SOPHOS

小売業界の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 16 か国の組織に所属する、IT およびサイバーセキュリティリーダー 3,400 人 (うち小売業界 361 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

ソフォスの「小売業界のランサムウェアの現状」レポートは今回で 5 年目を迎えました。本レポートでは、2025 年の小売業界におけるランサムウェアの最新情報をお伝えします。

今年のレポートでは、小売業者がこの 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、小売業が攻撃を受けることとなった運用上の要因や、小売業の 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も調査結果をお伝えします。

このレポートは、過去 1 年間にランサムウェアの被害を受けた 16 か国 361 人の小売業界の IT リーダーとサイバーセキュリティリーダーの現場での実体験に基づいており、以下のような貴重な洞察を提供しています：

- 小売業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ビジネスへの影響
- ランサムウェアによる人材への影響

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、2025 年 1 月から 3 月にかけてソフォスの依頼の元で、特定のベンダーに依存しない立場から、サードパーティの専門機関が実施した、ランサムウェアに関する組織の経験についての調査の結果に基づいています。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。

本レポートに含まれる 361 社の小売企業の回答者は、16 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

組織がランサムウェアの被害に遭う理由

- 被害を受けた小売業は、3 年連続で**脆弱性の悪用**が最も多い技術上の根本原因として挙げており、脆弱性は全体の 30% のインシデントで悪用されていました。
- 組織がランサムウェアの被害を受ける背景には、いくつかの運用上の要因があります。中でも最も多かったのは**組織が把握していなかったセキュリティギャップ**で、被害組織の 46% がこの要因を挙げています。これに僅差で続くのは、攻撃の 45% で要因となった**専門知識の不足**です (45% は調査対象となった全業界の中で最も高い割合)。3 番目に多かったのは、**保護機能の不足**で、44% の攻撃で要因として挙げられています。

データへの影響

- 小売業界における**データの暗号化**率は過去 5 年間で最も低い水準となりました。現在は攻撃の 48% でデータが暗号化されており、2023 年の 71% から大幅に減少しています。
- データが暗号化された小売業の 29% 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小売業の 98% が、データを復元することができました。
- 小売企業が暗号化されたデータを**バックアップ**から復旧する割合は過去 4 年間で最も低くなり、インシデント全体の 62% でしか使用されていませんでした。
- 小売業の被害組織の 58% がデータを取り戻すために**身代金を支払って**います。身代金を支払う割合は、前年の 60% からわずかに減少したものの、過去 5 年間で 2 番目に高くなっています。

身代金：要求額と支払額

- 小売企業に対する平均 (中央値) での**身代金要求額**は、昨年比で 2 倍に増加し、2024 年の 100 万ドルから 2025 年には 200 万ドルに達しました。この大幅な増加の主な要因は、500 万ドル以上の身代金支払いの割合が、2024 年の 17% から 2025 年には 27% へと 59% 増加したことによるものです。
- しかし、平均 (中央値) の**身代金支払額**は、2024 年の 95 万ドルから 2025 年に 100 万ドルへと、過去 1 年間でわずか 5% の増加に留まっています。これは、小売企業が過大な身代金要求に対してより抵抗を示すようになっていると考えられます。
- 小売業が**支払った身代金要求額の割合**は、2024 年の 85% から 2025 年には 81% に減少しました。
- **要求額と支払額**を詳細に分析すると、最初の要求額と同額を支払ったと回答した小売企業はわずか 29% でした。59% が最初の要求額よりも少ない金額を支払っており、11% がより多くの金額を支払っていました。

ランサムウェアによるビジネスへの影響

- 小売業における**ランサムウェア攻撃からの復旧にかかる平均コスト**は、昨年比 40% 減の 165 万ドルとなり、2024 年の 273 万ドルから減少しました。
- **復旧のスピード**を見ると、小売企業は復旧が速く、攻撃から 1 週間以内に復旧した割合は 2024 年の 46% から、2025 年には 51% に上昇しています。

ランサムウェアによる人材への影響

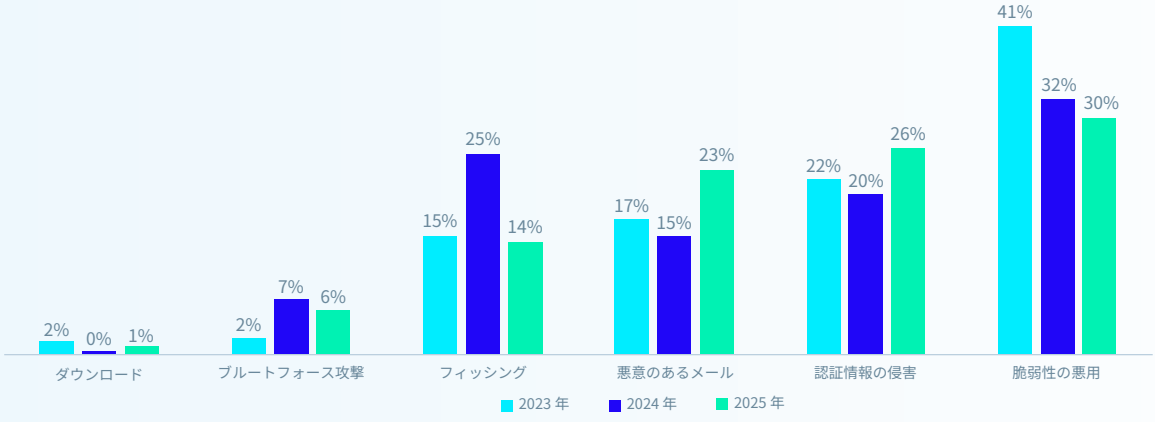
- データが暗号化されたすべての小売企業において、IT/ サイバーセキュリティチームに以下のような**直接的な影響**があったことが報告されています。
  - 小売企業の IT/ サイバーセキュリティチームのほぼ半数 (47%) が、シニアリーダーからの**プレッシャーが増加した**と答える一方で、30% は**評価が高まった**と報告しています。
  - 小売企業の回答者の 43% が、IT/ サイバーセキュリティチームへの影響として、今後の攻撃に対する不安やストレスの増加と、業務負荷の**継続的な増加**の両方を挙げました。
  - 41% が、インシデントの結果として**チーム / 組織構造**の変更を回答しました。
  - 37% 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。
  - 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。
  - 4 分の 1 (26%) のケースでは、攻撃を受けたことを理由に**チームのリーダーが交代**させられました。

