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

2015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

2016年３月25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．本調査の目的・経緯

【目的】

○重要インフラにおける情報セキュリティ対策の実施状況を通じて安全基準等の浸透状況を把握するとともに、行動計画の各施策の改善に資することを目的として実施し、重要インフラ専門調査会に報告。実施根拠は以下のとおり。

◆サイバーセキュリティ2015（2015年9月25日）

・「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」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化の５つの施策を実施する。

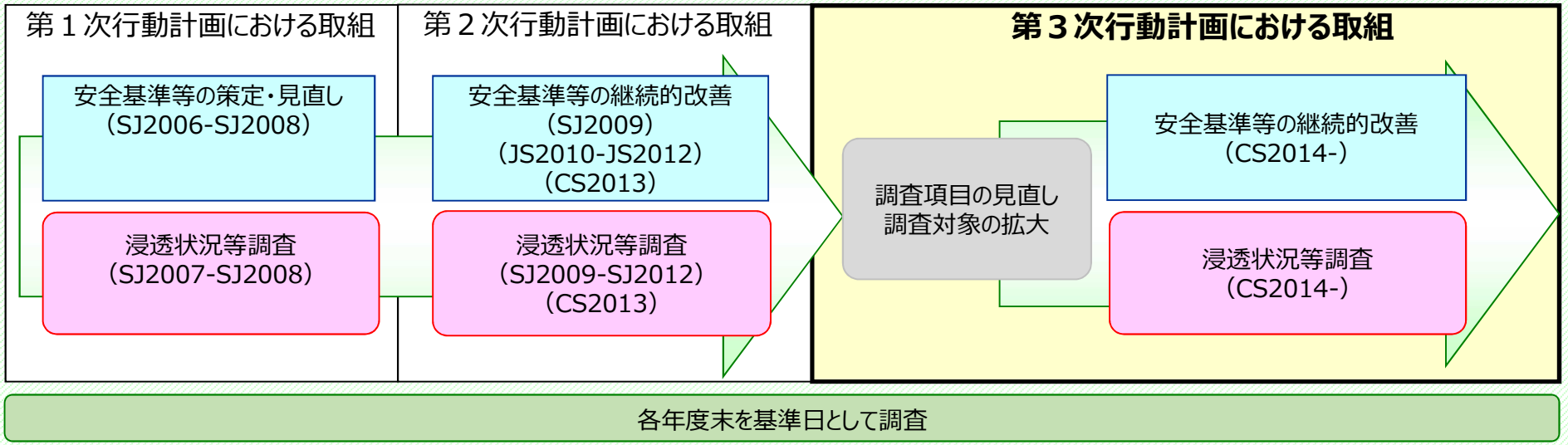
◆重要インフラの情報セキュリティ対策に係る第３次行動計画（2015年５月25日）

・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把握を目的に、内閣官房は、重要インフラ事業者等の対策状況を調査する。

【経緯】

○2007年度から開始し、以降継続的に実施。

○第３次行動計画の趣旨に基づき、2014年度調査から調査対象の拡大、調査項目及び報告内容の見直しを実施。



（SJ：セキュアジャパン　JS：情報セキュリティ　CS：サイバーセキュリティ）

2．本調査運営の概要

◆調査概要

調査対象範囲	：	事業者等の範囲を重要インフラ所管省庁が決定
調査方法	：	以下のいずれかを重要インフラ所管省庁が選択 ①NISCが提供する調査項目の活用 ②重要インフラ分野による独自調査結果をNISCが提供する調査項目に読替（回答負荷の軽減）
調査基準日	：	2015年3月末日（調査方法②の場合はその調査基準日）
調査資料の発出・回収	：	重要インフラ所管省庁が送付・回収方法を決定し、実施
分野毎の集計	：	送付・回収した重要インフラ所管省庁が集計（所管する各分野の状況把握の観点）
全体集計・とりまとめ	：	NISCが集計・とりまとめ

◆実施時期　（NISC提供の調査項目を活用する場合）

調査期間	：	2015年　7月～2015年11月
とりまとめ	：	2015年12月～2016年　2月

◆主な調査内容（NISC提供の調査項目）

①指針(*)の認知状況に係る事項　：　指針の認知に係る状況及び周知手段

*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）、同対策編、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情報セキュリティ対策の実施状況に係る事項：　Plan（方針、規定、計画、体制及び構築）、Do（平時、障害発生時の運用）、Check・Act（確認・課題抽出）の各状況

③情報セキュリティ対策に係る意見、要望等

※調査項目の詳細については、巻末の「７．　＜参考＞ －アンケート項目－」を参照

3．回答状況

アンケートを配布は3,507事業者等。回答は3,281事業者等。（昨年度比　配布数：+3.4%　回答数：+1.6%　回答率：▲1.6%）

重要インフラ分野		調査対象範囲	アンケート配布数 (括弧内は昨年度)	アンケート回収数 (括弧内は昨年度)	調査方法
情報通信	電気通信	電気通信事業者（一部抽出）	88 (97)	75 (73)	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	332 (237)	307 (237)	
	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 (194)	194 (194)	
金融		銀行等、証券会社、生命保険会社、損害保険会社	851 (855)	683 (737)	独自調査(*1)
航空	航空運送	航空運送事業者	2 (2)	2 (2)	NISC調査
	航空管制	官庁	2 (2)	2 (2)	
鉄道		ＪＲ、大手民鉄	22 (22)	22 (22)	
電力		一般電気事業者、日本原電(株)、電源開発(株)	12 (12)	12 (12)	
ガス		大手ガス事業者	12 (12)	12 (12)	
政府・行政サービス		地方公共団体	1,789 (1,789)	1,789 (1,789)	独自調査(*2)
医療		病院情報システムを導入する病院	60 (60)	46 (53)	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	91 (88)	91 (88)	
物流		物流事業者、業界団体（一部抽出）	16 (21)	10 (7)	
化学		石油化学事業者	9(-)	9(-)	
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		－－－	**3,507（3,391）**	**3,281(3,228)**	－－－

＊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：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：4月1日）

4．調査結果の総括 (1/2)

(1) 調査結果の概要

- ◆ 昨年度と比して回答数が増加したが、各項目の調査結果は概ね昨年度結果と同等の傾向であった。
- ◆ 従業員数1,000名を境に行った各集計の結果からは、相対的に取組が進んでいる対策項目は従業員数の多寡を問わず概ね同様であること、各項目とも従業員数1,000名以上の事業者等の取組状況の方が進んでいることがうかがえた。

①PDCAサイクルに沿った継続的な対策

- ✓ 全回答の集計結果における「初期対応」（PDCAのうちP（規定、体制、構築）の一部が該当）の実施率は概ね85%超。「継続的改善の起点となる課題抽出に基づく改善」（PDCAのうちCA（課題抽出・改善））の実施率は概ね５割程度の項目と概ね３割以下の項目に2分化されている。
- ✓ 従業員数別の集計結果における「初期対応」の実施率については、1,000名以上の事業者では95%程度、1,000名未満の事業者では８割程度。また、「継続的改善の起点となる課題抽出に基づく改善」の実施率については、1,000名以上の事業者では一部項目が３割程度も総じて概ね７割程度、1,000名未満の事業者では一部項目が５割程度も総じて概ね３割程度。

②経営層の在り方

- ✓ 全回答の集計結果における「経営層の関与」状況は、「重点化対策の合意」が約８割、「運用状況の把握」が約５割。
- ✓ 2015年度調査での「運用状況の把握」においては、1,000名以上の事業者では８割弱、1,000名未満の事業者では55%程度。
- ✓ 経営資源の継続的な確保に関連して、「対策費用補助の制度化」、「IT人材育成のための支援」、「最小限の負担で対応できるような支援」等の国に対する要望等の意見があった。

③事業者等による自らの責任における実施状況

- ✓ 昨年度調査にて指針_本編・対策編を両方知っていた事業者のうち、約1/3の事業者が指針_手引書を認知していない。
- ✓ 「企業の水準に合わせた、水準別対策などがあると、目標とし易いのではないか」との意見があった。

④情報共有体制

- ✓ 重要インフラサービスでの障害発生時の情報提供体制は、サービス利用者や所管省庁向けが８割超で存在、業界窓口向けは55%程度で存在。
- ✓ 「大規模なサイバー攻撃、セキュリティインシデント発生時の迅速な情報提供」を求める意見があった。

⑤広報公聴活動

- ✓ 指針等に関して「周知・広報活動、内容の説明がある定期的なセミナー開催」を求める意見、要点のみが明確に記載されたパンフレット的な簡略版の作成等の意見があった。

4．調査結果の総括 (2/2)

(2) 課題

①PDCAサイクルに沿った継続的な対策の改善

✓ 継続的改善に向けた「現状の把握」、「課題抽出」の実施・定着が課題と認められる。

②経営層の関与の強化

✓ 「運用状況の把握」、「対策の対外説明」の実施・定着が課題と認められる。

✓ 予算・人材等に係る国の支援への要望を受け、国が行い得る支援についての検討が課題と認められる。

③事業者等による自らの責任における情報セキュリティ対策の推進

✓ 優先順位付けを例示する指針_手引書の認知度の向上を通じた掲題の対策の推進が課題と認められる。

④情報共有体制の推進

✓ 共有すべき情報の範囲の見直しや情報共有の活性化が課題と認められる。

⑤広報公聴活動の強化

✓ 第３次行動計画や改訂後の指針に関し、周知・啓発を進める必要が認められる。

(３) 今後の対応

✓ 第３次行動計画が目指す「重要インフラにおけるサービスの持続的な提供」に向け、経営層の総合的判断の下、「情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するもの」との考えに基づき、情報セキュリティ対策の継続的改善が行われるよう、取り組んでいく必要がある。

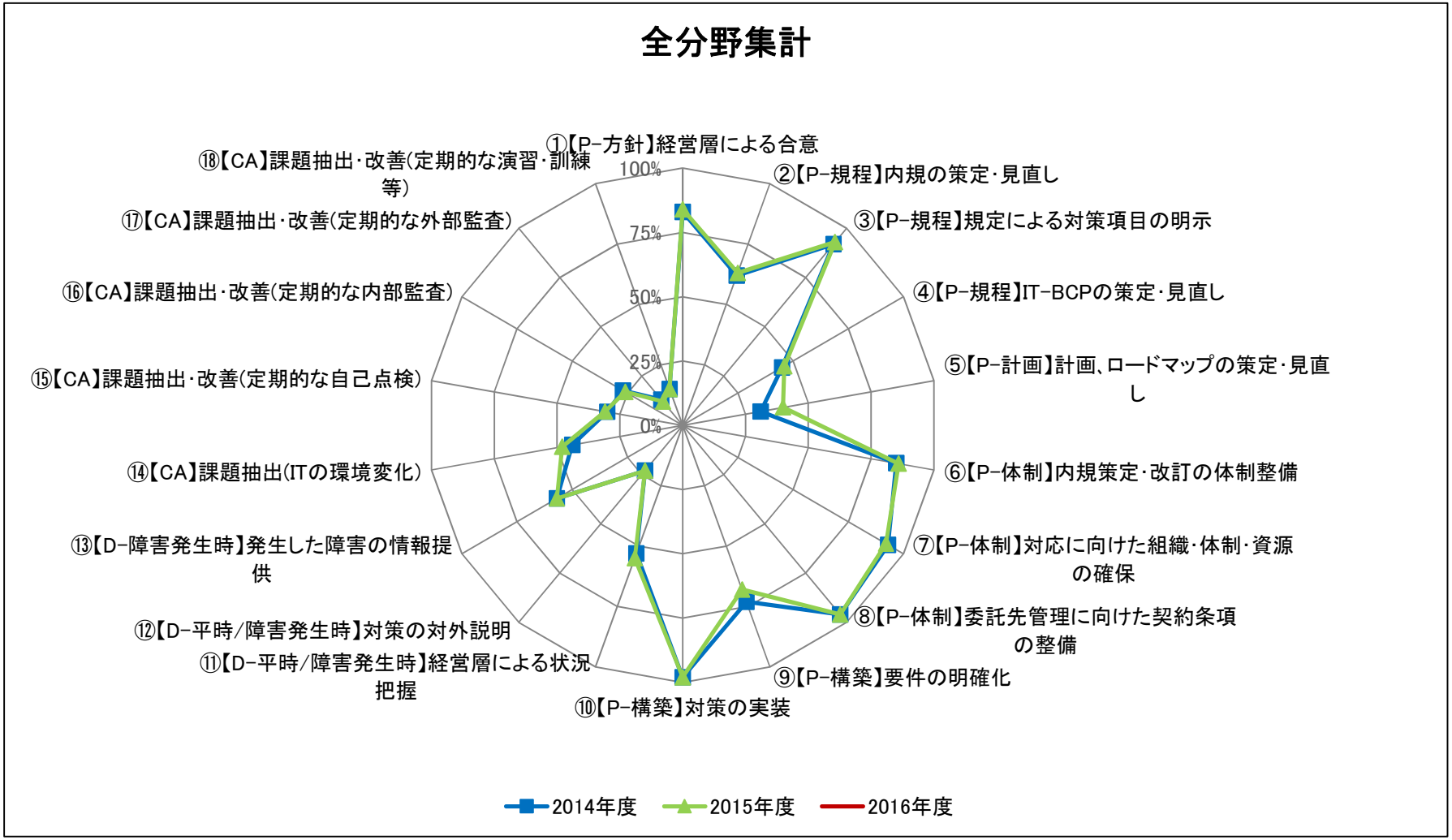
✓ 引き続き、重要インフラ事業者等との意見交換の場等を通じて、行動計画や指針が示す目的や考え方等の浸透を推進するとともに、国による支援の改善に資する情報や意見の収集に係る取組を、より充実させることとしたい。

５．調査結果

＜以降に示す各データの目次＞

5．調査結果 － 主要な基礎データ(１/８) －

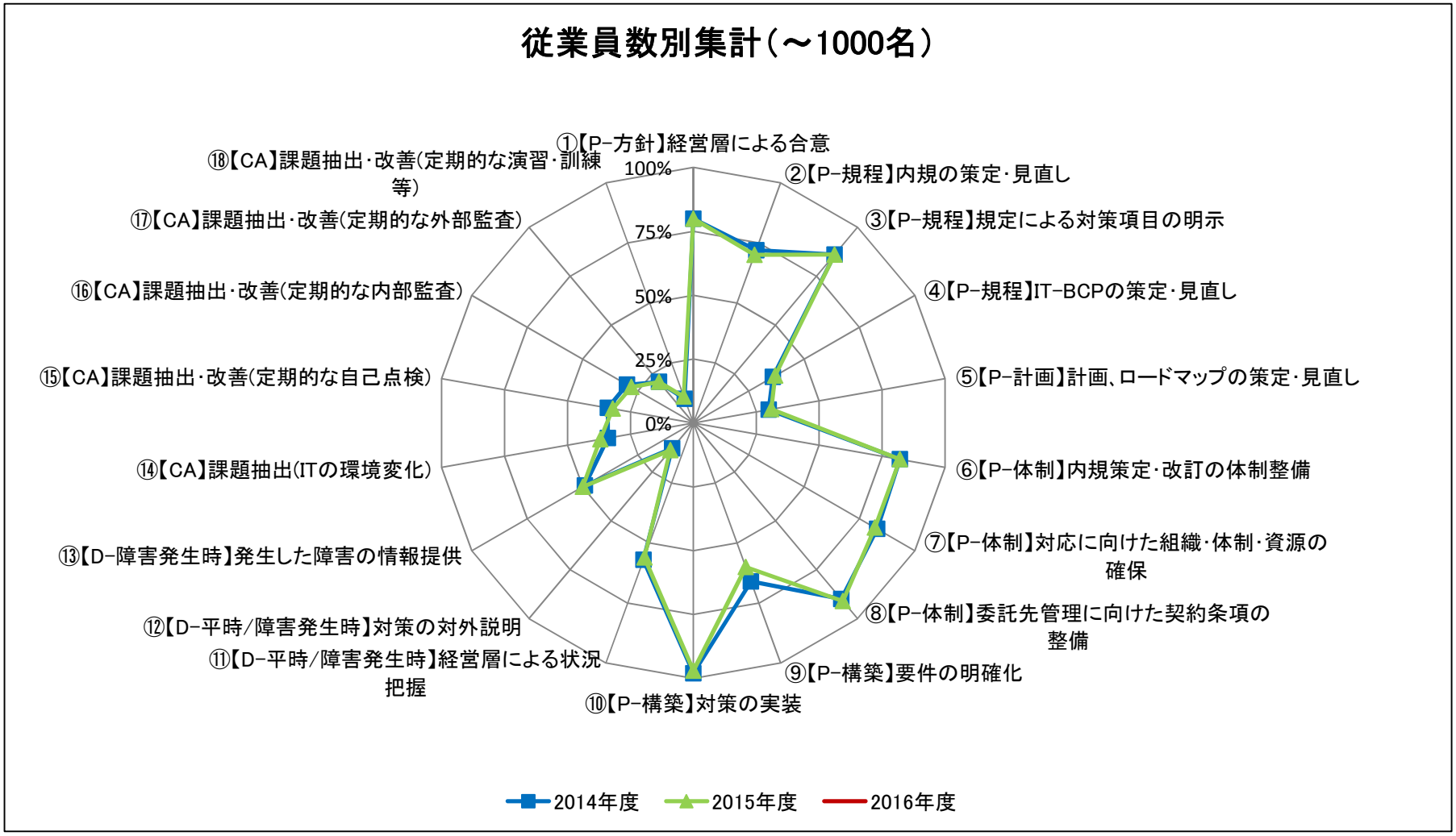
(1) PDCAに沿った情報セキュリティ対策の取組（その１：全体）



項目	2014年度	2015年度
①	83%	84%
②	62%	63%
③	92%	93%
④	45%	46%
⑤	31%	40%
⑥	85%	86%
⑦	93%	92%
⑧	96%	96%
⑨	73%	68%
⑩	98%	98%
⑪	53%	55%
⑫	23%	23%
⑬	57%	57%
⑭	44%	48%
⑮	30%	31%
⑯	27%	26%
⑰	13%	12%
⑱	15%	15%

