

生成AI活用基盤の構築

Building Enterprise Platform for AI Agents

*AXイノベーションセンター

要 旨

生成AIの活用が全社的に広がって、社内各部門で多様な生成AI活用の開発が進んでいる。生成AIの活用は一層拡大することが予想され、今回の取組みでは、開発したAI資産の再利用を実現する生成AI活用基盤を構築した。複数のAI資産を連携可能とするオーケストレーターと、AI資産と社内外データを接続するデータ連携機能を備えることで、利便性を高めた。また、オープンな標準プロトコルを採用し、外部AIサービスとの接続など柔軟な連携と拡張を可能とした。さらに、認証・認可基盤と連携した権限制御を実現し、利用者がアクセス可能な範囲の情報だけを扱う安心・安全な利用環境を整備した。この基盤を全社の業務改革に活用して開発、運用の効率化を図って、各部門の自走的なAI活用を加速する。

1. ま え が き

生成AI及びAIエージェントの市場は急速に拡大しており、各社とも業務・設計・製造から顧客接点に至るまで積極的な活用を検討している。多様な事業領域を抱える三菱電機が競争力を維持・向上していくためには、特定部門の個別取組みにとどめるのではなく、組織横断で生成AIの活用を広げていく必要がある。

当社では業務プロセスや設計・製造業務の改革、事業部門主導の個別取組みなど、複数の生成AI活用プロジェクトを並行して立ち上げているが、各プロジェクトの成果共有を十分に行わないと類似機能の再開発が発生する可能性がある。さらに、各プロジェクトが個別にデータ連携、認証・認可、監視ログを作り込むと、技術的な重複と品質ばらつきが発生する懸念がある。特に、生成AIが機密情報を扱う場合、部門ごとのアドホックなセキュリティ実装は情報漏洩(ろうえい)のリスクにつながる。

そこで今回の取組みでは、全社横断で再利用可能かつ“安心・安全”に利用できる生成AI活用基盤(以下“本基盤”という。)を構築した。本基盤の目的は、①社内の複数プロジェクトで開発された質の高いAIエージェント及びツールを全社

