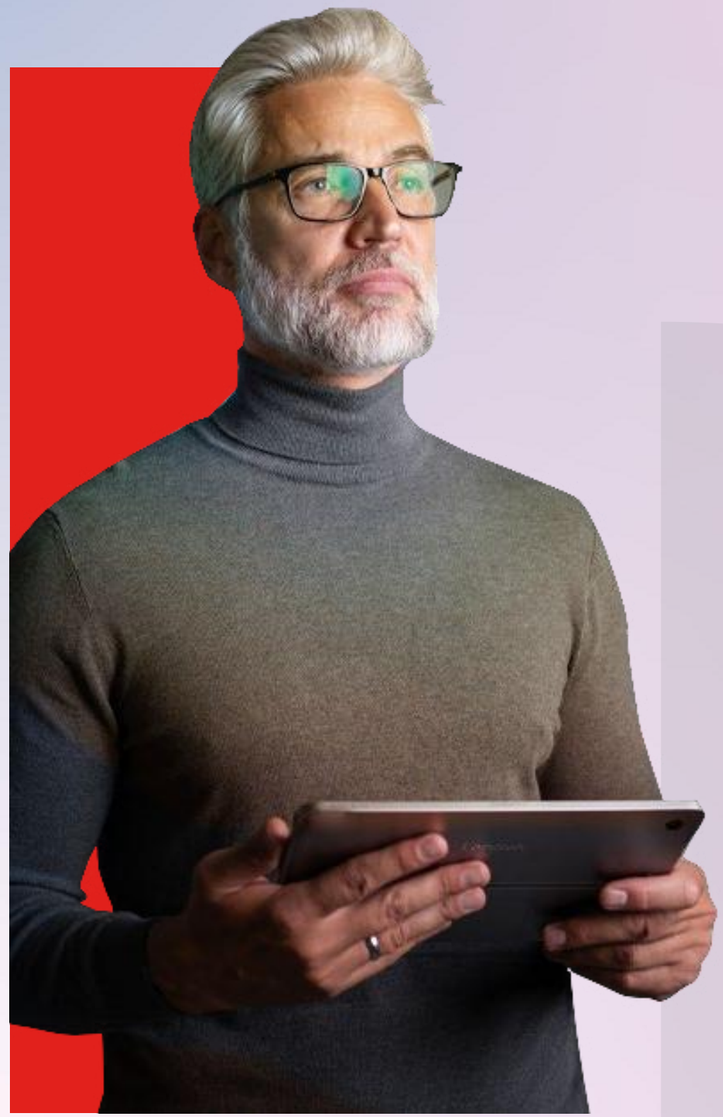


Lenovo Work Reborn Research Series 2025

現代における職場環境を強化する

AI脅威を正しく見極め、安心してデジタルワークプレイスを変革するために

続きを読む

Smarter technology for all

Lenovo

あらゆる変化に対応できるワークププレイスへ

AIを活用して、従業員の生産性を飛躍的に高めるために、ITリーダーはデジタルワークプレイスの変革に取り組む必要があります。
しかし、同時に進化し続けるセキュリティ脅威に備えながら進歩を止めないためには、防御体制も強化をしなければなりません。

Lenovoが発行した初回のWork Rebornレポートでは、ITリーダーにとって生産性や従業員のエンゲージメントが最も優先度が高いテーマであることを明らかにしました。
よりダイナミックで、AIを活用したパーソナライズされた職場環境を整えることで、従業員は創造的な問題解決と人との協働に集中できるようになり、本来の強みを発揮できるようになります。

さらに、多くのITリーダーがAIの生産性向上効果を最大限に引き出すためには、デジタルワークプレイスの根本的な変革が必要であると認識していることも分かりました。
AIが従業員それぞれのニーズを満たす環境を再構築し、ITサポートも従業員の業務を中断しない、シームレスな体験を提供できる環境へ見直す必要があります。

今回のレポートでは、AI時代のデジタルワークプレイス変革に欠かせないもう一つの重要な柱、サイバーセキュリティにも焦点を当てています。

AIの進化により、外部だけでなく内部からの新たな脅威も生まれています。
最新の調査では、企業のITリーダー600名に対して、どのAIセキュリティリスクを最も懸念されているか、そして見落としの可能性がある領域について尋ねました。

