SOPHOS
Cybersecurity evolved.

医療業界のランサムウェアの現状 2021年版

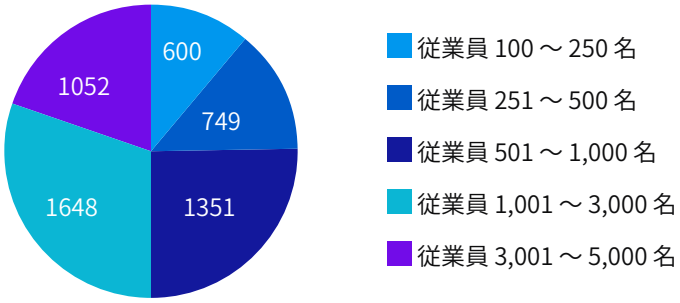
このレポートでは、医療分野におけるランサムウェアの現状に関する最新の調査結果と新しい洞察を紹介します。内容は、医療業界のランサムウェアの普及率、被害者への影響、ランサムウェア攻撃の修復コスト、および身代金支払い後の被害者が回復できたデータの割合の調査となります。また、この調査では、医療業界が他の業界とどのように匹敵するか、またこれらの攻撃に直面した場合の医療機関の将来的な期待と準備も明らかにしています。

ソフォスホワイトペーパー2021年 5月

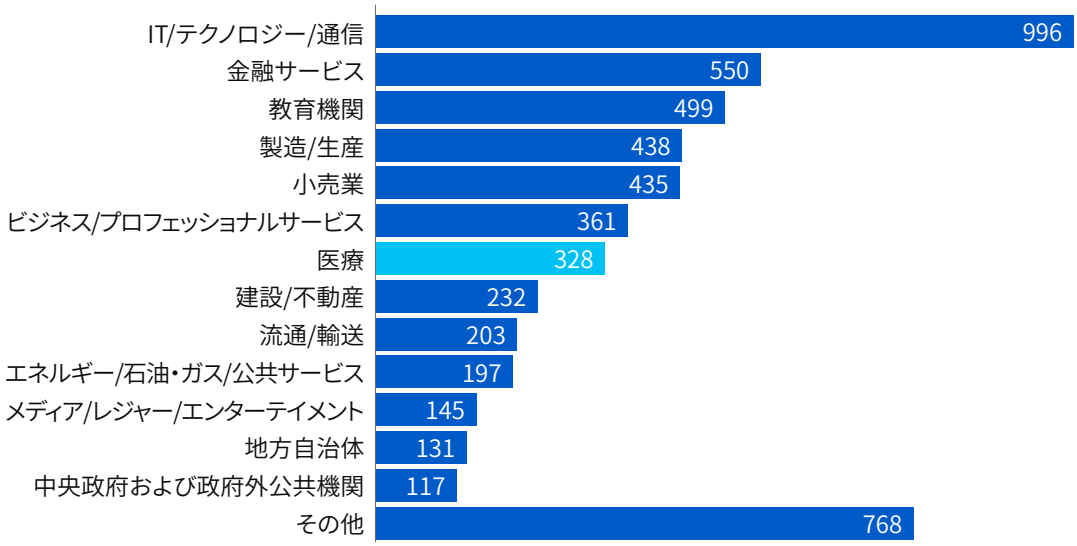
調査方法について

ソフォスは、独立系の調査会社 Vanson Bourne 社に委託して、30 か国にわたる 5,400 人の IT 意思決定者に調査しました。回答者は、**医療機関より 328人**を含むさまざまな分野からとなります。この調査は、2021年 1月と 2月に実施されました。

グローバルな従業員数[5,400]



組織の業種[5,400]



各国の回答者は、従業員数 100 ～ 1,000 名の組織が 50%、1,001～5,000 名の組織が 50%になっています。328人の医療機関の IT 意思決定者は、調査対象のすべての地域 (南北アメリカ、ヨーロッパ、中東、アフリカ、アジア太平洋) から来ました。

地域	回答者数
北米・中南米	66
ヨーロッパ	127
中東、アフリカ	37
アジア太平洋	98

医療分野 328人の IT 意思決定者

主な調査結果

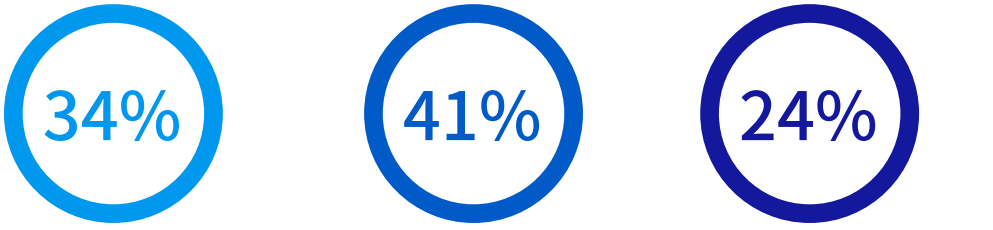
- **昨年、ランサムウェア攻撃を受けた**医療組織の割合は **34%** でした。
- 昨年、最も重大なランサムウェア攻撃で**組織のデータが暗号化されたと**回答した組織の割合は **65%** でした。
- データが暗号化されている組織の **44%** が、**データの復元にバックアップを使用していました。**
- 最も重大なランサムウェア攻撃でデータが暗号化され、**データを取り戻すための身代金を支払った**組織の割合は **34%** でした。
- しかし、身代金を支払った後に**暗号化されたデータを復元できた割合は 69%** でした *。
- 医療機関の **89%** は、**マルウェアインシデントの復旧計画**があります。
- **ランサムウェア攻撃の影響を修復するための平均総額**は、ダウンタイム、復旧のための人件費、人件費、デバイスのコスト、ネットワークのコスト、逸失利益、支払った身代金などを考慮すると、**127 万米ドル**になります。これは膨大な金額ですが、**調査対象のすべてのセクターの中で最も低い金額**でもあります。

* 指標数 – 低いレスポンスベース

医療分野におけるランサムウェアの普及率

ランサムウェアの被害を受けていない組織の大半が、将来的に攻撃を受けることを予想

調査対象となった 328人の医療機関の回答者のうち、34% が過去一年間にランサムウェアの被害に遭っていました。ランサムウェア攻撃によって、複数のコンピューターが影響を受けていましたが、必ずしもコンピューターのデータが暗号化されていたわけではありませんでした。昨年攻撃を受けなかった組織のうち、41% は将来ランサムウェアに攻撃されることを予測しており、24% は将来の攻撃に対して安全であると確信していました。レポートの後半では、将来的な攻撃を予想する理由と、今後の攻撃において自信を持っている回答者がいる理由についてさらに深く掘り下げます。

