資料６

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

2014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

２０１５年３月２６日

内閣官房　内閣サイバーセキュリティセンター(NISC)

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。

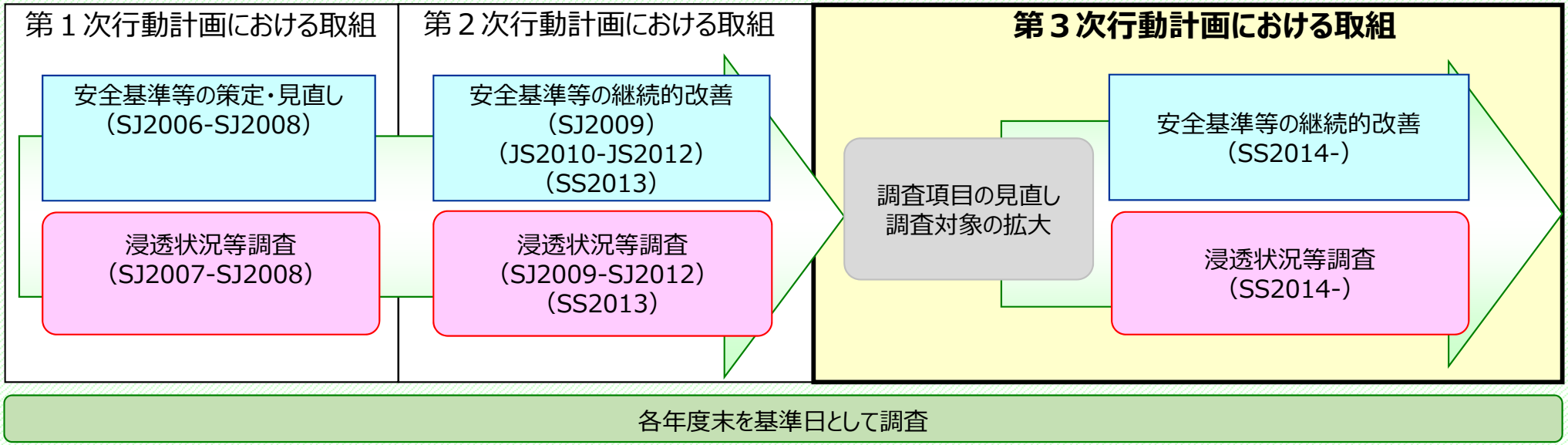
◆重要インフラの情報セキュリティ対策に係る第３次行動計画（2014年５月19日）
・重要インフラ事業者等における安全基準等の浸透状況の把握を目的に、内閣官房は、重要インフラ事業者等の対策状況を調査する。

◆サイバーセキュリティ2014（2014年7月10日）
・重要インフラ所管省庁の協力を得つつ、安全基準等の浸透状況等の調査を実施し、結果を公表する。

【経緯】

○2007年度より開始し、以降継続的に実施。

○第３次行動計画の趣旨に基づき、2014年度調査より調査対象の拡大、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　SS：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	：	2014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	：	2014年　7月～2014年11月
とりまとめ	：	2014年12月～2015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」策定にあたっての指針（第3版）および対策編

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３，３９１事業者等に、その回答は３，２２８事業者等から（回収率：95.2%　前年度比：+1.1%）

重要インフラ分野		活用する独自調査				浸透状況等調査		
		活用	名称	調査基準日	調査周期	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）
情報通信	電気通信	無	－－－	－－－	－	電気通信事業者（一部抽出）	97 (76)	73 (20)
	ケーブルテレビ	無	－－－	－－－	－	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	237 (241)	237 (221)
	放送	無	－－－	－－－	－	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		有	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	3月31日	1年毎	銀行等、証券会社、生命保険会社、損害保険会社	855 (892)	737 (796)
航空	航空運送	無	－－－	－－－	－	航空運送事業者	2 (2)	2 (2)
	航空管制	無	－－－	－－－	－	官庁	2 (1)	2 (1)
鉄道		無	－－－	－－－	－	ＪＲ、大手民鉄	22 (22)	22 (22)
電力		無	－－－	－－－	－	一般電気事業者、日本原電(株)、電源開発(株)	12 (12)	12 (12)
ガス		無	－－－	－－－	－	大手ガス事業者	12 (10)	12 (10)
政府･行政サービス		有	地方自治情報管理概要 －電子自治体の推進状況－	4月1日	1年毎	地方公共団体	1,789 (1,789)	1,789 (1,789)
医療		無	－－－	－－－	－	病院情報システムを導入する病院	60 (50)	53 (38)
水道		無	－－－	－－－	－	給水人口30万人以上の水道事業者、水道用水供給事業者	88 (45)	88 (45)
物流		無	－－－	－－－	－	物流事業者、業界団体（一部抽出）	21 (22)	7 (10)
全分野合計		－	－－－	－－－	－	－－－	**３，３９１ (3,356)**	**３，２２８ (3,160)**

4．調査結果の総括（1/2）

（1） 総括に当たっての前提

今回の調査実施期間（2014年７月～11月）は、第３次行動計画策定（2014.5.19）の直後であり、また適用する指針は第２次行動計画に基づく第３版である。

このことから今回の調査結果は、第３次行動計画策定時に認識した課題の妥当性に関する検証と位置付けられるとともに、今後の改善状況を測るための基準となるものである。

（2） 調査結果の概要

①PDCAサイクルに沿った継続的な対策

- ✓ 「初期対応」（PDCAのうちP（規定、体制、構築）の一部が該当）は概ね実施されている（ほぼ８割超）。
- ✓ 「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））の実施率はほぼ３割以下に留まる。

②経営層の在り方

- ✓ 「重点化対策の合意」は約８割で経営層が関与している一方、「運用状況の把握」では約５割に留まる。
- ✓ 経営資源の継続的な確保に関連して、「人員不足による対策の遅れ」（往訪調査でも同様の意見あり。）、「IT人材育成のための支援」や「対策費用補助の制度化」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

- ✓ 「企業体力に応じた評価指標や水準別の対策の提示」、「対策費用が利益、資産へ与える影響に関する指標の提示」等を国の支援として求める意見があった。

④情報共有体制

- ✓ 「重要インフラ事業者間でのリスク情報の共有」（往訪調査でも同様の意見あり。）、「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・啓発に役立つ資料の作成やセミナーの開催を求める意見があった。

4．調査結果の総括 (2/2)

(3) 課題

◆ 第３次行動計画の策定に際して第２次行動計画における改善点として抽出した項目が、今回の調査結果においても今後改善すべき課題であることを改めて確認することができた。具体的には以下のとおり。

①PDCAサイクルに沿った継続的な対策の改善

✓ PDCAサイクルに沿った継続的な対策の改善に関しては、「初期対応」の実施状況には向上の余地があり、「継続的改善」については実施の定着が課題と認められる。

②経営層の関与の強化

✓ 経営層においては、対策の必要性への認知はあるものの、予算・体制・人材等の経営資源の継続的な確保や運用状況の理解・把握には認知度の向上が課題と認められる。
また、予算・人材等において国の支援を求める声があるが、自らの責任における実施は第３次行動計画が期待するところであり、自助・共助・公助の精神も踏まえつつ、国がどの程度まで支援を行うべきかについては今後の課題として慎重な検討が必要と考えられる。

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

✓ 事業者等による自らの責任における実施状況に関しては、新設する指針_手引書が例示する優先順位付けに基づき、情報セキュリティ対策がどの程度進展するかについて今後の調査が必要と考えられる。

④情報共有体制の推進

✓ 情報共有体制の推進に関しては、適切に運営できているかについて調査の必要性が認められる。

⑤広報公聴活動の強化

✓ 防護基盤の強化（広報公聴活動）に関しては、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。

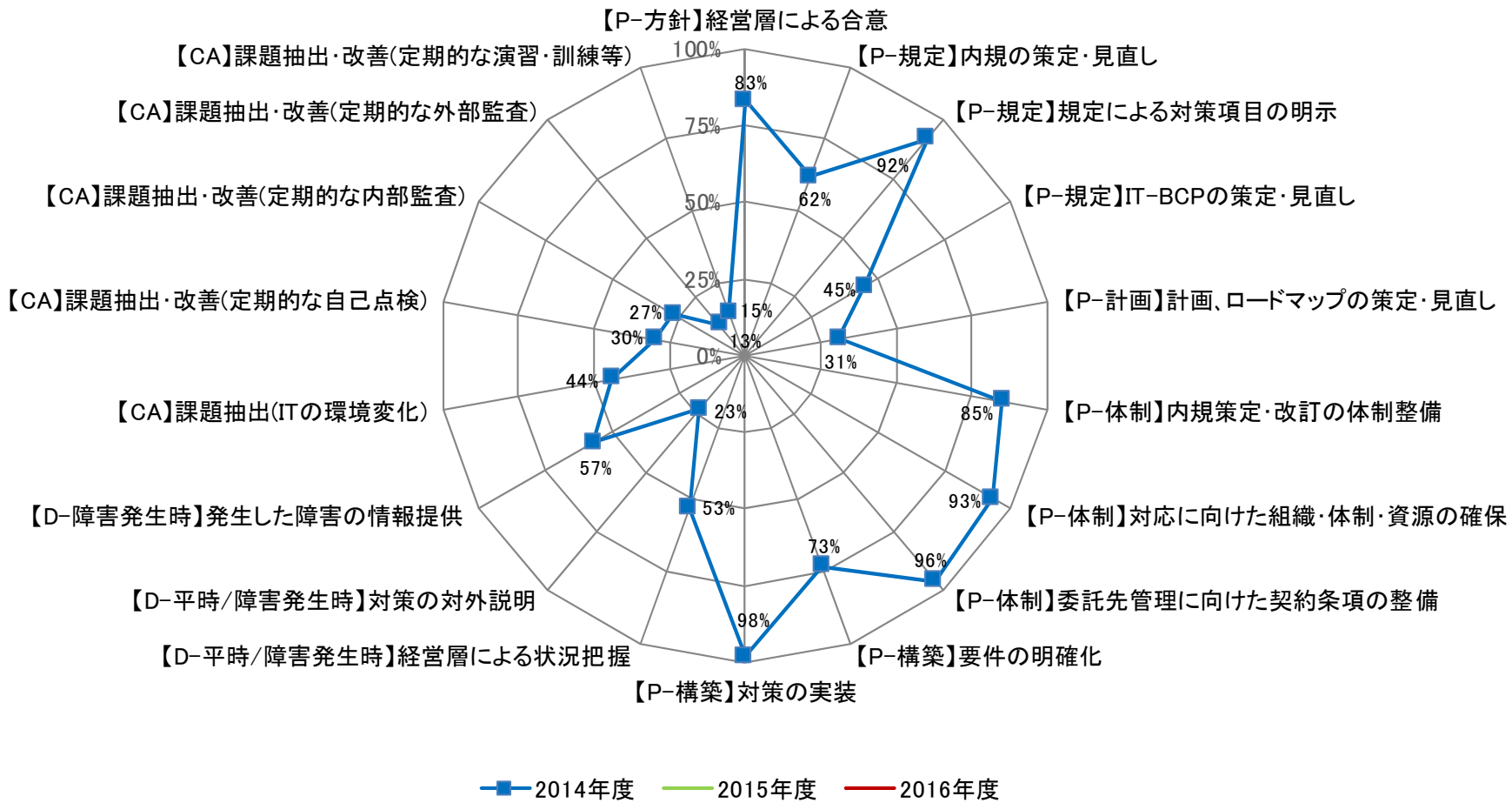
(4) 今後の対応

✓ 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、「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、「経営層の在り方」の浸透を中心に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。

✓ 具体的には、本調査及びこれを補う往訪調査、分野横断的演習、NISCが活動を支援するセプターカウンシル等、重要インフラ事業者等との意見交換の場等を通じて、行動計画や指針の目的や考え方、各施策の成果を説明し浸透を図るとともに、国の支援に対する各事業者等からの要望等を把握する取組を、より充実させることとしたい。

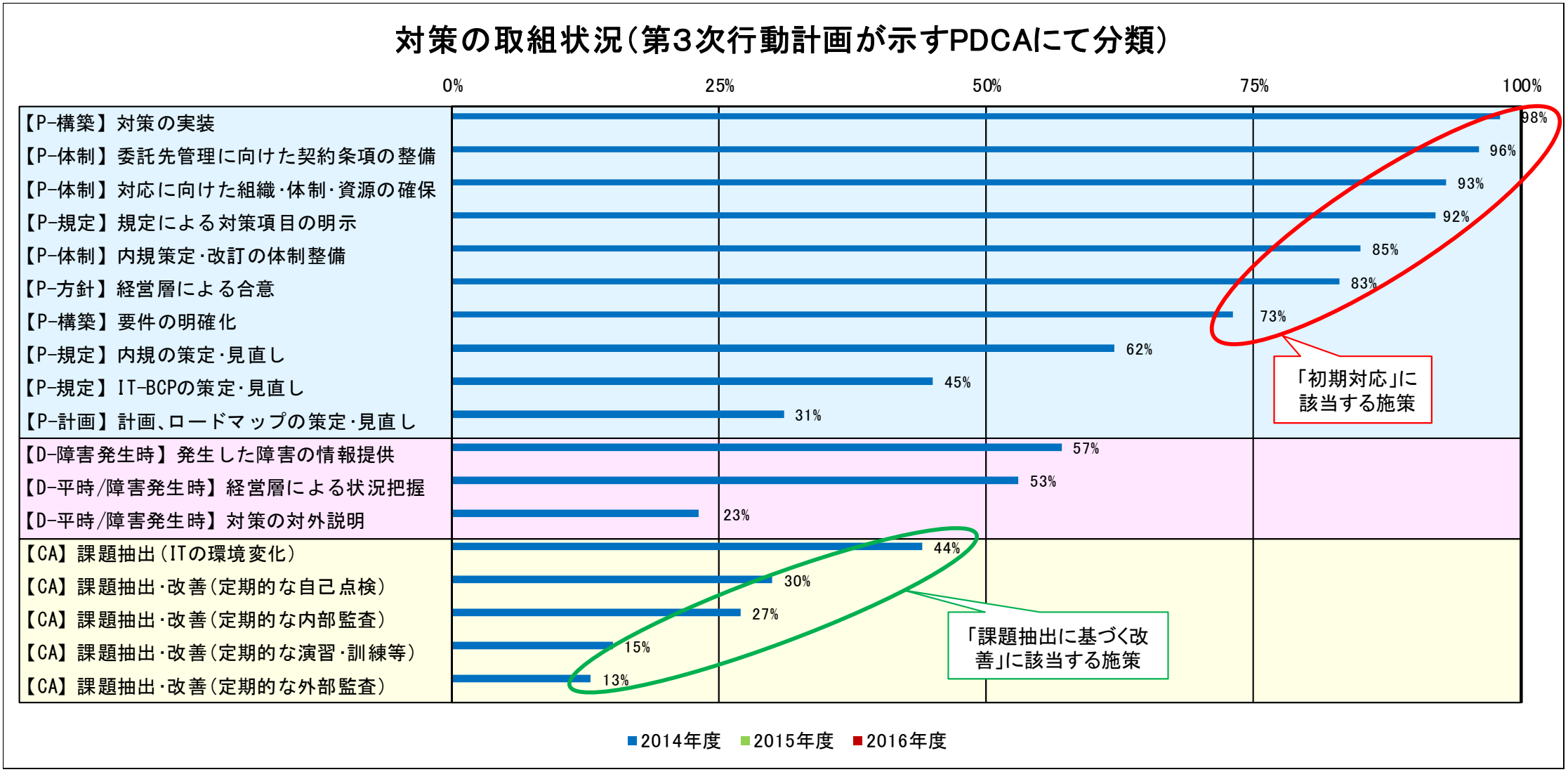
5．調査結果　－　主要な基礎データ(1/5)　－

(1)　PDCAに沿った情報セキュリティ対策の取組（その１：対策毎の実施状況）



5．調査結果 － 主要な基礎データ(2/5) －

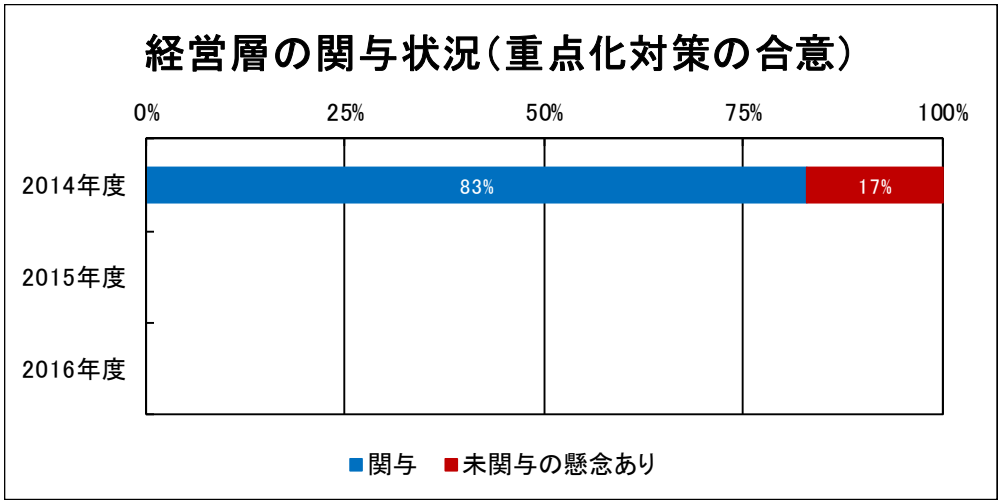
(1) PDCAに沿った情報セキュリティ対策の取組（その２：PDCA別の取組状況（実施率順に再配置））



