

Contents

● はじめに	3
--------	---

Part

1

自ら動き出すAIの時代 AIエージェントとは	9
---------------------------	---

001 AIエージェントとは何か	10
002 従来のAIや自動化ツールとの違い	12
003 AIエージェントの代表的な使い方	14
004 AIエージェントの分類と特徴	16
005 AIエージェントの仕組みと内部構造	18
006 AIエージェントを導入するメリット	20
007 AIエージェントに向いているタスク	22
008 AIエージェントに向かないタスク	24
009 RAGとAIエージェントの違い	26
Column タコとミツバチに学ぶAIエージェントの協働パターン	28

Part

2

自律する知能の設計図 AIエージェントの仕組み	29
----------------------------	----

010 AIエージェントはどう動くのか	30
011 生成AI（大規模言語モデル）とは何か	32
012 大規模言語モデルはどう考えるか	34
013 複雑タスクに強くなる推論技術の仕組みと進化	36

014 エージェントに一貫性を持たせるシステムプロンプト	38
015 AIエージェントを支える2つの記憶	40
016 制約を織り込むタスク設計	42
017 ツール連携 APIとFunction Calling	44
018 実行とモニタリング	46
019 ハルシネーションの正体とその対策	48
Column ビジネスマンでも作れるAIエージェント	50

Part

3

AI進化のロードマップ AIエージェントの発展段階とレベル定義	51
------------------------------------	----

020 AIエージェントの進化の全体像	52
021 レベル1：ルールベースRPA	54
022 レベル2：部分的に生成AIを組み込んだワークフロー	56
023 レベル3：AI自身が考える自律型ワークフロー	58
024 レベル4：複数エージェントの連携	60
025 レベル5：企業全体を貫く自律的AIエコシステムの実現	62
026 AIエージェントと人間組織の相似性	64
027 人間の役割はどう変わるか 監督・評価・設計への転換	66
028 AIエージェントを包括的に捉える3つの観点① システム連携度	68
029 AIエージェントを包括的に捉える3つの観点② タスク起動方式	70
030 AIエージェントを包括的に捉える3つの観点③ 自律性と人間協働	72
Column イシュー分析で組むマルチエージェント	74

Part

4

AIが変える仕事の現場 領域別にみるAIエージェント活用事例..... 75

031	個の力を解放するパーソナル・アシスタント.....	76
032	顧客接点を変革するセールス・マーケティングエージェント.....	78
033	サイロを壊すバックオフィス・プロセス・エージェント.....	80
034	経営者の右腕となる意思決定支援エージェント.....	82
035	業務効率化を加速する開発・IT支援エージェント.....	84
036	暮らしを豊かにするライフスタイル・エージェント.....	86
037	UI操作自動化のClaude Computer Use、 業務タスク自動化のOperator.....	88
038	営業や顧客対応を支援するSalesforce Agentforce.....	90
039	ソフトウェア開発に特化したエージェントDevin.....	92
040	対話型ショッピングエージェントRufus.....	94
041	事例に共通する価値創出の4つの要素.....	96
Column	AIエージェントでさらに重要になるプロンプトエンジニアリング.....	98

Part

5

安全と成長のマネジメント AIエージェント導入・設計・運用の実践..... 99

042	AIエージェントの設計要素.....	100
043	スモールスタートで始める導入計画.....	102
044	アジャイル開発の有効性.....	104
045	適用業務の見極めと優先順位づけ.....	106
046	AI主軸のワークフロー設計.....	108
047	ツール連携の重要性.....	110

048	AIエージェントのUI／UX設計.....	112
049	モニタリングと継続的改善サイクル.....	114
050	ガードレールとHuman In The Loop.....	116
051	権限管理とセキュリティ対策.....	118
052	MCPによる接続の最適化.....	120
053	運用体制と組織内役割.....	122
054	現場と経営が動かす成功のスイッチ.....	124
Column	AI エージェントは「使用人の民主化」か？.....	126

Part

6

AIと歩む新しい世界 AIエージェントと共創する未来..... 127

055	AIエージェントが拓く未来.....	128
056	汎用人工知能（AGI）への道標.....	130
057	AIエージェントと組織進化.....	132
058	エージェント・エコノミーの誕生.....	134
059	仕事の消滅と創出.....	136
060	超パーソナライゼーション社会の到来.....	138
061	未来の羅針盤、共創への招待.....	140

