企業向けAIエージェント導入に向けた技術アーキテクチャおよびセキュリティ評価報告書

Gemini 3.1 pro

エグゼクティブ・サマリーおよび情報システム部門における評価の文脈

企業環境における人工知能（AI）の活用は、単発のプロンプトに対してテキストやコードを生成する対話型AIの段階を脱し、ユーザーの指示に基づいて計画を立案し、自律的に複数のプロセスを実行する「エージェント型AI（Agentic AI）」へのパラダイムシフトを迎えている。社内の情報システム部門がこれら次世代のAIツールを評価し、エンタープライズ環境への導入を承認するためには、表面的な業務効率化のポテンシャルだけでなく、そのバックエンドで稼働する技術的メカニズム、アイデンティティおよびアクセス管理（IAM）との統合性、そして極めて厳格なデータ保護およびコンプライアンス要件への適合性を多角的に精査する必要がある。

本報告書は、社内への導入候補として挙げられている主要なAIエージェントプラットフォームであるManus、Genspark、Perplexity、およびFelo AIの4製品について、情報システム部門の審査基準となる深層のアーキテクチャ、セキュリティ統制、およびライセンスと運用コストの構造を網羅的に分析したものである。各ツールは「自律的なタスク実行」という共通の目的を持ちながらも、モデルのルーティング手法、メモリの管理方法、データガバナンスへのアプローチにおいて根本的に異なる設計思想を採用している。本分析は、情報システム部門が直面するシャドーITの抑止、データ流出（Data Exfiltration）の防止、および既存のアイデンティティプロバイダ（IdP）との安全な統合という観点から、各ツールの適格性を客観的に評価し、組織の要件に最適なプラットフォームを選定するための技術的根拠を提供する。

AIエージェントの技術的アーキテクチャと実行メカニズムの深層

AIエージェントが従来の言語モデルと一線を画す最大の理由は、与えられた目標に対して中間ステップを自律的に推論し、外部のツール（API、ブラウザ、ファイルシステム、コード実行環境）を操作して結果を導き出す点にある。この自律性を実現するための技術的なアプローチは、各プラットフォームによって大きく異なり、それぞれの処理速度、精度の安定性、およびタスクの性質に対する適性に直接的な影響を与えている。

Perplexity：複数モデルの動的オーケストレーションと専用ブラウザの統合

Perplexityは、高精度の回答エンジンとしての実績を基盤に、エンタープライズ向けの自律型機能である「Perplexity Computer」および専用の「Cometブラウザ」を展開している[1]。同プラットフォームのアーキテクチャの中核は、単一の巨大な言語モデルに依存するのではなく、最大20種類の最先端の専門的な大規模言語モデル（LLM）を動的にオーケストレーションするシステムにある[2]。ユーザー

から入力されたクエリの複雑さや要求されるタスクの性質をシステムが瞬時に解析し、深い学術調査に特化したモデル、複雑なコードのデバッグに特化したモデル、あるいはデータの視覚化に特化したモデルへとタスクを最適にルーティングする。この設計により、単一モデル特有のハルシネーション（事実誤認）リスクを構造的に低減し、常に高い精度の成果物を生成することが可能となっている。

また、Perplexityの実行環境において特筆すべきは、Cometブラウザを通じたリアルタイムのWebアクセスとアクション実行機能である[2]。エージェントは仮想的なサンドボックス内で推測を行うのではなく、実際のWeb環境にアクセスして情報を合成し、ユーザーのブラウザウィンドウ内で直接アクションを実行する。実証テストのデータによれば、複数サイトにまたがるデータスクレイピングや、GmailおよびGoogleカレンダーと連携したスプレッドシートへのデータ集約といったマルチステップのタスクにおいて、Perplexity Computerは競合であるManusと比較して5倍から10倍の速度で処理を完了し、わずか60秒でフォーマットの整った出力を提供する圧倒的なレイテンシの低さを実証している[1]。これは、日常的な業務フローにAIエージェントを組み込む上で、システム遅延によるユーザーのストレスを最小化する極めて実用的なアーキテクチャであると言える。

Manus：コンテキスト・エンジニアリングと「失敗を記憶する」仮想コンピュータ環境

近年Meta Platformsによって約20億ドルという巨額で買収されたシンガポール拠点のスタートアップによる「Manus」は、他のAIエージェントとは根本的に異なるアプローチを採用している[4]。Manusの設計思想は、人間のブラウジング行動やデスクトップ上の操作を忠実に模倣する「仮想コンピュータ（Virtual Computer）」モデルに基づいている[6]。

技術的な観点において最も革新的なのは、モデル自体のエンドツーエンドのファインチューニングに頼るのではなく、「コンテキスト・エンジニアリング」の限界に挑戦している点である[8]。LLMのコンテキストウィンドウ（一度に処理できるトークンの上限）は高価かつ有限であるため、Manusのエージェントフレームワークは情報を3つの階層に分割して動的にロードする仕組みを備えている。レベル1であるメタデータ（名称や説明）は起動時に最低限のトークン（約100トークン）でロードされ、レベル2のメイン命令文（約5000トークン未満）は該当するスキルがトリガーされた瞬間にロードされる。そして、レベル3のスクリプトや参照ファイルなどの重いリソースは、実際に参照が必要になったオンデマンドのタイミングで初めてコンテキストに読み込まれる[11]。この厳密なメモリ管理により、システムは不必要なリソースの浪費を防ぎ、クラウドインフラストラクチャにおけるKVキャッシュのヒット率を最大化して遅延とコストを抑える工夫を凝らしている[9]。

さらに情報システム部門が注目すべき点は、Manusがタスク実行時に発生したエラーや失敗をコンテキストから消去せず、意図的に保持し続ける「失敗のトラッキング機構」をアーキテクチャに組み込んでいることである[8]。多くのAIシステムはエラーを隠蔽し、直前の状態にロールバックしようとするが、Manusは外部の永続的なメモリとしてファイルシステムを活用し、失敗したアクションのログをモデルに学習させる。これにより、エージェントは「何が機能しなかったか」を理解し、同じ過ちを繰り返すことなく別のアプローチを自律的に立案する。この徹底した自己修正プロセスは、複雑なSaaSプロダクトの構築や広範なリサーチにおいて非常に高い精緻さをもたらすが、同時に処理速度の大幅な低下という明白なトレードオフを生じさせており、即時性が求められるタスクには不向きである[6]。

