ivanti

# Press Reset:

## 2023 サイバーセキュリティ体制の現状レポート

企業はサイバー攻撃から会社を守ろうと急いでいますが、業界では事後対応やチェックリストの考え方に悩まされています。

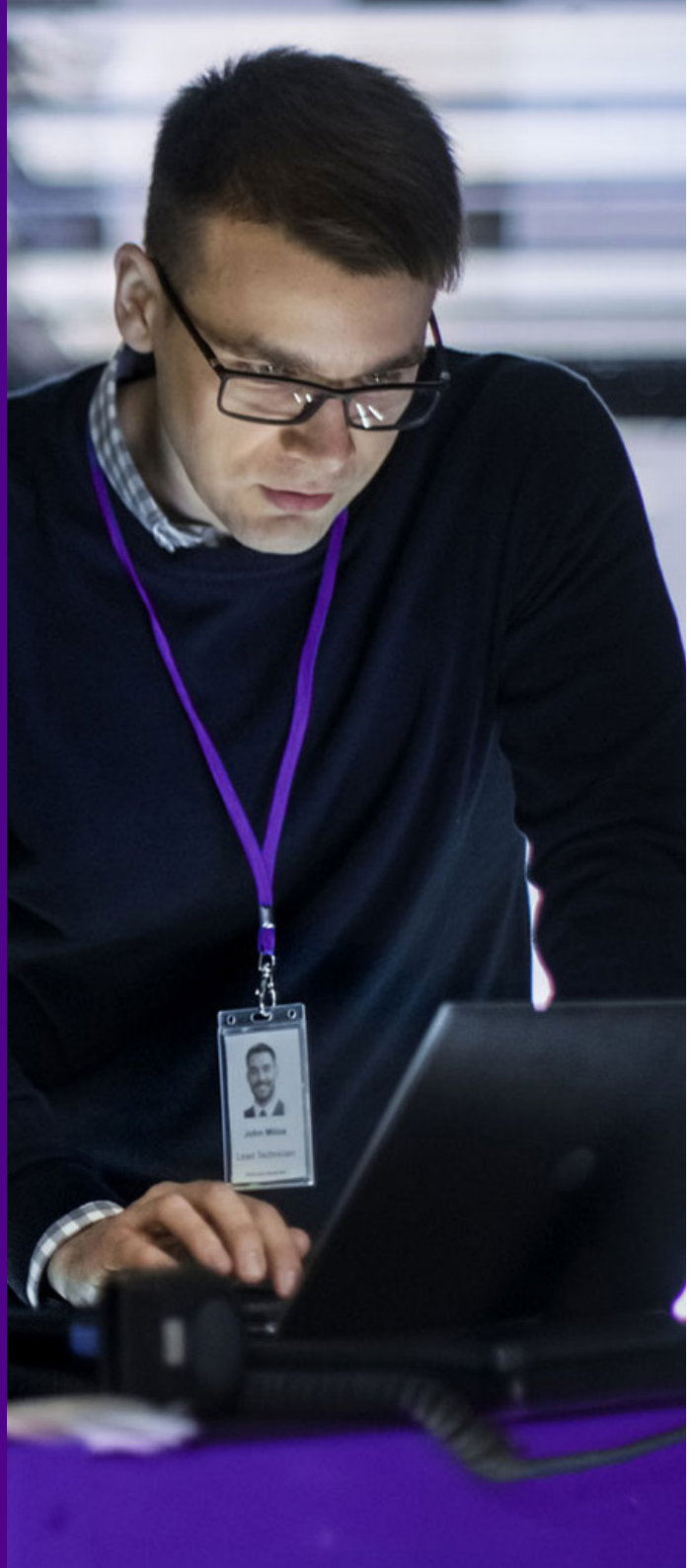
# チョコレートバーにたとえると

1,356 人の経営陣とセキュリティの専門家に、セキュリティ侵害の被害を食い止めるための組織の能力について質問しました。

**導入したセキュリティ対策にチョコレートバー1本分を賭けますか。**

**調査回答者の 5 人に 1 人が「いいえ」と答えました。**

ivanti



20% の回答者がチョコレートバー1本分の価値 (約 2 米ドル) さえ賭けたくないと言うほど、企業のサイバーセキュリティの状況は悲惨なものなのでしょうか。

企業として適切な人材を雇用し、相応のテクノロジーに投資し、的確なプロセスや手続きを踏んでいるにもかかわらず、ITセキュリティの強度に疑いが抱かれている理由とは何でしょうか。 そこで、今こそ効果的なサイバーセキュリティを実現するために、私たちのアプローチを見直すべき時だといえるでしょう。

Ivantiのサイバーセキュリティ体制の現状にまつわる一連のアンケートを通じて、6,550人にのぼる専門家の意見が調査されました。これにより、サイバーセキュリティにまつわる新たな脅威や、予算削減、企業が保護目的で導入しているテクノロジーやプロセスレイヤーなど、企業の直面している深刻な現状に対する洞察が得られました。

さらに、企業の経営陣、セキュリティの専門家、ナレッジワーカーの3つの視点から問題を捉え、経営陣で発見された衝撃的な脆弱性についても時間をかけて解説しています。

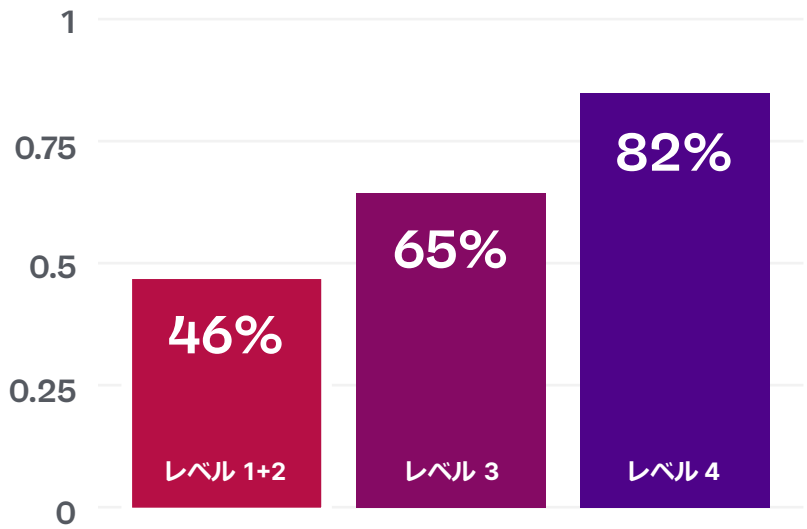
Ivantiのゴールは、セキュリティの責任者たちが自身の対策について楽観的であるにもかかわらず、自分たちのサイバーセキュリティ強度に対してキットカットのチョコレートバーさえ賭けたがらない理由を探るとともに、彼らが効果的でプロアクティブなセキュリティ対策のアプローチをいかにリセットできるか特定することにあります。

# 目次:



## 準備に対して楽観的に考えている経営陣

Q: 1年前と比較して、サイバーセキュリティ攻撃に対する防御の備えが強化されたと感じていますか、それとも弱くなったと感じていますか。




**「1年前と比べ、防御の準備が整ってきたと感じています。」**

サイバーセキュリティ成熟度グループについては、24 ページを参照してください 。

01

# 複雑につながった世界におけるセキュリティ

PwC の最近の調査では、「破滅的なサイバー攻撃が2023年のレジリエンス計画における最大のシナリオ」であり、経営者の3人に2人がサイバー犯罪を今後1年間で最も大きな脅威と考えていることが明らかになりました[1]

脆弱性が増し、未知の脅威さえ出現している世界で、準備するとは一体どのようなことなのでしょうか。 まずは、2023年のサイバーセキュリティの状況を評価することから始めましょう。

ivanti

# サイバーセキュリティの予算は、より大きく、より有害な脅威に対応するために拡大している

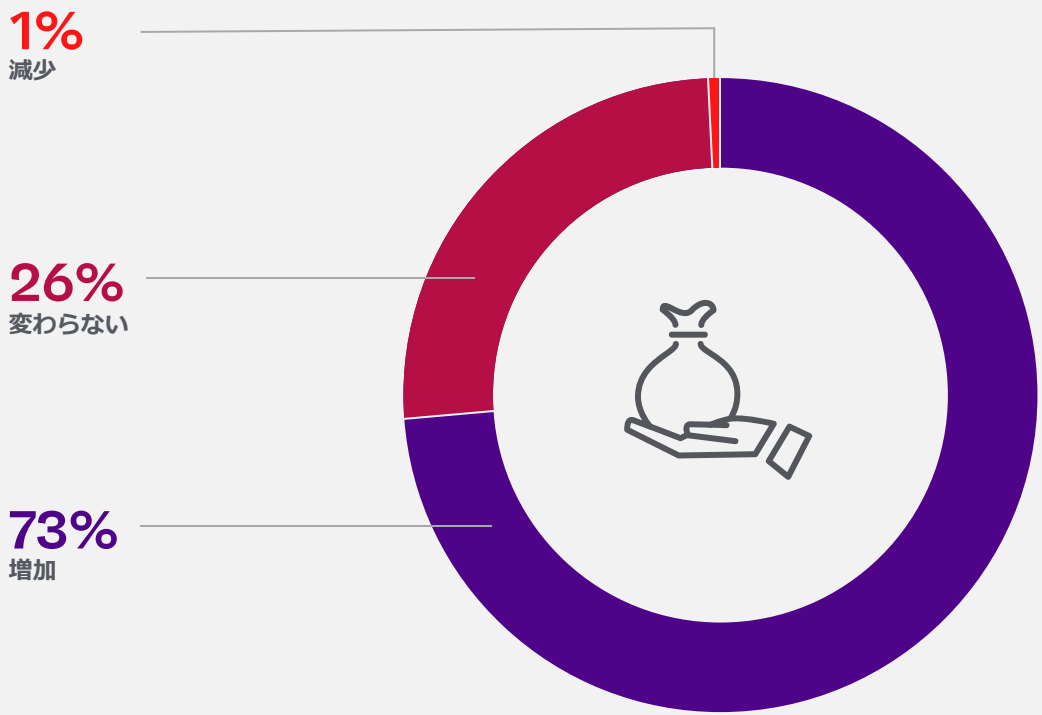
調査対象のセキュリティ専門家および経営陣のうち、73%が 2023年にサイバーセキュリティの予算が増加すると予測しており、平均で11%増加すると予想しています。 Society for Human Resource Managementによると、これは、2023 年に予想される報酬の予算増加のおよそ3倍に相当します。[2]

