変化し続ける
AI環境の中で、
セキュリティ強化に
向けた道筋を
どう描くのか

エージェント型AI、
自律的な脅威、防御の未来像

The better the question.
The better the answer.
The better the world works.

EY
Shape the future
with confidence

本調査について

2025年12月、Ernst & Young LLPは、情報セキュリティを統括・管理するディレクター職以上の情報セキュリティリーダー（経営層を含む）500人を対象に委託調査を実施しました。回答企業は、銀行・資本市場、ウェルス&アセットマネジメント、保険、石油・ガス、テクノロジー、工業製品、プライベートエクイティ、メディア・エンターテインメント、消費財、小売、ライフサイエンス、ヘルスケアなど、幅広いセクターにわたり、年間売上高は5億米ドル以上です。本調査は、情報セキュリティリーダーが、セキュリティ運用において人工知能（AI）の価値をどのように定量化し、今後2年間の予算およびテクノロジーに関する計画をどのように策定しているのかを把握することを目的としています。本レポートでは、実証的な調査結果に基づき、AI関連のリソースおよび投資から最大限の価値を引き出すための重要な示唆を提示しています。

1 サイバーセキュリティにおけるAIの最新動向

サイバーセキュリティ分野においてAIは、自動化や業務効率の向上といった機会をもたらす一方で、悪意をもって危害を加えようとする者の能力を大きく増幅させ得るという脅威も内包しています。いずれの場合においても、AIはサイバーセキュリティの在り方そのものを大きく変えつつあります。

こうした脅威の切迫に加え、AIが企業にもたらす変革のスピードとその影響の大きさを踏まえると、AIの活用には包括的で責任あるアプローチが不可欠です。一方で多くの企業では、AI導入に際し「信頼」が障壁となっています。機能性や実用性が導入を後押ししている反面、アウトプットへの信頼が十分に確立されていないことが、ユーザーによるAIを活用した新たなワークフローの受容を妨げています。AIに対する信頼は、抽象的な意識論や単一の統制で確立できるものではなく、サイバーセキュリティやガバナンス、コンプライアンス、透明性、説明可能性、倫理を横断的に組み込んだ「仕組み」として設計される必要があります。信頼の基盤が確立していない場合、AIの能力がいかに高度であっても、パイロット導入の段階を超えて本格的な運用に移行することは困難です。

AIは企業防御の要ですが、同時に切迫した脅威をもたらします。こうした二面性が、情報セキュリティリーダーの一見相反する認識として表れています。AIをサイバーセキュリティの中核的な防御ソリューションと捉えている情報セキュリティリーダーは96%にも及び、95%がすでにAIを活用したサイバーセキュリティ運用を行っています。その一方で、96%が、AIを悪用したサイバーセキュリティ攻撃を自社にとって重大な脅威と考えています。AIによって引き起こされる大規模なセキュリティ侵害に対して、自社の防御能力を強く確信している企業は46%と、半数に満たない状況です。また、回答企業の67%は依然としてパイロット段階にあり、AIテクノロジーの試行や戦略検討にとどまっています。

情報セキュリティリーダーの約半数（48%）が、過去1年間に発生したサイバー攻撃のうち、少なくとも4分の1はAIを活用したものだったと回答しています。こうした状況から、サイバー脅威への備えは喫緊の課題となっています。

情報セキュリティリーダーは、サイバー脅威への対応は、単にテクノロジーを導入するだけでは不十分であると認識しています。信頼に足る運用フレームワークを構築し、投資対効果（ROI）を実現するためには、投資の拡大、人間の判断を組み込むHuman-in-the-loop型フレームワークの確立と継続的な運用、そしてサイバーセキュリティガバナンスの成熟が、相互に連動して機能することが不可欠です。しかし、現状では、サイバーセキュリティにAIを活用している情報セキュリティリーダーの85%が、AIを悪用したサイバー脅威に対応するには、現在の予算では不十分だと考えています。また、AIサイバーセキュリティにおいて、ガバナンスの枠組みが完全に最適化され、企業文化として定着していると回答した企業は20%にとどまっており、依然として改善の余地が大きい状況です。

総じて本調査では、サイバーセキュリティにおけるAIの活用について一定の成果や前進が見られる一方、課題も残されていることが明らかになりました。また、AIが現代的なサイバーセキュリティプログラムの基盤であるという認識が広く共有されていることを示しています。

