

AIエージェントと業務システムをつなぐアクセス基盤「GAIA Governed AI Access」の提供を開始

AIエージェントの一元管理を実現。Claude・ChatGPT・Gemini等のAIに対応

アジアクエスト（東京都文京区、以下当社）は、複数のAIエージェントと社内の業務システムをつなぐアクセス基盤「GAIA Governed AI Access」（以下、GAIA）の提供を開始します。GAIAは、AIエージェントによるデータアクセスを制御・記録・管理するプラットフォームです。権限パスルーによる安全なデータ参照と、全アクセスの自動ログ記録により、企業のAI本番導入を後押しします。

アジアクエスト⇒ <https://www.asia-quest.jp/>**■サービス概要**

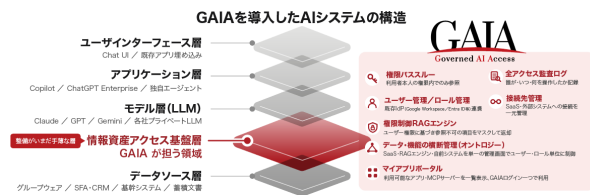
GAIAは、特定のAIモデルや製品に依存しない中立な基盤として、AIエージェントを安全・統一的に管理します。

- ・サービス名：GAIA Governed AI Access ・提供形態：クラウド型
- ・対応AI：Claude/ChatGPT/Gemini/Copilot/ChatGPTEnterprise/独自エージェント等
- ・接続規格：MCP（ModelContextProtocol）準拠—Anthropic社主導のAI接続標準仕様

■主な機能

▶**権限パスルー** AIエージェントは固定の広い権限を持たず、利用者本人の権限の範囲内でのみデータを参照。「権限を渡しすぎる」問題を根本から解消します。

▶**全アクセスの監査ログ** GAIAを経由した情報アクセスを自動記録。誰が・いつ・どの権限で・何を操作したかを追跡可能にし、コンプライアンス・稟議対応を後押しします。

**■接続対象システム（主なもの）**

- ・グループウェア：Microsoft365/Slack
- ・顧客・案件管理：SFA/CRM（Salesforce等）
- ・基幹システム：ERP/会計/人事システム等
- ・蓄積文書：社内図面・議事録・各種ドキュメント等

■導入期間イメージ

初期導入は以下の4フェーズで進めます（目安：最短6〜7週間）。実際の期間はお客様の環境により異なります。

- 1.事前設計（1〜2週間）要件ヒアリング、サイジング、IdP/SaaS接続点の合意、ネットワーク要件確認
- 2.環境構築（3〜7日）インフラプロビジョニング、GAIA本体インストール、IdP連携・コネクタ設定
- 3.データ接続（1〜2週間）対象SaaS・基幹システムのコネクタ設定、認証情報登録、ポリシー初期設定
- 4.本番化（1〜3週間）ユーザー展開、監査ログ要件確認、障害対応訓練、運用ドキュメント整備

■「野良AIエージェント」による権限管理の限界

企業のAI活用への期待が高まる中、組織内でのAI導入を阻む構造的な課題として浮上しているのが「野良AIエージェント」の問題です。複数のAIエージェントが社内システムに個別接続する状態が広がると、「どのAIが・いつ・どのシステムにアクセスしたか」を把握できず、権限管理も散漫になってしまいます。これにより、セキュリティの観点からAIに「権限を渡しすぎる」か「全く使わせない」かの二択を迫られ、結果的にAI活用が止まってしまうケースが後を絶ちません。また、AI業界全体を見渡すと、LLM（モデル層）やCopilot等（アプリケーション層）のサービスは充実している一方で、業務データソースとAIを安全につなぐ「基盤層」はいまだ手薄な状況です。この空白を埋めるために当社が開発したのが『GAIA』です。

■安全なAIエージェント活用に向けた権限管理基盤「GAIA」開発の背景と自社実践

当社は、「人とAIが共創し、人の創造的な価値を最大限に発揮できる社会」を目指すAIインテグレーターです。AIエージェントの急速な普及により、IT人材市場の二極化は加速しています。——コードを書くだけの単純作業はAIに代替されていく一方、複数のAIを統合・オーケストレーションし、ビジネス課題そのものを解決できる高度IT人材の価値は、ますます高まる——当社はその信念のもと、採用・育成・組織文化の全てをアップデートし続けています。約400名の国内エンジニアを擁し（2025年12月末時点）、ビジネス課題の理解から設計・実装まで担える「ビジネスエンジニア」が多数在籍。2025年7月には、クライアントに提供するAI活用の研究開発部門と、AIセキュリティ面を支える専門部門という「攻めと守り」の2部署を新設し、自らAIネイティブな組織へと変革を進めています。『GAIA』は、まさにその変革の過程で生まれ、自社での実践と運用のなかで磨き上げてきた、当事者だからこそ届けられるアクセス基盤です。

