September 25, 2025

AI Agents, Web3 AI Agents, and Japanese Law

So Saito
Shimpei Asano
So & Sato Law Offices

In this article, we will introduce AI agents, which have been gaining popularity since 2025, by explaining (1) what an AI agent is, (2) what Web3 AI agents are, and (3) the legal issues surrounding AI agents.

Because AI agents can take over any job, when considering the relationship between AI agents and the law, it is necessary to consider legal issues for all the jobs they perform. However, since it is difficult to cover all of this in a blog, this article first introduces the basic ideas for considering legal issues related to AI agents, and then discusses their relationship with regulation, focusing on financial regulation in particular.

However, we believe that this approach to financial regulation will also be useful to a certain extent when considering legal issues related to other AI agents.

I. Overview of AI Agents

1 What is an AI Agent?

An AI agent is generally an artificial intelligence system that autonomously performs specific tasks. It is capable of processing data from the environment, learning and making decisions as needed, and carrying out tasks without human instruction.

Generally, an AI agent has the following elements:

(i) Recognition: Processes the external environment and input data to understand the current situation.
(ii) Decision-making: Plans actions to accomplish tasks based on data.
(iii) Action: Executes actions that bring about changes in the environment based on the plan.
(iv) Feedback: Uses the results of execution to learn and improve actions next time.

This allows AI agents to perform repetitive tasks and make complex decisions on behalf of humans.

AI agents are currently attracting a great deal of attention as they are expected to transform our lives and how we do business.

For example, AI agents are expected to be used in the following applications:

Examples of AI Agent Uses:

(i) Generative AI Creativity Support:

Used in creative fields, such as generating text, images, videos, and music. In the media, advertising, and gaming industries, AI is expected to improve production efficiency and create new value.

(ii) Personal Assistant:

AI can provide support tailored to individual needs, such as life coaching, educational support, and business assistants. Applications that improve daily life efficiency, such as schedule management and health advice, are gaining attention.

(iii) Autonomous Use in Finance:

AI agents that support asset management and household finances use data to propose optimal investment strategies and savings methods. Automated trading and asset management are also advancing in decentralized finance (DeFi).

(iv) Business Process Automation:

Automating repetitive tasks such as human resources, finance, and customer service contributes to improving corporate productivity. Data analysis and decision-making support are also areas where AI agents excel.

(v) Healthcare:

AI agents are used for health management, telemedicine, and disease prediction. In particular, personalized services such as symptom analysis and mental health support are expected.

(vi) Autonomous Systems:

AI agents are expected to play an active role in handling physical tasks such as robot automation in warehouse management, logistics, and disaster response, as well as self-driving and drone operation.

AI agents have the potential to enrich our lives and make businesses more efficient, thanks to their personalization and autonomy, and these applications are areas where further advancements are expected in the future.

2 Specific examples of AI agents

The following are some specific examples of AI agent use both in Japan and overseas.

Service name	Provider	Features
Fujitsu Kozuchi AI Agent	Fujitsu Limited	An AI agent that autonomously promotes advanced tasks in cooperation with humans. For example, as a conference agent, AI can participate in meetings to share information and propose

		measures, or as a field support agent, analyze camera footage at manufacturing and logistics sites, propose improvements, and create work reports.
Agentforce	Salesforce, Inc	Autonomous AI assistants. For example, Service Agent, part of Agentforce, replaces traditional chatbots with autonomous AI, enabling accurate and fluent conversations with customers 24/7 without pre-programming scenarios.
Operator	OpenAI, Inc	AI operates a web browser on behalf of the user, automating everyday tasks. It uses its own browser to navigate web pages and perform operations such as typing, clicking, and scrolling according to the user's instructions, allowing it to automate tasks such as making restaurant reservations and online shopping.
Pactum AI	Pactum AI, Inc.	Walmart has introduced Pactum AI, an autonomous negotiation AI, to automate negotiations with over 100,000 suppliers. It automatically makes proposals in response to requests from suppliers based on pre-specified budgets and priorities, leading to optimal trading terms for both Walmart and the supplier.
Waymo Foundation Model	Waymo LLC	Waymo, which operates self-driving taxis, uses a proprietary AI model called the Waymo Foundation Model to enable advanced decision-making, from understanding the surrounding situation to generating driving plans.

3 Web3 AI Agents

AI agents are said to be compatible with Web3. The integration of Web3 and AI agents is expected to create new possibilities, such as the following:

Examples of Web3 AI Agent Use Cases : (i) Integration with Decentralized AI Agents and Smart Contracts: AI agents operate smart contracts on the blockchain and execute transactions autonomously. For

example, real estate and financial transactions can be completed without an intermediary.