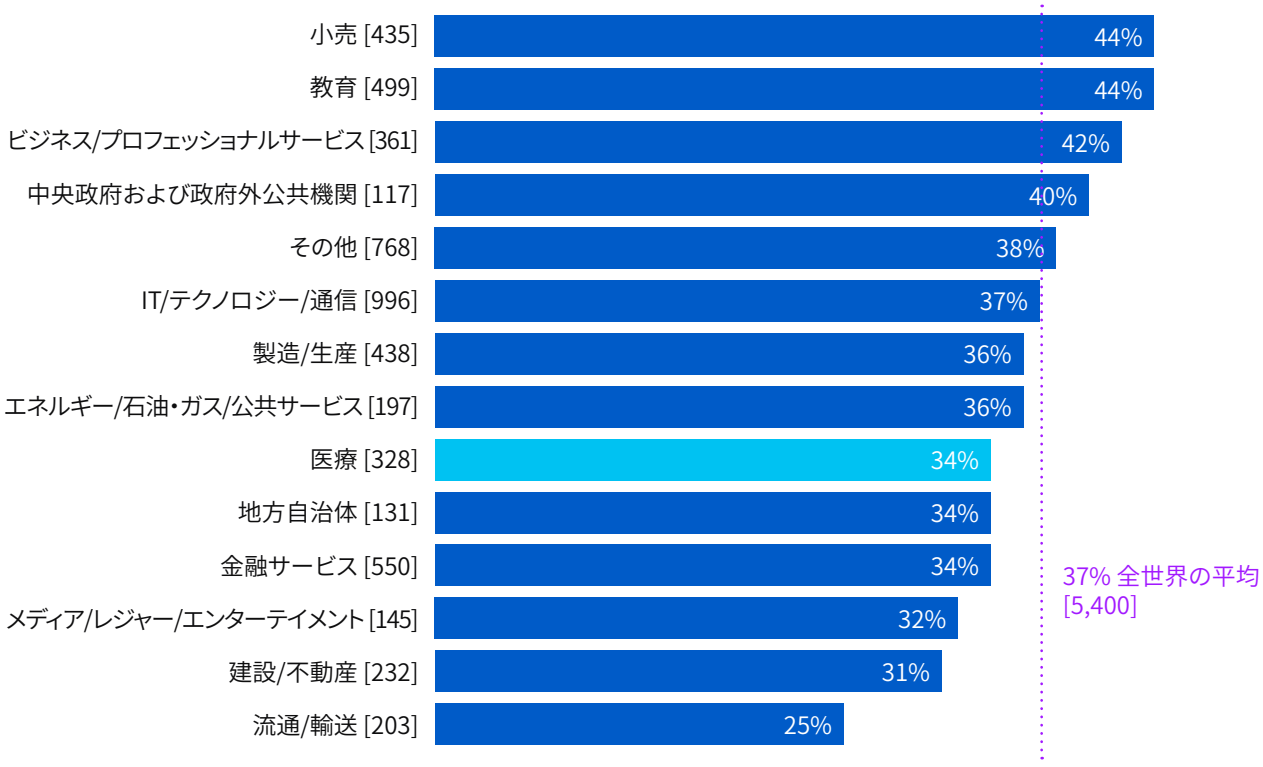


「昨年、ランサムウェア攻撃を受けましたか？」[328人の医療機関回答者]

平均レベル以下の攻撃に驚く医療機関

ランサムウェアの被害を受けていると報告している医療機関はわずか 3 分の 1 強で、実際すべての業界の世界平均である 37% よりわずか良い結果でした。**小売業**および**教育機関**は、ランサムウェア攻撃を受ける割合が最も高くなっており、回答者の 44% が攻撃を受けたことを報告しています。

昨年、ランサムウェア攻撃を受けた回答者の割合



「昨年、ランサムウェア攻撃を受けましたか？」「はい」と回答した組織 [回答した組織数] 一部の回答の選択肢を省略し、業種ごとに分割。

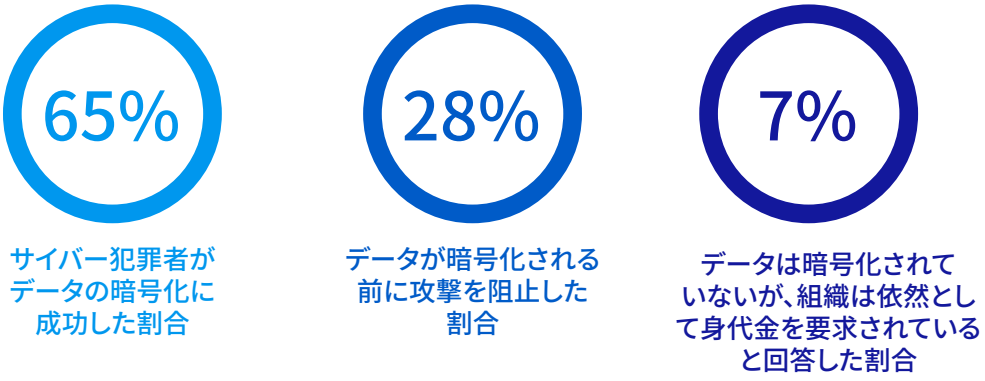
医療機関はランサムウェア攻撃でトップニュースになることが多いため、この分野での攻撃が平均を下回っていることは、おそらく喜ばしい驚きでしょう。ニュース報道での過剰な表現は、多くの商用組織が悪いニュースを非公開のままにできるのに対し、攻撃を公表するという医療機関の義務によるものと思われます。

世界中のすべての業種で、過去一年間にランサムウェアに攻撃された組織の割合は、51% が攻撃を受けたことを認めた昨年より大幅に減少しました。この減少は歓迎すべきニュースですが、SophosLabs と Sophos Managed Threat Response によって観察された攻撃者の行動の進化が原因である可能性があります。例えば、多くの攻撃者は、大規模で自動化された汎用性の高い攻撃から、手動によるハッキングなど、従来よりもさらに標的型の攻撃にシフトしています。全体的な攻撃数は減少しましたが、ソフォスは、このような標的型攻撃による被害はさらに深刻で甚大になっていると考えています。

