資料３

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

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年度）

2019年４月18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．安全基準等の浸透状況等に関する調査の位置づけ　P.2

２．安全基準等の浸透状況等に関する要約　P.３ - P.８

３．アンケート調査　P.９ – P.76

４．往訪調査　P.77– P.82

＜参考＞

参考１．アンケート調査の項目　P.84– P.86

1．安全基準等の浸透状況等に関する調査の位置づけ

※重要インフラの情報セキュリテイ対策に係る第４次行動計画（抜粋）

重要インフラ事業者等における安全基準等の浸透状況のより精緻な把握を目的に、内閣官房は、毎年、重要インフラ事業者等の対策状況についてのアンケート調査及び往訪調査を実施する。アンケート調査については、重要インフラ事業者等における安全基準等の浸透及び取組の改善につながるよう、随時調査項目の見直しを行う。

（中略）

また、アンケート調査結果から得られた仮説の検証及び良好事例の収集を目的に、重要インフラ事業者等へ往訪調査を行う。

なお、アンケート調査及び往訪調査によって得られた調査結果については、原則、年度ごとに公表するとともに、本行動計画の各施策の改善に活用する。

安全基準等の浸透状況等に関する調査 ＝

アンケート調査（P.9～）

◆ **目的**

・「安全基準等」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

◆ **調査内容**

・重要インフラ事業者等の情報セキュリティ対策の現状

◆ **調査数**

・回答2,050者（配付3,409者）

＋

往訪調査（P. 73～）

◆ **目的**

・アンケート調査結果から得られた仮説の検証及び良好事例の収集

◆ **調査内容**

・経営層の関わり方について
・演習や訓練について　等

◆ **調査数**

・アンケート調査結果・地域特性・事業規模を踏まえ、選定した16者

◆ **調査方法**

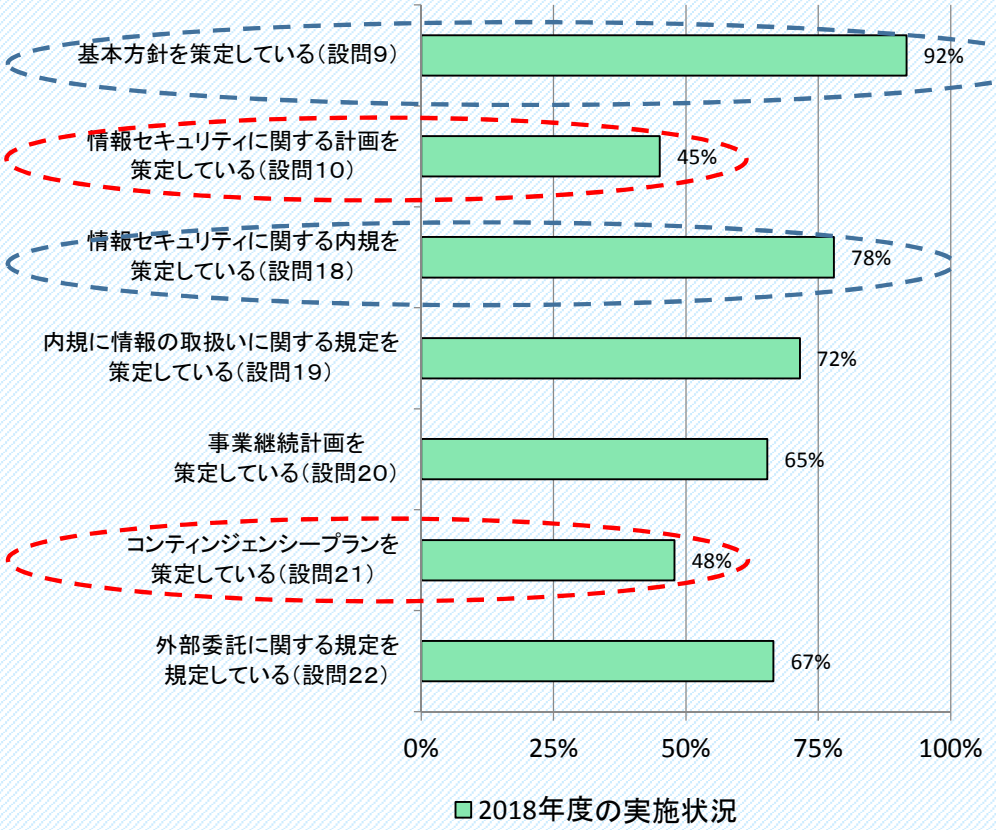
・アンケート調査結果を基にしたヒアリング

2.1. アンケート調査の要約（1/5）

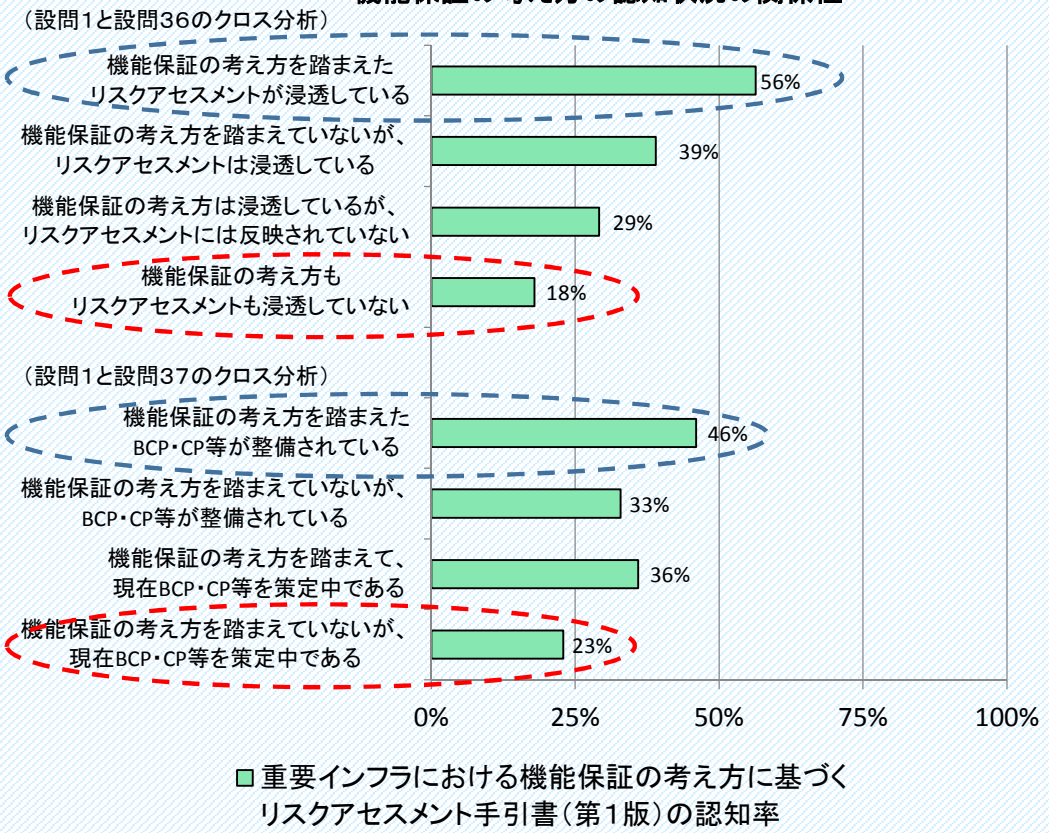
(1) 規定類の整備状況と機能保証の考え方についての状況

- 基本方針や情報セキュリティに関する内規が策定されている（グラフ① 青枠内）。一方で、情報セキュリティに関する計画・コンティンジェンシープランが策定されていない（グラフ① 赤枠内）。
  新たなリスクに対応し続けていくための計画である情報セキュリティリスク対応計画や初動対応（緊急時対応）の方針を定めたコンティンジェンシープランを策定する事業者を増やし、対処態勢整備を強化することが重要である。
- リスクアセスメント手引書を認知している事業者等は、「機能保証」の考え方を踏まえたリスクアセスメントの実施及びBCP・CPの整備が進んでいる（グラフ② 青枠内）。一方で、認知していない事業者等は取組が遅れている（グラフ② 赤枠内）。
  サイバーセキュリティ戦略にも記載されている、「任務保証」の考え方を踏まえたリスクアセスメント、BCP・CPの策定が重要であるため、見直し等により「機能保証」の考え方が盛り込まれるよう、リスクアセスメント手引書を普及・啓発が重要である。

グラフ① 各種規程類の整備状況（複数回答）



グラフ② リスクアセスメント手引書の認知状況と機能保証の考え方の認知状況の関係性

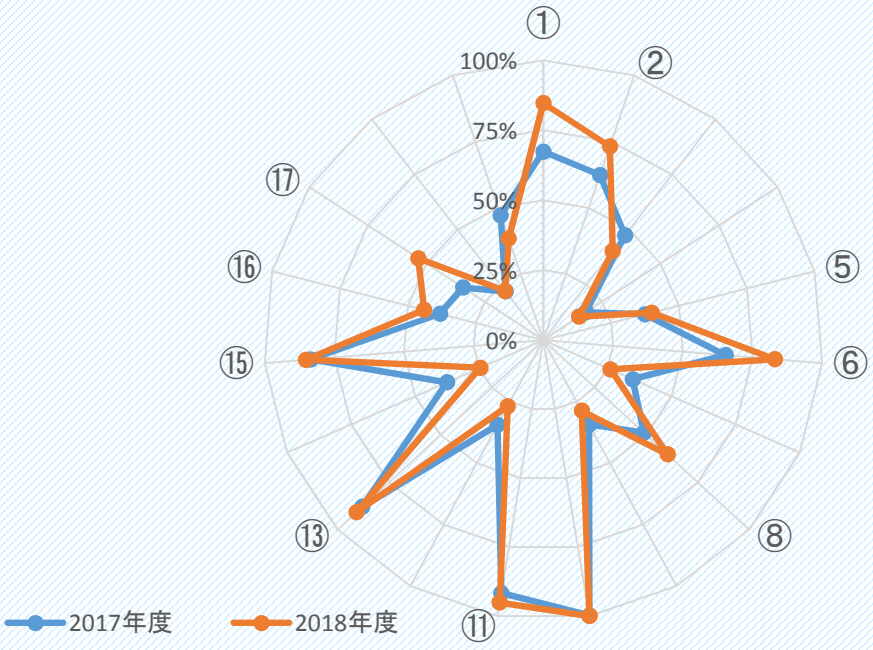


2.1. アンケート調査の要約（2/5）

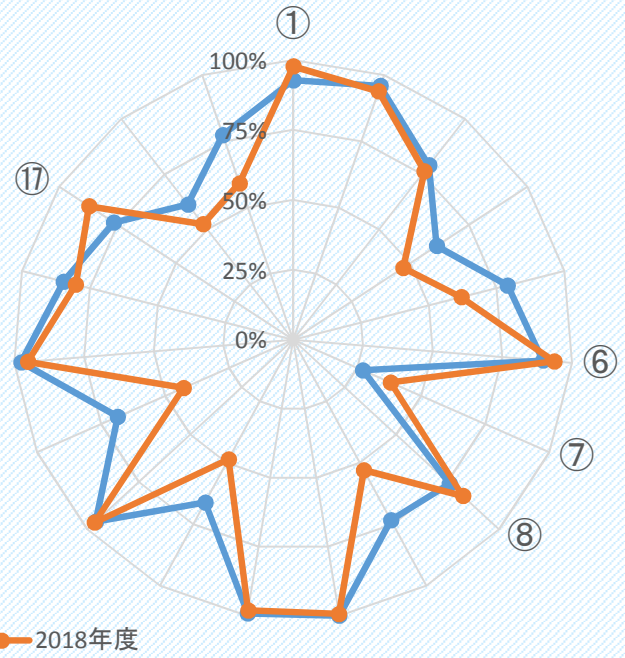
(2) 対策状況

- 従業員1,000人以下の企業（グラフ①）は、昨年からの各対策の強化による影響により以下の良化ポイントが見られる。
  ①情報セキュリティ対策に関する基本方針の策定　②情報セキュリティに関する内規の策定状況
  ⑤情報セキュリティ対策に関する計画策定状況　⑥情報セキュリティ対策の実施に向けた予算の確保状況
  ⑧全従業員向けセキュリティ研修の実施状況　⑪責任者へのセキュリティ対策の運用報告
  ⑬障害発生時における連絡体制の整備状況　⑮脅威や脆弱性等の情報収集
  ⑯情報セキュリティに関する監査実施状況　⑰【CA-平時】外部の演習等への参加状況
- 従業員1,001人以上の企業（グラフ②）は、昨年からの各対策の強化による影響により以下の良化ポイントが見られる。
  ①情報セキュリティ対策に関する基本方針の策定　⑥情報セキュリティ対策の実施に向けた予算の確保状況
  ⑦セキュリティ人材の確保状況　⑧全従業員向けセキュリティ研修の実施状況
  ⑰【CA-平時】外部の演習等への参加状況
- PDCAサイクルにおいて、取組が進んでいない（グラフ①,②上凹んでいる）項目については、取組が進んでいる事業者等に往訪調査等で確認し、全体を真円に近づけられるよう、得られた結果を展開する必要がある。

グラフ①　行動計画テーマ別グラフ（従業員1,000名以下）



グラフ②　行動計画テーマ別グラフ（従業員1,001名以上）

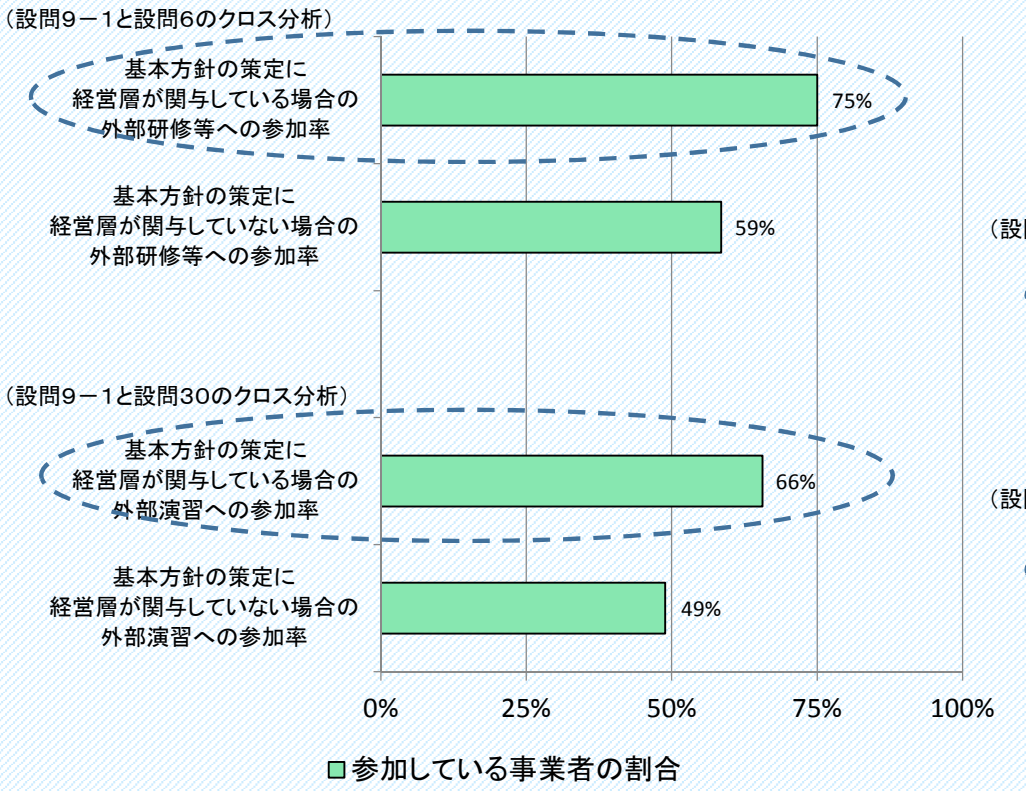


2.1. アンケート調査の要約（3/5）

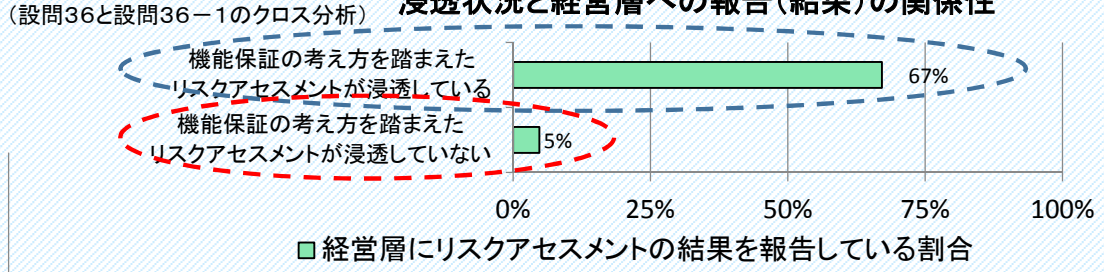
(3) 経営層の関与状況

- 基本方針の策定に経営層が関与している事業者等は、他事業者等の取組事例や外部研修等で推奨されている内容を把握するために、外部での研修や演習等に参加している傾向があるため、他事業者動向を認識する意義も含めて、分野横断的演習の参加を推奨していく必要がある（グラフ①）。
- 機能保証の考え方を踏まえてリスクアセスメントを実施している事業者は、経営層までリスクアセスメントの報告を行っている傾向があるため、機能保証の考え方を普及・啓発していくことが重要である（グラフ②）。
- リスク対応において経営層が積極的に関与している事業者等は、情報資産管理や管理している資産の格付けを実施している傾向があるため、リスク対応に関して、経営層に働きかけていく必要性が認められる（グラフ③）。

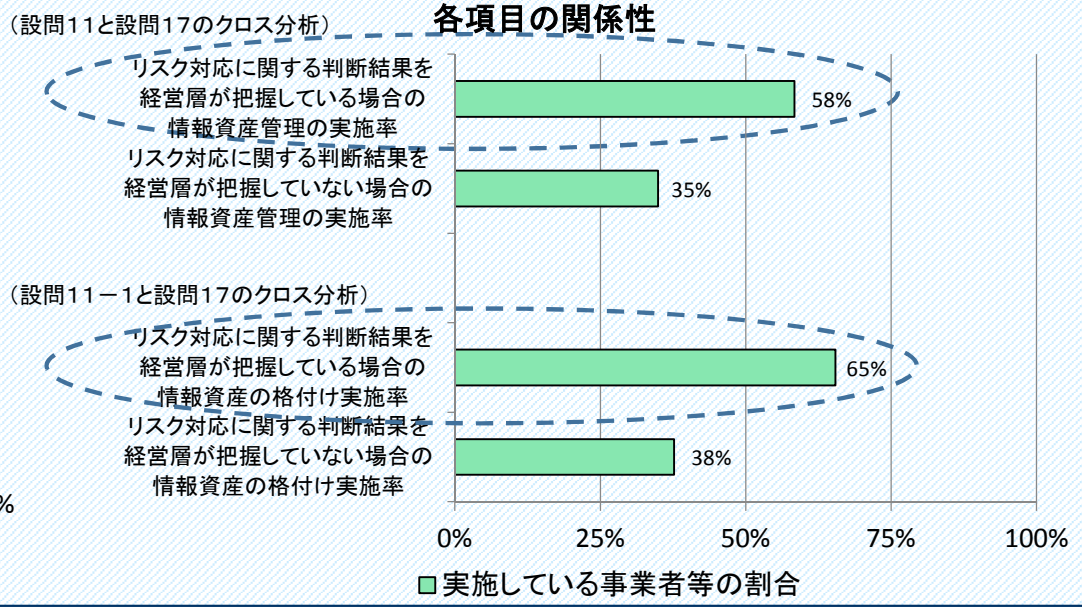
グラフ① 基本方針策定時の経営層の関与と各項目の関係性



グラフ② 機能保証の考え方（リスクアセスメント）の浸透状況と経営層への報告（結果）の関係性



グラフ③ リスク対応における経営層の関与と各項目の関係性

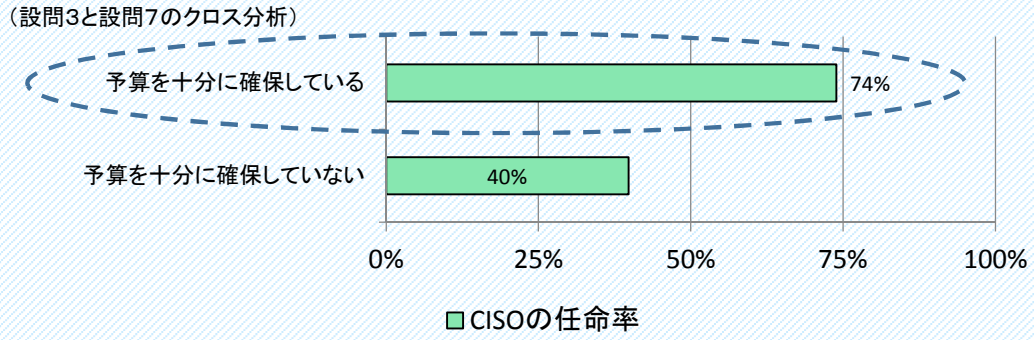


2.1. アンケート調査の要約（4/5）

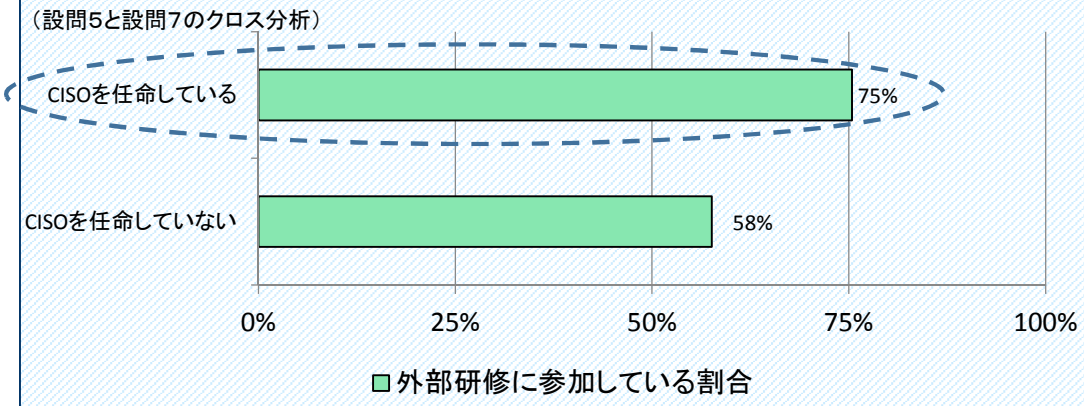
(4) CISOの任命状況

- 情報セキュリティ対策の実施を取り組む上で十分な予算が確保されている事業者等は、CISOを任命している割合が高く、経営層の働きかけにより、確保されていると考えられる（グラフ①）。
- CISOを任命している事業者等は、セキュリティ人材を育てるために、積極的に外部への研修に参加している（グラフ②）。
- 内規等を策定する際の参考文献として、所管省庁が発行しているガイドライン・指針等を参考にしている事業者等は、CISOを任命している傾向がある。NISCが定めている安全基準等策定指針にもCISOの任命を求めていることが、所管省庁発行のガイドライン・指針等に反映されているためであると考えられる（グラフ③）。

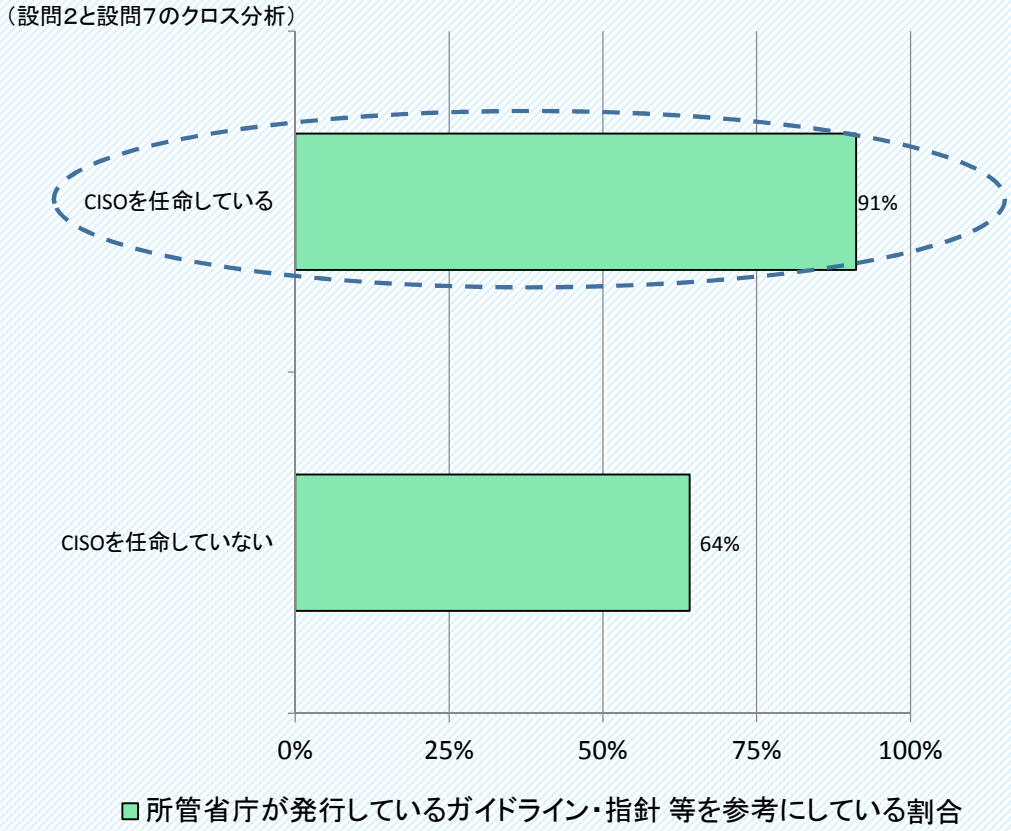
グラフ① 予算の確保状況とCISOの任命状況の関係性



グラフ② CISOの任命状況と外部研修の参加状況の関係性



グラフ③ CISOの任命状況と内規等を策定する際の参考文献の関係性



2.1. アンケート調査の要約（5/5）

(5) 自由意見

【安全基準等に関する意見・要望等】

- 事業規模を考慮した基準等や費用対効果の高い対策等の例示の要望があった。
  （備考：事業規模の小さい事業者の人材育成、費用を抑える仕組み等）

  ＜参考例＞ 中小企業の情報セキュリティ対策ガイドライン第３版　等　（IPA）
  サイバーセキュリティ経営ガイドラインVer 2.0実践のためのプラクティス集　等（IPA）

【安全基準等策定指針（第5版）に関する意見・要望等】

- 指針を活用したガイドラインにおいて、一部分野で参考資料としてチェックシートが作成されているが、多くの分野で対策例を示してほしいという要望があった。

  ＜参考例＞対策例：補完調査報告書（NISC）等

【情報共有体制に関する意見・要望等】

- 情報共有方法（メール、システム、電話等）の統一化してほしい。
- 最新の重要インシデント（ヒヤリハット含む）を早期に情報、評価結果、対策を情報共有できる体制。
- 報告ルート一本化による事業者負担を軽減してほしい。
- 情報システム部とセキュリティベンダーの月例会を実施し、サイバーセキュリティインシデントに関する情報交換を行っている。

【その他の意見・要望等】

- 初心者でもわかりやすい解説がほしい。

  ＜参考例＞　関連JIS　Q 27001の解説書　等
- 担当者が少ない事業者向けの良好事例を紹介してほしい。

  ＜参考例＞　中小企業における情報セキュリティ対策の実態調査（IPA）　等
- 国の演習や人材育成等の紹介してほしい。

  ＜参考例＞　CYDER（NICT）、分野横断的演習（NISC）等

2.2. 往訪調査で収集した良好事例のトピック

往訪調査を通じて収集した良好事例の中から、特に紹介したい良好な事例は下記である。

■新システムの導入を見据えたインシデント対応訓練（ P.７５ ）

重要インフラ事業者等は、標的型攻撃メール訓練や自社ルールに基づく訓練を、e-lerningや分野横断的演習などを通じて防護能力の維持・向上を図るべきである。

新システム導入による初動対応の変更点を訓練を通じて、定着化させている事業者等がある。具体的には、新システム導入により想定されるサイバー攻撃やシステム不具合の挙動を周知し、挙動を確認している。

訓練の時期：システム導入前

訓練対象者：重要システム関係者（運用者・保守員・設計者）

■社内の情報共有（社内CSIRT）（ P. ７６ ）

重要インフラ事業者等は、情報セキュリティ部門を中心に、情報共有体制を構築するべきである。

情報セキュリティ部門だけでなく制御部門に対して、国内外の最新インシデント情報やCSMS認証等の紹介を行い、情報セキュリティへの取り組み意識を醸成させている事業者等がある。

■外部委託事業者との外部委託契約での内部犯行の抑制（ P. ７７ ）

昨今のサプライチェーンリスクを鑑み、外部委託事業者やその再委託先等が重要インフラ事業者の資産にアクセスするリスクを低減する取組を行うべきである。

内部犯行対策として有効な事項を外部委託契約書に明記し、発注事業者と外部委託事業者の双方で内部犯行を防止している事業者等がある。

（犯行対策の例）

申請外作業の禁止、単独作業禁止、作業前セキュリティ更新プログラム（パッチ）の適用、セキュリティ教育受講　等

3.1. アンケート調査の目的、概要及び内容

◆アンケート調査の目的

アンケート調査は、重要インフラ所管省庁（以降、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（以下、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、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。

アンケート調査への回答を通じて、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、アンケート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。

◆アンケート調査の概要

・アンケート調査対象範囲　　：所管省庁にて調査対象の事業者等を決定
・アンケート調査方法と調査基準日：以下の方法のいずれかを所管省庁が選択
　① NISCが準備する調査票（アンケート）を活用　　（基準日：2018年3月末日）
　② 関連組織が独自に行う調査の結果をNISCで読み替え（基準日：各調査で設定した基準日）

注）今年度より政府・行政サービス分野は、NISCが準備する調査票（アンケート）を利用して回答を実施しているため、一部の設問で回答の傾向が大幅に変化している。

◆アンケート調査の内容

・安全基準等の整備・浸透に係る事項：① 行動計画※2や指針※3 、リスクアセスメント手引書※4等の認知状況
　② 事業者等が定める内規の策定・見直しの状況　等
・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
・意見、要望

※1 安全基準等
関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令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」、関係法令や国民・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。

※2 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　（サイバーセキュリティ戦略本部決定）
昨今のサイバー攻撃による急速な脅威の高まりや、2020東京オリンピック・パラリンピック競技大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第３次行動計画を見直したもの。

※3 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）　（サイバーセキュリティ戦略本部決定）
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導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。

※4 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（第1版）　（サイバーセキュリティ戦略本部決定）
情報セキュリティ確保に係るリスクアセスメントの考え方や具体的な作業手順に関するフレームワークを提供することにより、重要インフラ事業者等におけるリスクアセスメントの理解を深め、その精度や水準の向上に寄与するとともに、重要インフラ事業者等による自律的な情報セキュリティ対策を促進することを目的としているもの。

3.2. 重要インフラ分野のアンケート調査状況

NISC独自アンケートの配布は重要インフラ13分野(*1)の2,610事業者等。回答は1,381事業者等。
（昨年度比　配布数：284%　回答数：200%　回答率：-22.1ﾎﾟｲﾝﾄ*1 ）(*2)

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-CEPTOAR構成各社、電気通信事業者協会正会員各社	72	23	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	334	125	
	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）	196	191	
金融		銀行等、証券会社、生命保険会社、損害保険会社	(799)	(669)	独自調査(*3)
航空		航空運送事業者	2	1	NISC調査
鉄道		鉄道CEPTOAR構成員事業者	22	19	
電力		一般送配電事業者、主要な発電事業者	12	12	
ガス		ガスセプターを構成する主要ガス事業者	11	11	
政府・行政サービス		地方公共団体	1,788	866	
医療		電子カルテ等の医療情報システムを導入している医療機関の中からランダムで選定した事業者	31	18	
水道		現在給水人口30万人以上の水道事業者又は水道用水供給事業者	79	70	
物流		物流CEPTOAR構成員事業者	17	11	
化学		石油化学工業協会に加盟する事業者のうち主にエチレンセンターを運営する企業	13	9	
クレジット		リスクアセスメント対象会社（自社でオーソリゼーションシステムを保有しているクレジットセプター構成員）	21	18	
石油		石油精製企業	12	7	
全分野合計		－ － －	2,610 (3,409)	1,381 (2,050)	－ － －

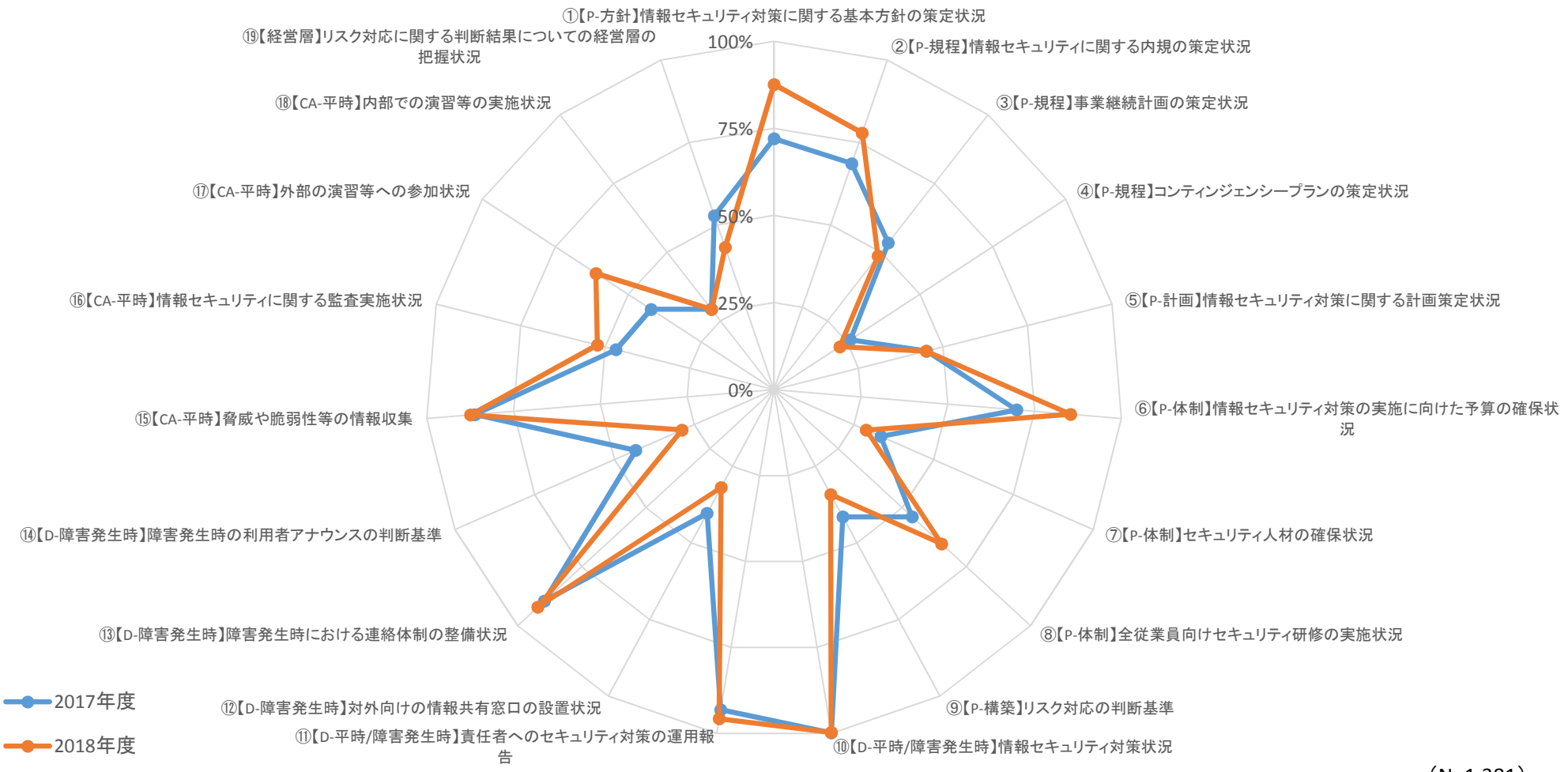
＊１：2018年3月末日基準のアンケート調査のため、2018年7月に重要インフラ分野として追加された「空港分野」は対象外である。
＊２：政府・行政サービス分野が、今年度からNISC独自アンケートを利用して、回答を実施したため。
＊３：金融機関等のシステムに関する動向及び安全対策実施状況調査（調査基準日：2018年3月31日）

3.3. アンケート調査結果概要 – PDCAサイクルに沿った対策状況(1/4) –

(1) 全分野の重要インフラ事業者

※2018年度は金融分野を、
2017年度は金融・自治分野を除く

行動計画のテーマ別グラフ(レーダーチャート(全分野集計))



(N=1,381)

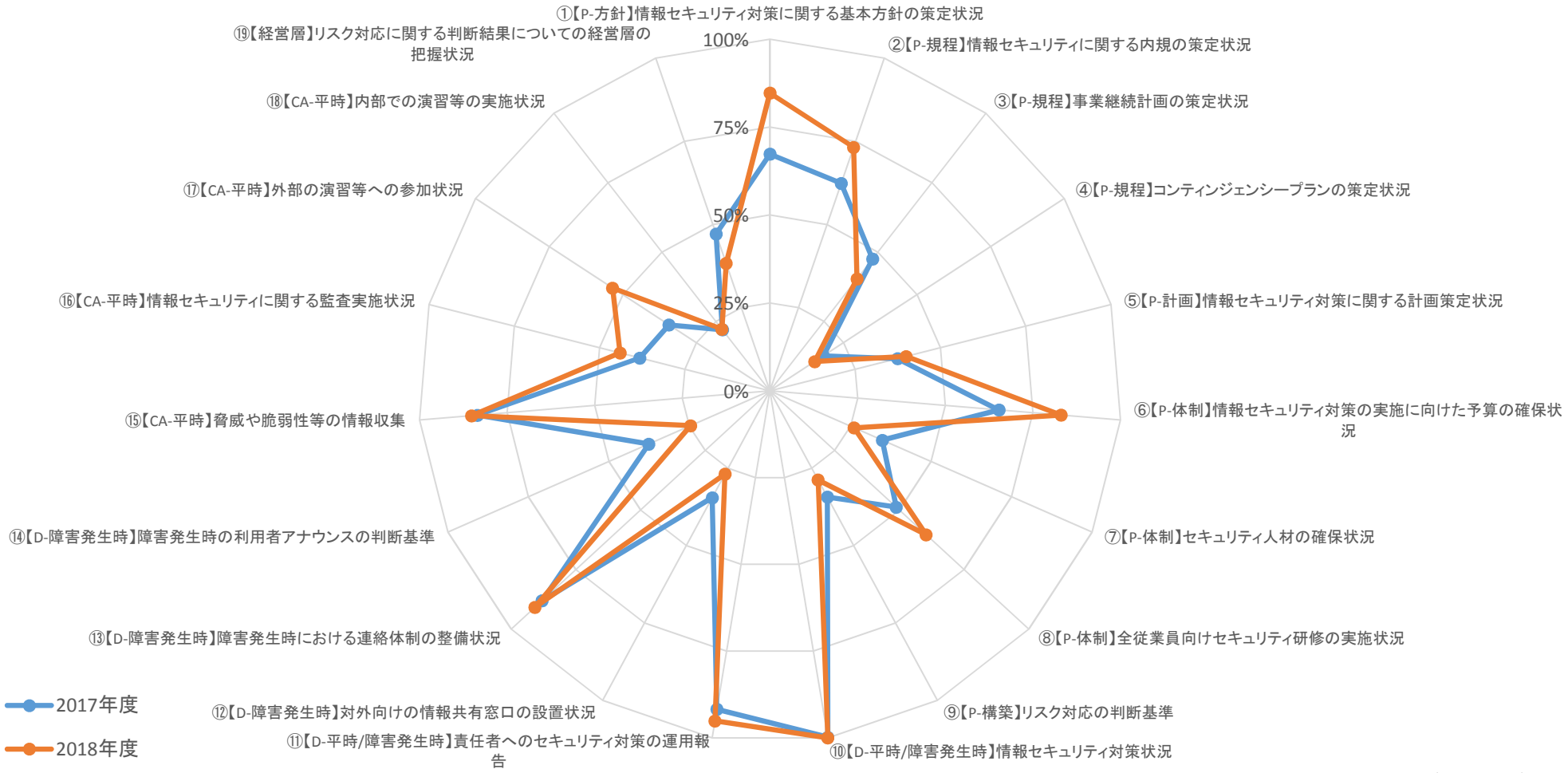
	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	72.0%	68.6%	53.4%	26.2%	45.1%	69.9%	33.4%	53.9%	41.5%	99.9%	93.1%	40.4%	89.5%	43.3%	86.1%	46.8%	42.2%	29.3%	52.8%
2018年度	87.6%	77.9%	48.6%	22.5%	45.0%	85.4%	28.9%	65.3%	34.2%	99.7%	95.7%	31.9%	92.1%	28.8%	87.4%	52.3%	61.0%	29.2%	43.2%
2019年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2020年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

3.3. アンケート調査結果概要 – PDCAサイクルに沿った対策状況(2/4) –

(2) 従業員1000名以下の重要インフラ事業者

※2018年度は金融分野を、
2017年度は金融・自治分野を除く

行動計画のテーマ別グラフ(レーダーチャート(1,000名以下の事業者等))



(N=1,064)

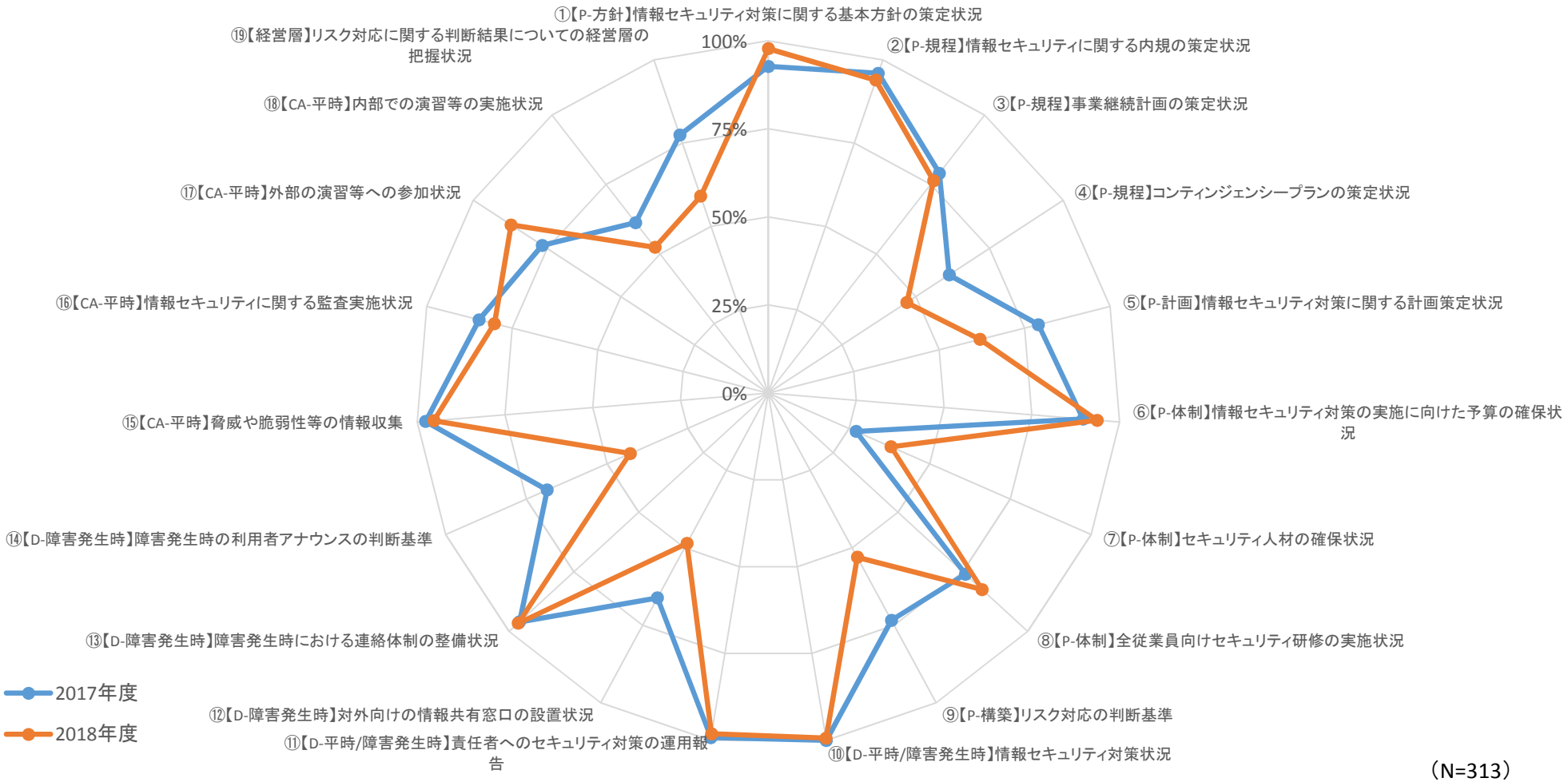
	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	67.3%	62.4%	47.5%	18.2%	37.4%	65.3%	34.9%	48.8%	34.3%	99.8%	91.7%	34.5%	88.1%	37.6%	83.5%	38.2%	34.3%	22.0%	47.2%
2018年度	84.7%	73.2%	40.3%	15.2%	39.9%	83.1%	26.1%	60.3%	28.8%	100%	95.1%	26.9%	90.9%	24.6%	85.2%	44.0%	53.5%	22.3%	38.3%
2019年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2020年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

3.3. アンケート調査結果概要 – 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

※2018年度は金融分野を、
2017年度は金融・自治分野を除く

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))

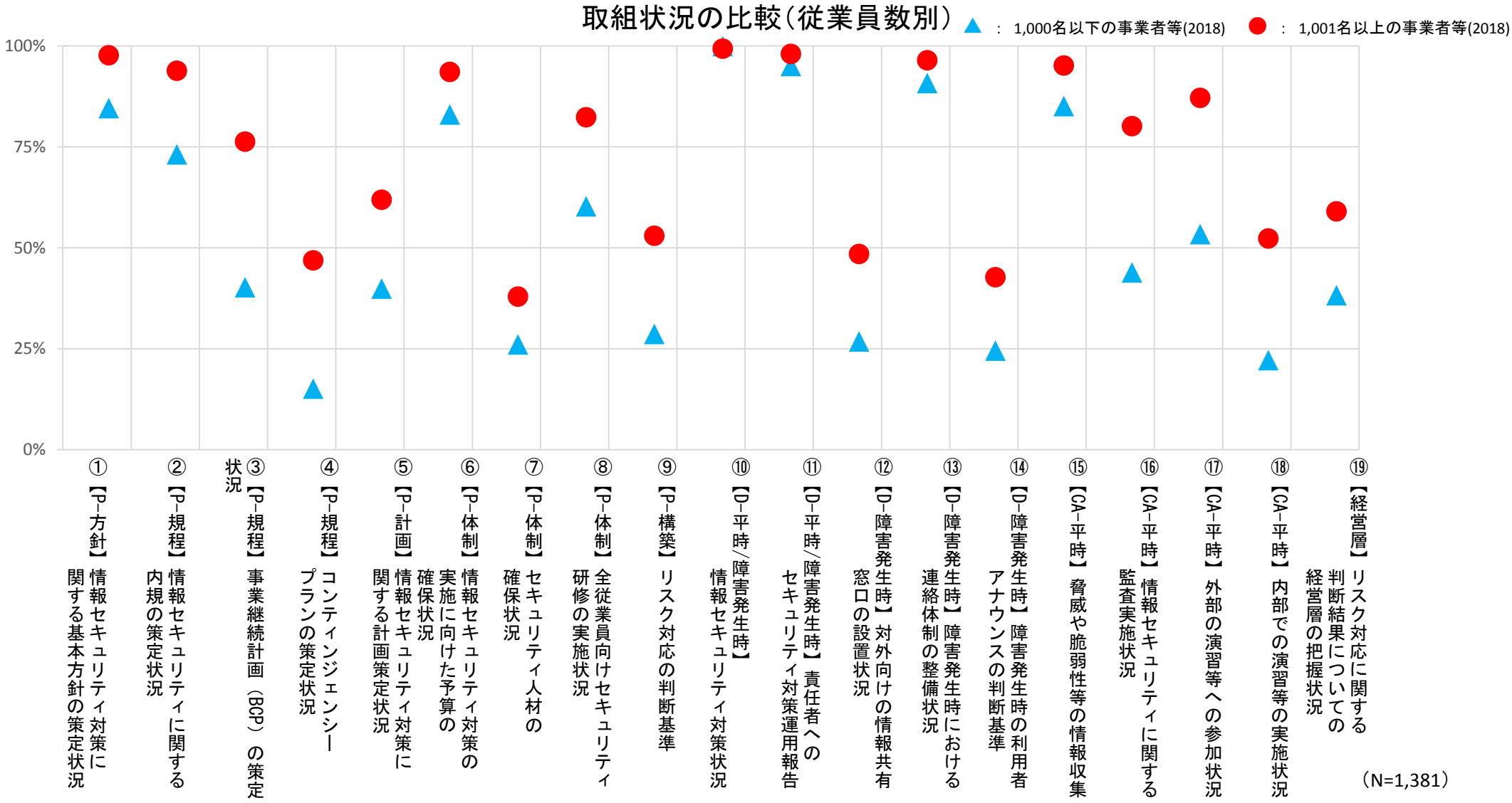


(N=313)

	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	97.8%	93.9%	76.4%	47.0%	62.0%	93.6%	38.0%	82.4%	53.0%	99.4%	98.1%	48.6%	96.5%	42.8%	95.2%	80.2%	87.2%	52.4%	59.1%
2019年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2020年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

3.3. アンケート調査結果概要 – 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（2018年度）



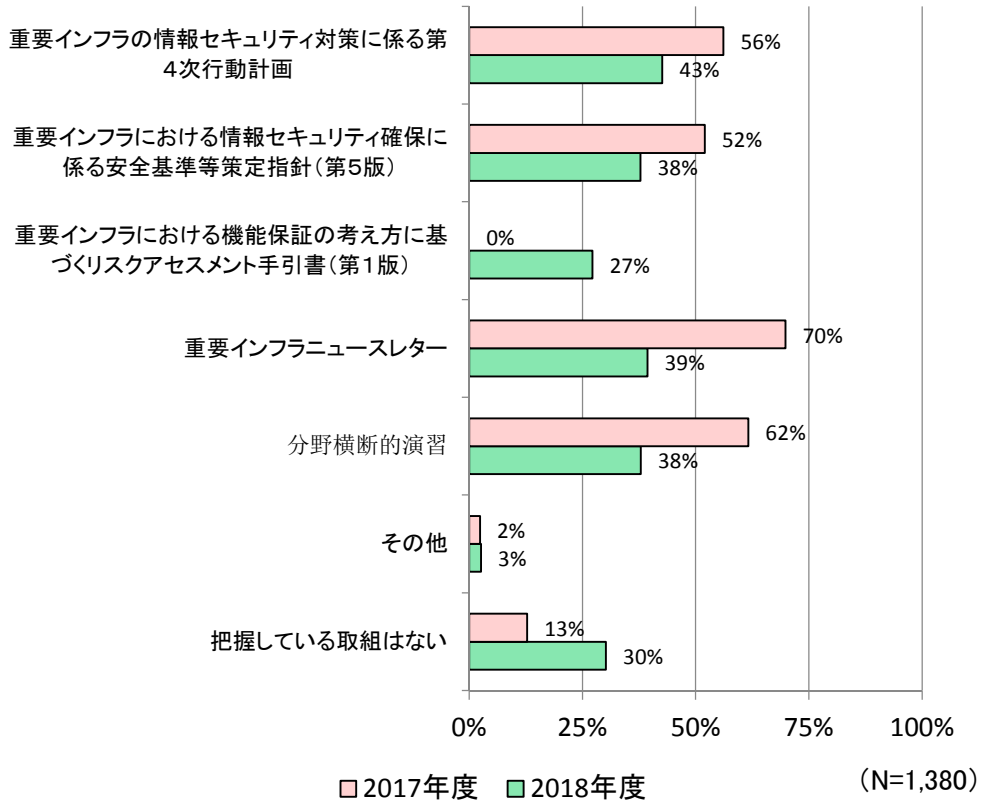
	①		②		③		④		⑤		⑥		⑦		⑧		⑨		⑩		⑪		⑫		⑬		⑭		⑮		⑯		⑰		⑱		⑲	
	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●
2017年度	67.3%	92.7%	62.4%	96.0%	47.5%	79.0%	18.2%	61.3%	37.4%	79.0%	65.3%	89.6%	34.9%	27.2%	48.8%	76.0%	34.3%	73.4%	99.8%	100.0%	91.7%	99.2%	34.5%	66.1%	88.1%	96.0%	37.6%	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	84.7%	97.8%	73.2%	93.9%	40.3%	76.4%	15.2%	47.0%	39.9%	62.0%	83.1%	93.6%	26.1%	38.0%	60.3%	82.4%	28.8%	53.0%	100.0%	99.4%	95.1%	98.1%	26.9%	48.6%	90.9%	96.5%	24.6%	42.8%	85.2%	95.2%	44.0%	80.2%	53.5%	87.2%	22.3%	52.4%	38.3%	59.1%
2019年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2020年度	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

3.4. アンケート調査結果詳細 －（1/58）－

設問1　NISCの取組の認知状況

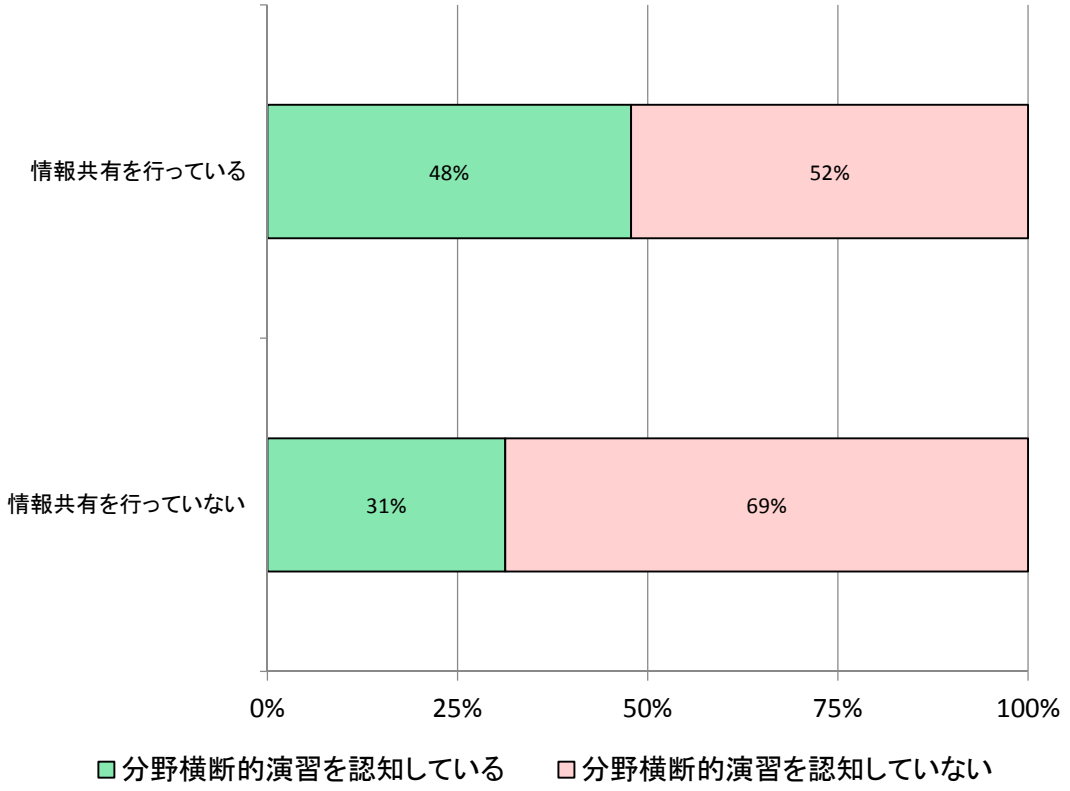
・行動計画や指針、リスクアセスメント手引書を認知している事業者等は、セキュリティ対策が進んでいる傾向がある。分野横断的演習を認知している事業者等は、情報共有を行っている傾向がある（参考①）。

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）

参考①　分野横断的演習の認知状況と情報共有の実施状況の関係性

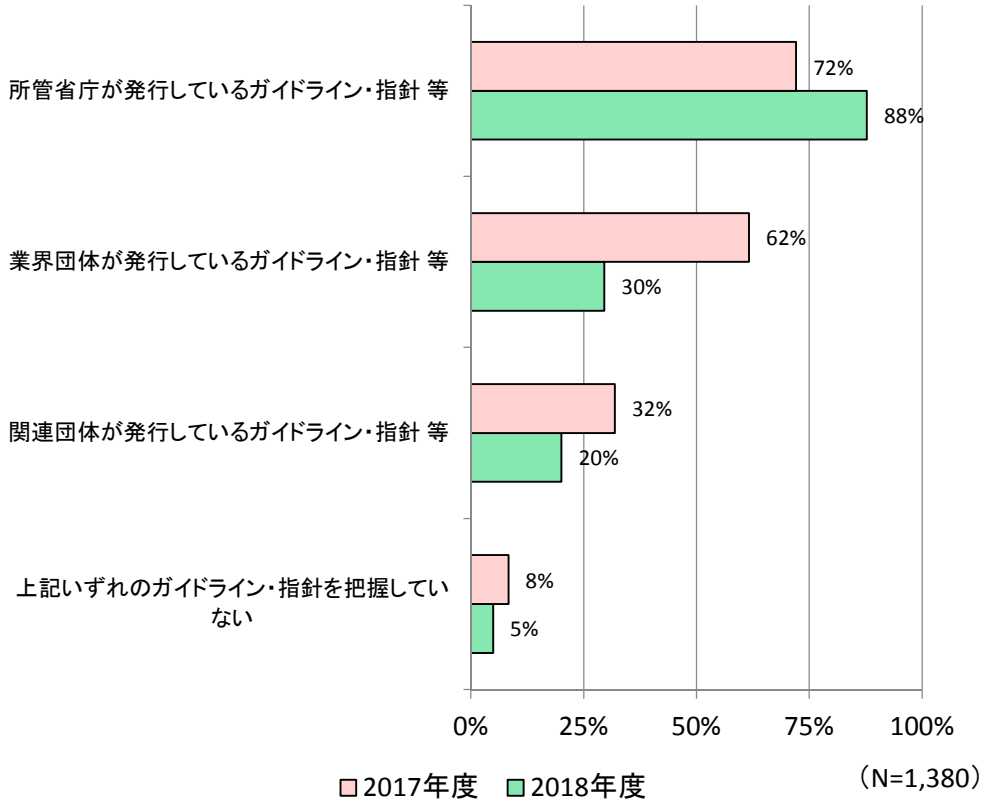


3.4. アンケート調査結果詳細 －（2/58）－

設問2　自分野の安全基準等の認知状況

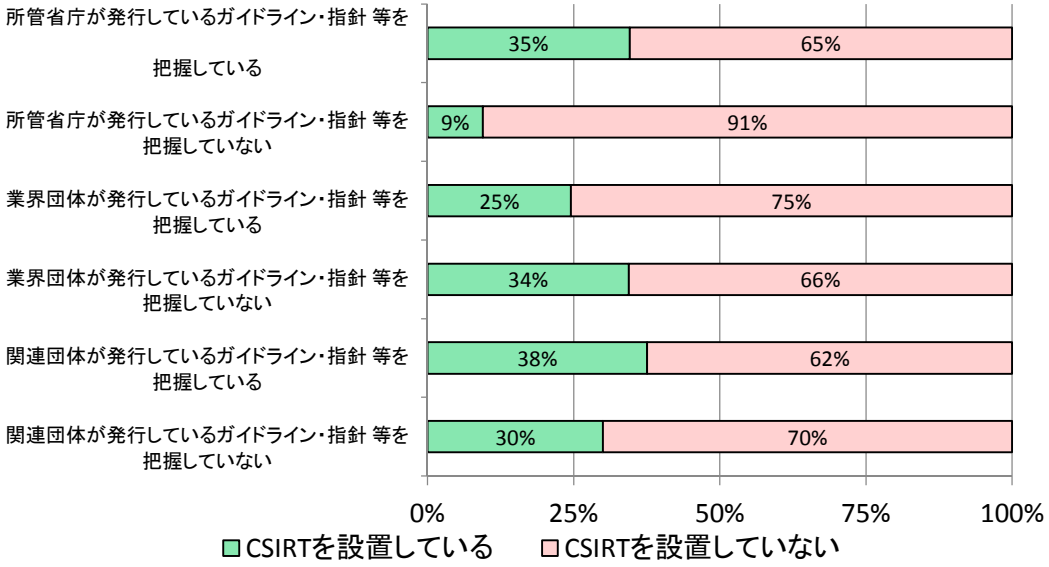
・CSIRTを設置している事業者は所管省庁が発行しているガイドライン・指針等を認知している傾向がある（参考①）。また、基本方針、計画、内規等の作成、外部演習への参加も同じ傾向がある。
・業界団体や関連団体が発行しているガイドラインや指針を確認している事業者等は、事業継続計画（BCP）やコンティンジェンシープラン（CP）を策定している傾向がある（参考②）。

