資料４

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

2017年度 重要インフラにおける「安全基準等の浸透状況等に関する調査」について

2018年3月20日

内閣官房　内閣サイバーセキュリティセンター(NISC)

目次

1．調査の目的、概要及び内容

◆調査目的

本調査は、重要インフラ所管省庁や業界団体等が定める「安全基準等※1」が、重要インフラ事業者等にどの程度浸透しているかを把握することを目的として、毎年、重要インフラ事業者等の情報セキュリティに関する取組状況を確認し、その分析結果を公表するものです。

本調査への回答を通じて、重要インフラ事業者等が自組織の情報セキュリティ対策の現状を確認し、改善・強化すべき方向性を把握できることを目指すと共に、本調査で得られた知見や課題は重要インフラ防護能力のための各施策へと展開します。

※1 安全基準等
業法に基づき国が定める「強制基準」、業法に準じて国が定める「推奨基準」及び「ガイドライン」、業法や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、業法や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等の総称を指す。

◆調査概要

調査対象範囲	：	重要インフラ分野の所管省庁（以降、所管省庁）にて調査対象の重要インフラ事業者等を決定
調査方法	：	以下の方法のいずれかを所管省庁が選択 ①NISCが準備する調査票（アンケート）を活用 ②各所管省庁、関連組織が独自に行う調査の結果をNISCで読み替え
調査基準日	：	調査方法①の場合、2017年3月末日 調査方法②の場合、各調査で設定した基準日

◆調査内容

①安全基準等の整備・浸透に係る事項　：　指針※2の認知、内規の策定・見直しの状況
②情報セキュリティ対策の実施に係る事項　：　PDCAサイクルに沿った具体的な情報セキュリティ対策の取組状況
③意見、要望

※2　指針
安全基準等の策定・改定に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目及び先進的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。次の各書で構成され、サイバーセキュリティ戦略本部で決定。
・重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）
・重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）対策編
・重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第１版）

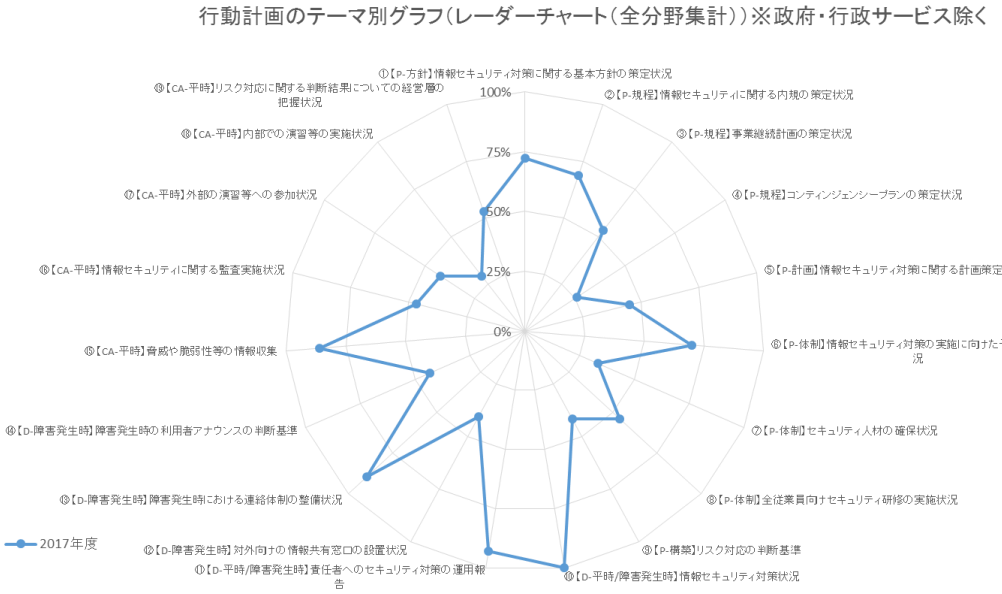
2．調査結果の要約

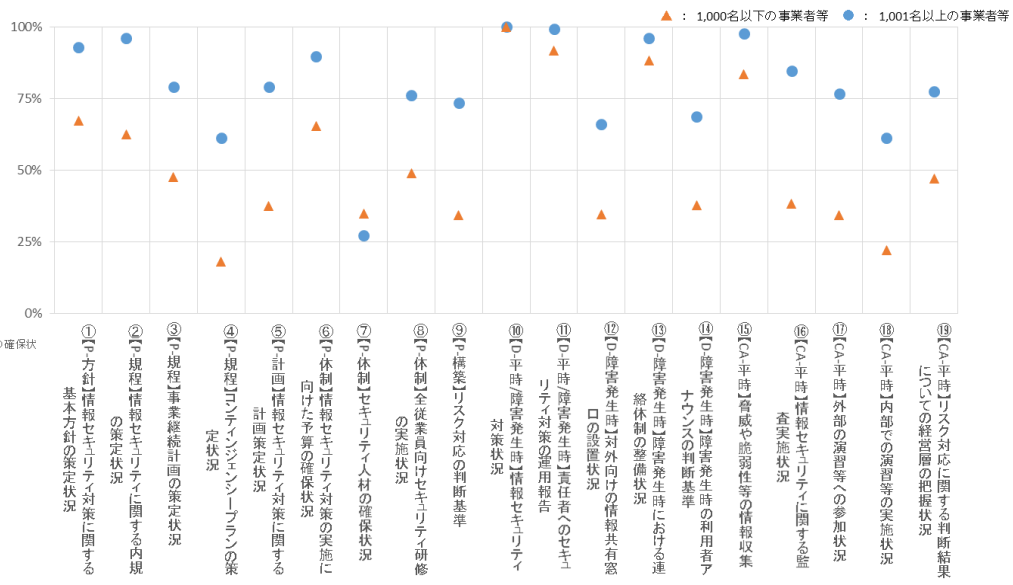
(1) 良好な点

- 事業継続計画は、9割弱の事業者等で策定されている（策定中も含む）ことから、計画策定の重要性が浸透していることがうかがえる。（設問20）
- ほぼ全ての事業者等で何らかの情報セキュリティ対策が取られていることから、セキュリティマインドが醸成されていることがうかがえる。（設問24）
- 監査を実施したほぼ全ての事業者等が対策の是正検討を行っていることから、監査の有効性がうかがえる。（設問29-1）
- 国の施策については、事業者や技術動向に則した取組となっている評価を8割程度の事業者等からいただけている。（設問38）

(2) 問題点

- 7割弱の事業者等がセキュリティ人材を確保できていない状況から、セキュリティ人材育成方法等を関係主体間で共有していく仕組みが必要である。（設問4）
- 継続して調査が行われた分野においては、CSIRTを設置した事業者等がほとんど増えていないことから、CSIRT設置を呼びかける必要性がある。（設問7）
- 基本方針策定に関しては、9割以上の事業者等において経営層が関与している状況である。しかし、リスク対応に関しては、半数の事業者等において経営層が関与していない。経営層の積極的な関与が期待される。（設問9-1、設問17）
- 機能保証の考え方を踏まえたリスクアセスメントは、十分に浸透しているとはいい難い状況である。（設問36）





(3) 今後の対応

- 機能保証の考え方を踏まえたリスクアセスメントを実施するため、公表を予定している「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」等を普及していく。
- 政府の取組に関して一定の評価をいただけているため、今後も事業者等の状況や技術動向を踏まえた上で、適切な取組を実施していく。

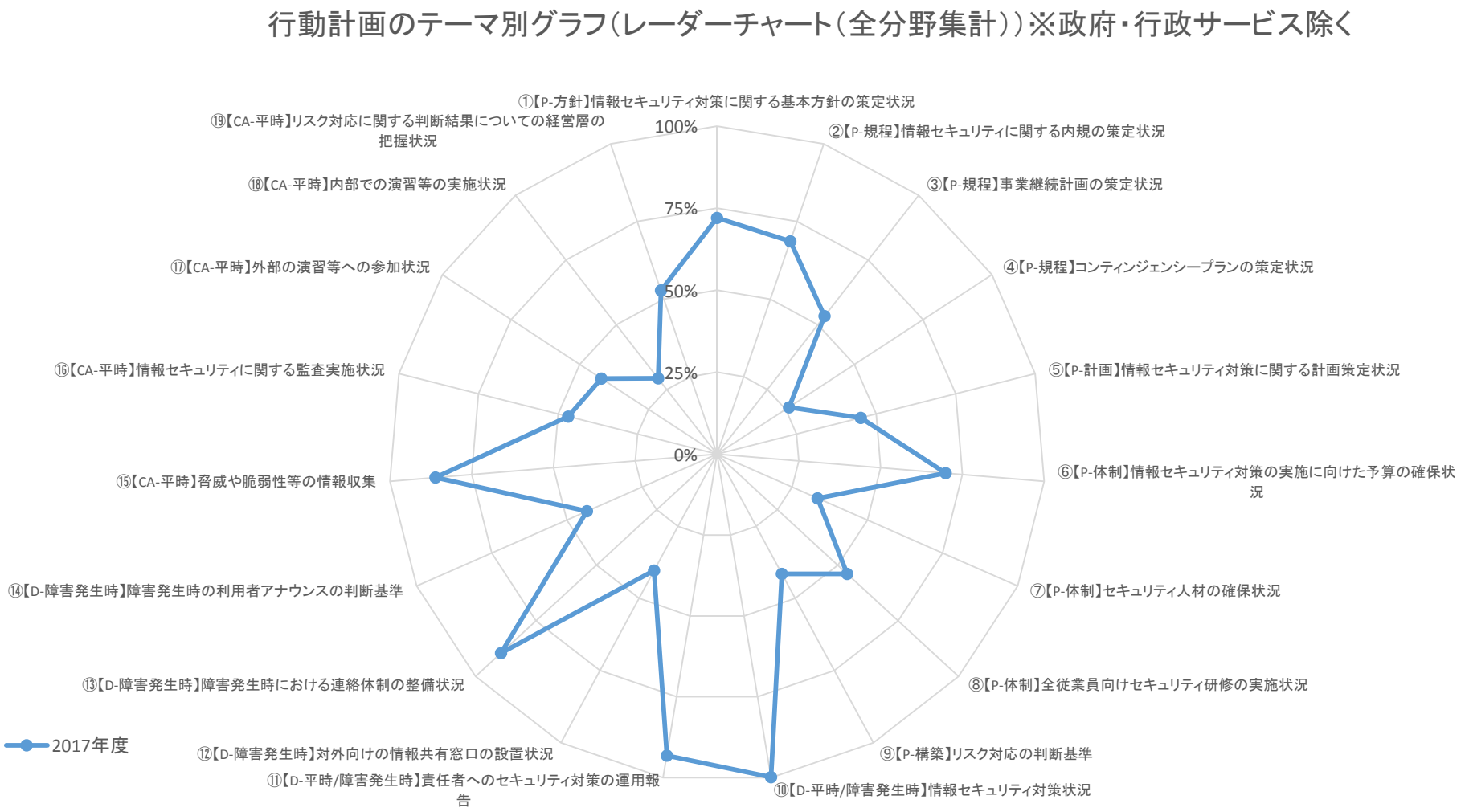
3．各重要インフラ分野の調査状況

重要インフラ分野		調査対象範囲	アンケート配布数	アンケート回収数	調査方法
情報通信	電気通信	TセプターもしくはTCAに加盟する電気通信事業者	85	36	NISC調査
	ケーブルテレビ	ケーブルテレビセプターに加盟する事業者	371	227	
	放送	日本放送協会（ＮＨＫ）、地上系民間基幹放送事業者（多重単営社及びコミュニティ放送事業者を除く）	195	195	
金融		銀行等、証券会社、生命保険会社、損害保険会社	828	665	独自調査 (*1)
航空		航空運送事業者	7	2	NISC調査
鉄道		鉄道事業者（ＪＲ，大手民鉄）	22	22	
電力		一般送配電事業者、主要な発電事業者	12	12	
ガス		大手ガス事業者	10	10	
政府・行政サービス		地方公共団体	（1,788）	（1,788）	独自調査 (*2,*3)
医療		医療情報システム導入病院	66	35	NISC調査
水道		給水人口30 万人以上の水道事業者及び同事業者に対して、その用水を供給している水道用水供給事業者	85	85	
物流		物流事業者	17	16	
化学		石油化学工業協会会員企業のうち、協会の情報セキュリティＷＧに所属している石油化学事業者	13	13	
クレジット		クレジットセプター加盟業者	28	28	
石油		石油精製企業	8	8	
全分野合計		－－－	3535	3142	－－－

＊１：金融機関等のシステムに関する動向及び安全対策実施状況調査（調査基準日：2017年3月31日）
＊２：地方自治情報管理概要　－電子自治体の推進状況－（調査基準日：2016年4月1日）URL:http://www.soumu.go.jp/main_content/000474755.pdf
＊３：本資料では集計されておりません。

4．調査結果概要　－　PDCAサイクルに沿った対策状況(1/4)　－

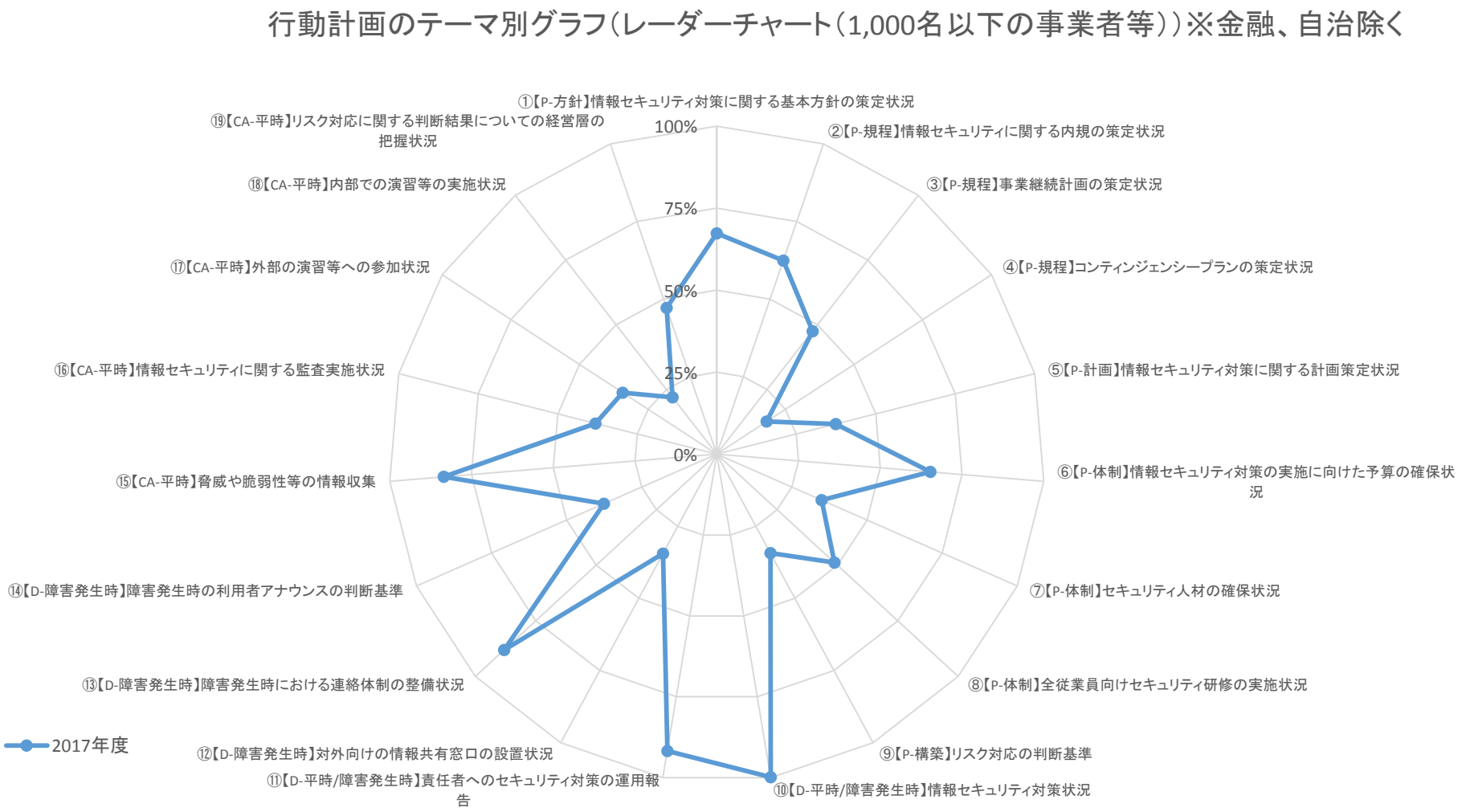
(1) 全体集計



	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	72.0%	68.6%	53.4%	26.2%	45.1%	69.9%	33.4%	53.9%	41.5%	99.9%	93.1%	40.4%	89.5%	43.3%	86.1%	46.8%	42.2%	29.3%	52.8%
2018年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

4．調査結果概要　－　PDCAサイクルに沿った対策状況(2/4)　－

(2) 従業員1,000名以下の重要インフラ事業者

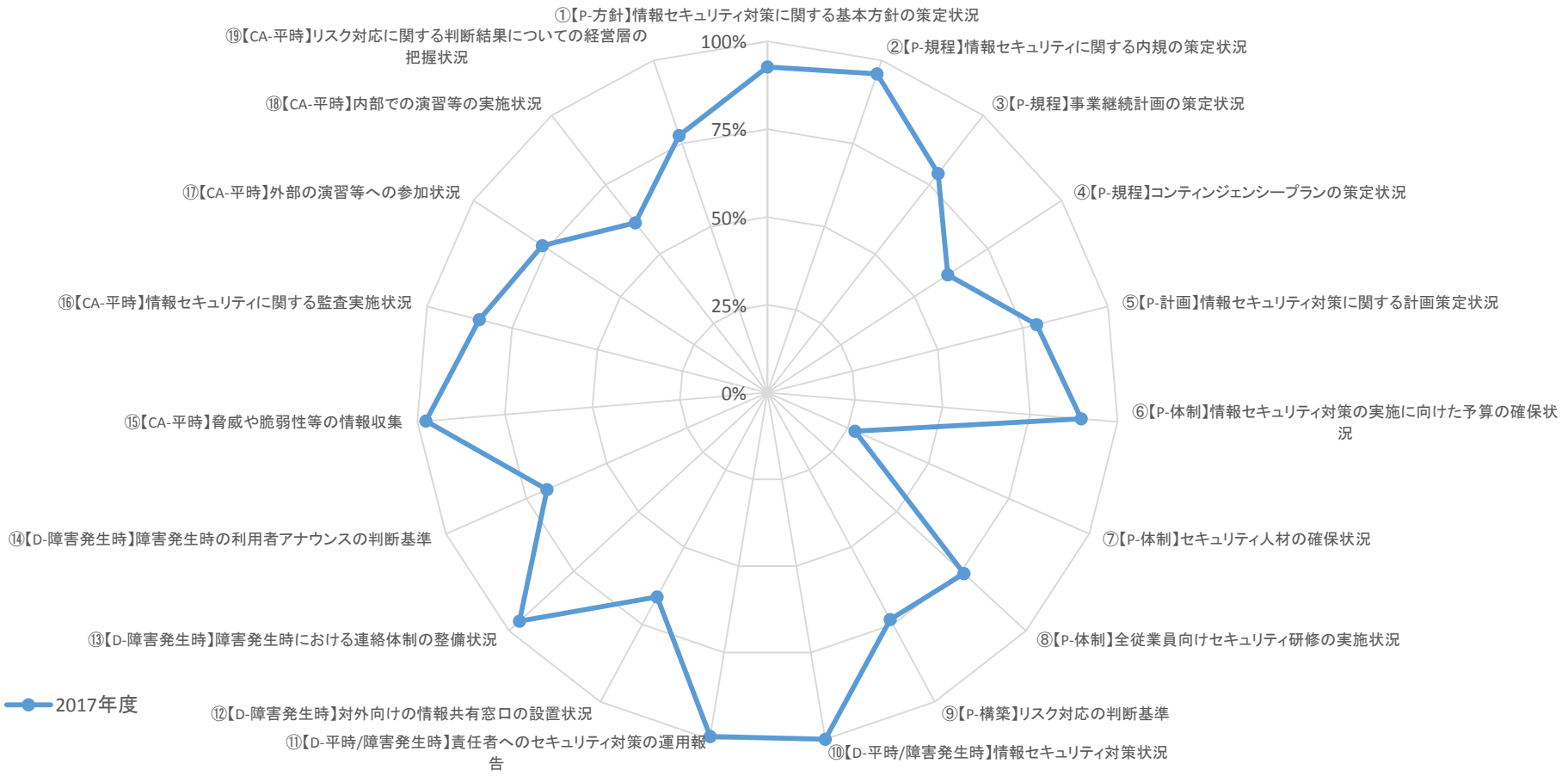


	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	67.3%	62.4%	47.5%	18.2%	37.4%	65.3%	34.9%	48.8%	34.3%	99.8%	91.7%	34.5%	88.1%	37.6%	83.5%	38.2%	34.3%	22.0%	47.2%
2018年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

