SOPHOS

サイバー保険とサイバー防衛 2024 年版: IT とサイバーセキュリティ分野のリーダーが伝える教訓

本書では、サイバー保険への加入、保険金の支払い、サイバーセキュリティの防御策と保険適用範囲の関係について、実際に企業を調査して得られた知見を共有します。

ソフォス ホワイトペーパー 2024 年 6 月

はじめに

現実的に、サイバーリスクを避けることはできません。デバイスをインターネットに接続している企業であれば、サイバーリスクを完全に排除することはできません。そのため、リスクを管理する方法が重要となっています。サイバーリスク管理の主なアプローチには、セキュリティ機能を導入し、ユーザーの行動を是正するリスク対策と、サイバー保険によってリスクを移転する対策の 2 つがあります。リスク対策とリスク移転を両輪とすることで、バランスのとれたサイバーリスク管理が可能になりますが、各組織はどのようなバランスを目指すのかを決定していく必要があります。

また、リスク対策とリスク移転は相互に関連しています。セキュリティ機能とユーザーの行動は、サイバー保険によるリスク移転にも直接的な影響があります。強力で効果的なサイバーセキュリティ機能を導入すればサイバーリスクを軽減でき、価格や等級などが有利なサイバー保険に加入して利用できるようになります。逆に、リスク対策が脆弱であれば、必要な要件を満たすサイバー保険を安価に利用できない場合も多くなります。

現在、多くの企業でサイバーリスクは経営幹部レベルの重要課題となっています。本レポートでは、中堅企業のサイバー保険加入に関する現状について、保険への加入を有利するための要因を含めて説明します。本書は、サイバー防御とサイバー保険の関係性についての最新の知見を提供し、セキュリティ防御を向上する投資によって、サイバー保険の加入条件を満たしやすくなり、有利な等級で契約できることについて解説します。また、保険金の請求が拒否される主な理由など、保険金請求の支払いについて調査した結果も公開しています。

5,000 名のリーダーを対象とした独自の調査に基づきます

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。

エグゼクティブサマリー

企業や組織にとって、サイバー攻撃は避けることができない問題となっています。サイバー防御とサイバー保険を組み合わせた包括的なアプローチでサイバーリスクを管理することで、重大なインシデントが発生する可能性を低減しながら、サイバーリスク管理の総所有コスト (TCO) を低減できます。

調査結果が示しているように、セキュリティ機能への投資において、サイバー保険には「アメとムチ」のような働きがあります。保険会社は、保険の適用を受けるための最低限のセキュリティ管理要件を設定しており、事実上、多くの組織にサイバー防御を強化するように求めています。一般的な要件には、多要素認証 (MFA) の導入があります。これは、保険を購入する前提条件となっていることも多くあります。

サイバー保険会社は、同時に、保険料の引き下げ、保険限度額の引き上げ、保険条件の改善などのインセンティブを与えることで、被保険者にリスクを削減するための強力で優れた保護対策や防御機能を認識してもらい、それらの対策を実施する労力に報いています。「アメ」の一例として、MDR サービスを利用する組織に対して、多くの保険会社は、保険適用の範囲を広げ、保険料を削減しています。

この調査では、保険等級を最適化するためにサイバー防衛に投資すると、2 つのメリットが得られることも明らかになりました。企業は、簡単かつ有利な価格で保険適用を受けることができるだけではなく、保護機能の向上、アラートの減少、IT スタッフの時間の解放など、さまざまな利点を報告しています。この結果は、サイバーリスクを削減するための投資を、総合的な対策に組み込んで検討することの重要性を浮き彫りにしています。

調査によって明らかになった懸念の一つは、購入した保険契約が自社のニーズを満たしていない可能性があることです。サイバー保険は投資であり、重大なインシデントが発生した場合、その保険によって必要な補償が得られることを確認しなければなりません。インシデントが発生した場合に最前線で対応にあたる IT チームやサイバーセキュリティチームなど、すべての利害関係者が保険契約の決定に関与し、すべての投資が自社のニーズを満たすことができるようにしなければなりません。

2024 年のサイバー保険の加入状況

この調査では、サイバー保険への加入は、従業員が 100 ～ 5,000 名の組織で広く普及しており、これらの組織の 90% が何らかのサイバー保険に加入していることが確認されました。これらの 50% がスタンドアロン型のサイバー保険契約に加入し、40% がより広範なビジネス保険契約 (一般賠償責任保険など) の一部としてサイバー保険に加入しています。

企業の売上高は、サイバー保険に加入する傾向にはほぼ影響していません。

- 年間売上高が 5,000 万ドル未満の企業の 92% がサイバー保険に加入している (回答者数 =664)
- 年間売上高が 10 億ドル以上の企業の 93% がサイバー保険に加入している (回答者数 =1,907)

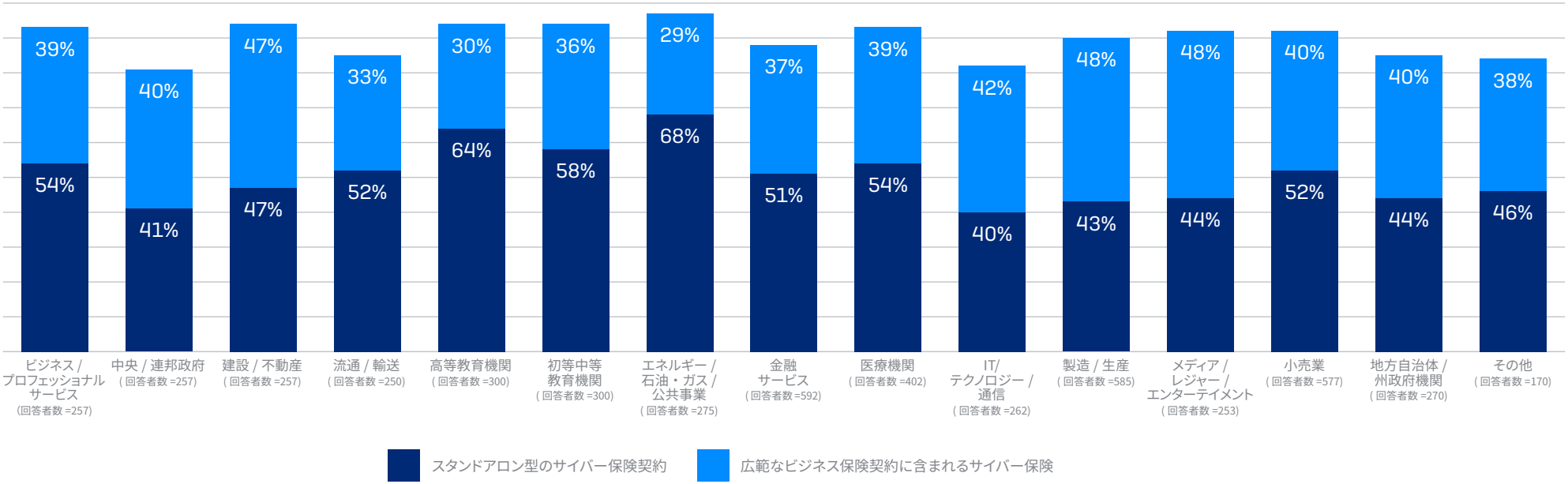
同じように従業員数も保険の加入率にほぼ影響はありません。従業員数別のデータを見ると、最も高い加入率 (従業員数が 100 ～ 250 人の組織で 93%) と最も低い加入率 (従業員数が 1,001 ～ 3,000 人の組織で 88%) の差はわずか 5% しかありません。

