資料3

NISC National Information Security Center

2013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

2013年11月29日

内閣官房情報セキュリティセンター（NISC）

「安全基準等の浸透状況等に関する調査」の概要（1/2）

「重要インフラの情報セキュリティに係る第2次行動計画」及び「サイバーセキュリティ2013」に基づき、各重要インフラ分野における安全基準等について、重要インフラ事業者等にどの程度浸透しているか、また重要インフラ事業者等が安全基準等に対して準拠しているかを把握するために、**毎年一定時期（定点）に**行う調査。

安全基準等は随時見直しがなされるものであり、また着実にその浸透を図るべきものであることから、定期的な本調査を通じて継続的に浸透状況等を把握し、施策の成果検証に活用する。

第1次行動計画における取組み

第2次行動計画における取組み

安全基準等の策定・見直し（SJ2006）	安全基準等の見直し（SJ2007）	安全基準等の見直し（SJ2008）	安全基準等の継続的改善（SJ2009）	安全基準等の継続的改善（JS2010）	安全基準等の継続的改善（JS2011）	安全基準等の継続的改善（JS2012）	安全基準等の継続的改善（SS2013）
	浸透状況等調査（SJ2007）	**浸透状況等調査（SJ2008～SJ2009）**	**浸透状況等調査（JS2010）**	**浸透状況等調査（JS2011）**	**浸透状況等調査（JS2012）**	**浸透状況等調査（SS2013）**	

2006年度に策定・見直しを行った安全基準等を対象

毎年一定時期に調査

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

第2次行動計画

・事業者自らが定める「内規」を含めた安全基準等の浸透を確実なものとするために、**「安全基準等の浸透状況等に関する調査」**を引き続き定期的に実施することとする。調査項目・調査主体等については、適宜見直しを行うこととする。
・**毎年一定時期に事業者自らが定める「内規」を含めた対策状況の客観的な把握**を行うこととする。

サイバーセキュリティ2013

・重要インフラ所管省庁の協力を得つつ、「安全基準等」の整備浸透状況について以下の調査を行う。
〈重要インフラ事業者等に対する調査〉
「安全基準等」の浸透状況に係る調査を行い、結果を公表する。また次年度の調査のための企画・準備を行う。

「安全基準等の浸透状況等に関する調査」の概要（2/2）

◆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	：	以下方法のいずれかを重要インフラ所管省庁が選択 ①重要インフラ分野が独自で行う調査を活用し、NISCが提供する調査項目に読替え ②NISCが提供する調査資料を活用
調査基準日	：	2013年3月末日（「①独自調査を活用」する場合は、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担当（発出・回収方法は重要インフラ所管省庁が決定）
分野毎の集計	：	集計担当については、以下のいずれかを重要インフラ所管省庁が選択 ① 重要インフラ所管省庁にて集計 ② NISCにて集計
全体集計・とりまとめ	：	NISCにて集計・とりまとめ

◆実施時期　（NISC提供の調査資料活用 の場合）

調査期間	：	2013年4月～2013年9月（再調査期間を含む）
とりまとめ	：	2013年10月～2013年11月

◆主な調査内容（NISC提供の調査項目）

①安全基準等の整備状況に係る事項
　指針・対策編の認知に係る状況及び手段
　内規策定・見直しの契機及び参考とする安全基準等の諸規格
②情報セキュリティ対策状況に係る事項
　組織・体制及び資源の確保に係る対策状況
　情報保護に係る対策状況
③安全基準等への準拠状況に係る事項
　自己点検、演習、訓練等に係る実施状況
④情報セキュリティ対策に係る提言、要望等

調査結果　アンケート回収状況と留意点

- 調査への協力を求めた3,356事業者等に対し、3,160事業者等からアンケートを回収　(回収率：94.1%　前年比：+0.9%)
- 全体集計においては、分野に共通の重み付け（正規化）をした上で実施

分野		既存調査活用	アンケート回収状況　＊カッコ内は昨年度の数値		
			調査対象範囲	配布数	回収数
情報通信	電気通信	しない	固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等	76 (79)	20 (28)
	ｹｰﾌﾞﾙﾃﾚﾋﾞ	しない	ケーブルテレビセプター参加事業者	241 (---)	221 (---)
	放送	しない	日本放送協会及び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）	194 (193)	194 (184)
金融		する	金融機関等	892 (921)	796 (789)
航空	航空運送	しない	航空運送事業者	2 (2)	2 (2)
	航空管制	しない	官庁	1 (1)	1 (1)
鉄道		しない	鉄道事業者２２社	22 (22)	22 (22)
電力		しない	一般電気事業者、日本原電(株)、電源開発(株)	12 (12)	12 (12)
ガス		しない	政令指定都市８社、同等の事業者２社	10 (10)	10 (10)
政府・行政ｻｰﾋﾞｽ		する	地方公共団体	1,789 (1,784)	1,789 (1,784)
医療		しない	医療機関（病院抽出）	50 (50)	38 (43)
水道		しない	水道事業体（事業者抽出）	45 (45)	45 (45)
物流		しない	物流事業者及び業界団体	22 (21)	10 (9)
全分野合計				3,356 (3,140)	3,160 (2,928)

留意点

留意点１：類似調査との重複回避
⇒既存調査の活用にて調査運営を効率化

留意点２：調査対象の範囲
⇒調査可能な範囲から取組み。調査対象の拡大は追って検討（範囲は重要インフラ所管省庁が決定）
（第２３回重要インフラ専門委員会資料より）

分野にて回収数が異なるため、分野に共通の重み付け（正規化）をした上で集計を実施

＜集計式＞

$$A = \frac{\left(a_1 / \alpha_1\right) + \left(a_2 / \alpha_2\right) + \cdots + \left(a_n / \alpha_n\right)}{n}$$

A：回答Ａに対する全体集　計（%）
a_n：分野ｎにおける回答Ａ　の数
α_n：分野ｎにおける回収数

※安全基準等の範囲にあわせて、情報通信を３つ、航空を２つに分けて集計するため、原則 n=13
（既存調査を活用する場合に読み替え可能な項目がない場合を除く）

＜参考1＞既存調査と浸透状況等調査の関係整理（2013年度実績）

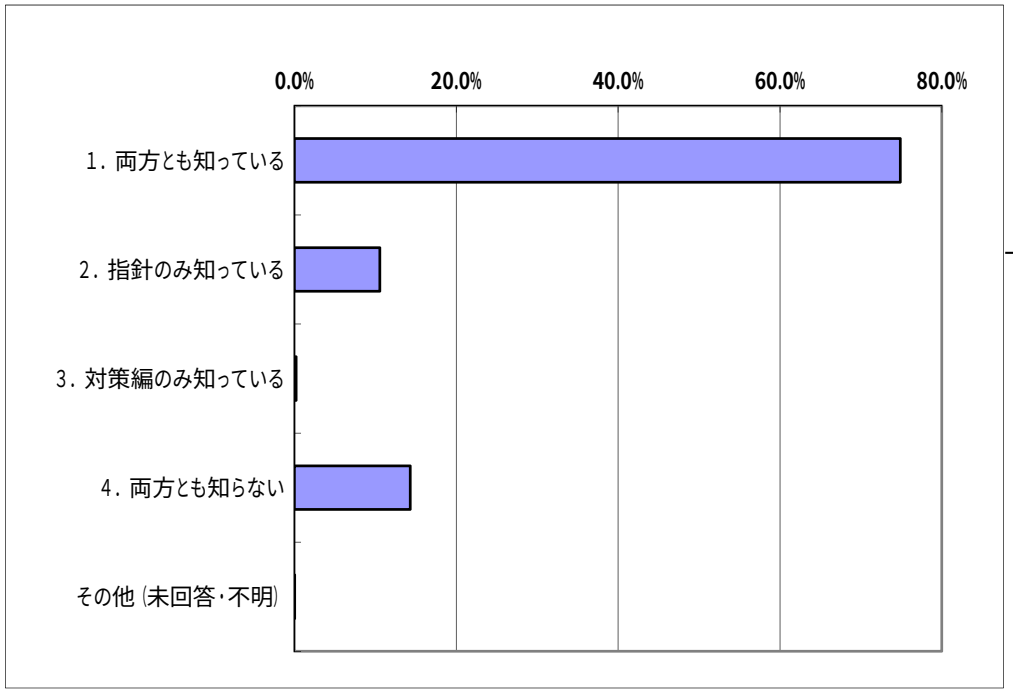
分野		既存調査				浸透状況等調査		
		有無	名称	調査基準日	調査周期	既存調査活用	調査対象範囲 ※既存調査活用する場合は、既存調査の範囲・数	ｱﾝｹｰﾄ配布数
情報通信	電気通信	なし				しない	固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等	76
情報通信	ケーブルテレビ	なし				しない	ケーブルテレビセプター参加事業者	241
情報通信	放送	なし				しない	日本放送協会及び地上系民間基幹放送事業者（多重単営社及びｺﾐｭﾆﾃｨ放送事業者を除く）	194
金融		あり	金融機関等のコンピュータシステムに関する安全対策実施状況調査書	3月31日	1年毎	する	金融機関等	892
航空	航空運送	なし				しない	航空運送事業者	2
航空	航空管制	なし				しない	官庁	1
鉄道		なし				しない	鉄道事業者２２社	22
電力		なし				しない	一般電気事業者、日本原電(株)、電源開発(株)	12
ガス		なし				しない	政令指定都市８社、同等の事業者２社	10
政府・行政サービス		あり	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	する	地方公共団体	1,789
医療		なし				しない	医療機関（病院抽出）	50
水道		なし				しない	水道事業体（事業者抽出）	45
物流		なし				しない	物流事業者及び業界団体	22