5．調査結果　－　主要な基礎データ(２/８）－

(1)　PDCAに沿った情報セキュリティ対策の取組（その２：従業員数別（1000名未満））

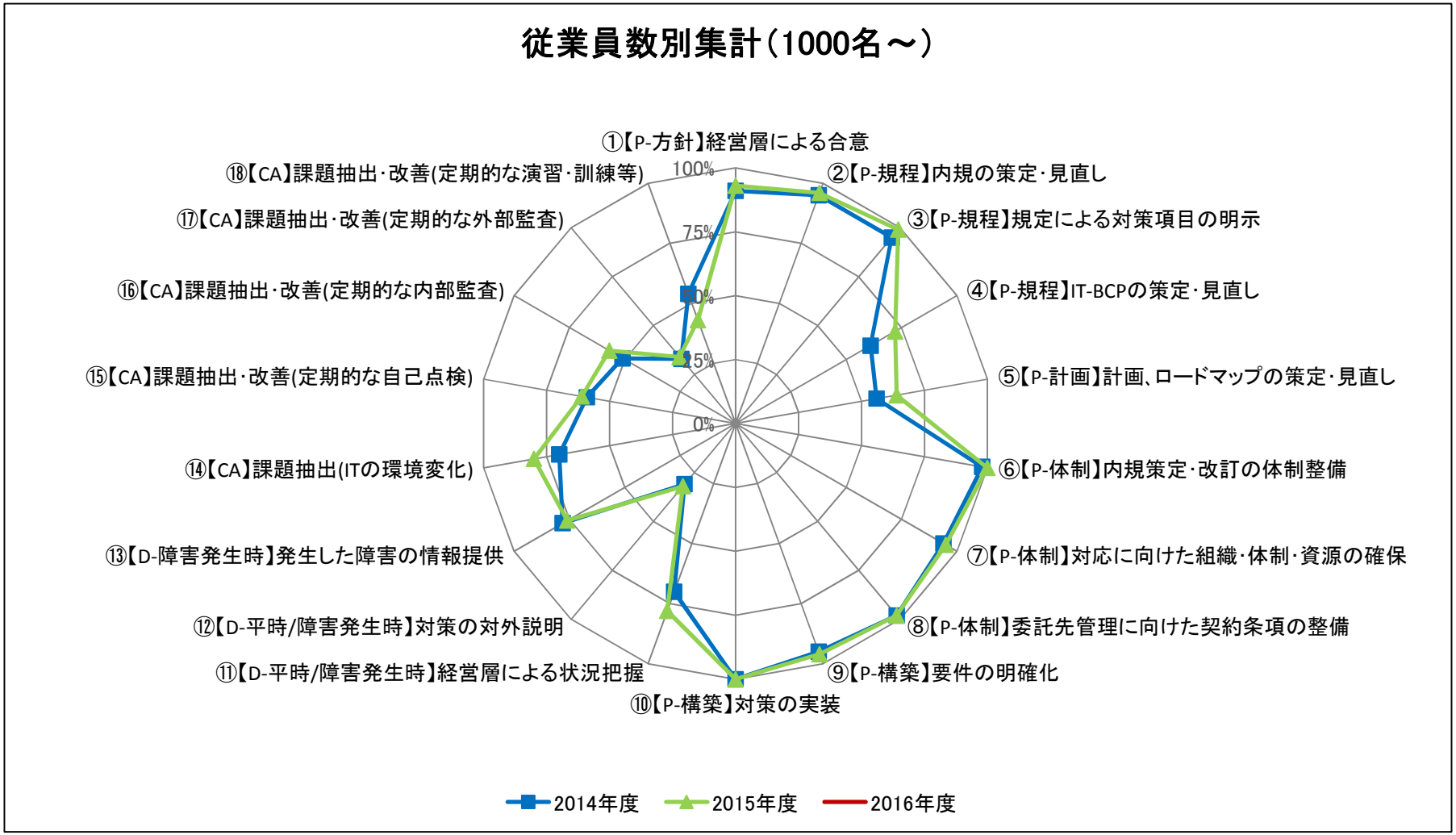


項目	2014年度	2015年度
①	80%	80%
②	72%	70%
③	86%	86%
④	36%	37%
⑤	30%	31%
⑥	82%	82%
⑦	83%	82%
⑧	90%	91%
⑨	66%	60%
⑩	98%	97%
⑪	57%	56%
⑫	13%	14%
⑬	49%	50%
⑭	34%	37%
⑮	34%	32%
⑯	30%	28%
⑰	21%	21%
⑱	10%	11%

※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、集計対象に含めず

5．調査結果 － 主要な基礎データ(３/８) －

(1) PDCAに沿った情報セキュリティ対策の取組（その３：従業員数別（1000名以上））

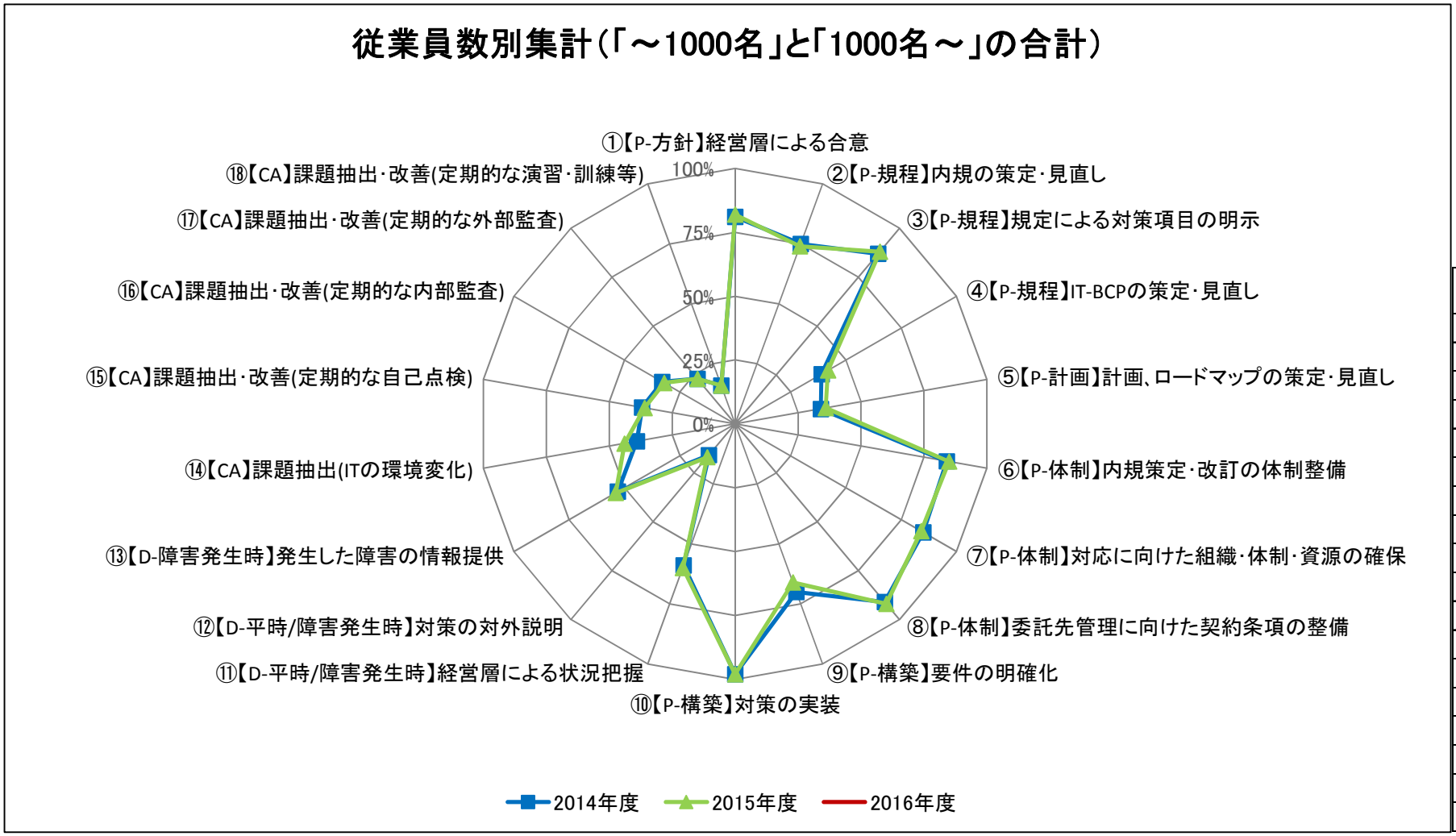


項目	2014年度	2015年度
①	91%	93%
②	95%	96%
③	95%	99%
④	61%	72%
⑤	56%	64%
⑥	98%	100%
⑦	94%	95%
⑧	98%	98%
⑨	95%	96%
⑩	100%	100%
⑪	70%	78%
⑫	31%	32%
⑬	78%	76%
⑭	70%	80%
⑮	59%	61%
⑯	51%	57%
⑰	33%	34%
⑱	54%	43%

※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、集計対象に含めず

4．調査結果 － 主要な基礎データ(４/８) －

(1) PDCAに沿った情報セキュリティ対策の取組（その4：従業員数別（1,000名未満と1,000名以上の合計））

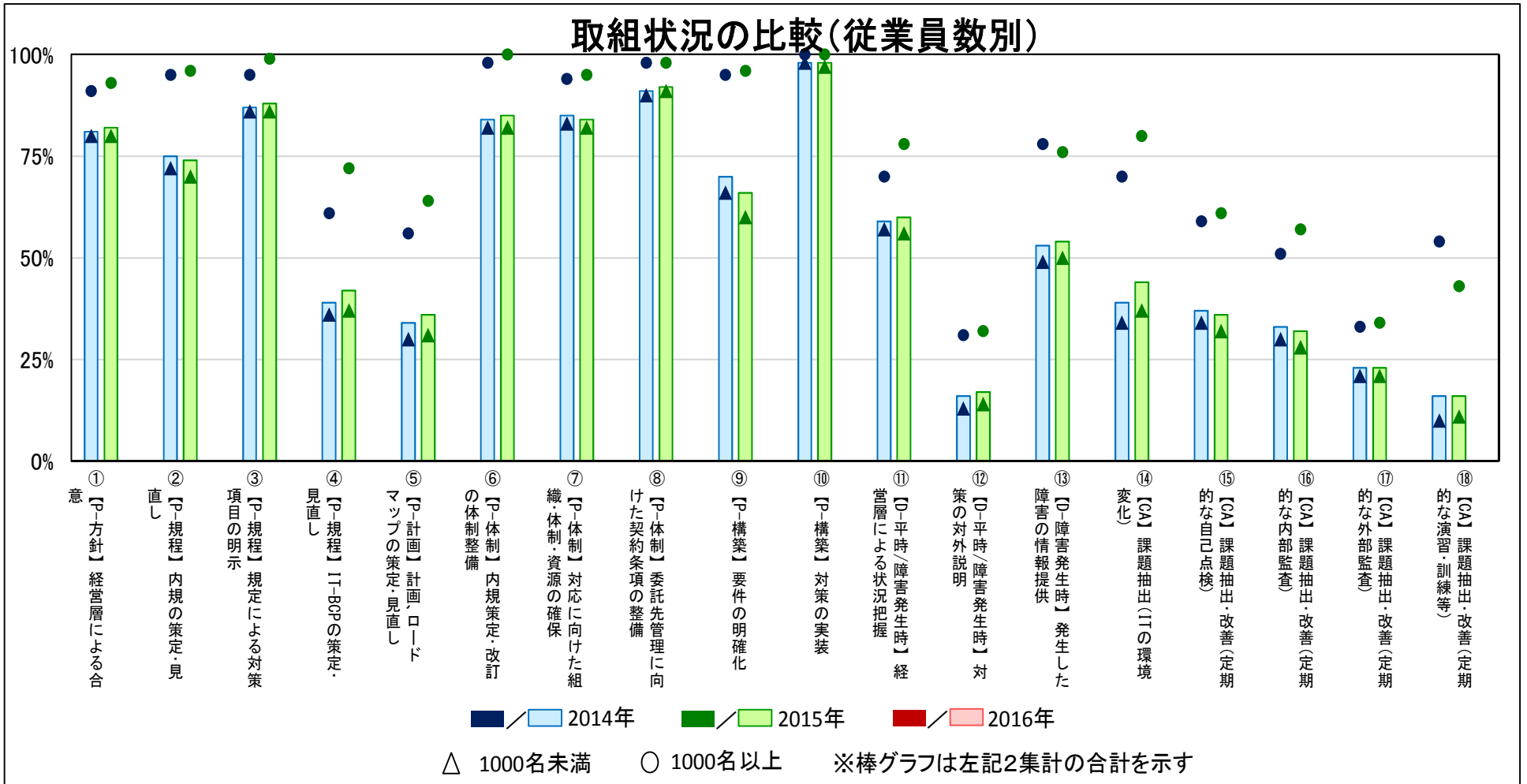


項目	2014年度	2015年度
①	81%	82%
②	75%	74%
③	87%	88%
④	39%	42%
⑤	34%	36%
⑥	84%	85%
⑦	85%	84%
⑧	91%	92%
⑨	70%	66%
⑩	98%	98%
⑪	59%	60%
⑫	16%	17%
⑬	53%	54%
⑭	39%	44%
⑮	37%	36%
⑯	33%	32%
⑰	23%	23%
⑱	16%	16%

※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、集計対象に含めず

5．調査結果 － 主要な基礎データ(５/８) －

(1) PDCAに沿った情報セキュリティ対策の取組（その５：従業員数別取組状況の比較）



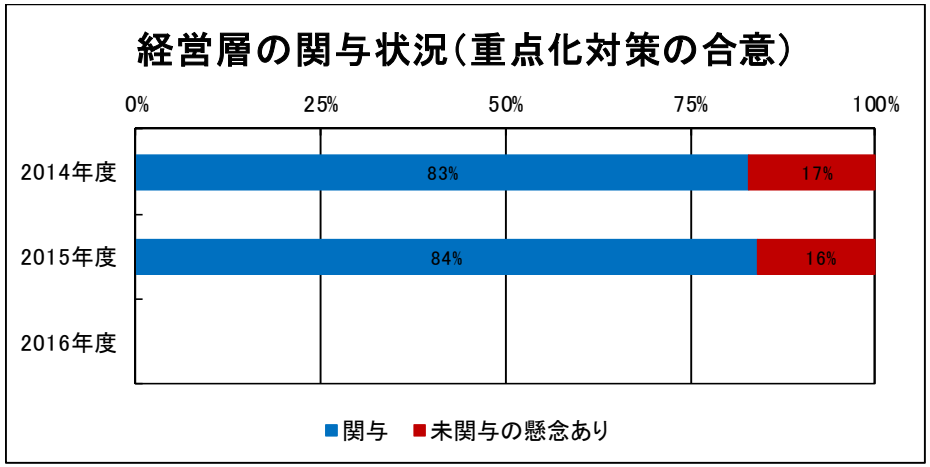
	①			②			③			④			⑤			⑥			⑦			⑧			⑨			⑩			⑪			⑫			⑬			⑭			⑮			⑯			⑰			⑱		
	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□
2014年度	80%	91%	81%	72%	95%	75%	86%	95%	87%	36%	61%	39%	30%	56%	34%	82%	98%	84%	83%	94%	85%	90%	98%	91%	66%	95%	70%	98%	100%	98%	57%	70%	59%	13%	31%	16%	49%	78%	53%	34%	70%	39%	34%	59%	37%	30%	51%	33%	21%	33%	23%	10%	54%	16%
2015年度	80%	93%	82%	70%	96%	74%	86%	99%	88%	37%	72%	42%	31%	64%	36%	82%	100%	85%	82%	95%	84%	91%	98%	92%	60%	96%	66%	97%	100%	98%	56%	78%	60%	14%	32%	17%	50%	76%	54%	37%	80%	44%	32%	61%	36%	28%	57%	32%	21%	34%	23%	11%	43%	16%