• Index.....	142
--------------	-----

AIエージェントの分類と特徴

自律性と用途で見るAIエージェントの分類と活用法

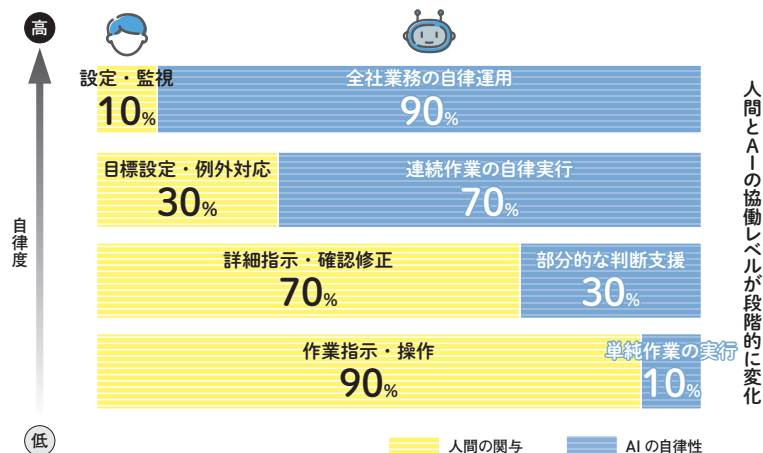
AI エージェントを理解するには、「**個人向けか企業向けか**」と「**どこまで自律して動けるか**」という軸で整理するとわかりやすくなります。まず用途の違いからです。パーソナルエージェントは個人の日常を支援します。旅行計画エージェントを例にすると、出発地と予算を伝えるだけで日程表を設計し、航空券やホテルを予約してくれます。企業エージェントは、組織のルールや基幹システムと連動し、業務プロセスを自動化したり、情報の流れを調整したりと、さまざまな業務の効率化や最適化を支援します。営業や経理、人事など幅広い領域で活用され、組織全体の生産性を高める役割を担います。

次に、自律性の度合いに応じたレベル分類です。あらかじめ決まった手順しか実行しない RPA をレベル 1 と定義します。たとえばコールセンターで着信件数を数えて定型フォームに振り分けるだけならここに当たります。レベル 2 では部分的に生成 AI を挟み、入力文の要約や分類を AI が担当することで柔軟性が増します。営業資料の骨子を AI が書き、人間が確認するシナリオが典型です。レベル 3 になると AI 自身が手順を立案し、外部ツールを呼び出して結果を吟味しながら完了まで走り切ります。レベル 4 では複数のエージェントが役割分担し、開発進捗を管理するエージェントと、リソース配分を調整するエージェントが連携してプロジェクトを円滑に進めるといった「エージェント間の協働」が可能です。**最上位のレベル 5 では会社全体の業務がほぼ自動化され、人間はモニタリングや緊急時対応のみを行います。**

パーソナル vs. 企業エージェントの違い

	パーソナルエージェント	企業エージェント
主な対象	個人ユーザー	組織・チーム
活用シーン	旅行、予定管理、日常支援	経費精算、在庫管理、業務自動化
動き方	ユーザーの予定や指示で自律行動	社内ルールと連携し業務を実行
シナリオ例	旅行予約・天気ですべてを自動調整	見積～請求の全自動処理

AIエージェントの自律度と人間の関与度



まとめ

- ☐ 自律性の段階に応じて分類
- ☐ 個人向けと企業向けで用途と設計思想が異なる

制約を織り込むタスク設計

複雑な制約条件を織り込んだ業務例

AI エージェントにおいて、タスクの設計は極めて重要です。**エージェントが実行すべきタスクは単なる指令の羅列ではなく、明確な目的を踏まえつつ、社内外の業務制約を織り込んだワークフローとして記述されなければなりません。**

たとえば「クライアント A に請求書を送る」という一見シンプルな業務でも、実際には多くの制約があります。顧客によって受け付け可能なファイル形式が異なり、社内では上長・部門長・経理の3段階承認が必要で、セキュリティ要件として暗号化送信が求められるといったルールが存在します。