業界別の保険加入率

エネルギー、石油・ガス、公益事業は、保険加入率が最も高い業界 (97%) であり、リスク移転のためにスタンドアロン型のサイバー保険契約を利用する割合も最も高くなっています (68%)。これは、これらの業界では厳格な規制が適用されており、インシデントが発生した場合の潜在的な責任の大きさを反映していると考えられます。また、これらの業界では旧式のテクノロジーやインフラが広く使用されていることから、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こともこの原因の一つと考えられます。

*中央 / 連邦政府*の保険加入率は、*IT*、*通信*、*テクノロジー業界*と共に最も引くなっています (両方ともに 81%)。しかし、すべての業界の 5 社に 4 社以上が保険に加入しており、サイバー保険への加入が常識となっていることは明らかです。

業界別のサイバー保険の加入

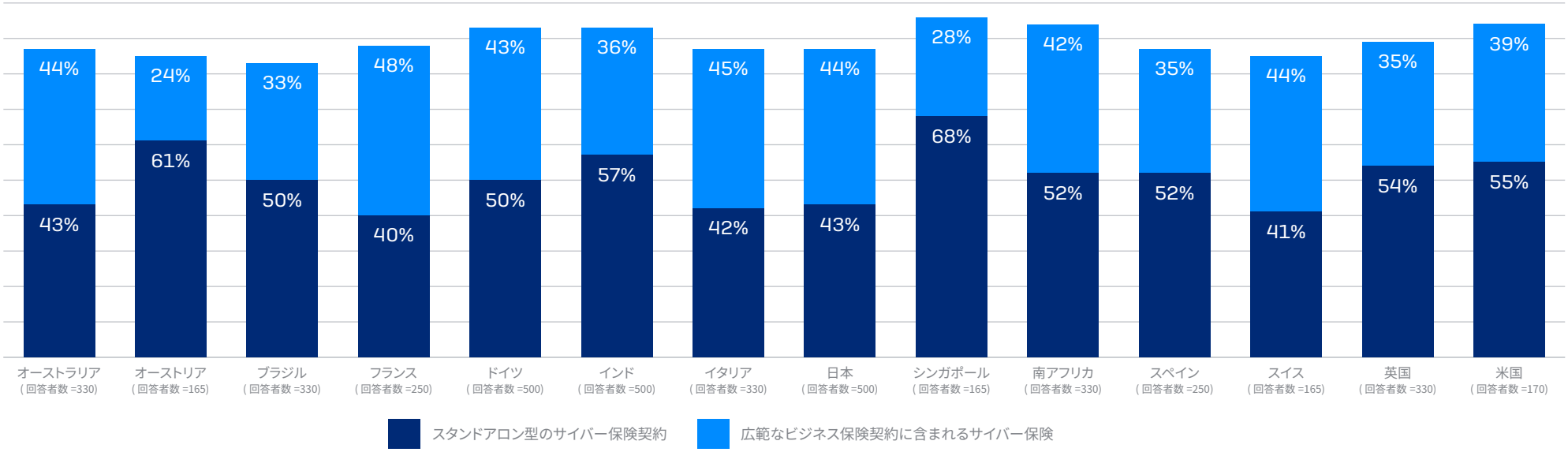


貴社はサイバー保険に加入していますか？はい、スタンドアロン型のサイバー保険に加入しています。はい、より広範なビジネス保険契約 (一般賠償責任保険など) の一部としてサイバー保険に加入しています。回答者数を図内に記載。

国別の保険加入率

調査対象となったすべての国で、サイバーリスクを移転するためにサイバー保険が広く利用されていました。加入率が最も高かったのはシンガポールの回答者 (96%) で、最も低かったのはブラジルの回答者 (83%) でした。また、スタンドアロン型のサイバー保険に加入している割合が最も高かったのはシンガポール (68%) であり、サイバー保険が含まれるパッケージ型のビジネス保険への加入率が最も高かったのはフランスでした (48%)。

国別のサイバー保険の加入



貴社はサイバー保険に加入していますか？はい、スタンドアロン型のサイバー保険に加入しています。はい、より広範なビジネス保険契約 (一般賠償責任保険など) の一部としてサイバー保険に加入しています。回答者数を図内に記載。

サイバー保険への加入を容易にする要因

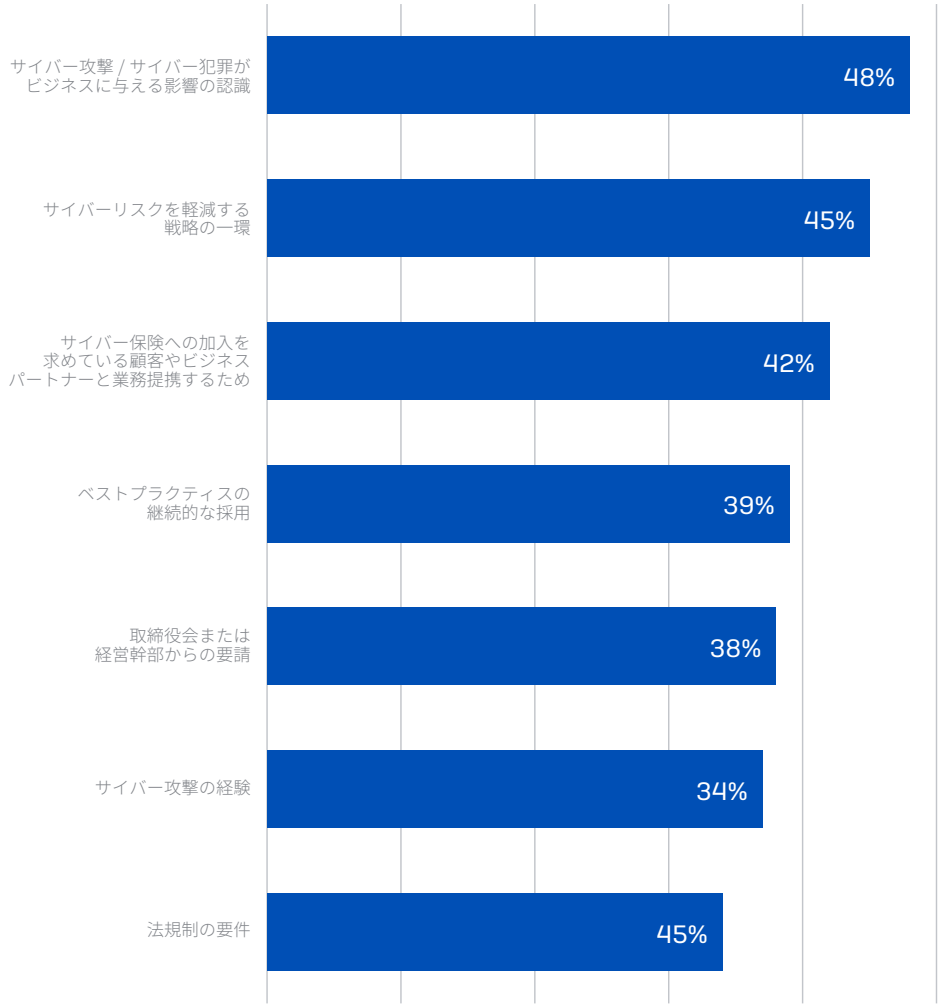
組織がサイバー保険に加入する動機はさまざまですが、*サイバー攻撃やサイバー犯罪が自社に与える影響を認識*していることが、保険を購入する最も一般的な理由であり、回答者の 48% がこの動機を挙げています。回答者の半数近く (45%) が、サイバー保険はサイバーリスクを軽減するための戦略の一部であると回答しています。