私たちは、モダンワークプレイスを守るためには以下にあげる、２つのアプローチが不可欠だと考えています。

１．AIによる新たな脅威を早く検知し、対策を強化すること。
２．AIをセキュリティ基盤に組込み、重要な資産を保護する体制を構築すること。

本レポートでは、ITリーダーが防御体制を進化させ、AIをサイバーセキュリティの中核に捉えるための具体的なステップを解説します。
これは、AIを基盤とする今日のワークプレイスにおいて、価値創造型への変革を実現するための道筋となるでしょう。

本レポートが皆さまのお役に立つことを願っています。

Rakshit

Rakshit Ghura
レノボ デジタルワークプレースソリューション
バイスプレジデント兼ゼネラルマネージャー

セキュリティを損なうことなく職場環境を変革

当社の調査は、AI時代において組織がサイバーセキュリティ防御をどのように進化させるべきかを明らかにしています。

セクションへ移動するにはクリックしてください:

1. **評価：**新たなAI脅威の特定
2. **進化：**AIにはAIで対抗
3. **強化：**Work Rebornへようこそ

評価

新たなAI脅威の特定

ITリーダーは、AIによってもたされるリスクに強い危機感を抱いています。
しかし、その脅威に十分対処できると自信を持てていないリーダーも少なくありません。

外部脅威から生じるリスクを理解する

ITリーダーは、AIに起因するサイバーセキュリティリスクに敏感です。特に懸念が高いのは、AIを悪用するサイバー犯罪者の存在であり、10名中6名以上が新たなリスク要因として認識しています。

90%

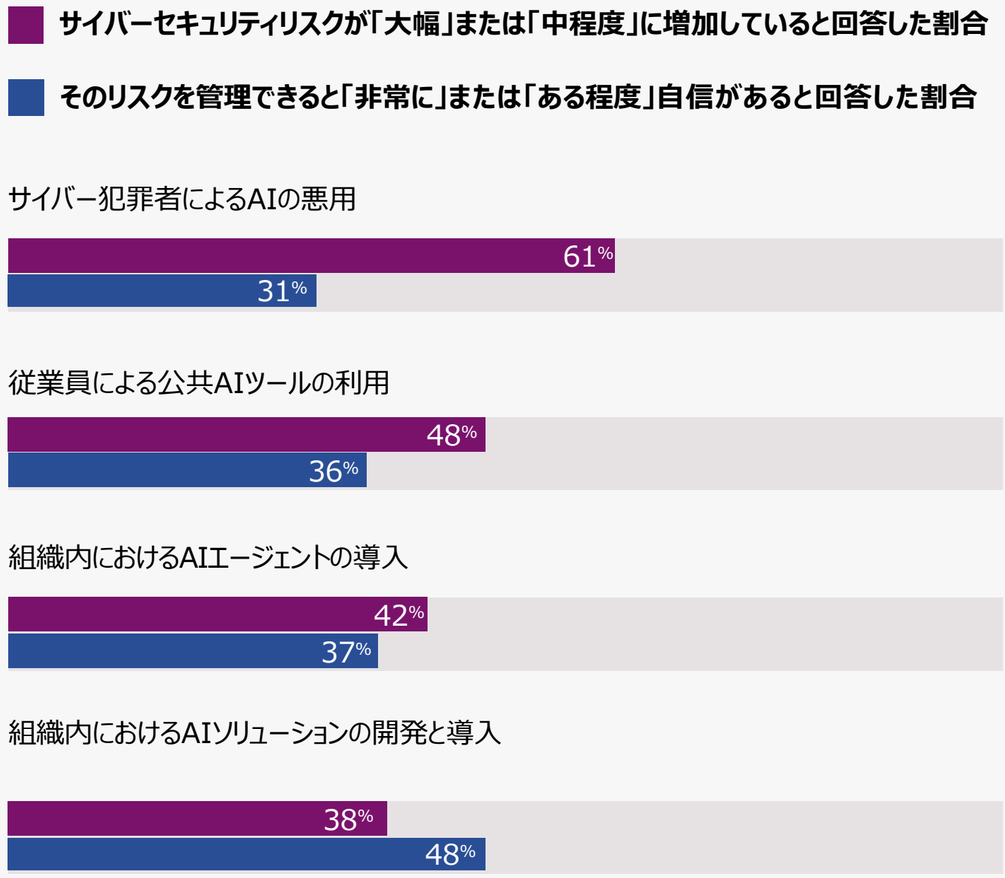
のITリーダーが
「AIを使うサイバー犯罪への対処に自信がない」
と回答している。

