2025 年 3 月 5 日

AI エージェント、Web 3 AI エージェントと日本法

創・佐藤法律事務所
弁護士　斎藤　創
同　浅野真平

本稿では 2025 年に入り急激に盛り上がりを見せる AI エージェントについて、(1)AI エージェントとは何か、(2)特にその中でも Web 3　AI エージェントとは何か、を紹介した上で、(3)AI エージェントに関連する法的論点を記載します。

AI エージェントはあらゆる業務に代替し得るため、AI エージェントと法律の関係を考える場合、本来は、AI エージェントが行うあらゆる業務について法的問題点を検討する必要があります。しかし、blog でそれを網羅することは難しいため、本稿では、AI エージェントの法的問題点を検討する際の基本的な考え方を紹介した後に、規制との関係では特に金融規制を中心に議論しています。ただ、この金融規制に関する考え方は他の AI エージェントに関する法的論点を検討する際にも、一定程度参考になると考えています。

Ⅰ　AI エージェントの概要

1　AI エージェントとは何か

AI エージェント(AI Agent)は、一般に「特定のタスクを自律的に遂行する人工知能システム」を指します。人間が指示を出さなくても、環境からデータを処理し、必要に応じて学習や意思決定を行い、タスクを実行することが可能です。

一般に AI エージェントは、以下の要素を備えています。

① 認識: 外部環境や入力データを処理し、現在の状況を理解。
② 意思決定: データに基づき、タスクを遂行するための行動を計画。
③ 行動: 計画に基づいて環境に変化を与えるアクションを実行。
④ フィードバック: 実行結果を学習に活用し、次回の行動を改善。

これにより、AI エージェントは人間の代わりに反復作業を行ったり、複雑な判断をしたりすることが可能です。

現在、AI エージェントは、私たちの生活やビジネスを変革する存在として、非常に注目を集めています。

AI エージェントは例えば下記のような用途で使用されることが期待されています。

AI エージェントの使用例

(1) ジェネレーティブ AI を活用した創造性の支援

文章や画像、動画、音楽の生成など、クリエイティブ分野での活用。メディア、広告、

ゲーム業界では、制作の効率化や新たな価値創出が期待されます。

(2) パーソナルアシスタント

ライフコーチ、教育支援、ビジネスアシスタントなど、個人のニーズに応じた支援が可能。スケジュール管理や健康アドバイスなど、日常生活をより効率的にする用途が注目されます。

(3) 金融分野での自律的な活用

資産運用や家計管理を支援する AI エージェントは、データを活用して最適な投資戦略や節約方法を提案します。分散型金融(DeFi)でも、自動化された取引や資産管理が進んでいます。

(4) 業務プロセスの自動化

人事や財務、顧客対応などの反復的なタスクを自動化することで、企業の生産性向上に寄与します。また、データ解析や意思決定支援も、AI エージェントの得意分野です。

(5) ヘルスケア

AI エージェントは、健康管理や遠隔医療、疾患予測などに活用されます。特に、症状の解析やメンタルヘルスのサポートなど、個人に寄り添ったサービスが期待されます。

(6) 自律型システム

倉庫管理や物流、災害対応などにおけるロボットの自律化、自動運転やドローン操作など、物理的なタスクを担う AI エージェントの活躍が期待されます。

AI エージェントは、個別化と自律性を強みに、私たちの生活をより豊かに、ビジネスをより効率的にする可能性を秘めています。これらの用途は、今後さらなる進化が期待される分野です。

2 AI エージェントの具体的な例

AI エージェントの国内外での具体的な活用事例として、以下のようなものが挙げられます。

サービス名	提供者	特徴
Fujitsu Kozuchi AI Agent	富士通株式会社	人と協調して自律的に高度な業務を推進する AI エージェント。例えば、会議エージェントとして AI が自ら会議に参加して情報共有や施策の提案をしたり、現場支援エージェントとして製造や物流の現場でカメラ映像を分析して改善提案をしたり作業レポートを作成します。
Agentforce	Salesforce, Inc.	自律型の AI アシスタント。例えば、Agentforce の一つである Service Agent は、従来のチャットボットを自律型 AI に置き換え、事前にシナ

		リオをプログラムしなくても、24 時間 365 日顧客と正確で流暢な会話を行います。
Operator	OpenAI, Inc.	AI がユーザーに代わってウェブブラウザを操作し、日常的なタスクを自動化。ユーザーの指示に従って独自のブラウザを使用してウェブページを閲覧し、入力、クリック、スクロールなどの操作を実施。それにより、例えば、レストランの予約やオンラインショッピングなどを自動化。
Pactum AI	Pactum AI, Inc.	Walmart では、自律型交渉 AI である Pactum AI を導入し、10 万社超のサプライヤーとの交渉を自動化。サプライヤーからの要求に対し、あらかじめ指示された予算額と優先事項に従って自動で提案を行い、Walmart とサプライヤーの双方にとって最適な取引条件を導きます。
Waymo Foundation Model	Waymo LLC	自動運転タクシーを運営する Waymo は、独自開発の Waymo Foundation Model と呼ばれる AI モデルを用いて、周囲の状況理解から運転計画の生成まで、高度な判断を可能にしています。

