資料４

NISC National Information Security Center

2011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

2012年3月 21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「情報セキュリティ2011」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」の継続的改善（JS2010）
- 「安全基準等」の継続的改善（JS2011）

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）

毎年一定時期に定点調査

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2011

・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〉

2011 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アンケート項目に準じて実施
調査基準日	：	2011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アンケート項目に準じて実施 の場合）

調査期間 ： 2011年6月～2011年9月
とりまとめ ： 2011年12月

◆主な調査内容（NISCアンケート項目）

①安全基準等の整備の状況に関する事項
　指針改定の認知度、改定を知った手段
　策定・見直しの契機
　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
⑤東日本大震災における情報システムの事業継続性確保に関する対策の効果

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3,111事業者等に対し、2,909事業者等からアンケートを回収（回収率 93．5%、前年比+1.0%）
- 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	68	26
	放送	しない	日本放送協会及び地上系一般放送事業者	194	176
金融		する	金融機関等	882	776
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	1,797	1,797
医療		しない	医療機関（病院抽出）	50	31
水道		しない	水道事業体（事業者抽出）	51	44
物流		しない	物流事業者	22	12
全分野合計				3,111	2,909

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（2011年度実績）

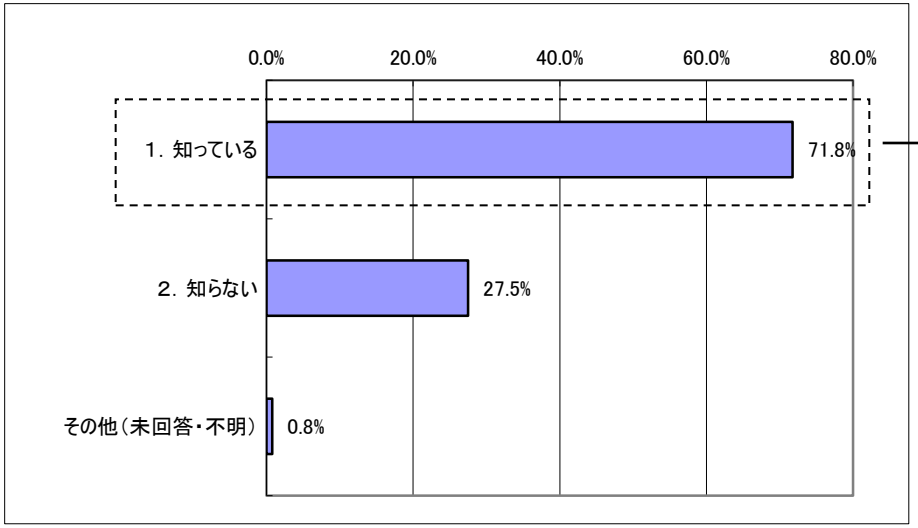
分野		既存調査				浸透状況等調査		
		有無	名称	調査基準日	調査周期	既存調査活用	調査対象範囲 ※既存調査活用する場合は、既存調査の範囲・数	アンケート配布数
情報通信	電気通信	なし				しない	固定系のネットワークインフラを設置する電気通信事業者、アクセス系の電気通信事業者、ISP事業者、携帯電話事業者等	68
情報通信	放送	なし				しない	日本放送協会及び地上系一般放送事業者	194
金融		あり	金融機関等のコンピュータシステムに関する安全対策状況調査	3月31日	1年毎	する	金融機関等	882
航空	航空運送	なし				しない	航空運送事業者	2
航空	航空管制	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	1,797
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）	51
物流		なし				しない	物流事業者	22

※既存調査の活用項目は、主な調査内容の①～③が対象

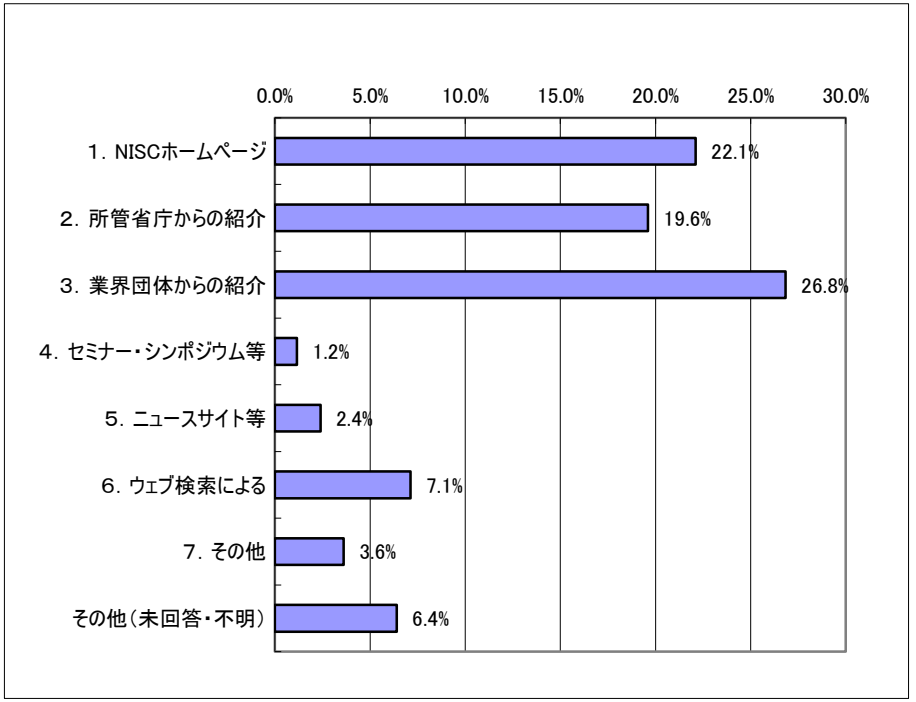
調査結果　①安全基準等の整備の状況に関する事項 (1/3)

- **2010年5月に改定された指針について、認識している事業者等は7割強であると推定**
- **指針の改定を認識していた事業者のうち、改定を知った手段は、業界団体からの紹介、NISCホームページ、所管省庁からの紹介が大半。**

(1)指針改定の認知度
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)改定を知った手段
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）

