SOPHOS

医療業界のランサムウェアの現状 2023年版

2023年の 1～3月に、14カ国の IT/サイバーセキュリティ担当者 3,000 人 (うち医療業界が 233人) を対象に実施した、ベンダー不問の独自調査の結果と考察を紹介します。

ソフォス ホワイトペーパー2023年 8月

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、医療業界が直面している現状を明らかにしました。調査では、攻撃の主な原因や、ランサムウェアによるこの業界への影響の違いについて探っています。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

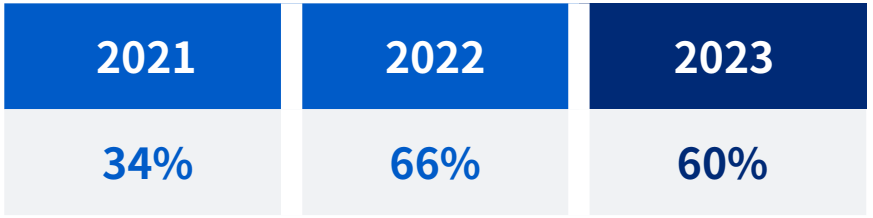
ソフォスは、北米/中南米、EMEA、アジア太平洋地域の計 14カ国で、従業員数 100～5,000 人の企業の IT/サイバーセキュリティ部門担当者 3000人 (うち医療業界が 233人) を対象とする調査を、独立した調査会社に依頼しました。調査は 2023 年 1 月から 3 月にかけて実施され、過去 1 年間の体験に基づいて回答してもらいました。

医療業界におけるランサムウェア攻撃の被害率

2023年の調査によると、医療業界におけるランサムウェア攻撃の割合が 前年比 66% から 60% に減少していることが明らかになりました。減少傾向にあるものの、2023年で報告を受けた攻撃率は、2021年の調査で報告されたランサムウェアの被害を受けた医療機関 34% と比較するとほぼ 2倍となっています。

この業界では攻撃頻度は減少してはいますが、昨年、医療業界のほぼ 3分の 2 がランサムウェアの被害を受けており、攻撃者が一貫して大規模な攻撃を実行できるのは明らかであり、ランサムウェアは今日の医療業界が直面する最大のサイバーリスクとなっています。

サイバー犯罪の世界では何年も前に RaaS（Ransomware as a Service）モデルが生み出され、その後、進化し続けています。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。



過去 1 年間にランサムウェア攻撃を受けましたか？はい。回答企業数 = 233 (2023 年)、381 (2022 年)、328 (2021 年)

医療業界でのランサムウェア攻撃率の減少とは対照的に、世界的な業界の傾向は横ばいのままです。2023年と 2022年の両方の調査で、全回答者の 66% が前年にランサムウェアの被害を受けたと報告しました。

業界全体で、最も被害率が高いのは教育関連で、初等中等教育機関で 80%、高等教育機関で 79% にのぼることがわかりました。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が強化されていることを示しています。

医療業界におけるランサムウェア攻撃の原因

医療業界で最も大きな影響を与えるランサムウェア攻撃の主な原因は、認証情報の侵害 (32%) であり、続いて脆弱性を悪用 (29%) でした。医療機関における攻撃の3分の 1以上 (36%) はメールベースの攻撃 (悪意のあるメールまたはフィッシング) が起点であり、これは部門全体の平均である 30% を上回っています。

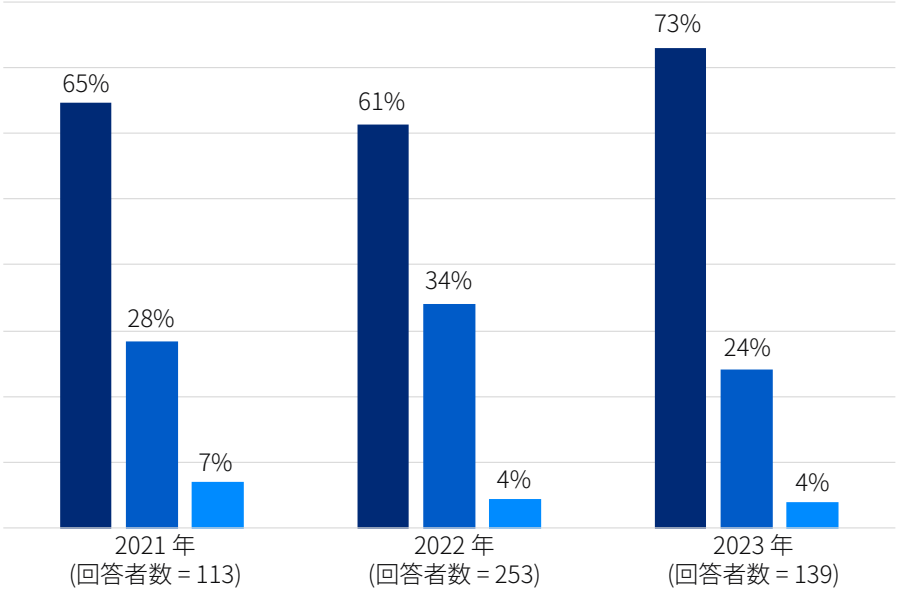
世界的に、業界間レベルでは、上位 2つの根本原因の順序が入れ替わり、脆弱性の悪用が最も一般的な根本原因 (攻撃の 36% で使用) で、次に認証情報の侵害 (攻撃の 29%) となっています。

	医療機関 (回答数=139)	全業界の平均 (回答数=1,974)
脆弱性の悪用	29%	36%
認証情報の侵害	32%	29%
悪意のあるメール	22%	18%
Phishing	14%	13%
ブルートフォース攻撃	1%	3%
ダウンロード	1%	1%

医療機関におけるデータの暗号化率

医療業界でのデータ暗号化率は、過去 3年間のレポートで最も高く、医療機関のほぼ 4分の 3 (73%) がデータが暗号化されたと報告しており、2021年のレポートの 65%、2022年のレポートの 61% から増加しています。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。

医療業界における恐喝のみの攻撃の割合は横ばいの 4% で、2021年の調査で報告された 7% を下回っています。



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

医療業界が報告するデータ暗号化の割合は高いですが、攻撃の 76% がデータ暗号化につながっている業界全体の平均を下回っています。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。