3 Web3 AI エージェント

AI エージェントは Web3 とも親和的と言われています。Web3 と AI エージェントの統合は、以下のような新しい可能性を生み出すと考えられます。

Web3 AI エージェントの使用例

(1) 分散型 AI エージェント

- **スマートコントラクトとの統合**:
  AI エージェントがブロックチェーン上のスマートコントラクトを操作し、自律的にトランザクションを実行。例えば、不動産取引や金融取引を仲介者なしで完了。
- **自律分散型組織(DAO)の一部として活動**:
  AI エージェントが DAO 内で意思決定プロセスに参加し、提案や投票を実施。

(2) ユーザー主権の強化

- **プライバシー保護**:
  AI エージェントがユーザーのデータをローカルで処理し、個人情報を分散型ストレージ(例：IPFS)に安全に保存。

- **自己所有データ(Self-Sovereign Identity, SSI)**:
  AI エージェントがユーザーの SSI を活用して、Web3 サービスへのアクセスや認証を簡素化。

(3) トークンエコノミーの自動化

- **トークン取引の自動化**:
  AI エージェントが分散型取引所(DEX)でユーザーの代わりに資産を管理・取引。
- **報酬の分配**:
  AI エージェントが Web3 プラットフォーム上で生成した価値に応じてトークンを受け取り、再分配。

(4) メタバースと AI エージェント

- メタバース内で AI エージェントがバーチャルアシスタントとして活動。例えば、ユーザーのために土地を管理したり、NFT を取引。

(5) ゼロ知識証明(ZKP)の活用

- AI エージェントが ZKP を用いることで、プライバシーを守りつつ Web3 アプリケーション上で信頼を提供。

なお、Web3 AI エージェントが世界的に大きく話題になった例として AI16Z(ai16z)があります。ai16z は、Solana ブロックチェーン上に構築された分散型 AI 投資ファンドであり、AI エージェントを活用して自律的に投資活動を行うプロジェクトです。

プロジェクト名: ai16z
基盤: Solana ブロックチェーン
特徴:

- AI が市場情報を収集・分析し、コミュニティのコンセンサスを考慮して自動的にトークン取引を実行。
- 投資家がトークンを通じてプロジェクトの運営や意思決定に参加可能できる分散型ガバナンスを採用。
- ブロックチェーン技術により、投資活動の透明性と信頼性を確保。

AI エージェント「Eliza」:

- 投資戦略の立案や実行を担当する AI エージェント。
- オープンソースとして公開されており、第三者による展開も可能。

ai16z という名称は、シリコンバレーの著名 VC である Andreessen Horowitz(a16z)をもじって命名されたものですが、ai16z と a16z は無関係です。

しかし、2024 年 10 月 27 日に a16z 創業者の一人であるマーク・アンドリーセン(Marc Andreessen)が X(旧 Twitter)で「GAUNTLET THROWN(挑戦状)」と投稿したり、ai16z の

メインアバターが来ているTシャツについて言及したりしたことにより、ai16zの名は一気に拡散しました[1]。

更に、 2024年1月初めには、ai16zの時価総額は一時3000億円を超え3か月で100倍以上の成長を遂げました。そのような事情もあり、2025年1月初頭時点では世界的に大きな話題になり、日本のX(旧twitter)でもAIエージェントの中心的な話題となっていました。

ただし、期待が大きすぎた等の理由によるのかもしれませんが、その後、価格が大幅に下落し、時価総額が 500 億円程度まで下がるなど、極めて投機的な値動きを見せている状況です。

II　本稿の法律パートの纏め

1　AIエージェントと法規制(考え方の基本)

(1) AI エージェントの「エージェント」は日本語に翻訳すると「代理人」となります。AI エージェントと呼ばれるサービスが、法的に厳密な意味で「代理人」に該当しない場合でも、特定のタスクを人間の「代わりに」実行する存在を指すことが通常です。

(2) AIエージェントに適用がある規制を考える場合、①類似行為を人間が行っていればどういう規制等が課されるかを検討し、②その上で、そのような行為をユーザーがAIを利用して行う場合にユーザーに何か規制等が課されるか、③事業者が当該 AI をユーザーに提供している場合、事業者には何か規制等が課されるか、を考えます。

(3) なお、DAO等で仮にAIエージェントが、完全に自律的に動いている、人間が関与していない等と言える場合には、そもそも法規制の適用がないと考える余地もあります。しかし、完全に規制対象となる運営者がいないといえるかは不明確なことが多いため慎重に検討する必要があると考えます。

2　AIエージェントとユーザーの関係、AIエージェント提供者とユーザーの関係

(1) 業務の一部を人間に委ねる場合、①業務委託(準委任・請負)、②労働者派遣、③雇用、等の形態がとられますが、業務の一部をAIエージェントに委ねる場合、AIエージェントとユーザーの関係において契約関係は生じず、単に人間が AI エージェントを事実上使っている、ということになります。

(2) AIエージェントの提供者とユーザーの関係は、AIエージェントの利用に際して、SaaS

[1] Fum氏「【AIエージェント解説シリーズ】ai16zとは一体何なのか？」
https://note.com/fumweb3/n/nc272d8d8d30b　参照

等のサービス利用契約や、AI エージェントのシステム開発契約等の契約関係により規律されます。

3　AI エージェントのミスと責任

(1)　提供者に対する責任追及の議論

AI エージェントの提供者とユーザーとの間の関係は、契約や規約により規律され、AI エージェントに不具合があればAI エージェントを提供するサービス提供者には債務不履行責任などの問題が生じます。

