

# OpenClawとManusの違いに関する多面的比較・分析 報告書

## エグゼクティブサマリー

本報告書は、比較対象を「OpenClaw」と「Manus」と明示した上で、両者を“自律型AIエージェント (task-executing agent)”として比較する。調査の同定結果として、OpenClawは「自分のデバイス上で動かす個人用AIアシスタント／オープンソース基盤」、Manusは「クラウド上の“仮想コンピュータ (サンドボックス)”を中核にした汎用AIエージェント (SaaS) +API+デスクトップ拡張」と整理できる。<sup>1</sup>

最も本質的な差分は**信頼境界 (trust boundary) と運用モデル**である。OpenClawは「あなたのマシン／あなたの鍵／あなたのデータ」を強く前提にし、メッセージングアプリ等の既存チャンネルで操作できる一方、強力なツール実行 (シェル実行・ファイル操作・Web取得・自動タスク等) ゆえに設定不備や拡張機構 (Skills/プラグイン) を通じた攻撃面が拡大しやすい。<sup>2</sup>

Manusは、クラウド上の隔離環境 (VM) でタスクを遂行し、OAuthコネクタやAPIにより業務ツールへ接続しやすい。さらに2026年3月の「My Computer」でローカルPCへ拡張しつつ、端末側のコマンド実行は明示承認を必須にする設計を打ち出している。<sup>3</sup>

性能・運用品質について、Manusは公式に「過去3か月で速度2倍・コスト5分の1」を主張し、長時間タスクを前提にした**状態管理 (非同期タスク、ステータス、Webhook、ファイル管理)**をAPIとして提供している。<sup>4</sup>

一方で、初期段階のManusは「サーバ過負荷やクラッシュ」等の不安定さも指摘されており、“便利さ (SaaS)”と“安定性・透明性”は運用上のトレードオフになり得る。<sup>5</sup>

導入コストの観点では、OpenClawはGitHub<sup>6</sup>上でMITライセンスのオープンソースとして配布され、ソフトウェア自体のライセンス費用は原則ゼロだが、(a) 常時稼働基盤、(b) LLM/外部API利用料、(c) セキュリティ運用 (監査・隔離・更新) を自前で負担するTCO構造になりやすい。<sup>7</sup>

Manusはクレジット制 (プラン・クレジット・並列タスク制限) を通じてコストをSaaS側に“パッケージ化”する設計で、価格体系は時期によって記述が揺れている (後述) が、少なくともクレジット制・月次リセット・アドオン等の概念は公式ドキュメントで説明されている。<sup>8</sup>

結論として、**機密データ／権限の強い自動化を“自分の統制下”で回したい個人・開発者・小規模運用**はOpenClawが適合しやすいが、セキュリティ成熟度 (設定・監査・拡張管理) が成果とリスクを決定づける。<sup>9</sup>

**チーム協働 (Slack等) や業務SaaS連携、API統合、クラウド実行の利便性**を重視する場合はManusが適合しやすいが、クラウド上の処理・データ取り扱い・運営主体 (Meta傘下化) に関するガバナンス適合性を別途評価する必要がある。<sup>10</sup>

## 調査対象の同定と方法

「OpenClaw」と「Manus」は一般名詞としても成立し得るが、本件の必須比較軸 (OS/SDK/API/エコシステム、導入コスト、運用事例、ロードマップ等) と、公式サイト・ドキュメントの存在から、**OpenClaw=openclaw.ai/openclaw/openclaw (自己ホスト型AIエージェント基盤)**、**Manus=manus.im/open.manus.im (クラウドAIエージェントSaaS)**を主対象として確定した。<sup>11</sup>

なお「Manus」にはVRグローブ等の別製品群が存在し得るが、本報告書は上記のAIエージェント群に限定する（他の“Manus”は比較対象外として未分析）。<sup>12</sup>

方法は、(1) 公式サイト／公式ドキュメント／公式ブログ／公式GitHubを一次情報とし、(2) 主要技術メディア・セキュリティベンダー・学術論文で補強し、(3) 日本語ユーザー記事・実運用記事を実装面の補助証拠として扱った。<sup>13</sup>

調査時点は日本時間2026年3月31日であり、急速に変化する領域（価格・機能・セキュリティ状況）は“日付きスナップショット”として扱い、未特定点は明示する。<sup>14</sup>

## 製品概要とアーキテクチャ

OpenClawは「自分のデバイスで動かす個人用AIアシスタント」で、既存のチャンネル（例：WhatsApp/Telegram/Slack/Discord等）で応答させる構成を前面に出し、Gatewayは“制御プレーン（control plane）”であり本体はアシスタントであると説明する。<sup>15</sup>

