2026年11月2日

各　　位

株式会社HODL1
代表取締役CEO　田原　弘貴
（証券コード：2345　東証スタンダード市場）
（お問合せ先）取締役CSO　田中　遼
電話番号　03-6427-7380（代表）

機密情報を守りながら働く「AIセキュリティ対策エージェント」の実用化へ

主要なオープンソースAIエージェントHermes向けのセキュリティソフト「Mordred」を活用。Ryodan Systems AGとの共同開発を開始

当社は、スイスの暗号技術企業Ryodan Systems AGとともに、AIエージェントによる機密情報の漏えいを防ぐセキュリティソフト「Mordred」を活用した「AIセキュリティ対策エージェント」の共同開発を開始いたしましたので、下記のとおりお知らせいたします。



記

1　経緯

昨今、企業の情報漏えいが相次いでおり、その一因にはAIの存在があると考えられています。攻撃者はAIを使って脆弱性の探索から攻撃コードの生成までを自動化する一方、企業の側でもAIエージェントが業務に入り込み、財務データや取引先情報をAIが日常的に扱うようになりました。攻撃にAIが使われるなら、守る側もAIを使う「AIをもっ

て AI を制す」の発想により、この度の共同開発に至りました。

当社は、自社の上場実務で 1 年以上にわたり構築・運用してきた経験をもとに、2026 年 5 月 8 日から「AI 経営管理エージェント」を外部提供しています。一方、Mordred は、AI エージェントが扱う情報の送信先や操作範囲を制御するオープンソースソフトウェアで、広く利用されている AI エージェント「Hermes」向けに開発されたものです。この度、共同開発を開始した「AI セキュリティ対策エージェント」は、決算・経理・内部監査など、実際に機密情報を扱う業務で培った知見に、Mordred の情報保護機能を組み合わせる構想です。

まず当社内で試験運用を行い、その結果を踏まえて既存サービスへの統合と、幅広い企業業務への展開を目指します。

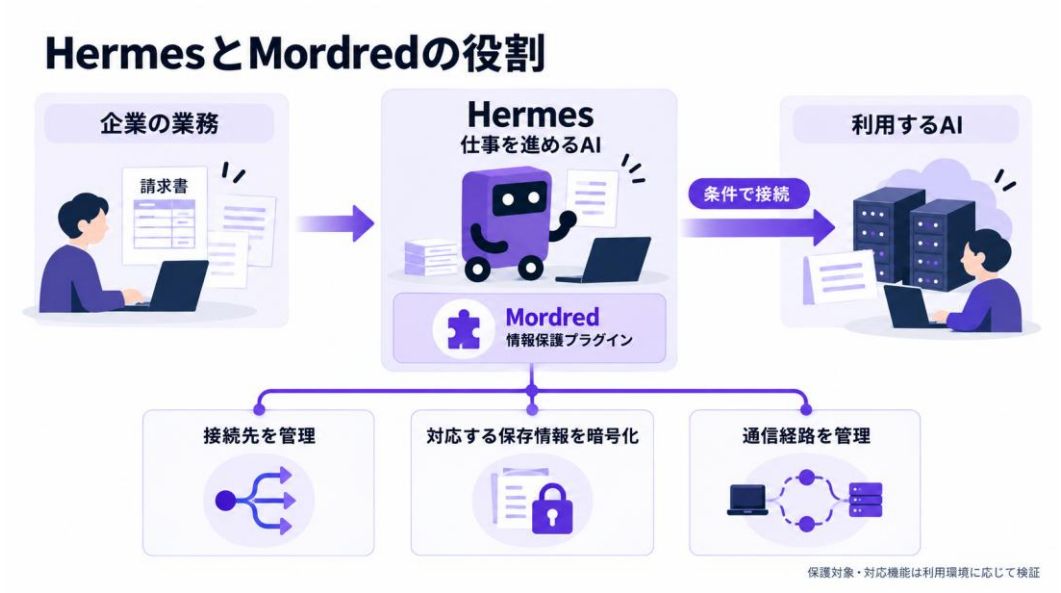
2　AI エージェントと企業の機密情報

AI エージェントは、依頼された仕事に必要な情報を集め、複数のソフトウェアを使いながら作業を進める AI です。例えば、請求書の内容を会計データと照合し、担当者が確認すべき項目をまとめるといった使い方があります。

仕事を任せる範囲が広がるほど、AI は財務情報や取引先情報など、企業の重要な情報に触れます。その分、外部の AI サービスへの情報漏えいや、悪意ある指示（プロンプトインジェクション）による誤った操作・送信のリスクも高まります。