Kelloggのグローバル最高情報責任者であるLesley Salmon（レスリー・サルモン）氏は、Wall Street Journal紙に次のように語っています。「もし私が予算上の課題に直面したら、それはサイバー (セキュリティ) に関する問題ではありません」。[3]

2023年の平均予算増加率11%と予測され、同時期のインフレ予測を大きく上回っています。

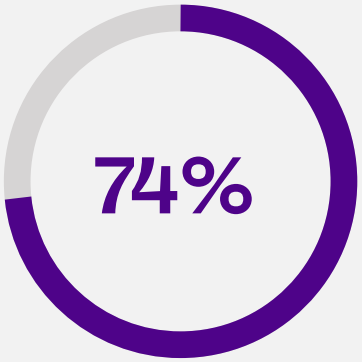
## サイバーセキュリティの予算は拡大している

Q: 2023年のサイバーセキュリティ予算は、2022年に比べて増加しますか、減少しますか。

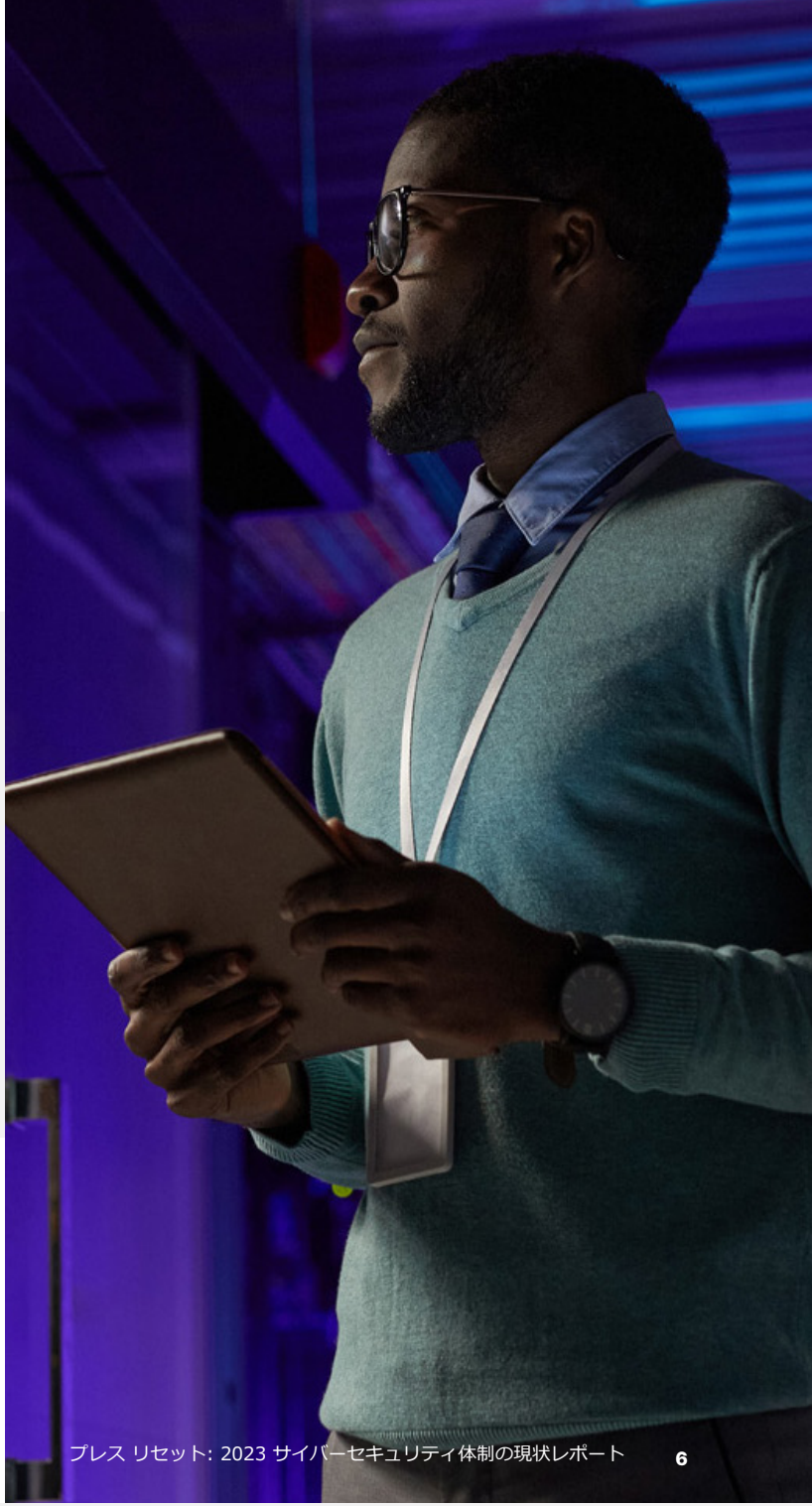


Ivantiの調査対象者となったセキュリティの専門家の約4人に 3人は、セキュリティ侵害のための資金を確保しています。また、侵害対策のための「緊急資金」予算はサイバーセキュリティ予算全体の約16%を占め、相当な額になっています。

IBMの「Cost of a Data Breach 2022」レポートによると、データ漏えいからの復旧コストは軽く7桁を超え、平均で企業は復旧に435万ドルを費やすことになります。さらに、医療や銀行などの業界は復旧の罰則が最も高額になります。[4]




がセキュリティ侵害のための予算を計上していると回答しており、平均して、侵害に備えた「緊急資金」はサイバーセキュリティ予算全体の16%を占めています。



# セキュリティスキルのギャップが大きく、技術スタックが複雑であるため、セキュリティが阻害される

セキュリティ専門家や経営陣が挙げた、卓越性を阻害する最大の障壁は、「技術スタックの複雑さ」と「セキュリティスキルのギャップ」であり、「予算不足」をはるかに上回る結果となりました。

**技術スタックの複雑さ**

セキュリティの専門家は、平均して6種類のサイバーセキュリティツールやプログラムを使用していると回答しています。

Microsoftのセキュリティ責任者であるCharlie Bell（チャーリー・ベル）氏は、あまりにも多くのセキュリティプラットフォームが蓄積された結果、同氏が「ある種のフランケンシュタイン・ソリューション」と呼ぶものが生まれたと述べています。Bell氏が説明するように、「問題は、あらゆるものを接着剤でくっつけると、継ぎ目ができてしまい、その継ぎ目が攻撃される場所になってしまいます。」"[5]

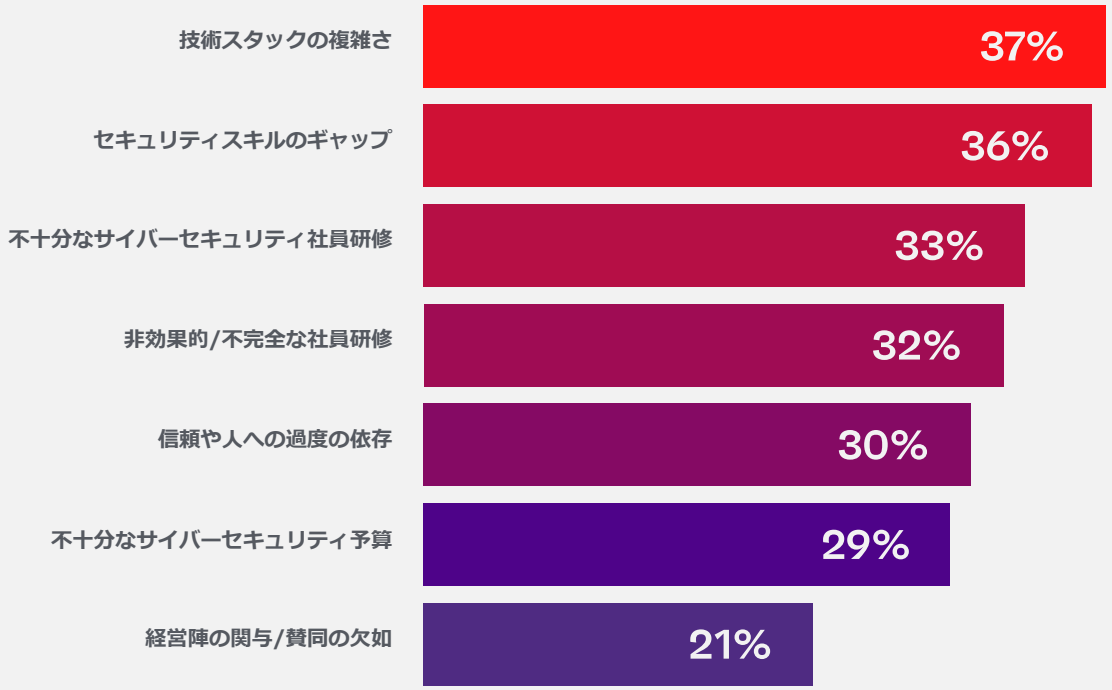
**セキュリティスキルのギャップ**

セキュリティの専門家にとって、「スキルギャップ」は他の項目を引き離す大きな課題であり、調査対象となったセキュリティ専門家の39%が挙げています。

2021年と比較して2022年には、世界のサイバーセキュリティ人材のギャップが26.2%増加し、資産を効果的に保護するためにはさらに340万人の労働者が必要であるとしたISC2の最近の報告書など、他の多くの研究による調査結果が、このギャップによって裏付けられます。[6]

