資料３－２

NISC National Information Security Center

2012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3月26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2012」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

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）
	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）	

2006年度に策定・見直しを行った安全基準等を対象

毎年一定時期に定点調査

毎年一定時期に定点調査

SJ：セキュアジャパン
JS：情報セキュリティ

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。

情報セキュリティ2012

・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〉

2012 年度に「安全基準等」の浸透状況、震災を踏まえた改善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	：	2012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 ： 2012年4月～2012年6月
とりまとめ ： 2012年10月～2012年11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・対策編の認知度、知った手段
- 内規策定・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

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3,140事業者等に対し、2,928事業者等からアンケートを回収
（回収率 93．2%、前年比　-0.3%）
- 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ことから、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	79	28
	放送	しない	日本放送協会及び地上系一般放送事業者	193	184
金融		する	金融機関等	921	789
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	1,784	1,784
医療		しない	医療機関（病院抽出）	50	43
水道		しない	水道事業体（事業者抽出）	45	45
物流		しない	物流事業者	21	8
全分野合計				3,140	2,928

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（2012年度実績）

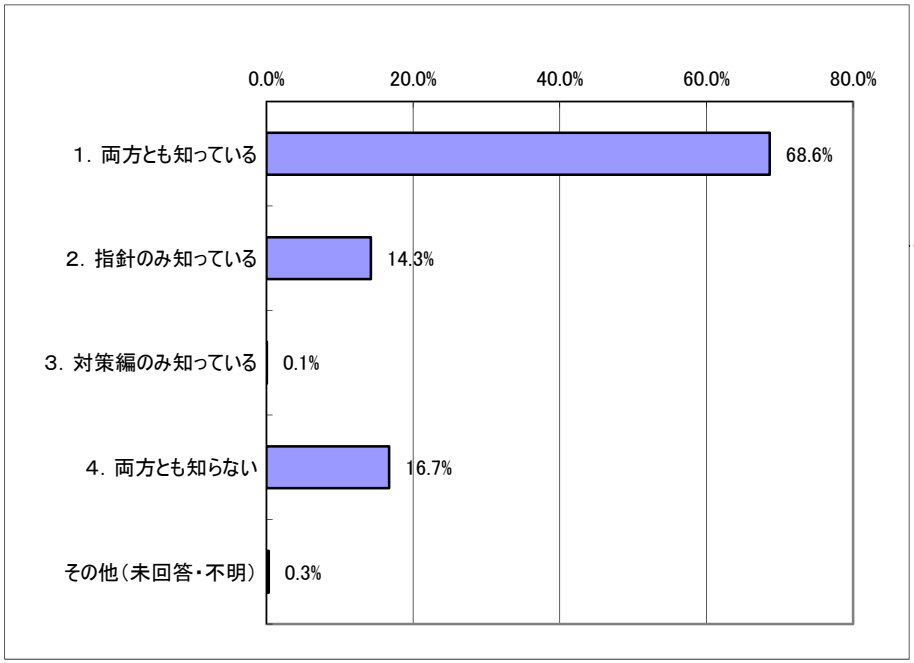
分野		既存調査				浸透状況等調査		
		有無	名称	調査基準日	調査周期	既存調査活用	調査対象範囲 ※既存調査活用する場合は、既存調査の範囲・数	アンケート配布数
情報通信	電気通信	なし				しない	固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等	79
情報通信	放送	なし				しない	日本放送協会及び地上系一般放送事業者	193
金融		あり	金融機関等のコンピュータシステムに関する安全対策状況調査	3月31日	1年毎	する	金融機関等	921
航空	航空運送	なし				しない	航空運送事業者	2
航空	航空管制	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	1,784
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	21

※既存調査の活用項目は、主な調査内容の①～③が対象

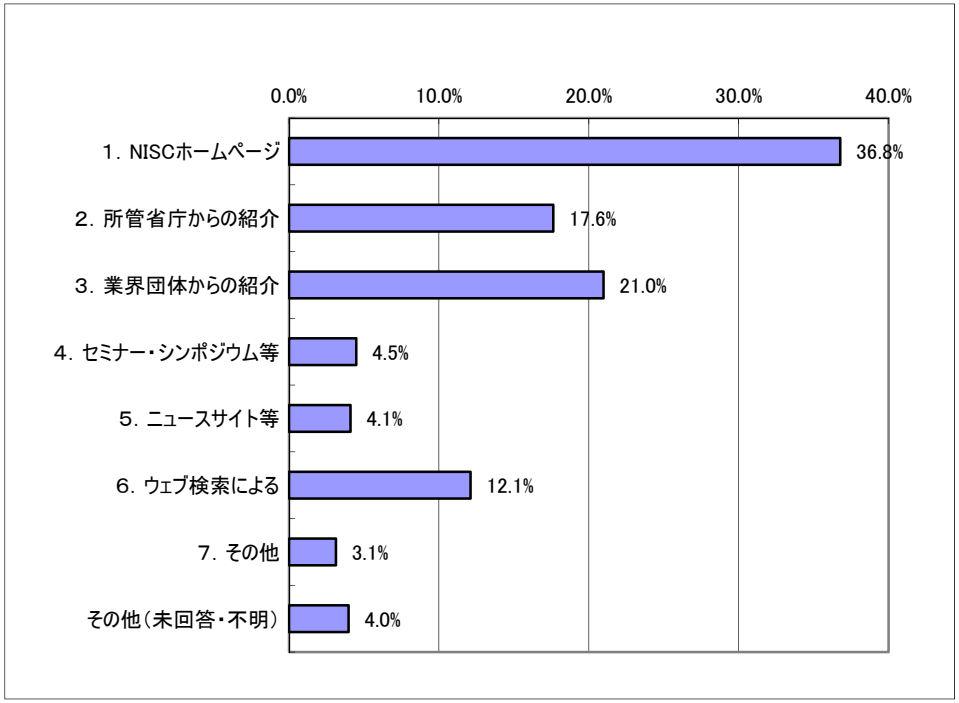
調査結果　①安全基準等の整備の状況に関する事項 (1/3)

- **指針について、認識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、NISCホームページが一番多く、業界団体からの紹介、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）



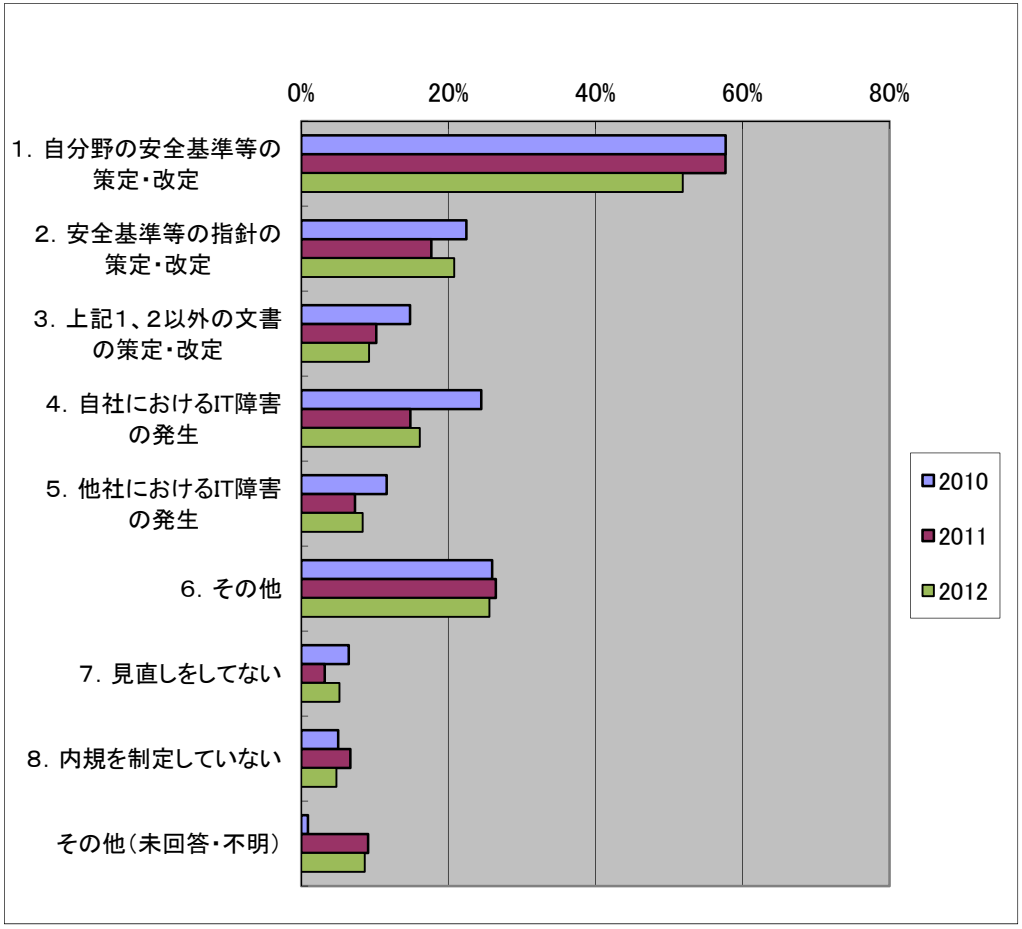
3)効果的に周知する手段
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）
※要望の多かった順に記載

