KEEPER®

学校におけるAIレポート
導入とリスクのバランス

2025年10月

概要

人工知能 (AI) は教育現場を大きく変えています。教師は授業計画や保護者・同僚とのやり取り、学習成果の分析にAIを活用し、生徒は調べ物やアイデア出し、創作活動に利用しています。AIは教室の時間を効率化し、新しい学びの機会を広げています。

しかし、導入のスピードに備えが追いついていません。すでに41%の学校がフィッシングや有害コンテンツの生成などAI関連のサイバー被害を経験しています。リスクに対する認識は高まっているものの、ポリシーは統一されておらず、脅威を見抜く力にもばらつきがあります。

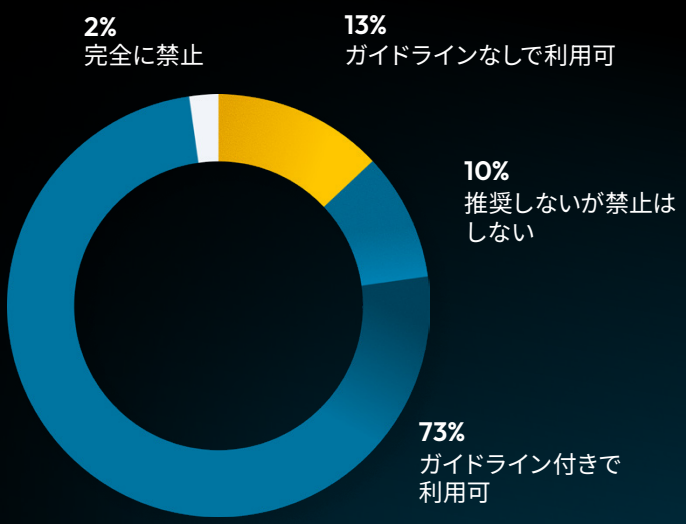
本レポートは、米国と英国の初等・中等・高等教育の教育リーダー1400人以上を対象にした調査を基に、学校でAIがどのように使われているか、どこに対策が整備され、どこに課題が残っているか、さらに教育を混乱させずに強化するために必要な取り組みを探っています。

教室と職員室で定着するAI

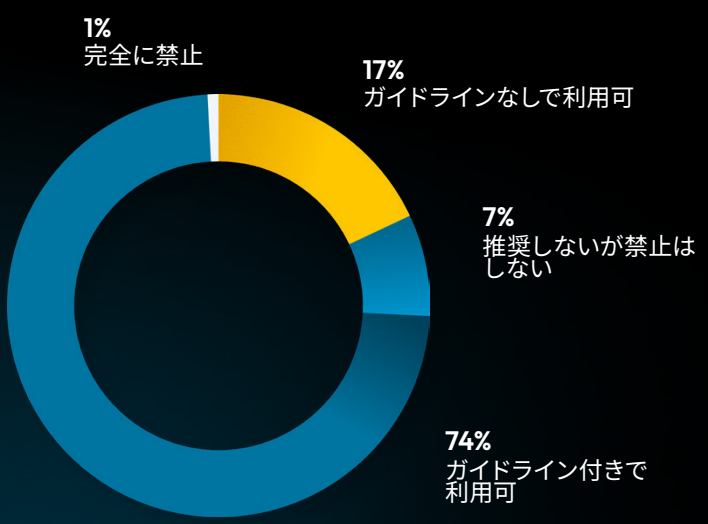
AIは教室でも職員室でも身近なものになっています。生徒は多くの学校 (86%) で利用を認められ、全面的に禁止しているのはごく少数 (2%) です。教職員の利用はさらに進んでおり、91%の学校で許可されていて、多くの場合はルールを定めて運用されています。

生徒は主に学習を補助したり、新しい発想を広げたりする目的でAIを利用しています。よく使われているのは調べ物 (62%)、アイデア出し (60%)、言語サポート (49%) で、続いて創作活動 (45%) や復習支援 (40%) が挙げられます。一方で、プログラミング (30%) や課題の仕上げ (27%) といった扱いに注意が必要な分野については、利用が制限される傾向があります