※既存調査の活用項目は、主な調査内容の①安全基準等の整備状況に係る事項、②情報セキュリティ対策状況に係る事項、③安全基準等への準拠状況に係る事項、が対象

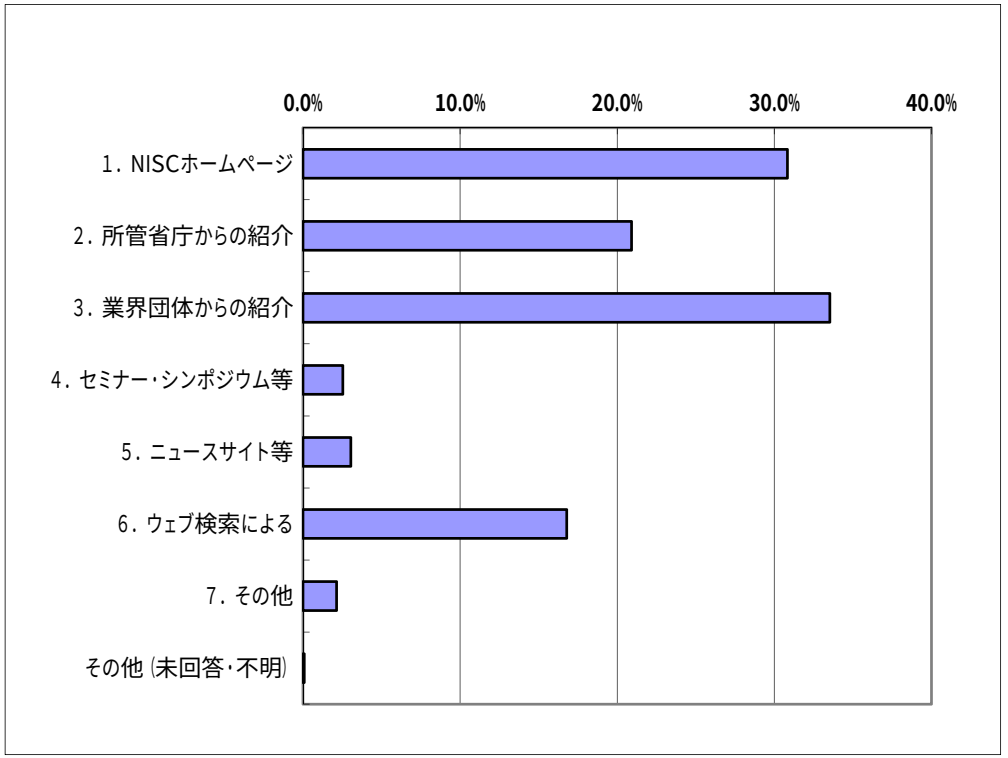
調査結果　①安全基準等の整備の状況に関する事項 (1/3)

・ 指針について、認知している事業者等は8割強であると推定。
・ 指針・対策編を認知している事業者のうち、それらを知った手段は、業界団体からの紹介が一番多く、NISCホームページ、所管省庁からの紹介が続く。

(1)指針・対策編の認知度
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



(2)指針・対策編を知った手段
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



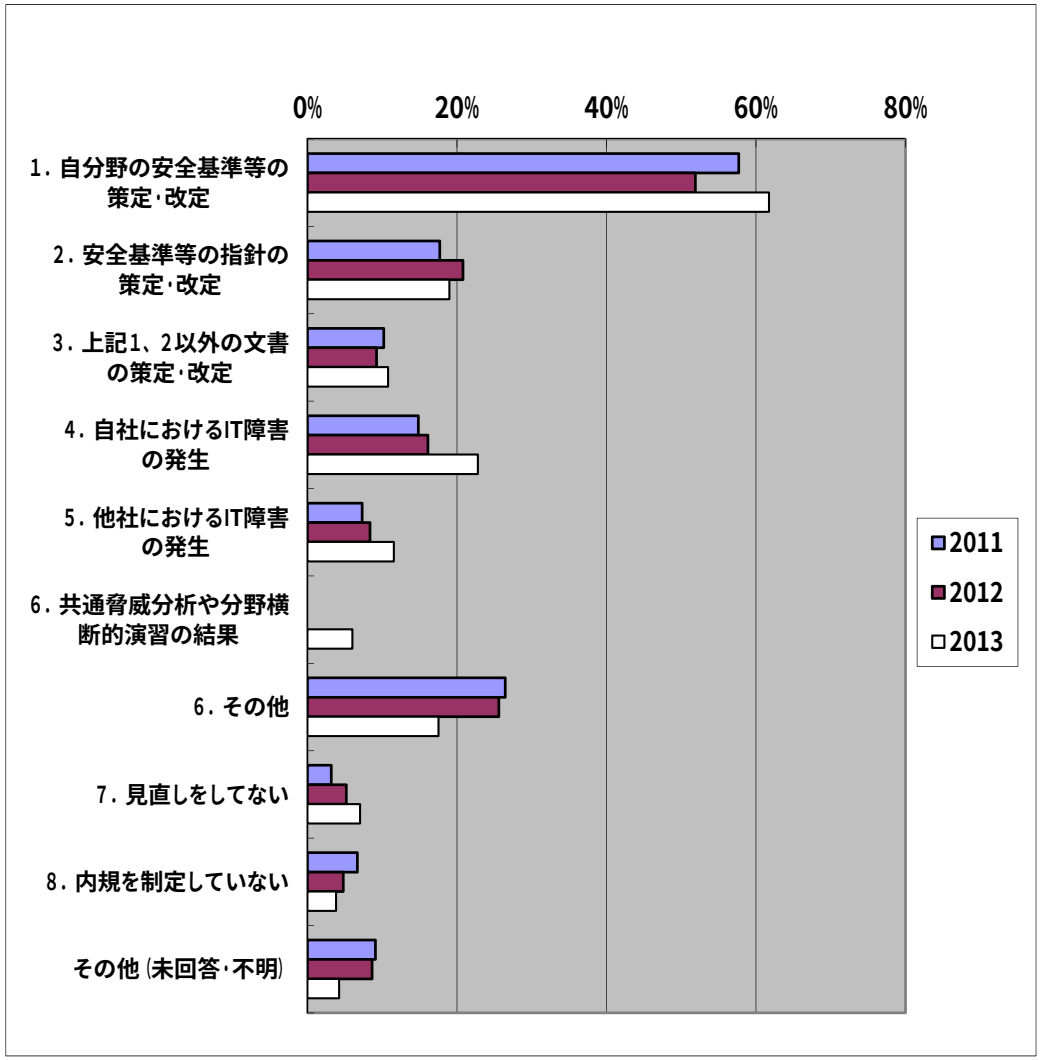
3)効果的に周知する手段
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

- 業界団体からの定期的な紹介
- 所管省庁からの情報提供
- 担当者宛メール通知
- セミナーやシンポジウムの開催
- マスメディアを通じた広報

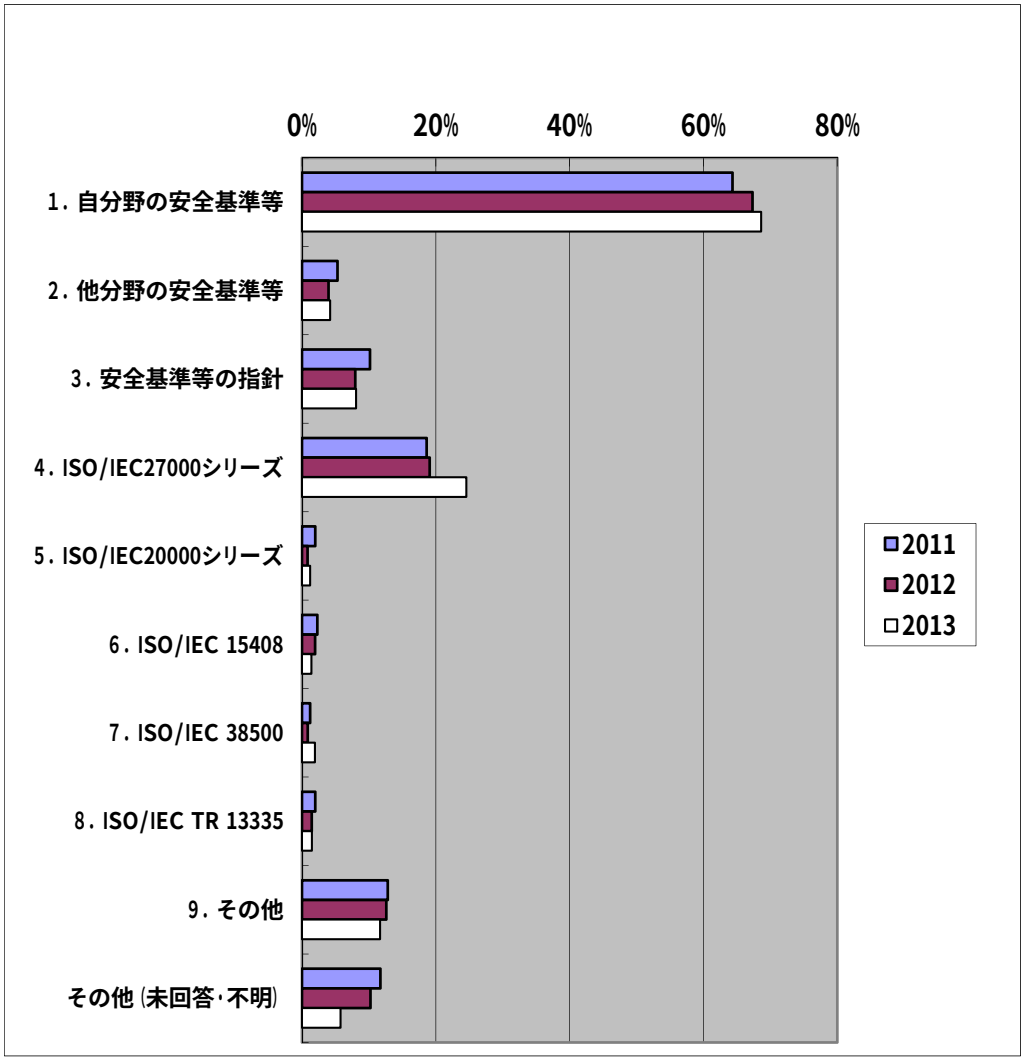
調査結果　①安全基準等の整備の状況に関する事項 (2/3)

