Securify

企業の
セキュリティ対策の
現状と課題を探る

セキュリティ関係者 1045人に聞いた！

実態調査（2024年5月）

3-SHAKE

はじめに

デジタル化が進展する現代において、企業のセキュリティ管理はますます重要となっています。
この度、Securify ではセキュリティ関連業務の担当者を対象にアンケート調査を実施しました。

具体的なデータを基に、
「担当者の情報」「企業の課題」 の 2 つの観点での結果をこのコンテンツで紹介します。
今回の調査、考察をご覧いただき、より安全なビジネス運営に向けた一助となることを目指しています。

■調査概要

- 調査期間：2024 年 4 月 17 日 ～ 19 日
- 調査対象者：セキュリティ関連業務に従事する方
- 調査人数：1045 人
- 調査手法：インターネット調査
- 調査元：株式会社ゼネラルリサーチ

■調査データの引用・転載に関して

本調査データを外部メディアなどに引用・転載される場合は下記の利用条件を守ってご利用ください。

《利用条件》

情報の出典元として、Securify（もしくはセキュリファイ）の名称を明記してください。

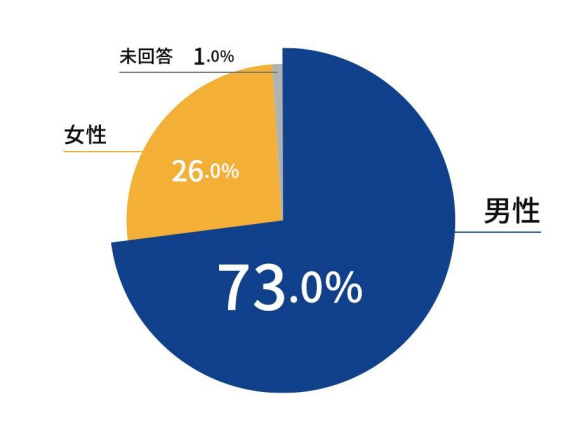
Securify

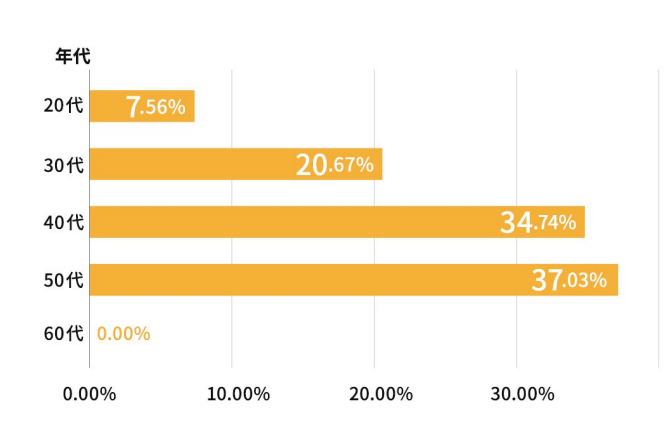
担当者の情報

セキュリティ関係者における性別と年代の分布は？

セキュリティに関連する業務を行っている担当者の性別と年代についてのデータは、
男性が全体の **約 73 %**、女性は **約 26 %**です。セキュリティ業界における性別の偏りがあるようです。

年代別に見ると、50代が最も多く**約 37.03 %**を占め、次いで40 代が **約 34.74 %**となっており、
これらの年代の経験豊富なプロフェッショナルが業界の中核を担っていることが見て取れます。
20 代は **約 7.56 %**と少なめであり、セキュリティ分野への新しい人材の流入が少ないのかもしれません。