これらは AI への指示だけでは防ぎきれません。AI の利用に対するサイバーセキュリティ対策を、企業が仕組みとして整備していることが欠かせません。

3　Hermes と Mordred の役割



■Hermes Agent

Hermes Agent は、Nous Research が公開する、広く利用されているオープンソースの AI エージェントです。情報収集、ファイルの操作、外部サービスとの連携など、複数の作業を組み合わせて実行できます。Mordred は、その Hermes にプライバシー保護機能を追加するプラグインです。

Nous Research は、2026 年 10 月に NVIDIA や Microsoft の M12 などから 9,000 万米ドル

の資金調達を公表しました。同社によると、Hermes のソフトウェアが複製された回数は 2,400 万回を超えています（同社公表値、2026 年 10 月時点）。

■Mordred

Mordred は、AI への指示に加えて、ソフトウェアで接続先や保存情報を管理します。設定した条件に合わない AI への接続を止め、対応する保存領域の情報を暗号化し、通信経路を管理する機能を備えています。

例えば、社内で動く AI だけに処理を限定する設定を使えば、Mordred が管理する AI 呼び出しの外部送信を止める設計が可能です。端末に保存する対応データには暗号化を適用します。当社は、利用環境ごとの対応機能と保護範囲を試験運用で確認し、企業の業務に合わせて組み込むことを目指します。

４　企業の実務につなげる HODL1 の役割

当社は、社員 2 名で、上場対応や人事労務を含む管理業務を運営しています。自社で構築・運用してきた AI 経営管理の基盤を外部提供し、経営ダッシュボード、仕訳連携、連結決算、内部監査サポートを通じて、顧客企業の経営管理業務を支援しています。

AI を悪用したサイバー攻撃の高度化・拡大に備え、当社は、AI への「機密情報を外部に送らない」という指示に加え、ソフトウェア側で情報の送信先を制限する構成を目指します。Mordred の厳格な設定では、管理対象の AI への接続が許可条件を満たさない場合、送信を止める仕組みが用意されています。例えば、社内で動く AI だけを使う設定により、対応する AI 呼び出しを外部へ送らない構成にすることで、機密情報を外部の AI 事業者へ渡す機会を減らします。

さらに、対応する保存情報を暗号化することで、保存ファイルを取得された際に内容を読まれるリスクを抑えます。当社は、Ryodan の情報保護技術に加え、AI が実行できる操作の範囲と、人の承認が必要な操作を業務ごとに定める方針です。送信先の制限で情報の持ち出しを抑え、暗号化で保存情報を守り、人の確認で重要な操作を管理するという、異なる役割の対策を重ねます。これにより、AI が誤った指示に従った場合にも被害を抑えられるよう、既存システムとの接続から日々の運用まで設計します。

５　自社検証から企業向けサービスへ

まず、当社内の対象業務を限定して試験運用を行い、業務品質や運用費用に加え、セキュリティ対策の有効性を重点的に検証する計画です。機密情報の意図しない外部送信や、悪意ある指示による操作を想定し、送信先の制限や人による承認が機能するかを確認します。暗号化の対象と保護範囲も確認し、その結果を踏まえて、「AI 経営管理エージェント」への統合と顧客企業への提供内容を具体化します。

試験運用で判明した課題を改善し、保護できる情報と運用条件を明確にしたうえで、顧客企業への展開を進める方針です。AI を利用した攻撃や情報漏えいのリスクに備え、セキュリティ対策と業務の使いやすさを継続して改善し、企業が安心して日常的に使えるサービスへつなげます。提供開始時期、価格、共同開発の条件は、今後の協議・検証を踏まえて定める方針です。



６　AI エージェントから AI 推論事業への展開

AI エージェントが仕事を実行するたびに、AI モデルが情報を処理する「推論」が必要になります。企業の業務に AI エージェントが定着すれば、日常の仕事に伴う推論サービスの継続利用につながります。

当社は将来的に、AI エージェントと推論サービスを組み合わせて提供する事業を目指します。AI の利用量を管理し、複数の AI モデルへの接続をまとめる LLM ゲートウェイや、GPU を用いた推論基盤との統合を検討します。

ここでいう AI トークンは、AI 推論サービスの利用枠を指します。顧客の利用需要と採算性を確認し、供給契約等の条件を整えながら、AI トークンの調達・販売への展開を検討します。

業務を担う AI エージェント、機密情報を守る機能、AI を動かす推論サービスを組み合わせ、企業が AI を継続して利用できる事業を育ててまいります。

なお、本提携が当社の業績に与える影響は軽微と見込んでおります。

以　上