## 複雑さと人材が最大の課題

Q: 次のうち、企業のサイバーセキュリティ対策を阻む大きな障壁はどれですか。



# サプライチェーンリスクへの対応競争

企業のデジタル変革、そして高度に接続されたサプライチェーンによって実現されるあらゆる効率化は、圧倒的なサプライチェーンリスクを伴います。

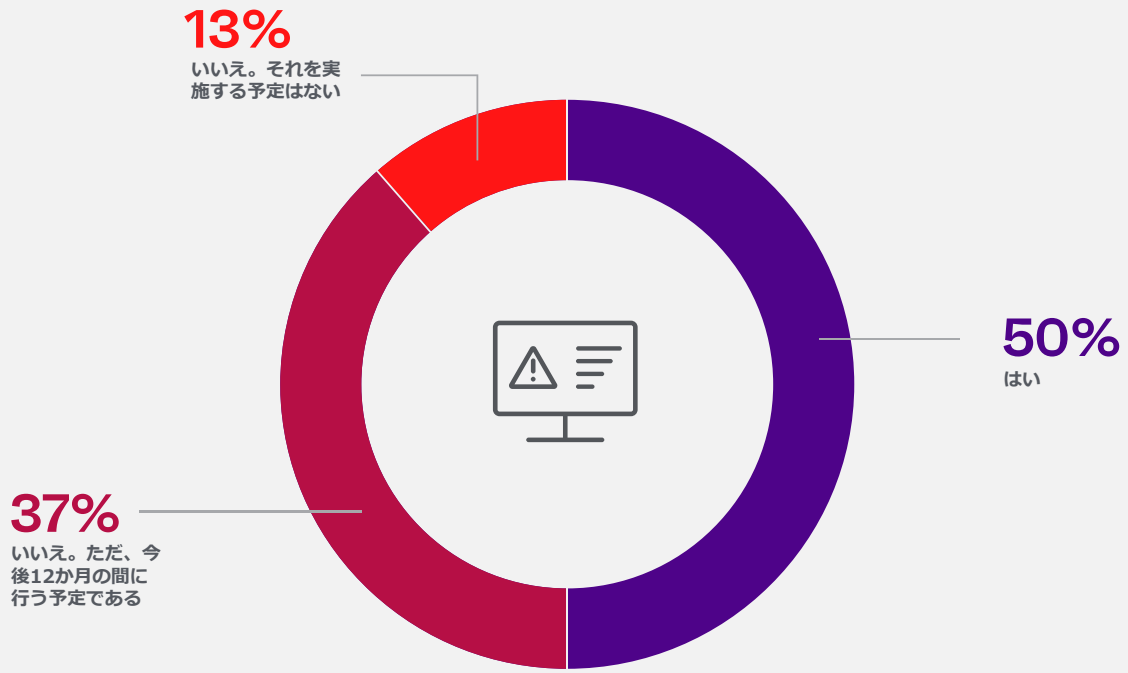
「今日のサプライチェーンは高度に相互接続されているため、あるパートナー (たとえばサードパーティベンダー) への脅威は、サプライチェーン全体への脅威となります」と、Ninjio の最高経営責任者である Shaun McAlmont 氏は述べています。[7]

CISO とそのセキュリティ組織は、サプライチェーンの脆弱性を特定し、強化するように急いでいますが、大多数はまだ深刻な遅れをとっています。

Ivantiの調査では、ソフトウェアのサプライチェーンにおいて最も脆弱なサードパーティシステムやコンポーネントをすでに特定していると答えたのは半数以下 (47%) でしたが、37%が今後 12か月以内にこのリスクに対処する予定であると回答しています。 また、46%が2023年のサプライチェーンの脅威を「高い」または「重大」だと評価しています。

## 懸念が高まるサプライチェーンリスク

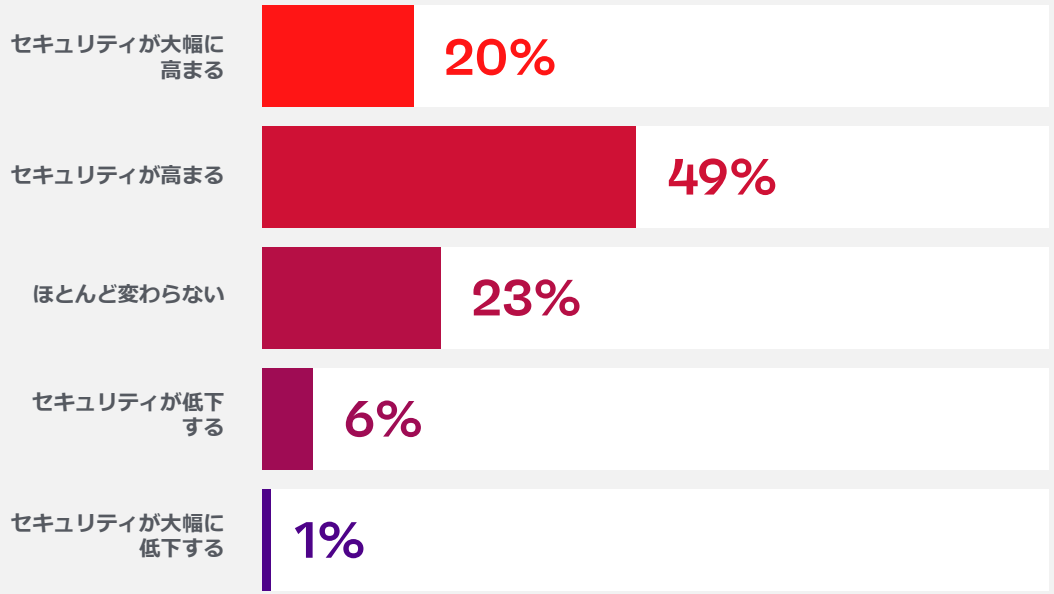
**Q:** あなたのチームでは、ソフトウェアのサプライチェーンにおいて最も脆弱であり、侵害された場合に組織に最大の影響を与えるサードパーティのシステム/コンポーネントを特定していますか。



# クラウドベースのリスクは過大評価されている

## クラウドベースのシステムは最終的にセキュリティを強化する

**Q:** クラウド環境で実現されるセキュリティリスクと機会の両方について考えてください。クラウドベースのシステムやストレージを採用することで、最終的にシステムのセキュリティが高まると感じますか、それとも低くなると感じますか。




### 3人に2人以上 (68%) が、クラウドベースのシステムやストレージを採用することで、システムのセキュリティが最終的に向上したと回答しています。

つまり、クラウドベースのシステムは、企業の許容範囲を超えたサイバーセキュリティリスクにつながるという誤解にもかかわらず、調査対象の経営陣やセキュリティの専門家は、リスクと機会を比較検討した結果、クラウドベースの環境はセキュリティを強化すると感じています。

Pure Storageの最高技術責任者である Andy Stone（アンディー・ストーン）氏は次のように述べています。「肯定的で安全な従業員のデジタル体験を確保することは、現代のIT経営者にとって新たな礎となります。 クラウドを安全かつ効果的に活用することで、従業員が好きな場所で、好きなデバイスを使って働くことができます。 デジタルファーストの世界では、安全にクラウドに移行できなければ、企業の成長は大きく停滞します。」

02

# 2023年 サイバーセキュリティの 注目点

サイバーセキュリティの担当者が2023年の上位の脅威と考えているのは何でしょうか。 また、既知の脅威と未知の脅威を含め、企業はどのような方法で攻撃に備えているのでしょうか。