4．調査結果概要　－　PDCAサイクルに沿った対策状況(3/4)　－

(3) 従業員1,001名以上の重要インフラ事業者

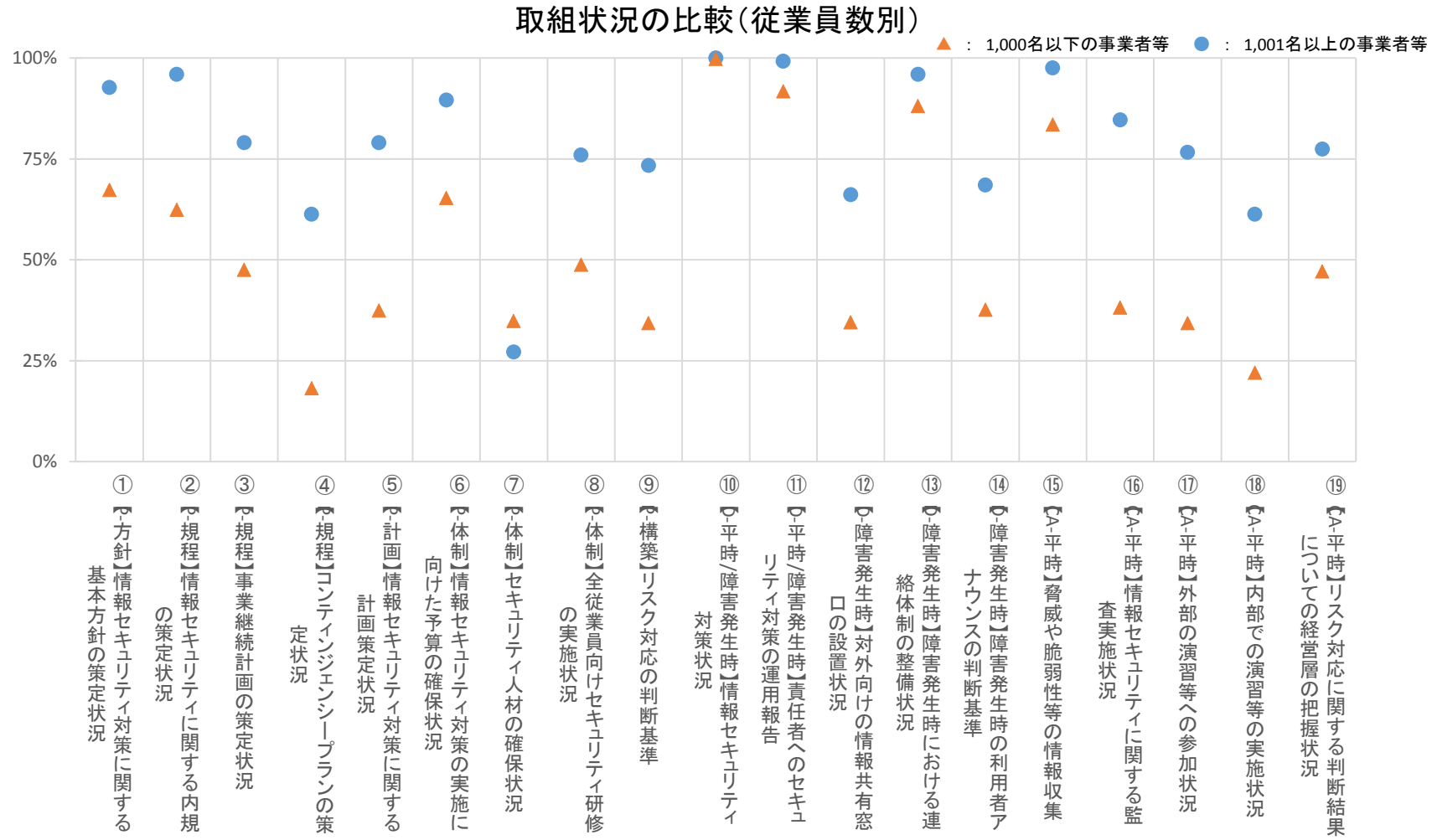
行動計画のテーマ別グラフ（レーダーチャート（1,001名以上の事業者等））※金融、自治除く



	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	92.7%	96.0%	79.0%	61.3%	79.0%	89.6%	27.2%	76.0%	73.4%	100.0%	99.2%	66.1%	96.0%	68.5%	97.6%	84.7%	76.6%	61.3%	77.4%
2018年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

4．調査結果概要　－　PDCAサイクルに沿った対策状況(4/4)　－

(4) 従業員1,000名以下と1,001名以上の重要インフラ事業者の対策状況の比較



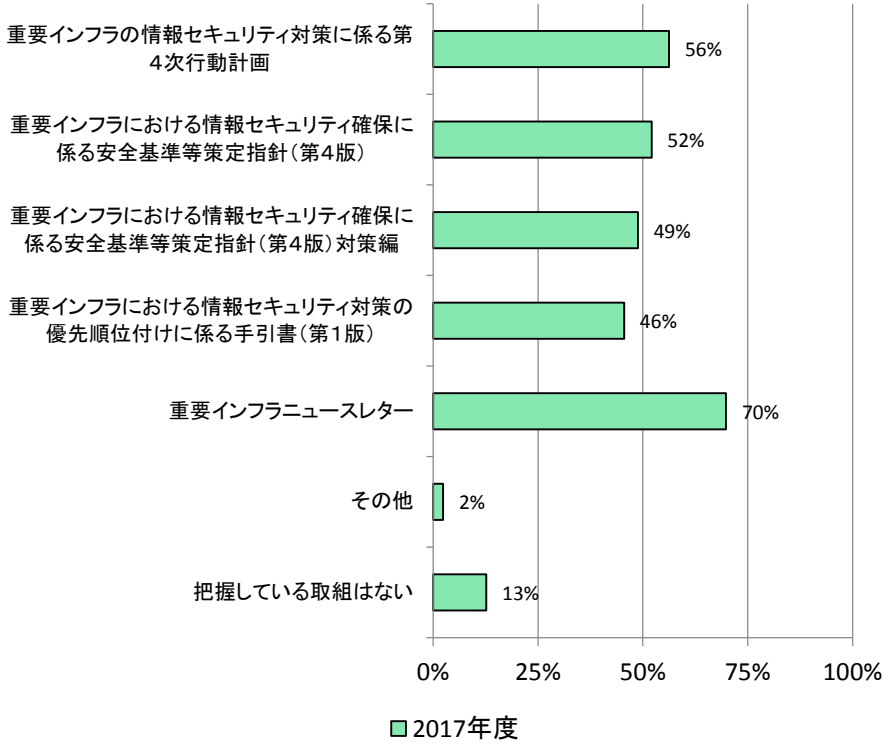
	①		②		③		④		⑤		⑥		⑦		⑧		⑨		⑩		⑪		⑫		⑬		⑭		⑮		⑯		⑰		⑱		⑲	
	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●
2017年度	67.3%	92.7%	62.4%	96.0%	47.5%	79.0%	18.2%	61.3%	37.4%	79.0%	65.3%	89.6%	34.9%	27.2%	48.8%	76.0%	34.3%	73.4%	99.8%	100.0%	91.7%	99.2%	34.5%	66.1%	88.1%	96.0%	37.6%	68.5%	83.5%	97.6%	38.2%	84.7%	34.3%	76.6%	22.0%	61.3%	47.2%	77.4%
2018年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

5．調査結果詳細 －（1/30）－

設問1　NISCの取組の認知状況

・NISCの取組を認知している事業者等は半数程度にとどまっており、更なる周知活動が必要と考えられる。
・事業者規模別に分析した結果、規模が小さくなるほど認知率が低くなる傾向がみられた。

NISCの取組の認知状況（複数回答）

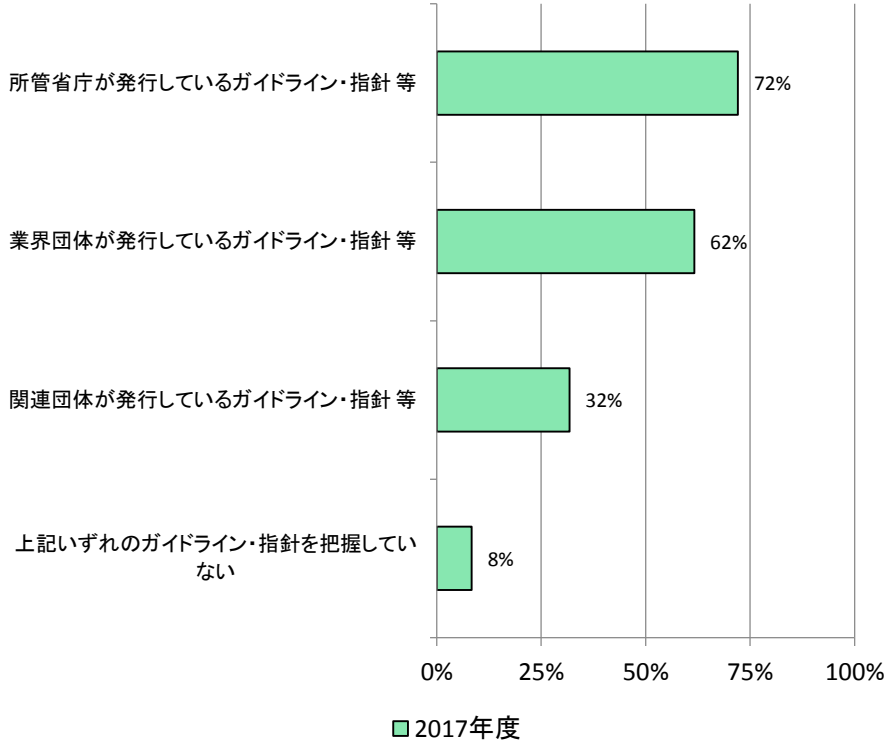


※金融は読替え可能項目なし（集計していません）

設問2　自分野の安全基準等の認知状況

・所管省庁または業界団体が発行しているガイドライン・指針等の認知率は６～７割程度となっている。発行団体からの周知や、事業者等が関心を持って情報を収集することが望まれる。

自分野の安全基準等の認知状況（複数回答）



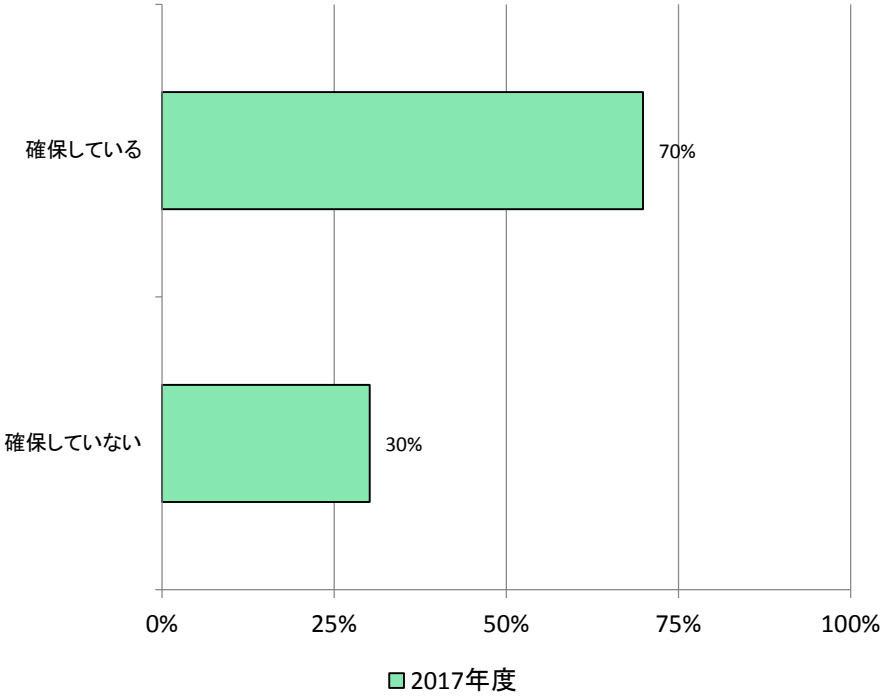
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (2/30) －

設問3　情報セキュリティ対策の実施に向けた予算の確保状況

・近年、情報漏えいやデータ等の不正利用等により、経営や事業が大きなダメージを受ける事象が発生している。このように、サイバー攻撃は経営にも大きな影響を与える可能性があるので、より多くの事業者等が経営層を巻き込んで予算を確保することが望まれる。

情報セキュリティ対策の実施に向けた予算の確保状況（単一回答）

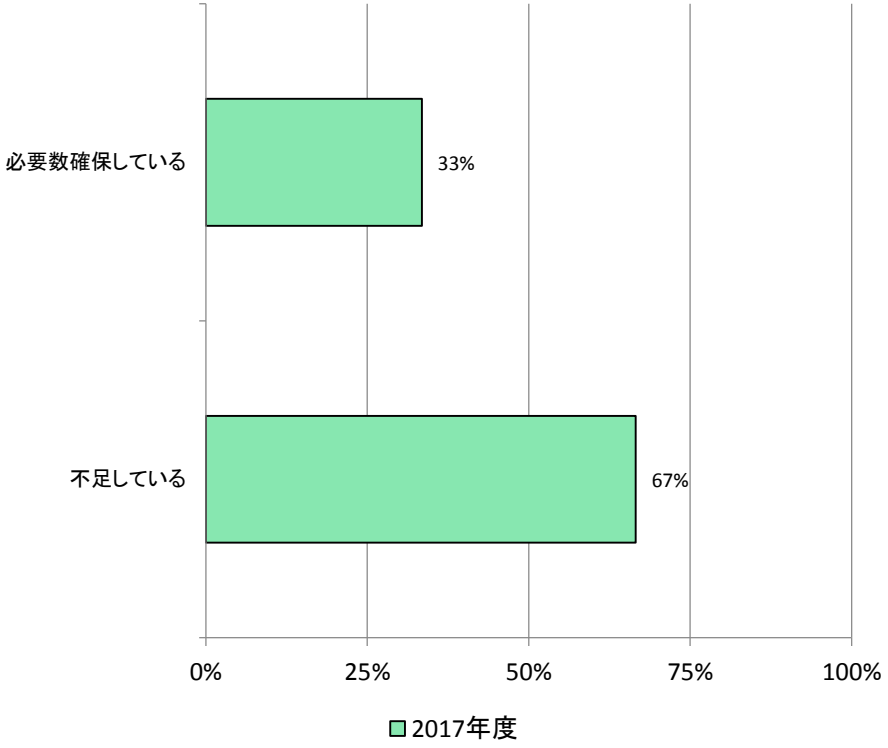


※金融は読替え可能項目なし（集計していません）

設問4　セキュリティ人材の確保状況

・セキュリティ人材に関して、7割程度の事業者等が不足していると考えていることが浮き彫りとなった。

セキュリティ人材の確保状況（単一回答）



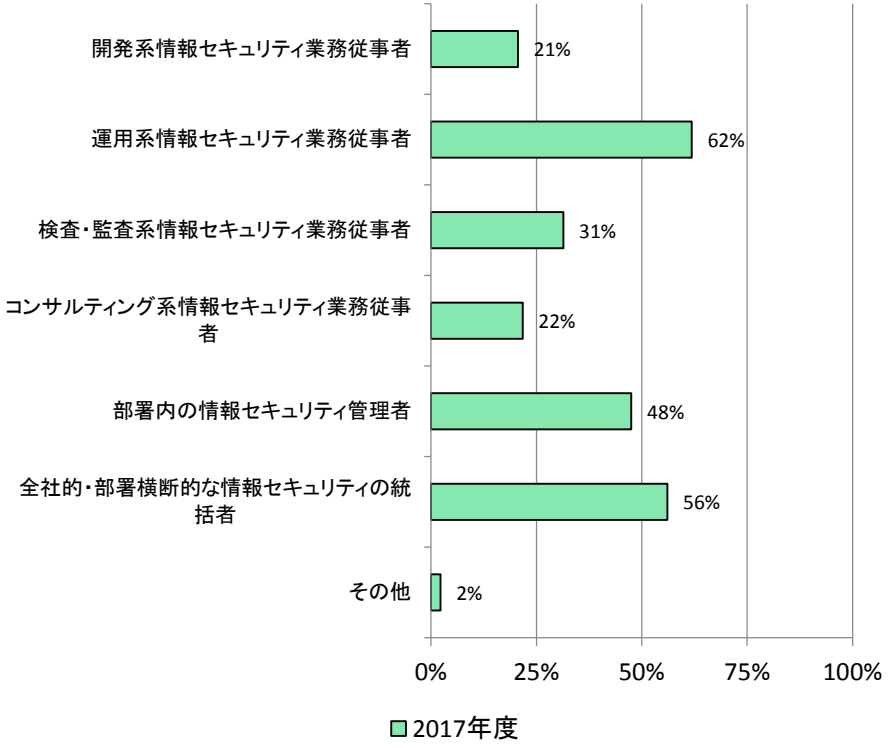
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (3/30) －

設問4-1　必要とする人材の職種

・「運用系情報セキュリティ業務従事者」、「部署内の情報セキュリティ管理者」及び「全社的・部署横断的な情報セキュリティの統括者」のニーズが高い。

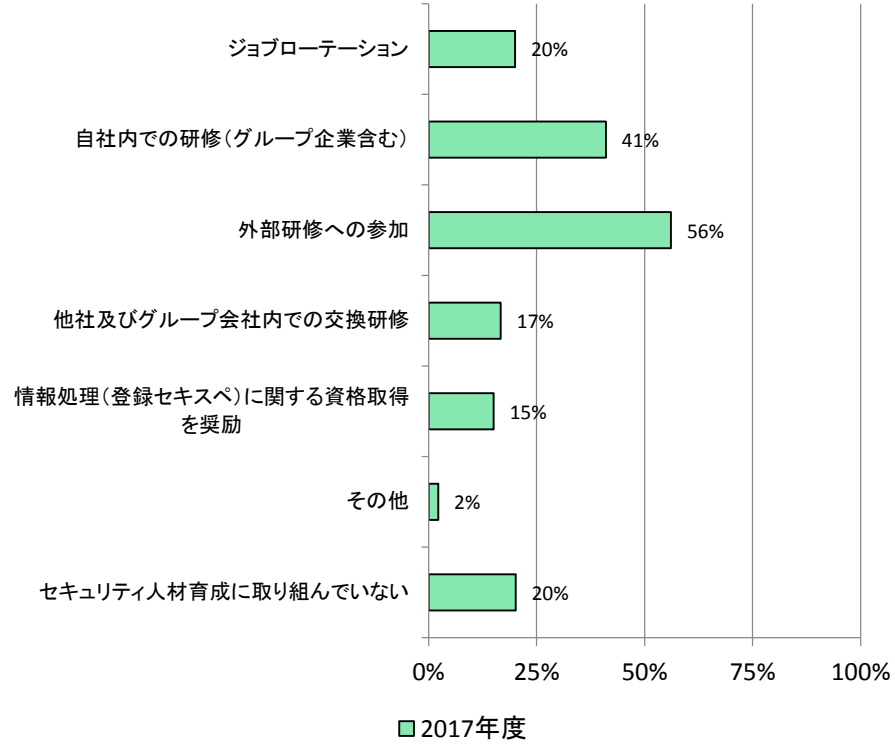
必要とする人材の職種（複数回答）



設問5　セキュリティ人材育成の取組状況

・人材育成の手段として、自社内（グループ企業含む）や外部の研修への参加が主なものとなっている。
・2割程度の事業者等が人材育成に取り組んでいないため、本設問の選択肢を参考とし、取り組むことが望まれる。

セキュリティ人材育成の取組状況（複数回答）



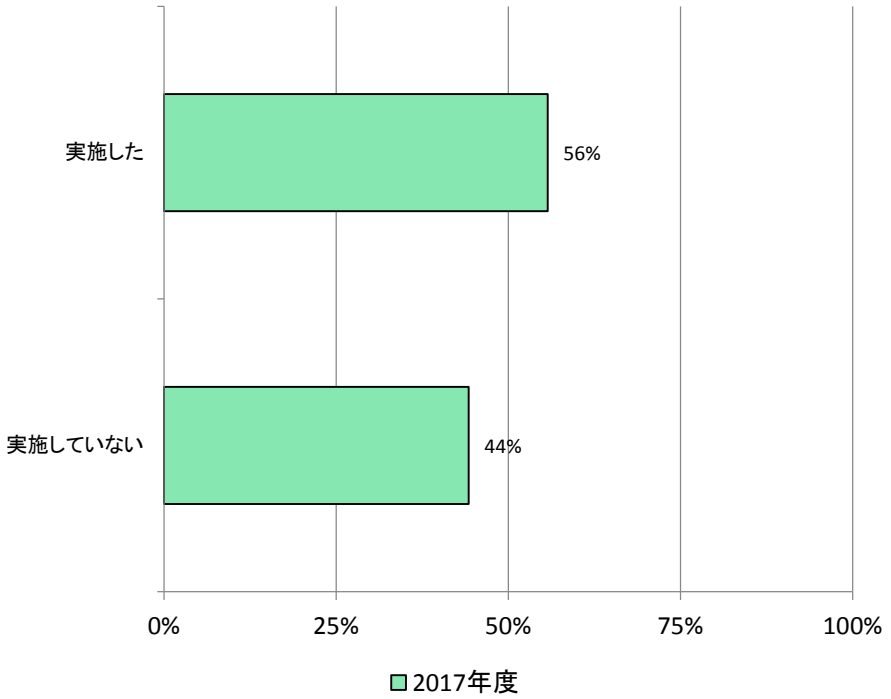
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － （4/30） －

設問6　全従業員向けセキュリティ研修の実施状況

・「サイバーセキュリティは全員参加」であるため、より多くの事業者等が、全社的にセキュリティ意識の水準を向上させる施策を実施することが望まれる。
・事業者規模別に分析した結果、特に小規模事業者等では、実施率が低いため、全従業員向けのセキュリティ研修を実施することが望まれる。

