DARKTRACE

AI サイバーセキュリティの現状

2025年レポート

サイバーセキュリティにおけるAIの
役割拡大についての世界的な視点

目次

エグゼクティブサマリー

サイバーセキュリティという分野は、これまでも常に変化が速く、複雑に入り組んでいました。この絶え間ない変化により実務者は常に新しい何かを学ぶ必要に迫られ、この分野を興味深いものにしています。しかしここ数年、AI（Artificial Intelligence）技術の急激な進化により、既に急速であった変化のペースがさらに加速し、攻撃者と防御者の間の戦いの条件が書き換えられようとしています。今日のセキュリティリーダーはこうした状況に先手を打つ戦略を構築し、攻撃の高度化に対応して防御を進化させられるようにしなければなりません。

サイバーセキュリティにAIの力を活用：今がその時

当社は1,500名を超える世界中のサイバーセキュリティおよびITプロフェッショナルを対象に、サイバーセキュリティにおけるAIに対する彼らの態度を理解するための調査を実施しました。この調査では、彼らが直面する脅威にAIがどのように影響しているか、および現在および将来においてAIが予防、脅威検知、インシデント対応、および修復ワークフローにどのような役割を果たすと考えているかを尋ねました。

この調査を実施するのは今回が2年目になります。そこで明らかになったことは、ますます多くのCISOが、AIを使った脅威が自社に与える影響は顕著であると認めていることです。大多数の回答者（89%）が、これらの脅威が今後も自社の組織を苦しめ続けると考えています。実務担当者は特に大きな心配を抱えており、SecOpsチームメンバーはCISOよりも高いレベルでAIの長期的影響を懸念していました。

この調査の主なポイント

AI サイバー脅威は現実のものであり、行動を起こすべき時は今である。

78% のCISOが、現在のサイバー脅威にAIが影響していると確信しており、自社を守るために対策を急いでいると答えています。サイバープロフェッショナルはAIサイバー脅威に対する準備が12か月前よりも格段に進んでいると感じていますが、**45%**はこの現実に対する準備がまだできていないと感じています。

防御 AI は SOC の一部となりつつあり、セキュリティチームの人員不足を補っている。

「人員不足」がAIによる脅威を防御する上での最大の障害と考えられているにもかかわらず、サイバーセキュリティスタッフの増員は調査回答者の優先順位の最下位であり、2025年にサイバーセキュリティスタッフの増員を計画していると回答した人は**わずか11%**であり、2024年よりも減少していました。

CISO はデータを組織内に保持しておくことのできる、プロアクティブかつプラットフォームベースのソリューションを求めている。

CISOはポイント製品よりも範囲の広いプラットフォームを好んでおり（**89%**）外部にデータを共有する必要のないソリューションを望んでいました（**82%**）。大多数の回答者は、よりプロアクティブになるためにAIが役立つということを確信していました。

サイバーセキュリティステークホルダーは、昨年よりもこの新しい現実に対する準備ができていると感じているものの、調査回答者の半数近く（45%）は、AI による脅威に対する自社の組織の準備度について自信を持っていません。また、サイバーレディネスを強化したいという強い意欲が見られ、組織全体に AI セキュリティポリシーを導入するといったリスク削減策について活発な議論がされています。しかし、AI の安全かつセキュアな利用についての正式な方針については、実際に導入した組織よりも、まだ議論している組織のほうが多い状況です。

AI 教育も始まりつつあり、AI（あらゆる形態の）を理解するステークホルダーの数も増えていますが、まだ道のりは長いと言えます。本年度の調査の参加者の半数以上（56%）が、自社の組織で使用しているサイバーセキュリティソリューションでどのタイプの AI が使われているか、詳しくは知らないことを認めています。昨年度見られた傾向は、サイバーセキュリティ防御において生成 AI が果たす役割を過大評価することでしたが、その傾向は本年度も続いていました。

実務者に力を与え、AI テクノロジーから得られる価値を最大化するには、教育とトレーニングが鍵となるでしょう。しかし、リーダーもまた、さまざまなタイプの AI の違い、それらがどのようにサイバーセキュリティソリューションに適用されているか、そしてそれらがどのように人間のアナリストの能力を補強し、SecOps チームを強化することにより同じリソースでより多くのことを達成できるか、について理解しなければなりません。

組織が AI ツールを取り入れ、ワークフローを効率化し、擬陽性を削減し、これまでに見られたことのない脅威の検知を実現するそれらの能力を活用していくために、早急な AI 教育の必要性は高まる一方です。脅威アクターは状況を一変させる潜在力を持つ AI をいち早く利用しようとしており、主要な SecOps プログラムも同様に AI に取り組んでいます。攻撃者は常に最も弱い標的を探しています。効果的な AI 駆動ソリューションを導入して可視性を強化し、複雑性を軽減し、生産性を向上させていない組織は、今後ますますそうした標的となっていくでしょう。私達はこの調査がこれらの増大するリスクに光を当て、組織がそれらを避けるのに役立つことを願っています。

以下の報告で、調査結果をさらに詳しくご説明していきます。また、今日の最大の課題のいくつかについての推奨策もご紹介します。

88%

セキュリティチームの88%は、既にAIの使用による大幅な時間節約効果を経験しています。

84%

調査参加者の84%は、モデルトレーニングまたはその他の目的でデータを外部に共有する必要のないAIソリューションが好ましいと回答しています。

95%

調査参加者の 95% は、AI によりサイバー防御のスピードと効率を向上できると考えています。

88%

調査参加者の88%は、セキュリティスタック内でAIを使用することはセキュリティチームの時間を節約してよりプロアクティブな業務を行えるようにするためにきわめて重要だと考えています。

63%

調査参加者の63%は、自社のサイバーセキュリティツールはほぼ生成AIまたは生成AIのみを使用していると思っていますが、おそらく実際とは異なります。

AI革命が進行中

エンタープライズ環境への AI の導入は 2024 年の初め頃からかなり進んでいますが、侵害の件数やサイバー犯罪による損害は減っていません。このことから、少なくとも防御者と同じくらい攻撃者も急速に AI を導入していると考えられます。

サイバーセキュリティ業界は予防、検知、対処、修復のワークフローへの AI の統合を急いでいますが、テクノロジーは人間のスキルセットよりも格段に急速に進化しています。新しい人材を採用することによってセキュリティオペレーションにおける慢性的問題、たとえば過労、在職期間の短さ、離職率の高さなどを解決することは、現在の状況ではほぼ不可能です。

ただ、良い知らせとしては、AI を適切に使用すれば組織がこれらの課題を克服するのに役立つかもしれない、という認識がステークホルダーの間で高まりつつあることが挙げられます。また、これに向けて踏み出すタイミングは今であり、攻撃者が AI テクノロジーを利用する能力を大幅に高める前に行うべきだという認識も高まっています。

この変化が起こりつつあることを示す兆候は既にあります。2 年あまり前に ChatGPT がリリースされて以来、脅威研究者は新手のソーシャルエンジニアリング攻撃の増加を観測しています。悪意ある E メールを分析すると、これらの脅威は従来型の E メールセキュリティツールを回避する能力が高まっていることがわかりました。またそれらはますます標的を絞り込むようになっており、これは脅威アクターが生成 AI を利用して特定の組織あるいは個人に対して専用のメッセージを作成していることの証拠です。[1]

そして残念なことに、昨年観測された問題の多くはまだ継続しています。AI 駆動テクノロジーの急激な導入への動きは、防御者に新しい課題をもたらしています。意思決定者はさまざまな製品や機能がどのように作用するのかを理解し、何を導入すべきかについて賢い選択を行えるようになる必要があります。セキュリティアナリスト、インシデント対応者、アーキテクトはこの新しいテクノロジーを実務においてどう使っていくかを学ぶ必要があります。しかし AI についての誤解はまだはびこっています。

当社は AI に関してリーダーの理解が進みサイバーセキュリティの成熟が進んでいることに励まされていますが、先進的な組織とそれ以外の一般的な組織の間にはまだ格差があります。AI による脅威は差し迫っていると同時に急激に変化し続けているため、すべての組織にとって状況に後れをとることのできない緊急の問題です。

[1] Darktrace, First 6:Half-Year Threat Report 2024、参照先：
https://cdn.prod.website-files.com/626ff4d25aca2edf4325ff97/66b11449115ff7537adb646b_First6_Half_Year_Threat_Report_2024-compressed.pdf

継続する進化：サイバー脅威ランドスケープに対するAIのインパクト

AIが攻撃者によってますます効果的に利用されていることを示す証拠は次々と発見されています。[2] たとえば、ダークトレースの脅威研究者は、Darktrace / EMAILユーザーを標的とした新手のソーシャルエンジニアリング攻撃が2023年に135%増加したことを確認していますが、これは ChatGPTの普及が拡大したのと同時期です。[3]