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

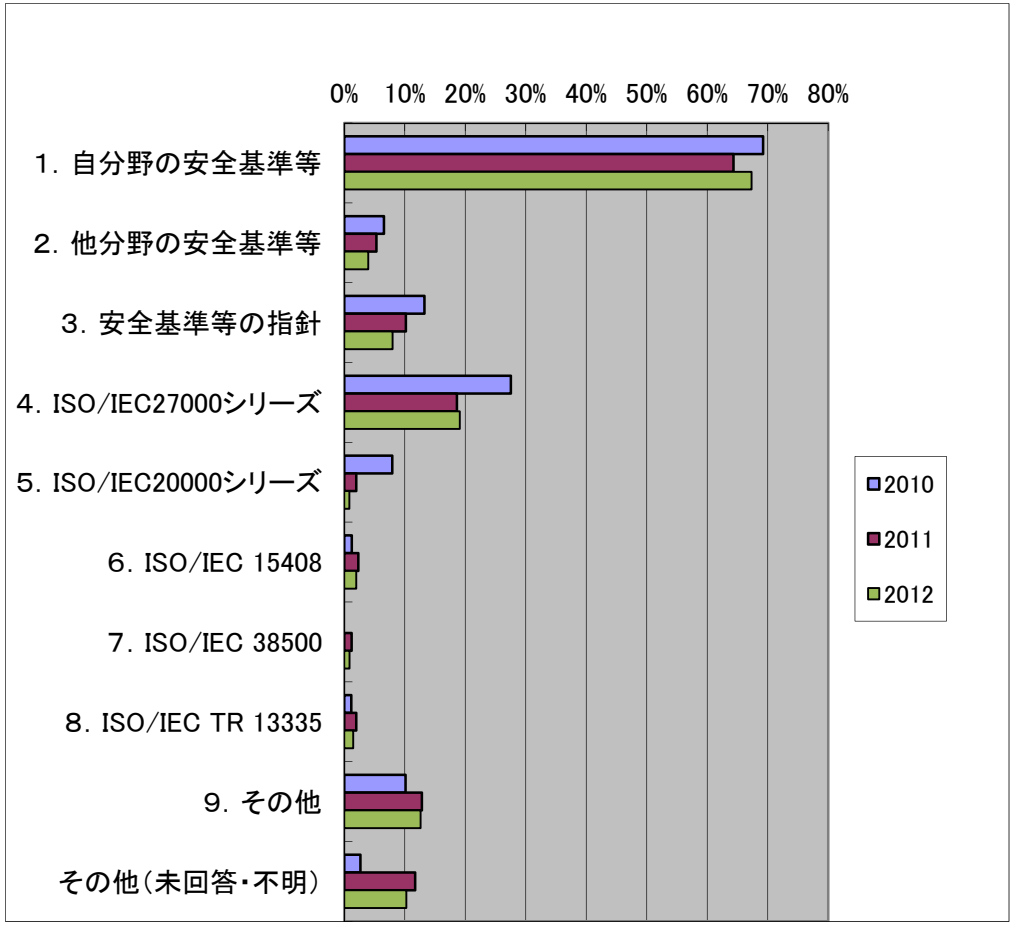
調査結果　①安全基準等の整備の状況に関する事項 (2/3)

- **内規策定・見直しの契機としては、自分野の安全基準等が約5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7割弱を占める。**

