

中国におけるエージェント型 AI の急拡大 ー金融業界での OpenClaw 活用事例ー

宋 良也

■ 要 約 ■

1. 中国では 2026 年に入り、エージェント型人工知能（AI）への関心が急速に高まっており、その代表例として OpenClaw が注目を集めている。OpenClaw は、当初の AI エージェントから、アップデートを経てより自律性の高いエージェント型 AI へ進化し、ユーザーからの複雑な目標を複数のタスクに分解して実行できるようになった。
2. OpenClaw はオープンソースのため、米中の規制の影響を受けにくい利用が可能であることに加え、ユーザーによる自由な大規模言語モデル（LLM）の選択による利用コスト削減が可能である。特にエージェント型 AI は、生成 AI よりもトークン（AI が生成する言語の最小処理単位）消費が遥かに多く、運用コストが高くなりやすい。こうした中、ユーザーが低価格な中国国産 LLM を利用可能なことが、OpenClaw の普及を後押ししている。
3. 中国の金融業界においても OpenClaw の導入が進み、証券会社や金融情報ベンダー等が関連サービスを相次いで展開している。例えば、東方財富証券は自社データベースを活用するプラグイン（拡張機能）を提供し、Wind 社は OpenClaw のマルチエージェント機能を活用し、OpenClaw に基づくサービスである「WindClaw」を提供した。
4. 一方で、中国政府は金融分野での OpenClaw 利用に伴うリスクに警戒を示し、銀行等での利用を制限している。今後、隔離環境で利用可能な「サンドボックス」が整備されれば、証券会社等の金融機関が安全性を確保しつつリサーチ業務を含む多様な業務の拡大に繋げることができると考えられる。また、エージェント型 AI の活用を通じた業務効率化により、人間にしかできない付加価値の高いビジネスの創出も可能となろう。

野村資本市場研究所 関連論文等

- ・坂上聖奈「AI エージェントの概念と金融分野における取り組みーウェルス・マネジメントでの利活用のポテンシャルー」『野村資本市場クォーターリー』2025 年春号。
- ・宋良也・塩島晋「中国における生成 AI 関連規制ー金融資本市場分野における新たな可能性ー」『野村サステナビリティクォーターリー』2025 年夏号。

I 中国で関心高まるエージェント型 AI の OpenClaw

2026 年に入り、エージェント型の人工知能（AI）が世界的に注目される中、中国においても関心が高まっている。具体的には、2025 年 11 月に開発されたオープンソース¹のエージェント型 AI である OpenClaw の活用事例が増加している。その背景には、同年 2 月に OpenClaw がアップデートを経て、AI エージェント²からエージェント型 AI への進化を遂げたことがある。

AI エージェント及びその進化系であるエージェント型 AI は、近年話題となってきた米オープン AI 社の ChatGPT や中国の DeepSeek 社が開発した生成 AI³とは異なる。一般的に、生成 AI は、主に個人のユーザー（利用者）がプロンプト（指示・質問）を入力し、大規模言語モデル（LLM）⁴による推論・計算を経て、文書、画像、コード等のコンテンツを自動生成する AI 技術を指す。これに対し、AI エージェント及びエージェント型 AI は、コンテンツ生成に留まらず、ユーザーが設定する目標の達成に向けて、生成 AI 技術を基盤とした LLM を利用し、自律的に計画、判断、行動することで、複数の手順からなる複雑な目標を遂行可能な AI を指す⁵。

OpenClaw は、オープンソースのため、米中政府の規制を回避した利用が可能である（詳細後述）。また、ユーザーが中国本土の LLM を自由に選択できることに加えて、サービス事業者が IT 初心者向けに OpenClaw を改良した自社アプリを開発することもでき、利便性が高い。そのため、OpenClaw は中国において短期間で人気を集めてきた。地方政府をはじめ、テンセントやバイトダンス等の大手プラットフォームや証券会社等による OpenClaw を用いた様々な取り組みが行われている。

他方で、中国政府は OpenClaw がもたらすリスクについて警戒を示している。中国政府は、国有企業、政府機関及び銀行等、国家・経済の安全保障の維持において重要な機関に対して、OpenClaw の使用を緊急に停止させており、インストール済の一部の機関に対して、アンインストールまたは安全検査・報告を求めている、と報じられている⁶。

