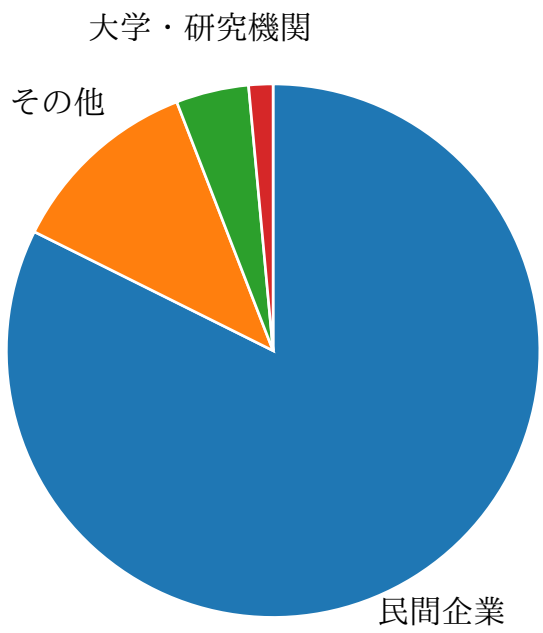
第12回 JSSMセキュリティ公開討論会 【午前の部】

講義データダウンロード（属性別）

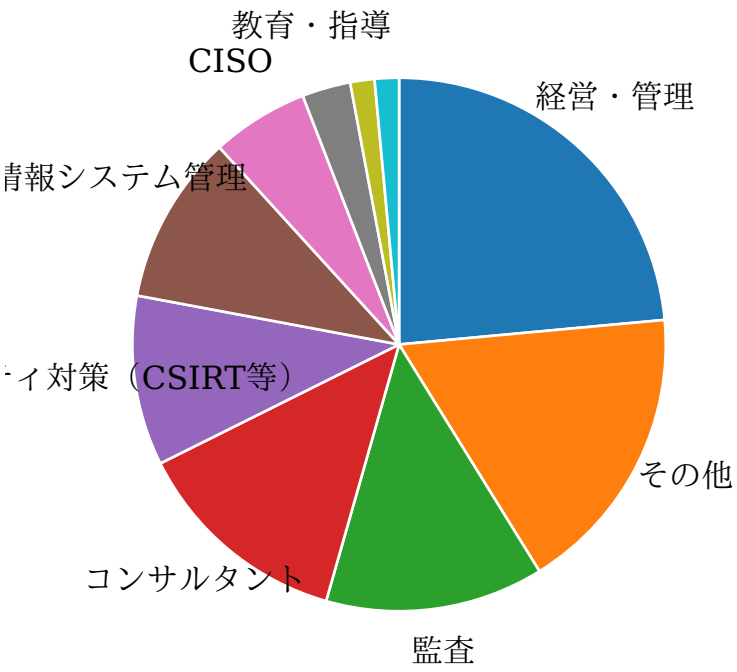
属性登録件数 69 件
※属性取得していない場合は参加者毎に付番した形式でダウンロードできます。

所属組織を選んでください



民間企業	**56**
その他	**8**
大学・研究機関	**3**
行政機関	**1**

ご自身の現在の役割を選んでください



経営・管理	**16**
その他	**12**
監査	**9**
コンサルタント	**9**
セキュリティ対策（CSIRT等）	**7**
情報システム管理	**7**
CISO	**4**
教育・指導	**2**
営業	**1**
システム開発	**1**