AIを悪用したサイバー攻撃を、自社にとって重大な脅威と捉える情報セキュリティリーダーの割合

2 財務面の実情：予算、コスト、投資動向

情報セキュリティリーダーの間では、自律型防御の導入が進み始めています。また、ほぼすべての回答者が、AIを戦略的に活用することで、予防型および防御型のサイバーセキュリティ戦略の在り方が大きく変わると確信しています（予防型・防御型いずれも99%）。

しかし、経営層からの防御強化に向けた資金拠出は、その必要性に見合う水準に達しているとは言えません。サイバーセキュリティにAIを活用している情報セキュリティリーダーの85%は、マクロ経済の不安定さも一因となり、現在の予算ではAIを使ったサイバー脅威に対応するには不十分であるとしています。例えばヘルスケア分野では、AI技術そのものが高コストであることに加え、人材育成や業務プロセスへの適応に伴う負担が、AI導入が進みにくい要因の1つとなっています[1]。

AIを戦略的に活用することで、予防型サイバーセキュリティ戦略が大きく変わると回答した情報セキュリティリーダーの割合

一方で明るい材料としては、経済的な圧力が続く中でも、情報セキュリティリーダーは予算の増加を見込んでいます。サイバーセキュリティ予算の25%以上をAI活用型サイバーセキュリティソリューションに充てる情報セキュリティリーダーの割合は、今後2年間で現在の9%から48%へと大きく増加する見通しです。総投資額ベースでは、サイバーセキュリティにAIを活用している情報セキュリティリーダーの67%が2年後に500万米ドル以上、34%が同期間に1,000万米ドル以上の投資を見込んでいます。

すでに投資を行っている企業では、その効果が着実に表れ始めています。こうした成果は、最近実施されたEY US AI Pulse Survey（第4回）[2]でも示されています。同調査でAI投資とそのROIについて尋ねたところ、すべての事業部門または複数部門にわたりAIに1,000万米ドル以上を投資している企業の経営層の71%が、過去1年間でAI関連の生産性が大幅に向上したと回答しています。一方、AI投資額が1,000万米ドル未満の企業では、その割合は52%にとどまっています。

99%

AIを戦略的に活用することで、防御型サイバーセキュリティ戦略が大きく変わると回答した情報セキュリティリーダーの割合

1. Andrei Kasyanau, Balancing The Cost of AI in Healthcare: Future Savings Vs. Current Spending, *Forbes*, www.forbes.com/councils/forbestechcouncil/2024/04/17/balancing-the-cost-of-ai-in-healthcare-future-savings-vs-current-spending/（2024年4月）
2. The dividend age: "How AI is turning promise into payoff," EY（2025年12月）