・Operating as part of a Decentralized Autonomous Organization (DAO): AI agents participate in the decision-making process within the DAO, making proposals and voting.

(ii) Strengthening User Sovereignty and Protecting Privacy: AI agents process user data locally and securely store personal information in decentralized storage (e.g., IPFS). ・Self-Sovereign Identity (SSI): AI agents leverage users' SSI to simplify access and authentication to Web3 services.

(iii) Automating the Token Economy and Automating Token Trading: AI agents manage and trade assets on behalf of users on a decentralized exchange (DEX).

・Reward Distribution: AI agents receive and redistribute tokens based on the value they generate on the Web3 platform.

(iv) Metaverse and AI Agents: AI agents act as virtual assistants within the metaverse. For example, managing land for users or trading NFTs.

(v) Utilizing Zero-Knowledge Proofs (ZKPs): AI agents can use ZKPs to provide trust in Web3 applications while protecting privacy.

One example of a Web3 AI agent that has attracted global attention is AI16Z (ai16z), a decentralized AI investment fund built on the Solana blockchain that utilizes AI agents to autonomously conduct investment activities.

Project name: ai16z
Platform: Solana Blockchain
Features:
・AI collects and analyzes market information and automatically executes token transactions taking into account community consensus.
・Uses decentralized governance that allows investors to participate in project management and decision-making through tokens.
・Blockchain technology ensures the transparency and reliability of investment activities.
AI Agent "Eliza":
・An AI agent responsible for planning and executing investment strategies.
・Released as open source, it can also be deployed by third parties.

The name ai16z is a play on Andreessen Horowitz (a16z), a well-known Silicon Valley VC, but ai16z and a16z are unrelated.

However, on October 27, 2024, Marc Andreessen, one of the founders of a16z, posted "GAUNTLET THROWN" on X (formerly Twitter) and mentioned the T-shirt worn by ai16z's main avatar, which caused the name of ai16z to spread rapidly[1].
Furthermore, in early January 2024, ai16z's market capitalization temporarily exceeded 300 billion yen, growing more than 100 times in three months. As a result, by early January 2025, the company had become a hot topic worldwide and in the case of a personal injury accident was also a major topic of discussion on AI agents on Japan's X (formerly Twitter). However, perhaps due to overly high expectations, the price has fallen sharply, with the market capitalization falling to around 50 billion yen, indicating extremely speculative price movements.

II. Summary of the legal part of this paper

1 AI Agents and Legal Regulation (Basic Concept)

(i) The word "agent" in AI agent translates to "proxy" in Japanese. Even if a service called an AI agent does not strictly qualify as an "agent" in the legal sense, it typically refers to an entity that performs specific tasks "on behalf of" a human.

(ii) When considering regulations applicable to AI agents, we first consider (1) what regulations would be imposed if a human were to perform similar actions, (2) whether any regulations would be imposed on the user if the user were to perform such actions using AI, and (3) whether any regulations would be imposed on the business if the business provides the AI to users.

(iii) Note that, in cases such as DAOs, if the AI agent can be said to operate completely autonomously and without human involvement, there is room to consider that legal regulations do not apply in the first place. However, since it is often unclear whether there are no operators who would be subject to regulation, careful consideration is required.

2 Relationships between AI Agents and Users, and Relationships between AI Agent Providers and Users

(i) When a part of a task is delegated to a human, it can take the form of ① outsourcing (quasi-agency or subcontracting), ② labor dispatch, or ③ employment. However, when a part of a task is delegated to an AI agent, no contractual relationship arises

[1] Fum, "What on earth is ai16z?" [AI Agent Explanation Series]
https://note.com/fumweb3/n/nc272d8d8d30b

between the AI agent and the user; the human is simply effectively using the AI agent.

(ii) The relationship between an AI agent provider and its user is governed by contractual relationships, such as a service agreement (e.g., SaaS) or a system development agreement for the AI agent.

3 AI Agent Errors and Liability

(i) Discussion of Holding Providers Liable

The relationship between an AI agent provider and its user is governed by contracts and regulations. If an AI agent malfunctions, the service provider providing the AI agent may be held liable for breach of contract or other issues.

(ii) Ordering Errors by an AI Agent (Unauthorized Orders or Unauthorized Agency)

① If an AI agent managed by a user places an incorrect order, the effects of the order generally belong to the user. Depending on the instructions given to the AI agent, its behavior, settings, and management status, there is theoretically room for consideration of canceling an order due to error. However, from the perspective of transaction security, such a claim would likely only be accepted in extremely limited cases.

② For AI agents managed by others, the issue is whether the AI agent provider acted without authorization. Regarding apparent agency, for example, if an AI agent is given a password or has order authority and transacts beyond that authority, the other party will have no choice but to consider the transaction legitimate, and apparent agency would essentially be established.

