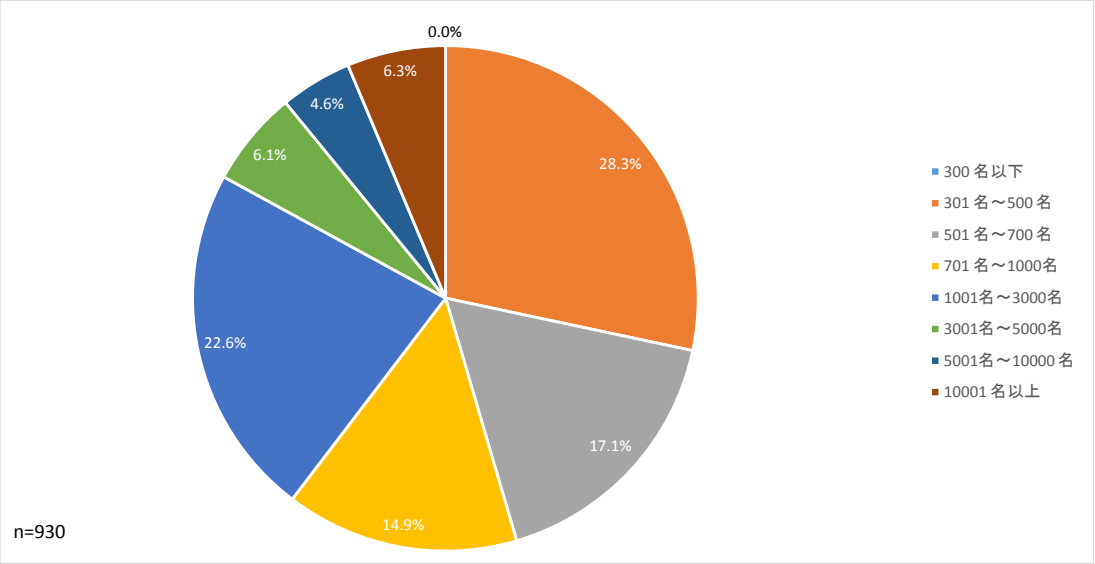
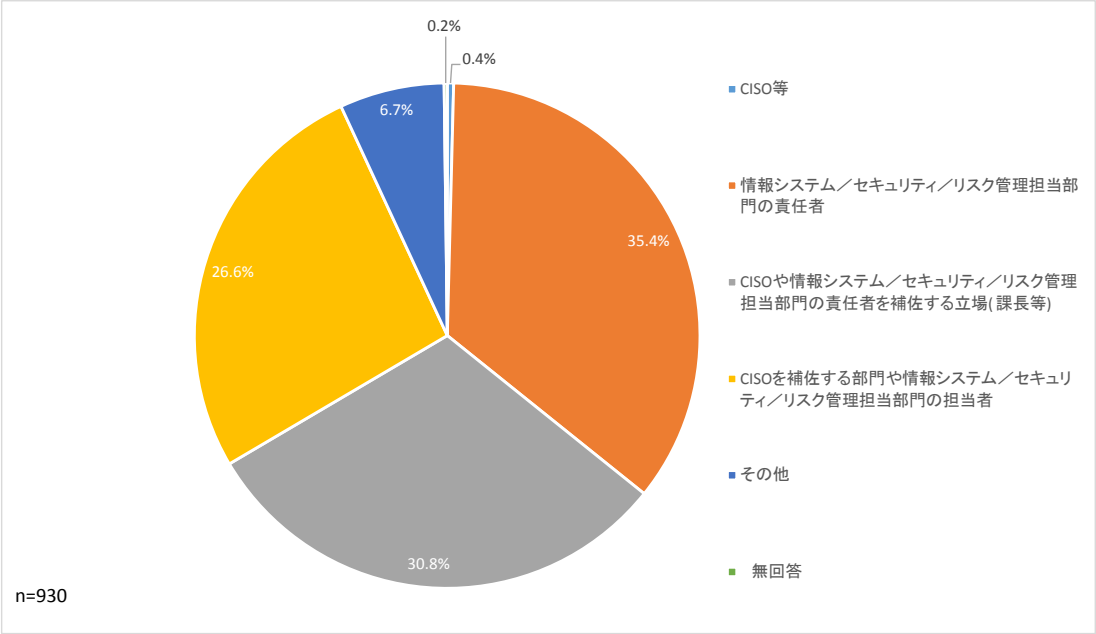
別冊資料　アンケート調査結果 単純集計

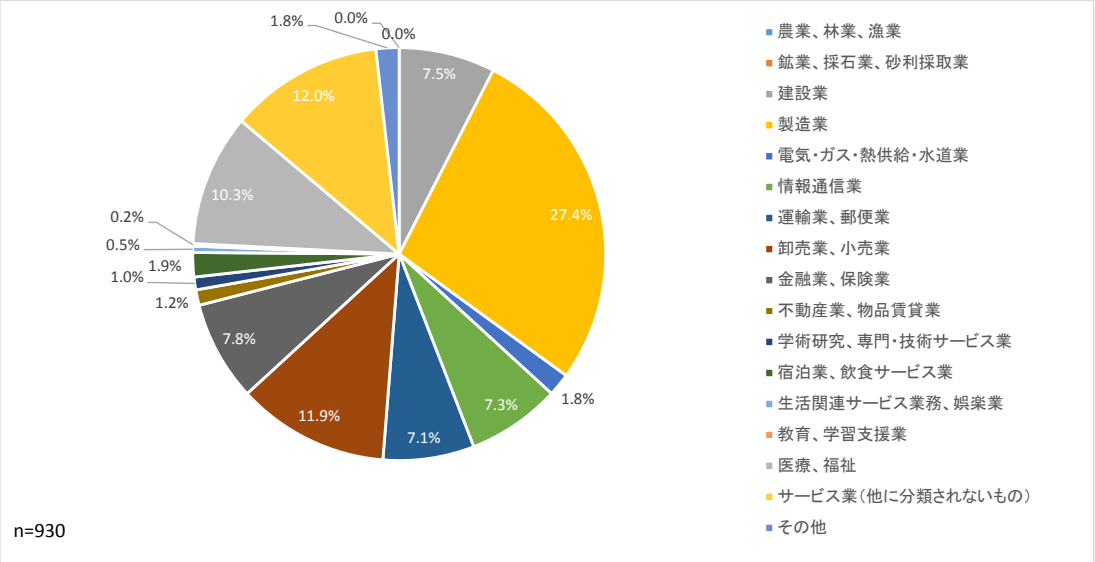
Q1. 総従業員数（有給役員,正社員・正職員,準社員・準職員,アルバイト等を含む）についてお聞きします。
直近の会計年度の人数を1つお選びください。（単一選択）



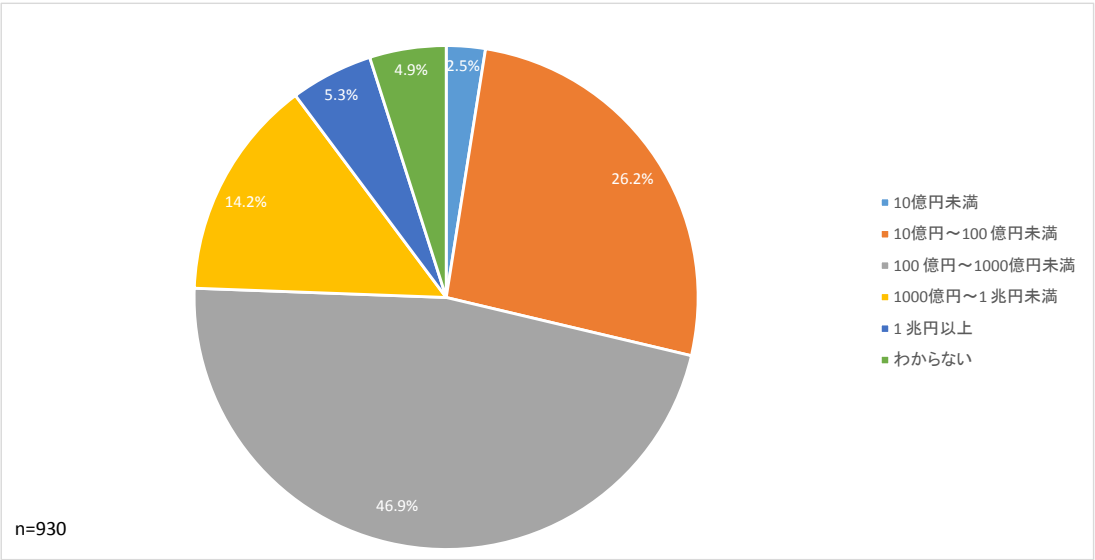
Q2.ご回答いただいている方ご自身の役職または立場として最も近いものを1つお選びください。（単一選択）



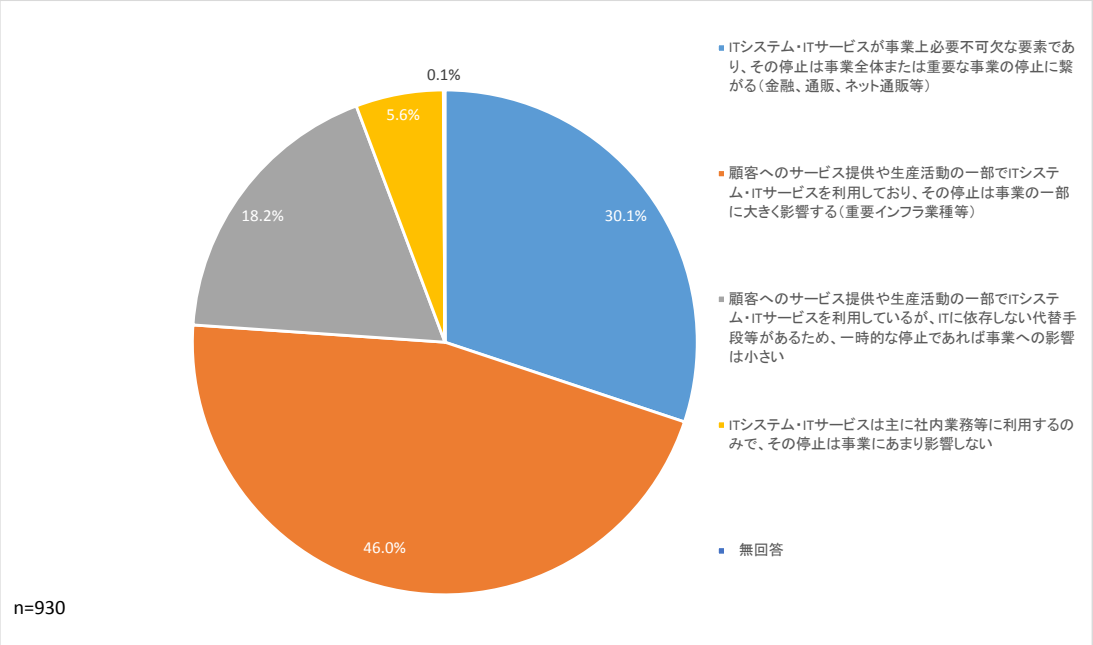
Q3. 貴社の業種*を1つお選びください。(単一選択) *日本標準産業分類に基づく



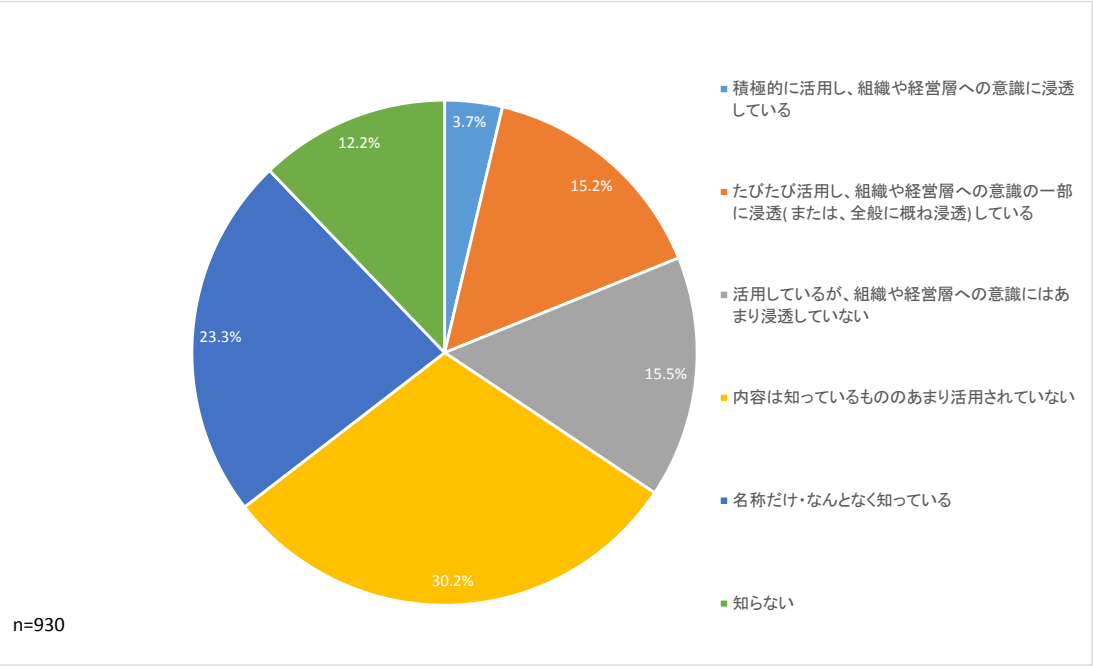
Q4. 直近の会計年度の総売上高を1つお選びください。(単一選択)



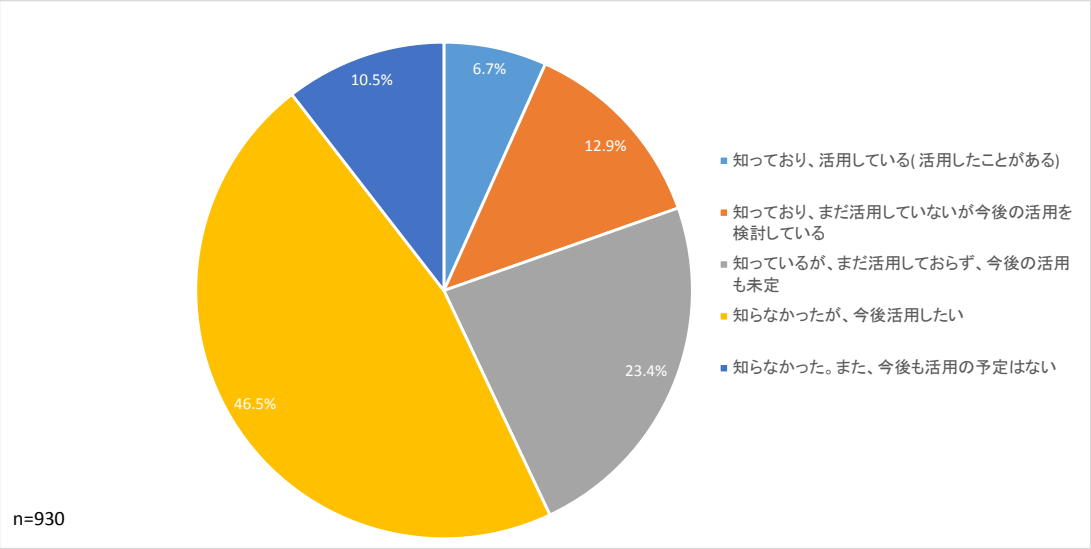
Q5. 事業のIT システム・IT サービスへの依存度について、最も近いものを1つお選びください。(単一選択)



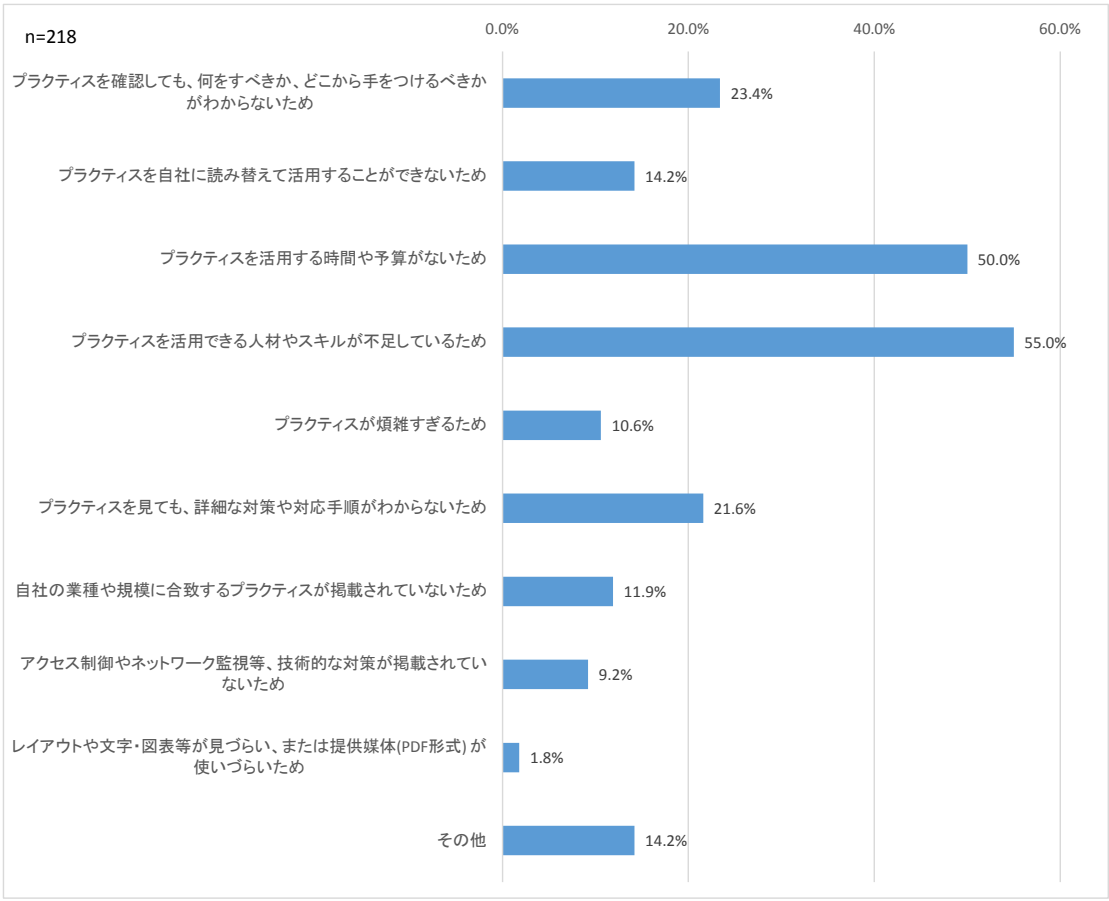
Q6. 経済産業省と独立行政法人情報処理推進機構(IPA)が2017年に策定した「サイバーセキュリティ経営ガイドラインVer2.0」を利活用していますか、もしくは知っていますか。当てはまるものを1つお選びください。(単一選択)



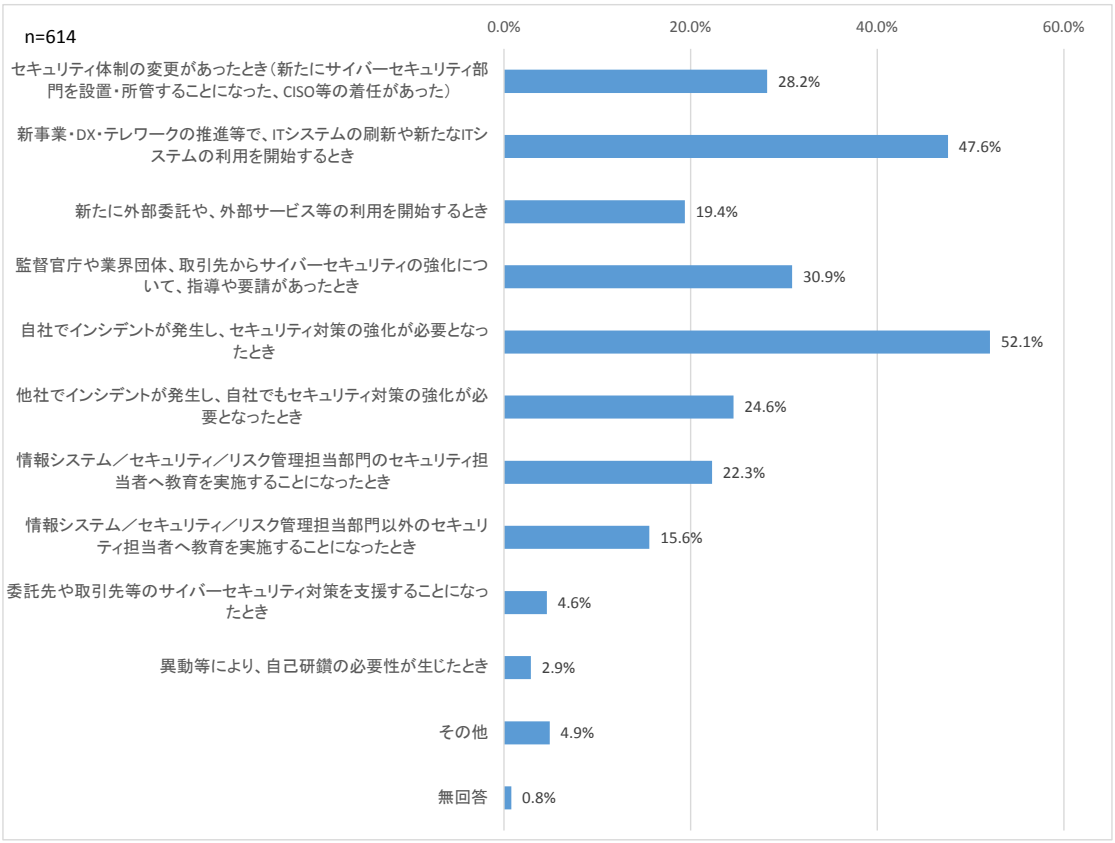
Q7.「経営ガイドライン実践のためのプラクティス集」を知っていましたか。また、これを利活用したことがありますか(今後活用したいと思いますか)。当てはまるものを1つお選びください。(単一選択)



