AIの可視化なくして信頼なし

死角はAIの脅威を隠すだけでなく、統制の信頼性も損なう

AIパルス調査 ― 第4弾

protiviti®
Global Business Consulting

目次

エグゼクティブサマリー

サイバーセキュリティとレジリエンスに焦点を当てたプロティビティの最新のAIパルス調査によると、今日のサイバー環境では二つの異なる現実が共存しています。IT部門のリーダーたちは、人工知能（AI）によってもたらされる脅威が現場レベルで大幅に増加していると見ていますが、経営陣の見解はより穏やかです。同じような認識のギャップは、経営層が従業員のAIツールの使用状況を把握できていない点にも現れています。多くの大規模組織（47%）[1] および中規模組織（68%）[2] が、管理されていないAIの利用、いわゆるシャドーAIに直面していることが判明しました。[3] 要するに、取締役会は企業全体で何が起きているかを把握できず、不完全な情報に基づいてリスク対策に資金を投じ、ガバナンスを行っていることになります。

従来、これらのギャップは、組織が新技術の導入においてしばしば直面する時間的な遅れや、リスクの結果が顕在化し、測定され、経営層や取締役会に報告されるまでに要する時間に起因すると考えられてきました。しかし、今日のAI脅威が高まる環境では、これらの遅延は深刻であり、慎重な検討を要します。これらは、優先順位の遅れ、資金不足のコントロール、古い情報に基づいたガバナンス上の意思決定に繋がる可能性があります。

ポジティブな材料も見られます。多くのリーダーは、AIがサイバーリスクを高めていることを認識しており、自社のセキュリティ統制が脅威の進化に追随できていると確信しています。ただし調査では、約3人に1人の経営幹部が自社の統制に十分な自信を持っていないという事実もあり、この楽観論に水を差しています。

なぜこれが重要なのでしょうか。国家主導の攻撃者や他の悪意のあるグループは、AIを利用してサイバー攻撃を加速・拡大し、サードパーティソフトウェア、SaaSアプリケーション、サプライチェーンなどの企業の弱点を悪用しています。[4]

コーディング、推論、自律的なセキュリティ能力が強化されたAIモデルが開発されるにつれ、脅威者によって悪用される前にこれらの脆弱性を特定し修正する取り組みを維持することが、ますます困難になる可能性があります。[5] こうした外部からの脅威は、強力なサイバーリスク管理の必要性を強調していますが、同時に同じくらい重要な内部に対する疑問も浮かび上がらせます。それは、組織が自社環境内で、AIがどのように使用されているかについて明確に把握し、統制出来ているかどうかということです。その内部的な可視化ができなければ、リーダーたちは全体的なサイバーセキュリティ成熟度、リソース、規模に関係なく、AIの死角を持ったまま運営していることになります。

AIガバナンスフレームワークを正式に導入したとしても、サイバー攻撃を防いだり、外部からの脅威を排除したりすることができるわけではありません。しかし、それは別の重要な課題―すなわち、内部におけるAI使用を明確性・説明責任・一貫性をもって統制するという課題―に対応するものです。明確な責任の所在を確立し、使用を許可する基準を定義し、組織全体で使用されるAIシステムとツールの監視に期待値を設定することによって、保証を加速する役割を果たします。

また、調査によると、AIセキュリティに対するより高い信頼は、正式なAIガバナンスの整備と密接に関連していることが示されました。これは、正式なAIガバナンスが、前提や仮定に依存するのではなく、測定可能な形でリーダー層による監督を可能にするためです。

1 この調査では、大規模組織は50億ドル以上の収益を持つ組織として定義されています。
2 中規模組織は、収益が1億ドル以上50億ドル未満の範囲にある組織です。
3 シャドーAIとは、正式な承認、可視性、またはガバナンスコントロールなしに、組織内でAIツール、モデル、またはAI機能を使用することを指します。これはしばしばIT/セキュリティの監視外で行われます。
4 例えば、ディープフェイク詐欺は現在、企業にとって最も急速に拡大しているソーシャルエンジニアリングの脅威であり、Onfidoによれば、北米では1年間で3000%増加しています。
5 2026年4月、Anthropicは、Claude Mythosモデルが主要なオペレーティングシステムやウェブブラウザ全体で数千の潜在的なゼロデイ脆弱性を特定できるため、完全な公開はリスクが高すぎると報告しました。

