

エージェントが生成AIの次の フロンティアである理由

情報から行動へ

AIの次の進化

知識ベースのAIから行動指向のAIへ。

そして質問に答えてコンテンツを作成するチャットボットのような生成型AIツール。

そして今：複雑なマルチステップタスクやワークフローを実行できるAI対応「エージェント」。

重要なのは、思考から行動へのシフトである。

AIエージェントとは？

エージェントは、ダイナミックな世界で独自に計画を立て、行動することができるデジタル・システムです。生成AIを搭載しているため、事前にプログラムされたルールに制限されることはありません。

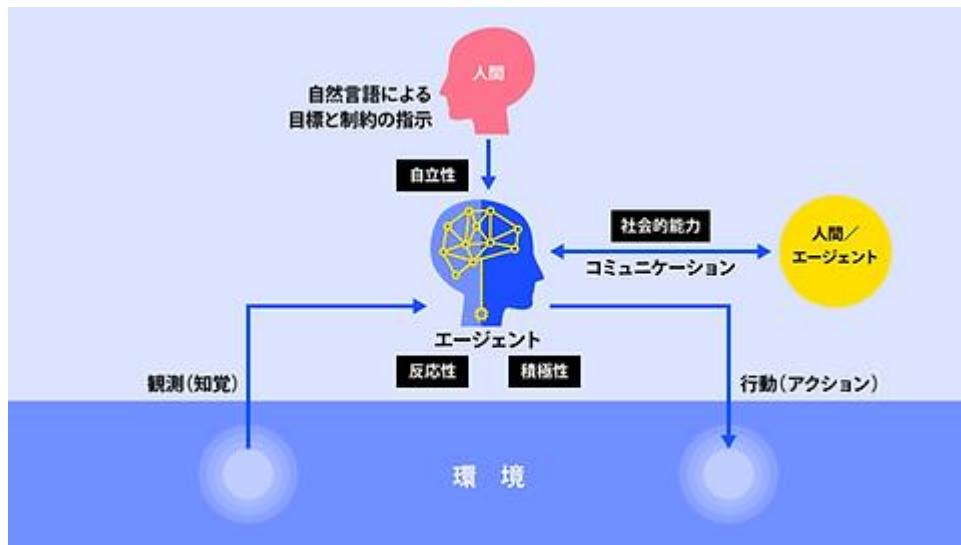
コア機能

- ・ **計画**：戦略を立て、複雑な目標をステップに分解する。
- ・ **ツールを使う**：ソフトウェア、ウェブサイト、データベースと連動する。
- ・ **協力する**：人間や他のエージェントと協働する。
- ・ **学ぶ**：経験やフィードバックに基づいてパフォーマンスを向上させる。
- ・ **自然言語**：日常的な言語で指示を理解し、受け取る。

熟練したバーチャルな同僚と考えてください。

AIエージェントとは？

- 自律性、反応性、積極性、社会的能力という4つの特性が連携して、AI Agentが目標達成する仕組みを表しています。



AIエージェントの主な特徴

AIエージェントは、ダイナミックなデジタル世界と相互作用することで、独立してタスクを完了できる高度なシステムである。AIエージェントは、環境からの情報に基づいて行動を起こすことができる、生成的AIのより有能なバージョンである。

思考から *行動* へのシフトである。

AIエージェントの主な特徴

- **自律性:** 人間が目標を設定し、エージェントは自ら最善の行動方針を見つけ出す。
- **行動指向:** ツールを使用し、外部システムとのインターフェイスを使ってタスクを実行する。
- **反復的改善:** エージェントはフィードバックを受け、タスクを継続的に改善することができる。
- **自然言語による指示:** ユーザーは、コードではなく、日常的な言語を使用して複雑なワークフローを指示することができます。
- **複雑なワークフロー管理:** 高レベルの指示をサブタスクに分解し、目標を達成するために他のエージェントやツールと調整します。

エージェントはどのように価値を生み出すか

エージェントは、これまで管理が困難であった複雑で変化しやすいタスクを自動化することができます。

1. **多様性を管理する**：厳格なルールベースのシステムとは異なり、不測の事態に適応し、さまざまなシナリオに対応できる。
2. **自然言語による指示**：技術者でない従業員でも複雑なワークフローを指示できるため、自動化がより身近になる。
3. **既存のツールとの統合**：エージェントは、すでに使用しているソフトウェア、アプリ、プラットフォームに接続し、操作することができます。

