レポート

ランサムウェアの現状 2026 年版

17 か国の IT およびサイバーセキュリティリーダー 2,158 人から得られた洞察

SOPHOS

はじめに

AI の登場により、ランサムウェアを取り巻く状況は急速に変化しています。サイバーセキュリティ対策への継続的な投資を行っている組織では、より良好な成果が得られていますが、ランサムウェア攻撃によって企業は依然として数百万ドル規模の損失を被っています。

本レポートは、ソフォスが毎年発行している「ランサムウェアの現状レポートの第 7 版で、前年におけるランサムウェア攻撃に関する新しいデータを提供しています。調査結果を次のセクションにまとめて解説します。

- 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

これらのデータから、高いコストを伴う被害が続く一方で、確かな前進も見られるという状況も浮かび上がっています。

- ランサムウェアの復旧コストは高額であり、平均的な復旧コストは 170 万ドルに達しています。
- ランサムウェア攻撃の半数以上 (56%) は、依然としてデータの暗号化に成功しており、その割合は 2025 年から上昇しています。
- 一方で、身代金要求額および支払額は減少傾向にあり、組織はより効果的に交渉して有利な結果を引き出せるようになっています。過去 2 年間で、身代金要求額の中央値は 65% 減少し、支払額の中央値も 62% 減少しています。
- 3 年間にわたり首位だった脆弱性の悪用は、ランサムウェア攻撃の最大の根本原因ではなくなりました (18%)。現在では、メールを起点とした攻撃 (フィッシング 24%、悪意のあるメール 26%) が最も一般的な攻撃ベクトルとなっています。

2,158

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 17 か国の IT およびセキュリティリーダーを対象に実施した、ベンダーに依存しないグローバル調査に基づいています。

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 7 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。

主な調査結果の概要

- **アイデンティティの侵害がランサムウェアの主な侵入経路に**
  - 悪意のあるメール (26%) とフィッシング (24%) は、ランサムウェア攻撃の主な根本原因となっています。
  - 過去 3 年間の最大の根本原因である脆弱性の悪用は、過去 1 年間で 14% 減少し、18% となりました。
  - ランサムウェアの被害者の 3 分の 2 (67%) が、ランサムウェアインシデントがアイデンティティ攻撃による最も重大な結果であると回答しています。
- **保護機能、セキュリティ対策、リソースの不足が組織を攻撃リスクにさらす**
  - 既知または未知の「セキュリティギャップ」は、2 年連続で最も多く挙げられた運用上の根本原因となり、62% を占めました。これに続いて、「人員またはスキルの不足」が 58%、「保護対策の不足または品質の低さ」が 57% となりました。
- **多要素認証 (MFA) 導入だけではランサムウェアを阻止できない**
  - 認証情報の侵害がランサムウェア攻撃の根本原因であったインシデントの 97% で、一定レベルの MFA が導入されていました。
- **半数以上のインシデントで、組織はランサムウェア攻撃の早期検知と阻止に失敗している**
  - ランサムウェア攻撃の半数以上 (56%) がデータの暗号化に成功しており、そのうちの 16% はデータの暗号化とデータの窃取の両方に成功しています。
- **データが暗号化された場合、攻撃者が身代金を受け取る確率は約 50%**
  - 48% の組織が、データを暗号化され身代金を支払いました。
  - 暗号化された場合に身代金を支払う割合は、現在 4 年間平均で 50% になっています。
- **身代金要求額は減少する一方、復旧が困難な特権システムへのアクセスを得た攻撃者は、より高額な身代金を要求している**
  - 身代金要求額の中央値は 698,000 ドルまで減少し、複数年にわたって減少傾向が続いています。2025 年版レポートでは 130 万ドル、2024 年版レポートでは 200 万ドルだった中央値から、さらに低下しました。
  - ファイアウォールの脆弱性悪用を起点とする攻撃では、59% のケースで身代金要求額が 100 万ドル以上となり、全体 (48%) を上回っています。
- **身代金の支払額は減少しており、多くの被害組織は当初の要求額を下回る金額での交渉に成功している**
  - 身代金支払額の中央値は 769,000 ドルとなり、昨年の 100 万ドルから大幅に減少しました。
  - 100 万ドル以上の支払いは半数弱 (48%) となり、前年の 52% から減少しました。
  - 身代金を支払った組織の約半数 (51%) が要求された金額よりも少ない金額を支払っています。これは 2025 年のレポート (53%) とほぼ同じ水準であり、2024 年のレポート (44%) よりも 7% 高くなっています。
- **ランサムウェア攻撃から復旧するためのコストは増加した**
  - 身代金の支払いを除くランサムウェア攻撃からの平均復旧コストは 170 万 200 ドルとなり、2025 年版レポートの平均コスト 152 万 5,716 ドルから 11% 増加しました。
- **データが暗号化されたほぼすべての場合、IT/ サイバーセキュリティチームのメンバーに影響を及ぼす**
  - データが暗号化されたランサムウェアの被害者の 99% が、IT/ サイバーセキュリティチームに影響を与えたと回答しています。
  - 今後の攻撃に対する不安やストレスの増加は、最も一般的な影響 (41%) であり、シニアリーダーからの圧力の増加 (40%) が続きます。
  - シニアリーダーからの評価の向上は、前年比で増加した唯一の影響であり、2025 年レポートの 31% から 36% に増加しています。

攻撃と防御の方法

攻撃の根本原因

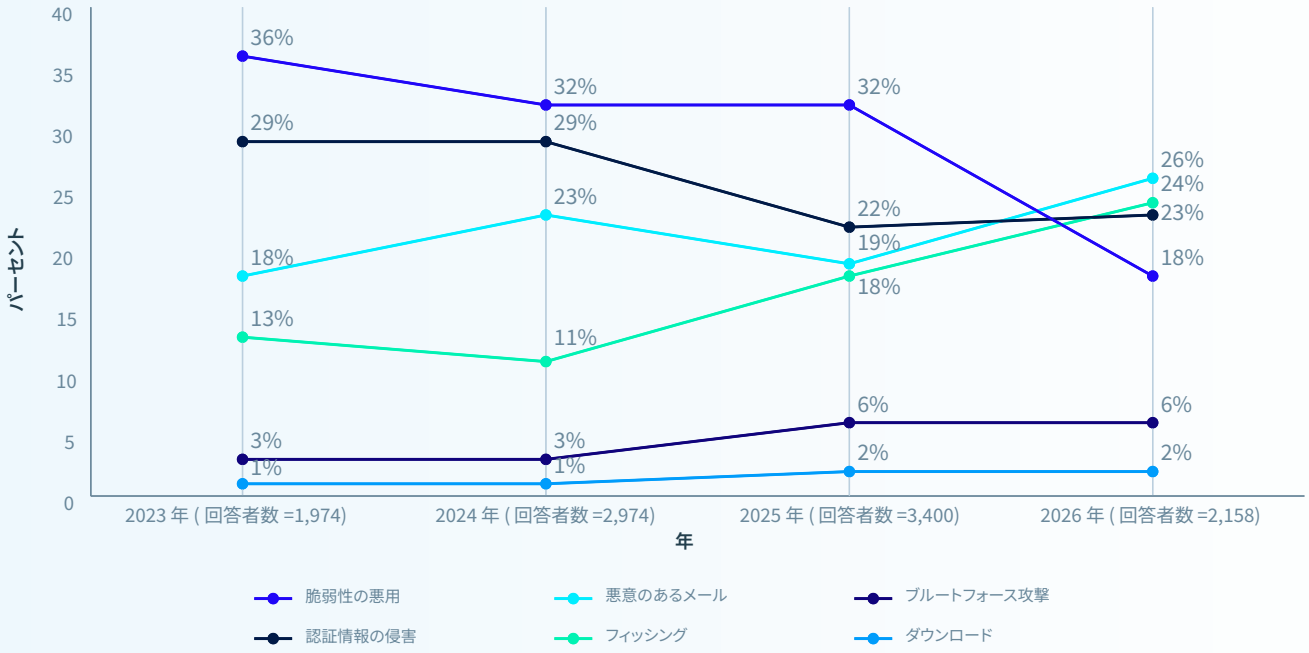
今年のレポートでは、ランサムウェア攻撃の技術的な根本原因の順位に変化が見られました。ランサムウェア攻撃の最も多い 2 つの根本原因は、悪意のあるメール (26%) とフィッシング (24%) であり、すべてのインシデントの半数を占めています。これまで脆弱性の悪用が一貫してランキングのトップでしたが、前年から大きな変化がありました。

脆弱性の悪用が根本原因だったとする回答は、2025 年版レポートの 32% から、2026 年版レポートでは 18% へと減少しました。しかし、最先端 AI による脆弱性発見能力が飛躍的に向上していることを踏まえると、今後 1 年間は、脆弱性の悪用を根本原因とするランサムウェア攻撃が増加する可能性があるため、組織は引き続き警戒を怠るべきではありません。

認証情報の侵害は、3 番目に多い根本原因であり、23% と前年と変わりませんでした。

攻撃の 79% はアイデンティティベースの手法によって開始されており、認証情報を窃取して悪用するケースと既に窃取された認証情報を悪用するケースの両方のアプローチが見られました。この結果は、包括的なセキュリティポスチャを向上するために、アイデンティティセキュリティが極めて重要な要素であることを示しています。

ランサムウェア攻撃の技術的な根本原因 (2023 年〜 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?回答数を図内に記載。