医療業界における攻撃の 3 分の 1 以上 (37%) では、データが暗号化されており、データも盗まれていました。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。

37%
ランサムウェアによってデータが暗号化された
医療業界のうち、盗難被害にもあった企業の割合

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、暗号化された / はい、暗号化されたうえに、データが盗まれた (回答数 = 101/37)

医療業界におけるデータの復旧率

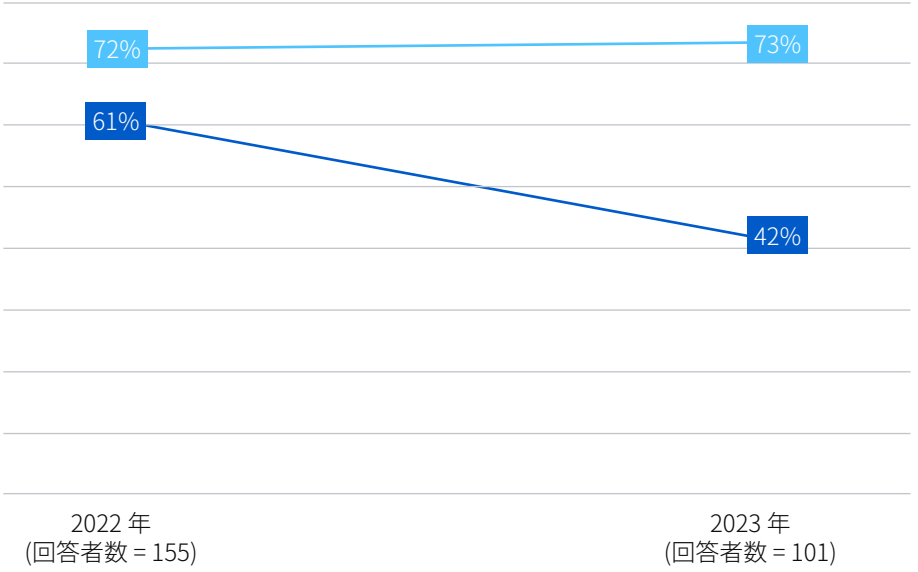
幸いなことに、データを暗号化していたすべての医療機関がデータを取り戻し、業界全体の平均である 97% を上回っています。

データを暗号化している医療機関の 73% がバックアップを使用してデータを復元しており、2022年の調査で報告された 72% からわずかに増加しています。注目すべき点は、暗号化されたデータを復旧するために身代金を支払う傾向が低下していることです。医療機関の回答者の 42% が、データを復旧するために身代金を支払ったと報告しており、昨年のレポートの 61% から減少しています。 なお、データを復旧した企業のうち 17% が、複数の方法を使用したと回答しています。

	医療機関	全業界の平均
データを復旧した	100%	97%
バックアップを使用してデータを復元した	73%	70%
身代金を支払ってデータを取り戻した	42%	46%
その他の方法でデータを復旧した	2%	2%

データを復旧できましたか？はい、バックアップを使用してデータを復元しました / はい、身代金を支払ってデータを取り戻しました / はい、その他の方法でデータを復旧しました。回答数 = 1,497 (全業界); 回答数 = 101 (医療業界)。

医療業界における身代金の支払い率は、前年比で大幅に低下しただけでなく、業界全体の平均である 46% を下回っています。世界的に、身代金の支払い率は前年と比べて横ばいで、バックアップの使用率は、2022年の調査では 73% から 2023年の報告書では 70% に低下しました。



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

保険への加入が身代金の支払い傾向に与える影響

医療業界全体のデータ復旧率は 100% でしたが、データ復旧に使用する方法は保険の適用範囲によって異なりました。スタンドアロンの保険契約を結んでいる組織は、より広範な保険の適用範囲の一部としてサイバー保険を使用している組織よりも、身代金を支払う傾向が高いと報告しています。

データを暗号化し、スタンドアロンのサイバー保険契約を持っている医療業界の半数以上 (53%) が身代金を支払いました。これは、サイバー保険を含んだより広範な保険契約を持つ組織では 34% に低下しました。

医療業界における身代金の支払いに対する保険の影響

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
53%	**34%**
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

データを復旧できましたか？という質問に対し、「はい、身代金を支払ってデータを取り戻しました」と回答した企業の割合。回答者数=101 (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と回答した医療組織。そのうち、45社がスタンドアロン型のサイバー保険に、53社がパッケージ型のサイバー保険に加入。10社はサイバー保険に未加入)

身代金の支払い

世界的な業界間のレベルでは、身代金を支払う全体的な傾向は昨年の調査と同じですが、支払い自体は大幅に増加しており、平均身代金の支払い額は前年比で812,360 ドルから 1,542,330 ドルへとほぼ 2倍となっています。身代金の支払いの中央値は、前年比で 76,500 ドルから 400,000 ドルに増加しました。

医療業界の場合、12の医療機関が支払われた正確な身代金額を共有し、中央値は2022年の 30,000 ドルから 2,500,000 ドルに増加しました。

9つの医療機関が 1,000,000 ドル以上の身代金を支払ったと報告し、100,000 ドル未満の身代金を支払ったのは 1つだけでした。調査のサンプル数が低いということは、2023年のレポートのデータが統計的に有意でないことを意味するため、あくまでも参考値として考える必要があります。この調査結果は、医療業界における身代金の支払いが増加していることを示しています。

	2022	2023
全業界の平均	$812,360 (平均値) $76,500 (中央値)	$1,542,330 (平均値) $400,000 (中央値)
医療機関	$196,749 (平均値) $30,000 (中央値)	$2,884,167 (平均値) $2,500,000 (中央値)

攻撃者に支払った身代金はいくらでしたか?「わからない」と外れ値は除外。全業界: 回答数=216 (2023)/ 965 (2022); 医療業界: 回答数=12 (2023)/ 83 (2022)。

* 2023年の医療業界の研究数値は少ないため、この結果はあくまで参考値としてお考えください。

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。業界全体で、支払われた身代金を除くと、ランサムウェア攻撃から復旧するための推定平均コストが182万ドルとなっています。これは、2022年のレポートの数値 (身代金の支払いを含む) の140万ドルに比べると増加しており、2021年の調査の身代金を含んだ185万ドルとほぼ同じです。