5．調査結果　－　主要な基礎データ(3/5)　－

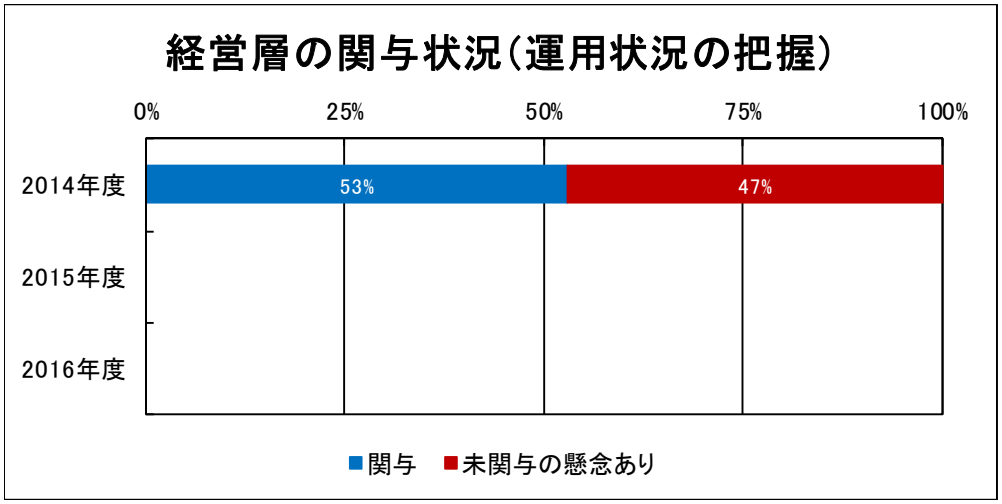
(2) 経営層の関与状況

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え可能項目なし（集計対象に含めず）

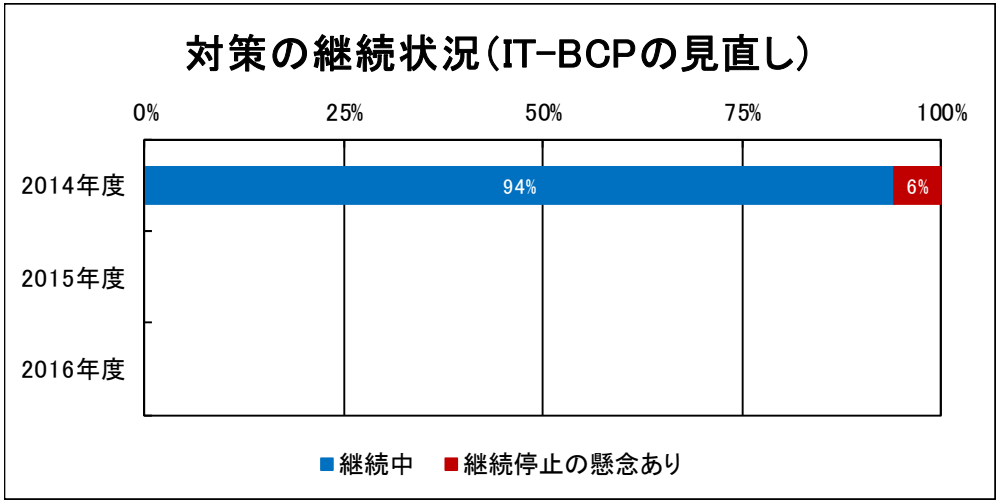
②経営層による運用状況の把握状況（D-平時／障害発生時）



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

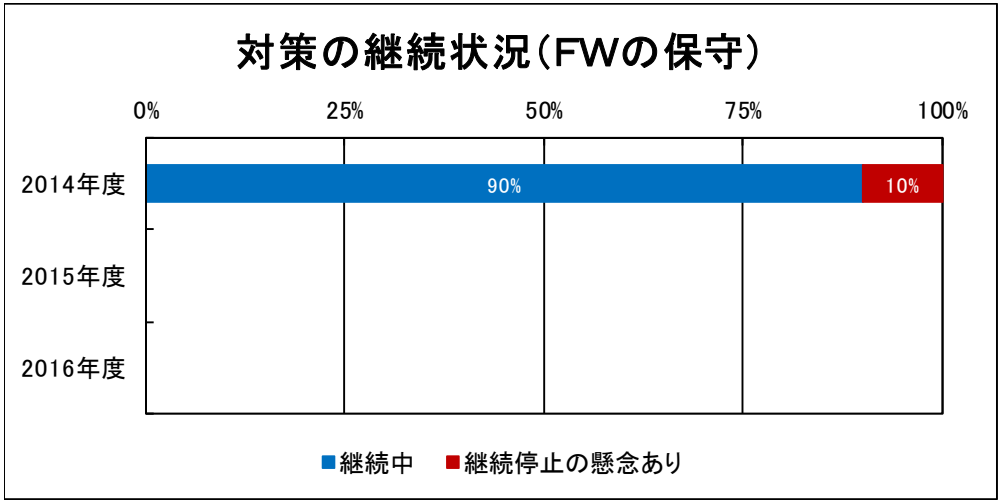
(3) 対策の継続状況

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え可能項目なし（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）

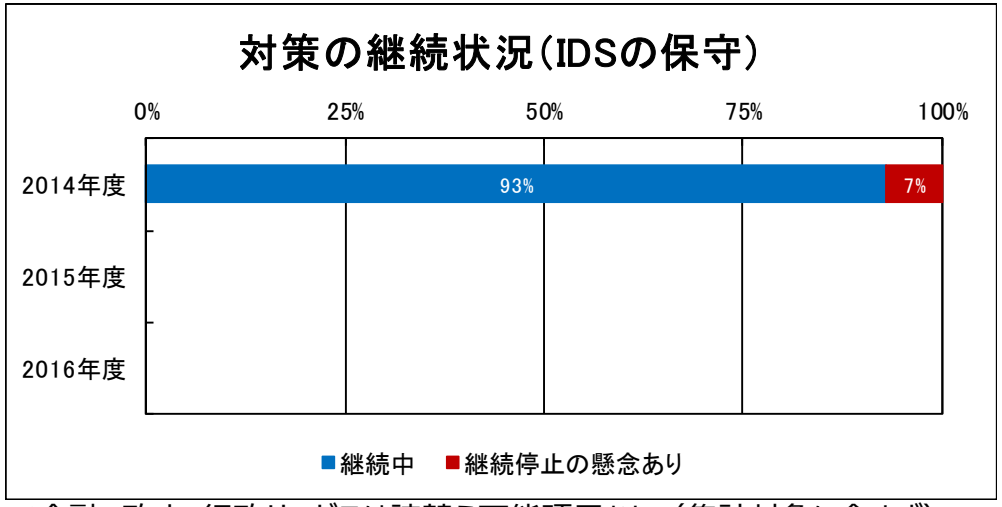


※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

5．調査結果 － 主要な基礎データ(4/5) －

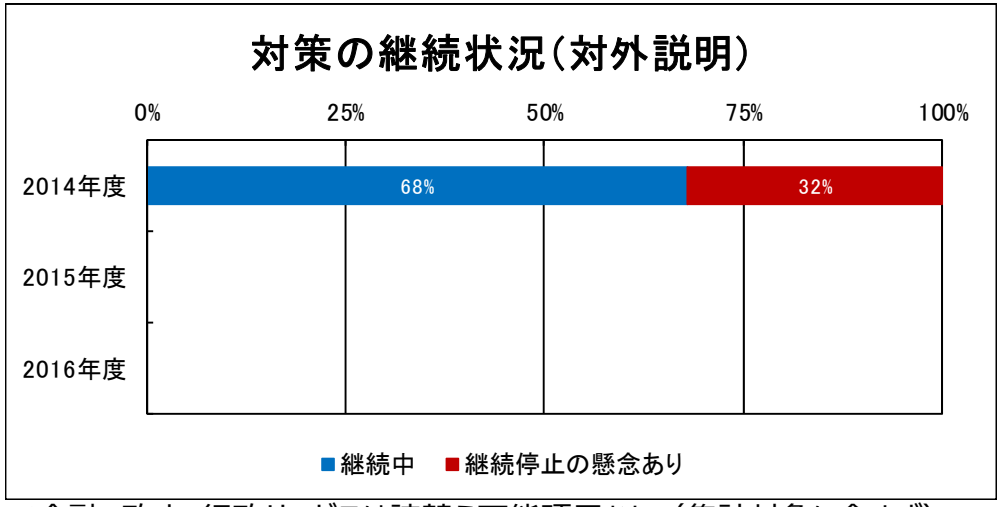
(3) 対策の継続状況（続き）

③侵入検知システムの保守継続状況（P-構築）



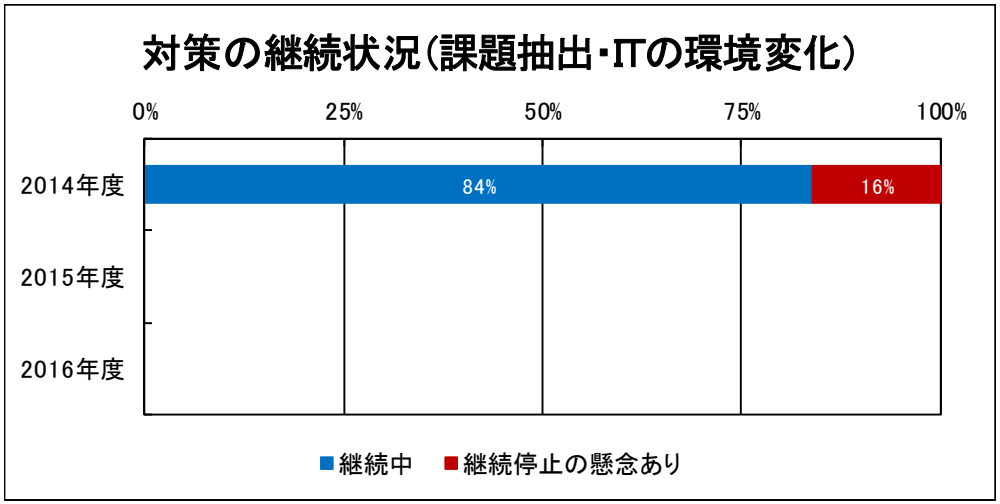
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

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）



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑤新たなリスク源に係る課題抽出の継続状況（CA）

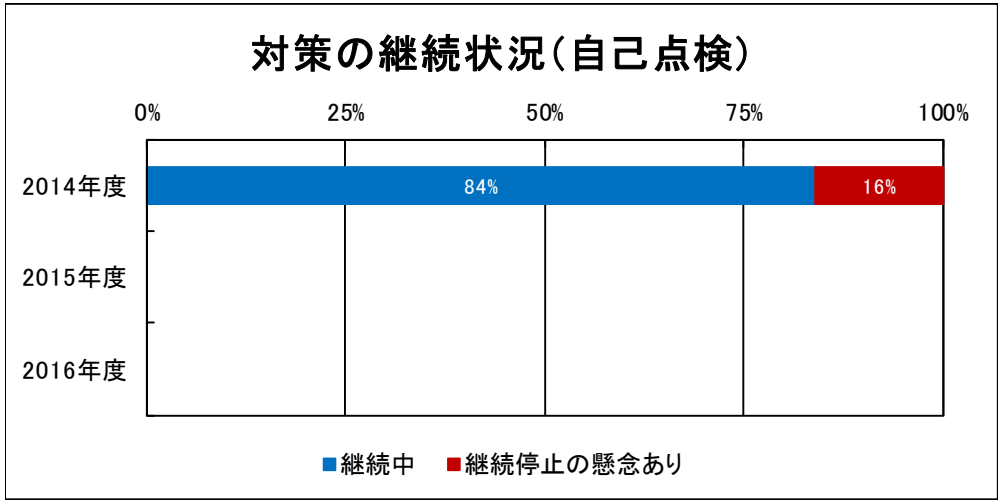


※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

5．調査結果 － 主要な基礎データ(5/5) －

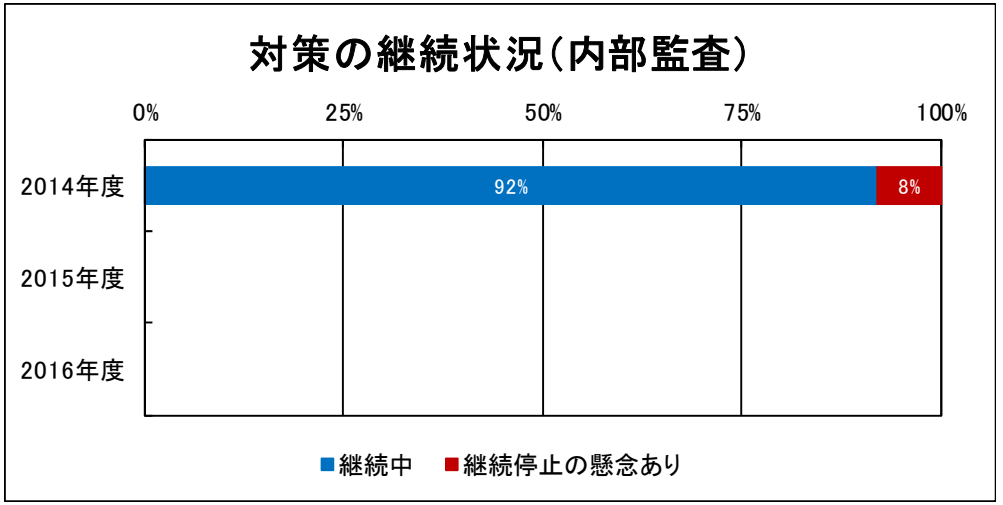
(3) 対策の継続状況（続き）

⑥自己点検による課題抽出・改善の継続状況（CA）



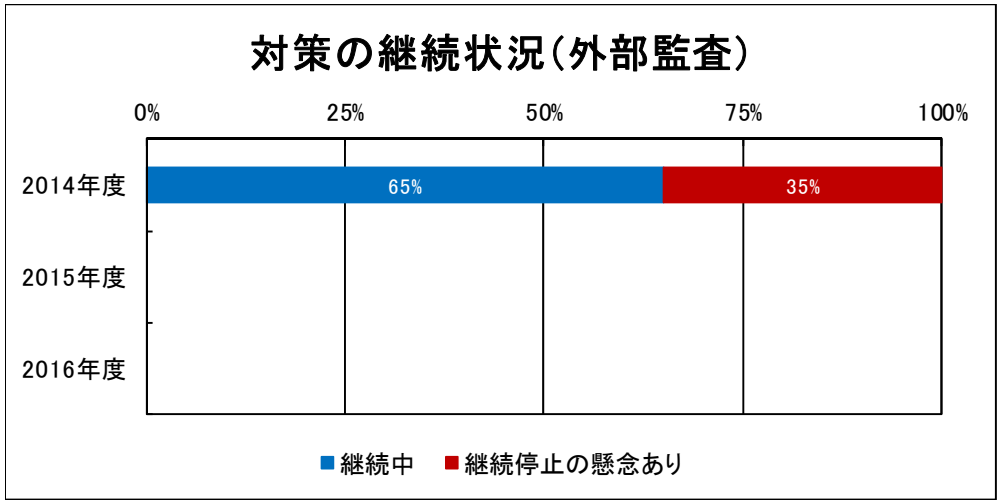
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑦内部監査による課題抽出・改善の継続状況（CA）



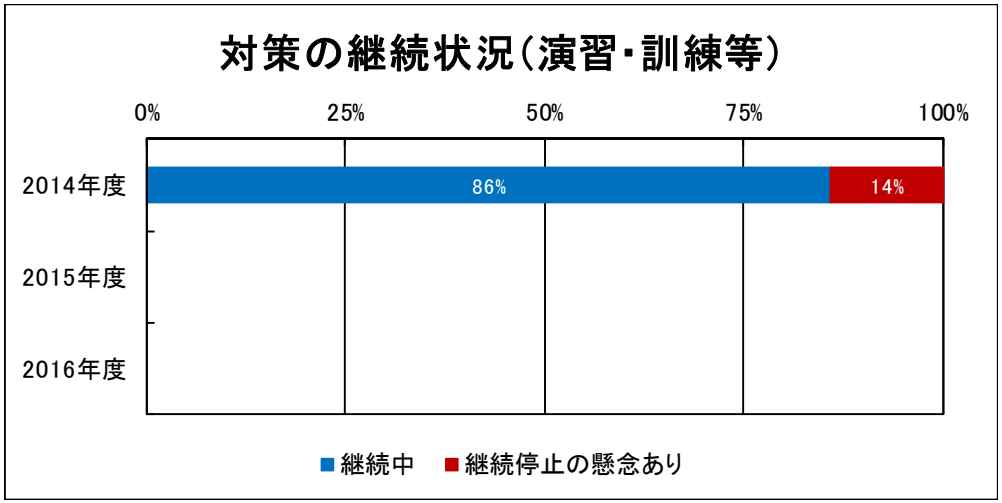
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑧外部監査による課題抽出・改善の継続状況（CA）



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑨演習・訓練等による課題抽出・改善の継続状況（CA）



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

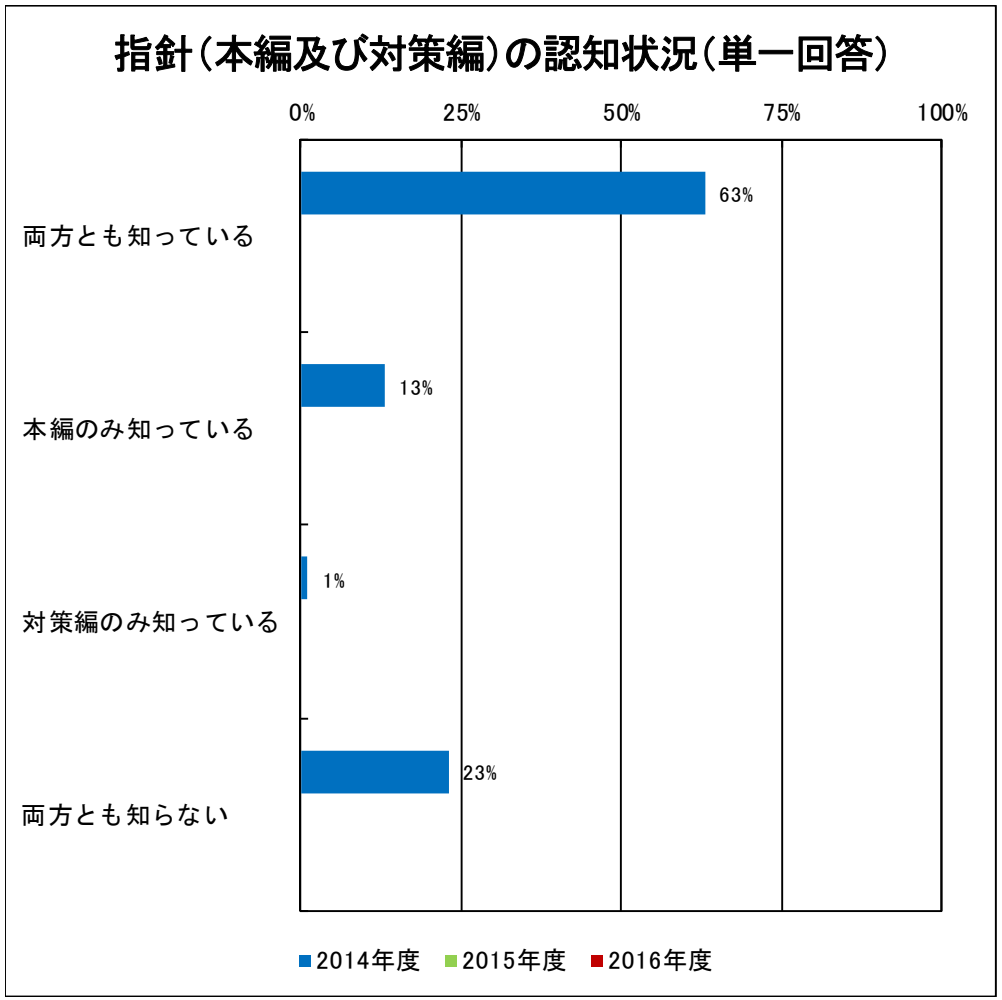
6．調査結果詳細　－　各個別設問のグラフ及び分析(1/19)　－

(1) 安全基準等の整備状況

① 指針の認知

(a) 指針（本編及び対策編）の認知状況

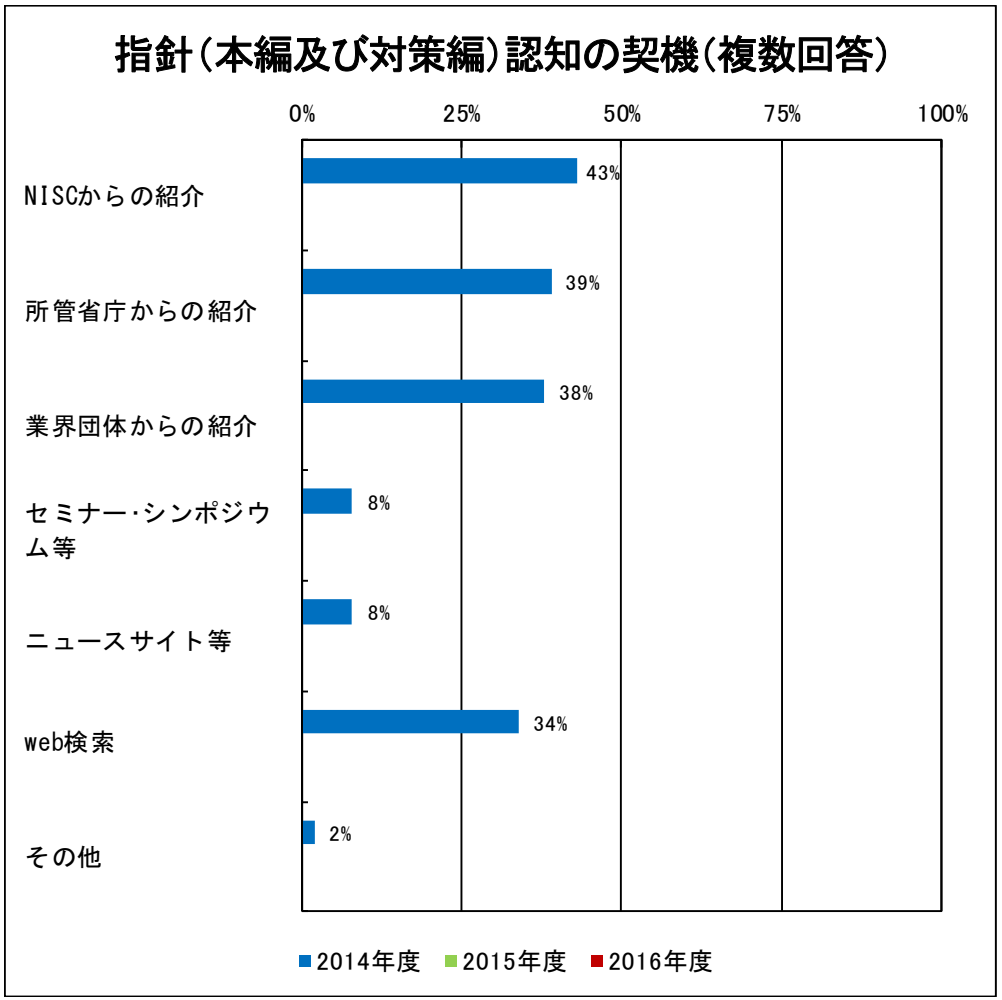
・指針の本編及び対策編の双方を認知している事業者は6割強。
2割強は双方とも認知していない状況。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