③ For example, if an AI agent provided by a financial institution such as a cryptocurrency exchange or securities company malfunctions and places an erroneous order, a user may be able to sue the financial institution for damages or claim cancellation due to error. Therefore, although it would reduce convenience, taking measures such as requiring a human (user) to personally confirm the final order details would be effective in addressing the risk of erroneous orders.

(iii) Liability for Damages Caused to Others through the Use of AI Agents

For example, if damages are caused to others through the use of an autonomous driving AI agent, who is liable? ① The driver of an autonomous vehicle owned by the user may be liable for damages under the Automobile Liability Act or the Civil Code;

② The automobile manufacturer may be liable for damages under the Product Liability Act (PL Act); and ③ The software provider providing the AI agent may be liable for damages under the Civil Code.

4 Web3 AI Agents and Financial Regulation

(i) If an AI agent trades cryptocurrencies or stablecoins on behalf of users on a DEX, it is necessary to consider whether regulations for cryptocurrency exchanges and electronic payment instruments trading businesses apply to the provider of the AI agent. While mere assistance to users is not subject to regulation, if the AI agent is deemed to act as an intermediary, it may become subject to regulation.

(ii) Investment advisory and management services for spot trading of cryptocurrencies and stablecoins are currently not subject to regulation under the Financial Instruments and Exchange Act. Therefore, even if an AI agent is conducting such transactions, these regulations are generally not applicable. On the other hand, investment advisory and management services for cryptocurrency and stablecoin "derivative trading" are subject to regulation under the Financial Instruments and Exchange Act. Even when services are provided by AI agents, the provider may be subject to regulations under the Financial Instruments and Exchange Act.

(iii) If a GK uses an AI agent to trade spot cryptocurrency or stablecoins when conducting fund management operations, such as in a GK-TK scheme, regulations under the Crypto Asset Exchange Business and Electronic Payment Instruments Business may not apply. On the other hand, if another company receives investment discretion from the GK and uses an AI agent to conduct such operations, regulations under the Crypto Asset Exchange Business and Electronic Payment Instruments Business may apply.

5 Other Laws

(i) When an AI agent provides customer service, measures must be taken keeping in mind the warnings regarding AI issued by the Personal Information Protection Commission. In relation to Article 4 of the Consumer Protection Act, measures must be taken to prevent hallucination.

III. Basic Concepts of AI Agents and Law

1 When considering regulations, first consider how similar actions would be handled if a person were to commit them.

The "agent" in AI agent is translated as "representative" in Japanese. Services called AI agents usually refer to entities that perform specific tasks "on behalf of" humans, even if they do not fall under the strict legal definition of a "representative."

When considering regulations that may apply to AI agents, consider the following steps:

(i) Consider what legal issues would arise if a human were to perform a similar act.

(ii) Then, consider whether any regulations would be imposed on users if they were to perform such acts using AI.

(iii) Consider whether any regulations would be imposed on businesses that provide the AI to users.

2 Regulation is directed at people and corporations, not at AI agents themselves

As mentioned above, AI agents are sometimes translated as "agents," but since they are neither people nor corporations, under current law, AI agents themselves are not subject to regulation. Instead, the natural persons and corporations that use or provide them are.

In relation to this "natural persons and corporations are subject to regulation," particularly in the context of DAOs, if an AI agent can be said to operate completely autonomously and without human involvement, the question arises as to whether legal regulations would not apply in the first place. However, since it is often unclear whether there are no operators who are completely subject to regulation, we believe that careful consideration is necessary.[2]

3 There are currently no laws regulating AI agents in general.

Currently, there are no laws that generally prohibit the provision or use of AI agents, so whether or not the current regulations that apply to natural persons and legal entities apply to each individual act must be considered.

4 AI itself does not become the subject of rights and obligations

---

[2] For example, in discussions about DeFi (decentralized finance), the existence of "trust points" (centralized elements that users are forced to trust unconditionally) such as development teams and administrative authority holders has been pointed out, and these individuals may be subject to regulation (Financial Services Agency Secretariat briefing document, June 20, 2022, "Analysis of DeFi Trust Points" https://www.fsa.go.jp/singi/digital/siryou/20220620/jimukyoku2.pdf).

In relation to point 2 above, even if we translate "agent" as "representative," AI is neither a natural person nor a legal entity, and AI itself cannot be the subject of rights or obligations. Therefore, for example, when an AI agent makes a mistake, the AI itself is not liable, but the user or the AI agent provider is.

IV. Relationship between AI agents and users, and between AI agent providers and users

1 Relationship between AI agents and users

AI agents are automating a variety of tasks.

