SOPHOS

ランサムウェアの現状 2024 年版

14 か国の IT/サイバーセキュリティリーダー 5,000 人を対象に 2024 年 1 月から 2 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、毎年ランサムウェアに関する調査結果を公開していますが、今年で 5 回目になりました。このレポートでは、世界各国の組織が実際に経験したランサムウェア攻撃の被害について、根本原因から攻撃の重大度、経済的な影響、復旧にかかった時間などの包括的な情報を提供しています。新たな知見と過去の調査の学びを組み合わせることで、企業が現在直面している問題だけではなく、ランサムウェアの影響が過去 5 年間でどのように推移してきたかを理解することができます。

今年のレポートでは、要求された身代金額と実際に支払った身代金に関する調査や、企業の売上別にランサムウェアの影響を調査した結果など、新しい分野についても調査を広げています。さらに、ランサムウェアの影響を修復するときの法執行機関の役割についても初めて調査しました。

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 2024 年版になっています。回答した企業や組織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 2023 年に発生しています。

調査について

本レポートは、ソフォスが独自した調査会社に依頼して、北米 / 中南米、欧州、アジア太平洋地域の 14 か国の IT/ サイバーセキュリティ部門のリーダー 5,000 人を対象に実施した調査結果に基づきます。すべての回答者は、従業員数が 100 ～ 5,000 名の組織に所属しています。本調査は 2024 年 1 月から 2 月にかけて市場調査を専門とする Vanson Bourne によって実施され、調査対象者には前年の経験に基づいて回答するよう依頼しました。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。

5,000
回答者数

14
か国

100 ～ 5,000 人
の従業員の組織
(100 ～ 1,000 名の組織 50%、1,001 ～ 5,000 名の組織 50%)

15
業界セグメント

ランサムウェア攻撃を受けた割合

昨年は 59% の組織がランサムウェア攻撃の被害を受けました。これは過去 2 年間の両方における攻撃を受けた割合の 66% からわずかですが、減少しています。僅かながら減少傾向が見られたことは喜ばしいことですが、半数以上の組織が攻撃を経験しており、警戒を決して緩めることはできません。

2020 年	2021 年	2022 年	2023 年	2024 年
51%	37%	66%	66%	59%

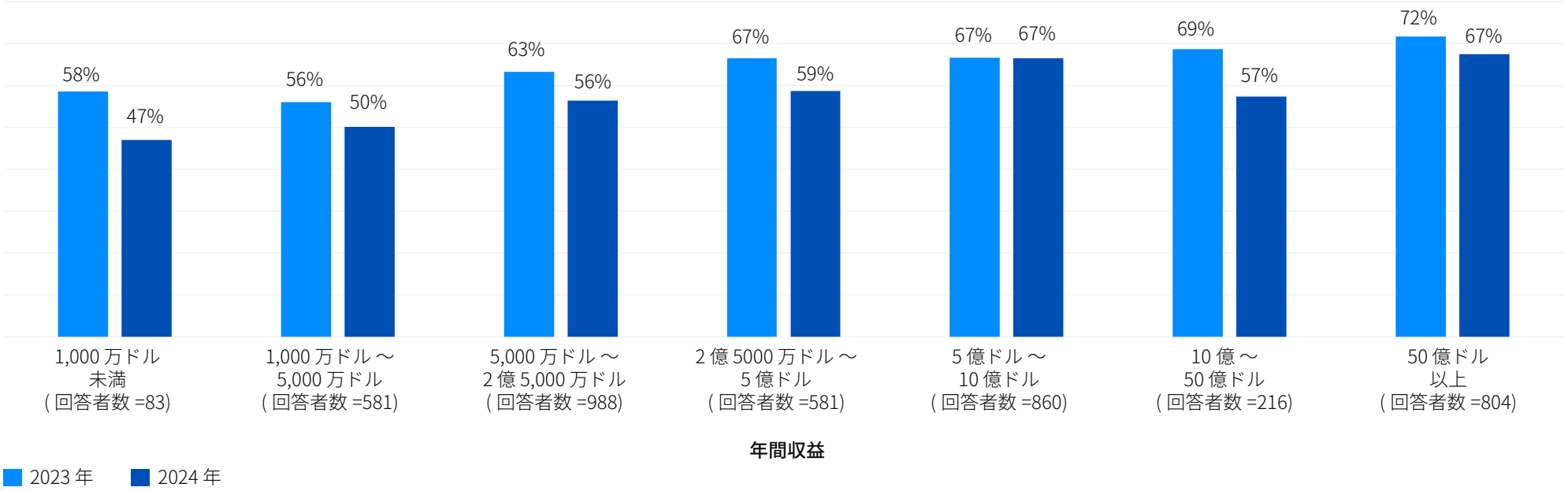
過去 1 年間にランサムウェア攻撃を受けましたか？
はい。 回答者数 = 5,000 (2024 年)、3000 (2023 年)、5,600 (2022 年)、5,400 (2021 年)、5,000 (2020 年)

売上別の攻撃率

5 億ドル～ 10 億ドルの企業が攻撃を受ける割合は 1% 未満の微減となりましたが、すべての売上カテゴリで、昨年 1 年間のランサムウェア攻撃率の減少が報告されたことは喜ばしいことです。

企業の売上高が大きくなるほど、ランサムウェア攻撃を受ける割合は通常高くなります。50 億ドル以上の企業では、攻撃を受ける割合が最も高くなっています (67%)。 しかし、規模が最も小さい企業 (売上高が 1,000 万ドル未満) であっても、依然として定期的に攻撃の標的になっています。昨年は半数弱の企業 (47%) がランサムウェアの被害を受けました。多くのランサムウェア攻撃は、高度な技術力と十分な資金を有するサイバー攻撃組織によって実行されていますが、スキルの低いサイバー攻撃者によって粗悪で安価なランサムウェアが使用されるケースが増加しています。

昨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？という質問に「はい」と回答した組織。回答者数 = 5,000 (2024 年)、3,000 (2023 年)2024 年の回答者数を図内に記載

業界別の攻撃率

一部の例外を除き、ランサムウェアの攻撃率は業界間でほぼ同じになっており、調査対象の 15 業界のうち 11 の業界で 60% から 68% の企業や組織が攻撃を受けています。今年の調査で目立ったのは、*州政府 / 地方自治体* (34%) と *小売業* (45%) であり、過去 1 年間で攻撃を受けたと回答した企業や組織者が半数以下でした。

興味深いことに、2 つの政府機関は全く異なる状況を示しました。*中央政府 / 連邦政府*は、すべての業界で最も高い攻撃率 (68%) を報告しましたが、これは、*州政府 / 地方自治体* (34%) の 2 倍です。ただ、すべての業界で攻撃が減少している傾向と同じように、*中央政府 / 連邦政府*も 2023 年の攻撃率 (70%) を下回りました。

中央政府と連邦政府が攻撃を受ける割合が高止まりしているのには、いくつかの理由が考えられます。2023 年には紛争が世界的に広がり、中央政府は政治的な動機のある攻撃を受ける環境にあったと考えられます。また、この結果は、州政府 / 地方自治体が昨年からサイバー攻撃への対策を強化する取り組みを進めていることや、州政府 / 地方自治体が身代金を支払う能力が限られていることをサイバー攻撃者が把握したためである可能性があります。

業界別のランサムウェアデータの昨年からの注目すべき変化には、以下が挙げられます。

- 攻撃を報告した割合が最も減少した業界は、*初等中等教育機関*であり (80%)、次に大きく減少した業界は*中央 / 連邦政府* (69%) でした。
- 教育業界はこれまで最も多くの攻撃を受けてきましたが、今年はその傾向に変化が見られました。昨年は*高等教育機関*が攻撃を受ける割合は 79%、*初等中等教育機関*が攻撃を受ける割合は 80% であったのに対し、今年はそれぞれ 66% と 63% に減少しました。
- ヘルスケア業界は 、昨年攻撃率が上昇した 5 つの業界のうちの 1 つであり、攻撃率は 60% から 67% に上昇しました。
- *IT、通信、テクノロジー業界*は、これまでとは異なり、最も攻撃を受けない業界ではなくなりました。昨年は 55% の組織が攻撃されており、2023 年の 50% から増加しました。

業種別のランサムウェア攻撃を受ける割合の詳細な内訳については、付録を参照してください。

国別の攻撃率

2024 年にランサムウェア攻撃を受けた割合が最も高かったのはフランスであり、回答した組織の 74% が過去 1 年間に攻撃を受けたと回答しました。次に多かったのは南アフリカ (69%) とイタリア (68%) でした。逆に、攻撃を受けた割合が最も低かったのは、ブラジル (44%)、日本 (51%)、オーストラリア (54%) でした。

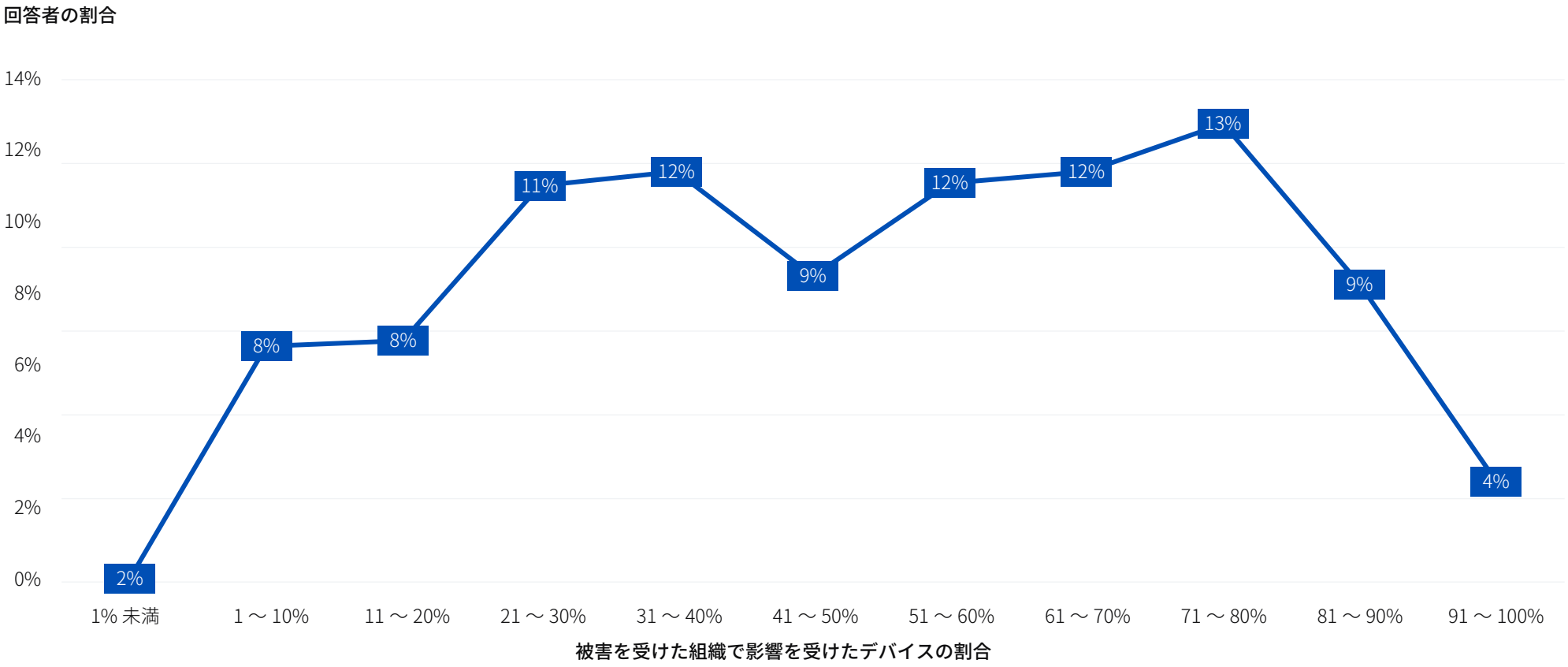
全体的には、9 か国が 2023 年よりも攻撃率が低くなったことを報告しています。2023 年よりも攻撃率が高くなった 5 か国はすべてヨーロッパ諸国であり、オーストリア、フランス、ドイツ、イタリア、イギリスでした (ドイツの増加率は 1 % 未満)。これは、欧州の企業や組織を標的とした攻撃が増加していること、あるいは欧州の企業の防御体制が他国に比べて不十分であり、サイバー攻撃の進化に追いついていないことを反映している可能性もあります。

国別のランサムウェア攻撃を受ける割合の詳細な内訳については、付録を参照してください。

影響を受けたコンピュータの割合

平均すると、組織のコンピュータの半分弱 (49%) がランサムウェア攻撃の影響を受けました。組織の環境にあるすべてのコンピュータが暗号化されるケースは極めてまれであり、91% 以上のデバイスが影響を受けたと報告した組織はわずか 4% でした。一方で、少数のデバイスにしか影響を与えなかった攻撃もありますが、これも極めてまれなケースであり、ランサムウェア攻撃を受けた組織で、その影響を受けたデバイスが 1% 未満であったと回答したのは 2% に過ぎません。

被害を受けた組織で影響を受けたデバイスの割合



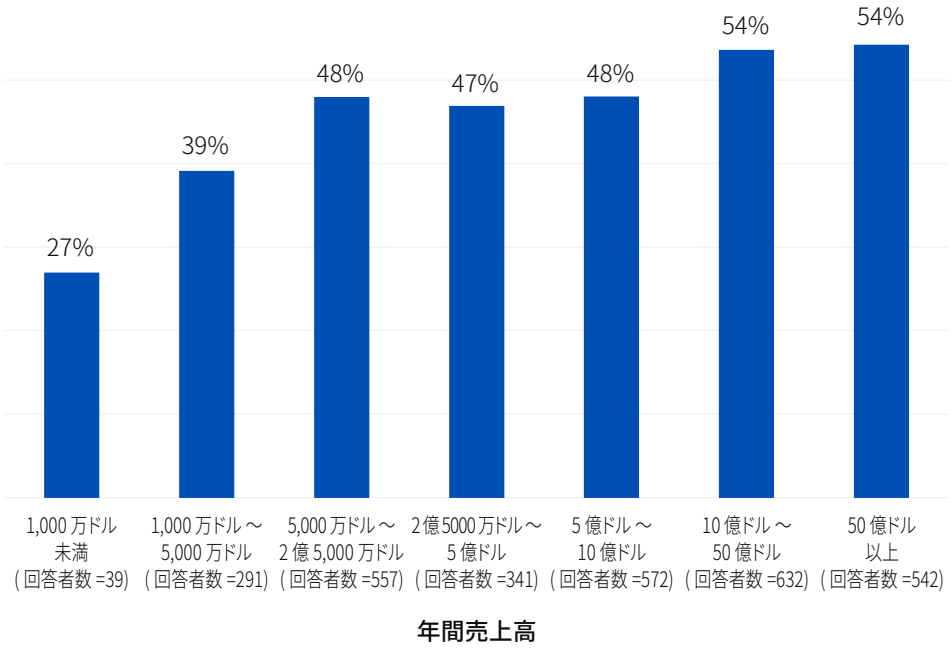
過去 1 年間にランサムウェア攻撃の影響を受けた組織のコンピュータの割合は？ 回答者数 = 2,974 (ランサムウェア攻撃を受けた組織の数)

影響を受けたコンピュータの割合 (売上別)

さまざまな規模の組織や業界全体を見ると、影響を受けたコンピュータの割合は広く分布しており、影響を受けたデバイスの割合に大きなばらつきが見られました。

売上が高くなるにつれて、ランサムウェア攻撃によって影響を受けるコンピュータの割合も増加しています。売上高が 10 億ドル以上の組織に比べて、1000 万ドル未満の売上高が最も少ない組織では影響を受けたコンピュータの割合が半分になっています (54% 対 27%)。

