deep instinct™

VOICE OF SECOPS 2024 年第 5 版

サイバーセキュリティにおける AI: 敵か味方か

調査レポート

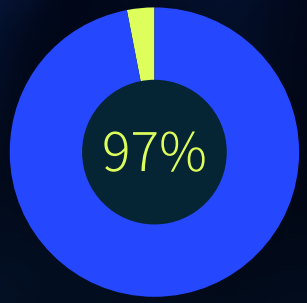
目次

概要

人工知能 (AI) はビジネスのやり方を**変革しています**。プロセスを簡素化し、イノベーションを促進し、組織構造に影響を与えています。実際、米国のすべての連邦政府機関には最高人工知能責任者を置くことが義務付けられるようになり、この流れはすぐに Fortune 500 企業にも波及するだろうというのがアナリストの予測です[1]。また、コーポレートガバナンスにも影響を与えており、半数以上の組織が何らかの形で RAI (責任ある AI) ポリシーを導入しています[2]。

AI は、ビジネスのやり方を変革する上で有益ですが、それは攻撃者にとっても同じです。攻撃者もまた、より巧妙で的を絞った攻撃を実行できるようプロセスを簡素化し、マルウェアのイノベーションを促進し、攻撃チェーンを自動化しています。

AI を悪意のある目的で広く使用するという新たな時代に入ったのです。ChatGPT や Gemini などの一般的なツール (さらにダーク AI ツール[3]) により、このテクノロジーが技術レベルの低い幅広いユーザーにも知られるようになり、こういったユーザーも簡単に、高度なフィッシング攻撃をカスタマイズしたり、新たなマルウェアの作成や開発を行ったりできるようになっています。一方、組織はその結果に対処するための準備ができていません。



敵対的 AI による セキュリティ インシデントの 発生を懸念している サイバーセキュリティ 専門家の割合

このような脅威情勢で EDR (エンドポイント検知・対応) ツールに全面的に頼るのは、警報級の大火災に対して散水ホースで消火しようとするようなものです。効果がなく、受身型であり、コスト高になりがちです。実際に **SecOps チームも、サイバーセキュリティ経費の 45% は無駄だと考えています。**何日、何週間、または何か月までであれば検知＆対応といった内容でも許容されるのでしょうか？

まったくの事後対応で修正に焦点を当てた戦略から、脅威が侵入する前に阻止できる予測・予防型のサイバーセキュリティテクノロジーに移行すべきという圧力は高まっています。**今年、半数以上 (53%) の企業で、予防ファーストのサイバーセキュリティ戦略を優先事項にせよという取締役会からのプレッシャーが高まっています。**

生成 AI の隆盛と、その脅威情勢への影響は、サイバーセキュリティ専門家にも負担をかけており、**56% が「ストレスレベルが去年よりも悪化している」と回答し、66% が「AI が燃え尽きやストレスの原因になっている」と回答しています。**

サイバーセキュリティ業界は、世界レベルの聡明かつ革新的で優秀な人材を擁しています。彼らは、悪意のある攻撃者とその AI の利用に一歩先んじるために、どのような対策を講じているのでしょうか？Voice of SecOps レポートの第 5 版では、セキュリティオペレーションの専門家が、どのように進化する脅威から防御し、高まるプレッシャーに対応しようとしているかを探ります。また、組織における将来的なサイバーセキュリティの見通しについても評価します。

1 https://www.forbes.com/sites/robtoews/2023/12/21/10-ai-predictions-for-2024/?sh=4a9ea9884898
2 https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence/what-is-responsible-ai/pwc-responsible-ai-maturing-from-theory-to-practice.pdf
3 FraudGPT、WormGPT、EvilGPT など – https://news.luddy.indiana.edu/story.html?story=Luddy%E2%80%99s-firstofitskind-research-exposes-LLM-risk

主な調査結果

EDR に過度に依存していると、次世代型サイバー攻撃に対する脆弱性を解消できない

- 昨年は、61% の企業でディープフェイクインシデントの増加が見られ、そのうちの 75% で CEO などの経営幹部のなりすましが行われていました。
- 97% が敵対的 AI によるセキュリティインシデントの発生を懸念しています。
- しかし、41% の企業は、敵対的 AI からの防御を EDR ソリューションに頼っています。
- 35% が EDR ソリューションの導入を計画しており、31% が未知の攻撃に備えて EDR 投資を増やす予定です。

AI 活用型サイバー攻撃が予防ファースト戦略への移行を促している

- 75% が、過去 12 か月の間に AI の隆盛によってサイバーセキュリティ戦略に影響または変化があったことに同意し、73% が予防に置く比重を増やしています。
- 53% のサイバーセキュリティ専門家が、経営陣からの予防ファースト戦略を実施せよという圧力を感じています。
- 42% の企業が現在、敵対的 AI から自社を守るために予測による予防プラットフォームを含めた予防テクノロジーを利用しています。
- 38% が未知の攻撃に備えて、予防ベースのソリューションを検討しています。

AI が燃え尽きを助長し、過度な負担を抱える SecOps チームはストレスに悩まされている

- サイバーセキュリティ専門家の 66% が、AI が燃え尽きやストレスの原因になっていると回答しています。
- 66% が、AI によって仕事へのプレッシャーが増していることを認めています。
- しかし、回答者の 35% は、AI ツールを導入することで、時間を作り、定型的な作業に費やす労力を減らしています。
- 35% はまた、予測による予防のようなプロアクティブなサイバーセキュリティ対策がストレスの軽減に役立っていると回答しています。

01

第 1 節：

サイバー脅威の進化が EDR 依存に疑問符を投げかける

AI を活用した高度なサイバー攻撃に EDR で対抗することには限界があるという認識が高まっており、近年のサイバー攻撃によって、EDR が無効であることの証明は積み上がるばかりです。たとえばマイクロソフトに対する攻撃では、攻撃者はネットワークに侵入したあとも数か月の間まったく検知されませんでした。検知して対応するまでに、どれだけ時間がかかるのでしょうか。

しかし、リソース不足、業務負荷の増加、今日のポスト EDR ブームにおいて最適な代替ソリューションが不明であるなどの要因から、企業は膨大な金銭的リスクと信用に対するリスクにさらされています。

新たなリスクが議題に上り、ディープフェイクが最大の懸念事項に

ディープフェイク、生体認証なりすまし、敵対的 AI は、2024 年における最大級のサイバーセキュリティリスクです。ランサムウェアや武器化したファイルなど従来のリスクがサイバーセキュリティチームを悩ませ続ける中、あまり一般的でなく、理解もされていない脅威に注意とリソースが集まりつつあります。

ディープフェイクという概念は、誕生してまだ 10 年足らずのものですが、その利用は最近になって爆発的に増えており、その影響は政治からエンターテイメント、企業のビジネスに至るまで、あらゆる領域に及んでいます。2024 年 2 月には、ある多国籍企業で従業員がディープフェイクに騙されて約 2,500 万ドルが失われました[4]。