従来の RPA は、これらを事前に決められた手順通りに処理するだけでした。しかし AI エージェントは違います。まず顧客のファイル形式要件を確認し、承認フローを呼び出し、コンプライアンス要件をチェックして、最終的に「**①要件確認→②書類作成→③社内承認→④ファイル変換→⑤暗号化送信**」という最適なワークフローを自動生成します。途中で例外が発生すれば人間に判断を仰ぐ仕組みも備えておくと安心です。

重要なのは、制約条件が変化したときの対応力です。**新しい規制やクライアント要望、社内ルールの変更があっても、AI エージェントは瞬時に作業手順を見直し、最短ルートを再構築できます。**この「状況に応じた自律的な判断力」こそが、業務効率化とリスク管理を同時に実現する鍵となります。

「AI に渡す仕事の設計図」であるタスク設計とは

1. なぜ重要か？

道に迷わない

人間と同様に、AI も指示が曖昧だと途中で行き詰まる

エラーを減らす

最初に細かく分解しておけば、どのステップで失敗したかがすぐわかり、リトライしやすい

再利用できる

いったん設計図を作れば、別の案件でも“型”として流用できる（社内標準プロセスになる）

2. 基本の 5 ステップ

ステップ	何をする？	具体例（出張の手配を任せる）
① 目的を宣言	ゴールと成功条件を一文で書く	「来週の大阪出張を最安値で手配し、旅程を共有して」
② 制約を列举	予算・納期・NG 事項を並べる	「宿泊 1.5 万円以内」「10:00 着必須」「社割サイトのみ」
③ 手順を分解	大タスク → 小タスクへ“箇条書き”	フライト検索 → 料金比較 → 予約 → 旅程作成
④ ツールを割当	各タスクで使う API やファイルを指定	Skyscanner API / 社内予約フォーム / Google カレンダー
⑤ モニター方法	途中結果をどう確認・修正するか決める	(1) 確定前に見積を Slack へ送信 → (2) OK なら実行

3. よくある質問

Q 全部 AI に考えさせればいいのか？

A ゴールと制約を伝えるだけで自動分解してくれる高度なエージェントもあります。ただし業務で使うなら“人間が理解できる設計図”を残すほうがリスク管理しやすいです

Q どの粒度で分解すればいい？

A 目安として「1 つの作業で 1 つのツールだけを使う」「作業結果の確認が簡潔にできる」程度が理想的です。作業が大きすぎるとエラーが起きたときに原因を特定するのが困難になり、逆に小さく分けすぎると作業の切り替えや管理にかかる手間が増えて非効率になります

まとめ

- ☐ 生成 AI はファイル形式・承認フローなど業務制約を踏まえ手順を生成
- ☐ 単純 RPA を超える自律的タスク設計が競争優位を生む

レベル4：複数エージェントの連携

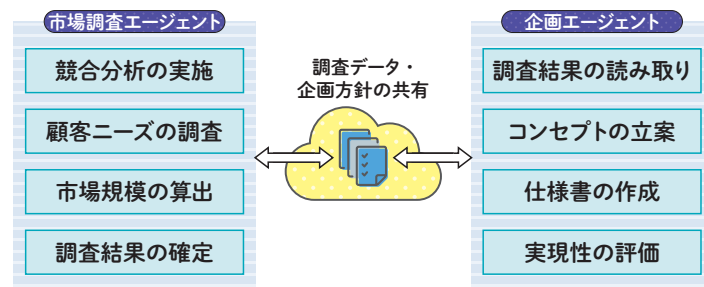
対話でタスクを受け渡す自律型マルチエージェント

レベル3までは、ひとつの生成 AI が計画から実行までをすべて担う「単独プレイヤー型」でした。これに対し、レベル4では**複数の AI がそれぞれの得意分野を担当し、メッセージをやり取りしながら連携して作業を進めるようになります。いわば「チーム型」の AI**です。たとえば、新商品開発では、市場調査エージェントが競合分析や顧客ニーズを調査し、その結果を企画エージェントに渡して商品コンセプトを立案します。さらに技術エージェントが実現可能性を検証し、マーケティングエージェントが販売戦略を策定するといった具合に、専門性の異なるエージェントが順次作業を引き継いでいきます。このように自律したエージェント同士が連携する仕組みをマルチエージェントシステムと呼びます。