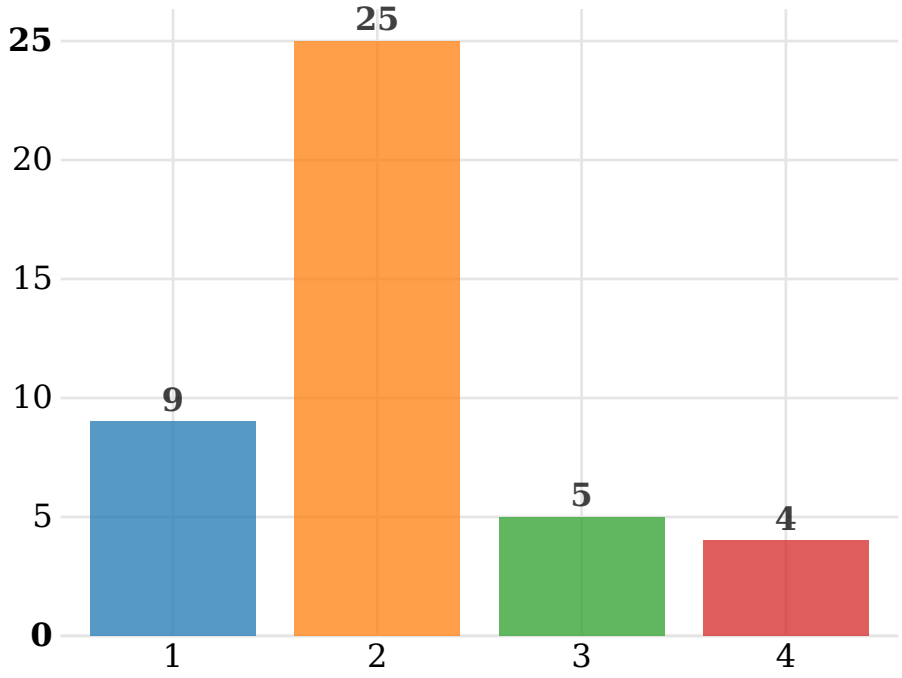
投票/投稿/アンケート結果

投票人数 69 件

1. FS-ISAC鎌田さんへの質問を記入してください

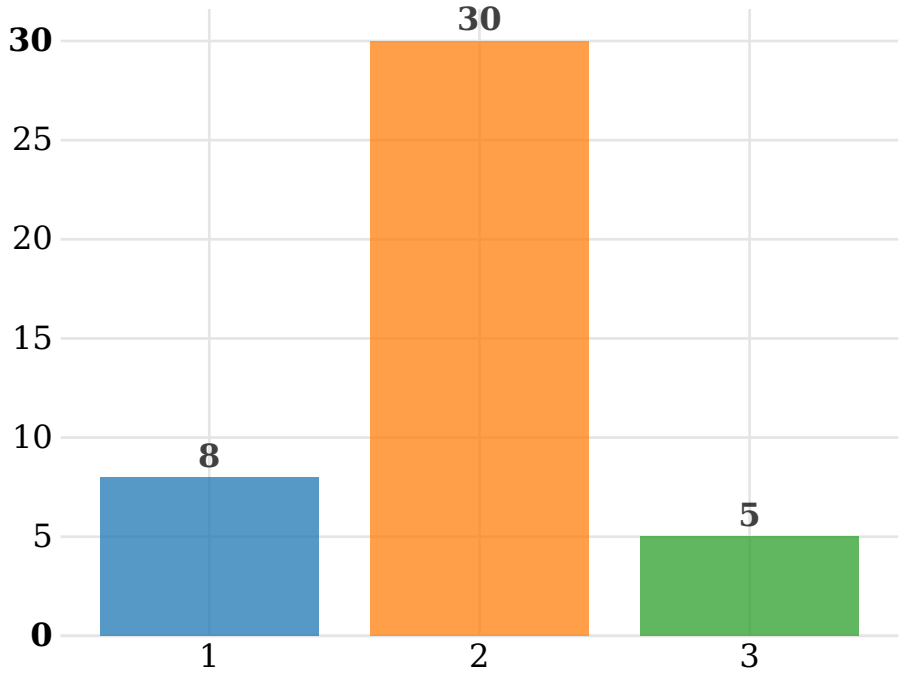
コメント内容	Good	Bad
真相が報道されないのは攻撃者を利するだけですね。	0	0
日本の金融機関にも国家レベルと思われる攻撃は確認されているのですか？	1	0
企業の実害として、世の中の風評被害のきっかけになるのが気になります。	1	0
BlackhatやDEFCONが落ちてきた中で、今1番尖った情報が入手出来るイベントは何でしょうか。	1	0
DEFCONのターゲットが変わってきている？（IoT、自動車、AIなど）	1	0
海外で、メールの添付ファイルのパスワード付きZIPって、使うんですか？ また、どのような方法でデータ交換をしているのですか？	0	0
「企業情報を対象としたサイバー攻撃の目的」の出典は？	0	0
くだらない理由が、やはり気になります。	0	0
CSFは経営者に理解しやすい内容だとおもいます。	2	0
CSFの具体的な項目を見ていくと、目がくらんできます。	0	0
悪い報告については、航空機の事故対策を参考にしています。	0	0
米国のISACは機能していないとの話も聞くのですが、実際はどうなのでしょう？	0	0
「インテリジェンスの3つの文脈」の「経営・戦略」情報のより具体的な想定礼イメージは？	1	0
「インテリジェンスの全体像」は「情報利用者」の3層毎にサイクルを回すのか？	0	0
米国では、ITアーキテクチャの構築に、CISOは絡むことは少ないのでしょうか？	1	0
たしかに日本ではフルタイムCISOは少ないですね、なぜでしょうか？	2	0
そもそも日本の企業がオフィサー制度じゃないからと思ってます＞フルタイムCISO	0	0
オフィサー制度が形だけはアグリーです。だとするとCISO頑張る議論しても寂しいですね・・・	1	1