ディープフェイクは有名人のなりすましに使われるだけではなくなりました。今では、企業の経営陣のなりすましに使われており、従業員を騙すのは以前よりも簡単になっています。**ディープフェイクが増加したと回答した人の 4 分の 3 (75%) は、それが CEO などの経営幹部のなりすましに使われていたと回答しています。事実、Deep Instinct の CEO である Lane Bess も、ディープフェイクを作成されたことがあります。**さらに悪いことに、現在のセキュリティ研修のカリキュラムではディープフェイクを十分に扱っておらず、SecOps チームと他部門の従業員との間に大きな教育格差が生まれています。

61%

の企業で過去 1 年間にディープフェイクによるなりすましが増加

ディープフェイクとは

ディープフェイクとは、ディープラーニングで生成された動画、画像、音声クリップのことで、通常は悪意のある目的で偽のシナリオに実在の人物を登場させるために生成されます。公開されている SNS の投稿や音声ファイル、動画を使って生成するのが一般的です。

図 1: 列挙された脅威のうち、自社のセキュリティに対する最大のリスクとなる課題は何かを質問

4 https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

事後対応に関する不確実性が存在し、EDR への過度な依存が続く

SecOps チーム内の自信レベルは、新たな脅威の量と巧妙さによって影響を受けています。**2023 年には、回答者の 67% が前年 (2022 年) よりも上手く脅威に対応できたと考えていました。それが今年は 58% に減っています。**

EDR への投資は、AI 活用型攻撃の防御には適さないにもかかわらず続いています。実際、**41% が、敵対的 AI からの保護に EDR などのエンドポイント保護ソリューションを使い続けようとしています。**さらに 35% 以上が、未知の攻撃の増加に備えて EDR の導入を計画しています。しかし、攻撃者が EDR の防御を回避し、長期にわたって検知されずに潜んでいたという事態は繰り返し発生しています。

このアプローチでは、サイバー犯罪者はチェスをしているのに、防御者だけは時代遅れのツールでチェスでなくチェッカーをしているようなものです。

勇気づけられる点を挙げるとすれば、**未知の攻撃から防御する方法のトップとして挙げられたのが、より優れた予防を提供できるソリューションを使用することであった点です。**昨年の調査の 3 位から 1 位に浮上しています。

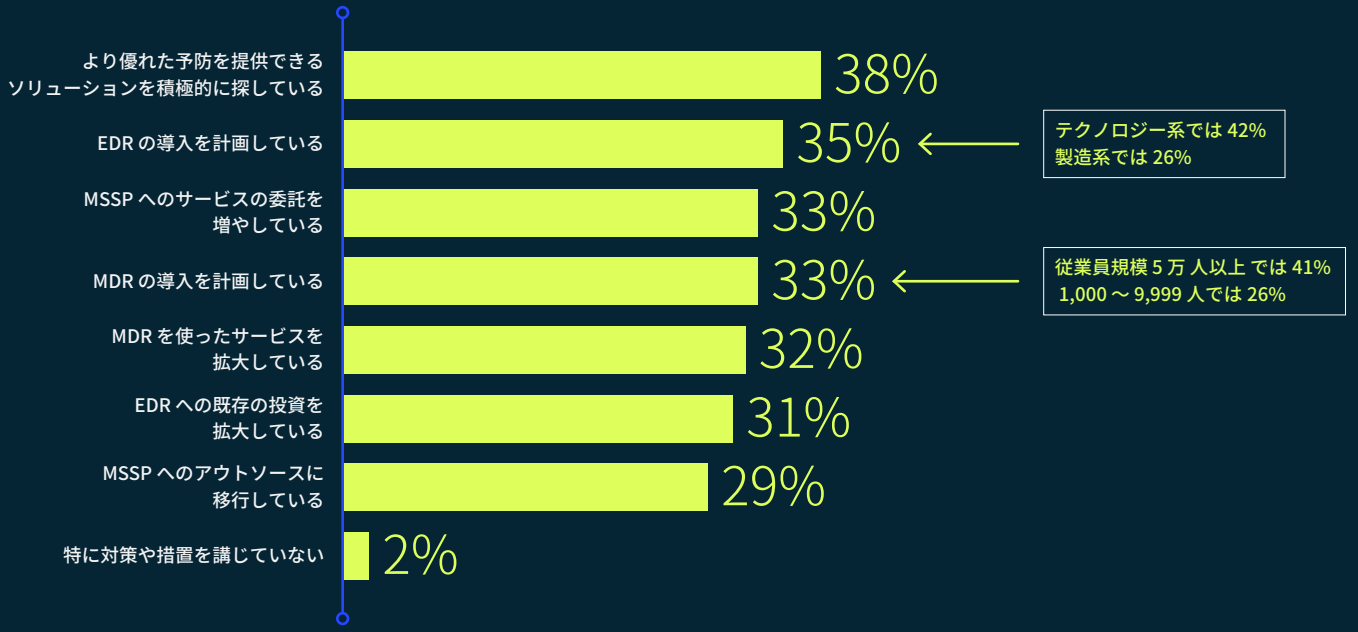


図 2: 未知の攻撃の増加に備えて措置を講じているか、講じていれば、それが何かを質問

AI を活用した脅威が既存の防御戦略を脅かしている

AI には良い意味で大きな可能性がありますが、サイバーセキュリティ専門家は、それがもたらす脅威も強く感じています。私たちの調査によると、**97% が、自社が AI 生成型のゼロデイ攻撃に見舞われることを懸念しています。また、同じ割合の回答者が、敵対的 AI が起こすセキュリティインシデントを恐れています。**

こういった背景から、**経営幹部は AI 活用型のサイバー脅威への自社の備えを疑問視しており、3 分の 1 (33%) が AI システムや AI ツールへの可視化不足を懸念しています。**

