KEEPER
Cybersecurity Starts Here®

2022年
英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英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、英国内のIT意思決定者512人の行動や態度を分析しました。Keeperによる2度目の英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度目の英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

ITリーダーの半数近くが、サイバー攻撃の数および攻撃の成功数の増加を予想

サイバー攻撃は、英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。そうした予想にもかかわらず準備は不足しており、サイバー攻撃の脅威に直面する心構えができていると感じている組織はごく少数です。企業は、自社組織やその財務、評判、従業員らを保護するために、緊急の行動を取らなければなりません。

ITリーダーの3分の1以上が、ITセキュリティの管理プラットフォームを所有していない

サイバー攻撃がもたらす脅威を認識しているにもかかわらず、ITリーダーはサイバー攻撃から身を守る適切なツールを持っていません。ハイブリッドワークやリモートワークの出現は、組織を保護するために必要な対策、そして利用可能な対策との間の差をさらに拡大しているにすぎません。リモートアクセスツールと同様に、クラウドやSaaSアプリをめぐるセキュリティは、現在の技術スタックが不十分であり企業が特に危険にさらされている分野です。

経営幹部らの3分の1が、組織がセキュリティを維持する上でリモートワークとハイブリッドワークが最大の懸念事項だと指摘

経営幹部の大多数は、サイバーセキュリティがビジネスにとって非常に重要な優先事項だと認識しています。この認識は、ITリーダーにとって健全な予算へと転換していますが、脅威の進化のスピードがITリーダーらの対応能力を凌駕している可能性があります。特にリーダーは、組織を安全に保つために必要なスキルのある人材を獲得することに苦戦しているのです。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。

ITリーダーの半数以上が、サイバー犯罪を認識しておきながら口外しなかったとの回答。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

担当部署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。そして、脅威の高まりについてのトレーニングを受けたことや懸念があるにもかかわらず、ゼロトラストやゼロ知識といったサイバーセキュリティの重要な概念については、ITリーダーも多方面の従業員も完全には理解していません。組織はチームを教育し、スキルアップすることに投資しなければなりません。重要なデータを保護できるソリューションと並行して、ITリーダーは透明性と説明責任の文化を培うことで、自社事業がサイバー脅威を完全に理解して適切に対応できるようにする必要があるのです。

