AI エージェント セキュリティ機能詳細比較レポート

Manus

本レポートは、企業での導入を検討している 4 つの AI エージェント（Manus、Genspark、Perplexity、Felo AI）について、情報システム部門が評価する上で重要となるセキュリティ機能の詳細を比較・整理したものです。

1. セキュリティ機能詳細比較表

各ツールのエンタープライズ向けプランにおけるセキュリティ機能を、以下の表にまとめました。

セキュリティ項目	Manus	Genspark	Perplexity	Felo AI
データ学習利用	利用しない（オプトアウト） [1]	利用しない（契約・技術的制御） [2]	利用しない（サードパーティ含む） [3]	利用しない（エンタープライズ版） [4]
暗号化（通信/保存）	TLS 1.3 / AES-256 [1]	TLS 1.3 / AES-256-GCM [2]	TLS 1.3 / AES-256 [5]	TLS 暗号化 [6]
データ保存場所	クラウド（AWS 等） [7]	US West（デフォルト）、VPC オプション [2]	US/EU データセンター [8]	日本国内（ISO 27001 認証 DC） [6]
SSO（シングルサインオン）	対応（SAML 等） [9]	対応（SAML 2.0 / OIDC） [2]	対応 [5]	対応 [4]
MFA（多要素認証）	対応 [9]	必須（コンソールアクセス） [2]	対応 [5]	不明
アクセス制御（RBAC）	対応 [9]	対応 [2]	対応（JIT アクセス制御含む） [5]	対応 [4]

セキュリティ項目	Manus	Genspark	Perplexity	Felo AI
監査ログ	対応 [9]	対応（30 日ローリングログ） [2]	対応（Enterprise ポータルで設定） [10]	不明
コンプライアンス認証	SOC 2 Type 1/2, ISO 27001/27701 [1]	SOC 2 Type 1（取得中）, ISO 27001（予定） [2]	SOC 2 Type 2, HIPAA, GDPR 準拠 [5]	ISO 27001（データセンター） [6]
インシデント対応	24/365 監視、72 時間以内通知 [1]	24/365 対応、72 時間以内通知 [2]	24/365 監視、Panther SIEM 活用 [5]	侵入テスト実施、99.5%稼働率 [6]
専用環境（分離）	サンドボックス（VM 隔離） [11]	論理的分離（VPC）、専用 VPC オプション [2]	AWS 環境での論理的分離 [5]	不明

---

2. 各ツールのセキュリティアーキテクチャと特徴

2.1 Manus

Manus は、高度な自律型 AI エージェントとして、インフラストラクチャから製品レベルまで多層的なセキュリティ対策を講じています。

- **コンプライアンス**: SOC 2 Type 1 および Type 2、ISO 27001:2022、ISO 27701:2019 の認証を取得しており、エンタープライズ要件を高いレベルで満たしています [1]。
- **インフラセキュリティ**: 暗号化キーへのアクセス制限、統合認証ゲートウェイの強制、リモートアクセスの暗号化と MFA 強制など、厳格なアクセス制御を実施しています [1]。
- **データ保護**: 顧客データはモデルのトレーニングに使用されず、退会時には確実に削除されるポリシーが運用されています [1]。

2.2 Genspark

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公開しています。

- **データライフサイクル管理**: 入力データは TLS 1.3 で暗号化されて送信され、保存時は AES-256-GCM で暗号化されます。処理後のログはセキュリティと課金目的で 30 日間のみ保持されます [2]。
- **デプロイメントモデル**: 標準のクラウド（マルチテナント）に加え、追加費用で専用 VPC オプションや、規制の厳しいワークロード向けのハイブリッド（Edge Gateway）モデルも提供予定です [2]。
- **コンプライアンス**: 現在 SOC 2 Type I の監査中で、2026 年には SOC 2 Type II および ISO 27001 の取得を目標としています [2]。