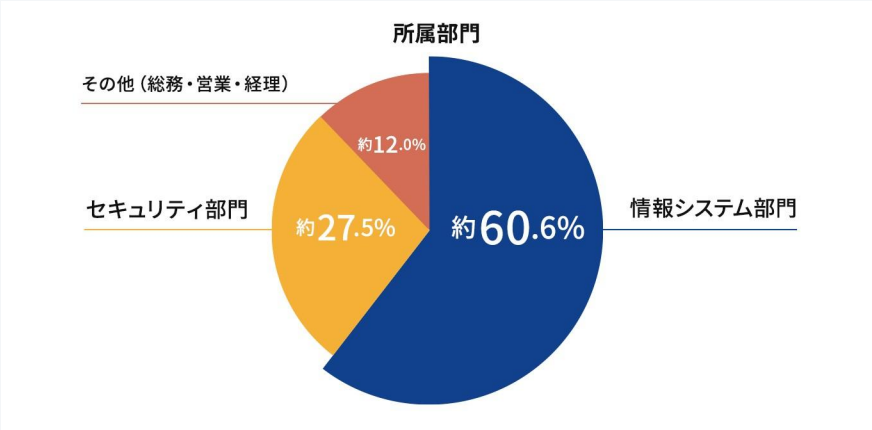


Securify

セキュリティ担当者の所属部門とその役割は？

セキュリティに関連する業務の担当者の所属部門の分布を見ると、**約 60 %**が情報システム部門に所属しており、
これには社内システムの開発や管理、IT 機器の運用といった業務が含まれます。
セキュリティはこれらの業務の一環として扱われることが多いです。

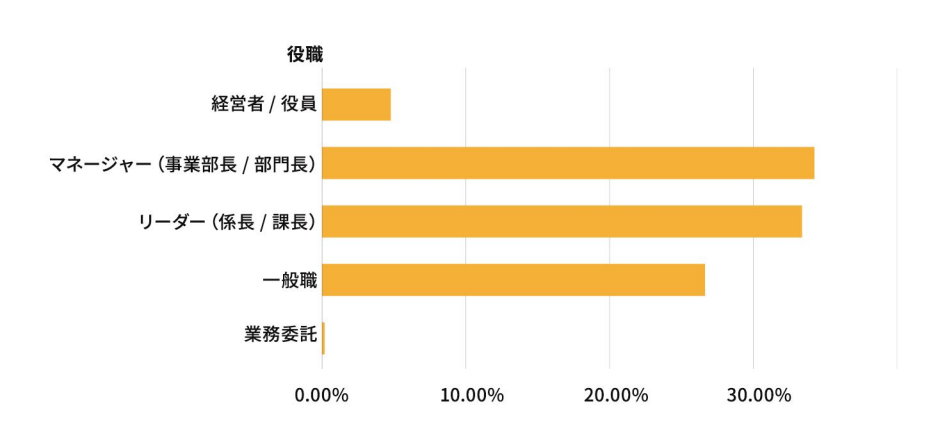
また、専門のセキュリティ部門に全専任で勤務している担当者は全体の**約 30 %**に上り、
セキュリティ専門のアナリストやエンジニアといった知識と技術が求められる業務を担当しています。
残りの **12 %** はその他の部門に属し、日常業務にセキュリティの責務を兼ねている様です。



セキュリティ関係者の役職は？

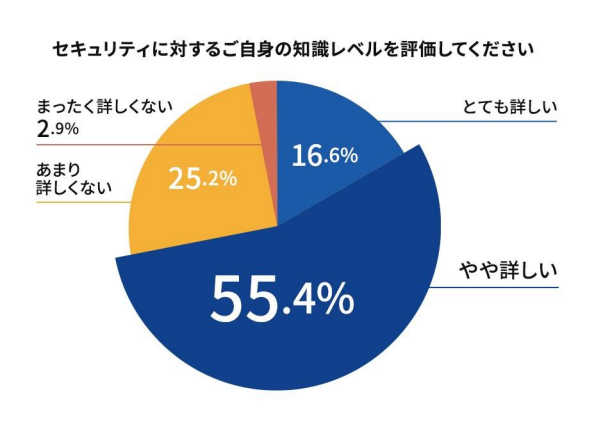
セキュリティについては中間管理職が特に重要な役割を担っていることが、以下のデータから明らかになりました。
組織内でセキュリティ文化の推進者として、また、具体的なセキュリティ対策の実行者としての責任が大きいためでしょうか。経営層の数は少ないものの、経営層の意思決定が組織全体のセキュリティ戦略に大きな影響を及ぼすため、セキュリティの重要性に関する理解とサポートを得ることが不可欠です。

