KEEPER
Cybersecurity Starts Here®

2022年
米国サイバーセキュリティ国勢調査レポート

序文

現在、サイバーセキュリティは米国企業の最優先事項として認識されています。しかし、サイバーセキュリティの脅威はリスクとして進化しており、それらを軽減するために必要な対応は急速に変化しています。攻撃者の一歩先を行くことは絶え間ない挑戦ですが、企業はそうした意図にもかかわらず、必ずしもペースを保っているわけではないのです。

この課題を解決するには、ITリーダーたちが理由を理解しなければなりません。ITリーダーは以下のような質問への答えを求めています。サイバーセキュリティはどのように変革しているのか？サイバー攻撃は企業にどのような損害を与えているのか？予防のためのトレーニングやツールへの投資の焦点はどこに置くべきか？リーダーはサイバーセキュリティを優先しているのか？そして、サイバーセキュリティは組織文化にどのように適合しているのか？

このような疑問に答えるために、Keeper SecurityはSapio Researchと提携し、米国内のIT意思決定者516人の行動や態度を分析しました。Keeperによる2度目の米国サイバーセキュリティ国勢調査であるこのレポートは、こうした専門家の洞察に基づいて、サイバーセキュリティの変革の状況をマッピングしています。

このレポートは、企業が直面する脅威をフォレンジック評価し、脅威を克服するために必要な緊急戦略についての詳細をリーダーに提供するものです。

概要

Keeperによる2度目の米国サイバーセキュリティ国勢調査で得られた4つの重要な留意事項

米国の平均的な企業が経験するサイバー攻撃は年間42回

サイバー攻撃は、米国内におけるあらゆる規模や業種の企業に深刻な影響を与えています。その結果、企業は組織や財務、評判への深刻なダメージに苦しんでいるのです。ITリーダーは、この猛攻撃が来年中に激化すると予想しています。回答者の大半は、サイバー脅威から組織を守る準備ができていると回答しています。しかし、回答者の圧倒的多数は過去1年間にサイバー攻撃による被害も経験しており、こうした被害の多くはコストのかかるものでした。

米国のITリーダーの57%が、サイバー攻撃への対応に時間がかかっていると回答

回答者の圧倒的多数が、サイバー攻撃から身を守るためのスキルやサイバーセキュリティソリューションが組織内に備わっていると回答しています。しかし、回答者の大半は、サイバー攻撃を特定し対処するためにチームが費やした時間が過去12ヶ月間で増加したと答えています。また、回答者は、リモートワークやハイブリッドワークによるセキュリティ上の影響や外部脅威の高まり、認証情報がソースコードにハードコード化されていることに対して深い懸念を表明しています。

米国企業の71%が、過去1年間にサイバーセキュリティ分野で人材の新規採用を実施

サイバーセキュリティは組織の経営幹部にとって重要ではないと回答したのは、回答者のわずか3%でした。この認識は、ほとんどのITリーダーにとって健全な予算へと転換していますが、大多数の組織がサイバーセキュリティへの十分な投資を行っていない可能性があり、脅威の進化のスピードがすべての組織の対応能力を凌駕している可能性があります。経済がますます不安定になる中、ITリーダーや多方面のビジネスリーダーは常に気を引き締め、必要不可欠なサイバーセキュリティソリューションや戦略、スキルセットを確実に身につけることに専念しなければなりません。

米国のITリーダーの48%が、サイバー攻撃を認識していたにもかかわらず口外しなかったと回答

関連する機関にサイバー攻撃を報告することになると、透明性の欠如が懸念されています。回答者の半数近くが、サイバー攻撃について認識していたと回答していますが、その情報は隠していたのです。これは、ITリーダーが攻撃について開示することに不安を感じるという、はるかに大きな文化的課題を暗示しています。重要なデータを保護できるソリューションと並行して、組織は透明性と説明責任の文化を培うと同時に、攻撃を報告した従業員を過度に非難したり罰したりしないことが求められます。これにより、事業体がサイバー脅威について完全に理解し、適切に対応できるようになるのです。

