H14－H004

わが国におけるシステム監査の現状

－システム監査普及状況調査結果－

平成１５年３月

財団法人　日本情報処理開発協会

KEIRIN

この資料は競輪の補助金を受けて作成したものです。

序

当協会では、このたびわが国におけるシステム監査の普及状況を把握するため、「システム監査普及状況調査」を実施いたしました。

今回の調査は監査担当部門および被監査部門（情報システム部門）の双方を対象に行い、システム監査普及の傾向を把握することを狙いとしています。

調査にあたっては、474事業体の監査担当部門、649事業体の被監査部門からご回答いただき、信頼できる調査データを収集することができました。ご回答いただいた事業体、および調査項目の検討、調査結果とりまとめ等にご協力いただいたシステム監査基準検討委員会委員をはじめとする関係各位に心から謝意を表します。

本調査結果が、システム監査推進の一助となれば幸いです。

平成15年3月

財団法人　日本情報処理開発協会

平成１４年度システム監査基準検討委員会

（敬称略／五十音順）

委員長	鳥居　壮行	駿河台大学　文化情報学部　教授
委　員	江藤　友保	(株)シーイーシー　事業推進本部　企画・業務部　マネジャー
委　員	川辺　良和	（有）インターギデオン　代表取締役
委　員	喜入　　博	ＫＰＭＧビジネスアシュアランス（株） シニアアドバイザー／シニアオーディター
委　員	橘和　尚道	ＮＰＯ法人日本システム監査人協会　副会長
委　員	小田　浩史	富士通エフ・アイ・ピー（株） オペレーション統括部マネージメントサービス部　課長
委　員	原田　要之助	（株）情報通信総合研究所　情報流通プラットフォーム研究グループ グループリーダ／エクゼクティブ・リサーチャー
委　員	本田　　実	（株）三井情報開発　総合研究所システムコンサルティングセンター 主席コンサルタント
ｵﾌﾞｻﾞｰﾊﾞ	金澤　祐治	経済産業省　商務情報政策局情報セキュリティ政策室　技術係長

目　　次

1．調査の概要

1．1　調査の概要

1.1.1　調査の目的

本調査は、わが国におけるシステム監査の普及状況を、監査担当部門および被監査部門（情報システム部門）に対して調査し、現状と問題点を把握するとともに、今後のシステム監査の普及促進に役立てることを目的として実施したものである。

1.1.2　調査の対象

当協会が隔年で実施している「システム監査普及状況調査」の母集団40業種4,000事業体を対象とした。

1.1.3　調査時期

調査票発送　　平成14年11月1日
回収締切　　平成15年1月21日

1.1.4　回収状況（表1－1－1、1－1－2参照）

発送数　　4,000件
監査担当部門　　474件（回収率：11.9%）
被監査部門　　649件（回収率：16.2%）

1.1.5　回答事業体の平均従業員数

監査担当部門　　3,113人
被監査部門　　2,246人

1.1.6　調査項目

（1）監査担当部門対象

Ⅰ．システム監査一般について
Ⅱ．貴社の監査体制について
Ⅲ．平成13年度のシステム監査実施について
Ⅳ．未実施および実施可能性について
Ⅴ．情報セキュリティの推進について
Ⅵ．電子メールの利用について

（2）被監査部門対象

Ⅰ．システム監査一般について
Ⅱ．平成13年度のシステム監査実施について
Ⅲ．システム監査のあり方について
Ⅳ．情報セキュリティの推進について
Ⅴ．電子メールの利用について

表１－１－１．監査担当部門の回収状況

業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数	業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数
食品・紙・パルプ・繊維・印刷	食品製造業	12	1,613	情報処理サービス業	情報処理サービス業・ソフトウェア業	67	1,010
	繊維工業	6	305	その他対事業所ｻｰﾋﾞｽ	農・林・漁・狩・水産養殖業	0	0
	紙・ﾊﾟﾙﾌﾟ・紙加工品製造業	2	5,724		鉱業	0	0
	印刷業・同関連産業	2	1,425		建設業	16	1,966
石油・化学・鉄鋼・非鉄・金属	化学工業	21	2,677		新聞業・出版業	2	610
	石油製品製造業	0	0		不動産業	2	546
	鉄鋼業	9	1,682		運輸・通信・倉庫業	13	1,766
	非鉄金属製造業・金属製品製造業	13	709		電力・ガス業	10	8,373
電気・一般・輸送・精密機械	一般機械器具製造業	17	1,560		放送業	4	223
	電気機械器具製造業	31	6,293		広告・調査・情報提供サービス業	1	380
	輸送用機械器具製造業	14	18,796		その他のサービス業	10	1,083
	精密機械器具製造業	14	1,955	公共ｻｰﾋﾞｽ	医療業	1	500
その他製造業	窯業・土石製品製造業	6	1,535		宗教法人	0	0
	その他製造業	19	2,515		高校	2	62
商　　業	卸業・商社	30	1,154		大学	12	1,174
	小売業	8	1,668		その他の教育機関	3	418
金融・保険業	金融業	64	2,835		学術研究機関	1	114
	証券業・商品取引業	1	4,650		法人団体・農協	8	2,210
	生命保険業	9	15,151	政府・地方公共団体	政府	4	3,050
	損害保険業	3	9,456		地方公共団体	37	3,391
小　　計		281	-	小　　計		193	-
合　　計						474	平均　3,113

表１－１－２．被監査部門の回収状況

業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数	業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数
食品・紙・パルプ・繊維・印刷	食品製造業	17	1,281	情報処理サービス業	情報処理サービス業・ソフトウェア業	59	1,649
	繊維工業	10	1,071	その他対事業所ｻｰﾋﾞｽ	農・林・漁・狩・水産養殖業	1	588
	紙・ﾊﾟﾙﾌﾟ・紙加工品製造業	3	346		鉱業	1	936
	印刷業・同関連産業	2	941		建設業	38	1,863
石油・化学・鉄鋼・非鉄・金属	化学工業	25	1,570		新聞業・出版業	2	2,025
	石油製品製造業	2	1,027		不動産業	2	546
	鉄鋼業	9	1,857		運輸・通信・倉庫業	23	1,836
	非鉄金属製造業・金属製品製造業	24	1,418		電力・ガス業	10	8,790
電気・一般・輸送・精密機械	一般機械器具製造業	22	1,197		放送業	8	396
	電気機械器具製造業	42	5,238		広告・調査・情報提供サービス業	4	2,448
	輸送用機械器具製造業	21	6,422		その他のサービス業	15	1,037
	精密機械器具製造業	22	2,296	公共ｻｰﾋﾞｽ	医療業	4	1,124
その他製造業	窯業・土石製品製造業	10	2,199		宗教法人	0	0
	その他製造業	30	1,027		高校	2	62
商　　業	卸業・商社	37	934		大学	20	891
	小売業	22	1,794		その他の教育機関	2	588
金融・保険業	金融業	69	1,262		学術研究機関	0	0
	証券業・商品取引業	2	2,751		法人団体・農協	13	1,196
	生命保険業	10	8,863	政府・地方公共団体	政府	6	2,471
	損害保険業	5	8,507		地方公共団体	55	2,923
小　　計		384	－	小　　計		265	－
合　　計						649	平均　2,246

2．調査結果の要約

本調査は監査担当部門および被監査部門に対し、それぞれの立場からみたシステム監査の実施状況等について質問を行っている。

また、本調査は平成２年から隔年で計７回の調査を行っているが、本文「３．調査結果の詳細」では平成６年度以降の調査結果を基に、どれだけシステム監査に対する意識が変化してきたかも分析している。

ここでは調査項目（前述「1.6」）ごとに集計結果を要約する。なお、両部門共通の質問項目については、調査項目の分野、質問番号順に限らず、一方の調査項目の中でとりまとめて紹介しているため、多少質問番号が前後している。

なお、文末に記載している（監／被Q××）はそれぞれの調査票での質問番号を指している。

2.1　システム監査一般について

経済産業省はシステム監査等セキュリティ関連施策として、システム監査基準、システム監査技術者試験、システム監査企業台帳制度、情報システム安全対策基準、コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準等を策定しているが、これらの認知度について両部門に対し調査を行った。

各基準の認知度はシステム監査基準（監:78.1%、被:86.7%）、情報システム安全対策基準（監：67.6%、被：80.8%）、コンピュータウイルス対策基準（監：66.9%、被：80.0%）、コンピュータ不正アクセス対策基準（監：63.9%、被：76.2%）となっており、いずれも監査担当部門よりも被監査部門での認知度が高い。なお、「利用したことがある」との回答については、前回調査と比べ、システム監査基準の利用率が 2.8 ポイント減少した。

システム監査台帳制度の認知度について、「知っている」との回答については両部門で差はほとんど見られない。（監：33.8%、被：33.0%）。台帳制度は外部のシステム監査企業に監査を委託する際の参考とすることを目的としており、監査実施時に台帳を「参考にしたい」とする回答は、被監査部門の方が監査担当部門を 9.4 ポイント上回っている。

日本情報処理開発協会が運用している「プライバシーマーク制度」および「ＩＳＭＳ適合性評価制度」の認知度については、被監査部門の方が監査担当部門よりも認知度が高い。（監／被Ｑ１～12）

2.2　回答事業体の監査体制について

監査担当部門に対し、自社の監査体制について調査を行った。

全回答事業体の 69.0%が自社に内部監査部門を設置しており、内部監査人の人数は平均 13.3 人、平均年齢 51.1 歳である。

システム監査担当者の設置については、「いる」との回答が 23.6%であり、システム監査人の人数は平均 4.0 人、平均年齢 48.9 歳である。内部監査人の設置状況と比較すると、設置状況、人数ともにかなりの差がでている。(監Q13～14)

システム監査技術者試験合格者数は平均 9.3 人で、所属部署については、「情報システム部門」が最も多く 69.9%、「内部監査部門」は 31.2%となった。(監Q15～16)

過去のシステム監査の実施状況について、監査担当部門では 38.4%が、また被監査部門では 39.3%の事業体が監査を実施している。平成２年度調査（監：24.3%、被：22.2%）から比べ、両部門ともに約 14～17 ポイント増加しており、システム監査を実施する事業体が徐々にではあるが増加してきていることがわかる。(監Q17、被Q14)

システム監査実施にあたり、体制上の問題点としては「システム監査人の不足」が、最も充実すべき点は「事前調査」、「実地調査」との指摘が多い。(監Q19, 21)

監査人の不足している知識・能力としては「業務知識」、「情報システムの知識」、「分析能力」があげられた。なお、「情報システムの知識」については被監査部門でも平成 13 年度監査実施上の問題点として指摘されている。(監Q23, 24、被Q22)

システム監査実施に際し、監査対象、監査テーマの決定はともに「内部監査部門（長）の判断」による事業体が多い。(監Q26、27)

システム監査は誰が実施するのが効果的であるかを両部門に調査した。監査担当部門で最も多かった「内部の監査人」(47.8%）について被監査部門では 16.6%、被監査部門で最も多かった「システム監査企業台帳に基づくシステム監査企業」(37.3%）について監査部門では 12.1%であり、両者の意見にかなり大きな差がみられる。(監：Q20、被：Q38)

2.3 平成１３年度の監査実施について

過去に監査を実施したことがある回答事業体に対し、平成 13 年度の監査内容について調査を行った。監査担当部門は監査実施者の立場から、また被監査部門は監査を受けた現場の立場からの意見である。

平成 13 年度に監査を「実施した」との回答は監査担当部門が 75.8%、被監査部門が 69.8%である。ともに「内部監査部門型」による監査が最も多い（監：70.3%、被：59.6%)。(監Q31, 32、被Q15, 18)

監査実施業務で多いのは「運用業務」(監：89.1%、被：89.3%)、「開発業務」(監：70.3%、被：69.7%）となったが、一部の業務のみを監査するというよりは、全体業務を監査する事業体が多い。(監Q35、被Q16)

また、今年度調査から、実施業務とは別に監査対象テーマ別の実施状況を調査した。両部門ともに「セキュリティ対策」の監査が圧倒的に多い（監：84.8%、被：78.7%)。(監Q36、被Q17)

監査担当部門からみた自社の情報システムの状態は、36.2%が「満足」しているが、「なんともいえない」(32.6%)、「多少不満」(21.0%）との意見も多い。(監Q49)

被監査部門が監査を受けた結果の効果について、72.5%の事業体が「効果があったと思う」と回答しており、「要員が規定・ルール等を意識して業務を実行」を挙げている事業体が 27.1%で

ある。また、監査により改善が図れたと思われる点は「セキュリティ対策の向上」(31.8%)、「規則・手続き等の遵守」(23.3%) である。(被Q31～33)

2.4 システム監査のあり方について

監査担当部門に対しては平成 13 年度の実施業務および実施テーマに対し最も重視した着眼点について、また被監査部門に対しては監査実施の際に重視すべき着眼点についての調査した。結果は次のとおりである。(監Q35～36、被Q34～35)

(1) 業務別にみた着眼点

- 企画業務で重視すべき着眼点は、監査担当部門が「採算性」(24.0%)、被監査部門が「適時性」(27.7%)
- 開発業務で重視すべき着眼点は、監査担当部門が「信頼性」(39.2%)、被監査部門が「生産性」(28.2%)
- 運用業務で重視すべき着眼点は「安全性」(監：42.3%、被：37.0%)
- 保守業務で重視すべき着眼点は「信頼性」(監：41.2%、被：43.0%)

(2) 着眼点別にみた監査対象テーマ

- 安全性を重視すべきテーマは「災害対策」(監：74.0%、被：71.8%)
- 信頼性を重視すべきテーマは「品質管理」(監：70.7%、被：64.6%)
- 機密性を重視すべきテーマは「個人情報保護対策」(監：56.6%、被：57.3%)
- 準拠性を重視すべきテーマは「ソフトウェア適正利用」(監 58.5%、被：41.1%)
- 採算性を重視すべきテーマは「コスト管理」(監：47.3%、被：60.2%)
- 適時性を重視すべきテーマは「進捗管理」(監：33.8%、被：32.5%)
- 生産性を重視すべきテーマは「要員管理」(監：31.3%、被：27.0%)
- 効率性を重視すべきテーマは監査担当部門が「コスト管理」(25.5%)、被監査部門が「要員管理」(25.4%)

両部門ともにそれぞれの着眼点を最も重視する業務、監査対象テーマはほぼ同一という結果となった。

コンピュータ犯罪防止および早期発見の観点からみたシステム監査で最も重視すべき分野は、「情報保管 (データ管理)」(監：40.6%、被：34.4%) である。

ヒューマンエラー防止および早期発見の観点からみたシステム監査で最も重視すべき分野は、「オペレーション」(監：39.9%、被：42.8%) である。

事故防止および早期発見の観点からみたシステム監査で最も重視すべき分野は、監査担当部門が「オペレーション」(18.8%)、被監査部門が「ハードウェア」(16.6%) である。

災害対策の観点からみたシステム監査で最も重視すべき分野は、監査担当部門が「ハードウェア」(23.2%)、被監査部門が「情報保管 (データ管理)」(27.7%) である。

個人情報保護の観点からみたシステム監査で最も重視すべき分野は、「情報保管」(監:77.5%、被：62.1%) である。(監Q37、被Q36)

2.5 未実施および実施可能性について

システム監査未実施事業体の監査担当部門に対し、未実施の理由等について調査した。

監査未実施の理由として最も多いのは「システム監査の実施よりもシステム化推進そのものに力点がある」(21.6%) である。これは平成２度調査から常に２～３割の事業体が未実施の理由として挙げている。

今後の対応については、「当面導入の予定はない」、「将来とも導入の予定がない」を合わせると62.0%の事業体が導入を予定していない。

今後監査を導入する予定がある事業体が主とする観点としては「安全性」(44.9%)、「機密性」(21.8%) である。(監Q57～60)。

2.6 情報セキュリティ推進について

情報セキュリティの推進体制、教育の実施状況等について調査した。

セキュリティポリシーの策定状況については、「策定／策定中」の事業体が５割を超えている(監：59.7%、被：56.1%) (監」Q61, 被：Q39)

情報セキュリティ推進体制は、両部門ともに「情報システム部門主導による実施」が最も多い(監：50.6%、被：52.5%)。また推進する上で最も重要と思われることは「全社的な推進体制」である (監：51.3%、被：48.2%)。

情報セキュリティに関し「情報セキュリティ体制の確立」、「情報セキュリティ教育の実施」を優先的に実施している。一方で、情報セキュリティ推進に対し「特に実施していない」とする事業体が約２割、また、情報セキュリティに関する教育を「特に実施していない事業体も約４割を占めている。(監：Q62～63、被：Q40～41)

2.7 電子メールの利用について

電子メールの利用状況について両部門を対象に調査を行った。

電子メールの利用のルールの策定については、両部門とも約６割がルールをすでに定めている。(監：59.1%、被：59.2%)

要員のメールの利用状況の監視については、監視または監視を予定している事業体 (監：52.3%、被：53.3%) の方が「監視していない」ところよりも若干多い。

社内のメールサーバへのリモートアクセスの認可については、「(許可制で) 認めている」事業体が若干５割を超えた程度である。(監：49.5%、被：51.9%) なお、電子メール利用に関する監査の実施率は8.9%とかなり低い結果となった。(監」Q67～72、被」Q44～48)

3．調査結果の詳細

3.1　監査担当部門対象

3.1.1　システム監査一般について

Q１．経済産業省から「システム監査基準」（平成８年改訂）が公表されていることを知っていますか。

1	利用したことがある	94	19.8
2	内容は知っているが、利用したことはない	116	24.5
3	存在だけは知っている	160	33.8
4	知らない	99	20.9
無回答		5	1.1
計		474	100.0

システム監査基準の認知度について、平成 14 年度調査（以下、「今回調査」という。）は、平成 12 年度調査（以下「前回調査」という。）を 3.7 ポイント下回る結果となったが、約８割の 78.1％がその存在を知っており、かなり高い認知度といえる。

