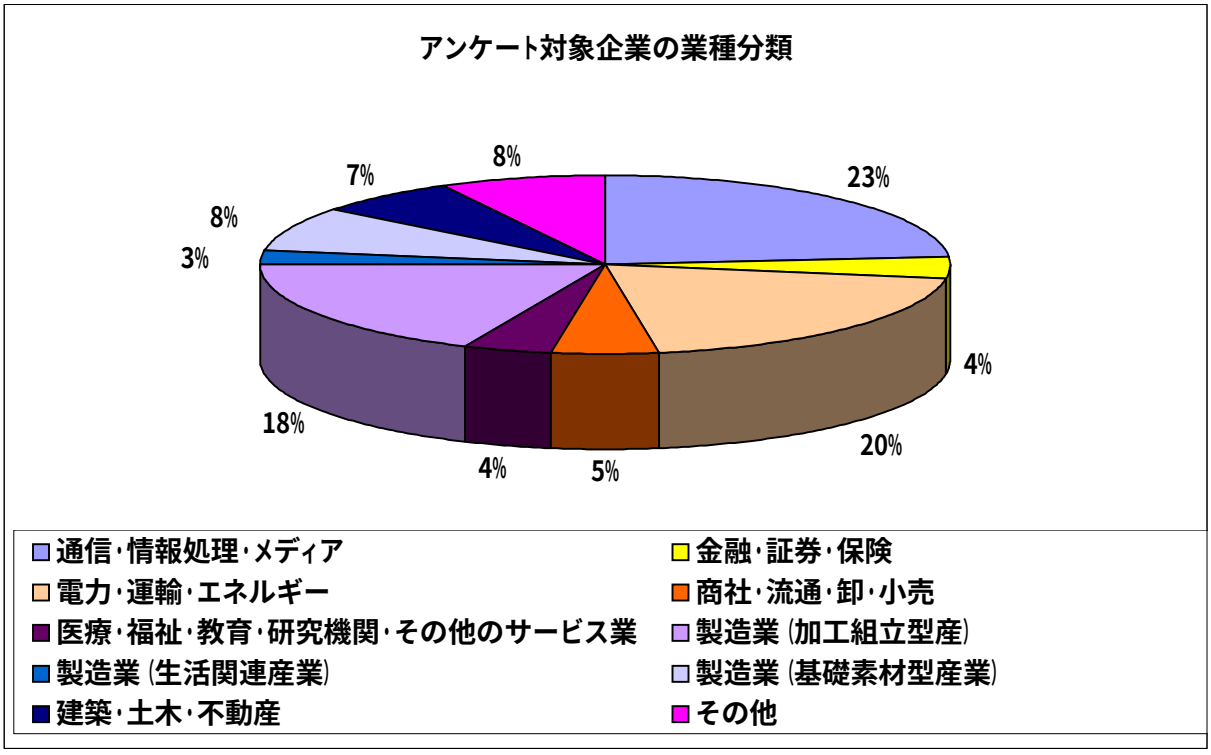
資料5－2

日本経団連加盟企業に対するアンケート詳細結果

平成１８年９月１５日
内閣官房情報セキュリティセンター

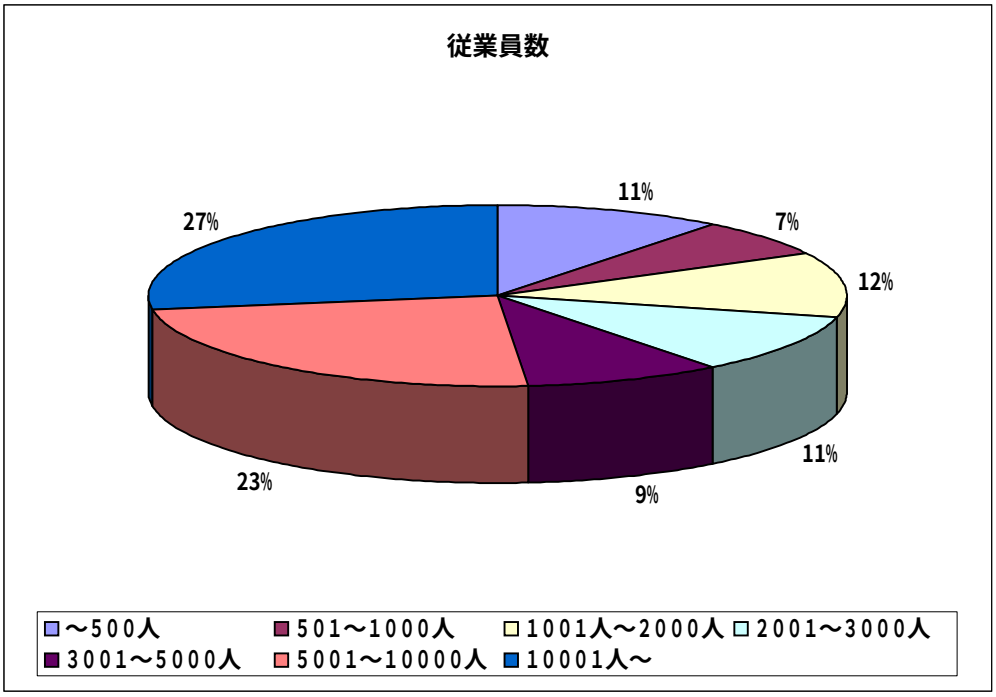
Q01　御社の業種を以下から選んで下さい。

	選択肢	回答数
1	通信･情報処理･メディア	18
2	金融･証券･保険	3
3	電力･運輸･エネルギー	15
4	商社･流通･卸･小売	4
5	医療･福祉･教育･研究機関･その他のサービス業	3
6	製造業（加工組立型産）	14
7	製造業（生活関連産業）	2
8	製造業（基礎素材型産業）	6
9	建築･土木･不動産	5
10	その他	6



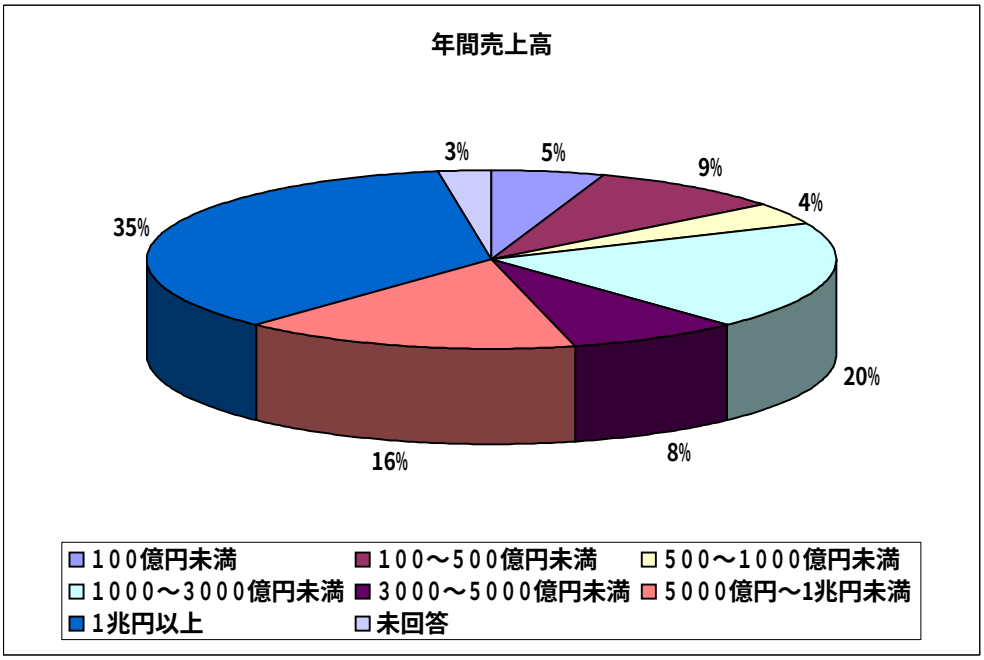
Q02　御社の従業員数は何人ですか。

従業員数	回答数
～500人	8
501～1000人	5
1001人～2000人	9
2001～3000人	8
3001～5000人	7
5001～10000人	18
10001人～	21



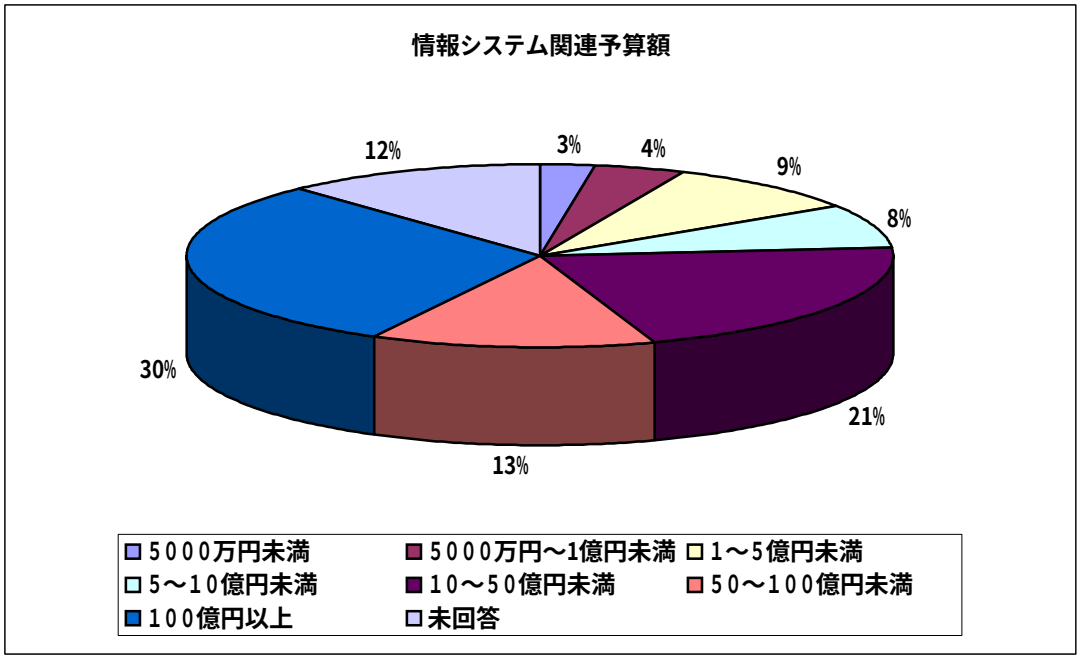
Q03　御社の平成17年度の年間売上高はいくらですか。

売上高	回答数
100億円未満	4
100～500億円未満	7
500～1000億円未満	3
1000～3000億円未満	15
3000～5000億円未満	6
5000億円～1兆円未満	12
1兆円以上	27
未回答	2



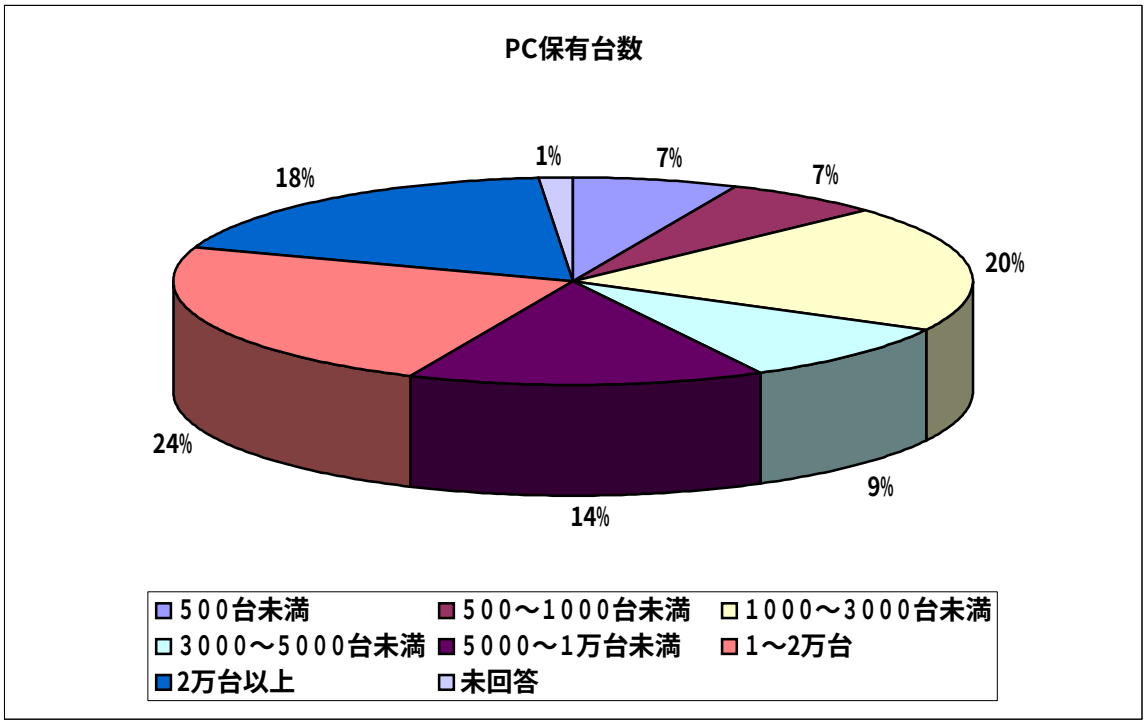
Q04　御社の年間の情報システム関連予算額はいくらですか。

システム関連予算	回答数
5000万円未満	2
5000万円～1億円未満	3
1～5億円未満	7
5～10億円未満	6
10～50億円未満	16
50～100億円未満	10
100億円以上	23
未回答	9



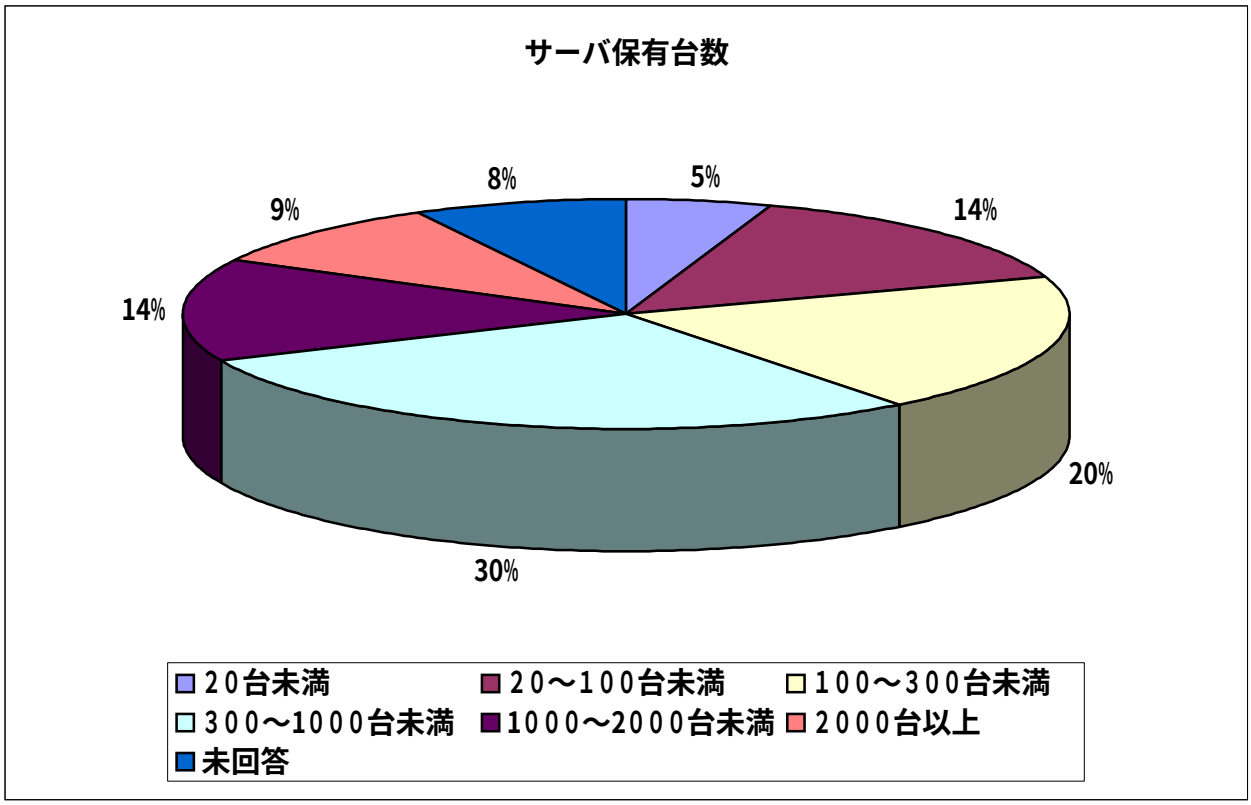
Q05　御社のＰＣの保有台数は何台ですか。

PC保有台数	回答数
500台未満	5
500～1000台未満	5
1000～3000台未満	15
3000～5000台未満	7
5000～1万台未満	11
1～2万台	18
2万台以上	14
未回答	1



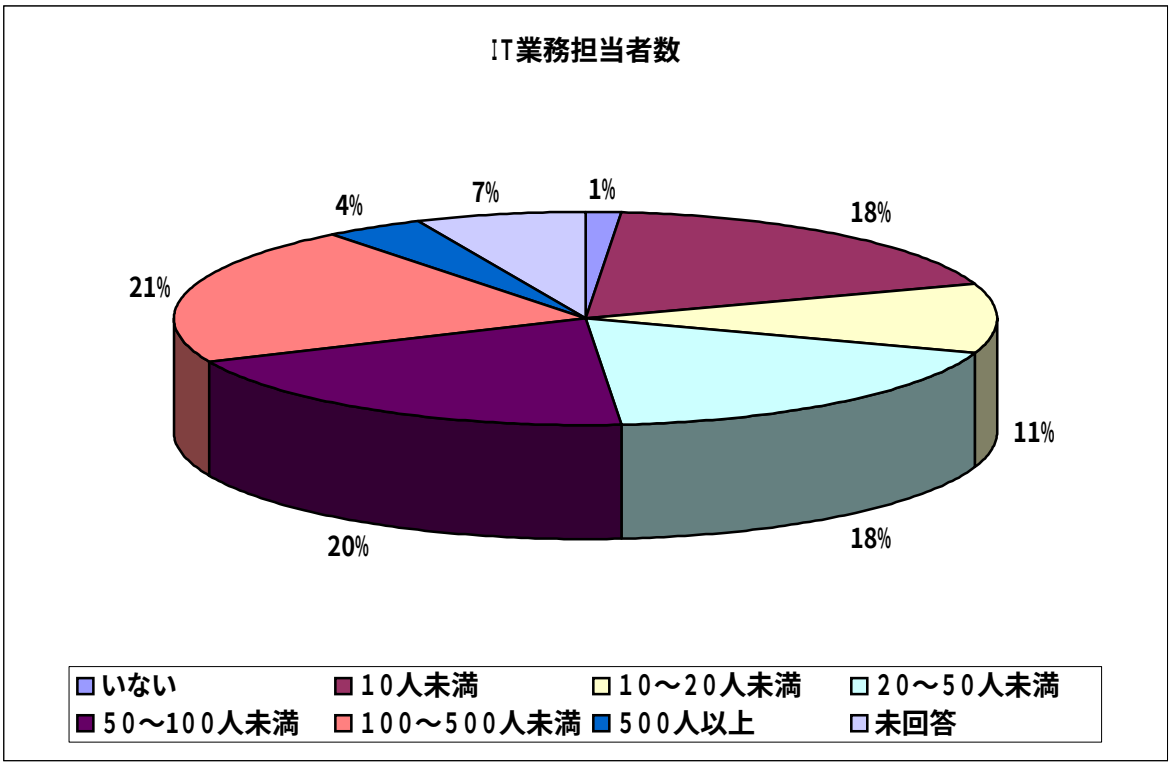
Q06　御社のサーバの保有台数は何台ですか。

サーバ保有台数	回答数
20台未満	4
20～100台未満	11
100～300台未満	15
300～1000台未満	22
1000～2000台未満	11
2000台以上	7
未回答	6