(1) 内規策定・見直しの契機



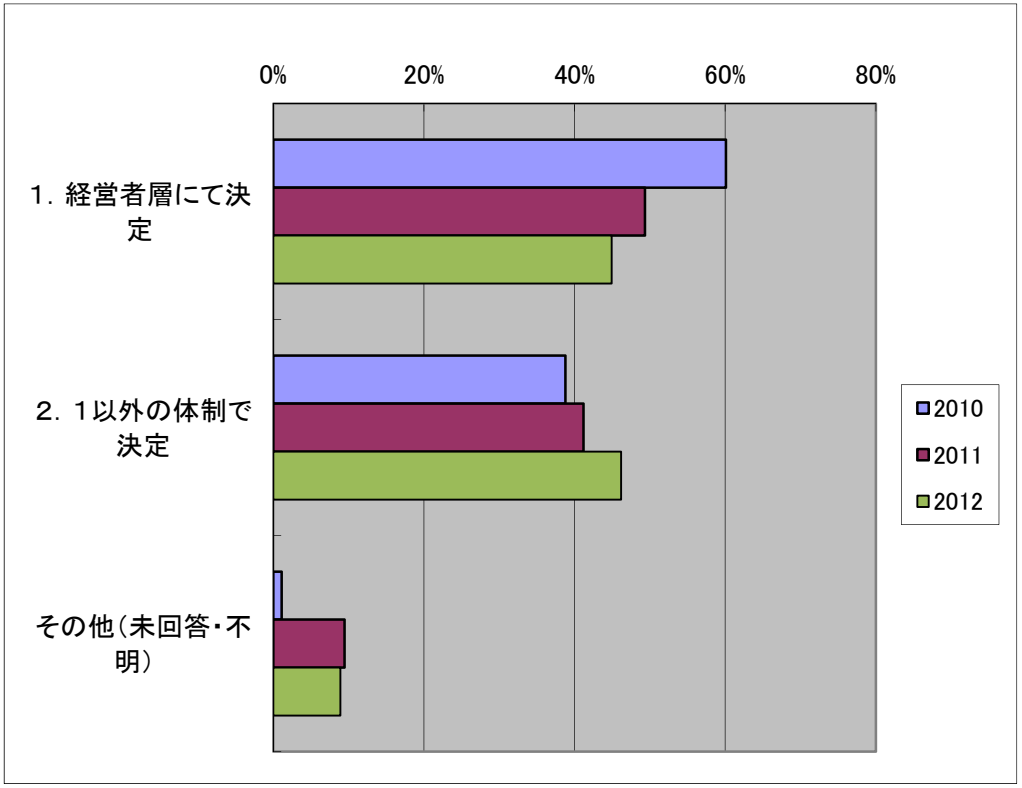
(2) 内規策定・見直しにあたり参考とする安全基準、規格等



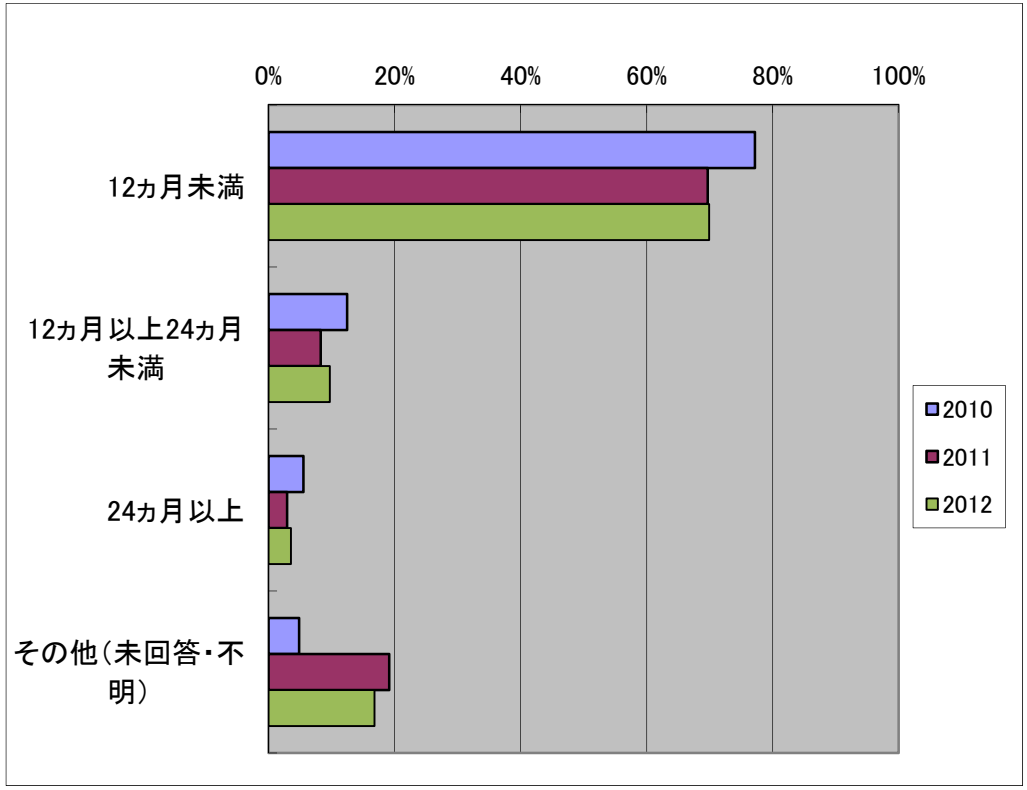
調査結果　①安全基準等の整備の状況に関する事項 (3/3)

- **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などによるものが大半。
- **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



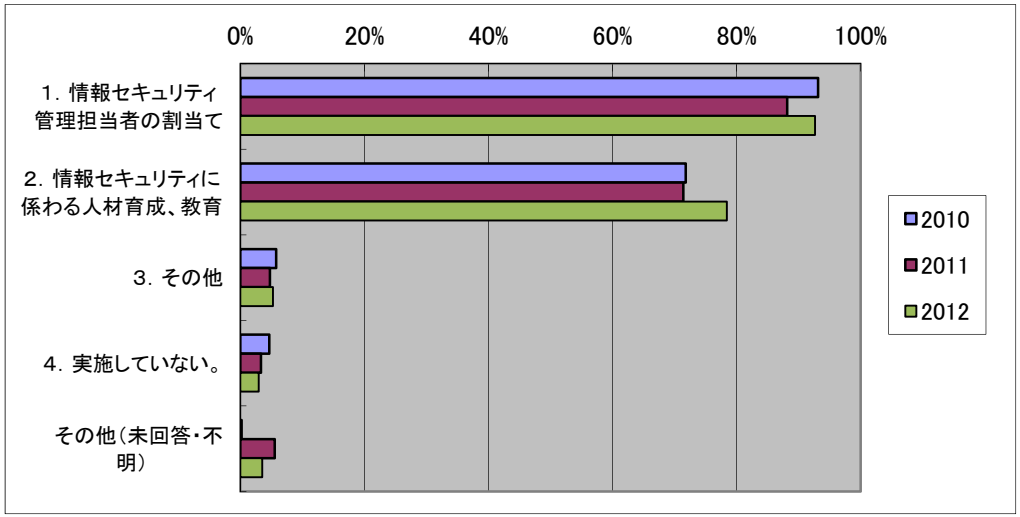
(4) 内規改定に要する期間
金融は読み替え可能項目なし（集計対象に含めず）



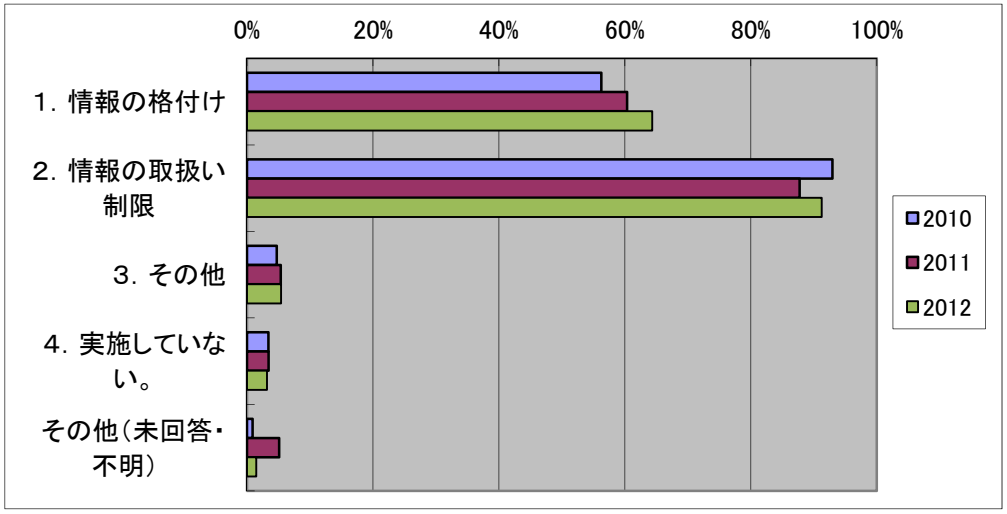
調査結果　②情報セキュリティ対策の実施状況に関する事項 (1/4)