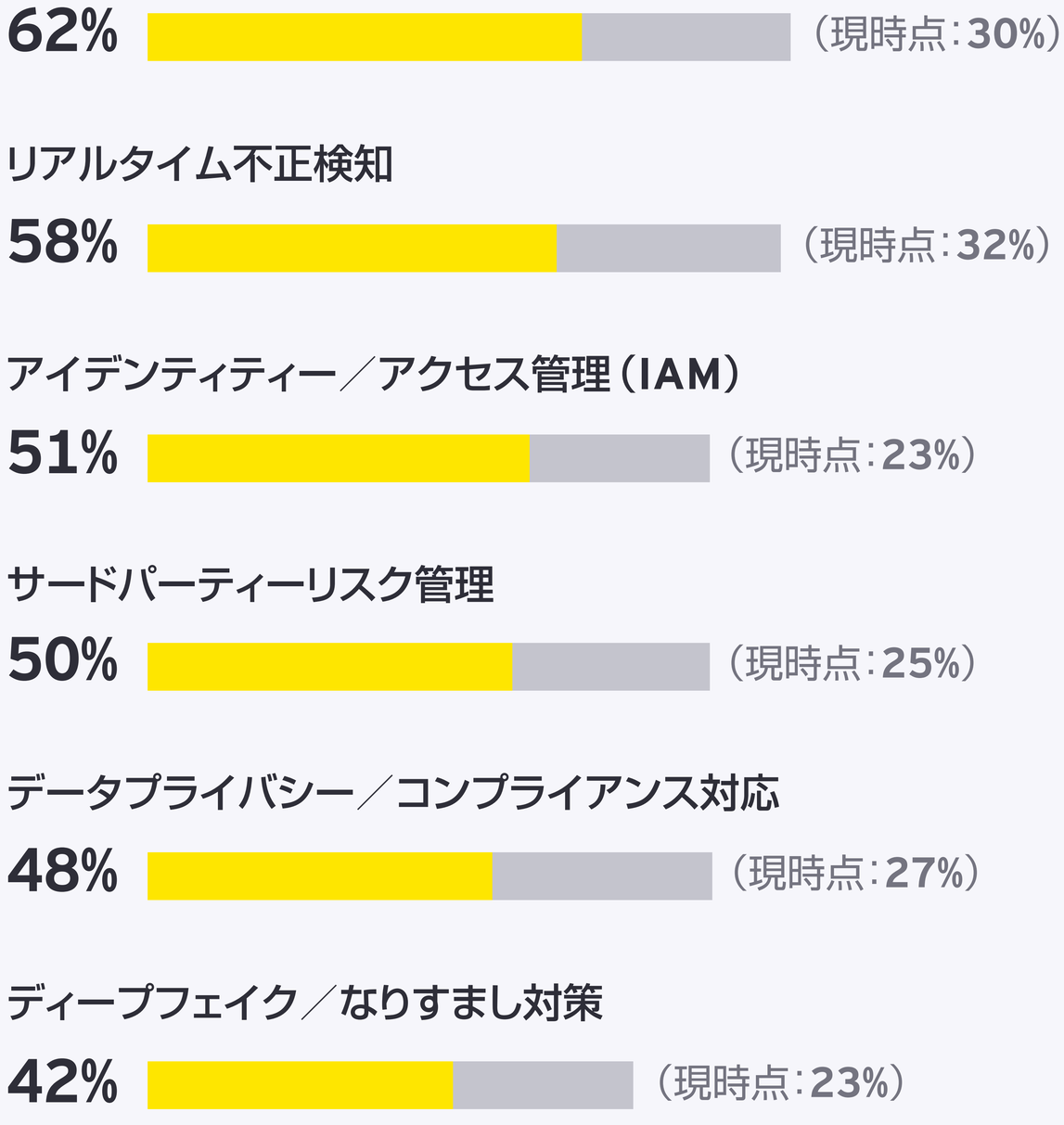
3 投資対効果：進展は緩やかだが、見通しは楽観的

サイバーセキュリティ分野でエージェント型AIの導入を進める企業では、投資対効果や業務効率の向上といった初期的な成果がすでに見え始めています。ただし、数値面では十分な成果が表れているとは言えません。

サイバーセキュリティにAIを活用している情報セキュリティリーダーの約半数（46%）が、エージェント型AIソリューションの導入によるコスト削減額が100万米ドル未満にとどまっていると回答しています。さらに12%は、コスト削減効果を把握していない、あるいは得られていないとしています。こうした結果は、企業間でばらつきがあるものの、多くが定型業務の自動化にとどまっており、コスト削減効果は限定的です。依然として、改善の余地が大きいことがうかがえます。

次のフェーズでは、エージェント型AIの適用範囲をより中核的な業務へと段階的に拡大するとともに、人材を戦略性の高い業務へとシフトさせていくことが重要となります。情報セキュリティリーダーは、2年以内にエージェント型AIによる運用が主流になるとされている新たな領域に注目しています（図1）。

図1：今後2年間で、サイバーセキュリティ機能の多くがエージェント型AI主導へ



AIの活用において、企業が評価軸として常に追求しているのは、売上高や利益といった数値指標だけではありません。サイバーセキュリティ分野では、リスク低減や競争力強化といった観点も重要視されています。例えば、異常の検知（67%）、脅威検知の高度化（60%）、さらには攻撃対象となり得る脆弱性の事前特定（59%）といった領域で、情報セキュリティリーダーはサイバーセキュリティにAIを活用するメリットを認識しています。これらは財務指標には直接表れにくいものの、平均復旧時間（MTTR）や平均検知時間（MTTD）の短縮、誤検知率（FPR）の低下といった、具体的かつ測定可能な指標の改善につながります。実際、情報セキュリティリーダーの97%が、今後2年間における市場での自社の競争優位性は、エージェント型 AIを活用したサイバーセキュリティ防御の成熟度合いによって左右されるとみています。