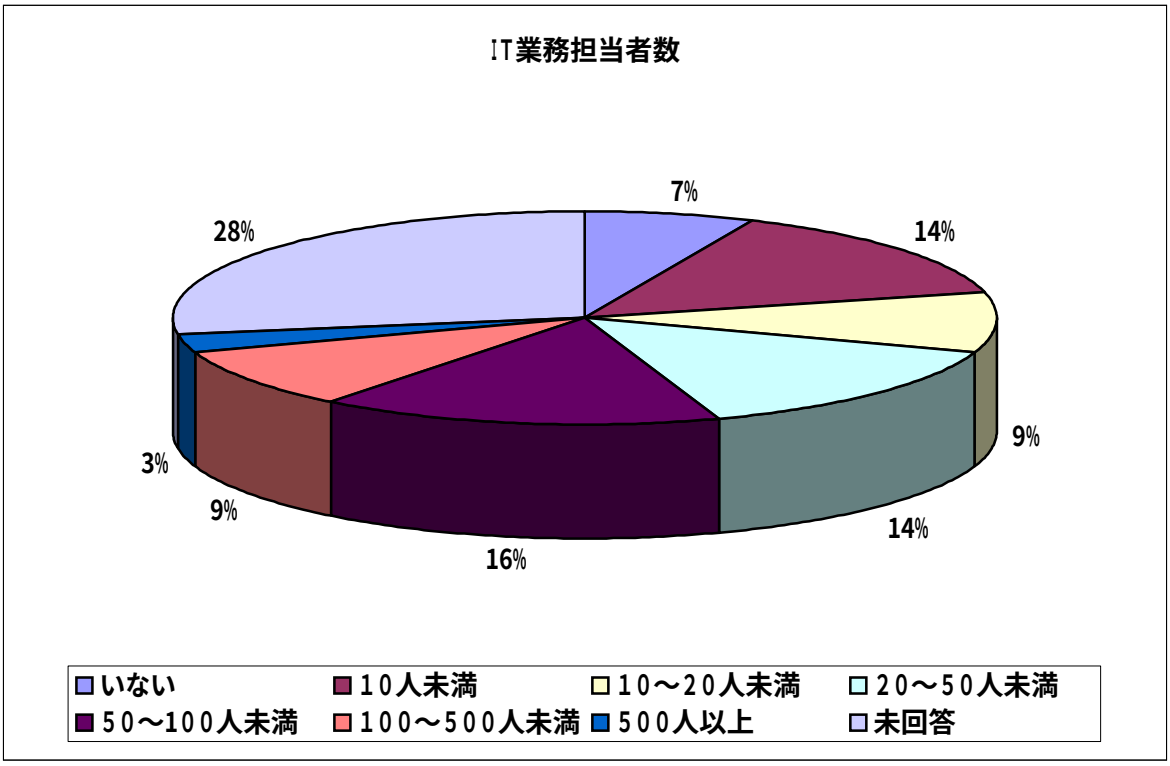
Q07　御社にIT業務を担当する方は何人いますか。(正社員)

正社員数	回答数
いない	1
１０人未満	14
１０～２０人未満	8
２０～５０人未満	14
５０～１００人未満	15
１００～５００人未満	16
５００人以上	3
未回答	5



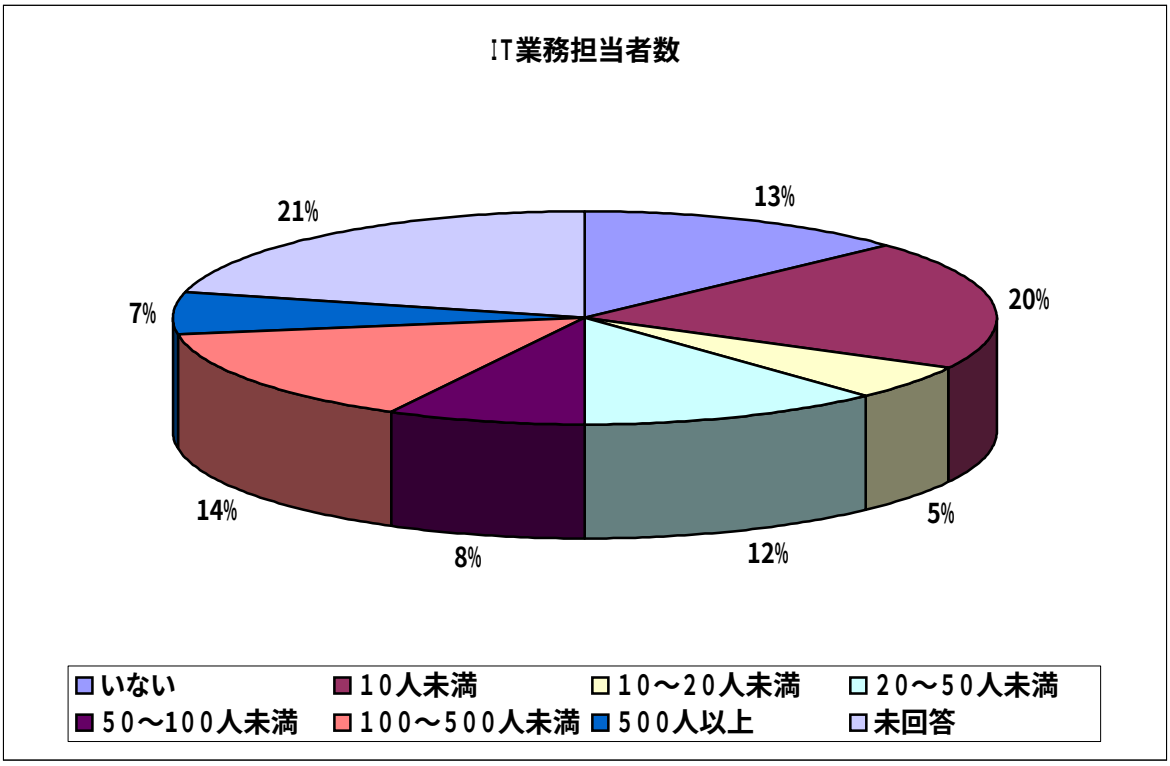
Q07　御社にIT業務を担当する方は何人いますか。(専任の正社員)

専任の正社員数	回答数
いない	5
10人未満	11
10～20人未満	7
20～50人未満	11
50～100人未満	12
100～500人未満	7
500人以上	2
未回答	21



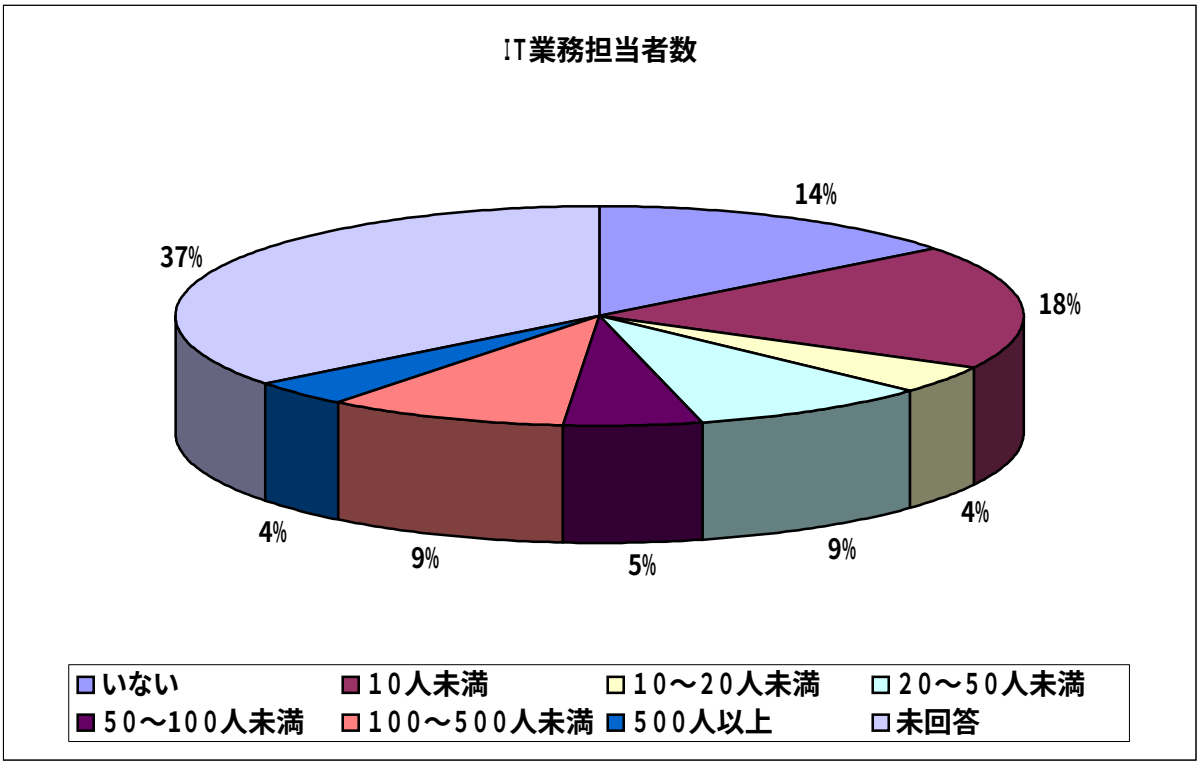
Q07　御社にIT業務を担当する方は何人いますか。(正社員以外)

正社員以外の数	回答数
いない	10
１０人未満	15
１０～２０人未満	4
２０～５０人未満	9
５０～１００人未満	6
１００～５００人未満	11
５００人以上	5
未回答	16



Q07　御社にIT業務を担当する方は何人いますか。(専任の正社員以外)

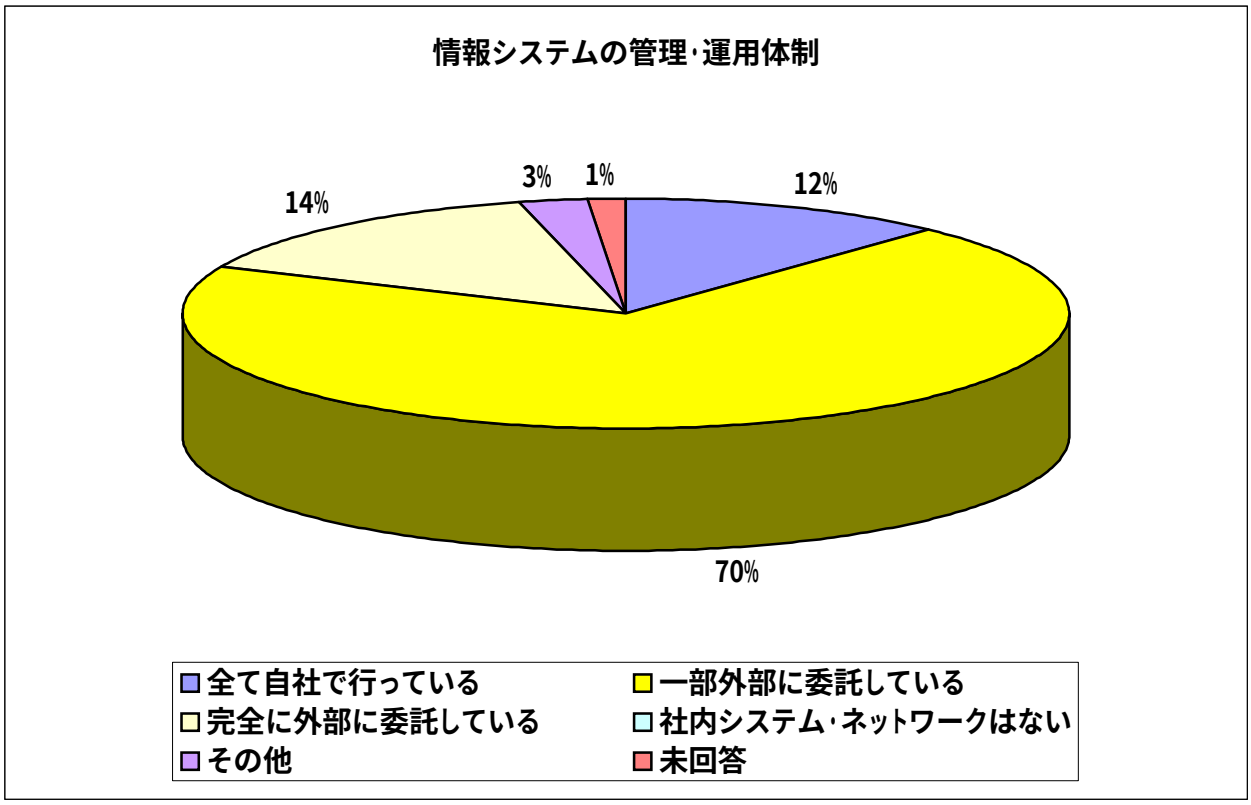
専任の正社員以外の数	回答数
いない	11
10人未満	14
10～20人未満	3
20～50人未満	7
50～100人未満	4
100～500人未満	7
500人以上	3
未回答	27



Q08　御社の情報システムの管理･運用体制はどのようになっていますか。

選択肢		回答数
1	全て自社で行っている	9
2	一部外部に委託している	53
3	完全に外部に委託している	11
4	社内システム･ネットワークはない	0
5	その他	2
	未回答	1

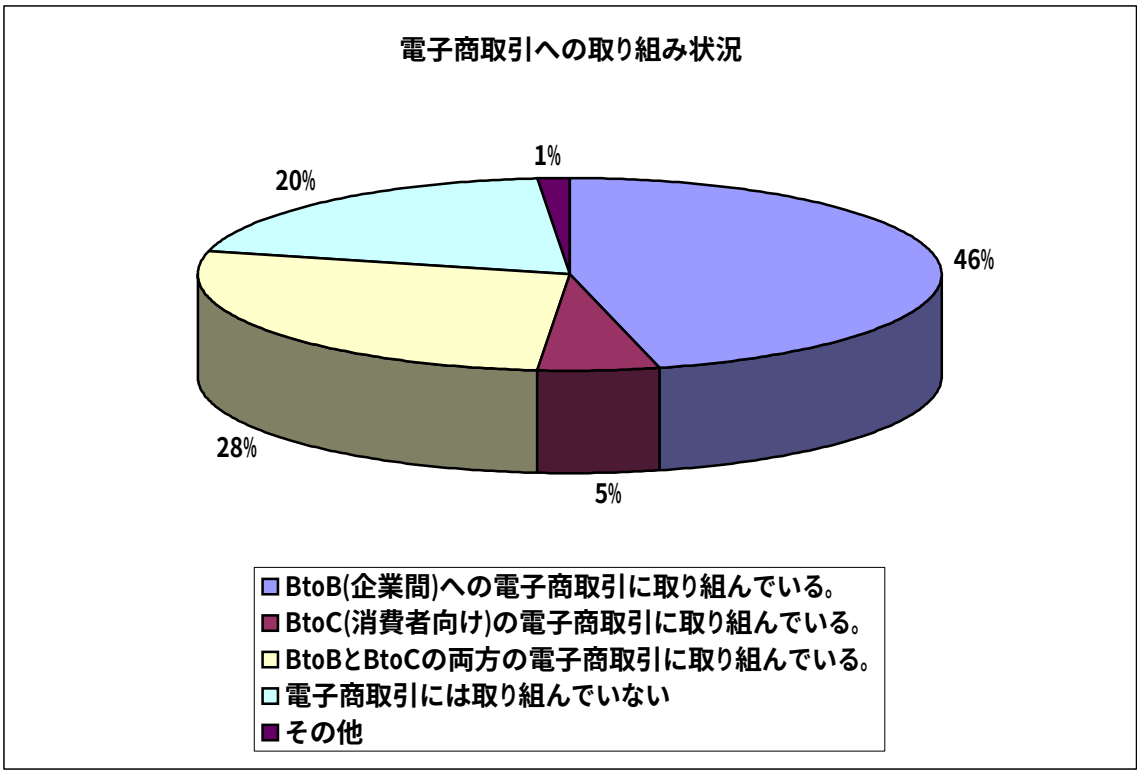
その他の回答内容
子会社に委託



Q09　電子商取引への取り組み状況を教えて下さい。

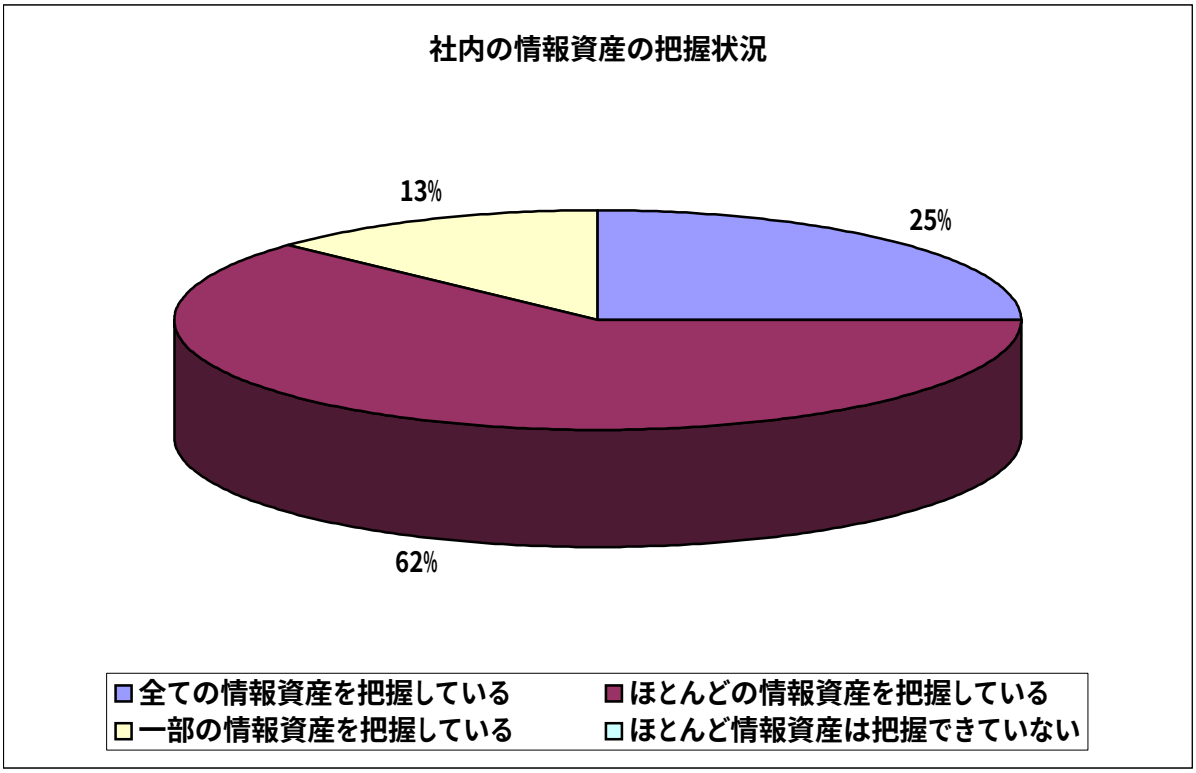
選択肢		回答数
1	BtoB(企業間)への電子商取引に取り組んでいる。	35
2	BtoC(消費者向け)の電子商取引に取り組んでいる。	4
3	BtoBとBtoCの両方の電子商取引に取り組んでいる。	21
4	電子商取引には取り組んでいない	15
5	その他	1