組織がランサムウェアの被害に遭う理由

攻撃の技術的な根本原因

3 年連続で、被害を受けた小売企業は脆弱性の悪用が最も多い技術上の根本原因として挙げており、脆弱性は攻撃の 30% で組織に侵入するために悪用されていました。認証情報の侵害は、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 20% から 2025 年には 26% に増加しました。メールは依然として主要な攻撃手法であり、小売企業の 23% がフィッシングを根本原因としており (2024 年の 15% から大幅な増加)、さらに 14% が悪意のあるメールを挙げています。

図 1：小売業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

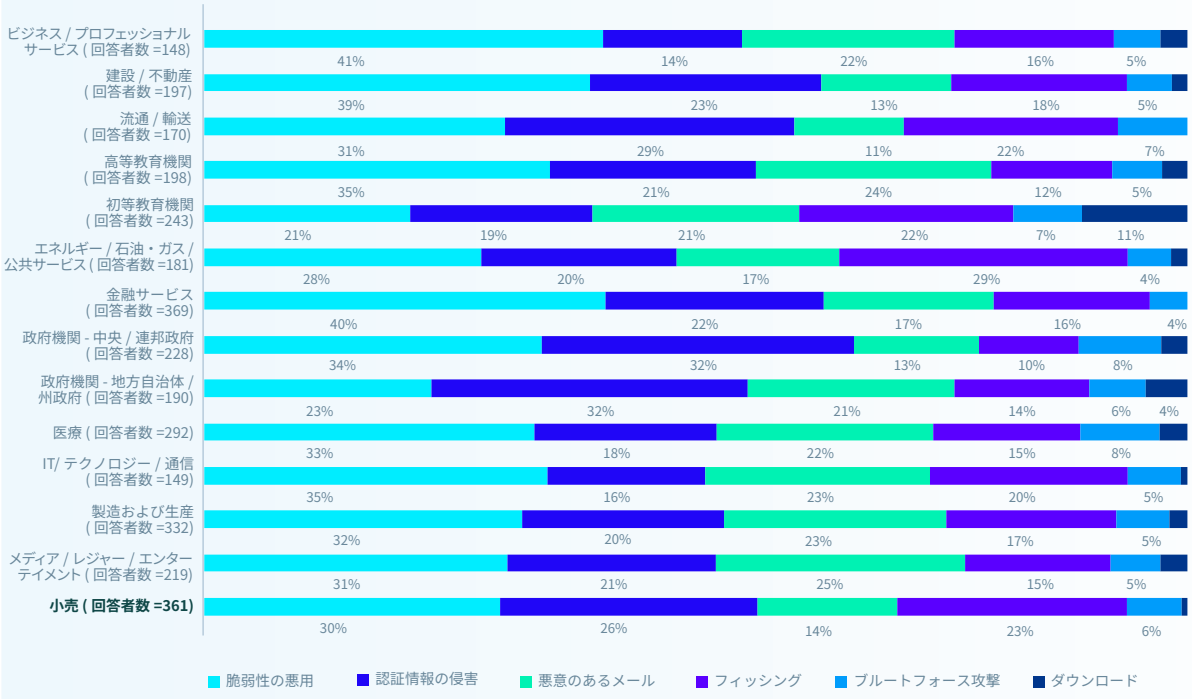


過去 1 年間に受けたランサムウェア攻撃の根本原因を把握していますか？はい。 回答者数 =359 (2025 年)、261 (2024 年)、243 (2023 年)。

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 (101%)** (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**で最も多い攻撃経路であり、インシデントのほぼ 3 分の 1 (32%) を占めています。

図 2：業界別のランサムウェア攻撃の技術的な根本原因

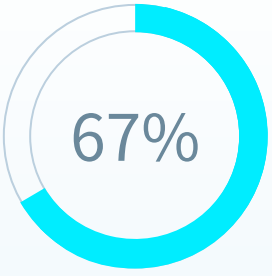


過去 1 年間に受けたランサムウェア攻撃の根本原因を把握していますか？はい。回答者数を図内に記載。

小売業におけるインシデントの組織的根本原因

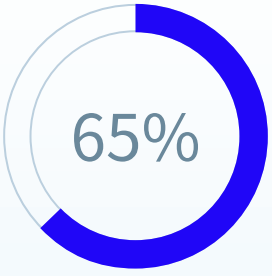
今年のレポートでは初めて、小売企業がランサムウェア攻撃を受けることになった組織的な要因に焦点を当てています。調査結果によると、被害を受けた小売企業は一般的に複数の組織的課題を抱えており、回答者は平均して 2.9 個の要因が攻撃の一因になったと述べています。

全体として、保護に関する問題、リソースの問題、セキュリティギャップの 3 つが、ほぼ同じ割合で組織的な根本原因として挙げられています。ただし、小売企業では、既知および未知のセキュリティギャップを主な要因として挙げる傾向がやや強く見られます。