しかしながら、基準の活用については、「利用したことがある」の回答は 19.8％（前回調査 22.6％）と２割にも満たず、基準活用への展開が望まれる。

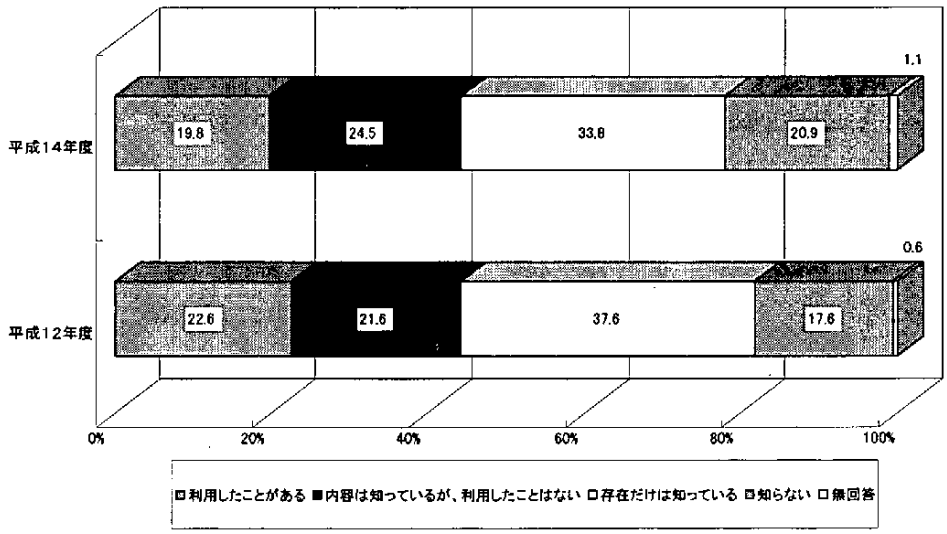

図3－1－1．システム監査基準の認知度（監査担当部門）

Q２．経済産業省の「システム監査企業台帳制度」（平成３年策定）を知っていますか。

1	知っている	160	33.8	
2	知らない	310	65.4	→Q４へ
無回答		4	0.8	
計		474	100.0	

平成３年に台帳制度が開始されてからすでに 10 年以上が経過しているが、「知っている」との回答は 33.8％と、いまだ台帳制度の認知度は低い。しかも、平成８年 29.6％、平成 10 年 30.5％、前回調査 34.4％と、前回までは認知度が増加していたが、今回調査では前回調査の値を下回る結果となった。

Ｑ３．システム監査を外部の企業に委託する場合「システム監査企業台帳」を参考にしたいと思いますか。

1	参考にしたことがある	15	9.4
2	今後参考にしたいと思う	103	64.4
3	参考にしたいと思わない	34	21.3
無回答		8	5.0
計		160	100.0

システム監査企業台帳制度を知る事業体に対する質問であるが、これまでに台帳を「参考にしたことがある」と回答した事業体は 9.4％と１割にも満たない。しかし、「今後参考にしたいと思う」という事業体は 64.4％と前回調査（29.5％）に比べ約 35 ポイントも増加しており、今後のシステム監査企業台帳の活用が期待できる。

Ｑ４．経済産業省の情報処理技術者試験制度で行われている「システム監査技術者試験」を知っていますか。

1	知っている	346	73.0
2	知らない	123	25.9
無回答		5	1.1
計		474	100.0

昭和 61 年にシステム監査技術者試験制度が開始されてから 15 年以上が経過しており、前回調査 68.9％から 4.1 ポイント増加し、73.0％がシステム監査技術者試験の存在を知っている結果となった。なお、試験制度自体が 2001 年度より新制度に移行したことにより、本試験は秋期から春期の試験区分に変更となった。

情報処理技術者試験制度については、下記ホームページを参照されたい。

○経済産業省「資格・試験」

http://www.meti.go.jp/information/licence/index.html

○日本情報処理開発協会情報処理技術者試験センター（JITEC）

http://www.jitec.jipdec.or.jp

Q５．経済産業省から「情報システム安全対策基準」（平成７年改訂）が公表されていることを知っていますか。

1	利用したことがある	105	22.2	
2	内容は知っているが、利用したことはない	87	18.4	
3	存在だけは知っている	128	27.0	
4	知らない	146	30.8	→Q７へ
無回答		8	1.7	
計		474	100.0	

情報システム安全対策基準が改訂されて７年が経過したが、67.6%が基準を「知っている」と回答している。平成10年68.7%、前回調査69.7%とここ数回の調査における約７割の認知度は、ほとんど変化がない。

一方、基準を「利用したことがある」との回答は22.2%（前回調査22.4%）とシステム監査基準とほぼ同様で約２割程度である。

Q６．「情報システム安全対策基準」の中でシステム監査が位置づけられていることを知っていますか。

1	知っている	251	78.4
2	知らない	68	21.3
無回答		1	0.3
計		320	100.0

情報システム安全対策基準では、技術基準と運用基準で監査を位置づけているが、このことを「知っている」との回答は、前回調査72.6%と比べ5.8ポイント増加して78.4%となり、８割近くが認知する高い結果となった。

Q７．経済産業省から「コンピュータウイルス対策基準」（平成７年改訂）が公表されていることを知っていますか。

1	利用したことがある	83	17.5	
2	内容は知っているが、利用したことはない	87	18.4	
3	存在だけは知っている	147	31.0	
4	知らない	151	31.9	→Q９へ
無回答		6	1.3	
計		474	100.0	

コンピュータウイルス対策基準の認知度は、平成10年66.5%、前回調査67.6%、今回調査66.9%とほとんど変化がない。この約７割の認知度は、情報システム安全対策基準とほぼ同じ状況といえる。

一方、基準を「利用したことがある」との回答は、調査ごとに増加してはいるが、未だに17.5%と2割にも満たず、その値は情報システム安全対策基準と比べて低い値となっている。新種・変種ウイルスの日常的な発生、ウイルス感染・発病の状況を考慮すると、単に「知っている」といったレベルに留まらず、基準を活用しウイルス対策を講じていくことが必要といえる。

Q8.「コンピュータウイルス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

1	知っている	209	65.9
2	知らない	103	32.5
無回答		5	1.6
計		317	100.0

システム監査はコンピュータウイルス対策基準の4つの基準すべてにおいて位置づけられているが、このことの認知度は、平成10年59.5%、前回調査61.7%、今回調査65.9%と着実に増加しており、ウイルス対策における監査の役割の重要性が認識されてきている。

Q9.経済産業省から「コンピュータ不正アクセス対策基準」(平成8年)が公表されていることを知っていますか。

1	利用したことがある	79	16.7	
2	内容は知っているが、利用したことはない	95	20.0	
3	存在だけは知っている	129	27.2	
4	知らない	165	34.8	→Q11へ
無回答		6	1.3	
計		474	100.0	

コンピュータ不正アクセス対策基準の認知度は、平成8年39.6%、平成10年59.2%、前回調査62.3%、今回調査63.9%と着実に増加してきてはいるが、他の基準に比べるとまだ低い状況である。

また、基準を「利用したことがある」の回答も平成10年12.9%、前回調査13.7%、今回調査16.7%と増加してはいるが、2割にも満たない状況である。

インターネットの目覚しい進展、不正アクセス禁止法が制定されるなどの状況を踏まえると、単に基準を「知っている」に留まらず、基準を活用し、対策を講ずることが必要といえる。

Q10.「コンピュータ不正アクセス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

1	知っている	209	69.0
2	知らない	91	30.0
無回答		3	1.0
計		303	100.0

システム監査はコンピュータ不正アクセス基準の５つの基準すべてにおいて位置づけられているが、このことについて、前回調査（64.0%）より５ポイント増加し、約７割の 69.0%が認知する結果となった。

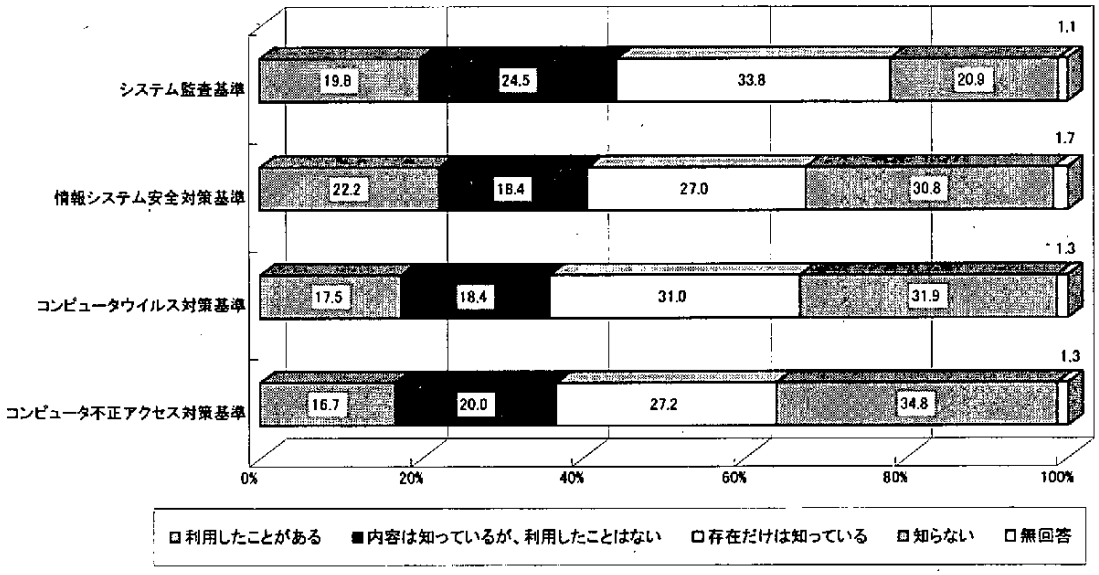

図3－1－2. セキュリティ関連基準の認知度（監査担当部門）

なお、上記のセキュリティ関連施策（情報処理技術者試験を除く）については、下記ホームページに掲載されているので、参照されたい。

○経済産業省「情報セキュリティ政策、署名認証、プライバシー」
http://www.meti.go.jp/policy/netsecurity/index.html

○日本情報処理開発協会「情報セキュリティ対策の推進」
http://www.jipdec.jp/security/security.htm

Q11. プライバシーマーク制度を知っていますか。

1	知っている	206	43.5
2	知らない	259	54.6
無回答		9	1.9
計		474	100.0

日本情報処理開発協会（JIPDEC）が運用しているプライバシーマーク制度は平成10年4月に発足し、翌11年には「JIS Q 15001　個人情報保護に関するコンプライアンス・プログラムの要求事項」に準拠した個人情報保護のための体制を整備している事業者に対する認定制度へと発展してきた。

業種別にみると、情報処理サービス業・ソフトウェア業などを中心に展開されていることもあり、その認知度は94.0％と非常に高いが、全体としての認知度は43.5％、すなわち4割程度の低い状況となっている。

○プライバシーマーク制度のホームページ　http://privacymark.jp

Q12. ＩＳＭＳ（情報セキュリティマネジメントシステム）適合性評価制度を知っていますか。

1	知っている	172	36.3
2	知らない	289	61.0
無回答		13	2.7
計		474	100.0

JIPDECが運用している「情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度は、平成13年度の情報サービス産業をベースとしたパイロット認証期間を踏まえ、平成14年度から本格的にスタートした。その認知度は、パイロット認証の対象となった情報処理サービス業・ソフトウェア業は85.1％と突出しているが、全体としては36.3％の3割強と初年度でもあり低い状況といえる。

また、プライバシーマーク制度の認知度43.5％と比較しても、7.2ポイント低い結果となっている。

○ＩＳＭＳ適合性評価制度のホームページ　http://www.isms.jipdec.or.jp

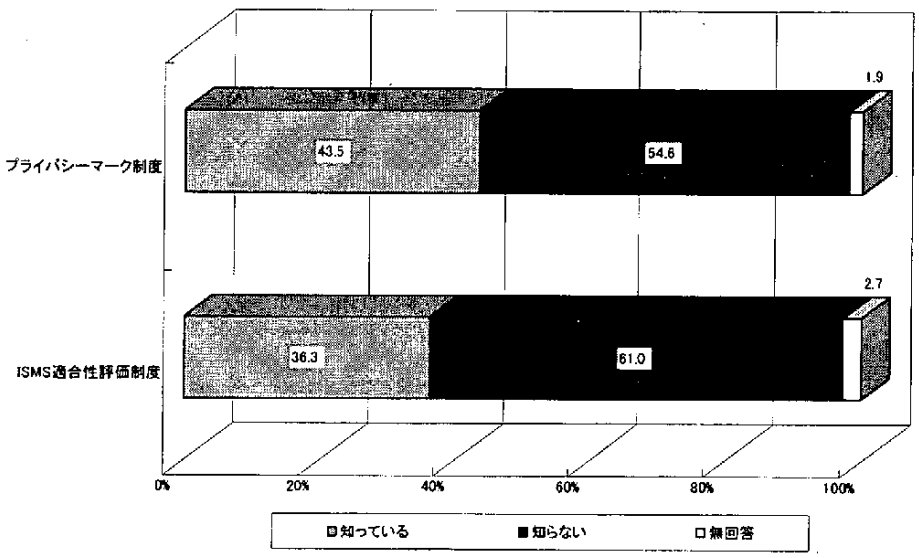

図3－1－3. プライバシーマーク制度とISMS制度の認知度（監査担当部門）

3.1.2 貴事業体の監査体制について

Q13. 貴社には内部監査部門（監査部、検査部等）が設置されていますか。

1	い る	327	69.0
2	いない	144	30.4
無回答		3	0.6
計		474	100.0

事業体内にシステム監査部門も含め、内部監査部門（監査部、考査部、検査部、監査委員会など）を設置している状況は、全回答の69.0%が「設置している」となっている。平成６年57.8%、平成８年62.9%、平成10年63.4%、前回調査68.5%、今回調査と、徐々にではあるが内部監査部門が設置されている割合は、高くなっている。

業種別にみると、どの業種も設置の割合が高くなっているが、生命保険業（100%）、金融業（95.3%）、電力・ガス事業(90.0%)、電気機械機具製造業（77.4%）、情報処理サービス業・ソフトウェア業（68.7%）、化学工業（66.7%）、卸売・商社（63.3%）が特に高くなっている。

Q13-１．内部監査人は何人いますか。

平均	13.3人	
１人	59	18.0
２人	45	13.8
３人	36	11.0
４人	41	12.5
５人	21	6.4
６～１０人	44	13.5
１１～１５人	15	4.6
１６～２０人	12	3.7
２１人以上	49	15.0
無回答	5	1.5
計	327	100.0

Q13-２．内部監査人は平均何歳ですか。（端数切捨て）

平均	51.1歳	
～３５歳	5	1.5
３６～４０歳	18	5.5
４１～４５歳	31	9.5
４６～５０歳	94	28.7
５１～５５歳	98	30.0
５６～６０歳	48	14.7
６１～６５歳	15	4.6
６６歳以上	4	1.2
無回答	14	4.3
計	327	100.0

内部監査部門を設置している場合の内部監査人の要員数の平均は13.3人であり、前回調査の10.1人に対して3.2人増加している。特に「21人以上がいる」とした回答が、前回調査では11.2%であったのに対し今回は15.0%であったことが増加の要因の１つといえよう。

内部監査人の要員数が「１～５人」の回答は、全体の61.7%となっている。全体平均を高くしているのは金融関係であり、「21人以上」の内部監査人がいると回答した15.0%の多くは金融業、生命保険業であった。

内部監査部門を設置している場合の内部監査人の平均年齢は51.1歳である。前回調査の平均年齢は51.4歳であり、２年経過したにもかかわらず、この間で0.3歳と若干の若返りとなっている。

平均年齢帯で最も多かったのは、「51 歳～55 歳」で、回答全体の 30.0％であった。

平均年齢 51.1 歳は、明らかに全社員平均を大きく上回っていると想定される。監査部門の要員は、他の部門に比べて経験が必要なことから、業務経験のあるベテランが配置されていると思われる。

Q14. 貴社にはシステム監査人（システム監査の担当者）がいますか。

1	い　る	112	23.6
2	いない	355	74.9
無回答		7	1.5
計		474	100.0

Q14-1．システム監査人は何人ですか。

平均	4.0人	
１人	39	34.8
２人	31	27.7
３人	12	10.7
４人	4	3.6
５人	5	4.5
６～１０人	13	11.6
１１～１５人	3	2.7
１６～２０人	1	0.9
２１人以上	4	3.6
計	112	100.0

Q14-2．システム監査人は平均何歳ですか。
（端数切り捨て）

平均	48.9歳	
～３５歳	4	3.6
３６～４０歳	9	8.0
４１～４５歳	11	9.8
４６～５０歳	43	38.4
５１～５５歳	32	28.6
５６～６０歳	7	6.3
６１～６５歳	0	0.0
６６歳以上	1	0.9
無回答	5	4.5
計	112	100.0

Q14-3．システム監査人を置いたのはいつですか。

１９９０年以前	30	26.9	１９９７年	2	1.8
１９９１年	2	1.8	１９９８年	13	11.6
１９９２年	1	0.9	１９９９年	8	7.1
１９９３年	0	0.0	２０００年	11	9.8
１９９４年	8	7.1	２００１年	13	11.6
１９９５年	4	3.6	２００２年	12	10.7
１９９６年	0	0.0	無回答	8	7.1
計				112	100.0

内部監査部門は、回答の約７割弱の事業体で設置されているが、「システム監査人を置いている」とした回答は23.6％となっている。これは、前回調査の22.2％に比べ、1.4ポイントの増加となっている。直接、情報システムを監査対象としない場合でも、情報システムを避けて監査することはできないことがこのような増加につながっていると思われる。システム監査人を置いて

いる割合が高い業種は、生命保険業が66.7%、金融業が60.9%、情報処理サービス業・ソフトウェア業が47.8%となっている。金融業は前回調査が46.4%であり、14.5ポイントの増加となっている。

システム監査人を置いている事業体のシステム監査人の平均人数は、今回の調査では、4.0 人である。過去の調査では、平成6年 6.9 人、平成8年 3.3 人、平成 10 年 3.3 人、前回調査が 4.8 人であった。平成6年調査の高い数字は、1社で多数のシステム監査人がいるとの回答があったためであり、当該事業体を除いた平均は他の調査年とほぼ同数であった。例年同様、今回の調査でも、回答の多くは1人あるいは2人であり、1人を置いているのは 34.8%、2人が 27.7%となっている。

システム監査人の平均年齢は、前回調査で 49.1 歳であったが、2年経過した今回調査では、0.2 歳若い 48.9 歳となっている。これまでの直近3回の調査でのシステム監査人の平均年齢は増加する一方であったが、今回の調査では僅かながらではあるが若返りとなった。「Q13-2 内部監査人の平均年齢」の若返りと合わせて、比較的、年配者の多い監査部門でも、世代交代の動きがあると思われる。

なお、システム監査人の平均年齢は、内部監査人の平均年齢 51.1 歳より 2.2 歳若くなっている。この傾向は従来からも同様であるが、情報システムの専門知識が必要なシステム監査人は内部監査人に比べ若くなっている。

システム監査人を初めて置いた時期は、「1990 年以前」が 26.8%、「1991 年以降」が 66.0%となっている。最近の 2001 年、2002 年が共に 10%以上であり、近年にシステム監査人を初めて配置した事業体が多くなっている。無回答が 7.1%と他の調査項目に比較して多くなっているが、これはかなり以前に配置したが、何年と特定することができないためではないかと思われる。

