SOPHOS

ランサムウェアの現状 2023 年版

14 か国の IT/サイバーセキュリティリーダー 3,000 人を対象に 2023 年 1 月から 3 月に独立した調査会社が実施した調査から得られた結果と考察。

はじめに

ソフォスは IT 部門やサイバーセキュリティ部門のリーダーに対して、ランサムウェアに関する状況を毎年調査しています。2023 年も調査を継続し、組織が直面している現状を明らかにしました。攻撃の一般的な根本原因を突き止め、組織におけるランサムウェアの体験がその売上高に応じてどのように異なっているのかを今回の調査で明らかにしました。本レポートでは、データを復元するためにバックアップではなく身代金を支払うことによって、企業と業務の運用にどのような影響が生じているのかも明らかにしています。

調査について

ソフォスは、北アメリカ、南アメリカ、EMEA およびアジア太平洋地域の 14 か国の組織 (従業員数 100～5,000 人) に所属する 3,000人の IT/サイバーセキュリティ部門のリーダーを対象とする調査を、独立した調査会社に依頼しました。調査は 2023 年 1 月から 3 月にかけて実施され、過去 1 年間の経験に基づいて回答してもらいました。

教育業界については、初等中等教育機関 (幼稚園、小学校、中学校、高校) と高等教育機関 (大学や専門学校) に分類して調査を行いました。

3,000
回答者数

14
か国

100 ～ 5,000 人
の従業員を擁する組織

2023 年 1 月～ 3 月
調査の実施期間

1,000 万ドル未満から 50 億ドル超まで
年間売上高

目次

ランサムウェア攻撃を受けた割合

今回の調査結果では、ランサムウェア攻撃を受ける割合は依然として横ばい傾向であり、過去 1 年間にランサムウェアに感染したと回答して組織は 66% となりました。これは、2022 年の調査と同じ数字でした。攻撃者は大規模な攻撃を絶えず実行しています。ランサムウェアは組織が現在直面している最大のリスクと言えるでしょう。

サイバー犯罪者は、数年前からサービスとしてランサムウェアを展開するビジネスモデルを開発し、発展させてきました。この運用モデルにより、ランサムウェア攻撃に参入するハードルが低くなった一方で、攻撃の各段階の専門化が進み、攻撃はさらに高度化しました。サービスとしてのランサムウェアの詳細については「ソフォス脅威レポート 2023 年版」」を参照してください。

2020	2021	2022	2023
51%	37%	66%	66%

過去 1 年間にランサムウェア攻撃を受けましたか？
はい。回答者数 = 3000 人 (2023 年)、5,600 人 (2022 年)、5,400 人 (2021 年)、5,000 人 (2020 年)

国別の攻撃数

報告されたランサムウェアの全体的な攻撃数は 2022 年の結果と比較して横ばいですが、国別に見ると変動しています。今年の調査でランサムウェア攻撃の発生率が最も高かったのはシンガポールであり、84% の組織が昨年被害を受けました。逆に、イギリスは攻撃を受けた割合が 44% と最も低くなりました。

攻撃を受けた割合が前年度比で最も低下したのはオーストリアであり、前回の調査の 84% から 50% に減少しました。攻撃を受けた割合が前年度比で最も増加したのは南アフリカで、2022 年の調査では 51% でしたが、2023年の調査では 78% に増加しました。

詳細については、20 ページの「国別のランサムウェア攻撃を受けた割合：2022 年と 2023 年の比較」を参照してください。

業界別の攻撃数

昨年、ランサムウェア攻撃を多く受けた業界は教育業界でした。初等中等教育機関の 80%、高等教育機関の 79% が攻撃を受けたことを報告しています。教育業界は他の業界と比べて、これまでもリソースが不足しており、技術的なスキルレベルも低いことが弱点となっていますが、今回のデータは攻撃者が教育業界のこの弱みを突いていることを裏付けています。

IT/テクノロジー/通信業界は、攻撃を受ける割合が最も低くなっており (50%)、サイバーセキュリティ対策と防御力のレベルが高いことを示しています。

詳細については、21 ページの「業界別のランサムウェア攻撃の割合」を参照してください。

66% の組織がランサムウェア攻撃を受けた

攻撃を受けた割合が最も高かった国は**シンガポール**

攻撃を受けた割合が最も低かった国は**英国**

攻撃を受けた割合が最も高かった業界は**教育業界**

攻撃を受けた割合が最も低かった業界は **IT/ テクノロジー / 通信**

組織の規模別の攻撃数 (従業員数と売上高)

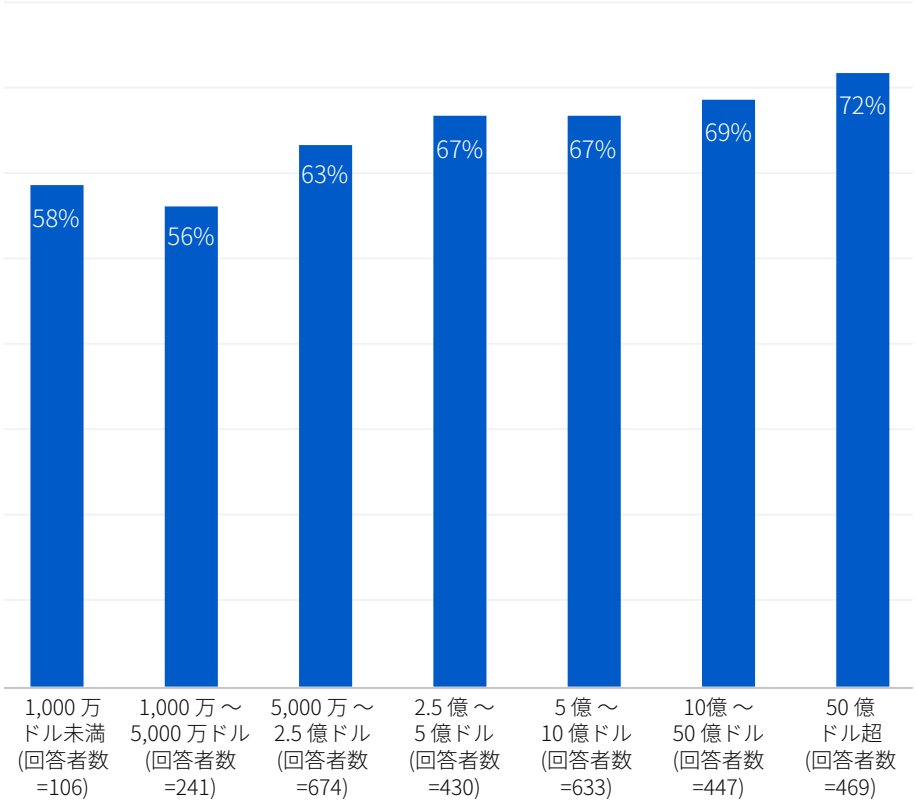
今回の調査で、年間売上高とランサムウェア攻撃を受ける割合には明らかな相関関係があることがわかりました。ランサムウェア攻撃を受ける割合は組織の売上高に比例して増加しています。昨年、売上高が 1,000 万ドルから 5,000 万ドルの組織の 56% がランサムウェア攻撃を受け、売上高が 50 億ドル以上の組織では攻撃を受ける割合が 72% に増加しました。

逆に、ランサムウェア攻撃を受ける割合と組織の従業員数には明確な関係性は見られませんでした。従業員が 1,001〜 3,000 人の組織以外では、ランサムウェア攻撃を受ける割合はほぼ同じでした。

- 従業員 100 〜 250 人　　62%
- 従業員 251 〜 500 人　　62%
- 従業員 501 〜 1,000 人　　62%
- 従業員 1,001 〜 3,000 人　　73%
- 従業員 3,001 〜 5,000 人　　63%

このデータから、攻撃を受ける可能性に影響する組織の規模に関する指標として、従業員数よりも年間売上高が有効な指標であると言えるでしょう。

ランサムウェア攻撃を受けた組織の割合 (売上高別)

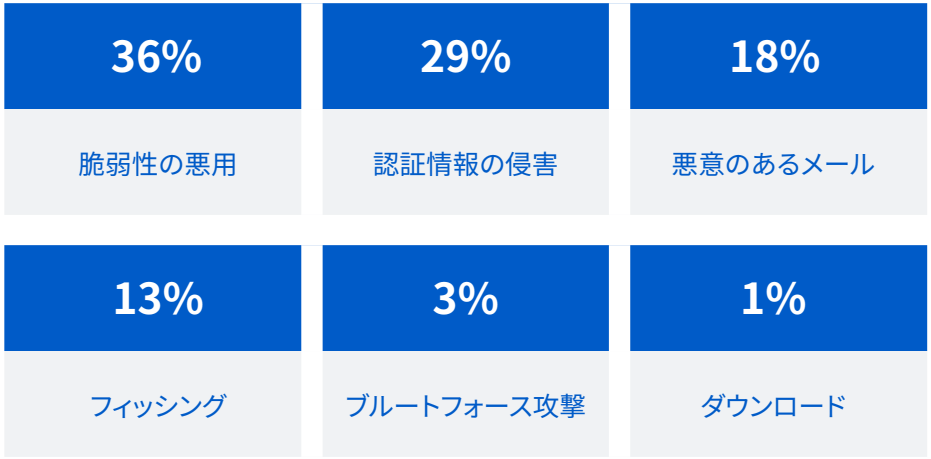


過去 1 年間にランサムウェア攻撃を受けましたか？はい。回答数はグラフ内

ランサムウェア攻撃の根本原因

調査の回答者は、ランサムウェア攻撃を受けた最も多い根本原因は脆弱性の悪用 (36%) であり、次に認証情報の侵害 (29%) であることを報告しています。これらの調査結果は、ソフォスが最新の 152 件の攻撃についてレトロスペクティブ分析を行った結果とほぼ一致しています。この分析では、インシデント対応チームと MDR チームが修復のために参加しましたが、攻撃の 37% が脆弱性を悪用しており、30% が侵害された認証情報を使用していました。