セクション1

サイバー攻撃

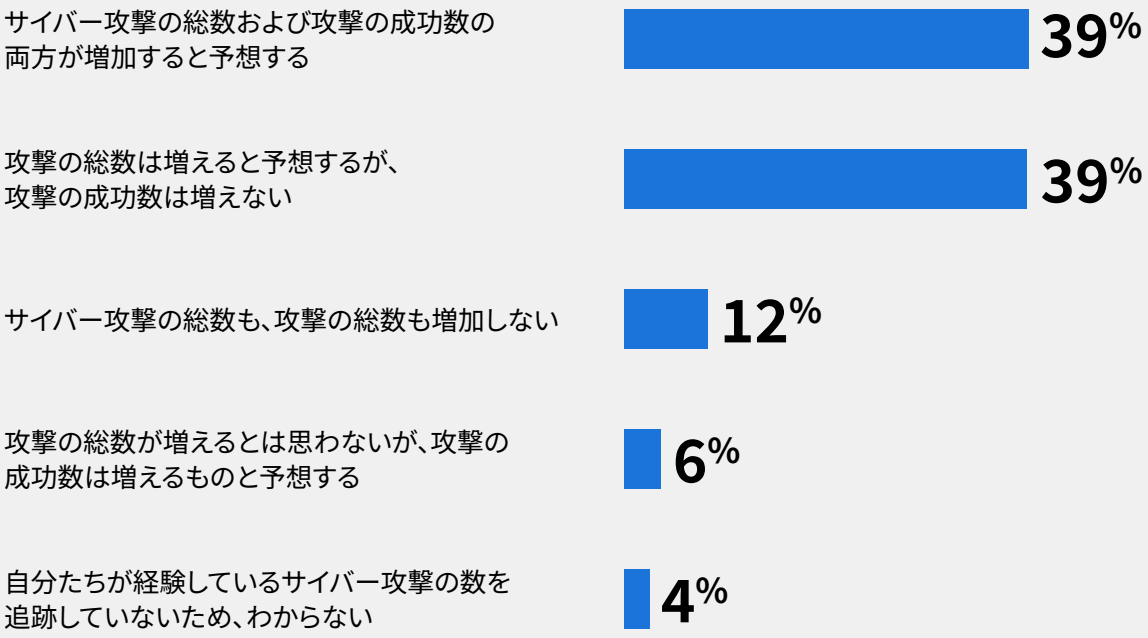
サイバー攻撃は増え続ける脅威を呈する

米国企業は毎年膨大な数のサイバー攻撃に直面しており、そのせいで組織は大きな影響を受けています。

平均的な米国企業は年間42回のサイバー攻撃を受けています。つまり、毎月3、4回ということになります。5分の1以上（22%）が毎年251件以上の攻撃を受けており、12%は毎年500件以上の攻撃を経験しているのです。

このような中、平均的な米国企業は毎年約3回のサイバー攻撃に直面しているのです。回答者の圧倒的多数が、来年にかけて攻撃の総数が増加すると考えており、39%がサイバー攻撃の成功数も増加すると予想しています。

ITリーダーはサイバー攻撃の数（成功数と総数）が今後12ヶ月間でどう変動すると予想しているのか



ほとんどの組織はサイバー攻撃に備えていると回答しています。しかし...

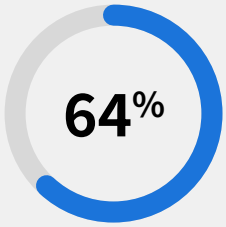
米国のほとんどの組織は、サイバー攻撃を未然に防ぐ準備ができていると回答しています。回答者の64%は準備状況について10ポイント満点のうち少なくとも8ポイント以上だと評価しており、28%は自身の準備状況は10点満点だと評価しています。自信を5ポイント以下だと評価したのは18%のみでした。しかし、他の組織の準備状況を評価する際、回答者はそれほど寛大ではなかったため、米国企業に少なくとも8/10以上の評価を与えてた回答者は48%にとどまりました。

しかし、次のサブセクションにもあるように、損失は増え続ける一方で、攻撃に対処する時間は増加しています。回答者の大多数（57%）が攻撃への対応に時間がかかっていると回答しており、反応が速くなっていると回答したのはわずか8%です。

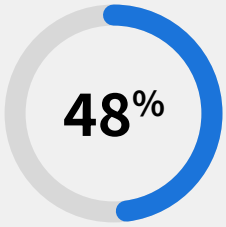
Darren Guccione、Keeper Security、CEO兼共同創業者

この調査は、サイバー攻撃が深刻な脅威を呈していることを実証しています。投資や教育、文化の変革といった予防策は、企業が回復力を高めると共にサイバー犯罪者から自社組織を保護するために不可欠です。