世界的な傾向に沿って、医療機関の復旧コストは前年比で185万ドルから220万ドルに増加し、2021年の調査で業界が報告した127万ドルのほぼ2倍になっています。今年の医療業界の復旧コストの増加は、ランサムウェア攻撃におけるデータ暗号化の頻度の増加の影響を受けている可能性があります。

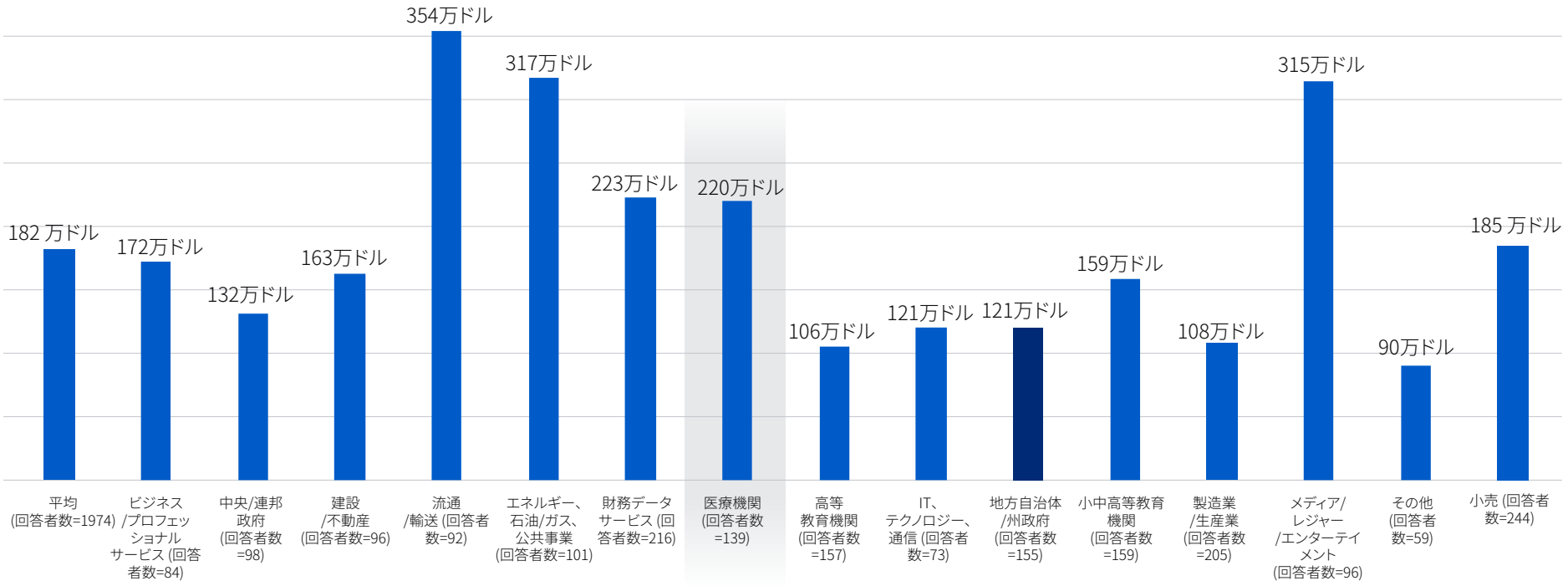
	2021	2022	2023
全業界の平均	185万ドル	140万ドル	182万ドル
医療機関	127万ドル	185万ドル	220万ドル

最も深刻なランサムウェア攻撃の被害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？全業界: 回答数=1,974 (2023)/ 3,702 (2022)/ 2,006 (2021); 医療業界: 回答数=139 (2023)/ 253 (2022)/ 113 (2021)

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

医療業界の復旧コストは、業界間全体の平均の182万ドルより上回っています。流通/輸送業が最も高い復旧コスト (354万ドル) を支払っており、これは世界平均のほぼ2倍に相当します。

最も深刻なランサムウェア攻撃からの復旧コスト (ドル)



最も深刻なランサムウェア攻撃の被害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

調査では、身代金を支払うよりも、バックアップを使用して暗号化されたデータを復旧する方が安価であることが確認されています。

復旧コストの全業界の中央値は、バックアップを使用した場合が 375,000ドルで、身代金を支払った場合の 750,000 ドルの半分となっています。同様に、復旧コストの平均値も、身代金を支払った場合と比較して、バックアップを使用した場合の方が 100 万ドル近く低くなります。

医療業界でも同様の傾向が見られ、バックアップを使用した場合の平均復旧コスト (211万ドル) は、身代金を支払った場合の請求額 (258万ドル) よりも低い額でした。