ランサムウェアによる被害

攻撃者は医療データの暗号化に成功

ランサムウェアの攻撃を受けた組織の回答者に、犯罪者によりデータが暗号化されたかどうかを調査しました。回答者の約 3 分の 2 である 65% が「はい」と答えています。28% は、データが暗号化される前に攻撃を阻止できたと回答しています。

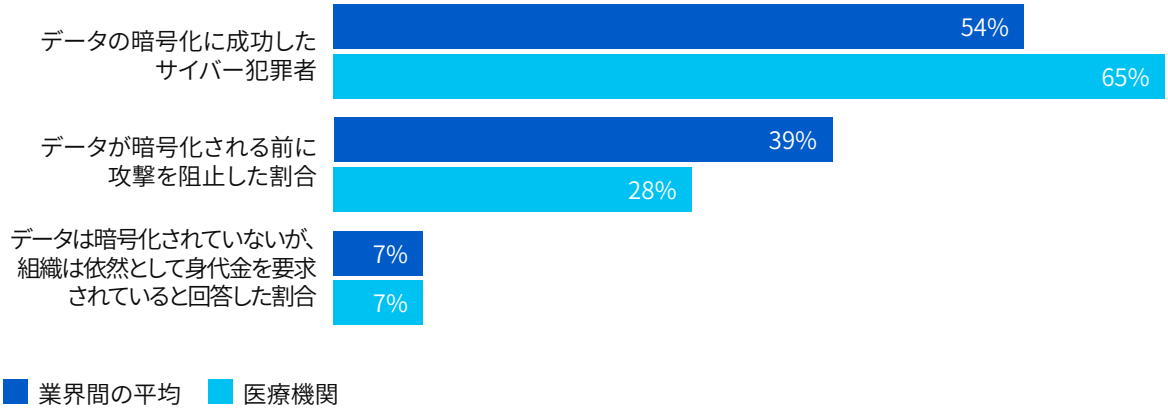


最も重大なランサムウェア攻撃でデータを暗号化されましたか?
[過去一年間でランサムウェアの被害に遭った 113 の医療機関]

さらに 7% が、データは暗号化されていないが、組織は依然として身代金を要求されていると回答しています。この理由は、一部の攻撃者が、ファイルを暗号化する代わりにデータを盗み出し、身代金を払わない場合にデータを公開すると脅す、恐喝型の攻撃に移行しているためです。これにより、作業の負担が軽減されます。暗号化または復号化する必要はありません。サイバー犯罪者は、データ侵害における懲罰的な罰金を利用して、身代金をさらに組織に要求してくる場合が多くあります。

医療機関は、他の業界に比べてランサムウェアの阻止能力が低い

世界の他の業界と比較すると、攻撃者による医療データの暗号化の成功率 (65%) は、世界平均 (54%) よりもはるかに高いです。また、医療機関は、データが暗号化される前に攻撃を阻止する成功率においても世界の平均を下回っています。28% 対 39% 。



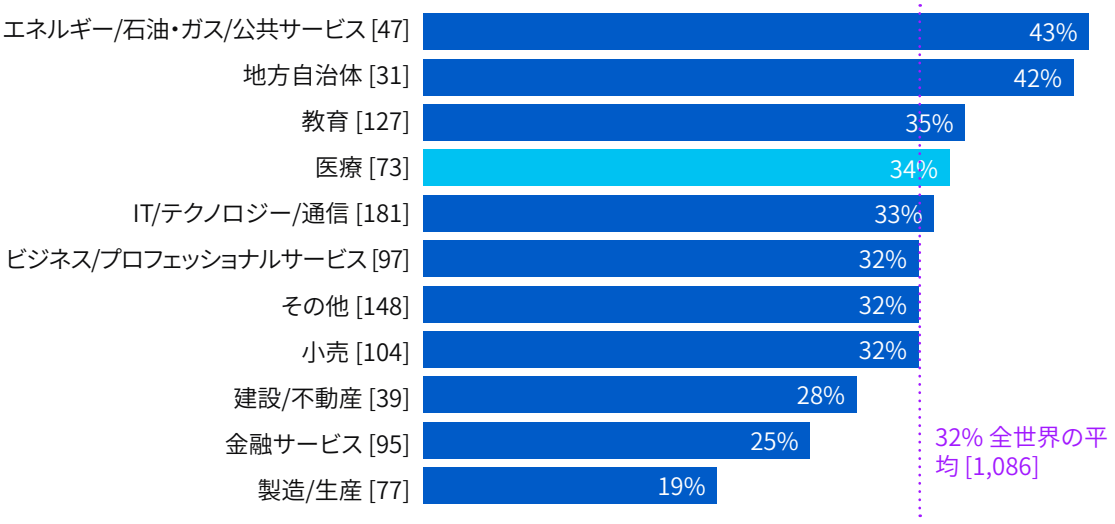
最も重大なランサムウェア攻撃でデータを暗号化されましたか? [2006 業界間; 過去一年間でランサムウェアの被害に遭った 113 の医療機関]

これは、医療機関の IT が直面する財政上やリソースの課題が原因である可能性があります。これらのチームは一般的に人材不足ですが、特に昨年はパンデミックによりさらに不足していました。同時に、多くの医療機関は、直接患者のケアに関連する医療リソースを購入するための資金提供を受けた場合は、資金をサイバーセキュリティに流用したくはありません。ランサムウェアが医療機関に与える影響が大きいもう 1つの要因は、更新やパッチ適用が困難な従来の機器にあり、攻撃者が簡単に侵入拠点を提供していることです。

医療機関は身代金を支払う可能性が高い

医療機関は身代金を支払う可能性が最も高い業界の 1つであり、業界間の平均 32% と比較するとデータが暗号化された回答者の 34% が身代金の支払いを認めています。これは、ヘルスケアチームがサービスの継続性を確保するというにプレッシャーが原因である可能性があります。

データを取り戻すために身代金を支払った割合



組織は最も重大なランサムウェア攻撃でデータを取り戻しましたか？身代金を支払った組織 [回答した組織数]
最も重大なランサムウェア攻撃で組織のデータが暗号化されたと回答した組織、一部の回答の選択肢を省略し、業種ごとに分割。

