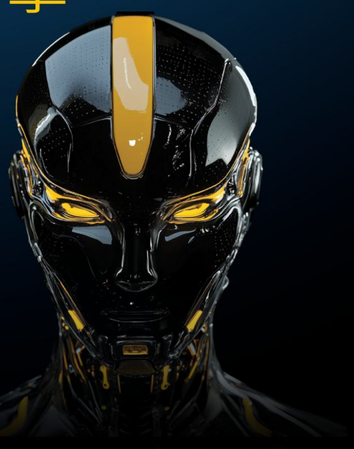
KEEPER

IT担当者達が直面する AIを駆使したサイバー攻撃



AIの登場によりサイバーセキュリティは大きく変わり、従来の対策では防ぎきれない複雑で高度なサイバー脅威が現れています。AI技術が進化することで、フィッシング詐欺やスミッシング詐欺といった従来のサイバー攻撃を見つけるのがさらに難しくなっているため、強力かつ柔軟に対応できるセキュリティ対策が必要になっています。

AI検出の課題

84%

IT担当者の84%が、AIによりフィッシング攻撃やスミッシング攻撃の検出が困難になったと感じている

ポリシー導入の急増

81%

81%の組織で従業員向けにAI使用に関するポリシーを導入

AIセキュリティの知識

77%

IT担当者の77%が、AIセキュリティのベストプラクティスについて「熟知している」または「よく知っている」と回答

Keeper Securityの調査によると、AIに関するポリシーの増加やAIを利用したサイバー攻撃への対応能力への自信が高まっているにもかかわらず、**全体的な準備状況に大きな不足があることが浮き彫りとなっています**。AIを駆使した攻撃、サプライチェーン攻撃、ディープフェイク技術が主な懸念事項として挙げられているにもかかわらず、多くの組織はこれらの高度なサイバー攻撃への対応能力の不足を解決するのに苦労しています。

主な脅威と対応能力の欠如

新たな脅威

51%

IT担当者の51%が、最も深刻な脅威はAIを利用したサイバー攻撃であると認識

36%

IT担当者の36%がサプライチェーン攻撃を懸念

36%

IT担当者の36%がディープフェイク技術を重大なリスクとして強調

対応能力の欠如

35%

IT担当者の35%が、AIを利用したサイバー攻撃への準備がほとんどできていないと感じている

30%

IT担当者の30%がディープフェイク技術について懸念を表明

この課題に対処するために組織が取り組んでいること

データの暗号化	従業員のトレーニングと意識向上	高度な脅威検出システム	安全なAIモデルの開発	定期的なセキュリティ監査
51%	45%	41%	40%	36%

> “AIを利用したサイバー攻撃は厄介な問題ですが、サイバーセキュリティの基本をしっかり強化し、先進的なセキュリティ対策を導入することで、日々進化する脅威に対しても未然に防ぐことができます。”

ダレン・グッチョーネ氏
Keeper Security社CEO兼共同創設者

AIを使った攻撃が増えている今、未然に防ぐための対策が重要です。データの暗号化や従業員のトレーニング、先進的な脅威検出といった基本的な対策は、常に最新の状態に保ち、強化しておかなければなりません。また、ゼロトラストや特権アクセス管理（PAM）といった高度なフレームワークとツールを導入することで、セキュリティ強度をさらに高められます。組織は常に警戒しながら、セキュリティポリシーを定期的に見直し、最新の対策を取り入れたり、AIを使った新たなサイバー脅威やサイバー攻撃に先手を打つ必要があります。