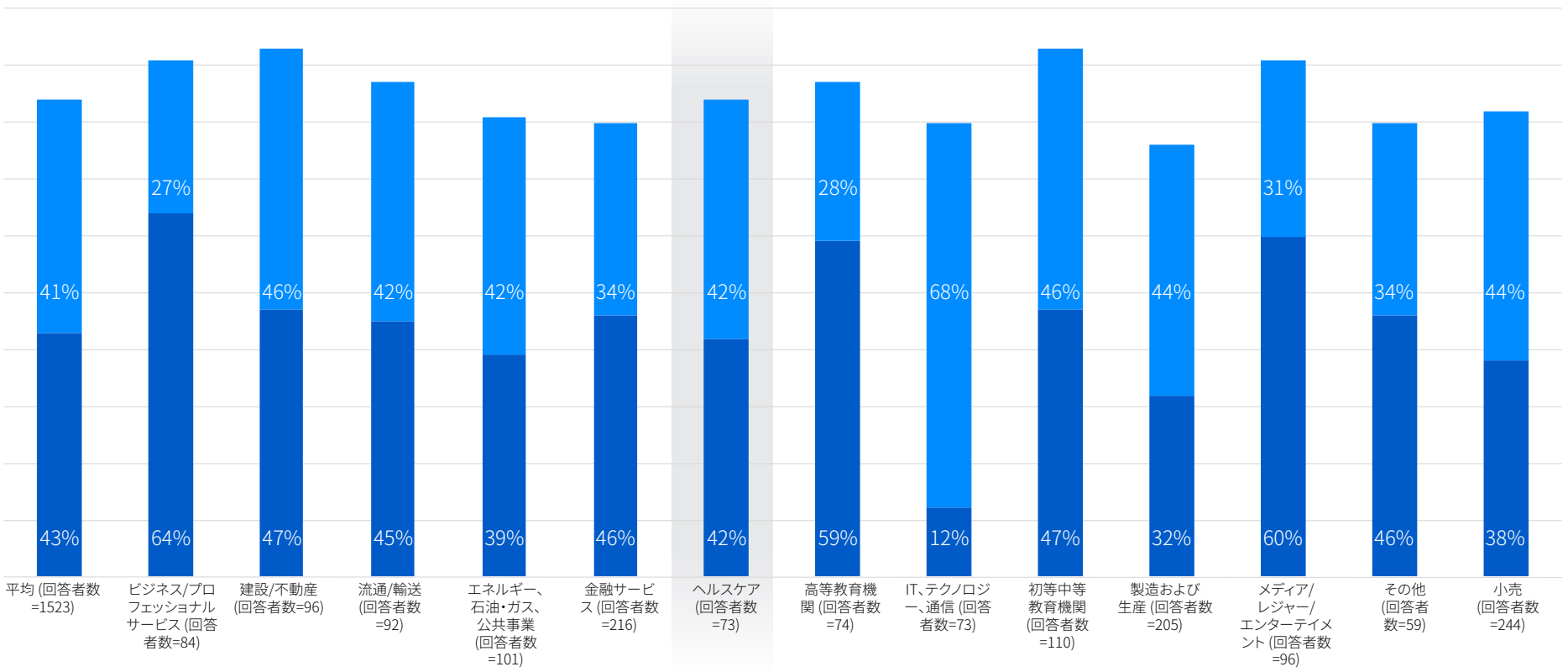
	身代金を支払ってデータを取り戻した	バックアップを使用してデータを復元した
全業界の平均	**$750,000** 中央値 **$2,600,000** 平均値	**$375,000** 中央値 **$1,620,000** 平均値
医療機関	**$750,000** 中央値 **$2,580,000** 平均値	**$750,000** 中央値 **$2,110,000** 平均値

最も深刻なランサムウェア攻撃の被害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？業界全体: 回答者数=694 (身代金を支払ってデータを取り戻した) 回答者数=1,053 (バックアップを使用してデータを復元した)

医療業界: 回答者数=42 (身代金を支払ってデータを取り戻した) 回答者数=74 (バックアップを使用してデータを復元した)

ビジネスへの影響

ランサムウェアの被害を受けた民間医療機関の 85% が、攻撃によりビジネスや収益が失われたと回答しており、これは全業界間の平均である 84% をわずかに上回っています。初等中等教育機関 (94%) と建設/不動産業界 (93%) は、ビジネス/収益の一部を失った可能性が最も高い一方、ビジネスおよびプロフェッショナルサービス業界は、多くのビジネス/収益を失ったと報告した割合 (64%) が最も高くなっていました。逆に、IT、テクノロジー、通信業界では対策が進んでおり、多くのビジネス/収益を失ったと報告した割合はわずか 12% でした。

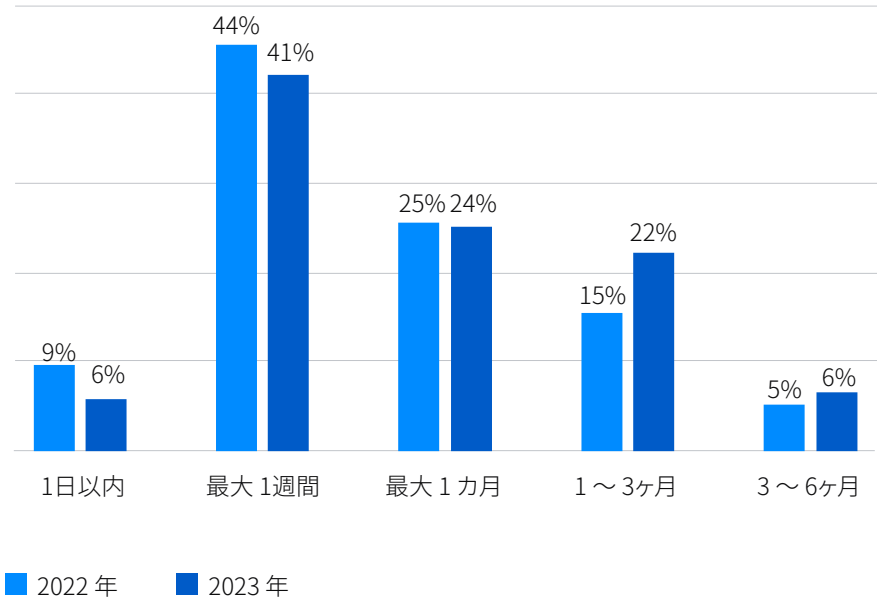


多少の事業の損失/減収があった　多くの事業の損失/減収があった

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

医療機関がランサムウェア攻撃から復旧するまでに時間がかかっており、2022年のレポートでは 54% だったのに対し、現在では 47% が 1週間以内に復旧しています。さらに、復旧に 1カ月以上かかった組織の割合は、前年比 20% (四捨五入) から 28% (四捨五入) に増加しています。



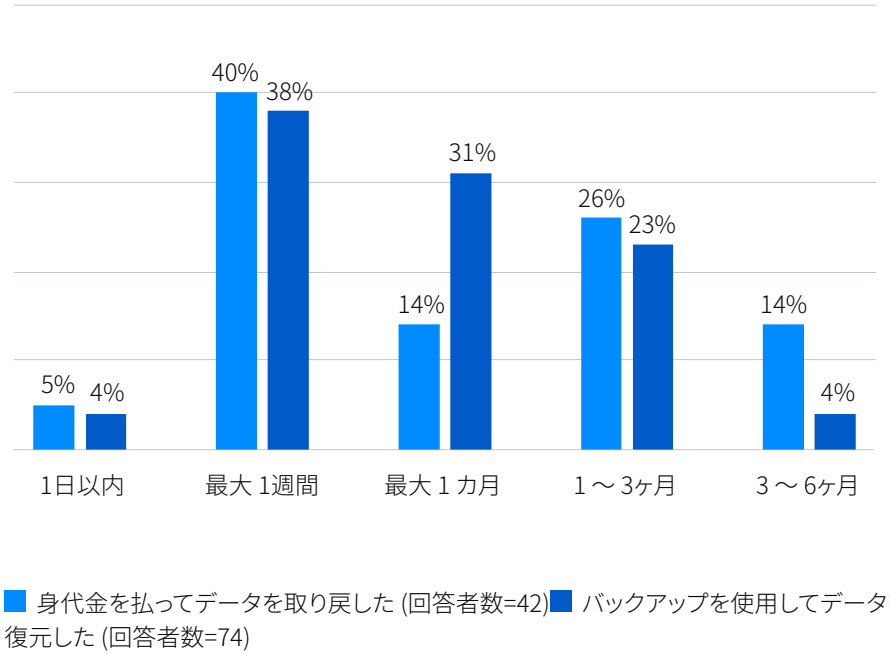
ランサムウェア攻撃から完全に復旧するのに、どのくらいの時間がかかりましたか？
139社 (2023年) /253社 (2022年) ランサムウェアに攻撃された医療組織の数

