



AI エージェントが拓く業務自動化の最前線

上田 雄登 (GenerativeX CAIO)

ChatGPT が登場し、生成 AI の旋風が吹き荒れてから約 2 年。対話型 AI の便利さは広く認知された一方、「実務を丸ごと置き換えるほどではない」という声も根強い。そこで登場したのが AI エージェント、すなわち"考えて答える"だけでなく"自ら動く"ことで、チャット型の限界を超えようとしている存在だ。本稿では、その基礎概念と従来方式との比較をあらためて整理しつつ、M&A やデューデリジエンス、管理会計などでの具体的ユースケースを紹介する。最後に、導入現場でよく聞く疑問と留意点もまとめたので、AI エージェントに詳しい方は復習がてら、これから活用法を学ぶ方はウォーミングアップがてら読んでいただきたい。

AI エージェントとは何か

「エージェント」と聞くと保険の営業担当や不動産仲介を連想するかもしれないが、AI の世界でも役割は似ている。ユーザーとシステムの間に立ち、目的達成のために必要な作業を段取り・実施してくれる"代理人"だ。

最大の特徴は「自律性」にある。ユーザーがエージェントに出す指示は「見積もりを取って比較しておいて」程度の曖昧なものでもよい。エージェントは自分で与えられたタスクを整理・分解し、作業手順を決め、途中で方針を微調整しながらゴールに向かう。さらに「行動能力」も持っており、必要に応じて外部 API や社内システムを呼び出して情報を入手し、完成品のファイルを生成・保存するところまで完結させる。要は「手と足」を持った生成 AI である。

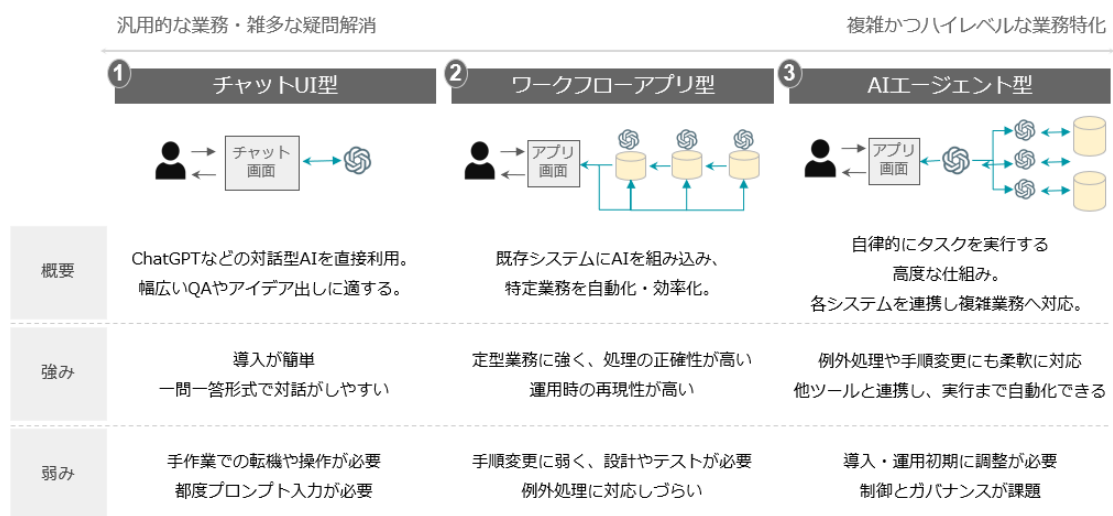
従来のチャットボットを"口だけ AI"とするなら、エージェントは"手足付き AI"といえるだろう。口だけ AI でも十分便利だが、資料作成やアプリケーションの操作は結局人手が要するため「あとひと押し感」が残っていた。その壁を越えようとしているのが、この AI エージェントである。

チャット型／ワークフロー型との違い

では、既存の生成 AI 活用方法とはどう違うのか。チャット型は一問一答の積み重ねであり、会話は楽だが転記が面倒という課題があった。都度プロンプト指示を入力する必要があり、手順を変更する際も毎回プロンプトを作り直す必要がある。例外処理が発生すれば、こちらもその都度人間が判断して対応しなければならない。

