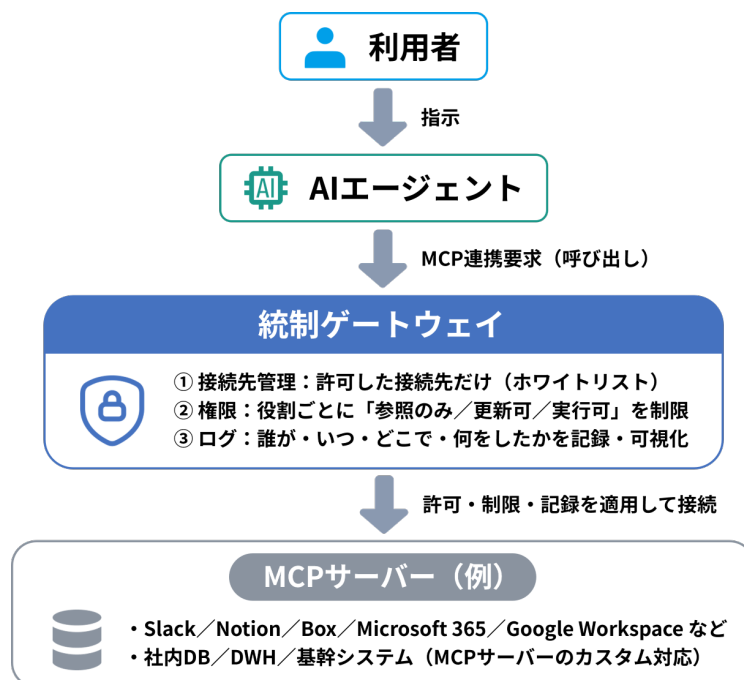


2026年4月9日

株式会社Hakuhodo DY ONE

Hakuhodo DY ONE、安全かつ管理可能な形で AI エージェントと業務システムをつなぐ MCP 導入支援を開始 ～セキュリティ・ガバナンス課題の解決に向け、設計・実装・運用を一貫サポート～

株式会社Hakuhodo DY ONE（本社：東京都港区、代表取締役社長：北爪宏彰、以下 Hakuhodo DY ONE）は、AIエージェントと外部データや業務システムを、「安全かつ管理可能な形でつなぐ」ためのMCP※¹導入支援を開始します。AIエージェントの業務適用が急速に進むなかで顕在化するセキュリティ・ガバナンス上の課題解決に向け、MCP導入を設計から実装・運用まで一貫してサポートし、企業のAI活用を推進してまいります。



■背景

生成AIの業務活用が拡大するなか、AIエージェントが外部データや業務システムと連携し、情報取得・更新・処理実行までを自律的に担うユースケースが増加傾向にあります。こうした連携を標準化するオープン規格としてMCPへの注目が高まり、Slack、Notion、BoxなどのSaaSのほか、社内データベースやDWHなどの業務システムとの接続を前提とした業務自動化の検討・導入が進んでいます。

一方で、MCPは接続を標準化する仕組みであり、接続先の管理、権限設定、ログ記録、認証といった機能を含みません。そのため、不審な接続先の混入、IT管理部門が把握しないデータアクセス、操

作ログの不足による原因特定の困難化など、新たなセキュリティ・ガバナンス上のリスクが顕在化しています。しかし、多くの企業ではこれらのリスクを十分に認識できておらず、適切な対策を講じられていないのが実情です。

Hakuhodo DY ONEは、博報堂D Yグループの横断的なAI専門家集団HCAI Professionalsの活動の一環として、2025年8月からAIエージェント型マーケティング支援サービス「ONE-AIGENT」※2を展開しています。そのなかで「AIエージェント構築支援サービス」を提供し、MCP導入に向けた技術支援・コンサルティングを推進しています※3。

今回、同サービスの強化として、MCPを用いたAIエージェント導入において「つなぐ」だけでなく、「安全かつ管理可能な形でつなぐ」ための設計・実装・運用を一貫してサポートします。これにより、企業はMCP導入に伴うセキュリティ・ガバナンス上のリスクを低減し、現業部門の利便性や業務効率化を進めながら、IT管理部門として必要な統制・監査・事故対応を両立できるようになります。Hakuhodo DY ONEは、広告・マーケティング領域でAIを業務に実装してきた知見をもとに、基盤の構築だけでなく、現場で運用できる権限設計、ルール整備、業務フローへの落とし込み、社内浸透・研修まで伴走し、AI活用を「ツール導入」で終わらせず、継続的な成果につなげます。