あなたの事業では、サイバー攻撃を回避する準備がどの程度整っていますか？他の米国企業はどの程度の準備ができていると思いますか？

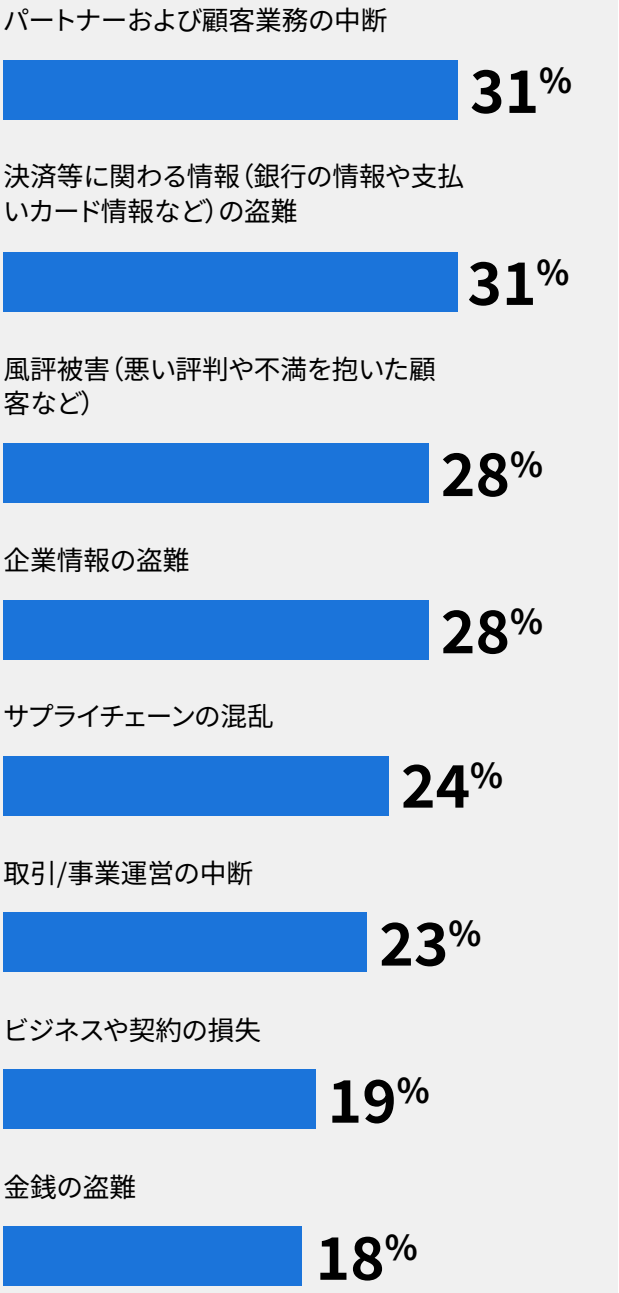


自分の事業は準備ができている
（少なくとも8/10



他の企業は準備できている
（少なくとも8/10）

サイバー攻撃の被害に遭ったことで、自分の事業に降りかかったことは次のうちどれですか？

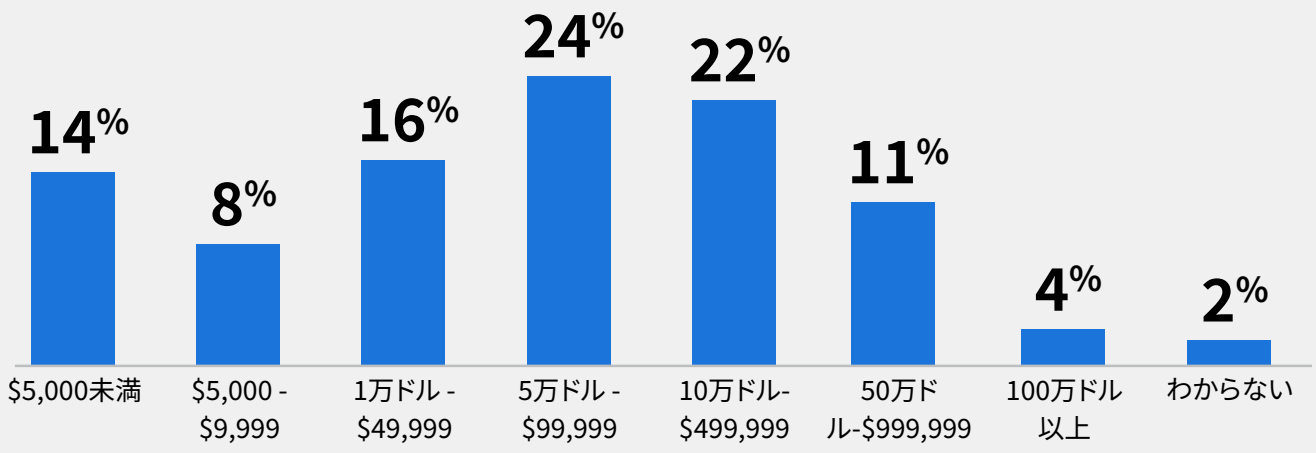


サイバー攻撃は企業に重大な損害を与えている

サイバー攻撃が成功すると、企業は深刻なダメージを受ける可能性があります。回答者の3分の1近く（31%）がサイバー攻撃を受けたことでパートナーや顧客との業務が中断されたことがあると回答しており、同じ割合の回答者が金融情報の盗難を経験、そして18%は金銭の盗難も経験しています。

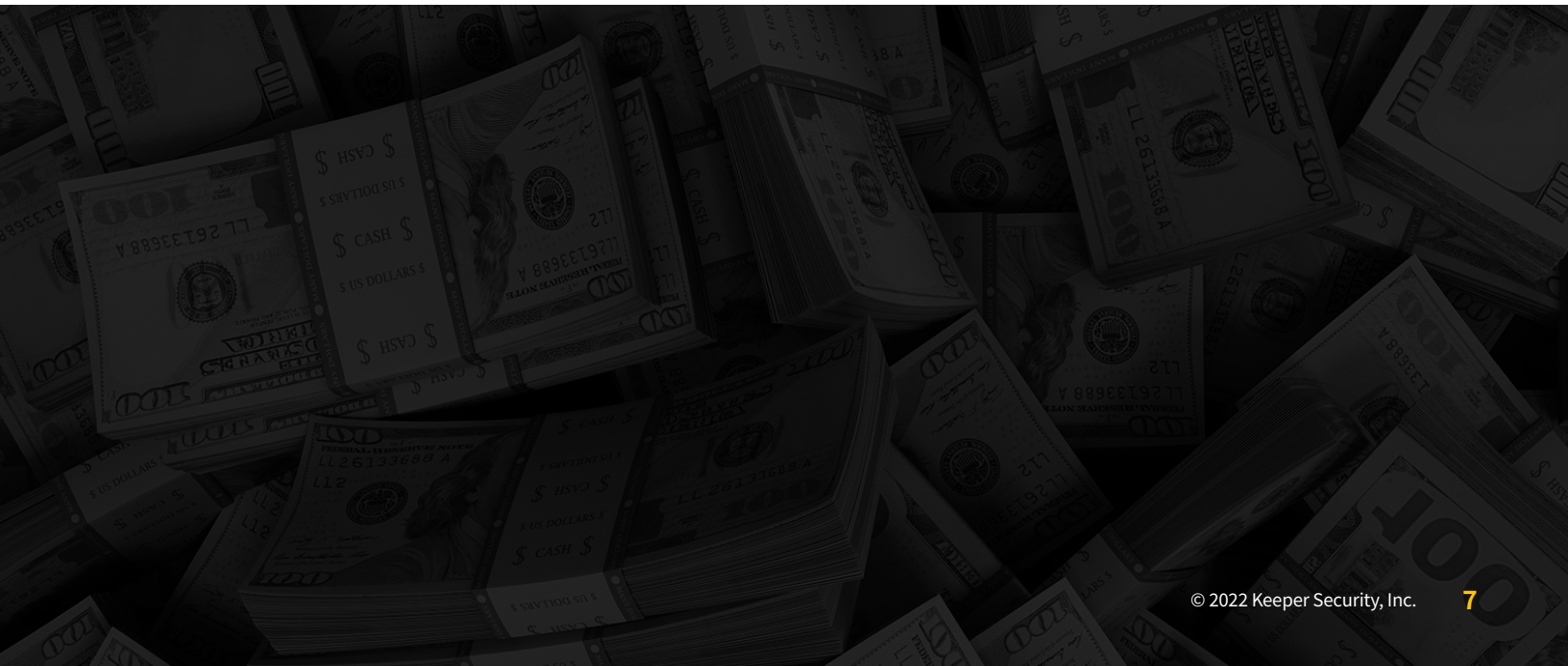
サイバー攻撃による金銭的コストは莫大なものです。サイバー攻撃の結果として金銭が盗まれた組織の中で、盗まれた金額の平均は75,000ドル以上であり、組織の37%は100,000ドル以上を失いました。