第 3 位となった要因は、サイバー保険への加入を求めている顧客やビジネスパートナーと*業務提携*するためでした (42%)。サイバー保険は幅広く業務提携するための条件となりつつあります。これは、取引先がサイバー保険に加入していることを確認し、サプライチェーン攻撃のリスクを軽減することを目的としています。次のページでは、業界別にこれらのデータを掘り下げていきます。

*取締役会または経営幹部からの要請*は、保険を購入した要因の 3 分の 1 以上 (38%) を占めており、サイバーインシデントがビジネスに重大な影響を与えることが広く認識されていることを示しています。 *法規制の要件*は、全体的には保険を購入する最も小さな要因 (34%) になっていますが、業界によってこの数値は大きく変わります。これは、コンプライアンス要件が業界によって異なることを反映しています。

- 最高
  - IT、通信、テクノロジー業界の回答者の 48%
  - エネルギー、石油・ガス、公益事業の回答者の 40%
- 最低
  - 地方自治体の回答者の 25%
  - 建設 / 不動産業界の回答者の 26%

サイバー保険の購入を決定した要因



貴社がサイバー保険への加入を決定した主な要因は何ですか？
回答者数 =4,498 (サイバー保険に加入している組織)

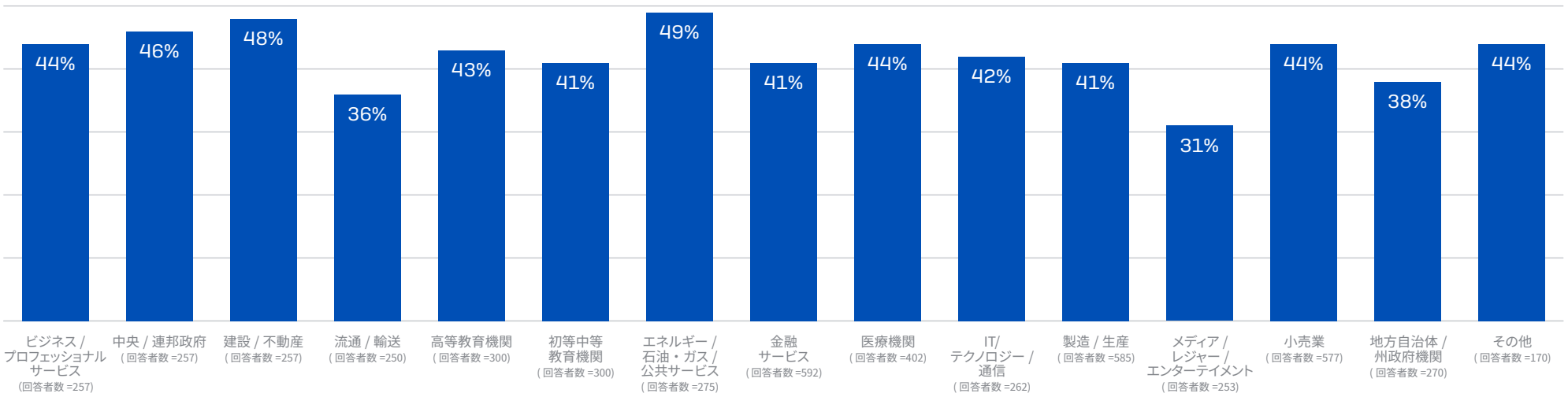
サイバー保険への加入が業務提携の条件

すべての業界において、保険購入の決定に至った要因の 42% は、「*保険加入を求めている顧客やビジネスパートナーと業務提携するため*」でした。このデータを掘り下げてみると、業界によってかなりの差異がありました。

業務提携を保険加入の要因として挙げた回答者の割合が最も高かったのは、エネルギー、*石油・ガス*、公益事業であり (49%)、*建設 / 不動産* (48%) が僅差で続いています。エネルギー / 公益事業では、サイバー攻撃が発生した場合の影響が極めて大きいこと、そして古いテクノロジーを使用しているという課題があることが、顧客や取引先からサイバー保険によってリスクを軽減するように求められている理由と考えられます。

逆に、メディア、レジャー、エンターテイメント業界は、保険の購買意欲が最も低くなっています (31%)、次に低い業界は流通 / 運輸 (36%) でした。攻撃によって物流企業の機能が麻痺すると、商品を配送できなくなり顧客に甚大な影響が発生することを考えると、物流業界のこの調査結果は驚くべきことです。

業務提携の条件としての保険 (業界別)



貴社がサイバー保険への加入を決定した主な要因は何ですか？サイバー保険への加入を求めている顧客やビジネスパートナーと業務提携するため。
回答者数 =4,498 (サイバー保険に加入している組織)

保険の適用範囲

サイバーインシデントが発生した場合、加入している保険によって何が補償されるのかを質問したところ、回答者は保険金を請求した場合、どのような支援を受けられるのかを把握していないケースが多いことがわかりました。

具体的には、サイバー保険に加入している回答者の 40% が身代金の支払いが補償されると考えているが確信が持てず、回答者の 41% が保険により収益損失について補償されると 考えているが確信が持てないと述べています。

これらの調査結果から、組織が以下のいくつかの懸念を抱えていることが明らかになりました。

1. **必要な補償を受けられないリスクがある。**企業のすべての関係者がサイバー保険に何を求めるのかを明確にし、購入する保険がそれらのニーズを満たしていることを確認することが不可欠です。
2. **保険請求が発生した場合に必要とするサポートを受けられないリスクがある。**大規模なサイバーインシデントが発生した場合には、対応に追われ、関係者全員がストレスとプレッシャーのかかる時間を過ごすことになります。攻撃が発生しているときに必要な支援が保険契約に含まれていないことが判明すると、修正の作業がさらに複雑化し、遅延やコスト増につながる恐れがあります。

保険の適用範囲が明確になっていない一部の原因は、保険を購入する担当者 (通常は、財務やコンプライアンスチーム) と、重大なインシデントが発生した場合に最前線で対応する担当者 (通常は IT およびサイバーセキュリティ部門) が断絶されていることです。組織は、購入する保険を決定するときに、すべての利害関係者を必ず関与させ、すべての関係者が保険の適用範囲を確認しなければなりません。共通の認識を形成しておくと、チームはギャップに対処するための代替案を講じることが可能になります。

