AI エージェント導入検討に向けた比較・説明資料

Manus

1. はじめに

本資料は、社内業務の効率化および高度化を目的として、AI エージェント（Manus、Genspark、Perplexity、Felo AI）の導入を検討するにあたり、情報システム部門向けに各ツールの仕組み、セキュリティ、データ取り扱いポリシーを比較・整理したものです。各ツールは単なるチャットボットを超え、自律的にタスクを計画・実行する「エージェント」としての機能を備えており、企業のセキュリティ要件を満たすエンタープライズ向けプランを提供しています。

2. 各 AI エージェントの仕組みと特徴

2.1 Manus

Manus は、Meta 社が買収した完全自律型の汎用 AI エージェントです。ユーザーの指示に基づき、自律的に計画を立て、ブラウザ操作、コード実行、データ分析などの複雑なタスクを遂行します [1] [2]。

アーキテクチャと仕組み Manus の最大の特徴は、「Manus Sandbox」と呼ばれるクラウド上の仮想マシン（クラウドコンピューター）をタスクごとに割り当てる点にあります。このサンドボックスは完全に隔離された環境であり、ネットワークアクセス、ファイルシステム、ブラウザ、各種ソフトウェアツールを備えています [3]。AI エージェントはこれらのツールを駆使してタスクを実行し、必要に応じてコードを記述・実行することも可能です。また、特定の LLM に依存しない（LLM-agnostic）設計を採用しており、タスクに応じて最適な基盤モデルを自動的に選択します [4]。

2.2 Genspark

Genspark は、AI 検索エンジンから発展したノーコードの自律型 AI エージェントプラットフォーム（Super Agent）です。自然言語の指示だけで、プレゼンテーション作成、動画生成、メール管理、電話発信などのワークフローを自動化します [5]。

アーキテクチャと仕組み Genspark の中核技術は、GPT-4、Claude、Gemini など複数の特化型大規模言語モデル（LLM）を組み合わせた「Mixture-of-Agents（MoA）」アーキテクチャです [5] [6]。このアプローチにより、複数のモデル間で出力を相互検証し、AI のハルシネーション（もっともらしい嘘）を低減するとともに、高い精度と信頼性を実現しています。また、80 以上のツールが統合されており、テキスト生成にとどまらない幅広いタスクの実行が可能です [5]。

2.3 Perplexity

Perplexity は、従来の検索結果のリンク一覧ではなく、信頼できる情報源に基づく直接的な回答を提供する AI 駆動の「アンサーエンジン」です。リアルタイムの情報検索と高度な AI モデルを組み合わせ、簡潔で検証可能な洞察を提供します [7]。

アーキテクチャと仕組み Perplexity のアーキテクチャは、静的なインデックスに依存せず、オンデマンドのクローリングと API インジェストによるリアルタイムの Web データ取得を基盤としています [7]。検索には「Retrieval-Augmented Generation（RAG）」を採用し、BM25 とベクトル埋め込みを用いたハイブリッド検索によって、回答を検証済みの情報源に紐付けます [7]。回答の生成には、OpenAI の GPT シリーズや Anthropic の Claude シリーズなど、複数の最先端 LLM をタスクに応じてルーティングして使用します [7]。

2.4 Felo AI

Felo AI は、日本発の AI 検索エンジンおよび自律型 AI エージェントシステムです。深掘り検索、動画要約、AI 翻訳などの複雑なタスクを実行でき、ユーザーは自然言語で独自のエージェントを構築することも可能です [8] [9]。

アーキテクチャと仕組み Felo Agent は、約 30 種類の事前設定されたエージェント（要約・翻訳、コンテンツ生成、データ分析・リサーチなど）を提供し、日常的なビジネスニーズに対応します [8]。また、「LiveDoc」と呼ばれる人間と AI の共創ワ

ークスペースを提供し、複数の AI エージェントが協働するマルチエージェントアーキテクチャを採用しています [10]。これにより、同時並行でのタスク実行や、セッションをまたいだ永続的なコンテキストの共有が可能となっています [10]。