セクション1

サイバー攻撃

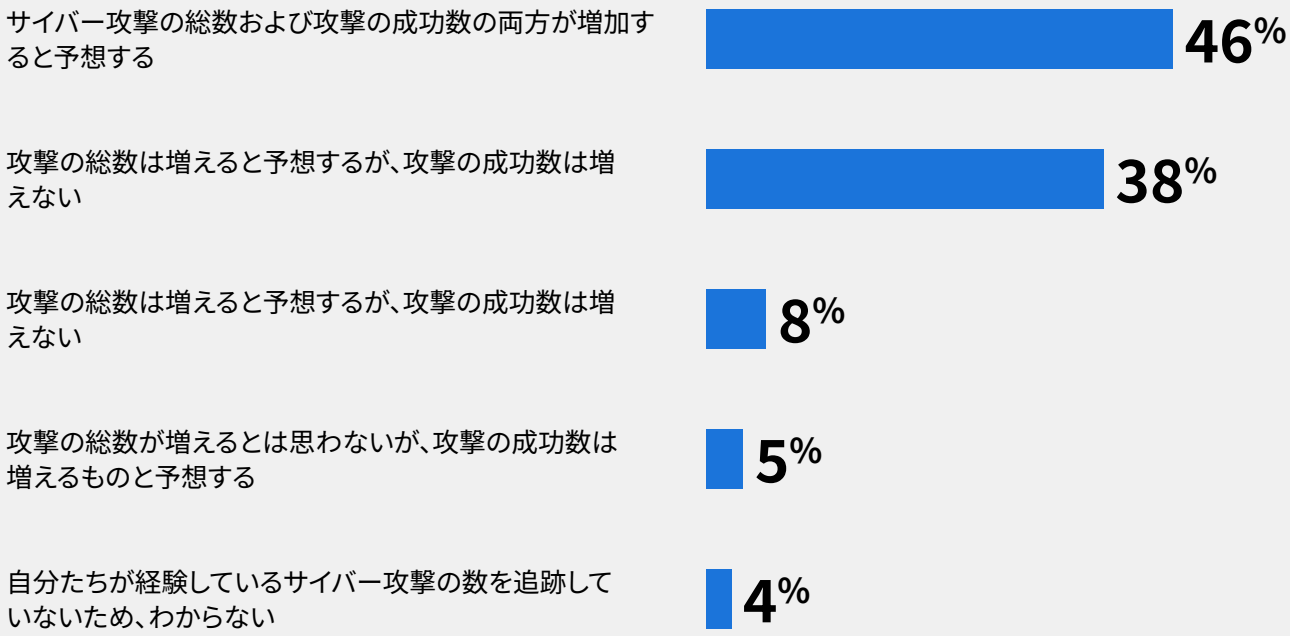
サイバー攻撃は増え続ける脅威を呈する

英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。

平均的な企業は年間44回のサイバー攻撃を受けています。つまり、毎月3回以上ということになります。およそ5分の1（17%）が年間500件以上の攻撃にさらされていますが、これは営業日ごとに約2件のサイバー攻撃に相当します。

このような中、平均的な企業は毎年約2回のサイバー攻撃に直面しているのです。しかし、ITリーダーは、こうした攻撃の頻度が激化するのを恐れています。回答者の半数近く（46%）が、攻撃の総数および成功数は来年にかけて増加すると予想しています。

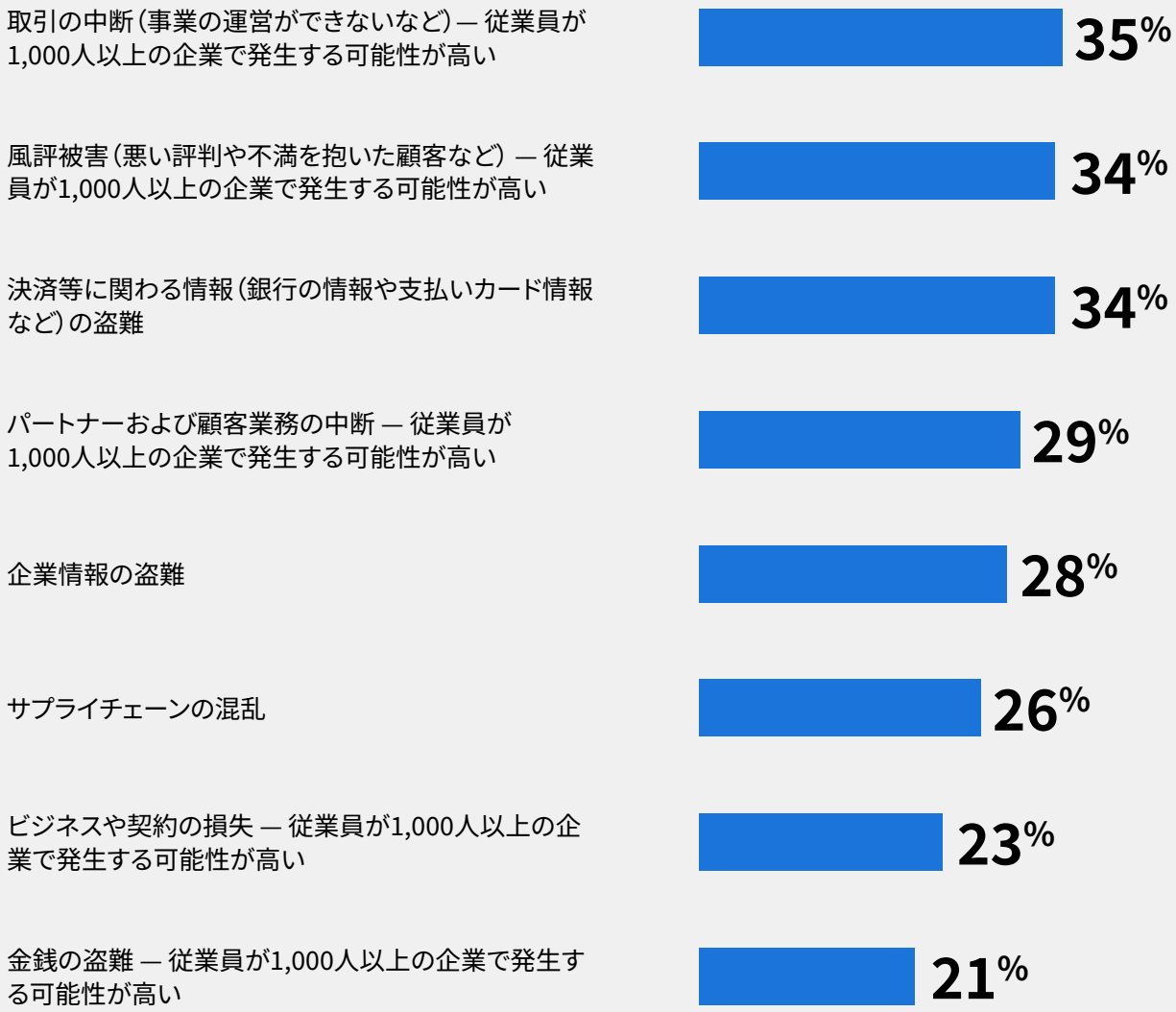
ITリーダーはサイバー攻撃の数（成功数と総数）が今後12ヶ月間でどう変動すると予想しているのか



