SOPHOS

# 教育機関における ランサムウェアの現状 2025 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 441 人を対象とした独自調査の結果。

ソフォス ホワイトペーパー 2025 年 8 月

# はじめに

第 5 版となる年次レポート「教育機関におけるランサムウェアの現状」へようこそ。このレポートでは、2025 年の初等中等教育機関 (18 歳までの学生 ) および高等教育機関 (18 歳からの学生 ) の両方におけるランサムウェアの実態を報告します。

今年のレポートでは、教育機関が過去 1 年間で経験したランサムウェアの被害について、発生原因とその影響の両面に焦点を当てて、明らかにしています。また、これまであまり注目されてこなかった領域についても取り上げています。例えば、教育機関が攻撃を受けることとなった運用面の要因や、教育機関の IT/ サイバーセキュリティチームの人材への影響について調査した結果をお伝えします。

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、441 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 243 名、高等教育 198 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。

- 教育機関がランサムウェアの被害に遭う理由
- データへの影響
- 要求された身代金額と支払った身代金
- ランサムウェアによる人材とビジネスへの影響

## 報告日に関する注記

年次調査のデータを簡単に比較できるように、調査を実施した年を報告書の名前に使用しており、今年のレポートの場合には 2025 年版になっています。回答した企業は前年度の経験について報告しています。このレポートで参照されている多くの攻撃は 2024 年に発生しています。

## 調査について

本レポートは、過去 1 年間にランサムウェア攻撃を受けた組織に所属する 3,400 人の IT/ サイバーセキュリティプロフェッショナル ( うち 441 人は教育業界の回答者 ) を対象とした、ベンダー中立の独立調査の結果に基づいています。この調査は、ソフォスの委託を受けて第三者専門機関が 2025 年 1 月から 3 月にかけて実施しました。回答者はすべて、従業員数 100 人から 5,000 人の組織に所属しており、過去 12 か月間の経験に基づいて回答しています。

回答者は、17 か国にまたがっており、調査結果は幅広く多様な経験を反映したものとなっています。本レポートには、前年の調査結果との比較も含まれており、年次比較が可能です。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

## 教育機関がランサムウェアの被害に遭う理由

- ランサムウェア攻撃の技術的な根本原因として、初等中等教育機関では**フィッシング**が最も多く報告されていますが (22%)、攻撃手法はフィッシング、悪意のあるメール、脆弱性の悪用、認証情報の侵害でほぼ同じ割合になっています。一方、高等教育機関では**脆弱性の悪用**が引き続き最も多い原因であり、攻撃の 35% で使用されていました。
- 運用面の根本原因に目を向けると、高等教育機関では**認識していなかったセキュリティギャップ**が最も多く挙げられ (49%)、初等中等教育機関では**専門知識の不足と攻撃に対応する人材や能力の不足**が最も多く報告されています ( それぞれ 42%)。

## データへの影響

- **教育業界におけるデータ暗号化率は、過去 4 年間で最低水準に低下しました。**初等中等教育機関では、攻撃の 29% でデータが暗号化されていますが、これは全業界の中で最も低い割合です。高等教育機関では、攻撃の 58% でデータが暗号化されており、
- また、データが暗号化された初等中等教育機関の 26%、高等教育機関の 33% が**データの流出**も経験しています。
- データを暗号化された教育機関の 97% が、データを復元することができました。
- **データ復旧のためのバックアップ利用**は減少しており、データが暗号化された初等中等教育機関のうち、バックアップを使用して復旧したのはわずか 59%、高等教育機関では 47% にとどまりました。
- また、初等中等教育機関の被害者の半数、高等教育機関の被害者の 54% が、**データを取り戻すために身代金を支払っていました。**

## 身代金：要求額と支払額

- **教育業界における身代金要求額の中央値は大幅に減少しました。**初等中等教育では 385 万ドルから 102 万ドルに、高等教育では 355 万ドルから 69.7 万ドルに減少しており、調査対象となったすべての業界の中でも最も低い水準となりました。
- **実際に支払われた身代金の中央値も大きく減少しています。**身代金支払額は初等中等教育では 660 万ドルから 80 万ドルに、高等教育では 441 万ドルから 46.3 万ドルに減少しており、2024 年には支払額が最も高い業界だった両方の教育機関が 2025 年には最も低い業界になっています。
- この傾向を反映して、**攻撃者が要求した身代金の要求額に対して、実際に支払われた金額の割合も減少しています。**初等中等教育機関では、2024 年の 115% から 2025 年には 84% へと低下し、高等教育機関では 122% から 69% へと大幅に低下しました。
- **要求額と支払額の比率**を詳しく見ると、初等中等教育機関では 41% が要求通りに支払い、41% は要求額より少なく支払い、18% は要求額より多く支払っています。高等教育機関では、要求通りに支払ったのは 26% にとどまり、60% が要求額より少なく支払い、14% が多く支払っています。

## ランサムウェアによるビジネスへの影響

- 2025 年、**教育業界における平均的な復旧コストは大幅に減少しました。**高等教育機関では、2024 年の 402 万ドルであった復旧コストが 2025 年には 90 万ドルへと 77% も急減し、全業種の中で最も低い水準 ( 同率 ) となりました。一方、初等中等教育機関では、前年の 376 万ドルから復旧コストが 39% 減少して 228 万ドルとなったものの、全業種の中で最も高い復旧コストを記録しました。
- **教育機関は攻撃で受けた影響を以前よりも迅速に復旧できるようになっています。**初等中等教育機関の半数、および高等教育機関の 59% が、1 週間以内に攻撃による影響から完全に復旧しています。この数値はいずれも 2024 年の 30% から上昇しています。

## ランサムウェアによる人材への影響

データが暗号化されたすべての教育機関 ( 初等中等および高等教育機関の両方 ) において、IT/ サイバーセキュリティチームに以下のような**直接的な影響**があったことが報告されています。

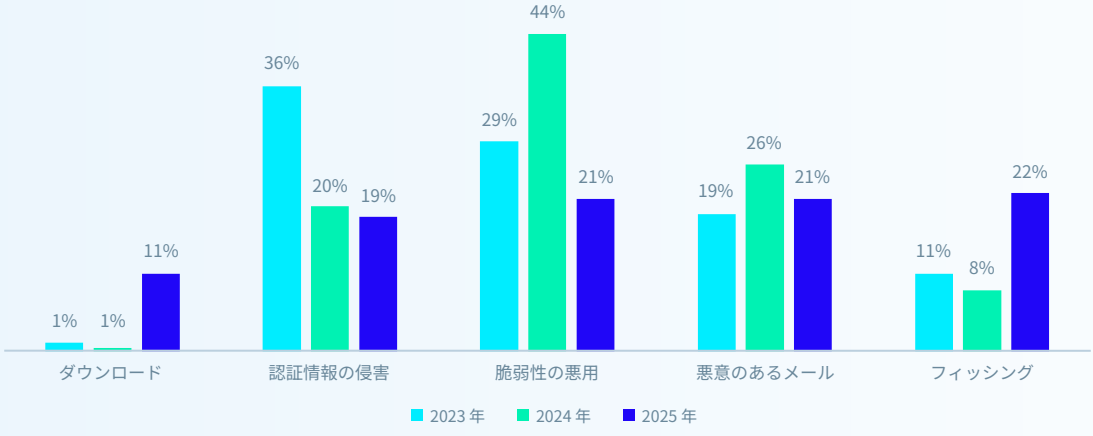
- 教育業界の IT/ サイバーセキュリティ担当チームの 41% が、**今後の攻撃に対する不安やストレスの増加**を報告しました。
- 40% は経営幹部からの**プレッシャーが増加した**と答える一方で、31% は**評価が高まった**と報告しています。
- 38% が IT/ サイバーセキュリティチームへの影響として、**チームの優先事項や注力領域の変化、業務量の継続的な増加**の両方を挙げました。
- 37% が、インシデントの結果として**チーム / 組織構造**の変更を回答しました。
- 3 分の 1 (34%) は、**攻撃を未然に防げなかったことに対する罪悪感をチームとして感じた**と回答しています。
- 31% のチームでは、攻撃に関連する**ストレスやメンタルヘルス**の問題により**スタッフの休職**を体験しています。
- 4 分の 1 のケースでは、攻撃を受けたことにより**チームのリーダーが交代**させられました。

