AIエージェント導入検討資料

情報システム部門向け

Manus / Genspark / Perplexity / Felo AI 比較

社内業務効率化・高度化に向けた技術・セキュリティ評価

本資料の目的と対象ツール

4つのAIエージェントを情報システム部門の視点で比較する

本資料は、社内業務効率化のためのAIエージェント導入を検討するにあたり、情報システム部門が懸念する観点から4ツールを比較・整理したものです。

1. **仕組みとアーキテクチャ**
2. **セキュリティ認証とコンプライアンス**
3. **データ取り扱いポリシー（学習利用の有無）**
4. **エンタープライズ向け管理機能（SSO等）**

Manus

Meta社傘下の完全自律型汎用AIエージェント。仮想マシンを駆使してタスクを実行。

Genspark

複数LLMを組み合わせたノーコード型エージェントプラットフォーム。MoAアーキテクチャで精度向上。

Perplexity

リアルタイム検索とRAGを組み合わせたAIアンサーエンジン。情報源の引用で信頼性を確保。

Felo AI

日本発・国内データセンター運用のAI検索エンジン＋エージェント。LiveDocで共創。

AIエージェントとは何か — 従来のAIチャットとの違い

AIエージェントは「回答する」のではなく「タスクを実行する」

従来のAIチャット（ChatGPT等）は、ユーザーの質問に対して「回答テキスト」を生成するにとどまります。AIエージェントは以下を自律的に行います。

- **タスクの計画立案** — 手順や戦略を自律決定
- **ツールの使用** — ブラウザ操作やコード実行などを実行
- **結果の検証と修正** — エラー時の対処と再試行
- **継続的な作業の遂行** — 複数ステップのワークフローを完遂

情報システム部門への説明ポイント

AIエージェントはシステムやデータに**実際にアクセスして操作を行う**ため、単なるチャットツール以上に重要な仕組みが必要です：厳格な権限管理・アクセス制御（SSO/MFA）・監査ログ・隔離された実行環境

Manus — Sandboxで動く自律エージェント

タスクごとに隔離されたクラウドコンピューターを使用

Manusの核はクラウド上の完全隔離された仮想マシン「Manus Sandbox」です。

完全隔離された仮想マシン

タスクごとに独立したVMで実行、他と完全に隔離されます。

フル機能の環境

ブラウザや実行環境、ファイル操作をAIが直接操作可能です。

LLM-agnostic設計

タスクに応じて最適な基盤モデルを自動選択します。

買収と継続性

Metaによる買収後もエンタープライズ向けサービスを継続中です。

情報システム部門への説明ポイント

サンドボックスの隔離により、他ユーザーのデータや環境への影響を防ぎます。**ゼロトラスト原則**で設計され、セッション終了後は環境を破棄してデータ残留リスクを低減します。

Genspark — 9つのLLMが協調するMixture-of-Agentsプラットフォーム

複数のAIモデルが相互検証することでハルシネーションを大幅に低減する

Gensparkは「Mixture-of-Agents（MoA）」アーキテクチャを採用しています。

9種類の特化型LLM

GPT-4.1、Claude、Geminiなど、複数の最先端モデルを組み合わせてタスクを実行します。

相互検証による精度向上

複数モデルが出力を相互検証し、誤情報（ハルシネーション）を低減します。

80以上の統合ツール

プレゼン作成・動画生成・電話発信・メール管理など、幅広い業務に対応します。

急速な市場浸透

Super Agent公開後、45日で年間収益3,600万ドルを達成した実績があります。

情報システム部門向けの要点

外部サービスへのデータ送信先を把握するため、**サブプロセッサー一覧の確認**が必須です。

Perplexity — RAGとリアルタイム検索で根拠ある回答を生成

情報源の引用を必ず付与することで、AIの回答の信頼性と検証可能性を担保する

Perplexityは「アンサーエンジン」として、検索とAI生成を融合しています。

リアルタイムWeb検索

常に最新の情報を取得します。

ハイブリッドRAG

BM25とベクトル検索を組合せ高精度に取得します。

情報源の明示

回答には必ず引用を付与し検証しやすくします。

社内データ連携

Google Drive等のドキュメントと連携可能です。

情報システム部門への説明ポイント

社内ドキュメントをコネクタ経由で連携する際は、アクセス制御を **Security Hubで細かく制御** できます。これにより意図しない機密情報の読み込みを防止します。

Felo AI — 日本発・国内データセンター運用のAI検索＋エージェント

データが日本国内に留まることで、国内法規制への対応と情報管理が容易になる

Felo AIは東京を拠点とするFelo株式会社が開発した日本発のAIサービスです。

高精度AI検索エンジン
多言語対応の検索

事前設定エージェント
約30種のエージェントで自動化

LiveDoc（共創ワークスペース）
協働するマルチエージェント環境

国内データセンター運用
日本国内のISO 27001認証データセンター

情報システム部門への説明ポイント

4ツールの中で唯一、データが **日本国内のデータセンター** に保存されます。個人情報保護法（PIPA）への対応や、データの国外移転を避けたい場合、または国内のコンプライアンス基準を厳格に満たす必要がある企業に特に有効です。