事業がサイバー攻撃で資金を失った場合、その金額はどれほどでしたか？



直接的な金銭上の損失に加えて、サイバー攻撃は事業に対する世間の認識や顧客の信頼、今後のパートナーシップとの円滑な運営に長期的な損害を与える可能性があるのです。回答者の4分の1以上（28%）がサイバー攻撃で被害を受けたことにより評判が損なわれ、19%が事業機会や契約の損失を報告しています。

このような直接的および間接的な損失は、米国内で働くすべての人の46.8%を雇用している中小企業（SMB）にとって壊滅的な打撃となる可能性があります。SMBの大半は資金繰りに苦労しています。利益を得られているのは40%だけであり、少なくとも5年間生き残れるのはわずか半分です。



セクション2

サイバーセキュリティへの投資とツール

サイバーセキュリティへの投資が不足していることにより、企業は脅威にさらされています。ユーザーの可視性、パスワードの強度、アイデンティティおよび権限は、事業規模やセクターを問わず基本的な必須事項ですが、それらが満たされていないのです。

リーダーは技術スタックに基本的なツールが欠けていることを認める

回答者の3分の1近く（32%）が、APIキーやデータベースのパスワード、特権認証情報など、ITシークレットを管理するプラットフォームがないと回答しています。回答者の実に84%が、ソースコードに存在するハードコーディングされた認証情報の危険性を懸念しており、25%がそれらを削除するソフトウェアが備わっていないと回答しています。

回答者の4分の1以上（26%）が、ITインフラストラクチャへのリモートアクセスを保護するためのリモート接続管理ソリューションがないと回答しています。アメリカ人労働者の58%は、少なくとも週に1日はリモートで働くことができると答えており、35%は週5日はリモート勤務が可能2だとしていますが、これはセキュリティ上の大きなギャップです。今日のデータ環境がますます複雑になり、デバイスやネットワーク、オペレーティングシステム、認証方法が増えるにつれて、セキュリティリスクは連鎖的に高まっています。ITリーダーは、勤務形態の急速な変化、そしてその変化がセキュリティに及ぼす影響に遅れを取るまいと苦闘しているのです。

26%

の回答者が、ITインフラストラクチャへのリモートアクセスを保護するためのリモート接続管理ソリューションが組織に不足していると回答しています。

セキュリティへの投資は計画されているが、早急な行動が必要である

セクション1で説明したように、米国のITリーダーのほとんどが、自分の組織はサイバー攻撃を回避する準備ができていると感じています。しかし、他の質問に対する回答からは、米国企業のセキュリティ体制における非常に深刻な弱点を明らかにしています。

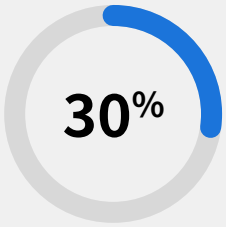
パスワードや認証情報は、緊急の投資を要する特定の分野です。パスワードとアクセス管理を規定する指針やベストプラクティスを従業員に示していると答えたのは、回答者の半数以下（44%）でした。

すべての従業員が、すべてのアカウントに強力で独自のパスワードを使用することは、最低限のセキュリティ対策です。しかし、回答者の30%が、パスワードの設定と管理を従業員に任せていると答えており、従業員同士がパスワードへのアクセスを共有することが多々あると認めています。一方、アイデンティティセキュリティを可視化し制御するために非常に高度なフレームワークを採用しているのは、わずか26%です。

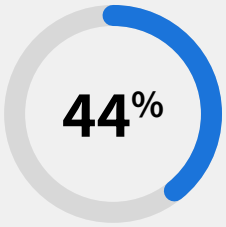
アクセス管理に対するこのような自由放任式のアプローチは、組織とその従業員を保護するために取り組むべきことがさらにあることを明らかにしています。

このような問題が企業にとって明らかな脅威となっているにもかかわらず、パスワード管理やネットワークベースの脅威の検出に役立つツール、インフラストラクチャシークレット管理に投資する計画があると答えた回答者は、半数未満でした。

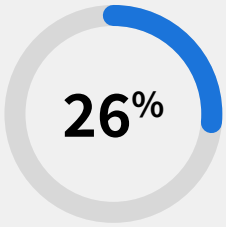
オンプレミスおよびクラウドシステムにおけるアイデンティティセキュリティの可視性と制御に関して、あなたの組織はどの程度成熟していますか？



