エージェンティックAI 新時代におけるCISOの手引き

ここ数年のAIブームは、依然として拡大を続ける衝撃波となり、従来の働き方を一変させ、新たなビジネス機会を生み出しています。イノベーションの爆発がいつか落ち着くのは必然ですが、今、世界の注目を集めている新たな進展がエージェンティックAI（Agentic AI）です。

2023年が「チャットボットの年」、2024年が「copilotの年」だったとすれば、2025年は「AIエージェントの年」 になるでしょう。このタイムラインは、AIが驚くべきスピードで進化してきた事実を物語っています。

では、エージェンティックAIはAI発展の “通過点” にすぎないのでしょうか。それとも、ビジネスに持続的かつ有意義な変革をもたらす “目的地” なのでしょうか。Gartnerなどの業界アナリストは後者を予測しており、エージェンティックAIが実際に組織へ提供する価値をレポートするとともに、「2028年までにIT運用ツールの60　%が同技術を搭載する」との見通しを示しています。

当然ながらサイバーセキュリティもテクノロジー主導の分野です。現在、多くのCISO（最高情報セキュリティ責任者） が抱く最大の関心は、「エージェンティックAI—そしてそれを原動力とするAIエージェント／ツールが　セキュリティオペレーションセンター（SOC）をどう向上させ得るか」という点にあります。

この問いに答えるには、まずエージェンティックAIの定義と適用範囲を明確にし、現実的な期待値を設定することが不可欠です。

ミッションクリティカルか、それともミッションシニカルか？

近年のAI技術の飛躍的進歩は、大規模言語モデル（LLM）の進化に端を発しています。LLMは機械学習（ML）と自然言語処理（NLP）を土台に、人間と直感的に対話

こうした機能が相次いで新ツールに組み込まれるなか、サイバーセキュリティリーダーや意思決定者は、技術導入を誇張・単純化するベンダーの“洪水”に直面しています。既存製品を「AI対応」と言い換えて派手なデモを見せるのは簡単ですが、実際に新規性と現場価値を備えたソリューションを開発することは別次元の難易度です。

十分な検証を行わないかぎり、その違いを見抜くのは容易ではありません。そのため、AI ブームの波のあとに、測定可能な成果をもたらさない製品だけが手元に残るという事態がたびたび起こっています。しかし、推測を排し、真に次世代型のAIツールを選定できれば、組織にとってゲームチェンジャーとなり得るのです。

AI選定・導入は一大勝負

近年のAIエージェントの登場により、CISOは再び「広告と実態の間」を読み解く作業に追われています。どの製品が戦略目標を本当に前進させるのか、何が単なるマーケティングなのかを見極めなければなりません。

しかも他部門の経営層が効率化やUXを主眼に置くのに対し、CISOには「新技術をいかに安全にエンタープライズ環境へ導入するか」という追加責務があります。

CISOはツールとベンダーを審査する際に賢さだけでなく速さも求められます。ビジネスや競合、顧客からの圧力に加え、ワークフローを拡張・自動化・高速化する新技術は必ず攻撃者にも悪用されるという現実があるからです。

サイバーセキュリティ分野における“FOMO（取り残される恐怖）”は、単に最新ガジェットを欲しがる心理ではありません。絶えず変化する攻撃者の戦術・技法を先読みし、芽の段階で摘み取る能力そのものなのです。

前回のAIブームから得た教訓

生成AIをめぐる過熱報道が示したとおり、「期待外れや幻滅のリスクは現実に存在する」という事実です。多くのベンダーが価値を語りますが、実際には旧製品を急造で「AI対応」とラベル替えしただけというケースも少なくありません。

さらに、「AI機能は高価なアドオンです」と謳うベンダーの場合、AIがプラットフォーム全体に深く統合されていない可能性が高く、機能・互換性・セキュリティ・ユーザー体験の面で不安が残ります。

今回こそAI 導入を成功させるには、CISOはAI エージェントをワークフローに完全統合し、自社の主要ビジネス目標を具体的に前進させられるベンダーを優先すべきです。さらにそのベンダーには、データの取り込み・保存・破棄方法を文書化し、プライバシー／保護規制に適合していることを示す堅牢なガバナンスが必須です。

CISOの戦略的優先事項

一般にエージェンティックAIは、意思決定・問題解決・自律的な実行という能力が強化されている点で、従来の生成AIと異なります。ただし技術論に入る前に、CISOが果たそうとする核心ニーズと、それを技術で埋められるかどうかを整理しましょう。