- (1)～(4)について、昨年度に比べて対策の実施率が全体的に増加している。

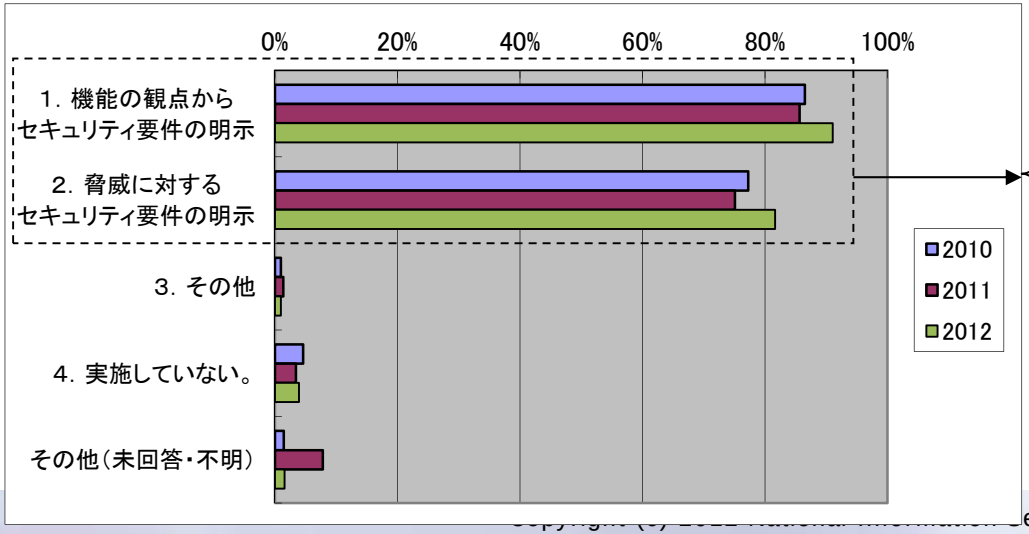
(1) 組織・体制及び資源の確保に関する対策



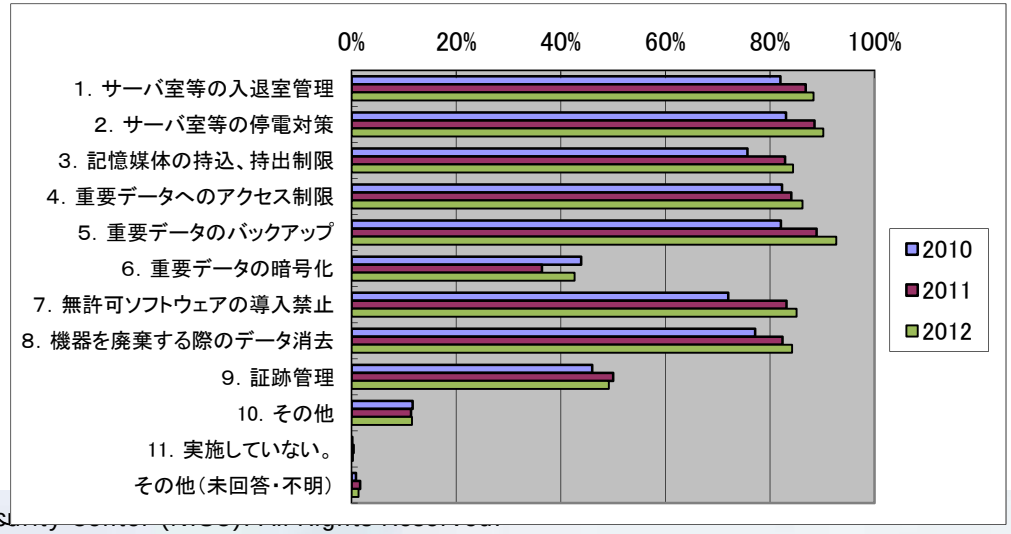
(2) 情報についての対策



(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）



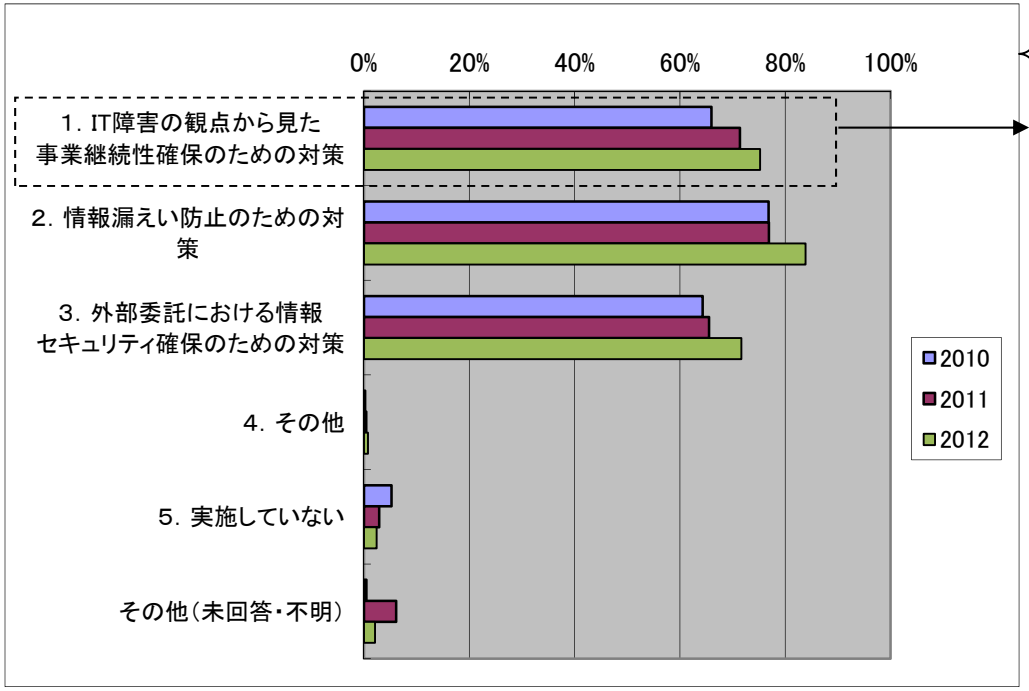
(4) 情報セキュリティ要件に対応した情報システムの対策



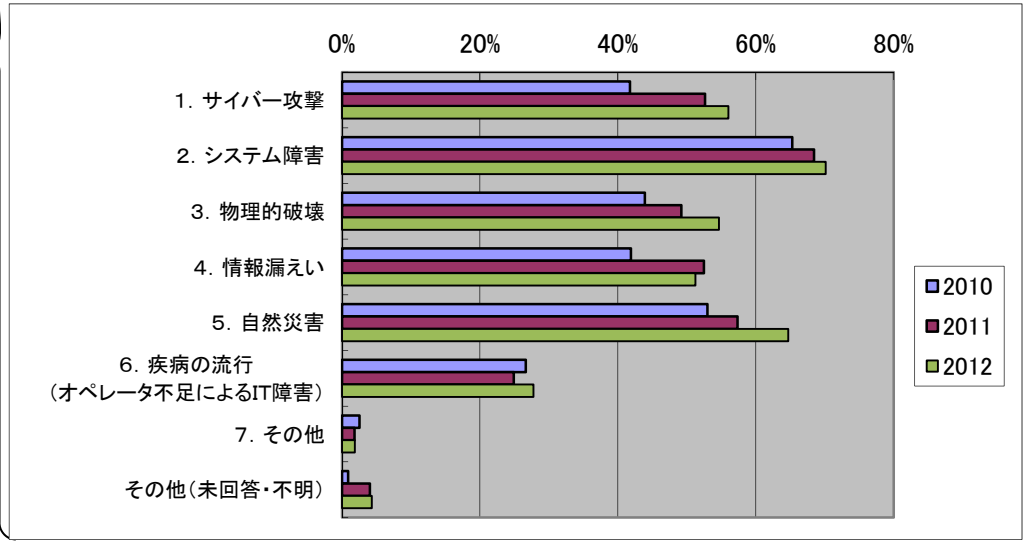
調査結果　②情報セキュリティ対策の実施状況に関する事項 (2/4)

- **事業継続性確保のための対策に関して、対象とする脅威として、物理的破壊、自然災害の比率が高まっている。東日本大震災を受けて、それらを脅威の対象とする事業者等が増加していることが推定される。**
- **事業継続計画の策定状況については、策定済みであり、定期的に見直しを実施している、また策定予定があるとした事業者等が増加している一方で、2割強の事業者等が依然として策定予定がないと回答。**