自分野の安全基準等の認知状況（複数回答）

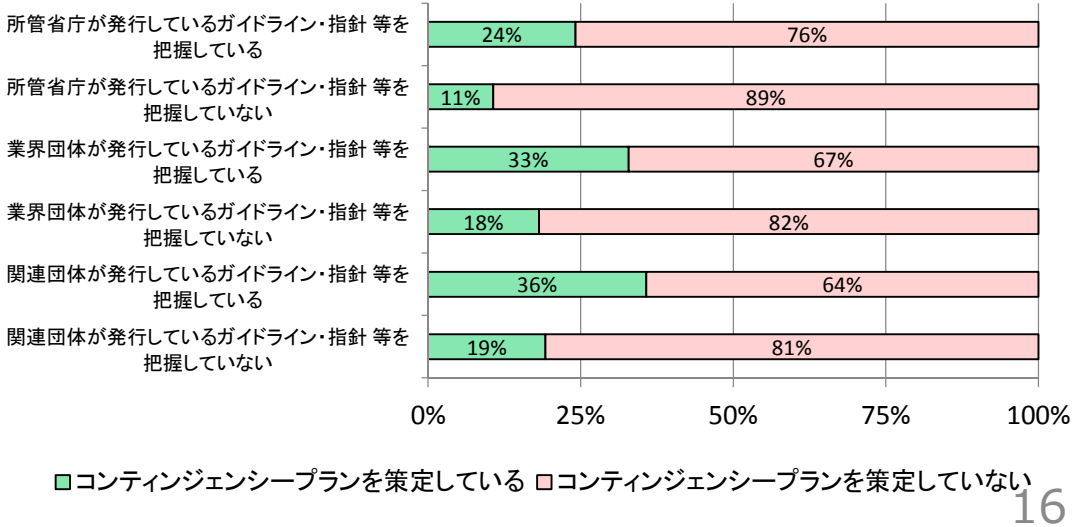


※金融は読替え可能項目なし（集計していません）

参考①　自分野の安全基準等の認知状況とCSIRTの設置状況の関係性



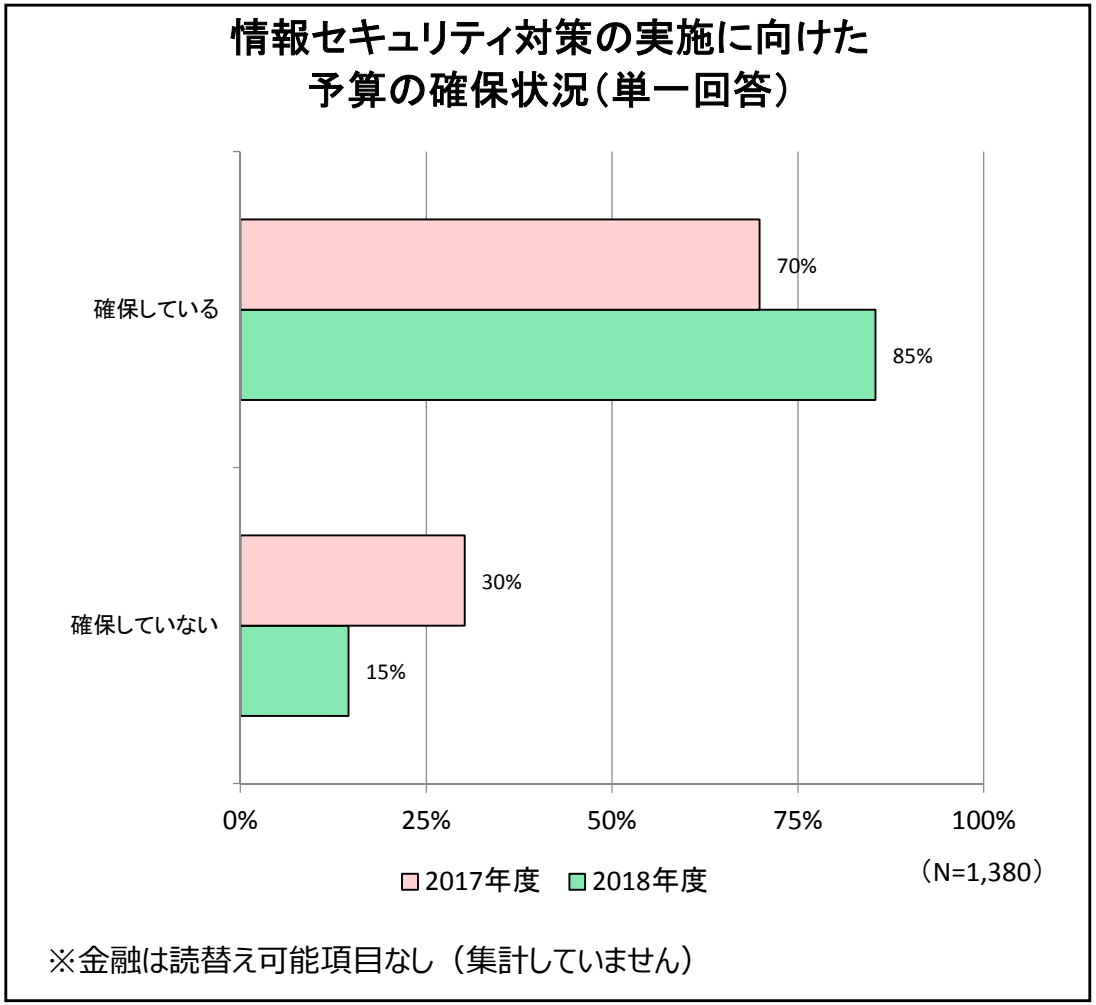
参考②　自分野の安全基準等の認知状況とコンティンジェンシープラン（CP）策定状況の関係性



3.4. アンケート調査結果詳細 －（3/58）－

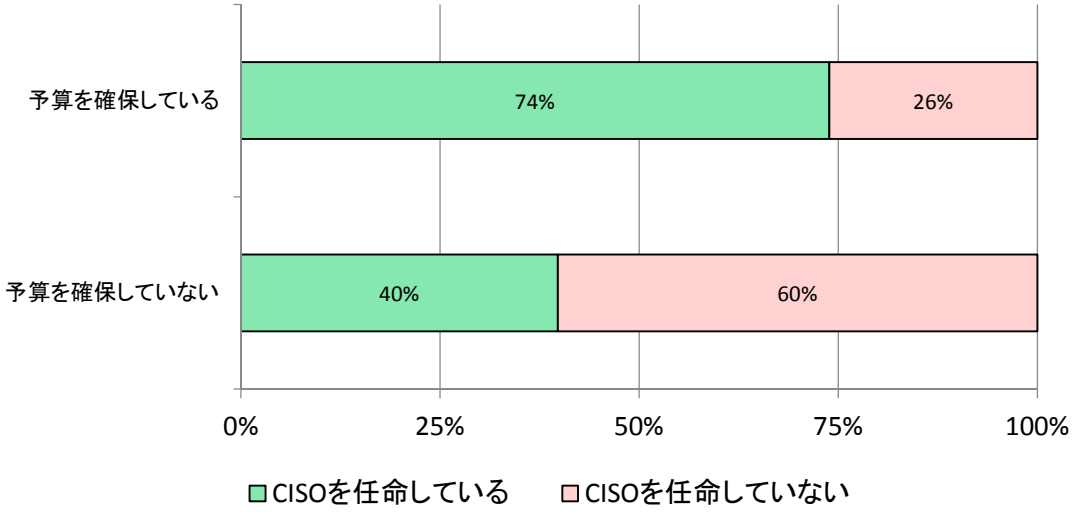
設問3 情報セキュリティ対策の実施に向けた予算の確保状況

・情報セキュリティ対策の実施を取り組む上で十分な予算が確保されている事業者等は、CISOを任命している割合が高く、経営層の働きかけにより、確保されていると考えられる（参考①）。
・予算の確保ができている事業者等は、情報セキュリティ対策に関する計画等が実施されている事業者等が多い傾向がある（参考②）。

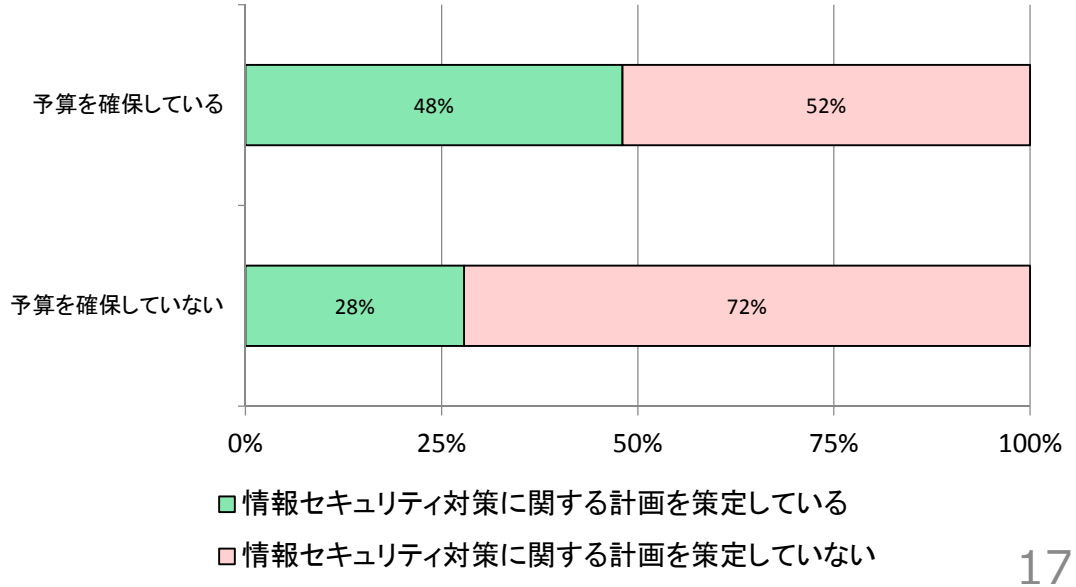


※金融は読替え可能項目なし（集計していません）

参考① 予算の確保状況とCISOの任命状況の関係性



参考② 予算の確保状況と情報セキュリティ対策に関する計画状況の関係性

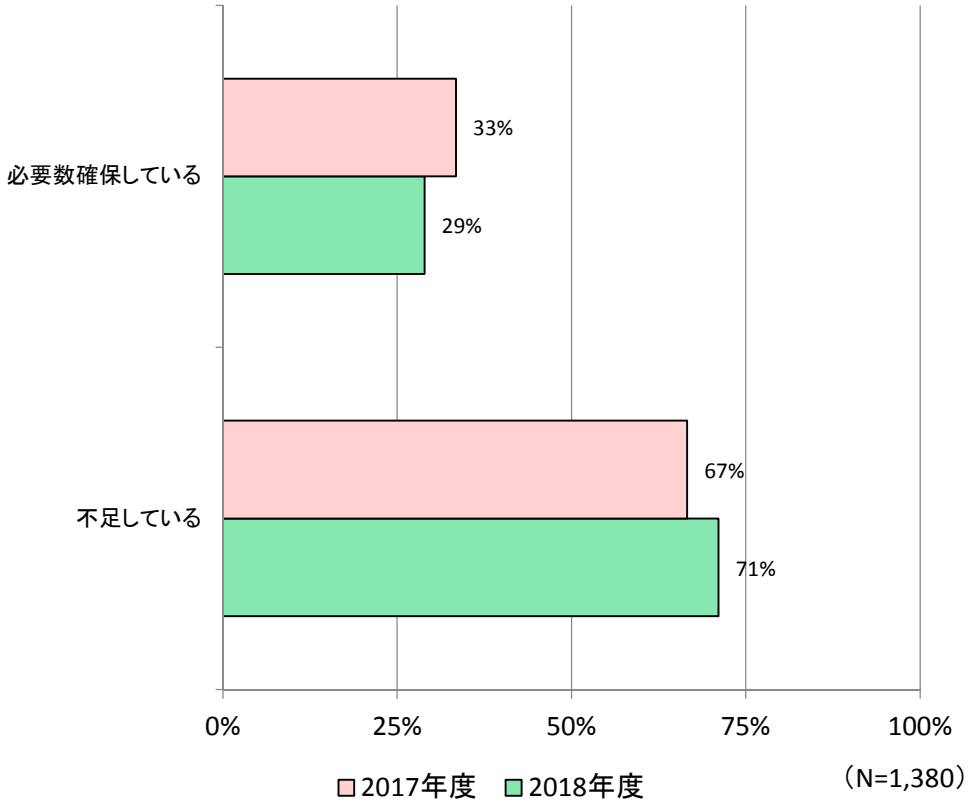


3.4. アンケート調査結果詳細 －（4/58）－

設問4　セキュリティ人材の確保状況

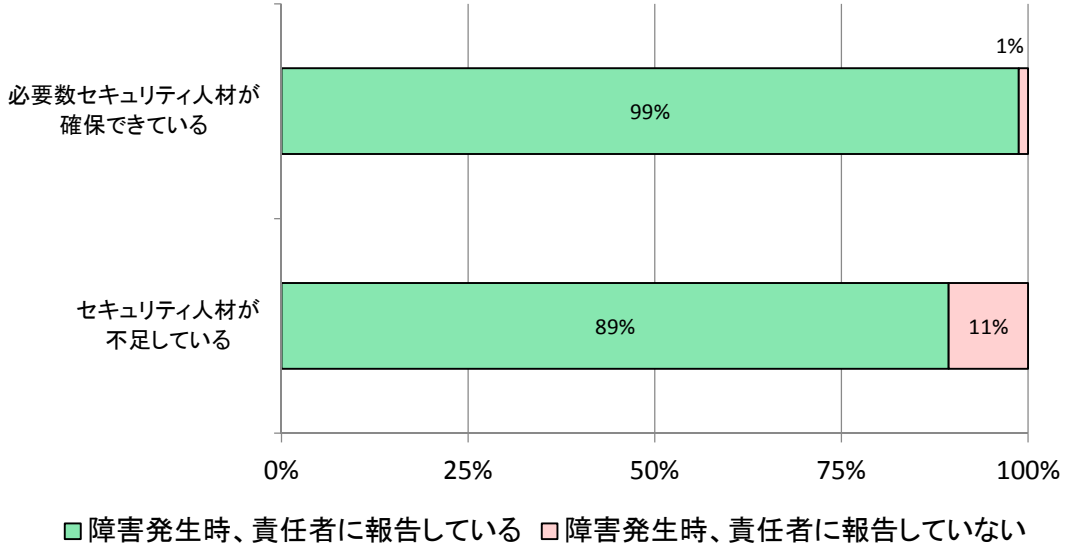
・セキュリティ人材が必要数確保できている事業者等は、障害発生時に経営層に報告し、情報セキュリティを経営リスクの一つとしてとらえていると考えられる（参考①）。
・セキュリティ人材が必要数確保できている事業者等は、社員に対する情報セキュリティの研修に力を入れる傾向が見られ、セキュリティ対策体制の構築が進められていると考えられる（参考②）。

セキュリティ人材の確保状況（単一回答）

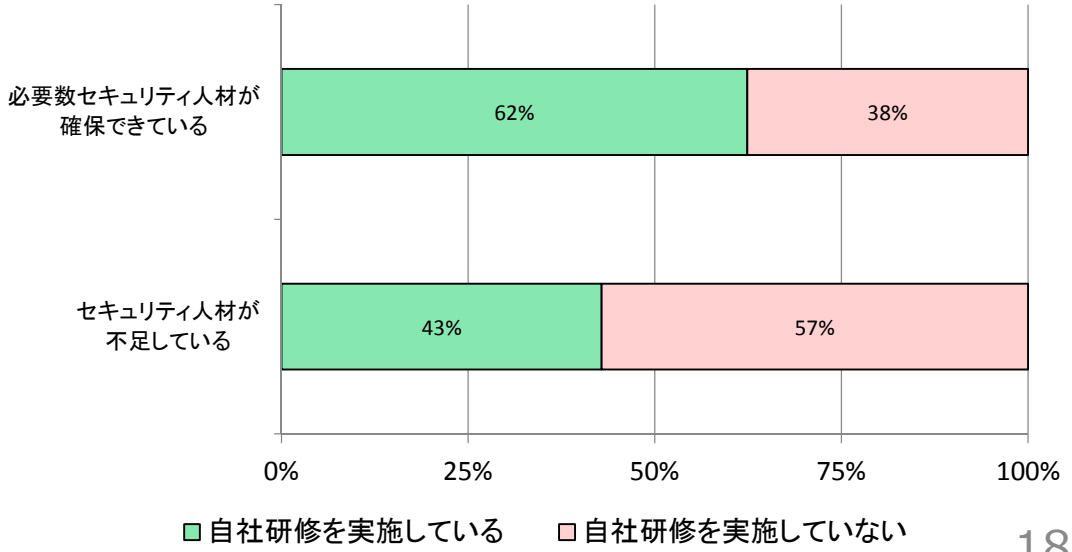


※金融は読替え可能項目なし（集計していません）

参考①　セキュリティ人材の確保状況と事業者等の責任者への報告状況の関係性



参考②　セキュリティ人材の確保状況と自社研修の実施状況の関係性

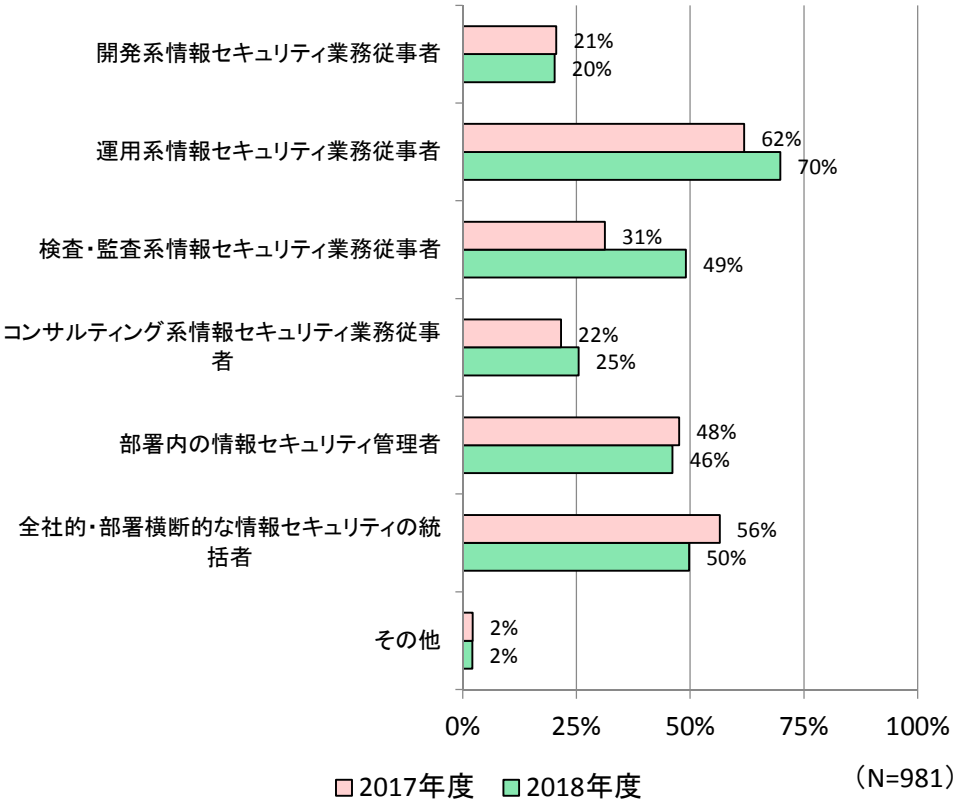


3.4. アンケート調査結果詳細 －（5/58）－

設問4-1　必要とする人材の職種

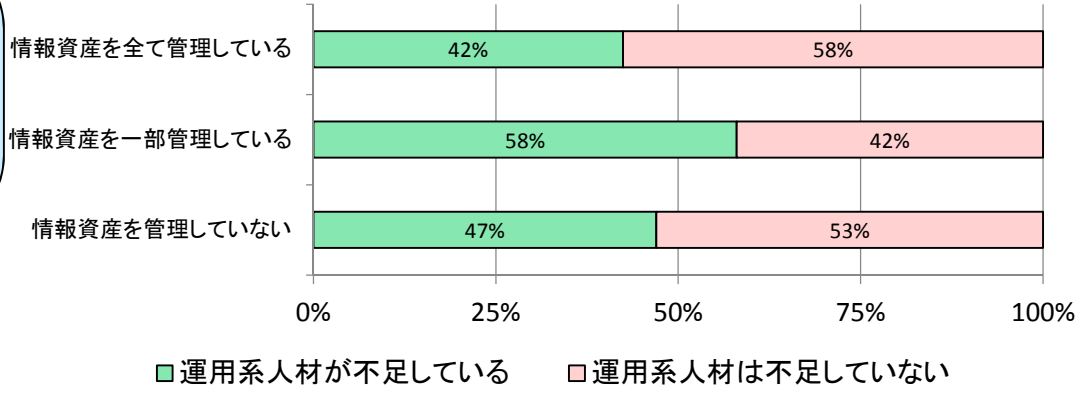
・運用系の人材が足りていない事業者等は、足りている事業者と比較して、情報資産の洗い出しを行い、台帳で管理している資産が一部にとどまっている傾向がある（参考①）。
・また、セキュリティ対策の統括者がいない事業者等は、情報資産の洗い出しができていないだけではなく、専門部署の設置や情報セキュリティ対策に関する計画、外部委託の規程ができていない傾向がある（参考②）。

必要とする人材の職種（複数回答）

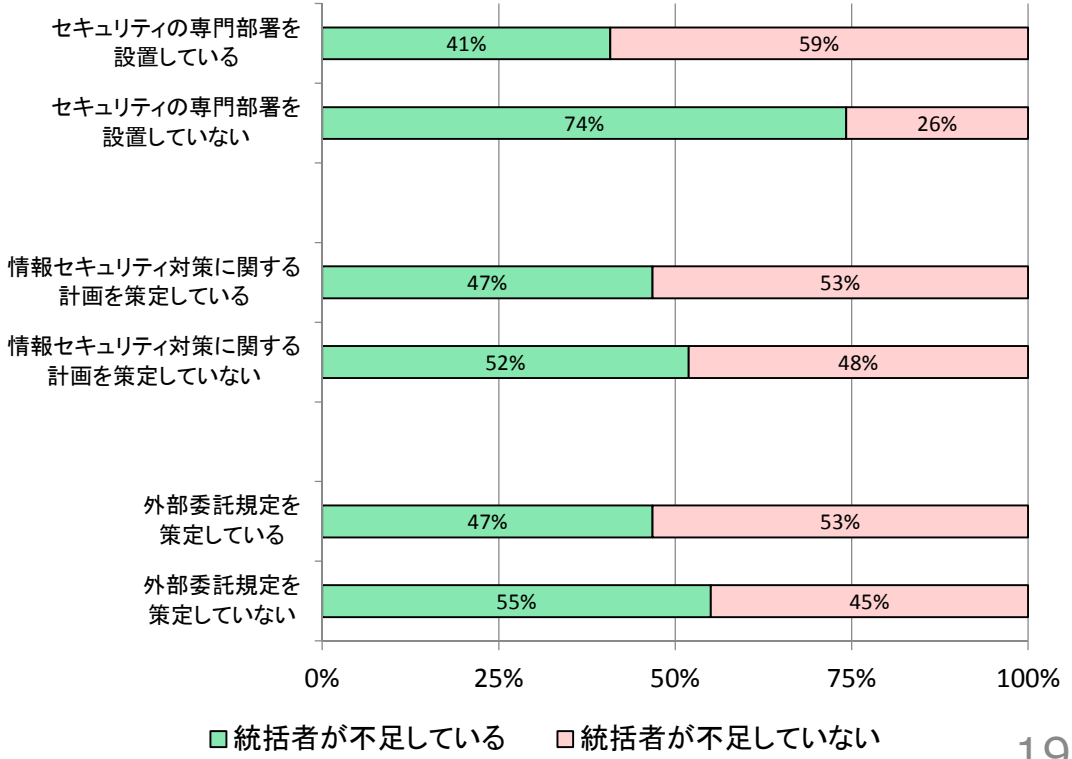


※金融は読替え可能項目なし（集計していません）

参考①　運用系人材の充足状況と情報資産管理状況の関係性



参考②　セキュリティ統括者の充足状況と各項目の関係性

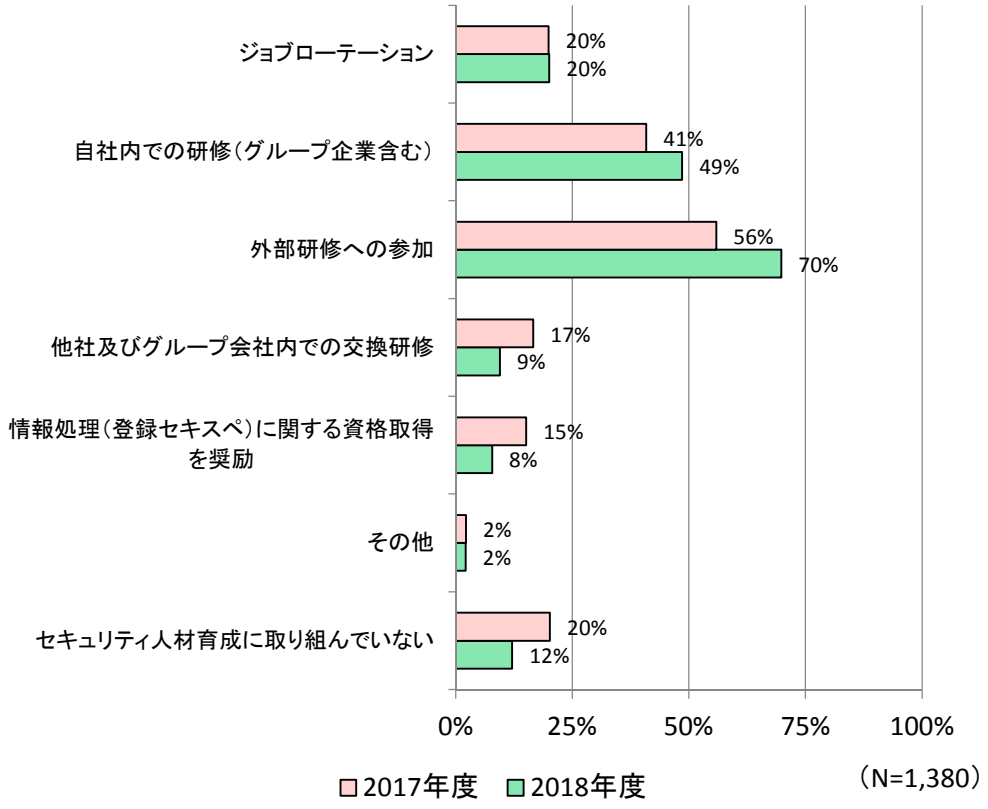


3.4. アンケート調査結果詳細 – （6/58） –

設問5　セキュリティ人材育成の取組状況

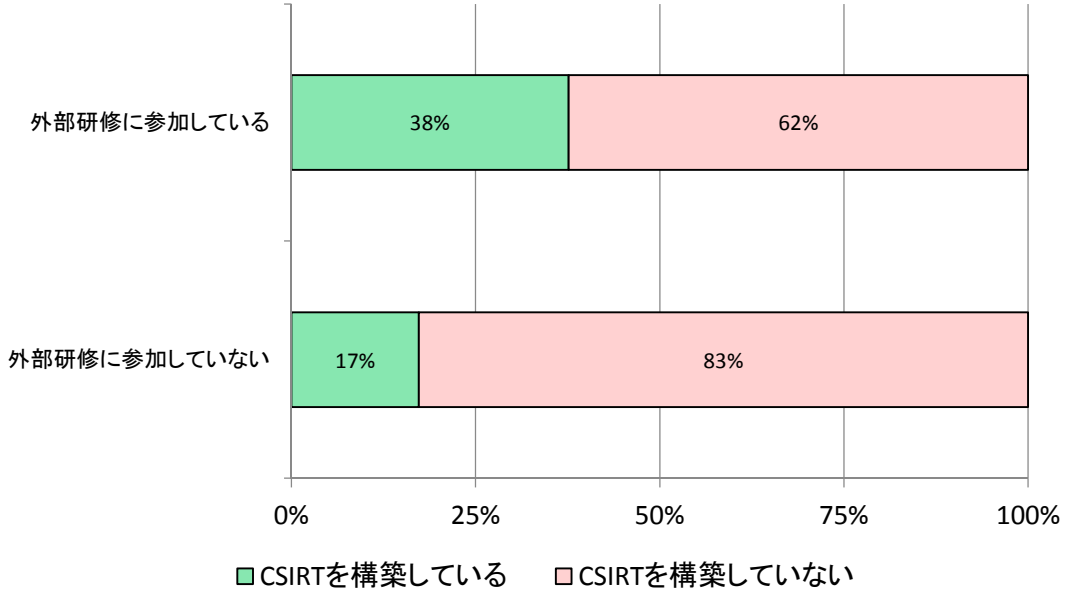
・セキュリティ人材育成のために外部研修に参加している事業者等は、社員のセキュリティ研修を実施している。また、外部研修に参加している事業者等はCSIRTの設置率が2倍を超えている（参考①）。
・セキュリティ人材を育成していない事業者等は、予算も確保されていない傾向がある（参考②）。

セキュリティ人材育成の取組状況（複数回答）

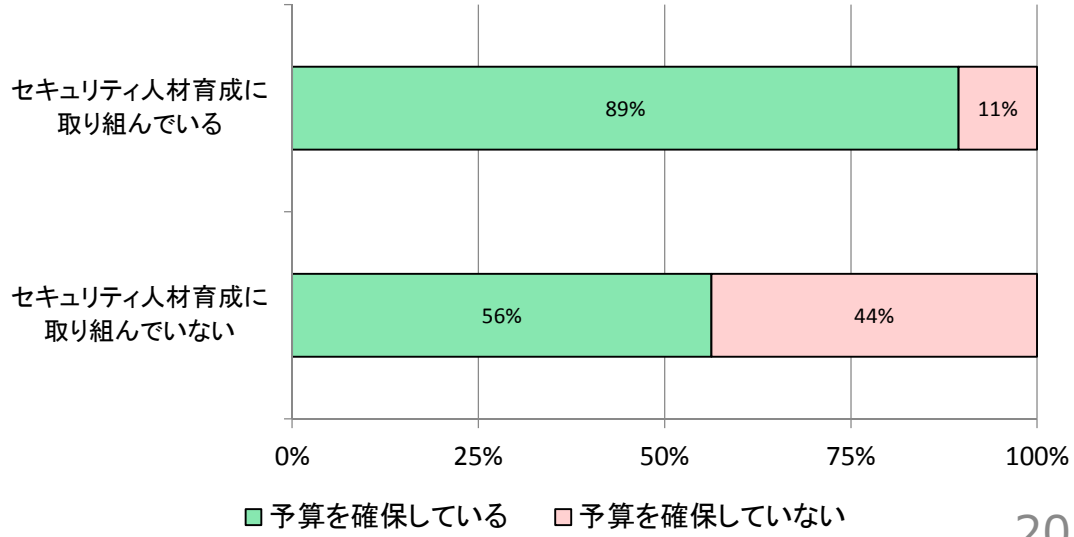


※金融は読替え可能項目なし（集計していません）

参考①　外部研修の参加状況とCSIRTの構築状況の関係性



参考②　セキュリティ人材の育成状況と予算の確保状況の関係性

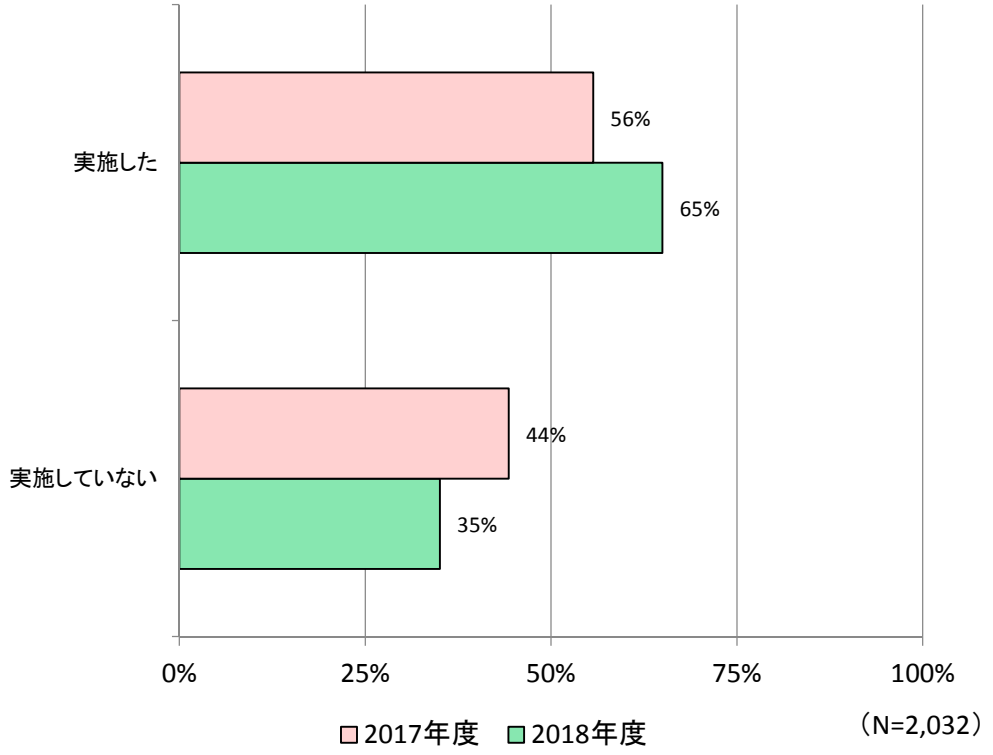


3.4. アンケート調査結果詳細 －（7/58）－

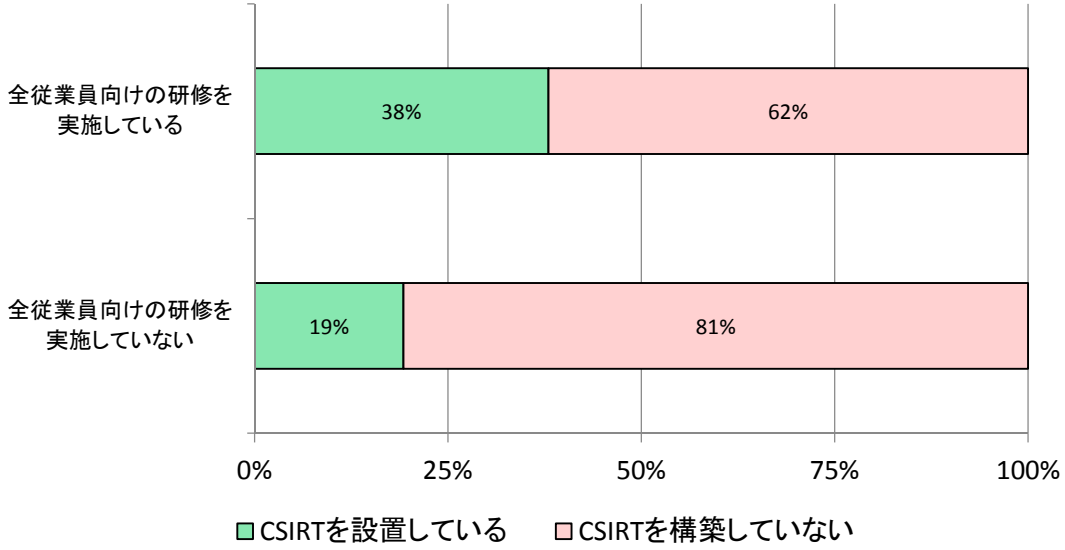
設問6　全従業員向けセキュリティ研修の実施状況

・全従業員向けのセキュリティ研修を実施している事業者等は、CSIRTの設置率が２倍である（参考①）。
・全従業員向けのセキュリティ研修を実施している事業者等は、情報セキュリティ基本方針を策定しており、セキュリティに関する規程類も策定している傾向がある（参考②）。

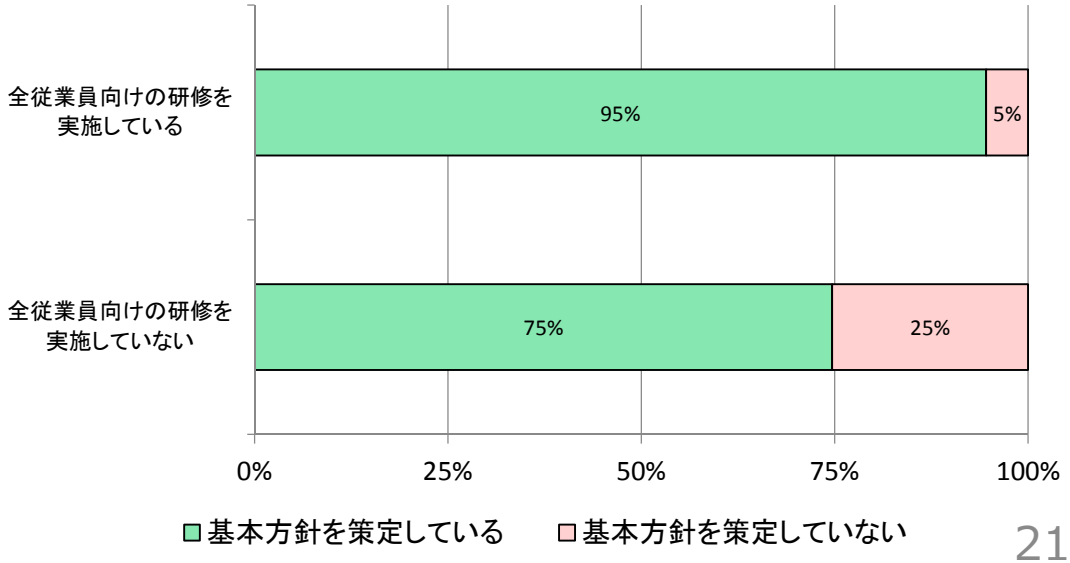
全従業員向けセキュリティ研修の実施状況（単一回答）



参考①　従業員向け研修の実施状況とCSIRTの設置状況の関係性



参考②　全従業員向け研修の実施状況と情報セキュリティ基本方針策定の関係性

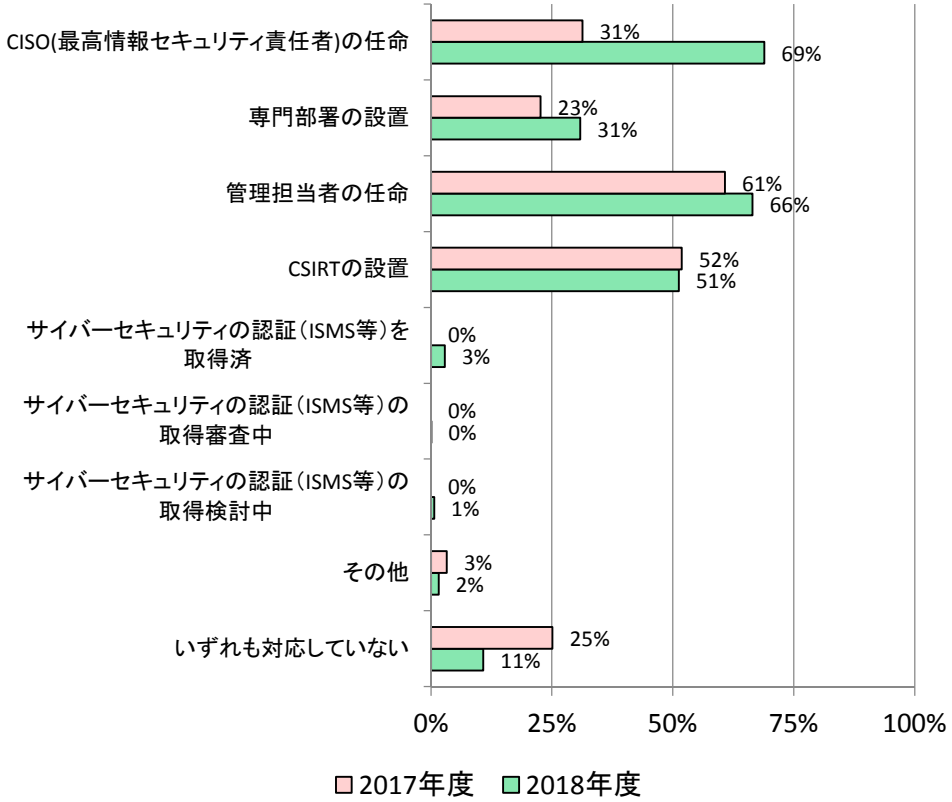


3.4. アンケート調査結果詳細 －（8/58）－

設問7　内部体制の取組状況

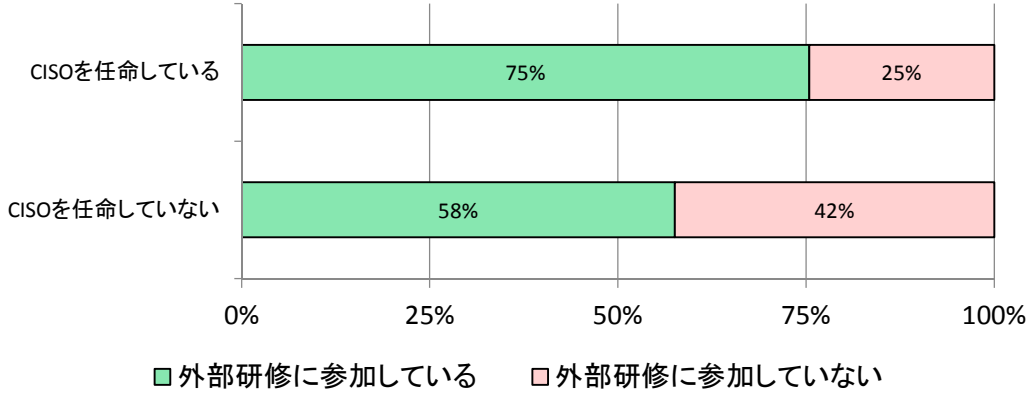
・CISOを任命している事業者等は、セキュリティ人材を育てるために、積極的に外部への研修に参加している。また、全従業員向けのセキュリティ研修を実施している（参考①）。
・CSIRTが設置されている事業者等は、分野横断的演習を認知している傾向がある（参考②）。
・ CISOを任命している事業者等は、 CSIRTが設置されている傾向がある（参考③）。

内部体制の取組状況（複数回答）

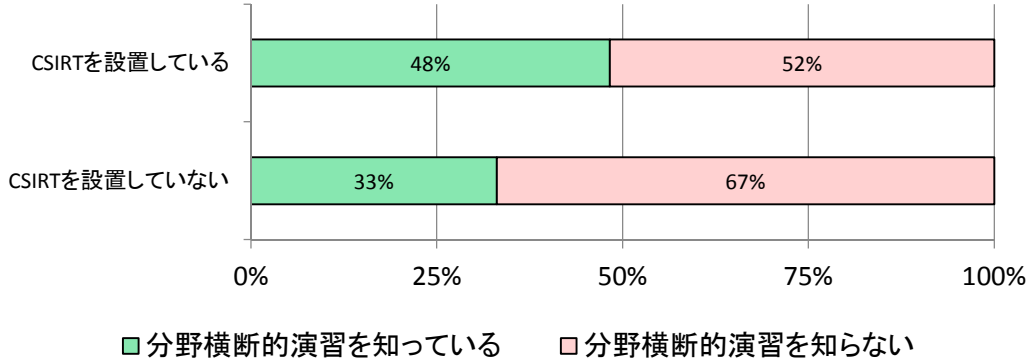


※一部選択肢において、金融は読替え可能項目なし（集計していません）

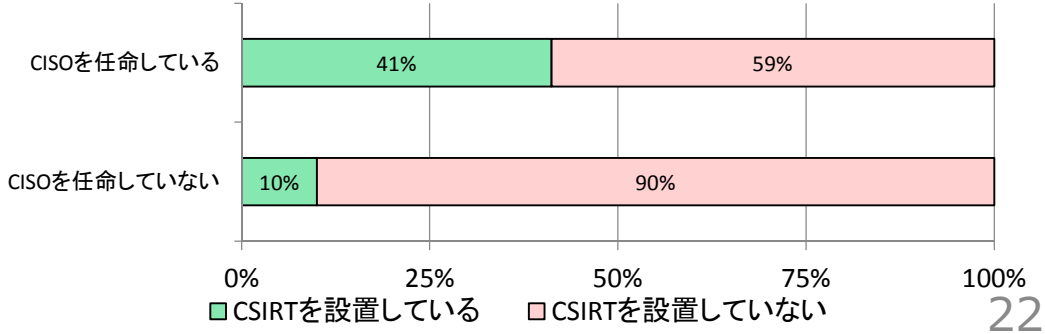
参考①　CISOの任命状況と外部研修の参加状況の関係性



参考②　CSIRTの設置状況と分野横断的演習の認知状況の関係性



参考③　CISOの任命状況とCSIRTの設置状況の関係性

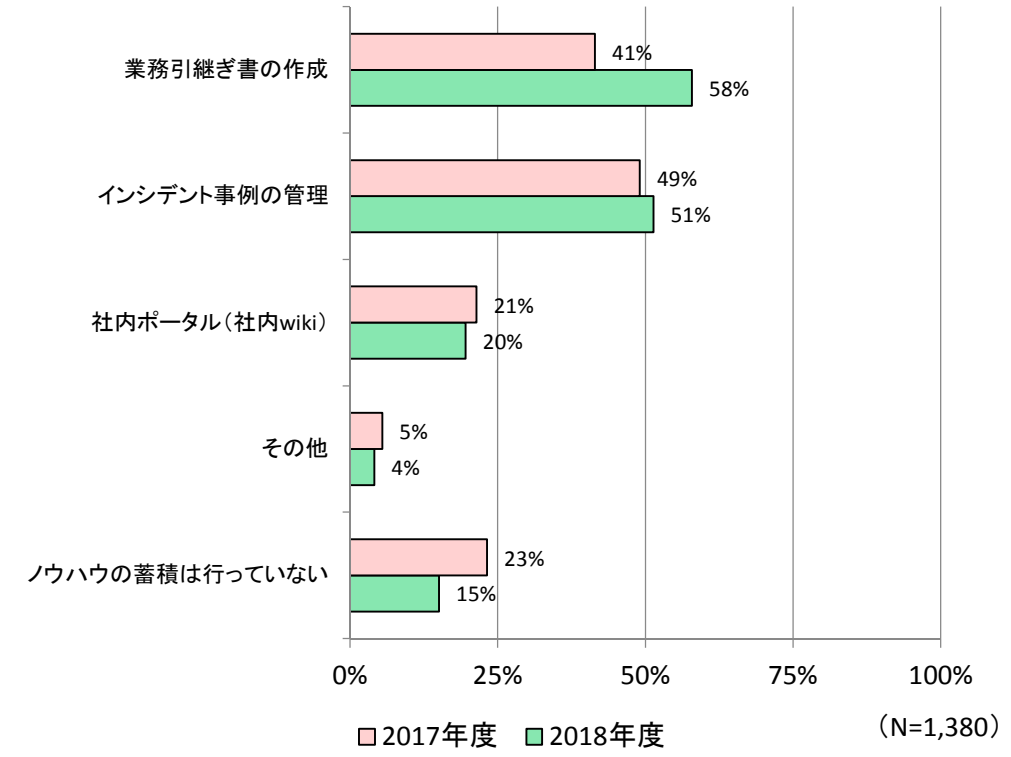


3.4. アンケート調査結果詳細 －（9/58）－

設問8　情報セキュリティ対策のノウハウの蓄積方法

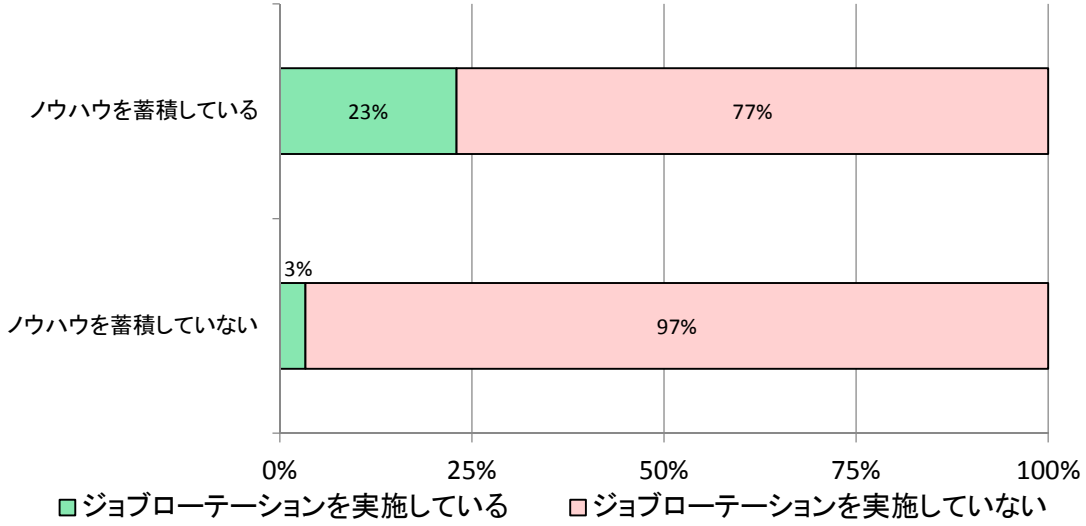
・人材育成の手法として、ジョブローテーションを実施している事業者等は、ノウハウの蓄積を行っている。セキュリティ人材の育成手法として、ジョブローテーションは有効であることが確認できる（参考①）。
・ノウハウの蓄積方法としては、予算が少ない事業者等も業務引継ぎ書の作成やインシデント事例の管理で実施している（参考②）。

情報セキュリティ対策のノウハウの蓄積方法（複数回答）

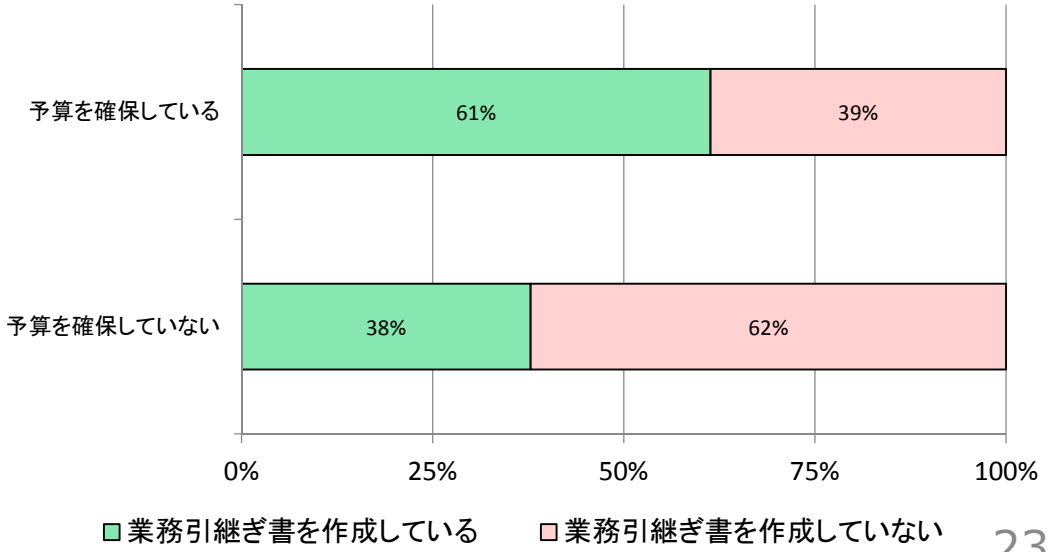


※金融は読替え可能項目なし（集計していません）

参考①　ノウハウの蓄積状況とジョブローテーションの実施状況の関係性



参考②　予算の確保状況とノウハウ蓄積方法の関係性

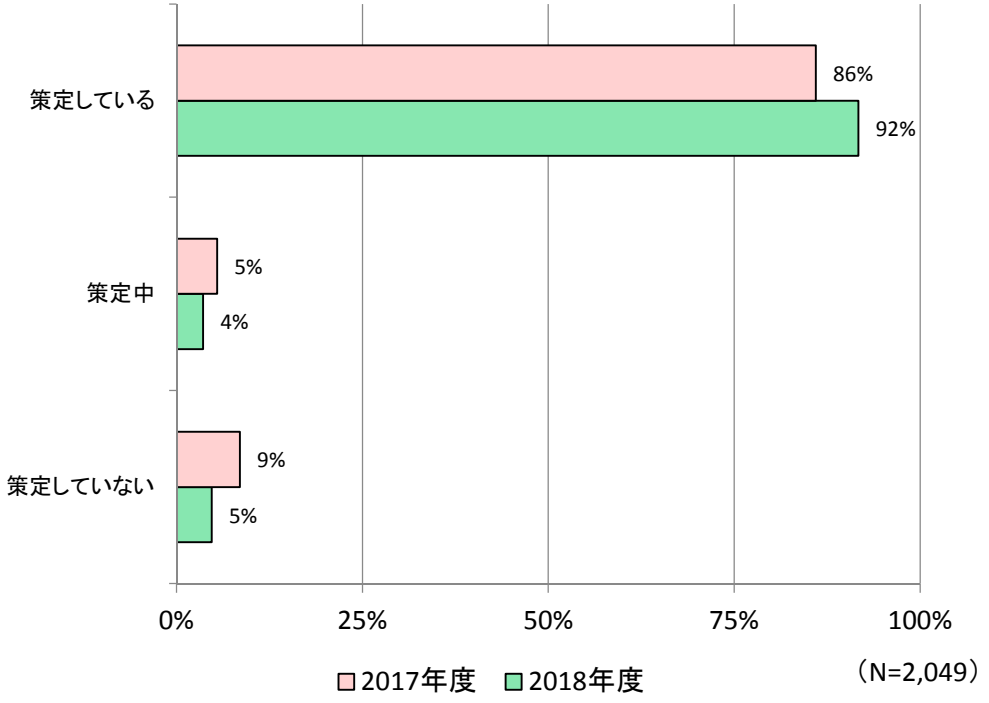


3.4. アンケート調査結果詳細 －（10/58）－

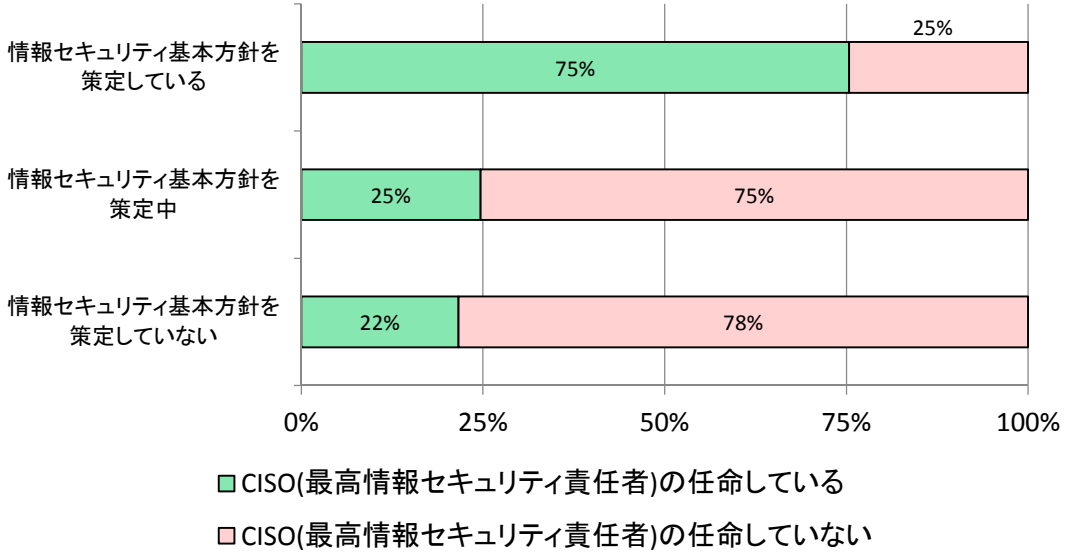
設問9　情報セキュリティ対策に関する基本方針の策定状況

・CISOが任命されている事業者等は、情報セキュリティ基本方針が策定されている（参考①）。
・情報セキュリティ基本方針が策定できていない事業者等は、内規等の策定も進んでいない傾向がある（参考②）。