ランサムウェア攻撃の根本原因としてメールは 30% を占めています。18% のランサムウェア攻撃が悪意のあるメールを、13% がフィッシングを起点としていました。3% のランサムウェア攻撃がブルートフォース攻撃から始まっており、ダウンロードを起点とするランサムウェア攻撃はわずか 1% でした。



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？ランサムウェア攻撃を複数受けている場合には、最も深刻なランサムウェア攻撃について回答してください。(回答者数 = 過去 1 年間にランサムウェア攻撃を受けた 1,974 社の組織)

業界別の根本原因

メディア/レジャー/エンターテイメント業界は、「脆弱性の攻撃」を根本原因とするランサムウェア攻撃を受けた割合が最も高った (55%) ことが報告されています。これは、この業界では脆弱性の管理が適切に実施されておらず、セキュリティギャップが広がっていること示しています。「認証情報の侵害」を起点とする攻撃の割合が最も高かった (41%) のは中央政府と連邦政府でした。これは、中央政府と連邦政府で認証情報の窃取が多い、窃取された認証情報の悪用を防ぐ能力が低い、あるいは、これら 2 つの要因の組み合わせが原因である可能性があります。

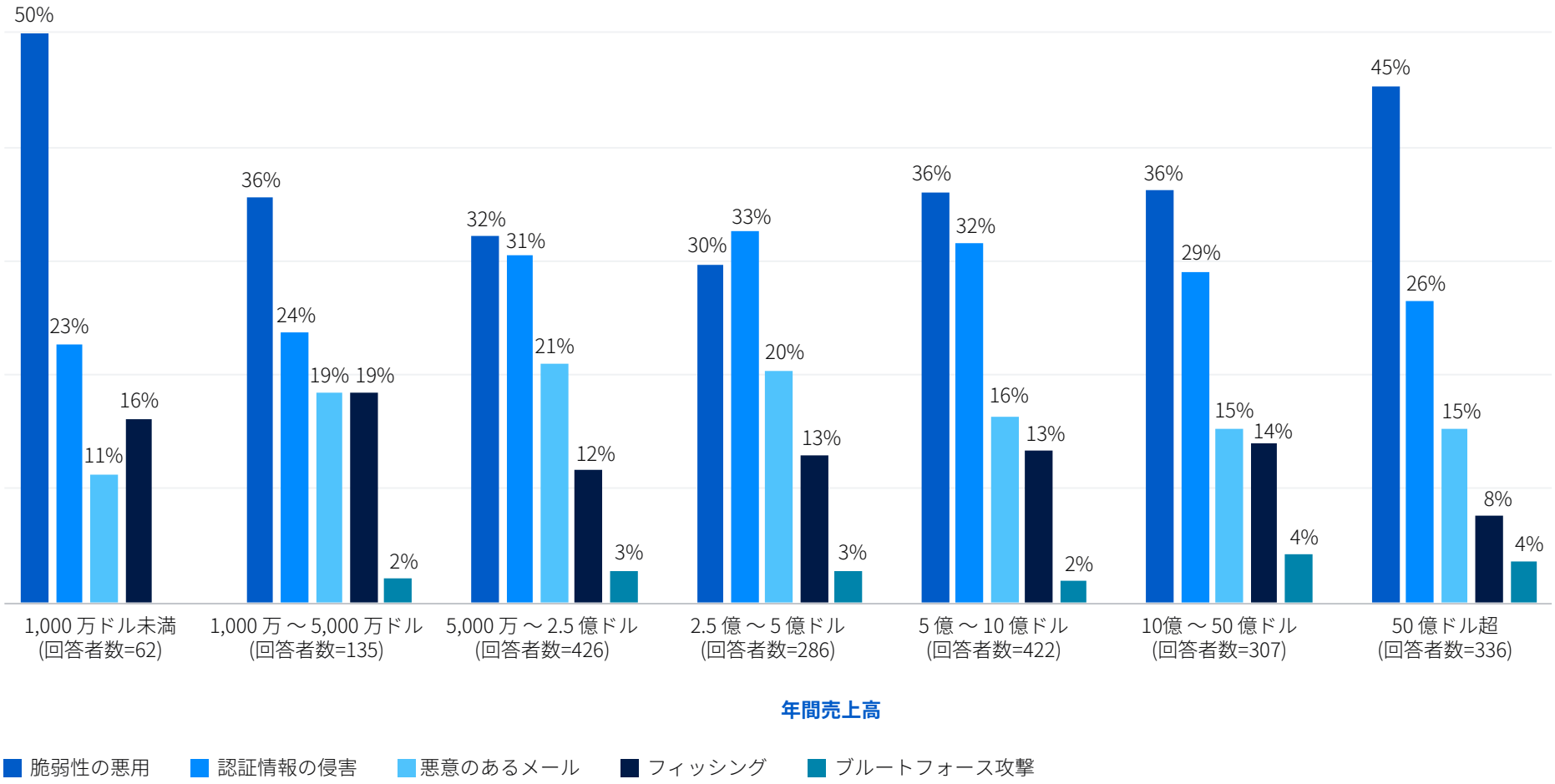
IT/テクノロジー/通信業界は、脆弱性の悪用 (22%) と認証情報の侵害 (22%) の両方を起点とするランサムウェア攻撃を受ける割合が最も低くなっています。これは、サイバーセキュリティの防御力が高いことを反映している可能性があります。しかし、この業界ではメールを起点とする攻撃の割合が最も高く、半数以上 (51%) が従業員の受信箱からランサムウェア攻撃が発生しています。

詳細については、22 ページの「業界別のランサムウェア攻撃の根本原因」を参照してください。

売上高別の根本原因

年間売上高別に根本原因を分析すると、脆弱性の悪用と認証情報の侵害がそれぞれ相反する傾向を示す曲線を描いていました。脆弱性を悪用した攻撃を受ける割合が最も高かったのは、売上高が最も低い組織 (1000 万ドル未満：50%) と最も高い組織 (50 億ドル以上：45%) であり、中間の組織 (2 億 5000万〜5 億ドル) では 30% に減少しています。

一方で、窃取された認証情報の使用については、売上高が中間の組織 (33%) が最も高く、売上高が最も低いおよび最も高い組織がそれぞれ 23% と 26% と低くなっています。

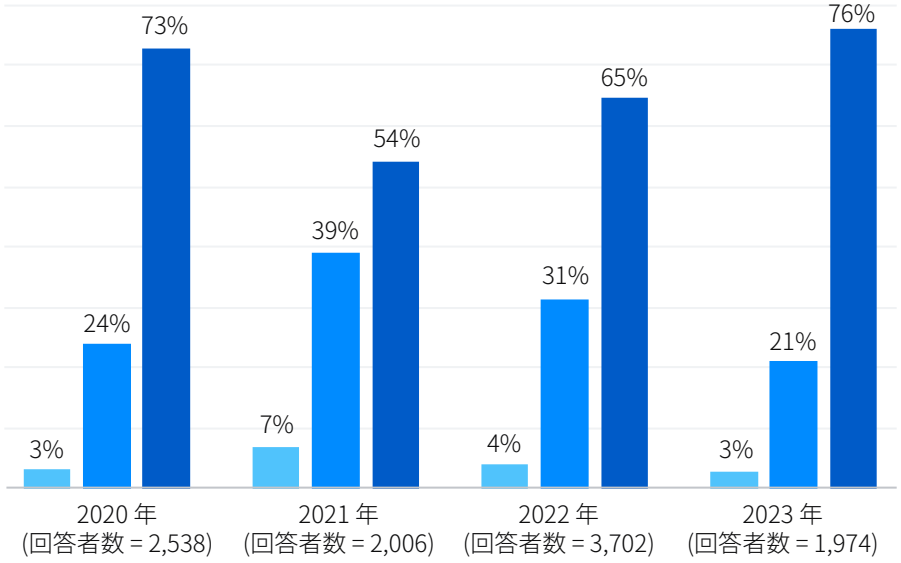


昨年受けたランサムウェア攻撃の根本原因を把握していますか？回答の選択肢を選択。回答数はグラフ内

データが暗号化される割合

データが暗号化される割合は引き続き増加しており、ランサムウェア攻撃の 4 分の 3 以上 (76%) で攻撃者はデータの暗号化に成功しています。実際、暗号化される割合は過去 4 年間で最高値に達しています。これは、攻撃者のスキルレベルが高まっており、新しいアプローチを取り入れて、攻撃を高度化していることを反映している可能性があります。

ランサムウェア攻撃でデータは暗号化されましたか？



- いいえ – データは暗号化されませんでしたが、それでも身代金を要求された (恐喝)
- いいえ – データが暗号化される前に攻撃を防止できた
- はい – データが暗号化された