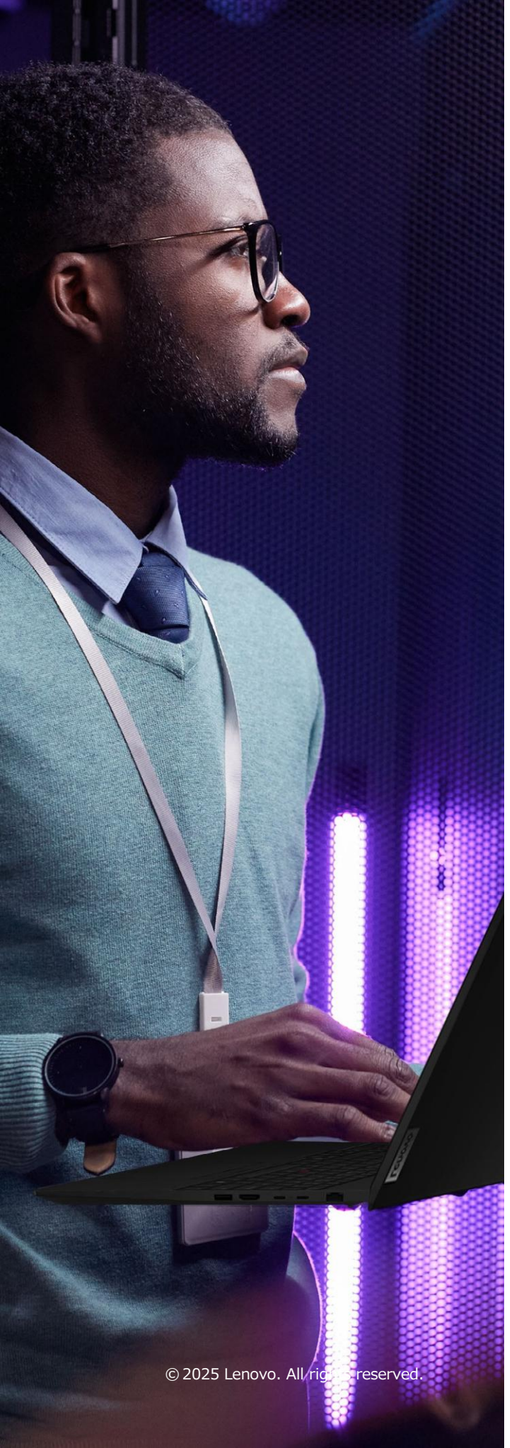
ITリーダーがサイバー犯罪者によるAIの活用を懸念するのは当然です。

AIは従来の攻撃手法に対する置き換えるのではなく、攻撃能力を増幅させ、
より高速かつ高度に従来の防御手段をすり抜ける手段を提供しています。

AIによって生成された攻撃は、防御する側の対策に応じて進化し、
人の行動を模範しながら多様な領域（クラウド、デバイス、アプリケーションなど）に対して
拡散することが可能です。

サイバーセキュリティリスクが増加している領域 vs ITリーダーの対応への自信





評価

内部に潜むAI脅威への対処

外部からのAIを悪用した攻撃を特定することは、AIセキュリティ全体への課題の一側面に過ぎません。
内部から生じるAIリスクにも、同様に備える必要があります。

10人中6人以上

ITリーダーの6割以上が、AIエージェントが新たな内部脅威を生み出しており、その脅威に対処する十分な準備ができていないと認識しています。

10人中7人

ITリーダーの7割は、従業員によるAIの誤用は、必ず対処が必要なリスクであると考えています。

10人中4人未満

これらのリスクを管理できると自信を持っているITリーダーは4割未満です。

AIは急速に進化しており、関連するサイバーセキュリティへの影響がようやく明確になり始めた段階です。これは、モデル、学習データ、プロンプトなどAI自体の保護にも範囲が及び、ITチームにとって重要なセキュリティ課題となっています。