その他の回答内容
　顧客から要望があるときのみBtoB対応



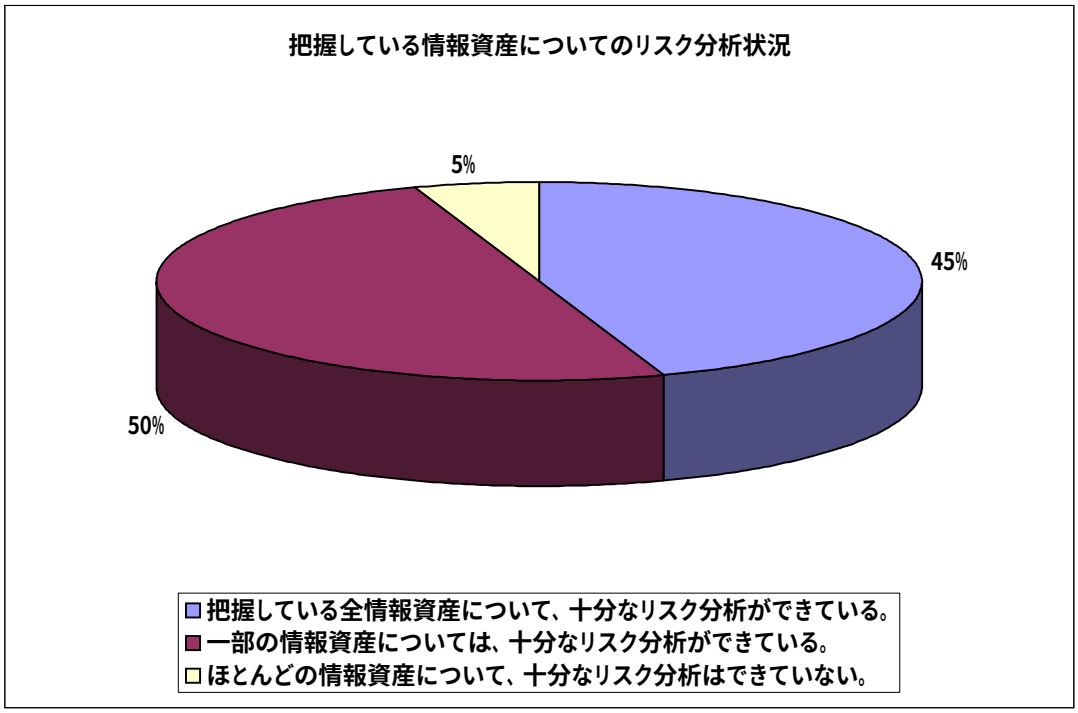
Q10　社内の情報資産について全て把握していますか。

選択肢		回答数
1	全ての情報資産を把握している	19
2	ほとんどの情報資産を把握している	47
3	一部の情報資産を把握している	10
4	ほとんど情報資産は把握できていない	0



Q11　把握している情報資産について、十分なリスク分析はできていますか。

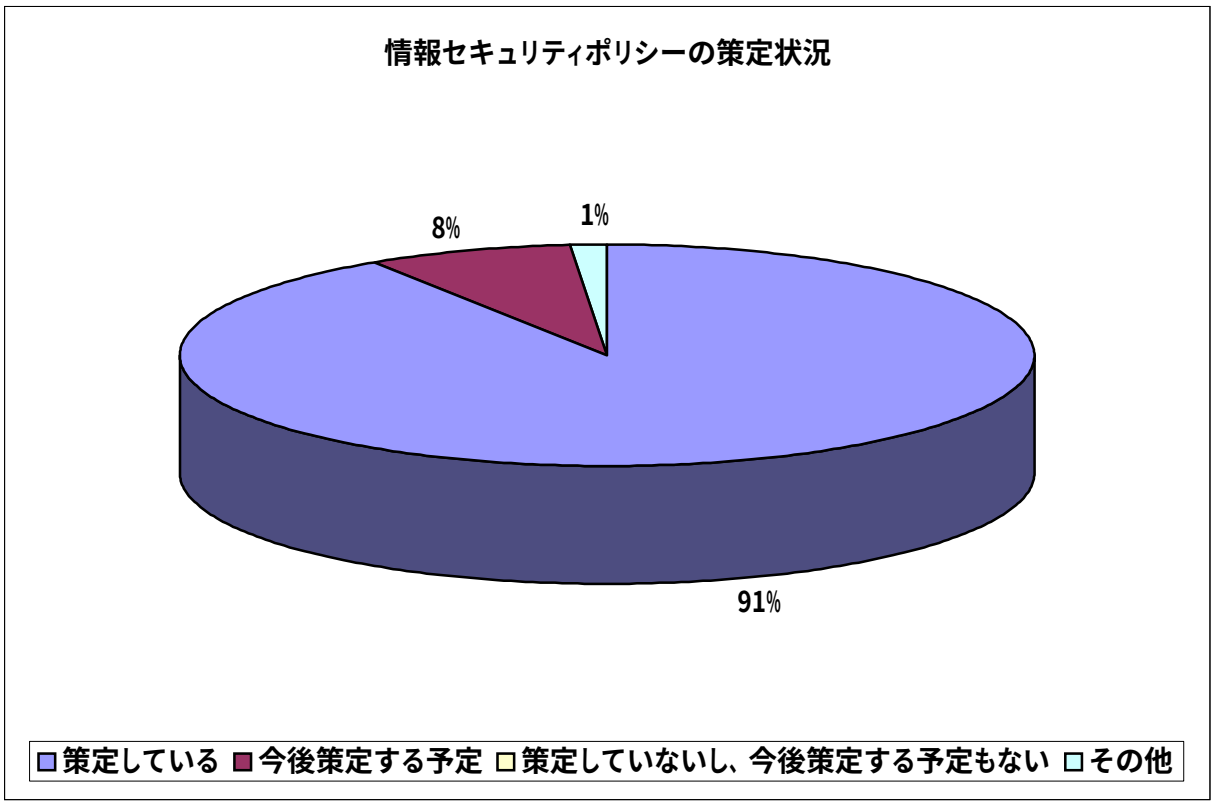
選択肢		回答数
1	把握している全情報資産について、十分なリスク分析ができている。	34
2	一部の情報資産については、十分なリスク分析ができている。	38
3	ほとんどの情報資産について、十分なリスク分析はできていない。	4



Q12　社内の情報セキュリティポリシーは策定されていますか。

	選択肢	回答数
1	策定している	69
2	今後策定する予定	6
3	策定していないし、今後策定する予定もない	0
4	その他	1

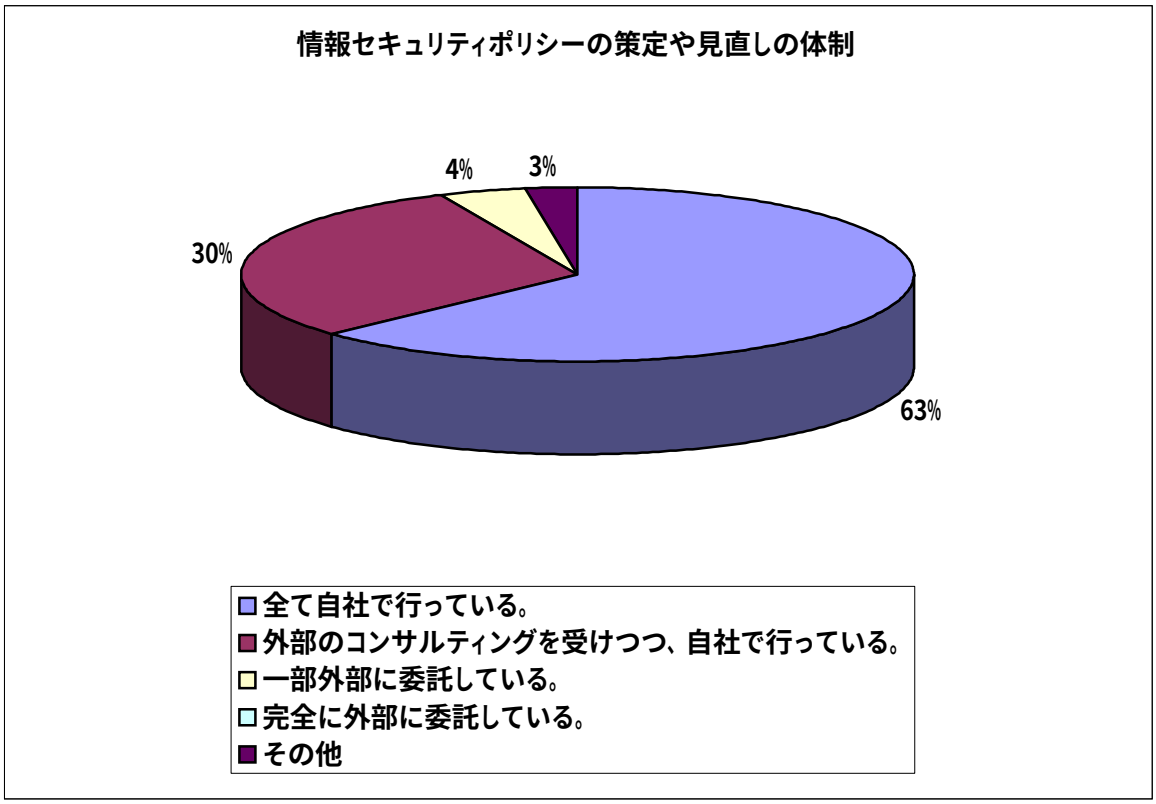
その他の回答内容
情報セキュリティガイドラインを制定



Q13　情報セキュリティポリシーの策定や見直しの体制はどのようになっていますか。

選択肢		回答数
1	全て自社で行っている。	48
2	外部のコンサルティングを受けつつ、自社で行っている。	23
3	一部外部に委託している。	3
4	完全に外部に委託している。	0
5	その他	2

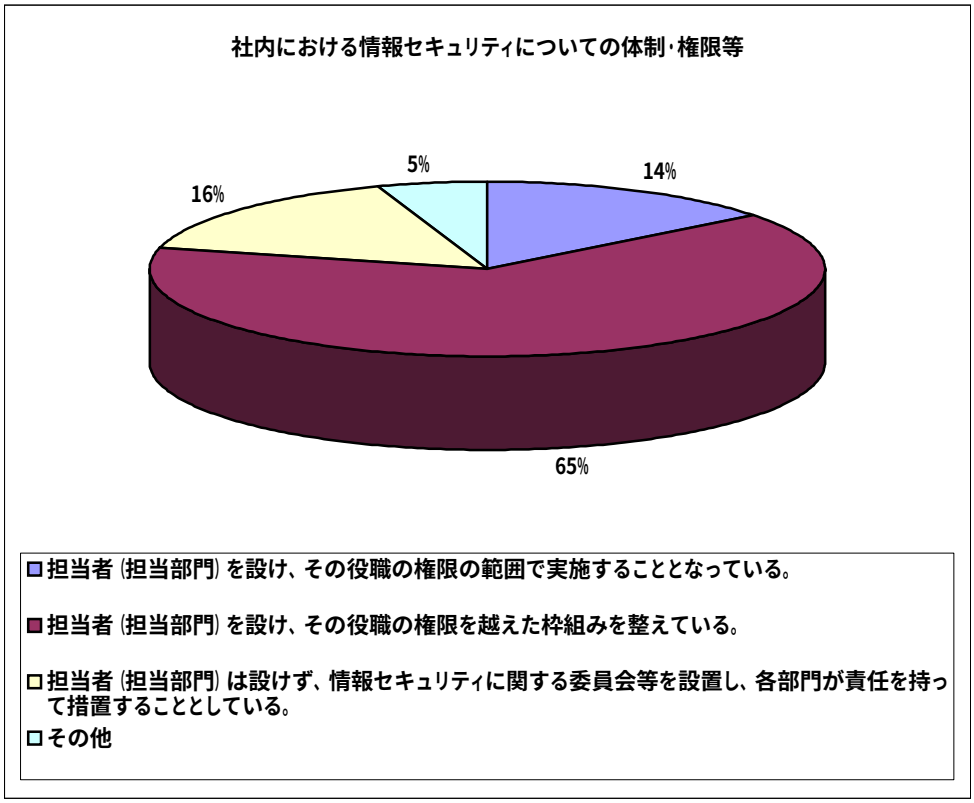
その他の回答内容
子会社と共同で策定中
グループ全体として取り組んでいる



Q14　御社の情報セキュリティについて、社内における体制･権限等はどのようになっていますか。

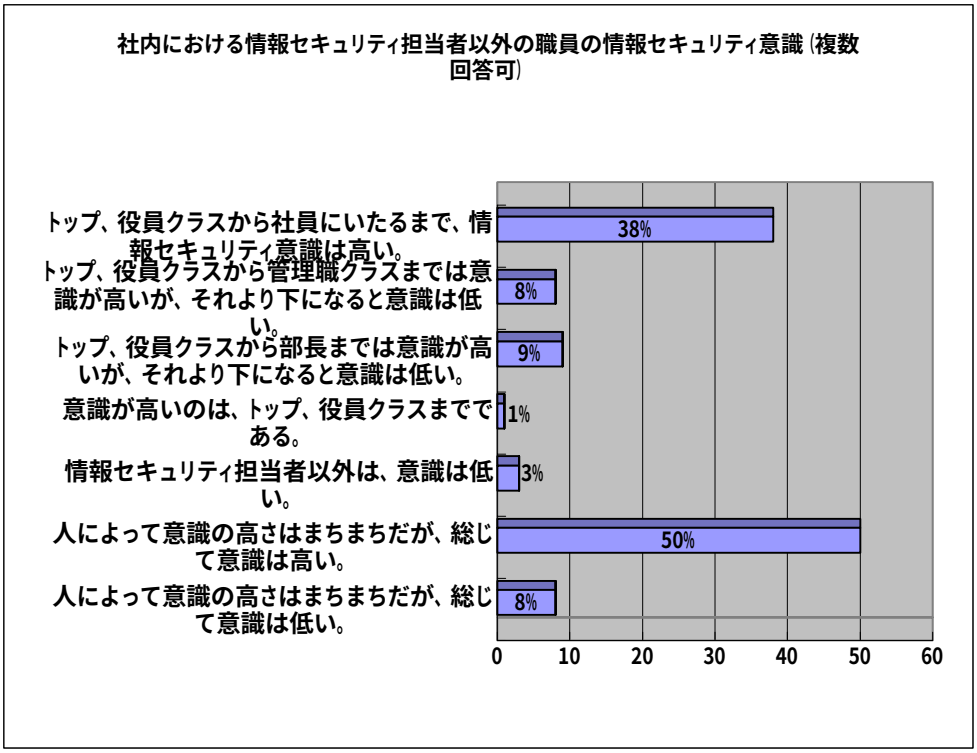
	選択肢	回答数
1	担当者（担当部門）を設け、その役職の権限の範囲で実施することとなっている。	11
2	担当者（担当部門）を設け、その役職の権限を越えた枠組みを整えている。	49
3	担当者（担当部門）は設けず、情報セキュリティに関する委員会等を設置し、各部門が責任を持って措置することとしている。	12
4	その他	4

その他の回答内容
情報セキュリティ委員会を設置し、全体を統括する担当者（担当部門）も設置している。
個人情報以外については100%子会社のシステム会社
推進の担当者を設けるが、委員会を設置し、各部門の実施にゆだねている。
情報システム部門で適宜実施している。



Q15　社内における情報セキュリティ担当者以外の職員の情報セキュリティ意識について教えて下さい。(複数回答可)

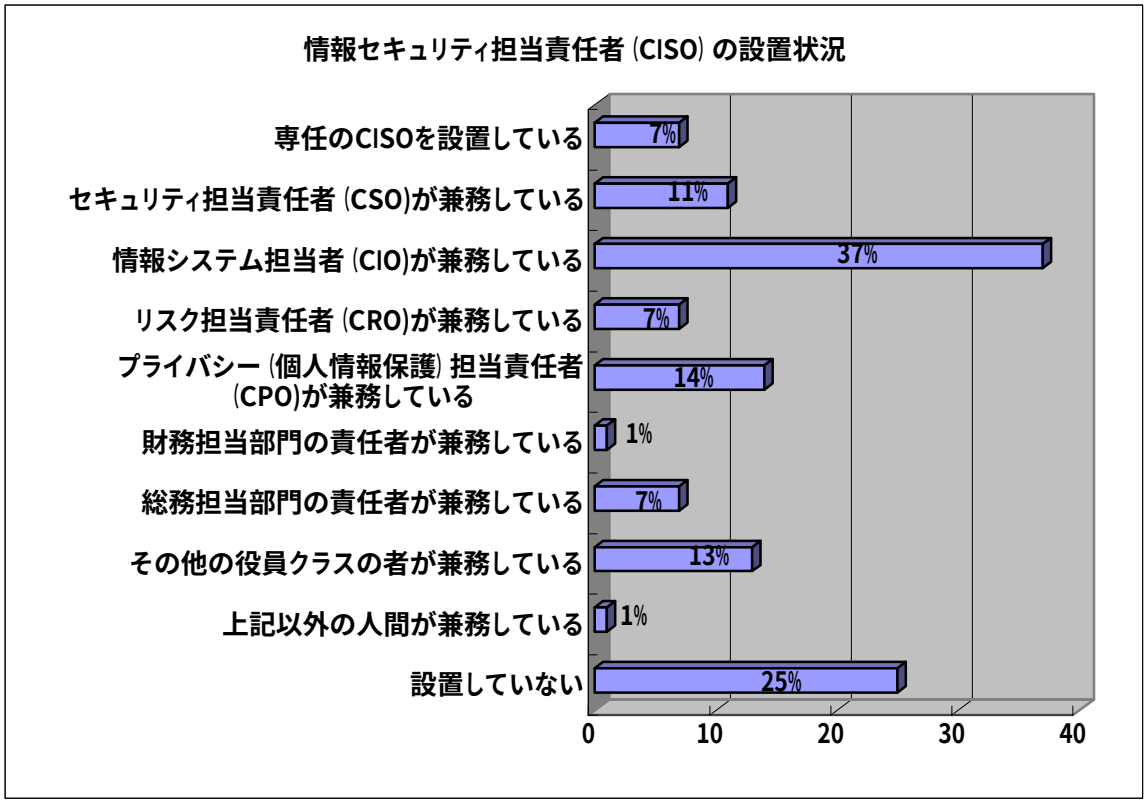
	選択肢	%	回答数
1	トップ、役員クラスから社員にいたるまで、情報セキュリティ意識は高い。	38	29
2	トップ、役員クラスから管理職クラスまでは意識が高いが、それより下になると意識は低い	8	6
3	トップ、役員クラスから部長までは意識が高いが、それより下になると意識は低い。	9	7
4	意識が高いのは、トップ、役員クラスまでである。	1	1
5	情報セキュリティ担当者以外は、意識は低い。	3	2
6	人によって意識の高さはまちまちだが、総じて意識は高い。	50	38
7	人によって意識の高さはまちまちだが、総じて意識は低い。	8	6