First, when a person delegates part of a task to another person, a contract of the following form is concluded.

Relationships between people (i) Outsourcing (quasi-agency/subcontracting) ● Generally suitable when outsourcing short-term work. ● Contracting (Article 632 of the Civil Code) is used when a specific output or task is required to be completed, and quasi-agency (Article 656 of the same Code) is used when a specific task is required to be performed. ● Main relevant laws and regulations: Subcontracting Act, Antimonopoly Act, Freelance Act, etc. (ii) Worker dispatching ● Generally suitable when temporarily supplementing one's own staff. ● Workers are employed by the dispatching company and perform work at the dispatched company. ● Main relevant laws and regulations: Worker Dispatch Act, etc. (iii) Employment (Article 623 of the same Code) ● Generally suitable when securing a stable workforce for ongoing work. ● Main relevant laws and regulations: Labor-related laws and regulations such as the Labor Standards Act.

On the other hand, under current law, the relationship between humans (users) and AI agents is merely that between humans and the software and hardware (that construct the AI agent) and is not a contractual relationship; it is merely a relationship in which humans are effectively using the AI agent.

2 Relationship between AI agent providers and users

AI agents are generally developed by companies, and many users either receive ready-made AI agents from those companies or commission the development of AI agents to those companies.
This relationship can be summarized as follows:

(i) Obtain a license to use the AI agent provided by a service provider such as a SaaS service provider and use it in compliance with the terms of use. (ii) Develop, install, and operate an AI agent system for your company.

V. AI Agent Malfunctions and Responsibilities

1 Damages caused to users of AI agents

If a user suffers damage due to a malfunction of an AI agent, the following liability claims and defenses may be taken:

The user's argument: ● Based on the contents of the SLA (Service Level Agreement), etc., the user may seek compensation for damages (Article 415 of the Civil Code) or terminate the contract (Articles 541 and 542 of the Civil Code). The service provider's possible arguments: ● There are exemptions and limitations on liability based on the terms of use; ● The service provider is not at fault (Article 415, Paragraph 1, of the same law); ● The user is also negligent (Contributory Negligence, Article 418 of the Civil Code).

2 AI agent ordering errors (unauthorized ordering or unauthorized representation)

(i) The problem of unauthorized human representation

For example, if a person asks another person to purchase Bitcoin and gives them authority to do so, but the agent ends up purchasing Ethereum, this will be considered unauthorized agency, and in principle the effects of the contract will not belong to the principal.
The main legal issues that arise when unauthorized agency occurs are as follows:

● Ratification of unauthorized agency (Articles 113 and 116 of the Civil Code) ● Liability of unauthorized agent for performance or damages (Article 117 of the same Code) ● Application of apparent agency (Article 110 of the same Code) ➞ If the counterparty has "legitimate reasons" to believe that the principal has the authority of agency, the effects of the contract may belong to the principal. For example,

if the agent has the means to prove the authority of agency (possession of a registered seal or power of attorney, etc.).
However, in the following cases, if the counterparty does not conduct an appropriate investigation or confirmation of the existence of the authority of agency, it may be determined that there is no "legitimate reason" and the apparent agency may not be established.
✓ If there are signs of tampering with the power of attorney
✓ If the seal on the power of attorney is a cheap seal
✓ If the transaction is disadvantageous to the principal

(ii) Unauthorized ordering or unauthorized representation by AI agents

①In the case of AI agents managed by users

Since AI agents are programs that operate based on user instructions, orders placed by AI agents are generally considered to be an expression of the user's intention, and the effects of such orders are also considered to belong to the user.
However, there are also cases where an AI agent places an order that differs from the user's true intention, and in such cases, the question arises as to whether the effects of the order belong to the user.
In this regard, it may be necessary to consider whether the user can revoke the expression of intention as a "mistake" (Article 95 of the Civil Code). There are two cases of mistake:

1. Mistake resulting in a lack of intention corresponding to the manifestation of intention (Article 1, Paragraph 1, Item 1)
In principle, rescission is possible if the mistake concerns an important matter.
2. Mistake resulting in an untrue understanding of the circumstances that formed the basis of the legal act (Article 1, Paragraph 2)
In principle, rescission is possible only if the mistake concerns an important matter and the circumstances were disclosed to the other party.

(a)When the user's instructions and the order result match

For example, if a user intends to "purchase cryptocurrency at the discretion of an AI agent" and issues such instructions, resulting in the purchase of an unexpected type and quantity of cryptocurrency, since the user's intention to "purchase cryptocurrency at the discretion of an AI agent" and the result match, it can be said that there is a user intention corresponding to the expression of intention (the AI agent's order), and unless the other party is informed that "the user thought the AI agent would operate within the user's

expectations," it is likely to be difficult to cancel the order due to mistake (paragraph 2 of the same article).