サイバー攻撃は企業に重大な損害を与えている

サイバー攻撃の成功を許すと、企業は深刻なダメージを受けて行き詰まってしまう可能性があります。サイバー攻撃の被害者の3分の1以上（35%）が、事業運営を行う能力など、取引に支障をきたしていると報告しています。

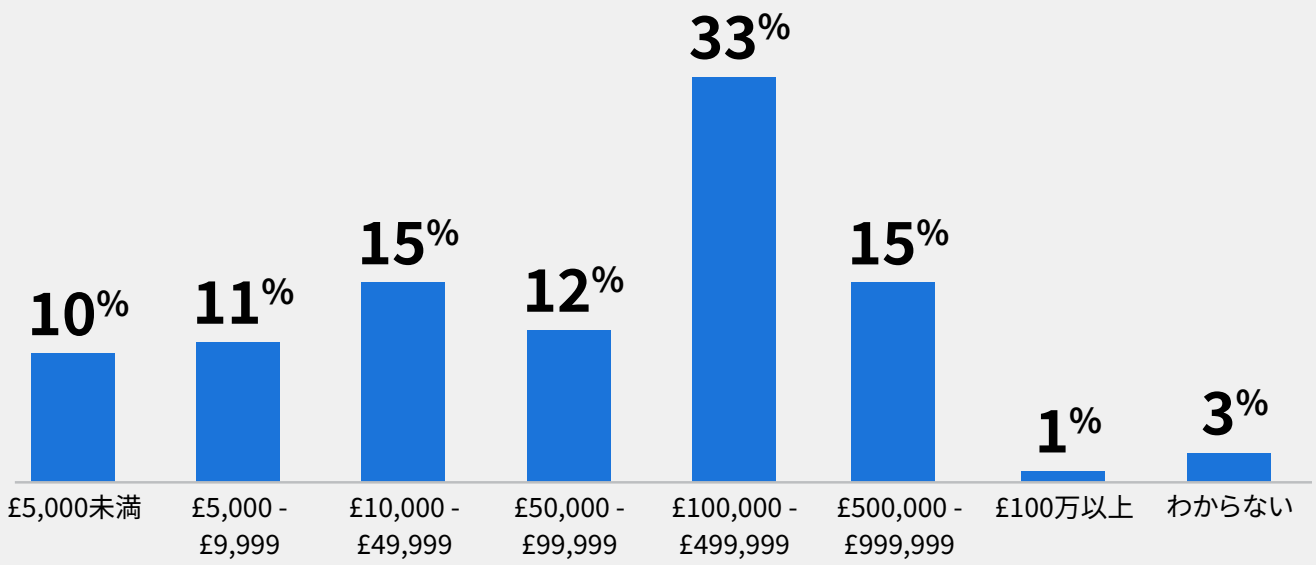
サイバー攻撃の成功を許したことで、自分の事業に降りかかったことは次のうちどれですか？



サイバー攻撃はあらゆる規模の企業に影響を与えます。たとえば、従業員が1,000人以上の組織の31%と、従業員が1,000人未満の組織の31%が、サイバー攻撃の成功を許したことによる金融情報の盗難を経験しています。同様に、従業員が1,000人以上の組織の22%と、1,000人未満の組織の21%が金銭の盗難を経験しました。