1.攻撃ボリュームが前例のないレベル

SOCが頼る多くの脅威検知メカニズムは、既知のシグネチャに基づきます。しかしAIの時代には、シグネチャを持たない新種の脅威が爆発的に増え、従来の脅威インテリジェンスでは捉えきれません。実際、AIで自動生成された攻撃が絶え間なく繰り返されており、人手だけでは対処不能な規模となっています。

いまやAIにはAIで対抗するしかありません。CISOが評価すべきは、AIエージェントが MTTR（平均対応／修復時間）をどこまで短縮できるかです。MTTRはサイバーセキュリティの最重要KPIであり、多くのSOCは脅威検知・調査・対応（TDIR）を支えるツールとワークフローを蓄積しています。

既存のUEBAなどは“TD（検知）”を得意としますが、“IR（インシデント対応）”を加速 する領域こそAIが得意な領域であり、なかでもAIエージェントが真価を発揮します。適切なデータに適切な問いを投げかけ、次に取るべき対応を自動で推奨・キューイングできるからです。

2. 収集されるデータ量は桁違い

現代の企業はこれまでになく大量のデータを収集・利用しており、その結果、日々数十億件のログファイルが生成されています。それぞれのログには、脅威ハンターにとって調査の要否を判断する手がかりとなる情報が数多く含まれています。

この膨大なデータを整理し、扱うことができる洞察にまで絞り込むことが、サイバーセキュリティ分野でAIが不可欠とされる主因です。AIの基盤である機械学習（ML）は、巨大な情報の中からパターンを学習し、異常を検知できるアルゴリズムを育成します。その上でチャットボットやCopilotは、自然言語処理（NLP）と、近年では大規模言語モデル（LLM）を活用して検索機能や平易な解説を提供できるようになりました。

現在、CISOs（最高情報セキュリティ責任者たち）が注視しているのは、エージェンティックAI（Agentic AI）がこうした能力をさらに発展させ、Tier 1アナリストが毎回Tier 3にエスカレーションしなくても、適切な判断と行動を取れるよう支援できるかという点です。

CISOsが痛感しているとおり、平均的なセキュリティアナリストは1日に100件ものケースを精査しなければなりません。しかし本来注力すべきは、最も重要な15〜20件です。新しいAIツールをSOCに導入する以上、アラートのトリアージ支援が期待されるのは当然でしょう。

とはいえ、AIをどこまで自律的にアラートへ対処させるかは慎重に考える必要があります。TDIRの各アクションは組織全体に重大な影響を及ぼす可能性があるため、AIエージェントに許容する自律性の度合いを明確に定義しなければなりません。

現時点で最良と考えられるアプローチは、脅威を検知した際に調査・対応の提案、選択肢、プレイブックを自動提示し、最終判断は人間が下す仕組みといえるでしょう。

3. SOC人材育成の急務

サイバーセキュリティ分野の人材不足は、CISOsにとって長年の課題です。離職と燃え尽き症候群（バーンアウト）が蔓延し、Tier 3アナリストの確保は特に困難です。

バーンアウトの主因には、生成AIを悪用したサイバー犯罪の急増があります。SOCアナリストはアラート疲労に悩まされ、推定62%ものアラートを誤検知かどうかを判断して却下しています。その結果、84%のセキュリティ専門職が「バーンアウトを経験した」と回答し、離職の50%はこれが原因とされています。

アナリストが辞めるたびに、組織のセキュリティ運用は損なわれます。Tier　1であっても、自社SOCの独自エコシステムを習得するには数か月を要します。この問題はCISOにとって 二つの優先課題が突き付けることになります。

1. 作業負荷とワークフローを最適化し、アナリストが日々の業務を快適にこなして離職を防ぐにはどうするか。
2. 限られたリソースでSOCの生産性を高め、Tier 1でもTier 3並みに活躍できる環境をどう整えるか。

67%の組織が「中度〜深刻なスキルギャップがある」と報告するいま、これらの問いに答えることは極めて重要です。うまく導入できれば、エージェンティックAIは不足スキルを補完し、現職のSOCアナリストに再び仕事のやりがいをもたらす原動力になり得ます。

4. SOC はその価値を証明しなければならない

サイバー犯罪の規模がSOCの能力を上回るなか、セキュリティリーダーの77%は「重大な侵害が起きれば自分のキャリアが終わるかもしれない」と懸念しています。そのため、組織のセキュリティ体制を継続的に強化することも重点課題になっています。