エージェントができる作業

- **カスタマーサポート**
- 顧客からの問い合わせに自律的に対応
 - 問題特定、解決策提示
 - 必要に応じた専門スタッフへの切り分け、引継ぎ
- **事務作業**
- 定型的な事務作業を自動化し、業務効率を向上
 - 会議の日程調整、議事録作成
 - メール対応（経緯要約、回答案生成）
- 従業員がよりクリエイティブな仕事に集中できる環境を提供
- **データ分析**
- データ解析と対話的なプロセスでユーザーの意思決定を支援
 - 「今期売上が最も伸びた商品は何か？」「その商品の売上が伸びた地域は？」といった問いへの回答
- **ソフトウェア開発**
- コード生成、デバッグ支援、タスクの自動化
 - 開発者の説明に基づくサンプルコード生成
 - エラーメッセージからの修正案提示
 - テストケースの生成や実行の自動化による品質向上

エージェントができる作業

- マーケティングコンテンツ作成
- SNS投稿やキャンペーン資料作成の支援
 - 新商品の特長に基づいたキャッチコピー、投稿文生成
 - ターゲット層に訴求するデザイン案や画像生成
- 教育
- 教育分野における個別最適化学習
 - 学習者の進捗分析、苦手分野特定、適切な練習問題提案
 - 教員向けの事務作業自動化（テスト採点、出席管理）
- バリエーション豊かなAIエージェント
- 役割や適用範囲は非常に幅広い
- 人間の意思決定や創造性支援に重きを置くもの
- 人間の負担軽減のための自動実行に重きを置くもの
- 特定業務に特化したAgentと、幅広い分野で活用できる汎用型Agentが存在

エージェントシステムの仕組み

ユーザーのリクエストは、協調的なマルチステッププロセスによって実行されます。

1. **ユーザーのプロンプト**：ユーザーが自然言語でタスクを割り当てます。
2. **計画と割り当て**：マネージャー」エージェントがゴールを解釈し、プランを作成し、サブタスクを専門エージェント（例：アナリストエージェント、プランナーエージェント）に割り当てます。
3. **実行とコラボレーション**：スペシャリストエージェントは、データを収集し、ツールを使用し、協力して課題を完了します。
4. **レビューと反復**：エージェントチームはアウトプットをユーザーと共有し、フィードバックを受け、目標が達成されるまで作業を改善します。

AIエージェント台頭の3つの理由

- **理由1: 大規模言語モデル (LLM) の飛躍的な進化**
 - GPT-3.5やGPT-4などの登場により、AIがより自律的にタスクを理解・実行可能に
- **理由2: AI技術のアクセシビリティ向上**
 - LLM APIやクラウドインフラの普及
 - LangChainなどのフレームワークにより、開発と実験が容易に
- **理由3: ビジネスにおけるAIエージェントへの関心の高まり**
 - 主要なテクノロジー企業が関連機能やサービスを導入
 - AIエージェントが「未来の技術」から「現在のビジネスチャンス」へと認識が変化

ユースケース1：ローン査定

課題信用リスクメモの作成に時間がかかり（1～4週間）、15以上のソースからデータを分析する必要がある。

エージェントのソリューション

- エージェントのチームが、リレーションシップ・マネージャー、財務アナリスト、評論家の役割を果たします。
- 彼らは書類を集め、財務比率を計算し、誤りを特定し、協力してメモの草案を作成する。
- 人間のチームが最終版をレビューし、フィードバックを提供します。

潜在的なインパクト時間を**20～60%**削減し、検証を容易にする完全な透明性を提供。

ユースケース2：コードの近代化

課題：レガシーソフトウェアのアップグレードにはコストと時間がかかり、エンジニアは古いコードを手作業で文書化する必要がある。

エージェントのソリューション

- ・ レガシーソフトウェアのエキスパート」エージェントが古いコードベースを分析し、そのロジックを文書化します。
- ・ 品質保証」エージェントがドキュメントを批評し、検証のためのテストケースを作成する。