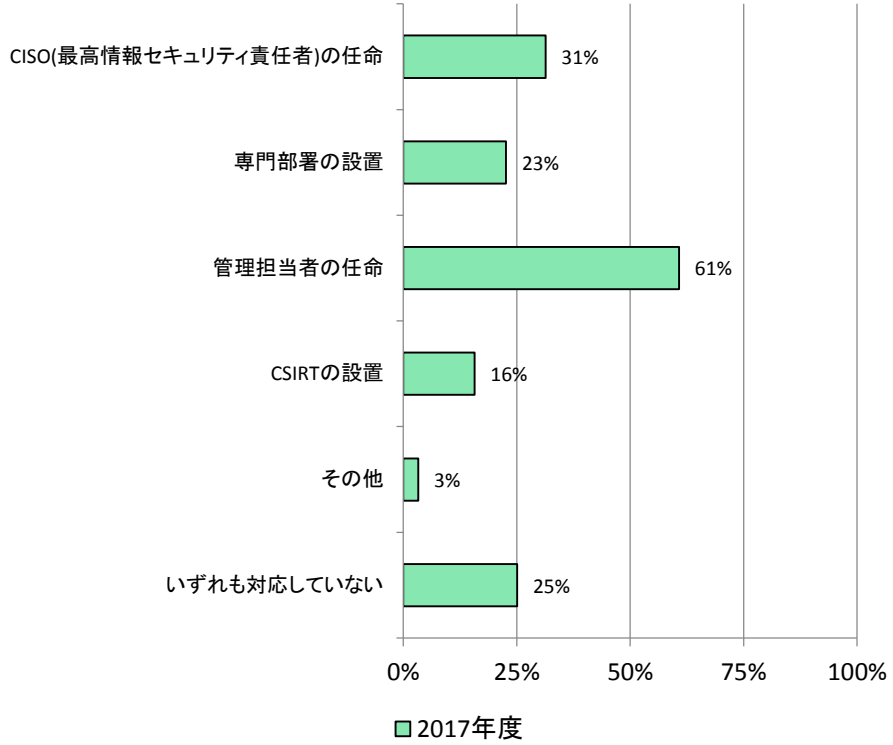
全従業員向けセキュリティ研修の実施状況（単一回答）



設問7　内部体制の取組状況

・「CSIRTの設置」について、「インシデントの一元管理」、「インシデント対応の統一的窓口」、「外部とのインシデント共有関係の構築」といった様々なメリットがあるが、今年度のCSIRT設置は2割程度となっており、CSIRTの設置が望まれる。

内部体制の取組状況（複数回答）

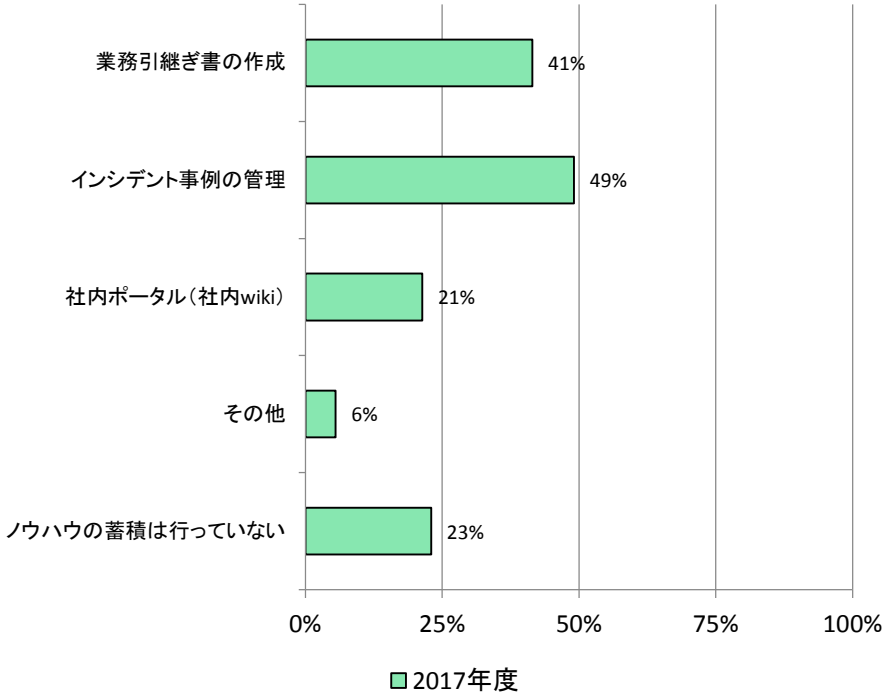


5．調査結果詳細 －（5/30）－

設問8　情報セキュリティ対策のノウハウの蓄積方法

・「情報セキュリティは一日にしてならず」、であるため、本設問の選択肢を参考とし、ノウハウの蓄積を行っていくことが望まれる。

情報セキュリティ対策のノウハウの蓄積方法
（複数回答）

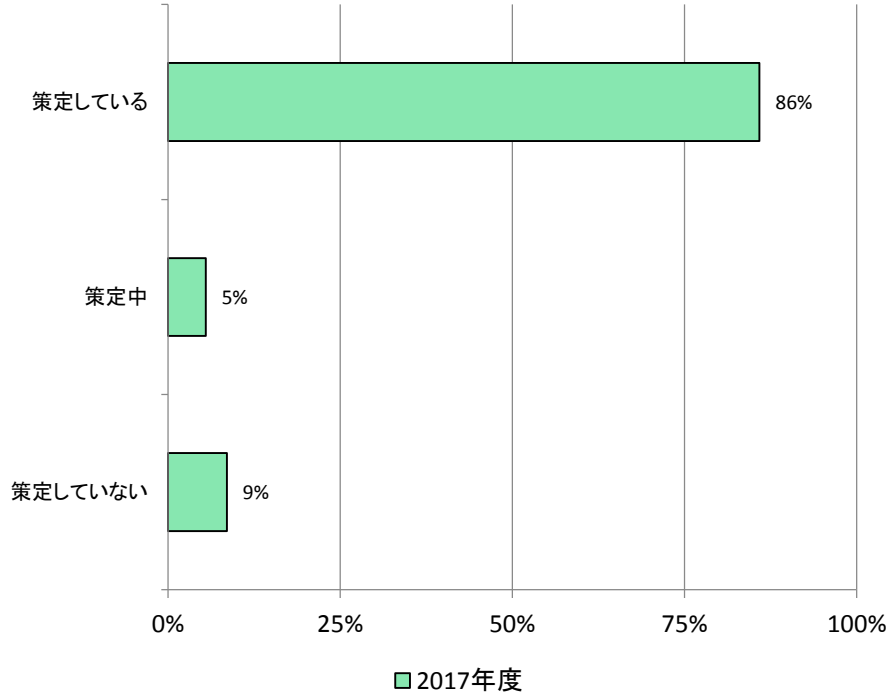


※金融は読替え可能項目なし（集計していません）

設問9　情報セキュリティ対策に関する基本方針の策定状況

・1割程度の事業者等が情報セキュリティ対策に関する基本方針を策定していない。基本方針は、情報セキュリティマネジメントシステムを構築する上で一番の基本となるため、策定されていることが強く望まれる。

情報セキュリティ対策に関する
基本方針の策定状況（単一回答）

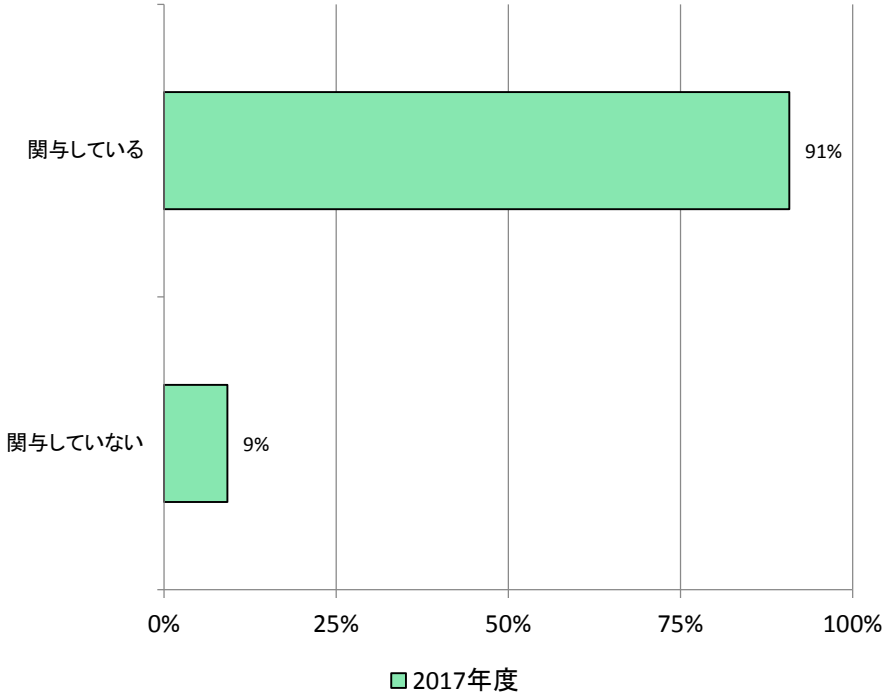


5．調査結果詳細 － (6/30) －

設問9-1　基本方針の策定に関する経営層の関与状況

・基本方針の策定に関与している経営層は9割程度であるが、より実効的な基本方針とするため、経営層の積極的な関与が望まれる。

基本方針の策定に関する経営層の関与状況
（単一回答）

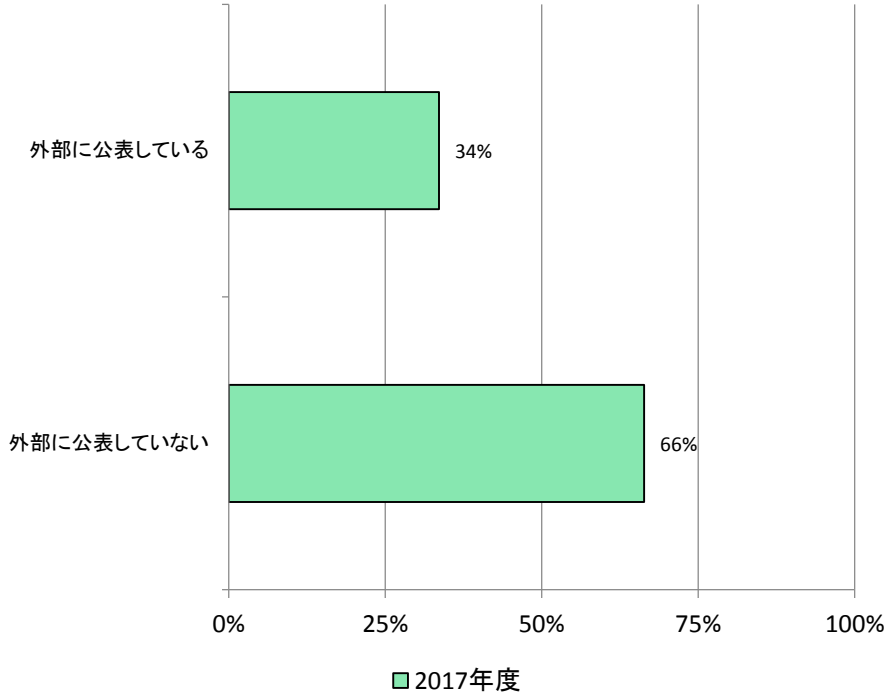


※金融は読替え可能項目なし（集計していません）

設問9-2　策定した基本方針の外部公表状況

・策定した基本方針については、3割程度の事業者等が外部に公表している。

策定した基本方針の外部公表状況
（単一回答）



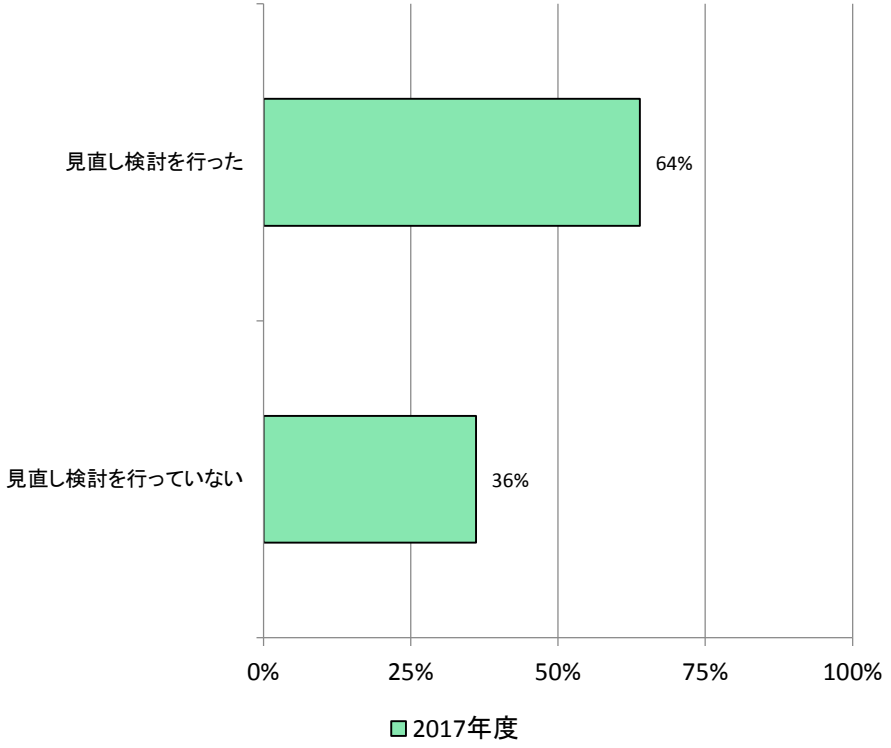
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (7/30) －

設問9-3　基本方針の見直し検討状況

・基本方針の見直し検討を行った事業者等は、6割程度であった。

基本方針の見直し検討状況（単一回答）

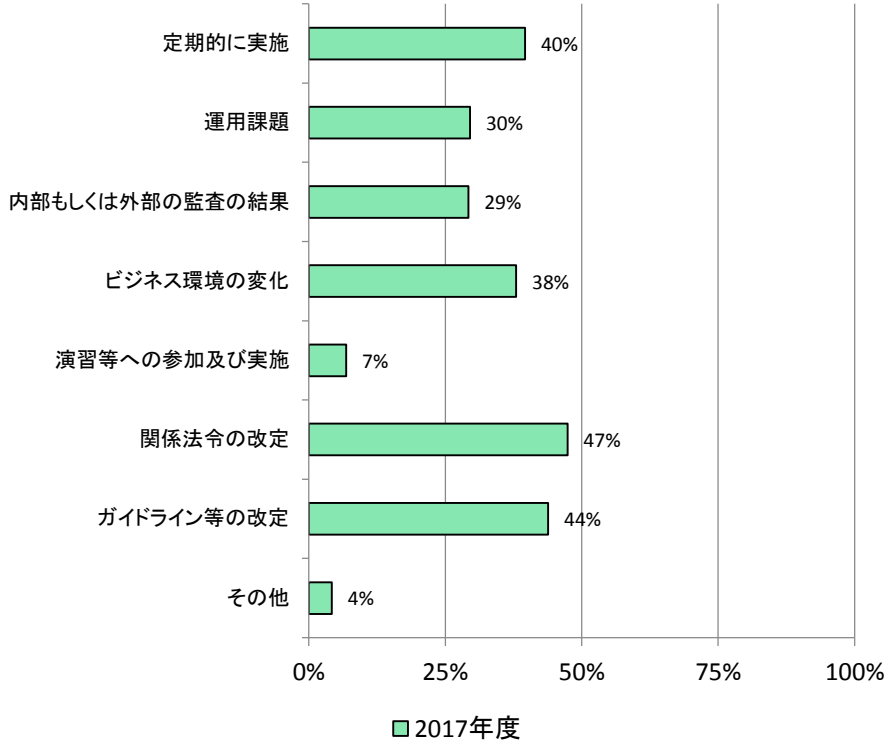


※金融は読替え可能項目なし（集計していません）

設問9-4　基本方針の見直し検討の契機

・基本方針の見直しについては、本設問の選択肢の契機を参考とし、必要に応じて実施することが望まれる。

基本方針の見直し検討の契機（複数回答）



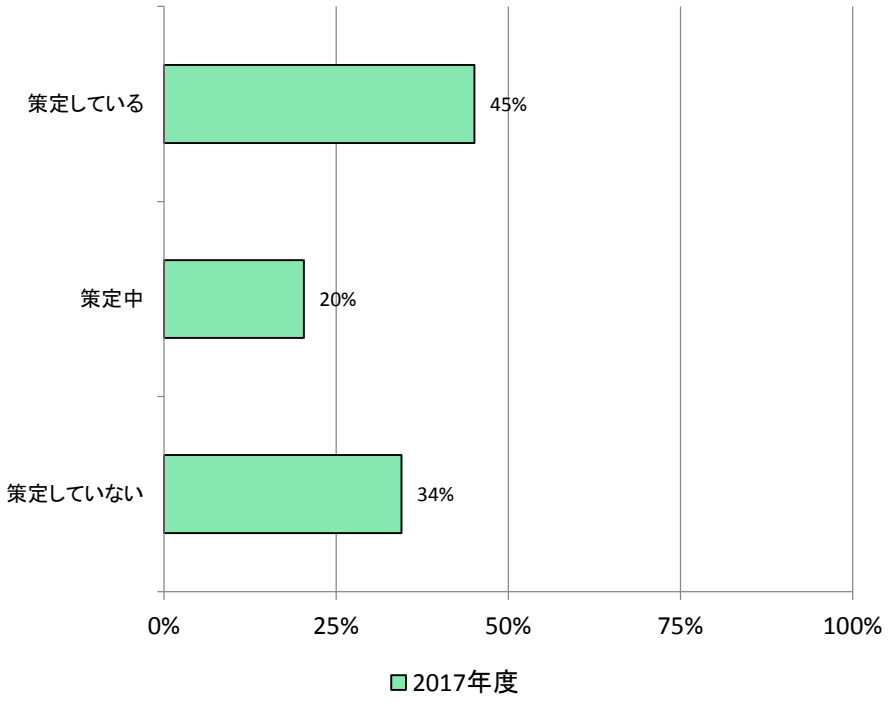
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (8/30) －

設問10　情報セキュリティ対策に関する計画策定状況

・情報セキュリティ対策に関する計画を策定していない3割程度の事業者等においては、計画を策定することが望まれる。

情報セキュリティ対策に関する計画策定状況（単一回答）

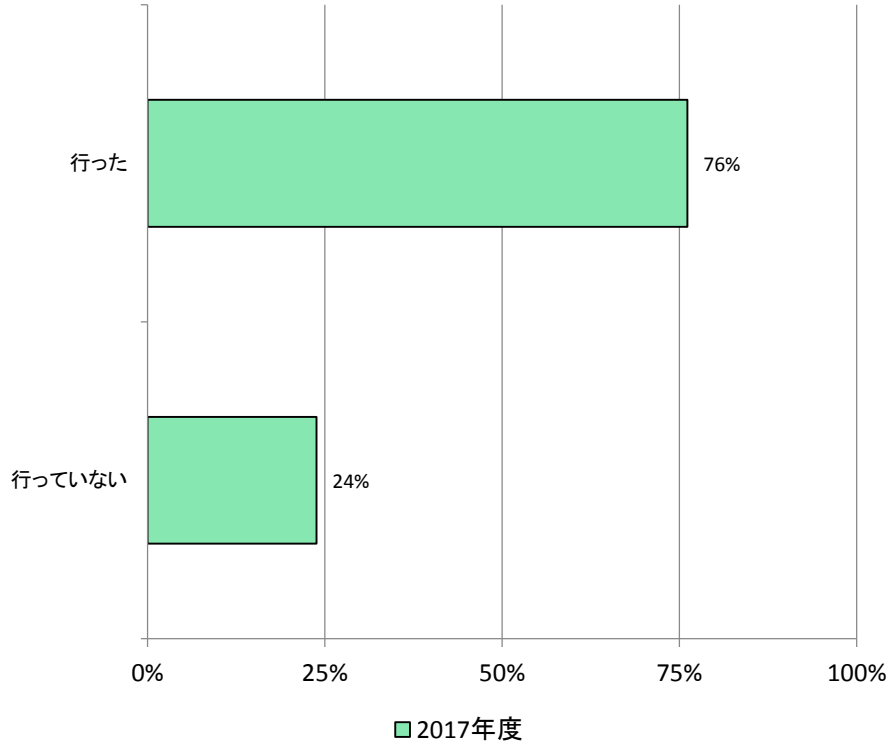


※金融は読替え可能項目なし（集計していません）

設問10-1　計画の見直し（又は修正）状況

・計画を策定している事業者等の内、8割程度は計画の見直しを実施している。

計画の見直し（又は修正）状況（単一回答）



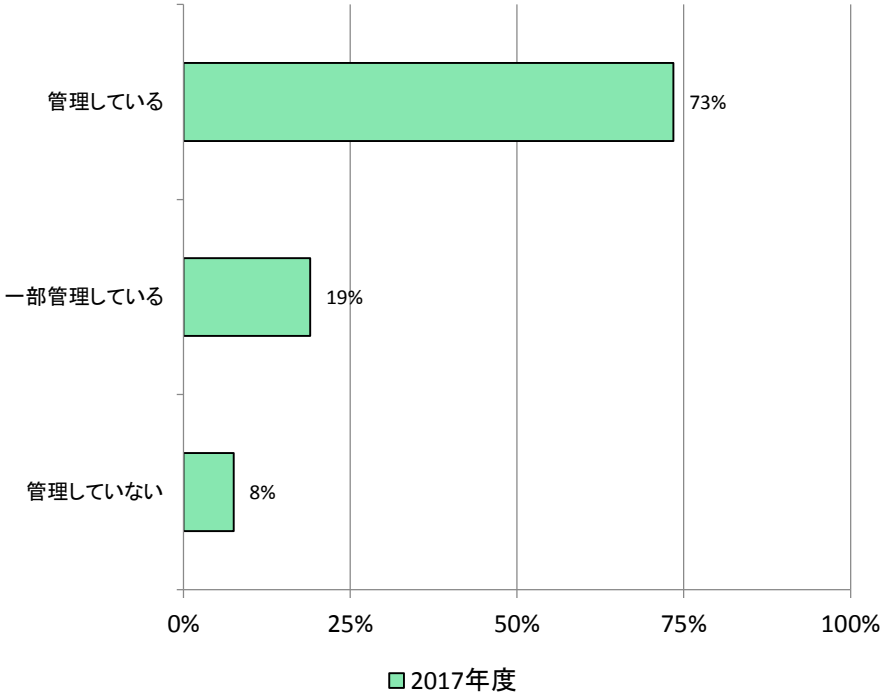
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (9/30) －