今後2年間における自社の競争優位性は、
エージェント型AIを活用したサイバー防御の
成熟度により左右されると考える
情報セキュリティリーダーの割合

最終的に目指すのは、人とAIエージェントが協働する、いわゆるマイクロソフトが提唱する「フロンティア組織」です。

4 Human-in-the-loop型サイバーセキュリティ：人材ギャップとガバナンスリスク

企業の間でAI主導のサイバーセキュリティツールの導入が加速する中、人の関与はこれまで以上に重要になっています。

AIを活用することで、アナリストは業務効率を高め、より付加価値の高い業務に注力できるようになります。一方、多くの企業では、依然として深刻な人材不足が続いており、高度な専門性を備えた人材によるHuman-in-the-loop型の統制の必要性に十分に対応できていないのが実情です。Human-in-the-loop型のサイバーセキュリティは、単なるリスク統制のための手段ではありません。それは、企業がAIによる判断を信頼する上で欠かせない、重要な枠組みです。人による判断、状況理解、説明責任をAI主導のワークフローに組み込むことで、自動化は責任ある意思決定を損ねるものではなく、むしろそれを補完・強化するものであるという認識が企業内に醸成されます。

重要なセキュリティ上の意思決定すべてにおいて、人の関与を必須とする要件を設けていると回答した情報セキュリティリーダーは85%に上ったほか、98%が、サイバーセキュリティにおけるエージェント型AIの投資対効果は、Human-in-the-loopを前提とした明確な統制戦略に左右されると考えています。こうした調査結果は、人による関与が、省略可能な付加的プロセスではなく、AIを活用した意思決定を支える、戦略的に不可欠な要素であることを明確に示しています。

企業がAIを活用したセキュリティツールの導入を拡大する中で、アナリストには、AIの判断を検証し、その意味や背景を読み解く役割が求められています。しかし、こうした要請に見合う高度な知識を備えた人材は不足しています。本調査でも、情報セキュリティリーダーの90%が、AI主導のセキュリティソリューションや防御に精通した専門人材の採用・定着に苦慮していると回答しています。また、89%が、AIを悪用したサイバー攻撃に対応するための研修を受けていないサイバーセキュリティ人材を、自社にとって最大のリスク要因と捉えています。こうした結果は、AIを導入するだけでは人に起因するリスクは低減されず、AIを適切に統制できる知見を備えた人材があってこそ、人的リスクの低減が可能になることを示しています。

特に、人材不足が深刻化する状況下では、対応策として研修や人材育成の重要性が一層高まります。従業員は職を失うことを恐れている、という見方もありますが、研修やスキルアップを自身の成長やキャリア形成につながるものだと捉えている従業員は少なくありません。EY Agentic AI Workplace Surveyによると、情報セキュリティ担当者に限らず、デスクワーカーの89%が、AIが業務に広く組み込まれた職場において、価値ある存在であり続けるためにはスキルアップやリスキリングが不可欠であると考えています[3]。一方で、デスクワーカーの59%が、エージェント型 AIに対応するためのスキル育成研修が十分に整っていない点を、企業が取り組むべき課題として指摘しています。

これを裏付けるように、高い専門性を備えたアナリストを擁する企業では、AIはこうした人材の能力を大きく引き出す推進要因として機能しています。サイバーセキュリティにAIを活用している企業の情報セキュリティリーダーの97%が、AI主導のサイバーセキュリティソリューションの導入によってアナリストの業務効率が明確に向上したと回答しており、同じく97%が、アナリストはより付加価値の高い戦略的な業務に注力できるようになったとしています。AIは人の専門知識に取って代わるものではなく、アナリストをより高次の推論、ガバナンス、意思決定の妥当性検証といった役割へと押し上げています。その結果、サイバーセキュリティ分野では、AIと人の能力が深く相互依存する関係が定着しつつあります。

最終的に目指すのは、人とAIエージェントが協働する、いわゆるマイクロソフトが提唱する「フロンティア組織」です[4]。これは、必要なときにAIの能力を即座に活用できる環境と、人とAIエージェントによるハイブリッドチームを前提に業務が設計された企業を指します。こうした企業では、迅速に規模を拡大し、高い俊敏性をもって事業を推進し、同業他社よりも速いスピードで価値を創出することが可能になります。この考え方をサイバーセキュリティに当てはめると、人を中核に据え、AIエージェントと協働しながらその挙動を指揮・統制することで、セキュリティを高度に統合された自動化機能へと進化させていくことを意味します。