この結果にはいくつかの要因が考えられます。小規模な組織は、すべてのデバイスを一元的に管理している可能性が低く、攻撃が組織全体に広がる機会が軽減されています。さらに、多くの中小企業やスタートアップ企業は SaaS プラットフォームを積極的に活用しており、ランサムウェアなどの脅威によって業務が停止されるリスクが軽減されています。



過去 1 年間にランサムウェア攻撃の影響を受けた組織のコンピュータの割合は？ 回答者数 = 2,974
(ランサムウェア攻撃を受けた組織の数)

影響を受けたコンピュータの割合 (業界別)

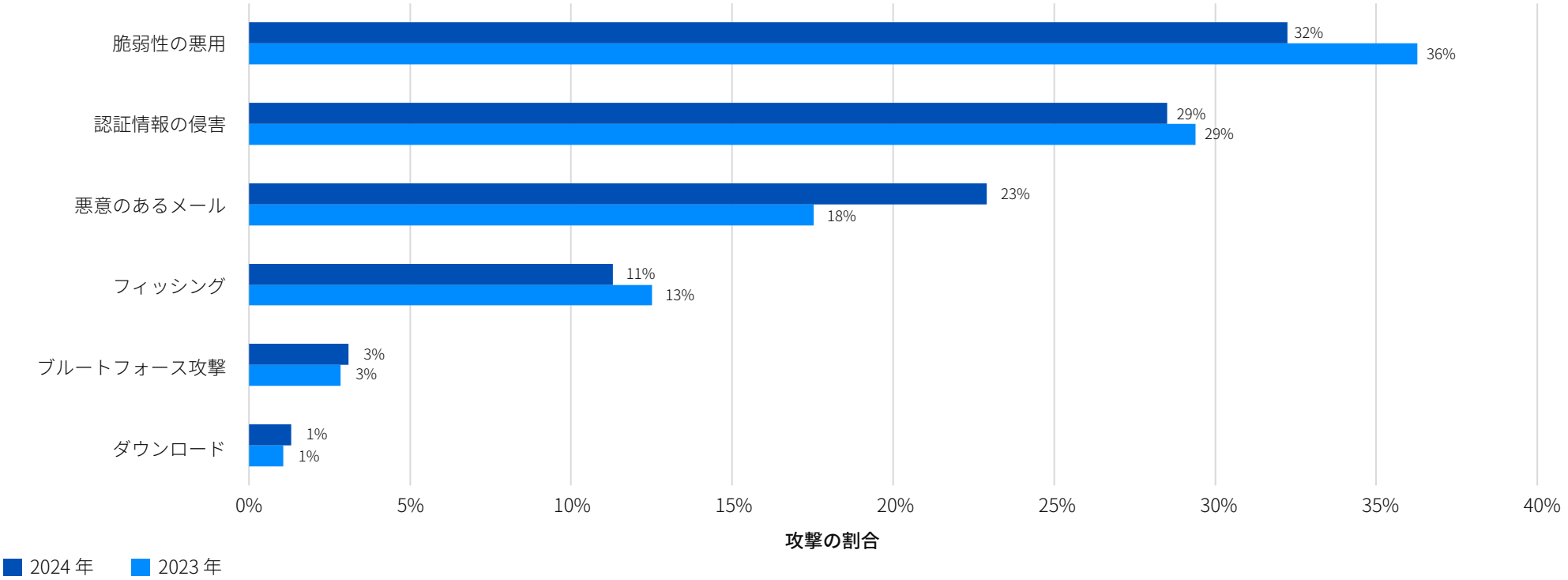
*IT、通信、テクノロジー*業界では、影響を受けたデバイスの割合が 33% と最も低くなっています。これは、この業界の組織がサイバー攻撃への堅牢な対策を広く実施していることを反映しています。 逆に、*エネルギー、石油 / ガス*、*公益事業*は、攻撃による影響が最も広範囲に及んでいる業界であり、平均して 62% のデバイスが影響を受けています。次に大きな影響を受けている業界はヘルスケア (58%) でした。これらの両方の業界では、レガシーテクノロジーや旧式のインフラ管理の仕組みが他の多くの業界よりも多く利用されており、デバイスの保護、ラテラルムーブメントの制限、攻撃の拡散防止が困難になっていると考えられます。

影響を受けるコンピュータの割合の業界別の詳細な内訳については、付録を参照してください。

ランサムウェア攻撃の根本原因

ランサムウェア攻撃を受けた組織の 99% が攻撃の根本原因を特定していますが、2 年連続で最も多かった根本原因は、「脆弱性の悪用」でした。全体的に、根本原因の順位は 2023 年の調査と一致していました。

回答者の 34% がメールでのアプローチを攻撃の根本原因として挙げており、フィッシング (メールなどの受信者を騙して機密情報を詐取するように設計されたメッセージ) と比較して、悪意のあるメール (マルウェアをダウンロードする悪意のあるリンクやファイルが添付されたメッセージ) を起点とする攻撃は約 2 倍になっています。フィッシングは通常、ログイン情報を詐取するために使用されており、認証情報を侵害するための最初のステップになっています。



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？はい。 回答者数 = 2,974 (ランサムウェアの被害を受けた組織)

脆弱性を悪用する攻撃

あらゆるランサムウェア攻撃は悪影響をもたらしますが、特に壊滅的な被害を及ぼすものもあります。パッチが適用されていない脆弱性の悪用から始まった攻撃を受けた組織は、認証情報の侵害で始まった攻撃を受けた組織よりも、さらに深刻な被害を報告しています。たとえば、以下のような被害が発生する傾向が高いことが確認されています。

- バックアップの侵害
  (成功率 75%、認証情報の侵害の場合は 54%)
- データの暗号化
  (暗号化率 67%、認証情報の侵害の場合は 43%)
- 身代金の支払い
  (支払率 71%、認証情報の侵害の場合は 45%)
- 身代金のコスト全額を社内の資金で負担
  (身代金全額を社内の資金で負担する割合 31%、認証情報の侵害の場合は 2%)

さらに、次の点も報告されています。

- 全体的な攻撃からの復旧コストが 300 万ドル
  (認証情報が侵害されたケースの復旧コスト 75 万ドルの 4 倍)
- 復旧に時間がかかる
  (1 か月以上かかるケースが 45%、認証情報の侵害の場合は 37%)

詳細については、「パッチが適用されていない脆弱性：最も凶悪なランサムウェア攻撃ベクトル」を参照してください。

業界別の根本原因

特定の業界には、サイバー防衛における弱点が多く存在しており、サイバー攻撃者はこのような弱点をすぐに見つけて悪用しています。そのため、ランサムウェア攻撃の根本原因は業界によって大きく異なります。

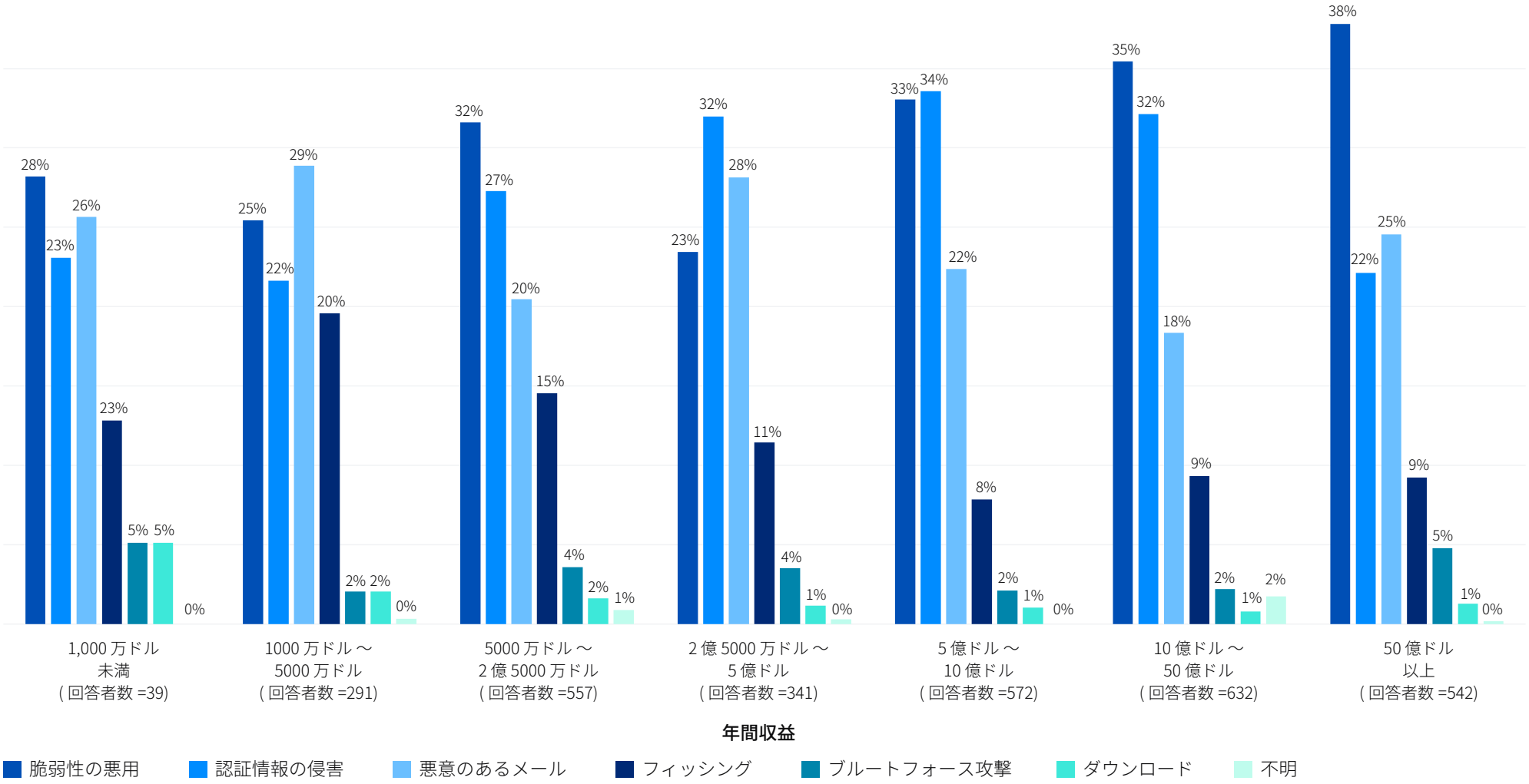
- *エネルギー、石油・ガス*、公益事業は、パッチが適用されていない脆弱性が悪用される可能性が最も高い業界であり、攻撃のほぼ半数 (49%) がこの方法から始まっています。一般的に、この業界では、他の多数の業界よりも、セキュリティギャップが生じやすい古い技術が多く使用されています。また、レガシーソリューションやサポートが終了したソリューションでは、パッチが提供されていない可能性もあります。
- 政府機関は、侵害された認証情報の悪用を起点とする攻撃に対して特に脆弱であり、*州政府 / 地方自治体*に対する 49% の攻撃および中央政府 / 連邦政府に対する 47% の攻撃が、窃取されたログインデータが使用されて始まっています。
- *IT、通信、テクノロジー*業界および*小売*業界の両方が、ランサムウェアインシデントの 7% が総当たり攻撃から始まったことを報告しています。パッチが適用されていない脆弱性や侵害された認証情報が減少したことで、サイバー攻撃者は、一部の攻撃では他の手法に集中せざるを得なくなった可能性もあります。

業界別の攻撃の根本原因の詳細な内訳については、付録を参照してください。

売上高別の根本原因

一般的に、大規模な組織になるほど、パッチが適用されていない脆弱性を起点とする攻撃を受ける可能性が高くなります。50 億ドル以上のカテゴリでは、この方法を起点とする攻撃の割合が最も高いことが報告されています (38%)。組織が成長するにつれて、IT インフラの規模も複雑さも増していきます。IT チームがすべてのリスクエクスポージャーを把握し、攻撃者に悪用される前にパッチを適用することが難しくなっています。

ランサムウェア攻撃の手法の 1 つとして利用される認証情報の侵害は、売上高が中 / 高レベルのグループでピークに達しており、2 億 5,000 万ドル～ 5 億ドルと 5 億ドル～ 10 億ドルの両方のグループでは攻撃原因のトップになっています。脆弱性や認証情報の侵害は重大な根本原因ですが、売上高が 1,000 万ドルから 5,000 万ドルのグループの企業から報告された根本原因のトップは悪意のあるメールです。全体として、メールベースの脅威は、このグループの企業に対する攻撃の半分弱 (49%) を占めています。



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？ 回答者数 =2,974 (ランサムウェア攻撃を受けた組織)

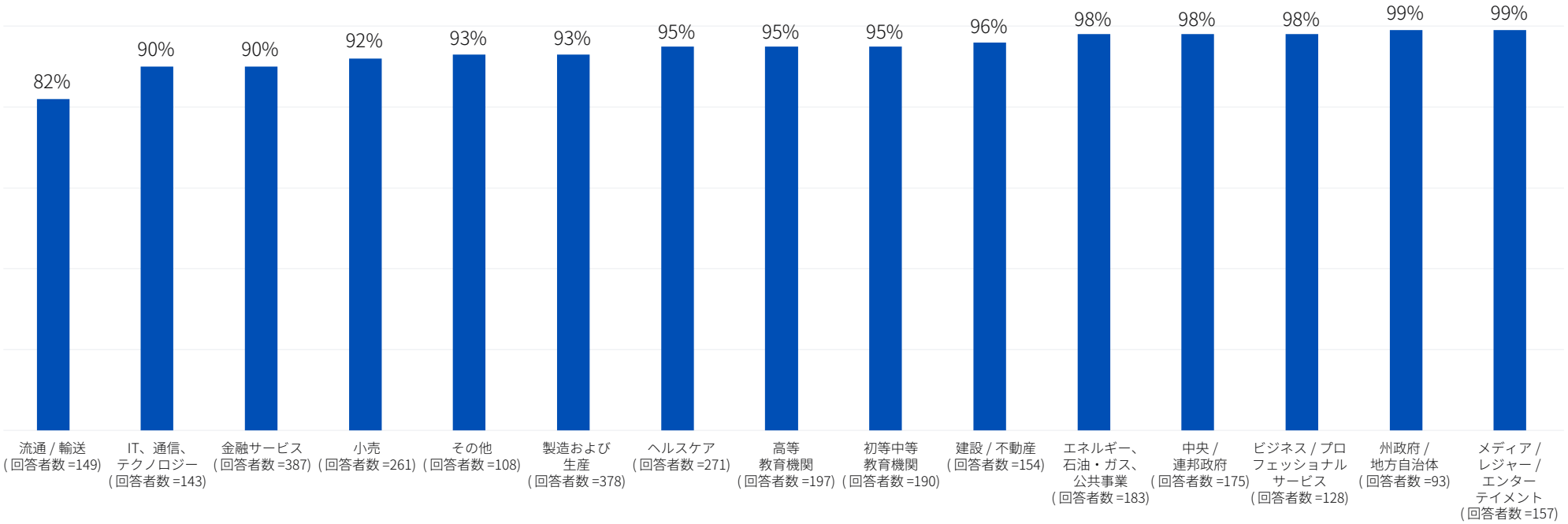
バックアップの侵害

ランサムウェア攻撃によってデータが暗号化された場合、それを復旧する方法は主に、バックアップから復旧するか、または身代金を支払うかのいずれかです。サイバー攻撃者は、バックアップを侵害することで暗号化したデータの復旧を阻み、組織に対して金銭を支払うようにプレッシャーをかけます。

バックアップ侵害の試行

過去 1 年間にランサムウェアの被害に遭った組織のうち 94% が、同時にバックアップの侵害も試みられたと回答しています。この割合は、*州政府 / 地方自治体*、メディア / レジャー / エンターテイメントの業界では 99% に達しました。この割合が最も低かったのは*流通 / 輸送*業でしたが、それでも 10 社中 8 社以上 (82%) の組織が、バックアップへのアクセスが試みられたと回答しています。