また、OpenClawは“行動する”能力（シェル実行、ファイル読み書き、任意URL取得、自動タスク、外部サービス/APIアクセス）を持つこと自体を価値と同時にリスク源泉として明示している。<sup>16</sup>

Manusは公式ドキュメントで「自律的にタスクを完遂し成果物を返す general AI agent」と位置づけ、クラウド上に“仮想コンピュータ（インターネット、永続ファイルシステム、ソフト導入、ツール作成能力を持つサンドボックス環境）”を持つ点を差別化としている。<sup>17</sup>

2026年3月にはデスクトップアプリの中核機能「My Computer」を導入し、従来クラウド内に閉じていた実行環境をローカル端末へ拡張し、端末上ではCLI実行を通じてローカルファイル／アプリへアクセス可能にしたと説明している。<sup>18</sup>

両者を“実行基盤”として抽象化すると、OpenClawは「ユーザー所有の実ホスト上でのエージェント運用」を基本とし、Manusは「クラウド隔離VM+（必要に応じて）ローカル端末拡張」を基本とする。この差分は、後述の安全設計・法的リスク・TCO・運用統制の全てに波及する。<sup>19</sup>

```
flowchart LR
  subgraph User["ユーザー"]
    UI["指示（自然言語）"]
  end

  subgraph OpenClawSys["OpenClaw（自己ホスト）"]
    OCChan["チャンネル（WhatsApp/Telegram/Slack等）"]
    OCGW["Gateway（制御プレーン）"]
    OCAgent["Agent Runtime"]
    OCTools["ツール：shell / fs / web / cron / 連携API"]
    OCSkills["Skills/Plugins（ClawHub等）"]
  end

  subgraph ManusSys["Manus（クラウド主体）"]
    MWeb["Web/モバイル/Slack等UI"]
    MCloudVM["クラウド隔離VM（ブラウザ/CLI/FS）"]
    MConn["Connectors（OAuth）"]
    MAPI["REST API / Webhooks"]
    MDesktop["Desktop: My Computer（ローカルCLI承認）"]
  end
```

```
U1 --> OCChan --> OCGW --> OCAgent --> OCTools
OCAgent --> OCSkills
U1 --> MWeb --> MCloudVM --> MConn
MCloudVM --> MAPI
MWeb --> MDesktop
```

(上図は公式記述を基にした概念図であり、内部実装の完全な同一性は未特定。) 20

## 機能・性能の比較

### ロボティクス用語（センサー／アクチュエータ等）の読み替え

ユーザー指定の比較軸にはロボティクス由来の項目（センサー、アクチュエータ、自由度、把持力）が含まれるため、本報告書ではAIエージェント領域へ以下のように写像して評価する（物理ハードの意味でのセンサー／把持力は両者とも原則“非該当”）。 21

- ・センサー：入力チャンネル／取り込み可能データ（メッセージ、ファイル、Web、コネクタ経由データ等）
- ・アクチュエータ：実行手段（ブラウザ操作、CLI、ファイル操作、メッセージ送信、API呼び出し等）
- ・自由度：行動空間の広さ（利用可能ツール群・拡張性・統合範囲）
- ・把持力：実行権限の強さ（“どこまで触れるか”と不可逆操作の可能性＝blast radius）
- ・精度：成果物の正確性・再現性（引用、推論、実行の失敗率等）
- ・応答性：待ち時間・進捗可視化・非同期性

### 入力（センサー相当）と実行（アクチュエータ相当）

OpenClawは、多数のメッセージングチャンネルを“既存UIとして流用”する方向性が強く、GitHubのREADMEだけでもWhatsApp/Telegram/Slack/Discord/Signal/iMessage/Teams/LINE等を含む広範なチャンネル列挙がある。 22

一方で“実行”はユーザーが与えるツール権限に依存し、シェル実行やファイル操作、任意URL取得、自動ジョブなど強い操作が可能であること自体が公式に明示されている。 23

ManusはクラウドVM内で「ブラウザ・CLI・ファイルシステム・ソフト導入」を前提にし、結果として“入力→計画→実行→成果物”の一連をSaaS側で完結させやすい。 24

さらにConnectorsとしてGmail/Notion/Google Calendar等をOAuthで接続し、アプリ側データへアクセス可能と説明している。 25

### 自由度（統合範囲）と拡張性

OpenClawはSkills/Pluginsを通じて拡張し、ClawHubをスキルのマーケット／レジストリとして扱う。 26  
ただし、拡張コードは「エージェントのコンテキストで実行され、ツールとデータにアクセスし得る」ため、供給網（supply chain）リスクが高いことも公式が前提としている。 27