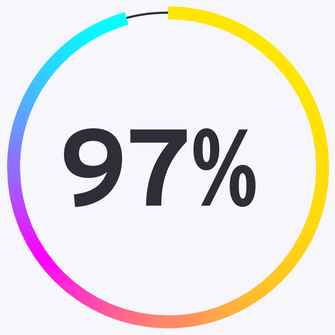
3. Unchanneled worker enthusiasm squanders agentic AI, EY（2025年10月）

4. The year the Frontier Firm is born, Microsoft Work Trend Index Annual Report, *Microsoft*, www.microsoft.com/en-us/worklab/work-trend-index/2025-the-year-the-frontier-firm-is-born?msockid=0a8508ac123f61690e411c5b13d96070（2025年4月）

5 責任と拡張性を備えたAIサイバーセキュリティを支えるガバナンス

企業がAIを活用したサイバーセキュリティの導入を急ぐ中、責任性・信頼性・拡張性を備えた展開を実現する上で、ガバナンスは不可欠な基盤として位置付けられるようになっています。

すでに多くの企業がガバナンスのフレームワークを中核プロセスに導入、あるいは組み込んでおり、ガバナンスは、AIの潜在力を具体的なビジネス価値へと転換する要諦として、その重要性が一段と認識されるようになっています。一方で、ガバナンスが脆弱または成熟していない場合、データ侵害やコンプライアンス違反といった重大なリスクにさらされます。



サイバーセキュリティでのAIの活用において、強固なガバナンスフレームワークはAIの潜在能力を収益性のあるビジネス価値へと転換する上で不可欠だと回答した情報セキュリティリーダーの割合

すでに企業の間では、ガバナンスの成熟化に向けた取り組みが進み始めています。AIセキュリティのガバナンスフレームワークを完全に最適化し、企業文化として定着させていると回答した情報セキュリティリーダーは20%にとどまるものの、一定の進展は見られます。実際、情報セキュリティリーダーの半数以上（51%）が、ガバナンスフレームワークを主要な業務プロセスに組み込み、運用していると回答しており、さらに26%は、関連する事業部門全体にわたってガバナンスを展開・統合しているとしています（図2）。しかし、こうした取り組みの進捗度の差は、信頼の確立をめぐる大きな課題を浮き彫りにしています。ガバナンスが日々の意思決定や企業文化に根付いていない場合、AIシステムが設計通りに機能していたとしても、広範な導入や長期的な価値創出に必要な信頼を得られない可能性があります。

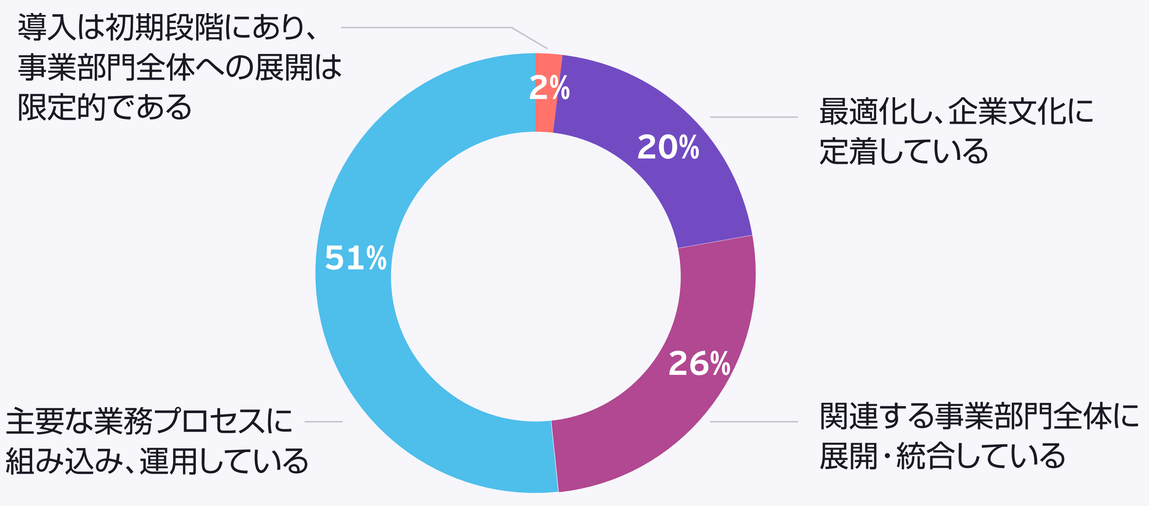
ガバナンス強化に向けた取り組みは、単なる形式的・手続き的な対応にとどまるものではありません。企業の多くは、サイバーセキュリティにおいてAIの真の価値を引き出す上で、ガバナンスが決定的な役割を果たすと考えています。実際、サイバーセキュリティにおいてAIガバナンスフレームワークが整備されている企業の情報セキュリティリーダーの98%が、AIを責任ある形で活用する上でガバナンスは欠かせないと認識しており、97%は、サイバーセキュリティでのAIの活用において、強固なガバナンスフレームワークはAIの潜在能力を収益性のあるビジネス価値へと転換する上で不可欠だと考えています。