これらの攻撃によって引き起こされる金融関係の混乱は、平均して10万ポンド以上という重大なものです。組織の16%では、その被害は50万ポンド以上でした。

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？



英国における現在のマクロ経済の不確実性および平均的な英国の中小企業の年間利益が11,000ポンド1に過ぎないという事実を考慮すると、そのような損失は壊滅的な打撃となる可能性があります。

しかし、サイバー攻撃の影響は金銭的なものだけではありません。3分の1以上（34%）が攻撃の影響で風評被害に苦しめられ、29%がパートナーによる業務の中断を重く受け止めました。要するに、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対し、長期的な損害を与える可能性があるのです。

組織は攻撃に対抗する準備が十分にできていない

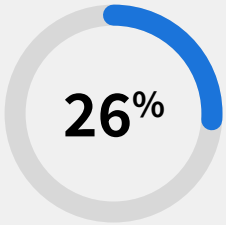
組織はサイバー攻撃がもたらす損害について認識し、経験したこともあるものの、サイバー攻撃から身を守る準備が十分にできていると考えている企業は実に26%にとどまっています。

一方で、攻撃に対処する時間は増えています。回答者の大多数（61%）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10%です

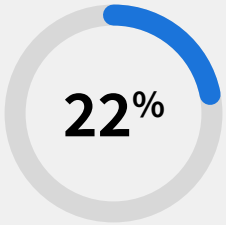
Darren Guccione、Keeper Security、CEO兼共同創業者

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？他の英国企業はどの程度の準備ができていると思いますか？



十分に準備できている
（自分の事業）



十分に準備できている
（英国企業全般）

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以上（35%）が、APIキーやデータベースのパスワード、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。また、およそ10人に9人（87%）が、ハードコーディングされた認証情報の危険性についての懸念も強調しています。

一方、回答者の29%は、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。

従業員の38%が完全な在宅勤務あるいは自宅とオフィスの両方で働いている[2],ことを考えると、このハイブリッドワークの時代におけるセキュリティの欠陥が浮き彫りにされています。ハイブリッド環境で使用されるデバイスやネットワーク、オペレーティングシステム、認証スキームが増えるにつれて、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。

29%

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。

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

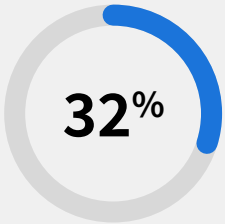
データは、ITリーダーが現在のセキュリティ対策に明らかな弱点があることを認識しているパターンを示しています。

パスワードや認証情報は早急に投資することが求められる特定の分野であり、パスワードや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回答者は半数未満（48%）でした。

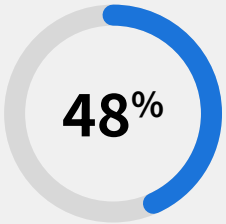
これは実践すべき最低限のベストプラクティスですが、回答者の約3分の1（32%）は、パスワードの設定を従業員に完全に任せており、従業員同士がログイン認証情報を共有することが多々あると答えています。その割合は、従業員が1,000人未満の組織で最大37%に達しています。アクセス管理に対するこのような自由放任式のアプローチは、組織とその従業員を保護するために取り組むべきことがさらにあることを明らかにしています。

一方で、システムへのアクセスを管理する高度なフレームワークを採用していると回答したのは21%にとどまっています。

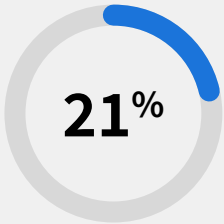
オンプレミスおよびクラウドシステムにおけるアイデンティティセキュリティの可視性と制御に関して、あなたの組織はどの程度成熟していますか？



