株式会社 スタイルズ

WEBセキュリティに関するアンケート調査

対象：中～大企業のシステム開発・運用に携わる
担当者51名

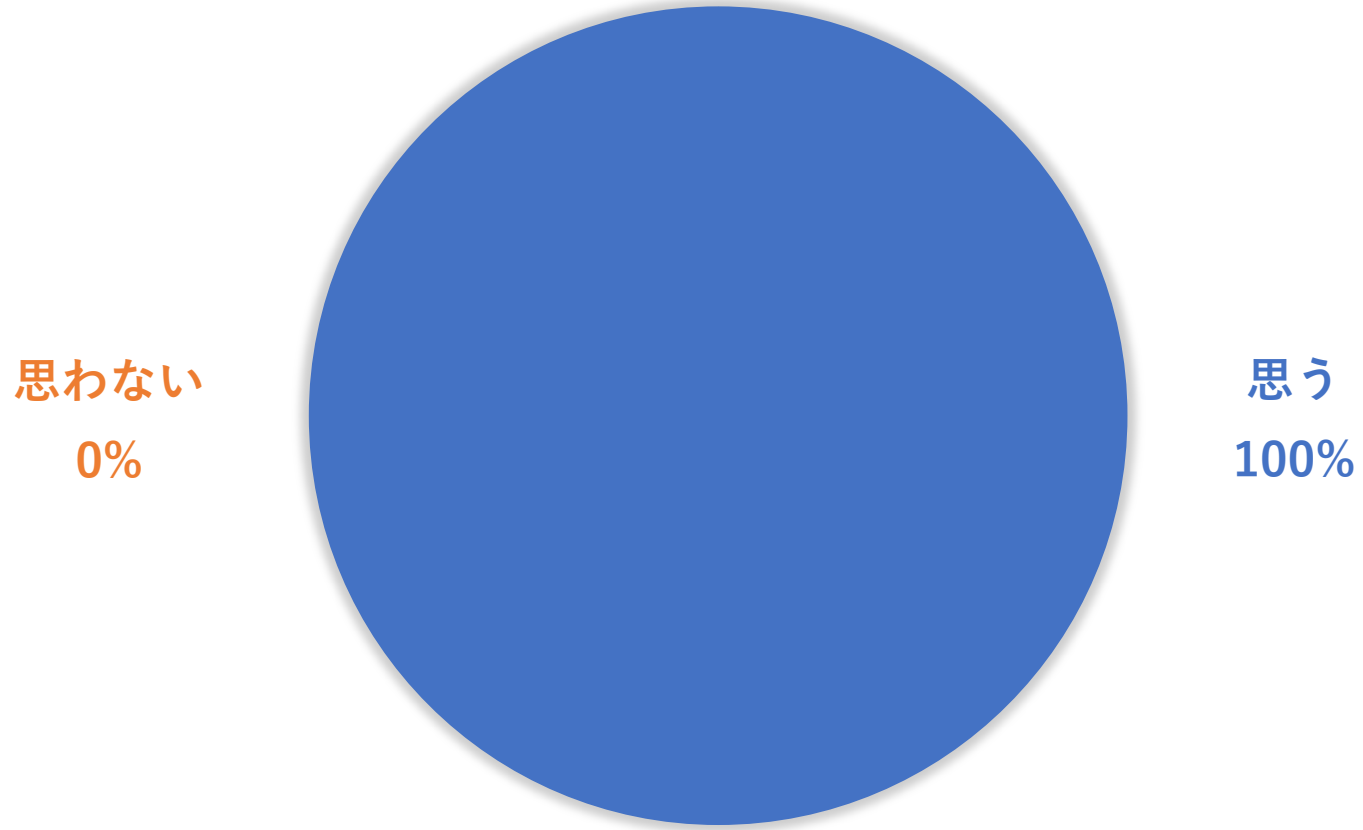
有効回答数：35名

調査手法：スタイルズ主催セミナー会場にて回収

調査期間：2018年6月27日（水）

調査主体：株式会社スタイルズ

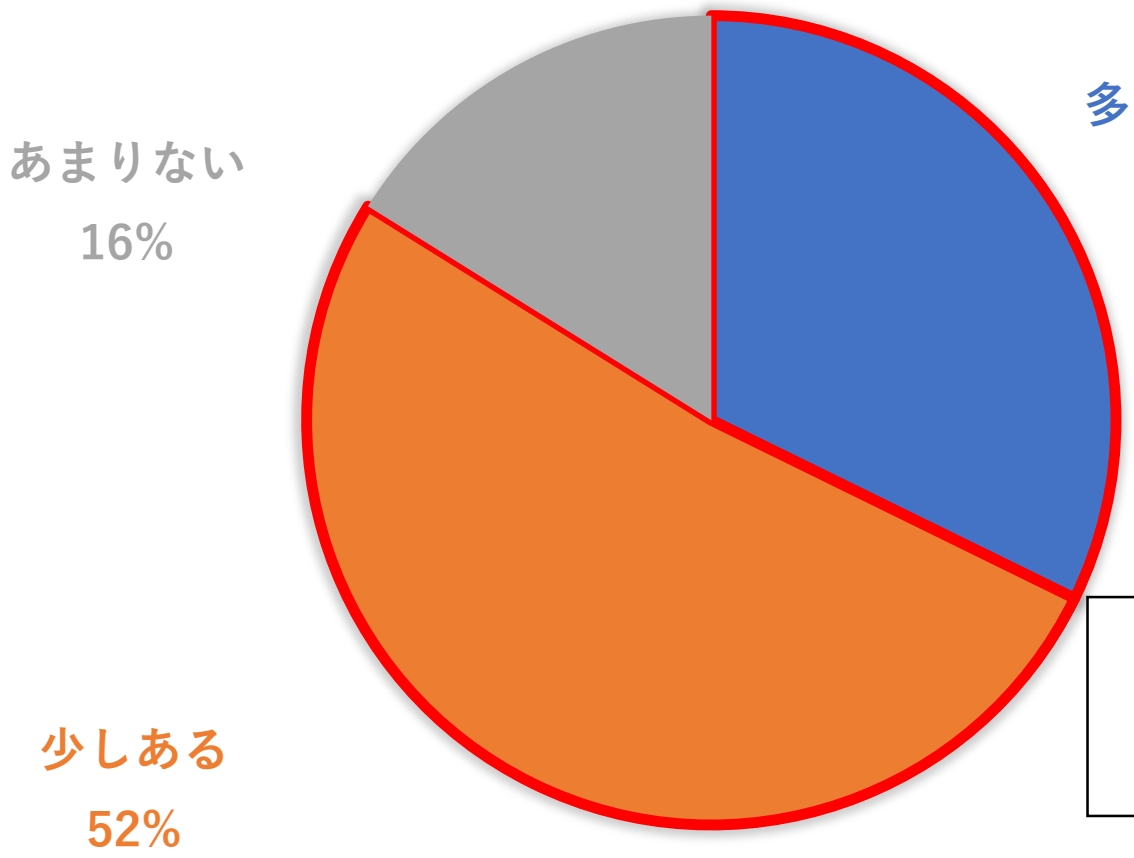
【質問】 情報セキュリティに投資をすることは企業の情報資産を守るために必要なコストだと思いますか？



全回答者が情報資産を守るために、投資することは必要と回答。
一方で、「必要だがコストをかけない工夫が求められている」「他予算の兼ね合いで後回しになる傾向がある」「ステークホルダーはあまりそう思っていない」という旨の回答もあり、担当者とステークホルダーとの意識の差を感じている回答者もいた。