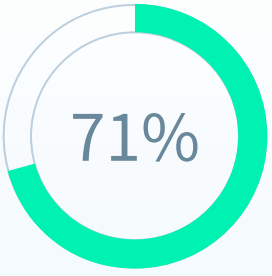
保護機能の問題

保護機能の不足または攻撃を阻止できなかった質の低いセキュリティソリューション



リソースの問題

人間の専門知識 (スキルや能力) が不足しており、攻撃を適切なタイミングで検知して防止できない



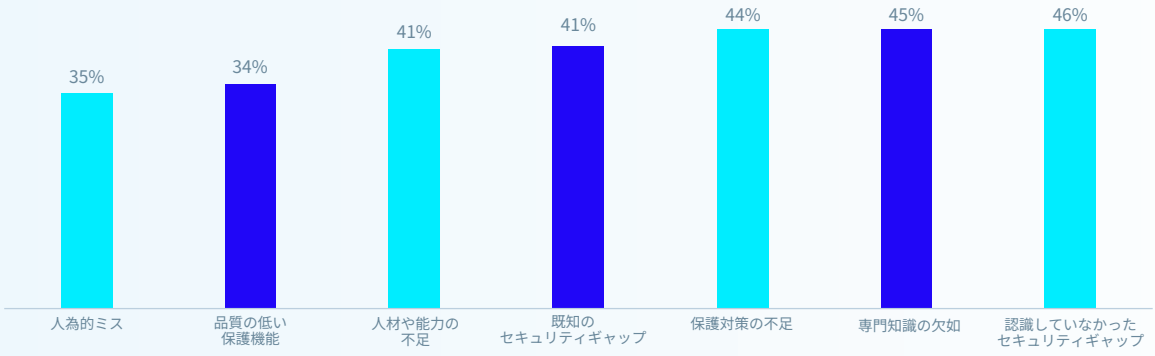
セキュリティギャップ

防御体制に、既知または未知の弱点があった

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＝ 361 集計結果。

未知のセキュリティギャップ (組織自身も認識していなかった防御上の弱点) が最も一般的な要因で、小売業の回答者の 46% が挙げています。これに僅差で続くのが専門知識の不足 (攻撃を適切なタイミングで阻止するためのスキルや知識が不十分であること) で攻撃の 45% を占めており、この特定の組織的根本原因において、全業界で最も高い割合となっています。3 位は保護対策の不足 (必要なサイバーセキュリティ製品やサービスが導入されていない状態) で、攻撃の 44% で要因として挙げられています。

図 3：小売企業に対するランサムウェア攻撃の運用面の根本原因

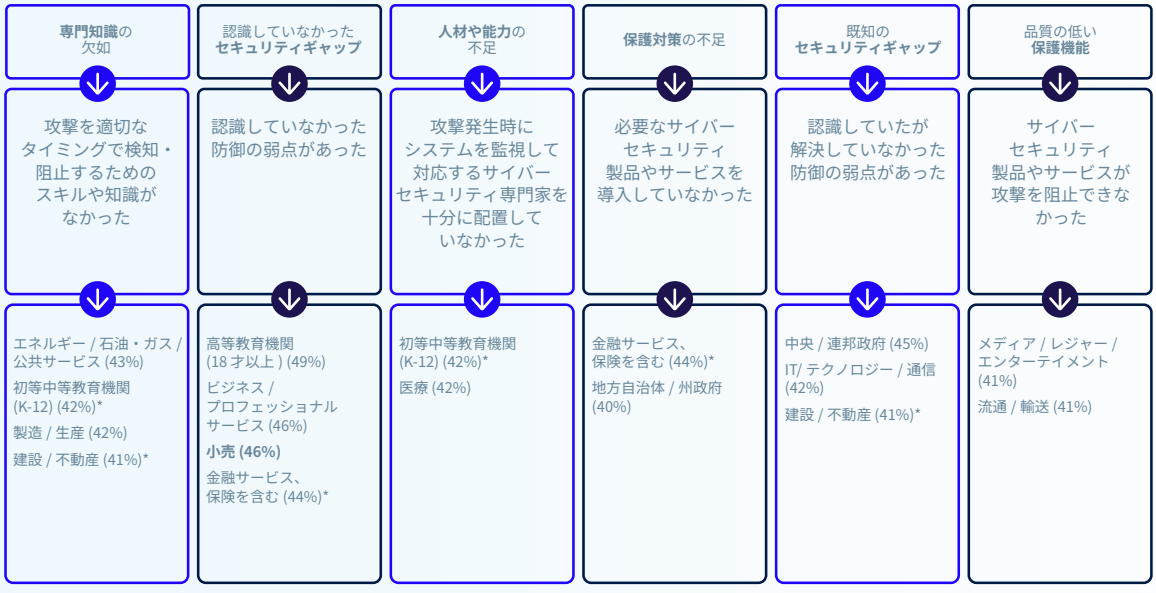


自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 回答者数＝ 361

業種別の組織的な根本原因

最も多い組織的な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 4：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



