SOPHOS

大規模企業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大規模企業に属する、IT およびサイバーセキュリティリーダー 1,733 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 12 月

はじめに

「大規模企業におけるランサムウェアの現状」レポートをご覧いただきありがとうございます。本レポートは、従業員 1,000 名以上の大規模企業を対象に、2025 年におけるランサムウェア攻撃の実態を明らかにした、ソフォス初の調査レポートです。

今年のレポートでは、過去 1 年間における大規模企業のランサムウェア被害について、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。大規模企業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 1,733 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。

- 大規模企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

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、ランサムウェアに関する組織の経験についての調査した結果に基づいています。サードパーティーの専門機関が 2025 年 1 月から 3 月にかけて調査を実施しました。大規模企業の回答者はすべて、従業員数 1000 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。

本レポートに回答した 1,733 社の大規模企業は、17 か国・14 業界にわたっており、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、過去の調査で得られたデータとの比較も含まれており、年ごとの動向を分析しています。財務データはすべて米ドルで表示されています。

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と影響は 2024 年に発生しています。

主な調査結果

大規模企業がランサムウェアの被害に遭う理由

- **最も一般的な攻撃の技術的な根本原因は、**脆弱性の悪用であり、インシデントの 29% で使用されています。**フィッシング**と**認証情報の侵害**が次に多く、いずれもインシデントの 21% で報告されています。
- 大規模企業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**認識していなかったセキュリティギャップ**であり、被害を受けた組織の 40% がこの要因を挙げています。これに僅差で続く要因として**人材や能力の不足**、そして**専門知識の欠如**が挙げられ、これらはいずれも攻撃の 39% の要因となっていました。

データへの影響

- 大規模企業におけるデータ暗号化率は過去 5 年間で最も低い水準となっており、**現在はランサムウェア攻撃の 49% でデータが暗号化されています。**これは、2022 年のピーク時 (64%) から低下しています。
- データを暗号化された大規模企業の 30% 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大規模企業の 96% が、データを復元することができました。
- 大規模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、バックアップが使用されたのはインシデントの 53% でした。
- **被害者を受けた大規模企業の 48% が身代金を支払って**データを取り戻しています。これは、これは今年の調査で記録された中でも最も低い水準の一つです。

身代金：要求額と支払額

- 大規模企業への**身代金要求額**の平均 (中央値) は、過去 1 年間で 56% も急減し、2024 年の 275 万ドルから 2025 年には **120 万ドル**となりました。この大幅な減少の主な要因は、500 万ドル以上の身代金が要求された割合が 24% 減少し、2024 年の 38% から 2025 年には 29% になったことです。しかし、100 万ドルから 500 万ドルの身代金が要求されたケースが 17% 増加したことには注意してください。
- 大規模企業が**支払った身代金**の平均額 (中央値) も減少しており、2024 年の 126 万ドルに対して 2025 年は **100 万**ドルとなりました。この減少の主な要因は、500 万ドル以上支払われた身代金の割合が 37% 減少したことです。ただし、500 万ドル未満の身代金支払いのほぼすべての帯域で増加が見られたことには注意が必要です。
- 大規模企業が**支払った身代金要求額**の割合は、2024 年の 95% から 2025 年には 86% に減少しました。
- **要求額と実際に支払われた金額**を詳しく見ると、約 3 分の 1 (31%) の大規模企業が、支払額が最初の要求額と同じであったと回答しています。51% 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

- ランサムウェア攻撃からの**復旧にかかった大規模企業の平均コスト**は、過去 1 年間で 41% 減少し、2024 年の 312 万ドルから 2025 年には **184 万ドル**となりました。
- **復旧にかかった期間**を見ると、大規模企業はより迅速に復旧する傾向にあり、1 週間以内に復旧できた大規模企業は 2024 年の 36% から 2025 年には 50% に増加しています。

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大規模企業において、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と報告されています。

- 40% の IT/ サイバーセキュリティチームは、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。
- 39% が、**業務量の継続的な増加**と、将来の攻撃に対する**不安やストレスの増大**の両方を報告しています。
- 37% が、**チームの優先事項や注力領域の変化**を報告しています。
- 回答者の 3 分の 1 以上（35%）が、インシデントの影響として、攻撃を阻止できなかったことへの**罪悪感**と、**チームや組織構造の変更**の両方を挙げています。
- 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 を超えるケース (27%) で、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。