攻撃者がバックアップの侵害を試行した攻撃の割合



サイバー犯罪者はあなたの組織のバックアップデータの侵害を試みましたか？はい。回答数を図内に記載。

バックアップ侵害の成功率

すべての業界において、バックアップを侵害する試みの 57% が成功しています。つまり、サイバー攻撃者は、被害を受けた半数以上の組織がランサムウェア攻撃で受けた影響を復旧する作業を妨害できたことになります。注意しなければならないのは、こうしたバックアップ侵害の成功率が業界によって大きく異なることです。

- 攻撃者がバックアップの侵害に成功する割合が最も高かったのは、*エネルギー、石油 / ガス、公益サービス* (成功率は 79%) と *教育業界* (成功率 71%) でした。
- *IT、通信、テクノロジー業界* (成功率は 30%) と *小売業界* (成功率 47%) は、バックアップの侵害に成功する割合が最も低くなっています。

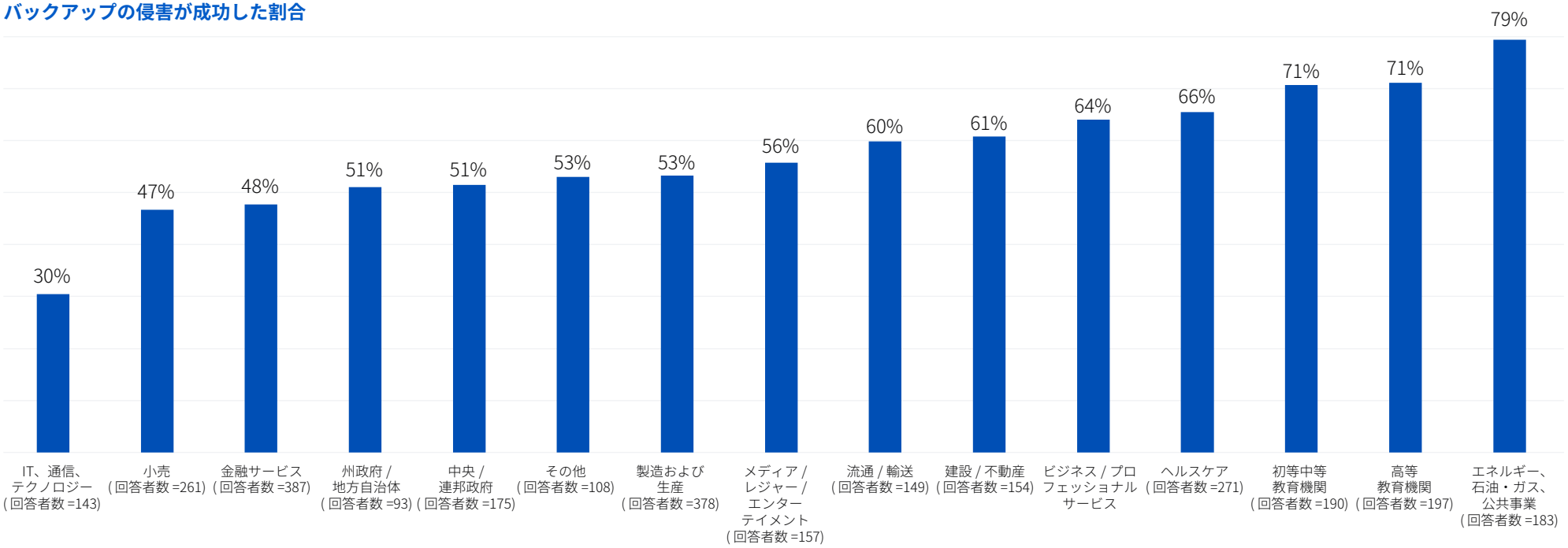
これには、いくつかの理由が考えられます。*IT、通信、テクノロジー業界*では、バックアップを保護するための強力な対策を整えており、他の業界と比較して攻撃への耐性が高かったことが考えられます。または、侵害が試行された段階での検出・阻止が効果を発揮した可能性もあります。

攻撃の根本原因に関わらず、バックアップが侵害された組織からは、侵害されなかった組織と比較して、以下のように被害が大きく拡大するとの結果が報告されています。

- 身代金の要求額は、バックアップが侵害されなかった組織の平均 2 倍以上 (最初に要求された身代金の中央値が 100 万ドル 対 230 万ドル)。
- バックアップが侵害された組織では、暗号化されたデータを復旧するために身代金を支払う割合が約 2 倍 (67% 対 36%)。
- 全体的な攻撃からの復旧コストの中央値は、バックアップが侵害された場合には 8 倍になるる (300 万ドル対 37 万 5,000 ドル)

この問題の詳細については、「ランサムウェアにおけるバックアップの侵害がもたらす影響」を参照してください。.

バックアップの侵害が成功した割合



サイバー犯罪者はあなたの組織のバックアップデータの侵害を試みましたかという質問に「はい」と回答。回答数を図内に記載。

データが暗号化される割合

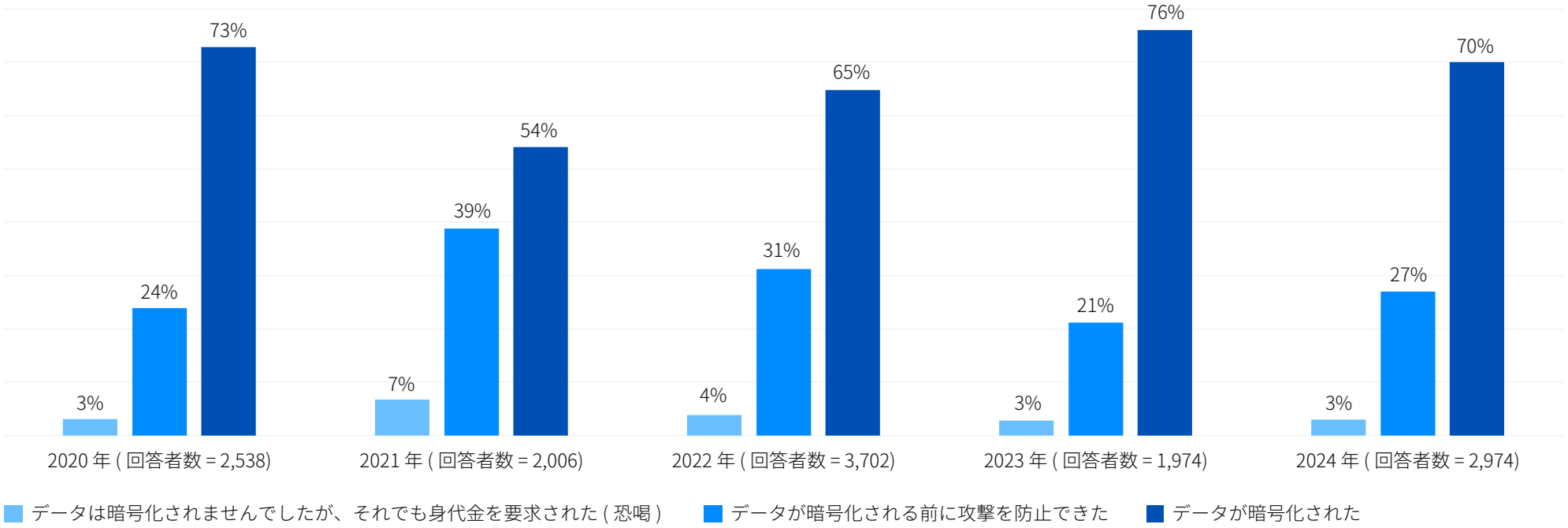
昨年発生した 10 件に 7 件 (70%) のランサムウェア攻撃で、データが暗号化されました。この割合は高いものの、2023 年に報告されたデータ暗号化に成功した攻撃の割合は 76% であり、わずかに低下しています。

データ暗号化率 (業界別)

2024 年の調査では、業界によって暗号化される割合にかなりのばらつきがあることが明らかになりました。

- 今年は、*州政府 / 地方自治体*は攻撃を受ける割合が最も低くなりましたが (ランサムウェア攻撃を受けた組織は 34%)、**データの暗号化率は最も高く**、98% の攻撃でデータが暗号化されたと報告されています。
- **データの暗号化率が最も低かったのは**、*金融サービス* (49%) であり、次いで小売 (56%) でした。
- *流通・運輸*は、**恐喝型攻撃**を受ける可能性が最も高い業界であり、17% の組織が「データは暗号化されていなかったが、身代金を要求された」と回答しています。この数値は、他の業界と比較して 3 倍高くなっています。

データの暗号化率の業界別の詳細な内訳については、付録を参照してください。



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。

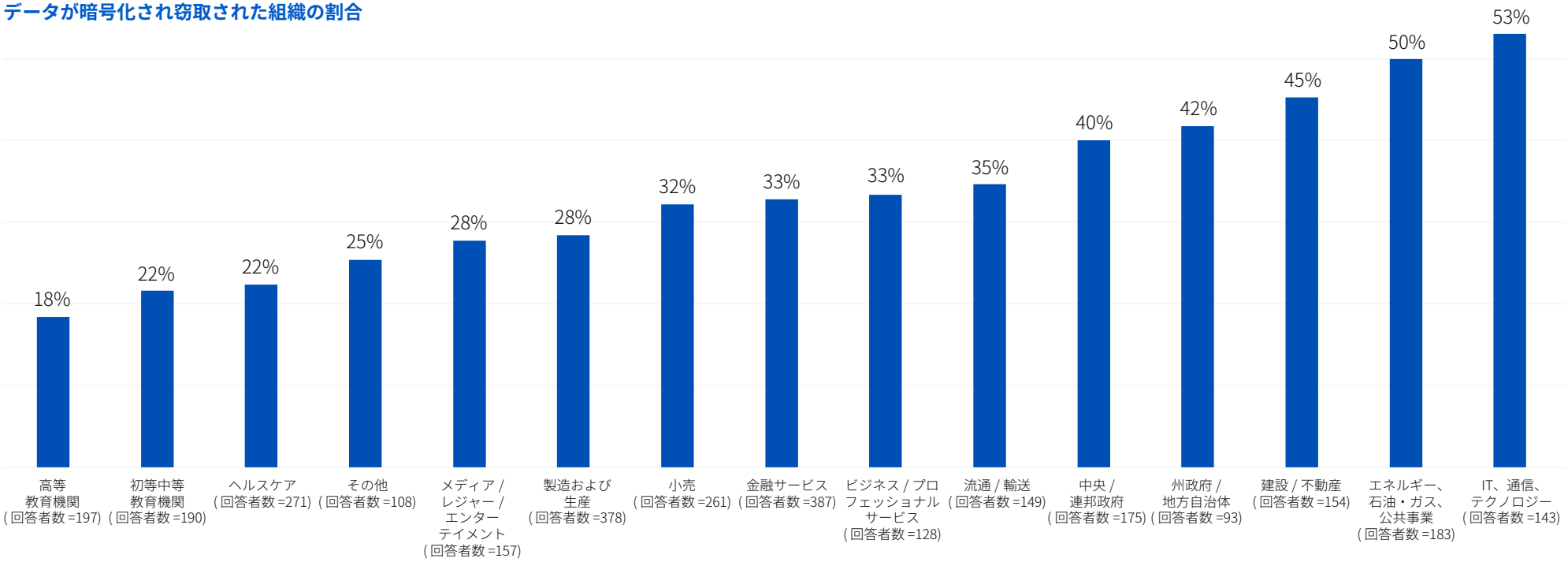
データの窃取

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。データが暗号化された 32% のインシデントでデータも窃取されています。これは昨年の割合 30% よりも若干増加しています。データが窃盗されると、被害を受けた組織から金銭を脅し取る可能性が高くなります。窃取したデータをダークウェブで販売することもでき、攻撃者はさらに多くの収益を得ることが可能になります。

データが窃取される割合も、業界によって大きな差異があります。最も悪い結果だったのは *IT、通信、テクノロジー*業界であり、データが暗号化された攻撃の 53% でデータも窃取されたと報告しています。*エネルギー、石油・ガス、公共事業*は第 2 位であり、データが暗号化された攻撃の 50% でデータも窃取されています。逆に、教育業界は攻撃によってデータが窃取されたことを報告した割合が最も低くなりました。 *高等教育機関*はデータが暗号化されて盗まれる割合が全業界で最も低く (18%)、次に低かったのは*初等中等教育機関*とヘルスケア業界であり、その割合は両方ともに 22% でした。

この結果は、各業界における調査能力の違いや、優先順位の違いを反映している可能性があります。データが流出したかどうかを判断するには、高度なフォレンジック機能が必要であり、多くの場合、EDR/XDR ツールのログを分析しなければなりません。*IT、通信、テクノロジー*業界は、他の業界よりもデータ窃取を特定する能力が高い可能性もあります。*エネルギー、石油・ガス、公益事業*の環境は単純であることが多く、この業界ではデータ窃取を特定することが容易なのかもしれません。逆に、教育機関はデータが窃取されたかどうかを判断するスキルやツールを導入していないケースが多くあります。また、データ漏洩により高額な保証が発生する可能性があるため、データが流出したかどうかを把握したくないと考える組織もあるかもしれません。

データが暗号化され窃取された組織の割合



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。はい。データも盗まれた。回答数を図内に記載。

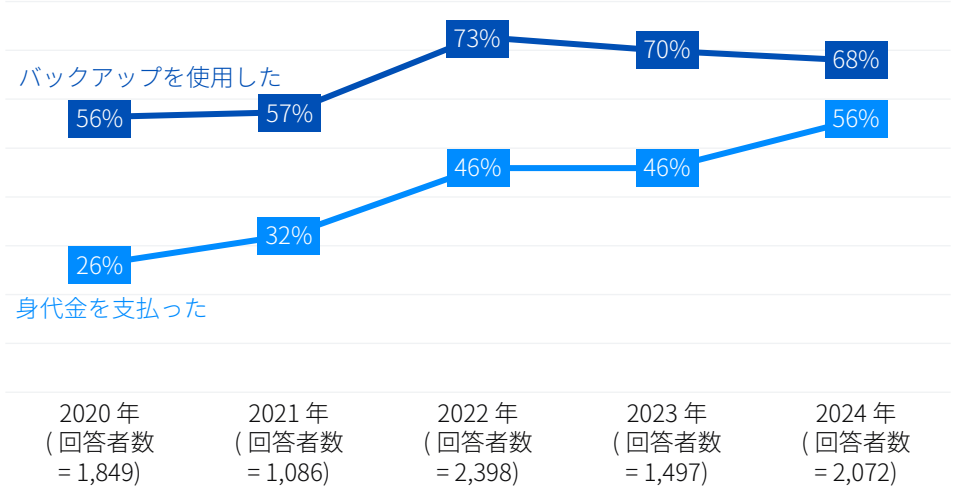
データの復元

データが暗号化された組織の 98% がデータを取り戻しています。データを復元する主な方法は、バックアップからの復旧 (68%) と、身代金を支払って復号鍵を入手する方法 (56%) の 2 つです。データが暗号化された組織の 26% が、データを取り戻すために「他の手段」を使用したと回答しています。この調査結果では、これらの他の手段については詳しく調査していませんが、法執行機関との協力や、公開されている復号鍵の使用などが含まれている可能性があります。

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
68%	56%	26%

昨年からの大きな変化として、被害を受けた組織が暗号化されたデータを復元するためにいくつかのアプローチ (身代金の支払いやバックアップの利用など) を用いる傾向が強まっていることが挙げられます。データが暗号化された組織の半数近く (47%) が、2024 年の調査では複数の方法を使用したと報告しています。これは 2023 年に報告された割合 (21%) の 2 倍以上です。