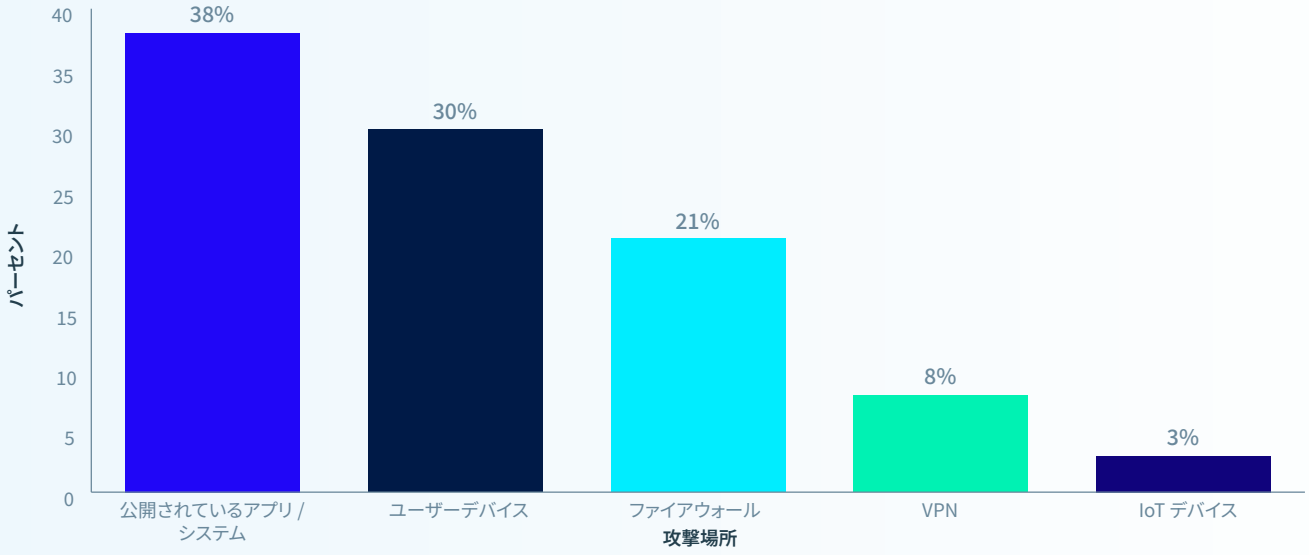
新しい調査

攻撃の開始場所

今年のレポートでは初めて、組織環境内のどの領域で根本原因が発生したのかを分析しています。攻撃がどこから始まるのかを把握することは、リスク低減戦略を策定するうえで重要な知見となります。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を起点としたランサムウェア攻撃では、**最も一般的な侵入経路は公開されたアプリケーションおよびシステム (38%) で**、次いでユーザーデバイス (30%)、ファイアウォール (21%) となりました。

公開されたアプリケーションが主な侵入経路となっている背景には、クラウドや SaaS 環境への移行が進んでいることがあります。こうした環境では、インターネットに公開されたシステムが広範囲かつ拡大を続けるアタックサーフェスとなっています。

ランサムウェア攻撃の場所



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が根本原因であると回答されましたが、これは自社環境のどこで発生しましたか？回答者数 =1,022

さらに詳しく分析すると、公開されたアプリやシステム、ファイアウォール、VPN、IoT デバイスにおいて、侵害された認証情報が広く利用されている実態がデータから明らかになりました。

組織環境内の各領域における主な根本原因

根本原因	公開されているアプリケーションまたはシステム	ファイアウォール	VPN	IoT デバイス
認証情報の侵害	59%	41%	44%	48%
脆弱性の悪用	31%	33%	41%	36%
ブルートフォース攻撃	10%	26%	15%	16%

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が根本原因であると回答されましたが、これは自社環境のどこで発生しましたか？一部の回答を掲載。回答者数 =711

公開されたアプリケーションおよびシステムでは、侵害された認証情報を悪用した攻撃が 59% と特に多くを占めており、外部からアクセス可能な資産の保護とアイデンティティ管理の強化が重要であることを裏付けています。

同じデータを別の切り口で分析したところ、侵害された認証情報やブルートフォース攻撃が主に標的としていた対象が明らかになりました。

ランサムウェア攻撃の起点となった場所

攻撃場所	合計 %	認証情報の侵害 %	ブルートフォース攻撃 %
公開されているアプリケーションまたはシステム	38%	46%	30%
ユーザーデバイス (ネットワーク上またはネットワーク外 - ノートパソコンやデスクトップなど)	30%	27%	13%
ファイアウォール	21%	18%	44%
VPN	8%	7%	9%
IoT デバイス	3%	3%	4%

認証情報の侵害またはブルートフォース攻撃が根本原因であると回答されましたが、これは自社環境のどこで発生しましたか？一部の回答を掲載。回答者数 =628

攻撃の種類によって、攻撃の対象になる場所が異なります。

- 認証情報が侵害されてランサムウェア攻撃が開始されたケースは、公開されているアプリケーションとシステムに集中しており (46%)、次に多かったのはユーザーデバイスでした。
- ブルートフォース攻撃では、44% のケースでファイアウォールが標的となっており、ネットワーク境界に配置されたデバイスで、レート制限やアカウントロックアウトポリシーを導入することの重要性が浮き彫りになっています。

新しい調査

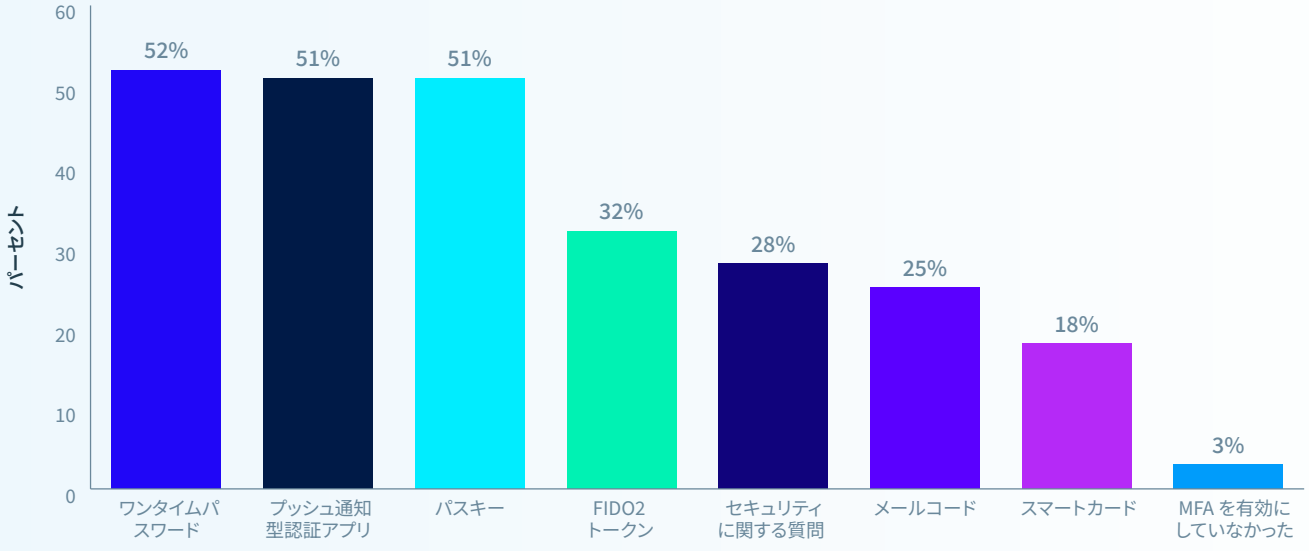
多要素認証 (MFA) の役割

今年のレポートでは初めて、ランサムウェア攻撃における MFA の役割についての新たな知見も紹介しています。

認証情報の侵害がランサムウェア攻撃の根本原因となった組織のうち 97% は、インシデント発生時点で何らかの形で多要素認証を導入していました。最も広く導入されていた MFA 方式は、ワンタイムパスワード (52%)、プッシュ通知型認証アプリ (51%)、およびパスキー (51%) でした。回答者は平均して 2.5 種類の MFA 方式を利用していると回答しています。

ランサムウェア攻撃を受けた組織の多くが、攻撃時点で MFA を導入していたという結果は、MFA が関連するすべてのシステムに完全には適用されておらず、その隙を攻撃者に悪用された可能性があることを示唆しています。また、この結果は、MFA は効果的なサイバー防御戦略に不可欠である一方、回避手法が進化し続けているため、認証情報を悪用した攻撃を防ぐには MFA だけでは十分ではないことを示しています。

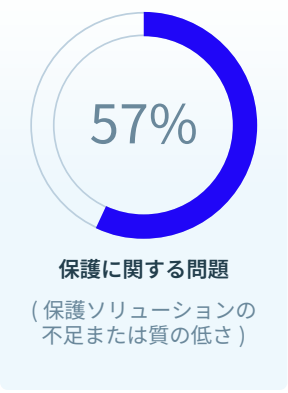
攻撃時に有効であった MFA の方法



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？回答者数：認証情報の侵害が原因で攻撃が発生した。回答者数 =503

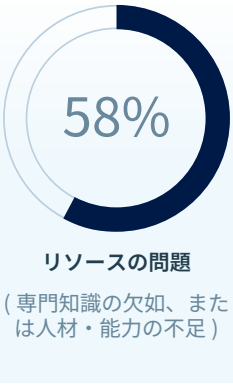
組織が脆弱になった要因

2 年連続で、組織が攻撃にさらされる原因となる突出した単一の運用上の要因は見られませんでした。回答者は、保護対策の欠落や品質の低い保護対策、人材 / スキル不足、セキュリティ上のギャップなど、幅広い課題を挙げています。



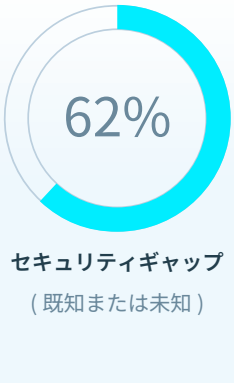
保護に関する問題

(保護ソリューションの不足または質の低さ)



リソースの問題

(専門知識の欠如、または人材・能力の不足)



セキュリティギャップ

(既知または未知)