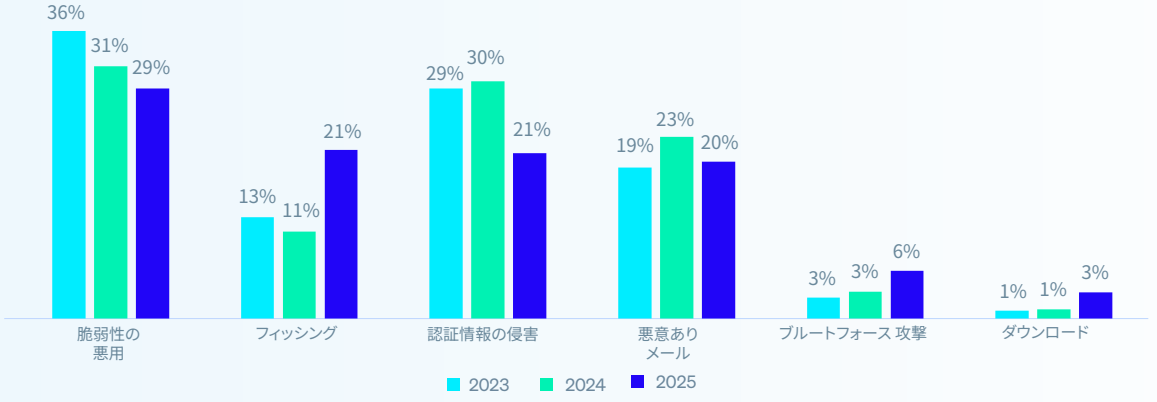
大規模企業がランサムウェアの被害に遭う理由

大規模企業における攻撃の技術的な根本原因

大規模企業は 3 年連続で、ランサムウェア攻撃の主な原因として**脆弱性の悪用**を挙げており、29% のインシデントの原因となっています。**フィッシングメール**が、2 位になっており、2024 年の 11% から 2025 年には 21% に急増しました。

認証情報ベースの攻撃は、依然として重大なリスクになっていますが、この攻撃経路の報告は大幅に減少し、2024 年の 30% から 2025 年には 21% に減少しています。対照的に、**中小企業** (従業員 100 人から 250 人の企業) は、認証情報ベースの攻撃をランサムウェア攻撃の主な原因として挙げており、インシデントの約 3 分の 1 (30%) がこの原因が占めています。

図 1：2023 年から 2025 年の大規模企業におけるランサムウェア攻撃の技術的な根本原因

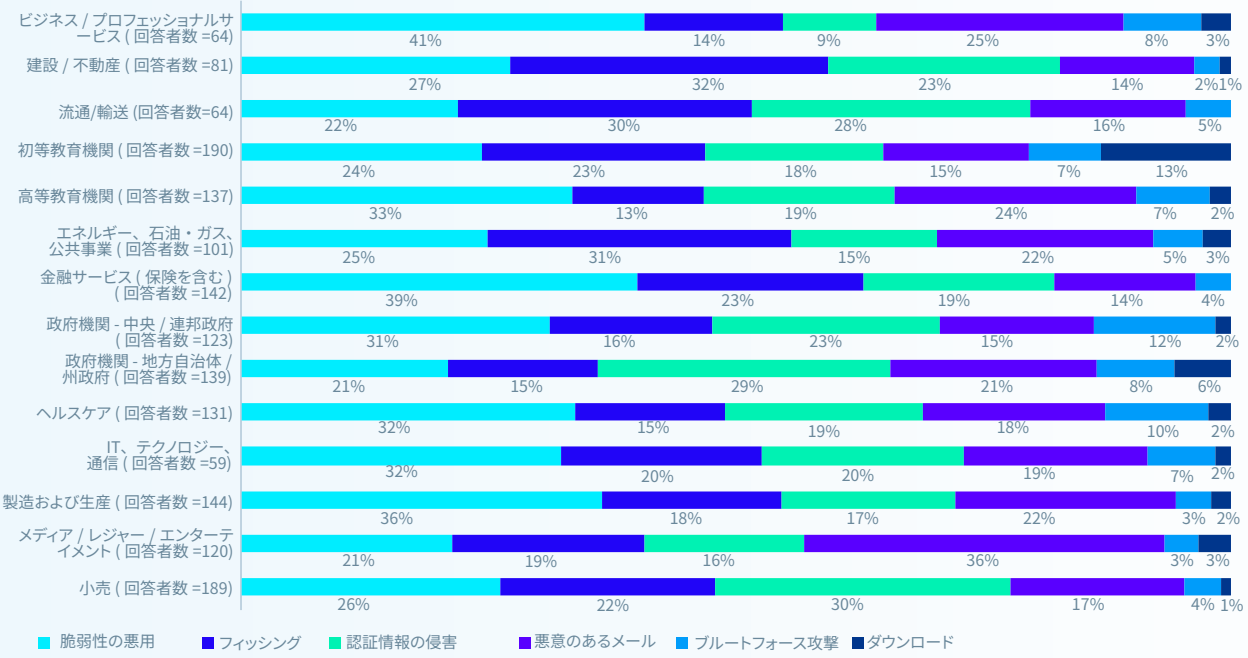


過去 1 年間に受けたランサムウェア攻撃の根本原因を把握していますか?はい。回答企業数 = 1,733 (2025 年)、1,409 (2024 年)、1,045 (2023 年)