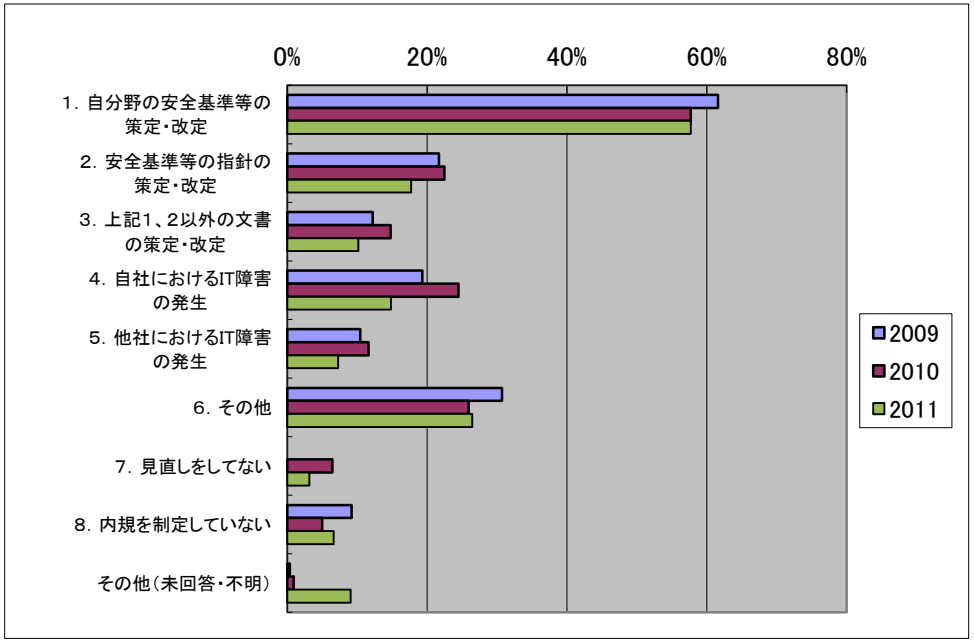
※要望の多かった順に記載

①担当者へのメールによる通知
②セミナーやシンポジウムの開催
③マスメディアを通じた広報
④所管省庁からの情報提供

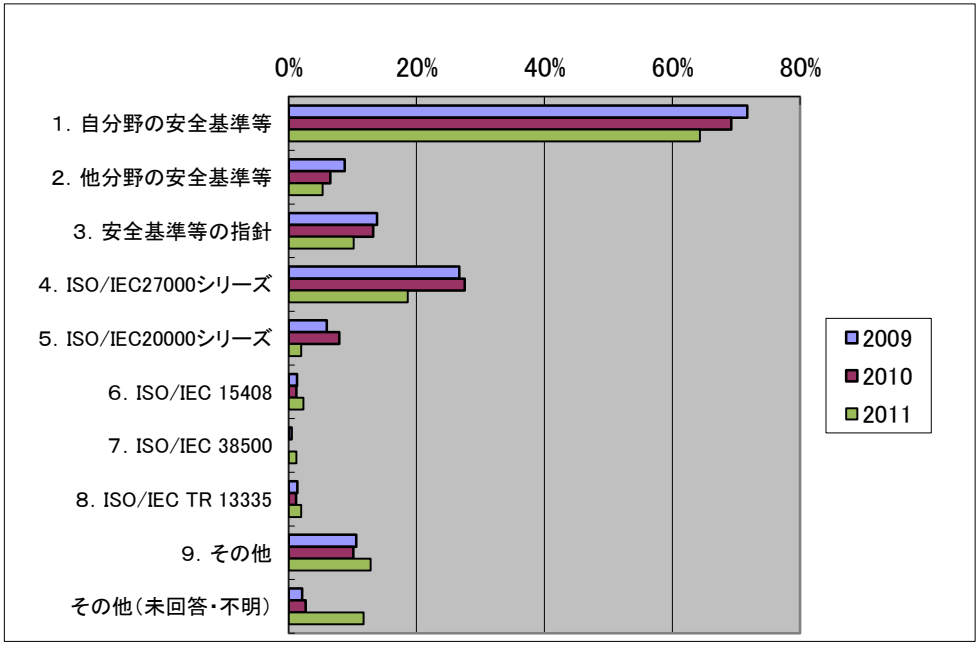
調査結果　①安全基準等の整備の状況に関する事項 (2/3)

- **内規見直しの契機としては、自分野の安全基準等が6割弱を占める。**
- **「その他（未回答・不明）」が増加しているのは、政府・行政サービスの既存調査結果を今年度調査より含めたため。**

(1) -1内規策定・見直しの契機
※項目7は2010年度より追加



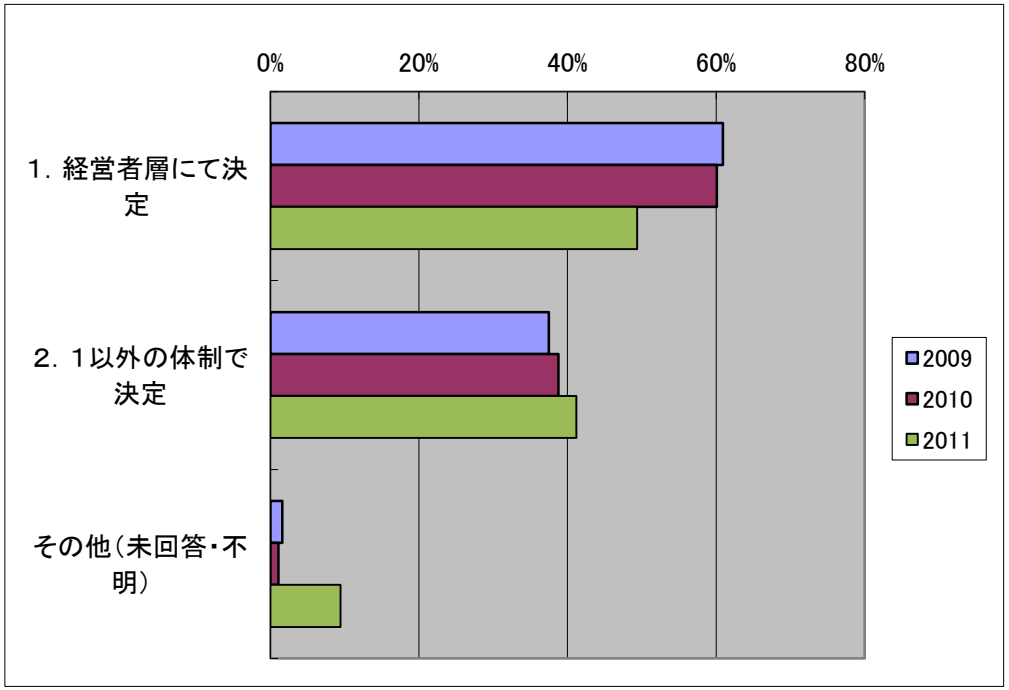
(2) 内規策定・見直しにあたり参考とする安全基準、規格等



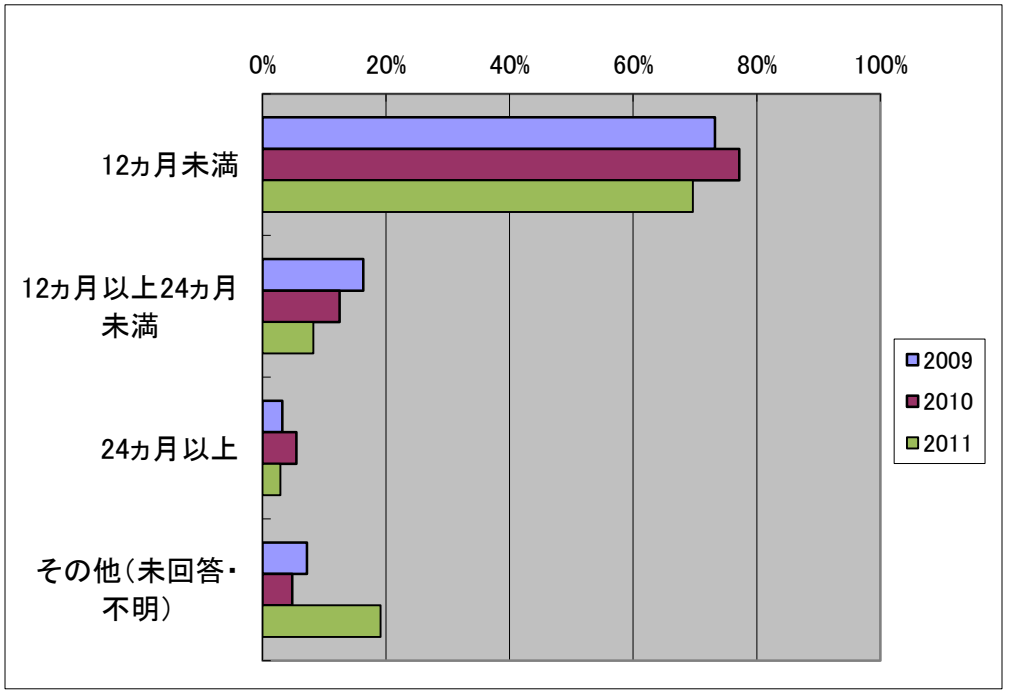
調査結果　①安全基準等の整備の状況に関する事項 (3/3)

- 内規の改定は、概ね１年未満で実施され、ほぼ半数の事業者では経営層にて決定されていると推定。
  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などによるものと推定。
- 「その他（未回答・不明）」が増加しているのは、政府・行政サービスの既存調査結果を今年度調査より含めたため。