- 内規策定・見直しの契機としては、自分野の安全基準等が約6割を占める。
- 参考とする安全基準、規格等も、自分野の安全基準等が約7割を占める。

(1) **内規策定・見直しの契機**



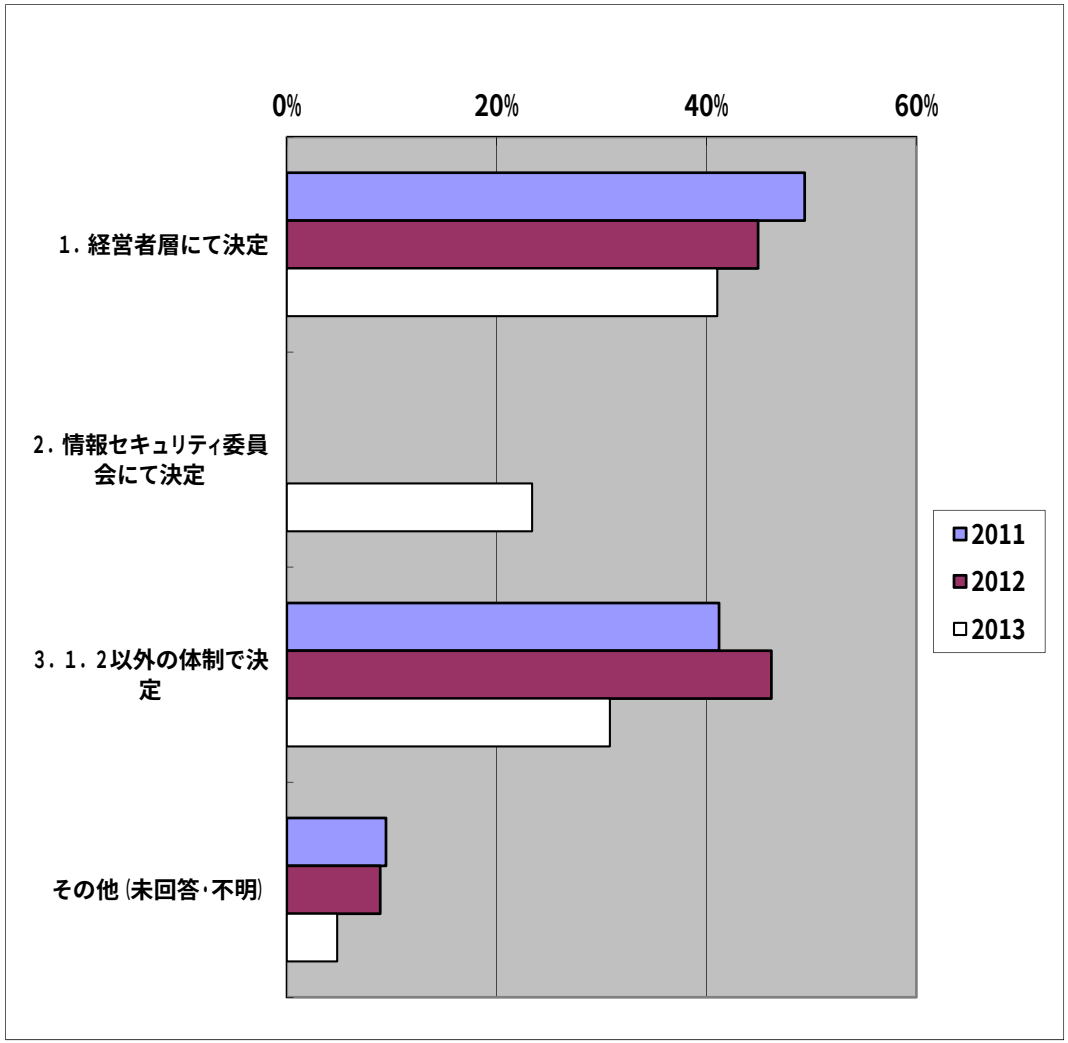
(2) **内規策定・見直しにあたり参考とする安全基準、規格等**



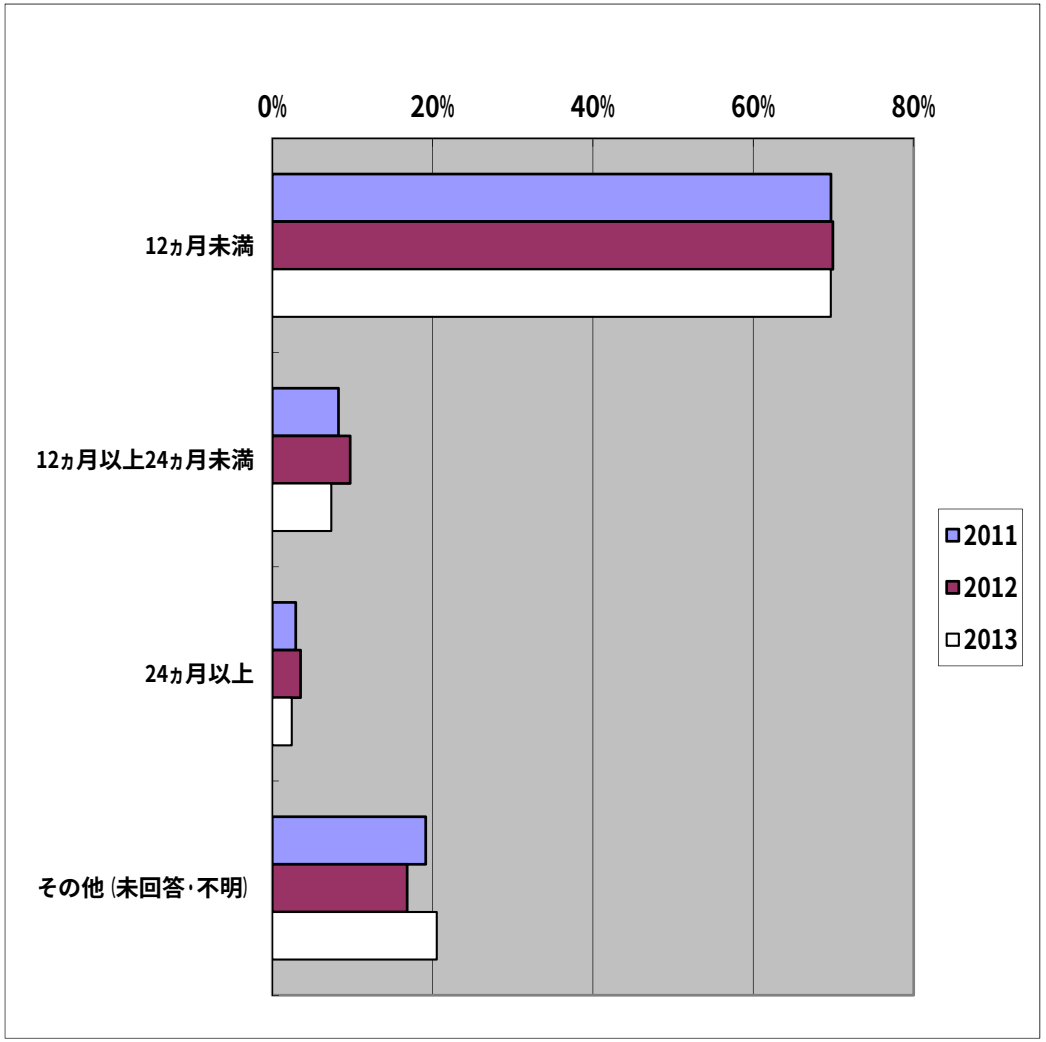
調査結果　①安全基準等の整備の状況に関する事項 (3/3)

- 内規改定を行う際の体制は、経営者層での決定が減少し、経営者層以外の体制での決定が増加。
  経営者層以外の体制での決定は、情報セキュリティ委員会によるものが大半。
- 内規の改定は、概ね１年未満で実施されている。

(3) **内規改定を行う際の体制**
項目２は2013年度に追加



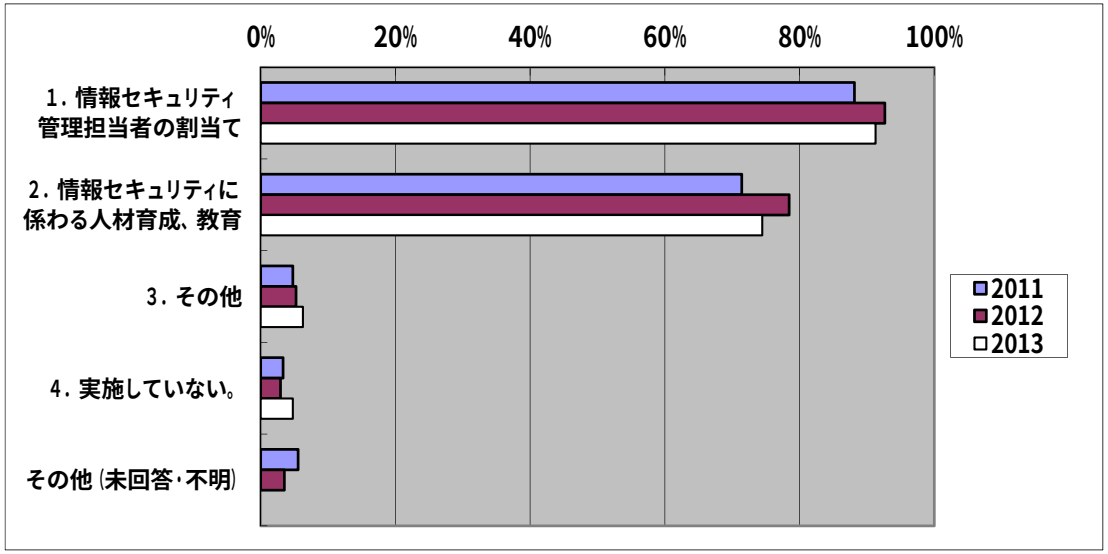
(4) **内規改定に要する期間**
金融は読み替え可能項目なし（集計対象に含めず）



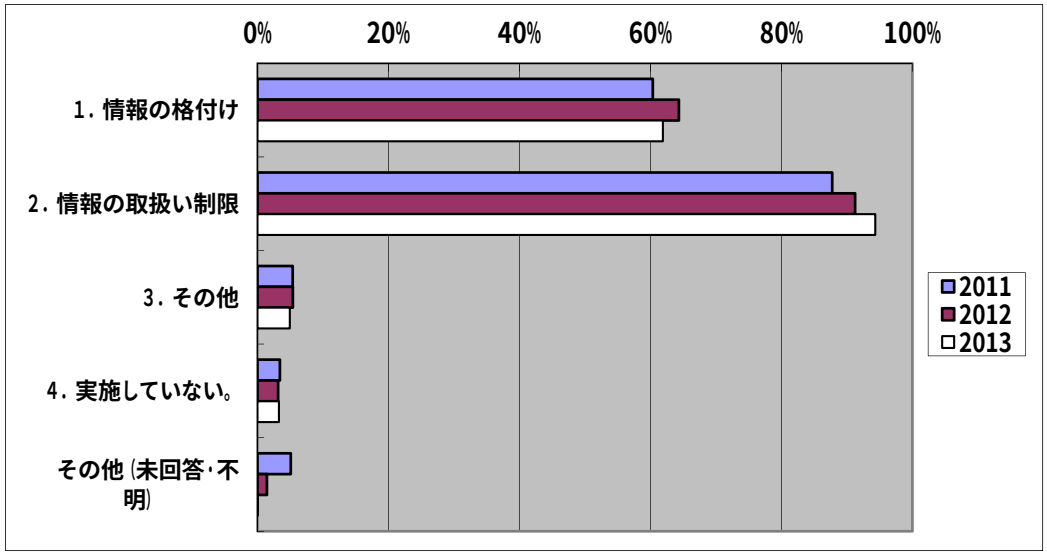
調査結果　②情報セキュリティ対策の実施状況に関する事項 (1/4)