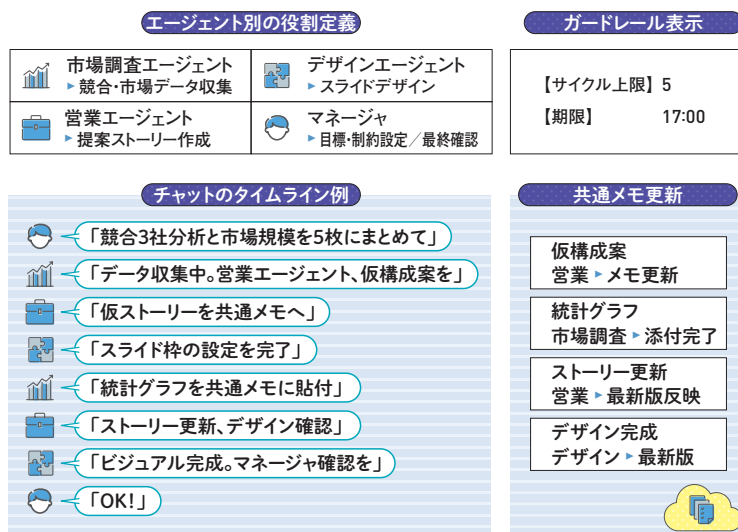
この仕組みを実現するためには、いくつかの工夫が必要です。まず、**それぞれのエージェントに明確な役割と責任を持たせる**こと。そして、全体の進捗や状況を共有できる「共通メモ」のような情報の土台を用意すること。さらに、作業が滞った場合にエージェント自身が計画を見直してやり直せる仕組みを整えることが重要です。

そのため、いきなり大きな仕組みを作るのではなく、**まずは2～3体の AI を使って小さなタスクから試すのが現実的**です。記録を観察しながら役割分担ややり取りの方法を調整し、徐々に精度を高めていくことが成功の鍵となります。こうして、チーム単位のエージェントが自律的に動くようになれば、次の段階である「組織全体の自動運営」へとつなげる土台が整います。

複数エージェントによる分業と連携のモデル



エージェント同士が対話しながらチームで協働



役割の明確化+チャットでの対話でタスクを受け渡し。ガードレール設定で迷走を防ぎ、チームでゴール達成

まとめ

- ☐ 専門AIが役割分担し対話で連携しながら業務を遂行
- ☐ 小規模から始めて連携の精度を高める段階的導入が重要

対話型ショッピングエージェント Rufus

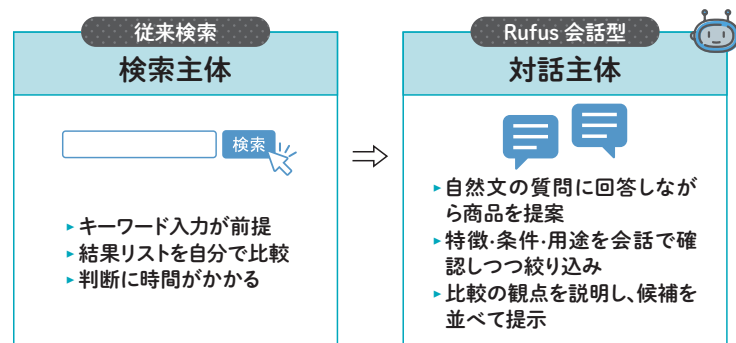
Amazonが拓く新しいEC体験

Amazon が2024年に発表した「**Rufus (ルーファス)**」は、生成AIを活用した対話型ショッピングエージェントです。従来のECサイトは検索窓にキーワードを入れて商品を探すのが基本でしたが、**Rufus は自然な質問に応じて商品候補を提示し、“会話のパートナー”のように機能することを目指しています**。利用者は知識のある販売員に相談しているような感覚を得られる点が特徴とされます。たとえば「初心者におすすめのランニングシューズは？」と尋ねると、価格やレビューだけでなく、特徴を比較しながら複数案を示すことがあります。単なる検索結果の羅列ではなく、「なぜその商品が良いのか」に触れる説明が加わることで、利用者は基準に合った選択をしやすくなります。さらに追加の質問を重ねることで選択肢を絞り込み、人間に相談するような体験に近づきます。