Q16　情報セキュリティ担当責任者を設置していますか。

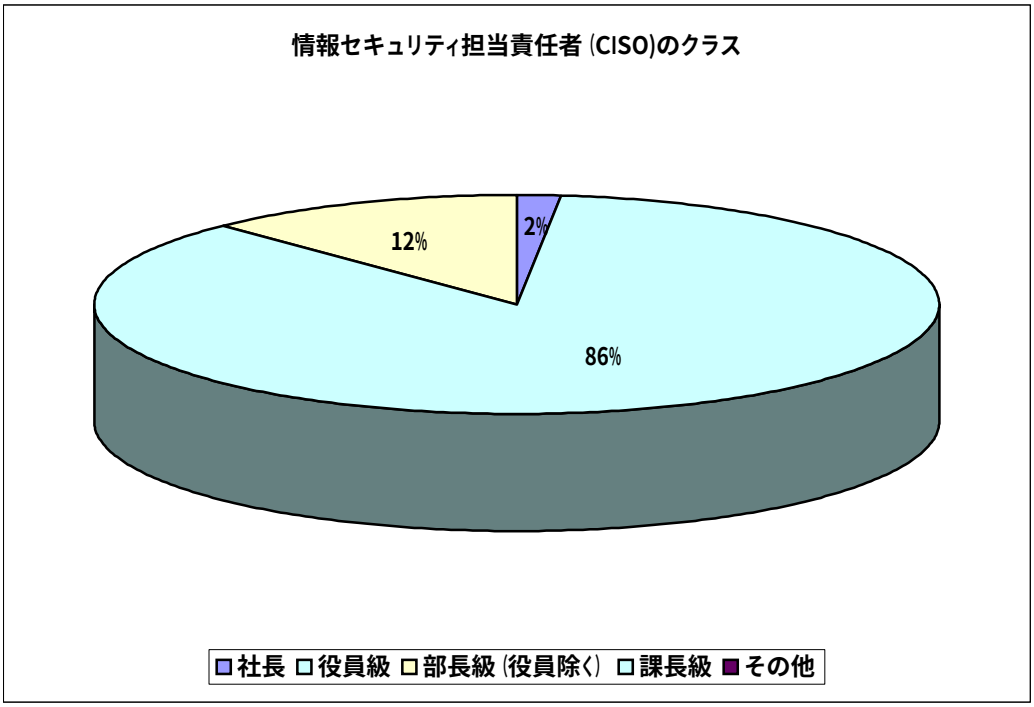
	選択肢	%	回答数
1	専任のCISOを設置している	7	5
2	セキュリティ担当責任者（CSO)が兼務している	11	8
3	情報システム担当者（CIO)が兼務している	37	28
4	リスク担当責任者（CRO)が兼務している	7	5
5	プライバシー（個人情報保護）担当責任者（CPO)が兼務している	14	11
6	財務担当部門の責任者が兼務している	1	1
7	総務担当部門の責任者が兼務している	7	5
8	その他の役員クラスの者が兼務している	13	10
9	上記以外の人間が兼務している	1	1
10	設置していない	25	19

複数回答	2、3	1
	2、3、4、5、7	1
	2、4、5	2
	2、5	1
	2、8	1
	3、5	2
	3、6	1
	3、8	1
	4、5	1
	5、7	1



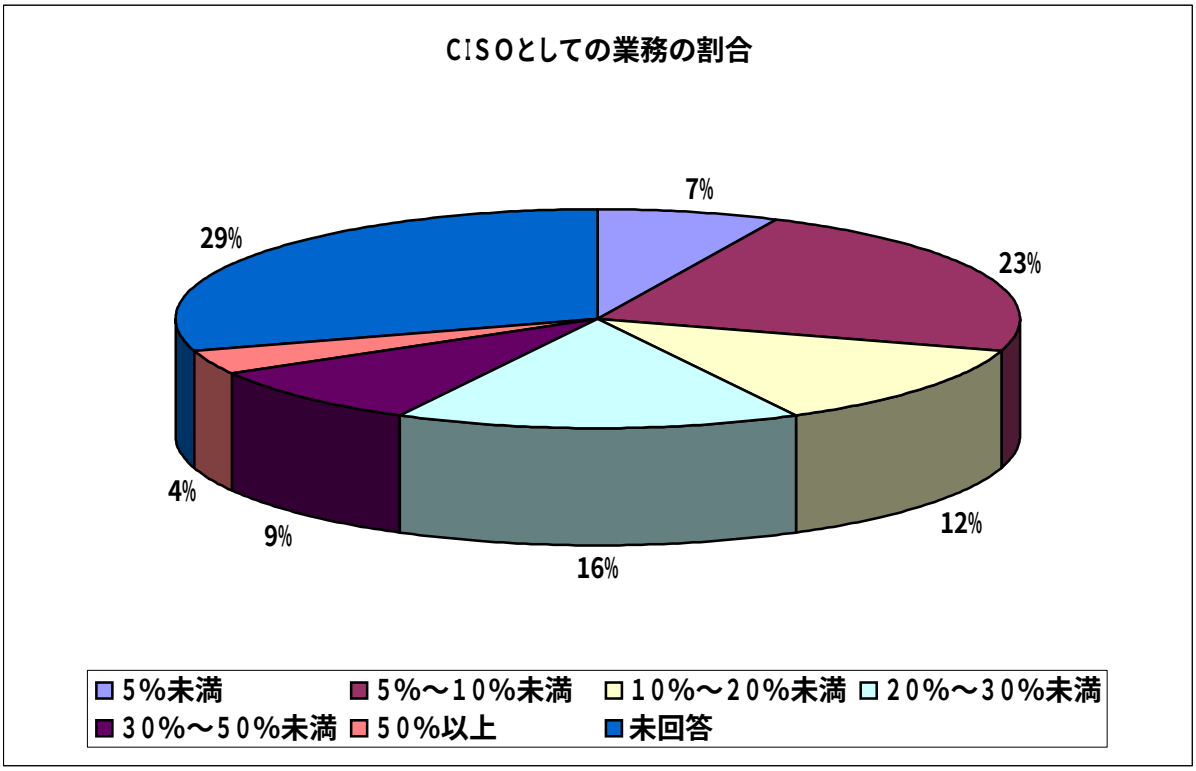
Q17　情報セキュリティ担当責任者（CISO)の方はどのようなクラスの方ですか。

	選択肢	回答数
1	社長	1
2	役員級	49
3	部長級（役員除く）	7
4	課長級	0
5	その他	0



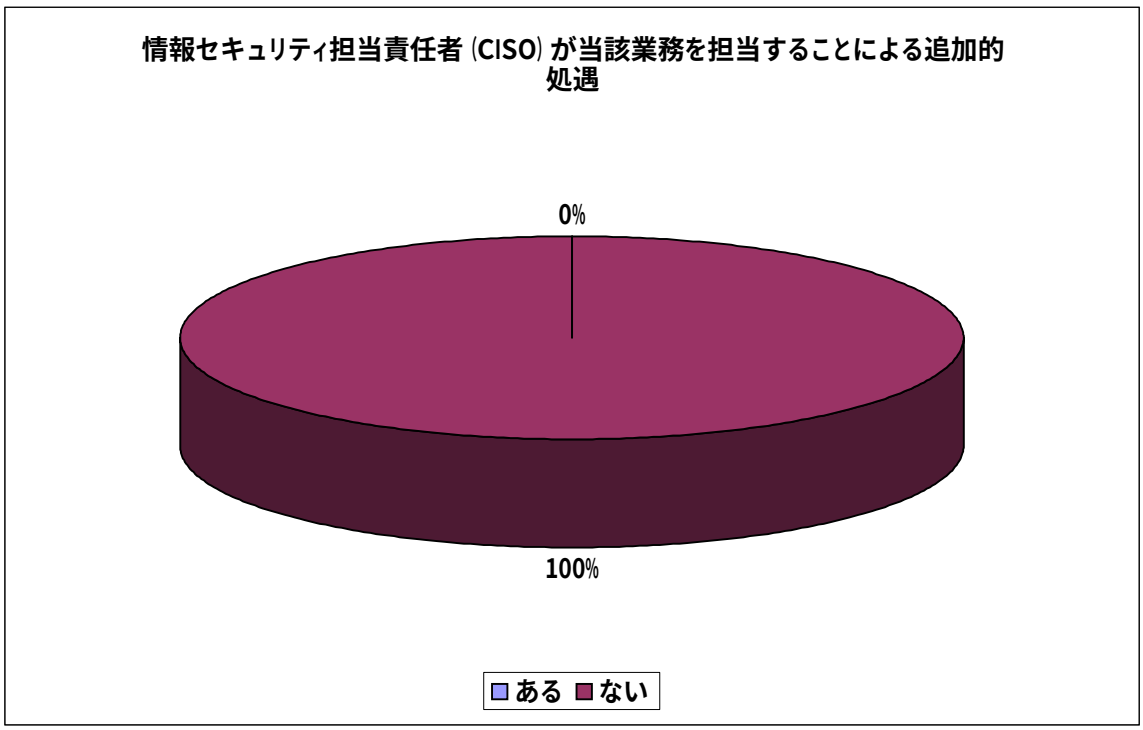
Q18　CISOを兼務している方の全業務のうち、CISOとしての業務は何%ぐらいですか。

CISOとしての業務	回答数
5%未満	4
5%～10%未満	13
10%～20%未満	7
20%～30%未満	9
30%～50%未満	5
50%以上	2
未回答	17



Q19　情報セキュリティ担当責任者（CISO）が当該業務を担当することによる追加的処遇はありますか

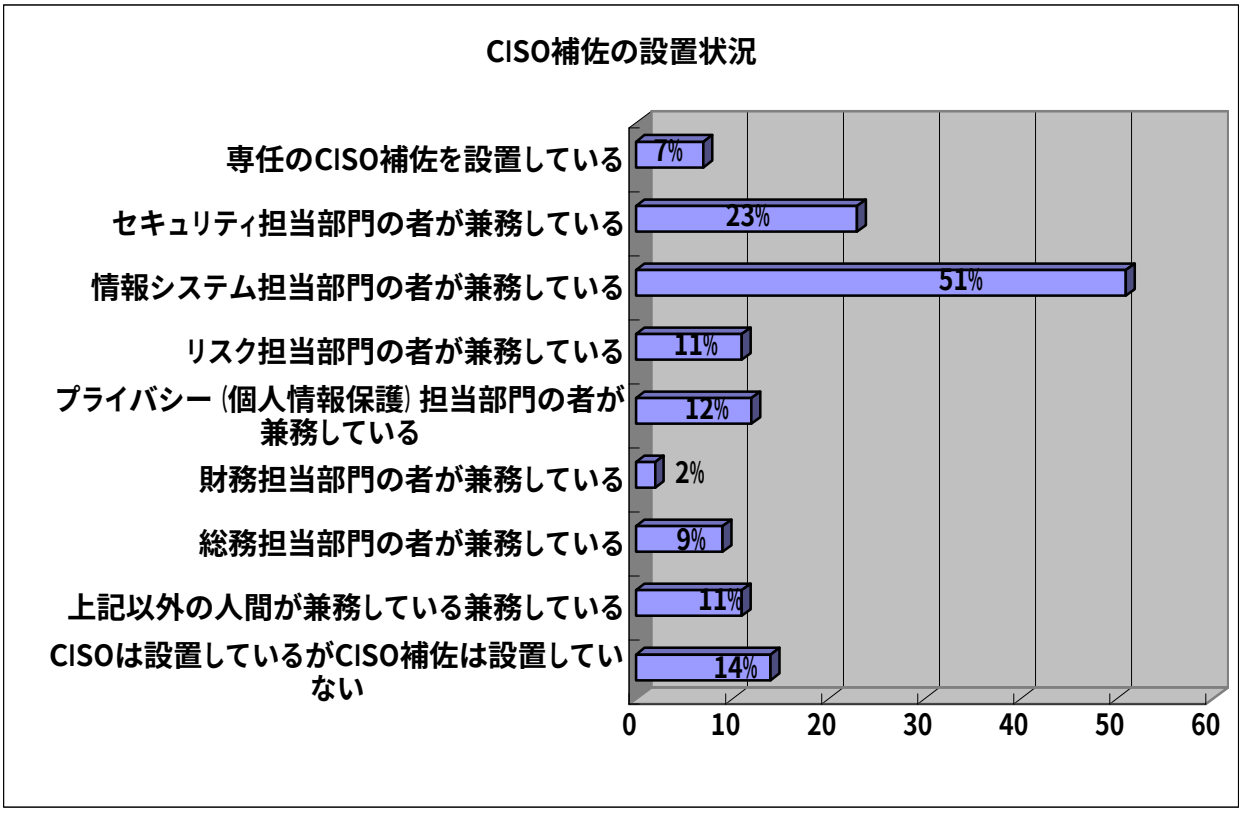
選択肢		回答数
1	ある	0
2	ない	57



Q20　CISO補佐を設置していますか。

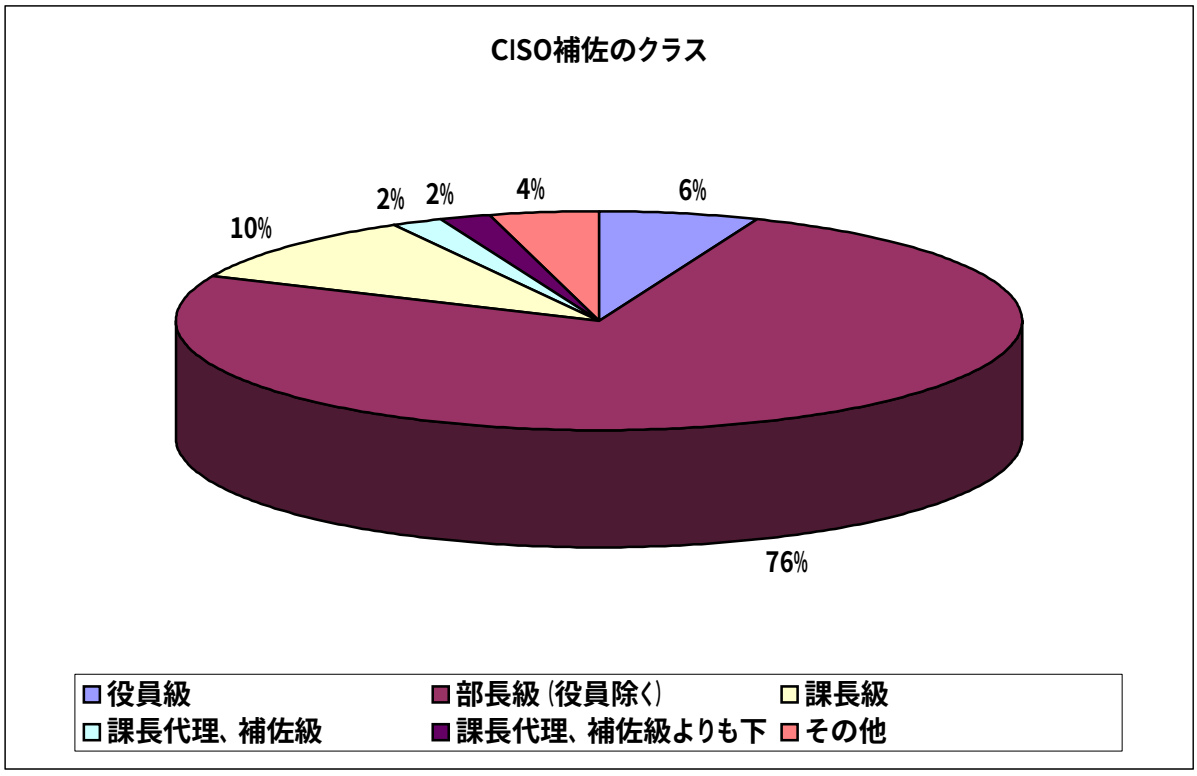
	選択肢	%	回答数
1	専任のCISO補佐を設置している	7	4
2	セキュリティ担当部門の者が兼務している	23	13
3	情報システム担当部門の者が兼務している	51	29
4	リスク担当部門の者が兼務している	11	6
5	プライバシー（個人情報保護）担当部門の者が兼務している	12	7
6	財務担当部門の者が兼務している	2	1
7	総務担当部門の者が兼務している	9	5
8	上記以外の人間が兼務している兼務している	11	6
9	CISOは設置しているがCISO補佐は設置していない	14	8

複数回答	2、3	2
	2、3、4	1
	2、3、4、5	1
	2、3、4、5、7	1
	2、3、4、5、6、7、8	1
	2、5	1
	3、5、8	1
	3、7	2



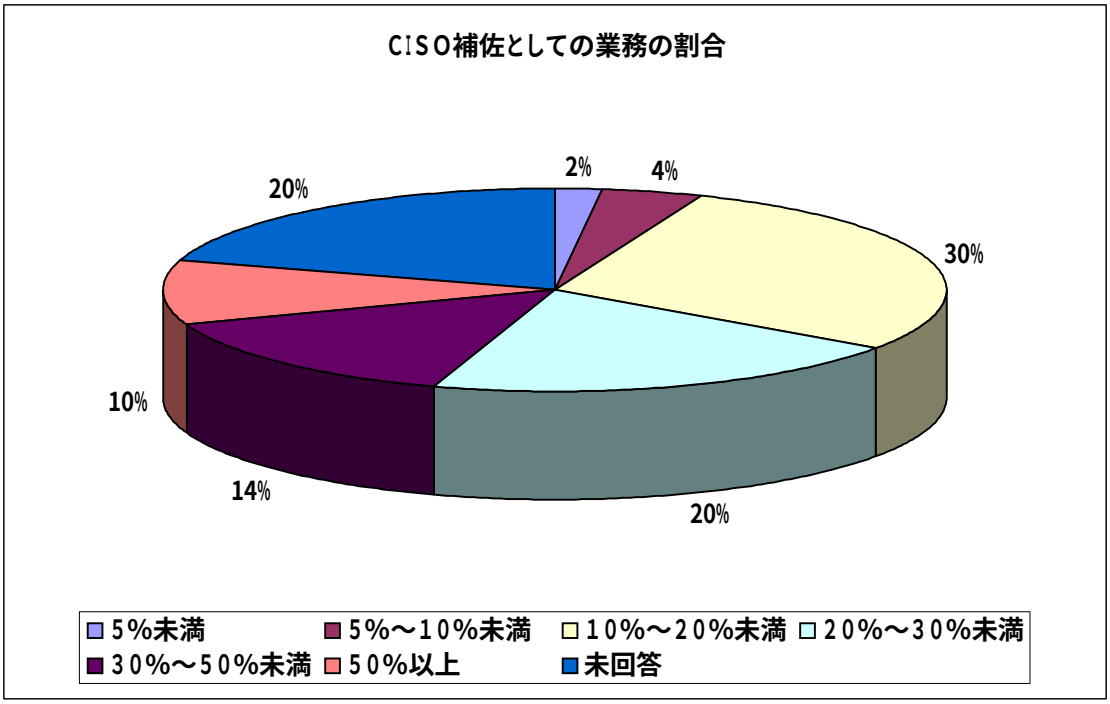
Q21　CISO補佐はどのようなクラスの方ですか。

	選択肢	回答数
1	役員級	3
2	部長級（役員除く）	37
3	課長級	5
4	課長代理、補佐級	1
5	課長代理、補佐級よりも下	1
6	その他	2



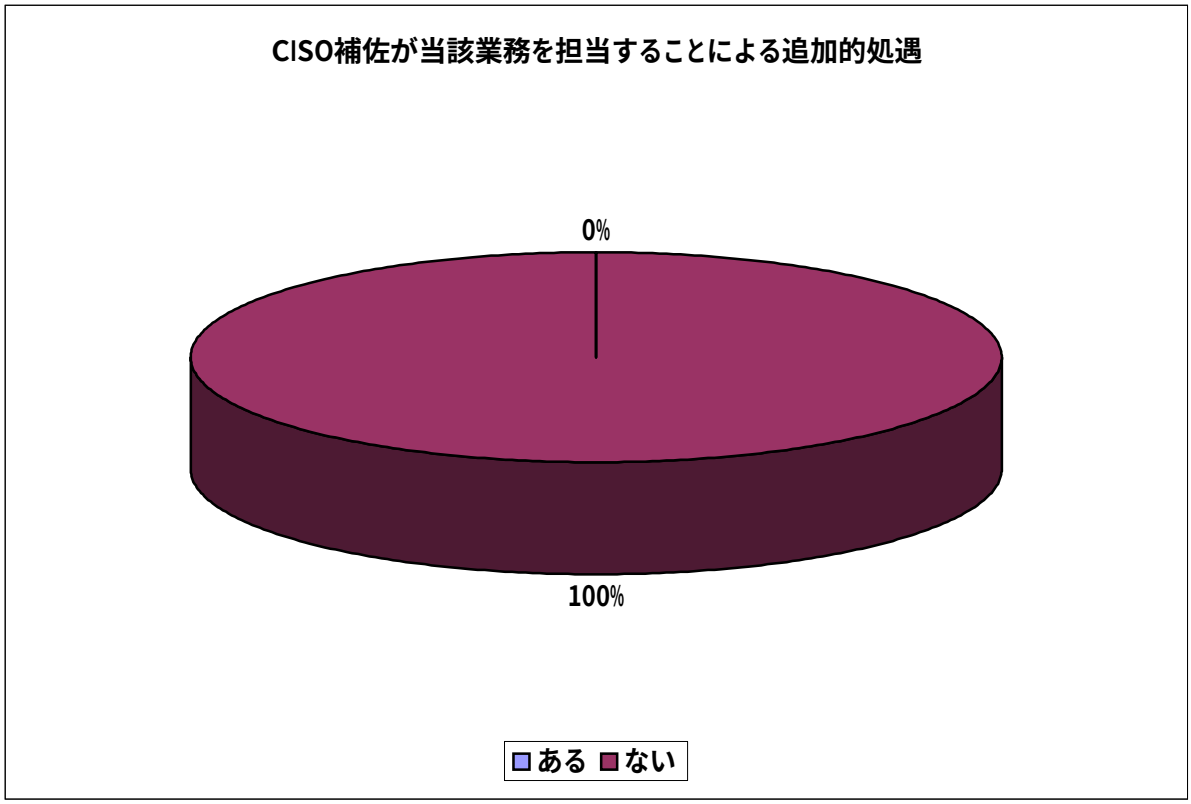
Q22　CISO補佐を兼務している方の全業務のうち、CISO補佐としての業務は何%ぐらいですか。