(2) AI エージェントによる発注ミス(無断発注や無権代理)

① ユーザー自らが管理している AI エージェントが間違って発注をした場合、基本的には発注の効果がユーザーに帰属することになります。AI エージェントに対する指示内容や AI エージェントの動作、設定・管理状況等によっては理論的には錯誤による発注の取消しを検討する余地がありますが、取引の安全性の観点からはこのような主張は極めて限定的な場合にしか認められないように思われます。

② 他人が管理している AI エージェントについては、AI エージェントの提供者による無権代理行為の有無が問題となります。表見代理の成否については、例えば AI エージェントにパスワードや発注権限が与えられており、その発注権限を越えて取引をした場合、相手方としては正当な取引があったと考えるしかなく、基本的には表見代理が成立するように思われます。

③ 例えば、暗号資産交換業者や証券会社等の金融機関が提供する AI エージェントが誤作動を起こして、誤発注が起こった、という場合には、ユーザーから当該金融機関に対する損害賠償請求や、ユーザーによる錯誤取消の主張が認められるケースがあると考えます。そのため、利便性が落ちることになりますが、最終的な発注内容の人間(ユーザー)自身の確認を必須とする等の措置を取ることが、誤発注リスクへの対策という観点では有効であると思われます。

(3) AI エージェント利用で他者に損害が生じた場合の責任

例えば、自動運転の AI エージェントの利用で他者に損害が生じた場合に、誰が責任を負うかについては、①自ら保有する自動運転車両の運転者等には自賠法や民法に基づく損害賠償責任が生じる可能性があり、②自動車メーカーには製造物責任法(PL 法)に基づく損害賠償責任が生じる可能性があり、③AI エージェントを提供するソフトウェア業者には民法に基づく損害賠償責任が生じる可能性があります。

4　Web3 AI エージェントと金融規制

(1) AI エージェントが、DEX で本人に代わって暗号資産やステーブルコインの売買を行う場合、AI エージェントの提供者について暗号資産交換業や電子決済手段等取引業の規制が適用されるか検討が必要となります。ユーザーに対する単なる補助であれば規制対象外ですが、AI エージェントが媒介等を行っているとされる場合、規制対象となりえます。

(2) 暗号資産・ステーブルコインの現物取引への投資助言・運用サービスは現在金商法の規制対象外であるため、AI エージェントが行う場合でも基本的には金商法の規制は適用されません。他方、暗号資産・ステーブルコインの「デリバティブ取引」への投資助言・運用サービスについては金商法の規制対象であり、AI エージェントが行う場合にも、その提供者に金融商品取引業の規制が適用される可能性があります。

(3) GK-TK スキームなどで GK がファンド運用業務を行う際に AI エージェントを自ら使用して暗号資産やステーブルコインの現物を取引する場合には、暗号資産交換業や電子決済手段等取引業の規制は適用されないと考えられます。他方で、GK から別の会社が投資一任を受けて AI エージェントを使用してそれらを行う場合には、暗号資産交換業や電子決済手段等取引業の規制が適用される可能性があります。

5　その他の法律

(1) AI エージェントが接客をする場合、個人情報保護委員会が AI に関して示している注意喚起を念頭に対策をする必要があり、消費者保護法 4 条との関係ではハルシネーションを抑制する策を講じる必要があります。

III　AI エージェントと法律の基本的な考え方

1　規制の検討の際には類似行為を人が行った場合にどう考えられるかをまず検討

AI エージェントの「エージェント」は、日本語では「代理人」と訳されます。そして、AI エージェントと呼ばれるサービスは、法的に厳密な意味で「代理人」には該当しない場合でも、特定のタスクを人間の「代わりに」実行する存在を指すことが通常です。

AI エージェントに適用がある規制等を考える場合、以下の手順で検討します。

① 類似の行為を人間が行った場合、どのような法的問題が生じるのかを検討。

② その上で、そのような行為をユーザーが AI を利用して行う場合にユーザーに何らかの規制等が課されるかを検討。

③ 当該 AI を事業者がユーザーに提供している場合、事業者に何らかの規制等が課されるかを検討。

2　規制の対象は人や法人であり、AI エージェント自体ではない

前述のとおり、AI エージェントは「代理人」と訳されることがありますが、当然、人でも法人でもないため、現行法上は、AI エージェント自体が規制対象になるわけではありません。それを利用し、又は提供する自然人や法人が規制対象になります。

この「自然人や法人が規制対象となる」ということに関連し、特に DAO の文脈において、仮に AI エージェントが完全に自律的に動作し、人間が関与していない等と言える場合には、そもそも法規制の適用がないと考えられないかが問題となります。しかし、完全に規制対象となる運営者がいないといえるかは不明確なことが多いため、慎重に検討する必要があると考えます[2]。

