



レポート

教育機関のランサムウェアの現状 2026 年版

過去 1 年間にランサムウェア攻撃を受けた 17 か国の教育機関に所属する、IT およびサイバーセキュリティリーダー 226 人を対象とした独自調査の結果。

はじめに

ソフォスの「教育機関のランサムウェアの現状」第 6 版をご覧くださいありがとうございます。このレポートでは、2026 年における初等中等教育機関 (K-12、小学校、中学校など、通常 18 歳未満の生徒を対象) および高等教育機関 (大学、カレッジ、同等の脅威機関など、通常 18 歳以上の生徒を対象) についてのランサムウェアの現状について明らかにしています。

今年のレポートは、攻撃が環境のどこから始まるのか、多要素認証 (MFA) とファイアウォールの防御的役割、アイデンティティ攻撃とランサムウェアの関連性など、これまで未踏であった分野にも新たな光を当てています。

過去 1 年間にランサムウェアの被害を受けた教育機関に所属する、226 名の IT およびサイバーセキュリティのリーダー (初等中等教育機関の 131 名、高等教育機関の 95 名) の実体験に基づいて、以下について独自の洞察を提供します。

- 攻撃と防御の方法
- データ暗号化と復旧
- 要求された身代金額と支払った身代金
- ビジネスと人間への影響

注: 本レポート全体を通して、「調査全体」とは、調査された全業界の回答者からの結果を指します。教育機関の回答者 226 人は、15 の業界にわたる計 2,158 人の回答者で構成される調査対象者全体の一部です。

調査について

本レポートは、ソフォスが委託した、特定のベンダーに依存しない立場から調査した結果に基づいています。この調査では、組織が経験したランサムウェア攻撃およびアイデンティティベースの侵害について質問し、身代金を支払った組織の割合、復旧コスト、復旧期間など、さまざまな指標を前年比で追跡しました。回答は 2026 年 1 月から 3 月にかけて収集され、回答者組織の過去 12 か月間の体験に基づいています。

17 か国の組織と 15 の業界組織から回答を得ており、これらの組織は、公共部門および民間部門の幅広い業界に所属しています。また、従業員数 100 人から 5,000 人までの企業を対象に、企業規模の分布が偏らないようサンプリングされており、その構成比は調査開始から 6 年間にわたり一貫して維持されています。財務データはすべて米ドルで表示されています。

主な調査結果

- 特にメールを介したアイデンティティ攻撃が教育分野で高かった。
 - 高等教育機関の 77% と初等中等教育機関の 71% の被害者が、ランサムウェア攻撃が自らにとって最も重大なアイデンティティ攻撃でもあったと確認しており、これは全業界の調査全体の 67% を上回っています。
 - 悪意のあるメールは、初等中等教育機関 (31%) および高等教育機関 (29%) におけるランサムウェア攻撃の主要な技術的根本原因でした。
 - 認証情報などを悪用するアイデンティティベースの攻撃手法 (悪意のあるメール、フィッシング、認証情報の侵害、ブルートフォース攻撃など) は、教育分野で発生した攻撃の 85% の起点となっており、全業界の 79% を上回りました。
- 教育分野における業務上の弱点は、調査全体 (全業界) を上回りました。
 - 高等教育機関で特に顕著だった課題は、専門知識でした。53% が、攻撃をすばやく検知して阻止するためのスキルが不足していると回答しました。調査全体では 35% でした。
 - 初等中等教育機関における運用上の主な根本原因は、人為的ミス (52%)、保護対策の不足 (47%)、認識していなかったセキュリティギャップ (42%)、人材や能力の不足 (41%) でした。
- ランサムウェア攻撃による暗号化率は初等中等教育機関で急増した。
 - 初等中等教育機関のデータ暗号化率は 2025 年の 29% から 2026 年には 61% へと 2 倍以上に増加しました。
 - 教育業界への攻撃の 58% で結果としてデータが暗号化されました。これは調査全体の 56% に近い値です。
- 教育機関は、データを復元する場合、バックアップに大きく依存していた。
 - 初等中等教育機関の 77% が、バックアップから暗号化されたデータを復元していました。これは、調査全体の暗号化率 66% を上回っていました。
 - 高等教育機関の 69% もバックアップを使用してデータを復元していました。
- 教育分野では、身代金の支払額は調査全体より少なかった一方、500 万ドル以上の身代金を支払ったケースが多く見られた。
 - 教育機関の身代金要求額 (中央値) は、77 万 5,200 ドルであり、調査対象全体の 69 万 8,000 ドルよりも高かったが、身代金支払額 (中央値) は 51 万 5,000 ドルとなり、調査対象全体の 76 万 9,000 ドルよりも低くなりました。
 - 教育機関の身代金要求額は 2 年連続で減少しましたが、支払額は 2025 年の報告書から 2026 年にかけて 15,000 ドル増加しました。
 - 教育機関では、500 万ドル以上の身代金を支払う可能性が高く、23% に上りました (調査全体では 16%)。
- 教育機関がランサムウェア攻撃による影響を復旧するには、より多くの費用がかかり、より長い時間を要している。
 - 教育分野における平均復旧費用は 226 万ドルに達し、調査全体の 170 万ドルを上回りました。
 - 教育分野の回復費用は、2025 年の報告書以降、166 万ドルから 226 万ドルに増加し、高等教育機関の復旧費用は 100 万ドル以上増加しました。
 - 教育機関の 26% がランサムウェア攻撃から完全に復旧するまでに 1 ~ 3 か月を要しており、これは全業界の 14% の約 2 倍に相当します。
 - 初等中等教育機関は、復旧が長期化した割合が最も高くなりました。31% が復旧までに 1 か月以上を要しており、これは他のどの業界よりも高い割合でした。
- セキュリティチームへの人的負担が増大した。
 - 高等教育チームの 53% が経営幹部からのプレッシャーが増加したと報告しており、これは全業界の 40% と比較して高くなっています。
 - 教育チームの約 39% が、ストレスやメンタルヘルスの問題による職員の欠勤を報告しており、これは全業界の 29% と比較して高い数値です。

攻撃と防御の方法

攻撃の根本原因

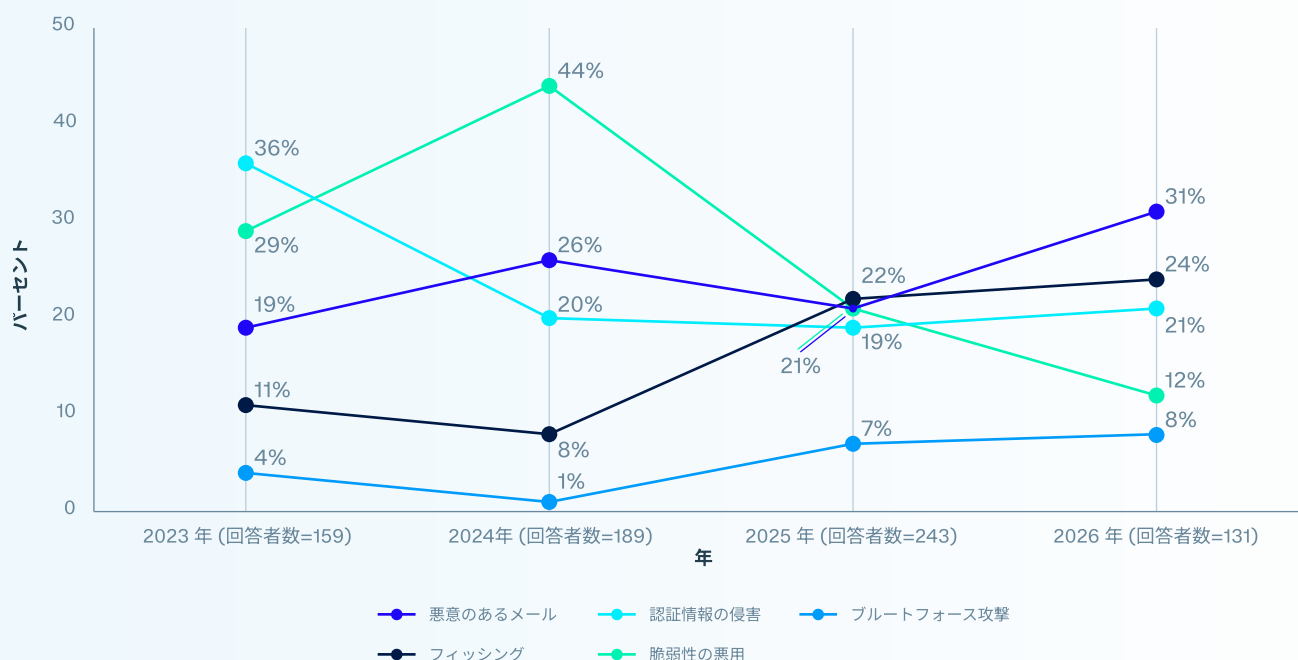
教育機関における今年のデータは、全業界で見られるのと同じ傾向を反映しており、アイデンティティベースの攻撃が増加しています。

悪意のあるメールが初等中等教育機関における最も一般的な技術的根本原因 (31%) であり、フィッシング (24%)、認証情報の侵害 (21%) が続いています。脆弱性の悪用は 12% に低下しており、調査全体 (全業界) でも 18% まで減少した傾向と一致しています。

85%

認証情報などを悪用するアイデンティティベースの攻撃手法 (悪意のあるメール、フィッシング、認証情報の侵害、ブルートフォース攻撃など) を起点とした教育機関への攻撃の割合は、調査全体の 79% を超えています。