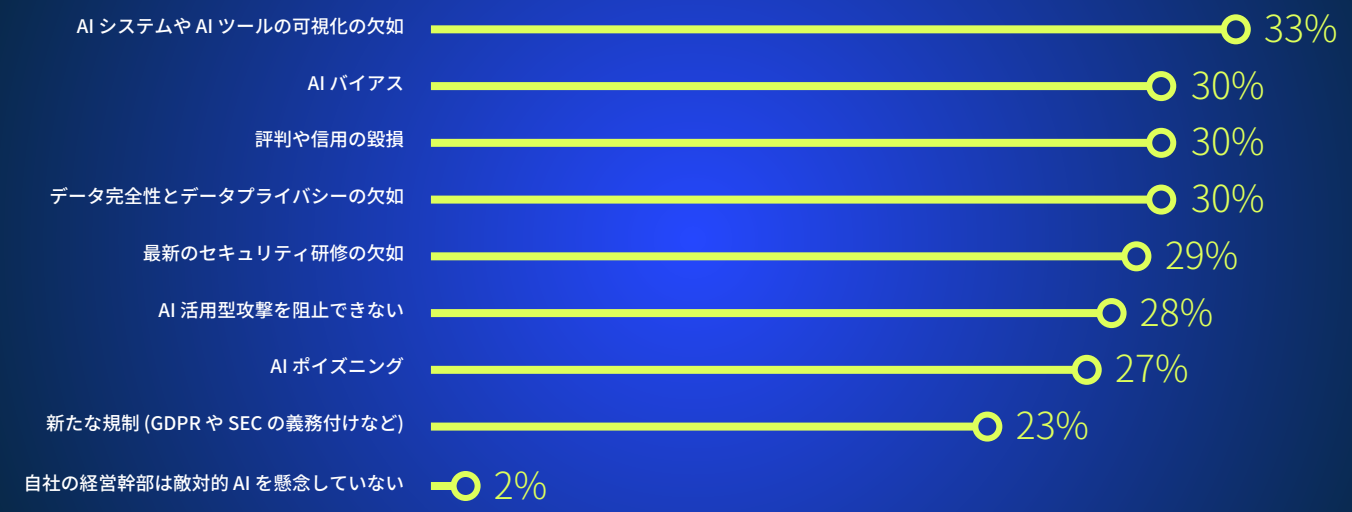


図 3: 敵対的 AI に関して自社の経営幹部が最も懸念していることを質問

「敵対的 AI」とは

人工知能 (AI) や機械学習 (ML) のシステムの能力を、操ったりミスリードしたりすることで阻害しようとするサイバー脅威を敵対的 AI と呼んでいます。攻撃者が危害を加えるために使用する多くの手法 (自動ハッキング、AI 活用型フィッシング、回避技術、ディープフェイクなど) の一つです。

約半数がサイバーセキュリティ投資を無駄と考えるが、改善のためのスキルは不足している

サイバーセキュリティ専門家は、現在、予算のほぼ半分 (45%) が無駄になっていると考えています。この驚くべき数字は、たとえば年間売上 750 億円で、その 3% を IT に費やしている[5] (その 13% がセキュリティ[6]) 企業の場合、毎年 約 1 億 300 万円を無駄にしていることになります。

進化を続ける脅威を特定および阻止するために 1 円も無駄にできない時代に、これほど多くの予算が効果のないソリューションに費やされている理由は何でしょうか？**社内の専門知識が限られていること、ベンダーからの影響、予算の制約などが主な理由として挙げられています。**しかし、この質問に対する回答がばらばらであることから、根本的な問題が真に理解されていないことが示唆されます。

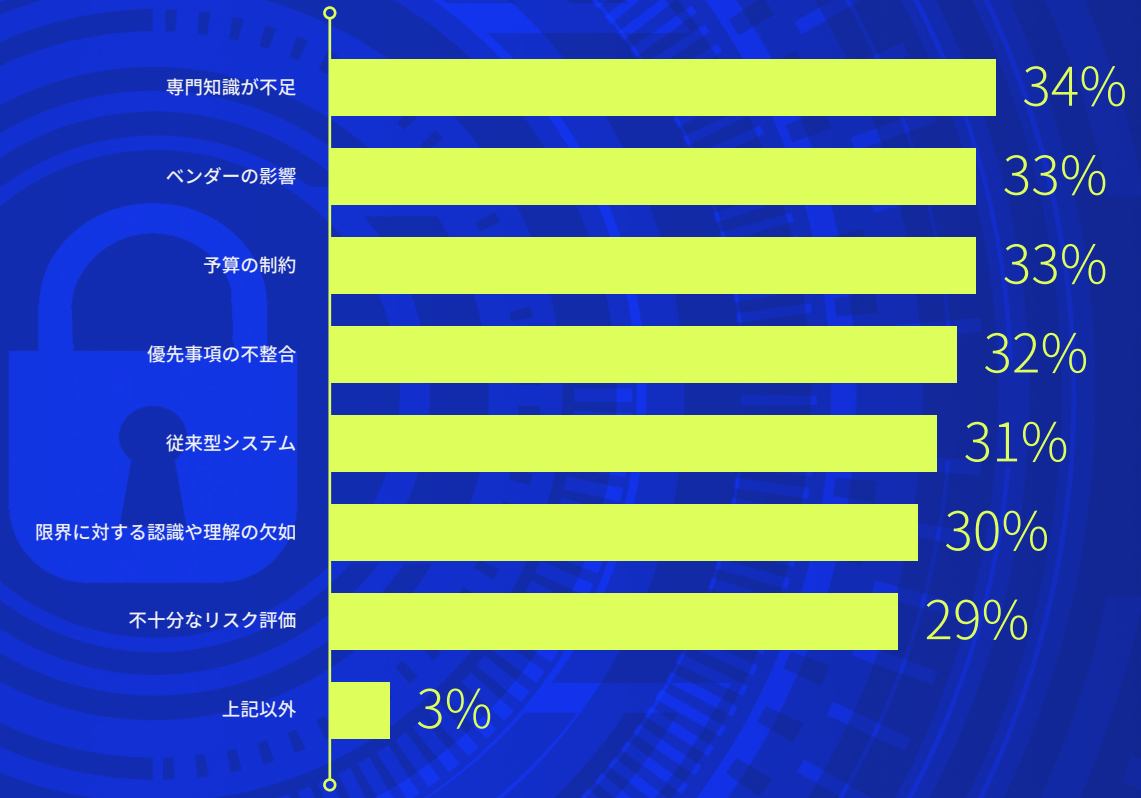


図 4: 防御に効果がない場合、それにまだ投資している理由を質問

5 https://www.techtarget.com/searchcio/definition/IT-budget-information-technology-budget
6 https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

02

第 2 節：

AI の悪用が事後対応から予防への移行を促進

AI で新たな発展があるたびに、攻撃者もそれを利用しようとします。既知の攻撃と未知の攻撃の両方の一歩先を行くには、予防を優先した対策を取るしかありません。経営幹部からの圧力が高まる中、研修と技術で脅威に対抗する取り組みが強化されています。

AI 活用型脅威との戦いには予防技術とトレーニングが重要

各企業は、悪意のある AI との競争に勝とうと、従業員のスキル向上を急いでいます。脅威が拡大し進化する中、ほぼ半数 (47%) の企業が、AI 攻撃に対抗するためのセキュリティ意識の向上とトレーニングプログラムに取り組んでいます。

また、回答者の 42% が、こういった脅威から被害を受ける前に身を守るためには**予測型予防プラットフォームが重要であることに同意しており、その認識は高まっています。**