(b)When the user's instructions and the order result do not match

On the other hand, if the user gives specific instructions specifying the type and quantity, and the AI agent places an order for a different type and quantity, it seems theoretically possible to argue that the cancellation was due to mistake, on the grounds that the user's intention (the AI agent's order) does not correspond to the expression of intention. However, if such cancellations were easily permitted, it would likely seriously undermine the safety of transactions. Therefore, Article 95, Paragraph 3 of the Civil Code stipulates that cancellations cannot be made if the user is "grossly negligent." For example, if there is a setting error or improper management of the AI agent, the user could be found to be "grossly negligent" and the cancellation could be denied. In the case of orders placed by a company, it may even be considered "gross negligence" if the user does not check the specific order contents themselves after using the AI agent.

(c)Special provisions for electronic consumer contracts

When consumers place orders using AI agents, Article 3 of the Electronic Consumer Contract Act (Act on Special Provisions of the Civil Code Concerning Electronic Consumer Contracts) is likely to apply. This Act, because of the high incidence of ordering errors in internet transactions, allows cancellation in the following cases in principle:

① Orders made by mistake (e.g., pressing the "Buy" button by mistake)
② Orders made by incorrect input (e.g., entering the wrong quantity)
③ Orders made differently from your intention due to automatic input or incorrect operation

Even when using an AI agent, if a consumer conducts a transaction using a computer in accordance with the procedures displayed on a computer screen by a business operator, this will be considered an electronic consumer contract (Article 2, Paragraph 1 of the same Act), and it is considered that this article also applies to transactions using an AI agent. However, this exception will not apply if a business takes measures to request confirmation of the consumer's intention, as described below.

① When a final confirmation pop-up asking "Do you want to confirm your purchase?" is displayed.
② When a confirmation screen is set up via the cart instead of one-click purchasing.

③ When the intention to purchase is confirmed using a system such as two-factor authentication.

Furthermore, if a consumer uses an AI agent to conduct a transaction without taking the necessary confirmation measures, this may fall under the provision of the same article, "where the consumer expresses their intention to the business operator that they do not need to take such measures," and the special provisions may no longer apply. In such cases, cancellation due to mistake is generally not permitted.

②In the case of an AI agent provided by another party

If an AI agent provided by another party is used and the AI agent conducts a transaction that the user did not intend, the issue of unauthorized agency by the AI agent provider may arise. When
the AI agent provider is an unauthorized agent, the following particular issues arise regarding the success or failure of apparent agency.

●In a typical agency relationship, whether the agent has a registered seal or a power of attorney is the key to determining whether there is "reasonable cause" to believe in the existence of agency authority over the other party. ●In the case of AI agents, transactions are digitalized, and it is common for there to be no use of a registered seal or presentation of a power of attorney.

Therefore, the question arises as to what constitutes a "legitimate reason" for the trading partner. If the AI agent is given, for example, a password or authority to place an order and uses it to place an order, the other party will basically have no choice but to believe that a legitimate transaction has been made, and it would appear that apparent agency would be established.

Column**:** Cases of erroneous orders made by AI agents provided by financial institutions such as cryptocurrency exchanges and securities companies and available within their services.
Consider the case of a cryptocurrency exchange or securities company providing an AI agent for use within its services (regulations are discussed in Section VI below). If this AI agent malfunctions and results in an erroneous order, the following situations can be considered: 1. When the counterparty is a third party.

If the counterparty to an erroneous order made by an AI agent malfunctions is a third party, the third party is likely to be protected by apparent agency or other protections. On the other hand, if the transaction is validly concluded through apparent agency, the financial institution providing the AI agent risks being sued for damages by the user (Articles 415 and 709 of the Civil Code).

2. When the counterparty is the financial institution itself.
If the counterparty to an erroneous order made by an AI agent is the financial institution itself, rather than a third party, the user may be deemed to have had no intention to respond to the erroneous order in the first place. Even if the user did express an intention to respond to the erroneous order, the user's claim for cancellation due to error is likely to be accepted, given that they were not grossly negligent in the erroneous order. Furthermore, if a contract is concluded with a financial institution due to a user's incorrect input, Article 3 of the Electronic Consumer Contract Act may apply, and the financial institution may not be able to claim gross negligence on the part of the user.

3. Implementing User Confirmation as a Risk Avoidance Measure
One way to shift the risk to financial institutions caused by AI agent malfunctions to users based on the above is to implement a system that always requires human (user) confirmation when placing a final order. In this case, even if an incorrect order occurs, it would be easier to argue that it is the human (user)'s responsibility.
Implementing this system would not result in full automation and would reduce convenience, but it is likely to be an effective measure in terms of addressing the risk of incorrect orders.

