Press Release

2026 年 9 月 25 日（金）

Exabeam Japan 株式会社

Exabeam調査：セキュリティリーダーが「AIエージェントのアクセス権」を最重要の内部リスクとして認識

約半数が、過剰・侵害・意図しないアクセス権を持つ AI エージェントを最大の脅威と回答。一方で、AI エージェントの行動コンテキストの把握とビジネスリスクへの換算が依然として大きな課題

- **セキュリティリーダーの48%が「過剰な権限」「侵害された権限」「意図しないアクセス権限」を持つ AI エージェントを、自社にとって最大の脅威と位置付けています。**
- **各組織は AI エージェントの監視を強化している一方で、行動の文脈、相関関係、およびその行動をシステム横断的に把握することに課題が残されています。**
- **セキュリティ部門と財務部門は、サイバーセキュリティにおけるリスクの認識について一致しているが、セキュリティリーダーの55%が、CFO が納得できる金銭的被害の観点からリスクを説明できなかったために、セキュリティ施策を遅延あるいは縮小しています。**

エージェンティックエンタープライズ（AI エージェントが業務の担い手となる企業）に向けた行動インテリジェンス（Behavior Intelligence）のリーダーである Exabeam は本日、AI エージェントが企業セキュリティチームにとって新たなインサイダーリスクの最重要課題になりつつあることを示す最新調査結果を発表しました。調査対象となったセキュリティリーダーの約半数（48%）が、「過剰な権限」「侵害された権限」「意図しないアクセス権」を持つ AI エージェントを、自社にとって最大の脅威と回答しました。これは、外部の攻撃者、アカウント侵害を受けた内部関係者、悪意ある内部関係者によるリスクを上回る結果です。さらに、多くの組織が AI エージェントの監視を強化している一方で、その行動をシステム横断的に理解し、ビジネスコンテキストに結びつけて評価することに課題を抱えていることも明らかになりました。

Exabeam は、最新レポート『**The Agentic Insider: From Monitoring to Understanding（エージェンティック・インサイダー：監視から理解へ）**』の作成にあたり、調査会社 Sapio Research に委託し、7カ国のセキュリティおよび財務部門の意思決定者600名を対象に調査を実施しました。本調査における AI エージェントとは、対話型チャットボットではなく、限定的な人手介入のもとで企業システムやデータにアクセスし、自律的に業務を遂行する目的駆動型システムを指します。

調査結果によると、AI エージェントが企業運営における信頼された担い手となるにつれ、多くの組織はその活動を監視するための取り組みを拡大しています。同時に、セキュリティリーダーは、現行の監視手法における主要な限界として、「行動コンテキストの把握とイベントの相関分析」を挙げています。さらに、システムを横断した可視性の欠如が引き続き大きな課題となっています。

「各組織は AI エージェントの監視において着実な進歩を遂げていますが、活動を監視することと、行動を理解することは同じではありません」と、Exabeam の最高 AI・製品責任者（Chief AI and Product Officer）であるスティーブ・ウィルソン（Steve Wilson）は述べています。「AI エージェントは正規のアクセス権を用いて複数のシステムをまたいで動作するため、個々の操作は一見すると正常な処理のように見えます。セキュリティチームには、こうした操作を時系列でつなぎ合わせるためのコンテキストが必要です。それにより、想定どおりの自動化なのか、悪用・侵害・意図しない挙動なのかを見分けることができます。」

AI エージェントのアクセスがインサイダーリスクを再定義する

AI エージェントは、悪意がなくてもリスクを生み出す可能性があります。本調査は、AI エージェントの急速な導入が、組織のインサイダーリスクに対する考え方を変えつつあることを示しています。

主な調査結果は以下のとおりです。

- **48%** のセキュリティリーダーが、過剰・侵害・意図しないアクセス権を持って動作する AI エージェントを、今日の自社にとって最大の脅威と回答。これは外部の攻撃者（28%）、アカウント侵害を受けた内部関係者（12%）、悪意ある内部関係者（12%）を上回る結果に。
- 機密データへのアクセス、意図された権限を超えた操作、調査の複雑化、AI エージェントの行動に対する可視性の欠如が、セキュリティおよび財務のリーダーにとっての主要な懸念事項として挙げられました。