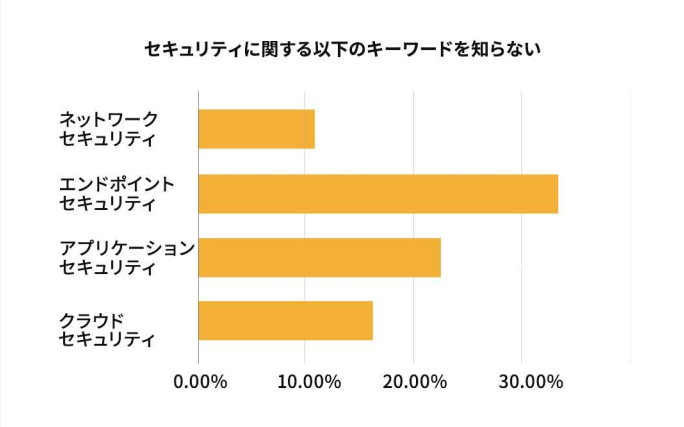
経営層の理解・支持があることで、セキュリティポリシーの策定が迅速に進み、必要なリソースの確保や適切な予算の配分が可能となり、全社的なセキュリティ対策の効果を高める鍵となっています。



セキュリティ担当者の知識レベルの自己評価と課題は？

実際にセキュリティ担当者は自身の知識レベルをどのように評価しているのでしょうか。
約 3 割が詳しくない傾向の回答をしております。進展、変化が激しいセキュリティ事情に自信が無い担当者が
一定以上存在することがわかります。特に「エンドポイントセキュリティ」と「アプリケーションセキュリティ」の
不知識率が **33.4 %**と **22.4 %**と高くなっておりました。
これらの領域は、比較的新しい技術や戦略を含むため、不知識率が高くなっていると伺えますが、
現代のサイバーセキュリティの中核をなす技術領域となるため、定期的な情報収集、知識更新が必要と言えます。

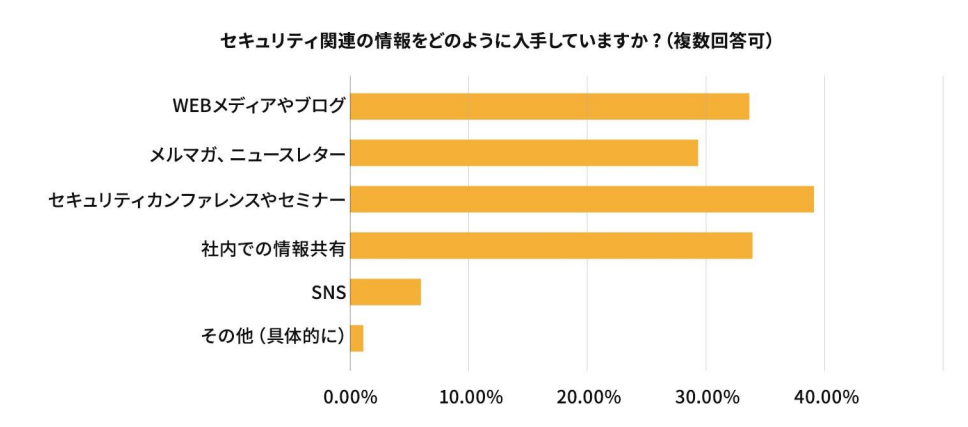




セキュリティ担当者の情報収集方法とその傾向は？

決まった媒体に依存するのではなく、情報収集のために多様な方法を利用していることが分かりました。
特にセキュリティカンファレンスやセミナーが最も利用されている情報源であることが示されており、
業界内での最新の知識とトレンドをキャッチアップするための重要な手段であることがわかります。

また、Webメディアやブログ、社内での情報共有も**約 40 %**と高い割合で利用されており、情報の即時性と
アクセシビリティが求められていることが伺えます。一方で、SNSの利用率が**7.08 %**と低いことは、
セキュリティ情報に関しては信頼性や専門性が重視される傾向にあることを示しているのかもしれません。