外部からのAI攻撃への防御には自信が低い一方で、内部のAI活用によるリスクには比較的自信があるという結果がでています。

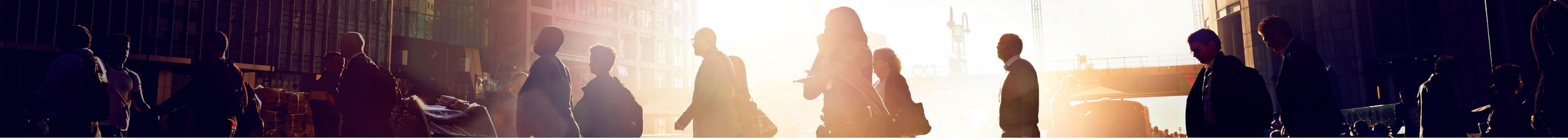
ITリーダーの約半数（48%）
社内でAIソリューションを開発・導入する際に発生し得るリスクについて「非常に」または「ある程度」管理できていると回答しています。

ただし、この自信は、適切なサイバーセキュリティ対策を既に導入している組織においては正当かもしれませんが、一部ではリスクを過小評価している可能性もあります。

「ITリーダーは複数のAIプロジェクトを急速に展開することに注力していますが、その過程で潜在的な脅威を見落とすリスクがあります。」

Tiago Da Costa Silva

レノボ デジタルワークプレースソリューション
セキュリティサービスディレクター



評価

新たなリスクには新たなアプローチが必要

従来のサイバーセキュリティ対策では、AI関連のリスクに対応するには不十分です。

ITリーダーは、自社のサイバーセキュリティ対策がAIに関連するリスクに追随できていることを確実にしなければなりません。多くの場合は、これらのリスクには従来とは抜本的に異なるセキュリティアプローチが求められます。

例えば、従来のデータ保護策（個人の役割に基づくアクセス制限など）は、AIが複数の文書を横断的に解析して回答を導き出す状況では、もはや十分とは言えません。

また、従来のエンドポイントセキュリティ対策（アンチウィルスなど）は、既知の脅威を検知することしかできません。AIは悪意あるコードをこれまでにない速度で生成でき、攻撃者は変異を続けるポリモーフィックマルウェアを容易に作り出すことができます。さらに、こうしたマルウェアは一般的な動作に紛れ込み、検知を回避します。

こうした新たなリスクに直面する中で、企業は防御能力を強化し、価値ある資産を保護するための対策を進化させ続ける必要があります。

「生成AIによって作られるポリモーフィック攻撃は、攻撃者に非対称な優位性を与えています。これにより、通常の業務に溶け込み、従来の検知技術をすり抜ける、より高速かつ巧妙な攻撃が可能になります。Zero Trustを導入していても、検知の失敗を前提に備える必要があります。」

David Majernik

レノボ シニア・オファリング・デザイン・テクノロジスト

AI時代のサイバーセキュリティのリスク要因

認識すべき新たな脅威：

- モデルポイズニング（データ汚染）
- AIモデルの改ざん
- AIによるデータプライバシー漏えいん
- AIへの過剰なアクセス権の付与
- AIへの敵対的攻撃（アドバーサリアル攻撃）
- AI生成によるマルウェア
- AI処理過負荷によるDoS（サービス拒否）攻撃
- AIによる幻覚（ハルシネーション）と誤情報
- AIアプリケーション経由のデータ漏洩
- シャドーAIの利用
- AIサプライチェーンリスク
- バイアスと倫理的リスクが引き起こす規制違反
- AIを活用したブルートフォース（総当たり）攻撃

評価

防御能力を見極める

IT リーダーは、データ保護と脆弱性管理が AI 関連の脅威に対抗するうえで最も重要なセキュリティ領域だと認識しています。しかし、その能力が十分だと自信を持っているわけではありません。