Manusも拡張の方向性を強めており、Anthropic 28 が提唱するオープン標準“Agent Skills”を「完全統合する」と表明し、Skillがファイルシステム資源としてワークフローやスクリプトをパッケージ化できる点、またManusの隔離VM（Ubuntu FS+shell実行）と相性が良い点を述べる。 29

したがって“自由度”はManusも十分に広く、今後は「SaaS+標準化されたスキル資産+コネクタ」が拡張の中核になると推測できる（ただし互換範囲・公開レジストリの成熟度は未特定）。 30

## 把持力（権限の強さ）と応答性・安定性

把持力の観点では、OpenClawはホスト上のshell実行・ファイル操作などを行えるため、設定次第で“実行権限”が非常に強くなり得る。<sup>16</sup>

実際に、スキル経由のマルウェア混入が報告され、暗号資産関連を装うスキルが秘密情報（ウォレット鍵、SSH資格情報、ブラウザパスワード等）を狙う事例が指摘された。<sup>31</sup>

Manusは「全タスクが隔離されたクラウドVM内で処理される」とヘルプセンターで説明し、メッセージング連携（Telegram/WhatsApp Business）でもアクセス範囲を“当該プライベートチャット内のDMに限定、他会話・グループ・連絡先・過去メッセージにアクセス不可”と明記している。<sup>32</sup>

さらにMy Computerではローカル端末のCLI実行が可能になる一方、「すべてのターミナルコマンドは実行前に明示承認が必要」と述べ、把持力を“承認ゲート”で制御する設計思想を示している。<sup>18</sup>

応答性について、Manusは長時間タスクを前提に「非同期タスク（running/pending/completed/error）」として管理し、WebhookもRSA-SHA256署名検証で保護する設計を公開している。<sup>33</sup>

他方で、初期の実地テストではサーバ過負荷・クラッシュが言及されており、SaaS基盤のキャパシティが体験を左右し得る。<sup>5</sup>

## 互換性・エコシステムと導入運用

### OS・SDK・API・サードパーティ対応

OpenClawは「Any OS. Any Platform」を掲げ、ユーザーのチャンネル群へ統合する思想が強い。<sup>34</sup>

一方で“公式に整備されたSDK/API”の位置づけは、少なくとも公開ドキュメント上ではGateway/CLI/ツール・プラグイン管理が中心であり、SaaS的な外部開発者向けAPI提供（Manus APIのような形）は比較上は弱い（もしくは未特定）と整理するのが妥当である。<sup>35</sup>

Manusは明示的に「Manus API（REST）」を掲げ、アプリからタスク起動・ファイル管理・結果受領をプログラマ的行えたと説明し、さらに“OpenAI SDK互換（Responses API互換）”として利用可能である旨をドキュメントに記載している。<sup>36</sup>

ConnectorsはOAuthで設定し、Gmail/Notion/Google Calendar等の例とともに“アプリへ直接アクセス・制御する”用途が説明されている。<sup>25</sup>

### セットアップ・学習曲線・ドキュメント

OpenClawはワンライナー導入（install.sh）を提示しつつ、セキュリティ監査・設定・プラグイン／スキル管理まで含めると学習曲線は相応に高い。<sup>37</sup>

実運用者の日本語記事でも、常駐マシン（例：Mac mini）での構築や、`openclaw security audit --deep`を含むセキュリティ強化が継続課題として語られている。<sup>38</sup>

ManusはSlack連携において「Slackを離れずに@manusをタグ付けし、スレッド全体のコンテキストを読み取らせて共同作業する」体験を日本語ドキュメントで詳細に説明し、導入手順も“接続→承認→利用”の流れで相対的に軽い。<sup>39</sup>

ただしMy Computerのようにローカル端末へ踏み込む機能は、承認モデルがあるとはいえ、社内ITポリシー／端末管理（EDR等）と整合させる追加検討が必要になる（具体的要件は未特定）。<sup>18</sup>

### 導入コストとTCO

OpenClawの直接費用は「オープンソース（MIT）」である点からソフトウェアライセンスは基本的に無料だが、(1) 常時稼働基盤（自宅/社内/クラウド）、(2) LLM/APIキー運用、(3) セキュリティ監査・隔離、(4) 更新

対応がTCOの中心になる。<sup>40</sup>

国家機関レベルでも、設定不備がサイバー攻撃・データ侵害につながり得るとして「公開ネットワーク露出の監査、認証・アクセス制御の強化」を促す注意喚起が報じられている。<sup>41</sup>

