NISC National Information Security Center

2010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

2011年 6月

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「情報セキュリティ2010」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、**毎年一定時期の定点調査として**、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、定期的に本調査を実施し、継続的に浸透状況等の把握を行い、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

- 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）

浸透状況等調査（SJ2007）

2006年度に策定・見直しを行った安全基準等を対象

第2次行動計画における取組み

- 安全基準等の継続的改善（SJ2009）
- 「安全基準等」の整備浸透状況調査（SJ2010）
- 安全基準等の継続的改善

浸透状況等調査（SJ2008～SJ2009）

浸透状況等調査（SJ2010）

浸透状況等調査

毎年一定時期に定点調査

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。

情報セキュリティ2010

・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〉

2010 年度当初に「安全基準等」の浸透状況等に関する調査を実施し、結果を公表する。

また次年度の調査のための企画・準備を実施する。

「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	：	調査対象とする事業者等の範囲は重要インフラ所管省庁が決定
調査方法	：	以下いずれかを重要インフラ所管省庁が選択 ①既存調査を活用 ②NISC案に準じて実施
調査基準日	：	2010年3月末日（「①既存調査を活用」の場合は、その調査基準日による）
アンケートの発出・回収	：	重要インフラ所管省庁が配布・回収（配布・回収方法は分野ごとに決定）
分野毎の集計	：	集計方法については、重要インフラ所管省庁が選択 ⅰ 重要インフラ所管省庁で集計 ⅱ NISCで集計
全体集計・とりまとめ	：	NISCが実施

◆実施時期 （②NISC案に準じて実施 の場合）

調査期間	：	2010年4月～2010年6月（集計は2010年7月まで）
とりまとめ	：	2010年9月

◆主な調査内容（NISC案）

①安全基準等の整備の状況に関する事項
- 指針見直し作業の認知度
- 策定・見直しの契機
- 参考とする安全基準等や諸規格

②情報セキュリティ対策の実施状況に関する事項
- 組織・体制及び資源の確保に関する対策
- 情報についての対策を実施

③安全基準等に対する準拠状況
- 自己点検の実施
- 演習、訓練等の実施

④政府への提言、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3,195事業者等に対し、2,956事業者等からアンケートを回収（回収率 92．5%、前年比-1.3%）
- 全体集計に際しては、単純集計では回収数の多い分野の影響が大きくなる等から、共通の重みづけで集計を実施

分野		既存調査活用	アンケート回収状況		
			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	34	31
	放送	しない	日本放送協会及び地上系一般放送事業者	195	149
金融		する	金融機関等	951	802
航空	航空運送	しない	航空運送事業者	2	2
	航空管制	しない	官庁	1	1
鉄道		しない	鉄道事業者22社	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
ガス		しない	政令指定都市8社、同等の事業者2社	10	10
政府・行政サービス		する	地方公共団体	1,847	1,847
医療		しない	医療機関（病院抽出）	50	27
水道		しない	水道事業体（事業者抽出）	49	45
物流		しない	物流事業者	22	8
全分野合計				3,195	2,956

留意点

留意点1：類似の調査との重複
⇒既存調査を活用することで調査を効率化

留意点2：調査対象の範囲
⇒調査可能な範囲から取り組み、調査対象の拡大は追って検討

（第23回重要インフラ専門委員会資料より）

上記に加え、単純集計では回収数の多い分野の全体集計への影響が大きくなることから、重要インフラ全体の状況把握をより適切に行うため、共通の重みづけで集計を実施

＜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、航空を2つに分けて集計するため、原則 n=12
（既存調査活用する場合に読み替え可能な項目がない場合を除く）

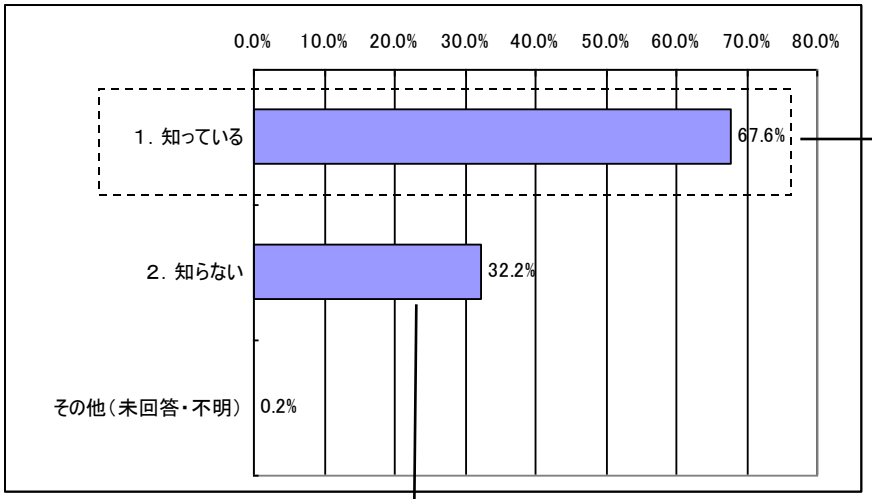
＜参考1＞既存調査と浸透状況等調査の関係整理（2010年度実績）

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	34
情報通信	放送	なし				しない	日本放送協会及び地上系一般放送事業者	195
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状況調査	3月31日	1年毎	する	金融機関等	951
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	地方公共団体における行政情報化の推進状況調査	4月1日	1年毎	する	地方公共団体	1,847
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）	49
物流		なし				しない	物流事業者	22

調査結果　①安全基準等の整備の状況に関する事項 (1/4)

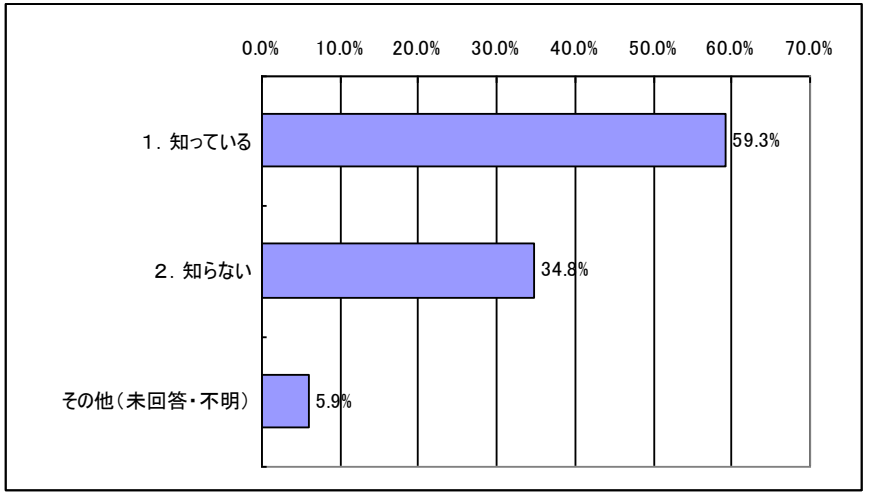
- 2010年5月に決定された指針の見直しについて、事前に認識している事業者等が7割弱であると推定
- 指針の見直しを認知している事業者のうち、指針見直しに伴う内規の見直しを、予定を含め行う事業者が3割程度あり、分野の安全基準等のほかに指針についても見直しの契機にする事業者が一定数あるものと推定。

(1)指針の見直し作業の認知度
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）

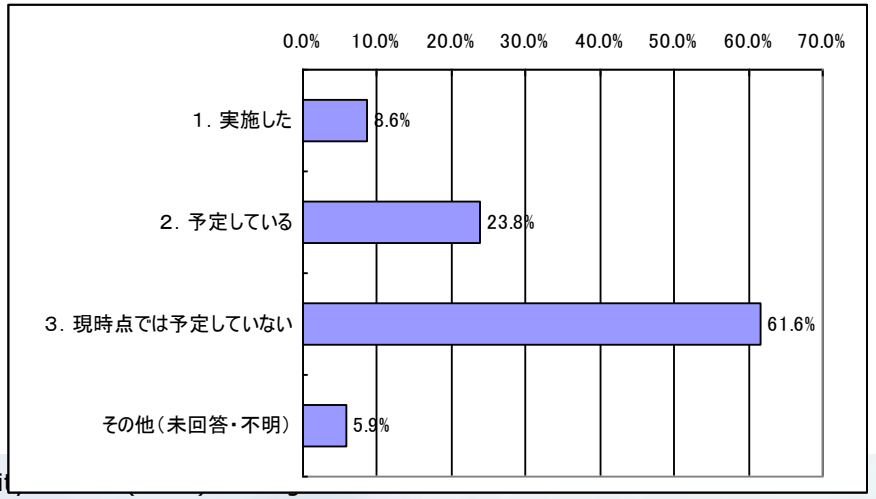


次ページ

(2)見直しの内容の認知度
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）



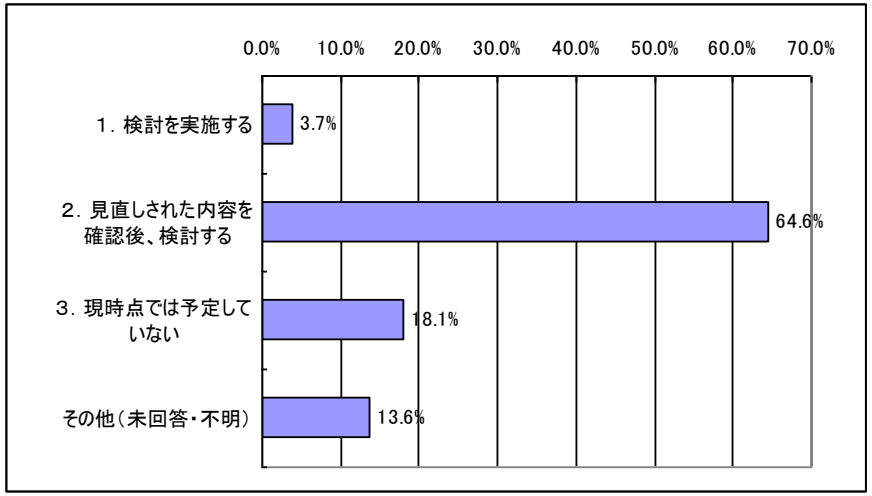
(3)指針見直しに伴う内規等の見直し準備
政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



調査結果　①安全基準等の整備の状況に関する事項 (2/4)

- **見直し作業を認知していない事業者のうち、内規等の見直しを予定していない事業者は（1）のデータと掛け合わせると全体の6％程度であり、分野の安全基準等が指針を参照していることが浸透してきているものと推定。**

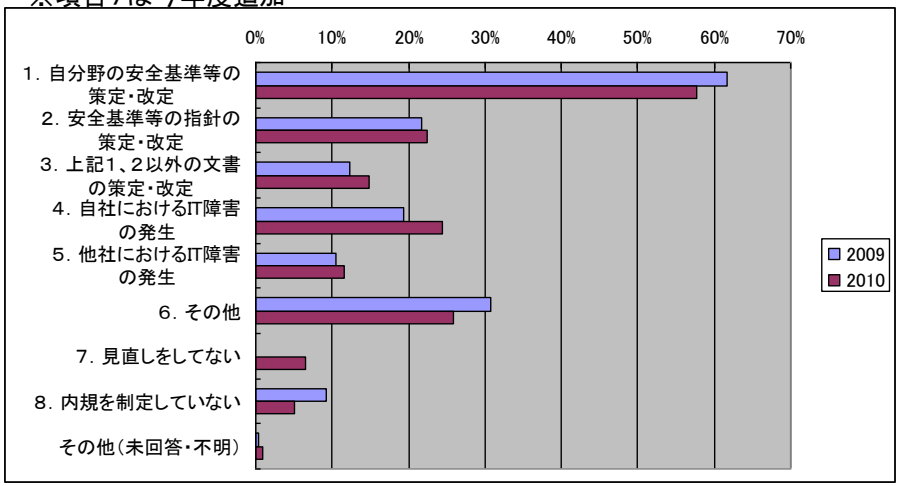
(4)指針見直しを知らない場合における指針改定時の内規等見直しの検討
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）
航空・電力・ガスは本質問に該当する選択が無かったため集計対象に含めず



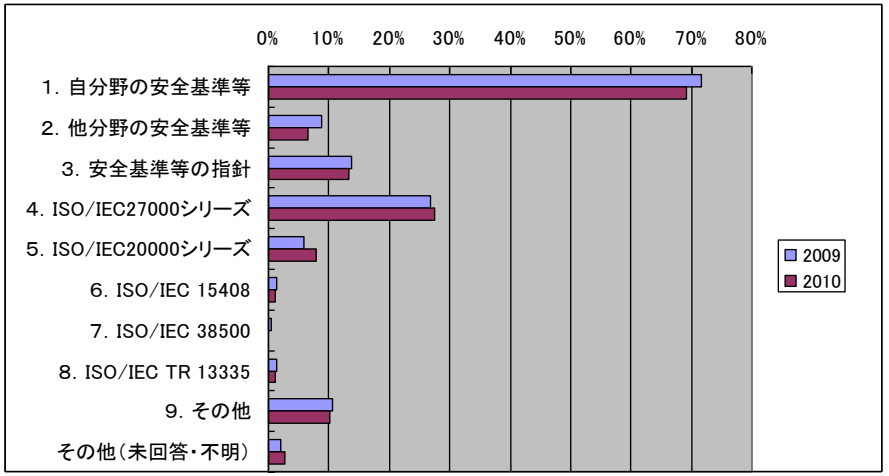
調査結果　①安全基準等の整備の状況に関する事項 (3/4)

- **内規見直しの契機として、自社におけるIT障害や、安全基準以外の文書が微増。少しずつ視野が広がっていると推定。**
- **内規を制定していない事業者のほとんどは中小規模の事業者であるが、減少傾向にあるものと推定。**

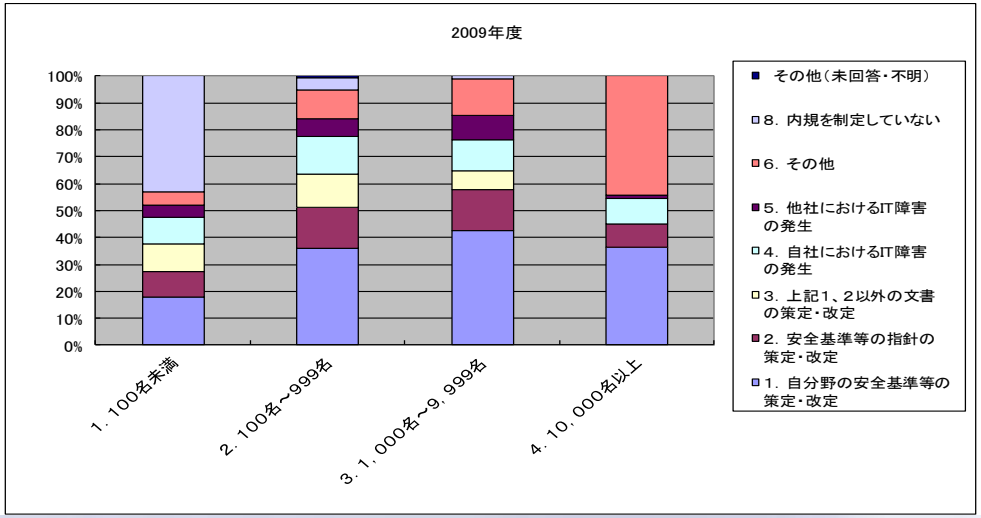
(1) -1内規策定・見直しの契機
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）
※項目7は今年度追加

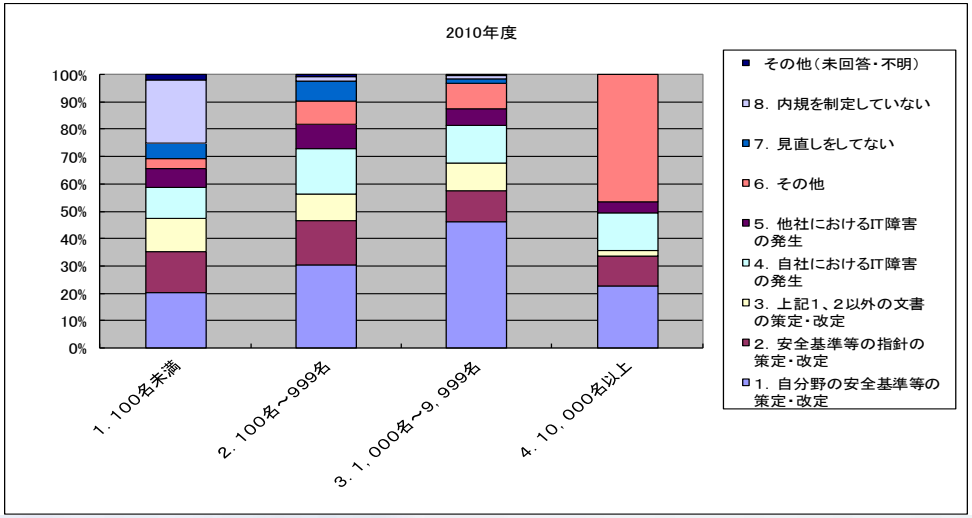


(2) 内規策定・見直しにあたり参考とする安全基準、規格等
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



内規策定・見直しの契機の事業規模毎の割合（2009年度、2010年度）

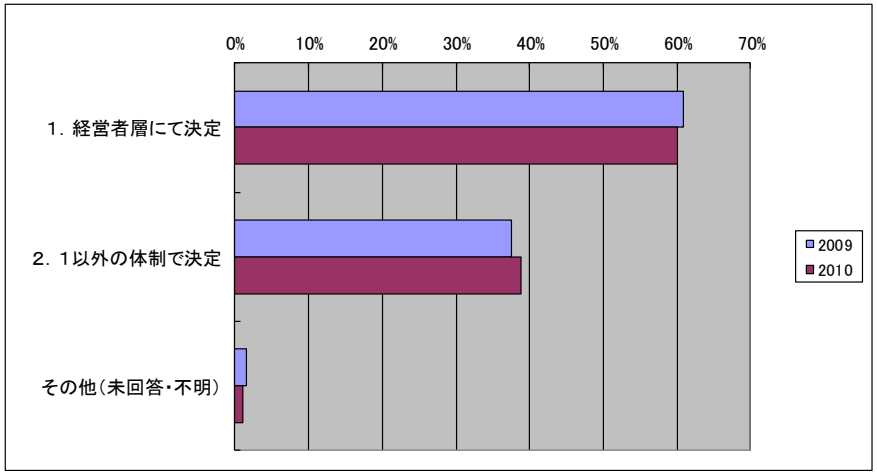




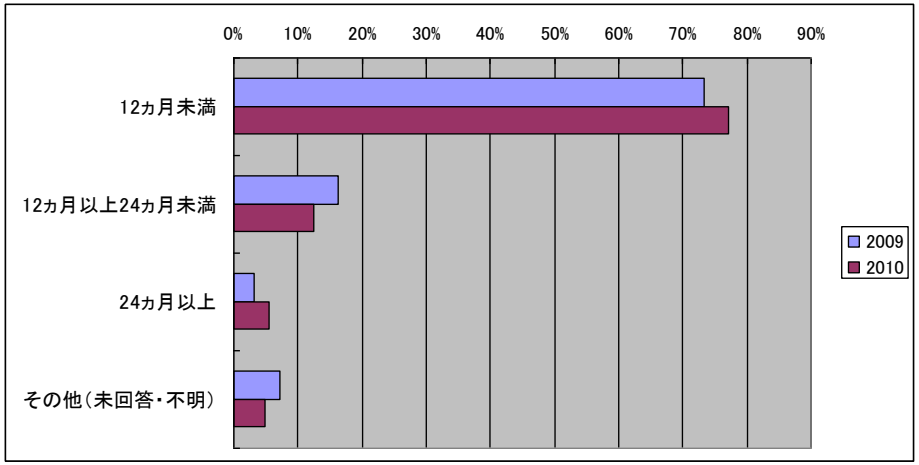
調査結果　①安全基準等の整備の状況に関する事項 (4/4)

- **内規の改定は、概ね1年未満で実施され、半数以上の事業者では経営層にて決定されていると推定**

(3) 内規改定を行う際の体制
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）



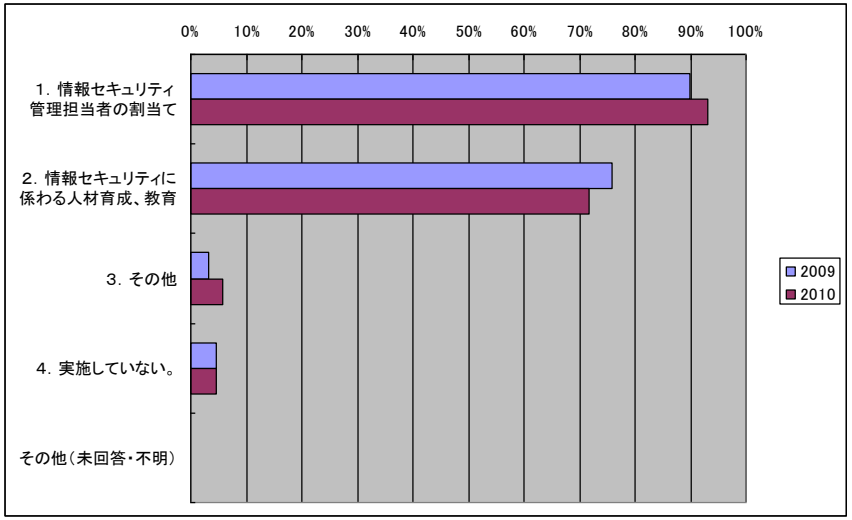
(4) 内規改定に要する期間
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



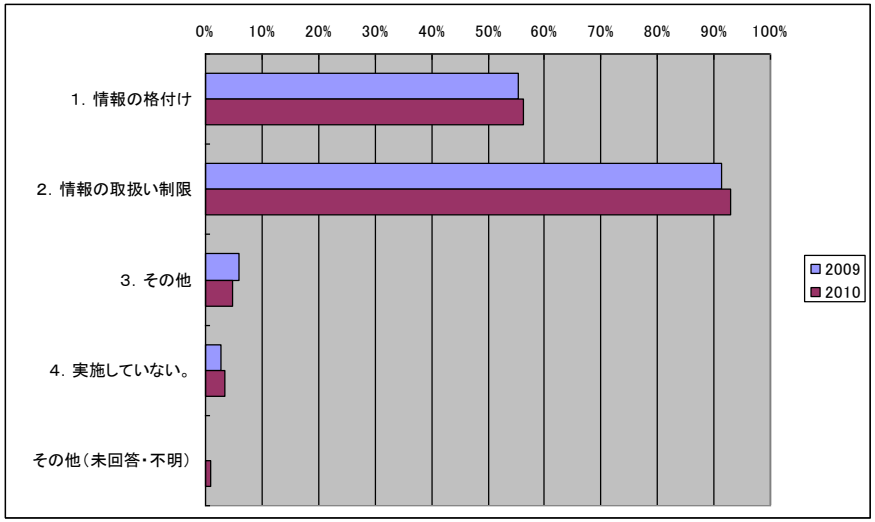
調査結果　②情報セキュリティ対策の実施状況に関する事項 (1/4)

- (1)～(3)について一定の事業者で対策を実施しておらず、実行する余裕がない事業者があるものと推定。
- 情報セキュリティ要件を明確化している事業者では、情報システムの対策をとられているものと推定。

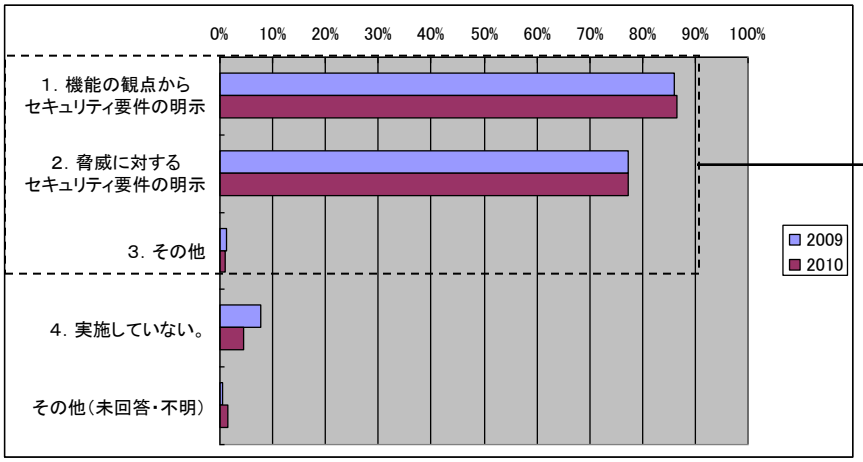
(1) 組織・体制及び資源の確保に関する対策
金融は読み替え可能項目なし（集計対象に含めず）



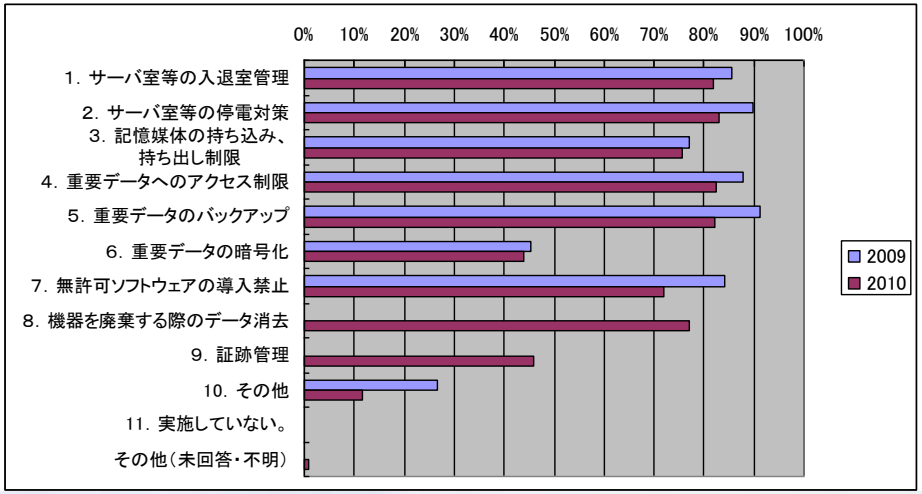
(2) 情報についての対策
金融は読み替え可能項目なし（集計対象に含めず）



(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）



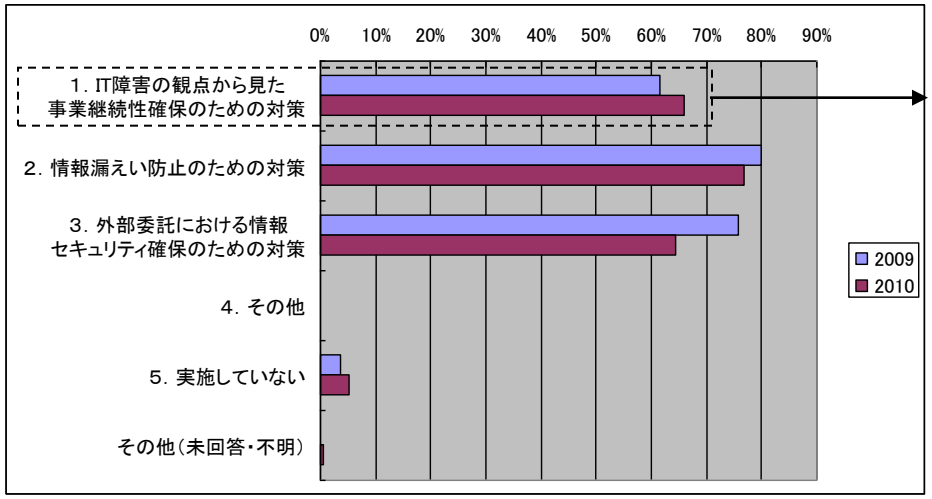
(4) 情報セキュリティ要件に対応した情報システムの対策
項目8，9は今年度追加