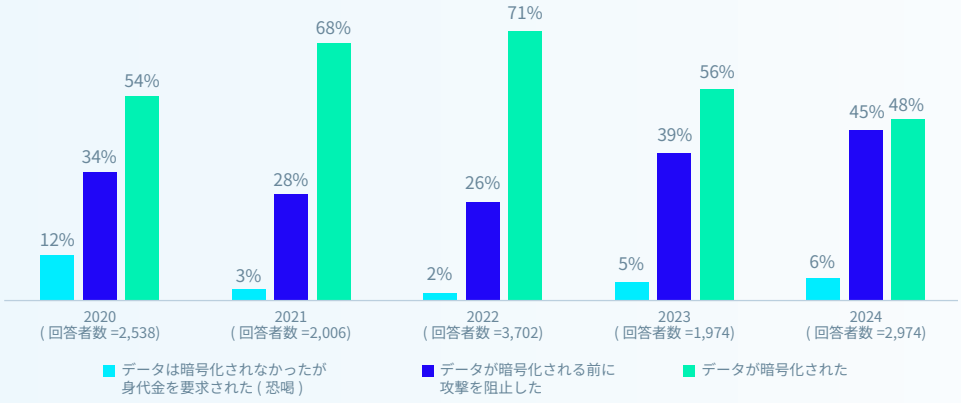
自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 回答者数＝ 3,400 業界別の内訳。

データへの影響

小売業におけるデータの暗号化

朗報として、ソフォスが過去 5 年間にわたって実施した調査の中で、小売企業のデータが暗号化された割合は今回が最も低く、攻撃によってデータが実際に暗号化されたケースは全体の 48% にとどまりました。過去 2 年間でデータが暗号化された攻撃の割合は、2023 年の調査の 71% から顕著に減少しました。これは、データが暗号化される前に攻撃を阻止する小売企業の能力が高まっていることを示しています。

図 5：小売業に対するランサムウェア攻撃のおけるデータ暗号化率 2021 ～ 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。

業界別のデータ暗号化率

流通・運輸業界の組織は、データが暗号化される割合が最も高い (64%) ですが、これは、この業界の組織は暗号化が始まる前に攻撃を検知・阻止する能力が低いことや、悪意ある暗号化をブロックおよびロールバックする能力が低いことを示しています。一方、**初等中等教育機関**ではデータ暗号化率がわずか 29% と最も低く、全業界の平均である 50% を大幅に下回っています。

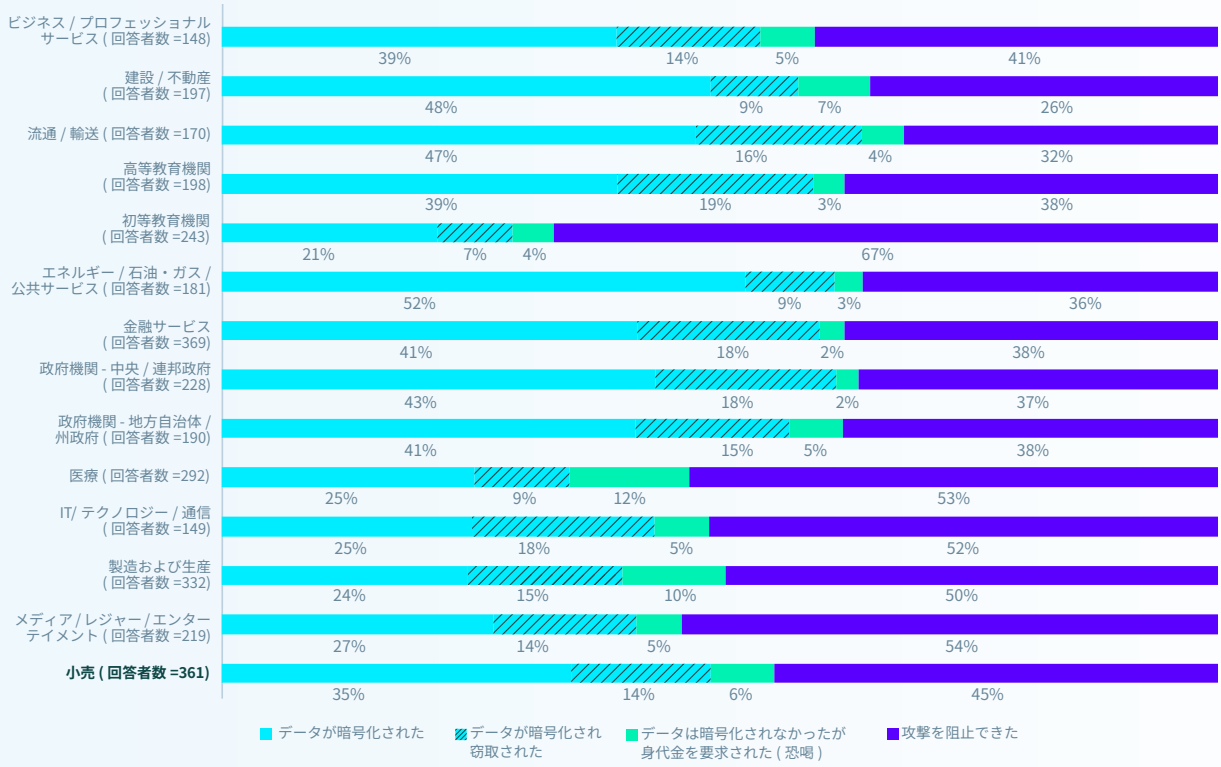
データの窃取

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。小売業界では、ランサムウェア被害者の 14% と、データを暗号化された被害組織の 29% がデータの盗難を経験しています。業界別に見ると、次のことがわかります。

- **IT/ テクノロジー / 通信**業界では、データを暗号化された組織の 42% がデータ盗難の被害も受けています。
- 一方、建設 / 不動産業界および**エネルギー / 石油・ガス / 公共サービス**業界では、暗号化と併せてデータ盗難を経験した組織は 15% に留まっています。

この差異は、小規模な組織の方がデータ窃取を防げている可能性もありますが、一方で、攻撃者が大規模組織を標的にしてデータ窃取を試みる傾向が強いことや、小規模な組織ではデータ窃取を特定しにくい可能性があることも要因として考えられます。