自信の不足が課題に

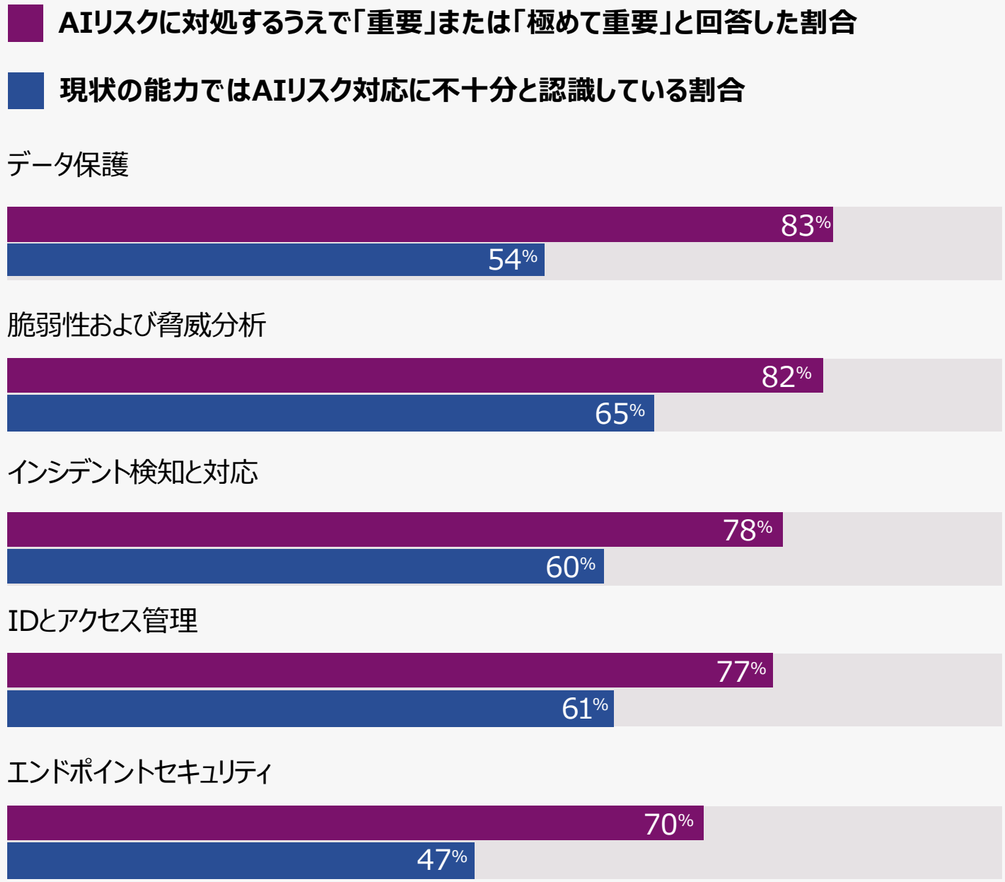
ITリーダーの過半数（**54%**）が、自社のデータ保護ツール、プロセス、スタッフの能力がAI関連のサイバーセキュリティ脅威に対処するには十分ではないと感じています。

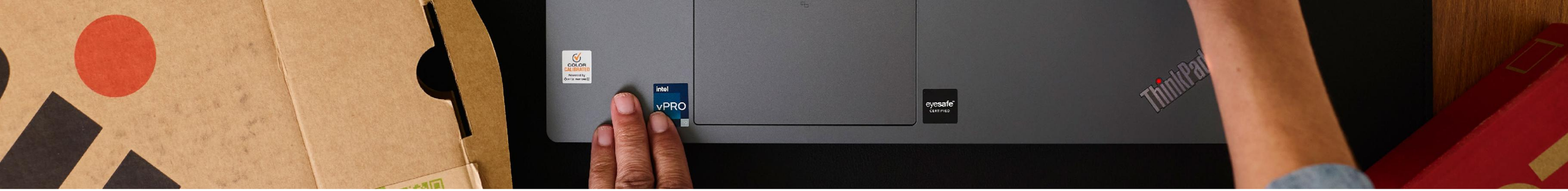
脆弱性分析や脅威分析の能力に自信を持っている企業はさらに少数です。

65%が、現状の能力ではAIの脅威に対処するには十分ではないと考えています。

また、大多数はインシデント検知と対応、IDおよびアクセス管理の能力においても同様に不十分だと認識しています。

ITリーダーが重要と考える機能 vs 実際に自信を持っている能力：





評価

AIリスクを理解し軽減するために

内部および外部から発生するAI由来のリスクを特定し、軽減するための推奨事項を紹介します。

外部脅威への対処

外部からの新たに発生するAI脅威を認識し、先手を打ってシステムを保護することが重要です。

セキュリティシステムの再評価

ITリーダーのサイバーセキュリティ能力に対する自信が低い現状において、企業はAI脅威に直面した際の防御能力を明確に把握することが不可欠です。その第一歩は、組織のサイバーセキュリティ体制と技術を動的に見直し、「企業が許容できるリスクレベルにあるか」を継続的に評価することから始める必要があります。