こうした調査結果は、AI活用におけるガバナンスの有無が決定的な差を生むことを示しています。ガバナンスが不十分なままでは、AIは可能性を秘めつつも、十分に統制された形では機能しません。一方、適切なガバナンスの下では、AIは信頼性と拡張性を備え、事業戦略と整合した形で価値を発揮する基盤となります。

ガバナンスへの投資を怠った場合のリスクも明確です。ガバナンスが脆弱であったり、一貫性を欠いていたりすると、企業は深刻なサイバーセキュリティ上の脅威にさらされることになります。その主な影響として、データ侵害リスクの高まり（58%）、エージェント型AIの挙動に起因するコンプライアンスリスク（58%）、データ漏えい（54%）などが挙げられます。これらは、ガバナンスの欠如が実務上の脆弱性に直結していることを示しています。本来はサイバーレジリエンスの強化に寄与するはずのAIも、統制が不十分であれば、結果として企業のリスクを増幅させかねません。

AIの活用に伴うこうした課題は、外部環境の不確実性によって、さらに深刻化しています。本調査で、サイバーセキュリティのフレームワークを有する情報セキュリティリーダーの91%が、AIサイバーセキュリティに関する政府レベルの規制が十分に整備されていないことに起因するコンプライアンスリスクに懸念を示しています。こうした状況を背景に、ガバナンスはもはや企業内部における先進的な取り組みにとどまらず、戦略上の必須要件となっています。規制の先行きが不透明な環境においては、成熟した社内ガバナンスが、AIの導入・活用における安全性・信頼性・コンプライアンス、さらには将来的な要件との整合を確保する基盤となり、外部政策の変化に左右されることのない安定的な運用を支えます。

図2: サイバーセキュリティにおけるAIガバナンス体制の成熟度*



*四捨五入のため、合計が100%にならない場合があります

Journey to the new way

重要な示唆と次に取るべき行動

今回の調査結果から、次の2つの現状が浮き彫りになりました。AIは現代のサイバー防衛に不可欠な存在となっている一方で、早急な対応を要する、新しく複雑なリスクも同時にもたらしています。こうした状況を踏まえ、AIを活用した価値創出を実現するため、情報セキュリティリーダーには次の4つの重要領域での対応が求められます。

1 予算の現実を踏まえ、投資をAI主導のサイバーセキュリティへと重点的に振り分ける

多くの企業では、サイバー脅威の進化スピードに資金面での対応が追いついていません。AIを悪用した攻撃に対抗し、防御能力の高度化で後れを取らないためには、テクノロジー投資全体を戦略的に見直し、AI主導のサイバーセキュリティを優先領域として位置付ける必要があります。投資が不十分な場合、自律的な脅威へのリスクが高まるだけでなく、AIを責任ある形で、安全かつスケーラブルに展開・活用していく能力も制約されます。

2 AI投資でROIを確保するには、エージェント型AIを中核のセキュリティ機能により深く組み込むことが不可欠である

実質的な投資対効果（ROI）は、エージェント型AIをサイバーセキュリティに組み込んでこそ初めて得られます。パイロット段階やタスク単位の自動化にとどまらずに、エージェント型AIが主導する統合的なセキュリティ運用へと移行した企業は、財務面でのリターンに加え、レジリエンス、対応スピード、分析精度の面でも、測定可能な改善を実現しています。