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、ほぼすべての業界の大規模企業で脆弱性の悪用が主要な攻撃経路となっています。ただし、以下の例外があります。

- **建設 / 不動産** (32%)、**流通 / 輸送** (30%)、**エネルギー / 石油・ガス / 公共事業 (31%) の事業者が、**最も多く挙げられたランサムウェアの主な原因はフィッシングでした。
- **認証情報の侵害**は、**小売業界**の大規模企業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 (30%) 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

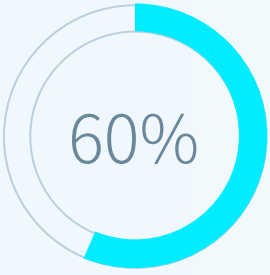


過去 1 年間に受けたランサムウェア攻撃の根本原因を把握していますか?はい。回答者数を図内に記載。

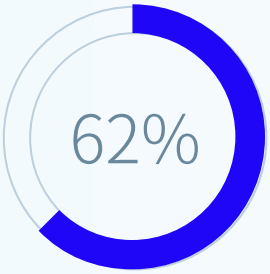
大規模企業におけるインシデントの運用面の根本原因

インシデントの技術的な根本原因と並行して、大規模企業が攻撃を受けた運用面な要因を理解することも重要です。調査結果によると、被害を受けた大規模企業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 つの要因がランサムウェア攻撃の一因になったと述べています。

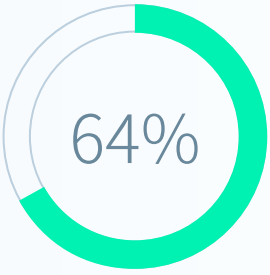
全体として、保護に関する問題、リソースの問題、セキュリティギャップの 3 つが、ほぼ同じ割合で運用面の根本原因として挙げられています。しかし、大規模企業は既知または未知のセキュリティギャップを主な要因としてやや多く挙げる傾向があります。



保護機能の不足または品質の低さ
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



人材やスキルの不足
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



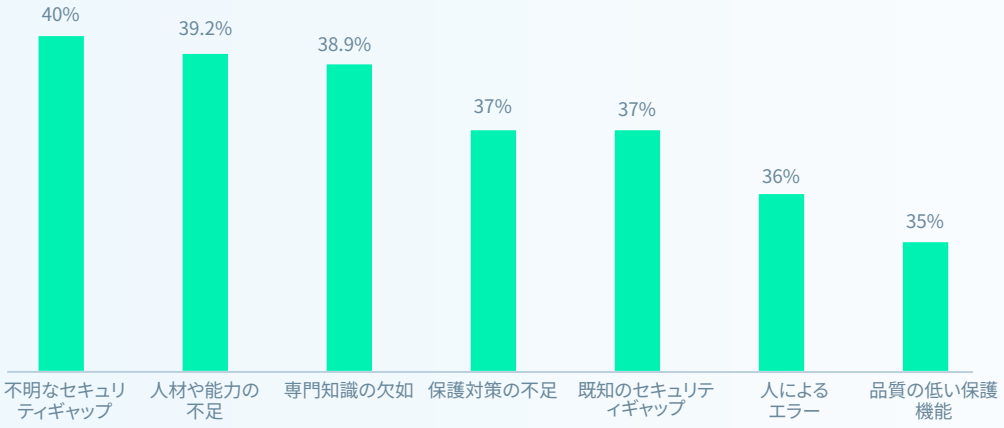
既知または未知のセキュリティギャップ
防御体制に、既知または未知の弱点があった

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= 1,733 集計結果。

未知のセキュリティギャップは、大規模企業において、最も多く指摘された個別の原因であり、回答者の 40% がこれを挙げています。これに僅差で続く要因として、**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) と、**専門知識の欠如** (攻撃を適切なタイミングで検知・阻止するための十分なスキルや知識がなかった) が挙げられており、いずれも大規模企業の 39% がランサムウェア攻撃の要因として挙げています。

興味深いことに、**中小企業**の 42% が、**人材や能力の不足**を、攻撃の被害に遭った主な一般的な原因として挙げており、リソースの制約は企業規模を問わず共通する課題であることが示されています。