AIの悪意ある使用について最も懸念の大きい分野には以下が含まれています：

新手のソーシャルエンジニアリング攻撃

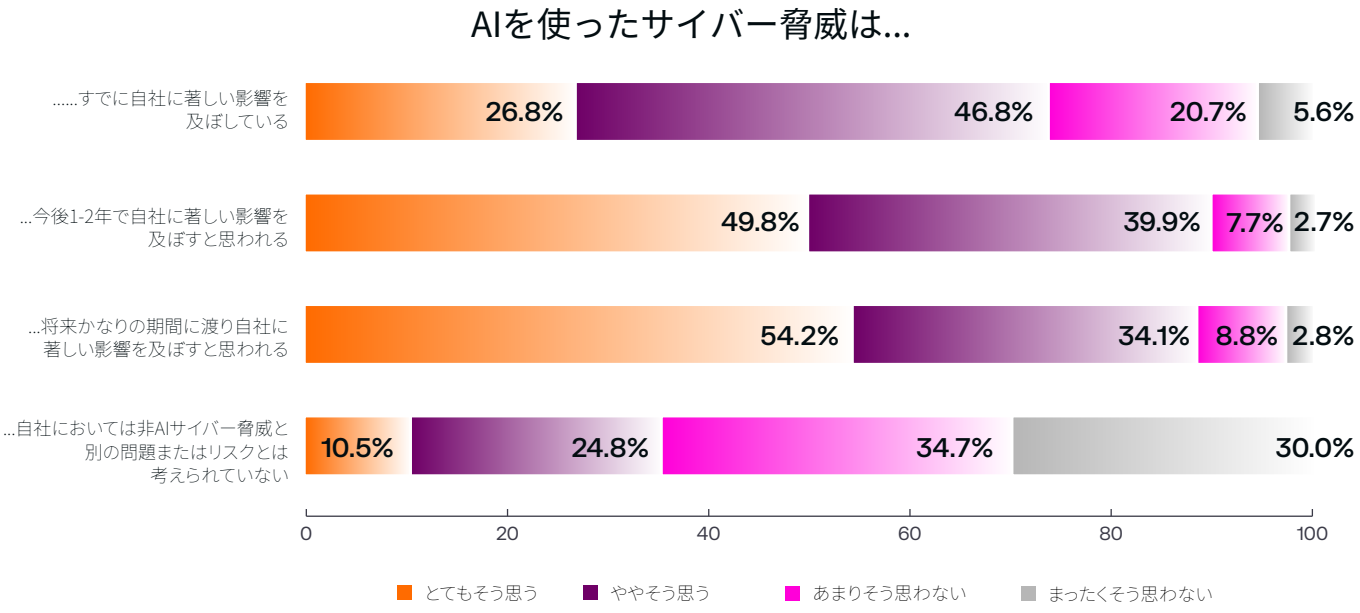
AI を使った攻撃は検知がより困難であり従来型の防御をすり抜けやすくなります。

高速かつ大規模に実行されるより高度な攻撃

AI を簡単に利用できるようになったため、より能力の低い脅威アクターが実行することができます。

AI システムを標的とした攻撃

機械学習モデル、トレーニングデータ、およびそれらにアクセスする API やインターフェイスを狙った攻撃があります。



調査参加者は脅威ランドスケープに AI が大きな影響を及ぼしていることを認識しています。4 分の 3 近く（74%）が、AI による脅威が自社の組織にとって現在大きな問題となっていることを認めています。調査参加者 10 人のうち 9 人（90%）が、AI による脅威が今後 1-2 年に渡って組織に著しい影響を与えると見ており、この数字は昨年の調査をわずかに上回っていました。

[2] Ibid.
[3] Darktrace, Generative AI:Impact on Email Cyber Attacks、参照先：https://darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks

AI によるサイバー脅威に影響を受けている産業：

最も多い

小売り

80%がすでにAIによる著しい影響を受けています。

テクノロジー

79%がすでにAIによる著しい影響を受けています。

製造業

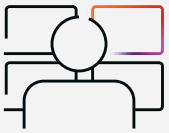
74%がすでにAIによる著しい影響を受けています。

政府機関

54%がすでにAIによる著しい影響を受けています。

最も少ない

AIによる脅威が現在影響を及ぼしていると回答した人の割合、職種別：



65%

SecOps実務者

vs.

78%

CIOまたはCISO

AIによる脅威が今後長期的に影響を及ぼすと回答した人の割合：

90%

SecOps 実務者

vs.

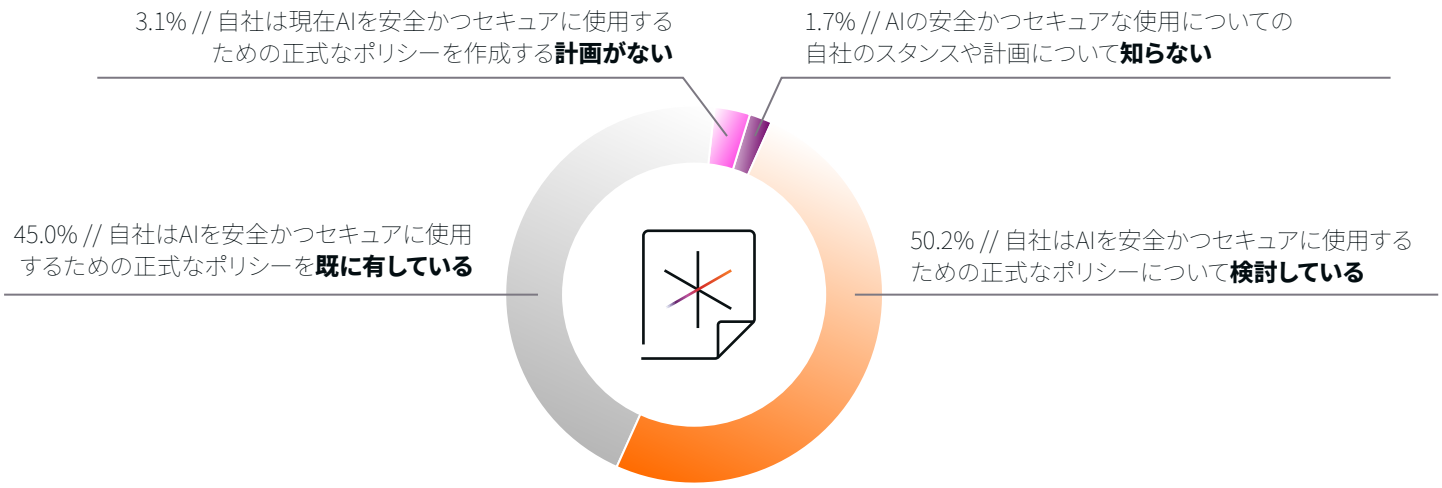
88%

CIOまたはCISO

大半の参加者（65%）は、自社の組織において、AIによる脅威はAIを使っていない脅威とは別の問題と考えられていると回答しました。攻撃がAIを使ったものかどうかを判断することがほぼ不可能であり、組織が直面する攻撃にAI脅威が占める割合がますます大きくなるなかで、この区別の意味は次第に薄れていきます。

むしろ、組織は別の課題に注意を移す必要があります。かつてないスピードで到来する、それぞれ違った脅威の増大に効率的に対応できるような、プロアクティブかつリスクベースのアプローチを防御に取り入れる必要があるのです。

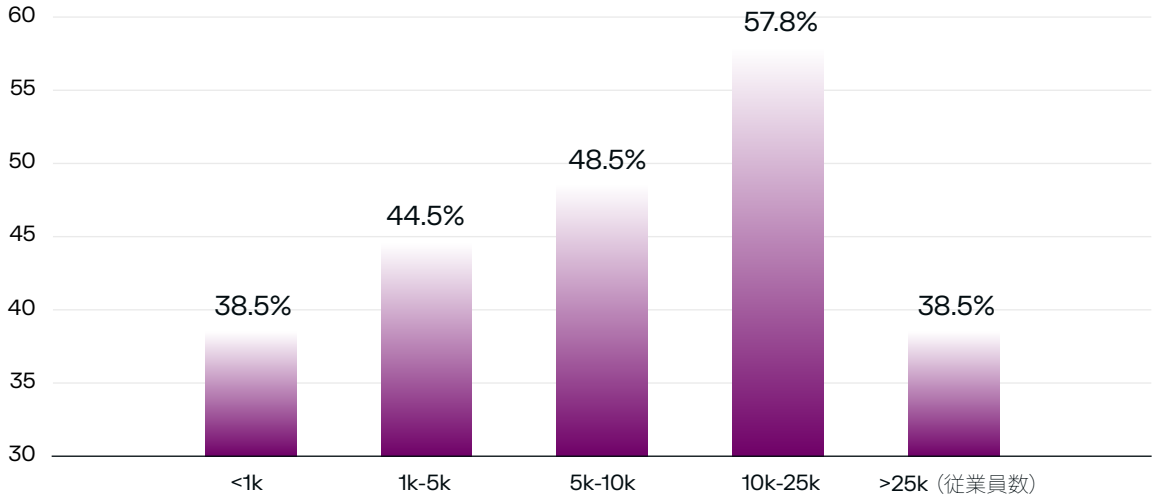
AIセキュリティポリシー：議論は活発だがアクションは少ない



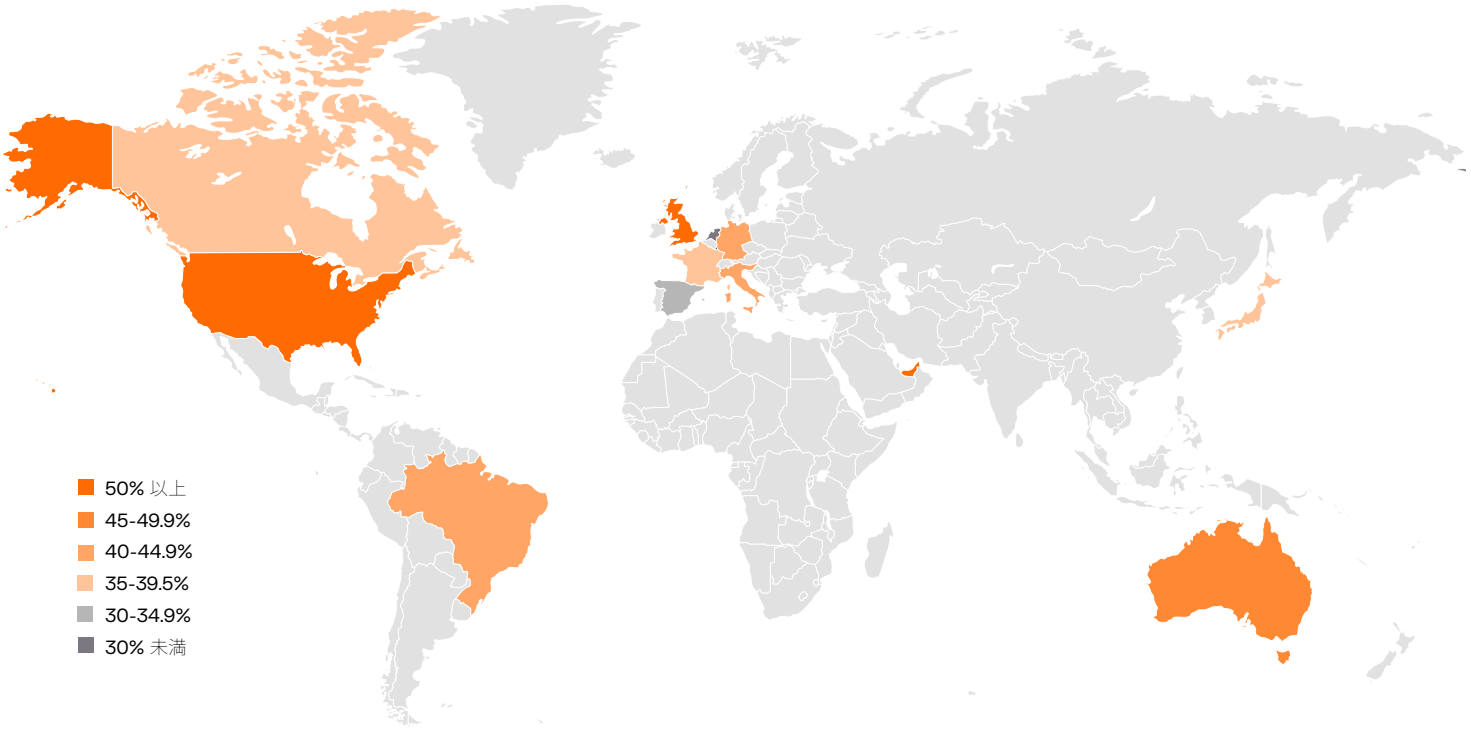
AIの安全かつセキュアな使用のためのポリシーを検討している、またはAIを既に導入していると答えた95%の参加者のうち、このようなポリシーを既に確立していると回答した人は半数以下（45%）でした。