5 年間の推移を見ると、バックアップを使用する割合と身代金を支払う割合の差異が縮小し続けています。バックアップを使用する割合は、わずかですが 2 年連続で減少しています。同時に、2023 年の調査以来、身代金を支払う割合は 10% 増加しています。身代金を支払うかどうかは、バックアップの有無など多くの要因に左右されますが、これは憂慮すべき傾向であり、被害を受けた組織の半数以上が復号鍵を入手するために身代金を支払っていることは大きな問題です。



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。回答者数を図内に記載。

データの復元 (売上別)

データを復元するために身代金を支払う傾向は、一般的に組織の売上が増加するにつれて高まります。売上の規模が最も小さい組織 (1,000 万ドル未満) が身代金を支払う割合が圧倒的に低い (25%) のに対して、売上の規模が最も大きい組織 (50 億ドル以上) が支払う割合は最も高く (61%) なっています。身代金の支払いに充てる資金を確保できるかどうかが大きな要因になっている可能性があります。規模の小さい多くの企業は、単に身代金を支払うための資金がない場合があります。

しかし、これまで見てきたように、データを復元するためには、バックアップと身代金のいずれかの方法を利用すれば良いわけではなくなっています。2024 年の数字を昨年の結果と比較し、詳細なデータを見ていくと、データを復元する方法に違いがあることがわかります。

1,000 万ドル以下のグループの企業以外では、すべての売上高のグループの企業が、身代金を支払う割合が昨年より増加したと報告しており、そのうちの 3 つのグループでは、データを復元するためにバックアップを使用した割合も増加しています。売上高が最も低いグループの企業がバックアップを使用する割合が最も高かった (88%) のに対し、2 億 5,000 万ドル～ 5 億ドルのグループの企業が僅差で (85%) で続いています。

データの復元 (業界別)

当然かもしれませんが、中央政府 / 連邦政府は、データを取り戻すために身代金を支払う割合が最も低くなっています (39%)。規制によって身代金を支払うことが厳格に制限されていることは間違いなくありません。また、この業界は、バックアップを使用する割合が 81% と最も高くなっています。

業界全体を見ると、バックアップの使用と身代金の支払いには明確な相関関係は見られません。

- メディア、レジャー、エンターテイメント業界は、データを復元するために身代金を支払う割合が最も高く (69%)、バックアップを使用する割合も高くなっています (74%)。
- エネルギー、石油 / ガス、公益事業は、バックアップを使用する割合が最低レベル (51%) で、身代金を支払う割合は 61% と他の 4 つの業界よりも低くなっています。

データを復元する方法の業界別の詳細な内訳については、付録を参照してください。

	年間売上高													
	1,000 万ドル未満 (回答者数 =39)		1,000 万ドル ～ 5,000 万ドル (回答者数 =291)		5,000 万ドル ～ 2 億 5,000 万ドル (回答者数 =557)		2 億 5000 万ドル ～ 5 億ドル (回答者数 =341)		5 億ドル ～ 10 億ドル (回答者数 =572)		10 億ドル ～ 50 億ドル (回答者数 =632)		50 億ドル以上 (回答者数 =542)	
使用したデータの復元方法	2023 年	2024	2023	2024 年	2023 年	2024 年	2023 年	2024 年	2023 年	2024 年	2023 年	2024 年	2023 年	2024 年
バックアップを使用してデータを復元した割合	80%	88% ▲	72%	68% ▼	77%	60% ▼	75%	85% ▲	68%	70% ▲	66%	65% ▼	63%	66% ▲
身代金を支払ってデータを取り戻した割合	36%	25% ▼	41%	49% ▲	42%	57% ▲	33%	50% ▲	51%	59% ▲	52%	56% ▲	55%	61% ▲

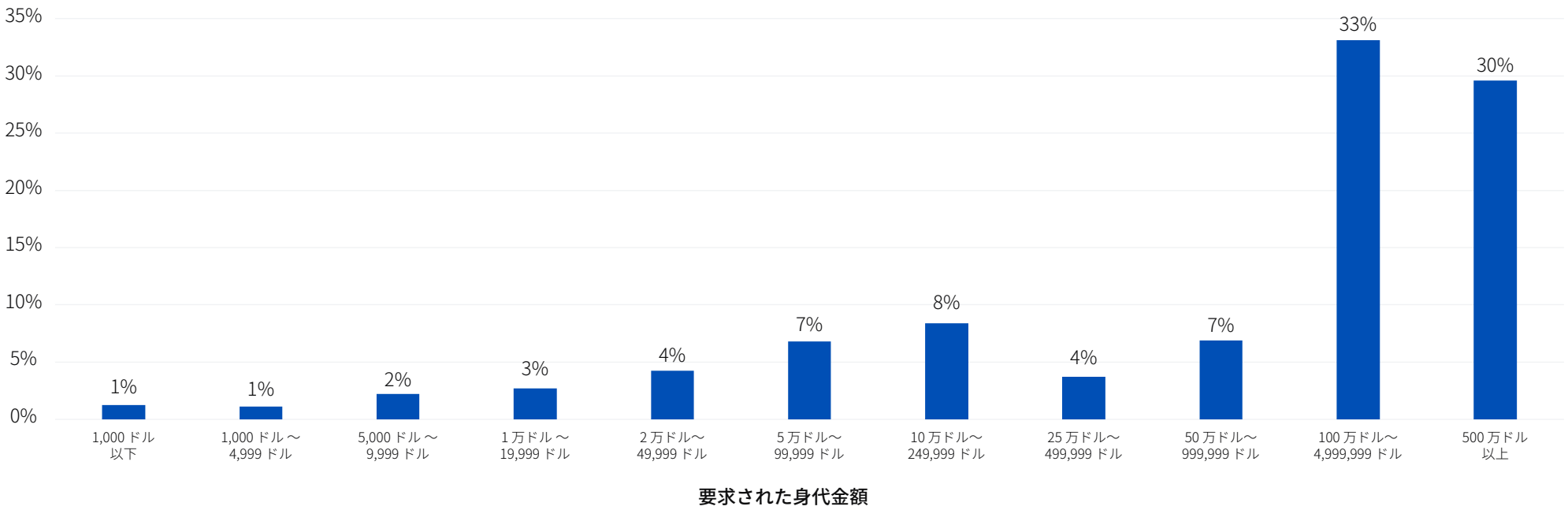
データを取り戻すことができましたか？はい、身代金を支払ってデータを取り戻しました。はい、バックアップを使用してデータを復元しました。2024 年の回答数を図内に記載。矢印は 2023 年と比較した増減を示します。

要求された身代金額

今年のレポートでは初めて、要求された身代金額と実際に支払った金額の両方を掲載しました。データが暗号化され、攻撃者から最初に要求された身代金額を共有した 1,701 の企業や組織全体の平均要求額は 4,321,880 ドル (平均値) であり、中央値は 200 万ドルでした。

今年の調査で最も注目すべき点は、要求される身代金の 63% が 100 万ドル以上であり、30% が 500 万ドル以上に達していることです。1000 万ドル以上の身代金を要求されたと報告した回答者もいましたが、これはごく少数です。

身代金が要求された割合



攻撃者から要求された身代金額はいくらでしたか？ 回答者数 = 1,701

要求された身代金額 (売上高別)

平均値と中央値の両方のデータを見ると、要求される身代金額は企業の売上高に合わせて上昇する傾向があります。サイバー攻撃者は、少なくとも部分的には、組織の支払い能力に応じて身代金の要求額を調整しています。

巨額の身代金が要求されるケースは、売上高が巨大な企業だけではなくなっており、100 万ドル以上の身代金を要求されるケースは、今では全ての企業にとってごく普通になっています。売上高が 1,000 万～ 5,000 万ドルの企業の 47% が、昨年 100 万ドルの身代金を要求されました。

要求された身代金額 (業界別)

身代金の要求ではカテゴリ別に大きな差異はなく、「その他」を除くすべてのカテゴリで、要求される身代金の中央値が 100 万ドル以上になっています。

- *小売*、*IT*、*通信*、*テクノロジー*業界の中央値が最も低く (100 万ドル) で、次に中央値が低いのは*建設業界* (110 万ドル) でした。
- *中央政府 / 連邦政府*は、中央値 (770 万ドル) と平均値 (990 万ドル) が最も高く、最も大きな標的となっています。

要求される身代金額の業界別の詳細な内訳については、付録を参照してください。

	年間売上高					
要求された身代金額	**1,000 万ドル～ 5,000 万ドル (回答者数 =207)**	**5,000 万ドル～ 2 億 5,000 万ドル (回答者数 =288)**	**2 億 5,000 万ドル～ 5 億ドル (回答者数 =158)**	**5 億ドル～ 10 億ドル (回答者数 =268)**	**10 億ドル～ 50 億ドル (回答者数 =366)**	**50 億ドル以上 (回答者数 =398)**
平均値	$1,774,941	$1,704,853	$3,407,796	$5,184,024	$4,281,258	$7,467,294
中央値	$330,000	$220,000	$840,000	$2,000,000	$3,000,000	$6,600,000

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。注：売上が「1,000 万ドル未満」と回答者した組織は少ないため、この表から除外しています。

身代金の支払い

身代金を支払った組織の回答者 1,097 人が、実際に支払った金額を共有しました。中央値と平均値の両方を見ると、支払った身代金は昨年大幅に増加しています。

- 支払い金額の中央値：200 万ドル (2023 年に報告された 40 万ドルから 5 倍に増加)
- 支払い金額の平均値：3,960,917 ドル (2023 年の 1,542,330 ドルから 2.6 倍に増加)

以下のグラフを見れば、低い身代金を支払う割合が過去 3 年間で減少傾向にある一方で、非常に高額な身代金を支払う割合が急増していることがわかります。100 万ドル以上の身代金を支払うことは、今や当たり前になっています。

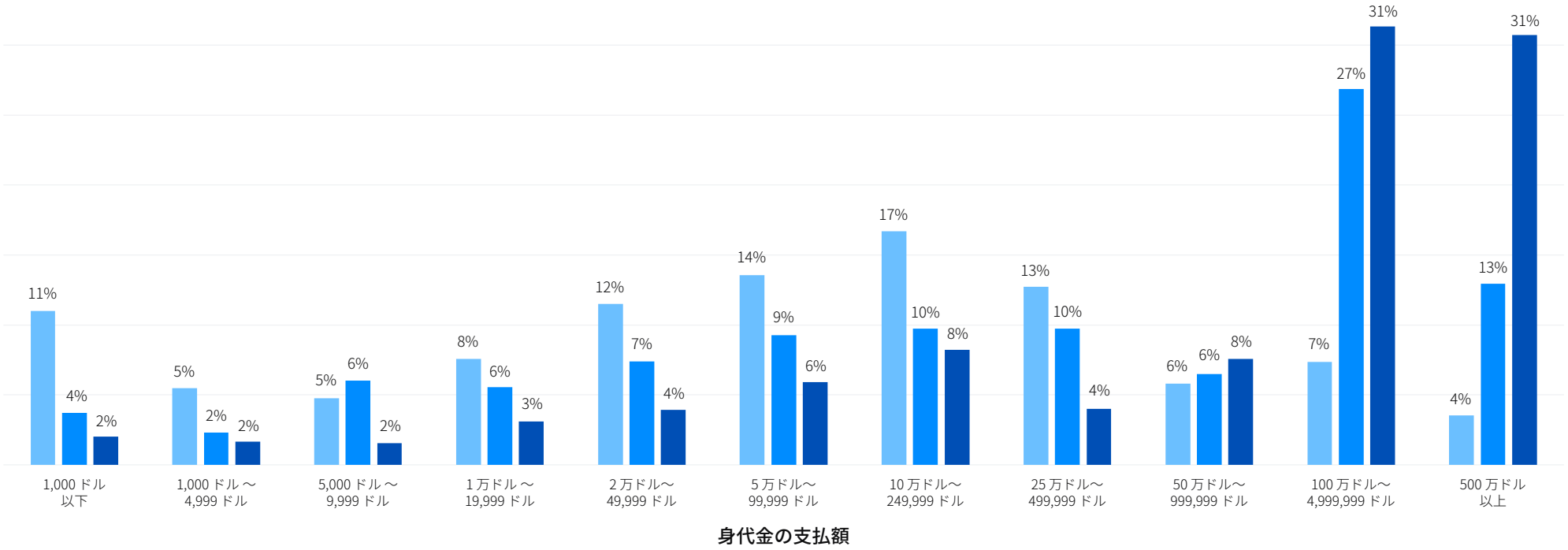
身代金支払額の分布 2022-2024 年

身代金の支払額 (業界別)

要求される身代金額の平均値は業界によって大きく異なりますが、支払った身代金額も業界によって大きく異なります。支払った身代金額の中央値が最も低かったのは *IT、通信、テクノロジー業界* であり (30 万ドル)、*流通 / 運輸業界* が次に低くなっていました (44 万ドル)。最も高かったのは、*初等中等教育機関* と *中央政府 / 連邦政府* の両方であり、中央値で 660 万ドルの身代金を支払っています。

要求される身代金額が低い場合には支払う金額も低くなり、要求される身代金額が高い場合には、支払う金額も高くなる傾向がありますが、例外もあります。特に *流通 / 運輸* 業界では、要求される身代金額の中央値は 280 万ドル以上でしたが、支払った身代金は平均で 44 万ドルでした。

支払った身代金額の業界別の詳細な内訳については、付録を参照してください。



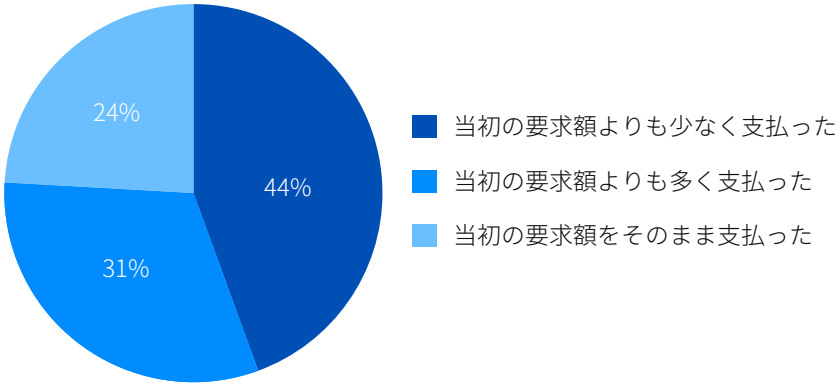
攻撃者に支払った身代金はいくらでしたか？回答者数を図内に記載。

要求された身代金額と支払った身代金の比較

データが暗号化されると、関係者全員が緊迫した時間を過ごすことになります。データが暗号化された組織は、金銭的な影響を最小限に抑えようとする一方で、攻撃者はできるだけ短い期間にできるだけ多くの金銭を得ようとします。多くの攻撃では、身代金の支払期限を設けて、その期限を超過すると、身代金を増額すると脅して、さらに圧力をかけています。

身代金額に関する交渉傾向

今回の調査では、被害を受けた組織が攻撃者から最初に要求された金額を支払うことは稀であることが明らかになりました。実際に支払った額が最初に要求された身代金額と同じと述べた回答者はわずか 24% でした。44% が最初に要求されたよりも少ない金額を支払っており、31% がより多くの金額を支払っていました。



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 = 1,097

業界別のデータを見ると、*ビジネスおよびプロフェショナルサービス業界*と*金融サービス業界*の 2 つのサービス業界では、身代金支払について交渉し、減額している傾向が最も高く、67% の回答者が最初の要求額よりも低い金額を支払ったと述べています。次に身代金を減額している傾向が高かったのは、*製造および生産業界*であり、この業界の 65% の企業が最初に要求された金額よりも少ない金額を支払っています。

逆に、最初に要求された身代金よりも多く支払う可能性が高いのは、公共機関です。

- *高等教育機関*は、最初に要求された身代金額よりも多くを支払う可能性が最も高く (67%)、最初に要求された身代金額よりも少なく支払う可能性が最も低くなっています (20%)。
- 最初に要求されたよりも高い身代金を支払っている業界の第 2 位はヘルスケア業界であり（57%)、第 3 位は*初等中等教育機関* (55%) でした。