ランサムウェアは、現在の企業が直面している最大のサイバー脅威の一つであり、被害を受けた場合、経済的に深刻な影響を受けることになります。身代金支払いの平均値（中央値）は現在 200 万ドルに達しており、身代金を除く全体的な復旧費用は 273 万ドルとなっています (出典：ランサムウェアの現状 2024 年版、ソフォス)。10 社に 1 社の組織が、身代金の支払い、侵害に関する通知、サイバー攻撃者との交渉、収益損失への補償など、ランサムウェア攻撃で発生する費用の多くを補償の適用外としている保険に投資していることは驚くべきことです。

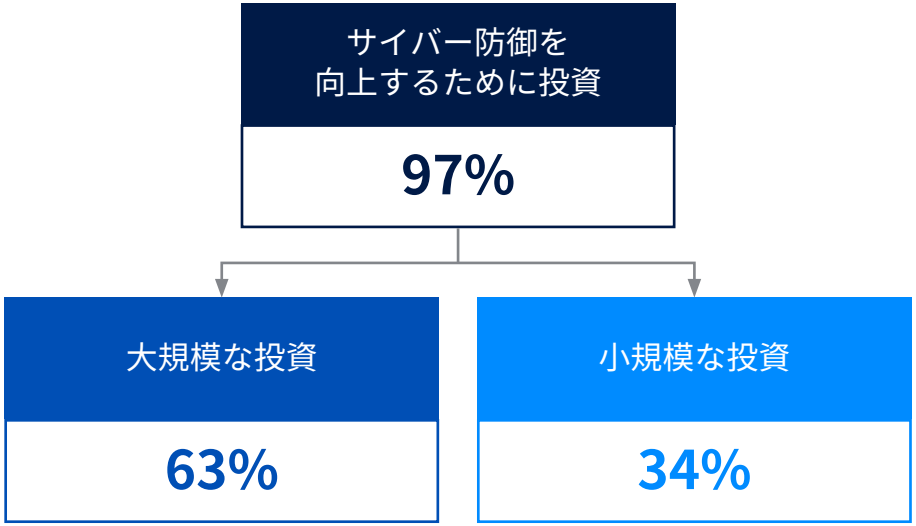
保険の適用範囲

	身代金の支払い	データ復旧サービス	侵害の通知	広報支援/レピュテーションマネジメント (評判管理)	インシデント対応のサポート	サイバー攻撃者との交渉	収益損失への補償	コンピューターシステムの修復
保険の適用範囲であることを把握している	50%	58%	47%	47%	54%	48%	49%	55%
保険の適用範囲であると考えているが、確信が持てない	40%	35%	43%	42%	38%	42%	41%	38%
保険の適用範囲外であることを把握している	10%	7%	9%	11%	8%	10%	10%	7%
わからない	0%	0%	0%	1%	0%	1%	0%	0%

自社が加入しているサイバー保険は、サイバーインシデントが発生したときにどのような補償を行いますか？回答者数 =4,498 (サイバー保険に加入している組織)

サイバー保険とサイバー防衛への投資

昨年サイバー保険に加入した組織の 97% が、保険等級を最適化するために防御対策を改善するための投資を行ったと回答しました。ほぼ 3 分の 2 (63%) がサイバー防御を向上するために大規模な投資を行ったと回答し、34% は小規模な投資を行ったと回答しました。



昨年サイバー保険に加入した場合、サイバー保険の等級を最適化するために、サイバー防御を向上するための投資を行いましたか？回答者数 =4,498。

業界別のサイバー保険とサイバー防衛への投資

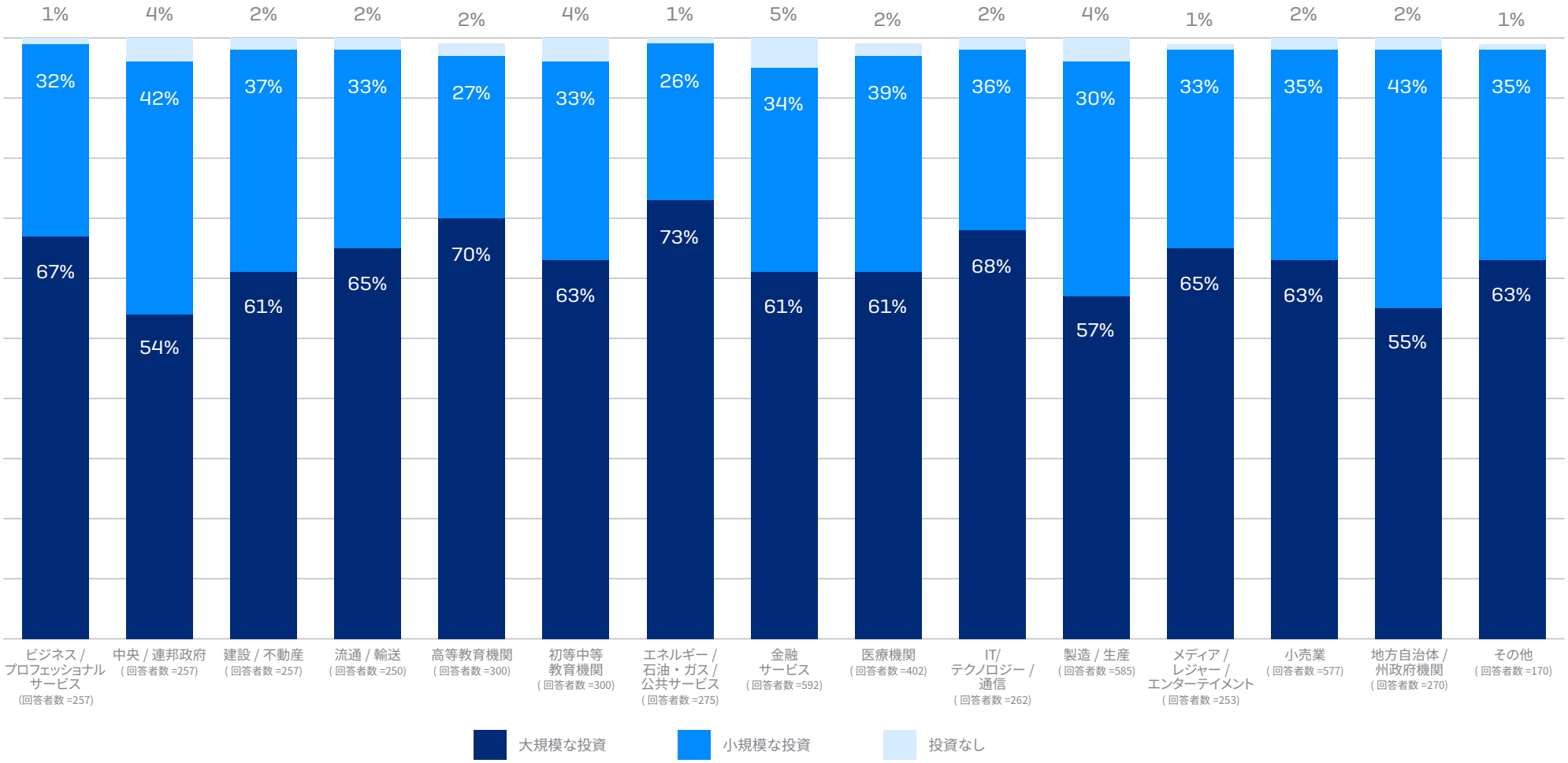
保険を購入したほぼすべての組織が、有利な条件で保険契約を行うために、防御を向上するための投資を行っていますが、投資の規模についても業界によって異なっています。