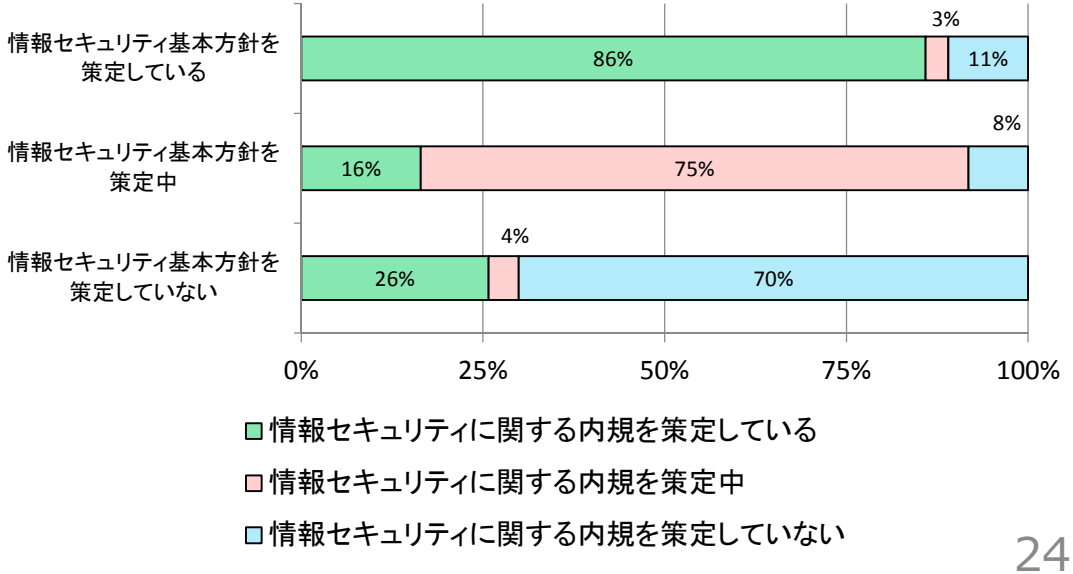
情報セキュリティ対策に関する
情報セキュリティ基本方針の策定状況
（単一回答）



参考①　情報セキュリティ基本方針策定状況と
CISOの任命状況の関係性



参考②　情報セキュリティ基本方針の策定状況と
内規の策定状況の関係性

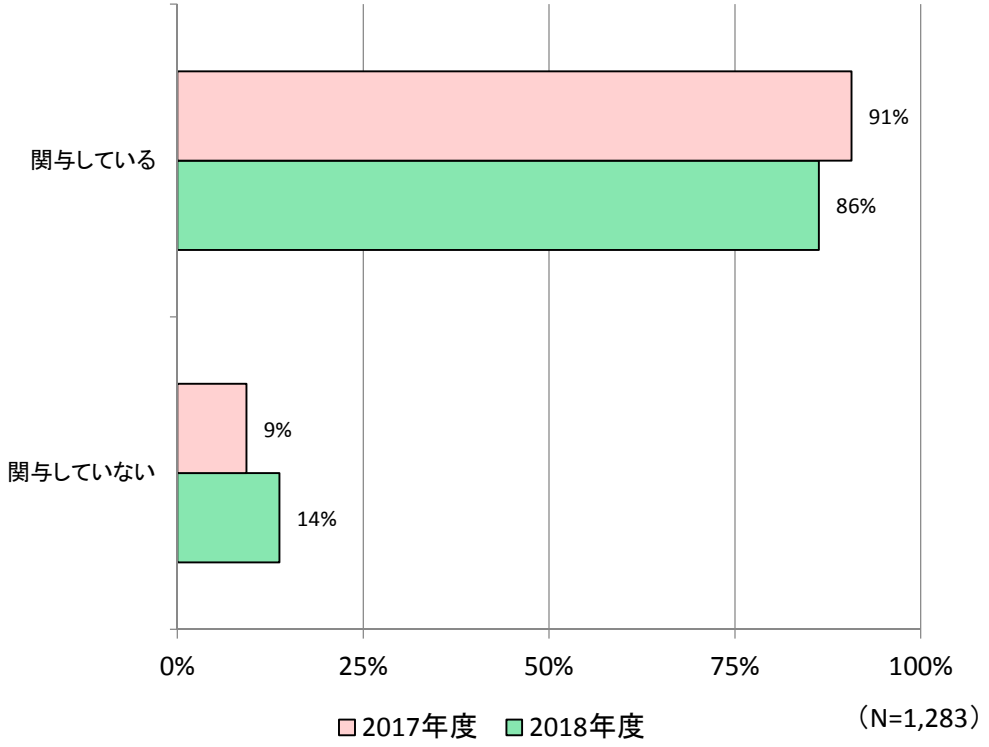


3.4. アンケート調査結果詳細 －（11/58）－

設問9-1　情報セキュリティ基本方針の策定に関する経営層の関与状況

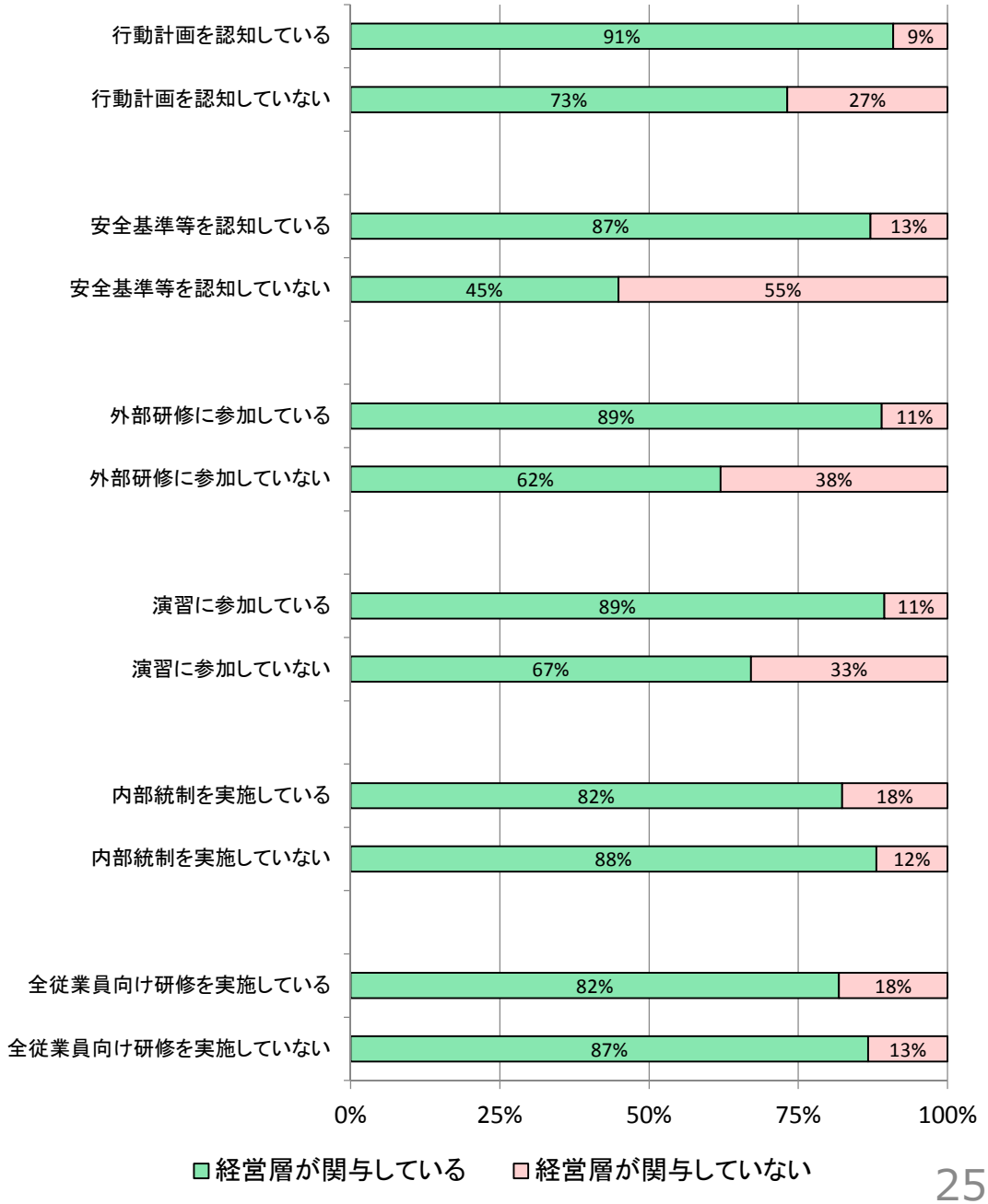
・行動計画やガイドライン等を認知し、外部への研修や演習等に参加しているような情報収集に積極的な事業者等は、経営層が関与している傾向がある（参考①）。

情報セキュリティ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）

参考①　経営層の関与状況と各項目との関係性

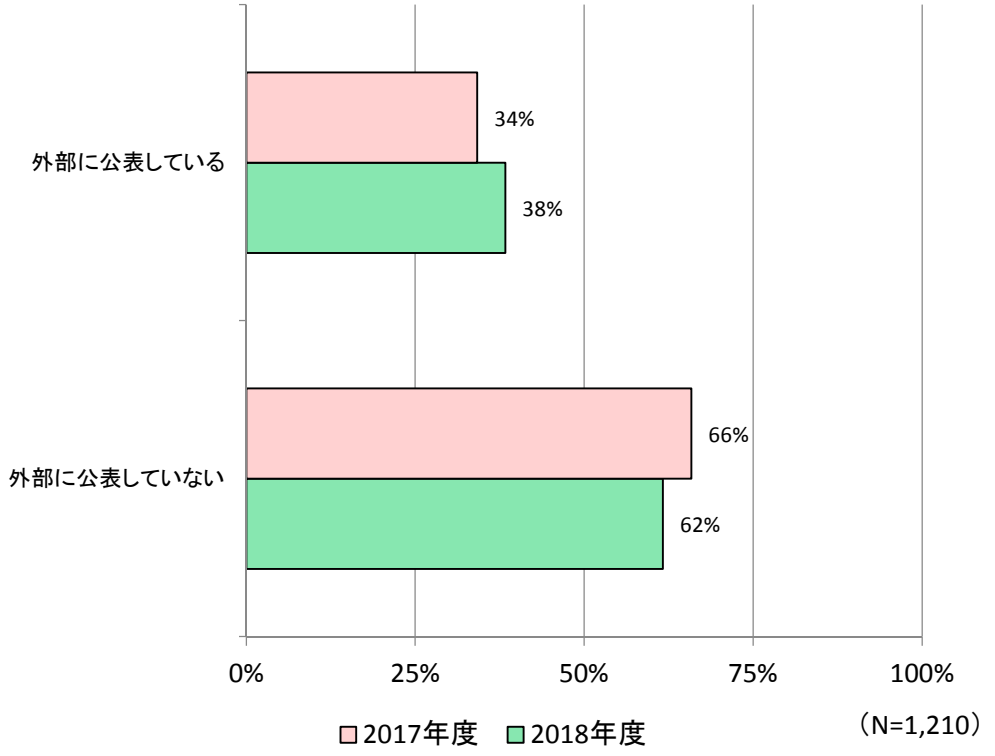


3.4. アンケート調査結果詳細 －（12/58）－

設問9-2 策定した情報セキュリティ基本方針の外部公表状況

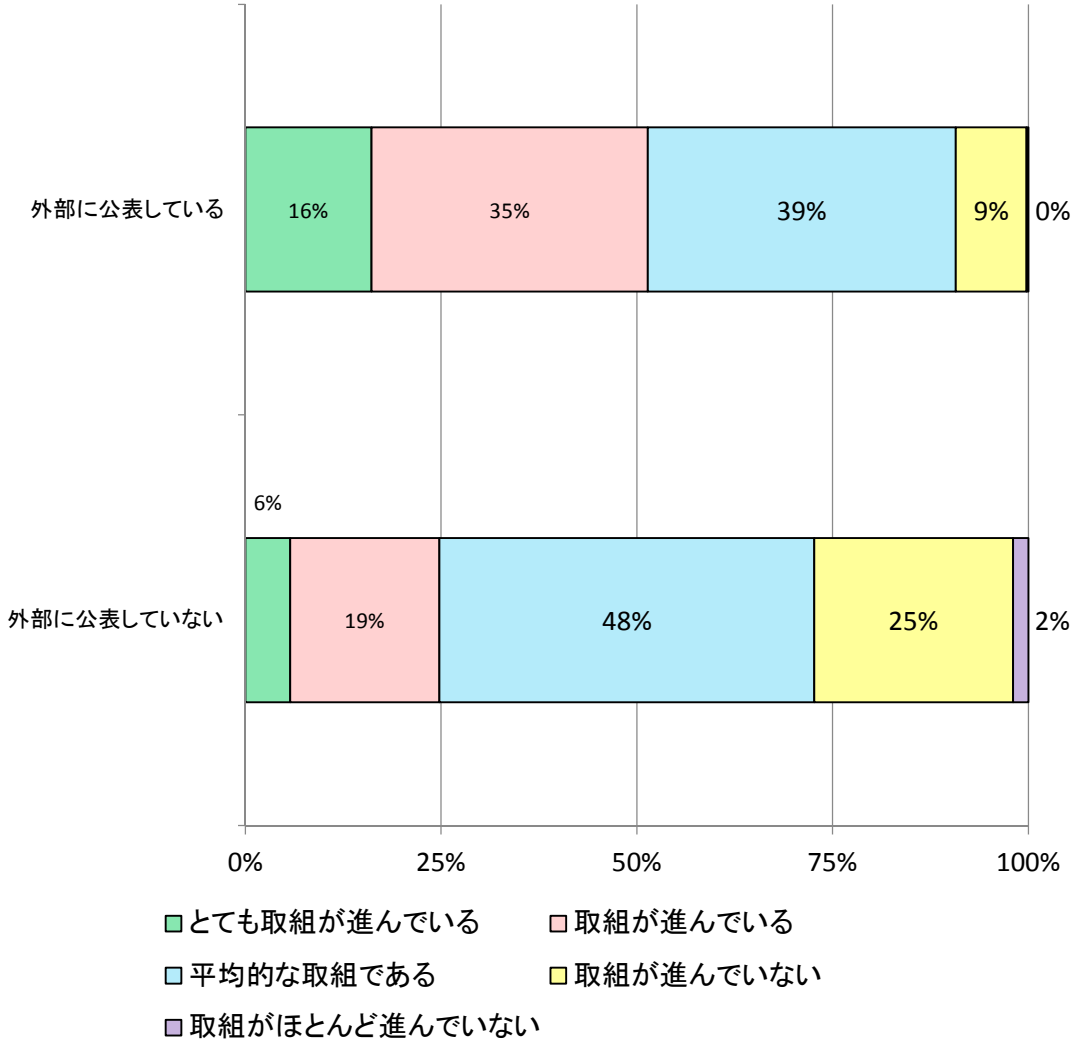
・情報セキュリティ基本方針を外部に公表している事業者等は、外部に公表していない事業者等に比べ、情報セキュリティの取り組みが進んでいる傾向が見られる。これは、外部への見せる安全や攻撃者への抑止効果を目指しているのではないかと感じる。また、外部に公表している事業者等は、情報セキュリティを経営リスクの一つととらえ、投資家からの評価も意識していると考えられる（参考①）。

策定した情報セキュリティ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）

参考① 情報セキュリティ基本方針の外部公表状況と情報セキュリティへの取組進捗状況の関係性

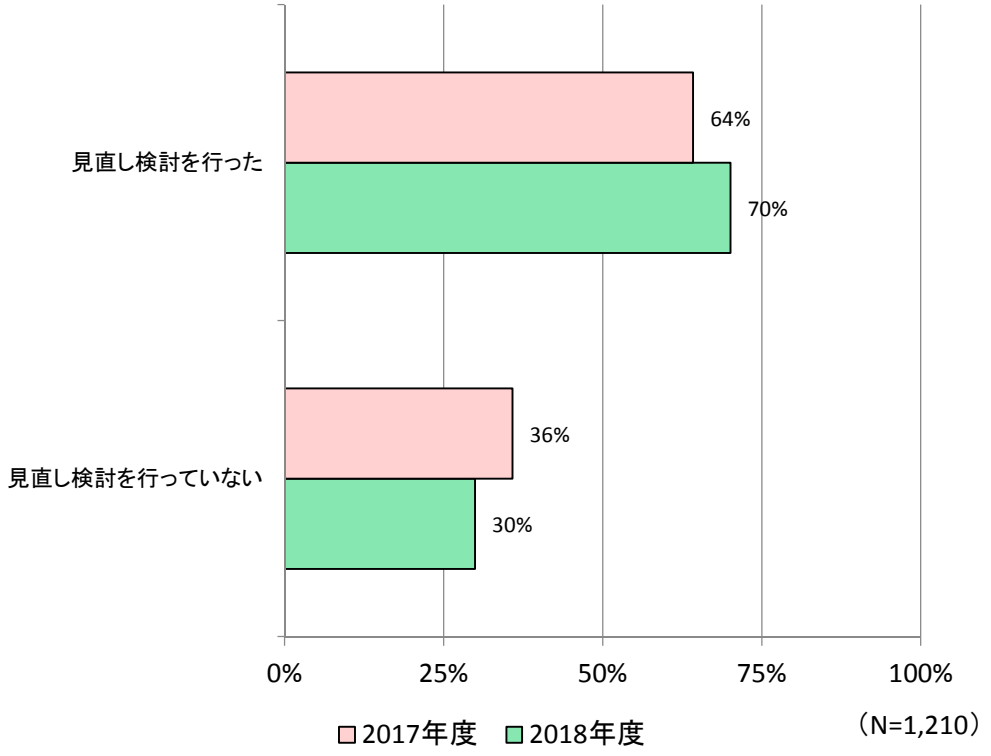


3.4. アンケート調査結果詳細 －（13/58）－

設問9-3 情報セキュリティ基本方針の見直し検討状況

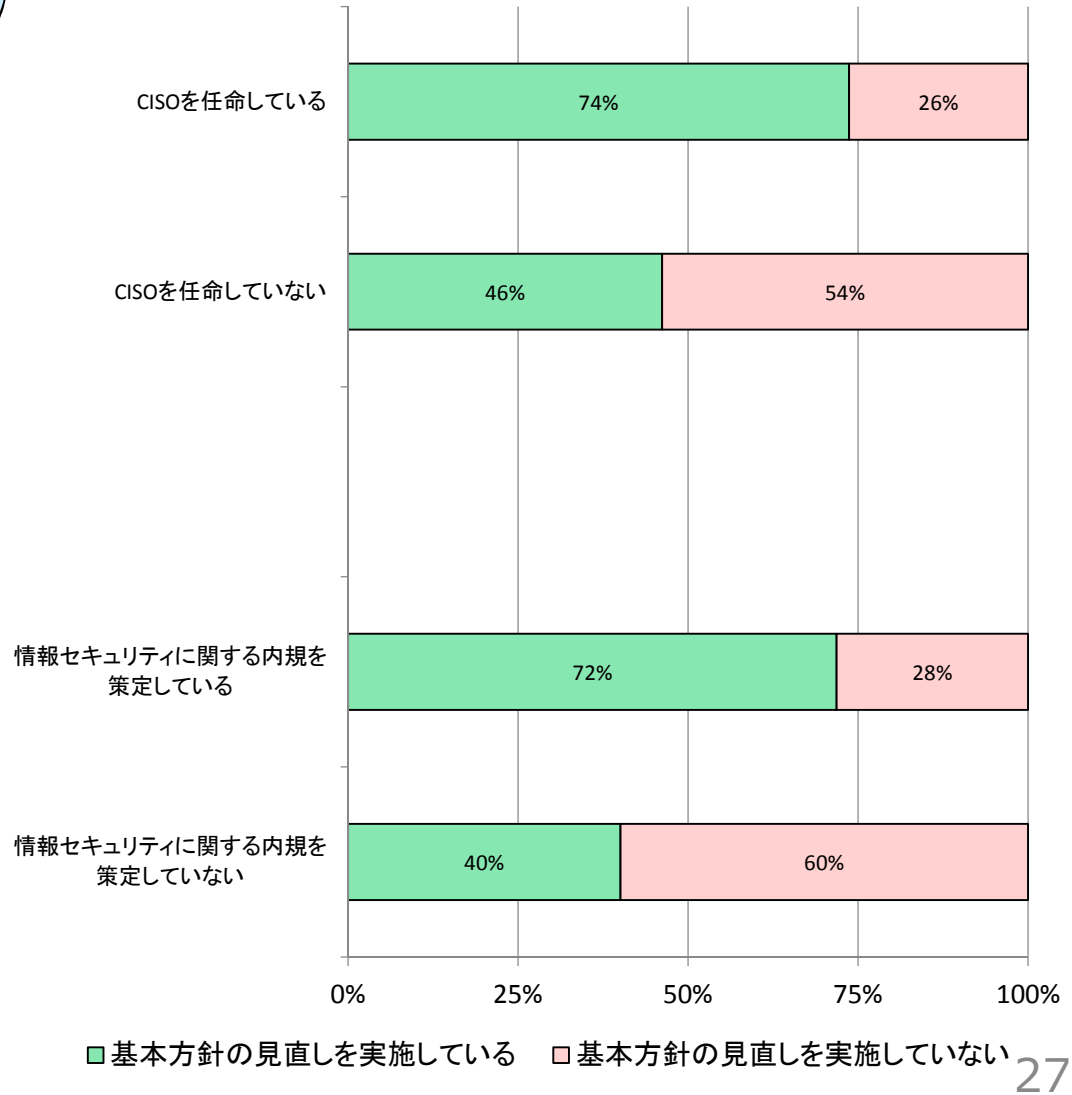
・CISOを任命している事業者等は、情報セキュリティ基本方針の見直し検討を行っている傾向がある。経営層が意識をもって実施している結果であると考えられる 。情報セキュリティ基本方針の見直し検討を行っている事業者等は、情報セキュリティに関する内規や外部委託の規程の策定が実施されている傾向もある。規程を策定することから意識改革ができると考えられる（参考①）。

情報セキュリティ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）

参考① 情報セキュリティ基本方針の見直し状況と各項目の関係性

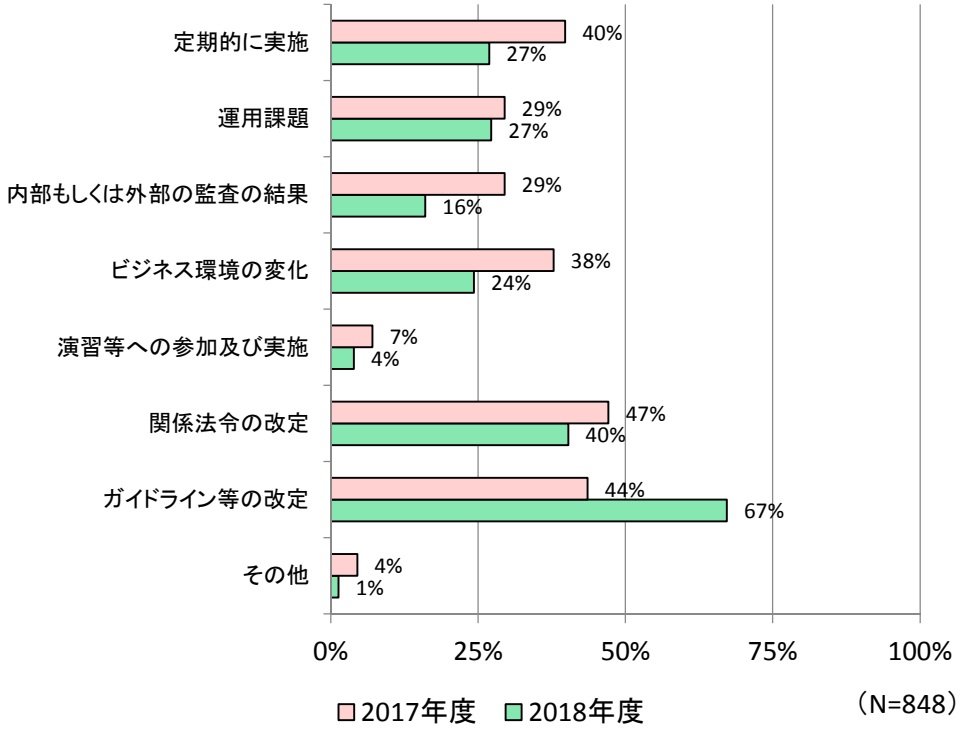


3.4. アンケート調査結果詳細 －（14/58）－

設問9-4 情報セキュリティ基本方針の見直し検討の契機

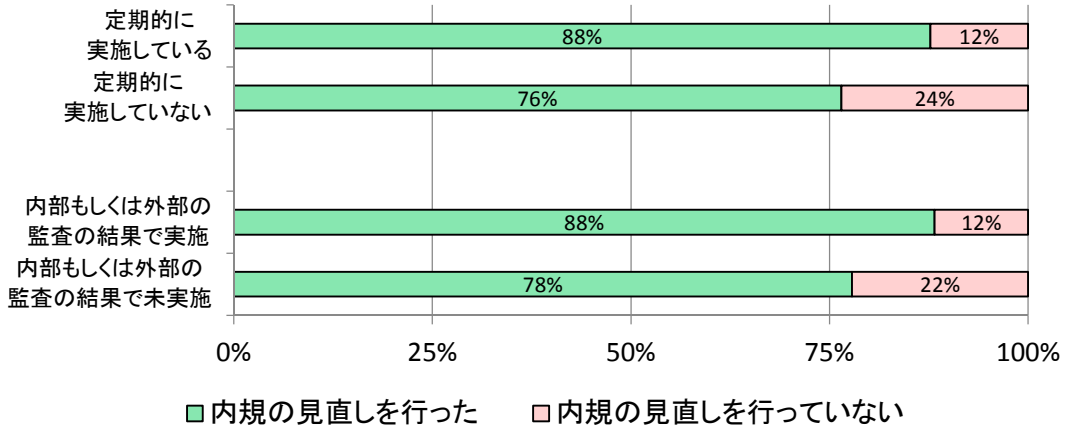
・情報セキュリティ基本方針を定期的もしくは監査の度に見直している事業者等は、基本方針だけではなく、内規の見直しも実施している傾向がある（参考①）。
・情報セキュリティ基本方針を運用課題として検討している事業者等は、インシデント事例の管理でノウハウの蓄積をしている傾向がある（参考②）。
・情報セキュリティ基本方針をビジネス環境の変化を契機にして見直している事業者等は、リスク対応要否に係る判断基準を定めている傾向がある（参考③）。

情報セキュリティ基本方針の見直し検討の契機（複数回答）

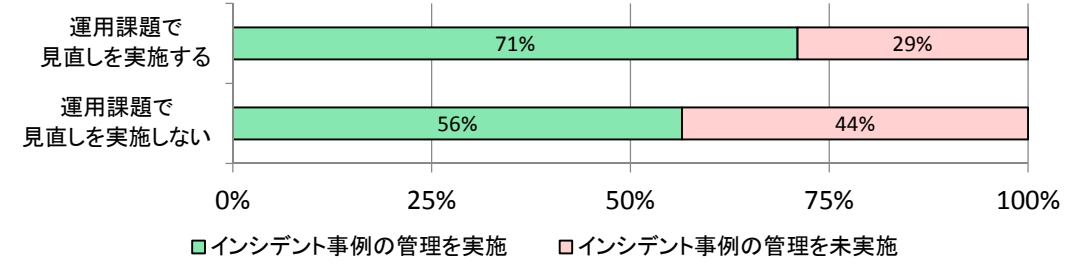


※金融は読替え可能項目なし（集計していません）

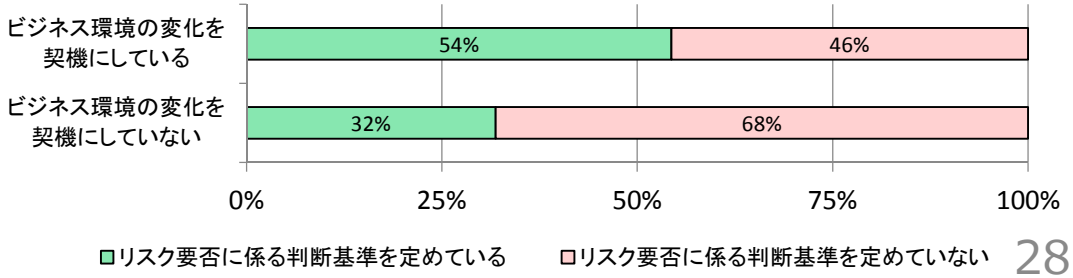
参考① 情報セキュリティ基本方針の見直し事由と内規の見直し状況の関係性



参考② 情報セキュリティ基本方針の見直し事由とインシデント事例管理状況の関係性



参考③ 情報セキュリティ基本方針の見直し事由とリスク要否の判断基準の決定状況の関係性

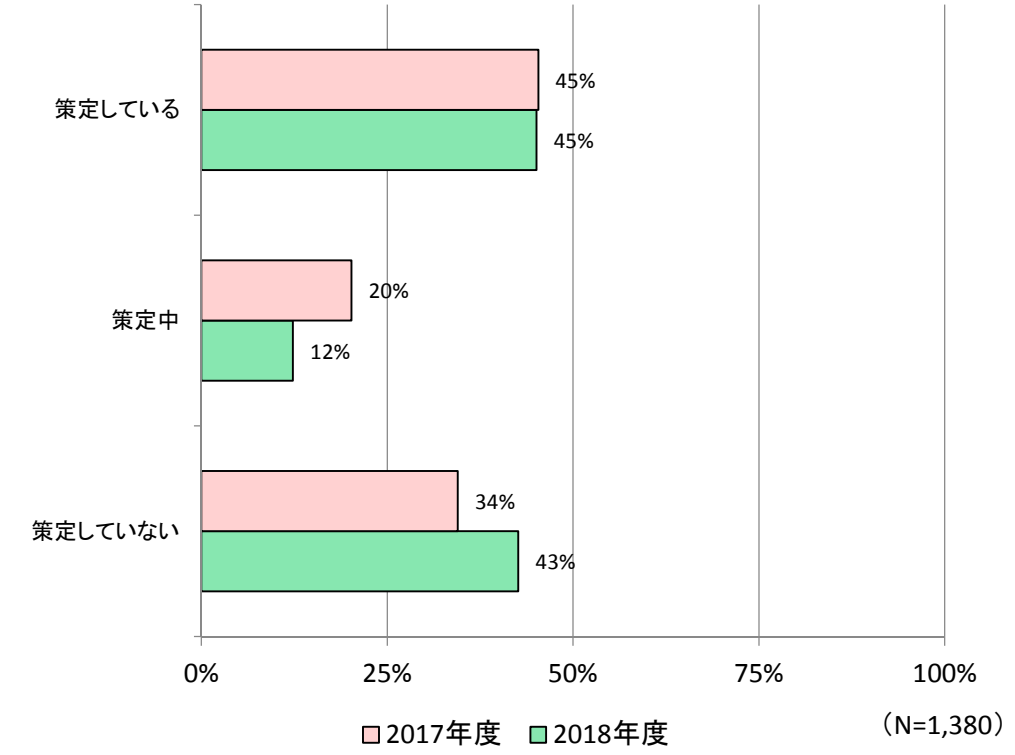


3.4. アンケート調査結果詳細 －（15/58）－

設問10　情報セキュリティ対策に関する計画策定状況

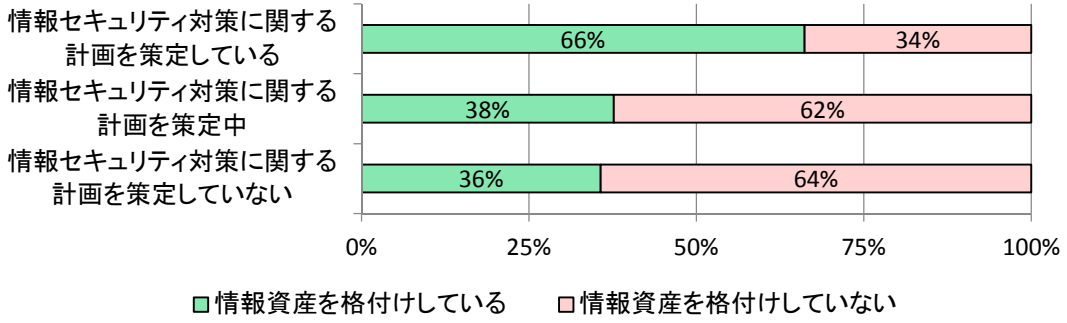
・情報セキュリティ対策に関する計画を策定している事業者等は、情報資産の格付けを実施しており、リスクの特定、対応要否の判断基準、対応優先順位づけ等を実施している傾向がある（参考①,②）。
・策定中になっている事業者等は、リスク対応に関しては未着手となっている傾向がある（参考②）。

情報セキュリティ対策に関する計画策定状況（単一回答）

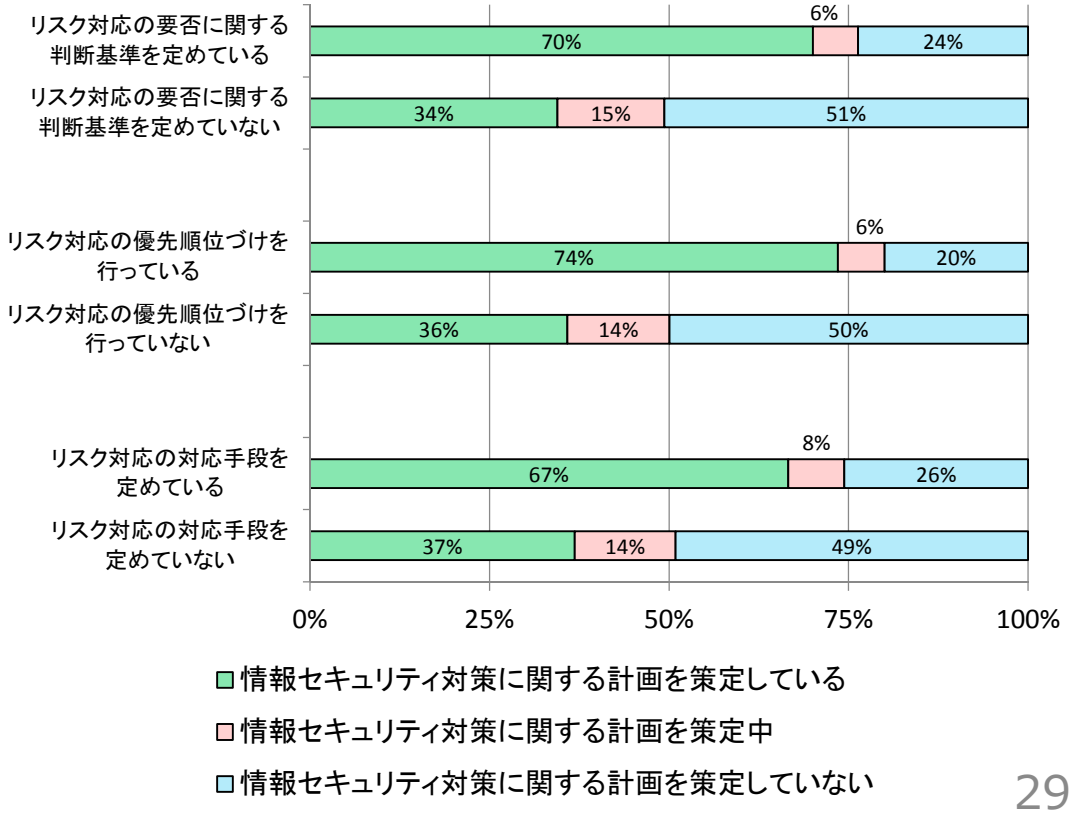


※金融は読替え可能項目なし（集計していません）

参考①　情報セキュリティ対策に関する計画策定状況と情報資産の格付け状況の関係性



参考②　情報セキュリティ対策に関する計画策定状況と各項目の関係性

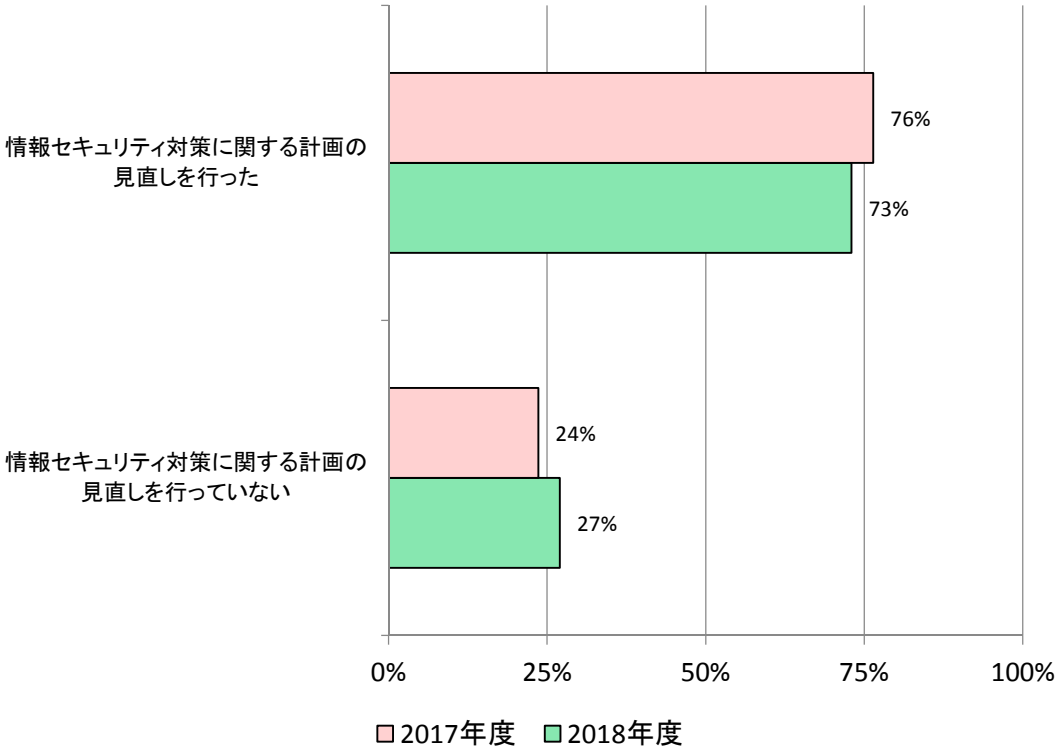


3.4. アンケート調査結果詳細 －（16/58）－

設問10-1 情報セキュリティ対策に関する計画の見直し（又は修正）状況

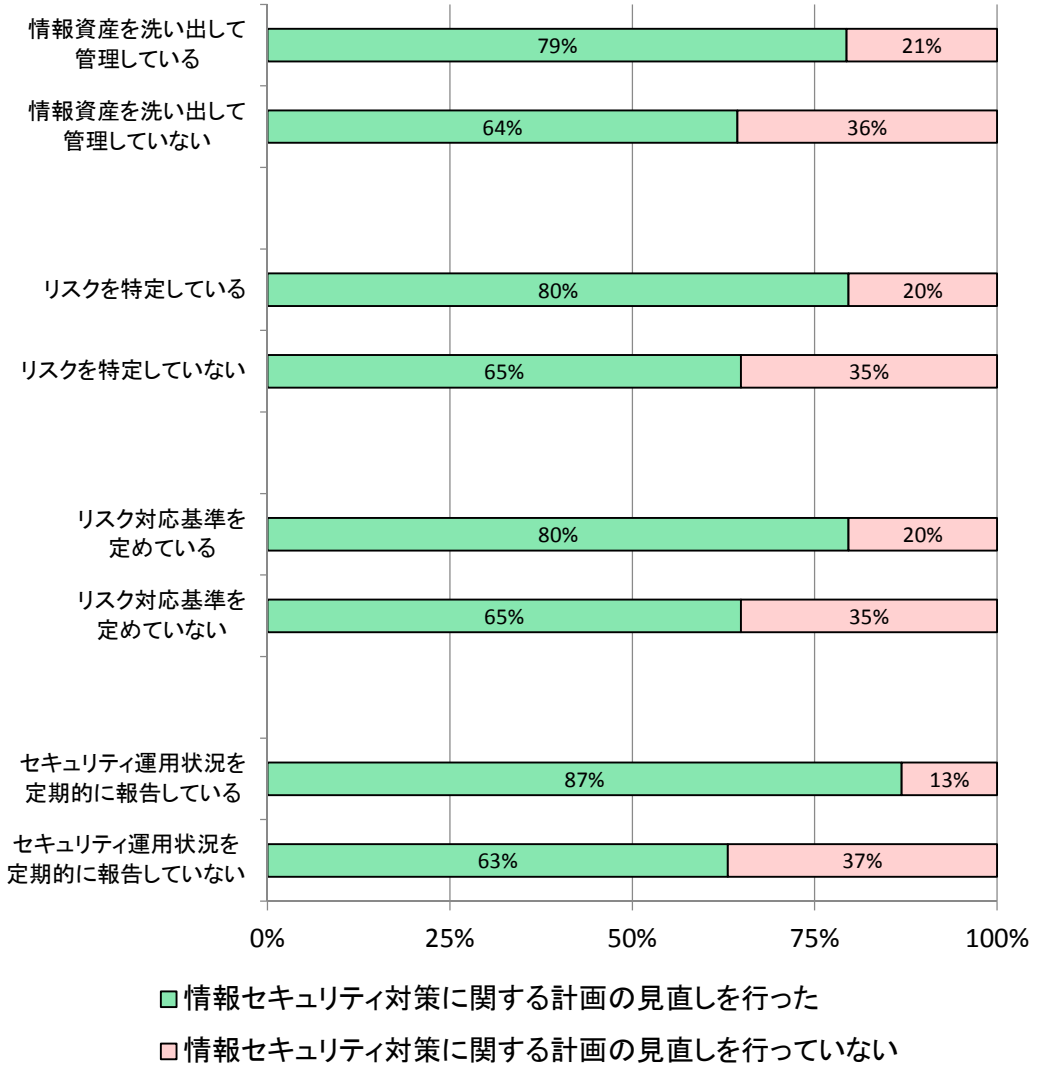
・情報セキュリティ対策に関する計画の見直しを行った事業者等は、情報資産の洗い出しやリスク特定、リスク対応基準の策定だけではなく、運用面において、セキュリティ対策状況を定期的に責任者と共有している傾向がある（参考①）。
・事業者等の内部で情報セキュリティ対策の計画を定め、計画に則り、PDCAを回せる事業者等は、多くの項目で良好な傾向がある。

情報セキュリティ対策に関する計画の見直し（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）

参考① 情報セキュリティ対策に関する計画の見直し状況と各種実施状況の関係性

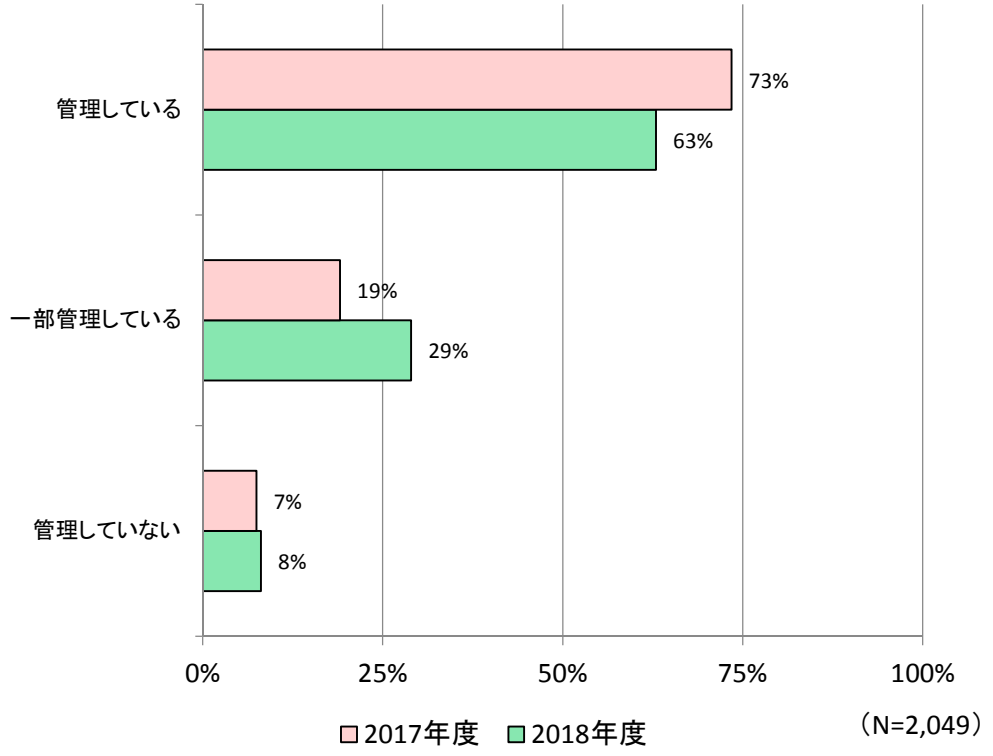


3.4. アンケート調査結果詳細 －（17/58）－

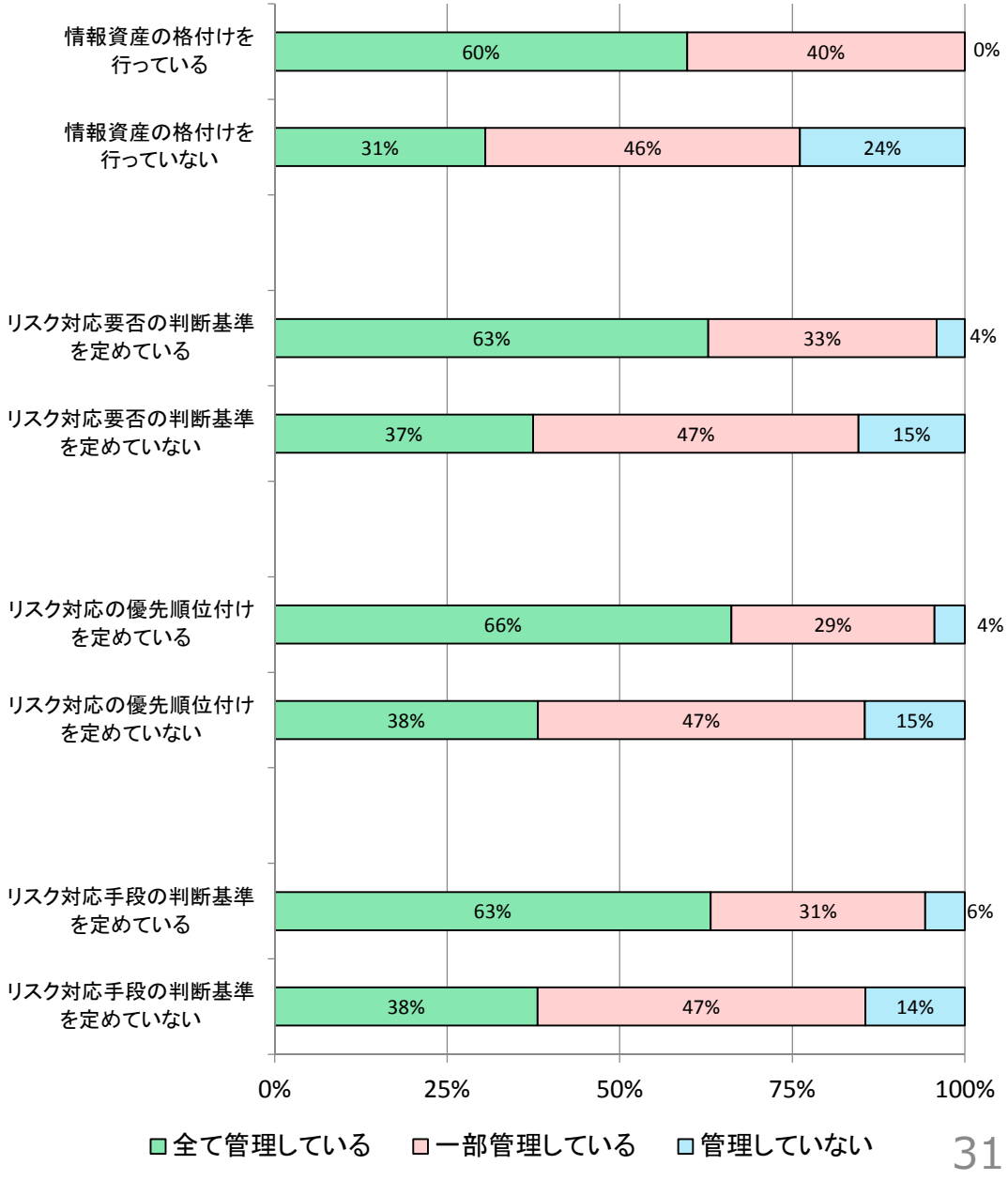
設問11　取扱い情報資産（システム含む）の洗い出し及び台帳等での管理状況

・取扱い情報資産の管理をしている事業者等は、情報資産の格付けまで実施している傾向やリスクの判断基準等が定められている傾向がある（参考①）。
・情報資産と重要度に応じた格付けを定めると共に、障害発生時に正しい判断や行動ができるように、リスク判断基準も明確になっており、管理と運用の両面で必要事項が定められている傾向がある。

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）



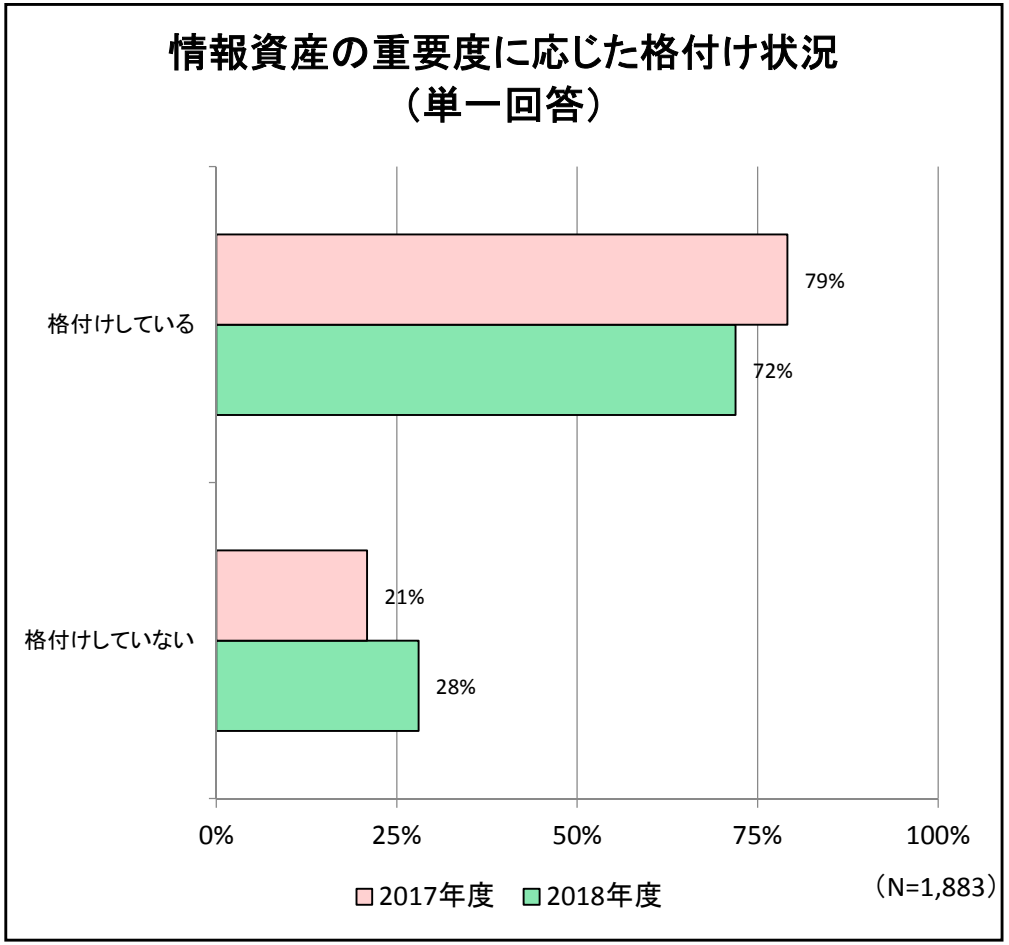
参考①　情報資産の管理状況と各項目の関係性



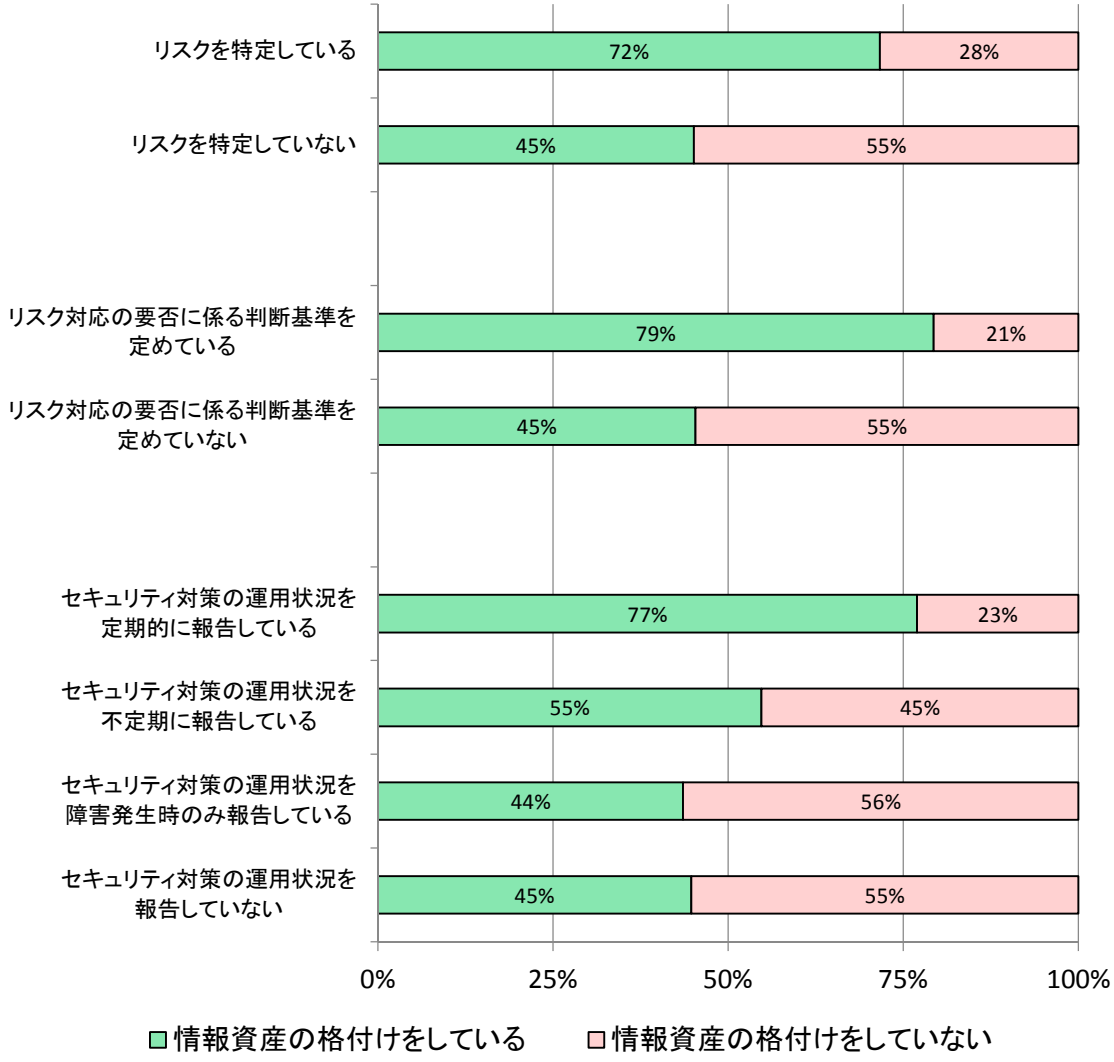
3.4. アンケート調査結果詳細 －（18/58）－

設問11-1 情報資産の重要度に応じた格付け状況

・情報資産の重要度に応じた格付けを実施している事業者等は、リスク特定、リスク対応基準等を定めている傾向がある。また、情報セキュリティに関する運用状況を定期的に報告している事業者等は、情報資産の重要度に応じた格付けもできている（参考①）。



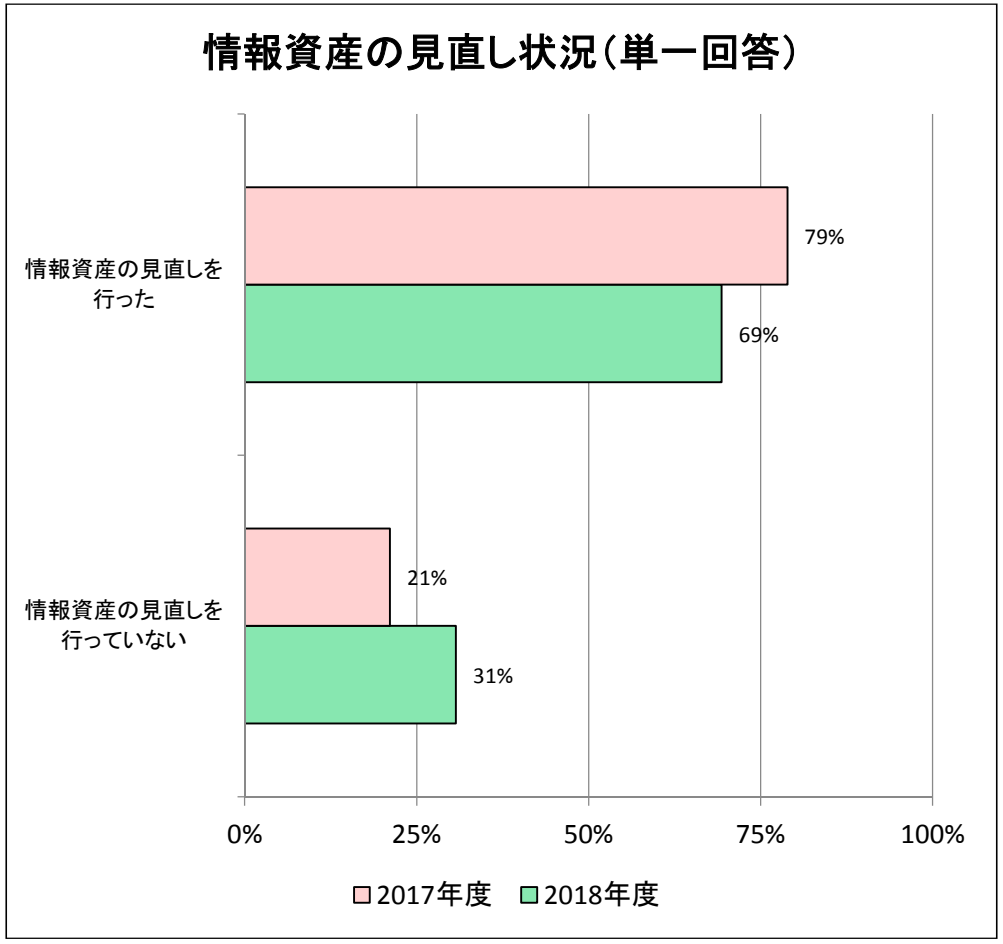
参考① 情報資産の格付け状況と各項目の関係性



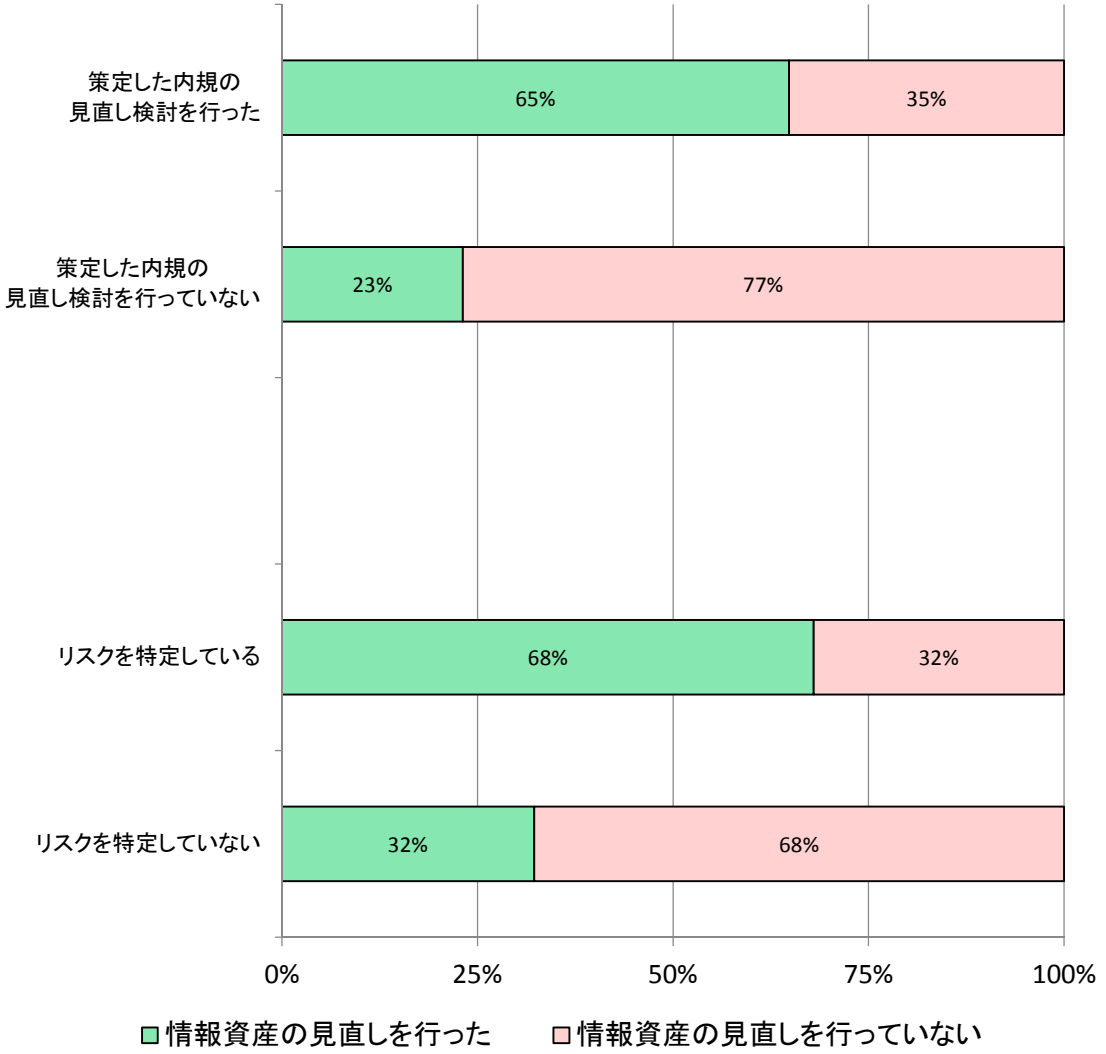
3.4. アンケート調査結果詳細 －（19/58）－

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る事業者等は、内規等の見直しを実施し、リスクの特定も実施している傾向がある（参考①）。内規等の見直しを契機に情報資産とリスクを適正に管理していることが推察できる。