セキュリティギャップは、2 年連続で運用上の根本原因として最も多く挙げられたカテゴリであり、62% でした。次に多かったのは、人材 / スキル不足 (58%)、保護対策の欠落や品質の低い保護機能 (57%) でした。

心強いことに、個別要因のほとんど (1 項目を除く) は前年から減少しました。**一方、人為的ミス (35%) は、前年から増加した唯一の運用上の要因となりました。**

2025 年と同様に、ランサムウェア被害を受けた組織は複数の運用上の課題を抱えていると回答しており、挙げられた要因は平均 2.5 項目でした **(前年は 2.7 項目)。**

35%

人為的ミス：唯一変わらないリスク。攻撃の運用上の根本原因のうち、2025 年版レポートから割合が減少しなかった唯一の項目。

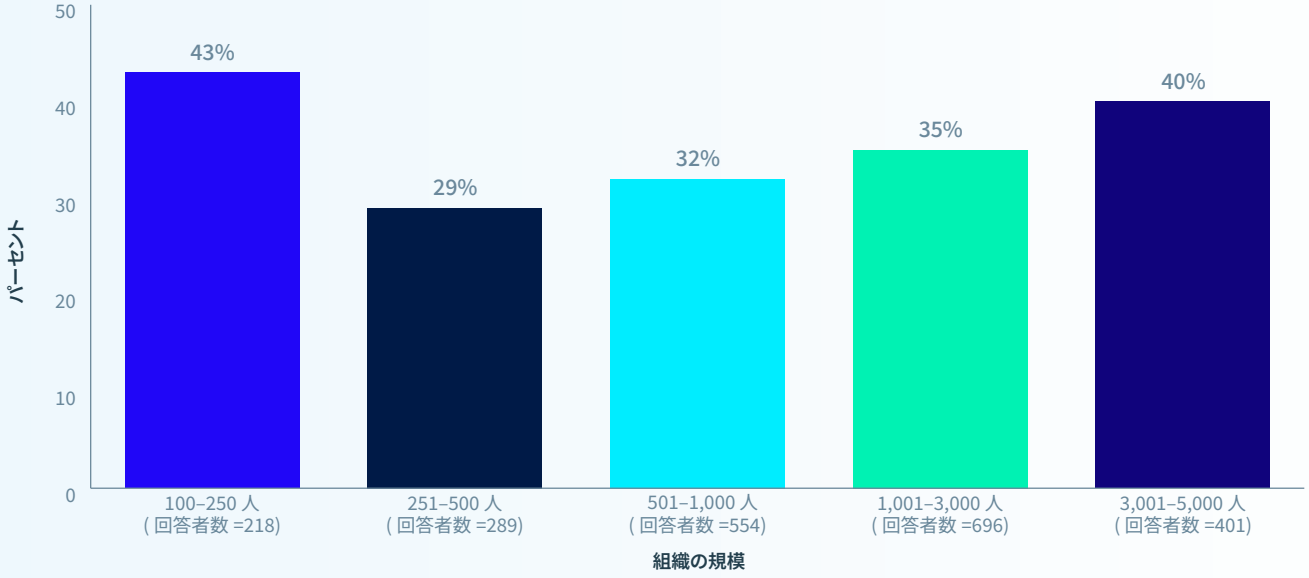
ランサムウェア攻撃の運用面の根本原因トップ 7

ランク	2025 年	%	ランク	2026 年	%
1	専門知識の欠如	40.2%	1	保護対策の不足	36.4%
2	不明なセキュリティギャップ	40.1%	2	不明なセキュリティギャップ	36.3%
3	人材や能力の不足	39.4%	3	既知のセキュリティギャップ	36.0%
4	保護対策の不足	39.0%	4	人材や能力の不足	35.3%
5	既知のセキュリティギャップ	38.2%	5	人為的ミス	35.3%
6	品質の低い保護機能	37.1%	6	専門知識の欠如	35.1%
7	人為的ミス	34.2%	7	品質の低い保護機能	32.6%

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 (2025 年)、回答者数 =2,158 (2026 年)

予想どおり、従業員数 100 ～ 250 人規模の組織では、人員や対応能力の不足が根本原因として挙げられる割合が特に高くなりました。一方で、従業員数 3,001 ～ 5,000 人規模の企業でも、約 4 割が対応能力不足を課題として挙げており、その割合は従業員数 100 ～ 250 人規模の組織よりわずか 3% 低いだけでした。このことは、組織規模が大きくなっても、人材やリソースの確保が必ずしも容易になるわけではないことを示しています。

人員や対応能力の不足がランサムウェア被害につながる要因に



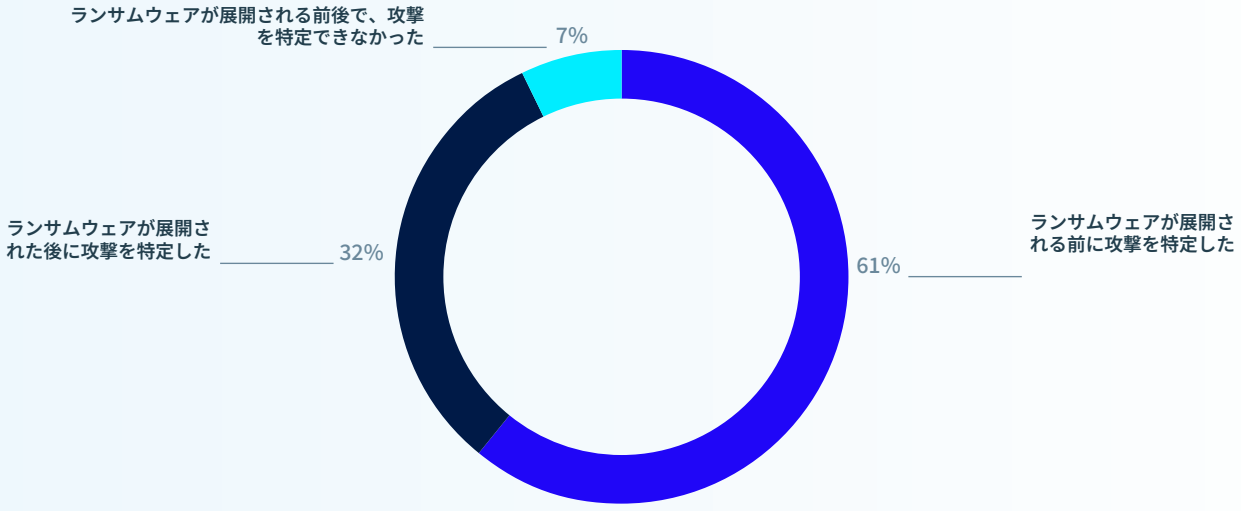
自社がランサムウェア攻撃の被害に遭った理由は何だと思いますか？ 攻撃発生時にシステムを監視して対応するサイバーセキュリティ専門家を十分に配置していなかった。回答数を図内に記載。

新しい調査

ランサムウェア対策におけるファイアウォールの役割

被害組織の 61% は、ランサムウェアのペイロードが実行される前にファイアウォールが攻撃を検知したと回答しました。一方、32% は、ランサムウェアが展開された後にファイアウォールが攻撃を検知したと回答しています。ファイアウォールが攻撃をまったく検知しなかったと報告した組織はわずか 7% でした。

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？回答者数 =2,158

ファイアウォールが攻撃を検知できなかった被害組織 (7%) では、データが暗号化される割合が 71% と最も高くなりました。一方、ランサムウェアが実行される前にファイアウォールが攻撃を検知した場合、その割合は 50% でした。ランサムウェアが展開された後に検知 (通常、インシデント発生後にランサムウェア攻撃との関連が判明したシグナルを特定したケース) した場合、データ暗号化率は 65% でした。

今回の調査結果から、ファイアウォールはランサムウェア攻撃の検知において重要な役割を果たしており、これらのデバイスから得られるテレメトリは、攻撃者の活動を早期に把握するための貴重なシグナルとなっています。ファイアウォールのテレメトリは、XDR ツールや MDR サービスを通じて、エンドポイント保護やメールセキュリティソリューションなどセキュリティ環境全体から得られる情報と組み合わせることで、防御担当者がデータが暗号化される前にランサムウェア攻撃を検知して阻止するための有力な手段となります。

ファイアウォールによる攻撃検知がデータ暗号化率に与える影響

	ランサムウェアが展開される前に攻撃を特定した	ランサムウェアが展開された後に攻撃を特定した	ランサムウェアが展開される前後で、攻撃を特定できなかった
サイバー犯罪者はデータの暗号化に成功した	50%	65%	71%
サイバー犯罪者はデータの暗号化に失敗した	50%	35%	29%

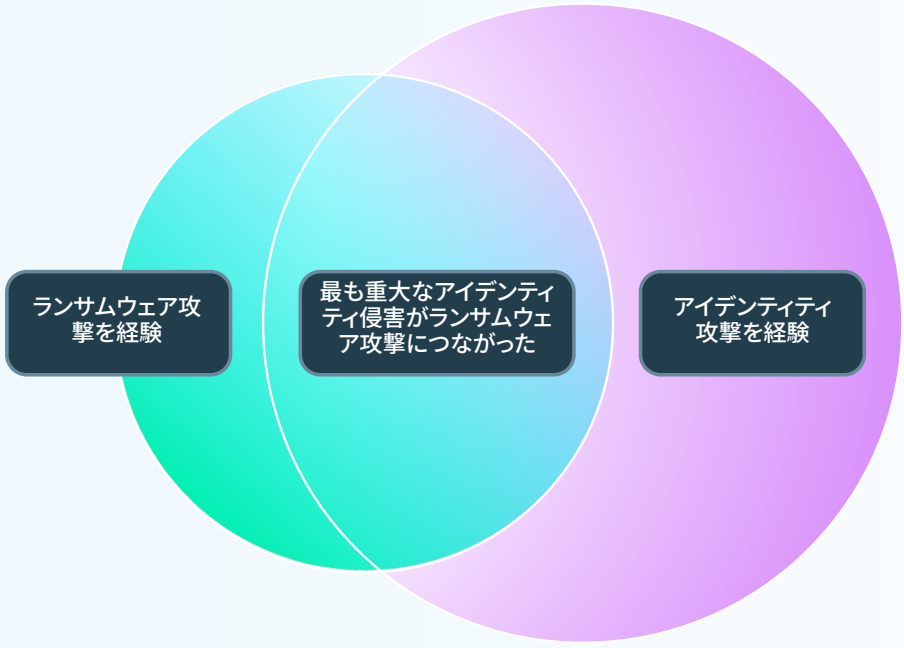
ファイアウォールは攻撃を特定するためにどのような役割を果たしましたか？ランサムウェア攻撃で組織のデータは暗号化されましたか？
回答者数 =2,158