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？

コンプライアンスの文化を作成する
45%

パスワード管理
45%

従業員セキュリティ意識向上トレーニング
44%

ガバナンス
43%

インフラストラクチャシークレット管理
38%

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
38%

パスワードレス認証
36%

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
33%

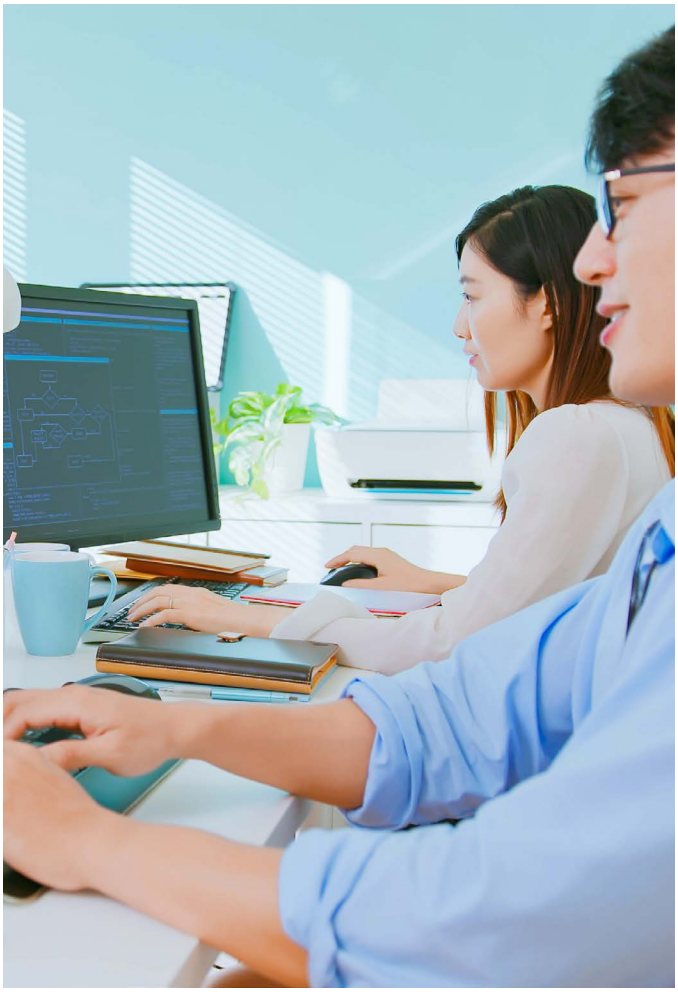
リモートアクセスセッションを保護するための特権アクセス管理
26%

これらの問題が企業にとって明らかに脅威であるにもかかわらず、パスワード管理やセキュリティの意識向上トレーニング、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。