3　AI エージェント一般を規制する法律は現在存在していない

現在、AI エージェントの提供や利用を一般的に禁止する法律はないため、個別の行為ごとに自然人や法人を対象とする現行規制の適用の有無を考えることになります。

4　AI 自体が権利義務の帰属主体になる訳ではない

上記 2 に関連し、エージェントを「代理人」と訳したとしても、AI は自然人でも法人でもなく、AI 自体は権利や義務の帰属主体になりえません。

そのため、例えば AI エージェントがミスをした場合の責任に関し、AI 自体は責任の対象とならず、ユーザー又は AI エージェント提供者が責任の主体になります。

IV　AI エージェントとユーザーとの関係、AI エージェント提供者とユーザーとの関係

1　AI エージェントとユーザーとの関係

AI エージェントでは様々な業務の自動化がなされています。

先ず、人が業務の一部を他者に委ねる場合には、以下のような形態の契約が結ばれます。

人と人との関係

(i)　業務委託(準委任・請負)

- 一般的には短期的な業務を外部に依頼する場合に適している。
- 特定の成果物や業務の完成を求める場合は請負(民法 632 条)、特定の業務遂行を求める場合は準委任(同法 656 条)。
- 主な関連法令：下請法、独占禁止法、フリーランス法など

(ii)　労働者派遣

[2] 例えば DeFi(分散型金融)に関する議論においては、開発チーム、管理権限保有者、等の「トラストポイント(利用者が無条件に信頼せざるを得ない中央集権的要素)」の存在が指摘されており、これらの者が規制対象になる可能性があります(2022 年 6 月 20 日金融庁の事務局説明資料「DeFi のトラストポイントに関する分析」https://www.fsa.go.jp/singi/digital/siryou/20220620/jimukyoku2.pdf)。

- 一般的には自社の人員を一時的に補う場合に適している。
- 労働者は派遣元企業に雇用され、派遣先企業で業務を行う。
- 主な関連法令：労働者派遣法など

(iii) 雇用(同法 623 条)

- 一般的には継続的な業務に関する安定した労働力を確保する場合に適している。
- 主な関連法令：労働基準法などの労働関連法令。

他方、人間(ユーザー)と AI エージェントとの関係は、現行法上は、あくまで人間と(AI エージェントを構築する)ソフトウェア・ハードウェアの関係であり、契約関係ではなく、単に人間が AI エージェントを事実上使っているという関係にとどまります。

2 AI エージェント提供者とユーザーとの関係

AI エージェントの開発は、一般に企業によってなされ、多くのユーザーが当該企業から、既製品の AI エージェントの提供を受け、又は企業に AI エージェントの開発を委託します。

この関係は以下のように整理できます。

(i) SaaS 等のサービス利用
企業が提供する AI エージェントの使用許諾を受け、利用規約を遵守しながら利用する。

(ii) システム開発により自社に導入
企業が自社向けの AI エージェントシステムの開発をし、導入・運用する。

V AI エージェントの不具合と責任

1 AI エージェントのユーザーに生じた損害

AI エージェントの不具合によってユーザーに損害が発生した場合、以下のような責任追及、及び防御がなされることが考えられます。

ユーザー側の主張

- SLA(サービスレベルアグリーメント)などの内容に基づき、サービス提供者に対し損害賠償請求(民法 415 条)や契約解除(同法 541 条、542 条)

サービス提供者側の考えられる主張

- 利用規約に基づく免責・責任制限があること
- サービス提供者の帰責性の不存在(同法 415 条 1 項ただし書)
- ユーザー側にも過失があったこと(過失相殺、同法 418 条)

2 AI エージェントの発注ミス(無断発注や無権代理)

(1) 人間による無権代理の問題

仮に、ある人が他者にビットコインの購入を依頼して代理権を与えたにもかかわらず、代理人がイーサリウムを購入してしまった場合、これは無権代理行為となり、原則として契約の効果は本人に帰属しません。

無権代理が発生した場合の主な法的問題は以下のとおりです。

- 無権代理行為の追認(民法 113 条、116 条)
- 無権代理人の履行又は損害賠償責任(同法 117 条)
- 表見代理(同法 110 条)の適用

  → 取引相手が、代理権があると信じる「正当な理由」がある場合、契約の効果が本人に帰属することがあります。例えば、代理人に代理権を証明する手段(実印・委任状の所持など)がある場合です。

  しかし、以下のようなケースにおいて、相手方が代理権の存在について適当な調査・確認を行わない場合、「正当な理由」がないと判断されて表見代理が成立しない可能性があります。

  - ✓ 委任状に改ざんの跡がある場合
  - ✓ 委任状の印が三文判である場合
  - ✓ 本人にとって不利益な取引である場合

(2) AI エージェントによる無断発注や無権代理

(i) ユーザーが管理する AI エージェントの場合

AI エージェントはユーザーの指示に基づいて動作するプログラムであることから、一般的に、AI エージェントの発注はユーザーの意思表示とされ、その効果もユーザーに帰属するものと考えられます。

しかし、AI エージェントがユーザーの真意とは異なる発注をしてしまうケースも想定され、この場合にも発注の効果がユーザーに帰属するかが問題となります。

この点については、「錯誤」(民法 95 条)としてユーザーが意思表示を取り消すことができるかを検討することが考えられます。錯誤には以下の 2 つのケースがあります。

① 意思表示に対応する意思を欠く錯誤(同条 1 項 1 号)
錯誤が重要な事項に関する場合、原則として取消し可能。

② 法律行為の基礎とした事情についてその認識が真実に反する錯誤(同項 2 号)
錯誤が重要な事項に関するものであり、その事情が相手方に示されていた場合に限り、原則として取消し可能。