ivanti

# 準備と経験のギャップ

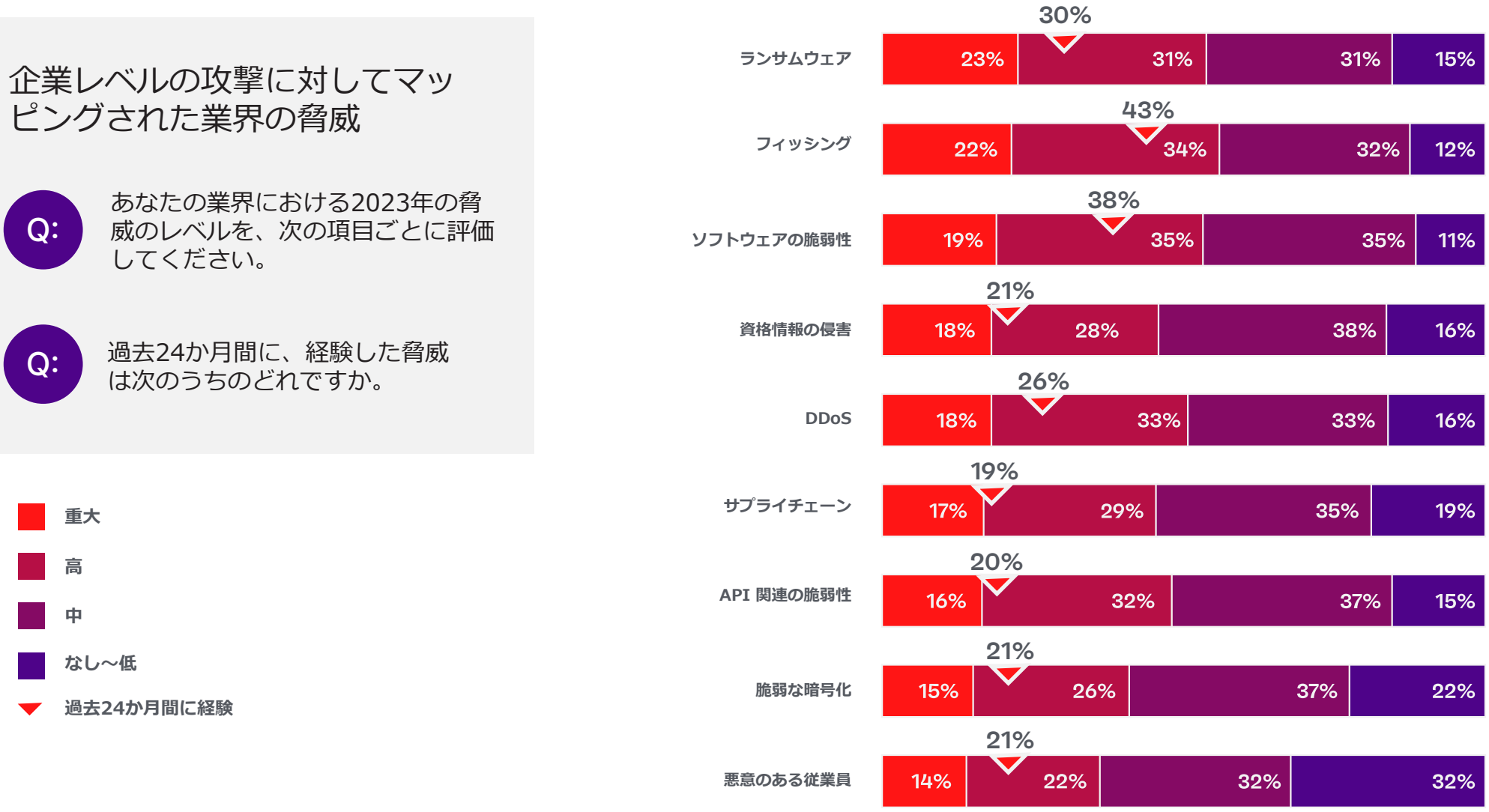
調査対象の専門家は、フィッシング、ランサムウェア、ソフトウェアの脆弱性を業界レベルの脅威の上位に挙げています。

企業が実際に経験した攻撃を比較すると、フィッシングやソフトウェアの脆弱性は、他のリスクを数倍上回っています。

## 企業レベルの攻撃に対してマッピングされた業界の脅威

**Q:** あなたの業界における2023年の脅威のレベルを、次の項目ごとに評価してください。

**Q:** 過去24か月間に、経験した脅威は次のうちのどれですか。



ある調査回答者は次のように答えました。

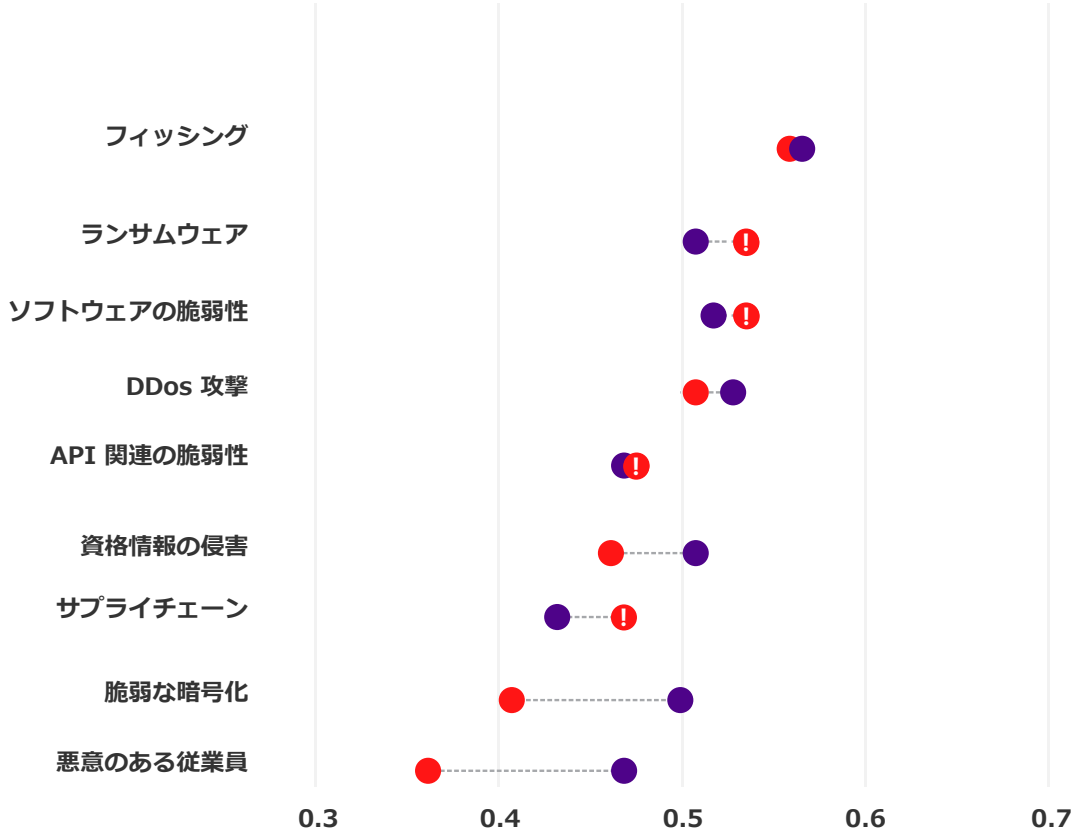
「高度なフィッシング詐欺を何度か経験したが、従業員は自分が狙われていることにまったく気づかなかった。この2年間で、この種の攻撃は非常に巧妙になり、経験豊富なスタッフでさえも餌食になっている。」

脅威の多様化にもかかわらず、回答者の多くが増大する脅威の状況に対応する準備ができていると回答しています。 約半数が、ランサムウェア、脆弱な暗号化、悪意のある従業員、ソフトウェアの脆弱性など、数え切れないほどの脅威に直面することに対して「十分に準備が整っている」と回答しています。

1つの注目点: サプライチェーンの脆弱性。 46%がサプライチェーンの脅威を高レベルの脅威と見なしている一方で、42%がサプライチェーンの脅威を保護することに対して十分に準備が整っていると回答しています。

