SECURITY EVALUATION REPORT

CONFIDENTIAL // IT GOVERNANCE PROTOCOL

TECHNICAL REVIEW 2024

AIエージェント導入に向けた技術・セキュリティ評価報告書

AIエージェント4製品の仕組みとセキュリティ特性を比較し、情報システム部門の承認を得るための評価ポイントを提示します。

PRODUCT SCOPE

Manus / Genspark / Perplexity / Felo AI

CATEGORY

Data Governance & Integration

01

INITIAL ASSESSMENT PHASE

SECURITY & GOVERNANCE ASSESSMENT

評価指標の定義とガバナンス基準

AIエージェント導入における情シス部門の主要な評価指標を定義し、セキュリティおよびガバナンスの基準を明確にします。データガバナンス、ID管理、データ主権の3つの観点から多角的に評価を行います。

データガバナンス

- **透明性の確保**
  入力データがAIモデルの学習に利用されないか、プロバイダーのポリシーを厳格に確認。
- **所有権の帰属**
  生成されたデータの所有権がユーザーに帰属し、ベンダーによる二次利用が制限されているか。

ID管理と認証

- **基盤連携**
  既存ID基盤（Okta, Azure AD等）とのシームレスな連携が可能であることを必須条件とする。
- **一元管理**
  SSOやSCIMによるプロビジョニングを活用し、アクセス権限のライフサイクルを統合管理。

データ主権

- **法規制遵守**
  サーバー設置場所の特定と、適用される法規制（GDPR等）の適合性を明確化。
- **地政学的リスク**
  中国の国家情報法など、地政学的なデータリスクの評価に基づき、利用範囲を限定。