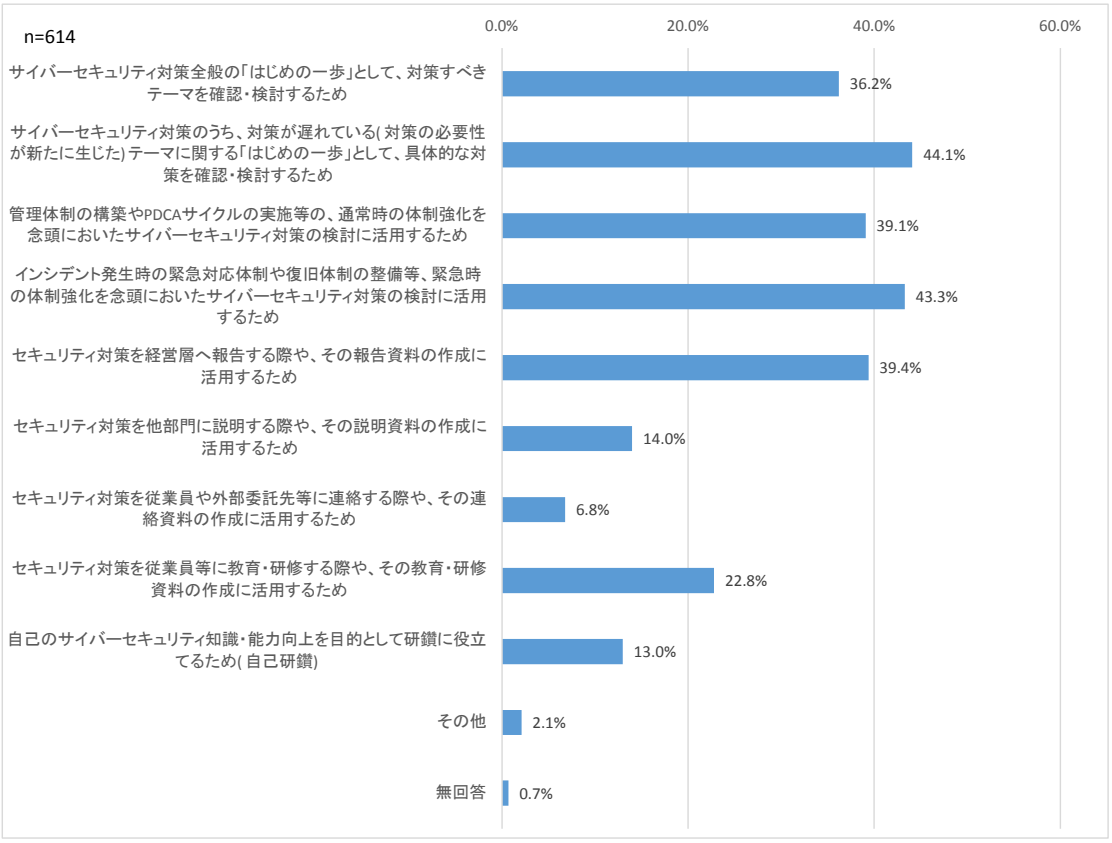
Q8.(Q7で(c)を選択した方に伺います)「経営ガイドライン実践のためのプラクティス集」を知っているが、まだ活用しておらず、今後の活用も未定である理由について、当てはまるものを最大3つまでお選びください。(複数選択可)



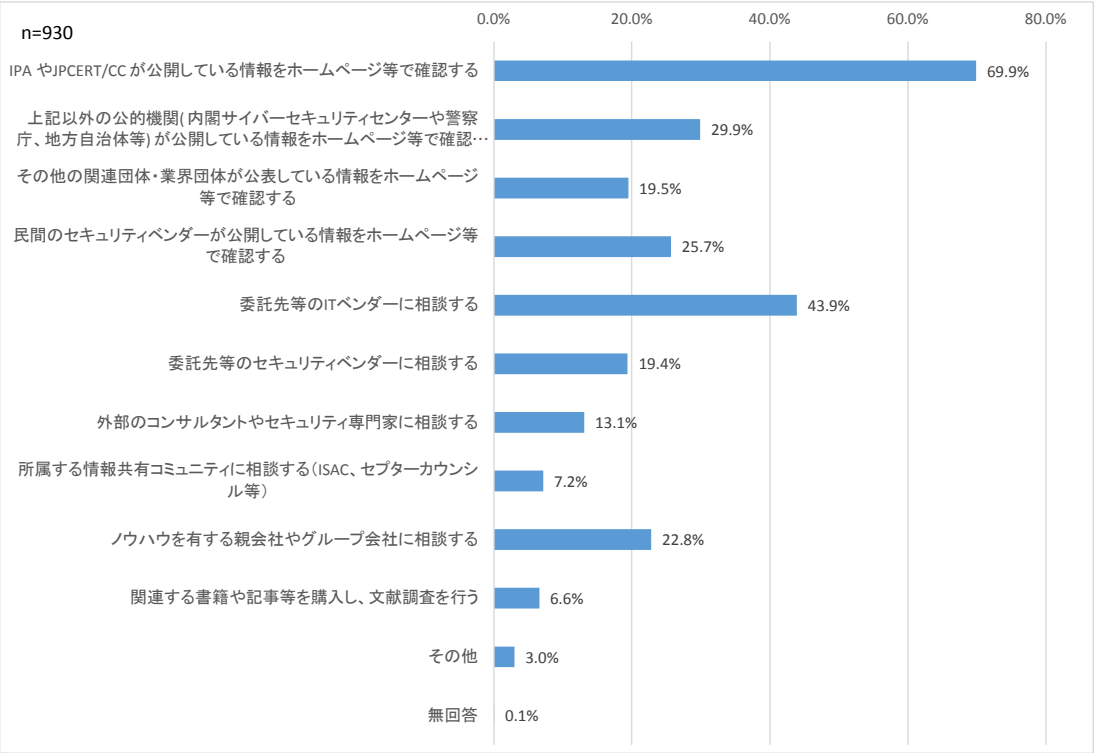
Q9. (Q7で(a)(b)(d)のいずれかを選択した方に伺います)「経営ガイドライン実践のためのプラクティス集」を活用するきっかけやタイミング(今後、活用するきっかけやタイミングとして想定されるもの)について、当てはまるものを最大3つまでお選びください。(3つまで複数選択可)



Q10. (Q7で(a)(b)(d)のいずれかを選択した方に伺います)「経営ガイドライン実践のためのプラクティス集」を活用する目的(今後、活用する目的として想定されるもの)について、当てはまるものを最大3つまでお選びください。(3つまで複数選択可)

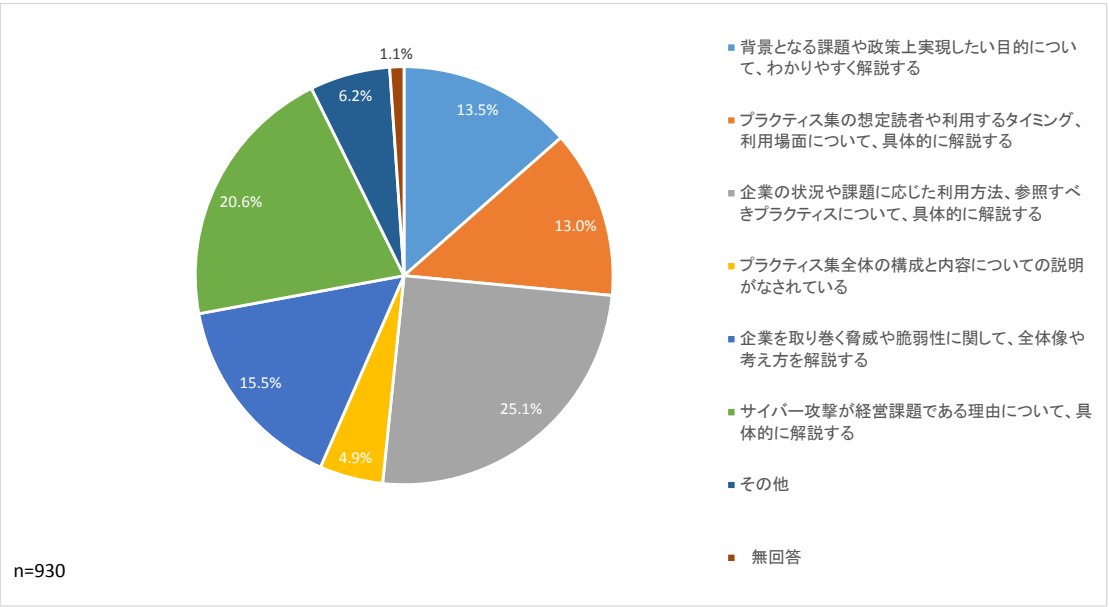


Q11. サイバー攻撃対策やセキュリティインシデント対応の強化等の取組みを新たに開始する際に、どのような方法で情報収集を行っていますか。当てはまるものを最大3つまでお選びください。(3つまで複数選択可)



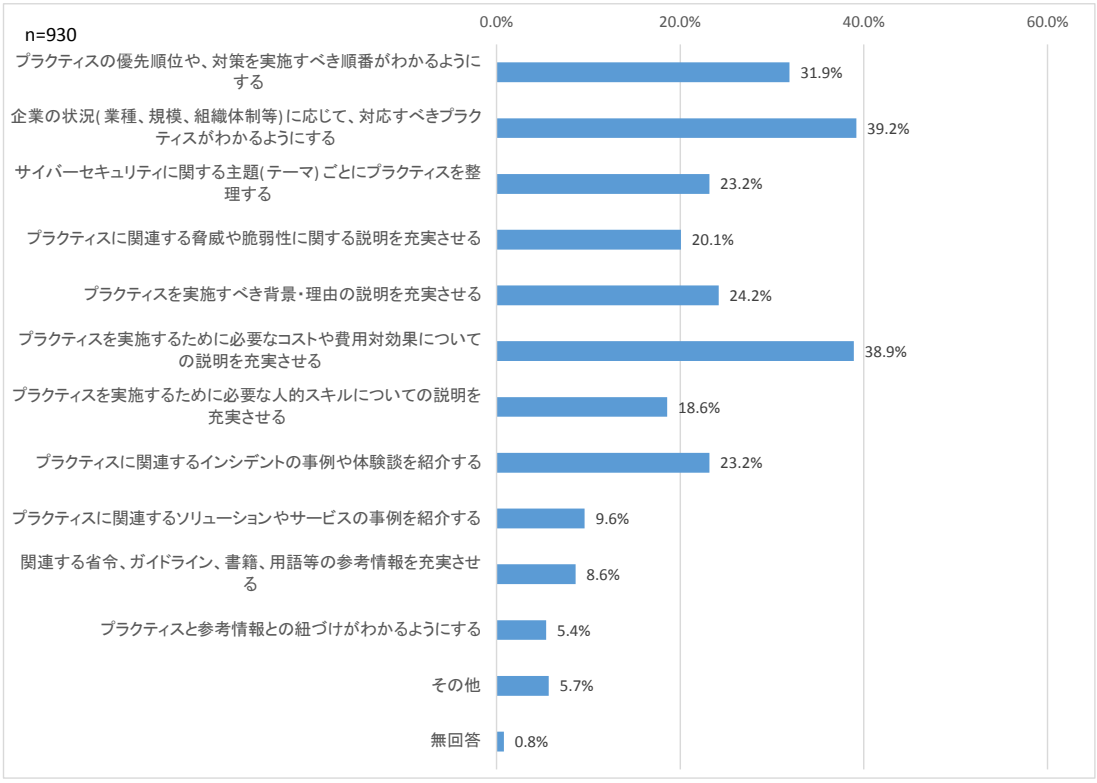
「経営ガイドライン実践のためのプラクティス集」では、「はじめに」および「第1章」にて、背景や目的、利用方法、経営とサイバーセキュリティの関係等について解説しています。

Q12. 「はじめに」および「第1章」の構成・内容について、今後どのような点を改善すれば、より活用しやすくなると考えますか。最も当てはまるものを1つお選びください。(単一選択)

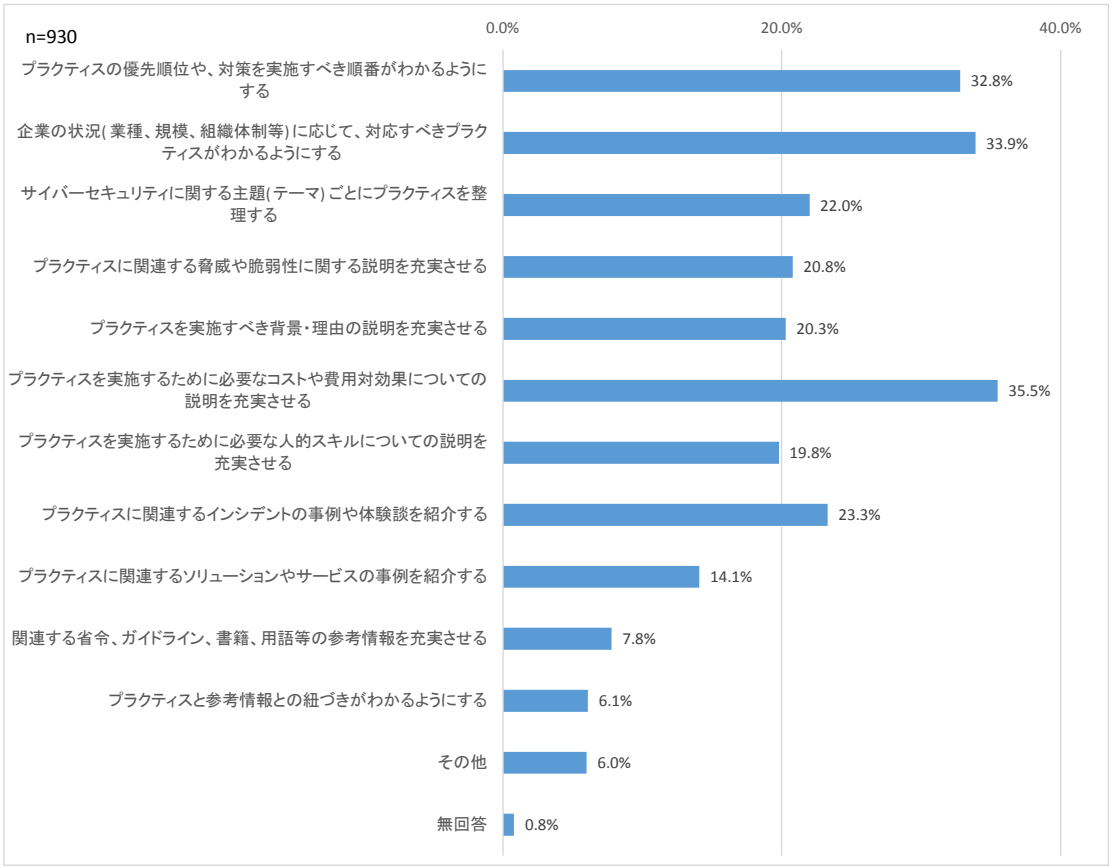


「経営ガイドライン実践のためのプラクティス集」では、「第2章」および「第3章」にて、具体的なプラクティスについての解説や参考情報を掲載しています。

Q13.「第2章」の構成・内容について、今後どのような点を改善すれば、より活用しやすくなると考えますか。
当てはまるものを最大3つまでお選びください。(3つまで複数選択可)

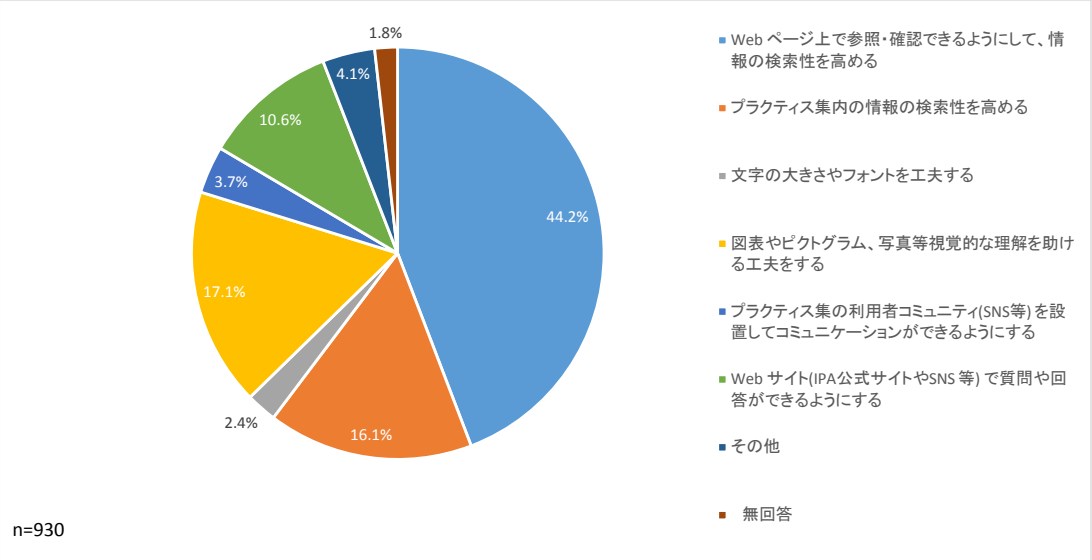


Q14.「第3章」の構成・内容について、今後どのような点を改善すれば、より活用しやすくなると考えますか。
当てはまるものを最大3つまでお選びください。(3つまで複数選択可)

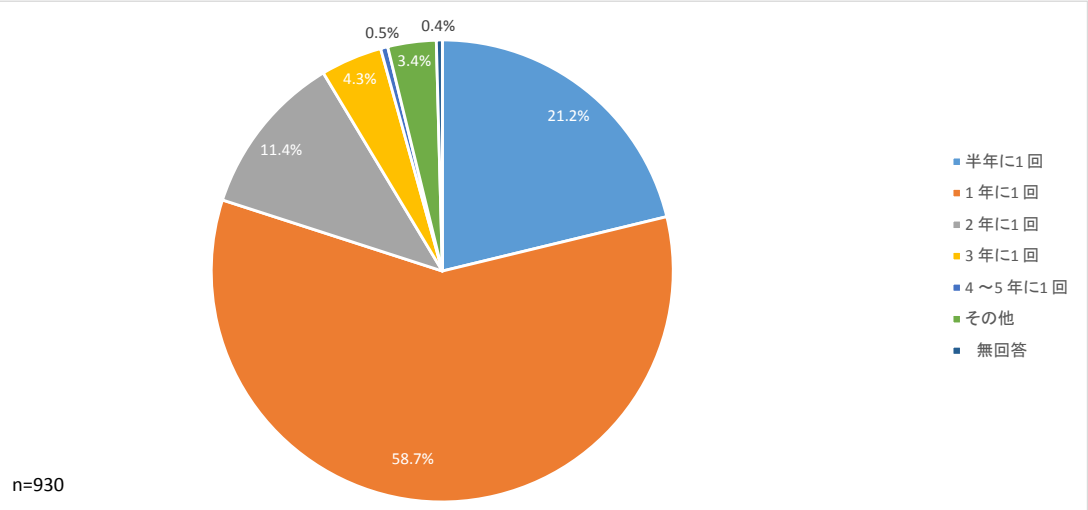


「経営ガイドライン実践のためのプラクティス集」は、現在IPAのホームページにてPDF形式で公表しています。

Q15.「経営ガイドライン実践のためのプラクティス集」の提供方法・媒体についてお聞きします。今後どのような点を改善すれば、より活用しやすくなると考えますか。最も当てはまるものを1つお選びください。(単一選択)

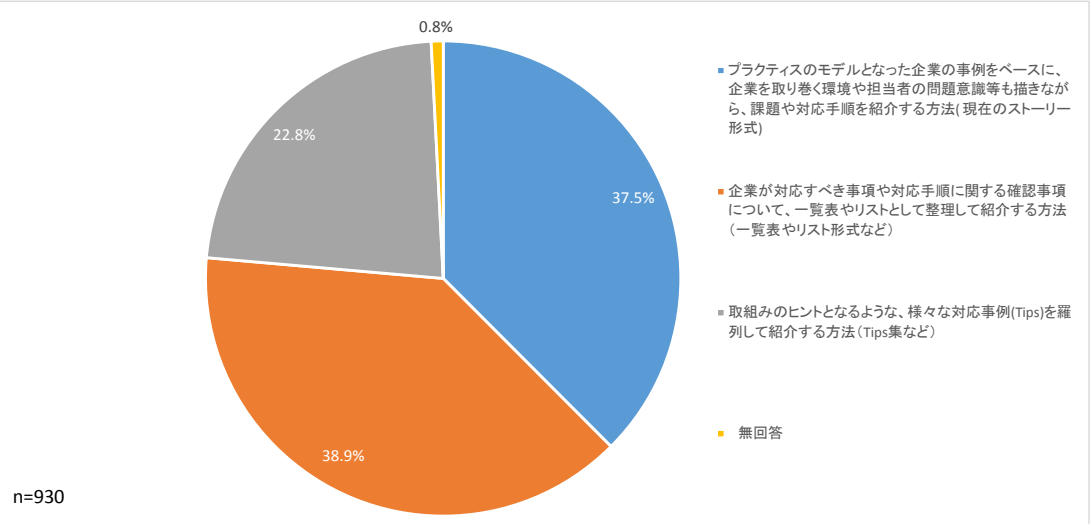


Q16.「経営ガイドライン実践のためのプラクティス集」として、どの程度の頻度で更新(見直し)されることが望ましいと考えますか。当てはまるものを1つお選びください。(単一選択)