情報セキュリティの重要性をステークホルダーにシステム運用担当者と同様に意識してもらうことが重要になる。

【質問】 貴社の企業の情報セキュリティのリスク管理とシステム部門の関わり方に改善の余地はありますか？

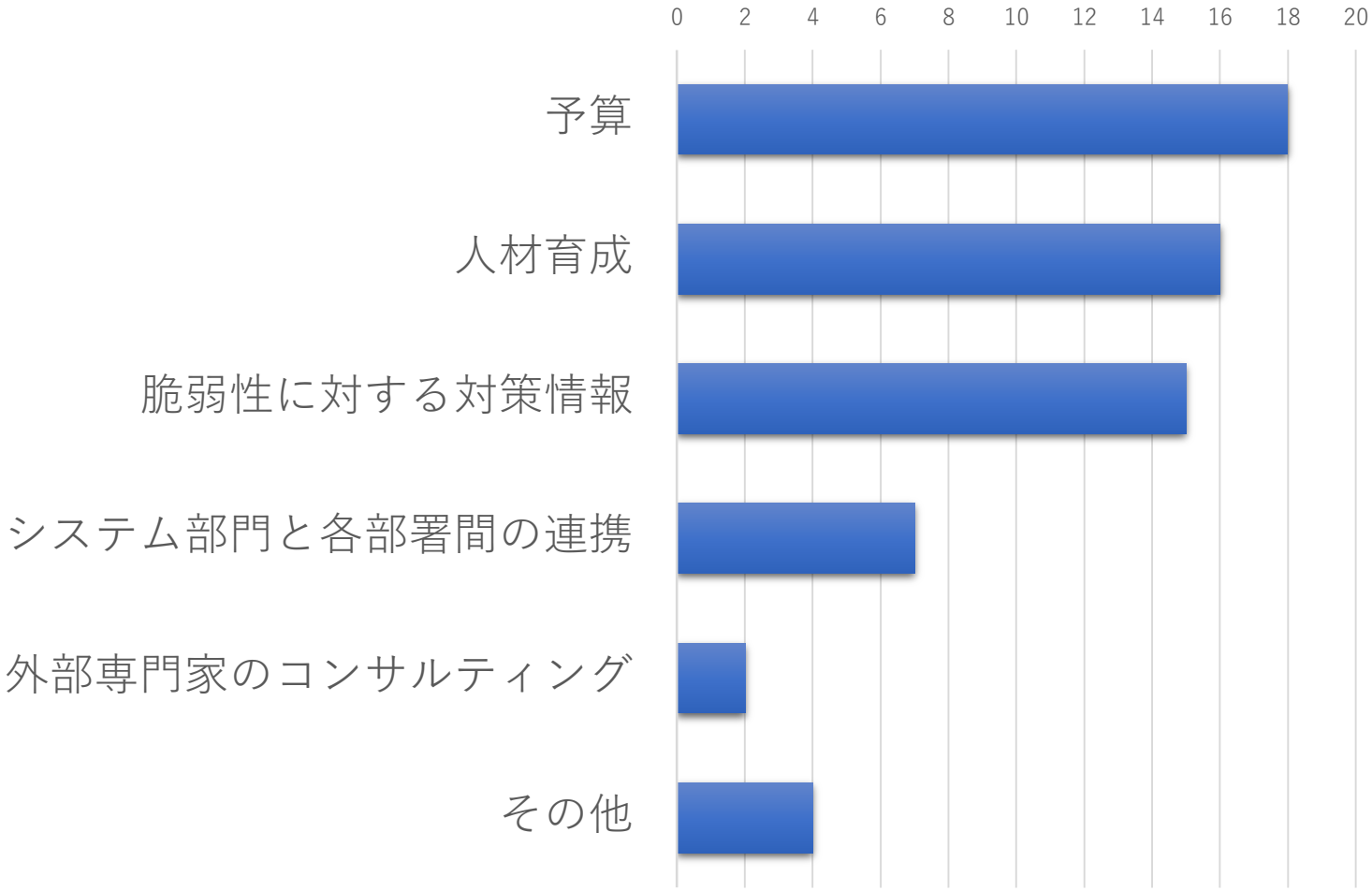


「改善の余地がある」
84%

84%の回答者が「改善の余地がある」と回答。
大多数のシステム部門がセキュリティリスクを管理していくうえで、課題や改善点があることが分かった。

具体的な課題については次ページ。

【質問】社内でレガシーシステムに対するセキュリティ対策を行うにあたり課題はありますか？（複数回答）