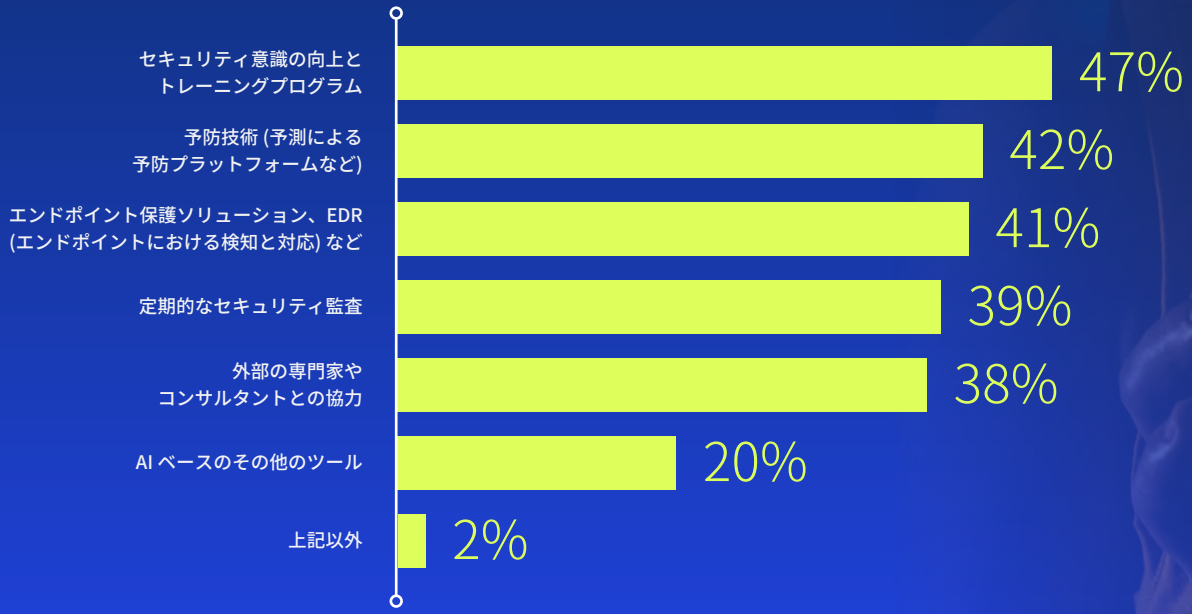


図 5: 現在、敵対的 AI から自社を守るのに役立っている既存のツールや手法を質問

「最高セキュリティ責任者、最高データ責任者、その他の AI に注力する経営幹部は、急速に進化する分野の最新テクノロジーが組織において利用されるよう積極的に取り組むべきです。たとえば、投資予算を策定する際に敵対的 AI ソリューションのエコシステムを理解し、評価するなどです。AI/ML セキュリティの研究とインフラ開発には資金のごく一部しか割り当てられていませんが、多くの民間企業、学術機関、政府機関が敵対的 AI 攻撃に対抗するソリューションの開発と投資を行っています」

Securing Government against Adversarial AI (Deloitte Insights)[7]

7 https://www2.deloitte.com/uk/en/insights/industry/public-sector/adversarial-ai.html

トップから予防ファースト戦略への優先を求める圧力が強まる

取締役会と経営幹部は、株主、顧客、アナリストにサイバーセキュリティ体制の堅牢性を保証すべきというプレッシャーを感じています。セキュリティオペレーションチームには、こうした外部からの圧力が伝わってきており、その**半数以上 (53%) が、サイバーセキュリティに予防ファーストアプローチを採用せよというプレッシャーが増していると回答しています。**

この傾向は**金融サービス業界で明確に見られ、回答者の約 3 分の 2 (65%) が経営陣から予防ファースト戦略の実施を迫られています。**金融サービス業界はサイバー犯罪の主要な標的となっています。2023 年の第 2 四半期だけで 130 万件のフィッシング攻撃が報告されていますが、金融サービス業界を狙ったインシデントは 23.5% と最多でした[8]。