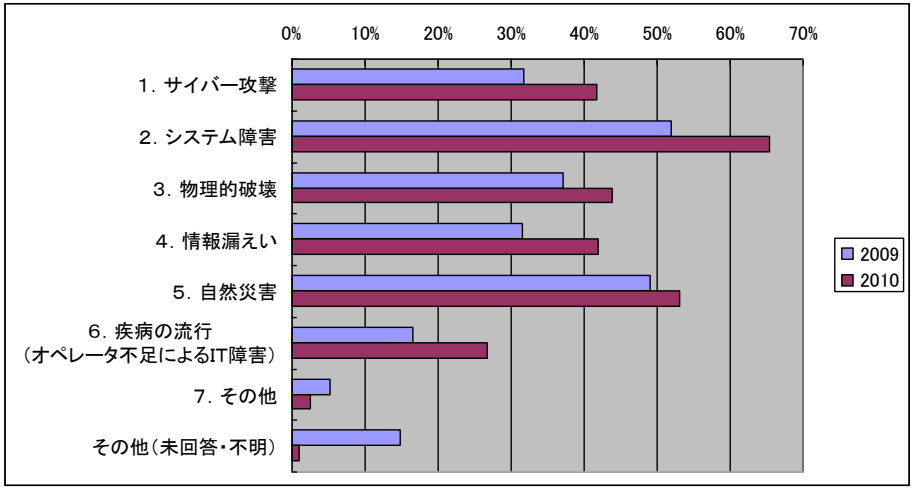
調査結果　②情報セキュリティ対策の実施状況に関する事項 (2/4)

- **IT障害の観点から見た事業継続性確保のための対策の障害となる脅威において、未回答が減少し脅威全般の比率が高まっていることから、情報セキュリティ対策の具体化が進んでいると推定**
- **事業継続計画の策定について、予定がある事業者減少した一方で策定予定していない事業者が増加し、策定を先送りする傾向があると推定。**

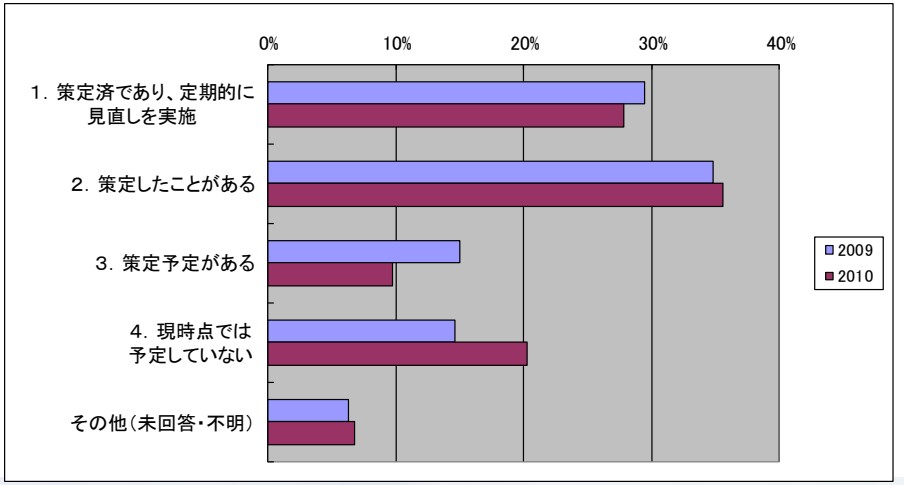
(5) 情報セキュリティ対策の運用に関する対策



(6)事業継続性確保のための対策に関して、対象とする脅威
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）



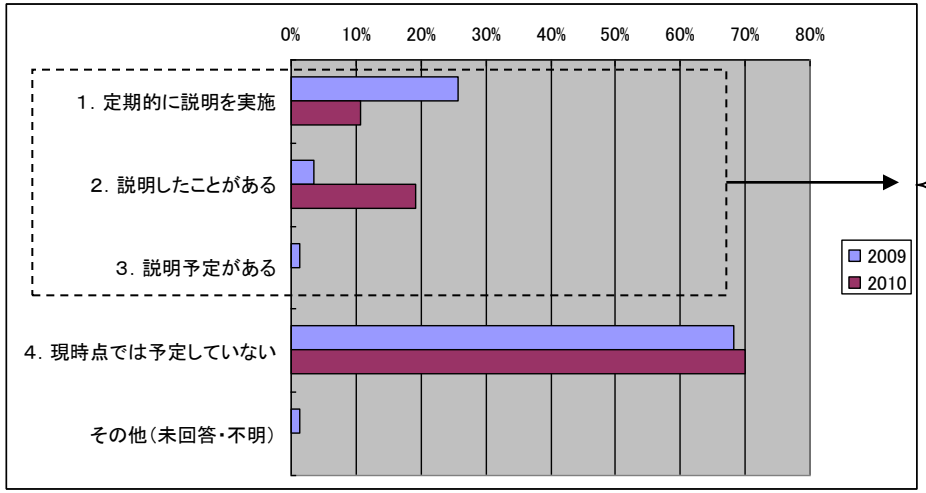
(7) 事業継続計画の策定状況



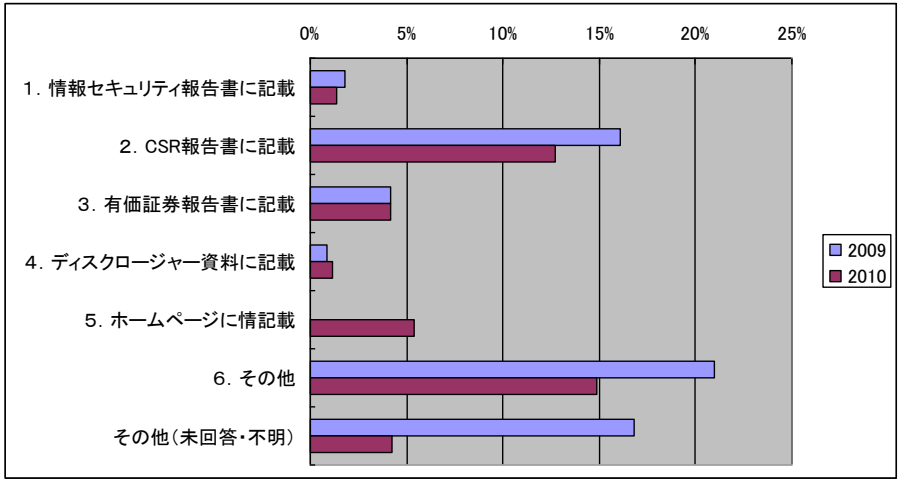
調査結果　②情報セキュリティ対策の実施状況に関する事項 (3/4)

- 情報セキュリティ対策の対外的な説明に関して、定期的な説明実施している事業者が減少し、説明したことのある事業者が増加している。また、説明方法において、定期的に発行するCSR報告書に記載する事業者が若干減少している。
- 一度は対外的な説明を行ったことがあるものの負担が大きい、または費用対効果が低いと考えている事業者が増加していると推定。但し、多くの事業者でIT障害時の情報提供に関して方策を内規に明示していると推定。