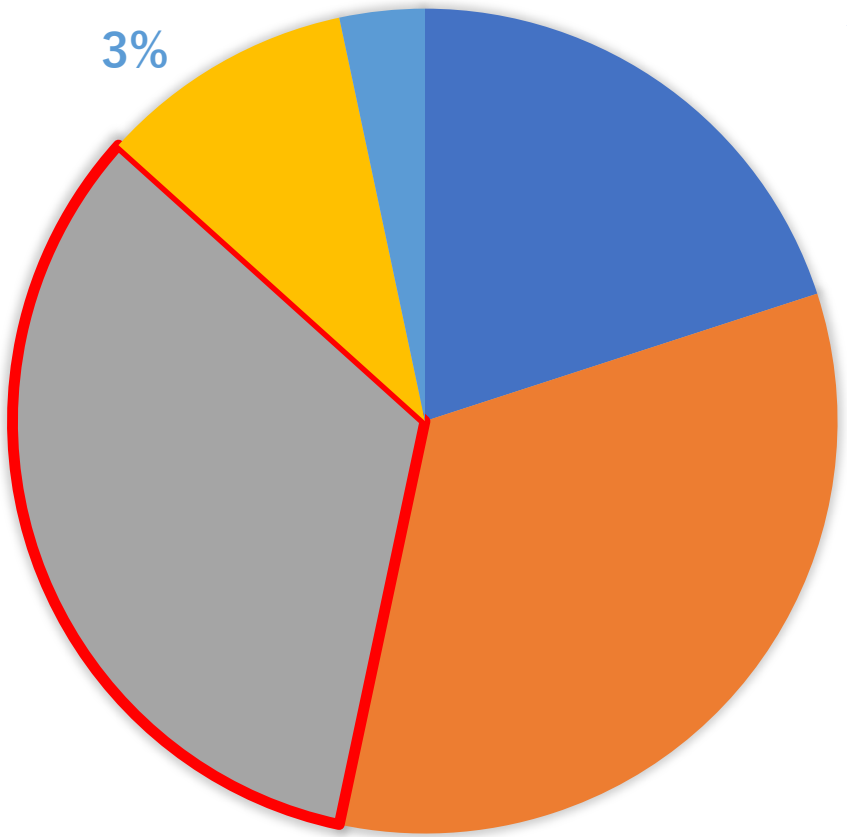


【回答者の比率】
予算　58%
人材育成　52%
対策情報　48%
各部署間の連携　23%
外部コンサルティング　6%
その他　13%

予算、人材育成、対策情報が1位～3位の結果となった。情報セキュリティに投資をすることを必要と回答している一方で、セキュリティ対策を能動的に行うために、十分な予算や人員を確保ができていない現状が想定される。

情報資産を守るために予算は必要と思っているものの、現実問題として担当者が満足のいく予算や人員がなく、現在の業務をこなすことで手一杯になっている可能性が考えられる。

