

Microsoft Entra ID を活用した AI エージェント基盤で ハイパーパーソナライゼーションを実現 ～ゼロトラストと ID 管理で安全かつ高精度な顧客体験を提供～

AI ソリューション事業を手がける株式会社ヘッドウォーターズ（本社：東京都新宿区、代表取締役：篠田庸介、以下「ヘッドウォーターズ」）は、Microsoft Entra ID を活用したセキュアかつ高精度なハイパーパーソナライゼーション基盤を発表しました。

本ソリューションは、AI エージェントと生成 AI を組み合わせることで、「探して選ぶ」から「託して導かれる」体験への転換を実現します。さらに、Microsoft Entra ID による ID ベースのアクセス制御とゼロトラスト設計により、安全性とパーソナライズ精度の両立を可能にします。

これにより、AI エージェントのセキュリティおよび精度品質に懸念を持つエンタープライズ大手顧客への導入が可能となります。



■背景

従来のパーソナライズは、過去データに基づく静的な最適化にとどまり、リアルタイムな文脈理解や複雑な意思決定には対応できませんでした。

ヘッドウォータースは、ハイパーパーソナライズをテーマにした「AI Challenge Day」の受賞を契機に、マルチエージェント構成とナレッジグラフ、Generative UI を組み合わせることで、ユーザーごとに最適な提案を瞬時に生成するハイパーパーソナライゼーションをエンタープライズ顧客へ展開を開始しました。

通常のパーソナライズとハイパーパーソナライゼーションの違い

項目	通常のパーソナライズ	ハイパーパーソナライゼーション
データ利用	過去の購買履歴や属性情報	リアルタイム文脈+嗜好+外部データ
アルゴリズム	ルールベースや機械学習（クラスタリング、コンテンツベース）による柔軟性のないレコメンド	AI エージェント+生成 AI+ナレッジグラフ+RAG
応答速度	バッチ処理	リアルタイム応答
UI/UX	固定 UI	Generative UI で文脈に応じた UI 自動生成
精度の源泉	過去データの統計傾向	「今この瞬間」の意図を理解し、複数エージェントで最適解を導出



■ソリューションの特徴

1. Microsoft Entra ID による ID ファーストのセキュリティ。

- ・ユーザー属性を安全に参照し、パーソナライズに必要な情報を正確に取得。
- ・AI エージェントごとに「Microsoft Entra Agent ID」を発行し、RBAC と PIM で権限を厳格に管理。
- ・A2A 通信や MCP 連携をトークン認証で保護し、外部 API 接続時の秘密管理を強化。

2. ハイパーパーソナライゼーション基盤

- ・マルチエージェント構成（提案、検索、価格最適化、レビュー要約）。
- ・ナレッジグラフと RAG を組み合わせ、根拠付きの回答を生成。
- ・Generative UI により文脈に応じた UI を自動生成し、マルチモーダルに対応。

3. MCP 連携の安全性

- ・Microsoft Entra ID により、MCP プラグインの認証・認可を統合。
- ・条件付きアクセスにより、リスクベースの制御を実現。
- ・Azure Key Vault を活用し、API キーや証明書を安全に管理。

4. Microsoft の AI エージェント基盤との連携

- ・Azure AI Foundry を利用し、モデル選定から評価、デプロイ、運用、フィードバック、再評価・再選定の「Agent Ops」を実現。
- ・Microsoft Fabric をデータプラットフォームとして活用し、ナレッジや履歴データを統合・蓄積。AI エージェントの精度を継続的に向上。
- ・Microsoft Copilot Studio + Azure AI Agent Service を活用し、業務プロセスに最適化された AI エージェントを迅速に構築。



■業界別ユースケースと想定 ROI

金融

- ・銀行（BtoB）：RM 向け顧客対応 AI → 工数▲30～50%、年間数千万円削減
- ・銀行（BtoC）：資産運用アドバイス → 売上+5～15%、AUM 増加で数億円規模
- ・保険：代理店見積支援、請求体験最適化 → 請求不備▲20～30%、TAT 短縮
- ・証券：投資提案最適化 → 成約率+10%、収益寄与数%～十数%

モビリティ

- ・自動車（BtoB）：フリート管理 → 稼働率+3～5%、保守コスト▲10%、数千万円～億単位削減
- ・自動車（BtoC）：安全運転支援 → 事故率▲10～15%、LTV 向上
- ・鉄道：運行・保守最適化 → 遅延▲20%、保守工数▲15%、年間数億円削減

製造

- ・BtoB：工程最適化・異常検知 → 段取り時間▲30%、不良率▲10%、OEE 改善
- ・BtoC：操作支援・メンテナンスナビ → 自己解決率+50%、サポートコスト▲20%、売上+5～10%

リテール

- ・BtoB：店舗スタッフ支援（在庫・価格最適化） → 作業時間▲30%、在庫ロス▲15%
- ・BtoC：顧客向け接客・EC レコメンド → CVR+10%、平均購買単価+8%、売上+5～12%

■今後の展開

ヘッドウォータースは、本サービスを通じて大手企業における PoC やトライアル支援を開始し、スマートストアや XR への展開も進めてまいります。

また、Microsoft Entra ID に含まれる「Entra Agent ID」は、AI エージェントの ID 管理を標準化できる唯一のプラットフォームであると確信しており、Entra ID を組み合わせた新たな AI エージェントソリューションの展開を通じて、更なる他社差別化を図ってまいります。