CISO補佐としての業務	回答数
5%未満	1
5%～10%未満	2
10%～20%未満	14
20%～30%未満	10
30%～50%未満	7
50%以上	5
未回答	10



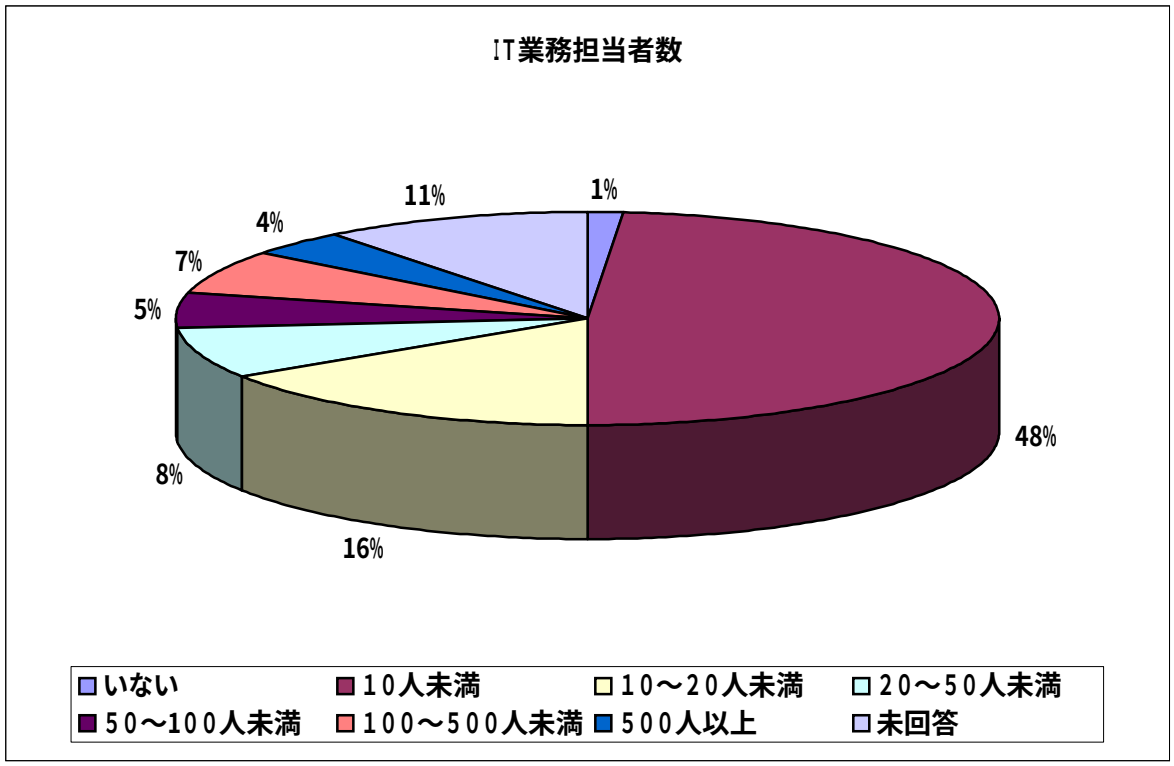
Q23　CISO補佐が当該業務を担当することによる追加的処遇はありますか

選択肢		回答数
1	ある	0
2	ない	49



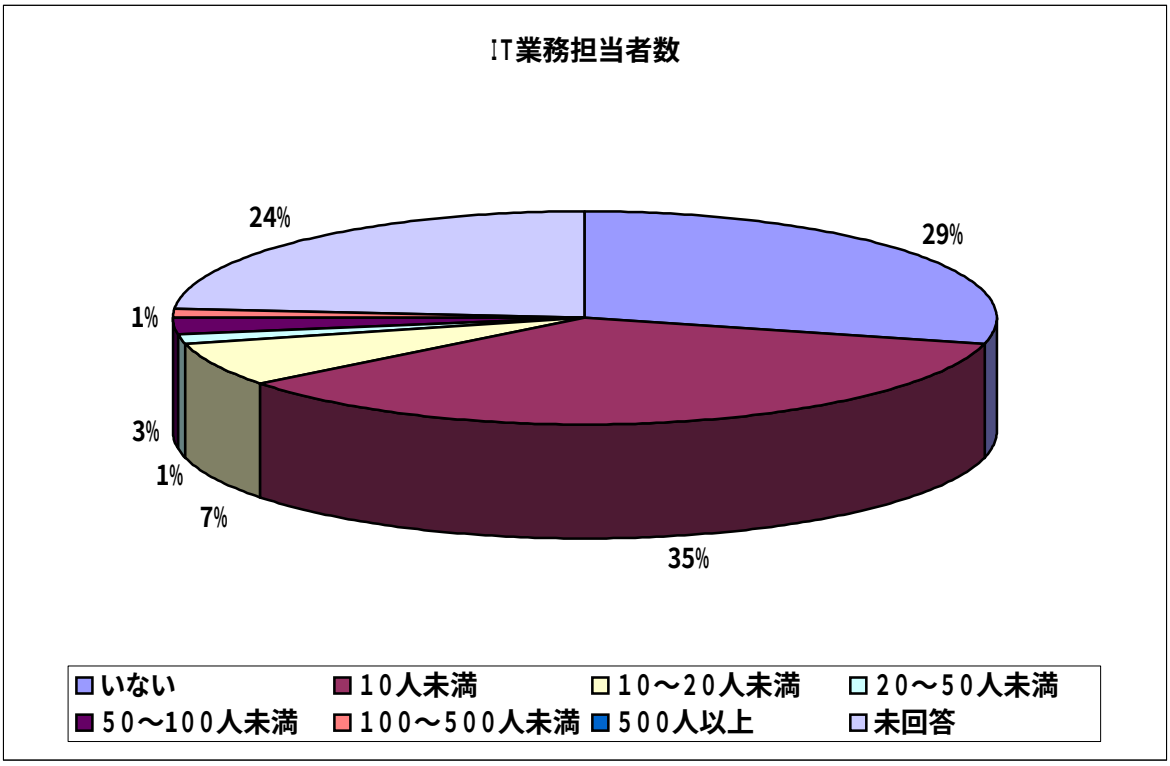
Q24　御社に情報セキュリティ業務を担当する方は何人いますか。(正社員)

正社員数	回答数
いない	1
10人未満	37
10～20人未満	12
20～50人未満	6
50～100人未満	4
100～500人未満	5
500人以上	3
未回答	8



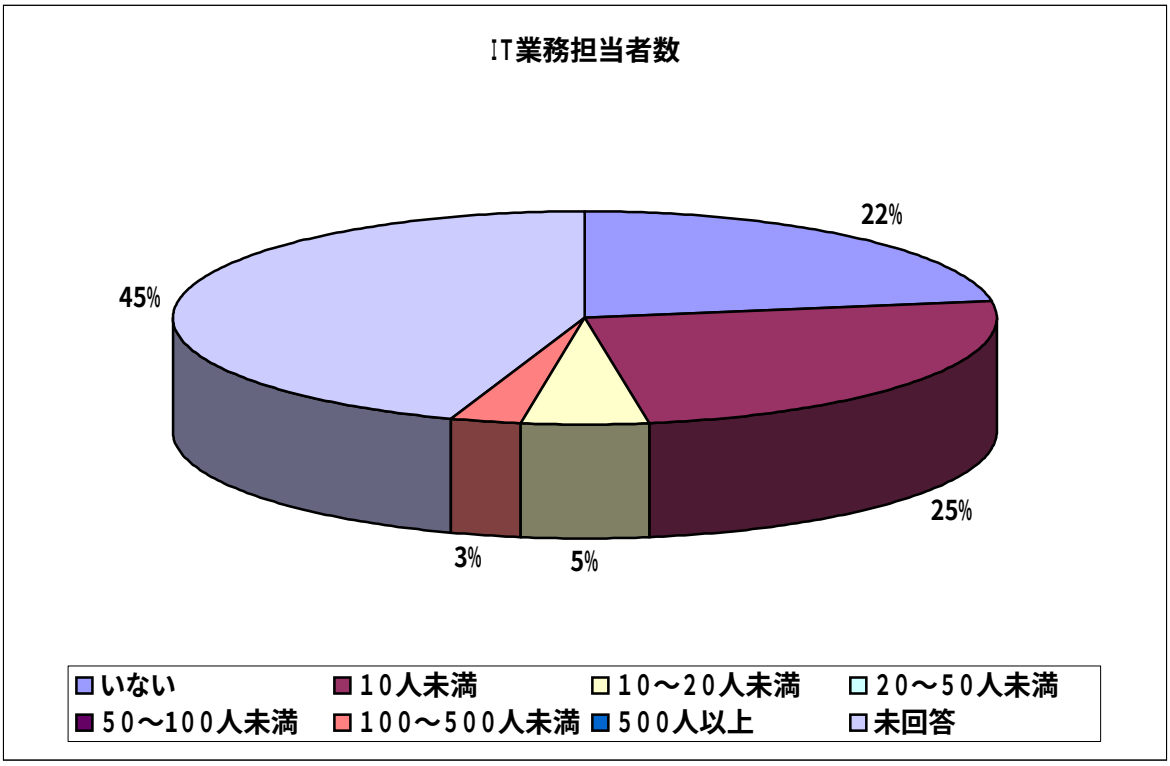
Q24　御社に情報セキュリティ業務を担当する方は何人いますか。(専任の正社員)

専任の正社員数	回答数
いない	22
１０人未満	27
１０～２０人未満	5
２０～５０人未満	1
５０～１００人未満	2
１００～５００人未満	1
５００人以上	0
未回答	18



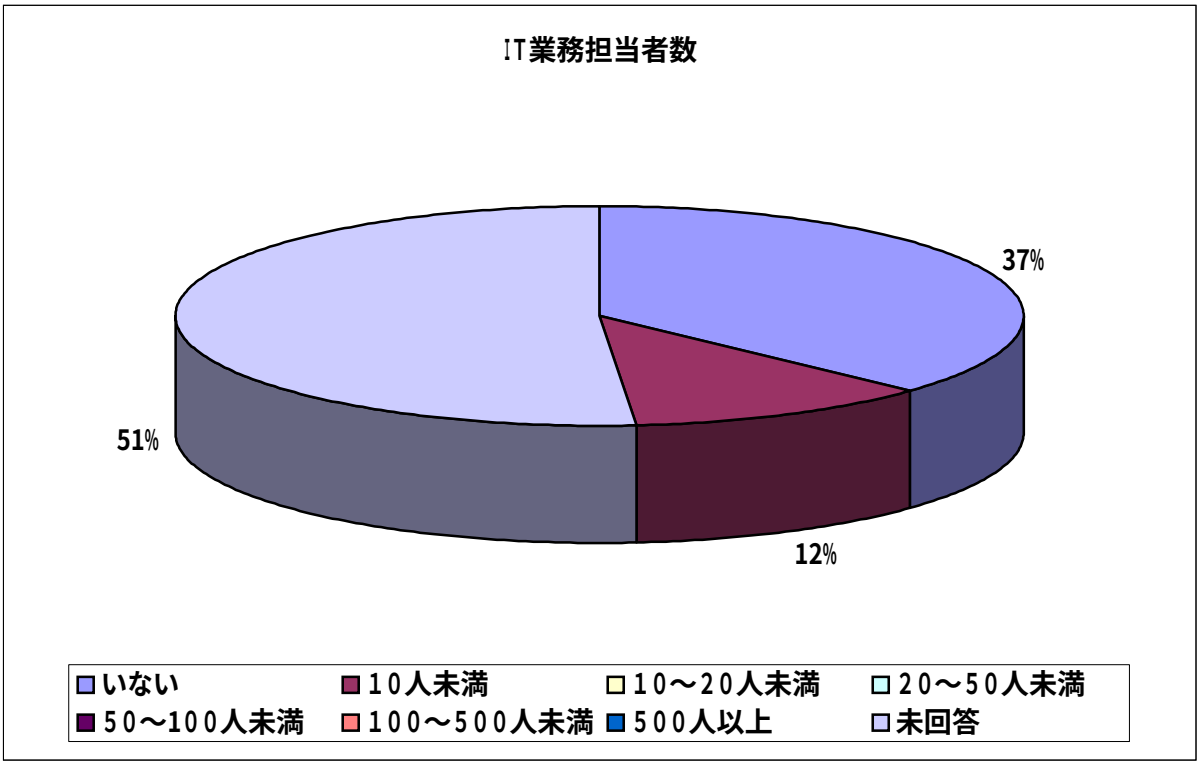
Q24　御社に情報セキュリティ業務を担当する方は何人いますか。(正社員以外)

正社員以外の数	回答数
いない	17
１０人未満	19
１０～２０人未満	4
２０～５０人未満	0
５０～１００人未満	0
１００～５００人未満	2
５００人以上	0
未回答	34



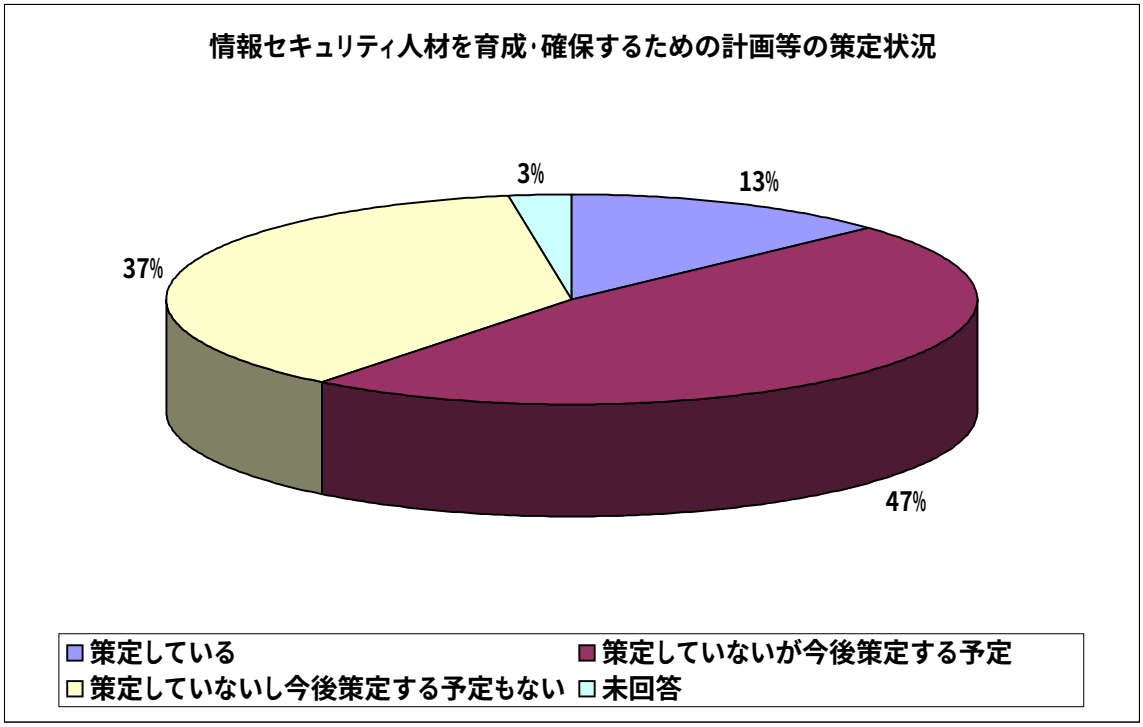
Q24　御社に情報セキュリティ業務を担当する方は何人いますか。(専任の正社員以外)

専任の正社員以外の数	回答数
いない	28
10人未満	9
10～20人未満	0
20～50人未満	0
50～100人未満	0
100～500人未満	0
500人以上	0
未回答	39