Manusはクレジット制で、タスクの複雑さに応じて消費され、月次更新・アドオン購入等を用意する、と公式ドキュメントで説明している。<sup>42</sup>

ただし、**具体的な料金表は公式pricingページが動的で本調査環境では機械可読に取得できず**、公式ブログ等に掲載された「時点別スナップショット」で整理する必要がある（＝現行プランの確定は未特定）。<sup>43</sup>

以下に、公式ドメイン上の記述から取得できた代表例を“時点付き”で列挙する。

- 2025年11月（公式ブログ内比較表の例）：Free（300 daily credits/1 task）、Basic \$19/1,900 credits、Plus \$39/3,900 credits、Pro \$199/19,900 credits。<sup>44</sup>
- 2026年3月（公式ブログ内の別記事の例）：\$20/月で4,000 credits、\$40/月で8,000 credits、\$200/月で40,000 credits等の記述。<sup>45</sup>
- 2025年3月（主要メディア報道の例）：Starter \$39（3,900 credits・同時2タスク）、Pro \$199（同時5タスク）といった説明。<sup>46</sup>

この“揺れ”は、(a) プラン改定、(b) 製品文脈（一般エージェント vs 特定機能のパッケージ）の差、(c) 地域/提供形態の差、のいずれか（または複合）が原因と考えられるが、公式pricingページの静的取得ができないため確定はできない。<sup>43</sup>

## 料金・クレジットの“性能差”チャート

下図は「2025年11月時点の公式ブログ記述（Basic/Plus/Pro）」に基づく、月額と付与クレジットの対応を可視化したものである（現行プランである保証はない）。<sup>44</sup>

```
xychart-beta
title "Manus 価格スナップショット（2025-11記事）：月額とクレジット"
x-axis ["Basic", "Plus", "Pro"]
y-axis "USD / credits" 0 --> 20000
bar "月額USD" [19,39,199]
bar "月次credits" [1900,3900,19900]
```

また、2026年3月の公式ブログ記述（\$20/4,000 credits等）が正式改定を反映している場合、1,000 creditsあたりの単価が概ね半減（\$10→\$5）する計算になるが、これは推測であり、現行体系は未特定である。<sup>47</sup>

## 安全性・法規制・倫理とリスク

### OpenClawの安全機構・設計思想

OpenClawは“パーソナルアシスタント（単一の信頼オペレータ境界）”を前提にし、敵対的マルチテナント境界としては設計していない、と明示する。<sup>48</sup>

安全機構として、DMのpairing、execのdeny（許可リスト外は拒否）、Gateway認証、SSRF保護、セッション分離等を“デフォルトで”持つと説明している。<sup>49</sup>

運用面では `openclaw security audit`（`--deep/--fix/--json`含む）を提供し、`--fix` は安全で決定的な修正（例：openなgroupPolicyをallowlistに、ログのセンシティブ情報のredact強化、権限制限）を行う一方で、トークン回転や危険ツール自体の無効化までは自動では行わない、と公式CLIドキュメントに明記されてい

る。 50

またGatewayセキュリティガイドは「完全に安全な設定はない」「最小権限から始める」等、踏み込んだ警告を含む。 51

供給連鎖対策として、OpenClawはVirusTotal 52 と提携し、ClawHubへ公開されるSkillsをハッシュ照合+Code Insight解析（疑わしい場合の警告、悪性のブロック、日次再スキャン等）でスキャンする仕組みを公開したが、同時に「銀の弾丸ではない」ことも明記している。 53

## Manusの安全機構・データプライバシー

Manusは、メッセージング連携（Telegram/WhatsApp Business）に関して、アクセス範囲（特定DMのみ、グループ不可、連絡先不可、接続前メッセージ不可）をヘルプセンターで明確化し、タスク処理は隔離されたクラウドVMで行うと説明する。 32

Team Planでは“タスク可視性（誰が何を見られるか）”を役割に応じて規定し、個人プランはデフォルト非公開、チームはオーナーがセッションデータへアクセスし得る等の運用ルールを示している。 54

アカウント削除後のデータ取り扱いについても、削除措置を講じつつ、法務・会計・不正防止等で一定期間保持があり得ると説明している（保持期間の具体値は未特定）。 55

My Computerでは、ローカル端末に対して「すべてのターミナルコマンドは実行前に明示承認」が必要で、ユーザーが指揮官であるという設計思想を明言する。 18

API面ではWebhookの署名検証（RSA-SHA256/2048-bit鍵）を推奨し、なりすまし対策を設計として提示している。 56

## 法規制・倫理・ガバナンス

Manusはサイト上で「Metaの一部になった」と明示し、買収に関してはAssociated Press 57 が“MetaがManusを買収し、Meta AIなどへ統合を進める意向”を報じている。 58