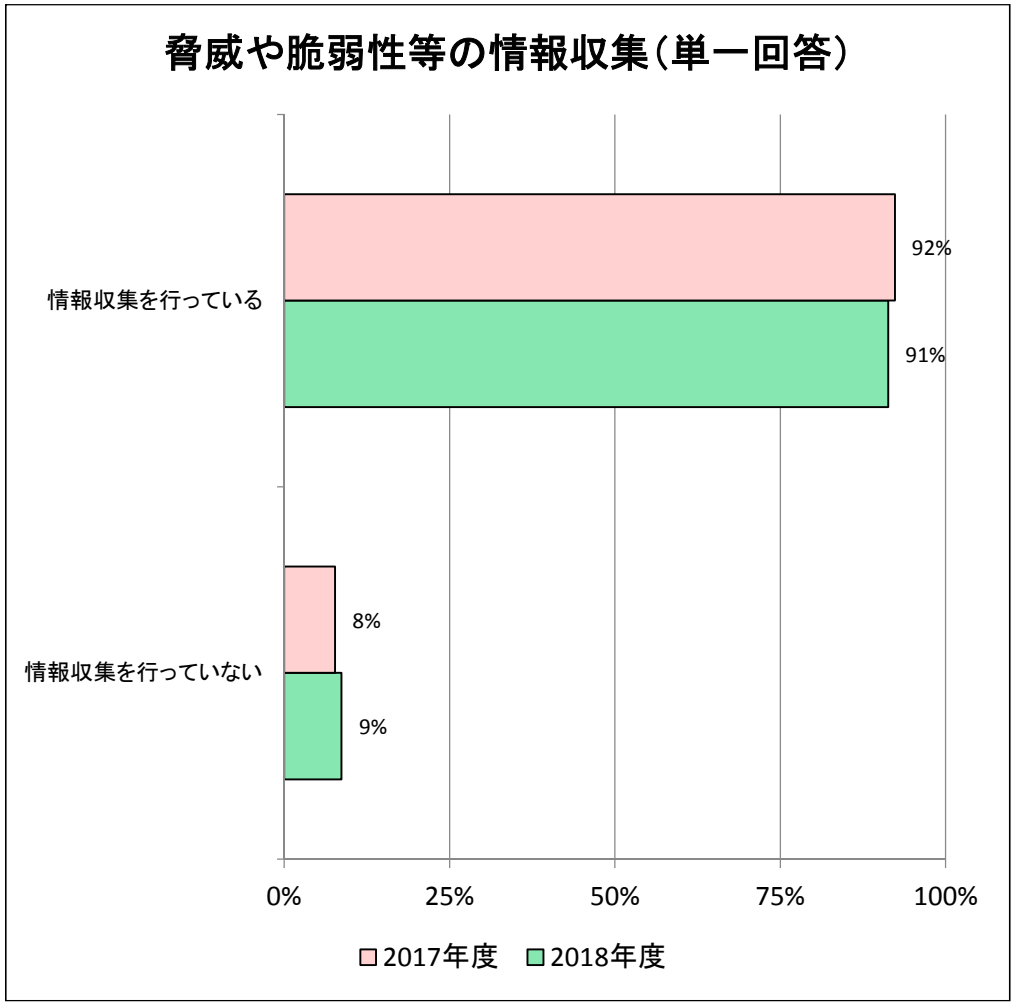
参考① 情報資産の見直し状況と各項目の関係性



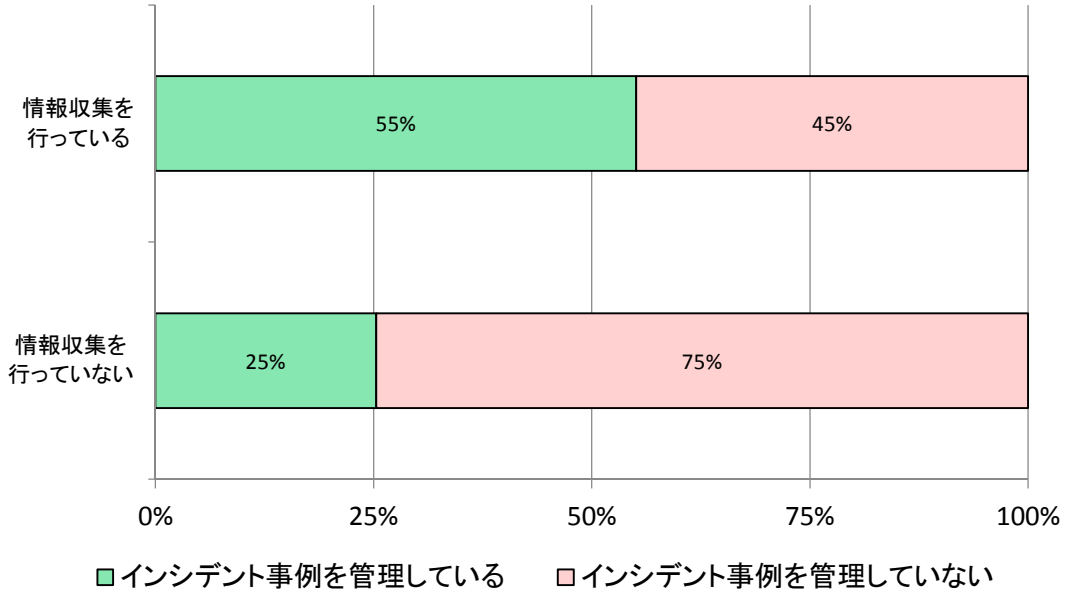
3.4. アンケート調査結果詳細 －（20/58）－

設問12　脅威や脆弱性等の情報収集

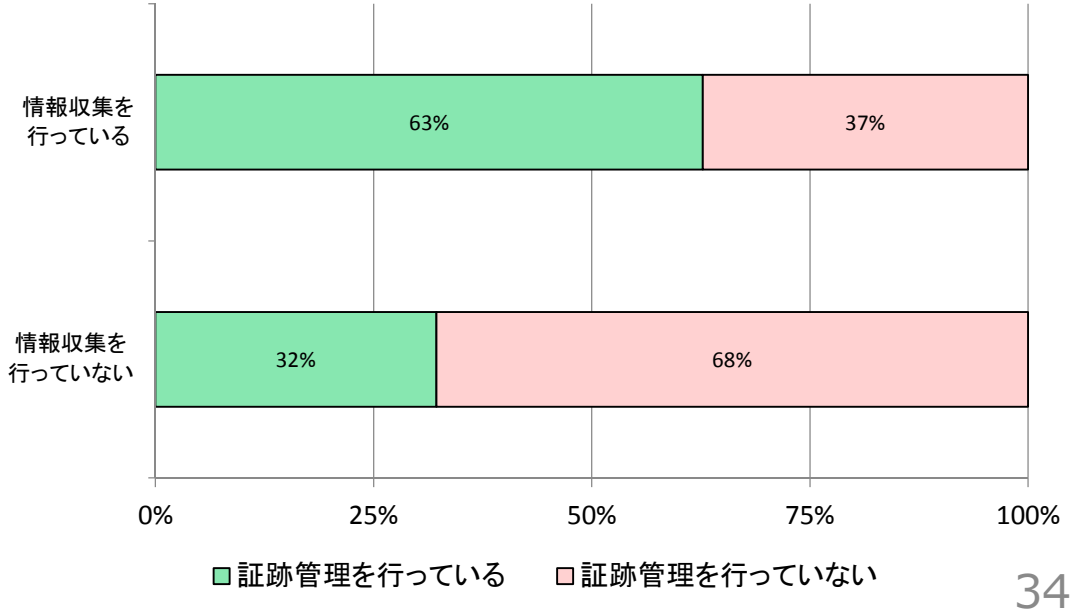
・情報収集を行っている事業者等は、自社内のインシデント管理を実施している傾向があり、セキュリティ対策としても証跡管理を行っていることが多い（参考①、参考②）。セキュリティ情報の収集を行っている事業者等は、収集したセキュリティ情報をもとに対策まで実施していると推察できる。



参考①　情報収集とインシデント事例管理状況の関係性



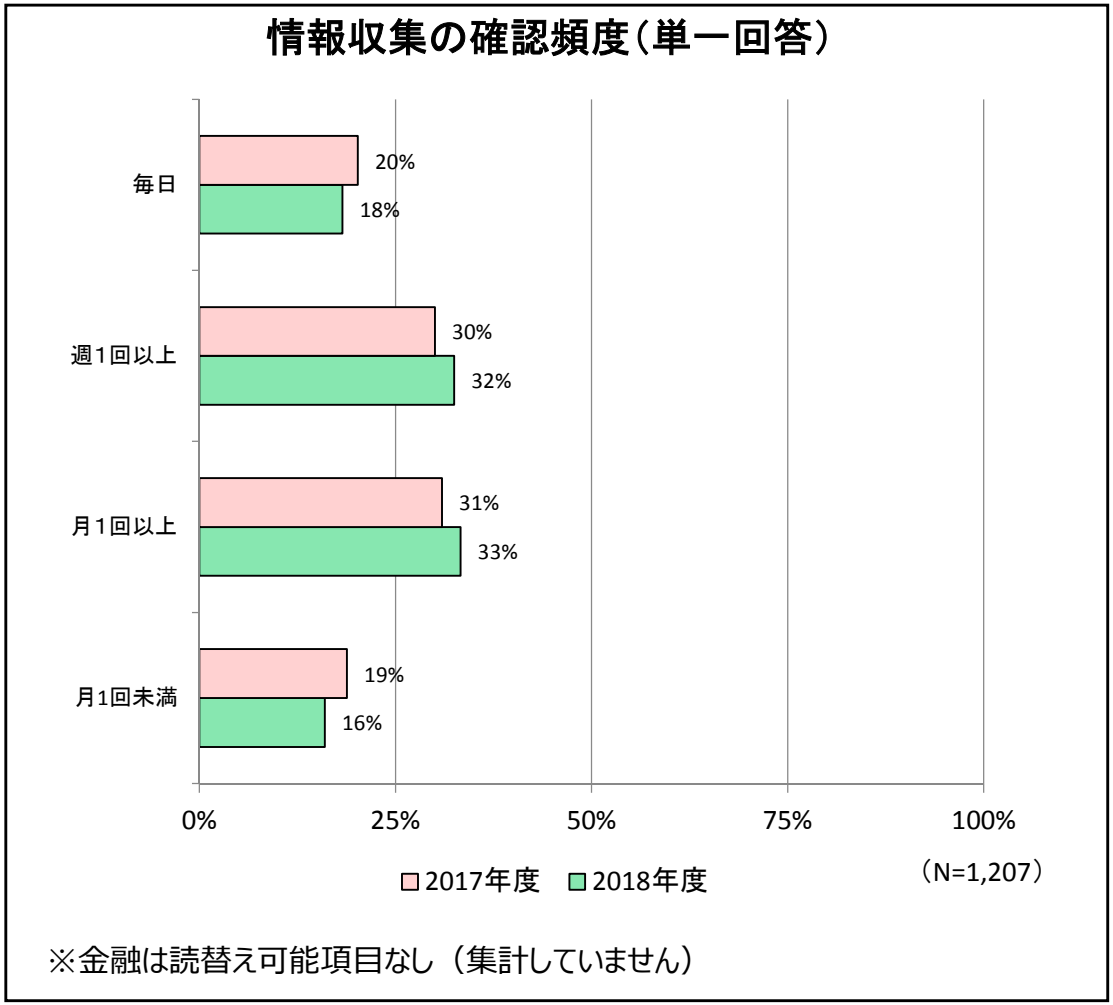
参考②　情報収集と証跡管理の関係性



3.4. アンケート調査結果詳細 －（21/58）－

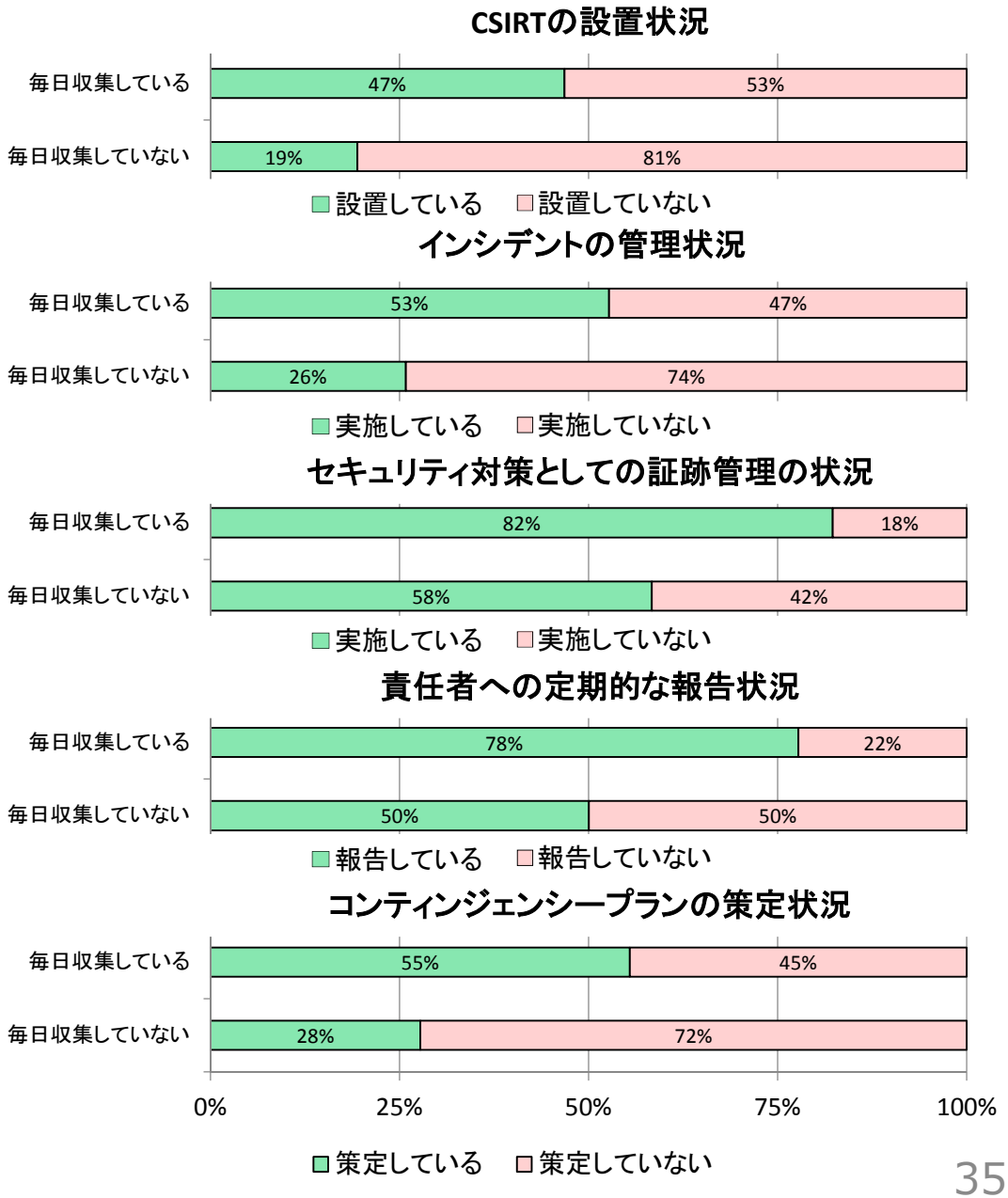
設問12-1 情報収集の確認頻度

・情報収集を毎日行っている事業者等は、CSIRTの設置、インシデント管理、証跡管理、責任者との情報連携、コンティンジェンシープラン（CP）の策定等、様々な取り組みが進んでいる傾向がある（参考①）。
・政府の動向やインシデント情報を収集し、事業者等のセキュリティ対策を実施していると推察できる。



※金融は読替え可能項目なし（集計していません）

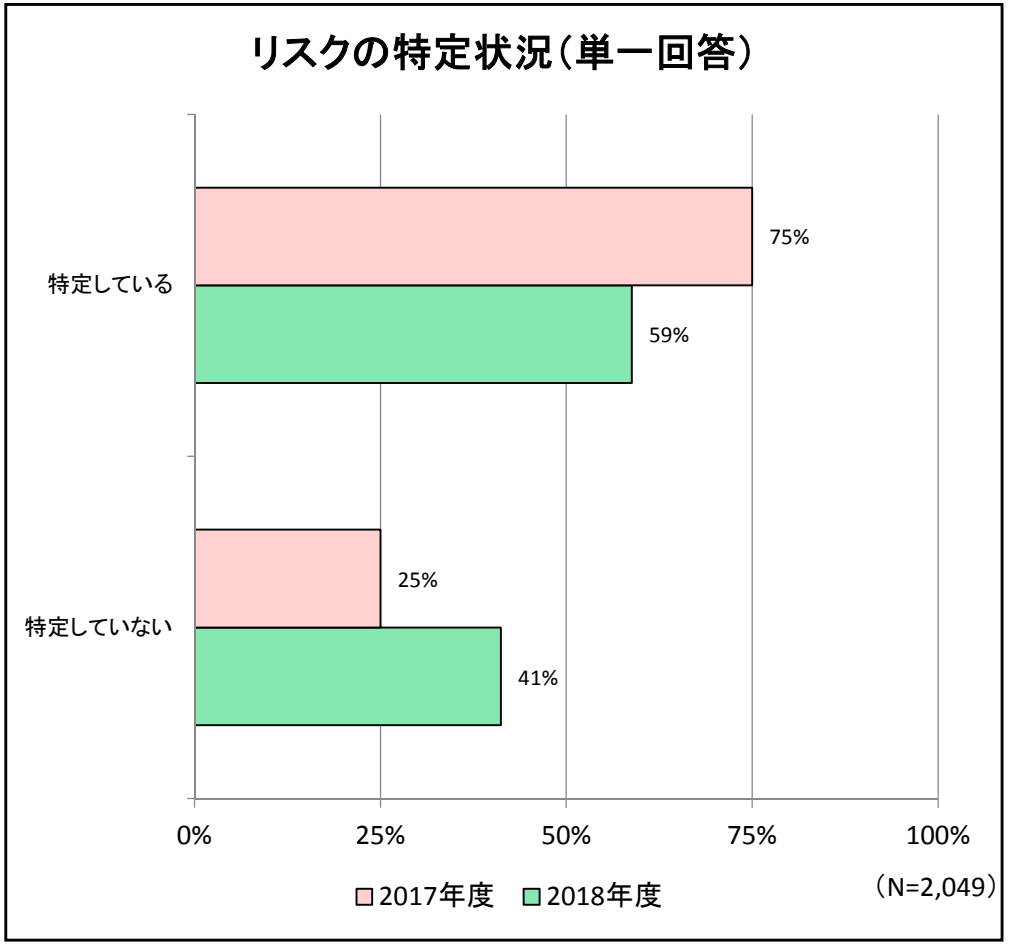
参考① 情報収集の頻度と各項目の関係性



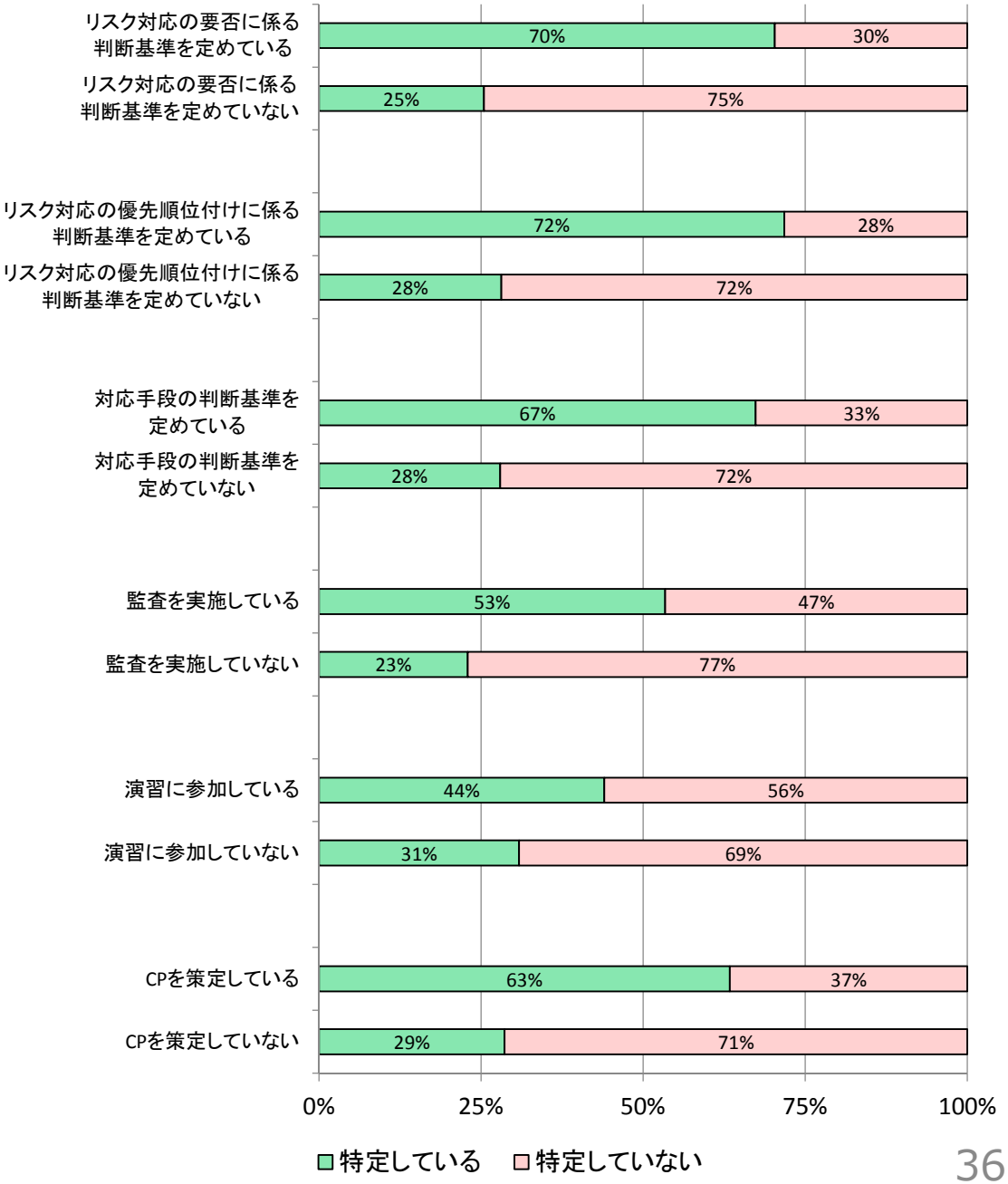
3.4. アンケート調査結果詳細 －（22/58）－

設問13 リスクの特定状況

・リスクの特定を行っている事業者等は、リスク対応要否の判断基準やリスク対応の優先順位づけ、リスク対応手段の判断基準等を策定していることから有事の際の対応を想定し、リスクの特定を行っている（参考①）。
・リスクの特定を行っている事業者等は、監査の実施や演習の参加割合が高いため、改善活動を進める上でリスクを特定することは、優先事項として取り組んでいると推察できる。



参考① リスクの特定状況と各項目の関係性



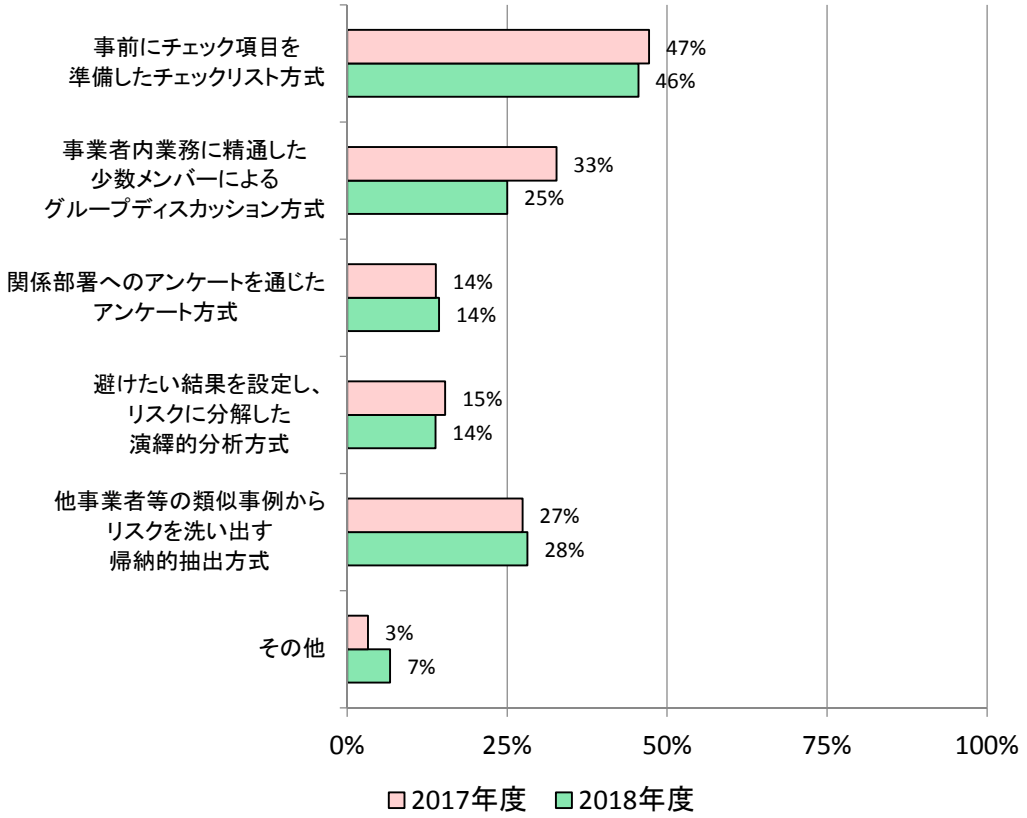
3.4. アンケート調査結果詳細 －（23/58）－

設問13-1 リスクの特定方法

・リスクの特定方法としてチェック項目の方式を用いる場合は、リスク対応要否の判断基準が定められている傾向があるため、リスク対応を強化したい場合は、チェックリスト方式を採用することが推奨される（参考①）。

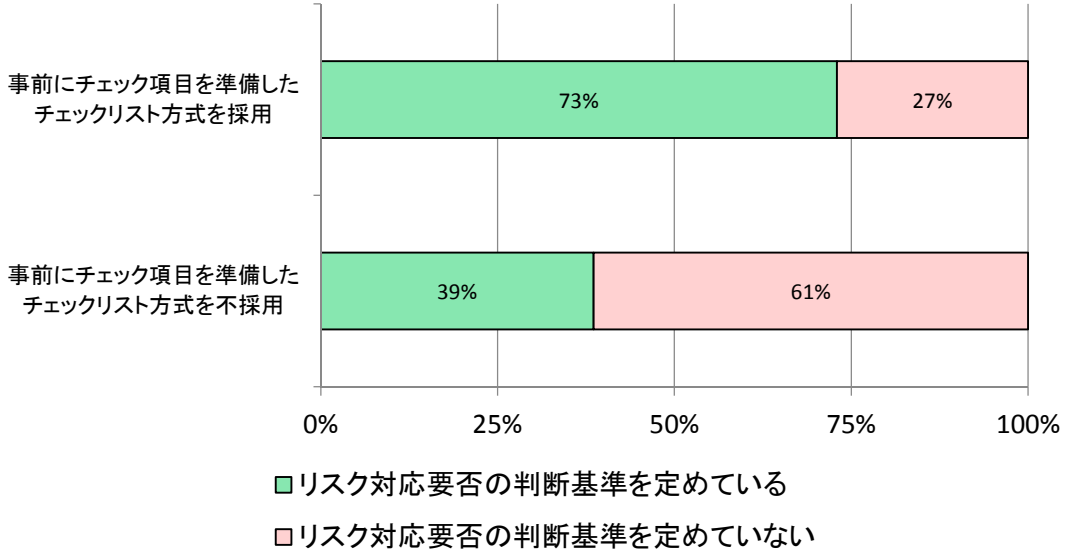
・リスクの特定方法として、他事業者等の類似事例からの帰納的抽出方式を用いた場合は、セプター事務局からの情報をしっかりと受け取っている傾向があるため、情報共有を強化したい場合は、演繹的分析方式を採用することが推奨される（参考②）。

リスクの特定方法（複数回答）

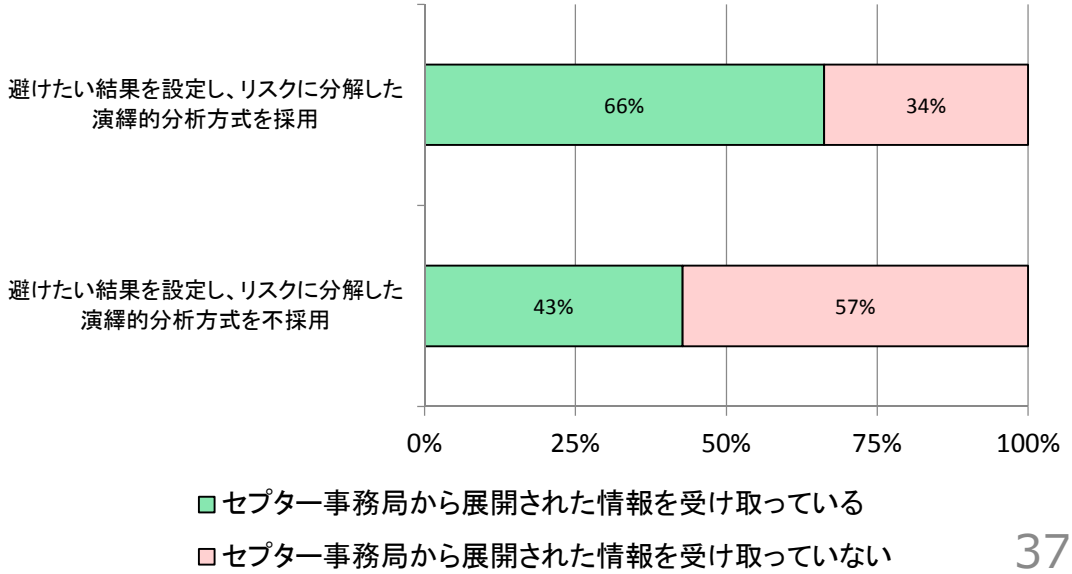


※金融は読替え可能項目なし（集計していません）

参考① リスクの特定方法とリスク対応要否の判断基準の関係性



参考② リスクの特定方法と情報共有の関係性

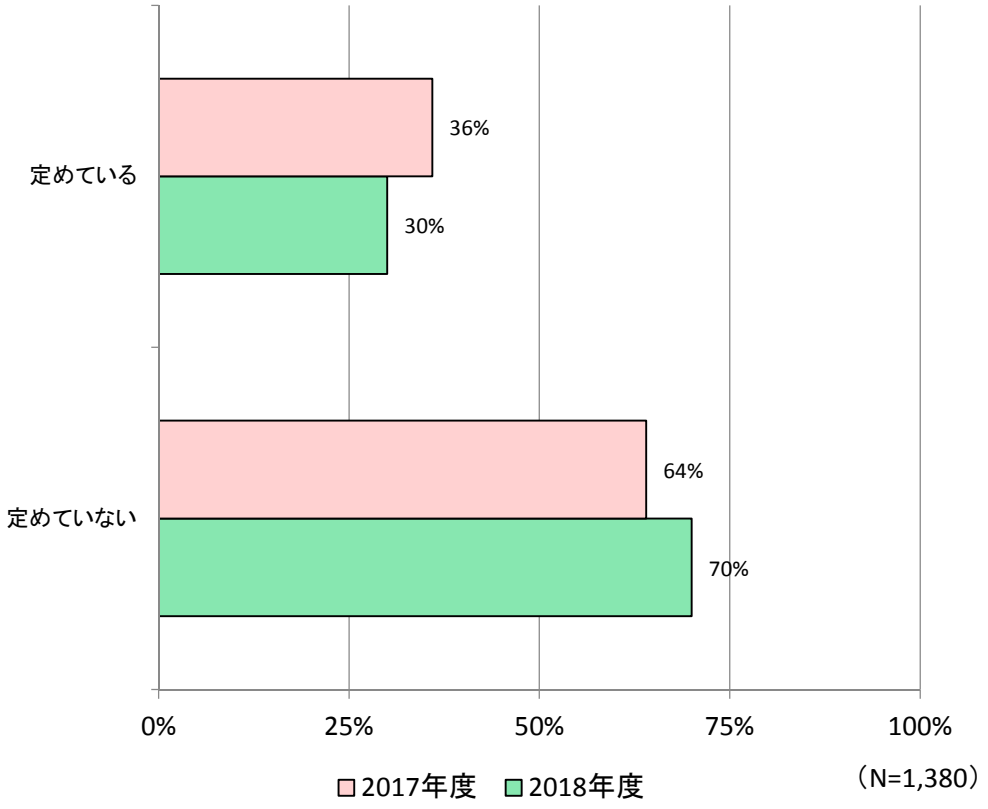


3.4. アンケート調査結果詳細 －（24/58）－

設問14 リスク対応の要否に係る判断基準

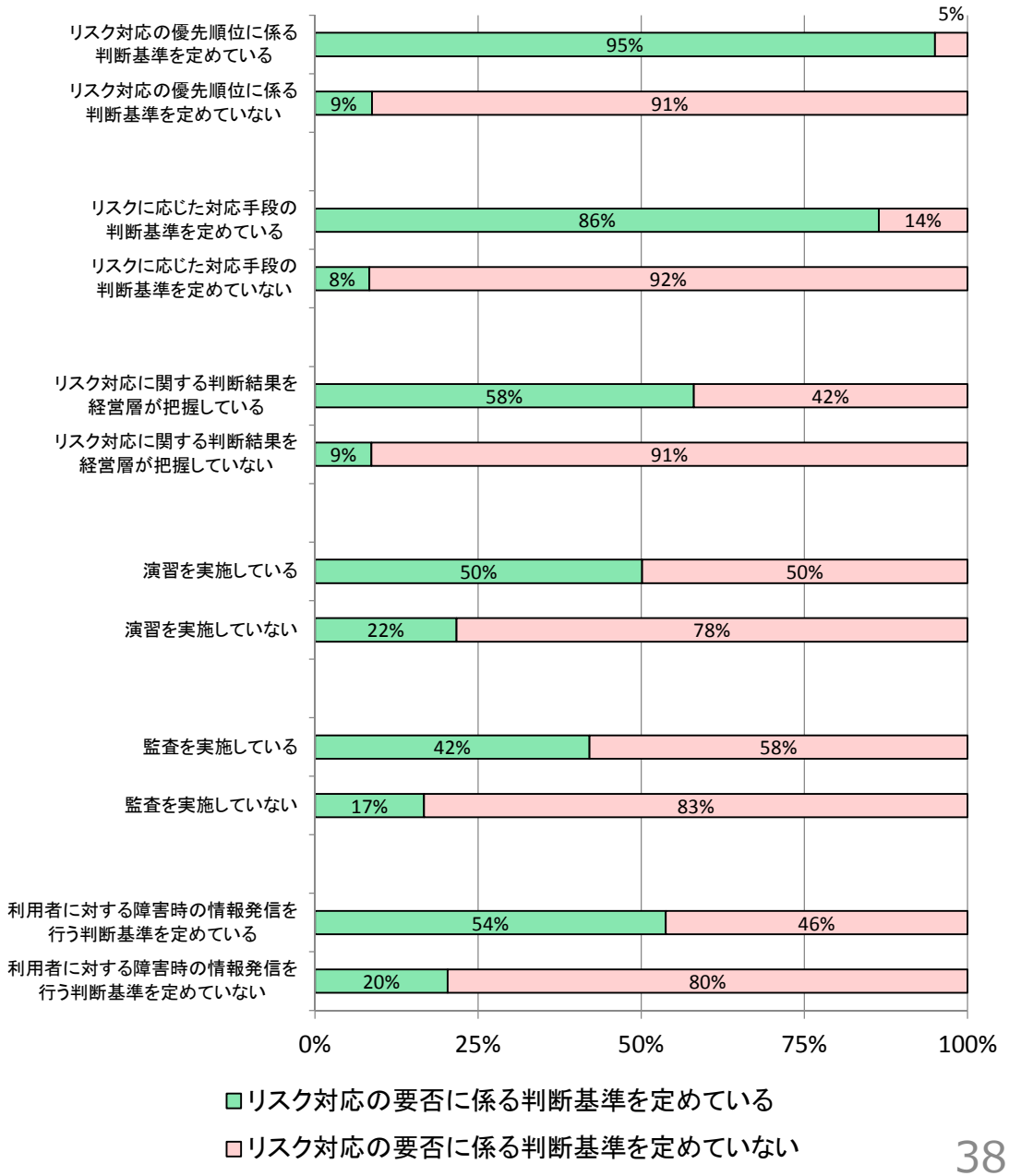
・リスク対応の要否に係る判断基準が決定している事業者等は、多くの項目において良好な傾向が見られた。特に、リスク対応の要否だけではなく、優先順位に係る判断基準も定められ、対応手順に至るまで決定している傾向がある。さらに、経営層の積極的な関わりも確認できることから、演習や監査の機会を通じて、情報セキュリティ体制の改善活動がされていると推察できる（参考①）。

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）

参考① リスク対応の要否に係る判断基準の決定状況と各項目の関係性

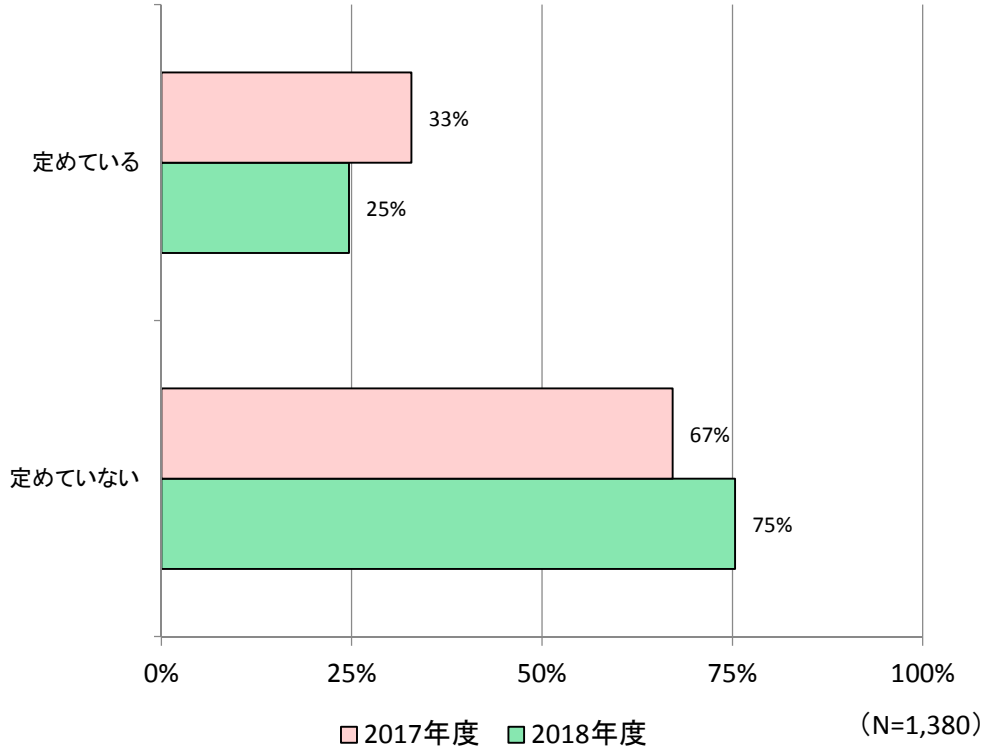


3.4. アンケート調査結果詳細 －（25/58）－

設問15 リスク対応の優先順位に係る判断基準

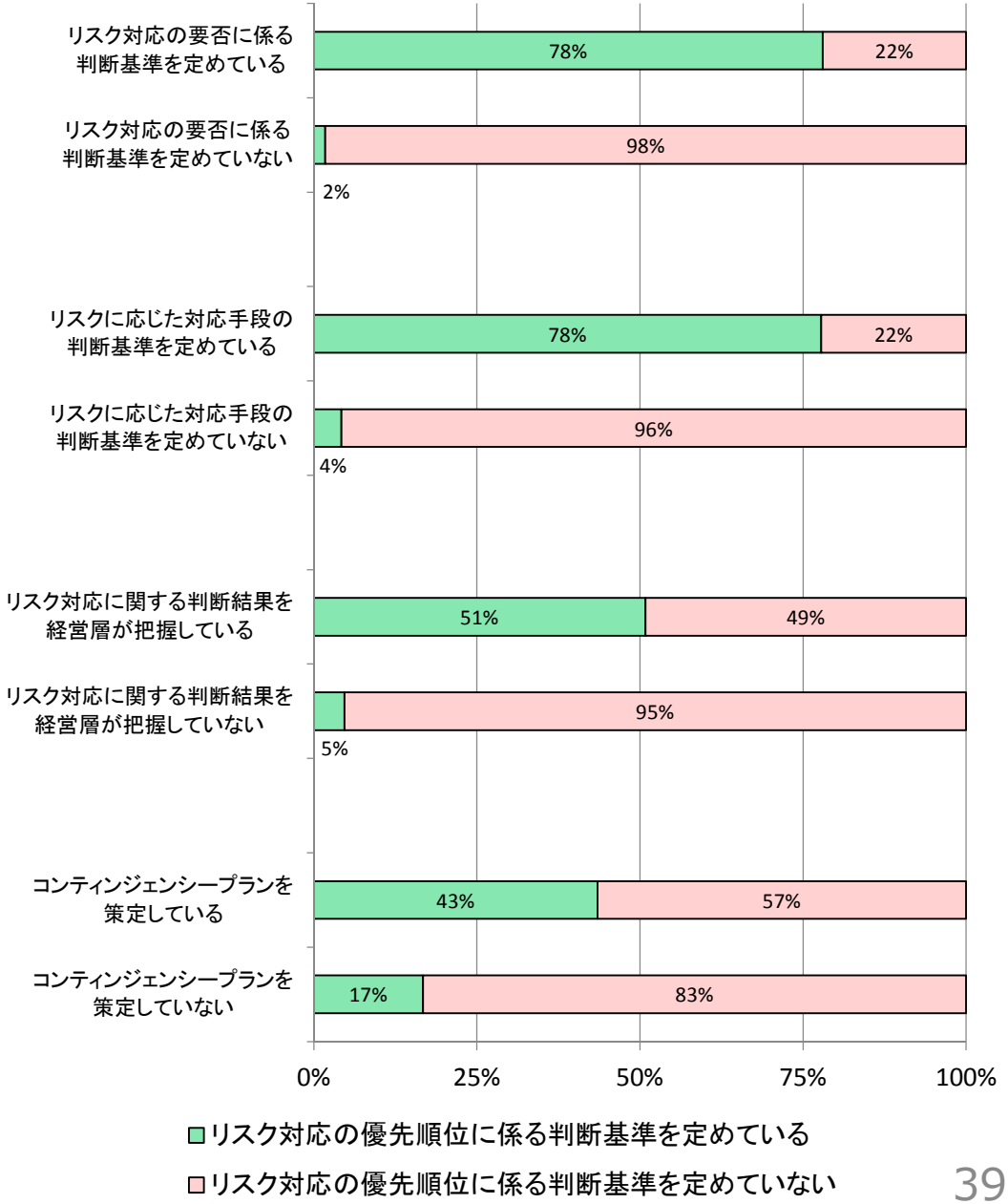
・リスク対応の優先順位が決定している事業者等は、多くの項目において良好な傾向が見られた。特に、対応手順に至るまで決定している傾向がある。さらに、経営層の積極的な関わりも確認できることから、演習や監査の機会を通じて、情報セキュリティ体制の改善活動がされていると推察できる（参考①）。

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）

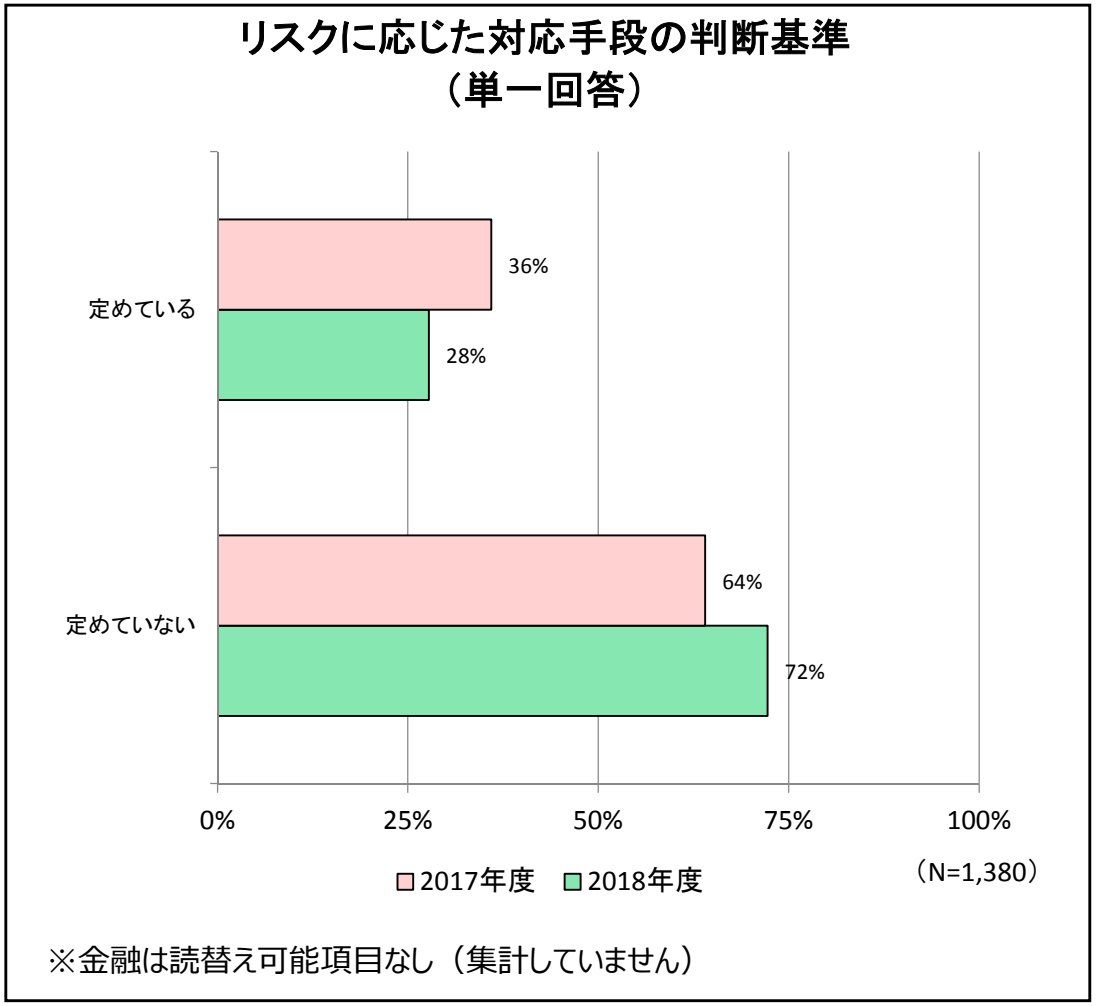
参考① リスク対応の優先順位に係る判断基準の決定状況と各項目の関係性



3.4. アンケート調査結果詳細 －（26/58）－

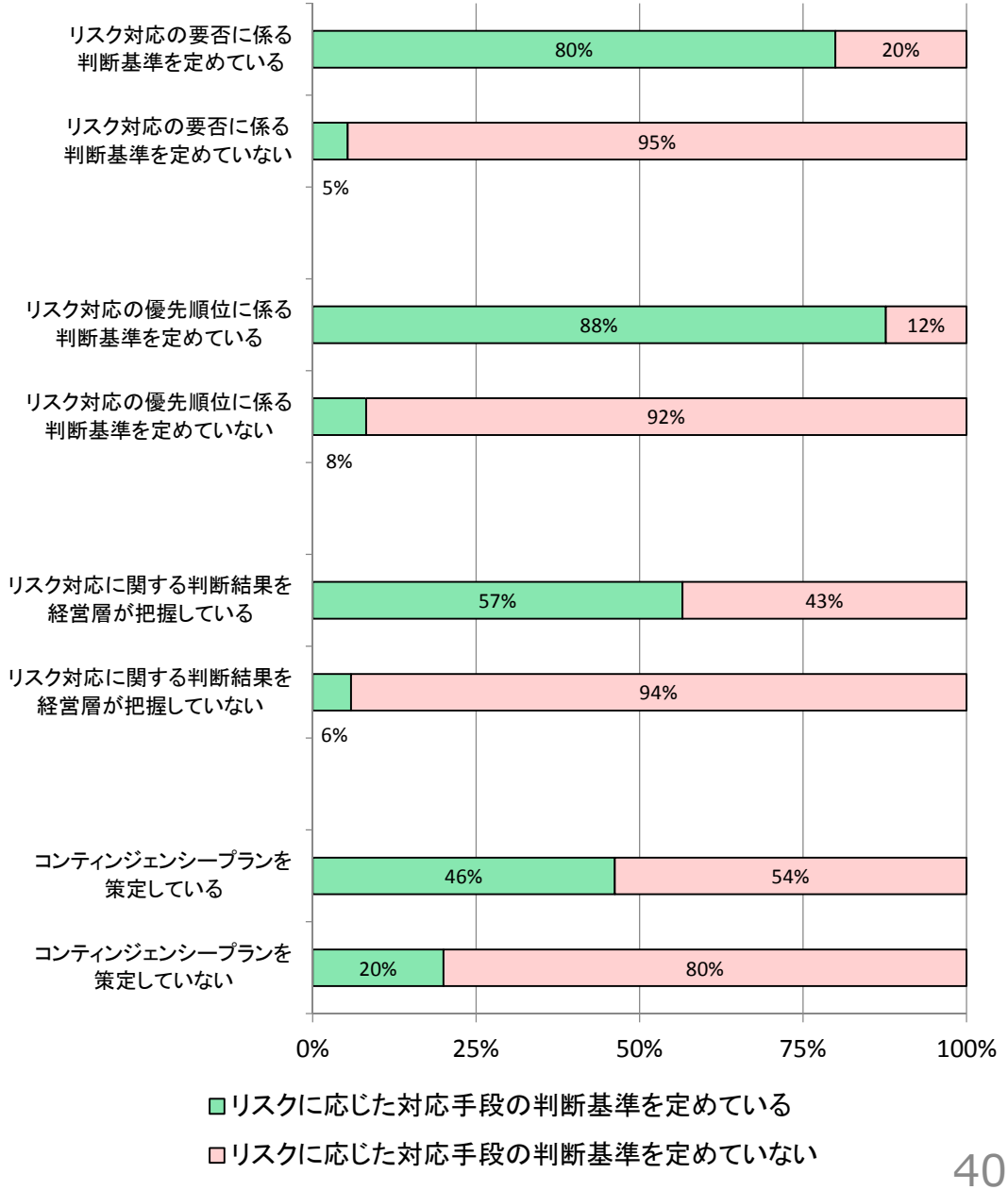
設問16 リスクに応じた対応手段の判断基準

・リスクに応じた対応手順の判断基準が決定している事業者等は、多くの項目において良好な傾向が見られた。さらに、経営層の積極的な関わりも確認できることから、演習や監査の機会を通じて、情報セキュリティ体制の改善活動がされていると推察できる（参考①）。



※金融は読替え可能項目なし（集計していません）

参考① リスクに応じた対応手段の判断基準の決定状況と各項目の関係性

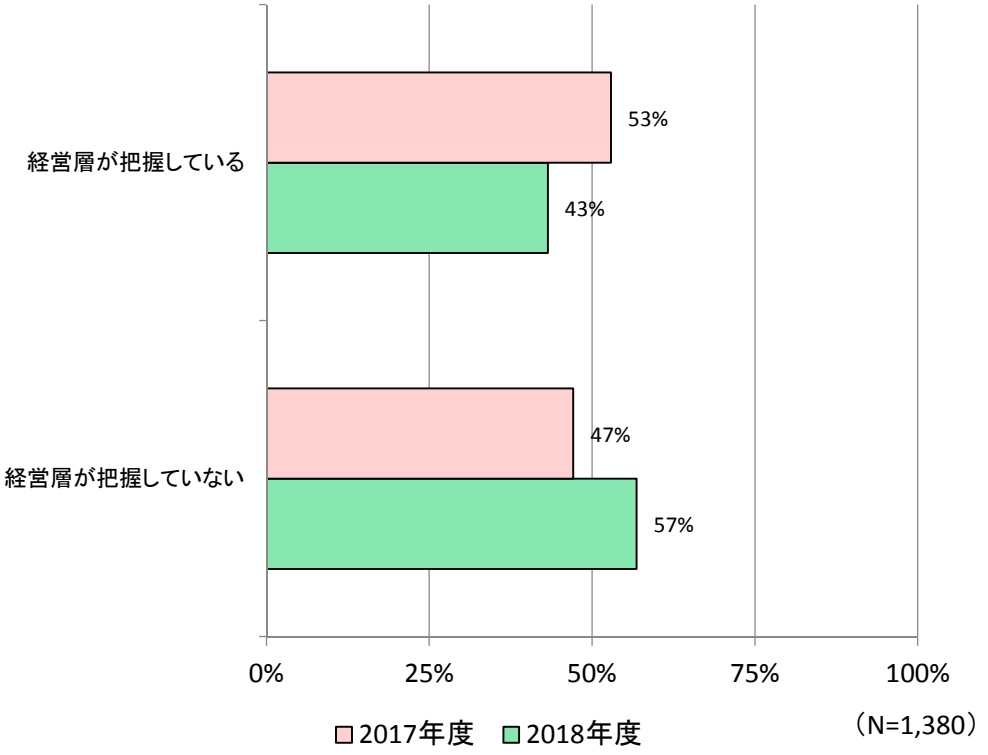


3.4. アンケート調査結果詳細 －（27/58）－

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

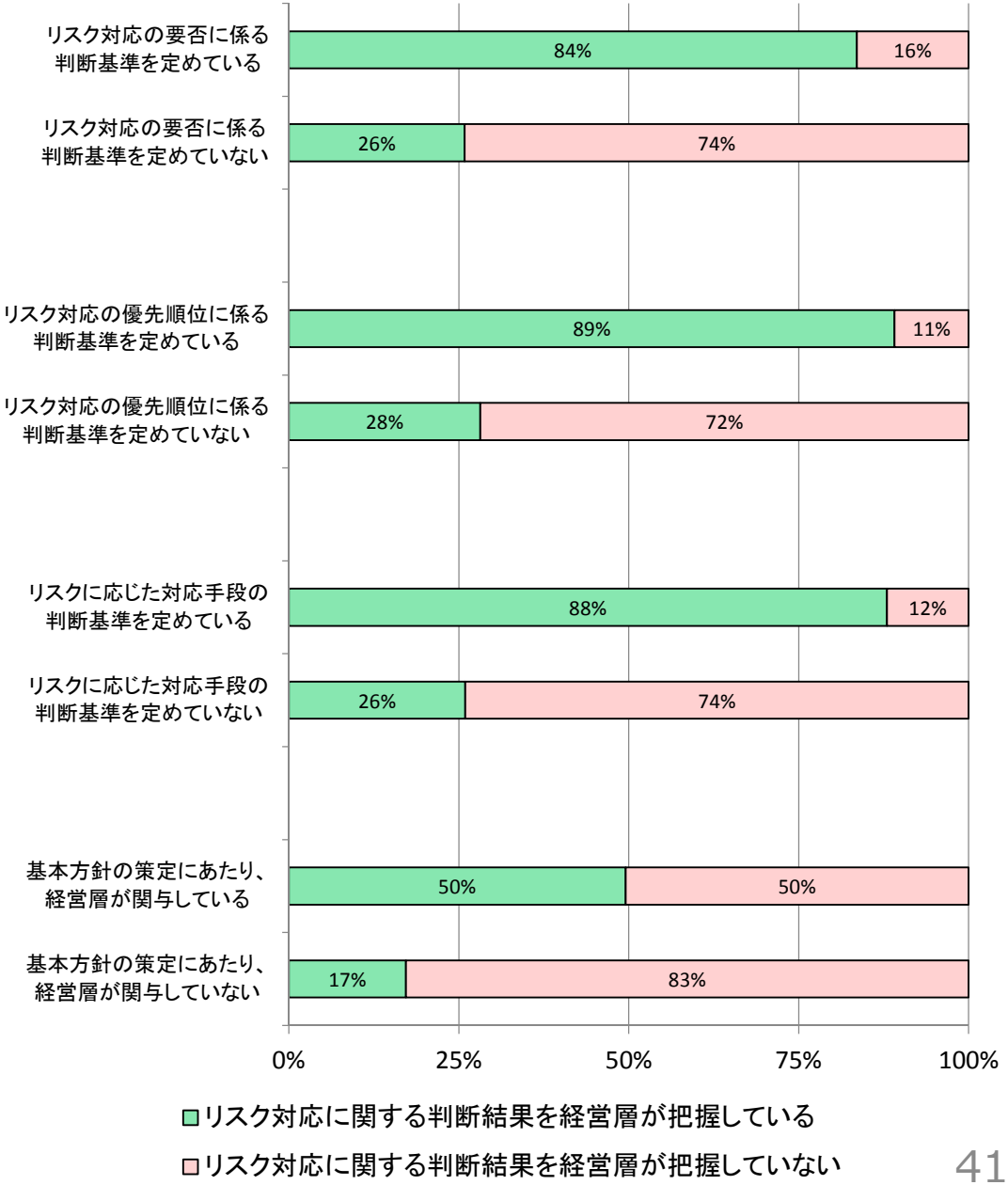
・リスク対応に関する判断結果を経営層が把握していない事業者等は、演習を実施しておらず、監査も実施していない傾向がある。また、障害発生時に利用者に対して情報発信を行う判断基準も策定されていない。さらに、経営層が把握している事業者等は、情報セキュリティ基本方針にも関与している傾向がある（参考①）。