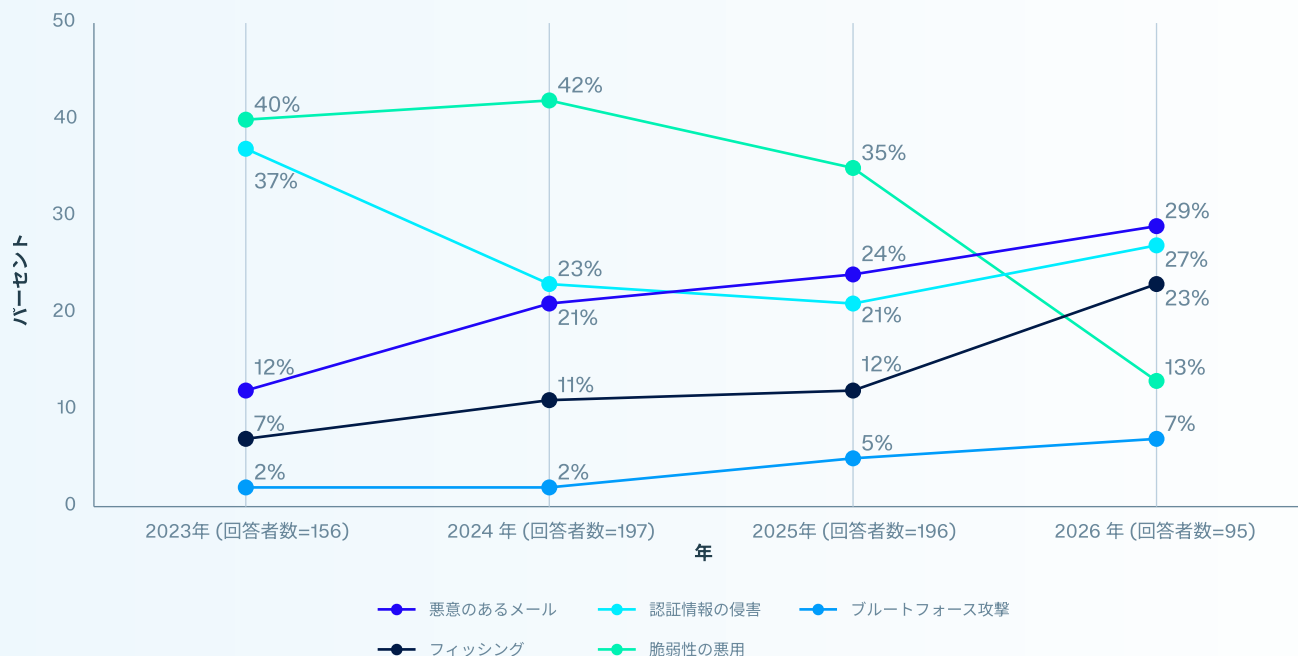
ランサムウェア攻撃の技術的な根本原因 2023 年～ 2026 年：初等中等教育機関



昨年受けたランサムウェア攻撃の根本原因を把握していますか？ダウンロードおよび「わからない」は、見やすさを考慮してグラフから除外しています。パーセンテージは 100% にならない場合があります。回答者数を図内に記載。

高等教育機関が報告した脆弱性の悪用も減少しています。この攻撃ベクトルは 2025 年には 35% でしたが、2026 年のレポートでは 13% まで低下しました。悪意のあるメール (29%) と認証情報の侵害 (27%) がほぼ同率で主要な原因となっており、フィッシング (23%) がそれに続いています。初等中等教育機関と高等教育機関の両方が、メールベースの攻撃を主な原因として報告しており、これは悪意のあるメール (26%) とフィッシング (24%) を合わせて全インシデントの半数を占めるという調査全体の結果と一致しています。

ランサムウェア攻撃の技術的な根本原因 2023 年～ 2026 年：高等専門教育機関

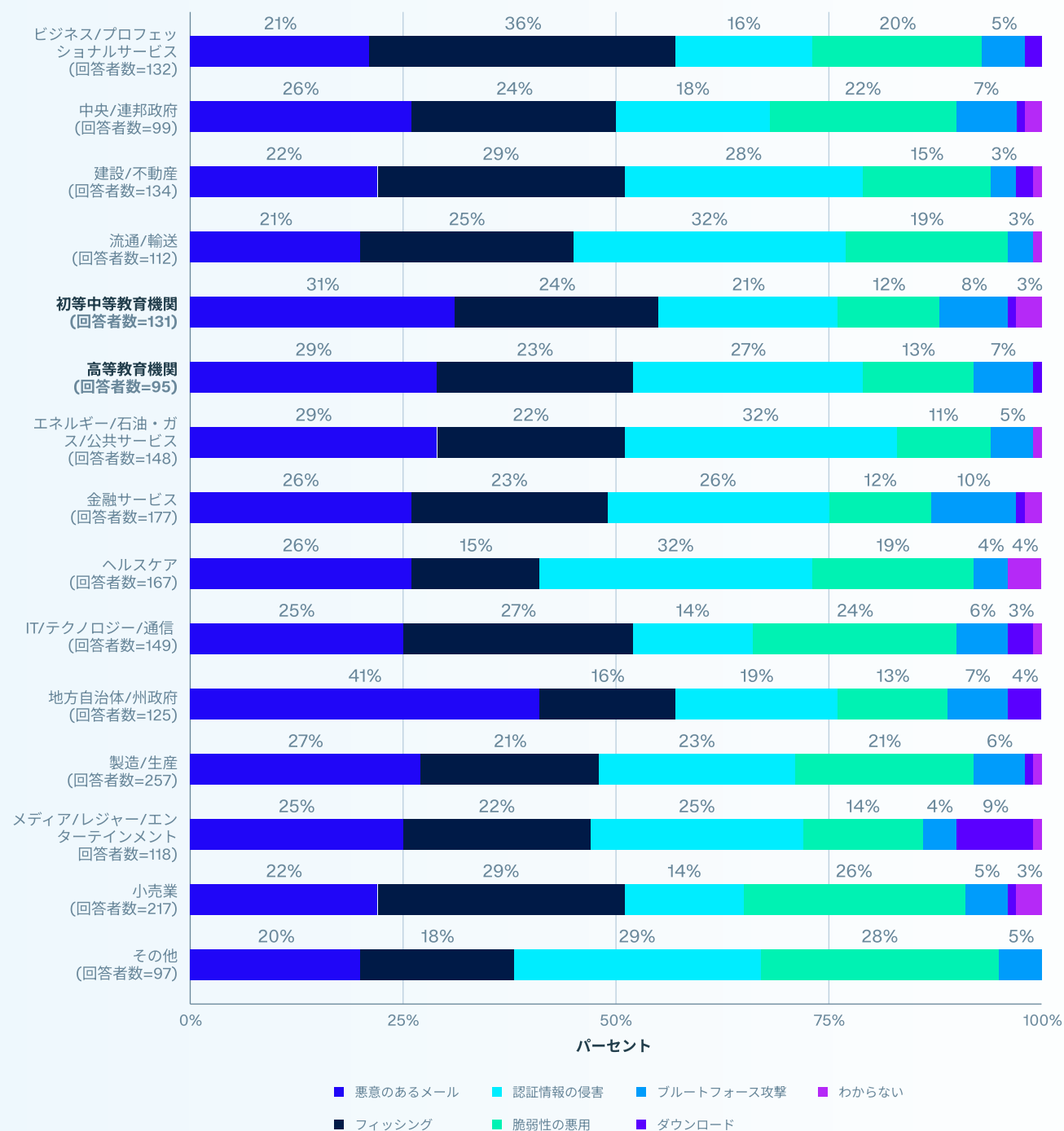


昨年受けたランサムウェア攻撃の根本原因を把握していますか？ダウンロードおよび「わからない」は、見やすさを考慮してグラフから除外しています。パーセンテージは 100% にならない場合があります。回答者数を図内に記載。

全体として、認証情報などを悪用するアイデンティティベースの攻撃手法 (悪意のあるメール、フィッシング、認証情報の侵害、ブルートフォース攻撃など) が教育機関への攻撃の 85% を占めています。これは、調査全体の 79% を上回っています。高等教育機関は 86% で最高であり、初等中等教育機関は 84% でそれに続いています。言い換えれば、教育機関に対する攻撃の 7 件うち 6 件がアイデンティティベースの攻撃を起点としています。これは、アイデンティティセキュリティをこの業界の防御において中核に据える必要があることを示しています。

教育分野でも、業界を問わず見られる、メールを起点とする攻撃の増加と、脆弱性の悪用に関する報告の減少という傾向が見られます。しかし、**ソフォスの専門家は、組織が最先端の AI によって発見された脆弱性へのパッチ適用に追いつけず、脆弱性の悪用が再び増加すると予想しています。**

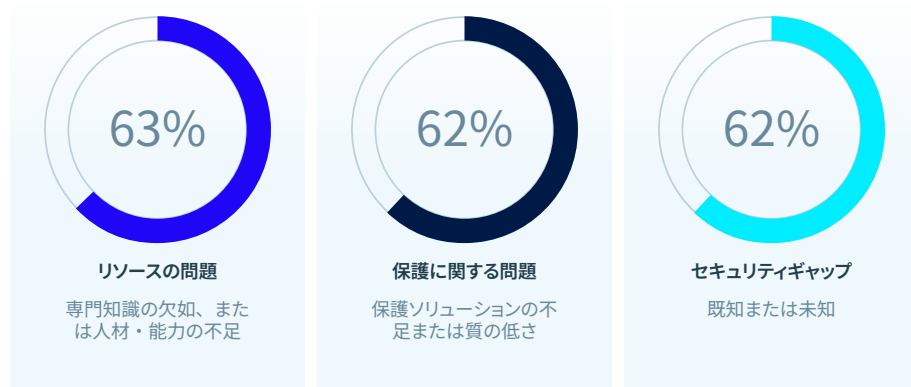
業界別技術的根本原因（2026 年）



昨年受けたランサムウェア攻撃の根本原因を把握していますか？回答者数を図内に記載。

組織が脆弱になった要因

教育機関は、保護対策、リソース、セキュリティギャップに関して幅広い課題を指摘しています。3つの統合カテゴリ全体で、リソースの問題（人材やスキルの不足）が教育機関の63%によって挙げられ、次いで保護対策の問題（62%）、セキュリティのギャップ（62%）が挙げられました。



自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 回答者数 = 226 集計結果。

教育分野全体では、既知のセキュリティギャップを除くほぼすべての運用面の根本原因について、調査全体よりも高い割合が報告されました。初等中等教育機関と高等教育機関に分けると、2つの異なる弱点が見えてきます。

高等教育機関で特に顕著だった弱点は専門知識でした。53%が、攻撃をすばやく検知して阻止するためのスキルや知識が不足していると回答しました。調査全体では35%で、18%の差があり、これは最大の差となりました。

初等中等教育機関の弱点は、能力とツールに集中していました。人為的ミスは、初等中等教育機関の52%（全業界では35%）によって挙げられ、保護対策の欠如は47%、人材や能力の不足は41%によって挙げられました。