業界別のデータの暗号化

ほぼすべての業界の組織が、データが暗号化される前に攻撃を防止するのに苦労しています。例外となった業界が 1 つありましたが、すべての業界でランサムウェア攻撃の 3 分の 2 以上でデータが暗号化されています。データが暗号化された割合が最も高い (92%) 業界は、ビジネス/プロフェッショナルサービスでした。

IT/テクノロジー/通信業界だけがこの傾向から外れており、データの暗号化に成功した割合は攻撃数の半分未満 (47%) となりました。これは、この業界のサイバーセキュリティの防御力と対策がレベルが高いことを示すもう 1 つの指標になっています。

詳細については、23 ページの「業界別のデータの暗号化」を参照してください。

情報窃取

データが暗号化された攻撃の 30% では、データも盗まれています。攻撃によってより多くの金銭を得るために、暗号化とデータ窃取によって「二重に稼ぐ」手法が増加しています。窃取されたデータは、公開するという恐喝に使用され、データは第三者に販売される恐れもあります。情報が窃盗されることが多くなっており、情報が外部に送信される前に迅速に攻撃を阻止することの重要性が高まっています。

30%

ランサムウェアによってデータが暗号化された攻撃の 30% では、データも窃取されている

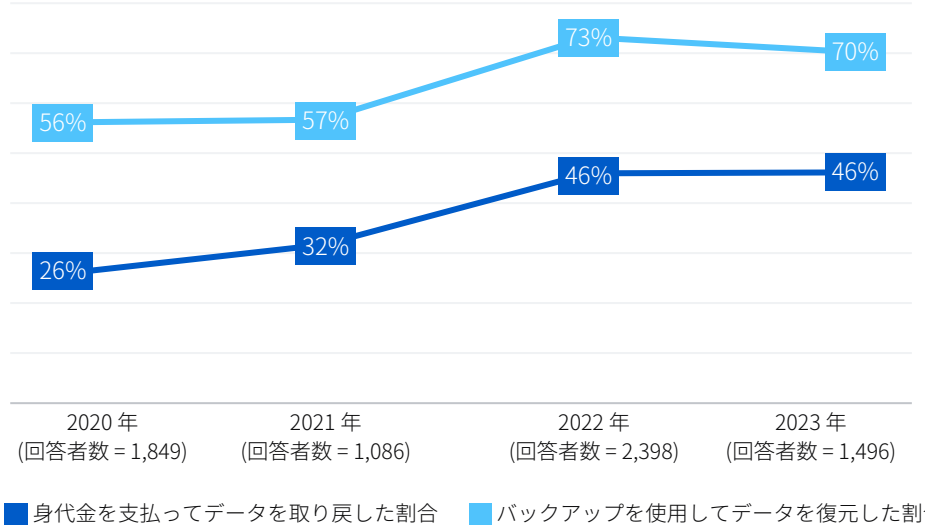
ランサムウェア攻撃でデータは暗号化されましたか？
はい。データも盗まれました。 回答者数 = 1,496

データの復元

データが暗号化された組織の 97% がデータを取り戻しています。データを復元するための方法としては、バックアップが最も一般的であり、インシデントの 70% で利用されました。46% が身代金を支払ってデータを取り戻し、2% が他の手段を使用して復元しています。全体として、5 社に 1 社 (21%) がデータを復元するために複数の方法を使用していました。データが暗号化された組織の 1% は身代金を支払ったものの、データを取り戻すことはできませんでした。

バックアップを使用してデータを復元した割合	身代金を支払ってデータを取り戻した割合	他の手段でデータを取り戻した割合
70%	46%	2%

気になるのは、昨年データを復元するためにバックアップが使用された割合は 73% でしたが、今年はこの割合が低下したことです。身代金の支払い率は昨年と同じ水準で推移しています。



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。回答数はグラフ内

国別のデータの復元

全体として、EMEA の回答者は、バックアップを使用する割合が総じて高く (75%)、身代金を支払う割合が総じて低く (40%) なっています (北アメリカと南アメリカの組織ではこれらの割合はそれぞれ 65% と 55% であり、アジア太平洋地域の組織では 67% と 49%)。国別に見ると、バックアップを使用する割合が最も高いのはフランス (87%) で、次いでスイス (84%) になっています。

バックアップによってデータを復元できた割合が低かったイタリア (55%) とシンガポール (57%) は、全体的なデータ復元率が最も低い国 (それぞれ 93% と 90%) にもなっており、バックアップの重要性が浮き彫りになりました。また、身代金を支払う傾向が最も高かったのはイタリア (56%) であり、米国とブラジル (55%) が続いています。

ほとんどのケースで、身代金を支払った組織はデータを復元できましたが、フランスとイギリスでは、身代金を支払った組織の約 10 社に 1 社がデータを復元できませんでした。

詳細については、24 ページの「国別のデータの暗号化」を参照してください。

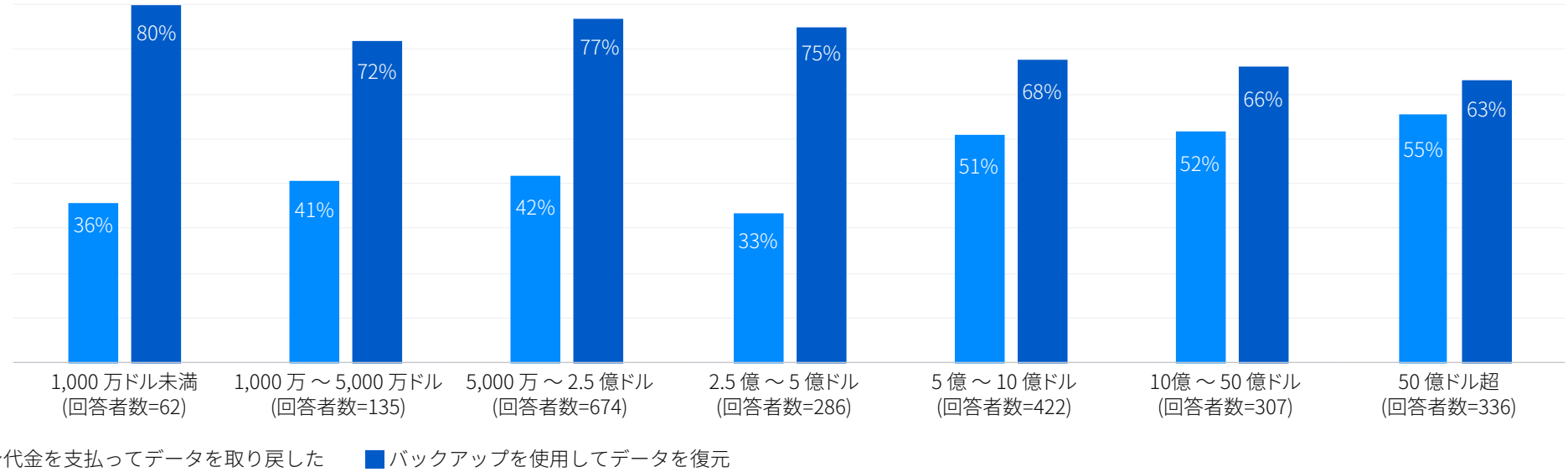
売上高別の身代金支払いとバックアップ使用

一般的に、年間売上高が増加するにつれて、身代金を支払ってデータを復元する割合も増加します。同時に、バックアップを使用する割合は低下します。

売上高が 50 億ドル以上の組織の 55% が、身代金を支払ってデータを取り戻し、63% がバックアップを使用していました。同時に、売上高が 1000 万ドル未満の組織の 36% が身代金を支払ってデータを取り戻し、80% がバックアップを使用してデータを復元していました。これは、バックアップを使用する割合が最も高い売上高グループになっています。

年間売上高が低い組織では、身代金を支払うだけの資金力に乏しく、データを復元するためにバックアップに注力しなければならない状況にあります。一方で、売上高の大きい組織の IT インフラは複雑であることが多く、バックアップを使用してデータを迅速に復元することが困難である場合があります。資金力が豊富であることから、金銭で (身代金を支払って) 問題を解決できる場合も多くあります。

売上高別の身代金支払いとバックアップの利用率



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。回答数はグラフ内

データ復元に対するサイバー保険の影響

サイバー保険に加入している組織は、加入していない組織と比較して、暗号化されたデータを復元できる可能性が非常に高くなっています。しかし、サイバー保険契約の種別では大きな差異は見られません。スタンドアロン型のサイバー保険を契約している組織では 98% が、パッケージ型のサイバー保険に加入している組織では 97% がデータを取り戻しています。一方、サイバー保険に加入していない組織で、暗号化されたデータを取り戻したのは 84% でした。

ランサムウェア攻撃を受けて暗号化されたデータを取り戻した組織の割合

98%	97%	84%
スタンドアロン型のサイバー保険に加入	サイバー攻撃への補償が含まれるパッケージ型の保険に加入	サイバー保険への加入なし

データを取り戻すことができましたか？ 回答者数 = 1,496 社 (昨年ランサムウェア攻撃を受けてデータが暗号化された組織)