■概要

① 統制されたMCP連携設計

MCPでAIエージェントが複数の業務システムへアクセスできる前提のもと、企業のIT管理部門が求める要件（下記5点）を満たす全体設計と実装方針を提示します。

- 接続先のホワイトリスト管理

従業員が利用できるMCPサーバー（接続先）を部署・個人単位でカタログ化し、許可された接続先のみ利用可能にします。正規サービスを装った不審な接続先の混入や、従業員が独自に未許可のITツールを導入・利用することを抑制し、意図しない情報漏洩を防止します。

- 権限の設計

MCPサーバーが提供する機能やデータに対して、「参照のみ／更新可／実行可」といった操作範囲を、利用者の役割（部署・職種・担当業務）ごとに定義します。必要最小権限の範囲に絞ることで、権限の逸脱を防ぎます。

- 操作ログの記録・可視化

AIエージェントによるMCP呼び出しについて、「誰が・いつ・どの接続先で・何を実行したか」をログとして記録し、従業員別・接続先別の利用状況を把握できる形で可視化します。監査対応に加え、インシデント時の原因特定を容易にします。

- 異常検知とインシデント対応（兆候検知～通知・遮断）

通常時の利用状況を基準に、異常な呼び出し頻度、未許可機能へのアクセス試行、大量データ取得などを検知し、IT管理部門へ通知します。必要に応じてアラート発火時の自動遮断ルール設定にも対応します。

- 既存のID管理との連携

企業が利用する既存のID管理基盤と連携し、追加の認証負荷やID管理といった二重運用を抑えた形での導入を支援します。

② 基幹システム等のカスタムMCP対応支援

SaaS（Slack、Notion、Box等）との連携に加え、社内独自のデータベース、DWH、基幹システムについても、AIツールから安全にアクセス可能にするための対応を支援します。

■今後の展望

Hakuhodo DY ONE は現在、AI エージェントが業務システムと連携する際の「統制ゲートウェイ」となる基盤プロダクトの提供に向け、開発を進めています。今後は、コンサルティングとプロダクトの両輪で、企業の MCP 導入におけるセキュリティ・ガバナンス上の課題解決を支援し、将来的には業界標準となる支援モデルの確立を目指してまいります。

※1 MCP (Model Context Protocol) は、AIが外部のデータや業務システムと連携するための「接続方法」を標準化するオープン規格。
米Anthropic社が2024年11月に発表。

※2 「ONE-AIGENT」について：<https://www.hakuhodody-one.co.jp/service/one-aigent/>

※3 2025年8月7日Hakuhodo DY ONEリリース「Hakuhodo DY ONE、AIと外部システムを標準化する「Model Context Protocol(MCP)」
導入支援サービスを提供開始～AIエージェント構築ための技術支援・コンサルティングを推進～」
https://www.hakuhodody-one.co.jp/news/news-release_202508072729/

以上

<会社概要>

■株式会社Hakuhodo DY ONE <https://www.hakuhodody-one.co.jp>

Hakuhodo DY ONEは、インターネット広告黎明期より培ったデジタル広告の知見とノウハウを活かし、統合的なデジタルマーケティングサービスを提供しています。マーケティング戦略立案力、クリエイティビティ、高度な運用力と技術開発力、媒体社・プラットフォームとの強固な関係性を強みとし、国内外のクライアント企業に対して、デジタル起点でのマーケティング戦略やテクノロジー活用を包括的に支援します。

博報堂DYグループの「デジタルコア」として、グループ内のナレッジやリソースを集約し、高い専門性と提案力を併せ持つ企業として業界随一のデジタルマーケティング事業会社となることを目指します。

クライアント企業にとって唯一の「ONE」の存在となるため常に挑戦・前進し、事業成長を支援するビジネスパートナーとして伴走することで、クライアント企業の持続的な成長と、企業価値向上に貢献してまいります。

本社所在地：〒107-6316 東京都港区赤坂5丁目3-1 赤坂Bizタワー

代表者：代表取締役社長 北爪宏彰

株主：博報堂DYグループ100%

社員数：3,172名（2025年4月1日時点）

創立：2024年4月1日

事業内容：デジタルマーケティング全般にまつわる企画・コンサルティング・代行事業・投資事業

【本件についてのお問い合わせ】

株式会社Hakuhodo DY ONE

広報担当 E-mail：info-pr@hakuhodody-one.co.jp