2. あなたの立場を選んでください



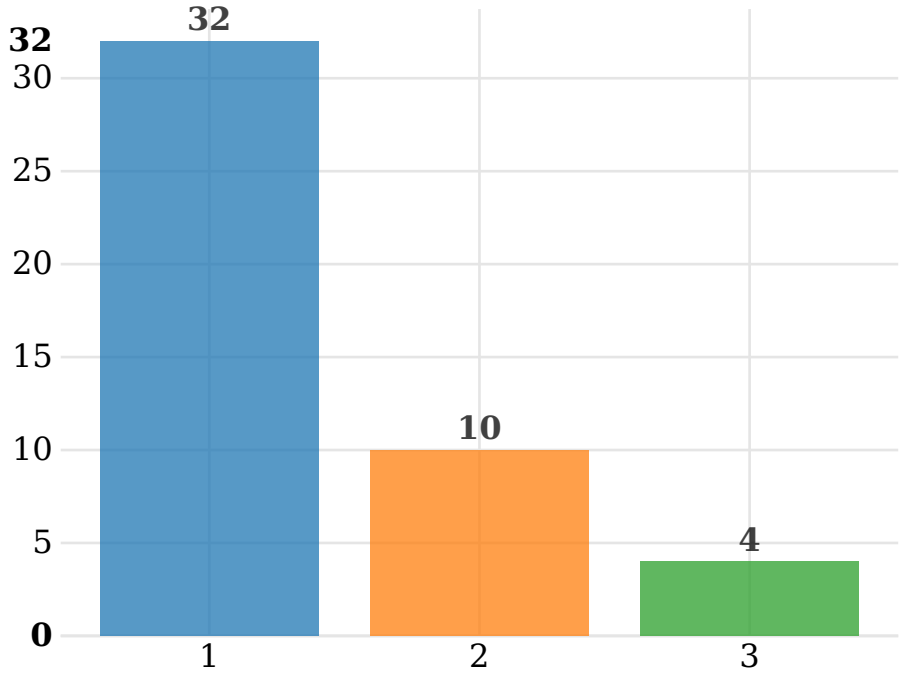
1.セキュリティベンダの立場	**9**
2.ユーザ企業・組織の立場	**25**
3.セキュリティ研究者の立場	**5**
4.その他	**4**