設問11　取扱い情報資産（システム含む）の洗い出し及び台帳等での管理状況

・ISMSにおいても、情報資産の洗い出しは、保護すべき資産を認識する第一歩となっている。しかし、取扱い情報資産（システム含む）の洗い出し及び台帳等での管理を行っていない事業者等は1割弱おり、資産の洗い出し及び管理を行うことが望まれる。

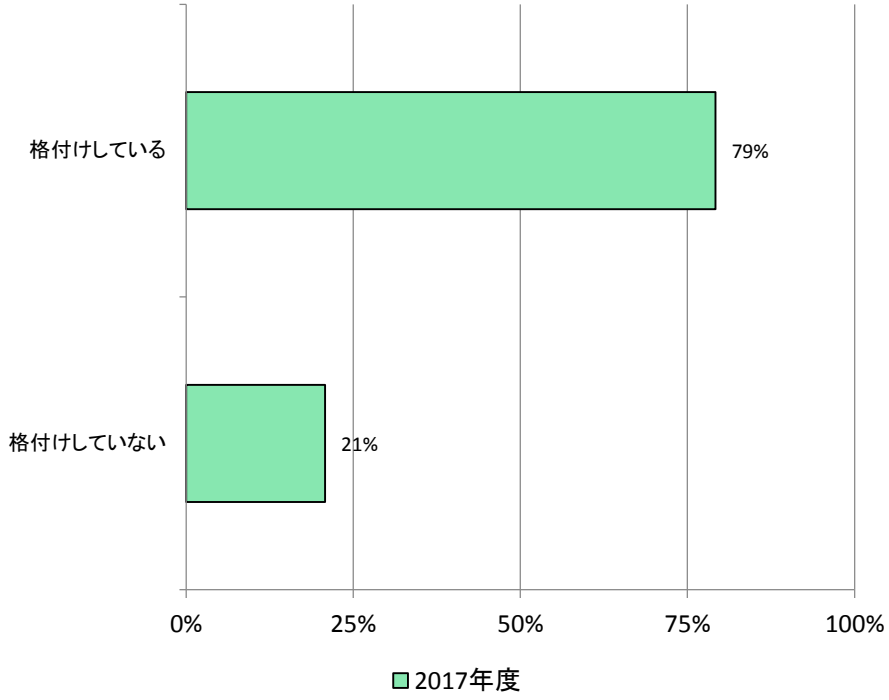
取扱い情報資産（システム含む）の洗い出し及び台帳等での管理状況（単一回答）



設問11-1　情報資産の重要度に応じた格付け状況

・多くの事業者等では、情報資産の重要度に応じた格付けを行っている。
　情報資産は、格付けを行うことにより、脅威やリスクに対して必要なアクセス制御等の対策が明確となるため、格付けの導入について検討することが望まれる。

情報資産の重要度に応じた格付け状況（単一回答）

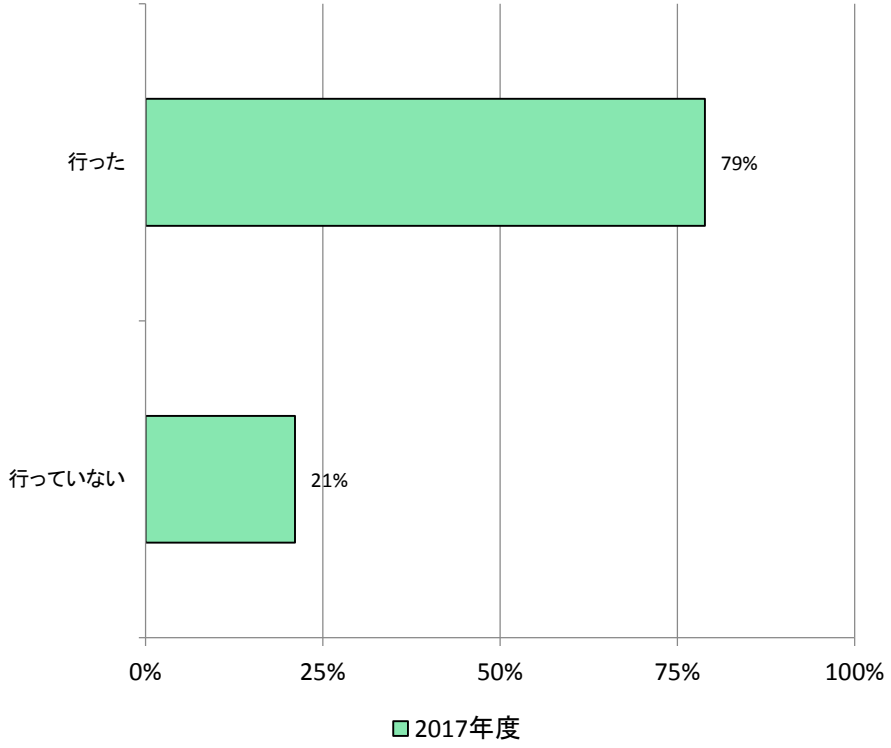


5．調査結果詳細 － (10/30) －

設問11-2 情報資産の見直し状況

・情報資産の見直しを行っていない事業者等が2割程度あるが、情報資産には生成から廃棄までのライフサイクルがあるため、定期的な見直しを実施することが望まれる。情報資産が多い場合には、運用負担が大きくなることが想定されるが、工夫して見直しを実施することが望まれる。

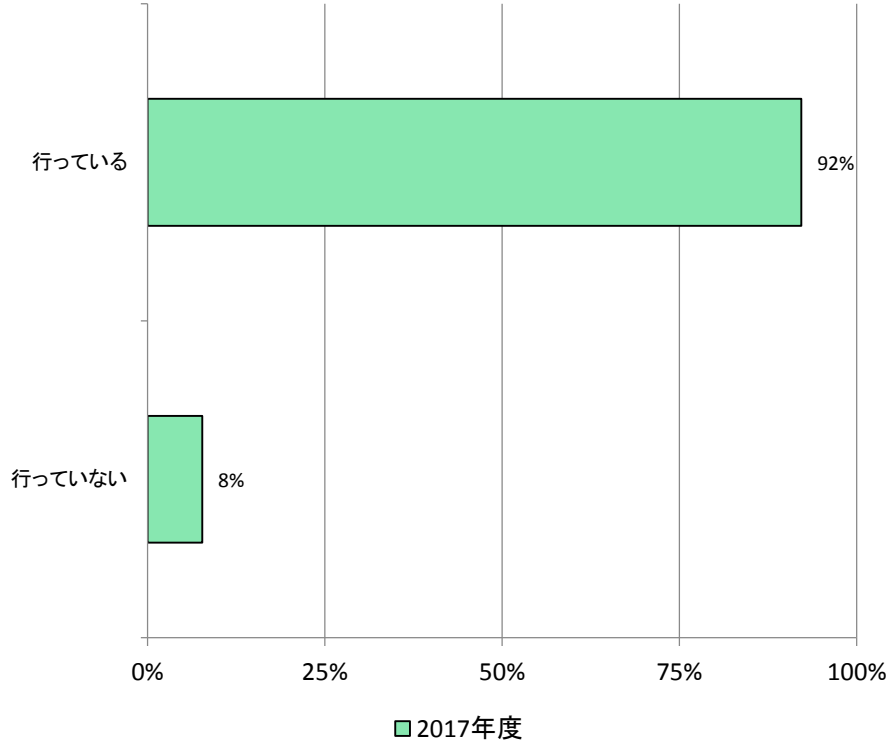
情報資産の見直し状況（単一回答）



設問12 脅威や脆弱性等の情報収集

・脅威や脆弱性等の情報収集を行っている事業者等は9割程度あるが、このような情報については、今後とも積極的に収集することが望まれる。

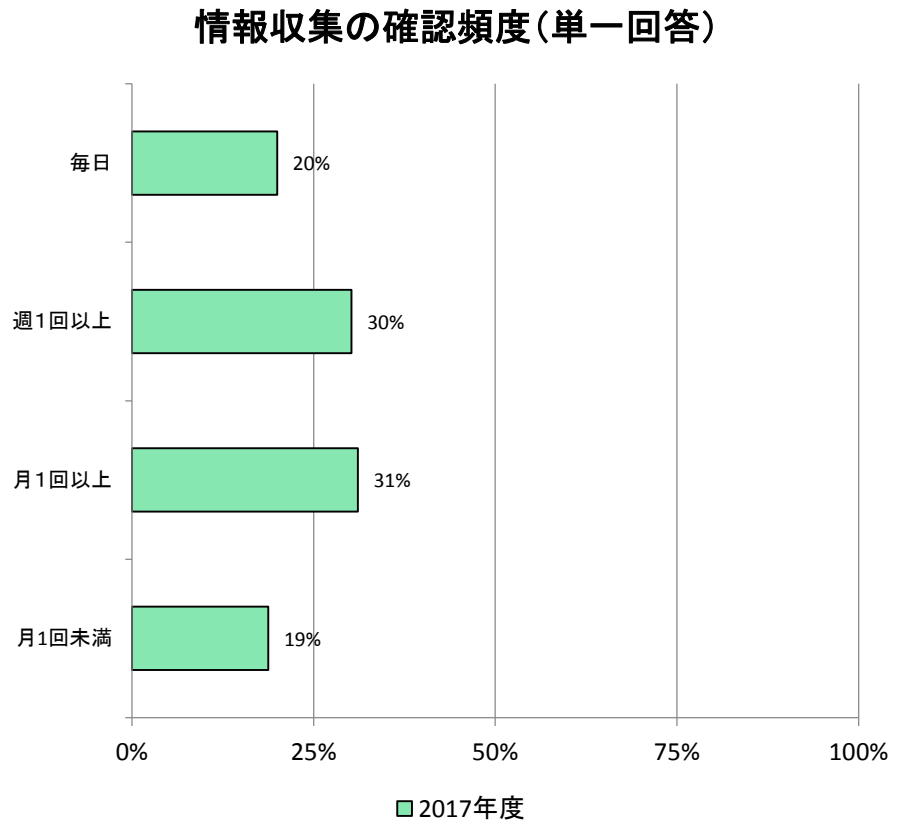
脅威や脆弱性等の情報収集（単一回答）



5．調査結果詳細 －（11/30）－

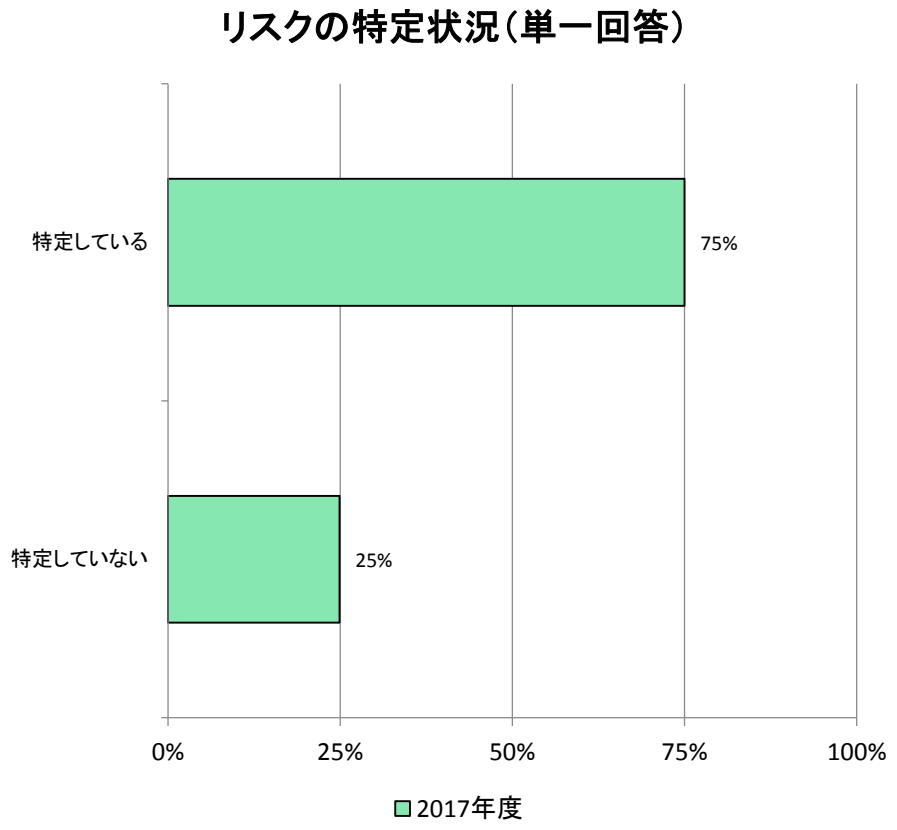
設問12-1　情報収集の確認頻度

・8割程度の事業者等が月に一回以上情報収集を行っている。
・脆弱性情報の公表から攻撃発生までの時間が短くなってきているため、情報収集の頻度を高めることが望まれる。



設問13　リスクの特定状況

・リスクの特定については8割程度の事業者等が実施している。ただし、中小規模の事業者等では、リスク特定の実施率が半数を切っているため、実施することが望まれる。



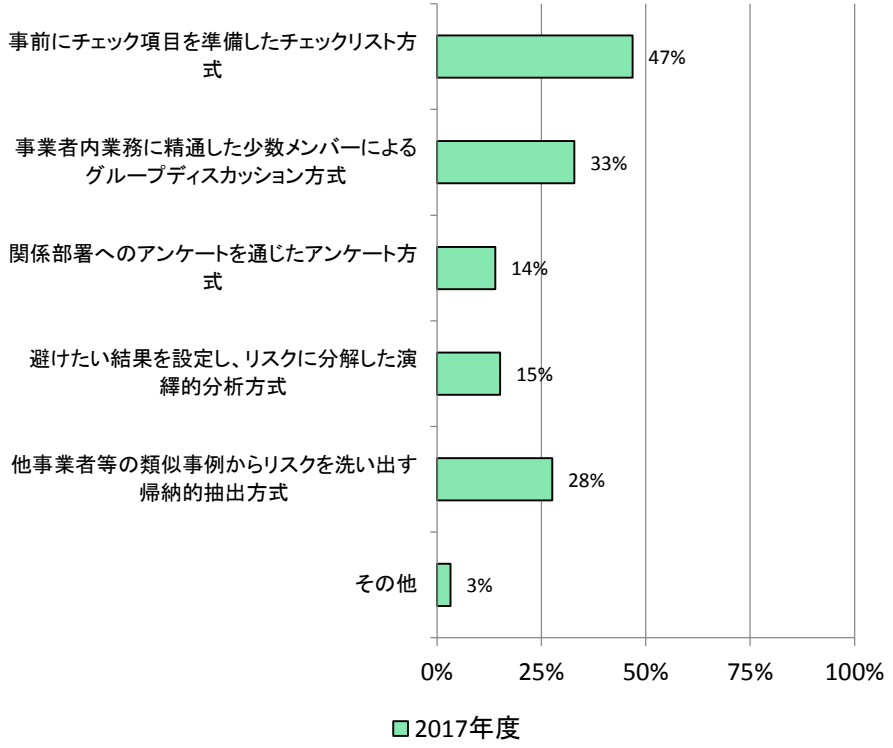
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（12/30）－

設問13-1 リスクの特定方法

・リスクの特定方法については、選択肢の方法を参考とし、自組織に適した手法を見つけ、実施することが望まれる。
・その他具体的な方法として、自組織の業務フローを整理し、その間に発生しうるリスクの洗い出しを実施している等の例もあった。

リスクの特定方法（複数回答）

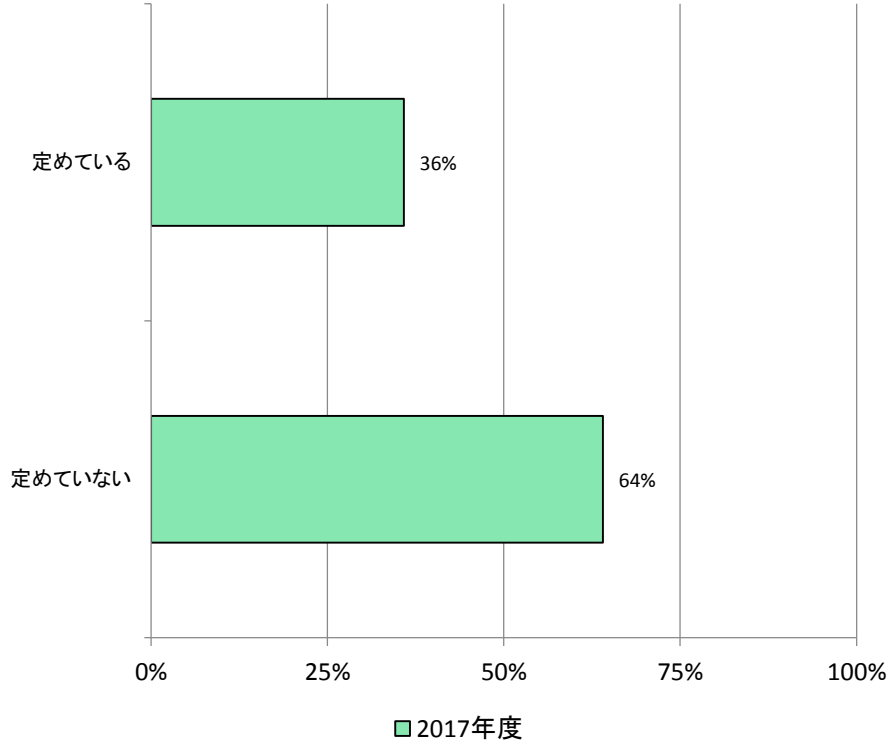


※金融は読替え可能項目なし（集計していません）

設問14 リスク対応の要否に係る判断基準

・事業者規模別に分析した結果、規模が小さくなるほど、リスク対応の要否に係る判断基準を定めている事業者等が少なくなっているが、リスク対応を属人化せずに進めるために、要否に係る判断基準を明文化しておくことが望まれる。

リスク対応の要否に係る判断基準（単一回答）



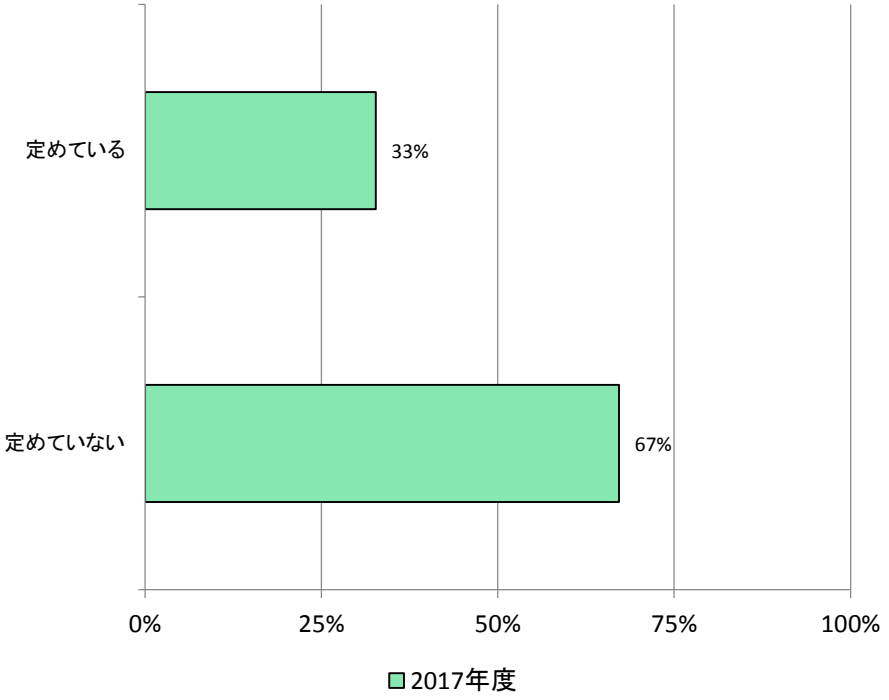
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（13/30）－

設問15 リスク対応の優先順位に係る判断基準

・事業者規模別に分析した結果、規模が小さくなるほど、リスク対応の優先順位に係る判断基準を定めている事業者等が少なくなっているが、リスク対応を属人化せずに進めるために、優先順位に係る判断基準を明文化しておくことが望まれる。

リスク対応の優先順位に係る判断基準
（単一回答）

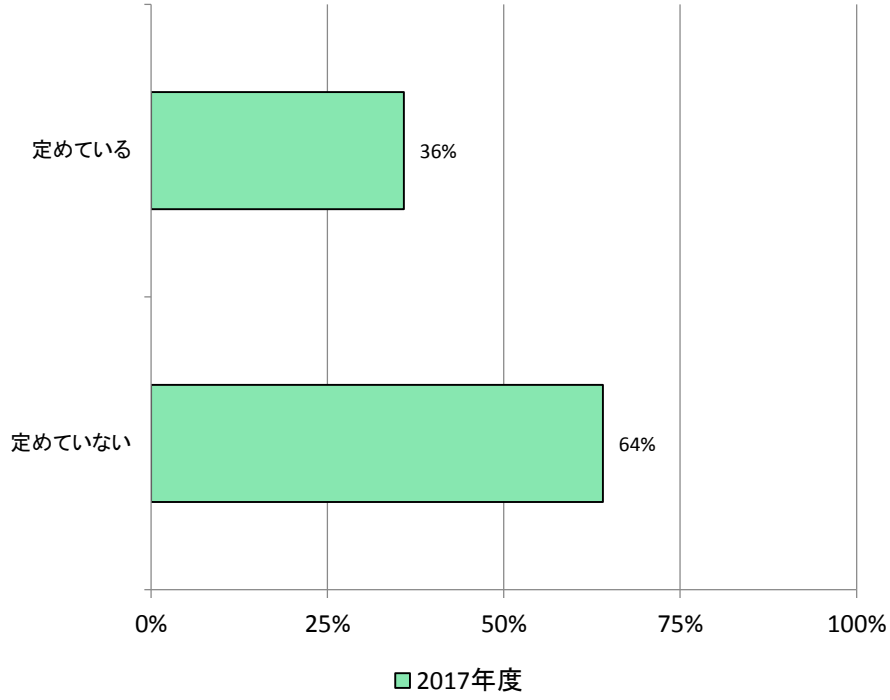


※金融は読替え可能項目なし（集計していません）

設問16 リスクに応じた対応手段の判断基準

・事業者規模別に分析した結果、規模が小さくなるほど、リスクに応じた対応手段の判断基準を定めている事業者等が少なくなっているが、リスク対応を属人化せずに進めるために、リスクに応じた対応手段の判断基準を明文化しておくことが望まれる。