運用上の根本原因：初等中等教育機関および高等教育機関と全業界の比較

運用上の根本原因	初等中等教育機関 (回答者数 =131)	高等教育機関 (回答者数 =95)	全業界 (回答者数 =2,158)
保護対策の不足	47%	36%	36%
不明なセキュリティギャップ	42%	38%	36%
既知のセキュリティギャップ	33%	35%	36%
人材や能力の不足	41%	37%	35%
人為的ミス	52%	36%	35%
専門知識の欠如	33%	53%	35%
品質の低い保護機能	38%	39%	33%

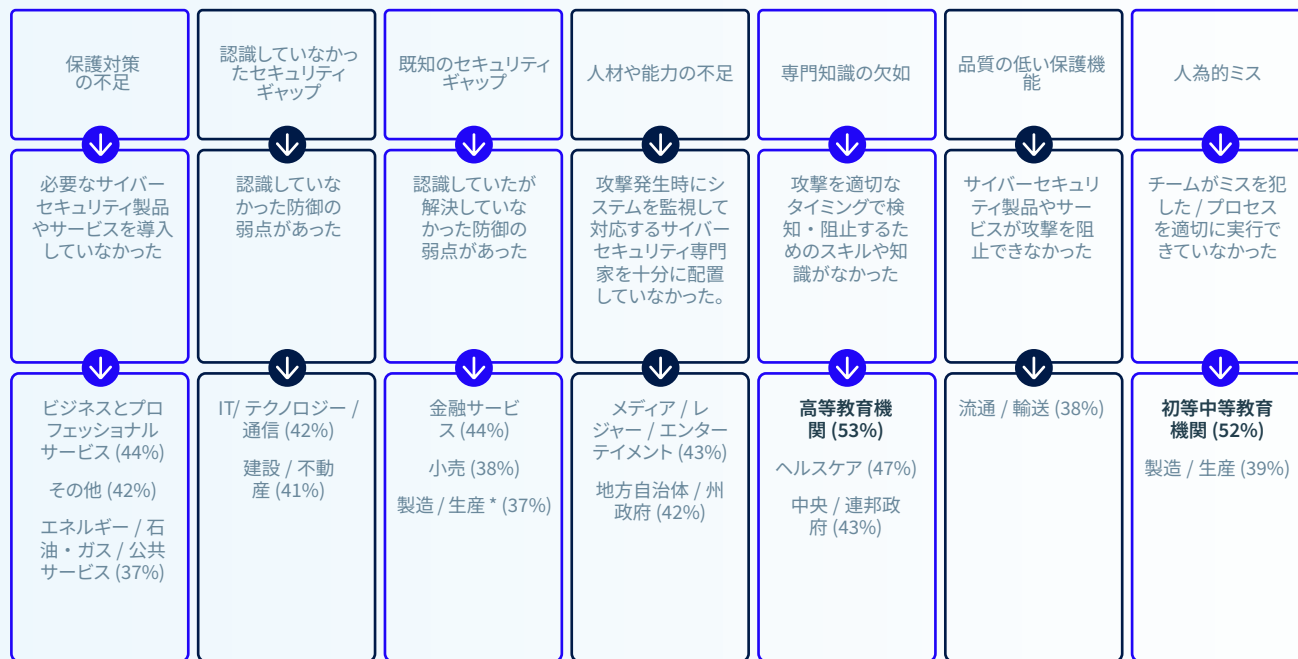
自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 複数回答可。回答者数を図内に記載。

53%

攻撃をすばやく検知して阻止するためのスキルや知識が不足していると回答した高等教育機関の被害組織は、調査全体を18%上回り、これが高等教育機関における最大の弱点となりました。

他の業界と比較すると、教育分野では、保護対策と専門知識の不足が課題となっています。下記の表は、各業界が最も挙げた運用上の根本原因の列を示しています。

業界別のランサムウェア攻撃における運用面の根本原因



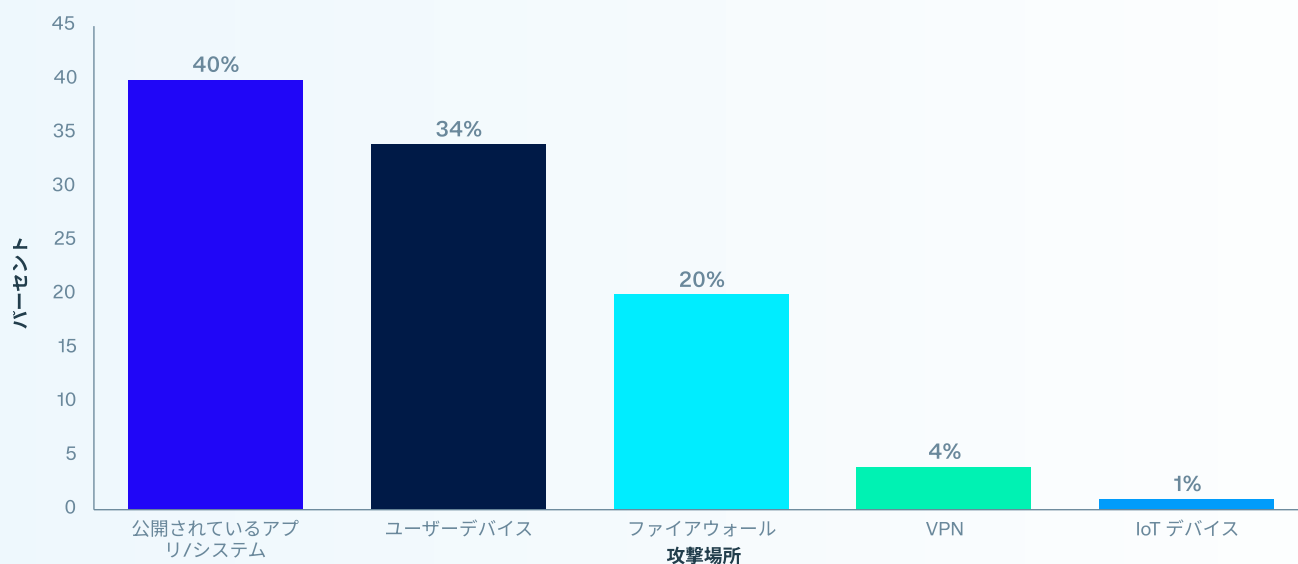
自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？複数回答可。
複数の根本原因で同率となった業界には、アスタリスク(*)を付けています。回答者数=2,158

攻撃の開始場所

今年の新しい調査では、特に脆弱性の悪用、認証情報の侵害、またはブルートフォース攻撃から始まったインシデントに関して、攻撃が環境のどこで始まったかという質問が追加されています。

教育分野において、露出したアプリケーションおよびシステムが最も一般的な侵入経路(40%)であり、続いてユーザーデバイス(34%)およびファイアウォール(20%)となっています。これらの数値は調査全体の結果(それぞれ38%、30%、21%)とほぼ一致しており、この点では教育分野に有意な差は見られません。

ランサムウェア攻撃の起点となった場所：教育機関全体



根本原因は、悪用された脆弱性、認証情報の侵害、またはブルートフォース攻撃であると述べました。この問題は自社環境のどこで起こりましたか？
高等教育機関と初等中等教育機関を合わせた全体。回答者数 = 99

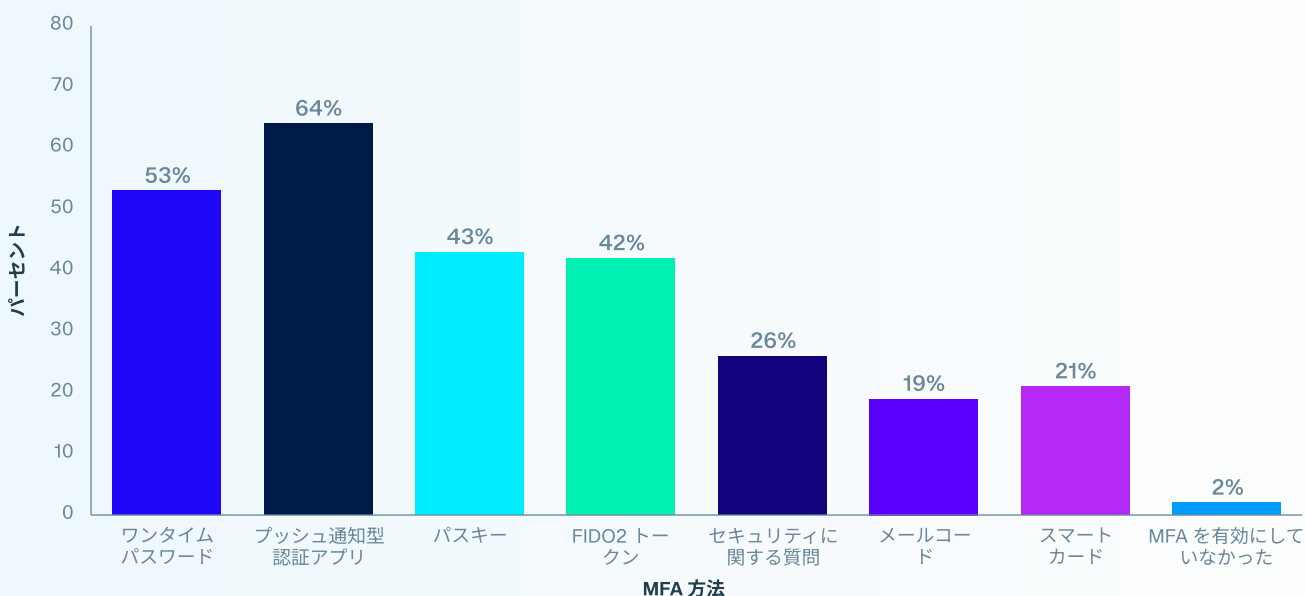
多要素認証 (MFA) の役割

また、侵害された認証情報から攻撃が始まった教育機関における当時の多要素認証 (MFA) の方法についても調査しました。教育分野の被害組織のほぼすべて (98%) で、何らかの MFA が有効になっていました。これは、認証情報を悪用した攻撃の大半で MFA が導入されていたという調査全体の結果 (97%) とも一致しています。

しかし、MFA について回答した教育機関のうち、MFA を有効にしていたにもかかわらず、81% がデータを暗号化されていました。これは、多要素認証 (MFA) がすべての重要システムで網羅的に展開されていなかったか、攻撃者が多要素認証 (MFA) の保護を回避する方法を見つけたか、あるいは攻撃ベクトルが認証情報の侵害のみに依存していなかったことを示唆しています。