このような業界では、身代金を交渉する専門家を雇って、コストを削減することが難しいことが考えられます。また、公的な業務であることから、「どれだけ多くの費用を支払っても」データを復旧させる必要があるのかもしれません。いずれにしても、最初に要求される身代金額と最終的に支払われた金額が異なっていることが今回の調査から明らかになりました。

要求された身代金額と実際に支払った身代金の業界別の詳細な内訳については、付録を参照してください。

要求された身代金に対して実際に支払った金額の割合

身代金額に関する交渉はほぼすべてのケースで行われていますが、最終的な金額の増減は比較的小さく、すべてのグループの回答者の平均値を見ると、最初に要求された金額の 94% が支払われています。

さらに詳細なデータを見ると、売上高が最も大きなグループを除くすべてのグループが身代金の支払額を減額できたことがわかります。5,000 万ドルから 2 億 5,000 万ドルのグループの組織は、最初に要求された身代金額よりも実際に支払った金額の割合が最も低くなりました (84%)。最初に要求された身代金額よりも多く支払った唯一のグループは、売上高が 50 億ドル以上のグループの企業であり、平均して 115% の金額を支払っています。

	年間売上高					
グループ	1,000 万ドル ～ 5,000 万ドル (回答者数 =100)	5,000 万ドル ～ 2 億 5,000 万ドル (回答者数 =206)	2 億 5,000 万ドル ～ 5 億ドル (回答者数 =104)	5 億ドル ～ 10 億ドル (回答者数 =175)	10 億ドル ～ 50 億ドル (回答者数 =233)	50 億ドル 以上 (回答者数 =275)
要求された身代金に対して実際に支払った金額の割合	93%	84%	90%	88%	85%	115%

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 = 1,097
注：「1,000 万ドル未満」のグループは、回答数が非常に少ないため、年間売上高の内訳から除外しています。

要求された身代金に対して実際に支払った金額の割合 (業界別)

業界別に見ると、身代金の減額交渉を最も行っている業界は、最初に要求された金額を支払った割合も最も低くなっています。また、減額交渉を最も行っていない業界は、最初に要求された金額を支払った割合が最も高くなっています。

100% 未満	100% 以上
製造 / 生産 (70%)	高等教育機関 (122%)
ビジネス / プロフェッショナルサービス (74%)	初等中等教育機関（115%）
金融サービス (75%)	ヘルスケア (111%)
その他 (79%)	州政府 / 地方自治体 (104%)
IT、通信、テクノロジー (82%)	中央 / 連邦政府 (103%)
小売 (84%)	エネルギー / 石油・ガス / 公共事業 (101%)
建設 / 不動産 (95%)	
流通 / 輸送 (95%)	
メディア / レジャー / エンターテイメント (95%)	

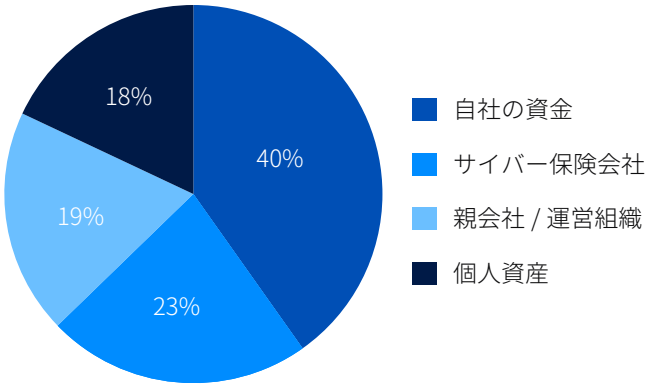
攻撃者から要求された身代金額はいくらでしたか？攻撃者に支払った身代金はいくらでしたか？ 回答者数 = 1,097

支払った身代金の出所

身代金を支払うための資金を誰が提供しているのかは、大きな関心事でしたが、今回の調査によって、多くの情報を収集できました。

- 身代金のための資金調達は共同作業であり、回答者の 5 分の 4 以上 (82%) が複数の資金源から調達していると報告している。
- 身代金の主な資金源は企業や組織本体であり、平均すると支払額の 40% を負担しています。企業の親会社や政府機関は通常 19% の資金を提供している。
- 保険会社は身代金の支払いに深く関わっている。
  - 身代金を支払うための資金の 23% は保険会社が拠出している。
  - 83% の攻撃で保険会社が身代金の支払いを支援している。
  - しかし、保険会社が身代金の全額を負担することは非常に稀であり (1%)、79% のケースで保険会社が負担したのは支払総額の半分以下である。

支払った身代金の出所



身代金の支払いに充てられた資金は、以下のどの資金源から提供されましたか？ 回答者数 = 1,168

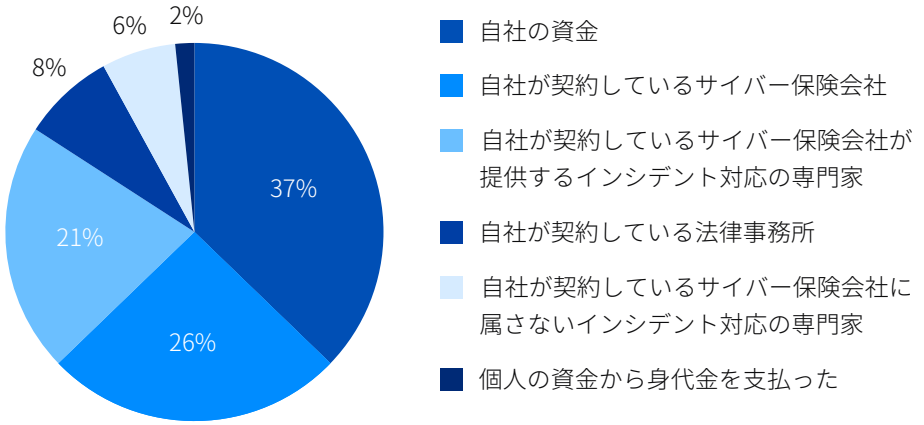
身代金取引の実行

身代金はいくつかの組織から拠出されることがありますが、通常、1 社から 1 回で送金されています。

世界全体では、保険会社が身代金支払いの約半数のケースで資金を直接 (26%) または指定されたインシデント対応の専門家 (21%) からを通じて送金しています。被害を受けた組織が支払うケースが 37%、被害を受けた組織の法律事務所が支払うケースが 8% でした。

全体の 28% のケース (四捨五入した値) は、保険会社 (21%) または他の当事者（通常は被害を受けた組織) (6%) によって指名されたインシデント対応の専門家によって行われています。

身代金送金の実施者



誰が身代金を支払いましたか？つまり、攻撃者の口座に送金したのは誰でしたか？ 回答者数 = 1,168

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。支払われた身代金を除くと、2024 年に組織が報告したランサムウェア攻撃の影響を復旧するための平均コストは 273 万ドルで、2023 年に報告された 182 万ドルから 100 万ドル近く増加しました。

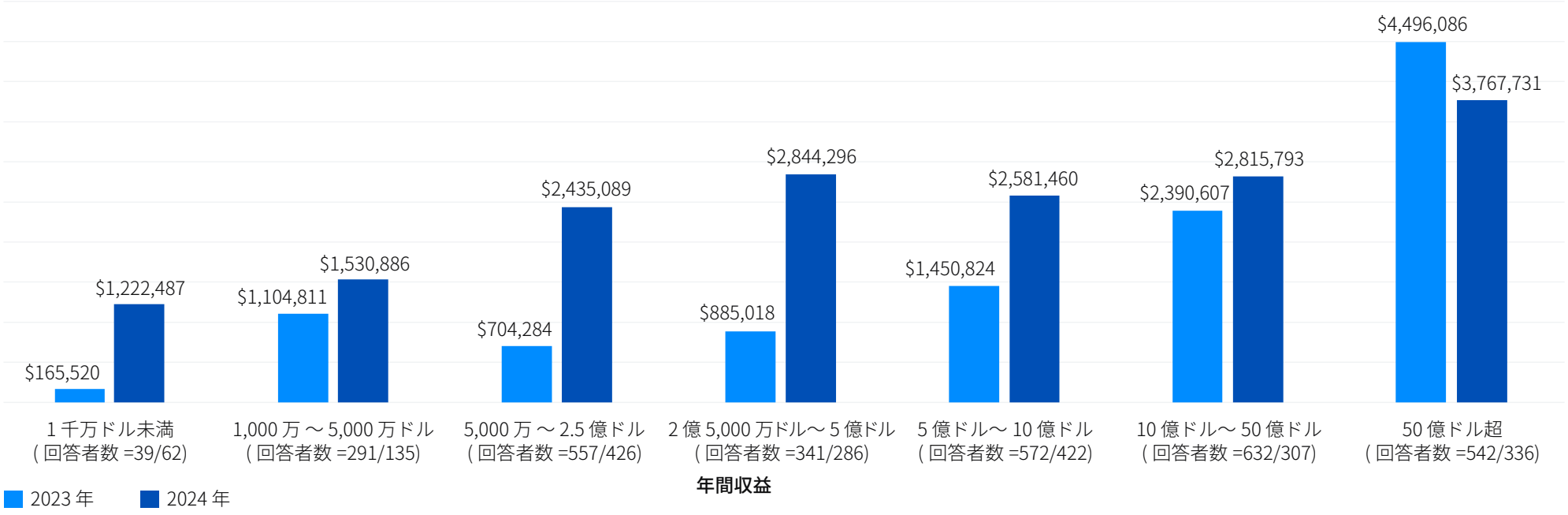
2021 年	2022 年	2023 年	2024 年
185 万ドル	140 万ドル	182 万ドル	273 万ドル

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) はどれぐらいですか？回答者数 = 2,974 社 (2024 年)、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。

全体的な復旧コストが最も増加したのは、売上高が低 / 中程度のグループです。2 億 5,000 万ドルから 5 億ドルのグループの復旧コストの増加額が最も大きくなり、200 万ドル (885,018 ドルから 2,885,296 ドル) も増加しています。

年間売上高が 10 億ドルから 50 億ドルの企業の復旧コストは、40 万ドル強の比較的小さな増加になりました。一方、年間売上高が 50 億ドル以上の規模が最も大きな組織では、復旧コストが唯一減少しており、4,496,096 ドルから 3,767,731 ドルに減少しました。

復旧コストの中央値を見ると、これらの傾向を確認できます。全体的には、復旧コストの中央値は昨年度の 37 万 5000 ドルから 75 万ドルに倍増しました。これらの増加の多くは売上高が低い 5 つのグループに集中しており、すべてのグループが大幅な復旧コストの増加を報告しています。一方で、売上高が大きな残りの 2 つグループは、復旧コストの変更はあまり見らませんでした。



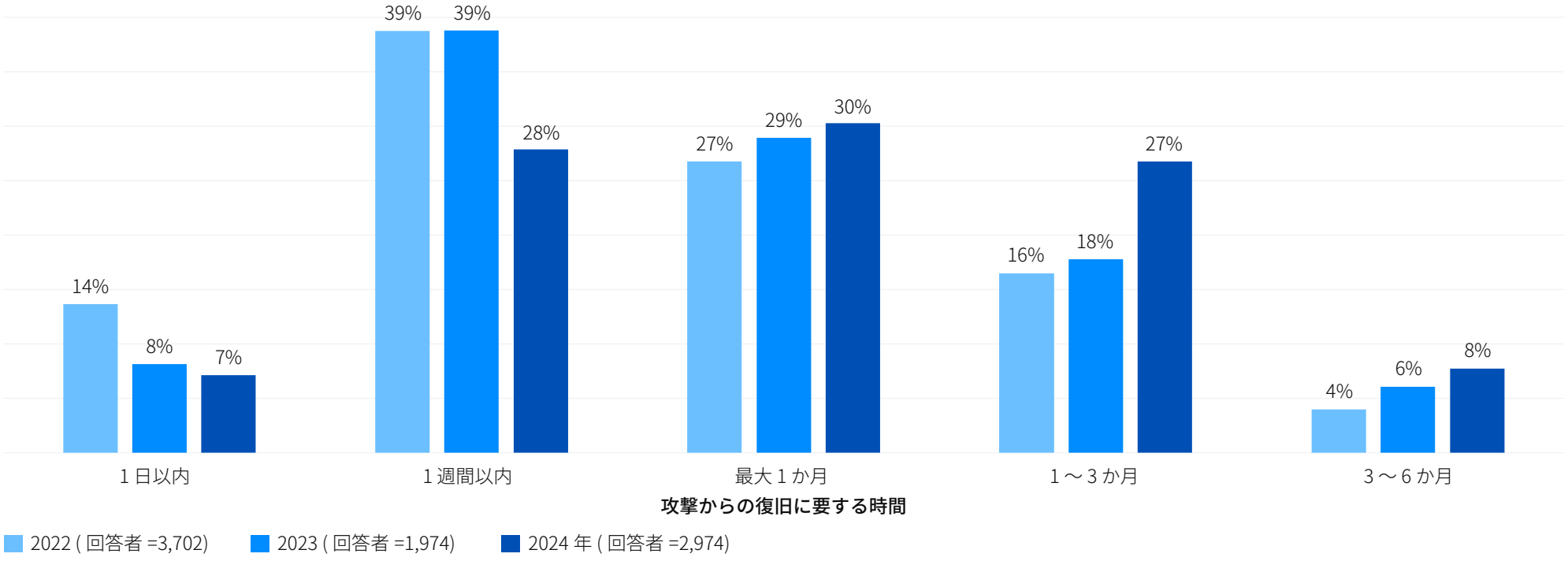
最も深刻なランサムウェア攻撃の影響において、組織が復旧に要した概算コスト (ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益など) はどれぐらいですか？
回答者数 = 2,974 社 (2024 年)、1,974 社 (2024 年)2024 年 /2023 年の売上別の回答者数を図内に記載。

復旧にかかる時間

ランサムウェア攻撃で受けた影響を復旧するのにかかる時間が長くなる傾向が継続しています。2024 年の調査では、以下が明らかになりました。

- 1 週間以内に完全に復旧できたのは、ランサムウェア攻撃の被害を受けた組織の 35% であり、2023 年の 47% および 2022 年の 52% から減少した。
- 3 分の 1 (34%) が復旧するまでに 1 か月以上を要しており、この数値は 2023 年の 24%、2022 年の 20% から増加した。

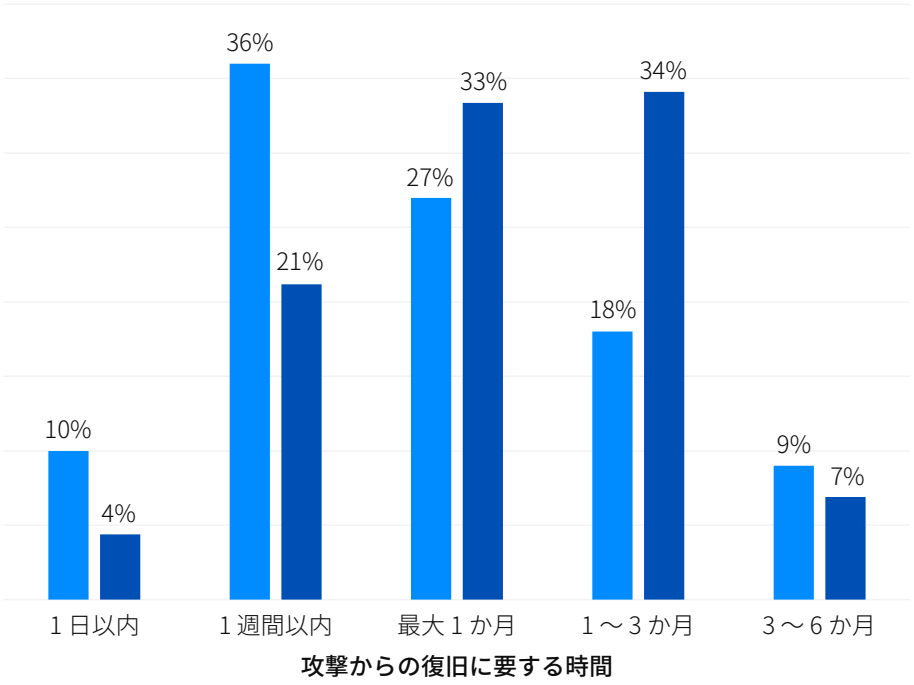
これらの数値が減少したのは、攻撃が複雑になり、影響が深刻化しており、より大規模な復旧作業が必要になったことを反映している可能性があります。また、復旧のための準備不足が深刻な問題になっている可能性もあります。