TARGET TOOLS

Manus | Genspark | Perplexity | Felo AI

SYSTEM ARCHITECTURE

Manusのシステムアーキテクチャ

> Manusは既存システムとの深い連携と、自律的なワークフロー完結に特化したエージェントです。

自律적タスク実行

ユーザーの指示に対し、自ら計画を立て、ウェブ検索、APIアクセス、データ分析を複数のステップで実行します。

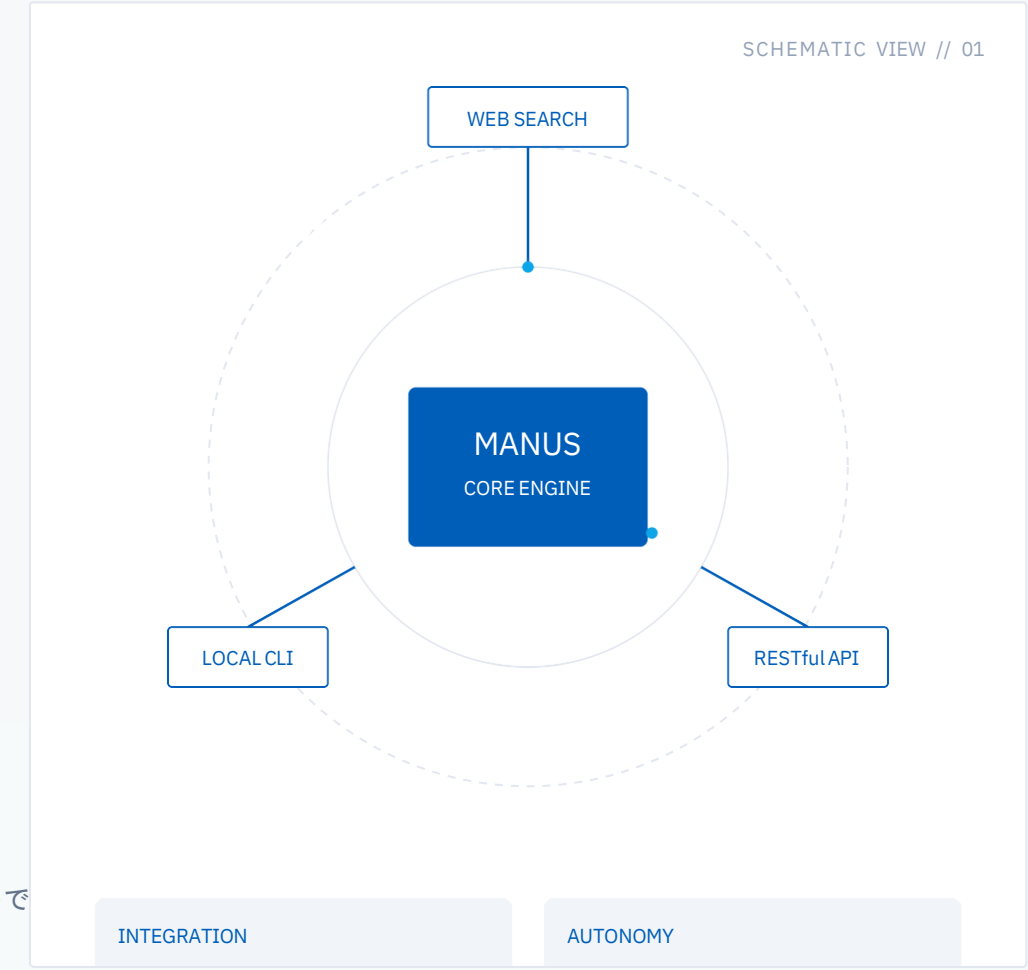
API中心の設計

RESTful APIを通じてプログラムから呼び出し可能であり、既存の業務フローに自律的な処理能力を組み込むことを目的としています。

ローカル環境拡張

許可された環境下で、コマンドラインを通じた直接的なファイル操作や処理を実行させることも可能です。

Manusは特定の大規模言語モデルに依存せず、外部システムとの「統合」を前提としたエージェントで



SECURITY ASSESSMENT OVERVIEW

Manusのセキュリティ評価

Manusは学習不使用を明記していますが、データ保存場所の特定と権限管理が評価の鍵となります。

Manusのデータ所有権、認証方式、および導入時の懸念事項について詳述します。

SYSTEM INTEGRITY CHECK: ACTIVE

AI学習への不使用

STATUS: SECURE

ユーザーが入力したデータをサービス改善や学習に利用しないことを明記しており、データの所有権はユーザーに帰属します。

認証方式

外部連携時にはOAuth 2.0やAPIキーを採用。最小特権の原則に基づき、限定的な権限範囲でのみアクセスを許可する設計となっています。

OAuth 2.0

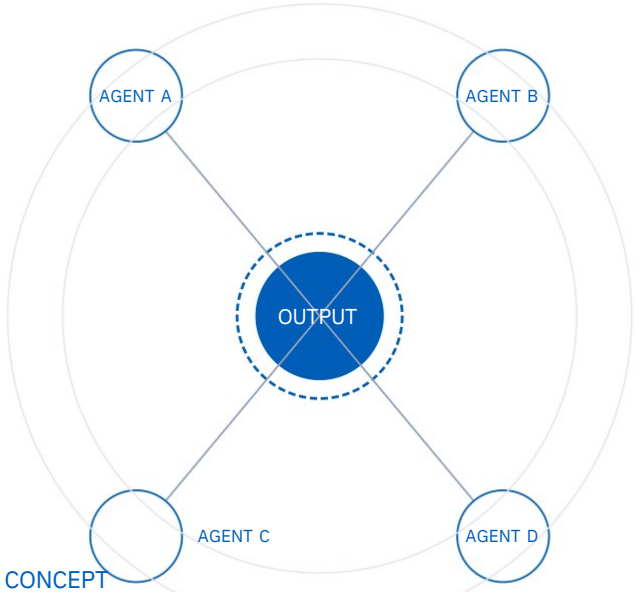
Least Privilege

注意点・懸念事項

- データの保存場所は「クラウド」とされていますが、具体的な地域が明示されていないため特定が必要です。
- API連携時のアクセス権限管理ポリシーの策定が不可欠です。

Gensparkの仕組みと特徴

MOA SCHEMATIC V1.0



CORE CONCEPT

Gensparkは複数のAIモデルを組み合わせ、調査から資料作成までを自動化する高機能ツールです。

01 Mixture-of-Agents (MoA)

複数のAIエージェントが並列でタスクを処理し、各モデルの強みを活かした最適な結果を統合。高度なレポートやスライドを自動生成します。

02 成果物作成の代行

単なる検索や回答にとどまらず、深層調査から最終的なアウトプット作成までをワンストップで完結させる「エージェント・ファースト」の思想を具現化。

03 統合環境

専用ブラウザやスライド作成機能がネイティブに組み込まれており、複数の外部ツールを個別に管理する手間を排除したシームレスな体験。

OVERVIEW: GensparkのMoAアーキテクチャと、業務代行型AIとしての特徴を説明します。

TECHNICAL GOVERNANCE REVIEW

Gensparkのガバナンス分析

> **Gensparkは高い生産性を持つ反面、データ主権と法的リスクに関する慎重な評価が求められます。**

Gensparkのプライバシーポリシーの不明瞭な点と、コンプライアンス上のリスクを分析します。

データ保存場所

LOW TRANSPARENCY

Microsoft Azure上で保存・処理されますが、具体的な国は不明です。データの物理的な所在の透明性に課題があります。

- INFRASTRUCTURE

法的リスク

HIGH REGULATORY RISK

創業者や資金調達の背景から、中国の国家情報法に基づく当局へのデータ開示リスクが専門家から指摘されています。

- COMPLIANCE

運用上の対策

MITIGATION REQUIRED

AI学習への利用を止めるには「オプトアウト設定」を全社的に徹底する必要があります。機密情報の取り扱いには適さない可能性があります。

- GOVERNANCE

SYSTEM INTEGRITY & ENTERPRISE SHIELD

Perplexityの信頼性と企業向け機能

信頼性の担保

ネット上の最新情報を要約し、回答に必ず出典リンクを提示。ソースを明示することで、AI特有のハルシネーション（もっともらしい嘘）リスクを大幅に低減し、ファクトチェックを容易にします。