プッシュ型アプリケーション (64%) とワンタイムパスワード (53%) が教育業界において最も一般的に導入されている方法でした。

攻撃時に有効であった多要素認証 (MFA) の方法：教育機関全体

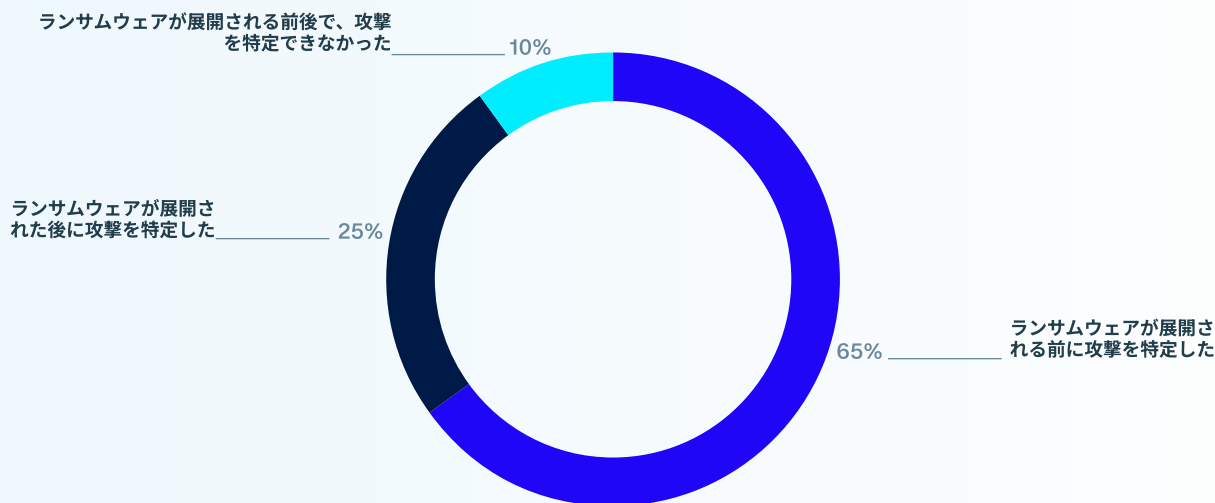


攻撃時に有効にしていた多要素認証の種類はありますか?複数回答可。回答者者：認証情報の侵害が原因で攻撃が発生した組織。高等教育機関と初等中等教育機関を合わせた全体。回答者数 =53

ファイアウォールの役割

教育分野において、ファイアウォールはほとんどの攻撃を特定しましたが、必ずしも攻撃の阻止に寄与したわけではありません。65% の教育機関が、ランサムウェアが展開される前にファイアウォールで攻撃を検知したと回答しました。一方、25% はランサムウェアの展開後に検知したと回答し、10% は攻撃をまったく検知できなかったと回答しました。これは調査全体の結果 (それぞれ 61%、32%、7%) とほぼ一致していますが、両端の割合がやや高くなっています。

ファイアウォールは攻撃を特定するためにどのような役割を果たしましたか？



ファイアウォールは攻撃を特定するためにどのような役割を果たしましたか？高等教育機関と初等中等教育機関を合わせた全体。回答者数 = 226

早期検知できたケースでも、教育分野の被害組織の 51% でデータが暗号化されていました。

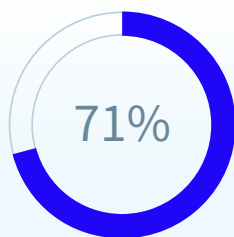
ファイアウォールは、攻撃を検知するためのデータ収集には優れていますが、検知された攻撃が同じ割合で阻止されているわけではありません。ファイアウォールは攻撃を検知し停止するために必要なデータをログに記録することが多いが、脅威を認識し、すばやく対応するためには、他のシステムと十分に深く連携できていない場合があります。

アイデンティティとランサムウェアの関連性

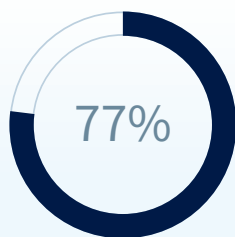
本調査で最も明確な発見の一つは、アイデンティティ攻撃とランサムウェアの間に直接的な関連があることです。全業界において、ランサムウェア被害者の3分の2(67%)が、そのインシデントが最も重大なアイデンティティ攻撃と同一の事象であったことを確認しています。しかし、教育分野ではその割合を上回っており、初等中等教育機関で71%、高等教育機関で77%でした(合計では73%)。

すべての攻撃がデータ暗号化に至ったわけではありませんが、この調査結果は、教育分野においてアイデンティティ攻撃とランサムウェア攻撃が強く関連していることを示しています。

ランサムウェア攻撃は、最も重大なアイデンティティ関連攻撃でもありました。



初等中等教育機関
(回答者数=131)



高等教育機関
(回答者数=95)

自組織はランサムウェア攻撃とアイデンティティ攻撃の両方を経験しましたか?ランサムウェアの被害を受けた組織回答数を図内に記載。

73%

ランサムウェアの被害者のうち、最も重大なアイデンティティ攻撃と同一の事象であった割合は、調査全体の67%を上回っています。

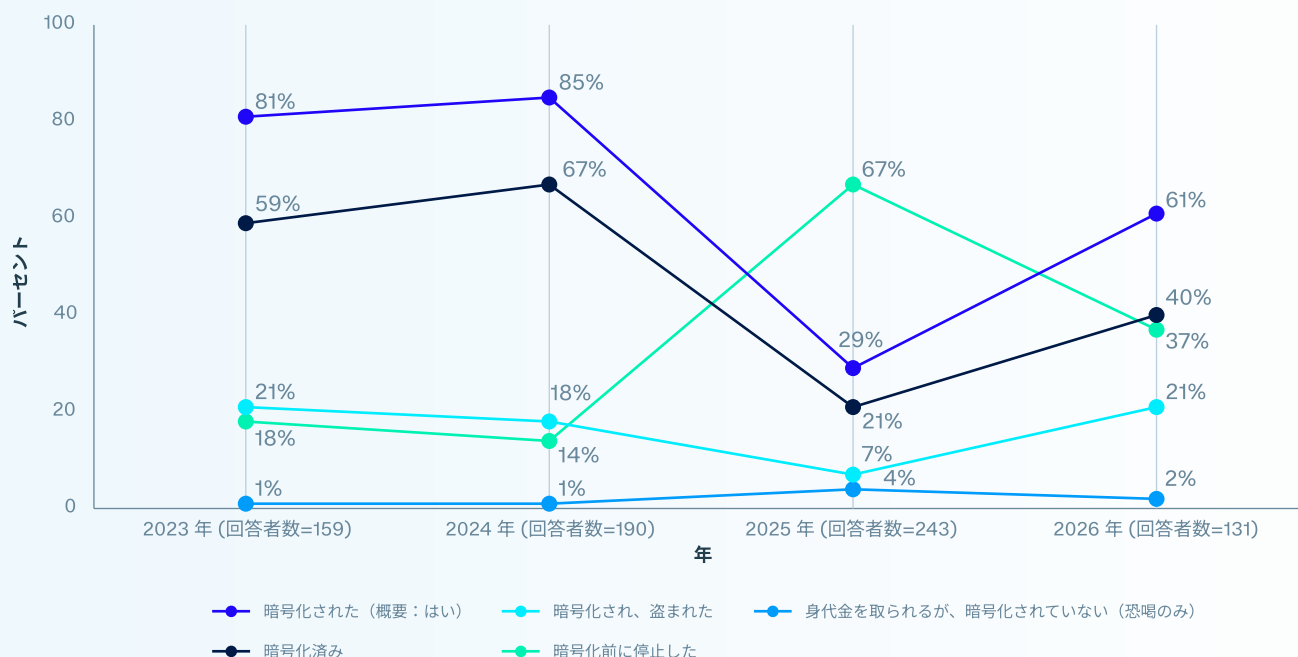
データ暗号化と復旧

データ暗号化率

2025 年の教育機関のランサムウェアの現状レポートによれば、初等中等教育機関において非常に良好な結果が示されましたが、残念ながら、今年のレポートでは、初等中等教育機関で以前の傾向に近い状況へと逆戻りしていることが示されています。

2025 年の報告書で初等中等教育機関の暗号化率が 29% に低下し、その年のどの業界よりも低い水準となった後、2026 年には初等中等教育機関に対する攻撃でデータ暗号化に成功した割合が 2 倍以上に増加し 61% に達しました。これは、調査全体の 56% を上回っています。今年、初等中等教育機関で暗号化の前に阻止された攻撃は、わずか 37% でした。前年のレポートにおけるこの数値は 67% でした。

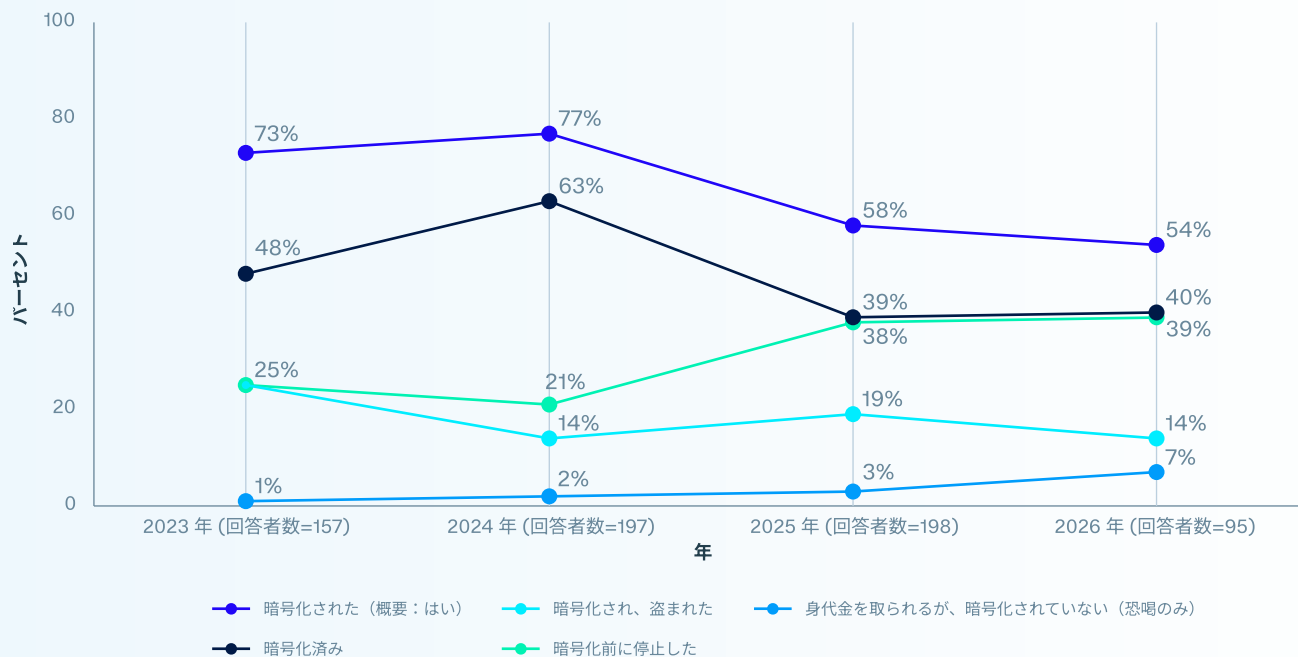
データ暗号化率の経時的変化：初等中等教育機関



二重脅迫 (データを暗号化するとともに窃取する攻撃) も初等中等教育機関で再び増加し、2025 年の 7% から 2026 年には 21% となりました。これは、2025 年以前の水準に戻った形です。こうした攻撃では、攻撃者が被害者に圧力をかけるための新たな手段が生まれます。暗号化せずに恐喝のみを行う攻撃 (暗号化せずに身代金を要求する攻撃) は、初等中等教育機関では 4% から 2% へとわずかに減少しました。