(3) 内規改定を行う際の体制



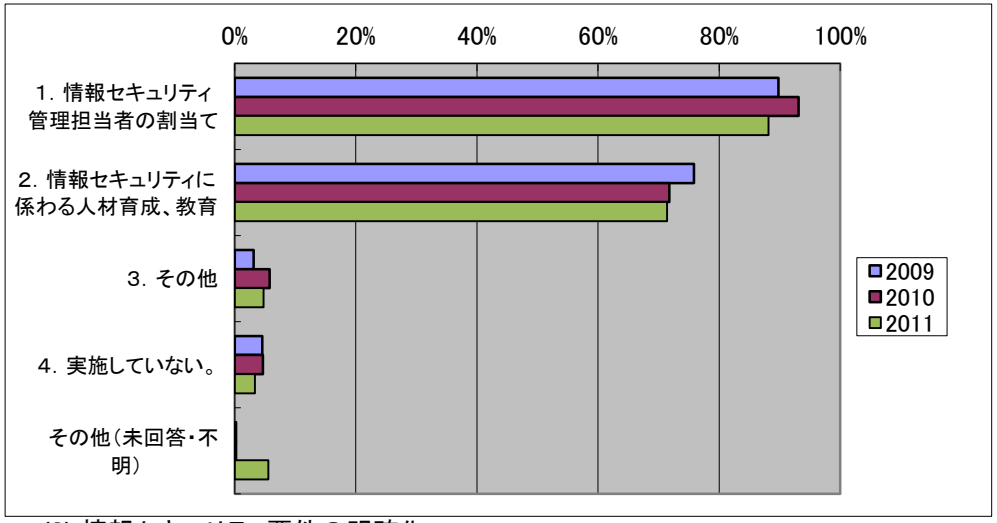
(4) 内規改定に要する期間
金融は読み替え可能項目なし（集計対象に含めず）



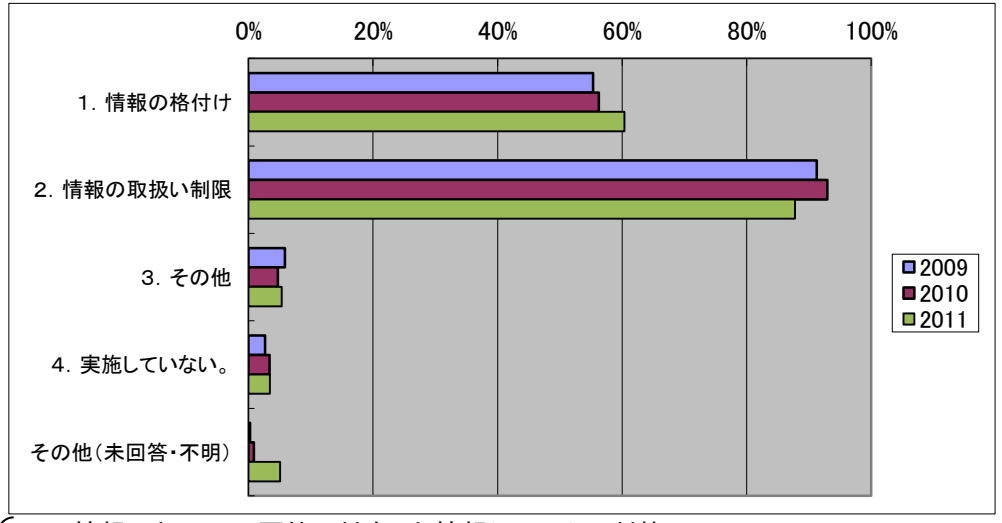
調査結果　②情報セキュリティ対策の実施状況に関する事項 (1/4)

- (1)～(3)について、対策を実施していない事業者は減少傾向。
- 情報セキュリティ要件を明確化している事業者では、情報システムの個々対策の実施率が上昇。

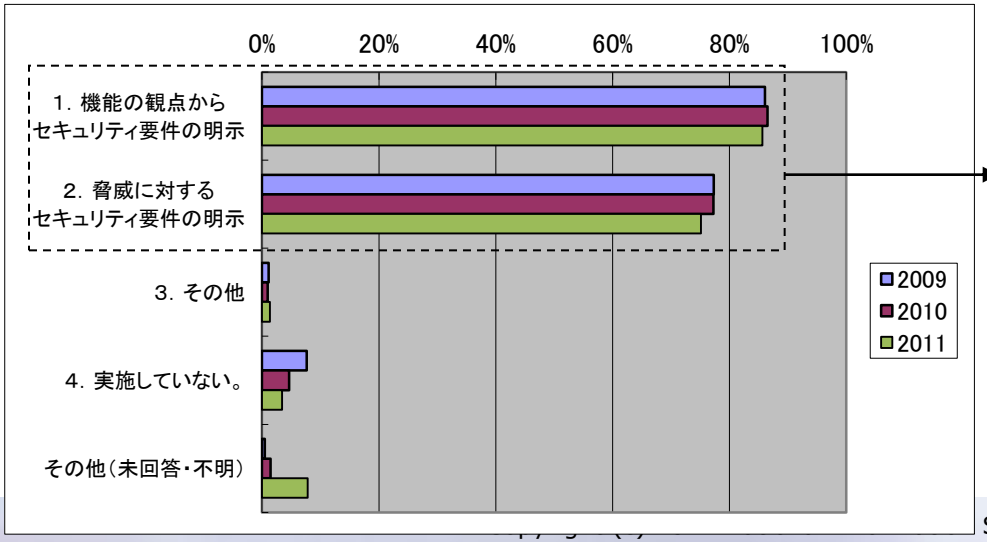
(1) 組織・体制及び資源の確保に関する対策



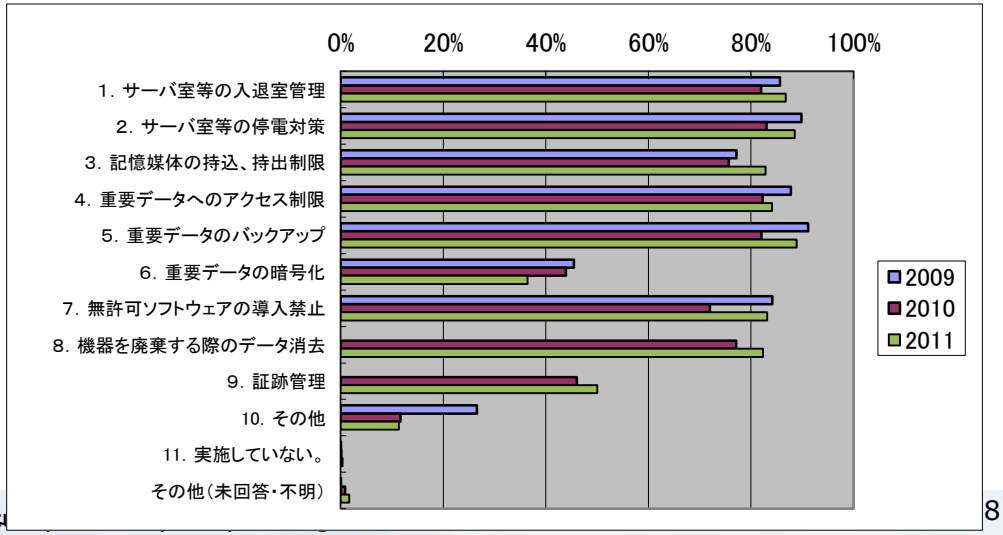
(2) 情報についての対策



(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）



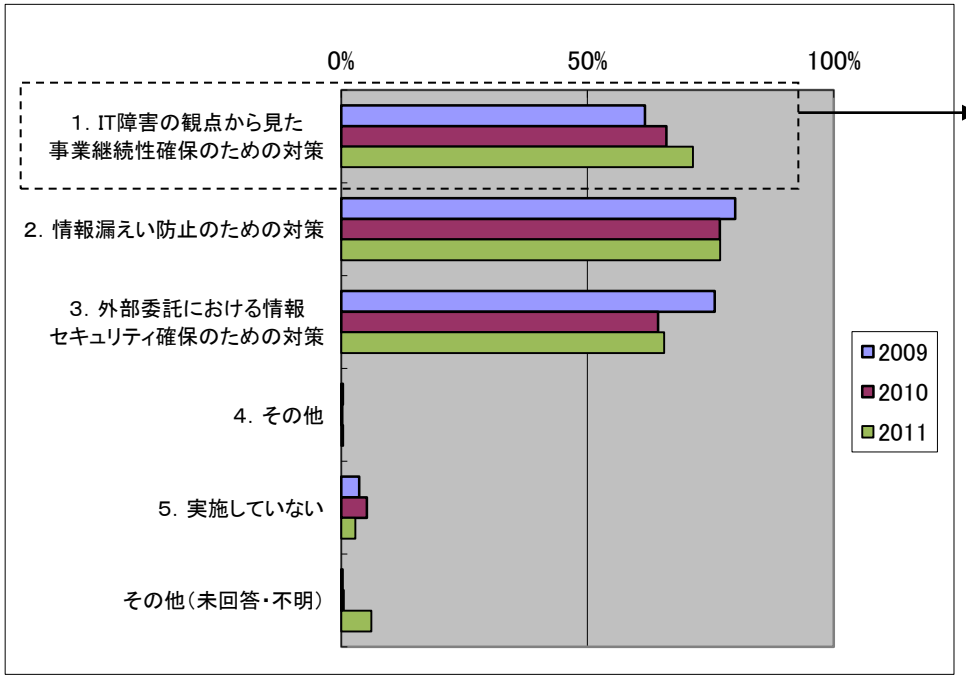
(4) 情報セキュリティ要件に対応した情報システムの対策
※項目8，9は2010年度に追加



