



マイクロソフト教育機関向けセキュリティ ツールキット

すべての教室とキャンパス向けに簡素化
されたセキュアな IT



ウェルカム レター

マイクロソフトでは、学校や教育機関が非常に標的となりやすく、複雑なデジタル環境で運用していることを理解しています。サイバー攻撃の頻度と巧妙さが増す中、サイバーセキュリティは、機密性の高い学生データ、研究、知的財産権の保護だけでなく、教育、学習、教育機関の運営の継続性を確保するためにも、不可欠な存在となっています。

マイクロソフトのコミットメントは、教育機関が妥協することなく安心して学業の成功を追求できる、セキュアでレジリエントかつ信頼性の高いデジタルエコシステムの構築を支援することです。

キャンパスのセキュリティに対するマイクロソフトのビジョンは、シンプルさ、拡張性、インテリジェンスに基づいています。

- インシデントの削減と学習および研究環境の保護を実現するために設計された、統合されたテクノロジー スタックによるシンプルな管理を提供します。
- データ保護、コンプライアンス、管理をマシンのスピードと規模で支援する、AI を活用したセキュリティ ソリューションを提供します。
- 自動化と統合ツールによって学校や教育機関がセキュリティ運用 (SecOps) を拡張できるよう支援するとともに、学生セキュリティ オペレーション センター (SOC) やスキル習得プログラムを通じて次世代のサイバー防御要員の育成に投資しています。

これらの柱が一体となって、回復力のある適応型のセキュリティ基盤を形成し、あらゆる規模の教育機関を保護して、安全で革新的な学習環境を実現します。

教育リーダーは、学習環境を保護し、デジタルレジリエンスを強化して、AI を活用した教育の未来に備えるために、タイムリーで戦略的な行動の必要性を認識しています。今こそ、絶好の機会です。教育機関は、キャンパスを保護し、サイバーセキュリティの未来を形作っています。学生をセキュリティ運用に参加させ、AI 主導のツールによる実践的な経験を提供することで、教育は事後対応型からプロアクティブなリーダーシップとデジタルレジリエンスへと進化しています。

世界中の学校や教育機関がすでにこの道を進み始めています。

- [シンガポール経営大学](#)は、マイクロソフトのゼロ トラスト フレームワークと Security Copilot を導入し、応答時間の短縮、セキュリティ チームの負担軽減、そしてより迅速かつ自信を持った IT の意思決定を実現しました。
- [オレゴン州立大学](#)は、Microsoft Sentinel と Defender によって保護された、学生が運営する SOC を開設し、学生に実践的なサイバーセキュリティ エクスペリエンスを提供するとともに、大学の脅威検出および対応能力を強化しました。
- [ニューヨーク市公立学校](#)は、Microsoft Intune を使用して 75 万台の生徒向け LTE 対応デバイスを管理し、米国最大級の学区全体でセキュアでスケーラブルかつ効率的なデバイス管理を実現しています。

Microsoft 365 上に構築されたマイクロソフトの統合セキュリティ プラットフォームは、Security Copilot、Sentinel、Defender XDR、Intune、Entra ID、Purview を単一の AI 搭載システムに統合します。このアプローチにより、教育機関はデバイスやデータの保護、コンプライアンス管理、脅威への迅速な対応を、統一されたダッシュボードから行うことができます。

注目すべき動向の 1 つは、学生主導の SOC の台頭です。これは、学習者をサイバー防御要員へと育成しながら、有意義なキャリア パスを築く強力な手段です。

セキュリティはもはや単なる防御策ではなく、イノベーションの触媒となっています。マイクロソフトの信頼性の高いソリューションを活用することで、教育機関は自信を持って AI を導入し、セキュアなリモート学習、グローバルな研究の支援、そして最も重要なもの、つまり学生のデータと教育の健全性の保護を実現できます。

マイクロソフトでは、セキュリティは単なる保護にとどまらず、可能性を広げるものだと考えています。共に力を合わせることで、学びが育まれ、研究が進展し、すべての学生が自信を持ってテクノロジーを探求できる、包摂的でセキュアな環境を創り上げることができます。



Matt Jubelirer
Microsoft Education、
ゼネラル マネージャー

目次

概要	お客様への効果の事例	実装
5 マイクロソフト セキュア フューチャー イニシアティブ	16 学習環境の保護: 初等中等教育キャンパスにおける効果の事例	43 初等中等教育における実装シナリオ
9 このセキュリティツールキットの利用ガイド	20 高等教育におけるセキュリティ イノベーションの実例	47 高等教育向けの実装シナリオ
11 マイクロソフトのセキュリティ ツールにより安全な学習を可能にする	24 セキュリティに関するその他のお客様事例	
ツール	計画	調査
13 Microsoft Security ツール	29 より安全な学習環境を実現するための戦略的計画	52 教育分野におけるマイクロソフトのセキュリティ: 展開からキャンパスへの効果まで
	31 キャンパスの現在のセキュリティ態勢を評価する	54 データと分析
	34 セキュリティ ガバナンスとポリシー	56 学術および業界動向
	36 テクノロジー セキュリティ戦略	58 用語集
	38 組織の準備状況	59 次のステップのチェックリスト
	40 財務的および戦略的正当性	

概要

このセクションの内容

- [マイクロソフト セキュア フューチャー イニシアティブ](#)
- [このセキュリティ ツールキットの利用ガイド](#)
- [マイクロソフトのセキュリティ ツールでより安全な学習を可能にする](#)



マイクロソフト セキュア フューチャー イニシアティブ

マイクロソフトは、学生、教育者、スタッフの機密データを守るために設計された専用のサイバーセキュリティ プラットフォームによって、進化するサイバー脅威に先んじて対応できるよう教育機関を支援しています。マイクロソフトの信頼性の高いクラウドファースト ソリューションは、学校がツールを統合し、セキュリティ オペレーションを合理化し、調達を簡素化しながら、IT の複雑さを軽減することをサポートします。

AI を活用した統合型脅威検出・対応により、学校や教育機関は可視性を向上させ、対応の迅速化と手作業の負荷軽減を実現でき、IT チームは学習支援に専念できるようになります。グローバルなセキュリティ基準に基づいて構築され、ゼロトラストの原則にを基盤とした Microsoft 365 プラットフォームは、侵害を想定して明示的に検証することで、各キャンパス環境のニーズに適応する堅牢な防御を実現します。

アプローチのすべての層は、セキュア フューチャー イニシアティブ (SFI) によって導かれている

- **セキュア バイ デザイン:** どの製品やサービスを設計する際も、セキュリティが最優先となります。SFI の UX ツールキットは、既定のセキュリティ機能を改善し、摩擦を減らすのに役立ちます。このツールキットは Windows、Azure、Defender の各製品チームによって導入されています。
- **セキュア バイ デフォルト:** セキュリティ保護が既定で有効になり、強制されます。追加の作業は必要なく、これは任意ではありません。Microsoft 365 Copilot 制御システム (CCS)、Windows スマートアプリ コントロール、Azure と Microsoft Entra ID の強制 MFA は、セキュリティの設定がいかに有効化され、維持されているかを示しています。
- **セキュアな運用:** セキュリティの制御と監視は、現在および将来の脅威に対応できるよう、改善されていきます。自動検出、不正防止、統合されたポリシー施行により、SFI はセキュアな運用を実効性で強化します。

セキュアな学習環境の実現

マイクロソフトは、安心かつセキュアで包括的な学習環境を構築し、学生データの保護、サイバー脅威の最小化、IT 管理の効率化を実現できるよう、教育機関を支援することに取り組んでいます。

- **デバイスの強化と ID の保護:** Windows 11 に搭載された機能で環境を強化し、Entra ID による ID 保護を適用するほか、Intune や Defender XDR などのソリューションでシステムを最新化します。
- **エンドポイントとアプリの保護:** Intune と Defender for Cloud Apps を活用して、学生用デバイスの保護、コンプライアンス遵守の支援、クラウドおよびエンドポイント全体でのアプリへのアクセスの保護を実現します。
- **オペレーティング システムの保護:** Windows 11 に搭載されたスマート アプリ コントロール、仮想化ベースのセキュリティ、カーネルモード保護などのセキュリティ機能を活用して、学習環境のセキュアな基盤を確立します。
- **ハードウェアベースの保護:** TPM 2.0 や Microsoft Pluton セキュリティ プロセッサなどのハードウェア機能により、デバイスの整合性を強化します。これらのハードウェア機能は、機密データを保護し、セキュア ブートと暗号化をサポートします。

「マイクロソフトは信頼の上に成り立っています。信頼は積み重ねていくものであり、維持していく必要があります。マイクロソフトは、何よりもサイバー セーフティを優先させることをお客様とコミュニティにお約束します。」

— **Charlie Bell**、
マイクロソフト セキュリティ担当 EVP

『[Windows セキュリティ ブック](#)』をご覧ください、マイクロソフトが教育機関のセキュアかつ信頼性の高い学習環境の構築をどのように支援しているかをご確認ください。セキュリティを強化し、学生の安全を大規模に支援するためのベストプラクティス、ツール、戦略をご紹介します。

初等中等教育および高等教育に共通する課題

ID のセキュリティ

初等中等教育	高等教育	マイクロソフトのソリューション
デバイスの柔軟性: 1 人 1 台のデバイスや共有デバイス向けのセキュアな MFA	高いユーザー回転率: 継続的な入学と卒業	Entra ID - 証明書ベースの認証 - 条件付きアクセス ポリシー - 外部 ID - FIDO 2 キー - マルチテナント組織 - 一時アクセス パス - ユーザー/グループ ラifecycle ポリシー - 検証された資格情報 - Windows Hello
混合環境: 生徒の個人デバイスと教室の共有コンピューター	外部パートナー: 来訪者、ベンダー、研究者	School Data Sync (SDS)
年齢に関する考慮事項: すべての学年に対応した年齢に応じた認証	複数の学部: 個別の学校と大学	
	卒業生によるアクセス: 卒業生との継続的なつながり	
	複雑な資格情報: すべてのログインとアクセス許可の管理	

データ セキュリティとコンプライアンス

初等中等教育	高等教育	マイクロソフトのソリューション
学生データの保護: 法的義務として学生データを保護する	機密データの保護: 研究、健康、入学、財務に関する機密データを保護する	Purview - DLP - 情報バリア - 情報の保護 - 内部関係者による脅威からの保護
多国間コンプライアンス: 複数の国でのコンプライアンス遵守を支援する	多国間コンプライアンス: 複数の国でのコンプライアンス遵守を支援する	Security Copilot
	内部関係者による脅威の防止: 内部関係者による脅威を防ぐ	

コンプライアンス要件

初等中等教育	高等教育	マイクロソフトのソリューション
規制遵守: FERPA、HIPAA、GDPR、EU AI 法、データ保持要件の遵守を支援する	規制遵守: FERPA、HIPAA、Title IX、GBLA、GDPR、EU AI 法の要件遵守を支援する	Entra ID 監査と報告
		Security Copilot
		Purview - コミュニケーション コンプライアンス - DLP - 電子情報開示 - 情報バリア - 情報の保護 - レコード管理

セキュリティ管理

初等中等教育	高等教育	マイクロソフトのソリューション
リソースの制約: 限られた技術リソースと人員の管理	分散した IT: 分散した IT 環境の管理	Defender XDR
攻撃への対応: 大量のサイバー攻撃に対応する	予算の制約: 予算とセキュリティ専門知識の制約に対処する	Security Copilot
保険の要件: サイバー保険の要件を満たす	学生プログラム: 学生向け SOC プログラムを導入する	Sentinel

デバイスのセキュリティ

初等中等教育	高等教育	マイクロソフトのソリューション
デバイスへのアクセス: 1 人 1 台デバイスおよび共有デバイスへのセキュアなアクセスを提供する 学区のコンプライアンス: 大規模学区でデバイスのコンプライアンスを支援する 脅威からの保護: マルウェアや不正アクセスから保護する	個人デバイスへのアクセス: 個人デバイスへのセキュアなアクセスを提供する 侵害の防止: データ侵害とマルウェアを防止する コンプライアンス要件: デバイスのコンプライアンス要件遵守を支援する	Defender for Endpoint - EDR ポリシー - ネットワークの保護 - Web コンテンツ フィルタリング Entra ID - デバイス コンプライアンスによる条件付きアクセス - インターネット アクセスとプライベート アクセス - Web コンテンツ フィルタリング Intune - アプリ保護ポリシー - デバイス コンプライアンス ポリシー Purview - DLP によるデータ共有

アプリのセキュリティ

初等中等教育	高等教育	マイクロソフトのソリューション
M365 の展開: 学生向けのセキュアな M365 アプリを展開する ポリシー管理: プラットフォームとアプリのセキュリティ ポリシーを管理する 脅威からの保護: アプリ内のマルウェアやフィッシングから保護する	マルチクラウド環境: マルチクラウド環境やマルチプラットフォーム環境をセキュアに運用する ハイブリッド セキュリティ: オンプレミスとクラウド アプリのセキュリティを管理する ID フェデレーション: フェデレーションおよびマルチテナントの ID をサポートする	Defender - Defender for Cloud Apps - Defender for Identity - Defender for Office 365 Purview - SharePoint ポリシー Entra ID - フェデレーション ID - マルチテナント組織 - グループとチームのポリシー Sentinel

AI のセキュリティ

初等中等教育	高等教育	マイクロソフトのソリューション
安全な AI アクセス: 学生が安全に AI を利用できるようにする 誤用の防止: AI の誤用や情報アクセスに関する懸念に対処する 通信の保護: AI ツール使用時の通信や機密データを保護する	高度な脅威防御: 複雑で拡張性の高い AI 主導の攻撃から防御する 内部関係者による脅威の防止: 内部関係者よる AI を悪用したデータ アクセスを防止する アクセス セキュリティの拡大: AI によるアクセス拡大に合わせてデータ セキュリティを強化する	Copilot - エンタープライズ データ保護 - 安全性とセキュリティの設定 Defender XDR - 脅威の監視 Sentinel Purview - コミュニケーション コンプライアンス - DLP ポリシー - 情報バリア - 情報の保護 - 内部関係者による脅威からの保護 - Security Copilot

このセキュリティ ツールキットの利用ガイド

マイクロソフト教育機関向けセキュリティ ツールキットは、学校、教育機関、地方および地域の教育部門、教育省の教育リーダーが IT 環境を簡素化し、安全に保護しつつ、安全で革新的な学習体験を実現できるよう支援します。1 つに統合されたマイクロソフト セキュリティ スタック、AI を活用した脅威検出、ゼロ トラストの原則を活用することで、学校や教育機関は IT の複雑さを軽減し、インシデント対応を迅速化し、学生、教職員、研究活動を保護できます。