※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、集計対象に含めず

5．調査結果 － 主要な基礎データ(６/８) －

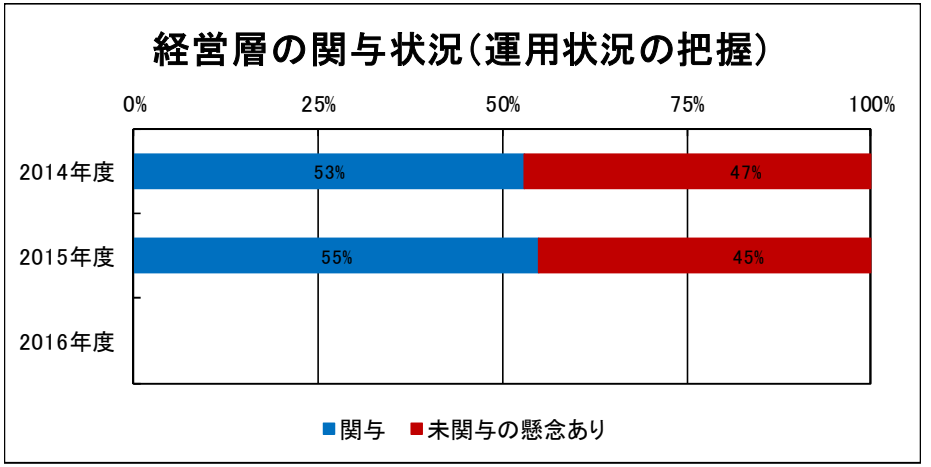
(2) 経営層の関与状況

①重点化対策への経営層の関与状況（P-方針）



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

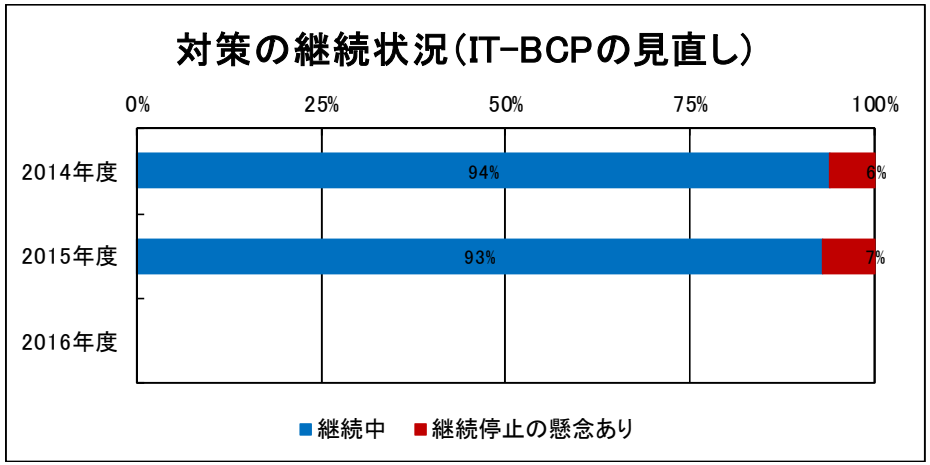
②経営層による運用状況の把握状況（D-平時／障害発生時）



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

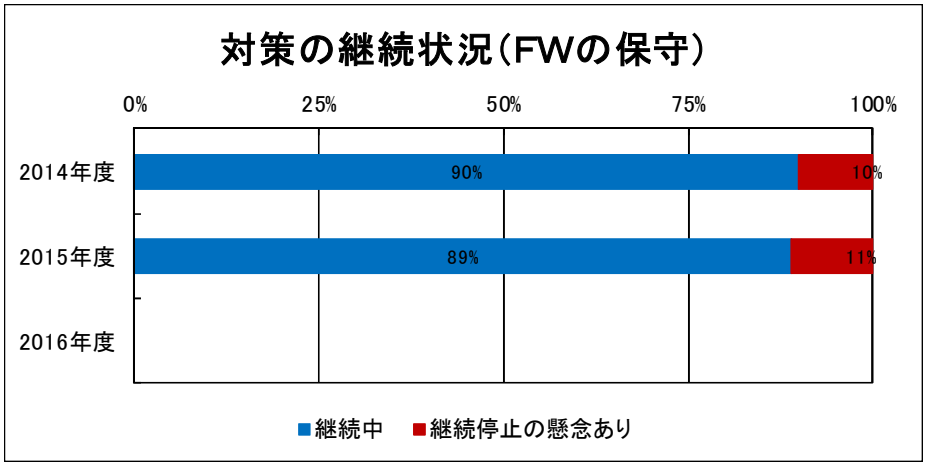
(3) 対策の継続状況

①IT-BCP策定、見直しの継続状況（P-規定）



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

②ファイアウォールの保守継続状況（P-構築）

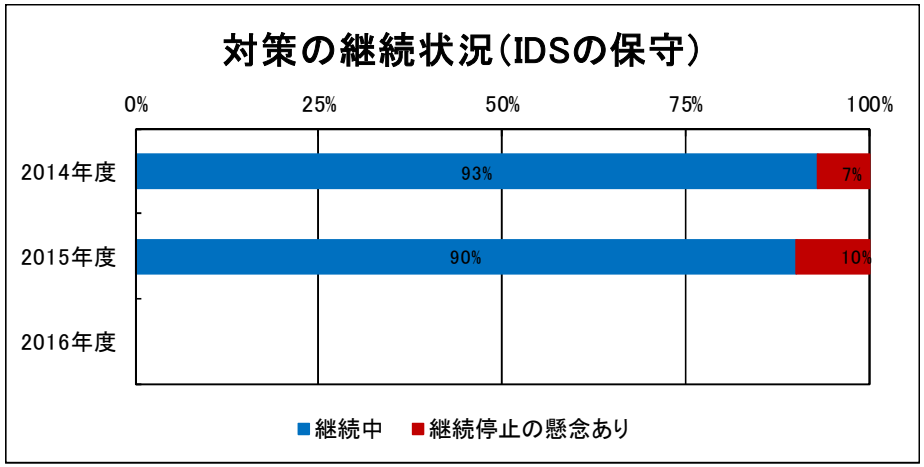


※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

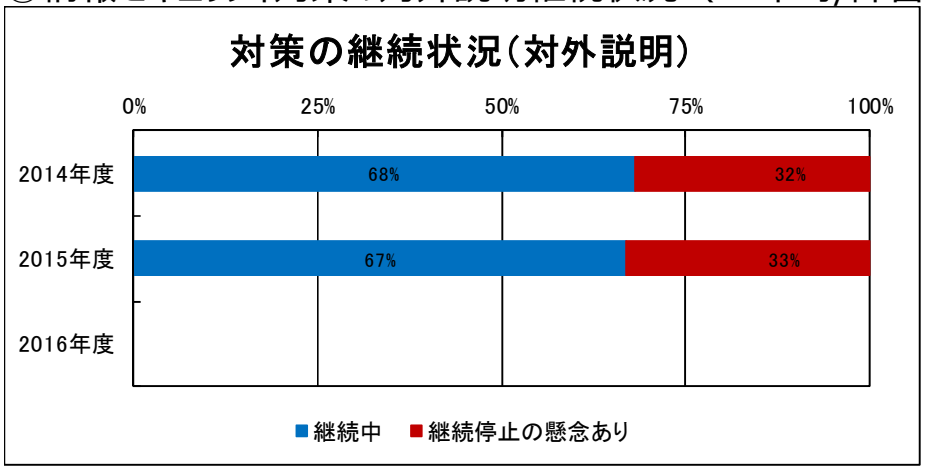
5．調査結果 － 主要な基礎データ(７/８) －

(3) 対策の継続状況（続き）

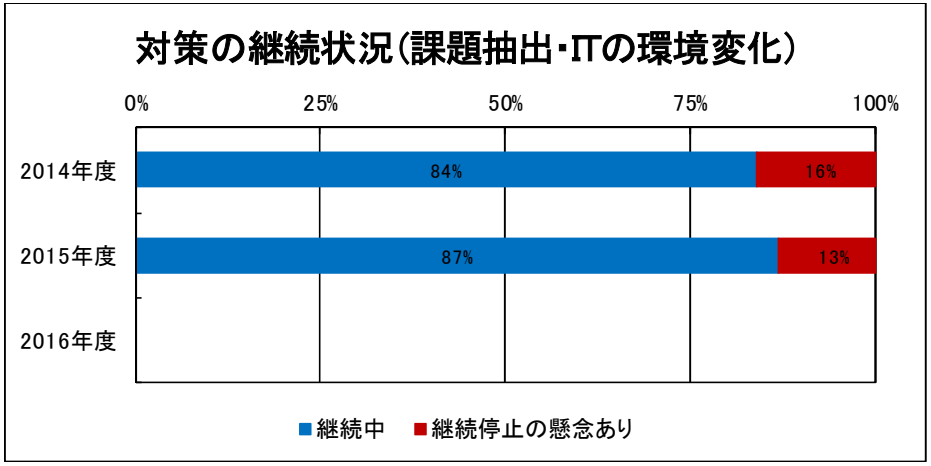
③侵入検知システムの保守継続状況（P-構築）



④情報セキュリティ対策の対外説明継続状況（D-平時/障害発生時）



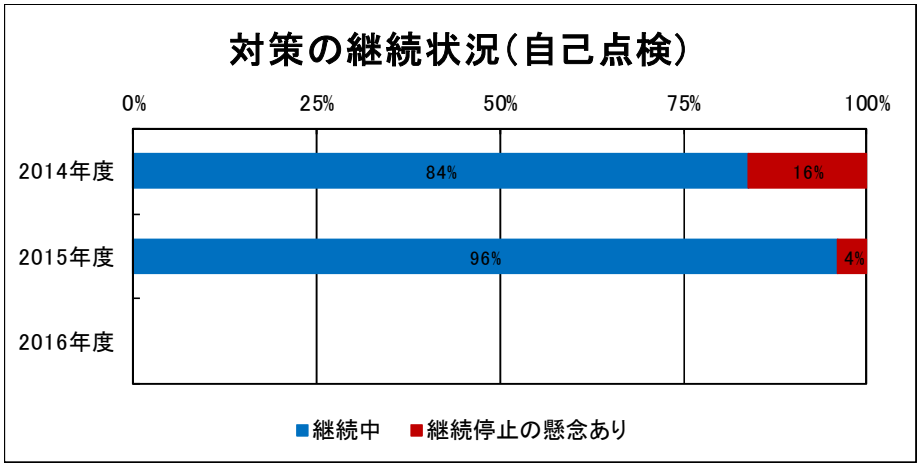
⑤新たなリスク源に係る課題抽出の継続状況（CA）



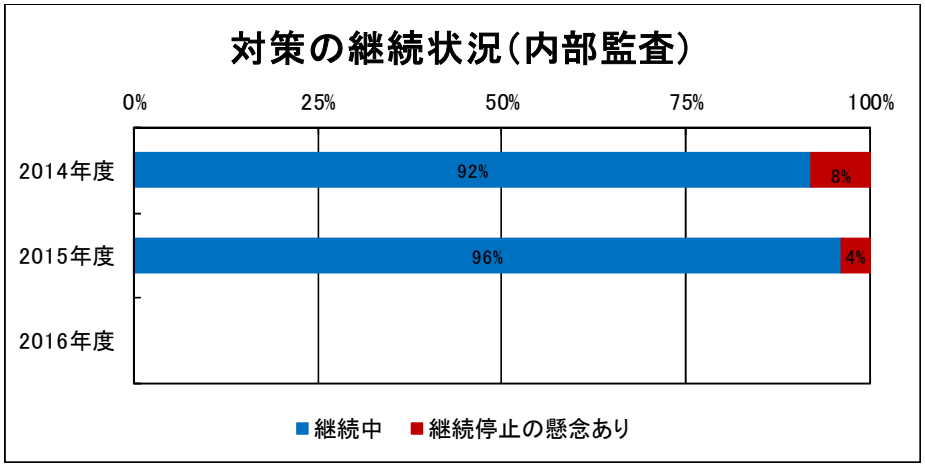
5．調査結果 － 主要な基礎データ(８/８) －

(3) 対策の継続状況（続き）

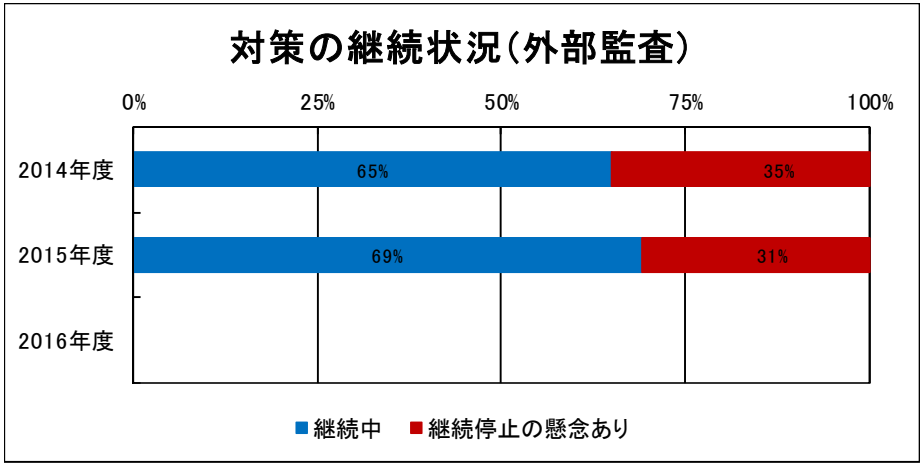
⑥自己点検による課題抽出・改善の継続状況（CA）



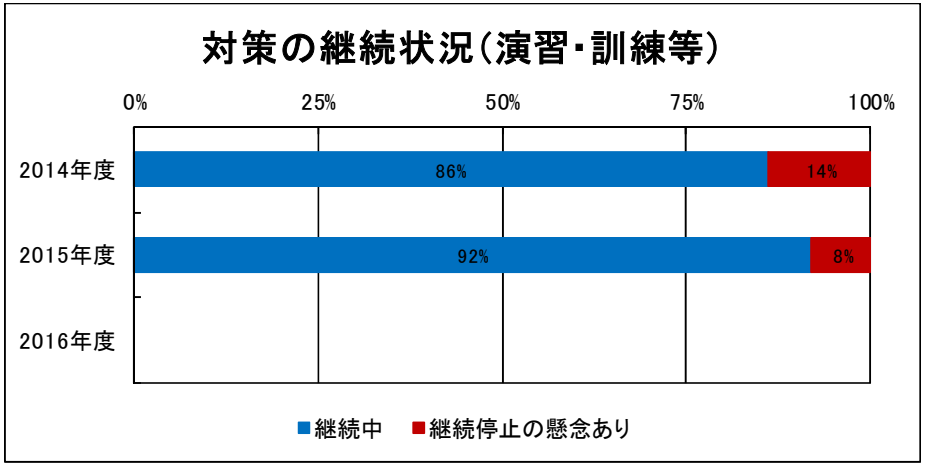
⑦内部監査による課題抽出・改善の継続状況（CA）



⑧外部監査による課題抽出・改善の継続状況（CA）



⑨演習・訓練等による課題抽出・改善の継続状況（CA）



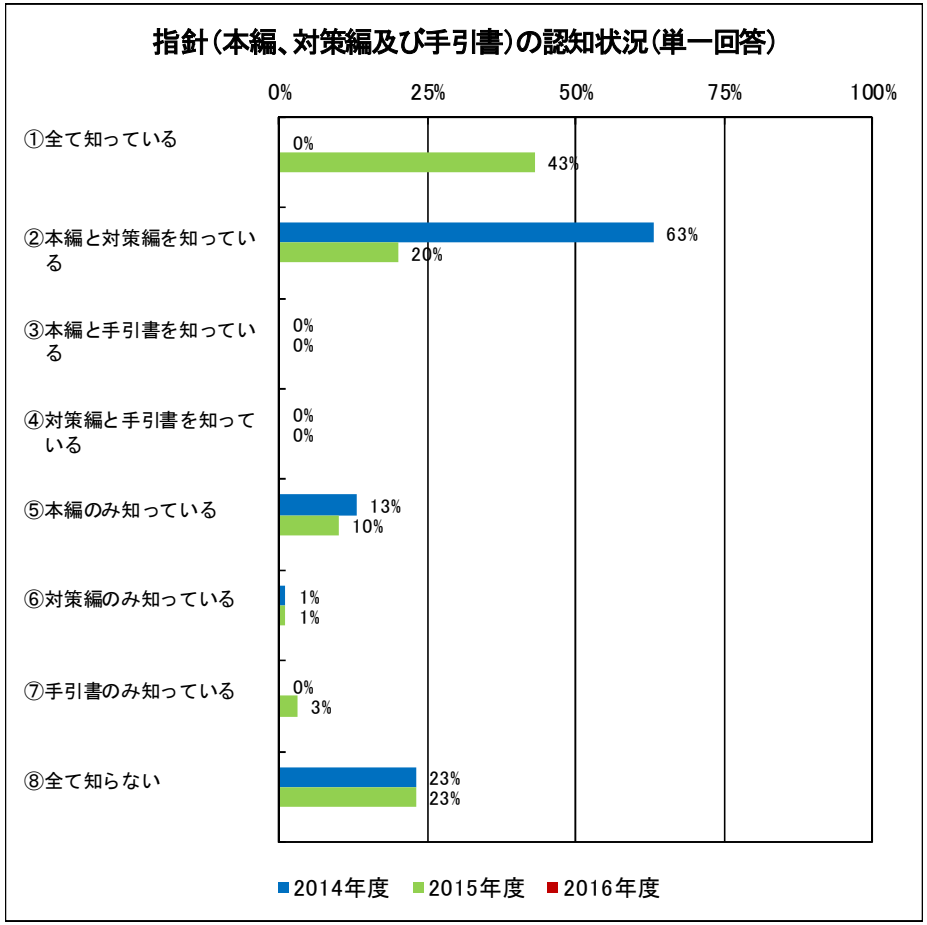
6．調査結果詳細　－　各個別設問のグラフ及び分析(1/19)　－

(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

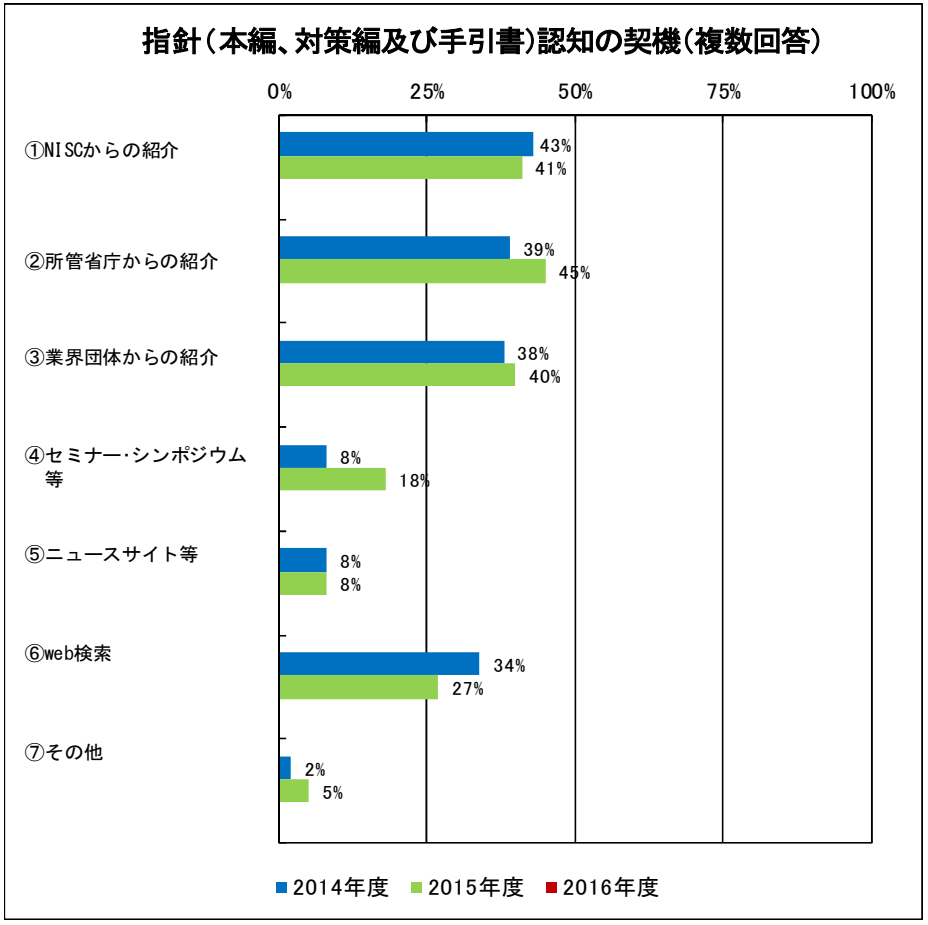
・指針_手引書新設後の初回調査。全て認知している事業者は４割強。２割強は全て認知していない状況。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）
※2015年度の指針_手引書新設に伴い、集計方法もあわせて変更

(b) 指針（本編、対策編及び手引書）認知の契機

・認知の契機は、NISC、所管省庁、業界団体からの各紹介が同程度（４割程度）。この他には、web検索が契機との回答が続く。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

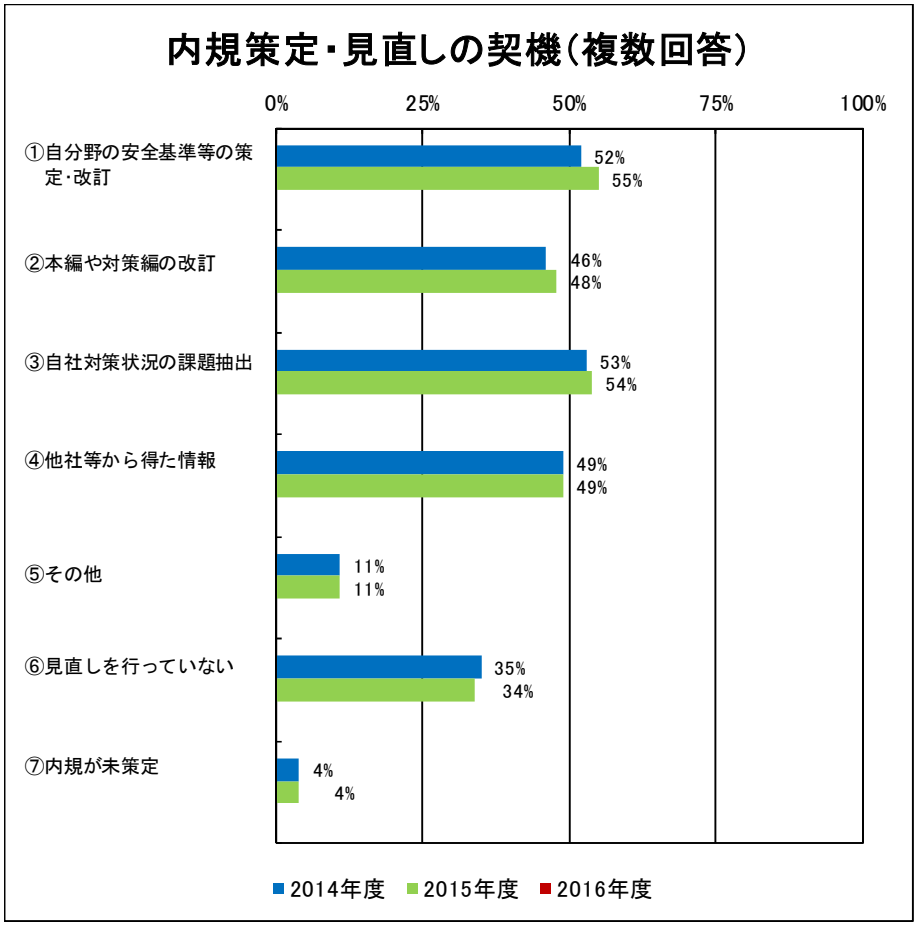
6．調査結果詳細　－　各個別設問のグラフ及び分析(2/19)　－

(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

・内規策定・見直しの契機は、自分野の安全基準等の策定・改訂、指針_本編・対策編の改訂、自社対策状況の課題抽出、他社から得た情報が同程度（５割程度）。
・内規策定後に見直しを行っていない事業者も35%程度存在。