# 教育機関がランサムウェアの被害に遭う理由

## 教育業界における攻撃の技術的な根本原因

攻撃の技術的な根本原因は、初等中等教育機関と高等教育機関で異なっています。今回の調査で初めて、初等中等教育機関に対する攻撃の主な原因として**フィッシング**が最も多く報告され、全体の 22% を占めました。ただし、フィッシング、悪意のあるメール、脆弱性の悪用、認証情報の侵害という 4 つの主要な攻撃手法が、いずれも 3% 以内の僅差で拮抗しており、他の業界では見られないほど均等な分布となっています。

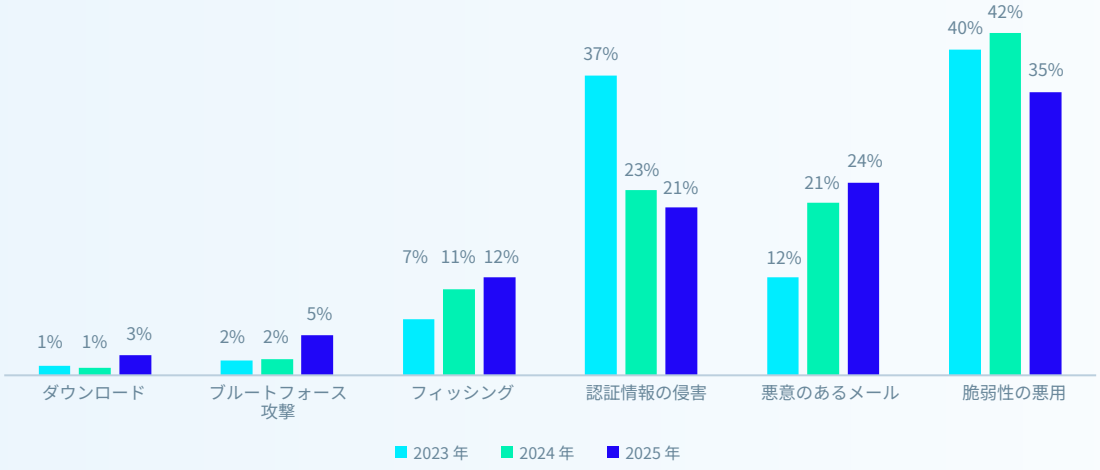
**図 1：初等中等教育機関におけるランサムウェア攻撃の技術的な根本原因 2023 ～ 2025 年**




過去 1 年間に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？はい。回答企業数 = 243 (2025 年 )、189 (2024 年 )、159 (2023 年 )

一方、高等教育機関では 3 年連続で**脆弱性の悪用**が最も多いランサムウェアの原因となっており、攻撃の 35% でこの手法が利用されています。この傾向は、他の多くの業界と一致しています。悪意のあるメールは、2 番目に多い攻撃手法として引き続き挙げられており、この手法を用いた攻撃の割合は、2024 年の 21% から 2025 年には 24% に増加しました。これに続くのが認証情報の侵害で、高等教育機関の 21% がこの根本原因を報告しています。

**図 2：高等教育機関におけるランサムウェア攻撃の技術的な根本原因 2023 ～ 2025 年**




過去 1 年間に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？はい。回答企業数 = 196 (2025 年 )、197 (2024 年 )、156 (2023 年 )

調査結果によると、根本原因は業界によって異なりますが、ほぼすべての業界において**脆弱性の悪用が主要な攻撃経路**となっています。主な例外：

- 最も一般的な根本原因はフィッシングで、初等中等教育機関 (22%) と エネルギー / 石油・ガス / 公共サービス (29%) のサービス提供者が挙げています。
- **認証情報の侵害**は、地方自治体 / 州政府で最も多く挙げられた攻撃経路であり、インシデントのほぼ 3 分の 1 (32%) を占めています。

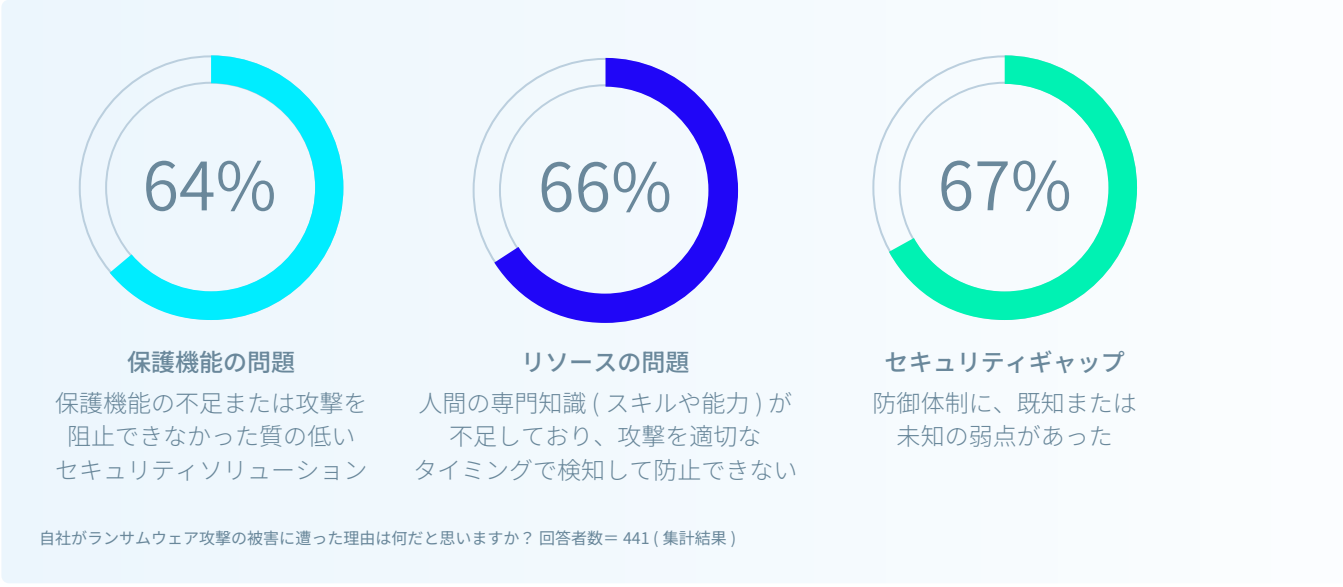
**図 3：業界別のランサムウェア攻撃の技術的な根本原因**


過去 1 年間に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？はい。回答者数を図内に記載。

## 教育業界におけるインシデントの運用面の根本原因

今回のレポートでは初めて、教育機関が攻撃を受けることにつながった運用面の要因について調査しました。調査結果によると、被害を受けた教育機関は一般的に複数の運用面の課題を抱えており、回答者は平均して 3 つの要因が攻撃の一因になったと述べています。