非常に小規模な組織（従業員1,000名未満）と非常に大規模な組織（従業員25,000名以上）はAIセキュリティポリシーを持っている割合が最も低く、これら2つのグループで既にポリシーを実施していると答えた回答者は38%のみでした。

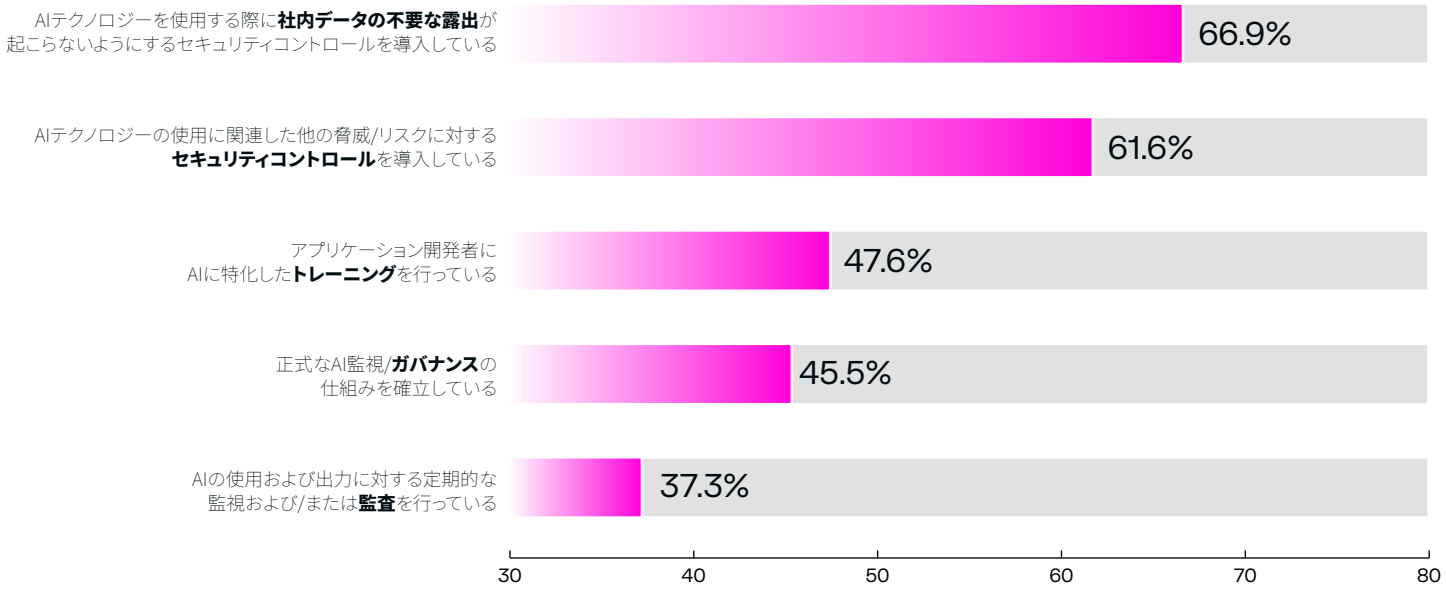
AIを安全かつセキュアに使用するための正式なポリシーを有している組織（組織の規模別）



AIを安全かつセキュアに使用するための正式なポリシーを有している組織（国別）



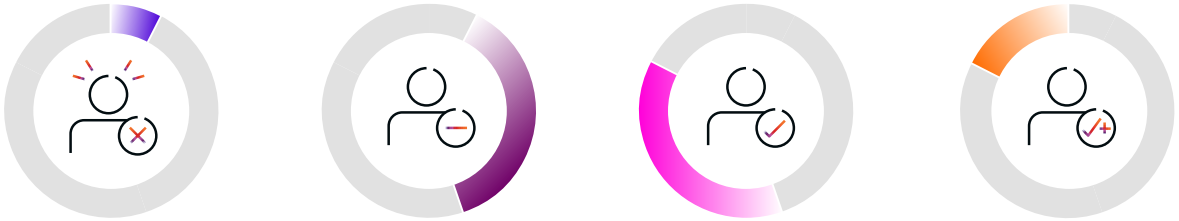
AIの安全かつセキュアな使用のために取られている対策



昨年の調査参加者の85%以上が、自社では既にAI導入に関連するリスクを緩和するための対策をとっていると答えました。今年の調査では、彼らはさらに進んで具体的なコントロール、トレーニング、監視を実施していることがわかりました。

金融サービスおよび小売業セクターに属する組織がより高いレベルの成熟度を示していた一方で、政府機関はこの点では後れをとっていました。

自信の欠如は引き続き蔓延：調査参加者の半数近くが、自社はAIを使った脅威に対して**適切な準備ができていない**と回答



7.6%
自社はAIによる脅威に対して適切な準備ができていない

37.2%
自社はAIによる脅威に対して多少は準備ができている

37.9%
自社はAIによる脅威に対して準備ができている

17.3%
自社はAIによる脅威に対して確実に準備ができている

この結果は昨年よりも自信が増していることを示しています。昨年は72%もの回答者が自社の組織は適切な準備ができていないと答えていました。それでも、AIによる脅威や攻撃に対する自社組織の準備度について強い自信を持っているのは18%未満であり、わずか2%増えたのみでした。

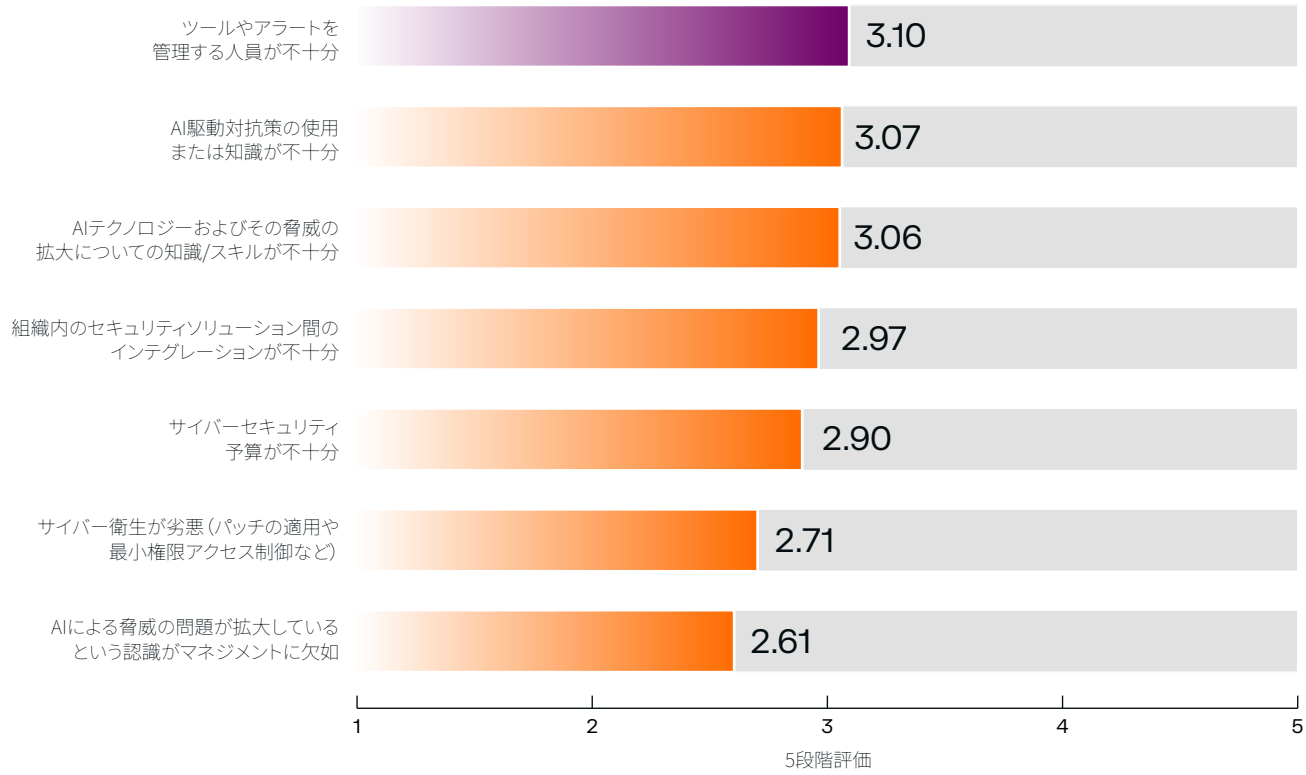
自信のギャップ

エグゼクティブクラスの参加者は、自社の組織が AI 駆動の脅威に対して準備ができていると回答する割合が、実務を担当している人よりも格段に高い（**62%** が概ね同意）傾向にありました。[4] そしてセキュリティオペレーション実務者の半数近く（**49%**）、およびセキュリティアーキテクトおよびエンジニアの **47%** が、自社組織の準備度に対して自信を示しました。

この自信度の違いは、リーダーと最前線の実務者の間の認識のずれを示しています。前線にいる人は、AI を使った敵との戦いはどういうものかを日々経験し理解しており、現状のソリューションの欠点がどこにあるかを明確に認識しています。

[4] エグゼクティブにはCIO、CISO、およびその他のITセキュリティエグゼクティブが含まれます。実務担当者とはセキュリティアナリスト、オペレーター、インシデント対応者、アドミン、アーキテクト、エンジニア等の役割を指します。

AIによる脅威を防御する組織の能力に対する最大の阻害要素



全世界の人材ギャップが500万人に近づきつつある現在、調査に参加した組織の71%が少なくとも1名のサイバーセキュリティ人材が欠員となっていると答えており、スキルギャップがあらゆる産業に渡って組織に著しいリスクを作り出していることは明白です。また、多くの組織がAIを使った防御システムを管理するのに必要なスキルを持ったプロフェッショナルを見つけるのに苦労していますが、これらのツールが新しいことを考えれば当然です。