(b) 指針（本編及び対策編）認知の契機

・指針を認知した契機は、NISC、所管省庁、業界団体が同程度。
この他、web検索が契機との回答も多い。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

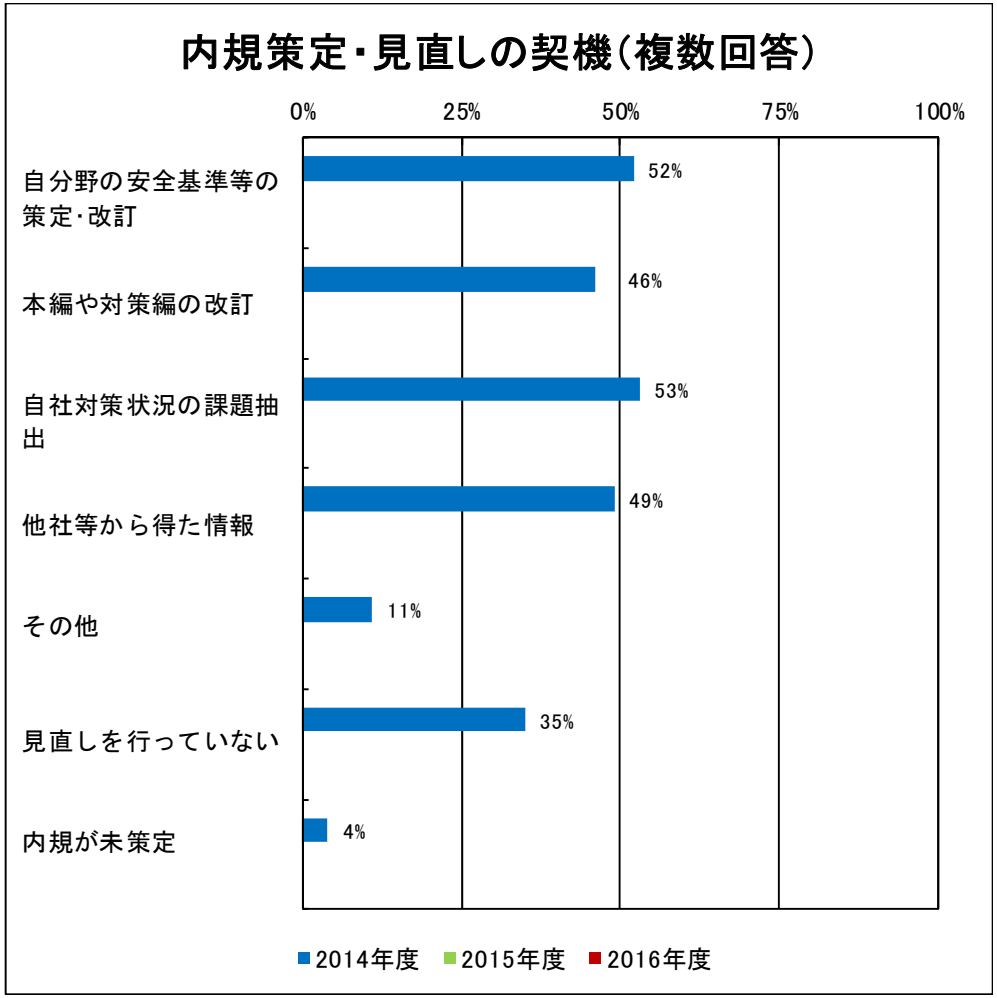
6．調査結果詳細　－　各個別設問のグラフ及び分析(2/19)　－

(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

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



※金融は読替え可能項目なし（集計対象に含めず）

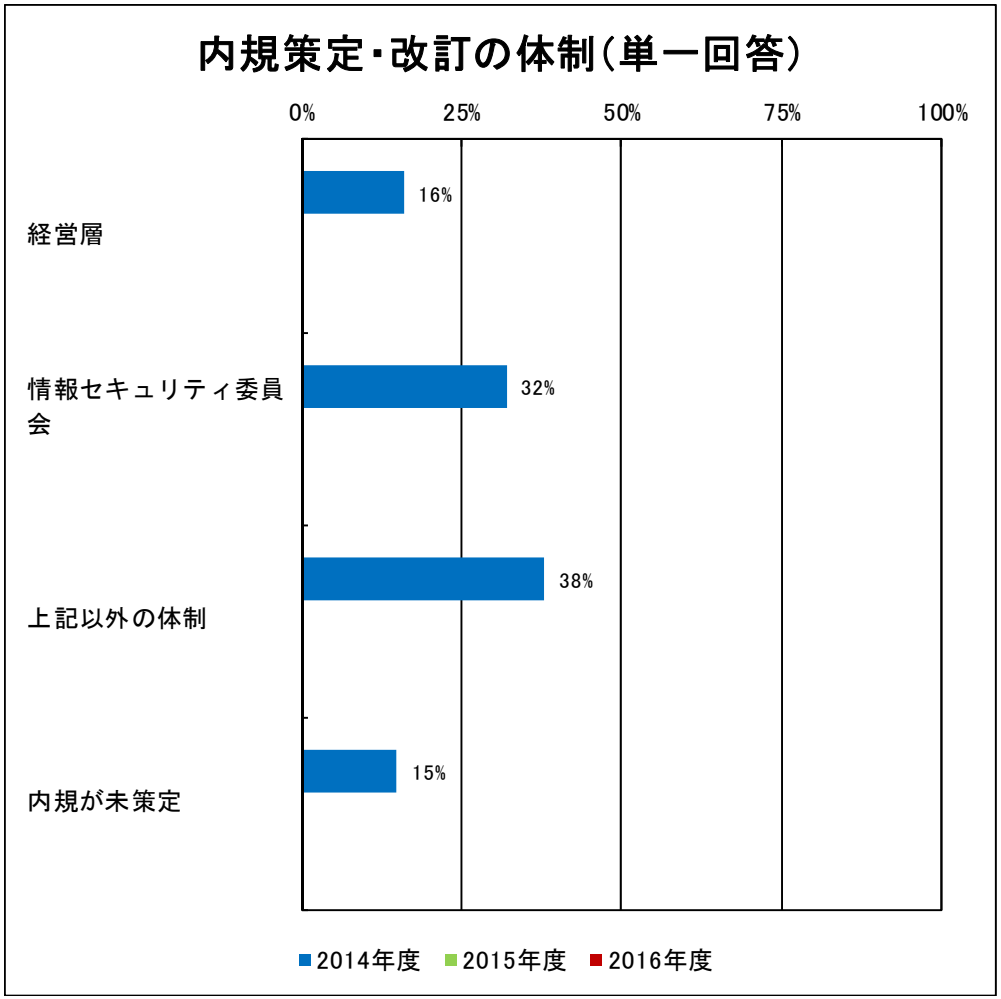
6．調査結果詳細　－　各個別設問のグラフ及び分析(3/19)　－

(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

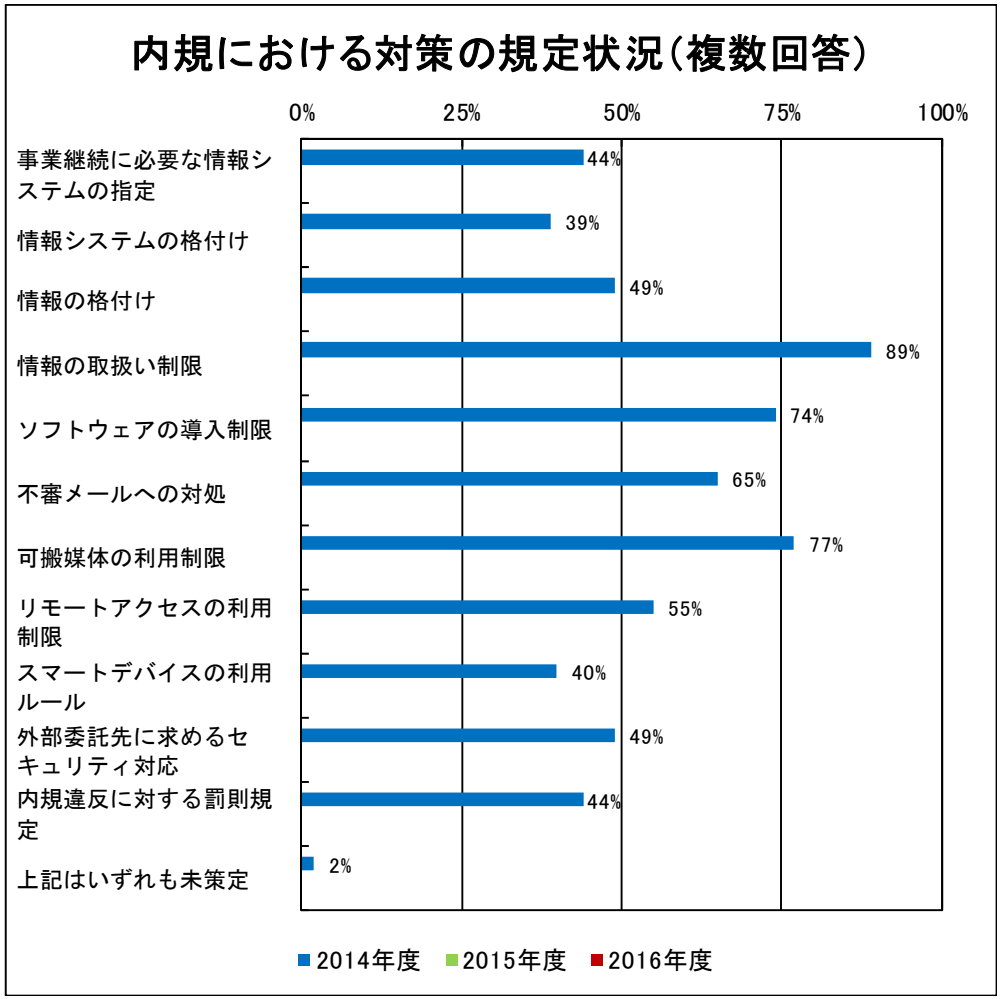
・経営層が関わる割合は15%程度、情報セキュリティ委員会が関わる割合は3割強、それ以外の体制が関わる割合は４割弱。
・内規が未策定の事業者も15%存在。



※金融、政府・行政サービスは読替え可能項目なし（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、可搬媒体の利用制限、不審メールへの対処など情報漏えい防止につながる対策を規定している割合が相対的に高い。



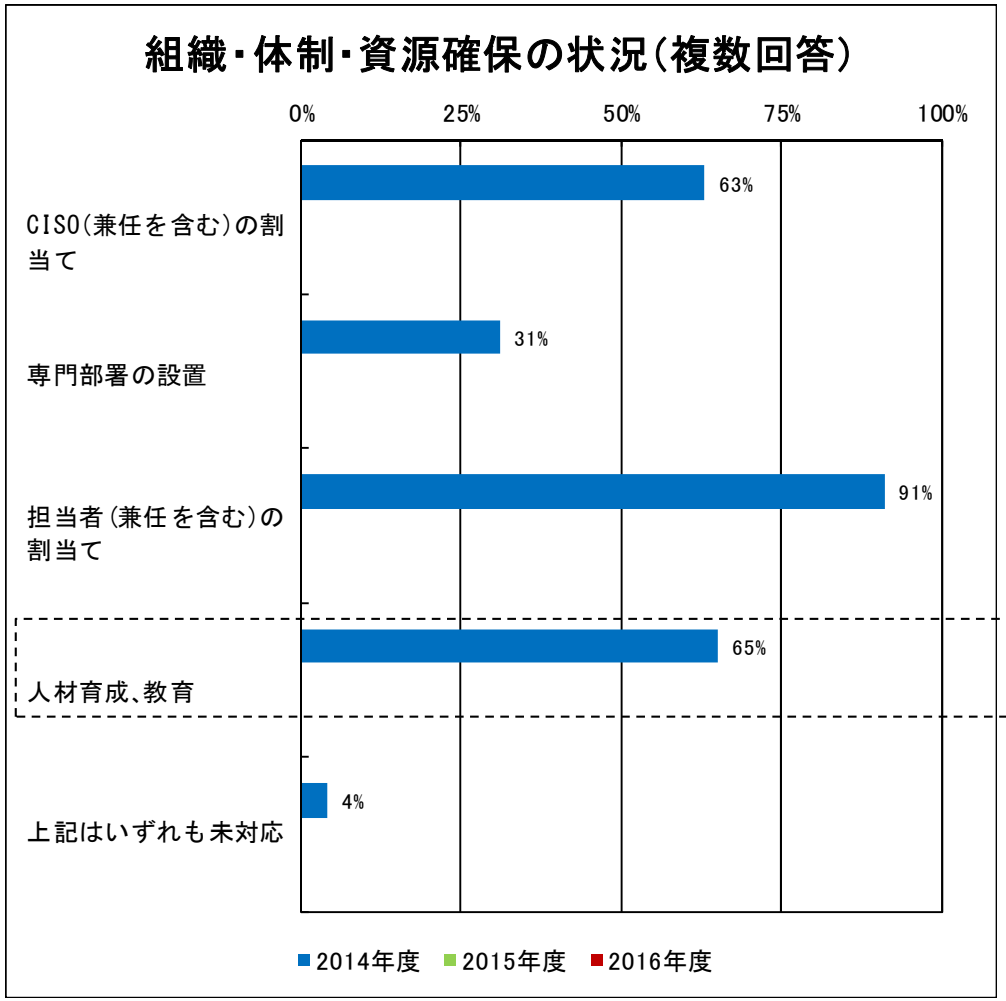
6．調査結果詳細　－　各個別設問のグラフ及び分析(4/19)　－

(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

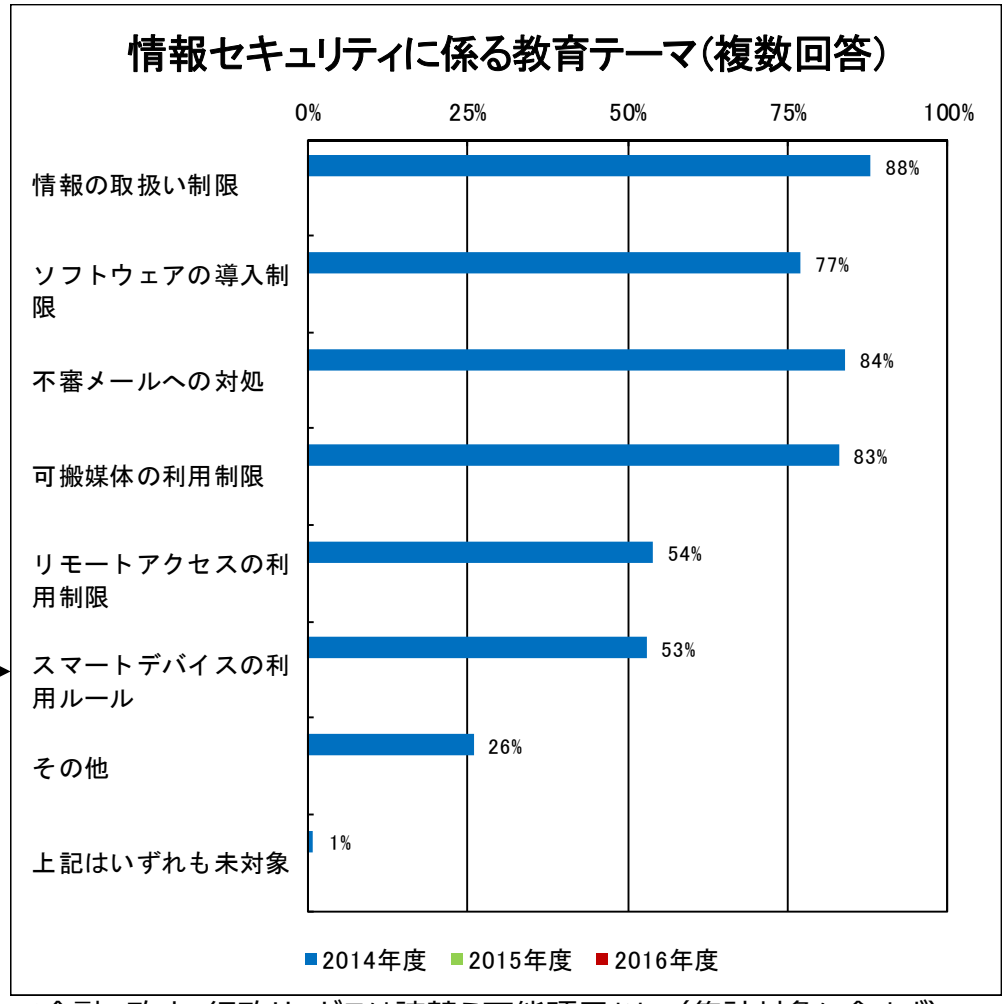
・組織・体制・資源確保については、9割強の事業者が担当者（兼任を含む）を割当。
・一方、専門部署を設置している事業者は3割強。