ファイアウォールは組織の IT インフラにおいて極めて重要な位置を占めており、侵害されると、環境内の他のシステムに比べてビジネスへの影響がより大きくなる可能性があります。攻撃者がファイアウォールの脆弱性の悪用に成功すると、多くの場合、組織全体にわたる広範なアクセス権限を取得します。これらのシナリオにおける身代金要求額の違いからも、このことが裏付けられます。**ファイアウォールの脆弱性悪用を起点とする攻撃では、59% のケースで身代金要求額が 100 万ドル以上となり、**攻撃全体 (48%) を上回っています。

新しい調査

アイデンティティとランサムウェアの関連性

今年の調査で最も注意すべき発見の一つは、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。昨年ランサムウェア被害を受けた組織のうち、3 分の 2 (67%) は、そのランサムウェアインシデントが自社における最も重大なアイデンティティ攻撃と同一のイベントであったと回答しています。すべての攻撃がデータ暗号化につながったわけではないものの、アイデンティティの侵害がランサムウェアを展開する主要な手段であることが示されています。



データの内訳：過去 1 年間にランサムウェア攻撃を受けましたか？という質問に「はい」と回答、回答者数 =5,000。過去 12 か月間に、アイデンティティ関連のセキュリティ侵害を受けましたか？という質問に「はい」と回答、回答者数 =5,000。[両方に当てはまる場合] ランサムウェアインシデントは、アイデンティティに関連する最も重大な攻撃と同じイベントでしたか？

データ暗号化と復旧

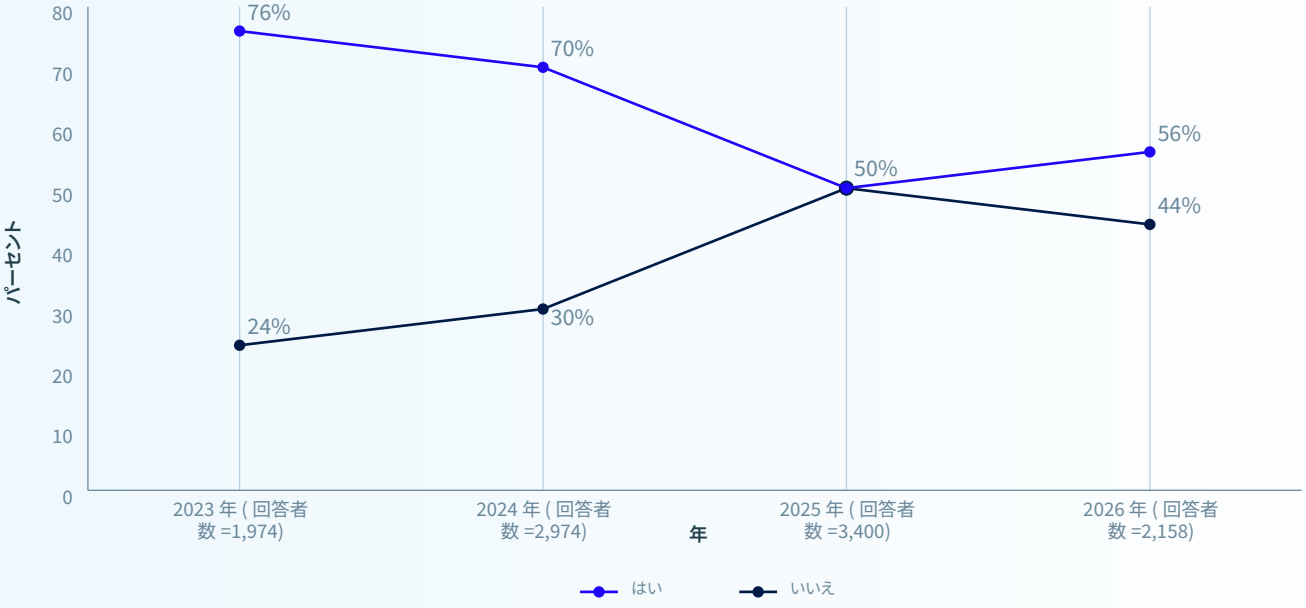
データ暗号化率

ランサムウェア攻撃の半数以上 (56%) がデータの暗号化に成功しました。この暗号化率には、データが暗号化されただけのケース (40%) と、データが暗号化され窃取されたケース (16%) が含まれます。攻撃の 41% は暗号化前に阻止され、2% は暗号化を伴わない恐喝型攻撃でした。

+6%

昨年のレポートからのランサムウェア暗号化率の増加率。

攻撃でデータが暗号化されましたか？ (要約：はい / いいえ)

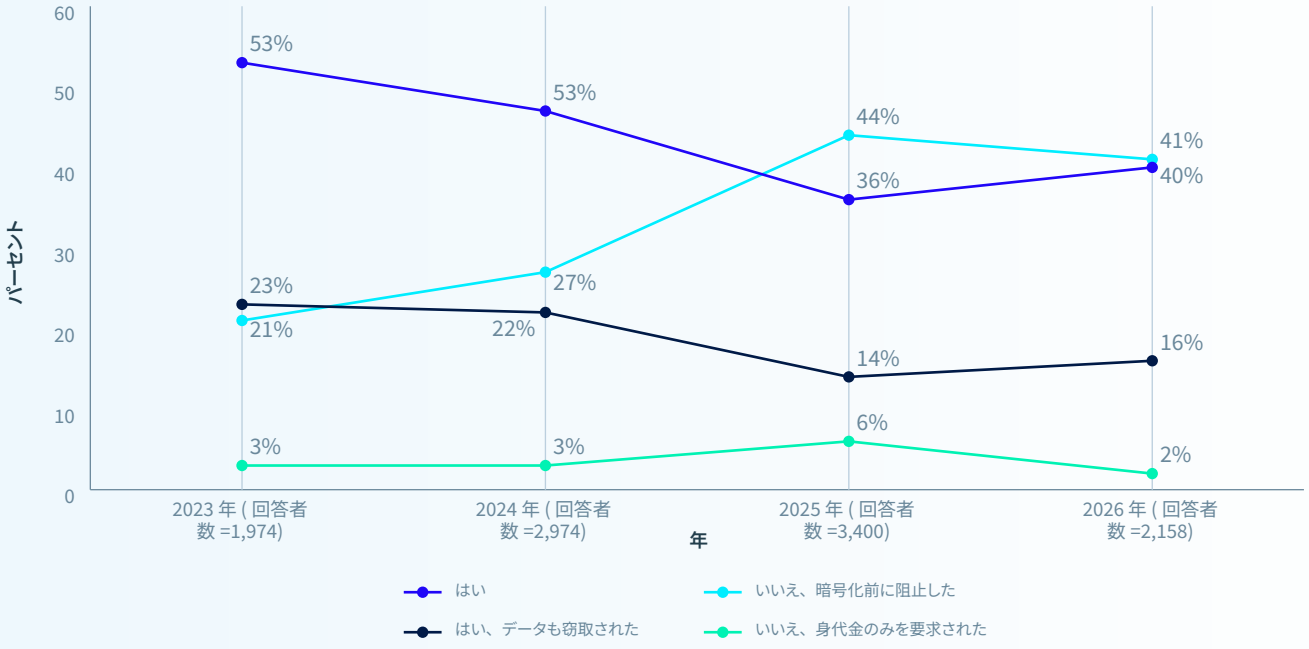


ランサムウェア攻撃で組織のデータは暗号化されましたか？要約された回答：はい / いいえ。回答数を図内に記載。

データ暗号化率は、2023 年版レポートで記録したピーク値 (76%) を依然として大きく下回っていますが、2025 年版レポートで記録した最低値 (50%) からはやや上昇しました。この反転には注意が必要です。2 年連続でデータ暗号化の成功率が低下しましたが、攻撃者は再び一定の優位性を取り戻しつつあるようです。

データの暗号化と窃取を組み合わせた攻撃は全体の 16% を占めており、特に警戒すべきです。こうした二重の被害をもたらす攻撃では、攻撃者が被害者を恐喝するための複数の圧力材料を確保できるためです。