VERIFIED SOURCES

Model Council機能

複数の最先端AIモデルの回答をリアルタイムで比較・統合。単一のモデルに依存せず、クロスチェックを行うことで客観的で信頼性の高い回答を生成する、Perplexity独自のアーキテクチャです。

MULTI-MODEL LOGIC

Enterpriseプラン

企業利用に最適化された高度な管理コンソールを提供。

- データプライバシーの保護
- 監査ログとSSO連携
- 厳格なセキュリティ要件への適合

CORPORATE GOVERNANCE

SECURITY & GOVERNANCE OVERVIEW

Perplexityのセキュリティ統制

> Perplexity Enterpriseは、SSO/SCIM対応と監査ログにより、高度なガバナンスを実現します。

ID管理(SSO/SCIM)

- **SAML 2.0対応**
  OktaやMicrosoft Entra IDとのシームレスな連携が可能。
- **SCIM同期**
  50シート以上のプランではユーザー同期の自動化をサポート。

ガバナンス機能

- リアルタイム監査ログ
  Webhook経由で管理者が操作ログを即座に取得可能。
- 高度な監視
  クエリ履歴やファイルアップロード操作を詳細に記録・追跡。

データ保持ポリシー

- 集中管理設定
  組織全体で検索履歴を無効化する強力な制御機能を完備。
- **AI学習への非利用**
  入力データは学習に使われず、保存期間も柔軟に指定可能。

PLATFORM CAPABILITIES

Felo AIの機能と利便性

Felo AIは検索から資料作成までをカバーし、
日本のビジネス環境に適した多機能ツールです。

MODULE 01

多機能アウトプット

単なる情報検索に留まらず、プレゼン資料の自動生成（PowerPoint形式）やマインドマップ作成など、思考の具体化を強力に支援します。

- Output Efficiency

MODULE 02

日本市場への最適化

日本の商習慣や法規制を深く意識した設計。日本語特有のニュアンスを汲み取った精度の高い情報収集と、ビジネスレベルの資料作成が可能です。

- Localized Intelligence

MODULE 03

Enterprise版の提供

企業導入に不可欠なデータセキュリティとプライバシー保護を強化。社内規定に合わせたデータ利用制限など、法人向けの高度な管理機能を提供します。

- Security Infrastructure

SECURITY ASSESSMENT / DATA SOVEREIGNTY

Felo AIのデータ主権と安全性

CORE ANALYSIS

データ保存場所とプライバシーポリシーの観点から、Felo AIの安全性を分析します。

Felo AIの国内データ管理体制と、企業導入におけるセキュリティ上のメリットを評価します。

データ保存場所の透明性

LOCATION

日本国内保存

Felo AIはデータ保存場所として「日本国内」を明記しており、国内の法規制やコンプライアンス要件が厳しい業界においても導入しやすい特徴があります。

ID: SEC_DATA_LOC

プライバシーポリシー

POLICY

非学習設定の遵守

ユーザーの同意なしにデータがAI学習に利用されることはなく、企業向けのデータ保護設定が充実しています。

ID: SEC_PRIV_OPT

企業向け管理機能

GOVERNANCE

一元的な管理体制

Enterprise版では、組織単位でのアクセス制御やデータ利用状況の可視化が可能であり、情シス部門による一元的な管理をサポートします。

ID: SEC_ENT_CTRL

SECURITY ASSESSMENT REPORT

セキュリティ特性の比較分析

学習ポリシー、保存場所、認証基盤の3軸で比較すると、PerplexityとFeloが統制面で優位です。

主要4製品のセキュリティ特性を比較し、情シス部門の承認を得るためのポイントを明確にします。

Perplexity
(Enterprise)

学習ポリシー

標準で不使用

データ保存場所

米国中心

認証基盤

SSO / SCIM完結

（最も充実した管理機能）

Felo AI
(Global Search)