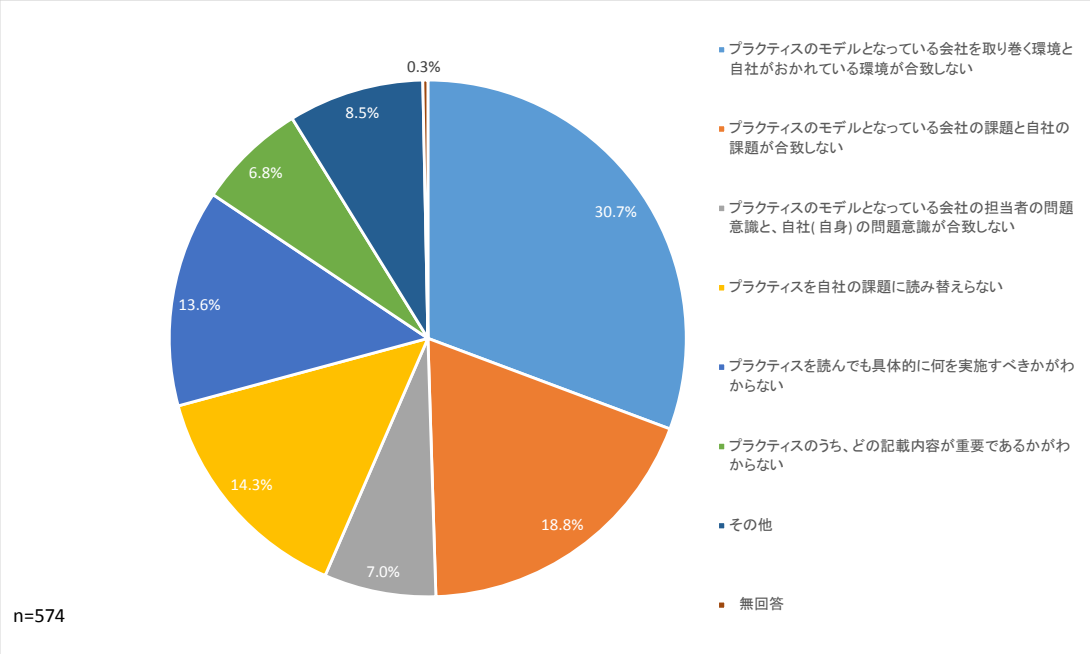


「経営ガイドライン実践のためのプラクティス集」では、「第2章」および「第3章」にて、実際の企業の取組みをモデルに、企業を取り巻く環境や担当者の問題意識等も描きながら、課題や対応手順を紹介しています。

Q17. 今後、各プラクティスがどのような記載(表現)方法で紹介されていれば、自社で利用しやすいと考えますか。
最も当てはまるものを1つお選びください。(単一選択)

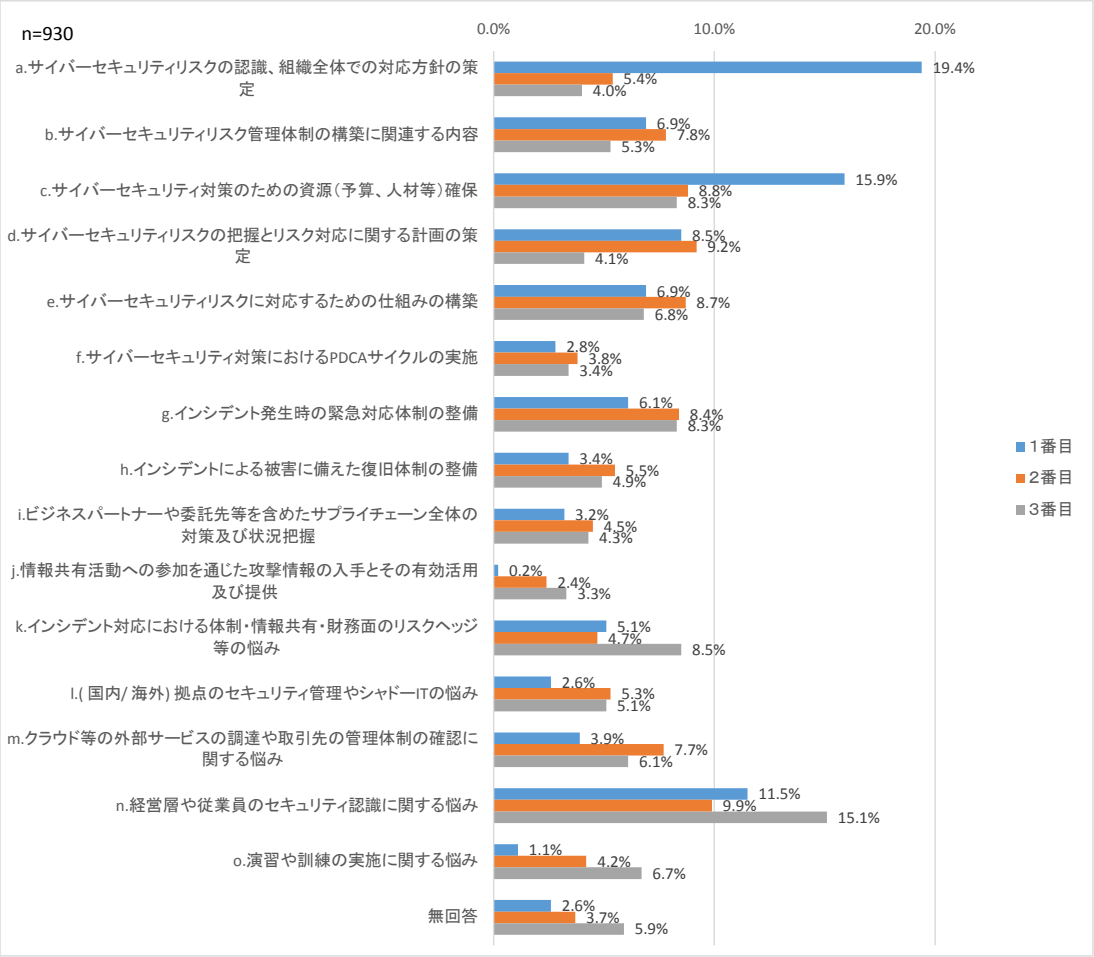


Q18. (Q17で(b)(c)のいずれかを選択した方に伺います)各プラクティスの表現方法について、Q17で(a)を選択しなかった理由について、
当てはまるものを1つお選びください。(単一選択)

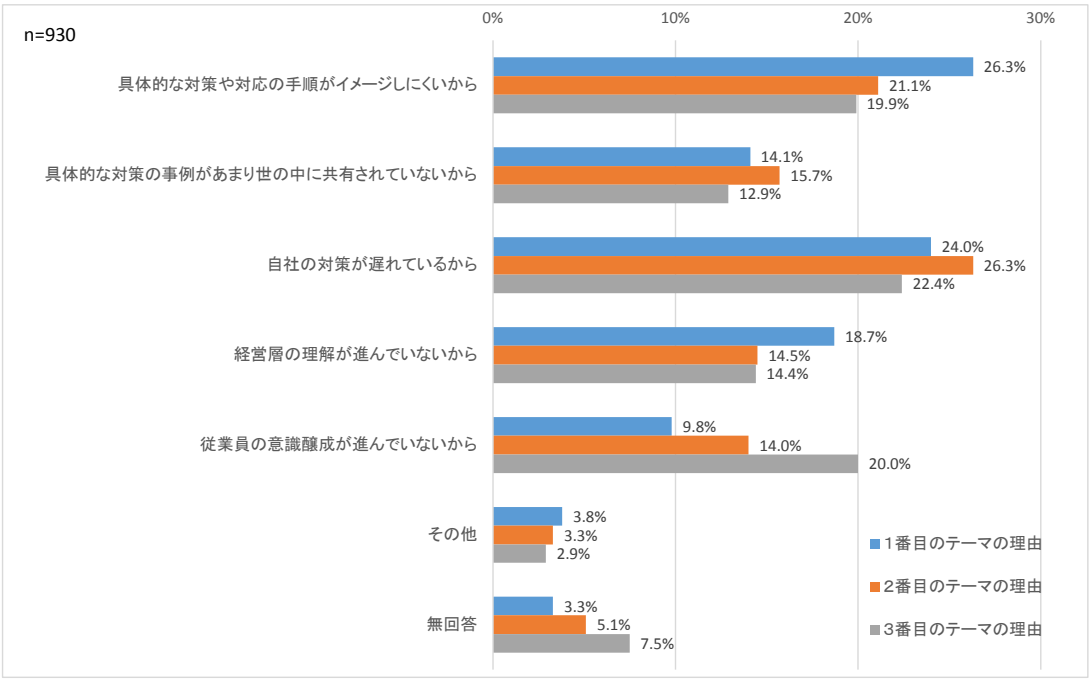


「経営ガイドライン実践のためのプラクティス集」の「第2章」では、「サイバーセキュリティ経営ガイドラインVer2.0」の「重要10項目」に関するプラクティスが、「第3章」では、セキュリティ担当者の悩みと取組に関するプラクティスを掲載しています。

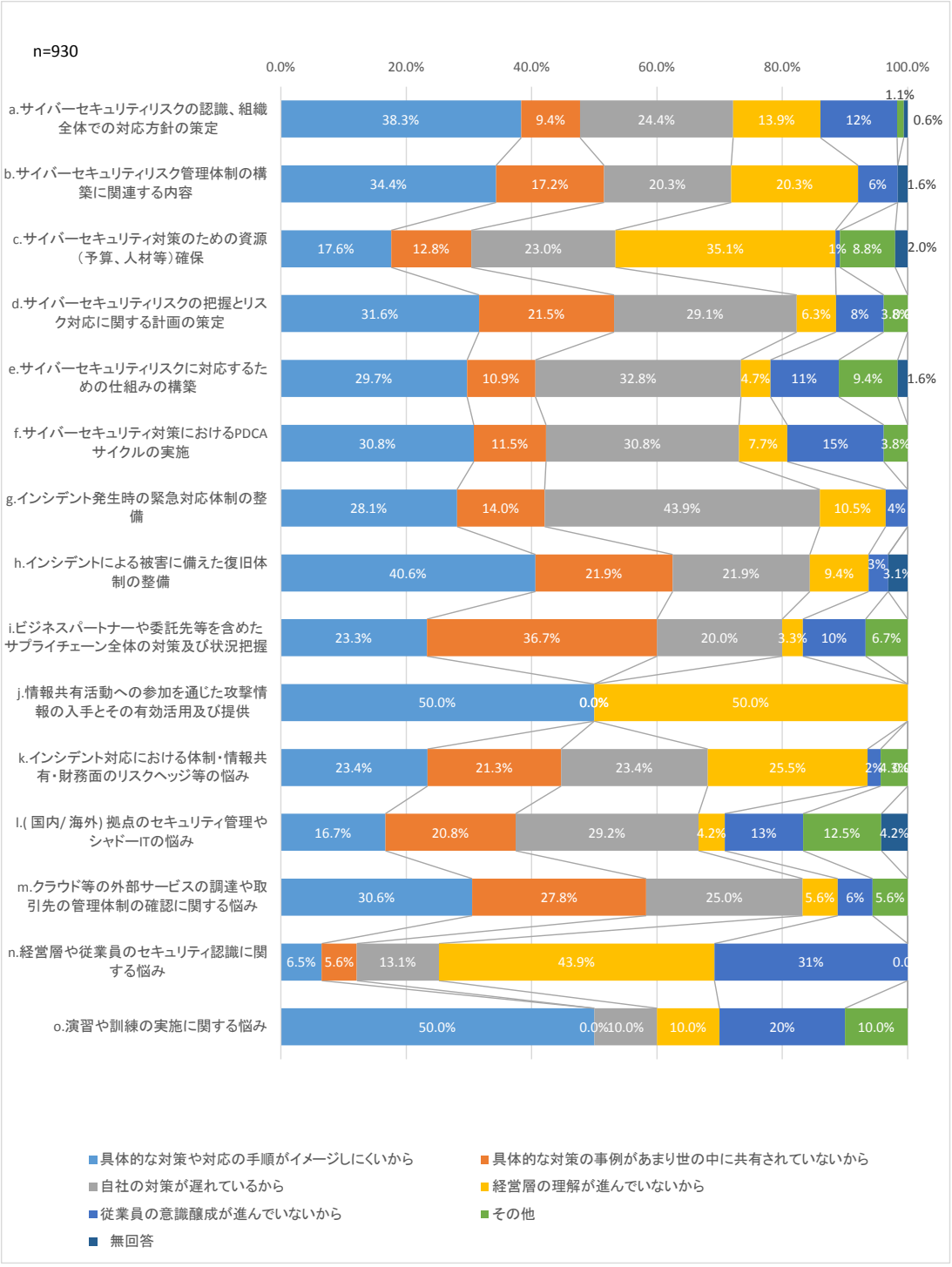
Q19. 今後、より多くのプラクティスの提供を望むテーマはどのテーマですか。当てはまるものについて、強く提供を望む順番に3つまで記載ください。(3つまで複数選択可)



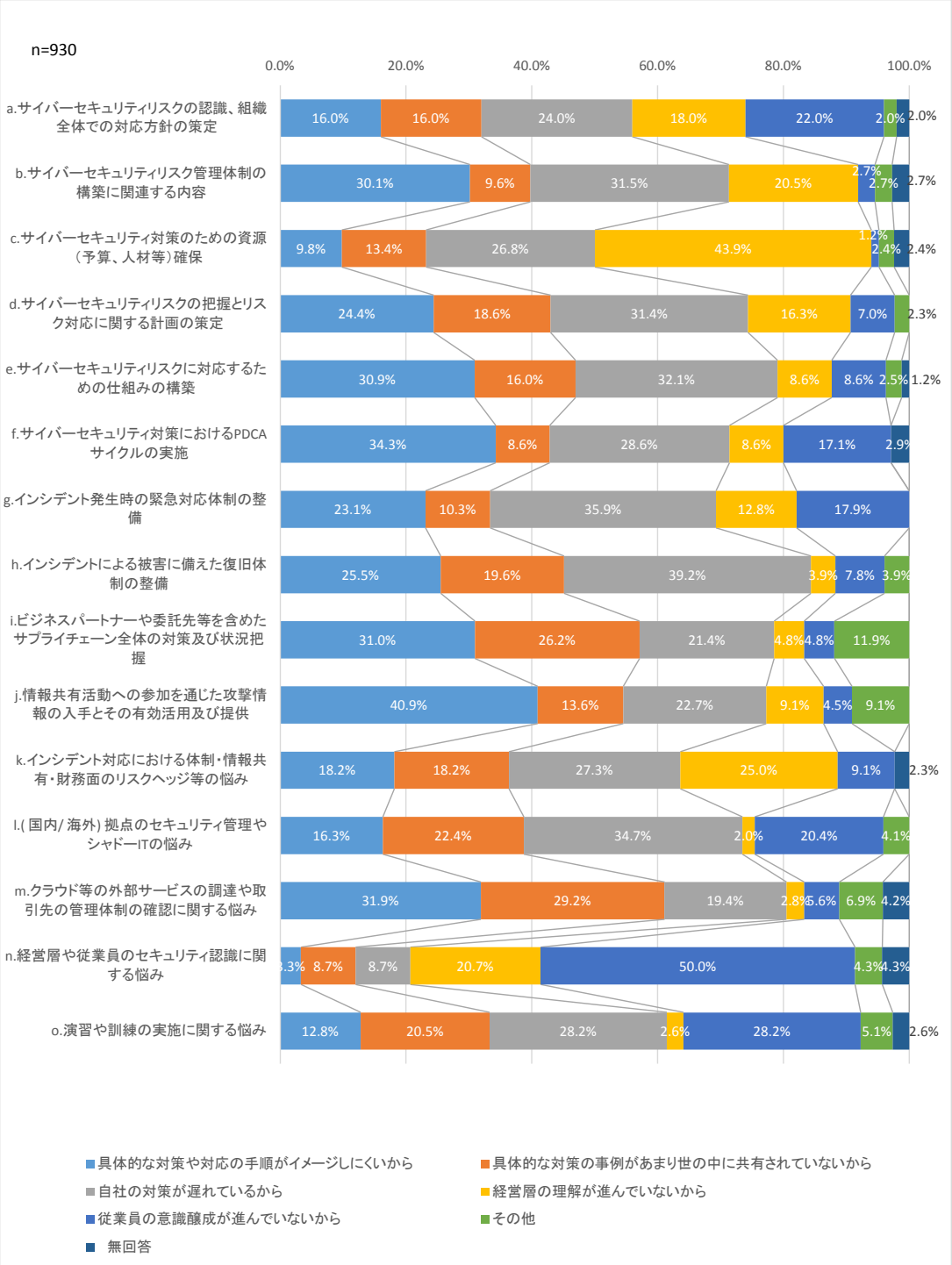
Q20. Q19で選択したそれぞれのテーマについて、プラクティスの提供を望む理由として、最も当てはまるものを、それぞれ1つずつお選びください。(単一選択)



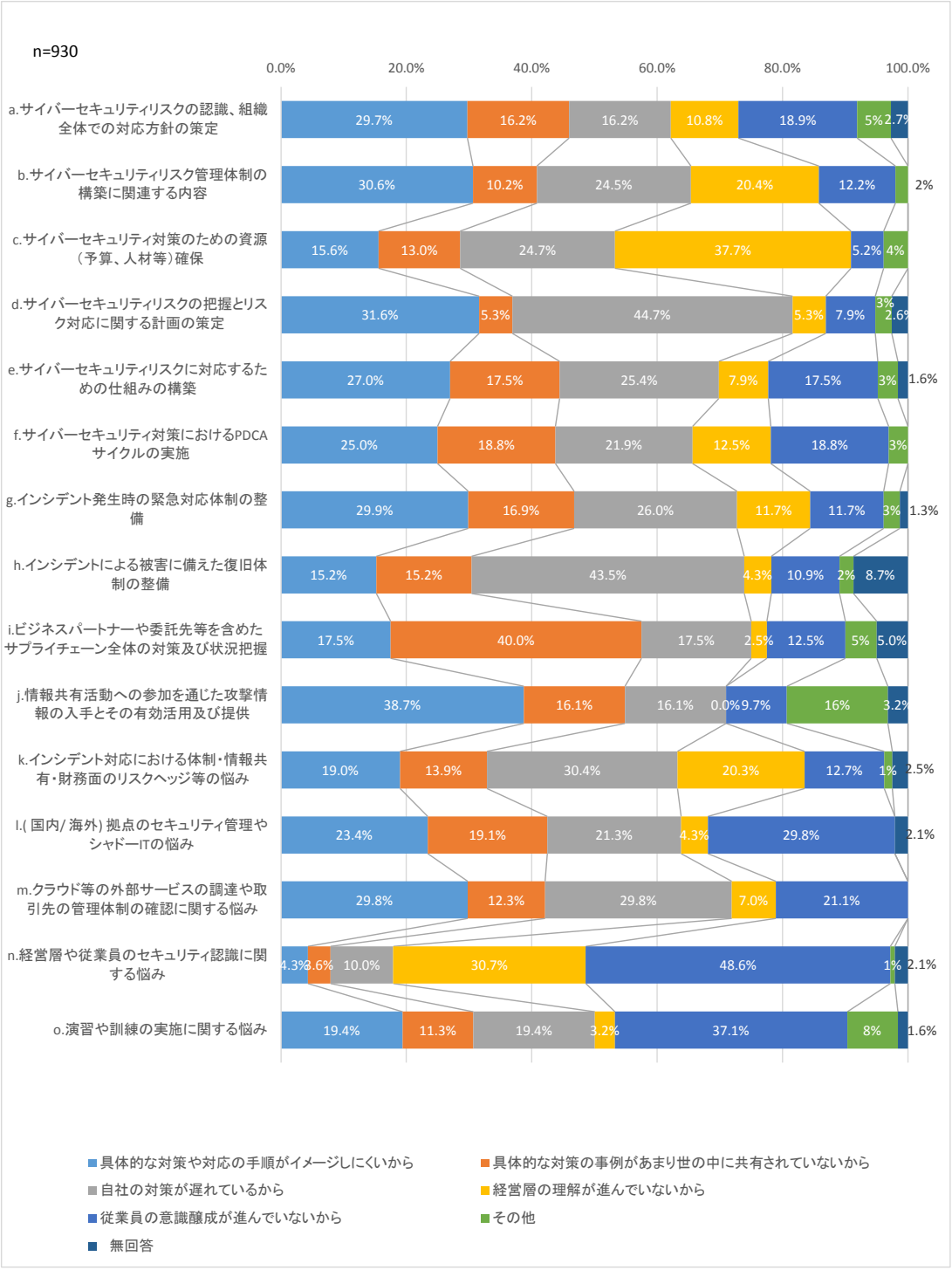
Q20. Q19で選択したそれぞれのテーマについて、プラクティスの提供を望む理由として、最も当てはまるものを、それぞれ1つずつお選びください。(単一選択)
1番目のテーマの理由