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。



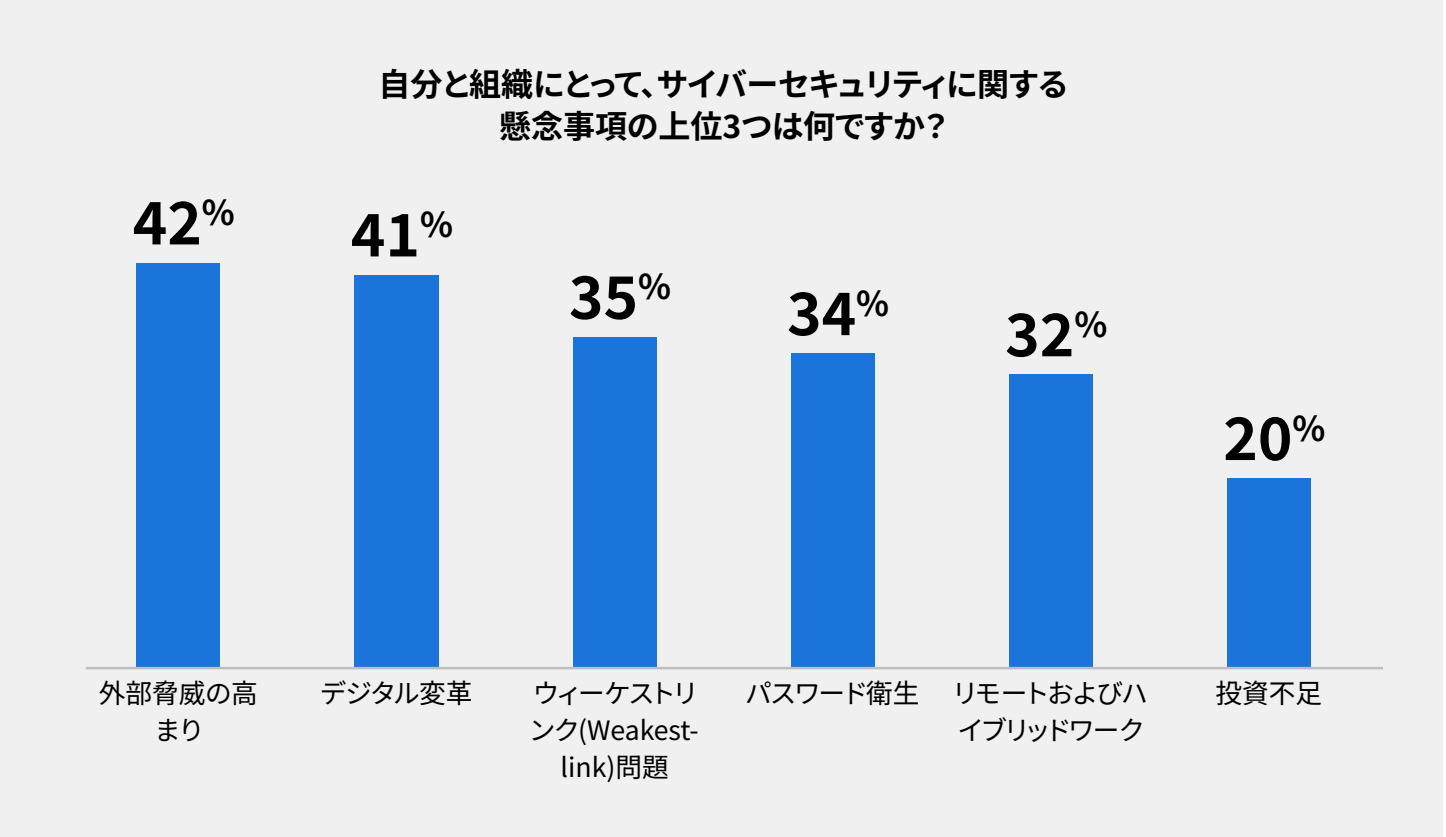
セクション3

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、組織の32%がリモートワークとハイブリッドワークを懸念事項として挙げており、1,000人以上の従業員を抱える組織では38%というさらに高い割合に達しています。



しかし、外部脅威の高まりはITリーダーにとって概して最大の懸念事項となっており、サイバーセキュリティの課題が増加しているというセクション1での知見を強めています。

肯定的な面としては、投資不足が懸念事項だと明言したのは回答者のわずか20%でした。これは、より多くの経営幹部がサイバーセキュリティは不可欠だと認識しているためだと考えられます。

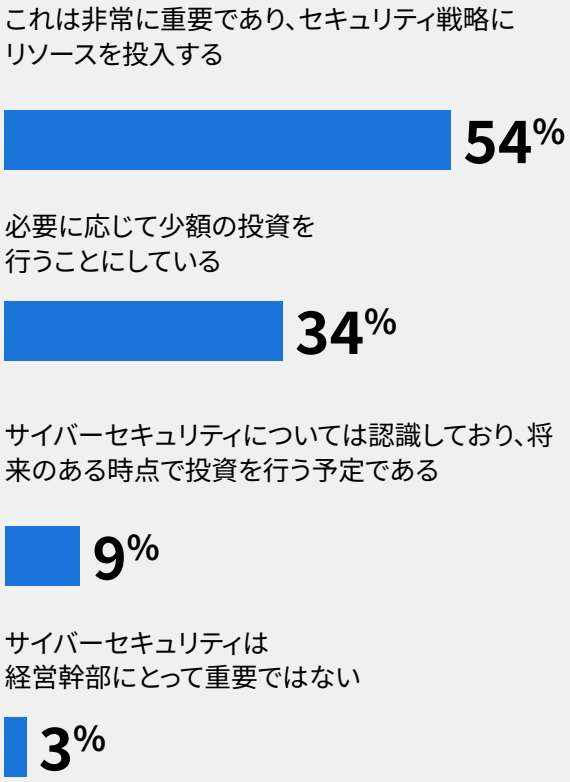
サイバーセキュリティは組織の上級リーダーにとって重要ではないと回答したのは、回答者の3%に過ぎません。対照的に、回答者の54%はその逆だと回答しています。

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

ビジネスリーダーはサイバーセキュリティの重要性を認識していますが、自分の組織を安全に保つために必要な人材を確保するまでには至っていません。

すでに適切な人材を確保していると答えた回答者は11%にとどまり、74%は過去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たと答えています。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

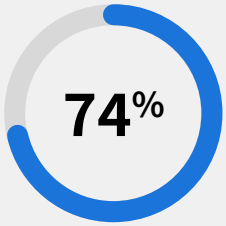
あなたの組織の全体的なセキュリティ体制に対する経営幹部のコミットメントを最もよく表すものはどれですか？