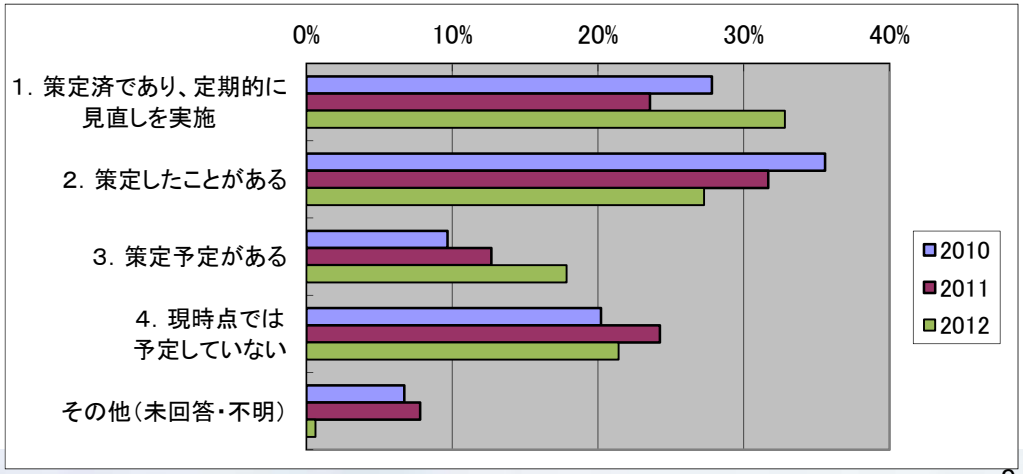
(5) 情報セキュリティ対策の運用に関する対策



(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



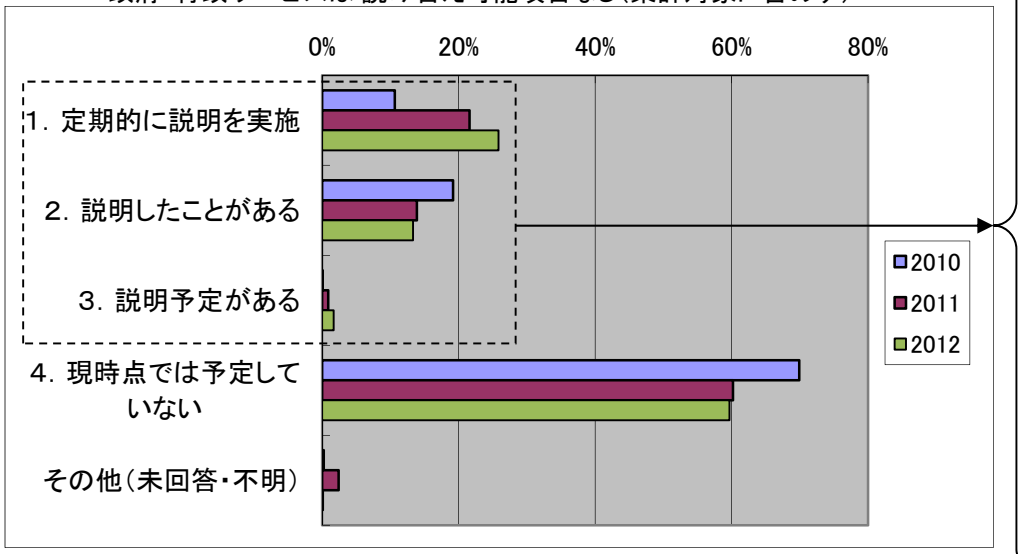
(7) 事業継続計画の策定状況



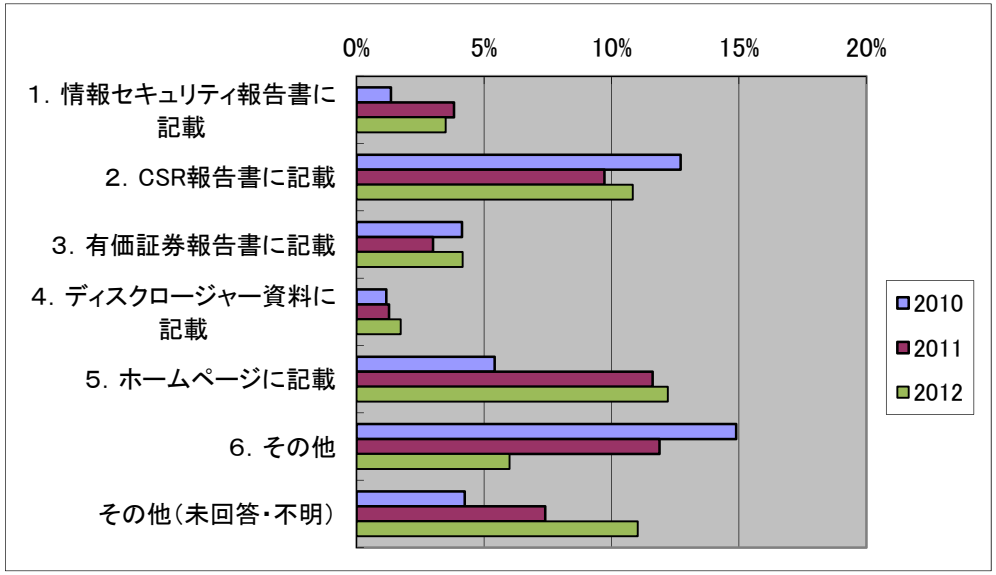
調査結果　②情報セキュリティ対策の実施状況に関する事項 (3/4)

- **情報セキュリティ対策の対外的な説明に関して、定期的に説明を実施している事業者等が増加している。また、説明方法において、CSR報告書、ホームページに記載している事業者等が多い。**
- **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。**

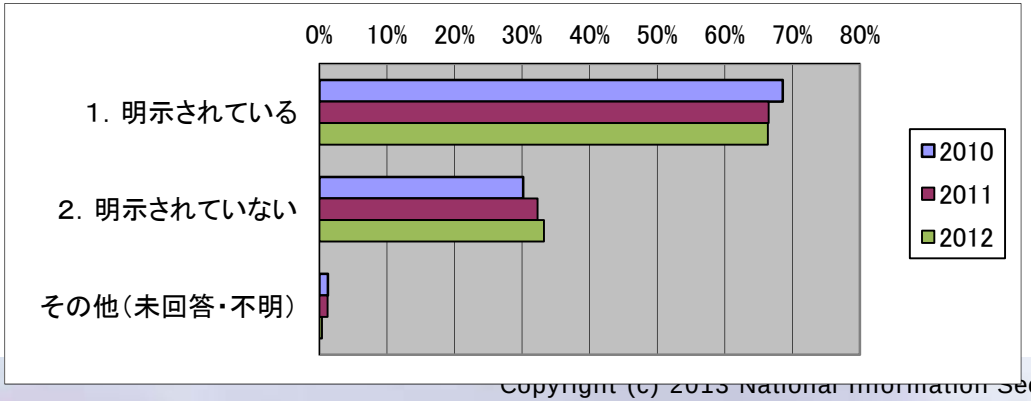
(8) 情報セキュリティ対策の対外的な説明の状況
政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



(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）



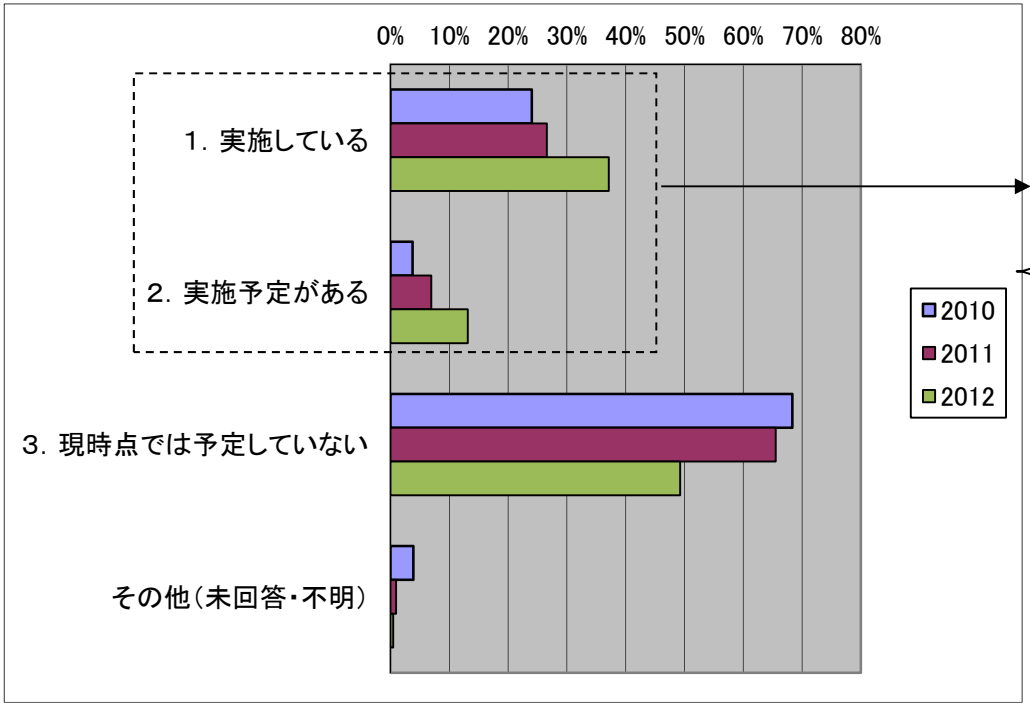
(10) IT障害時のユーザへの情報提供の方策
金融、政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



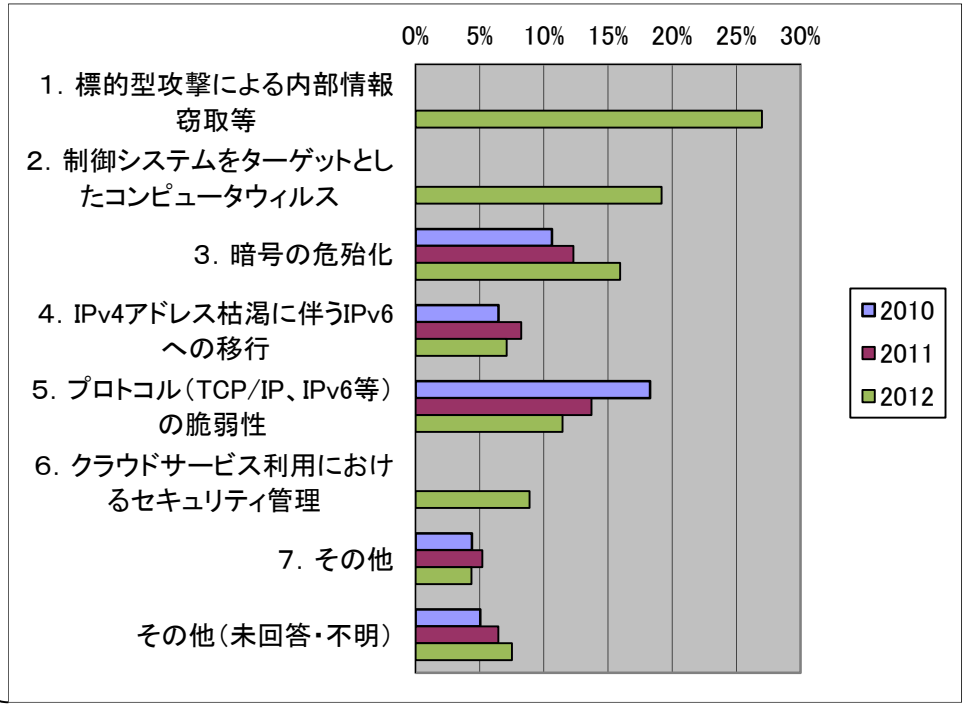
調査結果　②情報セキュリティ対策の実施状況に関する事項 (4/4)

- **ITに係る環境変化に伴う脅威に対して、対策を実施している(予定含む)事業者等が増加し、5割程度と推定。**
- **想定する脅威に関しては、今回調査から追加した標的型攻撃による内部情報窃取等が最も多かった。昨年度の防衛産業、政府機関等への攻撃多発を受け、脅威として想定する事業者等が多かったものと推定される。**

(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)



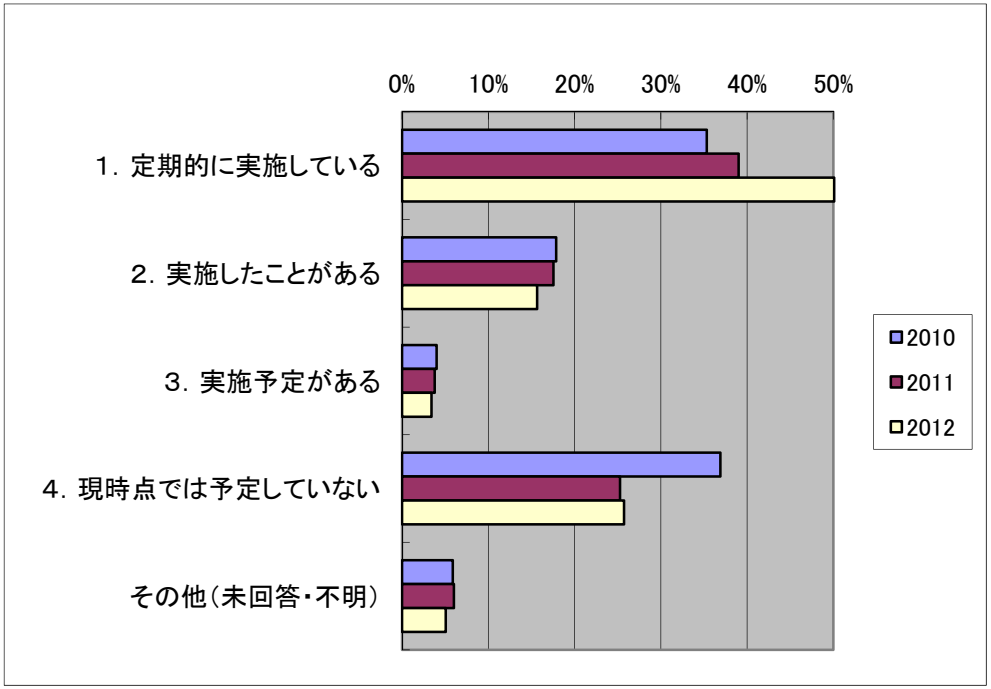
(12)　想定する脅威
政府・行政サービスは 読み替え可能項目なし(集計対象に含めず)
※項目1、2、6は2012年度に追加



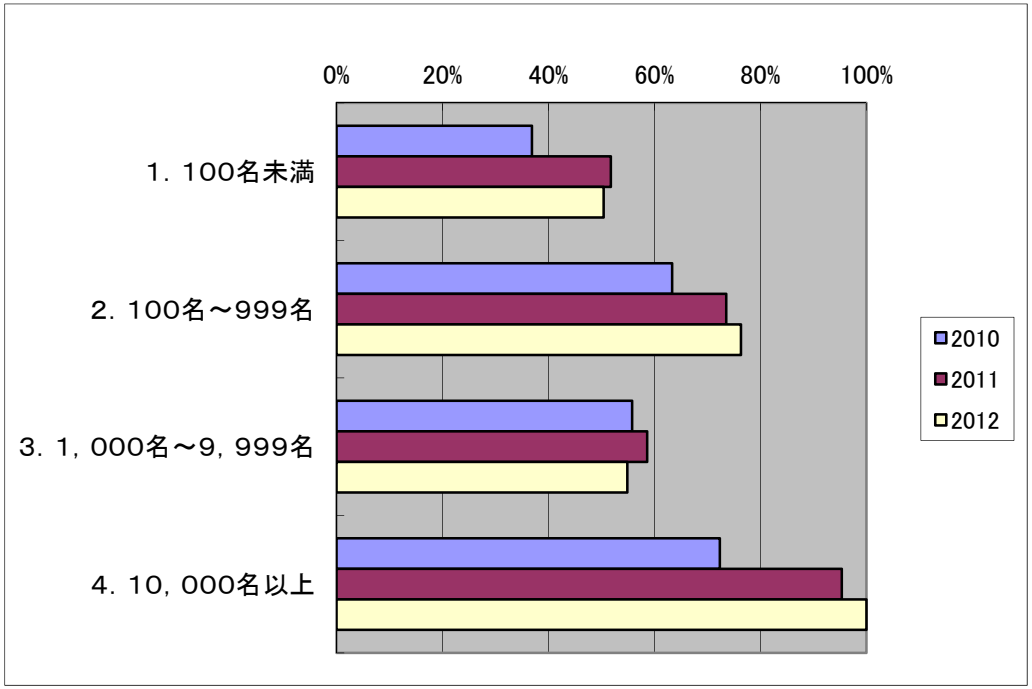
調査結果　③安全基準等に対する準拠状況に関する事項 (1/4)

- **自己点検を定期的に実施している事業者等が増加し、約5割。予定を含む実施割合は約7割と推定。**
- **1万名以上の事業者等では、ほぼ10割が実施（予定含む）。**