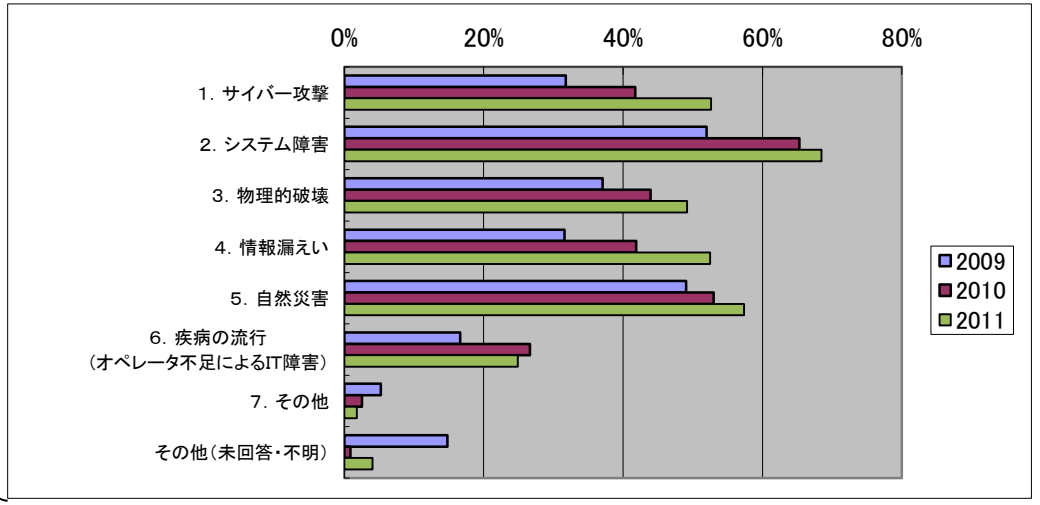
調査結果　②情報セキュリティ対策の実施状況に関する事項 (2/4)

- **IT障害の観点から見た事業継続性確保のための対策を実施している事業者が増加し、対象とする脅威全般の比率も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。**
- **一方、事業継続計画の策定状況については、今回より前問(５)の1との関連をなくしたことで、若干傾向に変化があるものの、全体としては前年と同じ傾向。**

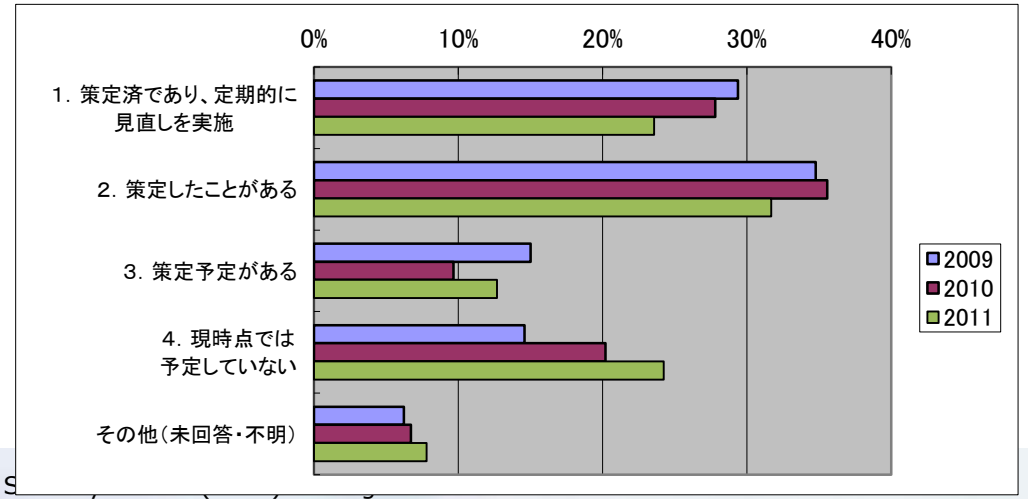
(5) 情報セキュリティ対策の運用に関する対策



(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



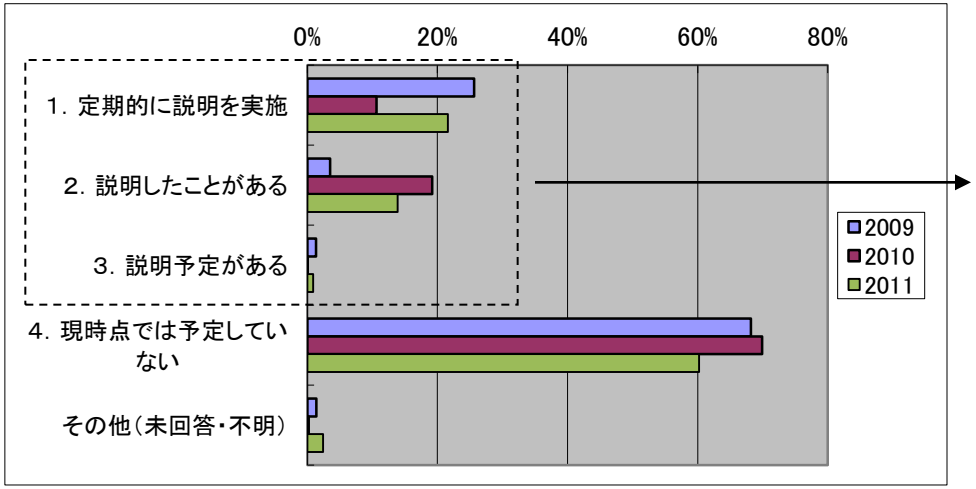
(7) 事業継続計画の策定状況



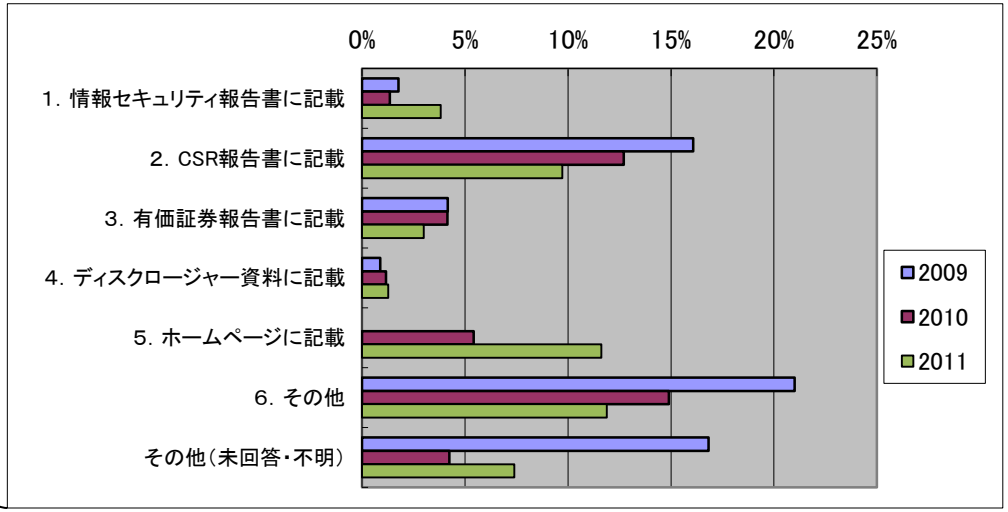
調査結果　②情報セキュリティ対策の実施状況に関する事項 (3/4)

- **情報セキュリティ対策の対外的な説明に関して、定期的な説明を実施している事業者が増加し、説明予定のない事業者が減少している。また、説明方法において、情報セキュリティ報告書、ホームページに記載する事業者が増加している。**
- **7割弱の事業者で、IT障害時の情報提供に関する方策を内規に明示。**