低成熟度
従業員にパスワード設定を任せており、アクセスはしばしば共有される



平均的な成熟度
パスワードとアクセス管理を運用するための指針やベストプラクティスを示している



高成熟度
自社システムへのアクセスを規制する高度なフレームワークを備えている

次のうち、組織内のサイバーセキュリティに関して、来年に行う予定の投資はどれですか？

従業員セキュリティ意識向上トレーニング
54%

コンプライアンスの文化を作成する
50%

パスワード管理
48%

ネットワークベースの脅威の検出に役立つ制御と可視性の向上
44%

インフラストラクチャシークレット管理
42%

パスワードレス認証
37%

アクセスポリシーとアクセスツール間の接続をさらに強力にする
35%

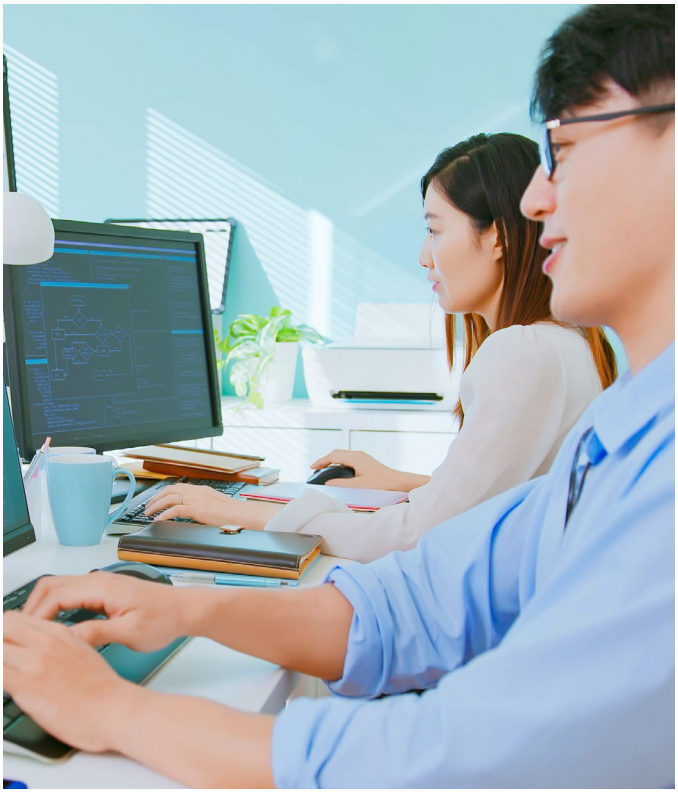
ゼロトラストおよびゼロ知識セキュリティのアプローチを採用する
32%

リモートアクセスセッションを保護するための特権アクセス管理
31%

サイバーセキュリティは複雑で多くの不確定要素や管理すべき優先事項の変動が伴うものですが、組織はさらなる対策を取ることができるはずだということが今回の調査で明らかになっています。

ITリーダーは、自分たちの防衛策には限界があることを自覚しており、それらの弱点が見うけられる箇所についての懸念を声高に表明しています。多くの組織は今後の投資を検討しているものの、外部脅威や既存の欠陥によって生じる需要の高まりにより、対抗できていない状況に陥っているのです。

リーダーシップにとっての優先事項という観点でサイバーセキュリティの順位を分析することは、こうした需要の変化に対応するために必要なリソースを実証するのに役立ちます。