図 3：大規模企業におけ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＝ 1,733

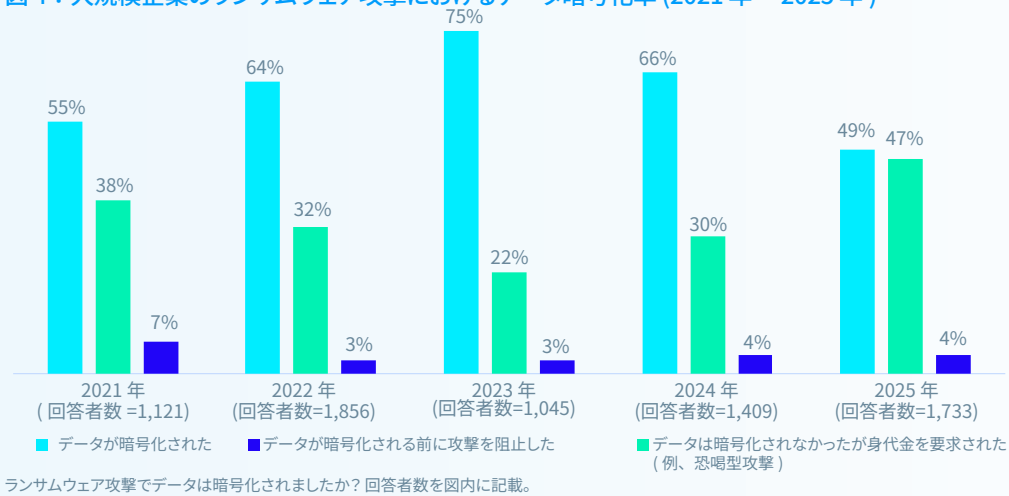
データへの影響：

大規模企業におけるデータ暗号化

明るい兆しとして、大規模企業におけるデータ暗号化率は、過去 5 年間の調査で最も低い水準となっています。現在、攻撃によってデータが暗号化された割合は半数未満 (49%) にとどまっており、2024 年に報告された 66% から低下しました。

一方、データが暗号化される前にランサムウェア攻撃を阻止した割合は過去 2 年間で倍増し、2023 年の 22% から 2025 年には 47% に上昇しています。これは、大規模企業が深刻な被害を受ける前に攻撃を検知して阻止する能力が向上していることを示しています。

図 4：大規模企業のランサムウェア攻撃におけるデータ暗号化率 (2021 年～ 2025 年)

