perplexity

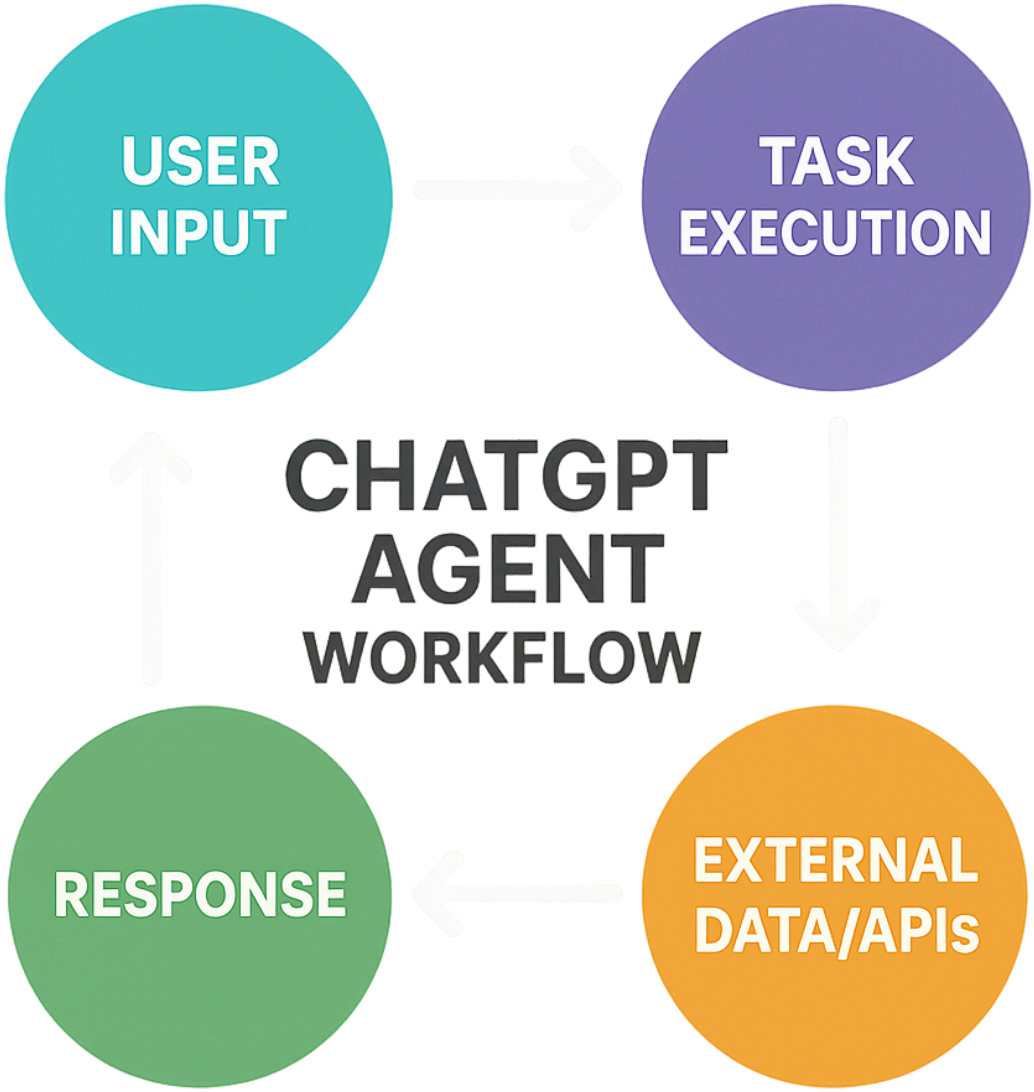
2025年7月17日リリース「ChatGPT Agent」の評判徹底調査報告

2025年7月17日に米OpenAIがリリースした「ChatGPT Agent」について、リリース直後から現在までの評判、技術的評価、ユーザー反応を包括的に調査し、その実態を明らかにした。本報告書では、技術仕様から実際のユーザー体験まで、多角的な視点からChatGPT Agentの現状と課題を分析する。

