SOPHOS

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の被害を受けた組織に所属する、17 か国 3,400 人の IT およびサイバーセキュリティリーダー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 6 月

はじめに

ソフォスの「ランサムウェアの現状レポート 2025 年版」は今回で 6 年目になりました。本レポートでは、2025 年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、過去 12 か月間におけるランサムウェア攻撃への体験について、発生原因とその影響の両面に焦点を当てて、この 1 年間でどのように変化したかを詳しく紹介しています。今回のレポートでは、従来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、組織が攻撃を受けることとなった運用上の要因や、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 17 か国 3,400 人の IT および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：

- 組織がランサムウェアの被害に遭う理由
- データへの影響
- 身代金：要求額と支払額
- 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 人の組織に勤務しており、過去 12 か月間の経験に基づいて回答しています。

参加者は 17 か国の幅広い業界から集まり、公共・民間部門にわたる多様な経験を反映しています。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、年ごとの動向分析が可能です。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

- 3 年連続で、被害を受けた組織は**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、脆弱性は全体の 32% 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**専門知識の欠如**で、被害者の 40.2% がこの要因を挙げています。2 番目に多かったのは、**組織が把握していなかったセキュリティギャップ**であり、全体の 40.1% の攻撃で要因となっていました。3 番目に多かったのは、**人手や能力の不足**で、39.4% の攻撃で要因として挙げられています。

データへの影響

- **データの暗号化**は過去 6 年間で最も低い水準となりました。現在は攻撃の 50% でデータが暗号化されており、2024 年の 70% から大幅に減少しています。
- データが暗号化された組織の 28% 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組織の 97% が、データを復旧することができました。
- 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 6 年間で最も低くなり、インシデント全体のわずか 54% でしか使用されていませんでした。
- 被害者の 49% 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 56% からわずかに減少したものの、過去 6 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

- 2025 年の平均 (中央値) での**身代金要求額**は、2024 年の 200 万ドルから約 3 分の 1 (34%) 減少し、1,324,439 ドルとなりました。
- また、**身代金の支払額**の平均 (中央値) も、2024 年の 200 万ドルから 2025 年には 100 万ドルと 50% 減少しました。支払額が減少した主な要因は、500 万ドル以上の高額な身代金を支払った割合が減ったことにあります。2024 年には支払いの 31% を占めていたのに対し、2025 年には 20% に低下しました。
- **要求額と支払額**を比較すると、最初に要求された同額を支払ったと回答した組織はわずか 29% でした。53% が最初に要求されたよりも少ない金額を支払っており、18% 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

- 身代金の支払いを除いたランサムウェア攻撃からの**復旧にかかる平均コスト**は、過去 1 年間で 44% 減少し、2024 年の 273 万ドルから 2025 年には 153 万ドルとなりました。
- **復旧のスピード**を見ると、組織はより迅速に復旧できるようになっており、攻撃から 1 週間以内にすべての影響を復旧した割合は 2024 年の 35% から、2025 年には 53% 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組織において、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。
  - 41% の IT/ サイバーセキュリティチームは、今後の攻撃に対する**不安やストレスが増加した**と回答しています。
  - 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。
  - 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。
  - 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。

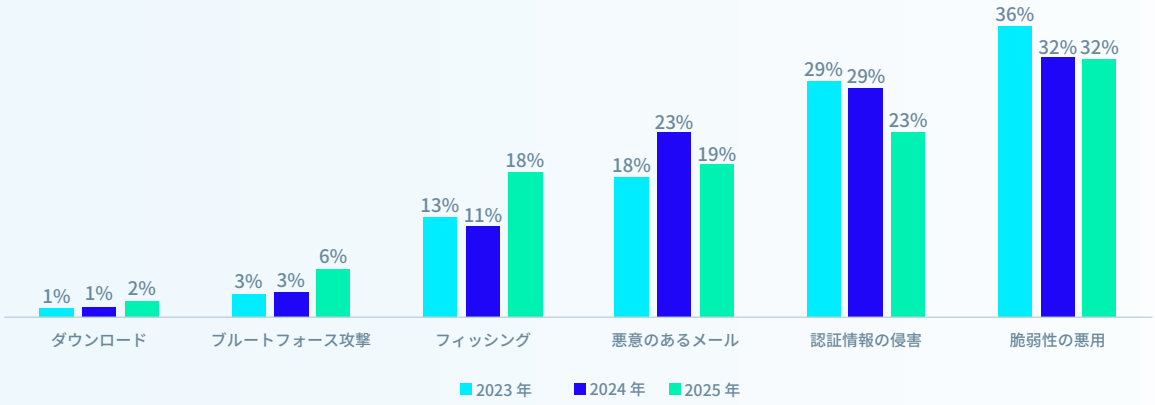
組織がランサムウェアの被害に遭う理由

攻撃の技術的な根本原因

3 年連続で、被害を受けた組織は**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、脆弱性は攻撃全体の 32% 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いましたが、侵害された認証情報が使用された攻撃の割合は、2024 年の 29% から 2025 年には 23% に減少しました。メールは依然として主要な攻撃手法の 1 つであり、19% の被害者が**悪意のあるメール**を根本原因として報告し、さらに 18% が**フィッシング**を挙げています。フィッシングは前年の 11% から大幅に増加しています。