この差異がある理由にはいくつかの要因が考えられます。最初の理由として考えられるのは、サイバー保険に加入するためには、通常、バックアップとリカバリ計画を作成する必要があります。保険会社は、ランサムウェア攻撃を受けた組織が被害を復旧するためのプロセスを提供して、被害を軽減することもできます。さらに、サイバー保険に加入している組織は、保険に加入していない組織よりも、データを取り戻すために身代金を支払う確率が高くなっています。

保険への加入が身代金の支払い傾向に与える影響

スタンドアロン型のサイバー保険	サイバー攻撃への補償が含まれるパッケージ型の保険	サイバー保険に未加入
58%	**36%**	**15%**
身代金を支払った組織の割合	身代金を支払った組織の割合	身代金を支払った組織の割合

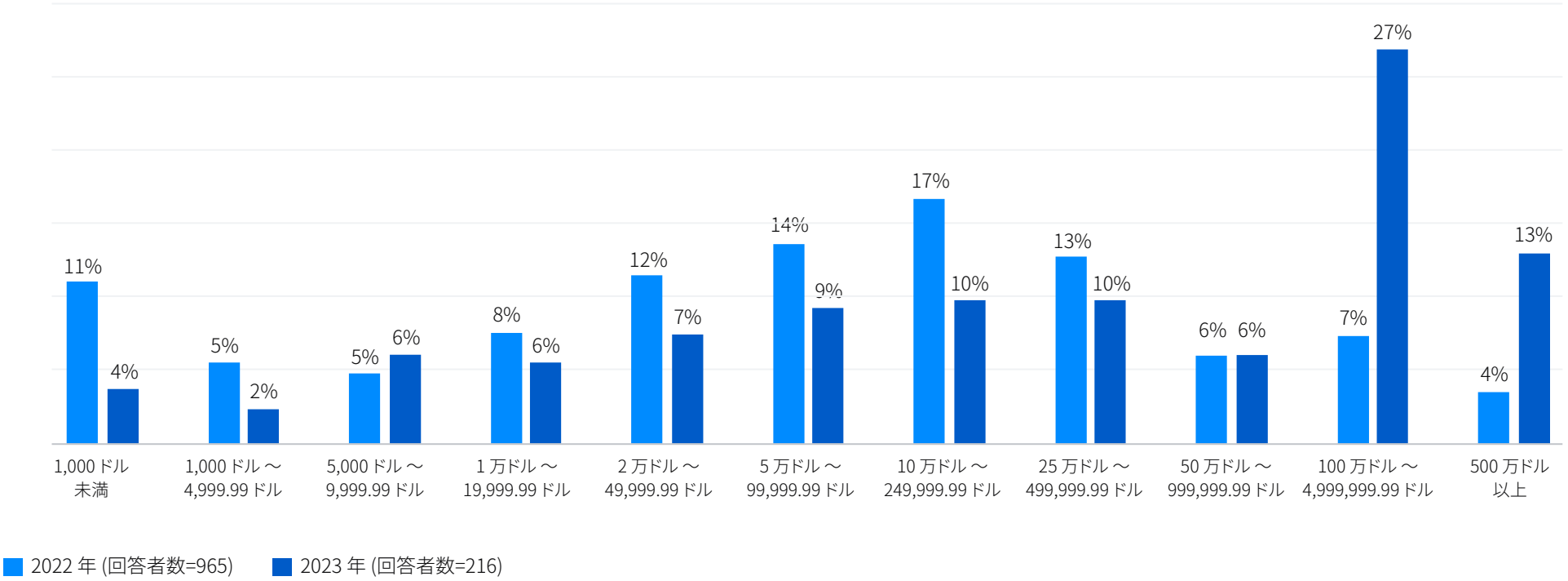
データを取り戻すことができましたか？はい、身代金を支払ってデータを取り戻した 回答者 = 過去 1 年間にランサムウェア攻撃を受けてデータが暗号化された 1,496 の組織 (771 社がスタンドアロン型の保険に加入、658 社がパッケージ型の保険に加入、67 社は保険に加入していない)

身代金の支払い

身代金を支払う傾向は昨年の調査と同じ水準になっていますが、支払われた身代金は昨年と比較して大幅に増加しており、身代金の平均支払額は 2022 年の 812,380 ドルから 2023 年には 1,542,333 ドルとなり、ほぼ倍増しました。今年の調査で報告された身代金の中央値は 40 万ドルでした。

今回の調査では、支払額は広く分布していますが、2022 年の調査と比較すると、より高額な身代金を支払った組織の割合は増加しており、100 万ドル以上を支払った組織は昨年の 11% から 40% に増加しました。逆に、10 万ドル未満の身代金を支払った組織は昨年の 54% から減少し、34% になりました。

身代金の支払い：2023 年と 2022 年



攻撃者に支払った身代金はいくらでしたか？「わからない」は除外。

売上高別の身代金支払い

当然ながら、売上高が最も多い組織は、支払う身代金を最も高額になっており、攻撃者が組織の支払い能力に基づいて身代金の金額を調整していることがわかります。この調査では、組織が直接身代金を支払った場合と、保険会社から支払った場合を区別していません。

興味深いことに、売上高が 2 億 5000 万ドルから 5 億ドルの組織と売上高が 5 億ドルから 10 億ドルの組織では、支払った身代金の平均値と中央値の両方にほとんど差異がありませんでした。

	5,000 万 ～ 2.5 億ドル (回答者数 =37)	2.5 億 ～ 5 億ドル (回答者数 =33)	5 億 ～ 10 億ドル (回答者数 =72)	10 億 ～ 50 億ドル (回答者数 =45)	50 億ドル超 (回答者数 =21)
身代金の支払いの平均値	$690,996	$1,523,652	$1,466,240	$2,049,817	$2,464,339
身代金の支払いの中央値	$145,000	$428,000	$425,000	$1,000,000	$3,000,000

攻撃者に支払った身代金はいくらでしたか？「わからない」は除外。母数が非常に少ないため、年間売上高が 5,000 万ドル未満の組織は除外。回答数はグラフ内。回答数が 30 未満のセグメントのデータは、参考として扱ってください。

復旧のコスト

ランサムウェア攻撃を受けた場合、身代金の支払いは影響を復旧するためのコストの 1 つにすぎません。ランサムウェア攻撃から復旧するためのコストは、支払った身代金を除いて、平均で 182 万ドルになりました。これは 2022 年の 140 万ドルから増加しており、2021 年に報告された 185 万ドルに匹敵しています。

注： 2021 年と 2022 年の調査の質問には、推定される復旧費用に支払った身代金が含まれていましたが、2023 年の調査の質問からは削除されています。そのため、前年比の数値は参考として扱ってください。

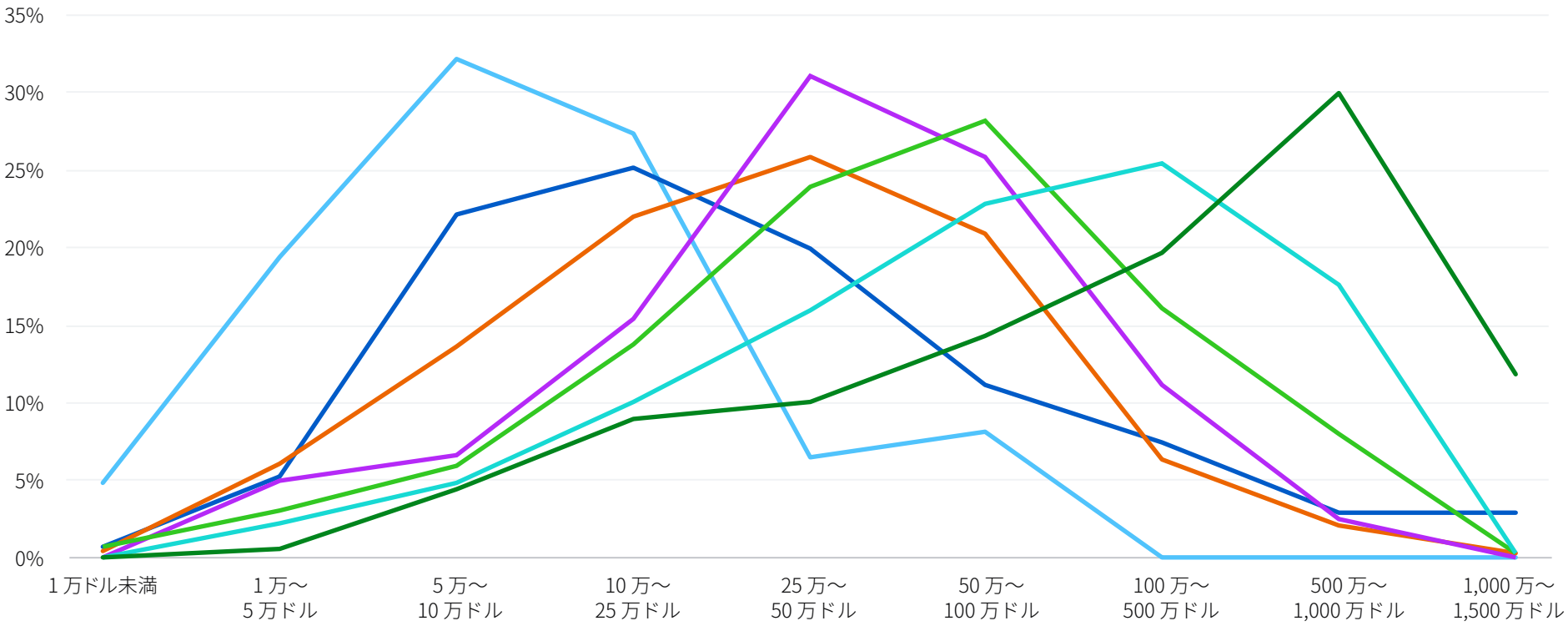
復旧にかかる平均コスト

最も深刻なランサムウェア攻撃の影響を復旧するため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) はどれぐらいですか？回答者数 = 1,974 社 (2023 年) / 3,702 社 (2022 年) / 2,006 社 (2021 年)。

