2026 年 11 月 16 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)

守りの知見を、AI の戦力へ。セキュリティのライフサイクル全体をつなぎ、AI エージェントの活用で企業のサイバーレジリエンス強化を支援する「Agentic Security Lifecycle Resilience」を提供開始

～組織の判断基準と検証・運用の知見を AI ハーネスへ反映し、AI エージェントが担う防御業務を拡大～

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」）と株式会社ヘッドウォータースコンサルティング（本社：東京都新宿区、代表取締役：加藤 健司、以下「ヘッドウォータースコンサルティング」）は、企業の AI 活用・DX 推進を安全に支え、サイバーレジリエンスの強化につなげるセキュリティサービス「Agentic Security Lifecycle Resilience（エージェンティック・セキュリティ・ライフサイクル・レジリエンス）」の提供を開始しました。サイバーレジリエンスとは、備え・防御・対応・改善を重ね、変化する脅威に対処しながら事業を継続できる状態を指します。



本サービスは、AI システムと、それを支える業務システム、クラウド環境、データ、組織・運用体制を対象に、戦略・ガバナンスから設計・開発、診断・攻撃検証、監視・運用、インシデント対応まで、セキュリティのライフサイクル全体を一貫して支援します。組織づくり、検証、運用で得た知見を「セキュリティ AI ハーネス」の判断ルール・対応手順・システム連携へ反映し、検証と改善を重ねながら、AI エージェントが実務を担う防御体制へ段階的に発展させることを目指します。

サイバーセキュリティ CoE、セキュリティ AI ハーネス、攻防一体のセキュリティエンジニアリングを、相互に強化する 3 本柱として提供します。

■ 背景：変化し続ける脅威には、継続的な対策が必要

情報漏洩や事業停止につながるサイバー攻撃への対応が問われるなか、AI は攻撃の速度・規模を変え、脆弱性の発見も加速させています。Microsoft の「Digital Defense Report 2026」は、攻撃に要する時間の短縮と、報告される脆弱性の増加を指摘しています。また、米国 CISA は、実際に悪用された脆弱性の情報を継続的に更新し、対策の優先順位付けへの活用を推奨しています。［1］［2］

AI エージェントの業務利用では、接続先やデータへのアクセス、実行権限、責任者を管理する必要があります。［3］両社は、攻撃の入口を特定の領域に限定せず、システムやデータ、ID、AI の利用、組織・運用、取引先との接点までを横断して対策を考えることが重要と捉えています。一度の診断や製品導入で対策を終わらせず、リスクの把握、優先順位付け、改修、再検証を繰り返すことで、防御の抜け漏れを減らす取り組みを支援します。

両社は、継続的な対策を担当者の増員や手作業だけで維持するのではなく、AI エージェントが防御の実務を担う仕組みを育てることを重視します。専門家の判断や検証で得た知見をルール・手順・連携に落とし込み、AI に任せられる業務を拡大します。人が重要な判断に集中しつつ、限られた人員でも対策を続けられる状態を目指します。

■ 本サービスが提供する価値

1. 人と AI で機能する推進組織をつくる「サイバーセキュリティ CoE」

セキュリティ対策室などの新設や既存体制の強化に向け、「サイバーセキュリティ CoE（組織横断でセキュリティ方針・標準・人材・運用を統括する中核組織）」の設計・立ち上げから運用の定着までを支援します。方針・責任・判断経路・全社標準を整え、人と AI の役割、AI に任せる業務、人が承認する操作を明確にします。組織の判断基準をセキュリティ AI ハーネスの権限・承認フローへ落とし込み、実務を通じて見直すことで、組織と防御の仕組みをともに育てます。

取引先のセキュリティ対策状況の確認や、取引先から求められるセキュリティチェックへの対応を支援します。SCS 評価制度（取引先を含むサプライチェーンのセキュリティ対策を評価する制度）の要求事項に照らした現状整理から、不足対策の実装、規程・委託先管理ルールの策定・改定、運用記録の整備までをつなげます。