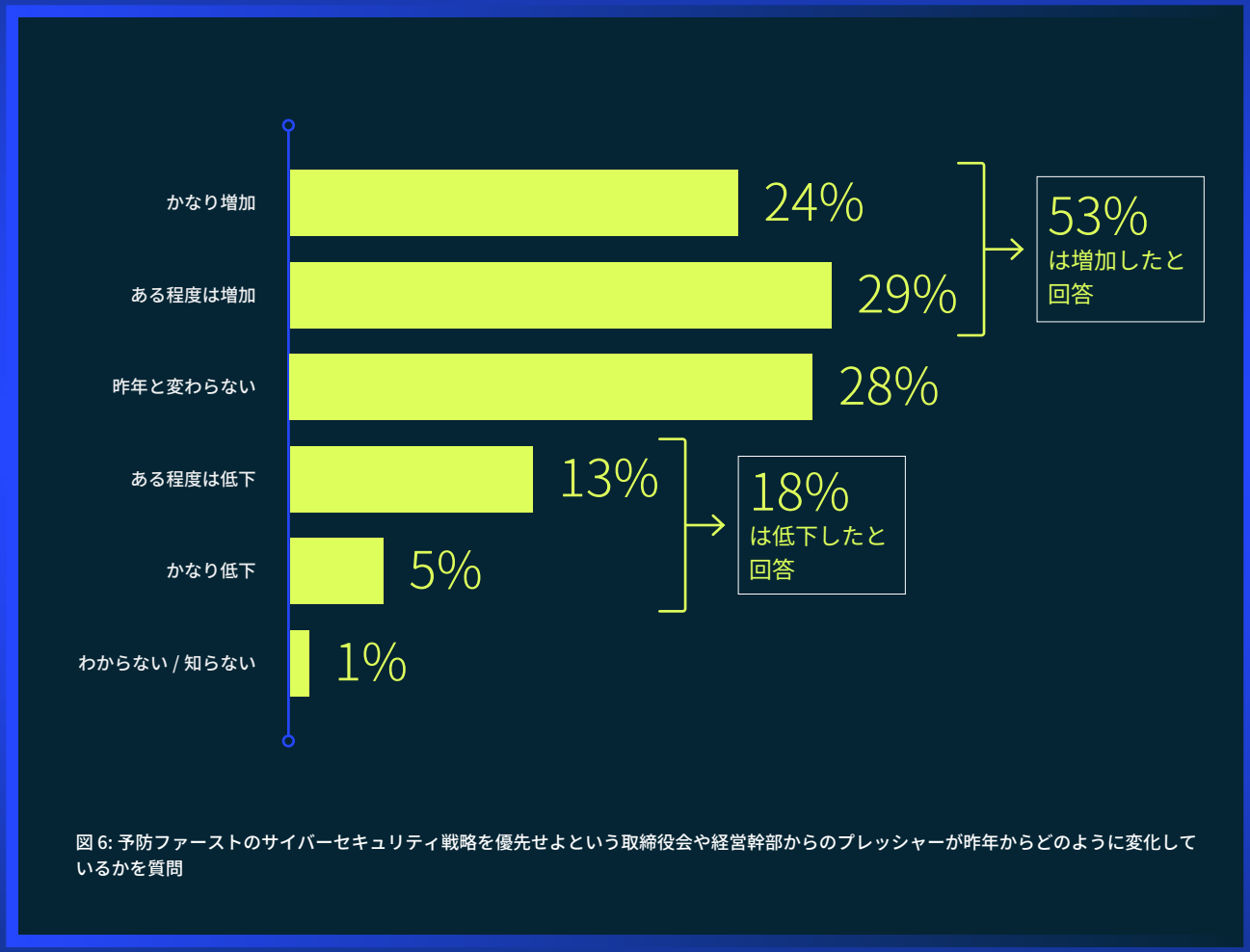


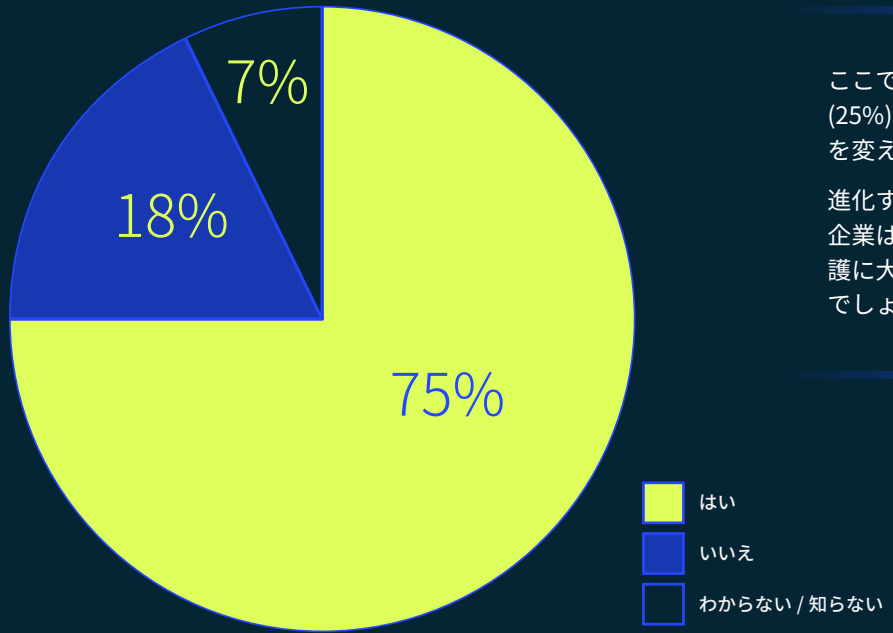
図 6: 予防ファーストのサイバーセキュリティ戦略を優先せよという取締役会や経営幹部からのプレッシャーが昨年からどのように変化しているかを質問

8 https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf

4 分の 3 がサイバーセキュリティ戦略の変更に取り組む

サイバーセキュリティという機能は、けっして立ち止まりません。技術の進化に合わせて、それを守る戦略も進化する必要があります。しかし、AI はこれまでにないほどの変化を推し進めています。**75% は、自社のサイバーセキュリティ戦略が AI の隆盛を理由に昨年から変更を余儀なくされていると回答しています。**

戦略に変更があったうち、ほぼ同じ割合である 4 分の 3 **(73%) が、重点が予防に移ったと回答しています。**



ここで最も驚くべきことは、4 分の 1 (25%) の企業が過去 12 か月間に方針を変えていないことです。

進化する脅威情勢に適応できなかった企業は、IT 資産や価値あるデータの保護に大きな問題があることを認識するでしょう。

図 7: 最近の AI の隆盛を受けて過去 1 年間 (2023 ～ 2024 年) に自社のサイバーセキュリティ戦略に変化があったかどうかを質問

大規模言語モデル (LLM) の活用は業種によって大きく異なる

AI を活用して自社のサイバーセキュリティをテストすることに関して、金融サービス業界が再び主導的な役割を果たしていることがわかります。全業種を通じた大規模言語モデルと新たなツールの最も一般的な用途は、標準的なセキュリティ作業の自動化です。

しかし、金融サービスの回答者の半数以上 (56%) が、セキュリティレジリエンスをテストするための敵対的 AI 関連の技術開発にメリットがあると考えているのに対して、公共部門では 27% にすぎませんでした。

図 8: 大規模言語モデルや新たなツールなどの進化をどのようにサイバーセキュリティに活用できるかを質問

03

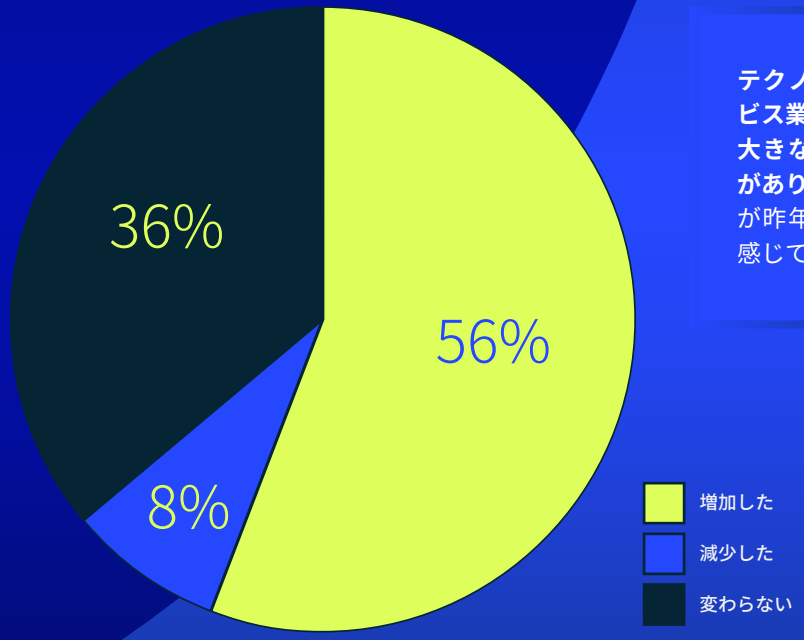
第 3 節：

燃え尽きとストレスが SecOps チームを悩ませ続ける

サイバーセキュリティ業界は従来からスキルの格差に悩まされてきました。こうした業界特有の人材不足に加えて、AI 活用型脅威への対応が、セキュリティ運用メンバーのストレスレベルを上昇させています。AI の悪用がこのプレッシャーに寄与する一方で、企業はこのテクノロジーの有益な面を活用して時間を作り、定型的な作業からより付加価値の高い仕事に重点を移しています。