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）

参考① リスク対応の判断結果の経営層の認知状況と各項目の関係性

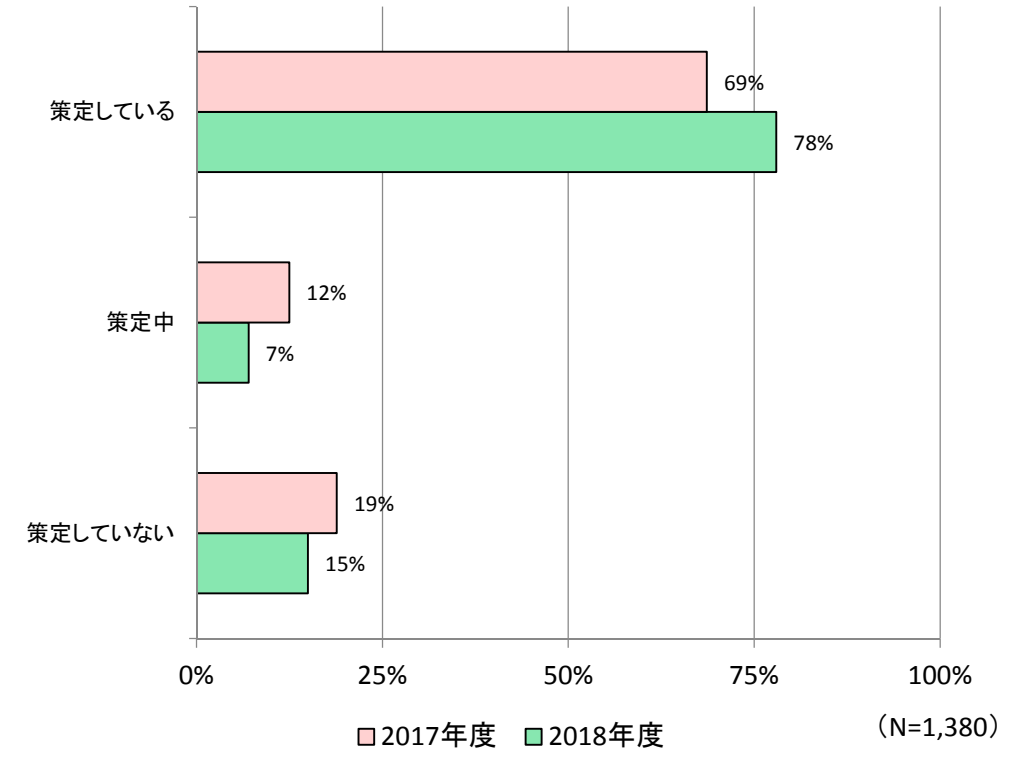


3.4. アンケート調査結果詳細 －（28/58）－

設問18 情報セキュリティに関する内規の策定状況

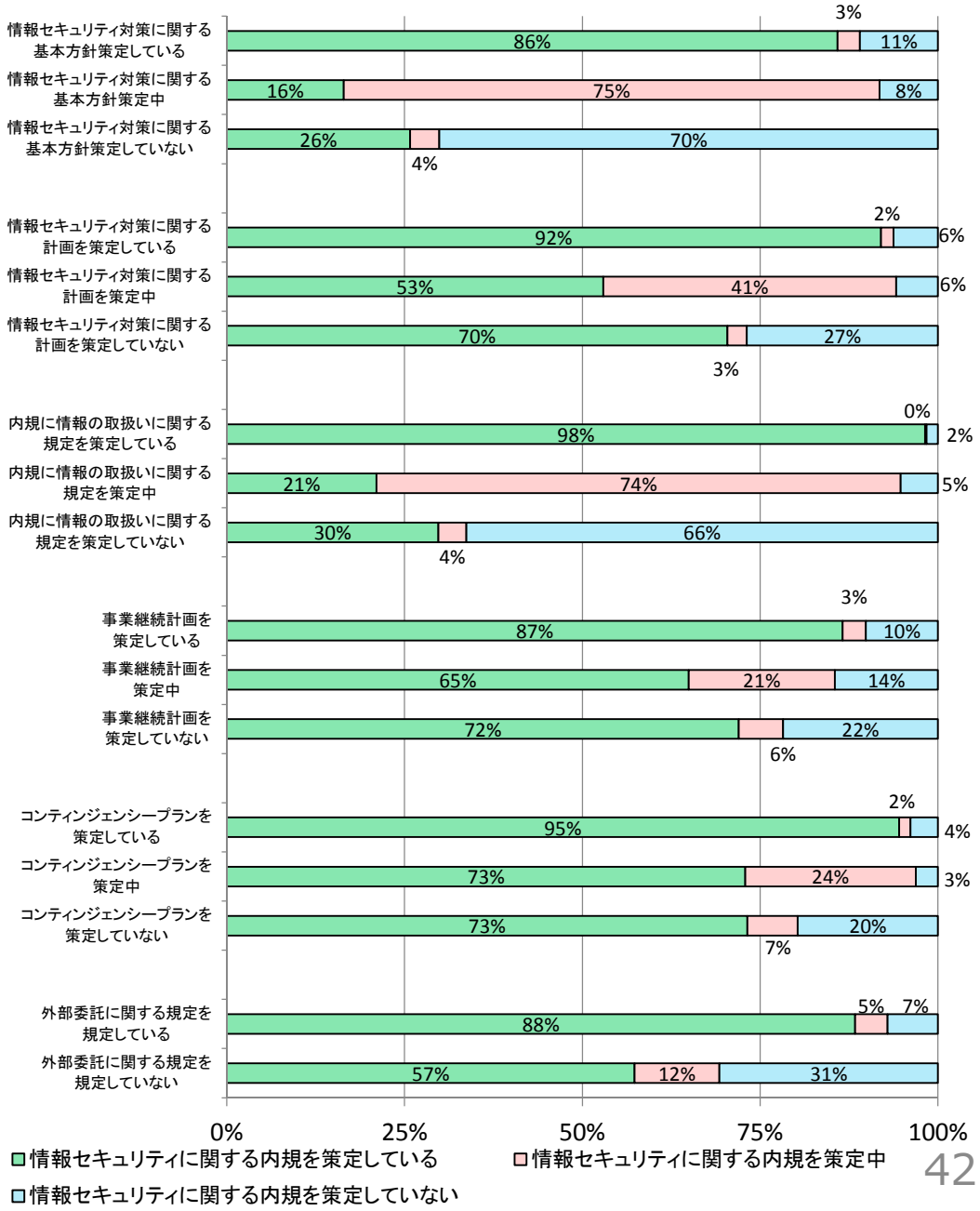
・情報セキュリティに関する内規まで策定している事業者等は、規定類が策定されている傾向がある（参考①）。ただし、事業継続計画（BCP）やコンティンジェンシープラン（CP）は、それほど大きな差は見られないことから、これらの策定については、規定類の整備とは異なるアプローチでの啓発活動が必要であると推察できる。

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）

参考① 情報セキュリティに関する内規の策定状況と各項目の関係性

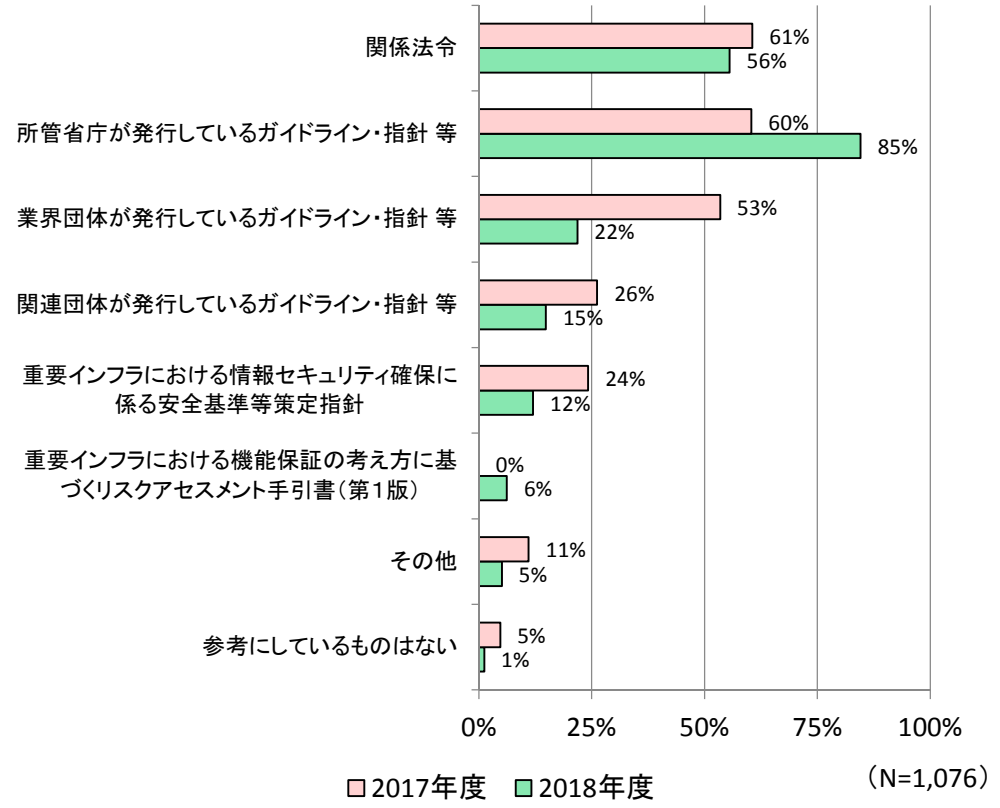


3.4. アンケート調査結果詳細 －（29/58）－

設問18-1　内規等を策定する際の参考文献

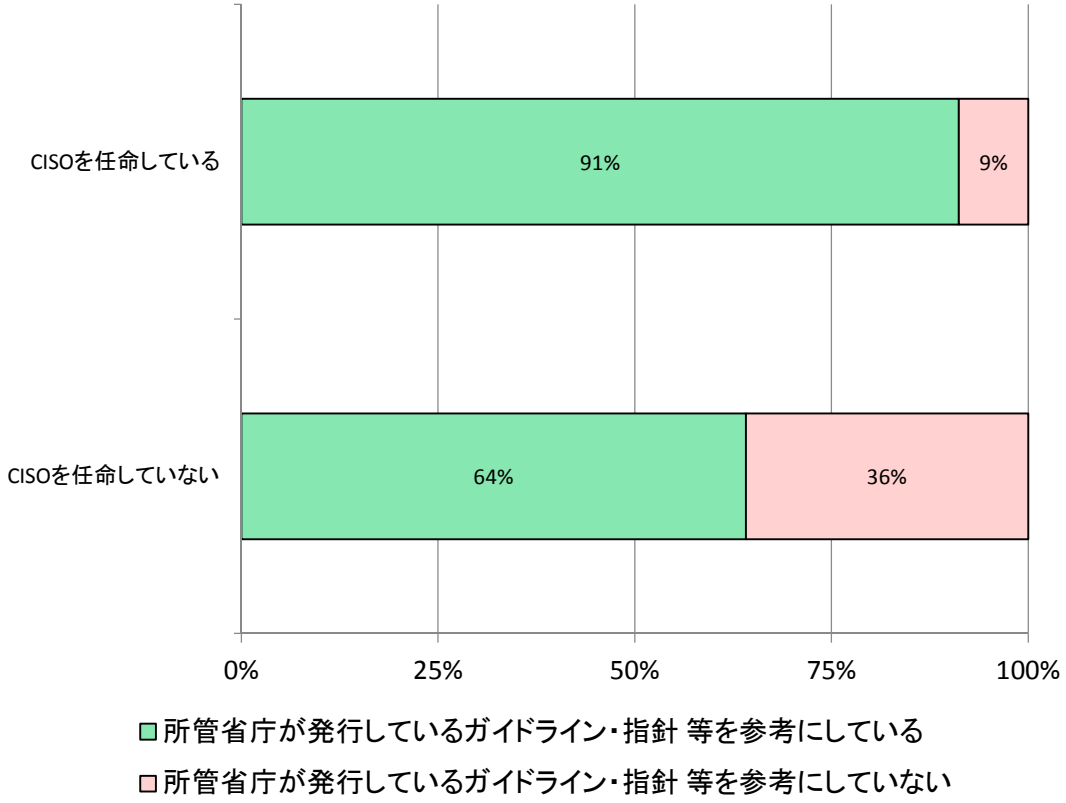
・内規等を策定する際の参考文献として、所管省庁が発行しているガイドライン・指針等を参考にしている事業者等は、CISOを任命している傾向がある。政府が指針等で、CISOの任命を求めていることが反映されているためであると考えられる（参考①）。

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）
※リスクアセスメント手引書は、2018年度から調査開始

参考①　CISOの任命状況と内規等を策定する際の参考文献の関係性

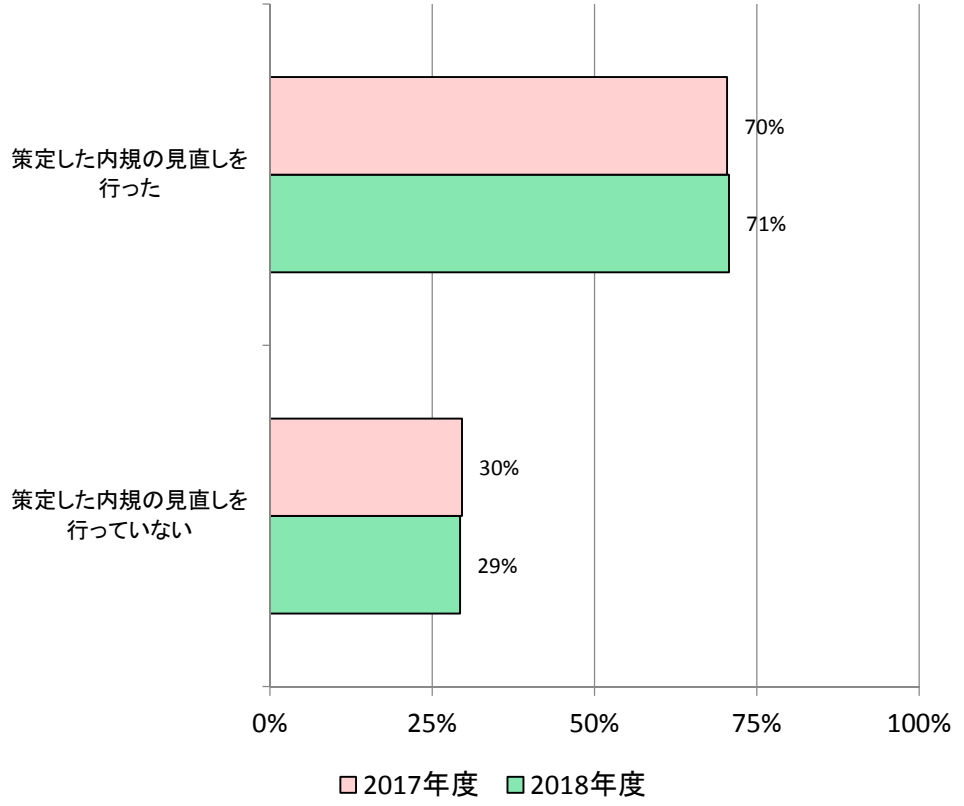


3.4. アンケート調査結果詳細 －（30/58）－

設問18-2　策定した内規の見直し検討状況

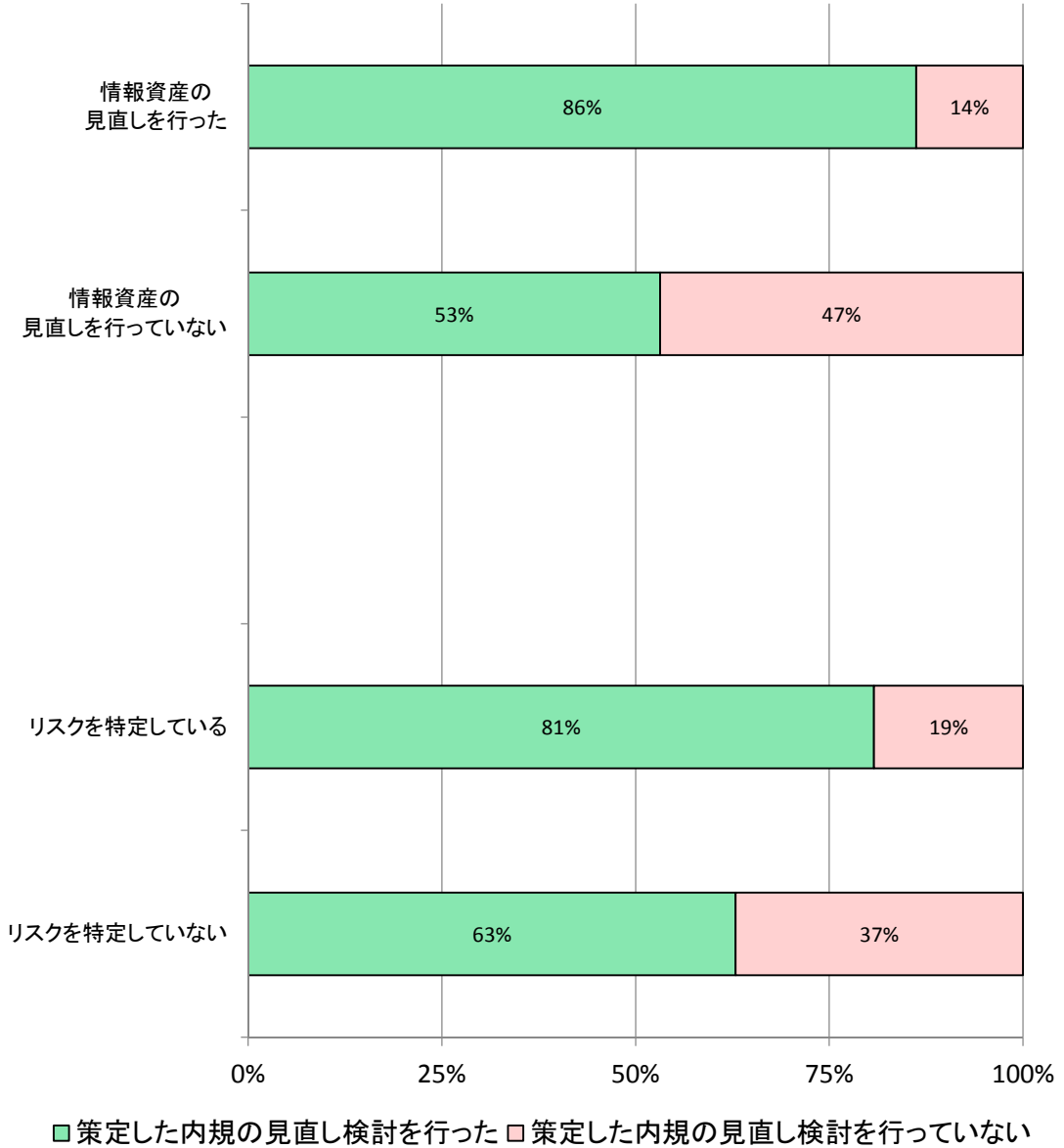
・策定した内規等の見直しを実施している事業者等は、情報資産の見直しも実施している傾向がある。また、リスクの特定も実施している傾向がある（参考①）。
・そのため、内規等の見直しに合わせて、情報資産の見直しがされる仕組みが循環していることが推察される。

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）

参考①　策定した内規の見直し検討状況と各項目の関係性

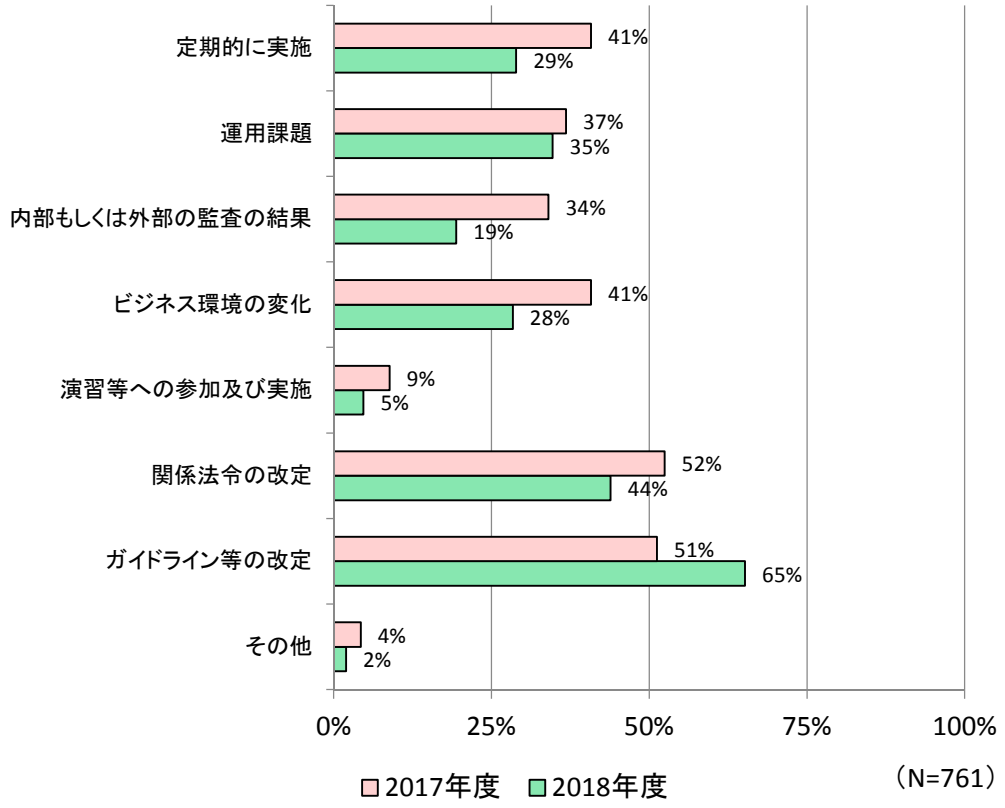


3.4. アンケート調査結果詳細 －（31/58）－

設問18-3 内規の見直し検討の契機

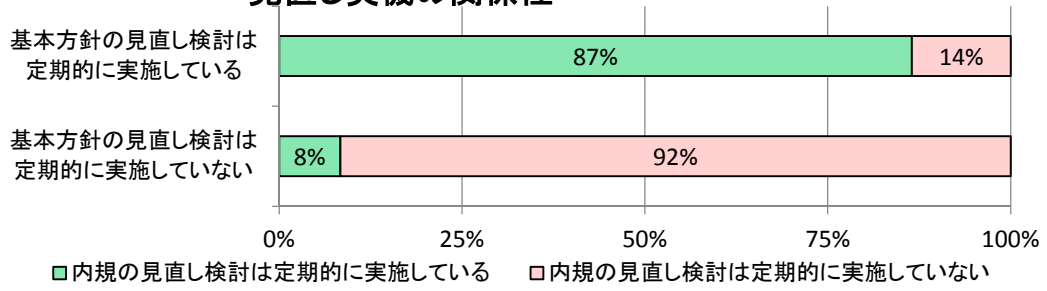
・内規の見直し検討の契機と情報セキュリティ基本方針の見直しの契機は、同じく定期的に見直し検討を行っていることが確認できる（参考①）。
・定期的もしくは運用課題を見つけて自発的に見直し検討を行っている事業者等よりも、ガイドラインや関係法令の改定といった外的要因により、見直しをしている割合が多い傾向がある。

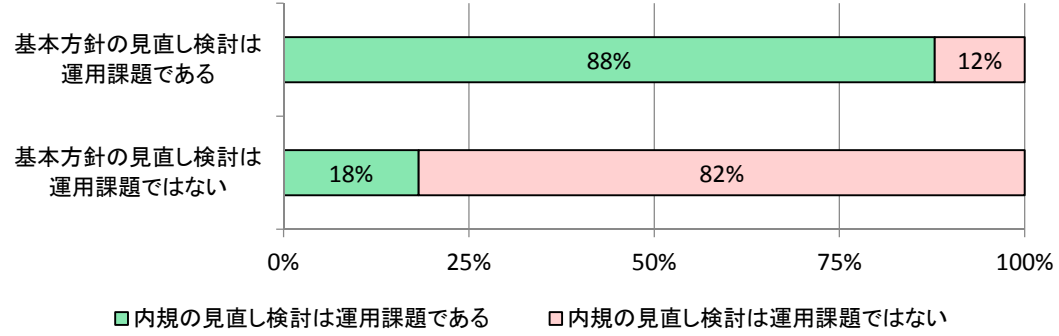
内規の見直し検討の契機（複数回答）

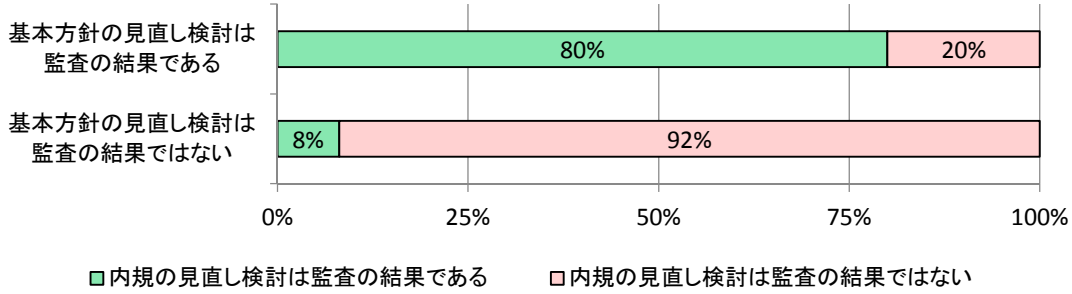


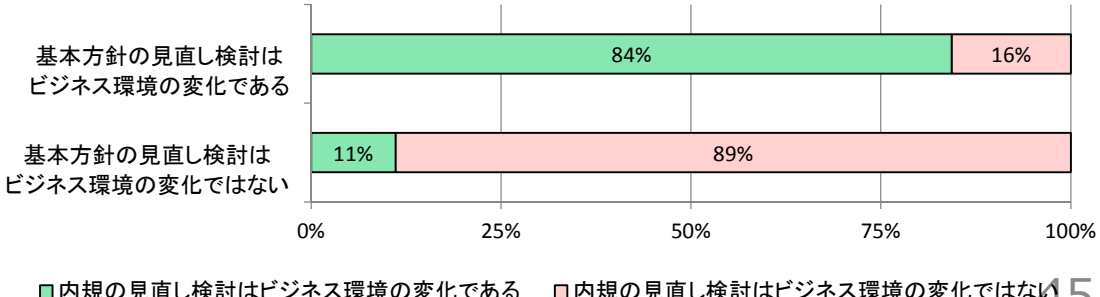
※金融は読替え可能項目なし（集計していません）

参考① 内規の見直し検討の契機と基本方針の見直し契機の関係性







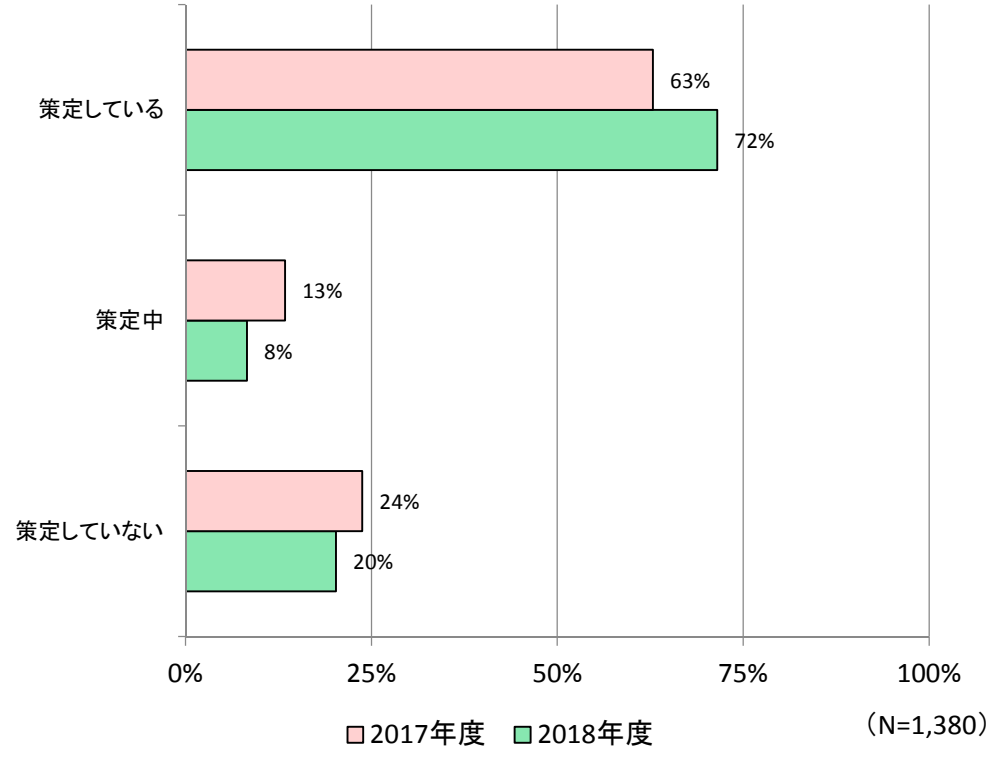


3.4. アンケート調査結果詳細 －（32/58）－

設問19 情報の取扱いに関する規定の策定状況

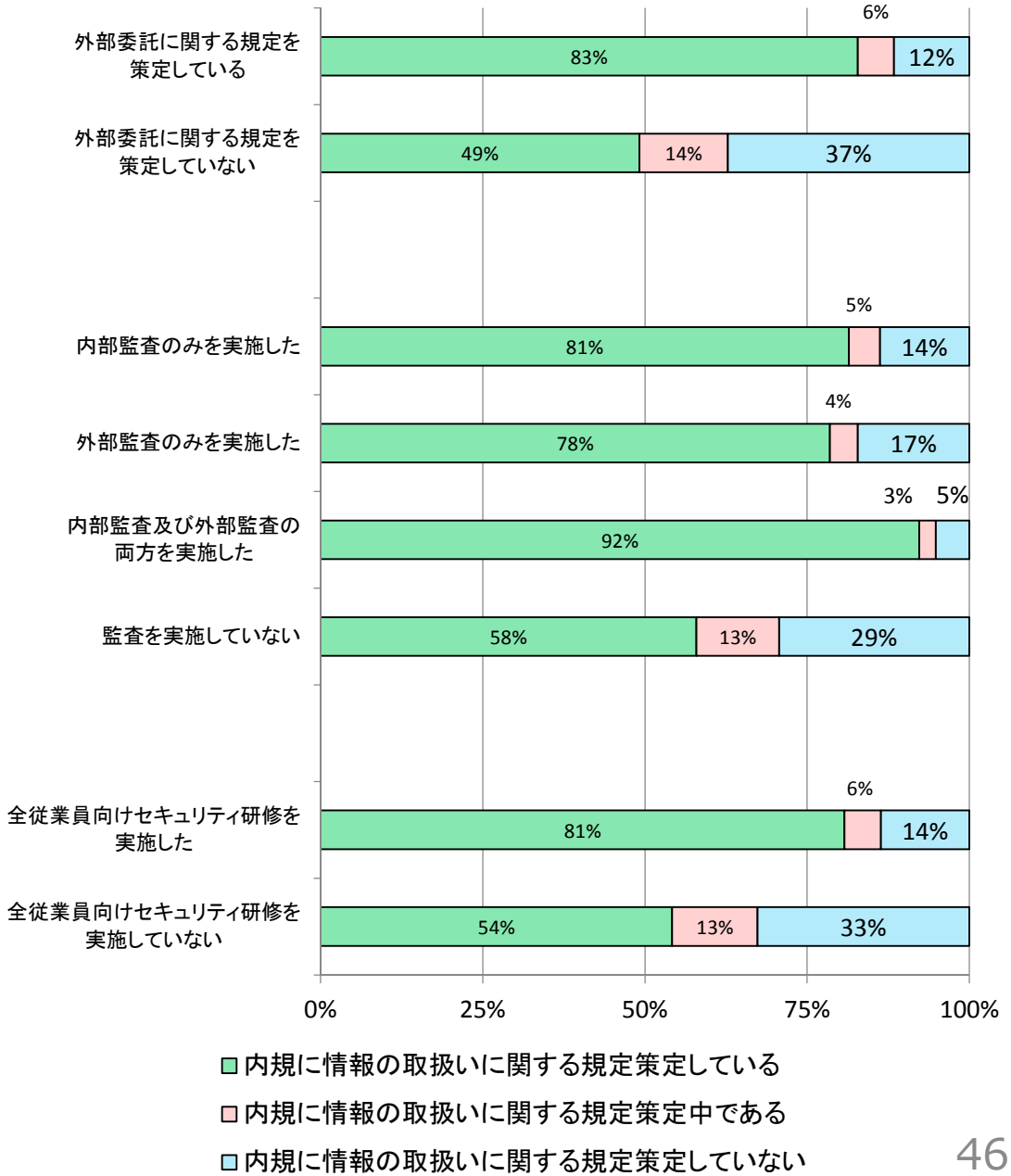
・情報の取扱いに関する規程を策定している事業者等は、外部委託に関する規程を策定している傾向がある。また、策定中の事業者等は、監査や従業員向けのセキュリティ研修（演習等）を実施していない傾向がある（参考①）。

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）

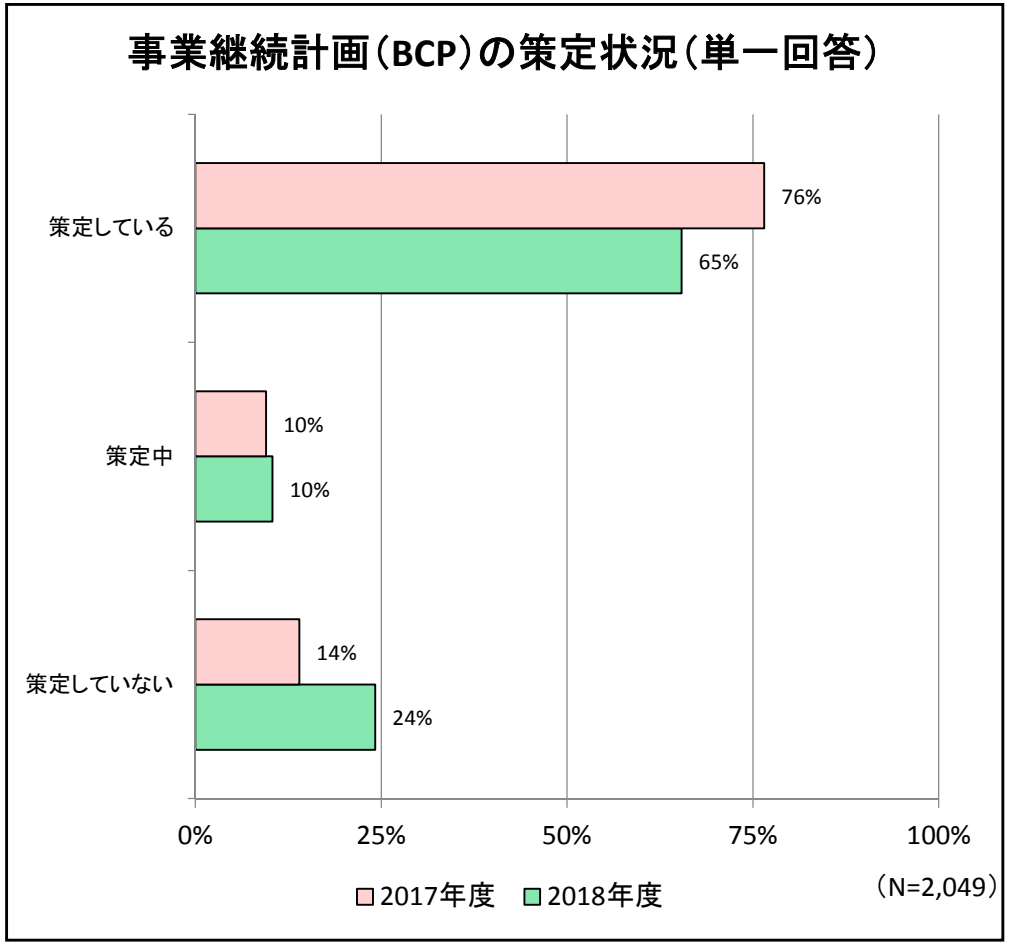
参考① 情報の取扱いに関する規定策定状況と各項目の関係性



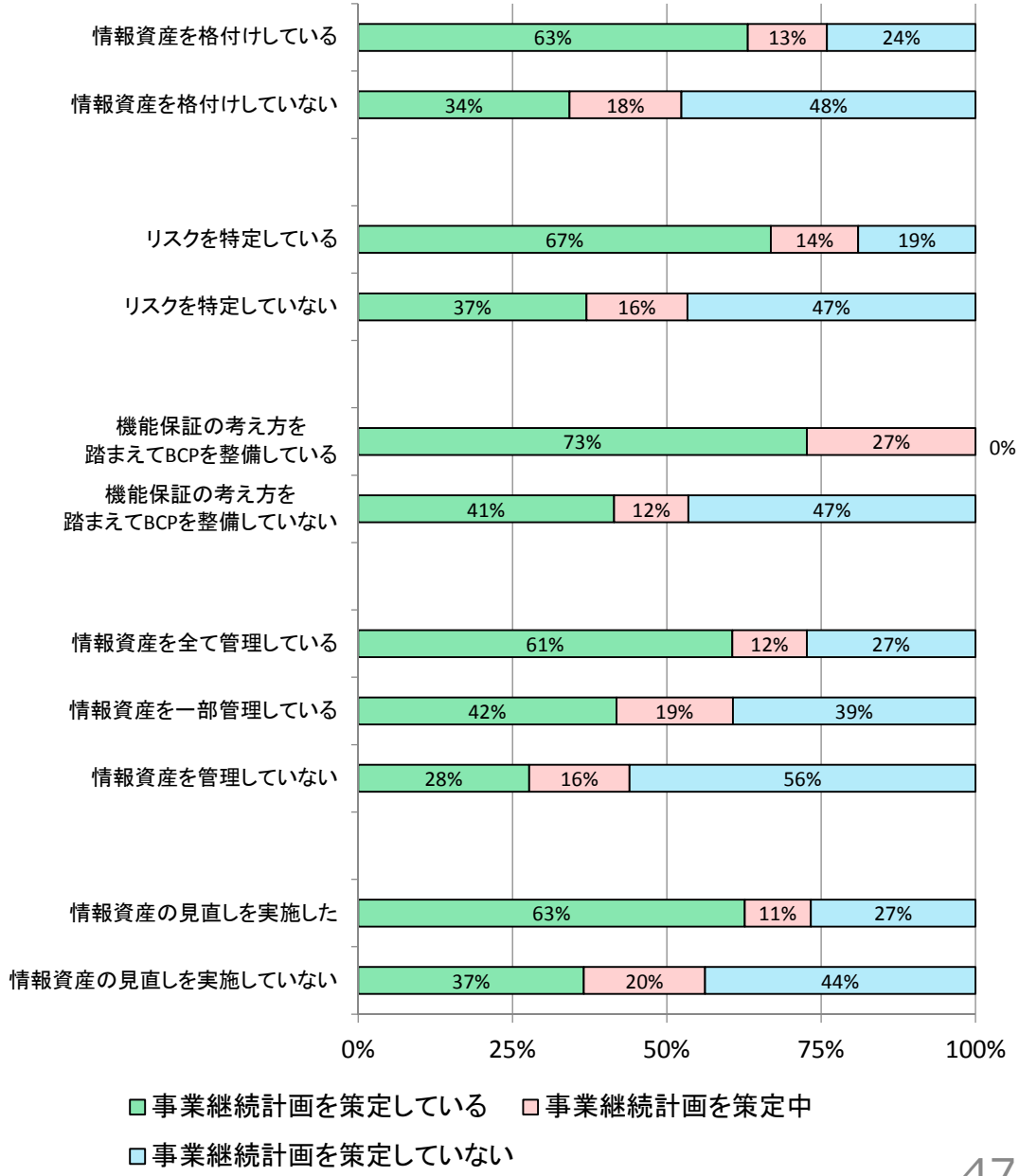
3.4. アンケート調査結果詳細 －（33/58）－

設問20　事業継続計画（BCP）の策定状況

・策定している事業者等は、情報資産の格付けやリスクの特定を実施している傾向がある。また、機能保証の考え方を踏まえて策定されている傾向がある（参考①）。



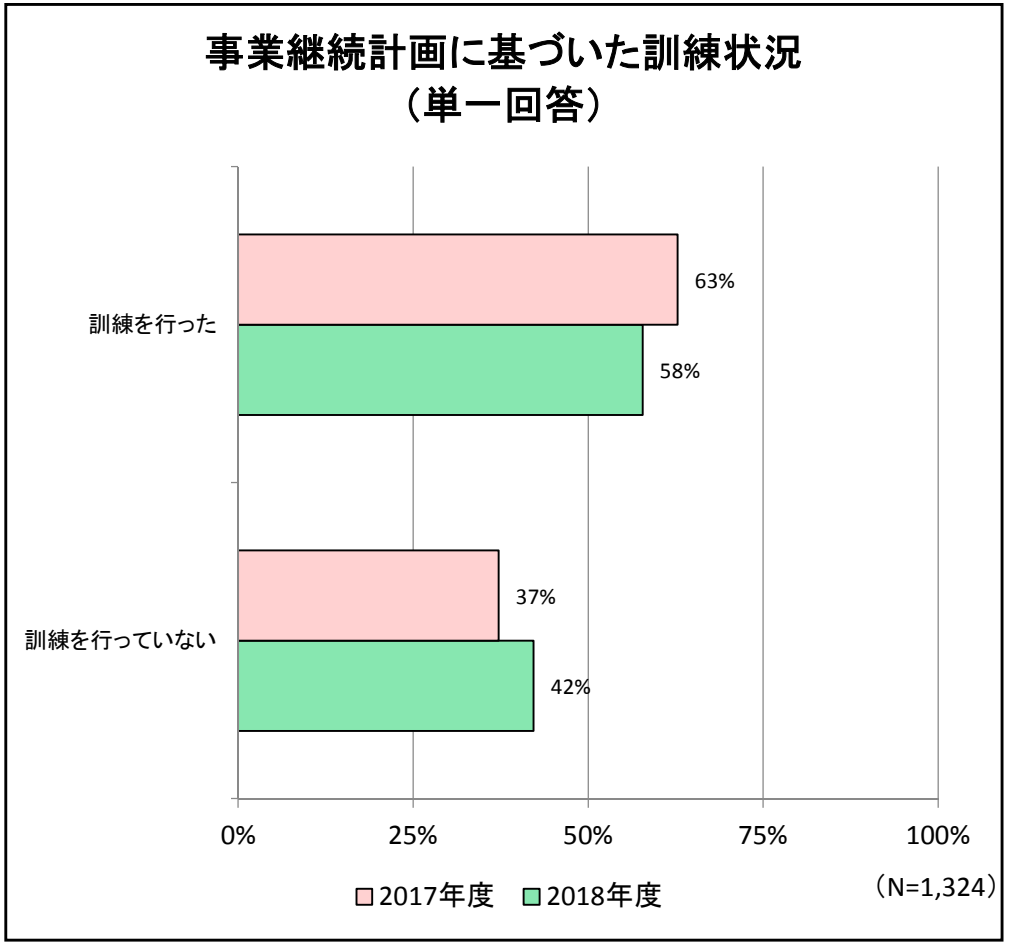
参考①　事業継続計画（BCP）の策定状況と各項目の関係性



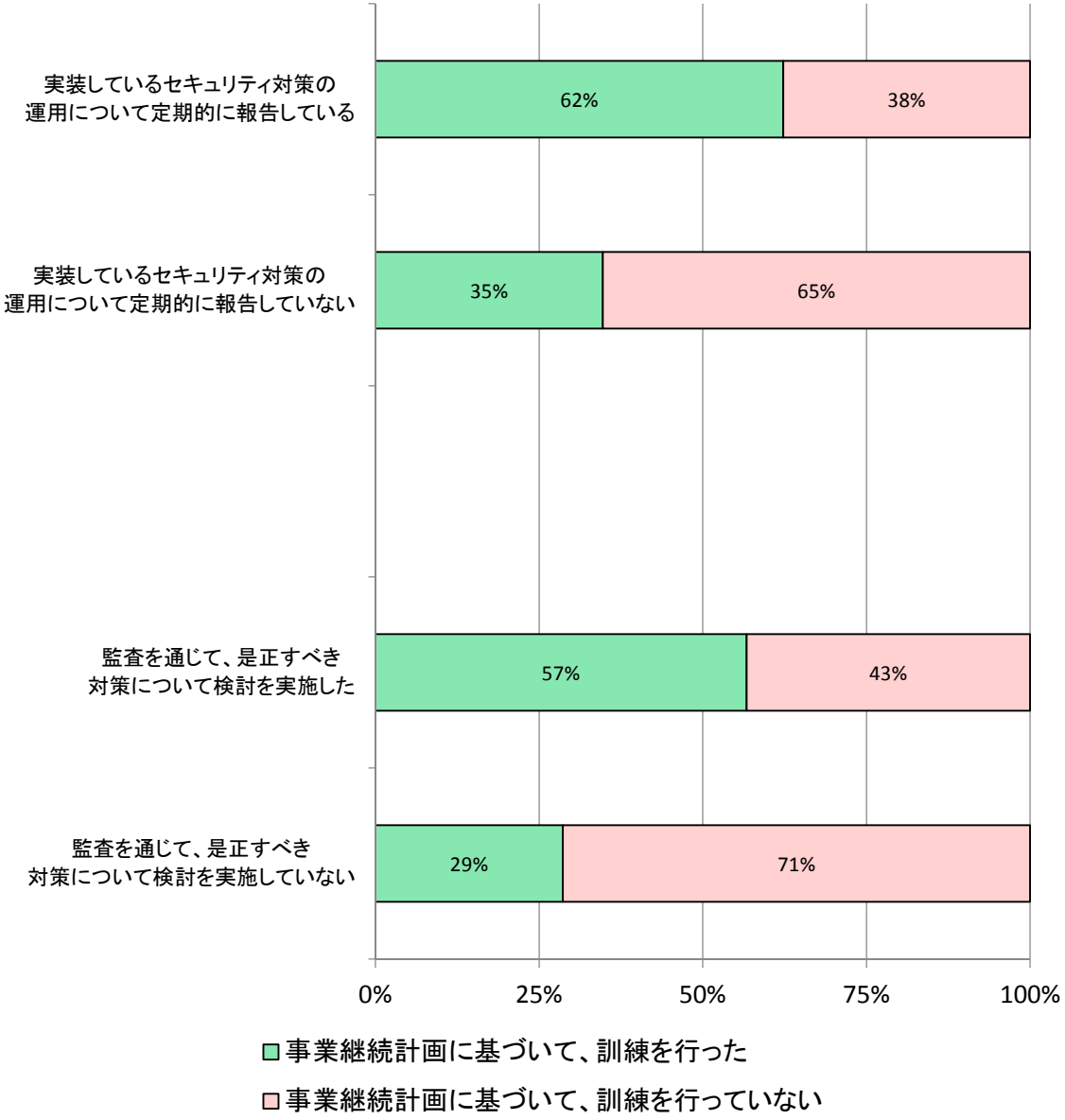
3.4. アンケート調査結果詳細 －（34/58）－

設問20-1　事業継続計画（BCP）に基づいた訓練状況

・訓練を行った事業者等は、運用状況を責任者に定期的に報告している傾向がある。また、監査を通じて是正すべき対策について検討している傾向がある（参考①）。



参考①　事業継続計画（BCP）に基づいた訓練状況と各項目の関係性

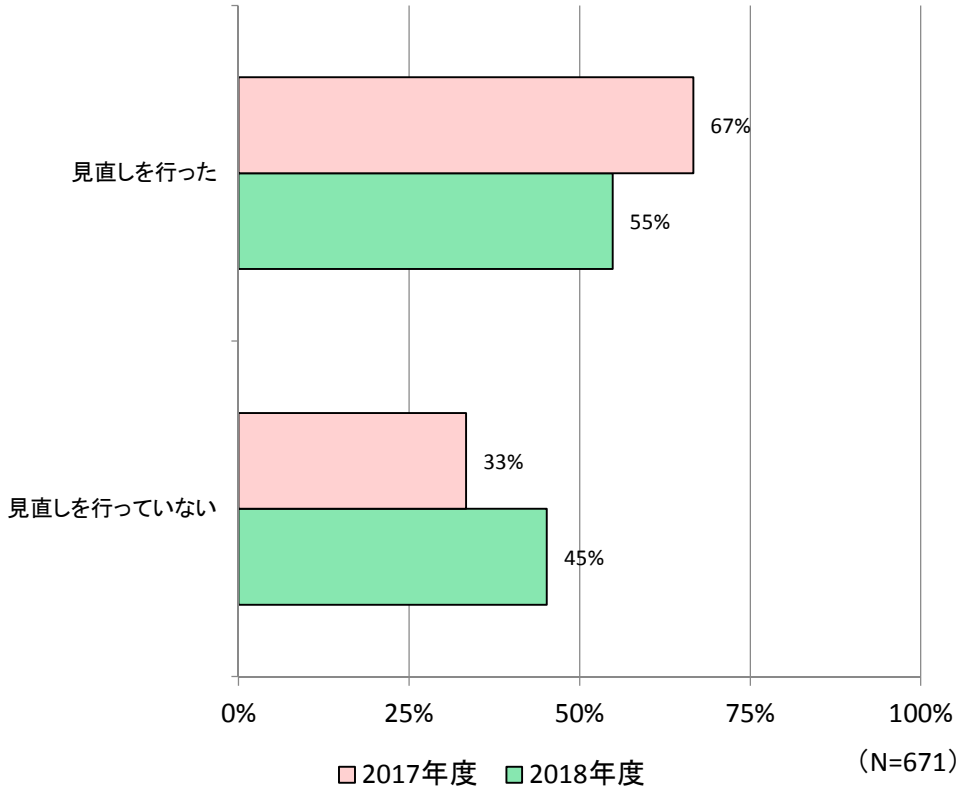


3.4. アンケート調査結果詳細 －（35/58）－

設問20-2 事業継続計画（BCP）の見直し状況

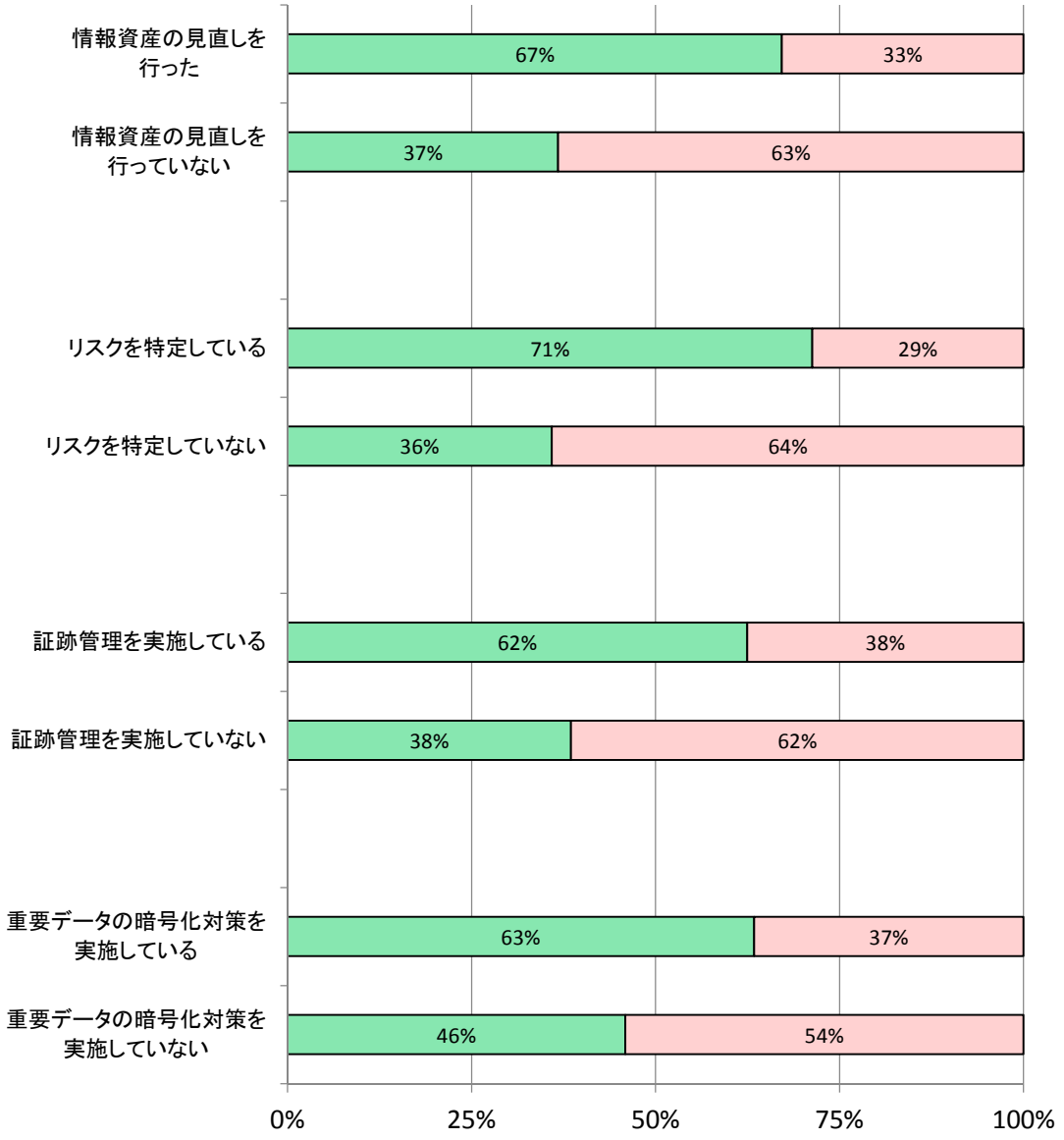
・事業継続計画（BCP）の見直しを行った事業者等は、情報資産の見直しを行っており、リスクの特定を実施している傾向がある。また、セキュリティ対策として、証跡管理や重要データの暗号化等の取組みがされている（参考①）。

事業継続計画（BCP）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）

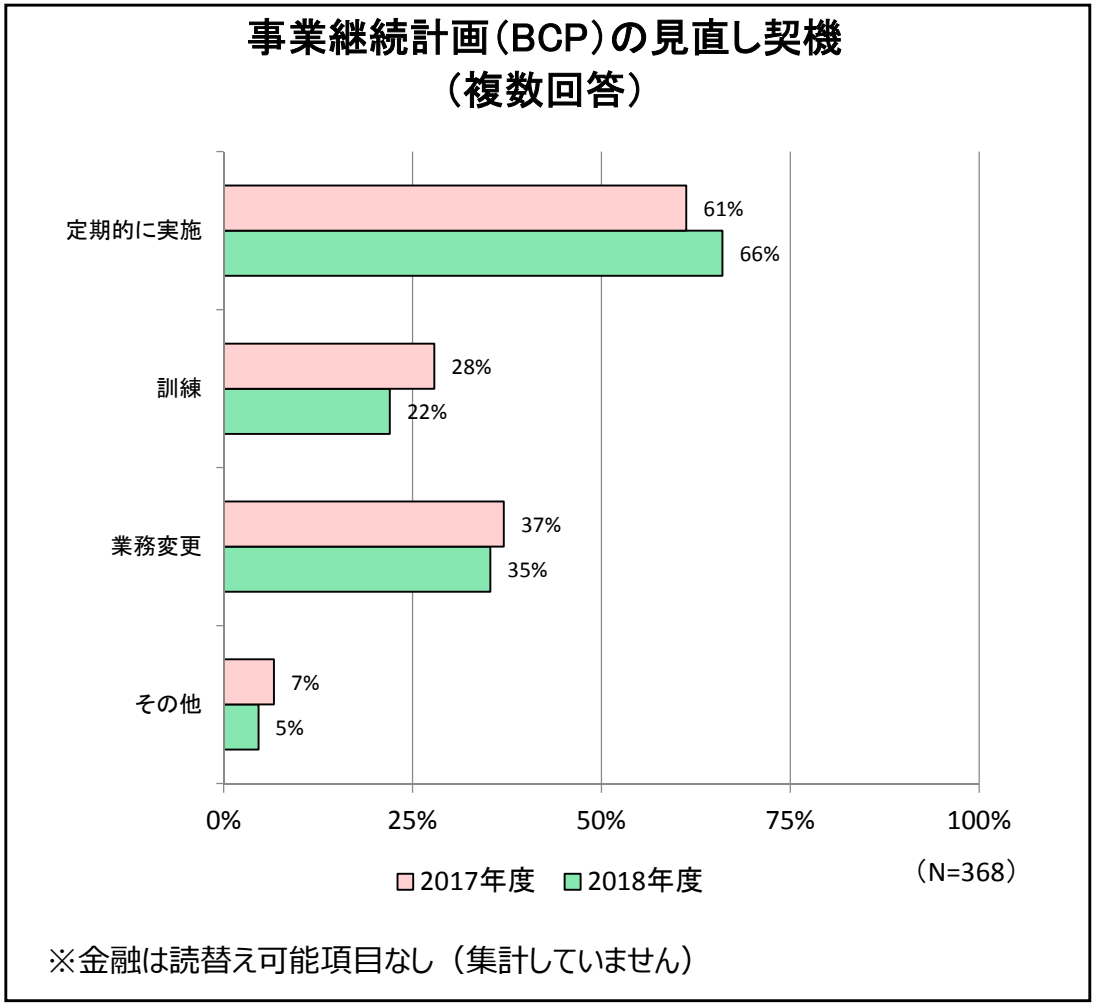
参考① 事業継続計画（BCP）の見直し状況と各項目の関係



3.4. アンケート調査結果詳細 －（36/58）－

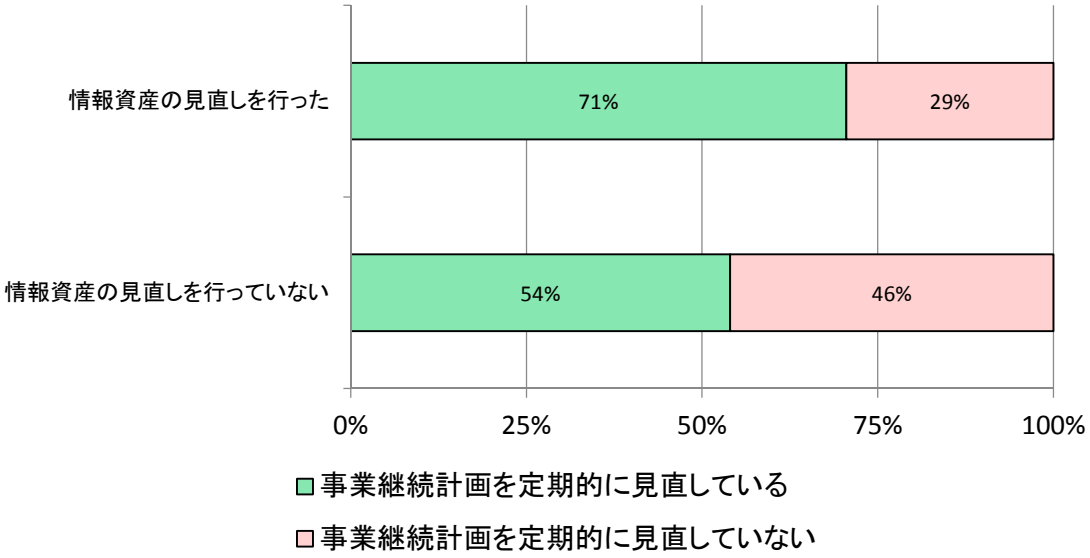
設問20-3 事業継続計画（BCP）の見直し契機

・定期的に事業継続計画（BCP）を見直しを実施している事業者等は、情報資産の見直しやリスクの特定を実施している傾向がある（参考①）。
・訓練を契機に事業継続計画（BCP）を見直している事業者等は、経営層にリスクアセスメントの結果を報告している傾向がある（参考②）。