主な調査結果

01

AIツール活用の把握に大きな死角

- AIの使用状況を完全に把握できていることは稀であり、一般的ではありません。特に中規模企業では、68%が部分的な把握しかできていない、または全く把握できていないと報告しています。
- 大規模組織の中で、従業員のAIツール使用状況を完全に把握していると報告しているのは53%に過ぎません。つまり、47%がシャドーAIに直面しています。

02

脅威認識のギャップ

- 経営幹部や取締役会の30%がAIによるサイバー脅威を重大と見なしている一方、セキュリティ運用部門またはIT部門のリーダーの45%が、AIがその脅威を大幅に増加させたと述べています。
- 経営層がリスクを抽象的に捉えている場合、組織は検知や対応への資金投入を控え、意思決定を遅らせ、AIコントロールテストの成熟度を過大評価する傾向が強まります。

03

セキュリティコントロールに対する信頼は普遍的ではない

- 約3人に1人のリーダーは、セキュリティコントロールがAI主導の脅威に対応できているという強い保証を持っていません。
- 経営幹部から現場の運用チームに下がるにつれて、その信頼はさらに低下します。

04

正式なフレームワーク：保証を加速する仕組み

- 大規模組織の64%が正式なフレームワークを導入・運用しているのに対し、小規模組織では30%です。
- ガバナンスが正式に確立されている場合、リーダーはより強力な保証のトレンド（使用状況把握、トレーニング、防御的なAIの使用）を報告しています。

05

サードパーティによるAI脅威

- 組織の32%が、組み込みAIへのリスク対応策として、ベンダーに対するより厳格なセキュリティ基準の導入を最優先事項に挙げています。
- 僅差で全体の2位になった対応策は、経営層および従業員向けのAI特化型トレーニングの積極的な実施です。