(a) ユーザーの指示と発注結果が一致する場合

例えば、ユーザーが「AI エージェントの判断で暗号資産を購入する」という意思を持ち、そのような指示を出した結果、想定外の種類・数量の暗号資産の購入がなされた場合、ユー

ザーの「AI エージェントの判断で暗号資産を購入する」という意思と結果が一致する以上、意思表示(AI エージェントの発注)に対応するユーザーの意思は存在するといえ、「ユーザーの想定内で AI エージェントが動作すると考えていた」という事情が相手に表示されなければ、錯誤による取消しは難しいと思われます(同条 2 項)。

(b) ユーザーの指示と発注結果が一致しない場合

一方で、ユーザーが種類・数量を指定した具体的な指示を出し、AI エージェントが異なる種類・数量の発注を行った場合、意思表示(AI エージェントの発注)に対応するユーザーの意思を欠くとして、錯誤による取消しを理論的には主張できるように思われます。

もっとも、このような取消が容易に認められるとすれば取引の安全性を大きく害すると思われます。そこで、民法 95 条 3 項では、ユーザーに「重大な過失」がある場合には取消しをすることができないと定めています。

例えば、AI エージェントの設定ミスや管理不備があれば、ユーザーに「重大な過失」があるとして取消しが否定され得ますし、企業による発注の場合、そもそも AI エージェントを使用した後に自身で具体的な発注内容を確認していないことが「重大な過失」になる場合もあるのではないかと思われます。

(c) 電子消費者契約の特例

消費者が AI エージェントを利用して発注する場合には、電子消費者契約法(電子消費者契約に関する民法の特例に関する法律)第 3 条が適用されると思われます。この法律は、インターネット取引の場合には発注のミスが多いことから、以下のような場合に原則として取消しを認めるものです。

① 誤クリックによる注文（例：「購入する」ボタンを誤って押した）
② 誤った入力による注文(例：購入数量を間違えた)
③ 自動入力や誤操作による意思と異なる注文

AI エージェントを利用する場合にも、事業者がコンピュータの映像面に表示する手続に従って消費者がコンピュータを用いて取引を行えば、それは電子消費者契約(同法 2 条 1 項)に該当することとなり、AI エージェントを利用した取引にも本条の適用があると考えられます。

ただし、以下のように事業者が消費者の意思確認を求める措置を講じた場合には、この特例の適用を受けることはできません。

① 「購入を確定しますか？」と最終確認のポップアップを表示した場合
② ワンクリック購入ではなく、カートを経由して確認画面を設けた場合
③ 二段階認証のような仕組みで購入意思を確認している場合

また、消費者が AI エージェントを利用して、これらの確認を求める措置における確認を省いて取引を行った場合、同条の「消費者から当該事業者に対して当該措置を講ずる必要が

ない旨の意思の表明があった場合」に該当し、特例の適用がなくなる場合があります。この場合、原則として錯誤による取消は認められないと考えられます。

(ii) 他者が提供する AI エージェントの場合

他者が提供する AI エージェントを利用したところ、AI エージェントがユーザーの意図せぬ取引を行ってしまったような場合には、AI エージェントの提供者による無権代理行為の問題が生じ得ます。

AI エージェントの提供者が無権代理人となる場合、表見代理の成否については特に以下のような問題が生じます。

- 通常の代理関係では、代理人が実印や委任状などを持っているかどうかが、取引相手について代理権の存在を信じる「正当な理由」を認めるポイント。
- AI エージェントの場合、取引はデジタル化されており、実印の使用や委任状の提示がないのが一般的。

そのため、取引相手にとって何が「正当な理由」となるかが問題になりますが、当該 AI エージェントが、例えばパスワードや発注権限を与えられ、それを使用して発注した場合、基本的には相手方は正当な取引がなされたと信じるしかなく、表見代理が成立するように思われます。

コラム

●暗号資産交換業者や証券会社などの金融機関が提供し、当該金融機関のサービス内で利用できる AI エージェントの誤発注の場合

例えば、暗号資産交換業者や証券会社などの金融機関が、自社のサービス内で利用できる AI エージェントを提供している場合を考えます(規制については下記 VI 以下で検討)。この AI エージェントが誤作動を起こし、その結果、誤発注が起こった場合については、以下のように整理することができます。

1.取引相手が第三者である場合

AI エージェントの誤作動により発生した誤発注の取引相手方が第三者である場合、第三者は表見代理等によって保護されるケースが多いと思われます。

他方、この取引が表見代理により有効に成立してしまった場合、AI エージェントの提供者である金融機関は、ユーザー本人から損害賠償請求(民法 415 条、709 条)を受けるリスクがあります。

2. 取引相手が金融機関自身である場合

AI エージェントによる誤発注の取引相手が第三者ではなく金融機関自身である場合、そもそもユーザーには誤発注に対応する意思表示がないとされる可能性があります。ま

た、仮に誤発注に対応する意思表示があるとしても、誤発注についてユーザーには重過失がないとして、ユーザーの錯誤取消の主張は認められやすいのではないかと思われます。

また、ユーザーの誤入力によって金融機関との間で契約が成立してしまったような場合には、電子消費者契約法第 3 条の適用があり、金融機関がユーザーの重過失を主張できないケースも考えられます。