データ復元方法別の復旧時間

データ復旧方法ごとの復旧時間の違いを調べたところ、医療業界においては、バックアップを使用したほうが、身代金を支払ったケースよりも短期間にデータを復旧し、攻撃の影響から迅速に業務を立て直していることが明らかになりました。

データの復旧に 1 週間以上要した企業の割合は、バックアップを使用した場合で回答者の約 4分の 1 (27%) であったのに対し、身代金を支払った場合は 40% にのぼっています (ともに四捨五入値)。

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、医療業界が直面する大きな脅威のままとなっています。今年のレポートでは、ランサムウェア攻撃の割合が低下したと報告されていますが、回答者のほぼ 3分の 2 (60%) がランサムウェアの被害に遭っています。

攻撃者が攻撃の戦術、手法、手順 (TTP) に磨きをかけ続ける中、防御側は遅れをとらないようにするのに苦労し、その結果一貫して高いレベルの攻撃と暗号化率の向上をもたらしています。ランサムウェアの被害を受けた医療業界のほぼ 4分の 3 (73%) が、データの暗号化をされ、前年の 61% から増加しています。さらに、データが暗号化されたと報告した 37% のケースでは、データも窃取されていました。

心強い点としては、医療業界では、暗号化されたデータを復旧するために身代金を支払う傾向が減少し、昨年の調査の 61% から 2003年のレポートでは 42% に減少したと報告されています。

同時に、医療機関によるバックアップの使用率は、前年比 72% から 73% へとわずかに増加しただけでした。良いニュースは、データを暗号化していたすべての医療機関は、攻撃後にデータを復旧できました。これは、業界間平均である 97% を上回っています。

組織の保険の等級は、データ復旧方法に影響を与えました。データが暗号化され、独立したサイバー保険契約を結んでいた医療業界の 53% が身代金を支払ったのに対し、サイバー保険を含んだ、より広範な保険契約を結んでいる組織では、その数は 34% に減少しました。

医療機関の全体的な復旧コストは、前年比で 185万ドルから 220万ドルに増加しました。これはおそらく、攻撃後の暗号化率の増加が一因です。医療業界の復旧コストは、業界間の平均である 182万ドルを上回りました。