※金融は読替可能項目なし（集計対象に含めず）

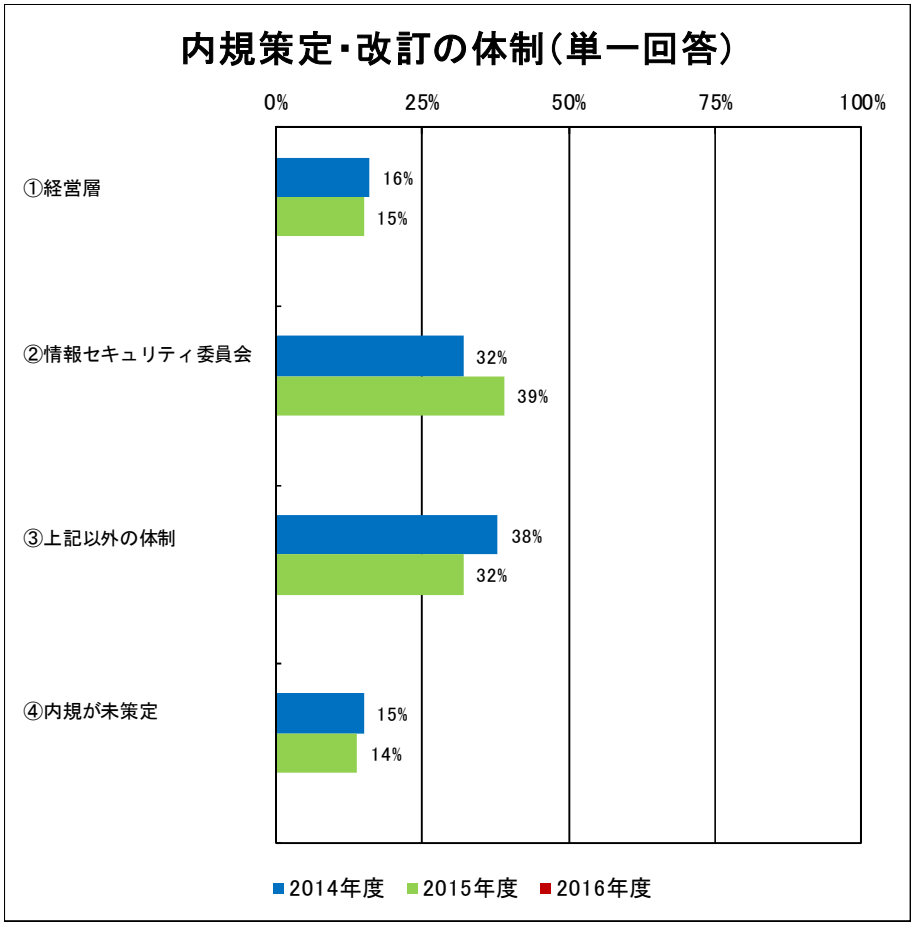
6．調査結果詳細　－　各個別設問のグラフ及び分析(3/19)　－

(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・改訂の体制

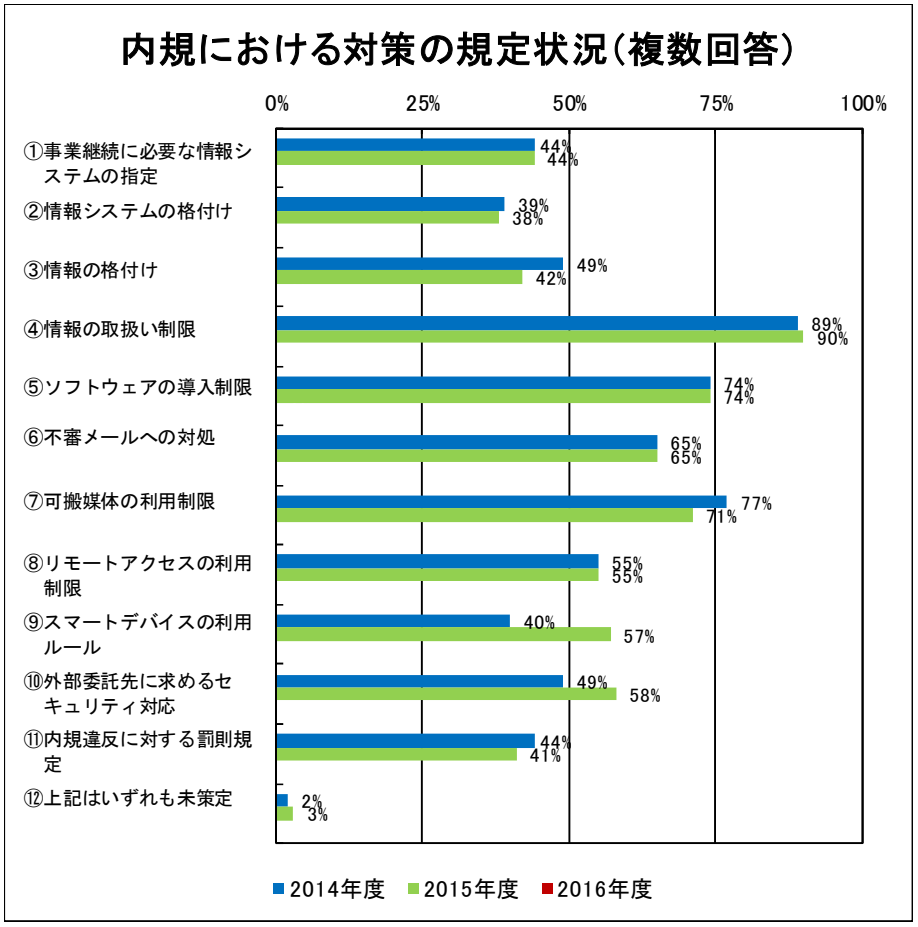
・経営層が関わる割合は15%程度、情報セキュリティ委員会が関わる割合は４割弱、それ以外の体制が関わる割合が４割弱。
・内規が未策定の事業者も15%程度存在。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(b) 内規における対策の規定状況

・情報の取扱い制限、ソフトウェアの導入制限、可搬媒体の利用制限、不審メールへの対処等の対策を規定している割合が相対的に高い。



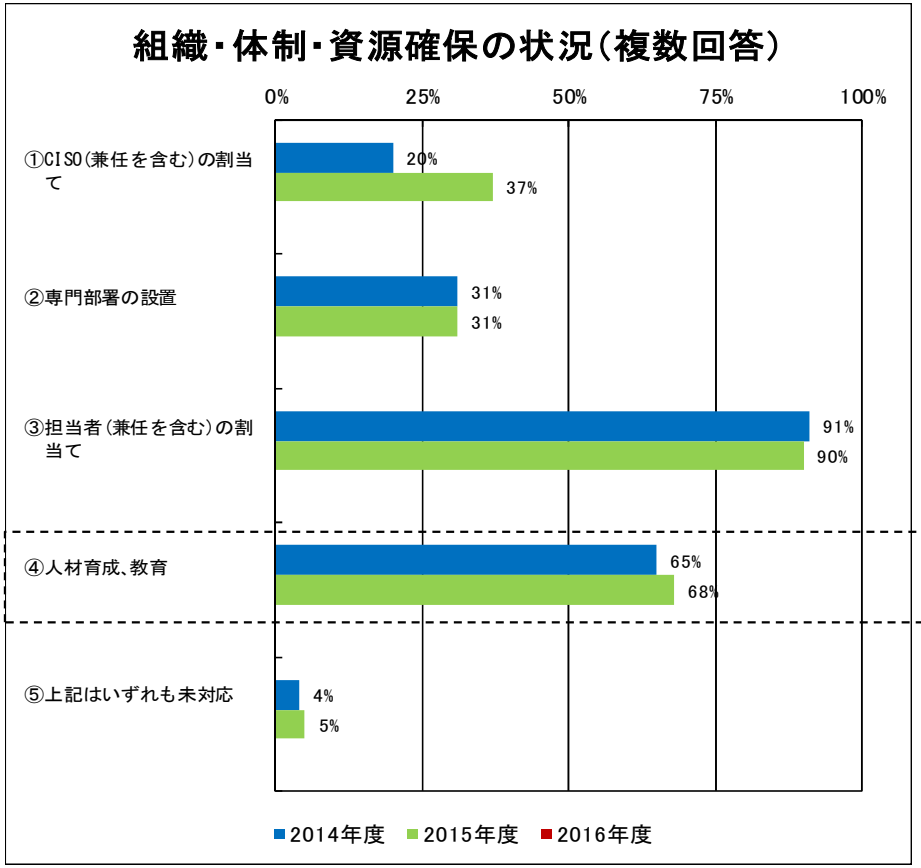
6．調査結果詳細　－　各個別設問のグラフ及び分析(4/19)　－

(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

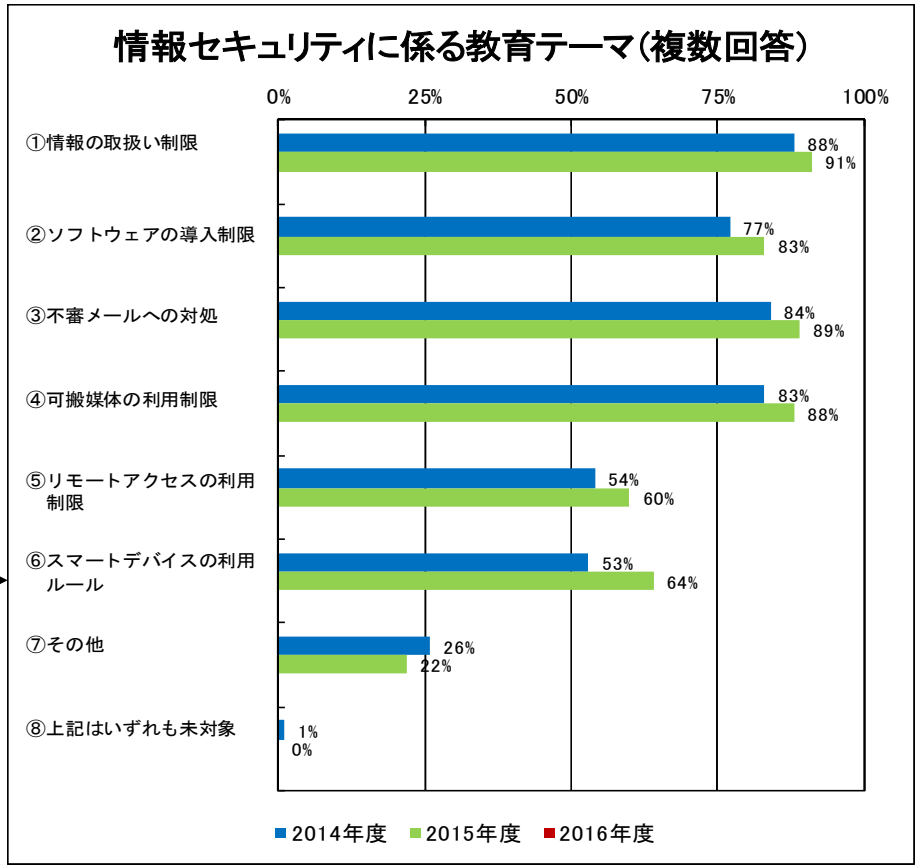
・組織・体制・資源確保として、９割程度の事業者が担当者（兼任を含む）を割り当てている。
・一方、専門部署を設置している事業者は３割強。



※金融は読替可能項目なし（集計対象に含めず）
※政府・行政サービスの調査において、本項目の読替により適した設問が追加されたことから、追加設問を新たに読替項目として適用する（2014年度の報告値には読替を適用しない）

(b) 情報セキュリティに係る教育テーマ

・教育テーマの採用率については、各テーマとも昨年度と比して上昇。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

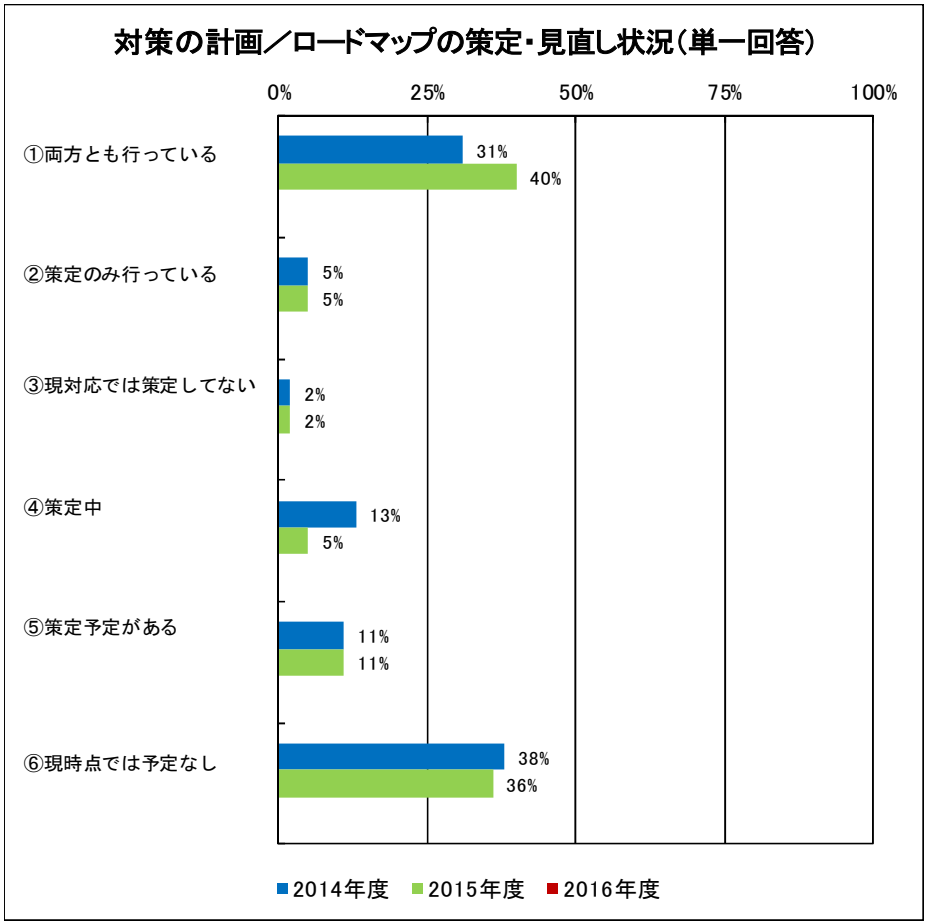
6．調査結果詳細　－　各個別設問のグラフ及び分析(5/19)　－

(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

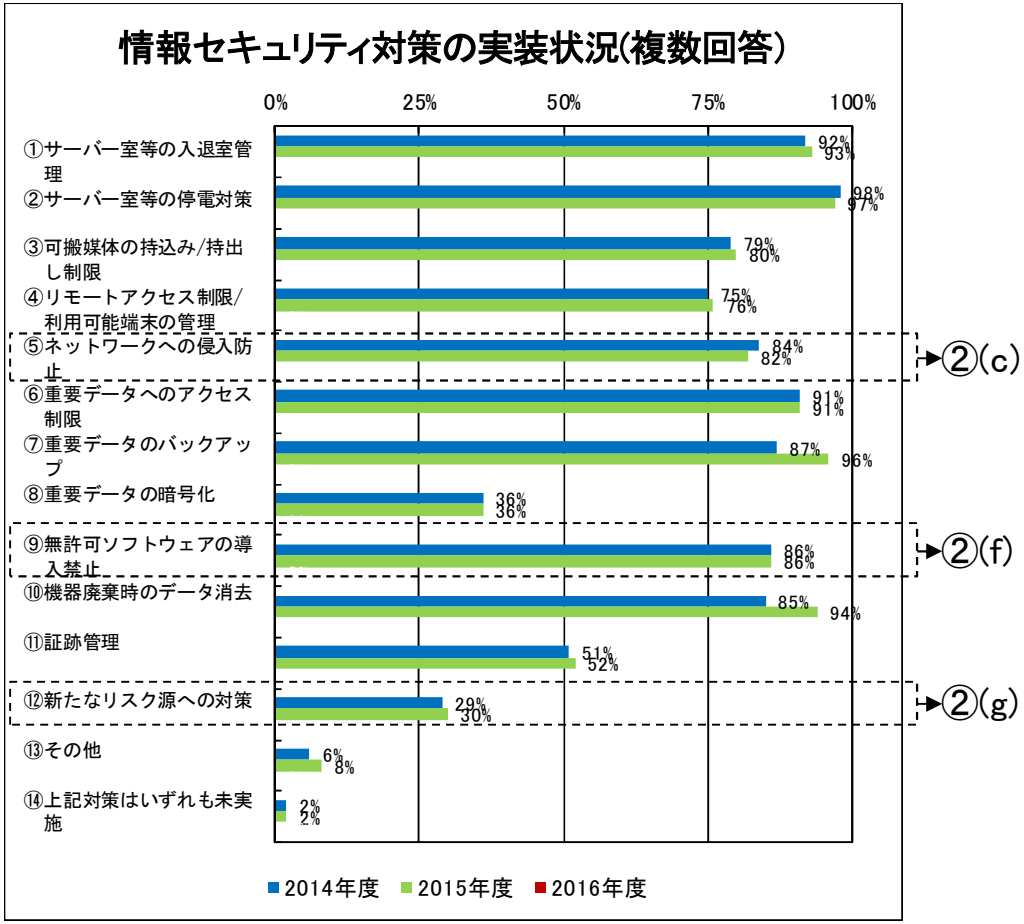
(a) 対策の計画／ロードマップの策定・見直し状況

・対策の計画／ロードマップの策定は45%程度の事業者が行っている。一方、35%程度の事業者は現時点で策定の予定もない。



(b) 情報セキュリティ対策の実装状況

・多くの対策が７割以上の実施率ではあるが、重要データの暗号化、証跡管理、新たなリスク源への対策の実施率は３～５割程度。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

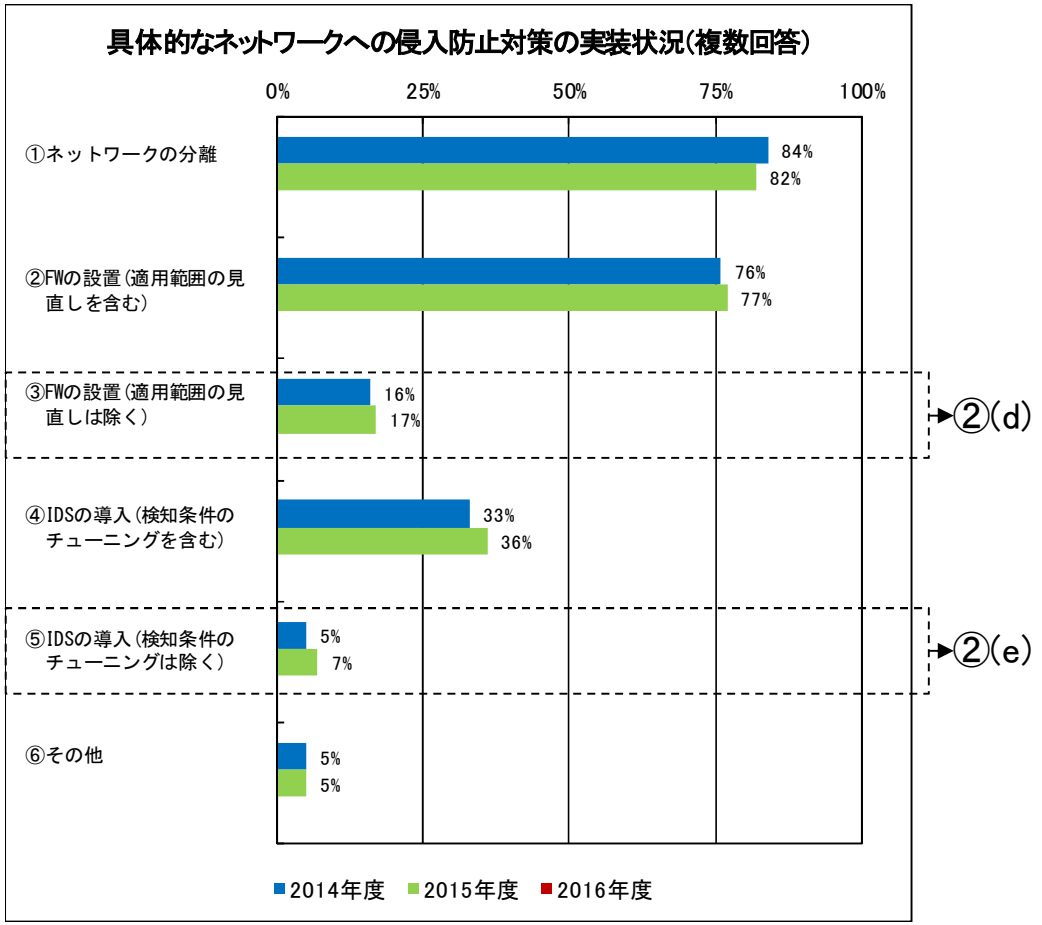
6．調査結果詳細　－　各個別設問のグラフ及び分析(6/19)　－

(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

・ネットワークの分離、ファイアウォールの設置（適用範囲の見直しを含む）の実施率が７～８割程度。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