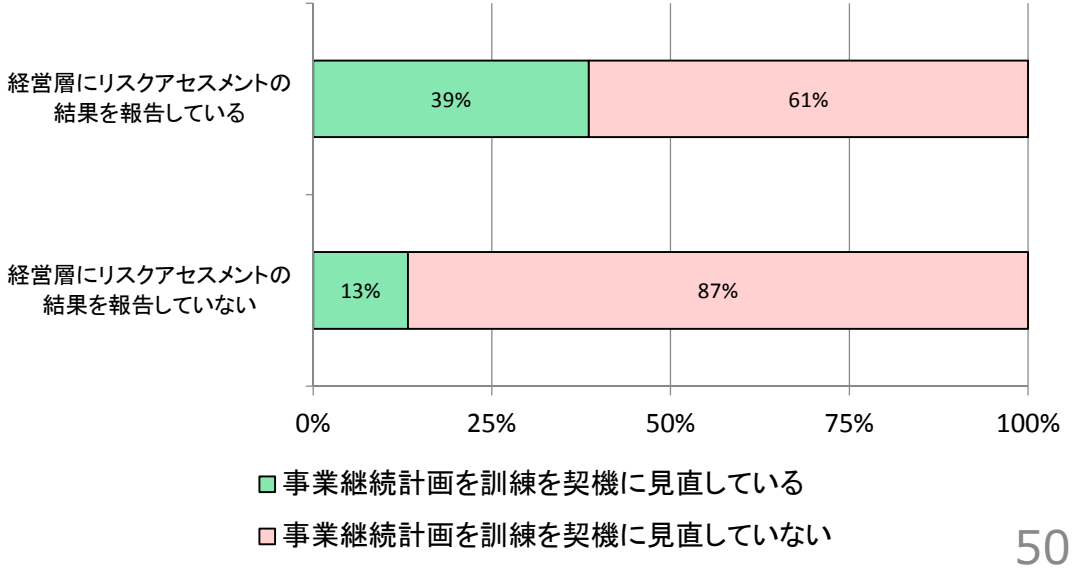


※金融は読替え可能項目なし（集計していません）

参考① 事業継続計画（BCP）の定期見直しと情報資産の見直しの関係



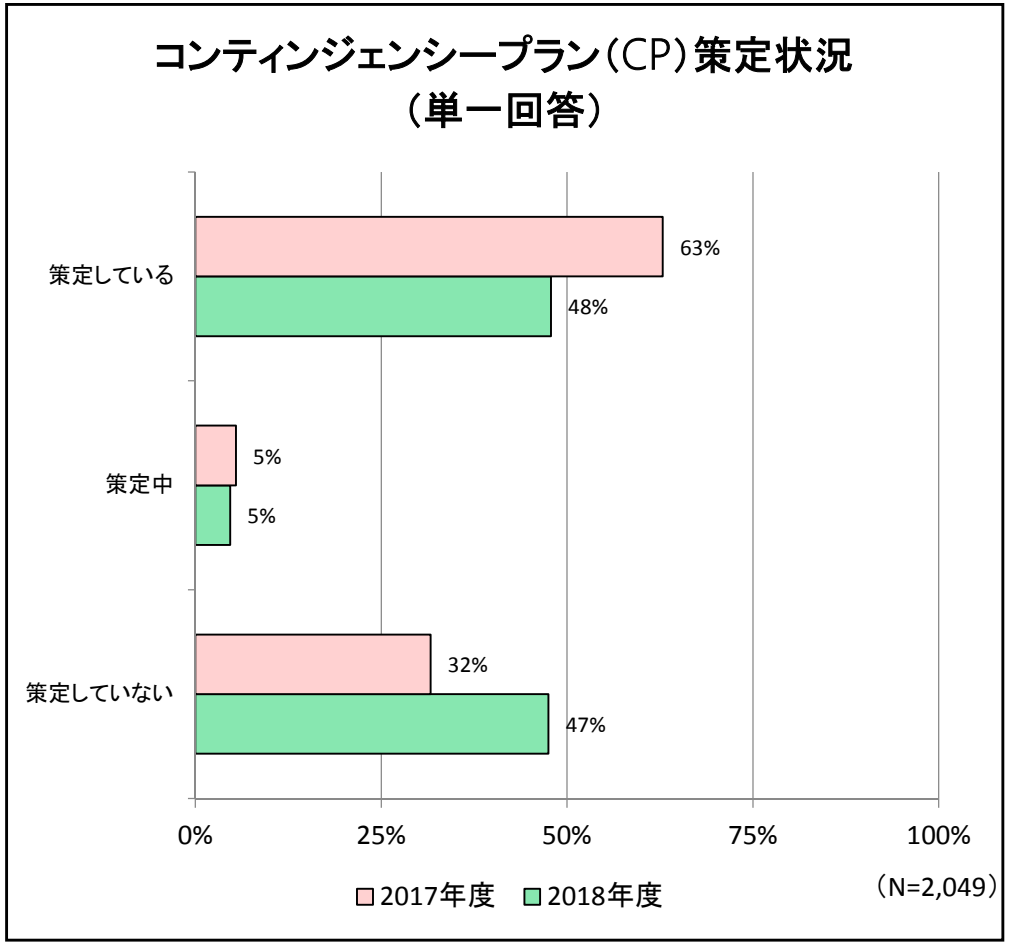
参考② 事業継続計画（BCP）の訓練ごとの見直しと経営層への報告の関係性



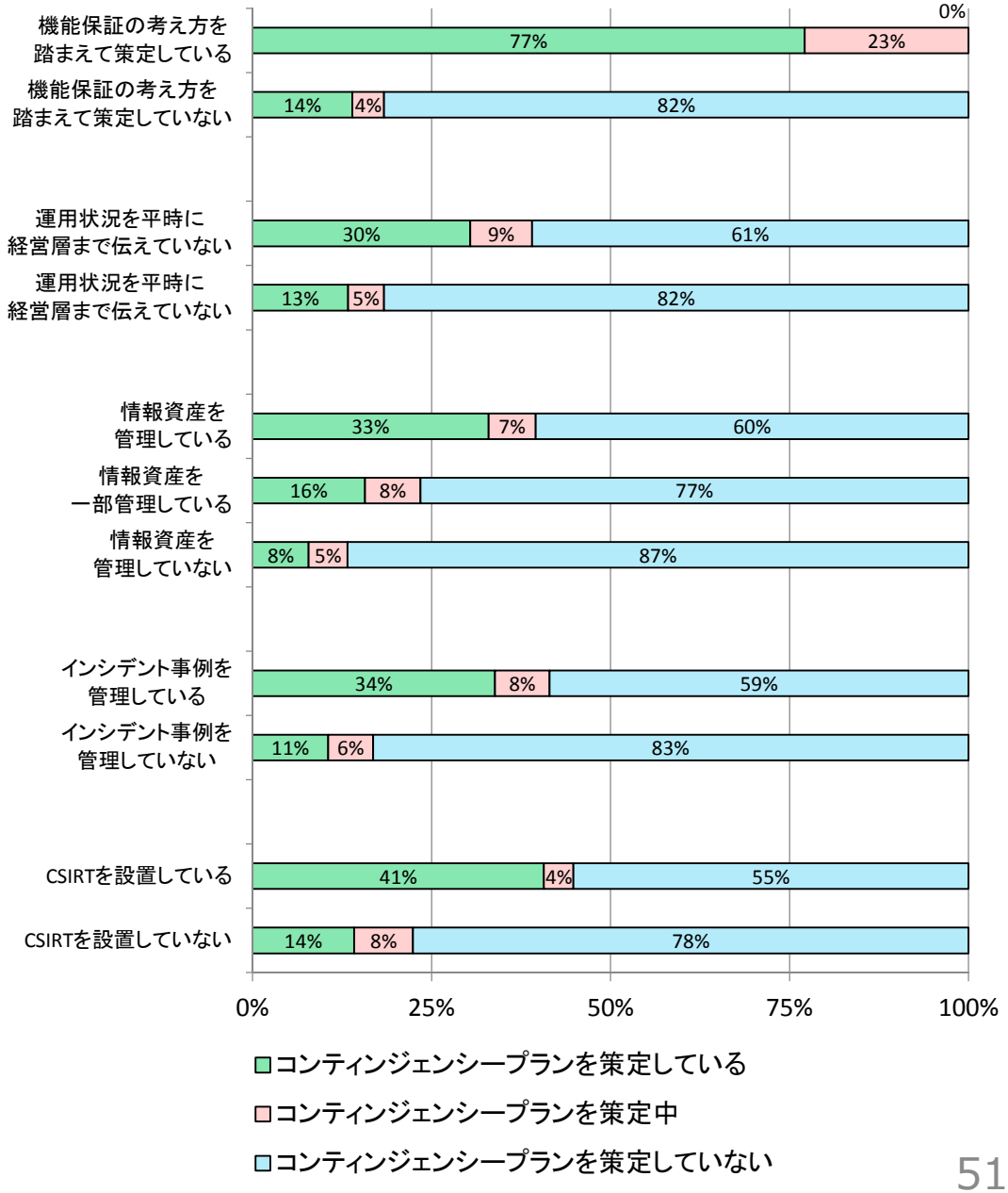
3.4. アンケート調査結果詳細 －（37/58）－

設問21 コンティンジェンシープラン（CP）策定状況

・コンティンジェンシープラン（CP）を策定している事業者等は、機能保証の考え方を踏まえた上で策定されている事業者等が多い。さらに、経営層まで状況報告されている事業者等も多い。また、コンティンジェンシープラン（CP）を策定している事業者等は、情報資産・インシデントを管理し、CSIRTが設置されている傾向がある（参考①）。



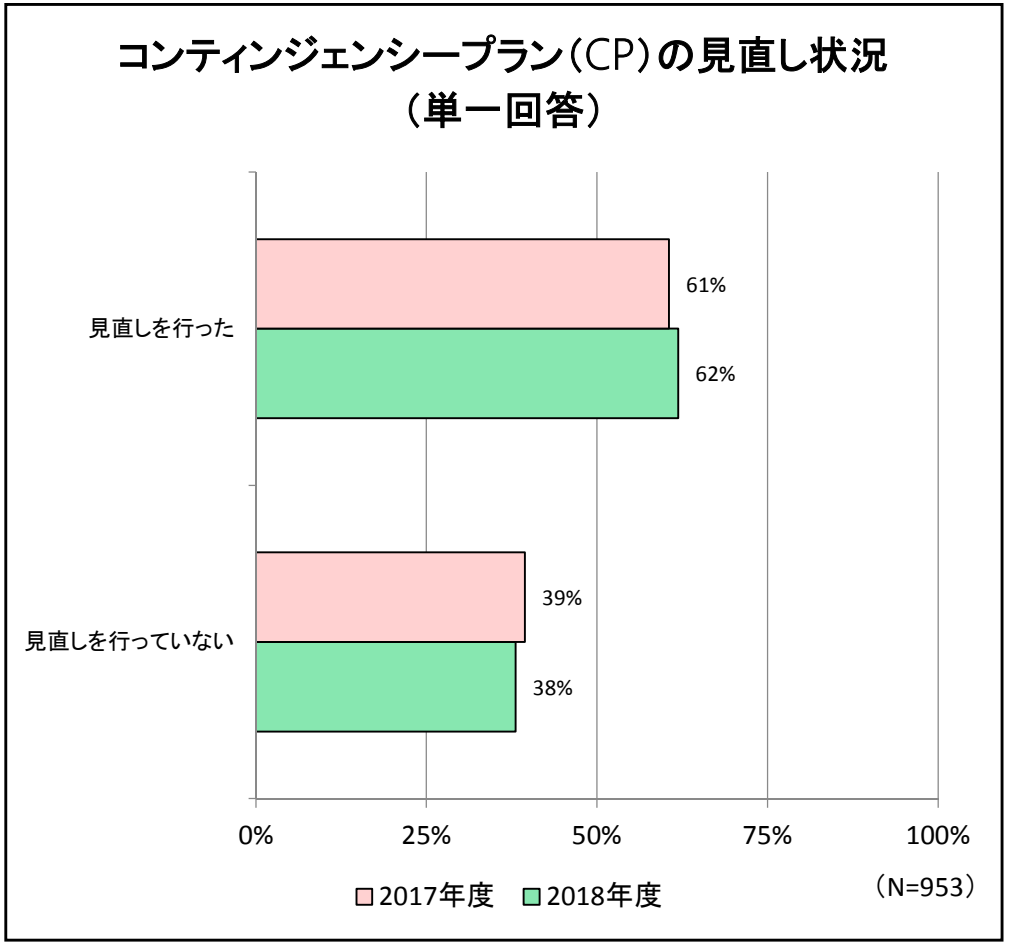
参考① コンティンジェンシープランの策定状況と各項目の関係性



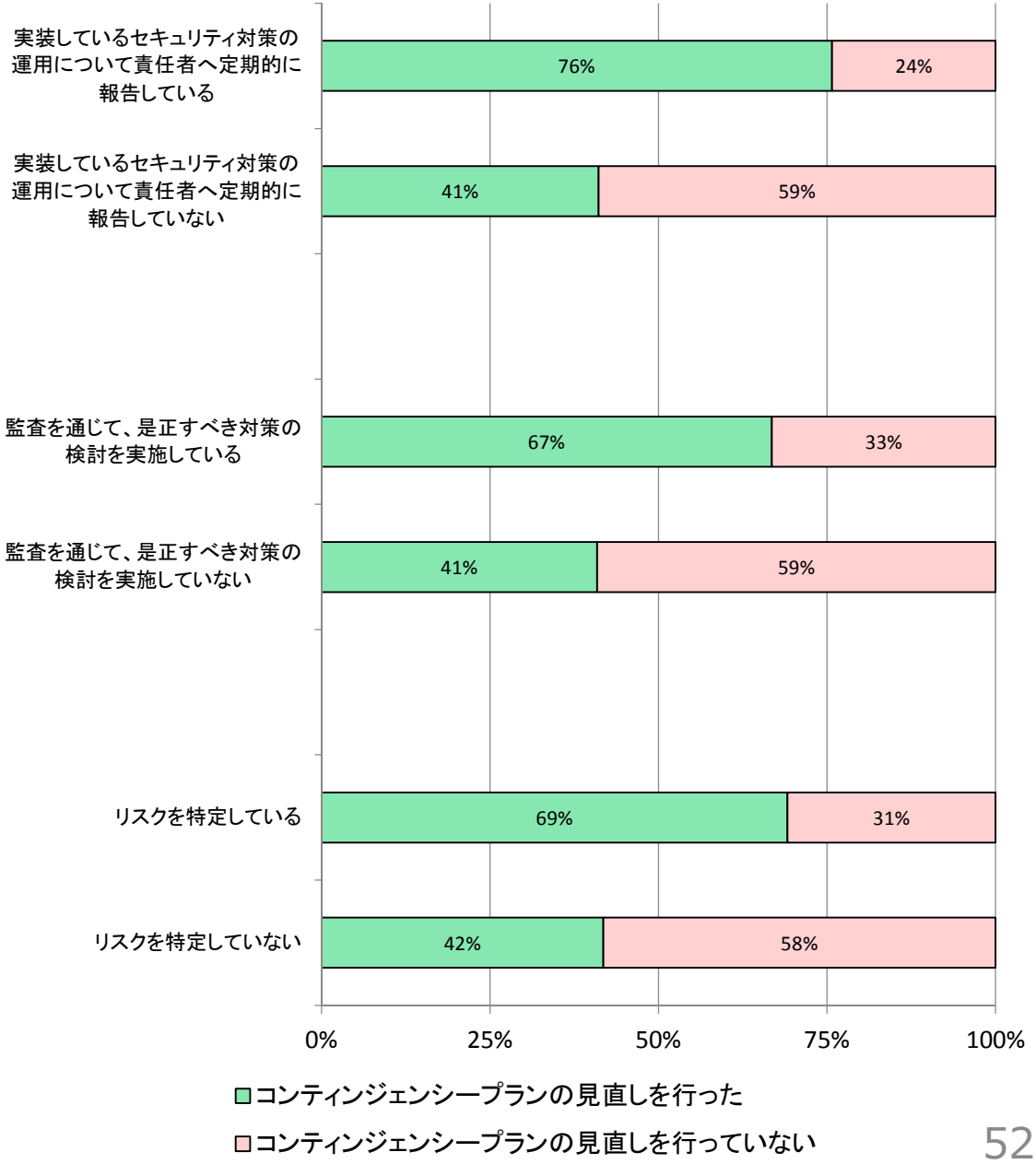
3.4. アンケート調査結果詳細 －（38/58）－

設問21-1 コンティンジェンシープラン（CP）の見直し状況

・コンティンジェンシープラン（CP）の見直しを行っている事業者等は、責任者に定期的に報告を行い、監査を通じて是正すべき対策を検討している傾向がある。また、コンティンジェンシープラン（CP）の見直すべき項目を検討するために、リスクの特定を実施していることが多い（参考① ）。



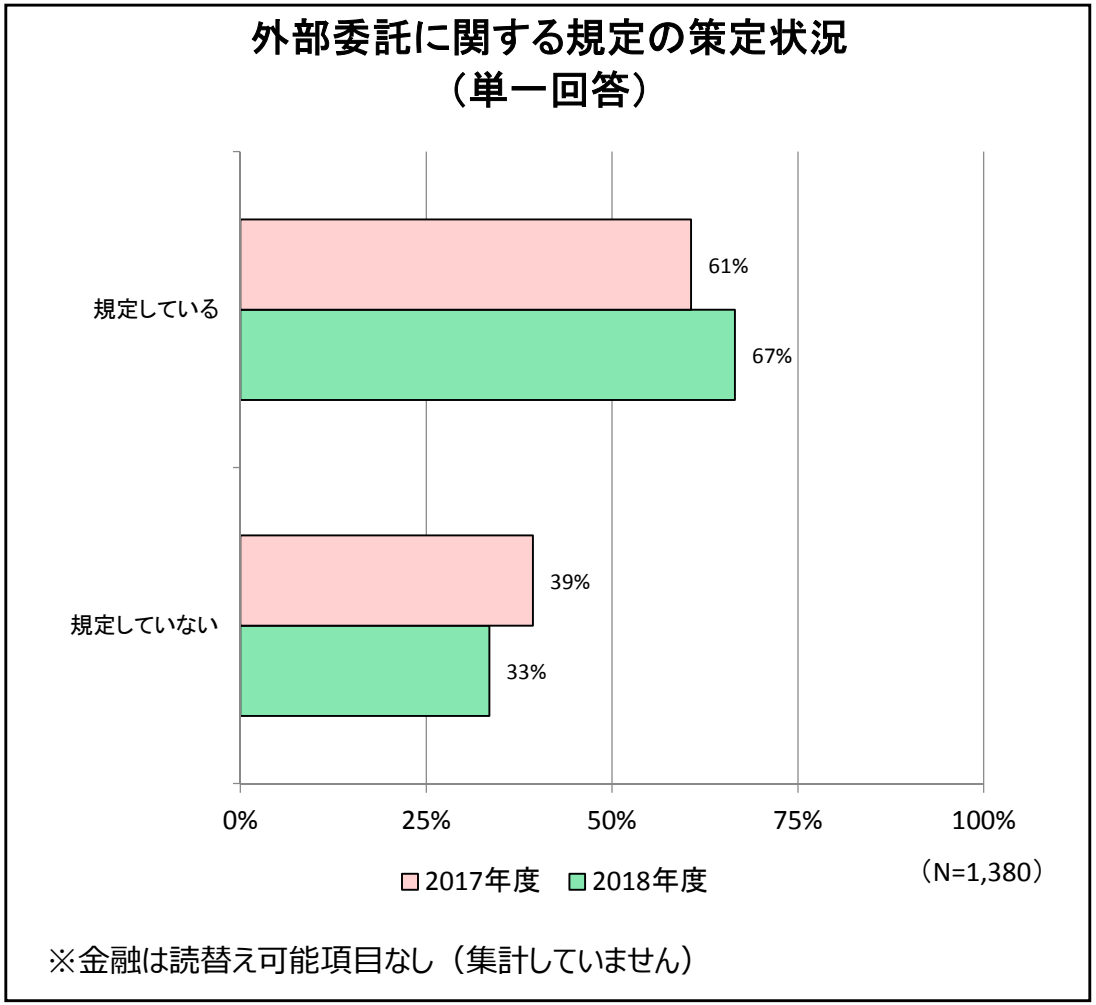
参考① コンティンジェンシープラン（CP）の見直し状況と各項目の関係性



3.4. アンケート調査結果詳細 －（39/58）－

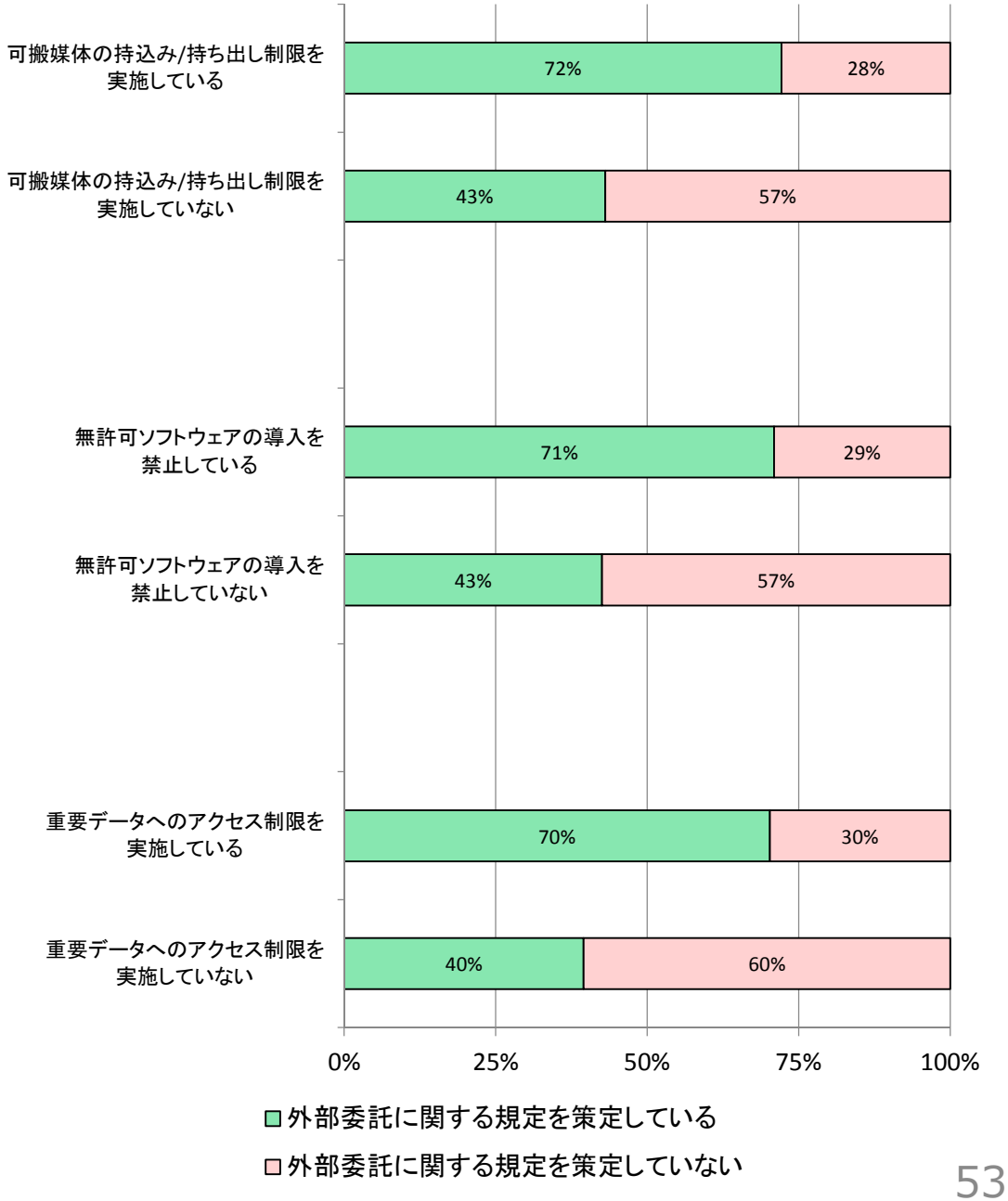
設問22 外部委託に関する規定の策定状況

・外部委託に関する規程を策定している事業者等は、可搬媒体の持込持ち出し制限を実施していたり、無許可ソフトウェアの導入を禁止していたり、重要データのアクセス制限を行っている傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

参考① 外部委託に関する規定の策定状況と各項目の関係性

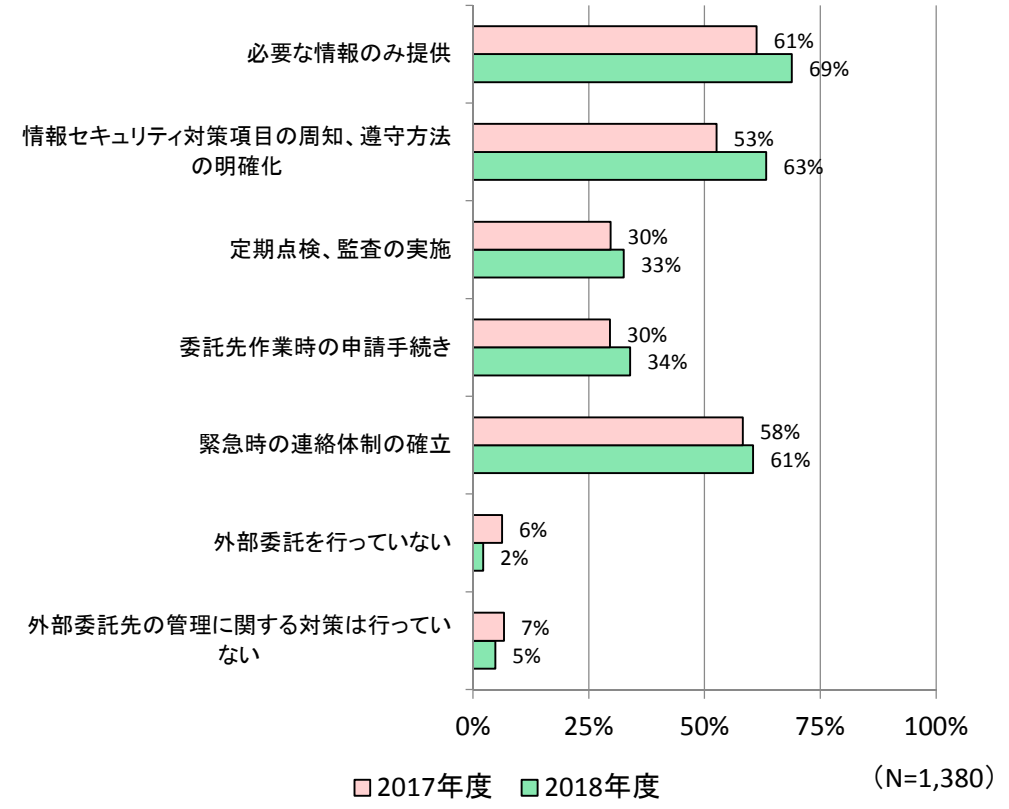


3.4. アンケート調査結果詳細 －（40/58）－

設問23 外部委託先管理に関する対策

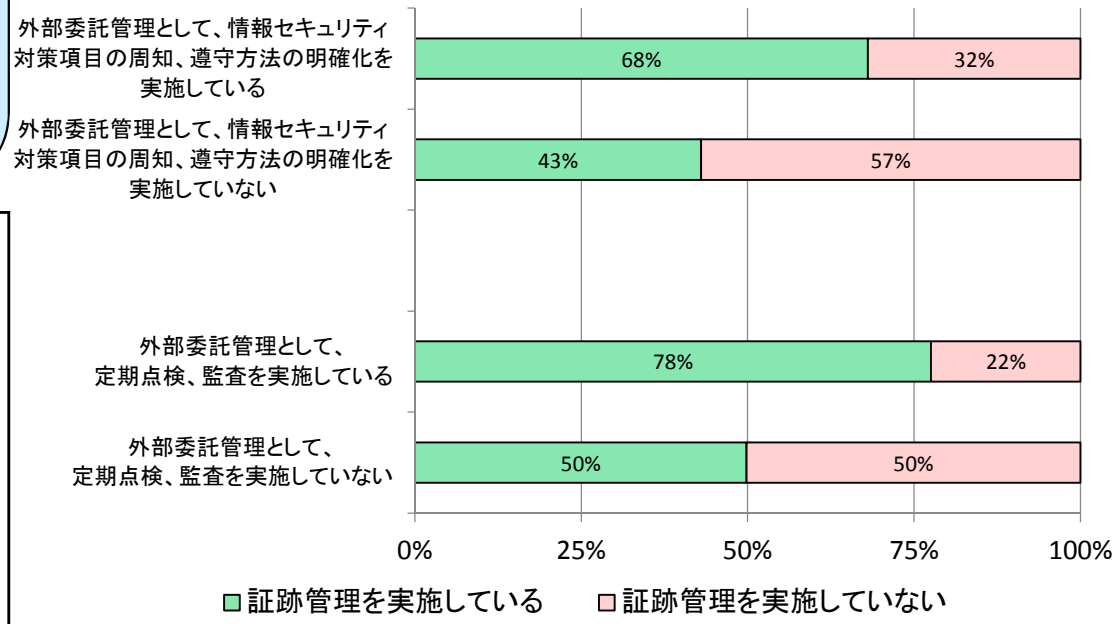
・証跡管理を行っている事業者は「対策項目の周知や定期点検・監査」を実施している傾向がある（参考①）。
・自事業者等も内部及び外部監査を実施している事業者は、外部委託先事業者等の定期点検・監査も実施している傾向がある（参考②）。

外部委託先管理に関する対策（複数回答）

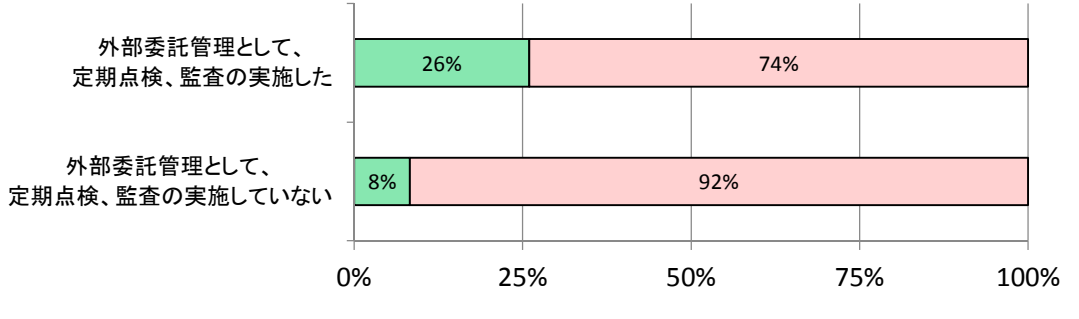


※金融は読替え可能項目なし（集計していません）

参考① 外部委託先管理に関する対策と証跡管理実施の関係性



参考② 外部委託先管理に関する対策と監査実施の関係性

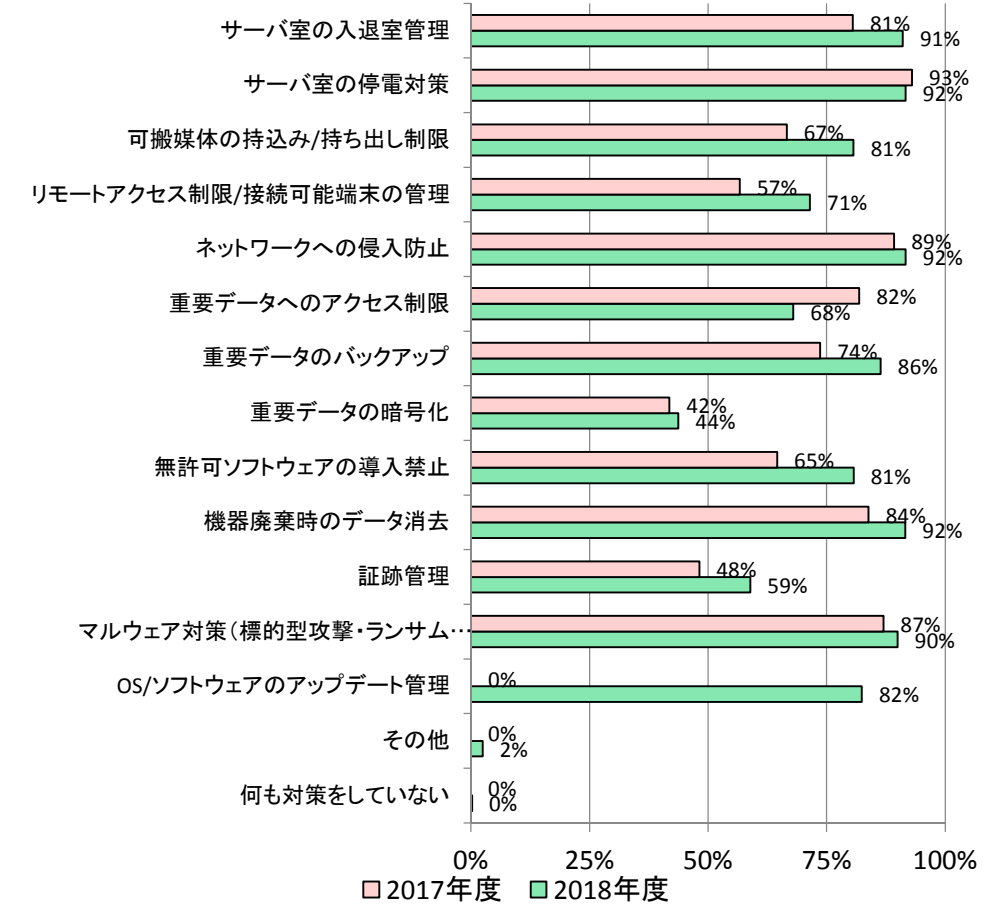


3.4. アンケート調査結果詳細 －（41/58）－

設問24　実施済みの情報セキュリティ対策

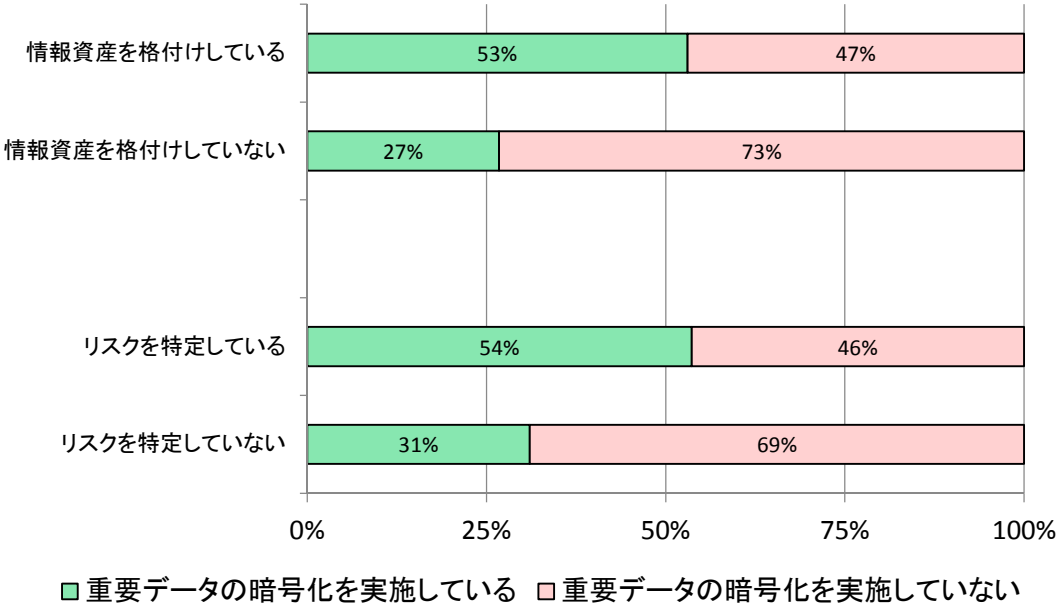
・重要データの暗号化を実施している事業者等は、情報資産の格付けを実施し、リスクの特定を行っている傾向がある（参考①）。
・証跡管理を行っている事業者等は、コンティンジェンシープラン（CP）を策定している傾向がある（参考②）。

実施済みの情報セキュリティ対策（複数回答）

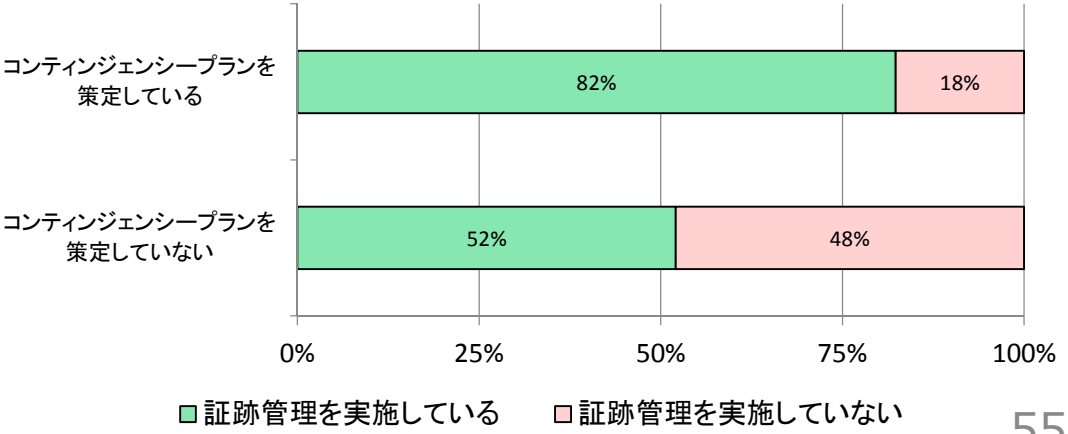


※一部選択肢において、金融は読替え可能項目なし（集計していません）
※OS/ソフトウェアのアップデート管理は、2018年度から調査開始　（N=2,031）

参考①　情報セキュリティ対策の実施状況と重要データ暗号化実施の関係性



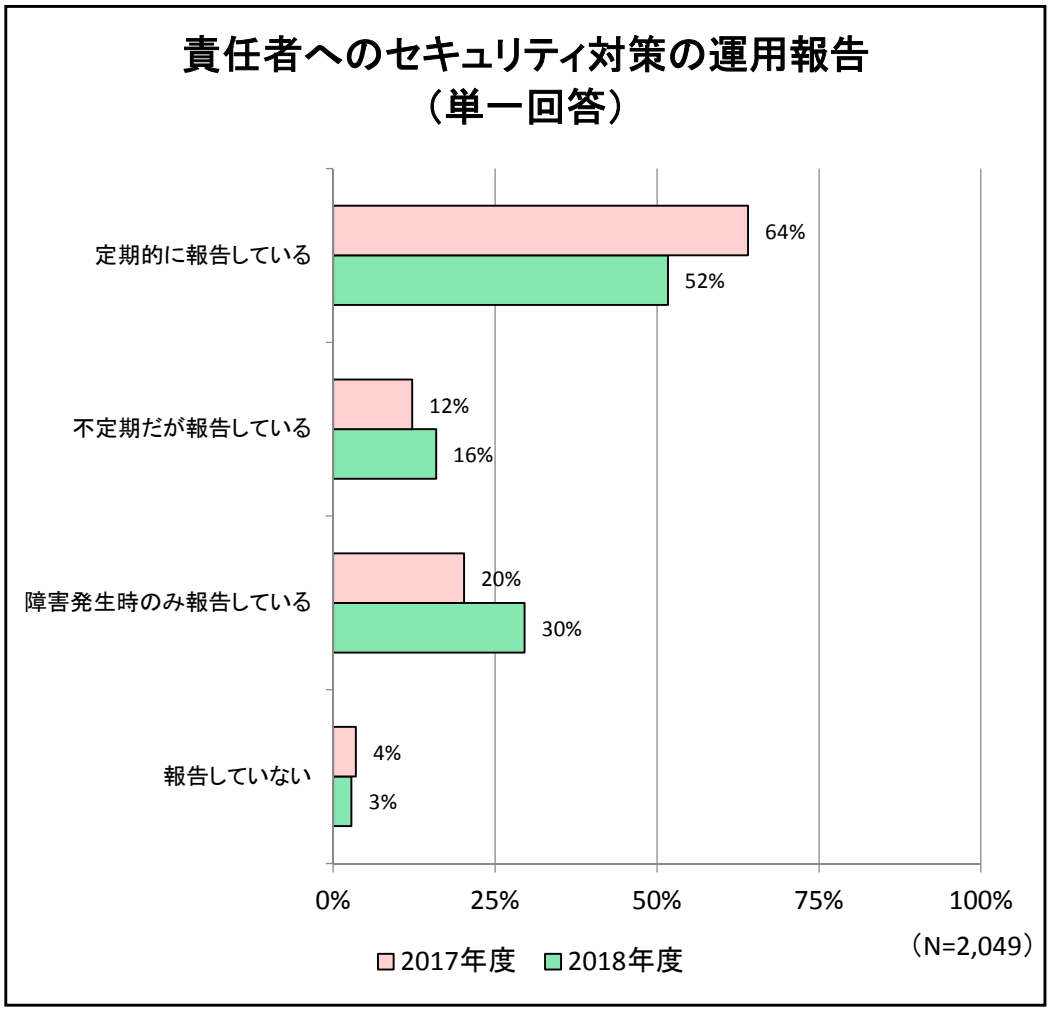
参考②　コンテンジェンシープラン（CP）策定状況と証跡管理実施の関係性



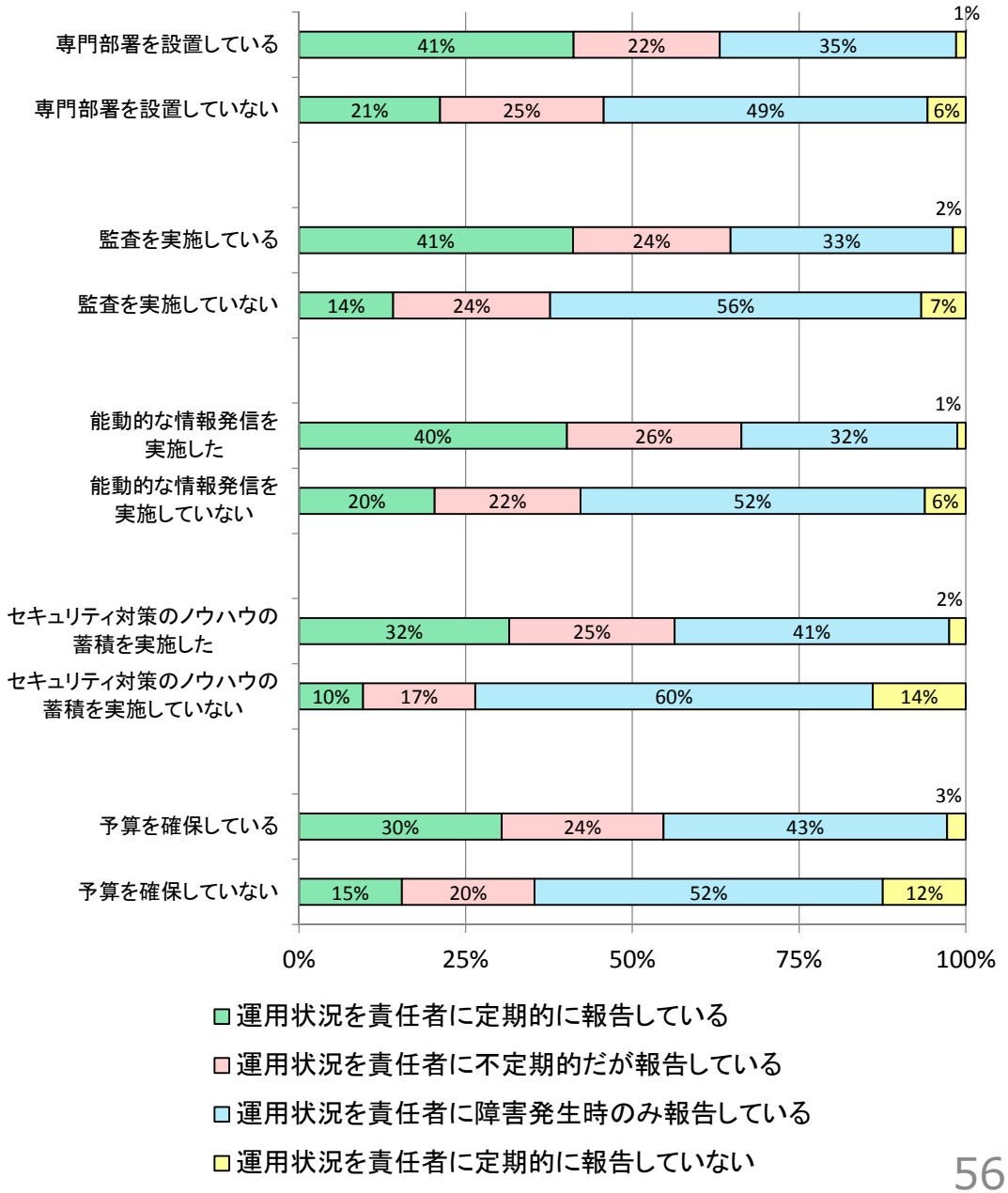
3.4. アンケート調査結果詳細 －（42/58）－

設問25　責任者へのセキュリティ対策の運用報告

・セキュリティ対策を実施する専門部署を設置している事業者等は、定期的に運用報告を行っている傾向がある（参考①）。
・障害発生時のみ責任者へ報告している事業者等は、監査を実施しておらず、能動的な情報提供を行っていない傾向がある（参考②）。



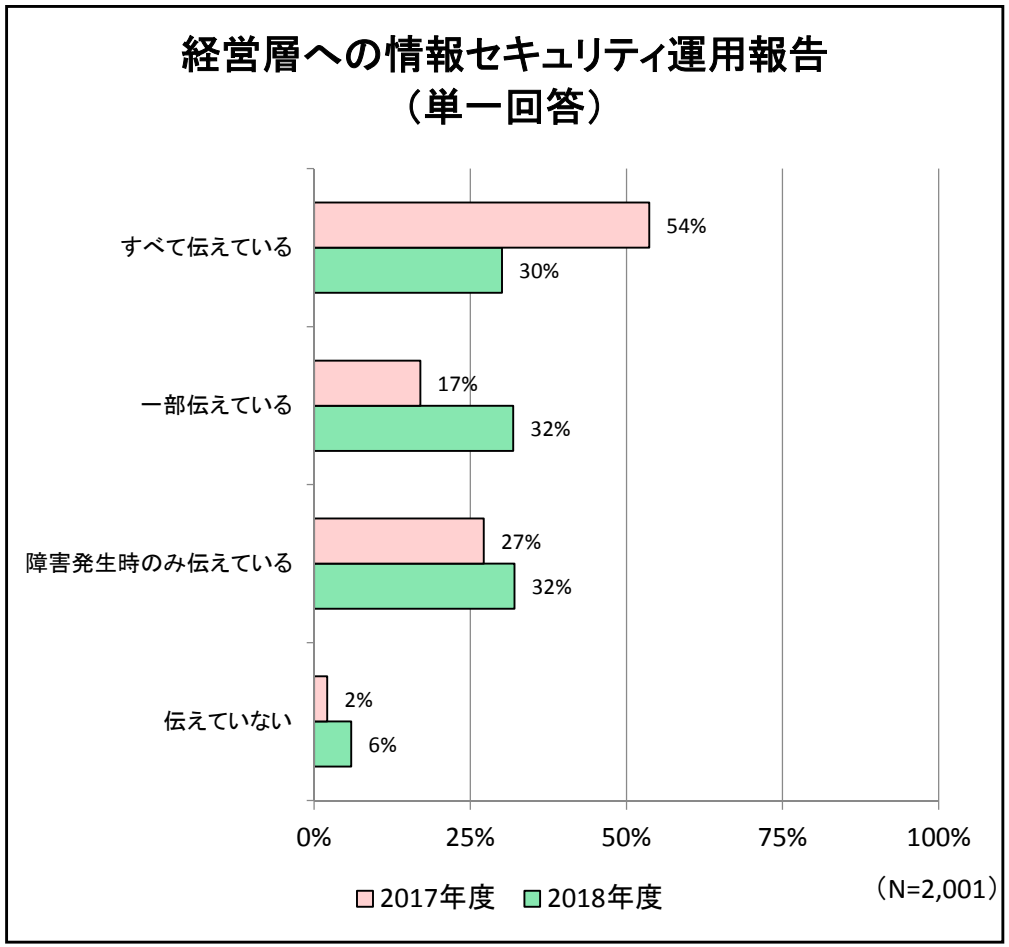
参考①　責任者へのセキュリティ対策の運用報告と各項目との関係性



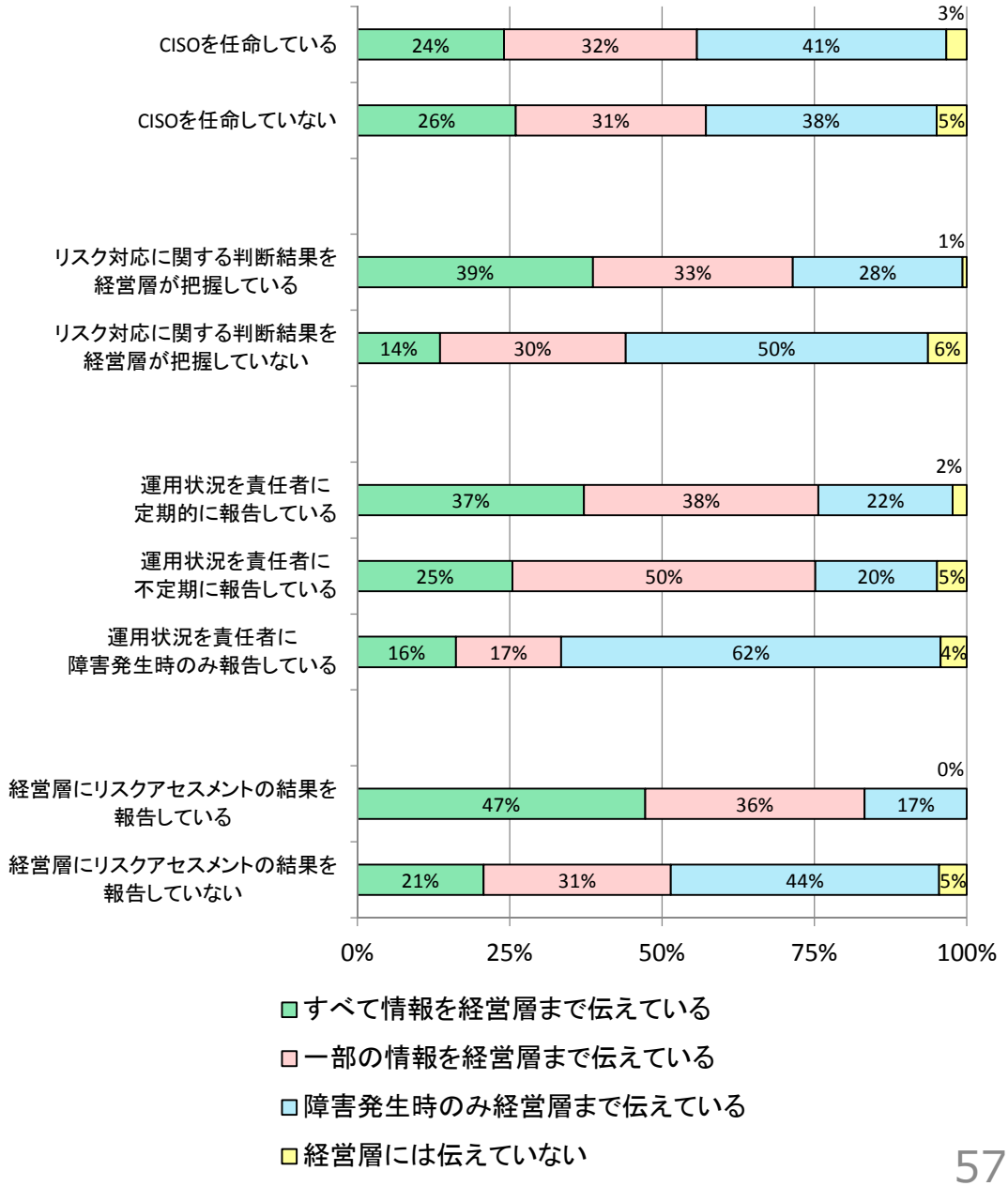
3.4. アンケート調査結果詳細 －（43/58）－

設問25-1　経営層への情報セキュリティ運用報告

・責任者に定期的に情報セキュリティ報告を行っている事業者等は、経営層にも定期的に情報を報告している傾向がある（参考①）。
・経営層に報告している事業者等はリスクアセスメントの結果についても、経営層に報告を行っている傾向がある（参考②）。



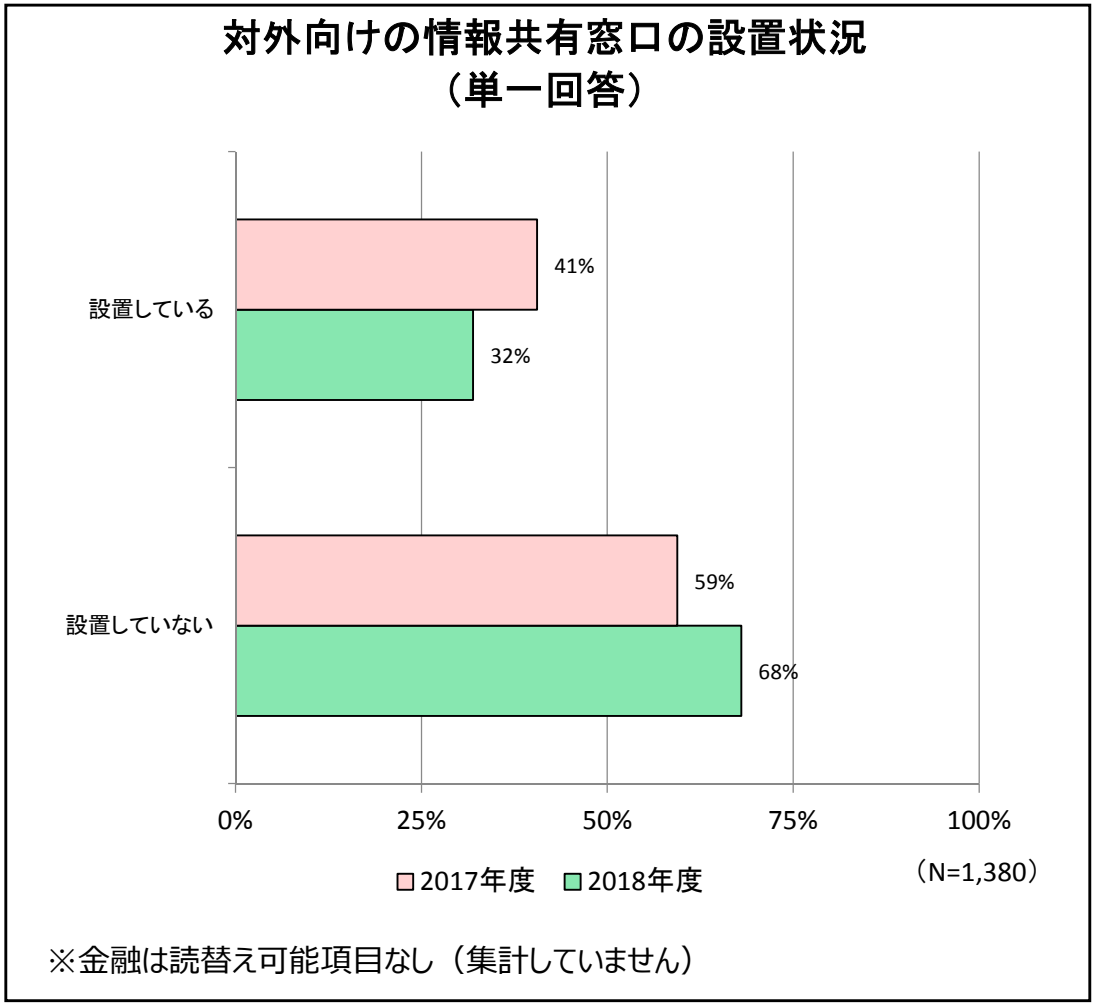
参考①　経営層への報告状況と各項目の関係性



3.4. アンケート調査結果詳細 －（44/58）－

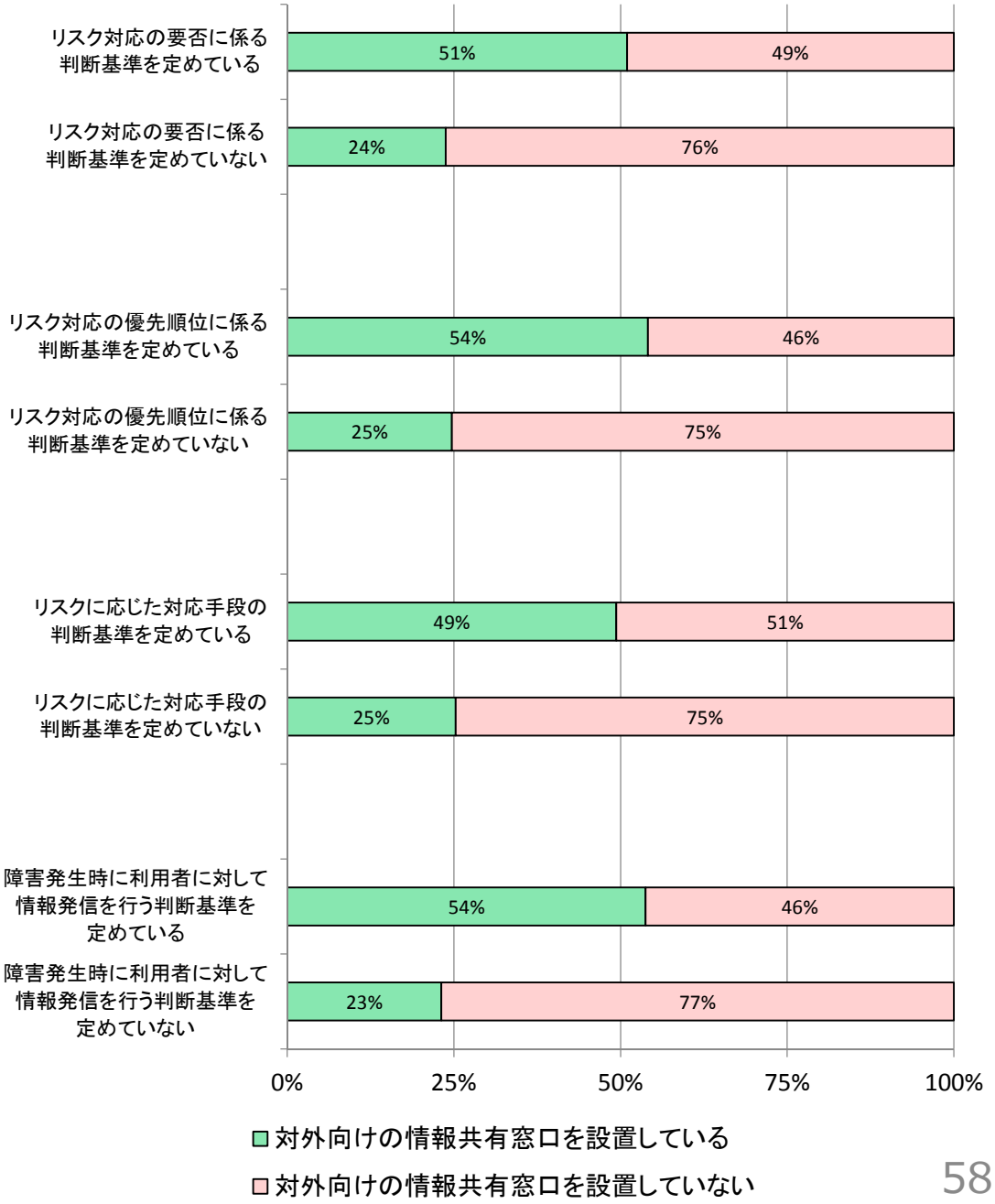
設問26　対外向けの情報共有窓口の設置状況

・対外向けの情報共有窓口を設置している事業者等は、リスク対応の優先順位に係る判断基準、対応要否に係る判断基準、リスクに応じた対応手段の判断基準が決められているだけではなく、障害発生時のサービス利用者への情報発信に関する基準も定めている傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