3. 御社は重要インフラ企業ですか？



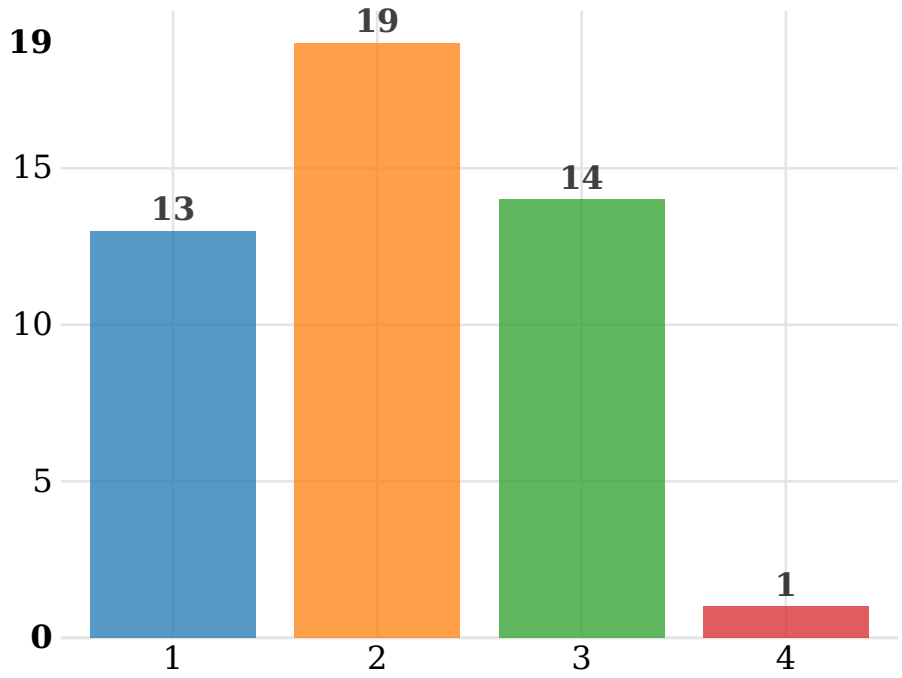
1.YES	**8**
2.NO	**30**
3.わからない	**5**

4. コアビジネスのITへの依存度は？



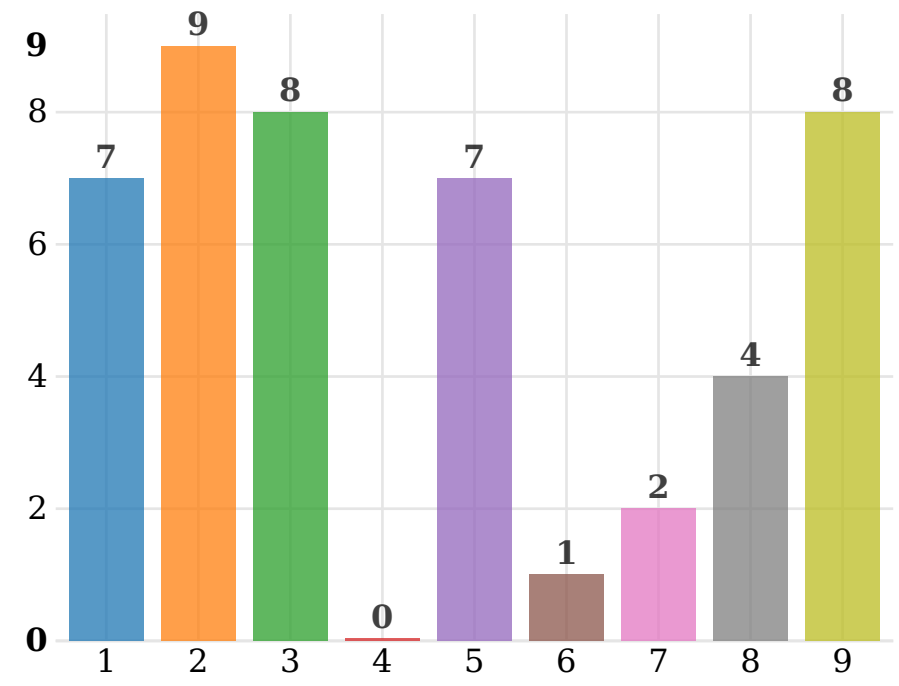
1.高い	**32**
2.普通	**10**
3.低い	**4**

5. 皆さんの会社のセキュリティマネジメントのレベルは？



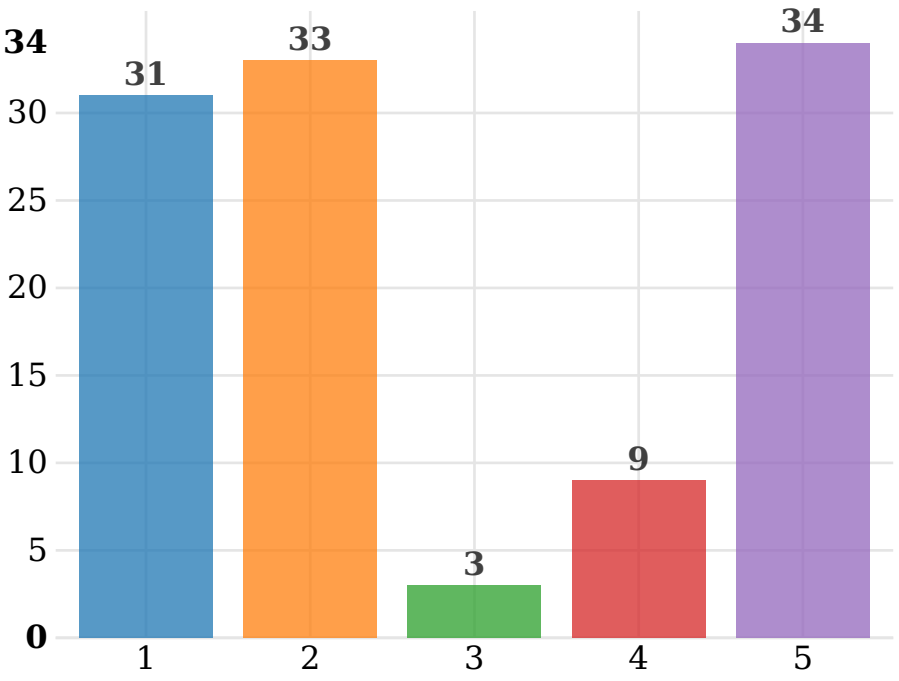