このツールキットは「**概要**」、「**カスタマーエクスペリエンス**」、「**計画**」、「**実装**」、「**効果**」の5つのセクションで構成されており、右側のナビゲーションタブを使って、フレームワーク、ガイドライン、実際の事例、実証済みの戦略を簡単に確認できます。それによって、セキュリティの全体像から実装までの支援を受けることができます。



Microsoft 365 Copilot を使用する

Microsoft 365 Copilot は AI アシスタントとして、セキュリティ関連のドキュメントの閲覧や機能の探索を自然言語のプロンプトでサポートします。Copilot に、なじみのないセキュリティ概念を説明してもらったり、複雑な実装手順を分かりやすい段階に分解してもらったり、あなたの環境に合わせたツールやリソースを提案してもらいましょう。セキュリティのエキスパートの方も、これから始める方も、Microsoft 365 Copilot は、明確さと自信を持ってドキュメントをナビゲートできるよう支援します。

自分に合った出発点を選ぶ

ご自身の現在のニーズに最も関連性の高いセクションに直接アクセスしましょう。

- **教育セキュリティに初めて取り組む場合:** まず「**概要**」セクションから始めて、マイクロソフトのセキュリティ ビジョンと、なぜ今セキュリティがこれまで以上に重要なのかを理解しましょう。
- **所属機関のケースを作成する場合:** 「**お客様事例**」セクションを参照し、他の教育機関がマイクロソフトのソリューションで実際に成果を上げている様子をご覧ください。
- **戦略を策定する場合:** 「**計画**」セクションのフレームワークを活用して、ギャップを特定し、セキュリティを教育機関の目標に合わせましょう。
- **ソリューションを展開する場合:** 「**実装**」セクションは、マイクロソフトのセキュリティ ソリューションやベスト プラクティスに関する詳細なガイダンスを提供します。
- **今後の展望を考える場合:** 教育セキュリティに関する最新のマイクロソフトのインサイト、業界動向、学術研究については、「**調査**」セクションを参照してください。

このツールキットは、包括的なガイドであると同時に、実用的なワークブックとしても活用できます。評価テンプレート、チェックリスト、フレームワークを活用し、イノベーションを促進しながら教育機関を保護するプログラムを構築してください。セキュリティは単なる保護にとどまらず、教育機関がデジタル トランスフォーメーションや AI の導入、現代教育を特徴づける革新的な教育手法を自信を持って取り入れられるようにするものです。

カスタマー エクスペリエンスを探索する

学校や教育機関がマイクロソフトと連携してセキュリティ態勢を強化した方法を学びましょう。Onslow County Schools がセキュリティと学習アクセスの両立を図った事例から、オレゴン州立大学が学生主導のセキュリティ オペレーション センターを構築した事例まで、これらの経験は機関のセキュリティ強化に役立つ実践的な分析情報を提供します。実装戦略の検討、共通の課題への対応、関係者への価値の提示を進める際に、これらを参考にしてください。

セキュリティ評価を開始する

このセキュリティ ツールキットを通じて、学校や教育機関のセキュリティ態勢を評価するための実践的な演習やアセスメント用プロンプトを利用できます。これらのツールは、課題の洗い出し、改善の優先順位付け、そして総合的な保護を実現するためのロードマップの構築を支援します。まず、現在のデバイスとアプリの管理体制、クラウドおよびオンプレミス環境全体のデータ保護機能、地域、国、グローバルのプライバシー規制へのコンプライアンスを確認してください。



Copilot プロンプト

[初等中等教育/高等教育] 機関のセキュリティ管理者の役割を担ってください。上位の一般的な項目を特定し、それぞれを重大度と NIST CSF カテゴリで分類して、各ギャップに対応する具体的なマイクロソフト ツールを提案してください。推奨事項を表にまとめ、評価を精緻化するために私から取得する必要がある追加情報をリストアップしてください。

ヒント

セキュア スコアの結果や最新のインシデント、リスクの高いシステムなどの項目を共有してください。具体的なシグナルは、Copilot が一般的な仮定ではなく、実際の環境に基づいてギャップ分析を生成する上で役立ちます。

マイクロソフトのセキュリティ ツールでより安全な学習を可能にする

教育におけるサイバーセキュリティは、単なる保護にとどまらず、安全で回復力のある学習を可能にすることです。学校や教育機関は、個人データ、研究、デジタル ツールが日々交差する、独自の価値と脆弱性を持つ環境で運営されています。デジタル学習の拡大に伴い、課題が増える一方で、信頼、アクセス、そして組織のレジリエンスを高める機会も広がっています。

Microsoft Security は、ゼロ トラストとセキュア バイ デザインの原則に基づき、教育機関向けに構築された統合セキュリティ スタックによって、学校や教育機関が一步先に行く支援をします。AI を活用したソリューションは、管理を簡素化し、スケーラブルな運用をサポートし、将来に向けてチームの準備を整えます。セキュリティは、学習を保護し、スタッフを支援して、教育コミュニティ全体にわたる信頼を構築するための戦略的優先事項です。

教育界における実際の効果

学校や教育機関がセキュリティを活用して新たな機会を生み出している方法をご紹介します。

- **戦略的推進要因:** セキュリティを活用してデジタル学習を加速し、公平性を推進し、労働力開発を支援します。
- **信頼の構築:** 学生のアクセス、卒業生のエンゲージメント、教育機関の評判全体にわたって信頼性を高めます。
- **運用の簡素化:** 統合ツールと直感的なダッシュボードにより、混乱を最小限に抑え、対応を自動化します。
- **キャリア スタート支援:** 実践的な経験と学生主導の SOC を通じて、学生のサイバーセキュリティ分野のキャリアに向けた準備を支援します。
- **成長促進要素:** クラウドファーストの柔軟なソリューションを活用し、教育・学習・研究環境全体にわたって保護を拡大します。
- **レジリエンスの推進要因:** ゼロ トラストを基盤とした、デフォルトでセキュア、設計段階からセキュアなソリューションで、組織の備えを強化します。
- **イノベーションの触媒:** 組み込みのコンプライアンスとセキュリティに支えられ、教育者や IT チームは自信を持って新しいテクノロジーを導入できます。

ツール

このセクションの内容

[Microsoft Security ツール](#)



Microsoft Security ツール

教育機関向けセキュリティ ソリューションを探る

マイクロソフトは、教育機関のニーズに合わせた包括的なセキュリティ ツールを提供しています。各ツールの目的やワークフローでの使い方をすばやく把握できるよう、カテゴリごとにわかりやすい要約と厳選したツールを提供しています。

学生のデバイスを保護する場合でも、コンプライアンス要件に対応する場合でも、将来のサイバーセキュリティの課題に備える場合でも、マイクロソフトの統合的なアプローチは、教育のニーズに合わせて構築された柔軟かつコスト効率の高い保護を提供します。



Windows 11 のセキュリティ

学生、教職員、スタッフに、チップからクラウドまでの包括的なセキュリティ保護を提供し、脅威から防御する、ハードウェアによる保護機能を備えています。

特長

- セキュア コア PC による保護
- Windows Hello パスワードレス認証
- BitLocker による暗号化
- Microsoft Defender ウイルス対策 (搭載)
- スマート アプリ コントロール
- Copilot+ PC オンデバイス AI セキュリティ



Microsoft Security Copilot

セキュリティと IT の日常業務のための生成 AI 搭載アシスタントにより、AI のスピードとスケールで機関を保護します。

特長

追加の Security Copilot エージェントは、Defender、Entra、Purview、Intune、Sentinel、サードパーティ製のセキュリティツールと連携して動作します。



Microsoft Defender

業界をリードする拡張検出および応答 (XDR) 製品を活用し、デバイス、ID、アプリ、メール、クラウドへの攻撃を検出して対応します。

特長

- Defender XDR
- Defender for Office 365
- Defender for Endpoint
- Defender for Identity
- Defender for Cloud Apps

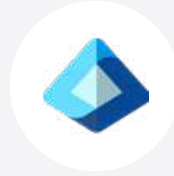


Microsoft Purview

統合された情報の保護、ガバナンス、コンプライアンス製品群を活用し、データがどこに存在していても安全性を確保します。

特長

- 情報の保護
- データ損失防止
- インサイダー リスク管理
- コミュニケーション コンプライアンス
- 情報バリア
- データ ガバナンスデータ マップと統合 カタログ
- 電子情報開示
- データ ライフサイクル管理
- コンプライアンス マネージャー
- AI 向けのデータ セキュリティ態勢管理 (DSPM)



Microsoft Entra

クラウド、プラットフォーム、デバイスにわたるすべての ID およびアクセス要求を、一連の ID およびアクセス管理製品で検証します。Entra Suite for Education の一部として利用できます。

特長

- Entra ID
- 条件付きアクセス
- ID 保護
- 外部 ID
- ID ガバナンス
- Privileged Identity Management
- Entra Domain Services
- 検証済み ID



Microsoft Intune

エンドポイント管理製品により、デバイスセキュリティを強化し、シームレスな業務エクスペリエンスを実現します。

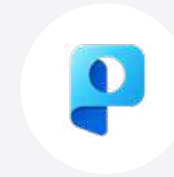
特長

- Intune for Education
- Windows AutoPilot
- モバイル アプリケーション管理 (MAM)
- デバイスのコンプライアンス
- エンドポイントの特権管理



Microsoft Sentinel

コスト効率に優れた長期保有とアドバンスド アナリティクスのための統合データ レイクを備えたセキュリティ情報およびイベント管理 (SIEM) ソリューションで、脅威に対する比類のない可視性を得ることができます。



Microsoft Priva

プロアクティブなリスク軽減とコンプライアンス管理により、学生とスタッフのプライバシーを尊重し、学校が FERPA、GDPR などのプライバシー要件を満たすことを支援します。

特長

- プライバシー リスク管理
- サブジェクト権利要求

お客様への 効果の事例

このセクションの内容

学習環境の保護: 初等中等教育キャンパスにおける効果の事例

高等教育におけるセキュリティ イノベーションの実例

セキュリティに関するその他のお客様事例



学習環境の保護: 初等中等教育キャンパスにおける効果の事例

初等中等教育機関は、数十万台ものデバイスの管理、教育へのアクセスとセキュリティの両立、限られた IT リソースでの機密データの保護など、複雑なセキュリティ課題に直面しています。マイクロソフトのソリューションによってセキュリティへの取り組みを変革した、先進的な3つの学校の事例をご紹介します。





ニューヨーク市公立学校



ニューヨーク市公立学校は Microsoft Intune を活用し、1,800 校に配備された 75 万台を超えるデバイスをわずか数日で管理しました。

課題

COVID-19 の影響で学習がオンラインに移行した際、ニューヨーク市公立学校は前例のない課題に直面しました。75 万人を超える生徒のデバイスを、通常は数か月かかるところを数日で展開および管理するという課題です。

ニューヨーク市公立学校は、Microsoft Intune を選択しました。それがクロスプラットフォームに対応し、コスト効率に優れており、また Microsoft 365 Education ライセンスに既に含まれていたためです。同学区は、550,000 台の LTE 対応 iPad と 200,000 台の Chromebook を展開し、一時的な住居にいる生徒やインターネット接続がない生徒に優先して配布しました。マイクロソフトの Intune チームと緊密に連携し、通常 6 か月かかる実装プロセスをわずか数日で完了させ、重要な展開フェーズでは毎日、場合によっては毎時間サポートを受けました。

効果

効果はすぐに現れ、かつ持続しました。Intune によってすべてのデバイスの種類を一元管理できるようになり、物理的なソフトウェア配布の必要がなくなりました。また、学習への妨げを最小限に抑えるサイレントかつ透明性の高い更新が可能となりました。

ニューヨーク市公立学校は現在も Intune を活用し、展開の自動化、全市規模でのデジタル評価の支援、デバイスの正常性とセキュリティの監視を行い、IT 運用の最新化を進めながら生徒たちの学びを継続させています。

「私たちは、史上最短の期間で史上最多の LTE 対応デバイスを展開するという、最大規模の導入を開始しました。デバイスが動作するのを待つ一分一分が、授業時間の損失につながります。Intune のおかげで、サイレントかつ透明な方法ですべてを管理でき、何十万もの資産を 1 つの画面で把握できます。」

—Alexander Horwatt 氏
ニューヨーク市公立学校、技術革新部門
エグゼクティブ ディレクター

主な検討事項

- ニューヨーク市公立学校のパンデミック対応のような迅速なデバイス展開能力により、学区は予期せぬ事態に備えてどのように準備できるでしょうか。
- 多様なデバイス プラットフォームの管理を一元化すると、IT チームの効率性とセキュリティ態勢にどのような効果がもたらされるでしょうか。
- 状況にかかわらずすべての生徒がインターネット接続可能なデバイスを持てるようにすることは、学区の公平性目標の達成にどう貢献するでしょうか。

マイクロソフトのツール

- [Microsoft 365 Education](#)
- [Microsoft Intune](#)
- [Windows AutoPilot](#)

➡ [ケーススタディ全文を読む](#)

オンスロー郡立学校



オンスロー郡は、Microsoft Intune エンドポイント特権管理を活用し、セキュリティとアクセスの両立を実現しました。

課題

ノースカロライナ州で第 11 位の規模を誇るオンスロー郡学区は、セキュアな試験ブラウザや設計ソフトウェアなどの重要な教育ソフトウェアへのアクセスを、セキュリティを損なうことなく生徒と教育者に与える必要がありました。最高技術責任者 (CTO) の Jeff Pittman 氏は、「マイクロソフトのテクノロジーは私たちの組織全体の基盤となっています」と述べていますが、学区ではイノベーションを実現しつつ、厳格なセキュリティを維持する必要がありました。

効果

オンスロー郡は、6 年生から 12 年生用の 14,000 台のデバイスに Microsoft Intune エンドポイント特権管理 (EPM) を展開することで、セキュリティ態勢を強化しただけでなく、教育の成果も向上させました。このソリューションにより、学生と教育者は、承認済みアプリケーションを、管理アクセス権がなくても最小権限のセキュリティ原則を守りながら利用できます。実装以来、同学区の Microsoft セキュア スコアはほぼ 3 倍に増加しました。

その効果はセキュリティの範囲にとどまりません。教育者は、従来は 48 時間待つ必要があったのに比べて、今では 30 分以内に新しいソフトウェアのアクセス権を得ることができます。Azure によるシームレスなクラウド管理により、オンスロー郡の IT チームはネットワークの内外を問わずデバイスを管理でき、セキュリティを損なうことなく継続的な学習を可能にしています。

「EPM を使用して不正行為防止ブラウザを実行することで学習成果が向上し、その結果、学生がより集中できる、セキュアかつ公平なテスト環境を提供できるようになりました。」