攻撃者の進化に対応する

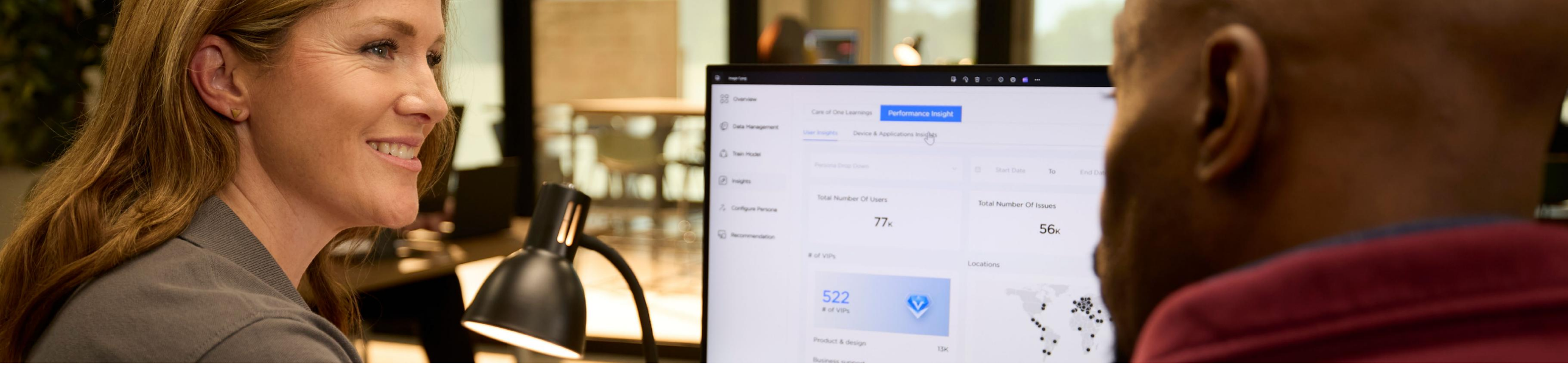
攻撃者はマシンスピードで行動し、企業が対応するまえに重大な損害を与える可能性があります。
従来型の防御だけでは不十分であり、組織はAIネイティブな状況認識（AI-native sensemaking）を取り入れる必要があります。
具体的には、
- テレメトリデータの統合
- 異なる領域を横断したリアルタイム分析
- 文脈に基づいた、インテリジェントな対応

といった仕組みを導入することで、脅威を理解し、被害が発生する前に対処できるようになります。

人的脆弱性の低減

AI脅威を特定するためには、従来の静的なセキュリティ教育では不十分です。
攻撃者はAIを使って、
- 音声ディープフェイク
- 動画によるなりすまし
- 高度なソーシャルエンジニアリング

といった手法で従業員をだまし、機密情報や資格情報を盗みだそうとします。
従業員は従来のフィッシングメールに気付けるだけでなく、AIを用いた巧妙な攻撃を識別し、対応できるように訓練されていることが必要になります。



内部脅威への対処

社内のAIシステムや運用によって生じる弱点を特定することが重要です。これらは、従来のセキュリティ対策では見落とされがちです。

AI利用ポリシーを明確化する

従業員は、パブリックなAIシステムに機密情報を入力すると、そのデータが組織外の第三者に共有されてしまう可能性があることを認識していない場合があります。そのため、従業員をリスクのある行動から守るために、明確な利用方針と管理ルールを定める必要があります。

アクセス権限を監査する

AIエージェントによるデータアクセスが厳密に管理されていない場合、内部のデータ保護を損なったり、攻撃者に乗っ取られる可能性があります。
機密情報を狙う攻撃者がAIの挙動を悪用しようとするケースもあるため、企業はAIシステムと従業員が必要な範囲のデータだけにアクセスしているかを継続的に監視する取り組みが必要になります。

AI開発ライフサイクルを保護する

社内でAIシステムを構築し、運用する際には新たなリスクが発生します。例えば、お客様向けAIソリューションの学習データがサイバー犯罪者に改ざんされた場合、企業は重大な風評被害や規制違反のリスクに直面します。そのため、組織はAIシステムに対する不正な操作や改ざんを防ぐため、内部統制とチェックプロセスを確立する必要があります。