全体として、保護に関する問題 (64%)、リソースの問題 (66%)、セキュリティギャップ (67%) の 3 つが、ほぼ同じ割合で運用面の根本原因として挙げられています。

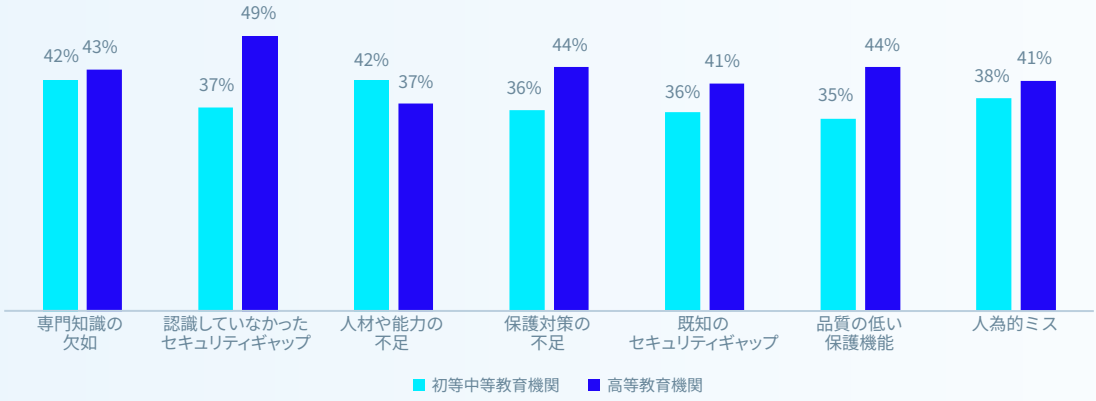



しかし、初等中等教育機関と高等教育機関の間には違いも見られます。特に初等中等教育機関では、攻撃の主な運用面の根本原因として、セキュリティギャップよりもリソースの不足がわずかに多く挙げられています。

運用面の根本原因を**個別に分析すると**、初等中等教育機関が被害を受けた主な理由として、攻撃を迅速に検知・阻止する**専門知識の欠如**と攻撃時にシステムを監視する**人材や能力の不足**がともに 42% で最多となっています。これに続くのが**人為的ミス** ( チームがミスを犯した、または適切に手順を遵守しなかった ) で、38% の攻撃の原因となっています。

高等教育機関では、**認識していなかったセキュリティギャップ** ( 防御の弱点 ) が個別の理由として最も多く挙げられており、回答者の約半数 (49%) が指摘しています。これは、調査対象となった全業界の中で最も高い割合です。これに続くのは**品質の低い保護機能** ( サイバーセキュリティ製品やサービスが攻撃を阻止できなかった ) と**保護対策の不足** ( 必要なサイバーセキュリティ製品やサービスを導入していなかった ) であり、どちらも 44% の攻撃の原因として挙げられています。

**図 4：教育機関に対するランサムウェア攻撃の運用面の根本原因**

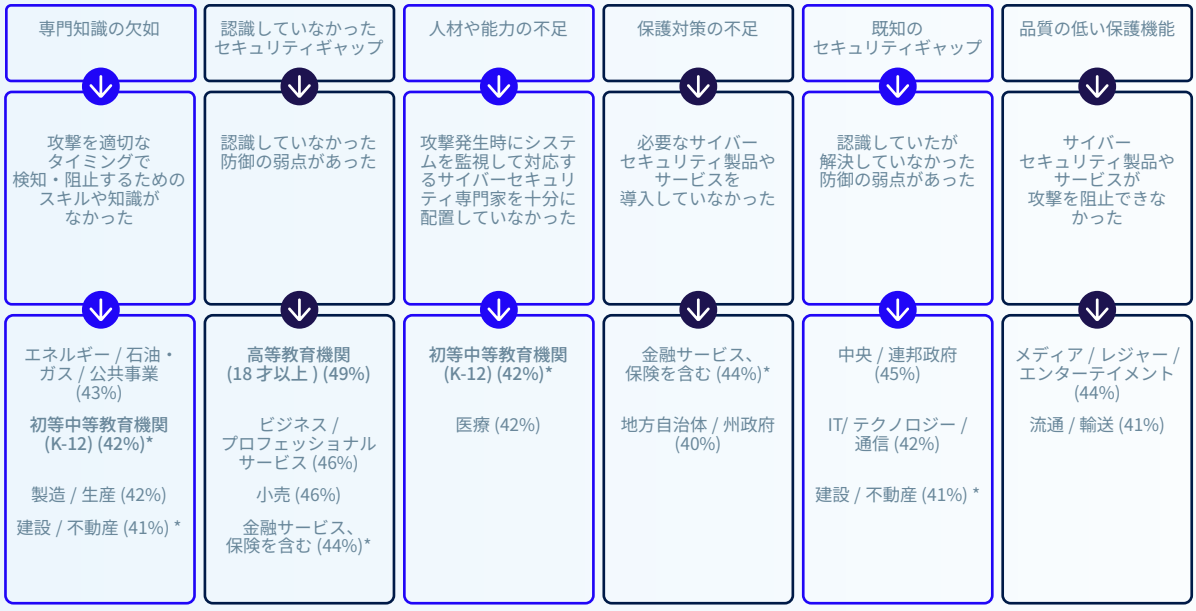



自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 回答者数＝ 243 ( 初等中等教育機関 )、198 ( 高等教育機関 )

## 業種別の運用面の根本原因

最も多い運用面の根本原因も業界によっても異なっており、各業界が直面する課題が異なっていることを反映しています。注目すべき点として、どの業界でも人為的ミスがランサムウェア攻撃を受けた最大の理由としては挙げられていませんでした。

**図 5：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**



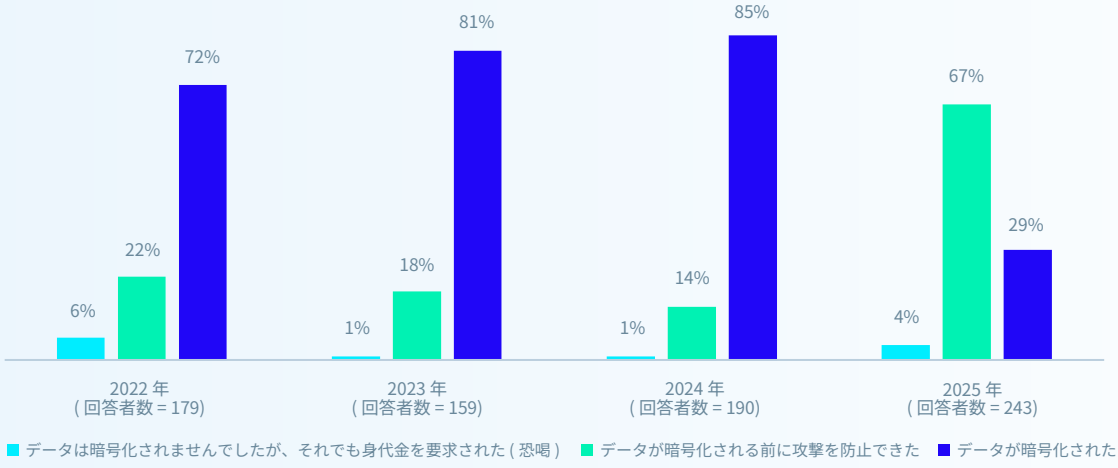

自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 回答者数＝ 3,400 業界別の内訳。
* は同率一位の複数の根本原因を示します