— **Tiffany Rhodes 氏**、
オンスロー郡立学校
教育者

主な検討事項

- オンスロー郡 EPM アプローチのように、セキュリティと教育アクセスの両立を図ることで、学区における相反する優先事項にどのように対応できるでしょうか。
- ソフトウェアの展開時間を 48 時間から 30 分に短縮した場合、教職員の生産性に対してどのような効果があるでしょうか。
- 教育成果を向上させながらセキュリティ スコアを 3 倍にすることは、学区のテクノロジー戦略にどのような変化をもたらすでしょうか。

マイクロソフトのツール

- [Azure](#)
- [Microsoft Defender for Identity](#)
- [Windows AutoPilot](#)
- [Microsoft Intune](#)
- Microsoft Intune Suite
- Microsoft Intune エンドポイントの特権管理

➔ [ケーススタディ全文を読む](#)



ウェストminster スクール



ウェストminster スクールは、Microsoft Defender Experts を活用してキャンパス全体の学生とスタッフのデータを保護しています。

課題

ウェストminster スクールは、1,350 人の生徒と 550 人のスタッフ メンバーの機密データを少数の IT スタッフで保護しなければならず、サイバーセキュリティ上の課題が増大していました。チームは毎週 3 ～ 4 件のセキュリティ インシデントを管理し、過剰な誤検知アラートに苦慮しており、ビザ情報、医療情報、個人データを保護するという重要な責務を担っていました。

ウェストminster はオーストラリアで初めて Microsoft Defender Experts for XDR を導入しました。IT 部門責任者の Chris Rowtcliff 氏は、このサービスを「同校のチームの延長線上にある」と表現しています。管理サービスは、人間主導の専門知識によるエンドツーエンドのセキュリティ保護を提供し、すべての真の脅威が完全に調査されるようにしながら、アラート ノイズを "ゼロ近くまで" 低減します。

効果

このパートナーシップはすぐにその価値を証明しました。学生が誤ってマルウェアのリンクをクリックした際、Defender Experts は脅威を遮断し、その発生源が別の学生であることを突き止めました。このインサイトにより、同校では技術的な修復に限定せず、教育的な支援で対応することができました。

その効果は脅威への対応だけにとどまりません。現在、同チームはアクション項目のほぼ 100% を是正し、エキスパートによる週次チェックインの恩恵を受け、協力的なフィードバックを通じてマイクロソフトの製品開発にも貢献しています。高度なツールと信頼性の高い専門知識により、同校はより安全な環境を築きながら、将来の脅威に対するレジリエンスも強化しました。

「Defender Experts for XDR がもたらした安心感は、いくら強調しても足りません。学校と生徒が安全だとわかっていることで、圧倒感がかなり軽減されています。」

— **Chris Rowtcliff 氏**、
ウェストminster スクール
IT 部門責任者

主な検討事項

- Defender Experts for XDR のようなマネージド セキュリティ サービスは、小規模な IT チームがアラート疲れではなく戦略的取り組みに集中できるようにする上で、どのように役立ちますか。
- 「オンデマンド専門家」は、学校がインシデントから学び、将来の脅威を防ぐ能力にどのような価値をもたらすでしょうか。
- セキュリティ ノイズを "ほぼゼロ" にまで減らすことで、IT チームの業務効率やウェルビーイングはどのように変わるでしょうか。

マイクロソフトのツール

- [Microsoft Defender](#)

➔ [ケーススタディ全文を読む](#)

高等教育におけるセキュリティ イノベーションの実例

機密性の高い研究データの保護から世界中の学生の安全確保まで、高等教育機関は革新的なソリューションが求められる独自のセキュリティ課題に直面しています。3つの有力大学が、教育ミッションを推進しながらセキュリティ態勢をどのように変革したかをご覧ください。





オレゴン州立大学



オレゴン州立大学は、研究データを保護するために Microsoft Sentinel と Defender を実装し、数週間かかっていた検出を数分に短縮しました。

課題

2021 年、重大なセキュリティ インシデントが OSU の重要な研究データを脅かし、R1 研究機関としての評判を守る必要性の緊急性が浮き彫りになりました。最高情報セキュリティ責任者の David McMorries 氏は、「サイバー環境で科学、学習、研究が安全に行える環境を整えたいと考えています」と述べています。」

効果

OSU は Microsoft 365 Education ライセンスを利用して Sentinel と Defender を実装し、SOC をセキュリティ基盤としました。マイクロソフトのエンジニアリング サポートにより、通常 5 年かかるセキュリティ成熟度を 2 年で達成しました。数千件のインシデントは 1 日あたり約 30 件に減少し、検出時間も数週間から数分に短縮されました。Sentinel は同校にとって脅威への対応のための "革命的な" 一元管理画面となりました。

また OSU は、Microsoft Security Copilot を統合することで、学生主体の SOC を支援しました。学生アナリストは、AI を活用して高度なクエリを作成し、プロセスを自動化することで、大学の研究を保護しながら重要な実務スキルを習得しています。研究を保護しつつ、将来のサイバーセキュリティ専門家を教育するというこの二重の使命は、保護と教育に対する OSU の取り組みを体現しています。

「Microsoft Security Copilot は、OSU の SOC で働く学生にとって素晴らしい教育ツールになるでしょう。」

— Emily Longman 氏、
オレゴン州立大学セキュリティ
オペレーション センター マネージャー

主な検討事項

- Security Copilot のような AI ツールによって強化された学生主体のセキュリティ運用は、貴校のセキュリティ ニーズと人材育成目標の両方にどのように貢献できるでしょうか。
- インシデント検出時間を数週間から数分に短縮することで、機密研究データや学生データの保護にどのような影響があるでしょうか。
- "本来 5 年かかる成熟度を 2 年間で達成する" ことは、オープンなコラボレーションと堅牢なセキュリティの両立における貴校の能力をどのように変革するでしょうか。

マイクロソフトのツール

- [Microsoft Sentinel](#)
- [Microsoft Defender](#)
- [Microsoft Security Copilot](#)
- [Microsoft Entra ID](#)
- [Microsoft 365 Education](#)

➡ [ケーススタディ全文を読む](#)



RMIT 大学



RMIT 大学は、世界中にいる 95,000 人の学生に即時デジタル認証を提供するために、Microsoft Entra Verified ID を展開しました。

課題

RMIT 大学は、230 か国にわたり 95,000 人の学生が在籍する中、ますますデジタル化が進む世界において学生の◇証明を強化する必要性を認識していました。エンタープライズ アーキテクトである Ajay Radhakrishnan 氏は、同校は ID テクノロジにおける "見逃された機会" に焦点を当てつつ、生涯学習のつながりに重点を置いていると述べています。課題は、グローバルなデータ保護法に準拠したセキュアで検証可能な資格情報を作成し、物理 ID カードの 14 日間の発行待ち期間を短縮することでした。

RMIT の Blockchain Innovation Hub はマイクロソフトと提携して Entra 確認済み ID を実装し、3 つの使用用途である、学生による図書館の利用やキャンパス割引の利用、就職活動のための卒業生の成績証明書、検証可能なトレーニング認定を開発しました。

効果

パイロット実証では、資格情報を 14 日間ではなく数秒で発行できることが示されました。学生は現在、モバイル デバイスを使って自分自身のデジタル資格情報を管理できるようになりました。図書館サービスから将来の雇用証明まで、すべてを 1 つの QR コードで利用できます。このソリューションは、RMIT の既存の Azure AD インフラを基盤として構築されており、将来的に他のパートナーとの相互運用性を可能にするオープン スタンドards もサポートしています。

「COVID-19 パンデミックによって、その必要性が急速に高まりました。なぜなら、私たちは学生が ID カードを受け取るためにキャンパスに来ることを望んでいなかったからです。Microsoft Entra Verified ID を活用してプロセスをデジタル化し、大幅な効率化を実現しました。」

— **Michael Fairbairn 氏**、
RMIT 大学 Blockchain Innovation
Hub アソシエイトディレクター

主な検討事項

- ブロックチェーンで検証される即時発行の資格情報は、入学から卒業生のエンゲージメントまで、同機関の学生エクスペリエンスをどのように変革できるでしょうか。
- 物理的な ID カードを廃止し、グローバルな管轄区域全体でセキュリティとコンプライアンスを強化することで、どのような運用効率が生まれる可能性があるでしょうか。
- 学生が管理する携帯可能な資格情報が広範なエコシステムと接続することで、従来のキャンパスの境界を越えてどのように価値を創出できるでしょうか。

マイクロソフトのツール

- [Microsoft Entra ID](#)
- Microsoft Entra Verified ID

➔ [ケーススタディ全文を読む](#)



ベンダ大学



南アフリカのベンダ大学は、Azure へ移行することで、15,000 人の学生の 99% の稼働率を達成しました。

課題

南アフリカで 15,000 人の学生が在籍するベンダ大学 (Univen) は、インフラ面で重大な課題に直面していました。散在するオンプレミス サーバーによりダウンタイムが頻繁に発生し、6 か月の調達サイクルが成長の妨げとなっていました。CIO の Sam Khoza 氏が述べるように、同校の使命は「最新のテクノロジーを通じて大学の戦略をサポート」し、世界的に競争力のある卒業生を輩出することでした。

効果

Univen は Microsoft Unified Support を利用して 18 のコア システムを Microsoft Azure に移行しました。移行には、ドキュメント管理システム、人事および財務プラットフォーム、Moodle LMS が含まれていました。結果はすぐに形となって現れました。可用性が 99% に向上し、試験のピーク時でもシステムにアクセスできないという報告は 1 件もなくなりました。

Univen は、Sentinel、Defender、Purview と Security Copilot を併用する、アフリカで初の大学の 1 校となりました。Khoza 氏は次のように述べています。「当大学はアフリカで初めて Microsoft Security Copilot を実装したパイオニア大学として、AI を活用したセキュリティ分野をリードしています。これにより、脅威の検出がより迅速になり、対応もよりスマートになったことで、自信が高まりました。」Microsoft Unified Support とのパートナーシップによって、テクノロジーの提供と校内の機能の構築が実現し、ICT チームは複雑なタスクを担い、イノベーションを推進できるようになりました。

「従来はプロビジョニングに半年かかっていたことが、Azure では数時間で簡単に完了できるようになりました。」

— Vusani Nengovhela 氏、
ベンダ大学
サーバー エンジニア

主な検討事項

- インフラのプロビジョニングを 6 か月から数時間に短縮することで、貴校の教育ニーズへの対応能力はどのように変わるでしょうか。
- 99% のサービス可用性は、学生の学習体験とスタッフの生産性にどのような影響を及ぼすでしょうか。
- AI を活用したセキュリティ分野における地域の先駆者となることで、貴校は重要なデータを保護しながら、どのようにしてテクノロジー リーダーとしての地位を確立できるでしょうか。

マイクロソフトのツール

- [Microsoft 365 for Education](#)
- [Azure](#)
- [Microsoft Sentinel](#)
- [Microsoft Security Copilot](#)
- [Microsoft Defender](#)
- [Microsoft Purview](#)
- [Exchange Online](#)

➔ [ケーススタディ全文を読む](#)

セキュリティに関するその他のお客様事例





メンフィス・シェルビー郡学区

初等中等教育 | 214のキャンパス | 110,000人の学生

ソリューション

Power Apps と Power Automate を活用してカスタム データ ツールを構築することで、カスタム データ収集およびレポート ツールを作成し、多様な運用ニーズに対応するとともに、新規ソフトウェア導入のコストを削減しました。

ツール

Azure SQL ・ Power Apps ・ Power Automate ・ Dataverse ・ Power BI ・ Power Pages

[→ 全文を読む](#)



ニューイングトン カレッジ

初等中等教育 | 3 のキャンパス | 3,200 人の学生

ソリューション

ニューイングトン カレッジでは、セキュリティ インシデントにより教育テクノロジーの保護と管理を強化する必要性が浮き彫りになったことから、Microsoft Education および Quorum と連携し、Quorum の Cyber One MDR、Microsoft 365、Intune を含む包括的なサイバーセキュリティ ソリューションを実装しました。

ツール

Azure ・ Microsoft 365 Education ・ Microsoft Defender for Endpoint ・ Microsoft Defender for Identity ・ Microsoft Intune ・ Microsoft Sentinel ・ Microsoft Defender for Cloud

[→ 全文を読む](#)



ニューヨーク市教育省

初等中等教育 | 1,600のキャンパス | 920,000人の学生

ソリューション

ニューヨーク市の 120 万人の学生がパンデミックによる学校の閉鎖や再開に直面した際、ニューヨーク市教育省は Azure Synapse Analytics 上でクラウドベースのリモート学習プラットフォームを迅速に展開し、高いパフォーマンス、合理化された管理、エンタープライズグレードのセキュリティを実現しました。

ツール

Azure ・ Azure Virtual Desktop ・ Azure Blob Storage ・ Azure Data Lake Storage ・ Azure Synapse Analytics ・ Microsoft 365 Education ・ Microsoft Teams ・ Microsoft Purview ・ Power BI ・ Windows 11

[→ 全文を読む](#)



オレンジ群統一学区

初等中等教育 | 42 のキャンパス | 26,000 人の学生

ソリューション

オレンジ群統一学区は、Microsoft 365 Education と Windows PC を活用して 3 万台のデバイスを学生とスタッフに展開することに成功し、少人数の IT チームによる管理の合理化、セキュリティの強化、そして将来の学生の成功に向けた学習環境の充実を実現しました。

ツール

Microsoft 365 Education ・ Microsoft Entra ID ・ Microsoft Defender for Endpoint ・ Microsoft Intune ・ Windows Autopilot ・ Windows 11

[→ 全文を読む](#)



ウィチタ公立学校

初等中等教育 | 90 のキャンパス | 47,000 人の学生

ソリューション

ウィチタ公立学校は、5 万人高くの生徒と 5,600 人の教育者を対象に、データ保護機能付きの Microsoft Copilot の導入を検討し、個々の生徒のニーズに合わせた、より多様でパーソナライズされた学習体験の提供を目指しています。

ツール

Azure ・ Microsoft 365 Education ・ Microsoft Teams ・ Office 365 ・ Windows 11

[→ 全文を読む](#)



バブソン大学

高等教育 | 2 つのキャンパス | 3,700 人の学生

ソリューション

バブソン大学は、Microsoft Copilot、Azure AI、Microsoft 365 Education を実装することで、老朽化したインフラを最新化し、要支援学生を特定するための予測モデルの開発、STEM 科目向けの数学ボットなどの AI を活用した学習ツールの開発、そして学生が AI スキルを身につけてキャリアに備えるための支援を行いました。

ツール

Power BI ・ Microsoft 365 Education ・ Microsoft Copilot ・ Azure OpenAI

[→ 全文を読む](#)