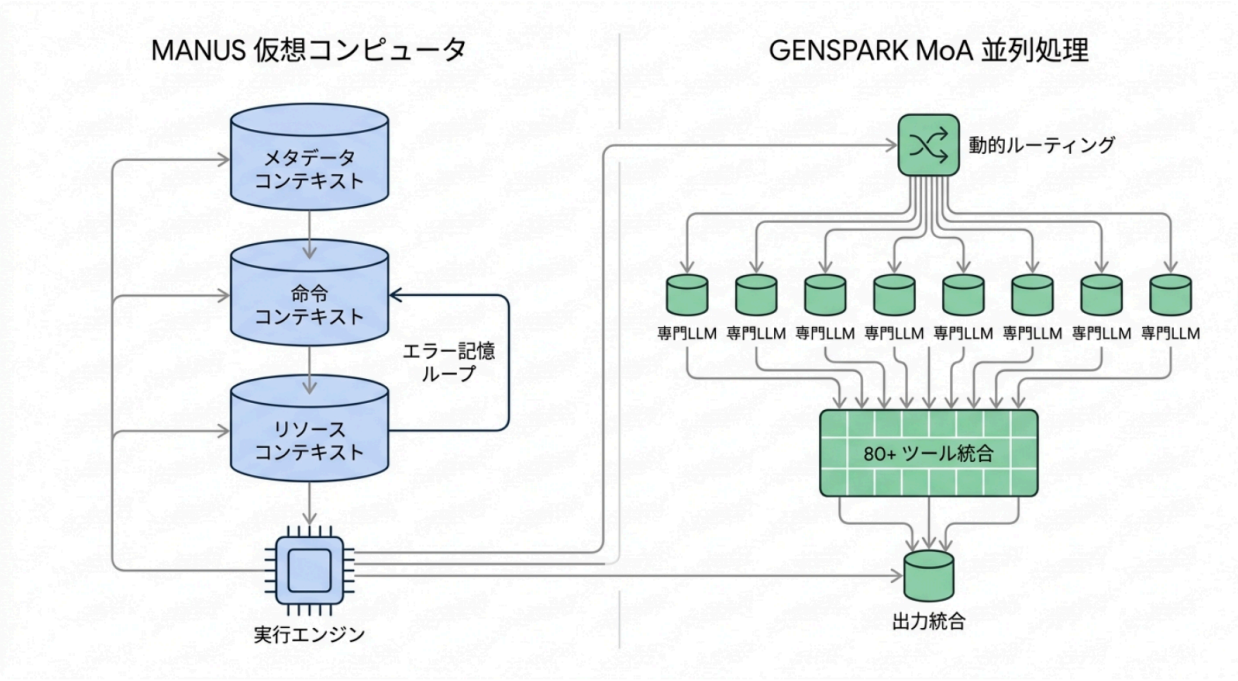
Genspark：Mixture-of-Agents (MoA)と厳格な出力フォーマットの強制

Gensparkの「Super Agent」は、単一ベンダーのLLMによる制約を回避するため、「Mixture-of-Agents（MoA）」と呼ばれる多層的なアーキテクチャを採用している[12]。このシステムは、背後で9つの専門的な大規模言語モデルと、80を超える多様な外部ツールを並行してオーケストレーションする能力を持つ[12]。

Gensparkの技術的優位性は、動的ルーティングと複数のモデルによる「コンセンサス検証」にある[12]。例えば、旅行の計画からレストランの予約（合成音声を用いた実際の電話予約を含む）、プレゼンテーションスライドの生成に至るまで、多岐にわたるタスクが入力されると、システムはタスクを細分化し、テキスト処理、画像生成（GPT-image-1など）、音声処理、データ分析のそれぞれに最適なモデルを割り当てる[14]。さらに、生成された事実関係の主張に対しては、複数のモデルが独立して回答を生成し、ソースと照らし合わせて自動的にファクトチェックを実行する機構が組み込まれている[12]。

また、情報システム部門が社内の他のシステムとAPI連携を行う際に重要となるのが、出力の安定性である。Gensparkのアーキテクチャは、すべてのエージェント出力に対して厳格なJSONフォーマットを強制する設計となっており、構造化されていない自然言語の揺らぎによって後続のデータ処理パイプラインが停止するリスクを防いでいる[12]。しかしながら、Gensparkは速度とデプロイの容易さ（そのまま公開可能なランディングページの即時生成など）を最優先しているため、出力されるコンテンツは美しく機能的である一方で、情報の深さや正確性において「それなりに近い（close enough）」レベルに留まることがあり、金融機関など厳密な精度が求められる専門的な業務フローにおいては信頼性に欠けるとの指摘も存在する[16]。

主要AIエージェントにおけるタスク実行アーキテクチャの比較



Manusは段階的なコンテキスト読み込みとエラー記憶によって深い自律性を確保する一方、Gensparkは複数モデルの並列処理（MoA）によってタスクを高速に処理する設計思想を持つ。

Felo AI：開発者向けエコシステムとのシームレスな統合と多言語インフラ

Felo AI（Felo Enterprise）は、特定のタスクに特化した検索エージェント機能に加え、開発者の既存のワークフローに直接統合されるオープンソースのツールキットを中核機能として位置づけている[18]。