サイバーセキュリティ運用のレベルアップに終わりはありません。CISOはSOCのパフォーマンスを追跡・測定できるだけでなく、セキュリティ運用がビジネスにもたらす価値とインパクトを示したいと考えています。SOCは測定可能なROIを生む戦略的資産であり、後回しにできるものではありません。しかし、その価値を証明するのは容易ではありません。

では、AIエージェントがこれらの領域をどう支援できるのでしょうか。エージェンティックAIはデータにアクセスし、傾向やパターンを洞察し、それを直感的かつ実行可能な形で提示できます。AIエージェントはコンサルタントの役割を担い、TDIRにとどまらず戦略面でもSOCを支援できるのでしょうか。

エージェンティックAIの実践的な定義

エージェンティックAIがCISOとSOCの優先課題達成をどう支えるのかを理解するには、従来の生成AIと異なる特徴を押さえる必要があります。主な差別化要素は次の3つです。

1. 能動的かつ先回りで行動する。エージェンティックAIは、解決すべき問題を認識・理解したうえで、自律的または半自律的に対処します。このプロアクティブなアプローチにより、従来の手動入力と遅い更新を前提としたソフトウェア開発と比べ、より迅速な対応とダイナミックな解決策を可能にします。
2. 高度な推論能力を備える。コンテキストを動的に把握し、複雑かつ多段階のタスクを解決できるよう行動を適応させます。継続的な学習により、進化するセキュリティ課題にも高精度で対処できます。
3. 3.協調・協働を組織化する。エージェンティックAIの大きな魅力は、マルチエージェントワークフローを実現できる点です。多数の専門特化したエージェントにタスクを分散し、柔軟でモジュラーな“機械主導のワークフォース”を構築します。

LLM技術を先回り型のエージェントとして活用すれば、適応型ソリューションを迅速に導入できます。従来手法が遅く硬直的であるのに対し、エージェンティックAIは少ない人手で脅威やユースケースの変化に柔軟・効率的に対応します。

マルチエージェント環境には依然として人間の監督が必要ですが、このレベルの自動化と連携は既に現実のものとなっています。New-Scale Security Operations Platform「Exabeam Fusion」では、Threat CenterでAI エージェントがアクティビティをリスクと関連付け、リアルタイムのインシデントおよび調査サマリーを提示します。Outcomes Navigatorでは、AIがマネージャーや経営層のSOC効果測定を支援します。

これらのエージェントはTier 1アナリストからCISOまで異なるペルソナ向けに設計されていますが、相互に連携し、よりインテリジェントで効率的なセキュリティ運用環境を実現します。

エージェンティックAI を賢く導入するには

サイバーセキュリティはもともとエージェンティックAIのような技術に対し、きわめて具体的で本質的なユースケースを持つ分野です。機械知能の活用はTDIRにおいて10年以上前から不可欠であり、エージェンティックAIの最も強力な適用領域もこの深い基盤の上に築かれるはずです。

ExabeamはUEBA（ユーザーおよびエンティティ行動分析）を業界に先駆けて開発し、革新的な機械学習（ML）モデルを展開してきました。複雑な脅威の検知、リスクのスコアリングと優先度付け、イベントや攻撃チェーンの横方向の進行を漏れなく追跡し、通常行動のベースラインを確立するといった機能を備えており、現在も重要な役割を果たしています。

一方、大規模言語モデル（LLM）は特定の領域では卓越した能力を示すものの、生の複雑なビッグデータをインテリジェントな検知へと変換する力はありません。データから洞察を引き出し、従来手法では見逃される異常を特定するには、特に行動分析を用いた MLが依然として不可欠です。

Threat Centerの導入により、Exabeamは新たなAI技術との連携をさらに進化させました。当初はケース・検知・アラートを一元管理するアナリスト用ワークベンチでしたが、ここにAIチャットボットやCopilotを重ねることで、直感的かつ意図的に脅威サマリーやアナリスト支援を提供し、具体的な価値を生み出しています。

LLMは膨大なデータから洞察を抽出して意思決定する用途には適していませんが、限定された文脈での言語変換には秀でています。

こうした特性を踏まえ、Exabeamが導入した AIイノベーションは顧客満足度がきわめて高く、過度な期待に応えられなかった他の生成AI製品とは対照的でした。また、これらのAI機能は追加費用なしで既存ライセンスに組み込まれており、ユーザーはすぐに活用できます。