ChatGPT Agentとは

ChatGPT Agentは、従来のChatGPTに「自律的タスク実行能力」を付与した統合型AIエージェントシステムである[1] [2]。これまで個別に提供されていた「Operator」（ブラウザ操作機能）と「Deep Research」（情報分析機能）を統合し、仮想コンピューター環境で複雑なワークフローを自動実行できる[3] [4]。

ユーザーは「カレンダーを確認して最近のニュースに基づき今後のクライアント会議について説明して」「競合他社3社を分析してスライド資料を作成して」といった複雑な指示を自然言語で与えるだけで、AIが必要な情報収集から資料作成まで一貫して処理する[5] [6]。



ChatGPT Agentのワークフロー図

技術仕様と統合機能

コア技術アーキテクチャ

ChatGPT Agentは以下の技術要素を統合している[2] [7]：

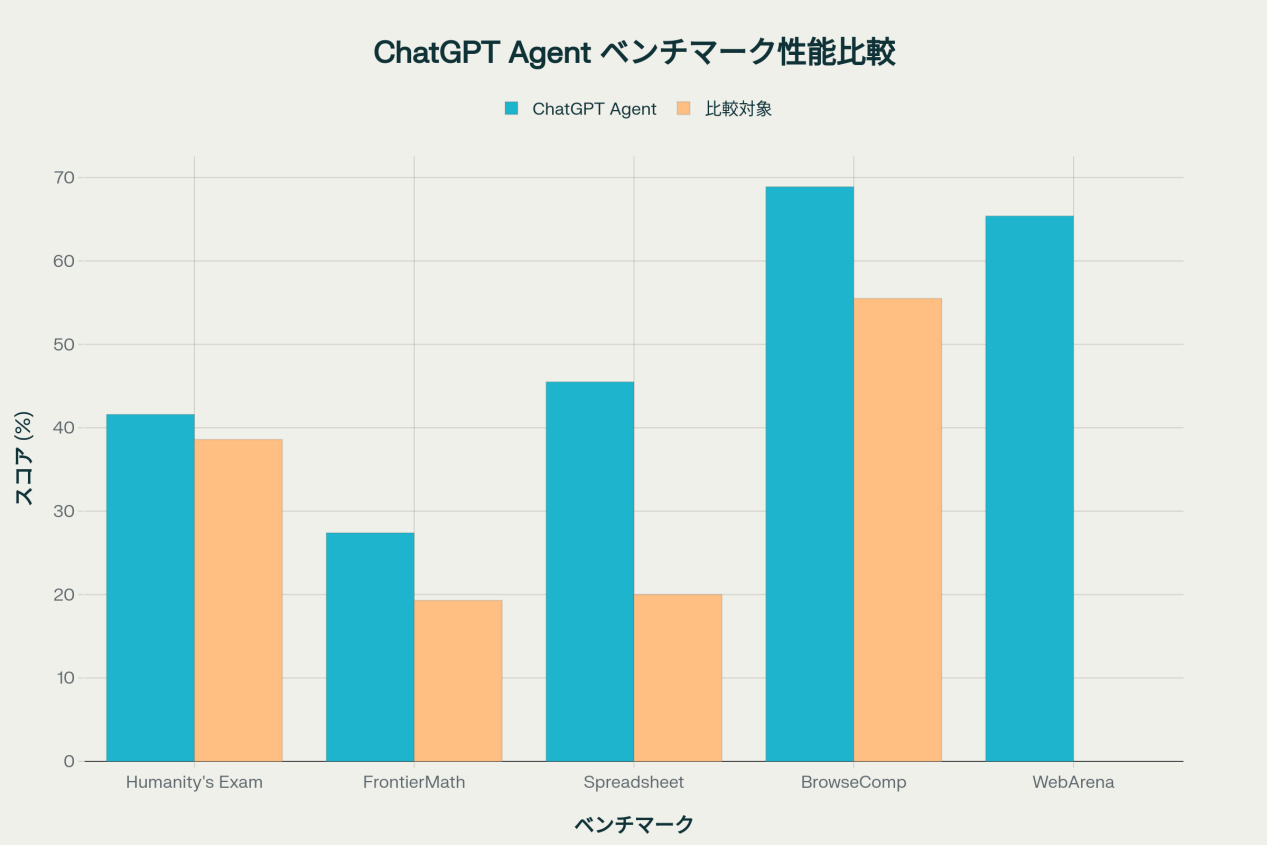
- **ビジュアルブラウザ**: グラフィカルユーザーインターフェースを通じたWeb操作
- **テキストブラウザ**: 高速な情報検索・収集のための軽量ブラウザ
- **ターミナルアクセス**: コード実行とファイル操作機能
- **API連携**: Gmail、Google Drive、GitHub等の外部サービス連携
- **強化学習モデル**: 状況に応じた最適ツール選択の自動判断