図 1：ランサムウェア攻撃の技術的な根本原因 2023 年～ 2025 年

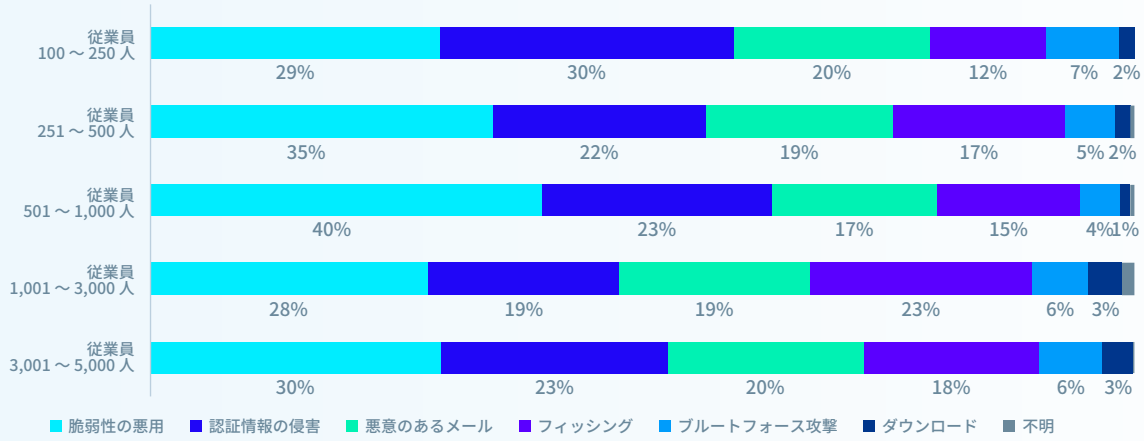


昨年受けたランサムウェア攻撃の根本原因を把握していますか？はい。 回答者数 =3,400 (2025 年)、2,974 (2024 年)、1,974 (2023 年)。

また、今回の調査で、組織の規模によって攻撃手法に違いがあることも明らかになりました。

- 従業員数 100 ～ 250 人の組織では、**認証情報の侵害**が最も多い根本原因であり、30% の攻撃で使用されていました。
- 従業員数 501 ～ 1,000 人の組織では、40% の攻撃が**脆弱性の悪用**から始まっていました。
- 従業員数 1,001 ～ 3,000 人の組織への攻撃の約 4 分の 1 (23%) は、**フィッシングメール**から始まっていました。

図 2：組織規模別のランサムウェア攻撃の技術的な根本原因

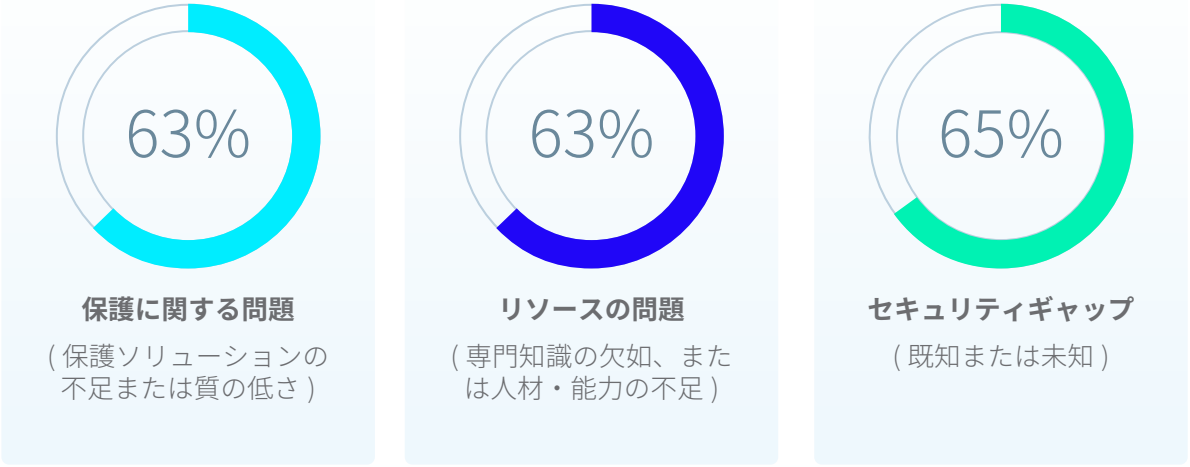


昨年受けたランサムウェア攻撃の根本原因を把握していますか？はい。 回答者数 =3,400

インシデントの運用面での根本原因

今年のレポートでは初めて、組織がランサムウェア攻撃に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、被害を受けた組織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 2.7 個の要因が攻撃の一因になったと述べています。