AIは、サイバー脅威の様相とサイバーセキュリティの在り方そのものを変えています。これら4つの重要領域における対応を怠れば、競争上の後れを取るリスクにつながりかねません。

3 AI活用において、Human-in-the-loopによる統制とスキル育成は欠かすことのできない前提である

AIシステムの自律性が高度化するにつれて、専門性を備えた人材による統制の重要性は、低下するどころか、むしろ高まっています。Human in the loop型の戦略を効果的に機能させるには、AIのアウトプットを適切に検証できる知見を備えた人材が不可欠です。しかし、AIを活用したサイバーセキュリティにおいて、慢性的な人材不足やスキルギャップが、最も深刻な脆弱性の1つとなっています。そのため企業には、既存人材のリスキリングやスキルアップに積極的に投資し、人とAIエージェントが効果的に協働できる体制を整えるとともに、ますます自律化が進むシステムに対する統制を維持することが求められます。

4 ガバナンスは、信頼性と拡張性を備えたAIサイバーセキュリティを支える基盤である

ガバナンスフレームワークは、AIシステムが、安全かつコンプライアンスと透明性が確保された形で運用されるためのガードレールです。その枠組みにより、AIの活用は企業が目指す価値や規制当局の期待に沿ったものとなります。サイバーセキュリティ、コンプライアンス、倫理、透明性、説明可能性がガバナンスに横断的に組み込まれていない場合、AIへの取り組みはリスク低減になるどころか、かえってリスクを増幅させかねません。ガバナンスを「継続的に改善され、企業文化や業務に組み込まれた基盤」として捉えている企業こそが、信頼を構築し、新たなリスクを管理し、AIイノベーションを持続的な競争優位性へと転換する上で、最も有利な立場にあります。

EY Cybersecurity Roadmap 調査について

本調査は、12のセクターにおいて年間売上高5億米ドル以上の企業に所属し、自社の情報セキュリティ（データおよびシステムを含む）を統括する米国在勤のディレクター職以上の情報セキュリティリーダー500人（経営層216人、その他284人）を対象に、2025年12月9日から2026年1月8日にかけて、オンラインで実施されました。全体サンプルの誤差範囲は、95%信頼区間で±4ポイントです。セクター別内訳は、銀行・資本市場（N=50）、ウェルス&アセットマネジメント（N=50）、石油・ガス（N=30）、消費財（N=50）、テクノロジー（N=30）、工業製品（N=30）、ライフサイエンス（N=50）、プライベートエクイティ（N=30）、小売（N=50）、メディア・エンターテインメント（N=30）、ヘルスケア（N=50）、保険（N=50）です。分析に当たっては、各セクターが均等になるようウエート調整を行いました。

執筆者

Ayan Roy
EY Americas Cybersecurity Competency Leader

Dan Mellen
EY Global Cyber Chief Technology Officer

Esther Lee
EY Americas Consulting, Cybersecurity

Ganesh Devarajan
EY Americas Consulting Cyber Risk Practice Leader

本記事の作成に当たり協力いただいた、Martin Glowik、Esther Lee、David Cooperに感謝の意を表します。

EY Japanの窓口

小川 真毅
EYストラテジー・アンド・コンサルティング株式会社
サイバーセキュリティ共同リーダー／
EY Japan金融サービス　パートナー

お問い合わせ

EY | Building a better working world

EYは、クライアント、EYのメンバー、社会、そして地球のために新たな価値を創出するとともに、資本市場における信頼を確立していくことで、より良い社会の構築を目指しています。

データ、AI、および先進テクノロジーの活用により、EYのチームはクライアントが確信を持って未来を形づくるための支援を行い、現在、そして未来における喫緊の課題への解決策を導き出します。

EYのチームの活動領域は、アシュアランス、コンサルティング、税務、ストラテジー、トランザクションの全領域にわたります。蓄積した業界の知見やグローバルに連携したさまざまな分野にわたるネットワーク、多様なエコシステムパートナーに支えられ、150以上の国と地域でサービスを提供しています。

All in to shape the future with confidence.

ey.com/ja_jp