高等教育機関では、より安定した推移となりました。暗号化率は2025年の58%から2026年には54%へとわずかに低下しましたが、調査全体とほぼ同じ水準を維持しています。

データ暗号化率の経時的変化：高等教育機関



ランサムウェア攻撃で組織のデータは暗号化されましたか？回答者数を図内に記載。
このグラフの「暗号化（サマリー：はい）」の項目は、「暗号化」と「暗号化および窃取」の回答を合計したものです。

高等教育機関では、暗号化を伴わない恐喝のみの攻撃が2025年の3%から2026年には7%へと増加しました。割合としては小さいものの、注視すべき動きです。

2026年の状況は、教育分野が長期的な傾向に戻ったことを示しています。2023年と2024年は、初等中等教育機関におけるデータ暗号化率が高等教育機関を上回っていました。2025年は例外であり、この年は初等中等教育機関の暗号化率が一時的に大幅に低下しました。今年は、初等中等教育機関の暗号化率が61%、高等教育機関が54%となり、長期的な傾向に戻りました。

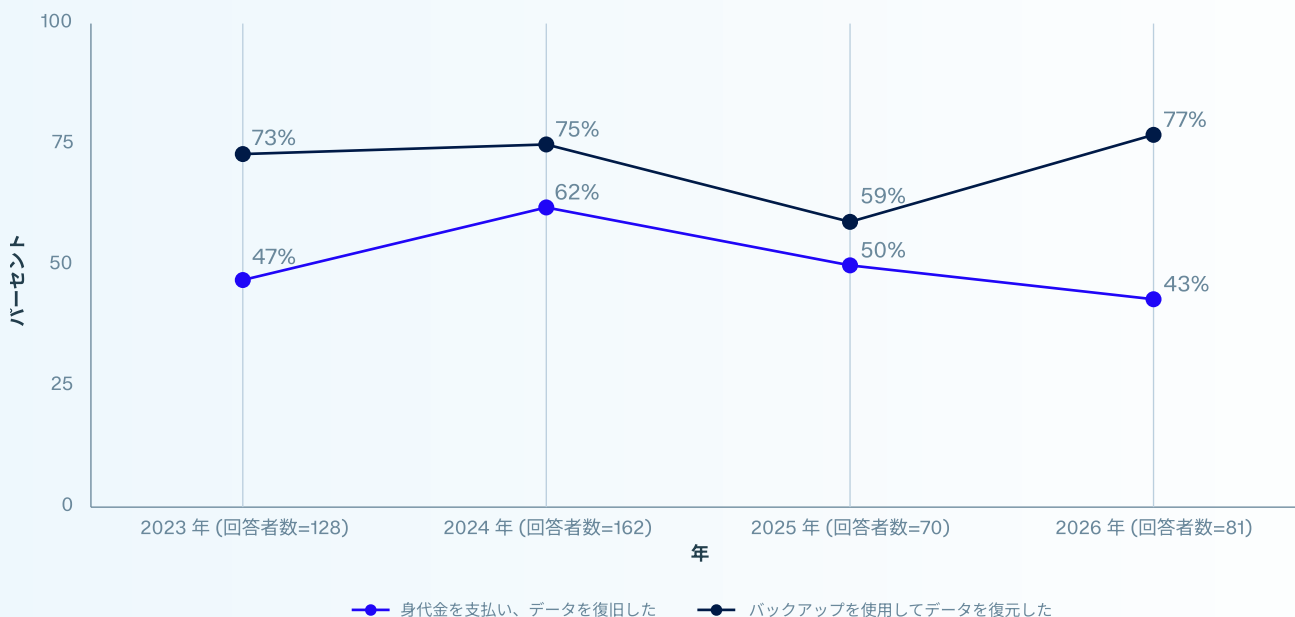
組織が暗号化されたデータを復旧した方法

バックアップは、2026年の教育機関がデータを復旧するための最も有効な手段でした。2025年にこの割合は低下した後（初等中等教育機関59%、高等教育機関47%）、今年はバックアップからの復旧が再び増加しました。**初等中等教育機関の77%、高等教育機関の69%がバックアップからデータを復元しましたが、どちらも調査全体の66%を上回っています。**この回復傾向は、教育分野でバックアップインフラへの投資が再び強化され、身代金要求に対するレジリエンスが再構築されつつあることを示唆しています。

77%

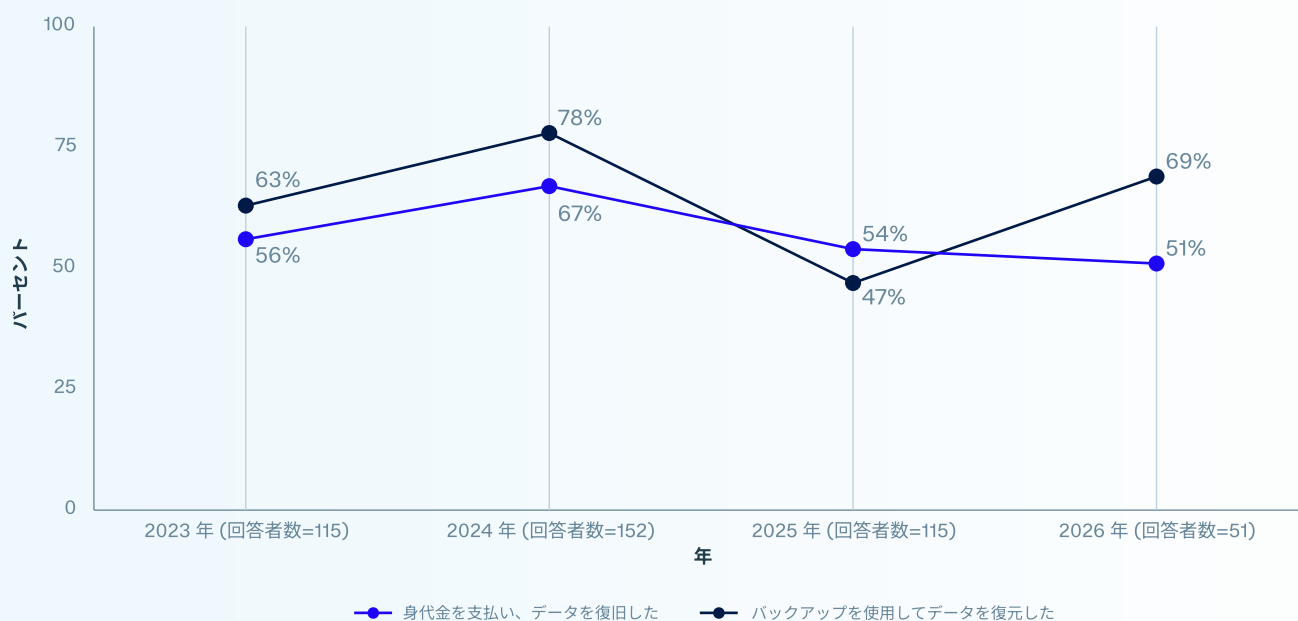
2026年にバックアップから暗号化されたデータを復元した初等中等教育機関の割合は、調査全体の66%を上回りました。

データ復旧方法の経時的変化：初等中等教育機関



どのようにデータを復旧しましたか？複数回答可。回答者数を図内に記載。

データ復旧方法の経時的変化：高等専門教育機関



どのようにデータを復旧しましたか?複数回答可。回答者数を図内に記載。

同時に、教育分野では身代金を支払うケースも減少しています。**身代金を支払い、データを取り戻した教育機関の割合は、2年連続で低下しています。**初等中等教育機関では2024年の62%から2025年には50%、2026年には43%となり、高等教育機関でもそれぞれ67%、54%、51%へと低下しました。

バックアップからの復旧が増加する一方、身代金の支払いによる復旧は減少しており、教育分野では、攻撃者の協力に頼るよりも、自らの能力によって復旧を進められるようになっています。

要求された身代金額と支払った身代金

身代金要求額

教育分野では、調査全体の他の業界と比べて、身代金要求額がより高額でした。教育機関に提示された身代金要求額の中央値は 77 万 5,200 ドルで、全業界の中央値である 69 万 8,000 ドルを上回りました。身代金要求額の分布も高額側に偏っており、**身代金要求の半数 (50%) が 100 万ドル以上、4 分の 1 (25%) が 500 万ドル以上**でした。全業界の調査対象では、それぞれ 46% と 23% でした。