攻撃でデータが暗号化されましたか？

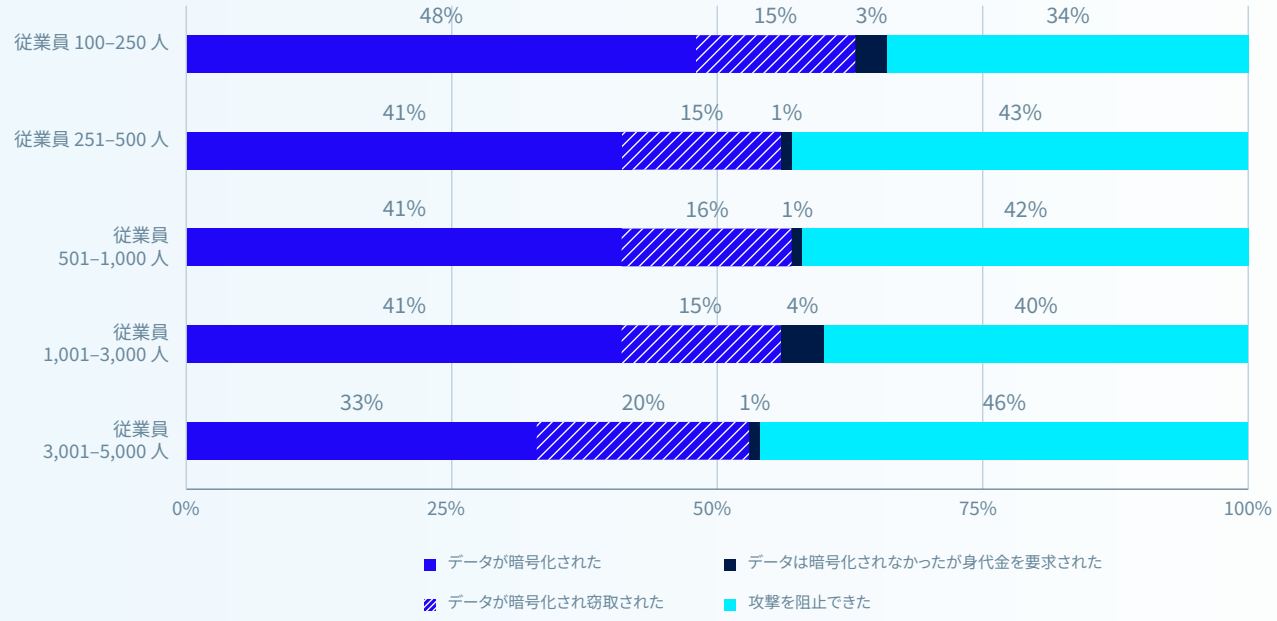


ランサムウェア攻撃でデータは暗号化されましたか？ (回答選択肢の全リスト) 回答者数：ランサムウェア攻撃を受けた組織。回答数を図内に記載。

データ暗号化の結果は組織規模によって異なり、**調査対象の中で最も規模の大きい組織 (従業員数 3,001 ～ 5,000 人) では、データの暗号化や恐喝に至る前に攻撃を阻止できた割合が 46% と最も高くなりました。**一方、最も規模の小さい組織 (従業員数 100 ～ 250 人) では、その割合は 34% にとどまりました。

一方、大規模組織で攻撃者がデータの暗号化に成功したケースでは、データ窃取も伴う割合が高くなりました。「データの暗号化と窃取の両方」の被害を受けた割合は、最も規模の大きい組織で 20% となり、その他の大半の組織の 15% を上回っています。ランサムウェアを展開するだけでなくデータも窃取することで、攻撃者は攻撃によって利益を得るための新たな機会を確保することが可能になります。

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組織のデータは暗号化されましたか？回答者数 =2,158

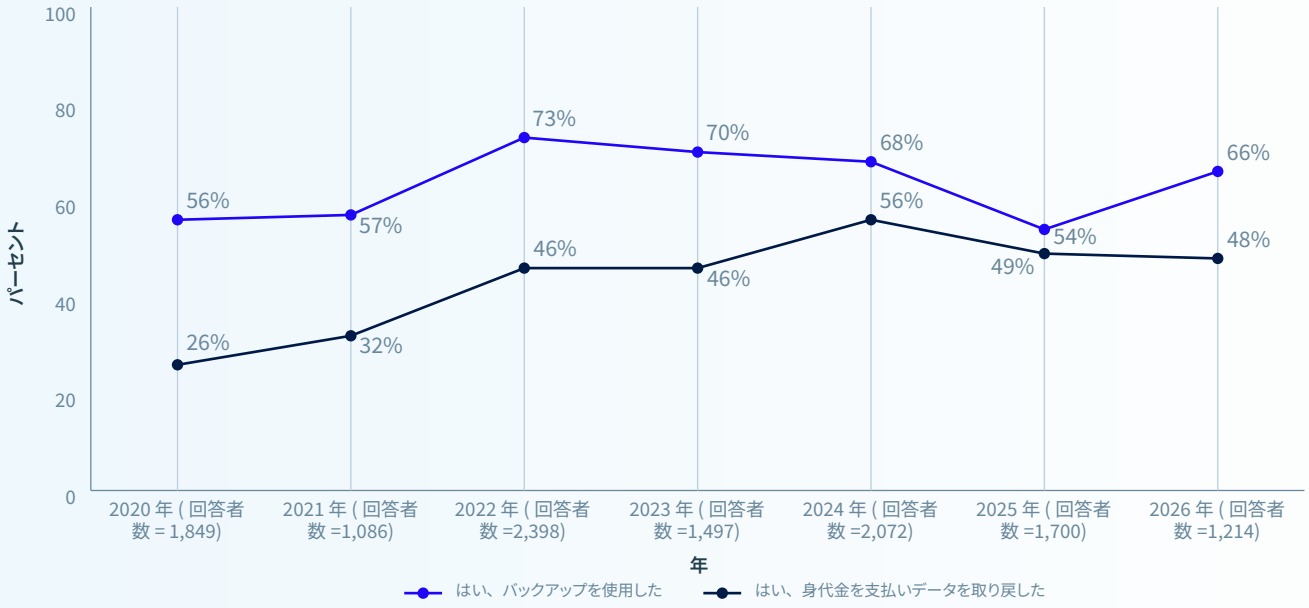
組織が暗号化されたデータを復旧した方法

データが暗号化された攻撃において、バックアップを利用して復旧した割合は 66% に増加し、2025 年版レポートの 54% から大きく上昇しました。この大幅な回復は、2025 年の利用率低下を受けて、組織がバックアップ基盤への投資を再び進め、身代金要求に対するレジリエンスを強化していることを示しています。

+12%

ランサムウェア攻撃からの復旧におけるバックアップ活用の増加率 (2025 年～ 2026 年)

ランサムウェア攻撃後、どのようにデータを復旧しましたか？



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。回答数を図内に記載。複数回答可のため、合計が 100% を超える場合があります。

データ復旧のために身代金を支払った組織の割合は 48% に低下し、過去 3 年間で最も低い水準となりました。データを一切復旧できなかった組織はわずか 2% にとどまりました。これは、データが暗号化された場合でも、何らかの手段による復旧がほぼ例外なく可能であることを示しています。

要求された身代金額と支払った身代金

身代金要求額

今年のレポートでは、身代金要求額の中央値は 69 万 8,000 ドルに低下し、数年にわたり減少傾向が続いています。これは、過去 2 年間で 65% 減少したことを意味します。この期間における身代金要求額の平均値も低下し、312 万 6,372 ドルとなりました。これは、2024 年版レポートから 28% の減少です。

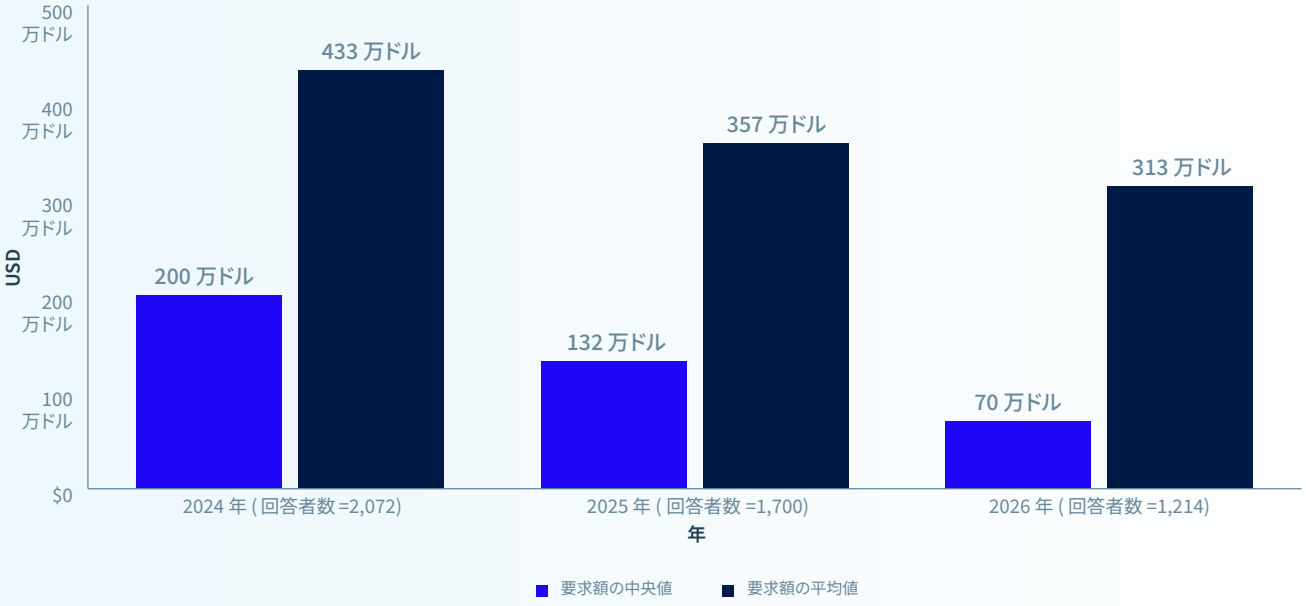
平均値と中央値の差が拡大していることは、分布が大きく偏っていることを示しています。少数の非常に高額な要求が平均値を押し上げている一方で、一般的な組織が直面する身代金要求額は 70 万ドル未満になっています。