本稿では、中国で OpenClaw が注目されるようになった背景を分析し、金融業界における OpenClaw を活用した取り組みを概観した上で、エージェント型 AI の今後の見通しについて考察する。

¹ ここでのオープンソースとは、ユーザーにプログラムのソースコード（プログラミング言語で書かれたコンピュータプログラムを表現するテキスト）が無償で公開され、再配布が可能であることを指す。

² オープン AI 社が 2025 年 1 月に AI エージェントである「オペレーター（Operator）」を発表したことをきっかけに、AI エージェントが生成 AI に代わる新たなトレンドになったとされている。

³ ChatGPT が 2023 年 2 月に爆発的に普及したことが、生成 AI の発足とされている。

⁴ LLM とは、膨大なテキストデータを使って事前学習されており、人間と同様に会話や論文などのテキスト生成が可能な言語に特化したモデルを指す。詳細は、坂上聖奈「AI エージェントの概念と金融分野における取り組みーウェルス・マネジメントでの利活用のポテンシャルー」『野村資本市場クォーターリー』2025 年春号参照。

⁵ 米 IBM 社 Cole Stryker 氏「エージェント型 AI とは」を参照。

⁶ “China Moves to Curb OpenClaw AI Use at Banks, State Agencies,” *Bloomberg News*, March 11, 2026.

Ⅱ OpenClaw の仕組みと中国における注目の背景・要因

1. エージェント型 AI に進化した OpenClaw

1) AI エージェントとエージェント型 AI の比較

エージェント型 AI に進化した OpenClaw について詳述する前に、AI エージェントとエージェント型 AI の相違点について整理する。コーネル大学のランジャン・サプコタ氏等によれば、AI エージェントは一般的に、簡単な目標をいくつかのタスクに分解し、各タスクを順次に実行する⁷。これに対し、エージェント型 AI は、より複雑な目標をいくつかのサブ目標に分解し、複数の AI エージェント（マルチエージェント）を組み合わせることで、全ワークフローを設計・調整し、各サブ目標を同時並行で実現することが可能である。その際に、エージェント型 AI は各タスクの途中結果に基づき計画を自律的に修正することで、ユーザーのモニタリングや確認を最小限に留めることができる。こうした点から、エージェント型 AI は、AI エージェントよりも自律性が高いと言える（図表 1）。

図表 1 生成 AI、AI エージェントとエージェント型 AI の違い

	AIエージェント	エージェント型AI	生成AI(参考)
主要な目的	外部ツールを用いて特定のタスクを実行	複雑なワークフローを自動化し、ハイレベルな目標を達成	ユーザーのプロンプトに基づき新規コンテンツを生成
メカニズム	プロンプト⇒ツール実行(利用)⇒LLM⇒アウトプット	目標⇒マルチエージェントの協調⇒アウトプット	プロンプト⇒LLM⇒アウトプット
構造	LLM+ツール	マルチエージェントシステム	シングルモデル
目標の柔軟性	低い (特定の目標のみ実行)	高い(目標を細分化し、進行状況に応じて柔軟に修正可能)	低い(プロンプトごとに固定した目標)
処理の継続性	単一タスクの実行中に限って、短期的な継続性を持つ	全ワークフローの複数段階にわたり、状態・目標・進捗等の継続性を持つ	前のやり取りや状態を維持しない、セッションが終わると継続性はない
学習・適応	限定的に学習・適応する	結果に基づき適応可能	静的(事前に学習済)
協調戦略	独立したタスク実行	階層的または分散的な協調	なし(単一段階の処理)

(出所) 各種資料より野村資本市場研究所作成

⁷ Ranjan Sapkota, Konstantinos I. Roumeliotis, Manoj Karkee, “AI Agents vs. Agentic AI: A Conceptual taxonomy, applications and challenges,” September 30, 2025.

2) エージェント型 AI である OpenClaw の仕組み

OpenClaw は当初、オープンソースの AI エージェントとして、オーストリア出身の著名ソフトウェアエンジニアであるピーター・スタインバーガー氏により 2025 年 11 月に開発された⁸。その後、OpenClaw は 2026 年 2 月のアップデートを経て、自律性やマルチエージェント機能が大幅に強化され、エージェント型 AI に進化したとされている⁹。OpenClaw の一般的な仕組みは以下の通りである。