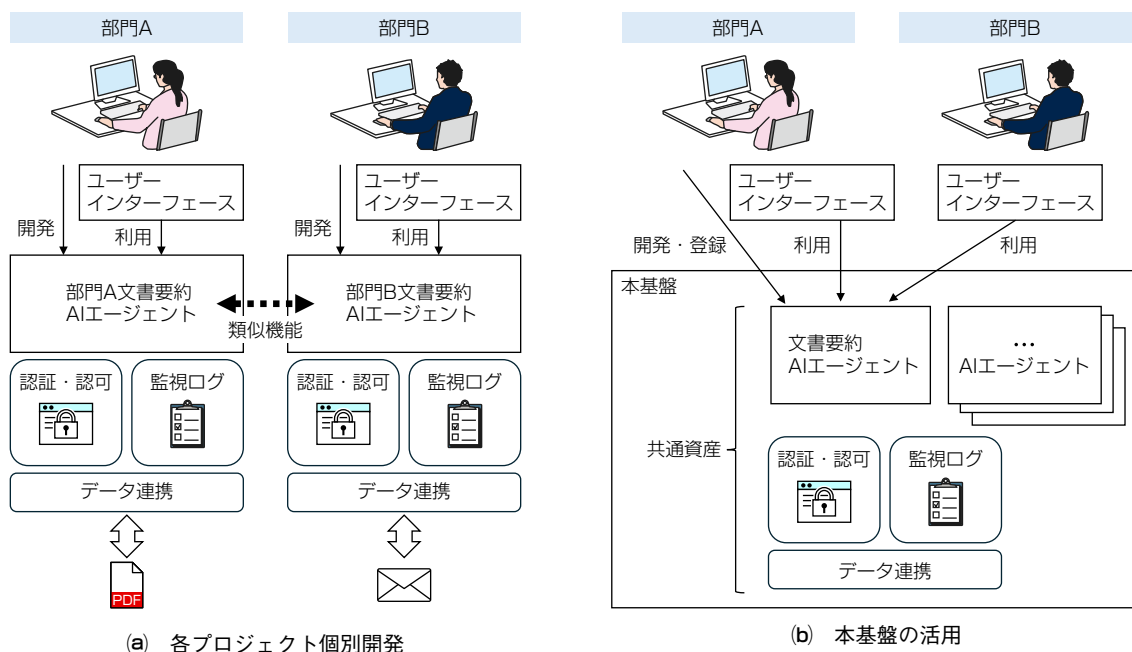


図1-本基盤による効果

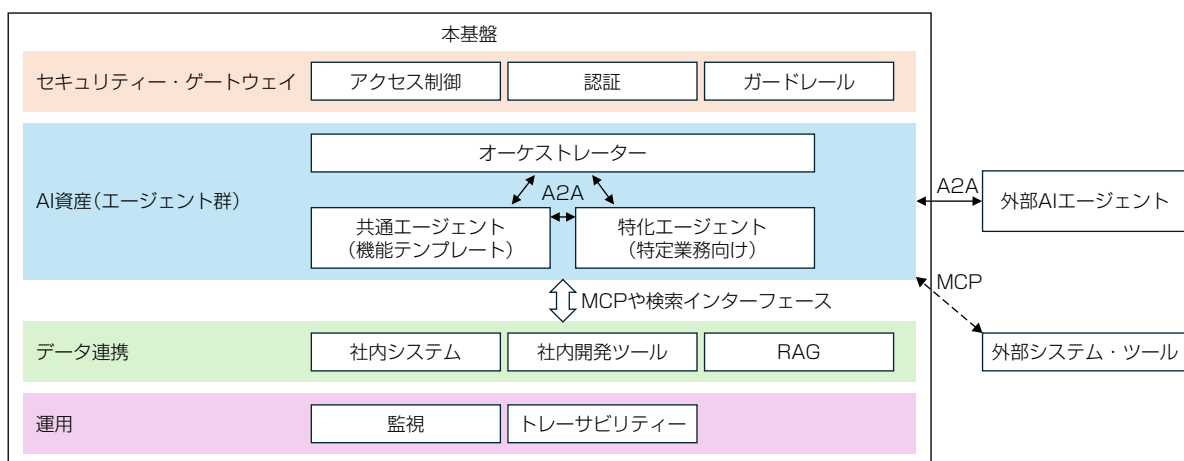
AI資産として再利用可能な形に整えて後続開発で活用できる仕組みを提供すること、②社内の認証・認可を踏襲した権限制御によって利用者がアクセス可能な範囲の情報だけを扱う仕組みを提供すること、③オープンな標準プロトコルを採用し、外部AIサービスとの接続性を確保することである。図1に、本基盤による効果を示す。複数部門による類似のAIエージェント開発を防いで、AIエージェントの再利用を促進する。

本稿では、本基盤のアーキテクチャー、主要機能と活用パターン、適用効果と今後の展望を述べる。

2. 本基盤のアーキテクチャー

本基盤は、蓄積したAI資産を全社で再利用して開発効率を高めること、情報管理とセキュリティを社内統制と整合させること、特定ベンダーの技術や環境への依存を排除して変化に柔軟に対応することを目的として、資産の再利用容易性、社内ガバナンスとの整合、構成要素間の疎結合の3点を設計原則とした。オープンな標準プロトコルとして、エージェント間協調はA2A (Agent to Agent Protocol)、データ連携はMCP (Model Context Protocol)を採用することで、エージェントのデプロイ先やデータの連携先を特定ベンダーの技術や環境に依存せず任意とできる点が本基盤の特徴である。

本基盤の構成要素を図2に示す。



RAG : Retrieval Augmented Generation

図2-本基盤の構成要素

(1) セキュリティ・ゲートウェイ

本基盤への入り口でアクセス制御と認証を担う。ガードレールも提供し、AIエージェントの不適切な回答の防止や暴走検知・停止を行う。

(2) AI資産(エージェント群)

利用者からの要求を分解して最適な実行手順を生成し、登録された複数のエージェントから適切なエージェントを選択して呼び出すオーケストレーターと、各部門・プロジェクトで開発されたエージェント(業務領域を問わずテンプレートとして再利用可能な共通エージェントと、特定業務に最適化された特化エージェント)で構成する。

(3) データ連携

社内外システムのデータソースやツールと安全かつ容易に連携するための仕組みである。RAGもこの層の機能の一つとして内包する。

(4) 運用

異なるベンダーのクラウド環境に対応してAI資産の稼働状態・応答時間・エラー率を可視化する監視と、呼出し履歴や処理経路を追跡可能にするトレーサビリティを備える。

2.1 A2A・MCPの採用

AIエージェント間の協調にはA2A、主要なデータ連携の手段にはMCPを採用した。オープンな標準プロトコルを採用することで、社内開発エージェントと外部ベンダー提供のAIエージェントや、MCP対応ツールを組合せ可能とした。

これによって、外部ベンダーより利便性の高いAIエージェントやツールが提供された際にも、迅速かつ柔軟に拡張可能になる。

2.2 セキュリティ・ガバナンス

本基盤は社内向け認証基盤と連携しており、社員はシングルサインオンで利用できる利便性を確保した。それに加えて、本基盤へのアクセスは社内環境からの接続に限定することで利用範囲を制御している。

また、AIエージェントは呼出しごとに利用者の権限を認可・検証する。AIエージェントは利用者本人がアクセスできる範囲内の情報だけ動作し、生成AIを介した意図しない情報越境を構造的に防止する。

3. 主要機能と活用パターン

本基盤は、再利用可能なAIエージェントを共通エージェントとして登録・提供する。共通エージェントは処理特性に応じて体系化しており、各プロジェクトはこれらを組み合わせることによって、短期間でアプリケーションを構築できる。本基盤では、特定業務向けに構築したAIエージェントや共通エージェントの組合せを特化エージェントとして登録し、社内展開することも可能である。