進化

AIにはAIで対抗する

AIがもたらすサイバーセキュリティリスクに対処するには、ITリーダーがAIの可能性を最大限に引き出すことが不可欠です。

リアクションスピードを強化する

攻撃速度が人間の対応能力を上回るセキュリティ環境において、人間の意思決定を支援・スケールアップするためにAIを活用することが重要です。

AIを統合したサイバーセキュリティシステムは、複数画面を行き来せずに、自然言語インターフェースで必要な情報へアクセスでき、セキュリティチームが迅速に行動できるように支援します。

「セキュリティの観点から言えば、状況を全体的に把握できるほど異常をいち早く発見できます。」

Mikkel Seiero

レノボグローバルセキュリティサービス提供責任者

統合された可視化を実現する

従来の企業向けサイバーセキュリティ体制では、データ保護や脆弱性分析などの機能は、専門ツールを使う別々のチームによって提供されます。しかし、生成AIを活用した攻撃者は、これらの機能間の盲点を突き、攻撃の検知を困難にします。

これらの攻撃に対処するには、サイバーセキュリティチームがドメイン横断の包括的なサイバーセキュリティ体制を構築し、複数のツールから情報を集約する必要があります。AIを活用することで、インテリジェンス抽出、動的セキュリティスコア、自動化対策が可能になります。

「可視化はAIセキュリティの第一歩です。AIモジュールやアプリケーションの機能、利用状況を完全に把握し、継続的に監視することで、機密データ保護し、セキュリティコンプライアンスを遵守し、新たなAI脅威への防御を実現します。」

Kamrul Hasan

レノボサイバーセキュリティアーキテクト

進化

AIとサイバーセキュリティを統合する際の障壁

将来の脅威に備えるため、ITチームはデジタルワークプレイス全体でAIを活用する必要があります。しかし、その実現は容易ではありません。

調査によると、多くの企業がすでにAIの導入を進めています。例えば、約半数の企業がエンドポイントセキュリティとIDアクセス管理（IAM）においてAIと自動化を「広範に」利用しています。

しかし、自社のセキュリティ能力がAIリスクに完全に対処できると自信を持つ企業は半数に満たず、改善の余地が大きいと言えます。

さらに、AIを活用してサイバーセキュリティ対策を強化することは、単に適切なツールを導入するだけではありません。多くの企業には克服すべき重大な障壁があります。

障壁1: 複雑化したIT環境

82％のITリーダーが「IT環境の複雑さ」がAI活用型セキュリティ導入の最大の障壁と回答しています。

当社の調査によると、最も多い障壁がIT環境の複雑性であることがわかりました。

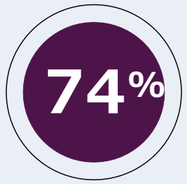
多くの企業は、数十年にわたって進化してきたIT資産を保有しており、その中には新しいAIプラットフォームに対応していない旧式ツールも含まれています。

障壁2: サイバーセキュリティ人材の不足

80%のITリーダーがセキュリティ機能における「熟練した人材不足」を主要な障壁と回答しています。

2番目に多い障壁は、組織内に熟練した人材が不足していることです。AIとサイバーセキュリティの両方のスキルは需要が高いにもかかわらず、供給が不足しており、両分野に精通した人材を確保するのは非常に困難です。さらに、セキュリティアナリストは高度な脅威に直面し、認知負荷の高いストレス環境で業務を行っているため、この不足は深刻化しています。

障壁3：コストと予算の制約



74%のITリーダーが「ソリューションのコスト／予算不足」を障壁と回答しています。

高度なツール、熟練した人材、そしてAI対応に向けた継続的な投資には、いずれも多大なリソースが必要です。多くの組織にとって、既存のツールが時代遅れであってもまだ機能している場合、予算が限られる中で新技術への投資を優先するのは難しい状況です。

進化

防御体制を進化させるために

AI由来の脅威に対抗するために、組織が実践できる具体的なステップを紹介します。

全体像を把握する

複雑化した IT 資産と人員不足のセキュリティチームを抱える環境では、ツールが分断されていることで、非効率や隠れたコスト、脅威の可視性不足が生じます。
ユーザー、エンドポイント、アプリケーション、クラウド全体のテレメトリーを統合することで、ツールの乱立を抑え、トレーニングコストも削減できます。
同時に、AI を活用した脅威の検出・対応をより迅速かつ効果的に行うための統合されたビジョンが得られます。