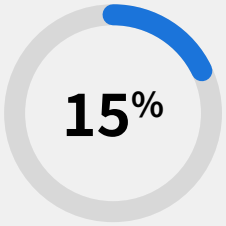
英国におけるサイバーセキュリティスキルのギャップ

デジタル、文化、メディア、スポーツ省は、英国全体で **事業体の約51%**[3] がサイバーセキュリティにおける基本的な人材が不足していることを認識しています。つまり、構成済みのファイアウォールの設定、個人データの安全な保存や転送などの簡単なタスクを実行するスキルが不足しているのです。一方、回答者の33%は高度なスキルのギャップ（ペネトレーションテストやセキュリティアーキテクチャのような分野）があると答えており、37%はインシデント対応と回復に関して内部スキルのギャップがあると答えています。

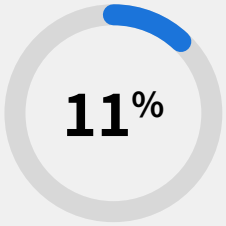
組織のサイバーセキュリティに関する専門知識を高めるために、過去12ヶ月間に新たな人材を採用しましたか？



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

サイバーセキュリティソリューションに関しては、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7%でした。これは、英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。

来年には経済的な逆風があらゆる事業に難題となる可能性がありますが、現在のサイバーセキュリティ予算は依然として健全であり、回答者の68%はサイバーセキュリティ予算が増えることさえ予測しています。

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明らかになります。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英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。

半数以上（55%）がサイバー攻撃を口外しなかった（つまり攻撃について担当部署に報告しなかったと考えられる）と回答しています。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。組織に対する信頼の欠如、あるいは報復に対する恐怖が、説明責任の欠如を煽っている可能性があります。しかし、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。

55%

のITリーダーはサイバー攻撃を認識しており、その事実を口外しなかったことがある（つまり、担当部署に報告しなかったことを示唆）。

一方、IT専門家の大多数（80%）が自分の組織内の漏洩を懸念していることから、チームを教育してメンバー全員がサイバーセキュリティのベストプラクティスに従っていることを確認するために、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

49%

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、まだそれを経験したことはありません

30%

いいえ、私は自分の組織内で漏洩を経験したことがなく、それについては懸念していません

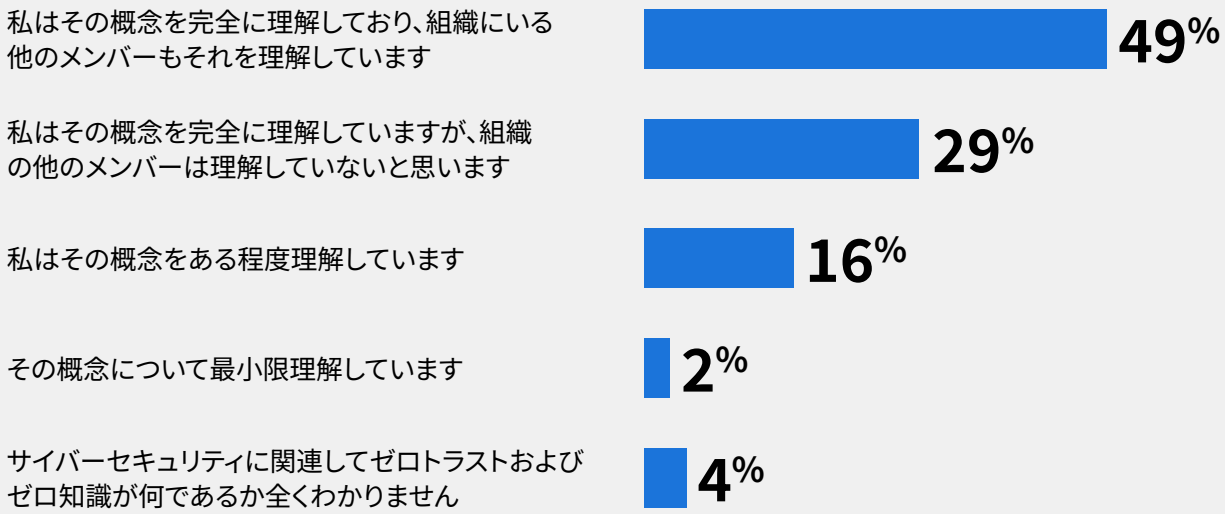
20%

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、回答者の大半（90%）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10%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。 さらなる教育が必要です。