リスクに応じた対応手段の判断基準
（単一回答）



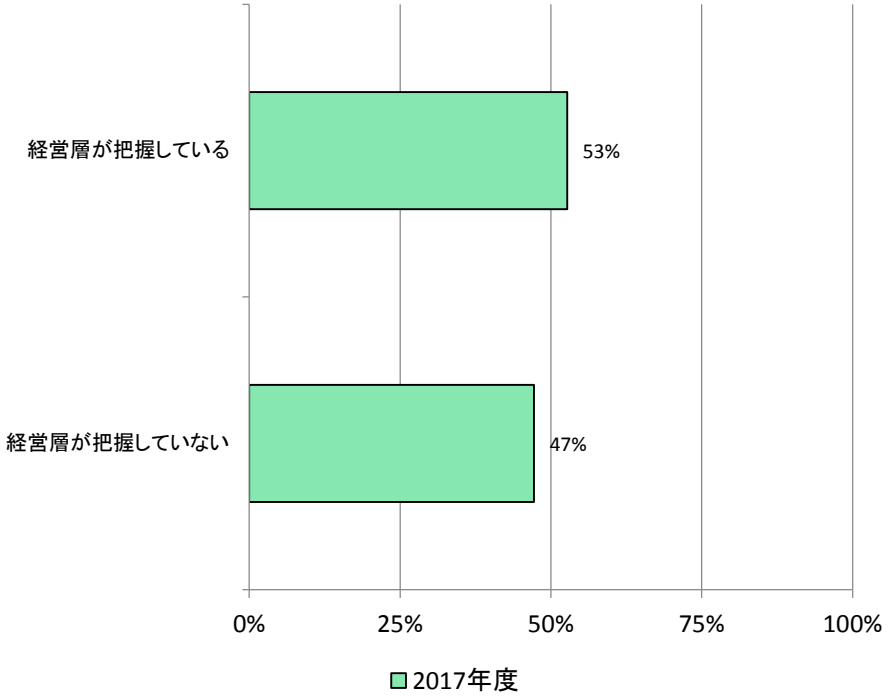
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（14/30）－

設問17　リスク対応に関する判断結果についての経営層の把握状況

・リスク対応に関する判断結果については、5割程度の経営層が把握しているが、判断結果については、経営層が把握しておくことが望まれる。

リスク対応に関する判断結果についての経営層の把握状況（単一回答）

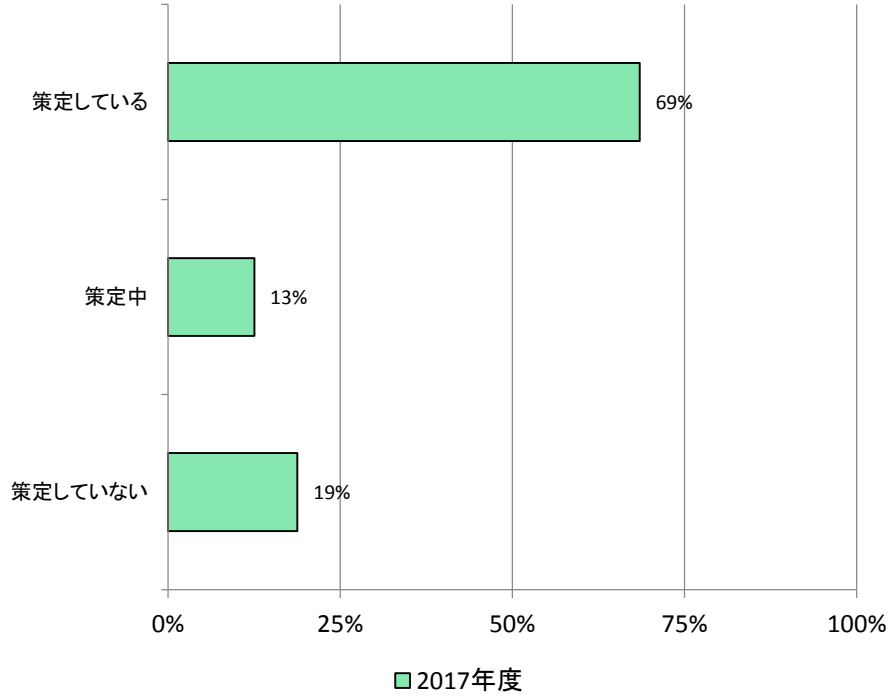


※金融は読替え可能項目なし（集計していません）

設問18　情報セキュリティに関する内規の策定状況

・事業者規模別に分析した結果、規模が小さくなるほど、情報セキュリティに関する内規を策定している事業者等の数が少なくなっているが、情報セキュリティに関する内規は策定されていることが強く望まれる。

情報セキュリティに関する内規の策定状況（単一回答）



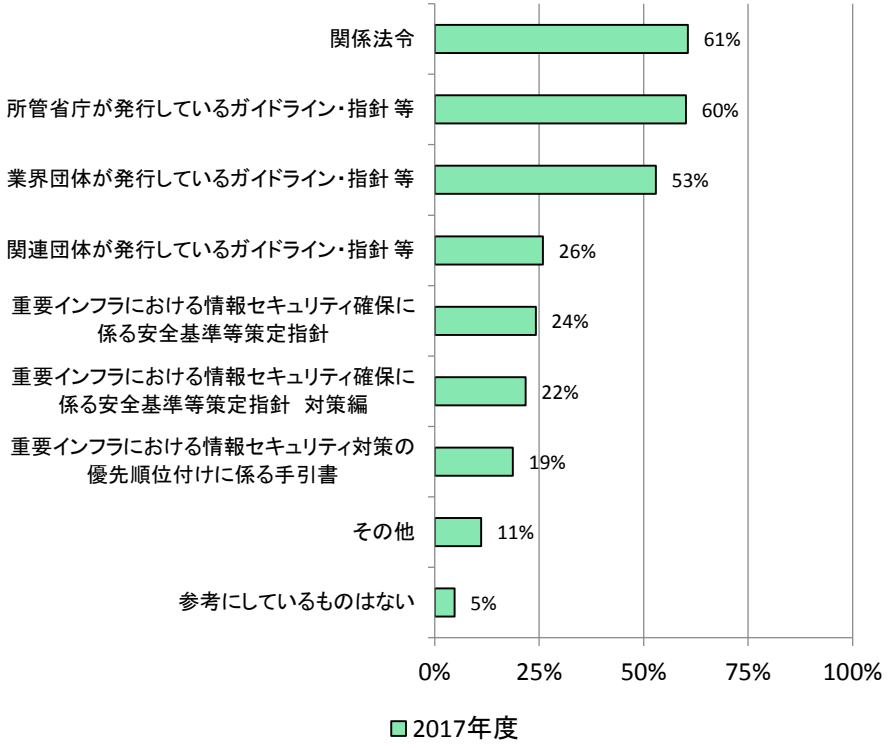
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（15/30）－

設問18-1　内規等を策定する際の参考文献

・内規等の策定・見直しの際には、選択肢にある文書を参考にすることが望まれる。
・その他の具体的内容として、ISO27001やJIS Q15001、J-CLICSチェックリスト(JPCERT)、情報セキュリティポリシーサンプル(JNSA)、重要インフラのサイバーセキュリティを向上させるためのフレームワーク(NIST)等が挙げられていた。

内規等を策定する際の参考文献（複数回答）

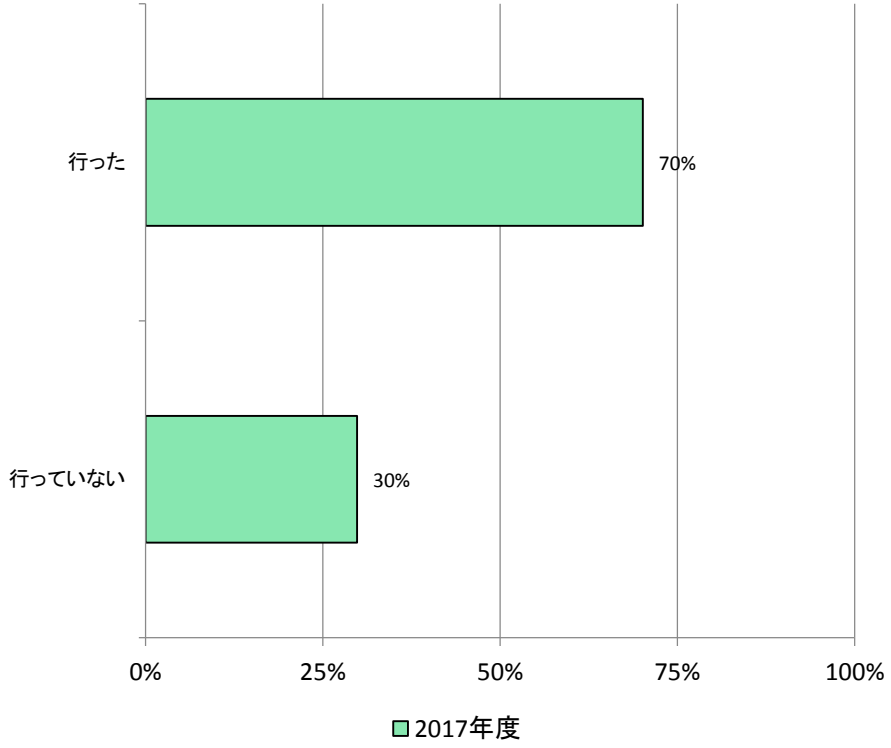


※金融は読替え可能項目なし（集計していません）

設問18-2　策定した内規の見直し検討状況

・内規の見直し検討を行った事業者等は7割程度であった。

策定した内規の見直し検討状況（単一回答）



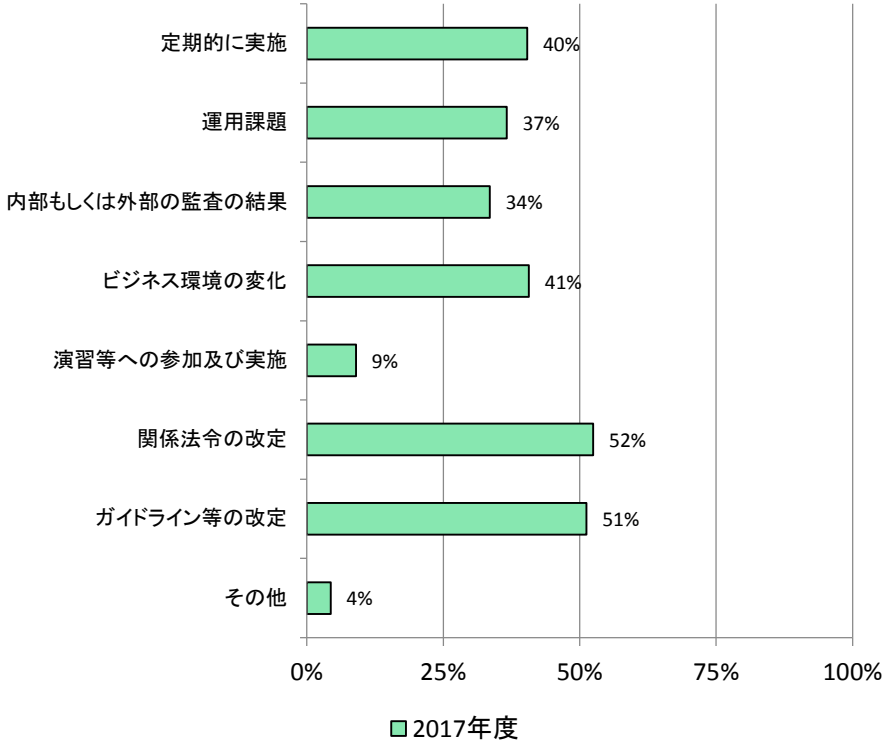
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（16/30）－

設問18-3　内規の見直し検討の契機

・選択肢の項目を参考とし、必要に応じて内規を見直すことが望まれる。
・その他の例として、自然災害や情報漏えい事案が起こった際などの例が挙げられていた。

内規の見直し検討の契機（複数回答）

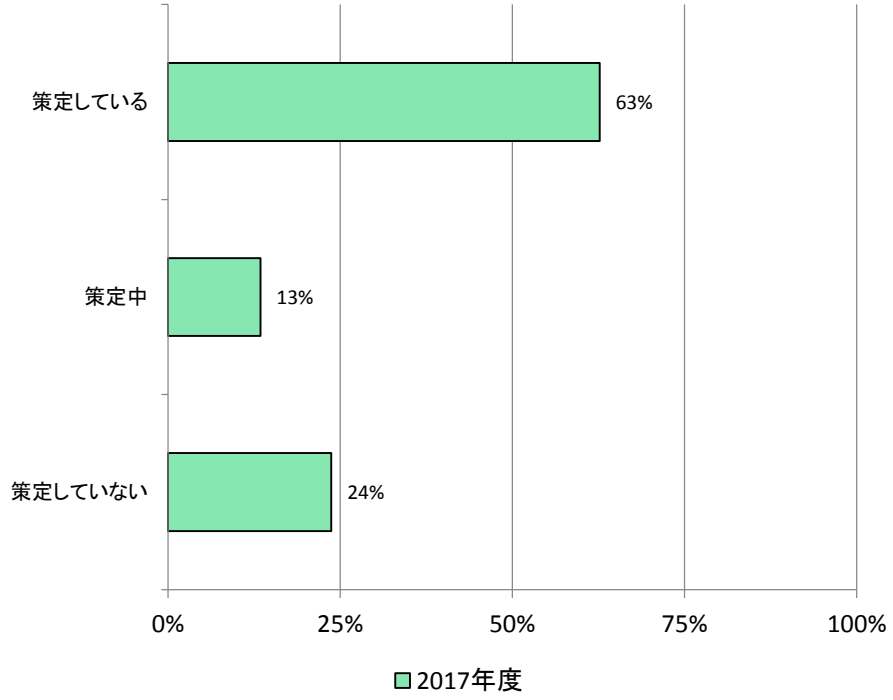


※金融は読替え可能項目なし（集計していません）

設問19　情報の取扱いに関する規定の策定状況

・情報の取扱いに関する規定を「策定している」または「策定中」の事業者等は8割程度であった。

情報の取扱いに関する規定の策定状況（単一回答）



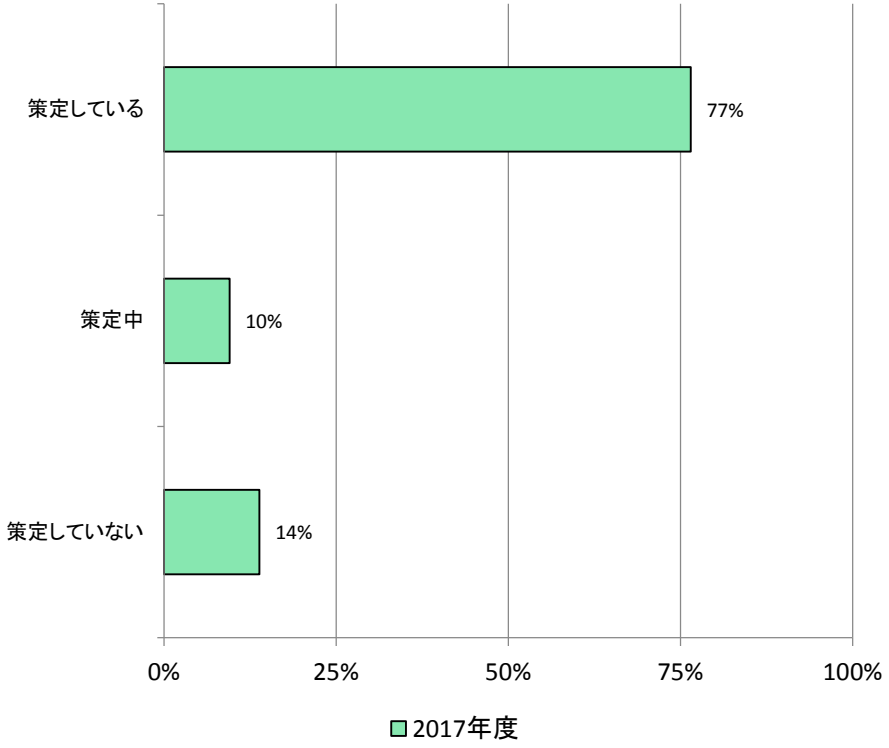
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (17/30) －

