お知らせ

HITACHI

2026 年 3 月 10 日

# 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

## 活動成果を HMAX に生かし安全な社会インフラの効率的な実現に貢献

株式会社日立製作所(以下、日立)はこのたび、日本企業で初めて、The Linux Foundation 傘下で、Agentic AI の透明性・標準化を推進する中立的な組織である「Agentic AI Foundation(以下、AAIF)[*1]」にゴールドメンバーとして加入しました。日立は、AAIF の中核プロジェクトである Model Context Protocol(以下、MCP)[*2] などの活動に参画し、AI エージェントがデータやアプリなどへアクセスする際の権限管理の標準化と実用化を支援していきます。これにより、世界中のメンバー企業・団体とともに社会課題を解決するイノベーションを推進します。また、日立が AI で社会インフラを革新する次世代ソリューション群「HMAX by Hitachi」(以下、HMAX)*[3] においても、この活動の成果を生かし、安全な社会インフラの効率的な実現に貢献していきます。

これまで日立は、Keycloak プロジェクト*[4] に参画し、AI エージェントが連携する環境での複雑なデータアクセスの認証・認可を MCP などのオープン・プロトコルにより統一的に管理・制御し、標準化や実用化を推進してきました。今回、AAIF の活動へ参画することで、進化の目覚ましい AI において、意図しないデータ流出や、AI エージェントの認証情報の改ざんといった、セキュリティリスクを防止するアクセス権限の管理や認証・認可を継続的に発展させていきます。

日立の HMAX はフィジカル・デジタル両方のアセットから得られる膨大なデータを活用し、フィジカル AI や Agentic AI などの先進的な技術を日立ならではの深いドメインナレッジで強化するとともに、各業界をリードするパートナーと連携し、社会インフラの複雑な課題を解決していきます。課題解決に向け、AI による現場レベルから経営レベルの複雑な判断の自動化といった変革を、パートナーとともに推進するためには、AI のアクセス権限管理の共通ルールに基づく安全性の確保が必要となります。その実現のために、日立は AAIF で AI のアクセス権限管理や認証・認可の規格や仕様の標準化を推進し、世界中のパートナーと連携して安全な AI 活用のユースケースを拡充していきます。

今後も日立は、これらの活動を通じ、AI がもたらす価値を誰もが安全に享受できる社会の実現に貢献していきます。

*1 詳細はこちらを参照ください。https://aaif.io/

*2 LLM アプリと外部のデータソース/ツールを標準的に接続するためのオープン・プロトコル

*3 ニュースリリース “日立、グローバルであらゆる業界に向けて HMAX を展開し社会イノベーションを加速” (2026.1.6)

*4 セキュリティ標準プロトコルに基づき構築された、アプリケーションやサービス向けのオープンソースの ID・アクセス管理を実現する OSS で、CNCF (Cloud Native Computing Foundation)傘下のプロジェクト

## Jim Zemlin 氏(Executive Director and CEO of the Linux Foundation)コメント

日立のオープンソースへの継続的な取り組みと貢献は、重要かつ最良な社会インフラが協力によってこそ構築されることを示唆しています。Agentic AI Foundation のゴールドメンバーとして日立を迎えられることを大変嬉しく思います。

## 関連サイト

・日立 OSPO について
https://www.hitachi.co.jp/products/it/oss/ospo/index.html
・日立の OSS(オープンソース・ソフトウェア)について
https://www.hitachi.co.jp/products/it/oss/index.html
・HMAX について
https://www.hitachi.co.jp/products/it/lumada/hmax/index.html

## 商標注記

記載の組織名、製品名などは、それぞれの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
お問い合わせフォーム：https://www.hitachi.co.jp/it-pf/inq/NR/

以上