図 6：データの暗号化と窃取 (業界別)



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。

恐喝型攻撃

図 5 に示しているように、データが暗号化されていないにもかかわらず身代金を要求される (恐喝型) 攻撃を受けた小売企業の割合は、3 年間で最高水準に達し、2023 年の 2% から 2025 年には 6% と 3 倍になりました。

業界別に見ると、**医療機関**が最も多くの恐喝型攻撃を受けています (12%)。これは、医療データ　(カルテなど) の機密性が高いことが要因と考えられます。一方、**金融サービス**プロバイダーと**中央 / 連邦政府**機関は、これらの攻撃を受けた経験が最も少なく、いずれも 2% に留まっています。

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。

小売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小売業の 98% が、データを復旧することができました。

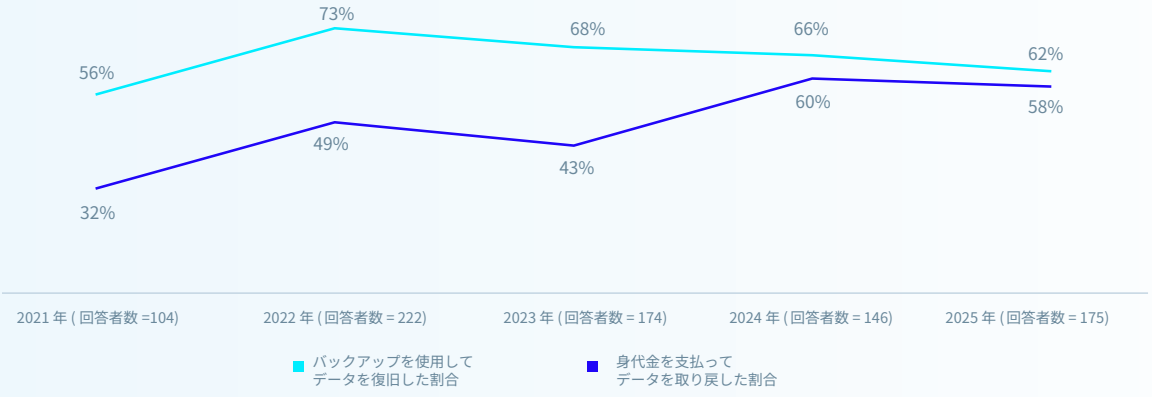
小売企業の 62% が**バックアップを使用**してデータを復旧しました。これは 4 年間で最も低い割合ですが、業界別のバックアップ利用率では依然として上位 3 位に入っています。

業界内の 58% が**身代金を支払い、データを取り戻しています**。身代金を支払う割合は、前年の 60% からわずかに減少したものの、過去 5 年間で小売業における身代金支払いの割合としては依然として 2 番目に高い水準です。

身代金を支払ってデータを復旧する小売企業と、バックアップを使用してデータを復元する小売業の間の差が縮まっていることは、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小売企業の 39% が、**データ復旧に複数の方法を使用した**と回答しました。この割合を上回る業界は他にありませんでした。

図 7：小売業界における暗号化されたデータの復旧 2021 ～ 2025 年



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

身代金

小売業に対する身代金要求

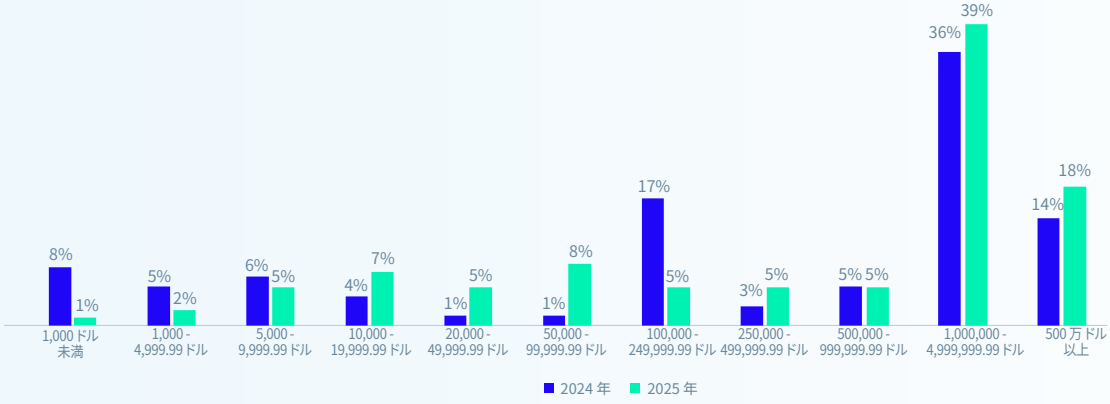
小売企業に対する平均 (中央値) での身代金要求額は、過去 1 年間で 2 倍に増加し、2024 年の 100 万ドルから 2025 年には 200 万ドルに達しました。小売業を標的とした身代金要求額の増加は、主に過去 1 年間で 500 万ドル以上の要求が 59% 増加したことによるものです。さらに、小売企業に対する身代金要求の 63% が 100 万ドルを超え、2024 年の 50% から急増しています。

一方、全業界の平均は、2024 年の 200 万ドルから 2025 年には 132 万ドルへと 34% 減少しています。

小売業の身代金支払額

身代金の要求額が急増したにもかかわらず、小売企業による身代金支払額の平均 (中央値) は 5% しか上昇していません。これは、小売企業が過大な身代金要求に対してより抵抗を示すようになっていると考えられます。ただし、小売企業が支払った身代金の中央値は緩やかに増加していますが、分布を見ると、全体として身代金支払額が高額化する傾向が見られ、小規模な支払いは明らかに減少しており、100 万ドルを超える支払いをした組織は増加しています。