生成 AI が続々と登場する中、SecOps チームは休む暇がない

ストレスレベルは昨年とほぼ同じ水準で、**56% が過去 12 か月に増加したと回答しました** (2023 年は 55%)。ただし今年は、**生成 AI によるリスクの増加に関係する懸念がストレス要因のトップとなり、**昨年の 3 位から上昇しています。



テクノロジー業界と金融サービス業界では、他の業界よりも大きなストレスレベルの上昇があり、それぞれ 64% と 61% が昨年よりもプレッシャーを感じていると回答しています。

66%
のサイバーセキュリティ専門家が、AI によって仕事に対するプレッシャーが高まっていると回答

66%
のサイバーセキュリティ専門家が、AI が燃え尽きやストレスの原因になっていると回答

図 9: 過去 12 か月で仕事中のストレスレベルがどのように変化したかを質問

人材不足とスキル不足が続き、燃え尽きの問題が深刻化

生成 AI への懸念と並ぶ主なストレス要因は、高いスキルを持ったサイバーセキュリティ人材の確保と定着が変わらず難しいことです。現在世界中のサイバーセキュリティ業界で約 500 万人が働いていますが、それでもまだ全世界で 400 万人が不足していると試算されています[9]。

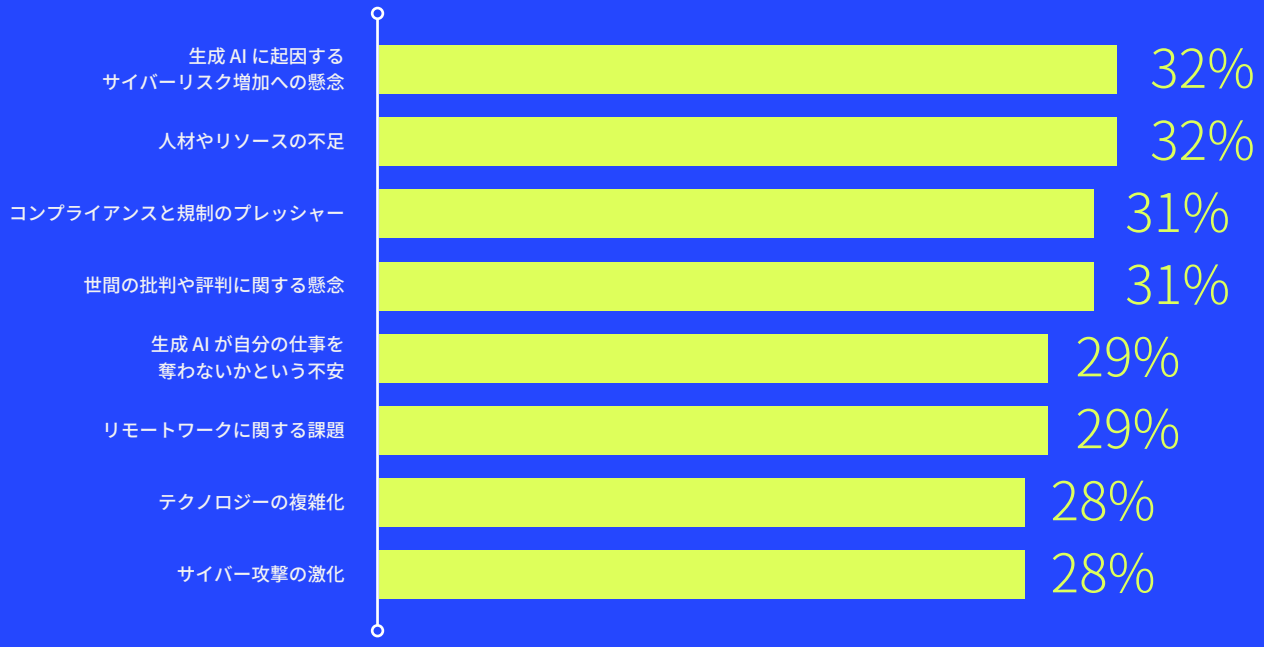
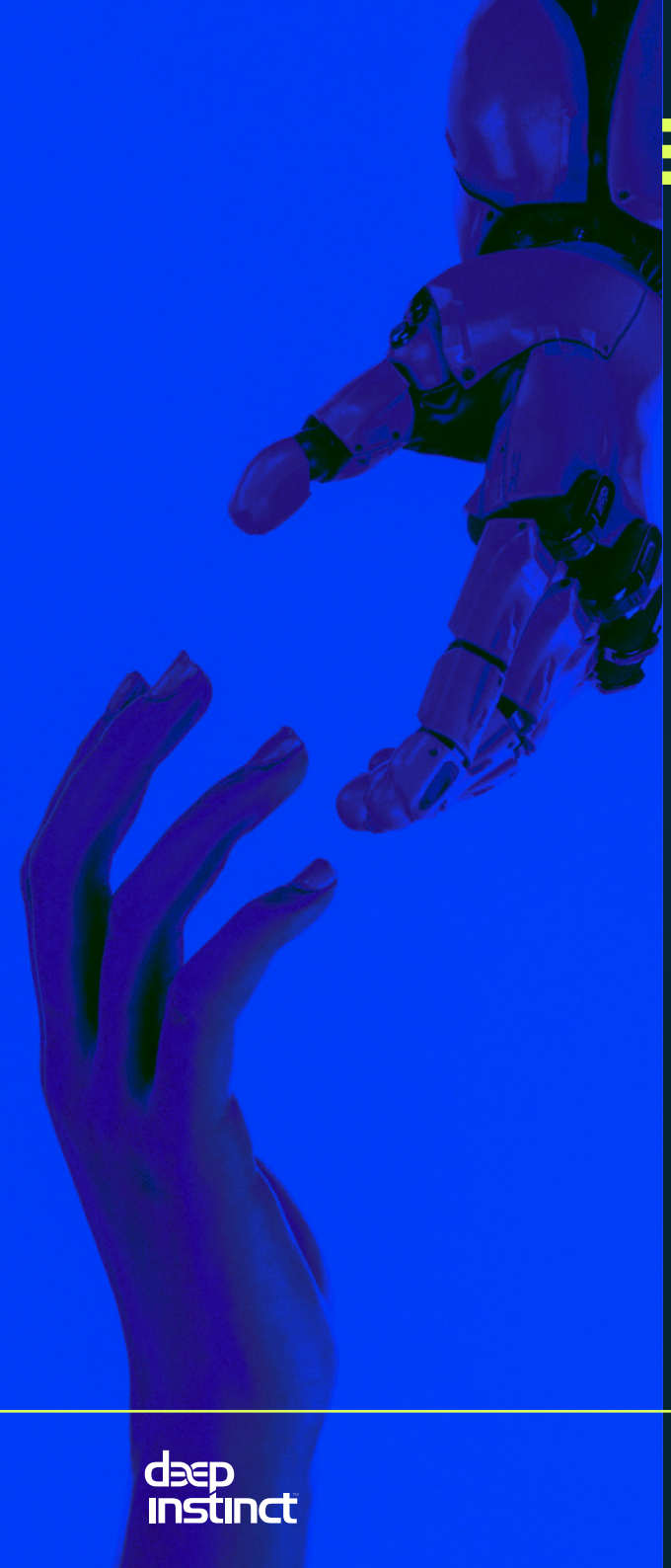