保険等級を最適化するためにサイバー防御に大規模な投資を行ったと述べた回答者の割合は、*エネルギー、石油 / ガス、公益事業*が最も高くなっていました (73%)。これは、旧式のテクノロジーが多く使用されていることや、重要インフラの稼働が停止した場合の影響が大きいことから、この業界がサイバーセキュリティ対策に苦慮していることを反映していると考えられます。

大規模な投資を行っていると回答した割合が次に高かった業界 (70%) は、*高等教育機関*でした。高等教育機関は、サイバー防衛への投資が十分ではなく、攻撃を受ける可能性も高い業界です。

中央 / 連邦政府と州政府 / 地方自治体の 2 つの政府機関は、防衛に大規模な投資を行った割合が最も低くなっています (*中央 / 連邦政府*では 54%、*州政府 / 地方自治体*では 55%)。政府予算が逼迫しており、これらの政府機関への予算の交付が減少していることが理由の一つとして考えられます。

業界別のサイバー保険とサイバー防衛への投資



サイバー保険に昨年加入したときに、サイバー保険の等級を最適化するために、サイバー防御を改善するための投資を行いましたか？回答者数を図内に記載。

サイバー防衛への投資がサイバー保険等級に与える影響

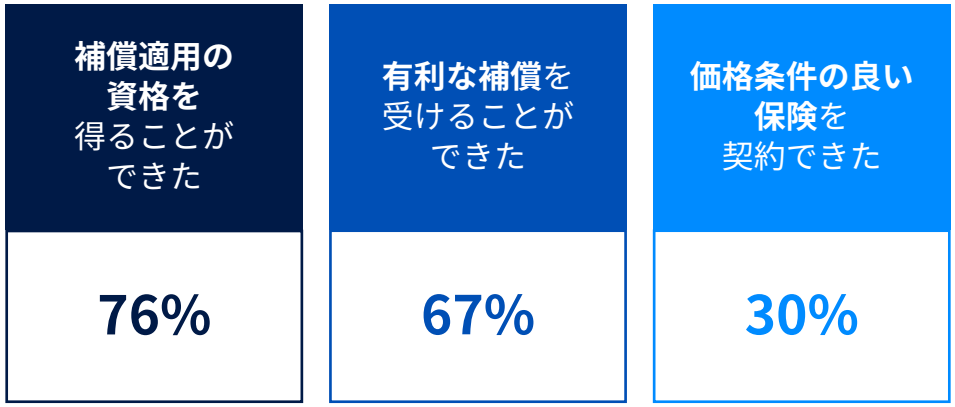
サイバー防衛への投資を検討している組織にとって良いニュースがあります。サイバー防御の向上に投資したほぼすべての企業が、サイバー保険の等級にプラスとなる影響があったと回答しています (回答者 4,370 人中の 4,351 人がそのように回答しており、全体の 99.6% にあたります)。

これは、防御を強化するサイバー保険の「ムチ」の役割を明確に示しており、回答者の 4 分の 3 以上 (76%) が、セキュリティ対策を強化するための投資によって、これまで対象ではなかった保険に加入できたと答えています。

また「アメ」の効果についても見ていきましょう。サイバー防御への投資により、3 分の 2 の組織が価格条件の良い保険 (例えば、保険料や免責金額の低下) を利用できるようになり、30% の組織は、より良い条件 (例えば、より高い補償限度額) で保険を契約できるようになったと回答しています。

これらの数字は、サイバーリスクを削減するための戦略を進めるときに、全体的な総所有コスト (TCO) を考慮することが重要であることをしています。**防御を向上するための投資は、サイバー保険費用の節約を可能**にしながら、重大なサイバーインシデントの影響を受けるリスクも低下させます。

サイバー防衛への投資の影響

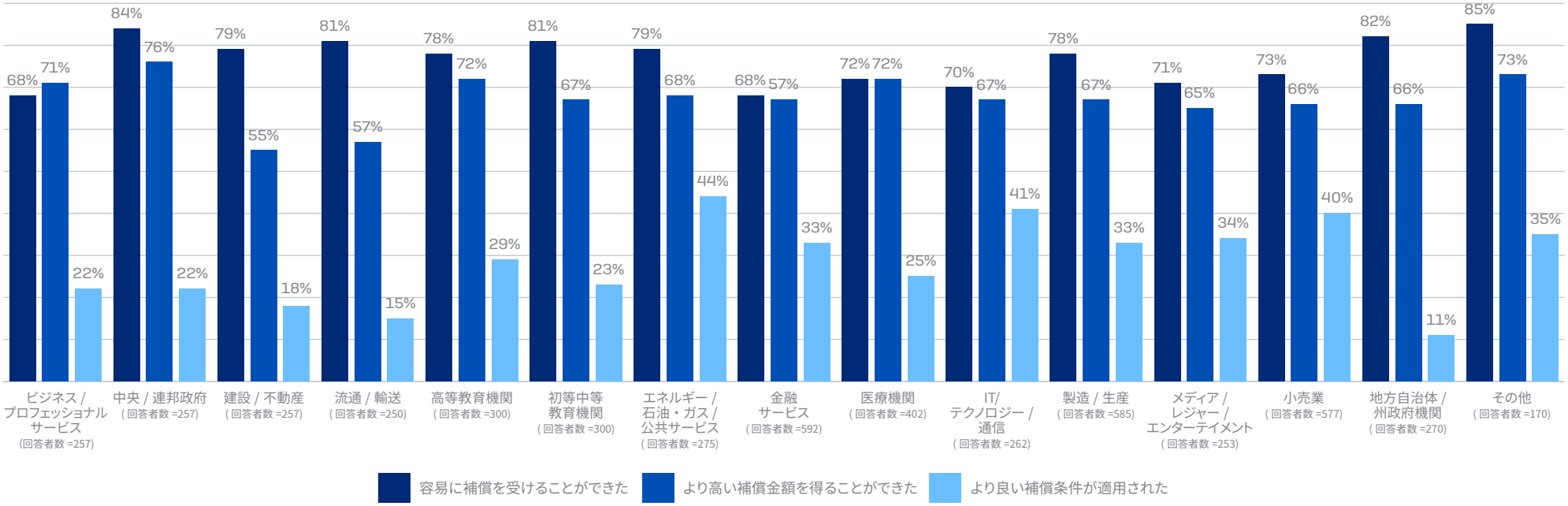


サイバー防御を向上するために投資したことで、保険等級にどのようなプラスの影響がありましたか？回答者数 =4,370。サイバー防御の向上に投資し、サイバー保険等級を最適化した組織