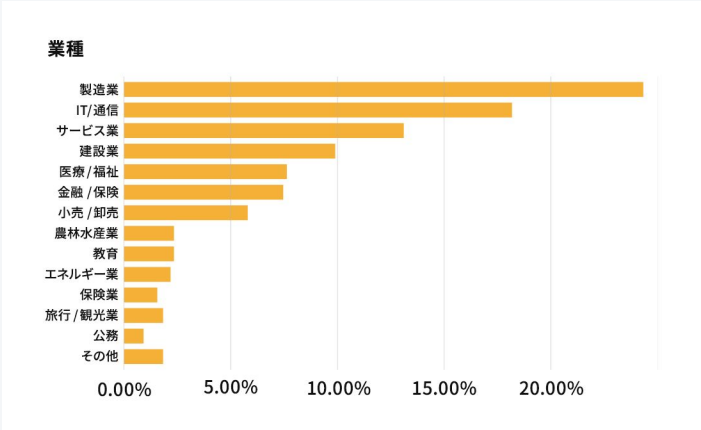


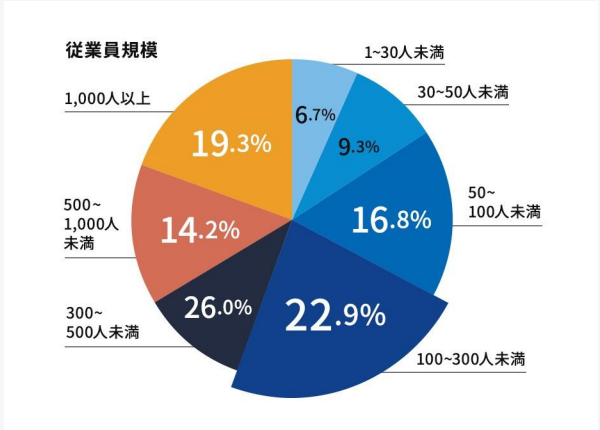
Securify

企業の課題

ご勤務先の業種、従業員規模を教えてください

多様な産業にわたってセキュリティの重要性が認識されていることが明らかです。
最も大きな割合を占めるのは製造業で **24.50 %**、次いでIT/通信業が **18.28 %**となっています。
これは、製造業が生産設備のデジタル化やIoT技術の導入が進む中でサイバーセキュリティのリスクが高まっていること、IT/通信業が業界として自然にテクノロジーと密接であるため、セキュリティ対策が不可欠であることを示しています。
従業員規模が 100 ～ 300 人未満の企業に所属と回答した層が **約 22.87 %**を占め、この規模の企業がセキュリティにおいて活発な取り組みを行っていることが分かります。全体の**約 19.33 %**にあたる1,000 人以上の大企業に所属と回答した層では、大規模なデータと複雑なシステムの管理が求められていると考えられます。



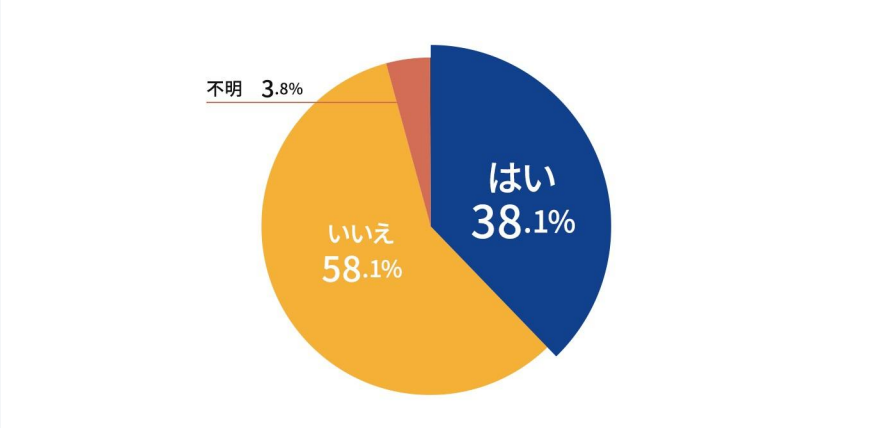


Securify

過去1年間に、セキュリティインシデント（データ漏洩、サイバー攻撃等）の経験はありますか？

過去１年間におけるセキュリティインシデント（データ漏洩、サイバー攻撃等）の発生状況を調査した結果、
回答者の **約 38.09 %**が何らかの形でセキュリティインシデントを経験していることが明らかになりました。
多くの企業がセキュリティの脅威に直面している現実を示しています。