ハワード大学

高等教育 | 1 つのキャンパス | 11,000 人の学生

ソリューション

歴史的黒人大学であるハワード大学は、2021 年のランサムウェア攻撃を乗り越え、Microsoft Azure への移行と Cloudforce との連携によって 1 年以内にセキュリティ スコアを倍増させました。これは、リソースが限られた大学でも、戦略的なクラウド導入によってセキュリティ強化、効率向上、コスト削減が可能であることを示しています。

ツール

Azure ・ Azure Virtual Desktop ・ Microsoft Entra ID

[→ 全文を読む](#)



ローワン大学

高等教育 | 6 つのキャンパス | 23,000 人の学生

ソリューション

ローワン大学は、Microsoft Azure のクラウドスマート戦略によって IT インフラを最新化し、アクセシビリティ、信頼性、セキュリティを強化するとともに、教授の指導時間を最大 50% 増加させることに成功しました。今後は AI テクノロジーへの拡大も計画されています。

ツール

Azure ・ Microsoft 365 Education ・ Microsoft Intune ・ Microsoft Sentinel

[→ 全文を読む](#)



イリノイ大学アーバナ・シャンペン校

高等教育 | 1つのキャンパス | 56,000 人の学生

ソリューション

イリノイ大学アーバナ・シャンペン校は、ユーザー中心のアプローチを使用して、週末の間に 35 万のユーザー ID を Microsoft Azure Active Directory へ移行することに成功し、同様の ID 管理の課題に直面している他の組織に貴重な教訓を提供しました。

ツール

Microsoft Entra ID

[→ 全文を読む](#)



ワシントン大学

高等教育 | 3つのキャンパス | 52,000 人の学生

ソリューション

ワシントン大学インフォメーション スクールは、サイバーセキュリティ科目用ラボを Azure Lab Services に移行し、コストのかかるオンプレミス機器を柔軟な仮想マシンへと変換することで、アクセスの簡素化、管理負担の軽減、学生の学習目標達成の支援強化を実現しました。

ツール

Azure ・ Azure Lab Services ・ Azure Compute

[→ 全文を読む](#)

計画

このセクションの内容

より安全な学習環境を実現するための戦略的計画
キャンパスの現在のセキュリティ態勢を評価する
セキュリティ ガバナンスとポリシー
テクノロジー セキュリティ戦略
組織の準備状況
財務的および戦略的正当性



より安全な学習環境を実現するための戦略的計画

キャンパスのセキュリティは計画から始まる

学校の IT チームとセキュリティ チームは、単なる技術の守護者ではなく、安全で回復力のある学習環境を築き、学校の使命を推進するための不可欠なパートナーです。セキュリティ リーダーは、デバイスやデータだけでなく、支援するすべての学生と教職員の未来も保護します。

この計画ガイドは、教育機関向けの包括的なセキュリティ戦略の構築に向けた体系的なアプローチを提供します。Microsoft Security ツールやプログラムを導入する前に、この計画ガイドは、目標の明確化、環境の評価、そして最も重要な事項の優先順位付けを支援します。初等中等教育を提供する単一の学校の IT 管理を担当している場合でも、複数キャンパスを持つ高等教育機関で複雑な研究ニーズに対応しながらセキュリティを主導している場合でも、このガイドは効果的で拡張性のあるサイバーセキュリティの確かな基盤づくりに役立ちます。



Copilot プロンプト

最新のセキュリティ戦略のリンクはこちらです [リンクを挿入]。

教師やスタッフに新しいセキュリティ戦略を説明するためのコミュニケーション計画とメッセージ テンプレートを作成してください。教育者、学校の指導者、IT 部門向けの各バージョンと、よくある懸念事項に対応する FAQ も含めてください。

ヒント

スタッフが圧倒されている、慎重になっている、好奇心を抱いているなど、スタッフの感情について記述してください。Copilot は、実際の懸念に対応し、導入を促進するために、トーンやメッセージを調整できます。

安全な学びへの道筋を描く

初等中等教育機関では、簡潔で効果的なセキュリティ対策が重視されます。Microsoft 365 A3 は、多要素認証 (MFA)、[Defender for Endpoint Plan 1](#)、[Intune](#) (デバイス管理用) など、必須のセキュリティ保護による強固な基盤を提供します。これらのツールは、学生の学習を保護しつつ、IT 運用の管理も容易にします。

Defender for Endpoint プラン1 は、Microsoft 365 A3 for Faculty ライセンスには含まれていますが、学生使用特典サブスクリプションには含まれていません。学生のデバイスについては、セキュリティ要件や予算に応じて、追加のライセンスや代替の保護策の導入をご検討ください。

Microsoft 365 A5 には、脅威の検出、コンプライアンス管理、AI ガバナンスのための高度な機能が導入されており、学校は進化するリスクに対して先手を打つことができます。全[機能の比較](#)をご覧ください。

高等教育機関は、機密性の高い研究の保護、広範囲にわたる複数キャンパスのネットワーク管理、厳格な規制基準の遵守など、独自の課題に直面しています。これらの機関には、多様な環境に拡張可能で、複雑なガバナンスのニーズに柔軟に対応できる包括的なセキュリティ フレームワークが必要です。マイクロソフトの高度なセキュリティ機能は、ID 保護、データ損失防止、セキュアなコラボレーションのための統合ツールによって、教育の要求を満たすように設計されています。



Copilot プロンプト

当校の **[初等中等教育/高等教育]** 環境における Microsoft 365 A3 または A5 ライセンスのセキュリティ機能を、セキュリティ、コンプライアンス、AI ガバナンス、デバイス管理に重点を置いて比較してください。私たちの優先事項に基づいて、どのプランが最適か、理由も含めて提案してください。結果を意思決定マトリクスで提示し、リーダーが考慮すべき主要な基準を挙げてください。

ヒント

スタッフのセンチメントを記述します。Copilot は、実際の懸念に対応し、導入を促進するために、トーンやメッセージを調整できます。



Copilot プロンプト

フィッシング耐性のある MFA の 30/60/90 日の段階的な導入計画を、管理者アカウントを皮切りに作成してください。前提条件、変更管理手順、トレーニング要件、リスクを含めてください。例外またはパイロットテストが必要なユーザー グループを特定してください。

ヒント

サインインやデバイス アクセスでよく苦勞しているユーザー グループを Copilot に伝えます。これは、教室での混乱を最小限に抑え、さらなる支援が必要なグループをサポートできるような MFA 導入計画を立てる上で役立ちます。

計画中に実施できる、効果の高い初期のステップ

フィッシング耐性のある MFA を有効にする:

すべてのユーザーに対して [Microsoft Entra ID](#) を使用した多要素認証を有効化します。パスキー (FIDO2)、Windows Hello for Business、証明書ベースの認証といったフィッシング耐性のある認証方式は、資格情報の盗用に対して非常に強力な保護を提供します。すべてのアカウントに対して多要素認証 (MFA) を有効にすることで、[99.9% を超えるアカウント侵害攻撃](#)を防ぐことができます。

MFA の展開を計画する

管理者アカウントやリスクの高いユーザーから始めて、教育機関全体に展開する段階的なアプローチを検討します。MFA は卓越したセキュリティ上のメリットを提供しますが、教育機関全体でフィッシングに強い認証を実装するには慎重な計画が必要です。マイクロソフトは、[包括的な展開ガイド](#)を提供して導入を支援します。

MICROSOFT DEFENDER を有効にする

[Microsoft Defender](#) と [Microsoft セキュア スコア](#) の態勢評価をベースラインとして使用し、継続的な改善を図ります。

キャンパスの現在のセキュリティ態勢を評価する

保持していることを把握していない資産は保護できません。

包括的なセキュリティ プログラムを計画するための最初のステップは、組織の現在の状況を把握することです。これにより、保護の強化、コンプライアンスの効率化、運用効率の向上を通じて、教育ミッションをさらに発展させる新たな機会を発見できます。

マイクロソフトの統合セキュリティ ソリューションを活用して、準備状況を評価し、投資に優先順位を付け、即時に価値を提供しましょう。

Windows 11 のセキュリティ基盤上に構築する

セキュリティ戦略はデバイス レベルから始まります。[Windows 11](#)は、搭載された保護機能により、チップからクラウドまでのセキュリティを提供します。

- **ハードウェアに裏打ちされたセキュリティで防御する:** [トラステッドプラットフォームモジュール \(TPM\) 2.0](#) と [セキュアコア PC](#) による保護を利用して、ファームウェア攻撃や資格情報の盗難から防御します。
- **パスワードレス認証を有効化する:** 生体認証または PIN を使用した [Windows Hello for Business](#) を実装します。これは特に初等中等教育の児童や生徒にとって有用です。
- **アプリケーションとデータを保護する:** [スマートアプリコントロール](#)を展開して、悪意のあるアプリケーションをブロックしながら、[BitLocker](#) でドライブを暗号化します。

Windows 11 を使用している組織は、[セキュリティ インシデントが 62% 減少](#)したことを報告しています。このセキュアな基盤は、[Microsoft Intune](#) や [Defender for Endpoint](#) とシームレスに統合されています。



搭載された安全対策で AI イノベーションを保護する

マイクロソフトは多層的な AI セキュリティ保護を提供しています。

[Copilot+ PC](#): セキュアコアによる保護と [Microsoft Pluton](#) セキュリティ プロセッサを搭載しています。ニューラル プロセッシング ユニット (NPU) はローカルでの AI 処理を可能にし、機密データをクラウドではなくデバイス上に保持することで、プライバシーを強化します。

Microsoft 365 Copilot: エンタープライズグレードのセキュリティが自動的に機能します。

- **既存の権限を尊重:** 教育機関のアクセス制御と秘密度ラベルを維持します。
- **有害なコンテンツをブロック:** アダルト コンテンツ、暴力、ヘイト スピーチをフィルタリングし、プロンプト インジェクション攻撃を防止します。
- **暗号化ポリシーを遵守:** [Microsoft Purview](#) の暗号化ポリシーと DLP ポリシーを自動的に適用します。
- **データをテナント内に保持:** プロンプトと応答を環境内に保存します。お客様のデータは[モデルのトレーニングには使用されません](#)。
- **監査証拠を提供:** Microsoft Purview を通じて、Copilot のすべてのやり取りを FERPA および COPPA のコンプライアンスのために監視・追跡します。

これらの保護措置により、強力なセキュリティと児童の安全基準を維持しながら、安心して AI を導入することができます。

一般的な脅威を認識する

教育機関は、学習を妨げたり機密データを危険にさらしたりする可能性のある、さまざまなサイバーセキュリティの脅威に直面しています。たとえば、システムをロックダウンするランサムウェア攻撃、教職員や学生を標的としたフィッシング攻撃、侵害されたアカウントやアクセス権を不正使用する内部関係者による脅威、研究やインフラを標的とする国家レベルの攻撃などがあります。

これらのリスクを正しく理解することで、チームは環境に即した戦略を立て、大切なものを守ることができます。

セキュリティ上の優先事項を検討する

以下の表を使って自身の環境を振り返り、活かせる強みを見つけましょう。評価を始めるにあたり、以下の重要な質問について検討してください。

質問	インサイト
使用している環境で最も重要なものは何か。	最も貴重な資産を最初に検討しましょう。重要な資産には、学生情報システム、研究データ、財務記録、学習管理プラットフォームなどがあります。これらのシステムは組織の使命を推進するものであり、優先的に保護すべきです。
アクセスが必要なユーザーは誰か。	学生、教職員、スタッフ、管理者、外部ユーザーなどのユーザー グループをマッピングします。各グループには異なるニーズとリスク プロファイルがあります。
何がうまく機能しているか。	既存のセキュリティ対策、成功しているポリシー、既に適切なセキュリティ実践を支えているユーザーの行動を記録します。始めは、強みを生かして取り組みましょう。

コンプライアンスと規制対応の準備を重視する

高いコンプライアンスを維持している学校は、コミュニティの信頼と安心を育みます。高等教育機関は、医療や研究プログラムなどの優先事項を推進するためにコンプライアンスが不可欠です。AI ツールの急速な導入に伴い、教育機関に新興技術に対するプロアクティブなガバナンスも必要としています。

[Microsoft Purview コンプライアンス マネージャー](#)は、複雑な規制対応を自動化されたワークフローへと変えます。チームはゼロから始める代わりに、事前に作成されたテンプレートを利用できます。これにより、次のような課題に対処できます。

- K-12 関連の規制 (学生記録に関する FERPA、年少児を対象とする COPPA、その他の規制要件)
- 高等教育では、国際学生のデータに関する GDPR、医療プログラムに関する HIPAA 対応準備、助成金のコンプライアンス保護などに重点が置かれています。

教育イノベーションに向けた AI ガバナンスの推進

[AI 用 Microsoft Purview データ セキュリティ態勢管理 \(DSPM\)](#) は、機密性の高い教育データが Microsoft 365 Copilot やサードパーティ製ツールなどの AI システムとどのようにやり取りされるかを可視化し、制御することができます。AI 用 DSPM は、教育機関が AI プロンプトでのデータ共有の監視、自動化された保護ポリシーの適用、監査証跡の保持、コンプライアンス インシデント発生前のリスクのある行動の検出を実現する上で役立ちます。



Copilot プロンプト

FERPA および COPPA コンプライアンス チェックリストを作成し、各要件に関連する Purview ツール (DLP、情報の保護、インサイダー リスク、電子情報開示) にマッピングしてください。

ヒント

過去の監査結果や既知のコンプライアンス ギャップを共有します。Copilot は、学区で最もリスクが高い分野に重点を置いて FERPA/COPPA チェックリストを作成できます。

構築を進める

測定主導の評価を行うことで、教育ミッションを支える戦略的なセキュリティ計画の基盤が構築されます。明確な指標は進捗の可視化に役立ち、継続的な改善の指針となります。

- [Microsoft セキュア スコア](#): 組織のセキュリティ態勢をパーセンテージで測定し、Microsoft 365 環境全体で推奨されるセキュリティ対策の完了状況を示します。
- [Microsoft Purview コンプライアンス マネージャー](#): FERPA や GDPR などの規制全体にわたる改善措置の進捗状況を追跡する、ポイントベースの評価システムを活用し、遵守状況を評価・管理します。

現在の態勢を理解することで、教育機関を強化するセキュリティ戦略の基盤を築くことができます。



Copilot プロンプト

Microsoft 365 の Microsoft セキュア スコアを活用してセキュリティ態勢を強化し、ゼロトラストのアプローチを実装できる方法を分析してください。今学期のセキュア スコアを向上させるための、インパクトの大きいアクションを 5 つ提案してください。これらのアクションは労力と影響度を比較して優先順位付けし、最初に対処すべき依存関係をすべて特定してください。