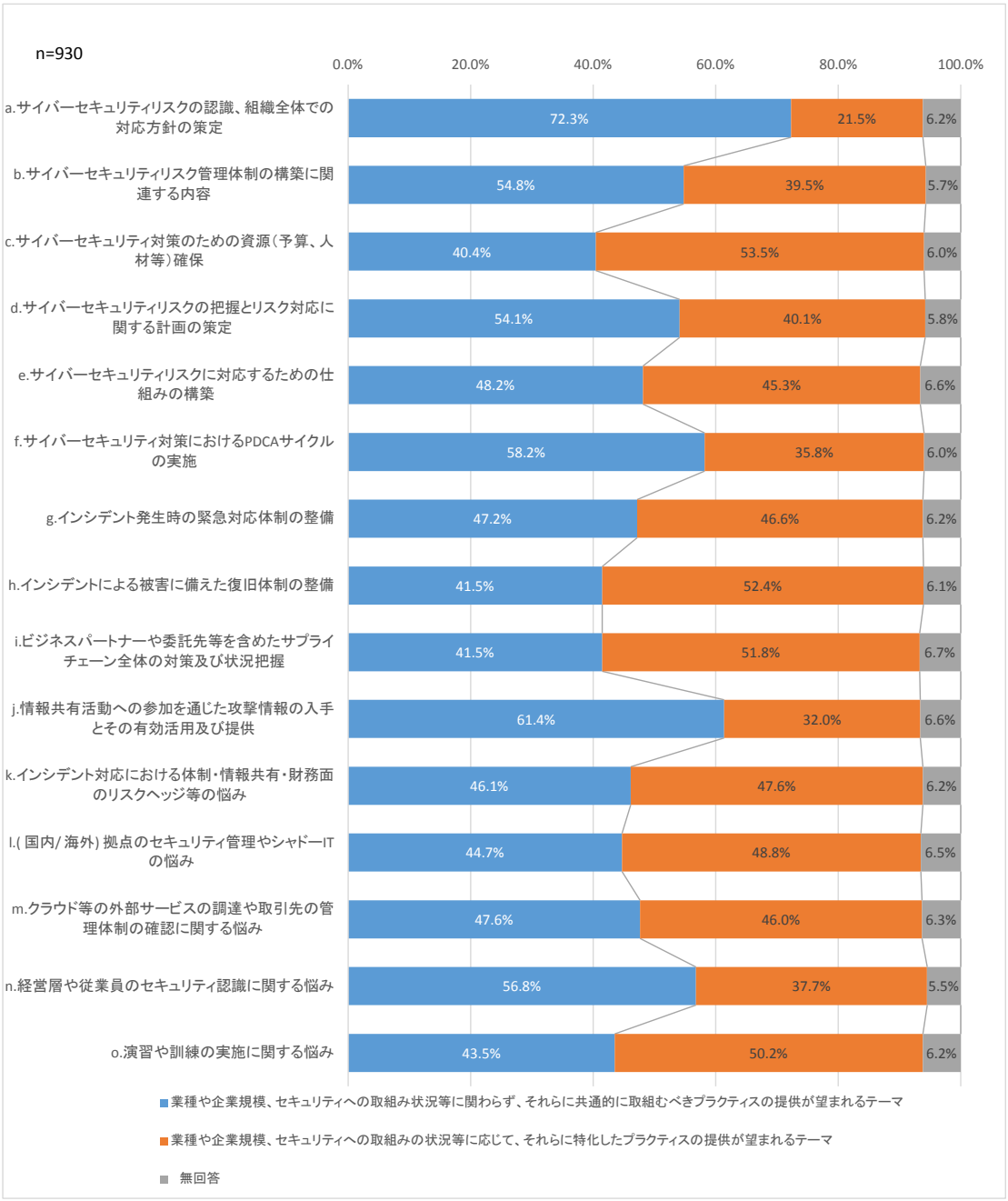
Q20. Q19で選択したそれぞれのテーマについて、プラクティスの提供を望む理由として、最も当てはまるものを、それぞれ1つずつお選びください。(単一選択)
2番目のテーマの理由



Q20. Q19で選択したそれぞれのテーマについて、プラクティスの提供を望む理由として、最も当てはまるものを、それぞれ1つずつお選びください。(単一選択)
3番目のテーマの理由

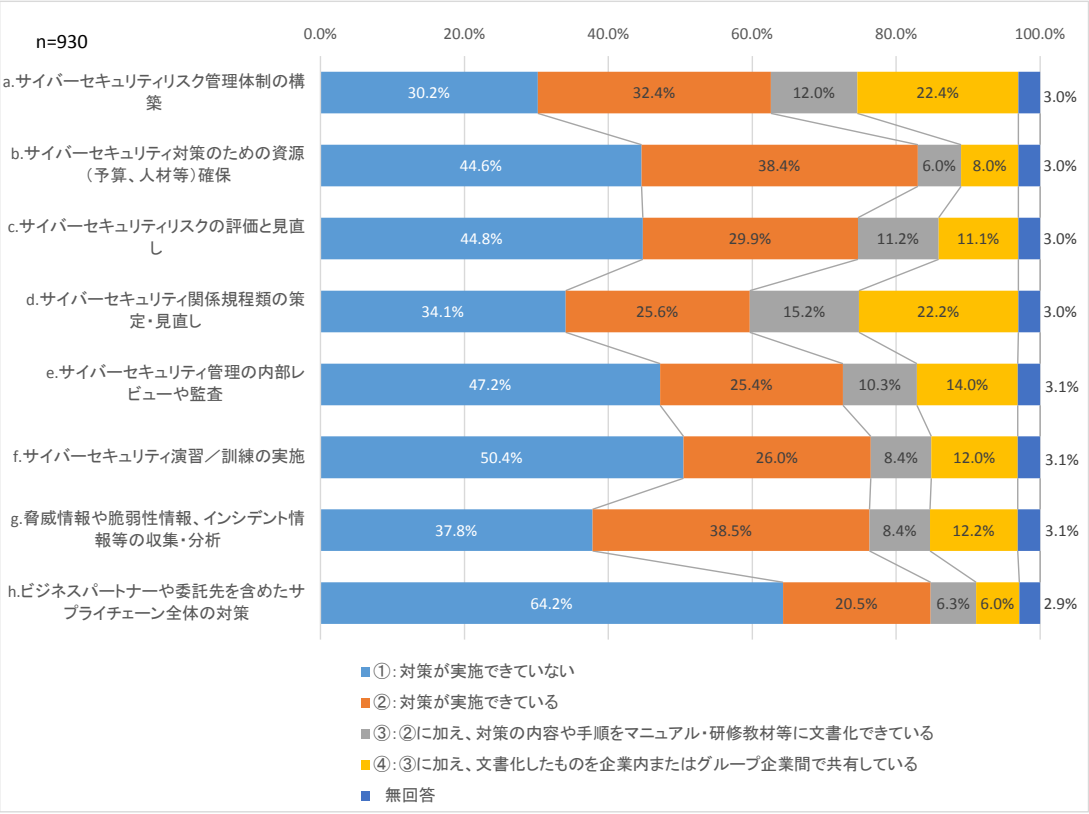


Q21. サイバーセキュリティ経営やセキュリティ担当者の悩みに関するテーマのうち、自社の状況を踏まえた場合に、「①：業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ」、「②：業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ」いずれに当てはまると考えますか。テーマ毎に1つずつお選びください。((a)～(o)それぞれに対して単一選択)



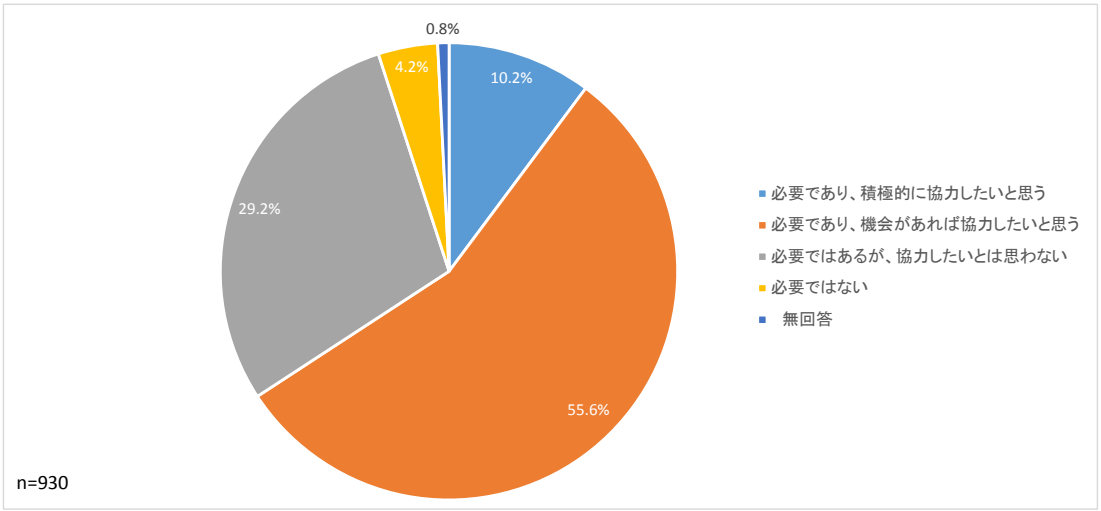
サイバーセキュリティ対策の推進や、対策内容の文書化を通じた自社・グループ企業間での共有についてお聞きします。

Q22. 以下のサイバーセキュリティ対策のうち、「①：対策が実施できていない」「②：対策が実施できている」「③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている」「④：③に加え、文書化したものを企業内またはグループ企業間で共有している」いずれに該当しますか。当てはまるものを1つずつお選びください。((a)～(h)それぞれに対して単一選択)

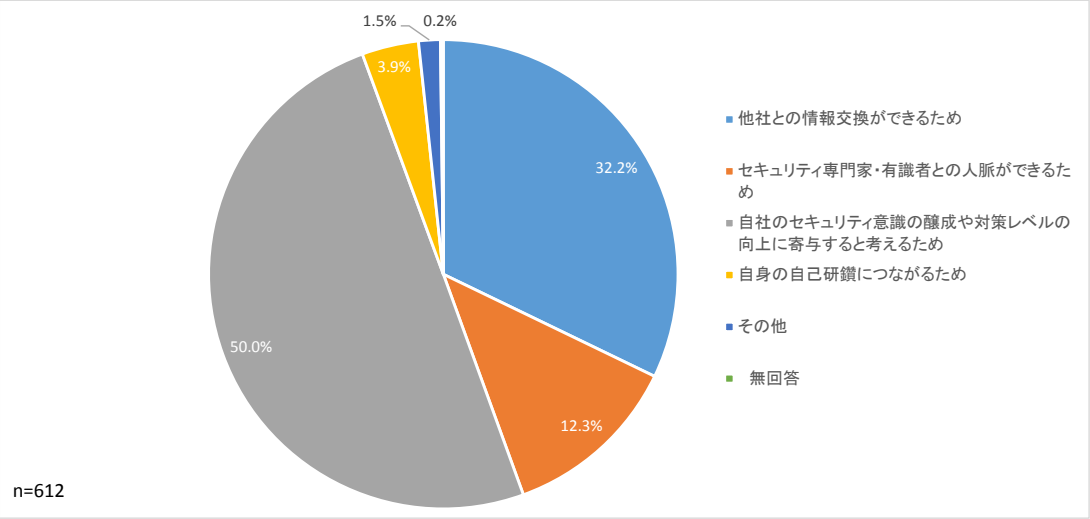


サイバーセキュリティに関するプラクティスについて、複数の企業のメンバーが共同で検討・策定し、外部に公表する枠組みや取組みについてお聞きします。

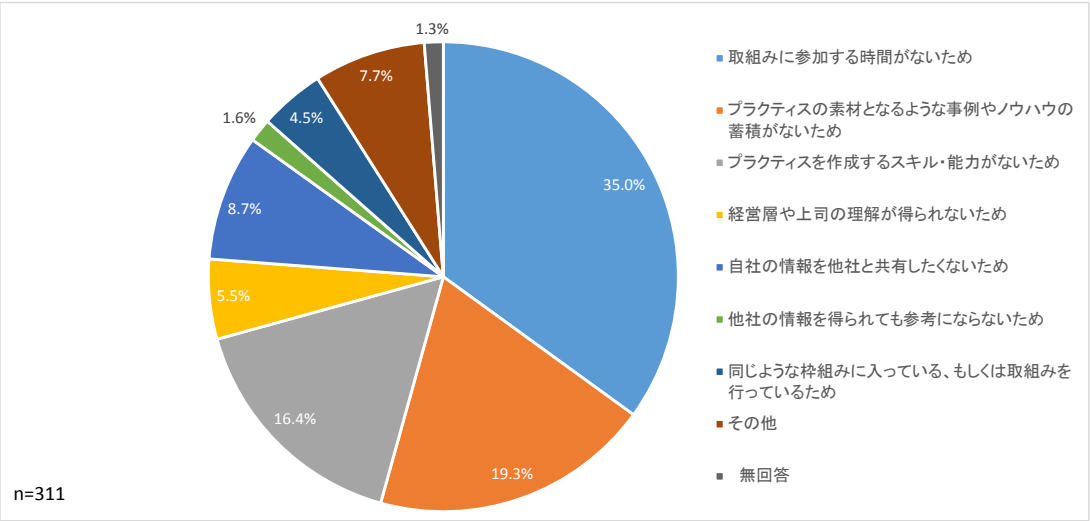
Q23. 今後こうした取組みは必要であると考えますか、またこうした取組みに自社として協力したいと考えますか。
当てはまるものを1つお選びください。(単一選択)



Q24. (Q23で(a)(b)のいずれかを選択した方に伺います)取組みに協力したいと思う理由は何ですか。当てはまるものを1つお選びください

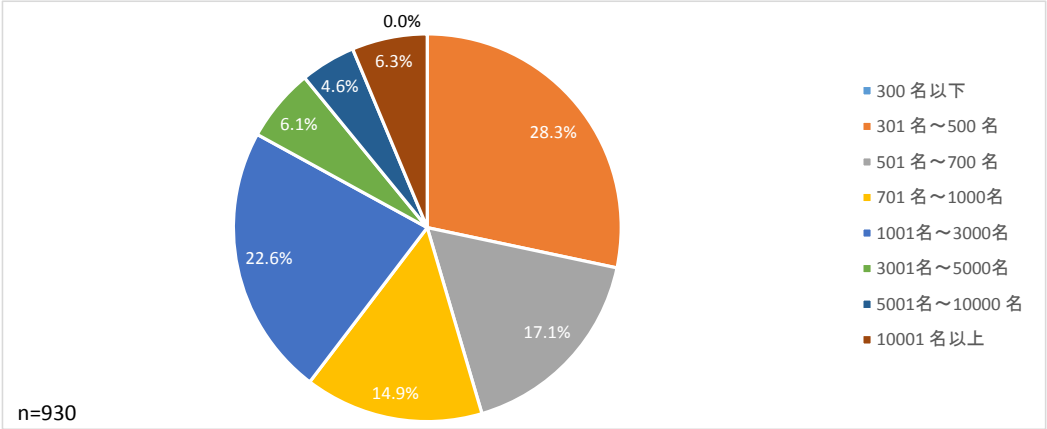


Q25. (Q23で(c)(d)のいずれかを選択した方に伺います)取組みに協力できない理由は何ですか。当てはまるものを1つお選びください



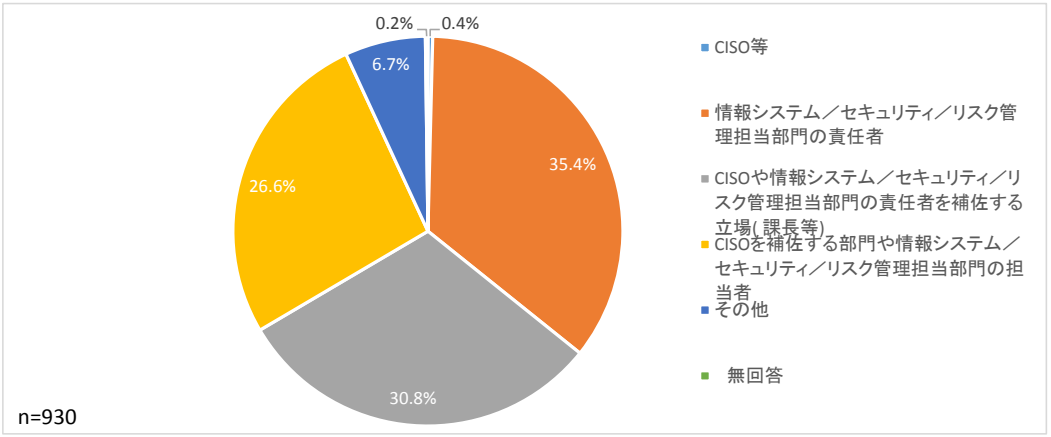
Q1. 総従業員数（有給役員,正社員・正職員,準社員・準職員,アルバイト等を含む）についてお聞きします。直近の会計年度の人数を１つお選びください。(単一選択)

n	930	100.0%
300 名以下	0	0.0%
301 名～500 名	263	28.3%
501 名～700 名	159	17.1%
701 名～1000名	139	14.9%
1001名～3000名	210	22.6%
3001名～5000名	57	6.1%
5001名～10000 名	43	4.6%
10001 名以上	59	6.3%
無回答	0	0.0%



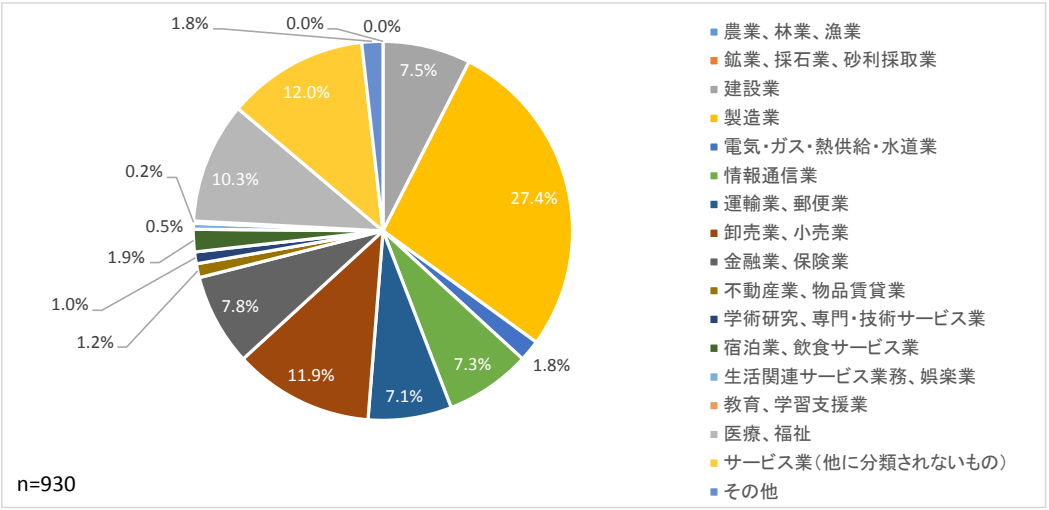
Q2. ご回答いただいている方ご自身の役職または立場として最も近いものを１つお選びください。(単一選択)

n	930	100.0%
CISO等	4	0.4%
情報システム／セキュリティ／リスク管理担当部門の責任者	329	35.4%
CISOや情報システム／セキュリティ／リスク管理担当部門の責任者を補佐する立場(課長等)	286	30.8%
CISOを補佐する部門や情報システム／セキュリティ／リスク管理担当部門の担当者	247	26.6%
その他	62	6.7%
無回答	2	0.2%



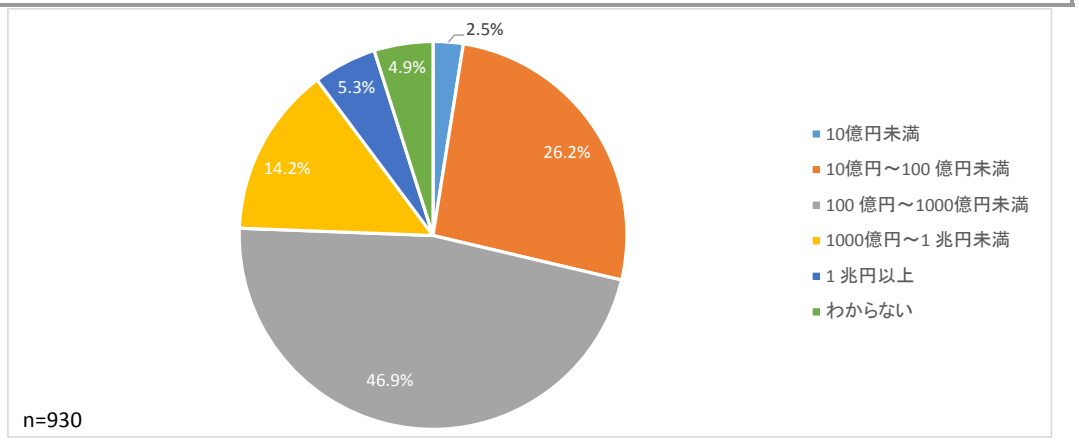
Q3. 貴社の業種*を１つお選びください。(単一選択) *日本標準産業分類に基づく

n	930	100.0%
農業、林業、漁業	0	0.0%
鉱業、採石業、砂利採取業	0	0.0%
建設業	70	7.5%
製造業	255	27.4%
電気・ガス・熱供給・水道業	17	1.8%
情報通信業	68	7.3%
運輸業、郵便業	66	7.1%
卸売業、小売業	111	11.9%
金融業、保険業	73	7.8%
不動産業、物品賃貸業	11	1.2%
学術研究、専門・技術サービス業	9	1.0%
宿泊業、飲食サービス業	18	1.9%
生活関連サービス業務、娯楽業	5	0.5%
教育、学習支援業	2	0.2%
医療、福祉	96	10.3%
サービス業（他に分類されないもの）	112	12.0%
その他	17	1.8%
無回答	0	0.0%