業界別のサイバー防衛への投資の影響

すべての業界で、サイバー防衛への投資による保険への大きな効果が確認されています。効果が見られなかった業界はありませんでしたが、*中央政府 / 連邦政府*は、サイバー防御を向上したことで、保険の適用範囲が広がったと述べた回答者の割合が最も高く (84%)、また、有利な価格で保険の適用を受けることができたと最も多く回答した (76%) 業界です。*エネルギー、石油・ガス、公益事業*は、サイバー防御への投資によって有利な補償条件で契約できたと述べた回答者の割合が最も高くなっています (44%)。

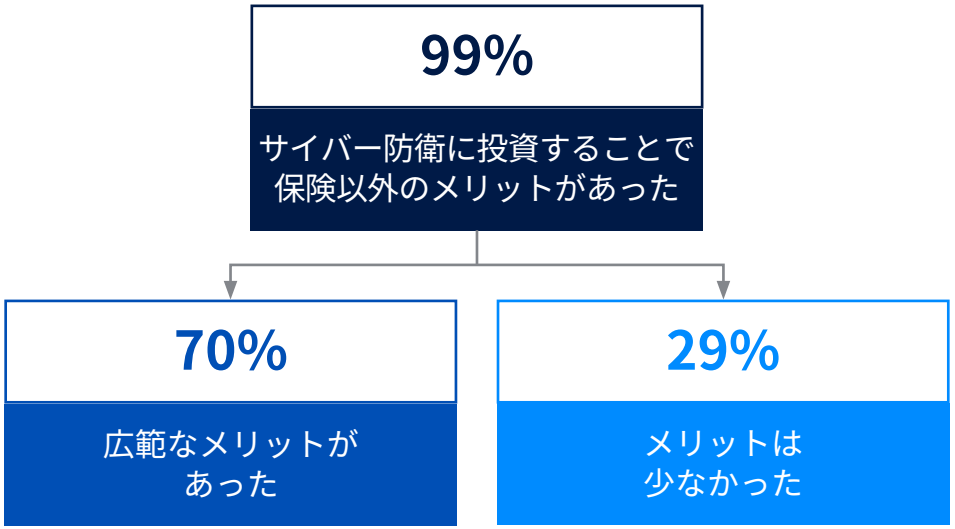
業界別のサイバー防衛への投資の影響



サイバー防衛の向上に投資したことで、保険等級にどのようなプラスの影響がありましたか？回答者数を図内に記載。

サイバー防御への投資による広範な影響

組織がサイバー防御の向上に投資した場合、保険に関する大きなメリットを享受しているだけではありません。回答者の 99% が、サイバー防御の改善、アラートの減少、IT スタッフの時間の確保など、より広範なメリットを報告しています。このデータを深く掘り下げると、70% の回答者がサイバー防御を向上することで幅広い分野で多くのメリットを得たと述べており、29% の回答者がわずかなメリットしか得ていないと述べています。



サイバー保険の加入条件を考慮してサイバー防御の向上に投資したことで、その他の分野でプラスの影響がありましたか？ 回答者数 =4,370。サイバー保険等級を最適化するために防御の向上に投資した組織。

すべての業界が、投資によって広範かつ大きなメリットが得られたと報告していましたが、エネルギー、石油・ガス、公益事業が、このように報告した割合が最も高くなっていました (82%)。逆に、製造と生産業界では、広範かつ大きなメリットがあったと報告する割合が最も低くなっていましたが、この業界でも 3 分の 2 近くの組織 (63%) が大きなプラスの影響があったと回答しています。

条件の良い保険に加入しやすくなるだけでなく、サイバーセキュリティのリスクも軽減できるという広範なメリットがあることは、サイバー防衛の向上を目指す組織にとって二重の喜びになっています。

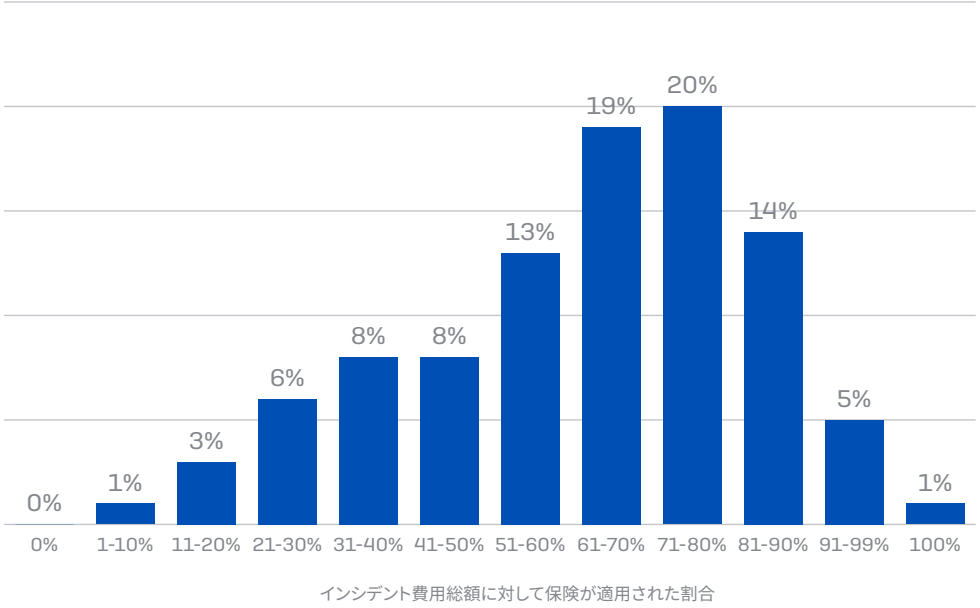
保険が適用される費用の割合

組織は、サイバー保険によってリスクを移転でき、最悪の事態が発生した場合でも、インシデント対応にかかるすべての費用を負担しなくても済むという安心感を得ることができます。

今回の調査結果から、保険会社がほぼすべてのケースで何らかの形で保険金を支払っていることが明らかなりましたが、サイバー保険に投資している組織にとってこの結果は安心材料となるのではないでしょうか。保険会社から保険金が全く支払われなかったと述べた回答者は全体で 1 社だけでした。

同じように、保険会社がインシデントの修復にかかる費用を全額負担することはほぼありません。保険会社が発生した費用の全額を負担したと述べた回答者は 1 % でした。全体的には、保険会社は通常、インシデントの費用総額の 63% を支払っており、保険の返戻率は 71 ～ 80% でした。