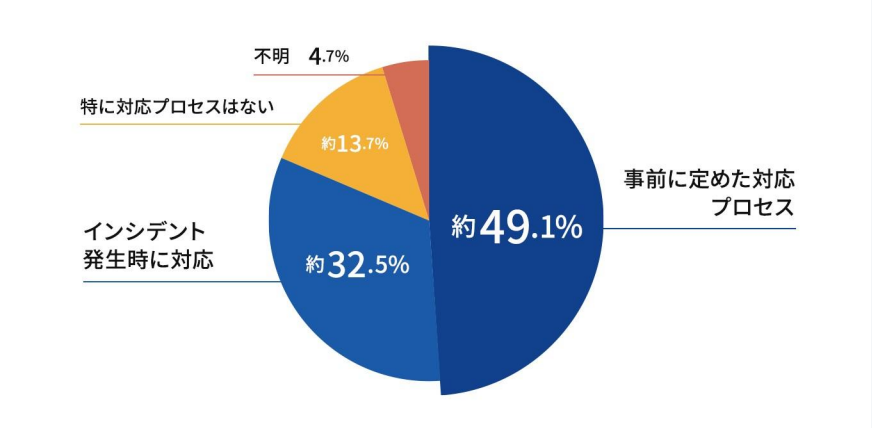
一方で、**58.09 %**の企業が過去１年間においてセキュリティインシデントを経験していないと報告していますが、
セキュリティリスクは常に進化するため、継続的な改善が必要となります。



Securify

セキュリティインシデントが発生した際の対応プロセスの有無を教えてください

セキュリティインシデントが発生した際の対応プロセスについて調査した結果、**約 49.09 %**が事前に定めた対応プロセスを持っていると回答されました。組織が予期しないセキュリティ事件に迅速かつ効果的に対応できる体制を整えていることは、予め策定されたプロセスがインシデント対応の質、速度を向上させることができ、非常に重要です。
対照的に**32.54 %**の企業はインシデントが発生した時点で対応を決定しており、これは計画的な対応よりも柔軟性を持たせている可能性がありますが、一方で対応の遅延や不整合が発生するリスクも伴います。
特に対応プロセスが完全に欠如していると回答した企業は**13.68 %**に上り、これらの企業はインシデントに対し無防備な状態にあると言えるでしょう。
4.69 %の企業が対応プロセスの有無について「不明」と回答しており、セキュリティ管理の観点から見直しが必要な層と捉えられます。

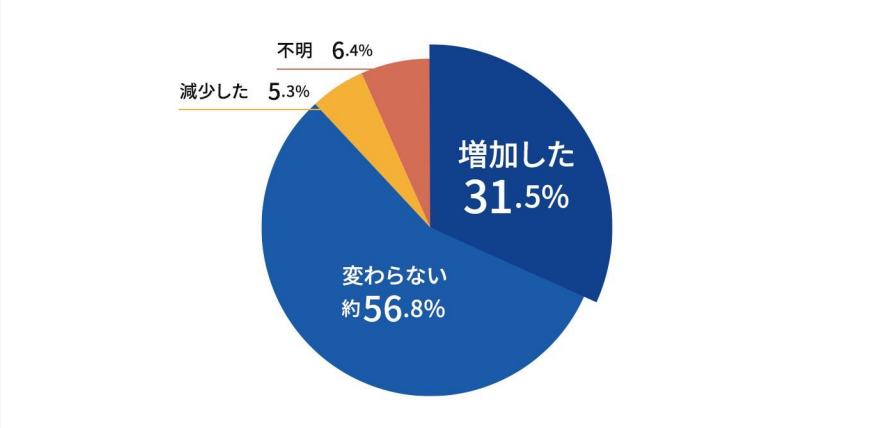


Securify

サイバーセキュリティに関する予算は、過去 1年間で変化しましたか？

約 31.48 %の企業が予算を増加させたと回答しました。サイバーセキュリティの脅威が増加し続ける現代において、新しい技術や手法への投資が不可欠であるという認識の反映ですね。最新のセキュリティ技術の導入や従業員の教育プログラムの強化、インシデント対応能力の向上など、具体的なセキュリティ強化措置に予算が充てられると考えられます。