1.高いレベルだと思う	**13**
2.普通のレベルだと思う	**19**
3.マネジメント出来ているとは言い難い	**14**
4.その他	**1**

6. 御社のセキュリティ担当者数は？（フルタイム・パートタイム合わせて）



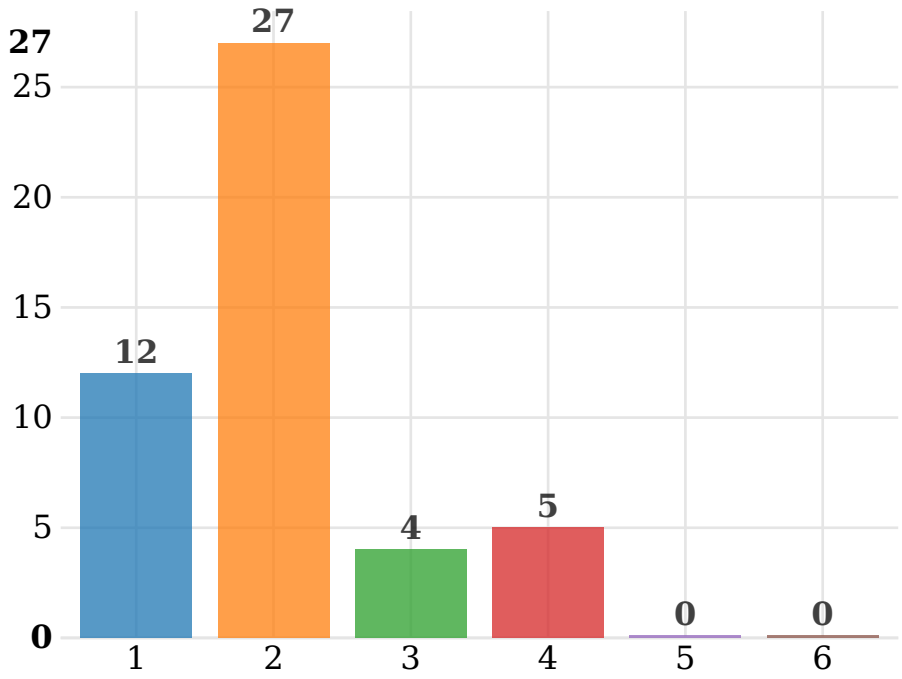
1.1人	**7**
2.5人未満	**9**
3.10人未満	**8**
4.20人未満	**0**
5.50人未満	**7**
6.100人未満	**1**
7.300人未満	**2**
8.300人以上	**4**
9.不明	**8**