注：このデータからは、4,000 万ドル以上の異常な身代金が削除されています。

77 万 5,200 ドル

教育機関に提示された身代金要求額の中央値は、調査全体の中央値である 69 万 8,000 ドルを上回りました。

教育機関への身代金要求の半数は 100 万ドル以上でした。

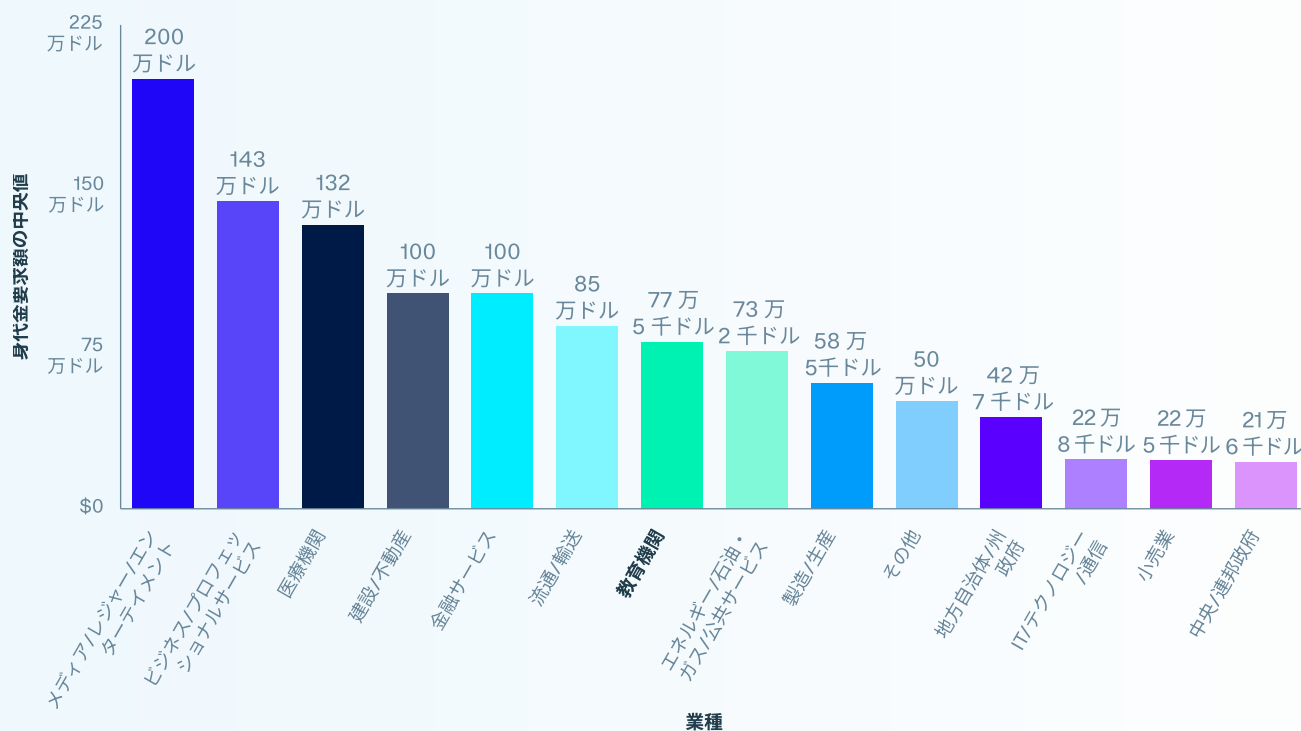
身代金要求額の中央値

	2025 年	2026 年
教育機関	98 万ドル (回答者数 =185)	78 万ドル (回答者数 =132)
全業界	132 万ドル (回答者数 =1,700)	70 万ドル (回答者数 =1,214)

攻撃者から要求された身代金額はいくらでしたか?回答者：データが暗号化された組織。回答者数を図内に記載。

他の業界と比較すると、教育分野は中間的な水準にあります。教育分野の身代金要求額の中央値は、メディア / レジャー / エンターテインメント (200 万ドル) やビジネス / プロフェッショナルサービス (143 万ドル) など、要求額が最も高い業界を下回っています。一方で、中央政府 (21 万 6,500 ドル) や小売 (22 万 5,000 ドル) など、要求額が低い業界を大幅に上回っています。

業界別の身代金要求額の中央値



攻撃者から要求された身代金額はいくらでしたか?回答者数: データが暗号化された組織。回答者数 =1,141

前年比では、改善と悪化の両方が見られます。教育分野全体の要求額（中央値）は、2025 年の 97 万 6,000 ドルから 2026 年には 77 万 5,200 ドルに減少しました。この減少は主に初等中等教育機関によるもので、身代金要求額の中央値が 103 万ドルから 73 万 7,600 ドルに低下しました。一方、高等教育機関ではこの傾向に反して、中央値が 69 万 7,086 ドルから 88 万 9,200 ドルへと上昇しました。

身代金の支払額

教育分野では、身代金要求額が高くても、実際の支払額が高くなるわけではありませんでした。身代金要求額は高かったものの、教育分野が実際に支払った身代金の中央値は、調査全体の他の業界と比べて低くなりました。教育機関が支払った身代金の中央値は51万5,000ドルで、調査全体の中央値である76万9,000ドルを下回りました。

教育分野では、支払額が最高額の層に集中することはありませんでしたが、500万ドル以上の支払いが占める割合は高くなりました。教育分野では、支払額の39%が100万ドル以上となり、調査全体の44%を下回りました。しかし、23%は500万ドル以上で、調査全体の16%を上回りました。教育分野では、身代金の支払額は他の業界より低い傾向にありますが、非常に高額な身代金を支払うケースも少なくありません。

51万5千ドル

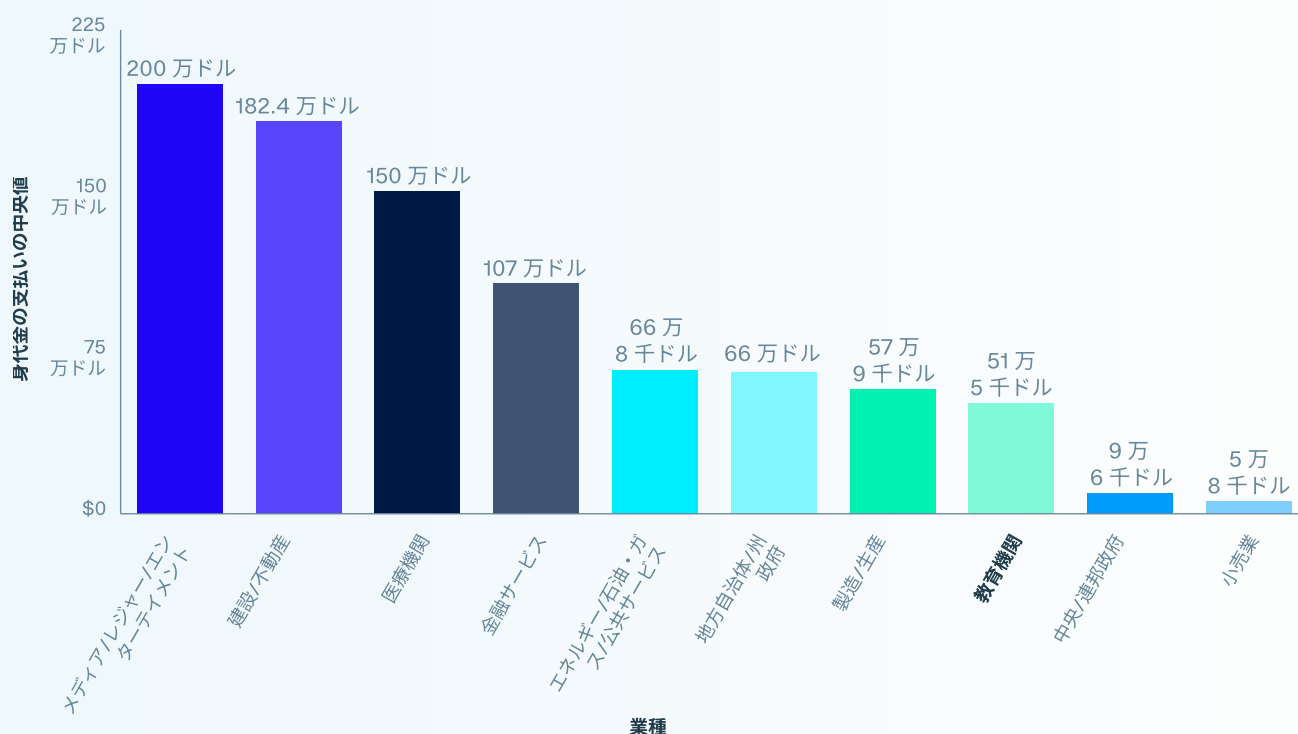
教育機関が支払った身代金の中央値は、要求額が高かったにもかかわらず、調査全体の中央値76万9,000ドルを下回りました。

身代金支払額の中央値

	2025 年	2026 年
教育機関	50 万ドル (回答者数 =100)	52 万ドル (回答者数 =62)
全業界	100 万ドル (回答者数 =847)	77 万ドル (回答者数 =587)

身代金として攻撃者に支払われた金額は、おおよそいくらでしたか?回答者：身代金を支払った組織。
回答者数を図内に記載。

業界別の身代金支払額の中央値



身代金として攻撃者に支払われた金額は、おおそいくらでしたか? 回答者: 身代金を支払った組織。回答者数 = 587。
この質問に対する回答者が 30 人未満の業界は除外します。