生徒によるAIツールの利用に関する方針



教職員によるAIツールの利用に関する方針

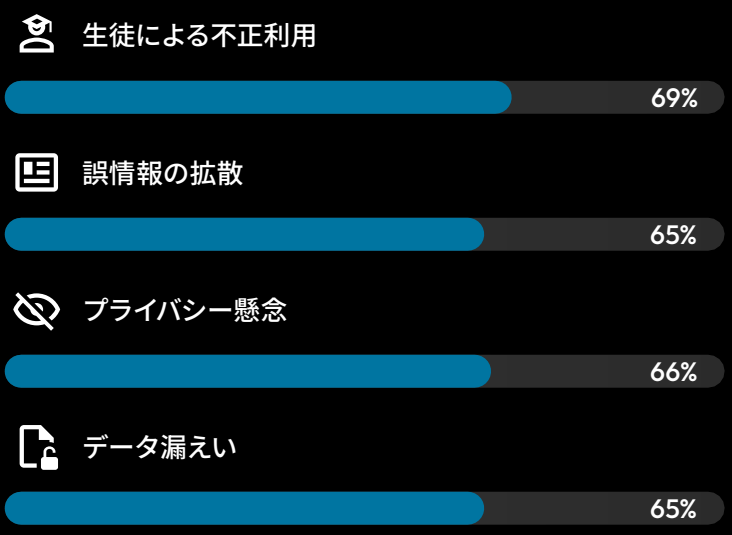


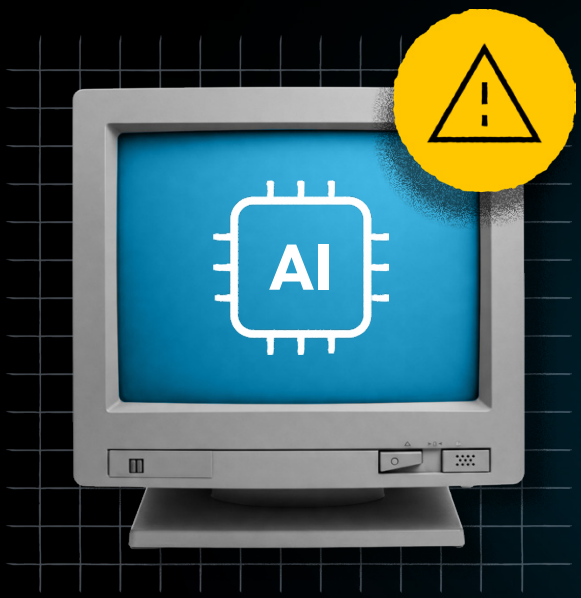
教職員は、業務を効率化するためにAIを積極的に取り入れています。特に多いのはスケジュール管理 (67%) や授業準備 (60%) で、加えて約半数の教育機関が、採点や生徒との関わり方の工夫、データ分析などへの利用を許可しています。

調査結果からは、教職員と生徒でAIの位置づけが異なることが分かります。教職員には業務を効率化する目的で活用を広げているのに対し、生徒については学習の公正さを守るため、利用を探究的な活動に絞っているのです。