調査参加者のほとんどにとって予算は懸念材料ではなく、これは昨年の調査でも同様でした。また、課題に対するマネジメントの認識不足問題も最下位となり、上層部の認識も大きな懸念ではないことを示しています。

従来型サイバーセキュリティツールに対する信頼は薄れつつある

調査に参加したサイバーセキュリティプロフェッショナルの 10 人に 1 人は、非 AI ベースのサイバーセキュリティソリューションが AI を使った脅威を検知できるとはまったく考えていません。そして参加者の半数（50%）はこうした従来型ツールの能力に強い信頼を置いていませんでした。

従来のサイバーセキュリティソリューション（AIテクノロジーを使用していないもの）がAIによる脅威や攻撃を検知し阻止することに対してどの程度の確信がありますか？

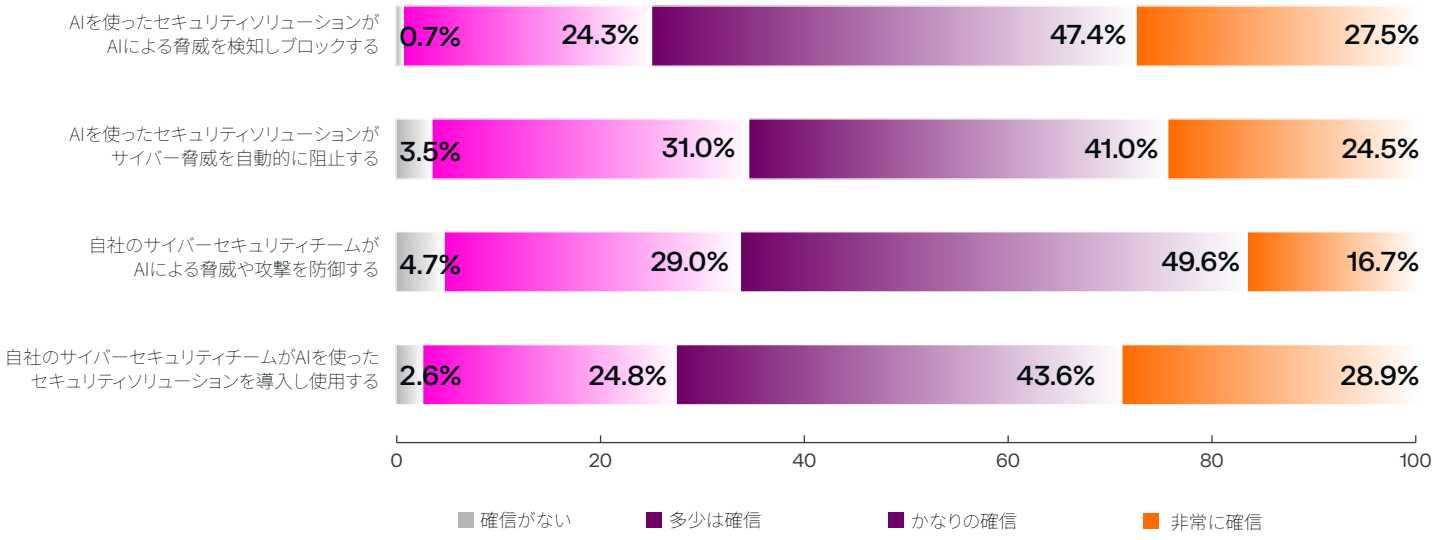
10.2%
確信がない

40.2%
ある程度確信

35.6%
かなりの確信

13.9%
非常に大きな確信

現在、次の能力についてどの程度確信を持っていますか？



従来型のサイバーセキュリティツールに対する信頼は低下しつつある一方で、セキュリティプロフェッショナルは AI を使ったソリューションを導入し使用することへの自信を高めつつあります。本年の調査では、調査参加者の 73% が、自社のセキュリティチームがセキュリティツールスタック内で AI を使いこなすことに自信を示しており、その割合は昨年よりも増加しています。

APAC 地域からの参加者は特に従来のサイバーセキュリティソリューションへの信頼のなさ（AI を使った脅威を阻止できないと考える回答者が 55%）を示す傾向が見られましたが、同時に自社のチームの防御能力にも自信がなく（AI を使った脅威を防御できると思わない回答者が 45%）、AI 駆動のツールを導入し使用する能力についても同様でした（40% が自信が持てないと回答）。

先進的な組織においては、AI を導入しその使用を最適化するため、AI をますます多くのワークフローに取り入れつつあります。AI を使い慣れるにつれ、実務者の信頼のレベルも高まる傾向が見られました。

SOC アナリストや管理者は、AI を使ったツールが AI を使った脅威を検知しブロックする能力についての信頼が若干低く、それぞれ 45% と 55% が確信のなさを表明していました。大規模な組織（従業員 25,000 名以上）のステークホルダーも、AI を使ったセキュリティソリューションに対する信頼が平均よりも低く、51% が確信のなさを表明していました。保護しなければならないアタックサーフェスがより幅広く多様な大規模エンタープライズは、直面する防御の課題もより複雑であり、どのツールを使うかに関係なく、セキュリティチームが取り組む問題はより難しいものとなります。

73%

調査参加者の73%が、自社のセキュリティチームがセキュリティツールスタック内でAIを使いこなすことに自信を示しており、その割合は昨年よりも増加しています。

55%

管理者の55%は、AIを使ったツールがAIを使った脅威を検知しブロックする能力についての信頼が若干低い傾向にあります。

51%

大規模な組織（従業員 25,000 名以上）のステークホルダーも、AI を使ったセキュリティソリューションに対する信頼が平均よりも低い傾向にあります。

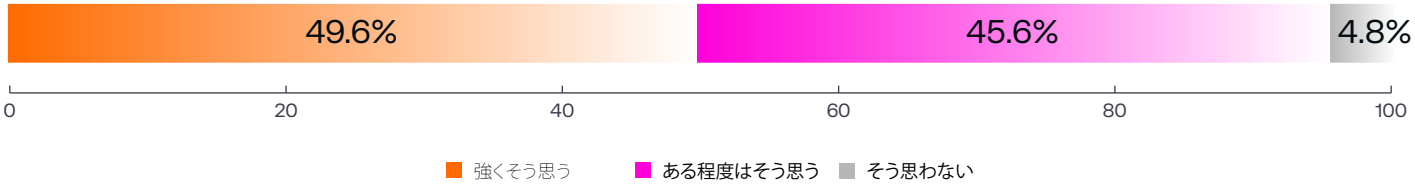
デジタルエコシステムの複雑性を乗り越える：AIがサイバーセキュリティソリューションに与えるインパクト

AIはSOC（Security Operations Center）チームが切実に求めているフォースマルチプライヤー（戦力倍増装置）として機能し、組織は人員を増やすことなく脅威を検知、調査、対処する能力を拡大することが可能になります。AIは膨大な量のデータを分析できるため、防御者がより速く、より正確に、そしてより効果的に行動するための力となります。SecOpsプログラムがAIを使って低レベルの繰り返し作業を自動化することにより、より戦略的な性質の、高価値なタスクに集中することが可能になります。

しかし、スキルギャップの解消という点では、AIはどれも同じように作られてはいません。さまざまなタイプのAIの強みと弱点、そしてそれぞれをどのユースケースに適用するのが最適かを最もよく理解できる組織が、効果的で効率的な防御を構築する上での優位性を持つことになるでしょう。

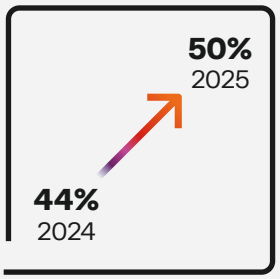
しかし全員がこの理解を持っているとは言えません。状況をさらに複雑にしているのは、サイバーセキュリティベンダーがAIについての過熱した宣伝を最大限に利用しようと躍起になっている一方で、ベンダーの主張は漠然としてわかりにくい場合があることです。