3. セキュリティおよびデータ取り扱いポリシー

情報システム部門が最も懸念するセキュリティ認証、データの学習利用、およびアクセス制御について比較します。

3.1 Manus のセキュリティ

Manus は、エンタープライズグレードのインフラストラクチャと厳格なコンプライアンス体制を構築しています。

- **セキュリティ認証**: ISO/IEC 27001:2022（情報セキュリティマネジメントシステム）、ISO/IEC 27701:2019（プライバシー情報マネジメントシステム）、および SOC 2 Type 2 を取得しています [11]。
- **データの学習利用**: Manus はユーザーのデータを AI モデルのトレーニングに使用しません。また、サードパーティのモデルプロバイダーとも、ユーザーデータをトレーニングに使用しない旨の正式な契約を結んでいます [4]。
- **データ保護とサンドボックス**: タスクごとに隔離された「Manus Sandbox」を使用し、ゼロトラスト原則に基づき運用されます。サンドボックス内のデータは暗号化され、セッション終了後（無料版は 7 日、有料版は 21 日）に自動的に削除されます [3]。
- **エンタープライズ機能**: Team プランでは、シングルサインオン（SSO）がサポートされており、管理者はメンバーのアクセスやクレジット利用を統合管理できます [12] [13]。

3.2 Genspark のセキュリティ

Genspark は、エンタープライズクライアント向けに明確なデータセキュリティおよびプライバシーポリシーを定めています。

- **セキュリティ認証**: SOC 2 Type I の監査を進行中であり、2026 年に SOC 2 Type II および ISO 27001 の取得を目標としています [14]。
- **データの学習利用**:「ゼロトレーニング」原則を掲げ、ユーザーデータをモデルのトレーニングに使用しないことを契約および技術的制御によって保証しています [14]。
- **データ保護と分離**: マルチテナント VPC における論理的な分離を行っており、転送時は TLS 1.3、保存時は AES-256-GCM で暗号化されます [14]。
- **エンタープライズ機能**: SSO（SAML 2.0 / OIDC）およびコンソールアクセス時の多要素認証（MFA）を必須としています。また、追加料金で専用 VPC の提供も可能です [14]。

3.3 Perplexity のセキュリティ

Perplexity Enterprise Pro は、企業のデータセキュリティとプライバシーを最優先に設計されています。

- **セキュリティ認証**: SOC 2 Type II に準拠しており、独立した第三者によるセキュリティプラクティスの検証を受けています [15]。
- **データの学習利用**: 企業データは、Perplexity の AI モデルのトレーニングや微調整には一切使用されません。サードパーティのモデルプロバイダーとも同様の契約を結んでいます [15]。
- **データ保護とアクセス制御**:「Security Hub」と呼ばれる中央管理コマンドセンターを提供し、管理者はファイルのアップロード/ダウンロード権限、共有コンテンツの管理、データ統合（コネクタ）の制御、使用可能な AI モデルの選択などを詳細に設定できます [15]。
- **エンタープライズ機能**: SSO と MFA をサポートし、短期間のセッション認証情報を組み合わせています。また、スレッドに添付されたファイルは 7 日後に自動的に削除されます [15]。

3.4 Felo AI のセキュリティ

Felo AI は、日本国内のデータセンターを利用し、日本のビジネス環境に適したセキュリティを提供しています。

- **セキュリティ認証**: Felo のサーバーは、日本国内にある ISO 27001 認証を受けたデータセンターで所有および管理されています [16]。
- **データの学習利用**: Felo Enterprise のプライバシーポリシーにおいて、ユーザーが入力するプロンプトやアップロードするファイル（ユーザーコンテンツ）は、明示的な同意がない限り、AI モデルの学習データとして利用しないと明記されています [17]。
- **データ保護**: ユーザーとサーバー間のすべてのデータ交換は TLS 暗号化で保護されています。音声翻訳ファイルやテキストは一時的に RAM に保存され、永続的なストレージには書き込まれません [16]。
- **エンタープライズ機能**: Felo Enterprise では、SSO（シングルサインオン）機能がサポートされており、安全なワンクリックアクセスとワークフローの簡素化を実現しています [18]。