設問20　事業継続計画の策定状況

・1割強の事業者等は事業継続計画を策定していないため、事業継続計画の策定が望まれる。

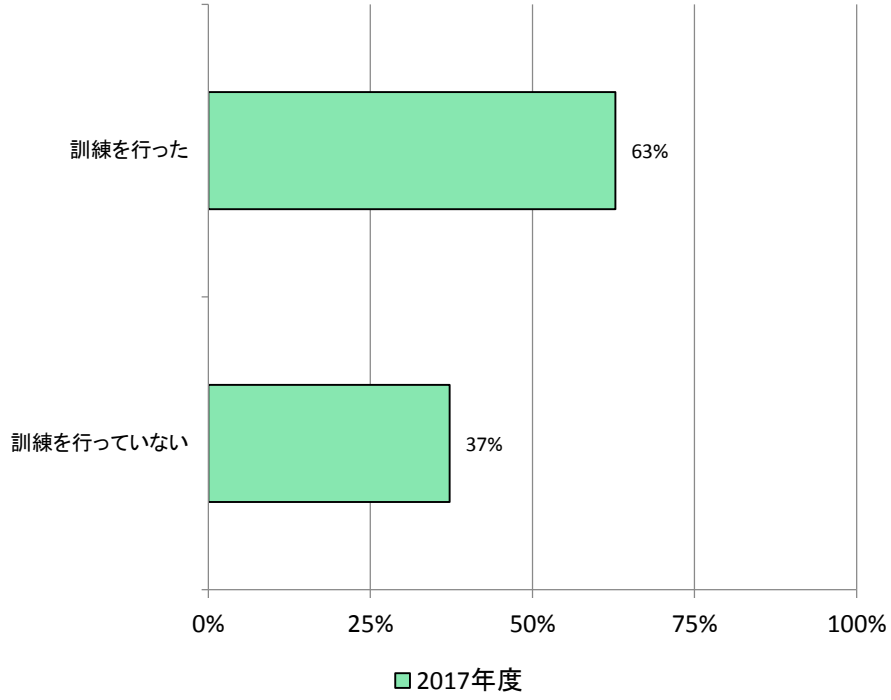
事業継続計画の策定状況（単一回答）



設問20-1　事業継続計画に基づいた訓練状況

・事業継続計画を策定している事業者等のうち、事業継続計画に基づいた訓練を行った事業者等は6割程度であった。

事業継続計画に基づいた訓練状況（単一回答）

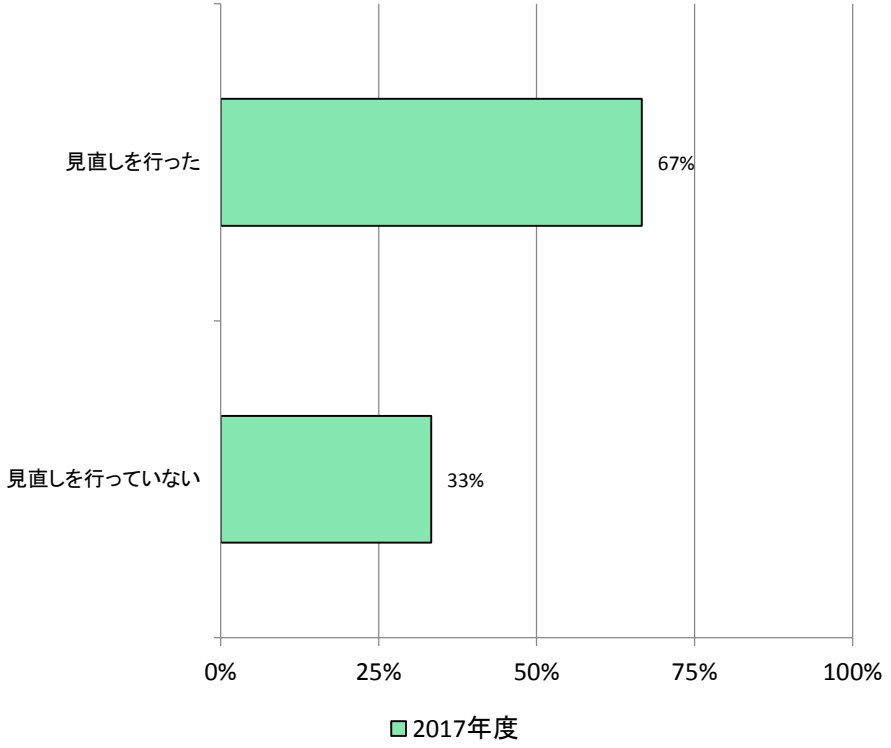


5．調査結果詳細 －（18/30）－

設問20-2　事業継続計画の見直し状況

・事業継続計画を策定している事業者等のうち、見直しを行った事業者等は7割程度であった。

事業継続計画の見直し状況（単一回答）

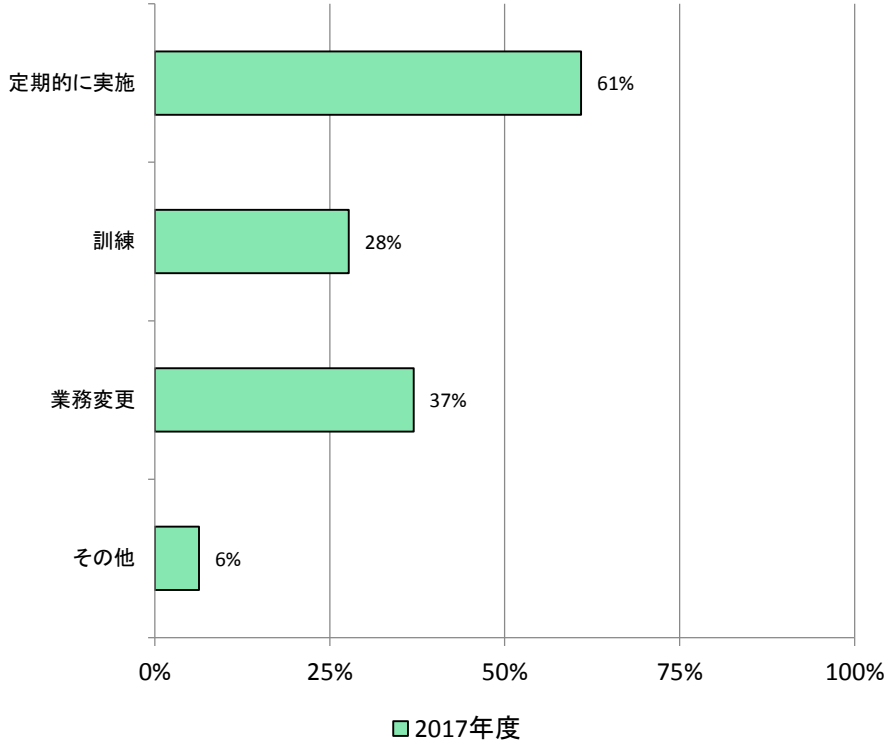


※金融は読替え可能項目なし（集計していません）

設問20-3　事業継続計画の見直し契機

・選択肢の項目に該当した場合、必要に応じて事業継続計画を見直すことを推奨したい。
・その他の例として、組織体制の変更があった際等が挙げられていた。

事業継続計画の見直し契機（複数回答）



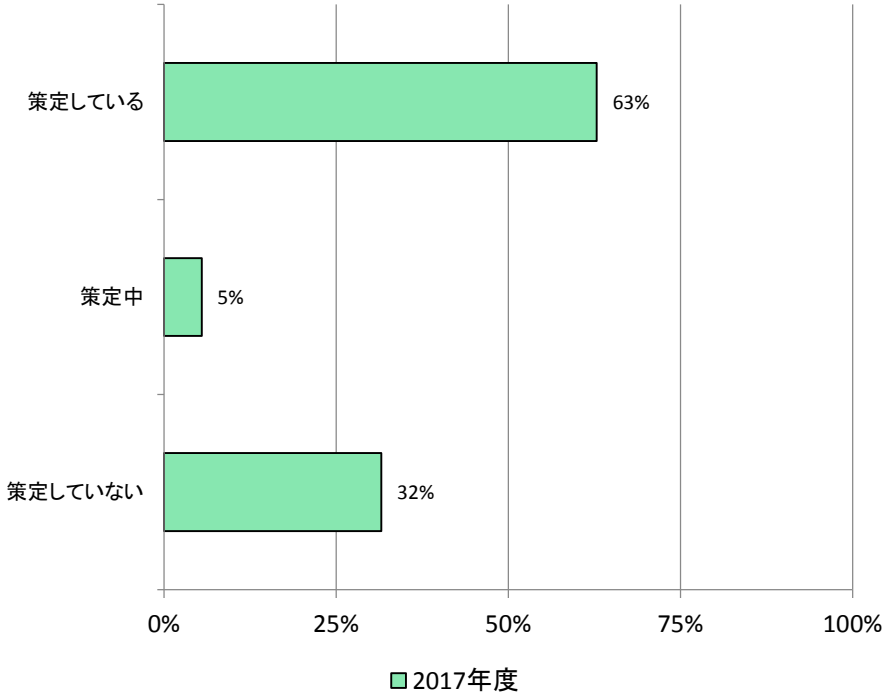
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (19/30) －

設問21　コンティンジェンシープラン策定状況

・コンティンジェンシープランについて、6割程度の事業者等で策定されている。

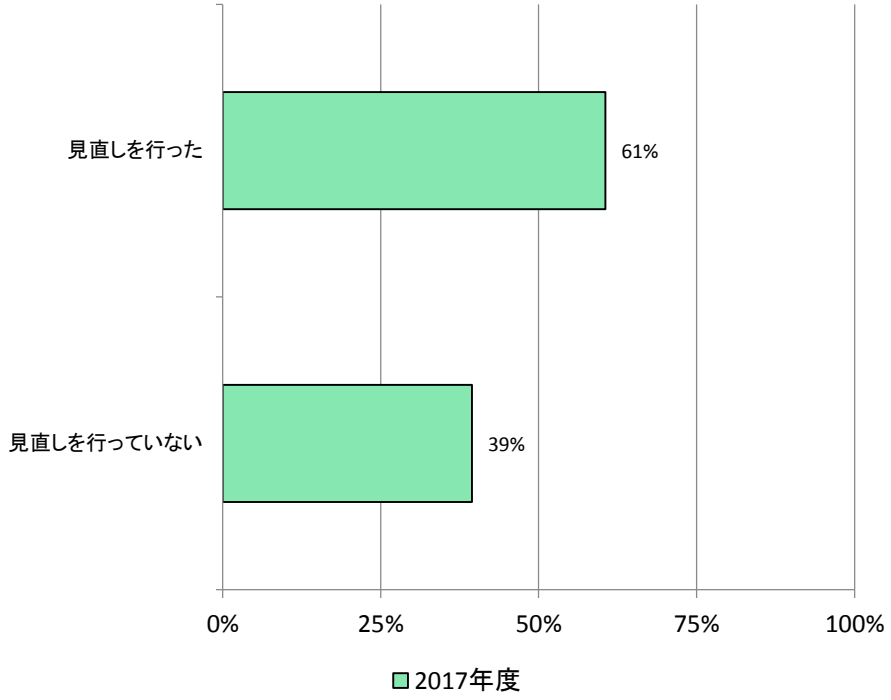
コンティンジェンシープラン策定状況
（単一回答）



設問21-1　コンティンジェンシープランの見直し状況

・約6割の事業者等がコンティンジェンシープランを見直しており、今後も必要に応じて見直しを行うことが望まれる。

コンティンジェンシープランの見直し状況
（単一回答）

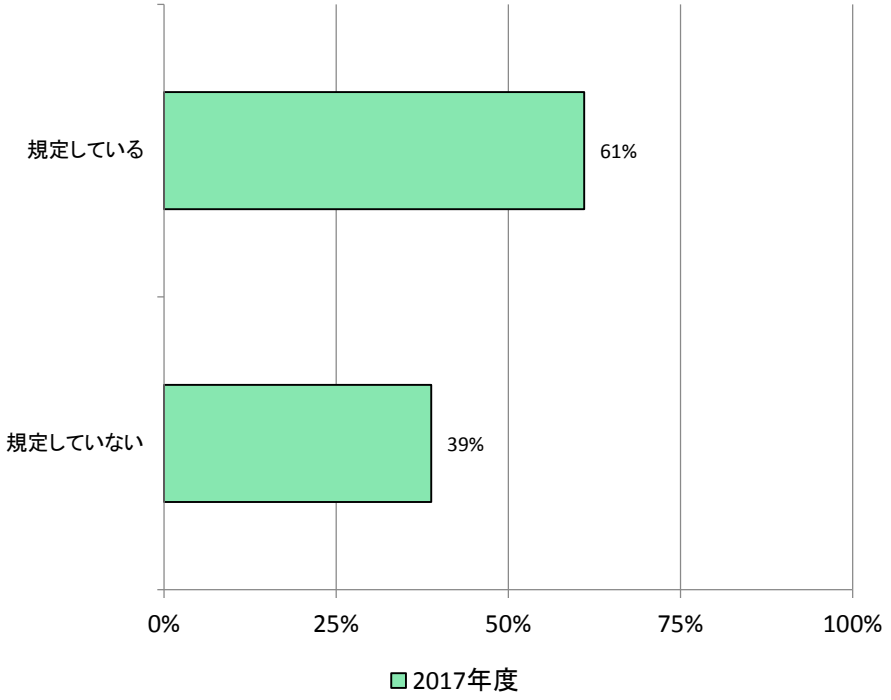


5．調査結果詳細 － (20/30) －

設問22　外部委託に関する規定の策定状況

・外部委託に関する規定については、6割程度の事業者等が策定していることが認められる。

外部委託に関する規定の策定状況（単一回答）

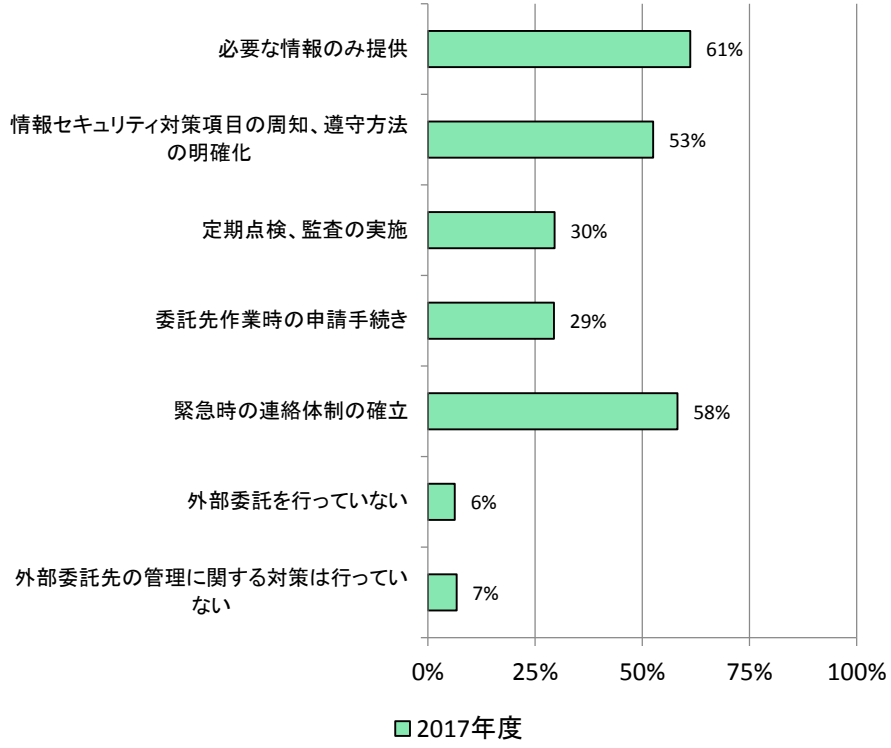


※金融は読替え可能項目なし（集計していません）

設問23　外部委託先管理に関する対策

・外部委託を実施している9割程度の事業者等が、外部委託先管理の対策を実施しているが、外部委託先管理に関する対策は、今後も継続していくことが望まれる。

外部委託先管理に関する対策（複数回答）



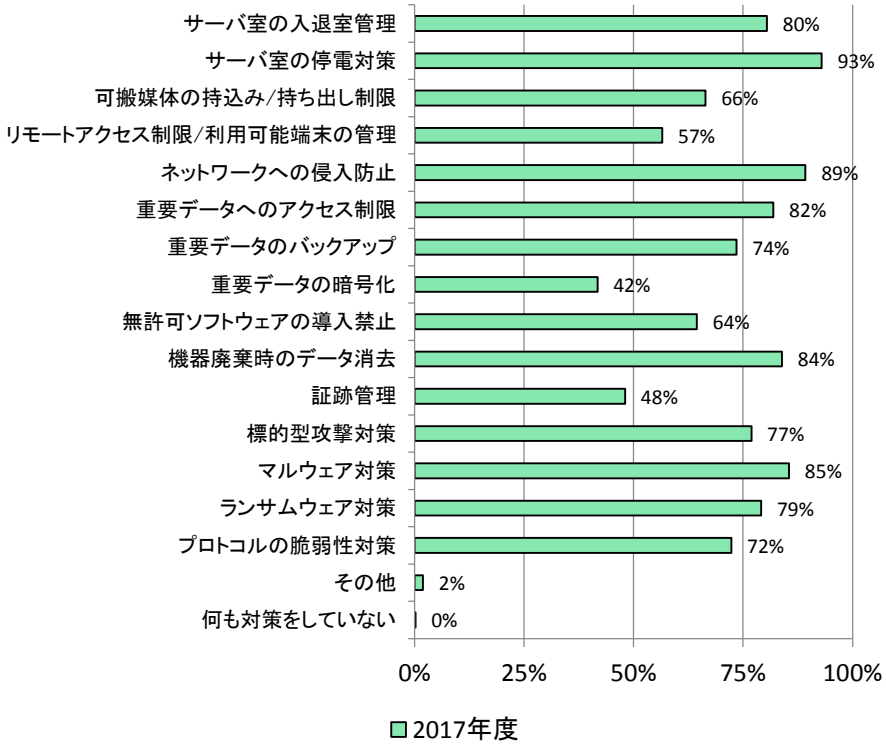
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (21/30) －

設問24　実施済みの情報セキュリティ対策

・おおよその対策は取られているが、「証跡管理」や「重要データの暗号化」に関しては、実施率が低いため、未実施の事業者等においては、必要に応じて実施することが望まれる。

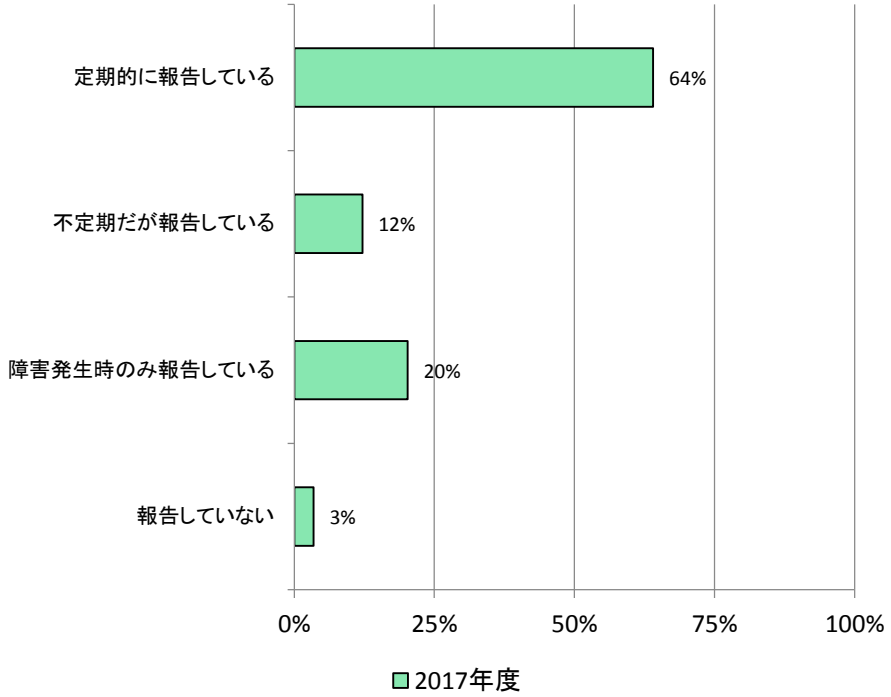
実施済みの情報セキュリティ対策（複数回答）



設問25　責任者へのセキュリティ対策の運用報告

・ほぼ全ての事業者等が責任者へ報告を実施しているが、今後も必要に応じて、報告を上げることが望まれる。

責任者へのセキュリティ対策の運用報告（単一回答）

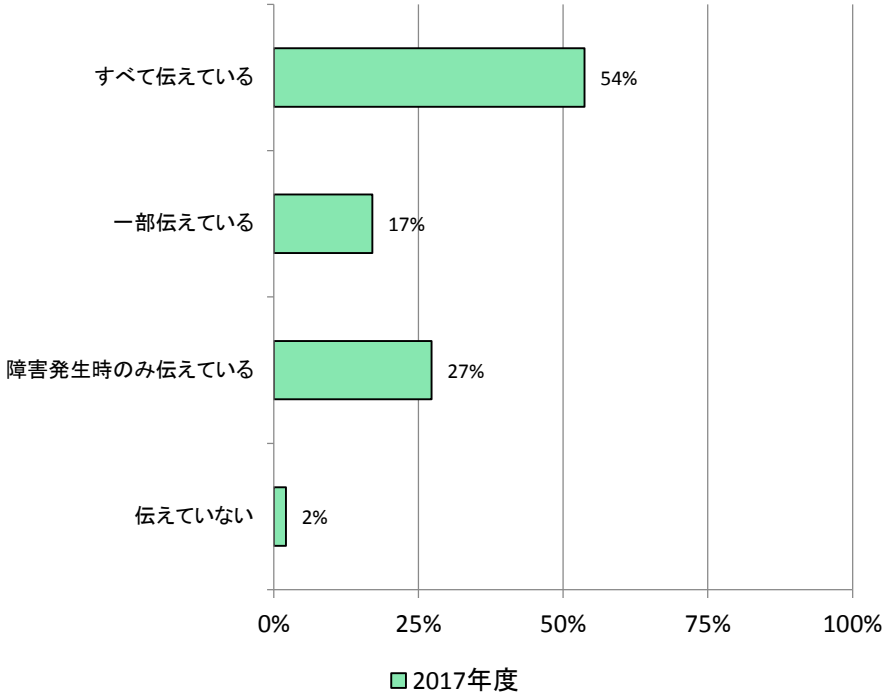


5．調査結果詳細 － (22/30) －

設問25-1　経営層への情報セキュリティ運用報告

・ほぼ全ての事業者等が、経営層まで適切に報告を行っている。

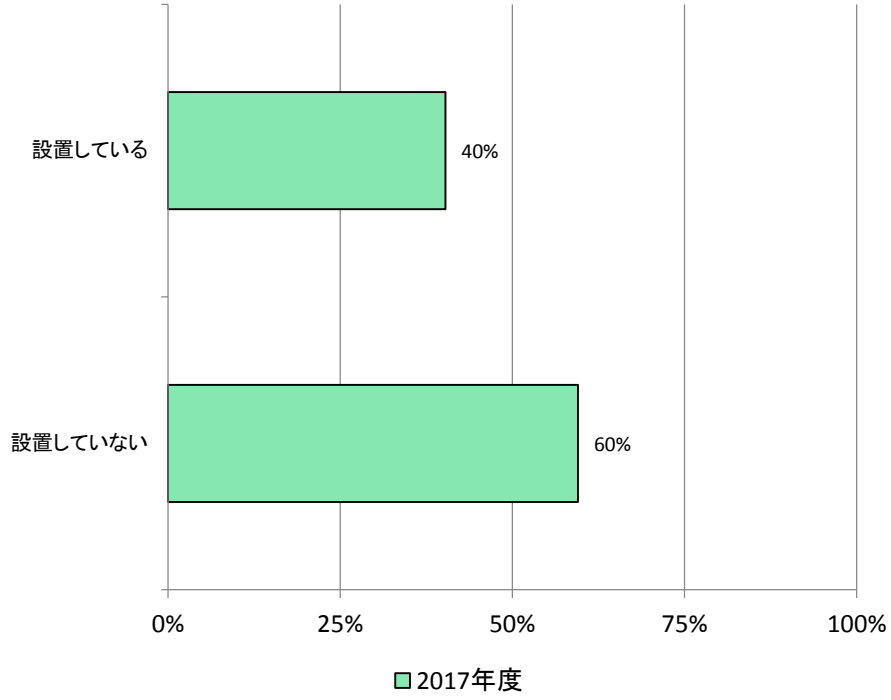
経営層への情報セキュリティ運用報告
（単一回答）



設問26　対外向けの情報共有窓口の設置状況

・対外向けの情報共有窓口については、4割程度の事業者等が設置している。

対外向けの情報共有窓口の設置状況
（単一回答）



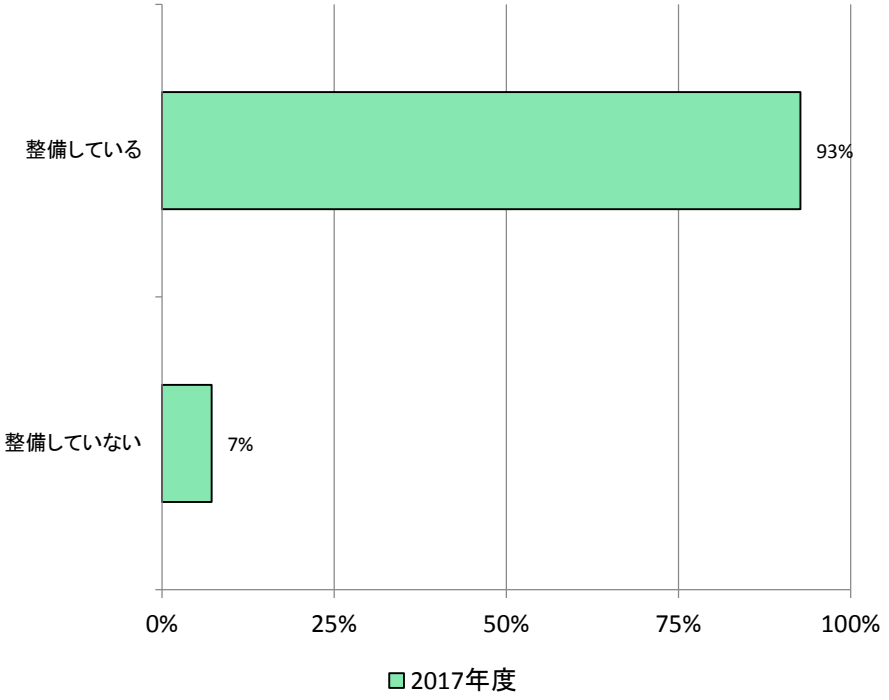
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (23/30) －

