2026 年 11 月 18 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)

ヘッドウォータース、Anthropic「Claude Security」の活用を本格化

～「Claude で作る」から「Claude で守る」へ、
推論型セキュリティでソフトウェア防御を高度化～

AI ソリューション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、Anthropic が提供する「Claude Security」の活用を本格化し、AI の推論能力で企業のソフトウェア資産を守る「推論型セキュリティ」の実践を進めます。



■ 背景：AI の高度化と、ソフトウェアを守る側の課題

生成 AI の進化は、ソフトウェアの設計、実装、テストのあり方を大きく変えつつあります。その一方で、企業が保有するソフトウェアは複雑化し、複数のファイルやコンポーネント、データフロー、アクセス制御、ビジネスロジックを横断して潜在的なリスクを捉える必要性が高まっています。

AI の高性能化に伴い、攻撃手法の高度化も懸念されます。対策業務の増大や専門人材の不足も課題となるなか、AI を防御側でも活用する意義は一段と大きくなっています。

■ **「Claude Security」の概要**

Claude Security は、Anthropic が Claude の高度な推論能力をサイバーセキュリティ領域へ応用したセキュリティソリューションです。ソフトウェアのコードベースを解析し、潜在的な脆弱性の探索や修正を支援します。Claude Enterprise のベータ機能として提供されており、複数のファイルやコンポーネントをまたぐ関係性や文脈を読み解くことで、既知パターンの検査だけでは捉えにくいリスクを探索できる点が特長です。高性能モデル「Claude Mythos」を利用したスキャンにも対応します。

既知パターンの検出に加え、AI がコードやシステム全体の意味と関係性を読み解き、潜在的な攻撃可能性を探索するアプローチを、ヘッドウォータースは「推論型セキュリティ」と位置づけています。

■ **ヘッドウォータースの活用：「Claude で作る」から「Claude で守る」へ**

Claude は、コーディングに加え、設計書・仕様書の生成などにも適用し、大手事業者を含む複数の受注プロジェクトで実運用してきました。この活用を「作る」領域にとどめず、「守る」領域へと広げます。対象も、AI 生成コードに限らず、企業が保有するソフトウェア資産全体へ広げていく考えです。コードやシステムの文脈を読み解く推論型セキュリティにより、ソフトウェア防御の高度化を目指します。

自社プロダクトの SyncLect などでは、日常のチェックを既存のセキュリティ機能で、リリース前のチェックを Claude Security で行う組み合わせを採っています。Backend、Frontend、Infrastructure、CMS など複数の領域で、検出された指摘への修正と再スキャンを重ね、重大度の高い指摘が解消されたことを確認しました。
指摘には、リクエスト制御の不足を悪用した大量アクセスや、複数の処理の組み合わせによって生じるリスクなど、コード単体の確認では捉えにくいものも含まれます。

■ **今後について**

AI が企業活動の一部を支援する存在から、開発や業務そのものを担う存在へ進化するほど、企業の AI 戦略には新たな要件が生まれます。性能の高い AI を導入するだけでは足りず、一つの AI やサービスの状況に左右されずに、AI を組み込んだ業務を継続できることが重要になります。

ヘッドウォータースは、Microsoft Copilot などのエンタープライズ AI と、Anthropic「Claude」、OpenAI などの高性能 AI を組み合わせ、用途に応じて最適な AI を活用するマルチモデル戦略を推進しています。Microsoft エコシステムにおける実装力と、Claude や OpenAI などの AI 活用力を掛け合わせ、性能やコストだけでなく、セキュリティ、可用性、事業継続性まで含めて AI 環境を設計し、AI が企業活動を担う時代の「業務を止めない AI」の実現を目指します。

自社でも、Customer Zero（自社での先行実践）として、Claude Security の利用基盤となる Claude Enterprise を導入し、Claude Code や Claude Security を実際の開発・セキュリティ領域で活用してい

ます。Claude はグループの全ての会社で利用されており、グループ会社では、Claude を活用した AI BPO など、AI を実際の業務プロセスへ組み込んだサービスも既に提供しています。

こうした自社・グループでの実践から得た導入、運用、コスト管理、セキュリティ、マルチモデル活用の知見は、顧客企業の「AI Native Company」への変革に還元してまいります。あわせて、DevSecOps などセキュアな AI 駆動開発を含め、顧客の AI 活用とセキュリティ強化を支援してまいります。

以上

■ **関連情報**

- Claude Security ソリューション
- Anthropic「Claude」を活用したガバナンス対応型 AI 駆動開発を本格推進

■ **参考情報**

- Anthropic : Claude Security
- Anthropic : Claude Mythos

■ **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/

■ **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/