セクション3

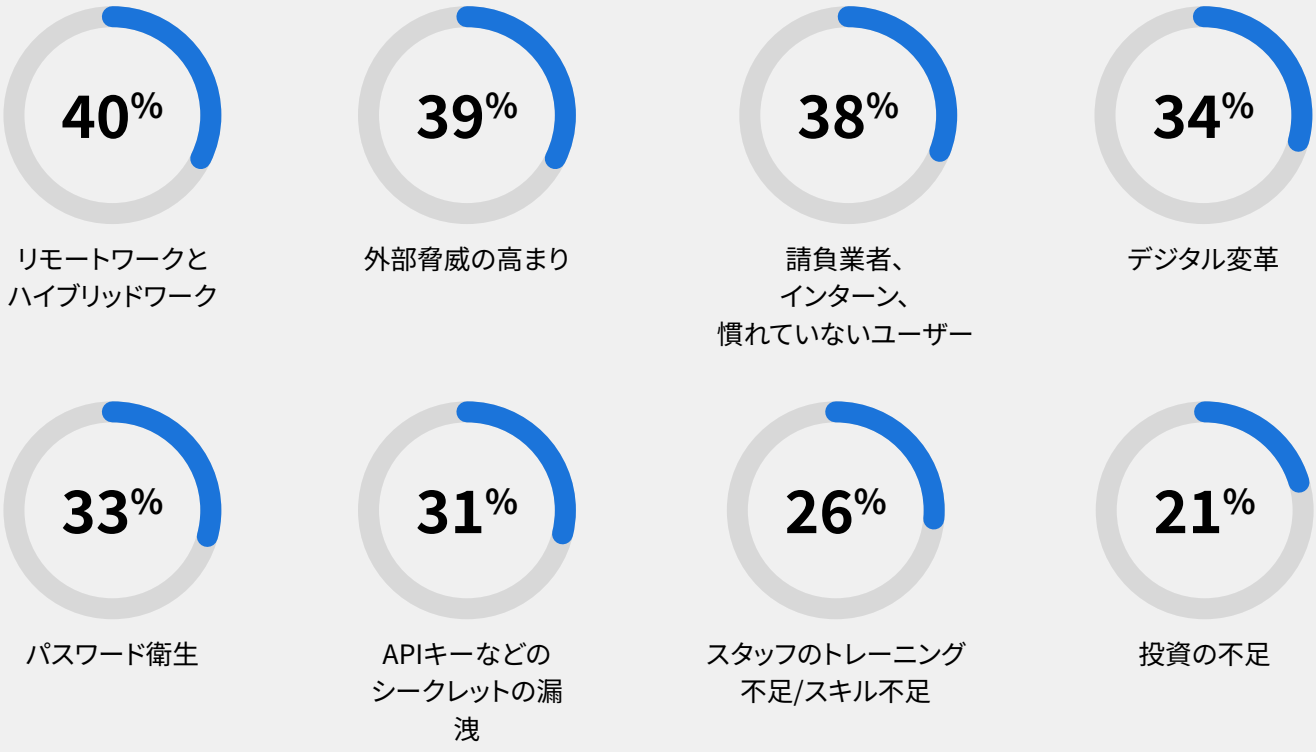
サイバーセキュリティにおけるリーダーシップ

増え続ける脅威に対抗しつつ事業をサイバー攻撃から保護することは、決して容易なことではありません。ITリーダーは、特にサイバーセキュリティ上の懸念が幅広いデジタル変革やハイブリッドワークの優先事項と競合しているため、ステークホルダーから計り知れないプレッシャーをかけられています。

サイバーセキュリティは経営幹部にとっての重要な懸念事項

リモートで働く従業員が増えるにつれて、企業はセキュリティを維持するための投資を考え直さなければなりません。実際、回答者の40%が、リモートワークとハイブリッドワークを最大の懸念事項として挙げており、外部脅威の高まり（39%）がそのすぐ後に続いています。

自分と組織にとって、サイバーセキュリティに関する懸念事項の上位3つは何ですか？



肯定的な面としては、投資不足が懸念として最も少なかった（21%）ため、自分の経営幹部によるサイバーセキュリティへのコミットメントは非常に重要だと回答者の60%が答えたことと一貫しています。サイバーセキュリティは組織の上級リーダーにとって重要ではないと回答したのは、わずか3%でした。

しかし、回答者の37%は、自社の経営幹部による投資が必要最低限でしかない、あるいは将来的には投資を行う予定だと回答しています。サイバー攻撃の頻度や巧妙さ、攻撃に費やすコストが急速に増加しているため、組織は明確に決まっていない時期ではなく、今すぐ積極的にセキュリティ対策に投資しなければならないのです。

リーダーシップは組織内のサイバーセキュリティをどのように形成しているのか

米国のビジネスリーダーは、組織を安全に保つために必要な人材を確保しようと躍起になっています。回答者の4分の3近く（71%）が、過去1年間にサイバーセキュリティ分野で新規採用を行なっており、58%は同時期にサイバーセキュリティトレーニングを強化したと回答しています。

調査対象の組織にサイバーセキュリティの専門知識が不足していることは、国全体であらゆるスキルが不足していることを反映しています。つまり、事業のマクロセキュリティに対する重大なリスクです。

あなたの組織の全体的なセキュリティ体制に対する経営幹部のコミットメントを最もよく表すものはどれですか？

これは非常に重要であり、セキュリティ戦略にリソースを投入する

60%

必要に応じて少額の投資を行うことにしている

29%

サイバーセキュリティについては認識しており、将来のある時点で投資を行う予定である

8%

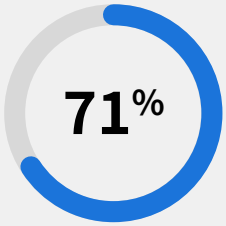
サイバーセキュリティは経営幹部にとって重要ではない

3%

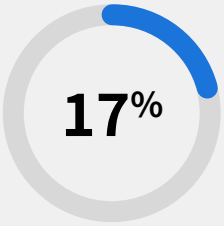
米国におけるサイバーセキュリティスキルのギャップ

Cyberseekによると、米国のサイバーセキュリティーワーカーは、雇用主が募集しているサイバーセキュリティ関連の求人の68%を埋められるだけの人数しかいません。平均して、サイバーセキュリティ職の採用には他のIT職の採用と比べて21%長く時間がかかります。.

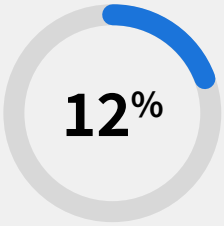
組織のサイバーセキュリティに関する専門知識を高めるために、過去12ヶ月間に新たな人材を採用しましたか?



はい、組織内のサイバーセキュリティ担当者に対する投資を実施しています



いいえ、しかし将来的にサイバーセキュリティの専門家を雇う計画があります



いいえ、すでに適切な人材を確保しています

回答者の半数（50%）が、サイバーセキュリティソフトウェアへの支出を増やしたと回答しています。過去1年間に技術スタックに変更を加えていないと回答したのはわずか8%でした。これは、米国企業全体でセキュリティ技術スタックを繰り返し進化させ続けるという広範なコミットメントを表しています。

来年には経済的逆風があらゆる事業にとって難題となる可能性があるものの、回答者の73%はサイバーセキュリティ予算が増えることを予想しています。

しかし、以下のセクションでは、財政上のコミットメントはサイバーセキュリティの全体像のほんの一部にすぎないことがわかります。サイバーセキュリティに対する文化的態度が新たな課題として浮上しているのです。

Craig Lurey、Keeper Security、CTO兼共同創業者

サイバーセキュリティは現在、上級ビジネスリーダーの優先事項として強く認識されています。来年には、その前向きな見解が、予算だけではなく、刻々と変化する脅威に直面して米国企業を安全に保つためのスキルやソリューションの強固な基盤という形で反映されなければならないのです。

セクション4

企業文化における サイバーセキュリティ

サイバー攻撃に対する透明性の欠如が不信の文化を煽る可能性

予算を確保するという誓約や、明確にサイバーセキュリティを優先事項とする指示が経営陣から出ているにもかかわらず、ITリーダー自身は組織内のサイバーインシデント報告に対する透明性が欠如しているという懸念を認めています。