一方で、出自や地政学的リスクを背景に「中国当局による審査」等が報じられており、規制・越境データ・投資審査の文脈で運用リスクが顕在化し得る（詳細はケース依存で未特定）。 59

OpenClawも、国家機関が設定不備によるリスクを警告し、公開露出や認証・アクセス制御の監査を促したと報じられている。 41

このため、両者とも“倫理”を抽象的に論じるより、具体的な権限設計・監査・責任分界・データ保持として落とし込む必要がある。 60

## リスク整理表

リスク類型	OpenClaw（主要リスク）	Manus（主要リスク）	低減策の方向性（共通/差分）
技術的	Skills/プラグイン供給網、設定不備で権限が過大化、秘密情報露出（実例として悪性スキル混入・キー窃取が指摘） 61	クラウド実行のブラックボックス性、初期の不安定さ（過負荷/クラッシュ）、ローカル拡張（My Computer）導入後の端末面リスク 62	最小権限・隔離（VM/別ホスト）・秘密管理・監査ログ・拡張の検証。 OpenClawは security audit の常用が中核。 63

リ ス ク 類 型	OpenClaw（主要リスク）	Manus（主要リスク）	低減策の方向性（共通/差分）
運 用 的	自前運用ゆえパッチ適用・監視・バックアップが自己責任。共有チャネル運用は信頼境界の崩壊に注意（公式も非推奨） <sup>48</sup>	SaaS依存（障害・価格改定・仕様変更）。チーム運用ではタスク可視性とデータ保持のガバナンスが必要 <sup>64</sup>	変更管理（リリースノート/更新頻度）、権限制御、チームポリシー整備。
法 的	公開露出・データ侵害時の責任分界（ユーザー側運用責任が大きい）。当局が設定不備リスクを警告 <sup>65</sup>	買収・規制審査・越境データの影響（組織要件次第で重大） <sup>66</sup>	監査証拠、データ保持・削除、第三者提供/越境の確認（詳細は各社ポリシーと契約で要確認＝未特定）。
供 給 連 鎖	Skills/Pluginsが直接実行コンテキストに入る。VirusTotalスキャン等の対策はあるが万能ではない <sup>67</sup>	Skills統合が進むとスクリプト資産の供給網リスクが増える可能性（VM内実行で隔離はあるが、出力や連携が攻撃面になり得る） <sup>68</sup>	レジストリ/配布経路の信頼、署名・審査プロセス、実行権限の縛り、監査（未特定機能は評価保留）。

## 実運用事例・ユースケースと将来性

Manusの公式ブログは、研究（deep research）やWebサイト構築、スライド生成、画像/動画生成、データ可視化などのユースケースを列挙し、次のロードマップとしてScheduled Tasks、Wide Research、Omni Search、各種アプリ統合（メール/カレンダー/ドライブ/タスク管理等）を挙げている。<sup>69</sup>

また、Skills統合についても「Project/Connector統合→Team Skill Library」と段階的ロードマップを提示している。<sup>29</sup>

My Computerの実例としては、写真の自動整理・請求書リネーム・SwiftによるMacアプリ作成などが挙げられ、さらに「端末がONでDesktopが動いていれば、外出先から指示して自宅PCで処理できる」構想を示す。<sup>70</sup>

チーム運用ではSlack連携が“会話の中のAI”として位置づけられ、スレッドの共有コンテキスト／共同作業／承認の流れまで具体的に書かれている。<sup>39</sup>

OpenClawは「受信箱整理、メール送信、カレンダー管理、フライトのチェックイン」等の“実務自動化”を前面に出し、コミュニティ規模も非常に大きい（GitHub上のスター数・リリース頻度が高い）。<sup>71</sup>

ただし、悪性スキル混入など“エージェント拡張の攻撃面”が現実の問題化しており、セキュリティ対策（VirusTotalスキャン、監査コマンド、セキュリティプログラム整備）を加速させている。<sup>72</sup>

研究面でも、OpenClaw向けに「ツール実行型エージェントのランタイム防御（PRISM）」を提案し、間接プロンプト注入・ツール濫用・秘密漏えい等に対して“ライフサイクル全域のフックで防御・監査する”という学術的枠組みが提示されている。<sup>73</sup>

## 主要バージョン・出来事タイムライン（確度つき）

以下は一次情報（公式ブログ/公式Docs/GitHub/主要報道）から時系列に“確実に言える範囲”をまとめた。なお、OpenClawの名称遷移やManusの買収等は外部報道も含むため、詳細は出典に依存する。<sup>74</sup>

timeline

title OpenClaw / Manus 主な節目 (2025-03~2026-03)