一方、ワークフロー型は RPA に"生成 AI の知恵"をまぶしたようなもので、作業過程を事前にワークフローとして練り上げ、これを起動させる決め打ちのボタンやフォームで操作する。段取りは固い分、ルートから外れると弱い。手順変更には再設計とテストが必要で、想定外の例外が発生すると処理が停止してしまう。

これに対してエージェント型は、RPG のパーティーリーダーのような存在だ。目的（クエスト）だけ伝えたと、仲間（ツール）を呼び出し、必要かもしれない作業に寄り道しつつも、できるだけ最短でゴールすることを目指す。手順の変更にも柔軟で、プロンプトを一部修正するだけで対応できる。例外処理に遭遇しても、AI が自らリトライしたり代替手段を探索したりする。



生成 AI エージェントのユースケース

実際に AI エージェントがどのように活用されているか、当社開発案件を参考にしながら、いくつかの事例を見てみよう。

M&A エージェントは、買収候補リストの整理や資料作成を担当する。企業情報をクロールして分析し、会社情報を検索。最終的には PowerPoint 資料の下書きまで生成する。初期検討にかかる"資料作成地獄"を大幅に短縮できるのが魅力である。

デューデリジェンス・エージェントは、大量の資料からリスク要素の有無を確認し、評価レポートのドラフトを作成する。資料が格納されているフォルダ構造から情報の所在を推定したりキーワード検索を駆使することで情報を抜粋・整理し、レポート雛形へ反映させる。雑多なフォルダでも「まず全件読む」のではなく、"怪しいエリア"に当たりを付けてから深掘りするため、速度と網羅性のバランスが良い。

管理会計エージェントは、会計データの異常検知と原因調査に特化している。会計システムへ API を通じてログインし、全仕訳を調査する。各項目の大幅な増減を抽出して過去のコミュニケーションログや関連稟議書を検索し、内容の妥当性に関するコメントや変動の原因を説明する報告書を生成する。ただし、会計システムへの書き込み権限は"要人間承認"として事故防止を図っている点が重要だ。

いずれの事例も、単なる生成 AI を超え、業務フローに組み込まれた"行動する AI"としての機能を発揮しており、他業務への展開においても大いに参考となるだろう。

よくある疑問への回答

導入検討時によく聞かれる疑問についても触れておこう。

まず「エージェントが勝手に暴走しないか」という懸念だが、これは適切な権限設計で十分に制御可能である。権限設計は"自動運転"と同じ発想で考えるとよい。データ閲覧は自動で OK、書き込みは必ず信号（承認）を挟む——これだけで大事故は避けられる。このようにデータの閲覧は自動化しつつ、システムへの書き込みには必ず承認フローを挟むという設計をすれば、万が一の場合でも被害は「時間の無駄」程度に限定できる。

「従来のワークフロー型システムとどう使い分ければよいか」という質問もよく頂く。実際のところ両者の境界は明確ではなくグラデーション的であるが、例外処理をルールとして書き切れない業務や、手順が頻繁に変更される業務であれば AI エージェントが向いている。AI エージェントは目的達成に向けて柔軟に判断・設計しながら動くことができるため、業務の手順や条件が固定されていない状況において、その力を発揮する。

また、「精度を高めるにはどうすればよいか」という質問に対しては、まず業務知識をどれだけ正確にプロンプトへ落とし込めるかが鍵になる。AI エージェントは“外付け脳”として動くため、プロンプトは新人研修のマニュアルと同じで、抽象的な指示では不安定になりやすい。細かな要件や判断基準を丁寧に記述することで、はじめて安定したパフォーマンスが得られる。曖昧な指示では、人間への「ムチャ振り」と同様に成果がばらついてしまうため、明確な指示の言語化が成功の鍵となる。

まとめ

AI エージェントは"万能ロボ"ではないが、「段取り＋実行」を丸ごと肩代わりできる初めての AI 形態と言える。段取りから柔軟に考えてくれる点が、ワークフロー型の自動化と異なる点である。導入の第一歩は、既にマニュアルやチェックリストが整備されている業務から小さく試すことだ。成功体験をチームで共有しつつ、プロンプトと権限設計をブラッシュアップすれば、次第に「AI が働き、人が判断する」未来図が具体化していくだろう。

生成 AI の進化は留まることを知らない。チャット型で満足することなく、ワークフロー型で妥協することなく、エージェント型という新たな選択肢を検討する時期に来ている。それは単なる効率化ツールではなく、私たちの働き方そのものを再定義する可能性を秘めているのだから。