このリスクは、準備のレベルが脅威の推定レベルに比べて遅れている「逆」の脅威のひとつに過ぎません。

## セキュリティの脅威に対するセキュリティの準備




Q: あなたの業界における2023年の脅威のレベルを、次の項目ごとに評価してください。

Q: ここに挙げた各種類の脅威に対処するために、どの程度準備が整っていますか。

- 高 + 重大な脅威
- 「十分に準備ができている」
- 逆の脅威

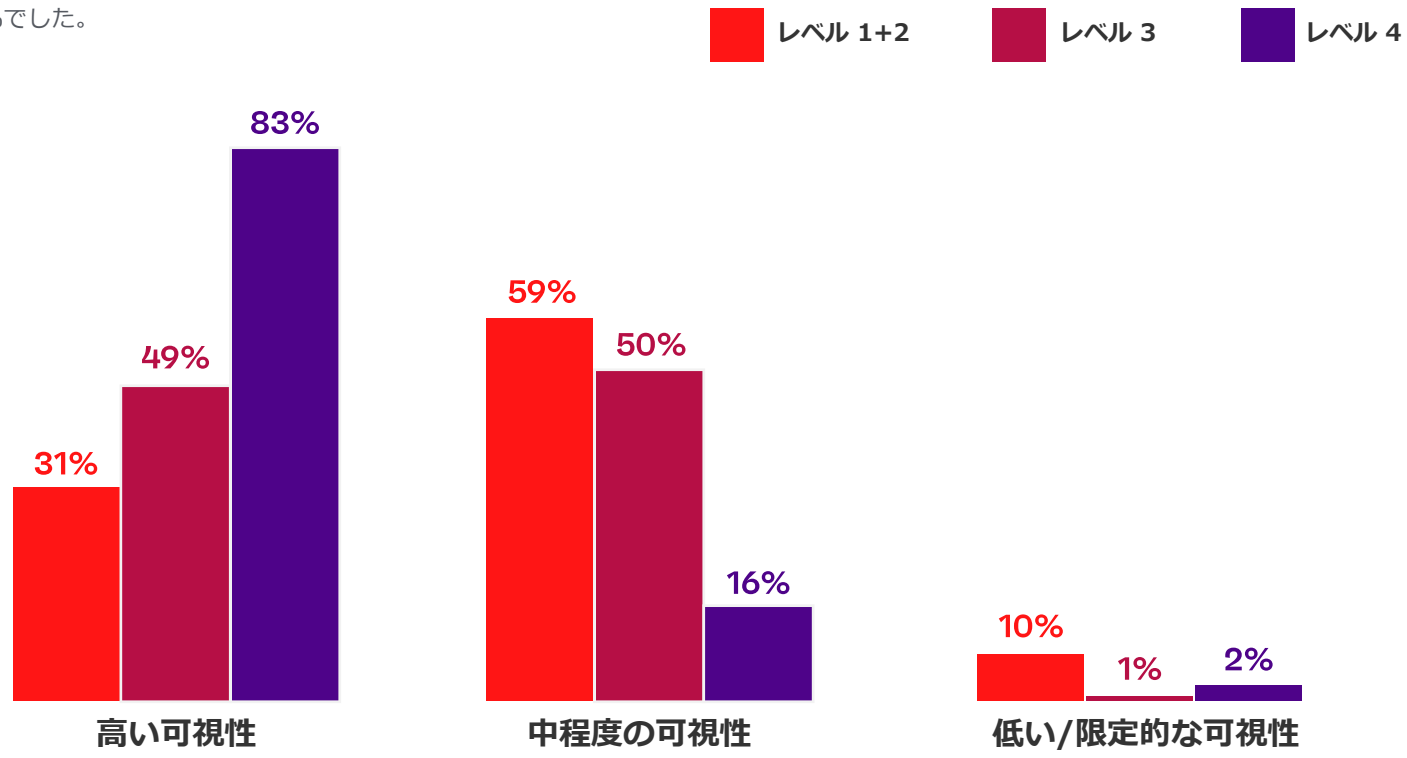
# 期待された保護対策が著しく欠如していることが判明

経営陣やセキュリティ専門家の半数強 (52%) が、ネットワーク上のすべてのユーザー、デバイス、アプリケーション、サービスに対して「高い可視性」があると回答しています。

また、資産検出プログラムを少なくとも週に1回実行していると答えたのは、わずか48%でした。

## 業界トップの企業は資産の可視性が高い

Q: あなたの会社では、ネットワーク上のすべてのユーザー、デバイス、アプリケーション、サービスがどの程度可視化されていますか。(サイバーセキュリティ成熟度レベルで示されます。)

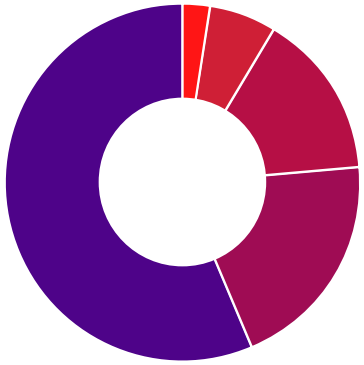


ほぼすべての企業が、デプロビジョニングのための正式なプロセスがあると回答し、大多数 (68%) が退職する従業員のデプロビジョニングは3営業日以内に行われると回答しています。 (外部ベンダーについては、81%が5営業日以内にプロセスが実施されると回答しています。)

しかし、セキュリティ専門家は、デプロビジョニングのガイダンスが3分の1の割合で無視されていると述べました。これは関連するリスクを考えると、衝撃の告白です。

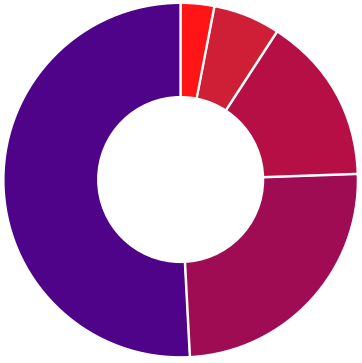
## デプロビジョニングについては、適正な手順が導入されていますが、結果はさまざまです。

**Q:** 従業員が退職した後、どの程度迅速に従業員の資格情報をデプロビジョニングしていますか。



- 2% 資格情報をデプロビジョニングする正式なプロセスがない
- 5% わからない
- 12% 8 営業日以上
- 16% 4 ～ 7 営業日
- 45% 2 ～ 5 営業日

**Q:** 契約終了時やサービス解除時に、サードパーティベンダー、コンサルタント、請負業者の資格情報をどの程度迅速にデプロビジョニングしていますか。



- 2% 資格情報をデプロビジョニングする正式なプロセスがない
- 4% わからない
- 10% 8 営業日以上
- 16% 4 ～ 7 営業日
- 33% 2 ～ 3 営業日

# 幽霊資格情報の蔓延

さらに顕著なのは、調査対象者の45%が、元社員や元契約社員が会社のシステムやファイルにまだアクセスできる疑いがあると答えています。これは、デプロビジョニングのガイダンスが正しく守られていなかったり、資格情報が無効化された後でもサードパーティ製アプリが隠れたアクセス権を提供したりしていることなどが原因だと考えられます。

Ivantiの最高製品責任者である Srinivas Mukkamala（スリニヴァス・ムッカマラ)博士は次のように述べています。「多くの場合、大企業は、従業員の退職時に、アクセスを許可するアプリ、プラットフォーム、サードパーティサービスという巨大なエコシステムを考慮できていません。 私たちはこれを幽霊資格情報と呼んでいますが、驚くほど多くのセキュリティ専門家や経営陣が、いまだに以前の雇用主のシステムやデータにアクセスできるのです。

**45%**

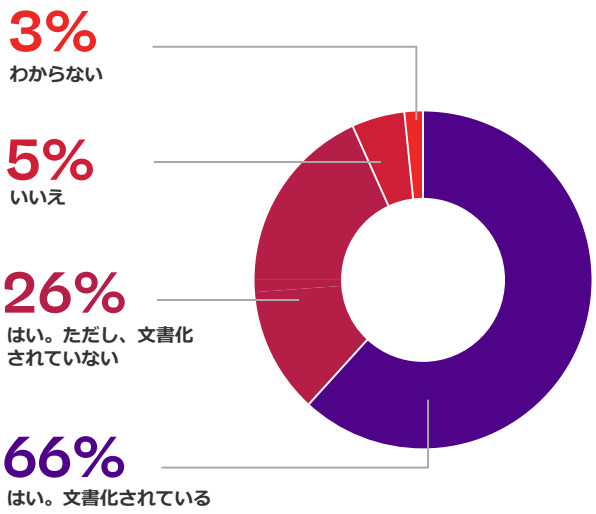
セキュリティの専門家の45%は、元従業員や元契約社員が、まだ有効なユーザー名、パスワード、ログイン情報の形でシステムやファイルにアクセスできる疑いがあるか、確実にアクセスできると回答しています。

# すべてのパッチが優先される場合、どのパッチも優先されることはない

92%がパッチを適用する脆弱性の優先度を決定する方法があると答えていますが、そのうちの4人に1人以上は、これらの方法が何らかの方法で文書化されていないと回答しています。

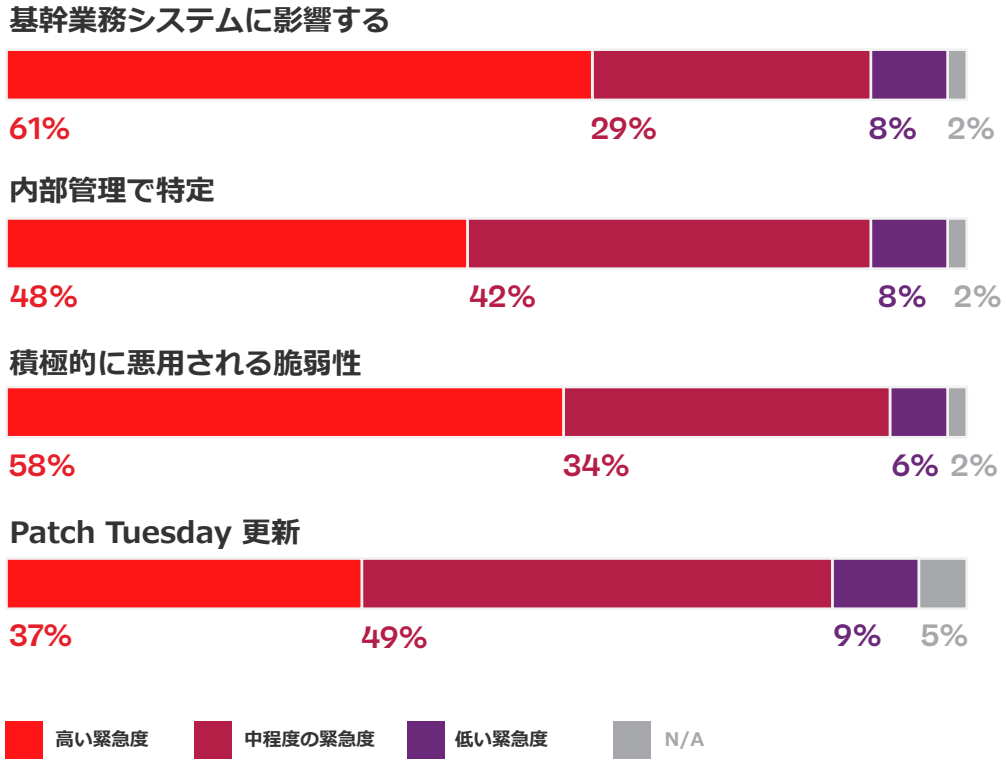
しかし、どの種類のパッチを優先するのかという質問に対しては、セキュリティ専門家は、すべての種類のパッチが上位にランクされると回答しています。つまり、何も優先されないということです。