脅威への自信はまちまち

認識されているAI関連リスク

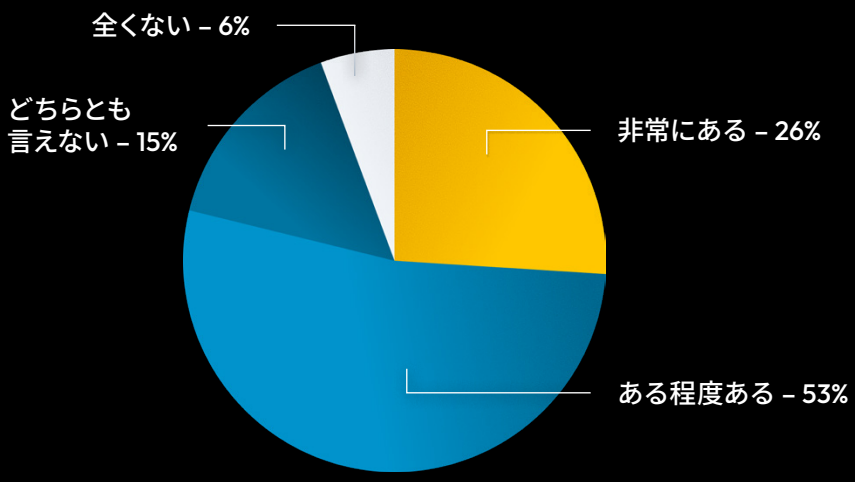




AIのサイバーリスクについて、多くの教育関係者が高い認識を持っており (83%)、心強い結果といえます

しかし、その理解度には差が見られます。データ漏えいやプライバシー問題、誤情報拡散など基本的なリスクは広く知られていますが、技術的に高度なものや新たに登場している脅威については認識が追いついていません。Keeper Securityのレポート『2025年のサイバー攻撃対策の未来』によれば、ITリーダーの95%が「サイバー攻撃は一段と巧妙になっており、新しい脅威への対応が不十分」と感じています。

ディープフェイクやAIを利用した フィッシングなどの脅威を見抜く自信

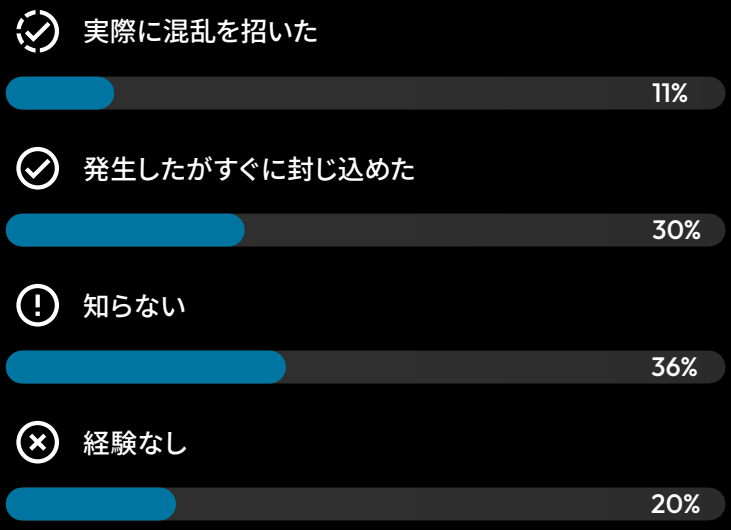


多くの教育関係者はAI詐欺を見抜けると考えていますが、自信を持って言えるのは4人に1人だけです。すでに41%の学校で被害が確認されていることを考えると、この認識と備えのギャップは大きなリスクとなり得ます。

対応には多層的なアプローチが必要で、職員の研修や意識向上に加え、データの暗号化、高度な脅威検知、アクセス制御 (パスワードマネージャーやPAMを含む) を組み合わせることで、AIを悪用した攻撃を防ぎ、被害を最小限に抑えることができます。

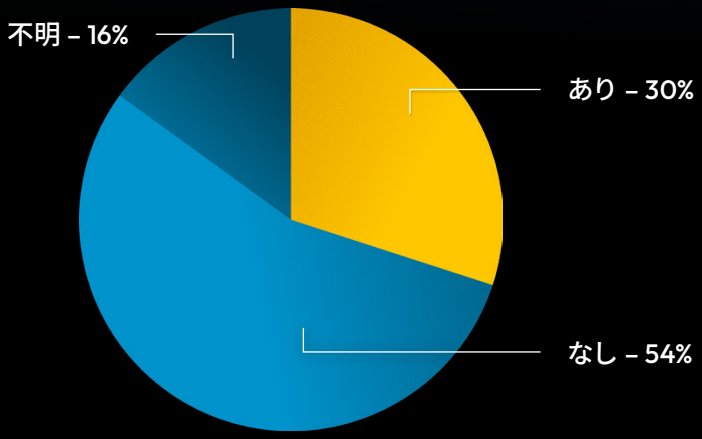
学校で実際に起きている AI被害

AI生成によるフィッシング・偽情報被害 (ディープフェイクや合成音声)