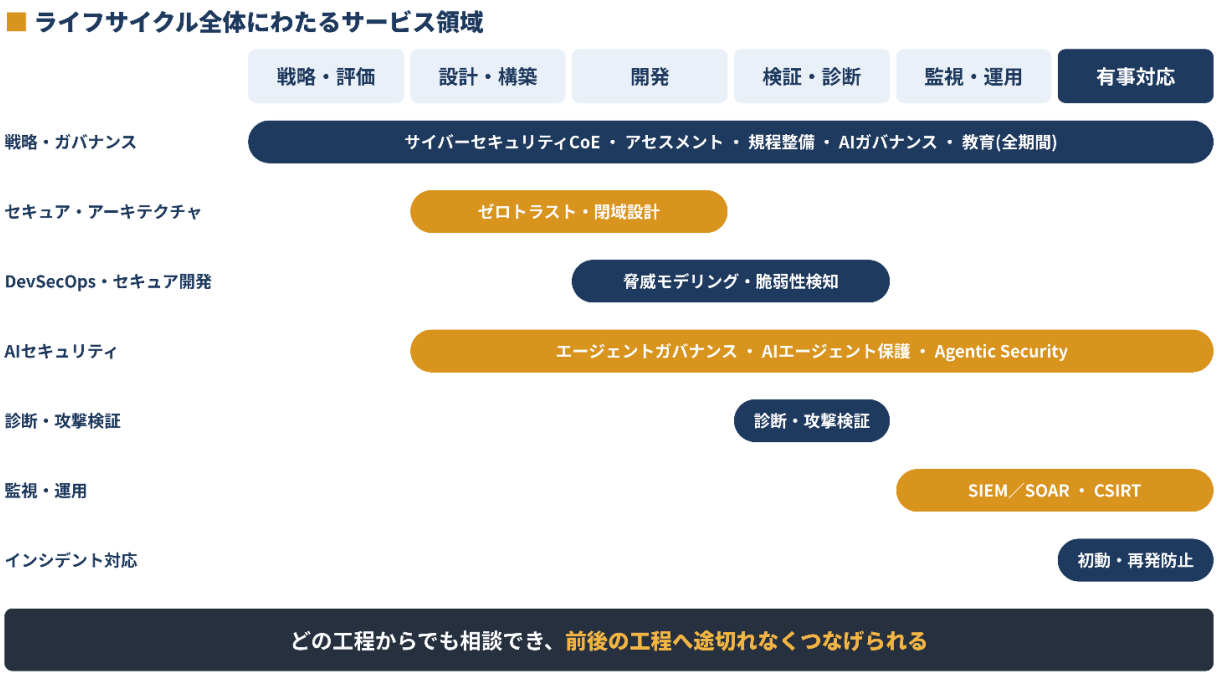
2. 知見を蓄積し、AI が担う防御業務を広げる「セキュリティ AI ハーネス」

AI エージェント、既存のセキュリティ製品、業務ルール、人による承認をつなぐ「セキュリティ AI

ハーネス」を設計・構築します。情報収集、一次分析、調査支援、承認済みの対処などを対象に、検証・運用で得た知見を判断ルールや対応手順、連携処理へ継続的に反映します。安全性と有効性を確認しながら AI が担う業務を段階的に広げ、人員増だけに頼らない防御の実行力を育てます。

3. **攻撃検証を改修・再検証までつなぐ「攻防一体のセキュリティエンジニアリング」**
   脆弱性診断、ペネトレーションテスト、レッドチーム演習、LLM／AI レッドチーミングによる検証を、指摘事項の報告だけで終わらせません。システム改修、権限・接続の見直し、検知・対処ルールの改善、再検証までを一体で進めます。検証や有事対応で得た知見を設計・開発標準とセキュリティ AI ハーネスへ反映し、システムの安全性と、AI が担う防御業務の質を継続的に高めることを目指します。

■ ライフサイクルを支える取り組み



セキュリティ・バイ・デザインで、設計・開発と運用をつなぐ

ゼロトラストの考え方に基づく認証・認可、ネットワーク・閉域設計、API セキュリティ、鍵・秘密情報管理などを通じて、設計段階から対策を組み込む「セキュリティ・バイ・デザイン」を支援します。DevSecOps では、脅威モデリングやコード・依存関係の脆弱性検知、開発・リリース環境の権限統制を開発プロセスに組み込みます。さらに、SIEM（セキュリティログの統合・分析）や SOAR（セキュリティ対応の連携・自動化）を活用した監視・対処へ接続し、検証や運用で得た知見を設計・開発標準に取り込みます。Microsoft 基盤を中心とした技術実装の知見を生かし、顧客の既存環境や運用ルールに合わせて設計・構築します。

エージェントを統制し、人と AI による継続防御を支える

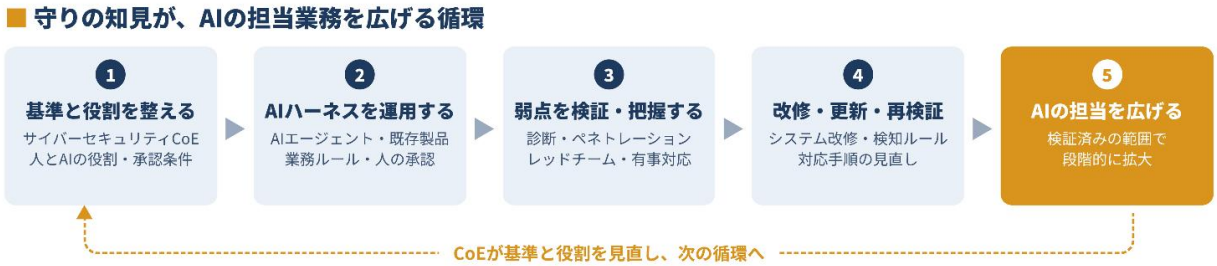
「エージェントガバナンス」では、AI エージェントごとの ID・責任者・接続先を明確にし、最小権限、