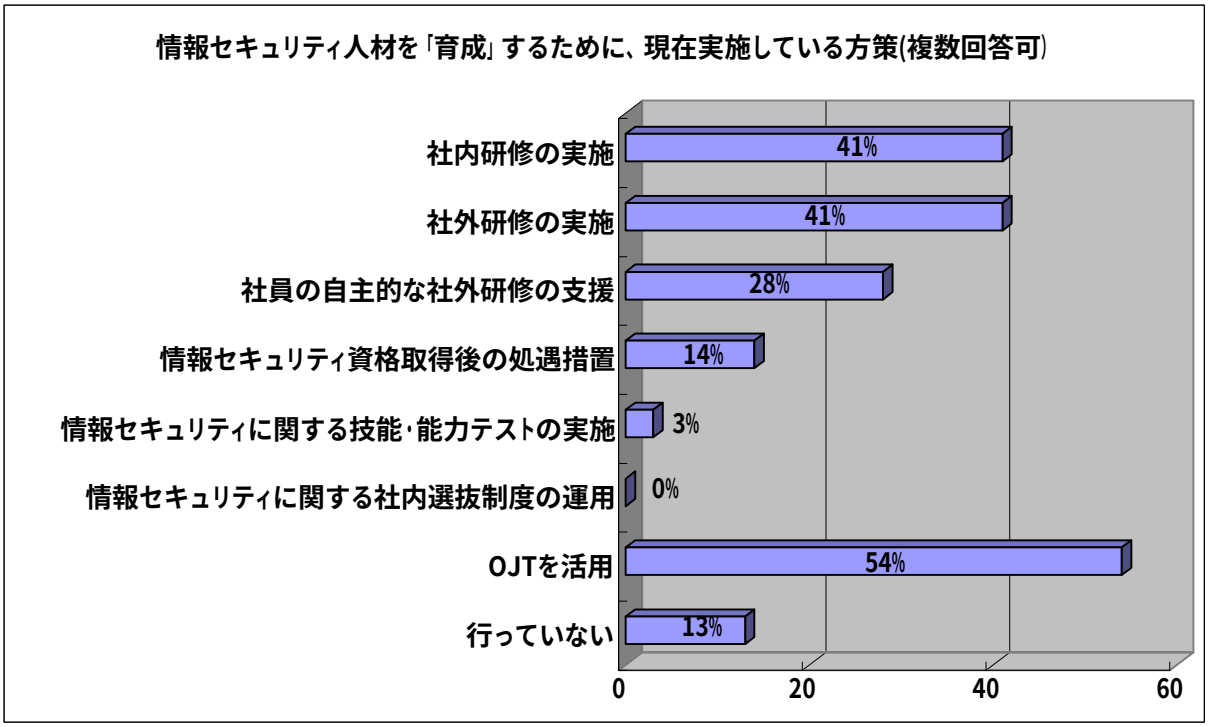
Q27　御社内で情報セキュリティ人材を育成･確保するための計画等を策定していますか。

選択肢		回答数
1	策定している	10
2	策定していないが今後策定する予定	36
3	策定していないし今後策定する予定もない	28
	未回答	2



Q28　情報セキュリティ人材を「育成」するために、現在御社で実施している方策を以下から選んで下さい。(複数回答可)

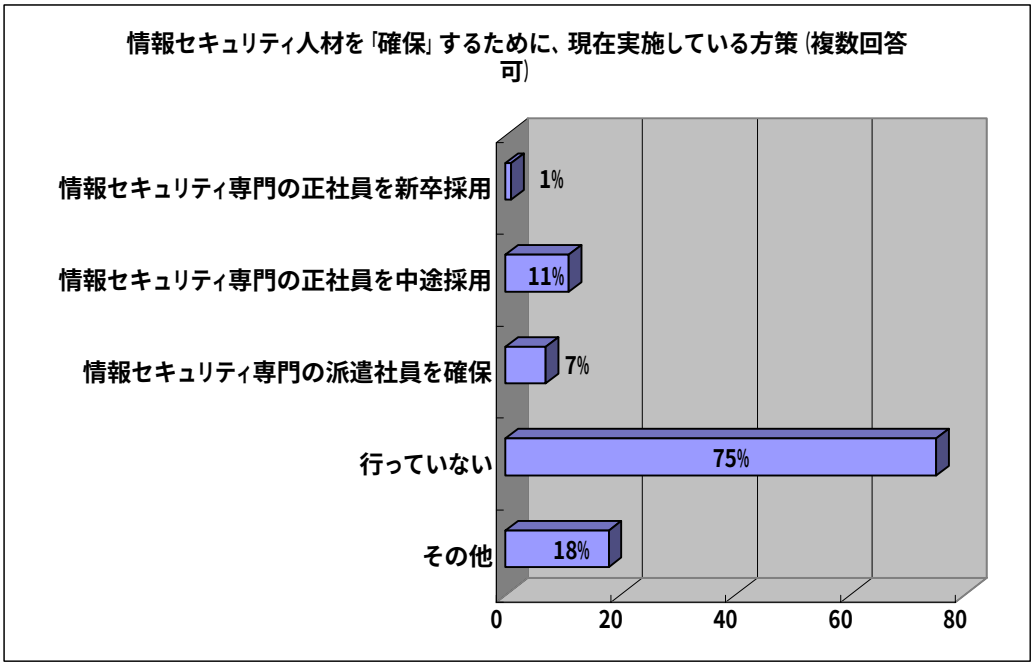
	選択肢	%	回答数
1	社内研修の実施	41	31
2	社外研修の実施	41	31
3	社員の自主的な社外研修の支援	28	21
4	情報セキュリティ資格取得後の処遇措置	14	11
5	情報セキュリティに関する技能･能力テストの実施	3	2
6	情報セキュリティに関する社内選抜制度の運用	0	0
7	OJTを活用	54	41
8	行っていない	13	10



Q29　情報セキュリティ人材を「確保」するために、現在御社で実施している方策を以下から選んで下さい。（複数回答可）

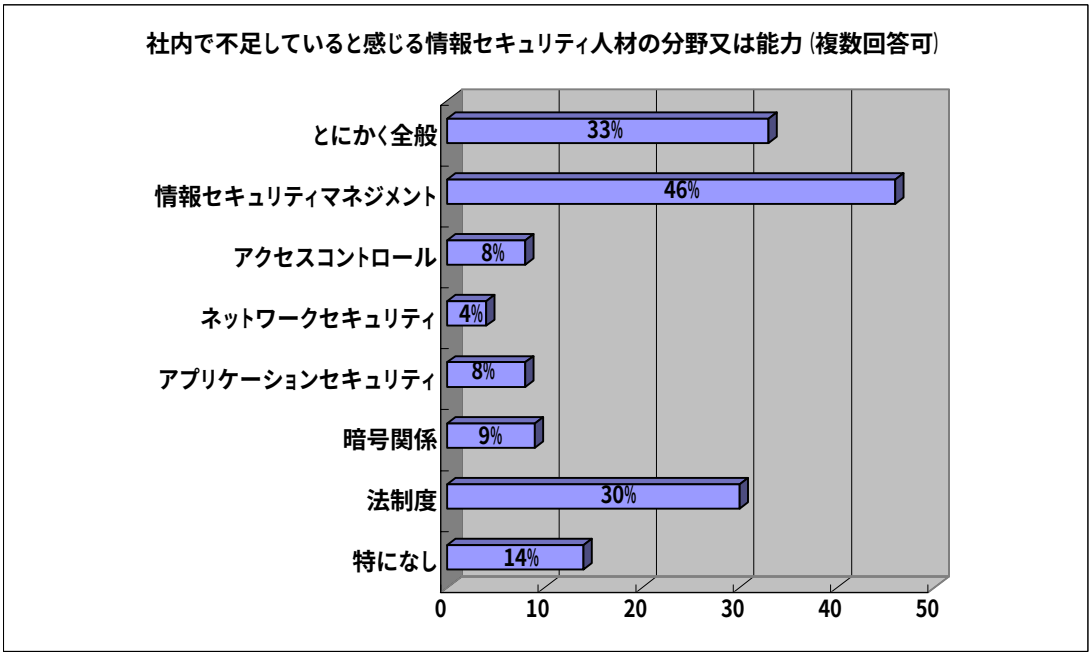
	選択肢	%	回答数
1	情報セキュリティ専門の正社員を新卒採用	1	1
2	情報セキュリティ専門の正社員を中途採用	11	8
3	情報セキュリティ専門の派遣社員を確保	7	5
4	行っていない	75	57
5	その他	18	14

その他の回答内容
育成のための外部研修を受講
一部業務委託しているが、情報セキュリティ人材は社内で育成
一部業務委託
採用時にセキュリティに関するスキルや経験をチェックしている
外部業務委託の活用
必要に応じ、外部専門家（コンサルト等）を活用
セキュリティポリシーの策定とそれに合ったインフラ作り及び運用のサービスレベルの統一
システム子会社のセキュリティ部門の全面協力を得ている
グループ会社の情報セキュリティ専門家からの支援を受けている
固定的な方策なし
社内公募
外部コンサルト等専門家の積極活用



Q30　現在社内で不足していると感じる情報セキュリティ人材の分野又は能力を以下から選んで下さい。(複数回答可)

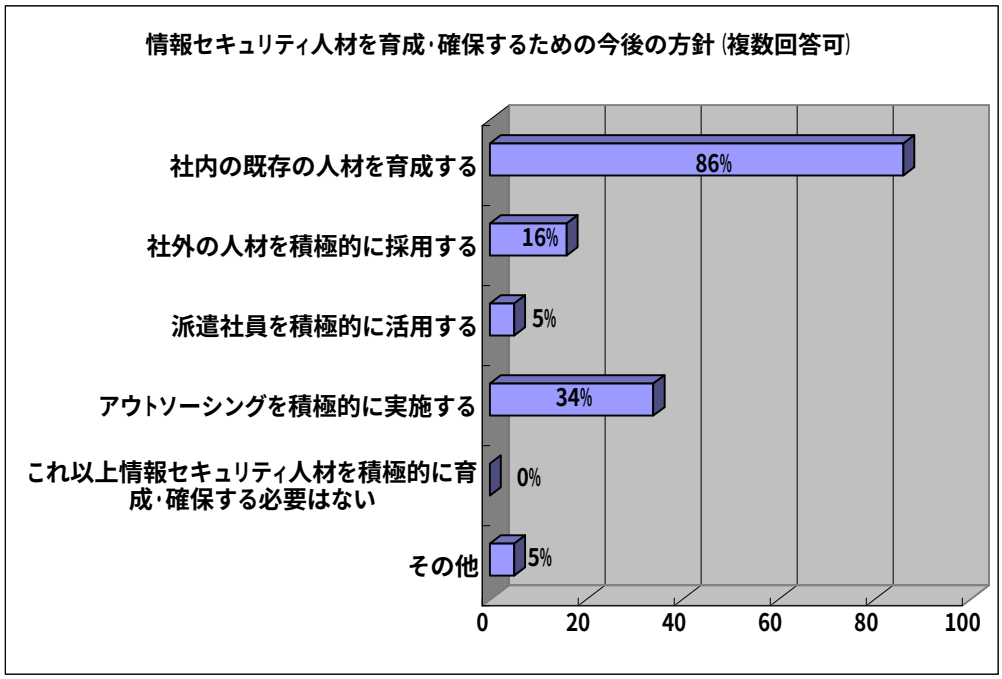
	選択肢	%	回答数
1	とにかく全般	33	25
2	情報セキュリティマネジメント	46	35
3	アクセスコントロール	8	6
4	ネットワークセキュリティ	4	3
5	アプリケーションセキュリティ	8	6
6	暗号関係	9	7
7	法制度	30	23
8	特になし	14	11



Q32　情報セキュリティ人材を育成･確保するための今後の方針を以下から選んで下さい。(複数回答可)

	選択肢	%	回答数
1	社内の既存の人材を育成する	86	65
2	社外の人材を積極的に採用する	16	12
3	派遣社員を積極的に活用する	5	4
4	アウトソーシングを積極的に実施する	34	26
5	これ以上情報セキュリティ人材を積極的に育成･確保する必要はない	0	0
6	その他	5	4

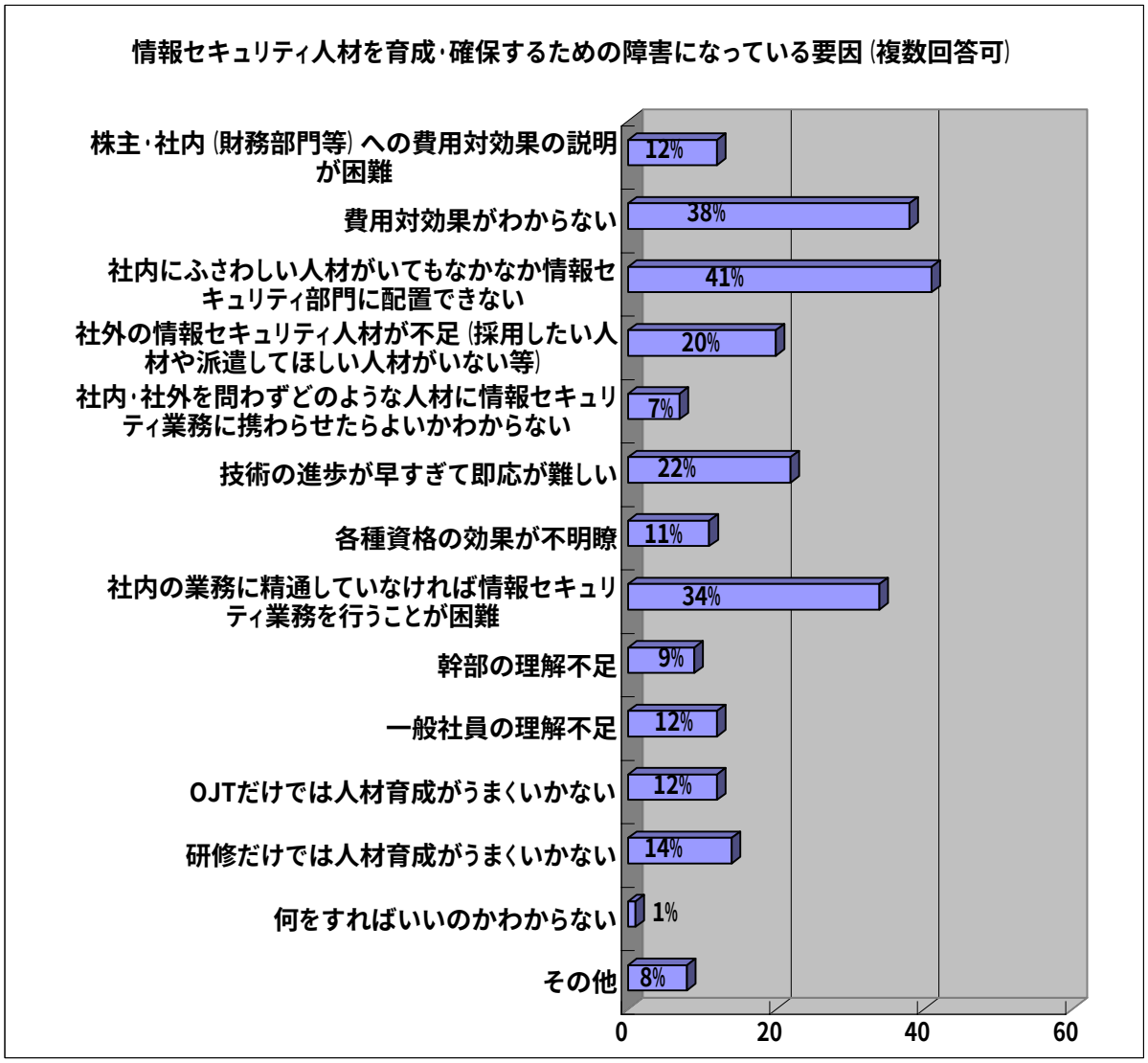
その他の回答内容
情報グループ会社を活用する
専門知識を持った人の社外からの調達
新卒採用者を育成していく
未定



Q33　情報セキュリティ人材を育成･確保するための障害になっていると思われる要因を以下から選んで下さい。(複数回答可)

	選択肢	%	回答数
1	株主･社内 (財務部門等) への費用対効果の説明が困難	12	9
2	費用対効果がわからない	38	29
3	社内にふさわしい人材がいてもなかなか情報セキュリティ部門に配置できない	41	31
4	社外の情報セキュリティ人材が不足 (採用したい人材や派遣してほしい人材がいない等)	20	15
5	社内･社外を問わずどのような人材に情報セキュリティ業務に携わらせたらよいかわからな	7	5
6	技術の進歩が早すぎて即応が難しい	22	17
7	各種資格の効果が不明瞭	11	8
8	社内の業務に精通していなければ情報セキュリティ業務を行うことが困難	34	26
9	幹部の理解不足	9	7
10	一般社員の理解不足	12	9
11	OJTだけでは人材育成がうまくいかない	12	9
12	研修だけでは人材育成がうまくいかない	14	11
13	何をすればいいのかわからない	1	1
14	その他	8	6

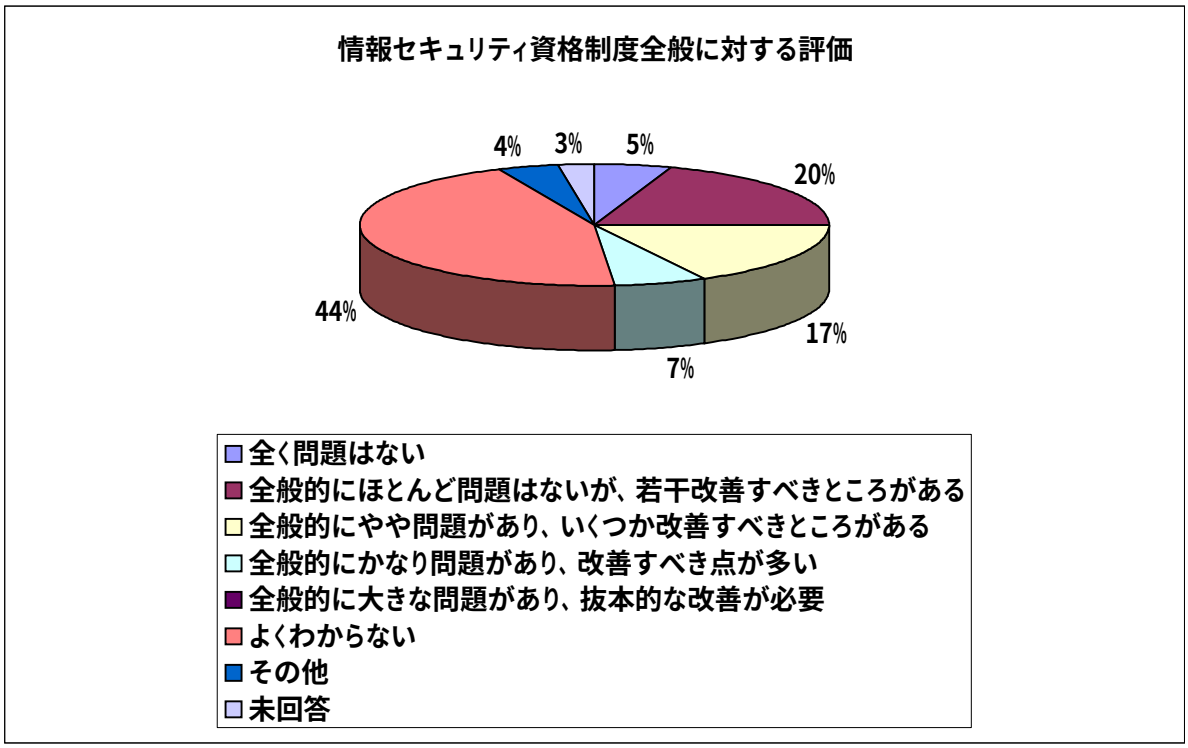
その他の回答内容
全社的に慢性的な人手不足
情報セキュリティ人材のキャリアパスが不明確
育成対象者の目標設定まで落とし込めていない
役割定義が明示できていない



Q34　現在提供されている、各種の情報セキュリティ資格制度全般に対する評価を以下から選んで下さい。

	選択肢	回答数
1	全く問題はない	4
2	全般的にほとんど問題はないが、若干改善すべきところがある	15
3	全般的にやや問題があり、いくつか改善すべきところがある	13
4	全般的にかなり問題があり、改善すべき点が多い	5
5	全般的に大きな問題があり、抜本的な改善が必要	0
6	よくわからない	34
7	その他	3
	未回答	2