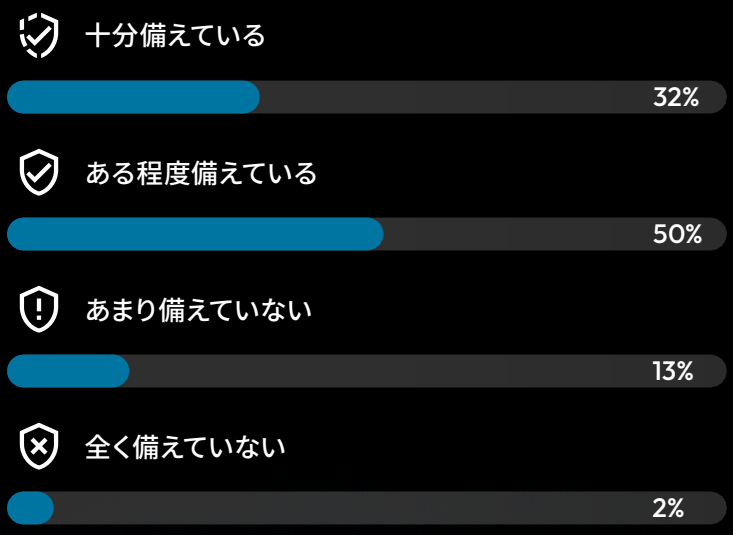


学校ではすでにAIに関わる問題が内外で起きています。41%がフィッシングや誤情報拡散といった被害を経験し、約30%は生徒が有害なAIコンテンツを作った事例を報告しています。報告されたケースの多くは「すぐに対応できた」(30%) ものの、39%は「発生したか分からない」と答えており、監視や認識の面で大きなギャップがあることが明らかになっています。

生徒による有害AIコンテンツ (クラスメートのディープフェイクなど) の生成



今後1〜2年の備え



多くの教育機関 (82%) はAI関連のサイバー脅威に「ある程度備えがある」と感じていますが、「十分備えている」と言えるのは32%にとどまります。こうした数字からは、リスクを理解していても全体の備えにはまだ不足があり、今の対策が本当に効果的かどうか不安が残っている様子がうかがえます。

教育現場を覆うサイバーセキュリティ不安

AI関連脅威への不安

37%
実際に混乱を招いた

53%
ある程度懸念している

10%
懸念していない

最も懸念されていること

65%
生徒のプライバシー侵害

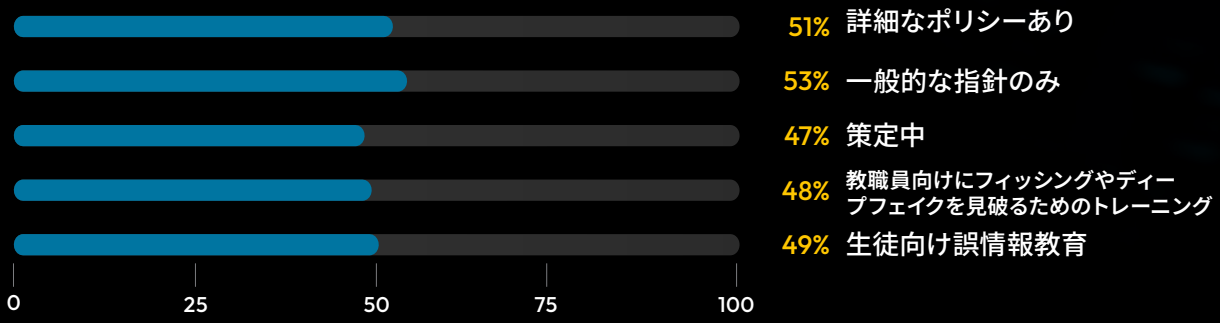
53%
学習の支障

52%
教職員や生徒のディープフェイク

すでに40%以上の学校が影響を受けていることから、教職員の多くがAI関連のサイバー脅威に強い不安を抱いており、90%が少なくとも「ある程度懸念している」と答えています。その中でも37%は「非常に懸念している」と回答し、生徒の安全や学習への影響、具体的にはプライバシーの侵害やディープフェイクによるなりすまし、授業の妨げなどが大きな不安材料になっています。さらに、AIの出力に偏りがあること (43%) や、学校の評判への悪影響 (37%)、財務的な損害 (36%) も懸念されており、学校運営や信頼を揺るがすリスクとして意識されています。