組織は AI エージェントの監視を拡大中

セキュリティリーダーは、AI エージェントの監視にさまざまなアプローチを用いていると回答しています。

- **60%** が、専用の AI セキュリティ／ガバナンスツールを使用。
- **56%** が、既存の SIEM・検知・監視プラットフォームを拡張して活用。
- **56%** が、行動監視およびベースライン化を実施。
- **29%** が、依然として手動レビューに依存。

こうした投資にもかかわらず、**27%** が「行動コンテキストと相関分析の不足」を現行の監視アプローチにおける最大の限界として挙げており、環境を横断した可視性の低さ、アラートの優先順位付け、手作業によるプロセスなども依然として大きな課題として残っています。

セキュリティ部門と財務部門はリスク認識で一致。ただし投資には強力なビジネス価値の説明が不可欠

本調査ではまた、セキュリティリーダーと財務リーダーの間に強い足並みの一致があることも明らかになりました。両部門の **93%** がサイバーセキュリティのリスク許容度について一致していると回答し、セキュリティリーダーの**81%**が「CFO は、自分たちが軽減しようとしているサイバーセキュリティリスクを理解している」と回答しました。

しかし、その一致が必ずしも投資に結びつくとは限りません。セキュリティリーダーの**55%**が、「CFO が納得できる財務的な観点でリスクを説明できなかったために、セキュリティ施策を遅延・縮小した経験がある」と回答しています。

「CFO がサイバーセキュリティリスクの存在そのものを疑うことはほとんどありません」と、Exabeam の最高財務責任者（Chief Financial Officer）であるマイク・バイロン（Mike Byron）は述べています。「重要なのは、提案された投資によってそのリスクがどれだけ低減されるのかを、測定可能なビジネス上の指標で理解することです。セキュリティチームが技術的な成果をビジネスインパクトに結びつけられれば、投資判断ははるかに容易になります。」

レポートの入手方法

『**The Agentic Insider: From Monitoring to Understanding**』のダウンロードは下記の URL にアクセスしてください。

www.Exabeam.com/from-monitoring-to-understanding

調査方法

本調査は、Sapio Research が Exabeam の委託を受け、2026年6月に、従業員500名以上の組織に所属する600名の専門家を対象に実施しました。内訳は、セキュリティを担当する IT 意思決定者300名と、財務の意思決定者300名です。回答者は、米国、カナダ、英国、フランス、ドイツ、オランダ、オーストラリアに拠点を置いています。調査はメールによる案内および調査パネルを用いてオンラインで実施されました。結果は信頼水準95%、誤差範囲±4.0ポイントです。

Exabeam について

Exabeam は、エージェンティックエンタープライズ（AI エージェントが業務の担い手となる企業）に向けた行動インテリジェンス（Behavior Intelligence）のリーダーです。企業がデジタルワーカーを導入し、マシンスピードで動く攻撃者に立ち向かう中で、Exabeam は AI エージェントを活用した分析により、人間と人間以外の双方のインサイダーの振る舞いを把握し、ガバナンスします。サイバーセキュリティ AI エージェント「Exabeam Nova」を統合し、人間と AI エージェントの双方をカバーする内部脅威対策と、より迅速かつ高精度な脅威の検知・調査・対応 （TDIR: Threat Detection, Investigation, and Response）を実現する、柔軟で実績豊富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の行動分析（UEBA: User and Entity Behavior Analytics）の パイオニアであり、エージェントの行動分析（ABA: Agent Behavior Analytics）を生み出したイノベーターとして、Exabeam は世界 3,000 社を超える企業に信頼され、リスクの低減、デジタルワークフォースの保護、セキュリティ運用の高速化を支援しています。詳細は www.exabeam.com をご覧ください。

Exabeam：内部脅威を、止める。人でも、AI でも。

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