保険の支払いがインシデントの総費用に占める割合



過去 1 年間に貴社がサイバー保険の保険金を請求したときに、保険が適用されたインシデント対応の費用は総額の何パーセントでしたか？ 回答者数 =3,945

費用の全額が適用されない理由

インシデントの対応にかかる費用の全額が保険によって補償されなかった理由は、今後保険に加入するときに有益な情報となります。

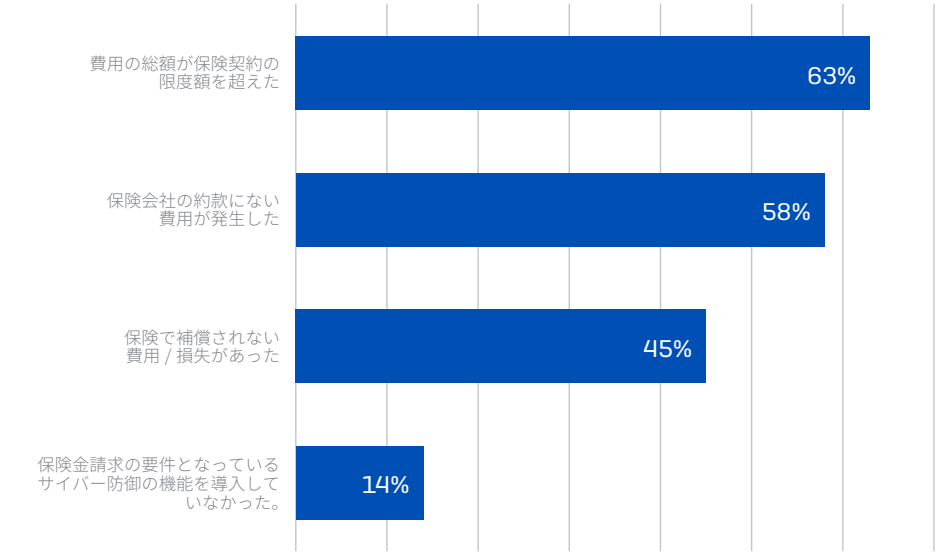
復旧にかかる費用の請求額が全額支払われなかった最も一般的な理由は、*費用の総額が保険契約の限度額を超えた*というものでした (63%)。現在、ランサムウェア攻撃によって受けた影響を修復するための平均コストは 273 万ドルに達しており、大規模なインシデントが発生した場合に契約している保険によって十分な補償が提供されることを確認しておく必要があります。

2 番目に多かった理由は、*保険会社の約款にない費用が発生した*というもので、58% の回答者がこの理由を挙げています。自社が契約している保険の要件と、保険金の請求が認められるために必要なプロセスを確認しておくことをお勧めします。

回答者の 45% が、*保険で補償されない費用や損失があった*と述べています。サイバー攻撃の被害を受けた回答者の約半数がこの理由を報告していることから、保険の対象と企業の要件のミスマッチが広く発生していることがうかがえます。

拒否された保険金申請の 14% (7 件に 1 件) は、*申請が承認されるために必要なサイバー防御を組織が実施*していなかったことが原因でした。保険会社は、保険金を適用する条件として、実施すべきセキュリティ管理を規定しています。これらの条件には、脆弱性に定期的にパッチを適用すること、サポートが終了しているソフトウェアを実行しないこと、EDR ソリューションを導入することなどがあります。これらの要件を順守していなければ、保険を契約していても十分な補償が得られないリスクがあります。

サイバー保険でインシデント費用の全額が補償されなかった理由



貴社のサイバー保険でインシデント費用の全額が補償されなかったのはなぜですか？
回答者数 =3,886。保険会社から請求の全額が補償されなかった組織

ランサムウェア攻撃を受けたときのサイバー保険の補償による影響

保険に加入する目的は、リスクが現実となった場合に組織が受ける影響を軽減することです。この目的と結果を調べるため、ソフォスが公開した「ランサムウェアの現状 2024 年版」の調査結果を分析し、組織がランサムウェアの被害を受けた場合の 5 つの重要な領域を中心に、保険の加入状況と結果にどのような相関関係があるかを確認しました。

- ランサムウェア攻撃を受けた割合
- データが暗号化された割合
- 身代金額
- 暗号化されたデータを復旧するために、身代金を支払った割合
- 全体的な復旧コスト（身代金支払いを除く）

この分析を参照する前に注意していただきたいのは、***ランサムウェア攻撃を受ける前に現在の保険に加入したのか、ランサムウェア攻撃を受けた後に加入したのか***が不明であり、ランサムウェア攻撃を受けたために保険を契約したのか、攻撃を受ける前にすでに加入していたのかがわからないことです。しかし、「ランサムウェアの現状」の調査に参加された組織がサイバー保険に加入している割合は、2024 年の調査では 90%、2023 年の調査では 91% と過去 2 年間で一定しており、これらのデータはこの分野の調査を進めるための合理的な指標として利用できると考えられます。

ランサムウェア攻撃を受けた割合

このデータでは、サイバー保険への加入の有無は、ランサムウェア攻撃を受ける割合にほぼ影響を与えておらず、以下の 3 つのグループとも過去 1 年間に攻撃を受けた割合はほぼ同じでした。

- スタンドアロン型のサイバー保険に契約している回答者の 62% が、昨年ランサムウェアの被害を受けた (回答者数 =2,523)
- 広範なビジネス保険契約の一部としてサイバー保険に加入している回答者の 57% が、昨年ランサムウェアの被害を受けた (回答者数 =1,975)
- サイバー保険に加入していない回答者の 58% が、昨年ランサムウェアの被害を受けた (回答者数 =489)

データが暗号化された割合

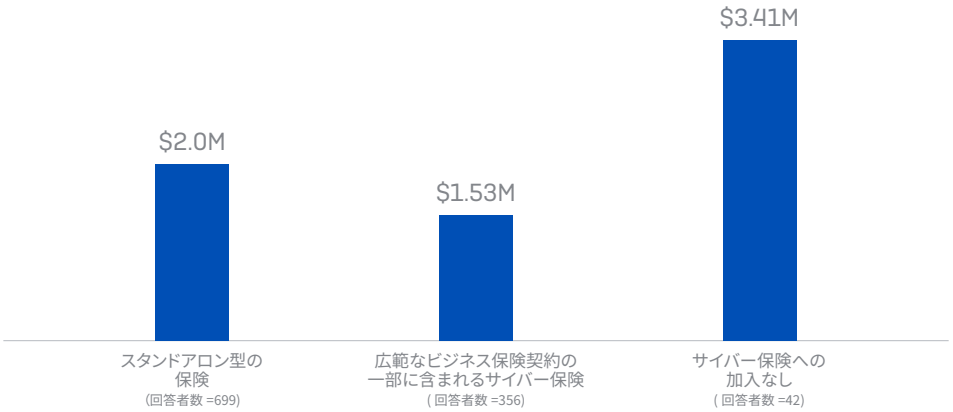
保険に加入している組織は、加入していない組織よりもデータが暗号化される可能性が高くなっていましたが、攻撃によってデータが流出する可能性は低くなっています。

- スタンドアロン型の保険に加入している回答者の 74% でデータが暗号化され、23% でデータが流出した (回答者数 =1,560)
- 広範なビジネス保険契約の一部としてサイバー保険に加入している回答者の 68% でデータが暗号化され、41% でデータが流出した (回答者数 =1,127)
- サイバー保険に加入していない回答者の 52% でデータが暗号化され、61% でデータが流出した (回答者数 =284)

身代金額

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よりも身代金の平均支払額が低くなっています。サイバー保険に加入していない場合の身代金支払額の中央値は 341 万ドルであり、スタンドアロン型の保険に加入している場合の 200 万ドル、広範なビジネス保険契約の一部としてサイバー保険に加入している場合の 153 万ドルを大幅に上回っていました。