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。

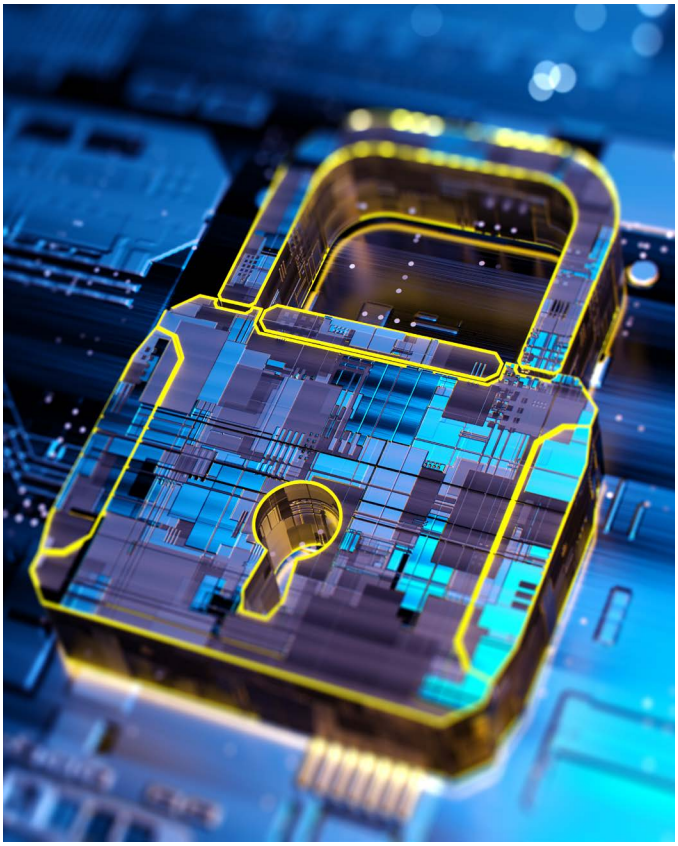
ゼロトラストのキャッチフレーズが「誰も信用しない」ならば、ゼロ知識のキャッチフレーズは「我々は何も知らず、あなたのデータにアクセスすることはできない」です。

また、組織には、サードパーティー製のソースから得た知識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。ITリーダーの半数（50%）が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最も信頼されている情報源として挙げており、22%がピアグループを挙げています。

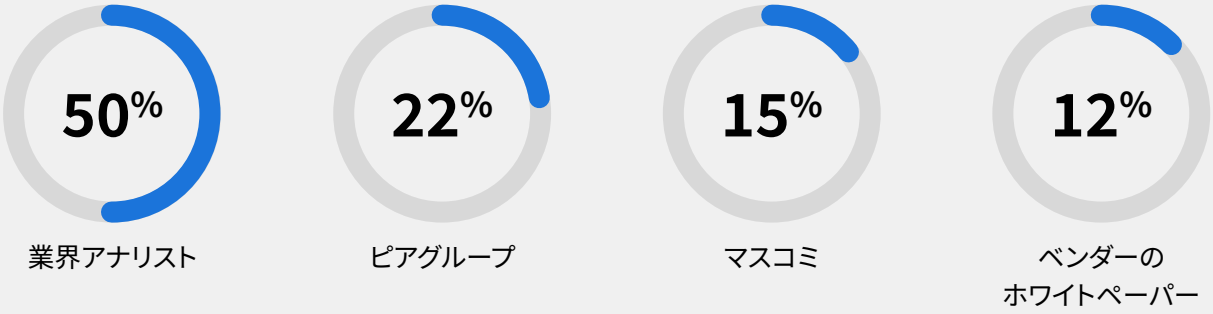
その専門知識を活用し、調査結果を掘り下げて探求する学習グループを作成することは、サイバーセキュリティを組織文化に組み入れる方法の1つになる可能性があります。

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

英国中の企業は、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、明確なギャップは残っています。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てとしても、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。攻撃とその影響から身を守る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、英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リーダーの大多数は、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があります。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柱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として理解されるべきですが、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] Statista, 2021年英国の中小企業利益の規模別平均）」（2022年）
[2] 国家統計局 ハイブリッドは定着するのか?）」（2022年）
[3] デジタル、文化、メディア、スポーツ省, （英国労働市場におけるサイバーセキュリティスキル：2022年調査結果レポート）」（2022年）