Q: サイバーセキュリティチームには、パッチを適用する脆弱性の優先度を決定する方法がありますか。




## パッチ管理は「すべてが緊急」の風潮に悩まされる

Q: どのようにパッチを適用する脆弱性の優先度を決定していますか。



この「すべてが緊急」という考え方は、セキュリティチームの優先度を混乱させるだけでなく、高いレベルのストレスや燃え尽き症候群を引き起こす可能性があります。

IBMが1,100人のインシデント対応者を対象に行ったグローバル調査では、68% が一度に2つ以上のインシデントを担当するのが一般的だと回答しています。 この調査では、「仕事の疲れが出ているようです。同程度の64%の人が、不眠、燃え尽き症候群、不安のために精神衛生上の支援を求めたことがあると答えています」と説明されています。[8]

Ivantiが以前に行った調査でも、同様の課題が明らかにされています。離職を促す要因は何かという質問に対して、IT担当者は、仕事量の多さ (41%) とチームにかかる非現実的な期待 (34%) を上位に挙げています。[9]

# ホエーリング攻撃の危険性

ホエーリング攻撃とは、サイバー脅威者がカスタマイズしたスピアフィッシングの手法を使って、CEO や政治家、政府高官といった重要で価値の高いターゲットである「クジラ」を追いかけることです。

いったん「クジラ」が危険にさらされると、攻撃者は機密情報へのアクセスを獲得し、電信送金を承認したり、上司に命令されないかぎり通常なら決して同意しないような行動を従業員に強制したりすることさえ可能になるのです。

# サイバーセキュリティのリスクは認識していると回答しながらも、まだリスクのある行動を取っている経営陣

経営陣 (CEO、副社長、取締役など) の約10人に9人が、職場でマルウェアやフィッシングなどの脅威を認識し、報告する体制が整っていると回答しています。

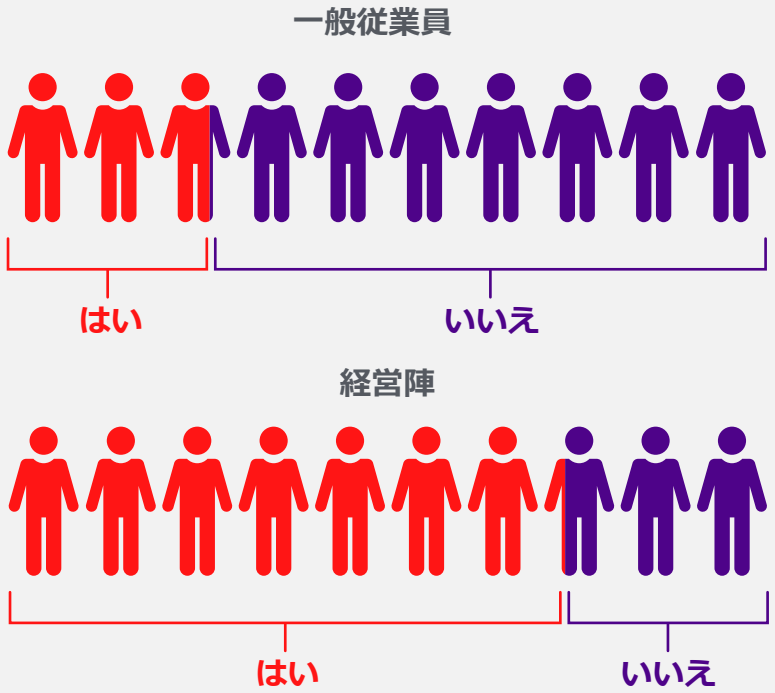
また、調査対象の他の従業員と比較して、質問や懸案事項がある場合にセキュリティチームに相談したことがあると回答した割合が有意に高くなっています。

このことは良い兆候なのですが、当社の調査によると、経営陣はセキュリティチームとの否定的な対話を報告する傾向が圧倒的に強く、セキュリティの問題を報告する際に「安全だと感じられない」と答える傾向が1.3倍にもなることがわかっています。

その上、経営陣の行動、つまり組織のリーダーが認める日常的な習慣は、さらに懸念されます。

セキュリティ対策に取り組んでいるという経営陣

Q: セキュリティに関する疑問や懸案事項を、職場のサイバーセキュリティ担当者に相談したことがありますか。



# 危険の大きい行動を取る経営陣

CEO、副社長、取締役などの「経営陣」の回答者は、他の知識労働者よりもセキュリティ上危険な行動を取る可能性が高くなっています。

- 調査対象の経営陣の3分の1以上がフィッシングのリンクをクリックした経験があり、これは他の従業員の4倍の割合になります。
- 経営陣の約4人に1人近くが覚えやすい誕生日をパスワードの一部として利用
- 経営陣は、従業員と比べ、パスワードを定期的に更新せず、何年も同じパスワードを使い続ける傾向が圧倒的に強くなっています。4人に1人がこの行為を行っています。
- 調査対象の経営陣は、パスワードを社外の人と共有する可能性が5倍も高くなっています。

ホエーリング攻撃の成功は、従来のフィッシングの試みよりもはるかに大きな脆弱性ですが、多くの企業では、いまだに比類ない巨大な脅威として捉えられていません。

より高度なフィッシング攻撃で狙われる経営陣は、他の従業員に比べ、4倍もフィッシングの被害に遭う確率が高いという点を考えてみてください。

(流し読みしている方のために繰り返します。最も価値の高い従業員は、攻撃者に対してセキュリティの扉を開いてしまうような行動を取る可能性が4倍も高いのです)。

このようなリスクから、企業はCEOやその他の上級幹部のために、カスタマイズされたトレーニングカリキュラムや技術的な介入を開発し、これらの非常に脆弱なターゲットに対する保護を強化する必要があります。

経営陣 (CEO、副社長、取締役など) の3人に1人以上がフィッシング詐欺の被害に遭い、詐欺のリンクをクリックしたり、送金したりした経験があります。

04

# 2023年以降の企業の将来を見据える方法

Ivantiの研究の一環として、研究チームは、サイバーセキュリティ成熟度の尺度でレベル 4と自己申告している、成熟度の高いサイバーセキュリティ組織である企業を調査しました。 調査内容: このグループはどのような点で優れているのでしょうか。また、他の組織はどのようにこれらの企業から学ぶことができるのでしょうか。

ivanti

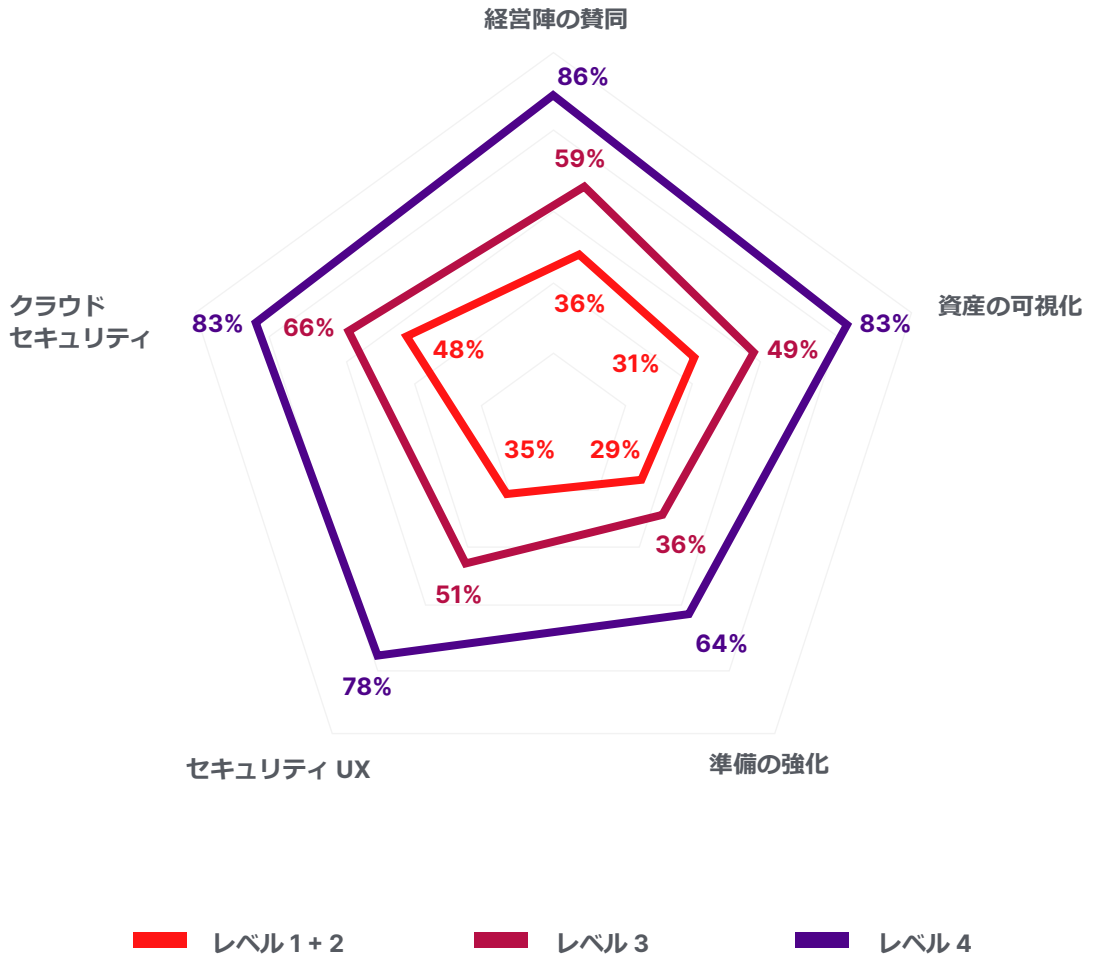
# サイバーセキュリティ成熟度の尺度

この調査では、サイバーセキュリティ業務に従事している回答者に、組織のサイバーセキュリティ準備レベルを基本 (レベル 1) から上級 (レベル 4) までの尺度で評価してもらいました。 そして、これらのコホートを比較することで、レベル 4 の組織の慣行と行動についてより詳しく分析しました。