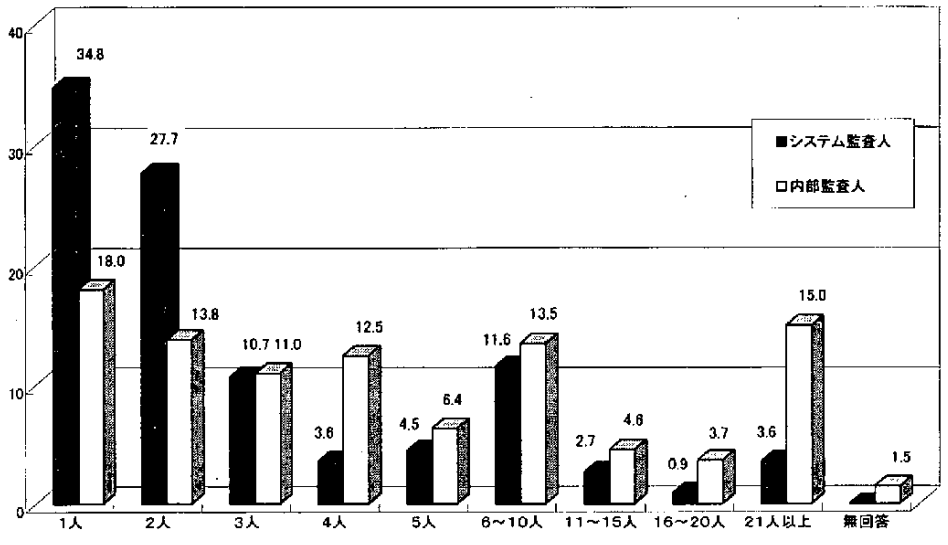

図3－1－4. 内部監査人とシステム監査人の配置状況(監査担当部門)

Q15. 貴社にはシステム監査技術者試験の合格者がいますか。(所属部門は問いません)

1	い　る	93	19.6	
2	いない	364	76.8	→Q17へ
無回答		17	3.6	
計		474	100.0	

Q15-1. 何人の合格者がいますか。

回答件数	93	-	平均	9.3 人	
1人	23	24.7	6～10人	12	12.9
2人	17	18.3	11～15人	2	2.2
3人	6	6.5	16～20人	5	5.4
4人	4	4.3	21人以上	11	11.8
5人	5	5.4	無回答	8	8.6

情報処理技術者試験が実施されて16年が経過(調査時点)した。全回答者に対する試験の合格者の有無の調査で、「合格者がいる」は、平成8年調査では18.3%、平成10年調査では19.4%、前回調査では19.3%であったが、今回調査では19.6%と前回調査とほぼ同様となった。業種別では、やはり情報処理サービス業・ソフトウェア業が59.7%と高く、ついで生命保険業が55.6%、輸送用機械器具製造業が28.6%、電気機械器具製造業が25.8%、金融業は21.9%となっている。

システム監査技術者試験の平均合格者数は9.3人であり、前回調査の8.0人に対し、1.3人増となった。内訳は、1人が24.7%、2人が18.3%であるが、一方、21名以上の回答は、11.8%となっている。21名以上の合格者がいると回答した業種は情報処理サービス業・ソフトウェア業が多く、他は電気機械器具製造業、生命保険業、金融業である。

業種グループ別に平均合格者数をみると、最も多いのが情報処理サービス業で13.9人、次に多いのが、電気・一般・輸送用機械器具製造業7.9人、金融・保険業7.8人となっている。

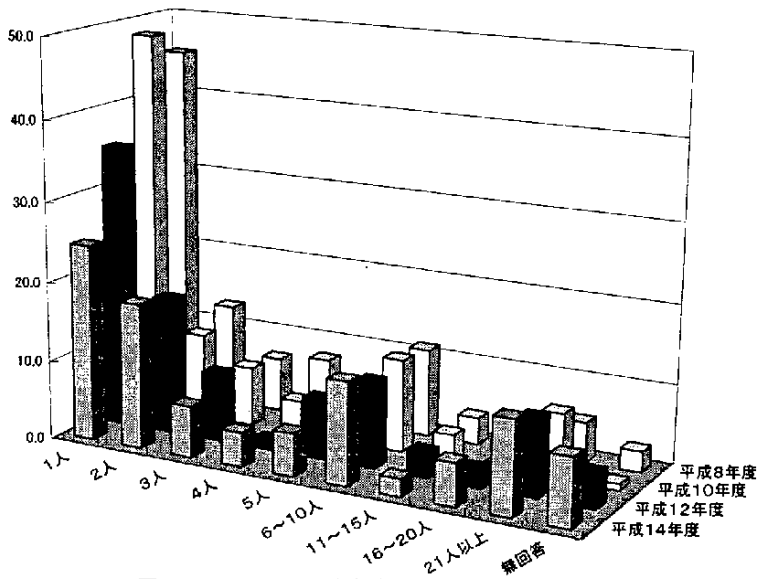

図3-1-5. システム監査技術者試験　合格者分布(監査担当部門)

Q16. 合格者はどこに所属していますか。(複数回答)

回答件数		93	-
1	内部監査部門	29	31.2
2	情報システム部門	65	69.9
3	その他	48	51.6

合格者が所属する部門(複数回答)は、「情報システム部門」が69.9%(前回調査72.0%)であり、「内部監査部門」に所属するのは31.2%(前回調査では29.0%)にすぎない。情報システム部門所属が内部監査部門所属を大きく上回っている。

「その他」の回答も51.6%となっており、合格者のいる事業体の約5割が、情報システム部門や内部監査部門以外の部門に所属させていることとなる。

Q17. 貴社ではシステム監査を実施したことがありますか。

1	ある	182	38.4	
2	ない	292	61.6	→Q57へ
計		474	100.0	

システム監査の実施状況は、監査担当部門、被監査部門の両部門に対し「過去にシステム監査を実施したことがあるか」、さらにシステム監査を実施したことがあるとした回答に対し、「2001年度に実施したか」の2項目の調査を行った。

「過去にシステム監査を実施したことがある」との回答は、監査担当部門では38.4%、被監査部門では39.3%となっている(Q14)。これまでの2回の調査においては、過去にシステム監査を「実施したことがある」が、平成10年調査では、監査担当部門は34.2%、被監査部門は33.6%、前回調査では監査担当部門36.7%、被監査部門35.4%となっている(被監査部門に関する分析は、「3.2.2」を参照のこと)。

この調査項目は、過去におけるシステム監査の実施状況の有無を問うもので、回答の母集団が同一であれば「実施した」の数値は徐々に増加するものであり、最初の調査が行われた昭和62年からその傾向となっている。今回の調査も前回調査と比較すると、監査担当部門は1.7ポイント、被監査部門は3.9ポイントの増加となっている。

過去にシステム監査を実施した状況を業種別にみると、監査担当部門の回答では、回答母数の多い業種に限ると、システム監査実施の割合が高いのは、金融業(70.3%)、情報処理サービス業・ソフトウェア業(55.2%)、電気機械器具製造業(45.2%)の順となっている。前回調査で金融業は58.0%であり、今回は12.3ポイント増加した。

回答数は少ないものの、損害保険業(100.0%)、生命保険業(88.9%)、電力・ガス事業(60.0%)、化学工業(47.6%)、輸送用機械器具製造業(42.9%)もシステム監査の実施率が高くなっている。

この調査の回答を、産業別にまとめると、建設・食品・繊維・化学・鉄鋼・電気などの製造業主体の第二次産業では31.0%、商業・金融・運輸・情報処理関連などのサービス業を主体とした

第三次産業では 49.4%となっている。

事業体の従業員数別でのシステム監査の実施状況をみると、実従業員数 1,000 人未満では 23.0%、1,000 人以上 5,000 人未満では 58.8%、5,000 人以上 10,000 人未満では 47.2%、10,000 人以上では 83.9%が監査を実施している。10,000 人以上では前回調査では 59.6%であったが、今回は 24.3 ポイントの増加となっている。

全体的傾向としては、従来からもそうであったが、社会的・公共的色彩の強い業種、あるいは規模の大きい事業体においてシステム監査の実施率が高くなっている。

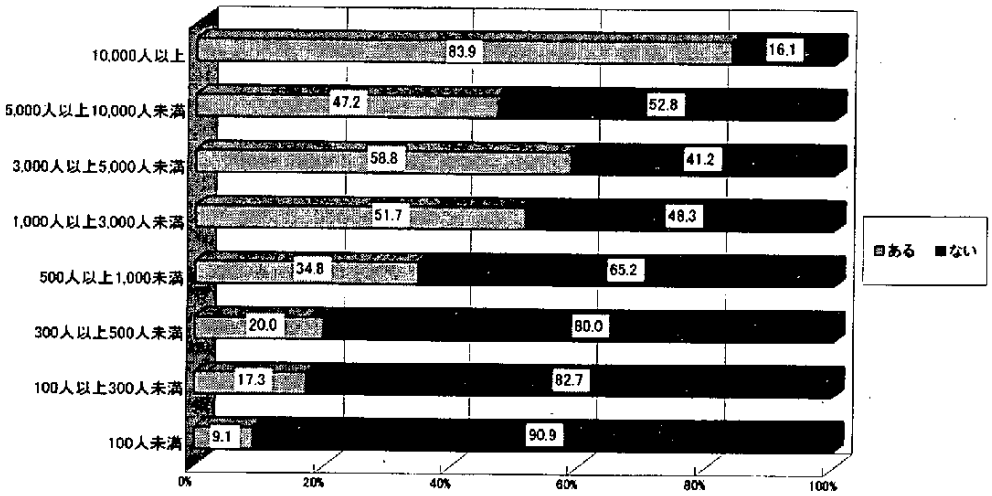

図3－1－6. システム監査実施状況(従業員数別－監査担当部門)

Q18. システム監査の実施に関する規程が定められていますか。

1	定められている	85	46.7
2	他の社内規程でシステム監査の実施が明記されている	35	19.2
3	定められていない	58	31.9
無回答		4	2.2
計		182	100.0

過去にシステム監査を実施した事業体のシステム監査規程を定めている状況については、監査担当部門では、「定められている」が 46.7%、「他の社内規定でシステム監査の実施が明記されている」が 19.2%であり、合計が 65.9%である。これまでの調査では、平成 8 年調査が合計 51.5%、平成 10 年調査が 54.7%、前回調査が 58.7%となっており、徐々に増加し、今回は 60%を大きく越えた。今回は、「定められている」が前回調査に比較し 1.3 ポイント減少したのに対し、「他の社内規定でシステム監査の実施が明記されている」が 8.5 ポイントの大幅な増加となっている。「定められている」割合が高い業種は、金融業の 77.8%、情報処理サービス業・ソフトウェア業の 48.6%、電気機械器具製造業の 50.0%である。

Q19. システム監査の実施において問題がありましたか。最も問題だと思われるものを1つ選んで下さい。

1	トップマネジメントのサポートが得られない	5	2.7
2	システム監査人が不足している	61	33.5
3	システム監査の実施に関する規程が整備されていない	21	11.5
4	システム監査のチェックリストが整備されていない	14	7.7
5	利用できるシステム監査技法が少ない	16	8.8
6	被監査部門の協力が得られない	1	0.5
7	委託先のシステム監査企業の実施内容が期待どおりでなかった	5	2.7
8	その他	16	8.8
9	問題はない	34	18.7
無回答		7	3.8
複数回答		2	1.1
計		182	100.0

システム監査を実施したことのある監査担当部門で、システム監査の実施体制の問題点について調査した。回答の約8割が何らかの問題点を挙げている。問題点としては、例年、「システム監査人の不足」を挙げている回答が多いが、今回調査でも33.5%が「システム監査人の不足」と回答している。ただし、前回調査では38.4%であったのに対し若干減少している。他の問題点としては、「システム監査の実施に関する規程が整備されていない」(11.5%)、「利用できるシステム監査技法が少ない」(8.8%)、「システム監査チェックリストが整備されていない」(7.7%)となっている。「その他」の回答は8.8%あった。

その他の意見としては、「社内の監査部門のノウハウ不足」、「専任体制(部署)がないことによる時間的制限や単年度内に監査できる領域の限度(限界)」等が挙げられた。

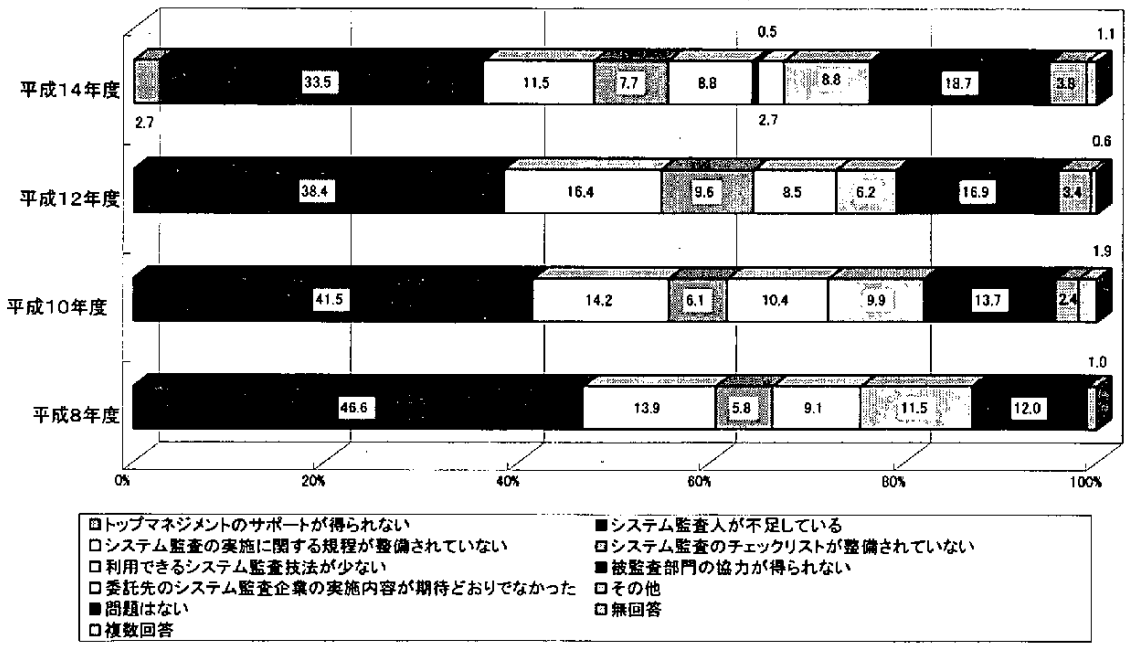

図3－1－7. システム監査体制上の問題点(監査担当部門)

Q20. システム監査は誰が実施するのが効果的だと思いますか。最も効果的と思うものを1つ選んで下さい。

1	監査役（団体等は監事、自治体は監査委員）	5	2.7
2	内部の監査人	87	47.8
3	情報システム部門の要員	10	5.5
4	システム監査技術者試験の合格者	20	11.0
5	監査法人・公認会計士	27	14.8
6	システム監査企業台帳に基づくシステム監査企業	22	12.1
7	その他	8	4.4
無回答		3	1.6
計		182	100.0

この調査は、システム監査を誰が実施するのが最も効果的であるかを監査担当部門、被監査部門に問うたものである。

システム監査を実施したことのある監査担当部門では、「内部の監査人」（47.8%）が高く、半数に近づいている。平成8年46.2%、平成10年45.3%、前回調査では42.9%であったが、今回調査では前回調査に比較して4.9ポイントの増加となっている。しかし約5割の値の回答は、実際のシステム監査の実施状況の調査でも内部監査部門型での実施率が高かったのと符合している。

「内部の監査人」についで高いのが、「監査法人･公認会計士」（14.8%）、「システム監査企業台帳に基づくシステム監査企業」（12.1%）、「システム監査技術者試験合格者」（11.0%）となった。前回調査では、「システム監査技術者試験合格者」（20.3%）、「システム監査企業台帳に基づくシステム監査企業」（16.4%）、「公認会計士」（6.2%）の順であった。今回の調査は、選択肢を「公認会計士」から「監査法人･公認会計士」に変更したことにより、数値の変化がおきたと思われる。

一方、被監査部門に対する同様の調査は全回答者が対象であるが、「システム監査企業台帳に基づくシステム監査企業」（37.3%）、「監査法人･公認会計士」（22.5%）、「内部の監査人」（16.6%）、「システム監査技術者試験合格者」（11.4%）となっている（Q38、被監査部門に関する分析は、「3.2.2」を参照のこと）。

その他の意見としては、「情報システムの企画・開発・運用の経験のあるシステム監査技術者試験の合格者」、「内部監査人と外部の有資格者による共同実施」等が挙げられた。

現在のシステム監査は、内部の監査人が実施している割合が高いが、誰が最もふさわしいかに関しては、監査担当部門と被監査部門の意見は大きく異なっている。監査担当部門が内部監査部門でよい、とするのに対し、被監査部門は外部からの監査の実施を望んでいる傾向があるといえる。この傾向はこれまでの調査でも同様であり、依然としてその傾向は変わっていない。

Q21. システム監査を実施する際、どのような点を充実させなければならないと思いますか。最も重要と思うものを1つ選んで下さい。

1	監査計画	29	15.9
2	事前調査	49	26.9
3	実地調査	41	22.5
4	改善勧告内容	26	14.3
5	監査報告会	2	1.1
6	チェックリスト	26	14.3
7	その他	4	2.2
無回答		5	2.7
計		182	100.0

システム監査の実施は、計画、実施、報告の段階からなり、実施では、事前調査と本調査からなる。またシステム監査を行う場合の確認項目を整理したチェックリストも、現場での監査作業を実施する際に重要である。これらのシステム監査の実施段階、あるいは準備作業等ではどの段階が重要と監査担当部門は考えているのだろうか。

今回の調査では、「事前調査」(26.9%)がトップとなり、以下、実地調査(22.5%)、「監査計画」(15.9%)、「改善勧告内容」、「チェックリスト」(ともに14.3%)であった。「事前調査」は、前回調査では16.9%であり、10.0ポイントの大幅な増加となった。しかし、それぞれの回答項目を比較しても大きな差はなく、いずれの段階も等しく重要である、との分析ができる。

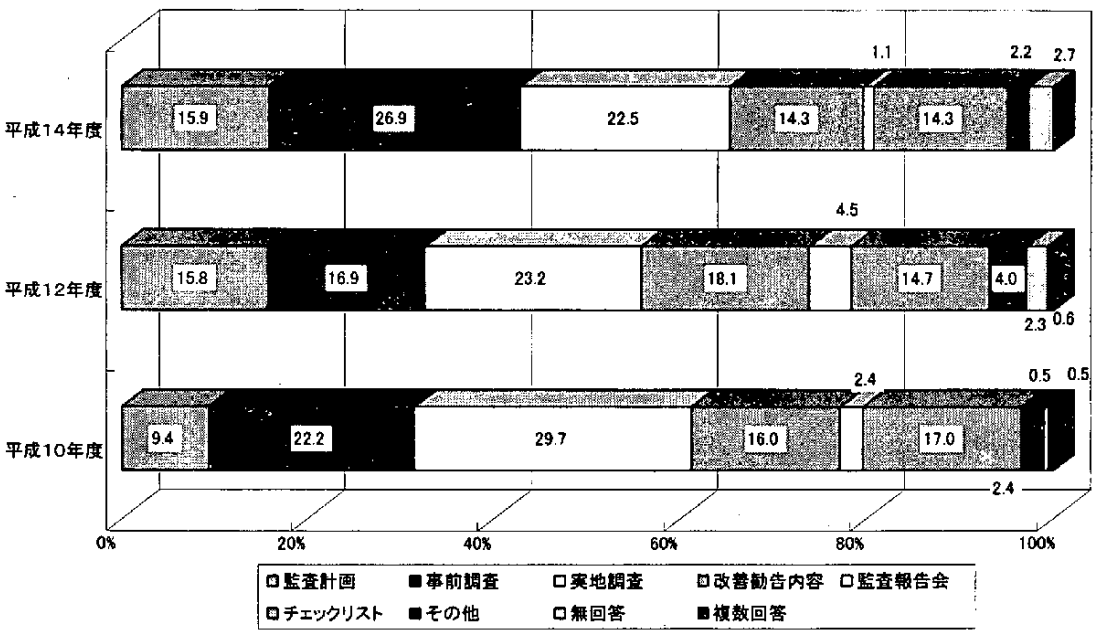

図3－1－8. システム監査で充実すべき点(監査担当部門)