- 今回からケーブルセプターが新たに調査対象となった。
- 経年変化（除、ケーブルセプター回答）については、(1) - (4)の各対策状況とも、ほぼ昨年度と同様の結果。

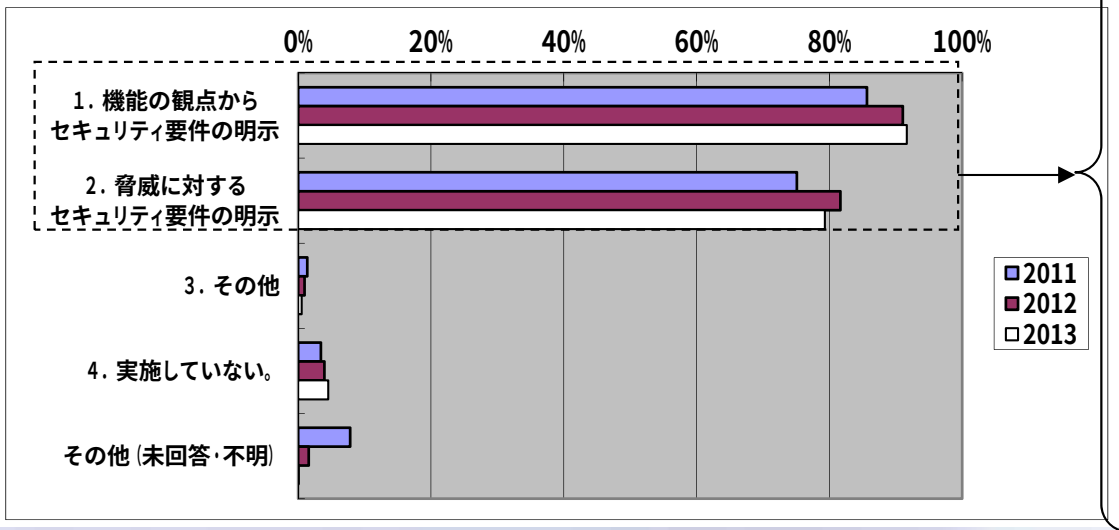
(1) 組織・体制及び資源の確保に関する対策



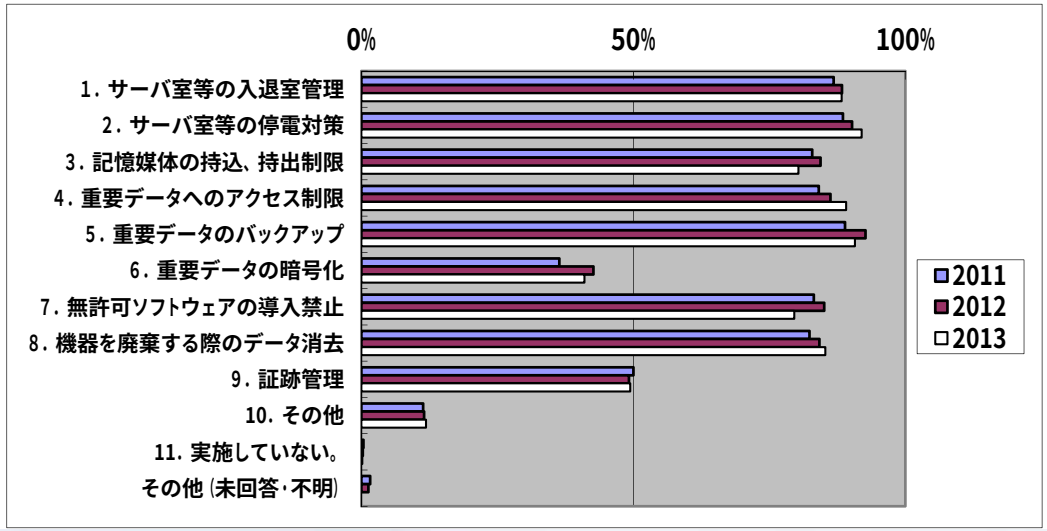
(2) 情報についての対策



(3) 情報セキュリティ要件の明確化
政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



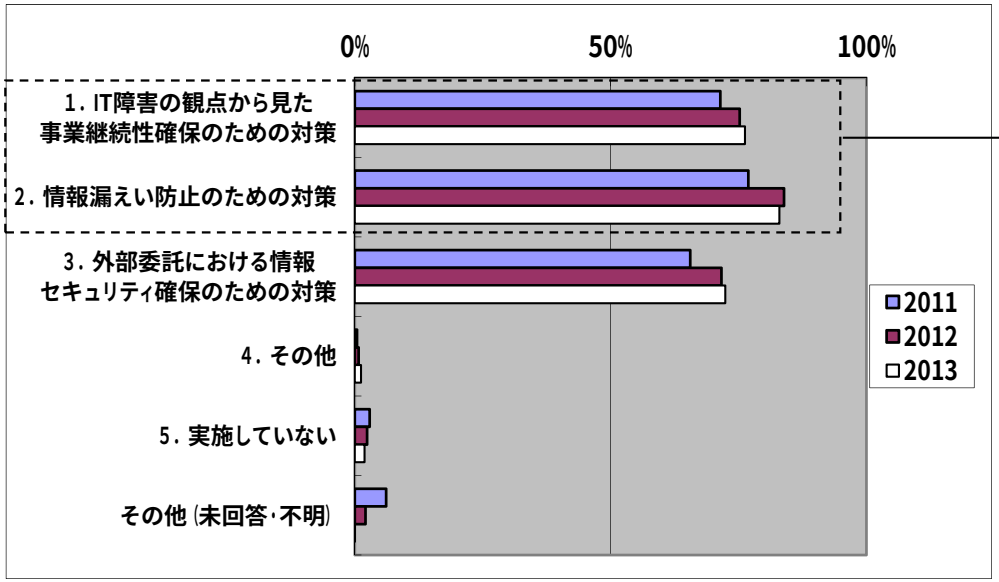
(4) 情報セキュリティ要件に対応した情報システムの対策



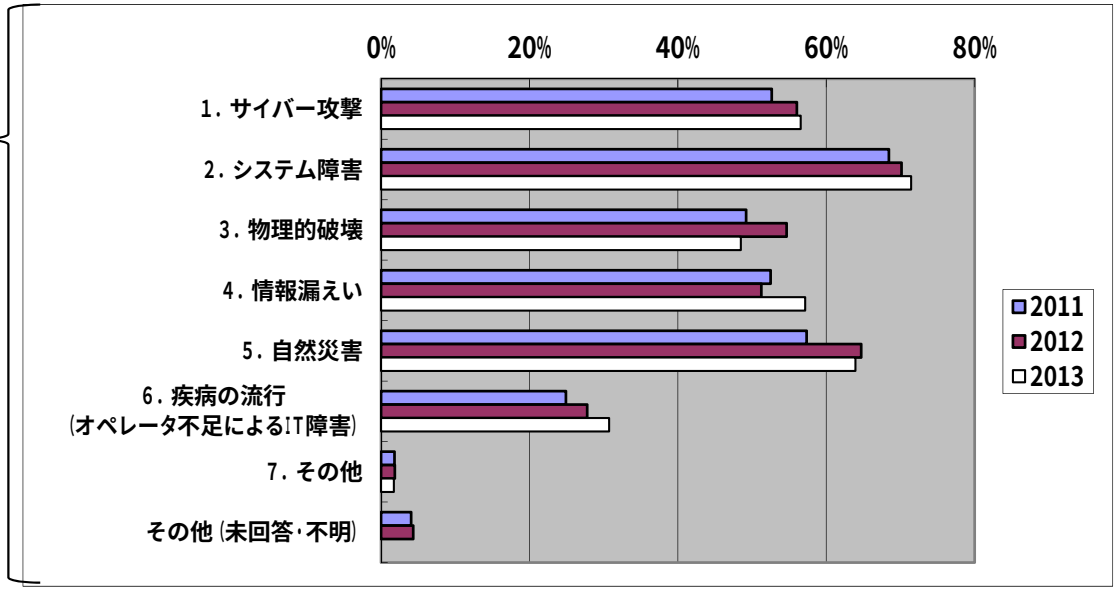
調査結果　②情報セキュリティ対策の実施状況に関する事項 (2/4)

- (5)-(6)の各対策状況とも、ほぼ昨年度と同様の結果。
- 事業継続計画の策定状況については、策定予定なしが暫時減少傾向にあり、策定予定を含めて策定が進んでいる傾向にある。一方、策定済みであるものの定期的な見直しについては減少した。