※金融は読替え可能項目なし（集計対象に含めず）

(b) 情報セキュリティに係る教育テーマ

・(1)③(b)で内規の規定割合が相対的に低い、リモートアクセスの利用制限、スマートデバイスの利用ルールについては、教育についても他テーマより実施割合が低い。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

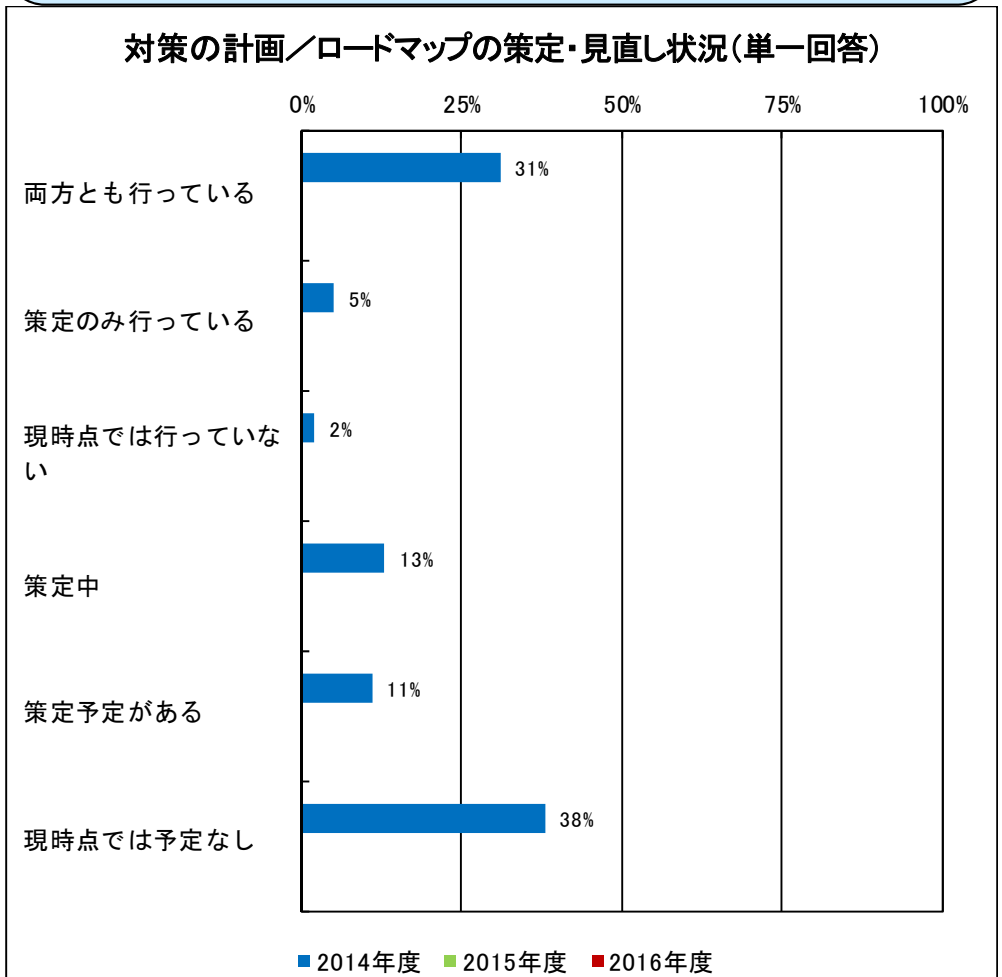
6．調査結果詳細　－　各個別設問のグラフ及び分析(5/19)　－

(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

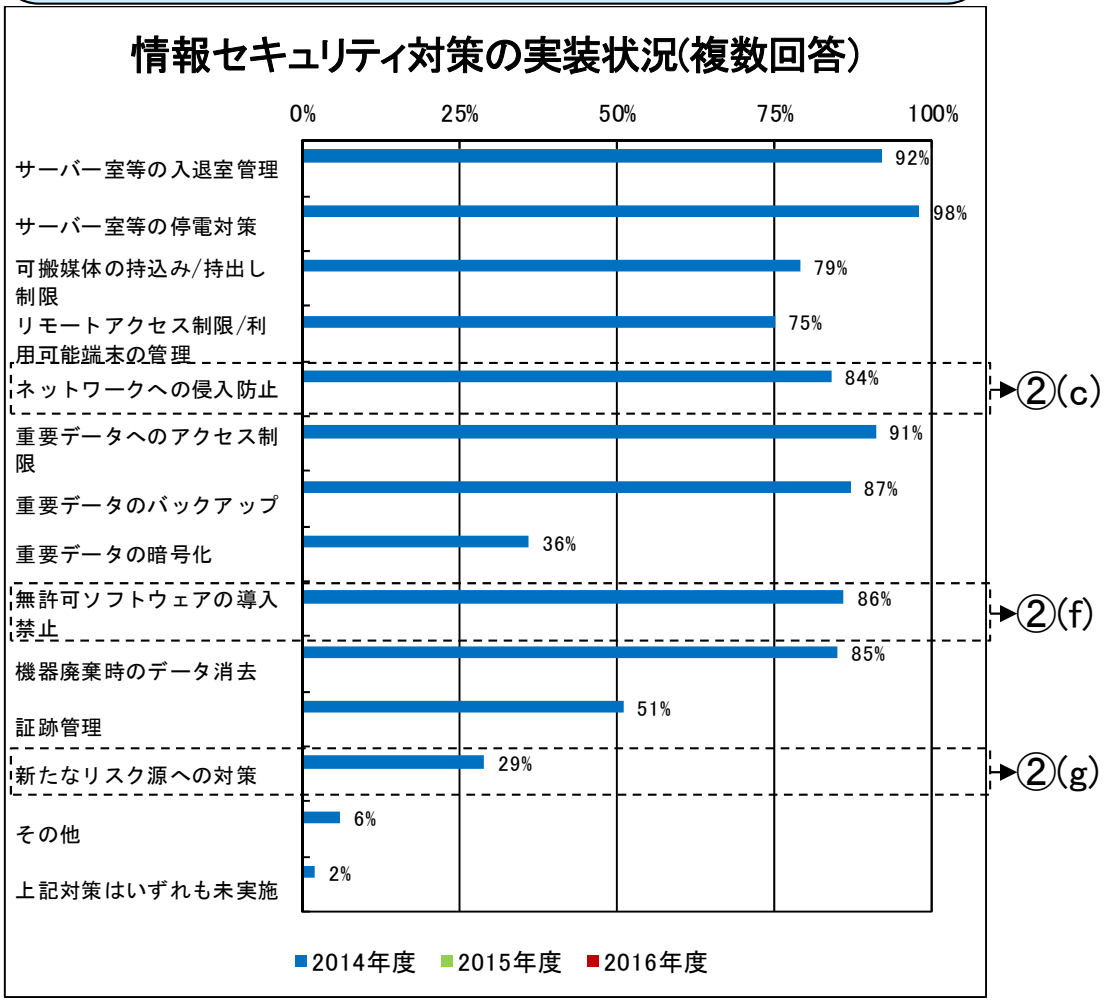
・65%程度の事業者が対策の計画／ロードマップの策定を行っていない。また、4割弱の事業者は、現時点で策定の予定もない。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

(b) 情報セキュリティ対策の実装状況

・多くの対策が7割以上の実施割合なのに対し、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割合は3～5割程度と、相対的に低い。



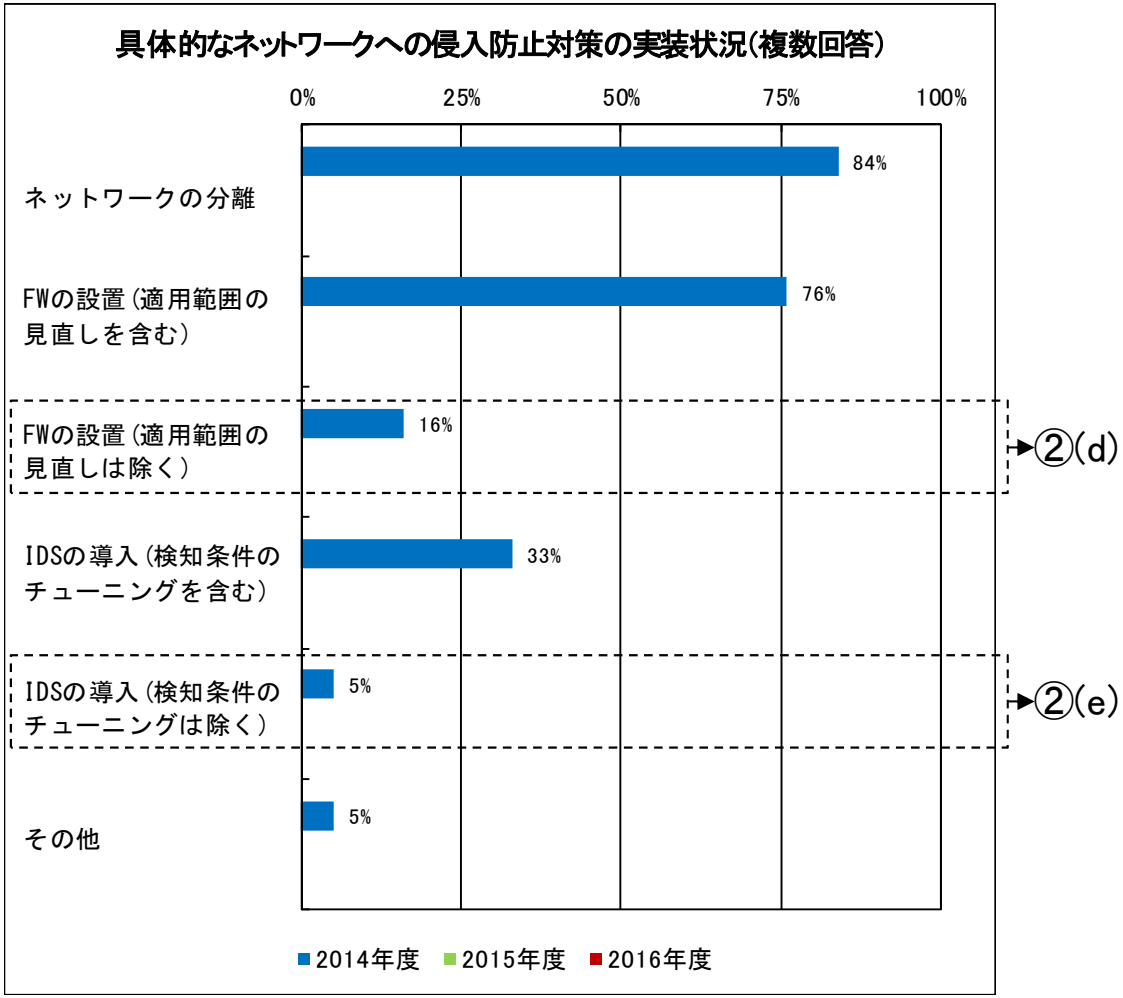
6．調査結果詳細　－　各個別設問のグラフ及び分析(6/19)　－

(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

・具体的なネットワークへの侵入防止対策としては、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割程度と、他の対策より相対的に高い。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

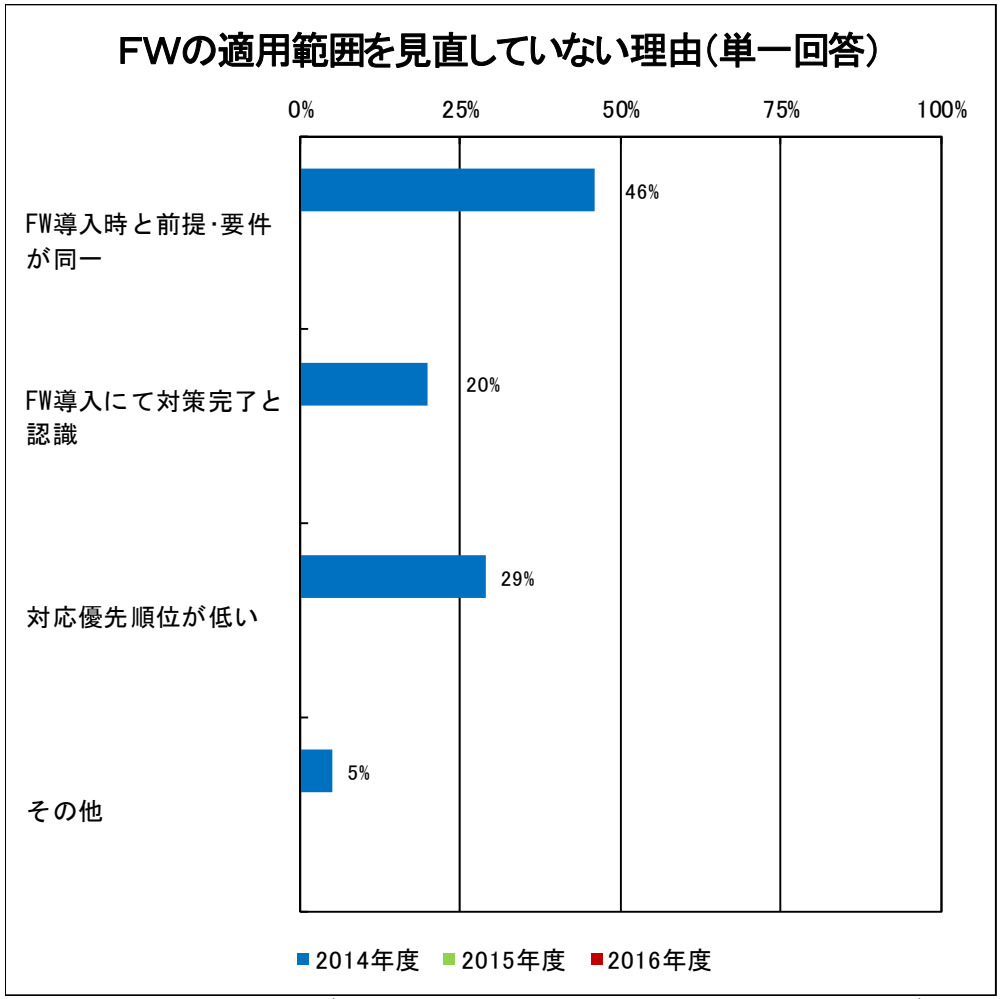
6．調査結果詳細　－　各個別設問のグラフ及び分析(7/19)　－

(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

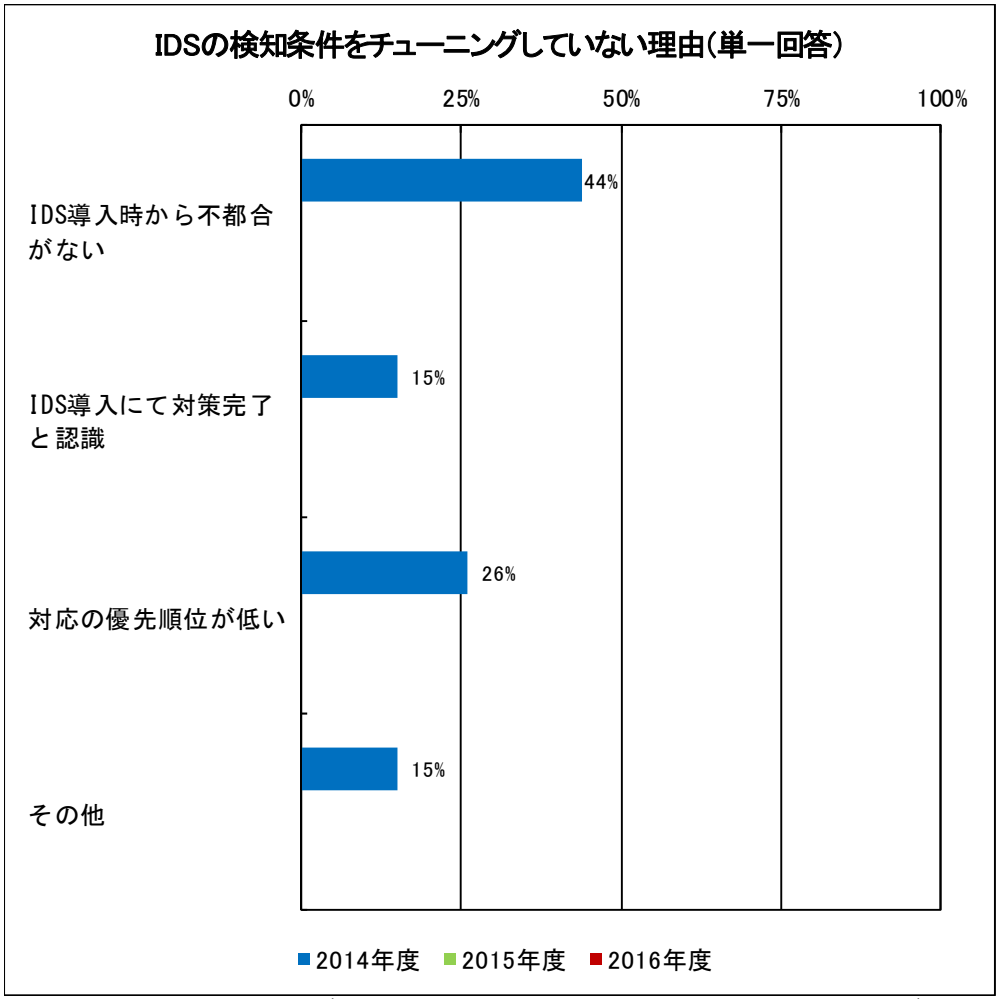
・ファイアウォールの適用範囲を見直していない理由としては、導入前と前提・要件が同じとの回答が最多。これに、対応優先順位が低いとの回答が続く。



※金融、政府・行政サービスは読替え可能項目なし（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

・侵入検知システムの検知条件をチューニングしていない理由としては、導入時から不都合がないとの回答が最多。これに、対応の優先順位が低いとの回答が続く。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