注記：2022 年および 2021 年の質問には、復旧コストに「支払った身代金」も含まれていました。

復旧にかかったコストの平均値は、年間売上高が 1,000 万ドル未満の組織の 165,520 ドルから始まり、50 億ドル以上の組織では 4,496,086 ドルにまで上昇しています。これらの数値からは復旧コストの範囲はわかりませんが、次ページの図に示すように、売上高に比例して復旧コストが増加する明確なパターンが見られます。

売上高別の復旧コスト



最も深刻なランサムウェア攻撃の影響を復旧するため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) はどれぐらいですか？」回答数はグラフ内

データ復元方法別の復旧コスト

どのような切り口でデータを見ても、ランサムウェア攻撃による影響を復旧するためにバックアップを使用する方が、身代金を支払うよりもはるかに安くなります。バックアップを使用した組織の復旧コストの中央値 (375,000 ドル) は、身代金を支払った組織のコスト (750,000 ドル) の半分になっています。同様に、バックアップを使用した場合の復旧コストの平均値も、約 100 万ドル低くなっています。バックアップの強化戦略に投資する財務上の利点について確固たる証拠が必要な場合は、このデータを役立ててください。

身代金を支払って データを取り戻した	バックアップを使用して データを復元した
750,000 ドル 中央値	**375,000 ドル** 中央値
260 万ドル 平均値	**162 万ドル** 平均値

最も深刻なランサムウェア攻撃の影響を復旧するため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) はどれぐらいですか？回答者数 = 身代金を支払ってデータを取り戻した 694 社の組織とバックアップを使用してデータを復元した 1,053 社の組織。

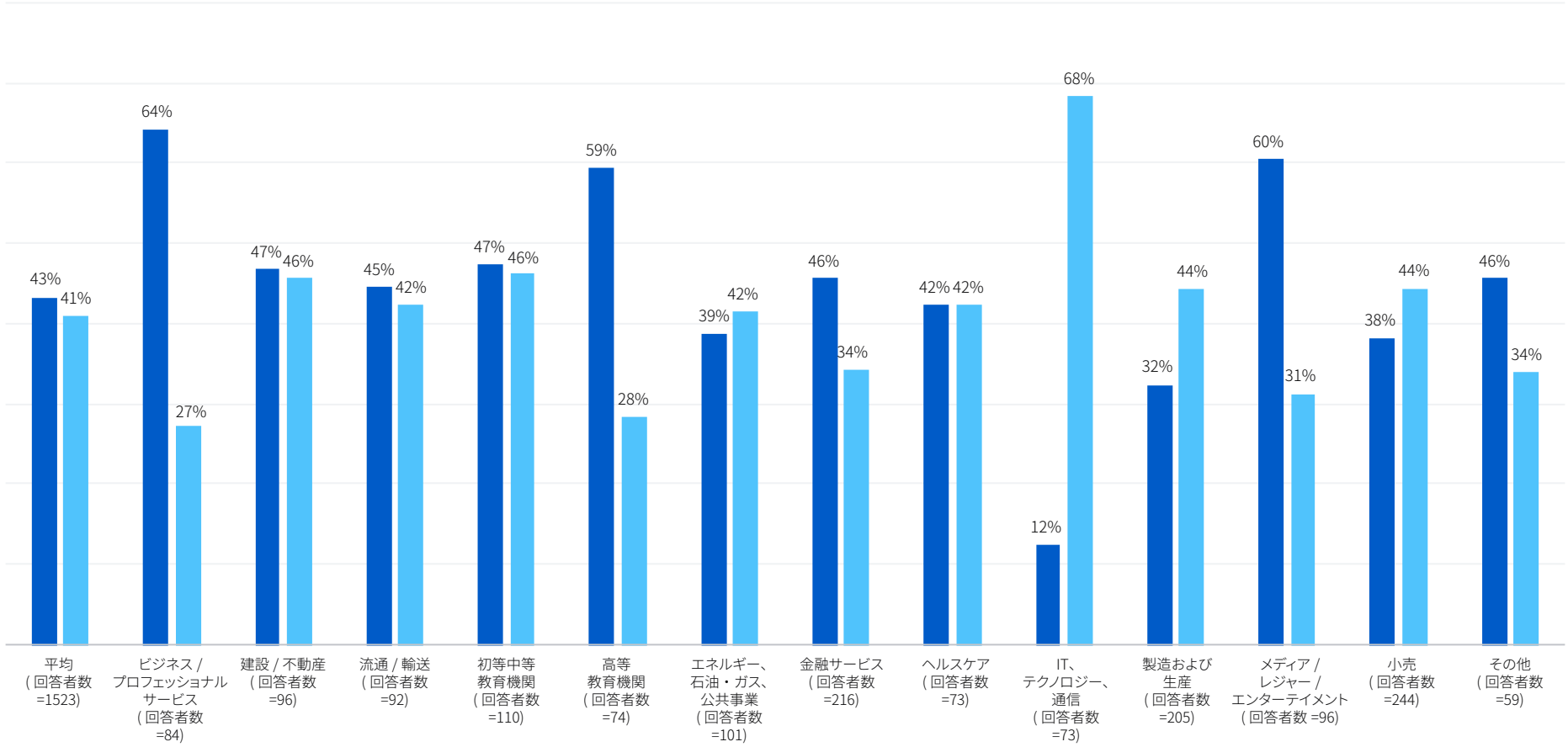
ビジネスへの影響

ランサムウェアの被害を受けた民間セクターの組織の 84% が、事業の損失や減収を招いたと回答しています。年間売上高がそれぞれ異なる組織では、事業の損失に与える影響に比較的差異はなく、2 億 5000 万ドルから 5 億ドルの組織は最も低く (79%)、1000 万ドル未満の組織と 50 億ドル以上の組織が最も高く (88%) なっています。

業種別で見ると、事業の損失と減収があったと回答した割合により顕著な傾向が見られます。全体として、初等中等教育機関 (94%) と建設/不動産業界 (93%) は、ランサムウェア攻撃による事業の損失や減収について最も多く報告しており、製造・生産業界の組織は最も低くなっています (77%)。

さらに詳細に見ていくと、事業の「大きな」損失と減収があったことを報告している業界には大きな違いがあり、ビジネスおよびプロフェッショナルサービス業界は 64% となり、IT/テクノロジー/通信業界 (12%) の 5 倍以上になっています。

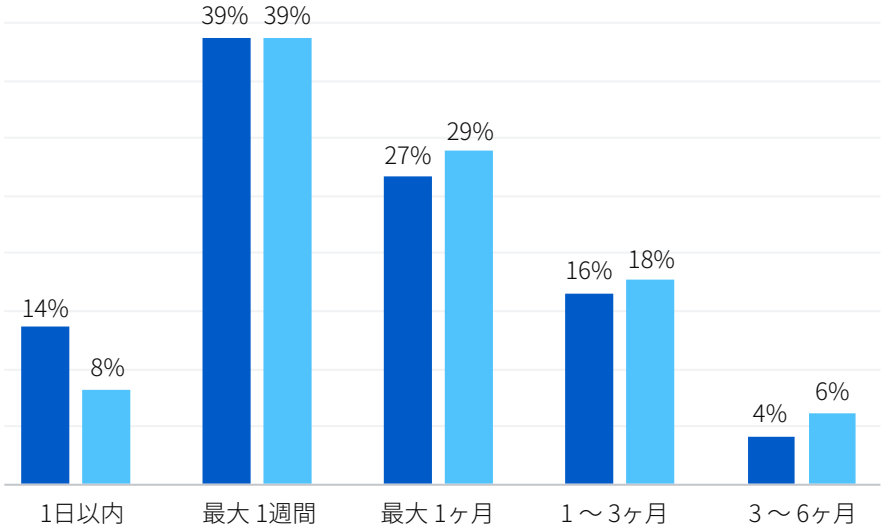
業界別の事業の損失 / 減収



ランサムウェア攻撃により、事業の損失 / 減収を招きましたか？はい、多くの事業の損失 / 減収があった
はい、多少の事業の損失 / 減収があったランサムウェア攻撃を受けた民間セクターの組織 (表中に回答数を表示)

