夜帯の柔軟な対応など、人手のみでは実現しがたい効果をもたらす場合には、「必要性」の要件を満たし得ると考えられます。そして、当該AIエージェントが、同種業務に従事する通常人の作業水準と比較して同等以上の精度や安全性を備えている場合には、「精度および安全性」の要件も満たし^{※4}、依拠／代替型AIに該当し得ると考えられます。

2 依拠／代替型AIエージェントの利用者の責任判断構造とAIガバナンス

(1) 依拠／代替型AI利用者の責任判断の枠組み

依拠／代替型AIでは、最終的な人の判断や行動の適切性が論点となる補助／支援型AIとは異なり、①AI利用者がAIシステムを組み入れた業務プロセスを適切に「構築」し、②AIの望ましくない出力が権利侵害や損害を生じさせる可能性を低減するため合理的に可能な「運用」を行っていたかが、過失^{※5}判断の対象になるとされています。そして、これらの観点においてAI利用者が適切な措置を講じていた場合には、AIが個別の場面で不適切な出力をしたとしても、その全てを検証して是正するまでの結果回避義務は負わないとされています。

① AIシステムを組み入れた業務プロセスの「構築」に関する注意義務

対象業務がAIによる自動化に適しているか、その業務に求められる水準の精度・安全性を備えたAIシステムを用いているかなどが問題となるとされています。また、AIのリスクを踏まえて適切な利用体制やガバナンスの構築を行っているかも重要な要素とされています。例えば、特定条件下で精度が低下する場合などには、業務プロセス

全体として望ましい精度・安全性を確保するために必要な人の関与を介在させることなどが注意義務の内容となり得ると考えられます。

② 構築した業務プロセスの「運用」に関する注意義務

AIの望ましくない出力により権利侵害が生ずる可能性を低減するため、AI利用者がシステムの運用において合理的な措置を講じていたかが問題となるとされています。例えば、AIは継続学習やアップデートにより事後的に精度などが変化し得るため、運用過程で精度が低下し、依拠／代替型AIとしての運用に適しない状態となっていないかを確認することのほか、誤出力のフィードバックおよびこれを踏まえたアーキテクチャの改善や、当該出力がAIによるものであり、誤りを含む可能性がある旨の表示などが注意義務の内容となり得ると考えられます。

(2) AI事業者ガイドラインなどを踏まえたAIガバナンス構築の重要性

AIシステムを組み入れた業務プロセスの「構築」と「運用」において、具体的にどのような措置を講じるべきかについて、本手引きは、AI事業者ガイドラインが示す、AIの利活用に伴うリスクをコントロールするためのガバナンスの内容を参考にして、合理的に可能な措置を講じることが考えられるとしています。例えば、2025年度に行われたAI事業者ガイドラインの「別添5.AI利用者向け」の更新の際には、AI利用者が留意すべき事項に関する具体的なアプローチとして、以下の措置などが追記されました。

● ログの定期的な確認

- ▶ システム利用状況や異常操作を把握するため、ログを定期的にレビューする
- ▶ 異常な操作を検知した場合に即時報告する体制を整備する

これは、AIエージェントが自律性を持って行動するため、定期的な操作履歴の確認や報告が重要であることを踏まえたものです^{※6}。こうした措置を参考にリスクに応じたAIガバナンスを構築することは、依拠／代替型AIエージェントを利用するうえで、不法行為責任リスクを低減

※4 消費者の重要な利益に関わる説明などを行う場面では、消費者保護の観点から高度の注意義務が認められやすく、依拠／代替型AIに求められる水準も高まるとされている点に留意が必要です。

※5 前記注2のとおり、不法行為に基づく損害賠償責任の発生には少なくとも「過失」が必要ですが、「過失」は、法的な注意義務（損害の発生を予見し得たこと（予見可能性）を前提とした、損害の発生を回避する規範的な義務（結果回避義務））の違反があった場合に認められます。

※6 総務省・経済産業省「AI事業者ガイドラインの令和7年度更新内容」（令和8年3月12日AIネットワーク社会推進会議（第32回）・AIガバナンス検討会（第30回）合同会議（https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02tsu shin06_04000138.html）【資料2】）参照。