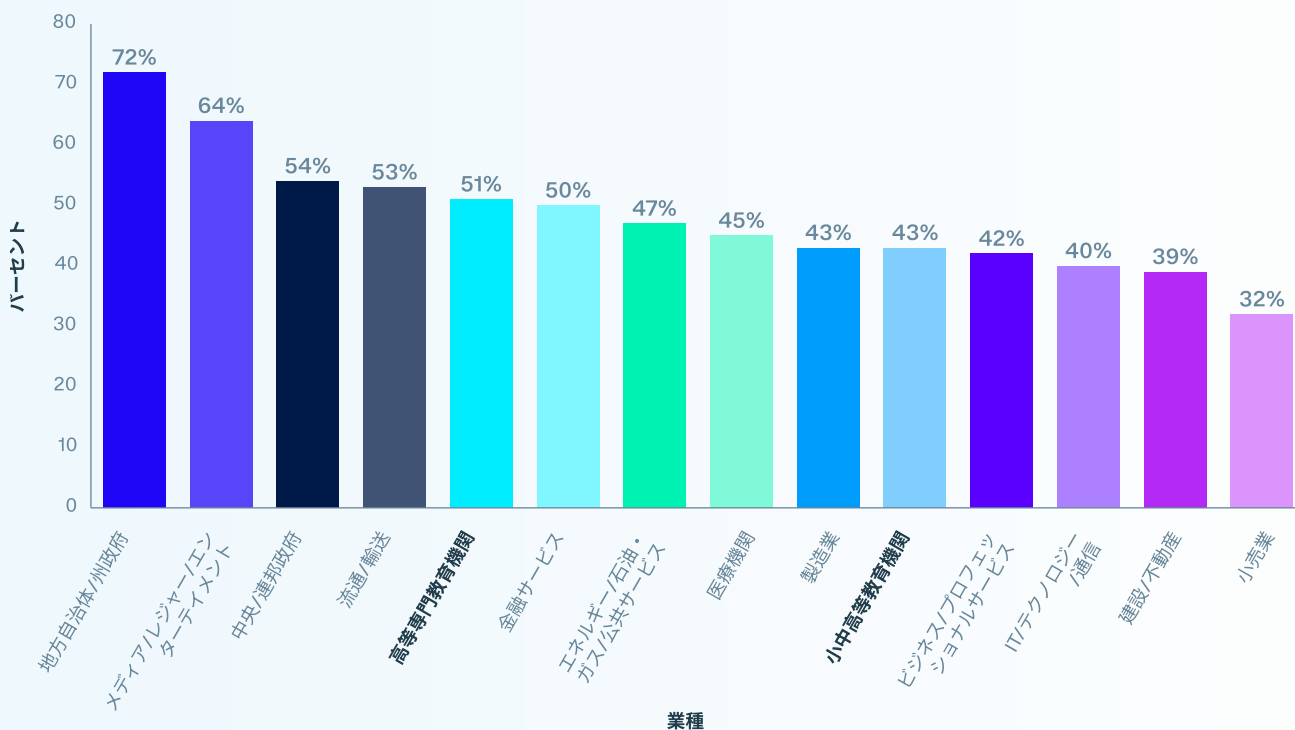
前年同期比の身代金支払い動向もまちまちでした。教育分野全体の身代金支払額の中央値はほぼ横ばいで、2025 年の 50 万ドルから 2026 年には 51 万 5,000 ドルへとわずかに上昇しました。同じ期間に、初等中等教育機関の身代金支払額の中央値は 80 万ドルから 32 万ドルへと大幅に減少しました。つまり、教育分野全体で見られたわずかな上昇は、高等教育機関によるものでした。

今年、支払額を報告した高等教育機関は 30 未満 (回答者数 = 27) だったため、高等教育機関の支払額について信頼できる単独の推移を示すことはできません。そのため、教育分野全体の支払額の推移を使用することを推奨します。

業界別の身代金を支払った組織の割合

身代金を支払う傾向は、初等中等教育機関と高等教育機関で異なりました。高等教育機関の被害者の51%が身代金を支払い、全体調査の48%を上回った一方、初等中等教育機関では43%にとどまり、全体調査よりも支払い率が低い傾向が見られました。

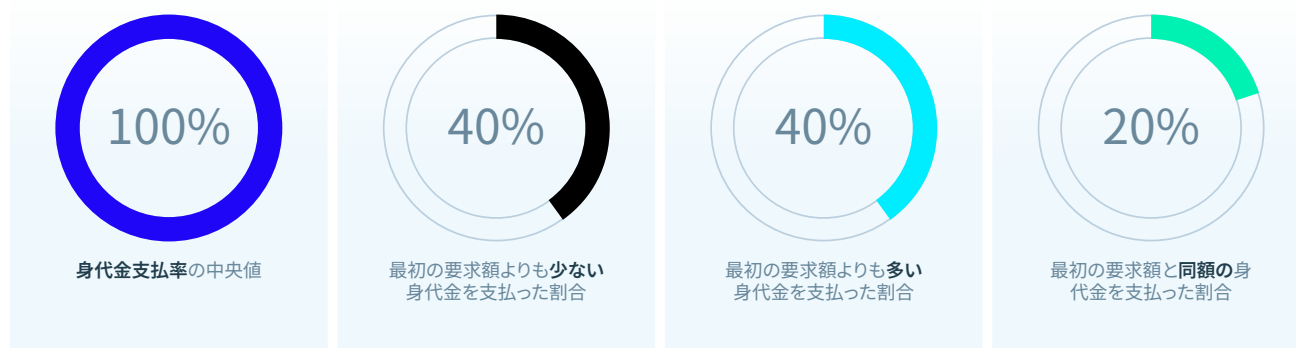
業界別の身代金支払率



どのようにデータを復旧しましたか? 回答者: データが暗号化された組織。回答者数 = 1,214

実際の身代金支払額と最初の要求額

身代金を支払った教育機関のうち、40% は当初の要求額を下回る金額を支払い、40% は要求額を上回る金額を支払い、20% は要求された金額をそのまま支払っていました。教育機関が支払った身代金の中央値は、要求額の 100% に達し、2025 年の 82% から上昇しています。つまり、かなりの割合の教育機関が交渉によって支払額を引き下げた一方で、同じ割合の教育機関が、当初の要求額を上回る金額を支払う結果となりました。



支払った身代金は、最初の身代金要求額を下回っていましたか、同額でしたか、それとも上回っていましたか？外れ値を除外。高等教育機関と初等中等教育機関を合わせた全体。回答者数 = 58

ビジネスと人間への影響

ランサムウェア攻撃の復旧コスト

教育分野では、平均を上回る復旧費用が発生しました。ランサムウェア攻撃から復旧するための平均費用（身代金を除く）は、初等中等教育機関で 246 万ドル、高等教育機関で 199 万ドルであり、どちらも調査全体平均の 170 万ドルを上回っています。

初等中等教育機関では、2 年連続で最も大きな負担となりました。初等中等教育機関の平均復旧費用は、2025 年の 228 万ドルから 2026 年には 246 万ドルへとわずかに増加し、教育分野の中で最も高額となりました。また、調査全体の 170 万ドルを大幅に上回っています。

復旧にかかる平均コスト（平均）

	2025 年	2026 年
初等中等教育機関	228 万ドル (回答者数 =243)	246 万ドル (回答者数 =131)
高等教育機関	90 万ドル (回答者数 =198)	199 万ドル (回答者数 =95)
全業界	153 万ドル (回答者数 =3,400)	170 万ドル (回答者数 =2,158)

最も深刻なランサムウェア攻撃の影響を修復するために組織が負担した概算費用は？身代金支払いを除く平均回答者数を図内に記載。

高等教育機関では、差が最も大きく拡大しました。高等教育機関の平均復旧費用は、2025 年の 90 万ドルから 2026 年には 199 万ドルへと 2 倍以上に増加しました。2025 年のレポートでは、高等教育機関の復旧費用は、全業界の中でも最も低い水準の一つでした。今年は、高等教育機関の復旧費用が上昇し、初等中等教育機関の水準に近づきました。両方の教育部門の復旧費用が調査全体の平均を上回っており、全体平均も 153 万ドルから 170 万ドルへと緩やかに上昇しました。

109 万ドル

2025 年から 2026 年にかけて、高等教育機関がランサムウェア攻撃から復旧するための平均費用の増加額。

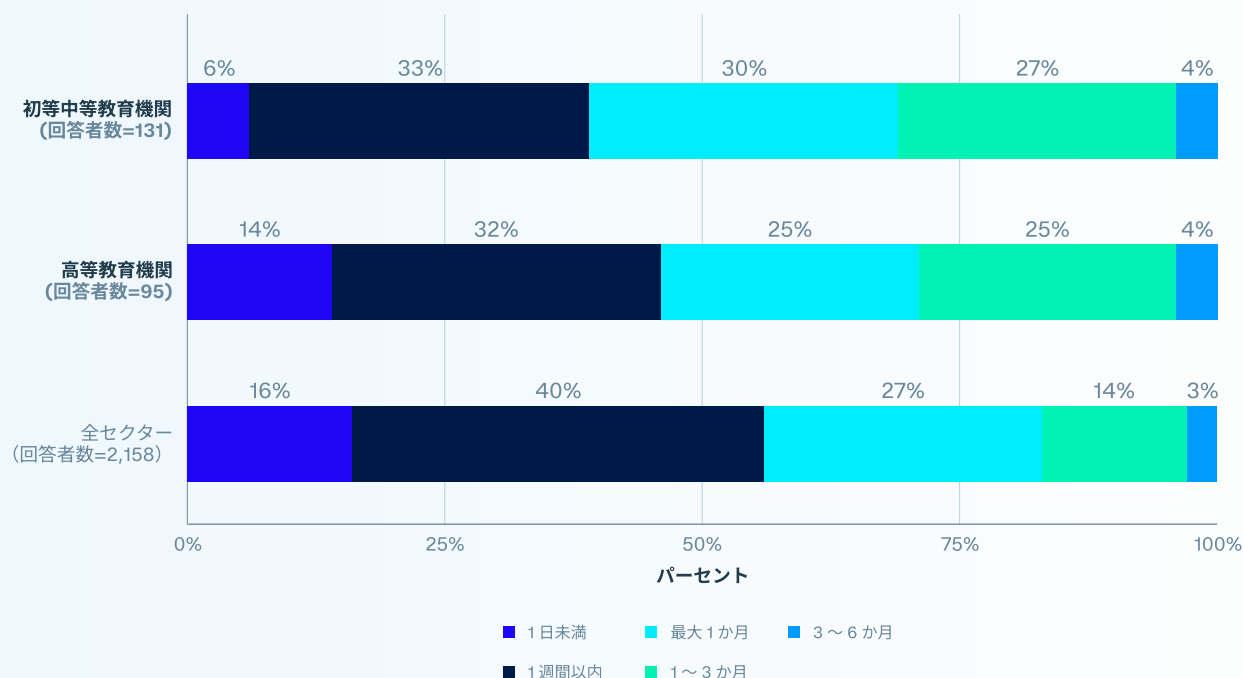
復旧にかかった時間

教育機関では、復旧のためにより多くの費用を支払っただけでなく、復旧にもより長い時間を要しました。最も明確な差が見られるのは、復旧に1～3か月を要したケースです。完全に復旧するまでに1～3か月を要した組織は調査全体ではわずか14%でしたが、初等中等教育機関では27%、高等教育機関では25%でした。**教育分野では、復旧に1か月以上を要する可能性が約2倍高くなりました。**

31%

初等中等教育機関で復旧に1か月以上を要した割合。これは全業界の中で最も高くなっています。

ランサムウェアから復旧するまでにどれくらいの時間がかかりましたか？



ランサムウェア攻撃から完全に復旧するのに、どれくらいの時間がかかりましたか？回答者数を図内に記載。

短期間で復旧できたケースについても、逆の傾向が見られます。1日以内に復旧できた初等中等教育機関はわずか6%でしたが、調査全体では16%、高等教育機関では14%でした。

