NISC National Information Security Center

2009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

2010年5月11日

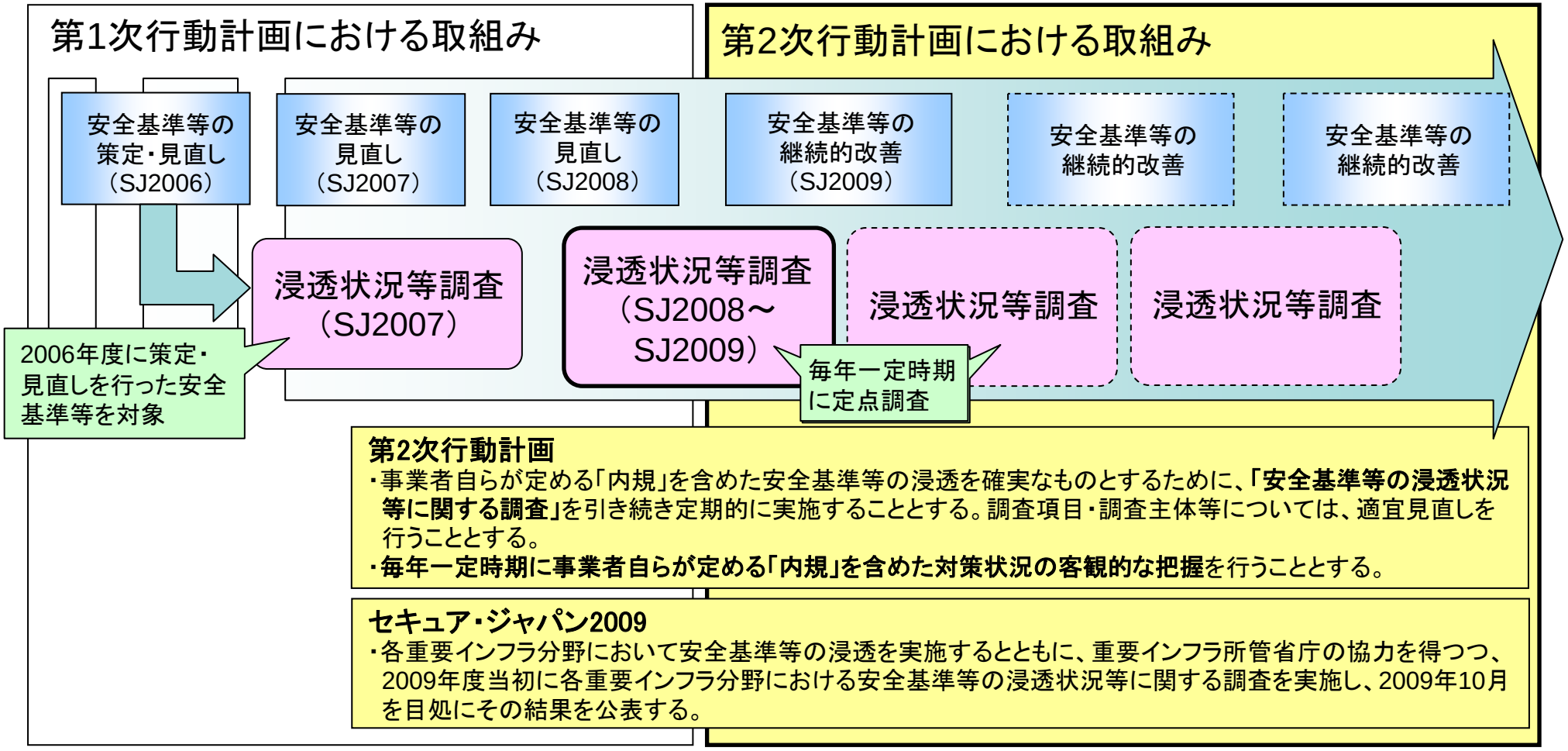
内閣官房情報セキュリティセンター（NISC）

資料2-2-3

「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「セキュア・ジャパン2009」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。

セキュア・ジャパン2009

・各重要インフラ分野において安全基準等の浸透を実施するとともに、重要インフラ所管省庁の協力を得つつ、2009年度当初に各重要インフラ分野における安全基準等の浸透状況等に関する調査を実施し、2009年10月を目処にその結果を公表する。

「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	：	2009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	：	2009年4月～2009年6月（集計は2009年7月まで）
とりまとめ	：	2009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
- 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3,220事業者等に対し、3,019事業者等からアンケートを回収（回収率 93.8％）
- 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	22	22
	放送	しない	日本放送協会及び地上系一般放送事業者	194	179
金融		する	金融機関等	977	829
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	1,858	1,858
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）	50	49
物流		しない	物流事業者	22	8
全分野合計				3,220	3,019

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＞浸透状況等調査の実施における留意点

・ 2007年度の浸透状況等調査の実施に際して明らかとなった以下点に留意して、「安全基準等の浸透状況等に関する調査」の企画・立案を行う

留意点１：類似の調査との重複について

・重要インフラ10分野には既に類似の調査を実施している分野があり 、新たに調査を実施すると重複する恐れがある
・既存調査で、安全基準等の普及・活用状況の把握が可能な場合がある

既存調査を活用することで調査を効率化
- 安全基準等の見直し周期や行動計画の進捗状況の評価周期にあわせて、調査周期は原則１年とする
- 調査内容のずれについては、調査実施前に調査実施主体とNISCの間で整合を図るべく努力する
- 2008年度以降は調査基準日を半年ずつずらし、既存調査との整合を確保する

留意点２：調査対象の範囲について

・分野に属する事業者等のうち、重要インフラ事業者等とみなすべき範囲が不明確な分野がある
・重要インフラ所管省庁の調査が及ぶ事業者等の範囲が限定される分野がある（都道府県認可の場合など）

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
- 個人事業者に至るまでのすべての事業者を網羅することは、重要インフラの趣旨を超えるため、当初は大規模事業者等を中心に調査を行い、段階的に調査範囲を拡大することを検討する
- 例えばCEPTOARの連絡体制等を活用するなど、各分野の状況に応じて調査体制の充実を検討する

＜参考２＞既存調査と浸透状況等調査の関係整理（2009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	22
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	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状況調査	3月31日	1年毎	する	金融機関等	977
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	1,858
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）	50
物流		なし				しない	物流事業者	22