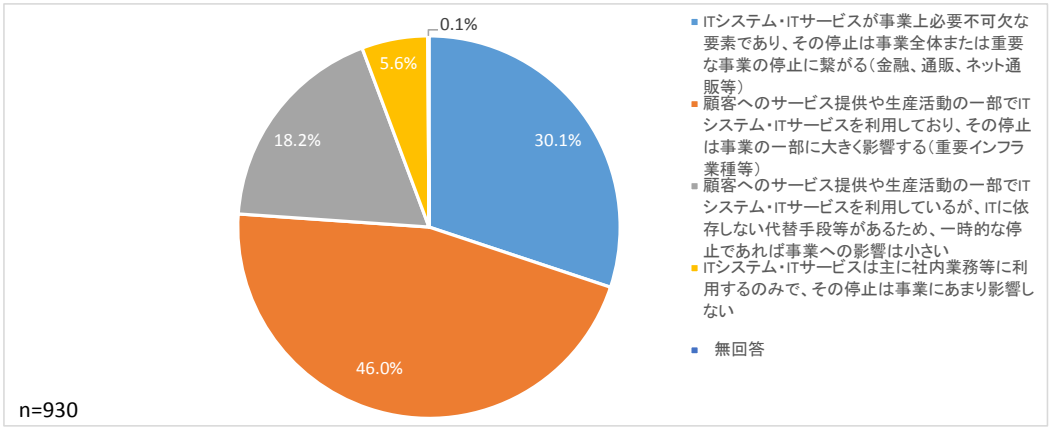
Q4. 直近の会計年度の総売上高を 1 つお選びください。(単一選択)

n	930	100.0%
10億円未満	23	2.5%
10億円～100 億円未満	244	26.2%
100 億円～1000億円未満	436	46.9%
1000億円～1 兆円未満	132	14.2%
1 兆円以上	49	5.3%
わからない	46	4.9%
無回答	0	0.0%



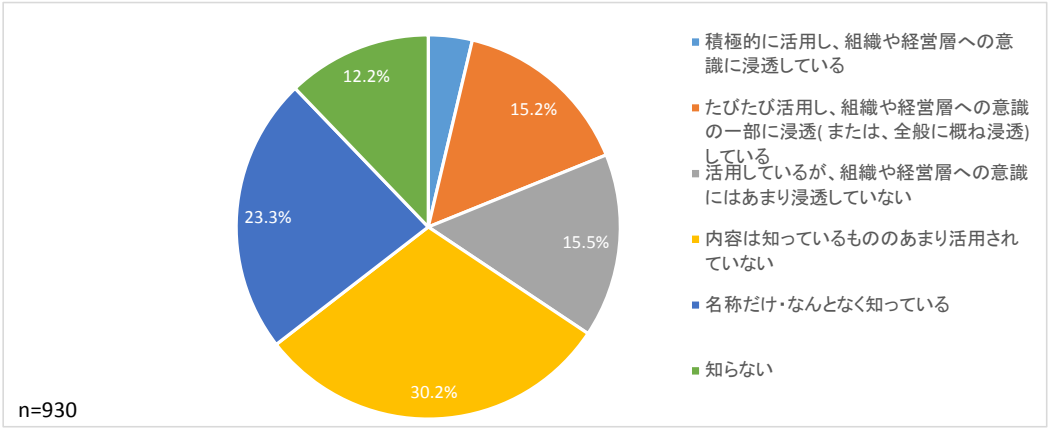
Q5. 事業のIT システム・IT サービスへの依存度について、最も近いものを 1 つお選びください。(単一選択)

n	930	100.0%
ITシステム・ITサービスが事業上必要不可欠な要素であり、その停止は事業全体または重要な事業の停止に繋がる（金融、通販、ネット通販等）	280	30.1%
顧客へのサービス提供や生産活動の一部でITシステム・ITサービスを利用しており、その停止は事業の一部に大きく影響する（重要インフラ業種等）	428	46.0%
顧客へのサービス提供や生産活動の一部でITシステム・ITサービスを利用しているが、ITに依存しない代替手段等があるため、一時的な停止であれば事業への影響は小さい	169	18.2%
ITシステム・ITサービスは主に社内業務等に利用するのみで、その停止は事業にあまり影響しない	52	5.6%
無回答	1	0.1%



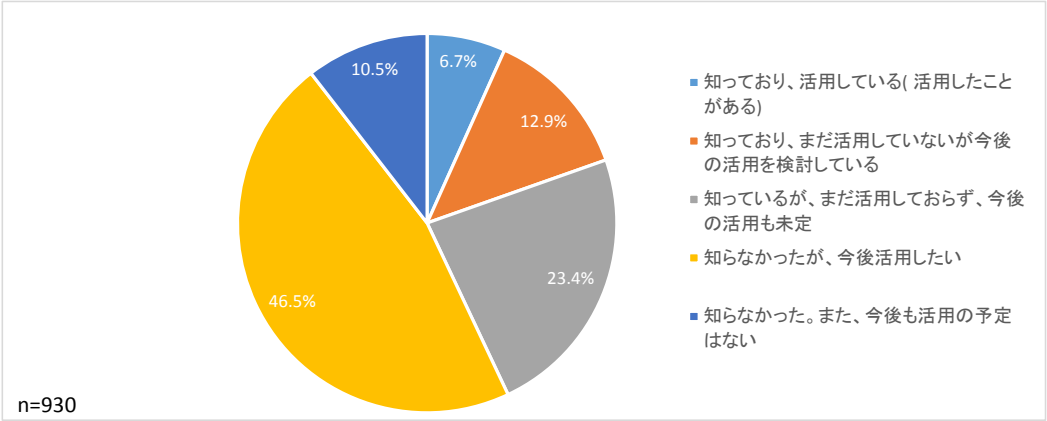
Q6.　経済産業省と独立行政法人情報処理推進機構(IPA)が2017年に策定した「サイバーセキュリティ経営ガイドラインVer2.0」※1を利活用していますか、もしくは知っていますか。当てはまるものを１つお選びください。(単一選択)

n	930	100.0%
積極的に活用し、組織や経営層への意識に浸透している	34	3.7%
たびたび活用し、組織や経営層への意識の一部に浸透(または、全般に概ね浸透) している	141	15.2%
活用しているが、組織や経営層への意識にはあまり浸透していない	144	15.5%
内容は知っているもののあまり活用されていない	281	30.2%
名称だけ・なんとなく知っている	217	23.3%
知らない	113	12.2%
無回答	0	0.0%



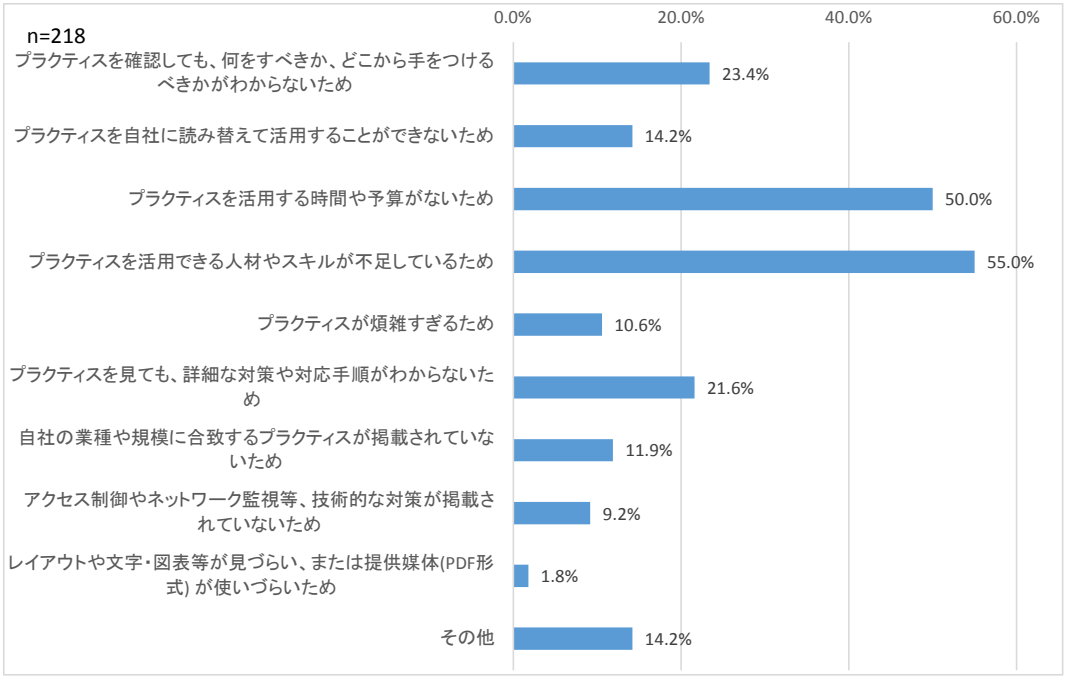
Q7.「経営ガイドライン実践のためのプラクティス集」を知っていましたか。また、これを利活用したことがありますか(今後活用したいと思いますか)。当てはまるものを１つお選びください。(単一選択)

n	930	100.0%
知っており、活用している(活用したことがある)	62	6.7%
知っており、まだ活用していないが今後の活用を検討している	120	12.9%
知っているが、まだ活用しておらず、今後の活用も未定	218	23.4%
知らなかったが、今後活用したい	432	46.5%
知らなかった。また、今後も活用の予定はない	98	10.5%
無回答	0	0.0%



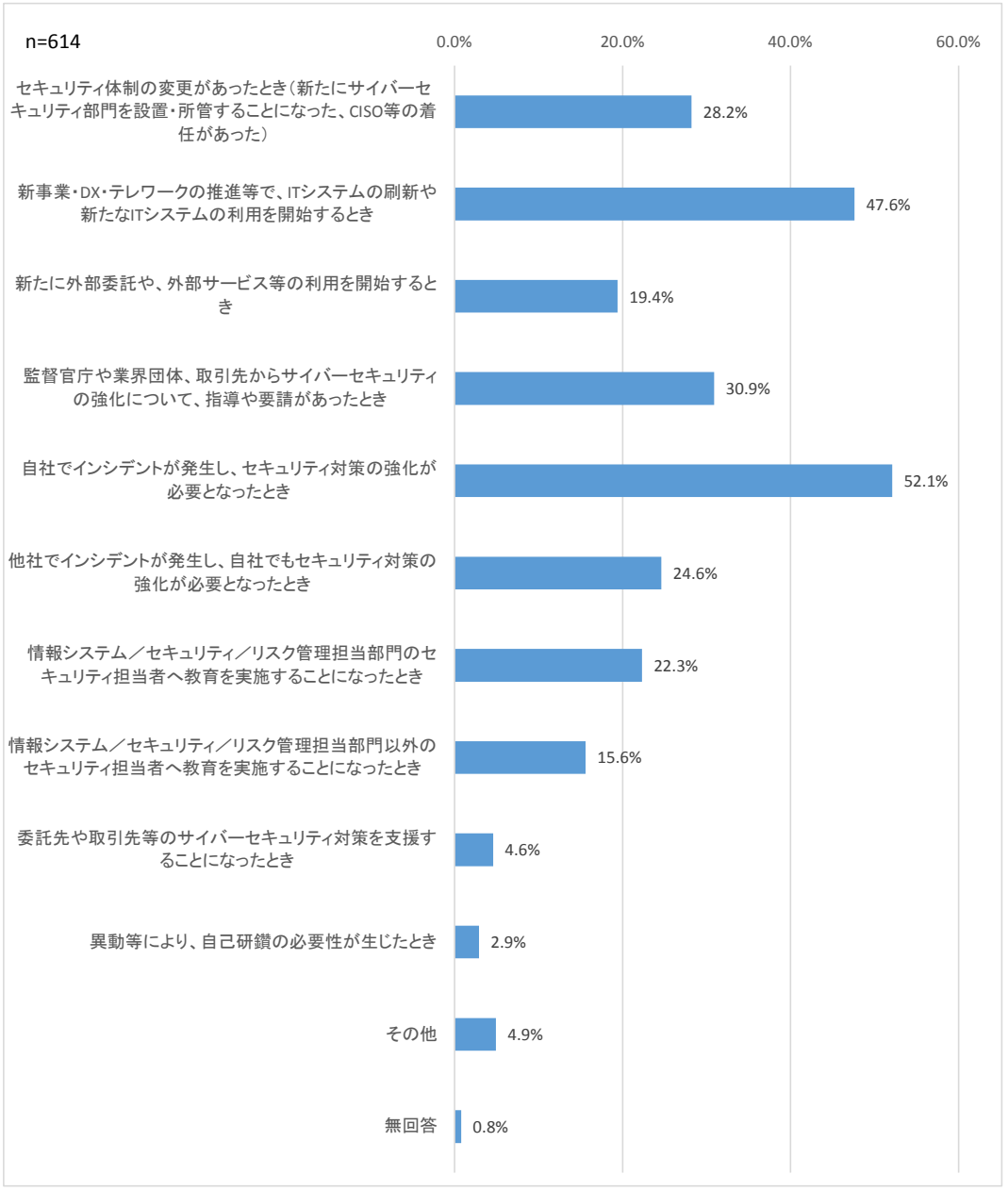
Q8. (Q7で(c)を選択した方に伺います)「経営ガイドライン実践のためのプラクティス集」を知っているが、まだ活用しておらず、今後の活用も未定である理由について、当てはまるものを最大３つまでお選びください。(複数選択可)

n	218	100.0%
プラクティスを確認しても、何をすべきか、どこから手をつけるべきかがわからないため	51	23.4%
プラクティスを自社に読み替えて活用することができないため	31	14.2%
プラクティスを活用する時間や予算がないため	109	50.0%
プラクティスを活用できる人材やスキルが不足しているため	120	55.0%
プラクティスが煩雑すぎるため	23	10.6%
プラクティスを見ても、詳細な対策や対応手順がわからないため	47	21.6%
自社の業種や規模に合致するプラクティスが掲載されていないため	26	11.9%
アクセス制御やネットワーク監視等、技術的な対策が掲載されていないため	20	9.2%
レイアウトや文字・図表等が見づらい、または提供媒体(PDF形式) が使いづらいため	4	1.8%
その他	31	14.2%
無回答	0	0.0%



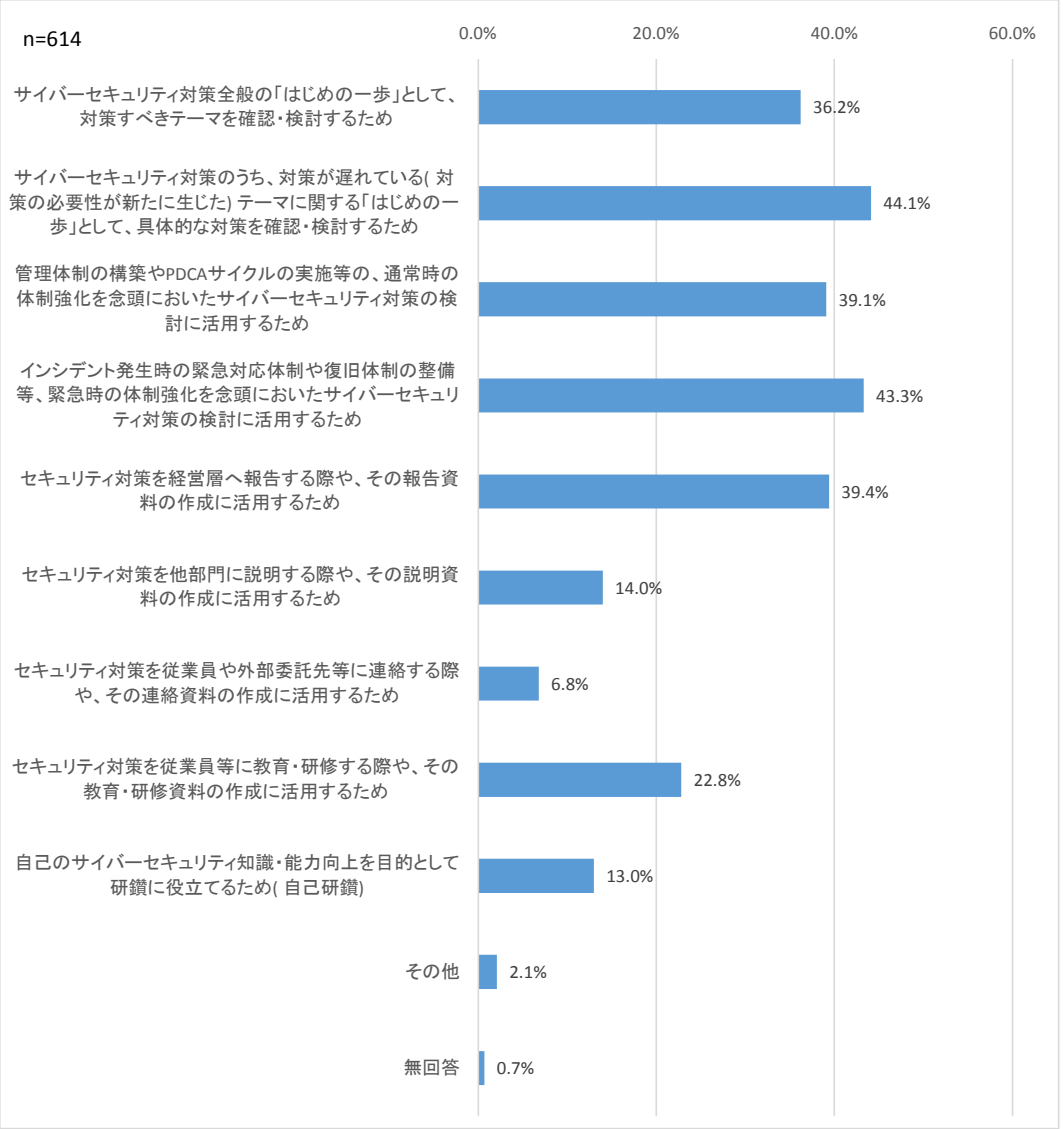
Q9. (Q7で(a)(b)(d)のいずれかを選択した方に伺います)「経営ガイドライン実践のためのプラクティス集」を活用するきっかけやタイミング(今後、活用するきっかけやタイミングとして想定されるもの)について、当てはまるものを最大３つまでお選びください。(３つまで複数選択可)

n	614	100.0%
セキュリティ体制の変更があったとき（新たにサイバーセキュリティ部門を設置・所管することになった、CISO等の着任があった）	173	28.2%
新事業・DX・テレワークの推進等で、ITシステムの刷新や新たなITシステムの利用を開始するとき	292	47.6%
新たに外部委託や、外部サービス等の利用を開始するとき	119	19.4%
監督官庁や業界団体、取引先からサイバーセキュリティの強化について、指導や要請があったとき	190	30.9%
自社でインシデントが発生し、セキュリティ対策の強化が必要となったとき	320	52.1%
他社でインシデントが発生し、自社でもセキュリティ対策の強化が必要となったとき	151	24.6%
情報システム／セキュリティ／リスク管理担当部門のセキュリティ担当者へ教育を実施することになったとき	137	22.3%
情報システム／セキュリティ／リスク管理担当部門以外のセキュリティ担当者へ教育を実施することになったとき	96	15.6%
委託先や取引先等のサイバーセキュリティ対策を支援することになったとき	28	4.6%
異動等により、自己研鑽の必要性が生じたとき	18	2.9%
その他	30	4.9%
無回答	5	0.8%



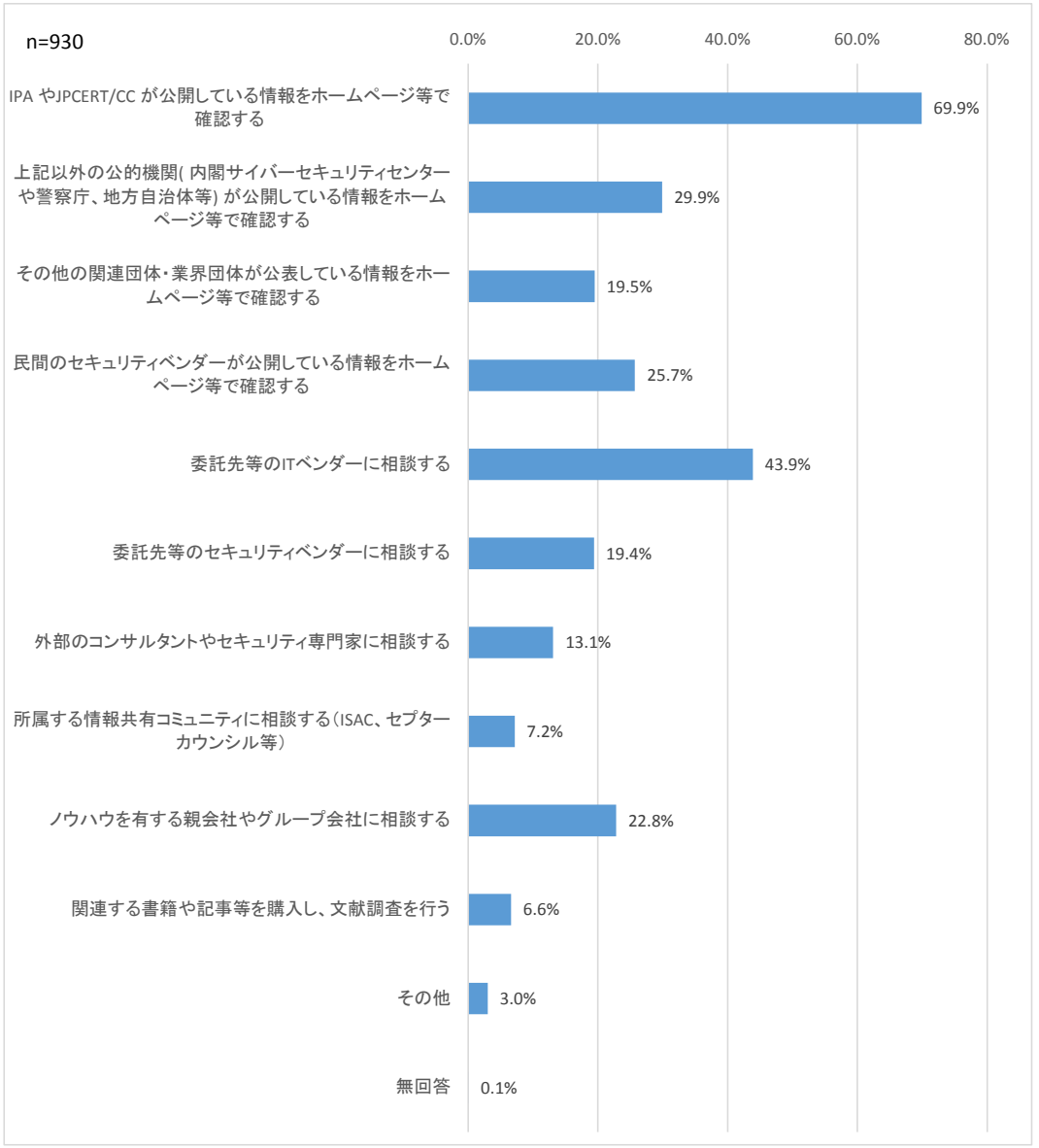
Q10. (Q7で(a)(b)(d)のいずれかを選択した方に伺います)「経営ガイドライン実践のためのプラクティス集」を活用する目的(今後、活用する目的として想定されるもの)について、当てはまるものを最大３つまでお選びください。(３つまで複数選択可)

n	614	100.0%
サイバーセキュリティ対策全般の「はじめの一歩」として、対策すべきテーマを確認・検討するため	222	36.2%
サイバーセキュリティ対策のうち、対策が遅れている(対策の必要性が新たに生じた)テーマに関する「はじめの一歩」として、具体的な対策を確認・検討するため	271	44.1%
管理体制の構築やPDCAサイクルの実施等の、通常時の体制強化を念頭においたサイバーセキュリティ対策の検討に活用するため	240	39.1%
インシデント発生時の緊急対応体制や復旧体制の整備等、緊急時の体制強化を念頭においたサイバーセキュリティ対策の検討に活用するため	266	43.3%
セキュリティ対策を経営層へ報告する際や、その報告資料の作成に活用するため	242	39.4%
セキュリティ対策を他部門に説明する際や、その説明資料の作成に活用するため	86	14.0%
セキュリティ対策を従業員や外部委託先等に連絡する際や、その連絡資料の作成に活用するため	42	6.8%
セキュリティ対策を従業員等に教育・研修する際や、その教育・研修資料の作成に活用するため	140	22.8%
自己のサイバーセキュリティ知識・能力向上を目的として研鑽に役立てるため(自己研鑽)	80	13.0%
その他	13	2.1%
無回答	4	0.7%