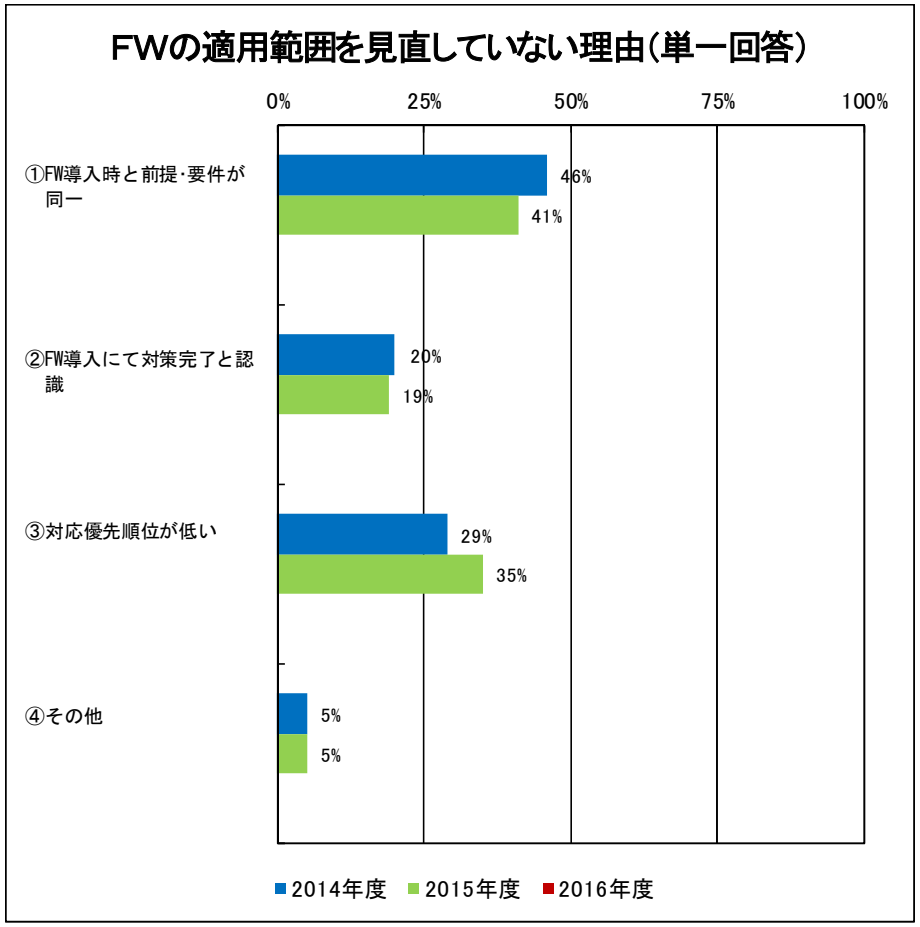
6．調査結果詳細　－　各個別設問のグラフ及び分析(7/19)　－

(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

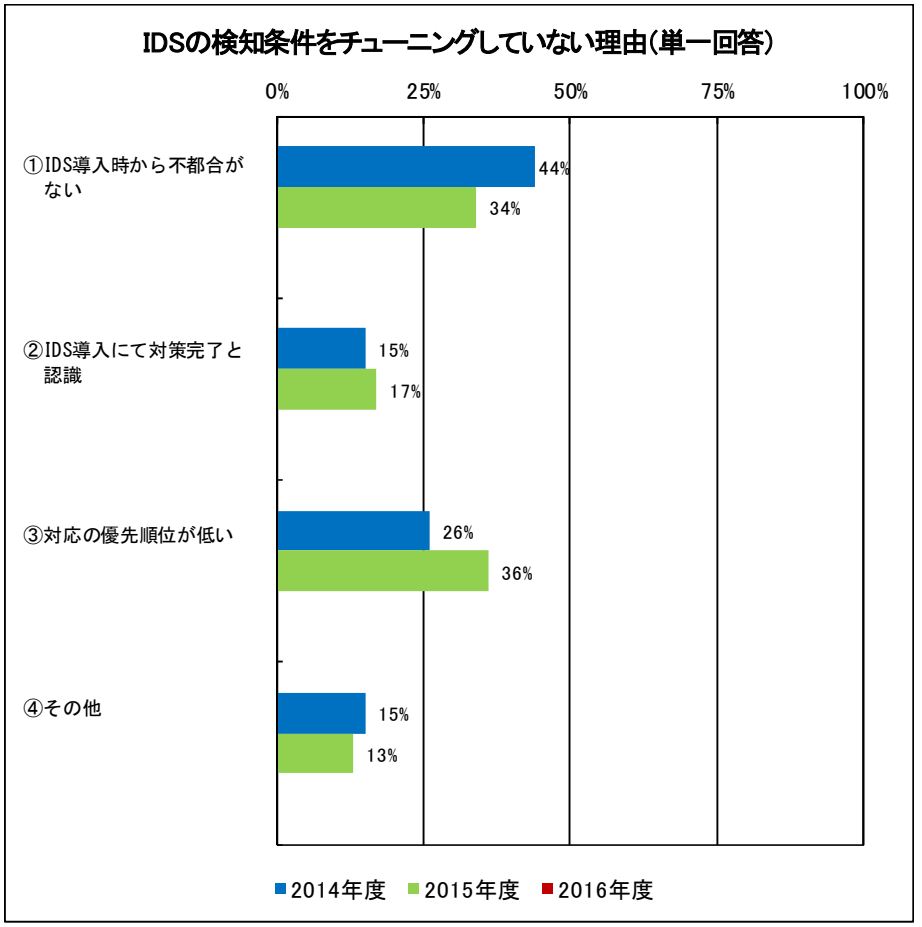
・ファイアウォール導入前と前提・要件が同一との回答が４割強。対応優先順位が低いとの回答が35%程度。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(e) IDSの検知条件をチューニングしていない理由

・導入時から不都合がないとの回答と対応の優先順位が低いとの回答が共に35%程度。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

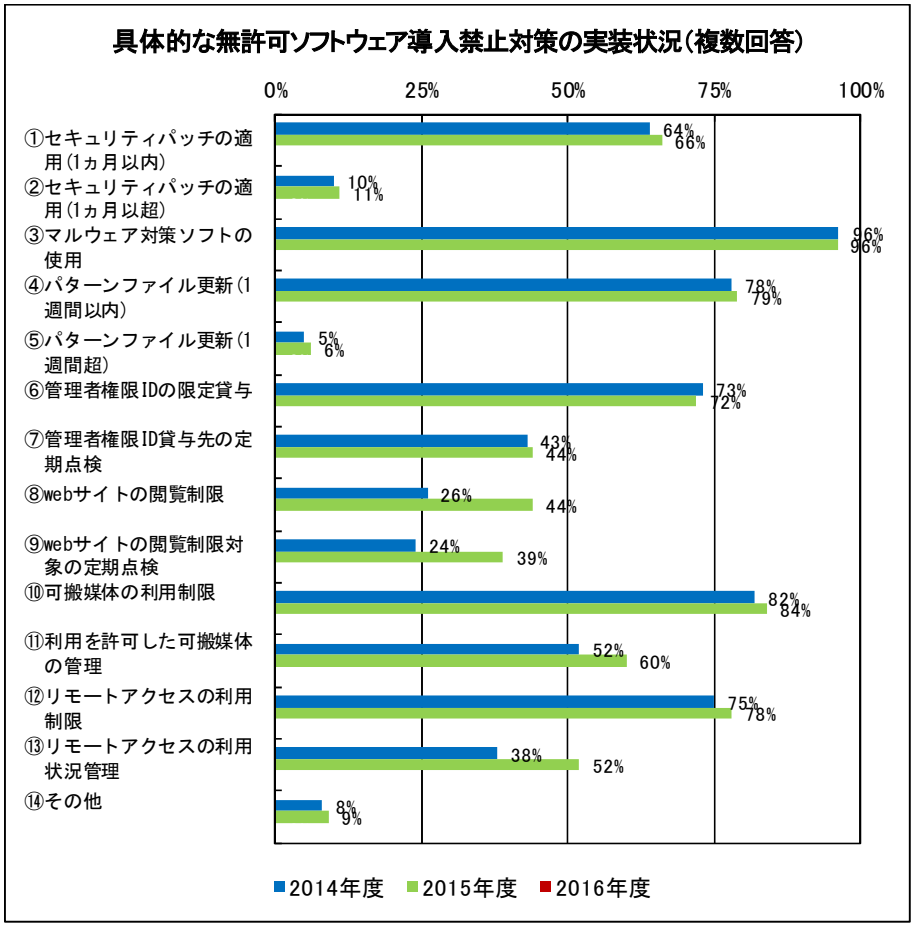
6．調査結果詳細　－　各個別設問のグラフ及び分析(8/19)　－

(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

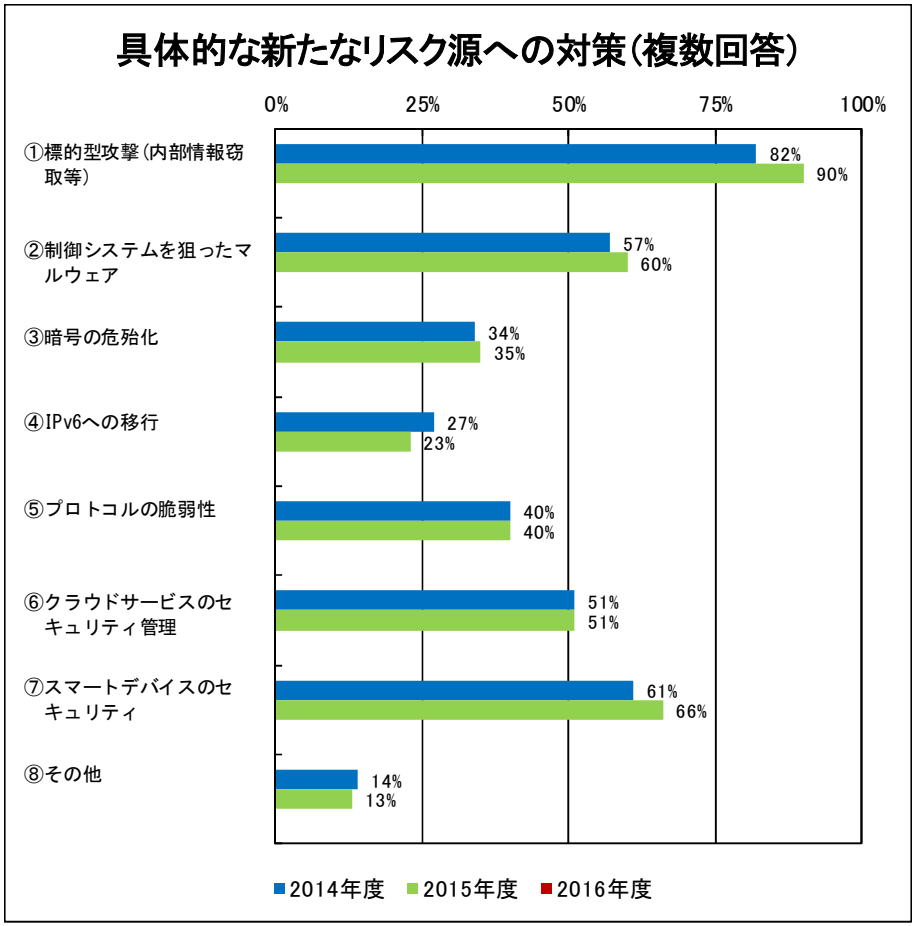
(f) 具体的な無許可ソフトウェア導入禁止対策の実施状況

・マルウェア対策ソフトの使用が95%程度で最多。これに可搬媒体の利用制限、リモートアクセスの利用制限が８割程度で続く。



(g) 具体的な新たなリスク源への対策

・新たなリスク源として対策が行われているのは、標的型攻撃が９割で最多。以降、スマートデバイスのセキュリティ、制御システムを狙ったマルウェアが６割程度。



※政府・行政サービスは読替可能項目なし（集計対象に含めず）

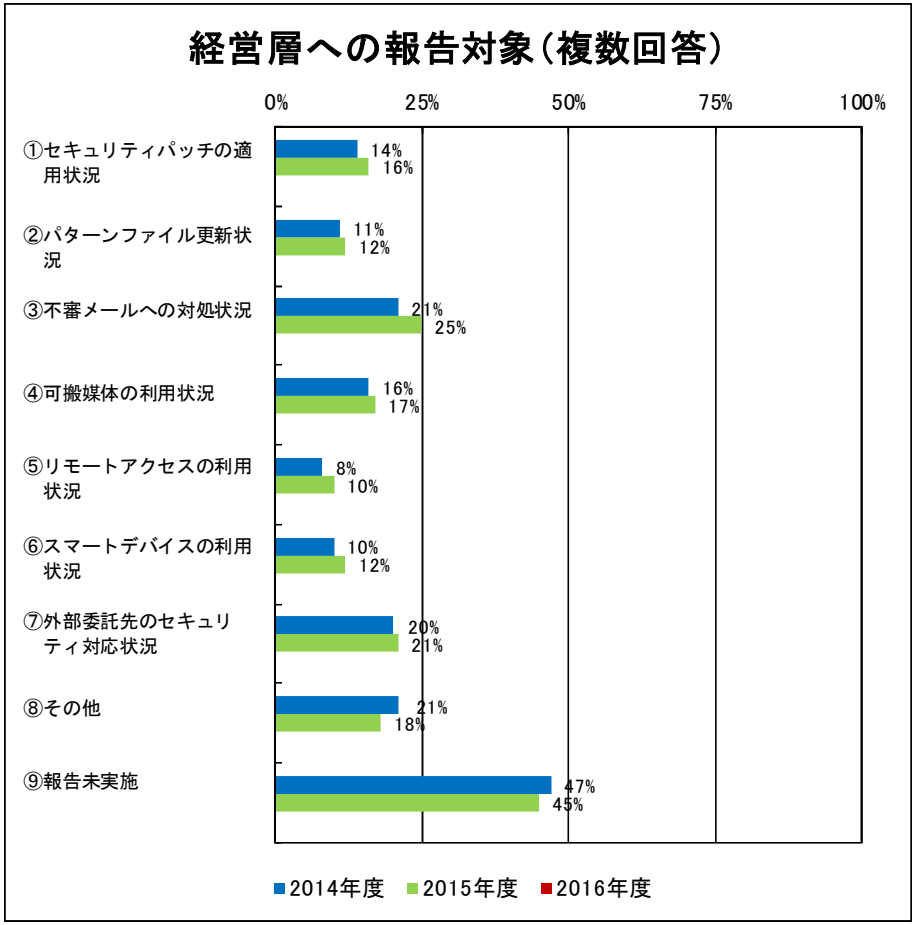
6．調査結果詳細　－　各個別設問のグラフ及び分析(9/19)　－

(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

・各状況とも、報告対象となっているのは概ね１～２割程度。また報告未実施の事業者が半数近くを占める。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