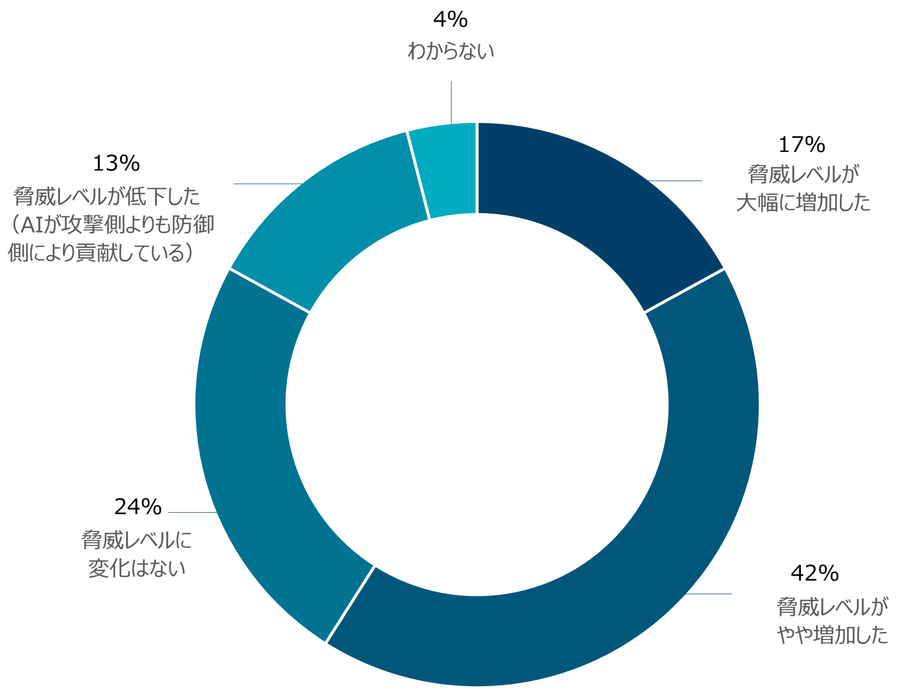
認識のギャップは深刻な結果をもたらす

ITリーダーの約半数は、AIによってサイバーリスクが大幅に増大したと認識している一方で、経営幹部や取締役会メンバーではその割合は30%にとどまります。さらに、セキュリティ統制への信頼は、経営幹部から現場のオペレーションチームに離れるほど低下してきます。

この認識のずれには、現実的な影響が伴います。

- 意思決定の遅れは、特にディープフェイクやその他のAIを利用したサイバー攻撃において、一分一秒が重要であるため、封じ込めやコミュニケーションを妨げる可能性があります。
- サイバーコントロールに対する過信は、AIコントロールやプロセスのテスト不足につながる可能性があり、リーダーがその危険性を十分に理解しないままAIの導入を急ぐ中で、重大なビジネスリスクを招く可能性があります。
- 脅威が過小評価され、管理されない場合、取締役会の支援と資金調達が危うくなります。

図1：脅威レベルのトップライン評価ー 全体結果



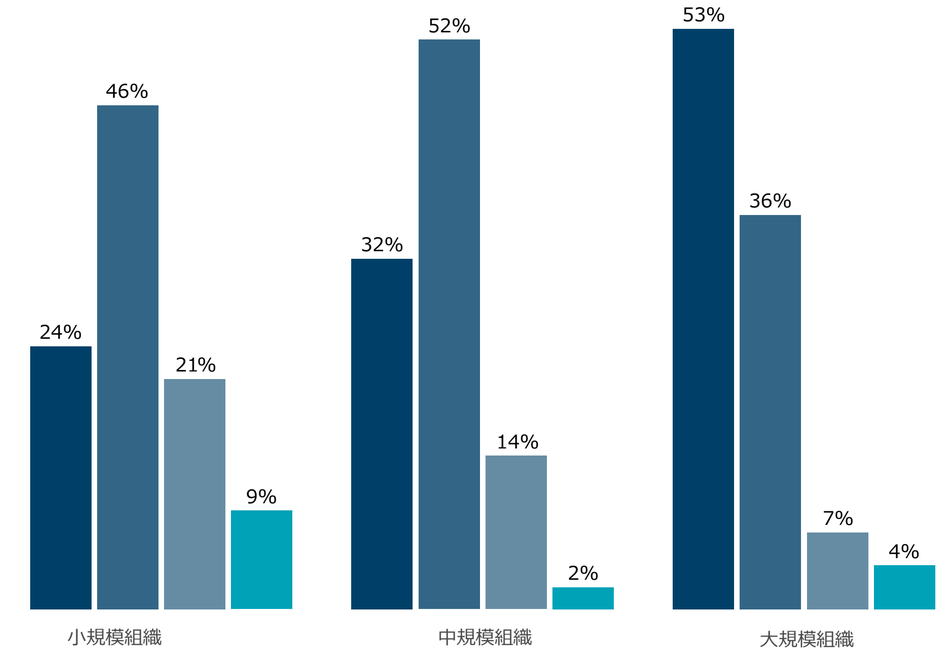
組織規模に関わらず死角はなくならない

3分の2の組織が、適切な監督なしに従業員によって展開または使用されるAIシステムに関して課題を抱えており、その結果、統制上のギャップが生じています。これらの大半は小規模組織[6]であり、検知能力があまり高度でなく、ベンダーの監督が弱く、承認プロセスが厳格でない傾向があります。このような状況では、シャドーAIが見過ごされたまま拡大しやすくなります。