社内の情報システム部門やソフトウェアエンジニアリング部門にとって、Felo AIの最大の技術的優位性は「Felo Skills」アーキテクチャの存在にある。これは、Node.jsのパッケージマネージャ（npm install -g felo-ai）を介してインストールされるオープンソースのCLI（コマンドラインインターフェース）コマンド群であり、Claude Code、OpenClaw、Gemini CLI、OpenAI Codexといった既存の開発エディタやターミナル環境に直接AIエージェントのスキルを埋め込むことができる[18]。通常、強力なAIコーディングエージェントであっても、モデルの学習データがカットオフされた日付以降の最新情報や、外部のドキュメント、APIリファレンスにはアクセスできないという致命的なギャップが存在する。Felo Skillsはこのギャップを埋めるものであり、開発者はターミナル環境からコンテキストを切り替えることなく、リアルタイムのWeb情報検索、特定のURLからのMarkdown形式でのコンテンツ抽出、YouTube動画の字幕データの取得、さらには最新のエラーログに関する解決策の検索までをシームレスに行うことができる[18]。

また、情報検索の基盤として、25以上の言語をサポートする独自のクロスランゲージ（多言語）検索アルゴリズムを搭載している点も重要である。ユーザーが母国語でクエリを入力すると、システムは

世界中の異なる言語で書かれた最新情報や学術論文、技術ドキュメントを瞬時に検索、自動翻訳し、構造化された形で合成して回答を生成する[23]。これに加えて、検索結果やアップロードされたファイルを基に、社内向けのプレゼンテーションスライド（PPT）、マインドマップ、長文のレポートをワンクリックで即座に生成する機能（AI Slides、LiveDoc AIなど）も備えており、ドキュメント作成の自動化という面でも極めて実用的なアーキテクチャを提供している[19]。

情報システム部門向け：セキュリティ要件およびコンプライアンスフレームワークの評価

エンタープライズ環境への新しいSaaSやAIツールの導入において、情報システム部門が最も重視するのは、情報漏洩を防ぐためのセキュリティ統制と、データプライバシーを保証するコンプライアンス要件への適合性である。これら4つのAIプラットフォームは、セキュリティの成熟度やデータガバナンスの考え方において、極めて明確な差異が存在しており、一部のツールには看過できないビジネスリスクが内包されている。

Perplexity：エンタープライズグレードの堅牢なセキュリティ基盤

セキュリティ・コンプライアンスの観点において、Perplexity（Enterprise Proプラン）は情報システム部門の厳格な要件を完全に満たす、最も成熟したフレームワークを構築している。

独立監査人によるSOC 2 Type 2認証を既に取得しており、情報セキュリティの内部統制が継続的かつ効果的に機能していることが第三者によって証明されている[25]。さらに、医療保険の相互運用性と説明責任に関する法令であるHIPAAのセーフガードに準拠するためのギャップアセスメントを実施しており、欧州の厳格な一般データ保護規則（GDPR）への対応、および決済情報保護のためのPCI-DSS（SAQ A）要件も完全に満たしている[25]。また、米国政府機関のクラウドセキュリティ基準であるFedRAMP（20x Low Information）の評価も進行中であり、公共部門水準のセキュリティを指向している[26]。

インフラストラクチャのアクセス制御は極めて強固である。本番環境と開発・テスト環境は、別々のAWSアカウントとネットワーク構成によって物理的かつ論理的に完全に分離されており、本番環境へのアクセス制御にはAWS IAM（Identity and Access Management）が利用されている[25]。エンジニアがデバッグなどの目的で機密リソースにアクセスする必要が生じた場合でも、一時的な権限のみを付与するJIT（Just-In-Time）アクセス制御が強制され、権限の悪用や漏洩リスクを最小化している[25]。従業員の端末管理にはMDM（モバイルデバイス管理）が導入され、エンドポイントでの脅威検知・対応（EDR）ソリューションが全組織のデバイスに展開されている[25]。さらに、クラウドインフラストラクチャのリアルタイムな脆弱性監視にはWizを利用し、AWS CloudTrailのログやアプリケーションログの監視にはPanther SIEM（セキュリティ情報イベント管理）を採用して、24時間365日体制での脅威検知・インシデント対応を行っている[25]。これに加え、年次でのサードパーティによるペネトレーションテスト（侵入テスト）の実施や、BugCrowdを通じたプライベートなバグバウンティプログラムの運営など、継続的な脆弱性管理プログラムを実践している[25]。

情報システム部門にとって最も重要となるデータ保護の確約についても、Enterprise Proの契約において「エンタープライズ顧客のデータ（社内ファイル、検索クエリ、プロンプト）をLLMのトレーニングに絶対に利用しない」という厳格なポリシーが明記されており、企業秘密がモデルの重みとして吸収さ

れる懸念を完全に払拭している[2]。ファイルの保持期間も管理者が最大1日まで設定できるなど、強力なデータ保持ポリシーの制御が可能である[2]。

Felo AI：データ主権と厳密なアクセス管理の保証

Felo AIのエンタープライズプランもまた、明確なデータ主権の保証を中核に据え、企業が安心してデータを預けられる環境を提供している。

同社は「ユーザーのデータは常にユーザーのもの」というデータ保護の原則を強く打ち出しており、エンタープライズ顧客が入力したデータやアップロードした社内ナレッジベースを自社のAIモデルの開発やトレーニングに流用することは一切ないと明言している[19]。また、外部のインフラストラクチャと連携する際、例えばGoogle Workspace APIを利用して社内カレンダーやドキュメントにアクセスする場合でも、そのデータ処理はFeloプラットフォームのセキュアなインフラストラクチャ内部に厳格に制限される。取得したデータをユーザー自身のコア機能提供以外の目的で利用することや、データマイニング、AIトレーニング、外部サービスへの転売、広告利用は固く禁じられている[29]。これは、情報システム部門がSaaSベンダーに対して要求するデータプロセッシングの範囲制限（DPA：データ処理契約）の基準を満たすものである。

情報開示の制御に関しても、安全第一の設計がなされている。従業員の検索履歴や構築したナレッジベースはデフォルトで非公開（Private by default）に設定されており、ユーザー自身が明示的に共有のアクションを選択しない限り、同じ組織内の他のチームメンバーや管理者からも不可視の状態で安全に保持される[19]。また、ISO 27001などの国際的なセキュリティ規格の認証も取得しており、バックエンドのシステム防御も標準的なエンタープライズ水準に達している[28]。