## 成熟度の高いサイバーセキュリティ組織は、より多くの賛同を得て、可視性とUXへの注目を高めていると報告

グラフは、次のように報告した回答者の割合を示しています。

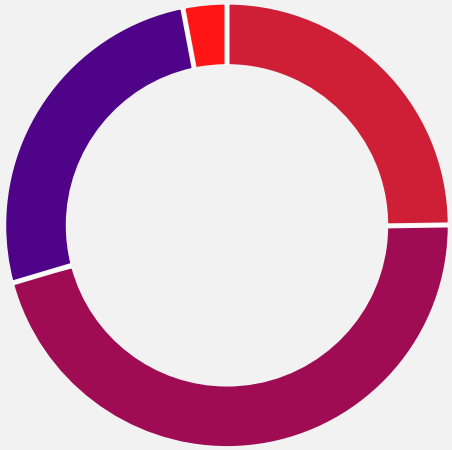
- 非常に協力的な経営陣 (「経営陣の賛同」)
- ネットワーク上のユーザー、デバイス、アプリケーション、サービスに対する高い可視性 (「資産の可視性」)
- 業界内のサプライチェーンの脅威に対して十分に備えている (「準備の強化」)
- サイバーセキュリティ関連の技術介入におけるエンドユーザー向けUXの優先度が高い (「セキュリティ UX」)
- クラウドベースのシステムやストレージの採用におけるセキュリティ強化 (「クラウドセキュリティ」)



注記: 人が自分の努力を評価する際にはバイアスがかかる可能性があるため、自己申告による情報収集には限界があります。 レベル1の回答が例外的に少ないのは自己申告の影響もあると思われます。このレポートでは、レベル1はレベル2にまとめられています。

この成熟度モデルに基づく次の調査結果は、サイバーセキュリティ分野に有益なシグナルを提供すると考えていますが、読者の皆様には研究の限界に留意されますようお願いいたします。

## サイバーセキュリティ専門家のレベル別回答

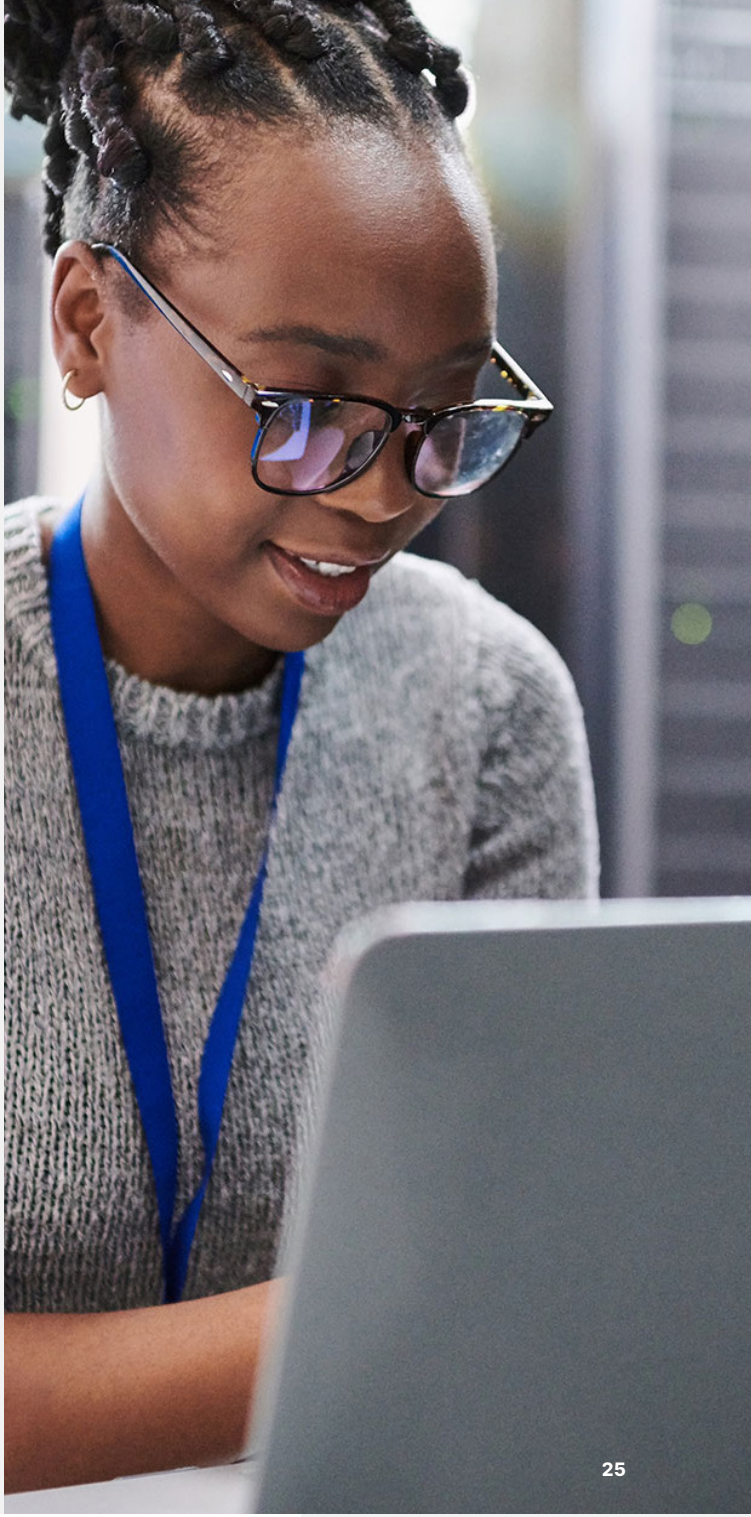


**4%**
**レベル 1:** 基本的なサイバーセキュリティ衛生

**25%**
**レベル 2:** 手順とポリシーが確立された中程度のサイバーセキュリティ衛生

**42%**
**レベル 3:** 堅牢で能動的なサイバーセキュリティ衛生

**29%**
**レベル 4:** 高度な脅威から組織を防御する高度な実証済みの能力



# レベル 4 のサイバーセキュリティ組織は何が違うのでしょうか

**経営陣の賛同:** 自己申告レベル4の組織の大多数 (86%) は、上層部からの賛同とサポートがあると回答しています。 費用対効果に関係なくCEOの最新の優先事項を追いかけるのではなく、防衛力を強化するための予算支援や、先を見越した戦略を設計するための自律性など、さまざまな形で賛同が表面化する可能性があります。

**資産の可視化:** ほとんどのレベル4 (83%) は、組織全体のユーザー、アプリケーション、デバイスを高いレベルで可視化しています。 実際に、レベル3の組織と比較すると、70% 以上の確率でこの点が実証されています。 デバイスやアプリケーションの数が爆発的に増える中、2023年には可視化が大きなテーマになることが予想されます。

最近、CISAは2022年末に新しい指令 (BOD 23-01) を発行し、この必要性を強調しました。 CISAの役員であるJen Easterly（ジェン・イー廃り―）氏は、「ネットワーク上に何があるかを知ることは、どの組織にとってもリスクを減らすための最初のステップです」と説明しています。

**サプライチェーンのレジリエンス:** サプライチェーンの準備に関しては、レベル 4 は、調査対象の他のすべての企業と比較して、十分に準備していると報告しています。サプライチェーンの脅威に直面した場合、64% が「十分に準備している」と答えているのに対し、レベル 3 ではわずか 36%でした。

EquinixのSVP兼CISOである Michael Montoya（マイケル・モントヤ）氏は次のように述べています。「サプライチェーンへの対策は、問題が非常に複雑化する可能性もあることから、多くの企業がいまだに適応に苦慮している分野の1つです。 「2023年には、ソフトウェア部品表 (SBOM) の導入から、ゼロトラストソリューションや包括的なアクセス制御の展開など、サプライチェーンのリスク低減が大きな投資分野となると予想しています。」

**リスクを低減するためのUX:** クラス最高の企業は、優れたユーザーエクスペリエンスがセキュリティの不可欠な要素であり、不十分な順守やリスクの高い回避策に対する解毒剤として効果的であることを理解しています。 ほとんどのレベル4の組織では、エンドユーザー向けのUXを「優先度が高い」または「最も重要度が高い」と回答した人が71%と、レベル3より20ポイントも高くなっています。

**クラウドのセキュリティ:** レベル4の組織は、クラウドベースのシステムでは最終的にセキュリティが高いと回答する割合が大幅に高くなっています。 実際、レベル3の組織に比べ、クラウド環境は「大幅にセキュリティが高い」と回答する割合が3倍にもなっています。

「現在のインフレ圧力とマクロ経済状況は、クラウド支出を刺激して引き付ける効果をもたらしています。 クラウドコンピューティングは、その機敏性、弾力性、拡張可能性により、不確実な時代の成長を支え、安全性とイノベーションの砦であり続けるでしょう。」― Sid Nag 氏 (Gartner®[11] 部長兼アナリスト)

ひとつだけ確かなことは、完全に防御的な戦術は 2023 年には通用しないということです。UnitedHealth Group のグローバルサイバーリスク・防御担当上級部長である Michael Levin（マイケル・レヴィン）氏は、次の概念をWall Street Journal紙で説明しました。「多くの組織が、まだ初期のチェックリストやコンプライアンスに集中しています。 言われたことは全部やったから安全だ』と考えるのではなく、『どうしたら安全になるのか』を考える必要があります。」[12]