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。

69 万 8,000 ドル

過去 1 年間のランサムウェアによる身代金要求額の中央値。

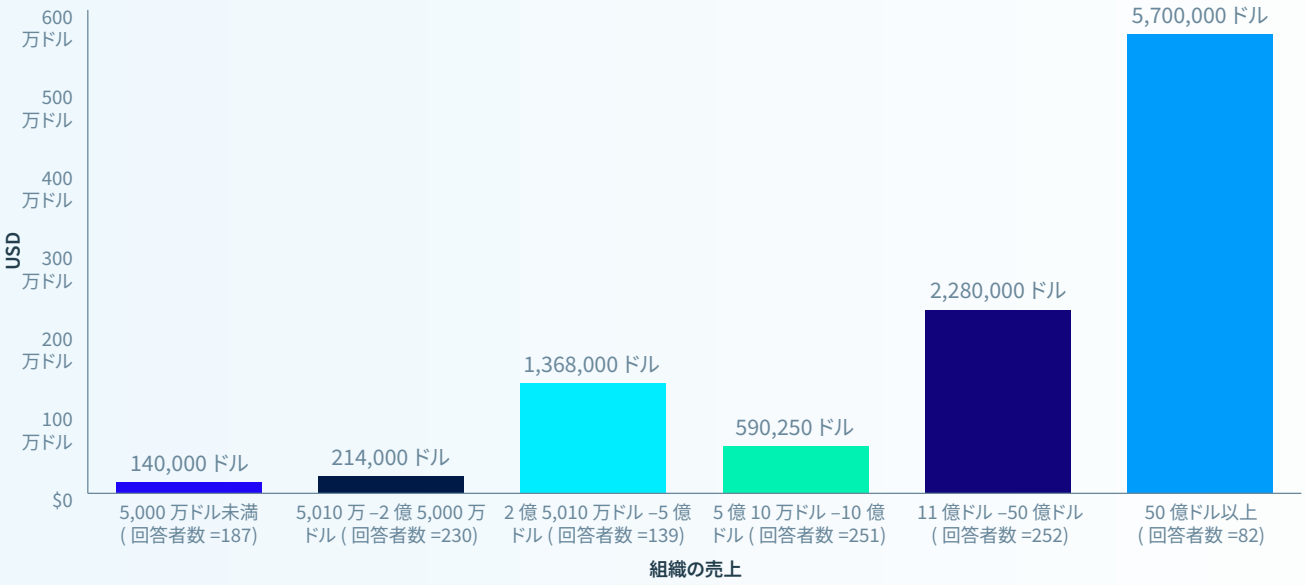
身代金要求額の平均値と中央値



攻撃者から要求された身代金額はいくらでしたか?対象：データが暗号化された組織。回答数を図内に記載。4,000 万ドル以上の異常な要求額は除外されています。

身代金の要求は、組織の売上規模に応じて急激に増加する傾向があります。売上高が 5,000 万ドル未満の組織では、身代金要求額の中央値は約 14 万ドルでした。一方、売上高が 50 億ドルを超える組織では、中央値が 570 万ドルに達しました。この傾向は、攻撃者が偵察活動を行い、標的組織の支払い能力を推定したうえで身代金要求額を調整していることを強く示唆しています。

身代金要求額の中央値



要求された身代金額はいくらでしたか？対象：データが暗号化された組織。回答数を図内に記載。4,000 万ドル以上の異常な要求額は除外されています。

身代金の支払額

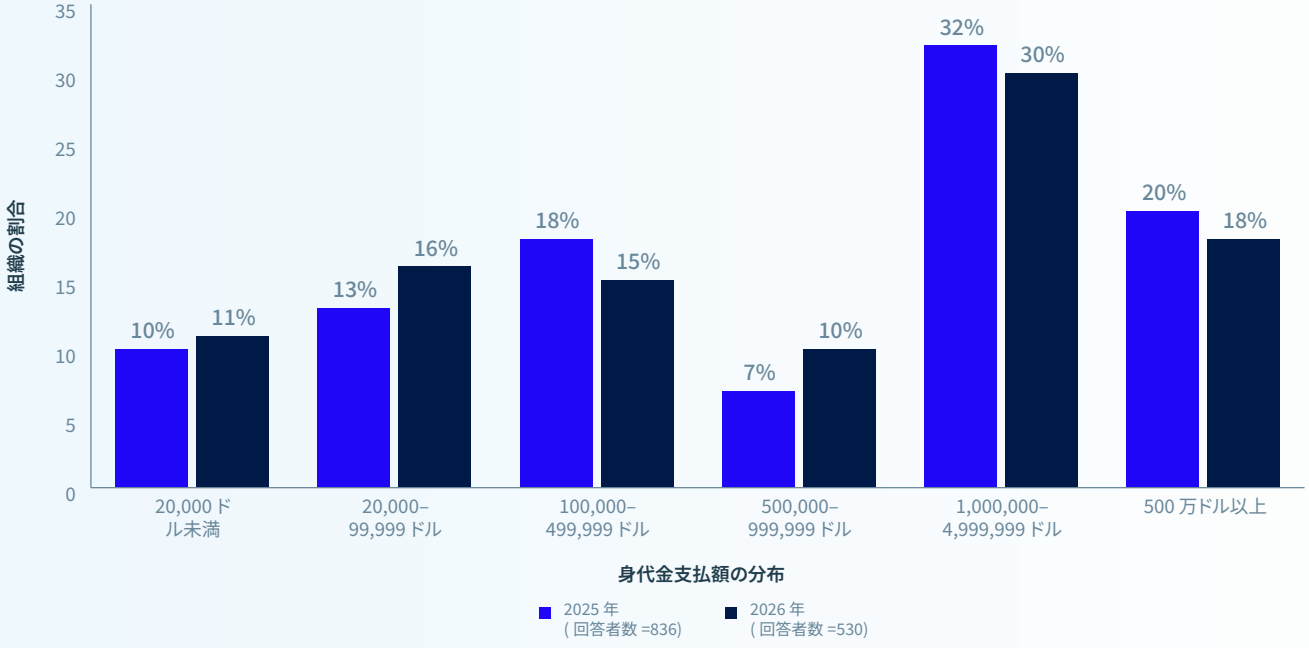
身代金を支払った 530 の組織から支払額に関する回答を得た結果、身代金支払額の中央値は 76 万 9,000 ドルとなりました。これは、前年のレポートで報告された 100 万ドルから大きく減少しています。100 万ドル以上の支払いは半数弱 (48%) となり、前年の 52% から減少しました。

支払額の分布全体を見ると、金額帯の中心が中間層へ移行していることがわかります。最も高額な 2 つの金額帯 (100 万～ 500 万ドル、500 万ドル以上) は、いずれも前年のレポートから減少しました。一方、20,000 ～ 99,999 ドルおよび 500,000 ～ 999,999 ドルの金額帯はそれぞれ増加しており、攻撃者と被害組織の双方が、低～中額の支払水準に移行しつつあることを示しています。

76 万 9,000 ドル

過去 1 年間の身代金支払額の中央値。

身代金支払額の分布

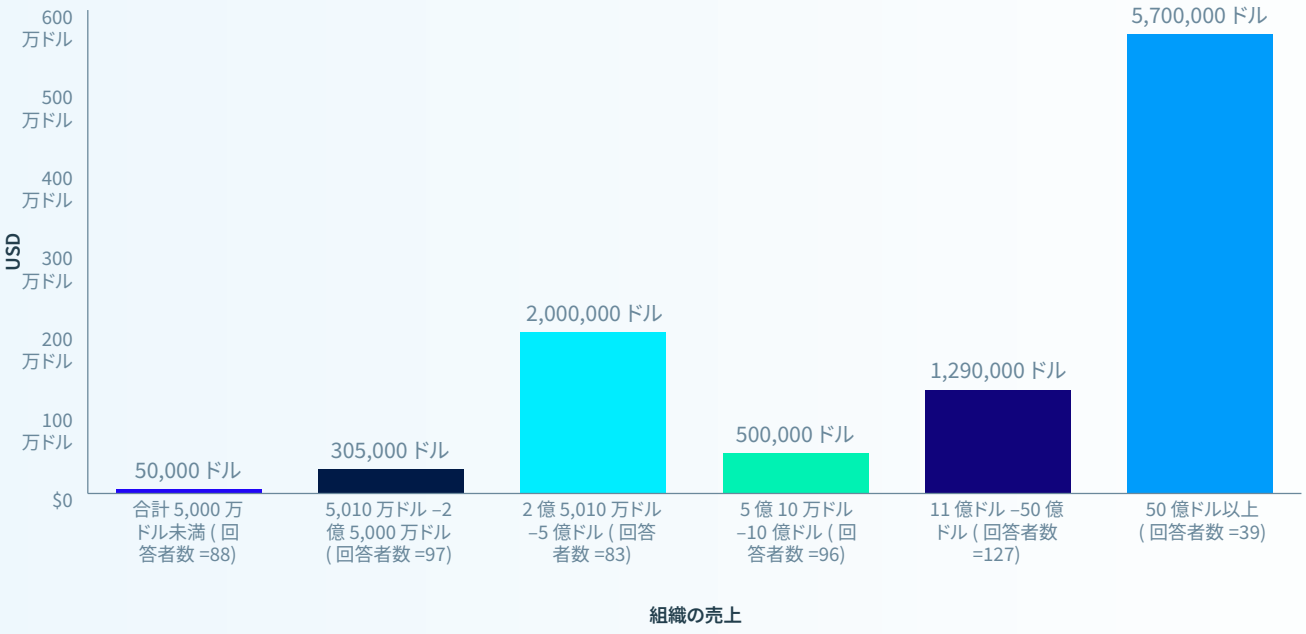


攻撃者に支払った身代金はいくらでしたか？回答数を図内に記載。

組織の売上規模別に身代金支払額を分析すると、売上高 2 億 5,010 万～ 5 億 ドルの組織で突出した値が見られ、支払額の中央値は 200 万ドルに達しました。これは、年間売上高 50 億ドル超の最大規模の組織を除き、すべてのセグメントを上回る水準であり、売上高 5 億 10 万～ 10 億ドルの組織の 4 倍に相当します。