Manus：コンプライアンスの進展と看過できない地政学的リスク

Manusは、グローバルなエンタープライズ市場への展開に向けてプラットフォームの信頼性向上に努めているものの、その組織的背景に由来する特有のコンプライアンス・リスクを抱えている点に注意が必要である。

基盤となるインフラストラクチャのセキュリティにおいては、独立監査によるSOC 2 Type 1およびType 2認証を取得し、さらにISO 27001:2022（情報セキュリティマネジメントシステム）およびISO 27701:2019（プライバシー情報マネジメントシステム）の国際認証も受けており、データセンターからアプリケーションレベルまでの統制が一定の基準を満たしていることを示している[30]。しかしながら、Perplexityが対応しているような医療業界向けのHIPAAや、欧州のGDPRに対する細粒度のサポートは不足しているとセキュリティ専門家から指摘されている[33]。そのため、厳格な規制要件が求められる金融機関や医療機関などが利用する場合には、追加のセキュリティレイヤーや予防措置が不可欠となる。また、プロンプトが内部のトレーニングデータとして他のユーザーに暴露される可能性に対する懸念も一部で報告されており、機密情報の入力には慎重な判断が求められる[33]。

さらに情報システム部門として最も留意すべきは、Manusを取り巻く地政学的リスクと規制当局による審査の動向である。Manusは元々「Butterfly Effect Pte Ltd」という企業名でシンガポールを拠点に設立されたが、中国出身の創業者（CEOのXiao Hong氏など）と中国国内での開発というバックグラウンドを持つ[4]。このため、2025年末に発表されたMeta Platformsによる約20億ドル規模の巨額買収は、中国の商務省による厳格な規制審査の対象となっている[4]。この審査は、中国内で開発された

AI技術が国家の技術輸出管理やデータ転送規則に抵触しないかを調査するものであり、その結果として、Manusの経営幹部に対して中国当局からの出国禁止措置（Exit ban）が発動されたとも報じられている[4]。米国と中国が先端AI技術を巡って政策を厳格化している現在の環境において、この買収取引の先行きは不透明である。情報システム部門としては、サービスが突如として停止するリスク、長期的なサービスの安定性、およびデータ主権が最終的にどの国の管轄に置かれるかに関して、無視できない「サプライチェーンリスク」および「レピュテーションリスク」を認識した上で導入を検討しなければならない。

Genspark：深刻なセキュリティ脆弱性とデータ取り扱いの懸念

情報システム部門が全社へのSaaS導入を検討する際、Gensparkについてはセキュリティおよびデータプライバシーの領域において極めて慎重な精査と警戒が必要である。専門のクラウドセキュリティ機関（LayerX Securityなど）による評価において、エンタープライズの要求基準を満たさない複数の重大な脆弱性が指摘されている[36]。

Gensparkのアーキテクチャには、エンタープライズレベルのデータ分類機能や、機密データ転送のリアルタイム監視機構、および高度なデータ損失防止（DLP：Data Loss Prevention）コントロールが決定的に欠如していると報告されている[36]。これにより、従業員がプロンプトやチャットインターフェースを通じて無意識に社外秘のソースコードや顧客の個人情報、財務データなどを入力した場合、AIの処理パイプラインを通じて外部へ情報が流出する「データ流出（Data Exfiltration）」のリスクが極めて高い状態にある。システム的な防御の面でも、プロンプトインジェクション攻撃への耐性の低さや、不十分なフィッシング保護、生成されるコードのセキュリティ上の欠陥など、多くの脆弱性がリストアップされている[36]。

さらに問題視されるべきは、Gensparkの不透明なデータ取り扱いとプライバシーポリシーの構造である。同社のプライバシーポリシーは複数のドメインにまたがって分散しており、データが物理的にどこで処理され、どれだけの期間保持されるのかに関する統一されたガバナンスが欠如している[36]。そして情報システム部門にとって致命的となるのが、ユーザーがアカウント設定から手動で明示的に「オプトアウト」を行わない限り、デフォルト設定では検索データやユーザーの入力したコンテンツが自社のAIモデルのトレーニングに利用されるという点である[36]。利用規約には「サービスを運営、促進、改善するため、および新しいサービスを開発するための限定的な目的のために、ユーザーのコンテンツを使用、保存、ホスト、複製、変更、適応させるライセンスを付与する」といった文言が含まれており、エンタープライズ向けにデータ保護を確約しているPerplexityやFelo AIとは対極の姿勢をとっている[37]。強力な監査・統制機能を提供する管理ダッシュボード（MicrosoftのAgent 365のような統合監視機能[38]）も存在しないため、現時点のセキュリティ体制のままGensparkを全社展開することは、コンプライアンス違反の重大なリスクを負うことと同義である。

主要AIエージェントのエンタープライズ・セキュリティ要件適合性

機能・要件	Perplexity	Manus	Felo AI	Genspark
SOC 2 Type II 認証	✓ 完備	✓ 完備	- 未対応	- 未対応
自社データ学習の除外	✓ 完備	！懸念あり	✓ 完備	！懸念あり
SSO（SAML）対応	✓ 完備	- 未対応	✓ 完備	- 未対応
HIPAA/GDPR対応	✓ 完備	- 未対応	- 未対応	！懸念あり
エンタープライズDLP・監視	✓ 完備	- 未対応	△ 一部対応	！懸念あり

PerplexityとFelo AIはエンタープライズデータの学習利用を明確に否定している一方、Gensparkはセキュリティ機能およびプライバシーポリシーに重大な懸念が報告されている。

データソース: Perplexity AI, Manus AI, Felo AI, LayerX Security, Azumo, Reddit

統合機能とアイデンティティ管理（IDaaS連携）の容易性

数百から数千のユーザーを抱えるエンタープライズ環境において、情報システム部門が新たなツールの運用保守にかかる工数を抑制し、セキュリティ体制を維持するためには、企業で既に導入されているアイデンティティ管理プロバイダ（IdP）との高度な連携機能が不可欠となる。