図 8：小売業界における身代金支払額 | 支払額の区分け

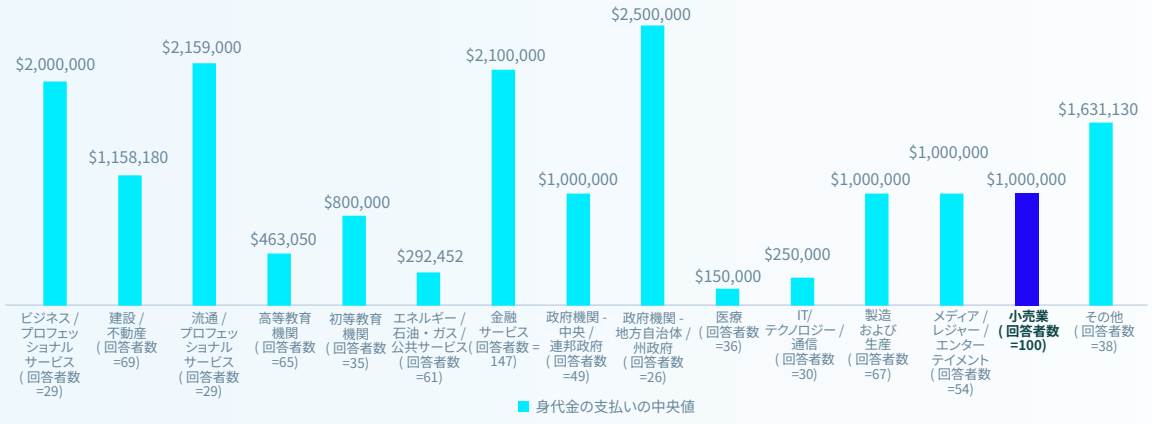


攻撃者に支払った身代金はいくらでしたか？ 回答者数 = 100 (2025 年)、78 (2024 年)

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い額でした。

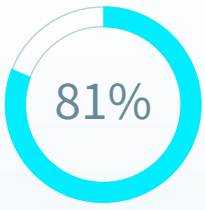
図 9：身代金の支払額 (業界別)



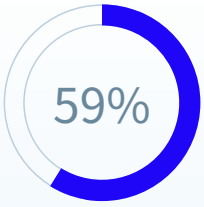
攻撃者に支払った身代金はいくらでしたか？回答者数を図内に記載。注：ビジネス / プロフェッショナルと政府機関 (地方自治体 / 州政府) の回答者数は少ないため、調査結果は参照情報として扱ってください。

小売企業が実際に支払った金額と初回の要求額の比較

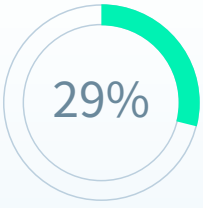
身代金を支払った小売企業 100 社が最初の身代金要求額と実際の支払額の両方を共有しており、平均すると初回の要求額の 81% を支払っていることが明らかになりました。この割合は、2024 年の 85% から減少しており、歓迎すべき結果です。全体では、59% が最初の要求額よりも少ない金額を支払っており (全業界平均の 53% を上回る)、11% がより多く支払い、29% が最初の要求額と同額を支払っていました。