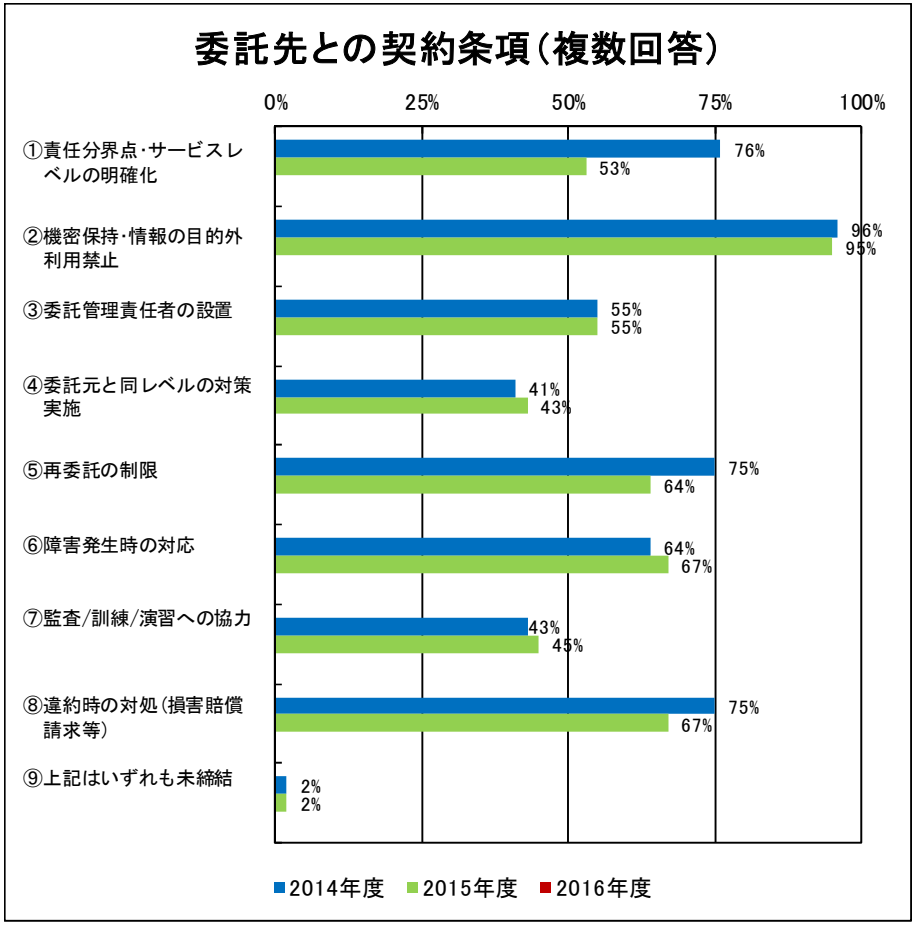
6．調査結果詳細　－　各個別設問のグラフ及び分析(10/19)　－

(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

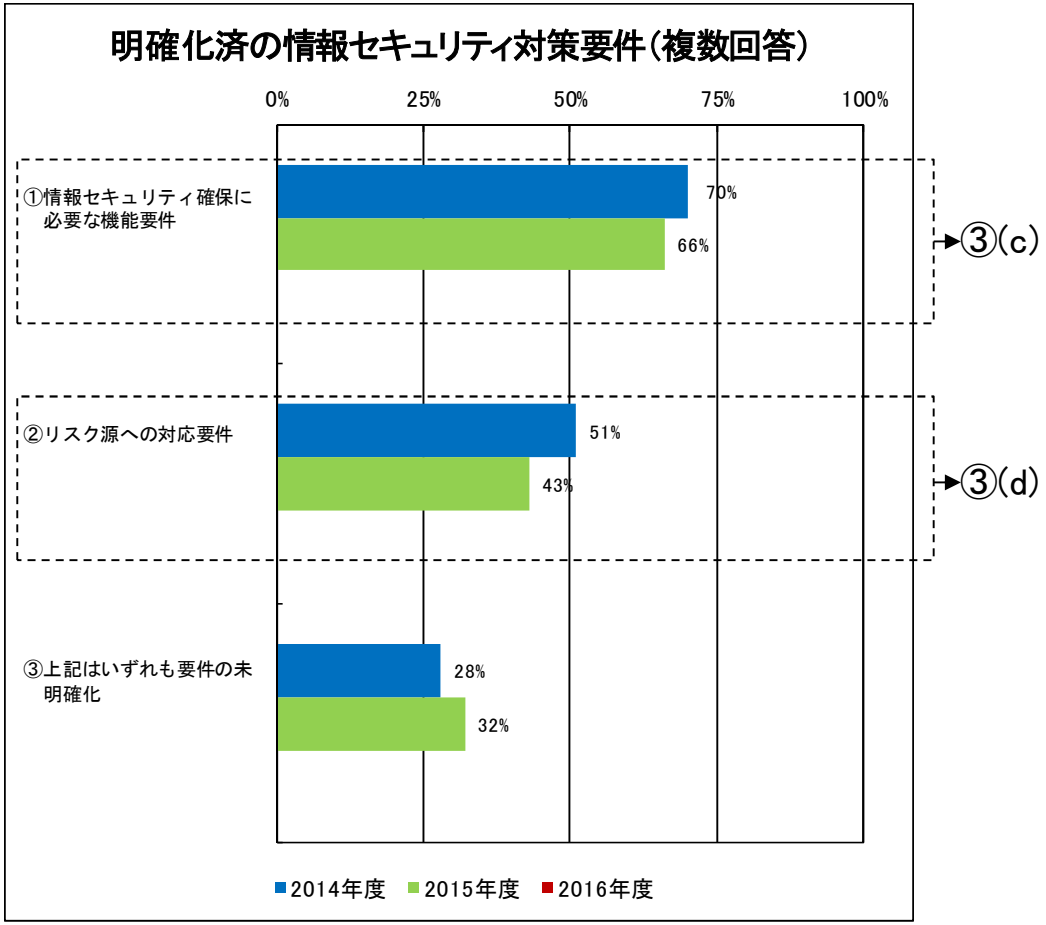
(a) 委託先との契約条項

・95%程度の契約で機密保持・情報の目的外利用禁止の条項が設けられている。
・一方、委託元と同レベルの対策実施、監査／訓練／演習への協力の条項が設けられているのは45%程度。



(b) 明確化済の情報セキュリティ対策要件

・明確化済の情報セキュリティ対策要件については、事業者の65%程度が情報セキュリティ確保に必要な機能要件、５割強がリスク源への対応要件を挙げている。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

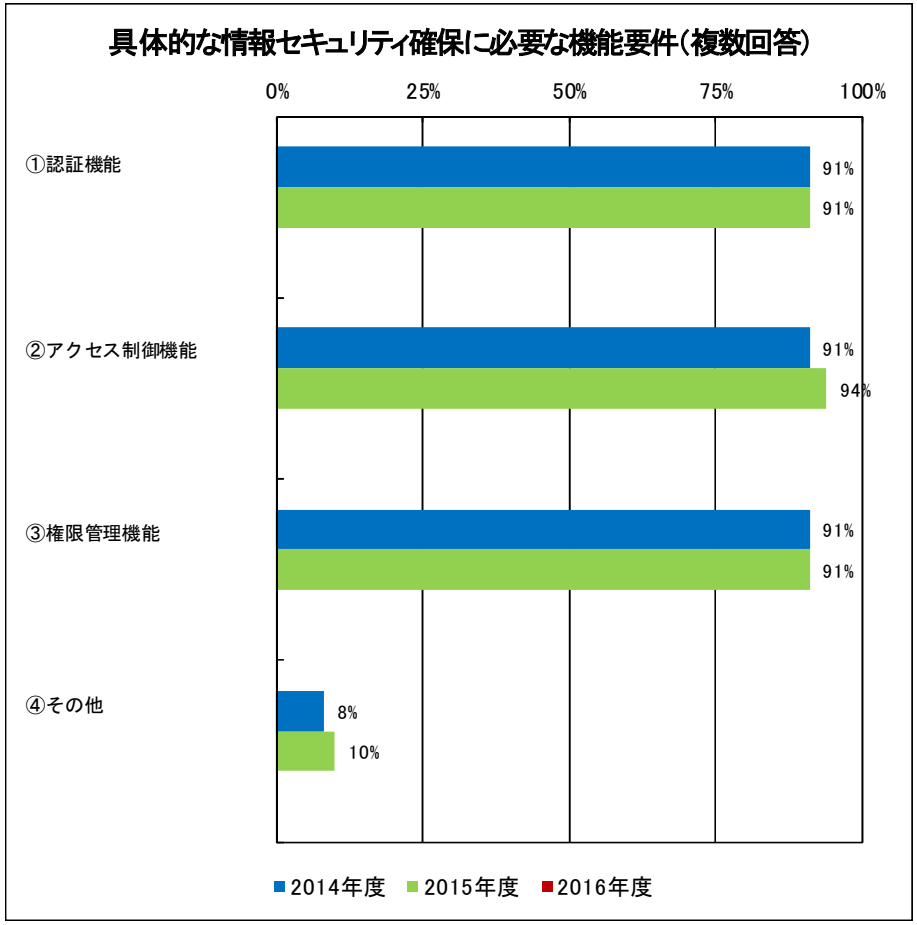
6．調査結果詳細　－　各個別設問のグラフ及び分析(11/19)　－

(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

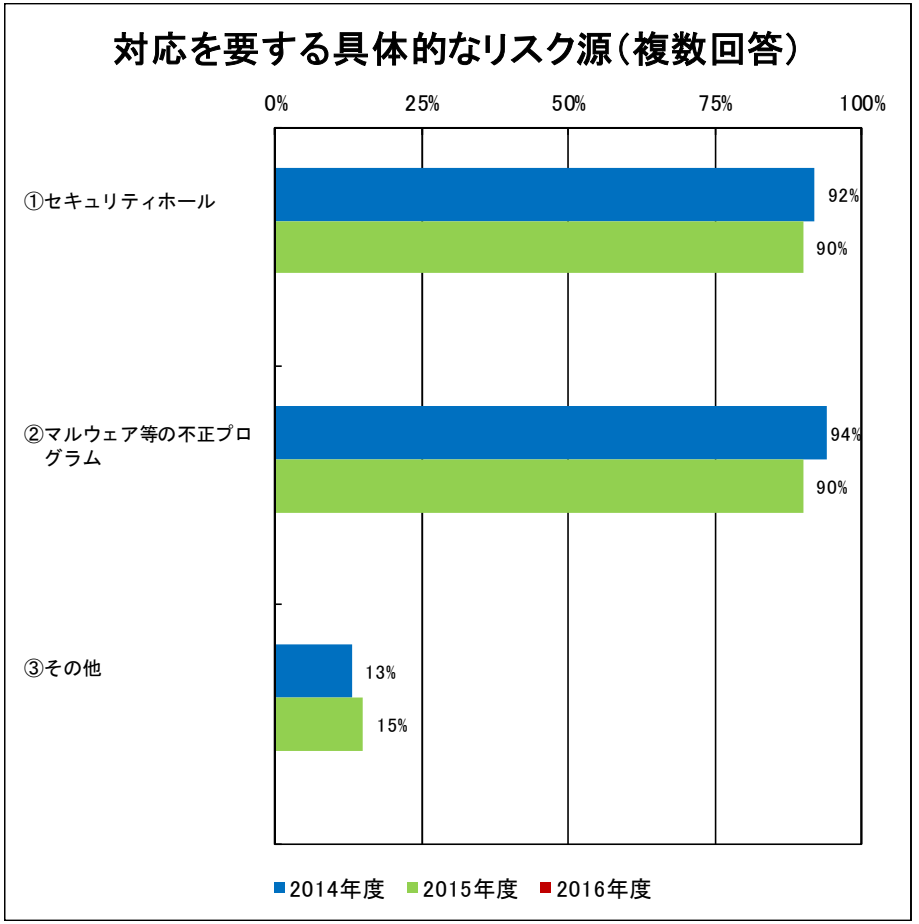
・情報セキュリティ確保に必要な機能要件として、認証機能、アクセス制限機能、権限管理機能のいずれもが９割強で挙げられている。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(d) 対応を要する具体的なリスク源

・対応を要する具体的なリスク源としては、セキュリティホール、マルウェア等の不正プログラムがいずれも９割程度で挙げられている。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

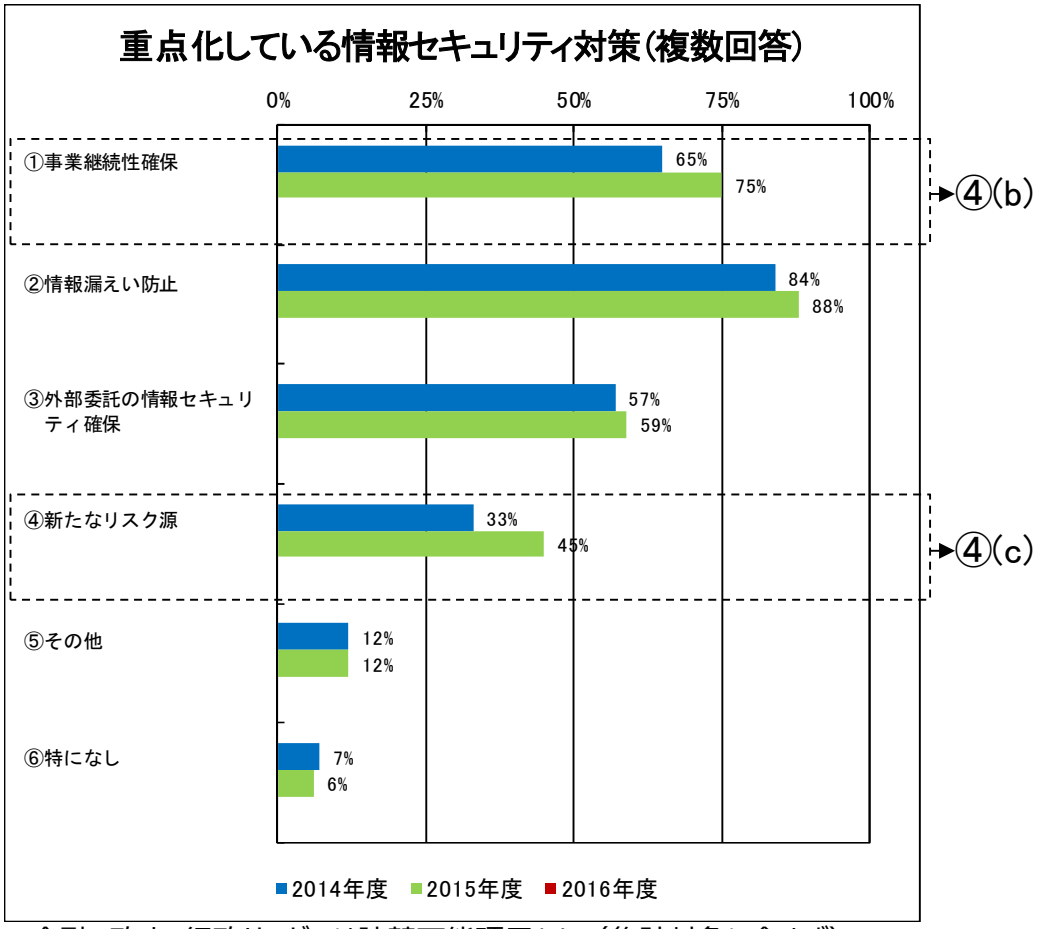
6．調査結果詳細　－　各個別設問のグラフ及び分析(12/19)　－

(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

・重点化している情報セキュリティ対策については、情報漏えい防止対策が９割弱と最多。以降、事業継続性確保が75%程度で続く。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

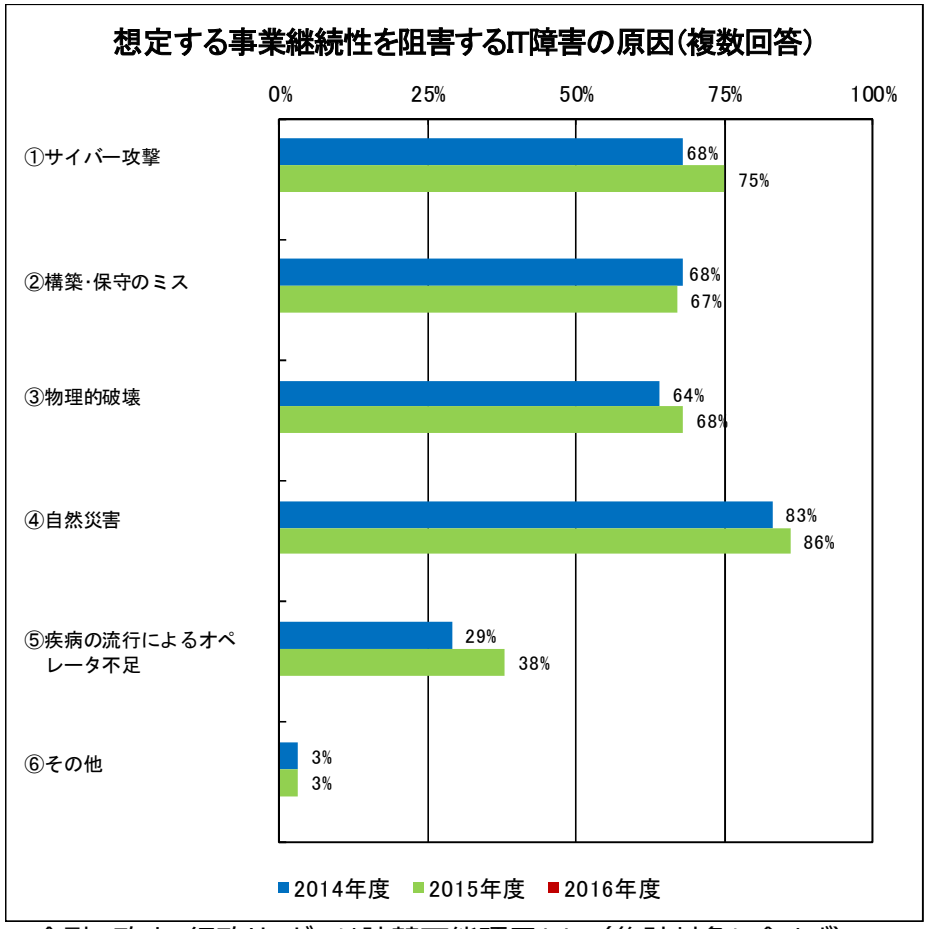
6．調査結果詳細　－　各個別設問のグラフ及び分析(13/19)　－

(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

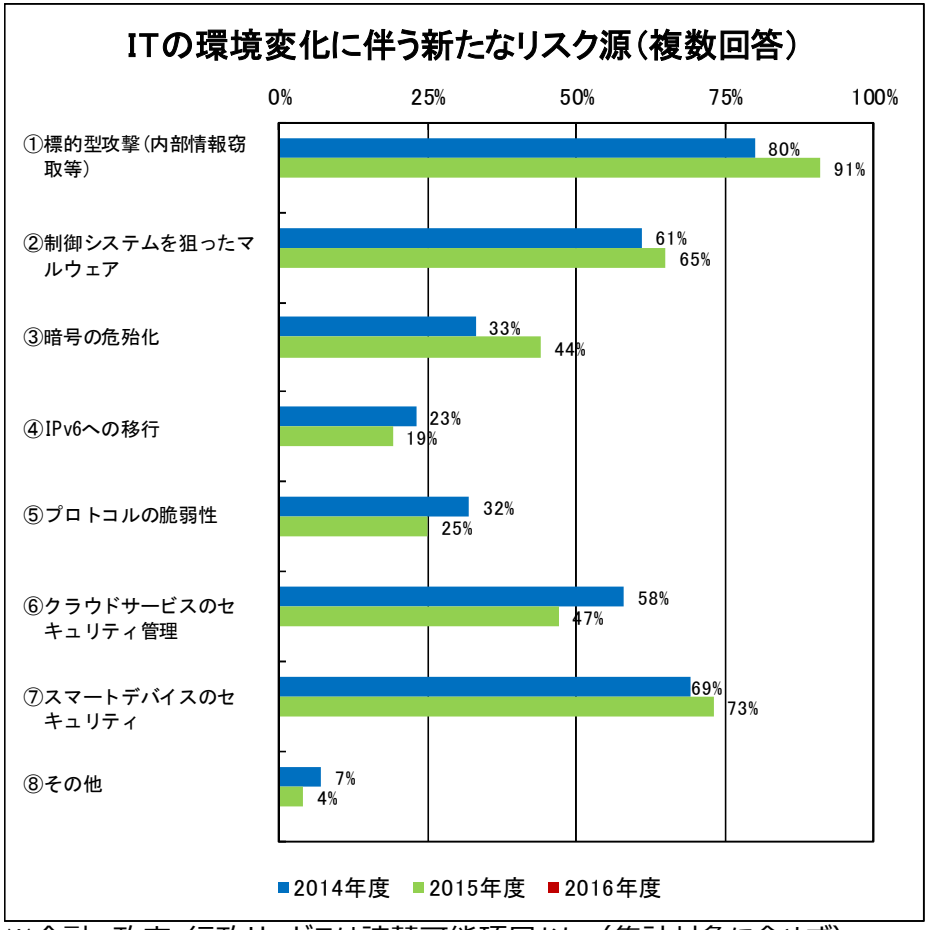
・85%程度の事業者が自然災害を挙げ、以降75%程度の事業者がサイバー攻撃を、7割弱の事業者が物理的破壊、構築・保守のミスを挙げている。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(c) ITの環境変化に伴う新たなリスク源

・９割強の事業者が標的型攻撃を挙げ、以降７割強の事業者がスマートデバイスのセキュリティ、65%程度の事業者が制御システムを狙ったマルウェアを挙げている。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