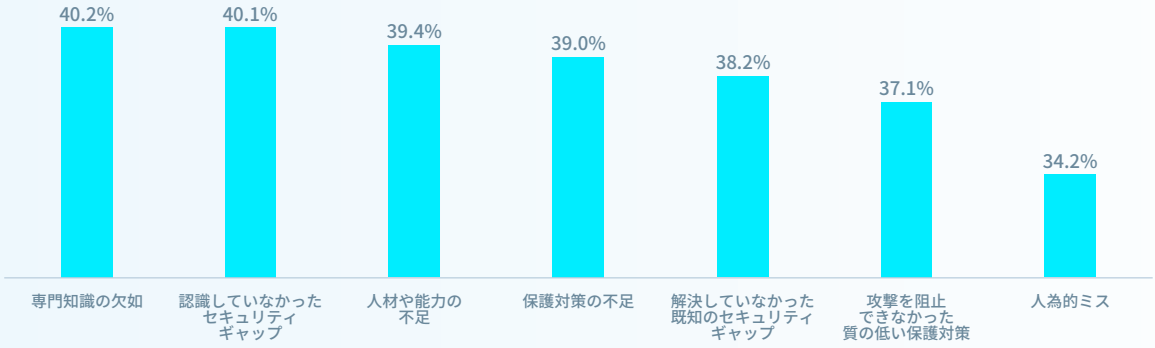
全体として、特定の要因が際立っているわけではなく、保護に関する問題、リソースの問題、セキュリティギャップがほぼ同じ割合で運用面での根本原因として挙げられています。



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

専門知識の欠如 (つまり、攻撃を適切に検知・阻止するためのスキルや知識がなかったこと) が、最も多く挙げられた運用面の理由で、40.2% の回答者がこの問題を挙げていました。次に多かったのが、**組織が認識していなかったセキュリティギャップ**であり、全体の 40.1% の攻撃において要因となっていました。3 番目に多かったのは、**人材や能力の不足** (つまり、攻撃時にシステムを監視する十分なサイバーセキュリティ人員がいなかったこと) であり、39.4% の攻撃において要因となっていました。

図 3：ランサムウェア攻撃の運用面の根本原因

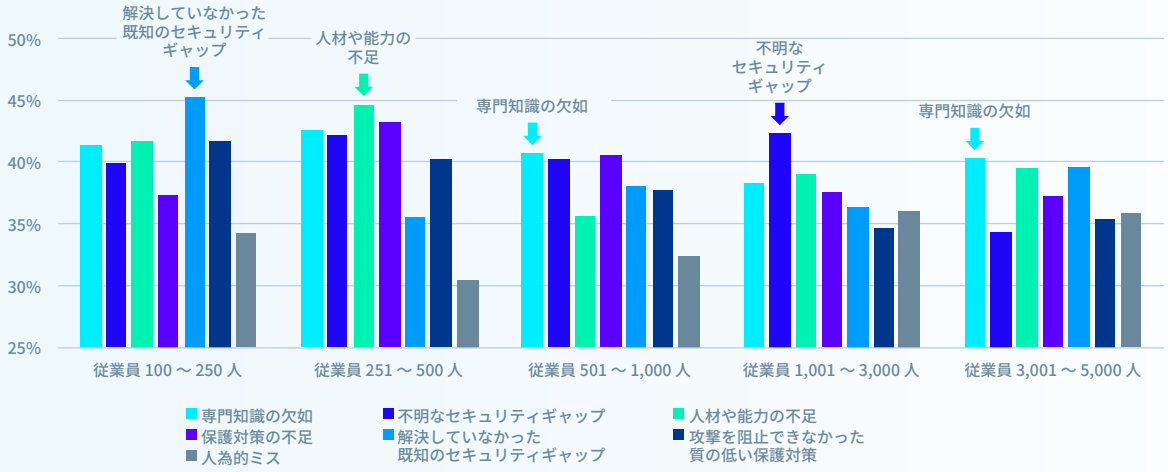


自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 回答者数＝ 3,400

組織規模別に見た運用面の根本原因

ランサムウェアの被害に遭った運用面での要因は、組織の規模によって異なっており、各規模の組織が直面する課題の違いが反映されています。本レポートで使用した従業員数による 5 つの規模区分では、4 つの異なる課題が、それぞれ最大の要因として挙げられています (下図を参照)。