以上

<用語解説>

・AI エージェント

AI エージェントとは、特定の目的や役割を持ち、ユーザーや他のシステムと自律的にやり取りしながらタスクを実行する AI プログラムです。AI エージェント市場は、CAGR 約 40～45% で急成長しており、特にエンタープライズ分野の導入が加速しています。Copilot や MCP などの標準化技術が、その普及を後押ししています。

- ・ Microsoft Entra ID

Microsoft のクラウド ID 管理サービス。ユーザーやアプリ、AI エージェントの認証・認可を一元管理し、ゼロトラストモデルを実現します。

ID・アクセス管理市場は年平均成長率（CAGR）約 12～15%で拡大中。

- ・ ゼロトラスト

「すべてのアクセスを信頼しない」前提で、ID・デバイス・リスクに基づき動的に認証・認可を行うセキュリティモデル。ゼロトラスト市場は CAGR 約 16.6～16.9%で成長中。

- ・ RBAC（Role-Based Access Control）

ユーザーやエージェントに役割（ロール）を割り当て、そのロールに応じてアクセス権限を制御する仕組み。RBAC 市場は CAGR 約 10～13%で成長中

- ・ PIM（Privileged Identity Management）

特権アカウントの権限を一時的に付与・管理する仕組み。不要な恒久権限を排除し、セキュリティを強化。PIM 市場は CAGR 約 13～24%で急成長中。

- ・ A2A 通信（Agent-to-Agent 通信）

複数の AI エージェント間でデータや指示をやり取りする通信。Entra ID のトークン認証で安全性を確保。エージェント AI セキュリティ市場は CAGR 約 33～41%で拡大中。

- ・ MCP（Model Context Protocol）

AI エージェントや外部ツール間で、コンテキスト情報を安全かつ標準化された形式でやり取りするための規格。Entra ID と組み合わせることで、認証・認可を統合し、A2A 通信のセキュリティを強化できます。MCP 市場は CAGR 約 35%で急成長中。エージェントエコシステムの拡大に伴い、MCP は「AI の USB-C」と呼ばれる標準化技術として注目されています。

- ・ Microsoft Copilot Studio

Microsoft の AI エージェント開発基盤。業務プロセスに合わせたカスタム Copilot を構築可能。

- ・ Azure AI Foundry

Microsoft Azure 上で AI モデルの選定・評価・デプロイを行うための統合プラットフォーム。

- ・ ハイパーパーソナライゼーション

リアルタイムの文脈や嗜好、外部データを組み合わせ、AI エージェントが一人ひとりに最適な提案を生成する高度なパーソナライズ。ハイパーパーソナライゼーション市場は CAGR 約 14～18%で成長中。

- ・ナレッジグラフ

データ間の関係性をグラフ構造で表現し、AI が文脈を理解するための基盤。ナレッジグラフ市場は CAGR 約 36.6%で急成長中。

- ・ RAG (Retrieval-Augmented Generation)

検索と生成 AI を組み合わせ、根拠付きの回答を生成する技術。RAG 市場は CAGR 約 49%で急成長。

- ・ Generative UI

ユーザーの状況やデバイスに応じて、AI が自動で UI (画面構成) を生成する仕組み。UI 自動生成は生成 AI 市場の一部として拡大中。

■ 参考

ヘッドウォータース、第 4 回「AI Challenge Day」で準グランプリを受賞 ～"探す"を託せるマルチエージェント型 EC アシスタントで、ハイパーパーソナライゼーションを実現 ～

https://www.headwaters.co.jp/news/4th_ai_challenge_day_runnerup.html

AI エージェントと業務データ連携で自律思考型 AI を可能にする 「Agentic RAG」サービス開始

https://www.headwaters.co.jp/news/hws_agentic_rag_service.html

Microsoft Azure で AI エージェントを検討している企業向けに「Azure AI Foundry Agent Service」ハンズオン型 AgentOps ラボサービス開始

https://www.headwaters.co.jp/news/azure_ai_foundry_agent_service_agentops_labo_service.html

AI エージェント基盤の導入や AI CoE を設置する Microsoft Azure、Microsoft 365 Copilot 利用企業向けに カスタム MCP サーバー導入ハンズオンラボサービスを開始

https://www.headwaters.co.jp/news/custom_mcp_server_implementation_hands_on%20_service.html

マイクロソフト ジャパン パートナー オブ ザ イヤー 2024 において 「AI イノベーション パートナー オブ ザ イヤー アワード」を受賞

https://www.headwaters.co.jp/news/microsoft_Japan_partner_year_award_2024.html

■ 商標について

Microsoft、Azure、Microsoft 365 は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。Microsoft 365 は、Microsoft Corporation が提供するサービスの名称です。その

他、記載されている製品名などの固有名詞は、各社の商標または登録商標です。

■会社情報

会社名：株式会社ヘッドウォータース

所在地：〒163-1304 東京都新宿区西新宿 6-5-1 新宿アイランドタワー 4 階

代表者：代表取締役 篠田 庸介

設 立：2005 年 11 月

URL : <https://www.headwaters.co.jp>

■本件のお問い合わせ先

株式会社ヘッドウォータース

メール：info@ml.headwaters.co.jp