お知らせ

2026 年 11 月 6 日

日立、Kong 社との協業により、AI エージェント連携ソリューションを拡充

増え続ける AI エージェントの多様な接続先を、安全かつ一元的に統制

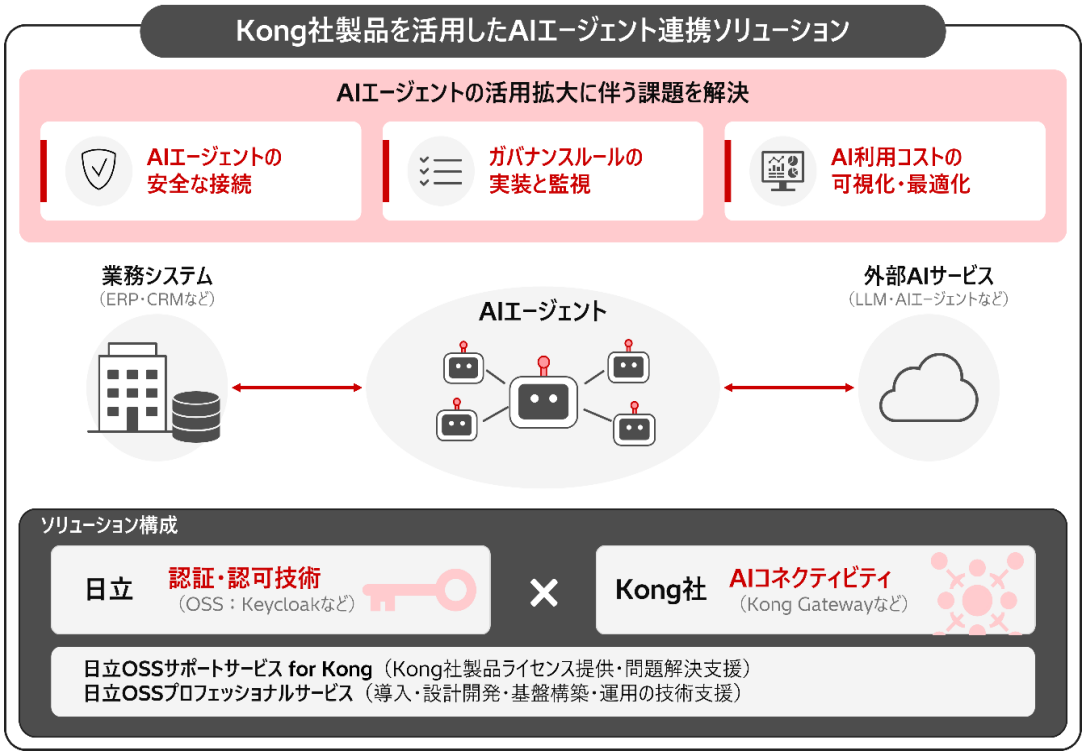


図 1｜Kong 社製品を活用した AI エージェント連携ソリューションの概要

株式会社日立製作所(以下、日立)は、このたび、AI コネクティビティ技術を提供する Kong 株式会社(以下、Kong 社)との協業をもとに、安全で統制された AI 連携基盤を実現する「AI エージェント連携ソリューション」を拡充し、提供を開始しました。本ソリューションは、AI エージェントの活用拡大に伴い課題となる、アクセス制御、ガバナンス、コスト管理を一元化するものです。具体的には、日立が技術や知見を活用してきた Keycloak[*1] などと、Kong 社の API・AI ゲートウェイ関連製品を組み合わせることで、増え続ける AI エージェントと業務システムや外部 AI サービスなどの多様な接続を、安全かつ一元的に統制することができます。あわせて、Kong 社製品のサブスクリプションライセンス提供およびワンストップ窓口で問題解決を支援する「日立 OSS サポートサービス for Kong」も提供開始します。また、既存の「日立 OSS プロフェッショナルサービス」を拡充し、Keycloak など本ソリューションを構成する他の製品を含め、導入・設計・構築から運用までの技術支援を行います。これらにより、企業における AI エージェントの活用拡大や、検証段階から実運用への移行などを支援します。

*1 ID 管理やアクセス管理(IAM: Identity and Access Management)を実現する OSS

近年、企業における AI エージェントの活用は、さまざまな業種・業務へと急速に広がっています。それに伴い、AI エージェント同士や、AI エージェントと業務システムや外部サービスとの接続が増加し、認証・認可といったアクセス制御に加え、ガバナンスルールの管理や利用状況の把握といった課題が顕在化しています。こうした中、AI エージェントを安全かつ効率的に活用するために、API や AI サービスへの接続・管理を担うゲートウェイの重要性が高まっています。

日立は、これまでも、OSS コミュニティにおいて Keycloak の主要機能の開発にメンテナとして携わるとともに、The Linux

Foundation 傘下で Agentic AI の透明性と標準化を推進する「Agentic AI Foundation(以下、AAIF)」[*2]において、MCP (Model Context Protocol)や A2A (Agent-to-Agent Protocol)など AI エージェントの相互運用を支える仕様策定や実装に貢献[*3]してきました。今回、こうした認証・認可技術や AI エージェント連携に関する技術・知見と Kong 社の API・AI ゲートウェイ関連製品を組み合わせ、「AI エージェント連携ソリューション」を拡充しました。