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

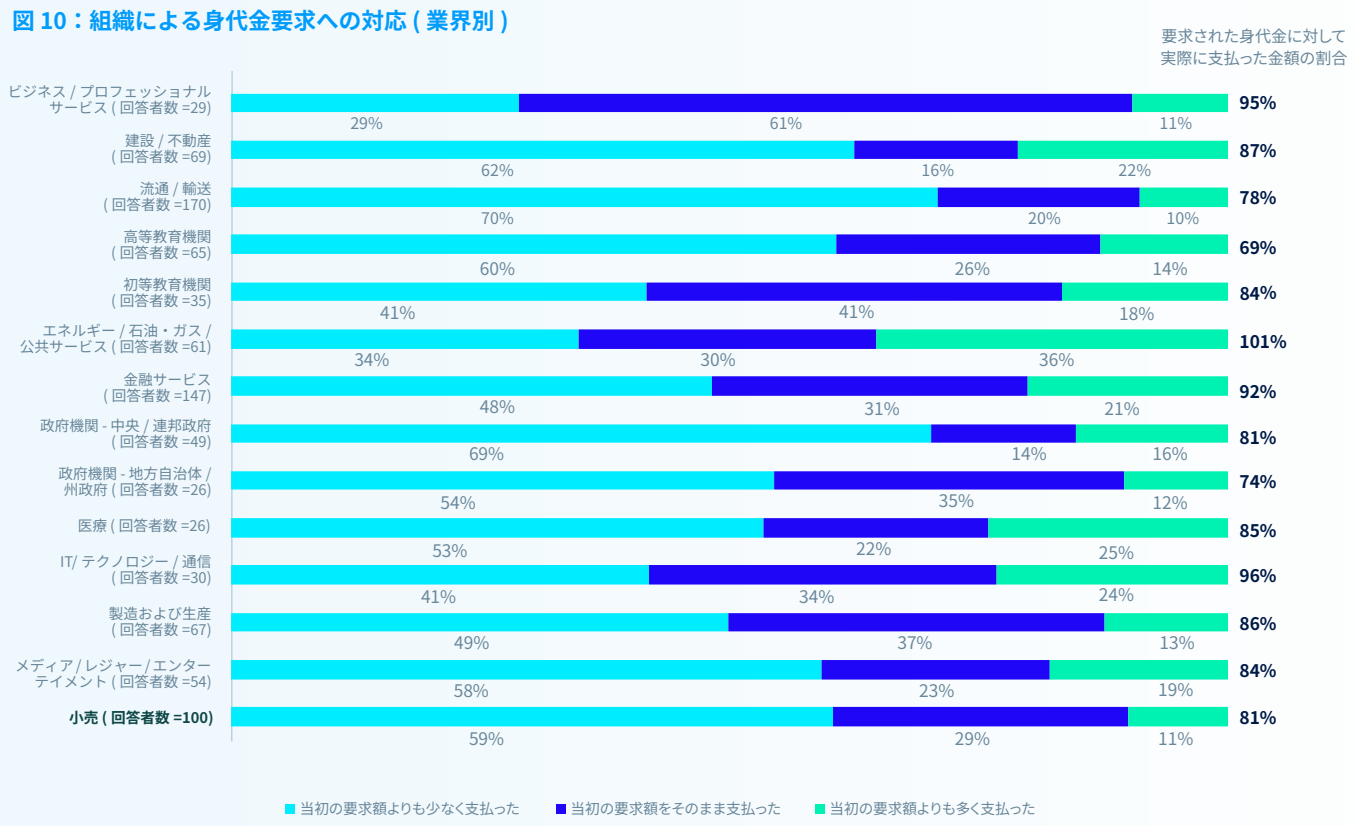


最初の要求額と**同額の**
身代金を支払った割合

最初の要求額より**多い**
身代金を支払った割合

業界別に見ると、幸いなことに、大多数の業界が最初の要求額よりも少ない金額を支払っていました。**流通・運輸**業界の組織は、最初の身代金要求額よりも少ない金額を支払った割合が最も高く (70%)、身代金要求に対する強い抵抗を示しています。一方、**エネルギー / 石油・ガス / 公共サービス**業界は、最初の要求額よりも多く支払った割合が最も高く (36%)、**ビジネス / プロフェッショナルサービス**業界は、最初の要求額と同額を支払った割合が最も高かったです (61%)。

図 10：組織による身代金要求への対応 (業界別)



攻撃者に支払った身代金はいくらでしたか？
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。回答者数を図内に記載。

小売企業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、一部の小売企業が初回の要求額を上回る金額を支払っている理由と、他の組織がそれを下回る支払いにとどめ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**多く支払った** 11 の小売企業が明らかにした理由を以下に示します。

- 45%：攻撃者が価値の高い標的と認識した。
- 45%：攻撃者が苛立ち、要求額を引き上げた。
- 45%：バックアップに失敗した、あるいはバックアップが正常に機能していなかった。
- 36%：攻撃者がより多くの身代金を支払えると考えた。
- 18%：迅速に支払わなかったため、身代金の金額が上がった。

小売企業が最初の要求額以上の身代金を支払う決断をした背景には、通常 2 つの要因があります。これは、被害組織がデータを復旧する際に直面する課題が 1 つではないことを示しています。

* 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**小売企業 60 社は、支払額を減らせた理由を以下のように説明しています。

- 60%：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。
- 47%：攻撃者が支払いを促すために要求額を下げた。
- 43%：第三者が攻撃者と交渉し、支払い額を下げた。
- 42%：身代金を迅速に支払ったため割引を受けた。
- 35%：攻撃者と交渉して支払額を下げた。

これらの組織も平均して 2 つの理由を挙げており、ランサムウェアの被害組織が複雑で多面的な状況に直面していることが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

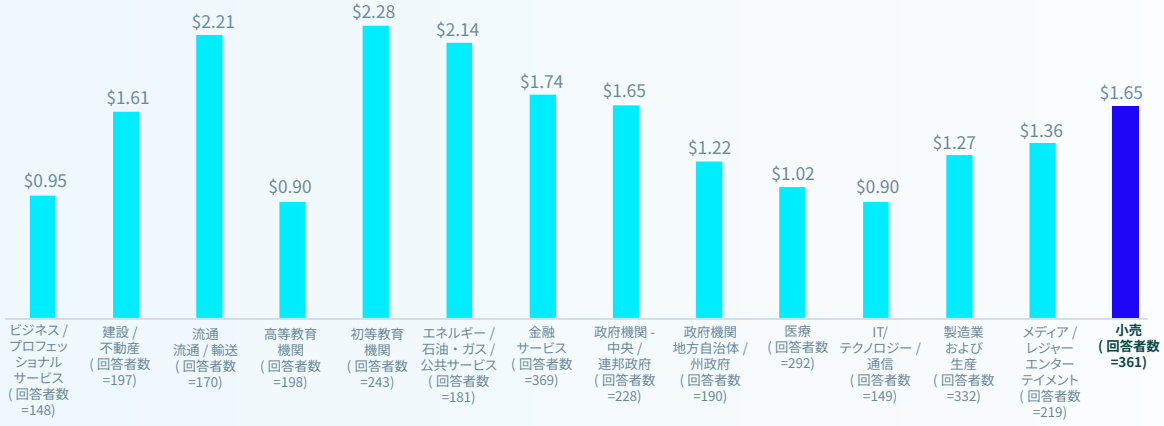
小売業界における復旧コスト：

小売企業におけるランサムウェア攻撃からの復旧にかかる平均 (中央値) コスト (身代金の支払額を除く) は、過去 3 年間で最も低い水準となり、過去 1 年間で 40% 減少して 165 万ドルとなりました (2024 年の 273 万ドルから減少)。これは 2023 年に報告された総復旧コストよりも 20 万ドル低くなっています。

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 =361 (2025 年)、261 (2024 年)、244 (2023 年)。