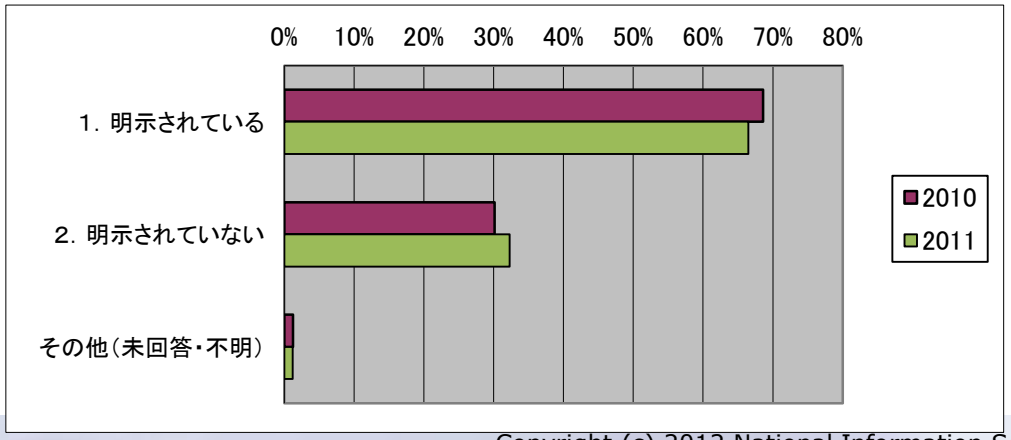
(8) 情報セキュリティ対策の対外的な説明の状況
政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



(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）



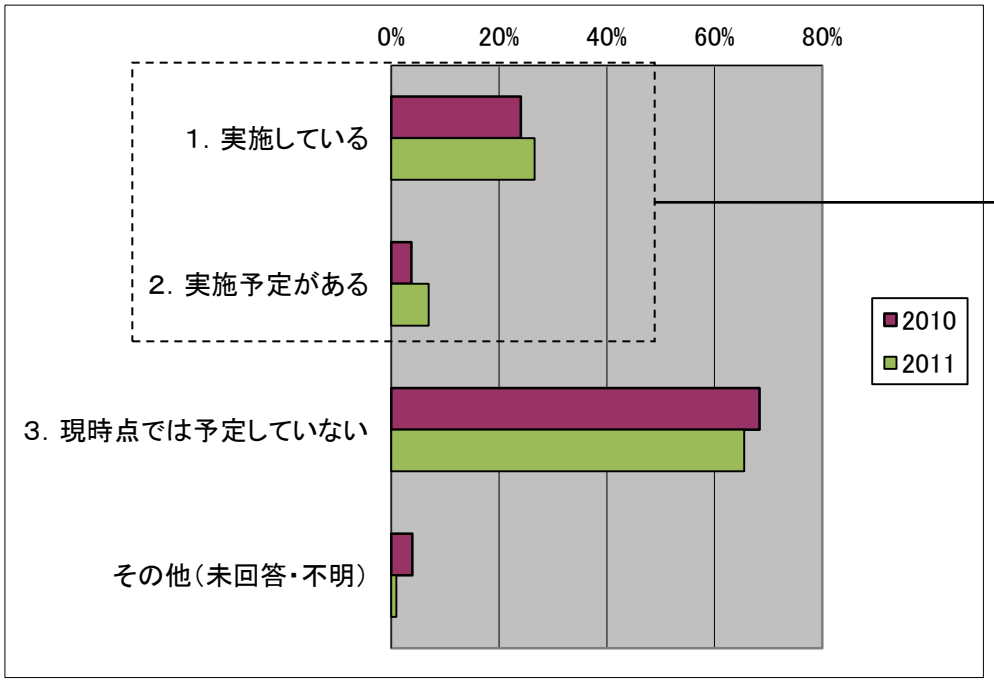
(10) IT障害時のユーザへの情報提供の方策
金融、政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



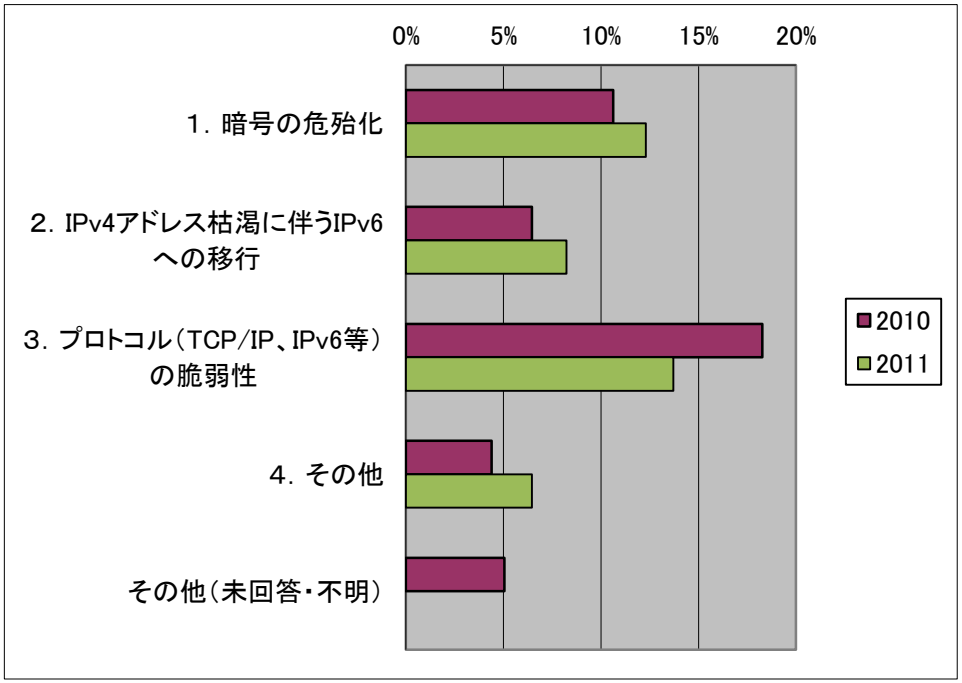
調査結果　②情報セキュリティ対策の実施状況に関する事項 (4/4)

- **ITに係る環境変化に伴う脅威に関しては対策を実施している(予定含む)事業者が4割弱と推定。**
- **暗号の危殆化、IPv6移行を脅威に想定する事業者が増加。その他としては、コンピュータウィルス、ソフトウェアの脆弱性を脅威に想定する事業者が多かった。**

(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)



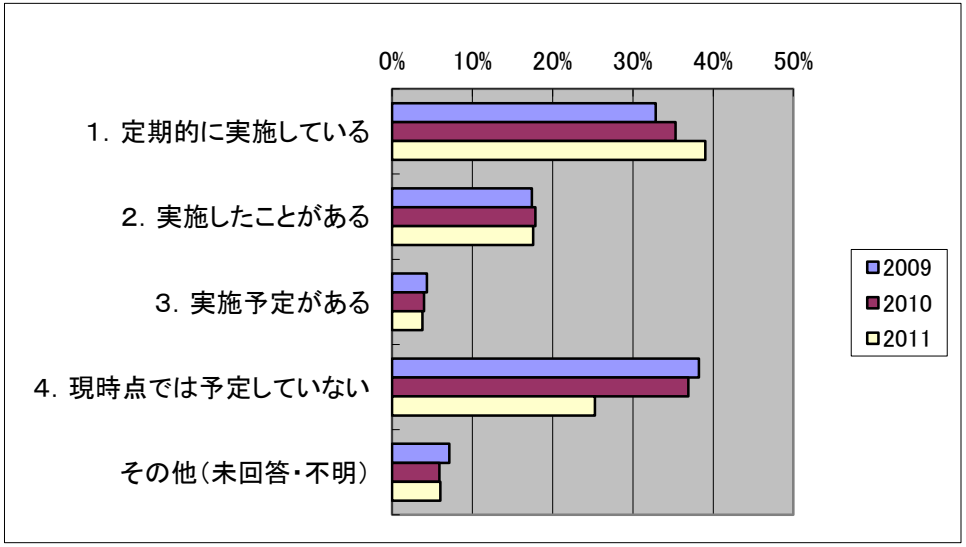
(12) 想定する脅威
政府・行政サービスは 読み替え可能項目なし(集計対象に含めず)