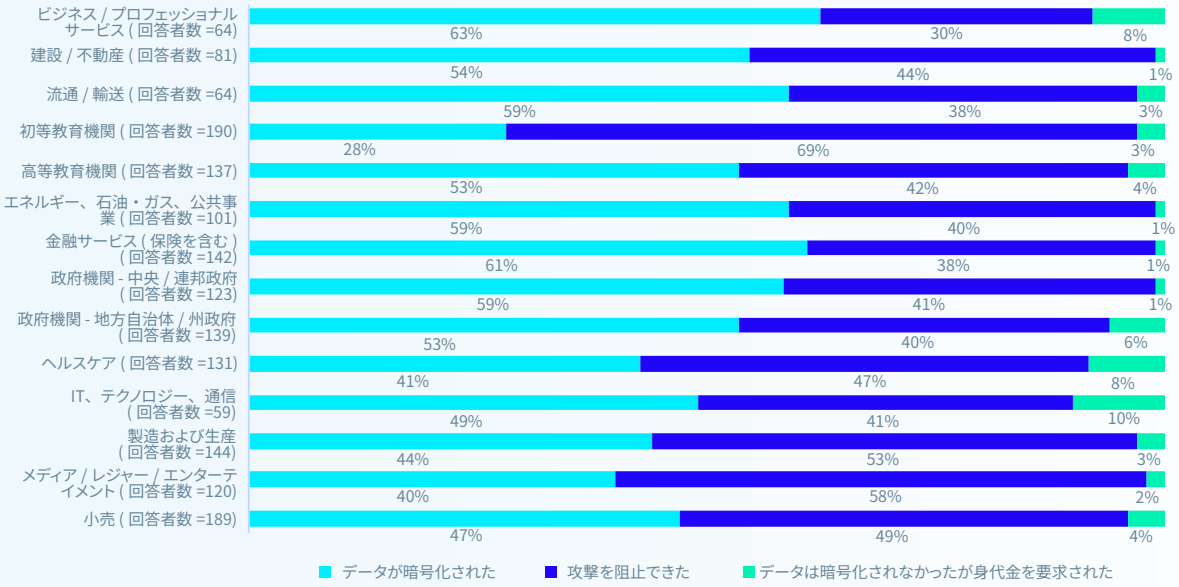


ランサムウェア攻撃でデータは暗号化されましたか？回答者数を図内に記載。

業界別のデータ暗号化率

ビジネス / プロフェッショナルサービス業界の大規模企業はデータが暗号化される割合が最も高くなっており (63%)、この業界の組織は、暗号化に至る前に攻撃を検知・阻止できる割合が低いことを示しています。また、悪意のある暗号化を防止する能力や、暗号化されたファイルをロールバックする能力も低いことが示されています。対照的に、**初等中等教育機関**はデータ暗号化率が最も低く、わずか 28% でした。

図 5：業界別の大規模企業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。大規模企業のすべてのランサムウェア被害者の 15%、そしてデータが暗号化された被害者の 30% がデータの窃盗を経験しています。業界別のデータの内訳は以下の通りです。

- **メディア、レジャー、エンターテインメント**業界は高い水準にあり、データを暗号化された大規模企業の 52% が、データも窃取されていました。
- 対照的に、企業のうちわずか 11% が **建設 / 不動産**業界で暗号化と同時にデータが窃取された大規模企業は僅か 11% でした。

恐喝型攻撃

図 4 に示すように、データ暗号化を回避しながら身代金を要求された大規模企業の割合は、前年比で横ばいの 4% でした。業界別に見ると、**IT、テクノロジー、通信**業界の企業がこのタイプの攻撃を最も多く受けています (10%)。一方で、**建設 / 不動産、エネルギー、石油・ガス、公益事業、金融サービス、中央 / 連邦政府**の大規模企業や大規模組織は最も影響が少なく、それぞれわずか 1% にとどまっています。

全体を見ると、**初等中等教育**の大規模組織は、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、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。

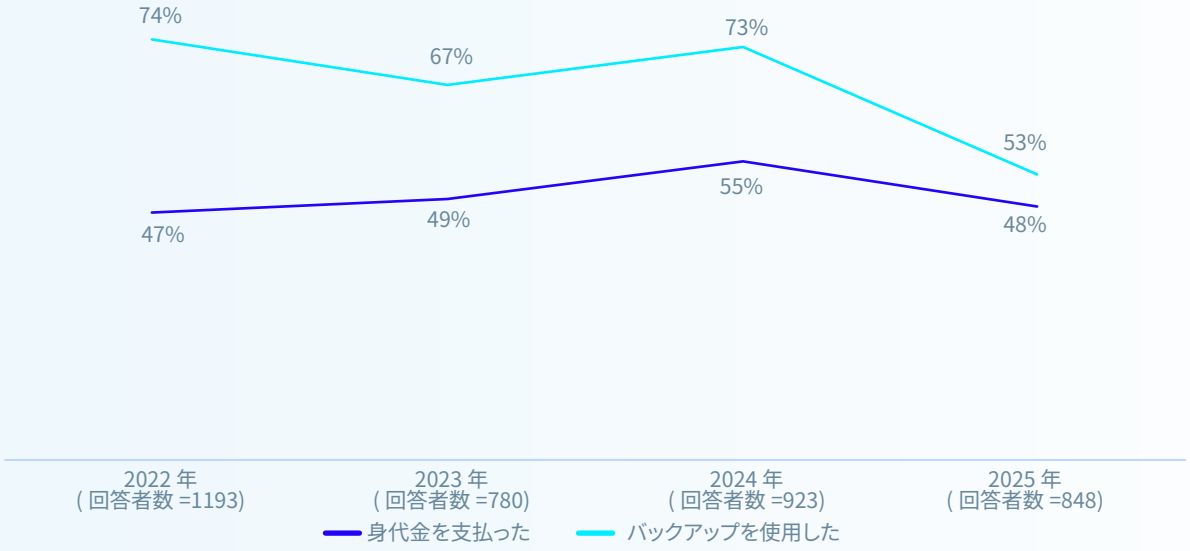
大規模企業における暗号化されたデータの復旧

データを暗号化された大規模企業の 96% が、データを復元しています。

2025 年には、大規模企業の 48% が**データ復旧のために身代金を支払いました**。これは 2024 年の 55% から減少しています。同時に、**バックアップの利用率**は過去 4 年間で最も低い水準まで大きく低下し、2024 年の 73% から 2025 年には 53% へと減少しました。これらの結果を総合すると、身代金要求に対する抵抗力が高まっている一方で、バックアップを利用したレジリエンスが十分ではなく、依然といて弱点があることを示しています。