# データへの影響

## 教育業界におけるデータの暗号化

教育業界における**データ暗号化率が低下**していることは歓迎すべきことです。初等中等教育機関では、攻撃によってデータが暗号化された割合はわずか 29% で、これは過去 4 年間で最も低い水準になりました。これは調査対象となった全業界の中でも最も低い割合です。暗号化率の低下に伴い、暗号化される前に攻撃を阻止できた割合は、2024 年 の 14% から 2025 年に 67% へと急増しました。これもまた、全業界の中で最も高い数字であり、平均値の 44% を大きく上回っています。これは、初等中等教育機関がランサムウェア攻撃による被害が出る前に検知して阻止する能力を、かつてないほど向上していることを示しています。

**図 6：初等中等教育機関に対するランサムウェア攻撃におけるデータ暗号化率 2022 ～ 2025 年**

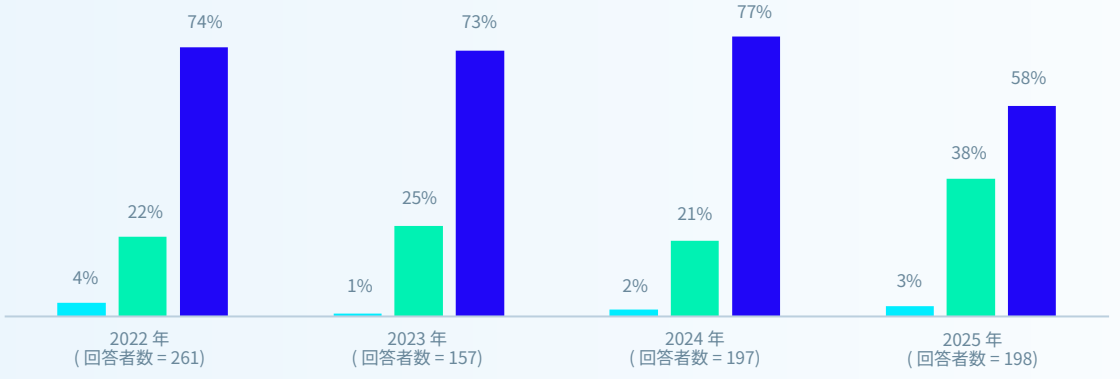



ランサムウェア攻撃でデータは暗号化されましたか？回答者数を図内に記載。

高等教育機関でもデータ暗号化率の減少傾向が続いており、2024 年の 77% から 58% へ減少し、過去 4 年間で最低となりました。これは歓迎すべき動向ですが、業界平均値の 50% よりはまだ高い水準です。

さらに良いニュースがあります。**暗号化される前に攻撃を阻止した割合**がほぼ倍増し、21% から 38% に増加しました ( ただし、業界平均の 44% には達していません )。これは防御力の向上を示す一方で、高等教育機関が依然として、複雑な IT 環境やレガシーインフラ、広範かつ分散したユーザー基盤を抱えていることから、脆弱なままである実態も浮き彫りになっています。

**図 7：高等教育機関に対するランサムウェア攻撃におけるデータ暗号化率 2022 ～ 2025 年**




ランサムウェア攻撃でデータは暗号化されましたか？回答者数を図内に記載。

## データの窃取

サイバー攻撃者はデータを暗号化するだけでなく盗み出します。高等教育機関はより大きなリスクに直面しており、被害者全体の 19%、データが暗号化された被害者のうち 33% がデータ窃取を報告しています。一方、初等中等教育ではこの値はそれぞれ 7% と 26% にとどまっています。これは、高等教育機関が保有しているデータの価値が高く、システムが分散し、広範に外部からアクセスされる環境になっていることから、検知や管理がより難しいことが原因と考えられます。この傾向は攻撃を防御できた成果とも一致しており、初等中等教育機関はデータが暗号化される前に 67% の攻撃を阻止したのに対し、高等教育機関は 38% にとどまっています。

## 恐喝型攻撃

表 6 および 7 に示すように、データは暗号化されなかったものの身代金を要求された ( 恐喝された ) 教育機関の割合は、この 1 年でわずかに増加しています。初等中等教育では 2024 年の 1% から 4% に、高等教育では 2024 年の 2% から 3% に上昇しており、防御が強化される中で攻撃者の手口が変化していることを示唆しています。

全体を見ると、初等中等教育機関は、ランサムウェア攻撃の影響を最も効果的に防いでいる ( データ暗号化の阻止、データ外部流出の防止、恐喝型攻撃の回避ができている ) と考えられます。これは、初等中等教育機関では予算が限られているにもかかわらず、早期の検知・対応において驚くほど効果を発揮していることを示しています。

## 教育業界における暗号化されたデータの復旧

データを暗号化された教育機関の 97% が、データを復元することができました。

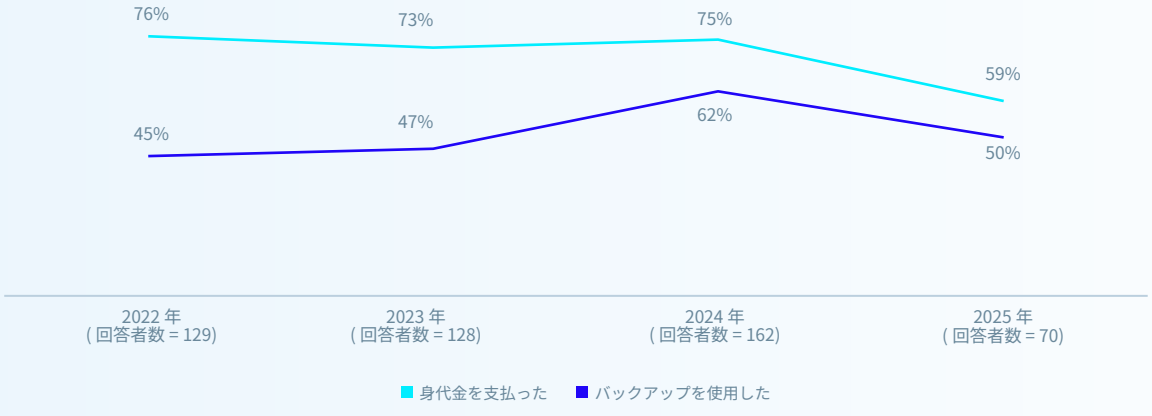
初等中等教育機関がデータを復旧するために**バックアップを利用した割合**は、2024 年の 75% から大幅に減少し、過去 4 年間で最低の 59% となりました。しかしながら、初等中等教育機関が今年の調査でデータを復旧するためにバックアップを使用する割合は、全業界の上位 4 位に入っています。

また、初等中等教育機関の半数が**身代金を支払ってデータを取り戻しています**。これは全業界平均の 49% とほぼ同じ水準です。身代金を支払う割合は、前年の 62% から顕著に減少したものの、過去 4 年間で初等中等教育機関における身代金支払いの割合としては 2 番目に高い数値となっています。

初等中等教育機関で、身代金を支払ってデータを復旧する割合と、バックアップを用いて復元する割合の差が縮小していることは、複数の復旧方法や代替の復旧方法への依存度が高まっていることを示しています。