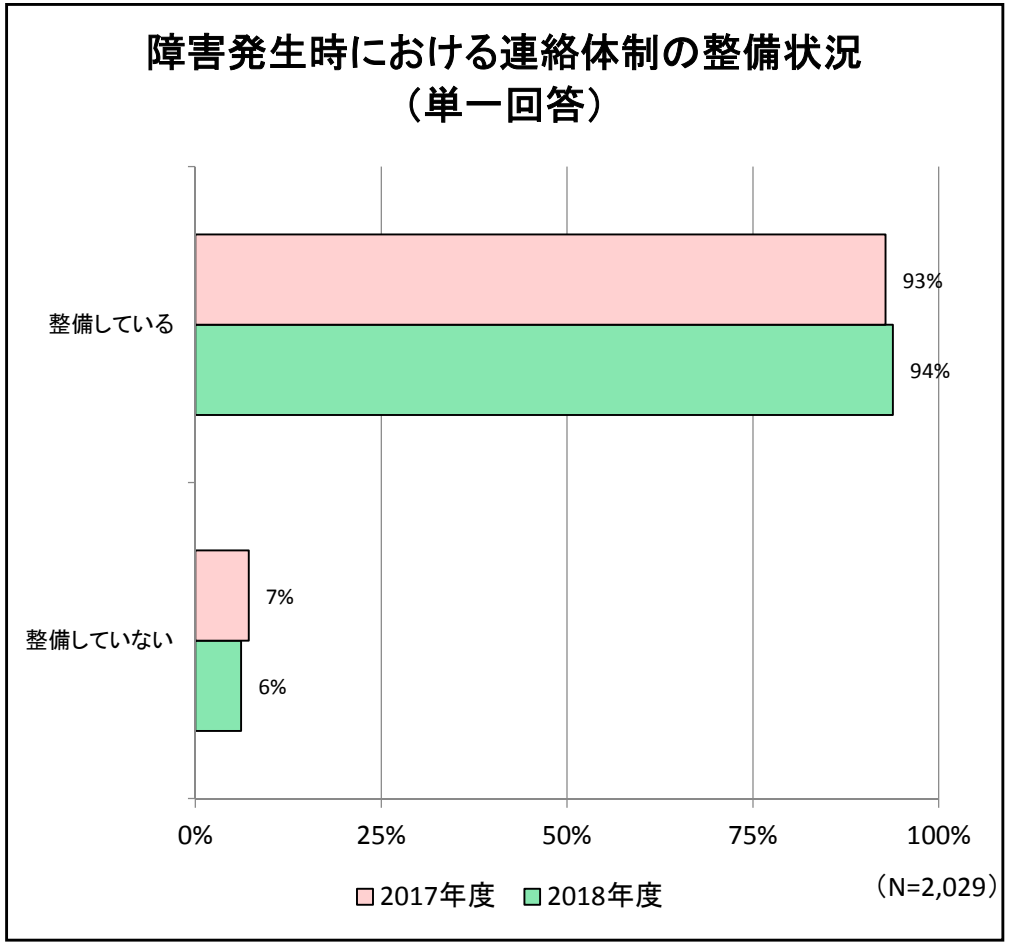
参考①　対外向け情報窓口の設置状況と各項目の関係性



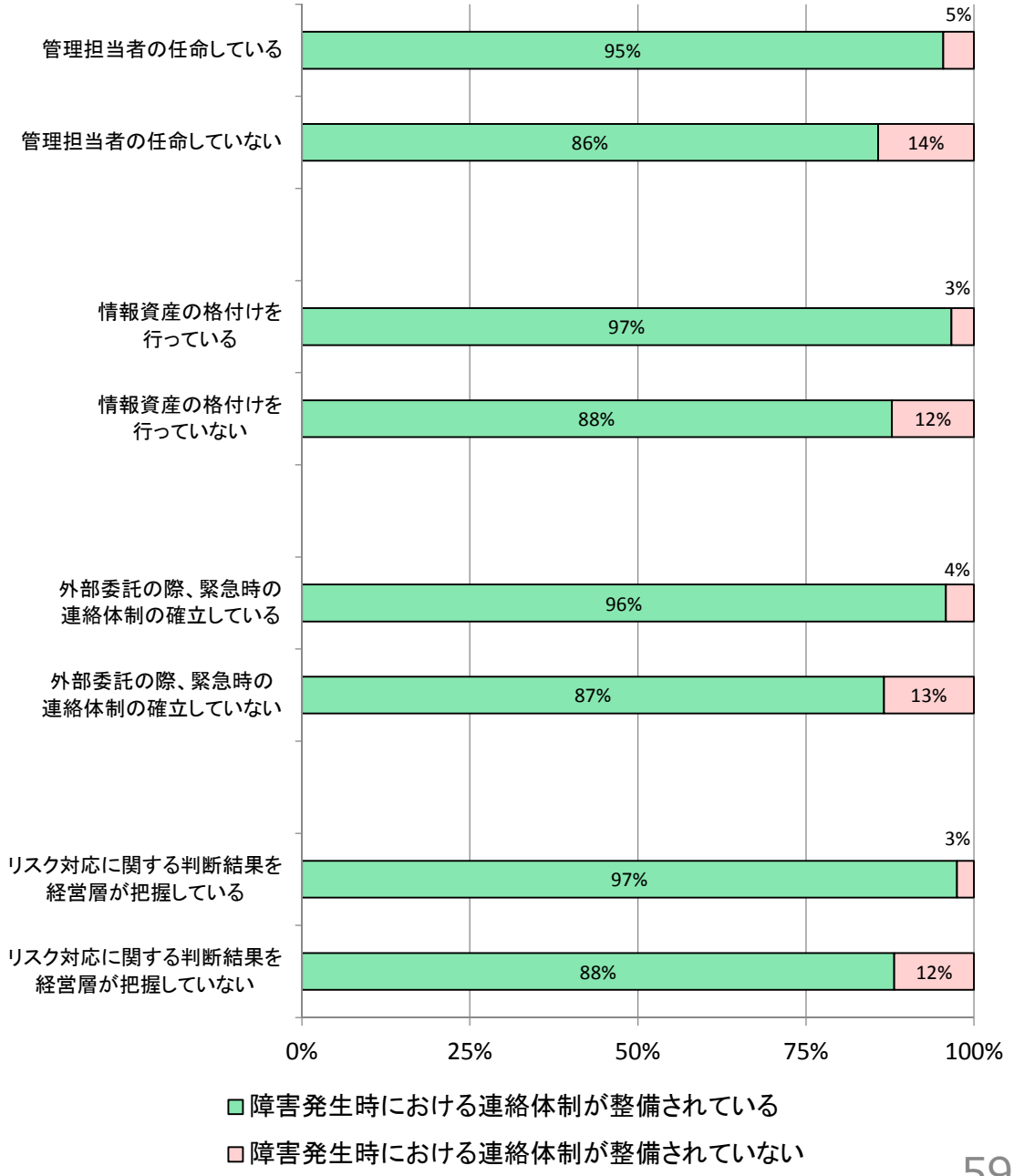
3.4. アンケート調査結果詳細 －（45/58）－

設問27　障害発生時における連絡体制の整備状況

・障害発生時における連絡体制を整備している事業者等は、情報セキュリティの管理担当者を任命しており、情報資産の格付けを実施し、外部委託の際に緊急連絡の体制を整備して、経営層にリスク対応に関する判断結果が共有されている傾向がある（参考①）。



参考①　障害発生時の連絡体制整備状況と各項目の関係性

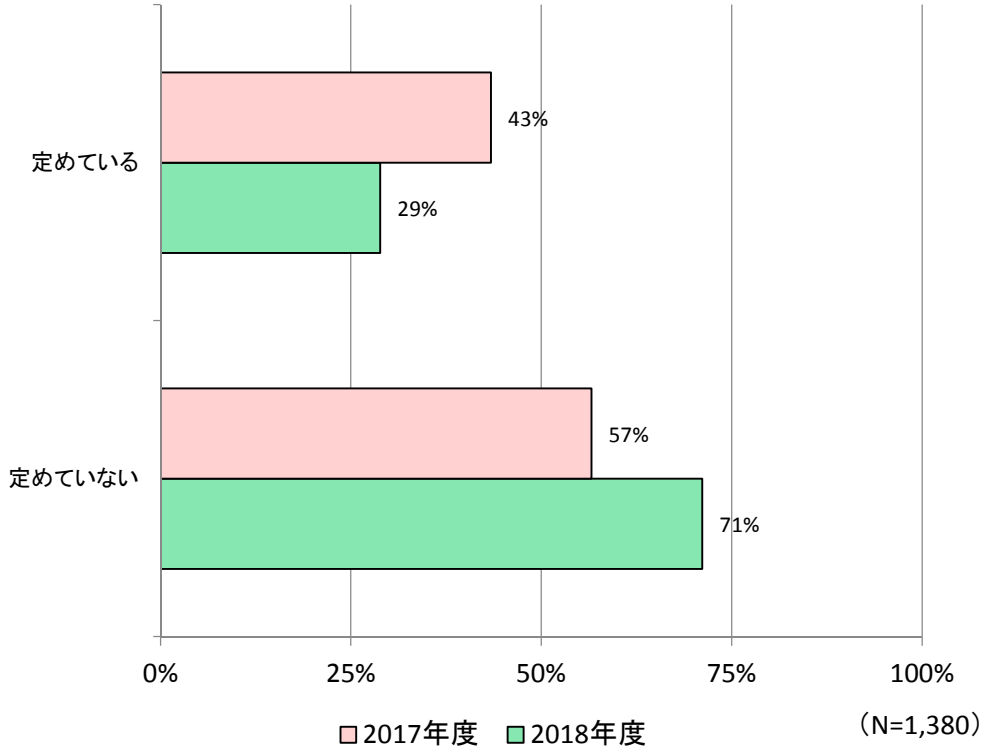


3.4. アンケート調査結果詳細 －（46/58）－

設問28　障害発生時の利用者アナウンスの判断基準

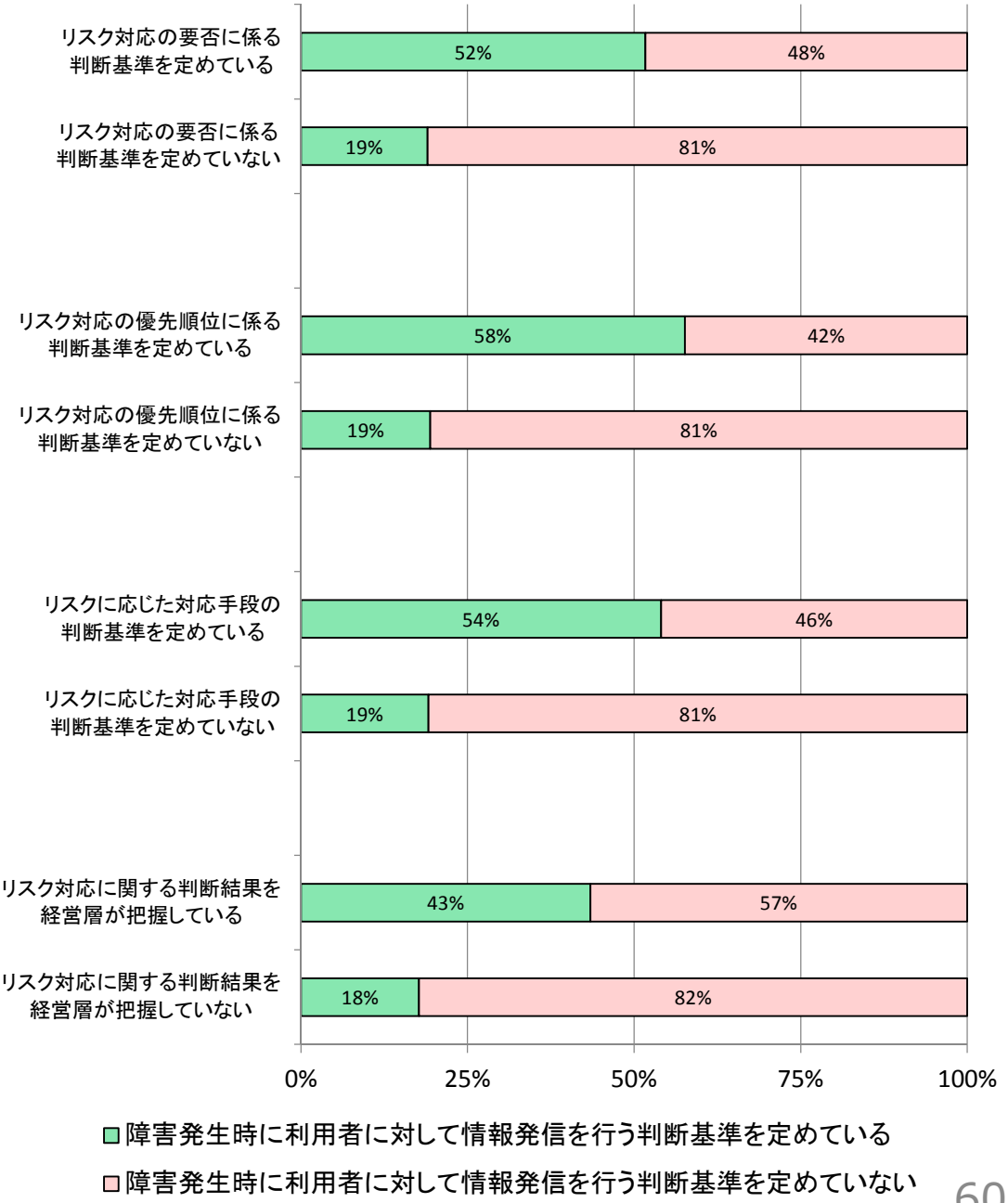
・アナウンスの判断基準を定めている事業者等は、リスクに対して判断基準もそれぞれ明確化されており、その基準および判断結果を経営層が把握している傾向がある（参考①）。

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）

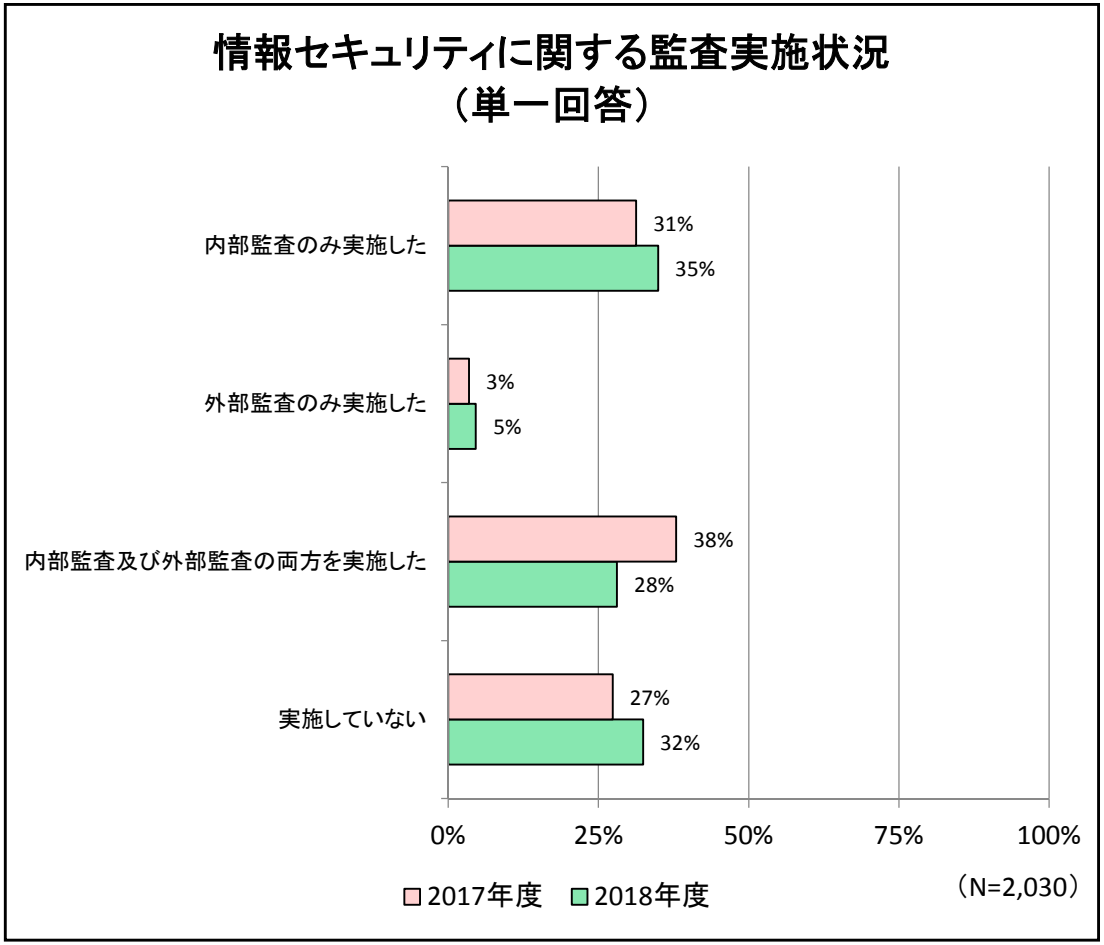
参考①　障害発生時の判断基準策定と各項目の関係性



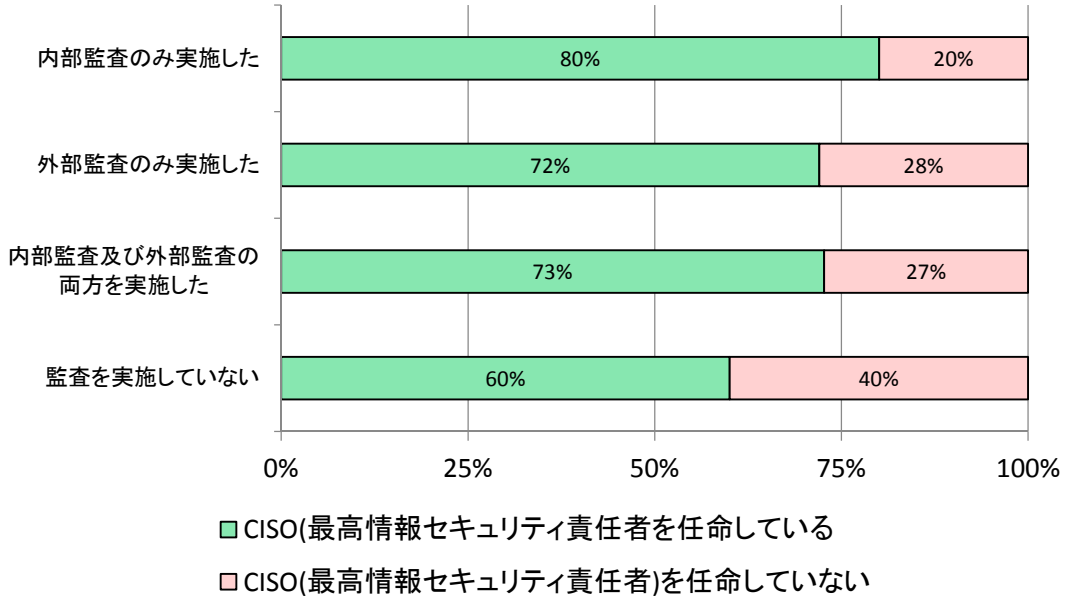
3.4. アンケート調査結果詳細 －（47/58）－

設問29 情報セキュリティに関する監査実施状況

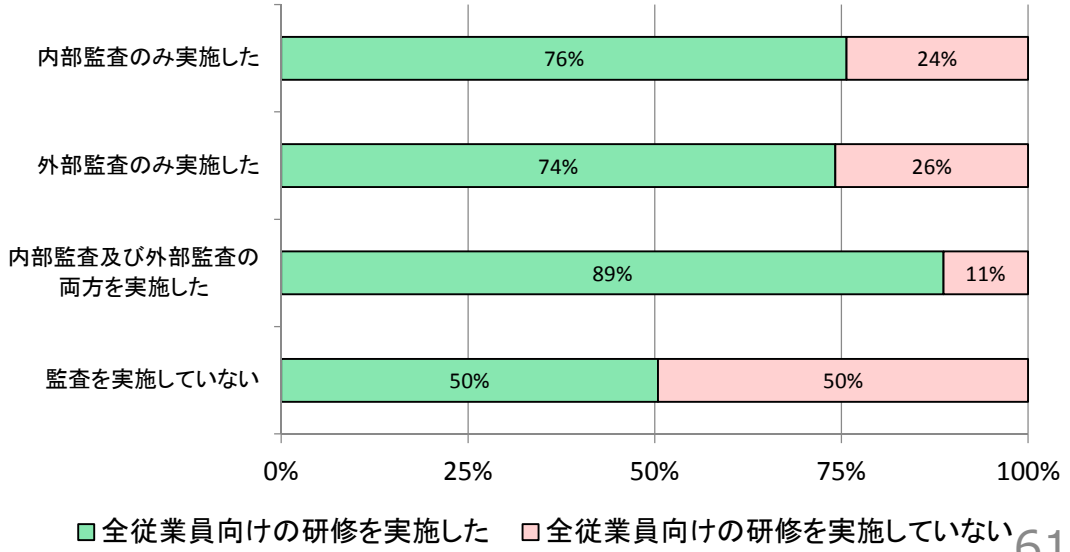
・CISOを任命している事業者は、内外監査を実施し、全従業員向けの研修を実施している傾向がある（参考①、参考②）。また、内部と外部の監査の両方を実施している９割の事業者等では、全社員向けの研修が行われている（参考②）。



参考① 監査の実施状況とCISOの設置状況の関係



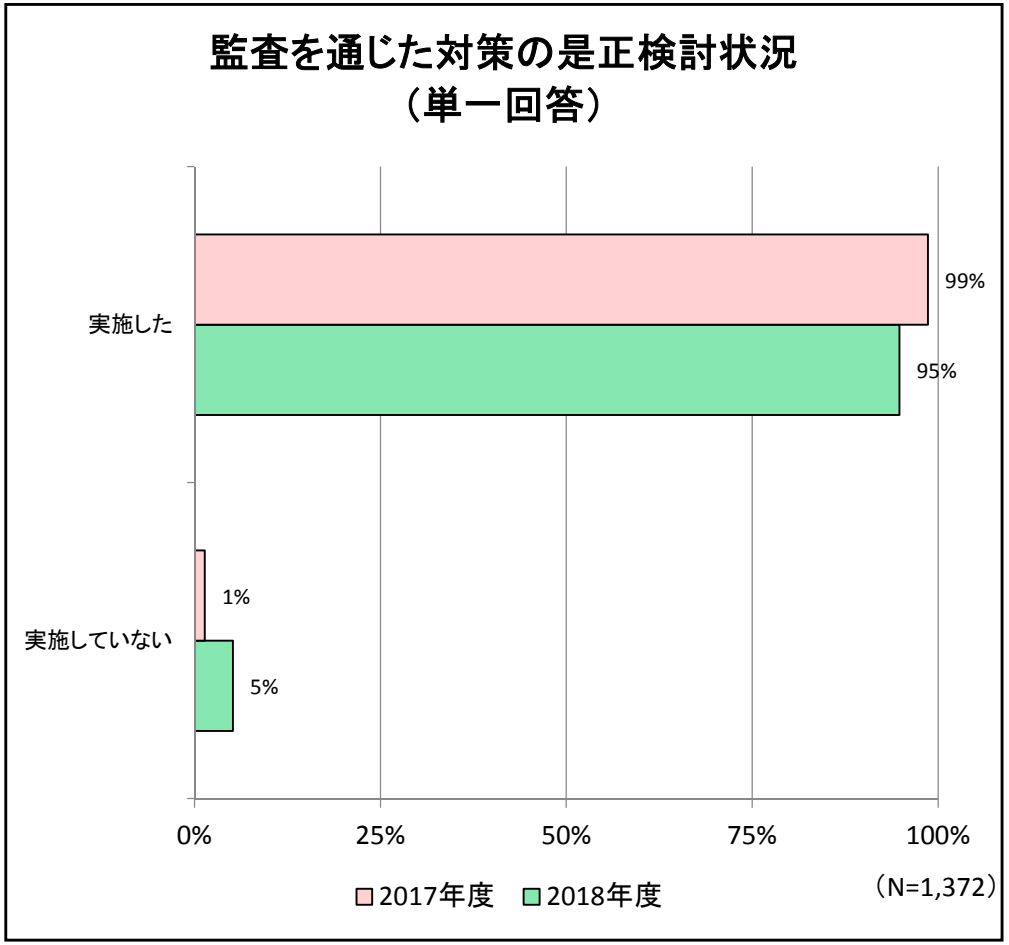
参考② 監査の実施状況と全従業員向けの研修実施状況の関係



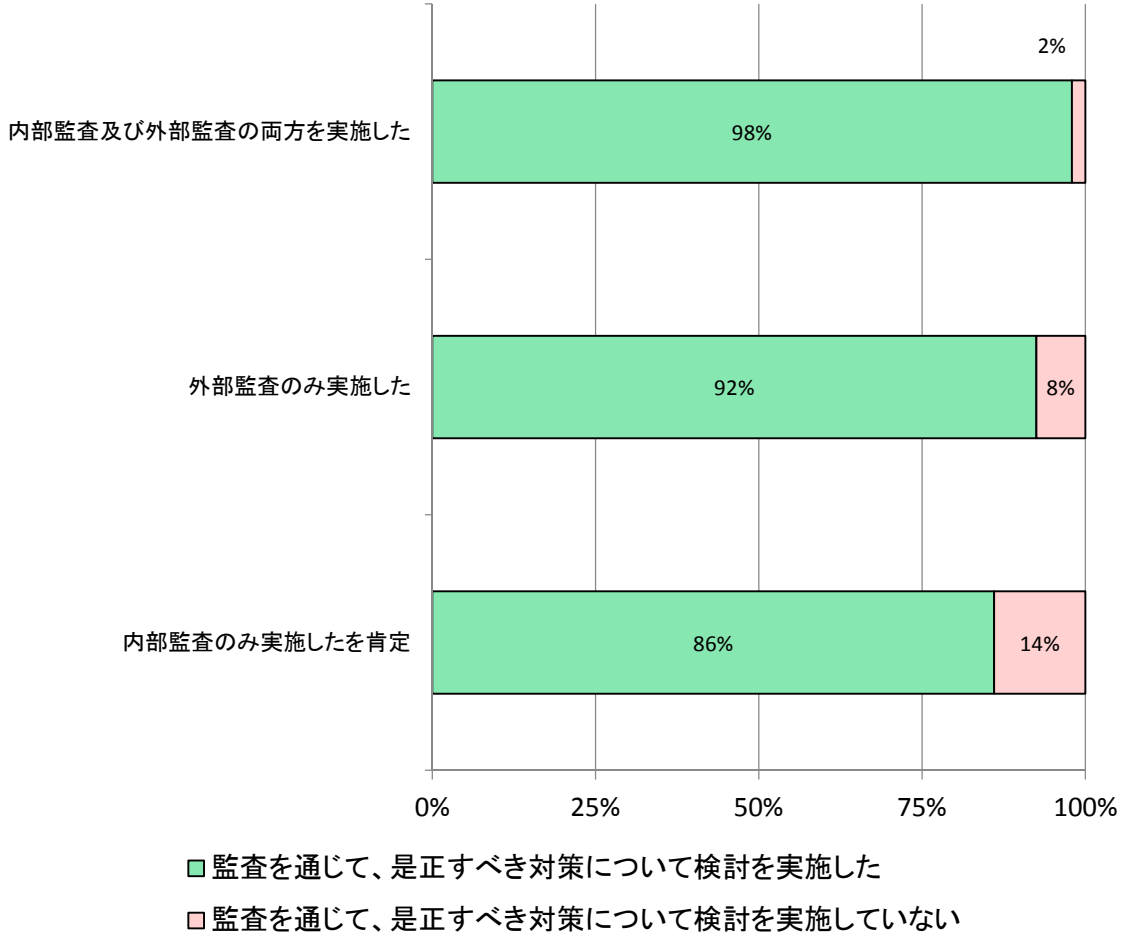
3.4. アンケート調査結果詳細 －（48/58）－

設問29-1　監査を通じた対策の是正検討状況

・監査を通じて対策の是正を実施している事業者等は、監査を、「内部・外部」＞「外部のみ」＞「内部のみ」の順で実施している。是正まで実施している事業者等は、全体的に取組が進んでいる傾向がある（参考①）。



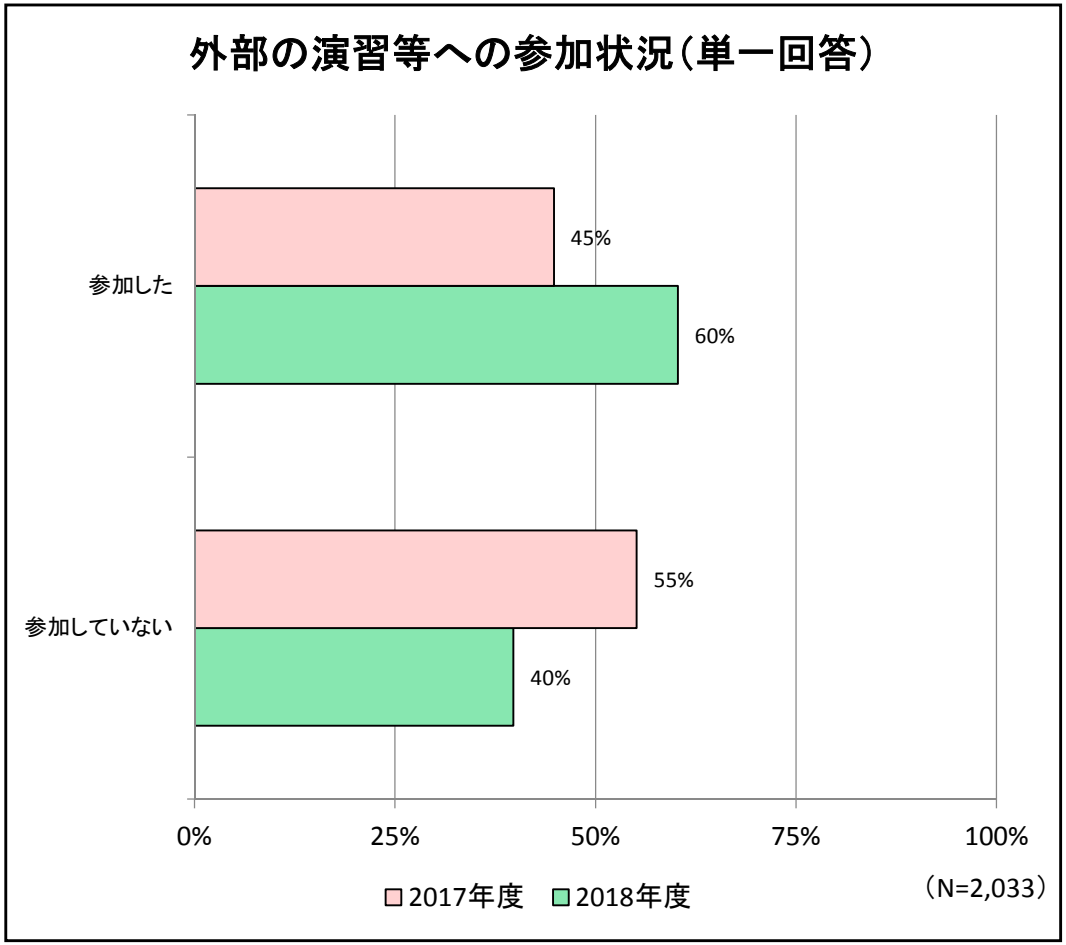
参考①　内部監査と外部監査の実施状況と対策の是正状況の関係性



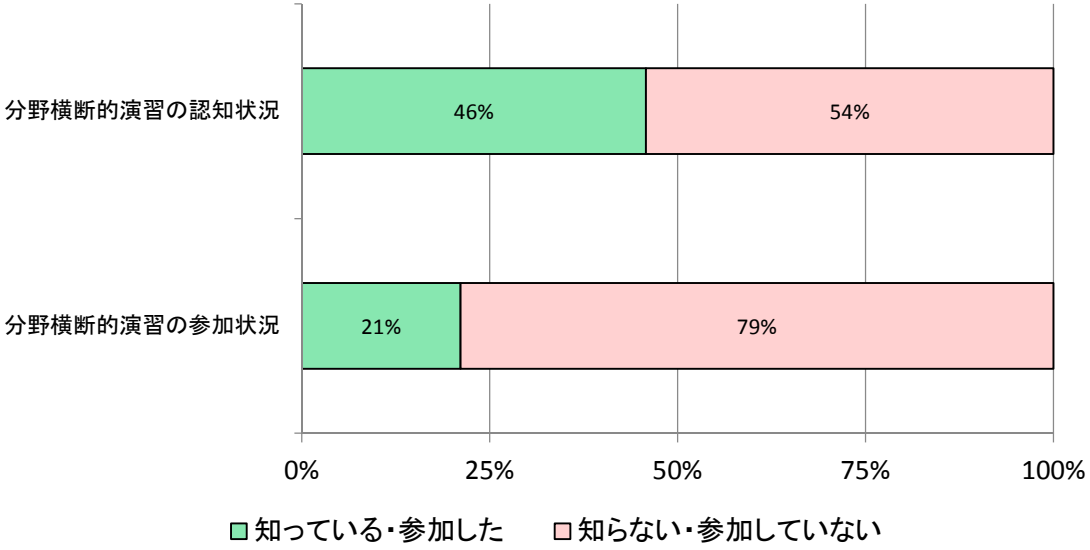
3.4. アンケート調査結果詳細 – （49/58） –

設問30 外部の演習等への参加状況

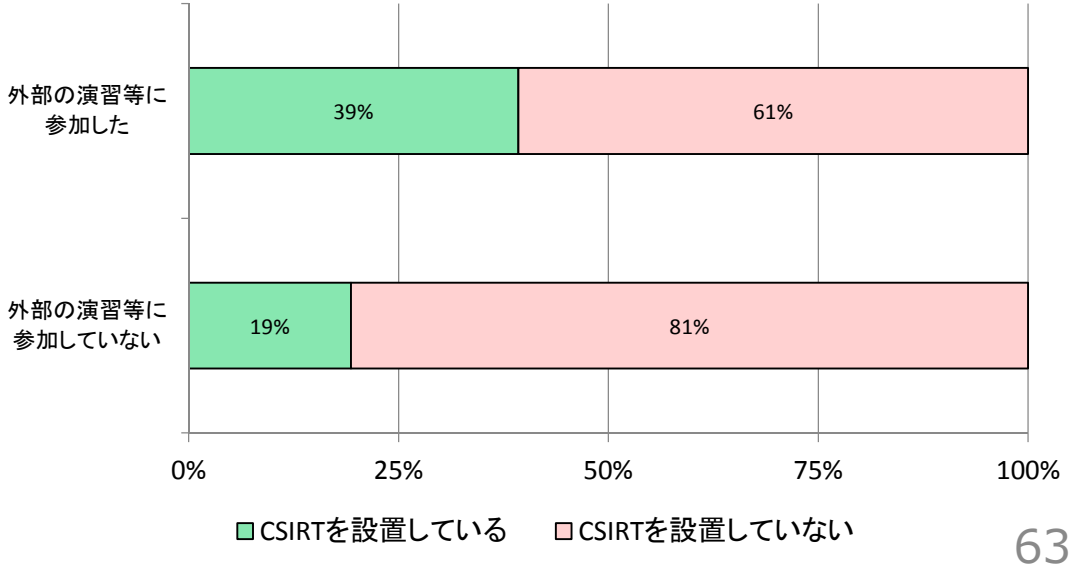
・外部の演習等に参加している事業者等のうち、５割弱が分野横断的演習を認知しており、約2割が分野横断的演習に参加した（参考①）。外部の演習等に参加するような演習に対して積極的な事業者等に対する分野横断的演習のPRは一定の効果が出ている。
・CSIRTが設置されている事業者等は「外部の演習等に参加している」傾向がある（参考②）。外部の演習等を通じて、他社の状況に刺激を受け、改善活動が進んでいると推察できる。



参考① 外部の演習等に参加している事業者等における分野横断的演習認知度と参加状況の関係性



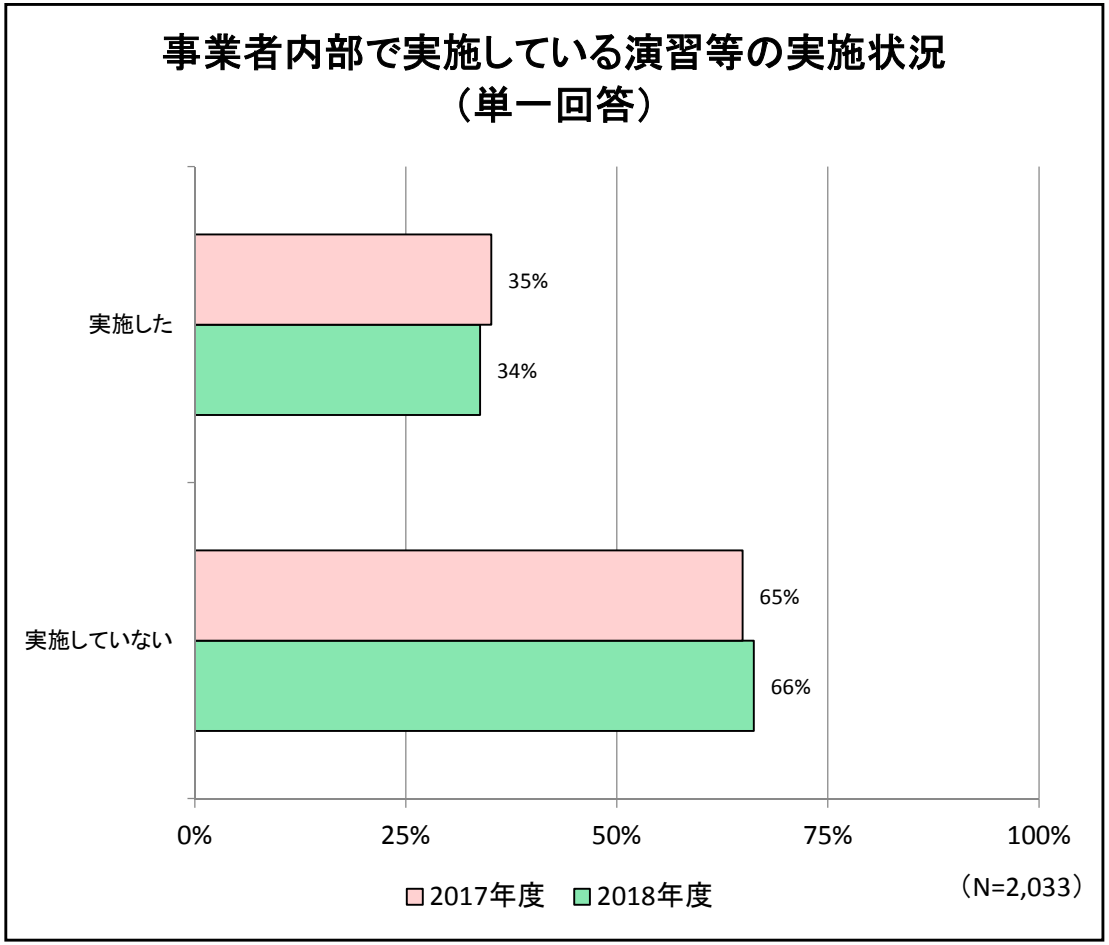
参考② 外部の演習等に参加している事業者等とCSIRT設置状況の関係性



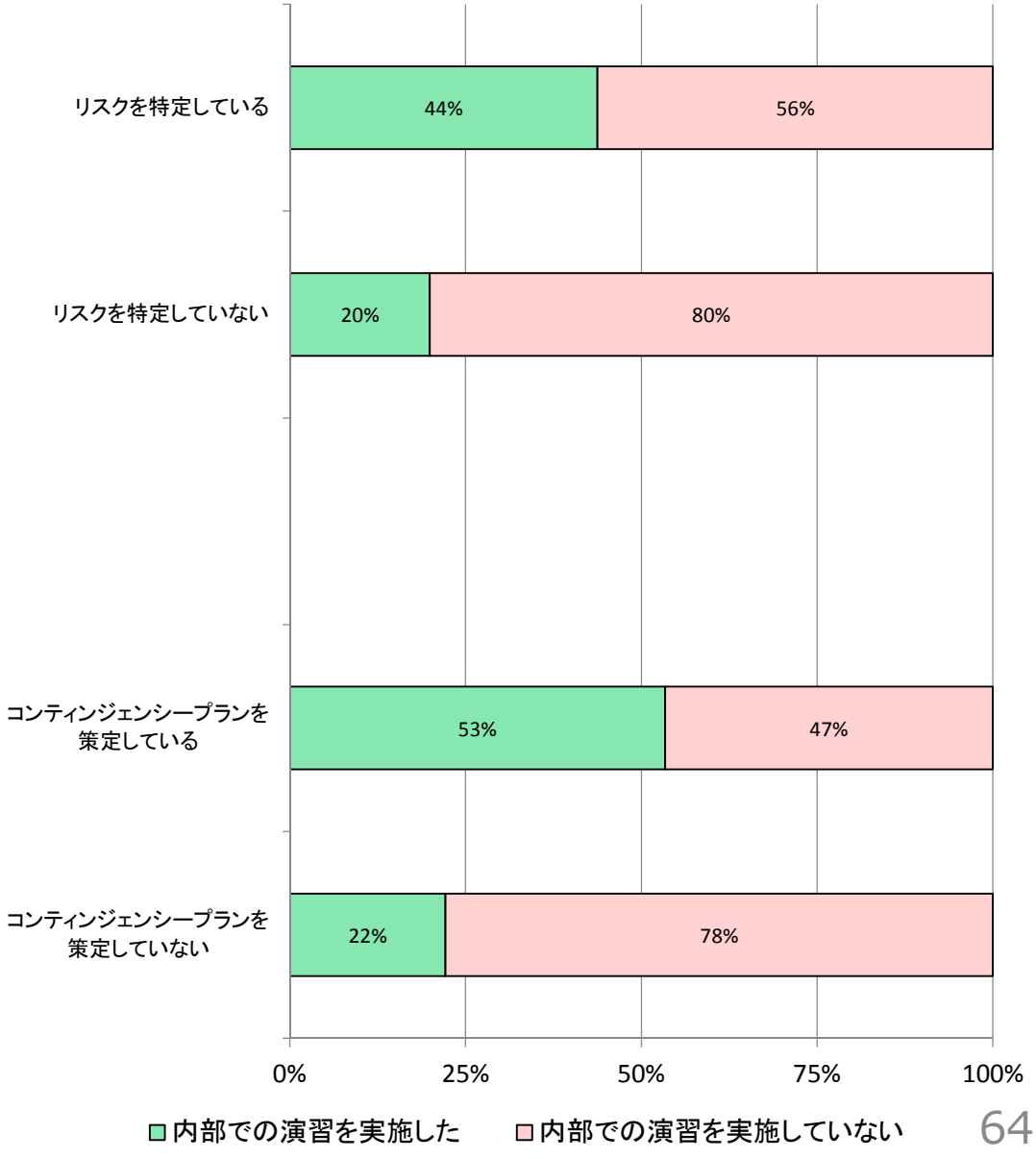
3.4. アンケート調査結果詳細 －（50/58）－

設問31　事業者等の内部で実施している演習等の実施状況

・事業者等ごとに演習を実施している事業者等では、リスクの特定やコンティンジェンシープラン（CP）の策定もできている傾向がある（参考①）。
・リスクの特定やコンティンジェンシープラン（CP）の策定ができている事業者等は、演習の機会を通じて、改善項目の洗い出しをしていると推察できる。



参考①　内部で実施している演習内容と各項目の関係性

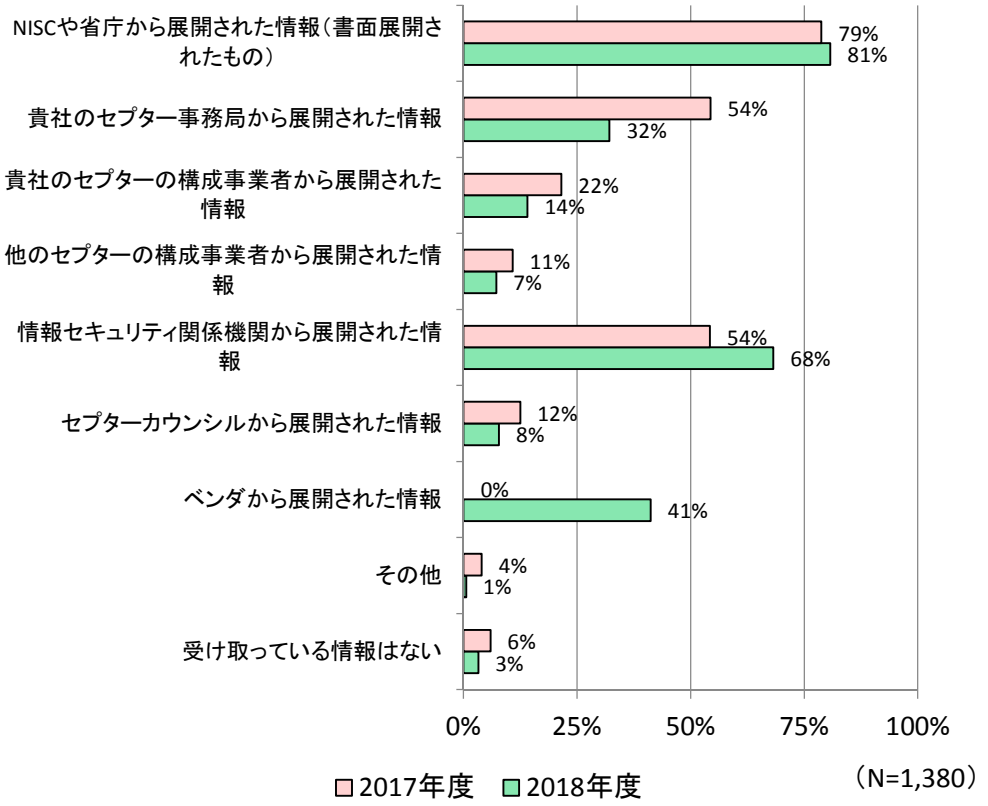


3.4. アンケート調査結果詳細 – （51/58） –

設問32　情報共有体制下での受信状況

・NISCや省庁、情報セキュリティ機関といった外部から展開された情報の受信については増加傾向があるが、セプター内、セプター間の情報共有が低調でありセプターの活動の活性化を図る必要がある。

情報共有体制下での受信状況（複数回答）

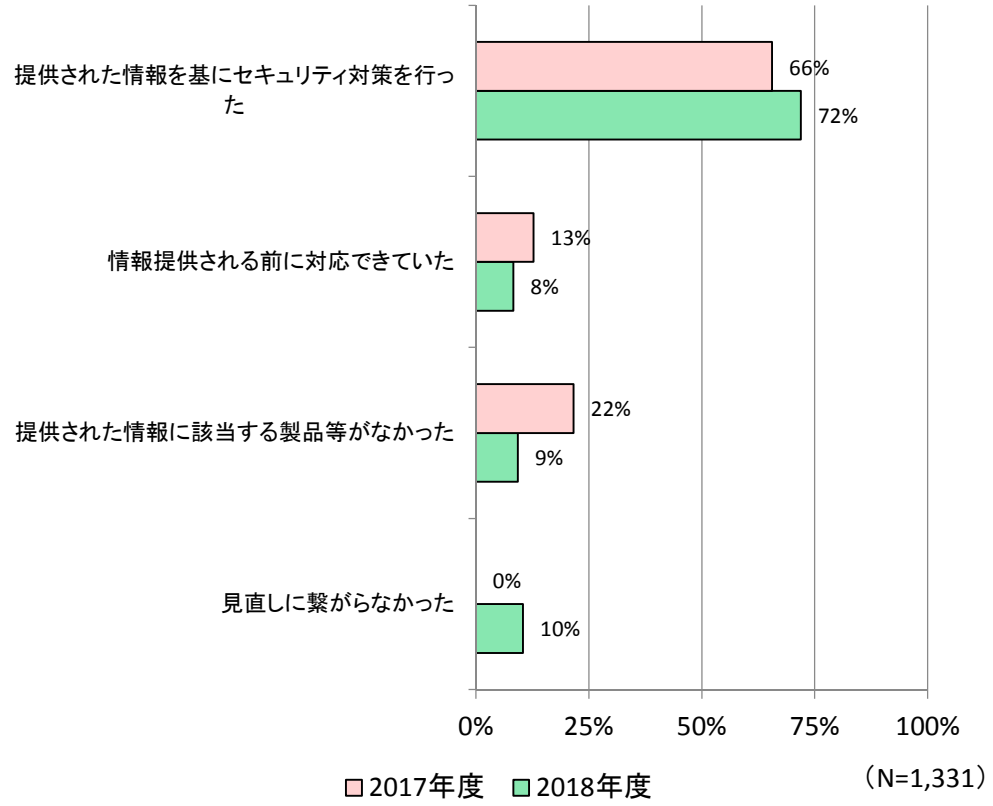


※金融は読替え可能項目なし（集計していません）
※ベンダから展開された情報は、2018年度から調査開始

設問32-1　受信情報の有効活用度

・提供された情報を基に対策を行っている事業者が増加しており、引き続き情報提供を着実に行うことが必要であると考えられる。

受信情報の有効活用度（単一回答）



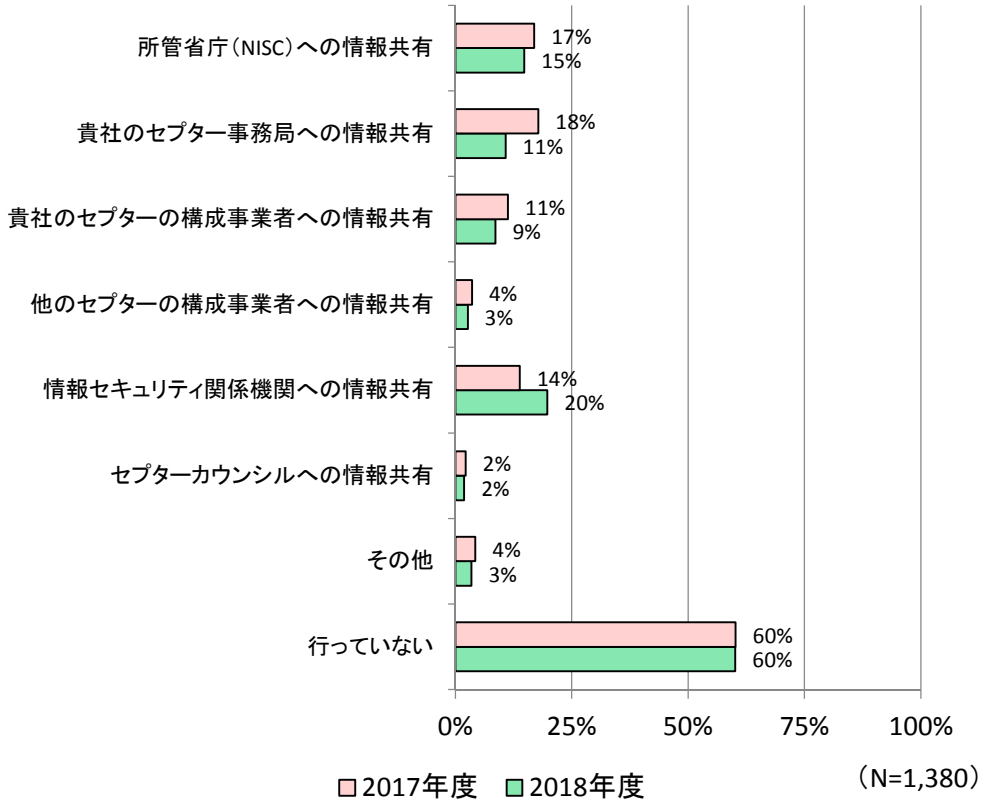
※金融は読替え可能項目なし（集計していません）

3.4. アンケート調査結果詳細 – （52/58） –

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が依然として半数以上となっている。また、情報セキュリティ機関への情報共有は増加している一方で所管省庁やセプターへの情報共有は低下しており、その状況も依然として低調である。情報共有の必要性の周知や、情報共有することによるメリットを示すなど、情報共有の活発化に向けた取組を行う必要がある。

能動的に行った情報共有状況（複数回答）

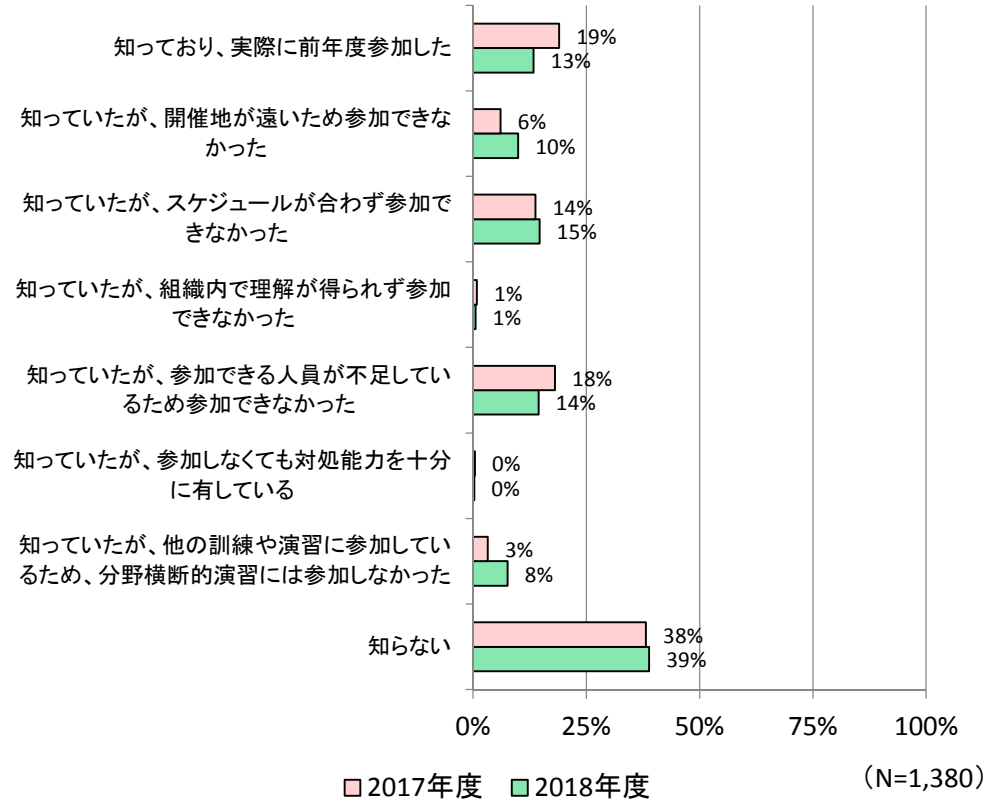


※金融は読替え可能項目なし（集計していません）

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」事業者に向け、自職場参加の推奨等にて参加を促し、分野横断的演習に可能な限り参加できるよう継続的な取り組みが望まれる。
また、「知らない」事業者に対しては、所管省庁等を通して広報活動を行う必要がある。