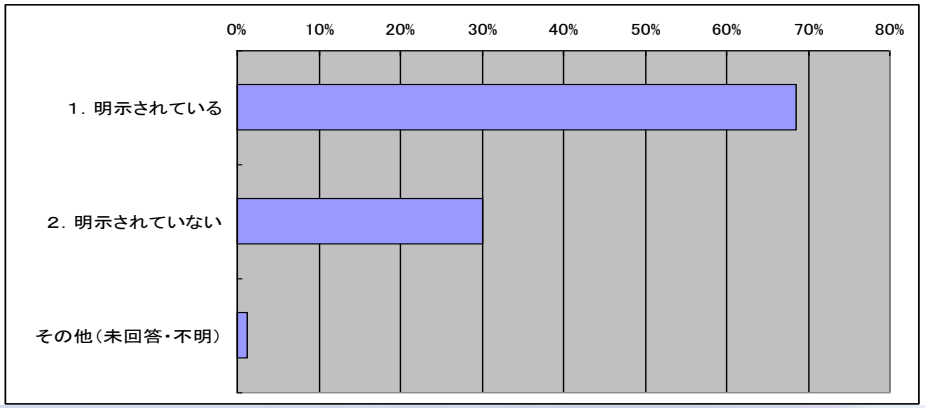
(8) 情報セキュリティ対策の対外的な説明の状況
金融、政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



(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）



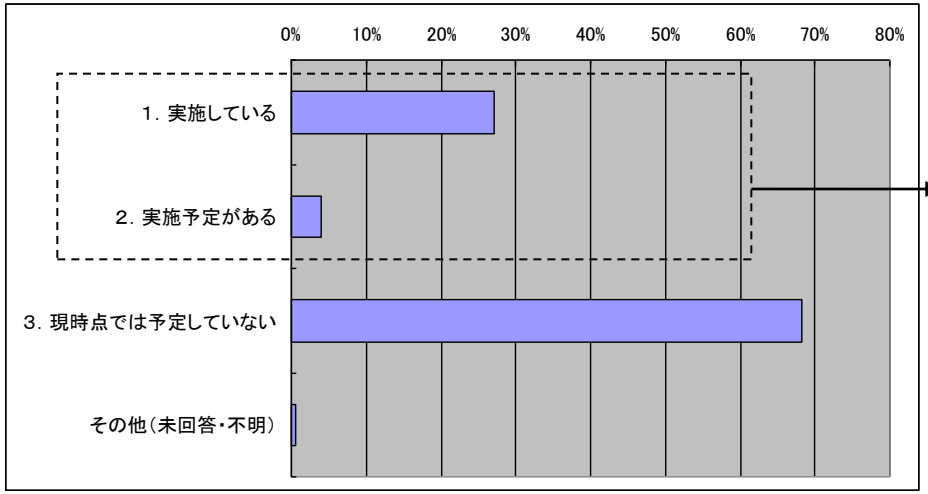
(10) IT障害時のユーザへの情報提供の方策
金融、政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



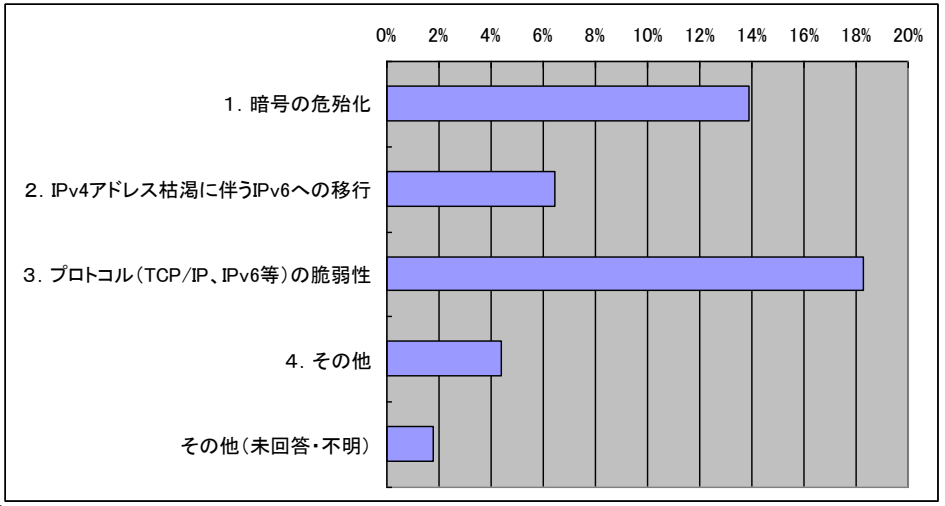
調査結果　②情報セキュリティ対策の実施状況に関する事項 (4/4)

- **ITに係る環境変化に伴う脅威に関しては対策を現時点で予定していない事業者が7割弱と推定**

(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）



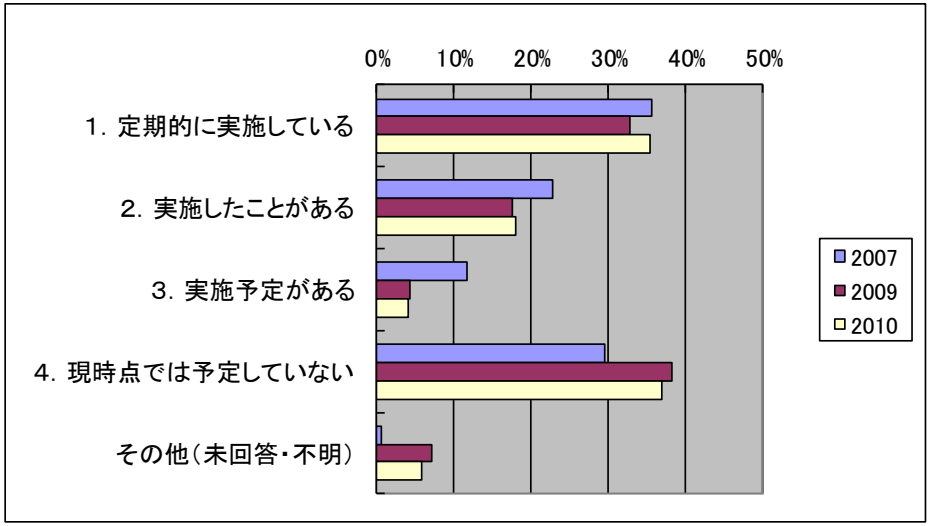
(12)　想定する脅威
政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



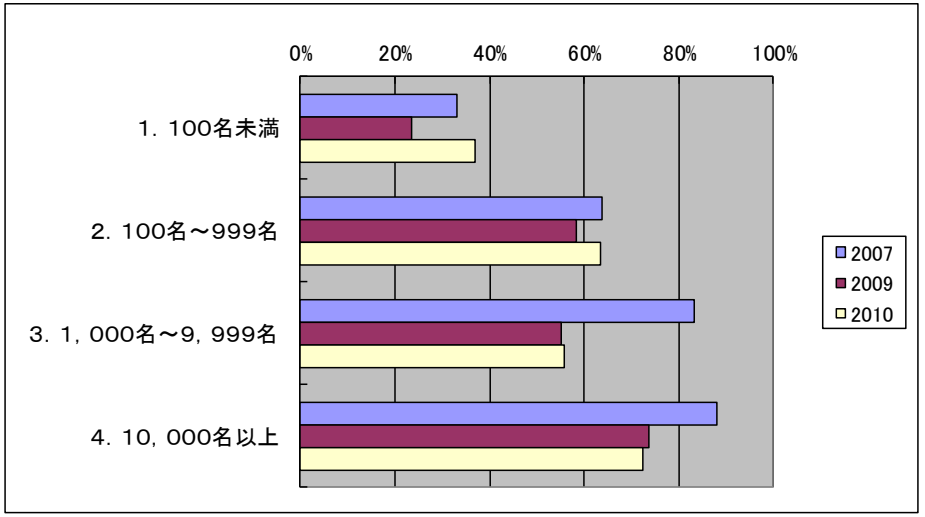
調査結果　③安全基準等に対する準拠状況に関する事項 (1/4)