(1) 自己点検の実施



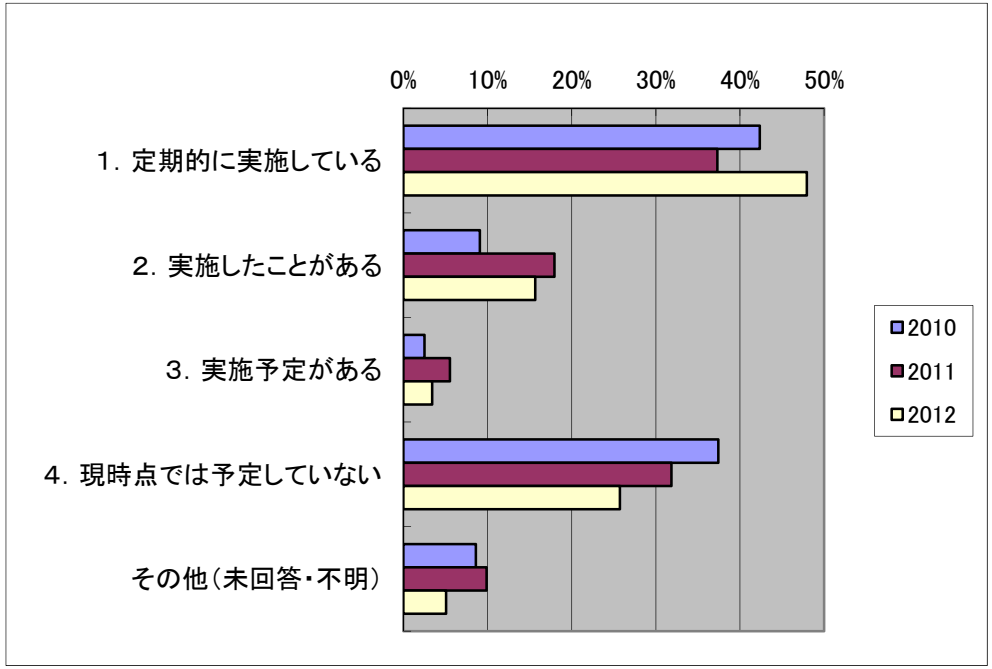
自己点検の事業規模ごとの実施割合（予定含む）



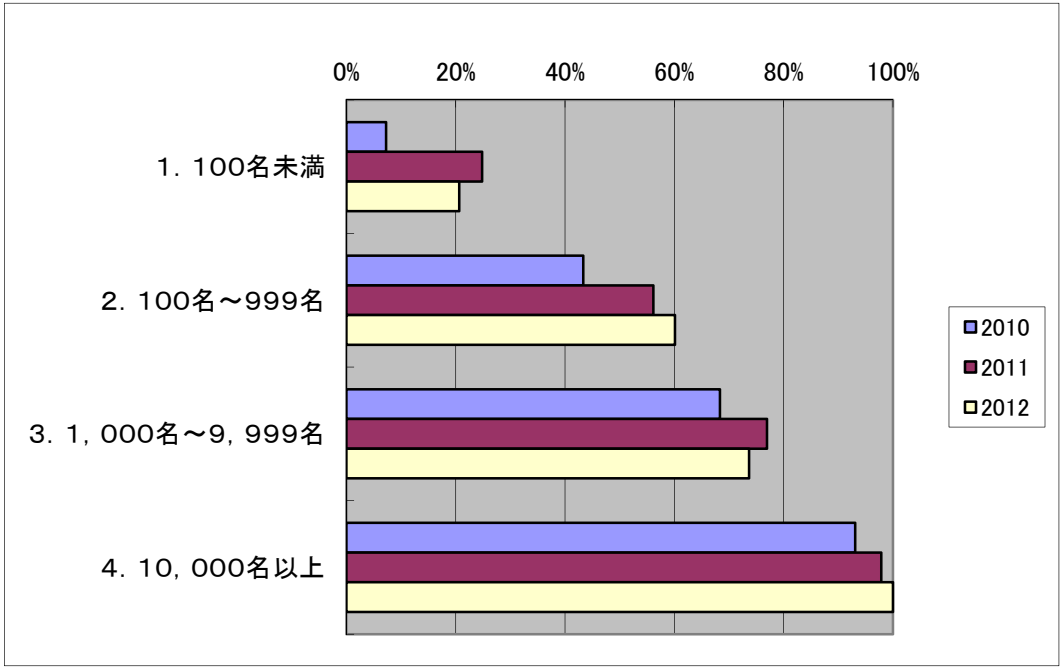
調査結果　③安全基準等に対する準拠状況に関する事項 (2/4)

- **演習・訓練を定期的に実施している事業者等が増加。予定を含む実施割合は約7割弱と推定。**
- **1万名以上の事業者等では、ほぼ10割が実施（予定含む）。**

(2)演習・訓練の実施



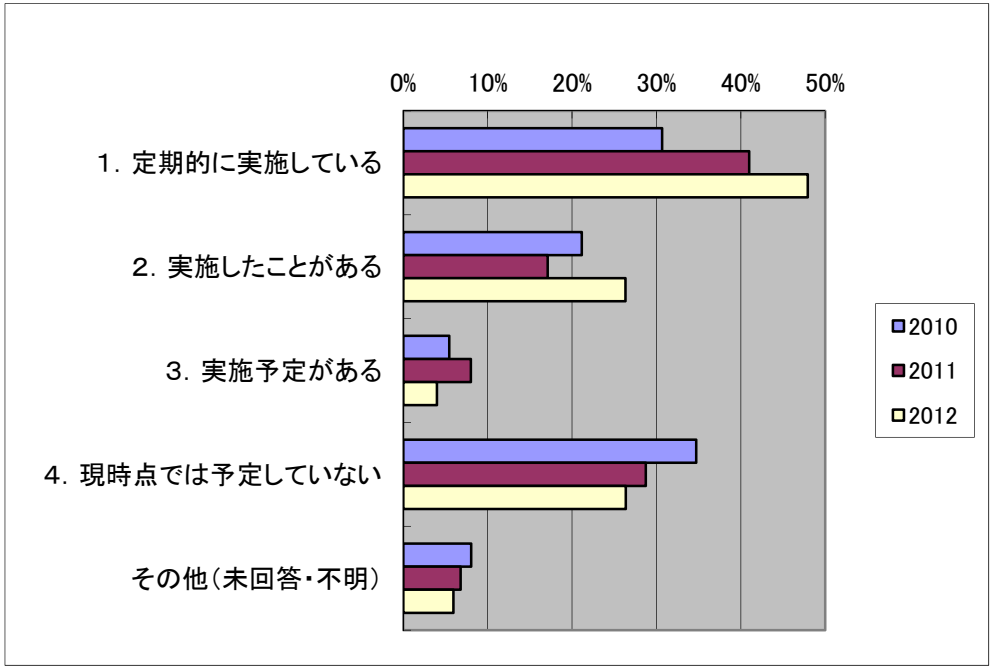
演習・訓練の事業規模ごとの実施割合（予定含む）



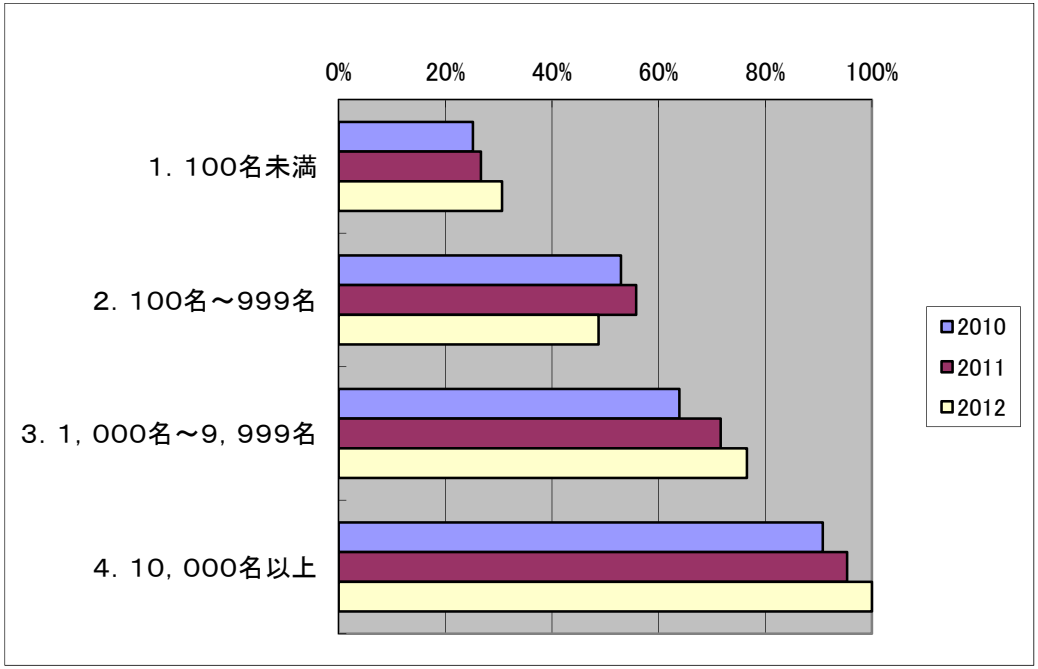
調査結果　③安全基準等に対する準拠状況に関する事項 (3/4)