復旧にかかる時間

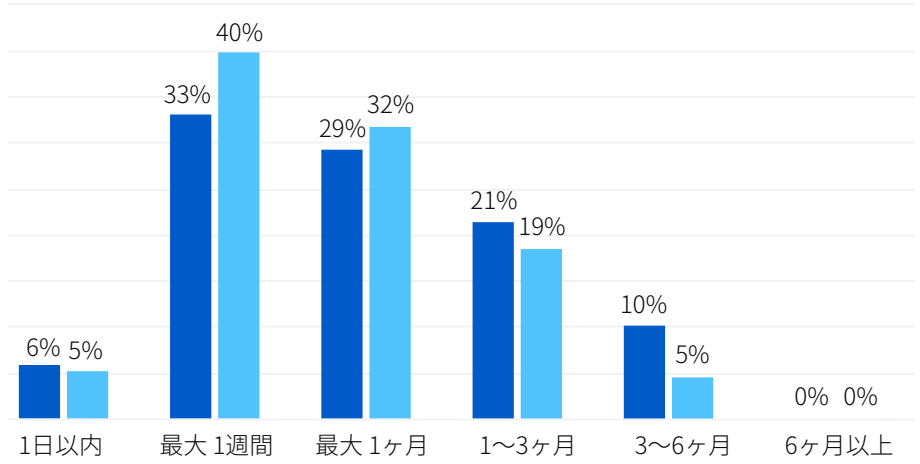
ランサムウェア攻撃から復旧するまでの時間は 2022 年のレポートとほぼ一致していますが、1 日以内に復旧できた組織の割合は 14% から 8% に低下しています。



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

データ復元方法別の復旧時間

調査によって、バックアップを使用してデータを復元している組織は、身代金を支払った組織よりも攻撃で受けた影響を迅速に復旧していることが明らかになりました。1 週間以内に復旧したのは、バックアップを使用している組織では 45% であり、身代金を支払った組織では 39% でした。復旧するまでに 1 か月以上かかった組織は、身代金を支払った組織は約 3 分の 1 (32%) ですが、バックアップを使用した組織では 23% (四捨五入) でした。これら 2 つの回答の選択肢は相互排他的ではなく、一部の回答者は身代金を支払い、さらにバックアップを使用していますが、バックアップを使用することが復旧する上で利点があることはデータからも明らかです。



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？
身代金を支払った、またはバックアップを使用してデータを復元した、あるいはその両方を使用した組織。回答数はグラフ内

まとめ

ランサムウェアは、売上高、地域、業界に関係なく、あらゆる組織にとって大きな脅威です。攻撃者が攻撃の戦術、手法、手順 (TTP) を進化させており、防御側の組織は対応することが困難になっています。その結果として、攻撃を受けてデータが暗号化される割合が高まっています。

暗号化されたデータを復元するためにバックアップが使用される割合が減少していることは、深刻な懸念材料です。バックアップの強化戦略に投資することが財務上および運用上の利点をもたらすことについて確固たる裏付けが必要でしたら、このレポートのデータを役立ててください。

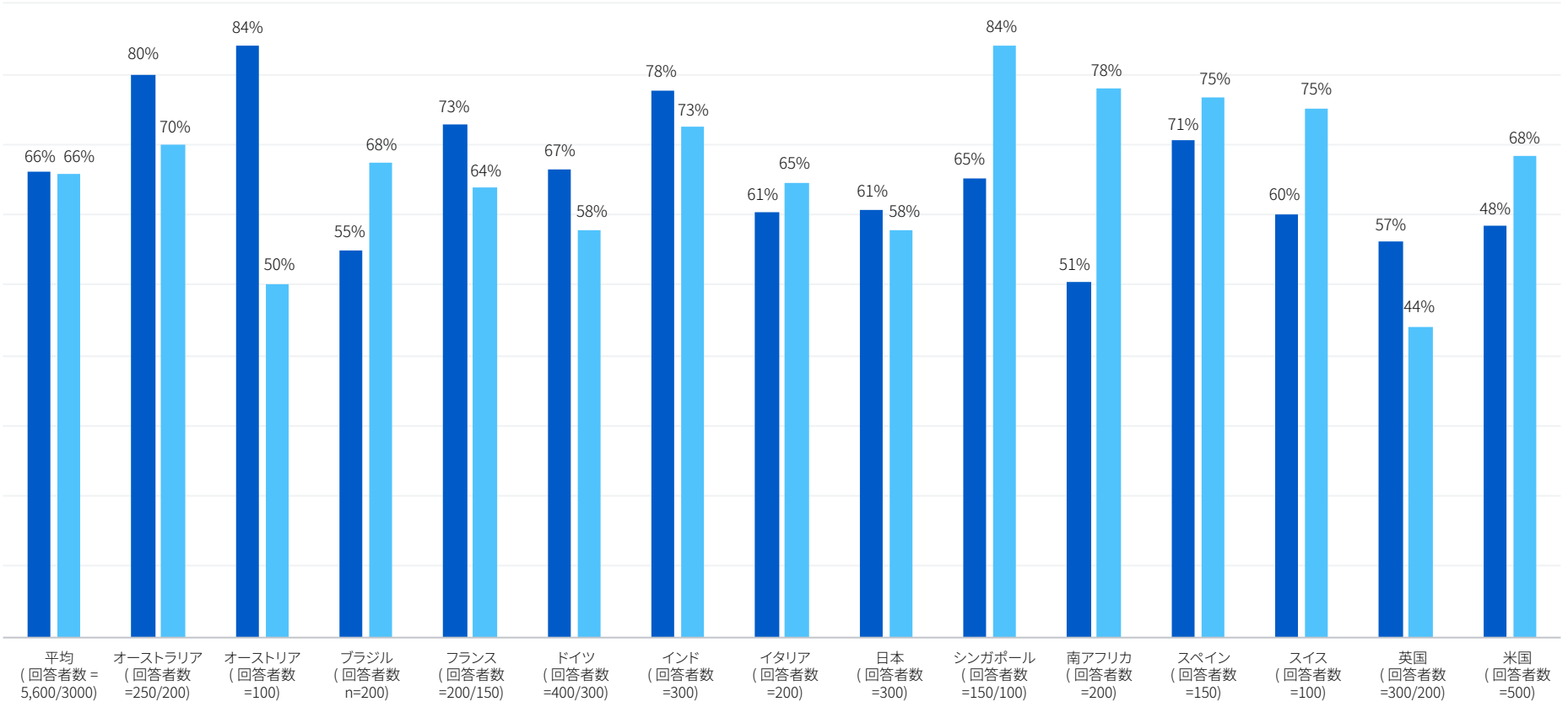
RaaS （Ransomware as a Service） のビジネスモデルが成長しているため、来年は攻撃が減少することは予測されていません。対策すべき重点ポイント：

- 以下のように、ランサムウェアへの対策をさらに強化してください。
  - 脆弱性の悪用を防ぐ強力なエクスプロイト対策機能を備えたエンドポイント保護、侵害された認証情報の悪用を阻止する ZTNA (Zero Trust Network Access) など、最も一般的な攻撃方法に対応して組織を防御するセキュリティツールを導入します。
  - 攻撃に自動的に対応し、攻撃者を妨害し、防御側が対応する時間を稼ぐことを可能にする適応型テクノロジーを導入します。
  - 24 時間年中無休で脅威を検出、調査、対応します。社内で実施することも、専門の MDR (Managed Detection and Response) サービスプロバイダーに依頼して連携して実施することも可能です。
- 定期的なバックアップの作成、バックアップからデータを復元する訓練、最新のインシデント対応計画の維持など、攻撃への備えを最適化します。
- タイムリーなパッチ適用やセキュリティツールの構成の定期的なレビューなど、適切なセキュリティ予防策の維持します。