サイバーセキュリティプロフェッショナルの95%は、AIを使ったソリューションは防御のスピードと効率を著しく向上させることができると回答しています。

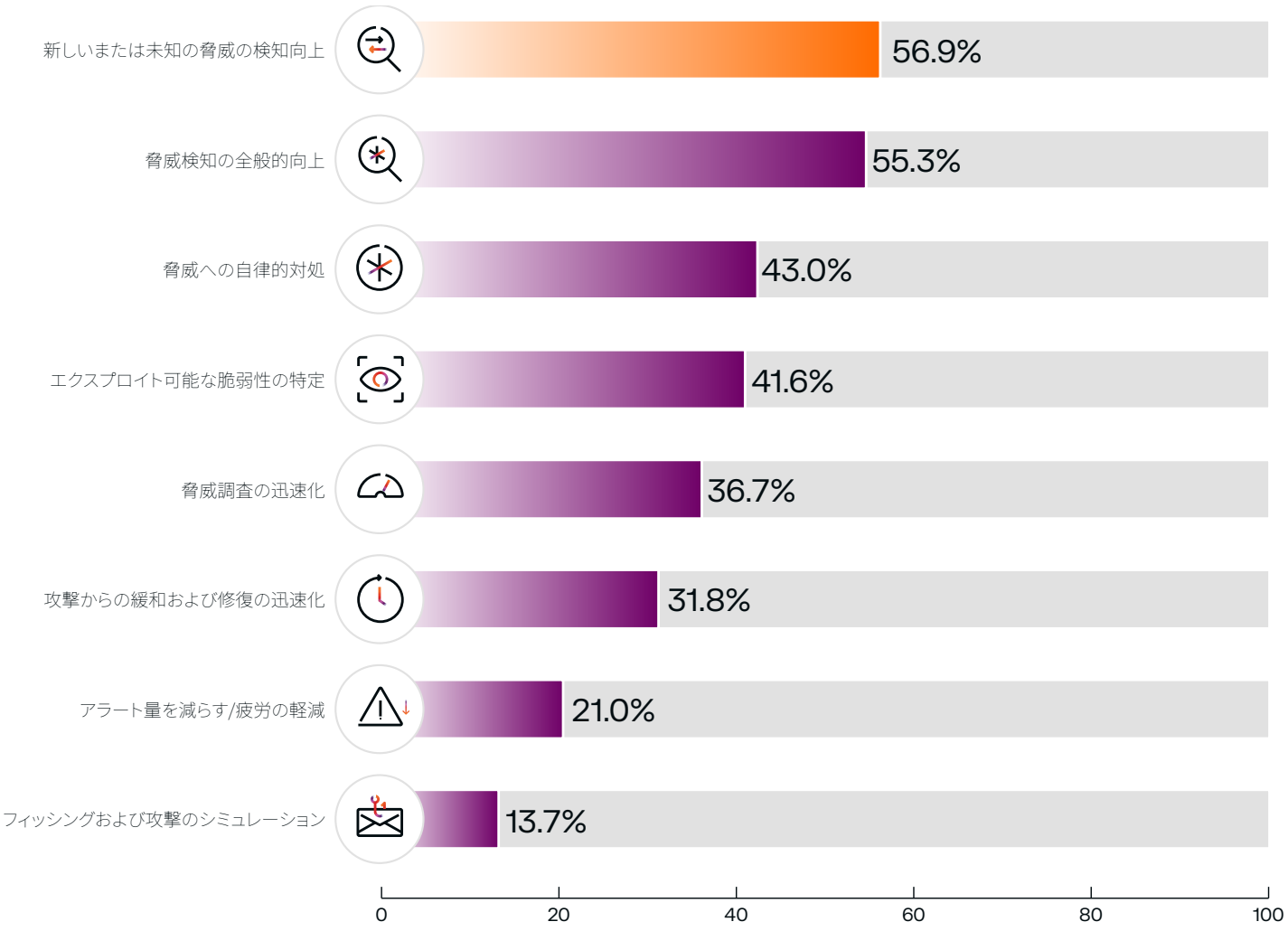


AIを使ったサイバーセキュリティソリューションによってセキュリティチームが脅威を予防、検知、対処、修復する能力が大きく向上するということについては、ほぼ万人が認めるところです。事実、調査参加者の95%がこのことに同意しています。

AI を使ったソリューションは防御のスピードと効率を著しく向上させることができると回答したサイバーセキュリティプロフェッショナルの割合は、2024 年から 2025 年にかけて増加しました。



防御AIのインパクトが最も大きいと期待される分野/領域

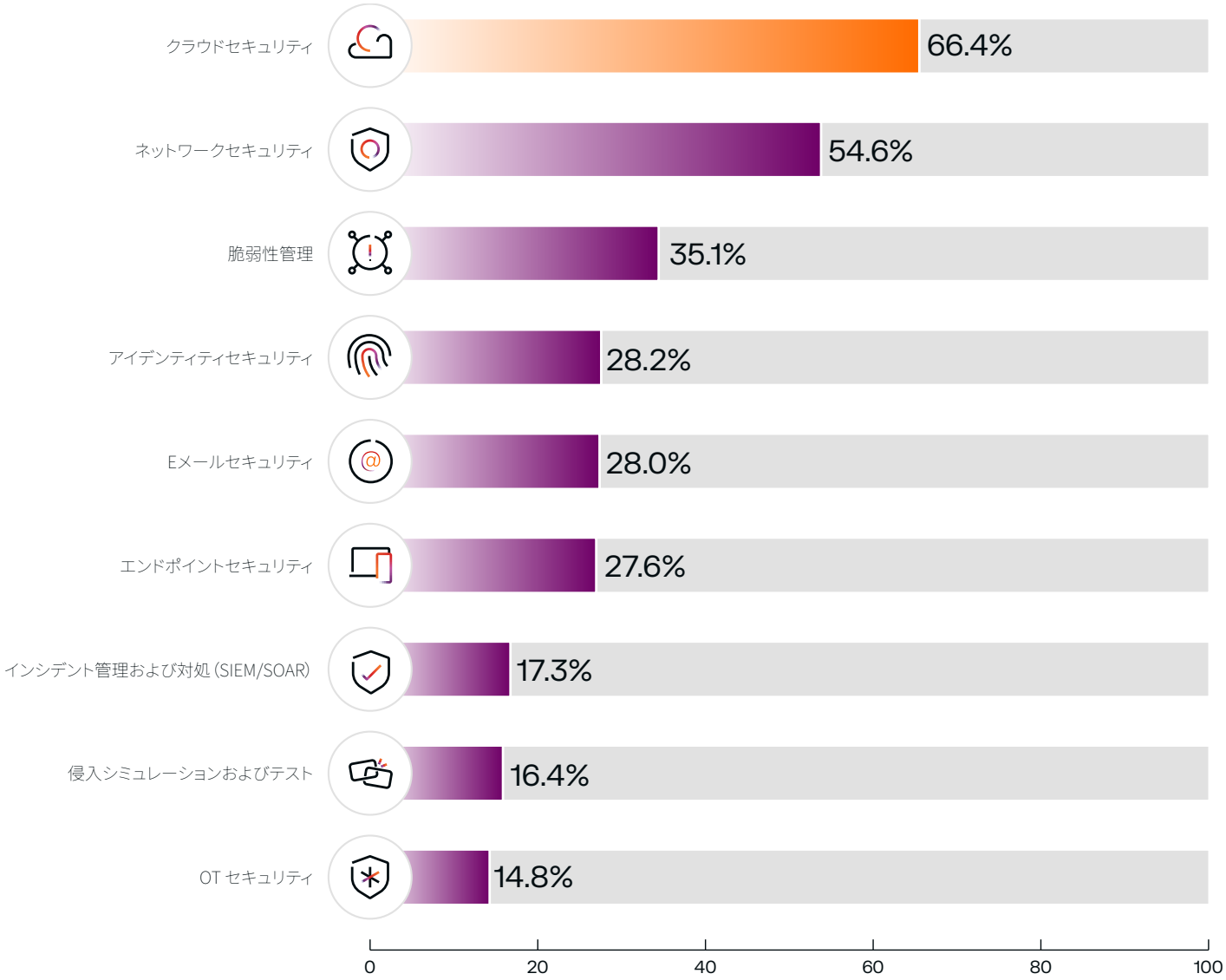


新手および未知の脅威の検知向上は、サイバーセキュリティにおいてAIが最も大きなインパクトを持つと期待されている分野です。組織のリアルタイムデータでトレーニングされたAIは、その組織内のあらゆるデバイス、アカウント、ユーザー、およびクラウドにとって何が通常の状態かを理解することができます。これにより異常な動作パターンやアクティビティが発生次第ピンポイントで識別することができ、新手の脅威であっても即座に発見し、阻止することができます。

調査参加者が低いランクを付けた分野（アラートの量やアナリストの疲労を削減すること、フィッシングおよび攻撃のシミュレーションも含まれます）では、AIが既に有効に機能しています。たとえばダークトレースのCyber AI Analystツールは、10,000を超える組織のレベル2 SOC分析の自動化を支援し、アラートの量をこれまでの数千件の個別のイベントからわずか数件の包括的インシデントに削減しています。おそらくこれらの分野では既にAIが幅広く利用され、価値を提供しているため、調査参加者はこれらのユースケースに対して今後3年間に最も大きな影響があるとは期待していないものとみられます。

新手および未知の脅威の検知向上はサイバーセキュリティにおいてAIが**最大の**インパクトを持つと期待されている分野です。

防御AIのインパクトが最も大きいと参加者が期待するサイバーセキュリティの領域



サイバーセキュリティにおいて防御AIのインパクトが最も大きいと期待される領域は、クラウドセキュリティ（66%）、ネットワークセキュリティ（55%）です。

昨年の調査以来、AIがクラウドおよびネットワークセキュリティに対して今後数年間でインパクトをもたらすという期待は高まりました（クラウドに対しては61%から66%、ネットワークに対しては46%から55%に増加）。脆弱性管理についてもかなり関心が高まっており、これを選択した参加者は23%から35%に増えています。

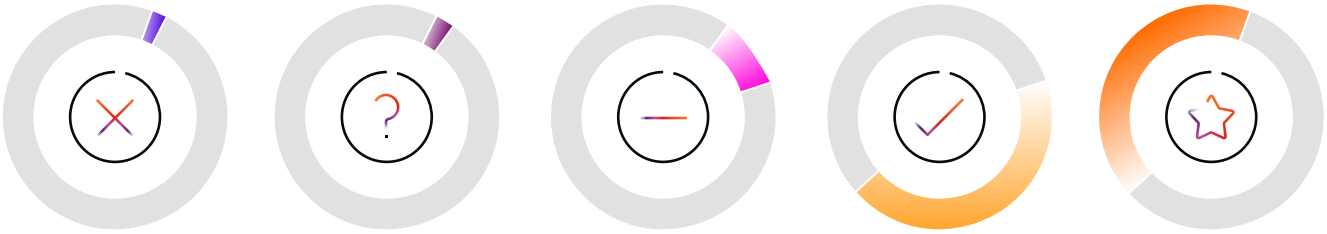
セキュリティプロフェッショナルがAIおよびそれが現実のワークフローにもたらすことのできる価値に慣れるにつれて、彼らの回答は早期に導入した人達の多くが経験した内容に近づいてきます。たとえば、セキュリティチームは既にインシデント対応等の分野にAIがもたらすことのできるインパクトを実感しているかもしれません。そこではAIが自律的に介入して進行中の脅威を封じ込め、より深い分析や修復を行うための時間を作り出すことができます。また、彼らはAIが侵入や攻撃のシミュレーションやテストを強化できることを認識しているかもしれません。

しかし、クラウドの複雑性は依然として困難な課題を突き付けています。エンタープライズがSaaSアプリケーションへの依存をますます高めるなかで、攻撃者はこれらの環境を標的とし、アカウント乗っ取りを通じて特権アカウントへの不正アクセスを獲得しようとするでしょう。クラウドリソースへの初期アクセスに成功すると、彼らは環境内を水平移動して高価値なデータや詐欺と恐喝の機会を探します。

知識は力：
AIのタイプとテクノロジーを理解する

現実の世界のオペレーションでAIの価値を最大化しようとするならば、さまざまなステークホルダーがAIとは何か、AIの各種タイプはどのように機能するのか、AIが最も価値を提供できるのはどこか、についてその複雑さを理解する必要があります。今日のサイバーセキュリティ意思決定者および実務者全員がこの必要な知識を持っているとはいえません。