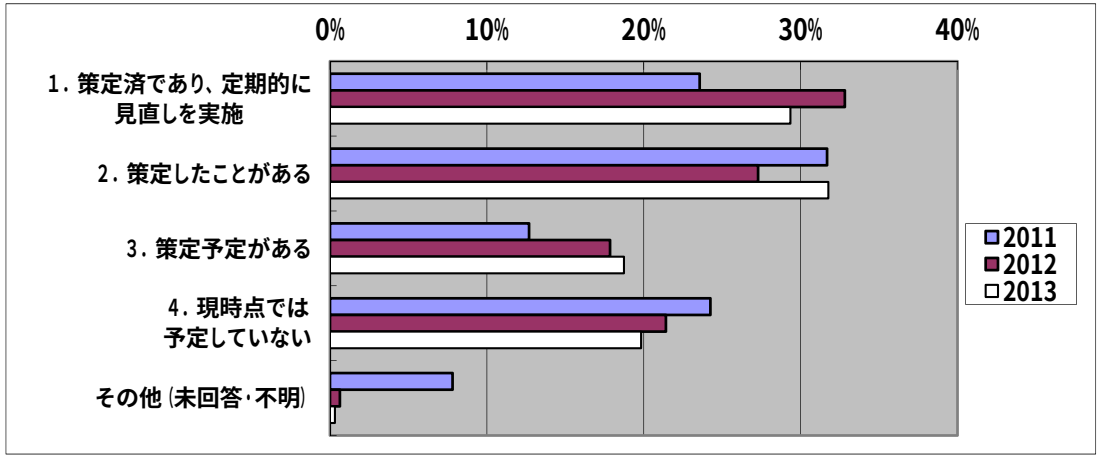
(5) 情報セキュリティ対策の運用に関する対策



(6)運用に関する情報セキュリティ対策において対象とする脅威



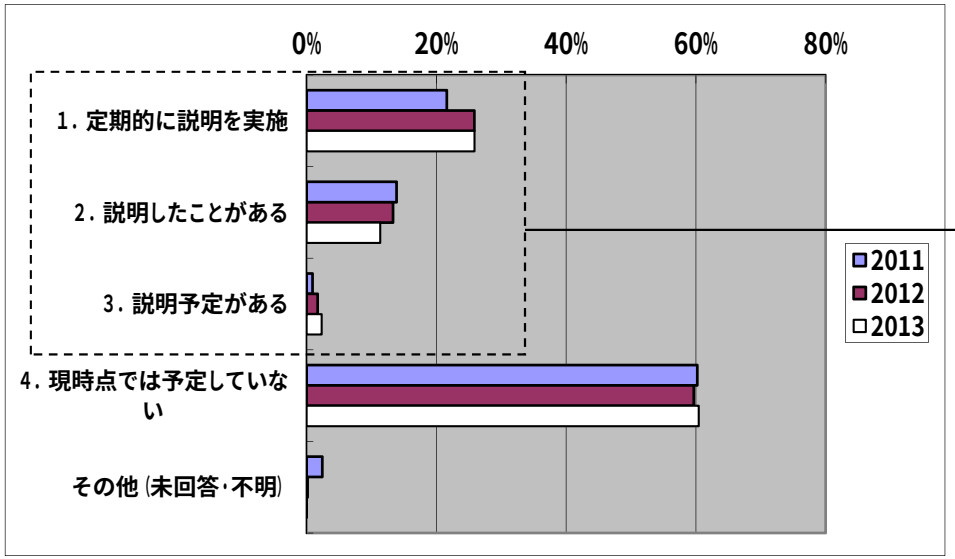
(7) 事業継続計画の策定状況



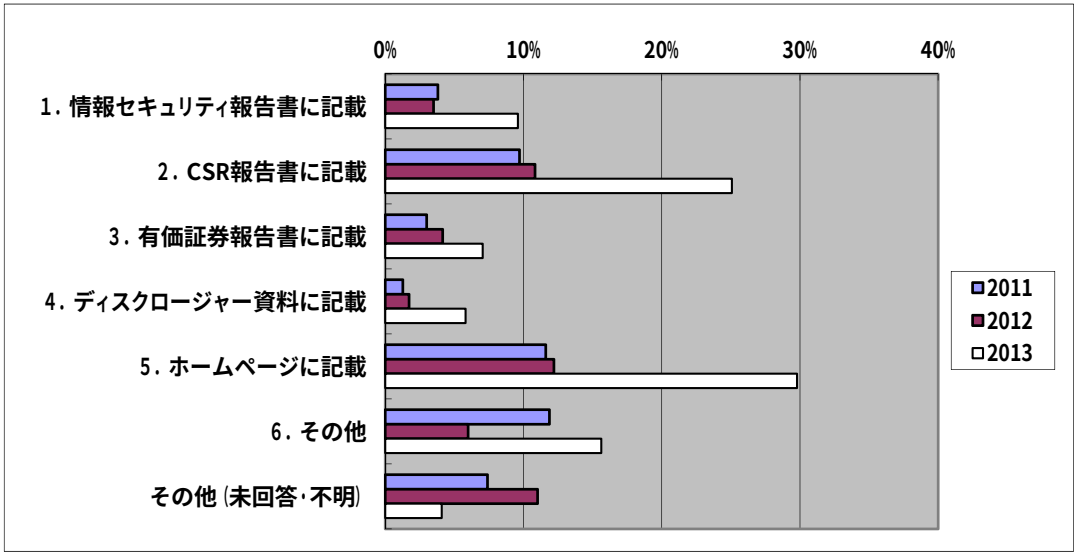
調査結果　②情報セキュリティ対策の実施状況に関する事項 (3/4)

- 情報セキュリティ対策の対外的な説明を定期的に実施している事業者等は昨年度同様約３割。また、説明方法については、ホームページ、ＣＳＲ報告書を用いている事業者等が多い。
- 昨年度同様6割強の事業者等で、IT障害時の情報提供に関する方策を内規等に明示している。

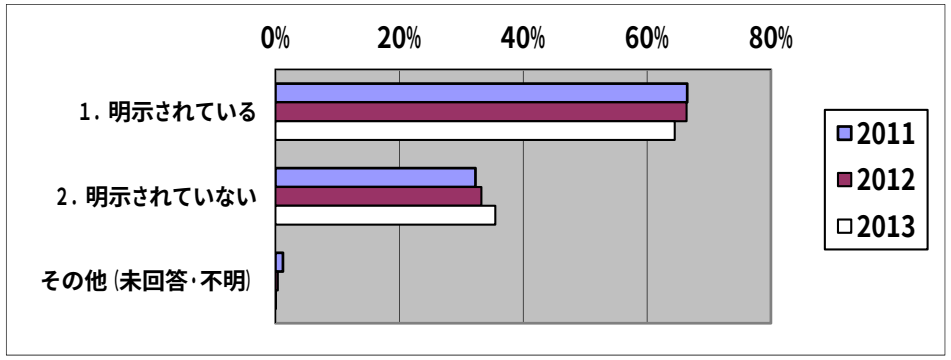
(8) 情報セキュリティ対策の対外的な説明の状況
政府･行政サービスは 読み替え可能項目なし (集計対象に含めず)



(9) 情報セキュリティ対策の対外的な説明の方法
金融、政府･行政サービスは 読み替え可能項目なし (集計対象に含めず)



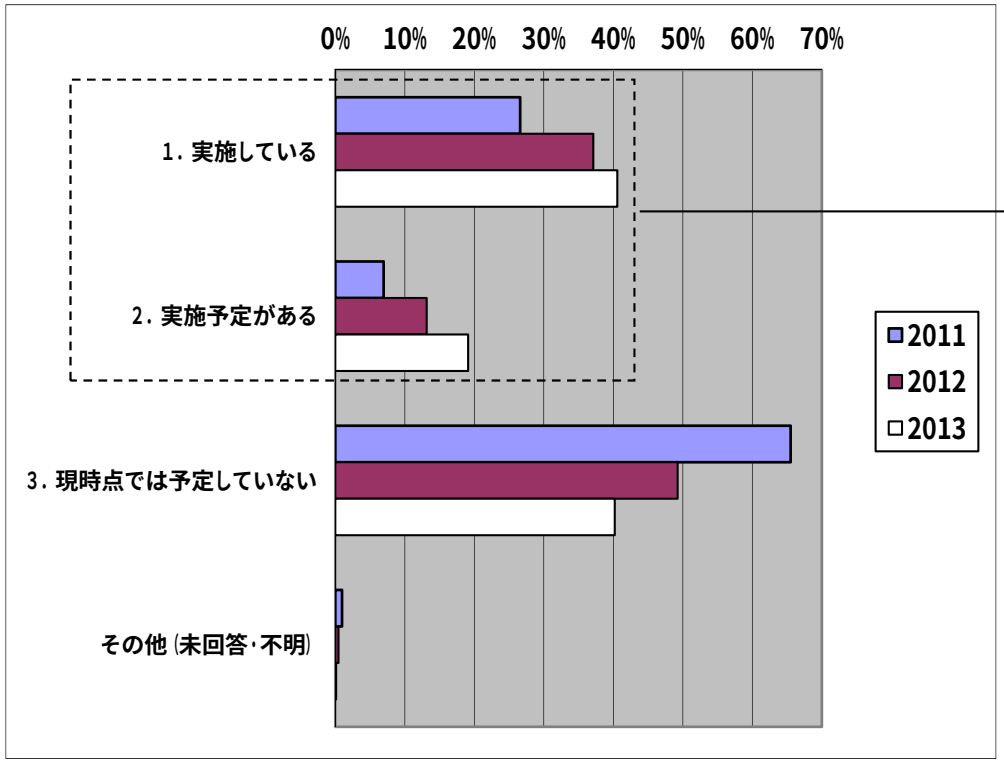
(10) IT障害時のユーザへの情報提供の方策
金融、政府･行政サービスは 読み替え可能項目なし (集計対象に含めず)



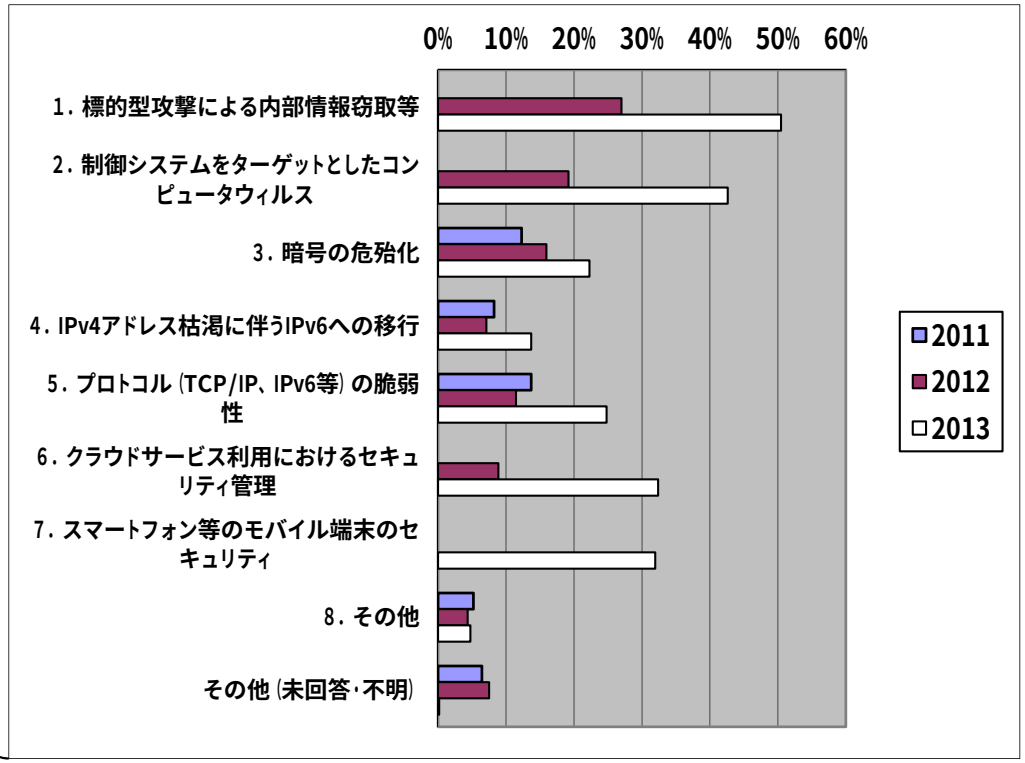
調査結果　②情報セキュリティ対策の実施状況に関する事項 (4/4)