データ保護、操作履歴の追跡を設計します。登録から稼働中の監視、権限の見直し、停止・廃止までを管理対象とし、利用拡大に伴う統制を支援します。

「Agentic Security」では、攻撃者視点の検証と防御側の検知・調査・対処をつなぎ、その結果をルールや手順の改善へ反映します。

既知のパターンに該当する事象には、事前に承認された手順・権限の範囲で AI エージェントが対処し、業務への影響が見込まれる場合は人の承認を得て実行します。権限の逸脱や高リスクの事象を検知した場合は、AI エージェントによる処理を停止し、担当者へ通知します。

人と AI エージェントが協働するセキュリティ運用モデル「Agentic SOC」では、CoE で定めた役割・承認条件に基づいて運用します。人の業務を一律に置き換えるのではなく、安全性と有効性を検証できた業務から AI エージェントの活用範囲を広げ、判断と実行の経緯を追跡可能にします。





※運用のイメージです。検証結果は、判断ルールと対応手順の更新に反映します。

■ 主なサービス領域

各サービスは、顧客の課題・目的、既存環境、対策の優先順位に応じて組み合わせて提供します。

領域	主な支援内容
戦略・ガバナンス	サイバーセキュリティ CoE、アセスメント、規程・委託先管理ルール整備、AI ガバナンス、教育、取引先チェック・SCS 評価制度への対応準備
セキュア・アーキテクチャ	ゼロトラスト、認証・認可、ネットワーク・閉域設計、API セキュリティ、鍵・秘密情報管理、クラウド態勢管理
DevSecOps・セキュア開発	開発プロセス診断、脆弱性検知、セキュアな開発・リリース環境の整備、脅威モデリング
AI セキュリティ	エージェントガバナンス（ID・権限・監査・ライフサイクル管理）、AI エージェント保護、LLM／AI レッドチーミング、Agentic Security

診断・攻撃検証	脆弱性診断、クラウド設定診断、ペネトレーションテスト、レッドチーム演習、外部公開資産の調査
監視・運用	SIEM／SOAR、セキュリティ AI ハーネス、Agentic SOC、セキュリティ監視、CSIRT（インシデント対応組織）の構築・運用支援、脆弱性情報提供
インシデント対応	初動対応、被害範囲・原因の調査、デジタルフォレンジック、再発防止策の実装、机上演習

■ **サービス提供の流れ(進め方の 5 ステップ)**

1. 現状把握：システム環境、セキュリティ対策、組織体制、AI の活用状況などを確認し、課題とリスクを整理します。
2. 方針・優先順位の整理：事業への影響と対応の緊急性を踏まえ、必要な対策と優先順位を決めます。
3. 設計・実装：セキュリティアーキテクチャ、権限、確認・承認フロー、監視ルールなどを設計し、既存の製品や AI エージェント、業務システムとの連携環境を構築します。
4. 検証・運用：脆弱性診断や攻撃検証で対策の有効性を確認し、監視・運用を通じて新たな課題や改善点を把握します。
5. 改善・拡張：検証・運用の結果を踏まえて必要な改善を実施し、対象範囲を段階的に拡張します。

■ **提供体制**

ヘッドウォータースコンサルティングは、事業・業務の目的とセキュリティ上の課題を整理し、対策の優先順位、推進体制、運用ルールへ落とし込みます。ヘッドウォータースは、その方針を技術面の設計・構築、開発、AI セキュリティ、監視基盤・運用自動化へ反映します。両社が一体となって相談窓口とプロジェクト管理を担い、課題整理から実装、検証、運用定着までをつなぎます。ご相談の内容に応じた工程から支援を始め、前後の工程にも対応します。

両社は、製品・サービスの提供や組織・規程の整備自体をゴールとせず、ヘッドウォータースの技術力を、顧客が安全に進化し続ける力へつなげることを重視します。

■ **今後の展開**

今後は、ホワイトハッカーなど高度な攻撃検証の専門人材を擁する企業との連携も視野に入れ、診断・攻撃検証と技術実装・運用改善をつなぐ支援体制の充実を図ります。あわせて、検証・運用で得た知見をセキュリティ AI ハーネスへ取り込む取り組みを進め、AI エージェントが担える防御業務の拡大を目指します。

以上

■ **出典**

［1］「Digital Defense Report 2026」

［2］CISA「Known Exploited Vulnerabilities Catalog」

［3］Microsoft Learn「How does Microsoft Entra support Agent 365?」

■ **商標について**

記載されている会社名、製品名、サービス名などの固有名詞は、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ズ

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/

会社名：株式会社ヘッドウォーターズコンサルティング

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　加藤 健司

設　立：2022 年 2 月

URL：https://consulting.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ズ

お問い合わせフォーム：https://www.headwaters.co.jp/contact/