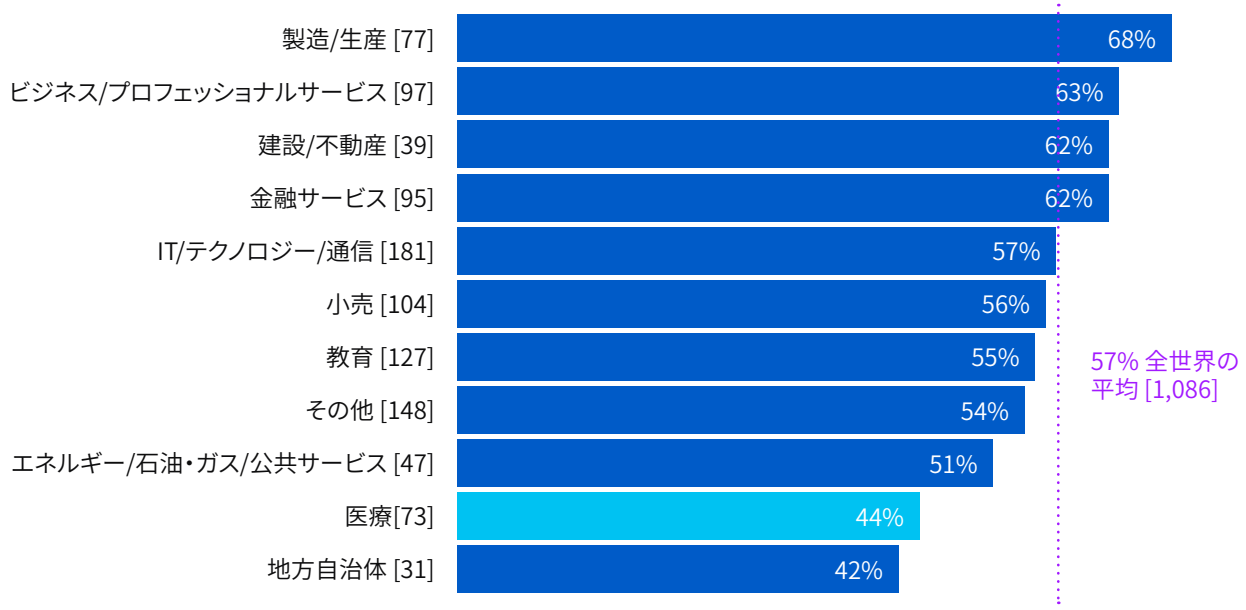
業界全体で、**エネルギー、石油/ガス、公益サービス**が身代金を支払う可能性が最も高く、43% が身代金の要求に応じています。この業界では、一般的に、簡単にアップデートできないレガシーインフラストラクチャを利用していることが多く、被害を受けた組織は事業を継続するために、身代金を支払わなければならないと感じているのかもしれません。

地方自治体は、身代金の支払が 2 番目に多くなっていました (42%)。これは、データが暗号化されている可能性が最も高い業界でもあります。地方自治体の組織が支払いに応じる傾向が高いことから、攻撃者は複雑で効果的な攻撃を地方自治体に集中させている可能性があります。

そして、データをバックアップする可能性は低い

医療業界の身代金の支払い率が高いのは、この業界の組織がバックアップからデータを復元できないことが原因である可能性もあります。世界的に、暗号化されたデータを使用している 組織の 57% が、バックアップからデータを復元できました。しかし、これは医療分野ではわずか 44% に減少し、調査対象のすべての業界の中で 2 番目に低い割合になります。

バックアップを使用してデータを復元した割合

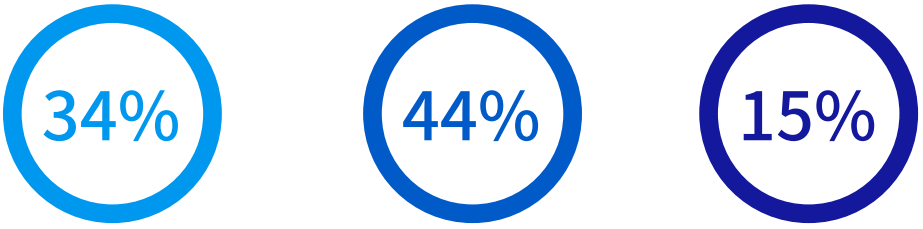


組織は最も重大なランサムウェア攻撃でデータを取り戻しましたか？

はい、バックアップを使用して、最も重大なランサムウェア攻撃でサイバー犯罪者によりデータの暗号化に成功した組織のデータを復元 [回答した組織数] 。一部の回答の選択肢を省略し、業種ごとに分割

93% の医療業界の組織がデータを回収

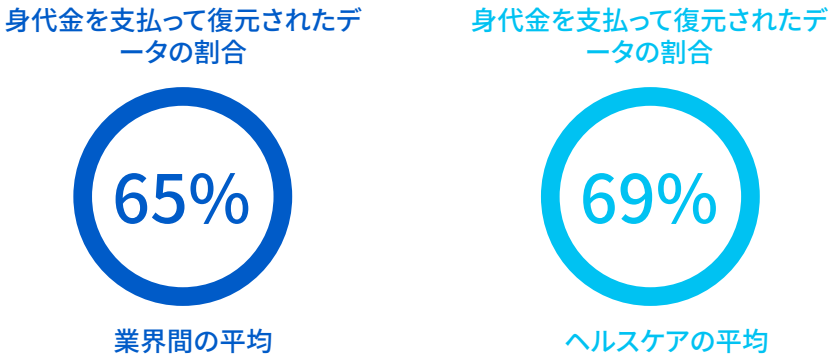
ランサムウェア攻撃後にサイバー犯罪者によってデータを暗号化された医療業界の回答者のうち、93% がデータを取り戻しました。これは、世界の業界間の平均である 96% と一致しています。このコーホートのうち、3 分の 1 強 (34%) が身代金を払ってデータを取り戻し、44% がバックアップを使用してデータを復元し、15% がデータを取り戻すために他の手段を使用しました。



組織は最も重大なランサムウェア攻撃でデータを取り戻しましたか？[73] 回答した医療機関数。

身代金を支払っても報われない

攻撃者が身代金を要求するときに明確に伝えていないことがあります。それは、たとえ身代金を支払ったとしても、すべてのデータを復元できる可能性は低いということです。身代金を支払った企業が、データを復元できた割合は 65% のみです。つまり、3 分の 1 以上のデータは失われたままです。



最も重大なランサムウェア攻撃を受けた組織が取り戻したデータ量の平均値 [344/25] 身代金を支払ってデータを取り戻した組織

医療業界の回答者の組織数は 25社だったため、このデータは確固たるものではありません。しかし、医療業界の回答者は、平均で 69% のデータを取り戻したと報告しています。これは世界平均よりもわずかに優れていますが、それでもデータのかなりの部分にアクセスできないままです。