初等中等教育機関ほど復旧が長期化した割合が高い業界はありません。31%の教育機関が完全に復旧するまでに1か月以上を要しました。

ランサムウェアによる人材への影響

教育分野では、攻撃による人的な負担が調査全体よりも大きく、初等中等教育機関と高等教育機関でその影響も異なっていました。高等教育機関では、特に大きな負担となったのは、上層部からの圧力でした。53%のチームが、攻撃後に経営幹部からのプレッシャーが強まったと回答しており、調査全体の40%を13%上回りました。チームや組織構造の変更も、高等教育機関ではより多く見られました（高等教育機関の43%に対し、全業界では32%）。

初等中等教育機関の多くは、評価の向上と業務負荷の増大を経験しています。初等中等教育機関のチームのほぼ半数（49%）が、経営幹部からの評価が高まったと回答しており、調査全体の36%を上回りました。評価が高まることはプラスの側面もありますが、業務負荷の増加はそうではありません。初等中等教育機関では、43%が業務負荷の継続的な増加を挙げており、全業界の31%を上回りました。注目が集まることには両面があり、評価が高まる一方で、より重く、長期化する業務負荷も生じています。

ランサムウェアによる人材への影響

影響	初等中等教育機関（回答者数=81）	高等教育機関（回答者数=51）	全業界（回答者数=1,214）
今後の攻撃に対する不安やストレスの増加	40%	33%	41%
シニアリーダーからのプレッシャーの増加	48%	53%	40%
シニアリーダーからの評価の向上	49%	29%	36%
チームや組織構造の変更	33%	43%	32%
チームの優先事項や注力領域の変化	33%	35%	32%
攻撃を阻止できなかったことへの罪悪感	31%	25%	31%
継続的な業務量の増加	43%	31%	31%
ストレスやメンタルヘルス問題によるスタッフの欠勤	40%	39%	29%
チームリーダーの交代	27%	29%	21%

ランサムウェア攻撃は、自社のIT/サイバーセキュリティチームのメンバーにどのような影響を与えましたか？

対象：データが暗号化された組織。回答者数を図内に記載。

初等中等教育機関と高等教育機関の双方で、従業員のウェルビーイングが損なわれました。高等教育機関の39%および初等中等教育機関の40%のチームが、ストレスやメンタルヘルスの問題による職員の欠勤を報告しており、調査全体の29%を大きく上回りました。

リーダーの交代も多く見られ、攻撃後にリーダーが交代したチームは、高等教育機関で29%、初等中等教育機関で27%に上りました。調査全体では21%でした。

53%

攻撃後に経営幹部からのプレッシャーが強まった高等教育機関のITおよびセキュリティチームの割合。調査全体では40%。

ソフォスの提言

ランサムウェア対策としてアイデンティティセキュリティを強化してください。教育機関のランサムウェア被害者の 73% が、そのランサムウェアインシデントが最も重大なアイデンティティ攻撃と同一のインシデントであったと確認しており、これは全体調査の 67% よりも高い割合であり、この分野におけるアイデンティティ侵害とランサムウェアの密接な関連性を強調しています。教育機関は、脅威の検知と対応 (ITDR) を優先し、すべてのアクセスポイントに多要素認証を適用し、人間および非人間の認証情報を定期的に監査する必要があります。

MFA を包括的に導入し、特にフィッシング耐性のある MFA を採用してください。調査では、認証情報が侵害された教育機関の 98% が、攻撃を受けた時点で何らかの形で MFA を有効にしていたが、それでもデータの暗号化率は高い水準にありました。MFA だけでは攻撃を阻止するには不十分であり、SaaS アプリなど MFA を強制するサービスだけで有効にし、VPN へのログインやファイアウォールの管理コンソール、レガシーアプリでは無効にするのではなく、包括的に導入する必要があります。

最先端の AI モデル悪用した攻撃に備え、エンドポイント保護を強化してください。このレポートでは脆弱性の悪用の報告は減少していますが、ソフォスの専門家は、組織が最先端の AI によって発見された脆弱性へのパッチ適用に追いつけず、脆弱性の悪用が再び増加すると予想しています。エクスプロイトを利用した攻撃を自動的にブロックできる強力なエンドポイント防御を備えることが不可欠です。

専門家の支援や MDR を活用する。人材、スキル、専門知識の不足は、教育分野全体で引き続き見られる課題であり、特に高等教育機関では深刻です。高等教育機関では、組織内に専門知識が不足していることが、特に顕著な弱点となりました。AI によって高度化した脅威への対応は、急速に進化する AI テクノロジーに追いつこうとするセキュリティチームに、さらに大きな負担をもたらします。自社だけでセキュリティオペレーションチームを十分に編成して運用できる確信がない場合は、24 時間 365 日体制の MDR ベンダーまたはマネージドサービスプロバイダーといった外部のスペシャリストに不足分を補ってもらうことを検討してください。AI と自動化を活用してより多くのインシデントに包括的に対応できるベンダーは、人材や運用能力を大きく補完し、スキル不足や対応能力の課題を解消する上で強力な支援となります。

バックアップと復旧インフラに投資してください。バックアップは、初等中等教育機関と高等教育機関の双方で、最も主要な復旧手段となっていました (それぞれ 77%、69% で、いずれも調査全体を上回りました)。バックアップは定期的にテストし、オフラインまたはイミュータブル (改ざん不可) な形式で保管するとともに、緊急時にも実行可能な文書化されたインシデント対応計画に組み込むべきです。

エクスポート管理プログラムを継続的に実施する。脆弱性の悪用は依然として主要な攻撃ベクトルであり、最先端の AI モデルが新たな弱点をより迅速に発見するようになるにつれて、今後さらに増加すると考えられます。組織は、迅速かつ継続的なパッチ適用を維持するとともに、ネットワークセグメンテーション、ゼロトラストネットワークアクセス (ZTNA)、MFA や継続的認証の導入など、多層的な緩和策を講じる必要があります。

ファイアウォールによってエクスポートを削減し、ファイアウォールテレメトリを活用して攻撃を早期に検知する。2026 年のデータから、ファイアウォールはランサムウェア攻撃の兆候を検知する能力に優れていることが明らかになりました。調査対象の 65% の組織では、ランサムウェアが実行される前に攻撃を特定するのに十分なデータが得られていました。しかし、こうした早期に兆候が検知されたケースでも、教育分野の被害組織の 51% ではデータが暗号化されていました。これは、他の制御ポイントからテレメトリを取得できなければ、ファイアウォールだけでは攻撃を確認したり阻止したりできないことが多いからです。ファイアウォールが迅速に、できれば自動的に更新されるようにするとともに、管理者アクセスやユーザーポータルなど、インターネットに公開されるサービスを最小限に抑えましょう。ファイアウォールを XDR や MDR と連携させ、ファイアウォールのテレメトリを活用することで、ランサムウェアのペイロードが展開される前に攻撃を検知できるようにしてください。この要件を満たすのが、各制御ポイントがシグナルを共有するサイバーセキュリティ防御システムです。

推奨される対策：

1. セグメンテーションによって攻撃者の動きを遅らせる
2. ZTNA でレガシー VPN を置き換え、アプリの脆弱性を封じ込める
3. アイデンティティ脅威の検知と対応 (ITDR) によるアイデンティティインフラの強化
4. フィッシングに耐性のある MFA を最終目標とする
5. インターネットに公開されたデバイスへの計画的なパッチ適用
6. 24 時間 365 日の検知と対応

まとめ

「教育機関におけるランサムウェアの現状 2026 年版」では、ランサムウェアを取り巻く脅威の状況が変化しつつあることが明らかになりました。

進展の兆しも見られました。身代金要求額は減少し、バックアップからの復旧は過去最高に近い水準まで増加しており、教育機関が支払う身代金も他の業界と比べて低い水準にあります。

一方で、依然として残る課題は重大です。教育分野を狙ったランサムウェア攻撃の半数以上で、依然としてデータの暗号化に成功しています。インシデント 1 件当たりの平均復旧費用は 226 万ドルに達し、調査全体を上回っています。また、初等中等教育機関では、復旧に 1 か月以上を要したケースの割合が最も高くなりました。

教育機関におけるリスクは、アイデンティティに関する問題に集中しています。教育機関では、ランサムウェアインシデントが最も重大なアイデンティティ攻撃と同一の事象だったと回答した割合が、調査全体を上回りました。すでに復旧に時間とコストがかかっている教育分野にとって、この密接な関連性を踏まえると、アイデンティティインフラへの投資が最も効果的だと考えられます。

教育機関は、今後 10 年間におけるサイバーセキュリティ上の最大の課題にも備える必要があります。AI によって強化された脅威です。その理由は、すでにデータからも示唆されています。教育機関の 62% が、既知または未知のセキュリティギャップを攻撃要因として挙げ、63% が人材またはスキル不足を指摘しています。AI によって攻撃の高速化し規模が拡大するにつれ、これら 2 つのギャップはいっそう重大な意味を持つようになります。攻撃者は AI を利用して弱点をより迅速に発見し、マシンスピードで複数の制御ポイントを狙う攻撃を組み立てるようになっています。

今年の根本原因に関するデータには、さらに深い意味も見られます。認識されている根本原因の構成は均等化しており、教育分野を含む全業界で、特定の攻撃ベクトルが突出する状況ではなくなっています。そのため、特定の根本原因に絞って防御を強化するのはリスクがあります。攻撃者は複数のベクトルを通じて攻撃を成功させているためです。

今年の調査結果に見られる傾向、特にファイアウォールによる検知や MFA の有効化が攻撃の結果に及ぼす影響の小ささは、一貫した方向性を示しています。つまり、防御対策が個別に機能しているだけでは、十分な成果を得ることはできなくなっています。AI 時代の攻撃とのギャップを埋めるには、より多くのツールを追加することよりも、すでに導入しているツール同士を連携させ、現代の脅威で求められる速度でコンテキストの把握、検知、対応を実行できるようにすることが重要になります。

今後のランサムウェア対策で最も優れた成果を上げる教育機関は、経営幹部がこの課題に対する関心を持ち続け、統合された AI 主導の防御システムを採用し、テクノロジーやプロセスだけでなく、日々脅威に対抗するセキュリティ人材にも継続的に投資する組織となるでしょう。



ランサムウェアの詳細と、ソフォ
ス製品がお客様の企業の防御に
どのように役立つかについては、
ソフォスの Web サイトをご覧ください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp