資料２

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

2016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

2017年３月２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、2016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）

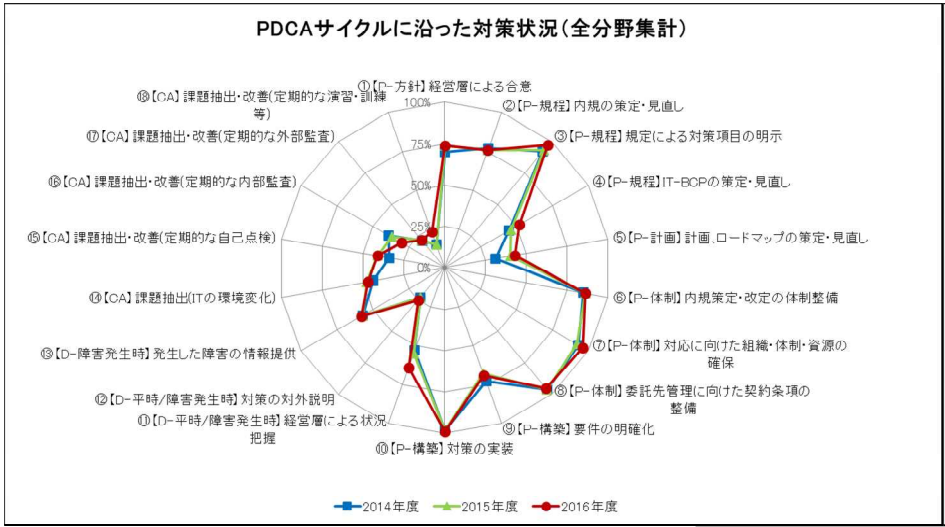
2．調査結果の要約

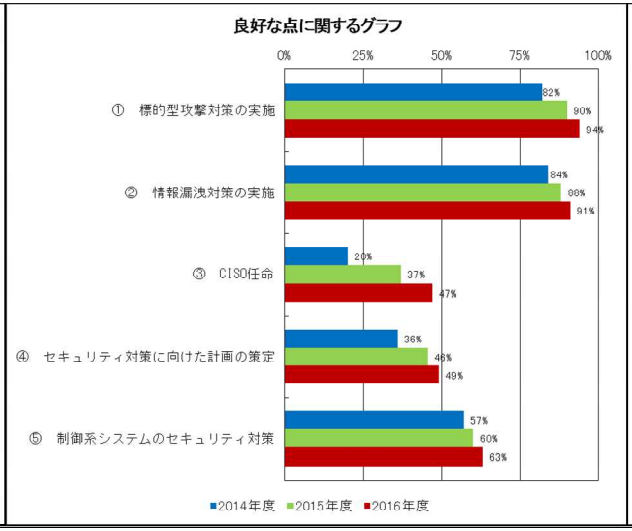
(1) 良好な点

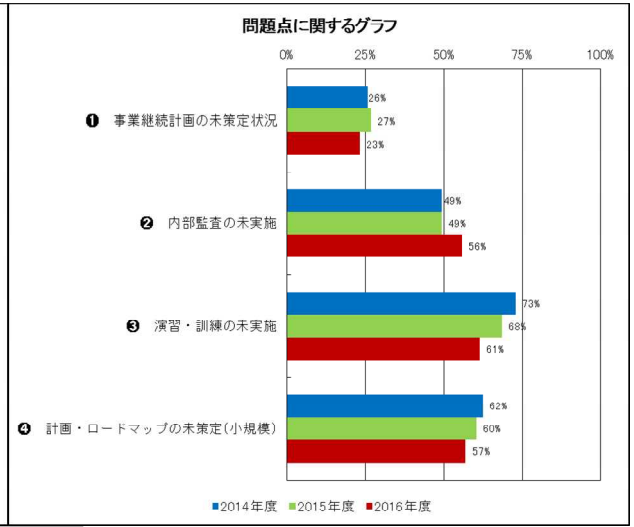
- 社会問題となっている標的型攻撃、情報漏えい等のリスクへの関心が高く、対策も進んでいる様子がうかがえる。(下中図①,②)
- 経営層の関与が高まるとともに、計画的に情報セキュリティ対策に取り組む事業者の数が増加している。(下中図③,④)
  ※往訪調査（P.32~35参照）でも同様の意見あり
- 情報系システムだけでなく、制御系システムに対するセキュリティ対策の意識が高まっている。(下中図⑤)

(2) 問題点

- 事業継続計画の必要性や、課題抽出における演習・訓練や監査の有効性に関し、事業者の理解を促進する必要がある。(下右図❶,❷,❸)
  ※往訪調査（P.32~35参照）でも同様の意見あり
- 小規模な事業者(概ね100名以下)の多くが、情報セキュリティ対策の推進に係る内規や計画・ロードマップを策定していない。(下右図❹)
- サイバーセキュリティ戦略等でCSIRT設置の必要性が指摘されているが、設置している事業者は20%程度に留まっている。(2016年度から調査)







アンケート配布は3,302事業者等。回答は3,144事業者等。

(3) 今後の対応

- 事業継続計画の必要性や演習・訓練及び監査の有効性等について、事業者の理解を促進する（指針の改定等）。
- 事業者への往訪調査等を通じて、CSIRT設置の詳細状況の把握や、小規模事業者の課題に関する原因分析を進める。
- 指針や安全基準等に関する意見を踏まえ、指針の改定を実施する。また、調査票の見直しを行うことにより、アンケート回答の負担を軽減しつつ、情報セキュリティ対策の取組状況を詳細に、かつ効率的に確認し、重要インフラ防護施策への更なる活用を図る。

◆調査内容
①安全基準等の整備・浸透に係る事項：指針※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

◆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、2016年3月末日
調査方法②の場合、各調査で設定した基準日

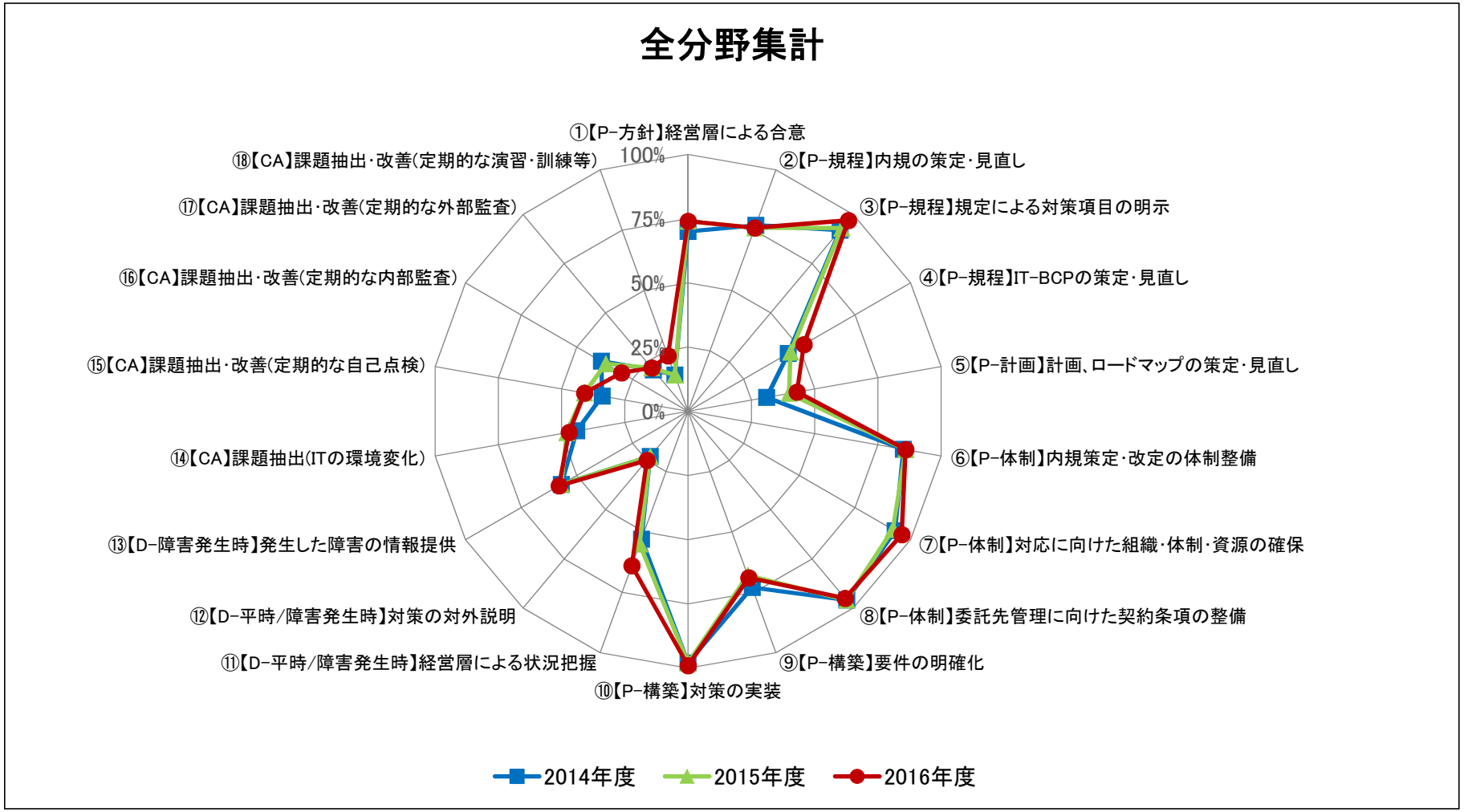
3．各重要インフラ分野の調査状況

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	電気通信事業者（一部抽出）	85	69	NISC調査
	ケーブルテレビ	一般社団法人日本ケーブルテレビ連盟加盟事業者のうち一定要件を満たすケーブルテレビ事業者	334	294	
	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）、一般社団法人日本民間放送連盟	194	191	
金融		銀行等、証券会社、生命保険会社、損害保険会社	650	566	独自調査 (*1)
航空	航空運送	航空運送事業者	2	2	NISC調査
	航空管制	官庁	2	2	
鉄道		ＪＲ、大手民鉄	22	22	
電力		一般電気事業者、日本原電(株)、電源開発(株)	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)
医療		病院情報システムを導入する病院	60	45	NISC調査
水道		給水人口30万人以上の水道事業者、水道用水供給事業者	87	87	
物流		物流事業者、業界団体（一部抽出）	16	16	
化学		石油化学事業者	13	13	
クレジット		クレジットカード会社等	18	18	
石油		石油精製・元売事業者	9	9	
全分野合計		－－－	**3,302**	**3,144**	－－－

＊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：2016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：2015年4月1日）

4．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

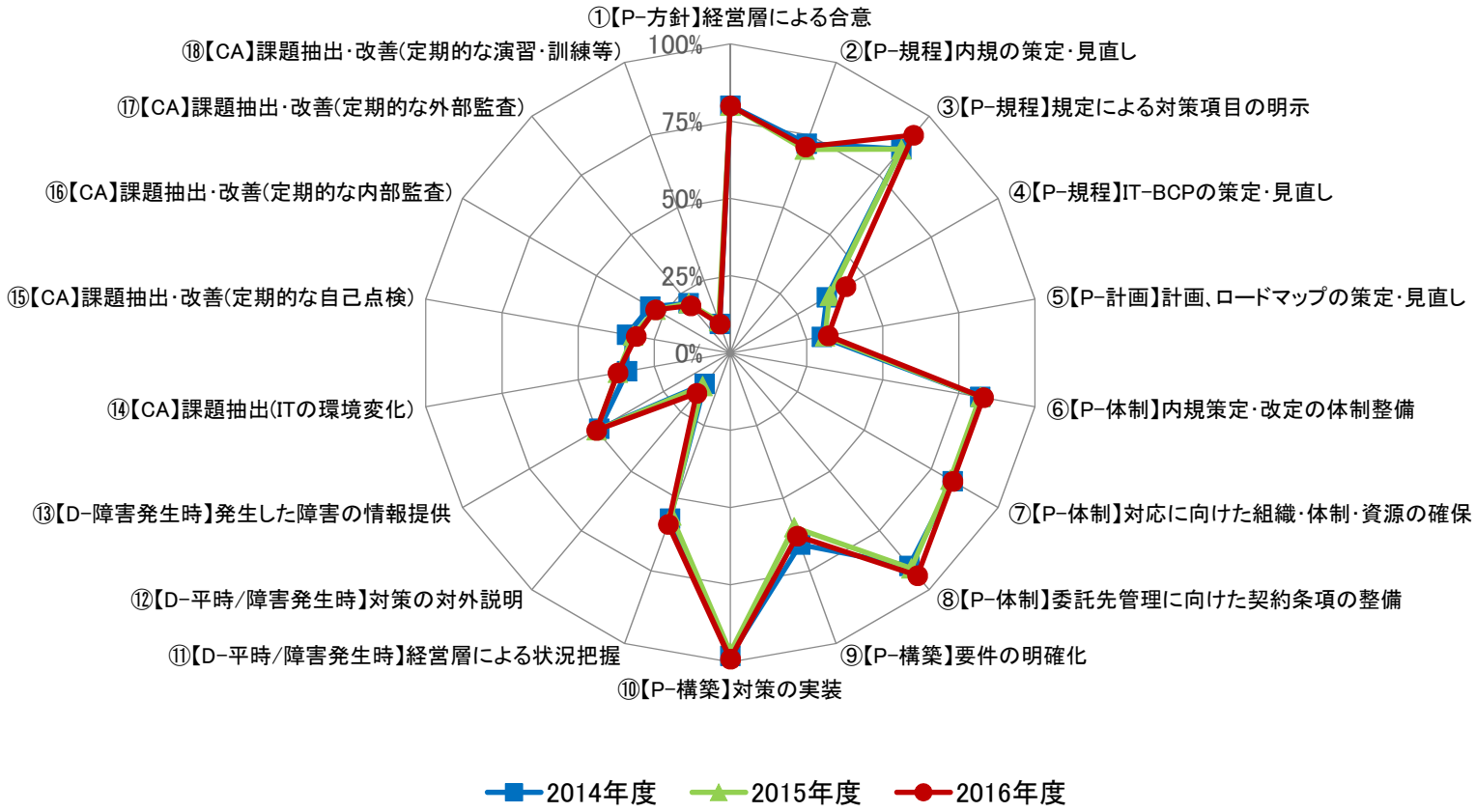


項目	2014年度	2015年度	2016年度
①	70%	74%	74%
②	77%	76%	76%
③	92%	93%	97%
④	45%	46%	52%
⑤	31%	40%	43%
⑥	85%	86%	86%
⑦	93%	92%	96%
⑧	96%	96%	95%
⑨	73%	68%	69%
⑩	98%	98%	99%
⑪	53%	55%	64%
⑫	23%	23%	25%
⑬	57%	57%	58%
⑭	44%	48%	47%
⑮	34%	41%	41%
⑯	39%	37%	30%
⑰	21%	22%	22%
⑱	15%	15%	23%

※ ①、③、⑫については、政府・行政サービス分野における独自調査結果の読替を実施している。

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1000名未満の重要インフラ事業者

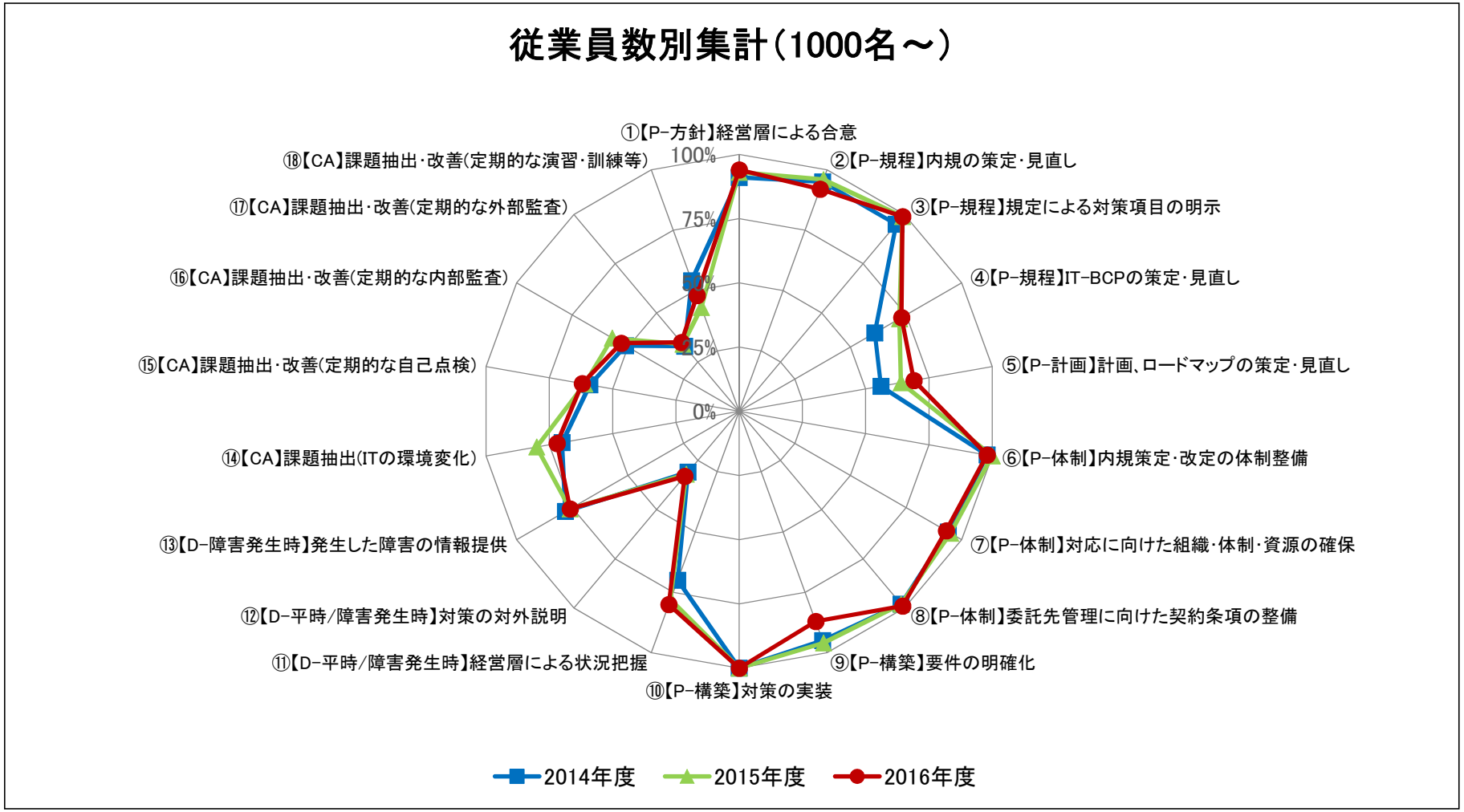


項目	2014年度	2015年度	2016年度
①	80%	80%	80%
②	72%	70%	71%
③	86%	86%	92%
④	36%	37%	43%
⑤	30%	31%	32%
⑥	82%	82%	83%
⑦	83%	82%	83%
⑧	90%	91%	94%
⑨	66%	60%	63%
⑩	98%	97%	99%
⑪	57%	56%	59%
⑫	13%	14%	17%
⑬	49%	50%	50%
⑭	34%	37%	37%
⑮	34%	32%	31%
⑯	30%	28%	28%
⑰	21%	21%	20%
⑱	10%	11%	10%

※従業員数が不明な回答（独自調査を読み替える金融、政府・行政サービス分等）は、集計していません。

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1000名以上の重要インフラ事業者

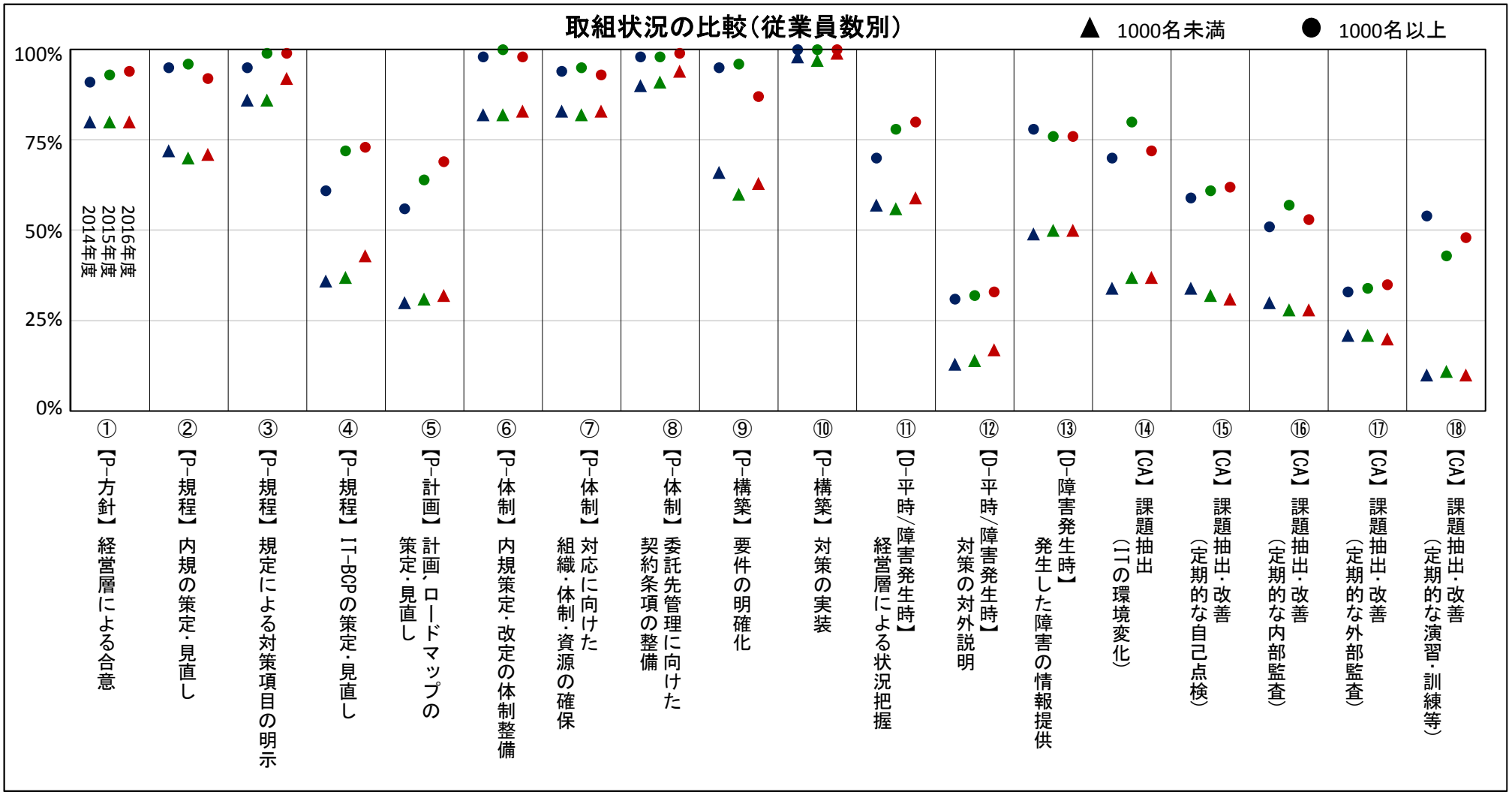


項目	2014年度	2015年度	2016年度
①	91%	93%	94%
②	95%	96%	92%
③	95%	99%	99%
④	61%	72%	73%
⑤	56%	64%	69%
⑥	98%	100%	98%
⑦	94%	95%	93%
⑧	98%	98%	99%
⑨	95%	96%	87%
⑩	100%	100%	100%
⑪	70%	78%	80%
⑫	31%	32%	33%
⑬	78%	76%	76%
⑭	70%	80%	72%
⑮	59%	61%	62%
⑯	51%	57%	53%
⑰	33%	34%	35%
⑱	54%	43%	48%

※従業員数が不明な回答（独自調査を読み替える金融、政府・行政サービス分等）は、集計していません。

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1000名未満と1000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	
	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●
2014年度	80%	91%	72%	95%	86%	95%	36%	61%	30%	56%	82%	98%	83%	94%	90%	98%	66%	95%	98%	100%	57%	70%	13%	31%	49%	78%	34%	70%	34%	59%	30%	51%	21%	33%	10%	54%
2015年度	80%	93%	70%	96%	86%	99%	37%	72%	31%	64%	82%	100%	82%	95%	91%	98%	60%	96%	97%	100%	56%	78%	14%	32%	50%	76%	37%	80%	32%	61%	28%	57%	21%	34%	11%	43%
2016年度	80%	94%	71%	92%	92%	99%	43%	73%	32%	69%	83%	98%	83%	93%	94%	99%	63%	87%	99%	100%	59%	80%	17%	33%	50%	76%	37%	72%	31%	62%	28%	53%	20%	35%	10%	48%

※従業員数が不明な回答（独自調査を読み替える金融、政府・行政サービス分等）は、集計していません。

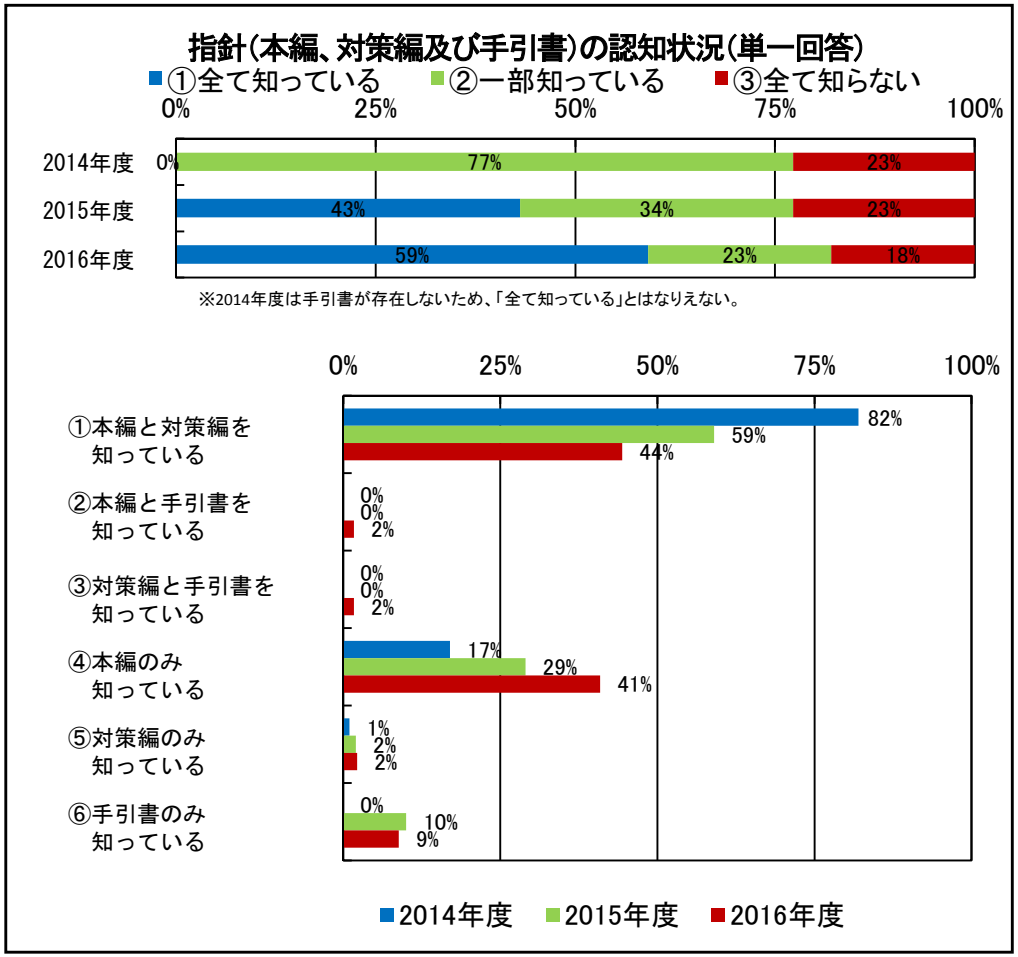
5．調査結果詳細 －（1/19）－

(1) 安全基準等の整備状況

① 指針の認知

(a) 指針（本編、対策編及び手引書）の認知状況

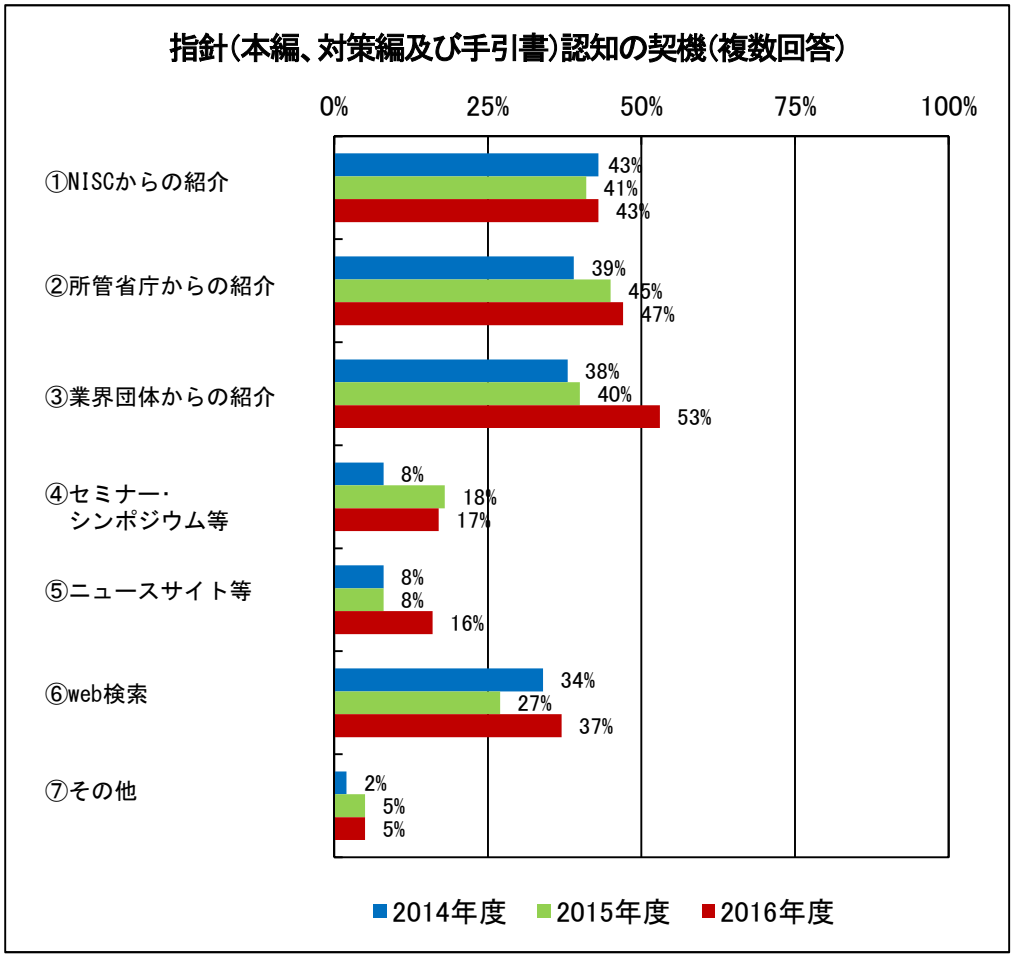
・指針本編、対策編、手引書の全てを知っている事業者は着実に増えてきていると認められる。
・2割弱の事業者は指針を全く知らないため、引き続き認知度向上に向けた取組を行う必要がある。



※金融、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）
※2015年度に手引書を新たに作成したことに伴い、集計方法を変更

(b) 指針（本編、対策編及び手引書）認知の契機

・業界団体からの紹介が増えていることから、情報セキュリティ対策の水準の向上、サイバー攻撃への対応能力の向上に必要不可欠である、各業界の情報共有が進んでいることが認められる。



※金融、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）

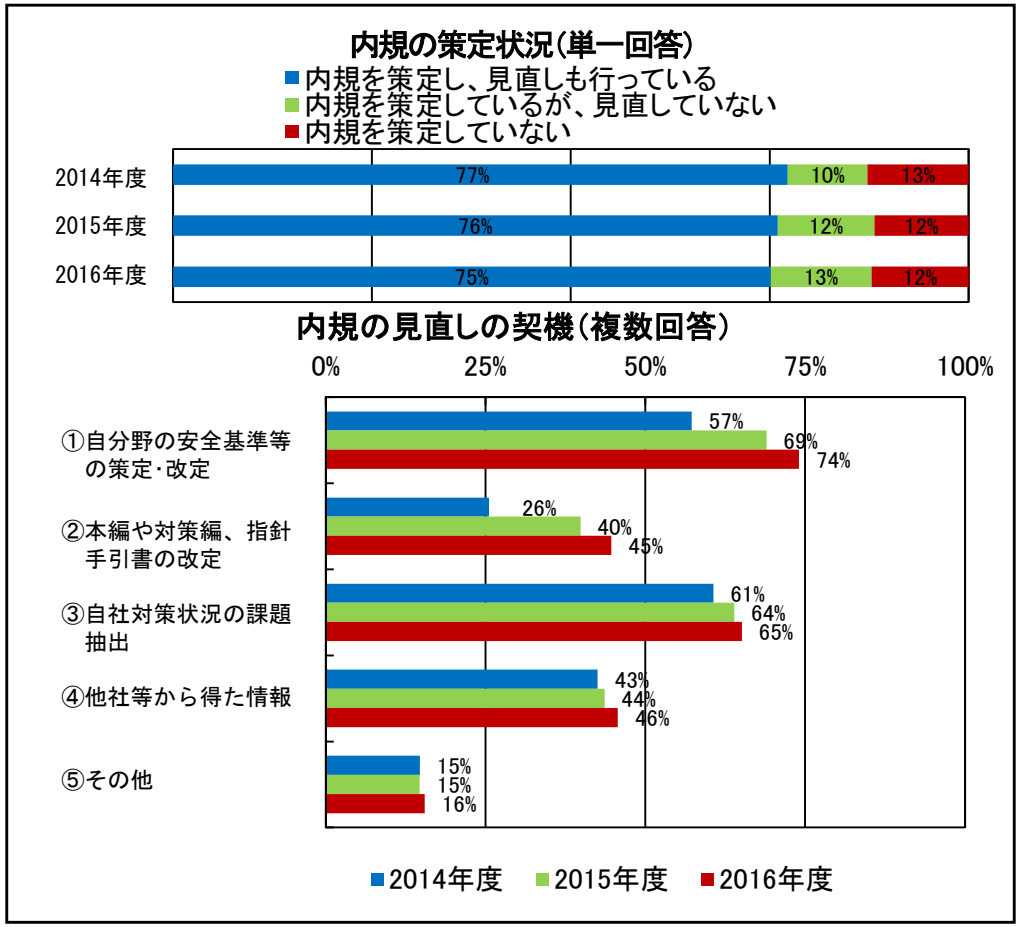
5．調査結果詳細 －（2/19）－

(1) 安全基準等の整備状況（続き）

② 内規の策定・見直し

(a) 内規策定・見直しの契機

・内規を策定していない事業者の約80%は100名未満の規模であり、今後も継続してアプローチする必要がある。
・安全基準等や指針の改定に合わせて内規を見直すといった、見直しの機会が着実に増えていることが認められる。



※金融、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）

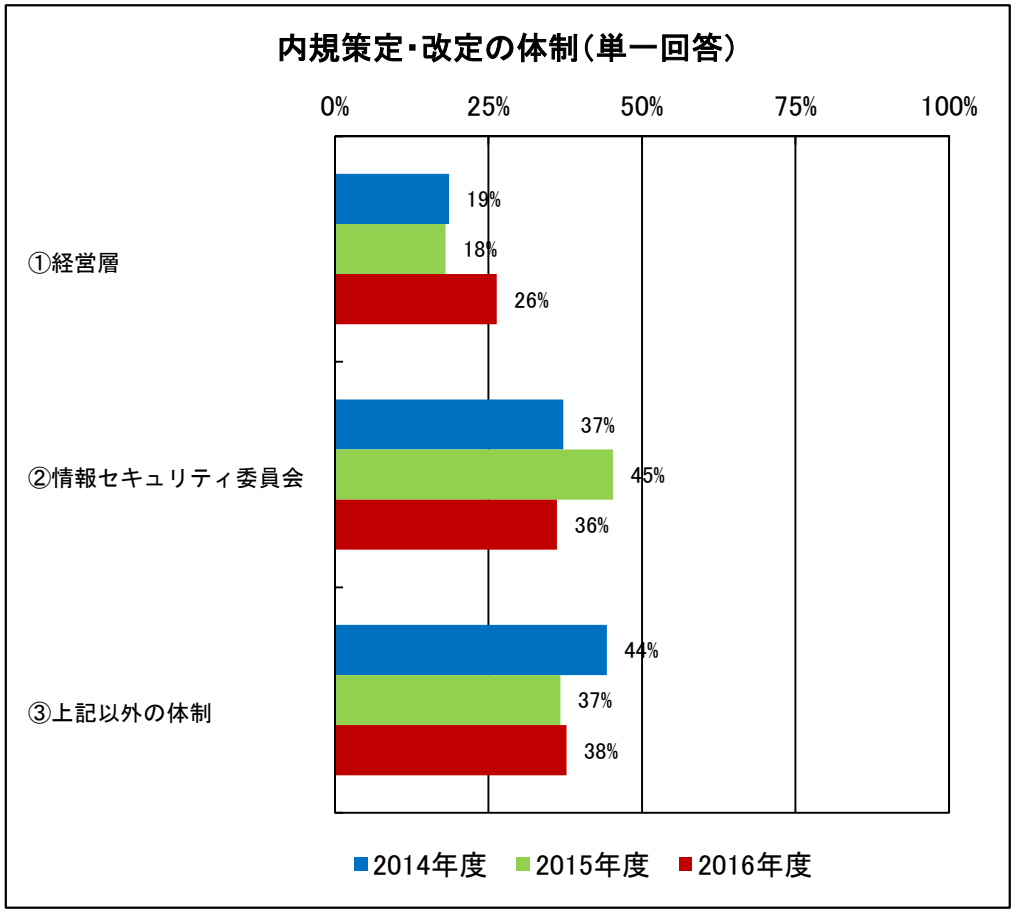
5．調査結果詳細 － (3/19) －

(1) 安全基準等の整備状況（続き）

③ 内規改定のプロセス

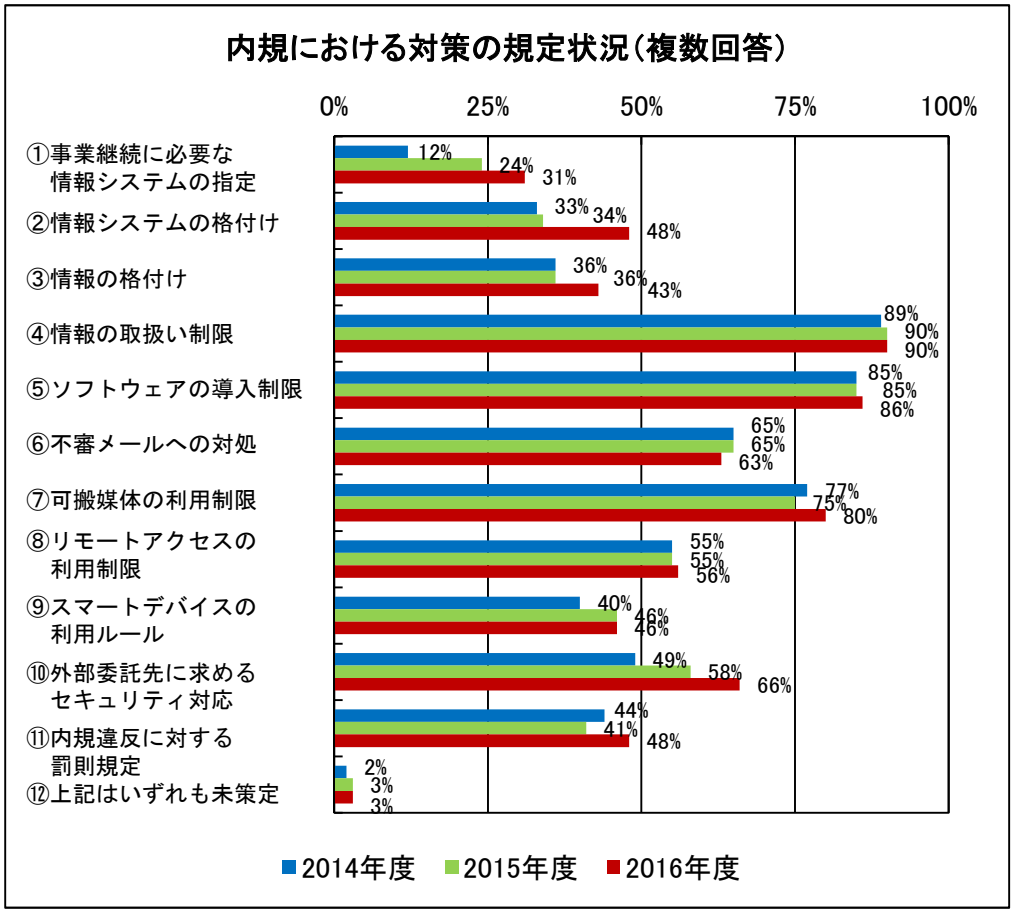
(a) 内規策定・改定の体制

・情報セキュリティ対策には経営層の関与が必要不可欠であるが、内規の策定・改定の体制に「経営層にて実施」の回答が増えていることから、経営層の意識が醸成されつつあると認められる。



(b) 内規における対策の規定状況

・直近数年間で委託先に起因するセキュリティインシデントが増えていること等を背景として、委託先に求めるセキュリティ対応が伸びたと推察される。



※金融、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）

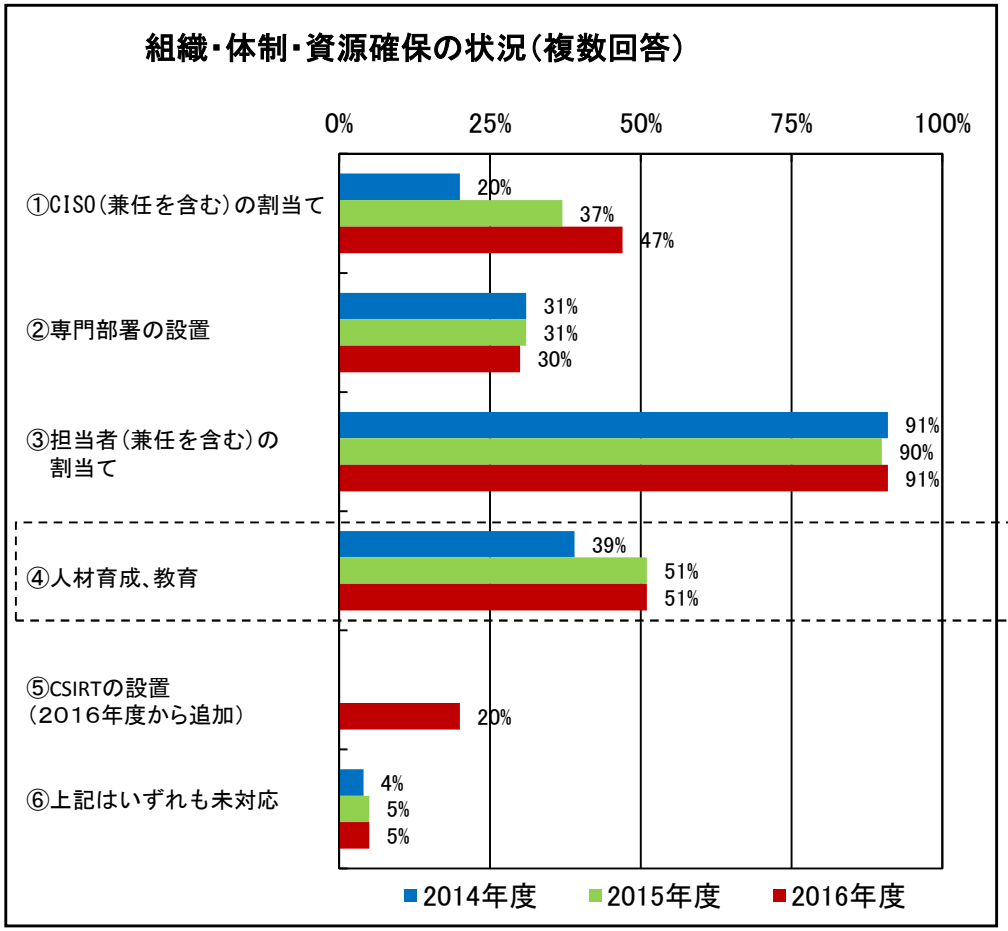
5．調査結果詳細 － (4/19) －

(2) 情報セキュリティ対策の実施状況

① 体制・資源の確保

(a) 組織・体制・資源確保の状況

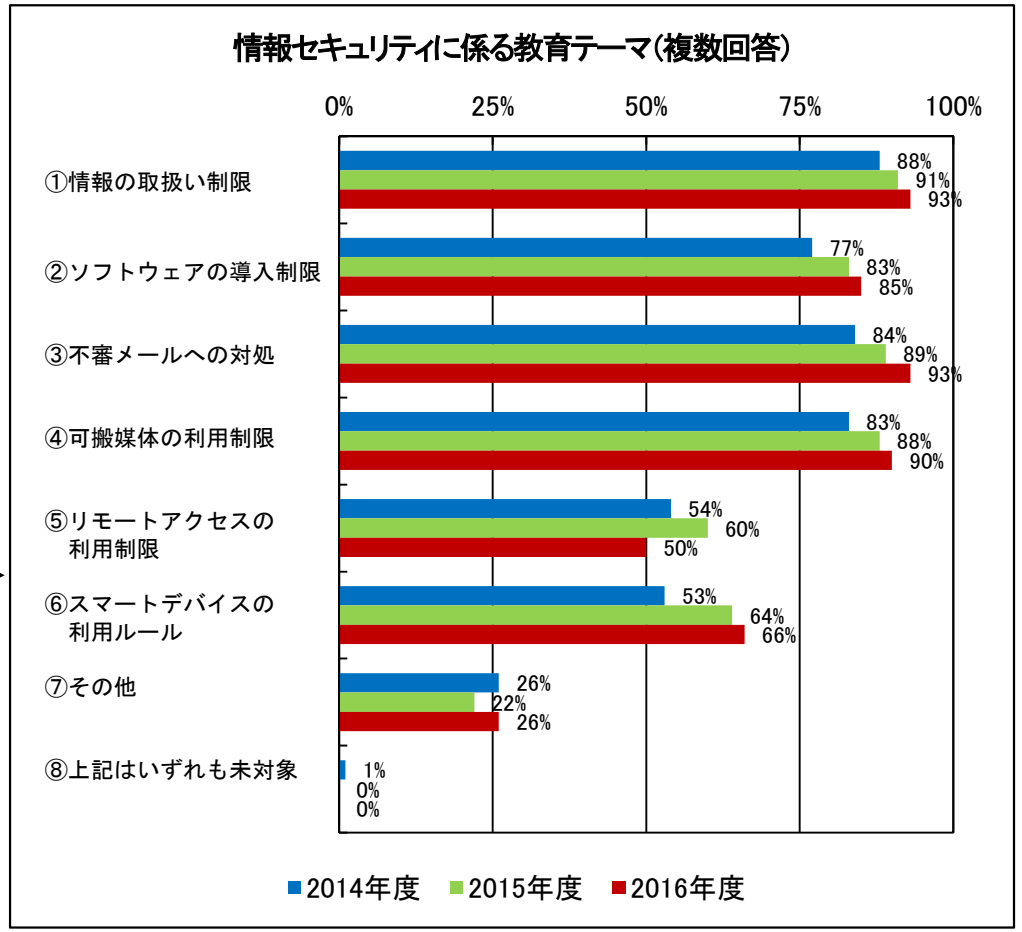
・CISOの割り当てが伸びていることから、情報セキュリティ対策に対する経営層の関与が増えたと認められる。
・CSIRTに関する一般の認知度は高まっているものの、設置している割合は多くない。



※金融は読替え可能項目なし（集計していません）

(b) 情報セキュリティに係る教育テーマ

・標的型攻撃メールの増加に伴い、不審メールに対する教育テーマが増えたと推察される。



※金融、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）

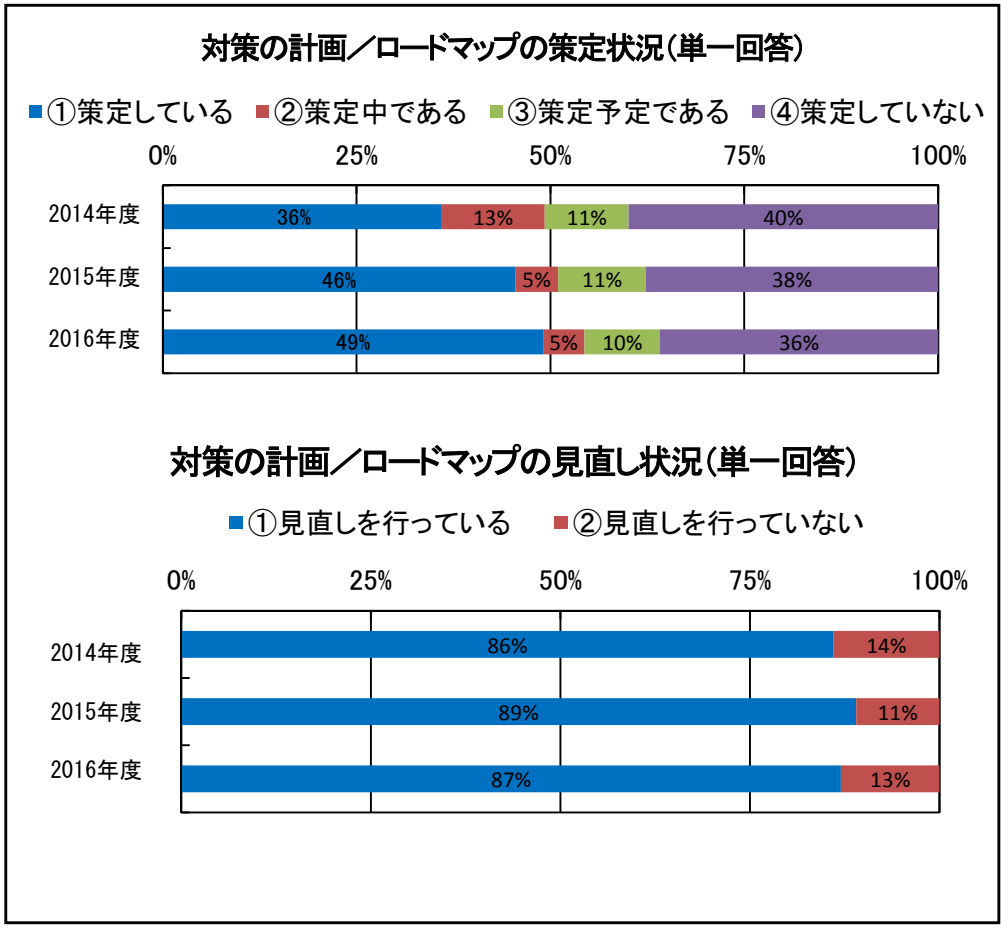
5．調査結果詳細 －（5/19）－

(2) 情報セキュリティ対策の実施状況（続き）

② 情報に係る対策

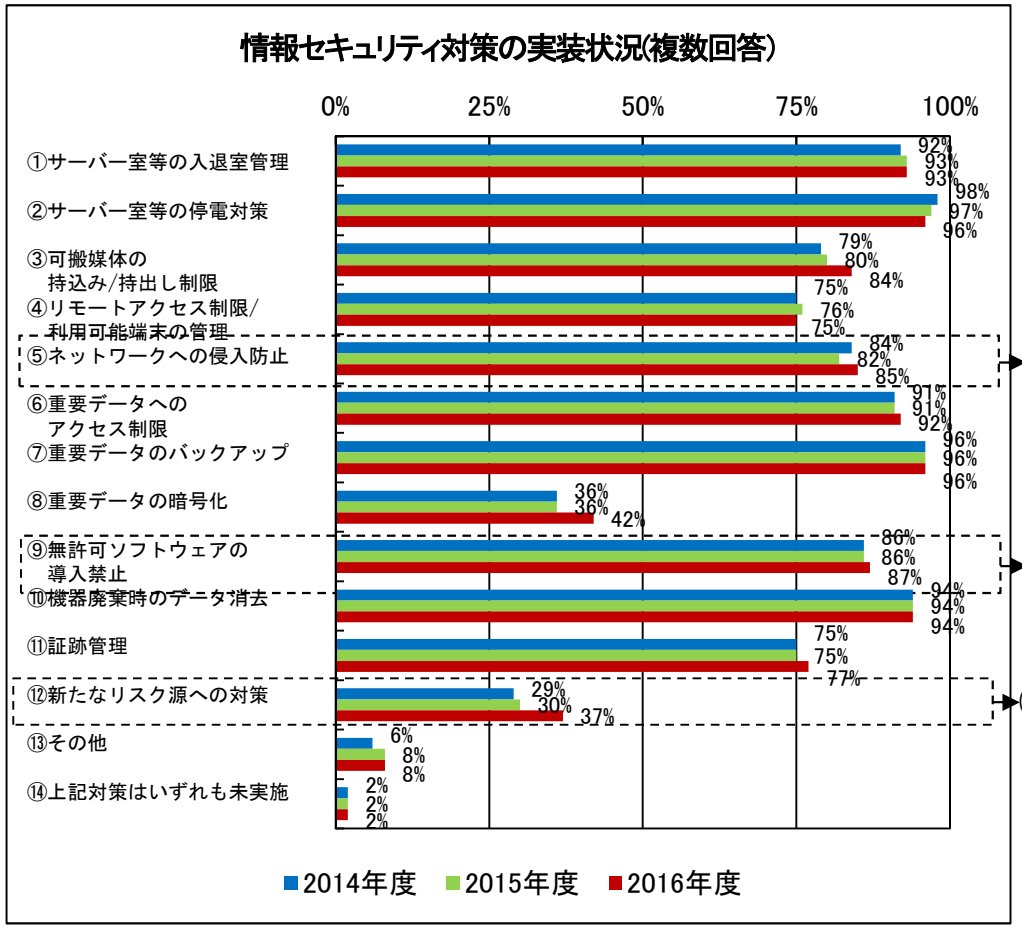
(a) 対策の計画／ロードマップの策定・見直し状況

・セキュリティ対策を計画的に実施する事業者が増えている。
・100名未満の事業者においては、計画/ロードマップの策定が行われおらず、原因分析が求められる。



(b) 情報セキュリティ対策の実装状況

・近年ランサムウェアによる被害が増えていることから、新たなリスク源への対策が増えていると推察される。



※金融、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）

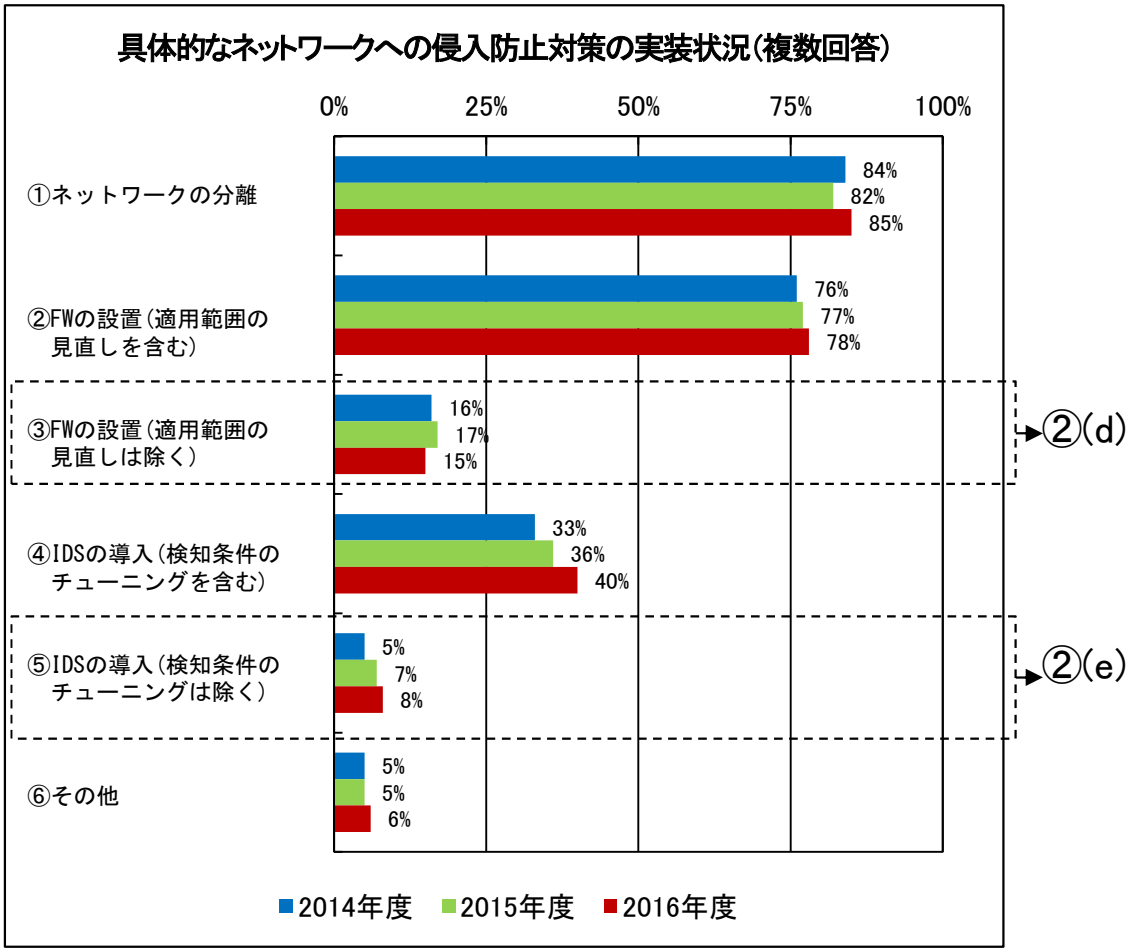
5．調査結果詳細 － (6/19) －

(2) 情報セキュリティ対策の実施状況（続き）

② 情報に係る対策

(c) 具体的なネットワークへの侵入防止対策の実装状況

・FWやIDSの導入効果を維持・向上させるには、定期的な見直し作業が必要不可欠であるという点について、指針等で啓発していく必要がある。



※金融、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）

※前設問(2)②(b)選択肢⑤選択事業者のみの回答

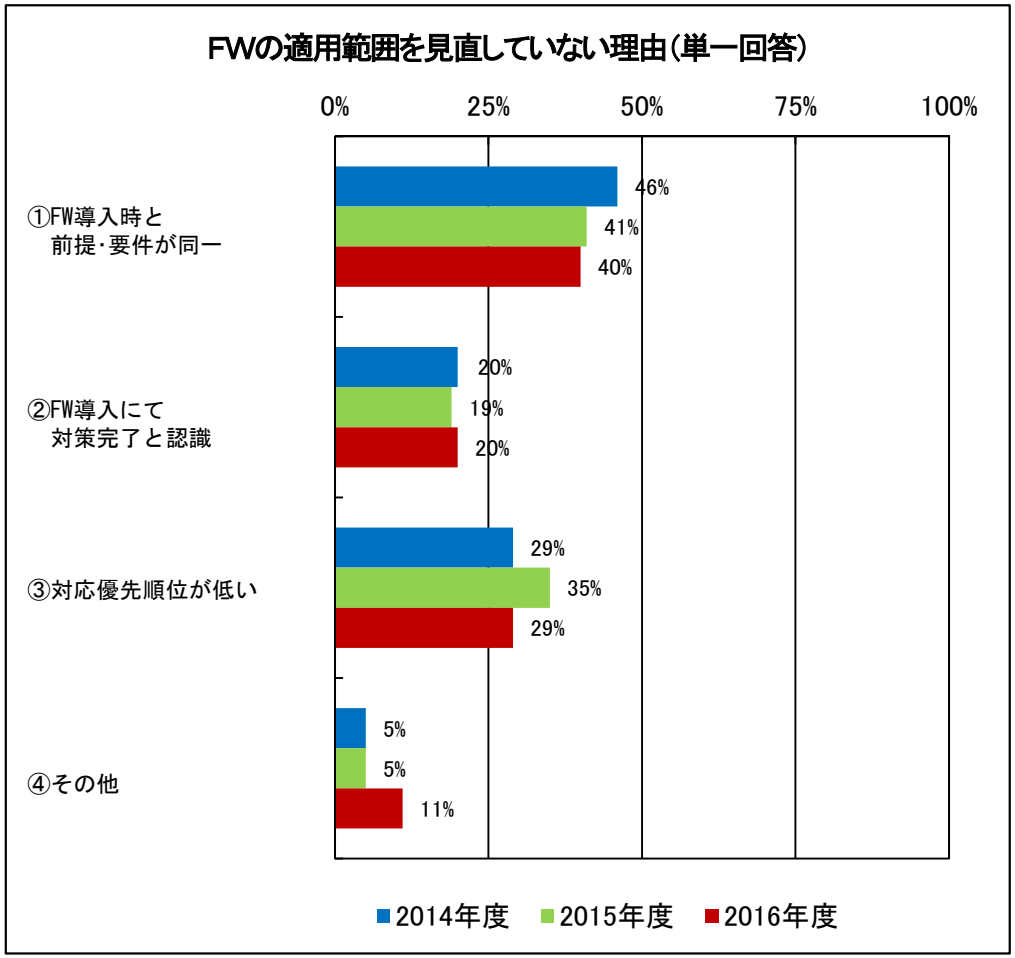
5．調査結果詳細 －（7/19）－

(2) 情報セキュリティ対策の実施状況（続き）

② 情報に係る対策

(d) FWの適用範囲を見直していない理由

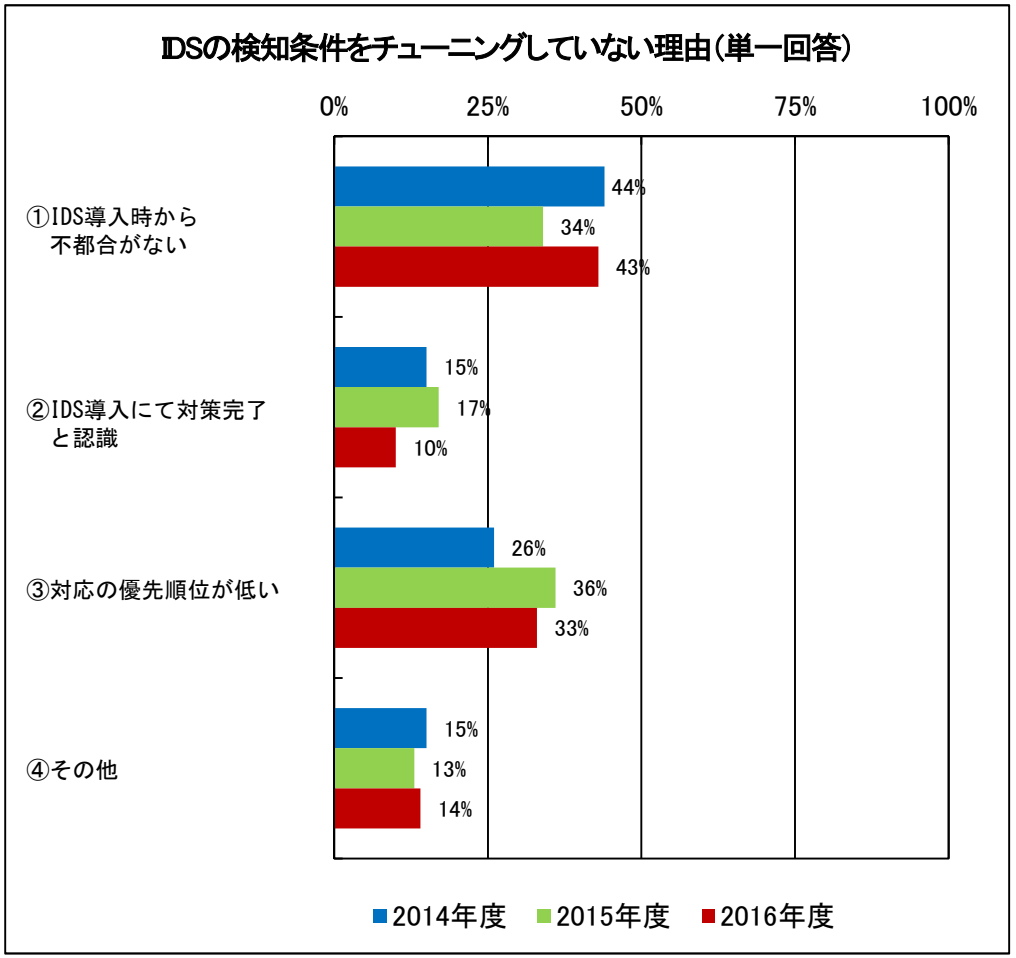
・FWの導入効果の維持・向上には、見直し作業が必要不可欠であること、また、その重要性・効果が組織内で理解され、取組につながるよう啓発していく必要がある。



※金融、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）
※前設問(2)②(c)選択肢③選択事業者のみの回答

(e) IDSの検知条件をチューニングしていない理由

・IDSの導入効果の維持・向上には、見直し作業が必要不可欠であること、また、その重要性・効果が組織内で理解され、取組につながるよう啓発していく必要がある。



※金融、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）
※前設問(2)②(c)選択肢⑤選択事業者のみの回答

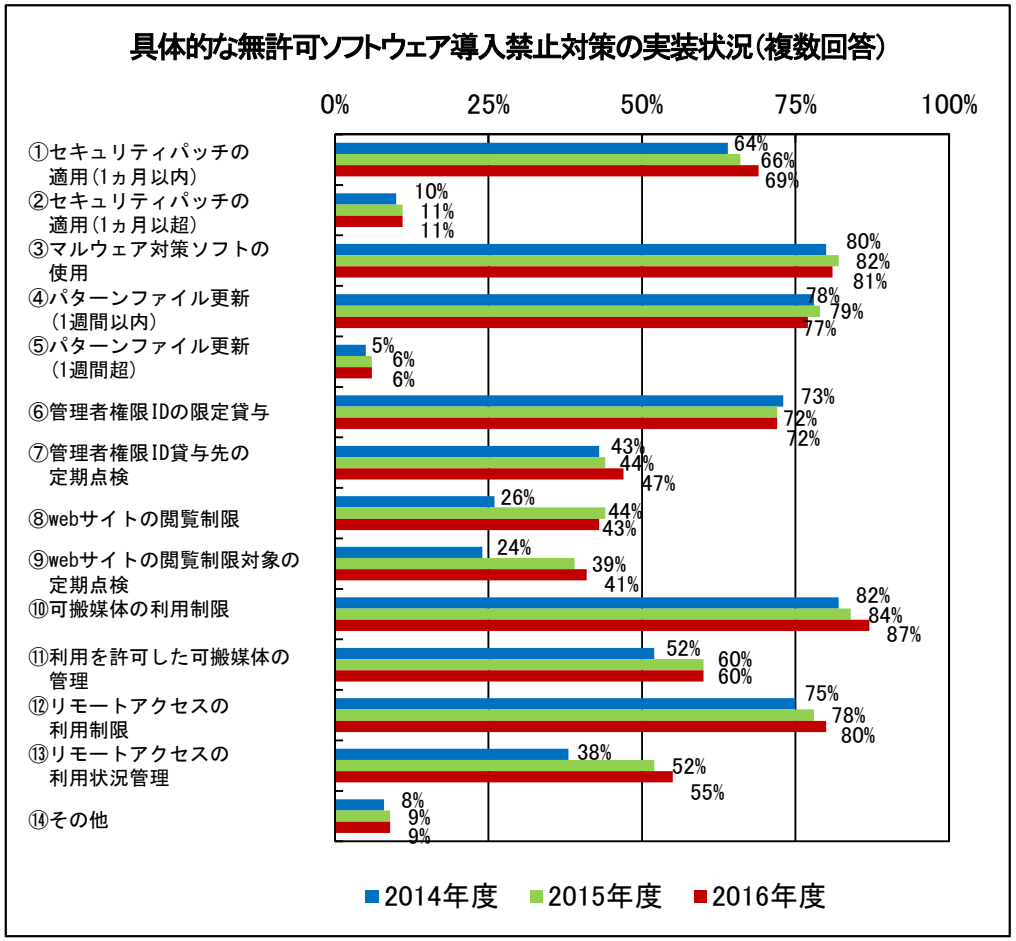
5．調査結果詳細 －（8/19）－

(2) 情報セキュリティ対策の実施状況（続き）

② 情報に係る対策

(f) PCにおける情報セキュリティ対策の実装状況

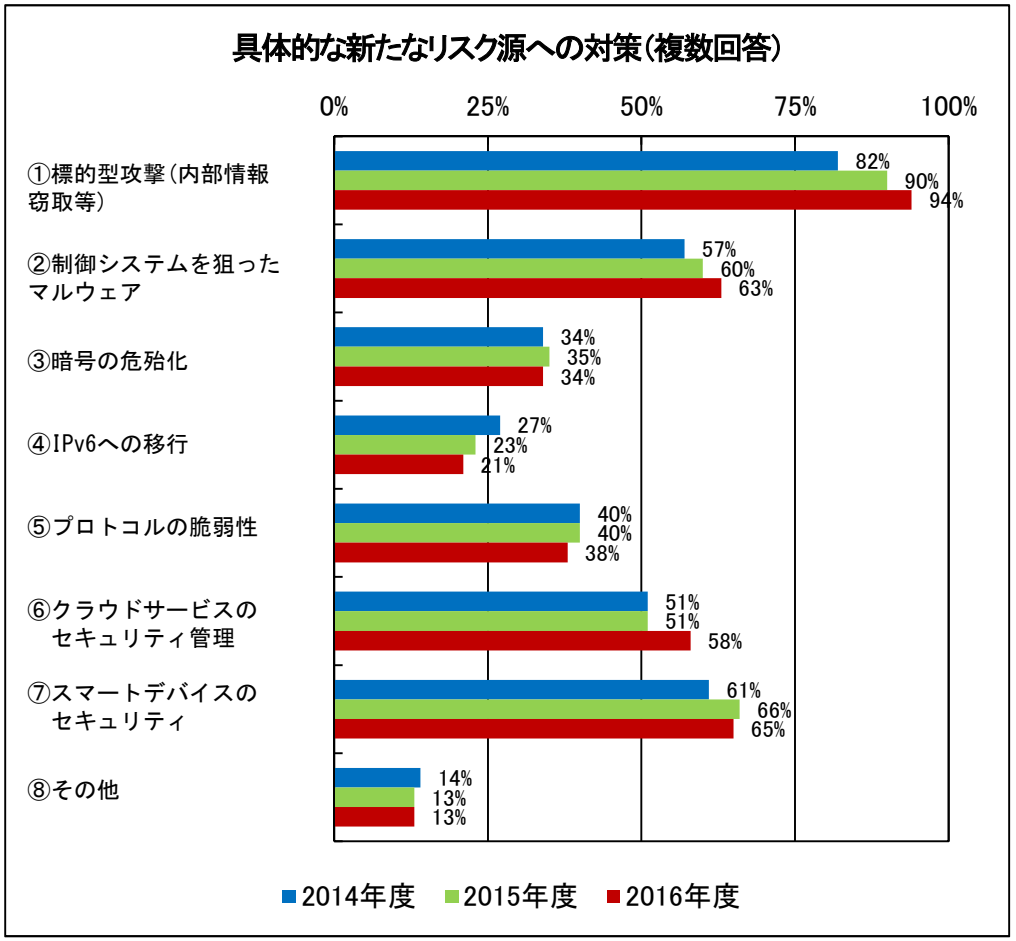
・可搬媒体の利用制限が伸びているが、昨今のスマートフォン等を利用した情報漏えい事例に対する対策のためと認められる。



※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）
※前設問(2)②(b)選択肢⑨選択事業者のみの回答

(g) 具体的な新たなリスク源への対策

・標的型攻撃の脅威が依然として高まっていることから標的型攻撃の対策が着実に伸びていると認められる。
・制御システムを狙ったマルウェアが伸びていることから、制御システムに対するセキュリティ意識が高まっていることが認められる。



※金融、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）
※前設問(2)②(b)選択肢⑫選択事業者のみの回答

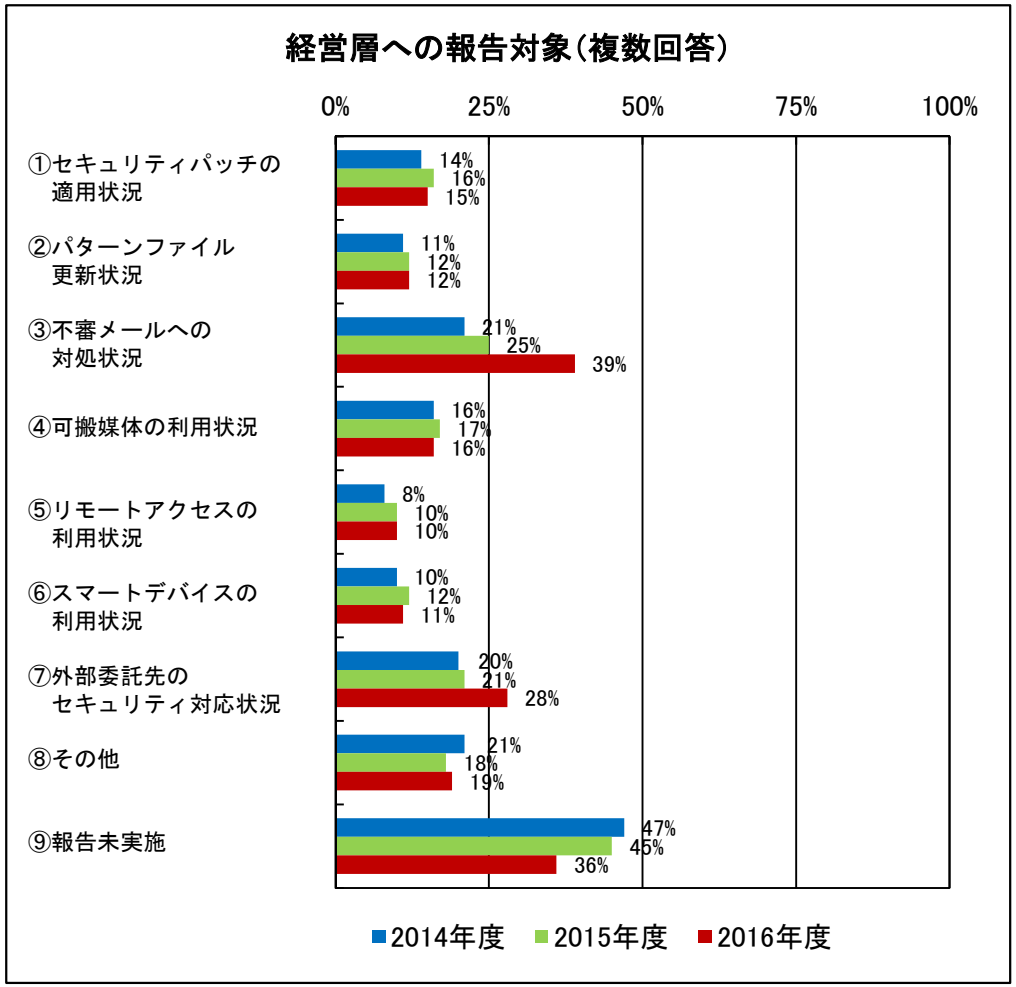
5．調査結果詳細 －（9/19）－

(2) 情報セキュリティ対策の実施状況（続き）

② 情報に係る対策

(h) 経営層への報告対象

・標的型攻撃メールは経営層を狙ったものが多いことから、不審メールへの対処状況に対する関心は高いと考えられる。
・昨今の情報漏えい事件を背景として、外部委託先のセキュリティ対策状況にも関心が高いと推察される。



※金融、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）

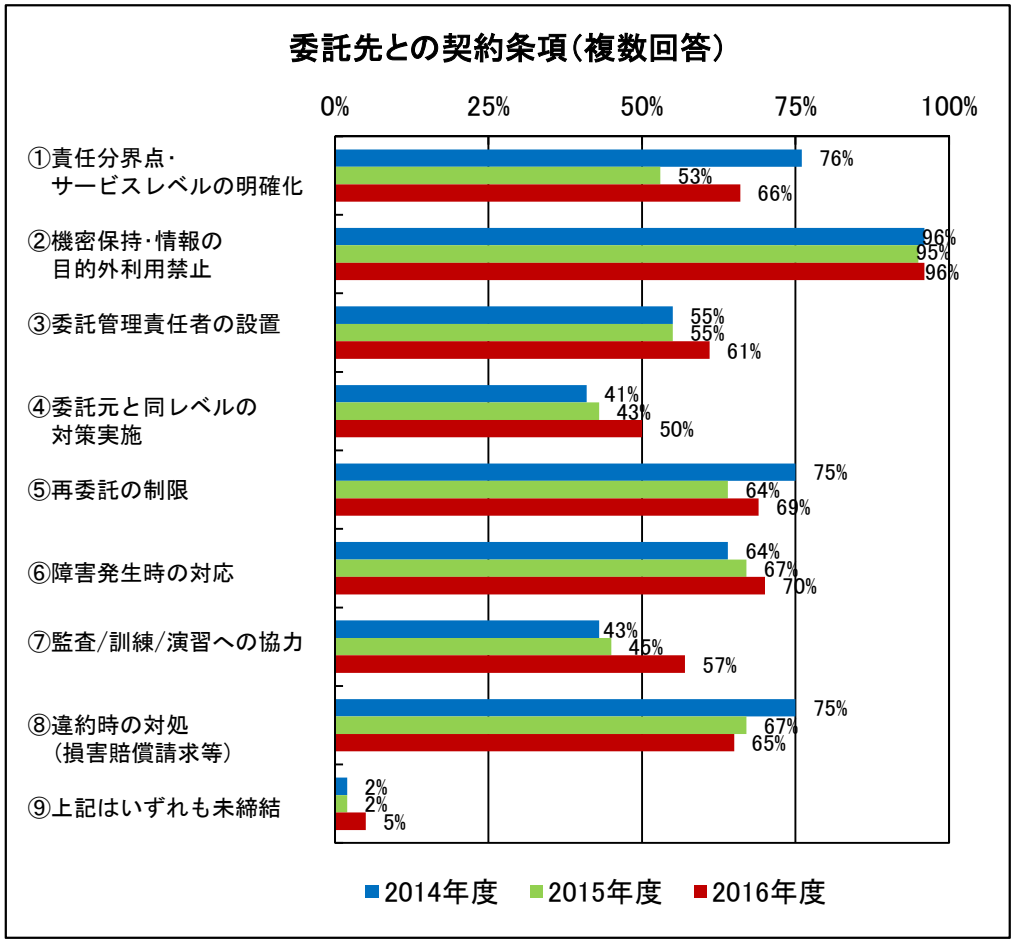
5．調査結果詳細 － (10/19) －

(2) 情報セキュリティ対策の実施状況（続き）

③ 要件の明確化

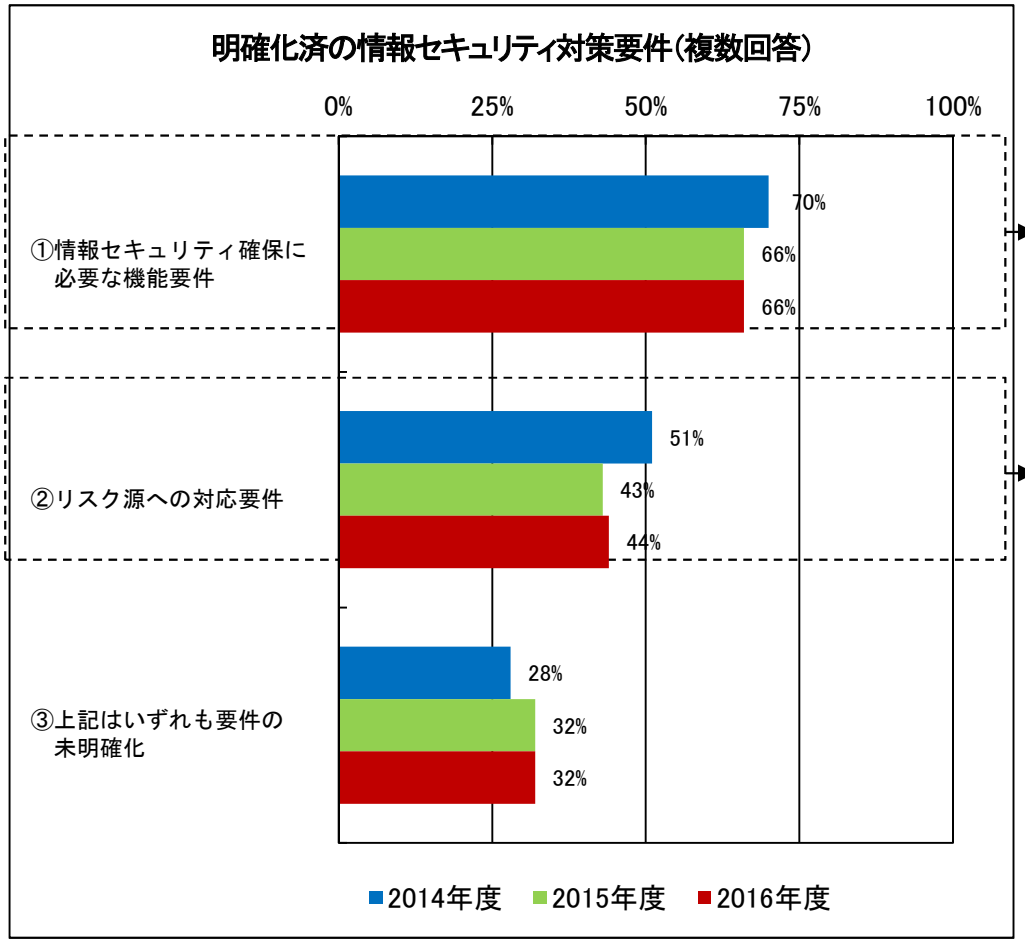
(a) 委託先との契約条項

・委託先も含めたセキュリティ対策が必要だと叫ばれる中、委託先との契約の中で監査/訓練/演習への協力を求める事業者が増加したと認められる。



(b) 明確化済の情報セキュリティ対策要件

・要件の明確化に関する大きな変化はない。



※金融、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）

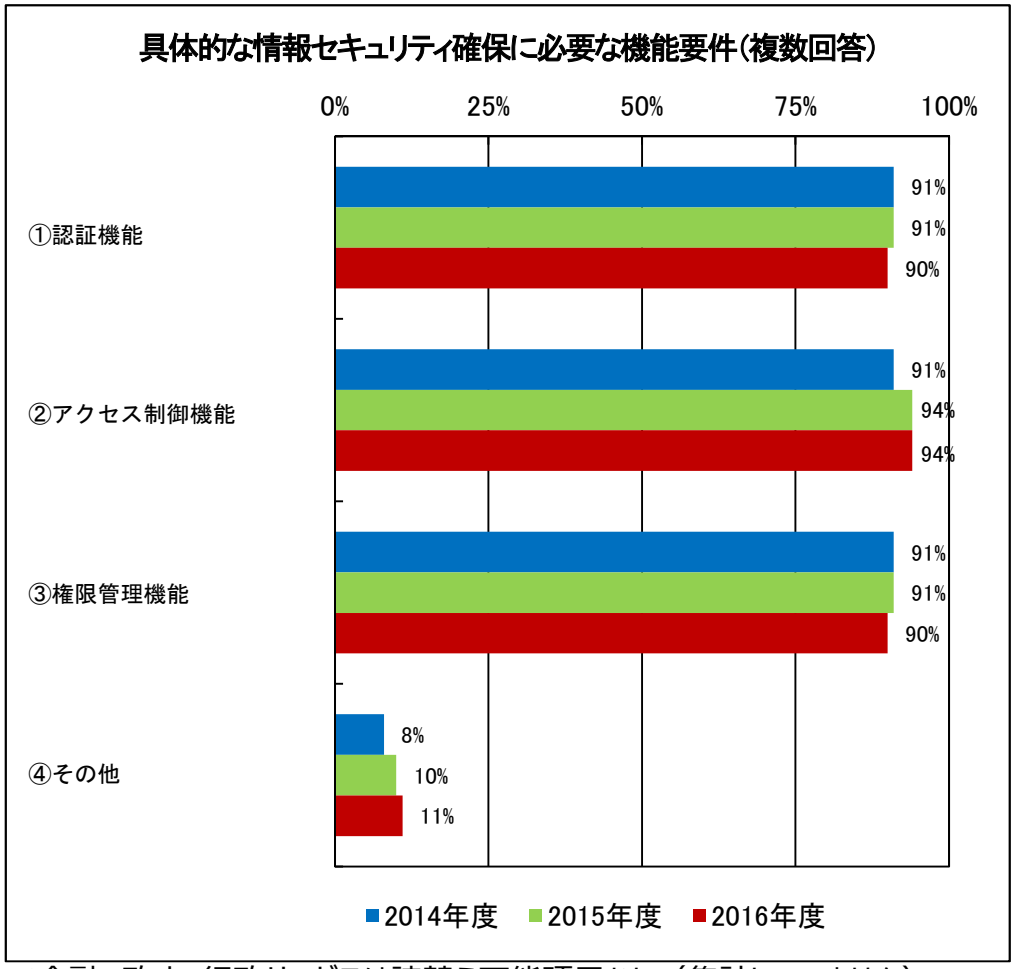
5．調査結果詳細 －（11/19）－

(2) 情報セキュリティ対策の実施状況（続き）

③ 要件の明確化

(c) 具体的な情報セキュリティ確保に必要な機能要件

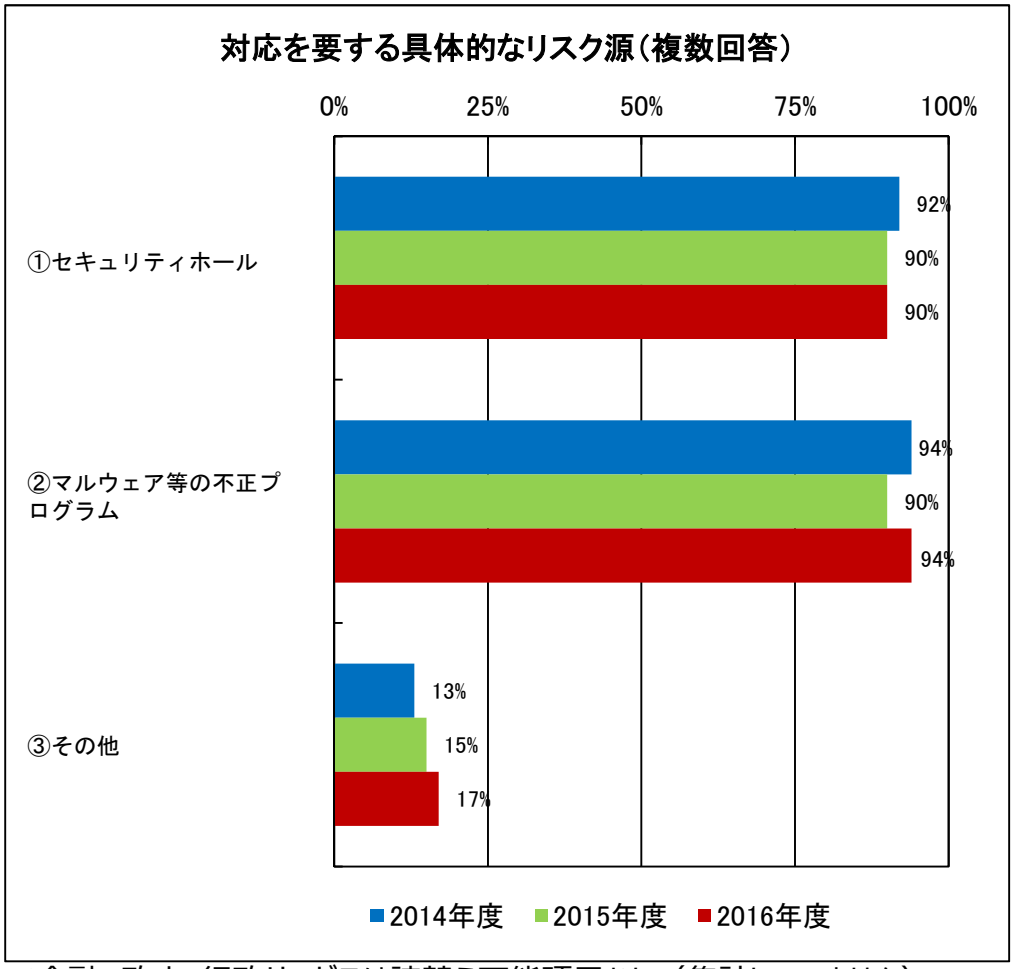
・認証、アクセス制御といった基本的な機能要件に関しては、これまで同様に実施できていると認められる。



※金融、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）
※前設問(2)③(b)選択肢①選択事業者のみの回答

(d) 対応を要する具体的なリスク源

・セキュリティホールやマルウェア等の不正プログラムといったリスク源に関しては、これまで同様に対応を要するリスク源として認識されていると認められる。



※金融、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）
※前設問(2)③(b)選択肢②選択事業者のみの回答

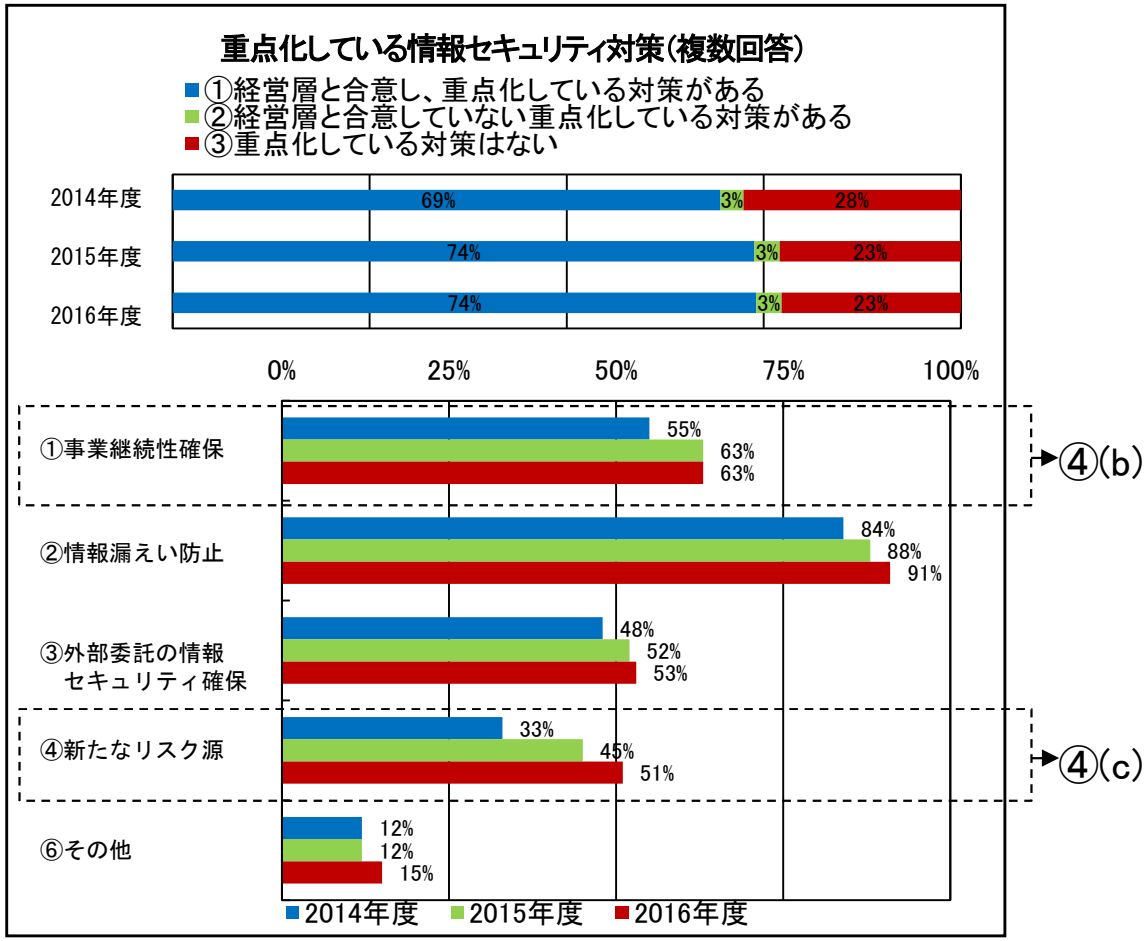
5．調査結果詳細 －（12/19）－

(2) 情報セキュリティ対策の実施状況（続き）

④ 重点化対策と対象とする脅威

(a) 重点化している情報セキュリティ対策

・経営層の関与の伸びに加えて、重点化している情報セキュリティ対策が全体的に伸びていることから、重要インフラ防護に対する意識が醸成されつつあると認められる。



※金融は読替え可能項目なし（集計していません）

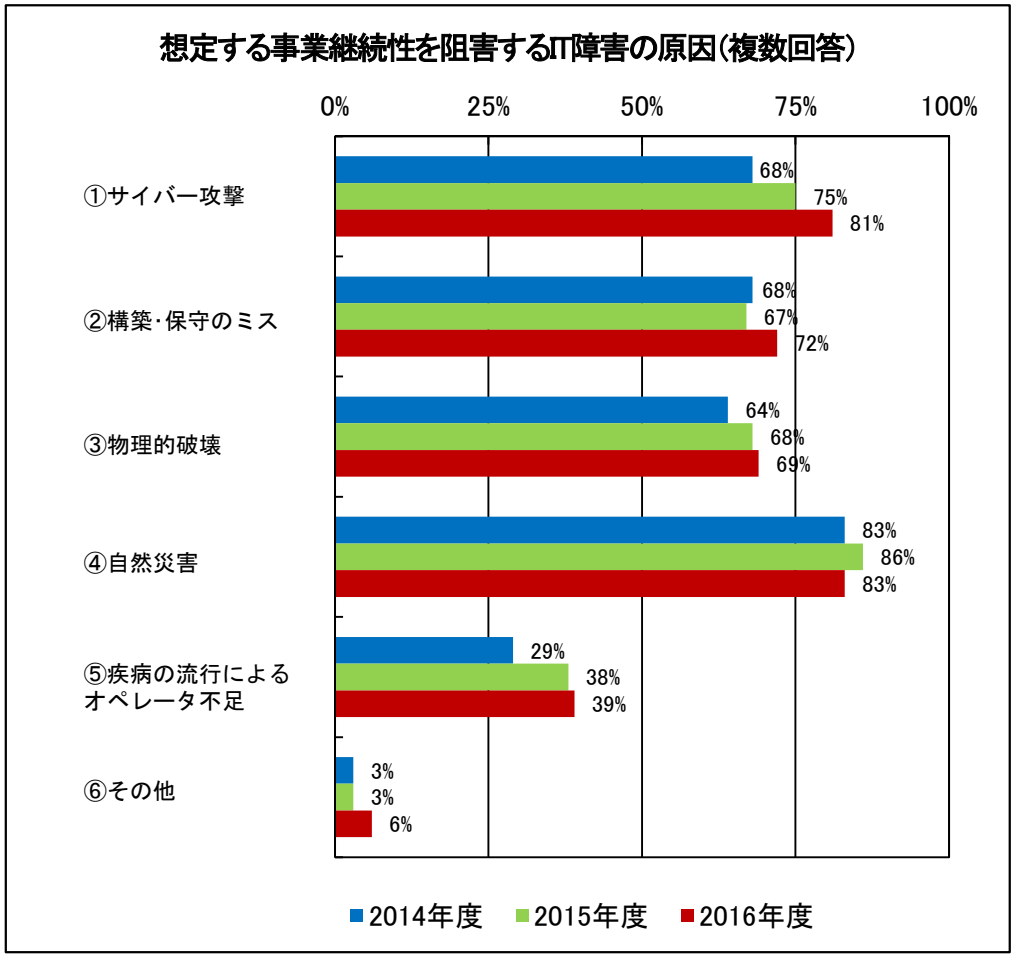
5．調査結果詳細 －（13/19）－

(2) 情報セキュリティ対策の実施状況（続き）

④ 重点化対策と対象とする脅威

(b) 想定する事業継続性を阻害するIT障害の原因

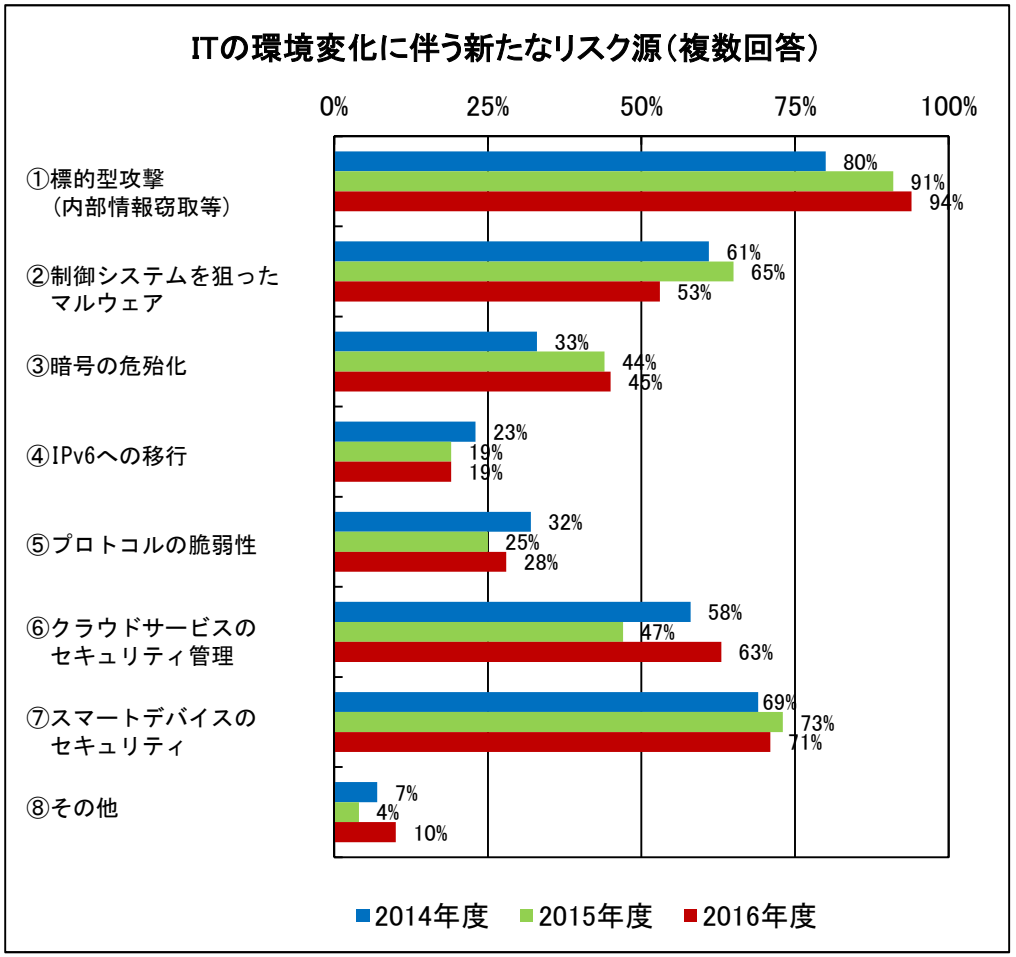
・サイバー攻撃により事業継続が阻害されるという事が認知されつつあると推察される。



※金融、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）
※前設問(2)④(a)選択肢①選択事業者のみの回答

(c) ITの環境変化に伴う新たなリスク源

・標的型攻撃の脅威は依然として高く、その対策が着実に伸びていると認められる。



※金融、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）
※前設問(2)④(a)選択肢④選択事業者のみの回答

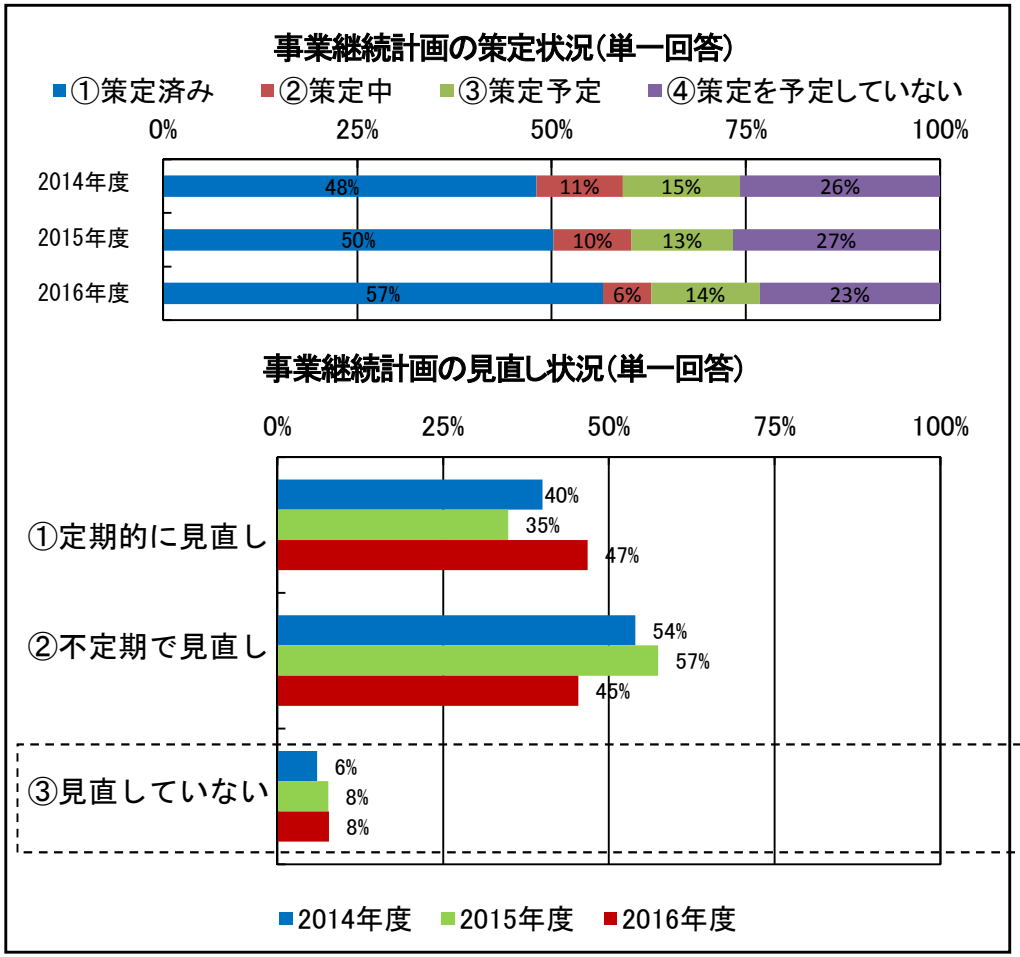
5．調査結果詳細 －（14/19）－

(2) 情報セキュリティ対策の実施状況（続き）

⑤ 事業継続計画の策定・改定

(a) 事業継続計画の策定・見直し状況

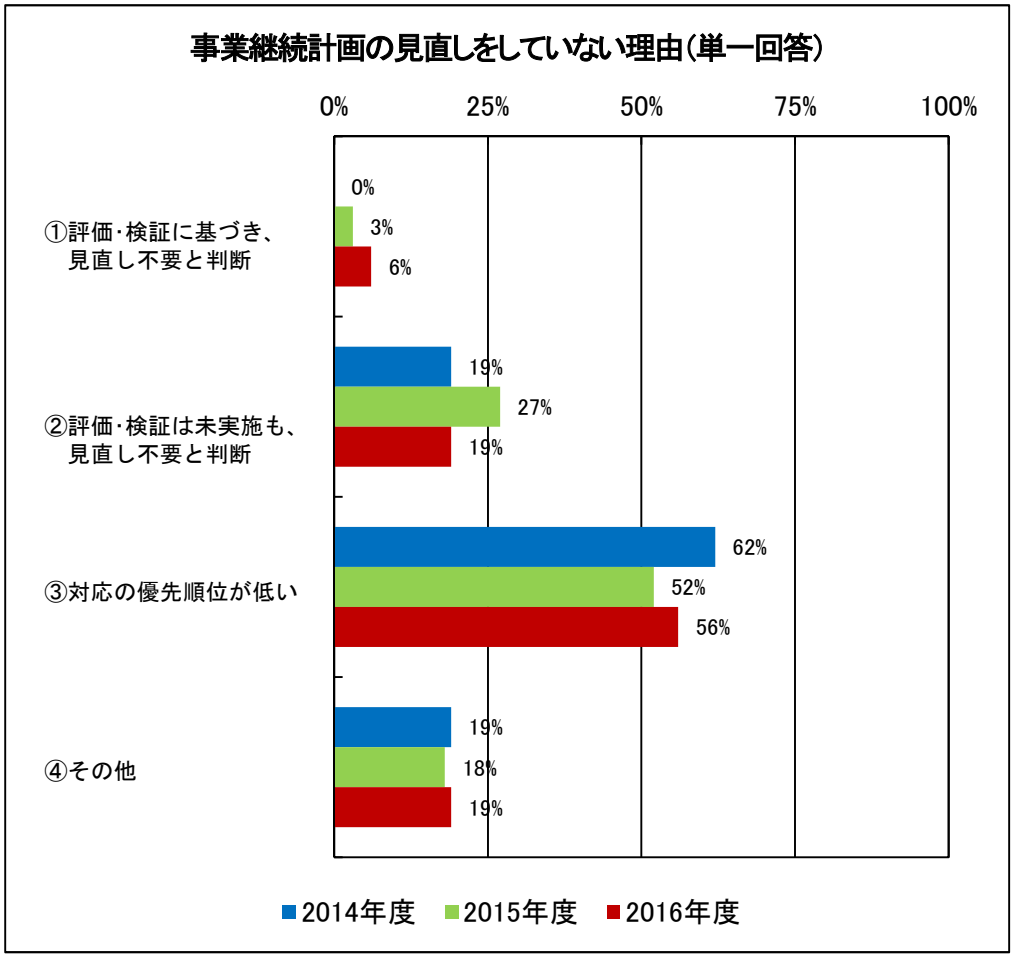
・事業継続計画が必要であるという意識が年々醸成されつつあると推察される。



※金融、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）

(b) 事業継続計画の見直しをしていない理由

・事業継続計画の見直しを実施していない事業者の大半においては、見直しの必要性・重要性が組織内で理解されていないと認められることから、指針等で啓発していく必要がある。



※金融、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 －（15/19）－

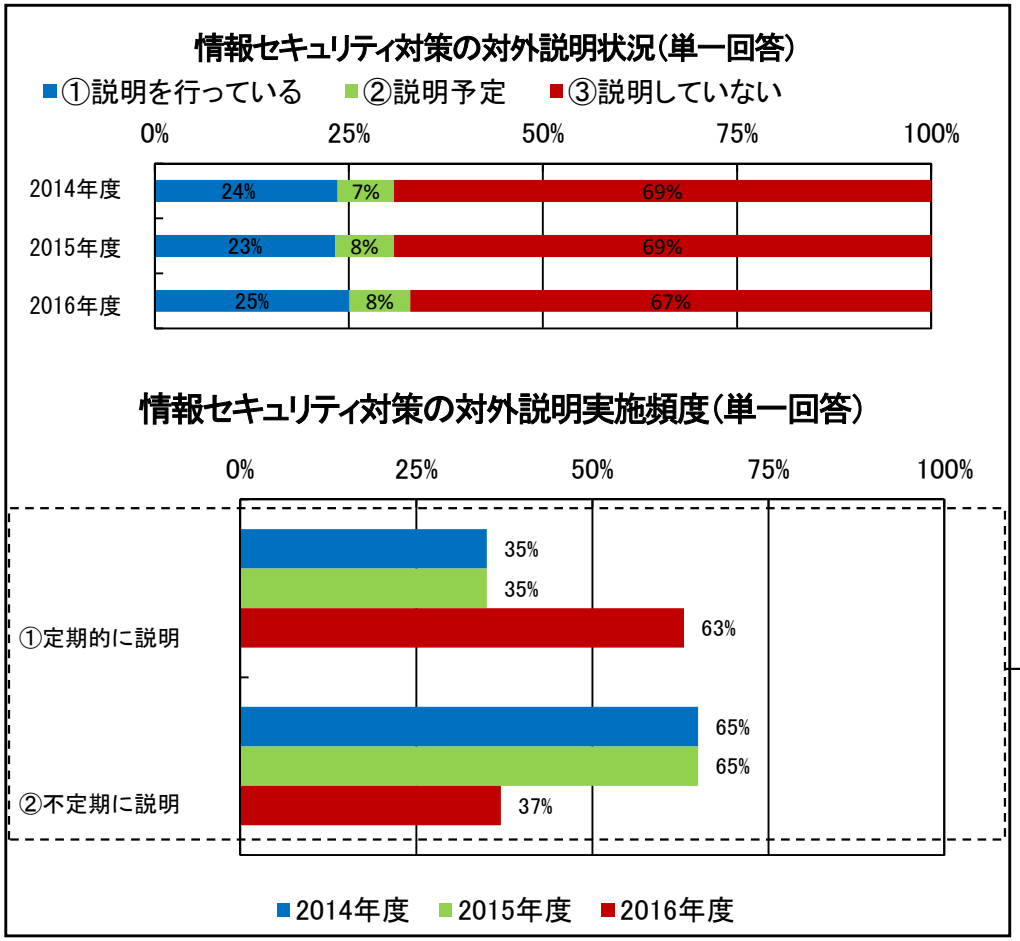
(2) 情報セキュリティ対策の実施状況（続き）

⑥ 対策の対外説明

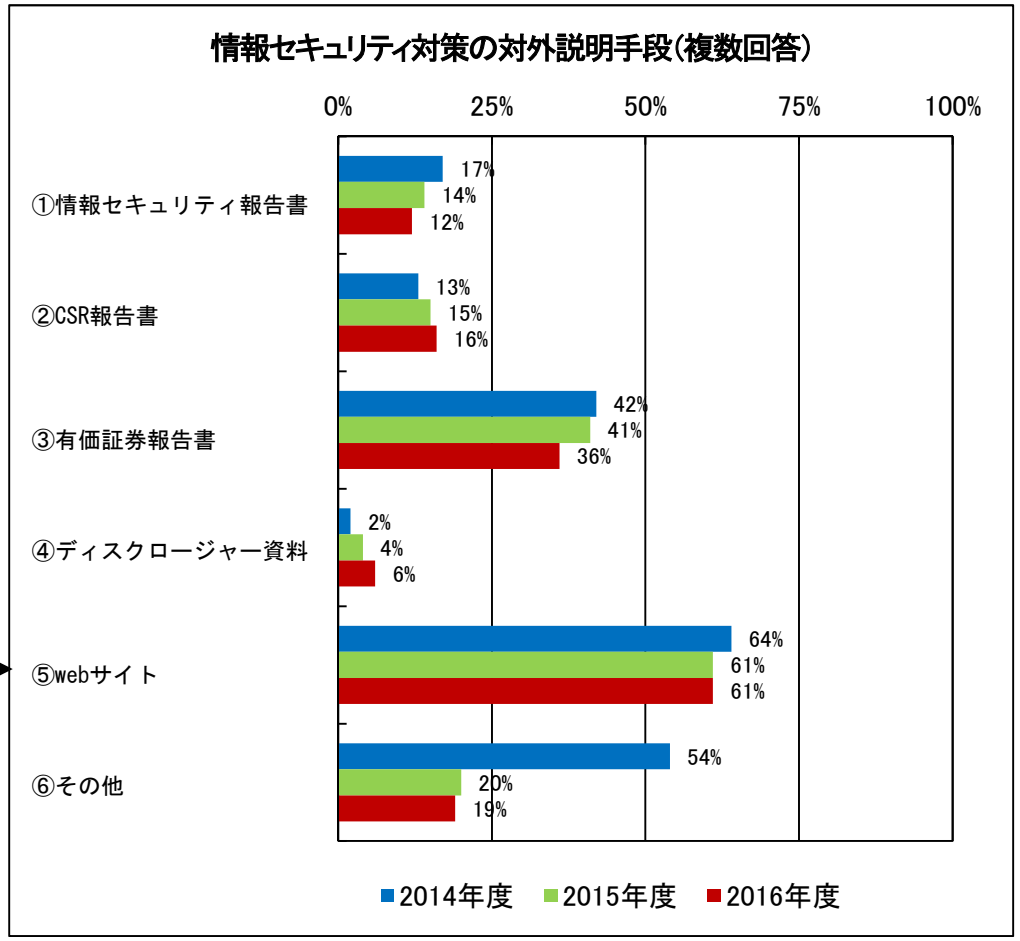
(a) 情報セキュリティ対策の対外説明状況

(b) 情報セキュリティ対策の対外説明手段

・国民の安心感を醸成させるべく、情報セキュリティ対策状況について、Webサイト、有価証券報告書等を通じて、定期的に説明するようになっていると推察される。



※金融、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）



※金融、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）

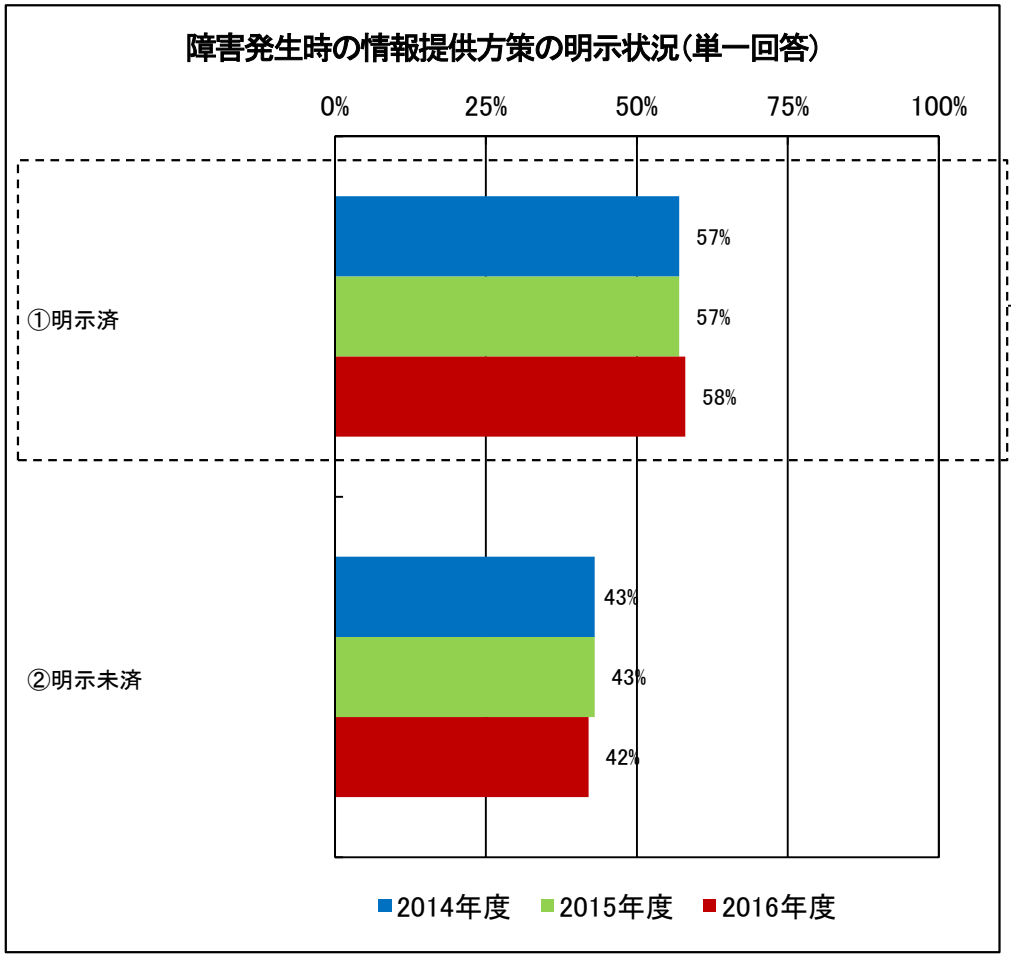
5．調査結果詳細 －（16/19）－

(2) 情報セキュリティ対策の実施状況（続き）

⑦ IT障害発生時の情報提供

(a) 障害発生時の情報提供方策の明示状況

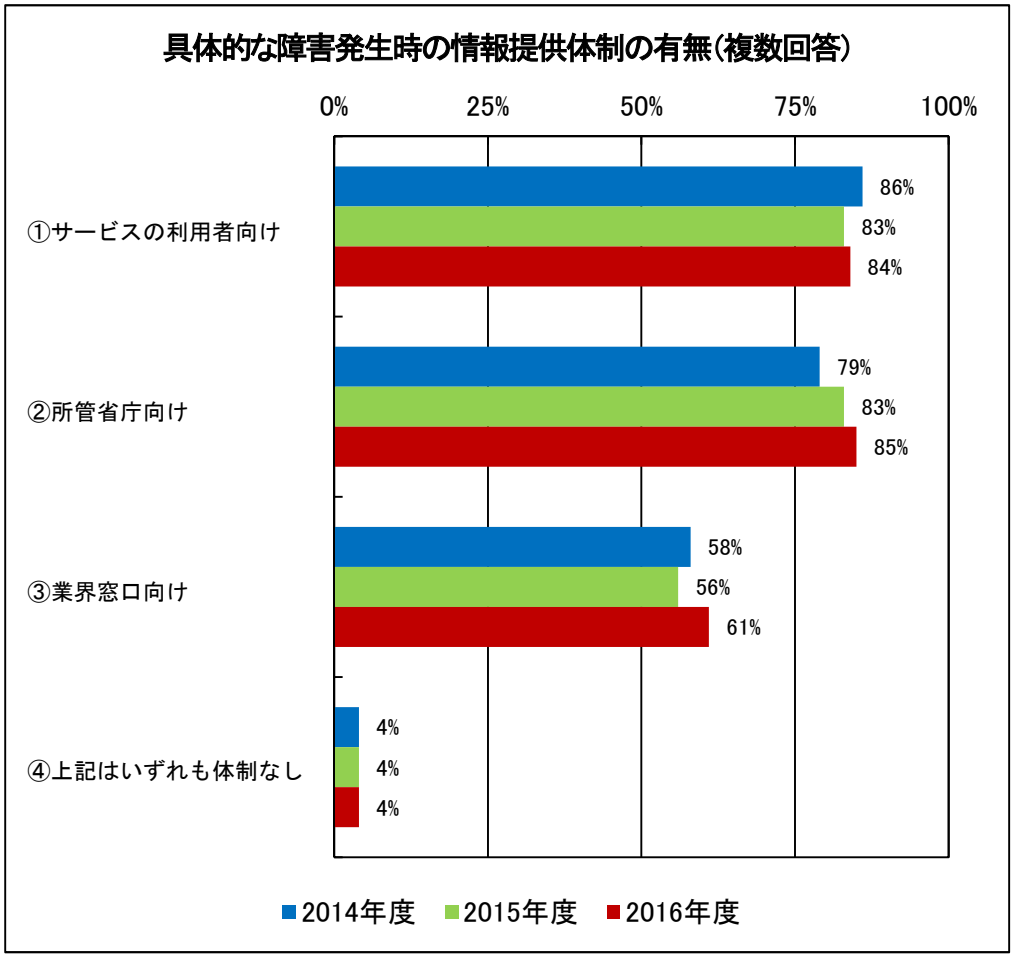
・障害発生時に即応できるような対策を取っている事業者等は6割弱をキープできていると認められる。



※金融、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）

(b) 具体的な障害発生時の情報提供体制の有無

・サービスの利用者向けだけではなく、所管省庁や業界窓口に向けての情報共有体制の構築が伸びており、障害発生時の対応強化に寄与していると認められる。



※金融、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）

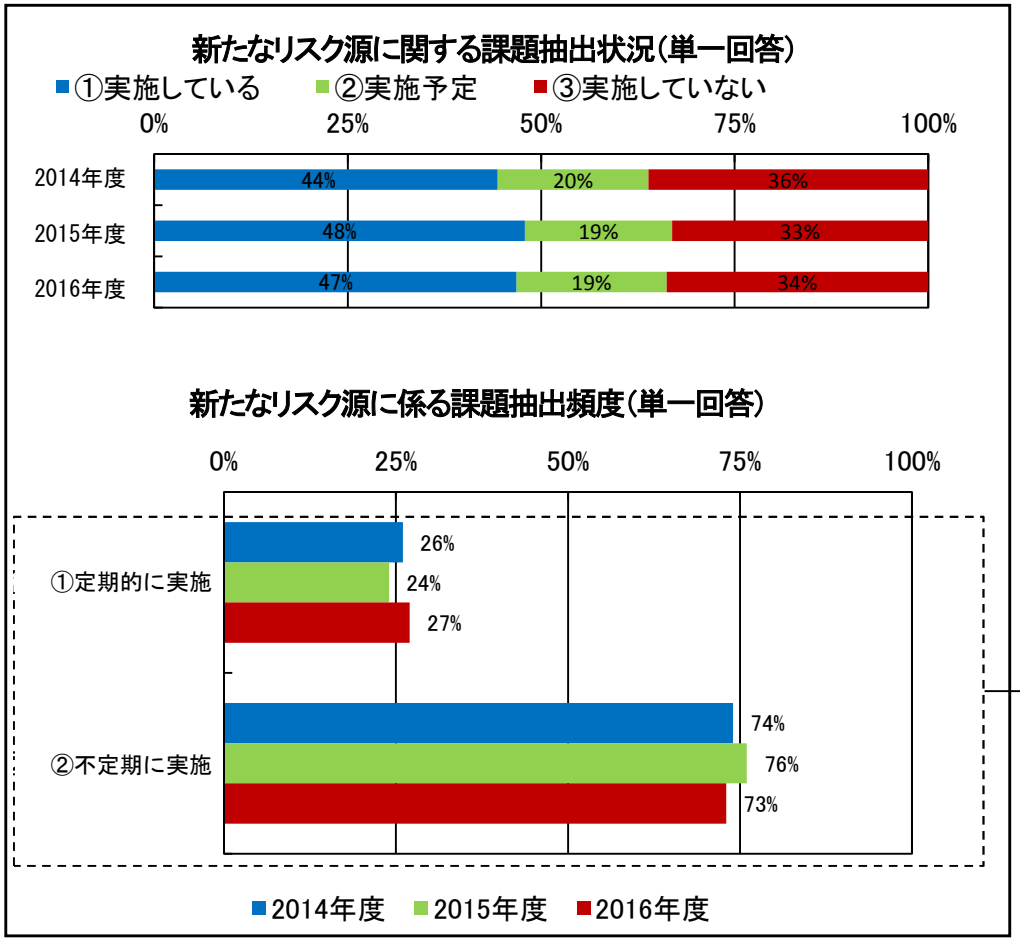
5．調査結果詳細 －（17/19）－

(2) 情報セキュリティ対策の実施状況（続き）

⑧ ITの環境変化に伴い想定する脅威

(a) 新たなリスク源に係る課題抽出状況

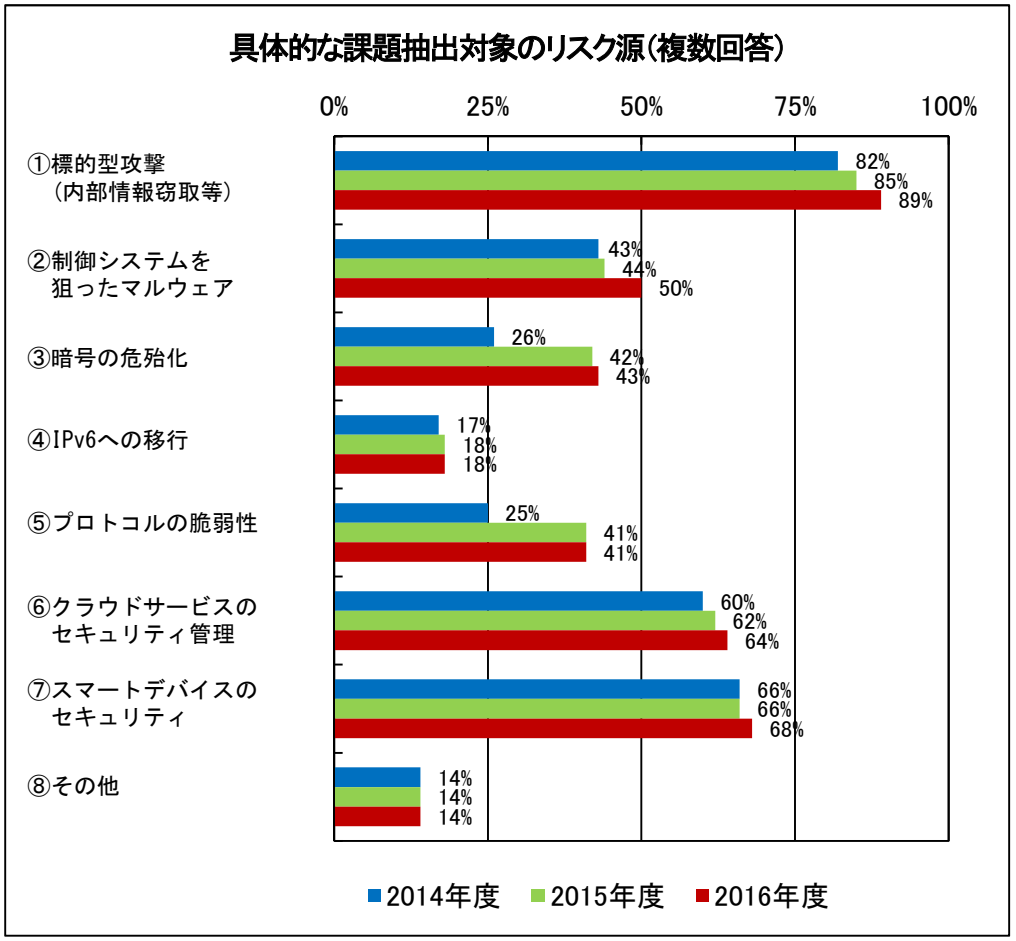
・新たなリスク源の発生は不定期であることから、課題抽出を定期的に実施する事業者等が増えていないと推察される。



※金融、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）

(b) 具体的な課題抽出対象のリスク源

・標的型攻撃の脅威が依然として高いことから、その対策が着実に伸びていると認められる。
・制御システムを狙ったマルウェアの事例が増えていることから、制御システムに対するセキュリティ意識が高まっていることが認められる。