3 Regarding cases where the use of AI agents causes harm to others (e.g., self-driving cars)

If another party suffers damages related to the malfunction of an AI agent, the provider of the AI agent or the user of the AI agent may be liable for damages.
This point is particularly noteworthy as an example of the use of AI agents, and autonomous driving is a typical use case in which the use of AI agents could cause harm to others.
In autonomous driving, an AI agent will be responsible for driving the car, but legal liability in the event of an accident may differ between when a human is driving and when an AI is driving.

(i) When a human is driving:

① In the case of a personal injury accident

In the event of a personal injury accident, the car owner or other operator (a person who operates a car for themselves) will be held liable under Article 3 of the Automobile Liability Insurance Act (Automobile Liability Insurance Act) in addition to tort (Article 709) of the Civil Code. When claiming damages under Article 3 of the Automobile Liability Insurance Act, the victim does not need to prove the driver's negligence. Under Article 3 of the Automobile Liability Insurance Act, the operator can be exempt from liability if they meet all of the following three exemption requirements:

(a) The driver and the victim were careful in operating the vehicle.
(b) The victim or a third party other than the driver acted intentionally or negligently.
(c) The vehicle had no structural defects or functional impairments.

② In the case of property damage accidents

Since the Automobile Liability Act does not apply to property damage accidents, victims must file a claim for damages based on tort liability in Article 709 of the Civil Code. In this case, the victim must prove the driver's intent or negligence.

(ii) When an AI agent is driving (assuming a socially accepted AI agent)

① In the case of a personal injury accident

Even if an accident resulting in injury or death occurs due to the autonomous driving of an AI agent, the Automobile Liability Act is generally considered to apply.[3] If there is a malfunction in the system of a fully autonomous driving AI agent, the victim may be entitled to claim damages from the operator under the Automobile Liability Act, as it would not meet requirement (c) of the above exemption requirements.

We believe that operators who have paid compensation and insurance companies who have paid insurance claims due to system failures caused by AI agents will seek compensation from automobile manufacturers, AI system software providers, and others.

② In the case of property damage accidents

In the case of property damage accidents, Article 3 of the Automobile Liability Act does not apply, so claims for damages based on tort liability will be made against the driver, etc. However, with fully autonomous driving, there will be no driver error, etc., so it will be

---

[3] Report (Summary) of the Study Group on Liability for Damages in Automated Driving https://www.mlit.go.jp/common/001226364.pdf

difficult to hold the driver responsible for intent or negligence, and it may be difficult to recognize the driver's liability for damages.
In this case, if there is a problem with the AI agent system, the victim may seek liability from the automobile manufacturer or software developer that provides it, as follows:

③ Claims against the automobile manufacturer

Victims may file a claim for damages against the automobile manufacturer under Article 3 of the Product Liability Act (PL Act).
The PL Act imposes strict liability on manufacturers when a defect in a product causes damage to life, body, or property. However, there are also the following issues:

- Software itself is not movable property, so it does not fall under the category of "products" under the Product Liability Act. However, if a vehicle incorporating the software is deemed to have a defect, the automaker may be held liable under the Product Liability Act.[4]
- Because AI-based self-driving systems are sophisticated and complex, it may be difficult for victims to prove a "defect" and a "causal relationship."●

Product liability is recognized based on defects that existed at the time of delivery by the manufacturer, etc., so if a defect occurs due to a software update performed remotely after the vehicle is delivered, product liability may not be recognized.

④ Claims against software providers

Victims may seek compensation for damages against software companies that provide AI agents, citing defects in the AI agents. In this case, because software is an intangible object and therefore product liability does not apply, victims may pursue tort liability under Article 709 of the Civil Code.
In this case, the victim will need to prove the software developer's intent or negligence, so the hurdle for claiming compensation is likely to be higher than in cases where damages are claimed under Article 3 of the Automobile Liability Act or Article 3 of the Product Liability Act.

---

[4] April 17, 2018, Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, Strategic Conference for the Promotion of Public and Private Data Utilization, "Outline of System Development for Automated Driving," p. 18 https://www.mlit.go.jp/common/001260125.pdf

VI. Web3 AI Agents and Financial Regulation

In this section, we will consider how financial regulations apply to AI agents in Web3, following the ideas in Section III above. Although we will be examining this in the context of Web3, similar ideas also apply to financial AI agents, such as stock investment AI agents.

(i) Trading of crypto assets and stablecoins, and AI agents

It is conceivable that AI agents will trade crypto assets and stablecoins on behalf of users on decentralized exchanges (DEXs). Utilizing such a system is expected to bring the following benefits:

- Fast trading through real-time market analysis
- Data-driven decision-making that is not influenced by human emotions

On the other hand, when conducting such transactions, it is necessary to consider whether there are any regulations regarding crypto asset exchange businesses, etc.