- ITに係る環境変化に伴う脅威に対して、対策を実施、または予定している事業者等は昨年度同様、6割程度と推定。
- 想定する脅威に関しては、標的型攻撃による内部情報窃取等、制御システムをターゲットとしたコンピュータウィルスが引き続き上位。続いてクラウドサービス利用におけるセキュリティ管理、スマートフォン等のモバイル端末のセキュリティといった新技術の脅威想定が伸長。

(11) ITに係る環境変化に伴う脅威に対する対策
政府・行政サービスは 読み替え可能項目なし (集計対象に含めず)



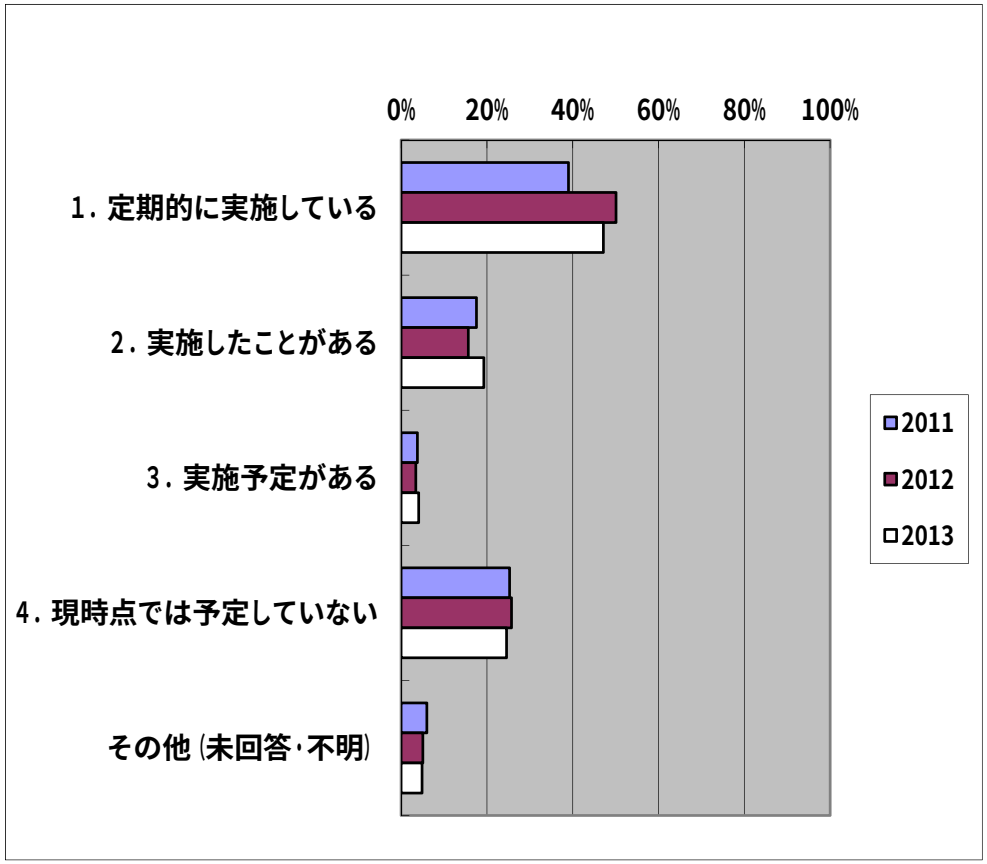
(12) 想定する脅威
政府・行政サービスは 読み替え可能項目なし (集計対象に含めず)
※項目1、2、6は2012年度に、7は2013年度に追加



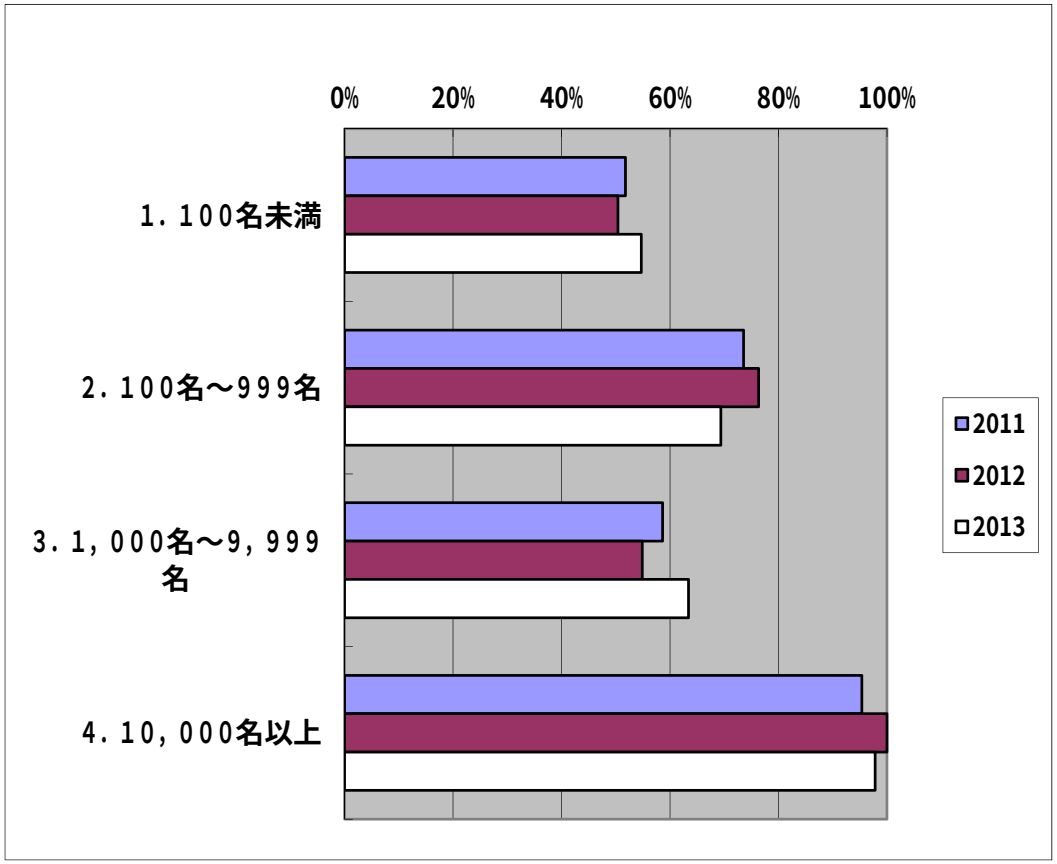
調査結果　③安全基準等に対する準拠状況に関する事項 (1/4)