しかし、より多くのリソースを有する中規模および大規模な企業の中でも、AI把握の死角は残るケースがあります。重複したテクノロジープラットフォーム、緩やかな統制、一貫性のないコンプライアンス対応に加え、複数の事業部門や地域、M&Aなどが影響し、47%の大規模組織がAI使用状況を十分に可視化できていないと回答しています。中規模組織では、AIツールの使用状況を十分に可視化できていないと報告している割合は68%に上ります。

重要なポイント：自社のAIの把握に死角がある場合、脅威検知に向けた共通認識や緊急性を組織全体で共有することができません。透明性が欠如すると、未承認のAIツールや拡張機能の無秩序な利用を招き、同意ポリシーの運用が一貫性を欠き、データ保護が弱体化する恐れがあります。

図2：貴組織は、従業員が現在使用している具体的なAIツール（承認済みおよび未承認）の可視化能力をどのように評価しますか。



6　この調査では、小規模組織は1億ドル未満の収益を持つ組織として定義されています。

10社中4社

組織の41%が正式なAIガバナンスフレームワークを導入済みであり、さらに43%がフレームワークの導入中であると回答しています。

正式なフレームワークが重要な理由

調査結果によると、正式なAIガバナンスフレームワークの導入が進むほど、組織規模に関係なくAIツール使用状況を把握できているという相関関係が示されています。また役職別に見ると、正式なフレームワークを導入していると認識しているリーダーほど、AIリスクの増加を「重大」と評価する傾向が強いことが分かりました。

さらに、正式なAIガバナンスフレームワークが、エビデンスに基づく保証の良い指標になることも示されています。具体的には、AIツールの可視化やテストが信頼度の向上と関連しており、これらが高い場合、リーダーはコントロールが脅威の進展に対応できるという確信を持ちやすい傾向があります。

表1：フレームワークは、統制に対する信頼性向上につながる

区分	正式なフレームワークを導入している	AIツールの使用状況を完全に把握している	セキュリティ統制に十分な信頼がない
全体	41%	35%	30%
大規模組織	64%	53%	21%
中規模組織	39%	32%	26%
小規模組織	30%	24%	39%

サードパーティ製の組み込みAI：可視化を左右する領域

組織がAIの使用状況やその活用場所を把握するのに苦労している理由の一つは、テクノロジーベンダーが企業向けツールやプラットフォームへ急速にAI機能を組み込んでいることが挙げられます。

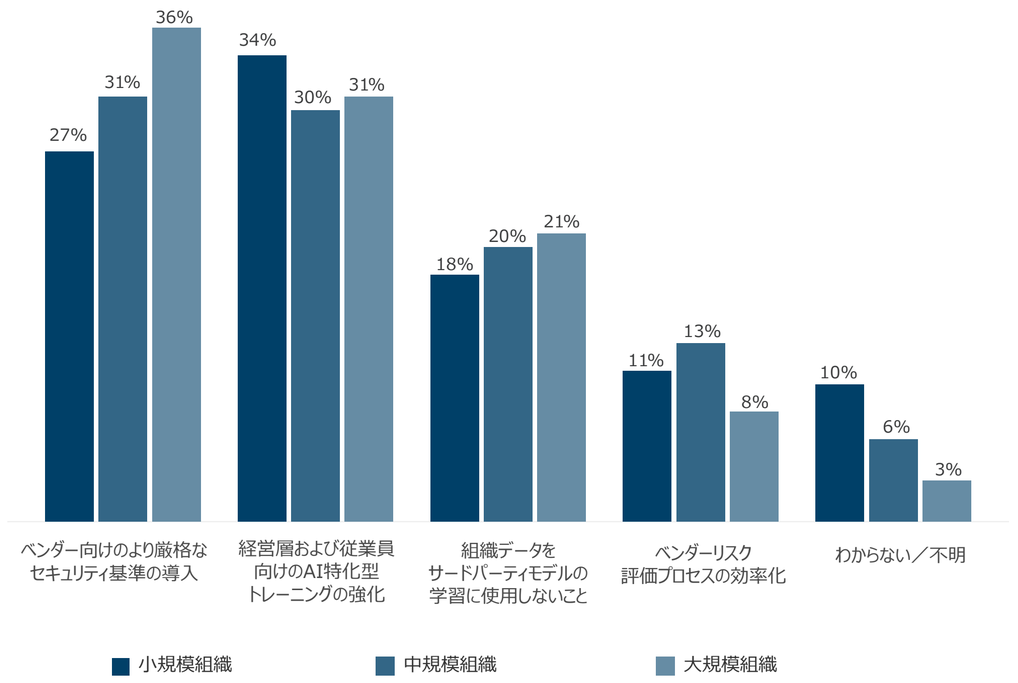
ベンダー管理下にあり、監督や範囲制限の対象外となっているAIの存在は、多くの組織にとって大きな盲点になっています。