エージェンティックAIも同様の道をたどります。強固な基盤の上に、SOCの実際のニーズを的確に満たすユースケースを築くことで真価を発揮します。

SOCを変革するエージェンティックAIはすでに稼働中

エージェンティックAIの能力は未来的に聞こえるかもしれませんが、すでに現実のものとなっています。ExabeamのAIエージェントExabeam Novaは、SOCを多方面でサポートします。従来のExabeam Copilotはインシデントを手早く把握できる脅威サマリーで好評を博しましたが、Novaはそこから更に進化し、脅威分類・優先度・根拠を含む詳細な調査サマリーを自動生成します。

この進化により、Tier 1／Tier 2アナリストは、すべてのケースをエスカレーションせずとも十分な判断材料を得られます。なぜなら、Novaは旧Copilotの10倍以上のデータをLLMに供給しているためです。

またNovaのThreat Explainer機能は、インシデントの詳細だけでなく、その影響や懸念点まで掘り下げて説明します。必要な情報が不足している場合は、その旨と不足分まで提示し、無理に回答しようとする従来型AIアシスタントとは一線を画しています。

さらにNovaは、マルチエージェントワークフローの可能性を示しています。用途別に組み込まれた複数のNovaエージェントが連携し、SOCを支援します。

- Attack Surface Insightsと連動し、エンティティ情報を自動取得
- Threat Centerのタイムラインを補完し、時系列情報と高度な検知を提供
- こうした仕組みによりコストと時間を大幅に削減し、エンタープライズSOCチームの業務体験を劇的に向上させます。激化するサイバー脅威に対処するうえで、まさに今最も求められている変革といえるでしょう

CISOにとって“次世代セキュリティコンサルタント”となるNova

さらにExabeam Novaはアドバイザリー機能を担い、CISOがSOCのパフォーマンス指標や実効性をエビデンス付きで示せるよう支援します。

たとえばOutcomes Navigator。2023年に導入されたこの生成AI支援機能は、MITRE ATT&CK®の主要テクニックに対する組織のセキュリティ体制を採点します。New-Scale Platformで最も人気の高いプロダクトの一つですが、ここにエージェンティックAIが加わったことでさらに進化しました。CISOはセキュリティ態勢のパフォーマンス推移を把握できるほか、AIがコンサルタントとして経営層向けレポートやカバレッジ改善サマリーを自動生成します。人間なら調査・作成に数日かかるレポートを、瞬時に入手できるのです。

ベストプラクティスが最高の成果を生む

AIの次なる導入・活用フェーズに直面する今、CISOは新たなハイプサイクルを見極め、デモや製品ロードマップで示されるエージェンティックAIの実力が本物かどうかを精査しなければなりません。こうした局面では、長年にわたりAIイノベーションを牽引し、Gartner Magic Quadrant®など業界レポートでリーダーとして評価されるベンダーを選ぶのが、最も賢明な選択肢となります。

Exabeamは10年以上にわたり、AIを核に事業を展開してきた稀有な企業です。機械学習 によるデータ処理とパターン認識は、UEBAが「正常行動ベースライン」を構築する基盤となり、その結果がTDIRのダッシュボードやタイムラインに反映されます。この高精度な検知情報を生成AIが活用することで、顧客に実質的な価値を提供してきました。そこへ今回、エージェンティックAI が新たなレイヤーとして加わり、従来の仕組みをさらに強化しています。

ExabeamにおけるAIデータ処理はすべてNew-Scale Analytics内で安全に行われます。同サービスはGoogle Cloud Platform（GCP）上で稼働し、GoogleのGemini LLMを使用します。すべてのLLMは事前学習済みであるため、顧客データで追加学習することは一切ありません。システムが取得するデータは揮発性（エフェメラル）で、標準のTLSプロトコルで暗号化され、評価プロセスはメモリ上で完結するため、データが保存・キャッシュ・保持されることはありません。

さらに、モデル処理は可能な限り顧客が指定した地理的リージョン内で実行されるため、データプライバシーと法規制遵守を確保しつつ、スピードとスケールを最適化できます。

Exabeamは業界のパイオニアとして、エージェンティックAIがワークフローを刷新し、CISO と企業SOC、そしてそのビジネスにもたらす多彩な価値をこれからも提供し続けます。

About Exabeam

Exabeamはインテリジェンスとオートメーションの分野をリードし、世界有数の企業のセキュリティ運用を支えています。

グローバルなサイバーセキュリティ革新企業として、Exabeamは実績豊富でセキュリティに特化した柔軟なソリューションを提供し、脅威の検出・調査・対応（TDIR）をより高速かつ正確に実現します。

exabeam

Learn more at www.exabeam.com →