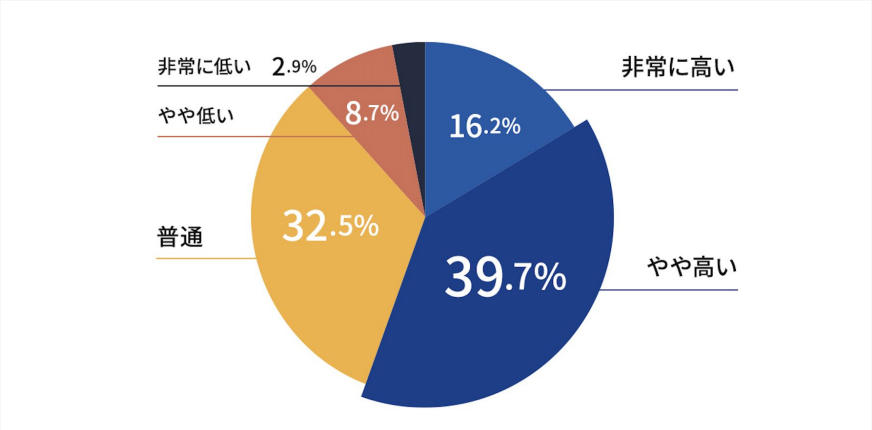
また、**56.84 %**の企業で予算が変わらないとの回答でした。予算制約の中で効果的なセキュリティ管理を行うことは難易度が非常に高い状況です。サイバーセキュリティの予算の増加が難しい企業には、低コストで進めることが可能な対策手法からスモールスタートすることをオススメします。



ご勤務先におけるセキュリティ対策の社内意識レベルを教えてください

回答者の **16.17 %** が「非常に高い」と回答しました。セキュリティが高い優先項目として位置づけられています。
こうした企業では、従業員全員がセキュリティリスクを認識し、積極的に対策を講じる文化が根付いていると思います。
39.71 % が「やや高い」と回答しており、多くの企業で定期的なセキュリティトレーニングやポリシーの見直しが行われ、
全社的な意識向上が図られている段階でしょうか。

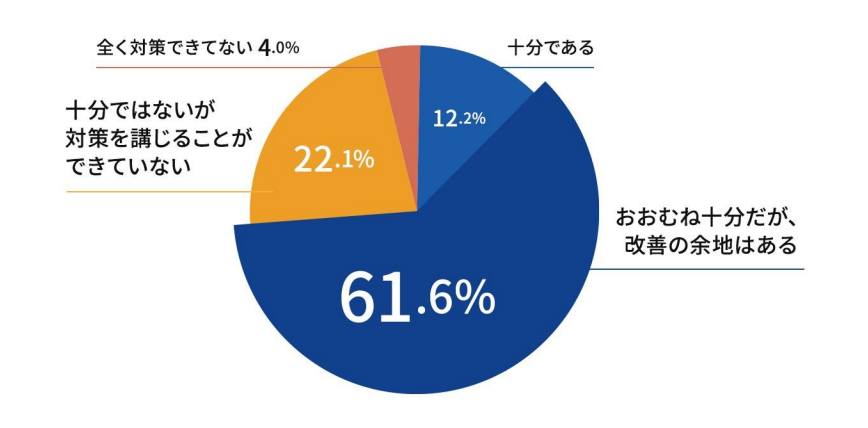
一方で、**32.54 %** が「普通」と回答しており、さらなるセキュリティ意識向上が必要と考えている様です。
全社員の意識レベルをさらに高めるための追加的な取り組みが必要と考えられます。



ご勤務先におけるサイバーセキュリティ対策の充実度を教えてください

セキュリティ対策の充実度に関するアンケート結果からは、各企業におけるセキュリティ対策の現状とその課題が明らかになりました。多くの企業がまだ対策強化の余地を持っていることが示されています。
最も多数を占めるのは「おおむね十分だが、改善の余地はある」と回答した**61.63 %**の企業です。
多くの企業にとって、基本的なセキュリティ対策を実施しているものの、日々変化する脅威の近況やAI などの新しい技術の登場により、常に改善と更新が必要であると考えられているのではないでしょうか。

また、「十分ではないが、対策を講じることができていない」「全く対策できていない」といった回答も約 1 / 4 を占めています。なぜ対策を進められないのか、その理由は次の質問で聞いています。