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？回答者数を図内に記載。

復旧にかかる時間：バックアップが侵害された場合の影響

バックアップが侵害された場合、全体的な復旧時間に大きな影響を与えます。バックアップが侵害されなかった組織のほぼ半数 (46%) が 1 週間以内に復旧しているのに対し、バックアップが侵害された組織では 1 週間以内に復旧している割合は 4 分の 1 (25%) になっています。バックアップが侵害されると、暗号化されたデータを復元する作業がさらに複雑化し、ランサムウェアに感染していない新しいバックアップを作成し、保護するための作業も必要となります。

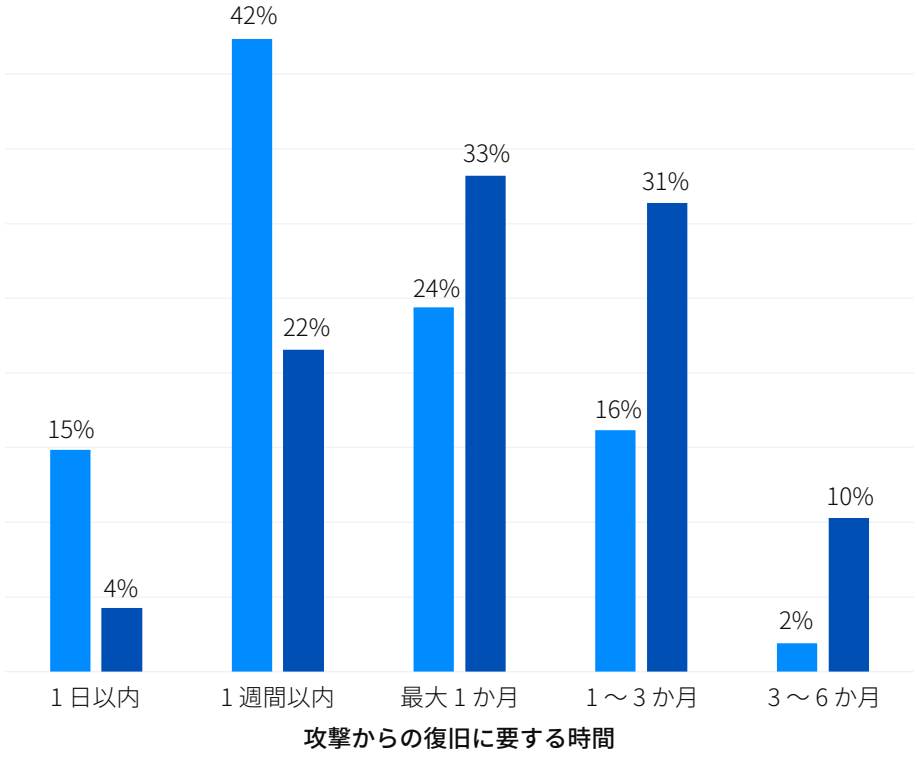


バックアップが侵害されていない場合 (回答者数 = 1,379)
バックアップが侵害された場合 (回答者数 = 1,595)

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。

復旧にかかる時間：データが暗号化された場合の影響

攻撃によってデータが暗号化されると、当然、復旧にかかる時間も大幅に増加します。データが暗号化されなかった組織の 57% が 1 週間以内に完全に復旧できたのに対し、データが暗号化された場合 25% の組織しか 1 週間以内に完全に復旧することはできませんでした。



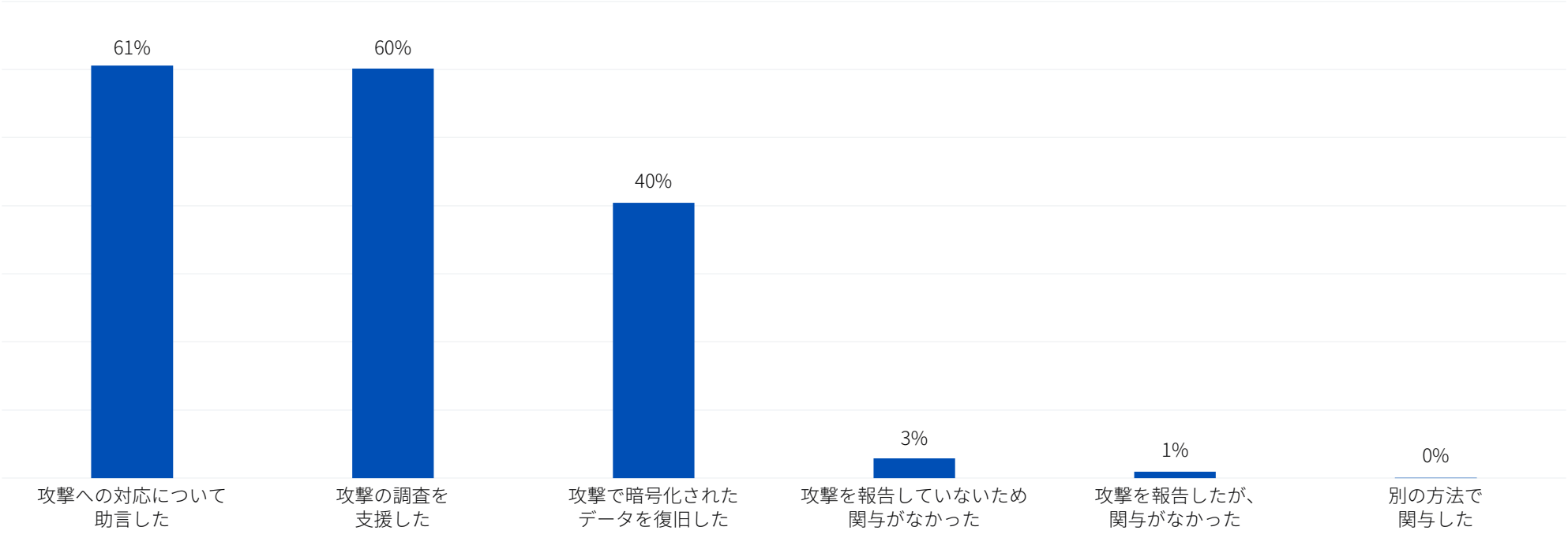
データが暗号化されていない場合 (回答者数 =902)
データが暗号化された場合 (回答者数 =2,072)

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。

法執行機関による関与

ランサムウェア攻撃に対して公的機関による支援を利用できるかどうかやその支援の内容は、サイバー攻撃を報告するツールと同様に、国ごとに異なります。たとえば、米国の被害者は、アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁 (CISA) から助言を受けることができ、英国の被害者は英国のサイバーセキュリティセンター (NCSC) から助言を得ることができます。また、オーストラリアの組織は、オーストラリアのサイバーセキュリティセンター (ACSC) に相談することができます。

ランサムウェア攻撃が常態化している中で、ランサムウェアの被害を受けた世界の組織の 97% が、攻撃について法執行機関や政府機関から何らかの支援を受けています。61% が攻撃への対処について助言を受けており、60% が攻撃の調査に関する支援を受け、40% が攻撃による影響を復旧するための支援を受けたと回答しました。

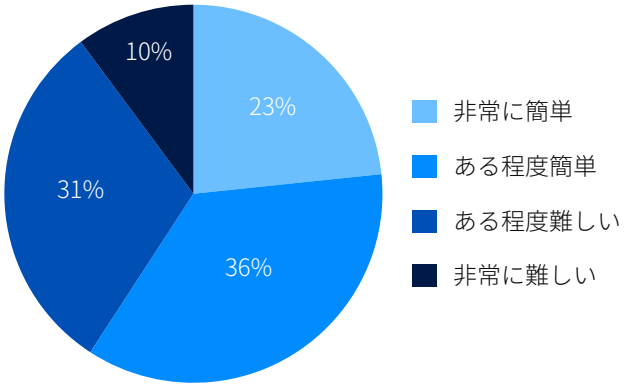


自社のインシデントに対する法執行機関や政府機関による関与

あなたの組織が法執行機関や政府機関に攻撃を報告したときに、それらの機関はどのように対応しましたか？

法執行機関や政府機関との連携のしやすさ

心強いことに、攻撃に関連して法執行機関や政府機関による支援を受けた組織の半数以上 (59%) が、これらの機関から簡単に支援を受けることができた (非常に簡単が 23%、ある程度簡単が 36%) と回答しています。支援のプロセスが非常に難しかったと回答した組織はわずか 10% であり、ある程度難しかったと回答した組織は 31% でした。



あなたの組織にとって、今回の攻撃について法執行機関や公的機関と連携して対応することは、容易でしたか、または困難でしたか？
回答者数 = 2,874 (「わからない」の回答を除く)

政府機関の不介入

3% (回答者数 86 人) の組織が攻撃を報告していませんが、その理由はさまざまであり、最も多かった理由は、「罰金、過料、追加の業務の発生など、組織に悪影響が及ぶことを懸念した (27%) 」と、「自社にとって利点がないと考えた」(同じく 27%) の 2 つでした。数人の回答者は、「社内で問題を解決できたため、政府機関に支援を求めなかった」と回答しました。

罰金、過料、追加の業務の増大などの負の影響が生じることを懸念した。	27%
攻撃を報告する利点があるとは考えられなかった。	27%
これらの機関が攻撃に関心があると考えなかった。	22%
攻撃への対応に追われており、これらの機関に関与してもらうことを考えなかった。	21%
攻撃者からこれらの機関に関わるなと警告された。	19%
報告すべき法執行機関や公的機関がわからなかった。	10%
攻撃を報告する法的な義務がなかった。	9%
その他 (具体的にご記入ください)	3%
わからない	1%

法執行機関や公的機関に報告しなかった理由は何ですか？ (n=86)。

まとめ

ランサムウェアは、世界各国のあらゆる規模の組織にとって依然として大きな脅威になっています。この 2 年間で、全体的な攻撃率は低下しましたが、攻撃による被害と影響は増大しました。サイバー攻撃者が繰り返され、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攻撃の進化に合わせていかなければなりません。

予防。ランサムウェア攻撃を受けても、侵入することができず被害が全く発生しなかったということが企業や組織にとって最も良い結果です。攻撃の 3 分の 1 は、パッチが適用されていない脆弱性が悪用されて始まっています。そのため、攻撃対象領域を適切に管理し、リスクの重大度に応じて適用するパッチの優先順位を付けることが重要です。認証情報の不正使用を制限するために多要素認証 (MFA) を使用することも、優先すべき対策です。フィッシングや悪意のあるメールを検出する方法について、ユーザーを継続的にトレーニングすることも不可欠であることに変わりはありません。

保護。エンドポイント、メール、ファイアウォールテクノロジーなどの基盤となる強力なセキュリティ機能は必須です。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、悪意のある暗号化を阻止してロールバックすることができる専用のランサムウェア対策を導入するなど、エンドポイントの防御を徹底する必要があります。最適な保護を実現するためには、セキュリティツールを正しく構成して展開しなければなりません。そのため、セキュリティ対策をシンプルかつ迅速に展開できるソリューションを探してください。複雑で導入が難しい保護機能は、リスクを軽減するどころか、むしろ増大させることにもなります。

検出と対応。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。バックアップを侵害されたり、データを暗号化されたりする前に、自社のネットワークに侵入したサイバー攻撃者を検出して、無力化することで、極めて優れた成果を上げることができます。

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。バックアップからデータを復元する訓練を定期的に実施し、攻撃の影響を受けている中で計画を実際に実行する必要が生じた場合でも、すばやく確実に計画を履行できるようにしてください。

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。

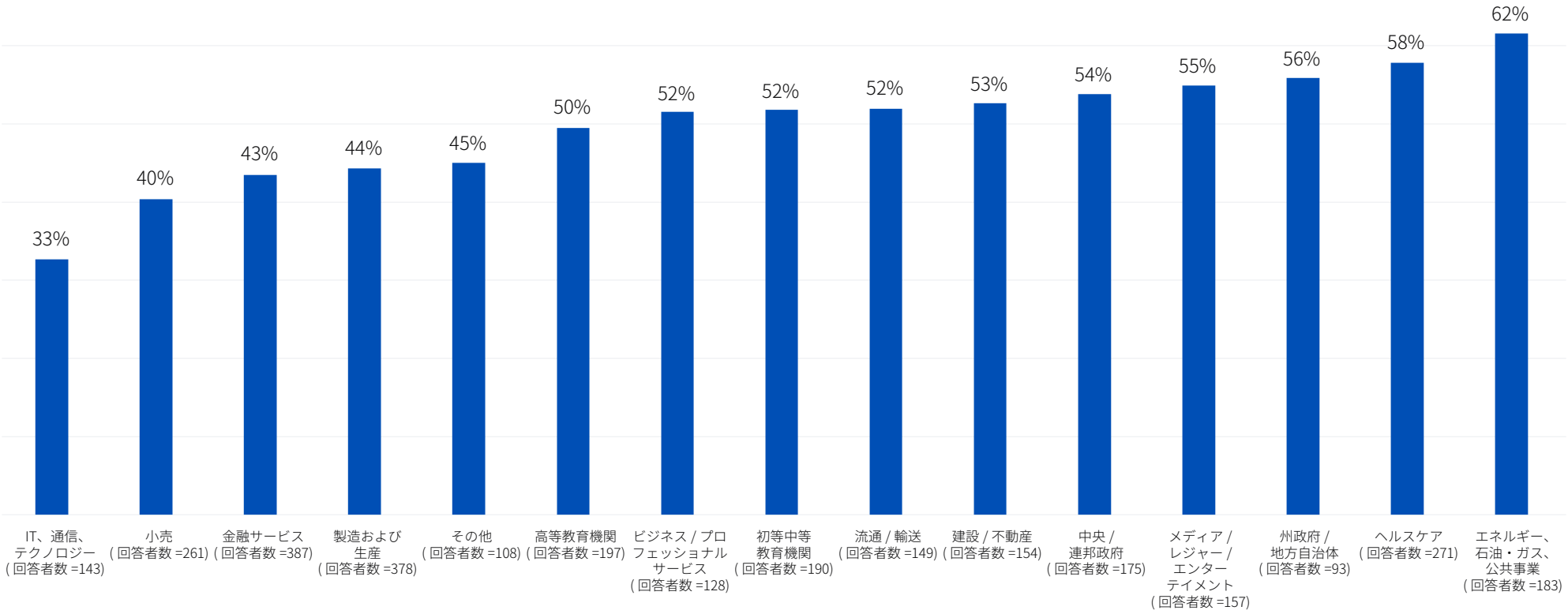
Vanson Bourne について

Vanson Bourne は、テクノロジー業界の市場調査を専門とする独立系の調査会社です。堅牢で信頼性の高い調査を元にした分析を実施しているため同社の評判は高く、厳密な調査方法とあらゆる業種と市場における技術および業務部門の上級意思決定者の意見を広く収集する能力が同社の基盤になっています。詳細は、www.vansonbourne.com を参照してください。

付録

影響を受けたコンピュータの割合 (業界別)