図 4：組織規模別の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＝ 3,400 組織規模 (従業員数) 別の内訳

業種別の運用上の根本原因

同様に、最も多い運用上の根本原因は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

専門知識の欠如	認識していなかったセキュリティギャップ	人材や能力の不足	保護対策の不足	既知のセキュリティギャップ	品質の低い保護機能
攻撃を適切なタイミングで検知・阻止するためのスキルや知識がなかった	認識していなかった防御の弱点があった	攻撃発生時にシステムを監視して対応するサイバーセキュリティ専門家を十分に配置していなかった	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	認識していたが解決していなかった防御の弱点があった	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
エネルギー / 石油・ガス / 公共事業 (43%) 初等中等教育機関 (42%)* 製造 / 生産 (42%) 建設 / 不動産 (41%)*	高等教育機関 (18 才以上) (49%) ビジネス / プロフェッショナルサービス (46%) 小売 (46%) 金融サービス、保険を含む (44%)*	初等中等教育機関 (K-12) (42%)* ヘルスケア (42%)	金融サービス、保険を含む (44%)* 地方自治体 / 州政府 (40%)	中央 / 連邦政府 (45%) IT/ テクノロジー / 通信 (42%) 建設 / 不動産 (41%)*	メディア / レジャー / エンターテイメント (41%) 流通 / 輸送 (41%)

* は同率一位の複数の攻撃根本原因を示します。

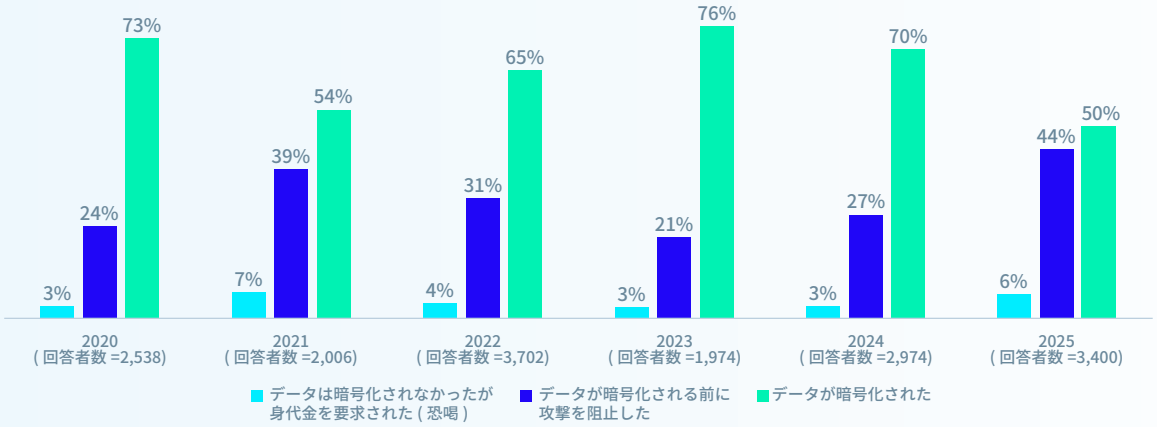
自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 回答者数＝ 3,400 業界別の内訳

データへの影響

データの暗号化

朗報として、ソフォスが過去 6 年間にわたって実施した調査の中で、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 50% にとどまりました。過去 1 年間でデータが暗号化された攻撃の割合は顕著に減少しており、2024 年の調査での 70% であった暗号化率は 2025 年には 50% へと減少しました。これは、暗号化ペイロードが展開される前に攻撃を阻止する組織の能力が高まっていることを示しています。

図 6：ランサムウェア攻撃のおけるデータ暗号化率 2020 年～ 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。

調査対象の中で最も大規模な組織ほどデータが暗号化される可能性が高くなっています。従業員数 3,001 ～ 5,000 人の組織に対する攻撃の 65% でデータが暗号化されています。これはすべての規模区分の中で最も高い暗号化率です。これは、大規模な組織は暗号化が始まる前に攻撃を検知・阻止する能力が小規模組織よりも劣っていること、または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。