前設問で「十分である」以外を選択された方にお聞きします対策を講じることができていない主な理由を教えてください（複数選択可）

主な理由として、以下の3つの要因が挙げられました。

❶ コストをかけられない

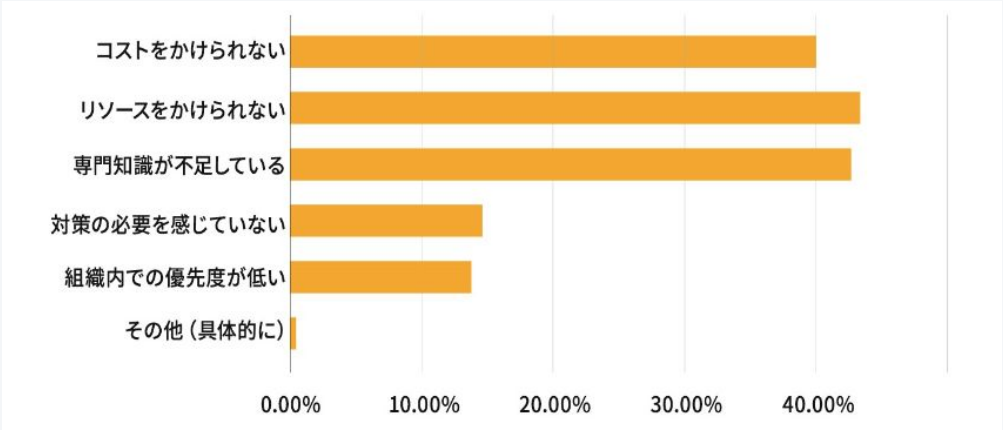
特に中小企業では、限られた予算内で運営を行う必要があるため、高額なセキュリティソリューションの導入が難しい場合があります。コスト効率の良いセキュリティ対策の選定を行う必要がありますね。

❷ リソースをかけられない

人材や時間のリソースが不足している場合、セキュリティ対策の実施が後回しにされがちです。
セキュリティ対策の自動化や、
専門的なセキュリティサービスのアウト
ソーシングを検討することが効果的です。

❸ 専門知識が不足している

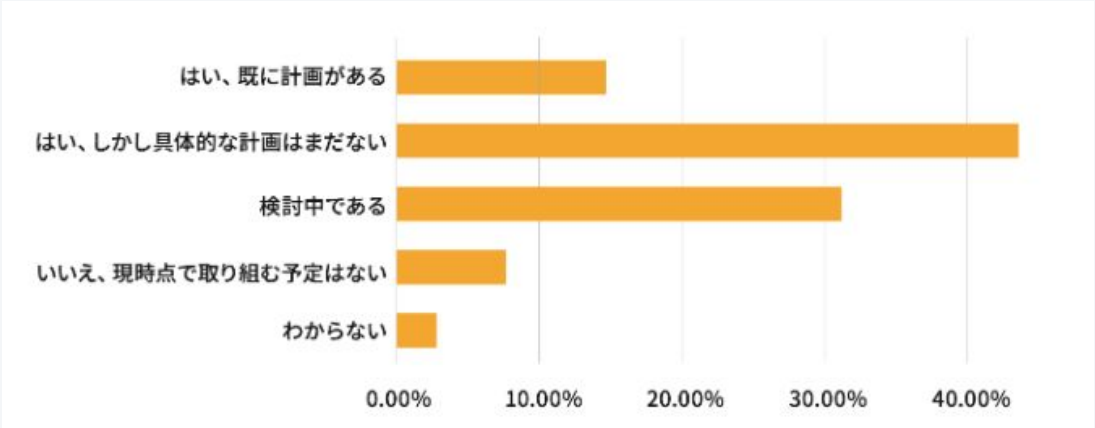
企業内にセキュリティ専門の知識がない場合、
外部の専門家に相談したり、簡単に扱える
ソリューションを選択することが重要です。