実行環境と安全対策

システムは独立したサンドボックス型仮想コンピューター環境で動作し、ユーザーのローカルファイルには直接アクセスしない[8] [7]。OpenAIは生物学・化学分野で「High capability」として分類し、最高レベルのセキュリティ対策を実装している[7] [9]。

ベンチマーク性能評価

OpenAIが公表した各種ベンチマークにおいて、ChatGPT Agentは競合システムを大幅に上回る性能を示している[2] [10]。



ChatGPT Agentの主要ベンチマークでの性能比較

特筆すべき成果として、SpreadsheetBenchでは45.5%のスコアを記録し、Microsoft Excel Copilot（20.0%）の2倍以上の性能を達成した[11] [10]。また、WebArenaにおいては実世界のWebサイト操作で65.4%の成功率を記録し、既存のAIエージェントを上回った[4] [2]。

ユーザー評価と市場反応

初期ユーザーの反応

リリース直後のユーザー評価は **「革命的だが未完成」** という評価に集約される。実際に4時間使用したユーザーは「AGIの一歩手前にいる存在」と評価しつつ、「完成度の高さ」を認める一方で実行速度や信頼性に課題があることを指摘した[12]。

専門家の評価

技術専門家からは、ChatGPT Agentが「単なる改善ではなく飛躍」として評価されている一方で、実用面での制約も指摘されている[13]。投資銀行・コンサルティング・研究といった専門職での活用可能性が認められている反面、日常業務での実用性には疑問視する声もある[13]。

主要な問題点と課題

実際の使用体験から明らかになった主要な問題点は以下の通りである。

動作速度とユーザビリティ

最も頻繁に指摘される問題は **動作速度の遅さ** である。実際のユーザーは「PC操作に慣れていないお爺さんの操作を後ろで見ているかのようなイライラ感」と表現し、クラウド上の仮想マシンの制約による処理速度の低下を指摘している[14]。

セキュリティ対策による制約

OpenAIは安全性を重視し、重要な操作前には必ずユーザーの確認を求める設計としているが、これが「頻繁な確認要求」として実用性を阻害している[14] [15]。ユーザーからは「マジ使えないシルバー人材センター」との厳しい評価も見られる[14]。

技術的制限

Googleアカウントへのログインができない制約により、Google Workspace環境での業務利用が困難となっている[14]。また、スライド生成機能は「ゴミ同然」との評価を受けており、他の専用ツール（GensparkやManus）に劣ると指摘されている[12]。

他社競合ツールとの比較

Manus AIとの性能比較

シンガポールのManus AIは公式にChatGPT Agentとの性能比較を実施し、10項目での比較結果を公表している[16]。実際の使用体験では、性能面でManusやGensparkとの大きな差は感じられないとの評価もある[12]。

従来システムとの違い

ChatGPT AgentとChatGPTの根本的な違いは、**受動的応答から能動的実行への転換** にある[17] [18]。従来のChatGPTがユーザーの質問に応答するのに対し、Agentはゴールベースでタスクを自律実行する点で大きく異なる[19]。

セキュリティリスクと対策

プロンプトインジェクション攻撃

ChatGPT Agentは **プロンプトインジェクション攻撃** という新たなセキュリティリスクに直面している[20] [9]。悪意あるWebサイトがAIに不正な指示を与え、ユーザーの機密情報を盗み出す可能性が懸念されている[20]。

OpenAIの安全対策

これらのリスクに対し、OpenAIは16人のPhD専門家による40時間のレッドチーム評価を実施し、110回の攻撃テストを通じて7つの主要脆弱性を発見・修正した[9]。その結果、視覚ブラウザでの無関係指示攻撃に対する防御率が82%から95%に向上した[9]。