第 1 に、OpenClaw は、ユーザーからプロンプトを入力してもらうに当たり、WeChat や Telegram 等のメッセージアプリをユーザーインターフェース（ユーザーとの接点）とする。第 2 に、OpenClaw のアーキテクチャ（構造）の中核ハブとしてのゲートウェイ（異なるネットワークを中継する仕組み）は、ローカル環境¹⁰にインストールされ、ユーザーの目標を複数のタスクに分解し、実行計画の策定等を行う。第 3 に、ゲートウェイは、各タスクに最も適合する「サブエージェント」¹¹を振り分け、それぞれのエージェントに LLM を呼び出す。第 4 に、OpenClaw は、一部の特定タスクや作業（アクション）を自律的に実行するため、適切なプラグイン（拡張機能）である「スキル」¹²を読み込むこともある。第 5 に、OpenClaw は、各タスクを自律的に実行した後、その結果を再び LLM を用いて評価し、タスクが遂行されたのかを確認する。ユーザーの目標が未達成の場合、OpenClaw は上記プロセスを再度行い、次の適切なステップを再計画するというループを続ける。

このように、OpenClaw は単一な AI エージェントから、エージェント型 AI へと進化したことで、より高度かつ複雑な目標を自律的に遂行することが可能となった。

2. 中国における OpenClaw への注目の高まり

より高度かつ複雑な目標を自律的に遂行できるエージェント型 AI の代表として OpenClaw が世界的に人気を集める中、中国においても注目が高まっている。その背景・要因として、①OpenClaw がオープンソースであるため、米中間の規制リスクが回避可能、②中国産 LLM を用いることでコスト削減が可能、という 2 点が挙げられる。

⁸ ピーター・スタインバーガー氏は、2025 年 11 月に OpenClaw を創設した後、2026 年にその成果が評価され、オープン AI 社に入社することとなった。

⁹ OpenClaw の当初の名前は「Clawd（Claude と Claw＝爪を掛けた名前）」であったが、米アンソロピック社と商標に関する紛争により、Clawd⇒Moltbot⇒OpenClaw と、2 回改名が行われた。

¹⁰ ローカル環境とは、インターネット上のサーバーではなく、ユーザー自身のパーソナルコンピューター（PC）上で構築された作業環境を指す。

¹¹ サブエージェントとは、OpenClaw のマルチエージェントの中で、プロジェクトマネージャーに相当する「オーケストレーターエージェント（親エージェント）」に帰属する、下位タスクの委任先としての子エージェントを指す。

¹² ここでのスキルは、ユーザーやその他開発者が自由に追加・共有することが可能であり、ファイル操作、ブラウザ制御、API 呼び出し、メール送信等、特定の任務を実行することが可能な行動パターンが設定されている。

1) 米中間の規制リスクの回避

中国企業は、米中間の技術・投資制限により、AI エージェントやエージェント型 AI を利用する上で制限を受けている¹³。例えば、中国国内の企業は、米アンソロピック社が開発した AI エージェントのクロードコード (Claude Code) を利用することができない。また、AI エージェントのマナス (Manus) 等を開発した中国のスタートアップ企業モニカ (Monica) 社は、中国国内でサービス提供をしているものの、2025 年 12 月にマナスを 20 億米ドルで米メタ社に売却したことを受けて、中国当局から警戒され、今後の中国国内でのサービス提供の先行きが不透明となっている¹⁴。これに対して、OpenClaw はオープンソースであり、そのプログラムを構成するソースコード¹⁵はサービス提供企業及びユーザー側に帰属するため、米中政府の規制による影響を受ける可能性が低いとされる。

また、OpenClaw は API (アプリケーションプログラミングインターフェース)¹⁶を通じて外部の LLM を利用する必要があるが、本稿執筆時点で、アンソロピック社の Claude (クロード) やオープン AI 社の GPT 等の米国製 LLM が中国本土で提供されていない中、DeepSeek 等の中国製 LLM が利用可能である。こうした点からも、OpenClaw は、中国でのサービス提供において優位性を有していると考えられる。

2) 中国国産 LLM の活用によるユーザーの利用コスト削減

OpenClaw はクロードコードとは異なり、ユーザーが LLM を選択可能であり、利用コストを削減できることも、中国において OpenClaw 人気が高い一因と考えられる¹⁷。