SSO（シングルサインオン）と自動プロビジョニングの深度

各AIエージェントともにエンタープライズ向けのプランにおいてSAMLベースのSSO（シングルサインオン）をサポートしているが、実装の深さやプロビジョニングの自動化、ライセンスモデルに対する考え方に大きな違いが存在する。

Perplexityは、アクセス管理において最もエンタープライズ要件に適合した実装を行っている。SAML 2.0に基づくSSO認証に加えて、多要素認証（MFA）を強制する機能を持ち、さらにSCIM（System for Cross-domain Identity Management）プロビジョニングに完全対応している[2]。SCIMプロビジョニングとは、Okta Workforce Identity CloudやMicrosoft Entra IDなどの企業側IdPで行われた従業員の入退社や部署異動の情報を、リアルタイムでPerplexity側に同期させる仕組みである。これにより、情報システム部門の管理者は、Perplexityの管理画面にログインして手動でアカウントを作成したり、退職者のアクセス権限を一つずつ剥奪したりする運用作業から完全に解放され、退職による

認証情報の残存リスク（オーファンアカウントの発生）を防ぐことができる。また、クリティカルなユーザーアクティビティを記録する詳細な監査ログ機能も提供し、システムへの可視性を高めている[2]。

Manusは、組織の規模拡張を支援するという戦略的アプローチから、30名以上のシート（座席）を契約するチームプランにおいて、SAMLおよびSCIMプロビジョニングによるSSO機能を「追加費用なし（無料）」で提供している[39]。これは、通常SSO機能に対して高額な追加料金を要求する多くのSaaSベンダー（いわゆるSSO Tax）とは異なる好意的なアプローチである。なお、30名未満の小規模なチームでSSOを利用する場合には、150米ドルの定額費用が発生する構成となっている[39]。SSOが有効化されたチーム環境においては、管理者が送信した招待メールの中のリンクをクリックするという面倒なプロセスを省略できる。従業員が自社のSSO認証画面を通過すると同時に、自動的にManusのチームワークスペースへとリダイレクトされ、アカウントが有効化されるシームレスなオンボーディングフローを実現している[40]。

Felo AIのエンタープライズプランもSSO認証を標準でサポートしており、従業員にシームレスな認証体験を提供している。管理者は専用のユーザー管理ダッシュボードを通じて、チームメンバーの追加・削除、および特定のAI機能を利用できるロール（役割）ベースのアクセス権限付与を直感的に一元管理できる[19]。対照的にGensparkは、標準的なメールアドレスとパスワードによるログイン認証システムは提供しているものの、SCIMプロビジョニングやエンタープライズ向けの高度なIdP連携に関する詳細な技術ドキュメントが乏しく、アクセスログの厳密な監査機能など、大企業が求める運用管理機能が不足している[41]。

APIによる外部連携と拡張性

社内の既存システム（ERP、CRM、社内ポータルなど）やデータレイクとAIエージェントをプログラム経由で統合するためのAPI機能も、ツール選定の重要な評価軸となる。

Manusは、Webブラウザ上のインターフェースだけでなく、システム間連携を可能にする堅牢なRESTful APIを公開している[42]。開発者はこのAPIを経由して、タスクのトリガー、ファイルのアップロードやダウンロード、そして結果の受信をプログラム上で自動実行し、Manusの強力なAI自律能力を自社のワークフローやカスタムアプリケーションに直接組み込むことができる[42]。また、セキュリティ面に配慮し、フロントエンドのコードに認証キーを露出させることなく、Manusのバックエンドシステムから安全に外部のサードパーティAPI（Google Mapsや企業の独自APIなど）を呼び出すためのセキュアなAPIシークレット管理機能も提供している[45]。

前述の通り、Felo AIはエンタープライズの開発者向けAPIとオープンソースエコシステムの構築に多大な投資を行っている。単なるAPIエンドポイントの公開にとどまらず、felo-skillsという開発者向けパッケージを通じて、既存のターミナル環境や統合開発環境（IDE）との摩擦のないインテグレーションを実現している[18]。GensparkもAPI連携の機能を有しており、Google AI StudioのAPIキーを利用してローカル環境で動作させるオープンソース版の提供や、Gensparkのワークフロー内部からOpenAIなどの外部APIを呼び出して機能を拡張するインテグレーション機能を備えている[46]。しかし、情報システム部門が社内の基幹システムからGensparkのSuper Agentを安全に呼び出して制御するための、詳細なエンタープライズ向けAPIドキュメントやSDKは限定的である。

コスト構造と投資対効果（ROI）の分析

ソフトウェアの全社導入における投資対効果（ROI）を算出するためには、各AIプラットフォームの価格モデルの違いを深く理解する必要がある。現在、AIエージェント市場の課金体系は、予算の予見性が高い「ユーザー単位（Seat-based）の固定料金モデル」と、利用量に応じて変動する「クレジットベースの従量課金ハイブリッドモデル」の二つに大別される。

固定料金モデルを採用している代表例がPerplexityとFelo AIである。Perplexity Enterprise Proプランは、1ユーザー（シート）あたり月額40ドル（年間一括払いの場合は20%割引が適用され年額400ドル）という極めてシンプルな価格体系である[48]。高度なリサーチやアプリ生成などの使用制限を拡張した最上位のEnterprise Maxプランは、1シートあたり月額325ドル（年額3,250ドル）と高額になるが、組織内でユーザーの要件に応じてProとMaxのシートを柔軟に組み合わせることが可能である[3]。Felo AIのエンタープライズ向けであるProプランは、個人および小規模チーム向けで月額14.99ドル（年間一括払いの場合は月額換算9.99ドル）、さらに高度な管理機能を持つBusinessプランは月額40ドルという競争力のある価格設定となっている[22]。この固定費モデルは、毎月のコストが明確に確定するため情報システム部門が年間予算を策定しやすく、従業員側も追加コストを気にすることなくツールの機能をフル活用できるという明確なメリットがある。