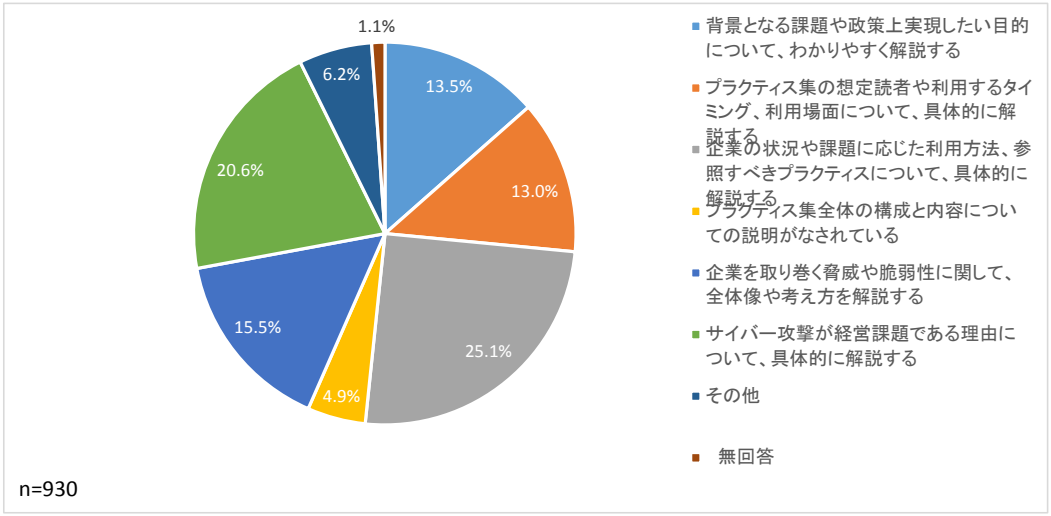
Q11. サイバー攻撃対策やセキュリティインシデント対応の強化等の取組みを新たに開始する際に、どのような方法で情報収集を行っていますか。当てはまるものを最大３つまでお選びください。（３つまで複数選択可）

n	930	100.0%
IPA やJPCERT/CC が公開している情報をホームページ等で確認する	650	69.9%
上記以外の公的機関(内閣サイバーセキュリティセンターや警察庁、地方自治体等) が公開している情報をホームページ等で確認する	278	29.9%
その他の関連団体・業界団体が公表している情報をホームページ等で確認する	181	19.5%
民間のセキュリティベンダーが公開している情報をホームページ等で確認する	239	25.7%
委託先等のITベンダーに相談する	408	43.9%
委託先等のセキュリティベンダーに相談する	180	19.4%
外部のコンサルタントやセキュリティ専門家に相談する	122	13.1%
所属する情報共有コミュニティに相談する（ISAC、セプターカウンシル等）	67	7.2%
ノウハウを有する親会社やグループ会社に相談する	212	22.8%
関連する書籍や記事等を購入し、文献調査を行う	61	6.6%
その他	28	3.0%
無回答	1	0.1%



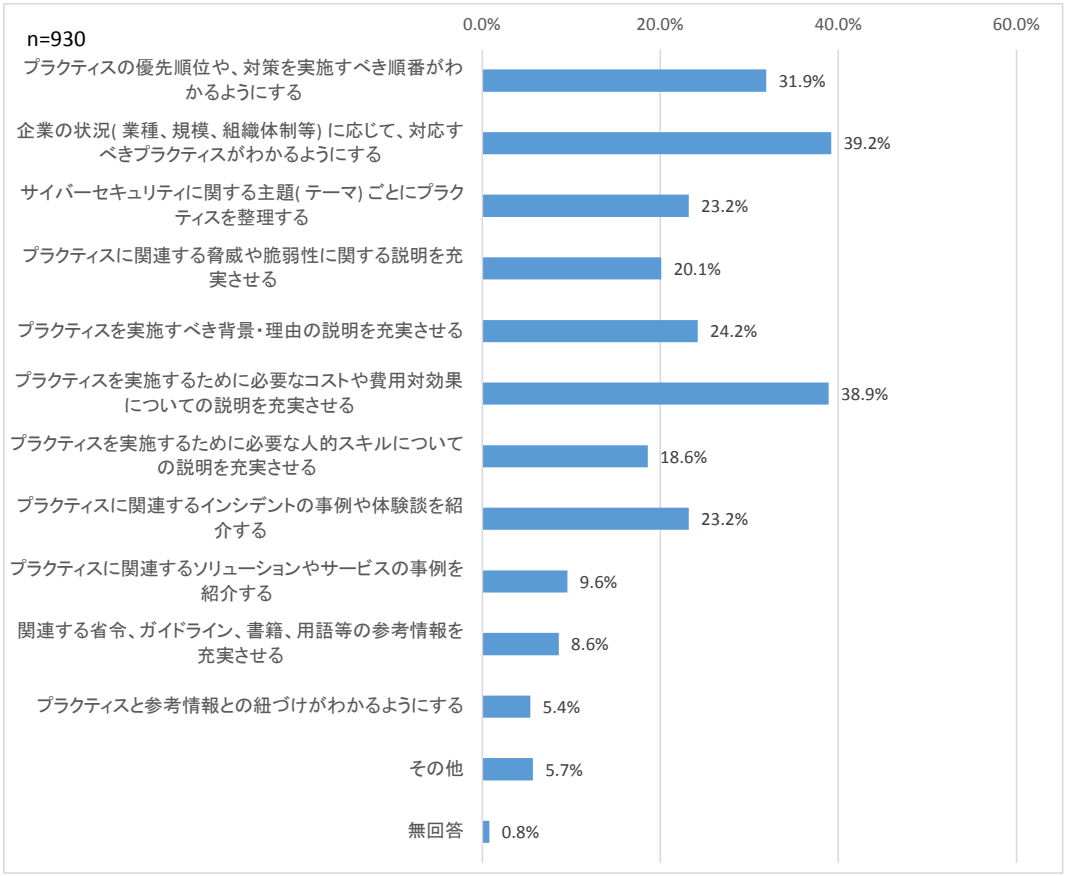
Q12.「はじめに」および「第１章」の構成・内容について、今後どのような点を改善すれば、より活用しやすくなると考えますか。最も当てはまるものを１つお選びください。(単一選択)

n	930	100.0%
背景となる課題や政策上実現したい目的について、わかりやすく解説する	126	13.5%
プラクティス集の想定読者や利用するタイミング、利用場面について、具体的に解説する	121	13.0%
企業の状況や課題に応じた利用方法、参照すべきプラクティスについて、具体的に解説する	233	25.1%
プラクティス集全体の構成と内容についての説明がなされている	46	4.9%
企業を取り巻く脅威や脆弱性に関して、全体像や考え方を解説する	144	15.5%
サイバー攻撃が経営課題である理由について、具体的に解説する	192	20.6%
その他	58	6.2%
無回答	10	1.1%



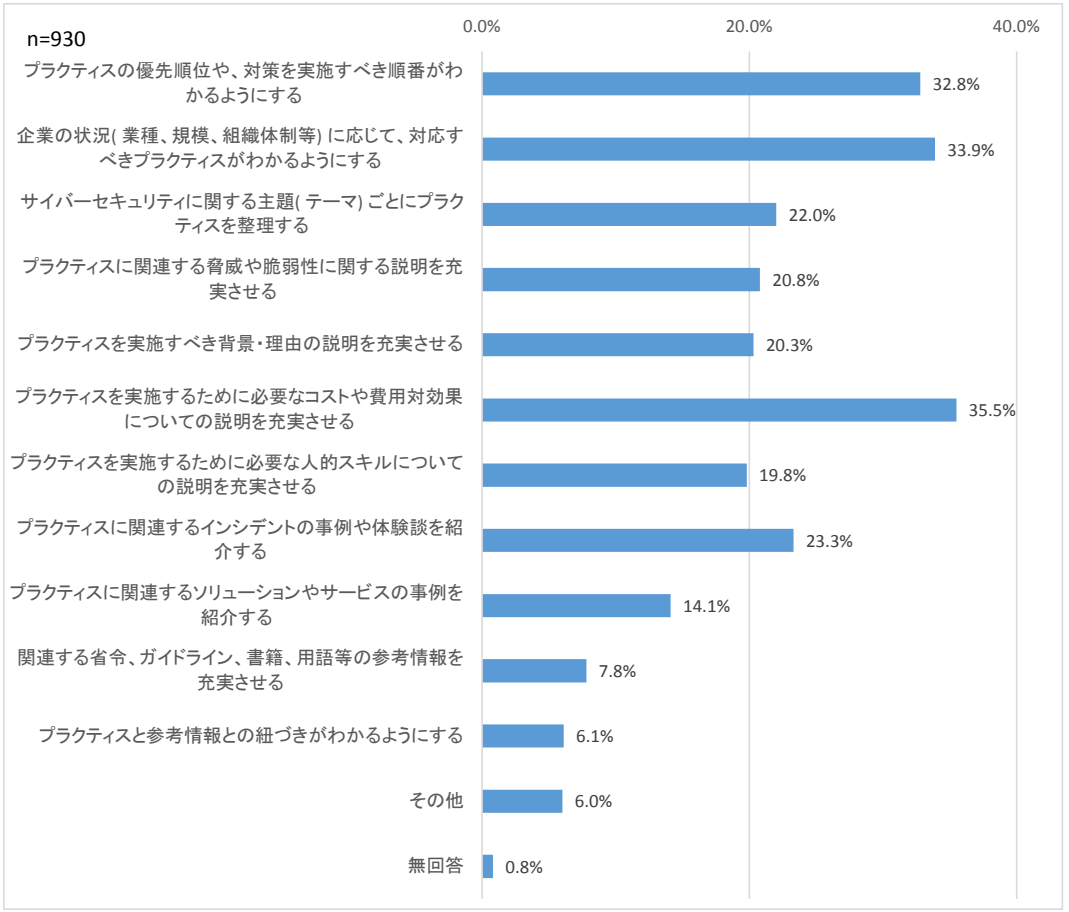
Q13.「第２章」の構成・内容について、今後どのような点を改善すれば、より活用しやすくなると考えますか。当てはまるものを最大３つまでお選びください。（３つまで複数選択可）

n	930	100.0%
プラクティスの優先順位や、対策を実施すべき順番がわかるようにする	297	31.9%
企業の状況（業種、規模、組織体制等）に応じて、対応すべきプラクティスがわかるようにする	365	39.2%
サイバーセキュリティに関する主題（テーマ）ごとにプラクティスを整理する	216	23.2%
プラクティスに関連する脅威や脆弱性に関する説明を充実させる	187	20.1%
プラクティスを実施すべき背景・理由の説明を充実させる	225	24.2%
プラクティスを実施するために必要なコストや費用対効果についての説明を充実させる	362	38.9%
プラクティスを実施するために必要な人的スキルについての説明を充実させる	173	18.6%
プラクティスに関連するインシデントの事例や体験談を紹介する	216	23.2%
プラクティスに関連するソリューションやサービスの事例を紹介する	89	9.6%
関連する省令、ガイドライン、書籍、用語等の参考情報を充実させる	80	8.6%
プラクティスと参考情報との紐づけがわかるようにする	50	5.4%
その他	53	5.7%
無回答	7	0.8%



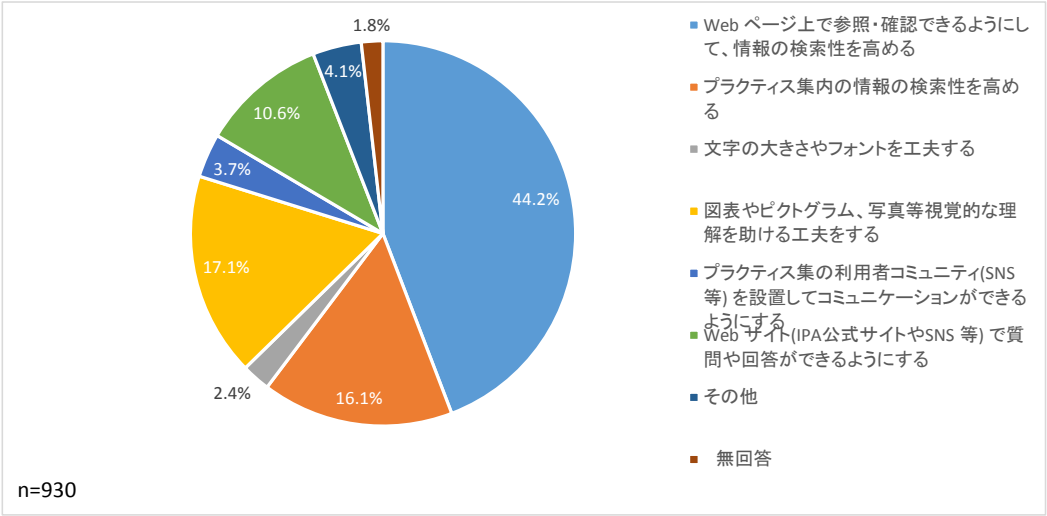
Q14.「第３章」の構成・内容について、今後どのような点を改善すれば、より活用しやすくなると考えますか。当てはまるものを最大３つまでお選びください。（３つまで複数選択可）

n	930	100.0%
プラクティスの優先順位や、対策を実施すべき順番がわかるようにする	305	32.8%
企業の状況(業種、規模、組織体制等) に応じて、対応すべきプラクティスがわかるようにする	315	33.9%
サイバーセキュリティに関する主題(テーマ) ごとにプラクティスを整理する	205	22.0%
プラクティスに関連する脅威や脆弱性に関する説明を充実させる	193	20.8%
プラクティスを実施すべき背景・理由の説明を充実させる	189	20.3%
プラクティスを実施するために必要なコストや費用対効果についての説明を充実させる	330	35.5%
プラクティスを実施するために必要な人的スキルについての説明を充実させる	184	19.8%
プラクティスに関連するインシデントの事例や体験談を紹介する	217	23.3%
プラクティスに関連するソリューションやサービスの事例を紹介する	131	14.1%
関連する省令、ガイドライン、書籍、用語等の参考情報を充実させる	73	7.8%
プラクティスと参考情報との紐づきがわかるようにする	57	6.1%
その他	56	6.0%
無回答	7	0.8%



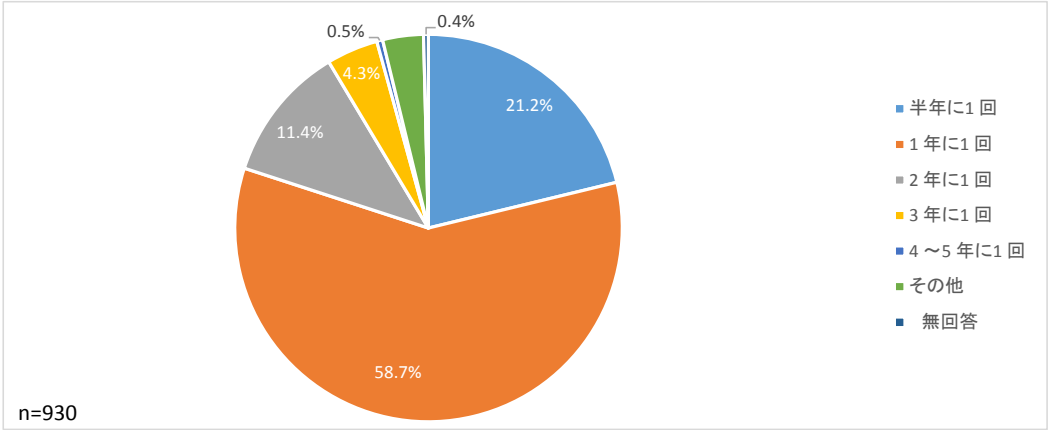
Q15. 「経営ガイドライン実践のためのプラクティス集」の提供方法・媒体についてお聞きします。今後どのような点を改善すれば、より活用しやすくなると考えますか。最も当てはまるものを１つお選びください。(単一選択)

n	930	100.0%
Web ページ上で参照・確認できるようにして、情報の検索性を高める	411	44.2%
プラクティス集内の情報の検索性を高める	150	16.1%
文字の大きさやフォントを工夫する	22	2.4%
図表やピクトグラム、写真等視覚的な理解を助ける工夫をする	159	17.1%
プラクティス集の利用者コミュニティ(SNS等) を設置してコミュニケーションができるようにする	34	3.7%
Web サイト(IPA公式サイトやSNS 等) で質問や回答ができるようにする	99	10.6%
その他	38	4.1%
無回答	17	1.8%



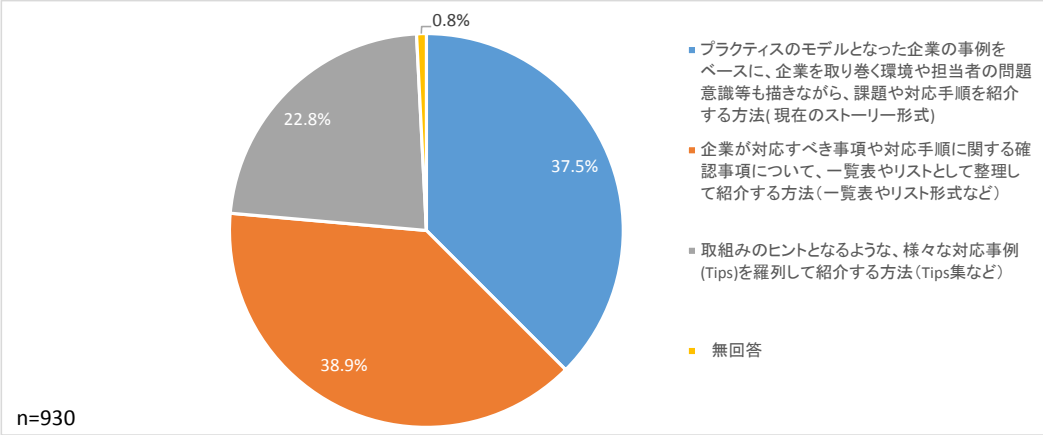
Q16. 「経営ガイドライン実践のためのプラクティス集」として、どの程度の頻度で更新(見直し)されることが望ましいと考えますか。当てはまるものを１つお選びください。(単一選択)

n	930	100.0%
半年に1 回	197	21.2%
1 年に1 回	546	58.7%
2 年に1 回	106	11.4%
3 年に1 回	40	4.3%
4 ～5 年に1 回	5	0.5%
その他	32	3.4%
無回答	4	0.4%