調査では、リーダーに対し、ベンダーソフトウェアに組み込まれたAIリスクをどのように管理しているかを尋ねました。その結果、「より厳格なベンダー向けセキュリティ基準の導入」が最優先事項として挙げられ、次いで「経営層および従業員向けのAI特化型トレーニング」が続きました。

また調査結果によると、事業規模が拡大するにつれて、企業はベンダーによってもたらされるAIリスクへの対応策として「強化されたベンダー向けセキュリティ基準」に最も依存する傾向があります。大企業にとって二番目の優先事項は、経営層および従業員向けのAI特化型トレーニングを提供することであり、これは日常的な承認や意思決定における人的判断の重要性を企業が重視していることを浮き彫りにしています。

「自社データをモデル学習に使用しない」という優先事項は、ベンダーAI機能におけるデータガバナンス、データ保持、二次利用への監視が強まっていることを反映しています。特に大企業における関心の高まりは、成熟した契約管理や監査可能性に対する期待が高まっていることを示しています。

図3：サードパーティベンダーのソフトウェアに組み込まれたAIがもたらすリスク管理において、貴組織が最も重視している事項は何ですか。



※ 大規模組織の1%が「その他」を選択

防御型AIとトレーニング：信頼性を向上する究極の方法

調査対象となった組織の約4分の1で、セキュリティ対策基盤においてAIが広く活用されています。規模別に見ると、大規模組織はセキュリティ目的でAIを最も積極的に活用している層の42%を占めており、中規模組織は21%、小規模組織は15%にとどまっています。

現在の脅威が高まっている環境において、セキュリティ対策基盤にAIを組み込むことで、組織は攻撃者がすでに展開している速度とパターン認識の優位性を得ることができます。同様に重要なのは、基本的なAI教育を超えた包括的なトレーニングを実施し、文化的な変革を促進し、リーダーシップや従業員のサイバーセキュリティ対応への信頼性を高めることです。

調査結果によれば、防御型AI対策と強固なトレーニングを組み合わせている組織は、従業員が企業全体でAIツールをどのように使用しているかについて、より適切に把握できている傾向があります。この理解の向上は、前述の通り、リーダーやあらゆる規模の企業におけるセキュリティ能力に対する信頼度の高まりとも関連しています。

見えないものは守れない―有効な施策への投資を

AIセキュリティリスクの管理に最も信頼を持つ組織は、意図（AIリスクを真剣に捉える）を、確証（可視化し、ガバナンスをかけ、防御できる）に変える具体的な能力に最も多く投資している組織です。
ここでは主な能力・施策をまとめます。

- 正式なAIガバナンスフレームワーク：明確な利用規則、所有権、責任、そして実効性のあるガードレールを企業全体で設け、統制を上回るスピードでAI利用が拡大することを防ぎます。
- AIツールのモニタリング：見えないものは管理できません。モニタリング機能への投資により、特にシャドーAIなどの脅威を早期に検出し、データ保護を含むコンプライアンスを強化するとともに、統制が有効に機能していることを証明できます。
- 組織の準備態勢とレジリエンス（回復力）：人為的な失敗を減らし、AIと共に働く「業務のあり方」に一貫性を構築します。
- AIを活用しAIに対抗する：セキュリティ対策基盤にAIを活用することで、サイバー攻撃の迅速な検知、パターン認識の精度向上、そしてAIによって加速される脅威への対応力が強化されます。
- 組み込みAIに対するベンダーコントロール：SaaSやサードパーティプラットフォーム内でAI機能が急速に拡大する中、新たに増大する死角を解消します。AIをセキュリティ対策基盤に活用している場合、より厳格なベンダーセキュリティ基準とAI特化型トレーニングが不可欠です。