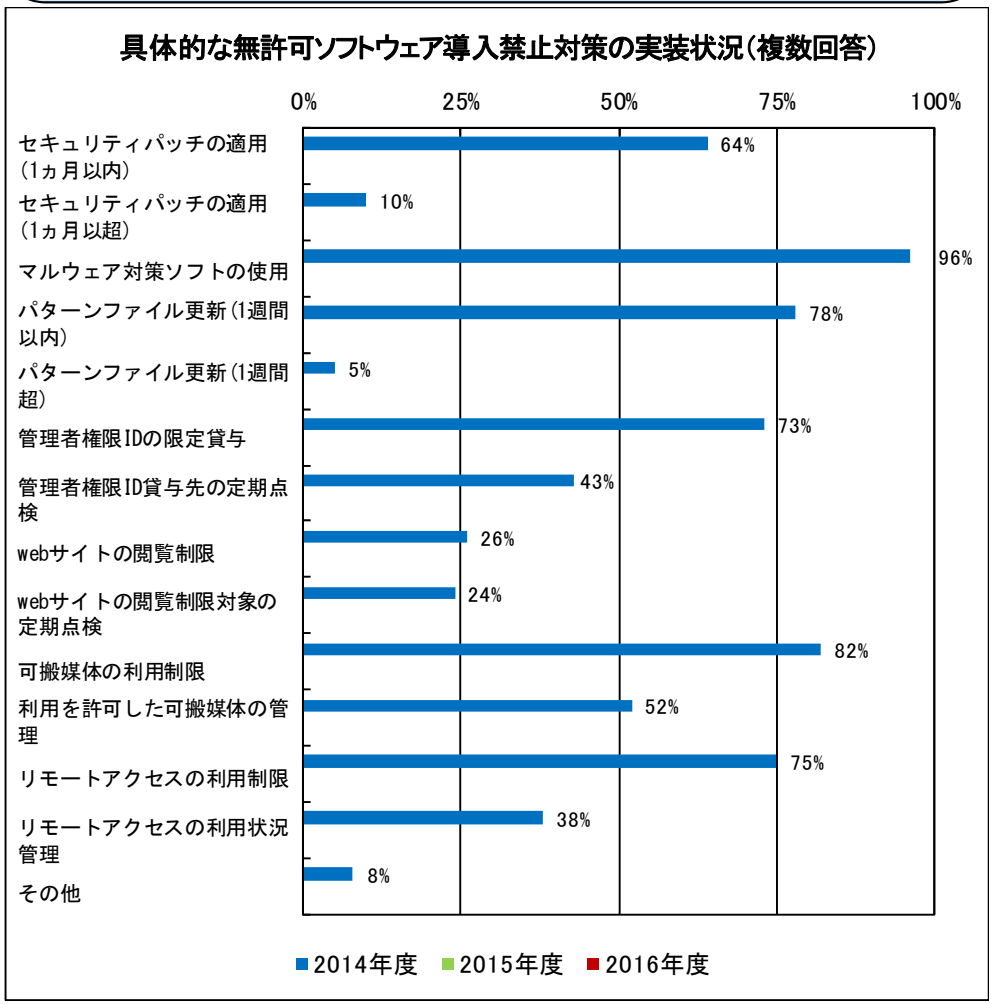
6．調査結果詳細　－　各個別設問のグラフ及び分析(8/19)　－

(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

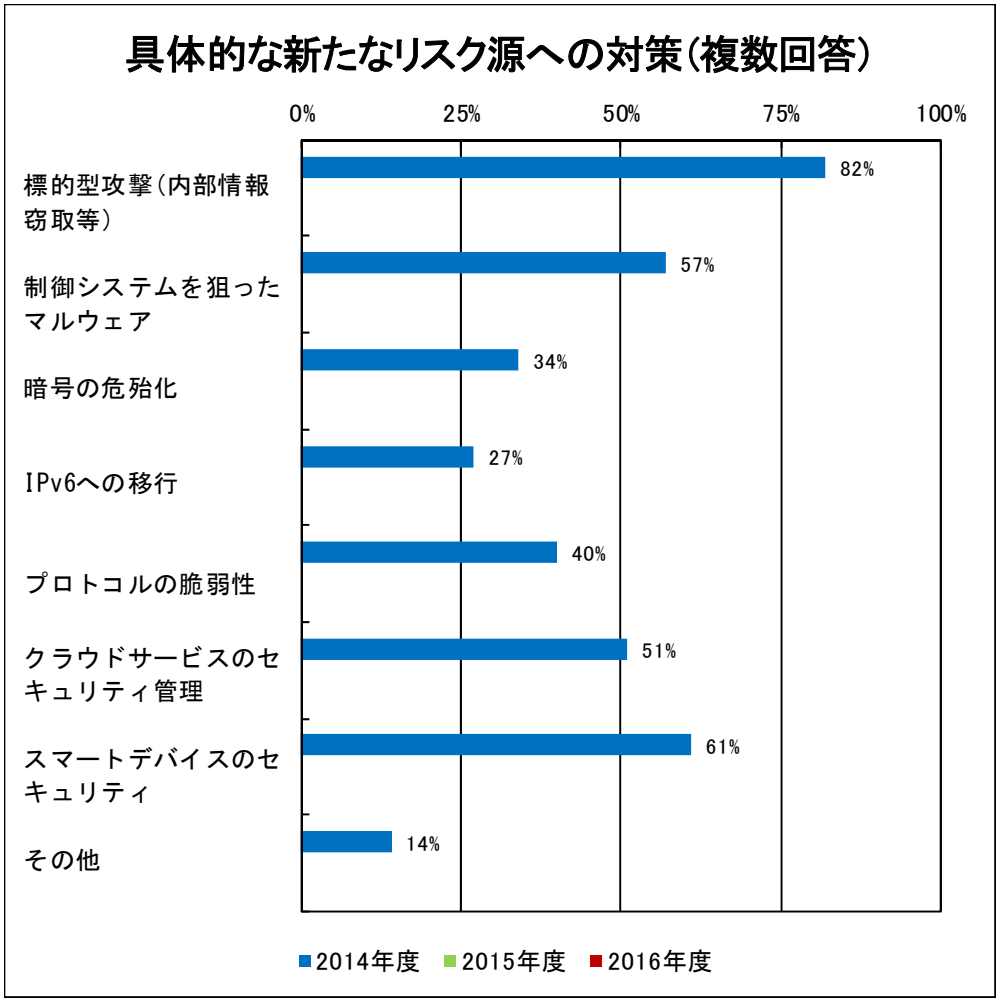
(f) 具体的な無許可ソフトウェア導入禁止対策の実施状況

・具体的な無許可ソフトウェア導入禁止対策の実装状況としては、マルウェア対策ソフトの使用が最多。これに、可搬媒体の利用制限、パターンファイル更新（1週間以内）、リモートアクセスの利用制限が続く。



(g) 具体的な新たなリスク源への対策

・具体的な新たなリスク源への対応としては、標的型攻撃が最多。これに、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、クラウドサービスのセキュリティ管理が続く。



※政府・行政サービスは読替え可能項目なし（集計対象に含めず）

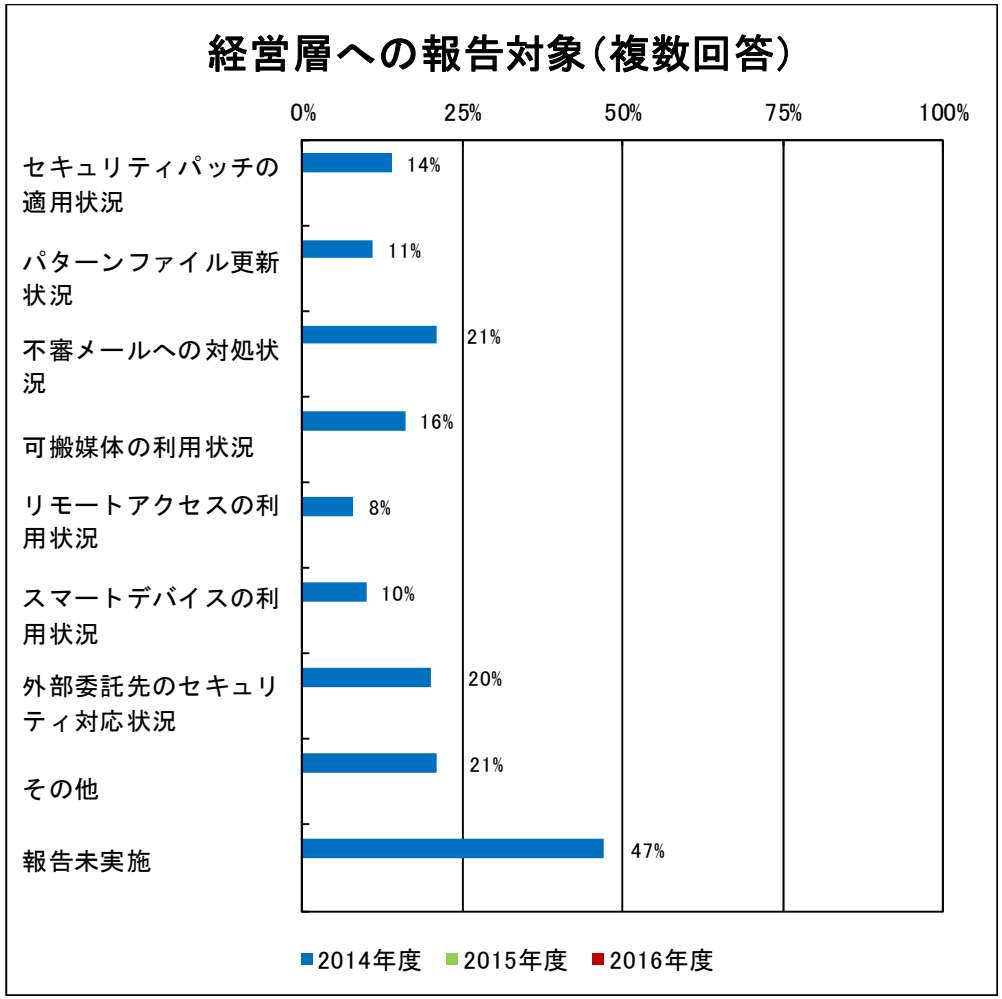
6．調査結果詳細　－　各個別設問のグラフ及び分析(9/19)　－

(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、報告対象としている割合は概ね1～2割の範囲。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え可能項目なし（集計対象に含めず）

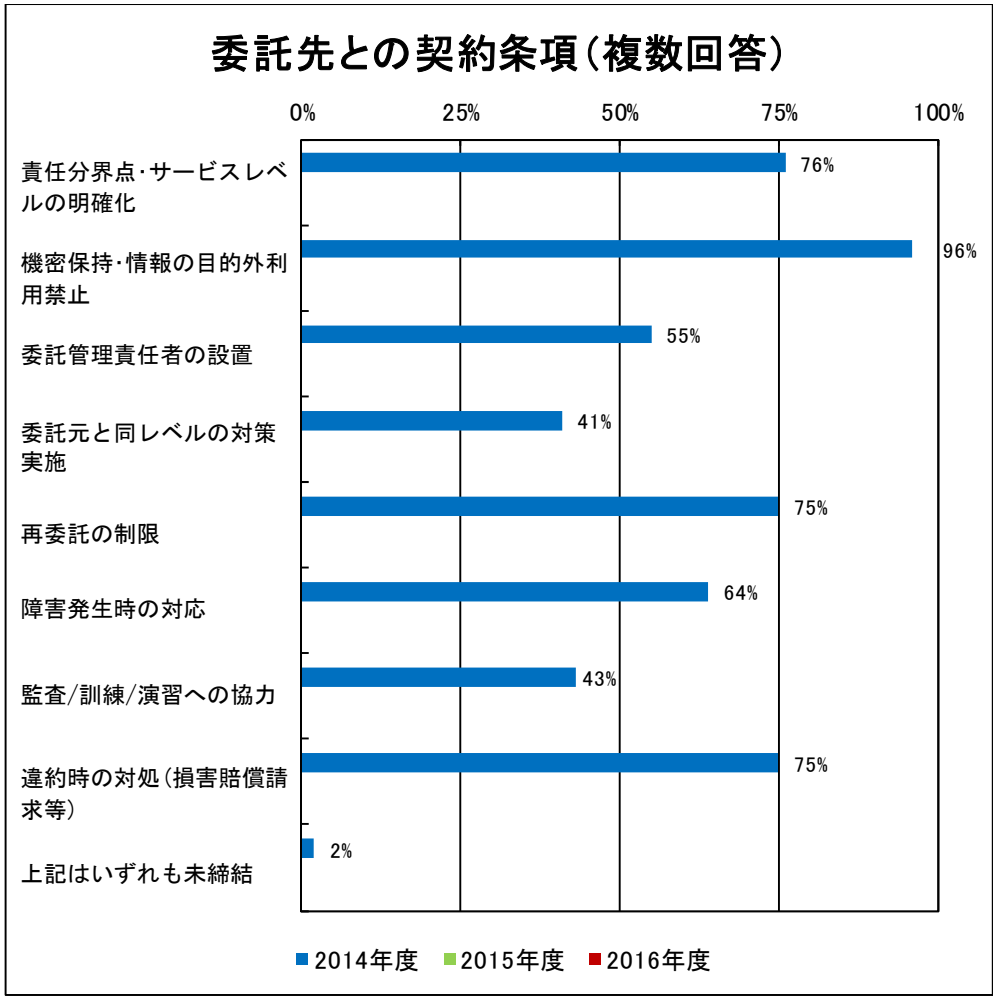
6．調査結果詳細　－　各個別設問のグラフ及び分析(10/19)　－

(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

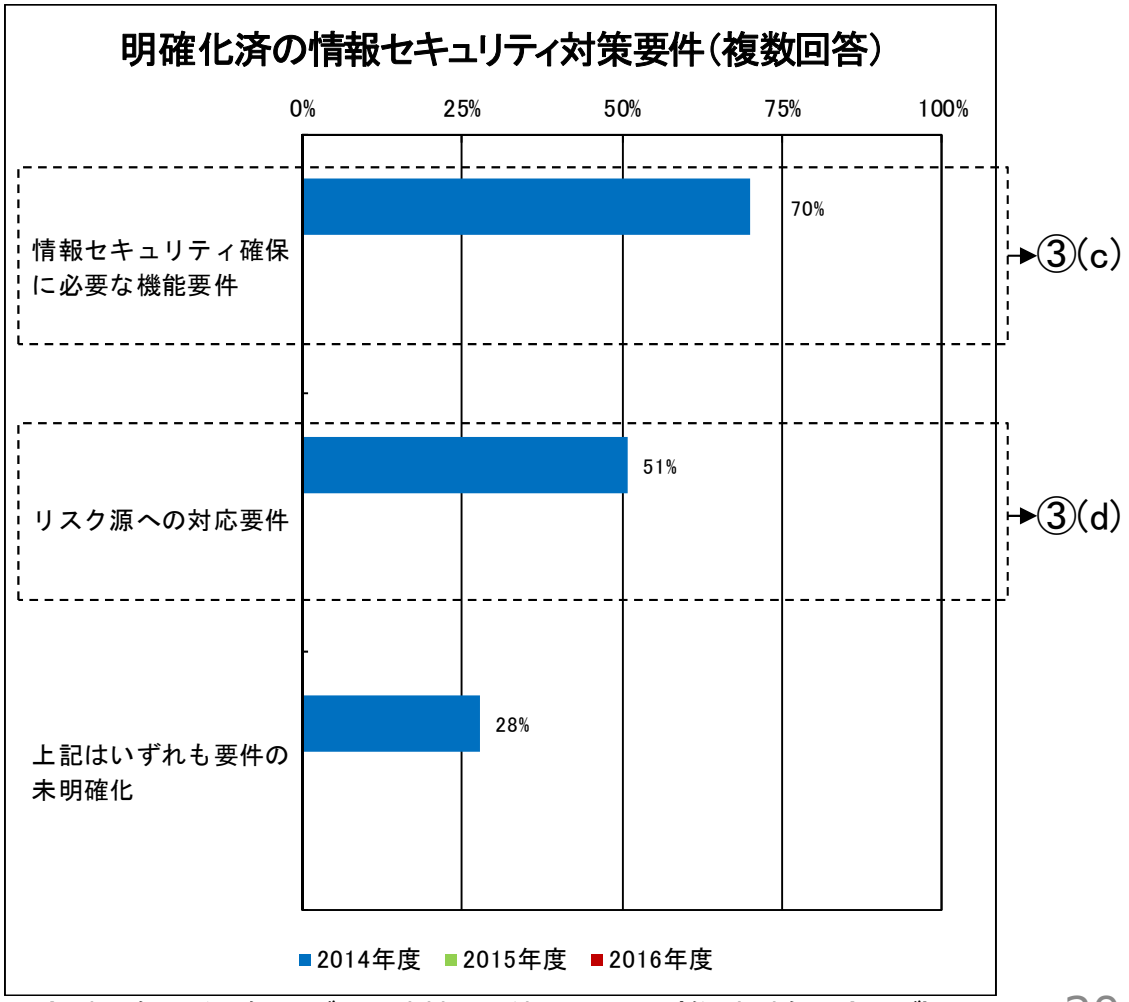
(a) 委託先との契約条項

・ほとんどの契約で機密保持・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/演習への協力の項目を設けている割合は4割強。



(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としては、事業者の7割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え可能項目なし（集計対象に含めず）