すべての業界の回答者のうち、29% が 50% 以下のデータを取り戻し、8% のみがすべてのデータを取り戻しました。

ランサムウェアのコスト

明らかにされた: 身代金支払い額

組織が身代金を支払ったと報告した業界全体の 357 人の回答者のうち、282 人が正確な金額を共有し、そのうちの 23 人は医療関係者でした。ここでも、医療機関の基となる数がやや低いため、ここでの調査結果は単なる指標として考慮する必要があります。

170,404 米ドル
平均的な世界の身代金支払い額

131,304 米ドル
平均的な医療機関の身代金支払い額

最も重要なランサムウェア攻撃で、お客様の組織が支払った身代金はいくらでしたか？[23/282社] データを取り戻すために身代金を支払った組織

すべての業界での身代金の平均支払い金額は 170,404 米ドルでした。しかし、医療機関では、平均的な身代金の支払い額は 40,000 米ドル近く下がった、131,304 米ドルでした。

身代金が、新聞の見出しを飾るような 1 億円以上から 100 万円程度まで、広範囲になっていることにはいくつかの理由があります。

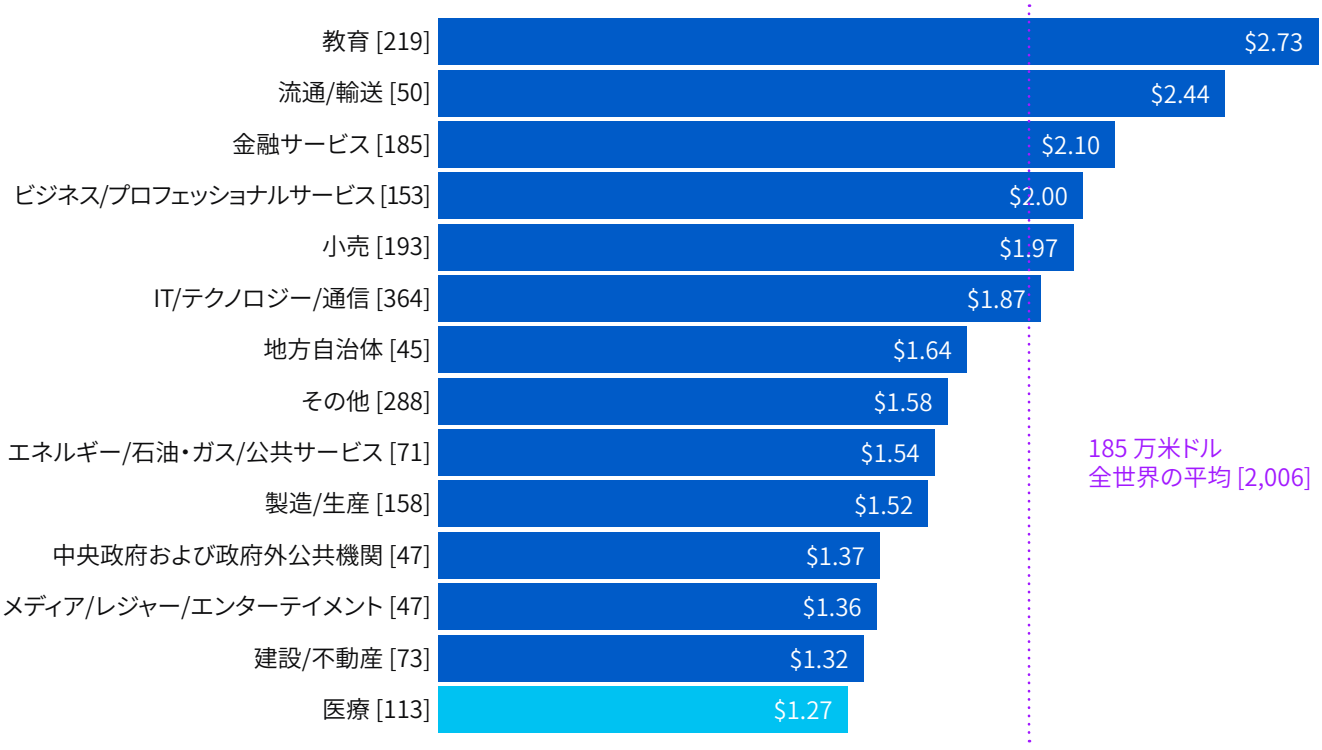
1. **組織の規模。**この調査の回答者は、一般的に大きな組織と比較すると資金力が少ない、従業員数が 100～5,000 名の中堅規模の組織の IT 意思決定者です。ランサムウェアを使用する攻撃者は、標的組織の支払い能力に応じて身代金の要求額を調整しており、通常、小規模な企業であれば、低額の身代金を要求して受け入れています。これを裏付けるように、従業員数が 100～1,000 名の組織が支払った身代金の平均額は 107,694 米ドルであり、従業員数が 1,001～5,000 名の組織が支払った身代金の平均額は 225,588 米ドルでした。

2. **攻撃の特徴。**ランサムウェアの攻撃者は多数存在しており、ランサムウェアの攻撃手法も多岐にわたります。個別の標的に合わせて高度な TTP (戦術、手法、手順) を使用するスキルの高い攻撃者から、「既製品」のランサムウェアを使用し、運任せに無差別な攻撃を実行し高度なスキルを持たない攻撃者までさまざまな攻撃者が存在します。標的型攻撃に多大な投資を行っている攻撃者は、その労力に見合った高額な身代金を求めますが、汎用的な攻撃を行っている攻撃者の多くは、「薄利多売」のようなビジネスを展開しています。

3. **地域性。**最初に見たように、この調査では世界 30 か国を対象としており、GDP レベルはさまざまです。攻撃者は、欧米先進国の標的に高額な身代金を要求していますが、これは、欧米先進国には多額の身代金を要求されても支払い能力がある組織が多いと考えているためです。身代金の支払い額が最も高かった 2 件は、いずれもイタリアの回答者によるものでした。一方で、インドでは、身代金の平均支払額は 76,619 米ドルで、世界の半分以下です (対象回答者：86 名)