Rufus は購買履歴や閲覧傾向を踏まえて文脈を解釈する仕組みも備えているとされ、過去の関心を反映した提案が行われることもあります。こうした仕組みによって、膨大な商品群の中から迷わず意思決定できるよう支援する狙いがあります。Amazon にとっては単なる検索機能の強化にとどまらず、買い物体験全体を再定義する試みとも位置づけられています。

現時点では米国を中心に展開されており、今後の拡大についても報じられています。Rufus は Amazon における AI エージェント活用象徴的な事例のひとつであり、EC の在り方を変える可能性を示しているといえるでしょう。

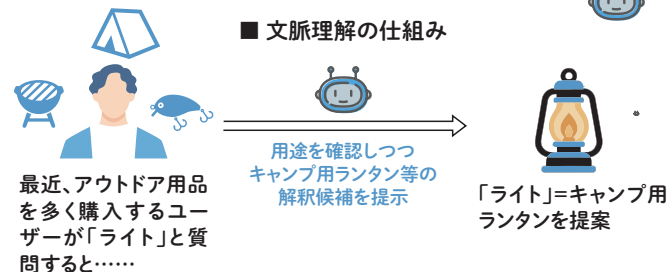
Rufusによる会話型AI検索と従来検索の違い



■ 利用シーン例



■ 文脈理解の仕組み



まとめ

- ☐ Rufusは会話型AIで迷いのない商品選びを実現する
- ☐ 検索主体から対話主体へ、購買体験が根本から変わる

AIエージェントのUI／UX設計

● 人間と生成AIが同じ風景を眺めるための“設計図”づくり

AIエージェントはチャットベースのUIではありません。**ユーザーが直感的に操作でき、業務フローに自然に溶け込むUI／UX設計こそが、AIエージェント導入成功の鍵**となります。

UI設計では、多様な操作方法を提供することが大切です。自然言語での指示入力に加えて、定型的なタスクについてはボタンやフォームによる簡単操作も併用することで、幅広いユーザーに対応できます。チャット形式に慣れていないユーザーでも、直感的に操作できるグラフィカルなインターフェースを提供することが効果的です。

また、**AIエージェントの動作状況を可視化するダッシュボードも欠かせません**。推論技術やリサーチ機能を使うとタスクの実行に時間がかかるためです。現在どのタスクを実行中なのか、進捗状況、エラーの有無をひと目で把握できる仕組みが必要です。複数のタスクを並行処理する場合には、優先度や完了予定時刻も表示することで、ユーザーの業務計画をサポートします。

さらに、**人間の介入や判断が必要な場面では適切な通知機能を組み込みます**。重要度に応じた通知方法の使い分けや、承認待ちのわかりやすい表示により、スムーズな協働を実現します。

UX設計では、既存の業務環境への自然な統合を目指します。Slackからのメンションで呼び出せるなど、ユーザーが慣れ親しんだツール内でシームレスに機能することで、学習コストを最小限に抑えます。また、AIの判断根拠を適度に可視化することで、ユーザーの信頼感を高め、安心して業務を任せられる環境を構築できます。