- **自己点検の実施状況はおおむね昨年度と同じ傾向であり、予定を含む実施割合が5～6割と推定。**

(1) 自己点検の実施
金融は読み替え可能項目なし（集計対象に含めず）



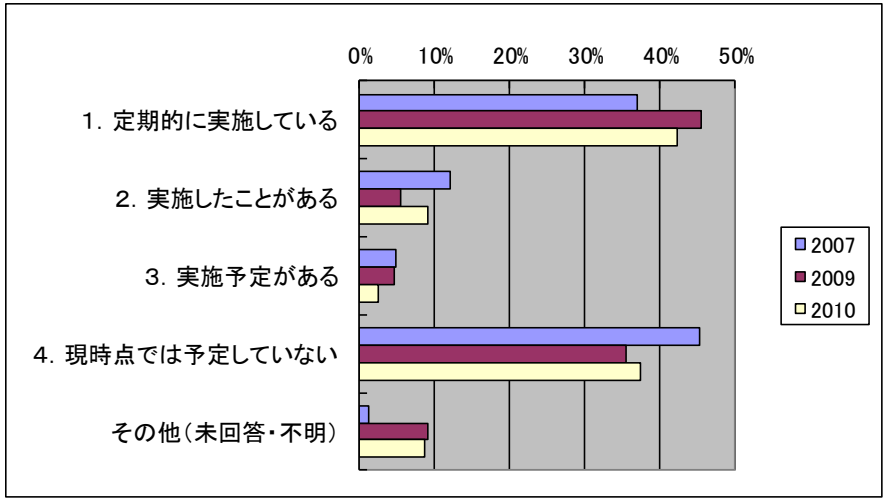
自己点検の事業規模ごとの実施割合（予定含む）



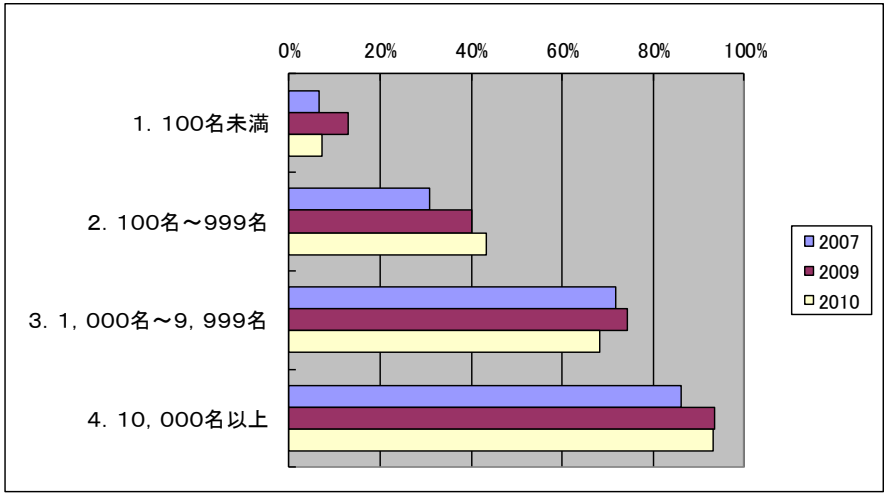
調査結果　③安全基準等に対する準拠状況に関する事項 (2/4)

- **演習・訓練の実施状況はおおむね昨年度と同様の傾向であり、予定を含む実施割合が5～6割と推定**

(2)演習・訓練の実施
金融は読み替え可能項目なし（集計対象に含めず）



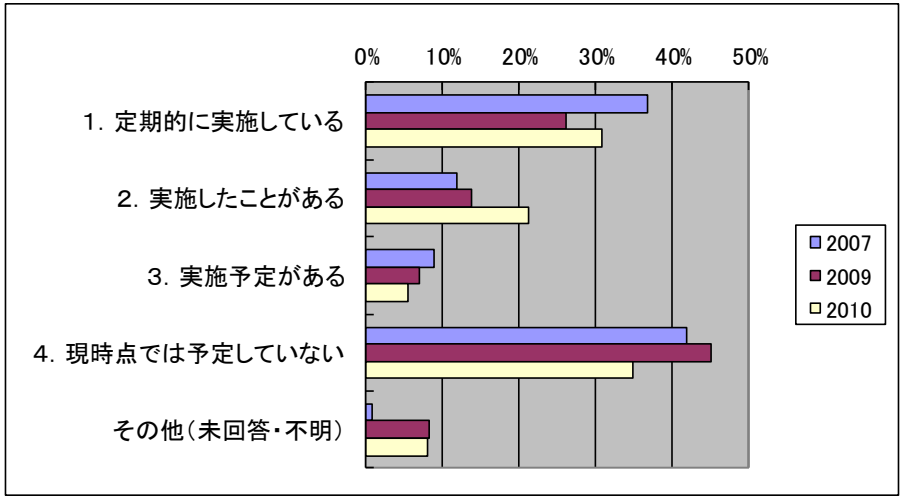
演習・訓練の事業規模ごとの実施割合（予定含む）



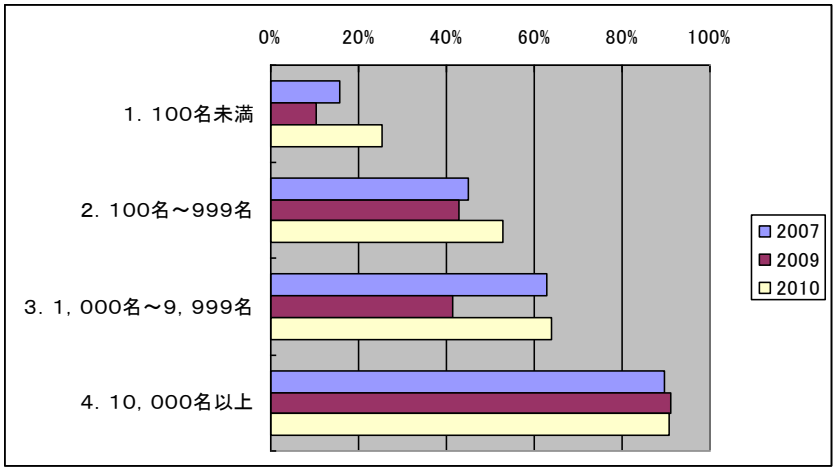
調査結果　③安全基準等に対する準拠状況に関する事項 (3/4)