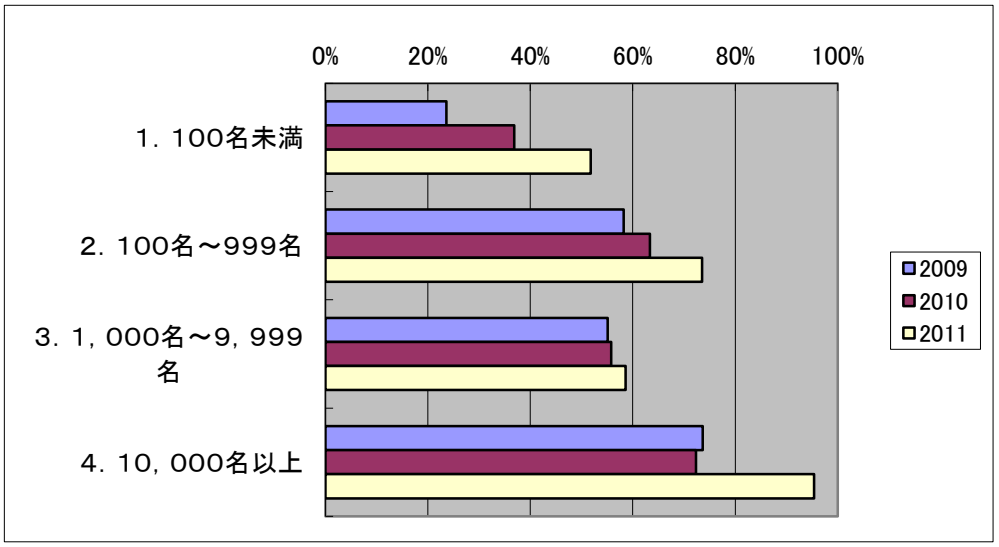
調査結果　③安全基準等に対する準拠状況に関する事項 (1/4)

- **自己点検の実施状況は、定期的に実施している事業者が増加。予定を含む実施割合は6割と推定。**

(1) 自己点検の実施



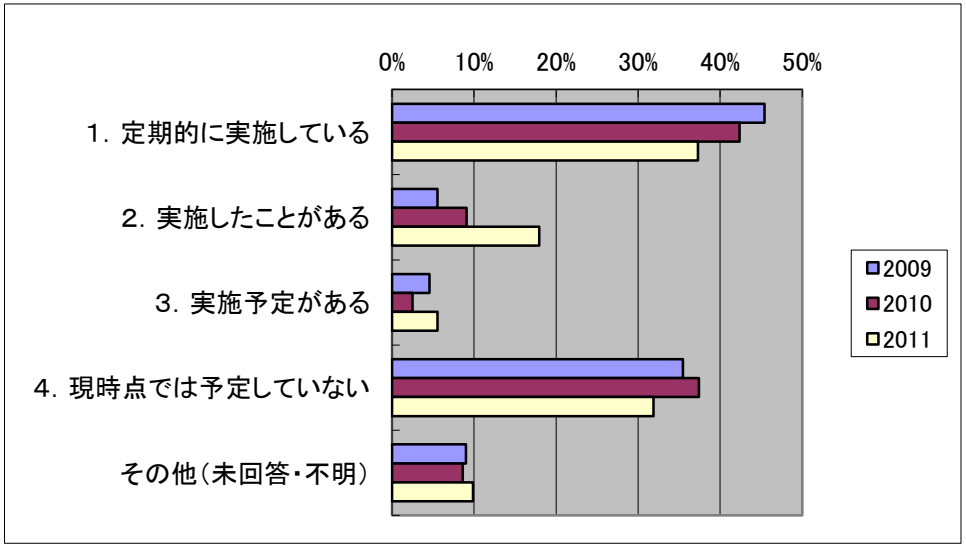
自己点検の事業規模ごとの実施割合（予定含む）



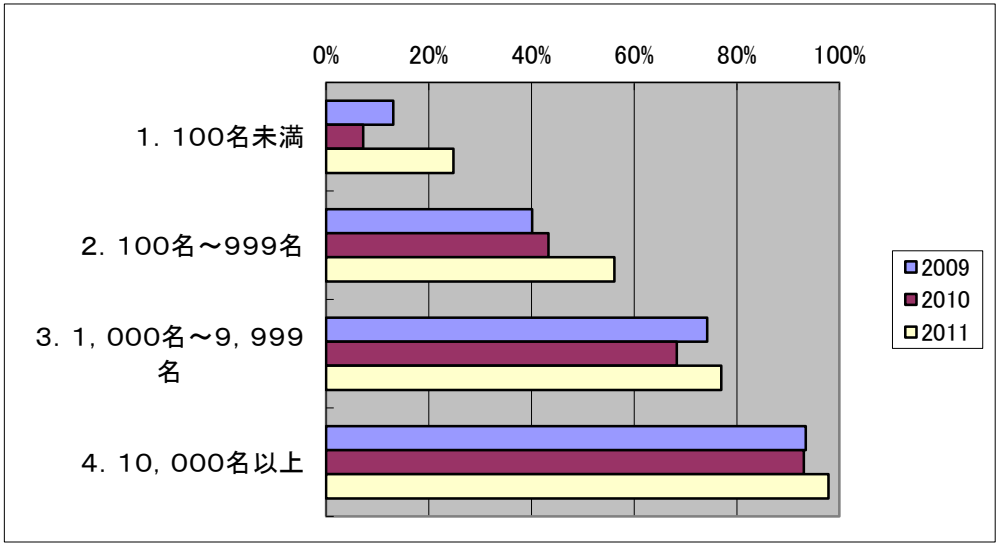
調査結果　③安全基準等に対する準拠状況に関する事項 (2/4)

- **演習・訓練の実施状況は、実施したことがある事業者が増加。予定を含む実施割合は6割と推定。**

(2)演習・訓練の実施



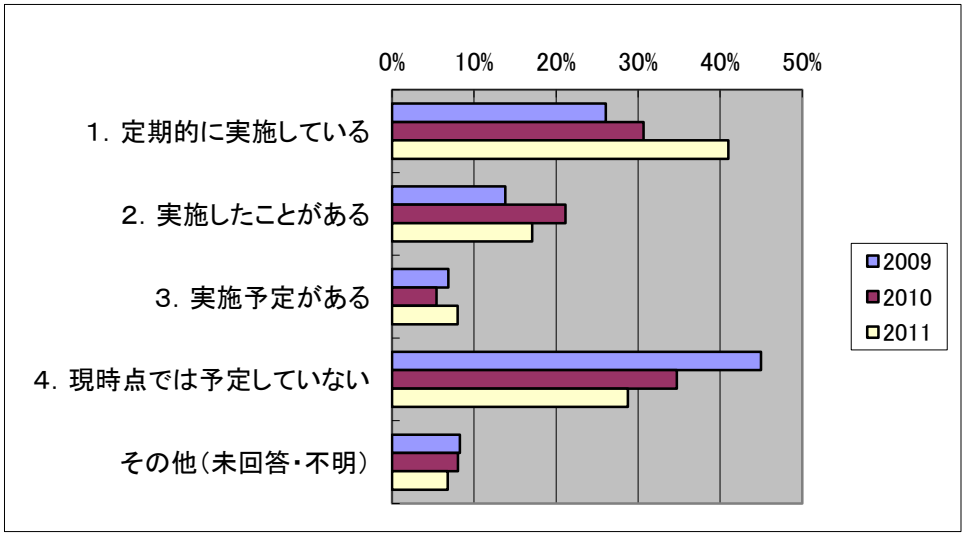
演習・訓練の事業規模ごとの実施割合（予定含む）



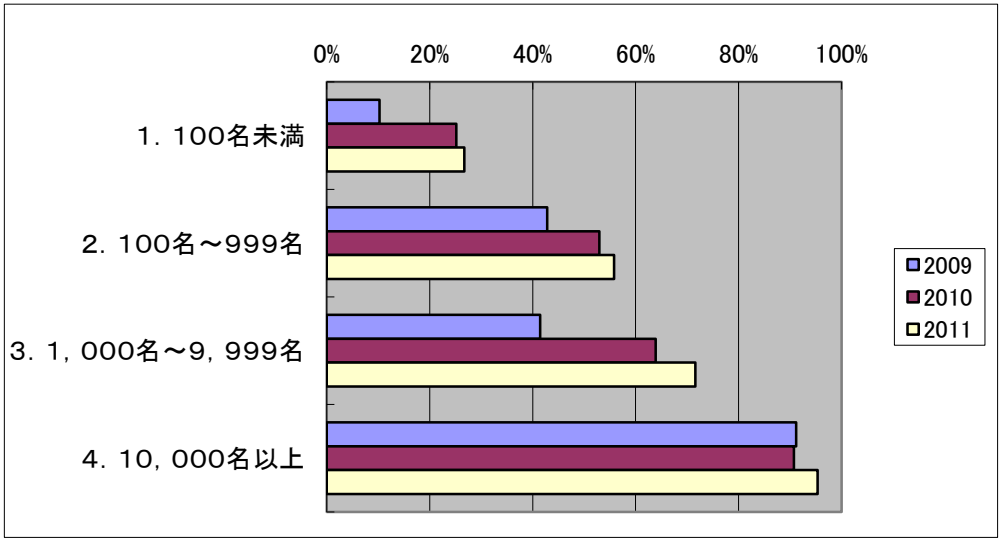
調査結果　③安全基準等に対する準拠状況に関する事項 (3/4)

