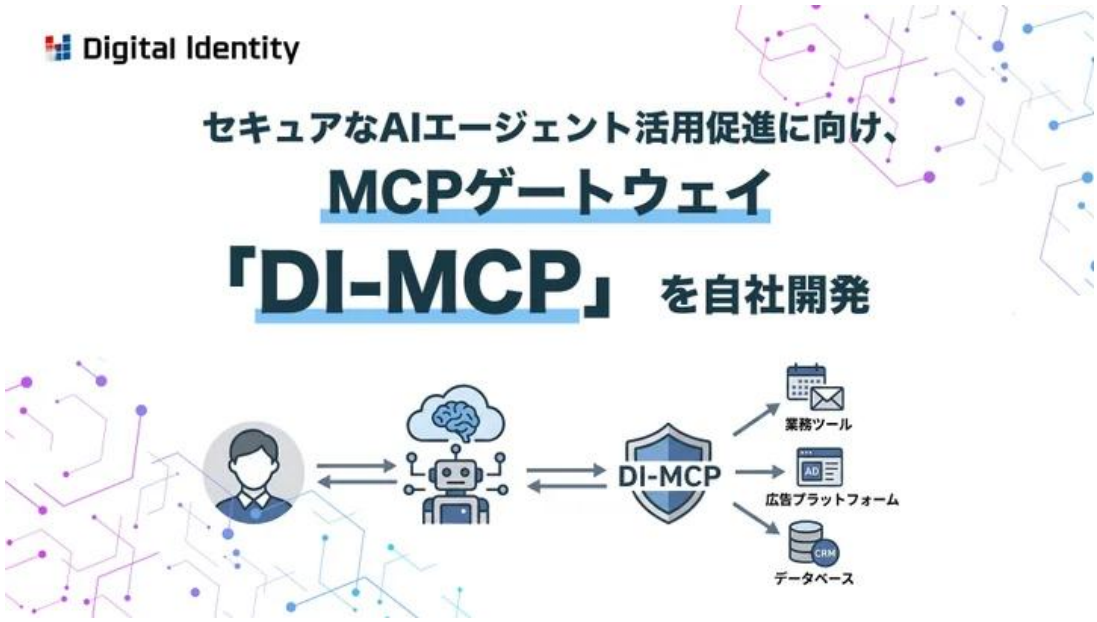
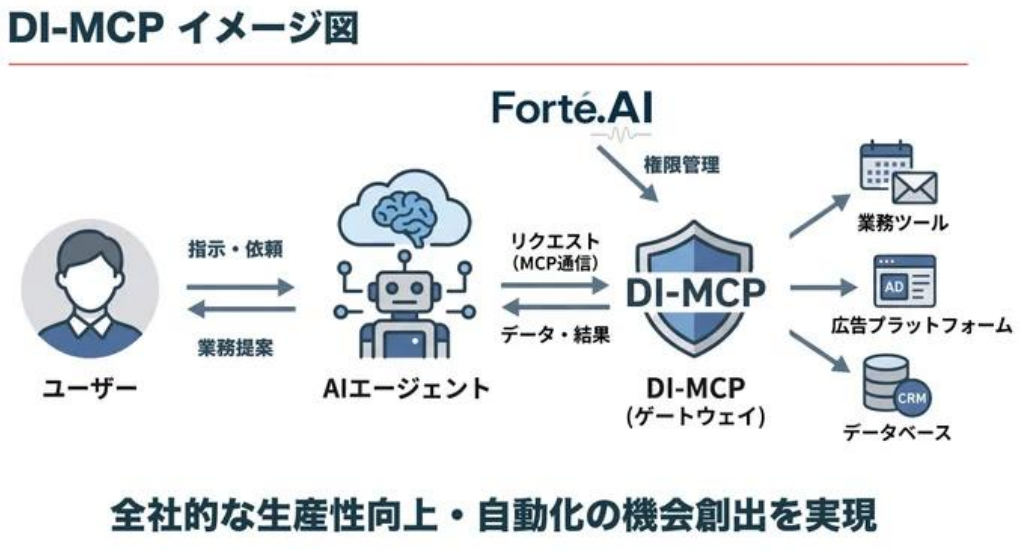
2026 年 5 月 27 日
株式会社 Orchestra Holdings
（証券コード：6533）

デジタルアイデンティティ、セキュアな AI エージェント活用促進に向け MCP ゲートウェイ「DI-MCP」を自社開発



株式会社 Orchestra Holdings（本社：東京都渋谷区、代表取締役社長：中村 慶郎）の子会社である株式会社デジタルアイデンティティ（本社：東京都渋谷区、代表取締役社長：鈴木 謙司、以下「デジタルアイデンティティ」）は、自社開発の AI プラットフォーム「Forté.AI（フォルテ・エーアイ）」の基盤拡張として、AI エージェントの安全な業務利用を実現する独自の MCP ゲートウェイ「DI-MCP」を開発し、社内運用を開始したことをお知らせいたします。