RaaS（Ransomware as a Service）のビジネスモデルが増え続けているため、2023年中に攻撃が減少することはなさそうです。

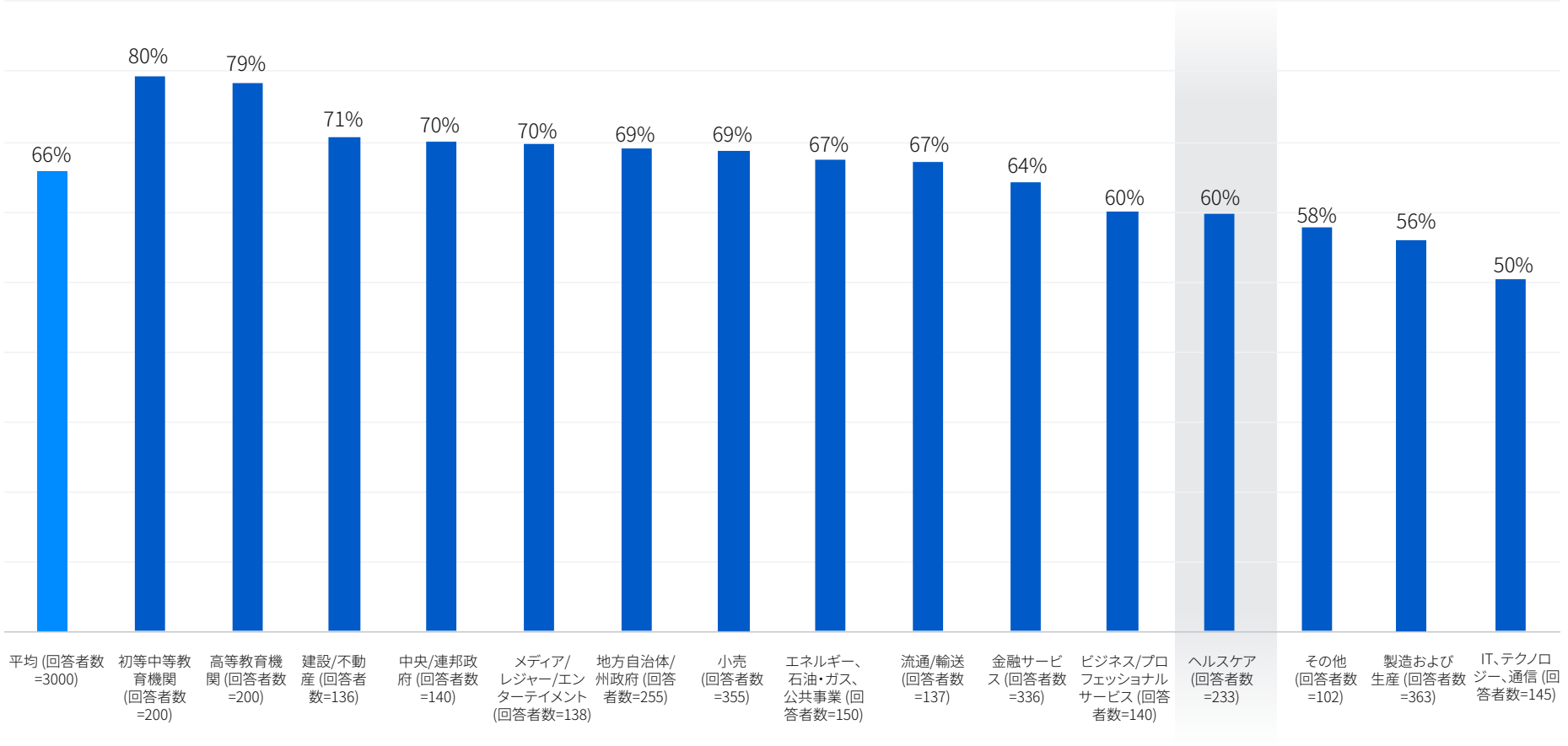
対策すべき重点ポイント：

- 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を維持します。

その他の図表

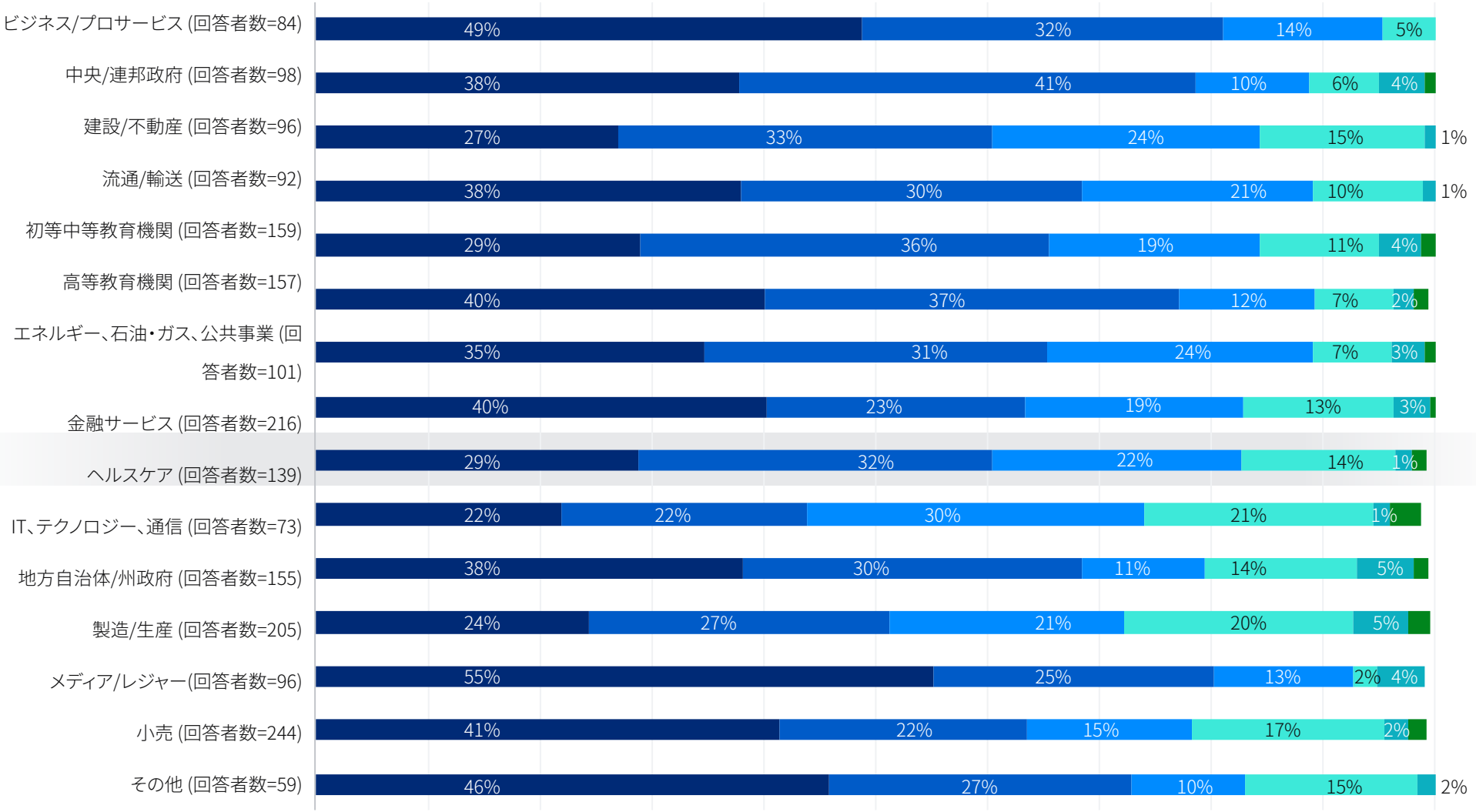
ランサムウェア攻撃 (業界別)