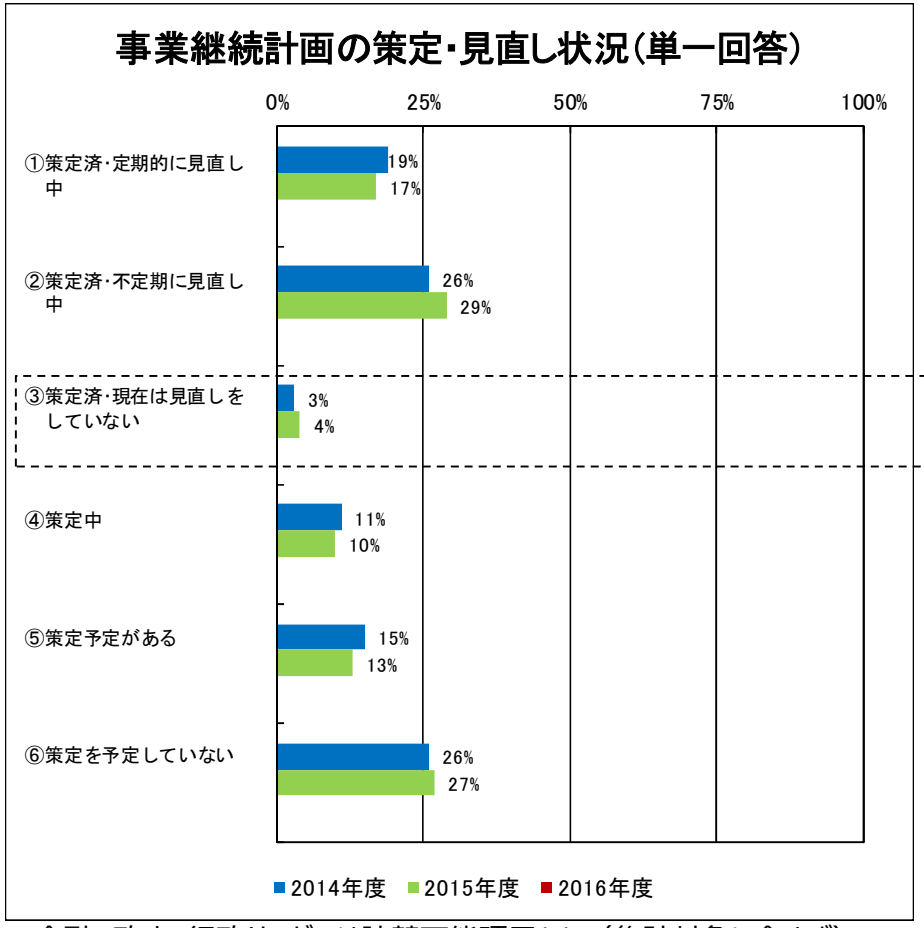
6．調査結果詳細　－　各個別設問のグラフ及び分析(14/19)　－

(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

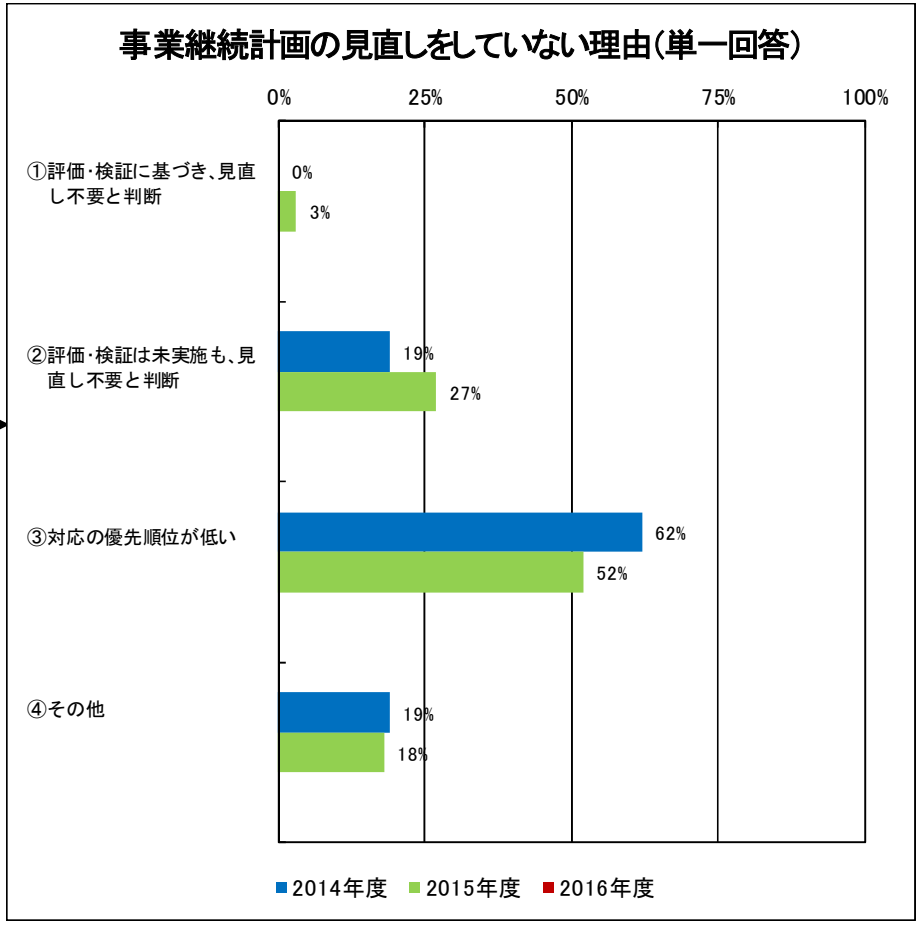
・45%程度の事業者が、事業継続計画を策定し、見直しを行っている。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(b) 事業継続計画の見直しをしていない理由

・事業継続計画を策定したものの現在は見直しを行っていない理由としては、対応の優先順位が低いとの回答が約半数で最多。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

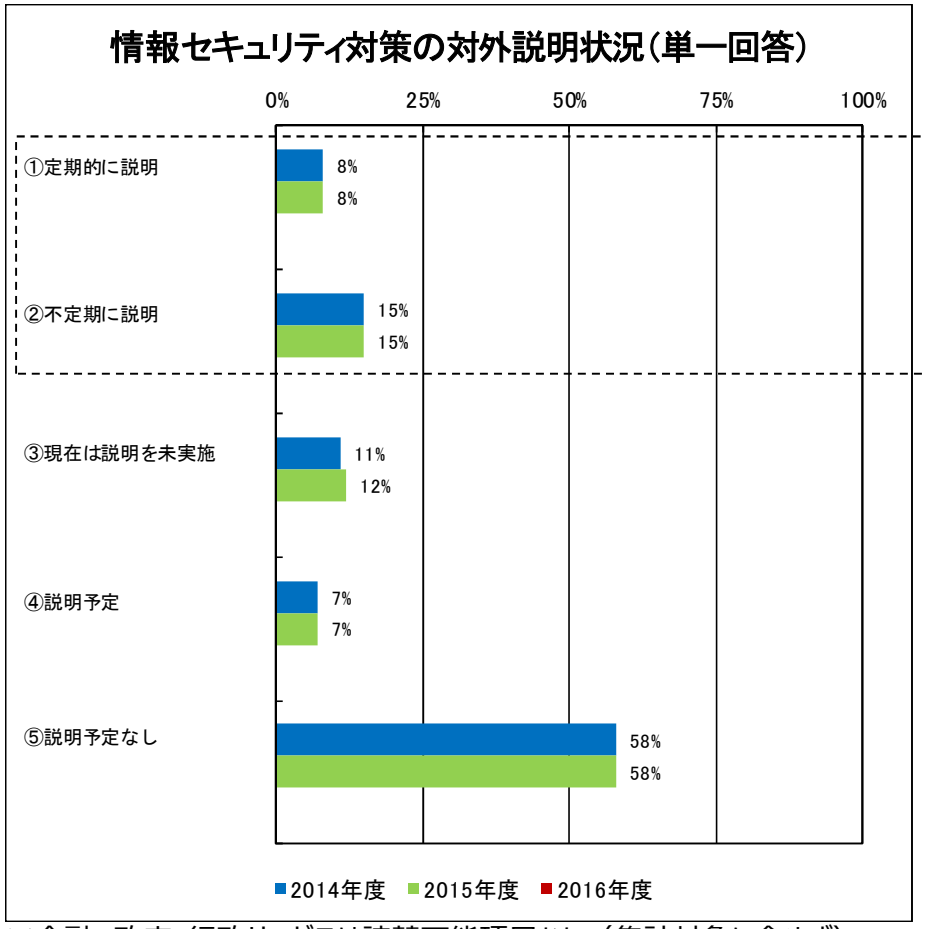
6．調査結果詳細　－　各個別設問のグラフ及び分析(15/19)　－

(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

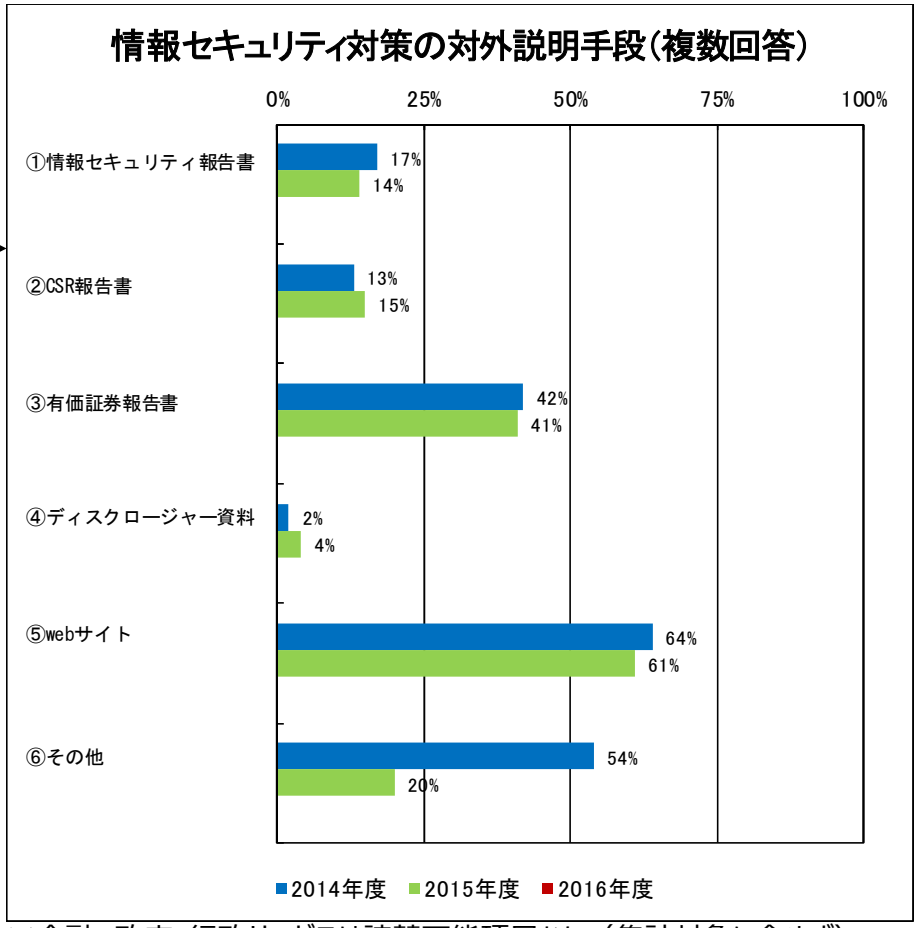
・情報セキュリティ対策の対外説明を行っている事業者は２割強。
・説明予定のない事業者が６割弱。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(b) 情報セキュリティ対策の対外説明手段

・対外説明手段としては、webサイトが６割強。これに有価証券報告書が４割強で続く。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

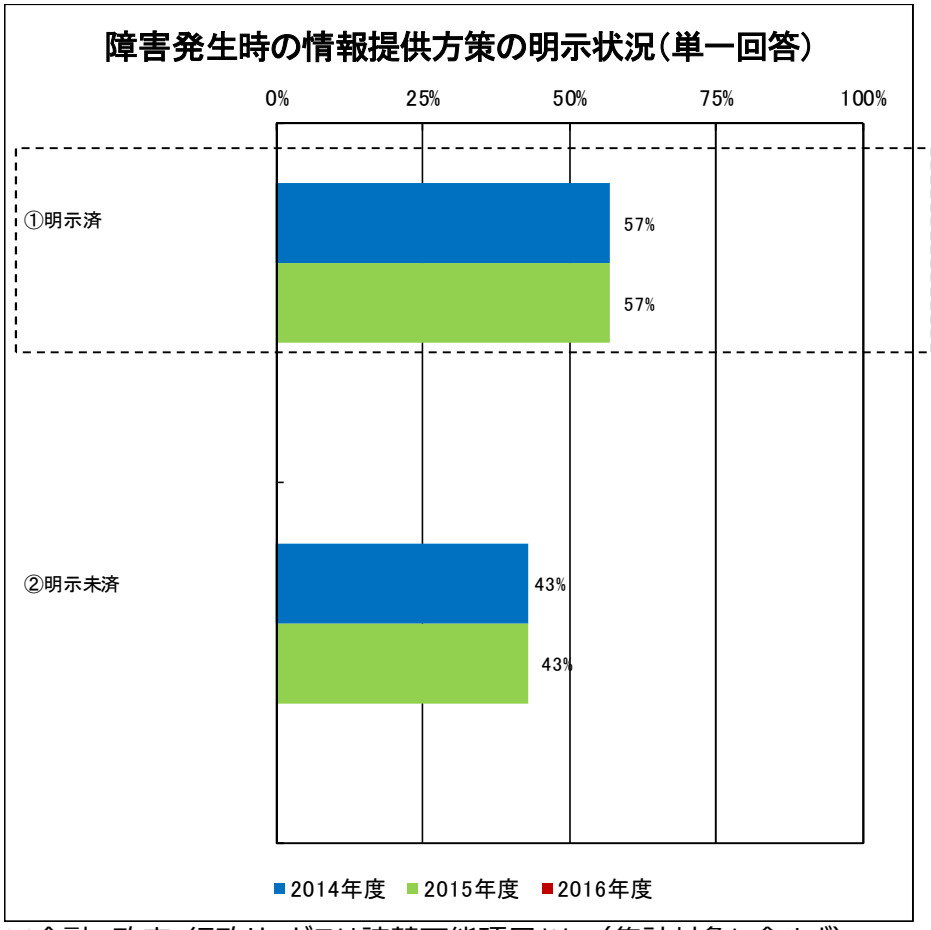
6．調査結果詳細　－　各個別設問のグラフ及び分析(16/19)　－

(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

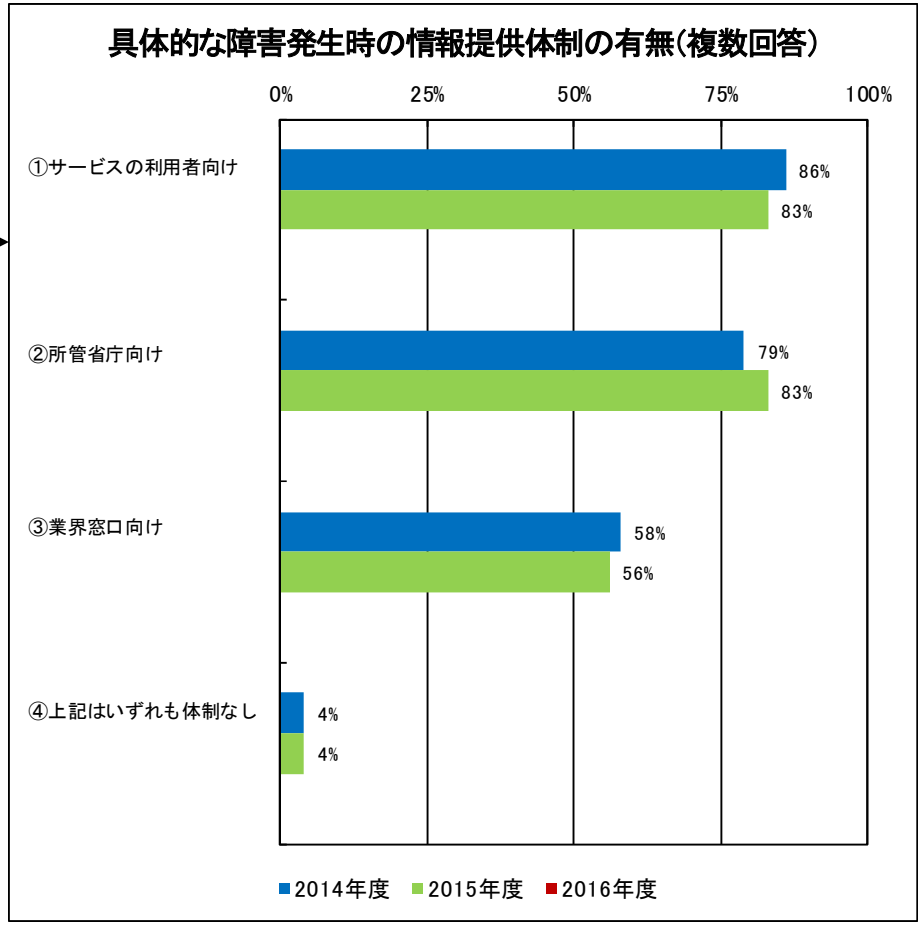
・6割弱の事業者が、障害発生時の情報提供方策を明示済。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(b) 具体的な障害発生時の情報提供体制の有無

・情報提供体制として、サービスの利用者向けと所管省庁向けが共に8割強、業界窓口向けが55%程度。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

