masuda funai

News & Types: 知的財産関連情報

エージェント型AIの出現：イノベーションと法的リスクにおけるニューフロンティアとなるか

9/29/2025

By: マイケル ゴーレンソン

Practices: 知的財産テクノロジー

人工知能（以下「AI」といいます）が進化を続ける中で、新たなAIシステムの類型として「エージェント型AI（agentic AI）」が登場しました。それは企業の事業運営の在り方を大きく変革する可能性を秘めています。従来型のAIシステムや生成AIが入力された内容に受動的に反応するのとは異なり、エージェント型AIは、人間の関与をほとんど、あるいはまったく伴わずに、主体的に行動し、意思決定を行い、目標を追求するよう設計されています。これらのAIエージェントは複数の工程を要するタスクを計画・実行し、ソフトウェアやAPIと相互作用し、さらにはタスクの一部を他のエージェントに委任することさえ可能です。その自律性は、企業にとって大幅な効率性の向上や新たな可能性をもたらす一方で、前例のない運用上、倫理上、法律上の課題をも生じさせます。

エージェント型AIの重要性を理解するためには、生成AIとの対比が有益です。生成AIとエージェント型AIの主要な相違は、自律性の程度と機能にあります。大規模言語モデルや画像生成モデルに代表される生成AIは、ユーザーのプロンプトに直接応答してテキスト・画像・コード等のコンテンツを生成するものであり、主体性を持たず、タスク間のメモリーもない、反応するだけのツールとして機能します。これに対し、エージェント型AIは、生成AIの能力を基盤とし、さらに自律性、目標指向性、意思決定能力をも備えたものです。エージェント型AIは複数の工程にわたって計画・実行・修正を行うことが可能であり、最小限の指示で目的を達成するためにしばしばツールやAPI、外部システムを活用します。例えば、市場参入戦略の調査を命じられたエージェント型AIは、ユーザーの継続的な指示がなくとも、自律的にデータを収集し、競合分析を行い、報告書を作成し、そのアウトプットの修正を行うことができます。この静的な生成から動的な主体性への転換は、きわめて大きな技術的飛躍を意味します。

しかし、エージェント型AIを強力にする、その自律性こそが、企業にとって多岐にわたる重大な法的リスクをもたらします。例えば、責任の問題から見ていくと、AIエージェントが有害な意思決定を行ったり、過失を犯したり、契約に違反した場合、もし責任を問われる誰かがいるとすれば、誰がその法的責任を負うのかが依然として不明確です。もう一つの重大な課題はデータガバナンスです。自律的なエージェントが適切な監督を欠いたまま機密データへアクセスしたり、あるいは機密データの処理や転送を行えば、EU一般データ保護規則（GDPR）、カリフォルニア州プライバシー権法（CPRA）、医療保険の携行性と責任に関する法律（HIPAA）といったプライバシー規制に違反するおそれがあります。加えて、AIエージェントが第三者の知的財産権を

意図せずに侵害し、あるいは機密データを誤って利用して、コンテンツを生成した場合には、知的財産に関する懸念も生じます。

これらの主要なリスクに加えて、エージェント型AIは、（i）自律的システムによって成立した契約の有効性、（ii）偏見や差別的結果が生じる可能性、（iii）サイバーセキュリティ上の脆弱性、（iv）クロスボーダー規制の抵触、（v）監査能力の欠如による財務報告義務及び業務報告義務違反の可能性、といった多様な法的問題を提起します。 これらの課題に対応するためには、企業環境において、エージェント型AIの安全かつコンプライアンスに準拠した導入を可能にする積極的な法的枠組みと内部的な安全対策が必要となります。

これらの課題を踏まえると、エージェント型AIを導入しようとする組織は慎重な対応を取らなければなりません。企業は、エージェントの行動を監視し、重要なシステムへの自律的アクセスを制限し、意思決定の追跡可能性を確保するために、強固なガバナンス体制を整備する必要があります。また、AIベンダーとの契約上の明確性を確保し、厳格なリスク評価を行い、新たに策定されつつあるAI規制に積極的に対応することが不可欠となります。

本稿の内容に関してご質問がございましたら、著者または増田・舟井法律事務所の知的財産テクノロジー部門のメンバーまでお問い合わせください。

増田・舟井法律事務所は、米国でビジネスを展開する日本企業の代理を主な業務とする総合法律事務所です。

当事務所は、シカゴ、デトロイト、ロサンゼルス、およびシャンバーグに拠点を有しています。