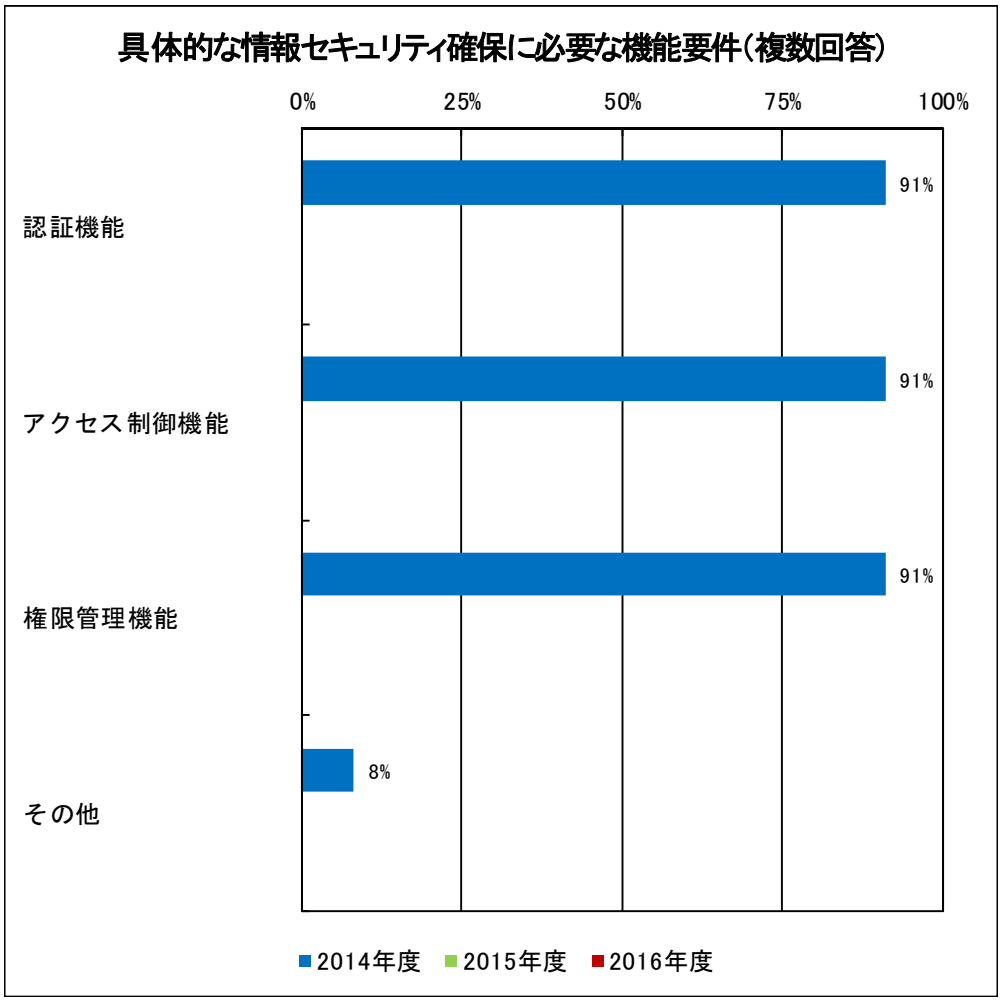
6．調査結果詳細　－　各個別設問のグラフ及び分析(11/19)　－

(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

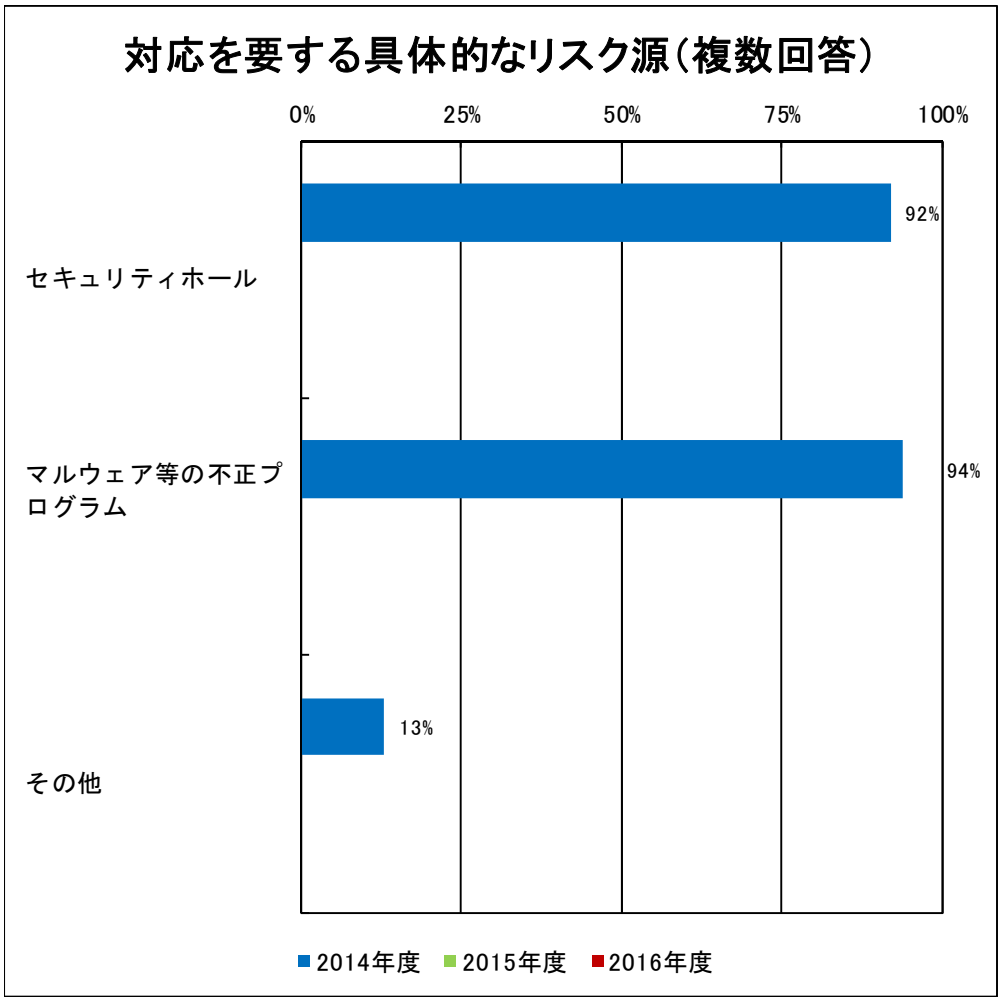
・情報セキュリティ確保に必要な機能要件としては、認証機能、アクセス制限機能、権限管理機能のいずれも同程度の割合。



※金融、政府・行政サービスは読替え可能項目なし（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同程度の割合。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

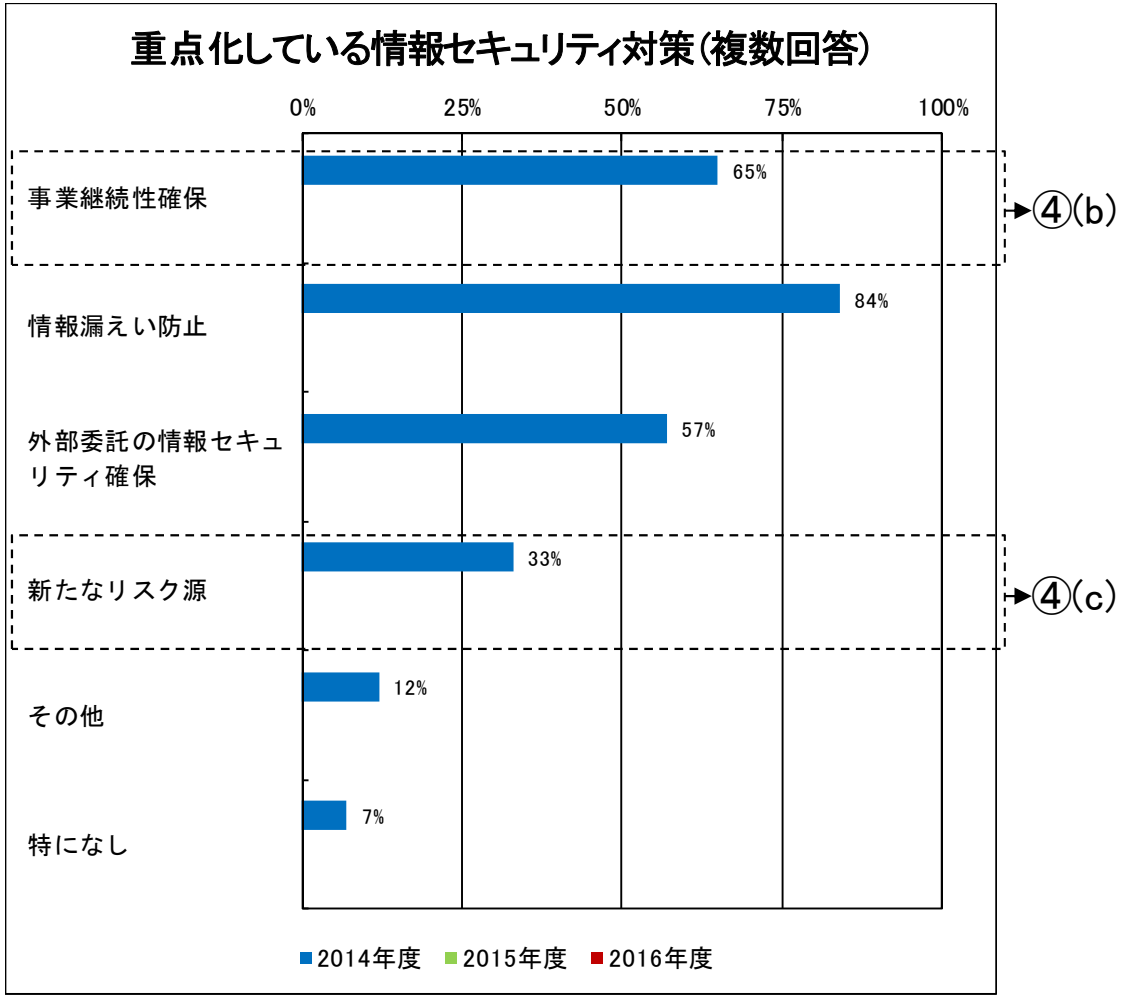
6．調査結果詳細　－　各個別設問のグラフ及び分析(12/19)　－

(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としては、情報漏えい防止が8割以上と最も多く、これに事業継続性確保が続く。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

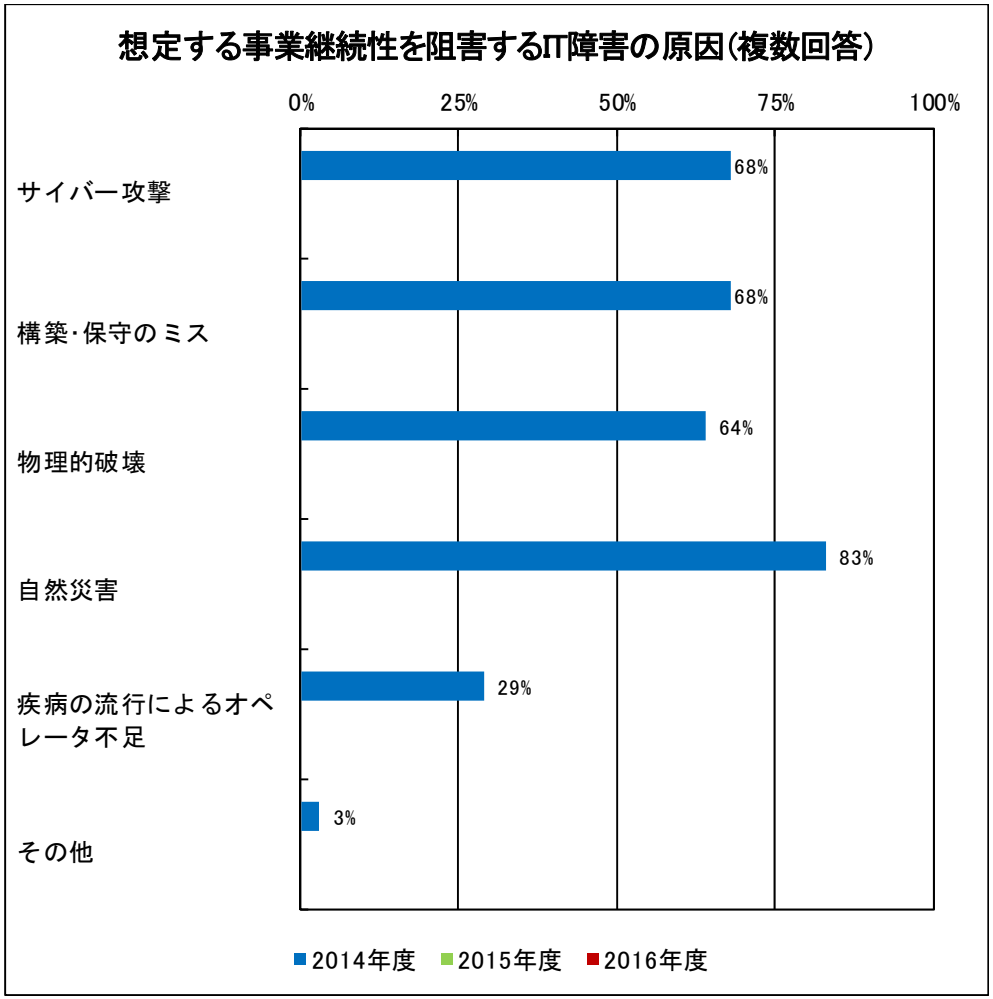
6．調査結果詳細　－　各個別設問のグラフ及び分析(13/19)　－

(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

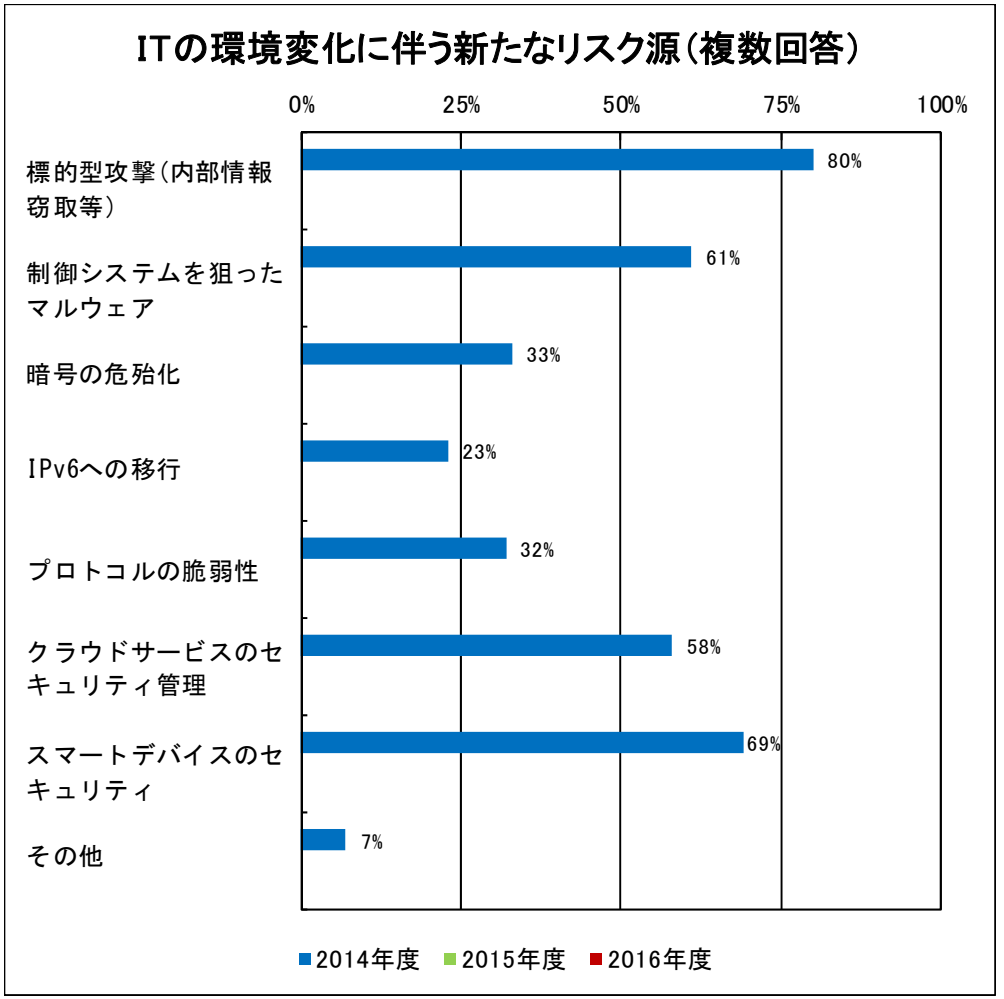
・想定する事業継続性を阻害するIT障害の原因としては、8割強の事業者が自然災害を挙げ、これにサイバー攻撃、構築・保守のミス、物理的破壊が続く。



※金融、政府・行政サービスは読替え可能項目なし（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

・ITの環境変化に伴う新たなリスク源としては8割の事業者が標的型攻撃を挙げ、これに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、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え可能項目なし（集計対象に含めず）

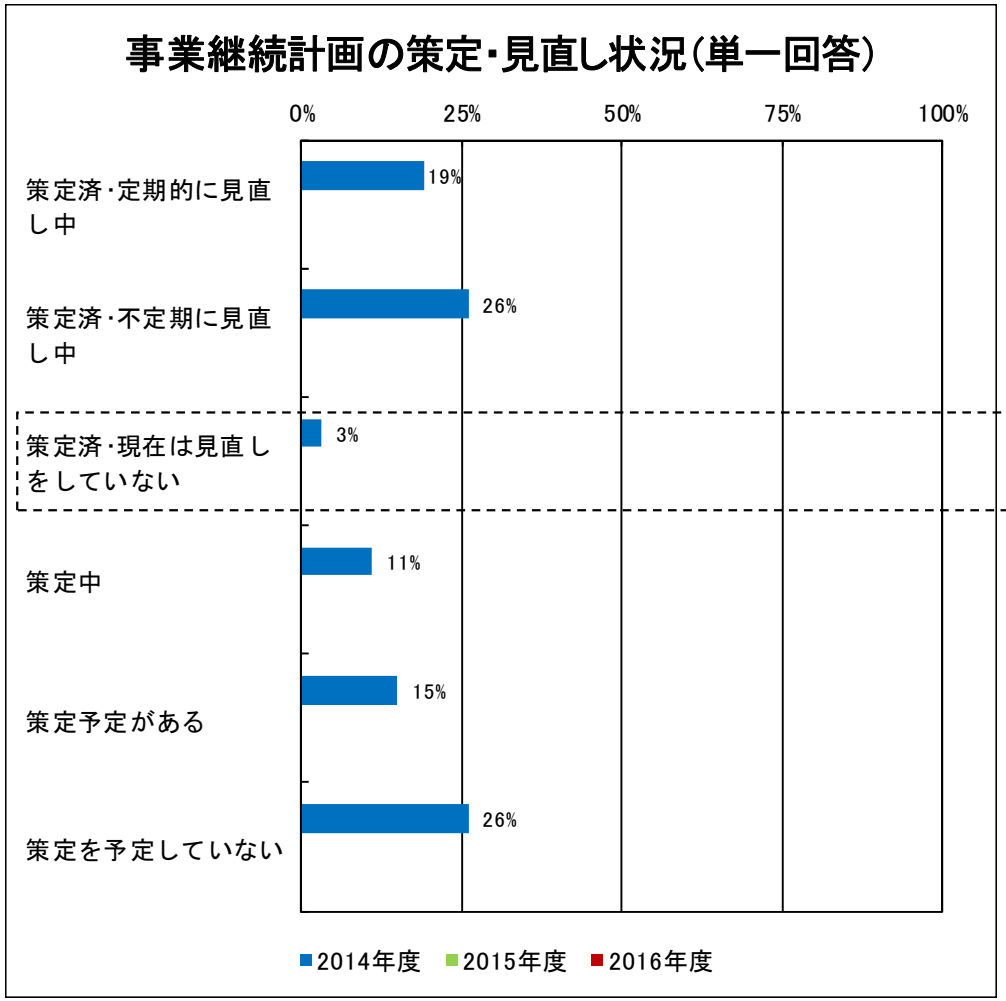
6．調査結果詳細　－　各個別設問のグラフ及び分析(14/19)　－

(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

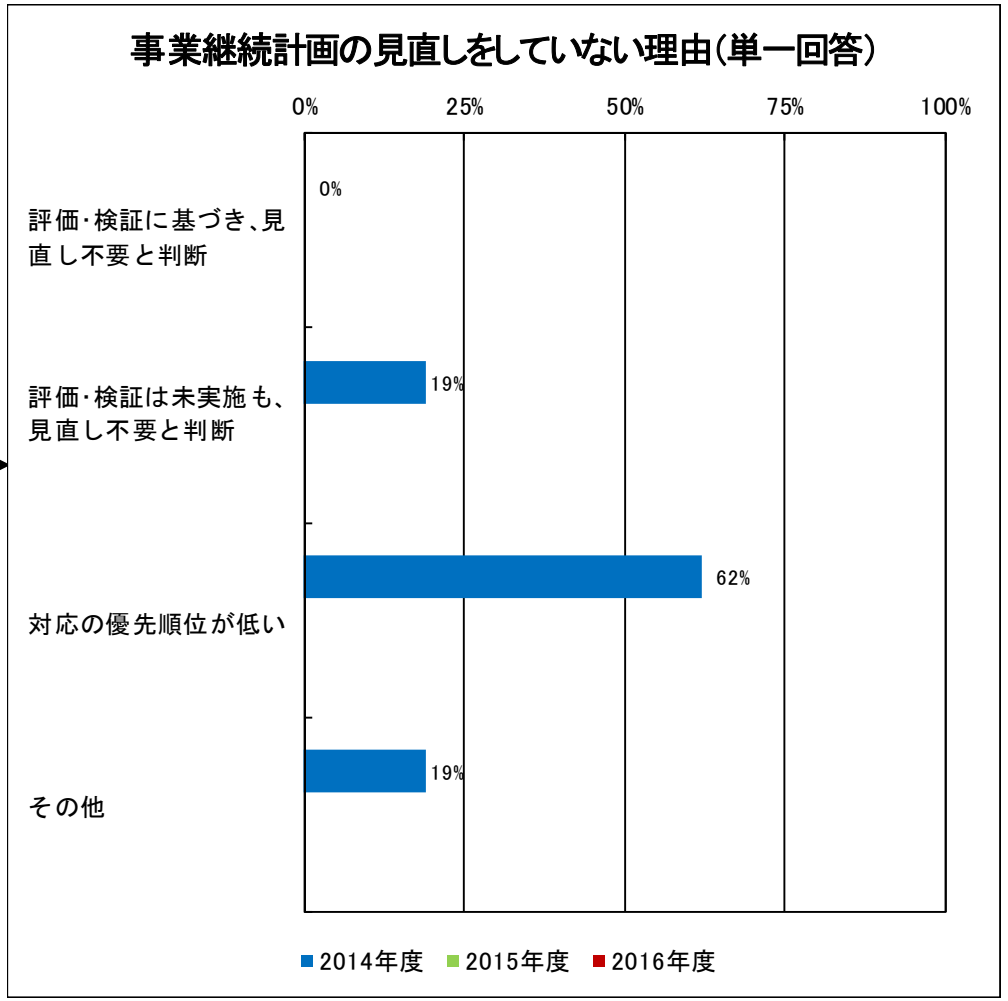
・事業継続計画は、55%程度の事業者が現在未策定の状況。



※金融、政府・行政サービスは読替え可能項目なし（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ためとの回答が6割強で最多。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