この傾向を裏付けるように、データが暗号化された初等中等教育機関の 3 分の 1 (34%) が、**データ復旧に複数の方法を使用した**と回答しました。

**図 8：初等中等教育機関における暗号化されたデータの復旧 2022 ～ 2025 年**




データを復元できましたか？はい、身代金を支払ってデータを取り戻した。
はい、バックアップを使用してデータを復旧した。回答者数を図内に記載。

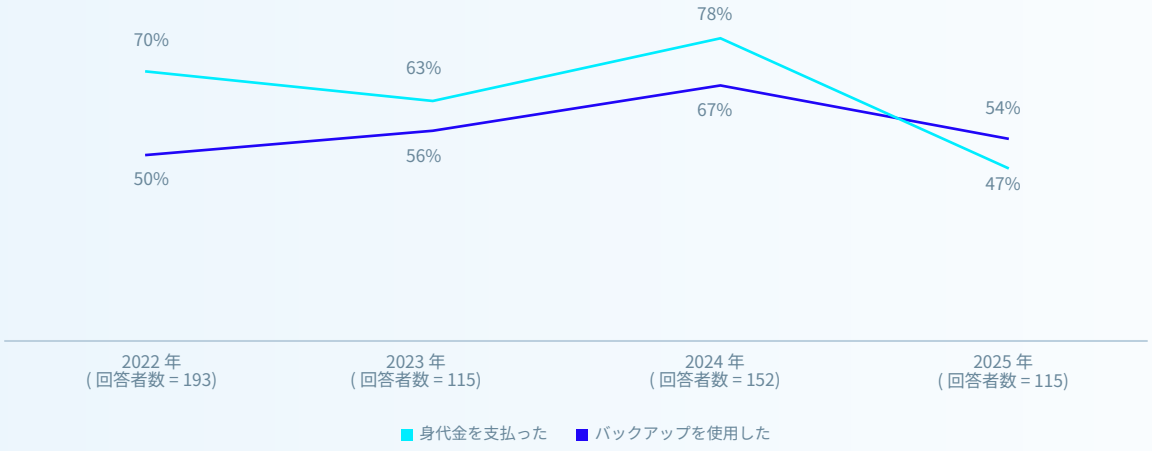
高等教育機関のうち、**バックアップを使用してデータを復元した割合**はわずか 47% で、2024 年の 78% から大幅に減少し、バックアップ利用率が低い業界の上位 3 位に入っています。これは、高等教育機関に多く見られる分散型の IT インフラ、複雑なデータ環境、レガシーシステム、バックアップの運用に一貫性がないことが影響している可能性があります。

また、高等教育機関の 54% が**身代金を支払ってデータを復旧**しており、全業界の平均である 49% をやや上回るものの、2024 年の 78% からは減少しており、歓迎すべき傾向です。

初等中等教育機関で観測されているように、高等教育機関でも身代金を支払ってデータを復旧する割合と、バックアップを使用してデータを復元する割合の差が縮小していることは、複数の復旧方法や代替の復旧方法への依存度が高まっていることを示しています。

この傾向を裏付けるように、データが暗号化された高等教育機関の 38% が**複数の方法を用いてデータを復旧した**と回答しており、これは全業界の中で 3 番目に高い割合となっています。

**図 9：高等教育機関における暗号化されたデータの復旧 2022 ～ 2025 年**




データを復元できましたか？はい、身代金を支払ってデータを取り戻した。
はい、バックアップを使用してデータを復旧した。回答者数を図内に記載。

# 身代金

## 教育機関に対する身代金要求額

**教育機関に対する身代金要求額の平均 ( 中央値 ) は、昨年に比べて大幅に減少しました。**初等中等教育に対する身代金要求額は、2024 年の 385 万ドルから 74% 減少し、102 万ドルに急落しました。一方、高等教育に対する要求額も 2024 年の 355 万ドルから 69.7 万ドルに減少し、調査対象となった全業界の中でも最も低い要求額の 1 つとなっています。

| | 2024 年 | 2025 年 |
|---|---|---|
| **初等中等教育機関** | **385 万ドル** ( 回答者数 =154) | **102 万ドル** ( 回答者数 =69) |
| **高等教育機関** | **355 万ドル** ( 回答者数 =130) | **69.7 万ドル** ( 回答者数 =112) |

*攻撃者から要求された身代金額はいくらでしたか？回答者数を図内に記載。*

業界全体における平均値も同様の傾向を示しており、2024 年の身代金要求額の平均は 200 万ドルから 2025 年には 34% 減少して 132 万ドルとなりました。

教育機関に対する身代金要求額の減少は、高額な身代金が要求されるケースが大幅に減少したことが主な要因です。初等中等教育機関では 500 万ドル以上の要求が 86% 減少し、高等教育機関では 100 万ドル以上の要求が 34% 減少しています。これは、攻撃者が高額な身代金を狙うのではなく、少額でも迅速に金銭を得る方向へと戦略を転換している可能性があります。

## 教育機関による身代金支払額

要求された身代金と同様に、初等中等教育機関および高等教育機関の**身代金支払額の平均 ( 中央値 )** も**昨年に比べて大幅に減少**しました。2024 年には全業界でも最も高い水準だった支払額が、2025 年には最も低い水準にまで下がっており、過剰な要求に対して教育機関がより効果的に抵抗できるようになっている可能性を示しています。

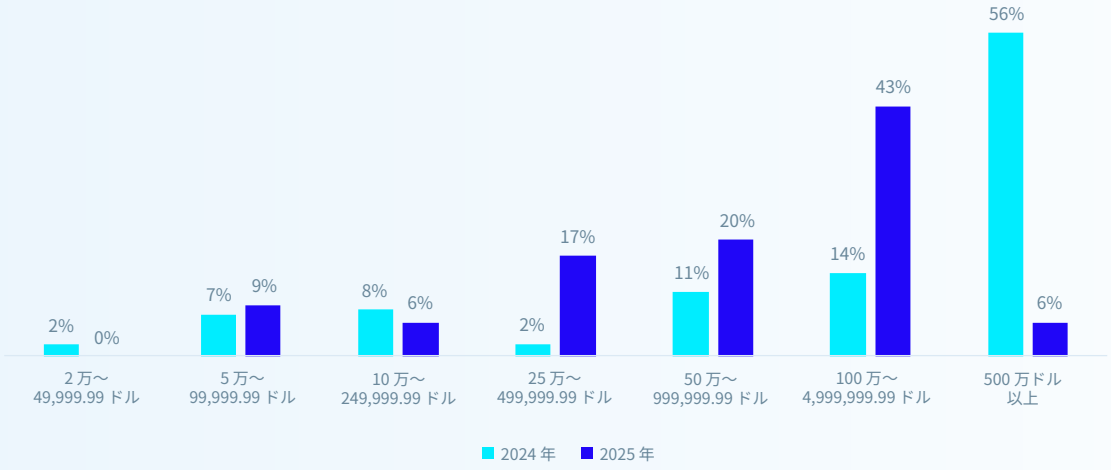
初等中等教育機関の支払額の中央値は、2024 年の 660 万ドルから 88% 減少して 80 万ドルに急落しました。高等教育機関の支払額も、2024 年の 441 万ドルからわずか 46.3 万ドルに減少し、今年の調査で記録された全業界の中で 4 番目に低い支払額となっています。

| | 2024 年 | 2025 年 |
|---|---|---|
| **初等中等教育機関** | **660 万ドル** ( 回答者数 =99) | **80 万ドル** ( 回答者数 =35) |
| **高等専門教育機関** | **441 万ドル** ( 回答者数 =92) | **46.3 万ドル** ( 回答者数 =65) |