図 10: 過去 12 か月間のストレスレベルの増加の背景にある主な理由を質問

9 https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020



ストレスを軽減しようと AI に目を向ける企業

企業の 3 分の 1 以上 (35%) が、サイバーセキュリティ専門家の職場におけるプレッシャーを軽減するために、AI のメリットを活用しています。こういったツールは、時間の余裕を生み、より付加価値の高い仕事に集中できるように使用されています。

他の**ストレスを減らすための戦略のトップは、予測型予防のようなプロアクティブなサイバーセキュリティ対策の導入です。**SecOps チームが対応する必要のあるインシデントの数と、侵害への対処に関連したストレスを削減します。

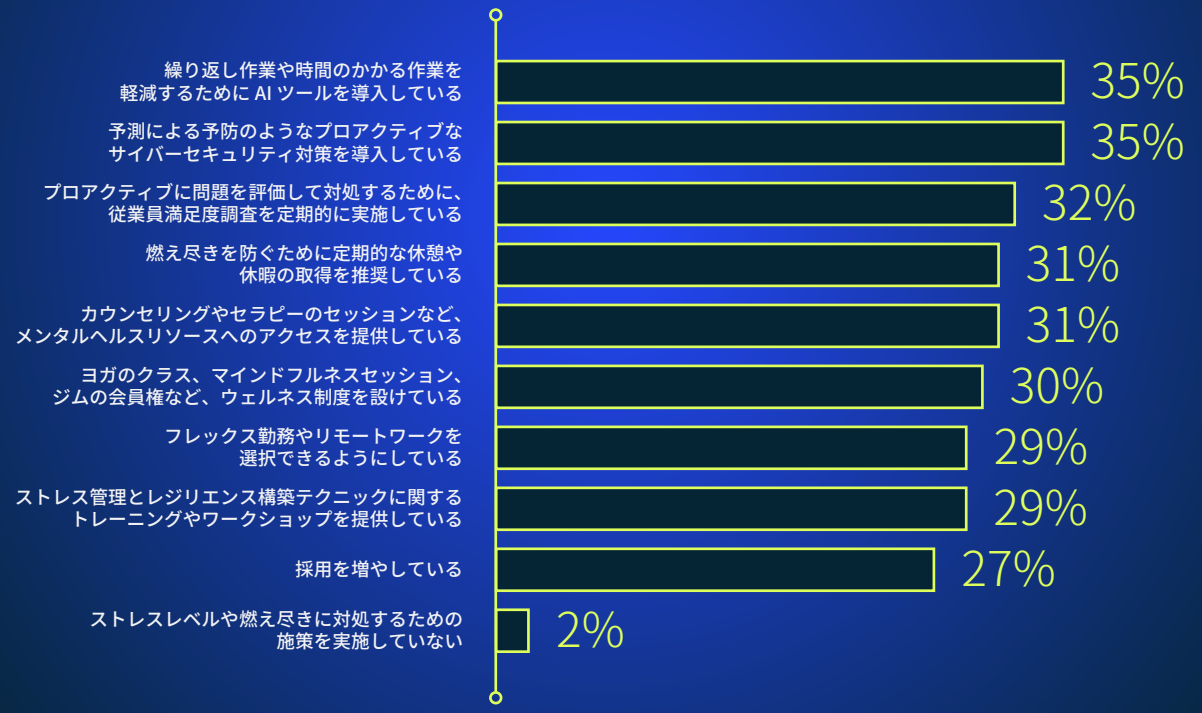


図 11: ストレスレベルと燃え尽きに対処するために行っていることがあれば、それがどのようなものかを質問

セキュリティ研修は期待外れ

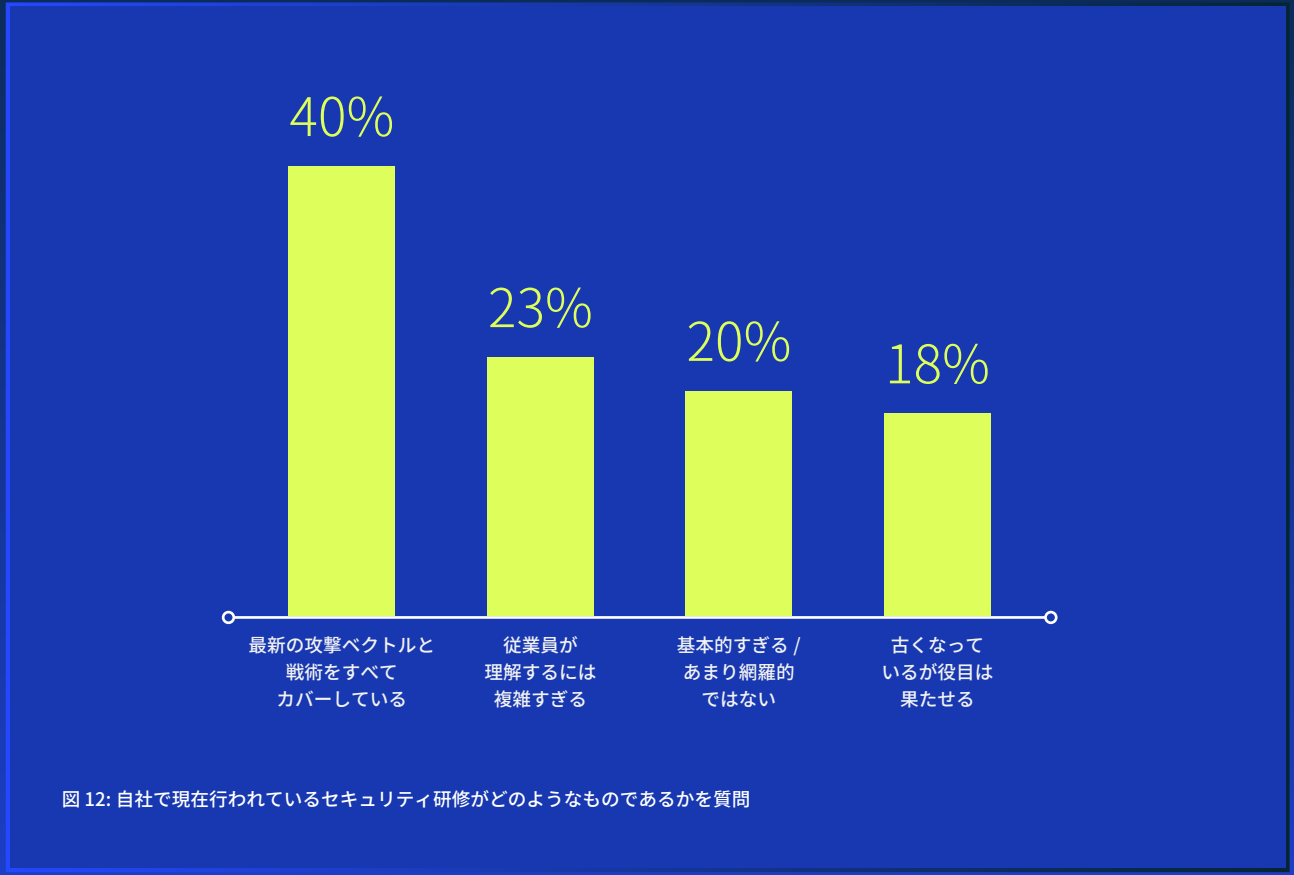


図 12: 自社で現在行われているセキュリティ研修がどのようなものであるかを質問

41% の組織が、セキュリティ研修は毎月更新すべきだと考えていますが、実際に更新しているのは 29% にすぎませんでした。さらに、回答者の 8% は、所属する組織でセキュリティ研修がまったく行われていないことを認めています。

研修内容に関しても、期待と現実の間に同様の不一致が明らかに見られ、**61% が複雑すぎる、簡単すぎる、あるいは内容が古いと回答しています。**

「セキュリティリーダーは、意識を高めることから行動の変化を促すことに重点を移すことで、サイバーセキュリティのリスクを減らすことができると認識しています。2027 年までに、大企業の CISO の 50% が、サイバーセキュリティに起因するビジネス上の摩擦を最小化して制御の内容を最大化するために、人間を中心に据えたセキュリティ設計手法を採用するでしょう。SBCP (セキュリティ行動・文化プログラム) は、従業員の行動に関連したサイバーセキュリティインシデントを最小限に抑える全社的なアプローチをまとめたものです」

Top Cybersecurity Trends for 2024 (Gartner)[10]

10 https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

すべての AI が同じというわけではない - ディープラーニングの力

悪意のある AI 脅威に対抗するために検知・対応型ツールを使用するのは、馬が逃げ出してから馬小屋の戸を締めようとするようなものです。確かに、サイバーセキュリティ戦略の中に EDR や XDR のようなソリューションが必要な場面もありますが、現代の変わりやすい脅威情勢において、それでは不十分です。

私たちは、古い戦術に投資を続けることがいかに無意味であるかを見てきました。実際に SecOps チームも半分ほどの予算が無駄になっていると考えています。ランサムウェアの身代金と評判の毀損による損害額に、効果のないサイバーセキュリティツールのコストが加われば、維持不可能なレベルの支出となります。

サイバーセキュリティ専門家の 3 分の 1 がベンダーの影響によって予算が無駄になっていると回答するような環境では、正当な疑問を呈することが、将来のセキュリティ体制を堅牢にするために重要となります。AI から守るには、AI が不可欠なのです。

しかし、すべての AI が同じように作られているわけではありません。基本的な機械学習 (ほぼすべてのサイバーセキュリティベンダーが採用している技術) は、現在の脅威情勢において限界に達しています。「悪質な」AI には勝てません。ディープラーニングは最も先進的な AI であり、次の脅威を効果的に予防するための唯一の手段です。