ランサムウェア攻撃を受けた組織の割合



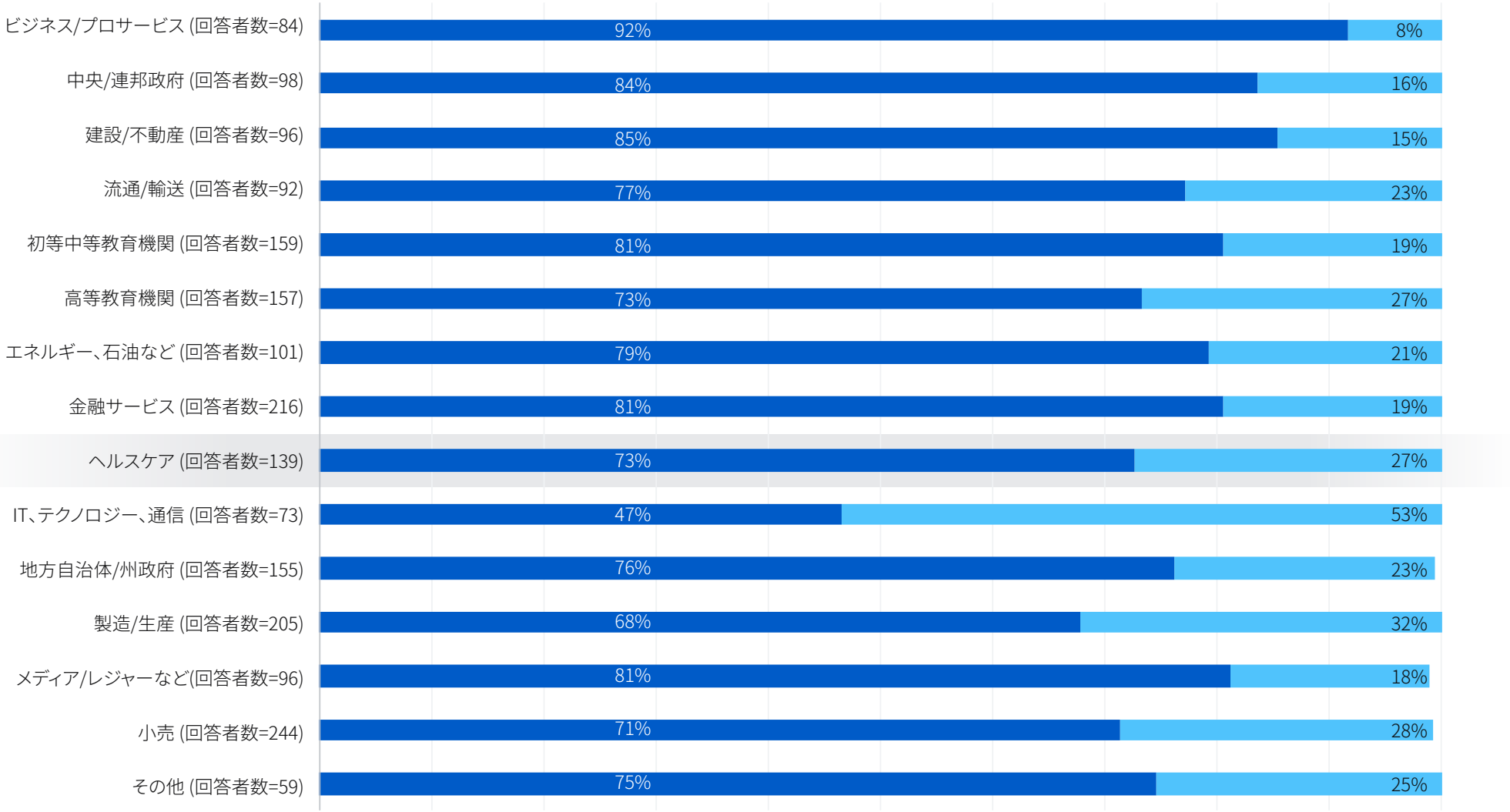
過去 1 年間にランサムウェア攻撃を受けましたか?回答数はグラフ内

業界別の攻撃の根本原因



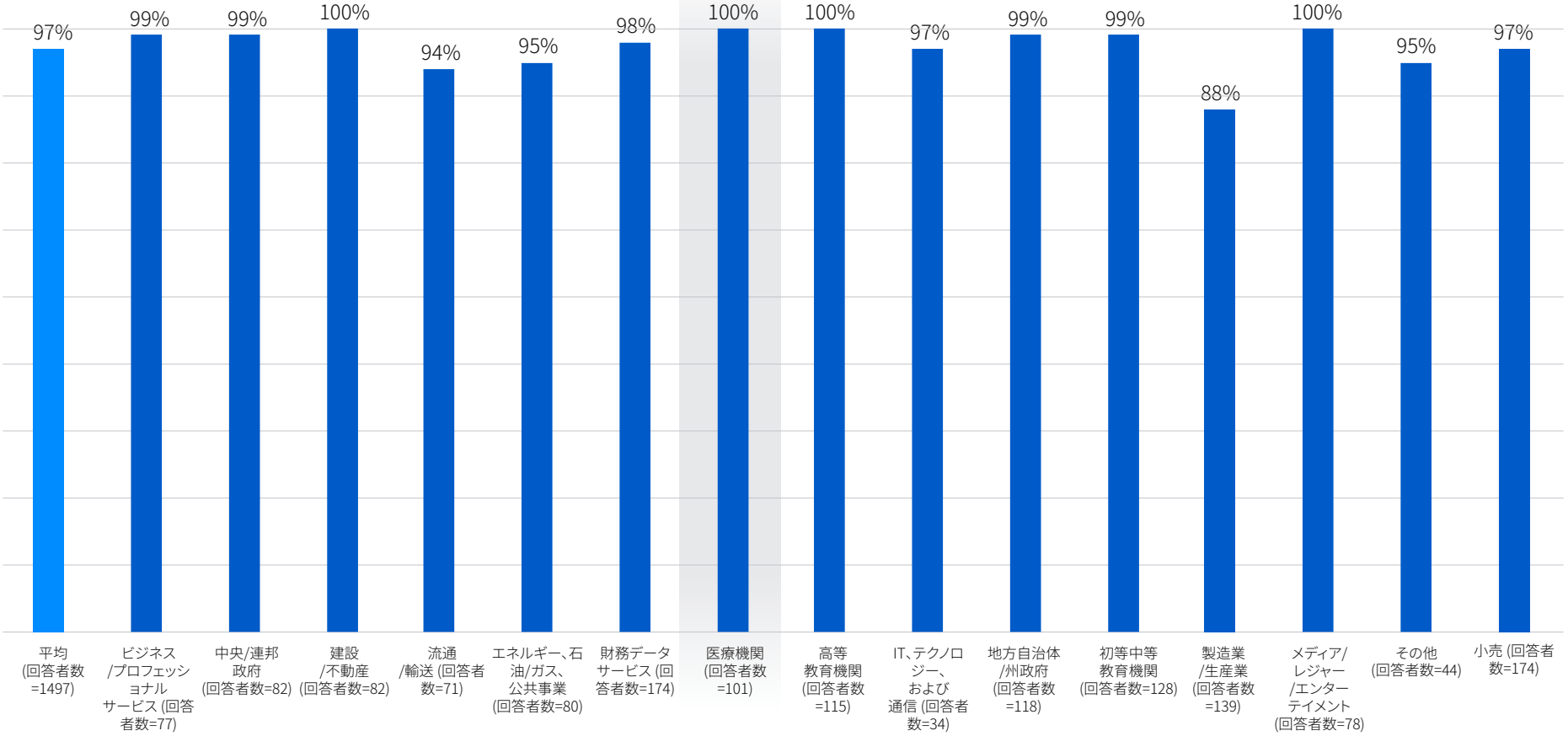
昨年受けたランサムウェア攻撃の根本原因を把握していますか? 回答の選択肢を選択。回答数はグラフ内