・ 昨年度同様、自己点検を定期的に実施している事業者等が約５割、予定を含む実施割合が約７割と推定。

(1) 自己点検の実施



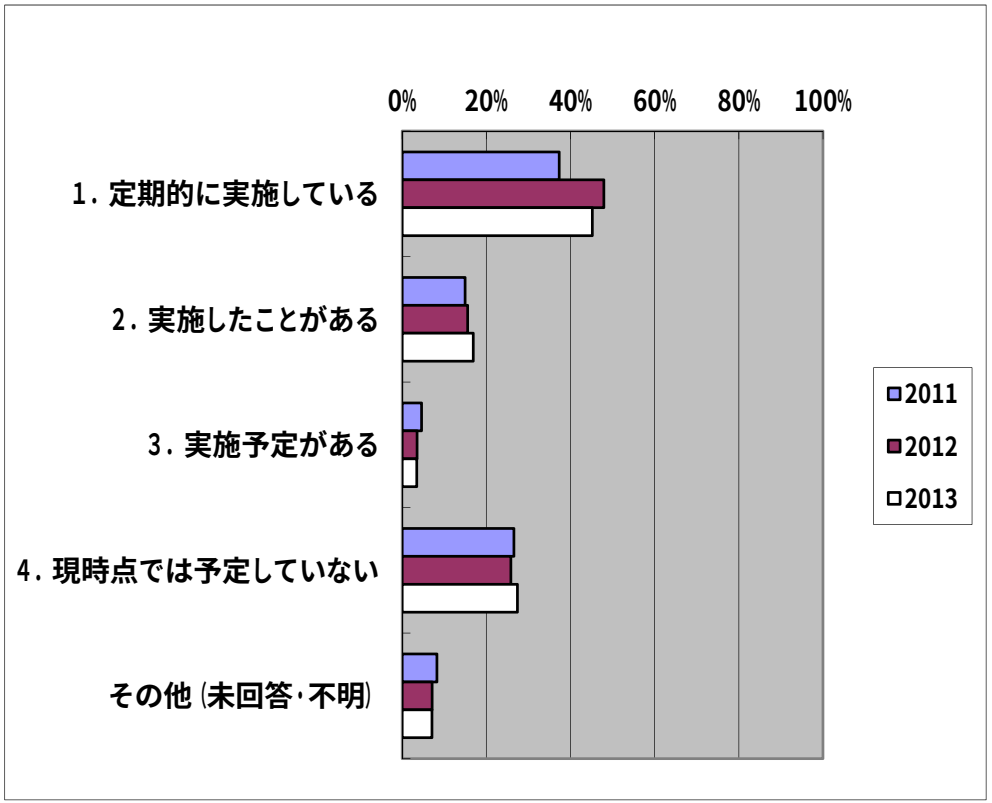
自己点検の事業規模ごとの実施割合（予定含む）



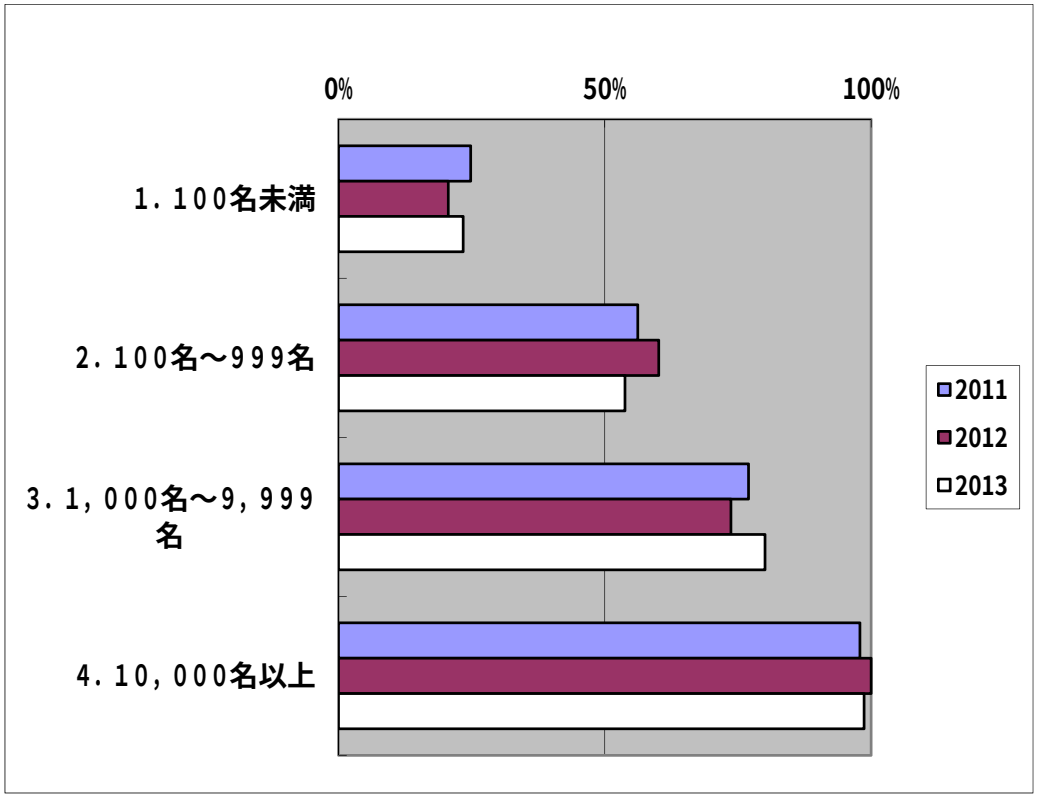
調査結果　③安全基準等に対する準拠状況に関する事項 (2/4)

・ 演習・訓練の実施状況については、総じてほぼ昨年度水準。

(2)演習・訓練の実施



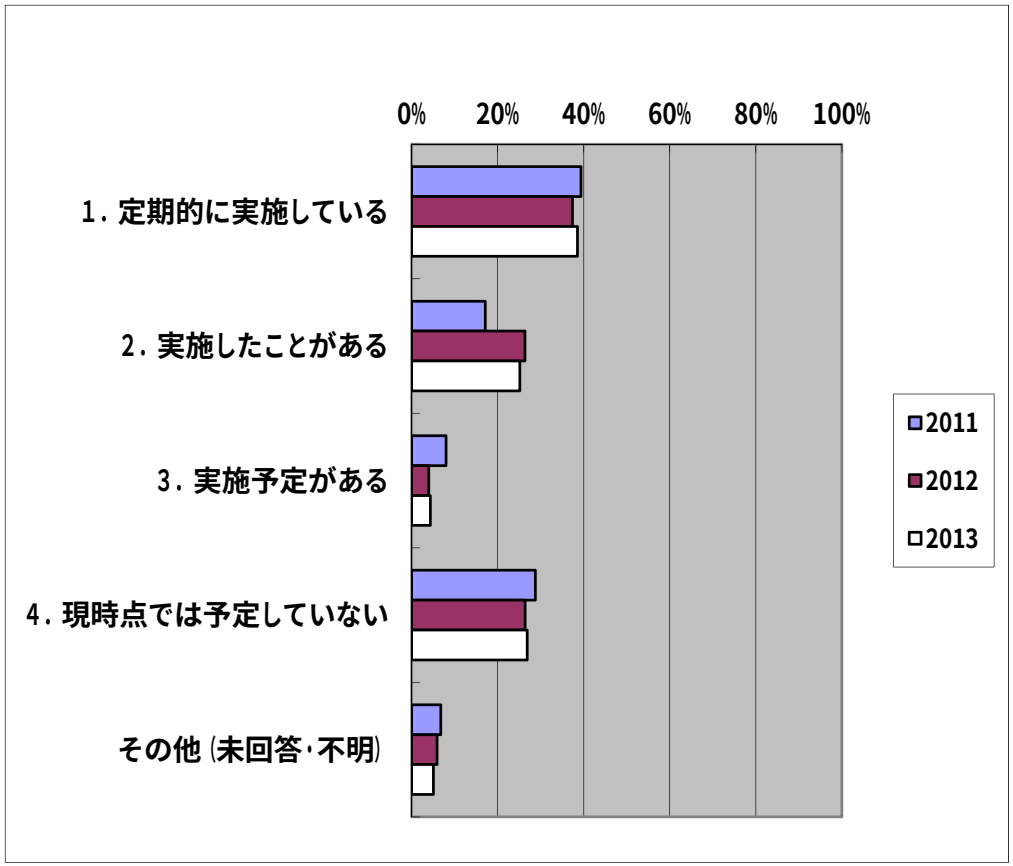
演習・訓練の事業規模ごとの実施割合 (予定含む)



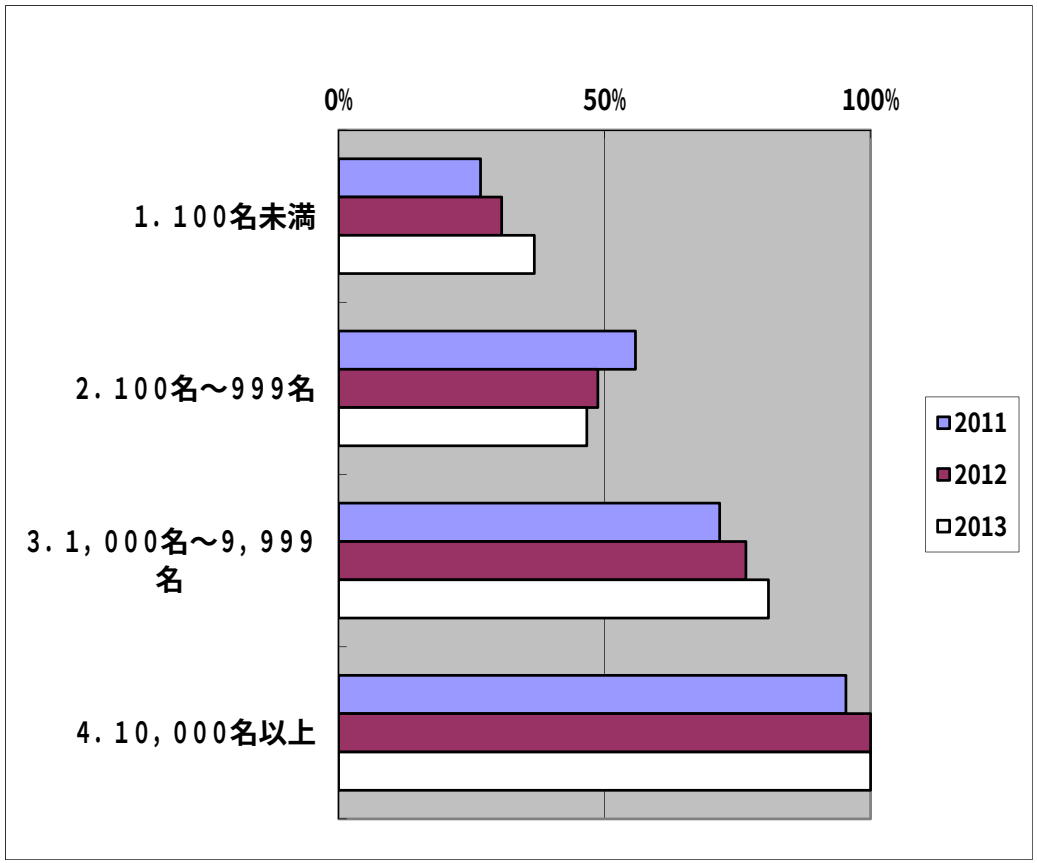
調査結果　③安全基準等に対する準拠状況に関する事項 (3/4)