2025-03-06 : Manus 公開 (プレビュー期) とされる

2025-06-26 : Manus 速度2倍・コスト5分の1等の改善/ロードマップ言及

2025-11-13 : Manus 料金スナップショット (Basic/Plus/Pro等) の例

2025-11 : OpenClaw 起点 (“11月に登場”と報道/言及)

2026-01-27 : Manus Skills統合ロードマップを公表

2026-01-29 : OpenClaw “Road Ahead”でSecurity最優先等を記述

2026-02-07 : OpenClaw×VirusTotal (ClawHubスキャン) 発表

2026-02-05 : 中国当局がOpenClawの設定不備リスクを警告 (報道)

2026-03-16 : Manus Desktop “My Computer”発表 (macOS/Windows)

2026-03-29 : OpenClaw GitHub 最新リリース日 (2026.3.28)

(個別日付の厳密性：Manusの公開日やOpenClawの“11月登場”は報道・外部まとめに依存するため、法務用途では追加確認が必要。) <sup>75</sup>

## 機能比較表と用途別結論

### 機能比較表

以下はユーザー指定の比較軸を網羅するため、ロボティクス用語は“AIエージェントの入出力/権限”へ読み替えて記載する (物理センサー・把持力は原則非該当)。<sup>21</sup>

比較軸	OpenClaw	Manus
製品形態	自己ホスト型 (ユーザーのデバイス上で実行) <sup>15</sup>	SaaS (クラウド隔離VM) + Desktop拡張 (My Computer) <sup>76</sup>
センサー (入力)	多数のメッセージングチャンネル (WhatsApp/Telegram/Slack/Discord等) + 音声入出力 (macOS/iOS/Android言及) <sup>22</sup>	Web/モバイル/Slack等 + コネクタ経由データ (Gmail/Notion/Google Calendar等) <sup>77</sup>
アクチュエータ (実行)	ホスト上のshell、workspaceのファイルR/W、任意URL取得、自動タスク、外部サービス/APIアクセス等 (公式が能力として明示) <sup>23</sup>	クラウドVMのブラウザ/CLI/FS/ソフト導入 + API (タスク/ファイル) + コネクタ操作。DesktopではローカルCLI (承認必須) <sup>78</sup>
自由度 (拡張性)	Skills/Plugins、ClawHub等 (供給網リスクも大) <sup>27</sup>	Skills (Agent Skills標準) 統合を表明し、Project/Connector統合→Team Skill Libraryをロードマップ化 <sup>30</sup>
把持力 (権限の強さ)	設定次第でホストへの広範な操作権限 = blast radius大。悪性スキル混入事例で顕在化 <sup>79</sup>	原則クラウドVM内に隔離、メッセージング連携のアクセス範囲を限定。ローカル端末はコマンド承認ゲート <sup>80</sup>
精度 (成果物)	利用モデル (外部LLM) ・ツール設定に依存し変動 (公式ベンチマーク値は未特定) <sup>81</sup>	実地テストで“有能なインターン”の比喩、ただし誤推測や手抜き、クラッシュも報告 <sup>5</sup>

比較軸	OpenClaw	Manus
応答性 (待ち/ 進捗)	ローカル環境性能+外部LLM遅延に依存。自動ジョブ (cron) 等で継続実行可能だが危険ツールとして管理される <sup>82</sup>	非同期タスク (status) + Webhook設計。過去3か月で速度2倍・コスト5分の1を主張 <sup>83</sup>
互換性・ エコシス テム	“Any OS/Any Platform”主張、チャンネル数が強み。API/SDKの外部公開度は相対的に未特定 <sup>34</sup>	REST API、OpenAI SDK互換、OAuthコネクタ、Slack統合。DesktopはmacOS/Windows提供 <sup>84</sup>
導入コス ト・TCO	ソフトはオープンソース (MIT) だが基盤/LLM費/運用 (監査・隔離・更新) がTCOの主要因 <sup>40</sup>	クレジット課金+プラン (月次更新/アドオン)。具体料金は時点により揺れ、現行は未特定 <sup>8</sup>
ユーザビ リティ	チャンネル統合は自然だが、セキュリティと運用の学習が不可欠 <sup>48</sup>	Slack等での“会話内AI”は導入が軽い。ローカル拡張は承認モデル付きだが統制要検討 <sup>85</sup>
安全性・ 認証	pairing/allowlist、Gateway認証、security audit、VirusTotalスキャン等 (ただし万能でない) <sup>86</sup>	VM隔離、アクセス範囲制限、Webhook署名、My Computerの承認制。公式Privacy本文は本環境で未取得だがヘルプが補完 <sup>87</sup>
信頼性・ 耐久性・ メンテ	高頻度リリース (GitHubで多数リリース)。ただし運用責任がユーザー側に寄る <sup>88</sup>	SaaS側で運用されるが、初期に過負荷/クラッシュ報告。機能拡張が速い (My Computer等) <sup>89</sup>
サポー ト・コ ミュニ ティ	OSSコミュニティ (GitHub/Discord) 規模が大きい <sup>90</sup>	Help Center/Docs/Academy等が整備。買収後はMeta方針の影響も考慮 (将来性は未特定要素あり) <sup>91</sup>