潜在的なインパクト生産性を大幅に向上させ、ソフトウェア移行のコストを削減する再利用可能なプロセスを作成します。

ユースケース3：オンラインマーケティング

課題 キャンペーンの立ち上げは、多くのデジタルツールを含む複雑なワークフローです。

エージェントのソリューション

- マーケティング担当者がキャンペーンの目標をわかりやすく説明します。
- 戦略、コンテンツ、デザインのスペシャリストによるエージェントシステムが、キャンペーンのアイデアを開発し、テストします。
- エージェントはマーケットリサーチプラットフォームとアナリティクスツールを使い、ターゲットを絞ったコンテンツを作成する。

潜在的なインパクト マーケティング・エコシステム全体をつなぎ、ブランド・リスクを最小限に抑えながらキャンペーンのインパクトを最適化。

エージェントの時代にどう備えるか

知識を成文化する：ビジネス・プロセスと専門知識を文書化する。これはエージェントを指導・訓練するための資料となる。

戦略的技術計画：データおよびITシステムを整理し、エージェントが効果的にアクセス、操作できるようにする。

ヒューマン・イン・ザ・ループ・コントロールの確立：明確な監督メカニズムを構築する。人間は、アウトプットを検証し、エージェントの自主性を管理し、正確性とコンプライアンスを保証できなければならない。

利点と機会

AIエージェントの主な価値は、歴史的に対処が困難でコストのかかる、入力と出力が大きく変化する複雑なユースケースを自動化することです。

主な利点

1. **生産性の向上**：エージェントが面倒な反復作業を処理することで、人間はより高度な作業に専念することができます。
2. **複雑なワークフローの自動化**：リアルタイムで予期せぬ状況に適応することで、ルールベースのシステムの「もろさ」を克服します。
3. **アクセスしやすい自動化**：自然言語による指示により、技術者でない従業員でもプロセスを自動化できます。
4. **シームレスなツール統合**：エージェントは、既存のソフトウェア、アプリケーション、プラットフォームを接続し、操作することができます。

利点と機会

エージェントの自律性は、重大な新たな課題をもたらす。

主な懸念事項

- **プロンプト・インジェクション攻撃**：悪意のある行為者がエージェントを騙して予期せぬ有害な行動を取らせる可能性がある。
- **データプライバシーとセキュリティ**：エージェントは膨大なデータを推論するため、適切に保護されなければ漏洩のリスクが生じる。
- **事実の正確さ（幻覚）**：LLMのミスが連鎖的に影響し、金融や臨床の場面で深刻な結果を招く可能性がある。
- **人間とエージェントの信頼関係**：ユーザーはエージェントを信頼しすぎる（改善の妨げになる）か、信頼しすぎる（監視の欠如につながる）可能性がある。

独自のリスクを理解する

エージェントの自律性は、慎重な管理を必要とする新たな課題をもたらす。

- **潜在的に有害なアウトプット**：一つのエラーや幻覚が、重大な悪影響に連鎖する可能性がある。
 - 緩和策人間による監督、説明責任の枠組み、透明性。
- **ツールの悪用**：セキュリティの脆弱性を見つけたり、巧妙な詐欺を行ったりするために、エージェントが悪意を持って使用される可能性がある。
 - 緩和策厳格なガードレール、アクセス制御、リアルタイムの監視。
- **信頼の問題**：ユーザがエージェントをあまり信頼しないために、エージェントの改善が妨げられたり、エージェントをあまり信頼しすぎるために、重要な判断ができなくなったりする可能性がある。
 - 緩和策意思決定における透明性と、人間による明確な説明責任。

エージェントの時代への準備

組織と個人は、急速に進歩するこのテクノロジーに備えるべきである。

1. **ユースケースを特定する**：エージェント・システムによって加速できるコア・プロセスを評価する。
2. **知識を体系化する**：エージェントのトレーニングに使用するビジネスプロセスと専門知識を文書化する。
3. **戦略的技術計画**：エージェントとの効率的なインタフェースを実現するために、データとITシステムを整理する。
4. **ヒューマン・イン・ザ・ループ・コントロールの導入**：これは、自律性とリスクのバランスをとるために不可欠である。人間がアウトプットを検証し、最終的な権限を保持しなければならない。

結論

- ・ **チャンス** : エージェント主導型オートメーションは、複雑な作業にかつてないスピードと能力をもたらし、業界に革命をもたらす。
- ・ **現実** : このテクノロジーはまだ初期段階にあり、大規模に展開する前に、かなりの開発、テスト、トレーニングが必要である。

初期の段階であっても、この新世代のバーチャルな同僚が新たなチャンスを大きく広げることは明らかだ。