Q22. 貴社ではシステム監査人は何人位必要だと思いますか。

平均	3.9人	
1人	22	12.1
2人	57	31.3
3人	38	20.9
4人	9	4.9
5人	13	7.1
6～10人	17	9.3
11～15人	3	1.6
16～20人	2	1.1
21人以上	2	1.1
無回答	19	10.4
計	182	100.0

監査担当部門ではシステム監査人の不足を訴えているが、システム監査人は何人位必要と思っているのであろうか。平成8年で平均3.6人、平成10年では平均3.7人、前回調査では5.5人と大きく増加したが、今回調査では前々回までの水準である3.9人となった。3.9人必要との値は、「Q14-1. システム監査人の人数」の平均であった4.0人とほぼ同じである。

Q23. システム監査人に最も不足していると思われる知識は何ですか。次の中から1つ選んで下さい。

1	経営に関する知識	17	9.3
2	業務知識	45	24.7
3	法律知識	17	9.3
4	監査知識	27	14.8
5	情報システムの知識	42	23.1
6	その他	8	4.4
7	わからない	14	7.7
無回答		11	6.0
複数回答		1	0.5
計		182	100.0

Q23、Q24でシステム監査人に最も不足している知識・能力について調査した。選択は、最も必要とされるものを1つのみ選択する質問形式であったが、知識に関しては、「業務知識」（24.7%）と「情報システムの知識」（23.1%）がほぼ同数であった。これまでもこの2分野がほぼ同数で並んでいる。今回の調査では、これまでの調査の選択肢としてはなかった「わからない」を設けたが、7.7%と予想より多い回答であった。

Q24. システム監査人に最も不足していると思われる能力は何ですか。次の中から1つ選んで下さい。

1	インタビュー能力	20	11.0
2	分析能力	60	33.0
3	判断能力	25	13.7
4	報告書作成能力	14	7.7
5	その他	8	4.4
6	わからない	41	22.5
無回答		13	7.1
複数回答		1	0.5
計		182	100.0

監査の実施には、監査能力を備えた監査人が実施することが、監査結果の妥当性と監査の有効性の観点から重要である。監査能力には「インタビュー能力」、「分析能力」、「判断能力」、「報告書作成能力」等があるが、監査人に対して現在不足している能力に関しての質問では、「分析能力」(33.0%)が圧倒的にトップであり、ついで「判断能力」(13.7%)、「インタビュー能力」(11.0%)となっている。今回の監査では、選択肢として新たに「わからない」(22.5%)を設けたが、この選択肢の回答が予想外に多かった。これは、いずれの能力も十分であるのか、あるいは逆に不足しているのかが、分析はできない。

Q25. システム監査人に対してどのような教育方法をとっていますか。主に行っているものを1つ選んで下さい。

1	外部セミナーを利用	61	33.5
2	社内教育	4	2.2
3	ＯＪＴ	29	15.9
4	通信教育	1	0.5
5	その他	3	1.6
6	特に教育は実施していない	47	25.8
7	監査を外部委託しているため該当しない	20	11.0
無回答		16	8.8
複数回答		1	0.5
計		182	100.0

システム監査人の知識や能力の向上を望む声は強いが、監査担当部門がシステム監査人に対してとる教育方法に関する調査では、前回調査とは異なり「外部セミナーを利用」(33.5%)がトップとなり、「特に教育は実施していない」(25.8%)を抜いた。今回の調査で新たに設定した選択肢「監査を外部委託しているため該当しない」は、11.0%であった。

Q26. システム監査の対象はどのようにして決定していますか。(複数回答)

回答件数		182	-
1	トップマネジメントの要求に基づいて決定	53	29.1
2	監査役（団体等は監事、自治体は監査委員）の要求に基づいて決定	21	11.5
3	内部監査部門長の判断に基づいて決定	99	54.4
4	システム監査人の独自の判断で決定	58	31.9
5	特定システムオペレーション（ＳＯ）企業認定制度に基づいて決定	9	4.9
6	プライバシーマーク制度の要求事項に基づいて決定	17	9.3
7	ISMS制度の要求事項に基づいて決定	12	6.6
8	その他	22	12.1
無回答		7	3.8

限られたシステム監査人の要員数、コスト、定められた期間等の制約の下で、幅広い情報システムのシステム監査を実施することは困難であり、どの分野に対して実施するかの決定は難しい課題である。システム監査の対象の決定方法に関しては、「内部監査部門長の判断に基づいて決定」(54.4%)、ついで「システム監査人の独自の判断で決定」(31.9%)、「トップマネジメントの要求に基づいて決定」(29.1%)、「監査役（団体等は監事、自治体は監査委員）の要求に基づいて決定」(11.5%) となっている。

「内部監査部門長の判断に基づく決定」は前回調査で40.1%であり、14.3ポイントの増加となり、依然としてトップである。これは実施方式の約7割が内部監査部門型であることと関連している。

注目できるのは、「トップマネジメントの要求に基づいて決定」(29.1%) が大幅に増加したことである。平成10年調査では10.4%、前回調査では16.4%であった。前回調査に比較しても倍増に近く、システム監査を普及させるには、トップマネジメントの理解が重要とされている状況で、大いに注目されるところである。

また、特定システムオペレーション（ＳＯ）企業認定制度やプライバシーマーク制度のそれぞれの制度の要求事項に基づいて決定されることも多くなってきている。

その他の意見としては、「監査法人の方針に基づいて決定する」、「親会社、グループ会社の要求により決定」、「内部監査規程に基づいて決定する」等が挙げられた。

Q27. 監査テーマはどのようにして決定していますか。(複数回答)

回答件数		182	-
1	トップマネジメントの要求に基づいて決定	51	28.0
2	監査役（団体等は監事、自治体は監査委員）の要求に基づいて決定	19	10.4
3	内部監査部門の判断で決定	103	56.6
4	システム監査人の独自の判断で決定	56	30.8
5	各種認定制度等の要求事項に基づいて決定	18	9.9
6	その他	20	11.0
無回答		9	4.9

システム監査の対象を決定した後には、具体的なシステム監査のテーマを決定する。この調査においても、システム監査の対象の決定と同様に「内部監査部門の判断で決定」が56.6%とトップとなっている。「システム監査人の独自の判断で決定」は30.8%、「トップマネジメントの要求に基づいて決定」は28.0%であり、「監査役の要求に基づいて決定」は10.4%となっている。これらの値は、いずれも前問のシステム監査対象の決定と近似している。ここでも、注目するのは「トップマネジメントの要求に基づいて決定」であり、前回調査の11.9%から28.0%と11.6ポイント増加している。

その他の意見は「Q26　監査対象」とほとんど同じ内容であった。

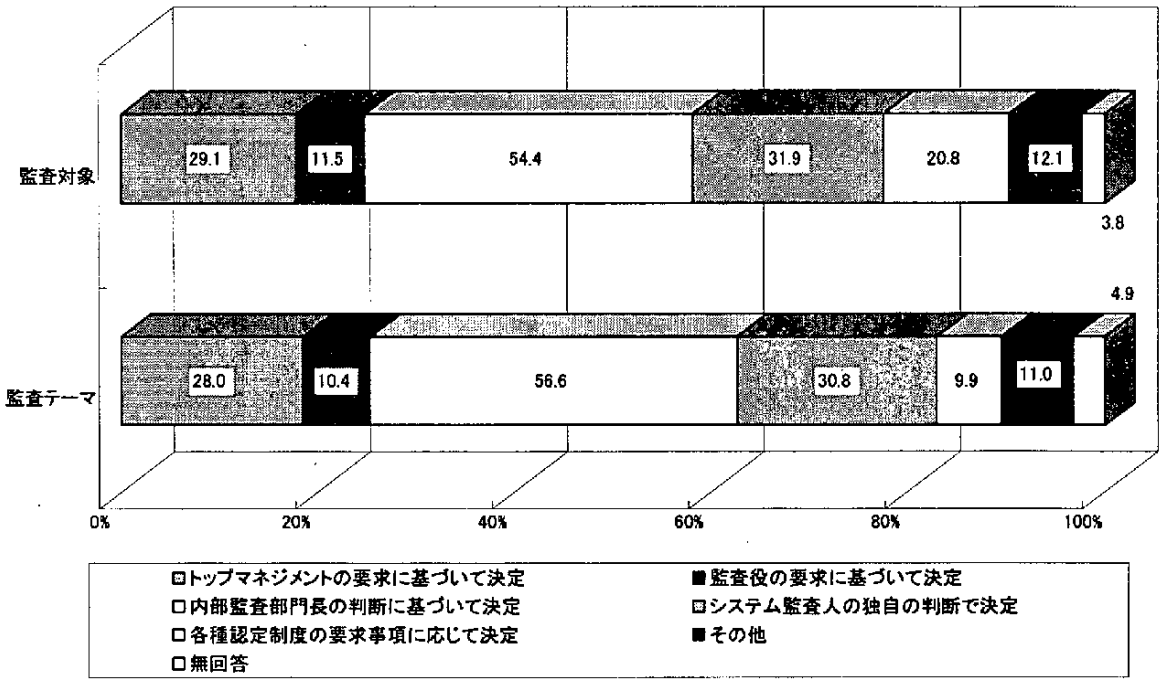

図3－1－9. システム監査対象／テーマの決定要件（監査担当部門）

Q28. システム監査の基本（年度）計画書を策定していますか。

1	い　る	91	50.0	→Q30へ
2	いない	89	48.9	
無回答		2	1.1	
計		182	100.0	

システム監査基本（年度）計画書は当該年度に実施する監査対象、重点監査テーマ、実施体制、年間スケジュールを内容とする計画であるが、システム監査を過去に実施した監査担当部門の50.0%が策定している。前回調査では53.1%であり、若干の減少となった。ただし、Q29にもあるように、実質的にシステム監査基本（年度）計画書を策定している事業体は多いと想定される。システム監査基本（年度）計画の立案とそれに基づく実施は、事業体でのシステム監査の定着に必要な事項であり、策定が定常化することが望まれる。

Q29.（Q28 の「2」を回答した場合）システム監査基本計画書を作成していない理由はなぜですか。（複数回答）

回答件数		89	-
1	必要性がない	4	4.5
2	個別計画書だけで十分である	4	4.5
3	内部監査計画に含まれている	31	34.8
4	システム監査基本計画書作成のルールがない	18	20.2
5	外部に委託しているので作成していない	13	14.6
6	必要に応じてシステム監査を実施しているため、作成していない	20	22.5
7	その他	8	9.0
無回答		6	6.7

今回調査から、システム監査の基本（年度）計画書を策定していない理由を新たに調査した。その結果、「内部監査計画に含まれる」(34.8%）がトップとなった。内部監査計画に含まれることは、実質的にシステム監査の基本（年度）計画を策定していると同様とみなせることができる。

Q30. システム監査を実施する場合、事前に被監査部門へ通知していますか。

1	い　る	164	90.1
2	いない	17	9.3
無回答		1	0.5
計		182	100.0

過去にシステム監査を実施したことのある監査担当部門にシステム監査を実施する場合、事前に被監査部門に対して通知しているかについて調査を行った。90.1%が「通知している」とし、「通知していない」の9.3%を大きく上回っている。前回調査では、「通知している」が83.6%であり、6.5ポイント増加した。前回調査で通知をしていない回答の割合が高い業種は金融業で32.5%であったが、今回調査では15.6%と低くなっている。金融業では、各部門、営業店に対する業務検査を予告なしに行うことが多く、システム監査にもその影響が現れていたが、システム監査では通知する場合が多くなっている。

3.1.3　平成13年度のシステム監査実施について

Q31. 平成13年度にシステム監査を実施しましたか。

1	した	138	75.8	
2	しない	43	23.6	→Q61へ
無回答		1	0.5	
計		182	100.0	

Q17の質問項目「過去にシステム監査を実施したことがある」との回答は、監査担当部門では38.4%であったが、このうち、平成13年度にシステム監査を実施した事業体は75.8%と、約4分の3が監査を実施している。

平成13年度に監査を実施した状況を業種別にみると、過去の実施状況と同様、生命保険業(100%)、金融業(86.7%)、情報処理サービス業・ソフトウェア業(86.5%)、化学工業(80.0%)、電気機械器具製造業(71.4%)となっており、これらの業種でシステム監査を継続的に実施している傾向が強いといえる。

Q32. システム監査は次のどの方式で実施しましたか。(複数回答)

回答件数		138	-	
1	内部監査部門型(監査部、検査部等が実施)	97	70.3	
2	部門監査型(情報システム部門が実施)	14	10.1	
3	指名方式 (トップから指名された者がシステム監査人となって実施)	5	3.6	→Q35へ
4	委員会方式(システム監査委員会を設置して実施)	5	3.6	
5	チームアプローチ(ｼｽﾃﾑ監査ﾌﾟﾛｼﾞｪｸﾄﾁｰﾑを編成して実施)	4	2.9	
6	外部委託型(システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託)	46	33.3	→Q33へ
7	その他	8	5.8	→Q35へ
無回答		1	0.7	

平成13年度にシステム監査を実施した事業体の監査担当部門に対する実施方式の調査(複数回答)では、70.3%が「内部監査部門型(監査部、検査部等が実施)」となっており、ついで「外部委託型(システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託)」(33.3%)、「部門監査型(情報システム部門で実施)」(10.1%)となっている。前回調査に比較して外部委託型が4.4ポイント増(前回調査28.9%)、内部監査部門型の3.1ポイント増(前回調査67.2%)、部門監査型が4.0ポイント減(前回調査14.1%)となっている。

一方、「指名方式(トップから指名された者がシステム監査人となって実施)」(3.6%)、「委員会方式(システム監査委員会を設置して実施)」(3.6%)、「チームアプローチ方式(システム監査プロジェクトチームを設置して実施)」(2.9%)の各方式は少ない。

その他の意見として、「親会社、グループ会社の監査部門」等が挙げられた。

Q33.（Q32で「6」を回答した場合）外部委託企業は、システム監査企業台帳登録企業ですか。

1	はい	25	54.3
2	いいえ	0	0.0
3	わからない	20	43.5
無回答		1	2.2
計		46	100.0

この調査項目は今回新たに設けたものであるが、システム監査を委託している場合の委託先企業について、その状況がわかる場合の回答は、すべてがシステム監査企業台帳登録企業であった。また、登録企業か否かが不明の回答も多かった。

Q34. 外部委託の場合、どこが実施しましたか。

1	監査法人（公認会計士を含む）	40	87.0
2	コンサルタント（個人／企業）	3	6.5
3	情報処理サービス業者	1	2.2
4	その他	1	2.2
無回答		1	2.2
計		46	100.0

この調査項目も今回新たに設定したものである。回答は、圧倒的に「監査法人（公認会計士を含む）」（87.0%）が多かった。

Q35. システム監査を実施した業務欄の数字に○をつけ、その業務について右欄の着眼点で最も重視した項目を1つ選んで下さい。（業務は複数回答）

着眼点／業務	実施業務	安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性	無回答	複数回答	計
企画業務	75	3	8	4	13	18	14	1	11	0	3	75
	54.3	4.0	10.7	5.3	17.3	24.0	18.7	1.3	14.7	0.0	4.0	100.0
開発業務	97	9	38	5	12	4	4	11	8	1	5	97
	70.3	9.3	39.2	5.2	12.4	4.1	4.1	11.3	8.2	1.0	5.2	100.0
運用業務	123	52	24	17	8	3	0	2	4	2	11	123
	89.1	42.3	19.5	13.8	6.5	2.4	0.0	1.6	3.3	1.6	8.9	100.0
保守業務	85	23	35	6	6	1	2	1	5	0	6	85
	61.6	27.1	41.2	7.1	7.1	1.2	2.4	1.2	5.9	0.0	7.1	100.0
計	138											
	100.0											

2001年度にシステム監査を実施した監査担当部門に、Q35、Q36でシステム監査実施業務を調査した。Q35は、システム監査基準のシステム構築の工程区分に準じた「企画業務」、「開発業務」、

「運用業務」、「保守業務」の各業務ごとに最も重視した着眼点を回答する方式とした。

システム監査の実施業務は、「企画業務」が54.3%（前回調査50.0%）、「開発業務」が70.3%（前回調査67.2%）、「運用業務」が89.1%（前回調査88.3%）、「保守業務」が61.6%（前回調査63.3%）であった。業務別で調査した結果は、これまでも実施率の高い順から「運用業務」、「開発業務」、「保守業務」、「企画業務」であり、その傾向は変わらない。システム監査の実施率の向上と共に「保守業務」を除く他の業務では実施率がわずかではあるが増加している。

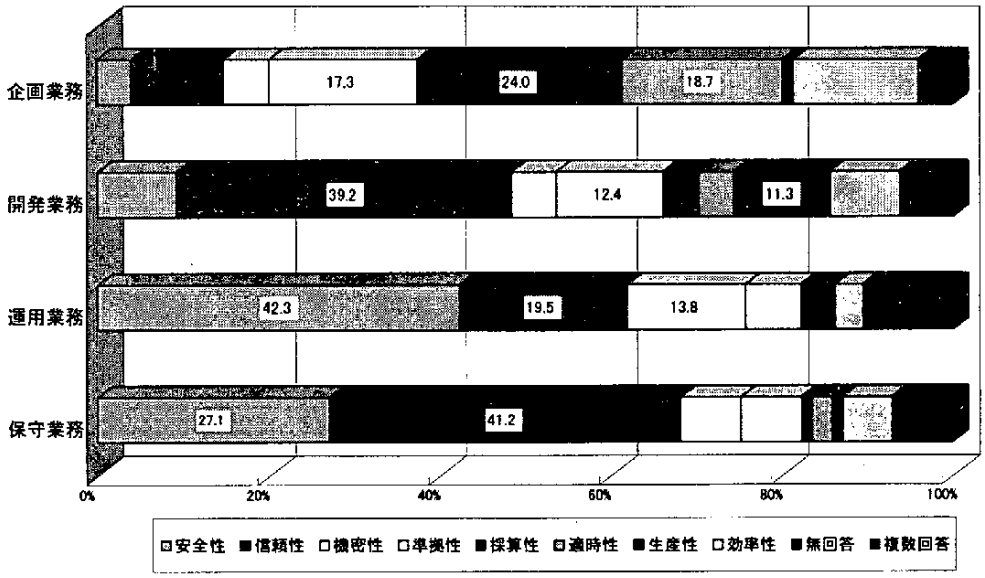

図3－1－10. 監査で重視した着眼点（業務別－監査担当部門）

システム監査をより効果的なものにするためには、企画業務、開発業務、運用業務、保守業務の各業務で、システム監査で最も重視する着眼点は異なってくる。それぞれの業務においてシステム監査の実施時に最も重要視する着眼点を調査した。