3. リスク回避策としてのユーザー確認の導入

上記を踏まえたAIエージェントの誤作動による金融機関のリスクをユーザーに転嫁する方法としては、最終的な発注時には常に人間(ユーザー)の確認を必要とする仕組みを導入することが考えられます。この場合、誤発注が発生したとしても、それは人間(ユーザー)の責任である、と言いやすくなります。

この仕組みを導入した場合、完全自動化とはならず利便性は落ちることになりますが、誤発注リスクの対策という観点では有効な措置になるのではないかと思われます。

3　AI エージェントの利用により他者に損害が生じた場合について(例：自動車の自動運転)

AI エージェントの不具合に関連して他者が損害を被った場合、AI エージェントの提供者や AI エージェントのユーザーが損害賠償責任を負う可能性があります。

この点、AI エージェントの活用事例として特に注目されており、AI エージェントの利用により他者に損害が発生し得る典型的なユースケースとして、自動運転が考えられます。

自動運転では、AI エージェントが自動車の運転を担うことになりますが、人間が運転する場合と AI が運転する場合では、事故が発生した際の法的責任が異なる可能性があります。

(1) 人間が運転していた場合

① 人身事故の場合

人身事故を起こした場合、車の保有者などの運行供用者(自動車を自己のために運行する者)は、民法の不法行為(709 条)のほか、自動車賠償責任保障法(自賠法)3 条に基づく責任を負うことになります。自賠法 3 条に基づき損害賠償請求をする場合、被害者は、運転者の過失を立証する必要がありません。運行供用者は、自賠法 3 条に基づき、以下の 3 つの免責要件をすべて満たした場合には責任を免れることができます。

(a) 自己及び運転者が自動車の運行に関し注意を怠らなかったこと
(b) 被害者又は運転者以外の第三者に故意又は過失があったこと
(c) 自動車に構造上の欠陥又は機能の障害がなかったこと

②　物損事故の場合

物損事故では自賠法が適用されないため、被害者は民法 709 条の不法行為責任に基づく損害賠償請求を行うことになります。この場合、被害者としては、運転者の故意又は過失を

自ら立証しなければなりません。

(2) AI エージェントが運転していた場合(社会的に認められた AI エージェントを想定)

① 人身事故の場合

AI エージェントの自動運転により人身事故が生じた場合でも、基本的には自賠法の適用があると考えられています[3]。完全自動運転の AI エージェントのシステムに障害があった場合には、上記の免責要件のうち(c)の要件を満たさないとして、被害者から運行供用者に対して自賠法に基づく損害賠償請求権が認められる可能性があります。

AI エージェントのシステム障害に起因して賠償金を支払った運行供用者や保険金を支払った保険会社等は、自動車メーカーや AI システムのソフトウェア業者などに求償を行うことになると考えます。

② 物損事故の場合

物損事故の場合には自賠法 3 条が適用されないため、運転者等に不法行為責任に基づく損害賠償請求を行うことになりますが、完全自動運転であれば、運転者の操作ミス等がなくなるため、運転者の故意又は過失を問うことが難しくなり、運転者の損害賠償責任が認められにくくなる可能性があります。

この場合、被害者としては、AI エージェントのシステムに障害があれば、それを提供する自動車メーカーやソフトウェア開発業者などに対して以下のとおり責任追及をすることが考えられます。

③ 自動車メーカーに対する請求

被害者は、自動車メーカーに対して、製造物責任法(PL 法)3 条に基づく損害賠償請求を行うことが考えられます。

PL 法は、製造物の欠陥が原因で生命、身体又は財産に損害を与えた場合、製造業者等に無過失責任を課す法律です。ただし、以下のような課題もあります。

- ソフトウェア自体は動産ではないため、PL 法の「製造物」に該当しない。ただし、ソフトウェアが組み込まれた車両に欠陥があると評価されれば、PL 法に基づき自動車メーカーが製造物責任を負う可能性がある[4]。
- AI による自動運転システムは高度で複雑なため、被害者が「欠陥」と「因果関係」を立証するのが困難である可能性がある。

---

[3] 自動運転における損害賠償責任に関する研究会 報告書（概要）
https://www.mlit.go.jp/common/001226364.pdf

[4] 2018 年 4 月 17 日 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議「自動運転に係る制度整備大綱」18 頁 https://www.mlit.go.jp/common/001260125.pdf

- 製造物責任は、製造業者等による引き渡し時に存在した欠陥に基づき認められる責任であるため、車両の引渡し後の遠隔で行われたソフトウェアのアップデートにより欠陥が生じたような場合には、製造物責任が認められない可能性がある。

④ ソフトウェア業者に対する請求

被害者は、AI エージェントを提供するソフトウェア業者に対し、AI エージェントの欠陥を理由として損害賠償請求をすることが考えられます。この場合、ソフトウェアは無体物であるため製造物責任の適用がないことから、民法 709 条に基づく不法行為責任等を追及することになります。

この場合、被害者がソフトウェア開発者の故意・過失を立証する必要があることから、上記の自賠法 3 条に基づく損害賠償請求のケースや、PL 法 3 条に基づく損害賠償請求のケースよりも、賠償請求のハードルが高くなることが考えられます。

VI　Web3 AI エージェントと金融規制

本項目では、上記 III の考えに従い、Web3 の AI エージェントに対してどのように金融規制が適用されるかを検討します。なお、Web3 の文脈で検討しますが、類似の考え方が、株式投資の AI エージェントなど、金融系の AI エージェントにも当てはまります。