ヘルスケアはランサムウェアの回収コストが最も低い

ランサムウェア攻撃から回復し、最新の攻撃の影響を修正するための組織の平均的なおおよそのコスト (ダウンタイム、損失時間、デバイスコスト、ネットワークコスト、機会の損失、身代金の支払いなど) を見ると、医療業界は、全体的な修復コストが 1 億 2700 万米ドルと最も低い報告をしています。これに対し、業界間の平均は 18 億 5000 万米ドルです。



最近発生したランサムウェア攻撃において、復旧作業にかかった平均コスト (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、身代金など) [回答した組織数] 昨年ランサムウェア攻撃を受けたと回答した組織、業種別に分割、100 万米ドル

医療費の削減には、次のような要因が考えられます。

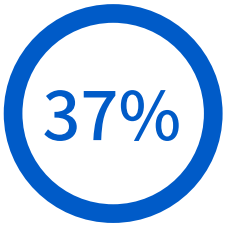
1. 医療機関は多くの場合、他の多くの業界よりも予算が少ないため、修復に費やすことができる金額に制限があります。
2. 世界の多くの地域で、医療は公共サービスです。たとえランサムウェアの攻撃を受けたとしても、特定の医療施設を利用する以外選択肢がほとんどないため、レピュテーションコストや機会コストはほとんど、もしくはまったく発生しません。このことは、他のほとんどの業界が攻撃を受けているときとは対照的なパターンです。

展望

今後の攻撃に対する医療業界の期待

昨年ランサムウェアの被害を受けなかったと回答した医療関係者の約 3 分の 2 (63%) は、将来的にランサムウェアの被害を受けると予測しています。逆に、37% は攻撃を予測していません。

将来的に攻撃を受けることを予測している割合



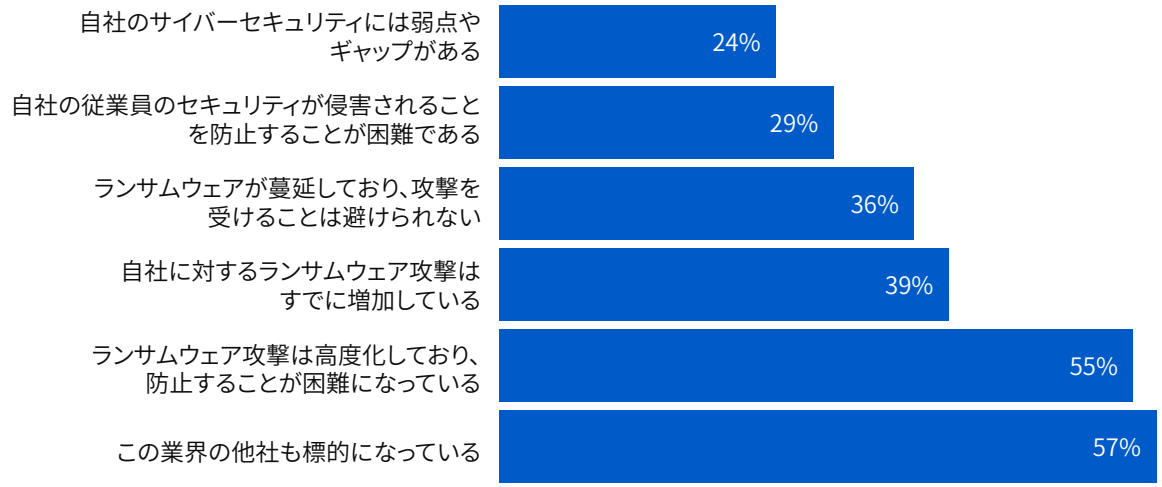
将来的に攻撃を受けることを予測していない割合

[214人]「昨年、ランサムウェア攻撃を受けましたか？」という質問に「いいえ」と答えた回答者数

このグループ内の組織でも、ランサムウェア対策に関する考え方や自信に大きな違いが見られます。

医療業界が攻撃を受けると予測する理由

ランサムウェアの被害は受けていないが、今後被害を受けると予想する医療機関の 63% のうち、最も一般的な理由 (57%) は、医療業界の他の組織が標的にされていることです。さらに、回答者の 55% は、ランサムウェア攻撃が巧妙化しているため、阻止するのがますます難しくなっていると回答しています。これは高い数字ではありますが、これらの組織がランサムウェアの進化に警戒していることは良いことでもあります。このような慎重な姿勢は、昨年、ランサムウェア攻撃を防止できた要因かもしれません。



今後、組織がランサムウェア攻撃の影響を受けると予測する理由は何ですか？[ランサムウェア攻撃の影響を受けなかったが、今後被害に遭う恐れがあると考えている 135 の医療組織、一部の回答の選択肢を省略]

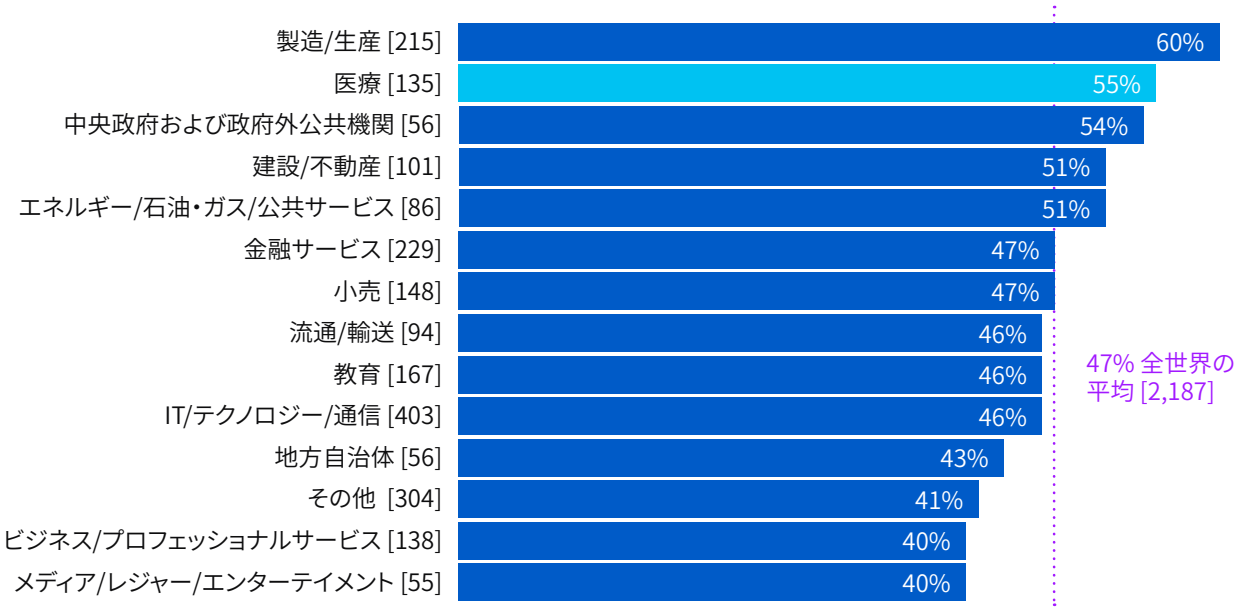
回答者の 29% は、今後ランサムウェアの被害に遭う主な原因として、従業員のセキュリティが侵害されることを挙げています。巧妙な攻撃を受けている中で、多くの IT チームが個別のユーザーを非難するという安易な選択肢を取らないことは心強いことです。