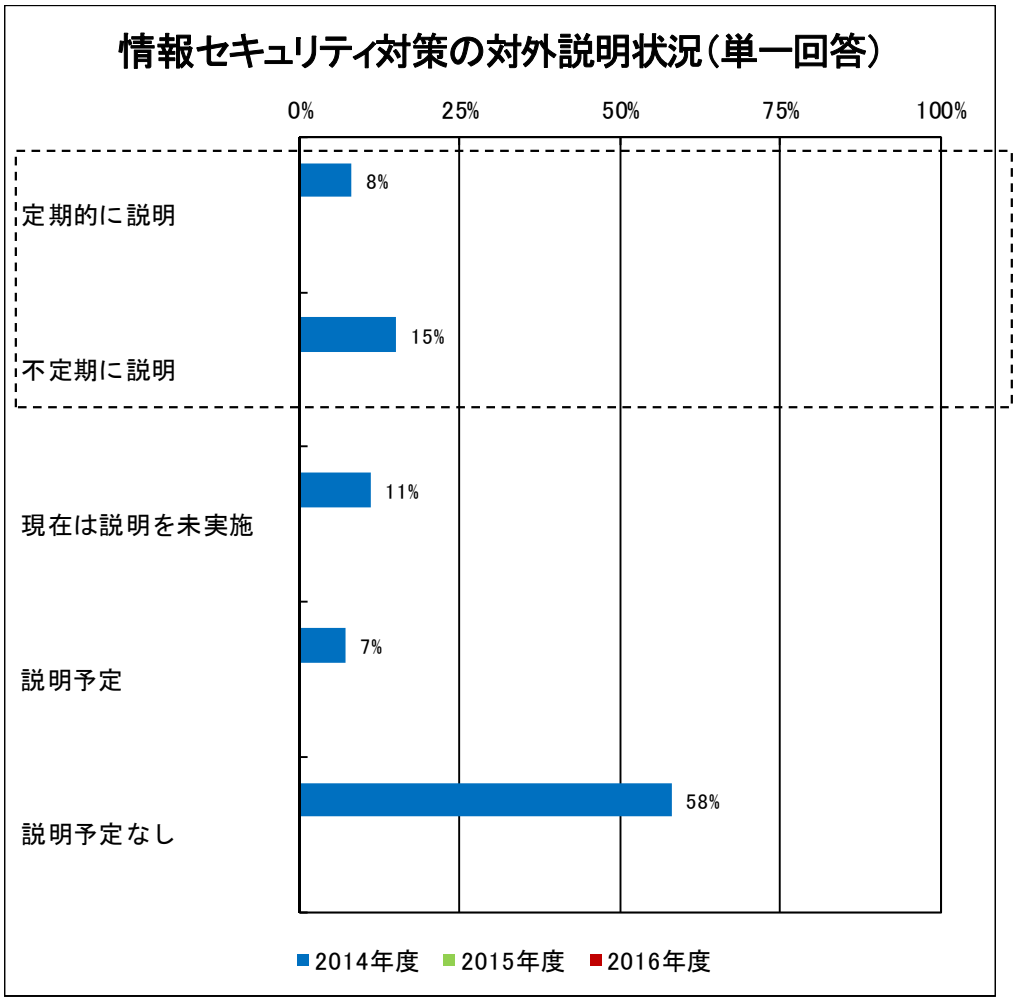
6．調査結果詳細　－　各個別設問のグラフ及び分析(15/19)　－

(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

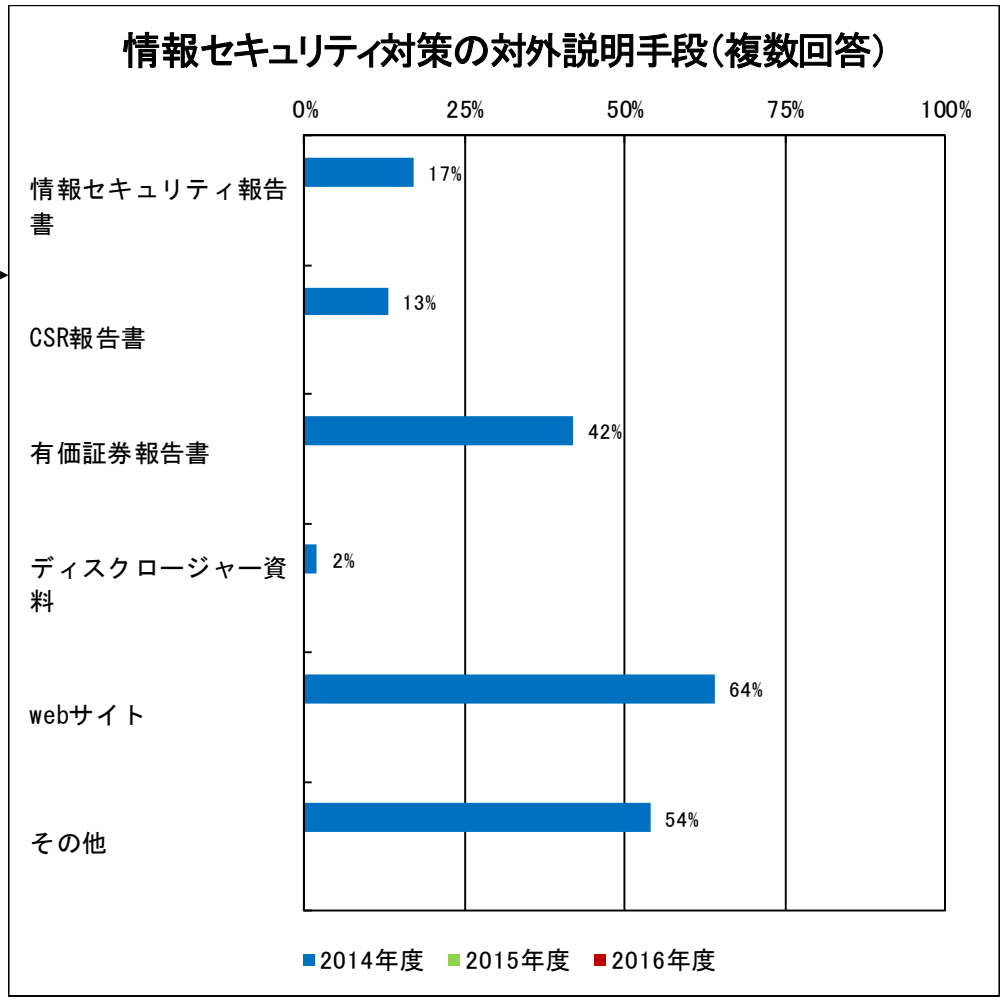
・情報セキュリティ対策の対外説明を現状実施している事業者は2割強である一方、予定していない事業者は6割弱で最多。



※金融、政府・行政サービスは読替え可能項目なし（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

・情報セキュリティ対策の対外説明を実施している事業者が用いる手段としては、webサイトが65%程度と最多。これに、その他の手段、有価証券報告書が続く。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

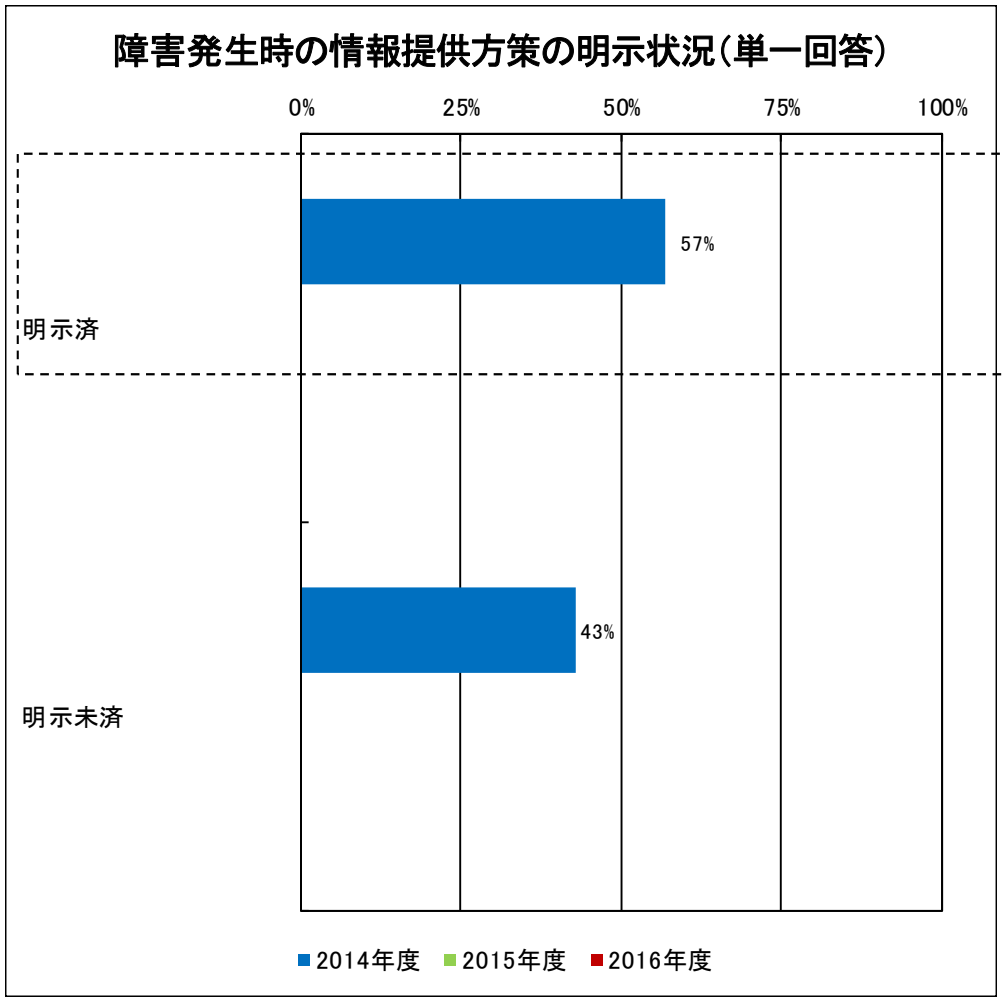
6．調査結果詳細　－　各個別設問のグラフ及び分析(16/19)　－

(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

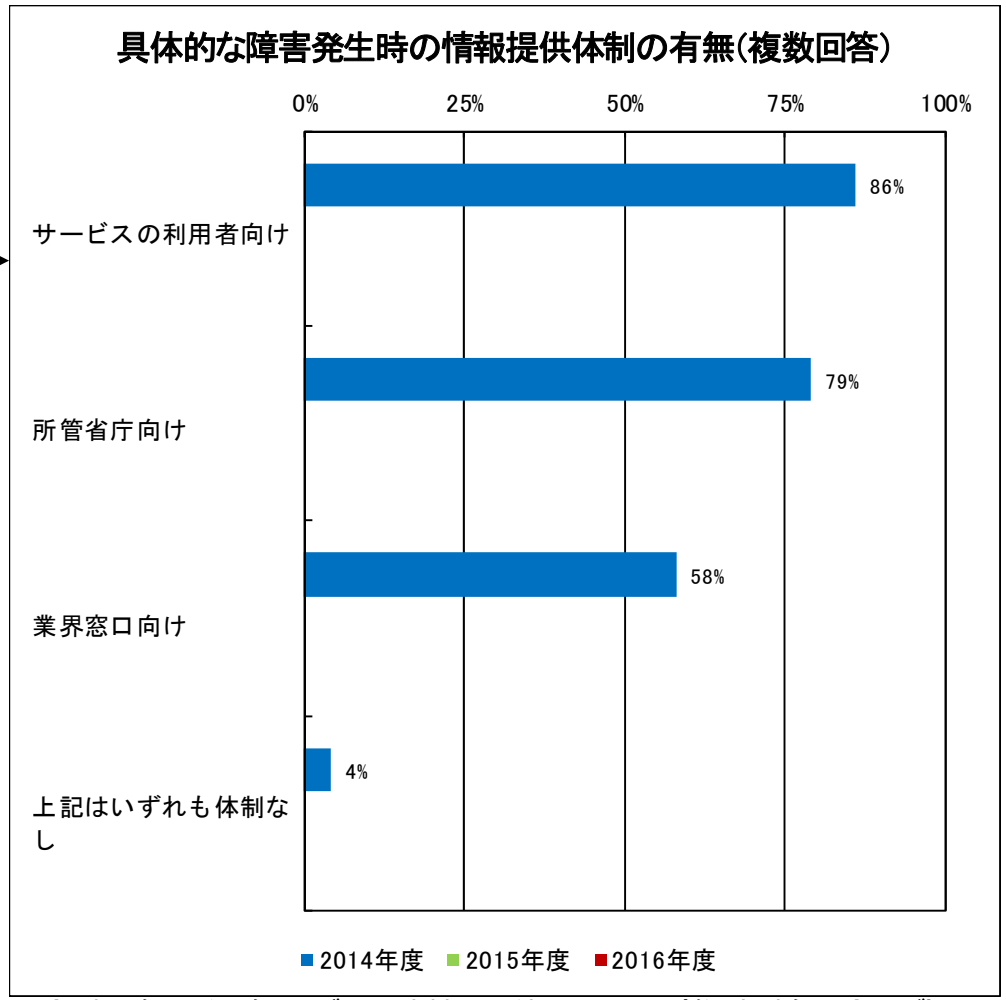
・約6割の事業者が、障害発生時の情報提供方策を明示済。



※金融、政府・行政サービスは読替え可能項目なし（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

・障害発生時の情報提供体制としては、サービスの利用者向けが8割強と最多。これに、所管省庁向け、業界窓口向けが続く。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

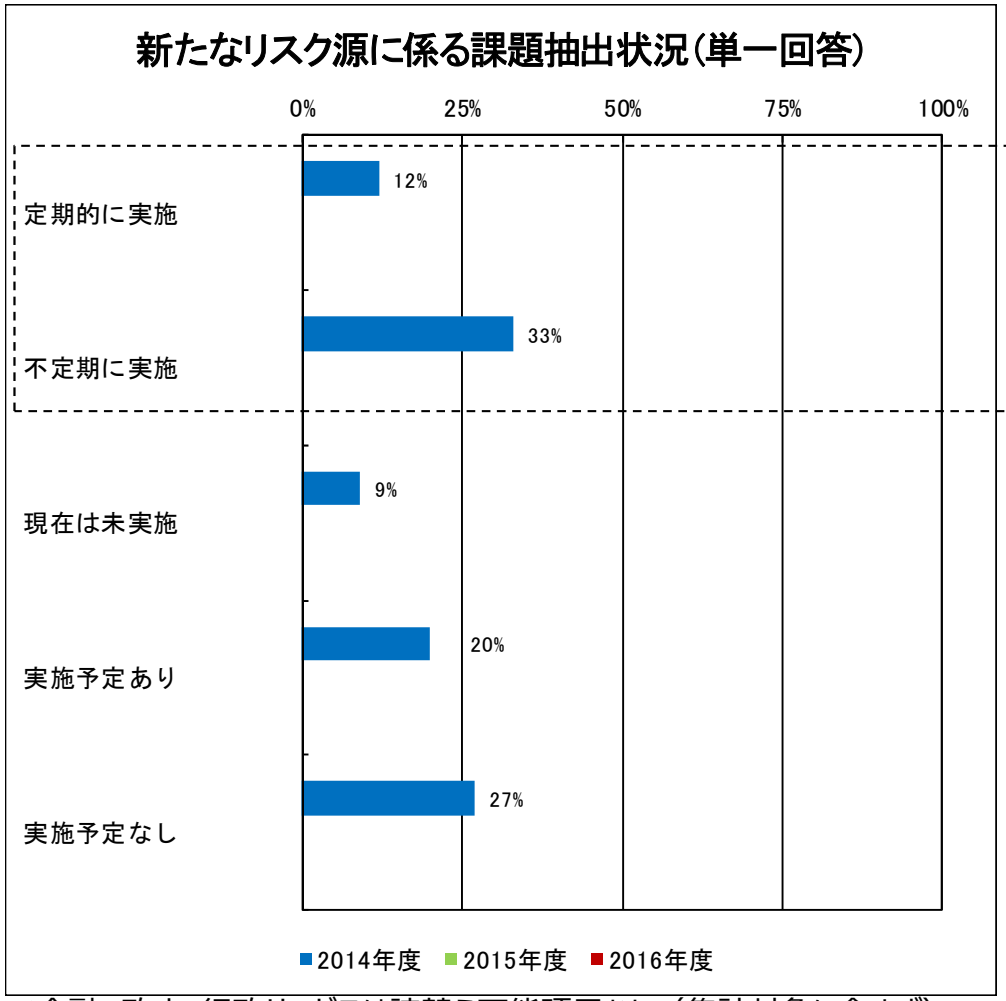
6．調査結果詳細　－　各個別設問のグラフ及び分析(17/19)　－

(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

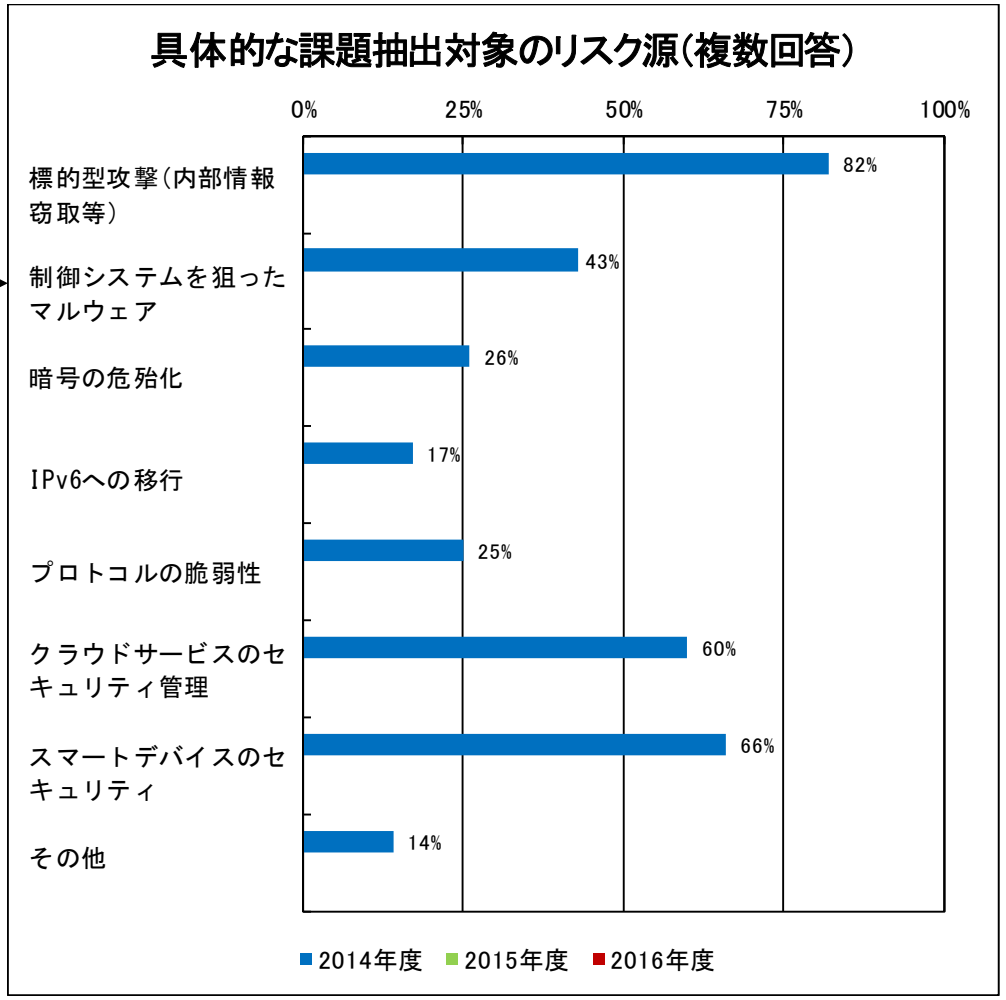
・新たなリスク源に係る課題抽出を現状実施している事業者は5割弱、実施予定なしの事業者は3割弱。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