※金融、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）

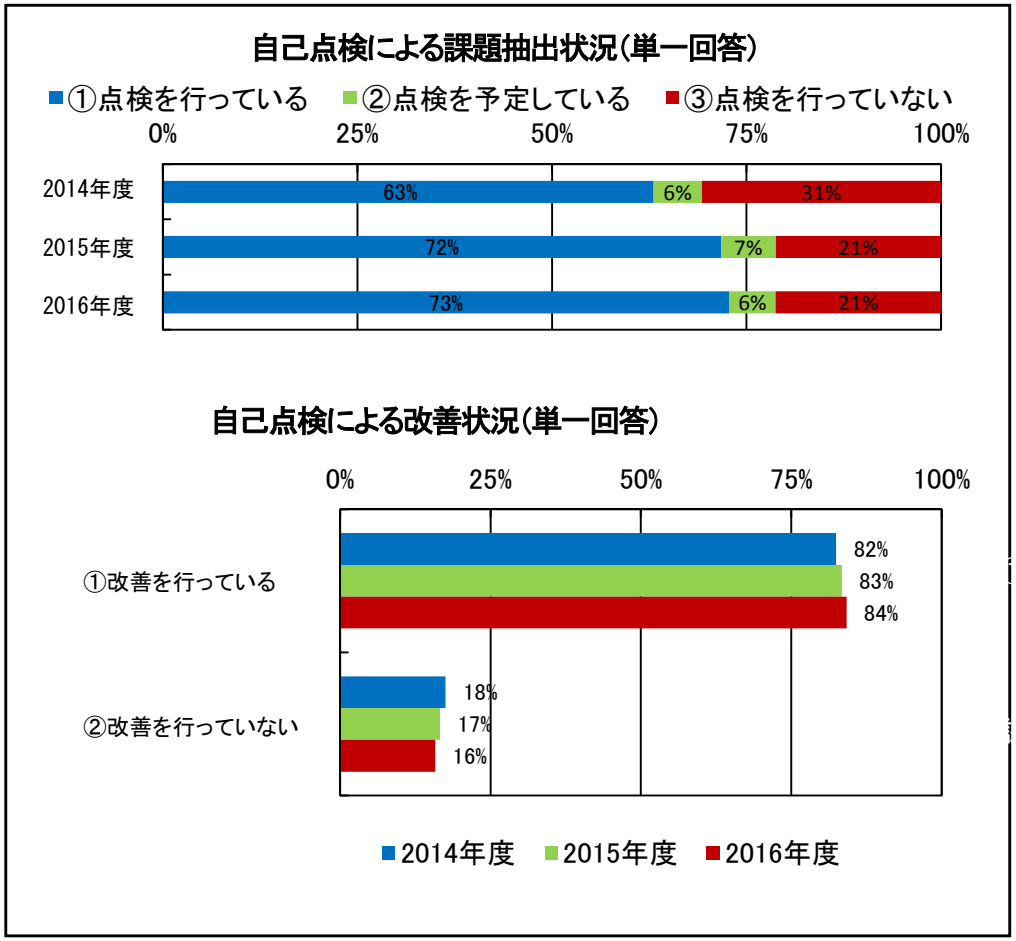
5．調査結果詳細 － (18/19) －

(3) 安全基準等の準拠状況

① 内規に基づく自己点検の実施

(a) 自己点検による課題抽出・改善状況

・自己点検を行う事業者が増えていることから、情報セキュリティ対策のＰＤＣＡの重要性が認識されつつあると推察される。

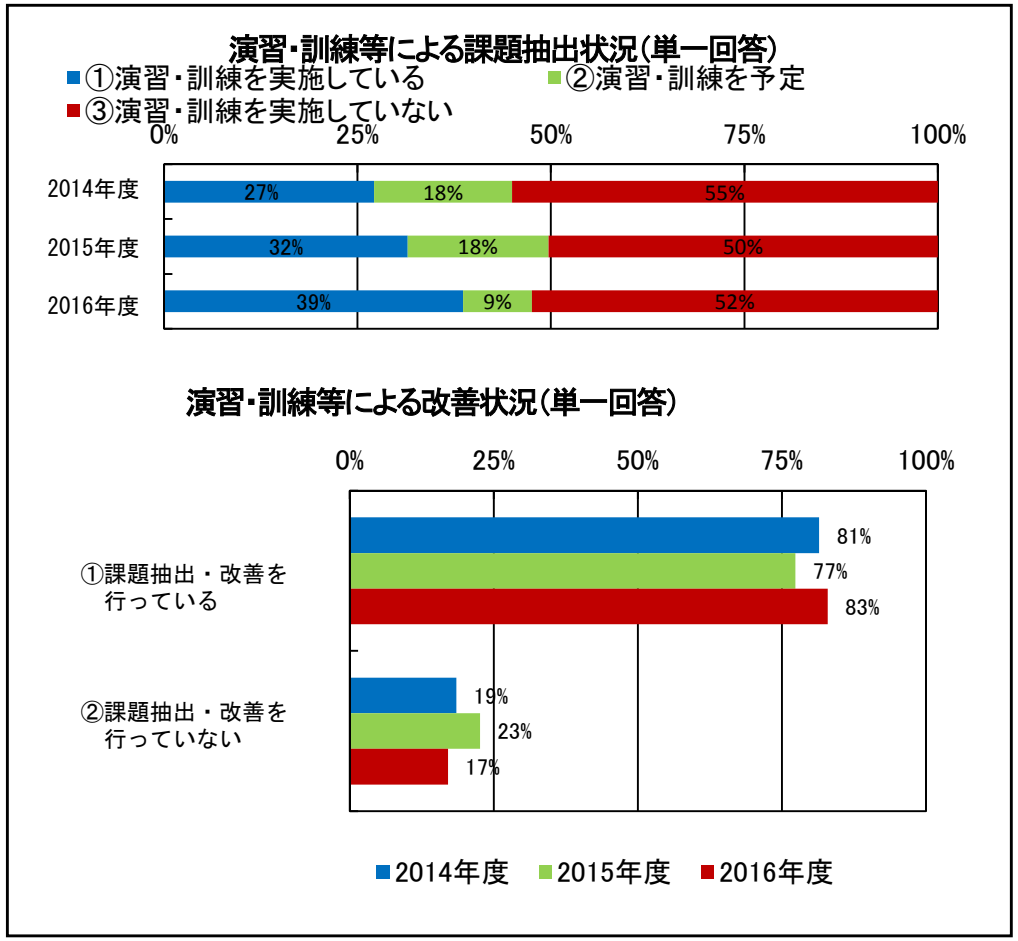


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

② 演習・訓練等の実施

(a) 演習・訓練等による課題抽出・改善状況

・実施している事業者は着実に増加しており、課題抽出・改善を行っている事業者も伸びていることから、演習・訓練の有用性が浸透していると認められる。



※金融、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）

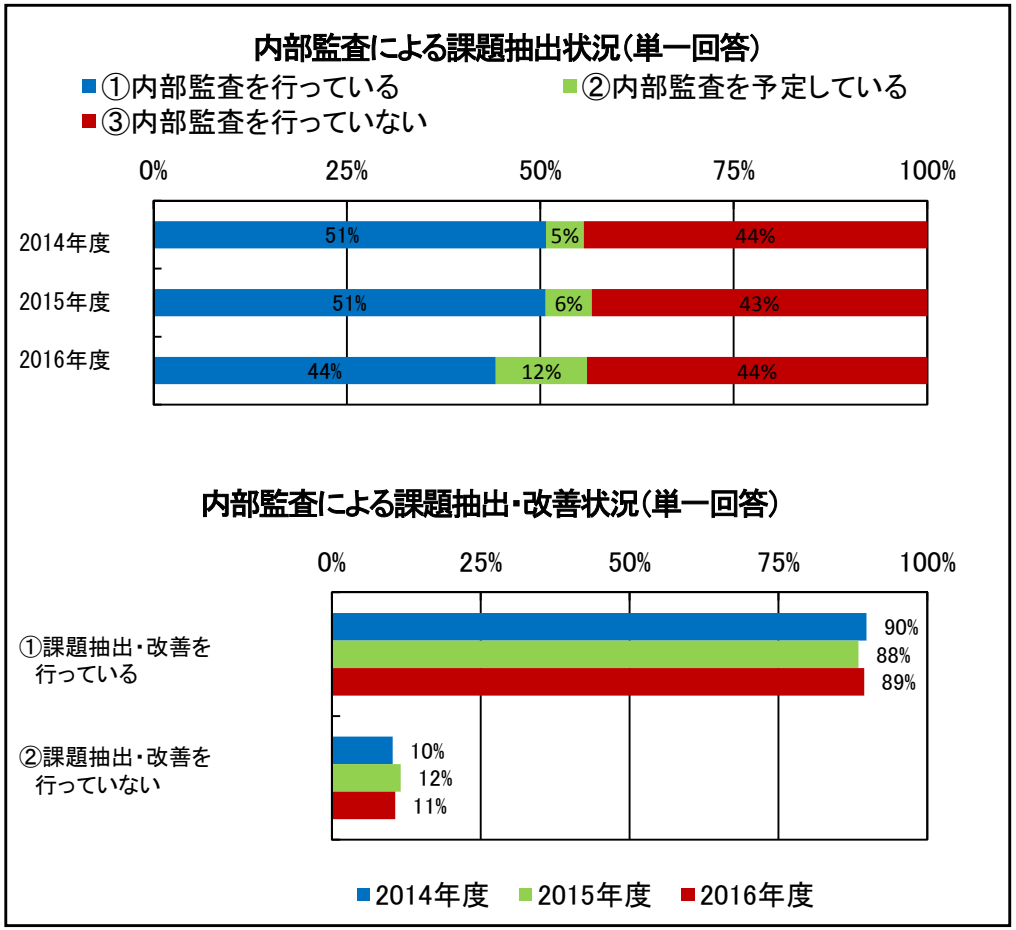
5．調査結果詳細 －（19/19）－

(3) 安全基準等の準拠状況（続き）

③ 内部監査の実施

(a) 内部監査による課題抽出・改善状況

・内部監査の実施事業者等については、大きな伸びが認められない。

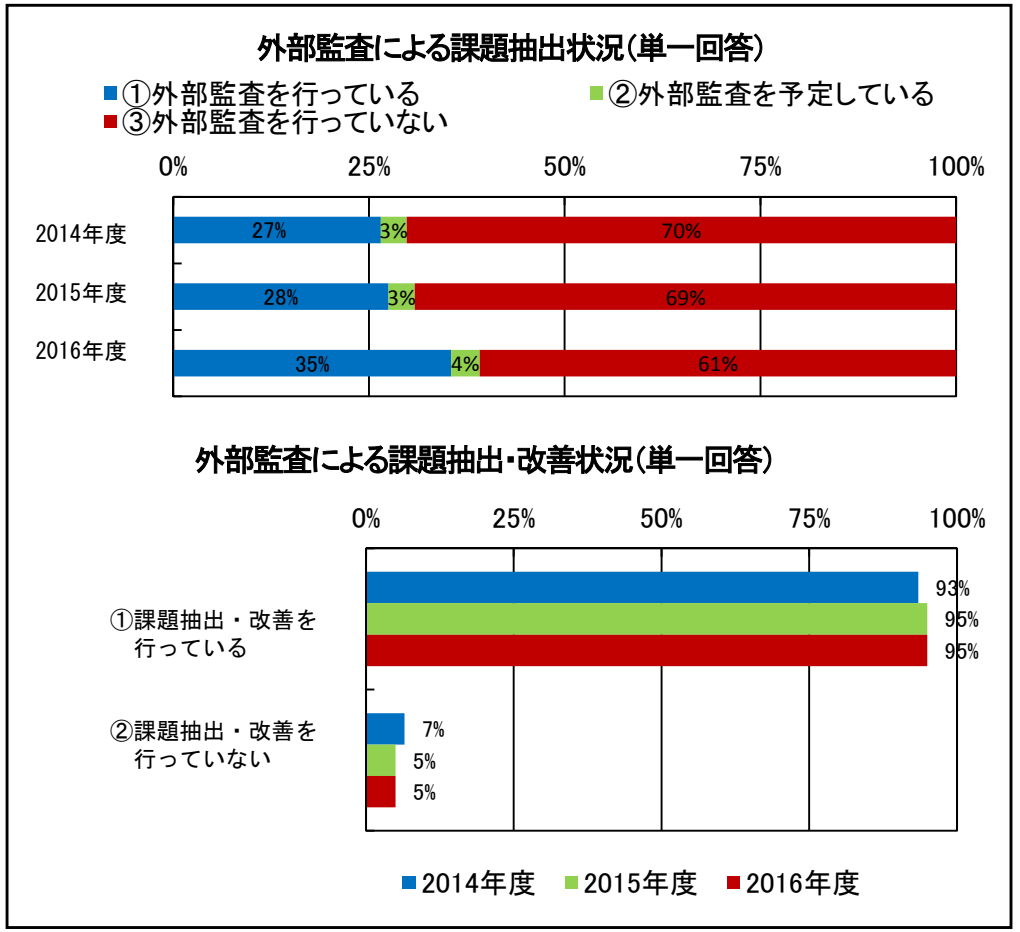


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

④ 外部監査の実施

(a) 外部監査による課題抽出・改善状況

・外部監査を実施している事業者等が伸びているため、外部監査の有用性が認知されつつあると認められる。



※金融、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　－　自由意見 (1/2) －

【安全基準等に関する意見】

- 業界団体や所管省庁等が発行するガイドライン等において、分野特有の組織特性や慣習等を考慮した内容にしてほしい。
- 情報セキュリティ対策の強化の必要性は理解をしているが、対策の導入においては、企業規模に応じて事業性・採算性を含め検討していくため、全事業者に共通した強制基準にならないようにしてほしい。
- 事業者の規模に応じた規模別対策や、規模別のセキュリティ対策に向けたロードマップなどがあると、目標としやすいのではないか。

【指針に関する意見】

- 政府が主導して、情報セキュリティ対策における有効な手段を示してほしい。
- 指針に関する説明会や情報セキュリティ対策の講習会を開催してほしい。
- リスク対策における表記について、指針とISO31000シリーズの表記を統一してほしい。
- 記載されている用語は、専門的知識なしでも理解できるようにしてほしい。

【情報共有体制の推進に関する意見・要望等】

- インシデント事例や他社の情報セキュリティ対策への取組事例等の情報がほしい。
- 匿名で情報提供や共有する仕組みが必要。
- 各社間の交流の活発化を進めてほしい。

5．調査結果詳細　－　自由意見 (2/2) －

【アンケートに関する意見】

- WEB上のアンケート等で、簡潔なアンケートにしてほしい。
- アンケート項目が多すぎる。

【国・政府に対する意見・要望等】

- 助成金や減税措置を導入してほしい。
- 将来を考えた人材育成の支援を重視してほしい。
- 事業者単独でセキュリティ人材を育成することは困難。
- オリンピック・パラリンピックに向けたセキュリティ対策の整備を進めてほしい。

【その他の意見】

- 制御システム系に対する情報セキュリティ対策の重要性は認識している。
- 予算が許すなら、全ての情報セキュリティ対策を導入したい。
- 少人数、特に兼任のみで管理していくのは、すでに限界となっている。

6．＜参考＞　－　アンケート項目(1/2)　－

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」を参照(当該ｸﾞﾗﾌについては各項目の末尾を参照)

【Ⅰ．基礎的事項】

貴社（又は貴団体）の従業員数を選んでください。

【Ⅱ．指針の認知状況に係る事項】

(1) 指針_本編、指針_対策編及び指針_手引き書をご存知ですか。[(1)①(a)]
(2) 指針_本編、指針_対策編及び指針_手引き書を何で知りましたか。[(1)①(b)]
(3) 今後の周知方法の検討に活かしたいと思いますので、効果的に周知する手段について良いと思われるものがありましたらご紹介ください。

【Ⅲ．情報セキュリティ対策の実施状況に係る事項】

(1) 情報セキュリティ対策にあたって、経営層と合意の上、重点化しているものをお知らせください。[(2)④(a)]
(2) （ＩＴ障害防止等の観点から見た事業継続性確保のための対策を重点化している場合）
事業継続性を阻害する具体的な想定原因をお知らせ下さい。[(2)④(b)]
(3) （ＩＴの環境変化に伴う新たなリスク源への対策を重点化している場合）対象とするリスク源等をお知らせください。[(2)④(c)]
(4) 内規の策定・見直しの契機をお知らせ下さい。[(1)②(a)]
(5) 内規策定・改定を行う際の体制をお知らせ下さい。[(1)③(a)]
(6) 内規改定に要するおおよその期間をお知らせ下さい。
(7) 内規において規定済のものをお知らせ下さい。[(1)③(b)]
(8) 対策に係る計画またはロードマップの策定・見直し状況をお知らせ下さい。[(2)②(a)]
(9) 事業継続計画の策定・見直し状況をお知らせ下さい。[(2)⑤(a)]
(10) （事業継続計画の策定・見直しを行ったことはあるが、現在は見直しを行っていない場合）現在は見直しをしていない理由をお知らせ下さい。[(2)⑤(b)]
(11) 組織・体制及び資源の確保として行っているものをお知らせ下さい。[(2)①(a)]
(12) （情報セキュリティに係る人材育成、教育を行っている場合）教育テーマの対象としているものをお知らせ下さい。[(2)①(b)]
(13) 委託先との契約において締結されているものをお知らせ下さい。[(2)③(a)]
(14) 情報セキュリティ要件を明確にしているものをお知らせ下さい。[(2)③(b)]
(15) （情報セキュリティ確保のために求められる機能の観点から、情報システムに導入すべきセキュリティ要件を明確化している場合）
明確化した情報セキュリティ要件をお知らせ下さい。[(2)③©]
(16) （情報セキュリティについてのリスク源に対して、情報システムに導入すべきセキュリティ要件を明確化している場合）
明確化した情報セキュリティ要件にて対象とするリスク源をお知らせ下さい。[(2)③(d)]

6．＜参考＞　－　アンケート項目(2/2)　－

【Ⅲ．情報セキュリティ対策の実施状況に係る事項】（続き）

(17) 明確化した情報セキュリティ要件への対応として、対策を行っているものをお知らせ下さい。[(2)②(b)]
(18) （明確化した情報セキュリティ要件への対策として「ネットワークへの侵入防止」を行っている場合）
具体的に対応しているものをお知らせ下さい。[(2)②©]
(19) （明確化した情報セキュリティ要件への対策として「ファイアウォールの導入」を行っているが、適用範囲の妥当性評価・必要に応じた見直しは行っていない場合）適用範囲の妥当性評価・必要に応じた見直しを行っていない理由をお知らせ下さい。[(2)②(d)]
(20) （明確化した情報セキュリティ要件への対策として「侵入検知システムの導入」を行っているが、検知条件の妥当性評価・必要に応じたチューニングは行っていない場合）検知条件の妥当性評価・必要に応じたチューニングを行っていない理由をお知らせ下さい。[(2)②(e)]
(21) （情報セキュリティ要件への対策として無許可ソフトウェアの導入禁止を行っている場合）具体的に対応しているものをお知らせ下さい。[(2)②(f)]
(22) （ＩＴの環境変化に伴う新たなリスク源への対策を行っている場合）対象としているリスク源をお知らせ下さい。[(2)②(g)]
(23) 経営層への報告対象としているものをお知らせ下さい。[(2)②(h)]
(24) 情報セキュリティ対策についての対外的な説明状況をお知らせ下さい。[(2)⑥(a)]
(25) （情報セキュリティ対策についての対外的な説明を行っている場合）その説明方法をお知らせ下さい。[(2)⑥(b)]
(26) 重要インフラサービスに障害が発生した場合に、障害の状況や復旧等の情報提供の方策が明示されていますか。[(2)⑦(a)]
(27) （重要インフラサービスに障害が発生した場合における情報提供の方策が明示されている場合）
提供先において情報提供に向けた体制がありますか。[(2)⑦(b)]
(28) ＩＴの環境変化に伴う新たなリスク源について、リスクの特定・分析等を通じた確認・課題抽出を行っていますか。[(2)⑧(a)]
(29) （ＩＴの環境変化に伴う新たなリスク源について確認・課題抽出を行っている場合）
現時点で対象とする新たなリスク源等をお知らせ下さい。[(2)⑧(b)]
(30) 安全基準等や内規等に基づく情報セキュリティ対策の実施状況の自己点検を行い、同対策の改善につなげていますか。[(3)①(a)]
(31) 情報セキュリティ対策の実施状況に係る内部監査を行い、同対策の改善につなげていますか。[(3)③(a)]
(32) 情報セキュリティ対策の実施状況に係る外部監査を行い、同対策の改善につなげていますか。[(3)④(a)]
(33) ＩＴ障害発生を想定した演習・訓練等を実施し、情報セキュリティ対策の改善につなげていますか。[(3)②(a)]

【Ⅳ．　その他一般的事項】

(1) 本編、対策編に対してのご意見がありますか。（自由意見を記載）
(2) 安全基準等に対してのご意見がありますか。（自由意見を記載）
(3) その他、ご意見がありますか。（自由意見を記載）

6．＜参考＞　－　往訪調査（1/4）　－

1.往訪調査の位置付け

安全基準等の浸透状況調査の補完として、アンケート形式による安全基準等の浸透状況調査以外に、直接重要インフラ事業者等に意見を聞き、具体的な対策状況に係る課題抽出及び良好事例の収集を行う。

※重要インフラの情報セキュリティ対策に係る第３次行動計画（平成27年５月25日サイバーセキュリティ戦略本部改訂）

2.調査方法

事前に往訪先事業者からいただいたシステム構成図及び事前アンケートに対する回答を基にした現地ヒアリング

3.主な調査内容

【主な調査項目】

① 経営層の関与状況　② 規程類や契約類の遵守状況

③ 人材育成の考え方　④ 障害対応体制　⑤ その他

※その他、情報共有や最近のサイバー攻撃及び分野内のセキュリティ動向などについて意見交換を実施

4.調査対象

重要インフラ事業者１０社（医療・金融・物流・化学・石油）

※所管省庁や関係セプターと調整の上、対象事業者を選定

5.調査期間

2016年1月～2016年10月

6．＜参考＞　－　往訪調査 (2/4)　－

(1) 良好な点

1.　経営層の関与

- 内部の障害対応訓練に役員が参加することが通例となっており、他業務よりも優先すべきという意識が醸成されている。
- 経営層が委員長となっているリスクマネジメント会議を設けており、情報セキュリティについてもその場で共有している。
- IT系部署と制御系部署の管理権限の一部を特定の部門に一本化することで、情報共有できる体制を構築している。

2.　規定類や契約類の遵守状況

- 規定類やセキュリティガイドライン等は、国内及び海外事業所で統一したものを運用している。
- 規定類は、内部監査や外部監査の結果を受けて、適時改正している。

3.　人材育成

- 人事異動が発生するごとにセキュリティ教育を実施しているほか、一部の事業者では月に1度、全社員を対象に情報セキュリティに関するe-learningを実施している。

4.　障害対応体制

- システム障害が発生しても、手作業によりサービスを継続することができるように準備しており、ステークホルダーを含めた全職員で訓練を実施しており、同訓練を年に一回程度実施している事業者も存在する。
- インシデント発生時は、CSIRTに連絡し、深刻度に応じて社長の指示により対応する運用としている。

※上記記載内容は、一部事業者の意見を記載しているだけであり、往訪調査を行った全事業者の意見を総括しているわけではありません。

6．＜参考＞　－　往訪調査 (3/4)　－

(2) 問題点

1. 経営層の関与

- 一部の事業者では、経営層から情報セキュリティに関する指示が出てくることがほとんどない。
- 担当役員の情報セキュリティに対する理解の度合いにより、投資への意識が大きく異なっている。

2. 規定類や契約類の遵守状況

- 一部の事業者では、IT-BCPは策定しているものの、改定作業を行っていない。
- BCPは策定しているが、ITに特化したものは策定していない。

3. 人材育成

- 一部の事業者では、情報セキュリティに特化した教育は行っていない。
- 情報セキュリティ人材については、社会全体として不足していると感じる。
- 事業者単独でセキュリティ人材を育成することは困難である。

4. その他

- 一部の事業者では、NISC発行の重要インフラニュースレター以外の情報源がない。
- 一部の事業者では、社員個人のセキュリティ意識やITリテラシーが低いと感じられる。
- 上位役職者へのセキュリティ教育をどのように行えば効果的か思案している。

※上記記載内容は、一部事業者の意見を記載しているだけであり、往訪調査を行った全事業者の意見を総括しているわけではありません。

6．＜参考＞　－　往訪調査 (4/4)　－

(3) 考察

- 経営層の情報セキュリティに対する理解度が高い事業者では、経営層が障害対応訓練や情報共有を主導的に行っているが、経営層の理解度が低い事業者では、サイバー攻撃対策への投資が推進されていない傾向にあるため、経営層の情報セキュリティに対する理解度を高める必要がある。
- 一部の従業員数1000名未満規模の事業者では、IT-BCPを策定していない、もしくは策定しているが、定期的な見直しを実施できていない事業者が見受けられる。また、情報セキュリティ教育を実施していない事業者では、社員の情報セキュリティに対する意識の低くなっている。このことから、従業員数1000名未満規模の事業者の取組支援を強化する必要がある。
- 往訪先事業者の多くは、情報セキュリティ人材が不足していると感じていることから、情報セキュリティ人材の育成を支援する必要がある。
- 制御系部署とIT系部署の管理権限の一部を組織的に統合し、円滑な情報共有の実施、および障害対応体制を確立している事業者があるが、制御系・IT系に精通した人材の有無により、取り組みの度合いに違いがあると考えられる。制御系部署、IT系部署ともに人材が固定化される傾向が見受けられたことから、ローテーションによる人材育成が重要である。
- システム障害対応訓練をステークホルダーと合同で行っている事業者があり、情報セキュリティに関する意識が醸成されている。このことから、常日頃から関係組織との意思統一および情報共有が重要であると考えられる。