一方、ManusとGensparkは、背後で稼働するAIモデルへの推論負荷やリソース消費量に応じてクレジットが消化される「クレジットベースモデル」を採用している。Manusは、無料プラン（毎日300クレジットが付与される）から始まり、月額20ドルのStandard（月間4,000クレジット）、月額40ドルのCustomizable（月間8,000クレジット）、月額200ドルのExtended（月間40,000クレジット）という4つの階層を設けている[52]。どの有料プランにおいても同時実行可能なタスク数は20までに設定されており、年間契約を選択した場合はすべてのプランで17%の割引が適用される[52]。Gensparkも同様の階層型クレジットシステムを採用しており、Plusプランが月額24.99ドル（年間割引なし）、大幅に制限が引き上げられるProプランが月額249.99ドル（年間契約で月額換算199.99ドル）、そしてチーム機能や高度なアナリティクスが追加されるEnterpriseプランが月額29.75ドル（年間契約で月額換算22.50ドル）と設定されている[55]。

クレジットベースのモデルは、システムを利用する頻度が低いライトユーザーにとっては月額の運用コストを最適化できるという利点がある。しかしながら、全社的に展開した際に、特定のパワーユーザーがデータスクレイピングや動画生成などの高負荷な自律タスクを大量に実行した場合、月半ばで割り当てられたクレジットが枯渇するリスクが伴う。業務を継続させるためには、都度アドオンで追加のクレジットパックを購入する必要が生じ、結果として初期の見積もりを大幅に上回る予算超過（オーバーラン）が発生する危険性を情報システム部門は織り込んでおくべきである[53]。

エンタープライズ向け価格モデルおよび管理機能の比較

プラットフォーム	主要プラン（エンタープライズ向け）	課金モデル	価格目安	SSO・統合に関する注意事項
Perplexity	Enterprise Pro Enterprise Max	シート単位の定額制	$40 / ユーザー / 月 (Pro: 年払 $400) $325 / ユーザー / 月 (Max: 年払 $3,250)	特記事項なし
Manus	Team Extended	クレジット従量制	カスタム料金 (Team) $200 / 月 (Extended: 40,000クレジット)	30名以上のチーム 30名未満のチーム $150 ＋税
Genspark	Enterprise (Team)	ユーザー単位（クレジット超過時の追加購入リスクあり）	$29.75 / ユーザー / 月 (年払平均 $22.50 / 月)	特記事項なし
Felo AI	Enterprise	カスタム制（コンタクト数に応じた段階的アドオン）	カスタム（要問い合わせ）	特記事項なし

定額制を採用するPerplexityは予算の予見性に優れる。ManusやGensparkのクレジット制は、利用状況に応じてコストが変動するリスクを考慮する必要がある。

Data sources: Manus Help Center, Flowith, Felo AI, Metaflow, Skywork AI, NoCode MBA, Spectrum AI, Perplexity Help Center, Perplexity, Finout

ユースケースに基づく比較分析と戦略的導入アプローチ

情報システム部門がAIエージェントの導入承認を下すにあたり、単一のツールで社内のすべての部門の要求とセキュリティ要件を完全に満たすことは困難である。それぞれのアーキテクチャがもたらす長所と、セキュリティやコンプライアンス上のトレードオフを理解した上で、利用部門の業務シナリオに応じた適材適所の判断が求められる。

高度な事業リサーチと社内ナレッジの安全な運用（経営企画・法務・全社利用）

社内の機密ドキュメントを読み込ませての分析や、経営層向けの高度なリサーチにおいて推奨される最適解は、圧倒的にPerplexity Enterprise Proである。この判断の根拠は、機能面よりもまずセキュリティとコンプライアンスの堅牢性にある。SOC 2 Type 2認証、GDPRおよびHIPAA準拠のセーフガード、強力なデータ保護の確約（トレーニングデータのオプトアウト）という要件を完璧にクリアしており、情報システム部門が最も安心して全社展開の承認を出せるプラットフォームである。複数のLLMをオーケストレーションするアーキテクチャは情報の精度が高く、さらに「Internal Knowledge Bases」機能を用いて社内のPDFや規定集を横断検索するような、セキュアな社内ポータルとしての運用に最も適している。

グローバルリサーチと開発者ワークフローの自動化（海外事業部・エンジニアリング部門）

海外市場の動向調査や、ソフトウェア開発チームでの利用において高い効果を発揮するのがFelo AI（Felo Enterprise）である。海外事業部などが、自社の母国語を使用して現地語のニュースや学術論文を即座にリサーチするタスクにおいて、同プラットフォームのクロスランゲージ（多言語）検索技術は代替困難な価値を提供する。また、情報システム部門自体や開発部門においては、felo-skillsを利用して既存の開発エディタやターミナル環境に直接AIを組み込める点が、コンテキストスイッチングを減らし大幅な生産性向上に寄与する。エンタープライズデータの学習除外やISO認証の取得も明言されており、セキュリティ面での導入ハードルは極めて低い。

複雑な長期ワークフローとWebアプリ構築（R&D・イノベーション部門）

自律的に複数のWebサイトをブラウジングし、データの収集からソフトウェアの構築までを長期間にわたって完遂するようなタスクには、仮想コンピュータ環境を有するManusが機能面では適している。しかしながら、情報システム部門の立場からは、機能の有用性以上に、中国規制当局の審査や経営幹部の出国禁止といった地政学的な規制リスク、およびHIPAAやGDPRに対する細粒度のサポート不足という不確実性を重く見るべきである。導入を検討する場合でも、全社展開は直ちに見送り、社内の非機密タスクを扱う特定のR&D部門などに限定したPoC（概念実証）からのスモールスタートとし、常に代替手段を確保しておく（ベンダーロックインを避ける）ことが強く推奨される。

クリエイティブおよびコンテンツ生成（マーケティング部門）

調査結果から即座にランディングページ、プレゼンテーション資料、あるいは動画コンテンツを自動生成する能力において、GensparkのMoAアーキテクチャはマーケティング部門の大きな助けとなる。しかし、エンタープライズレベルでの情報システム部門の評価としては、同ツールは現時点で社内承認を下すべきではないとの結論に至る。ユーザー入力をデフォルトでAIの学習データとして使用する規約、データ損失防止（DLP）機能の決定的な欠如、および専門機関から指摘されている多数のセキュリティ脆弱性は、企業にとって受け入れがたい情報漏洩の重大なリスクを孕んでいる。利用部門から強い導入要望がある場合は、機密情報や社外秘のソースコードなどを一切入力しないという厳格な社内運用ルールの策定と、サンドボックス環境での孤立した運用が必須条件となる。