セキュリティスタック内のすべてのタイプのAI について十分に理解していると回答した人は、セキュリティプロフェッショナルの42%にとどまりました。



2.1%
該当しない - 現在サイバーセキュリティスタック内でいずれの形のAIも使用していない

2.6%
サイバーセキュリティスタック内でどのタイプのAIが使用されているのか知らない

9.9%
サイバーセキュリティスタック内でどのタイプのAIが使用されているのか漠然とした理解しかない

43.3%
サイバーセキュリティスタック内でどのタイプのAIが使用されているのかある程度理解している

42.0%
サイバーセキュリティスタック内でどのタイプのAIが使用されているのか完全に理解している

調査参加者のなかでは、エグゼクティブの方が、他の役割の参加者よりも高いレベルの理解を持っていると回答（彼らの60%が自社で使用しているAIのタイプは何かを具体的に知っていると回答）していました。これは技術的熟練度の高さではなく、リーダーがしばしば示すことを求められる高いレベルの自信、を示しているものかもしれません。現場でより多くの実際の仕事をしているにも関わらず、SecOps実務者や管理者の多くは、自社の組織で使用されているAIのタイプについて "ある程度の理解” を持っている（それぞれ45%と55%）と回答していました。

大規模な組織（従業員10,000名以上）の参加者からはより低い理解のレベルが報告されました

26%

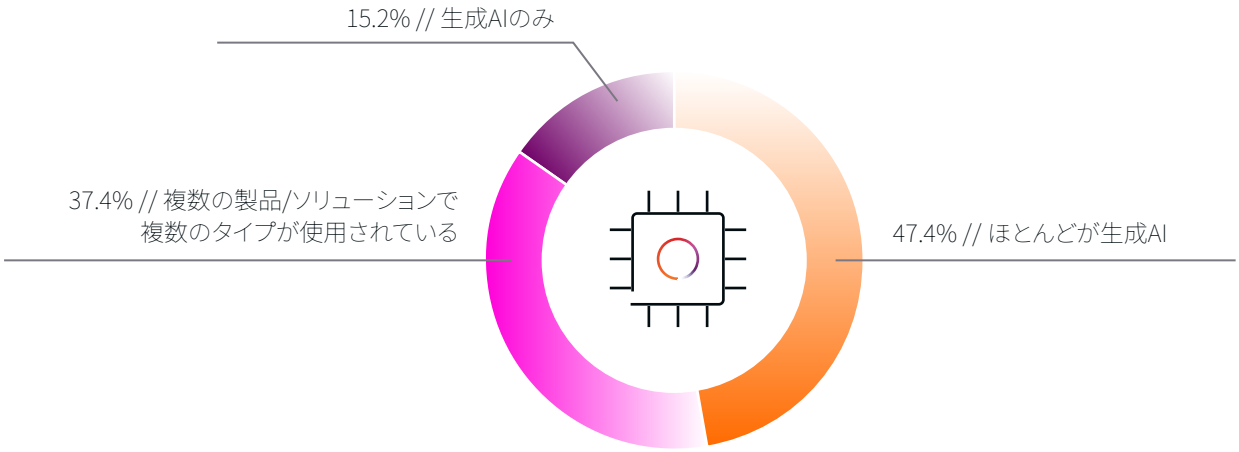
彼らの26%は組織のサイバーセキュリティスタックで使われているAIテクノロジーについて漠然としか理解していない、あるいはまったく理解していないと回答し、この結果は全体平均の2倍でした。

17%

APAK地域の参加者の17%は、自社の組織がサイバー防御に使用しているAIについて漠然としか理解していない、あるいはまったく知識がないと回答しました。

明らかになったのは、さまざまなベンダーが AI を使った新しいソリューションや機能を、従業員がそれらの使い方のトレーニングを受けるよりも速いペースで次々と発表しているということです。組織が AI の価値を最大化しようとするならば、人間と AI の効果的なコラボレーションを推進する必要があります。そのためには、サイバーセキュリティプロフェッショナルは AI システムをどのように活用し、理解し、協調作業できるかについてのトレーニングを受けなければなりません。AI の導入は人間のセキュリティチームのスキルを高めるのに役立つかもしれませんが、セキュリティプロフェッショナルに適切なリソースと教育へのアクセスを提供して支援しなければそれは不可能です。

セキュリティステークホルダーの63%は、自社の既存のサイバーセキュリティスタックが生成AIのみを使用またはほとんど生成AIを使用していると回答



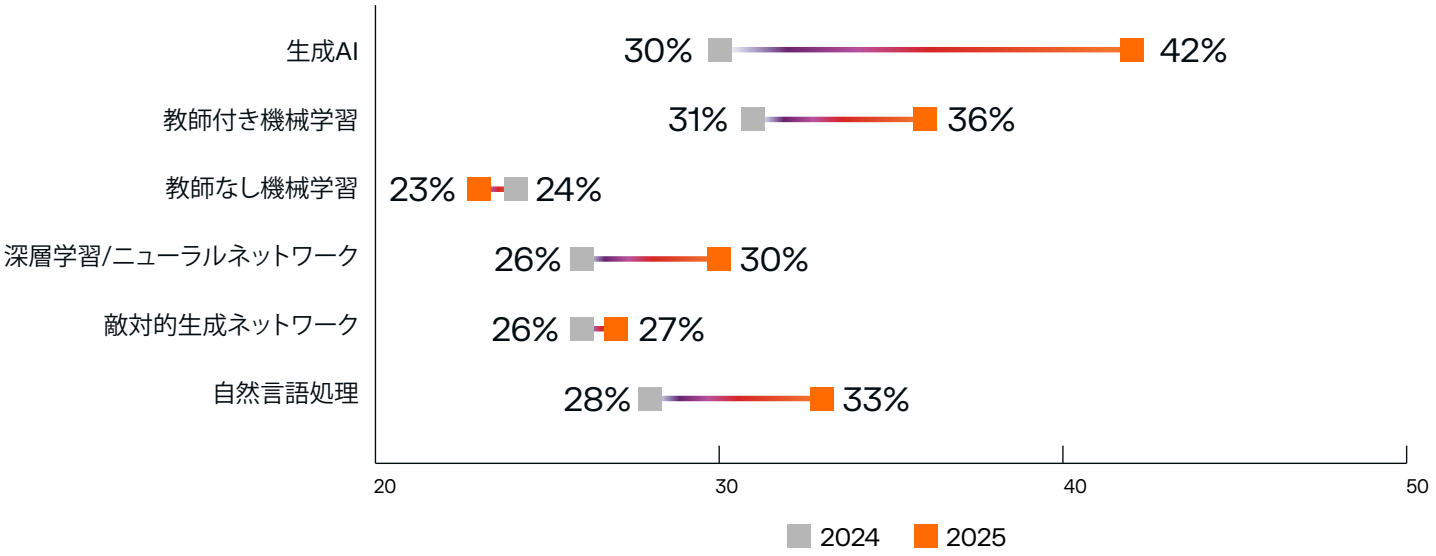
本年度も昨年度も、調査参加者は生成AIがサイバー防御に実際よりもかなり大きい役割を果たしていると信じる傾向を示していました。3分の2近く（63%）の人が、自社の組織のサイバーセキュリティツールで使用されているのは生成AIのみまたは生成AIがほとんどだと思っていたのです。ラテンアメリカ地域からの参加者は特にこの誤解に陥りやすい傾向にあり、83%の人が自社のサイバーセキュリティスタックでは生成AIのみ、または主に生成AIが使われていると信じていました。

実際には、そうであることは稀です。生成 AI は、フィッシングシミュレーションや、SecOps アナリストチームが脅威ハンティングやトリアージワークフローで自然言語インターフェイスを使って作業できるようにするなど、限られた数のユースケースにしか使用できません。他のタイプの AI の方が格段に幅広いユースケースに価値を提供できます。たとえば、攻撃者の行動を予測する、検知と修復を加速する、予防的ワークフローを補完する、などです。

ダークトレースはサイバーセキュリティで現在使用されているさまざまなAIのタイプやテクニックを詳しく紹介したテクニカルホワイトペーパーを発行しています

レポートを読む →

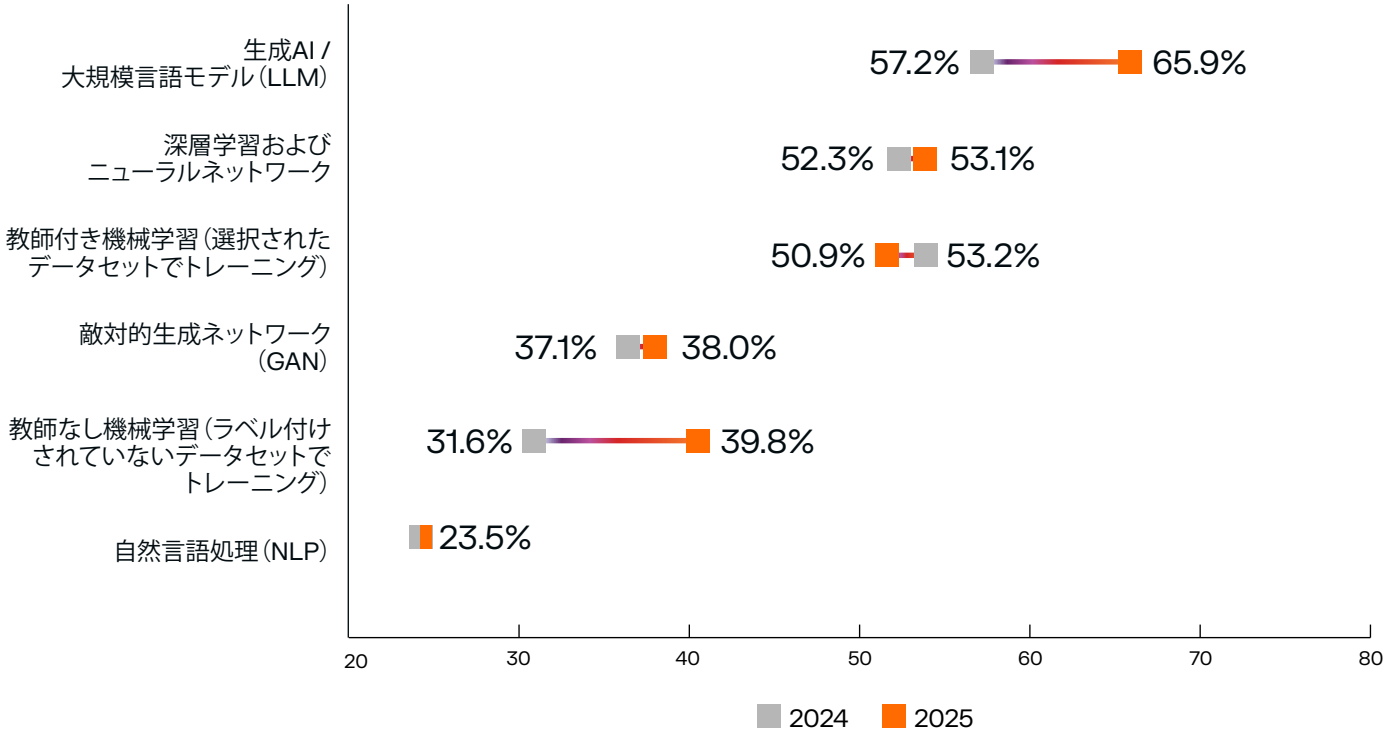
AIのタイプによって認識度は異なりますが、全体にレベルは上がる傾向にありました。各タイプのAIについて「良く知っている」と答えた回答者の割合