回答者の半数近く（48%）が、サイバー攻撃については認識していたものの、それを隠していたことを認めており、担当部署に報告しなかったことを示唆しています。この数字は、企業やITリーダーどちらにとっても警鐘とすべきものであるはずです。

ITリーダーは事業内でサイバー攻撃発生の事実を共有できなければなりません。攻撃が報告されなければ、企業はそれらに対応できなくなるのです。脅威の規模は不明瞭なものとなり、最終的には事業の安全性が低下します。組織に対する信頼の欠如、あるいは報復に対する恐怖が、透明性の欠如を煽っている可能性があります。

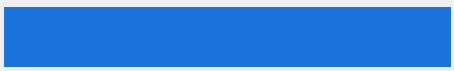
48%

のITリーダーが、サイバー攻撃を認識していたにもかかわらず口外しなかったと回答

一方、IT専門家の大多数（79%）が組織内での漏洩を懸念しており、47%が漏洩を経験したことがあると回答しています。これは、チームを教育し、誰もがサイバーセキュリティのベストプラクティスに確実に従うようにするために、より多くの取り組みを行う必要があることを示唆しています。

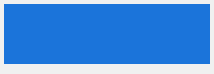
自分の会社はこれまでに組織内の漏洩を経験したことがありますか？また、そのことについて心配していますか？

はい、私は自分の組織内で侵害を経験したことがあり、それについて懸念してます



はい、私は自分の組織内で漏洩が発生する脅威について懸念していますが、まだ経験したことはありません

いいえ、私は自分の組織内で漏洩を経験したことがなく、懸念していません

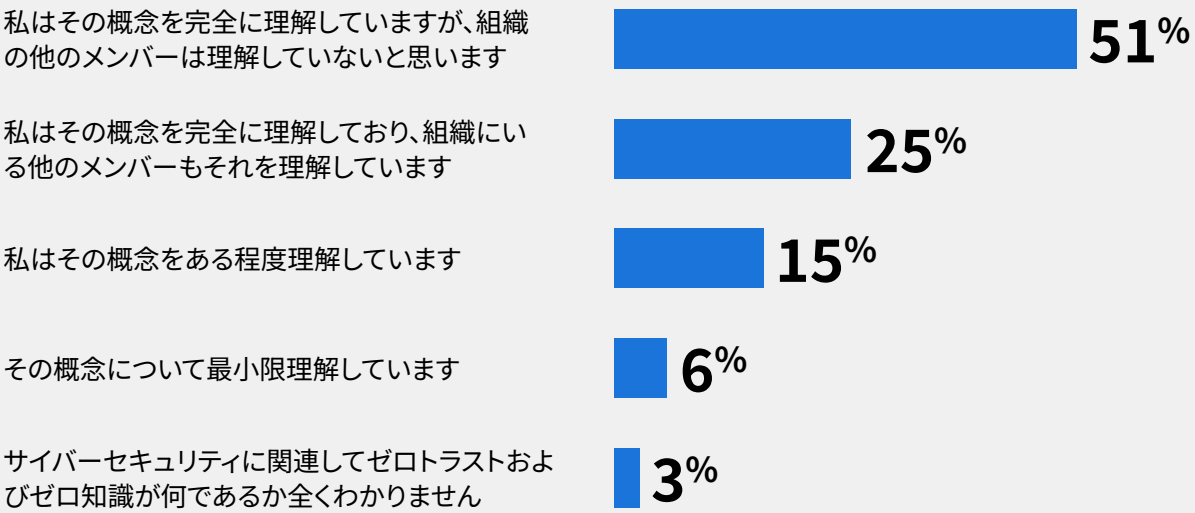


より堅牢なサイバーセキュリティ教育、トレーニング、計画策定が必要とされる

ベンダーや技術面でのサイバーセキュリティ環境は複雑ですが、回答者10人のうち9人（89%）は、サイバーセキュリティのロードマップを作成することは可能あるいは容易であると回答しています。プロセスが複雑あるいは不可能だと回答したのはわずか11%です。

しかし、ITの専門家は自らロードマップを作成できると感じているものの、ITチームとより広範な事業体の両方において、セキュリティにおける重要な概念を理解することには明確なギャップがあります。

サイバーセキュリティに関連するゼロトラストおよびゼロ知識の概念を理解していますか？



サイバーセキュリティにおけるゼロトラストおよびゼロ知識とは？

- **ゼロトラストは、**すべてのユーザーとデバイスには侵害される可能性があると想定し、人間も機械も含めすべてのユーザーは、ネットワークにアクセスする前に検証される必要があるというものです。
- **ゼロ知識** は、クライアント側の独自の暗号化とデータ分離のフレームワークを使用するセキュリティモデルであり、データ漏洩から保護することでゼロトラストをサポートするのに役立ちます。