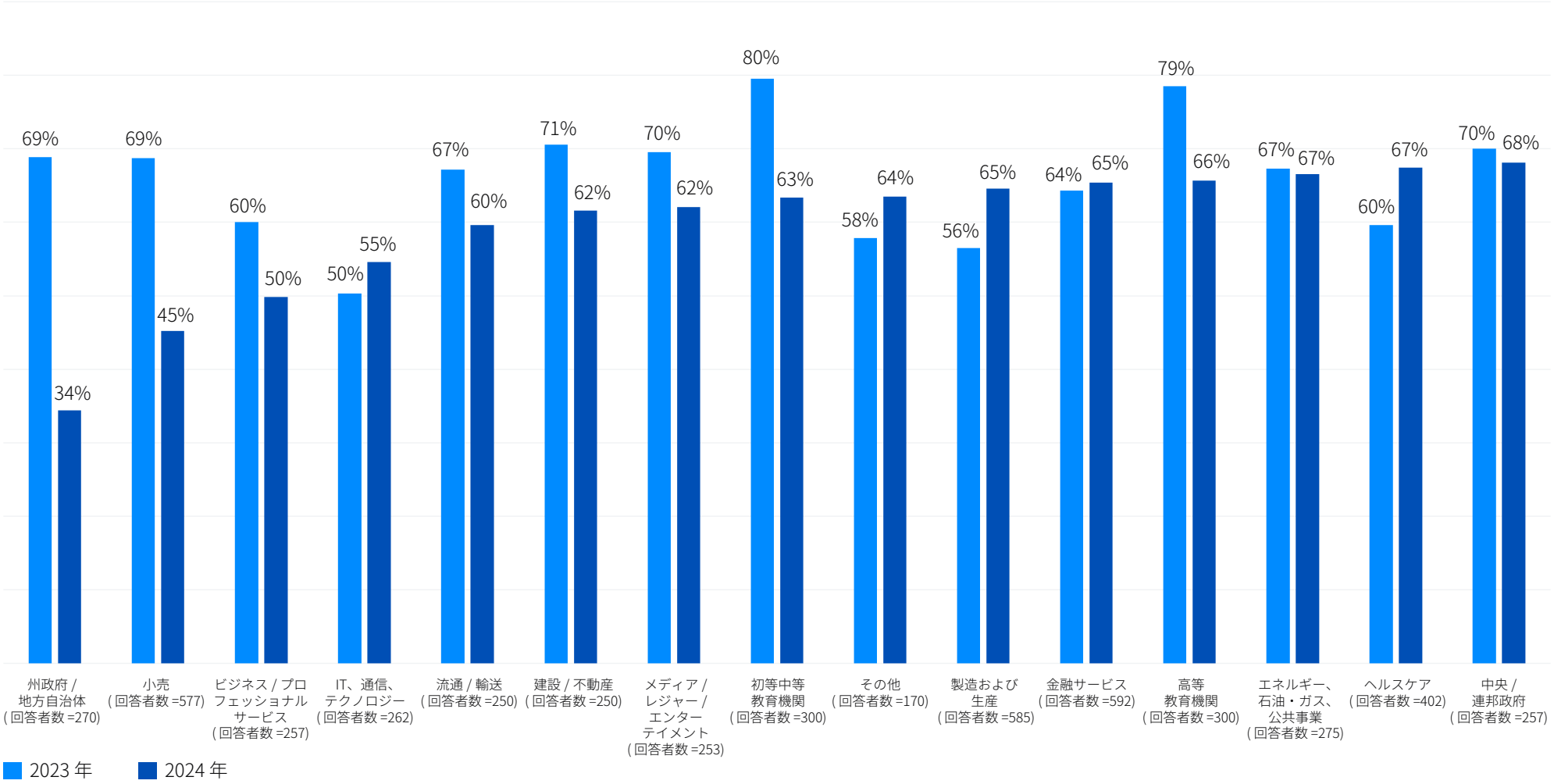
影響を受けたデバイスの割合



過去 1 年間にランサムウェア攻撃の影響を受けた組織のコンピュータの割合は？ 回答者数 = 2,974 (ランサムウェア攻撃を受けた組織の数) 業界別の回答者数を図内に記載

業界別のランサムウェア攻撃を受けた割合

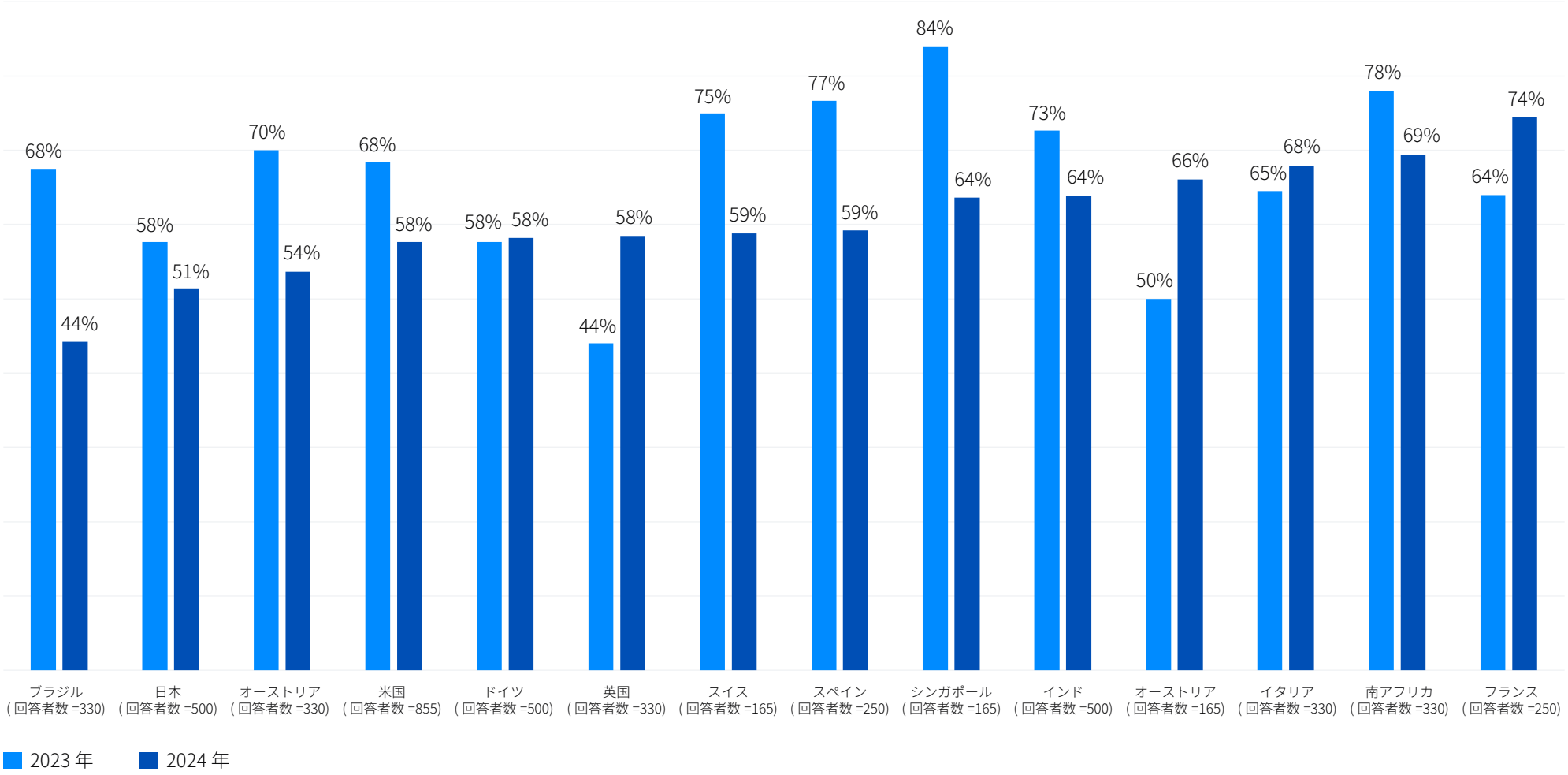
昨年ランサムウェア攻撃を受けた組織の割合



過去 1 年間にランサムウェア攻撃を受けましたか？はい。回答者数 = 5,000 (2004 年)、3,000 (2023 年)、5,600 (2022 年)2024 年の業界別の回答者数を図内に記載

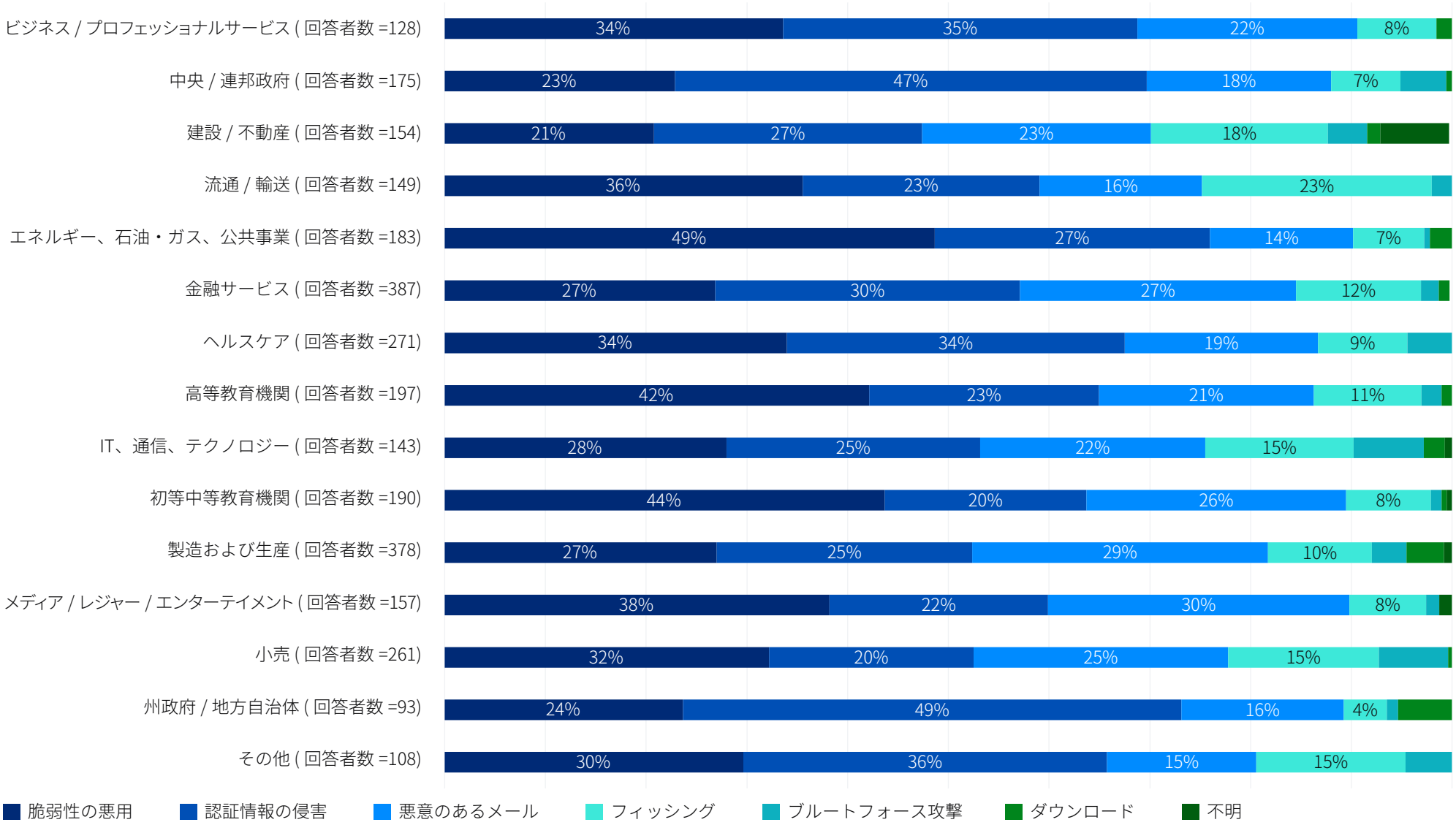
ランサムウェア攻撃を受けた割合 (国別)

昨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？はい。回答者数 = 5,000 (2024 年)、回答者数 = 3,000 (2023 年)2024 年の国別の回答者数を図内に記載

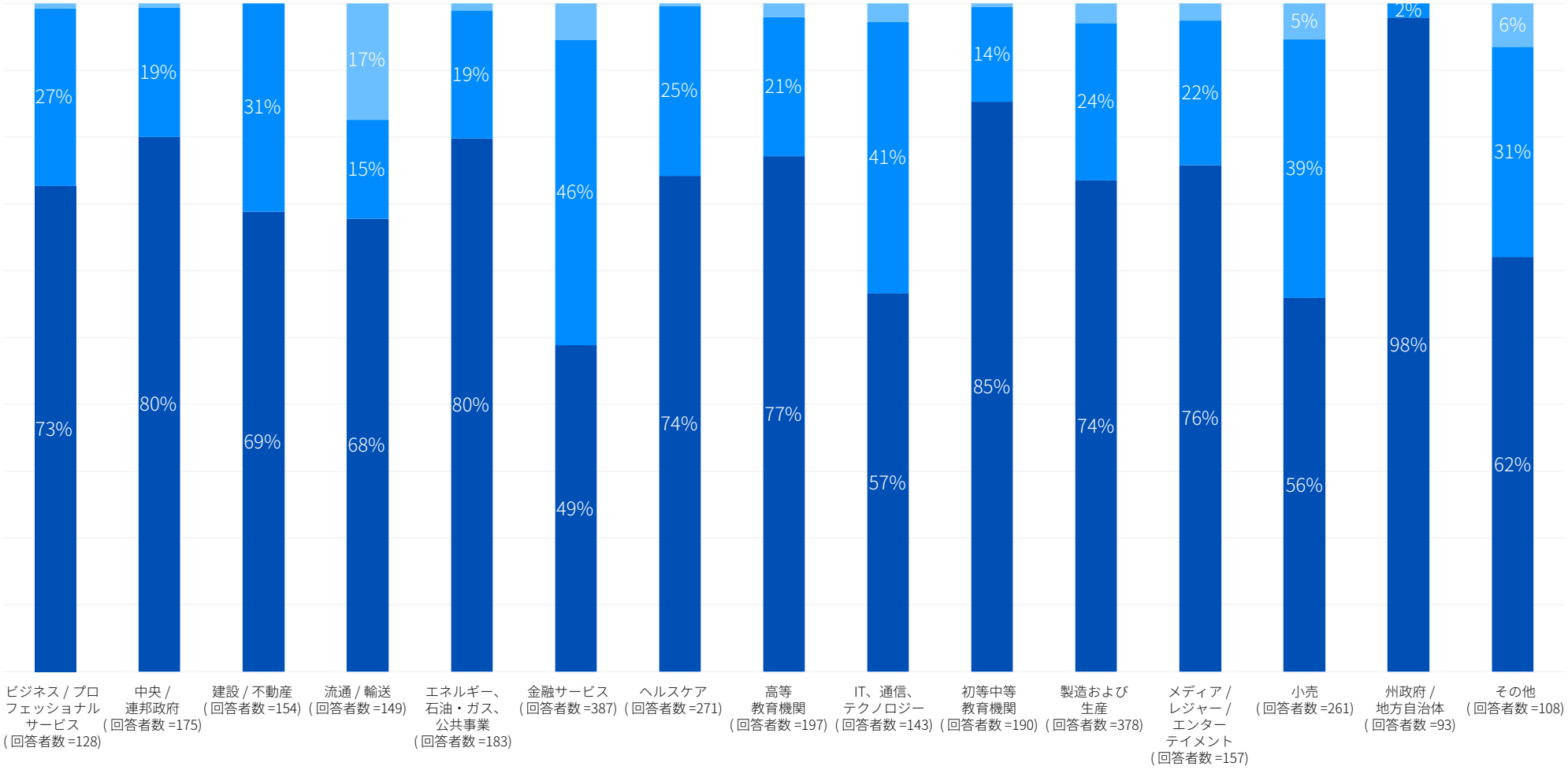
業界別の攻撃の根本原因



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？ 回答者数 =2,974 (ランサムウェア攻撃を受けた組織).