7. 設問の回答がYESの人は投票してください



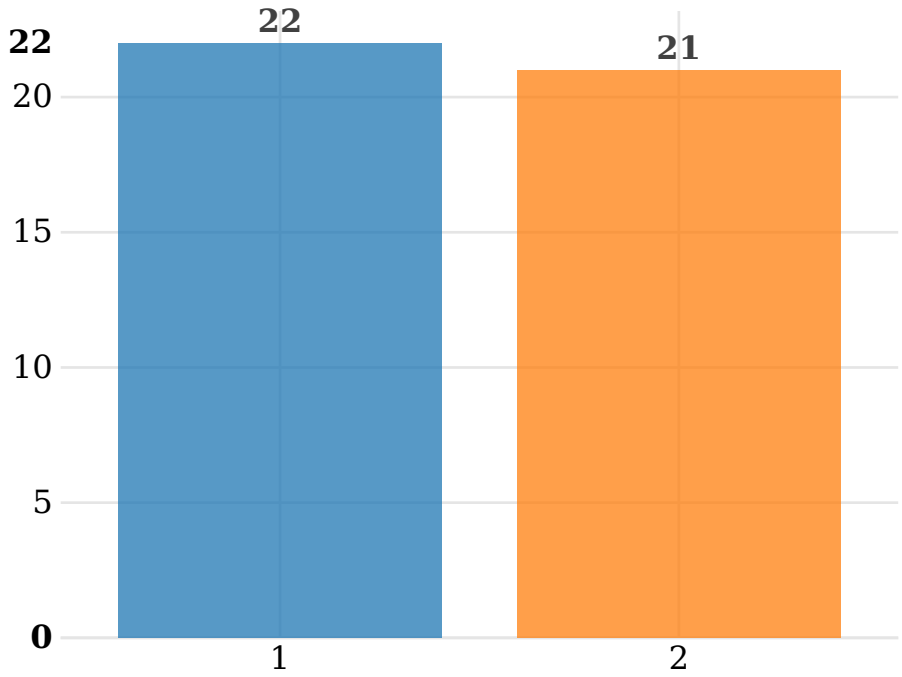
1.セキュリティ情報収集を自ら行っていますか？	**31**
2.セキュリティに関連した国際的なフレームワークやスタンダードに目を通したことがありますか？	**33**
3.セキュリティ対策のほとんどは製品やサービスを導入することで解決すると考えていますか？	**3**
4.自社において実害の出た（情報漏えい、もしくは業務停止1日以上）インシデントを中心的な立場でハンドリングしたことありますか？	**9**
5.自社はセキュリティに対する意識を高くすることが常に求められていると思うか？	**34**

8. サイバー攻撃によって全社的にパソコンが利用できないことになった場合、何日まで許容できそうですか



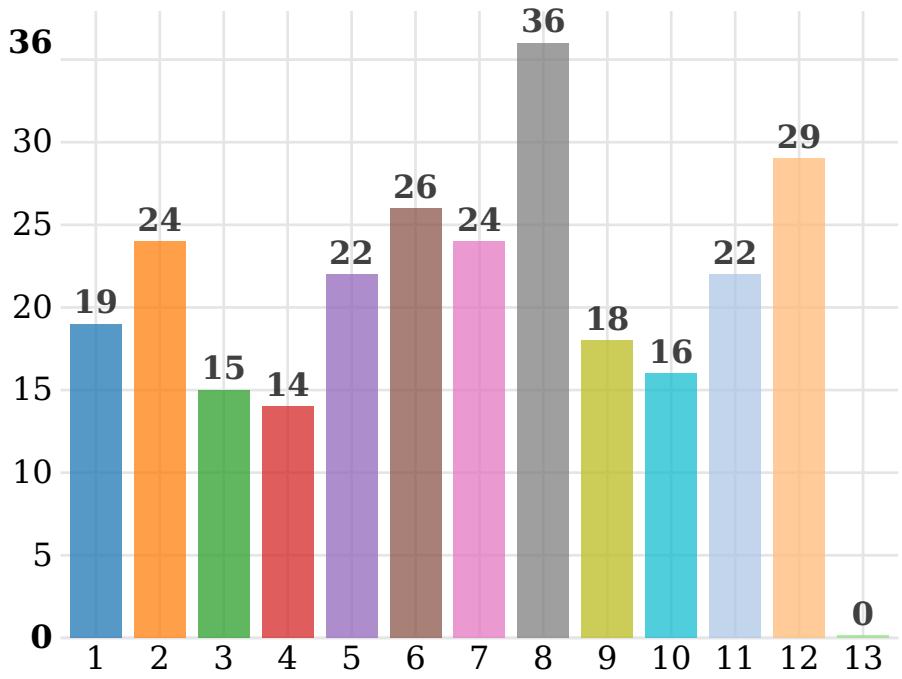
1.2～3時間	**12**
2.1日以下	**27**
3.3日以下	**4**
4.1週間以下	**5**
5.1ヶ月以下	**0**
6.1ヶ月以上	**0**