● UI／UXの実例

■ AI エージェント利用における UI／UX 要素

自然な統合・信頼性
Slack連携、根拠提示

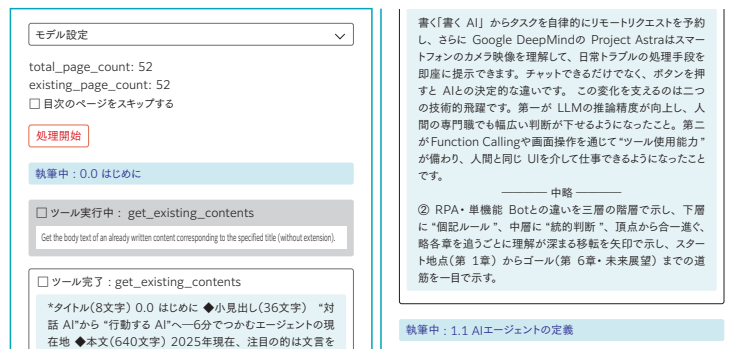
可視化と通知
ダッシュボード、承認通知

基本操作性
チャット、ボタン、フォーム

■ Slack からのメンションで呼び出しする例



■ 「どのタスクを実行中か」「どの段階まで進んでいるか」がひと目でわかる UI



まとめ

- ☐ 業務フローを可視化し、人間とAIの切り分けを明確に
- ☐ 入力負荷を減らし、AIを感じさせない設計に

汎用人工知能 (AGI) への道標

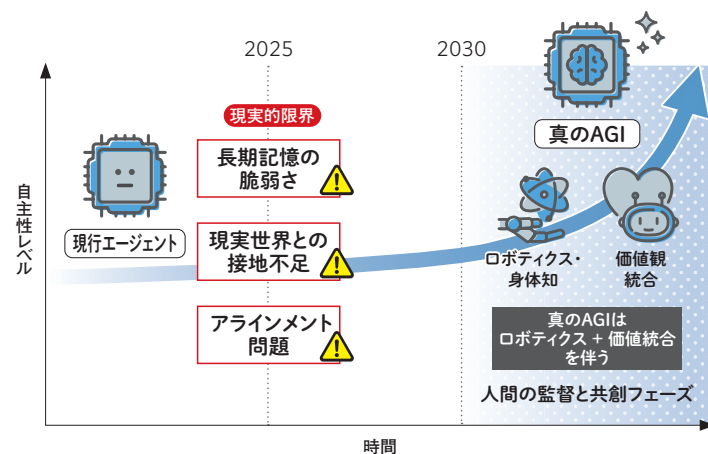
数年先に見える可能性と長期的な課題

汎用人工知能 (AGI = Artificial General Intelligence) は、特定の分野に限らず幅広い仕事をこなせる AI の究極形とされます。OpenAI は「**経済的に価値ある大半の仕事で人間を上回る高自律システム**」と定義し、2025 年初頭には「AGI の作り方を理解した」と発言しました。ただし、定義は研究者や企業によって揺れがあり、性能を測る共通の基準も確立していません。現行の大規模言語モデルは膨大な計算資源や電力を必要としつつも、常識や現実世界との結びつき、長期記憶の維持といった点に課題を抱えています。研究の進展は見られるものの、飛躍的に汎用性が高まったとまでは言えません。そのため、AGI の議論は技術的な進歩だけでなく、持続可能性や社会的受容といった観点から行われる必要があります。

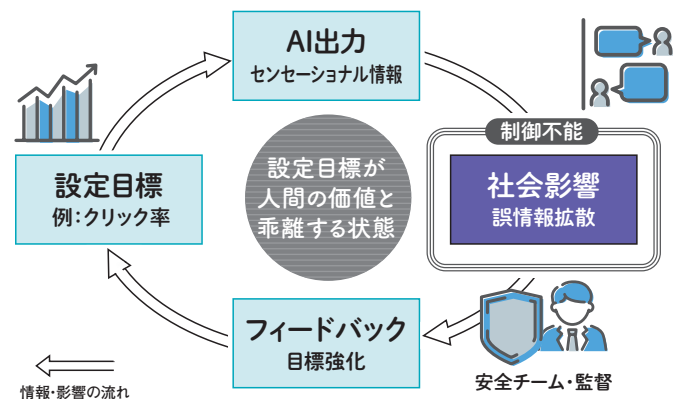
出力が社会に及ぼす影響を人間が完全に制御しきれない「**アライメント問題**」も依然として残っています。たとえば、クリック率の最大化を目的とする仕組みでは、センセーショナルな情報が優先表示される可能性があります。課題に対応するため、OpenAI を含む各社は安全体制を見直し、リスク管理を強化しています。

専門家の多くは、デジタル領域に限定すれば「実用上の AGI」と呼べる性能が数年内に到来する可能性を認めています。一方で、身体を伴う知能や価値観の統合には長い時間がかかるとの見方が一般的です。つまり、エージェントの自律性は確実に高まるものの、人間の監督や協調が欠かせない段階が当面続くというのが、2025 年現在の現実的な展望と言えるでしょう。

AGI 到達のロードマップ



アライメント問題^[*]とは



[*] アライメント問題とは、AI が人間の意図や価値観から外れた行動をとってしまう危険性をどう防ぐか、という課題のこと

まとめ

- ☐ AGI は定義・評価が未整備で、克服すべき課題が残る
- ☐ 当面は限定領域で自律性を活かしつつ、人間との共創型が現実解となる