■アジアクエストのセキュリティへの取り組み

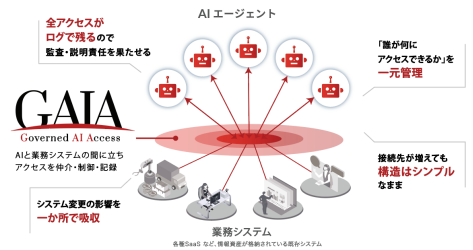
全システムにおいて、情報セキュリティを設計の根幹に据えています。役割・職責に基づく厳格なアクセス権限管理と最小権限の原則を徹底し、必要な人が必要なデータのみアクセスできる環境を実現します。利用するAIツールはいずれも企業向けセキュリティ基準に準拠したサービスを採用。社内データ・顧客情報がAI学習に利用されないことを保証するとともに、AI攻撃を受けた際の影響範囲を最小化する運用体制を整えています。また、社内規程・ガイドラインの整備、定期的な監査・モニタリング、全社員へのセキュリティ教育を継続的に実施し、安全なAI活用環境の維持に努めています。

■関連プレスリリースアジアクエスト、AIネイティブな組織づくりに向けた全社AI基盤の構築を推進 <https://www.asia-quest.jp/information/20260512>**■AIインテグレーターについて**

従来の強みである幅広い技術力による「デジタルインテグレーション」と、業界知見や課題理解に基づく提案力を持つ「ビジネスエンジニア」に加え、AIオーケストレーションをはじめとする高度な「AIエージェント開発」を組み合わせることで、意思決定や業務プロセスの高度化を実現するプロフェッショナル集団です。アジアクエストは、最適なドメイン特化型AIエージェントを提供し、お客様の戦略的パートナーとして社会に貢献する「AIインテグレーター」を目指します。

■アジアクエスト株式会社について

アジアクエストは、高度なAI技術を核に、AIX（AIトランスフォーメーション：AIによる業務変革）およびDXの実現を支援するAIインテグレーターです。AI・IoT・クラウドなど多様な技術に加え、建設・製造・小売といった各業界の知見をあわせ持つプロフェッショナル集団として、コンサルティングから設計・開発・運用、人材育成まで一貫して伴走。PoCから大規模システム構築まで、確かな実装力で、お客様と共に新たな価値の創出と変革を実現しています。

**AIエージェントのデータアクセスを「GAIA」で一元管理**

▶**ユーザー管理/ロール（権限）管理** GoogleWorkspaceやMicrosoftEntraIDなど既存のID基盤と連携。ユーザーごとにアクセス可能なMCP・データ・エージェントを管理します。

▶**接続先管理** 対象のSaaSや外部システムへの接続設定を一元管理。接続先を増やしても構造はシンプルに維持されます。

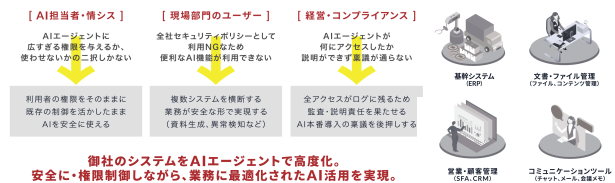
▶**権限制御RAGエンジン** ドキュメントの参照権限を項目レベルで制御。ユーザーの権限に基づき、参照不可の項目をマスクして返却します。

▶**データ・機能の横断管理（オントロジー）** 接続先のSaaS・RAGエンジン・自前システムを問わず、単一の管理画面で利用可能なデータとシステム操作をユーザー・ロール単位で制御します。

▶**マイアアプリポータル** 利用者は自分が使えるアプリケーションやMCPサーバーを一覧で確認。GAIAへのログイン一つで横断的に利用できます。

■GAIAのできる業務別課題解決例

AIエージェントの活用が進むほど、立場によって直面する課題は異なります。GAIAは、AI担当者・情シス部門、現場部門のユーザー、経営・コンプライアンス部門と言った、様々な部門が抱える権限管理・利用範囲・説明責任の課題に対応し、安全性と利便性を両立したAI活用を後押しします。



御社のシステムをAIエージェントで高度化。安全に・権限制御しながら、業務に最適化されたAI活用を実現。

特定のAIや製品に依存しない、オープンで安全なアクセス基盤を提供