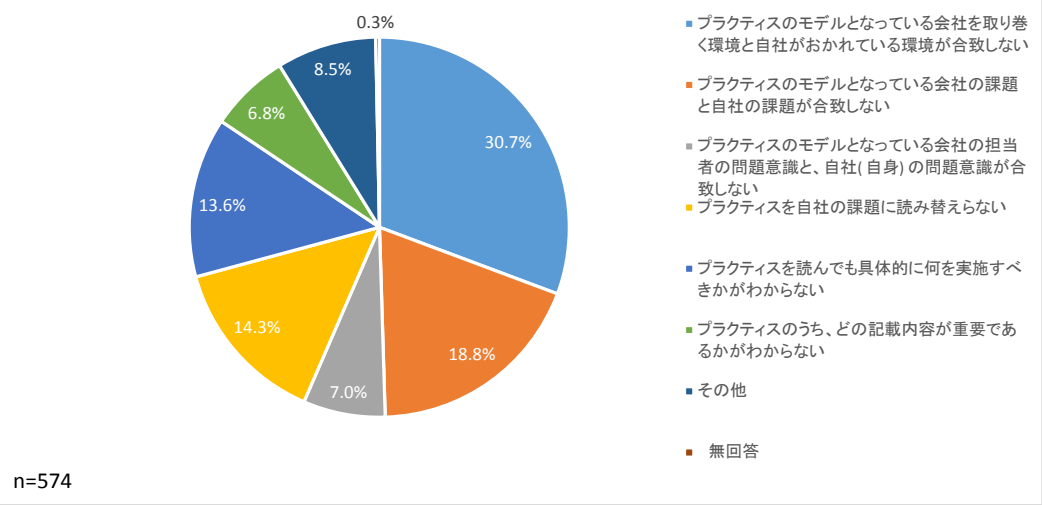
Q17. 今後、各プラクティスがどのような記載(表現)方法で紹介されていれば、自社で利用しやすいと考えますか。最も当てはまるものを１つお選びください。(単一選択)

n	930	100.0%
プラクティスのモデルとなった企業の事例をベースに、企業を取り巻く環境や担当者の問題意識等も描きながら、課題や対応手順を紹介する方法(現在のストーリー形式)	349	37.5%
企業が対応すべき事項や対応手順に関する確認事項について、一覧表やリストとして整理して紹介する方法（一覧表やリスト形式など）	362	38.9%
取組みのヒントとなるような、様々な対応事例(Tips)を羅列して紹介する方法（Tips集など）	212	22.8%
無回答	7	0.8%



Q18. (Q17で(b)(c)のいずれかを選択した方に伺います)各プラクティスの表現方法について、Q17で(a)を選択しなかった理由について、当てはまるものを１つお選びください。(単一選択)

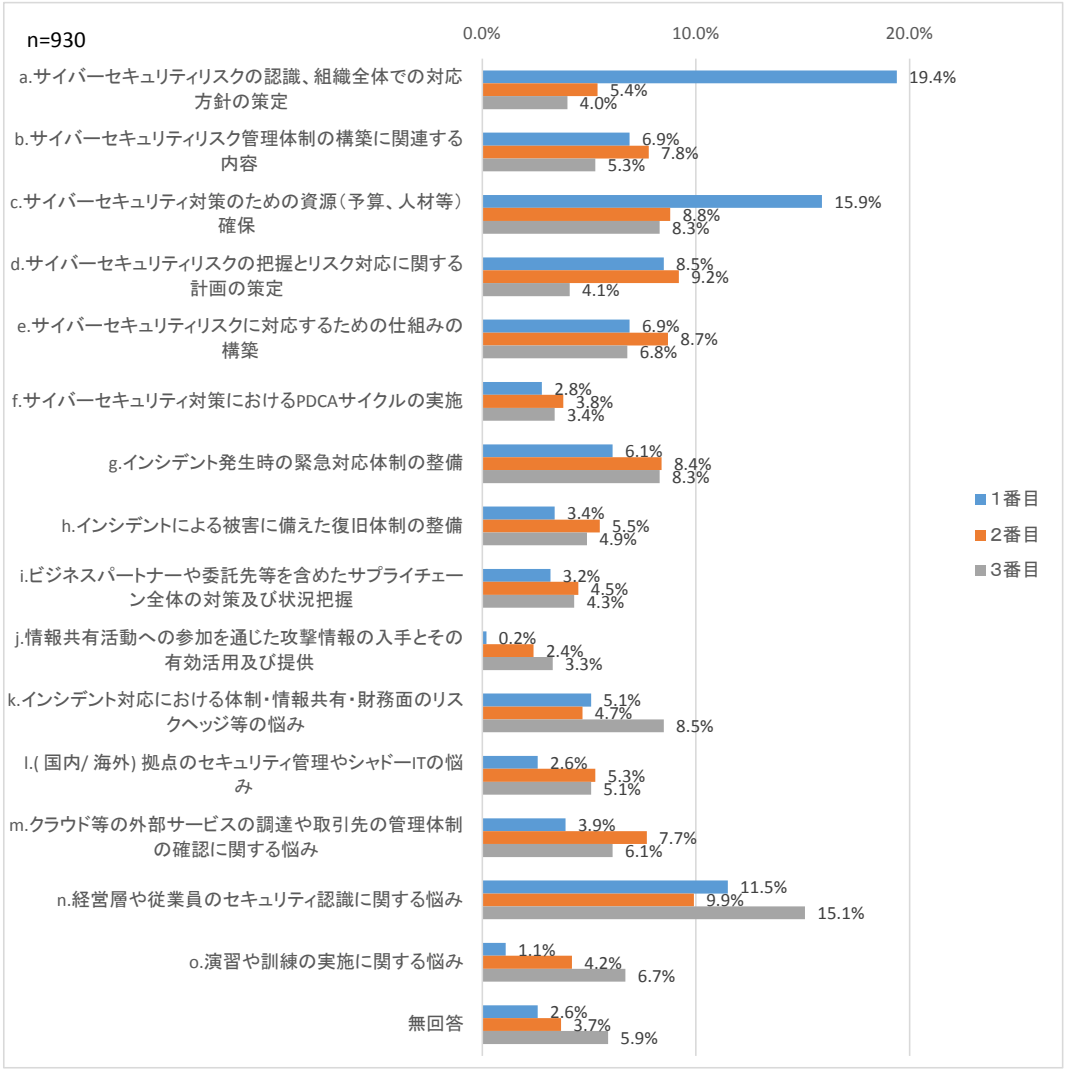
n	574	100.0%
プラクティスのモデルとなっている会社を取り巻く環境と自社がおかれている環境が合致しない	176	30.7%
プラクティスのモデルとなっている会社の課題と自社の課題が合致しない	108	18.8%
プラクティスのモデルとなっている会社の担当者の問題意識と、自社(自身) の問題意識が合致しない	40	7.0%
プラクティスを自社の課題に読み替えらない	82	14.3%
プラクティスを読んでも具体的に何を実施すべきかがわからない	78	13.6%
プラクティスのうち、どの記載内容が重要であるかがわからない	39	6.8%
その他	49	8.5%
無回答	2	0.3%



Q19. 今後、より多くのプラクティスの提供を望むテーマはどのテーマですか。当てはまるものについて、強く提供を望む順番に３つまで記載ください。（３つまで複数選択可）

１番目

n	930	100.0%
a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	180	19.4%
b.サイバーセキュリティリスク管理体制の構築に関連する内容	64	6.9%
c.サイバーセキュリティ対策のための資源（予算、人材等）確保	148	15.9%
d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	79	8.5%
e.サイバーセキュリティリスクに対応するための仕組みの構築	64	6.9%
f.サイバーセキュリティ対策におけるPDCAサイクルの実施	26	2.8%
g.インシデント発生時の緊急対応体制の整備	57	6.1%
h.インシデントによる被害に備えた復旧体制の整備	32	3.4%
i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	30	3.2%
j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	2	0.2%
k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み	47	5.1%
l.(国内/ 海外) 拠点のセキュリティ管理やシャドーITの悩み	24	2.6%
m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み	36	3.9%
n.経営層や従業員のセキュリティ認識に関する悩み	107	11.5%
o.演習や訓練の実施に関する悩み	10	1.1%
無回答	24	2.6%



２番目

n	930	100.0%
a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	50	5.4%
b.サイバーセキュリティリスク管理体制の構築に関連する内容	73	7.8%
c.サイバーセキュリティ対策のための資源（予算、人材等）確保	82	8.8%
d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	86	9.2%
e.サイバーセキュリティリスクに対応するための仕組みの構築	81	8.7%
f.サイバーセキュリティ対策におけるPDCAサイクルの実施	35	3.8%
g.インシデント発生時の緊急対応体制の整備	78	8.4%
h.インシデントによる被害に備えた復旧体制の整備	51	5.5%
i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	42	4.5%
j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	22	2.4%
k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み	44	4.7%
l.(国内/ 海外) 拠点のセキュリティ管理やシャドーITの悩み	49	5.3%
m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み	72	7.7%
n.経営層や従業員のセキュリティ認識に関する悩み	92	9.9%
o.演習や訓練の実施に関する悩み	39	4.2%
無回答	34	3.7%

３番目

n	930	100.0%
a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	37	4.0%
b.サイバーセキュリティリスク管理体制の構築に関連する内容	49	5.3%
c.サイバーセキュリティ対策のための資源（予算、人材等）確保	77	8.3%
d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	38	4.1%
e.サイバーセキュリティリスクに対応するための仕組みの構築	63	6.8%
f.サイバーセキュリティ対策におけるPDCAサイクルの実施	32	3.4%
g.インシデント発生時の緊急対応体制の整備	77	8.3%
h.インシデントによる被害に備えた復旧体制の整備	46	4.9%
i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	40	4.3%
j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	31	3.3%
k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み	79	8.5%
l.(国内/ 海外) 拠点のセキュリティ管理やシャドーITの悩み	47	5.1%
m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み	57	6.1%
n.経営層や従業員のセキュリティ認識に関する悩み	140	15.1%
o.演習や訓練の実施に関する悩み	62	6.7%
無回答	55	5.9%

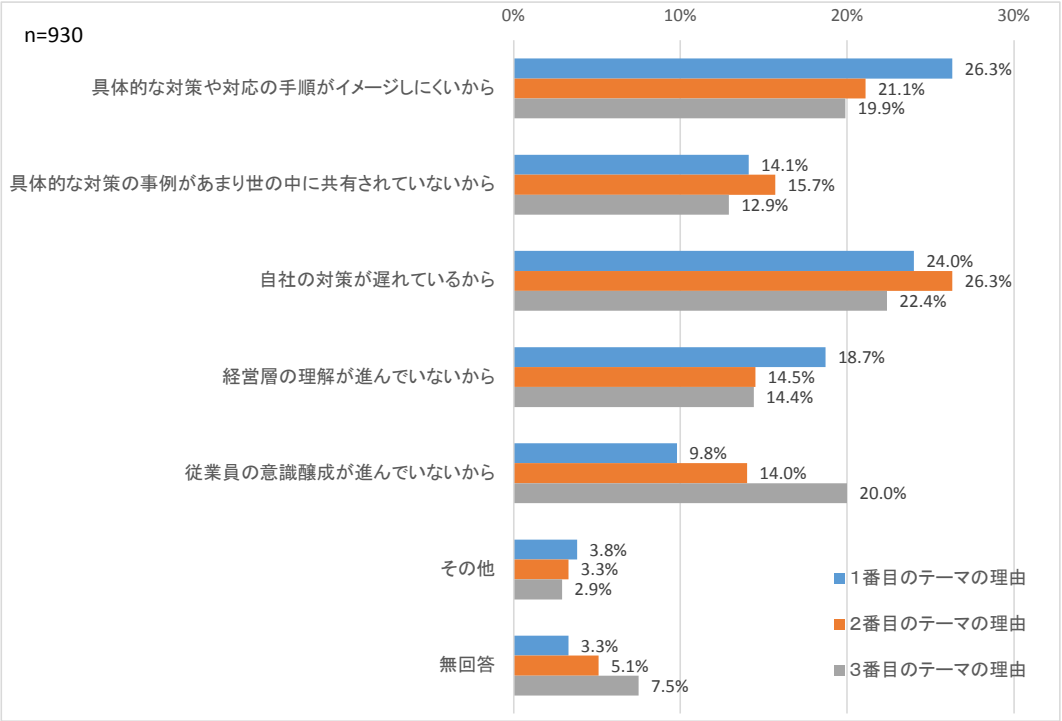
Q20. Q19で選択したそれぞれのテーマについて、プラクティスの提供を望む理由として、最も当てはまるものを、それぞれ１つずつお選びください。(単一選択)

１番目のテーマの理由

n	930	100.0%
具体的な対策や対応の手順がイメージしにくいから	245	26.3%
具体的な対策の事例があまり世の中に共有されていないから	131	14.1%
自社の対策が遅れているから	223	24.0%
経営層の理解が進んでいないから	174	18.7%
従業員の意識醸成が進んでいないから	91	9.8%
その他	35	3.8%
無回答	31	3.3%

２番目のテーマの理由

n	930	100.0%
具体的な対策や対応の手順がイメージしにくいから	196	21.1%
具体的な対策の事例があまり世の中に共有されていないから	146	15.7%
自社の対策が遅れているから	245	26.3%
経営層の理解が進んでいないから	135	14.5%
従業員の意識醸成が進んでいないから	130	14.0%
その他	31	3.3%
無回答	47	5.1%



３番目のテーマの理由

n	930	100.0%
具体的な対策や対応の手順がイメージしにくいから	185	19.9%
具体的な対策の事例があまり世の中に共有されていないから	120	12.9%
自社の対策が遅れているから	208	22.4%
経営層の理解が進んでいないから	134	14.4%
従業員の意識醸成が進んでいないから	186	20.0%
その他	27	2.9%
無回答	70	7.5%

Q21. サイバーセキュリティ経営やセキュリティ担当者の悩みに関するテーマのうち、自社の状況を踏まえた場合に、「①：業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ」、「②：業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ」いずれに当てはまると考えますか。テーマ毎に１つずつお選びください。((a)～(o)それぞれに対して単一選択)

a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定

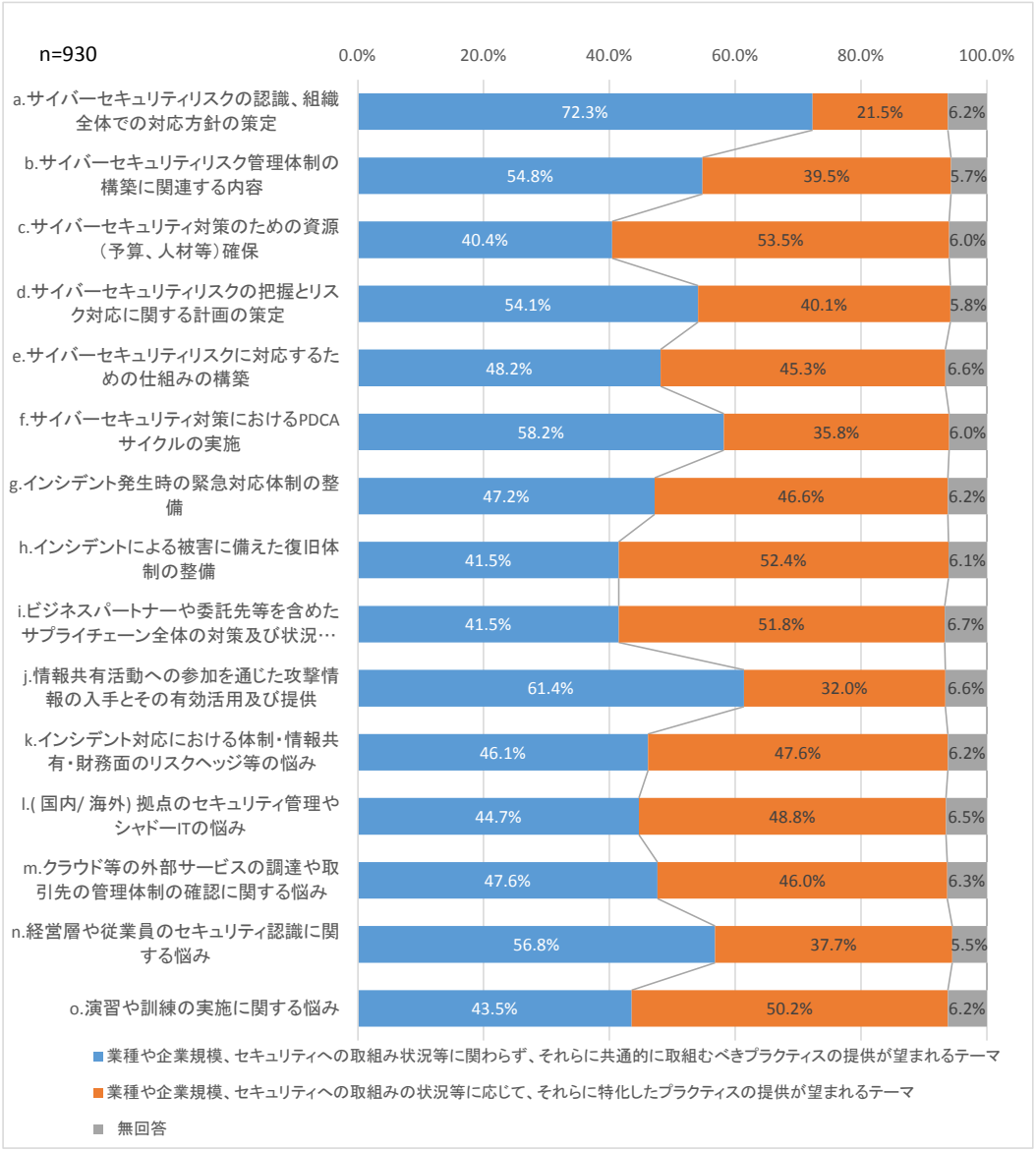
n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	672	72.3%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	200	21.5%
無回答	58	6.2%

b.サイバーセキュリティリスク管理体制の構築に関連する内容

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	510	54.8%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	367	39.5%
無回答	53	5.7%

c.サイバーセキュリティ対策のための資源（予算、人材等）確保

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	376	40.4%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	498	53.5%
無回答	56	6.0%



d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	503	54.1%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	373	40.1%
無回答	54	5.8%

e.サイバーセキュリティリスクに対応するための仕組みの構築

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	448	48.2%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	421	45.3%
無回答	61	6.6%

f.サイバーセキュリティ対策におけるPDCAサイクルの実施

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	541	58.2%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	333	35.8%
無回答	56	6.0%

g.インシデント発生時の緊急対応体制の整備

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	439	47.2%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	433	46.6%
無回答	58	6.2%

h.インシデントによる被害に備えた復旧体制の整備

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	386	41.5%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	487	52.4%
無回答	57	6.1%

i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	386	41.5%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	482	51.8%
無回答	62	6.7%

j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	571	61.4%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	298	32.0%
無回答	61	6.6%

k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	429	46.1%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	443	47.6%
無回答	58	6.2%

l.(国内/ 海外) 拠点のセキュリティ管理やシャドーITの悩み

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	416	44.7%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	454	48.8%
無回答	60	6.5%

m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	443	47.6%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	428	46.0%
無回答	59	6.3%

n.経営層や従業員のセキュリティ認識に関する悩み

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	528	56.8%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	351	37.7%
無回答	51	5.5%

o.演習や訓練の実施に関する悩み

n	930	100.0%
業種や企業規模、セキュリティへの取組み状況等に関わらず、それらに共通的に取組むべきプラクティスの提供が望まれるテーマ	405	43.5%
業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ	467	50.2%
無回答	58	6.2%