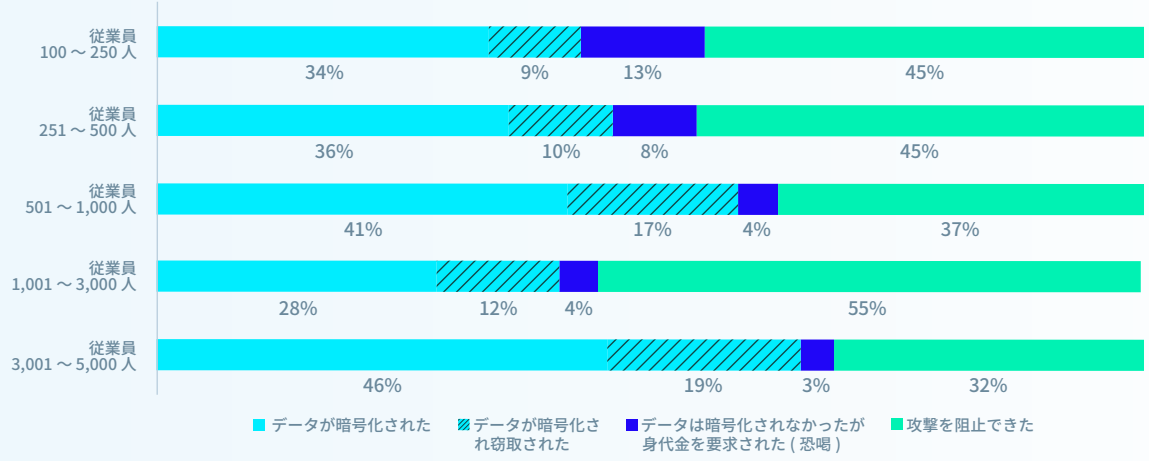
データの窃取

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。すべてのランサムウェア被害者の 14%、そしてデータが暗号化された被害者の 28% がデータの窃盗を経験しています。企業規模別に見ると、小規模組織は大規模組織に比べて、データを窃取される可能性が約 40% 低くなっています。

- 従業員数 100 ～ 500 人の組織では、データが暗号化されたケースの 22% でデータも窃取されています。
- 従業員数 501 ～ 5,000 人の組織では、データが暗号化されたケースの 30% でデータも窃取されています。

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 7：組織の規模別のランサムウェア攻撃におけるデータ暗号化率



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 =3,400

恐喝型攻撃

図 6 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) 攻撃を受けた組織の割合は、昨年の 3% から 2025 年に 6% へと倍増しました。小規模組織は、大規模組織よりもデータが暗号化されなくても身代金を要求される恐喝型攻撃を受けやすい傾向にあります。

- 被害を受けた従業員数 100 ～ 250 人の組織の 13% が恐喝型攻撃を経験しています。
- 被害を受けた従業員数 3,001 ～ 5,000 人の組織の 3% が恐喝型攻撃を経験しています。

全体を見ると、従業員数 1,001 ～ 3,000 人の組織は、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、こうした規模の組織が十分なサイバーセキュリティツールと専門知識を備えていながら、大企業ほどの組織的な複雑さに直面していない、いわば「ちょうど良い規模」にあるためと考えられます。

暗号化されたデータの復旧

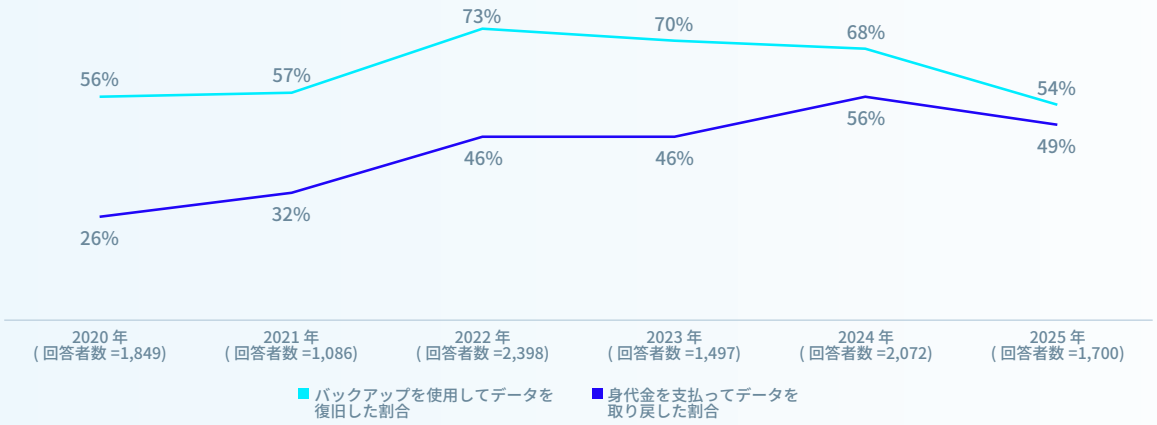
データを暗号化された組織の 97% が、データを復元することができました。

これらの組織の半数強 (54%) はバックアップを使用してデータを復旧していますが、この数字は 3 年連続で減少しています。全体として、バックアップからのデータ復旧率は過去 6 年間で最も低い水準となっています。

約半数 (49%) の組織が身代金を支払い、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 56% からわずかに減少したものの、過去 6 年間で 2 番目に高くなっています。