さらに、大規模企業で、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旧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。これを裏付けるように、データが暗号化された大規模企業の約 3 分の 1 (30%) が、**他の手段を用いてデータを復旧**したと回答しています。他の手段としては、シャドウコピーからの復元、エンドポイント保護製品のロールバック機能の活用、影響を受けなかったシステムからのデータ復旧などが挙げられます。

図 6：企業組織における暗号化データの復旧 (2021 年～ 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

大規模企業への身代金要求額

大規模企業に対する身代金の平均要求額 (中央値) は、過去 1 年間で 56% も減少し、2024 年の 275 万ドルから 2025 年には 120 万ドルとなりました。大規模企業を標的とした身代金要求額の減少は、主に過去 1 年間で 500 万ドル以上の要求が 24% 減少したことによるものです。ただし、100 万ドルから 500 万ドルの要求額は 17% 増加して全体の 27% を占めており、2024 年の 23% から上昇していることに注意が必要です。

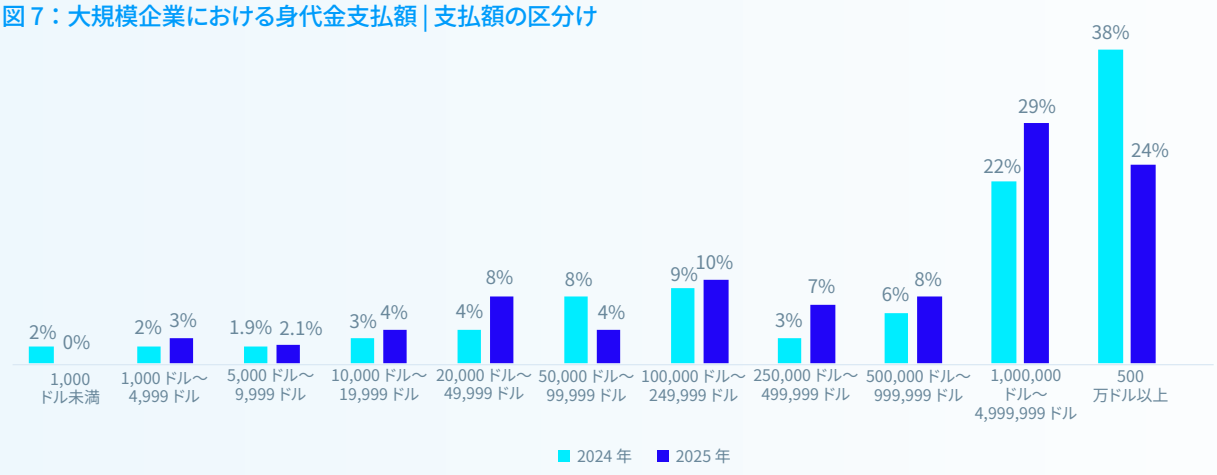
大規模企業の身代金支払額

身代金要求額が減少した傾向に続き、大規模企業が支払った平均 (中央値) の身代金も 2024 年の 126 万ドルから 2025 年には 100 万ドルに減少しました。これは主に、昨年 500 万ドル以上の支払いが 37% 減少したことが要因です。ただし、本レポートでは、500 万ドル未満のほぼすべての支払い金額帯で、前年比で増加していることが明らかになっています。

これらの傾向は、攻撃者が極めて高額な身代金要求から離れ、代わりに大規模企業に中程度の金額帯の身代金を要求する方向へ移行していることを示唆しています。これは、依然として大きな損害を与えつつも、より現実的に回収が見込める金額を狙っているためと考えられます。

中小企業 でも同じ傾向が見られていますが、要求額と支払額の減少はさらに顕著でした。中央値の身代金要求額と支払額は、2024 年の 200 万ドルからそれぞれ 2025 年には 12.6 万ドルおよび 20 万ドルへと急減しました。これは攻撃者がすべての規模の組織に対して、より現実的に回収可能な金額を狙う方向に調整しているという傾向を裏付けています。