・ 内部監査の実施状況については、総じてほぼ昨年度水準。

(3) 内部監査の実施



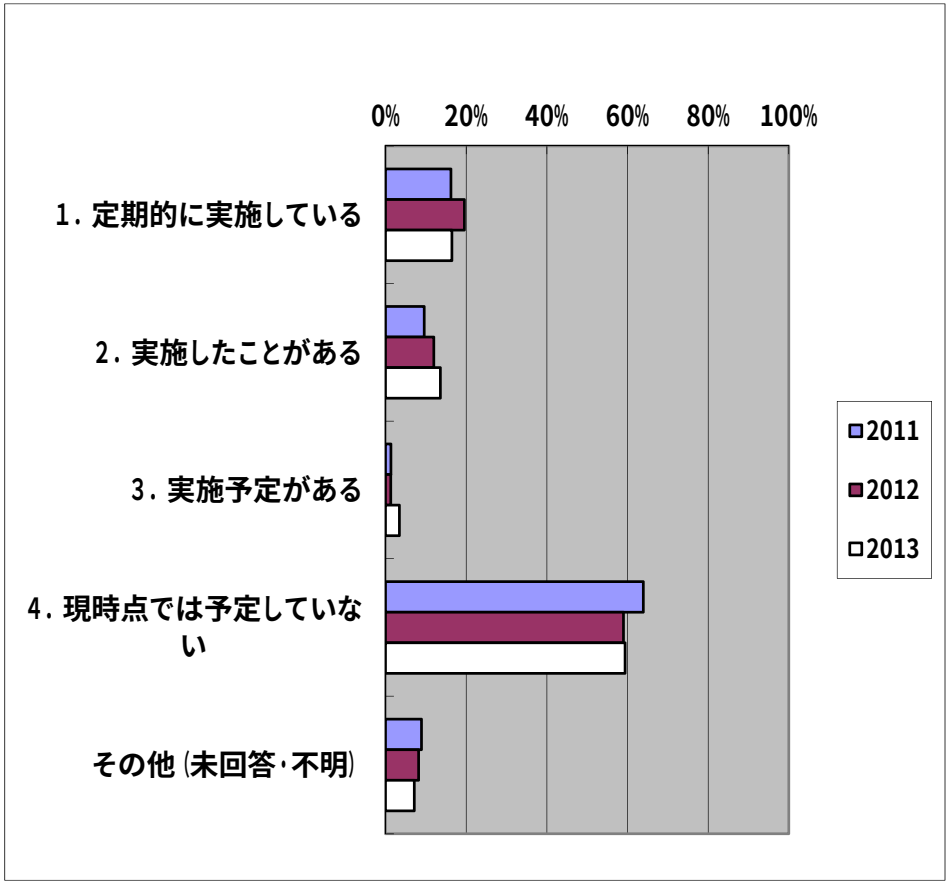
内部監査の事業規模ごとの実施割合（予定含む）



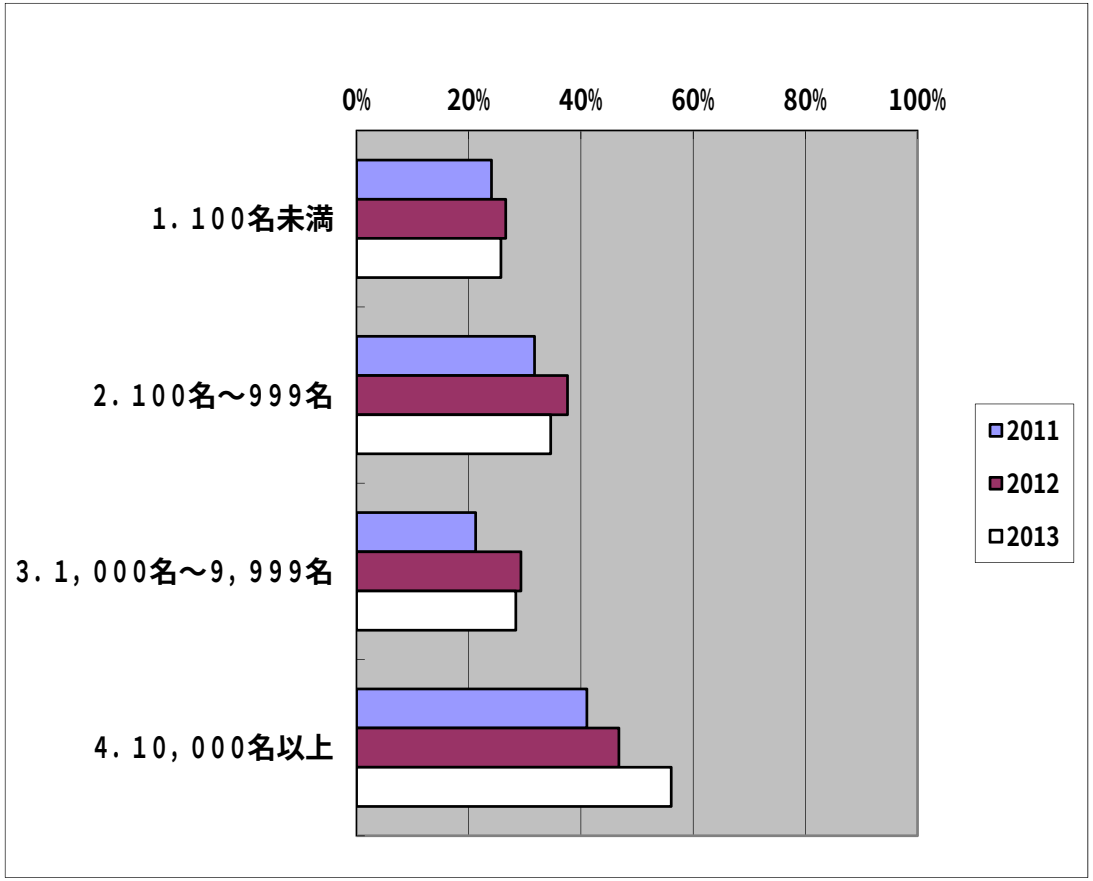
調査結果　③安全基準等に対する準拠状況に関する事項 (4/4)

- 外部監査の実施状況については、総じてほぼ昨年度水準。
- 費用のかかる外部の監査機関の利用は大規模事業者では増加傾向だが、他事業者ではやや微減。

(4) 外部監査の実施
金融は読み替え可能項目なし（集計対象に含めず）



外部監査の事業規模ごとの実施割合（予定含む）



調査結果　④安全基準等への提言、要望等 (1/2)

・ 安全基準等の指針に対する意見としては、対策の段階化（最低限必要なレベル、望ましいレベル、理想レベル）等による企業規模に見合った指針化、取り組み易い具体策の提示等、より実効性を求める要望があった。

・ 安全基準等に対する意見としては、事例提供・分野内共通の留意点の提示・セミナー開催等の情報提供、事業者としての必要最低限の対応の担保に向けた法制化を視野に見直しを進めることの検討着手について意見があった。

1．安全基準等の指針に対して

① 最低限必要な対策、望ましい対策、理想とする対策など段階的な指針にするとわかりやすい
② 情報セキュリティ政策会議で策定している指針や対策編は参考になるが、次元がハイレベルのように感じる
③ 対策編で更なる具体的な内容を示してほしい
④ チェックシートなどがあるとさらに有意義になるのではないか

2．安全基準等に対して

① ガイドライン適用の参考としたく、出来るだけ多くの事例を提供いただきたい
② 内規案があるとより理解、対策が可能となる
③ 一般論ではなく、規模・コスト別の対策例を提示いただきたい
④ 必要最低限にすべき。過度に基準を設定しても、実行できなければ意味を呈さない
⑤ 安全基準等は参考するも、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
⑥ 日々発見される脅威への対応が充分なのか不安な面が多々ある。多くの安全基準等のセミナー開催を希望
⑦ 営利企業においては、情報セキュリティの重要性は理解できても、それに要するコストは常にメリットとの見合い。
その意味で政府等が示すガイドラインは、強制力がなく、状況に応じた事業者判断を可能としている形態は適切と考えられる。
一方で昨今の情報セキュリティを巡る情勢から、各事業者が足並みをそろえた対応すべき点も生じることが想定される。事業者の必要最低限な対応の担保に向け、法制化も視野に対策見直しを進めることも要検討だと考えられる

※金融、政府・行政サービスは、調査対象外

調査結果　④安全基準等への提言、要望等 (2/2)

・ 自由意見としては、IT人材育成支援・情報セキュリティ相談窓口、セキュリティ対策費用の助成等の支援、政府レベルでのＯＳ不具合・ウイルスソフト等の情報公開・対策、セキュリティ対策の一定水準の義務付け、サイバーテロ等に対する取り締まりと法的措置の強化といった意見があった。

3．その他（自由意見を記載）

① IT人材育成のための支援を重視して頂きたい
② 情報セキュリティの相談窓口の設置をお願いしたい
③ 対策実施には多額の設備投資を要する箇所もある。支援して頂けるような枠組みがあれば助かる
④ 情報セキュリティに関して、一定の水準を保つよう義務付けるとともに、セキュリティ費用等における助成の検討をお願いしたい
⑤ セキュリティ全般に対するＯＳの不具合、ウイルスソフト等を政府として迅速に公開してほしい
⑥ 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ある。真の脅威を未然に防ぐためにも国の研究機関等が、重要なコンピュータウイルス対策を行うべきではないか
⑦ サイバーテロ、不正アクセス、ウイルス散布、スパムメール等に対する取り締まりと法的措置の強化を実施して頂きたい

※金融、政府・行政サービスは、調査対象外

まとめ

・ 重要インフラ事業者等における情報セキュリティ対策の実施状況を分野横断的に把握

- **回答選択の傾向は総じて昨年とほぼ同様であった。また、回収率は９４．１％（対前年度＋０．９％）であった。**
- **想定する脅威として、「クラウドサービス利用におけるセキュリティ管理」、「スマートフォン等のモバイル端末のセキュリティ」といった環境変化を挙げる事業者が増加している。**
- **一部項目において見られた対策状況の率の減少（対前年比）については回答者の追加・入替え等に起因するものであり、追加・入替え等を除く対策状況については横ばいから微増であった。**
  このことから、現調査対象範囲における安全基準等の対策状況は、対策途上期から成熟期に移行しつつあることが推定される。

≪さらなる情報セキュリティ対策の拡充に向けて≫

- **環境変化、とりわけ新技術に係る重要インフラ事業者等によるリスク分析への支援について検討を要する。**
- **現調査対象範囲からの対象拡張及び具体的な対策状況確認を通じて、本調査結果（特に課題）を国の施策にフィードバックする機能の実現に向けた検討を要する。**

- **今後の重要インフラ事業者等における情報セキュリティ対策の実施状況の把握については、本調査による以下の実現を目指し、一部調査運営を見直した上で継続して実施する。**
  - ✓ **調査対象範囲の拡張にて、より広範な重要インフラ全体の状況確認**
  - ✓ **より具体的な対策状況の確認を通じたより深化した課題抽出**
  - ✓ **成熟期への移行推定に基づく率の減少（対策退化傾向）の検知**

＜参考＞　アンケート項目

・ 以下のアンケート項目にて調査を実施（「NISCアンケート項目に準じて実施」の場合）
・ 「既存調査を活用」する場合は、全体集計に際して、可能な範囲でアンケート項目との読み替えを実施

【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。

【① 安全基準等の整備の状況に関する事項】
（1） 指針及び対策編をご存知ですか。
（2） 指針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。
（4） 内規の策定・見直しの契機を以下からお知らせ下さい。
（5） 参考とする安全基準等や諸規格をお知らせ下さい。
（6） 内規改定を行う際の体制をお知らせ下さい。
（7） 内規改定に要する大体の期間をお知らせ下さい。

【② 情報セキュリティ対策の実施状況に関する事項】
（1） 組織・体制及び資源の確保に関する対策を実施していますか。
（2） 情報についての対策を実施していますか。
（3） 情報セキュリティ要件の明確化を実施していますか。
（4） 明確化した情報セキュリティ要件に対応した情報システムの対策を実施していますか。
（5） 情報セキュリティ対策の運用に関する対策を実施していますか。
（6） 事業継続計画の策定状況をお知らせ下さい。
（7） 事業継続計画の対象とする脅威をお知らせ下さい。
（8） 貴社（又は貴団体）における情報セキュリティ対策の対外的な説明状況をお知らせ下さい。
（9） 情報セキュリティ対策の対外的な説明の方法をお知らせ下さい。
（10）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、復旧等の情報提供の方策が明示されていますか。
（11）環境変化に伴う脅威に対する対策を実施していますか。
（12）対象とする脅威をお知らせ下さい。

【③ 安全基準等に対する準拠状況に関する事項】
（1） 安全基準等や貴社（又は貴団体）の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っていますか（予定を含む）。
（2） IT障害発生を想定した演習、訓練等を実施していますか（予定を含む）。
（3） 情報セキュリティ対策の実施状況に関する内部監査を実施していますか（予定を含む）。
（4） 情報セキュリティ対策の実施状況に関する外部監査を実施していますか（予定を含む）。

【④ 政府への提言、要望等】
（1） 安全基準等の指針に対して（自由意見を記載）
（2） 安全基準等に対して（自由意見を記載）
（3） その他（自由意見を記載）