2026 年 8 月 7 日
株式会社ヘッドウォータース
(コード番号：4011 東証グロース)

AI エージェント時代のサイバー防御を自律化、「Agentic Security」市場へ参入

～企業の AI 本番活用を支える新たなセキュリティ運用基盤を構築～

AI プラットフォーム事業を手がける株式会社ヘッドウォータース（本社：東京都新宿区、代表取締役：篠田庸介、以下「ヘッドウォータース」）は、AI エージェント時代における新たなセキュリティ需要を見据え、「Agentic Security」市場へ参入します。



生成 AI や AI エージェントの活用は、情報検索や文章生成にとどまらず、企業データや業務システムへアクセスし、外部サービスと連携しながら、判断・実行を伴う業務へ広がりつつあります。一方で、AI が自律的に動作する領域が拡大するほど、ID、権限、データ接続、実行履歴をどのように把握・統制するかが、企業の AI 本番活用における重要な課題となります。

ヘッドウォータースは、AI エージェントが利用する ID、権限、データ接続、実行履歴を継続的に把握・保護しながら、セキュリティ運用そのものにも AI エージェントを活用する「Agentic Security」により、企業が AI を安全に本番活用できる環境の実現を目指します。

■ AI エージェントの本番活用拡大が生む新たなセキュリティ需要

AI エージェント市場は、世界・日本ともに 2033 年に向けて高い成長が見込まれており、世界市場では年平均 49.6%、日本市場では年平均 49.9%の成長が予測されています。［1］［2］

企業における AI 活用も、実証実験や業務効率化の段階から、AI エージェントを業務プロセスやシステムへ組み込む本番活用の段階へ移行しつつあります。Microsoft の「2025 Work Trend Index Annual Report」でも、経営層の 81%が今後 12 カ月から 18 カ月以内に AI エージェントが自社の AI 戦略へ一定以上組み込まれると回答しています。［3］
一方で、AI エージェントの導入拡大に伴い、ID、権限、データ接続、実行履歴を継続的に把握・統制する必要性も高まっています。Okta の調査では、69%がセキュリティ上の懸念によって AI エージェントの導入が遅れていると回答しています。［4］
国内サイバーセキュリティ市場も 2026 年度に 2 兆 1,220 億円へ拡大すると予測されており、AI エージェントとセキュリティ運用が重なる領域には、新たな需要が生まれています。［5］

ヘッドウォータースは、この領域を「Agentic Security」と位置付け、AI エージェント時代における企業の安全な AI 本番活用を支援してまいります。
※約 2 兆円という数値は国内サイバーセキュリティ市場全体の規模であり、Agentic Security 単独の市場規模を示すものではありません。

■ **Agentic Security が企業にもたらす価値**

Agentic Security は、AI の利用を制限するための仕組みではなく、企業が AI を安全に本番活用するためのセキュリティ運用基盤です。
ヘッドウォータースは、AI エージェントの利用拡大に伴って増加する ID、権限、データ接続、実行履歴を継続的に把握し、脅威の検知、影響分析、対処、検証までを一連の運用サイクルとして高度化します。

これにより、企業はリスクの低い処理を自動化しながら、業務への影響が大きい処理や重要な判断については、人による承認へ切り替えることが可能になります。AI 活用を止めるのではなく、統制を維持しながら本番展開を広げられることが、Agentic Security の重要な価値です。

また、セキュリティ運用で得られたリスク判断、対処手順、承認条件、検証方法などを標準化し、企業内で再利用可能な知識として蓄積します。これにより、属人化していたセキュリティ運用の知見を、組織全体で活用できる資産へと転換します。

■ **Agentic Security を実現する「Agentic Security Harness」**

ヘッドウォータースは、Agentic Security を実現するためのアーキテクチャとして「Agentic Security Harness」を位置付けています。
Agentic Security Harness は、AI エージェント、既存のセキュリティ製品、企業固有の業務ルール、人による承認を連携させ、脅威の検知、影響分析、対処、検証を一連のセキュリティ運用サイクルとして機能させる仕組みです。

単一の AI モデルや製品にセキュリティ対応を委ねるのではなく、企業ごとに異なる業務、データ、権限、リスク許容度に応じて、どこまで AI に任せ、どの条件で処理を停止し、どの判断を人へ戻すかを設計します。
これにより、既存のセキュリティ製品や専門人材を置き換えるのではなく、それらを活かしながら、AI エージェント時代に求められるセキュリティ運用を高度化します。