## 用途別推奨を含む結論表

代表用途	推奨	根拠 (要点)	注意点 (失敗モード)
個人の機密データ (ローカルファイル/端 末) に踏み込む自動化 を“自己統制”で実施	OpenClaw	ローカル実行で権限・ 鍵・データを自分で管理 する思想。ツール実行 (shell/fs/web/cron) を 前提にできる <sup>92</sup>	権限が強いほど事故・侵害の 被害が大。悪性スキル等の事 例あり。最小権限・隔離・監 査が必須 <sup>93</sup>
Slack中心のチーム協働 (スレッド文脈を共有 し共同で成果物を作 る)	Manus	Slack統合が“会話の中の AI”として詳細設計され、 共同作業や承認フローま で説明がある <sup>39</sup>	Team運用では“誰がタスクを 見られるか”を理解し、情報 区分に合わせた運用が必要 <sup>54</sup>
SaaS連携 (Gmail/ Notion/Calendar等) を 前提に、APIで業務シス テムへ組み込みたい	Manus	OAuthコネクタ+REST API+OpenAI SDK互換で 統合が明示されている <sup>94</sup>	料金体系の変動可能性、デー タ保持・削除・越境等の契約 確認が必要 (本環境で Privacy本文未取得) <sup>95</sup>

代表用途	推奨	根拠 (要点)	注意点 (失敗モード)
長時間の調査・分析・成果物生成をバックグラウンドで回したい (非同期・Webhook)	Manus	非同期タスク状態とWebhook署名検証をドキュメント化。性能改善 (速度2倍等) も主張 <sup>83</sup>	初期には過負荷/クラッシュ報告。SaaS稼働状況に依存 <sup>5</sup>
エージェント拡張 (スキル/プラグイン) を使い込みたい開発者	同等 (目的依存)	OpenClawはClawHub/Plugins、ManusはAgent Skills統合とロードマップを提示 <sup>96</sup>	両者とも供給連鎖リスク。OpenClawは悪性スキル事例が顕在化、Manusもスクリプト資産共有が進むと同種リスク増の可能性 <sup>97</sup>
規制・ガバナンス (組織統制、地政学リスク) を強く意識する導入	追加調査が必須 (未特定)	ManusはMeta傘下化・規制審査等の報道があり、OpenClawは設定不備リスクの当局警告が報じられる <sup>98</sup>	どちらも“統制設計次第”。法務/セキュリティ要件 (監査、保持、越境、責任分界) を契約・構成で詰める必要

(補足) “どちらが上か”ではなく、「どこに信頼境界を置くか」「誰が運用責任を負うか」「拡張をどう統制するか」で優劣が反転するタイプの比較である。 <sup>99</sup>

<sup>1</sup> <sup>7</sup> <sup>13</sup> <sup>14</sup> <sup>15</sup> <sup>20</sup> <sup>22</sup> <sup>34</sup> <sup>40</sup> <sup>74</sup> <sup>81</sup> <sup>88</sup> <sup>90</sup> <https://github.com/openclaw/openclaw>  
<https://github.com/openclaw/openclaw>

<sup>2</sup> <sup>9</sup> <sup>11</sup> <sup>19</sup> <sup>92</sup> <https://openclaw.ai/blog/introducing-openclaw>  
<https://openclaw.ai/blog/introducing-openclaw>

<sup>3</sup> <sup>17</sup> <sup>24</sup> <sup>76</sup> <sup>78</sup> <https://manus.im/docs/introduction/welcome>  
<https://manus.im/docs/introduction/welcome>

<sup>4</sup> <sup>69</sup> <https://manus.im/blog/what-we-saw-in-the-past-three-months-and-what-we-see-in-the-future>  
<https://manus.im/blog/what-we-saw-in-the-past-three-months-and-what-we-see-in-the-future>

<sup>5</sup> <sup>62</sup> <sup>89</sup> <https://www.technologyreview.jp/s/357540/everyone-in-ai-is-talking-about-manus-we-put-it-to-the-test/>  
<https://www.technologyreview.jp/s/357540/everyone-in-ai-is-talking-about-manus-we-put-it-to-the-test/>