ヒント

最優先のセキュリティ目標 (学生データの保護やインシデント応答時間の短縮など) を共有すると、Copilot はそれらの目標を直接支援するセキュア スコア アクションを優先的に提案できます。

セキュリティ ガバナンスとポリシー

効果的なガバナンスは、セキュリティを事後対応型から戦略型へと変革できます。適切なフレームワークは運用を合理化し、コミュニティの信頼を築き、機関固有の要件に適合します。

[アメリカ国立標準技術研究所 \(NIST: National Institute of Standards and Technology\)](#) は、自主的なガイダンスを提供しており、多くの教育機関が実践的な実装方法とリスク管理のためにこれを活用しています。[Microsoft Security Copilot](#) がプロビジョニングされている機関では、AI を活用したポリシー マッピングによって、現在のポリシーを NIST のカテゴリに照らして分析し、重点的に取り組むべき分野を特定できます。

研究および医療プログラムを持つ高等教育機関では、[ISO 27001](#) 認証が必要となる場合もあります。この国際的に認められた情報セキュリティ管理基準は、機密性の高い研究環境に求められる包括的なデータ保護、リスク管理、コンプライアンス体制をサポートします。

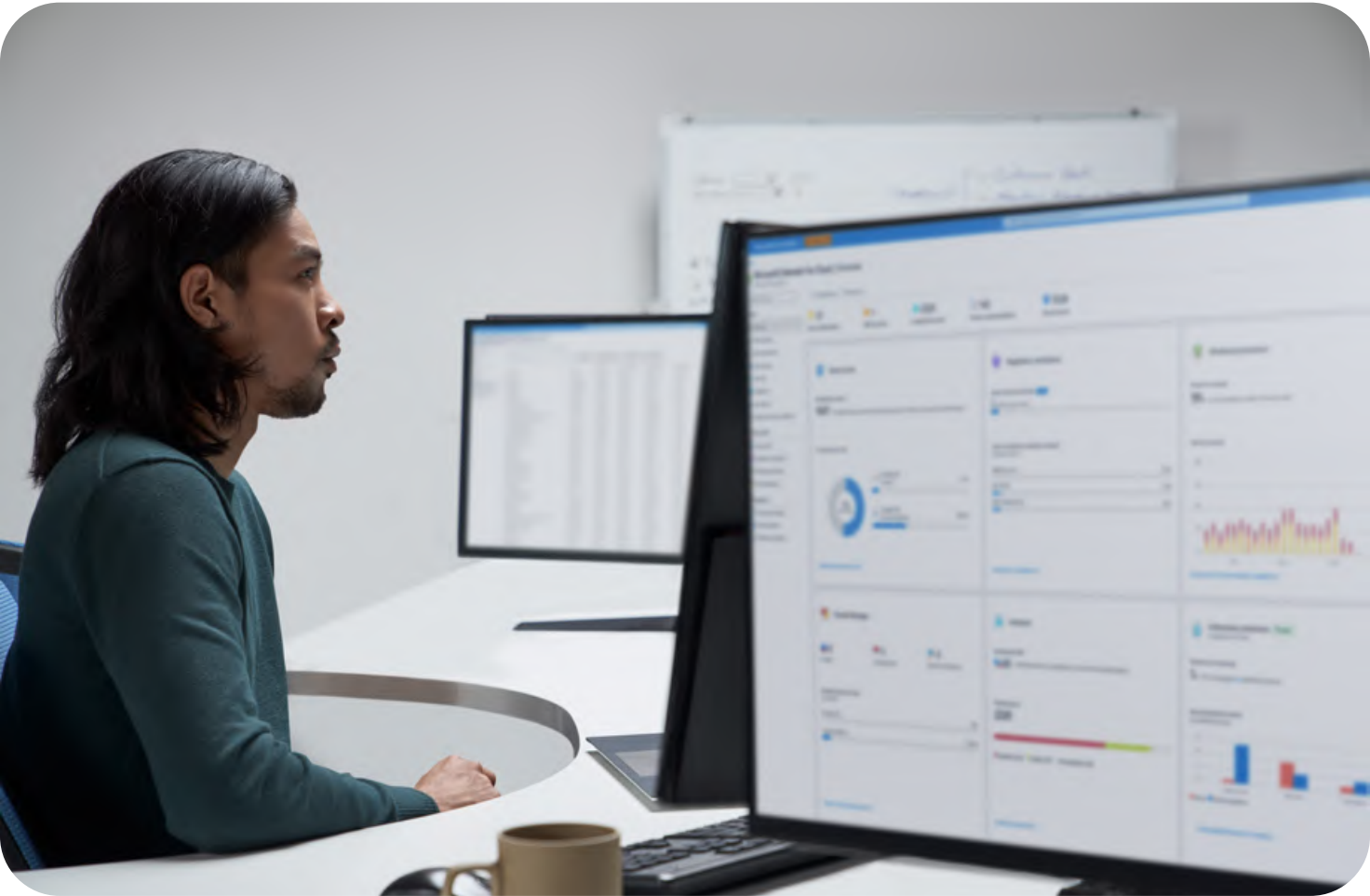


Copilot プロンプト

すべてのユーザー グループ（学生、教職員、代替教員、研究者、請負業者）のアクセス要件を洗い出し、Entra ID を使用して、推奨される条件付きアクセス ポリシーを生成してください。リスク レベルを含めたポリシー マトリックスとしてこれを提供してください。

ヒント

季節的または一時的なアクセスのニーズ（代替教員、請負業者、教育実習生、客員研究員など）を記述すると、Copilot は動的なアクセス ポリシーを設計できます。



ユーザー アクセスの管理の簡素化

[Microsoft Entra ID](#) は、ユーザーのニーズが急速に変化する教育環境の複雑さに対処します。条件付きアクセス ポリシーは、学術現場の実態を反映し、一時的なユーザーや季節的なアクセス ニーズ、学期ごとに変化するコラボレーション要件などを考慮する必要があります。以下の表を使用して、学術環境を反映したユーザー アクセス ポリシーを策定してください。

初等中等教育のユーザー	両方	高等教育のユーザー
生徒	教職員および教育者	研究者
代替教員	スタッフ	大学院生
ボランティア スタッフ	管理者	業界パートナー
保護者や後見人によるアクセス	IT 担当者	
	ゲスト ユーザー	
	請負業者	

インシデント対応の実例：
期末試験期間中のランサムウェア

期末試験期間中に、疑わしいファイル暗号化アクティビティによって教育機関のネットワーク全体でアラートが発生しました。

1. 脅威を検出: [Microsoft Defender XDR](#) がランサムウェアのシグネチャを特定し、[Microsoft Entra ID 保護](#)が外部 IP アドレスからの異常な管理者ログイン試行にフラグを立てます。

2. 自動対応: 数分以内に、[Microsoft Sentinel](#) プレイブックが [Microsoft Defender for Endpoint](#) を通じて影響を受けたデバイスを隔離し、侵害された管理者アカウントを [Microsoft Entra ID](#) 経由で無効化して、IT スタッフと学長に [Teams](#) 通知を送信します。

3. 回復とガイダンス: [Microsoft Security Copilot](#) がプロビジョニングされている機関では、AI を活用した分析により攻撃パターンに関するインサイトと修復の推奨事項が提供され、[Microsoft Purview](#) が保険の請求や規制報告のためにすべてを文書化します。
4. 将来の攻撃を防ぐ: [Microsoft Defender for Office 365](#) は、ランサムウェアが含まれたメールや悪意のある添付ファイルがユーザーに届く前にプロアクティブにブロックし、[安全な添付ファイルと安全なリンク](#)機能によって、ランサムウェア攻撃の前兆となることが多いフィッシングの攻撃活動に対して追加の保護層を提供します。

5. 結果: 自動化されたシステムが脅威を封じ込め、復旧作業のガイダンスを提供する間、授業は中断されずに継続されます。

プロアクティブなインシデント対応計画は、期末試験期間のような重要な時期でも、教育機関が継続性を維持し、学習を保護するのに役立ちます。

テクノロジー セキュリティ 戦略

テクノロジーに関する意思決定は、セキュリティを強化し、初日から学びを支援するための好機となります。マイクロソフトと連携し、組み込みのセキュリティ機能を活用することで、教育機関は保護と生産性が両立する環境を作り出すことができます。

効率化とセキュリティ強化

[Microsoft 365 A3 for Education](#) を利用して必須のセキュリティ機能と生産性ツールを提供し、学区が初期段階からリソースと保護を最適化できるよう支援しましょう。

- [Microsoft Defender for Endpoint](#): 教職員向け A3 ライセンスに含まれる Defender for Endpoint プラン1を利用して高度な脅威からの保護を展開し、教育デバイス環境向けに設計された必須のエンドポイント セキュリティを提供します。注意: 学生使用特典サブスクリプションには、Defender for Endpoint の追加ライセンスが必要です。
- [Microsoft Intune for Education](#): 教室環境向けに設計されたデバイス管理を、学習ワークフローを妨げることなく簡素化します。
- AI 用 [Microsoft Purview データ セキュリティ 態勢管理](#) (DSPM): 基本的な AI 監視を展開して AI の使用パターンを可視化し、学生データの不適切な共有から保護します。
- [Microsoft 365 Education](#) ストレージ: 搭載された FERPA コンプライアンス、データ レジデンシー保護、自動バックアップ、予測可能な運用コストを備えたクラウドファースト ストレージを実装します。



研究に対応した包括的なセキュリティを構築する

より複雑なニーズを持つ高等教育機関では、包括的なアプローチが堅牢な保護とコンプライアンスの支援に役立ちます。[Microsoft 365 A5 for Education](#) を使用して、高度なセキュリティ、分析、コンプライアンス機能を有効化し、複雑な研究環境や複数キャンパスの運営を支援しましょう。

- ゼロ トラストの基盤: [Microsoft 365 Copilot](#) や [Security Copilot](#) のような高度な AI ツールを展開する前に、不可欠なセキュリティ基盤を確立します。
 - ハイブリッド インフラ戦略: クラウドでの共同作業とオンプレミスの研究システムのバランスを保ち、規制遵守、データ主権、知的財産権の保護を図ります。
 - [Microsoft Sentinel](#): AI 搭載のセキュリティ情報イベント管理 (SIEM) を構成して、複数のキャンパスや研究ネットワークにわたるエンタープライズ規模の脅威検出を実現します。
 - [Microsoft Purview](#): 助成金要件の遵守、国際的な研究協力、規制に関する報告の自動化を実現するための包括的なデータ ガバナンスを導入します。
 - [Microsoft Purview AI 用 DSPM](#): 詳細な分析、ポリシーの適用、コンプライアンス管理を活用して、高度な AI ガバナンスを構成し、セキュアな研究運用を支援します。
- マイクロソフトの実績ある[クラウド導入フレームワーク](#)を利用して、クラウド移行とデータ レジデンシーの戦略を計画しましょう。



Copilot プロンプト

複数のキャンパスを含む学区で Microsoft Intune を展開するためのステップバイステップの計画を提示してください。この計画には、Autopilot のセットアップ、コンプライアンス ポリシー、共有デバイスと 1 人 1 台のデバイスの加入契約オプション、推奨されるパイロット シーケンスを含めてください。推奨事項はチェックリスト形式で提示してください。

ヒント

デバイスの組み合わせ、ネットワークの制限、デバイスの利用形態 (共有または 1 人 1 台) に関する詳細を提供します。これによって、Copilot は Intune の加入契約とポリシーの推奨事項をお客様の環境に合わせてカスタマイズできます。

組織の準備状況

サイバーセキュリティのスキル向上は、成熟したプログラムの不可欠な要素です。組織の準備体制を整えることで、熟練した人材、積極的なユーザー、ミッションを支える強固なサイバー衛生管理を通じて、最大限の価値を提供できるようになります。



Copilot プロンプト

学生向け SOC プログラムを立ち上げる手順をまとめてください。必要なマイクロソフト ツール (Sentinel、Defender XDR、Security Copilot)、カリキュラムのリソース、教職員のスポンサーシップ、学生の役割、12 週間の実装タイムラインを含めてください。

ヒント

利用可能な人材プール (サイバーセキュリティ クラブ、STEM アカデミー、勤労学生など) と推定監督時間を提供してください。Copilot はそれによってキャパシティや学生のスキル レベルに合わせたプログラムを設計できます。

準備段階を進める

マイクロソフトは、キャンパス全体のメンバーがサイバーセキュリティの知識とスキルを身につけ、高めるためのリソースを提供します。以下の実装段階を順に実施してください:

1. 基盤の構築: Microsoft Learn と Microsoft Education のサイバーセキュリティ意識向上プログラムを機関全体に導入します。
2. エンゲージメントの拡大: 学生向けサイバーセキュリティ プログラムを実施し、セキュリティ文化とスキル育成の継続的な計画を策定します。
3. 高度な機能: Microsoft Student SOC Toolkit を利用して学生向けセキュリティ オペレーション センター (SOC) プログラムを立ち上げます。このツールキットは、Microsoft Defender XDR、Sentinel、Security Copilot における実践的な体験ができる体系的な学習モジュールを提供します。

表を利用して、チームに最も適したリソースとスキル習得の道筋を特定しましょう。

これらのリソースは、教育機関のすべてのメンバーがセキュアで回復力のある学習環境に貢献するのに役立ちます。

準備状況の焦点	基盤の構築	拡張と高度なスキル習得
K-12 の IT スタッフ IT 管理者向けのセキュリティ基本事項と自動化された脅威対応	Microsoft Learn セキュリティ ハブ マイクロソフト認定資格: セキュリティ、コンプライアンス、ID の基礎 Microsoft Security Copilot のコア機能について説明する	セキュリティのベスト プラクティスと優先順位に沿ってソリューションを設計する Microsoft Security Copilot を使用してセキュリティ運用を強化する
高等教育機関の IT スタッフ AI 拡張とエンタープライズ規模の脅威ハンティングによる高度な SecOps	Microsoft Learn セキュリティ ハブ Microsoft Sentinel 環境を構成する Microsoft Security Copilot を使用してセキュリティ運用を強化する	マイクロソフト認定資格: セキュリティ、コンプライアンス、ID の基礎 Microsoft Security Operations Analyst
教職員、スタッフ、管理者 教室のサイバーセキュリティ、安全な技術慣行、研究データの保護	初等中等教育の教室におけるサイバーセキュリティのレジリエンスをマイクロソフトのツールで構築する サイバーセキュリティとは? 研究者向け Azure パート 1: クラウド コンピューティングの概要	Minecraft Education を使用してサイバーセキュリティの概念を教える マイクロソフトのツールを利用して初等中等教育学校のサイバーセキュリティ指導力を強化する 研究者向け Azure パート 2: クラウド セキュリティとコスト管理
初等中等教育学校の児童・生徒 デジタル市民権、AI の安全な探求	初等中等教育サイバーセキュリティの会話ガイド および インフォグラフィック Minecraft サイバーおよびデジタル市民	セキュリティの基礎 (SC-900) クラスルーム ツールキット: 安全にかつ責任を持って生成 AI の可能性を引き出す
高等教育機関の学生 キャリアの準備と実践的なセキュリティの経験	Microsoft Student Security Operations Center Toolkit Microsoft Learn Student Hub の学生の認定資格	マイクロソフト認定資格: セキュリティ、コンプライアンス、ID の基礎 マイクロソフト サイバーセキュリティ奨学金プログラム