■ **セキュリティ運用知識を企業 OS へ蓄積し、継続的に再利用**

本リリースにおける「企業 OS」とは、一般的なコンピューターの基本ソフトウェアではなく、企業活動に必要な業務知識、判断基準、権限、データ、AI を、組織横断で再利用可能にする知識・実行基盤を意味します。
Agentic Security は、導入時に一度だけ安全性を確認して完了する取り組みではありません。AI エージェントが追加され、利用するモデル、アクセスするデータ、外部サービスとの接続、付与される権限が変わるたびに、保護対象とリスクも変化します。また、攻撃手法や脆弱性、企業内のセキュリティポリシーも継続的に変化します。

ヘッドウォータースは、Agentic Security の運用から得られた脅威の検知方法、リスクの判定基準、自動対処の範囲、人へ承認を求める条件、対処後の検証方法などを、再利用可能なスキル、ルール、テンプレートとして標準化し、企業 OS へ蓄積します。
これにより、特定の担当者や個別プロジェクトに閉じていたセキュリティ運用知識を組織資産へ変換し、顧客企業内の他部門、グループ会社、別業務への横展開を可能にします。
また、案件ごとに得られたセキュリティ運用知識を標準資産として再利用することで、新たな環境への導入期間と個別開発工数を段階的に削減し、案件を重ねるほど展開速度と対応力を高められる事業モデルを目指します。

■ **将来的にデジタルから Physical AI へ保護領域を拡張**

AI の活動領域は、企業データや業務システムにとどまりません。今後、ロボット、車両、製造設備、カメラ、センサー、エッジデバイスなどと接続し、AI の判断が物理的な動作へ反映される Physical AI の普及が見込まれます。
デジタル領域における誤った判断は、情報漏えいや不正アクセス、業務処理の誤りにつながります。一方、Physical AI における誤判断や不正な指示は、設備停止、製品不良、事故、事業継続への影響など、物理的な損失へ発展する可能性があります。

ヘッドウォータースは、Physical AI Harness で進めてきた実行前制御の考え方を Agentic Security へ接続します。AI の判断を物理的な動作へ移す前に、安全条件や設備の状態、業務ルールに照らして評価し、必要に応じて動作を停止または人へ判断を戻せる仕組みへ発展させます。

これにより、企業が AI による自動化の範囲を、デジタル空間から物理空間へ安心して拡大できる環境を目指します。

■ **今後について**

ヘッドウォーターズは、まず企業内のデータ、ID、権限、コード、業務システムを対象に、Agentic Security に関する技術検証と顧客企業とのユースケース創出を進めます。
あわせて、運用から得られるセキュリティ運用知識を企業 OS へ蓄積・標準化し、再利用可能な AI エージェント、スキル、判断ルール、承認フロー、テンプレートとして継続的に拡充していきます。
将来的には、ロボット、車両、製造設備、センサー、エッジ AI などと接続し、AI による判断を物理的な動作へ移す前に、実行、停止、人への確認を制御する Physical AI 領域への展開も視野に入れています。

ヘッドウォーターズは、AI の利用を制限して安全性を確保するのではなく、AI エージェントの増加と活動領域の拡大にセキュリティ対応力を追随させることで、企業が AI を安心して本番環境へ展開できる状態の実現に取り組んでまいります。

以上

■ **データ参照元**

［1］Grand View Research : AI Agents Market Size, Share & Trends Analysis Report
［2］Grand View Research : Japan AI Agents Market Size & Outlook
［3］Microsoft : 2025 Work Trend Index Annual Report
［4］Okta : Survey - AI agent security is now a priority for enterprise buyers
［5］矢野経済研究所：サイバーセキュリティ市場に関する調査を実施（2026 年）

■ **参考情報**

- マイクロソフトの上位パートナー認定資格「Accelerate Developer Productivity with Microsoft Azure Specialization」を取得
  https://www.headwaters.co.jp/news/accelerate_developer_productivity_with_microsoft_azure_specialization.html
- ヘッドウォーターズ、GitHub 認定パートナーとして「Agentic DevOps ソリューション」の提供を開始
  https://www.headwaters.co.jp/news/github_partner_agenticdevops.html
- ヘッドウォーターズ、「NVIDIA Omniverse Partner Council Japan」に参画
  https://www.headwaters.co.jp/news/nvidia_omniverse_partner_council_japan.html

■ **商標について**

Microsoft、Azure およびその他の Microsoft 製品・サービス名は、Microsoft Corporation の米国およびその他の国における商標または登録商標です。

GitHub は、GitHub, Inc.の米国およびその他の国における商標または登録商標です。

NVIDIA、NVIDIA Omniverse およびその他の NVIDIA 製品・サービス名は、NVIDIA Corporation の米国およびその他の国における商標または登録商標です。

その他、記載されている会社名、製品名およびサービス名は、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