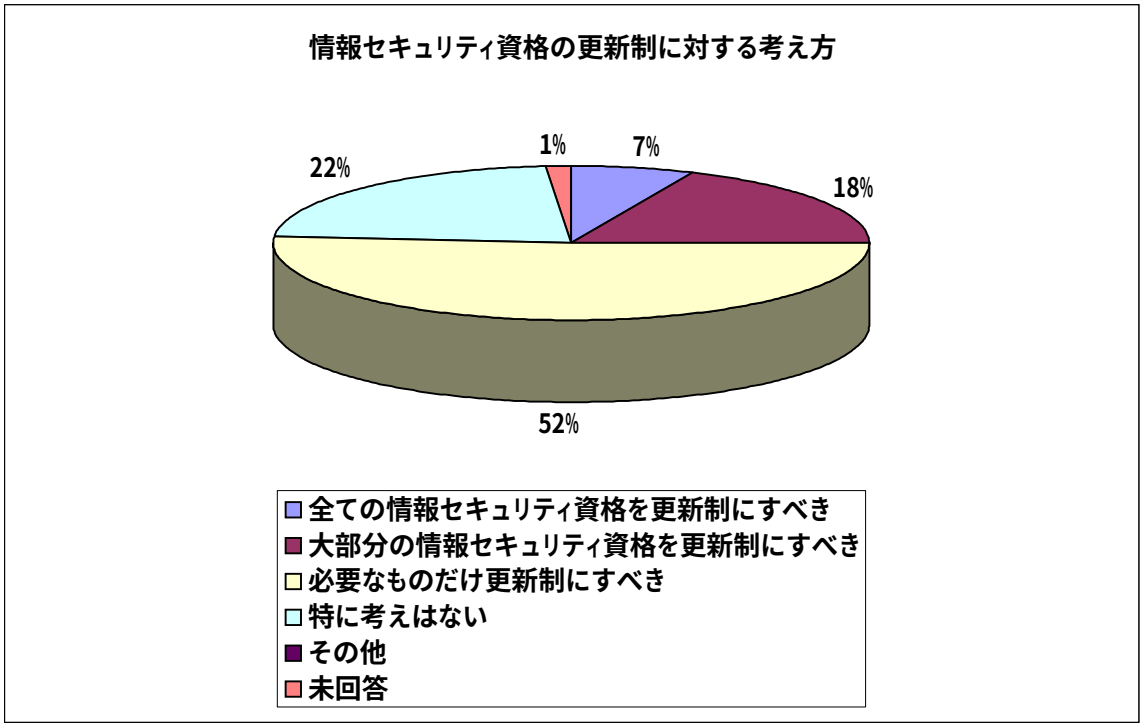
その他の回答内容
資格にこだわっていない
資格はあまり役に立ってないと思う
資格のための資格になっている



Q36 情報セキュリティ資格の更新制に対する考え方を以下から選んで下さい。

	選択肢	回答数
1	全ての情報セキュリティ資格を更新制にすべき	5
2	大部分の情報セキュリティ資格を更新制にすべき	14
3	必要なものだけ更新制にすべき	39
4	特に考えはない	17
5	その他	0
	未回答	1

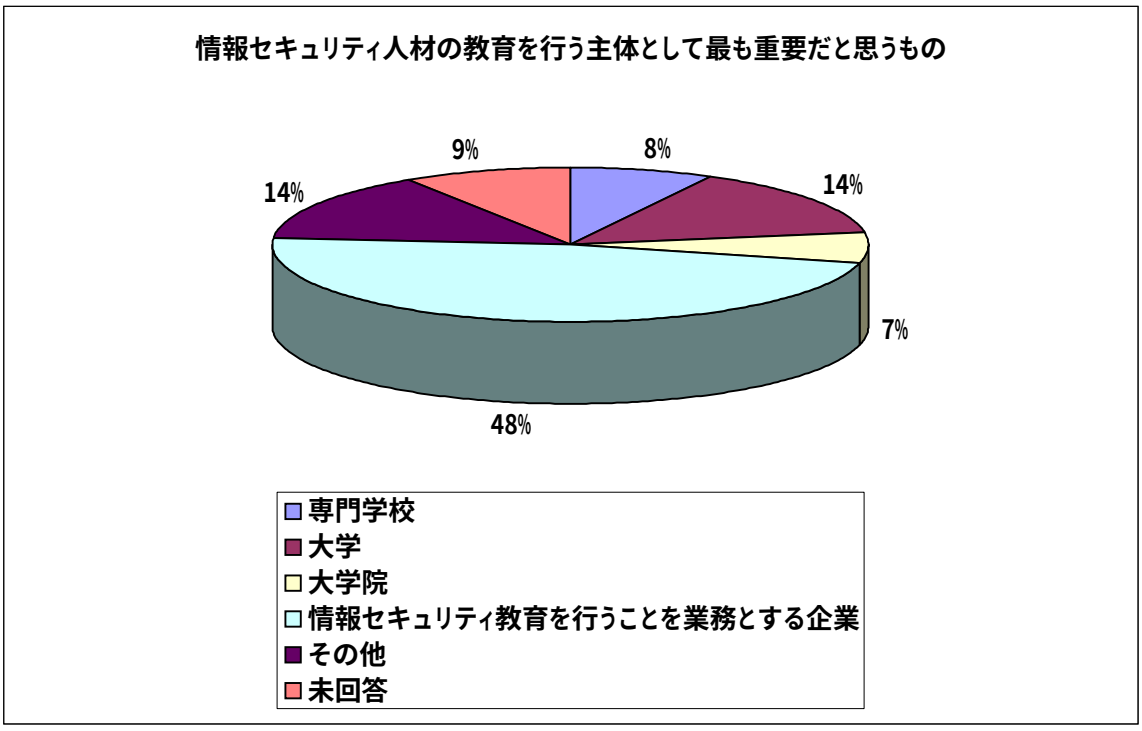
その他の回答内容



Q38 情報セキュリティ人材の教育を行う主体として最も重要だと思うものを以下から選んで下さい。

	選択肢	回答数
1	専門学校	6
2	大学	11
3	大学院	5
4	情報セキュリティ教育を行うことを業務とする企業	36
5	その他	11
	未回答	7

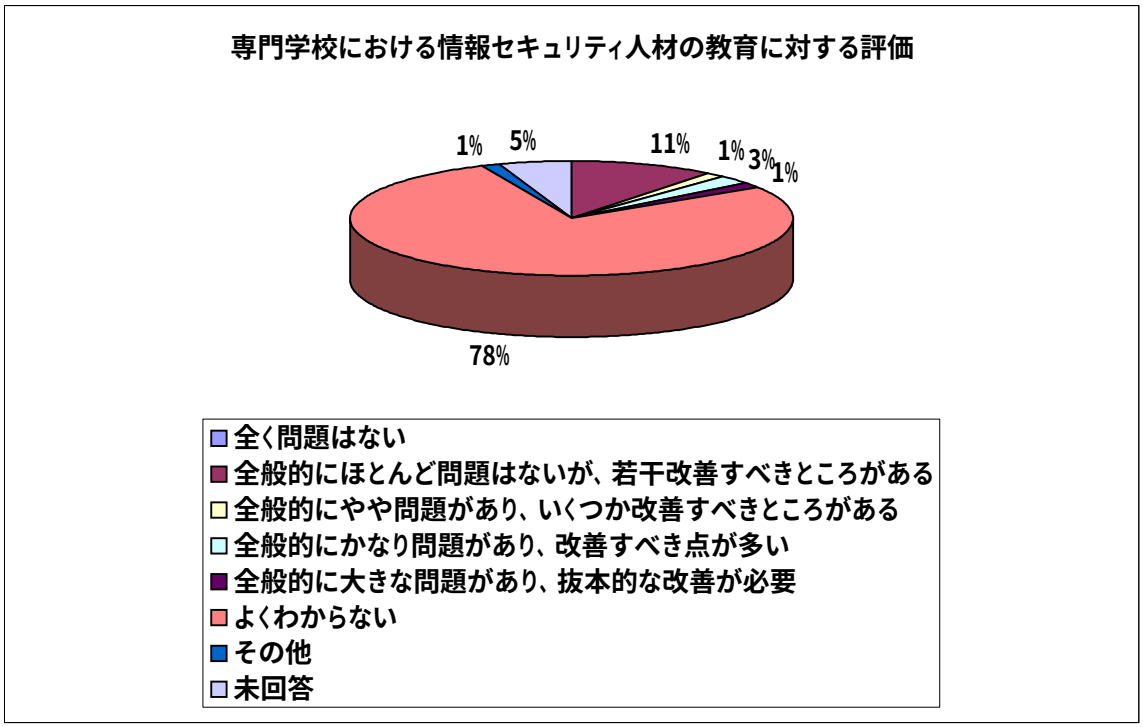
その他の回答内容
公的機関
大学で基礎、企業で実務
中学･高校
大学、企業の両者
専門学校、大学の両者
専門学校、企業の両者
種々の媒体があってよい



Q39　専門学校における情報セキュリティ人材の教育に対する評価を以下から選んで下さい。

	選択肢	回答数
1	全く問題はない	0
2	全般的にほとんど問題はないが、若干改善すべきところがある	8
3	全般的にやや問題があり、いくつか改善すべきところがある	1
4	全般的にかなり問題があり、改善すべき点が多い	2
5	全般的に大きな問題があり、抜本的な改善が必要	1
6	よくわからない	59
7	その他	1
	未回答	4

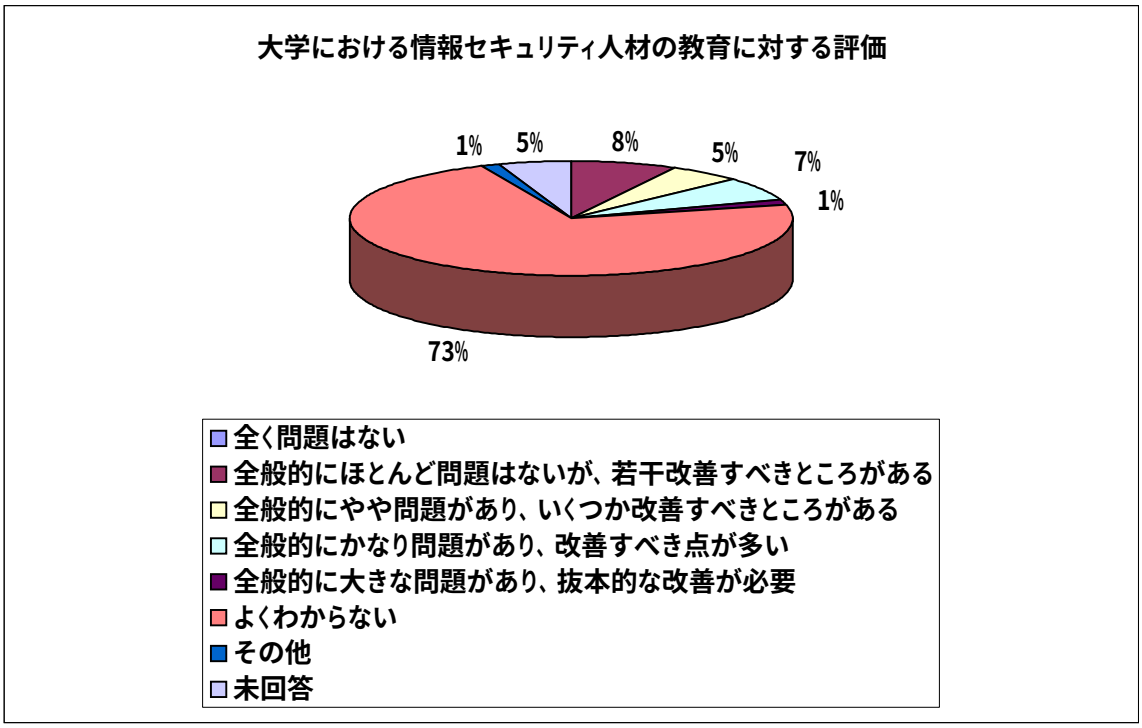
その他の回答内容
　まだ評価に値しないレベル



Q41　大学における情報セキュリティ人材の教育に対する評価を以下から選んで下さい。

	選択肢	回答数
1	全く問題はない	0
2	全般的にほとんど問題はないが、若干改善すべきところがある	6
3	全般的にやや問題があり、いくつか改善すべきところがある	4
4	全般的にかなり問題があり、改善すべき点が多い	5
5	全般的に大きな問題があり、抜本的な改善が必要	1
6	よくわからない	55
7	その他	1
	未回答	4

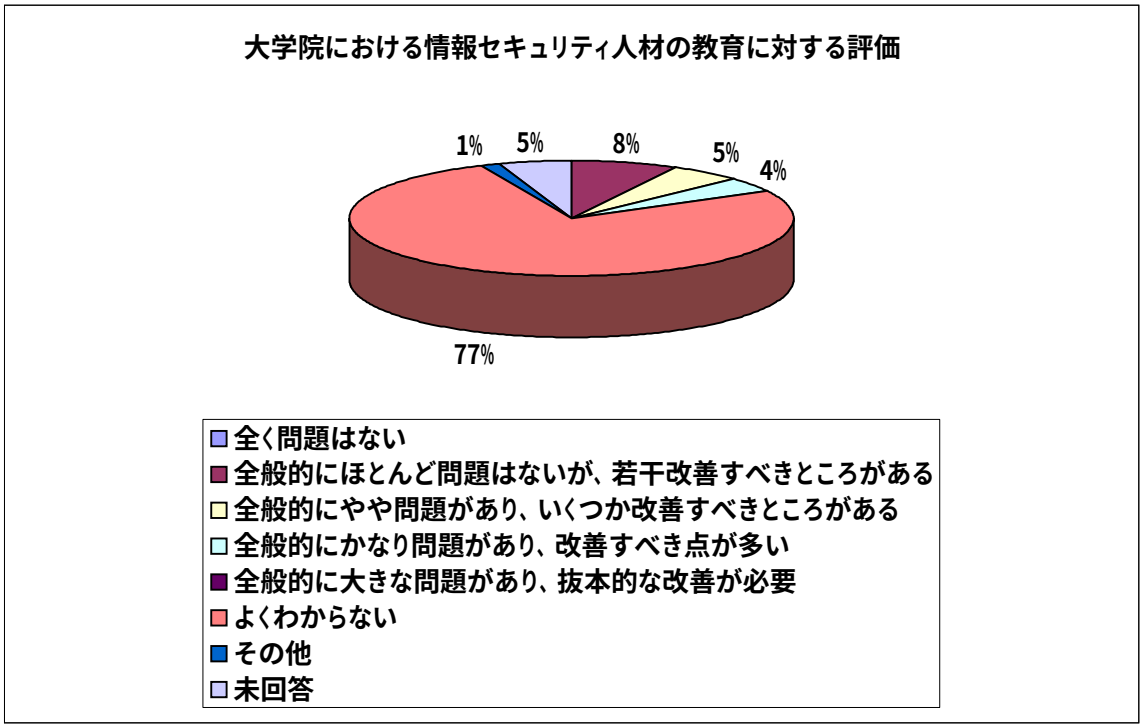
その他の回答内容
　どのような取組みがなされているのか不明



Q43　大学院における情報セキュリティ人材の教育に対する評価を以下から選んで下さい。

	選択肢	回答数
1	全く問題はない	0
2	全般的にほとんど問題はないが、若干改善すべきところがある	6
3	全般的にやや問題があり、いくつか改善すべきところがある	4
4	全般的にかなり問題があり、改善すべき点が多い	3
5	全般的に大きな問題があり、抜本的な改善が必要	0
6	よくわからない	58
7	その他	1
	未回答	4

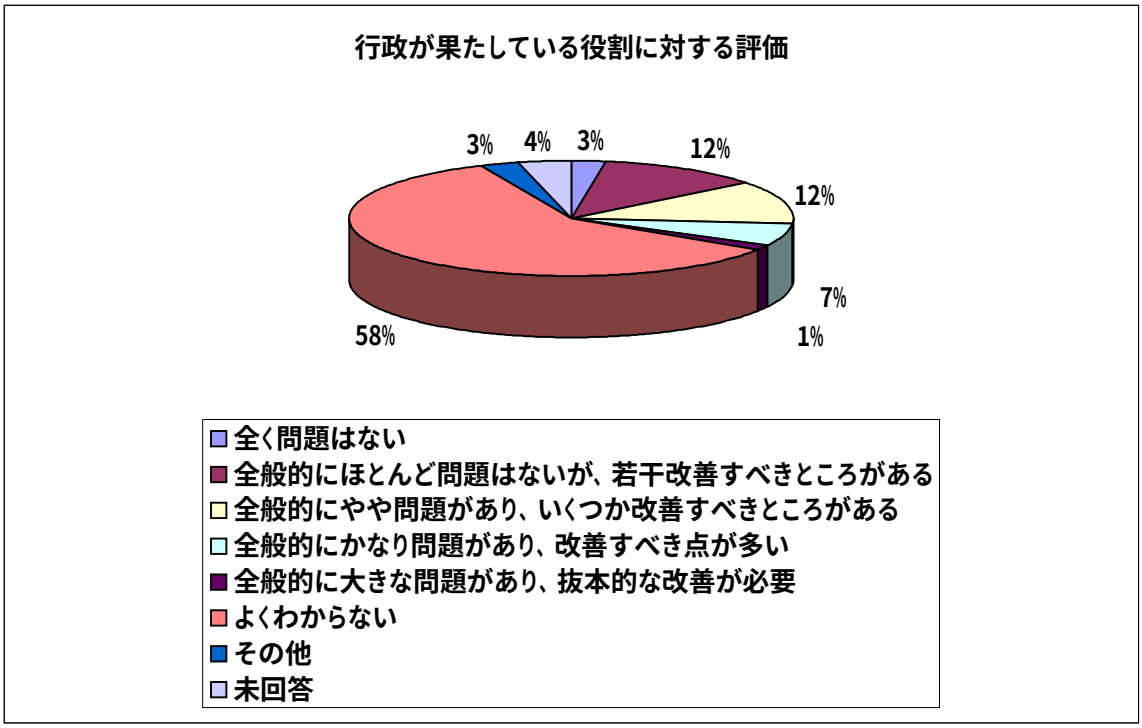
その他の回答内容
　どのような取組みがなされているのか不明



Q45　情報セキュリティ人材の育成･確保について行政が果たしている役割に対する評価を以下から選んで下さい

	選択肢	回答数
1	全く問題はない	2
2	全般的にほとんど問題はないが、若干改善すべきところがある	9
3	全般的にやや問題があり、いくつか改善すべきところがある	9
4	全般的にかなり問題があり、改善すべき点が多い	5
5	全般的に大きな問題があり、抜本的な改善が必要	1
6	よくわからない	45
7	その他	2
	未回答	3

その他の回答内容
民間が必要に応じて取り組めばよく、行政が出て行く必要はない。
資格制度を設けている点で評価できる



記述式回答部分の結果

Ｑ３１　今後確保したい必要な情報セキュリティ人材のイメージを教えて下さい。

＜回答概要＞

情報セキュリティマネジメントに関する能力を持つ人材に関する解答が非常に多かった。これは、Ｑ３０において社内で不足している人材の分野又は能力として情報セキュリティマネジメントが最も多く挙げられたこととも一致する。

その他には、社内業務への適応や法制度等幅広い知識への対応に関する回答が多かった。

Ｑ３５　情報セキュリティ資格全般について改善すべき点を教えて下さい。

＜回答概要＞

資格制度の乱立・重複等についての回答と、実務との乖離についての回答が多かった。

Ｑ３７　現存の個別の情報セキュリティ資格で役に立たないと思うものや改善が必要だと思うものがあれば、具体的資格の名称と改善すべき点を教えて下さい。

Ｑ４０　専門学校における情報セキュリティ人材教育について改善すべき点を教えて下さい。

Ｑ４２　大学における情報セキュリティ人材教育について改善すべき点を教えて下さい。

Ｑ４４　大学院における情報セキュリティ人材教育について改善すべき点を教えて下さい。

＜回答概要＞

これらについては、それほど回答がなかった。これらに関する選択式の回答では、改善すべき点があるという趣旨の回答がいくらか見られたが、それ以上に「よく分からない」という回答が多く、企業の担当者が、個別の資格及び教育機関ついてあまり意識していないことがうかがえた。