プロティビティの専門家のご紹介

Andrew Retrum

マネージングディレクタ、プロティビティ

Tom Andreesen

マネージングディレクタ、プロティビティ

調査概要

本AIパルス調査は2026年2月に実施されました。約900名（n=863）の参加者がアンケートに回答し、150名の取締役会メンバーや経営幹部が含まれています。ただし、AIに関する技術的、業務的、経営的観点をより深く理解するために、本レポートでは経営層、取締役、ITリーダーからの回答を個別に抽出して分析しています。

経営幹部の参加者の中で、CEOが最大の割合（37%）を占め、次いでCTO（19%）、CIO（13%）、CFO（11%）、COO（10%）が続きました。機能別では、ITリーダーが回答者の約3分の1（31%）を占め、業務部門が21%、財務部門が10%を占めています。

回答は多様な業界から収集され、特にテクノロジー（10%）、政府機関（8%）、小売（8%）、製造（7%）、航空宇宙および防衛（6%）が多くを占めました。地理的には、調査は広範な国際的な範囲を反映しており、米国が回答者の41%を占め、次いでインド（14%）、英国（12%）、オーストラリア（10%）、カナダ（9%）が続きます。

年間収益が1億ドルから49.9億ドルの中規模組織が回答者の最大の割合を占め、年間収益が1億ドル未満の小規模組織は全体の4分の1以上を占めました。年間収益が50億ドル以上の組織は、回答者の約5分の1を占めています。

プロティビティのAIに関するケイパビリティについて

プロティビティは、測定可能なビジネス価値を創出するAIソリューションの優先順位付けから構築、提供までを一貫して支援しています。私たちは、革新性があり、かつ適切に統制され、事業に対して説明責任を果たせるAIの実現に注力しており、すべてのAIソリューション提供が安全で、透明性が高く、お客様の目標と整合していることを重視しています。当社の専門家チームは、クライアントが安心して活用できるAIソリューションを構築し、強固なガバナンス、責任ある設計、そして全社規模で自信を持ってスケールできる仕組みによって、企業の信頼と成果を支えます。

また、変革のマネジメントや定着化の最大化を通じて、人材が学び、適応し、自信を持ってAIを活用・リードできるよう支援します。私たちのAIスタジオ、独自のアクセラレーター、技術パートナー、AIファクトリーを通じて、戦略策定からソリューション開発、導入、運用後のライフサイクル管理までを網羅するエンドツーエンドの支援を提供しています。これにより、AIを安全かつ効果的に、そして継続的に価値を生み出す存在として維持するための、信頼できるマネージドサービスパートナーとして、お客様を支援します。

プロティビティについて

プロティビティは、クライアントがビジネスの変革や防護、また計画された事象や予期せぬ事象に対応できるように支援するグローバルコンサルティングファームです。25カ国、90を超える拠点で、プロティビティとそのメンバーファームはクライアントに、テクノロジー、AI、データ、オペレーション、ファイナンス、法務、コンプライアンス、人事・組織、マーケティング、デジタル、リスク、内部監査の分野において、高い専門性とお客様ごとに的確なソリューションを提供しており、組織の変革の加速、リスクへの対応、最も重要な価値の保護を実現します。

2015年以降、米国フォーチュン誌の働きがいのある会社ベスト100に11年連続で選出され、Fortune 100の80%以上、Fortune 500の約80%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティはRobert Half（RHI）の100%子会社です。

Face the Future with Confidence®

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. 0426

protiviti®
Global Business Consulting