企画業務の着眼点は、「採算性」の回答が最も多く24.0%、ついで「適時性」が18.7%、「準拠性」が17.3%であった。前回調査では、「採算性」（28.1%）、「準拠性」（18.8%）、「適時性」（17.2%）の順であり、採算性重視の傾向は変わらない。これは昨今の経営環境の変化に対して情報システムの構築のコスト対効果を重要視してきていることが現れているものと思われる。いずれにせよ、この3点の着眼点は、特に企画業務で明確にしておかなければならない点であり、企画業務のシステム監査で効果が得られるものである。

開発業務で最も重視した着眼点は、「信頼性」（39.2%）で回答の約4割近くを占めている。前回の調査でもトップであったが、そのときの38.4%よりさらに高い割合を占めている。ついで「準拠性」（12.4%）、開発業務では重要な観点とみられている「生産性」（11.3%）となっている。企画業務における準拠性は、法制度、ガイドライン等事業体外のルール等に対する準拠状況の監査が多いと思われるが、開発業務のそれは事業体内の開発規約、開発ルールに対する準拠性であり、その内容は異なると思われる。

システム監査が最も実施されている運用業務では「安全性」（42.3%）、「信頼性」（19.5%）、「機密性」（13.8%）の順となった。前回調査ではトップが「信頼性」（34.5%）であり、ついで「安全性」（31.0%）、「機密性」（7.1%）と、今回調査では信頼性が15.0ポイントも減少したの

に対し、安全性が11.3ポイント増、同じく機密性が6.7ポイント増となった。情報セキュリティ対策の必要性が強くなっている事の現れであるといえよう。

保守業務では、「信頼性」が最も多く41.2%である。ついで「安全性」が27.1%であり、ここでは前回調査より信頼性が0.5ポイント微増したのに対し、安全性が5.0ポイント減少した。

Q36. システム監査を実施したテーマ欄の数字に○をつけ、そのテーマについて右欄の着眼点で最も重視した項目を1つ選んで下さい。(テーマは複数回答)

①実施テーマ

回答件数	138	-
ドキュメント管理	82	59.4
進捗管理	68	49.3
品質管理	75	54.3
コスト管理	55	39.9
要員管理	64	46.4
外部委託（開発の委託）	74	53.6
外部委託（アウトソーシング）	72	52.2
セキュリティ対策	117	84.8
ネットワーク管理	81	58.7
ソフトウェアの適正利用（ライセンス管理）	65	47.1
個人情報保護対策	83	60.1
ＰＣ管理、モバイル機器管理	70	50.7
コンピュータウイルス対策	82	59.4
情報システム関連のリスク管理	80	58.0
災害対策	77	55.8
その他	9	6.5
無回答	3	2.2

今回調査では、「企画業務」から「保守業務」のシステムのライフサイクルの工程とは別の切り口として、監査対象分野ごとの実施状況の調査を実施した。その結果、最も多かったのは「セキュリティ対策」(84.8%)の監査であり、情報システムの安全性に対する関心度の向上がうかがえる。安全性の観点からのシステム監査としては、「個人情報保護対策」(60.1%)、「コンピュータウイルス対策」(59.4%)、「情報システム関連のリスク管理」(58.0%)、「災害対策」(55.8%)も多くなっている。

②着眼点

テーマ＼着眼点	安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性	無回答	複数回答	計
ドキュメント管理	5	12	9	41	0	6	0	3	1	5	82
	6.1	14.6	11.0	50.0	0.0	7.3	0.0	3.7	1.2	6.1	100.0
進捗管理	3	3	0	11	0	23	11	11	1	5	68
	4.4	4.4	0.0	16.2	0.0	33.8	16.2	16.2	1.5	7.4	100.0
品質管理	7	53	1	5	1	1	2	1	0	4	75
	9.3	70.7	1.3	6.7	1.3	1.3	2.7	1.3	0.0	5.3	100.0
コスト管理	0	1	1	3	26	0	5	14	1	4	55
	0.0	1.8	1.8	5.5	47.3	0.0	9.1	25.5	1.8	7.3	100.0
要員管理	7	3	5	5	3	2	20	15	1	3	64
	10.9	4.7	7.8	7.8	4.7	3.1	31.3	23.4	1.6	4.7	100.0
外部委託（開発の委託）	8	21	14	5	5	1	8	7	0	5	74
	10.8	28.4	18.9	6.8	6.8	1.4	10.8	9.5	0.0	6.8	100.0
外部委託（ｱｳﾄｿｰｼﾝｸﾞ）	15	11	19	5	9	1	2	3	2	5	72
	20.8	15.3	26.4	6.9	12.5	1.4	2.8	4.2	2.8	6.9	100.0
セキュリティ対策	59	9	38	3	0	0	0	0	0	8	117
	50.4	7.7	32.5	2.6	0.0	0.0	0.0	0.0	0.0	6.8	100.0
ネットワーク管理	35	17	18	1	0	1	0	3	1	5	81
	43.2	21.0	22.2	1.2	0.0	1.2	0.0	3.7	1.2	6.2	100.0
ｿﾌﾄｳｪｱの適正利用（ﾗｲｾﾝｽ管理）	5	5	6	38	1	3	0	0	2	5	65
	7.7	7.7	9.2	58.5	1.5	4.6	0.0	0.0	3.1	7.7	100.0
個人情報保護対策	14	2	47	14	0	0	0	0	0	6	83
	16.9	2.4	56.6	16.9	0.0	0.0	0.0	0.0	0.0	7.2	100.0
ＰＣ管理、モバイ機器管理	14	4	25	13	2	2	1	2	0	7	70
	20.0	5.7	35.7	18.6	2.9	2.9	1.4	2.9	0.0	10.0	100.0
コンピュータウイルス対策	60	8	5	2	0	0	0	0	0	7	82
	73.2	9.8	6.1	2.4	0.0	0.0	0.0	0.0	0.0	8.5	100.0
情報システム関連のリスク管理	37	13	7	14	0	3	0	2	0	4	80
	46.3	16.3	8.8	17.5	0.0	3.8	0.	2.5	0.0	5.0	100.0
災害対策	57	5	0	6	1	3	0	1	0	4	77
	74.0	6.5	0.0	7.8	1.3	3.9	0.0	1.3	0.0	5.2	100.0
その他	0	1	1	3	0	0	0	2	2	0	9
	0.0	11.1	11.1	33.3	0.0	0.0	0.0	22.2	22.2	0.0	100.0

平成13年度にシステム監査を実施した監査担当部門に、監査分野ごとの最も重視する着眼点を調査した。

ドキュメント管理では「準拠性」が 50.0%と圧倒的に多く、これはドキュメントの作成状況、網羅性、記述様式など、ドキュメントの作成要領などへの遵守を重要視しているものと思われる。

進捗管理では「適時性」が 33.8%でトップであり、ついで「準拠性」、「生産性」、「効率性」（ともに 16.2%）となっている。

外部委託関係では、開発の委託とアウトソーシングがあるが、開発の委託では「信頼性」（28.4%）、アウトソーシングでは「機密性」（26.4%）を最も重視しており、若干異なっている。

セキュリティ関連のセキュリティ対策、個人情報保護対策、コンピュータウイルス対策、情報システムのリスク管理などは、当然ながらそれぞれ「安全性」、「信頼性」あるいは「機密性」が圧倒的に高くなっている。

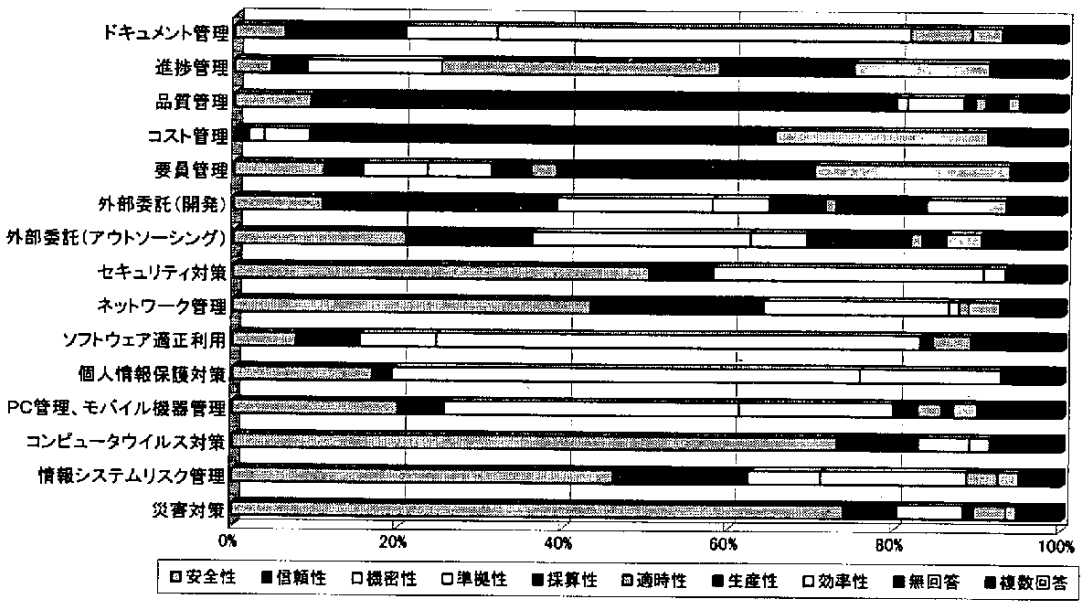

図3－1－11. 監査で重視した着眼点(テーマ別－監査担当部門)

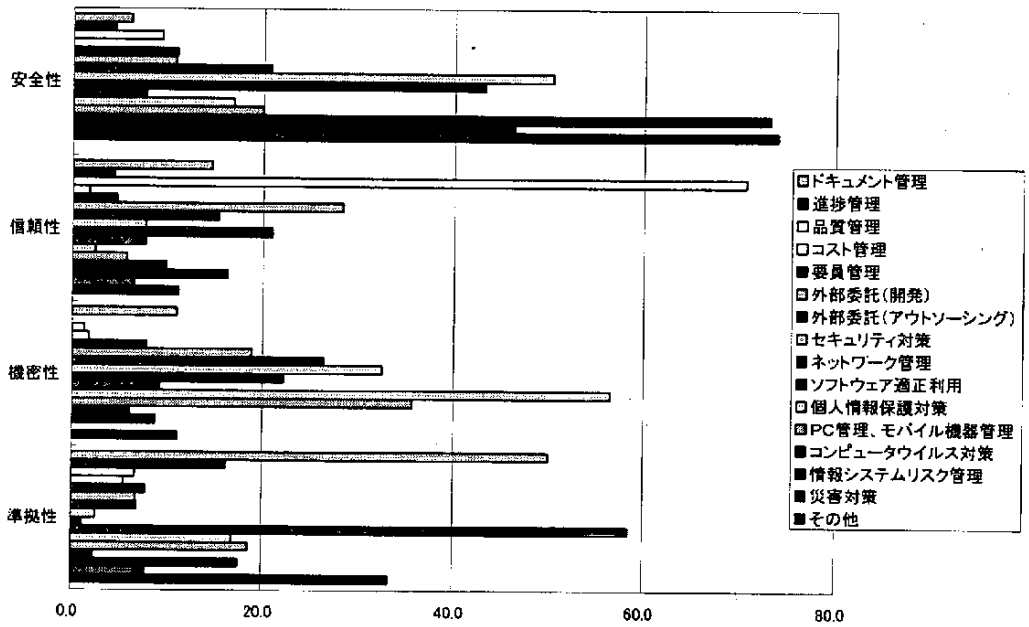

図3－1－12－1. システム監査で実施した着眼点(監査担当部門)

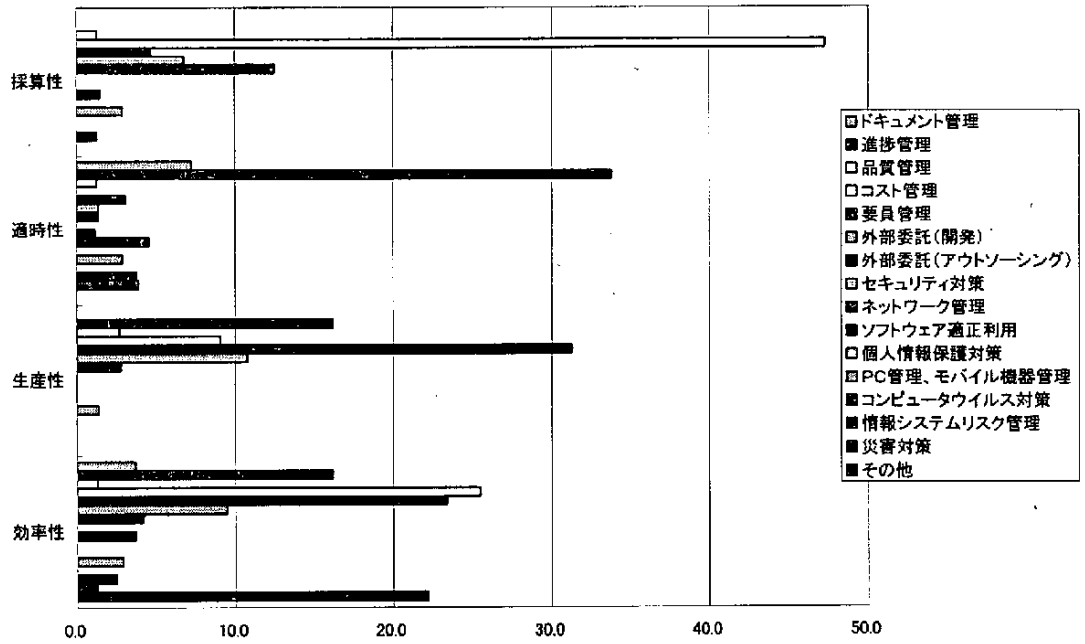

図3－1－12－2. システム監査で重視した着眼点(監査担当部門)

Q37. コンピュータ犯罪、ヒューマンエラー、事故、災害対策、個人情報保護の５項目について、防止ならびに早期発見の観点から、システム監査において特に重視すべき分野はどこだと思いますか。各項目ごとに最も重要と思われる分野（１～１２）を１つだけ選んで下さい。

分野／項目	データの入力プロセス	データ処理プロセス	出力プロセス	プログラム変更	オペレーション	情報保管(データ管理)	入退室(館)管理	システム開発	ハードウエア *1	ソフトウエア *2	ネットワーク	電源設備	無回答	複数回答	計
コンピュータ犯罪防止	8	10	3	10	7	56	12	0	0	5	21	0	5	1	138
	5.8	7.2	2.2	7.2	5.1	40.6	8.7	0.0	0.0	3.6	15.2	0.0	3.6	0.7	100.0
ヒューマンエラー防止	27	8	0	20	55	5	4	11	0	2	0	0	6	0	138
	19.6	5.8	0.0	14.5	39.9	3.6	2.9	8.0	0.0	1.4	0.0	0.0	4.3	0.0	100.0
事故防止	2	6	1	9	26	13	11	18	18	8	11	5	8	2	138
	1.4	4.3	0.7	6.5	18.8	9.4	8.0	13.0	13.0	5.8	8.0	3.6	5.8	1.4	100.0
災害対策	0	1	0	0	7	29	6	3	32	2	22	29	7	0	138
	0.0	0.7	0.0	0.0	5.1	21.0	4.3	2.2	23.2	1.4	15.9	21.0	5.1	0.0	100.0
個人情報保護	2	3	10	0	2	107	3	3	0	0	2	0	5	1	138
	1.4	2.2	7.2	0.0	1.4	77.5	2.2	2.2	0.0	0.0	1.4	0.0	3.6	0.7	100.0

＊1　CPUと周辺機器／＊2　基本ソフトとアプリケーションソフト

コンピュータ犯罪、ヒューマンエラー、事故、災害対策、個人情報保護に対してトラブル防止および発生時の早期発見の観点からシステム監査を実施する場合の最も重視すべき分野を情報システムを構成する要素、行為に分けて調査した。

コンピュータ犯罪防止では、「情報保管（データ管理）」（40.6％）が圧倒的に多かった。この傾向は、当然ながら個人情報保護でも情報保管（データ管理）は77.5％と高かった。

ヒューマンエラー防止では、「オペレーション」（39.9％）、「データの入力プロセス」（19.6％）が高く、事故防止では回答は分散しているものの、比較的、「オペレーション」（18.8％）、「システム開発」（13.0％）が高くなっている。

災害対策では「ハードウェア」（23.2％）、「情報保管（データ管理）」、「電源設備」（ともに21.0％）、「ネットワーク」（15.9％）が多くなっている。ハードウェアの回答は、二重化やバックアップ構成を重要視しており、電源設備の回答は自己の事業体のトラブルより電源の供給停止を想定したものである。またネットワークは、事業体内外のネットワークの迂回路を重要視したと想定される。回答の選択肢に「施設」があれば、バックアップ施設の設置、あるいは施設の災害に対する強化措置の実施などの回答により、調査結果は異なっていたかもしれない。

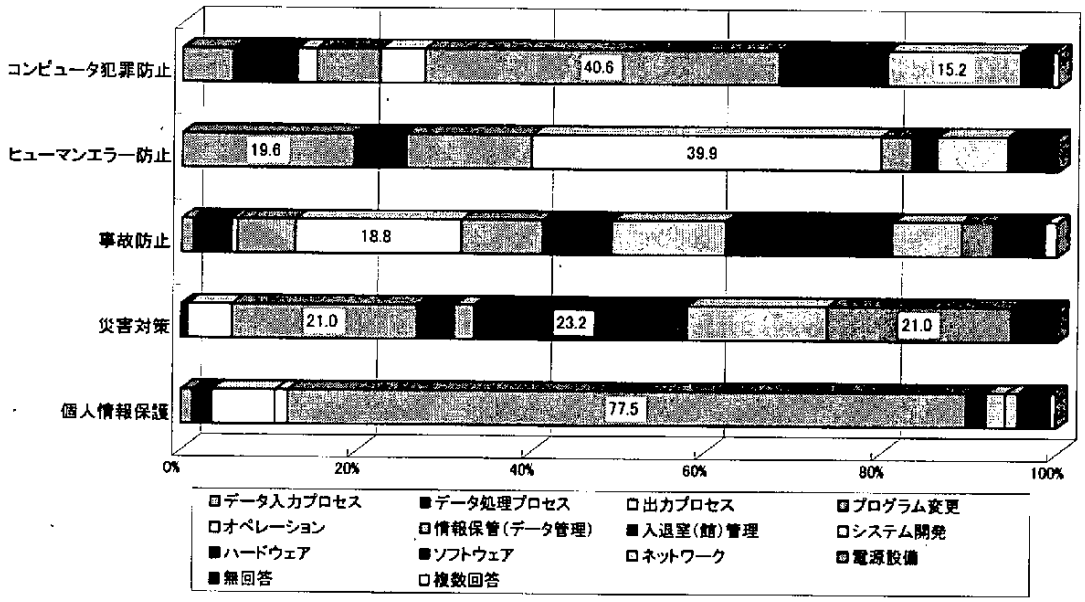

図3－1－13. コンピュータ犯罪防止、ヒューマンエラー防止、事故防止、災害対策、個人情報保護の観点から最も重視すべき分野（監査担当部門）

Q38. システム監査を実施する際に、以下の基準等を利用しましたか。

基準類 ＼ 利用状況	利用した		利用しない		無回答		計	
システム監査基準	100	72.5	30	21.7	8	5.8	138	100.0
情報システム安全対策基準	85	61.6	44	31.9	9	6.5	138	100.0
コンピュータウイルス対策基準	69	50.0	58	42.0	11	8.0	138	100.0
コンピュータ不正アクセス対策基準	66	47.8	60	43.5	12	8.7	138	100.0
プライバシーマーク監査ガイドライン	41	29.7	85	61.6	12	8.7	138	100.0
ＩＳＭＳガイド	29	21.0	94	68.1	15	10.9	138	100.0