設問27　障害発生時における連絡体制の整備状況

・9割程度の事業者等において、障害発生時の連絡体制が整備されているが、一歩進んで連絡体制がきちんと機能するか確認を行うことが望まれる。

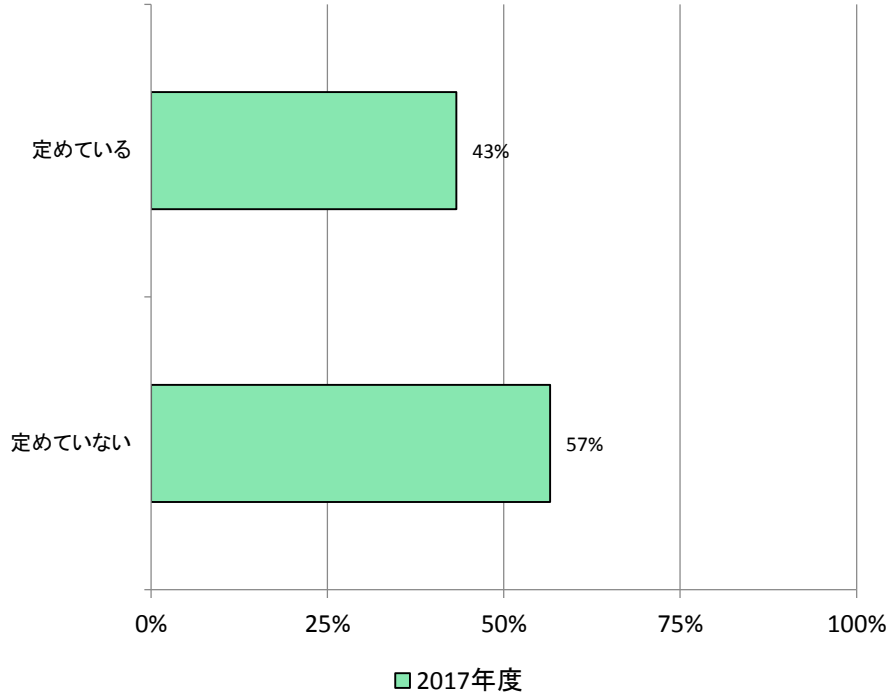
障害発生時における連絡体制の整備状況
（単一回答）



設問28　障害発生時の利用者アナウンスの判断基準

・全ての障害に対して判断基準を策定することは難しいと思われる。しかしながら、想定される障害については素早い意思決定ができるよう、判断基準を定めておくことが望まれる。

障害発生時の利用者アナウンスの判断基準
（単一回答）



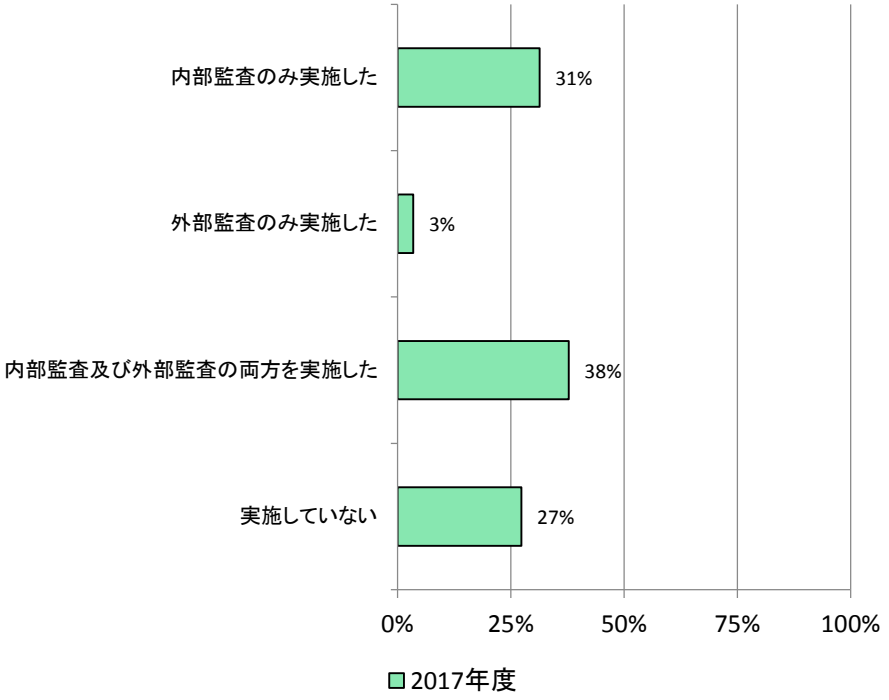
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (24/30) －

設問29　情報セキュリティに関する監査実施状況

・監査の実施率について、昨年度と比較して多少伸びてはいるが、実施していない事業者等においては実施することが望まれる。

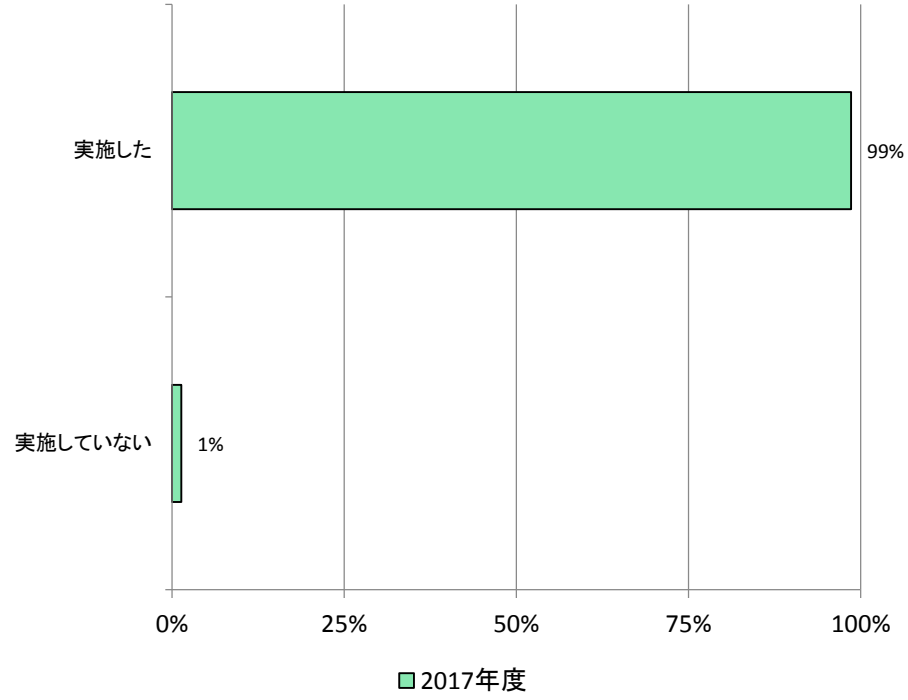
情報セキュリティに関する監査実施状況
（単一状況）



設問29-1　監査を通じた対策の是正検討状況

・ほぼ全ての事業者等が監査を通じて是正検討を行っていることから、監査の有効性が認められる。

監査を通じた対策の是正検討状況
（単一回答）



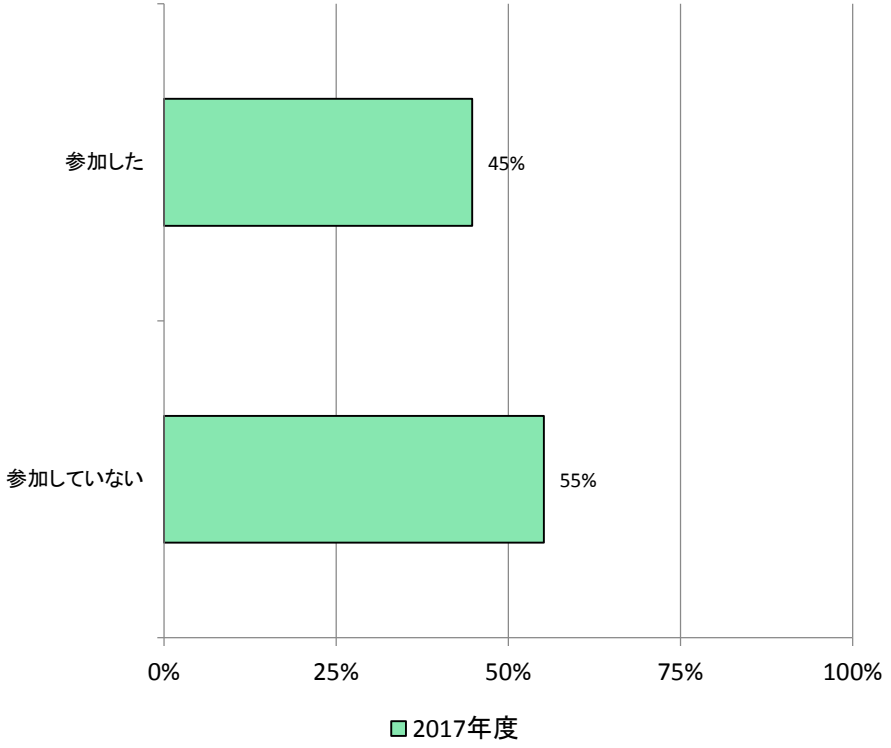
※政府・行政サービスは読替え可能項目なし（集計していません）

5．調査結果詳細 － (25/30) －

設問30　外部の演習等への参加状況

・外部演習等への参加が半数以下にとどまっている。演習に参加することで、セキュリティ対策の重要性や自組織内での課題を認識する機会が得られるため、参加していない事業者等においては、機会を見つけて参加することが望まれる。

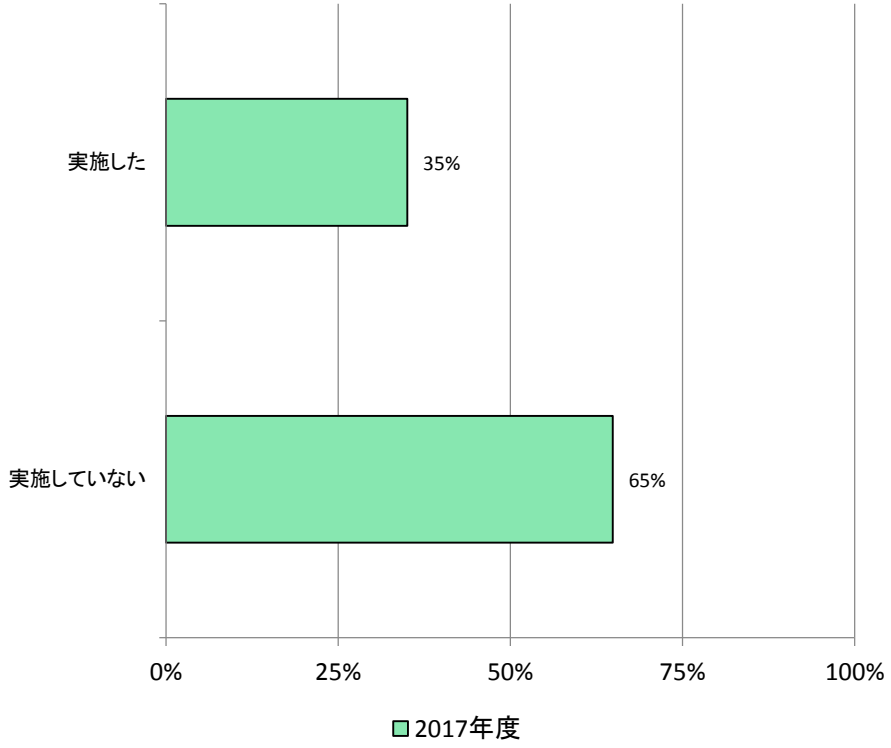
外部の演習等への参加状況（単一回答）



設問31　内部での演習等の実施状況

・内部での演習を実施する事業者等は3割程度にとどまっている。セキュリティ対策に関する意識の向上を図るため、事業者内での実施が困難な場合は、外部の演習等への参加を検討することが望まれる。

内部での演習等の実施状況（単一回答）

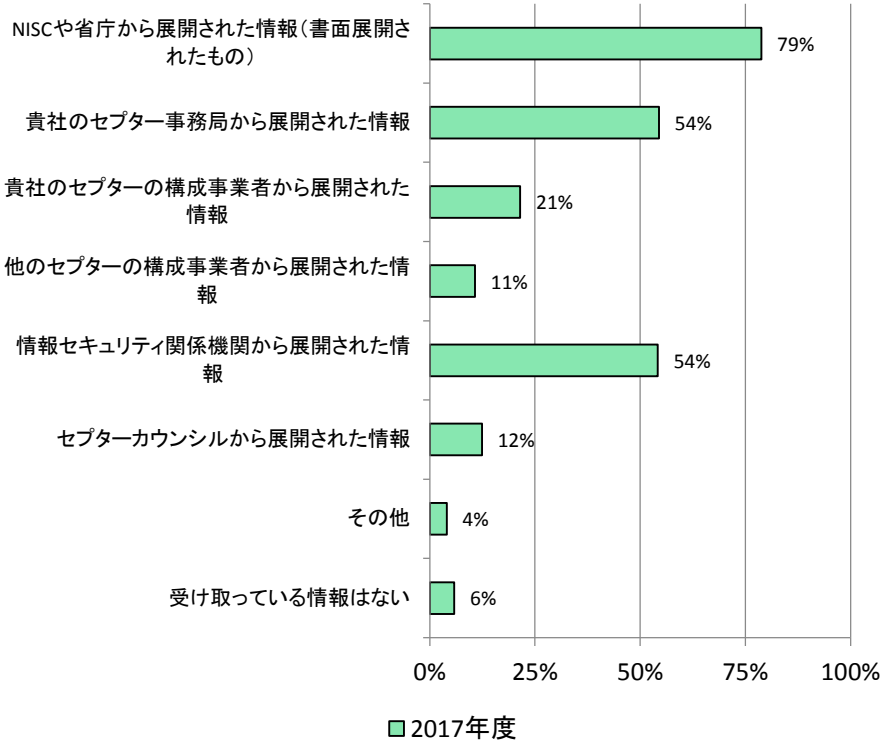


5．調査結果詳細 －（26/30）－

設問32　情報共有体制下での受信状況

・NISCや省庁経由から展開された情報の受信状況は8割程度の事業者等ではあるが、セプター事務局・セプター構成員からの情報共有はまだ多くはなく、セプター内における情報共有をより活性化することが望まれる。

情報共有体制下での受信状況（複数回答）

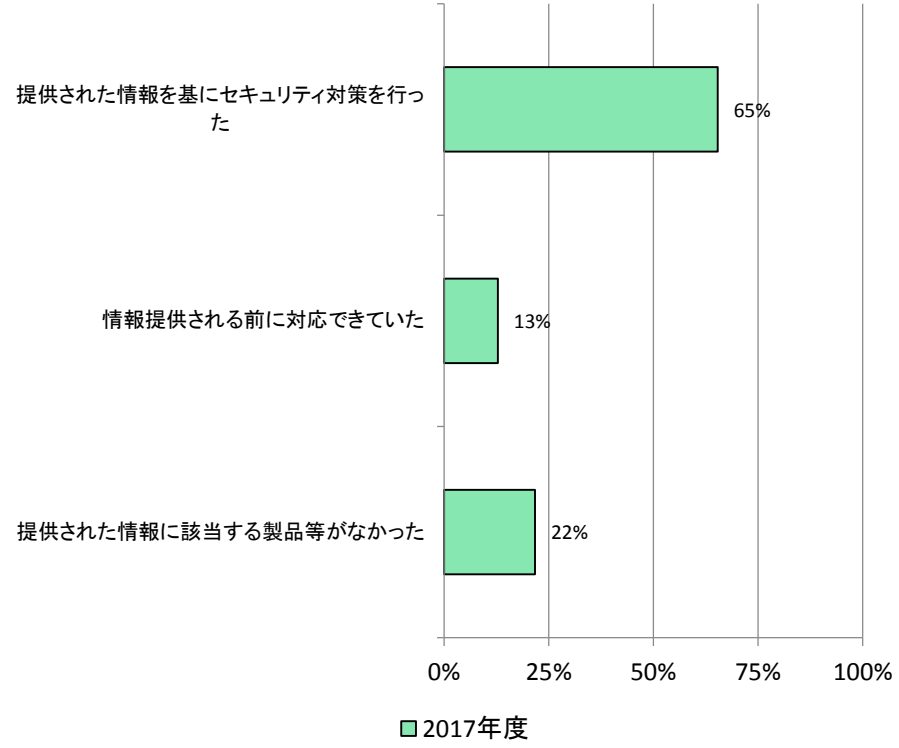


※金融は読替え可能項目なし（集計していません）

設問32-1　受信情報の有効活用度

・6割以上の事業者等において、提供された情報を有効活用している。

受信情報の有効活用度（単一回答）



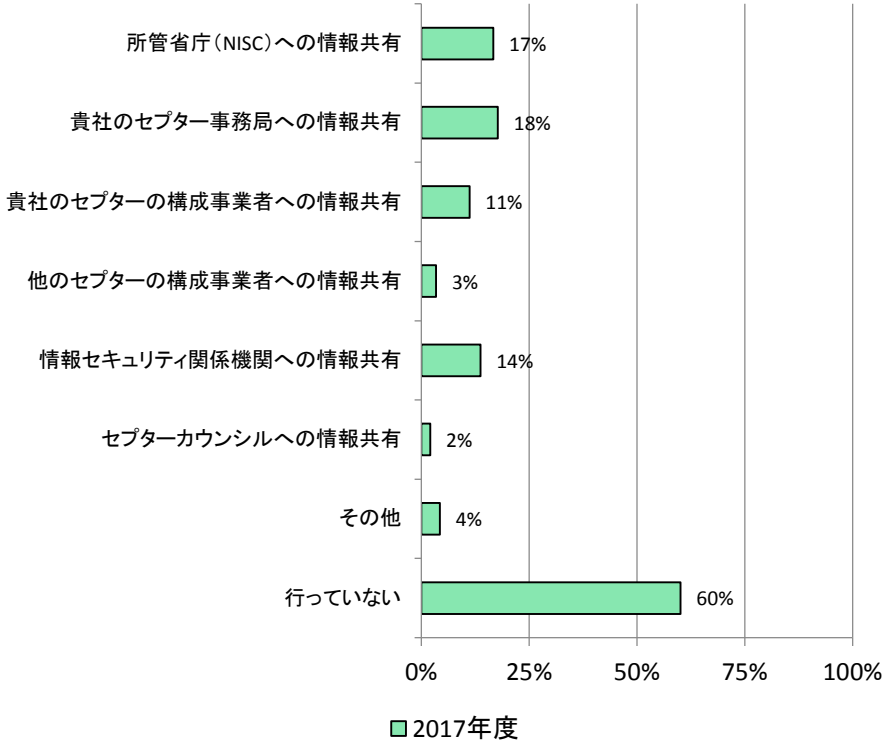
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 － (27/30) －

設問33　能動的に行った情報共有状況

・「能動的に情報共有を行っていない」事業者等は6割程度になっている。「重要インフラの情報セキュリティ対策に係る第４次行動計画」等を参照し、情報共有体制の強化に向けた取組を進めることが望まれる。

能動的に行った情報共有状況（複数回答）

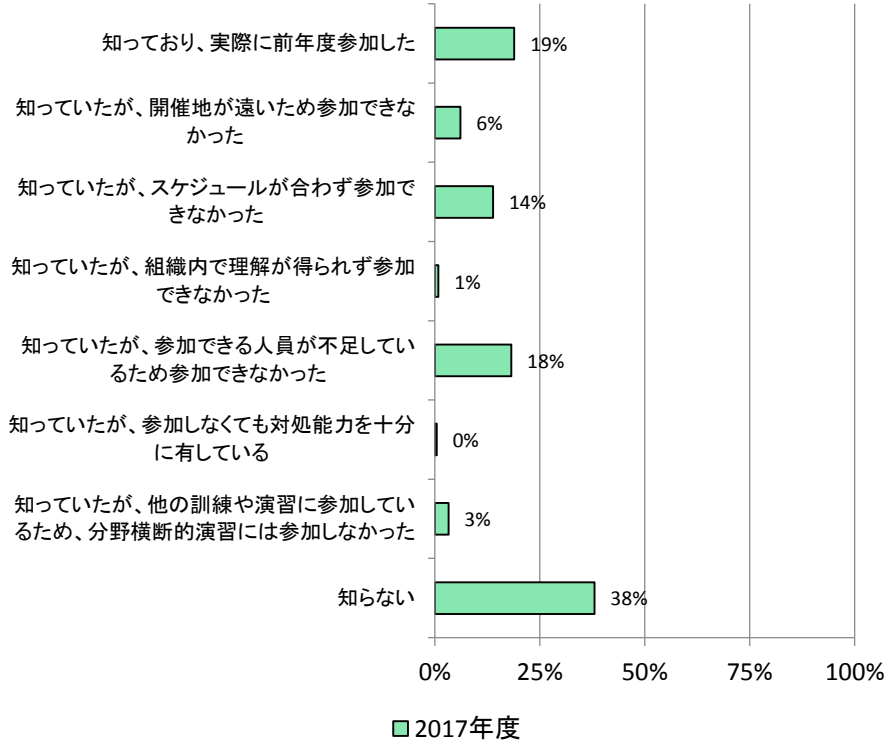


※金融は読替え可能項目なし（集計していません）

設問34　分野横断的演習の認知状況

・「知っているが参加していない」、「知らない」事業者等は8割程度になっている。「知っている」にとどまっている事業者等においては、自職場参加という形態もあるため、分野横断的演習に可能な限り参加し、セキュリティ対策の重要性に気づく機会を得ることが望まれる。また、知らない事業者等に対しては、これまで以上の広報活動も検討する。