その他の図表

国別のランサムウェア攻撃を受けた割合 2022 年と 2023 年

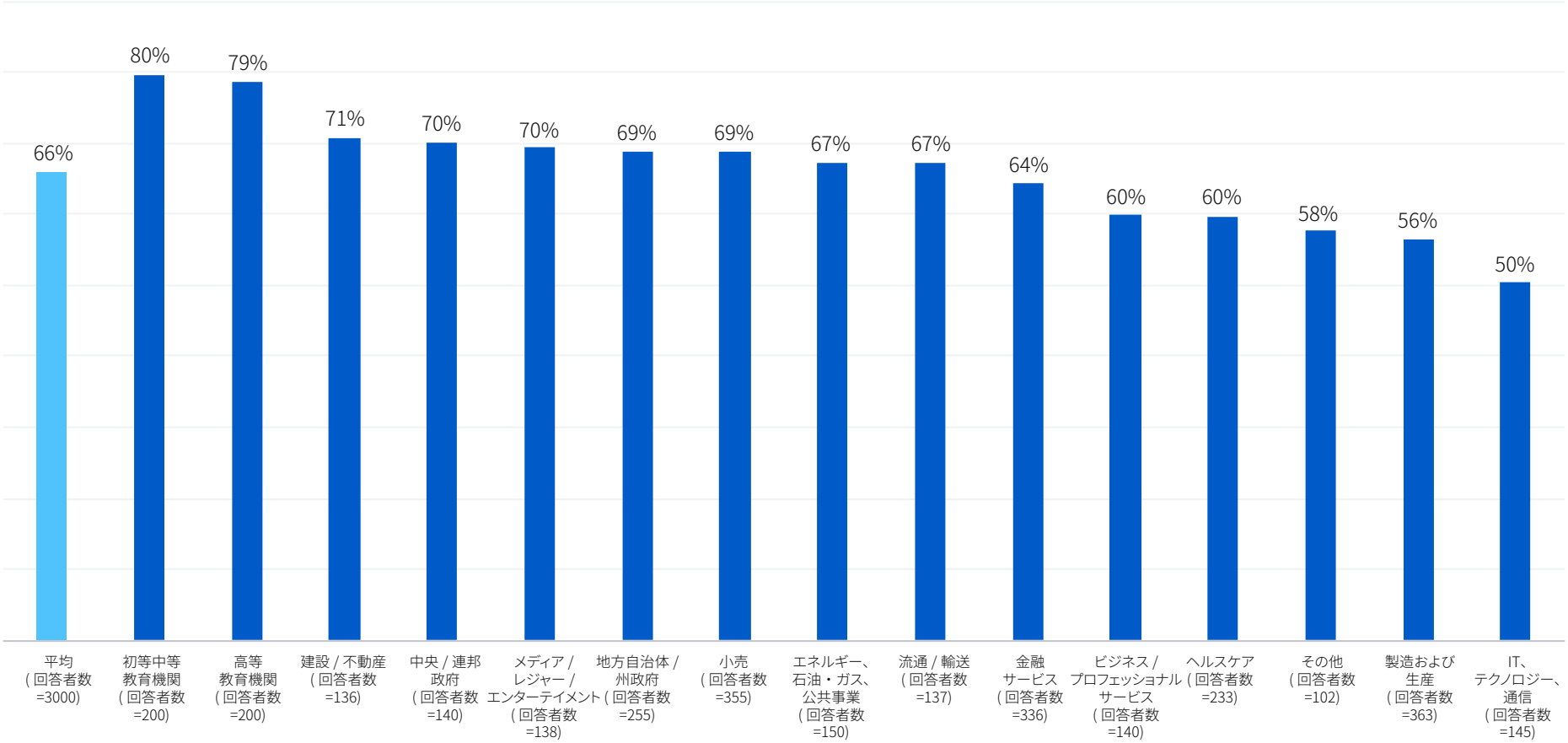
ランサムウェア攻撃を受けた組織の割合



過去 1 年間にランサムウェア攻撃を受けましたか？回答数はグラフ内

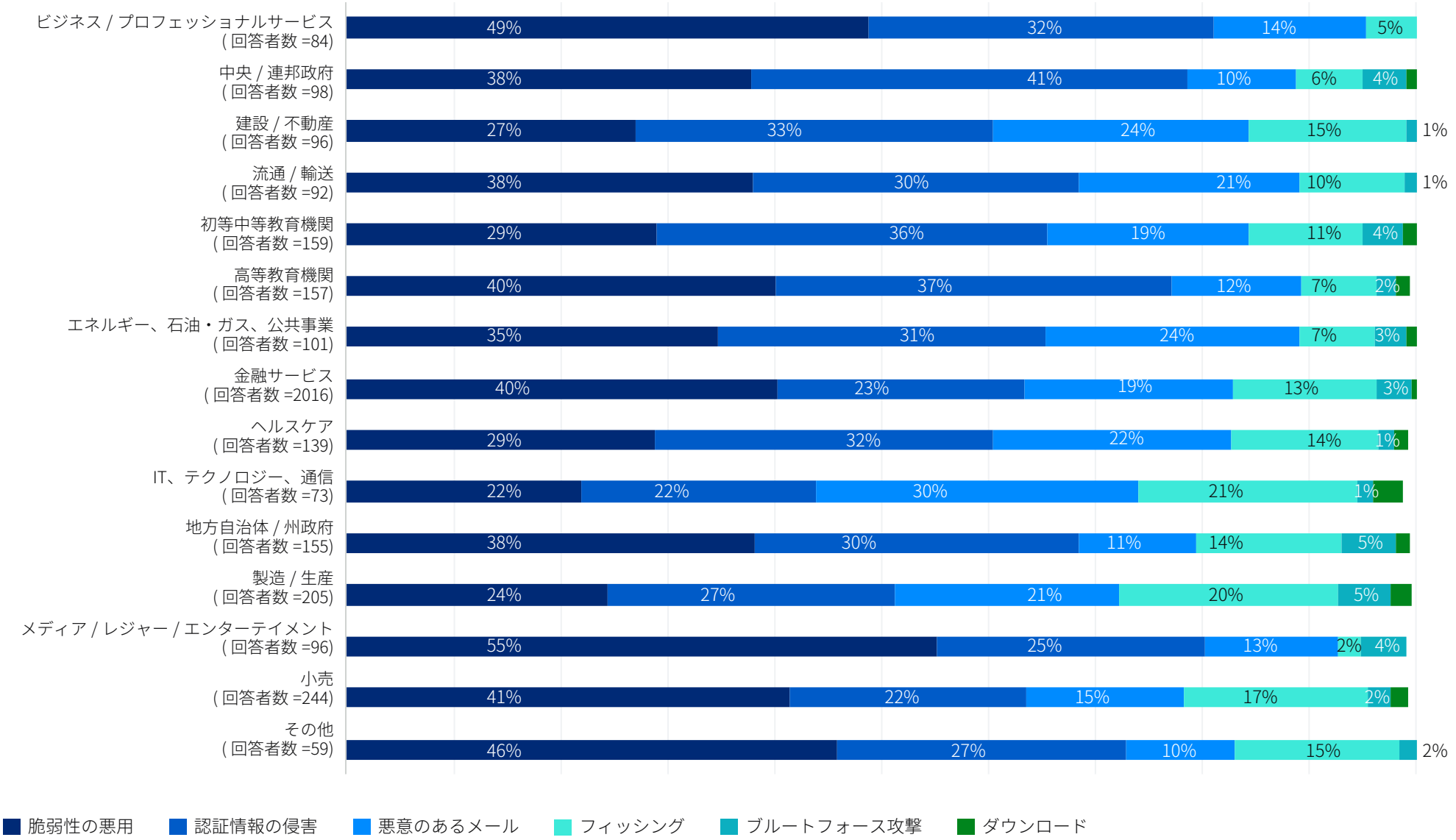
業界別のランサムウェア攻撃を受けた割合

ランサムウェア攻撃を受けた組織の割合



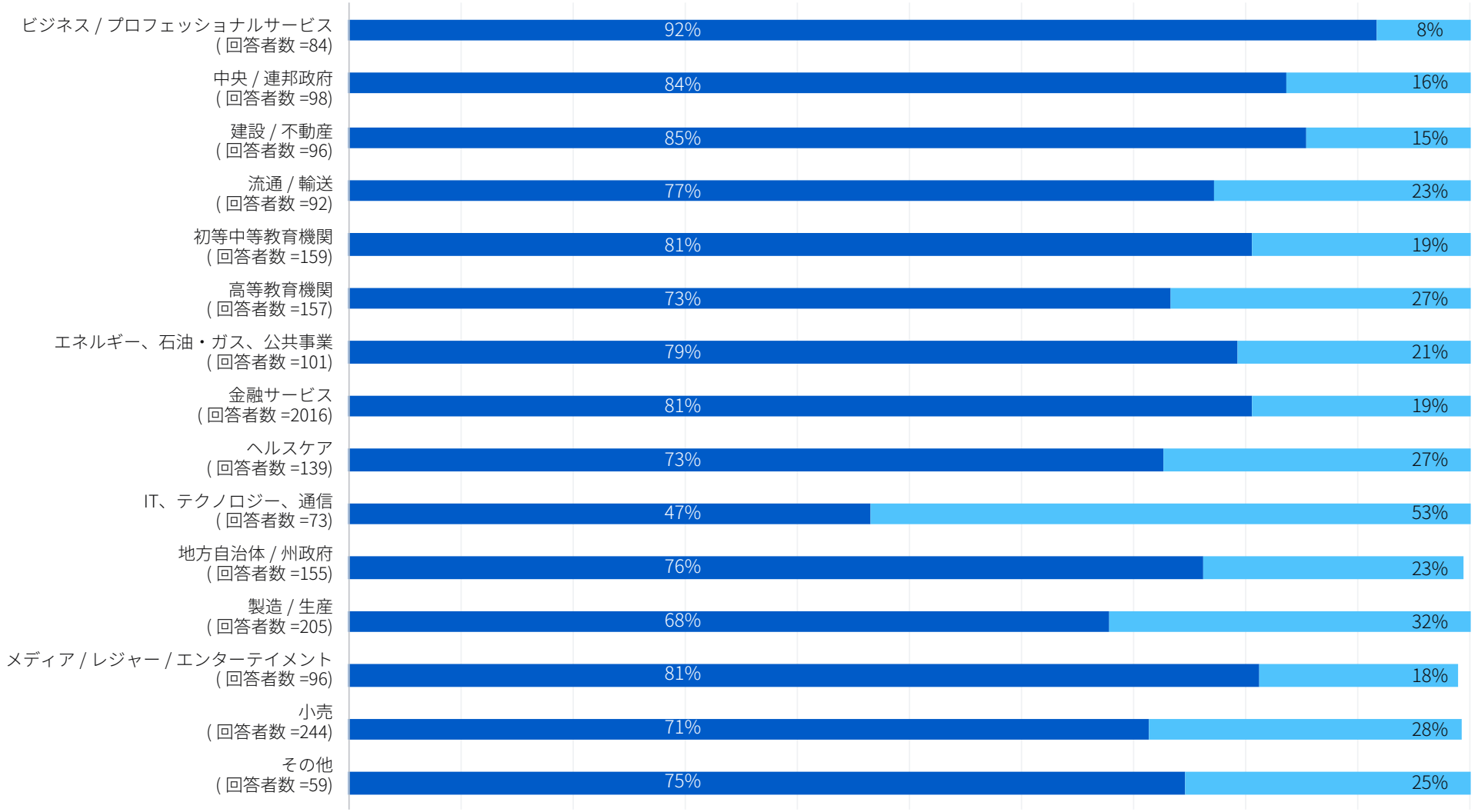
過去 1 年間にランサムウェア攻撃を受けましたか？回答数はグラフ内

業界別の攻撃の根本原因



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？回答の選択肢を選択。回答数はグラフ内

業界別のデータの暗号化



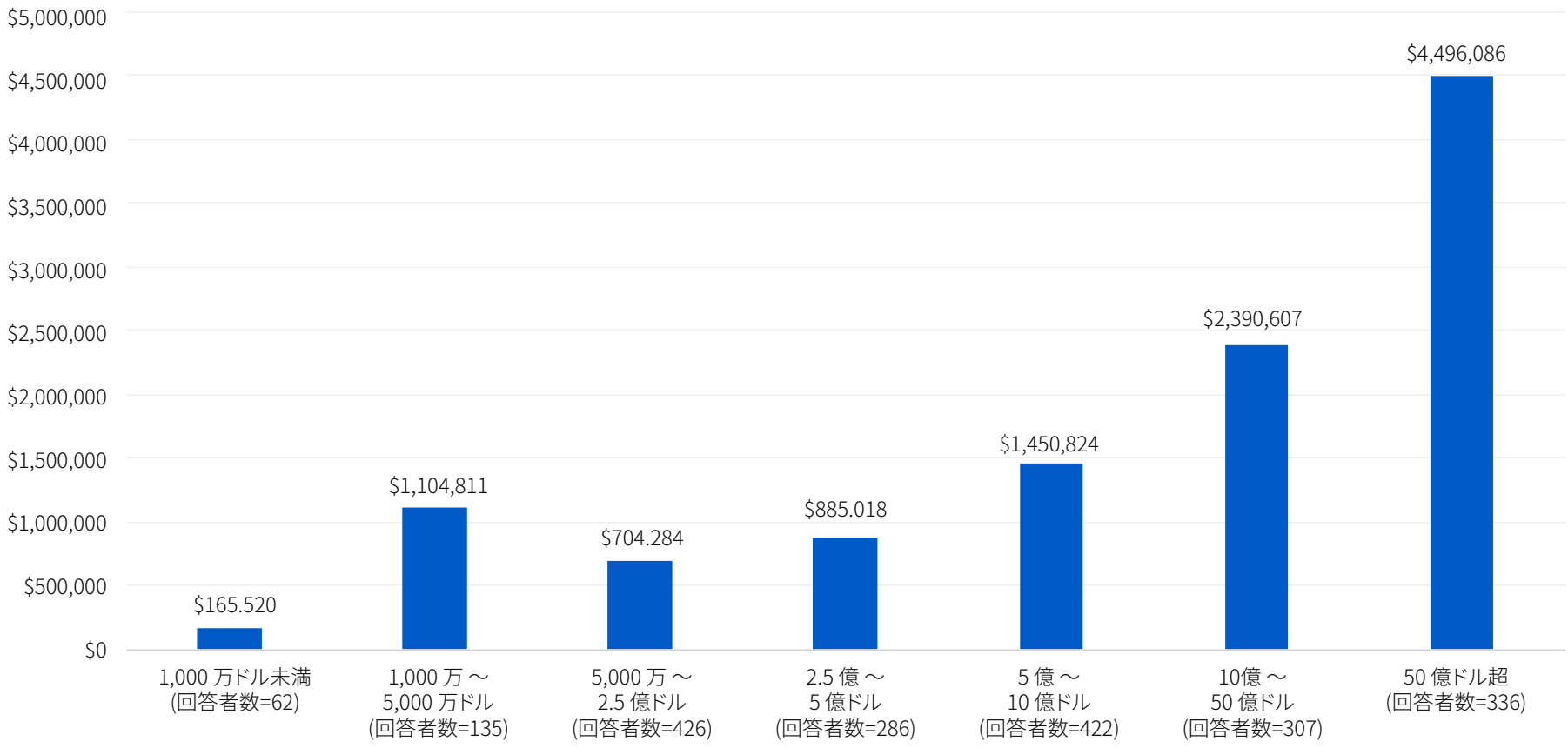
ランサムウェア攻撃でデータは暗号化されましたか？回答の選択肢を統合。回答数はグラフ内

国別のデータの復元

データを取り戻すことができましたか？

	米国 (回答者数 =274)	ブラジル (回答者数 =98)	ドイツ (回答者数 =122)	オーストリア (回答者数 =48)	スイス (回答者数 =68)	英国 (回答者数 =66)	イタリア (回答者数 =82)	スペイン (回答者数 =93)	フランス (回答者数 =68)	南アフリカ (回答者数 =139)	インド (回答者数 =167)	オーストリア (回答者数 =96)	日本 (回答者数 =125)	シンガポール (回答者数 =51)
はい。身代金を支払いデータを取り戻した	54%	55%	44%	42%	38%	44%	54%	29%	22%	45%	43%	53%	52%	53%
はい。バックアップを使用して暗号化されたデータを復元した	66%	61%	78%	73%	84%	68%	55%	81%	87%	76%	73%	73%	60%	57%
はい。他の手段を使用してデータを取り戻した	1%	4%	1%	0%	3%	0%	0%	0%	3%	3%	3%	3%	6%	0%
いいえ。身代金を支払ったのにデータを取り戻すことができなかった	1%	0%	0%	0%	0%	5%	2%	0%	3%	0%	1%	0%	0%	0%
いいえ。身代金は支払っていない	0%	1%	2%	2%	1%	2%	5%	2%	0%	0%	1%	1%	5%	10%