経済産業省などで公表している各種の基準、ガイドラインを自己のシステム監査の実施時に活用しているかの調査を行った。当然ながら「システム監査基準」（72.5%）の活用が多く、「情報システム安全対策基準」（61.6%）がこれに続いている。コンピュータウイルス対策基準」（50.0%）や「コンピュータ不正アクセス対策基準」（47.8%）も約半数で使用されており、これらの基準は広く活用されていると言えよう。

一方、「プライバシー監査ガイドライン」（29.7%）、「ＩＳＭＳガイド」（21.0%）は、特定の分野（プライバシーおよびセキュリティ全般）を対象としたものであり、また公表されてから日も浅いため、今回の調査では低い値となっている。

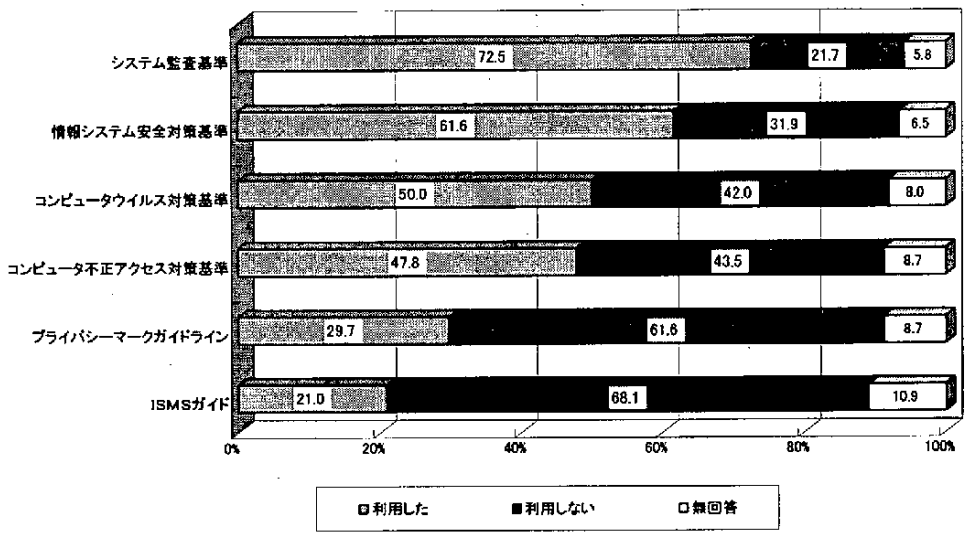

図3－1－14. システム監査実施時の利用基準類(監査担当部門)

Q39. システム監査において自社用のチェックリストを作成していますか。

1	い　る	107	77.5
2	いない	29	21.0
無回答		2	1.4
計		138	100.0

システム監査の実施ではなんらかのチェックリストを使用することが多い。システム監査におけるチェックリストの利用状況についてシステム監査を実施したことがある監査担当部門に対し調査を行った。

「利用している」は77.5%と高く、「利用していない」は21.0%であった。これは前回調査に対して、「利用している（前回調査82.8%）が5.3ポイント減少したのに対し、「利用していない」（前回調査5.5%）は15.5ポイント増加した。なお、前回調査での「チェックリストを利用している」の77.5%の回答は、「既存のチェックリスト（例：システム監査基準）をそのまま利用」（7.0%）、「既存のチェックリストを修正して利用」（28.9%）、および「独自のチェックリストを作成している」（46.9%）の合計である。

今回の「作成している」の減少は、設問の「自社用のチェックリストを作成」の文言から、既存のチェックリストの利用や修正利用の事業体が「いない」と回答した可能性がある。

Q40 からQ49 では、監査担当部門の情報システムに対する評価を信頼性、安全性、効率性の観点からみている。

Q40. 貴社の情報システムの信頼性は十分だと思いますか。

1	十分だと思う	11	8.0
2	やや十分だと思う	55	39.9
3	普通だと思う	41	29.7
4	やや不十分だと思う	21	15.2
5	不十分だと思う	7	5.1
6	わからない	2	1.4
無回答		1	0.7
計		138	100.0

情報システムの品質を維持し障害の発生を減少させる観点ある信頼性は、「十分である」(8.0%)、「やや十分だと思う」(39.9%)で半数近くになっている。

Q41. 貴社の情報システムの信頼性を高めるために改善の余地があると思いますか。

1	思　う	130	94.2
2	思わない	5	3.6
3	わからない	2	1.4
無回答		1	0.7
計		138	100.0

監査担当部門が情報システムの信頼性に対して「改善の余地」があると感じている比率は94.2%ときわめて高い。

Q40 では、自社の情報システムの信頼性に対してプラスの評価が高かったが、それでも「改善の余地がある」と監査部門では評価をしている。このことは信頼性に限らず、この後の調査項目である安全性、効率性においても同様の回答結果となっている。

Q42. 貴社の情報システムの信頼性を高めるためにもっと投資すべきだと思いますか。

1	思　う	90	65.2
2	思わない	28	20.3
3	わからない	19	13.8
無回答		1	0.7
計		138	100.0

監査担当部門が評価する情報システムの信頼性に対して、もっと投資を行い信頼性を向上させる必要があると判断している割合は65.2%と高くなっている。

Q40 からQ42 までの信頼性の評価を整理すると、次のようになる。

監査担当部門は自社の情報システムの信頼性に対し、約半数が信頼性は十分、あるいはやや十分としており、３割が普通として評価している。しかし、信頼性を高めるための改善作業はほとんどの監査担当部門が必要と認識し、全体の３分の２の監査担当部門では、投資をして信頼性を向上させる必要があるとしている。

Q43. 貴社の情報システムの安全性は十分だと思いますか。

1	十分だと思う	9	6.5
2	やや十分だと思う	57	41.3
3	普通だと思う	34	24.6
4	やや不十分だと思う	23	16.7
5	不十分だと思う	11	8.0
6	わからない	3	2.2
無回答		1	0.7
計		138	100.0

自然災害、不正アクセスおよび破壊行為から情報システムを護る観点である安全性に対して、監査部門は「十分だと思う」(6.5%)、「やや十分だと思う」(41.3%) をあわせると、信頼性と同様、約半数がプラスの評価をしている。しかし、前回調査に比較して、「十分だと思う」は 0.5 ポイントの減少（前回調査 7.0%)、「やや十分だと思う」は 5.6 ポイントの減少（前回調査 46.9%）となっており、セキュリティに対しての関心が高まってきていることに関連し、若干ではあるが辛い評価が増加している。

Q44. 貴社の情報システムの安全性を高めるために改善の余地があると思いますか。

1	思　う	125	90.6
2	思わない	8	5.8
3	わからない	4	2.9
無回答		1	0.7
計		138	100.0

この調査も信頼性と同様、安全性も十分、やや十分と評価はしているものの、さらに改善の余地があるとしている。

Q45. 貴社の情報システムの安全性を高めるためにもっと投資すべきだと思いますか。

1	思　う	94	68.1
2	思わない	26	18.8
3	わからない	17	12.3
無回答		1	0.7
計		138	100.0

投資に関しても、信頼性と同様、安全性に対しても約７割がその必要性を回答している。

Q46. 貴社の情報システムの効率性は十分だと思いますか。

1	十分だと思う	1	0.7
2	やや十分だと思う	41	29.7
3	普通だと思う	50	36.2
4	やや不十分だと思う	30	21.7
5	不十分だと思う	12	8.7
6	わからない	3	2.2
無回答		1	0.7
計		138	100.0

情報システムの資源の活用および費用対効果の観点からの効率性に対しては、監査部門は「十分だと思う」(0.7%)、「やや十分だと思う」(29.7%)とプラス面を評価する回答は全体の3割である。一方「やや不十分だと思う」(21.7%)と「不十分だと思う」(8.7%)も同様に約3割であり、いずれともいえない。これは、監査担当部門が信頼性、安全性と比較して、効率性に対しては厳しい見方をしていることを現している。

前回調査では、「十分だと思う」(2.3%)、「やや十分であると思う」(35.9%)であり、いずれも今回調査では減少し、より厳しい見方となった。

Q47. 貴社の情報システムの効率性を高めるために改善の余地があると思いますか。

1	思　う	129	93.5
2	思わない	3	2.2
3	わからない	5	3.6
無回答		1	0.7
計		138	100.0

効率性に関しては、信頼性、安全性同様、大多数の回答が改善の余地があるとしている。

Q48. 貴社の情報システムの効率性を高めるためにもっと投資すべきだと思いますか。

1	思　う	96	69.6
2	思わない	22	15.9
3	わからない	19	13.8
無回答		1	0.7
計		138	100.0

投資に関しても、信頼性と同様、効率性に対しても約7割がその必要性を回答している。

Q49. 貴社の情報システムは、総合的に見て満足できる状態ですか。

1	十分満足	2	1.4
2	満足	48	34.8
3	なんともいえない	45	32.6
4	多少不満	29	21.0
5	大いに不満	10	7.2
6	わからない	1	0.7
無回答		3	2.2
計		138	100.0

事業体ではさまざまな情報システムがあり、またその機能や運用形態もさまざまである。それぞれの情報システムには長所や改善必要な事項など異なったさまざまな状況であるが、あえて監査担当部門に総合的な見地から情報システムを評価してもらった。

「十分満足」(1.4%) および「満足」(34.8%) と評価する割合が回答の約３分の１となっている。この結果は、前回調査の「十分満足」(1.6%) および「満足」(39.8%) に比較するとわずかではあるが厳しい見方となっている。

一方、「多少不満」(21.0%)、「大いに不満」(7.2%)のマイナスの評価は約３割となっている。選択肢の「なんともいえない」(32.6%) は、普通として理解してよいのか、あるいは満足な情報システムもあれば不満足な情報システムもある、と理解してよいかなんともいえない。

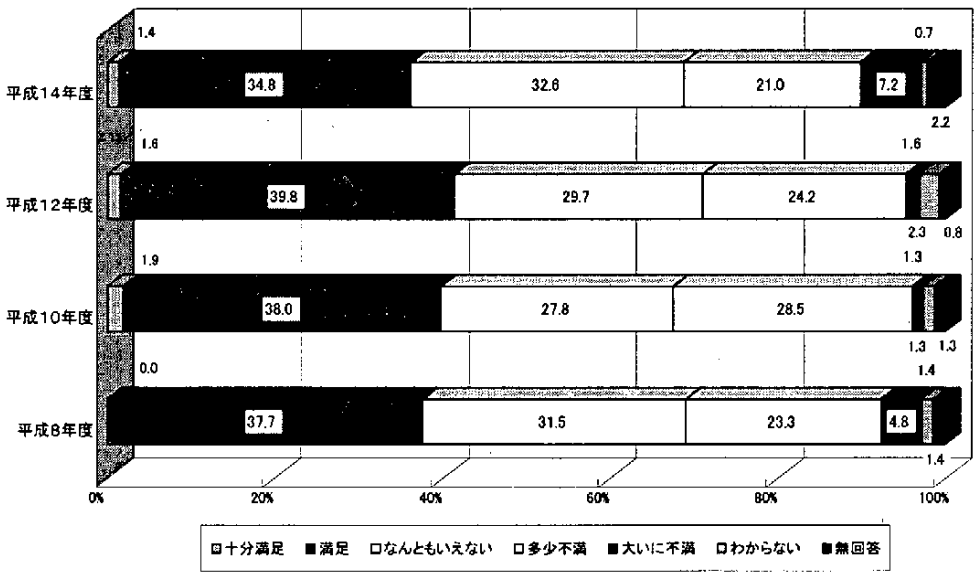

図3－1－15. 情報システムに対する評価(監査担当部門)

今回の調査ではQ50 で公表会の開催状況を、Q51 で報告会の開催状況を調査した。

システム監査の目的は、情報システムの信頼性、安全性、効率性のレベルを向上し、情報システムに係るリスクを回避することにある。そのためには、被監査部門がシステム監査結果について十分に理解、納得することが重要である。その結果として監査結果がシステム改善等に反映されることが必要である。

講評会は、監査報告書の作成前に監査担当部門と被監査部門との間で開催されるものであり、システム監査実施時の事実誤認を排除するとともに、被監査部門のシステム監査結果に対する理解を深めることを目的とする。

一方、監査報告会は、監査報告書作成後に監査担当部門が関係者に対し行うものであり、監査報告における指摘事項・改善勧告への対応を明確にすることを目的とする。システム監査実施の目的を達成し、その効果を高めるためには、講評会、監査報告会の実施が不可欠である。

Q50. 監査結果について、情報システム部門との間での講評会（監査報告書を作成する前に意見交換、確認等を行うことをいう）を行いましたか。

1	行った	125	90.6
2	行わなかった	10	7.2
無回答		3	2.2
計		138	100.0

講評会はシステム監査実施事業体の90.6%で開催されている（なお、被監査部門に対する同一の調査では84.3%であった（Q25）。被監査部門に関する分析は、「3.2.3」を参照のこと）。

Q51. 監査報告書の作成後に関係者を含めた監査報告会を行いましたか。

1	行った	98	71.0	
2	行わなかった	36	26.1	→Q53へ
無回答		4	2.9	
計		138	100.0	

監査報告会の実施状況は、システム監査実施事業体の7割強の71.0%で実施されている（なお、被監査部門に対する同一の調査では69.1%であった（Q26）。被監査部門に関する分析は、「3.2.3」を参照のこと）。7割の実施率は、過去の調査結果と大きな違いはない。

Q52. 監査報告会に出席したのは誰ですか。（複数回答）

回答件数		98	-
1	最高経営者（会長、社長、知事、市長等）	45	45.9
2	財務担当役員	20	20.4
3	情報システム担当役員	47	48.0
4	監査役	38	38.8
5	情報システム部門の管理者	72	73.5
6	内部監査人	59	60.2
7	ユーザ部門の管理者	42	42.9
8	外部のシステム監査人	11	11.2
9	その他	9	9.2

監査報告会への出席者は、「情報システム部門の管理者」（73.5%）、「内部監査人」（60.2%）、「情報システム担当役員」（48.0%）、「最高経営者」（45.9%）、「ユーザ部門の管理者」（42.9%）、「監査役」（38.8%）、「財務担当役員」（20.4%）の順となっている。「情報システム部門の管理者」の出席が最も多いが、前回調査（74.2%）に比べ0.7ポイント減少している。これに対し、「最高経営者」は前回調査（36.6%）に対し、今回調査では45.9%、9.3ポイント増加した。

その他の出席者としては、「関連部門の管理責任者」、「(内部)監査部門の担当役員」、「弁護士」等が挙げられた。

Q53. 監査報告書（原本）は誰に提出（報告書の宛先）しましたか。

注）複数部署に配布している場合は、その中で最高権限者を選んで下さい。

1	最高意思決定機関（取締役会、理事会、議会等）	19	13.8
2	最高経営者（社長、理事長、首長等）	79	57.2
3	担当役員	18	13.0
4	監査役（団体等は監事、自治体は監査委員）	3	2.2
5	内部監査部門長	6	4.3
6	その他	5	3.6
無回答		4	2.9
複数回答		4	2.9
計		138	100.0

監査報告書の提出先については、「最高経営者」が57.2%、「最高意思決定機関」が13.8%、「担当役員」が13.0%となっており、この三者で約9割近くとなっている。大部分の事業体で監査報告書がトップマネジメントに提出されているといえよう。

被監査部門、監査役、会計監査人への監査報告書の写しの配布状況をQ54～Q56で調査した。

Q54. 監査報告書の写を被監査部門に配布しましたか。

1	し　た	130	94.2
2	しない	7	5.1
無回答		1	0.7
計		138	100.0

「被監査部門への配布」（94.2%）の調査結果に見られるように、多くの事業体に被監査部門に監査報告書を配布している。

Q55. 監査報告書の写を監査役に配布しましたか。

1	し た	99	71.7
2	しない	36	26.1
無回答		3	2.2
計		138	100.0

「監査役への配布」（71.7%）となっており、前回調査の 75.0%と大きな変化はない。

Q56. 監査報告書の写を貴社の会計監査人に配布しましたか。

1	し た	28	20.3
2	しない	104	75.4
無回答		6	4.3
計		138	100.0

被監査部門、監査役に対しての監査報告書の配布は多かったが、これに対し、会計監査人に配布している事業体は依然として少ない。時系列でみると、

10.1%（平成２年調査）
12.8%（平成４年調査）
14.2%（平成６年調査）
17.8%（平成８年調査）
20.3%（平成 10 年調査）
25.8%（平成 12 年調査）

と前回調査までは年々増加する傾向にあったが、今回は、20.3%と減少した。

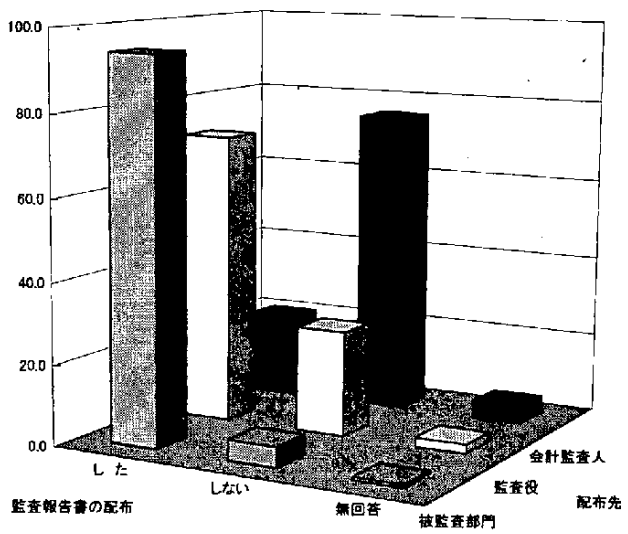

図3－1－16. 監査報告書の配布先（監査担当部門）

3.1.4. 未実施および実施可能性について

（Q57からQ60までは、Q17でシステム監査を実施していない企業のみの回答）

Q57. システム監査を実施していない理由はどのような点ですか。次の中から主な理由を1つ選んで下さい。

1	システム監査についてトップマネジメントの認識が欠如している	11	3.8
2	システム監査の実施のためのコンセンサス、組織風土が十分に育っていない	44	15.1
3	システム監査の実施よりもシステム化推進そのものに力点がある	63	21.6
4	システム監査を実施する担当者（部門）の確保が難しい	49	16.8
5	システム監査の方法、制度、手続きなどが十分でない	52	17.8
6	システム監査の効果が明確でない	5	1.7
7	システム監査の必要性を感じない	27	9.2
8	その他	11	3.8
無回答		26	8.9
複数回答		4	1.4
計		292	100.0