図 7：大規模企業における身代金支払額 | 支払額の区分け

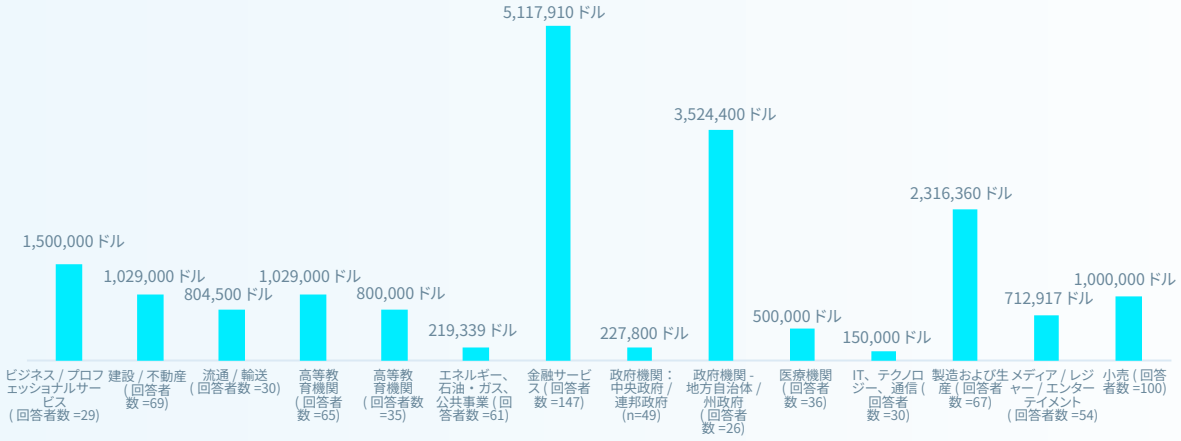


攻撃者に支払った身代金はいくらでしたか? 回答者数 = 414 (2025 年)、470 (2024 年)

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、金融サービス業界の大規模企業が最も高く (中央値)、攻撃者に支払った平均額は 510 万ドルでした。これは、金融サービス業界の事業運営におけるリスクが高く、業務停止への許容度が低いことに起因している可能性があります。攻撃者はより高額の身代金でも受け入れられやすいと考えている可能性があります。

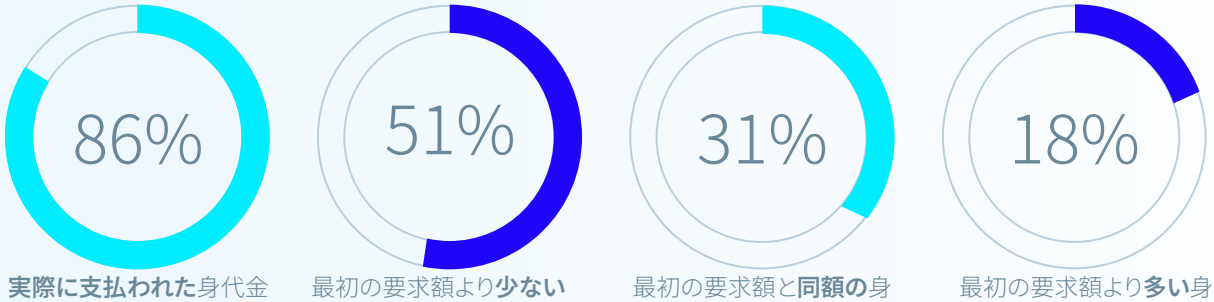
図 8：身代金の支払額 (業界別)



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 : 回答数が 30 未満の場合は、調査結果は参考値としてお考えください。

大規模企業が実際に支払った金額と初回の要求額の比較

身代金を支払った大規模企業 414 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 86% 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 95% から減少しており、歓迎すべき結果です。全体を見ると、51% 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、約 3 分の 1 (31%) が同額を支払っています。



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

大規模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

この調査では、一部の大規模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、他の大規模企業がそれを下回る支払いにとどめている理由についても調査を行い、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** 72 社の大規模企業が明らかにした理由を以下に示します。

- 61%：攻撃者がより多くの身代金を支払えると考えた。
- 49%：攻撃者が価値の高い標的と認識した。
- 42%：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。
- 39%：攻撃者が苛立ち、要求額を引き上げた。
- 31%：迅速に支払わなかったため、身代金の金額が上がった。

大規模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。

一方、最初の要求額より**少なく支払った** 214 社の大規模企業は、支払額を減らせた理由を以下のように説明しています。

- 49%：攻撃者と交渉して支払額を下げた。
- 46%：身代金を迅速に支払ったため割引を受けた。
- 45%：攻撃者が支払いを促すために要求額を下げた。
- 43%：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。
- 38%：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