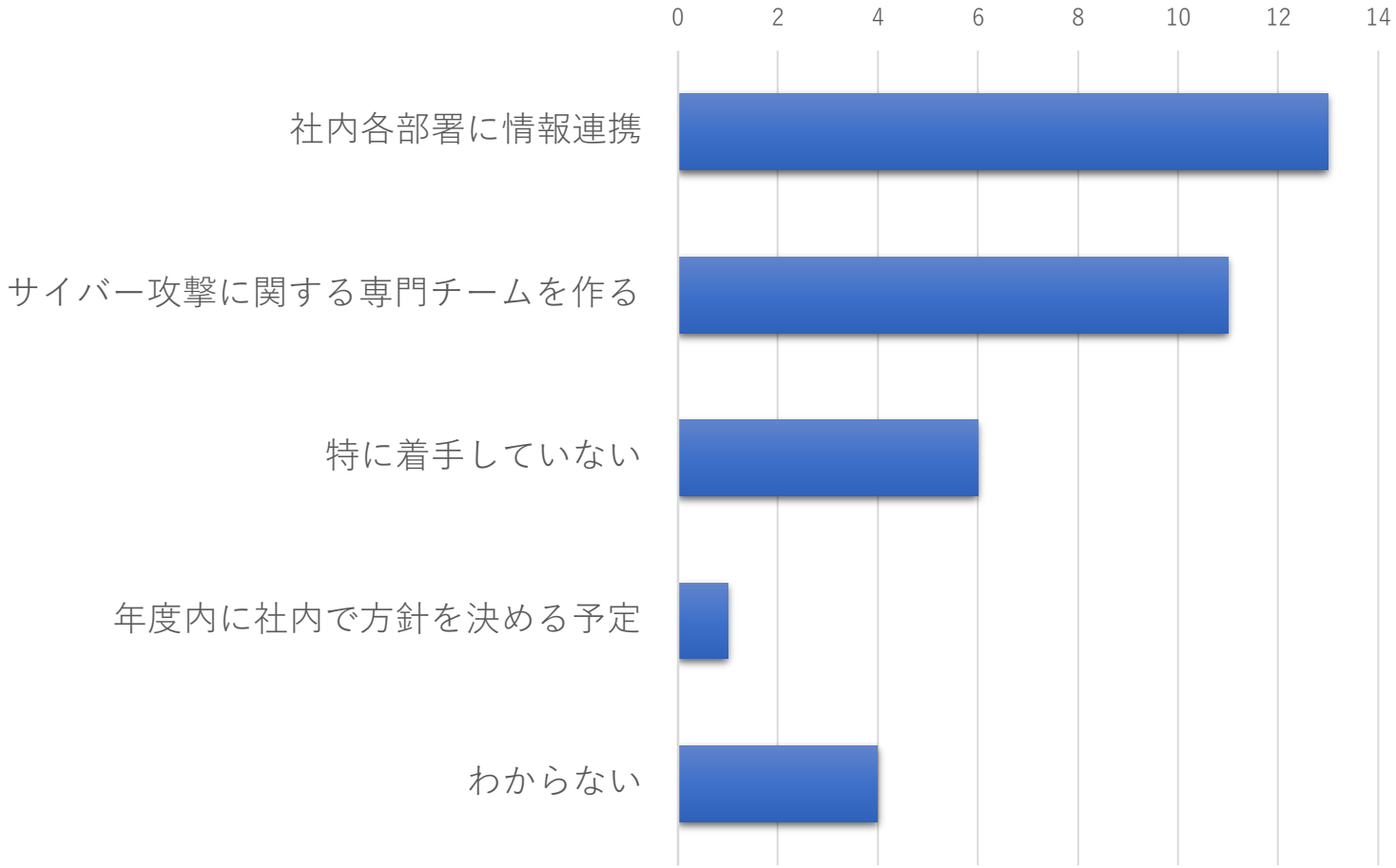
【質問】 貴社内で情報セキュリティに決められた予算はありますか？



定期的な情報セキュリティに対する予算が確保されているとの回答は20%と少ない。「決められた予算はなく、監査や上層部から指摘された部分に対して投資する」とし後手のセキュリティ対策をしている回答が33%と目立った。

定期的なセキュリティ対策にかける予算を確保することで、サイバー攻撃を未然に防ぐ施策ができる。
担当者が積極的にセキュリティ対策における情報収集を行い、会社に働きかけていくことが重要。