これまでシステム監査を実施しなかった監査担当部門に対し、未実施の理由を調査した。回答は、主な理由を1つ選択するもので、「システム監査の実施よりもシステム化推進そのものに力点がある」（21.6%）が、前回調査（22.0%）と比較して微減してはいるが最も多い回答となっている。ついで「システム監査の方法、制度、手続き等が十分でない」（17.8%）、「システム監査を実施する担当者（部門）の確保が難しい」（16.8%）、「システム監査の実施のためのコンセンサス、組織風土が十分に育っていない」（15.1%）となっており、前回調査で4位であった「システム監査の方法、制度、手続き等が十分でない」が2位となっている。

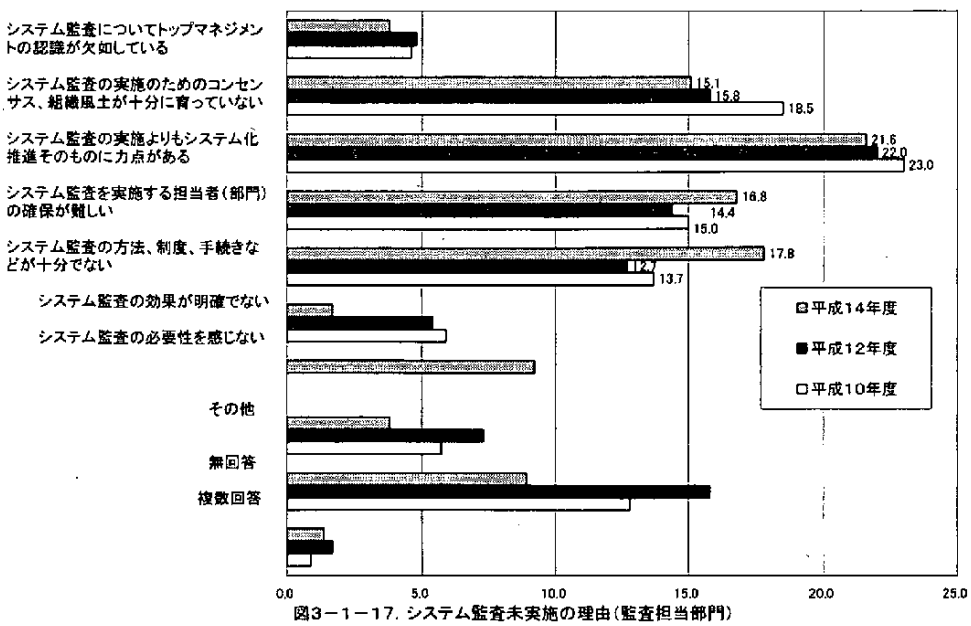

図3－1－17. システム監査未実施の理由（監査担当部門）

Q58. 今後、システム監査についてどのように対応されますか。次の中から1つ選んで下さい。

1	現在、システム監査の導入を計画中	29	9.9	
2	2～3年以内には導入の予定	49	16.8	
3	当面導入の予定はない	163	55.8	→Q61へ
4	将来とも導入の予定はない	18	6.2	→Q61へ
5	その他	8	2.7	
無回答		25	8.6	
計		292	100.0	

同じくシステム監査未実施の回答者に対する今後のシステム監査実施の可能性の調査では、「現在システム監査の導入を計画中」が9.9%、「2～3年以内には導入予定」が16.8%と、前回調査と比べそれぞれ4.0ポイント、3.5ポイント増加している。

一方、「当面導入の予定はない」は55.8%、「将来とも導入の予定はない」は6.2%と、あわせて62.0%の事業体がシステム監査の導入を予定していない。

Q59. どのような体制で進められる予定ですか。(複数回答)

回答件数		78	-
1	内部監査部門型（監査部、検査部等が実施）	39	50.0
2	外部委託型（システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託）	9	11.5
3	決まっていない	32	41.0
無回答		1	1.3

現在計画中、および2～3年以内には導入を予定している監査担当部門のシステム監査の実施体制は、「内部監査部門型」(50.0%) と多く、「外部委託型」(11.5%) となっている。

Q60. 特にどのような観点から監査を進められる予定ですか。次の中から1つ選んで下さい。

1	安全性（システムの物理的安全性／不正防止）	35	44.9
2	信頼性（ハードウェア／ソフトウェアの正確さに基づく信頼性）	9	11.5
3	機密性（データの権限者以外への機密）	17	21.8
4	準拠性（法律、条例、規則等への準拠）	8	10.3
5	採算性（コスト面からの効率）	2	2.6
6	適時性（開発、導入、アウトプット作成等のタイミング）	0	0.0
7	生産性（リソース面からの効率）	0	0.0
8	効率性（システム目標の達成度合い）	2	2.6
無回答		1	1.3
複数回答		4	5.1
計		78	100.0

システム監査を実施する場合の、主とする観点は何であるかについては、「安全性」が高く44.9%（前回調査32.9%）、ついで「機密性」21.8%（前回調査19.0%）、「信頼性」11.5%（前回調査10.1%）、「準拠性」10.3%（前回調査6.3%）が高く、「効率性」、「採算性」（ともに2.6%）は低くなっている。

増加が顕著なのは「安全性」（12.0ポイント）および「準拠性」（4.0ポイント）で、セキュリティ対策の重視とコーポレートガバナンス強化の影響があるものと思われる。一方、「効率性」は11.3ポイントの減少となっている。

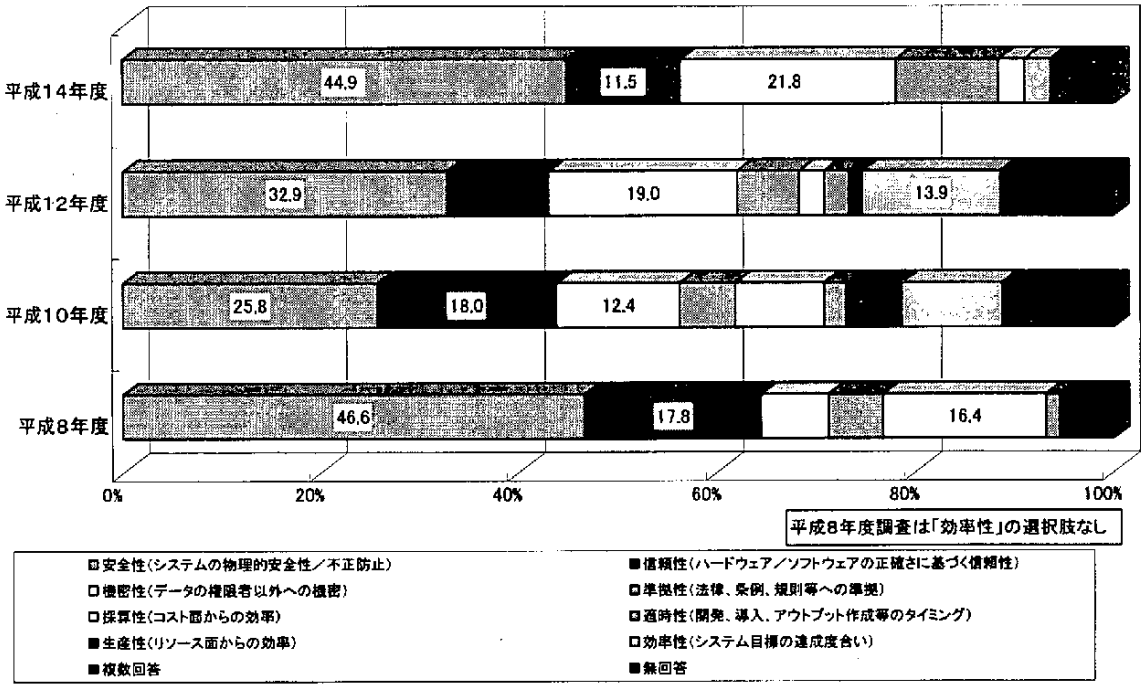

図3－1－18. システム監査を実施する際に重視する観点（監査担当部門）

3.1.5 情報セキュリティの推進について

Q61. 貴社では情報セキュリティポリシーを策定していますか。

1	定めている	207	43.7
2	現在作成中である	76	16.0
3	作成を検討している	96	20.3
4	現在、定める予定がない	84	17.7
無回答		11	2.3
計		474	100.0

情報セキュリティポリシーの策定状況について、「定めている」が43.7%と半数に近い状況であり、「現在作成中」を含めると59.7%、さらに、「作成を検討している」を含めると80.0%の事業体が情報セキュリティに対して積極的な姿勢であることがわかる。同一の質問を被監査部門にも行っている（Q39）が、「定めている」との回答については監査担当部門の方が策定率が高い。

（Q61～Q65の質問については被監査部門でも同一の調査を行っているので、「3.2.4」を参照のこと。）

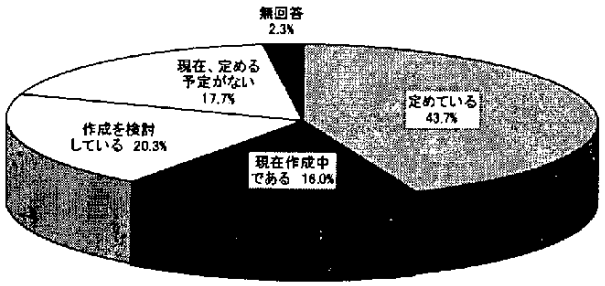

図3－1－19. 情報セキュリティポリシーの策定状況(監査担当部門)

Q62. 貴社では情報セキュリティをどのような体制で推進していますか。(複数回答)

回答件数		474	-
1	情報セキュリティ担当役員を設置している	92	19.4
2	情報セキュリティ委員会を設置している	109	23.0
3	情報システム部門主導で実施している	240	50.6
4	情報セキュリティ専任者を設置している	65	13.7
5	各部門・拠点にセキュリティ担当者を設置している	102	21.5
6	外部のセキュリティコンサルタントを活用している	31	6.5
7	特に実施していない	95	20.0
8	その他	7	1.5
無回答		14	3.0

情報セキュリティ推進体制について、情報セキュリティを推進する責任者としての「情報セキュリティ担当役員」、意思決定と推進を行う「情報セキュリティ委員会」、また、情報セキュリティを実効的に推進する「情報セキュリティ専任者」（情報セキュリティ管理者等）やユーザ側で情

報セキュリティを推進する「情報セキュリティ担当者」（情報セキュリティアドミニストレータ等）の設置、自社に十分なノウハウが蓄積されていない場合の「外部の人材の活用」などについて調査を行った。ただし、日本の場合、過去の経緯から情報システムの運用・保守、情報システムの開発を行う「情報システム部門」が情報セキュリティについても推進役となっていることから、これらの推進体制について調査した。

「情報セキュリティ担当役員」を設置しているのは、19.4％と全体の約５分の１であった。「情報セキュリティ委員会」は23.0％であったが、「情報セキュリティ専任者」は13.7％と前者と比べ9.3ポイント低い。

これらの結果から、事業体が情報セキュリティの重要性を認識していることがわかる。ただ、担当役員を置いていても、情報セキュリティを推進する実行組織がなければ、なかなか情報セキュリティは進展しない。この点からは、「情報セキュリティ委員会の設置」が 23.0％であったとはいえ、「担当役員の設置」（19.4％）に比べると、まだ低い状況にあるといえよう。

一方、「外部のセキュリティコンサルタント活用」が6.5％というのはかなり低く、いまだ情報セキュリティの推進は自組織内で進めていく意向が強いことがわかる。なお、20.0％が情報セキュリティを推進する体制ができていない。

Q63. 情報セキュリティ推進体制で最も重要と思われることを１つだけ選んで下さい。

1	経営者のリーダーシップ	82	17.3
2	全社的な推進体制	243	51.3
3	情報システム部門の推進体制	35	7.4
4	利用部門の理解・協力	94	19.8
5	その他	2	0.4
無回答		17	3.6
複数回答		1	0.2
計		474	100.0

事業体としての情報セキュリティの推進にあたっての意識について、監査担当部門では「全社的な推進体制」が51.3％と最も多く、「経営者のリーダシップ」（17.3％）を大幅に上回っており、経営者よりも全社的な推進体制を希望していることがわかる。これは、監査担当部門はシステム監査を通じて情報セキュリティの推進を図っており、このためには全社的な情報セキュリティに対する推進体制が重要と考えていることがわかる。

わが国では経営者のリーダシップや全社的な推進体制を作ってトップダウン型に情報セキュリティを推進するよりも、利用部門からのボトムアップで進めていく方が効率がよい場合もある。「利用部門の理解・協力」について、監査担当部門19.8％、被監査部門22.5％と、いずれも約５分の１がボトムアップ型で情報セキュリティを進めている実態がわかる。情報セキュリティは最も情報セキュリティの弱いところから破綻することもある。したがって、事業体として一致して情報セキュリティ対策をとらなければならないことも多い。ただし、トップダウンで命令しただけでは、たとえばユーザにＩＤやパスワードの管理を徹底するのは難しいことも指摘されており、今後、事業体の中でどのように情報セキュリティを推進するか、より重要となると思われる。

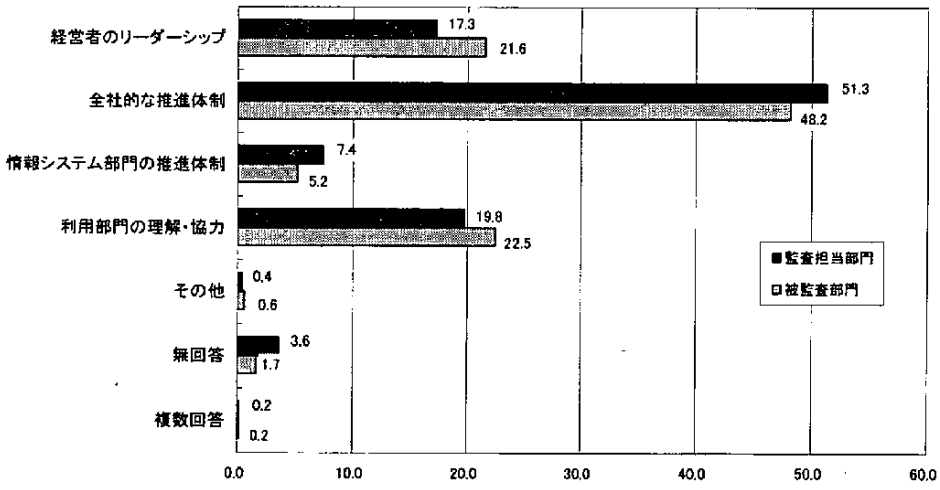

図3－1－20. 最も重要と思われる情報セキュリティ推進体制

Q64. 貴社では情報セキュリティについて、優先的に実施しているものを3つまで選んで下さい。
（複数回答）

回答件数		474	－
1	情報セキュリティ対策コストの確保	88	18.6
2	リスク分析の実施	110	23.2
3	システム監査の実施	88	18.6
4	情報セキュリティ教育の実施	170	35.9
5	情報セキュリティ体制の確立	241	50.8
6	情報セキュリティアドミニストレータの確保	16	3.4
7	情報資産の洗い出し	78	16.5
8	ＩＳＭＳの取得	30	6.3
9	プライバシーマークの取得	27	5.7
10	その他	8	1.7
11	特に実施していない	106	22.4
無回答		19	4.0
複数回答（４つ以上選択）		1	0.2

事業体が情報セキュリティを推進する場合、さまざまな対策項目を行わなければならない。しかし、事業体では戦略と整合性が必要であり、また、情報セキュリティ対策には費用が発生するため、全体の中でバランスをとりながら進めていかなければならない。ここでは、このような背景の中で具体的にどのような項目を優先して進めているかの実態を調査した。調査結果では、監査担当部門、被監査部門の間であまり大きな乖離はみられなかった。

監査担当部門で高い評価のものからあげると、「情報セキュリティ体制の確立」、「情報セキュリティ教育」、「リスク分析」、「情報セキュリティ対策コスト」、「システム監査」、「情報資産の洗い出し」の順となっている。この順番はきわめて妥当なものであり、情報セキュリティの重要性が認識されつつあることを意味しているといえよう。

Q65. 貴社では情報セキュリティについてどのような教育を実施していますか。(複数回答)

回答件数		474	-
1	新入社員教育を実施している	120	25.3
2	一般社員向け教育を実施している	170	35.9
3	管理職教育を実施している	91	19.2
4	役員教育を実施している	17	3.6
5	派遣要員向け教育を実施している	35	7.4
6	情報セキュリティ担当者の専門教育を実施している	52	11.0
7	その他	20	4.2
8	特に実施していない	195	41.1
無回答		19	4.0

事業体で一人一台のパソコン環境が実現され、また多くがインターネット接続されるようになった現在、情報セキュリティは、もはや専門家だけが対応すればよい、というものではなくなっている。特に、新しくインターネットやパソコンを利用するようになった従業員や事業体の構成員に正しい情報セキュリティ教育や訓練を行い、正しい使い方ができるようにすることが望まれる。以上のことから、事業体でどのような教育を行っているかが今後情報セキュリティに敏感な対応のとれる組織に発展するためには欠かすことができない事項となる。

今回の調査結果から、教育の実態は監査担当部門および被監査部門で大変よく似た傾向にあることがわかる。ただ、「管理職教育の実施」や「派遣要員向け教育の実施」の２項目については監査担当部門の方が若干上回っている。おそらく管理職が自分の持ち場で情報セキュリティをきちんと守れるように組織的に行うためには、監査担当部門を有する事業体の方が啓蒙の点から優れているといえよう。ただし、懸念されるのは、現在、インターネットの急速な広がりやブロードバンドの低価格化に伴いインターネットの利用者の方がセキュリティ対策の実施よりも早く広がっており、インターネットのウイルス、DoS 攻撃、不正侵入などがどんどん深刻化を増している。このような現実の中で、教育はアンケート調査にあるように新入社員や一般社員向けの教育のみならず、専門家への再教育、より高度な教育も必要である。この観点から、「情報セキュリティ担当者の専門教育を実施している」がわずか 10％を越えた程度では、現実の厳しい情報セキュリティ対策を進めるうえで心許ないと言わざるを得ない。

Q66. 貴社では情報セキュリティポリシー監査を実施したことがありますか。

1	あ　る	59	12.4
2	な　い	402	84.8
無回答		13	2.7
計		474	100.0

この調査は監査担当部門のみに対して行っている。

「JIS X 5080:2002　情報技術－情報セキュリティマネジメントの実践のための規範」(以下、「JIS X 5080:2002」という。) では、定期的に情報セキュリティポリシーを見直すことが述べられている。