データが暗号化された組織の 29% は、「その他の方法」でデータを復旧したと回答しています。この「その他の方法」には、過去に公開された復号鍵を利用したケースが含まれている可能性があります。

図 8：バックアップおよび身代金支払によるデータの復旧 2020 年～ 2025 年



データを復旧できましたか？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。回答数はグラフ内

身代金

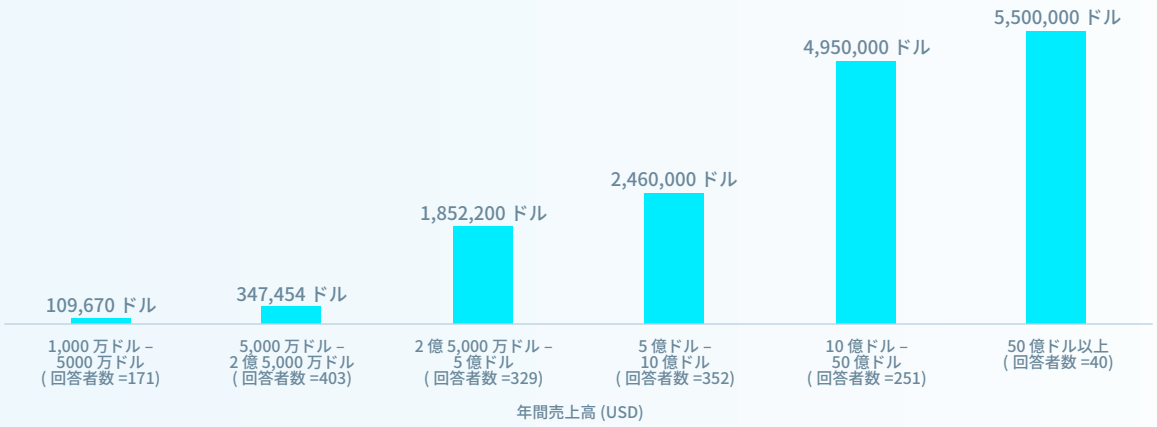
身代金要求額

2025 年の平均 (中央値) での身代金要求額は、2024 年の 200 万ドルから約 3 分の 1 (34%) 減少し、1,324,439 ドルとなりました。500 万ドル以上の高額な身代金が要求されるケースが 30% から 24% に減少したことがこの主な要因です。この減少は歓迎すべきですが、身代金要求額の 57% が 100 万ドル以上であることから、楽観は禁物です。

身代金の要求額は組織の売上高に比例して高くなる傾向があり、攻撃者は被害者の支払い能力を見越して「価格設定」していると考えられます。

- 109,670 ドル：年間売上が 1,000 万ドル～ 5,000 万ドルの組織に対する身代金要求額の中央値。
- 5,500,000 ドル：年間売上が 50 億ドル以上の組織に対する身代金要求額の中央値。

図 9：企業の年間売上高別の身代金の要求額



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。

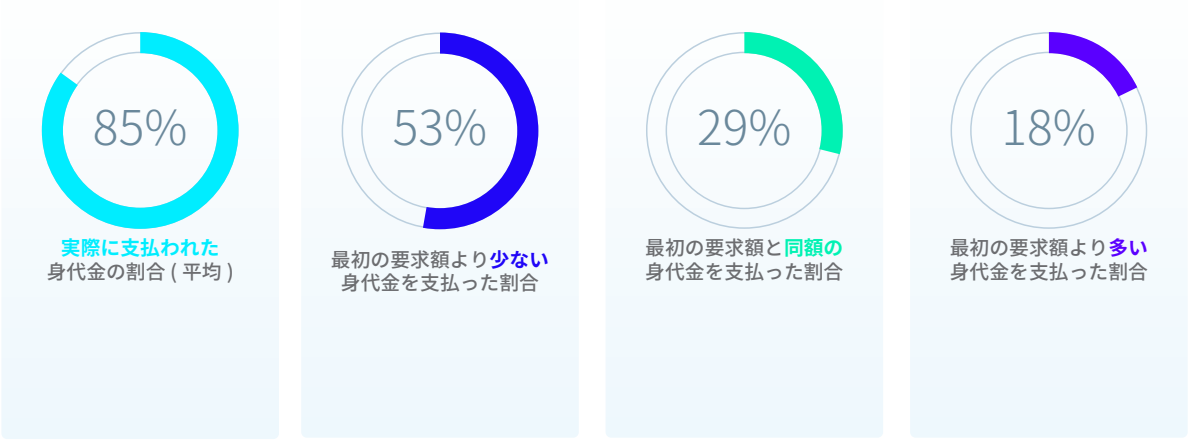
身代金の支払額

また、身代金の支払額の平均 (中央値) も、2024 年の 200 万 ドルから 2025 年には 100 万ドルと変化し、50% 減少しました。身代金要求額と同様に、支払額の中央値が減少した主な要因は、500 万ドル以上を支払った割合が 2024 年の 31% から 2025 年に 20% に減少したことです。