財務的および戦略的正当性

マイクロソフトのセキュリティ ソリューションへの投資は、教育機関が測定可能なリターンを得て、リソースの充実を図り、コンプライアンスを強化するのに役立ちます。

マイクロソフトの委託により Forrester が実施した Total Economic Impact 調査では、Microsoft 365 Education A5 を導入している初等教育および高等教育機関におけるセキュリティの ROI を分析しました。

- [複合初等中等教育組織](#): 3 年間の利益が 422 万ドル、コストが 1,94 万ドルで、ROI は 118%。
- [複合高等教育機関](#): 利益が 728 万ドル、コストが 319 万ドルで、ROI は 128%。
- [Microsoft Security Copilot の予測 ROI](#): 99 ~ 348%、予測される正味現在価値は 50 万 ~ 180 万ドル。

戦略的価値の表で、セキュリティへの戦略的投資が機関にもたらす具体的な利益をご確認ください。

投資の焦点	定量化されたメリット	財務的・業務的影響
AI を活用したセキュリティ運用	• Security Copilot により SecOps の生産性が 23 ~ 47% 向上 • 迅速な脅威対応により侵害防止を強化	さまざまな業界で 99 ~ 348% の投資収益率 (ROI) を達成。
セキュリティとコンプライアンス	• 重大な侵害を 15% 削減 • 侵害の修復コストを 29% 低減	節約額: 初等中等教育機関では 972,800 ドル、高等教育機関では 120 万ドル。
ベンダーの集約	• セキュリティ ライセンスのコストを 30% 削減 • 単一のベンダーに統合することで管理を簡素化	節約額: 初等中等教育機関では 110 万ドル、高等教育機関では 170 万ドル。
人員配置の効率性	• IT セキュリティ チームの大規模な拡大を回避 • 競争の激しい人材市場で重要な強みを提供 • 採用および人材定着に関する課題を軽減	節約額: 初等中等教育機関では 545,700 ドル、高等教育機関では 110 万ドル。 現在の人員の運用効率を最大化し、増員の必要性を大幅に軽減。
生産性の向上	• 社員 1 人あたり 15 分の業務時間を節約 • セキュリティに関するユーザー エクスペリエンスとシステムの可用性を強化 • 迅速な脅威対応により侵害防止を強化	節約額: 初等中等教育機関では 170 万ドル、高等教育機関では 330 万ドル。 • Security Copilot を活用することで SecOps の生産性を 23 ~ 47% 向上 • さまざまな業界で 99 ~ 348% の ROI を達成

ライセンスを最適化する

組織に適した Microsoft 365 Education プランを選択しましょう。現在のセキュリティ リスク、チームのキャパシティ、利用可能なリソースなどの要素を考慮してください。

- **A3 基盤アプローチ:** 既存のマイクロソフトの投資を活用した基本的なセキュリティから始め、まず MFA を導入し、セキュリティ レイヤーを段階的に追加していきます。
- **A5 包括アプローチ:** 複数キャンパスの運用や総保有コストの最適化を支援する、エンタープライズ向けの脅威からの保護とコンプライアンス ツールを利用して、高度なセキュリティ、コンプライアンス、分析を展開します。



Copilot プロンプト

現在利用しているセキュリティ ベンダーを評価し、どのツールがマイクロソフト セキュリティ スタックで置き換え可能かを示す統合マップを作成してください。予測されるコスト削減額、統合のメリット、段階的な移行計画を含めてください。

[既存のすべてのセキュリティ ベンダーと、有効になっているアプリおよび機能の一覧のリンクを提供するか、一覧を含むドキュメントをアップロードしてください。]

ヒント

現在のベンダー リストを提供し、コストが高いまたは維持が難しいツールを記載してください。Copilot は、最大のコスト削減と効率向上をもたらす統合を優先できます。

予算の計画と正当化

チームは展開タイムライン、ROI によるコスト削減効果、そしてコストの補填に利用できるその他のリソースがあるかどうかについても検討する必要があります。

- **段階的アプローチ:** 基盤の展開 (A3 ベースライン) から始め、その後戦略的に拡大 (A5 アップグレード) し、最終的に機関全体で最適化を行います。
- **予算計算フレームワーク:** リスク軽減効果を算出し、運用効率の向上を加味して、戦略的能力開発を含めて包括的な ROI の正当性を立証します。
- **コストの回避:** 2025 年には [1 件あたり平均 444 万ドル](#) の損害をもたらすセキュリティ インシデントを防止し、コンプライアンスの自動化により開発コストを削減します。またインフラの統合により、教育分野の調査で実証されたように 118 ~ 128% の ROI を達成します。
- **教育分野に特化した資金調達機会:** FERPA、COPPA、GDPR の規制要件へのコンプライアンスを実証しながら、セキュリティ プログラムへの投資を支援する助成金の申請や業界パートナーシップを探します。

実装

このセクションの内容

[初等中等教育における実装シナリオ](#)

[高等教育向けの実装シナリオ](#)



初等中等教育における実装シナリオ

ID のセキュリティ

共有モデルや1人1台モデルなどのテクノロジー アクセス モデルは、IT チームに特有の課題をもたらします。

課題の概要

1人1台デバイス向けのプログラムでは、学生が多要素認証（MFA）に苦勞することがよくあります。パスワード忘れであれ、プロンプトの遅延であれ、二次デバイスの必要性であれ、こうした障壁は学びを妨げ、フラストレーションを生み出します。

共有環境（ラボ、カート、図書館など）では、従来の MFA は実用的ではなくなります。多数の生徒が短時間で同じ端末を使い回すため、サインインの繰り返しが生徒のボトルネックを引き起こし、授業の進行が遅れて IT リソースを圧迫します。

マイクロソフトのソリューションの実例

マイクロソフトのツールは、学習の妨げにならずに学生データを保護できる柔軟なサインイン オプションを提供します。

1人1台のデバイス

課題	マイクロソフトのツール	実際の効果
学生がパスワードを忘れたり、個人のデバイスで MFA に苦勞したりする。	Windows Hello for Business: ユーザーが従来のパスワードの代わりに生体認証データや PIN を使用して Windows デバイスにサインインできるようになります。	指紋、顔認識、または PIN を使用したセキュアなサインインを可能にし、ログインの手間を減らして、フィッシングのリスクを最小限に抑えます。
学生が授業や試験の直前に認証情報を忘れる。	Entra ID 一時アクセス パス (TAP): 一度限りまたは複数回サインインできるように構成できる、時間制限付きのパスワードを提供します。	教員や IT スタッフは、時間制限付きのセキュアな認証情報を発行できるため、授業を遅れなく順調に進行できます。
教員と学生が毎日複数のアプリやログインを使い分けている。	Entra ID フェデレーション ID: シークレットを管理する必要なく、Microsoft Entra で保護されたリソースへのアクセスを提供します。	アプリ間でのシームレスなシングルサインオンを提供することで、ログイン疲れを軽減し、授業をスムーズに進めることができます。

共有デバイス

課題	マイクロソフトのツール	実際の効果
共有デバイス（ラボ、カート、図書館）には迅速なアクセスが必要なのに、従来の MFA ではサインインが遅い。	Entra ID FIDO2 キー: ユーザー名やパスワードを入力せずに認証します。	ポータブル セキュリティ キーによるタップアンドゴーアクセスを実現することで、個人のスマートフォンの必要性がなくなり、セッションの生産性が維持されます。
学区の IT 部門が、大規模な環境にわたってユーザーとデバイスを検証する必要がある。	Entra ID 証明書ベースの認証: Microsoft Entra ID で認証された X.509 証明書を使用して直接認証するよう、ユーザーに要求します。	公開鍵インフラ (PKI) を利用してセキュアなサインインを拡張することで、ヘルプ デスクへの問い合わせ件数が減り、共有環境全体のコンプライアンスが強化されます。
学区リーダーは、学習を妨げることなく機密データを保護しなければならない。	条件付きアクセス ポリシー: ユーザーにアクセスを得るための操作を義務付けることで、機関の資産を保護します。	役割、リスク レベル、デバイスのコンプライアンスに基づいてアクセス権を動的に調整し、保護とユーザビリティを両立させます。

開始する

学区は ID セキュリティを強化するために、確実な段階的アプローチを実施できます。パイロット教室から導入を始めることで、学校や教育機関は、ステップバイステップのセットアップ ガイドを活用しながら Microsoft Entra ID ソリューションを探り、最適な方法を見極めて、効果的な戦略を全学区に展開できます。その間も学習は途切れずに続きます。

MICROSOFT ENTRA ID
ソリューションを探索する

ステップバイステップのセットアップ ガイドを確認し、教室環境でパイロット運用した後、地区全体に拡大します。

[→ 詳細情報](#)

重要なポイント

学生の指紋によるサインインから、学区リーダーによる数千アカウントの保護まで、マイクロソフトの ID ソリューションは保護とシンプルさを両立しています。Windows Hello、Entra ID ツール、柔軟なアクセス ポリシーを組み合わせることで、学校は学習に重点を置きながらデータを保護できます。



データ セキュリティと コンプライアンス

学校は個人を特定できる情報（PII）にアクセスし、保存します。この情報は、学生の安全確保と規制遵守のために保護する必要があります

課題の概要

サイバー犯罪者は学校を標的にしてシステムに侵入し、機密データを抽出します。強力なサイバーセキュリティ対策がなければ、脅威アクターはデータにアクセスし、身代金が支払われるまで学校がシステムを利用できなくする可能性があります。

システム管理者は、学生に関する機密データへのアクセスを求める**データ リクエストをベンダーから**受け取ることがよくあります。こうしたリクエストが本部リーダーとの連絡のような確立された手順を迂回して行われると、本来なら拒否されるデータが共有されてしまうことがあります。

教育者は、個別教育計画（IEP）の作成や成績評価表の作成のために、**学業成績や行動記録などの PII** にアクセスする必要があります。学校が膨大な情報を保管している場合、すべてのアクセスを許可せずに必要最小限のアクセス権のみを付与することは困難です。

子供の肖像利用を制限するメディア許可フォームに家族が署名する場合に、教育者やスタッフが**生徒の写真や動画などの個人データ**を開示しないようにすることは、問題となる可能性があります。

マイクロソフトのソリューションの実例

マイクロソフトは、教育や運用に支障をきたすことなくデータを保護するセキュリティ ツールを提供しています。

課題	マイクロソフトのツール	実際の効果
SIS オペレーターが、サービス提供にアクセスを必要としないベンダーから学生データの共有を求められる。	Purview 情報バリア: Microsoft Teams、SharePoint、OneDrive でのグループやユーザー間の双方向コミュニケーションとコラボレーションを制限します。	ベンダーとのコミュニケーションや共同作業は制限されており、データの共有が妨げられ、既存のデータ保護が維持されます。
特別支援教育の教育者は、IEP を作成するために特定の生徒の学業および行動データにアクセスする必要がありますが、学校全体の全生徒のブローファイルへのアクセス権を持つべきではありません。	Purview 情報の保護: 機密情報がどこにあっても、どこを移動していても、検出、分類、保護します。	IT 担当者は、教育者がその役割に応じて適切なデータにアクセスできるように、すべての学生データへの一律のアクセス権を与えることなく、データを分類しラベル付けします。
校長が、生徒、教育者、家族の笑顔が写った最近の学校行事の写真をソーシャル メディアに投稿する。	Purview データ損失防止: 内部ユーザーが機密データをアクセス権限のないユーザーと不適切に共有することを防ぎます。	写真などの機密情報の不正な共有、使用、転送は、すべてのユーザー グループのプライバシーを維持するために制限されます。

ソリューションの実装方法

Microsoft Purview の使用を開始するには、まず、学区で最も機密性の高いデータの種類と、アクセス権が必要なスタッフの役割を特定します。次に、Purview のコア機能を確認し、適切な共有制限とデータ ラベルを適用します。

マイクロソフト ソリューションを探索する

インフラ全体にわたってデータのリスクを特定し、コンプライアンスを管理して、データ損失を防止する方法をご確認ください。

[➡ Microsoft Purview を探索する](#)

実例: プリンス・ウィリアム郡公立学校

バージニア州のプリンス・ウィリアム郡公立学校の管理者は、学区が支給したモバイル デバイスやノート PC を利用する生徒に、より安全なデジタル体験を提供するための施策を実施しました。学区は、Microsoft Purview 製品を活用して、目立たない方法でネットいじめや嫌がらせを特定し、生徒が共有した有害または不適切なコンテンツについてインサイトを得ることができました。これにより、学区は FERPA および CIPA の違反を検出し、特にインシデントが発生した場合や生徒が支援を必要とする際に、速やかに対応できるようになりました。

プリンス・ウィリアム郡公立学校が、Purview ファミリーの製品を活用して連邦規則の遵守を維持し、より安全なデジタルエクスペリエンスを生徒に提供した事例をご覧ください。

[➡ 事例を読む](#)

重要なポイント

Microsoft Purview は、アクセスと共有に明確な境界を設定することで、学校が機密データを保護し、プライバシー規制への準拠に対応するのに役立ちます。情報バリア、情報の保護、データ損失防止などの機能により、IT 部門は不正な開示を防ぎつつ、教育者や管理者が必要な情報にアクセスできるようにすることができます。

高等教育向けの実装シナリオ

データ セキュリティ

教育機関は、機密性の高い研究データ、医療データ、財務記録、入学情報、PII を保存、アクセス、利用しているため、データ セキュリティに関する特有の課題に直面しています。

課題の概要

助成金を活用した研究を行うには、他機関とのコラボレーションやコミュニケーションが必要です。スタッフは、承認されたグループ間で機密データを共有し、データの漏洩を防ぐ必要があります。

リーダーシップ チームは、他のグループと共有すべきでない**戦略的なガイダンスを含むファイル**を配布することがよくあります。機密情報へのアクセス制御は極めて重要です。