攻撃者に支払った身代金はいくらでしたか？回答者数を図内に記載。

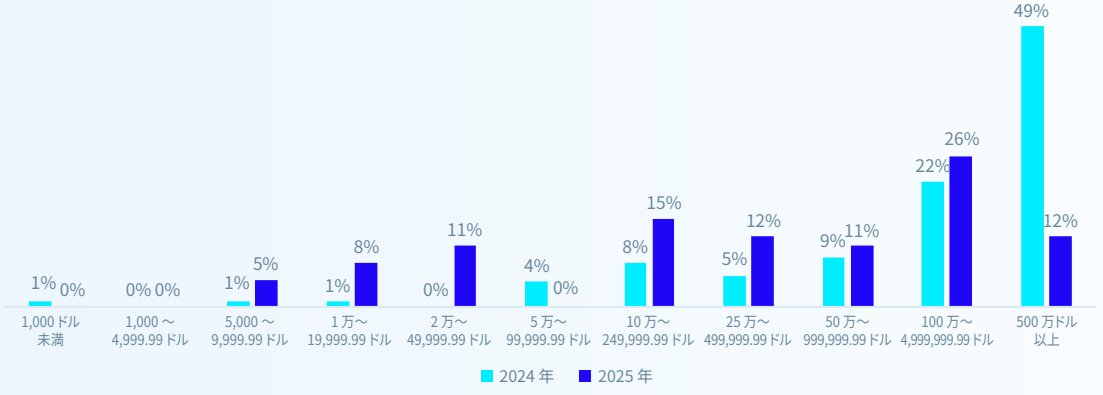
教育機関が支払う身代金が減少しているのは、主に 500 万ドル以上の高額な身代金を支払うケースが大幅に減少したためです。このようなケースは、初等中等教育機関では 89%、高等教育機関では 75% 減少しています。

**図 10：初等中等教育機関における身代金支払額 | 支払額の区分け**




攻撃者に支払った身代金はいくらでしたか？ 回答者数 = 35 (2025 年 )、99 (2024 年 )

**図 11：高等教育機関における身代金支払額 | 支払額の区分け**

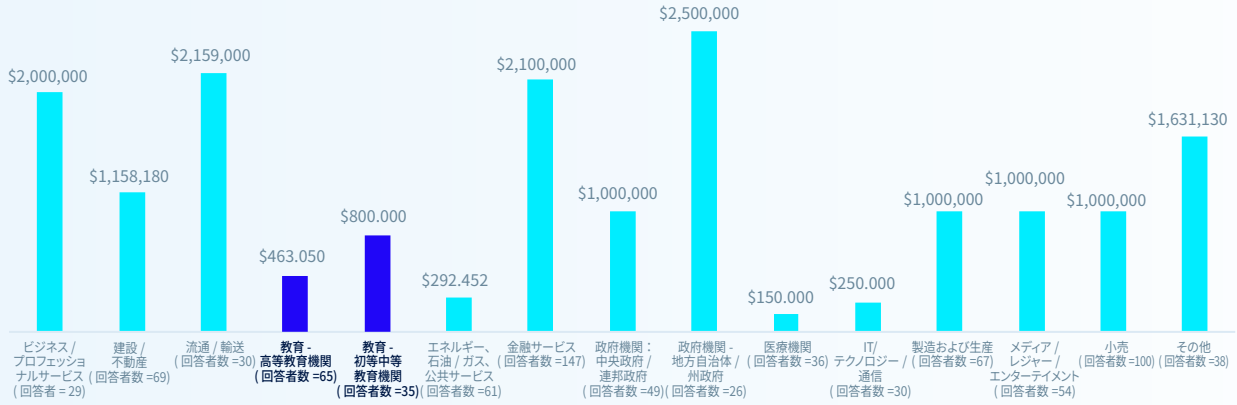



攻撃者に支払った身代金はいくらでしたか？ 回答者数 = 65 (2025 年 )、92 (2024 年 )

## 身代金の支払額 ( 業界別 )

身代金の支払額は業界によって大きく異なり、地方自治体 / 州政府が最も高く、攻撃者に支払った平均額は 250 万ドルでした。これは、重要なサービスを提供するというプレッシャー、サイバーレジリエンスが限定的であること、そして迅速に復旧しなければならないという焦りを攻撃者が悪用したためと考えられます。一方、医療機関は 15 万ドルと最も低い支払額でした。

**図 13：身代金の支払額 ( 業界別 )**

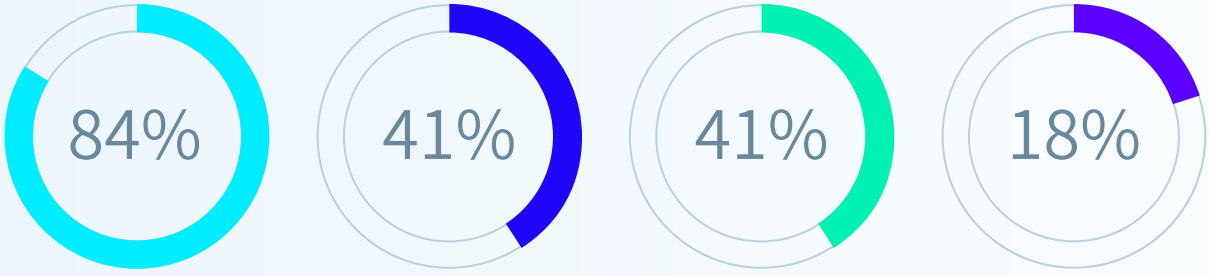



攻撃者に支払った身代金はいくらでしたか？回答者数を図内に記載。
注：ビジネス / プロフェッショナルと政府機関 ( 地方自治体 / 州政府 ) の回答者数は少ないため、調査結果は参照情報として扱ってください。

## 教育機関が実際に支払った金額と初回の要求額の比較

身代金を支払った初等中等教育機関 34 社が最初の身代金要求額と実際の支払額の両方を共有しており、平均すると初回の要求額の 84% を支払っていることが明らかになりました。この割合は、2024 年の 115% から減少しており、歓迎すべき結果です。全体では、41% が最初の要求額よりも少ない金額を支払っており ( 全業界平均の 53% を大きく下回る )、18% がより多く支払い、41% が最初の要求額と同額を支払っていました。

**身代金を支払った 34 の初等中等教育機関が最初に要求された身代金額と実際の支払額の両方を共有しており、以下の結果が明らかになりました。**




**実際に支払われた**
身代金の割合 ( 平均 )

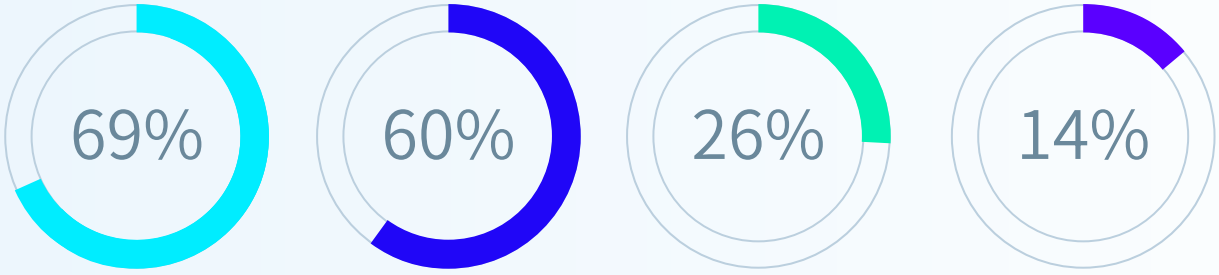
最初の要求額より**少ない**
身代金を支払った割合

最初の要求額と**同額の**
身代金を支払った割合

最初の要求額より**多い**
身代金を支払った割合

身代金を支払った高等教育機関 65 社が最初の身代金要求額と実際の支払額の両方を共有しており、平均すると初回の要求額の 69% を支払っていることが明らかになりました。これは、2024 年に記録された 122% から大幅に減少しており、今年の調査で記録された中で最も低い割合です。全体では、60% が最初の要求額よりも少ない金額を支払っており ( 全業界平均の 53% を上回る )、14% がより多く支払い、26% が最初の要求額と同額を支払っていました。