業界別のデータの暗号化



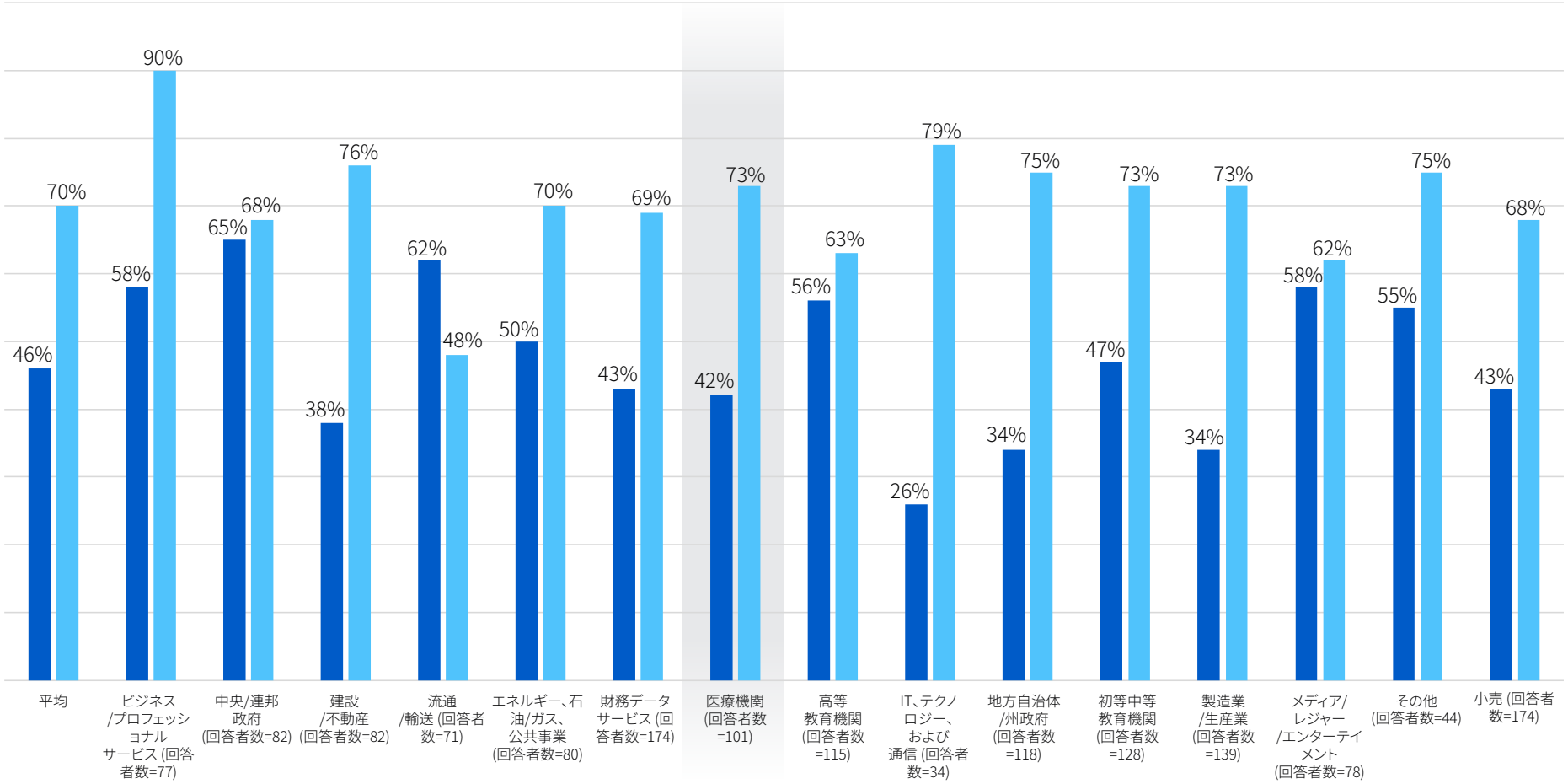
ランサムウェア攻撃でデータは暗号化されましたか?回答の選択肢を統合。回答数はグラフ内

データの復旧率



データを取り戻すことができましたか? 回答者数 = 1,497社 (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)

データ復元の方法: 身代金の支払いまたはバックアップの使用



データを取り戻すことができましたか? 回答者数 = 1,497社 (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)

調査方法

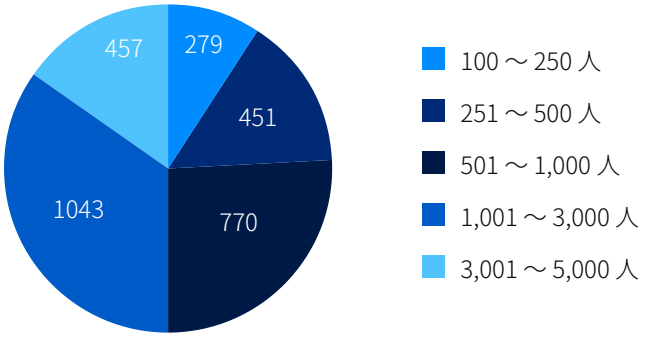
ソフォスは、2023 年 1 月から 3 月にかけて 3,000 名のサイバーセキュリティと IT 部門のリーダーに対して調査を実施しました。本調査は特定のベンダーに関連していない独立した調査機関に委託されています。回答した組織は、北アメリカ/南アメリカ、EMEA、アジア太平洋地域の 14 か国を拠点としています。

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。

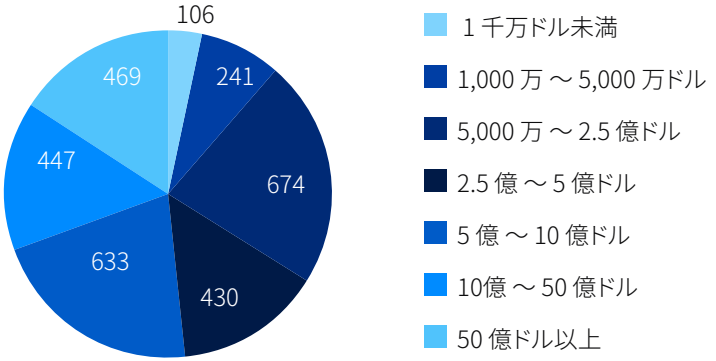
国別の回答者数

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。

2023-08-03 (WP-NP)

SOPHOS