IT 担当者は、インフラのリスクと脆弱性を評価しています。内部データ侵害などのインシデントが発生した際、CTO はセキュリティ チームに**原因の分析と再発防止**を依頼します。その一方で、他の重要なタスクを管理する必要があります。

マイクロソフトのソリューションの実例

マイクロソフトは、研究、教育、運用を中断することなくデータを保護するセキュリティ ソリューションを提供します。

課題	マイクロソフトのツール	実際の効果
機密性の高い研究を行っている教員が、情報を公開せずに他大学と情報交換を行う必要がある。	Purview 情報バリア: Microsoft Teams、SharePoint、OneDrive でのグループやユーザー間の双方向コミュニケーションとコラボレーションを制限します。	機密性の高い研究に関するコミュニケーションは、認可されたグループに制限され、データ共有を防止するとともに既存のデータ保護を維持します。
教務担当副学長が、教職員やスタッフと共有すべきではない諮問委員会からのメモを学部長たちに配布する。	Purview 情報の保護: 機密情報がどこにあっても、どこを移動していても、検出、分類、保護します。	このメモは、学部長のみがファイルを開いて閲覧できるようにするため、機密扱いのラベルが付けられます。
新しく採用された非常勤講師が、教員専用データベースへのログイン方法を学生に示す PDF 手順書を Teams チャンネルに投稿する。	Purview データ損失防止: 内部ユーザーが機密データをアクセス権限のないユーザーと不適切に共有することを防ぎます。	この講師の行動によってアラートが発生し、今後 PDF や類似のデータ形式へのアクセスをブロックするポリシーの調整が促されます。
スタッフ メンバーが誤って戦略計画をメディアと共有した後、CTO が IT 担当者にシステム全体の脆弱性を洗い出すよう指示する。	Purview インサイダー リスク管理: 機関における悪意ある行為や不注意による行為を検出、調査し、対処することで、内部リスクを最小限に抑えます。	IT 担当者は、不正なデータ開示を検出し、キャンパス全体で同様のインシデントを防ぐためのポリシーに従って対処します。
大学のセキュリティ オペレーション センター (SOC) に所属する学生は、IT スタッフが部門の終日研修に参加している間、キャンパス全体の脅威を監視する必要があります。	Security Copilot: セキュリティと IT の日常業務のための生成 AI 搭載アシスタントにより、AI のスピードとスケールで機関を保護します。	学生は、AI を活用したサポートを活用して Microsoft Defender からのシグナルを分析し、システム全体の異常を検出します。IT スタッフが不在の間も、ステップバイステップの指示を利用して脅威を封じ込めることができます。

ソリューションの実装方法

Microsoft Purview の利用を開始するには、まず大学で最も機密性の高いデータの種類と、アクセス権が必要な教職員の役割を特定します。次に、Purview のコア機能を確認し、適切な共有制限とデータ ラベルを適用します。

マイクロソフト ソリューションを探索する

インフラ全体にわたってデータのリスクを特定し、コンプライアンスを管理して、データ損失を防止する方法をご確認ください。

➔ [Microsoft Purview を探索する](#)

見落とされがちな脅威を検出し、脅威に素早く対応し、AI 支援を活用してチームの専門性を強化する方法をご紹介します。

➔ [Security Copilot の詳細を確認する](#)

実例: オレゴン州立大学

革新的なセキュリティへの取り組みの一環として、オレゴン州立大学の管理者はインシデント発生後、セキュリティ態勢を強化するために Security Copilot を導入しました。Security Copilot の導入により、IT 担当者は脅威の検出と対応プロセスを自動化できるようになり、アナリストは付加価値の高い業務や高度な調査に集中できるようになりました。その結果、インシデントの早期解決、運用コストの削減、機密性の高い研究や学生データの保護強化が実現しました。

Security Copilot がオレゴン州立大学の脆弱性対策と、キャンパス全体でのよりプロアクティブなセキュリティ対策の実施にどのように貢献したかをご覧ください。

➔ [事例を読む](#)

重要なポイント

高等教育機関は、許可されているユーザー同士が安全に共同作業できるようにしながら、機密性の高い研究を保護し、データの共有を制限して、特権データを適切に保護する必要があります。Microsoft Purview と Security Copilot の導入により、大学はアクセス管理、データ漏洩防止、新たなリスクへの迅速な対応を、教育や研究活動を妨げずに実現できます。



Copilot プロンプト

当機関におけるインサイダー リスク管理の実装計画を作成してください。データ漏洩、危険なユーザーの行動、研究データの取り扱いに関するポリシー テンプレートを含めてください。教職員、スタッフ、大学院生助手に対して、責任あるデータ管理に関するガイダンスを提供してください。

ヒント

過去に発生した意図しない開示や、頻発するリスク行動 (個人のメールでの PDF の共有など) について記述してください。Copilot は、これらのパターンを使用して、より関連性の高いインサイダー リスクポリシーを作成できます。

データ コンプライアンス

大学が資金や契約を受けるためには、FERPA、HIPPA、GDPR などの、連邦規制で定められたデータ プライバシー、データ保持、データ ガバナンスの要件を満たす必要があります。

課題の概要

元社員が、教育機関を離れた後も**内部システムへのアクセスを維持している**ことがあります。大学は、法的リスクや評判の低下につながる不正な開示を防ぐために、機密データへのアクセス権が取り消されるようにする必要があります。

教職員は、教育機関のメール アドレスを使用して、**個人的または政治的見解を学生と共有**することがあります。大学は、学問の自由を尊重しつつ、公の論争を避けるために、公式なコミュニケーションに明確な境界を設ける必要があります。

研究チームは、**複雑なプロジェクトで国際的なパートナーと共同作業**することがよくあります。適切な許可なしに機密技術データを共有すると、連邦規制に違反し、将来の資金調達の機会を危険にさらす可能性があります。

マイクロソフトのソリューションの実例

マイクロソフトは、機関が規制要件を遵守できるよう支援する、コンプライアンス ソリューションを提供しています。

課題	マイクロソフトのツール	実際の効果
大学の保健センターが HIPAA コンプライアンスを確認せずにサードパーティの遠隔医療プラットフォームを統合した結果、学生の医療記録への不正アクセスが発生する。	Purview コンプライアンス マネージャー: マルチクラウド環境全体のコンプライアンスを自動的に評価し、管理します。	一元的に定義された施行ポリシーにより、医療記録へのアクセスが許可される前に、非準拠プラットフォームを検知します。
奨学金や助成金の詳細が記載された報告書を、財務支援担当者が誤って権限のない内部部署に送信してしまい、調査が開始される。	Purview インサイダー リスク管理: 機関における悪意ある行為や不注意による行為を検出、調査し、対処することで、内部リスクを最小限に抑えます。	自動化されたポリシーは、財務支援データが無許可の受信者と共有された場合にこれを検知し、アラートのトリガーやアクセス制限により、さらなる非準拠の開示を防止します。
教授が政治色が濃い発言を学生にメールで送信し、その内容が後に漏洩してメディアに取り上げられる。	Purview コミュニケーション コンプライアンス: 組織内で不適切な可能性のあるメッセージを検知、キャプチャ、対処するのを支援することで、コミュニケーション リスクを最小限に抑えます。	メッセージ内の政治的な発言は送信前に自動的に検出され、フラグ付けされるため、風評被害を最小限に抑えるための早期介入が可能になります。
教育省から大学に対し、学生への学費援助の支給に関する取り扱いについて、監査通知が届く。	Purview レコード管理: 規制、法務、および事業上重要な記録を管理します。	すべての学費援助データは、規制に沿った保持期間を持つレコードとしてラベル付けされ、監査や調査のためにデータが利用可能な状態に維持されます。
機関を退職した後も内部システムへのアクセス権を保持していた元社員が、機密性の高い生物医学研究データにアクセスし、漏洩する。	Purview 情報の保護: 機密情報がどこにあっても、どこを移動していても、検出、分類、保護します。	研究データはポリシーに従って自動的にラベル付けされ、暗号化されるため、組織に所属していない者は機関のデータにアクセスできません。
大学の医療センターの職員が、ある学生のメンタルヘルスに関する記録に本人の同意なしにアクセスし、教授と共有する。	Purview データ損失防止: 内部ユーザーが機密データをアクセス権限のないユーザーと不適切に共有することを防ぎます。	IT 担当者は、メンタルヘルスに関する記録がメールやチャットで不適切に共有されるのを防ぐため、自動化されたポリシーを設定し、HIPAA の遵守を支援します。
防衛テクノロジー プロジェクトに取り組んでいる研究チームが、SharePoint を通じて機密性の高い技術データを海外の協力者と共有したことで、不正なエクスポートの可能性が生じた。	Purview情報バリア: Microsoft Teams、SharePoint、OneDrive でのグループやユーザー間の双方向コミュニケーションとコラボレーションを制限します。	ポリシーは、国際組織とのファイルの共有やファイルへのリンクを制限し、極めて機密性の高いデータの外部流出を防ぐように構成されています。
IT 管理者が高額なソフトウェア ライセンスを誤って許可されていないユーザーに割り当てたことで、調達ポリシーとライセンス契約に違反した。	Purview 監査: セキュリティ イベント、フォレンジック調査、内部調査、コンプライアンス義務に対応します。	監査ログには、ライセンスの割り当て者、割り当て日時、ポリシー違反の有無が記録されており、是正措置やコンプライアンス要件のための文書化が可能になります。



ソリューションの実装方法

大学が、すべての Purview ソリューションを一度に実装する必要はありません。まずは主要なデータ ソースとコンプライアンスの優先事項を特定することから始めましょう。次に、Purview に搭載されたテンプレートとスキャン ツールを使用してリスクを評価し、部門をまたがった適用範囲を徐々に拡大します。

マイクロソフト ソリューションを探索する

インフラ全体にわたってデータのリスクを特定し、コンプライアンスを管理して、データ損失を防止する方法をご確認ください。

[➔ Microsoft Purview を探索する](#)

重要なポイント

データ コンプライアンスを維持するために、大学は機密性の高い機関データへのアクセスや共有を行うユーザーをプロアクティブに管理する必要があります。Microsoft Purview の活用により、教育機関はプライバシーの保護、データ漏洩の防止、複雑な学術環境全体での説明責任の確保を実現できます。



Copilot プロンプト

セキュリティ ツール (Defender、Purview、Sentinel、Entra ID) 向けの実装後のレポート フレームワークを作成してください。月次 KPI、リーダーシップ向けダッシュボード、改善マイルストーン、コンプライアンスや監査準備状況に関連する指標を含めてください。

ヒント

Copilot に、リーダーシップが最も重視する指標（稼働時間、コンプライアンス、インシデントの削減、監査結果）を伝えてください。Copilot ではこれらの優先順位に合わせてレポート フレームワークを調整します。

調査

学校や教育機関が Microsoft Security を利用し、AI を活用した脅威検出、ゼロ トラスト戦略、および IT を簡素化しレジリエンスを強化する接続されたツールを活用して、学生、スタッフ、データを保護している様子をご覧ください。

このセクションの内容

教育分野におけるマイクロソフトのセキュリティ: 展開からキャンパスへの効果まで

データと分析

学術および業界動向

用語集

次のステップのチェックリスト



教育分野におけるマイクロソフトのセキュリティ: 展開からキャンパスへの効果まで

Microsoft Security ソリューションの展開、利用、ベスト プラクティスに関する実践的なガイダンスをご覧ください。

自信を持って規制コンプライアンスを達成: ゼロ トラストでコンプライアンス プロセスを合理化し、将来の変化に備える

マイクロソフト、2025 年

教育機関がマイクロソフトの統合されたセキュリティ、コンプライアンス、ID ソリューションを活用して、変化するコンプライアンス要求に先んじて対応する方法をご紹介します。アクセスを継続的に検証し、機密データを保護し、組織全体のセキュリティ ツールを統合するゼロ トラスト戦略を導入しましょう。この最新のアプローチでは、断片化したレガシー システムを、より優れた可視性、制御、レジリエンスを提供する統合ソリューションに置き換えることで、規制コンプライアンスを簡素化します。

[リソースにアクセスする](#)

意思決定者向けの包括的セキュリティ ガイド: 現在の組織を保護するための主な戦略

マイクロソフト、2025 年

ゼロ トラスト フレームワーク上に構築された、マイクロソフトの包括的な統合アプローチを導入することで、ユーザー、デバイス、データ、アプリケーション全体でアクセスを継続的に検証し、セキュリティを一元化しましょう。この戦略では、ツールを統合し、デジタル環境全体の保護を合理化することで、運用の簡素化、リスクの軽減、セキュリティ投資の価値の最大化を実現します。

[リソースにアクセスする](#)

セキュリティ態勢を迅速に最新化: ゼロ トラスト フレームワークを使用して、社員、パートナー、顧客、その他の関係者との信頼を築く

マイクロソフト、2025 年

共有戦略に沿ってリーダーシップを調整し、リスクを優先的に管理し、ゼロ トラストの原則を体系的に適用して防御を強化することで、セキュリティ態勢を強化する方法を説明します。この eBook は、組織が自信を持って脅威に対応し、全体的なセキュリティ態勢を強化して、進捗状況が測定可能で意思決定者に効果的に伝達されるようにする上で役立ちます。

[リソースにアクセスする](#)

最も機密性の高いデータを保護: ゼロ トラスト セキュリティ フレームワークで重要な資産を保護する

マイクロソフト、2025 年

ゼロ トラスト戦略を実装し、自動ラベル付け、暗号化、アクセス制御を用いてクラウド、オンプレミス、モバイルなどすべての環境で機密データを特定、分類、保護する方法をご紹介します。この eBook は、セキュリティの強化、内部と外部からの脅威の低減、コンプライアンスの確保を支援しながら、シームレスなコラボレーションと生産性向上を実現するのに役立ちます。

[リソースにアクセスする](#)

どこにいても安全に作業: ゼロ トラスト アプローチでデータ セキュリティを強化 する

マイクロソフト、2025 年

すべてのアクセス要求を検証し、エンドポイントを保護して、強力な ID 管理を適用するゼロ トラスト フレームワークを導入することで、セキュアなリモートおよびハイブリッド ワーク エクスペリエンスを提供しましょう。これによって、サイバー攻撃のリスクを軽減し、柔軟な業務環境をサポートして、生産性を損なうことなくデータとデバイスのセキュリティを確保できます。

[リソースにアクセスする](#)

生徒向け SOC: 実装ガイド

マイクロソフト、2025 年

実践的なエクスペリエンスや業界認定の取得、ゼロ トラストなどの戦略との連携を通じて、SOC がいかに労働力の準備と組織のセキュリティの強化に貢献するかをご紹介します。

[リソースにアクセスする](#)