質問されたすべてのタイプのテクノロジーについて、最もよく知っていると回答したのはエグゼクティブでした（91% が生成 AI について、74% が GAN についてよく知っていると回答）。これは、テクノロジーについて知っているという意味をより抽象的にとらえていることの反映かもしれません。実務的役割を持つ人たちは " 知っている " ということの意味をより深くとらえているため、SecOps 実務者は生成 AI について知っていると回答したのは 61%、教師付き機械学習については 60%、GAN については 30% にとどまりました。

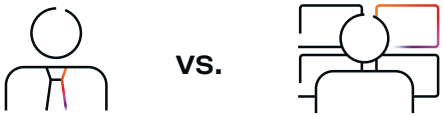
組織のセキュリティスタック全体に渡り AI を効果的に導入しようとするならば、組織のすべてのステークホルダー（技術的職種と非技術的職種両方）に対し、AI とは何か、AI がどのように機能することでサイバー防御を強化できるか、についてよりよく理解するためのトレーニングに投資する必要があります。

今後3年間でサイバーセキュリティに最も大きなインパクトをもたらすと期待されるAIのタイプは次のうちどれですか？



全体として、よく知られているAIタイプ（前述の質問を参照）の方が、現場にインパクトをもたらしていると認識される傾向にあります。

エグゼクティブは将来的に生成AIがSecOpsを変革する可能性についてとりわけ大きな期待を寄せていましたが、実務者は深層学習、ニューラルネットワーク、教師付き機械学習が生成AIよりも大きなインパクトをもたらすと予測していました。



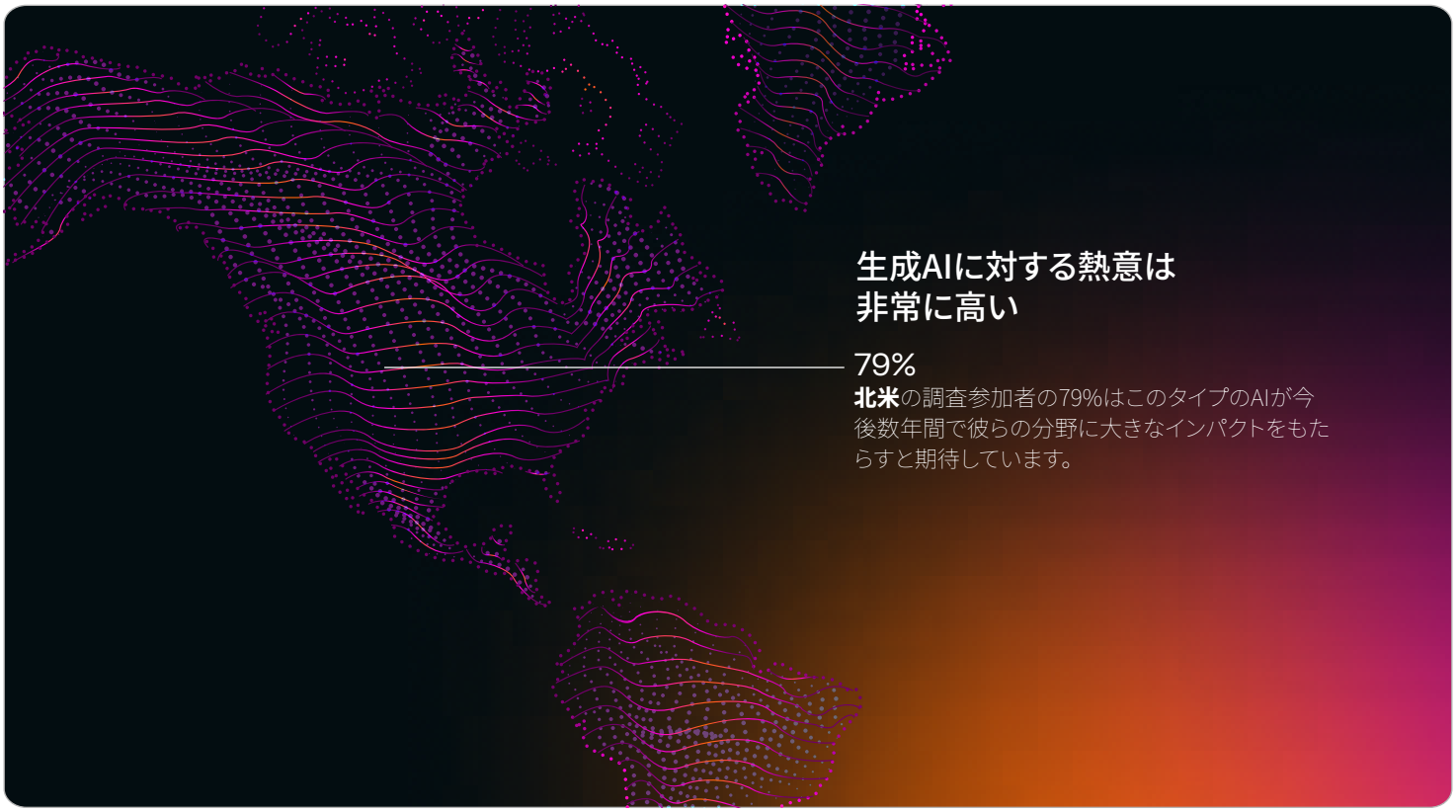
71%

生成AIによるSecOpsの変革を期待するエグゼクティブの割合

vs.

50%

生成AIによるSecOpsの変革を期待するSecOps実務者の割合

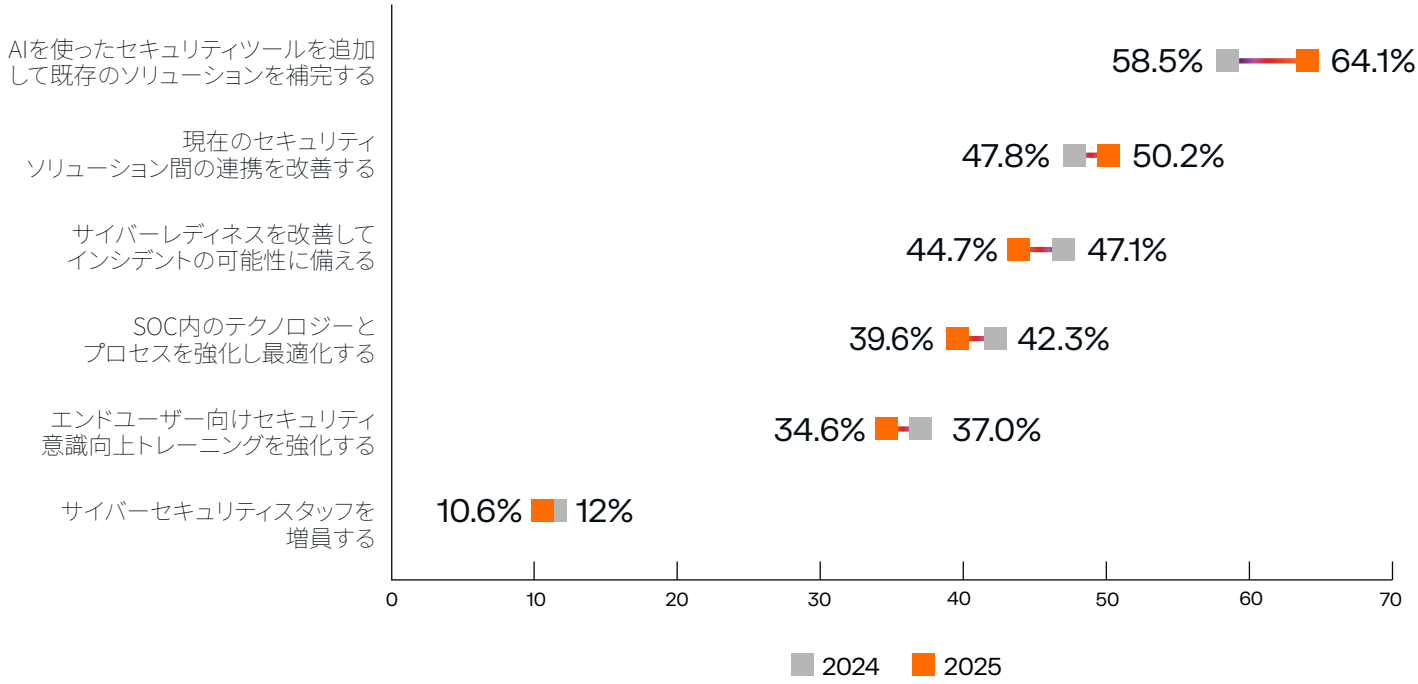


事実、実務者の仕事の有効性は、従来型のサイバーセキュリティツールで見逃されてしまう情報を提供することのできる、教師なし機械学習等のテクノロジーによって高められる可能性の方が大きいでしょう。教師なし機械学習は、組織にとって何が通常の状態かを継続的に学習し、未知の攻撃や新手の攻撃も含む、あらゆる種類の攻撃の検知を可能にします。これにはゼロデイエクスプロイト、アカウント乗っ取り、内部関係者による脅威、水平移動、クロスドメイン攻撃も含まれます。教師なし機械学習はこれらの目的に対して既にDarktrace ActiveAI Security Platform等のソリューションで利用されており、これまでに見られたことのない脅威に対してかつてない可視性を提供しています。こうしたソリューションを使用している実務者は、このタイプのAIが現在既に多大なインパクトをもたらしているため、将来大きなインパクトをもたらすと回答しない傾向にあります。

将来への視点：優先順位と目標

セキュリティプロフェッショナルはこの分野が急速に変化していることを知っています。彼らはAIの台頭により、新しいツールを導入し効果的に使用する方法を学ぶ必要があることを認識しています。それでも、将来に備えてどのように計画をたて、何に投資すべきかについて常に確信を持てるわけではありません。