表1に共通エージェントの体系を示す。

表1-共通エージェント体系

項目	機能概要	想定活用場面
認識・解析	文字・音声・画像・動画等の非構造データを正規化し、構造化データに変換する	設計図面の認識、帳票読み取り、音声の議事録化、動画を手順書化
検索・抽出	指定情報に基づいて、情報源から必要な情報を検索・抽出する	技術動向の調査、登録された社内ナレッジの検索、ソースコードの自然言語検索
分類・スコアリング	パターンや相関・因果関係を見だし、類型化・評価・要因特定を行う	不具合情報の分類、リスク評価、品質のスコアリング
分析・最適化	目的関数を最大化する数値予測や解候補の探索を行う	製造工程の最適化、スケジュール最適化、需要予測
予測・推薦・推論	数値予測や提案、結論の導出を行う	故障予知、コンテンツ推進、意思決定支援
要約・生成	コンテンツの取りまとめや生成を行う	レポート生成、組み込み機器向けコード生成

本基盤では、次の三つの活用パターンを提供する。社内活用では、利用者は社内認証基盤を用いたシングルサインオンで認証を受けて、セキュリティ・ゲートウェイを通過した後、オーケストレーター経由又は個別に直接エージェントを呼び出すことで基盤を利用する。オーケストレーター及び各エージェントで利用者権限を認可・検証するため、AIエージェントは利用者の権限範囲内の情報だけを参照・処理する。

(1) Webアプリケーション構築

基盤の共通エージェントを組み合わせることで、各部門の業務に特化したWebアプリケーションを構築する。AIエージェントの処理や運用を基盤側に委ねることができて、各部門はユーザーインターフェースや生成AI以外の機能開発に注力できる。

(2) 非同期呼出し

利用者の操作やシステムからの通知をトリガーとして基盤に処理要求を行い、基盤側がバックグラウンドで処理を行う。大量のデータ分析や定期的なレポート生成など、即時応答を要しない処理を効率的に実行する。

(3) 既存システム組み込み

データ連携を用いて既存の業務システムから基盤を呼び出して、生成AIを活用した機能を後付けする。システム刷新を伴わず段階的にAI化を進められる。

4. 適用効果と今後の展望

本基盤の導入によって、生成AIを活用したアプリケーション開発では、開発者が社内認証との連携、データ連携、AIエージェント、ユーザーインターフェースと個別に設計・実装していた機能のうち、共通化可能な部分を基盤側で提供できるようになった。これによって、開発者はユーザーインターフェース開発やAIエージェントの選定・組合せ、AIエージェント以外の機能開発に専念しやすくなり、次の効果を見込む。

(1) PoC工数の短縮

AIエージェントの実現性や効果測定のためのPoC(Proof of Concept)に際して、認証連携・データ連携・AIエージェント設計・実装を開発工程から除外できるため、迅速に実施できる。

(2) 開発費の削減

共通エージェントの再利用によって、プロジェクト当たりの新規開発範囲をユーザーインターフェースや共通エージェント以外の設計・開発に集約できるため、開発作業の効率化が期待できる。

(3) 運用費の削減

共通エージェントの再利用では、監視やトレーサビリティの仕組みを基盤側に集約できるため、個別プロジェクトごとに運用する必要がなくなり、効率化が期待できる。

図3に本基盤の今後の展望を示す。本基盤を全社に展開した上で、各部門が生成AIアプリケーション開発を自走・量産できる仕組みの構築、生成AIリスク統制、共通エージェントの拡充を進めることで、利用容易性を高めて、活用の幅を広げていく計画である。

また、日々進化するAI技術をタイムリーに取り入れた最新のアーキテクチャーを全社に提供するため、本基盤のアーキテクチャーは適宜見直す計画である。

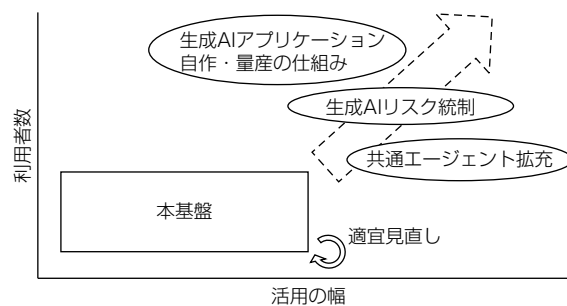


図3-本基盤の今後の展望

5. む す び

社内の複数プロジェクトで開発された質の高いAIエージェントを共通エージェントとして体系化・共通資産化し、社内の認証基盤と連携したセキュリティ・ガバナンスと、オープンな標準プロトコル(A2AやMCP)を採用することで、柔軟性を実現した本基盤の構築について述べた。本基盤は全社の業務プロセスや設計・製造業務の改革に活用しPoC立ち上げて、開発、運用の各段階の効率を図った。

今後は各部門の自走的なAI活用を支える共通基盤として、使用容易性の向上や活用の幅を広げる取組みを進めるとともに、日々進化するAI技術の動向を確認し、適宜アーキテクチャーを見直していく計画である。

参 考 文 献

- (1) A2A Protocol : Agent2Agent (A2A) Protocol (2026)
<https://a2a-protocol.org/>
- (2) Model Context Protocol : What is the Model Context Protocol (MCP)? (2026)
<https://modelcontextprotocol.io/>