大規模企業における復旧コスト

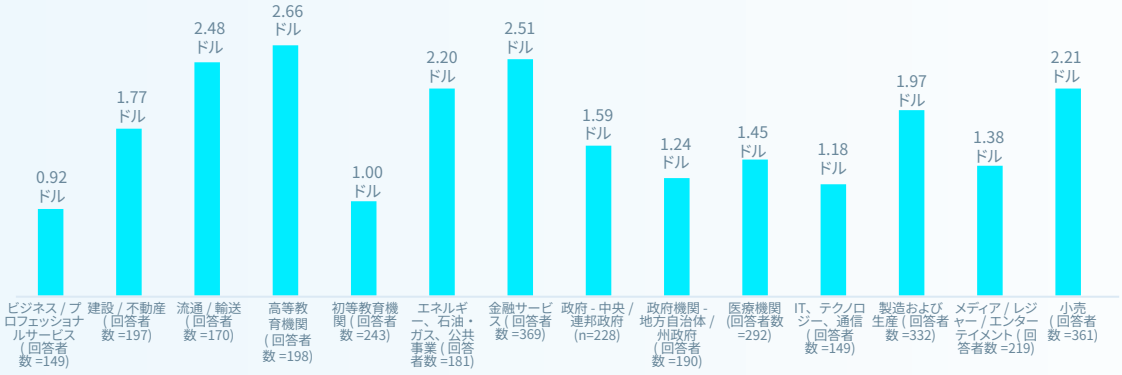
大規模企業がランサムウェア攻撃から復旧するための身代金支払いを除く平均費用は、過去 3 年間で最も低い水準にまで低下し、2024 年の 312 万ドルから 41% 減少し、2025 年に 184 万ドルとなりました。また、これは 2023 年に報告された 217 万ドルと比べても 33 万ドル少なくなっています。

2023	2024	2025
217 万ドル	312 万ドル	184 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 =1,733 (2025 年)、1,409 (2024 年)、1,045 (2023 年)

業界別に見ると、復旧コストの状況は大きく異なります。**初等中等教育機関**の大規模組織は、インシデントの復旧に要する平均コストが 266 万ドルと最も高くなっています。対照的に、**ビジネス / プロフェッショナルサービス**業界の大規模企業が復旧に要する平均コストは最も低く、92 万ドルでした。おそらく、この差異は、攻撃からの復旧に必要な IT インフラ再構築の労力の違いを部分的に反映しており、教育機関は一般に民間サービスプロバイダーよりも古いシステムを運用していることが要因と考えられます。

図 9：業界別の別のランサムウェア攻撃の復旧コスト (USD：100 万)

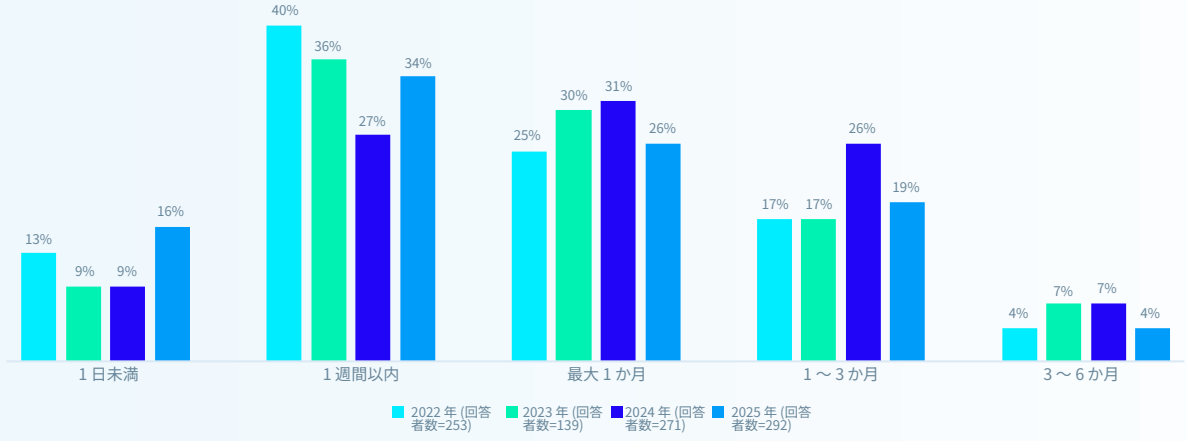


最も深刻なランサムウェア攻撃の影響において、組織が復旧に要した概算コスト (ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益など) は、支払った身代金を除いて、どれぐらいですか? 回答数を図内に記載。

大規模企業が復旧にかかる時間

データによると、2025 年には大規模企業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。大規模企業の半数は 1 週間以内に復旧しており、2024 年の 36% から増加しました。同時に、復旧に 1 ～ 3 か月かかる割合は 2024 年の 26% から 19% に減少しました。全体として、被害を受けた大規模企業の 95% が 3 か月以内に完全に復旧しており、これら企業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 10：ランサムウェア攻撃から大規模企業が復旧に要する時間 (2022 年から 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。

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、大規模企業の 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、自社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 =848

提言

過去 1 年間で大規模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、影響を軽減できます。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。質の高いバックアップを確実に作成し、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。

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。

2025-12-08 WP (MP)