Press Release

2026 年 6 月 25 日（木）

Exabeam Japan 株式会社

Exabeam、AIエージェントやデジタルワーカーの ”動作検証”を実現するオープンソース「Praxen」を公開

本番投入前に、AI エージェントが "担うべき業務" を理解し、"許可された行動" を検証し、
"想定とのギャップ" を特定する、新たな実践手段。

コロラド州ブルームフィールド、2026年6月23日 – エージェンティック・エンタープライズ（AI エージェントが人と協働して業務を自律的に進める企業モデル）向け Behavior Intelligence（行動インテリジェンス）のリーダーである Exabeam は本日、本番環境に投入される前に、その設定・権限・統制が "本来担うべき責務" と整合しているかを検証する新たなセキュリティ領域のツール 「Agent Behavior Verification （ABV）／エージェント動作検証」を発表しました。

AI エージェントは、企業環境において、単なるアシスタントから ”業務を自ら遂行する実行主体” へと役割を広げつつあります。エージェントはシステムにアクセスし、ツールを起動し、ワークフローを実行し、より高い自律性をもって意思決定を行います。これに対し、脆弱性スキャンやレッドチーミングといった既存のアプローチは、稼働中のエージェントの活動を統制・監視・テストする手段としては有効である一方、本番投入の”前”に、そのエージェントが安全に稼働できる状態にあるかどうかを実務的に判断する手段はこれまでに存在しませんでした。

Agent Behavior Verification （ABV） は、こまさにこの空白領域を埋めるものです。既知の脆弱性や個別のコード成果物だけに着目するのではなく、エージェントを1つの完結したシステムとして評価し、「許可された役割」を定義したうえで、その実装・権限・統制が当初の目的と一致しているかを評価するためのフレームワークを提供します。

この考え方を組織が実践に移せるよう、Exabeam は ABV のオープンソース・リファレンス実装である Praxen を併せて公開します。

「企業は AI を実験段階から運用段階へと急速に移行させています」と、Exabeam の Chief AI Officer であり、OWASP Gen AI Security Project の創設者兼共同議長を務める Steve Wilson は述べています。「エージェントがデジタルワーカーとして機能するようになる今、セキュリティチームに必要なのはランタイムでの可視化にとどまりません。本番投入の前に、適切な権限・適切な統制・適切な境界をそのエージェントが備えていると確信できることが

不可欠です。Agent Behavior Verification（ABV）は、極めて本質的な問いに答えるための手段です。すなわち、"このエージェントは、与えられた仕事を、与えられた仕事だけ、きちんと遂行できるのか？" という問いです。」

Praxen が Agent Behavior Verification（ABV）の運用を可能にする

Praxen は、ABV の中核概念である remit（レミット／役割契約）— そのエージェントが何をして良いか、どのリソースにアクセスして良いか、どの境界の中で動くべきかを定義したポリシー契約 — を用います。これにより開発者と運用者は、エージェントの実装・ツール・設定・メモリ・連携・実行環境が、定義された役割と一致しているかを検証できます。

Praxen は、"意図された振る舞い" と "実装された振る舞い" のギャップを特定して報告することで、本番投入前に開発者へ具体的な改善策と動作上のリスクを提示します。レポートには、個別の検出事項、改善のための推奨事項、そしてエージェントのセキュリティ態勢に関する総合的な成熟度スコアが含まれます。

「従来のセキュリティツールは、ソフトウェアのどこに脆弱性があるかを教えてくれます」と Wilson は続けます。「Praxen が評価するのは、まったく別の問いです。すなわち、エージェントの機能・権限・ツール・制御が、そのエージェントに認可された役割と整合しているか、という問いです。これは、高度に自律的なエージェントがもたらす最も重大なリスクの1つに正面から取り組むものであり、エージェントのライフサイクル全体にわたる継続的なガバナンスのための、より強固な基盤を確立します。」

Agent Behavior Verification（ABV）は、Exabeam のエージェントセキュリティ戦略における"本番投入前の基盤"と位置づけられます。本番環境において異常または高リスクなエージェントの挙動を検知する ABA（Agent Behavior Analytics／エージェント行動分析）を補完するものです。

Praxen は、agentic coding agent skill（エージェンティック・コーディング・エージェント・スキル）として実装され、Apache 2.0ライセンスの下で公開されます。透明性・拡張性を備え、開発者・研究者・セキュリティ実務者が誰でも利用・検証できるよう設計されています。

「多くのセキュリティツールは "何が脆弱か" を教えてくれます。Praxen が問いかけたのは、まったく別の問いでした。"このエージェントの実際の振る舞いは、それが守るべきガバナンスや業務範囲と一致しているか?" という問いです」と、Medigram の CEO、Shelli Douville 氏は述べています。Praxen が示したコードレベルの是正策は、ファイルに綴じておくためのリスクレポートではありませんでした。それは、私たちが即座に行動に移せる、極めて具体的なエンジニアリング・ロードマップでした。エンタープライズにおける AI 導入では、"エージェントが許可されている動作"と"実際に実行しうる動作"の間のギャップこそが、運用リスクの温床なのです。」

自律型 AI システムにおける透明性と信頼の促進

Exabeam が Praxen をオープンソースとして公開するのは、ABV を業界共通のベストプラクティスとして育てていくためです。AI エージェントをどう統制し、監視し、検証すべきか — 業界はいまだその定義を模索している段階にあります。

Praxen をオープンソース化することで、開発者・研究者・セキュリティ実務者は、このフレームワークを精査し、機能強化に貢献し、それぞれの環境のなかで ABV の原則を適用できるようになります。

「Praxen」は、Apache 2.0ライセンスのもと、以下より入手いただけます：
https://open-agent-ai-security.github.io/praxen/

Exabeamについて

Exabeamは、Agentic Enterprise（AIエージェントが人と協働して業務を自律的に進める企業モデル）向け行動インテリジェンスのリーダーです。組織がデジタルワーカーを導入し、機械のスピードで行動する敵に直面している今、Exabeamはエージェントを活用した分析によって、人間と人間以外の内部関係者の行動を両方とも理解し管理します。Exabeamは、統合されたExabeam Novaサイバーセキュリティエージェントにより、人間とエージェント両方による内部脅威をカバーし、より高速かつ正確な脅威の検知、調査、対応（TDIR）を実現する、業界でも実績のある柔軟なソリューションを提供します。ユーザーとエンティティ行動分析（UEBA）のパイオニアであり、エージェント行動分析（ABA）のイノベーターであるExabeamは、リスクの低減、デジタルワーカーの保護、セキュリティ運用の迅速化を実現するベンダーとして、世界中の3,000社以上の企業から信頼されています。詳細については、www.exabeam.comをご覧ください。

Exabeam： 内部不正対策。人間も、AI も。

【本プレスリリースに関するお問合せ】
10Fold Communications
Exabeam@10fold.com