Ｑ４６　情報セキュリティ人材の育成・確保に関して行政が果たしている役割について改善すべき点を教えて下さい。

＜回答概要＞

法制度・ガイドラインの整備に関する回答が多く、行政に対しては、そのような役割が求められているということがうかがえる。

Ｑ４７　その他、企業における情報セキュリティ対策の現場の立場から見た情報セキュリティ人材の育成・確保に対しての提言、要望、参考となる事項等ありましたら教えて下さい。

＜回答概要＞

ベストプラクティス、ガイドライン等の整備に関する要望がいくつか見られた。また、公的機関、教育機関、資格制度に関する回答もいくつか見られ、それぞれが取組む必要があることがわかった。

Ｑ３１　今後確保したい情報セキュリティ人材のイメージ

＜マネジメント能力を有する人材を求める回答

○　情報セキュリティマネジメントについての専門家
　①設計、構築、運用等の技術に関わる専門家
　②教育、推進等の管理に関わる専門家

○　セキュリティ技術の知識を有し、情報セキュリティマネジメントの企画・実行・推進ができる人材

○　人材はマネジメントに専門化した人材と、セキュリティに関する各種の技術に特化した人材の、スキルの２極化が進むと思われる。

○　技術・法制度全般にわたって情報セキュリティ全体を掌握できた上で業務プロセス改革のＰＤＣＡサイクルを回すことができる人材

○　情報セキュリティ施策の立案、社内への展開・監査業務を行うことができる人材

○　情報セキュリティマネジメントにおいて、グローバルに統一のとれた活動を推進できる人材

○　情報セキュリティ管理のＰＤＣＡサイクル運用を推進していく人材

○　セキュリティに対する制度的知識を基本要件として具備し、その上で、現場の状況、運用実態を理解して、実効のある施策を展開していける人材

○　情報セキュリティマネジメント分野と技術的セキュリティ分野（アクセスコントロール、ネットワークセキュリティ、アプリケーションセキュリティ等）の両方に精通した人材

○　的確なリスクマネジメントを行い、それによって得られる優先順位に従って、限られた社内資産をリスク回避への投資と分配する眼を持つ人材

○　情報セキュリティマネジメントのできる人材

○　ＩＴ、内部統制を理解できる人材

＜社内業務への適応力を有する人材を求める回答＞

○　当社業務の特性にマッチした対応策を企画・実行できる人材

○　情報セキュリティ専門知識より、社内業務への適切な適用を判断できる人材を社内に育成したい

○　事業特性を考慮したリスク分析ができる人材

○　事業規模・目的に合ったセキュリティ対策の立案・実施ができる人材

○　適用対象業務並びにそこへの適用に際しての問題点を理解することができ、バランス感を持った解決策の提示・推進を行うことができる人材

○　自社にとって適切なＩＴ技術の評価・選択ができる人材

○　リスク分析ができ、コストを意識しつつ有効な施策を考え、社内に効果的効率的に施策を展開できる人材

○　組織における調整能力の高い人材

○　情報セキュリティ関連の新技術を理解でき、関連法令、社内ルールに詳しく、これらを分かりやすく説明するための資料作成能力及び説明・相談のためのコミュニケーション能力を持った人材

＜法制度に関する知識を有する人材を求める回答＞

○　最新の法令・社会の動向・技術動向を見据えて、セキュリティポリシーの実施手順の見直しを行うことができる人材

○　今後、情報セキュリティ関連の法制度が整備されてくることに対応し、法律や条令への対応ができる知識を持った人材。

○　広範囲で正確な知識（法務）を持ち、システム開発やＮＷ設定の経験を持つ人材

○　情報システムと法務の両方の知識・経験がある人材

○　法制度、様々な基準類を理解しかつ社内の情報システムを理解できる人材。または、これらの知識が万全でなくとも、危機管理意識が高く、複眼思考で質問力が高くかつ全体を俯瞰する力のある人材

○　情報セキュリティ関連の新技術を理解でき、関連法令、社内ルールに詳しく、これらを分かりやすく説明するための資料作成能力及び説明・相談のためのコミュニケーション能力を持った人材（再掲）

＜情報セキュリティ技術を有する人材を求める回答＞

○　情報セキュリティに関する専門技術的なスキルを有し、実際の作業を遂行することができる人材

○　情報セキュリティ技術全般をバランス良く取得した人材

○　テクニカルな分野に精通している人材

○　ＩＳＭＳ、ＩＴＩＬに準拠したノウハウで構築された環境をサービスとして利用することを前提として評価・設計ができる人材

○　データ削除の痕跡の調査を行うことができる能力を保有する人材

○　人材はマネジメントに専門化した人材と、セキュリティに関する各種の技術に特化した人材の、スキルの２極化が進むと思われる。（再掲）

＜グローバルな対応力を有する人材を求める回答＞

○　英語ができる人材

○　グローバル対応できる人材

○　海外拠点の情報セキュリティ対策を任せられる人材

＜その他の回答＞

○　事業戦略と技術戦略両面からセキュリティを検討することができる人材

○　情報セキュリティのみに特化はしないものの、情報システム全般を理解し、かつ、経営や業務についても精通している人材

○　役員クラスの人材

○　セキュリティに関する問題点把握と対処方法提言の能力を有する人材

○　業務そのものは外注するので、委託先と調整できるレベルの総合的知識を有する人材

○　技術的な専門性は必要に応じ外部専門家を活用することを前提として、社内には、それらを評価し、全社展開を企画できる人材

○　企業内の情報セキュリティニーズ・優先度と外部の脅威を把握し、バランス良い施策をタイムリーに実施できる人材。

○　ビジネスニーズを理解できる人材

○　少人数による迅速な対応ができる人材

○　役所、役割に応じた情報セキュリティの知識・能力を社員各人が備えていること。

○　情報資産管理におけるリスク分析ができる人材

Ｑ３５　資格制度全般についての改善点

＜資格制度の乱立・重複等について指摘する回答＞

○　資格の種類が多すぎる。

○　資格制度がベンダーごとに乱立しているため、ＣＤＰに盛り込みにくい。例えば経済産業省制定のものなどに一本化した方が良い。

○　重複感がある。

○　多種の資格制度が乱立し、何が必要で適性かが不明確。体系の整備を望む。

○　各資格の適用範囲が問題。

○　似たような資格が多すぎる。

○　主務官庁が複数にまたがっているためか、公的資格の付与機関が多すぎる。

○　資格制度が乱立し、どれを選択すれば良いのかわかりにくい。技術系、マネジメント系各分野別に整理が必要。

＜実務との乖離について指摘する回答＞

○　業務実施資格との乖離、資格の効力の明確化。

○　学問の域を出ていない感がある。制度はツールとしては有効かもしれないが、社内における実行との間にはかなりの距離感がある。

○　総じてインフラ中心の情報セキュリティ認証のため、システム開発・保守領域・ＩＴ以外の情報セキュリティのノウハウを評価する仕組みが不足している。

○　「資格＝能力」とは必ずしもなっていない。資格をとったからといって仕事ができるとの納得感が必ずしも得られない。即ち、実務に直接役立つものになっていない。

○　実践的な教育が不足している。

○　資格の持つ価値が定量的に見えない。基準に合ったサービスを認定するほうが現実的ではな

いか。

○　セキュリティ技術、法制度の知識を問うことが主になっているが、本来はサイバー攻撃から実際に守る実践力を問うべき。

＜その他の回答＞

○　全体的に維持更新が大変である。（時間的にも金銭的にも）

○　一般ユーザ企業として、技術の概要についての知識は必要であるが、より経営的観点から捉えるべき問題としていくべきである。

○　費用さえ出せば取得可能なものが多い。

○　技術面が重視されすぎ、システム環境やリソース関連への知識取得のモチベーションが低い。

Ｑ３７　個別資格についての改善点

○　ベンダー系の情報セキュリティ資格は、個別の要素技術に特化しすぎであり、国による資格に個別の要素技術も取り入れるなど一本化を図った方が良い。また、セキュリティ対策の実施者だけでなく、監査や内部統制の観点からモニタリングする視点も盛り込んだ方が良い。

○　全て。特にメーカー名のついた資格はメーカーの売上げの一部としかなってないと思われ、全く不要。

○　実態的にあまり意味のない継続教育要件が要求されている資格は見直した方が良い。

○　情報セキュリティ監査人は他の資格との重複感がある。

○　具体的資格名は挙げられないが、単にセキュリティ技術、法制度等の知識を問うだけだと役に立たない。

○　情報セキュリティ分野は技術的に日進月歩であり、有資格者のモチベーションが高ければまだしも、そのあたりを確認する為にも更新制など確認をしなければ、国ベースで必要な人材を育成出来ているか否かもわからない。

Ｑ４０　専門学校についての改善点

○　知識の教育に偏っている感があり、社内における実行との間にはかなりの距離感がある。

○　ツールの使い方が中心のところがあり、その場合、情報セキュリティの基本的考え方、本質の教育が不足している可能性がある。

Ｑ４２　大学についての改善点

○　理論や技術が中心となり、実践的なスキル、実践力が不足する可能性がある。社会に出てから磨くという考え方もあると思うが。

○　指導教授自身が、現場・実社会との距離感があるのではないかとの危惧がある。

○　大学の教育課程として情報セキュリティ教育が組み込まれているかが疑問。実践的な場面との乖離があるように思える。

○　学問に重点が置かれている点。

○　基礎から体系的な教育ができていない。

○　大学・大学院で育成すべき人材として、セキュリティ対策技術・ツールに詳しい者と、ＩＴ環境面からそれを如何に応用するかというコンプライアンス面も含めて詳しい者が必要だと思う。両面でのアプローチが少し弱いのではないか。

○　法的あるいは知的財産の観点もわかる人材の育成。

Ｑ４４　大学院についての改善点

○　教育内容が情報技術に偏重している気がする。会社の中で情報セキュリティを保つためには、様々な業務改革を自ら推進していく能力が問われるが、そういった面の教育が手薄だと思う。

○　実践面との乖離があるように思える。

○　学問に重点が置かれている点。

○　一般の大学院でセキュリティ人材にフォーカスした教育が少ない。

○　コースそのものが少ないと思う。また、教えることが出来る人材も少ないのではと思う。

Ｑ４６　行政の役割についての改善点

＜法制度・フレームワーク・ガイドライン等の整備に関する回答＞

○　人材育成のフレームワークの明確化

○　人材育成等を含めた情報セキュリティ対策における行政としての方針を法制化することにより、国としての役割をより明確にすべきである。

○　資格制度の体系整理と企業として何が必要かのガイドライン整備を望む。

○　企業や団体が備えるべきセキュリティレベルとして、企業規模や業種別に、分野や必要人員数等、ある程度の指針を示していただきたい。

○　ベンダーサイドとユーザサイドに分け、ユーザ企業として必要な人材育成カリキュラムを整備して欲しい。

○　情報技術の開示・普及について一層の改善が必要と思われる。その上で、一般企業（中小～大企業まで）において、何処まで施すべきなのかといったガイドラインを徹底して欲しい。

＜その他の回答＞

○　情報セキュリティ施策の重要性について、社会的認識をより高めてもらうことで、人材の育成・確保の重要性が高まると考える。

○　資格、制度の整備だけでなく、情報セキュリティの必要性を社会に認識させ、それを担う人材の社会的地位を上げる施策の強化が必要だと思う。

○　資格制度は整備されているが、他に実務経験者の大学受入支援制度の導入が望まれる。

○　情報セキュリティ確保の必要性の積極的な広報及び資格制度のみならず、実践に即した人材育成のための教育やその費用の助成をお願いしたい。

○　実務に役立つ資格とすること。（作業スキルレベルの資格、プランニングあるいはコンサルティングレベルの資格のいずれも）

○　学校、企業、社会に対して、積極的に指導、支援、補助等を行うべきである。

○　情報セキュリティ人材として、ＩＳＯ１５４０８のようにセキュリティ対策技術の専門家と、いかにツールを応用・適用するかという２種類があると思う。Ｗｉｎｎｙを使わないようにという国からの指導は、後者になると考えるが、両面での一層の指導・提言をお願いする。

○　公的資格の設立は意味がないのではないか。

○　各省庁の役割を一本化して欲しい。（経済産業省、内閣官房など）

Ｑ４７　その他要望等

＜ベストプラクティス・ガイドライン・法制度の整備等に関する回答＞

○　米国 SOX 法など内外の法制度に則した、タイムリーかつ実効的な政策を期待する。

○　今後出てくる日本版ＳＯＸ法やシステム監査基準と、情報セキュリティとの整合性をとったガイドラインを出して欲しい。

○　ベンダーサイド、ユーザサイドの役割などを明確に区別したガイドラインを作って欲しい。

○　各省庁からのガイドラインが多すぎるので一本化して欲しい。
　例：個人情報保護法の経済産業省、総務省など

○　情報セキュリティに関する法制度の拡充

○　人材育成の前に、情報セキュリティ確保に関する具体的基準やベストプラクティスを整備する必要がある。

○　各企業（海外含め）で発生している事件・事故の事例を原因と対策を含め開示して欲しい。

＜公的機関による支援等に関する回答＞

○　情報セキュリティの現場は、技術動向の変化、新たな脅威の出現のスピードが早く、知識・経験がすぐに陳腐化する。そのため、制度的技術確保のための制度的支援を希望する。

○　国内全体のセキュリティレベルを底上げするという方針に沿い、企業への人材育成のための助成金制度等、具体的な施策が必要。

○　補助金制度

○　不正アクセスやサイバーテロなどを仕掛けてくる側の技術、情報、ツールなどのレベルが上がってきており、守る側の対応が追いつかない状況になっている。
　各企業が独自に対応するのではなく、効果的で実用的な対応技術やその適用に必要な人材を公的機関が育成する制度が望まれる。

＜教育機関による取組みに関する回答＞

○　専門学校・大学・大学院の人材教育が、会社で役に立つものとはとうてい思えない。ほとんどの場合、再教育が必要。一般的な知識としては意味があるのかもしれない。とにかく、現在は「セキュリティ」をキーワードとして儲け主義的な活動が世の中に溢れているので、そういったものを一度掃除して欲しい。

○　企業のおける情報セキュリティ人材は不足しており、入社する以前にある程度のセキュリティに関する知識・常識を身につけるよう、高校～大学のカリキュラムに組み込む等の施策を進めていただきたい。

○　企業により対応の力の入れ具合が異なる。学生のときからカリキュラムに取り入れるべき。

○　昨年より自宅パソコンからＷｉｎｎｙなどのファイル交換ソフトを悪用したウイルスにより個人情報や機密情報等の漏洩事件が多発している。特に学生の利用により被害が拡大している。

　情報を活用する者として最低限の知識や意識付けが必要であるため、事件概要・問題点、防衛策などを題材とした授業を中学又は高校で教育するようにしてセキュリティレベルの底上げをして欲しい。

＜資格制度に関する回答＞

○　資格の効果がわかるような第三者評価が欲しい。

○　企業における育成体制及び公的な資格制度を適切に組み合わせ、その成果（結果）が評価に結びつくよう、推進することが重要。

＜その他の回答＞

○　情報セキュリティ対策は情報システムの立場からだけで実現するものではない。企業内の監査業務、法務業務等と密接に関係する必要がある。

　セキュリティの技術とルールの実行を確保する体制や権限との整合のとれた組織作りを担える人材の育成・確保が重要である。

○　ビジネスを遂行する上でパートナー（協力会社）との連携が必須であり、パートナーの情報セキュリティも高める必要がある。中小・零細企業では人材を独自に育成することはかなり厳しい。発注元として各社が諸施策を打っていると思うが、そういう企業へのセキュリティ対策

をサポートする人材や組織の整備が必要ではないだろうか。

○　情報セキュリティだけしかできない人材は価値が低い。
　業務改革、システム改革ができた上で、情報セキュリティもできる人を育てる工夫が必要。

○　セキュリティ責任者の社会的地位向上等、魅力ある職業としての位置づけをつくる企業を超えた社会全体の活動が必要。

○　実際のセキュリティ対策では、リスクの大きさ、対策コスト、利便性の低下等、複数の要素を考慮して、現実的な施策を実施していく必要がある。そのため情報セキュリティ人材には、法制度や各種基準類の理解とシステム開発・運用に関する知識を広範囲にバランスよく習得することが求められる。
　また、情報セキュリティ対策は、トップから現場職員に至る全ての社員が危機管理意識、それを支えるモラルとモチベーションを持てるようになることが最も重要。

○　予防（防止）策を有効なものとするための十分な要員の配置が確保される必要がある。

○　日本全体に言えることだと思うが、ＩＴは仕事や生活を充実させていくためのツールのひとつであり、仕事上ではそろばんや電卓と同様に利用する人次第であるという主体的認識が薄いと感じる。若い世代はわからないが、特に中高年に「専門家がやってくれるもの」という意識が強く、結果として、情報セキュリティの意識についても主体性がない。時節柄、重要なものという認識はあるだろうが、社会のルールだから守るという受身の意識である。その様な意識の持ち主は主体的ではないので、責任感もなく、何かあれば専門家の責任とする傾向にある。情報セキュリティの管理責任者は日々この様な壁と戦っている。一個人としての主体性がないのは国民性なのか。国やマスコミ、知識人にこの様な風土を変えていく努力を期待する。

○　セキュリティ脅威は企業毎に異なるものではないと思う。国と産業界が協力して、情報共有・共通対応をしていくことが効率的と考える。

○　広く海外の知識・技術等を常に取り入れ、活用していけるような人材の育成を期待する。

アンケート結果の分析（1）

従業員数とIT業務担当社員の有無の状況

	専任者がいる		兼任者しかいない		IT業務担当社員がいない 若しくは 無回答
	正社員の専任者がいる	正社員以外の専任者しかいない	正社員の兼任者がいる	正社員以外の兼任者しかいない	
大規模 （5000人以上規模）	22社 (56%)	0	12社 (31%)	0	5社 (13%)
中規模 （1000人以上規模）	19社 (76%)	0	4社 (16%)	0	2社 （8%）
小規模 （1000人未満規模）	8社 (67%)	2社 (17%)	2社 （17%）	0	0

アンケート結果の分析（2）

従業員数と情報セキュリティ担当社員の有無の状況

	専任者がいる		兼任者しかいない		情報セキュリティ担当社員がいない若しくは無回答
	正社員の専任者がいる	正社員以外の専任者しかいない	正社員の兼任者がいる	正社員以外の兼任者しかいない	
大規模（5000人以上規模）	22社 (56%)	0	10社 (26%)	1社 (3%)	6社 (15%)
中規模（1000人以上規模）	9社 (36%)	0	14社 (56%)	0	2社 (8%)
小規模（1000人未満規模）	5社 (42%)	1社 (8%)	5社 (42%)	0	1社 (8%)

アンケート結果の分析（3）

従業員数と情報セキュリティ担当社員資格の取得の有無の状況

	正社員に情報セキュリティ資格取得者がいる	正社員以外にのみ情報セキュリティ資格取得者がいる	情報セキュリティ資格取得者がいない若しくは未回答
大規模（5000人以上規模）	17社 (43%)	2社 (5%)	20社 (51%)
中規模（1000人以上規模）	7社 (28%)	1社 (4%)	17社 (68%)
小規模（1000人未満規模）	4社 (33%)	0	8社 (67%)