Securify

前設問で「十分である」以外を選択された方にお聞きします。
今後、セキュリティ対策に取り組む予定はありますか？

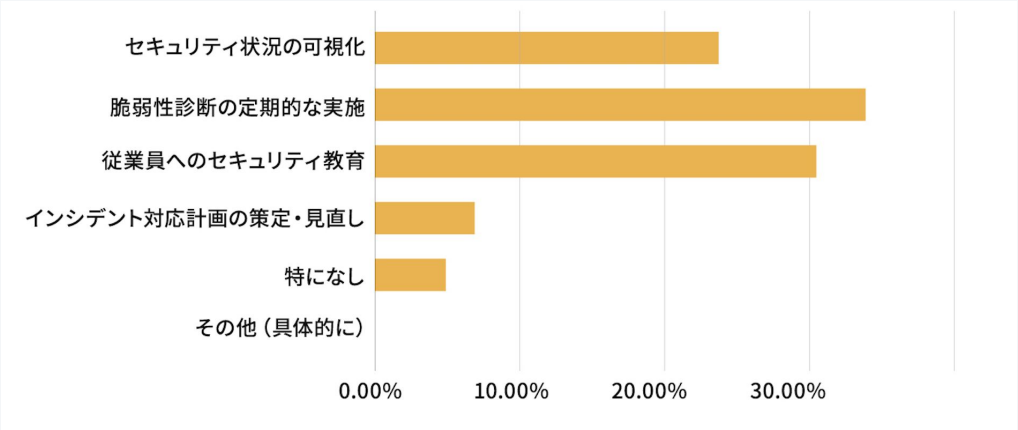
「はい、しかし具体的な計画はまだない」と回答した**43.40 %**が最も多く、
これに続いて「検討中である」との回答が**31.19 %**でした。
多くの企業がセキュリティ対策の重要性を認識しつつも、具体的な対策計画の策定には至っていない状況の様です。
具体的な計画が未定であるという回答は、企業がリスクを認識しながらも、どのようにして対応すべきかの道筋を
見出せていないため、セキュリティ対策の専門的なアプローチや外部の支援を求めていくことが効果的です。



Securify

サイバーセキュリティ対策において、今後最も強化すべきだと思う対策は何ですか？

最も強化すべき対策として「脆弱性診断の定期的な実施」、次いで「従業員へのセキュリティ教育」「セキュリティ状況の可視化」と続いています。企業が直面しているサイバーセキュリティのリスクに対して、予防的な対策としての脆弱性診断の重要性、および教育の必要性を示しています。
多くの企業が最も強化すべきと考えている脆弱性診断は、サイバーセキュリティ対策の基本であり、セキュリティを維持するためには欠かせないプロセスです。定期的な診断を行い、システムを常にセキュアな状態に保つ必要がありますが、工数、費用が大きくなる場合があり、十分な対応ができていない企業も多いです。
昨今では、診断を自動化できるツールを利用し、脆弱性診断を内製化していく動きを取る企業も増えてきています。



まとめ

Securify

■担当者の情報

- 性別：男性が73 %、女性が 26 %
- 年代：50 代が 37.03 %、40 代が 34.74 %、30 代が 20.67 %、20 代が 7.56 %
- 所属部門：情報システム部門が 60%、セキュリティ専門部門が30 %、その他の部門が2 %
- 役割と知識レベル：中間管理職が重要な役割を担う。約 3 割の担当者が自身の知識レベルに自信がない。
- 情報収集方法：セキュリティカンファレンスやセミナー、Web メディアやブログ。SNS の利用は少ない。

■企業の課題

- セキュリティインシデント：過去 1 年間で 約 38.09 %がセキュリティインシデントを経験。
- 対応プロセス：49.09 %が事前に定めた対応プロセスを持っている。
- 予算：31.48 %の企業がセキュリティ予算を増加させた。
- 優先度：「非常に高い」と回答したのが16.17 %、「やや高い」が39.71 %
- 対策実施の障壁：コスト、リソース不足、専門知識の欠如が主な障壁。

■強化すべき対策

- 脆弱性診断：33.97 %が最も強化すべき対策として挙げる。
- 従業員教育：30.53 %が必要性を認識。

さいごに

今回の調査では、セキュリティ担当者の属性、情報収集の方法、企業のセキュリティ対策状況について詳しく見てきました。
セキュリティ対策の実施においては、コストやリソース、専門知識の不足が大きな障壁となっています。
これらの課題を克服するためには、コスト効率の良い対策の選定や専門的な支援の活用が求められます。
今回の調査結果が、企業やセキュリティ担当者が今後のセキュリティ対策を検討する際の参考になれば幸いです。

株式会社スリーシェイクの提供する「 **Securify** 」は、企業のシステム及びサービスのセキュリティ品質の向上を目指し、
引き続きサービスを拡充して参ります。今後も、企業のセキュリティニーズに対応する豊富なソリューションの提供を
通じて、日本のセキュリティ環境の向上に努めてまいります。

セキュリティ対策をワンストップで。

Securify ［セキュリファイ］