以上の詳細な分析結果を踏まえ、情報システム部門としては、全社的な生産性向上とデータセキュリティの担保を両立させる基盤としてPerplexity Enterprise Proの採用を第一候補とし、開発部門などの特化型ニーズを補完するアドオンとしてFelo AIの並行導入を検討するアプローチを提言する。

ManusおよびGensparkについては、コンプライアンス上の重大な懸念が払拭されるまで、正式な全社導入を見送ることが企業資産の保護において妥当な判断である。

引用文献

1. Perplexity Computer vs. Manus - Which One's Actually Better? - YouTube, 4月 19, 2026にアクセス、https://www.youtube.com/watch?v=-u2glMOMsVM
2. Perplexity Enterprise, 4月 19, 2026にアクセス、https://www.perplexity.ai/enterprise
3. Which Perplexity Subscription Plan is right for you?, 4月 19, 2026にアクセス、https://www.perplexity.ai/help-center/en/articles/11187416-which-perplexity-subscription-plan-is-right-for-you
4. Manus (AI agent) - Wikipedia, 4月 19, 2026にアクセス、https://en.wikipedia.org/wiki/Manus_(AI_agent)
5. Meta buys startup Manus in latest move to advance its artificial intelligence efforts - AP News, 4月 19, 2026にアクセス、https://apnews.com/article/meta-manus-purchase-ai-agents-aaf01029923011a403ceeb949cf3db5e
6. AI Super Agent Showdown: Perplexity Labs vs Manus vs GenSpark Comparison (Video Course) - Complete AI Training, 4月 19, 2026にアクセス、https://completeaitraining.com/course/ai-super-agent-showdown-perplexity-labs-vs-manus-vs-genspark-compar-video-course/
7. The 5 Best AI Agents for Your Desktop in 2026 - Manus, 4月 19, 2026にアクセス、https://manus.im/blog/best-ai-agents-for-desktop
8. From Theory to Practice: How Manus AI Validates Context Engineering Principles - Medium, 4月 19, 2026にアクセス、https://medium.com/@dario.fabiani/from-theory-to-practice-how-manus-ai-validates-context-engineering-principles-723ca524570d
9. Agentic AI Architecture Design: Building Effective AI Agents for Millions of Users - YouTube, 4月 19, 2026にアクセス、https://www.youtube.com/watch?v=u4Ox4SBSwLI
10. Context Engineering for AI Agents: Lessons from Building Manus, 4月 19, 2026にアクセス、https://manus.im/blog/Context-Engineering-for-AI-Agents-Lessons-from-Building-Manus
11. Manus AI Embraces Open Standards: Integrating Agent Skills to Usher in a New Chapter for Agents, 4月 19, 2026にアクセス、https://manus.im/blog/manus-skills
12. Genspark Agent AI: Features, Access & How It Works, Click to Use! - Skywork, 4月 19, 2026にアクセス、https://skywork.ai/blog/models/genspark-agent-ai-features-access-how-it-works/
13. Genspark ships no-code personal agents with GPT-4.1 and OpenAI Realtime API, 4月 19, 2026にアクセス、https://openai.com/index/genspark/
14. Genspark's Super Agent ups the ante in the general AI agent race | VentureBeat, 4月 19, 2026にアクセス、https://venturebeat.com/ai/gensparks-super-agent-ups-the-ante-in-the-general-

ai-agent-race
15. Genspark AI API: API Access, Docs & Integration Guide, Click to Use! - Skywork, 4月 19, 2026にアクセス、https://skywork.ai/blog/models/genspark-ai-api-api-access-docs-integration-guide/
16. I tested Genspark AI's 2026 features: Here's what worked | Lindy, 4月 19, 2026にアクセス、https://www.lindy.ai/blog/genspark-ai-features
17. How is Perplexity Computer different from Genspark? - Reddit, 4月 19, 2026にアクセス、https://www.reddit.com/r/Perplexity/comments/1rgb42p/how_is_perplexity_computer_different_from_genspark/
18. Felo Skills: The Open-Source Toolkit That Gives AI Coding Agents Real-World Capabilities, 4月 19, 2026にアクセス、https://felo.ai/blog/felo-skills-open-source-toolkit-ai-coding-agents/
19. Enterprise Pro - Felo - Your Free AI Search Engine, 4月 19, 2026にアクセス、https://felo.ai/enterprise
20. Felo Skills & Plugins for Claude Code, OpenClaw & Codex CLI - Felo AI, 4月 19, 2026にアクセス、https://felo.ai/en/skills
21. Felo-Inc/felo-skills - GitHub, 4月 19, 2026にアクセス、https://github.com/Felo-Inc/felo-skills
22. Best AI Developer Tools in 2026: What Actually Ships Code | Felo Search Blog, 4月 19, 2026にアクセス、https://felo.ai/blog/best-ai-developer-tools-2026/
23. Felo vs GenSpark vs Perplexity: Comparison of AI Search Tools | Felo Search Blog, 4月 19, 2026にアクセス、https://felo.ai/blog/felo-genspark-perplexity-ai-search-comparison/
24. Felo AI Pricing: Free vs. Pro — Is the Paid Plan Worth It for Daily Research Workflows?, 4月 19, 2026にアクセス、https://flowith.io/blog/felo-ai-pricing-free-vs-pro-worth-daily-research
25. Perplexity Enterprise, 4月 19, 2026にアクセス、https://www.perplexity.ai/enterprise/security
26. Trust Center - Perplexity AI, 4月 19, 2026にアクセス、https://trust.perplexity.ai/
27. How Perplexity Enterprise Pro Keeps Your Data Secure, 4月 19, 2026にアクセス、https://www.perplexity.ai/hub/blog/how-perplexity-enterprise-pro-keeps-your-data-secure
28. Introducing Felo Enterprise Plan: The Smartest AI Solution for Your Team's Productivity, 4月 19, 2026にアクセス、https://felo.ai/blog/introduction-felo-enterprise/
29. Privacy Policy - Felo Account, 4月 19, 2026にアクセス、https://account.felo.ai/policies/privacy-policy
30. Security - Manus, 4月 19, 2026にアクセス、https://manus.im/security
31. Resources - Trust Center - manus.ai, 4月 19, 2026にアクセス、https://trust.manus.im/resources
32. Trust Center - manus.ai, 4月 19, 2026にアクセス、https://trust.manus.im/
33. Manus AI: Key Benefits, Limitations & Production Readiness - Azumo, 4月 19, 2026にアクセス、