身代金の要求額と支払額は減少傾向にあり、支払額の減少が最も大きくなったことは歓迎すべきです。とはいえ、100 万ドルという金額は依然として極めて高額であり、多くの組織にとって深刻な影響を及ぼしています。

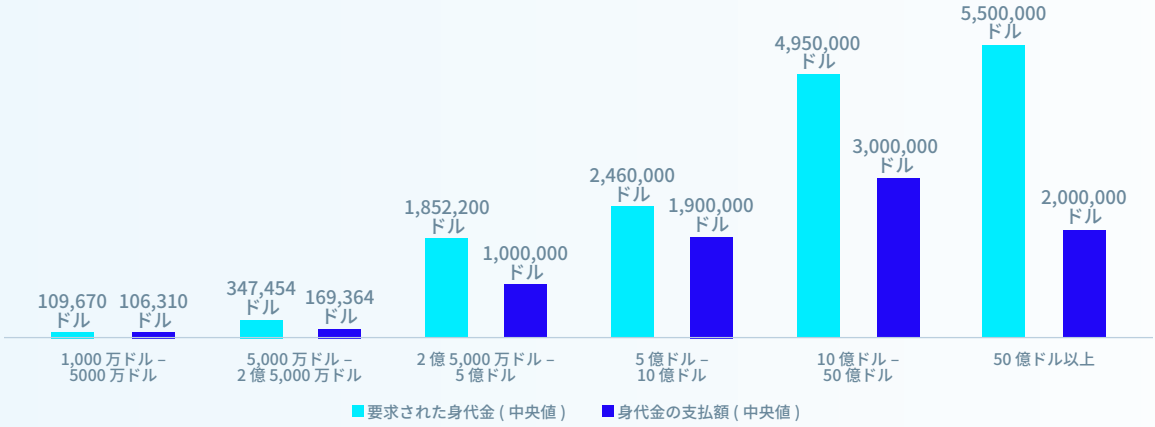
実際の支払額と初回の身代金要求額の比較

身代金を支払った 826 の組織が、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、平均すると初回の要求額の 85% を支払っていることが明らかになりました。全体を見ると、53% の組織が最初の要求額より少ない金額を支払い、18% が要求額以上を支払い、29% が同額を支払っています。



年間売上別に見ると、すべての売上の組織で実際の支払額は平均して最初の要求額を下回っています。しかし、最も売上の大きい組織 (年間売上 50 億ドル以上) は最も大きく減額しており、外れ値を除くと実際の平均支払額は 200 万ドルで、最初の要求額の 550 万ドルのわずか 36% になっています。一方、年間売上が 1,000 万ドル～5,000 万ドルの組織は最も減額幅が小さく、中央値の支払額は中央値の要求額の 97% でした。

図 10：企業の年間売上別の身代金要求額と身代金支払額の比較



攻撃者から要求された身代金額はいくらでしたか？攻撃者に支払った身代金はいくらでしたか？ (回答者数 =1,552/836)

多くの身代金支払額が最初の要求額と異なる理由

今年は初めて、一部の組織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** 151 の組織が明らかにした理由を以下に示します。

- 50%：攻撃者がより多くの身代金を支払えると考えた。
- 48%：攻撃者が価値の高い標的と認識した。
- 38%：攻撃者が苛立ち、要求額を引き上げた。
- 38%：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。
- 32%：迅速に支払わなかったため、身代金の金額が上がった。

組織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。

一方、最初の要求額より**少なく支払った** 445 の組織は、支払額を減らせた理由を以下のように説明しています。

- 47%：攻撃者と交渉して支払額を下げた。
- 45%：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。
- 45%：攻撃者が支払いを促すために要求額を下げた。
- 43%：身代金を迅速に支払ったため割引を受けた。
- 40%：第三者が攻撃者と交渉し、支払い額を下げた。