分野横断的演習の認知状況（単一回答）

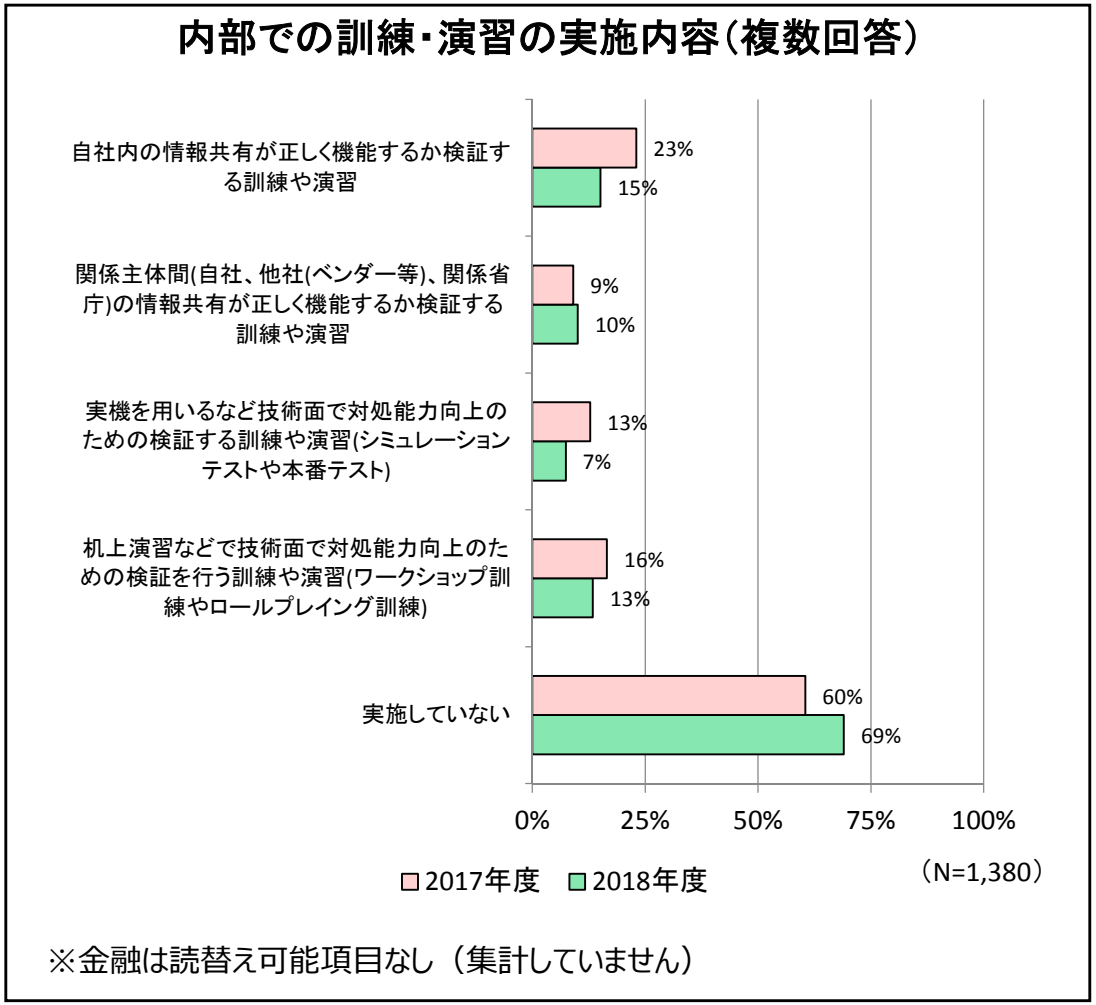


※金融は読替え可能項目なし（集計していません）

3.4. アンケート調査結果詳細 －（53/58）－

設問35　内部での訓練・演習の実施内容

・「実施していない」事業者については、まずは分野横断的演習等の演習に参加することが有効であると考えられるため、継続して演習開催の取り組みを行う必要がある。



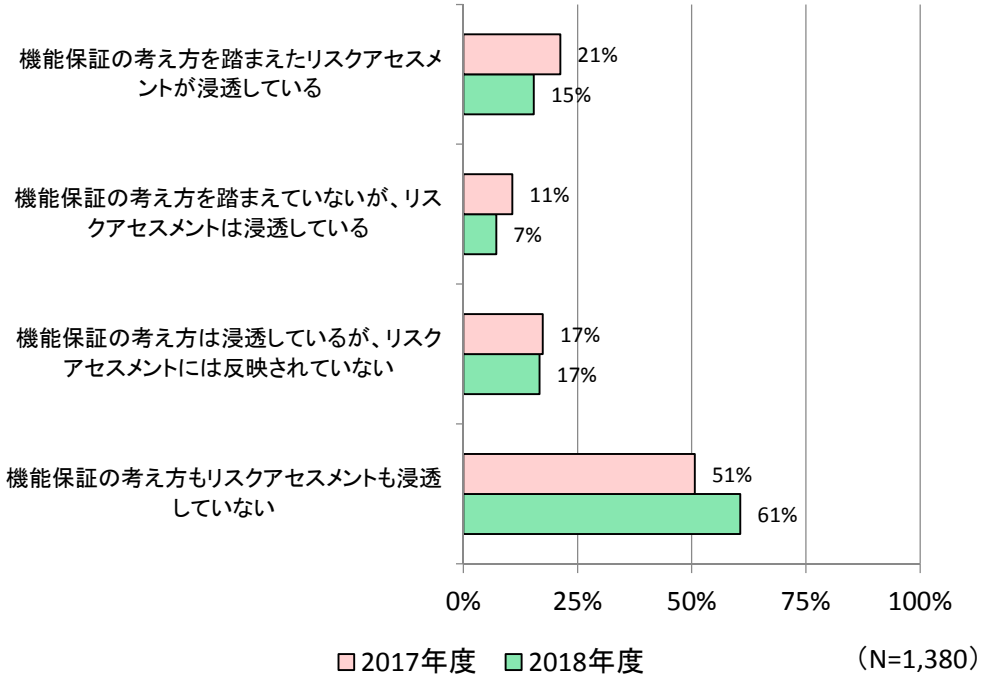
※金融は読替え可能項目なし（集計していません）

3.4. アンケート調査結果詳細 －（54/58）－

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

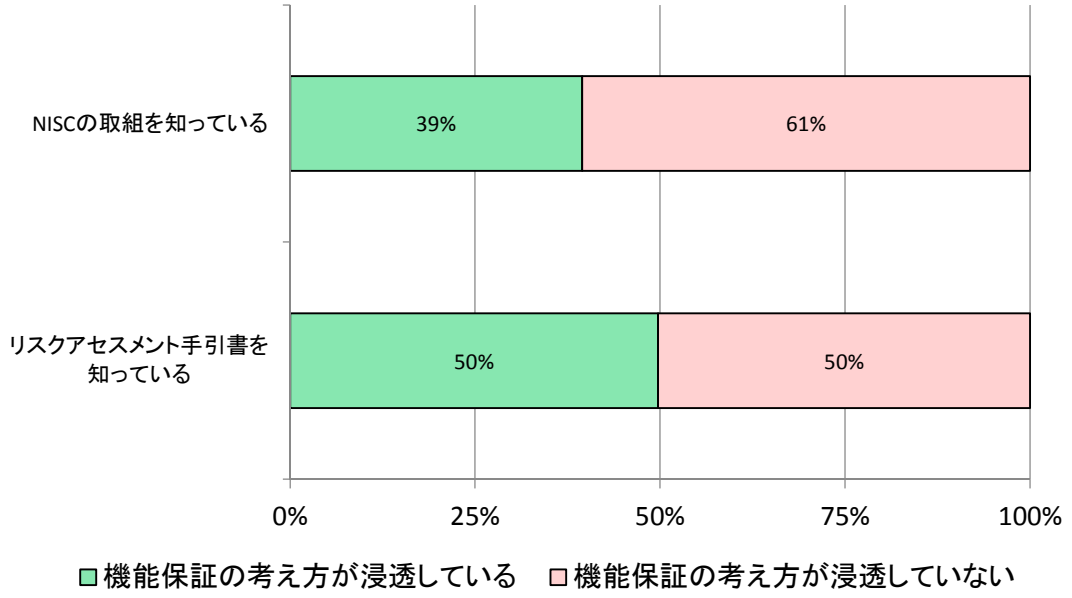
・何らかのNISCの取組を把握している事業者等のうち、６割の事業者で機能保証の考え方が浸透していない。また、リスクアセスメント手引書を把握している事業者等は５割である。そのため、一層の周知・啓発の必要性が認められる（参考①）。
・機能保証の考え方を踏まえたリスクアセスメントが浸透している事業者等であっても、うち4割がリスク対応の優先順位に係る判断基準を定めていないため、一層の実践が期待される。（参考②）

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）

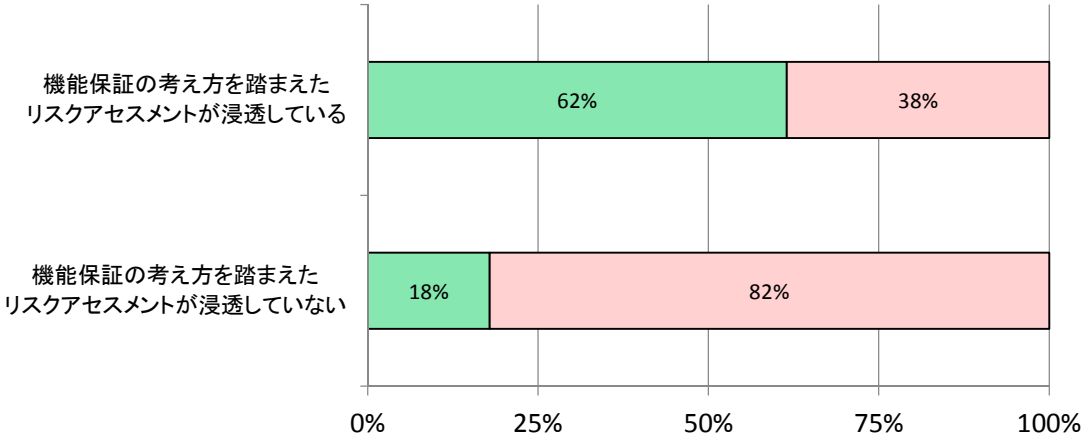


※金融は読替え可能項目なし（集計していません）

参考①　機能保証の考え方とNISCの取組認知度の関係性



参考②　リスクアセスメントの浸透とリスク対応の判断基準（優先順位）の関係性

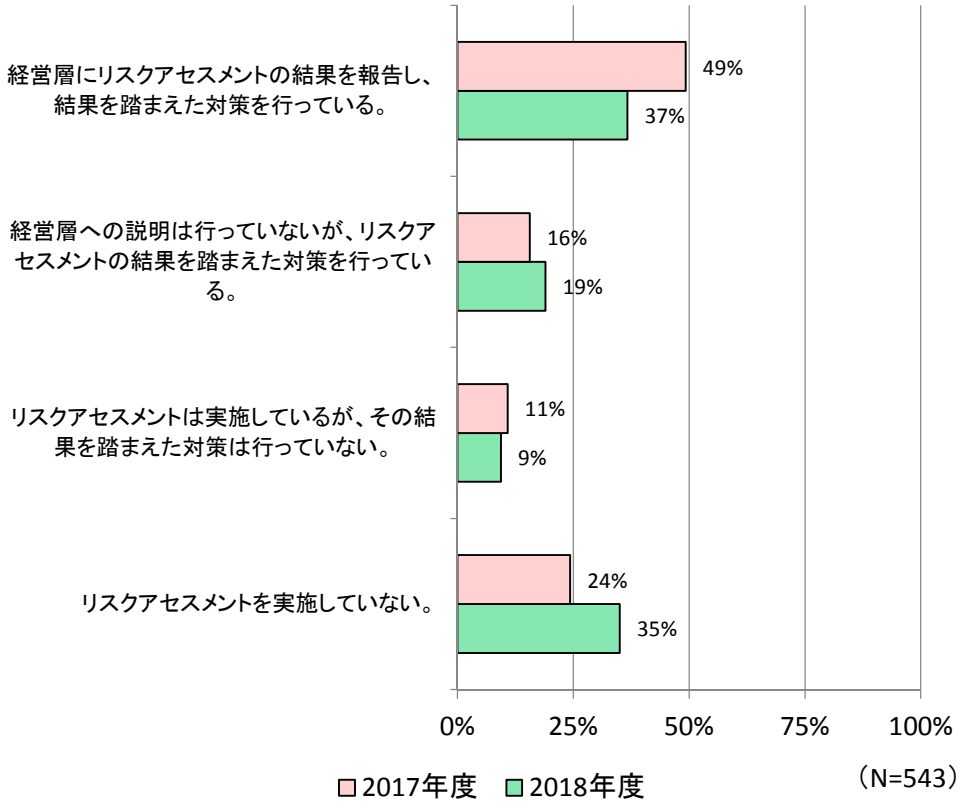


3.4. アンケート調査結果詳細 －（55/58）－

設問36-1　結果を踏まえた対策の実施状況

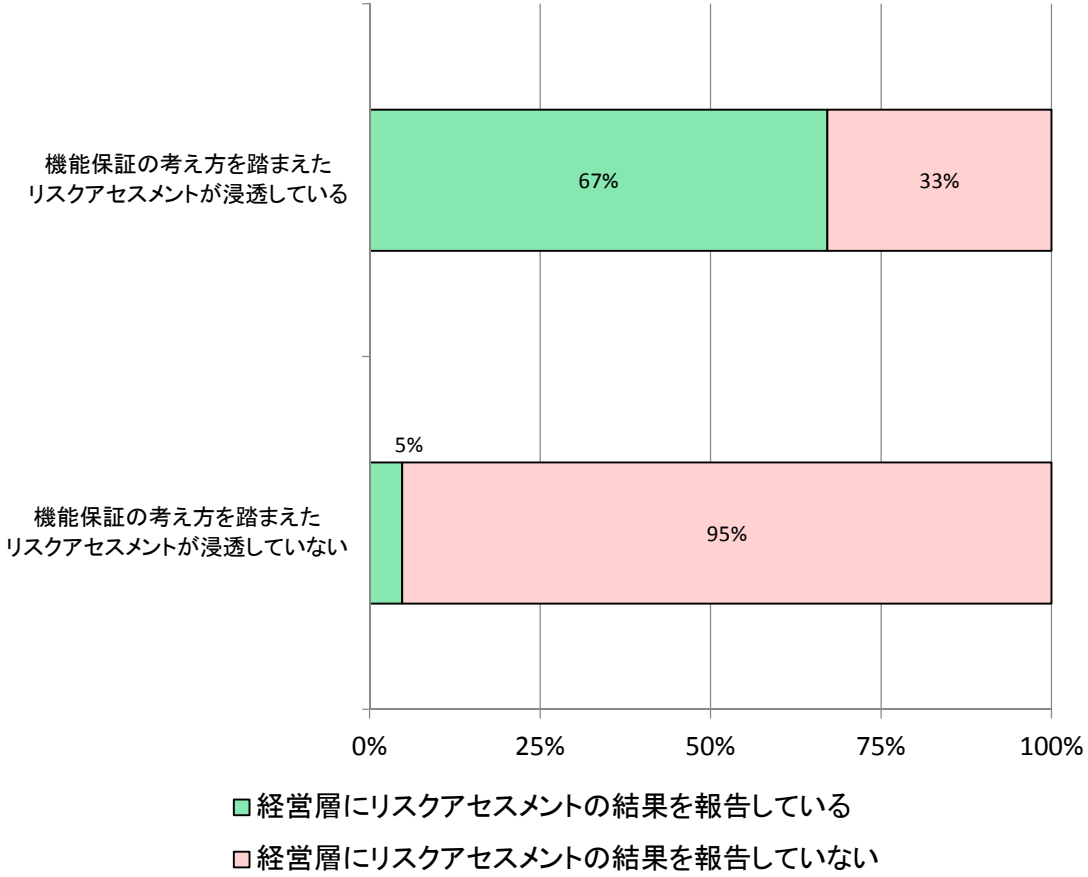
・機能保証の考え方を踏まえたリスクアセスメントが浸透している事業者等のうち7割の事業者等が、リスクアセスメントの結果を経営層へ報告していることが分かる（参考①）。一方で、全体ではリスクアセスメント自体の認知率・実施率ともに昨年より悪化している。リスクアセスメントの結果を踏まえたリスク低減等の対応を戦略的に講じることは経営者の責務であるため、機能保証の考え方の浸透も含め、経営層への更なる働きかけが必要である。

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）

参考①　機能保証の考え方（リスクアセスメント）の浸透状況と経営層への報告（結果）の関係性

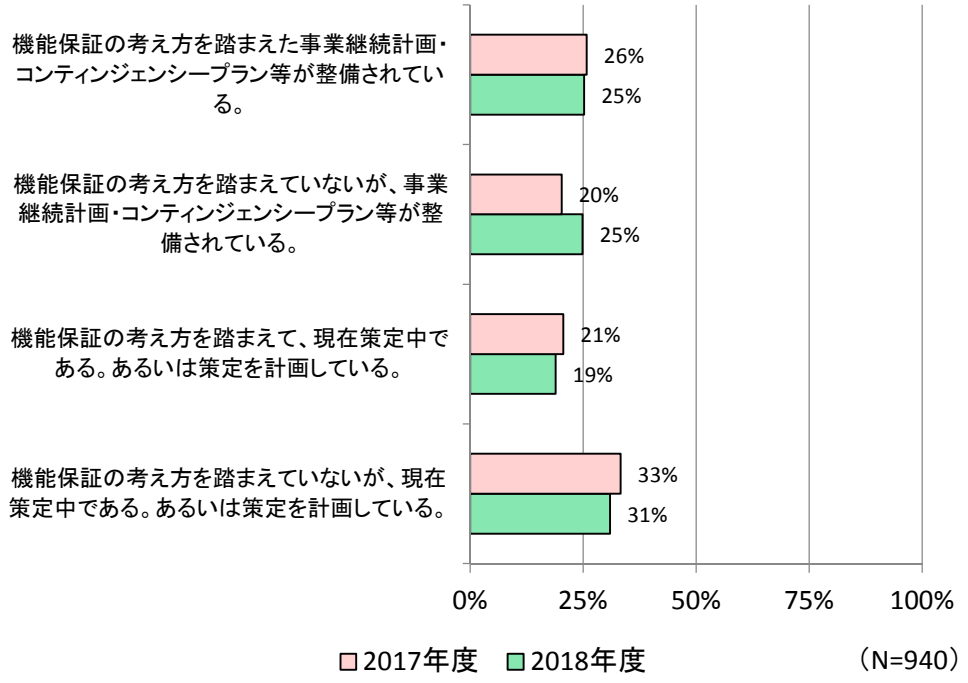


3.4. アンケート調査結果詳細 －（56/58）－

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

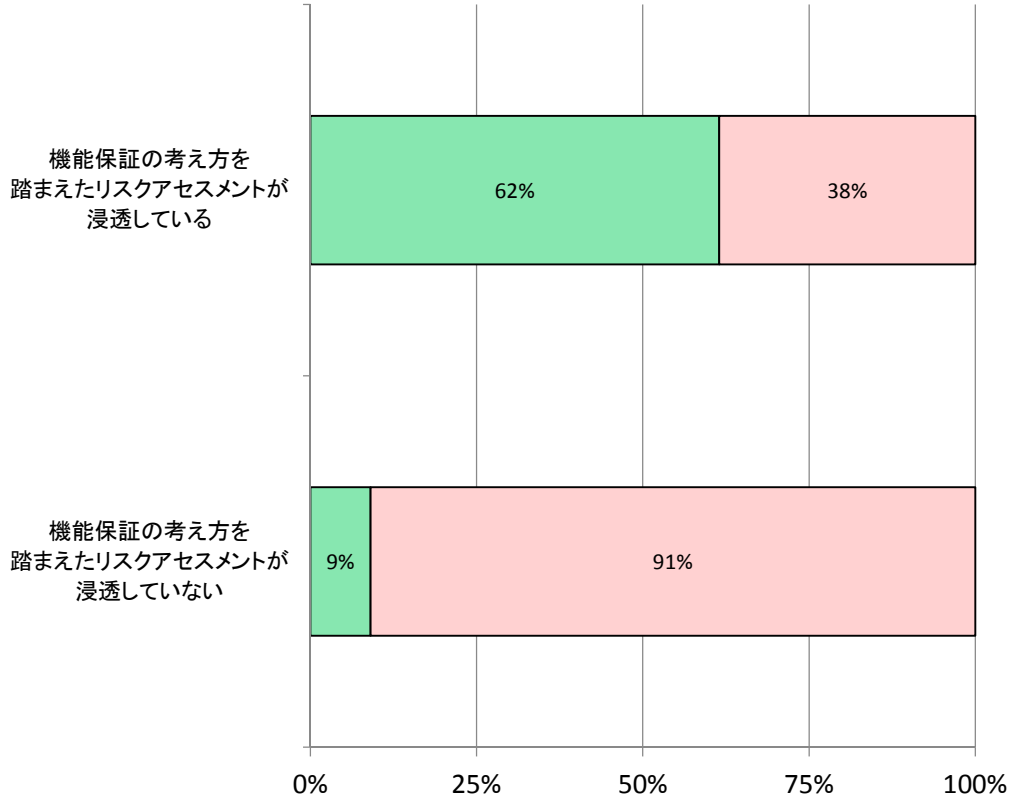
・機能保証の考え方を踏まえたリスクアセスメントが浸透している事業者のうち、機能保証の考え方を踏まえた事業継続計画（BCP）・コンティンジェンシープラン（CP）等が整備されている事業者は6割に留まっており、一層の実践が期待される（参考①）。
・策定中・計画中の事業者も合わせると８割になるため、それらの事業者への支援も有効と考えられる。
・全体では機能保証の考え方そのものの浸透に課題があり、まずはその普及・啓発が必要と考えられる。

機能保証の考え方を踏まえた事業継続計画（BCP）・コンティンジェンシープラン（CP）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）

参考①　機能保証の考え方の浸透状況と事業継続計画/コンティンジェンシープラン整備状況の関係性

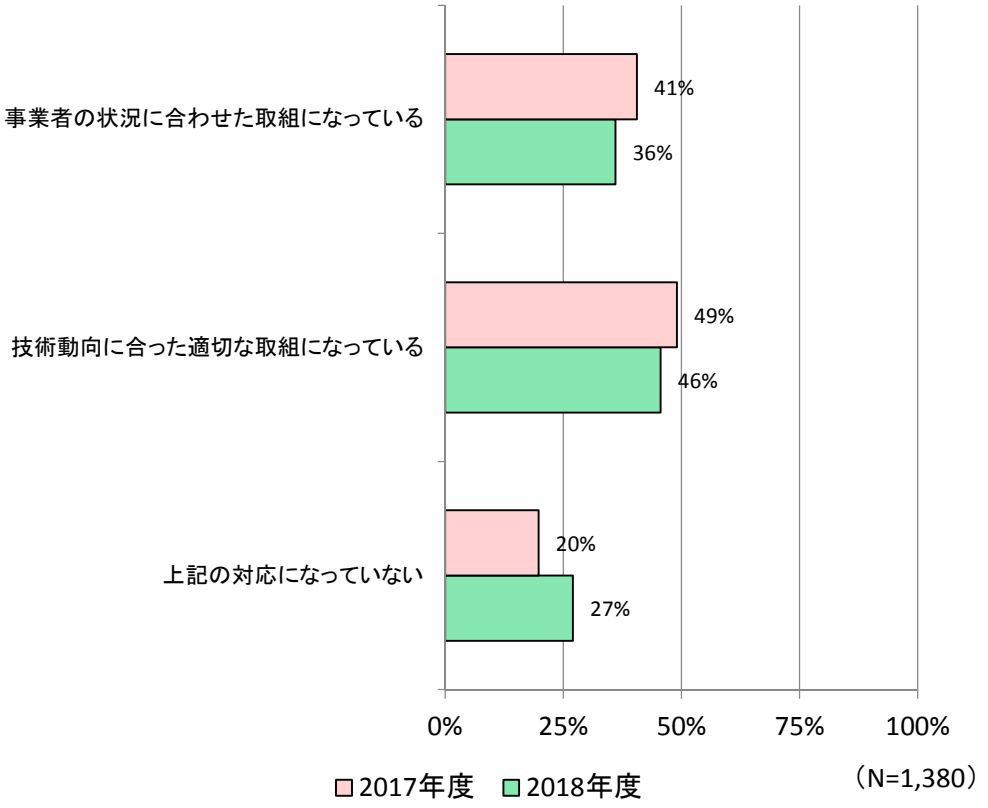


3.4. アンケート調査結果詳細 －（57/58）－

設問38　国の施策に対する意見

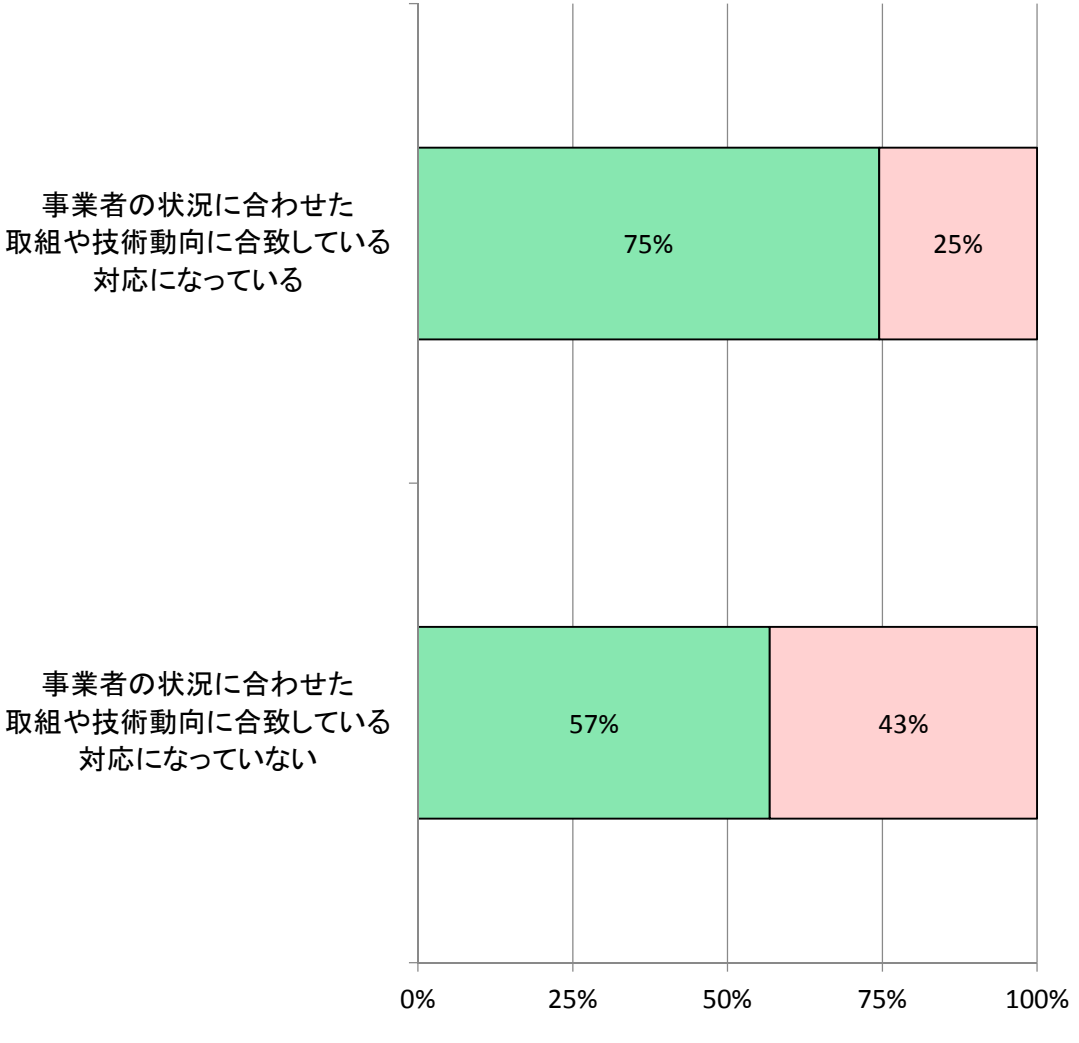
・事業者の状況に合わせた取組や技術動向に合致していると回答した者は、NISCの取組や自分野のガイドラインを把握している傾向があり、国の施策を理解した上でセキュリティ対策に取り組んでいるものと考えられる（参考①）。

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）

参考①　NISC等の取組把握状況と事業者等のセキュリティ対策の取組の関係性

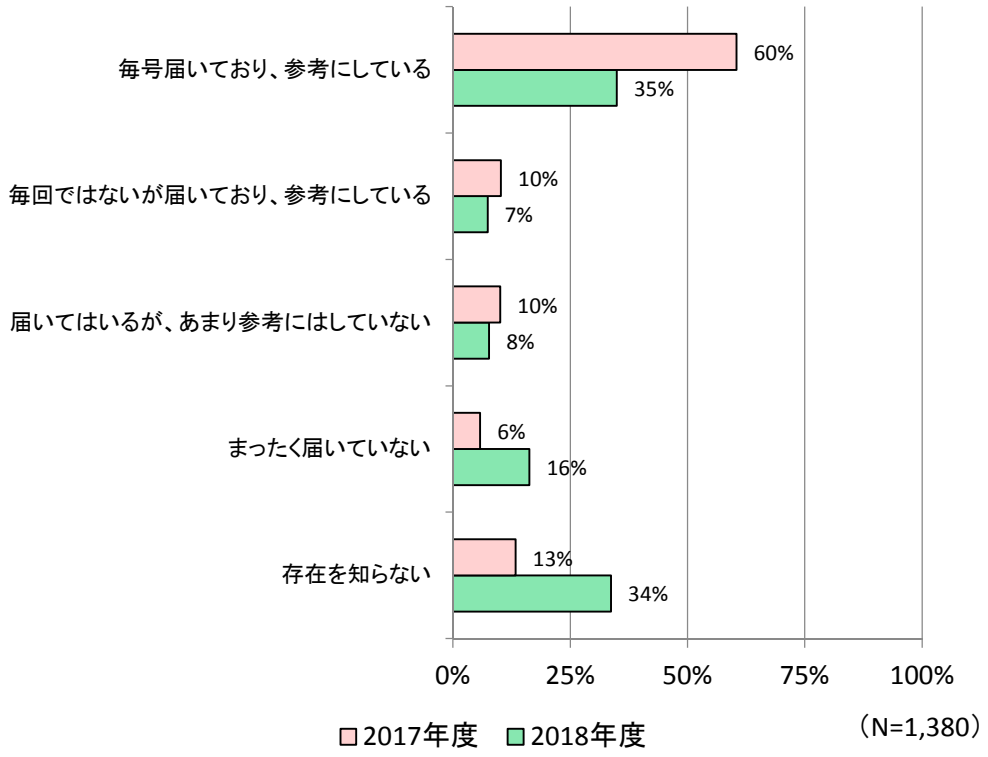


3.4. アンケート調査結果詳細 －（58/58）－

設問39　重要インフラニュースレターに関する状況

・重要インフラニュースレターが届いていない、あるいはその存在すら知らないという事業者が増加しており、その結果参考にしている事業者についても減少してしまっている。事業者が求める内容を調べるとともに、周知活動や配信先の確認等を行う必要がある。

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）

3.5. アンケート調査の自由意見（1/4）

【安全基準等に関する意見・要望等】

- 情報セキュリティポリシーを策定する際には、安全基準等や関連組織が発行しているガイドブック等を参考にしている。
- 販売されている情報システムの製品については、購入時点で情報セキュリティのガイドライン等に準拠することができるよう、政府として動いていただきたい。
- 分野特有のシステムに汎用的なOSの採用やバックアップの回線にインターネットVPNの採用等の新たなリスクが増加していることから、安全基準等を改正する際には、事業者の現状を把握する必要がある。
- 安全基準等は、策定する所管省庁ごとに事業者に求める対策水準が異なるため、設備によっては対策水準が異なる。分野によらない一律の対策水準を策定していただきたい。
- 安全基準等を策定する際は、最終目標だけでなく、各事業者等の事情を踏まえ、状況に応じた段階的な対応策及び業務支援の拡充を考慮したうえで、円滑な対応ができるよう検討いただきたい。
- 安全基準等の内容が抽象的である。安全基準等として、どの程度の対策水準を求めているのか、またどの対策の水準を満たせば十分なのか具体的かつ明確に示していただきたい。
- 事業規模が小さい事業者では、人材面や資金面が十分ではないため、政府や情報セキュリティ関連団体が要求する事項を実施することは難しい。対策を実施するのに障壁が高いセキュリティ対策を要求するのであれば、実現可能な手立ても併せて提示していただきたい。事業規模に合わせた対策内容や優先順位、ロードマップ等を示していただきたい。
- 事業規模が小さい事業者は人材や資金が乏しいため、安全基準等の対策をすべて講じることは難しい。事業規模を考慮した安全基準等を策定していただきたい。
- 安全基準等の充足度が事業者でも確認できるチェックリストがほしい。
- 安全基準等の改訂があった場合は、わかりやすい新旧対照表をいただきたい。
- 一部の安全基準等は、難しい専門的用語やカタカナ英語を用いているので、わかりにくい。初心者でも理解し、読み手全員が共通の認識を得られるように、解説や例示を設ける等の配慮をいただきたい。
- 安全基準等に基づき規則・基準・内規等を整備したとしても、その実効性に疑問がある。また、訓練や演習、監査も人材面や資金面の負担が大きい。そのため、費用対効果の高い対策等を示していただきたい。
- 重要サービスの提供に関わる重要な施設は広大であり、様々な職種の方が作業に関わるため、入退管理制限対策を行い、部外者の侵入を完全に塞ぐことは難しい。

3.5. アンケート調査の自由意見（2/4）

【指針に関する意見・要望等】

- 一部の分野では、指針を参考にガイドラインが策定され、チェックシート等が整備された。
- 具体的にどのような対策を進めていくべきか、明示的に示してほしい。
- 「機能保証」は重要であるが、これを前提すると情報セキュリティ以外も考慮する必要が発生してしまう。

【情報共有体制の推進に関する意見・要望等】

- 一部の分野では、業法に基づいて報告する事案でないヒヤリハット等を情報共有できるルートが設定されている。
- 第４次行動計画の情報共有体制では、業法に関わる事案やヒヤリハットで匿名化の処置が必要な事案によって、報告ルートが異なっている。インシデント対応は対応事項が多いので、報告ルートを統一化し、事業者負担の軽減してほしい。
- 政府やセプター事務局、セキュリティ関係機関は、脅威の大きさに関わらず注意喚起を行っているため、その件数が多い。結果、事業者が情報の確認や評価する負荷が増加したため、脅威情報の検知等が遅くなるリスクが増加している。情報提供元が情報を集約し、評価していただきたい。
- 報告先により、情報共有方法（メール、システム、電話等）が統一されていない。この部分も、統一化していただきたい。
- 情報共有の手法が、情報共有ツールを用いたシステム化が進んでいるが、一部の事業者ではセキュリティ上の思想により、情報共有ツールが遮断されているケースもあり、情報の共有にタイムラグが生じている。
- 政府の施策が改善され、事業者まで周知が必要な事項の場合は、連絡していただきたい。
- 情報システム部とセキュリティベンダーの月例会を実施し、サイバーセキュリティインシデントに関する情報交換を行っている。
- 情報セキュリティのインシデント事例の提供は有難い。必要に応じて、関係部署と共有し、セキュリティ強化を図っている。
- セキュリティ情報は積極的に収集しているが、情報報告や社内展開には消極的である。
- セキュリティベンダーの担当者から定期的にセキュリティパッチ配信や情報セキュリティの助言をいただいている。
- 地域的に近い事業者や同じ分野の事業者、ITユーザ会の参加事業者と情報システム部会を開催し、意見交換している。
- 技術の進展やソフトウエアの開発によって、リスクや脅威の変化するので、最新の状況を連携していただきたい。
- 情報システムや情報セキュリティの発展速度が著しく早いため、習得したノウハウがすぐに過去のものになってしまう。また、情報セキュリティの情報は公開されにくいため、最新情報が簡単には得にくい。

3.5. アンケート調査の自由意見（3/4）

【国・政府に対する意見・要望等】

- NISCが発行している重要インフラニュースレターは、必要な情報がまとめられており、対策検討や注意喚起に役立っている。
- 重要インフラニュースレターの情報は、専門性が高く、送られてくる情報が理解できない部分がある。
- 政府や情報セキュリティ関係機関から早期警戒情報や脆弱性情報等の情報が届くが、提供元ルートを一元化してほしい。
- 分野的横断演習のインデント対応の中で、自社の対応における問題点や課題が明確になった。
- 「重要インフラ事業者等」に該当する事業者等の定義を明確にしていただきたい。
- ランサムウェア等によるシステム不全に陥るようなサイバー攻撃が目立ってきているが、現状では、マルウェアの対策はソフトウェア業界任せになっており、表面化していない脅威に積極的に取り組んでいるとは言い難い。そのような脅威を未然に防ぐためにも、政府の研究機関等が、マルウェア対策に取り組んでいただきたい。
- 情報セキュリティに関わる「人材育成」を重要課題と捉え、積極的な支援や方策等について取り組んでいただきたい。
- 情報セキュリティ対策に関わる補助金などを準備いただきたい。
- 情報セキュリティの担当者が少ない事業者でも取り組めるセキュリティ対策良好事例を紹介いただききたい。
- ネットワークを含めたセキュリティの基礎から習得する必要があるため、Cyderだけでなく、ベンダーが実施している有償の技術研修にも参加している。セキュリティ対策への理解が得られなければ、予算の確保もできないため、Cyder等の研修において、ネットワークを含めたセキュリティの基礎から習得する研修を設定してほしい。
- CSIRT構築など情報セキュリティ対策として求められる要件を鑑みて、最低限義務付ける人員・業務項目を提示いただくとともに、ハードルの高いセキュリティ対策を要求するなら、実現可能な手立てや態勢整備のための支援・補助を期待する。
- 情報セキュリティや情報システムを保守する技術職の人材不足で、十分な対応ができない。また、次世代の育成にも問題を抱えている。政府として、事業規模の小さい事業者でも、情報セキュリティや情報システムを保守する技術職の従業員が十分確保できるような施策を行っていただきたい。
- IoT機器やSNSの普及により、インターネット環境が必要不可欠となってきている。利便性を高めつつ、セキュリティ強化をする必要があり、設備費用や運用費用も高額になっている。政府として、費用を抑える仕組みを検討していただきたい。

3.5. アンケート調査の自由意見（4/4）

【アンケートに関する意見・要望等】

- アンケート後に表示される事業者に向けた「アドバイス」があり、大変参考になった。
- 情報セキュリティ対策のノウハウを蓄積するという考えそのものがなく、大変参考になった。
- 情報セキュリティの専門知識を有する従業員が少ない事業者等もいるため、情報セキュリティ用語の説明や推奨される取り組み等のURLを増やして頂けると他部署の従業員等への情報の共有や浸透に、より一層利用しやすくなる。
- 重要インフラサービス提供に最も大きく影響するシステムに対する設問への回答が、実態とそぐわない場合がある。そのシステムについて回答を求める場合は、実態に合った設問に修正していただきたい。
- 重要システムの運用管理部門と全体統制を行う部門が異なるため、各設問項目において、回答すべき部門や回答を想定しているシステム等を明記していただきたい。（「システム運用部門への問い」「全社的なリスク統括部門への問い」 等）
- 「アンケート設問に対する注釈の内容が読めない」「解説文のアドレスをコピーできない」「表示されるURLがリンク切れしている」等があるため、必要に応じて改善していただきたい。また、シートの保護を解除する件について、ご検討いただきたい。

【その他の意見】

- 情報セキュリティは社内を横断した対策を求められることから様々な知見が必要だが、情報セキュリティを一括して相談できる窓口がない。コンサルタントに相談することも考えられるが、資金が必要となるため、事業規模の小さい事業者では、現実的な選択肢ではなく、対策の取り組みが滞ってしまう。

4.1. 往訪調査について

1.本調査の目的

- アンケート調査結果から得られた仮説の検証及び良好事例の収集
- 各分野の状況把握や技術動向等の情報収集に努め、随時施策に反映

※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（平成29年4月18日サイバーセキュリティ戦略本部決定）

2.調査方法

安全基準等の浸透状況等調査の結果を基にした現地ヒアリング（2時間程度）

3.主な調査内容

① 経営層の関わり方について
② 演習や訓練について
③ 情報共有体制について
④ 内部・外部犯行対策について
⑤ システムの出入り口対策について

4.調査対象

重要インフラ事業者等　16者

情報通信分野・航空分野・鉄道分野・物流分野・ガス分野・クレジット分野

※アンケート調査結果・地域特性・事業規模を踏まえ、選定

※所管省庁や関係セプター事務局と調整の上、対象事業者を選定

5.調査期間

2018年1月～2018年12月

6.調査結果

往訪先事業者等から得られた検証結果と良好事例を取りまとめた。

※調査対象を公表することにより事業者に不利益が生ずる可能性があるため、個社名は非公表

4.2．往訪調査結果（1/5）　経営層の関わり方について

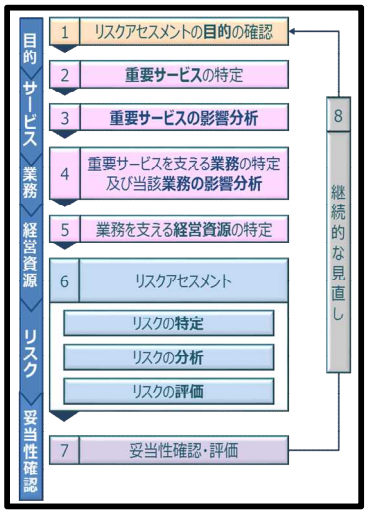
【経営層の働きかけ（トップダウン）】 経営層が情報セキュリティの積極的な取り組みを従業員に働きかけている。

- 東京オリンピック・パラリンピック競技大会や主要国首脳会議等のような国際的イベントに目標を合わせて、従業員の士気を上げながら情報セキュリティへの取り組みを加速させている。国際的イベントを見据え構築した情報セキュリティ体制を社内のレガシーとして定着化させることも視野に体制を整えている。
- 経営層が率先して情報セキュリティの取り組みは将来への投資であると説明し、情報セキュリティの取り組みを先導している。

■経営層の働きかけ

- 国際的イベントを万全な設備・組織体制で迎えられるように、重要システムに対するリスクアセスメントを実施し、改善活動をしている。また、過去の国際的イベントで発生したサイバー攻撃の事例を洗い出し、社員への情報共有及び対策状況の確認・対策の実施を指示している。
- 国際的イベントに向けて構築している情報共有体制やインシデント対応の規則・基準等をレガシーとして、定着化させている。
- 経営層が情報セキュリティの改善活動を統括する立場になり、セキュリティ連絡部会を発足し、平時からの情報共有やPDCAに沿った改善活動を行い、組織的な情報セキュリティ体制を構築している。また、毎月セキュリティ連絡部会を開催し、経営層が直接進捗を確認している。さらに、サイバーセキュリティの資金はコストではなく、投資であると経営層自ら社員に説明し、活発な取り組みを経営層が先導している。

リスクアセスメント手順



【経営層への働きかけ（ボトムアップ）】 従業員が経営層に、情報セキュリティの動向を報告し、経営層の積極的な関与を促している。

- 情報セキュリティのインシデント情報や政府の動向等の最新情報を経営層に定期的に報告し、経営層の積極的な働きかけを促している。

■経営層への働きかけ

- 流行しているサイバー攻撃やマルウェアの傾向等の情報を収集し、自社の重要システムが被害を受けた場合に想定される重要サービス支障の大きさを分析し、経営層に報告している。また、リスクを除去するために必要な設備対策や人材配置等の意見具申を行い、経営層を巻き込んだ取り組みを活性化させている。
- 政府が求める取り組みや同業他社の取り組み等を経営層に説明して、情報セキュリティの取組みにおける自社の状況と自社が取り組むべき事項を報告し、経営層と改善活動を行っている。

報告内容（例）

■最新動向
・インシデントの動向
・政府や同業他社の動向（取り組み状況）

■世間のインシデント状況
・流行しているサイバー攻撃の事例
・マルウェアに感染した場合の想定される被害

■その他
・リスクアセスメントの結果
・必要な設備・人的対策　等

4.2．往訪調査結果（2/5）　演習や訓練について

【インシデント発生を予防する訓練】 サイバー攻撃の被害を受けないための訓練・演習を実施している。

- 標的型攻撃やマルウェア感染等のサイバー攻撃を受けないように、平時から全従業員に対して、訓練や演習を行い、危機意識を高めている。

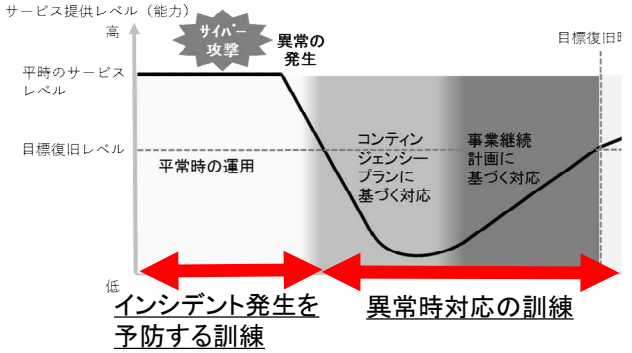
■ 標的型攻撃メール訓練

- 業務関係者を模した巧妙なメールを送り、標的型攻撃メール攻撃を体験し、情報セキュリティの危機意識を高めている

✓ 訓練の頻度：年間３回程度

✓ 訓練対象者：全従業員（契約社員含む）

✓ 訓練の手段：事前告知なしで標的型攻撃メールを模した訓練メールを送付



【異常時対応の訓練】 重要インフラサービスの提供に支障が発生した場合を想定した訓練・演習を実施している。

- 自社や政府の演習・訓練を活用して、コンティンジェンシープラン（CP）と事業継続計画（BCP）の機能とインシデント対応力の確認・改善を行っている。
- 新システム導入によって生じる初動対応の変更点等を周知し、訓練を通じてインシデント対応の流れを定着させ、インシデント対応力の強化を図っている。

■ CPとBCPの発動を想定した訓練実施（自社訓練）

- サイバー攻撃の被害を受けている想定の下、規則・基準・対応マニュアルに則り、正しい判断・行動や社内連携ができるかを検証している。

✓ 訓練の頻度：年間１回程度

✓ 訓練対象者：従業員（契約社員含む）、ベンダ、メーカ
サービスを提供する上で関係する事業者　等

■ NISC主催の分野横断的演習の活用

- 分野横断的演習で、自社のリスクに合わせたシナリオを作成し、政府への情報連絡や社内連携、CPやBCPが発動した場合のインシデントの対応等を検証し、PDCAサイクルに沿った改善活動を行っている。

✓ 訓練の頻度：年間１回

✓ 訓練対象者：情報システム部門、制御部門、広報部門、ベンダ　等

■ e-learningを用いた訓練

- e-learningを用いて、マルウェア感染や標的型攻撃を受けた場合の被害を体験している。さらに、被害を受けた後の初動対応や報告等の一連のインシデント対応の流れをe-learningを用いて訓練している。

✓ 訓練の頻度：年間１回程度

✓ 訓練対象者：従業員（契約社員含む）

■ 新システムの導入を見据えたインシデント対応訓練

- 新システム導入により想定されるサイバー攻撃やシステム不具合の挙動を周知し、挙動を確認した場合の初動対応を確認している。また、新システム導入による初動対応の変更点を訓練を通じて、定着化させている。

✓ 訓練の時期：システム導入前

✓ 訓練対象者：重要システム関係者（運用者・保守員・設計者）

4.2．往訪調査結果（3/5） 情報共有体制について

【情報共有体制の構築】 情報セキュリティに関わる情報を担当者に早急に伝えるため、十分な情報共有体制を構築している。

- 社内では部署を跨いだ情報共有の仕組みを構築し、収集した情報を担当部署に適切に展開する体制を構築している。
- 社外からの情報収集窓口を複数設け、最新のインシデント情報を確実に収集できる体制を構築している。

■社内の情報共有（社内CSIRT）

- 重要システムを保守している制御部門が情報セキュリティに関わる対策を適切に行うため、情報システム部門や制御部門等で構成する社内CSIRTを結成すると共に、情報交換する連絡会を設けている。
- 情報セキュリティの取り組みが遅れがちである制御部門に対して、国内外の最新インシデント情報やCSMS認証等の紹介を行い、情報セキュリティへの取り組み意識を醸成させている。
- 情報セキュリティのインシデントが発生した場合、経営層や様々な部署がインシデント対応に関わることが想定されるため、対応に関わるメンバーで訓練に参加し、対応の流れの確認や課題の洗い出しを行い、体制の強化を図っている。

■グループ（親会社・子会社）内で情報共有

- 情報セキュリティのリソース（作業者、資金等）が不足している子会社も情報セキュリティの取組みを進めるため、親会社から子会社に情報セキュリティの情報提供を行い、協力して情報セキュリティに取り組んでいる。
  （情報共有の例）
  ・国内外の最新インシデント情報や政府の動向等の最新情報
  ・セキュリティポリシー,BCP,CP,対応マニュアル等の規則や内規類　等
- グループ外からの情報セキュリティに関わる情報は、リソースが豊富な親会社が統括的に管理し、必要な情報を担当者に直接展開している。

■日本CSIRT協議会との連携や地域的な取り組み

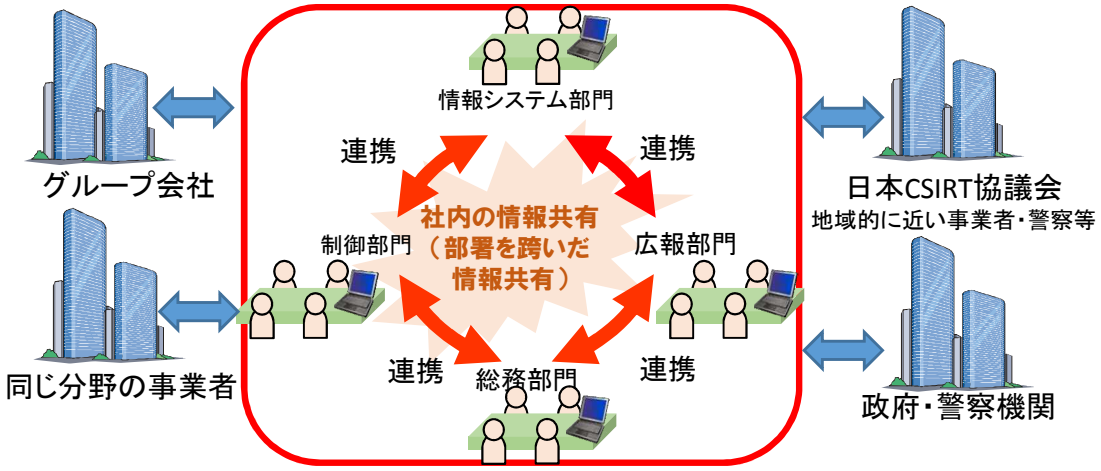
- 日本CSIRT協議会に加盟した事業者内でサイバーセキュリティの情報を共有している。
- 地域におけるセキュリティを守ることを目的に、最新情報を地域的に近い事業者や警察等と共有をしている。

■警察機関との連携

- サイバー攻撃を受けた場合、警察機関との早急な対応が求められることから、日頃から、警察機関と情報共有を行い、「顔の見える関係」を構築している。また、警察機関から情報セキュリティの情報を収集している。
- 警察機関が開催している訓練に参加し、警察機関との連携体制や情報共有すべき情報の再確認を行っている。

■同じ分野内での情報共有

- 分野内の事業者等が情報共有できる環境を設け、情報セキュリティに関する情報を共有している。
- 日頃の業務を通じて、担当者間の「顔の見える関係」が構築されている。その結果、見ず知らずの人と情報共有をするという障壁が少なく、意見交換が活発に行われていると共に、インシデント発生時に利害関係なく、相談・協力がされている。



4.2．往訪調査結果（4/5）　内部・外部犯行対策について

【内部犯行対策（人的リスク対策）】 悪意のある従業員や外部委託事業者の作業者から重要システムを守っている。

- 適切な情報資産の管理や閲覧・使用権限の設定を行い、従業員が不正な作業ができない環境を構築している。
- 外部委託事業者の不正な作業を防止するため、外部委託契約内容に対策事項を明記し、発注事業者と外部委託事業者の双方で管理している。

■情報資産の管理

- 情報セキュリティとして管理すべき情報資産（電子データや情報システム等）を洗い出し、経営上の影響度合いや関係法令上の規則に応じて、情報資産の重要度を明文化している。さらに、情報資産の重要度に準じて、閲覧権限や使用権限を設けている。その結果、従業員による内部犯行や目的外使用等を抑止する環境を構築されている。
- 運用上、最低限の従業員に特権IDを付与すると共に、特権IDの取得者同士で定期的に相互監視を行い、特権者の不正を防止している。
- 定期的に情報資産や使用・閲覧権限、特権ID等の棚卸を行い、情報資産を管理する上で、漏れがないか確認する体制が規則化されている。

■重要システムに関わる作業ログの監視

- 事前に申請（計画）した作業以外の作業がされていないか、作業終了後に、作業内容や権限変更等の作業ログを確認している。

■外部委託事業者との外部委託契約

- 内部犯行対策として有効な事項を外部委託契約書に明記し、発注事業者と外部委託事業者の双方で内部犯行を防止している。
  （外部委託契約書に明記した内部犯行対策の例）
  - ・重要システムに関わる申請外作業の禁止
  - ・重要システムに関わる作業の単独作業禁止
  - ・PCや外部記憶媒体の作業前セキュリティ更新プログラム（パッチ）の適用
  - ・作業者の条件に情報セキュリティ教育受講を追加　　等

■単独作業の禁止（作業監視者の配置）

- 重要システムに関する作業は、単独作業を禁止し、監視者を設けている。また、作業内容の事前確認を行い、悪意を持った作業の抑止や誤った作業を防止する体制が構築されている。
- 外部委託事業者のみの作業を禁止し、発注事業者が作業監視を行っている。

【外部犯行対策（物理的侵入防止策）】 重要インフラサービスの提供に係る重要な施設への物理的な侵入を防止している。

- 重要インフラサービスの提供に係る重要な施設（データセンタ、指令所、電気機械室　等）への施設出入り口に、監視カメラや侵入アラームを設置する対策や２要素認証対策の入退出管理システム等を設ける等の物理的侵入防止対策を設けている。

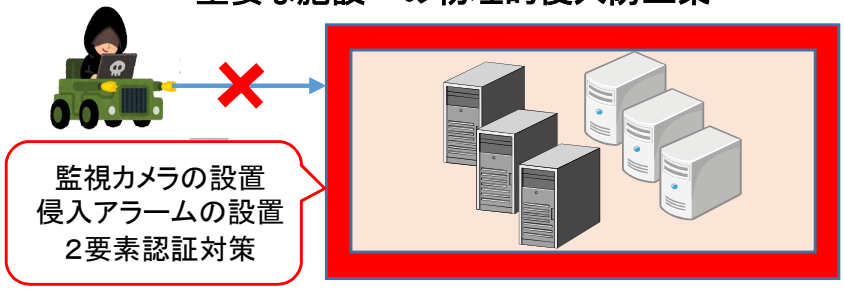
■監視カメラや侵入アラームの設置

- 重要インフラサービスの提供に係る重要な施設（データセンタ、指令所、電気機械室　等）の出入り口に監視カメラや侵入アラームを設置し、部外者の侵入防止と侵入された場合の早期発見ができる環境を設けている。

■　２要素認証対策の導入

- 重要インフラサービスの提供に係る重要な施設（データセンタ、指令所、電気機械室　等）への入退室には、記憶・所持・生体情報のいずれか２つ以上を用いた２要素認証を設け、部外者の侵入を防止している。

重要な施設への物理的侵入防止策



4.2．往訪調査結果（5/5） システムの出入り口対策について

【ネットワーク侵入対策（出入り口対策）】 重要システムへの侵入防止対策や侵入検知対策を行っている。

- 重要システムのリスクアセスメントを実施し、外部から重要システムにサイバー攻撃ができる経路を洗い出し、その侵入経路に必要な対策を実施している。
- 重要システムにマルウェアや不正なアクセスが発生した場合に、早期に異常を検知するため、ネットワーク侵入検知対策を実施している。

■保守用PCや外部記憶媒体（USBメモリ等）

- 保守用PCや外部記憶媒体（USBメモリ等）の正規の目的使用以外の使用を禁止し、マルウェア感染等のリスクを低減させている。
- 保守用PCや外部記憶媒体の正規な目的使用は、管理者の承認を得てから使用するという運用を規則化し、万が一、マルウェア感染が発生した場合に感染経路を特定し、迅速な処置がされている。
- 保守用PCや外部記憶媒体の管理者および重要システムの管理者は、定期的かつ作業前に、セキュリティ更新プログラム（パッチ）を適用することを規則化させ、マルウェア感染等のリスクを低減させている。

■インターネット

- 従来、制御システムはクローズドな環境で運用してきたが、一部の制御システムの情報（発電情報、運行情報　等）をインターネット経由で公開する運用が求められるようになった。そこで、境界に片方向のゲートウェイ（データダイオード）を導入し、外部からの不正なアクセスを防止している。
- 不正なアプリケーションの実行や不審なウェブサイトへのアクセス制限させるため、ホワイトリストまたはブラックリスト型のFWを設けている。また、最新情報の収集を行い、必要に応じてFWの設定を更新している。

■メンテナンス回線

- メンテナンス（保守）用の回線は、一貫して自社で敷設・管理した信頼性の高い専用回線を用いている。
- 平時は、専用回線を接続しておらず、メンテナンスや異常時対応等の場合に限り接続するという運用ルールを用いている。インシデント発生時等のメンテナンス回線を接続する場合は、作業終了後に作業ログを確認し、不正な作業をおこなっていないか確認している。

■メールやファイルのダウンロード

- 外部から不審なメールを受信させないように、送信元や添付ファイル等を確認するシステムを導入している。
- 不審なデータやファイルをダウンロードしないように、ダウンロードするデータやファイル等に規制を設けている。

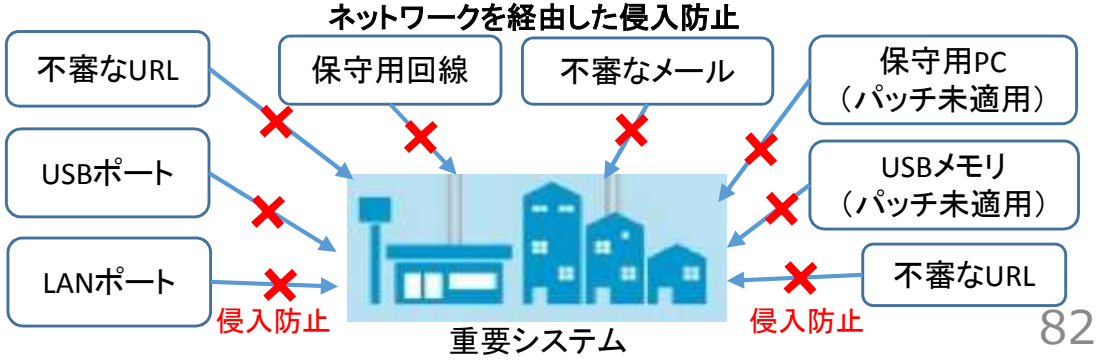
■ USBポートやLANポート

- 未使用のUSBポートやLANポートから情報の窃取やサイバー攻撃等を防ぐ対策を導入している。
  （未使用のUSBポートやLANポート対策の例）
  - ・空きポートを物理的に塞ぐ
  - ・承認されていない機器が接続されても検知させない
  - ・承認されていない機器が接続された場合、アラームを鳴動させる　等

■ IPSやIDS等のネットワーク監視機器の導入

- 不正なアクセスや挙動が発生した場合に、早期に不具合を発見するため、IPS※1やIDS※2等のネットワーク監視機器を導入している。また、24時間365日の体制で機器の監視を行うと共に異常時の連絡体制を整備し、十分な初動対応体制を構築している。

※1 IPS（Intrusion Prevention System）：侵入防止システム
※2 IDS（Intrusion Detection System）：侵入検知システム



参考

参考１．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

参考１．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（BCP）の策定状況
設問20-1	事業継続計画（BCP）に基づいた訓練状況
設問20-2	事業継続計画（BCP）の見直し状況
設問20-3	事業継続計画（BCP）の見直し契機
設問21	コンティンジェンシープラン（CP）策定状況
設問21-1	コンティンジェンシープラン（CP）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

参考１．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（BCP）・コンティンジェンシープラン（CP）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（BCP）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）