AIによる脅威に対する防御を改善するための、セキュリティステークホルダーの最優先事項には、AIを使ったソリューションで既存のツールスタックを補強し、セキュリティツール間の統合を強化することが含まれます



昨年度同様、セキュリティステークホルダーは、追加のスタッフを雇用することよりも、既存のセキュリティスタックに新しくAIを使ったツールを追加することに関心を示していました。調査参加者はその前に（11ページを参照）、AI駆動の攻撃に対する効果的な防御を構築する上での最大の阻害要因は人員不足であると回答しているにも関わらず、このような結果になっています。

疲労が蔓延し、人材不足が新たなピークに達し、ますます多くの企業がサイバーセキュリティの欠員を埋めることができないなかで、彼らは人員をいくら増やしても、到底この問題を解決することはできないと気づいているのかもしれません。

実際、セキュリティスタッフの雇用に対する関心は昨年度より下がっており、さらにAIを使ったツールをセキュリティスタックに追加することを重要と考える参加者は58%から64%に増加しています。エグゼクティブはAI駆動ツールを取り入れることに対して特に積極的でしたが、SecOpsはセキュリティ意識向上トレーニングの改善やサイバーセキュリティツールの統合の強化のほうに関心を示していました。

昨年の調査と本年を比較して態度の変化から導き出すことのできる1つの結論は、セキュリティスタッフの増員ができるならばそれは助かるが、AIを使ったツールを導入して現在の従業員がよりスマートに働くことができるようにすることのほうが、ますます不可欠条件になりつつあるということです。

新しいソリューションを追加する際の優先項目

“ 新しいセキュリティ機能を購入する、あるいは既存の製品を置き換える場合、自社組織では個別のポイント製品よりも、より幅広いプラットフォームの一部としての機能を導入することを好む。”

87% が同意

エグゼクティブでは 89%；セキュリティオペレーター & アナリストでは 78%

これらの結果は昨年度と同様であり、ほぼ10人のうち9人が、プラットフォーム指向のセキュリティソリューションのほうが個別の製品の寄せ集めよりもサイバー脅威を阻止するのに効果的であると答えています。

“ 自社のセキュリティスタック内で AI を使用することは、セキュリティチームをよりプロアクティブ（リアクティブではなく）にするためにきわめて重要である。”

88% が同意

エグゼクティブでは 92%；セキュリティオペレーター & アナリストでは 80%

参加者の大多数が、自社のサイバーセキュリティスタック内でAIを使用することで既に実務者の時間が解放され、よりプロアクティブなアプローチをとることが可能になっていると答えています。AIそのものが、リアクティブからプロアクティブなセキュリティへの変化に貢献し、リスク優先付けの改善や、ASM（Attack Surface Modeling）や攻撃経路モデリングなどの予防的戦略の自動化などを可能にします。また、セキュリティチームはAIを活用することでより効果的なセキュリティ意識向上トレーニングプログラムを構築できます。

“ 自社としては、組織内のデータを外部に共有する（外部 LLM にフィードするなど）ことを必要としない防御 AI ソリューションが望ましい。”

84% が同意

エグゼクティブでは 82%；セキュリティオペレーター & アナリストでは 86%

この選好性は、生成AIの普及により生じているデータプライバシーやセキュリティへのリスクについての意識の高まりを反映していると思われます。また、規制当局によるデータ保存場所についての要件や、その他の制限についての認識の高まりも反映されているかもしれません。

モデルトレーニングデータやその他のAIに対する入力の扱い方は、ベンダーによってさまざまです。その多くは顧客環境内の専有データを集中管理されたデータレークに移動し、他の何百もの組織からのデータと組み合わせてモデルのトレーニングに使用します。

また、顧客のすべてのデータをオンサイトまたはプライベートクラウドに保存するオプションを提供しているベンダーもあります。さらに、分析手法にもさまざまな種類があり、コンテンツではなくメタデータを分析することでプライバシーを保護する非侵襲的な手法もあります。データの使用や保存方法について法的規制がある組織においては、検討している各ベンダーに対してAIガバナンスについて質問することがきわめて重要です。

今がその時：AIサイバー成熟度の達成

昨年来、脅威アクターは生成 AI を使って、本物とよく似た大量のフィッシング E メールを送信するなど、比較的簡単な攻撃を大規模に仕掛けてきました。彼らはより高度な目的に使用するために他のタイプの AI も利用しつつありますが、そうした攻撃の発生はまだ小規模です。しかし間違いなく、これらのイノベーションや新しいツールの活用の努力は実を結ぶでしょう。今後数か月、あるいは何年もにわたり、AI 駆動攻撃の成功例がますます増えていくと予想されます。

防御者側もこの進化を十分に認識しており、AI をセキュリティスタックに組み込むことが脅威の段階的な発達に対抗する上で不可欠であることを理解しています。しかしながら、テクノロジーに対する理解のレベルは組織によってまちまちであり、導入と実装の成熟度も異なります。

Darktrace ActiveAI Security Platform は、組織が人材のギャップを埋めサイバーセキュリティ成熟度のレベルを引き上げるのを支援することを目的として設計されています。このプラットフォームはコラボレーションを推進し学習曲線を効率化するよう構築されており、経験の浅いまたはスキルのあまりないアナリストに対する障壁を引き下げています。また、ダークトレースはエキスパートによるトレーニング、サイバーセキュリティアナリストへの 24 時間週 7 日のアクセス、チームをサポートするマネージド型サービスも提供しています。

ダークトレースは 10 年以上に渡って AI をサイバーセキュリティに使用しています。ダークトレースはこの分野の先駆者として、イノベーションをプロセスと一体化させています。

Darktrace ActiveAI Security Platform は組織固有のビジネスデータでトレーニングされる多層的な AI を使用して、エンタープライズ全体にその組織専用のセキュリティを構築します。このアプローチでは、モデルが常時オン、かつ常時学習する包括的かつ信頼性の高いカバレッジが実現でき、セキュリティチームは攻撃をリアルタイムに阻止できます。さらに、デジタルエステート全体のデータを使用するというダークトレースの特徴は、データプライバシー、解釈可能性、データ転送コストの点で利点をもたらします。

ダークトレースは、アプリケーションに実証済みの保護対策を徹底し、出力が常に説明可能であることを保証することにより、AI の責任ある使用を推進しています。独自のアプローチと継続した製品のイノベーションを通じ、ダークトレースは人間のセキュリティチームを補強し、最新の、最も斬新なサイバー脅威も含めた、進化する攻撃からのリアルタイムの保護を可能にします。人間と AI の間の前向きかつ効果的な関係を促進することにより、ダークトレースは組織それぞれの固有のニーズに対応します。

次のステップを踏み出す

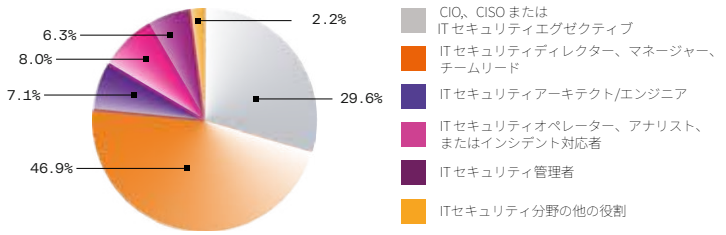
AIによる混乱の新たな波を乗り越える

お近くで開催される Darktrace LIVE に参加し、同じ問題に取り組む人々と交流し、エキスパートによる講演やライブデモをご覧ください。

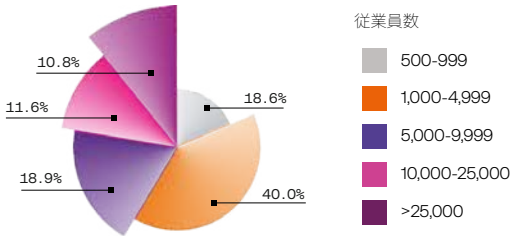
調査手法

この調査は 2024 年 9 月にオンラインで実施されました。回答者は情報セキュリティ分野のさまざまな役職の人で構成されています。およそ 30% が CIO、CISO、またはその他のシニアリーダー職でした。調査参加者は北米、ラテンアメリカ、ヨーロッパ、アジア太平洋の 4 つの地域の 14 ヶ国から参加しています。組織の規模としては従業員 500 人規模から 25,000 人規模までであり、ほとんどの参加者（59%）は従業員 1,000 人以上 10,000 未満の組織に勤めていました。

調査参加者の役職



調査参加者の組織の規模



免責事項：

本報告書は、サイバーセキュリティおよび IT プロフェッショナルがサイバーセキュリティにおける AI についてどのような見方をしているかを評価するための調査から得られたデータに基づいています。調査結果は、調査参加者の自己回答による評価や主観的意見に基づくものであり、客観的パフォーマンス指標や独立して検証されたデータに基づくものではありません。

本報告書は、市販可能性または特定目的への適合性の黙示の保証、または非侵害の保証を含めてこれらに限らず、明示または黙示のいかなる保証あるいは表明もなく提供されるものです。ダークトレース、執筆者、および関係する組織は、本報告書に含まれる情報の完全性、正確性、あるいは信頼性について、特に調査の回答の主観的性質に関して、何らの表明または保証も行いません。

ダークトレース、執筆者、および関係する組織は、本報告書の内容の間違い、脱落、あるいは本報告書の内容に基づいてとられた行動に対して何らの責任も負いません。本調査書をお読みになる方は、AI を使ったサイバーセキュリティおよび組織の準備に関する最新かつ最も包括的な情報について、追加の情報源を参照し、専門家に相談されることをお勧めします。

■ **ダークトレースについて**

ダークトレース（ロンドン証券取引所上場、ティッカーシンボル：DARK）はAIサイバーセキュリティのグローバルリーダーで、サイバー破壊から世界を解放することを使命としています。ダークトレースの技術は「御社」についての知識を常時学習・更新し、その理解を適用してセキュリティオペレーションの変革およびサイバーリジリエンスの強化に貢献します。 ダークトレースの各研究開発センターにおける画期的なイノベーションにより、これまでに200件以上の特許を出願中です。従業員数は世界各国で2,400名を超え、10,000社以上の顧客を既知、未知および新手のサイバー脅威から保護しています。

北米：+1 (415) 229 9100　ヨーロッパ： +44 (0) 1223 394 100　日本： (03) 5456 5537　ラテンアメリカ：+55 11 4949 7696

darktrace.com/ja | japan@darktrace.com