ゼロトラストのキャッチフレーズが「誰も信頼しない」ならば、ゼロ知識のキャッチフレーズは「我々は何も知らず、

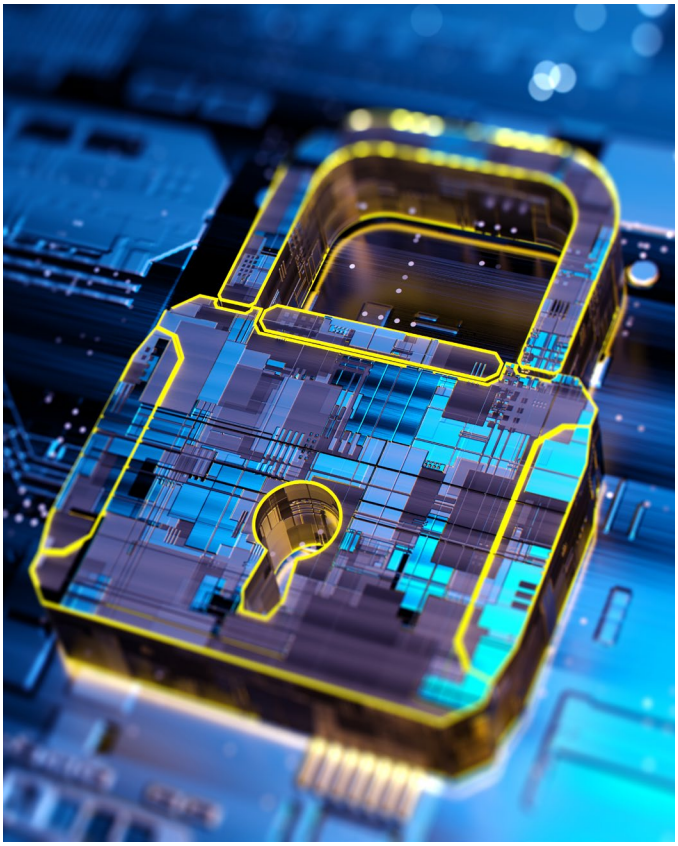
あなたのデータにアクセスすることはできない」です。

また、組織には、サードパーティー製のソースから得た知見を活かして堅牢なサイバーセキュリティ文化を構築する方法を探求することも求められます。回答者は、サイバーセキュリティに関する指針としてGartnerやForresterなどの業界アナリストを圧倒的に信頼しています（59%）。

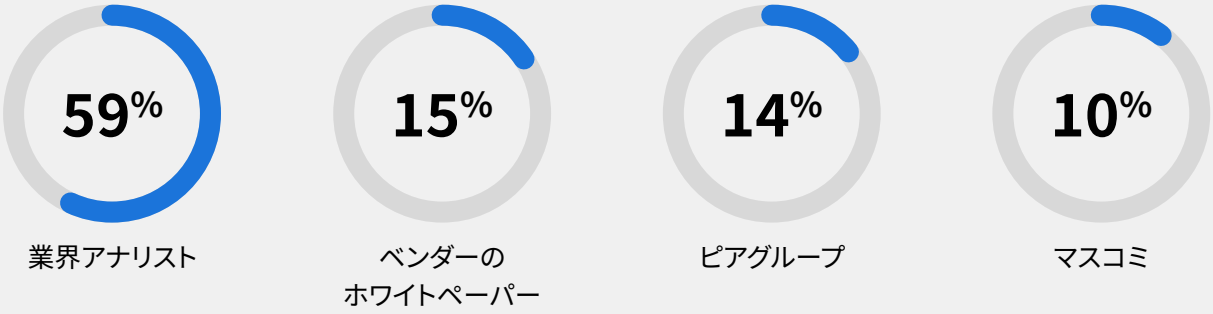
その専門知識を活用し、調査結果を掘り下げて探求する学習グループを作成することは、サイバーセキュリティを組織文化に組み入れる方法の1つになる可能性があります。

サイバーセキュリティの脅威が高まるにつれて、ITリーダーは模範を示さなければなりません。

攻撃について他のリーダーとまっすぐ向き合うことが最初のステップです。これらの問題に関するオープンな対話は、組織が直面するサイバーセキュリティの課題の程度を把握するために不可欠です。その認識があってはじめてリソースが教育に費やされ、サイバーセキュリティの考え方を組織文化に真に組み込むことができるのです。



サイバーセキュリティの指針について、あなたは誰を最も信頼していますか？



結論

米国中の企業は、サイバーセキュリティを最優先事項としています。しかし、努力や投資にもかかわらず、明確な溝は残っています。当社の調査は、小さな前進はあったものの、大きな飛躍はないことを示しています。

脅威が企業に打撃を与える量とペースは増加しており、リーダーシップには待つ余裕はありません。何も対策を講じないでいると、金銭的な不利益や評判上の不利益、そして組織的な罰則は厳しいものになります。

同様に、ハイブリッドワークやリモートワークが普通のこととなるなど、働き方が劇的に変化してきたため、企業もサイバーセキュリティの適応力を構築する方法について再考する必要があります。

経済の不確実性が新たな時期に突入する中、私たちは気を緩めてはなりません。サイバー攻撃に対処するための予算を割り当てることを迫られたとしても、攻撃のペースが落ちることはないでしょう。予防策のコストは、長期的に見ると常に安いものとなります。組織がサイバー攻撃とその影響から身を守るために、防御的なソリューションを展開することは不可欠です。

しかし、米国企業が真に安全になるために必要な最大の変化は、文化的なものだと考えられます。ITリーダーの半数近くが、サイバー攻撃に気付きながらも口外しなかった（そのため担当部署に報告しなかった）ことを認めています。この数字はビジネスリーダーに衝撃を与えるはずです。信頼や説明責任、対応の文化がなければ、サイバー犯罪者は今後も栄えることでしょう。

近い将来、企業やITリーダーはサイバーセキュリティに対するコミットメントを表明するだけでなく、それに基づいて行動する必要もあります。職場がどのように進化してきたかを認識し、見直しされた技術スタックでの新しい働き方に対応することが求められます。

何よりも重要なことは、サイバーセキュリティを組織文化の一部にすべきだということです。サイバーセキュリティはすべての優れた事業体の柱であるべきですが、理解や説明責任、教育、進歩は上層部からスタートする必要があるのです。

[1] Mckinzey American Opportunity survey(英語文献のみ)