する対応として重要と考えられます。

一方で、本手引きでは、AI事業者ガイドラインについて、そこに記載された事項を全て遵守することが求められるものではなく、また、各場面に即して求められる措置が網羅的に記述されているわけではないとされている点にも留意が必要です。以下は筆者らの私見ですが、依拠／代替型AIエージェントの利用者に課せられる注意義務は、個々の状況に応じて不法行為法の観点から定まるものであることに加え、不法行為責任リスクが顕在化するの訴訟などの紛争に至った段階です。そのため、不法行為責任リスクを低減するうえでは、AIガバナンスの構築に際し、AI事業者ガイドラインのみに依拠することは十分と言いがたいように思われます。裁判例^{※7}を含む不法行為法の知見や立証・和解などの訴訟・紛争実務の知見も踏まえ、どのような措置をどこまで講ずるかを個別具体的に検討することが肝要と考えます。

※7 本手引きでは、AIの自律性やブラックボックス性を踏まえた、既存の民事責任ルールの解釈適用について裁判例の蓄積はないとされている一方で、依拠／代替型AIを利用する際の責任判断の枠組みについては、預金払戻しシステムに係る裁判例を踏まえて検討されています。このように、直接の裁判例がなくとも、当該事案と一部共通点を有する裁判例を参照することは、個々の状況に応じたAIガバナンスの構築にあたって有効なアプローチとなり得ると考えられます。

北村 導人 (きたむら みちと)

PwC弁護士法人 パートナー

2000年弁護士登録、1996年公認会計士登録。大手法律事務所を経て、2016年にPwC弁護士法人にパートナーとして入所、2020年より同法人パートナー代表。企業法務、サステナビリティ（ビジネスと人権を含む）、税務などの分野を専門とし、AIと人権（差別、プライバシー、自己決定権など）の観点からAIガバナンス領域も扱う。

メールアドレス：michito.kitamura@pwc.com



山田 裕貴 (やまだ ひろき)

PwC弁護士法人 パートナー

2008年弁護士登録、2016年米国ニューヨーク州弁護士登録。大手法律事務所を経て、2017年にPwC弁護士法人に入所、2022年より同法人パートナー。個人データ・プライバシー保護対応、パブリックセクター案件、M&A その他各種企業法務の案件を取り扱う。

メールアドレス：hiroki.yamada@pwc.com



黒瀧 海詩 (くろたき かいし)

PwC弁護士法人 弁護士

2019年弁護士登録。大手法律事務所、国内法律事務所を経て2024年にPwC弁護士法人に入所。情報法、知財、ヘルスケア分野に注力しており、AI導入に関するものも含め、個人データ・プライバシー保護対応や特許・著作権・営業秘密といった知財取引などの案件を扱う。



3 おわりに

以上のとおり、依拠／代替型AIエージェントの利用にあたり、不法行為責任リスクを効果的に低減するためには、本手引きが指摘するAI事業者ガイドラインの知見に加え、不法行為法の知見や訴訟・紛争実務の知見も踏まえてAIガバナンスを構築することが必要と考えられます。

AIエージェントの利活用を、リスクを理由に控えるのではなく、リスクを適切にコントロールしつつベネフィットを最大化するための仕組みを早期に設計し、改善を重ねていくことが、今後の重要な競争力になると考えます。

PwC Japanグループでは、PwC弁護士法人（第一東京弁護士会所属）やPwCコンサルティング合同会社をはじめとしたメンバーファームが協働することで、こうした法的知見・弁護士実務知見と、AI活用状況の現状把握、リスク評価、ポリシー・ガイドラインの策定、AIガバナンス実施体制の構築、モニタリングプロセスの策定といったコンサルティングサービスを組み合わせ、法的リスクにも対応したAIガバナンス構築を一貫して支援することが可能です。

高松 礼奈 (たかまつ れな)

PwC弁護士法人 弁護士

2020年弁護士登録。国内法律事務所を経て、2021年にPwC弁護士法人に入所。個人データ・プライバシー保護対応、知的財産、M&A その他各種企業法務の案件を取り扱うほか、AI・リーガルテック分野にも注力する。



橋本 哲哉 (はしもと てつや)

PwCコンサルティング合同会社 トラストコンサルティング事業部 パートナー

外資系ITベンダーを経て、2015年にPwCコンサルティング合同会社に入社。2022年よりAIガバナンス領域のリードを担う。官公庁を含む多業種において豊富なAIガバナンスプロジェクトの経験を有する。サイバーセキュリティや事業継続、デジタル関連規制対応などの幅広い案件を取り扱う。

メールアドレス：tetsuya.hashimoto@pwc.com