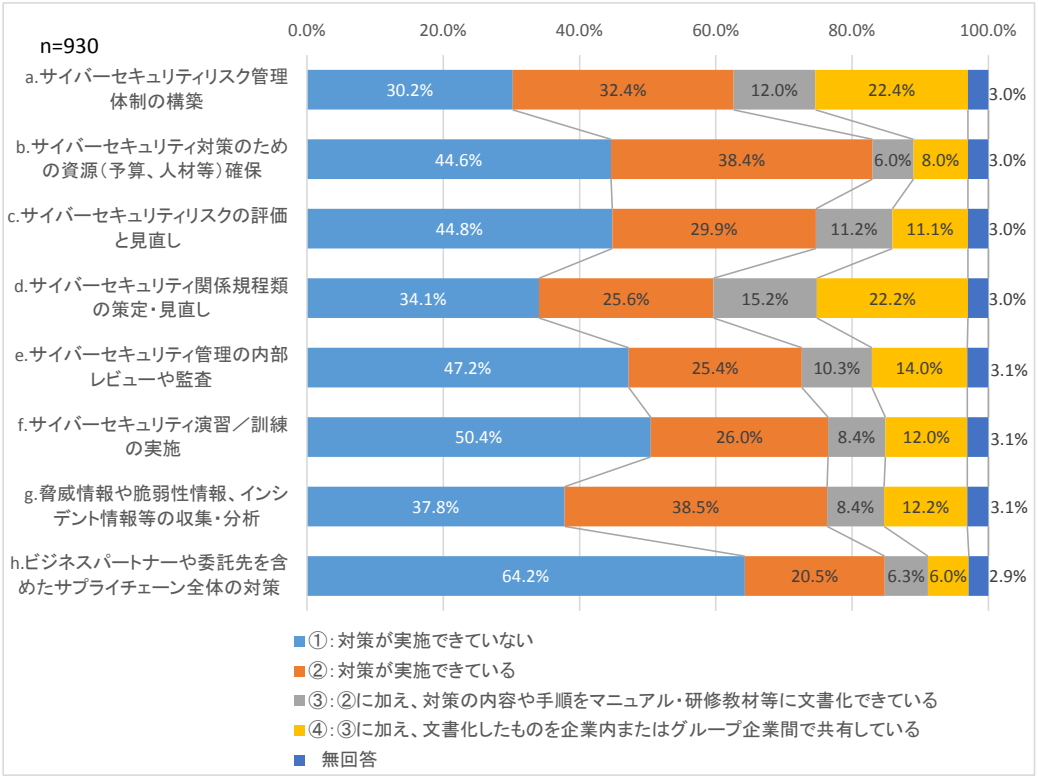
Q22.　以下のサイバーセキュリティ対策のうち、「①：対策が実施できていない」「②：対策が実施できている」「③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている」「④：③に加え、文書化したものを企業内またはグループ企業間で共有している」いずれに該当しますか。当てはまるものを1つずつお選びください。((a)～(h)それぞれに対して単一選択)

a.サイバーセキュリティリスク管理体制の構築

	n	
n	930	100.0%
①：対策が実施できていない	281	30.2%
②：対策が実施できている	301	32.4%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	112	12.0%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	208	22.4%
無回答	28	3.0%

b.サイバーセキュリティ対策のための資源（予算、人材等）確保

	n	
n	930	100.0%
①：対策が実施できていない	415	44.6%
②：対策が実施できている	357	38.4%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	56	6.0%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	74	8.0%
無回答	28	3.0%



c.サイバーセキュリティリスクの評価と見直し

n	930	100.0%
①：対策が実施できていない	417	44.8%
②：対策が実施できている	278	29.9%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	104	11.2%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	103	11.1%
無回答	28	3.0%

d.サイバーセキュリティ関係規程類の策定・見直し

n	930	100.0%
①：対策が実施できていない	317	34.1%
②：対策が実施できている	238	25.6%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	141	15.2%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	206	22.2%
無回答	28	3.0%

e.サイバーセキュリティ管理の内部レビューや監査

n	930	100.0%
①：対策が実施できていない	439	47.2%
②：対策が実施できている	236	25.4%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	96	10.3%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	130	14.0%
無回答	29	3.1%

f.サイバーセキュリティ演習／訓練の実施

n	930	100.0%
①：対策が実施できていない	469	50.4%
②：対策が実施できている	242	26.0%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	78	8.4%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	112	12.0%
無回答	29	3.1%

g.脅威情報や脆弱性情報、インシデント情報等の収集・分析

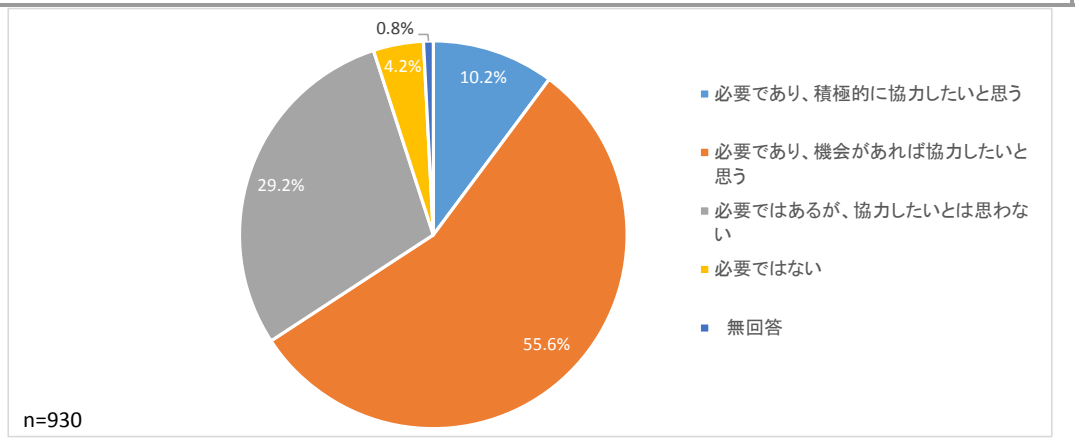
n	930	100.0%
①：対策が実施できていない	352	37.8%
②：対策が実施できている	358	38.5%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	78	8.4%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	113	12.2%
無回答	29	3.1%

h.ビジネスパートナーや委託先を含めたサプライチェーン全体の対策

n	930	100.0%
①：対策が実施できていない	597	64.2%
②：対策が実施できている	191	20.5%
③：②に加え、対策の内容や手順をマニュアル・研修教材等に文書化できている	59	6.3%
④：③に加え、文書化したものを企業内またはグループ企業間で共有している	56	6.0%
無回答	27	2.9%

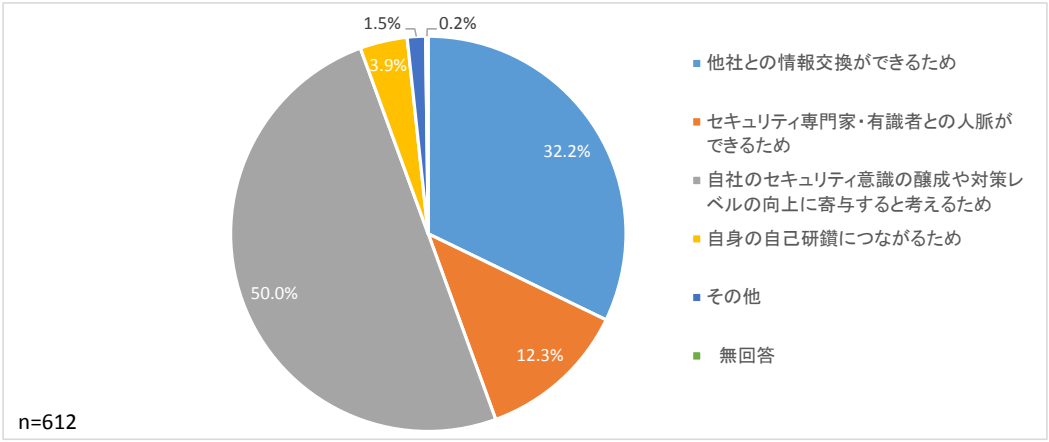
Q23. 今後こうした取組みは必要であると考えますか、またこうした取組みに自社として協力したいと考えますか。当てはまるものを1つお選びください。(単一選択)

n	930	100.0%
必要であり、積極的に協力したいと思う	95	10.2%
必要であり、機会があれば協力したいと思う	517	55.6%
必要ではあるが、協力したいとは思わない	272	29.2%
必要ではない	39	4.2%
無回答	7	0.8%



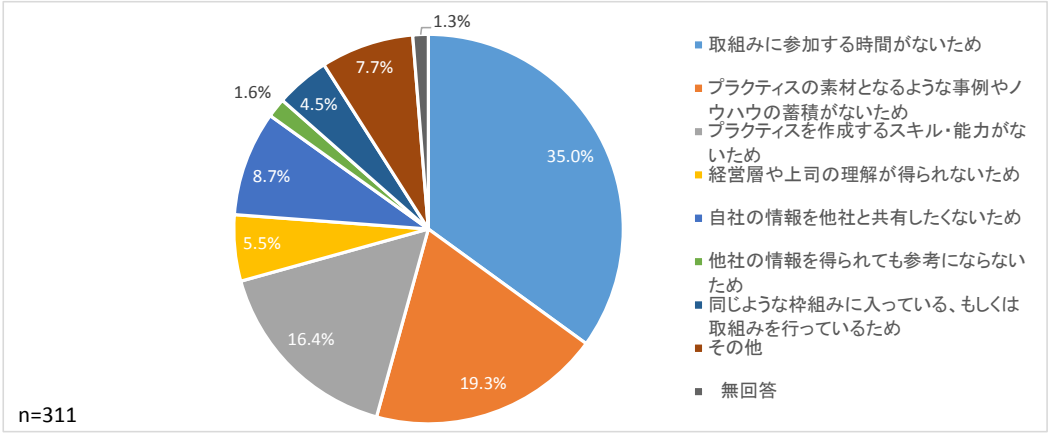
Q24. (Q23で(a)(b)のいずれかを選択した方に伺います)取組みに協力したいと思う理由は何ですか。当てはまるものを1つお選びください

n	612	100.0%
他社との情報交換ができるため	197	32.2%
セキュリティ専門家・有識者との人脈ができるため	75	12.3%
自社のセキュリティ意識の醸成や対策レベルの向上に寄与すると考えるため	306	50.0%
自身の自己研鑽につながるため	24	3.9%
その他	9	1.5%
無回答	1	0.2%



Q25. (Q23で(c)(d)のいずれかを選択した方に伺います)取組みに協力できない理由は何ですか。当てはまるものを1つお選びください

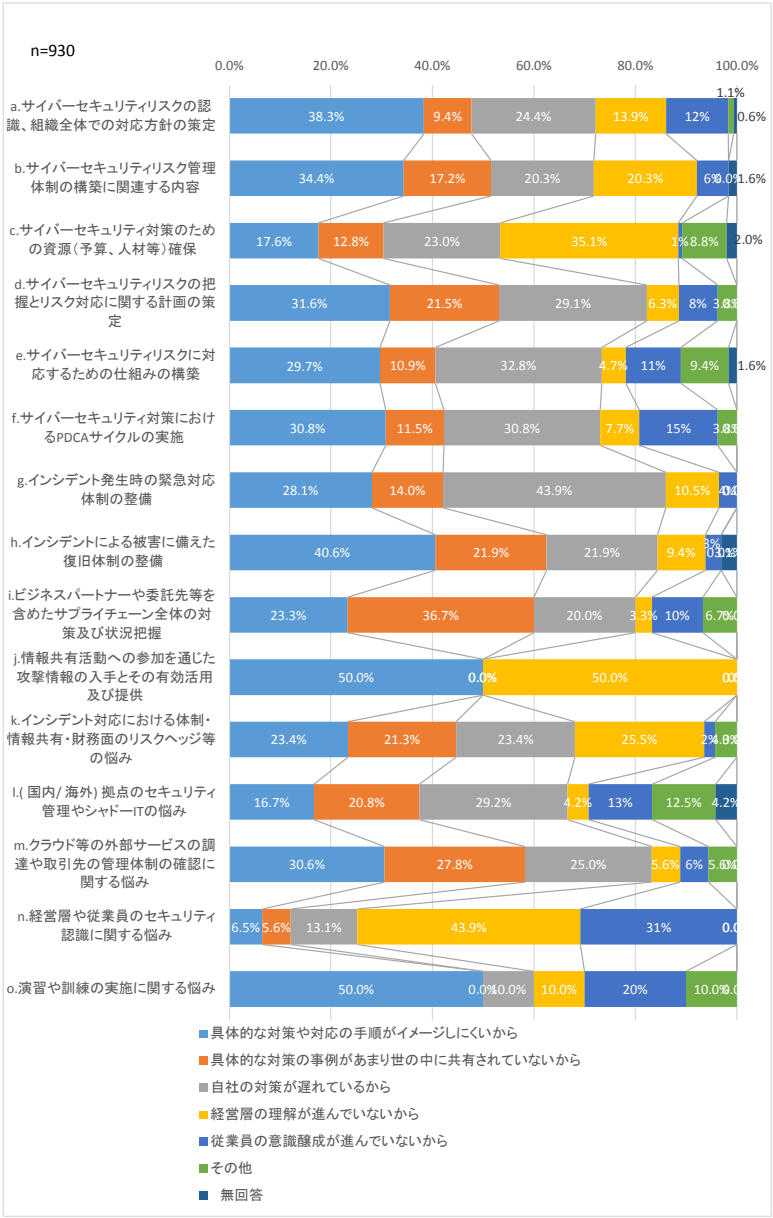
n	311	100.0%
取組みに参加する時間がないため	109	35.0%
プラクティスの素材となるような事例やノウハウの蓄積がないため	60	19.3%
プラクティスを作成するスキル・能力がないため	51	16.4%
経営層や上司の理解が得られないため	17	5.5%
自社の情報を他社と共有したくないため	27	8.7%
他社の情報を得られても参考にならないため	5	1.6%
同じような枠組みに入っている、もしくは取組みを行っているため	14	4.5%
その他	24	7.7%
無回答	4	1.3%



Q20. Q19で選択したそれぞれのテーマについて、プラクティスの提供を望む理由として、最も当てはまるものを、それぞれ１つずつお選びください。(単一選択)

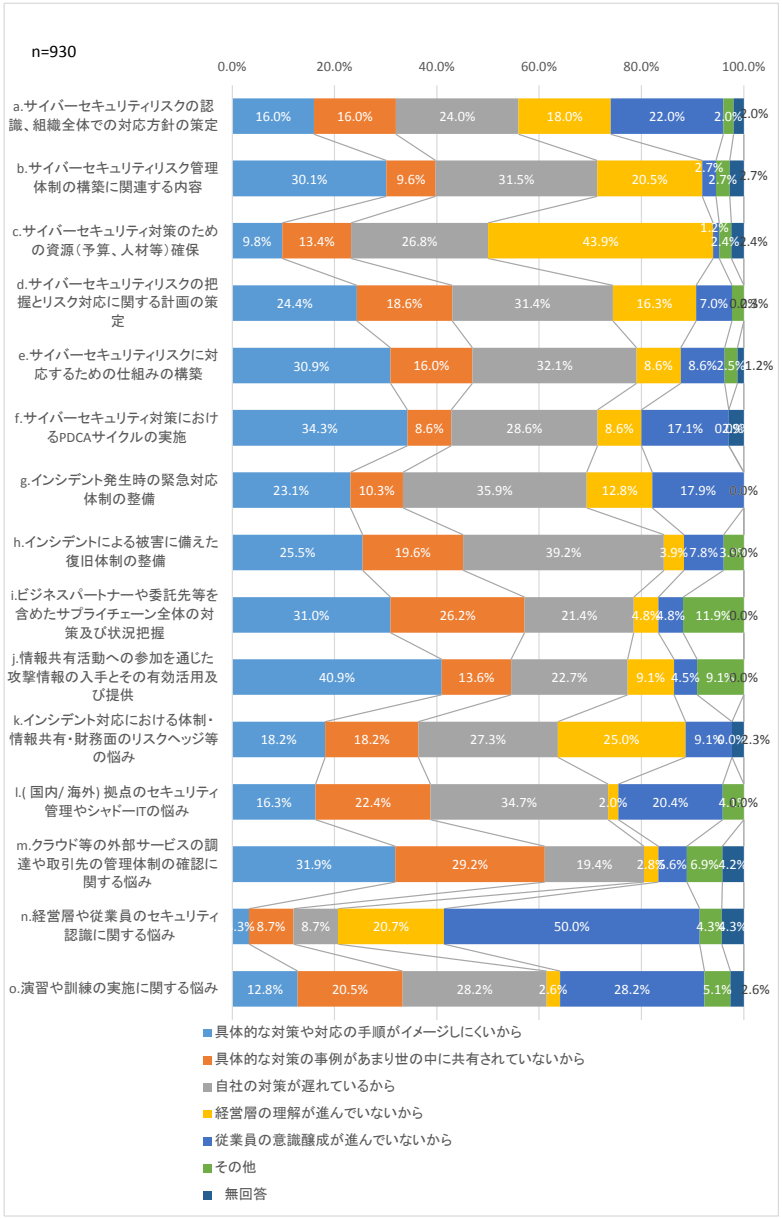
１番目のテーマの理由

		n	具体的な対策や対応の手順がイメージしにくいから	具体的な対策の事例があまり世の中に共有されていないから	自社の対策が遅れているから	経営層の理解が進んでいないから	従業員の意識醸成が進んでいないから	その他	無回答
１番目全体		930	26.3%	14.1%	24.0%	18.7%	9.8%	3.8%	3.3%
１番目	a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	180	38.3%	9.4%	24.4%	13.9%	12.2%	1.1%	0.6%
	b.サイバーセキュリティリスク管理体制の構築に関連する内容	64	34.4%	17.2%	20.3%	20.3%	6.3%	0.0%	1.6%
	c.サイバーセキュリティ対策のための資源（予算、人材等）確保	148	17.6%	12.8%	23.0%	35.1%	0.7%	8.8%	2.0%
	d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	79	31.6%	21.5%	29.1%	6.3%	7.6%	3.8%	0.0%
	e.サイバーセキュリティリスクに対応するための仕組みの構築	64	29.7%	10.9%	32.8%	4.7%	10.9%	9.4%	1.6%
	f.サイバーセキュリティ対策におけるPDCAサイクルの実施	26	30.8%	11.5%	30.8%	7.7%	15.4%	3.8%	0.0%
	g.インシデント発生時の緊急対応体制の整備	57	28.1%	14.0%	43.9%	10.5%	3.5%	0.0%	0.0%
	h.インシデントによる被害に備えた復旧体制の整備	32	40.6%	21.9%	21.9%	9.4%	3.1%	0.0%	3.1%
	i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	30	23.3%	36.7%	20.0%	3.3%	10.0%	6.7%	0.0%
	j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	2	50.0%	0.0%	0.0%	50.0%	0.0%	0.0%	0.0%
	k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み	47	23.4%	21.3%	23.4%	25.5%	2.1%	4.3%	0.0%
	l.(国内/海外)拠点のセキュリティ管理やシャドーITの悩み	24	16.7%	20.8%	29.2%	4.2%	12.5%	12.5%	4.2%
	m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み	36	30.6%	27.8%	25.0%	5.6%	5.6%	5.6%	0.0%
	n.経営層や従業員のセキュリティ認識に関する悩み	107	6.5%	5.6%	13.1%	43.9%	30.8%	0.0%	0.0%
	o.演習や訓練の実施に関する悩み	10	50.0%	0.0%	10.0%	10.0%	20.0%	10.0%	0.0%
	無回答	24	4.2%	0.0%	0.0%	0.0%	0.0%	0.0%	95.8%



２番目のテーマの理由

		n	具体的な対策や対応の手順がイメージしにくいから	具体的な対策の事例があまり世の中に共有されていないから	自社の対策が遅れているから	経営層の理解が進んでいないから	従業員の意識醸成が進んでいないから	その他	無回答
２番目全体		930	21.1%	15.7%	26.3%	14.5%	14.0%	3.3%	5.1%
２番目	a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	50	16.0%	16.0%	24.0%	18.0%	22.0%	2.0%	2.0%
	b.サイバーセキュリティリスク管理体制の構築に関連する内容	73	30.1%	9.6%	31.5%	20.5%	2.7%	2.7%	2.7%
	c.サイバーセキュリティ対策のための資源（予算、人材等）確保	82	9.8%	13.4%	26.8%	43.9%	1.2%	2.4%	2.4%
	d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	86	24.4%	18.6%	31.4%	16.3%	7.0%	2.3%	0.0%
	e.サイバーセキュリティリスクに対応するための仕組みの構築	81	30.9%	16.0%	32.1%	8.6%	8.6%	2.5%	1.2%
	f.サイバーセキュリティ対策におけるPDCAサイクルの実施	35	34.3%	8.6%	28.6%	8.6%	17.1%	0.0%	2.9%
	g.インシデント発生時の緊急対応体制の整備	78	23.1%	10.3%	35.9%	12.8%	17.9%	0.0%	0.0%
	h.インシデントによる被害に備えた復旧体制の整備	51	25.5%	19.6%	39.2%	3.9%	7.8%	3.9%	0.0%
	i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	42	31.0%	26.2%	21.4%	4.8%	4.8%	11.9%	0.0%
	j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	22	40.9%	13.6%	22.7%	9.1%	4.5%	9.1%	0.0%
	k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み	44	18.2%	18.2%	27.3%	25.0%	9.1%	0.0%	2.3%
	l.(国内/ 海外) 拠点のセキュリティ管理やシャドーITの悩み	49	16.3%	22.4%	34.7%	2.0%	20.4%	4.1%	0.0%
	m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み	72	31.9%	29.2%	19.4%	2.8%	5.6%	6.9%	4.2%
	n.経営層や従業員のセキュリティ認識に関する悩み	92	3.3%	8.7%	8.7%	20.7%	50.0%	4.3%	4.3%
	o.演習や訓練の実施に関する悩み	39	12.8%	20.5%	28.2%	2.6%	28.2%	5.1%	2.6%
	無回答	34	0.0%	0.0%	2.9%	2.9%	2.9%	0.0%	91.2%



3番目のテーマの理由

		n	具体的な対策や対応の手順がイメージしにくいから	具体的な対策の事例があまり世の中に共有されていないから	自社の対策が遅れているから	経営層の理解が進んでいないから	従業員の意識醸成が進んでいないから	その他	無回答
3番目全体		930	19.9%	12.9%	22.4%	14.4%	20.0%	2.9%	7.5%
3番目	a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	37	29.7%	16.2%	16.2%	10.8%	18.9%	5.4%	2.7%
	b.サイバーセキュリティリスク管理体制の構築に関連する内容	49	30.6%	10.2%	24.5%	20.4%	12.2%	2.0%	0.0%
	c.サイバーセキュリティ対策のための資源（予算、人材等）確保	77	15.6%	13.0%	24.7%	37.7%	5.2%	3.9%	0.0%
	d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	38	31.6%	5.3%	44.7%	5.3%	7.9%	2.6%	2.6%
	e.サイバーセキュリティリスクに対応するための仕組みの構築	63	27.0%	17.5%	25.4%	7.9%	17.5%	3.2%	1.6%
	f.サイバーセキュリティ対策におけるPDCAサイクルの実施	32	25.0%	18.8%	21.9%	12.5%	18.8%	3.1%	0.0%
	g.インシデント発生時の緊急対応体制の整備	77	29.9%	16.9%	26.0%	11.7%	11.7%	2.6%	1.3%
	h.インシデントによる被害に備えた復旧体制の整備	46	15.2%	15.2%	43.5%	4.3%	10.9%	2.2%	8.7%
	i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	40	17.5%	40.0%	17.5%	2.5%	12.5%	5.0%	5.0%
	j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	31	38.7%	16.1%	16.1%	0.0%	9.7%	16.1%	3.2%
	k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み	79	19.0%	13.9%	30.4%	20.3%	12.7%	1.3%	2.5%
	l.（国内/ 海外）拠点のセキュリティ管理やシャドーITの悩み	47	23.4%	19.1%	21.3%	4.3%	29.8%	0.0%	2.1%
	m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み	57	29.8%	12.3%	29.8%	7.0%	21.1%	0.0%	0.0%
	n.経営層や従業員のセキュリティ認識に関する悩み	140	4.3%	3.6%	10.0%	30.7%	48.6%	0.7%	2.1%
	o.演習や訓練の実施に関する悩み	62	19.4%	11.3%	19.4%	3.2%	37.1%	8.1%	1.6%
	無回答	55	0.0%	0.0%	3.6%	1.8%	0.0%	0.0%	94.5%