4. 比較サマリー表

項目	Manus	Genspark	Perplexity Enterprise Pro	Felo Enterprise
主な特徴	仮想マシン(Sandbox)を駆使した完全自律型エージェント	複数 LLM を組み合わせた MoA アーキテクチャによるタスク自動化	RAG とリアルタイム検索に基づく高精度なアンサーエンジン	日本発、マルチエージェントによる共創ワークスペース(LiveDoc)
セキュリティ認証	ISO 27001, ISO 27701, SOC 2 Type 2	SOC 2 Type I (進行中)	SOC 2 Type II	ISO 27001 (データセンター)
AI 学習へのデータ利用	利用しない（サードパーティ含む）	利用しない（ゼロトレーニング原則）	利用しない（サードパーティ含む）	利用しない（明示的な同意がない限り）
データ保存場所	AWS US (Virginia) 等	US West (デフォルト)、要件に応じ選択可	AWS 等のセキュアなクラウドインフラ	日本国内のデータセンター

項目	Manus	Genspark	Perplexity Enterprise Pro	Felo Enterprise
エンタープライズ管理機能	SSO 対応、チーム管理、アクセス制御	SSO (SAML/OIDC)、MFA、専用 VPC(オプション)	Security Hub による詳細な権限管理、SSO、MFA	SSO 対応

5. 導入に向けた推奨事項

情報システム部門への説明においては、以下のポイントを強調することを推奨します。

1. **AI 学習へのデータ利用の防止**: 検討している 4 つのツールすべてにおいて、エンタープライズ向けプランでは入力データが AI の学習に利用されないことが明記されており、機密情報の漏洩リスクが極めて低いこと。
2. **国際的なセキュリティ基準の準拠**: Manus および Perplexity はすでに SOC 2 Type 2 等の厳格な認証を取得しており、Genspark や Felo AI も ISO 27001 等の基準に準拠した運用を行っていること。
3. **管理者によるガバナンスの確保**: 各ツールとも SSO（シングルサインオン）に対応しており、既存の社内認証基盤（Entra ID 等）と統合することで、情報システム部門による一元的なアカウント管理とアクセス制御が可能であること。
4. **用途に応じたツールの選択**:
    - 複雑な業務プロセスの完全自動化やコード実行を伴うタスクには **Manus**
    - プレゼン作成や外部ツール連携など多様なタスクの自動化には **Genspark**
    - 社内ドキュメントや最新の Web 情報を統合した高精度なリサーチには **Perplexity**
    - 日本国内でのデータ完結や、チームでのドキュメント共創には **Felo AI**

References

[1] https://www.datacamp.com/blog/manus-ai [2] https://dxpo.jp/college/ai-agent/ai-manus.html [3] https://manus.im/blog/manus-sandbox [4] https://trust.manus.im/faq [5] https://skywork.ai/blog/models/genspark-agent-ai-features-access-how-it-works/ [6] https://medium.com/algomart/genspark-ai-explained-the-autonomous-ai-workspace-that-can-do-your-work-for-you-4143070c7184 [7] https://www.frugaltesting.com/blog/behind-perplexitys-architecture-how-ai-search-handles-real-time-web-data [8] https://felo.ai/blog/felo-ai-feature-overview/ [9] https://aismiley.co.jp/ai_news/what-is-felo/ [10] https://felo.ai/blog/help-livedoc-faq/ [11] https://trust.manus.im/ [12] https://help.manus.im/en/articles/12697595-what-is-the-current-single-sign-on-sso-subscription-pricing-for-manus-team [13] https://help.manus.im/en/articles/11711750-what-is-manus-team-plan [14] https://www.genspark.ai/policies/enterprise-clients-data-security-and-privacy-policy [15] https://www.perplexity.ai/ja/hub/blog/how-perplexity-enterprise-pro-keeps-your-data-secure [16] https://felo.me/ja/security [17] https://felo.ai/enterprise/privacy-policy [18] https://felo.ai/ja/blog/enterprise-sso-integration/