① When humans trade

When buying and selling cryptocurrencies and stablecoins (which are linked to the value of legal tender and redeemable at face value), it is necessary to consider the application of regulations regarding crypto asset exchange businesses (Article 2, Paragraph 15 of the Payment Services Act) and electronic payment instruments trading businesses (Article 2, Paragraph 10, Item 2 of the same Act).

Under the law, trading crypto assets as a mere investor does not constitute a "business" and is not subject to regulation.[5] On the other hand,

sales to the general public or acting as an agent for sales to the public are subject to regulation.

② When an AI agent trades

Even if an AI agent buys and sells cryptocurrencies or stablecoins on behalf of a user, there are no particular regulations for the user if the AI agent is used for the user's own investment purposes.

Also, even if there is a company that provides an AI agent to place buy and sell orders, there are likely to be no regulations if the agent simply assists users with the administrative procedures for buying and selling.

---

[5] Financial Services Agency Public Comments, March 24, 2017, p. 47, No. 94, p. 48, No. 95 https://www.fsa.go.jp/news/28/ginkou/20170324-1/01.pdf

On the other hand, AI agents could act as intermediaries, for example, to easily connect users to DEXs.[6] and is deemed to be managed and operated by a party other than the user, the provider of the AI agent may be subject to regulations on crypto asset exchange businesses and electronic payment instrument trading businesses (intermediary regulations).

(ii) Investment Services and AI Agents

In the Web3 field, AI agents can develop investment strategies and provide investment advice and asset management services related to spot trading of crypto assets and stable coins, as well as derivative trading of crypto assets and stable coins.
In this section, we will explain the main legal issues that must be considered when AI agents provide such investment services, comparing them with when provided by humans.

① When performed by humans

When providing investment advisory and management services, different legal regulations apply.

(i) Investment advisory services

Investment advisory services refer to the business of providing advice on investment decisions regarding securities and derivative transactions by entering into a contract (investment advisory contract) for providing investment advice and receiving compensation.
The key points of regulation are as follows:

●Registration as an investment advisory and agency business is required under the Financial Instruments and Exchange Act (Article 2, Paragraph 8, Item 11, Paragraph 3, Item 1, Articles 28 and 29 of the Financial Instruments and Exchange Act). However, advice provided free of charge is not subject to regulation. ●Advice regarding spot trading of crypto assets and stable coins is not subject to regulation. ●Advice regarding derivative trading of crypto assets and stable coins (which fall under electronic payment methods) is subject to regulation. ●It is necessary to be aware of whether the advice is for spot trading or derivative trading.

(ii) Investment management services

---

[6] For the scope of "intermediary," please refer to the Financial Services Agency's Crypto Asset Exchange Business Guidelines I-1-2-2 ②
https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf

Investment management services are primarily considered to be (a) businesses that invest capital contributions from fund holders primarily in securities and derivative transactions (fund management businesses), and (b) businesses that invest and manage securities and derivative transactions after being entrusted with the authority to make investment decisions and manage assets by customers (discretionary investment businesses).
Key points of the regulations are as follows:

●Registration as an investment management business is required (FIEA Article 2, Paragraph 8, Item 12 (b), Article 2, Paragraph 8, Item 15, Article 28, Paragraph 4, and Article 29). Even if the service is provided free of charge, it is subject to regulation if it constitutes a "business."
●(a) With regard to fund management business, self-offering generally requires registration as a Type II Financial Instruments Business (FIEA Article 2, Paragraph 8, Item 7, and Article 28, Paragraph 2, Item 1). However, there are exceptions, such as Special Business for Qualified Institutional Investors, etc. (FIEA Article 63).
●(b) If customer assets are entrusted to custody through discretionary investment business, registration as a Type I Financial Instruments Business is also required (FIEA Article 28, Paragraphs 5 and 1, Item 5, Article 29, and Article 42-5).
●If the investment target is spot trading of crypto assets or stable coins (in the case of (a) fund management business, if the investment target is "primarily"), it does not constitute an investment management business. On the other hand, if the investment target is derivative trading of crypto assets or stable coins (which constitutes an electronic payment instrument), it is subject to regulation as an investment management business.
●GK-TK Scheme[7] , all investments made by anonymous partners belong to the assets of the GK (operator) (Article 536, Paragraph 1 of the Commercial Code), and the GK conducts business in its own name. Therefore, (a) if the GK buys and sells spot crypto assets based on its fund management business, it is generally considered to be a transaction for the purpose of self-investment and therefore does not require registration as a crypto asset exchange business.[8] In the case where the investment target is a physical stablecoin, it is considered to be a parallel case and would not be considered an electronic payment instruments trading business.
●(b) In the case of a GK-TK scheme, etc., where a GK entrusts investment operations to another company and the other company also buys and sells crypto assets and