2.3 Perplexity

Perplexity Enterprise Pro は、堅牢なセキュリティ基盤の上に構築されており、特にアクセス制御とモニタリングに強みを持っています。

- **アクセス制御と認証**: AWS IAM を活用し、SSO と MFA をサポート。さらに、エンジニアに対しては必要な時のみアクセスを許可する JIT（Just-In-Time）アクセス制御を導入しています [5]。
- **インフラと監視**: 本番環境とテスト環境を厳格に分離し、Cloudflare による DDoS 保護や WAF を導入。Wiz を使用したクラウド環境の継続的な監視と、Panther SIEM による脅威検知を 24 時間 365 日体制で行っています [5]。
- **データ保持コントロール**: 管理者は Enterprise Security Hub から、ファイルのダウンロード許可や共有設定、データ保持期間（インコグニートモードの強制など）を細かく制御できます [10] [12]。

2.4 Felo AI

Felo AI は、特に日本国内でのデータ保管を重視する企業に適したセキュリティ体制を構築しています。

- **データセンター**: サーバーは日本国内の ISO 27001 認証を取得したデータセンターに設置されており、物理的なセキュリティ対策も施されています [6]。

- **データストレージ**: 音声翻訳ファイルやテキストは RAM に一時的に保存されるのみで、永続的なストレージには書き込まれない仕様となっており、情報漏洩リスクを低減しています [6]。
- **セキュリティテスト**: 内部および外部のペネトレーションテストを定期的に実施し、インフラとアプリケーションの脆弱性を継続的に評価・修正しています [6]。

---

3. 情報システム部門としての評価ポイント

1. **コンプライアンス認証の重視**: 既に SOC 2 Type 2 や ISO 27001 を取得している Manus や Perplexity は、社内のセキュリティ監査を通過しやすいと言えます。Genspark は現在取得プロセス中である点に留意が必要です。
2. **データ保存場所の要件**: 官公庁案件や特定の業界規制により「データが日本国内に保存されること」が必須要件となる場合、Felo AI が有力な選択肢となります。
3. **管理者コントロールの粒度**: Perplexity は Enterprise Security Hub を通じて、ファイル共有やダウンロード権限、コネクタ（Google Drive 等）のアクセス許可を細かく設定できるため、ガバナンスを効かせやすい設計になっています。
4. **環境の分離要件**: より高度なデータ隔離が求められる場合、Genspark の専用 VPC オプションや、Manus のサンドボックス環境による隔離アーキテクチャが有効に機能します。

References

[1] Manus Security. https://manus.im/security [2] Genspark Data Security & Privacy Policy for Enterprise Clients. https://www.genspark.ai/policies/enterprise-clients-data-security-and-privacy-policy [3] Perplexity Data Retention and Privacy for Enterprise Organizations and Users. https://www.perplexity.ai/help-center/en/articles/11187708-data-retention-and-privacy-for-enterprise-organizations-and-users [4] Felo AI Enterprise Pro. https://felo.ai/enterprise [5] Perplexity Enterprise Security.

https://www.perplexity.ai/enterprise/security [6] Felo AI Data Security. https://felo.me/security [7] Manus Selects AWS to Power General Purpose AI Agent. https://press.aboutamazon.com/aws/2025/12/manus-selects-aws-to-power-general-purpose-ai-agent-serving-millions-globally [8] Perplexity AI for Business Use: Enterprise Deployment Guide. https://neuraplus-ai.github.io/blog/perplexity-ai-for-business-use.html [9] Manus Trust Center Controls. https://trust.manus.im/controls [10] Perplexity Audit Logs. https://www.perplexity.ai/help-center/en/articles/11652747-audit-logs [11] Manus Sandbox Architecture. https://manus.im/blog/manus-sandbox [12] Perplexity Enterprise Security Hub Settings. https://www.perplexity.ai/help-center/en/articles/10517443-enterprise-security-hub-settings