(1) 暗号資産やステーブルコインなどの売買と AI エージェント

AI エージェントが分散型取引所(DEX)でユーザーの代わりに暗号資産やステーブルコインの取引を行うことが考えられます。このような仕組みを活用することで、以下のようなメリットが期待できます。

- リアルタイム市場分析による迅速な取引
- 人間の感情に左右されないデータドリブンな意思決定

一方で、このような売買を行う場合、暗号資産交換業等の規制がないか検討が必要となります。

①人間が取引する場合

暗号資産の売買やステーブルコイン(法定通貨の価値と連動し、額面で償還されるもの)の売買については、暗号資産交換業(資金決済法 2 条 15 項)や電子決済手段等取引業(同法 2 条 10 項 2 号)に関する規制の適用を考える必要があります。

同法では、単なる投資家として暗号資産等を売買する場合は、「業として」に該当せず、規制対象ではありません[5]。

[5] 2017 年 3 月 24 日金融庁パブリックコメント 47 頁 No.94、48 頁 No.95

他方、広く公衆に対して売買する場合や、公衆に対して売買の代理を行う場合には規制の対象となります。

②AI エージェントが取引する場合

AI エージェントがユーザーの代わりに暗号資産やステーブルコインを売買する場合であっても、自分自身の投資目的で AI エージェントを使う場合、ユーザー自身には特に規制はかかりません。

また、売買の発注をする AI エージェントを提供する会社があっても、それが単にユーザーの売買手続の事務を助ける、というだけの場合には、規制はないと思われます。

他方、AI エージェントが、例えばユーザーを DEX に容易に繋ぐといった媒介等[6]と言われる範囲の動作を行っており、その AI エージェントをユーザー以外の者が管理運用している、とみられるような場合、当該 AI エージェントの提供者に、暗号資産交換業や電子決済手段等取引業の規制(媒介規制)が課される可能性があります。

(2) 投資サービスと AI エージェント

Web3 分野では、AI エージェントが投資戦略を立案し、暗号資産・ステーブルコインの現物取引、暗号資産・ステーブルコインのデリバティブ取引に関する投資助言や資産運用を行うサービスが考えられます。

本パートでは、AI エージェントがこのような投資サービスを提供する際に検討すべき主要な法的問題について、人間が行う場合と比較しながら説明します。

① 人間が行う場合

投資助言・運用サービスを提供する場合、それぞれ異なる法的規制が適用されます。

(i) 投資助言サービス

投資助言サービスとは、投資助言をして報酬を受け取る契約(投資顧問契約)を締結し、有価証券やデリバティブ取引に関する投資判断について助言を行う業務を指します。

規制のポイントは以下のとおりです。

- 投資助言・代理業として金融商品取引法に基づく登録を要する(金商法 2 条 8 項 11 号、3 項 1 号、28 条、29 条)。ただし、無償の助言は規制対象外。
- 暗号資産やステーブルコインの現物取引に関する助言は規制対象外。
- 暗号資産や(電子決済手段に該当する)ステーブルコインのデリバティブ取引に関す

---

https://www.fsa.go.jp/news/28/ginkou/20170324-1/01.pdf

[6]「媒介」の範囲については、金融庁の暗号資産交換業事務ガイドライン Ⅰ－1－2－2 ②
https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf

る助言は規制対象。

- 助言の対象が現物取引かデリバティブ取引かを意識する必要がある。

(ii) 投資運用サービス

投資運用サービスは、主に、(a)ファンド持分を有する者からの出資金を主に有価証券やデリバティブ取引に投資する業務(ファンド運用業務) 、(b)顧客から投資判断と資産運用の権限を一任されて、有価証券やデリバティブ取引に投資運用する業務(投資一任業務)、が考えられます。

規制のポイントは以下のとおりです。

- 投資運用業の登録を要する(金商法 2 条 8 項 12 号ロ、2 条 8 項 15 号、28 条 4 項、29 条)。無償で提供する場合でも「業」に該当する場合は規制対象。
- (a)ファンド運用業務については、自己募集には原則、第二種金融商品取引業の登録が必要(同法 2 条 8 項 7 号へ、28 条 2 項 1 号)。ただし、適格機関投資家等特例業務(同法 63 条)などの例外あり。
- (b)投資一任業務により顧客資産を預かる場合、第一種金融商品取引業の登録も必要(同法 28 条 5 項・1 項 5 号、29 条、42 条の 5)。
- 暗号資産・ステーブルコインの現物取引を投資対象とする場合((a)ファンド運用業務の場合は「主として」投資対象とする場合)は、投資運用業に該当しない。他方、暗号資産・(電子決済手段に該当する)ステーブルコインのデリバティブ取引を投資対象とする場合は投資運用業の規制対象。
- GK-TK スキーム[7]では、匿名組合員による出資はすべて GK(営業者)の財産に帰属し(商法 536 条 1 項)、GK が自己の名をもって事業を行うため、(a)GK がファンド運用業務に基づき、暗号資産の現物の売買を行う場合、自己投資目的で行う取引であるとして一般的には「業」には当たらず、暗号資産交換業の登録を要しないと考えられ[8]、投資対象がステーブルコインの現物である場合もパラレルに考えれば、電子決済手段等取引業に該当しないと考えられる。
- (b)GK-TK スキームなどで GK が別の会社に投資業務を一任し、当該別会社が暗号資産やステーブルコインの売買等まで行う場合、暗号資産交換業や電子決済手段等取引業の規制を受ける可能性がある[9]。