利用料金とアクセス状況

料金体系

ChatGPT Agentは有料プランユーザーのみに提供され、以下の利用制限がある[21] [2]：

- **Proプラン（$200/月）**：月400メッセージ
- **Plus/Teamプラン（$20～）**：月40メッセージ
- **Enterprise/Education**: 数週間後に提供開始予定

地域制限

現在、欧州経済地域（EEA）とスイスでは利用できない状況が続いている[21] [2]。日本を含むアジア地域では段階的にロールアウトが進行中である[22]。

実用性評価と将来展望

現状の実用性

産業界への影響

AI生産性ツール市場は2024年の109.7億ドルから2034年には1,091.2億ドルへの拡大が予測されており、ChatGPT Agentはこの成長の牽引役となる可能性がある[23]。企業の顧客サービス、営業、HR領域での活用が期待されている[23]。

技術的課題と改善予定

OpenAIはスライドショー生成機能について「現在ベータ版であり、フォーマットや仕上がりが未熟」と認めており、次期バージョンでの大幅改善を約束している[2]。また、ユーザー監視の必要性を減らし、より自律的な動作を可能にする改良も計画されている[2]。

結論

ChatGPT Agentは **AIエージェント時代の幕開けを告げる画期的な製品** である一方で、**実用面では多くの課題を抱えている** というのが現在の評価である。技術的な性能面では競合を上回る結果を示しているものの、動作速度、ユーザビリティ、コストパフォーマンスの面で実用的な制約が多い。

特に月額200ドルという高額な料金設定に見合う価値提供ができているかについては、ユーザー間で意見が分かれている。ITスキルの高いユーザーにとっては「ほとんど何の役にも立たない」との厳しい評価がある一方で、非技術系ユーザーにとっては「これまでできなかったことを可能にする」ツールとしての価値が認められている。

今後の成功は、動作速度の改善、セキュリティと利便性のバランス調整、そして何より **ユーザーとAIの間の信頼関係構築** という根本的な課題の解決にかかっている。現時点では「AGI見習い」としての位置づけが適切であり、真の実用性獲得には更なる技術的進歩が必要と考えられる。

⁂

1. https://zenn.dev/schroneko/articles/introducing-chatgpt-agent
2. https://openai.com/index/introducing-chatgpt-agent/
3. https://chatgpt-lab.com/n/n3790bc17e6ba
4. https://qiita.com/softbase/items/dbe0787cb94fae717dcb
5. https://www.itmedia.co.jp/aiplus/articles/2507/18/news053.html
6. https://www.watch.impress.co.jp/docs/news/2032302.html
7. https://openai.com/index/chatgpt-agent-system-card/
8. https://techpilot.ai/chatgpt-agent-review/
9. https://venturebeat.com/security/openais-red-team-plan-make-chatgpt-agent-an-ai-fortress/
10. https://qiita.com/RepKuririn/items/752ed1566a53af25e126
11. https://aismiley.co.jp/ai_news/what-is-chatgpt-agent/
12. https://note.com/holy_fox/n/n63099b68b3ce
13. https://note.com/dalhi/n/n4a5798ef1162
14. https://note.com/shi3zblog/n/n2d4abbb0123c
15. https://wirelesswire.jp/2025/07/88936/
16. https://www.itmedia.co.jp/aiplus/articles/2507/18/news096.html
17. https://bizfreak.co.jp/blog/50nb591bccd
18. https://www.linkedin.com/pulse/from-chatgpt-enterprise-ai-agents-understanding-shift-raj-8gsmc
19. https://hypermode.com/blog/chatgpt-vs-ai-agents
20. https://www.techradar.com/computing/artificial-intelligence/chatgpt-agent-shows-that-theres-a-whole-new-world-of-ai-security-threats-on-the-way-we-need-to-worry-about
21. https://help.openai.com/en/articles/11794368-chatgpt-agent-release-notes
22. https://skift.com/2025/07/18/openai-launches-chatgpt-agent-mode-what-it-could-mean-for-the-travel-industry/

23. https://www.ainvest.com/news/rise-ai-driven-productivity-openai-chatgpt-agent-reshaping-enterprise-software-2507/