身代金の平均支払い額



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。回答者数を図内に記載。

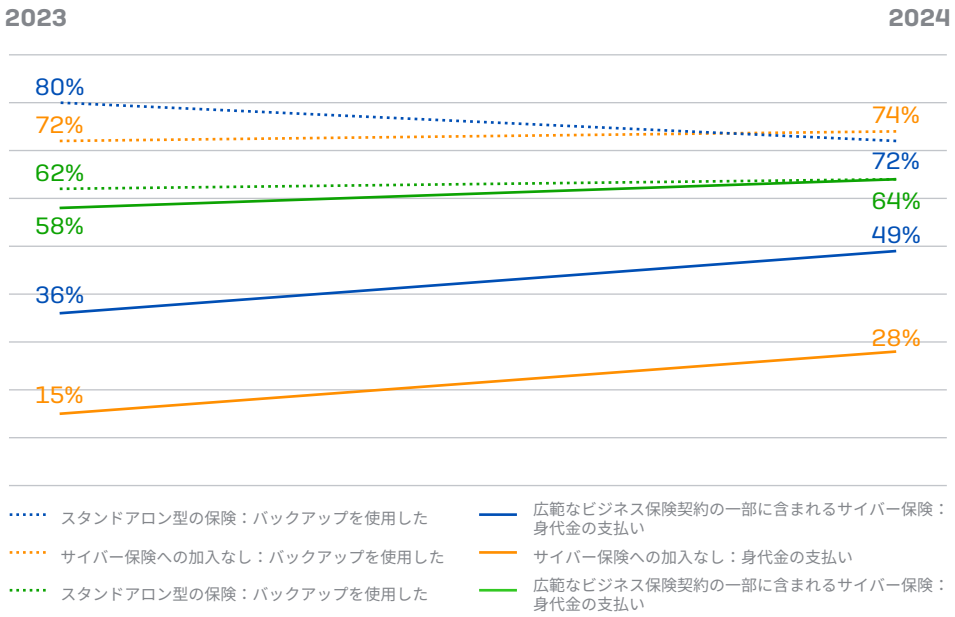
暗号化されたデータを復旧するために、身代金を支払った割合

調査結果のデータは、保険に加入している場合、データを取り戻すために身代金を支払う傾向が高くなることを示しています。スタンドアロン型の保険を契約している場合、身代金を支払う割合が最も高く、サイバー保険に加入していない場合と比較して身代金を支払った割合が 2 倍以上になっています (64% 対 28%)。スタンドアロン型の保険を契約しているグループは、暗号化されたデータを復元するためにバックアップを使用するよりも身代金を支払った割合が高かった唯一のグループでもありました。

身代金を支払ってデータを取り戻した割合

64%	49%	28%
スタンドアロン型のサイバー保険に加入	**広範なビジネス保険契約の一部に含まれるサイバー保険**	**サイバー保険への加入なし**
(回答者数 =744)	(回答者数 =375)	(回答者数 =42)

2024 年の調査では、3 つのグループすべてが身代金を支払う割合が 2023 年よりも高くなったと回答しています。スタンドアロン型の保険に加入しているグループやサイバー保険に加入していないグループも、暗号化されたデータを復旧させるためにバックアップを使用する頻度が昨年よりも高くなったと回答しています。



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た。はい、バックアップを使用してデータを復元した。 回答者数 =2,072 (2024 年)、1,497 (2023 年)。注：データを復元するために複数の方法を使用した場合、両方の選択肢を選ぶことができます。

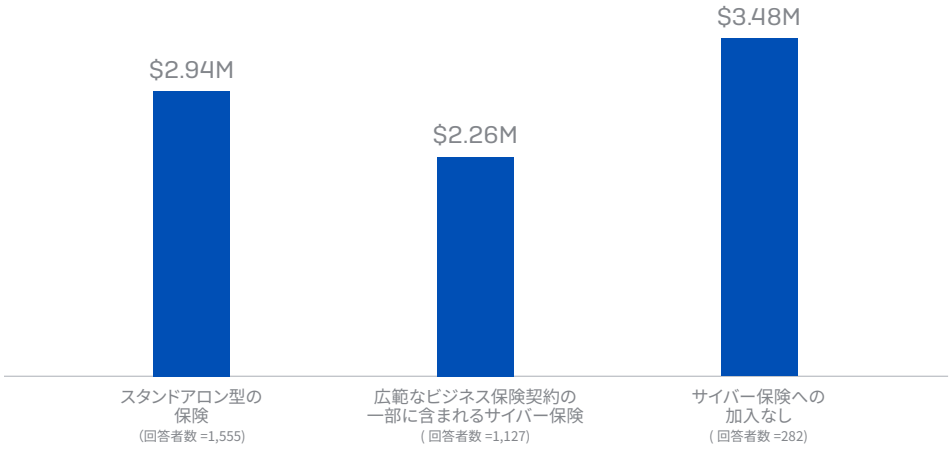
このデータから、サイバー保険、特にスタンドアロン型の保険に加入していると、身代金を積極的に支払っているように見えるかもしれませんが、保険への契約が身代金を支払う前か後かは不明であることに注意してください。身代金を支払って財務的に窮地に陥った組織が、スタンドアロン型の保険に加入することを選択した可能性もあります。また、保険契約から身代金の資金が拠出されたために、身代金を支払うことができた可能性もあります。

復旧費用の総額

身代金の支払いは、復旧費用の一部に過ぎません。身代金を支払ったかどうかに関わらず、侵害について通知するコスト、取引不能になることによる機会損失のコスト、修復作業を担当するスタッフの時間など、いくつもの要因が全体的な財務的影響に関連します。

ランサムウェア攻撃の影響を復旧するためのすべての回答者の推定コストの平均値は 273 万ドルでした。調査結果のデータから、すべての組織がランサムウェア攻撃によって金銭的に大きな影響を受けていることがわかりますが、保険に加入していない組織は最も大きな影響を受けています。

ランサムウェアの復旧費用の総額 (身代金支払いを除く)



最も深刻なランサムウェア攻撃を受けた影響において、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 =2,964。回答者数を図内に記載。

繰り返しになりますが、今回の分析データは、この分野の調査をさらに進めるためのベースとして考える必要があります。多くの組織がサイバー保険に加入し、ランサムウェア攻撃を受けていることから、保険への加入がランサムウェア攻撃の経験にどのような影響を及ぼしているのかをさらに深く掘り下げることは有益となるはずです。

結論

現在、サイバー保険への加入はサイバーリスクを軽減するための多くの重要な戦略の一部になっています。サイロ型のソリューションから、サイバー防衛とサイバー保険の相互作用を活かした包括的なサイバーリスク管理に移行することが求められています。サイバー防御を向上するための投資をスマートに行うことで、サイバー保険に関する費用を大幅に削減しながら、幅広い業務上のメリットを享受し、攻撃を受けるリスクを軽減できます。

サイバー防御の要件については、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。

2024-06-17 (WP-DD)

SOPHOS