*2 お知らせ "日立、日本企業で初めて Agentic AI Foundation に加入し、AI のアクセス権限管理の標準化を支援" (2026.3.10)
*3 お知らせ "日立の社員が、初代 Agentic AI Foundation アンバサダーに就任し、日本初開催「AGNTCon + MCPCon Japan 2026」でキーノート登壇" (2026.8.24)

日立は、「AI エージェント連携ソリューション」を、現場の暗黙知やデータを統合する「HMAX Data Fabric」や AI の安全な自律運用を支える「HMAX AI Operations」の関連サービスとして、AI 活用基盤の安全性と効率性の向上などに活用していく予定です。

Kong 社製品を活用した AI エージェント連携ソリューションの特長

1. AI エージェントと業務システムや外部 AI サービスを安全につなぐ認証・認可基盤

AI エージェントと各種サービスをつなぐ Kong 社の API・AI ゲートウェイ関連製品と、Keycloak を組み合わせることで、MCP および OAuth[*4] に対応し、既存の認証基盤やバックエンド認可サーバーと連携できます。これにより、AI エージェントに作業を依頼した利用者が本来もつ権限の範囲内、かつ、AI エージェントの役割に応じたアクセス制御を実現します。これにより、AI が過剰な権限を持つことを防ぎ、企業内の AI エージェントを安全に活用できる連携基盤を実現します。また、AI エージェント同士や AI エージェントとサービス間の接続を標準化することで、新たな AI エージェントやサービスの追加・拡張を容易にします。

2. AI エージェントのガバナンスを一元管理し、開発運用の品質向上とエンジニアの負荷軽減を実現

Kong 社の API・AI ゲートウェイに、認証、プロンプトガード[*5]、PII サニタイズ[*6]などの各種ポリシーを適用することで、AI エージェントごとの開発を最小限におさえながら、ガバナンスルールを一元管理できます。マルチクラウドやオンプレミス、エッジなどが混在する環境でも、API や AI エージェントを一貫したルールのもとで管理でき、部門や拠点をまたいで再利用を容易にします。これにより、API や AI エージェントのガバナンスに関する開発運用プロセスの効率化と自動化を促進できるため、開発運用の品質向上とエンジニアの負荷軽減ができます。

3. AI 利用状況の可視化やトークン量の抑制などにより、AI 利用コストを最適化

Kong 社の API・AI ゲートウェイ関連製品を活用することで、AI エージェントや LLM の利用状況、トークン数、レイテンシ[*7]、コストを可視化できます。また、プロンプト圧縮によるトークン数の削減や、セマンティックキャッシュ[*8]の活用により LLM へのリクエスト回数を減らして AI 利用コストを削減するとともに応答の高速化を実現します。さらに、用途とコストに応じて適切な LLM への自動的な振り分け、レート制限[*9]やヘルスチェック[*10]により、想定外の利用を抑止します。例えば、あらかじめ設定したトークン量やコストに達した際に、自動的にリクエストを停止・制限します。これらにより、AI 利用コストを最適化します。

*4 OAuth (Open Authorization)：ユーザーID やパスワードを開示せず、特定のリソースへのアクセス権限だけを委譲する標準的な認可(Authorization)フレームワーク
*5 プロンプトガード：不適切なプロンプトや機密情報の入力を検知し、AI への送信を制御すること
*6 PII サニタイズ：テキストやデータから個人を特定できる情報である PII (Personally Identifiable Information)を検出し、削除・マスキング・匿名化する処理
*7 レイテンシ：データの送受信や処理にかかる時間的な遅れ
*8 セマンティックキャッシュ：意味が似た過去の質問と回答を再利用し、AI の応答速度向上とコスト削減を実現する仕組み
*9 レート制限：一定時間内に利用できるリクエスト数を制限し、過剰利用やシステム負荷の増大を防ぐこと
*10 ヘルスチェック：LLM などの接続先が正常に稼働しているかを確認すること

Kong 社との協業について

日立は、Kong 社との技術検証やお客さまへの共同提案を進め、今回拡充した AI エージェント連携ソリューションを、金融・製造分野を中心に展開します。AI エージェントと既存の業務システムやサービスとの安全な接続・管理を通じて、AI 活用の検証段階から実運用への移行を支援します。高い信頼性や厳格なデータ管理が求められる金融分野では、既存の基幹システムや業務アプリケーションと AI サービスを接続する際の API 管理とガバナンス強化に貢献します。また、製造分野では、設備やセンサーから得られる現場データ、業務システム、AI サービスを接続し、フィジカル AI の活用および実装を支えるデジタル基盤の整備を推進します。

関連サイト

・Kong 社製品を活用した AI エージェント連携ソリューション
http://www.hitachi.co.jp/products/it/harmonious/cloud/service/kong/?ni=261106
・日立の OSS サポートサービス for Kong
https://www.hitachi.co.jp/products/it/oss/solution/kong/?ni=261106
・Hitachi OSPO
https://www.hitachi.co.jp/products/it/oss/ospo/?ni=261106
・HMAX Data Fabric・HMAX AI Operations
https://www.hitachi.com/ja-jp/products/digital/data-fabric-operations/?ni=261106

商標注記

記載の会社名、組織名、製品名などは、それぞれの会社、組織の登録商標もしくは商標です。

お問い合わせ先

株式会社日立製作所 AI＆ソフトウェアサービスビジネスユニット マネージド＆プラットフォームサービス事業部
お問い合わせフォーム：https://www.hitachi.co.jp/it-pf/inq/NR/

以上