(b) 具体的な課題抽出対象のリスク源

・課題抽出を実施している事業者の具体的な課題抽出対象のリスク源は標的型攻撃が8割強で最多。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え可能項目なし（集計対象に含めず）

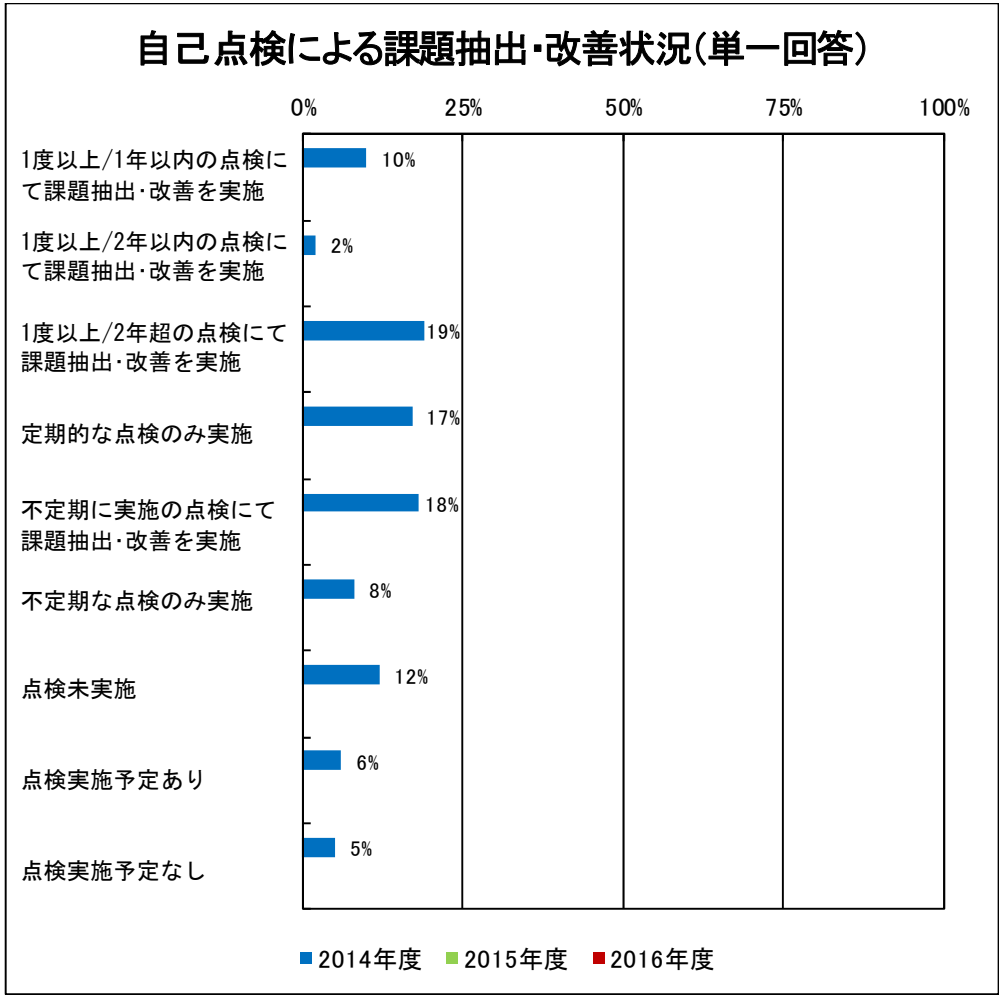
6．調査結果詳細　－　各個別設問のグラフ及び分析(18/19)　－

(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。

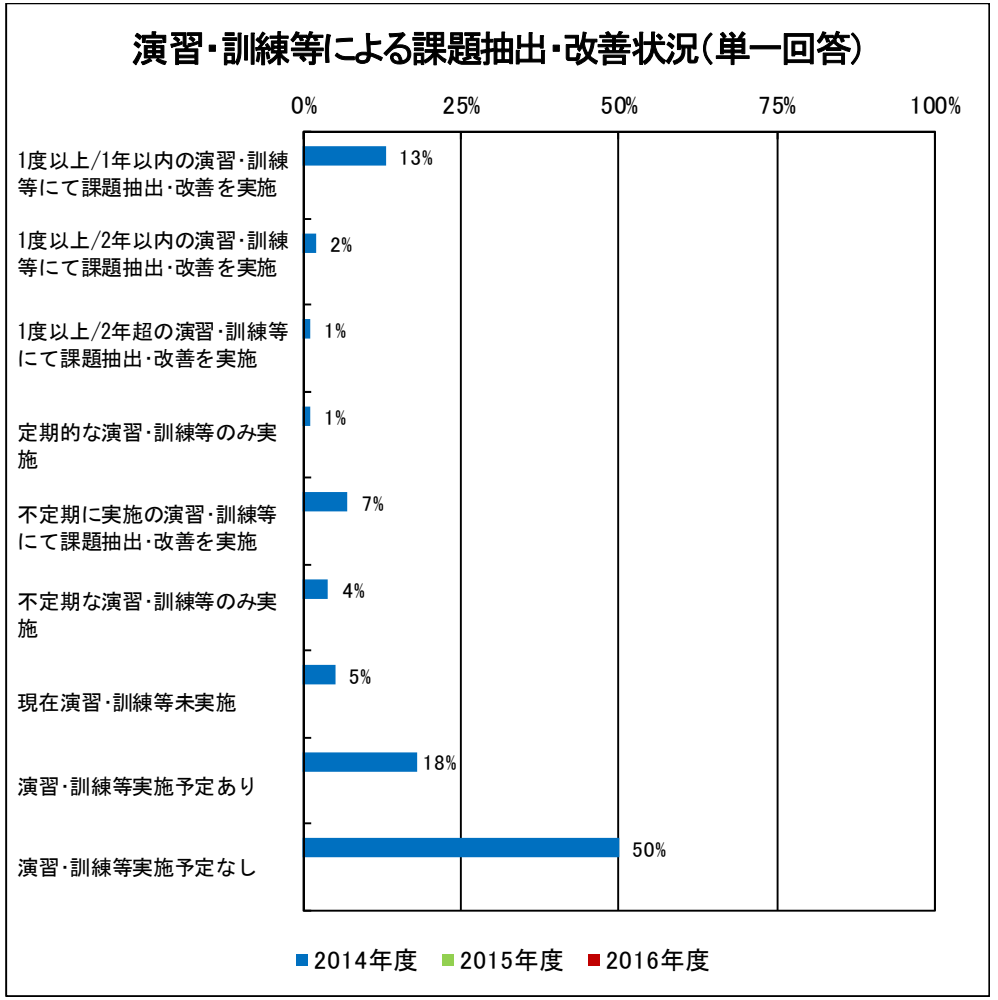


※金融は読替え可能項目なし（集計対象に含めず）

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・改善の実施状況も同程度。
・一方、5割の事業者は実施予定なしと回答。



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

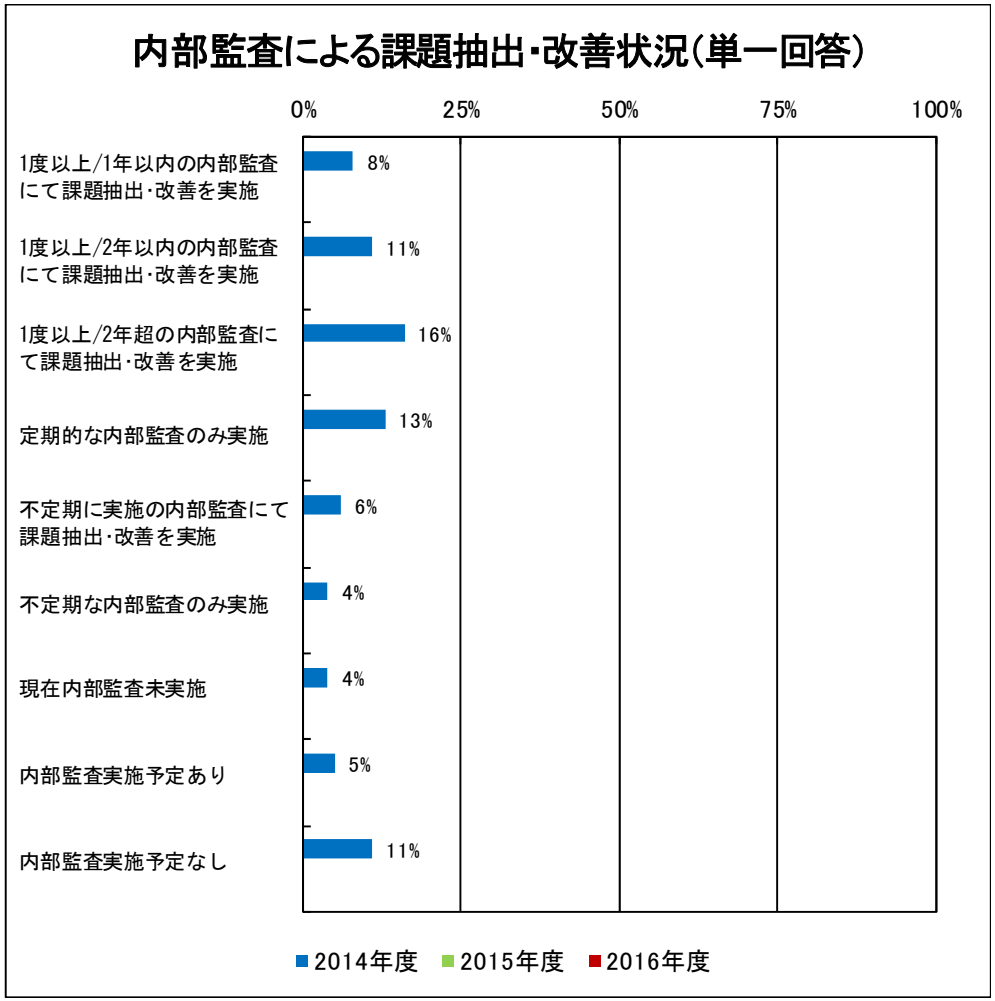
6．調査結果詳細　－　各個別設問のグラフ及び分析(19/19)　－

(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5割弱。定期的な内部監査に基づく課題抽出・改善の実施状況は35%程度。

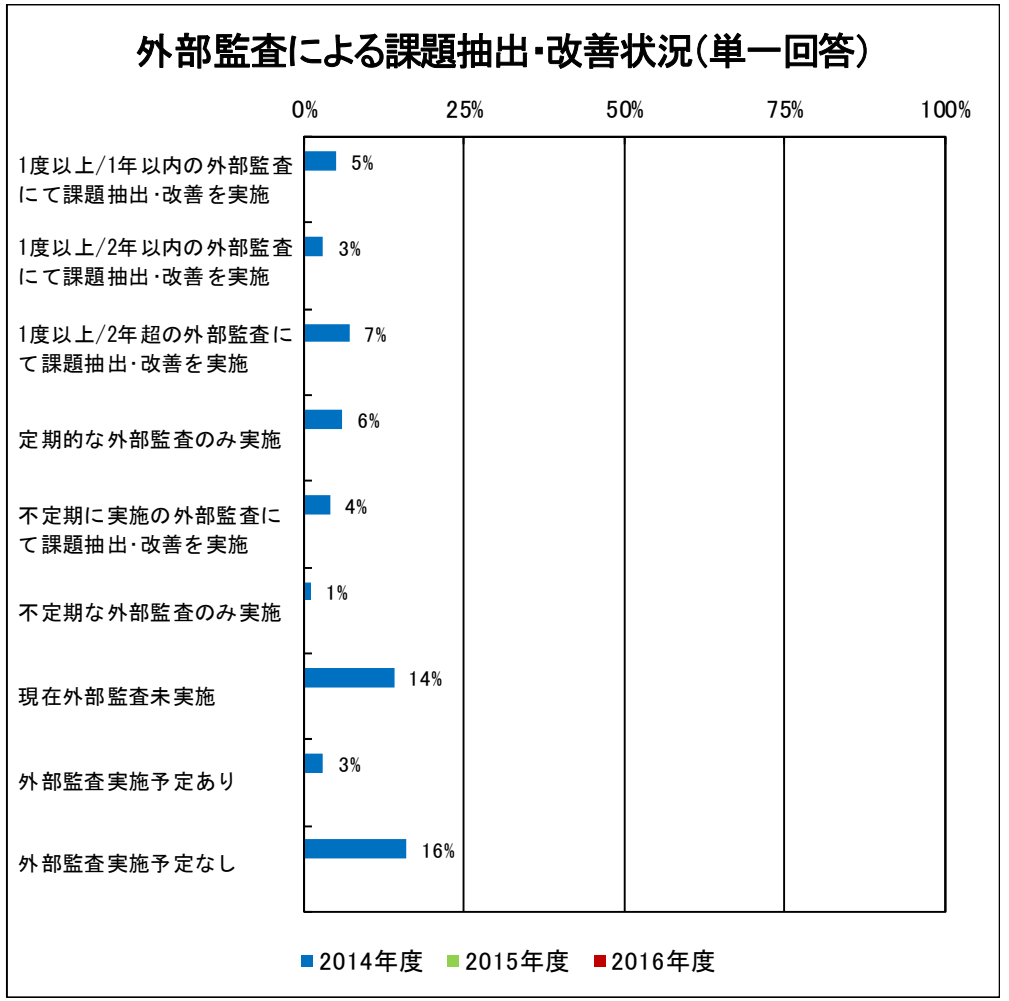


※金融は読替え可能項目なし（集計対象に含めず）

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割強。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%。



※金融は読替え可能項目なし（集計対象に含めず）

6．調査結果詳細　－　自由意見(1/2)　－

【経営層の在り方に関する意見】

- 人員が少なく、なかなか対策に手が回らない。（往訪調査でも同様の意見あり。）
- 小規模の事業体では、セキュリティ対策の必要性を理解していても、対策の策定や見直しには人的時間的に制約があり、実施できない状況がある。
- ＩＴ人材育成のための支援を重視して頂きたい。
- 一企業の立場で情報セキュリティ対策を講じようとすると、それなりの費用がかかる。これに対して一定額の補助を国として制度化していただけるなら、もっと良い対策を講じることができると考える。

【事業者等による自らの責任における実施状況に関する意見】

- 企業の体力に応じた評価指標などがより充実すると、効果的なセキュリティ対策ができると考える。
- 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やすいのではないか。
- セキュリティ対策（現状では主にサイバー攻撃対策）はどれだけ強化しても利益を生み出すわけではなく、一般的にその重要性は理解されても、必要性は軽視されがちであり、特に費用面ではある意味軽減を図りやすい一面がある。こういった問題点を広くかつ分かりやすく知らしめる観点からも、対策を怠ることによる影響額（被害額＋投資コスト）がどれだけの利益、資産等の損失に至るかの指標的なものを示してほしい。

【情報共有体制の推進に関する意見】

- 現実のリスクの公開と情報共有が必要。セキュリティベンダー間では実現しているが、ユーザー間ではリスクの共有がなされていない。
- 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対応をお願いしたい。
- 引き続きNISCメール等による情報提供をお願いする。
- 国からの脆弱性情報等が届いていない。（往訪調査時の意見）

※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(2/2)　－

【防護基盤の強化（広報公聴活動）に関する意見】

- 指針の重要部分を抜粋した概要資料があれば、周知・理解に役立つと考える。
- セミナー等を開いていただければ内容がより理解できると思う。
- 公的機関での広報活動をもっと積極的に行ってほしい。

【その他の意見】

- 本編、対策編の策定は大変ありがたい。欲を言えば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と思う。
- ＩＴ関連の危険性を学校教育の場で教えておいた方がよいのではないか。
- 今回の質問について、社内セキュリティの観点から答えにくい点があった。
- 本アンケートについて、用語の意味合いや問いの位置付けが難解であった。
- 情報セキュリティの相談窓口の設置をお願いしたい。
- 現在、コンピュータウィルスの対策はソフトウェア業界任せであり、真の脅威に積極的に取り組んでいるとは言い難いと思う。真の脅威を未然に防ぐために国の研究機関が重要なコンピュータウィルス対策を行うべきではないか。
- ISMS認証やプライバシーマークの取得が、継続的なセキュリティ対策の改善につながっている。（往訪調査時の意見）
- 自社のセキュリティ対策の水準が、どの程度なのかを知りたい。（往訪調査時の意見）
- 同業他社との意見交換の場を設け、自社のセキュリティ対策の水準や最新動向等を把握するように努めている。（往訪調査時の意見）

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。

【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) 本編及び対策編をご存知ですか。
(2) 本編及び対策編を何で知りましたか。
(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) （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。
(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。
(4) 内規の策定・見直しの契機をお知らせ下さい。
(5) 内規策定・改訂を行う際の体制をお知らせ下さい。
(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。
(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。
(9) 事業継続計画の策定・見直し状況をお知らせ下さい。
(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。
(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。
(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。
(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。
(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。
(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。
(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。

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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。

【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）