汎用性の高いツールを導入する

大企業では、ビジネスクリティカルなシステムが旧式のレガシープラットフォーム上に残っており、容易に移行できないケースが多くあります。
AIを活用したセキュリティを最大限活用するには、こうした環境にも対応できる幅広いOSとアプリケーションをサポートするセキュリティソリューションを導入することが重要です。
サポート終了が迫るシステムに対しても有効な対策が求められます。

経験豊富なパートナーと連携し、セキュリティチームを強化する

AI 脅威は急速に進化しており、社内チームを育成するには時間とコストがかかります。
そのため、経験豊富なパートナーとの協業によって、必要なスキルを迅速かつ適切な規模で獲得し、能力を拡張することが可能になります。
これは、今日の脅威に対抗するために不可欠な手段です。

強化された「Work Reborn」へようこそ

進化する AI 時代において、デジタルワークプレースを保護するためには、
企業がサイバー脅威を**監視し、把握し、対応し、そしてデジタル資産を運用する方法を根本から再構築**する必要があります。

生成AIの脅威に対抗するために
企業が取るべき行動：

- **検知能力の強化**

  AI を活用した脅威は防御をすり抜けやすいため、
  企業は重要資産を守る取り組みをこれまで以上に強化しなければなりません。
  特に狙われやすいのは以下の領域です：
  ・AI システムそのもの（エージェント、モデル、学習データ、プロンプトなど）
  ・AI を動かす基盤や管理情報
  こうした AI コンポーネントは、攻撃者にとって非常に価値の高いターゲットとなっています。

- **AIの能力を活用**

  企業は、より柔軟でリアルタイムに対応できるセキュリティ態勢を確立する必要があります。
  そのためには、攻撃者が利用しているのと同じ AI の能力を用いて、セキュリティチームが高度な洞察・文脈理解・迅速な推奨アクションを手に入れることが不可欠です。

この２つのアプローチにより、もたらされる優れたビジネス成果：

生産性の向上

AIをセキュリティ運用に組み込むことで、セキュリティ担当者の生産性を高めることができます。
MicrosoftのSecurity Copilot（サイバーセキュリティチーム向けAIアシスタント）の評価によるとSecOpsチームの生産性を23%～47%向上させる可能性があります。[1]
さらにMicrosoftの分析では、デバイスポリシーの競合解決が54%高速化[2]、インシデント対応が30%迅速化されると報告されています。[3]

コスト削減

防御体制の変革は、収益面でも様々なメリットをもたらします。
例えば、AIを活用してセキュリティ運用全体を包括的に把握することで、ツール利用に必要なトレーニングコストを削減できます。
また、使用するツール数を最適化することでメンテナンスコストを最小限に抑え、標準的な機能は、コスト効率に優れたパートナー企業へ委託する機会も生まれます。

シームレスな変革

最も重要なのは、急速に進化するAI時代に向けたサイバーセキュリティの再構築が、デジタルワークプレイス変革を完全に受け入れる自信をもたらす点です。
過去の調査では、ビジネスリーダーのセキュリティ懸念がAI導入の最大の障壁の一つであることが判明しています。
そして、こうした懸念は決して根拠のないものではありません。したがって、AI主導のデジタルワークプレイス変革には、サイバーセキュリティの強化が必ず伴わなければなりません。

[1]出典：New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot, Forrester Research 2024年11月
[2]出典： Security Copilot: Evidence of Productivity Gains in Live Operations, Microsoft Corporation, 2025年3月
[3]出典： Generative AI and Security Operations Center Productivity: Evidence from Live Operations, Microsoft Corporation, 2024年11月

安全に、そして確実に
職場環境の変革を始めませんか？

AI脅威を正しく評価し、デジタルワークプレイスを近代化する際の確かなセキュリティを確保しましょう。

まずはここから開始してください。

お客様が描く未来のビジョンを、レノボが共に実現するお手伝いをします。

調査方法

本調査では、レノボが2025年4月と5月に600名のITリーダーを対象に調査を実施しました。調査対象は米国（17%）、カナダ、英国、フランス、ドイツ、インド、日本、シンガポール、ブラジル、メキシコ（各8%）、オーストラリア（4%）、ニュージーランド（4%）からの回答者が含まれています。回答者には、従業員1,000名以上の企業に所属するITリーダーや、様々な業界のITリーダーが含まれています。

Smarter technology for all

Lenovo