不十分なポリシーと対策

学校や大学でのAIリスクへの対応状況*



- 51% 詳細なポリシーあり
- 53% 一般的な指針のみ
- 47% 策定中
- 48% 教職員向けにフィッシングやディープフェイクを見破るためのトレーニング
- 49% 生徒向け誤情報教育

学校や大学ではAI利用を管理するための枠組みづくりが進んでいますが、その実施状況にはまだばらつきがあります。詳細なポリシーを定めているのは半数程度 (51%) で、非公式なガイドラインにとどまっているところも多く (53%)、AI検知ツールや生徒向け教育プログラムを導入しているのは6割に満たない状況です。すでに40%以上が影響を受けているのに、専用予算を確保しているのは34%、インシデント対応計画を持っているのは37%にとどまっており、備えに大きな不足があることが明らかになっています。

*その他
技術ツール導入: 20%
外部セキュリティ機関との連携: 19%
何もしていない: 3%

今後の課題
導入と備えのギャップを埋める

今求められているのは、「AIを導入するかどうか」ではなく、「どう管理し、安全に使いこなし、既存や新たに出てくる脅威を抑えていくか」です。今回の調査では、AI導入のスピードに対して、ポリシーやガバナンス、予算の整備が追いついていない現状が明らかになりました。ガバナンスや研修、セキュリティ対策の遅れは、すでにAIを悪用した脅威が報告されている状況を考えると、将来さらに深刻な影響をもたらす恐れがあります。

教育機関が今取るべき3つの優先事項は以下の通りです。

- **ポリシーの整備:** 利用を推進しつつ責任ある使い方を確立する
- **レジリエンス強化:** トレーニング、意識啓発、検知ツール導入で備える
- **信頼の確保:** プライバシーや倫理に配慮し、学校や地域社会の信頼を守る.

具体的な行動例としては、以下が挙げられます。

- 全システムで多要素認証 (MFA) を徹底し、アカウント侵害を防ぐ。
- 特権アクセス管理 (PAM) を導入し、重要データやシステムへのアクセスを制御する。
- 強力なパスワード管理を徹底させ、攻撃者が最も狙いやすい入口を塞ぐ。
- フィッシングやディープフェイクを素早く特定・対応するためのリアルタイムの検知と監視を導入。
- AIポリシーを定期的に見直し、技術やリスクの進化に合わせて更新する。

今後2年間は、AIが教育において信頼できる味方となるのか、それとも脆弱性を抱え続ける存在になるのかを決定づける重要な時期となります。早急に対策を進めることで、導入のスピードに対応しつつ、新たな脅威にも先手を打つことが可能です。

調査方法

Keeper Securityは、独立系調査会社TrendCandyに委託し、米国と英国の教育機関管理者1460人を対象に、学校におけるAI導入・利用状況・サイバーセキュリティ体制に関する調査を実施しました。

調査はオンラインで行われ、参加者には謝礼が支払われました。米国と英国の教育機関のリーダー層を対象に、ランダム抽出やダブルブラインド方式、データ品質管理など、厳しい基準に基づいて実施されています。

本調査の信頼水準95%における誤差範囲は±3%です。

Keeper Securityについて

Keeper Securityは、世界中の多くの人々や組織のサイバーセキュリティを革新的な方法で保護するソリューションを提供しています。エンドツーエンド暗号化を採用したKeeperのサイバーセキュリティプラットフォームは、「フォーチュン100」に名を連ねる企業からも信頼を得ており、あらゆる場所やデバイスを使用するユーザーの保護に対応します。特許取得済みのゼロトラストおよびゼロ知識の特権アクセス管理 (PAM) ソリューションにより、企業や組織向けのパスワード管理、シークレット管理、接続管理を、ゼロトラストネットワークアクセスおよびリモートブラウザ分離と統合。KeeperはID管理とアクセス管理を単一のクラウドベースソリューションに統合することで、完全な可視性、セキュリティ、制御が実現し、コンプライアンスや監査要件の遵守にも利用できます。最新のサイバー攻撃の脅威から組織を保護する仕組みについては、KeeperSecurity.comをご覧ください。