- **内部監査を実施したことがある事業者等が増加し、予定を含む実施割合は約8割弱と推定。**
- **1万名以上の事業者等では、ほぼ10割が実施（予定含む）。**

(3) 内部監査の実施



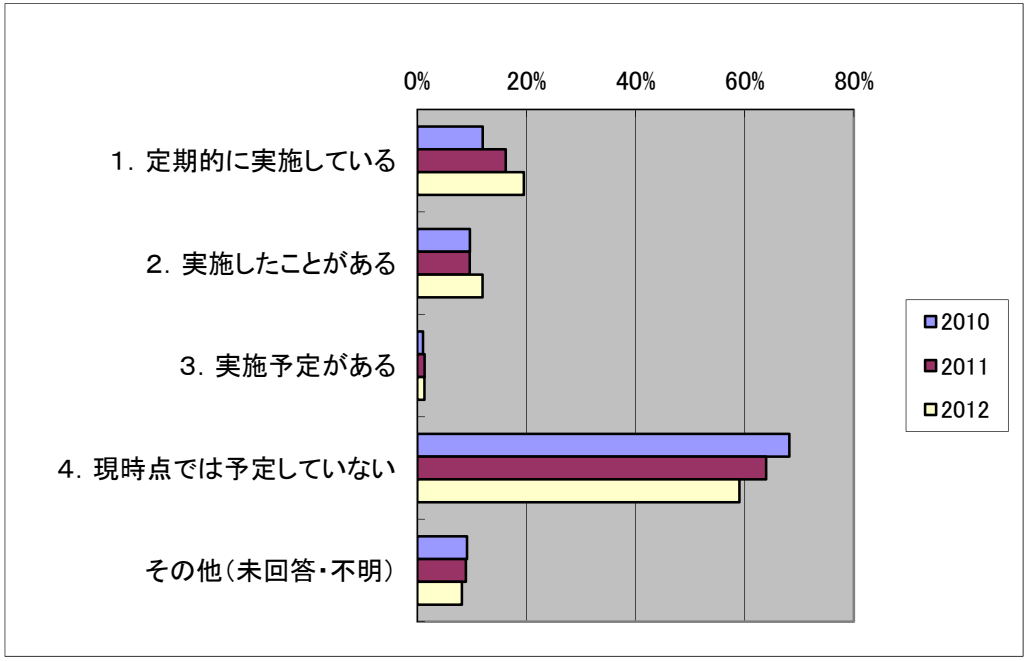
内部監査の事業規模ごとの実施割合（予定含む）



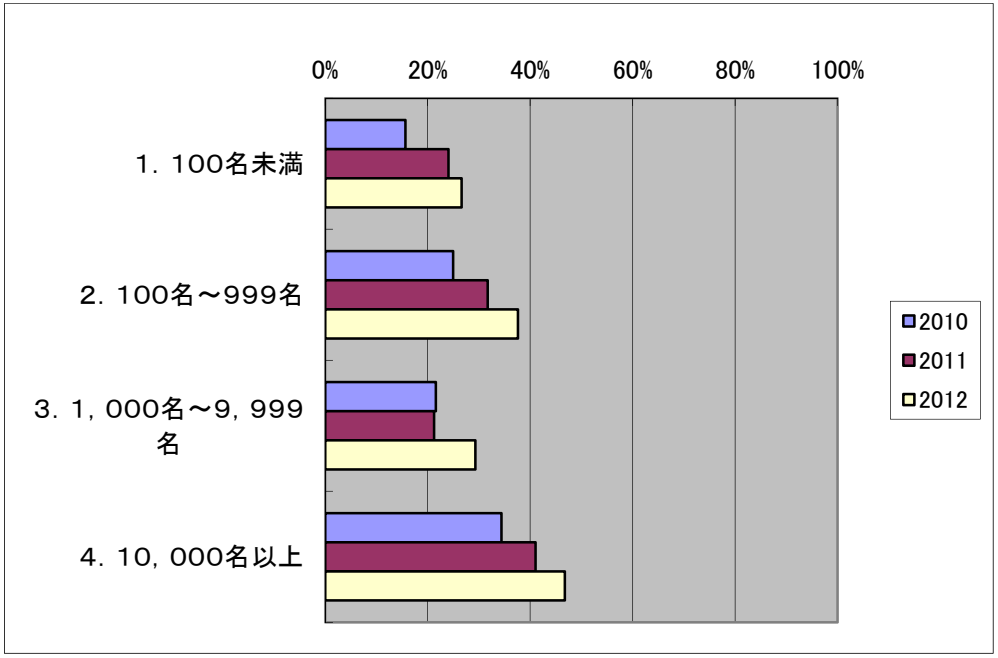
調査結果　③安全基準等に対する準拠状況に関する事項 (4/4)

- **外部監査の実施状況は、予定を含む全体の実施割合は3割強程度。**
- **全事業規模で増加傾向であるが、費用のかかる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、業種、企業規模に見合った基準、セキュリティとユーザビリティのバランスに関するものがあった。**
- **安全基準等に対する意見としては、各分野、事業の実態に合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 情報セキュリティ対策をしっかり実施していると自負していますが、反面、PC利用の自由度が失われています。仕事によっては、自宅PCの方が快適に作業出来る、という矛盾があります。難しい問題ですが、公のお立場から、適度な対策・管理・規制をお願い致します。
   ② 企業状況（規模の大小・業態）等により柔軟な対応が必要ではないかと思います。
   ③ 情報システムのトラブル時に、早期復旧を行うためにリモートアクセス回線を設置することがあるが、このような場合の指針があるとよい。
   ④ 国民を守る情報セキュリティ戦略及び本指針を含め概念的な位置づけでしかないため、これらを現実的に実施し、国としてのセキュリティレベルを高めようとするのであれば、例えばOSI参照モデルの階層毎に事業者・システム毎に実施できるチェックシート等を付加されてはどうでしょうか。人的な研修等も必要ですが、それを補完する、概念ではなく実際に利用できるツールがあれば、国が目指している方向性がより具体的にわかると思います。

2. 安全基準等に対して
   ① サービスの信頼性、安全性の処置は、事業性、採算性を含めて講じることになるため、安全基準等の強化を一方的に決定することにならないように配慮いただきたい。
   ② 業界・業種によってリスク範囲に差異があるので、それぞれの実態に合った指針を盛込んで欲しい。

※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、情報セキュリティの重要性や安全基準等の周知、一定の水準を保つためのセキュリティ対策費用の助成等の意見が多い。**

3. その他（自由意見を記載）

① 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と法的措置の強化を実施すべき。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 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）対策編の「5つの重点項目」については、項目の重要度や手順等を加えて、分かりやすい内容にして頂きたい。

③ 事例を集めてQ＆A集を充実させてほしい。

④ 中小規模の事業者は、使い勝手を優先する方向にあるので、セキュリティに関して経営者が読む雑誌などで情報セキュリティの重要性を喚起してもらいたい。

⑤ IT障害については、よく耳にするのですが、障害が発生した企業等がその後、どのような対策を実施したのか具体例を教えてほしい。

⑥ 情報セキュリティの相談窓口の設置をお願いしたい。

⑦ ガイドライン等の告知を能動的（ホームページ掲載のみならず）に行ってほしい。

⑧ 複数の公的機関から似たような情報をいただいているが、全体像の理解・把握が難しい。もう少しシンプルにならないものでしょうか？

※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ほぼ同様であった。また、回収率は93．2%（対前年度－0．3%）であった。
- 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率が全体的に増加している。また、自己点検、演習・訓練、監査（内部、外部）の実施率（予定含む）も増加しており、安全基準等の浸透が進んでい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≫

- 標的型攻撃による内部情報窃取を脅威と想定する事業者等が多い。標的型攻撃の情報共有をセプターカウンシル情報共有に関する検討推進WG等で推進していくことが望まれる。
- BCPを作成している（予定含む）事業者等が増加しており、BCPの実効性確認のために分野横断的演習が一層活用されるように、普及・啓発を図る。
- 情報セキュリティの重要性、安全基準等の周知に関する要望が多いので、今回の指針・対策編の改定に合わせて、周知方法等について検討する。

- 次回調査においても、引き続き、東日本大震災や標的型サイバー攻撃等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)