ディープラーニングは人間の脳の学習能力から着想を得ています。サイバーセキュリティに適用すると、**自立的に脅威を予測して既知のマルウェア、未知のマルウェア、ランサムウェア、ゼロデイ攻撃を阻止します。クラウド分析や接続には依存しません。**

セキュリティ境界を巡る戦いの中で、ディープラーニングを活用した予防ファースト戦略こそが、次世代の AI 脅威に対抗する手段なのです。予測による予防を優先して、「侵入を前提」するマインドセットを過去のものにする時がやって来たのです。

> “どの AI も同じというわけではなく、このことはサイバーセキュリティベンダー業界では極めて顕著です。ディープラーニングは、CISO とセキュリティチームが、攻撃者の次の動きを予測して阻止することでイタチごっこに勝利できる唯一の手段です。
>
> **Deep Instinct CEO、Lane Bess**

調査方法

Sapio Research が、米国の従業員数 1,000 人以上の企業で 500 人の上級サイバーセキュリティ専門家に調査を行いました。インタビューは、2024 年 4 月にメールでの招待状とオンラインアンケートを使ってオンラインで実施されました。

回答者の勤務先は、金融サービス、テクノロジー、製造、小売、医療、公共部門、重要インフラ (電気通信、エネルギー、公益機関、輸送など) です。

経営幹部は、最高責任者、グローバル責任者、部門責任者、ディレクターの役割を持つ人を指し、部下は、マネージャー、管理者、アナリスト、チームリーダー、役員の役割を持つ人を指します。

Deep Instinct について

Deep Instinct は、世界初かつ唯一、サイバーセキュリティ専用のディープラーニングフレームワークを使用してランサムウェアなどのマルウェアを阻止する予防ファーストアプローチを採用しています。既知の脅威、未知の脅威、ゼロデイ脅威を予測し、20 ミリ秒未満という、最高速のランサムウェアによる暗号化の 750 倍の速さで阻止します。Deep Instinct のゼロデイ精度は 99% を超え、その誤検知率は 0.1% 未満を保証しています。Deep Instinct Predictive Prevention Platform は、ハイブリッド環境全体で脅威に対する完全な多層保護を提供する、すべてのセキュリティスタックに不可欠なコンポーネントです。www.deepinstinct.com/ja にアクセスして、詳細をご覧ください。

Sapio Research について

Sapio Research は、高品質で効率的かつ誠実な調査ソリューションで企業の成長を支援する、B2B 型テック市場の調査をフルサービスで提供する機関です。熱意と目的意識のある専門の市場調査チームであり、定量的調査と質的調査のすべての分野において、ブランドと PR・コミュニケーション代理店を情熱を持って支援しています。

クライアントが顧客を理解し、優れたコンテンツと見出しを作成し、市場に関連するビジネス上の重要な意思決定を行うことに役立つ、価値のあるエビデンスを提供しています。

英国を拠点とし、130 か国の 1 億 4,900 万人以上にアクセスがあります。一流のテック企業からグローバルコンサルタント、PR・コミュニケーション代理店、有名ブランドまで、さまざまなクライアントと提携しています。

Sapio Research でメッセージとなる“声”を見つけ、市場を魅了し、成長を促進しましょう。

Andrew White
Sapio Research
CEO 兼創業者

Jessica Bunce
Sapio Research
COO 兼創業者

Sapio Research

Pentagon House
52-54 Southwark St
London SE1 1UN
United Kingdom

sapioresearch.com
+44 (0) 207 236 1604