身代金要求額のデータでも、売上高 2 億 5,010 万 –5 億ドルのセグメントで同様の突出が見られ、身代金要求額の中央値は 137 万ドルでした。これは、その上の売上規模のセグメントの 59 万ドルと比べても高く、このセグメントがランサムウェアの影響を特に受けやすいことを示しています。

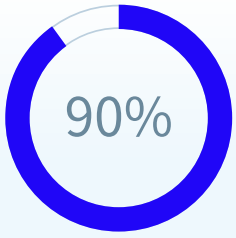
身代金の支払いの中央値



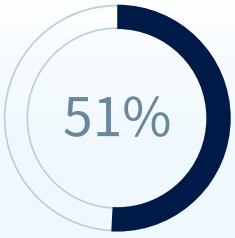
攻撃者に支払った身代金はいくらでしたか？調査対象：組織が身代金を支払った組織。回答数を図内に記載。

実際の支払額と最初の要求額の比較

身代金要求額と支払額の両方を共有した 507 の組織のデータから、組織が攻撃者との交渉でどの程度成果を上げているかが明らかになりました。**支払額の中央値は要求額の 90% (平均値では 85%)** でした。初回の要求額を下回る金額を支払った組織がわずかに過半数以上の 51% を占め、要求額どおりに支払った組織は 30%、要求額を上回る金額を支払った組織は 18% でした。これらの数値は前年の結果とほぼ同じであり、身代金要求額と実際の支払額の関係が比較的安定して推移していることを示しています。

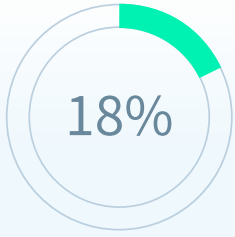


身代金支払率の中央値



最初の要求額よりも**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



最初の要求額よりも**多い**身代金を支払った割合

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？調査対象：身代金要求額と支払額の両方を共有した組織。回答者数 =507

前述のとおり、標的となった組織の売上高が高いほど、身代金要求額の中央値は通常高くなります。しかし、最終的な支払額をどの程度まで減額できるかは、売上規模の区分によって異なります。

中規模組織 (売上高 5,000 万ドルから 2 億 5,000 万ドル) は、代金要求額からの減額交渉で最も成果が低く、25% が要求額を上回る金額を支払っていました。最大規模の企業 (売上高 50 億ドル超) は、身代金額の減額交渉で最も高い成果を上げており、初回の要求額を上回る金額を支払った割合は 11% にとどまる一方、57% は要求額を下回る金額を支払っています。これは、すべての規模区分の中で最も高い割合です。

売上高 5 億ドルを超える組織では、身代金要求額を下回る金額での支払いに成功する割合が高くなっています。高額な身代金交渉では、攻撃者が大きな要求額を前提として一定の割引に応じる傾向があることを示しています。売上高 5,000 万ドル未満の組織でも、身代金支払額の削減において一定の成果を上げていました。

組織の売上別で見た身代金を支払った割合 (中央値)

売上	身代金を支払った割合 (中央値)
5,000 万ドル以下	95%
5,010 万ドル –2 億 5,000 万ドル	100%
2 億 5,010 万ドル –5 億ドル	100%
5 億 10 万ドル –10 億ドル	83%
11 億 ドル –50 億ドル	83%
50 億ドル以上	83%

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？調査対象：身代金要求額と支払額の両方を共有した組織。回答者数 =507

業界別の身代金の支払額

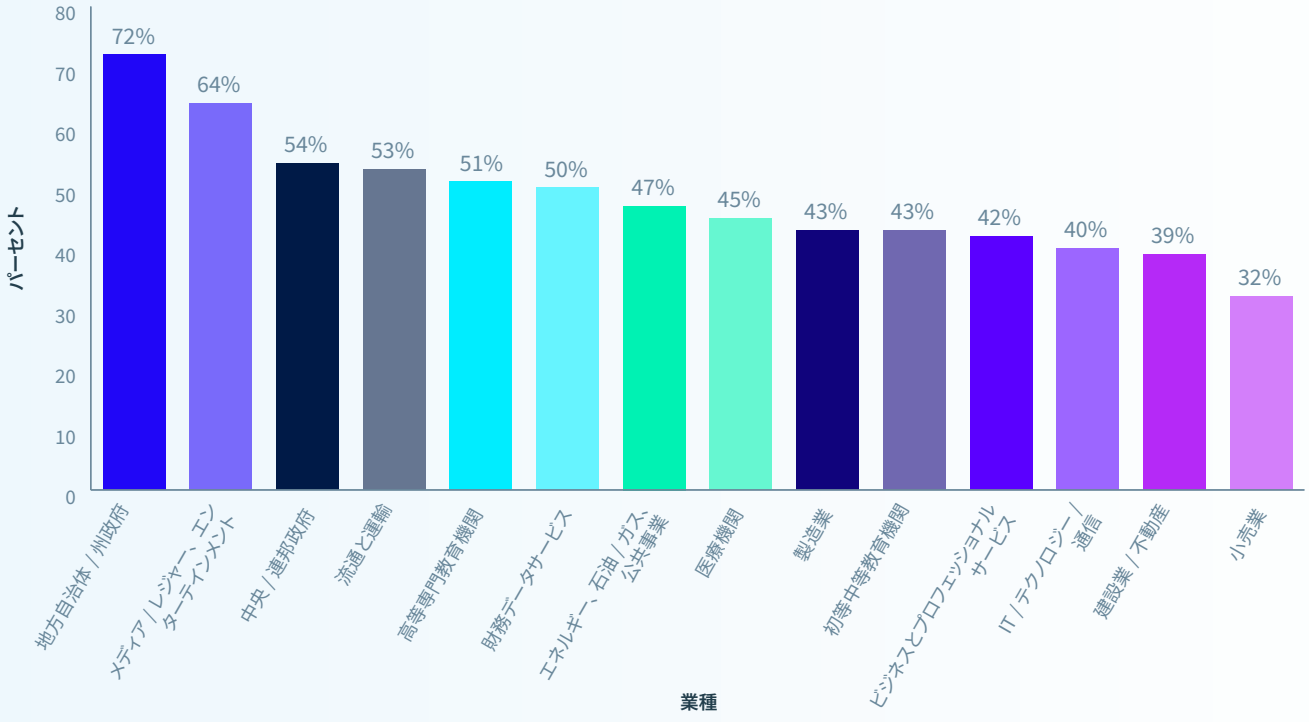
身代金を支払う傾向は業界によって異なります。**地方自治体 / 州政府 (72%) とメディア / レジャー / エンターテイメント (64%) は、身代金を支払う可能性が最も高く、**小売業 (32%) の 2 倍以上でした。

公共部門やメディア業界の組織は、市民向けサービスや時間的制約の大きいサービスを迅速に復旧させる必要に迫られることが多い一方、小売業では、一時的な混乱があっても事態の収束を待つという選択を取りやすい傾向があります。

小売業

は、ランサムウェア攻撃者に身代金を支払った割合が最も低い業界で、その割合は 32% でした。

業界別に見た身代金を支払った組織の割合



どのようにデータを復旧しましたか？身代金を支払った調査対象：データが暗号化された組織。回答者数 =1,214

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

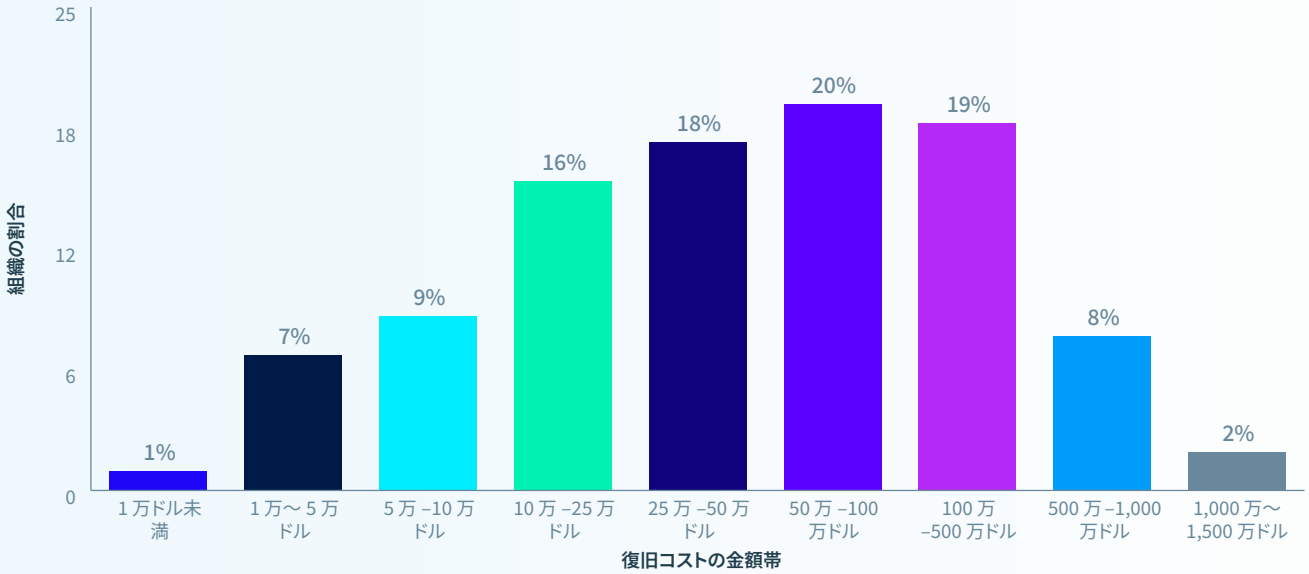
過去 1 年間で、身代金の支払いを除くランサムウェア攻撃からの復旧にかかった平均コストは 170 万 200 ドルでした。これは、2025 年版レポートの平均コスト 152 万 5,716 ドルから 11% 増加した一方で、2024 年版レポートで記録した最高額 273 万 684 ドルを依然として 38% 下回っています。復旧コストの中央値は 37 万 5,000 ドルで、前年のレポートから変化はありませんでした。