【質問】サイバー攻撃に関わる貴社の取り組みについて教えてください。（複数回答）



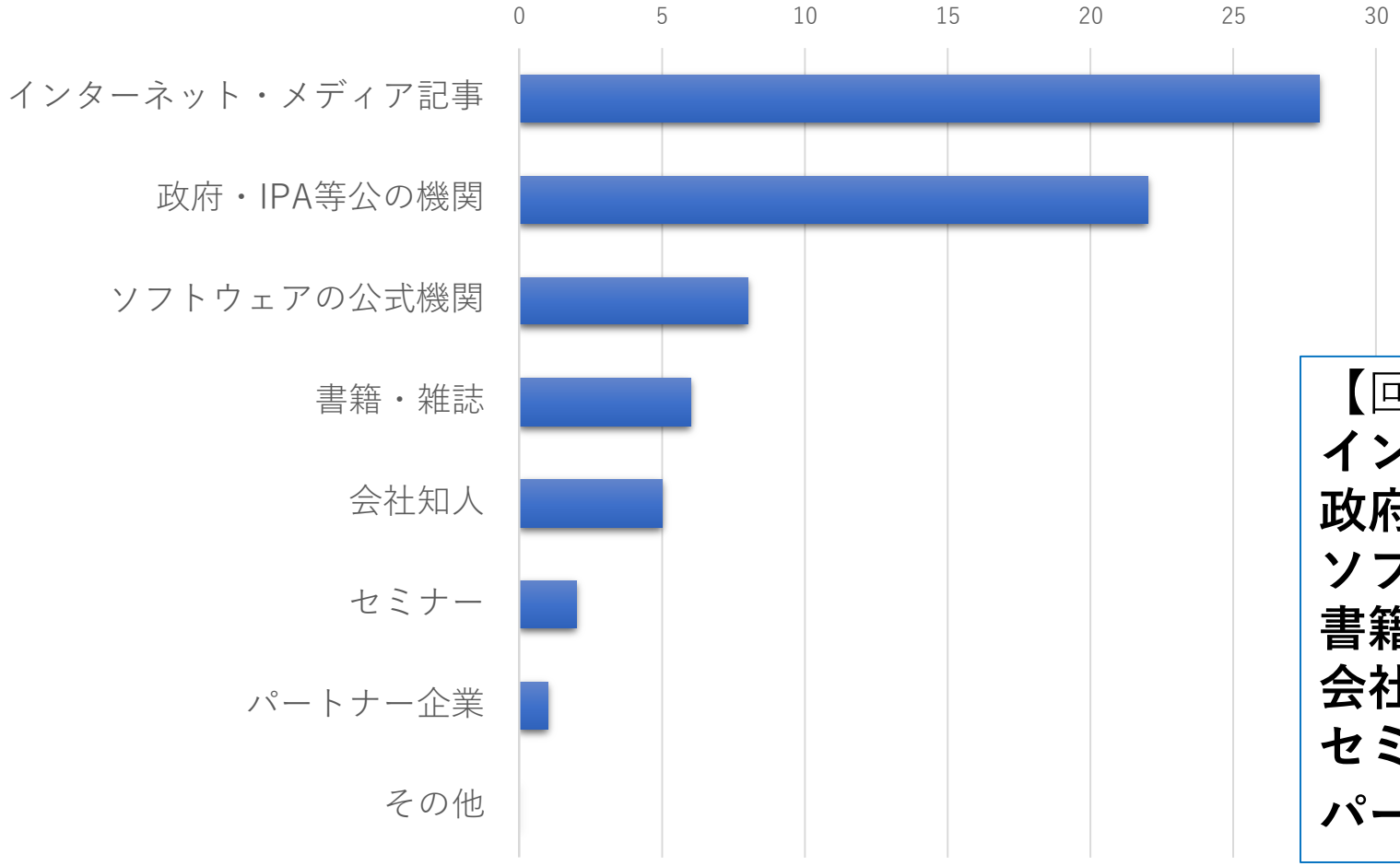
【回答者の比率】

社内各部署に情報連携	37%
専門チームを作る	31%
特に着手していない	17%
年度内に方針決定	3%
わからない	11%

サイバー攻撃の実施している対策については、脆弱性情報等を「社内各部署に情報連携をしている」の回答が1位。
その中で、部署や担当者間での温度差があるという旨の回答もあった。「特に着手していない」「わからない」の回答もあり、ここでも全社で情報セキュリティ対策がとれていない企業が多数いることが想定される結果となった。