https://azumo.com/artificial-intelligence/ai-insights/manus-ai-limitations-benefits
34. Why Meta bought Manus — and what it signals for your enterprise AI agent strategy, 4月 19, 2026にアクセス、https://venturebeat.com/orchestration/why-meta-bought-manus-and-what-it-means-for-your-enterprise-ai-agent
35. China Halts Meta's Manus Takeover, Puts Mega Acquisition Under Investigation - YouTube, 4月 19, 2026にアクセス、https://www.youtube.com/watch?v=S-RCAghh4wI
36. Genspark Security Risks and Vulnerabilities - LayerX, 4月 19, 2026にアクセス、https://layerxsecurity.com/generative-ai/genspark-risks-and-vulnerabilities/
37. Genspark, take this warning seriously or you will lose. : r/genspark_ai - Reddit, 4月 19, 2026にアクセス、https://www.reddit.com/r/genspark_ai/comments/1r6aym7/genspark_take_this_warning_seriously_or_you_will/
38. Microsoft Agent 365: The Control Plane for Agents, 4月 19, 2026にアクセス、https://www.microsoft.com/en-us/microsoft-agent-365
39. What is the current Single Sign-On (SSO) subscription pricing for Manus Team?, 4月 19, 2026にアクセス、https://help.manus.im/en/articles/12697595-what-is-the-current-single-sign-on-sso-subscription-pricing-for-manus-team
40. Where can I enable/subscribe to a Single Sign-On (SSO) Subscription for Manus Team?, 4月 19, 2026にアクセス、https://help.manus.im/en/articles/12807937-where-can-i-enable-subscribe-to-a-single-sign-on-sso-subscription-for-manus-team
41. Genspark Login: Official Login Guide & Troubleshooting Tips, Click to Use! - Skywork, 4月 19, 2026にアクセス、https://skywork.ai/blog/models/genspark-login-official-login-guide-troubleshooting-tips/
42. Manus Documentation - Manus API, 4月 19, 2026にアクセス、https://manus.im/docs/integrations/manus-api
43. Overview - Manus API, 4月 19, 2026にアクセス、https://open.manus.ai/docs/v1/overview
44. Integrate Manus with Your Existing Tools, 4月 19, 2026にアクセス、https://manus.im/docs/integrations/integrations
45. Third-Party Integrations - Manus Documentation, 4月 19, 2026にアクセス、https://manus.im/docs/website-builder/third-party-integrations
46. README.md - ComposioHQ/open-genspark · GitHub, 4月 19, 2026にアクセス、https://github.com/ComposioHQ/open-genspark/blob/main/README.md
47. Can I integrate Genspark with other APIs? - LinkGo, 4月 19, 2026にアクセス、https://linkgo.dev/faq/i-integrate-genspark-with-other-apis
48. Enterprise Pricing and Billing: Frequently Asked Questions | Perplexity Help Center, 4月 19, 2026にアクセス、https://www.perplexity.ai/help-center/en/articles/10352986-enterprise-pricing-and-billing-frequently-asked-questions
49. Perplexity Enterprise Pricing - Get Started Today, 4月 19, 2026にアクセス、

https://www.perplexity.ai/enterprise/pricing
50. Perplexity Pricing in 2026 for Individuals, Orgs & Developers - Finout, 4月 19, 2026にアクセス、https://www.finout.io/blog/perplexity-pricing-in-2026
51. Felo AI Pricing 2026: Free vs. Pro — Is the Paid Plan Worth It for Daily Multilingual Research? - Flowith Blog, 4月 19, 2026にアクセス、https://flowith.io/blog/felo-ai-pricing-2026-free-vs-pro-daily-multilingual-research
52. Manus AI Pricing 2026: Plans, Credits & Costs Compared - No Code MBA, 4月 19, 2026にアクセス、https://www.nocode.mba/articles/manus-ai-pricing
53. Manus AI Pricing for 2026: A Detailed Breakdown of Each Plan | Lindy, 4月 19, 2026にアクセス、https://www.lindy.ai/blog/manus-ai-pricing
54. Manus AI Pricing 2026: Free Plan, Credits & Which Plan Is Worth It - AI Spectrum AI Labs, 4月 19, 2026にアクセス、https://spectrumailab.com/blog/manus-ai-pricing-plans-cost-guide-2026
55. GenSpark Pricing vs. Metaflow AI: Which Pays Back Faster in 2026?, 4月 19, 2026にアクセス、https://metaflow.life/blog/genspark-pricing
56. Genspark Price: Pricing Review, Plans & Best Option, Click to Use! - Skywork, 4月 19, 2026にアクセス、https://skywork.ai/blog/models/genspark-price-pricing-review-plans-best-option/
57. Genspark Pricing: Breakdown of Plans and Alternatives to Try | Lindy, 4月 19, 2026にアクセス、https://www.lindy.ai/blog/genspark-pricing
58. Actual Genspark Pricing Plans 2026 Revealed Free vs Plus vs Pro - Scribe, 4月 19, 2026にアクセス、https://scribehow.com/page/Actual_Genspark_Pricing_Plans_2026_Revealed__Free_vs_Plus_vs_Pro__AG1EbHBFTZCTNG32TcYtUg
59. Plans and Pricing - Manus Documentation, 4月 19, 2026にアクセス、https://manus.im/docs/introduction/plans