<sup>6</sup> <sup>54</sup> <sup>64</sup>

- 18 70 <https://manus.im/blog/manus-my-computer-desktop>  
<https://manus.im/blog/manus-my-computer-desktop>
- 25 94 <https://open.manus.im/docs/connectors>  
<https://open.manus.im/docs/connectors>
- 26 27 28 37 53 67 96 <https://openclaw.ai/blog/virustotal-partnership>  
<https://openclaw.ai/blog/virustotal-partnership>
- 29 30 52 68 <https://manus.im/blog/manus-skills>  
<https://manus.im/blog/manus-skills>
- 31 61 72 79 93 97 <https://www.theverge.com/news/874011/openclaw-ai-skill-clawhub-extensions-security-nightmare>  
<https://www.theverge.com/news/874011/openclaw-ai-skill-clawhub-extensions-security-nightmare>
- 32 80 87 <https://help.manus.im/ja/articles/14033996-telegram%E3%81%A7manus-agent%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E9%9A%9B-%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AF%E5%AE%89%E5%85%A8%E3%81%A7%E3%81%99%E3%81%8B>  
<https://help.manus.im/ja/articles/14033996-telegram%E3%81%A7manus-agent%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E9%9A%9B-%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AF%E5%AE%89%E5%85%A8%E3%81%A7%E3%81%99%E3%81%8B>
- 33 83 <https://open.manus.im/docs/openai-compatibility>  
<https://open.manus.im/docs/openai-compatibility>
- 35 50 63 <https://docs.openclaw.ai/cli/security>  
<https://docs.openclaw.ai/cli/security>
- 36 84 <https://manus.im/docs/integrations/manus-api>  
<https://manus.im/docs/integrations/manus-api>
- 38 <https://dev.classmethod.jp/articles/openclaw-closed-loop/>  
<https://dev.classmethod.jp/articles/openclaw-closed-loop/>
- 41 65 <https://www.reuters.com/world/china/china-warns-security-risks-linked-openclaw-open-source-ai-agent-2026-02-05/>  
<https://www.reuters.com/world/china/china-warns-security-risks-linked-openclaw-open-source-ai-agent-2026-02-05/>
- 43 <https://manus.im/ja/pricing>  
<https://manus.im/ja/pricing>
- 44 <https://manus.im/blog/vs-gamma>  
<https://manus.im/blog/vs-gamma>
- 45 47 <https://manus.im/blog/best-ai-app-builders>  
<https://manus.im/blog/best-ai-app-builders>
- 46 <https://m.economictimes.com/tech/artificial-intelligence/manus-ai-launches-monthly-subscription-plans-mobile-app-for-ios-users/articleshow/119813404.cms>  
<https://m.economictimes.com/tech/artificial-intelligence/manus-ai-launches-monthly-subscription-plans-mobile-app-for-ios-users/articleshow/119813404.cms>
- 48 51 60 82 86 99 <https://docs.openclaw.ai/security>  
<https://docs.openclaw.ai/security>

55 <https://help.manus.im/ja/articles/11711823-%E3%82%A2%E3%82%AB%E3%82%A6%E3%83%B3%E3%83%88%E3%82%92%E5%89%8A%E9%99%A4%E3%81%97%E3%81%95%E5%80%8B%E4%BA%BA%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AF%E5%89%8A%E9%99%A4%E3%81%95%E3%82%8C%E3%81%BE>

56 <https://open.manus.im/docs/webhooks/security>  
<https://open.manus.im/docs/webhooks/security>

57 91 <https://help.manus.im/ja/collections/13762620-%E3%83%97%E3%83%A9%E3%82%A4%E3%83%90%E3%82%B7%E3%83%BC%E3%81%A8%E3%83%9D%E3%83%AA%E3%82%B7%E3%83%BC>

59 75 [https://en.wikipedia.org/wiki/Manus\\_%28AI\\_agent%29](https://en.wikipedia.org/wiki/Manus_%28AI_agent%29)  
[https://en.wikipedia.org/wiki/Manus\\_%28AI\\_agent%29](https://en.wikipedia.org/wiki/Manus_%28AI_agent%29)

66 98 <https://apnews.com/article/aaf01029923011a403ceeb949cf3db5e>  
<https://apnews.com/article/aaf01029923011a403ceeb949cf3db5e>

71 <https://openclaw.ai/>  
<https://openclaw.ai/>

73 <https://arxiv.org/html/2603.11853v1>  
<https://arxiv.org/html/2603.11853v1>