業界別に見ると、復旧の状況は大きく異なります。**初等中等教育機関**は、インシデントの修復に要する平均コストが 228 万ドルと最も高くなっています。一方、**高等教育機関**と **IT/ テクノロジー / 通信業界**は、いずれも 90 万ドルと最も低コストでした。

図 11：会社の規模別のランサムウェア攻撃の復旧コスト

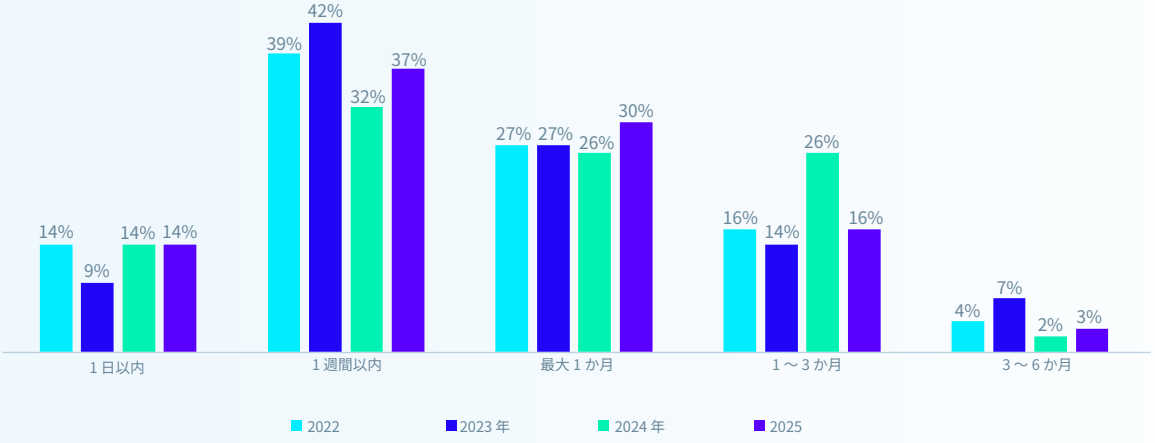


最も深刻なランサムウェア攻撃の影響において、組織が復旧に要した概算コスト (ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益など) は、支払った身代金を除いて、どれぐらいですか？ 回答数を図内に記載。

復旧にかかる時間

データによると、2025 年には、ランサムウェア攻撃を受けた小売企業の復旧が速まっている兆候が見られました。1 週間以内に復旧できた企業は半数以上 (51%) であり、2024 年の 46% から増加しています。一方、1 ～ 3 か月かけて復旧した企業の割合は、2024 年の 26% から 16% に激減しました。全体として、小売業の被害組織の 96% 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 12：小売企業におけるランサムウェア攻撃からの復旧時間 2022 ～ 2025 年



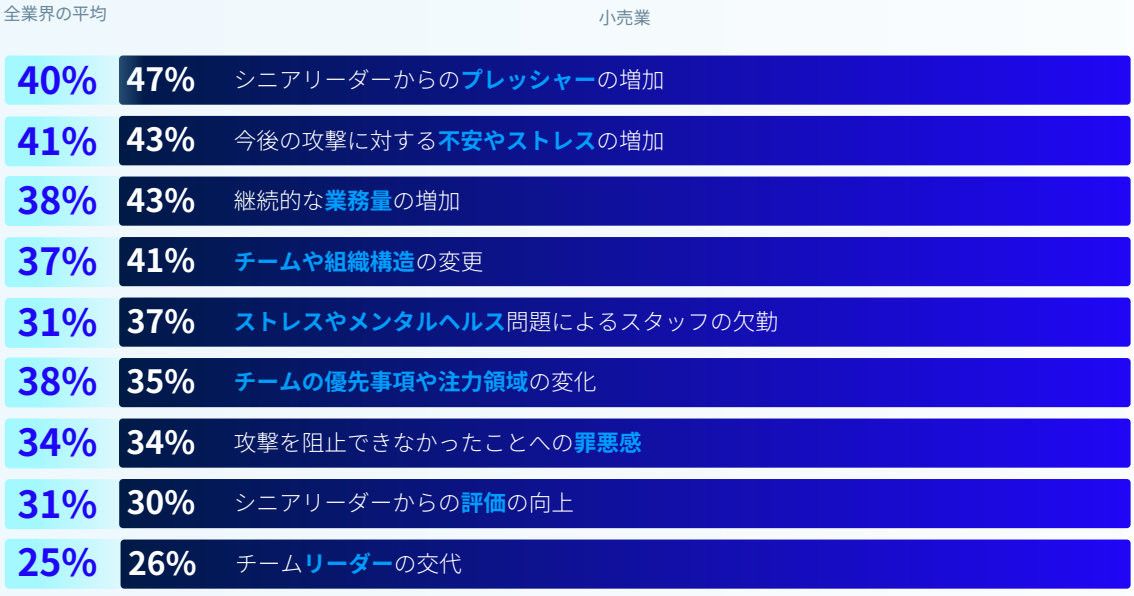
ランサムウェア攻撃から完全に復旧するのに、どのくらいの時間がかかりましたか？回答者数を図内に記載。

ある程度予想できることですが、データが暗号化された小売企業は、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。データが暗号化された組織のうち、1 日で完全復旧したのは 6% であったのに対し、暗号化を阻止できた組織の 22% が 1 日で完全復旧しています。

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、小売業界では、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 13：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



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 =175

ソフォスの提言

過去 1 年間で小売企業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の段階で阻止できれば、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れば、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止めることができます。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。

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をご覧ください。

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。

© Copyright 2025.Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK.
Sophos は、Sophos Ltd. の登録商標です。本書に記載されている製品や企業名はすべて、各所有者の商標または登録商標です。

2025-08-04 WP (MP)