- **内部監査を定期的に実施している事業者が増加し、予定を含む実施割合は6割強と推定**

(3) 内部監査の実施



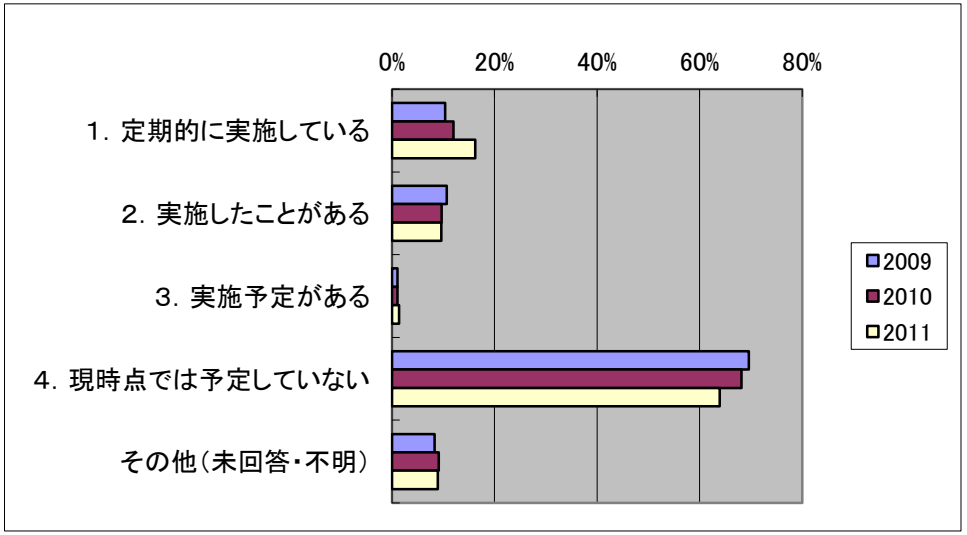
内部監査の事業規模ごとの実施割合（予定含む）



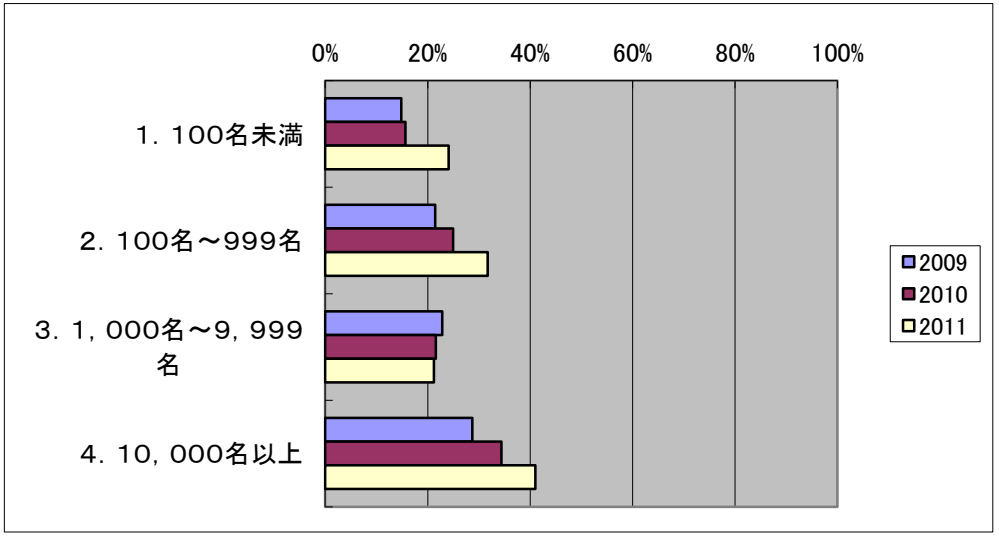
調査結果　③安全基準等に対する準拠状況に関する事項 (4/4)

- **外部監査の実施状況は増加傾向であるが、予定を含む実施割合は3割弱程度。費用のかかる事業者外部の監査機関の利用は自己点検、内部監査と比べて少ないものと推定。**

(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、チェックシート、説明冊子の作成に関するものが多い。**
- **安全基準等に対する意見としては、各分野、業種の実態に合った基準、企業規模のレベルにあった基準への要望が多い。**

1. 安全基準等の指針に対して
   ① チェックシート等があるとさらに有意義なものになると思う。
   ② 必要な実施項目について説明された冊子があれば、スムーズに取り組めるのではないか。
   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 各業態や業種によってリスクに差異があると思われるので、実態に合った基準が欲しい。
   ② 企業の規模や業種でレベルを勘案し、具体的な対策例や被害があった場合の重大性を示したほうがいいと思う。
   ③ サービスの事業性、採算性を含めて、信頼性、安全性の処置を講じるため、むやみに安全基準等の強化を一方的に決定することがないよう留意いただきたい。

※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)

- **自由意見については、一定の水準を保つためのセキュリティ対策費用の助成、情報セキュリティ人材の育成支援等、運用に関する要望が多く、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）

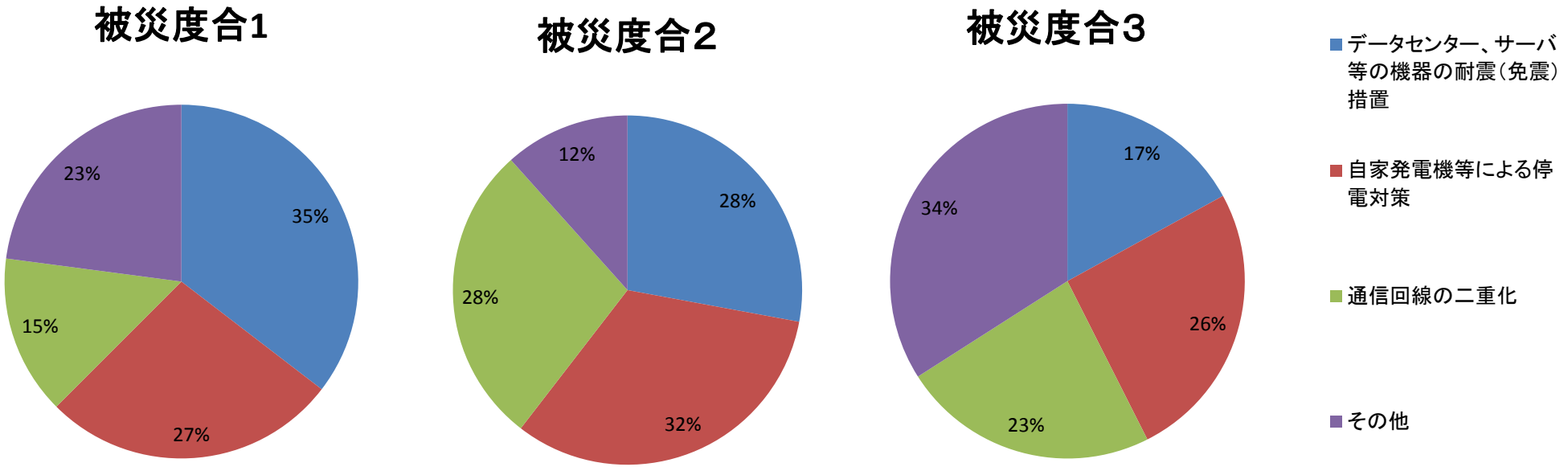
① 情報セキュリティに関して、一定の水準を保つよう義務付けるとともに、セキュリティ費用等における助成の検討をお願いしたい。
② IT人材育成のための支援を行ってほしい。
③ サイバー攻撃の場合は、被害者であるだけでなく間接的加害者になりかねないので、もう少し拘束力のある指針や規則が必要と思う。
④ 情報セキュリティ相談窓口を設置してほしい。
⑤ 専門知識を有する人材が非常に不足している。
⑥ 情報セキュリティ管理者育成のための教育制度を望む。
⑦ 指針や安全基準等の改定が行われた場合の周知の工夫をしてほしい。