AI のセキュリティとゼロ トラスト: アジャイルなビジネスのためのアジャイルな セキュリティ

マイクロソフト、2024 年

AI システム内でアクセスを検証し、特権を制限するゼロ トラスト セキュリティ フレームワークを実装することで、データ、アプリケーション、インフラを保護しましょう。AI システムへのゼロ トラスト アプローチは、データのプライバシーを強化し、規制コンプライアンスに対応するため、組織は AI による変革を実現できます。

[リソースにアクセスする](#)

一般的な攻撃と、マイクロソフトのゼロ トラスト機能が組織を保護する方法

マイクロソフト、2024 年

セキュリティで保護されていないシステムにおいて、サイバー犯罪者が ID、デバイス、ネットワーク攻撃をどのように開始するかを理解し、Microsoft Security ソリューションとゼロ トラスト アプローチによってどのようにデータ、エンドポイント、重要なインフラを保護できるかを学びましょう。

[リソースにアクセスする](#)

Cyber Signals 第 8 号 | 包囲された教育: サイバー犯罪者が学校を標的にする手法

マイクロソフト、2024 年

オープンなデジタル環境、個人デバイスの広範な利用、限られたセキュリティ リソースが、初等中等教育の学校や高等教育機関へのサイバー攻撃につながる仕組みを理解しましょう。ゼロ トラストのようなプロアクティブな戦略を採用し、ネットワークやデバイス全体の可視性と制御を強化することで、学校や教育機関は機密データをより安全に保護し、ますます巧妙化する脅威による混乱のリスクを低減できます。

[リソースにアクセスする](#)

ゼロ トラストの基本ガイド: AI を活用し たセキュリティへのリーダーシップのア プローチ

マイクロソフト、2024 年

マイクロソフトのゼロ トラスト アーキテクチャを応用し、ID、データ、アプリ、エンドポイント、ネットワーク、インフラ、AI にわたる保護をアダプティブ アクセスと継続的な脅威評価によって体系的に整理することで、エンタープライズ セキュリティを強化する方法を学びます。この構造化されたアプローチにより、リスクを軽減し、コンプライアンスを高め、セキュアなイノベーションを実現するとともに、組織全体において展開と管理を簡素化できます。

[リソースにアクセスする](#)

マイクロソフト デジタル防衛レポート 2024 年

マイクロソフト、2024 年

進化する脅威の状況、戦略的にサイバーセキュリティに取り組む方法、AI 導入に伴う新たなセキュリティ課題について探ります。このレポートには、毎日 78 兆を超えるセキュリティ シグナルを分析する Microsoft 脅威インテリジェンスのデータと統計情報が含まれています。

[リソースにアクセスする](#)

Microsoft Security ソリューションが学校や教育機関にどのような定量化可能なメリットをもたらすかをご覧ください。

The Forrester Wave: Zero Trust Platforms、2025 年第 3 四半期

Forrester、2025 年。

マイクロソフトの戦略的ロードマップ、製品の機能、顧客からのフィードバックが、Forrester の調査においてゼロ トラスト プラットフォーム プロバイダーのリーダーへと導いた理由をご確認ください。本レポートは、マイクロソフトが中核的なセキュリティ製品全体で ID 管理を強化し、Microsoft Security Copilot によって AI で強化された保護を組織にもたらす取り組みに焦点を当てています。

[リソースにアクセスする](#)

The Total Economic Impact of Microsoft Sentinel

Forrester、2024 年

時代遅れのシステムを Microsoft Sentinel に置き換えることで、セキュリティ運用を最新化するメリットをご確認ください。Microsoft Sentinel は、AI と自動化を活用し、脅威の検出と対応をより迅速かつ効率的に行うクラウドベースのプラットフォームです。この Forrester 調査では、234% の投資収益率、大幅なコスト削減、誤検知の減少、チームの生産性向上が確認されました。その結果、Sentinel は、スケーラブルでセキュアかつ費用対効果の高いサイバーセキュリティ ソリューションを求める教育リーダーにとって、戦略的なツールとなっています。

[リソースにアクセスする](#)

New technology: The projected Total Economic Impact of Microsoft Security Copilot

Forrester、2024 年

Microsoft Security Copilot が生成 AI を活用して脅威の検出、調査、対応を合理化し、セキュリティ運用において測定可能な改善をもたらす仕組みをご覧ください。本調査では、SecOps タスクの生産性が平均 46% 上昇し、SecOps の集約によりコスト効率が向上して、ROI が 348% に達することが予測されています。これらの結果は、マイクロソフトの Security Copilot のような AI 主導のツールをサイバーセキュリティ戦略に統合することが、保護の強化と労働力不足への対応の両面で重要であることを示しています。

[リソースにアクセスする](#)

The Total Economic Impact of Microsoft Security

Forrester、2023 年

Microsoft Security が SIEM、コンプライアンス、ID 管理ソリューションを通じてサイバーセキュリティの効率性とリスク軽減をどのように改善しているかをご覧ください。調査の結果、侵害発生の可能性が 72% 減少し、ライセンスコストと運用コストが 25% 削減され、IT チームとセキュリティ チームの効率が 50% 向上したことが示されました。

[リソースにアクセスする](#)

The Total Economic Impact of Microsoft SIEM and XDR

Forrester、2022 年

マイクロソフトの SIEM および XDR ソリューションを活用して、脅威への対応時間を短縮し、可視性を向上させ、ベンダー統合を支援する方法をご覧ください。調査の結果、脅威の調査にかかる時間が 65% 削減され、対応時間が 88% 短縮され、ベンダーと管理を統合することで年間約 160 万ドルを節約できることが明らかになりました。

[リソースにアクセスする](#)

初等中等教育と高等教育の教室における堅牢なセキュリティ、コンプライアンス、プライバシー保護の重要性について学びましょう。

ゼロトラスト アーキテクチャを実装: 概要 レベルの文書

アメリカ国立標準技術研究所 (NIST: National Institute of Standards and Technology)、2024 年

オンプレミス環境とマルチクラウド環境にわたってエンタープライズ リソースへのセキュアで承認されたアクセスを実現する、ゼロ トラスト アーキテクチャ (ZTA) の実装方法を学びましょう。このアーキテクチャにより、ハイブリッド ワーカーは組織のミッションを支援するために、いつでも、どこからでも、どのデバイスからでもリソースにアクセスできます。NIST Special Publication (SP) 800-207「ゼロ トラスト アーキテクチャ」で概説されている概念と原則に沿って ZTA を実装する方法をご確認ください。

[リソースにアクセスする](#)

The NIST Cybersecurity Framework (CSF) 2.0

アメリカ国立標準技術研究所 (NIST: National Institute of Standards and Technology)、2024 年

NIST Cybersecurity Framework (CSF) 2.0 で、サイバーセキュリティ リスクを管理する方法をご確認ください。CSF は、学校や教育機関がサイバーセキュリティへの取り組みをより深く理解および評価し、優先順位を付け、伝達するために活用できる、高水準のサイバーセキュリティ標準と成果の分類法を提供します。

[リソースにアクセスする](#)

2024 Educause Horizon Report: Cybersecurity and Privacy Edition

Educause、2024 年

急速な技術的および地政学的な変化の中で、高等教育機関がサイバーセキュリティとプライバシーを強化する方法を探ります。この報告書は、ゼロ トラストなどのフレームワークの採用、セキュリティ意識向上トレーニングの実施、リスク管理の強化が、教育機関のデータと学生のプライバシーを保護するために重要であることを強調しています。

[リソースにアクセスする](#)

First Annual Generative AI Study: Business Rewards vs. Security Risks

Information Security Media Group (ISMG)、2023 年

リーダーと最高情報セキュリティ責任者 (CISO) の両者の視点から、生成 AI のビジネス チャンス、リスク、そしてその影響についての貴重なインサイトを得ることができます。この調査は、さまざまな業界やセクターにおけるこれら主要な役割の視点を包括的に捉えた概観を提供します。

[リソースにアクセスする](#)

Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats

Cybersecurity and Infrastructure Security Agency (CISA)、
2023 年

初等中等教育機関が直面しているサイバーセキュリティ リスクと、人々やデータを保護するための推奨事項の適用方法を理解しましょう。この報告書の主なポイントは、高い効果のあるセキュリティ プロトコルの実装、学校の最優先事項としてセキュリティを位置づけること、地方、地域、国レベルの機関と連携してリスクを低減することです。

[リソースにアクセスする](#)

Implementing Phishing-Resistant MFA

Cybersecurity and Infrastructure Security Agency (CISA)、
2022 年

多要素認証 (MFA) を利用することで、サイバー犯罪者が侵害された認証情報を使ってデータ、ネットワーク、情報システムにアクセスするリスクを低減する重要性について学びます。フィッシング耐性 MFA およびセキュリティに対するゼロ トラスト アプローチの実装方法に関するガイダンスに従ってください。

[リソースにアクセスする](#)

Cybersecurity Incident Planning for Institutes of Higher Education

米国教育省、日付なし

高等教育機関向けの NIST CSF に準拠したリスク管理のベスト プラクティスを通じて、セキュリティ態勢を改善しましょう。ネットワークへの被害を抑え、緩和を促進し、法執行機関による攻撃者の特定と逮捕能力を強化するために、インシデント対応計画を整備する重要性について学ぶことができます。

[リソースにアクセスする](#)

用語集

教育分野のサイバーセキュリティに関して使用される一般的な用語をご確認ください。その他の用語や定義については、National Initiative for Cybersecurity Careers and Studies のサイトにアクセスしてください。

アクセス: システムとの通信や相互作用、システム・リソースを利用した情報処理、システム内の情報に関するナレッジの取得、システムの構成要素や機能の制御を行う能力や手段

認証: ユーザー、プロセス、あるいはデバイスの ID やその他の属性を検証するプロセス

バックドア: コンピューター システム、ネットワーク、ソフトウェア アプリケーションにおいて、許可されているユーザーまたは許可されていないユーザーが通常のセキュリティ対策を迂回し、高度なユーザーアクセス権限 (root 権限) を取得するあらゆる手法

侵害: 情報システムの機密性、完全性、可用性に対する重大な損失、あるいは運用システムの安全性やレジリエンスに対する深刻な影響が、不正利用に起因して生じること

分散型サービス拒否 (DDoS): 攻撃者が標的に対して大量のインターネット トラフィックを送り込み、ユーザーがオンライン サービスやサイトにアクセスできないようにするサイバー犯罪

暗号化: 権限のないユーザーには容易に理解できない形式にデータを変換するプロセス

ファイアウォール: ネットワーク トラフィックをアクセスの許可・不許可に関するルールに基づいて制限する機器またはソフトウェア

インシデント対応: インシデントの短期的かつ直接的な影響に対処する活動 (短期的な回復も含む)

インシデント対応計画: サイバー インシデントを検出し、対応するために事前に策定し、文書化された一連の手順

インサイダー脅威: 組織のリソースに対して認可されたアクセス権や知識を持つ人物が、それを利用して損害を与えるリスクのこと

マルウェア: 不正な機能やプロセスを実行することで、システムの動作を損なうソフトウェア

軽減策: 望ましくない事象の発生可能性を低減し、その影響を緩和するために 1 つ以上のセキュリティ対策を活用すること

多要素認証 (MFA): パスワード、PIN、指紋、顔認識など複数の検証方法を用いて、ユーザーの本人確認 (認証) を行うプロセス

パスキー: 公開鍵暗号方式と指紋認証・顔認識などの生体認証やデバイスの PIN を組み合わせて、アカウント所有者の本人確認を行う多要素認証の一形態

パスワードレス: ユーザーがパスワードやその他の知識ベースの秘密情報を入力せずにコンピューター システムにサインインできる認証方法

フィッシング: ユーザーを騙して、パスワードや個人を特定できる情報 (PII) などの個人情報を漏らさせ、機密データを盗んだり損傷したりするために使われるサイバー攻撃

プライバシー: エンティティに関する特定の情報の機密性とアクセスが保護されるという保証

ランサムウェア: コンピューター、サーバー、またはデバイス上のファイルやフォルダーを破壊または暗号化し、データの復号と引き換えに金銭を要求する、マルウェアやフィッシングによるサイバーセキュリティ攻撃の一種

レッド チーム: 企業のサイバーセキュリティ態勢において、潜在的な敵の攻撃または悪用能力を模倣するために認可され、組織されたグループ。

レジリエンス: 困難な状況下でも重要な運用能力を維持し、迅速に業務を回復する能力

リスク: 特定の脅威が特定の脆弱性を悪用する可能性に基づいて決まる、インシデントやイベント、発生した出来事に起因する望ましくない結果または不利益が生じる可能性

リスク評価: 業務、資産、または個人に対するリスクを特定し、評価し、優先順位付けするプロセス

SecOps (セキュリティ運用): IT セキュリティ チームと IT 運用チームの連携やコミュニケーションを強化するために、IT マネージャーが 導入する方法論

SIEM (セキュリティ情報およびイベント管理): 業務が中断される前に脅威を検出するのに役立つセキュリティ ソリューション

ソーシャル エンジニアリング: 欺瞞や心理的トリック、説得、搾取を用いてユーザーを誘導し、誤って機密情報やデータを漏洩させる行為

スパム: 電子メッセージング システムを悪用し、大量の迷惑メッセージを無差別に送信すること

脅威: 不正アクセス、破壊、開示、変更、サービス拒否によって、運用、資産、個人に悪影響を及ぼす可能性のあるイベントまたは状況

脅威アクター (サイバー犯罪者): システムの侵害、データの窃取、サービスの妨害を目的として、有害なデジタル活動を行う個人またはグループ

脆弱性: セキュリティ システム、セキュリティ手順、内部統制、または実装の中に存在し、脅威によって悪用または引き起こされる可能性のある弱点

XDR (拡張検出および応答): 組織のエンドポイント、ハイブリッド ID、クラウド アプリケーションとワークロード、メール、データ ストアなど、より幅広いドメインにわたり、検出、調査、対応の機能を統合するサイバーセキュリティへのアプローチ

ゼロ トラスト: すべてが脅威であることを前提とするサイバーセキュリティのアプローチ。ゼロトラストは、明示的な検証、最小限の特権アクセスの使用、不正侵入の想定という 3 つの原則に従います。

次のステップの チェックリスト

- ゼロ トラストに関する研究を確認し、ID、エンドポイント、アプリ、インフラ、データ、ネットワークにわたって 3 つの基本原則をどのように適用できるかを検討します。
- Microsoft Security ソリューションの定量的なメリットを IT 担当者、財務意思決定者、リーダーと共有します。
- CISA、NIST、米国教育省などの機関が発表している推奨事項やガイドラインを確認します。



マイクロソフトとマイクロソフトのロゴは、マイクロソフトまたはその子会社の商標です。その他の名称およびブランドは、他者の財産として権利が主張されている場合があります。