担当者やシステム部門だけでなく、会社規模でサイバー攻撃に関する情報連携の仕組みを構築いくことが、情報セキュリティを全社に根付かせるための施策の一つと考えられる。

【質問】 情報セキュリティやサイバー攻撃に関して普段どこから情報収集をされていますか？（複数回答）



【回答者の比率】

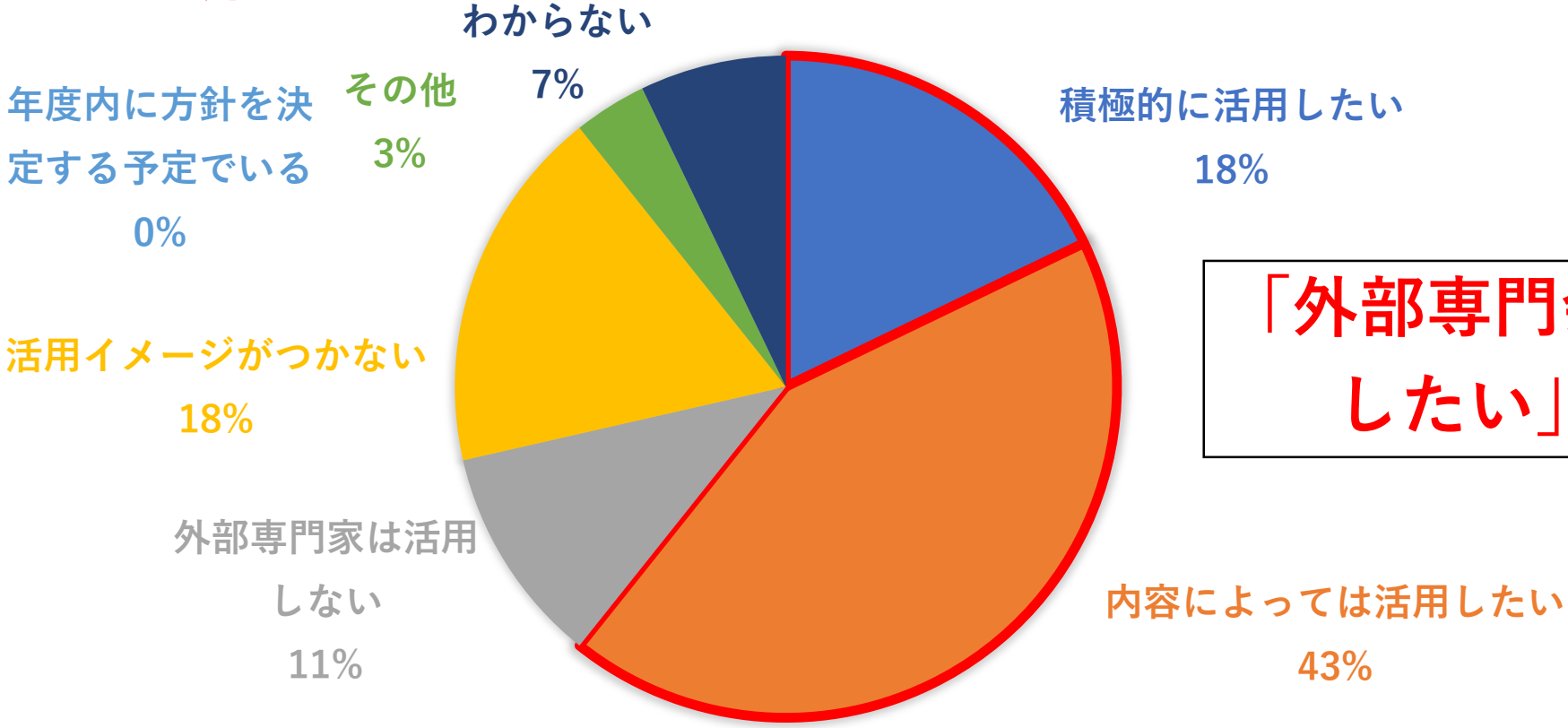
インターネット・メディア記事	85%
政府・IPA等公の機関	67%
ソフトウェアの公式機関	24%
書籍・雑誌	18%
会社知人	15%
セミナー	6%
パートナー企業	3%

回答者の85％が「インターネット・メディア記事」から情報収集をしていると回答。SNSで拡散されているWEBニュースで情報収集をし、正式な情報を公の機関で確認していると想定される。一方で「ソフトウェアの公式機関」の回答は24％にとどまり、一方的な情報ではなく、第三者による見解や評価をシステム運用担当者は期待しているようだ。