データ暗号化率 (業界別)

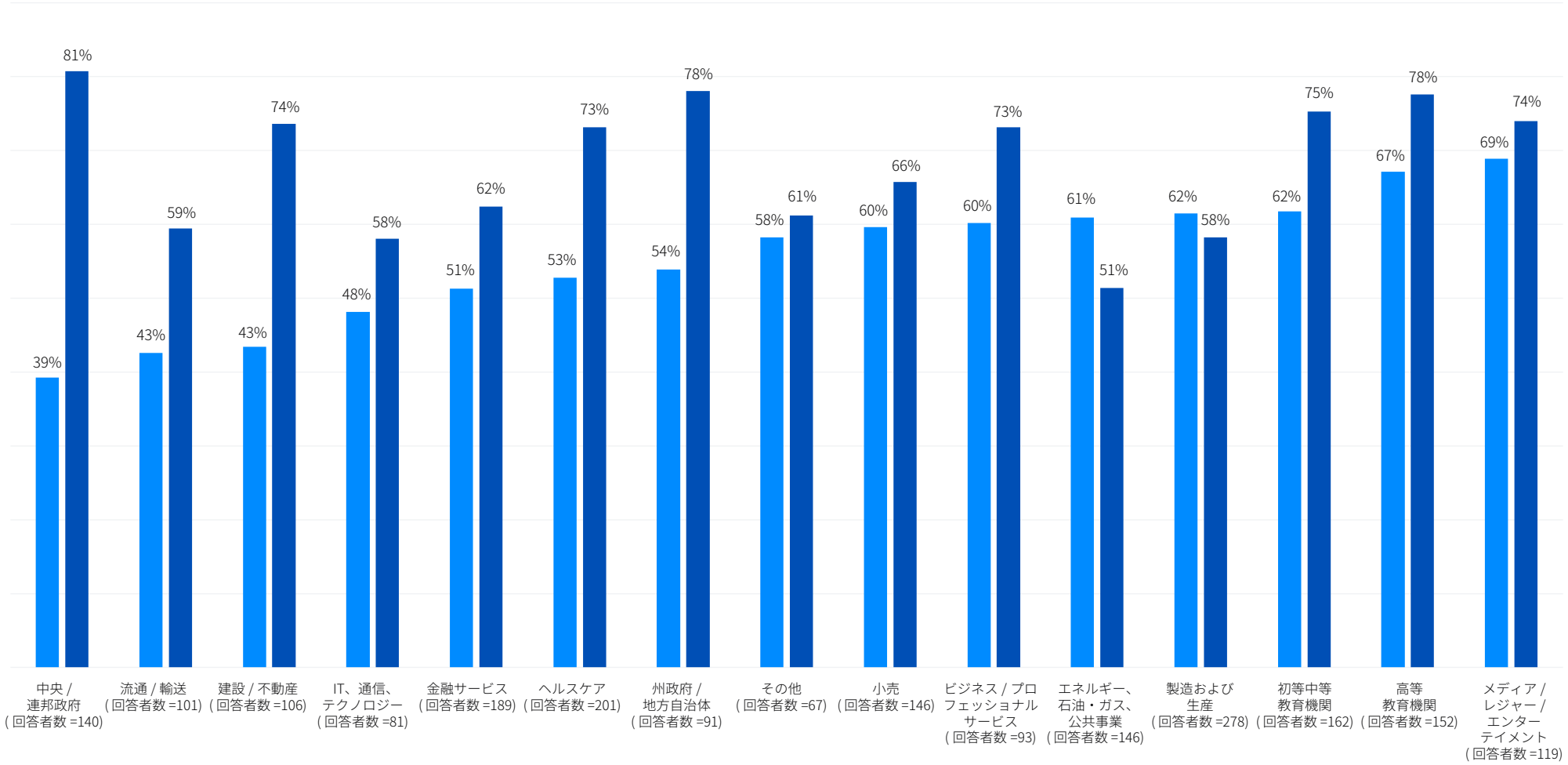
攻撃によってデータが暗号化された割合



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。

データの復元方法 (業界別)

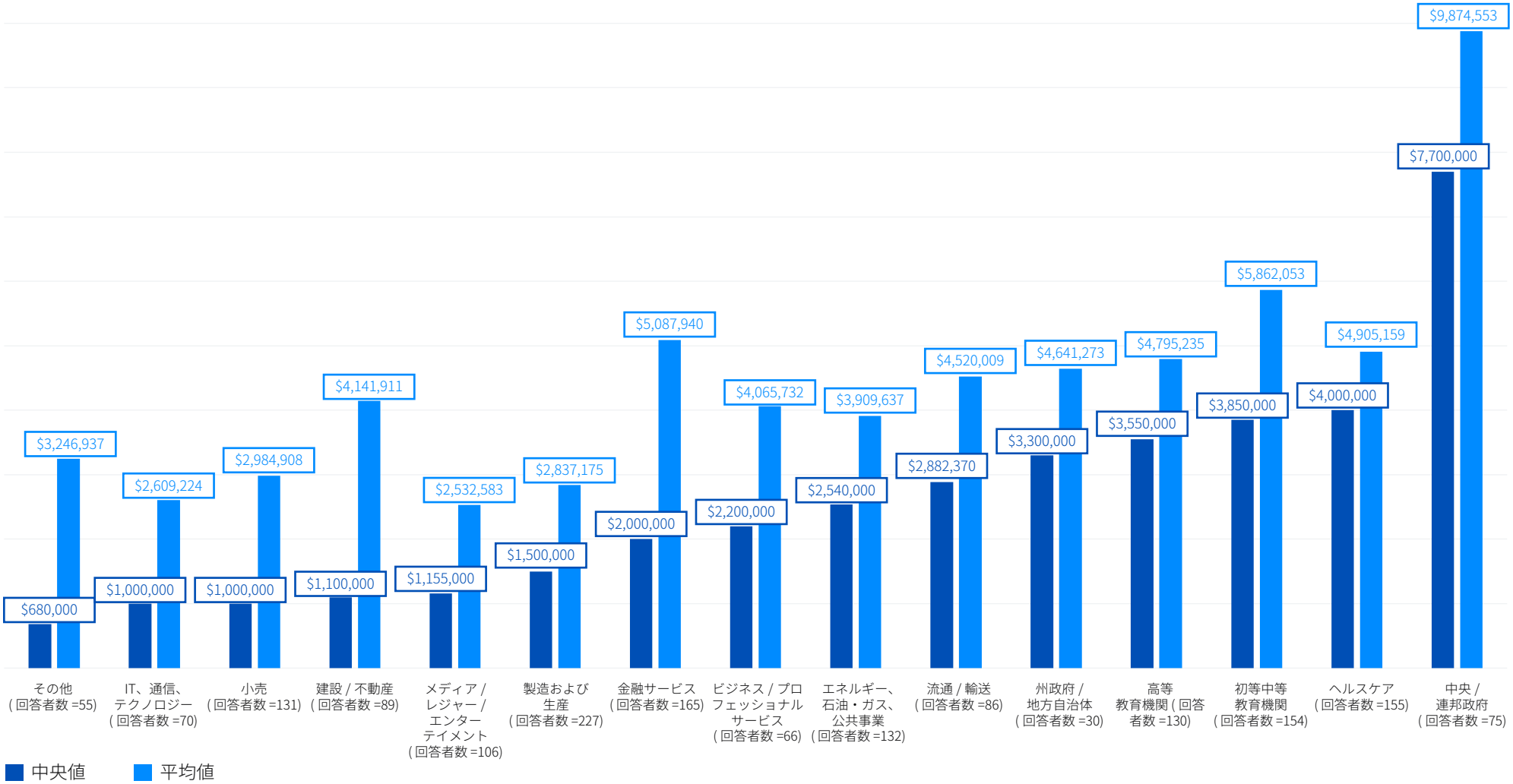
バックアップを使用し、身代金を支払ってデータを復元した頻度



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。身代金の支払いに応じる傾向の順番に表示

要求された身代金額 (業界別)

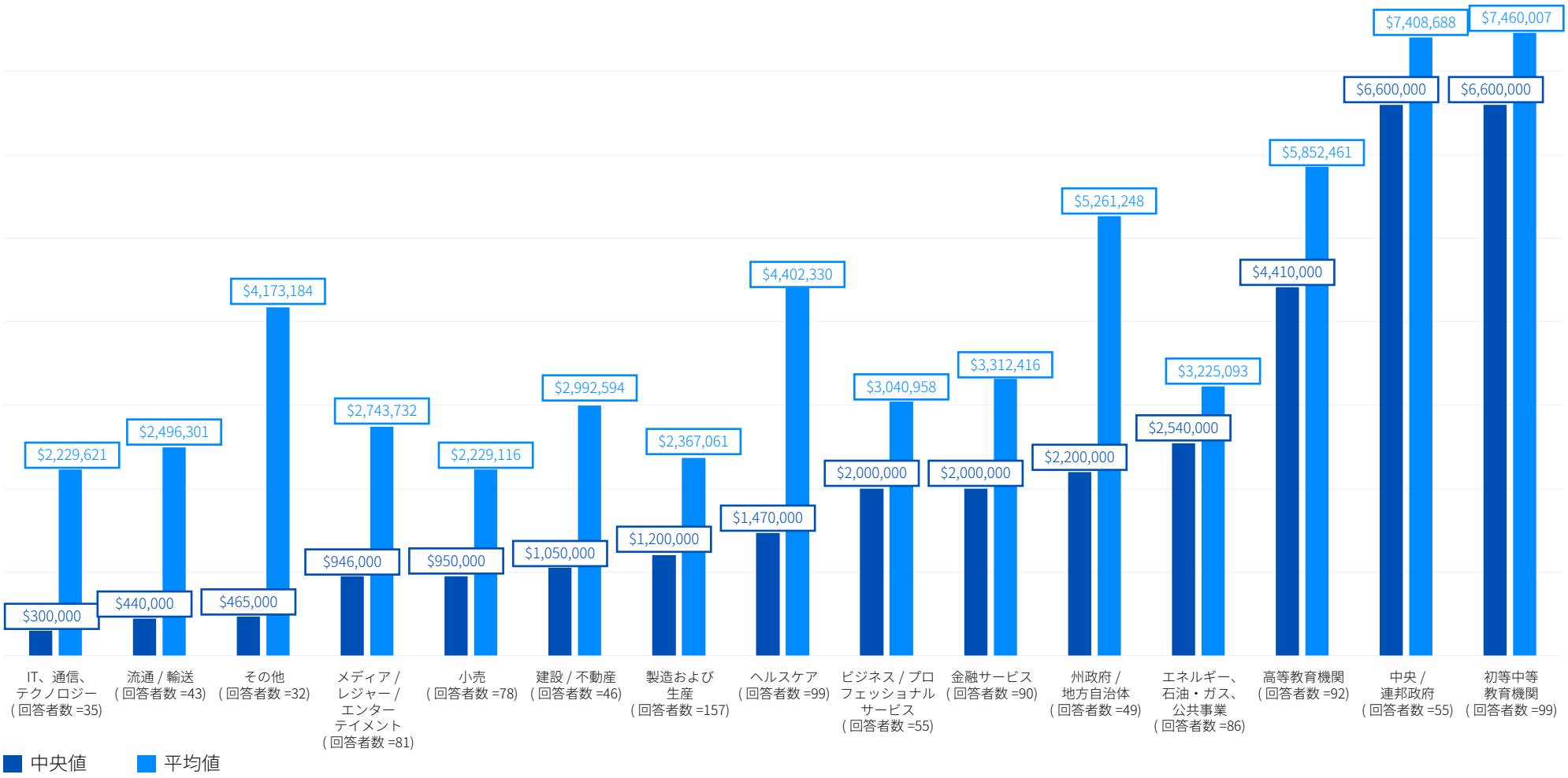
身代金を要求



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。要求された金額の中央値順。

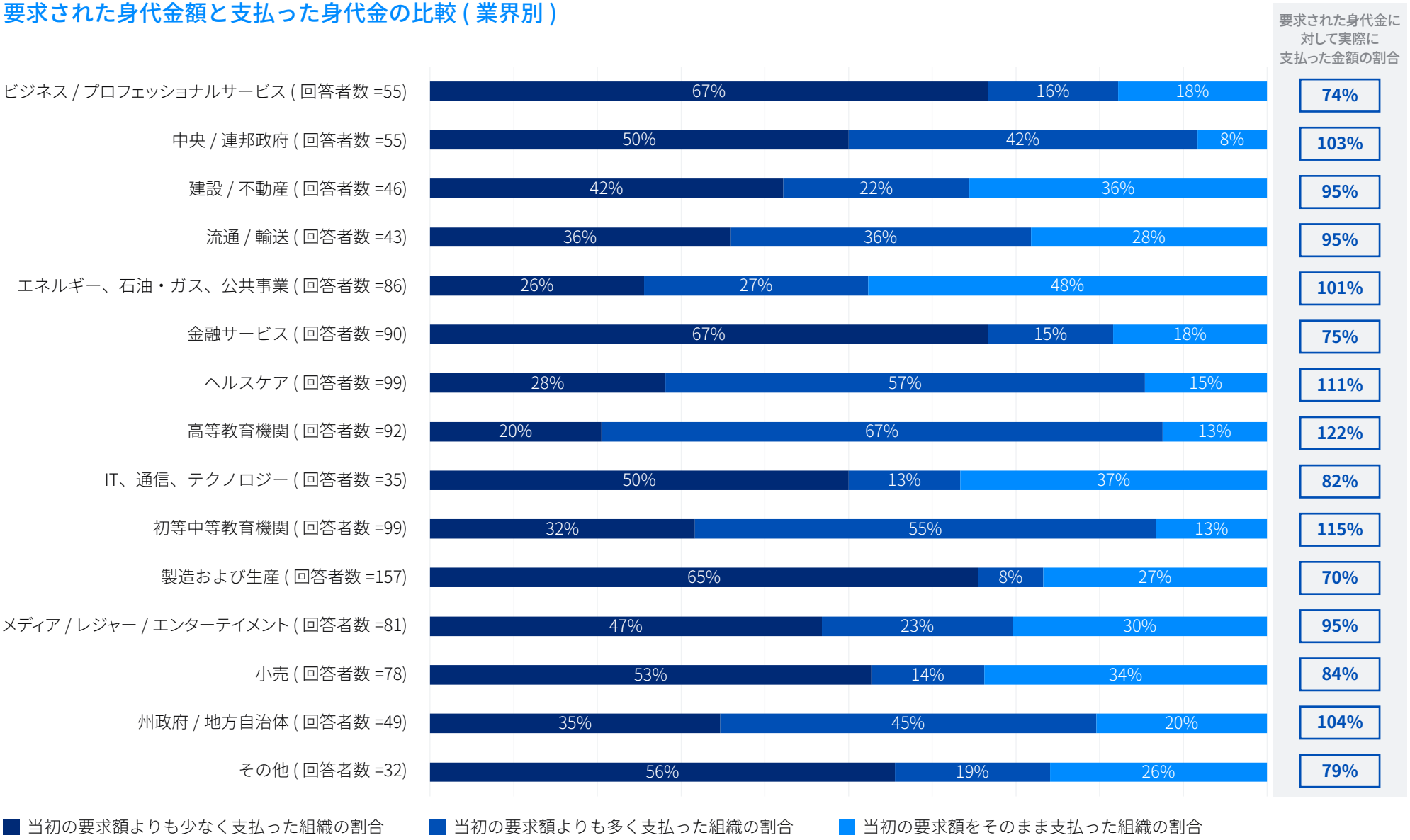
身代金の支払額 (業界別)

身代金の支払額



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。支払額データ (中央値順)。

要求された身代金額と支払った身代金の比較 (業界別)



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？回答者数を図内に記載。

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。

2024-04-16 (WP-PC)