セキュリティ認証・コンプライアンス比較

4ツールすべてが国際的なセキュリティ基準に準拠または取得を目指している

項目	Manus	Genspark	Perplexity	Felo AI
SOC 2 Type 2	**取得済**	取得目標(2026)	**取得済**	—
ISO 27001	**取得済**	取得目標(2026)	—	**データセンターが取得済**
ISO 27701	**取得済**	—	—	—
GDPR	**対応**	対応(進行中)	**対応**	**対応**
HIPAA	—	対応(進行中)	**対応**	—
データ保存場所	AWS米国	米国西部(デフォルト)	AWSクラウド	**日本国内**

評価ポイント: ManusとPerplexityはSOC 2 Type 2取得済みで第三者検証が完了しています。一方、Felo AIは4ツールの中で唯一、日本国内のデータセンターを利用しており、国内データ完結の要件を満たします。

データの学習利用ポリシー — 4ツール共通の重要な保証

エンタープライズプランでは、4ツールすべてが入力データをAI学習に利用しない

企業が最も懸念する「入力した情報がAIの学習に使われるか」という問いへの回答：

Manus

ユーザーデータをモデルのトレーニングに使用しません。

Genspark

契約と技術的制御で学習利用を行わないことを保証します。

Perplexity

企業データは学習や微調整に使用されません。

Felo AI

明示的な同意がない限り、学習データとして利用しません。

重要：無料プランとエンタープライズプランの違い

無料プランでは学習利用の可能性があるため、企業利用では**エンタープライズ/有料プランを使用すること**を推奨します。

アクセス管理・エンタープライズ機能比較

SSOと管理者コントロールにより、情報システム部門による一元管理が可能

機能	Manus	Genspark	Perplexity	Felo AI
SSO対応	○ (SAML等)	○ (SAML/OIDC)	○	○
MFA	○	○ (必須)	○	—
管理者コンソール	○	○	○ (Security Hub)	○
監査ログ	○	○	○	—
専用環境	サンドボックス	専用VPC(オプション)	AWSセキュアクラウド	日本国内DC
インシデント通知	72時間以内	72時間以内	—	—

SSOを活用することで、既存の社内ID管理基盤（Microsoft Entra ID、Okta等）と統合し、**退職者アカウントの即時無効化**などのガバナンスを確実に確保できます。

用途別推奨ツール

業務の性質と情報管理要件に応じて最適なツールを選択する

Manus

推奨用途：複雑なワークフローの自動化

リサーチからレポート作成までの複数ステップを自律実行。隔離VMで安全にコード実行やブラウザ操作が可能。

Genspark

推奨用途：高精度な調査と連携

複数LLMの相互検証（MoA）で誤情報を抑制。外部ツール連携が求められる業務に適しています。

Perplexity

推奨用途：社内データ連携とファクトチェック

Web検索と社内ドキュメント連携によるRAG検索で、情報源が明示される運用に向きます。

Felo AI

推奨用途：国内データ完結と多言語リサーチ

国内でデータを完結させる必要があるプロジェクトや、多言語情報収集に適しています。

導入のポイント： 部署ごとの業務特性（自動化重視 / 検索精度重視 / データ保管重視）に応じて、複数のツールを使い分けるのが有効です。

情報システム部門への推奨アクション

段階的な導入アプローチで、リスクを管理しながら効果を最大化する

PHASE 1

要件定義とツール選定

自社のセキュリティポリシーと業務要件に照らし合わせ、最適なツールを選定します。

- ✓ データ保存場所の要件確認（国内必須か等）
- ✓ 必要な連携先（社内DB等）の洗い出し
- ✓ エンタープライズプランの契約

PHASE 2

PoC（概念実証）の実施

情報システム部門および一部の業務部門でテスト導入を行い、管理機能を検証します。

- ✓ SSO連携とプロビジョニングのテスト
- ✓ 管理者コンソールでの権限設定
- ✓ 監査ログの取得と監視体制の構築

PHASE 3

ガイドライン策定と展開

安全な利用のためのルールを定め、全社または対象部門へ展開します。

- ✓ 入力禁止情報の定義（機密情報等）
- ✓ AI出力結果のファクトチェック義務化
- ✓ 定期的な利用状況のモニタリング

◎ **最も重要な第一歩：** まずは情報システム部門内で実際に各ツールのエンタープライズ版を試用し、**「管理機能の使い勝手」**と**「既存のセキュリティ基盤（IdP等）との親和性」**を直接評価することを強く推奨します。

まとめ — 情報システム部門が確認すべき3つのポイント

適切なプランと管理体制を整えれば、4ツールすべてが企業利用に適している

1

エンタープライズプランの必須化

無料プランは入力データが学習に使われる可能性があります。業務利用では学習利用をオプトアウトできるエンタープライズ契約が必要です。

2

セキュリティ要件と保存場所の適合

SOC 2等の第三者認証の有無や、データの保存場所（国内完結等）を自社のセキュリティポリシーに合わせて選定します。

3

SSOとアクセス制御の統合

既存のID基盤とSAML/OIDCで連携し、プロビジョニングや退職時の無効化を自動化する体制を構築します。

結論：AIエージェントは強力な業務効率化ツールです。情報システム部門が主導して安全な環境（エンタープライズ版）を提供することが最大のリスクヘッジです。