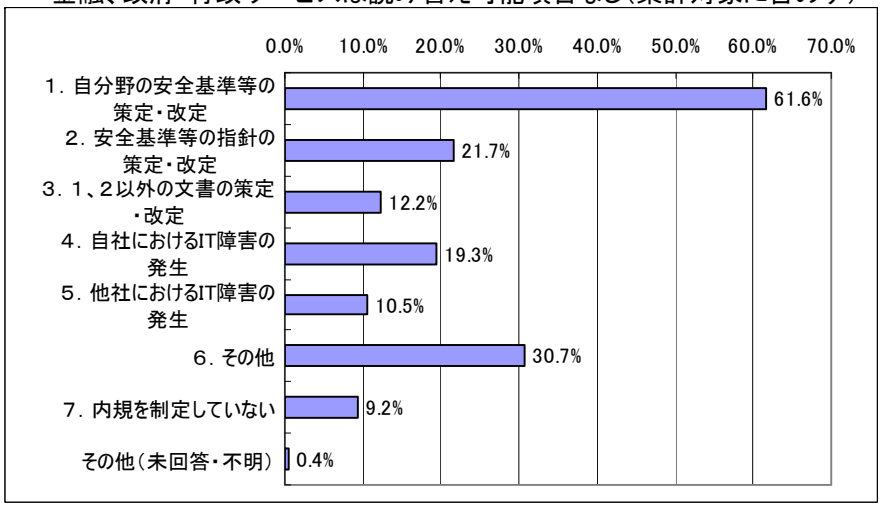
留意点１に対応

留意点２に対応

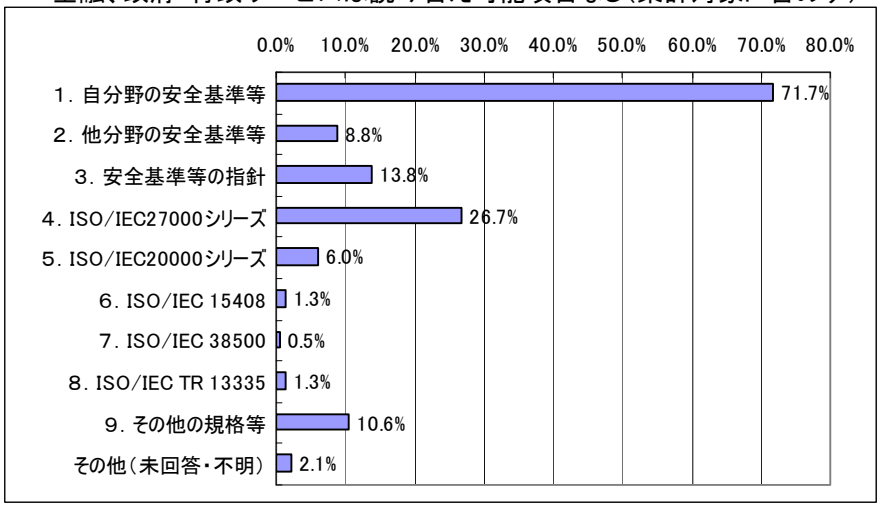
調査結果　①安全基準等の整備の状況に関する事項 (1/1)

- **内規見直しは、自分野の安全基準等の改定を契機とする事業者等が多いと推定**
- **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**

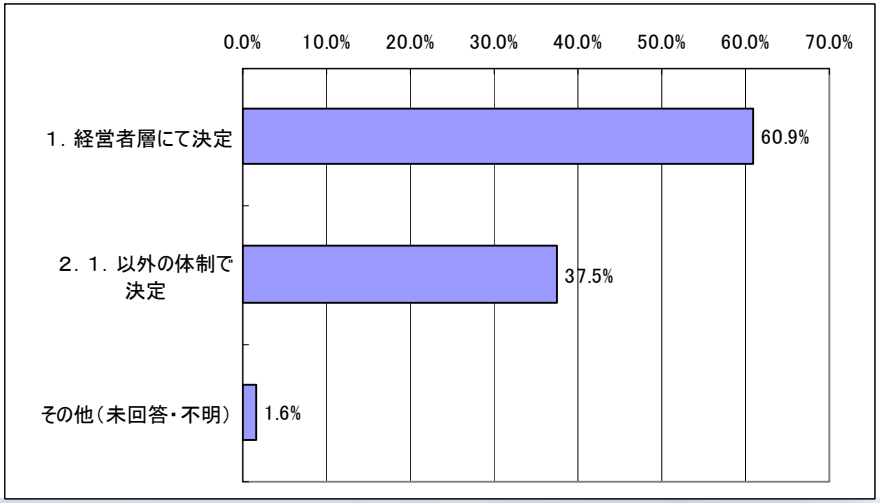
(1) 内規策定・見直しの契機
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



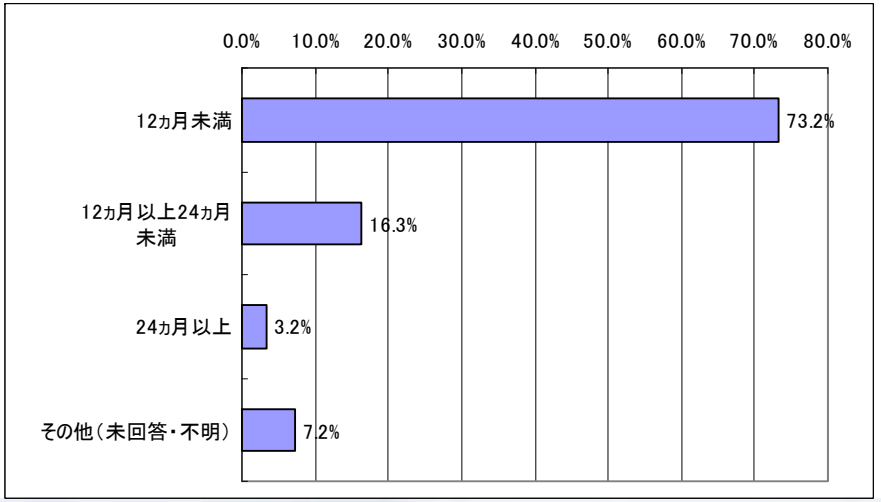
(2) 内規策定・見直しにあたり参考とする安全基準、規格等
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



(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）



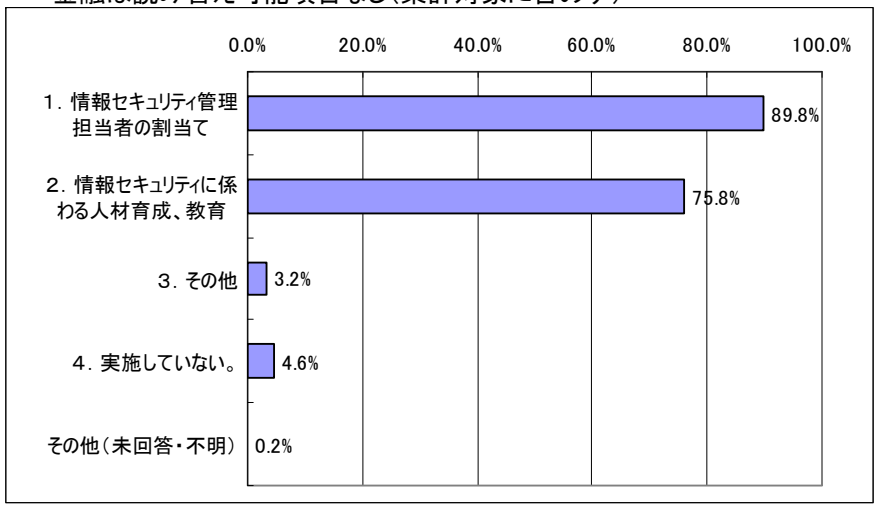
(4) 内規改定に要する期間
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