※金融、政府・行政サービスは、調査対象外

調査結果　⑤東日本大震災における事業継続性確保の対策の効果(1/3)

1. 有効に機能した対策

- **データセンター・サーバ等の機器の耐震(免震)措置については、被災度合の大きい事業者ほど有効に機能したと回答している。**
- **自家発電機等による停電対策は、被災度合によらず一定の回答があった。被災度合3の回答は、計画停電に対するものと推定される。**
- **直接被災地域(被災度合1)以外では、通信回線の二重化がより有効に機能したと推定される。**

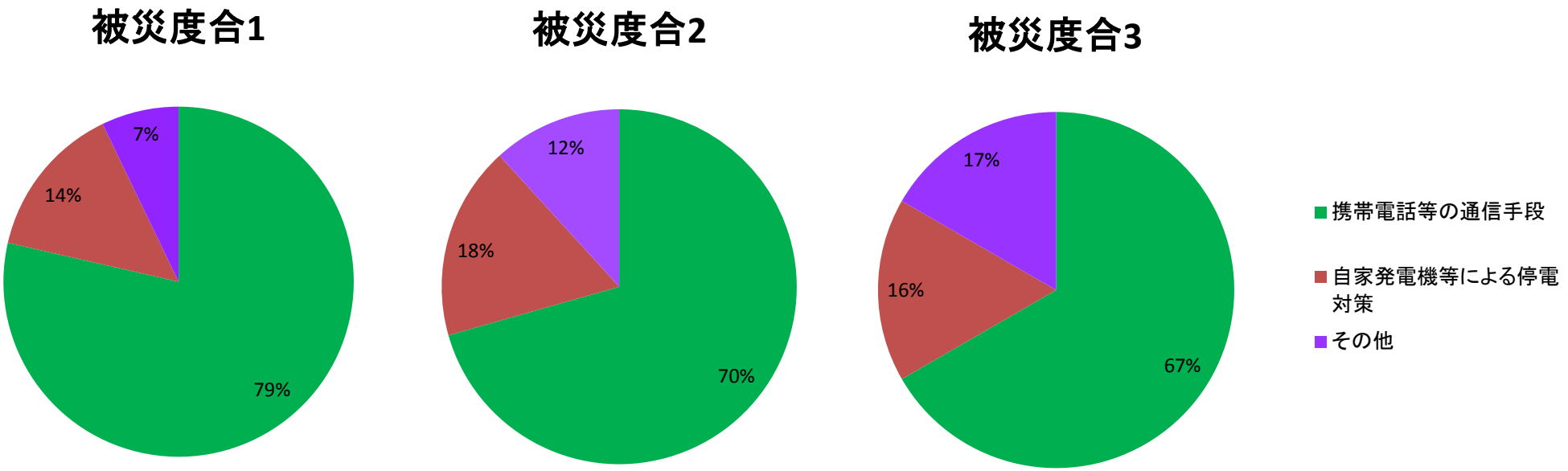


被災度合1:直接被災した
被災度合2:直接被災はしていないが、間接的な影響を受けた
被災度合3:大きな影響はなかった

※金融、政府・行政サービスは、調査対象外

2. 有効に機能しなかった対策

- **有効に機能しなかった対策としては、いずれの被災度合についても、携帯電話等の通信手段に関するものが多かった。**
- **自家発電機等による停電対策と回答したのは、バッテリーの持続時間や燃料備蓄分が停電時間を超過したことによるものと推定される。**



被災度合１：直接被災した
被災度合２：直接被災はしていないが、間接的な影響を受けた
被災度合３：大きな影響はなかった

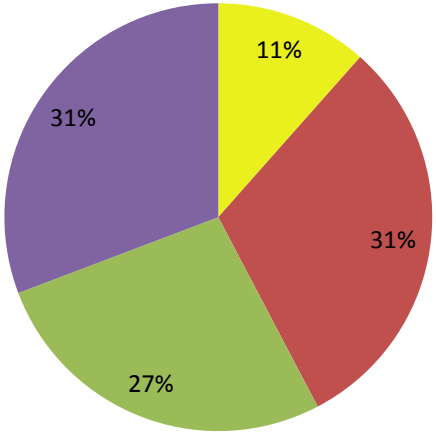
※金融、政府・行政サービスは、調査対象外

調査結果　⑤東日本大震災における事業継続性確保の対策の効果(3/3)

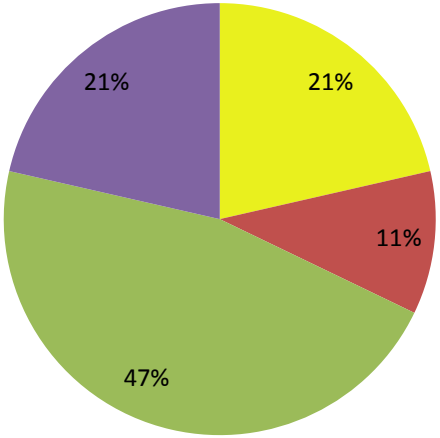
3. 今後追加すべき対策

- **被災度合1、2で、衛星携帯電話等の通信手段の多様化の回答が多かったのは、被災地では電力の復旧よりも通信の復旧に時間を要したことが原因と推定される。**
- **被災度合1、2では、自家発電機等による停電対策と携帯電話等の通信手段の多様化を足したものの比率が高い。被災地では、ライフラインの維持を強く意識していることによるものと推定される。**
- **被災度合3で、携帯電話等の通信手段の多様化の回答が少ないのは、通信手段途絶の今回の震災における体験の差と推定される。**

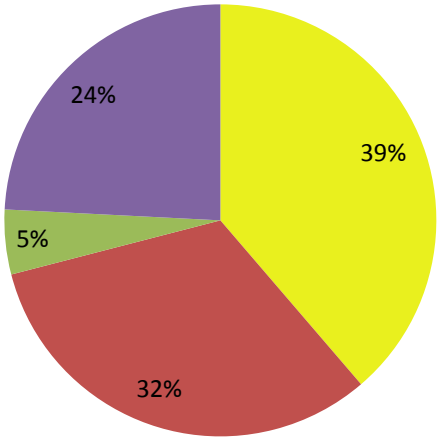
被災度合1

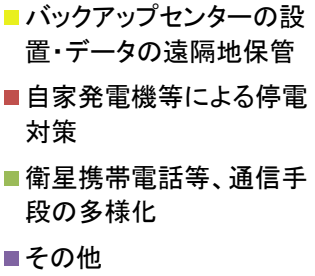


被災度合2



被災度合3





被災度合1：直接被災した
被災度合2：直接被災はしていないが、間接的な影響を受けた
被災度合3：大きな影響はなかった

※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

- 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（93．5%）は若干上昇（＋1．0%）しており、本件調査が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セキュリティの個別対策の実施率が増加しており、安全基準等に沿ったセキュリティ対策の浸透が推定される。

≪さらなる情報セキュリティ対策の拡充に向けて≫

- 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で実施し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より増加しており、NISCにおける分野横断的演習と連携して引き続き普及・啓発を図る。
- 対策実施において参考とするチェックリスト、説明冊子等に関する要望が多いため、指針対策編等の周知方法を検討する。

- 次回調査においては、東日本大震災において得られた課題・教訓を受け、安全対策・業務継続対策の浸透状況に変化があるものと思料する。
- 今後も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） 昨年、指針が改定されたのをご存知ですか。
（2） 指針が改定されたこと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)

【⑤ 東日本大震災における情報システムの事業継続性確保に関する対策の効果について】
（1） どのような影響をうけましたか。
（2） 情報システムに関する事業継続性確保のための対策について、今回の震災にあたり、以下に該当するものをご記入ください。
　　有効に機能した対策・機能しなかった対策・今後追加すべきと感じた対策