■ MCP ゲートウェイ「DI-MCP」について



MCP（Model Context Protocol）とは、AI エージェントが外部のツールやデータソースと安全に通信・操作を行うための標準プロトコルです。今回開発した「DI-MCP」は、この MCP 通信の中継システム（ゲートウェイ）として機能します。

AI エージェントから主要な業務ツールや外部サービスへの操作リクエストが発生した際、本システムがユーザーの権限情報と即座に照合し、実行の許可・拒否を安全にコントロールします。

本システムは当社の社内 AI プラットフォーム「Forté.AI」に組み込まれており、数百名規模の全社的な利用を想定したスケーラブルな設計となっています。

■　開発の背景・目的

近年、AI は単なるアシスタントの枠を超え、自ら各種ツールを操作して生産性を高める『自律型エージェント』として、本格的な業務への導入が進んでいます。

特にデジタルマーケティングの現場では、多岐にわたる広告プラットフォームの運用やデータ集計といったオペレーション負荷が高く、人間が戦略やクリエイティブに専念するため、AI エージェントによる業務の効率化が急務となっています。

しかし、マーケティング業務での AI エージェント活用ニーズが急増する一方で、実業務に導入するためには、以下のような課題が存在していました。

・本番環境への意図しない変更・削除などの実行リスク
・API キーなどの認証情報の配布に伴うセキュリティリスク
・AI エージェントに対するユーザーの認知不足に伴う活用範囲の限界

これらの壁をクリアし、安全かつ利便性の高い利用環境を構築することを目的に「DI-MCP」を自社開発いたしました。

■　実務に即した柔軟かつ厳格な権限管理

「DI-MCP」では、各種ツールにおける重要な操作を安全に実行するため、外部ツール全体に対する単純な「許可/拒否」ではなく、担当者やクライアント単位など、きめ細やかな権限設定を実現しています。
これにより「A 社の案件担当者のみ、A 社のレポート出力を実行できる」「管理者からのリクエストのみデータベースの更新を許可する」といった、セキュアな運用が可能となりました。

■　API キー・トークン等の安全な管理

従来の外部ツール連携では、担当者に API キーやトークンを直接配布・管理させる必要があり、これが大きなセキュリティリスクとなっていました。

「DI-MCP」では、システム側が認証情報と権限管理を一元化して仲介する仕組みを実装しています。
これにより、社員への直接的な API キーやトークンの配布が不要となり、情報漏洩や不正利用のリスクを軽減する運用体制を実現しています。

■　エージェントによる機能の把握と能動的な提案

「DI-MCP」の実装に伴い、AI エージェント自身が以下の項目を把握できるようになりました。

・利用可能な外部ツール・API
・利用可能な機能
・ユーザーの権限で実行可能範囲

これにより、AI はユーザーからの指示を待つだけにとどまらず、利用可能な機能等を利用者へ提案することが可能となりました。
エージェント自身がナビゲーターの役割を果たすことで、潜在的な自動化の機会を引き出し、業務効率化の効果を最大化します。

■　今後の展望

デジタルアイデンティティでは、「DI-MCP」を通じて連携可能な業務ツールや外部サービスを順次拡充し、対応領域を広げるとともに、エンジニア以外のあらゆる職種のメンバーが日常業務において安全に AI エージェントを活用できる環境を整備し、全社的な生産性向上を推進します。

さらに、本取り組みを通じて蓄積したエンタープライズ向けの権限モデルや運用体制に関する実践的な知見は、今後 AI エージェントの本格活用を検討する他企業様への情報発信や支援にも活かしていく予定です。

■株式会社 Orchestra Holdings
所在地:東京都渋谷区恵比寿四丁目 20 番 3 号
代表取締役社長：中村 慶郎
事業内容: グループ戦略の立案、実行および子会社経営管理
URL：https://orchestra-hd.co.jp/

■株式会社デジタルアイデンティティ
所在地：東京都渋谷区恵比寿南 1-15-1 A-PLACE 恵比寿南 5F
代表者：代表取締役社長　鈴木 謙司
事業内容：DX 支援、WEB サイト構築、MA、CRM、WEB 広告、SEO 等デジタルマーケティング事業全般
URL：https://digitalidentity.co.jp/

■本件に関するお問い合わせ
株式会社 Orchestra Holdings コーポレートマネジメント部門
E-mail：ir@orchestra-hd.co.jp