[7] A business investment model that combines a limited liability company (GK) and a anonymous partnership (TK).
[8] Financial Services Agency Public Comments, March 24, 2017, p. 47, No. 94, p. 48, No. 95 https://www.fsa.go.jp/news/28/ginkou/20170324-1/01.pdf

stablecoins, there is a possibility that it will be subject to regulations for crypto asset exchange businesses and electronic payment instruments trading businesses.[9]

② When performed by an AI agent

When an AI agent provides investment advisory or management services, the question arises as to whether that business is subject to financial regulations. Generally, it is thought that the application of regulations to those who provide AI agents will be considered.
The key points of regulation are generally the same as when a human does the work, but the following points are particularly important in the case of AI agents.

- Even when holding customer funds for discretionary investment management, there is a possibility that registration as a Type I Financial Instruments Business may not be required if the customer funds are held in a smart contract that is not operated by the AI agent provider.
- After the AI agent is provided, it may not be subject to regulation, especially if the AI agent operates completely autonomously as a DAO, without the developer being involved in its operation, and investment management is automatically executed by smart contract.

VII. Other Laws

(i) Personal Information Protection Act, Consumer Contract Act

AI agents could potentially act as virtual assistants, assisting with sales and answering inquiries. For example, when selling products or services within the metaverse, avatars equipped with AI agents could be expected to automatically provide customer service.
In this section, we will discuss the main legal issues surrounding AI agents providing customer service, comparing them with traditional human services.

① When a human handles a customer

When humans handle customer interactions, they must comply with laws and regulations, for example, from the following perspectives:

(a) Handling of Personal Information

When acquiring and using personal information when dealing with customers, you must comply with the following rules of the Personal Information Protection Act.

---

[9] April 3, 2020, Financial Services Agency, Public Comments, page 62, No. 228
https://www.fsa.go.jp/news/r1/sonota/20200403/01.pdf

● Specify the purpose of use as clearly as possible (Article 17, Paragraph 1 of the Personal Information Protection Act) ● Do not use personal information beyond the scope of the specified purpose (Article 18, Paragraph 1 of the same Act) ● Notify or publicize the purpose of use to the individual (Article 21, Paragraph 1 of the same Act)

(b) Consumer protection regulations

When explaining services or providing information to consumers, you must comply with the following regulations based on Article 4 of the Consumer Contract Act.

●Do not give false explanations about important matters. ●Do not provide definitive judgments about uncertain future matters. ●Avoid intentionally or through gross negligence withholding facts that are detrimental to consumers.

In the event of any of these breaches, the consumer has the right to cancel the contract, so it is important to provide accurate and sufficient information.

② When AI agents handle customer inquiries

(a) Handling of personal information

Even when AI agents deal with customers, they must handle personal information with care.

The Personal Information Protection Commission has issued a warning to OpenAI service providers, including that they must "notify or publicly announce, in Japanese, the purpose of use of personal information of users and other individuals," and that they must not acquire sensitive personal information without the consent of the individual.[10] In addition, the government has issued a warning to businesses that use generative AI to handle personal information, stating that "when a business handling personal information inputs prompts containing personal information into a generative AI service, it must fully confirm that the input is within the scope necessary to achieve the specified purpose of use of the personal information."[11]

---

[10] Personal Information Protection Commission, June 2, 2023, "Summary of the Alert Regarding OpenAI" https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf

[11] June 2, 2023, Personal Information Protection Commission, "Caution Regarding the Use of Generative AI Services" https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

When handling personal information using AI agents, it is necessary to keep these precautions in mind.

(b) Hallucination by AI agents

From the perspective of complying with Article 4 of the Consumer Contract Act, etc., there is a risk of "hallucination," where an AI agent provides insufficient information or gives incorrect answers based on insufficient training data or outdated information.
The following measures can be considered to prevent this problem.

● Continuously train the AI agent using the latest and most accurate learning data. ● Implement a feedback function that allows consumers to report misinformation. ● Operators should check the AI agent's responses as appropriate and make corrections as necessary.

Reservations:

- The contents of this article have not been confirmed by the relevant authorities and merely describe arguments that are reasonably considered legally. Furthermore, the contents of this article are merely the authors' current views and are subject to change.
- This article does not recommend the use of AI agents or Web3 AI agents.
- This article merely describes general ideas regarding AI agents and does not provide legal advice regarding specific cases.
- If you require specific legal advice, please consult a lawyer.