**身代金を支払った 65 の高等教育機関が最初に要求された身代金額と実際の支払額の両方を共有しており、以下の結果が明らかになりました。**




**実際に支払われた**
身代金の割合 ( 平均 )

最初の要求額より**少ない**
身代金を支払った割合

最初の要求額と**同額の**
身代金を支払った割合

最初の要求額より**多い**
身代金を支払った割合

## 教育機関が支払った身代金の大半の金額が最初の要求額と異なる理由

今年は初めて、一部の教育機関が初回の要求額よりも少ない金額を支払っている理由について調査を行い、ランサムウェア攻撃への対応における重要な要因を明らかにしました。

最初の要求額よりも**少なく支払った** 15 の**初等中等教育機関**が明らかにした理由を以下に示します。

- 67%：攻撃者が支払いを促すために要求額を下げた ( 今年の調査では、この要因の割合が最高 )
- 60%：身代金を迅速に支払ったため割引を受けた。
- 53%：メディアや法執行機関など外部からの圧力により、攻撃者が要求額を引き下げた。
- 53%：第三者が攻撃者と交渉し、支払い額を下げた。
- 33%：攻撃者と交渉して支払額を下げた。

** 注：回答数が非常に少ないため、調査結果はあくまで参考値です。*

一方、最初の要求額より**少なく支払った** 39 の**高等教育機関**は、支払額を減らせた理由を以下のように説明しています。

- 59%：攻撃者と交渉して支払額を下げた ( 今年の調査では、この要因の割合が最高 )
- 46%：身代金を迅速に支払ったため割引を受けた。
- 44%：攻撃者が支払いを促すために要求額を下げた。
- 41%：第三者が攻撃者と交渉し、支払い額を下げた。
- 38%：メディアや法執行機関など外部からの圧力により、攻撃者が要求額を引き下げた。

最初の要求額よりも少ない金額を支払った理由については、初等中等教育機関と高等教育機関では大きく異なります。初等中等教育機関は、**攻撃者が支払いを促すために要求額を下げた**ことを主な理由として挙げているのに対し、高等教育機関は、支払額を抑えられた主な要因として**交渉の成功**を挙げています。これは、高等教育機関が今回の調査で身代金の支払額が最も低い業界の 1 つとなった背景の一因と考えられます。

最後に、初等中等教育機関と高等教育機関はいずれも、身代金支払額が少なくなった理由として複数の要因 ( それぞれ 3 つと 2 つ ) を挙げており、ランサムウェアの被害を受けた組織が複雑で多面的な状況に直面していることが改めて浮き彫りになっています。

# ランサムウェアによるビジネスへの影響

## 教育機関における復旧コスト

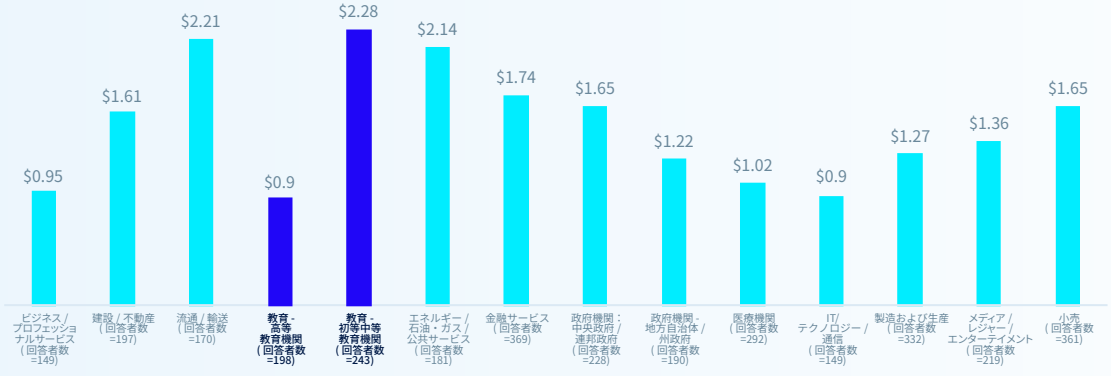
2025 年、教育機関における復旧コストの平均 ( 中央値 ) は大幅に減少しました ( 身代金支払いを除く )。高等教育機関では復旧コストが 77% 減少して 90 万ドルとなり、調査対象となった中で最も低い業界の 1 つとなりました。対照的に初等中等教育機関は、2024 年の 376 万ドルから 39% 減少したものの、復旧コストは 228 万ドルであり、調査対象業界の中で平均復旧コストが最も高くなりました。これは、初等中等教育機関では IT リソースが限られていたり、システムが旧式化や断片化したりしていることが影響している可能性があります。

| | 2023 年 | 2024 年 | 2025 年 |
|---|---|---|---|
| 初等中等教育機関 | 159 万ドル ( 回答者数 =159) | 376 万ドル ( 回答者数 =197) | 228 万ドル ( 回答者数 =243) |
| 高等専門教育機関 | 106 万ドル ( 回答者数 =157) | 402 万ドル ( 回答者数 =190) | 90 万ドル ( 回答者数 =198) |

最も深刻なランサムウェア攻撃の影響において、組織が復旧に要した概算コスト ( ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益など ) は、支払った身代金を除いて、どれぐらいですか？回答者数を図内に記載。

業界別に見ると、復旧コストの状況は大きく異なります。インシデントの平均復旧コストについては、初等中等教育機関に次いで、流通 / 輸送業が 221 万ドルと最も高い数値を報告しました。一方、IT/ テクノロジー / 通信業界は、高等教育と並んで 90 万ドルで最も低いコストを報告しました。

**図 12：業界別の別のランサムウェア攻撃の復旧コスト**



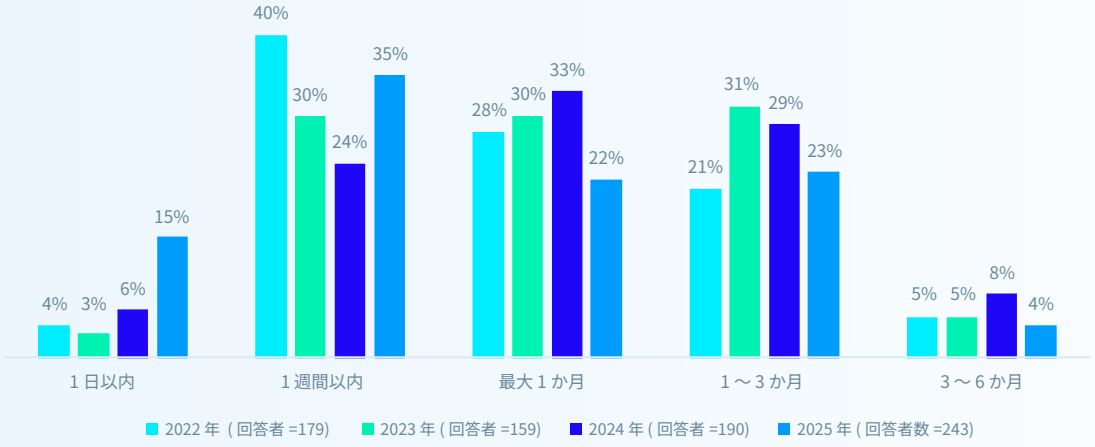

最も深刻なランサムウェア攻撃の影響において、組織が復旧に要した概算コスト ( ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益など ) は、支払った身代金を除いて、どれぐらいですか？回答数を図内に記載。調査結果は参照情報として扱ってください。