分野横断的演習の認知状況（単一回答）



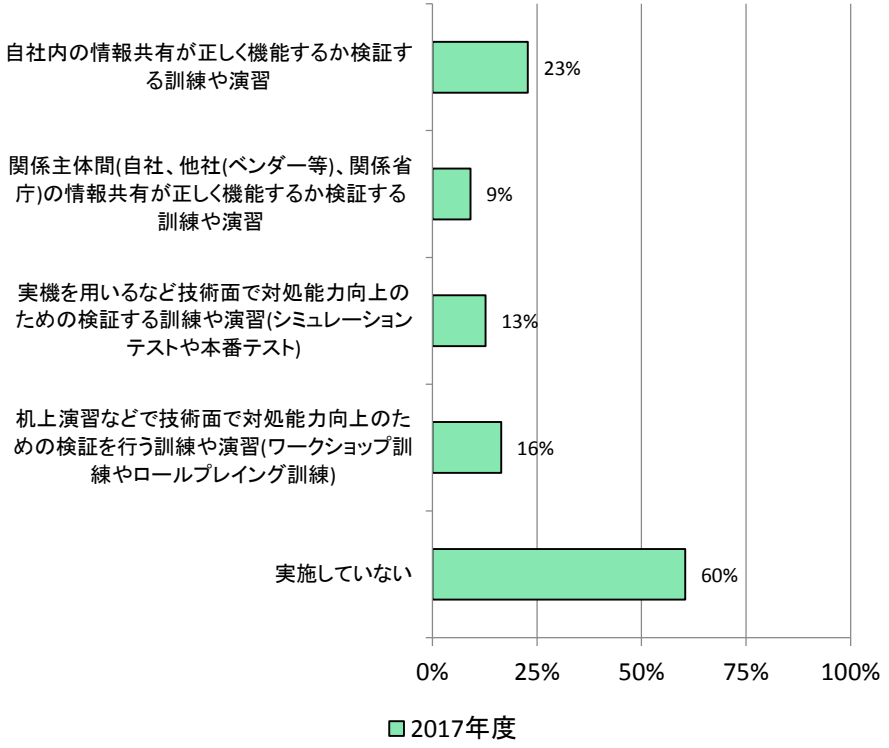
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（28/30）－

設問35　内部での訓練・演習の実施内容

・内部での訓練・演習を実施していない事業者等は6割程度になっている。内部での訓練・演習が難しい場合、分野横断的演習等、外部の訓練・演習に参加することが望まれる。

内部での訓練・演習の実施内容（複数回答）

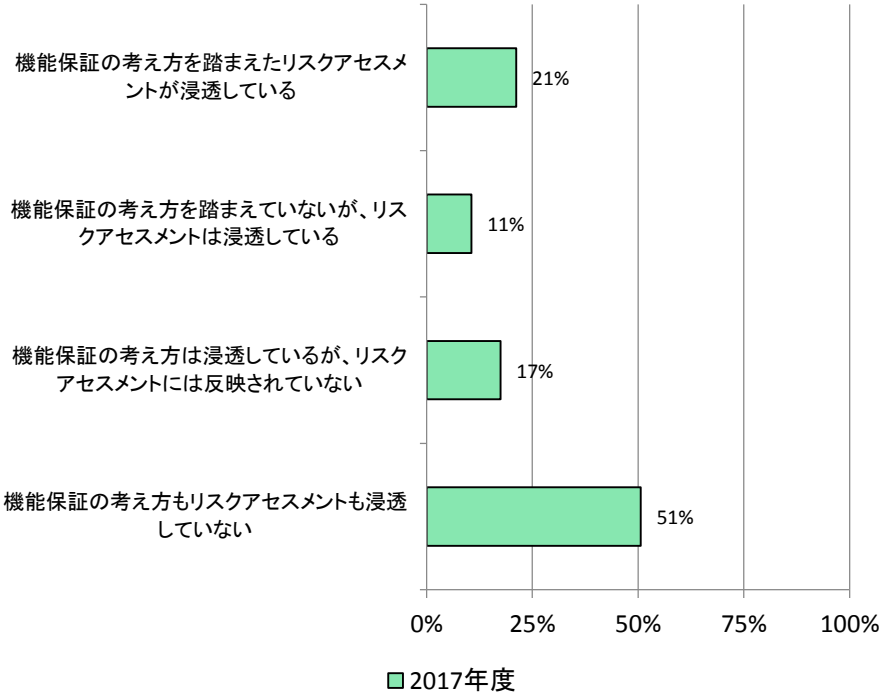


※金融は読替え可能項目なし（集計していません）

設問36　機能保証の考え方を踏まえたリスクアセスメントの認知状況

・機能保証の考え方を踏まえたリスクアセスメントは、まだ十分には浸透していない。今後公表予定の、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」や、関連文書である「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」等を参照し、機能保証の考え方を踏まえたリスクアセスメントの取組を進めてほしい。

機能保証の考え方を踏まえたリスクアセスメントの認知状況（単一回答）



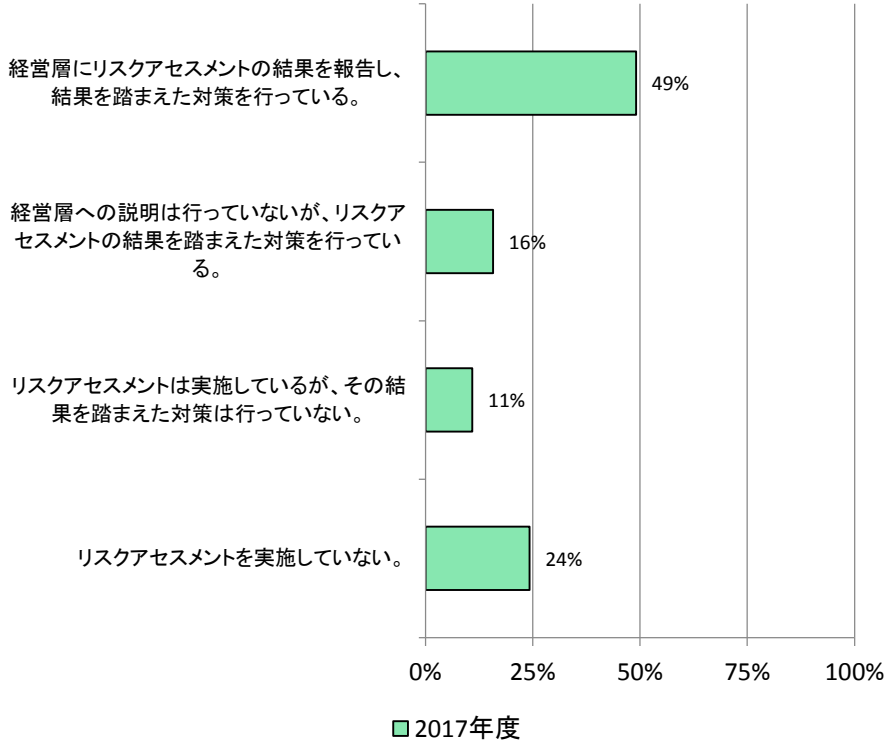
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（29/30）－

設問36-1　結果を踏まえた対策の実施状況

・リスクアセスメントの結果を経営層へ報告している事業者が半数にとどまっている。リスクアセスメントの結果を踏まえたリスク低減等の対応を戦略的に講じることは経営者の責務であるため、経営層への更なる働きかけが必要である。NISCでは、経営層が果たすべき役割を盛り込んだ「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」等を、今後公表予定である。

結果を踏まえた対策の実施有無（単一回答）

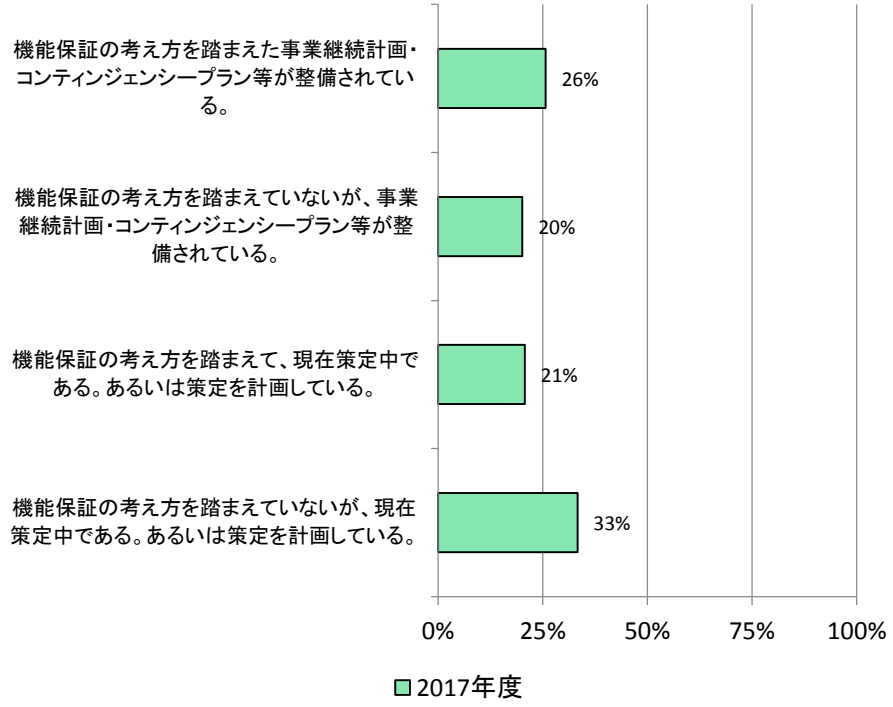


※金融は読替え可能項目なし（集計していません）

設問37　機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の策定状況

・事業継続計画やコンティンジェンシープランの策定は一定浸透しているが、機能保証の考え方はまだ一部にしか浸透していない。今後公表予定の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」等を参考に、機能保証の考え方を取り入れることが望まれる。

機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の策定状況（単一回答）



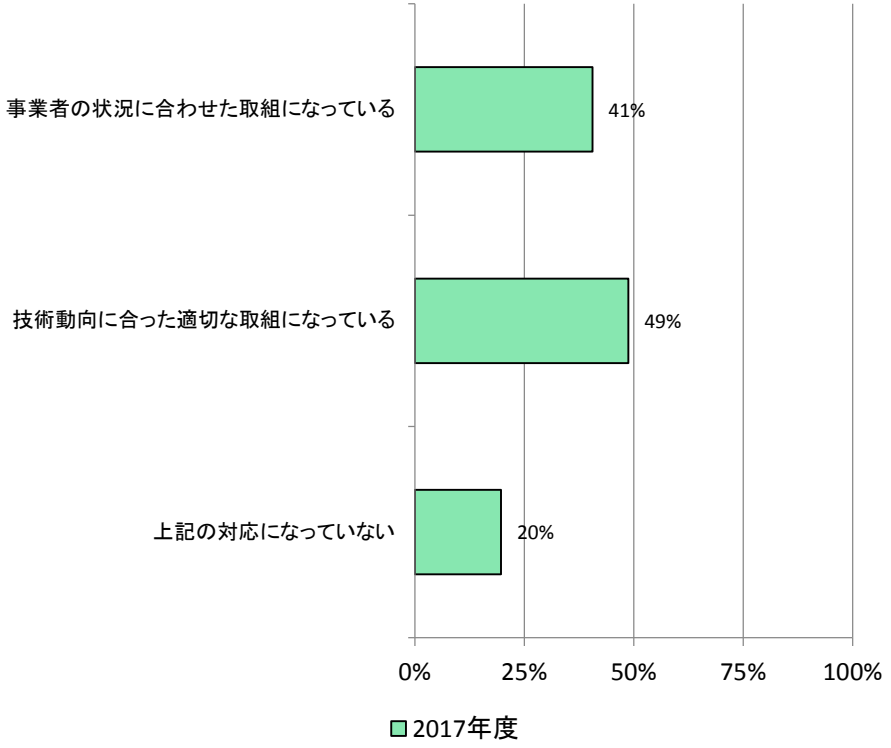
※金融は読替え可能項目なし（集計していません）

5．調査結果詳細 －（30/30）－

設問38　国の施策に対する意見

・多くの事業者等が、国の施策について「事業者の状況に合わせた取組になっている」又は「技術動向に合った適切な取組になっている」と考えており、今後も事業者の状況や技術動向を踏まえ、適切な取組を行っていきたい。

国の施策に対する意見（単一回答）

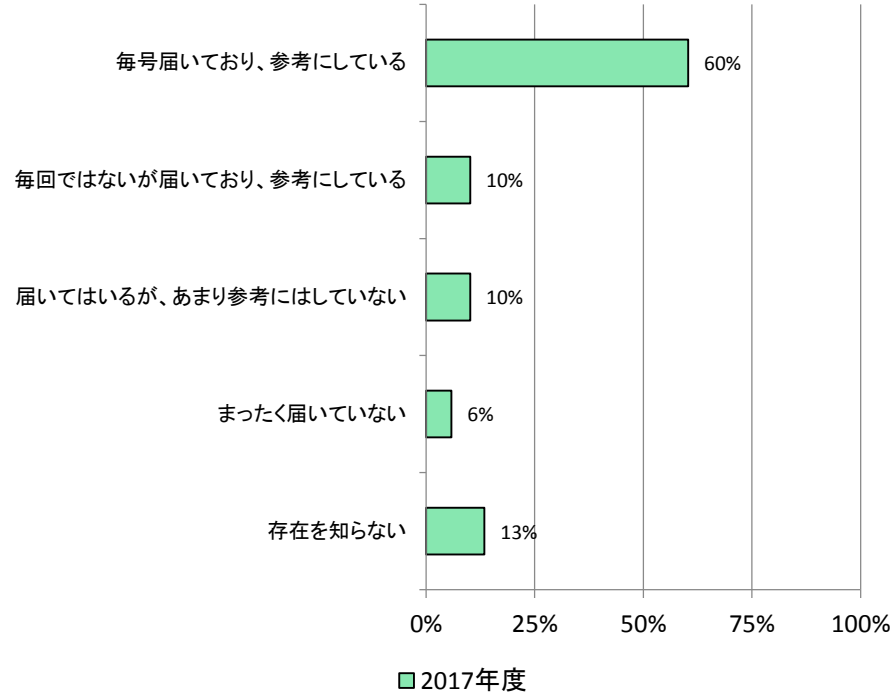


※金融は読替え可能項目なし（集計していません）

設問39　重要インフラニュースレターに関する状況

・7割程度の事業者等が重要インフラニュースレターを参考にしており、今後もより多くの事業者等にとって有益なものとなるよう、内容の充実や周知をさらに進めていきたい。

重要インフラニュースレターに関する状況（単一回答）



※金融は読替え可能項目なし（集計していません）

5．調査結果詳細　－　自由意見 (1/2) －

【安全基準等、指針に関する意見】

- 規模の大きい事業者等を前提としているように感じるため、小規模事業者等用など規模ごとに分類されていれば参考になるのではないか。
- 改定があった場合は、新旧比較表を出してほしい。
- 安全基準等は、複数あってもよいのではないか。（ex.経営層向け、運用者向け、オペレータ向け、ユーザー向け 等）
- セキュリティ対策を実施しなければいけないことは十分承知しているが、中小規模の事業者等では、人員や予算の関係上、なかなか対策に踏み出しきれないのが現状。

【情報共有体制の推進に関する意見・要望等】

- 共有されている情報が多岐にわたり詳細に記載されているため非常に参考になっている。しかし、同一情報源の重複する情報も多く共有されているため、閲覧に時間が取られてしまうのが現状。
- 各所から様々な情報が提供されているが、分かりにくい。情報提供も同一組織からまとめて提供されるような体制があると、各事業者等も情報を管理しやすくなるのではないか。
- 関係省庁や関連団体、NISC等から情報発信されることで、そのリスクや対応方法を知ることができるだけではなく、内規の見直しの契機にもなる。今後とも積極的に情報提供いただきたい。
- 情報の入手については積極的に行っているが、情報発信（報告）については消極的であるのが現状。

5．調査結果詳細　－　自由意見 (2/2) －

【アンケートに関する意見】

- 本アンケート調査は専門用語が多く、回答が難しい。より多くの理解を得るためにも、分かりやすく丁寧な説明が必要。
- こういったアンケート調査に回答することで、自組織の対策状況が把握できるため、非常に役立っている。
- 業界団体経由での依頼だが、その団体がセプター事務局であっても業界団体経由での提出は情報セキュリティ上問題があると考える。業界団体・事務局スタッフは、同業他社のスタッフでもあり得るためである。アンケート回答が守秘されるよう検討いただきたい。
- WEBアンケート等を利用し、もう少し簡単にアンケートに回答できるようにしてほしい。

【国・政府に対する意見・要望等】

- セキュリティ対策の項目等は専門用語をできるだけ避け、図やチャートで説明するような取組が必要ではないか。
- 分野によっては、インセンティブが働かない限り、セキュリティ関連の対策（システム導入、人材育成、教育等）は取られないのではないか考える。
- これまで報告している安全関係の報告以外にも、セキュリティに関するインシデントの報告意識の醸成が必要。
- 中小事業者等向けの情報セキュリティ対策に関わる補助金等を整備いただきたい。
- IT人材育成に向けた支援を重視していただきたい。

【その他の意見】

- 社内や外部でのCTFを実施するのもよいのではないか。

6．＜参考＞　－　アンケート項目(1/3)　－

調査に用いたｱﾝｹｰﾄ項目は以下の通り。なお、各項目のｸﾞﾗﾌについては「5.調査結果詳細」の該当設問を参照のこと

【Ⅰ．前提条件】

分野の選択
従業員数（規模）の選択

【Ⅱ．浸透状況等調査項目】

設問1	NISCの取組の認知状況
設問2	自分野の安全基準等の認知状況
設問3	情報セキュリティ対策の実施に向けた予算の確保状況
設問4	セキュリティ人材の確保状況
設問4-1	必要とする人材の職種
設問5	セキュリティ人材育成の取組状況
設問6	全従業員向けセキュリティ研修の実施状況
設問7	内部体制の取組状況
設問8	情報セキュリティ対策のノウハウの蓄積方法
設問9	情報セキュリティ対策に関する基本方針の策定状況
設問9-1	基本方針の策定に関する経営層の関与状況
設問9-2	策定した基本方針の外部公表状況
設問9-3	基本方針の見直し検討状況
設問9-4	基本方針の見直し検討の契機
設問10	情報セキュリティ対策に関する計画策定状況
設問10-1	計画の見直し（又は修正）状況
設問11	取扱い情報資産（システム含む）の洗い出し及び台帳等での管理状況
設問11-1	情報資産の重要度に応じた格付け状況
設問11-2	情報資産の見直し状況
設問12	脅威や脆弱性等の情報収集
設問12-1	情報収集の確認頻度
設問13	リスクの特定状況
設問13-1	リスクの特定方法
設問14	リスク対応の要否に係る判断基準

6．＜参考＞　－　アンケート項目(2/3)　－

【Ⅱ．浸透状況等調査項目】（続き）

設問15	リスク対応の優先順位に係る判断基準
設問16	リスクに応じた対応手段の判断基準
設問17	リスク対応に関する判断結果についての経営層の把握状況
設問18	情報セキュリティに関する内規の策定状況
設問18-1	内規等を策定する際の参考文献
設問18-2	策定した内規の見直し検討状況
設問18-3	内規の見直し検討の契機
設問19	情報の取扱いに関する規定の策定状況
設問20	事業継続計画の策定状況
設問20-1	事業継続計画に基づいた訓練状況
設問20-2	事業継続計画の見直し状況
設問20-3	事業継続計画の見直し契機
設問21	コンティンジェンシープラン策定状況
設問21-1	コンティンジェンシープランの見直し状況
設問22	外部委託に関する規定の策定状況
設問23	外部委託先管理に関する対策
設問24	実施済みの情報セキュリティ対策
設問25	責任者へのセキュリティ対策の運用報告
設問25-1	経営層への情報セキュリティ運用報告
設問26	対外向けの情報共有窓口の設置状況
設問27	障害発生時における連絡体制の整備状況
設問28	障害発生時の利用者アナウンスの判断基準
設問29	情報セキュリティに関する監査実施状況
設問29-1	監査を通じた対策の是正検討状況
設問30	外部の演習等への参加状況
設問31	内部での演習等の実施状況

6．＜参考＞　－　アンケート項目(3/3)　－

【Ⅲ．国の施策の取組状況調査】

設問32　情報共有体制下での受信状況
設問32-1　受信情報の有効活用度
設問33　能動的に行った情報共有状況
設問34　分野横断的演習の認知状況
設問35　内部での訓練・演習の実施内容
設問36　機能保証の考え方を踏まえたリスクアセスメントの認知状況
設問36-1　結果を踏まえた対策の実施状況
設問37　機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の策定状況
設問38　国の施策に対する意見
設問39　重要インフラニュースレターに関する状況

【Ⅳ．　自由記述】

a.　本編及び対策編に対する意見（自由意見を記載）
b.　安全基準等に対する意見（自由意見を記載）
c.　その他の意見（自由意見を記載）
d.　NISCの取組についての意見（自由意見を記載）
e.　セキュリティ人材についての意見（自由意見を記載）
f.　人材育成についての意見（自由意見を記載）
g.　内部統制強化についての意見（自由意見を記載）
h.　ノウハウの蓄積方法についての意見（自由意見を記載）
i.　基本方針の見直し契機についての意見（自由意見を記載）
j.　リスクの特定方法についての意見（自由意見を記載）
k.　内規の策定する際の参考文献に関する意見（自由意見を記載）
l.　内規の見直し契機についての意見（自由意見を記載）
m.　事業継続計画の見直し契機についての意見（自由意見を記載）
n.　セキュリティ対策の実施手法に関する意見（自由意見を記載）
o.　情報共有（受信側）に関する意見（自由意見を記載）
p.　情報共有（送信側）に関する意見（自由意見を記載）