学習ポリシー

同意なしには不使用

データ保存場所

日本国内を明記

認証基盤

API連携 / 個別管理

Manus / Genspark

学習ポリシー

Manus: 標準不使用

Genspark: オプトアウト必要

データ保存場所

具体的な特定が必要

認証基盤

個別管理が主

TECHNICAL EVALUATION

拡張性と外部連携の評価

API提供状況や外部ツールとの連携のしやすさを比較します。情報の信頼性とアウトプットの再利用性に焦点を当てた、システム統合の視点からの評価です。

「業務自動化ならManus、情報検索の組み込みならPerplexity、資料作成ならFeloが適しています。」

Manus

強力なAPIとローカル実行能力を持ち、特定の業務プロセスを自動化する「開発・統合」に向いています。

AUTO-PROCESS INTEGRATION

Perplexity

検索APIを提供し、社内ポータルなどへの組み込みが容易です。情報の信頼性とリアルタイム性を既存システムに付与します。

Felo AI

生成した資料をPPTXでエクスポートできるなど、既存のオフィスソフトとの親和性が高く、アウトプットの再利用性に優れます。

Genspark

プラットフォーム内での完結を重視しており、外部連携よりも単体での多機能性を活用する形態に適しています。

STRATEGIC ADOPTION ROADMAP // VER 1.0

戦略的導入シナリオの提示

組織の優先順位（ガバナンス、データ主権、自動化）に応じて、最適なツールを選択すべきです。調査結果に基づき、4つの導入推奨シナリオを提示します。

REF: PPLX-01

Perplexity (Governance Focused)

既存のID管理プロセスに完全に統合したい、大規模組織でのガバナンスを最優先する場合に最適です。

PRIMARY GOAL: ENTERPRISE INTEGRATION

REF: FELO-02

Felo AI (Data Sovereignty)

データ主権（日本国内管理）を重視し、かつ幅広い部署で資料作成まで効率化したい場合に有力な選択肢となります。

PRIMARY GOAL: REGIONAL COMPLIANCE

REF: MANU-03

Manus (Automation Focused)

特定の高度な自動化ワークフローを構築したい開発部門主導のプロジェクトに適しています。

PRIMARY GOAL: WORKFLOW EFFICIENCY

REF: GSPK-04

Genspark (Limited Pilot)

調査能力は高いですが、法的リスク評価が完了するまでは、非機密情報の取り扱いに限定した試験導入に留めるべきです。

PRIMARY STATUS: RISK MITIGATION

STRATEGIC EXECUTION PLAN

導入プロセスの実行計画

導入を具体化するための4つのアクションアイテムを定義します。承認に向けた最終ステップとして、詳細な仕様確認と法務連携、PoCの実施を提案します。

01 ライセンス体系の確認

PerplexityのSCIM対応など、高度な機能が必要な場合の最小シート数とコストの確認を行います。運用規模に応じた最適解を導き出します。

02 データ保存場所の書面確認

ManusやGensparkについて、ベンダーからデータ保存地域に関する公式回答を取得。セキュリティポリシーへの適合性を客観的証拠に基づき証明します。

03 法務部門との連携

特にGensparkの法的リスクについて、自社のコンプライアンス基準に照らした最終判断を仰ぎます。利用規約の精査とリスク許容範囲を確定させます。

04 PoC（概念実証）の実施

特定の部署で限定的に導入し、実際の利便性とセキュリティ設定の有効性を多角的に検証。実務レベルでのボトルネックを早期に解消します。

CONCLUSION // EVALUATION SUMMARY

結論：最適なツールの選択

各ツールの強みと懸念を正しく理解し、自社に最適なAIエージェントの導入を実現しましょう。

本報告書の結論として、各ツールの立ち位置を総括します。

統制のPerplexity

SSO/SCIM対応が唯一充実しており、情シス部門の管理負担が最も低い。企業ガバナンスを最優先する場合の最適解です。

RECOMMENDED FOR: CORPORATE GOVERNANCE

安全のFelo

国内データ管理と明確なポリシーにより、データ主権の懸念を払拭可能。法規制やコンプライアンス要件が厳しい業界に適しています。

RECOMMENDED FOR: COMPLIANCE-HEAVY INDUSTRIES

自動化のManus

API連携により、業務プロセスの抜本的な自動化が可能。単なる検索を超えた、AIによる実行力を求める組織に最適です。

RECOMMENDED FOR: PROCESS AUTOMATION

機能のGenspark

高機能だが、ガバナンスと法的リスクの慎重な評価が前提。先進的な機能を早期に取り入れたい技術重視のチーム向け。

RECOMMENDED FOR: TECH-FORWARD TEAMS

CLOSING PROTOCOL

ご清聴ありがとうございました

AIエージェント導入による業務変革を、
安全なガバナンス体制のもとで推進しましょう。

本資料に関するご質問や詳細な技術仕様の確認が必要な場合は、担当者までご連絡ください。