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

復旧コスト

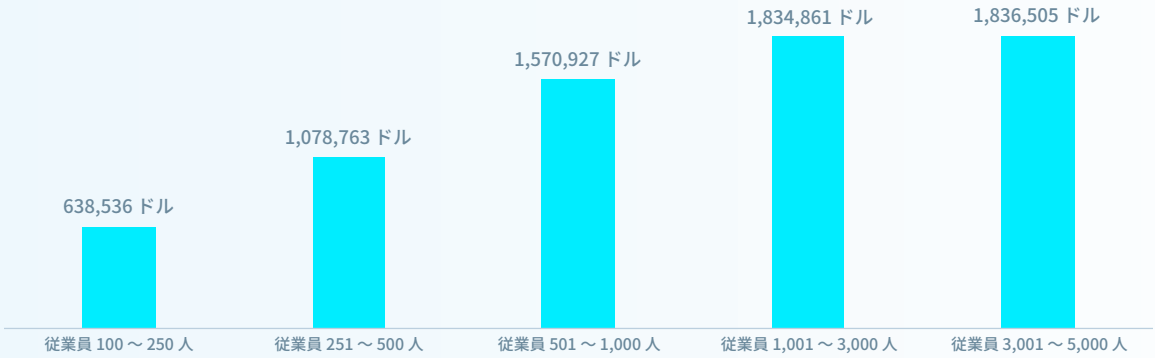
ランサムウェア攻撃からの復旧にかかる平均 (中央値) コストは、身代金の支払額を除いて、過去 1 年間で 44% 減少し、2024 年の 273 万ドルから 2025 年は 153 万ドルとなりました。これは 2023 年に報告された総復旧コストよりも約 30 万ドルほど低くなっています。

2023	2024	2025
182 万ドル	283 万ドル	153 万ドル

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 =3,400 (2025 年)、2,974 (2024 年)、1,974 (2023 年)

復旧コストは組織の規模に応じて増加していき、従業員数が 1,000 人から 5,000 人の組織から横ばいになります。従業員数が 100 ～ 250 人の組織は復旧コストの平均が 638,536 ドルであるのに対し、1,000 ～ 5,000 人の組織は 183 万ドルとなっています。

図 11：会社の規模別のランサムウェア攻撃の復旧コスト

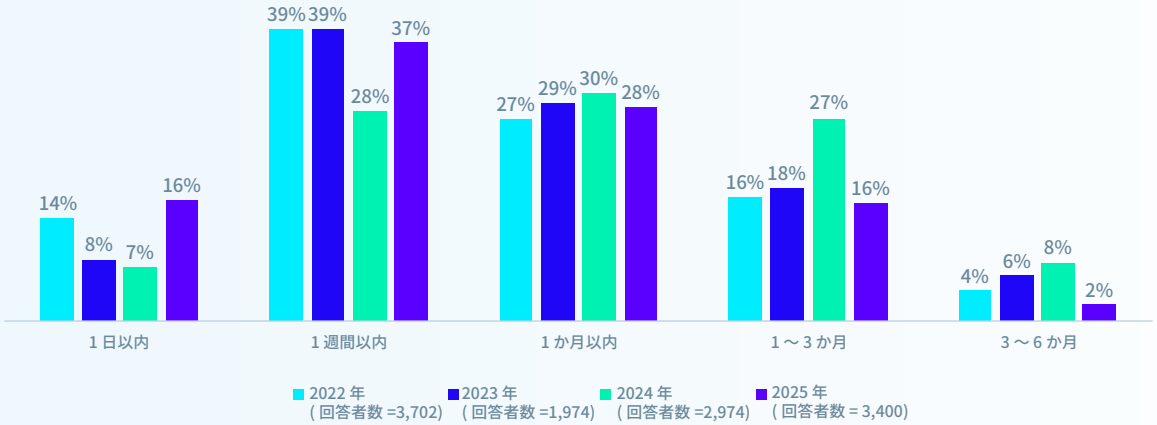


最も深刻なランサムウェア攻撃の影響において、組織が復旧に要した概算コスト (ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益など) は、支払った身代金を除いて、どれぐらいですか？ 回答者数 =3,400

復旧にかかる時間

データから、組織は攻撃で受けた影響を復旧するまでの時間を短縮しており、1 日以内に完全復旧した組織は 16% で、2024 年の 7% および 2023 年の 8% から増加しています。1 週間以内に復旧した組織は 53% にのぼり、2024 年の 35% から大きく増加しました。全体的には、被害を受けたほぼすべての組織 (97%) が攻撃から 3 か月以内に完全復旧しています。復旧までの期間が短縮されているのは、過去 1 年間にわたり組織がサイバーインシデントへの対応や復旧体制に投資してきたことを示している可能性があります。

図 12：ランサムウェア攻撃の復旧にかかる時間 2022 年 –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？回答数はグラフ内

ある程度予想できることですが、データが暗号化された組織は、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 9% であったのに対し、暗号化を阻止できた組織の 24% 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、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に大きな影響を受けています。回答者全員が、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 =1,700

ソフォスの提言

過去 1 年間でランサムウェアに対する組織の体験にはいくつかの変化が見られましたが、依然としてあらゆる組織にとってランサムウェアは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。質の高いバックアップを確実に取得し、データを迅速に復旧できるよう、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。

2025-06-26 JA-WP (DD)

SOPHOS