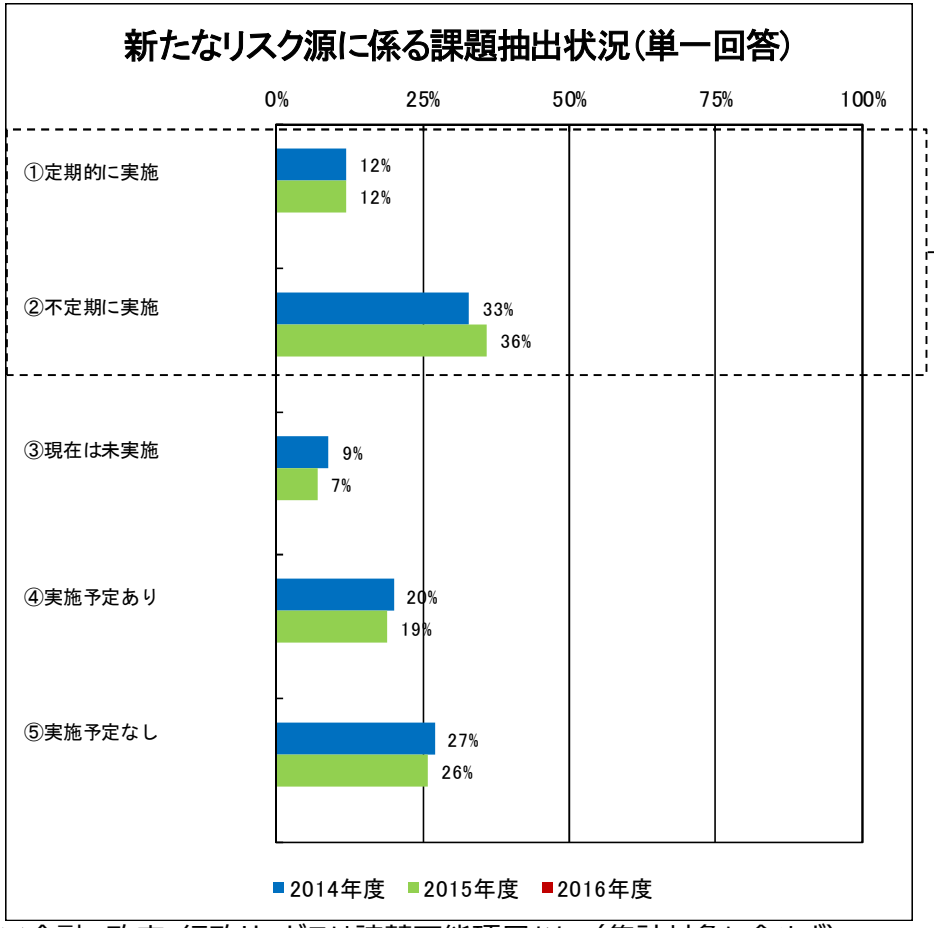
6．調査結果詳細　－　各個別設問のグラフ及び分析(17/19)　－

(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

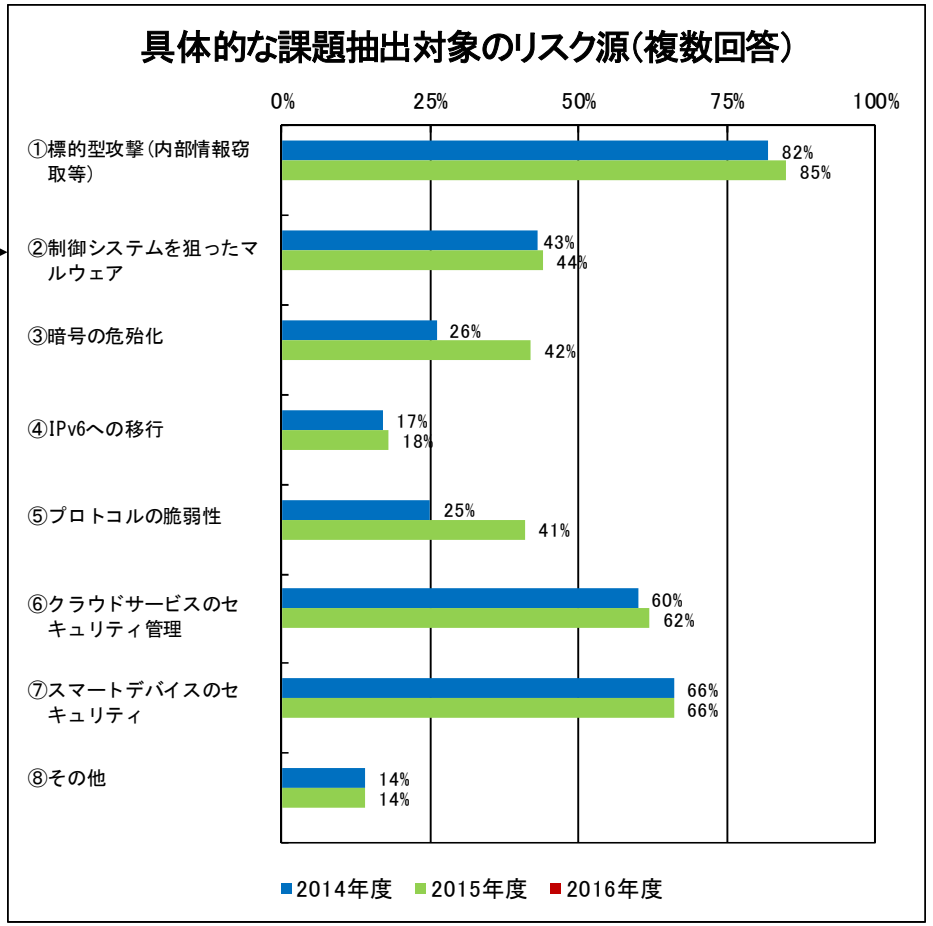
・新たなリスク源に係る課題抽出を行っている事業者は５割弱。
・実施予定なしの事業者は25%程度。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

(b) 具体的な課題抽出対象のリスク源

・課題抽出対象とするリスク源は、標的型攻撃が85%程度。これにスマートデバイスのセキュリティ、クラウドサービスのセキュリティ管理が続く。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

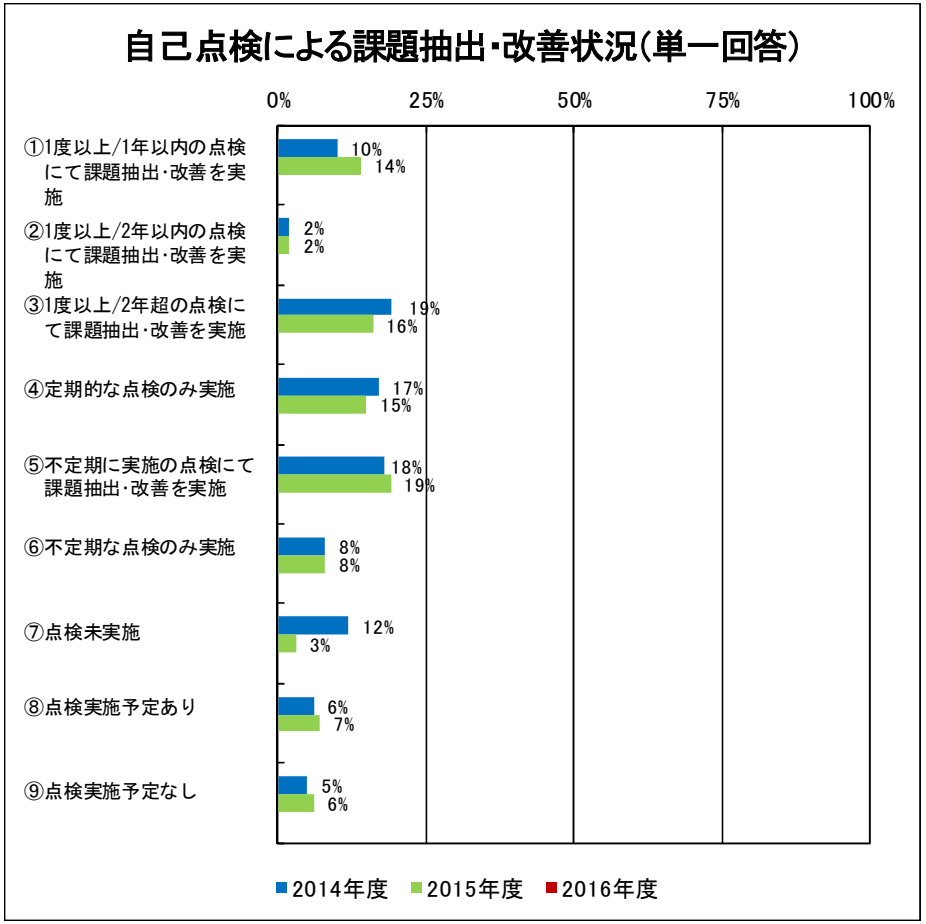
6．調査結果詳細　－　各個別設問のグラフ及び分析(18/19)　－

(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

・定期的な点検の実施状況は５割弱。定期的な点検に基づく課題抽出・改善の実施状況は３割強。

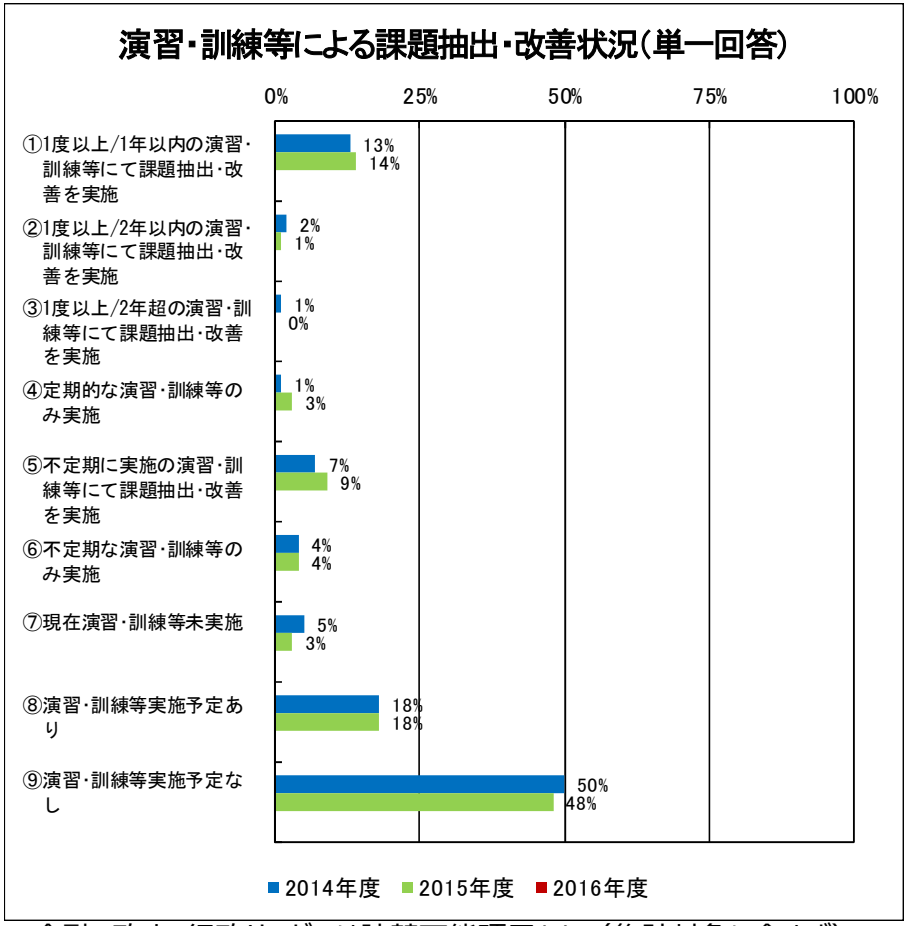


※金融は読替可能項目なし（集計対象に含めず）

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

・定期的な演習・訓練等の実施状況は２割弱。定期的な実施に基づく課題抽出・改善の実施状況は15%程度。



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

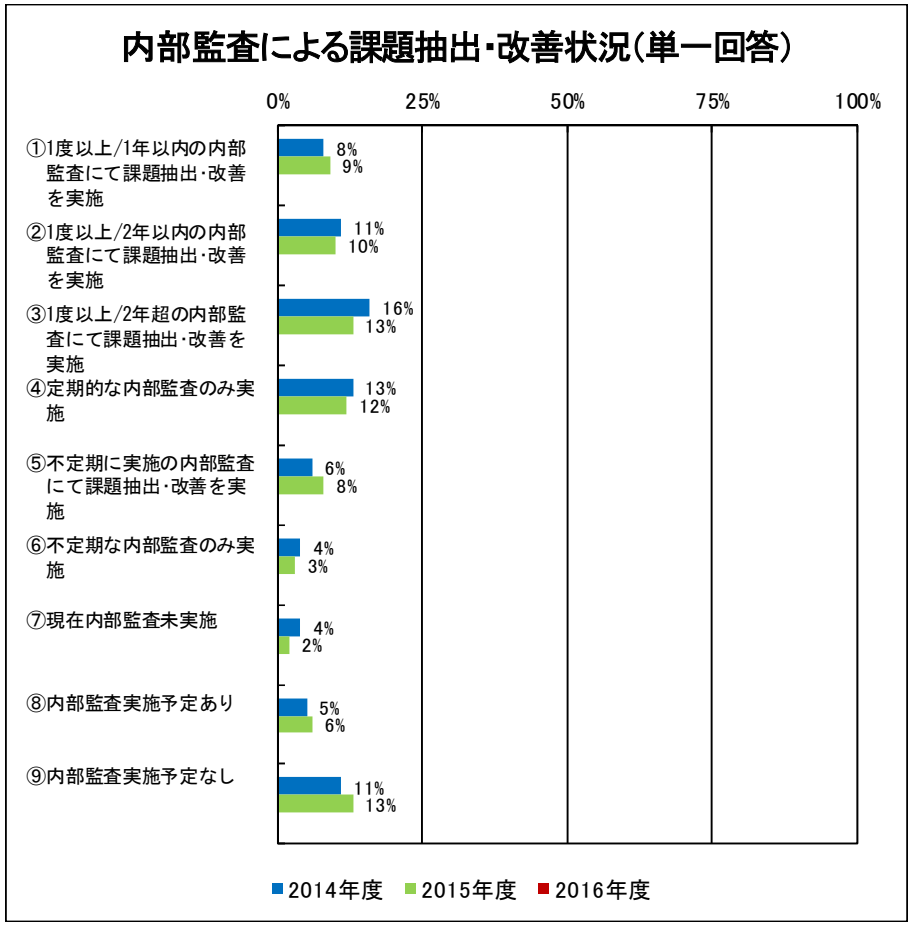
6．調査結果詳細　－　各個別設問のグラフ及び分析(19/19)　－

(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

・定期的な内部監査の実施状況は45%程度。定期的な内部監査に基づく課題抽出・改善の実施状況は３割強。

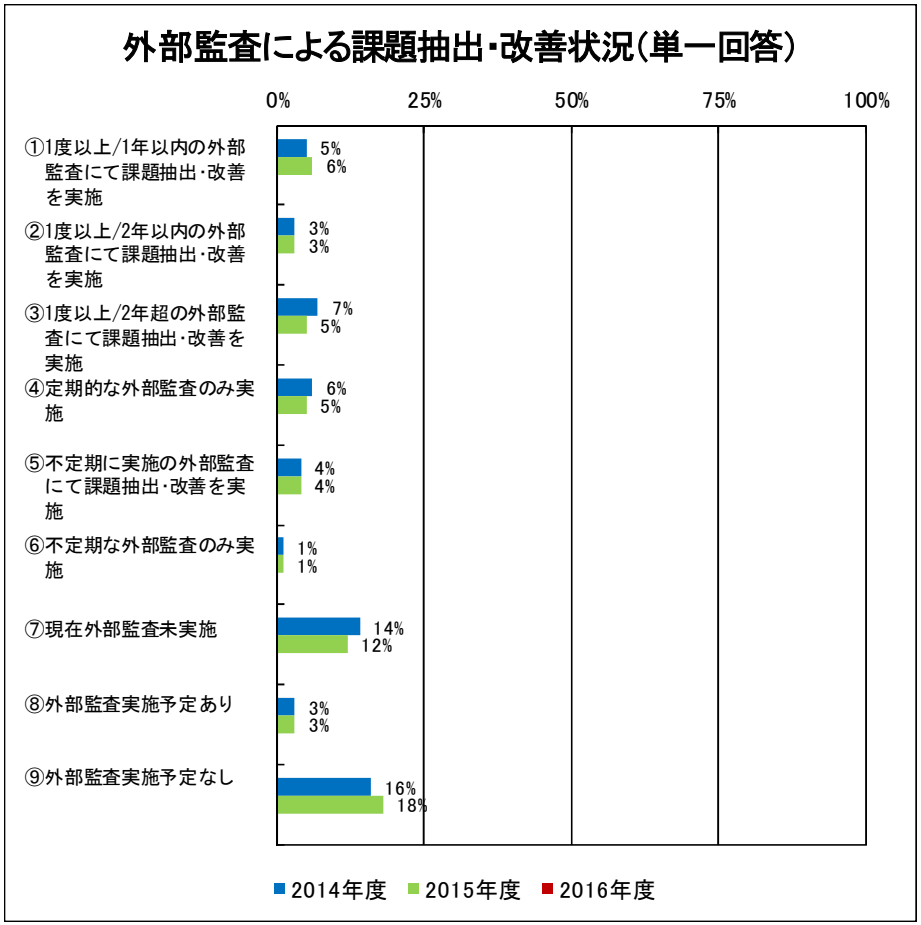


※金融は読替可能項目なし（集計対象に含めず）

④ 外部監査の実施

(a) 外部監査による課題抽出・改善状況

・定期的な外部監査の実施状況は２割弱。定期的な外部監査に基づく課題抽出・改善の実施状況は15%程度。



※金融は読替可能項目なし（集計対象に含めず）

6．調査結果詳細　－　自由意見　－

【国・政府に対する意見・要望等】

- 過去の事例をもとに必要性と効果について分かり易く説明することが必要と感じる
- 情報セキュリティ対策の向上に対しては、国の助成をお願いしたい。
- 情報セキュリティの相談窓口の設置をお願いしたい。
- セキュリティ対策の裏口をつくようなコンピュータウイルスが目立ってきたように思います。現在、コンピュータウイルスの対策はソフトウエア業界任せであり、真の脅威に積極的に取り組んでいるとは言い難いとの思いがいたします。真の脅威を未然に防ぐためにも国の研究機関なりが、重要なコンピュータウイルス対策を行うべきではないでしょうか。
- 政府が行っている情報セキュリティ対策の推進については理解しておりますが、一般企業（重要インフラであっても）でこれに追随できる対策を行えている所は少ないのではないかと思います。それぞれの企業の水準に合わせた、水準別対策などがあると、目標とし易いのではないかと思います。
- 情報セキュリティの分野は利益を生まないので、優先順位が低くなりがちです。いろんな意味での「負担」をできる限り少なく対応できるようサポートしてもらえることを望みます。
- 他の企業（団体）が講じている具体的なセキュリティ対策の情報を収集するための意見交換会を開催していただきたい。システム開発やセキュリティ対策などについては開発ベンダーとの協議でほぼ確定しますが、常にセキュリティ対策のレベル（金額面も含めて。）が課題となっています。既存システムも含めて様々な情報を収集できれば大変参考になります。
- 情報セキュリティ対策の重要性について広く認識されているかについて疑問がある。担当セクションが無い社もある。
- IT人材育成のための支援を重視して頂きたい。

【情報共有体制の推進に関する意見・要望等】

- 大規模なサイバー攻撃、セキュリティインシデント発生時の迅速な情報提供をお願いしたい。
- 緊急性が高いセキュリティ事故が発生した場合、即座に対策が出来るように早急な連絡（メール等）をお願いしたい。

※分野個別の意見は別途所管省庁へ提示

6．調査結果詳細　－　自由意見　－

【指針に関する意見】

- 所管省庁や業界団体による周知、広報活動、内容の説明がある定期的なセミナー開催を希望
- 経営層にも見ていただける様、また、手軽に見れる様、冊子での配布が効果的ではないか
- より普及や周知に向け要点のみが明確に記載された一般用のさらなる簡略版（パンフレット的なもの）を作ってみてはどうか
- 具体的な対策の例示、チェックシートなどがあるとさらに有意義なものになる
- 指針としては理解できるが、それを実現場に落としこむ作業が非常に大変。内容をより具体化する、個別の案件に対してのQ&A窓口を設置するなどの対応を希望
- 安全基準等は参考にしているが、日々変化する環境に対して見直しが追いついていないように感じる。ITが専門ではない事業分野においては、対策を最新に保つのが難しいので、事業分野に共通する留意点を専門的な立場から提示して頂きたい
- 各社にて自社システムの状況を考慮したセキュリティ対策等を講じているため、指針等による画一的なセキュリティ基準等は経済的にも負担が大きく、２重投資になる可能性も高い
- 監督官庁毎に明示される指針が異なる可能性も否定できないため、省庁間での連携をお願いしたい
- 今回のアンケートにて初めて内容を再確認した。今後の改訂においては変更箇所を知らせて欲しい
- 重要インフラ活動の担当者には、直接周知してほしい。今回の指針等は全く知らなかった

【安全基準等に関する意見】

- 事業者規模に分別した安全基準の基本要綱（雛形）を希望する
- 安全基準に則り対策を講じる必要性は非常に感じているが、そこまでなかなか実施できていないのが現状です。最低限取り組むべきものなどの具体例があれば示すことができないでしょうか

※分野個別の意見は別途所管省庁へ提示

7．＜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・改訂を行う際の体制をお知らせ下さい。[(1)③(a)]
(6) 内規改訂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)]

7．＜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）