一般的に、ユーザーが AI プログラムを利用する際に、API を通じた外部 LLM の利用料金は、消費したトークン数に比例する従量課金制が採用されていることが多い¹⁸。例えば、生成 AI の場合、1 分間の映像を生成するには 100 万トークンを消費するとされる¹⁹。これに対して、エージェント型 AI は、自律的な思考 (ユーザーの目標達成のための推論) の手順を繰り返すことや、過去の検索結果やコード実行履歴等を「現在の状況」として認識する必要があり、そのための前後関係を含むテキストを何度も再入力することで、会話が長くなることがある。これらの影響により、エージェント型 AI は一般的にチャット型の生成 AI よりも数百倍から数千倍のトークンを消費すると

¹³ 米中間では、AI、半導体、量子技術等の最先端の技術分野において、相手国の企業が自国の企業に対する投資を制限する規制が設けられている。

¹⁴ 中国国家発展改革委員会の外商投資安全審査工作机制弁公室は 4 月 27 日、メタ社によるマナス買収案件を法令に基づき禁止する決定を下し、モニカ社とメタ社の 2 社に取引撤回を求めた。また、マナスの創業者である肖弘氏及びチーフサイエンティストである季逸超氏には、それ以前から監督審査を理由に出国制限が掛けられている。

¹⁵ ソースコードとは、プログラミング言語で書かれたコンピュータプログラムを表現するテキストを指す。

¹⁶ API とは、ソフトウェアやプログラムが互いの機能を共有・連携するためのインターフェースを指す。

¹⁷ クロードコードでは、自社のクロード LLM を利用することを前提にしている。ユーザーが無理やりクロードコードに他社 LLM を組み込むことは、アンソロピック社の利用規約違反となる恐れがある。

¹⁸ トークンとは、AI が言語を解釈・生成する際の最小処理単位を指す。英語であれば、1 単語・空白・句読点ごとに 1 トークンに相当、日本語・中国語であれば、1~1.5 文字が 1 トークンに相当する。

¹⁹ 「小詞元扶動智能經濟大市場」『人民日報』2026 年 4 月 3 日。

される²⁰。特に OpenClaw によるトークン消費量は多いとされており、1ヶ月のトークン消費量が数千万トークンとなるケースもあるという²¹。

トークン消費量が高い OpenClaw にとって、LLM 利用料金を抑えることが重要となる。OpenClaw が、中国 AI 企業であるミニマックス社が開発した LLM である「MiniMax-M2.7」を使用する場合、利用料金が 100 万出力トークン当たり約 2～3 ドルとなっている²²。これは、アンソロピック社が開発した LLM の Claude4.5 を使用する場合の 6 分の 1 程度である²³。このように、OpenClaw のユーザーは中国国産 LLM を用いることでエージェント型 AI 利用コストを大幅に削減できることが可能である。

Ⅲ 中国における OpenClaw に関する取り組みと潜在的なリスク

本章では、中国における OpenClaw 関連の取り組みについて概観し、金融業界における OpenClaw 活用事例を紹介する。その上で、中国政府が懸念している OpenClaw の潜在的なリスクについて整理する。

1. 中国における OpenClaw に関する取り組み状況

中国では、地方政府、大手 IT プラットフォーマー、情報ベンダー、証券会社等が OpenClaw に関する様々な取り組みを進めている（図表 2）。

図表 2 中国における OpenClaw に関する主な取り組み

主体	機関名	関連施策・ブランド	具体的な内容
地方政府	深圳市龍崗区	「OpenClaw 及び OPC 発展を支援するための若干の措置（意見募集稿）」	OpenClaw 関連ツールを開発研究を行う企業等に対し、龍崗区政府から最大 200 万元の補助金や、公共データの利用費用の削減、OpenClaw の応用プロジェクトの奨励を含む 10 項目にわたる支援策を提供。
	無錫市高新区	「OpenClaw 等オープンソースプロジェクトと OPC の融合発展の支援に関する若干の措置（意見募集稿）」	OpenClaw 関連ツールの開発・研究を行う企業や、自社ビジネスにおいて OpenClaw に基づくツールを応用する企業等に対し、無錫市高新区政府から最大 500 万元の補助金等、12 項目にわたる支援策を提供。
大手プラットフォーム	テンセント（騰訊）	Qclaw、ClawBot 等	OpenClaw をベースにしたローカル環境で動作する AI エージェント。メール管理：メールの検索、整理、送信、削除等。
	バイドゥ（百度）	DuClaw	ローカルディスクのファイル管理：検索、整理、編集、キャッシュ削除等。
	アリババ（阿里巴巴）	JVSClaw	定型的なワークフローの自動化に対応。
	バイトダンス（字節跳動）	ArkClaw、飛書妙搭	
LLM を提供する AI 企業	ムーンショット AI	KimiClaw	OpenClaw をベースにしたローカル環境で動作する自律型 AI エージェント。
	智譜 AI	AutoClaw	
	ミニマックスグループ	MaxClaw	LLM は自社開発のものを使用することが特徴的。