同様に、24% の回答者が、自社のサイバーセキュリティ対策には弱点やギャップがあることを認めています。もちろん、セキュリティホールがあることは良いことではありませんが、これらの問題を認識することは、防御力を高めるための重要な第一歩です。

医療業界で高度化するランサムウェアに対する高い認識

医療業界の回答者は、巧妙化してきているランサムウェアに対して、最も警戒している業界の 1つ (55%) であることが分かります。世界平均は 47% でした。

攻撃が増加し巧妙化してきていると答えた回答者の割合



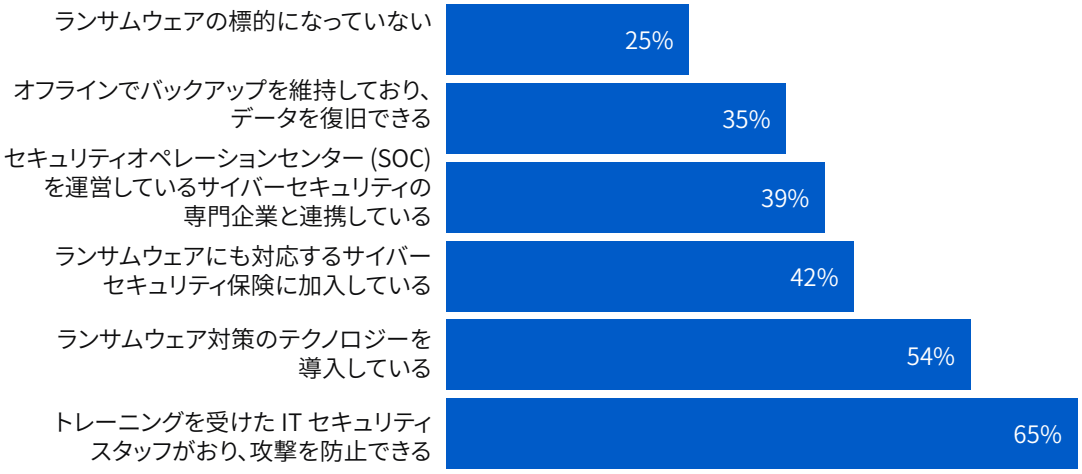
今後、組織がランサムウェア攻撃の影響を受けると予測する理由は何ですか?[2,187] 将来的に攻撃されると予想している理由として、ランサムウェア攻撃が巧妙化してきているため、阻止するのがますます難しくなっていると挙げた組織数

この質問の回答者は、昨年、自社がランサムウェアの被害に遭ったわけではありませんが、各業界で発生したさまざまなランサムウェア攻撃の影響を受けていると考えられており、医療業界が多くの成功した攻撃の矢面に立ってきています。

トレーニングを受けた IT スタッフの存在がランサムウェア対策に安心感を与える

昨年はランサムウェアの被害に遭わなかった 79 名の医療関係の回答者は、今後も組織は被害に遭うことはないと答えています。ランサムウェア攻撃を受けてもその対処に自信を持てる最大の理由は、攻撃を阻止できるトレーニングを受けた IT スタッフを採用していることが、ランサムウェア対策テクノロジーへの自信となっているからです。回答者の半数以上がランサムウェア対策テクノロジーを導入していることは心強いことです。

組織が今後ランサムウェア攻撃の影響を受けないと回答者が予測する理由は何ですか?



今後、組織がランサムウェア攻撃の影響を受けないと予測する理由は何ですか?[79] ランサムウェア攻撃の影響を受けず、今後も影響を受けないと考えている医療組織数、一部の回答の選択肢を省略

ランサムウェア対策を効果的に実施するためには、高度で自動化されたテクノロジーが不可欠ですが、人間が手動で実行している攻撃を防止するには、高いスキルを有する専門家による監視と介入も必要です。自社のスタッフでも外部の専門家でも、人間の専門家は、ランサムウェアを操る攻撃者が自社を狙っていることを示すいくつかの動かぬ兆候を見分けることができます。継続的なランサムウェアの脅威に直面する中で、すべての組織が専門知識を身に付けることを強くお勧めします。

ランサムウェアの被害を受けておらず、今後もランサムウェアの被害を受けないと予測している医療業界の回答者の 39% は、SOC (セキュリティ オペレーション センター) を運営する専門のサイバーセキュリティ企業と連携しています。これは、中規模企業向けのサイバーセキュリティの提供における大きな変化を表しています。ほんの数年前まで、SOC は最大規模の組織に独占されていましたが、現在は SOC が主流であることがデータで示されています。

朗報ばかりではありません。懸念される結果も明らかになっています。

- 被害に遭うと予測していない回答者の 47% は、ランサムウェアによる影響を保護しないアプローチを妄信しています。
  - 回答者の 35% は、「オフラインでバックアップを維持している」ことを、攻撃の影響を受けない理由として挙げています。これまで見てきたように、バックアップは攻撃を受けた後にデータを復元するための貴重な方法となりますが、バックアップをしたからといって、攻撃を防ぐことはできません。
  - 回答者の 42% が、サイバーセキュリティ保険に加入していることを、ランサムウェア攻撃の影響から保護される理由に挙げています。繰り返しになりますが、攻撃を受けた後の対処には役立ちますが、攻撃自体を防ぐことはできません。