セキュリティの専門家や経営陣の圧倒的多数が、1年前と同じかそれ以上の準備を整えていると回答しています。なんと、97%がこのように回答しています。 しかし、5人に1人はチョコレートバーを賭けないのです。 楽観主義、現実を見る。

変化の激しい、まだ見ぬ脅威に対処するためには、組織が「やるべきことはすべてやった」という反応的なルールベースのスタンスから脱却することが必要です。

成熟しているサイバーセキュリティチームは、次の点についても検討してください。

**自動化:** 自動化を導入して資産の可視性を高め、リスクに応じた優先順位でパッチをします (いずれも2023年の安全な企業の必須条件)。また、スマートUXを使用して、従業員が強制的に優れたセキュリティ行動を取るようにします (例: 例外や回避策がかえって面倒になる)。

**レジリエンス:** 一部の攻撃は必然的に突破することを認識した上で、停電時間を短縮し、波及効果を抑えるための対応・復旧計画を策定します。

**権限委譲:** サイバーセキュリティチームに与える、セキュリティの課題を設定するための独立性を拡大します。ニュースになる最新の脅威に対して軽率に反応したり、常に変化する膨大な優先事項リストを達成できなかったことでチームを罰したりすることはもうありません。

**全体的なリスク管理:** 場所に縛られない働き方 (WFE) やハイブリッド社員、サードパーティの請負業者やベンダーなど、組織の壁を越えたセキュリティについて考えます。 このような相手に対しては、リスクとリターンを考慮したアプローチを取ります。経営幹部や高度に組み込まれたソフトウェアサプライヤーなど、セキュリティの「クジラ」に対しては最大限の注意を払うようにします。

## 最終的に、サイバーセキュリティに対する準備が、反応的で防御的なものから、将来を見据えた回復力が高いものへとリセットされたとき、チョコレートバーの賭けに応じる組織が増えると考えています。

05

# 調査方法

Ivantiは、2022年10月に 6,500人以上の経営陣、サイバーセキュリティの専門家、従業員を対象に調査を実施しました。 目的としては、セキュリティ専門家と他のすべての従業員の視点から今日の脅威を理解し、まだ知られていない将来の脅威に企業がどのように備えているのかを把握することです。

この調査はRavn Researchが実施し、パネリストの募集は MSI Advanced Customer Insights が行いました。 調査結果は重み付けなしで表記されています。 国別の詳細については、お問い合わせください。

## 調査対象サンプル

従業員
5,202

セキュリティの専門家
902

経営陣
454

## 業界別

6%
教育

12%
金融サービス

12%
政府

13%
製造/処理

3%
非営利/慈善事業

18%
その他 (具体的に)

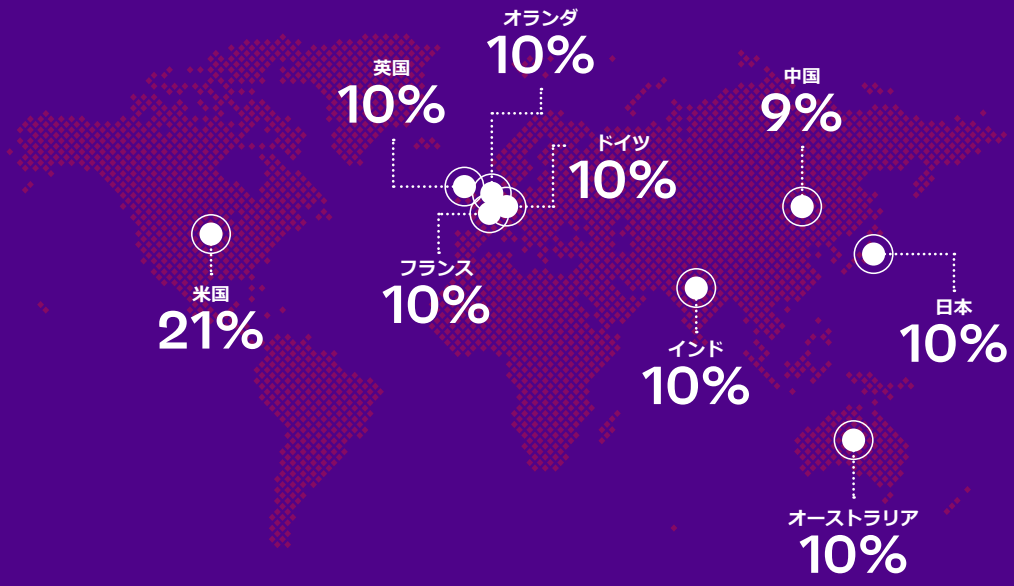
8%
プロフェッショナルサービス

11%
小売・eコマース・卸売

14%
技術

3%
通信

## 国



# 参考文献

このレポートのすべてのグラフは、「方法論」で説明したように、Ivanti State of Cybersecurity Preparedness 2023 シリーズの一環として収集された調査データから作成したものです。


1. PwC: “A C-suite united on cyber-ready futures: Findings from the 2023 Global Digital Trust Insights,” Sept. 2022. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

2. SHRM: “2023 Salary Budgets Projected to Stay at 20-Year High but Trail Inflation,” Sept. 2022. https://www.shrm.org/resourcesandtools/hr-topics/compensation/pages/2023-salary-increase-budgets-stay-trail-inflation.aspx

3. The Wall Street Journal: Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate,” Oct. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

4. IBM: “Cost of a data breach 2022: A million-dollar race to detect and respond,” July 2022. https://www.ibm.com/reports/data-breach

5. The Wall Street Journal: “Microsoft’s New Security Chief Says It Is Time to Take Shelter in the Cloud,” Feb. 2022. https://www.wsj.com/articles/microsofts-new-security-chief-says-it-is-time-to-take-shelter-in-the-cloud-11645624800

6. InfoSecurity Group: “Cybersecurity Workforce Gap Grows by 26% in 2022,” Oct. 2022. https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows/

7. Supply Chain Brain: “Why Cybersecurity Has Never Been More Important for the Supply Chain Sector,” Oct. 2022. https://www.supplychainbrain.com/blogs/1-think-tank/post/35798-why-cybersecurity-has-never-been-more-important-for-the-supply-chain-sector

8. The Wall Street Journal: “Rise in Cyberattacks Stretches and Stresses Defenders,” Oct. 2022. https://www.wsj.com/articles/rise-in-cyberattacks-stretches-and-stresses-defenders-11664962202

9. Ivanti: “State of IT in 2021,” Dec. 2021. https://www.ivanti.com/company/press-releases/2021/new-ivanti-study-finds-the-biggest-challenge-for-it-departments-is-keeping-up-with-digital-transformation-and-keeping-talent-in-technical-roles

10. CISA: “CISA Directs Federal Agencies to Improve Cybersecurity Asset Visibility and Vulnerability Detection,” Oct. 2022. https://www.cisa.gov/news/2022/10/03/cisa-directs-federal-agencies-improve-cybersecurity-asset-visibility-and

11. Gartner Press Release: “Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023,” Oct. 2022. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023. GARTNER は Gartner, Inc. およびその関連会社の米国内および国際的な登録商標およびサービスマークであり、 許可を得て本書で使用しています。 All rights reserved.

12. The Wall Street Journal: Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate,” Oct. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102


# 追加のグラフ情報

Pg. 3 - セキュリティおよび経営陣の回答者; n=1,356

Pg. 5 - セキュリティおよび経営陣の回答者; n=1,356

Pg. 7 - セキュリティおよび経営陣の回答者; n=1,356

Pg. 8 - セキュリティ回答者; n=902

Pg. 9 - セキュリティおよび経営陣の回答者; n=1,341

Pg. 11 - セキュリティ回答者; n=902

Pg. 13 - セキュリティ回答者; n=902

Pg. 14 - セキュリティおよび経営陣の回答者; n=1,356

Pg. 15 (「従業員の資格情報」) - セキュリティ回答者; n=902

Pg. 15 (「サードパーティベンダーの [...] 資格情報」) - セキュリティ回答者; n=882

Pg. 17 (「優先度を決定する方法」) - セキュリティ回答者; n=902

Pg. 17 (「優先度を決定する方法」) - セキュリティ回答者; n=886

Pg. 20 - 経営陣と従業員の回答者; n=5,656

Pg. 21 (「3 分の 1 以上」) - 経営陣と従業員の回答者; n=1,949

Pg. 21 (「約 4 人に 1 人」) - 経営陣と従業員の回答者; n=5,656

Pg. 21 (「経営陣は圧倒的に」) - 経営陣と従業員の回答者; n=5,373

Pg. 21 (「調査対象の経営陣」) - 経営陣と従業員の回答者; n=5,656

Pg. 24 (「経営陣の賛同」) - セキュリティと経営陣の回答者; n=1,356

Pg. 24 (「資産の可視性」) - セキュリティと経営陣の回答者; n=1,356

Pg. 24 (「準備の強化」) - セキュリティ回答者; n=902

Pg. 24 (「セキュリティ UX」) - セキュリティ回答者; n=902

Pg. 24 (「クラウドセキュリティ」) - セキュリティと経営陣の回答者; n=1,341

# Press Reset:

## 2023 サイバーセキュリティ体制の現状レポート

企業はサイバー攻撃から会社を守ろうと急いでいますが、業界では事後対応
やチェックリストの考え方に悩まされています。

ivanti

ivanti.co.jp
+81 (0)3-6432-4180
contact@ivanti.co.jp