[7] 合同会社(GK)と匿名組合(TK)を組み合わせた事業投資モデル。

[8] 2017 年 3 月 24 日金融庁パブリックコメント 47 頁 No.94、48 頁 No.95
https://www.fsa.go.jp/news/28/ginkou/20170324-1/01.pdf

[9] 2020 年 4 月 3 日金融庁パブリックコメント 62 頁 No.228
https://www.fsa.go.jp/news/r1/sonota/20200403/01.pdf

② AI エージェントが行う場合

AI エージェントが投資助言・運用サービスを行う場合、その業務が金融規制の適用を受けるかどうかが問題となります。通常、AI エージェントを提供する者について規制の適用を検討することになると考えます。

規制のポイントは人間が行う場合と概ね同じですが、特に AI エージェントの場合には以下の点がポイントになります。

- 投資一任業務で顧客資金を預かる場合でも、AI エージェントの提供者が運用していないスマートコントラクトで顧客資金の預託を受ける場合には第一種金融商品取引業の登録が不要となる可能性がある。
- AI エージェントの提供後、特に開発者が運用に関わらず、AI エージェントが完全に DAO として自律的に動き、投資運用についてもスマートコントラクトにより自動執行される等の場合には規制の対象外となる可能性がある。

VII　その他の法律

(1) 個人情報保護法、消費者契約法

AI エージェントがバーチャルアシスタントとして、サービスの販売支援や問い合わせ対応を行うことが考えられます。例えば、メタバース内で商品やサービスを販売する場合にも、AI エージェントが搭載されたアバターが自動接客を行うことが想定されます。

本パートでは、AI エージェントが接客サービスを提供する際の主要な法的問題について、従来の人間による業務と比較しながら説明します。

①人間が顧客対応する場合

人間が顧客対応を行う場合、例えば以下のような観点から法規制を遵守する必要があります。

(i) 個人情報の取扱い

顧客対応の際に個人情報を取得・利用する場合は、個人情報保護法の以下のルールなどを遵守する必要があります。

- 利用目的をできるだけ明確に特定すること(個人情報保護法 17 条 1 項)
- 特定した目的の範囲を超えて個人情報を利用しないこと(同法 18 条 1 項)
- 利用目的を本人に通知又は公表すること(同法 21 条 1 項)

(ii) 消費者保護に関する規制

消費者に対してサービスの説明や情報提供を行う際には、消費者契約法 4 条に基づく以下の規制などを遵守する必要があります。

- 重要事項について虚偽の説明をしないこと
- 将来の不確実な事項について断定的な判断を提供しないこと

- 消費者に不利益となる事実を故意又は重過失により伝えないことを回避すること

これらの違反があった場合、消費者は契約を取り消す権利を持つため、正確かつ十分な情報を提供することが重要です。

②AI エージェントが顧客対応する場合

(i) 個人情報の取扱い

AI エージェントが顧客対応を行う際にも、個人情報の取扱いには慎重な対応が求められます。

個人情報保護委員会は、OpenAI のサービス提供者に対し、「利用者及び利用者以外の者を本人とする個人情報の利用目的について、日本語を用いて、利用者及び利用者以外の個人の双方に対して通知し又は公表すること。」ということや、本人の同意なしに、要配慮個人情報を取得しないことなどの注意喚起を行っています[10]。

また、生成 AI を利用して個人情報を取り扱う事業者に対しては、「個人情報取扱事業者が生成 AI サービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること」などの注意喚起を行っています[11]。

AI エージェントにより個人情報を取り扱う場合には、これらの注意喚起を念頭に置いて対応する必要があります。

(ii) AI エージェントによる誤情報(ハルシネーション)の問題

消費者契約法 4 条などを遵守する観点では、AI エージェントが不十分な学習データや古い情報をもとに不十分な情報提供や誤った回答をする「ハルシネーション」のリスクが問題となります。

この問題を防ぐために以下のような対策をとることが考えられます。

- 最新かつ正確な学習データを用いて、AI エージェントを継続的にトレーニングすること
- 消費者が誤情報を報告できるフィードバック機能を実装すること
- 運営者が AI エージェントの回答を適宜チェックし、必要に応じて修正を行うこと

[10] 令和 5 年 6 月 2 日個人情報保護委員会「OpenAI に対する注意喚起の概要」
https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf

[11] 令和 5 年 6 月 2 日個人情報保護委員会「生成 AI サービスの利用に関する注意喚起等」
https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

留保事項

・本稿の内容は関係当局の確認を受けたものではなく、法令上合理的に考えられる議論を記載したものにすぎません。また、本稿に記載された内容は筆者らの現時点での見解にすぎず、今後変更がありえます。

・本稿は AI エージェントや Web３ AI エージェントの利用を推奨するものではありません。

・本稿は AI エージェントに関する一般的な考え方を記載したものに過ぎず、具体的な案件に関する法務アドバイスを提供するものではありません。具体的な法的助言が必要な場合は、各自、弁護士にご相談下さい。