2024 年	2025 年	2026 年
273 万ドル	153 万ドル	170 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 =2,158 (2026 年)、3,400 (2025 年)、2,974 (2024 年)

復旧コストは幅広い金額帯に分布しており、20% の組織では 50 万～ 100 万ドル、19% の組織では 100 万～ 500 万ドルの費用が発生しました。

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を修復するために組織が負担した概算費用は？ 回答者数 =2,158

復旧にかかった時間

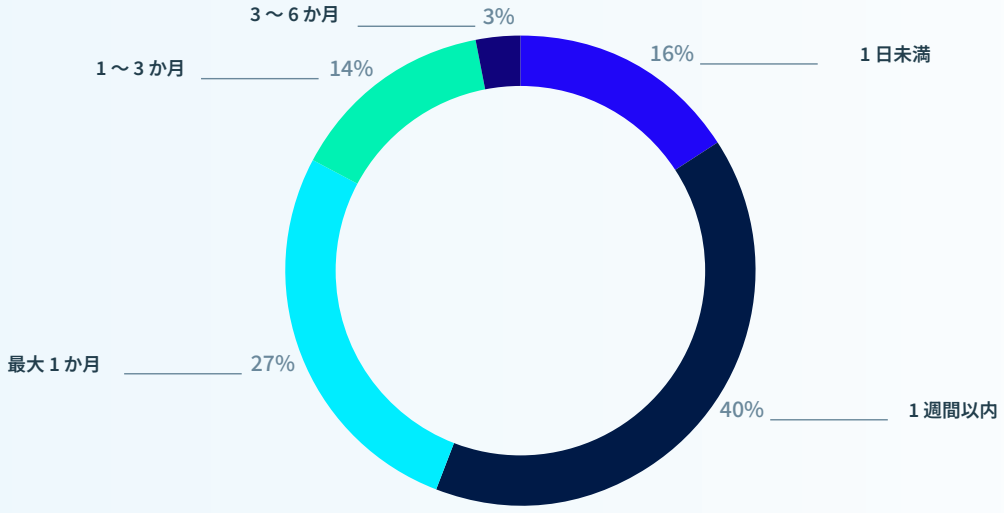
半数を超える組織 (55%) がランサムウェア攻撃から 1 週間以内に復旧しており、そのうち 16% は 1 日未満で復旧しました。また、83% の組織が 1 か月以内に復旧しています。復旧に 3 か月以上かかった企業はわずか 3% でした。

1 週間で復旧した割合は 55% となり前年比で 3% 増加しています。復旧に要した平均期間は 3 週間で、2025 年版レポートと同水準であり、2024 年版の 5 週間から改善した状態が続いています。

55%

ランサムウェア攻撃から 1 週間以内に復旧した組織の割合。

復旧に要した時間



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 =2,158

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ほぼすべての組織 (99%) が、IT チームとサイバーセキュリティチームに長期的な影響があることを報告しています。最も大きな影響として回答があったのは、今後の攻撃に対する不安やストレスの増加 (41%) と、シニアリーダーからの圧力の増加 (40%) でした。被害を受けた組織の 5 社に 1 社以上 (21%) が、攻撃の直接的な結果として経営幹部が交代されました。

シニアリーダーからの評価の向上は、前年比で増加した唯一の影響であり、31% から 36% に増加しています。調査対象となったその他の影響はいずれも減少しており、チームの優先事項の変更と継続的な業務量の増加はいずれも 7 パーセント低下し、チームの再編は 5 パーセント低下しました。

21%

ランサムウェア攻撃を受けて交代した IT/ サイバーセキュリティ部門のリーダーの割合。

ランサムウェアが IT/ サイバーセキュリティチームに与えた影響

影響	2026 年	2025 年からの変更
今後の攻撃に対する不安やストレスの増加	41%	-
シニアリーダーからのプレッシャーの増加	40%	-
シニアリーダーからの評価の向上	36%	5% 上昇
チームや組織構造の変更	32%	5% 下落
チームの優先事項や注力領域の変化	32%	6% 下落
攻撃を阻止できなかったことへの罪悪感	31%	3% 下落
継続的な業務量の増加	31%	7% 下落
ストレスやメンタルヘルス問題によるスタッフの欠勤	29%	2% 下落
チームリーダーの交代	21%	4% 下落

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？対象者：データが暗号化された組織。回答者数 =1,214 (2026 年)、回答者数 =1,700 (2025 年)

経営幹部による認識の高まりは、本レポートで示されたその他の前向きな運用面の傾向にも寄与している可能性があります。経営幹部の関心が高まることで、サイバーセキュリティプログラムに対するリソースの確保や組織的な支援が充実しやすくなるためです。

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する。ランサムウェア被害を受けた組織の 3 分の 2 は、そのランサムウェアインシデントが、自組織で発生した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回答しており、アイデンティティ侵害とランサムウェアが密接に関係していることを裏付けています。組織は、ITDR (アイデンティティ脅威の検知と対応) 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、人間と人間以外の両方のアイデンティティ認証情報を定期的に監査する必要があります。攻撃を受けた時点で 97% の組織が何らかの形で MFA を導入していたという調査結果が示すとおり、MFA だけでは攻撃を防ぐことはできません。また、MFA はすべての対象システムやアカウントに対して包括的に適用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する。最先端の AI は、脆弱性の発見や悪用を加速させています。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、中小企業から大企業まで共通する継続的な課題です。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プロフェッショナルに、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 ベンダーやマネージドサービスプロバイダー (MSP) などの外部のスペシャリストと連携し、不足している人材や専門性を補うことを検討してください。また、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。

メールセキュリティに優先的に取り組む。本レポートで示したように、フィッシングや悪意のあるメールがランサムウェア攻撃の根本原因の半数を占めています。そのため、組織は高度なメールフィルタリングを導入し、DMARC、DKIM、SPF プロトコルを実装するとともに、定期的なフィッシング対策トレーニングに投資することが重要です。メールを悪用した攻撃が増加していることを踏まえると、技術的な脆弱性へのパッチ適用だけでは不十分です。

バックアップと復旧インフラに投資する。堅牢なバックアップ体制を維持していた組織では、暗号化されたデータの復旧率が、過去最高に迫る水準となりました。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。

エクスポージャー管理プログラムを継続的に実施する。根本原因として脆弱性の悪用が占める割合は 14% 低下しており、前向きな結果と言えます。しかし、脆弱性を悪用する攻撃は依然として主要な攻撃経路の一つであり、最先端の AI モデルによって新たな脆弱性がより短期間で発見されるようになるにつれ、今後増加する可能性があります。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ジャを削減し、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。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 ソリューションと連携させ、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。

サイバーセキュリティチームをインシデント後も継続的に支援する。ランサムウェアの影響を受けたチームの 99% が何らかの余波を経験しており、ランサムウェアがもたらす人的な負担はほぼすべての組織に及んでいることが分かります。組織は、インシデント発生後の支援に関する明確な手順を整備し、経営幹部の関心の高まりを、テクノロジーだけでなく人材への継続的な投資にも確実につなげるべきです。

まとめ

「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。

防御側の組織には確かな進展が見られました。身代金の要求額と支払額はいずれも減少し、バックアップを利用した復旧は過去最高に近い水準まで増加しています。また、身代金を支払う場合でも、組織は交渉によってより良い結果を引き出せるようになっています。脆弱性の悪用を利用した攻撃が大幅に減少したことは、AI による脆弱性発見技術の進展や、パッチ管理への継続的な投資が成果を上げていることを示しています。

データから読み取れる最も前向きな兆候は、サイバーセキュリティチームに対する経営幹部の認識が高まっていることかもしれません。経営幹部の関心が高まれば、必要なリソースも確保されることになります。本レポートで見られた、バックアップ利用の向上や身代金交渉結果の改善などの前向きな傾向は、この好循環を反映している可能性があります。

一方で、依然として残る課題は重大です。ランサムウェア攻撃の半数以上では依然としてデータの暗号化に成功しており、1 件あたりの復旧コストは平均 170 万ドルに達しています。また、サイバーセキュリティチームへの人的な負担は、ほぼすべての組織で発生しています。

ランサムウェア被害を受けた組織の 3 分の 2 が、そのインシデントの発端をアイデンティティ侵害にまでたどったことは、**ランサムウェア対策においてアイデンティティセキュリティが極めて重要な役割を担っていることを示しています。**アイデンティティを後付けの対策ではなく、セキュリティの基盤として位置付けている組織は、攻撃を未然に防ぐ上でより有利な立場にあります。

組織はまた、**今後 10 年間のサイバーセキュリティにおける最大の課題にも備える必要があります。それは、AI によって高度化する脅威です。**その理由は、すでにデータからも示唆されています。被害を受けた組織の 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、58% 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。

ファイアウォールによって脅威を早期に検知することで攻撃への対応が改善していることや、バックアップを利用した復旧が大幅に増加したことなど、今年の調査結果全体に見られる傾向は、一貫した方向性を示しています。**それは、防御機能が個別に動作するのではなく、相互に連携することで、より良い成果が得られるということです。**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組織は、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。

調査方法

本調査は、2026 年第 1 四半期にソフォスの委託を受けて Vanson Bourne が実施しました。過去 12 か月間にランサムウェア攻撃を受けた 17 か国の組織の 2,158 人の IT およびサイバーセキュリティ意思決定者にインタビューが行われました。対象となった国は、米国、ブラジル、チリ、コロンビア、メキシコ、英国、フランス、ドイツ、イタリア、スペイン、スイス、オーストラリア、インド、日本、シンガポール、南アフリカ、およびアラブ首長国連邦です。回答者は、15 の業界にわたる従業員 100 ～ 5,000 人規模の組織から構成されています。

SOPHOS

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

2026-06-09 JA (DD)