9. CISOに相当する方は意思決定会議のメンバですか？



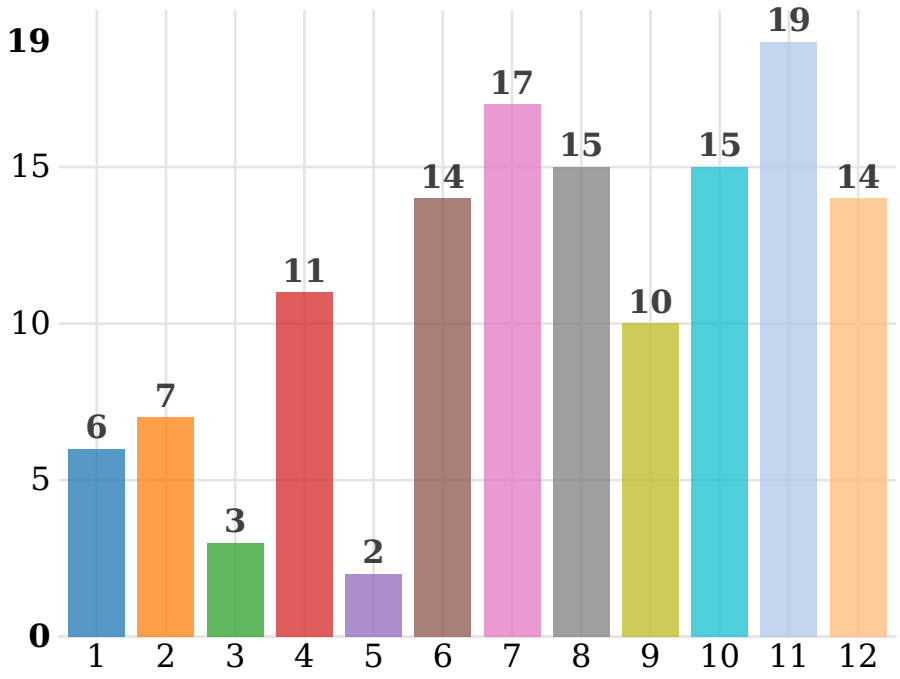
1.YES	**22**
2.NO	**21**

10. CISOの役割と責任について、あなたの責任・担当範囲であてはまるものをすべて選択してください



1.ネットワークセキュリティと境界線防御	19
2.アプリケーションセキュリティの方針・標準の策定と実施	24
3.システム・セキュリティテストツールの選定と導入	15
4.業務システムへのサイバー脅威検知ツールの選定と導入	14
5.システムの脆弱性リスクの管理	22
6.社内の全システム資産のセキュリティとリスクの測定と管理	26
7.業務環境におけるインシデントレスポンス(CSIRT)組織への指揮	24
8.役員会へのセキュリティ状況の報告	36
9.情報セキュリティ推進・システム調達・ソフトウェア開発チームへの訓練	18
10.自社サービスあるいは製品に起因するインシデントレスポンス(PSIRT)組織への指揮	16
11.一年以上の将来に向けてセキュリティ戦略を策定し実行する	22
12.役員・役職者・一般社員向けのセキュリティ教育の計画と実施	29
13.その他（自由記入）	0

11. 皆さんの会社のセキュリティマネジメントで当てはまるものを選んでください



1.①経営方針とのアライメントができている。	**6**
2.①経営にアラインできていない。	**7**
3.②柔軟性があり想定外のリスクに対応可能	**3**
4.②硬直的で形骸化している。	**11**
5.③ 経営者はゼロリスク思考である。	**2**
6.③ 経営者はリスクコントロール思考である。	**14**
7.④ 利便性を犠牲にしてもセキュリティ対策が優先される。	**17**
8.④ 利便性に配慮したセキュリティ対策が好まれる。	**15**
9.⑤ クラウドやSaaS利用に対応する新しいマネジメントスタイルに移行している。	**10**
10.⑤ 10年以上前に作ったセキュリティポリシを堅持している。	**15**
11.⑥ セキュリティマネジメント担当者は最新のクラウド環境の知識がある。	**19**
12.⑥ IT系の知識が少なく、いわゆるマネジメント系人材が多い。	**14**