- **内部監査の実施を予定していない事業者が減少し、予定を含む実施割合は5～6割に増加しているものと推定**

(3) 内部監査の実施
金融は読み替え可能項目なし（集計対象に含めず）



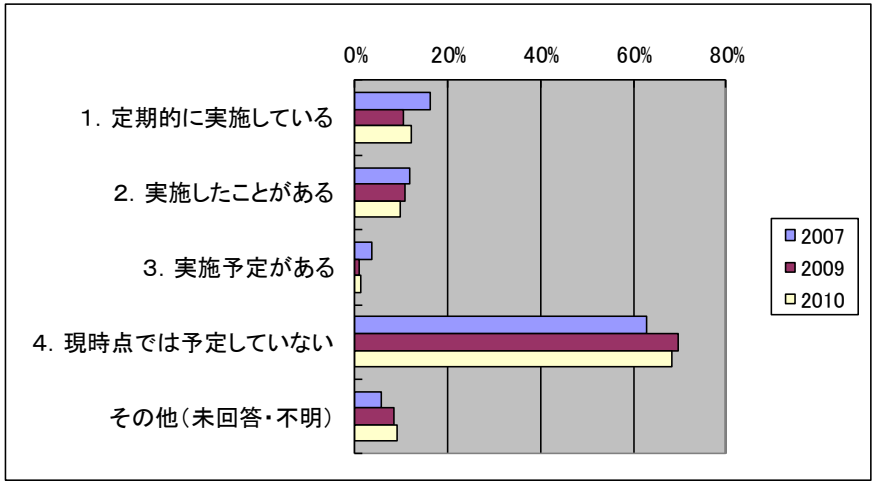
内部監査の事業規模ごとの実施割合（予定含む）



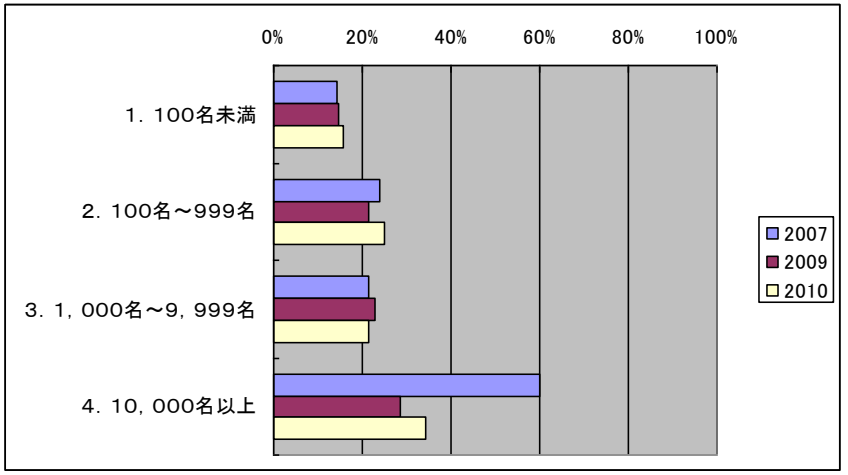
調査結果　③安全基準等に対する準拠状況に関する事項 (4/4)

- **外部監査の実施状況はおおむね昨年度と同じ傾向で、予定を含む実施割合が2割程度であり、費用のかかる事業者外部の監査機関の利用は少ないものと推定**

(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関する意見においては、指針の中身に関する意見がなくなり、具体的事例の共有、データベースの一元化に関する国の指導といった個別対応に変わりつつある。**
- **安全基準等に対する意見としては、安全基準等そのものに関する意見から、実施のためテンプレートや事前対応の要望へと変化している。**

1. 安全基準等の指針に対して
   ① 情報セキュリティ対策を実施する際に利用できるチェックシートがあるとなお良い。
   ② 指針が厳しすぎて人と費用がかかりすぎる。
   ③ 「ガイドライン」「指針」といった法的拘束力のない形ではなく，法令＋基準のような法的拘束力のある形のほうが望ましいと考える。

2. 安全基準等に対して
   ① 情報セキュリティ対策を実施する際に利用できるチェックシートの添付を希望する。
   ② 厳しすぎて予算の捻出が難しい。
   ③ 新たなIT設備を導入してから未然防止のための対策をする前に、メーカー等、新たな技術を開発する時点でIT障害対策を組み込んでいただき、別途経費がかからないようにお願いしたい。

調査結果　④安全基準等への提言、要望等 (2/2)

- **自由意見については、安全基準のような管理規定をどのように作るべきかという段階から、事例の共有や、規定の運用に対する支援に関心が移ってきており、安全基準等の確実な浸透が確認できた。**

3. その他（自由意見を記載）

① 指針、基準、ガイドラインの作成にあたっては、同業界でも企業規模の大小があることを勘案いただきたい。
② スパムメールの対策強化を希望する。
③ ウィルス対策をソフトウェア業界任せにせず、国の研究機関等が主導すべき。
④ 情報セキュリティに対するリテラシーの低い企業にも導入可能なように、最低限必要なセキュリティーを具体的に明示してほしい。
⑤ セキュリティに関しては、目に見える成果がない上にコストが高いので、経営者が集まる場でのセキュリティ確保の重要性のさらなる周知・広報をお願いしたい。
⑥ 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、セキュリティ対策費用等における助成の検討をお願いしたい。
⑦ 収益が上がらない部門への投資はリスキーであるため、業界のIT化を進めるのであれば、助成金等を見直して頂きたい。
⑧ サイバーテロ、不正アクセス、ウイルス散布、スパムメールに対する取締りと法的措置の強化を実施すべき。
⑨ 専門知識を有する人材が不足している
⑩ 情報システム提供側（ベンダー）に指針等をもう少し理解してもらいたい
⑪ セキュリティ対策としてシステムを構築する上での具体的対策を情報提供して頂きたい。
⑫ 事業者が所属する上位組織の管轄で情報セキュリティ対策の取り組みを行っており、事業者が個別に行ってはいない。

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

- 指針(第3版)の決定時期が調査対象期間外にずれ込み、改訂の反映状況は調査対象にならなかったため、昨年度と同様の環境下での調査になり全体的に回答選択の傾向は昨年と同様であった。また、回収率も同じ水準にあり、本件調査自体は定着してきたものと思料する。
- 重要インフラ事業者における内規の制定は9割以上の事業者で実施されており、また、未実施においても上位組織の規定に従っているところがあり、ほぼすべての事業者が何らかの形で制定しているものと思料。

≪さらなる情報セキュリティ対策の拡充に向けて≫

- 事業継続性確保のための情報セキュリティ対策の具体化が進んでいるものと思料。
  (NISCで作っている事業継続計画の充実に資するための情報セキュリティ対策のあり方の検討にも反映)
- 演習・訓練の実施状況は昨年度と同様であり、NISCにおける分野横断的演習と連携して引き続き普及・啓蒙を図る。
- 対策実施において参考とするチェックリスト等に関する要望があり、指針対策編等の周知啓蒙を図る。

- 次回調査においては、指針第3版の決定(2010年5月) 並びに指針対策編の決定(2010年7月)を受け、浸透状況に変化があるものと思料する。
- 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継続的に把握する。

＜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案に準じて実施」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） 現在、指針が見直されているのをご存知ですか。
（2） 見直しの内容についてご存知ですか。
（3） 指針の見直しに伴い、内規等の見直しの準備をしていますか。
（4） 指針が見直されるのに伴い、内規等の見直しの検討を実施しますか(予定を含む)。
（5） 策定・見直しの契機を以下からお知らせ下さい。
（6） 参考とする安全基準等や諸規格をお知らせ下さい。
（7） 内規改定を行う際の体制をお知らせ下さい。
（8） 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)

※ 既存調査を活用する分野で読み替え可能な項目がない場合には、全体集計の対象には含めず