第三者の目線による見解が、サイバー攻撃やソフトウェアの脆弱性については重視されている。

株式会社 スタイルズ

【質問】 情報セキュリティやサイバー攻撃に関して、外部専門会社を活用にすることについてどのようにお考えですか？

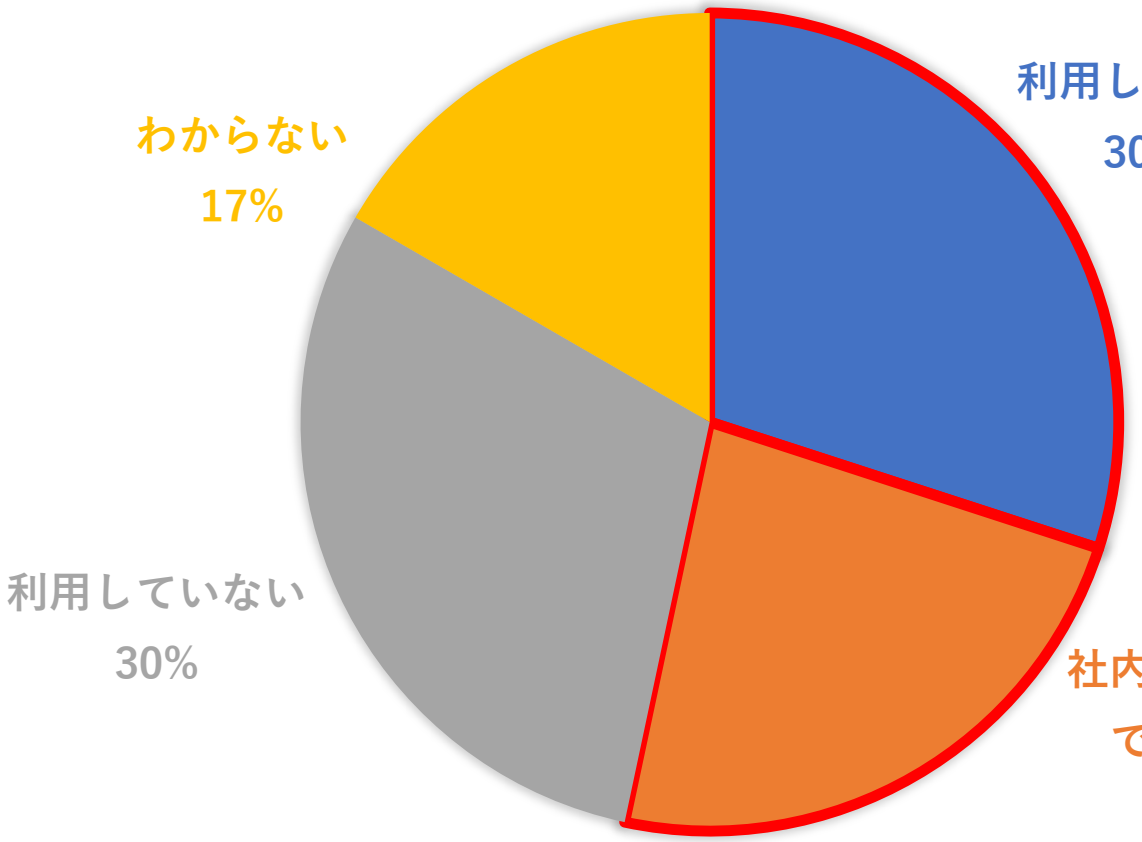


「外部専門会社を活用したい」61%

外部専門会社を「活用したい」の合計は61%にも上り、セキュリティ対策を専門的に迅速に行う外部専門会社が一定の支持を得ていることがわかった。一方で「活用イメージがつかない」の回答も18%となり、どのタイミングで外部専門会社に相談・依頼するべきか、どのような対策を提供しているのか等、セキュリティに関する外部専門会社の情報発信にも課題が想定される結果となった。

情報セキュリティに関して、「外部専門会社を活用したい」の回答は6割以上。
今後、外部専門会社がセキュリティ対策や方法について発信していくことも課題として見えた。

【質問】 現在、サポート終了したJavaフレームワークを利用されていますか？



「サポート切れJavaフレームワークを利用」
53%

サポート終了Javaフレームワークを「利用している」の合計は半数以上にも上った。システムの脆弱性が発見された場合でも、対処するためのソースコードが提供されないサポート終了Javaフレームワーク。これを使い続けることは非常に危険にも関わらず、対策が先延ばしになっている企業が多いことが浮き彫りとなった。

5割の企業は情報漏洩の危険性を伴うシステムを運用し続けている。

【まとめ】

- システム運用担当者にとって、会社の情報資産を守るために、投資することは必要と認識している一方で、予算や人員の不足などから、万全なセキュリティ施策をとっているとは言えない企業が多いようです。

- また、決められた予算はなく、監査や上層部から指摘された部分に対してセキュリティ投資を行うという回答33%に上り、定期的にセキュリティチェックを行うための予算を確保している会社は20%を上回りました。

- 定期的なセキュリティ対策にかける予算を確保することで、サイバー攻撃を未然に防ぐ施策ができます。システム運用担当者がセキュリティ対策における情報収集を行い、全社に情報連携をするなど、積極的に会社に働きかけていくことが重要です。

- 社内人員で賄えない業務を実施してくれるセキュリティに関する外部専門会社は、システム運用担当者から一定の支持を得ている一方、利用イメージがつかないとの回答もありました。

- 今後、忙しいシステム運用担当者のため、わかりやすい情報で、かつ効率的なセキュリティ対策を専門会社が提供することが求められています。同時にサイバー攻撃やソフトウェアの脆弱性に対して、第三者の目線による評価・見解を伝えていく報道が期待されています。