わからない	0%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
何らかの方法でデータを取り戻した	99%	99%	95%	98%	99%	94%	93%	98%	97%	100%	98%	99%	95%	90%
データを復元するために、複数の方法を使用した	22%	21%	27%	17%	26%	18%	16%	12%	12%	24%	20%	29%	22%	20%
身代金を支払った	55%	55%	44%	42%	38%	48%	56%	29%	25%	45%	44%	53%	52%	53%
身代金を支払った組織で、データを取り戻すことができなかった組織の割合	1%	0%	0%	0%	0%	9%	4%	0%	12%	0%	3%	0%	0%	0%

売上高別の平均復旧コスト



最も深刻なランサムウェア攻撃の影響を復旧するため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) はどれぐらいですか？」回答数はグラフ内。

調査の方法

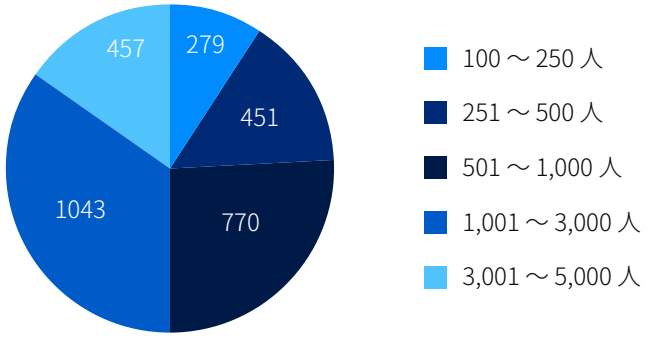
ソフォスは、2023 年 1 月から 3 月にかけて 3,000 名のサイバーセキュリティと IT 部門のリーダーに対して調査を実施しました。本調査は特定のベンダーに関連していない独立した調査機関に委託されています。回答した組織は、北アメリカ/南アメリカ、EMEA、アジア太平洋地域の 14 か国を拠点としています。

すべての回答者は従業員数 100～5,000 人未満の組織 (従業員数 100～1,000 人未満の組織が 50%、1,001～5,000 人未満の組織が 50%) に属しています。調査対象となった組織の年間売上高の範囲は、1000 万ドル未満から 50 億ドル以上です。

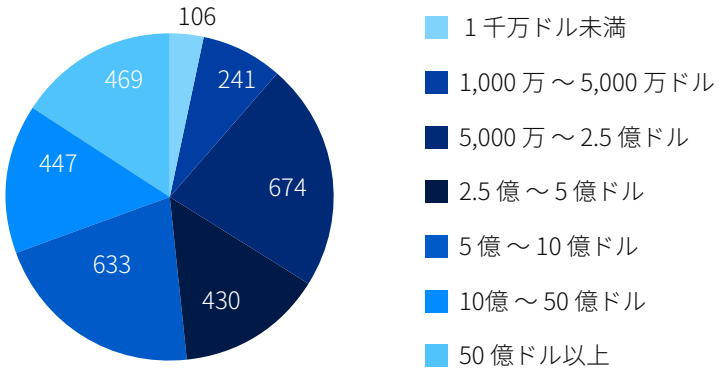
国別の回答者数

国名	回答者数	国名	回答者数
米国	500	英国	200
ドイツ	300	南アフリカ	200
インド	300	フランス	150
日本	300	スペイン	150
オーストラリア	200	オーストリア	100
ブラジル	200	シンガポール	100
イタリア	200	スイス	100

組織規模 (従業員数) 別の回答者数



組織規模 (年間売上高) 別の回答者数



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。

2023-05-05 (WP-DD)