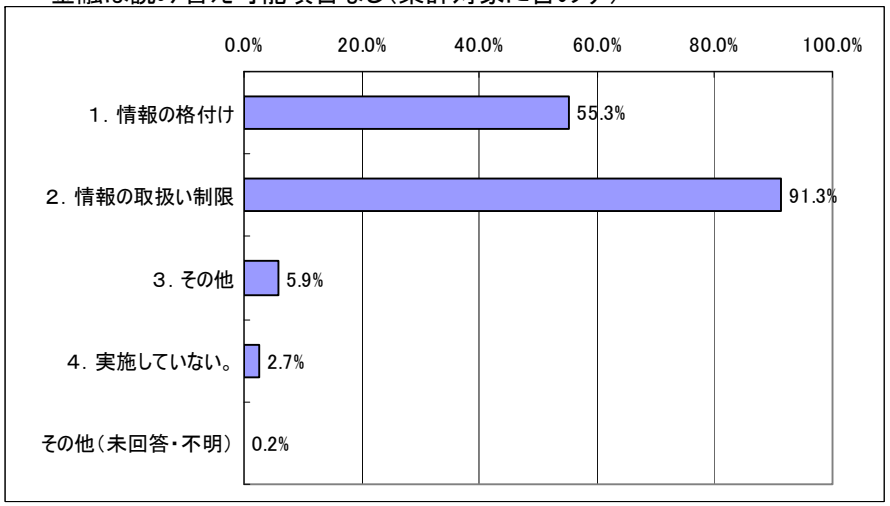
調査結果　②情報セキュリティ対策の実施状況に関する事項 (1/3)

- **情報セキュリティ対策は、多くの事業者で実施していると推定**
- **さらに情報の取扱い制限、重要データのバックアップ等を複合して実施している事業者等が多いと推定**

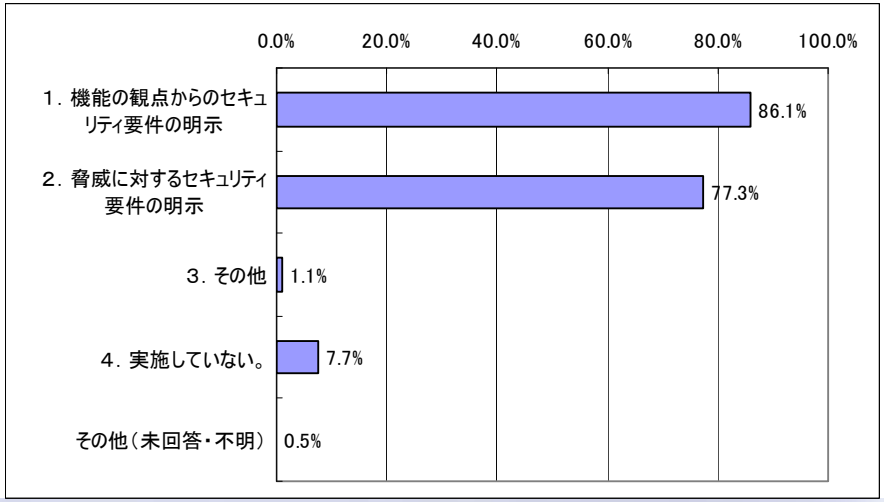
(1) 組織・体制及び資源の確保に関する対策
金融は読み替え可能項目なし（集計対象に含めず）



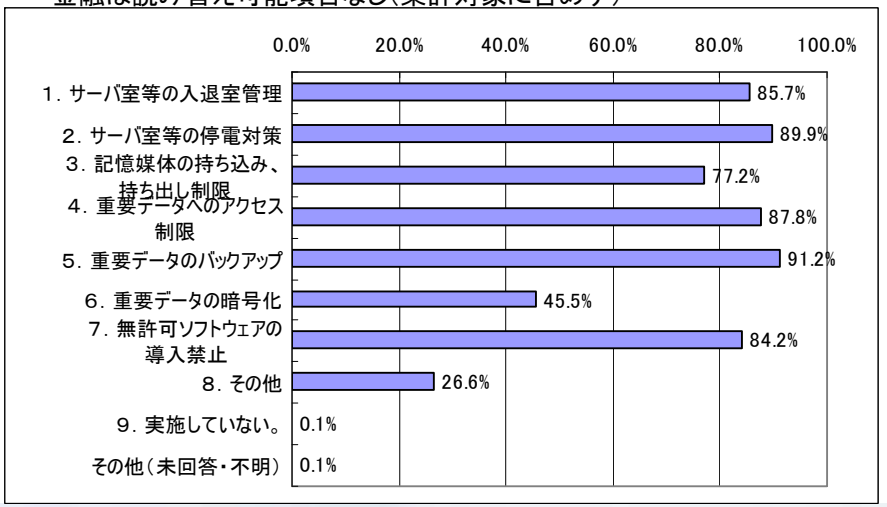
(2) 情報についての対策
金融は読み替え可能項目なし（集計対象に含めず）



(3) 情報セキュリティ要件の明確化
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）



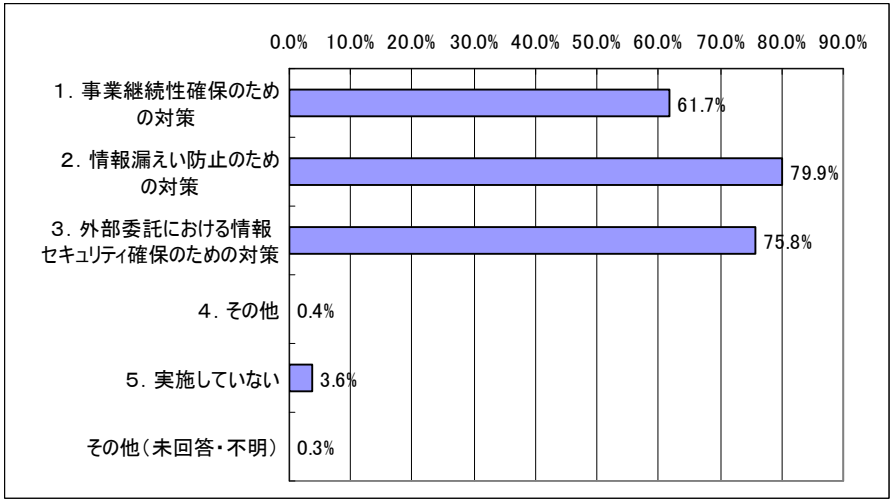
(4) 情報システムに対する対策
金融は読み替え可能項目なし（集計対象に含めず）



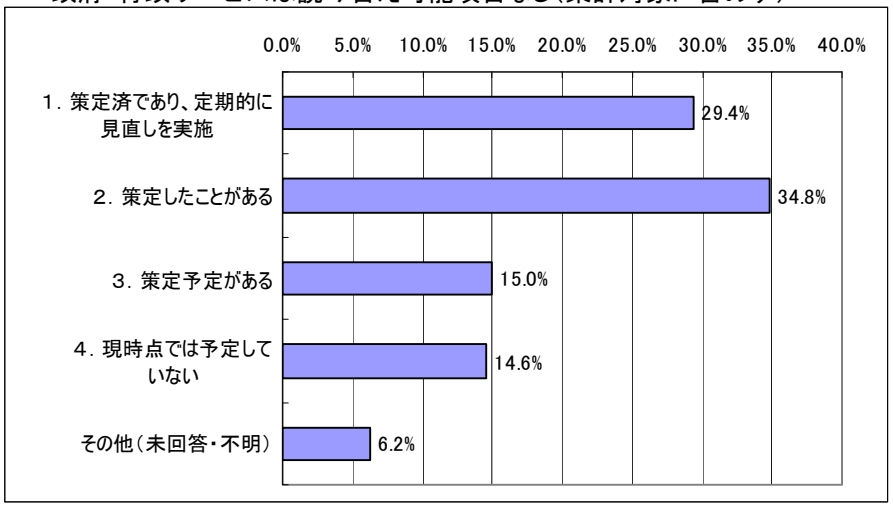
調査結果　②情報セキュリティ対策の実施状況に関する事項 (2/3)

- **事業継続性確保のための対策は6割以上の事業者等で実施済みと推定**
- **事業継続計画の対象とする脅威として、システム障害、自然災害を取り上げている事業者等が多いと推定**

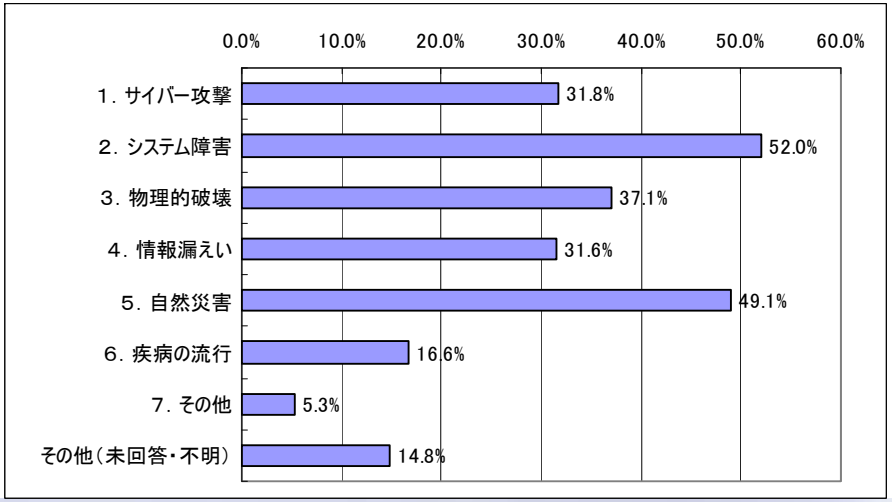
(5) 運用に関する対策



(6) 事業継続計画の策定状況
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）



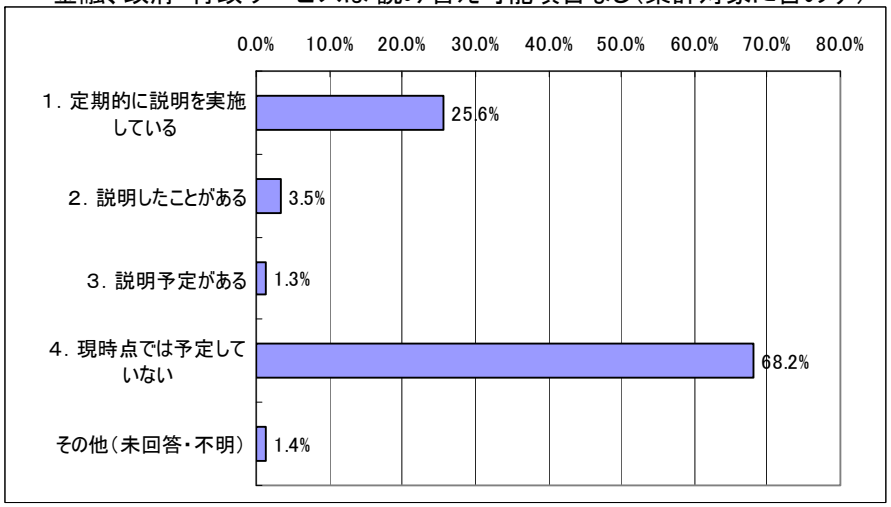
(7) 対象とする脅威
政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



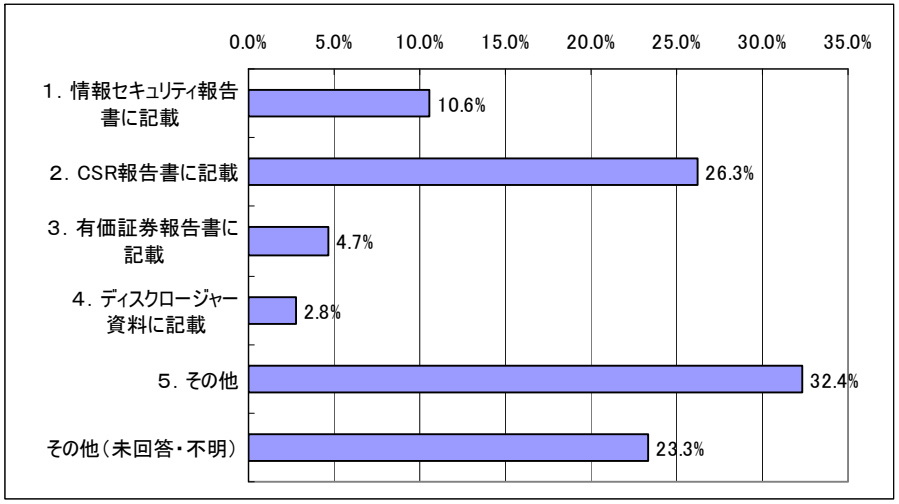
調査結果　②情報セキュリティ対策の実施状況に関する事項 (3/3)

- **情報セキュリティ対策の対外的な説明を実施している(予定含む)事業者等は3割程度と推定**
- **対外的な説明方法は、CSR報告書のほか、ホームページなどの広報の一環として実施している事業者等が多いと推定**

(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)

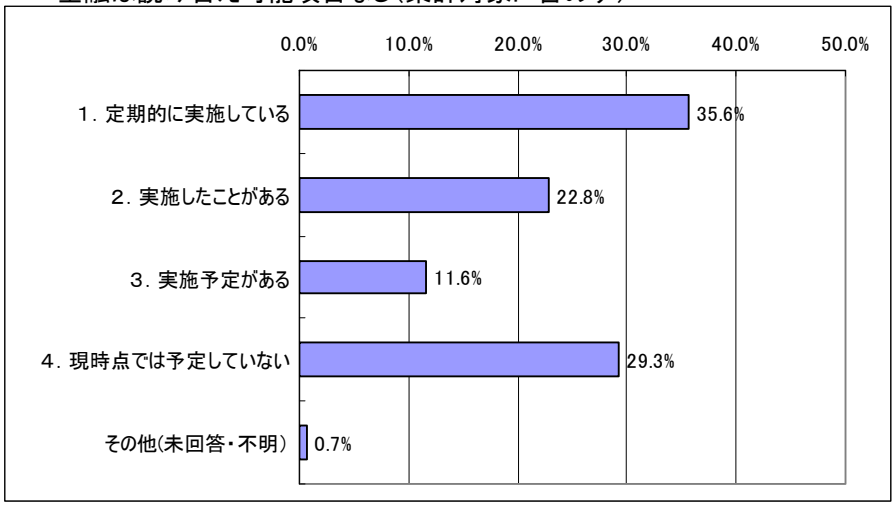


調査結果　③安全基準等に対する準拠状況に関する事項 (1/4)

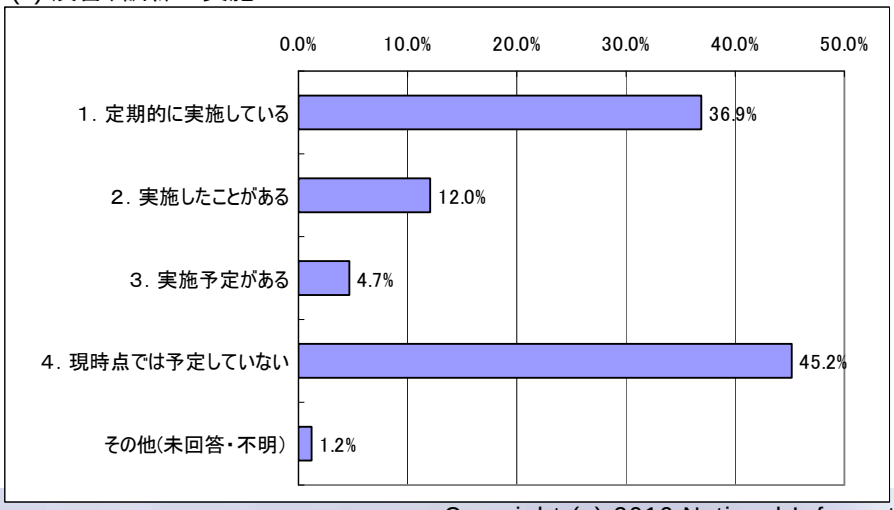
- 2007年度に引き続き、自己点検、演習・訓練、内部監査、外部監査の実施状況について調査
- 自己点検の実施、演習、訓練の実施は、概ね2007年度と同じ傾向と推定

2007年度の結果

(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）

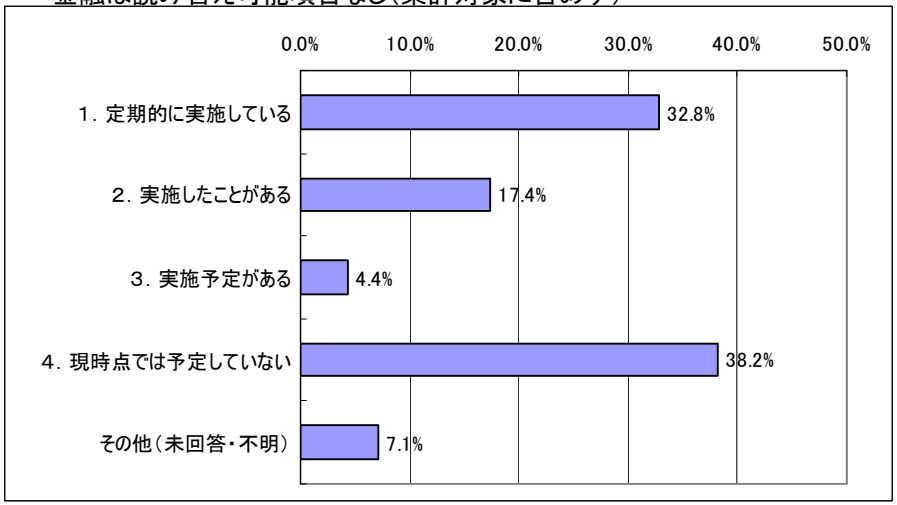


(2) 演習、訓練の実施

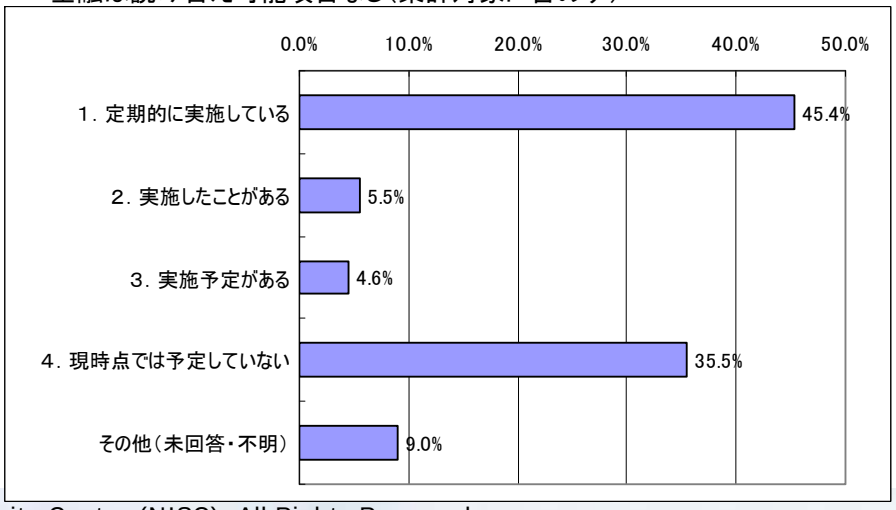


2009年度の結果

(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）



(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）

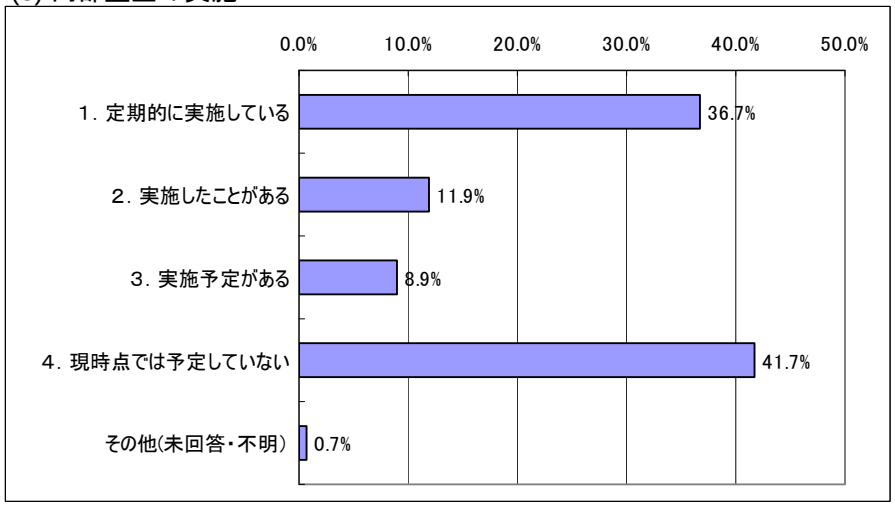


調査結果　③安全基準等に対する準拠状況に関する事項 (2/4)

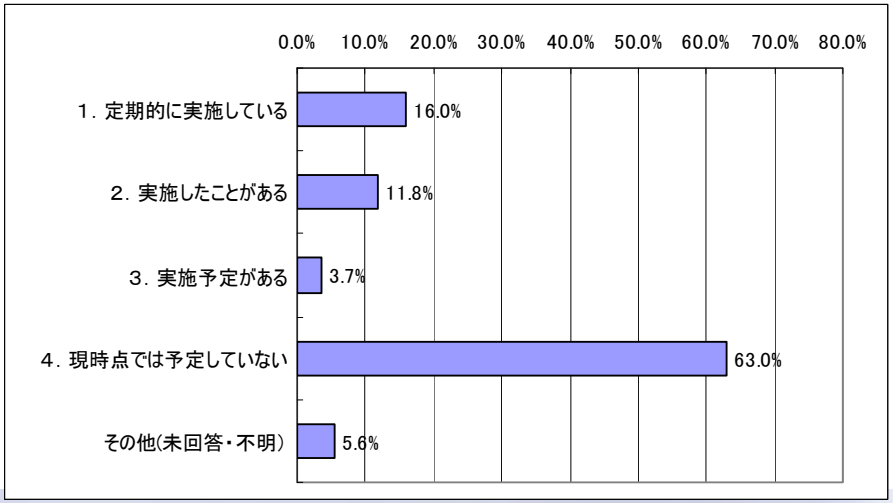
- **内部監査の実施、外部監査の実施は、概ね2007年度と同じ傾向と推定**
- **特にこの期間中、指針の改定等が行われなかったため、大きな変化はなかったものと推定**

2007年度の結果

(3) 内部監査の実施

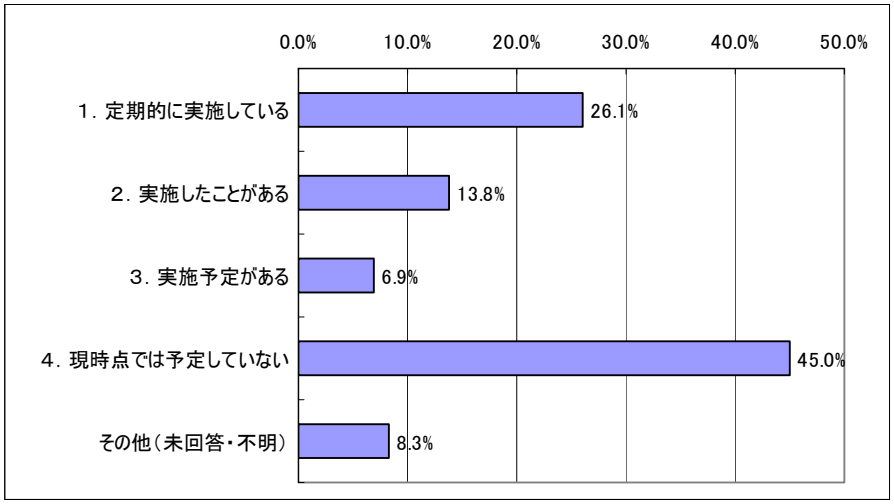


(4) 外部監査の実施

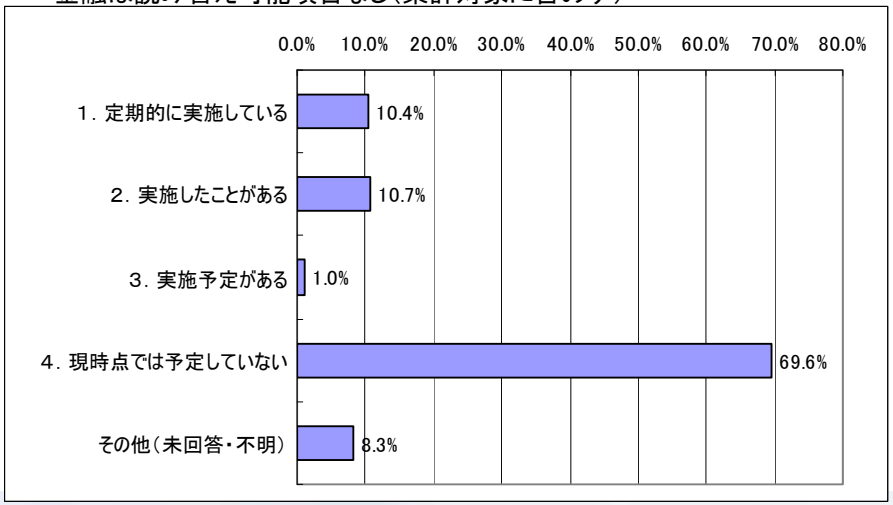


2009年度の結果

(3) 内部監査の実施



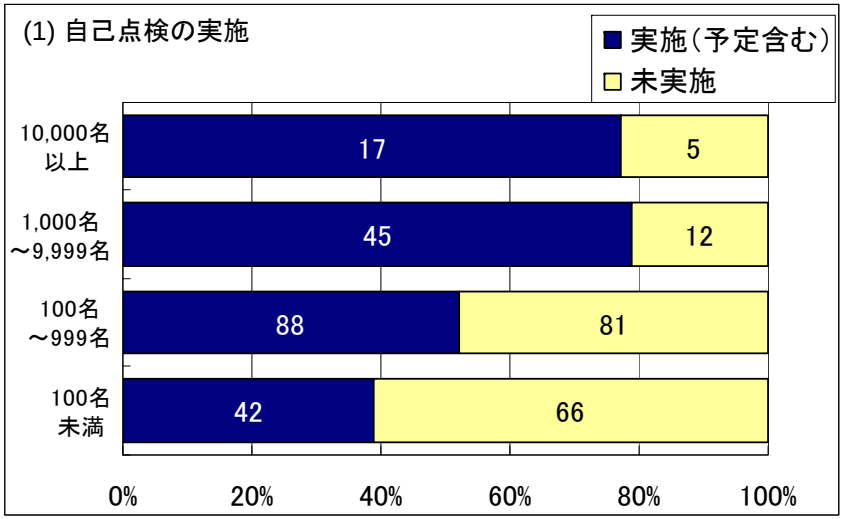
(4) 外部監査の実施
金融は読み替え可能項目なし（集計対象に含めず）

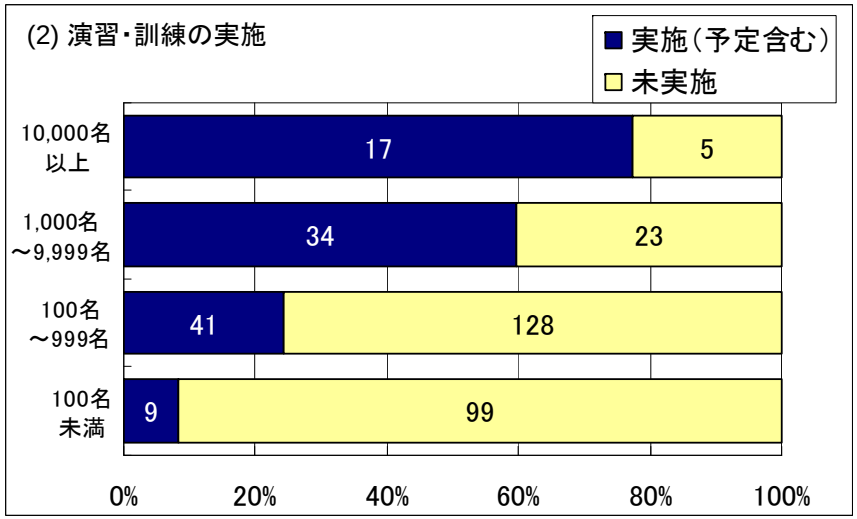


調査結果　③安全基準等に対する準拠状況に関する事項 (3/4)

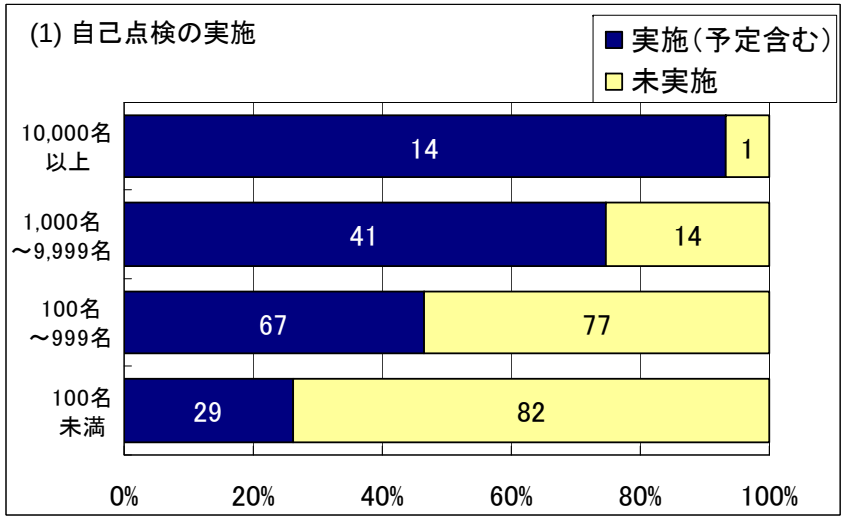
- **従業員数別の安全基準等に対する準拠状況は、概ね2007年度と同じ傾向と推定**

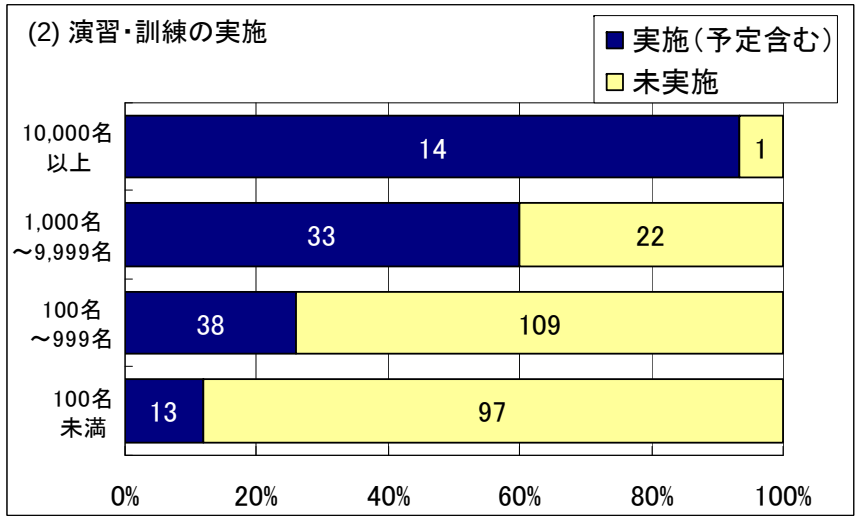
2007年度の結果





2009年度の結果



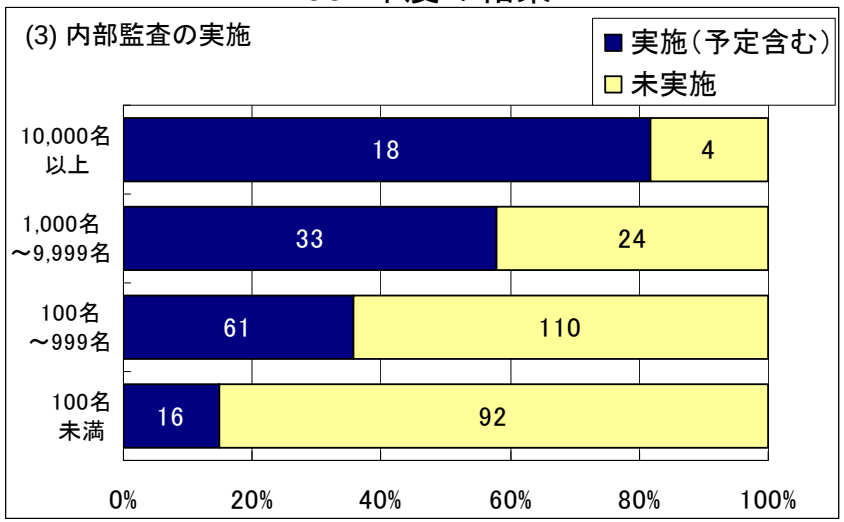


※金融、政府・行政サービスは従業員数別内訳なし、「その他（未回答・不明）」を除く（集計対象に含めず）

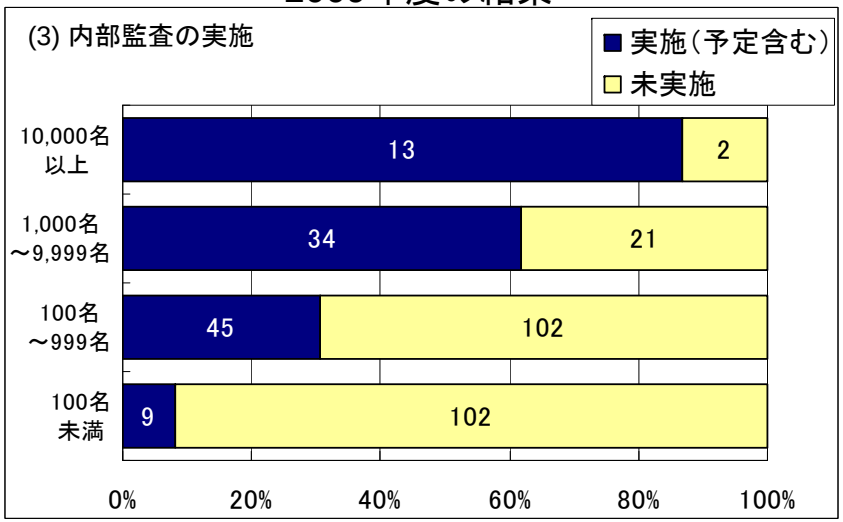
調査結果　③安全基準等に対する準拠状況に関する事項 (4/4)

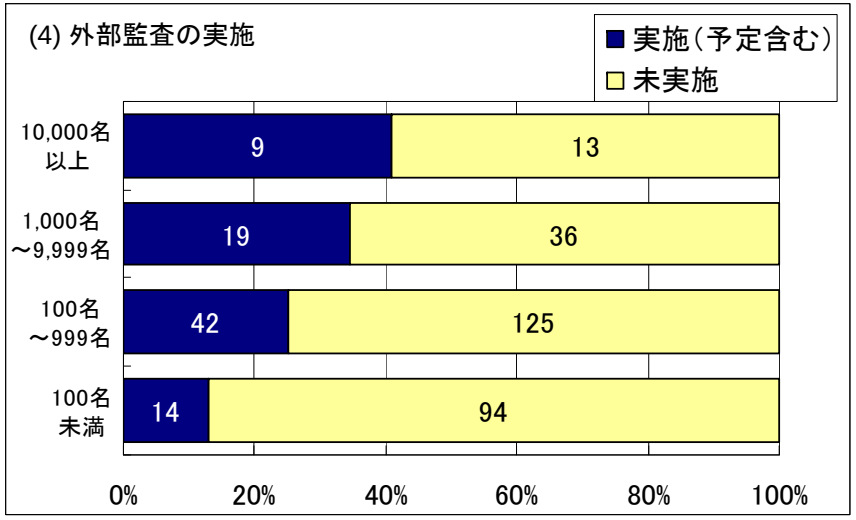
- 2007年度と同様に企業規模が大きくなる程、実施率が高くなっているので、企業規模に係わらず、実施できるような負担軽減も重要と推定

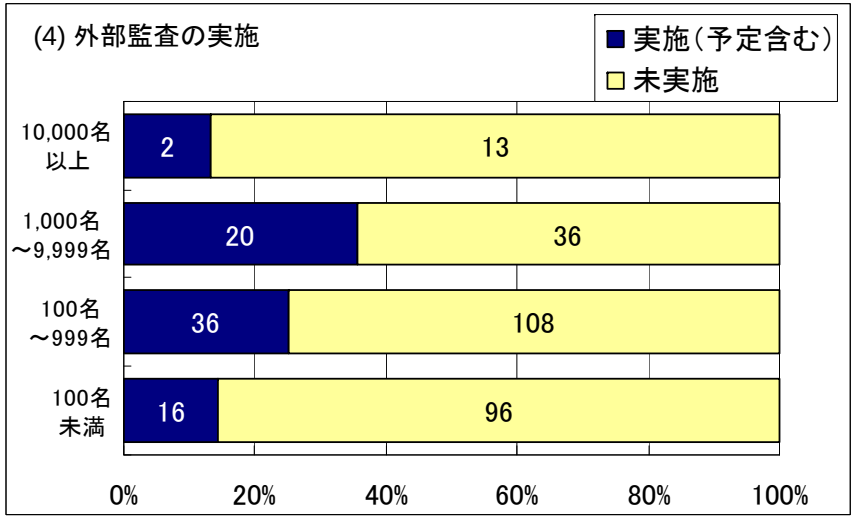
2007年度の結果



2009年度の結果







※金融、政府・行政サービスは従業員数別内訳なし、「その他（未回答・不明）」を除く（集計対象に含めず）

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、安全基準等に関する主な意見を記載**

1. 安全基準等の指針に対して

① 一般的なセキュリティだけでなく、重要インフラ保護の観点について広く記述されていることから、指針の位置づけを「安全・信頼性確保」または「危機管理」に係る安全基準策定にあたっての指針としてはどうか。
② 例示を掲載すると企業の理解が深まるのではないか。
③ 情報セキュリティー施策に関して、「何を」「どの程度」するべきかの指針として参考になった。

2. 安全基準等に対して

① 事業形態の違いにより各事業者の安全基準への対応は異なってくることをふまえ、保護すべきサービスやシステムをより具体的に示す等、安全基準に対する解説、例示等の充実を検討するべきではないか。
② 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提示してもらえないか。
③ 重要インフラを担う企業に対しては、情報セキュリティの質をある一定水準確保するよう義務づけすることも必要ではないか。

調査結果　④安全基準等への提言、要望等 (2/2)

- **自由意見について主な内容を記載**

3. その他（自由意見を記載）

① 情報セキュリティ対策への支援、助成、優遇措置、質の向上につながる施策の実施。
② 小規模事業者では、情報セキュリティ対策は実施しているがマニュアルなどの整備が追いつかない。
③ システムの安定確保と情報セキュリティ対策の兼ね合いが難しい。
④ 情報セキュリティ対策の経営者層への必要性の周知と広報活動の充実。
⑤ サイバー攻撃、不正アクセス等に対する取り締まりと法的措置の強化。
⑥ 政府主催の情報セキュリティセミナーの実施。
⑦ セキュリティに関する具体的な取組み内容を開示することは、かえってリスクの増大につながる恐れがあるため、十分に留意して欲しい。
⑧ システムを構築する上でのセキュリティー上の留意点、具体的な対策、トラブル事例などの情報を提供していただきたい。
⑨ 制御系システムに関する監査範囲や内容等を記載したマニュアルの整備。

まとめ

- **2007年度に続き、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**

① 安全基準等の整備の状況に関する事項
- 内規見直しは、自分野の安全基準等の改定を契機とする事業者等が多いと推定
- 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

② 情報セキュリティ対策の実施状況に関する事項
- 情報セキュリティ対策は、多くの事業者で実施していると推定
- 事業継続計画の対象とする脅威として、システム障害、自然災害を取り上げている事業者等が多いと推定
- 情報セキュリティ対策の対外的な説明を実施している（予定含む）事業者等は3割程度と推定

③ 安全基準等に対する準拠状況に関する事項
- 安全基準等に対する準拠状況は、概ね2007年度と同じ傾向と推定
- 特にこの期間中、指針の改定等が行われなかったため、大きな変化はなかったものと推定
- 2007年度と同様に企業規模が大きくなる程、実施率が高くなっているので、企業規模に係わらず、実施できるような負担軽減も重要と推定

- 指針の策定・見直し、これを踏まえた各分野毎の安全基準等の策定・見直しが実施され、これらの定期的な見直しサイクルが実施されていると推定
- 今回の調査時点で、指針の改定等がなく前回と同じ傾向であったが、今年度は指針の改定が行われ、かつ、内規の改定が概ね1年未満で実施されることから次回以降、浸透状況に動きがあるものと推定。
- 9割の事業者が内規を制定しているが、一方、演習・訓練の未実施が3割強となっており、NISCにおける分野横断的演習と連携して、更なる周知・啓蒙を図る。
- セキュリティ対策の運用としては情報漏洩防止、外部委託における情報セキュリティ確保を目的としているのが8割に対して、事業継続性確保は6割に止まっており、この比率を向上すべく周知・啓蒙を図る。

- 第2次行動計画の策定において、指針の見直し等の時期と調査時期の整合を図ったことから、定期的に本調査を実施することで、安全基準等の浸透状況を適格に把握できるようになり、適時、改善等に役立つものと思料。
- 既存調査との調査項目を合わせるべく調査実施前に調査実施主体とNISCの間で整合を図るよう努力する。

＜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）　策定・見直しの契機を以下からお知らせ下さい。
（2）　参考とする安全基準等や諸規格をお知らせ下さい。
（3）　内規改定を行う際の体制をお知らせ下さい。
（4）　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。

【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