## 教育機関の復旧時間

データによると、2025 年には**教育機関はランサムウェア攻撃で受けた影響をより迅速に復旧したことが明らかになっています。**初等中等教育機関の半数、および高等教育機関の 59% が、1 週間以内に攻撃による影響から完全に復旧しています。この数値はいずれも 2024 年の 30% から大幅に上昇しています。一方、復旧に 1 ～ 3 か月かかった割合は、初等中等教育機関で 29% から 23%、高等教育では 34% から 14% に減少しました。

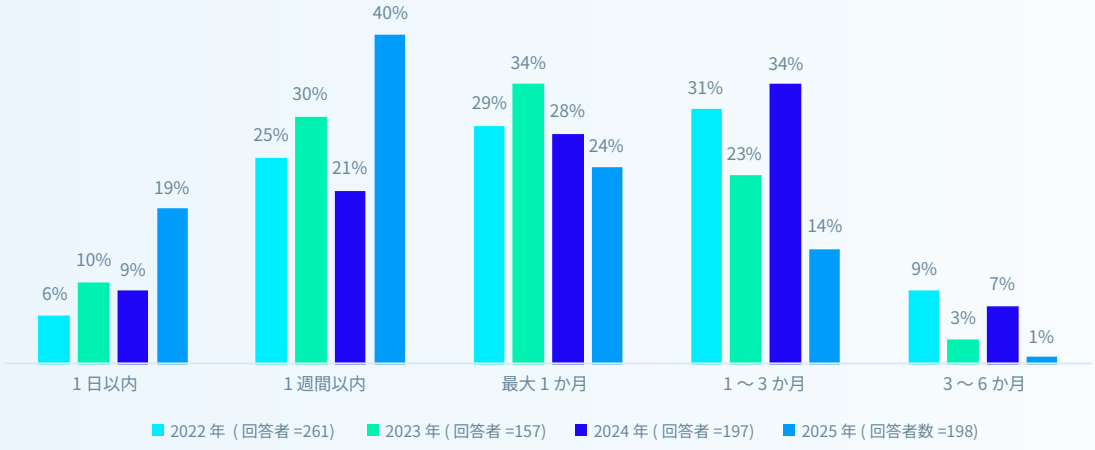
全体として、被害を受けた教育機関の 95% が 3 か月以内に完全に復旧しており、業界全体のレジリエンスと復旧能力の向上が浮き彫りになっています。

**図 13：教育機関におけるランサムウェア攻撃からの復旧時間 2022 ～ 2025 年**




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

**図 14：高等教育機関におけるランサムウェア攻撃からの復旧時間 2022 ～ 2025 年**




予想されることではありますが、データが暗号化された教育機関は、暗号化を阻止できた組織よりも復旧に時間がかかる傾向があります。1 日で完全復旧したのは、データが暗号化された組織では 13% であったのに対し、暗号化を阻止できた組織では 19% になっています。

# ランサムウェアによる人材への影響

今回の調査によると、教育業界では、ランサムウェア攻撃でデータが暗号化された場合、IT/ サイバーセキュリティチームは大きな影響を受けています。回答者全員が、自身のチームが何らかの形で影響を受けたと述べています。

**図 15：データが暗号化されたことによる IT/ サイバーセキュリティチームへの影響**

| 初等中等教育機関 | | 高等教育機関 | |
|---|---|---|---|
| 41% | シニアリーダーからの**プレッシャー**の増加 | 53% | シニアリーダーからの**プレッシャー**の増加 |
| 40% | 継続的な**業務量**の増加 | 50% | **チームや組織**構造の変更 |
| 37% | 今後の攻撃に対する**不安やストレス**の増加 | 40% | 今後の攻撃に対する**不安やストレス** の増加 |
| 37% | 攻撃を阻止できなかったことへの**罪悪感** | 37% | 継続的な**業務量**の増加 |
| 36% | シニアリーダーからの**評価**の向上 | 36% | 攻撃を阻止できなかったことへの**罪悪感** |
| 34% | **チームの優先事項や注力領域**の変化 | 34% | シニアリーダーからの**評価**の向上 |
| 29% | **チームや組織構造**の変更 | 33% | チーム**リーダー**の交代 |
| 26% | **ストレスやメンタルヘルス**問題による スタッフの欠勤 | 31% | **チームや組織**構造の変更 |
| 26% | チーム**リーダー**の交代 | 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 |

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？回答者数 =70 ( 初等中等教育機関 )、115 ( 高等教育機関 )

# 提言

過去 1 年間で教育機関におけるランサムウェアへの対応にはいくつかの変化が見られましたが、ランサムウェアが深刻な脅威であることに変わりはありません。サイバー攻撃が繰り返され、進化し続ける中で、防御側の組織は自社のサイバー攻撃対策を、ランサムウェアや他の脅威の進化に合わせていかなければなりません。本レポートの洞察を活用し、防御体制を強化するとともに、脅威への対応力を高めることで、ランサムウェアがビジネスや人材に及ぼす影響を最小限に抑えてください。攻撃を未然に防ぐために、次の 4 つの重要な分野に重点的に取り組んでください。

- **予防**。ランサムウェアに対する最も効果的な防御は、攻撃を未然に防ぐこと、つまり、攻撃者による組織への侵入を許さないことです。本レポートで明らかになった技術的および運用面の根本原因を取り除くための対策を講じてください。
- **保護**。基盤となるセキュリティ機能を強化することは必須です。エンドポイントやサーバーは、ランサムウェアの主要な攻撃対象であるため、専用のランサムウェア対策機能を搭載しているエンドポイント保護製品を導入して、悪意のある暗号化を阻止してロールバックできるようエンドポイントの防御を徹底する必要があります。
- **検知と対応。**攻撃をできる限り早期に阻止できれば、影響も軽減することができます。24 時間体制の脅威検知と対応は、今や不可欠な防御層となっています。社内のリソースやスキルが不足している場合は、信頼できる MDR プロバイダーと連携することを検討してください。
- **計画と準備。**インシデント対応計画を策定し、計画をテストしておけば、最悪の事態が発生し、大規模な攻撃を受けた場合でも、攻撃の影響を最小限に抑えることができます。データを迅速に復旧できるよう、質の高いバックアップを作成し、バックアップから復旧するテストを定期的に実施してください。

ソフォスがランサムウェア対策の最適化を支援する方法について、ソフォスのアドバイザーにご相談いただくか、www.sophos.com をご覧ください。

## 最新のランサムウェア情報と、ソフォスが組織をどのように保護するかをご確認ください。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。



2025-08-28 WP (NP)