（出所）各種資料より野村資本市場研究所作成

²⁰ 前掲脚注 19 を参照。

²¹ 「大模型、雲厂商紛紛下場“養蝦”，入局“Token 經濟”」『中国証券報』2026 年 3 月 17 日。

²² “The rise of China’s hottest new commodity: AI tokens,” *Financial Times*, March 26, 2026.

²³ 実際には中国国内において米国企業が開発する LLM を使用できないが、ここでは LLM のコストを比較することを目的として関連データを示している。

例えば、地方政府は、管轄区域内で OpenClaw に関する開発研究を行う企業や OpenClaw 関連サービスを顧客向けに提供する企業を対象に、補助金等の支援策を検討している。また、テンセント等の大手プラットフォームは、自社の SNS プラットフォームでユーザーによるプロンプト入力を可能にする OpenClaw サービスの提供に注力している。さらに、LLM を提供する AI 企業でも、自社開発の LLM を使用し、OpenClaw をベースにしたローカル環境で動作する AI エージェントサービスを提供している。

2. 金融業界における OpenClaw の活用事例

中国では金融業界においても、OpenClaw に関する取り組みが活発に行われている。例えば、証券会社のリサーチ部門は、投資家向けの OpenClaw の構築・活用方法を解説する研究レポートを相次いで発表している。他にも、一部の証券会社は、OpenClaw を自社のリサーチ関連業務で活用していることに加えて、顧客向けにも OpenClaw 関連のサービスを提供している。更に、金融情報ベンダーが自社のデータベースに基づいた情報取得を促進させるべく、OpenClaw 関連サービスを提供するケースも見られる。

以下では、親会社が情報ベンダーである東方財富証券の OpenClaw 用プラグインの提供と、金融情報ベンダー大手の Wind 社による OpenClaw を活用した個人顧客向けのサービス提供の2事例を紹介する。

1) 東方財富証券による OpenClaw 用プラグインの提供

東方財富証券は、上海に本社を置くインターネット金融会社の東方財富信息股份有限公司を親会社に持つ。同会社は情報ベンダーを中心とした業務を展開していたが、2015 年に西藏同信証券を買収し、証券業に進出した。東方財富証券は、情報ベンダーである親会社の自社データベース²⁴を用いて他社との差別化を図ってきた。

OpenClaw が中国で注目されることを受け、東方財富証券は OpenClaw を活用して自社顧客にサービスを提供すべく、2026 年 3 月 12 日に、OpenClaw で使用可能なプラグインである「妙想スキル」を発表した。妙想というブランドは、同社が開発した金融業に特化した LLM である「妙想金融 LLM」をベースとした、投資家による調査支援用の AI アシスタントとして知られている。その上で、妙想スキルは、上記の自社開発の妙想金融 LLM を OpenClaw で使用するためのプラグインとして、金融に特化した特定の任務を実行することが可能な行動パターンが予め設定されている。

具体的に、妙想スキルには、①情報検索スキル、②金融データスキル、③知能銘柄スクリーニングスキル、④仮想ポートフォリオ管理スキル、⑤ウォッチリスト管理スキル、の5つが含まれる。その中で、①については、投資家は同スキルを使って、東方財富証券がベンダーとして保有するデータベースの情報にアクセスでき、投資家の指示に基づき、OpenClaw は情報の収集、まとめ、ユーザーが必要な情報を出力する

²⁴ 具体的には、東方財富ネットの「Choice 金融端末」を指す。

等の作業を行う。④については、OpenClaw は投資家が設定した投資戦略に基づき、自律的に株式を選択し、ポートフォリオを組成する²⁵。また、⑤については、OpenClaw は投資家の株式ウォッチリストに登録している銘柄の模擬売買注文を、投資家の代理で行う。今後、投資家が OpenClaw の下で上記スキルを利用し、実際に株式売買及びポートフォリオ組成を行うことができるようになることが想定される。

2) OpenClaw のマルチエージェント機能を活用する Wind 社

Wind 社は、2026 年 3 月 11 日に同社の OpenClaw に基づくサービス「WindClaw」を公開した。WindClaw の最大の特徴は、単一の AI エージェントではなく、OpenClaw のマルチエージェント機能を活用し、複数の AI エージェントが役割を分担する「投資研究 AI チーム」を設計した点である。WindClaw は OpenClaw フレームワーク全体を含む「プロ版 OpenClaw」として設計されており、難しい環境構築が不要で、ユーザーは WindClaw を初めて使用する際に、直接アプリを PC 環境にインストールすることが可能になるなど、ユーザーにとっての利便性が高いとされている。

WindClaw が実装されたエージェントは 6 つある。それぞれの役割を見ると、いずれも個人・機関投資家または証券アナリストを対象にしており、Wind のデータベースをソースとしたもので構成される（図表 3）。また、ユーザーの入力した目標が複雑であれば、OpenClaw はマルチエージェントの協調メカニズムに基づき、複数のエージェントで実行できるようにしている。その際に、WindClaw はユーザーとのやり取りを通じて、ユーザーの投資方針や選好を継続学習し、分析ロジックと出力結果

図表 3 WindClaw の各 AI エージェントの役割

エージェント名	主要機能	データソース・特性
① 板情報チェック	- 市場全体の動向を継続的に追跡 - 大口投資家の資金フローの追跡 - 当日の注目セクターを自律的に追跡し、ユーザーに該当情報を送信	Wind即時相場データベース・資金フローデータ
② 個別銘柄チェック	- 特定銘柄の価格帯や出来高の異常、重大な公告を監視 - トリガー条件設定後、エージェントがユーザーに自律的に通知	個別株の公告データベース・テクニカル指標データベース
③ 情報チェック	ユーザーが選択した業界における企業の重大政策、公告、リサーチレポートをリアルタイムで取得・整理	コンプライアンス公告データベース・Wind レポートデータベース
④ 株式アナリスト	- 上場企業の公告を自律的に取得し解読する - 業界関連のリサーチレポートのまとめ - 複数期間にわたる財務データを分析	財務データデータベース・EDGAR(米国 SECの開示書類データベース)や中国证券监督管理委员会の政策書類データベースと連携
⑤ マクロ研究者	- 中国・グローバルのマクロ経済データとHFT業界指標を統合 - トップダウンの投資フレームワーク構築を支援	マクロ経済指標データベース・Windマクロ経済データベース
⑥ ストラテジー・マイナー	- Windの過去データで株式の選択ロジックをバックテスト - 投資仮説の定量検証を自然言語で実行	Windの時系列の過去価格・財務情報データベース

（出所）WindClaw ホームページより野村資本市場研究所作成

²⁵ 本稿執筆時点では、同スキルはユーザーのポートフォリオを組成するための模擬テストのみが可能である。

を最適化する。ユーザーが WindClaw を長期に利用すればするほど、自身の投資スタイルにカスタマイズできる設計となっている。また、WindClaw のサイトには、「WindClaw フォーラム（策略工場）」というユーザー向けのオンラインのコミュニティもあり、ユーザーが自らの戦略ロジックや研究結論を共有することや、他ユーザーのエージェント設定を参照することができる。これは単なる Q&A ではなく、投資研究関連知識が集合化された Wind 独自のプラットフォームであり、ネットワーク効果がユーザー定着率を高める設計になっている。

このように、中国において金融情報ベンダーとして既に独占的な地位を確立している Wind 社が WindClaw を開発する目的は、個人・機関投資家を含む幅広い顧客に自社のデータベースに基づくエージェント型 AI を利用させることで、自社のサービスへの依存度を高め、独占的な地位を維持・向上することであると考えられる。

3. 金融業界での OpenClaw 利用における潜在的なリスク

金融業界において OpenClaw に関する取り組みが広がりつつある中、中国政府は潜在的なリスクへの懸念を表明している。具体的には、中国の国家インターネット応急センターが 3 月 10 日に公表した「OpenClaw の安全応用に関するリスクの通達」によれば、OpenClaw を利用するには、オペレーションシステムに対して最も高い権限（スーパーユーザー権限〔Root 権限〕）が必要とされるため、誤操作によりローカル環境の重要なファイルが OpenClaw により削除されることや、情報漏洩に繋がる恐れがある、とされている²⁶。これは金融分野に限らず、全ての企業に共通するものとして見て取れるが、特に金融分野におけるリスクの影響が大きいため、当局が強い懸念を示していると考えられる。

次に、工業と情報化部傘下の「ネットワーク安全脅威と脆弱性情報共有プラットフォーム（NVDB）」は、①スマートオフィス、②（ソフトウェア・システムの）開発・運営（デブオプス）、③AI パーソナルアシスタント、④金融取引、という OpenClaw の 4 つのユースケースにおける関連リスクを提示している。その上で、OpenClaw を利用する際に、「六つの実施事項と六つの禁止事項（中国語：六要六不要）」を明示している。そのうち、金融分野の OpenClaw 利用に関するリスクについて、①メモリ汚染（Memory Poisoning）により、AI が誤った売買指示を出したり、取引価格の誤認等が発生するリスク、②身分認証の回避（不正アクセス）による口座盗用のリスク、③悪意のあるコードを含むプラグイン（スキル）の導入による取引認証情報の窃盗リスク、④極端な場合に、サーキットブレーカーや緊急対応メカニズムの不備により AI エージェントが制御不能となり、頻繁な発注を行うリスク、等が想定されている²⁷。これらのリスク事項が、金融機関の基幹システムで発生した場合、金融機関のみならず、金融システム全体へと大きく影響する可能性

²⁶ 国家インターネット応急センター「OpenClaw の安全応用に関するリスク提示」2026 年 3 月 10 日。

²⁷ 工業・情報化部傘下 NVDB「关于防范 OpenClaw（“龍蝦”）開源智能体安全風險〔六要六不要〕建議」、2026 年 3 月 12 日。

もある。前述のように、中国政府が国有企業、政府機関や銀行等に対し OpenClaw の利用を制限したのは、こうしたリスクへの懸念によるものと考えられる。

Ⅳ サンドボックスによる金融業界でのエージェント型 AI の普及

中国における OpenClaw への関心の高まりは、オープンソースの OpenClaw がはじめてエージェント型 AI の水準までアップデートしたことに伴い始まった。これにより、エージェント型 AI は中国で急速に普及し、金融機関を含む多業種の生産性向上につながる可能性が出てきた。一方で、前述のように、OpenClaw の利用に伴うリスクが顕在化している。

こうした中、中国における金融機関は、OpenClaw をはじめとするエージェント型 AI の利用において、自社の基幹システムで OpenClaw を直接導入するというやり方だけでは、上記リスクを解決できず、更なる利用拡大に支障が生じる可能性がある。そのため、個別企業の自助努力だけでなく、中国政府または市場全体による支援制度の導入も重要と考えられる。

その一案として、金融機関のみを対象とした「サンドボックス」におけるエージェント型 AI の試験運用の促進が有力な手法となり得る。中国では既に、中国人民銀行と証監会の各々の管轄下で、FinTech サンドボックス制度が運用されている²⁸。金融機関が、これら既存の FinTech サンドボックスを利用することで、自社の基幹システムに OpenClaw を導入することなく、金融システムに影響を与えないような隔離された環境で OpenClaw のユースケースを開発し、試験運用を行うことができると考えられる。その際に、①ゲートウェイの認証、②プラグインの事前監査、③不要なネットワーク通信におけるデータの出入口（ポート）の閉鎖、④サーキットブレーカー型の緊急停止メカニズムの整備、等のリスク対策を導入し、その効果を検証することが想定される。

こうした対策が講じられれば、証券会社をはじめとする金融機関は、OpenClaw を含むエージェント型 AI を安全に活用することができ、リサーチ業務を含む多様な業務の拡大に繋げることができると考えられる。また、金融機関はエージェント型 AI の活用による従業員の業務効率化を通じて、既存ビジネスモデルの変革を促進するとともに、人間にしかできない付加価値の高いビジネスの創出も可能になる²⁹。

²⁸ 中国人民銀行が2019年12月に主導で、北京市において実施された「FinTechイノベーション監督管理テスト」や、証監会が2021年11月に北京市で実施した「資本市場 FinTech イノベーションテスト」が挙げられる。

²⁹ 例えば、証券会社のリサーチ部門であれば、アナリストは担当企業の報告書解読や財務データ整理といった、定型的な作業をエージェント型 AI に遂行させ、空いた時間を企業の現地調査や経営陣へのインタビュー等の人間にしかできない業務に使うことで、他社との差別化を図ることができる。