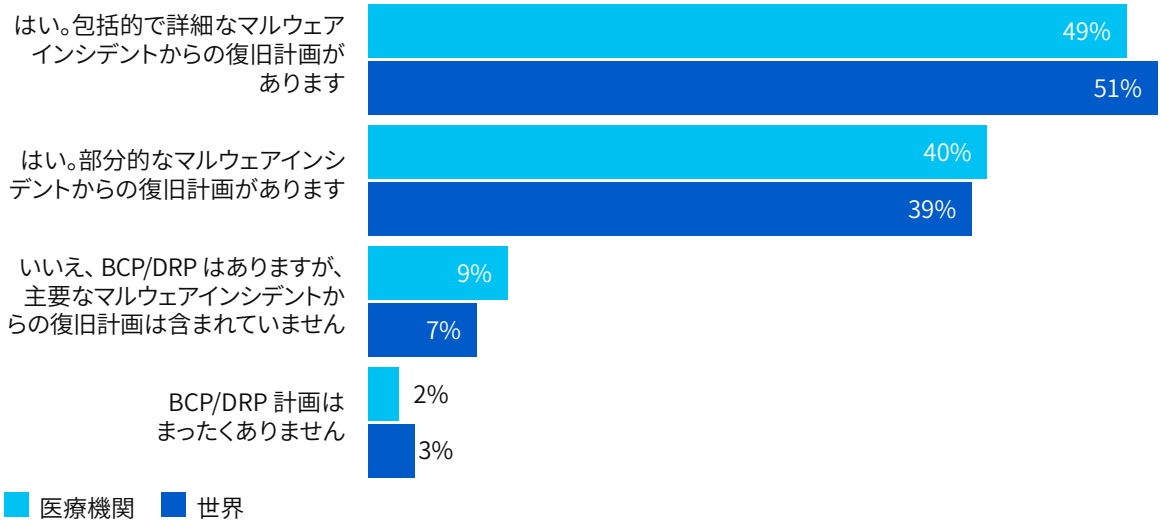
一部の回答者は上記の両方の選択肢を選択しており、47 人がこれら 2 つの選択肢の少なくとも 1 つを選択しています。

- 25% の回答者は、自社はランサムウェアの標的にはならないと考えています。残念ながらこれは事実ではありません。安全な組織は存在しません。

ほとんどの医療機関は、マルウェアインシデントの復旧計画があります。

大規模なサイバー攻撃やインシデントへの対応は、非常に大きなストレスとなります。攻撃への対応によるストレスを完全に排除することはできませんが、効果的なインシデント対応計画を導入すれば、必ず影響を最小限に抑えることが可能です。

そのため、医療機関の 89% がマルウェアインシデントの復旧計画を作成、半数弱 (49%) が完全かつ詳細な計画を作成、そして計画の一部を作成しているのは 40% であるということが分かったのは心強いことです。これらの統計情報は、業界間の平均値と非常に一致しています。



組織の事業継続計画 (BCP)/災害復旧計画 (DRP) には、大規模なマルウェアインシデントの復旧計画が含まれていますか?[世界 5,400 人 / 医療機関の回答者 328 人]

提言

これらの調査結果を踏まえて、ソフォスの専門家は以下のベストプラクティスを提言します。

1. **攻撃を受ける前提で対策を講じてください。**ランサムウェアは依然として多く発生しています。業界、国、組織の規模を問わず、このリスクから免れることはできません。サイバー攻撃についても「備えあれば憂いなし」です。

2. **バックアップを作成してください。**バックアップは、攻撃を受けた後に企業がデータを復旧するための最も重要な手段です。また、身代金を支払っても、すべてのデータが戻ってくることはほぼ皆無ですので、攻撃を受けた場合には、いずれにしてもバックアップを利用する必要があります。

バックアップ戦略のヒントは、3-2-1 の法則です。これは少なくとも **3 つ**のコピーを作成し (現在使用しているデータの他に 2 つ以上のコピーを保管)、少なくとも **2 つ**の異なるバックアップシステムを使用し (1 つのバックアップシステムで障害が発生する場合に備えて)、少なくとも **1 つ**のコピーをオフラインで、できればオフサイト (攻撃者が改ざんできない場所) に保存する戦略です。

3. **多層防御を導入してください。**恐喝型の攻撃が大幅に増加している中で、攻撃者を自社の環境に寄せ付けないことがこれまで以上に重要になっています。サイバー犯罪者はネットワーク環境内のさまざまな場所を攻撃しています。これらの多くの場所で攻撃を防御できるように多層防御のアプローチを使用してください。

4. **人の専門家とランサムウェア対策テクノロジーを融合させます。**ランサムウェアを阻止するには、ランサムウェア対策の専用のテクノロジーと人間主導の脅威ハンティングを組み合わせた防御が鍵となります。これらのテクノロジーにより、大規模で自動化された攻撃を防止できるようになります。一方で、人の専門家は、高度なスキルを有する攻撃者による侵入の痕跡を検出・特定する戦術、技術、手順において優れた能力を発揮します。社内にスキルを持つ方がいない場合は、専門のサイバーセキュリティ会社のサポートを検討してください。SOC は現在、あらゆる規模の組織にとって現実的なオプションとなっています。

5. **身代金は支払わないでください。**ランサムウェア攻撃により組織の業務が停止してしまった場合、身代金を支払って問題を解決したいと思われるかもしれません。身代金を支払うことには倫理的な問題もありますが、データを取り戻すための効果的な方法でもありません。身代金を支払っても、攻撃者が復元するのは全体のファイルの 3 分の 2 ほどであることを念頭に、費用とその効果について分析してください。

6. **マルウェア攻撃からの復旧計画を準備しておきます。**サイバー攻撃が甚大な侵害をもたらすセキュリティ侵害に発展するのを防ぐには、事前に準備をしてことが最善です。攻撃の被害に遭った多くの企業は、インシデント対応計画を適切に導入していれば、多額のコスト、被害、混乱を回避できたと考えています。

その他の資料

ソフォスのインシデント対応ガイドは、組織がサイバーセキュリティのインシデント対応計画のフレームワークを定義し、計画に追加するべき 10 の重要な対策について説明しています。

セキュリティ対策の担当者の方は、インシデント対応の専門家による 4 つの重要なヒントもご覧ください。サイバーセキュリティインシデントへの対応に関する大切な教訓を紹介しています。

これらの資料は、数千件ものサイバーセキュリティのインシデントに連携して対応してきた Sophos Managed ThreatResponse チームと SophosRapidResponse チームの実際の経験をベースに作成されています。

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ており、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から企業をリアルタイムで保護します。実績のある次世代の先進の機能により、ビジネスデータは、AI と機械学習を活用するソフォスの製品によって効果的に保護されます。

2021-05-05 (SB-NP)

SOPHOS