3.1.2　**見直し及び評価**　基本方針には，定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者が，存在することが望ましい。見直し手続によって，当初のリスクアセスメントの基礎事項に影響を及ぼす変化（例えば，重大なセキュリティの事件・事故，新しいぜい（脆）弱性，又は組織基盤若しくは技術基盤の変化）に対応して確実に見直しを実施することが望ましい。

（「JIS X 5080:2002」3.1.2から抜粋）

ここで重要なのは、情報セキュリティ基本方針を情報セキュリティ環境が技術の進歩や社会へのインターネットの広がりに合わせて大きく変化することに対応していかなければならないことである。このためには、情報セキュリティポリシーを定期的に見直し、その環境に対応して重要な情報資産を保護する必要がある。この観点から、情報セキュリティポリシーに対する監査も重要な要素といえる。これについて「JIS X5080:2002」は次のように監査や第三者によるレビューを示唆している。

・情報セキュリティの他者によるレビュー　情報セキュリティ基本方針文書（3.1参照）には，情報セキュリティの基本方針及び責任を記述する。組織の行動が基本方針を適切に反映し，基本方針が実行可能及び有効であることを保証するために，情報セキュリティ基本方針の実施を他者がレビューすることが望ましい（12.2参照）。
このようなレビューは，内部監査部門，他部門の管理者又はそのようなレビューを専門とする第三者組織が実施してもよい。ただし，その場合，レビューを実施する者は，適切な技能及び経験をもつものとする。

（「JIS X 5080:2002」3.1.2から抜粋）

しかし、今回の調査では、情報セキュリティポリシーに関する監査については、わずか12.4%しか実施しておらず、84.8%が未実施という結果となった。

この事実を事業体のトップに知ってもらい、早急に見直せる体制を作ることが必要である。

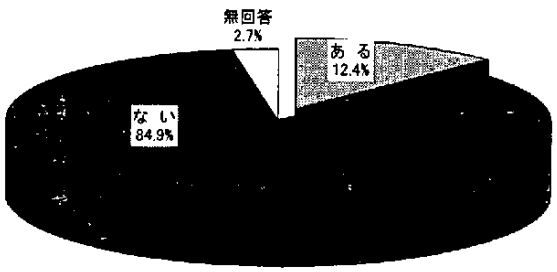

図3－1－21. 情報セキュリティポリシー監査実施状況(監査担当部門)

3.1.6 電子メールの利用について

（Q67～71 の質問については被監査部門での同一の調査を行っているので、「3.2.5」を参照のこと。）

Q67. 電子メール利用のルールを定めていますか。

1	定めている	280	59.1	
2	現在作成中である	23	4.9	
3	作成を検討している	63	13.3	
4	現在、定める予定がない	64	13.5	
5	わからない	29	6.1	
6	電子メールを利用していない	6	1.3	→終了
無回答		9	1.9	
計		474	100.0	

電子メールの利用が一般化している中で、77.3%の事業体が利用のルールを作成もしくは作成の必要性を感じている。この傾向は特定の業種に偏ったものではない。従業員数が多い事業体ほど、ルールの必要性を感じている。

Q68. 要員の電子メールの利用状況を監視していますか。

1	監視している	175	38.1	
2	今後、監視する予定がある	65	14.2	
3	監視していない	185	40.3	→Q70 へ
4	わからない	33	7.2	→Q70 へ
無回答		1	0.2	
計		459	100.0	

電子メールを利用している事業体のうち、52.3%が利用状況を監視または監視を予定している。

業種グループ別にみると、機械器具製造業や金融・保険業、情報処理サービス業での実施率は高いが、政府・地方公共団体の実施率が低い。

Q69.（Q68 で「1」、「2」を回答した場合）電子メール利用状況の監視について、ルールを定めていますか。

1	ルールを定め、社員に周知している	128	53.3
2	ルールは定めているが、社員に周知していない	36	15.0
3	現在作成中である	19	7.9
4	作成を検討している	41	17.1
5	現在、定める予定がない	10	4.2
6	わからない	4	1.7
無回答		2	0.8
計		240	100.0

電子メールの利用状況を監視または監視を予定している事業体のうち、53.3%がそのルールを定め、社員に周知している。

Q70. 自宅や出張先からメールサーバへのリモートアクセスを認めていますか。

1	認めている	106	23.1
2	許可制で認めている	121	26.4
3	認めていない	200	43.6
4	わからない	25	5.4
無回答		7	1.5
計		459	100.0

電子メールを利用している事業体のうち、43.6%がリモートアクセスを認めておらず、中でも政府・地方公共団体で「認めていない」とする割合が高い。情報漏洩や外部からの攻撃を防御するためには、リモートアクセスを認めない方針が妥当だが、モバイル運用の必要に応える必要性もあり、複数のセキュリティ対策を組み合わせて実施する必要がある。

Q71. 自宅の個人アドレスへの社内メールの転送を認めていますか。

1	認めている	133	29.0
2	許可制で認めている	56	12.2
3	認めていない	204	44.4
4	わからない	60	13.1
無回答		6	1.3
計		459	100.0

電子メールを利用している事業体のうち、44.4%が自宅の個人アドレスへ転送を認めておらず、政府・地方公共団体では66.7%が認めていない。

Q72. 電子メールの利用に関して、監査を実施したことがありますか。

1	あ　る	41	8.9
2	な　い	417	90.8
無回答		1	0.2
計		459	100.0

電子メールの利用がリスクマネジメント上、大きな脅威になっているが、監査対象として実施された割合が8.9%と非常に低い。

3.2 被監査部門対象

3.2.1 システム監査一般について

Q１．経済産業省から「システム監査基準」（平成８年改訂）が公表されていることを知っていますか。

1	利用したことがある	92	14.2
2	内容は知っているが、利用したことはない	188	29.0
3	存在だけは知っている	282	43.5
4	知らない	87	13.4
計		649	100.0

システム監査基準の認知度は 86.7％で９割近くが基準を「知っている」状況であり、高い認知度といえる。この値は平成 10 年 87.2％、前回調査 86.4％とほぼ一定している。

しかしながら、実際に基準を「利用したことがある」との回答は 14.2％（前回調査 14.5％）と 15％にも満たない低い値である。

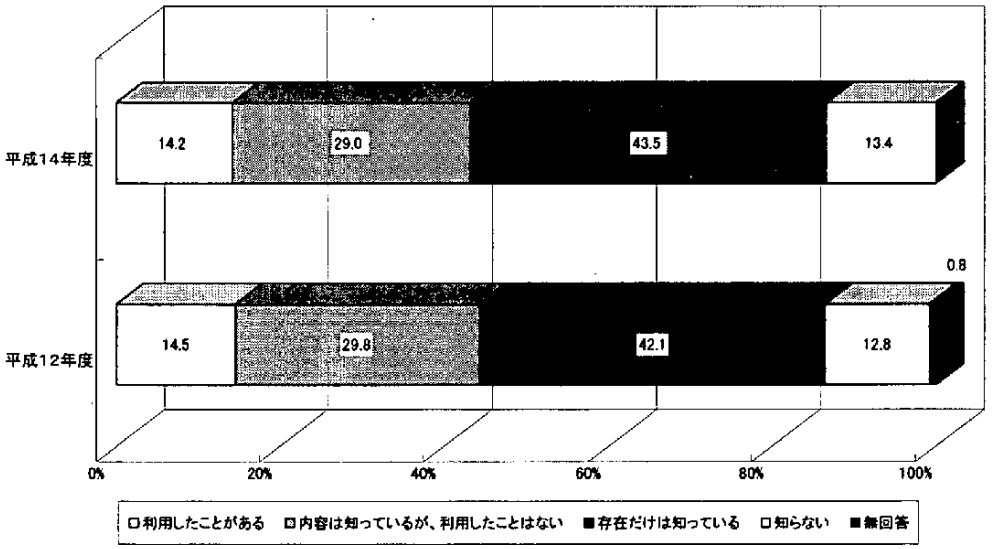

図3－2－1．システム監査基準の認知度（被監査部門）

Q２．経済産業省の「システム監査企業台帳制度」（平成３年）を知っていますか。

1	知っている	214	33.0	
2	知らない	435	67.0	→Q４へ
計		649	100.0	

平成３年に台帳制度が開始されてからすでに 10 年以上が経過し、認知度も平成８年 25.0％、平成 10 年 27.9％、前回調査 31.3％、今回調査 33.0％と着実にアップしてはいるが、いまだ３割程度であり、台帳制度の認知度は低い。

Q３．システム監査を外部の企業に委託する場合「システム監査企業台帳」を参考にしたいと思いますか。

1	参考にしたことがある	15	7.0
2	今後参考にしたいと思う	158	73.8
3	参考にしたいと思わない	34	15.9
無回答		7	3.3
計		214	100.0

システム監査企業台帳制度を知る事業体に対する質問であるが、これまでに台帳を「参考にしたことがある」と回答した事業体は7.0％と１割にも満たない。しかし、「今後参考にしたいと思う」という事業体は73.8％と高い値となっており、今後のシステム監査企業台帳の活用が期待される。

Q４．経済産業省の情報処理技術者試験制度で行われている「システム監査技術者試験」を知っていますか。

1	知っている	556	85.7
2	知らない	93	14.3
計		649	100.0

システム監査技術者試験の認知度は、平成８年86.0％、平成10年86.4％、前回調査84.1％、今回調査85.7％と、ほぼ一定して高い。システム監査技術者試験が情報処理技術者試験の中に位置づけられている影響からか、監査担当部門（73.0％）と比較して被監査部門の方が10ポイント以上も高い値となっている。（監査担当部門に関する分析は、「3.1.1」を参照のこと。）

Q５．経済産業省から「情報システム安全対策基準」（平成７年改訂）が公表されていることを知っていますか。

1	利用したことがある	127	19.6	
2	内容は知っているが、利用したことはない	179	27.6	
3	存在だけは知っている	218	33.6	
4	知らない	125	19.3	→Q７へ
計		649	100.0	

情報システム安全対策基準の認知度は、平成10年80.2％、前回79.0％、今回80.7％とほぼ一定して高い値となっている。また、監査担当部門（67.6％）と比較して10ポイント以上高い値となっている。

その一方、基準を「利用したことがある」との回答は19.6％（前回調査21.1％）と約２割の結果となった。

Q６．「情報システム安全対策基準」の中でシステム監査が位置づけられていることを知っていますか。

1	知っている	387	73.9
2	知らない	133	25.4
無回答		4	0.8
計		524	100.0

情報システム安全対策基準では、技術基準で監査機能を運用基準でシステム監査を位置づけているが、このことを「知っている」との回答は、前回調査（73.8％）とほぼ同じ 73.9％であった。

Q７．経済産業省から「コンピュータウイルス対策基準」（平成７年改訂）が公表されていることを知っていますか。

1	利用したことがある	119	18.3	
2	内容は知っているが、利用したことはない	184	28.4	
3	存在だけは知っている	216	33.3	
4	知らない	130	20.0	→Q９へ
計		649	100.0	

コンピュータウイルス対策基準の認知度は、平成８年 62.7％、平成 10 年 76.8％、前回調査 80.6％と増加してきたが、今回調査では 80.0％と、前回とほとんど変化がない状況である。現状の約８割程度の認知度は、情報システム安全対策基準の認知度とほぼ同じ状況となっている。

その一方、基準を「利用したことがある」との回答は、調査ごとに増加はしているが 18.3％と２割にも満たない状況である。認知度自体は、監査担当部門（66.9％）と比べ 10 ポイント以上高くなっているのに対し、その利用は、ほとんど差がない状況であり、基準を活用しウイルス対策を講じていくことが必要といえる。（監査担当部門に関する分析は、「3.1.1」を参照のこと。）

Q８．「コンピュータウイルス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

1	知っている	327	63.0
2	知らない	189	36.4
無回答		3	0.6
計		519	100.0

システム監査は、コンピュータウイルス対策基準の４つの基準すべてにおいて位置づけられているが、このことの認知度は、平成 10 年 47.6％、前回調査 56.2％、今回調査 63.0％と着実にアップしており、ウイルス対策における監査の役割の重要性が認識されてきている。

Q９．経済産業省から「コンピュータ不正アクセス対策基準」（平成８年）が公表されていることを知っていますか。

1	利用したことがある	98	15.1	
2	内容は知っているが、利用したことはない	182	28.0	
3	存在だけは知っている	215	33.1	
4	知らない	154	23.7	→Q11へ
計		649	100.0	

コンピュータ不正アクセス対策基準の認知度は、平成８年 39.3%、平成 10 年 66.9%、前回調査 74.3%、今回調査 76.2%と着実に増加してきているが、他の基準に比べると、若干ではあるが認知度は低い状況である。

また、基準を「利用したことがある」の回答も平成 10 年 11.7%、前回 13.2%、今回 15.1%と増加はしているが、依然として２割にも満たない状況である。インターネットの目覚しい進展、不正アクセス禁止法が制定されるなどの状況を踏まえると、単に基準を「知っている」に留まらず、基準を活用し、対策を講ずることが必要になっている。

Q10.「コンピュータ不正アクセス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

1	知っている	321	64.8
2	知らない	172	34.7
無回答		2	0.4
計		495	100.0

システム監査はコンピュータ不正アクセス基準の５つの基準すべてにおいて位置づけられているが、平成 10 年 48.9%、前回調査 58.4%、今回調査 64.8%と着実にアップし、現状では基準を６割以上が認知している結果となった。

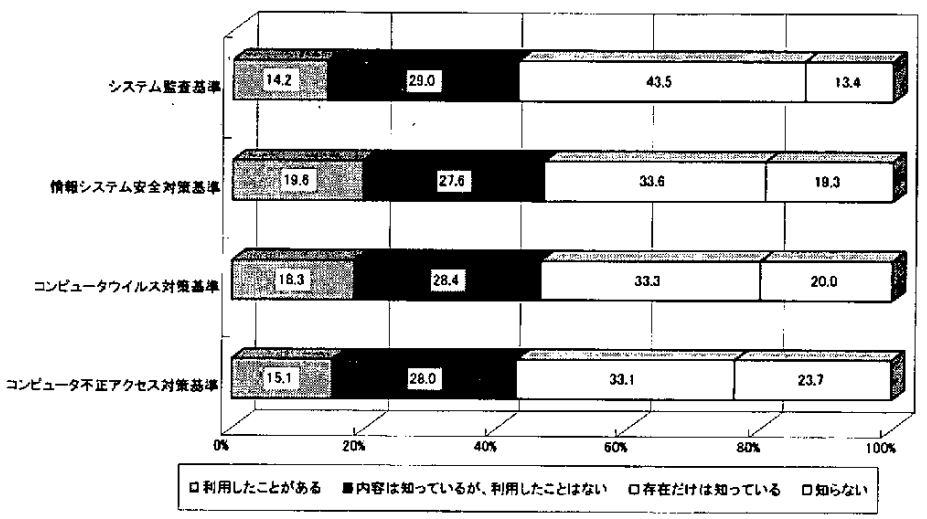

図３－２－２．セキュリティ関連基準の認知度（被監査部門）

Q11. プライバシーマーク制度を知っていますか。

1	知っている	354	54.5
2	知らない	295	45.5
計		649	100.0

プライバシーマーク制度の認知度については、情報サービス産業などを中心に取得が展開していることもあり、情報サービス産業の認知度は 89.8%と非常に高いが、全体としての認知度は54.5%の５割強の状況である。

認知度を監査部門（43.5%）と比較すると、被監査部門の方が 11.0 ポイント高くなっている。（監査担当部門に関する分析は、「3.1.1」を参照のこと。）

Q12. ＩＳＭＳ（情報セキュリティマネジメントシステム）適合性評価制度を知っていますか。

1	知っている	301	46.4
2	知らない	344	53.0
無回答		4	0.6
計		649	100.0

ＩＳＭＳ適合性認証制度の認知度は、前述の情報サービス産業は88.1%と非常に高いが、全体としては46.4%の４割強と低く、プライバシーマーク制度の認知度54.5%と比較すると、8.1ポイント低い結果となっている。

また、監査部門（36.3%）と比較すると、被監査部門の方が 10.1 ポイント高くなっている。（監査担当部門に関する分析は、「3.1.1」を参照のこと。）

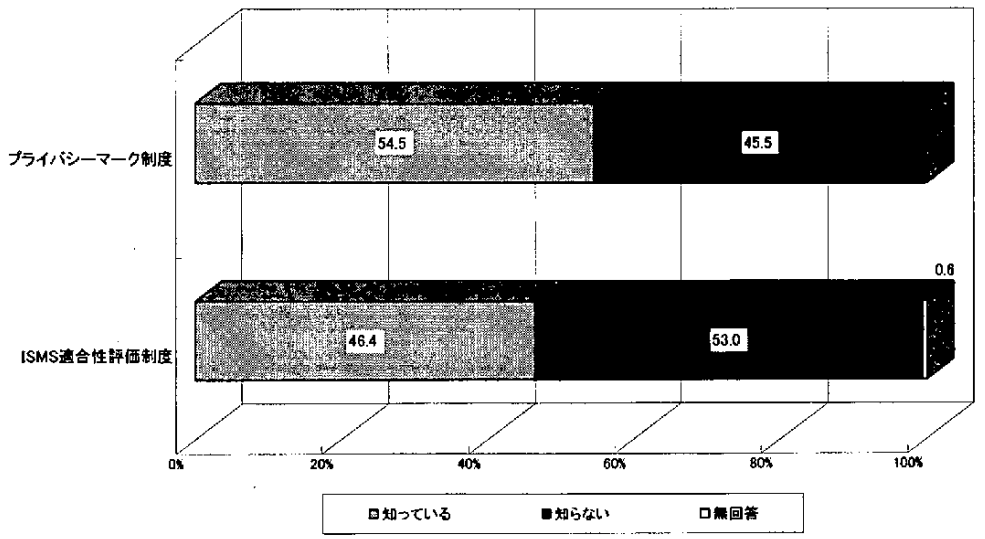

図3－2－3. プライバシーマーク制度とISMS制度の認知度（被監査部門）

3.2.2　平成１３年度のシステム監査実施について

Q13. 貴社にはシステム監査人がいますか。

1	い　る	114	17.6
2	いない	535	82.4
計		649	100.0

被監査部門に対するシステム監査人の有無の調査では、17.6%が「いる」と回答している。これは、前回調査に比較して0.2ポイント増であるが、変化はほとんどない。同一の質問を監査担当部門に対して実施しているが、その回答では23.6%であり（Q14)、被監査部門の回答と大きな差はない。

被監査部門に対する調査で、システム監査人を置いている割合が高い業種は、情報処理サービス業・ソフトウェア業が50.8%、生命保険業が50.0%、金融業が36.2%となっている。金融業は、監査担当部門に対する調査では60.9%となっており（Q14)、被監査部門に対する回答値との差は大きい。(監査担当部門に関する分析は、「3.1.2」を参照のこと。)

Q14. 貴部門では、システム監査を受けたことがありますか。

1	あ　る	255	39.3	
2	な　い	394	60.7	→Q34へ
計		649	100.0	

システム監査の実施状況は、監査担当部門、被監査部門の両部門に対し「過去にシステム監査を実施したことがあるか」、さらにシステム監査を実施したことがあるとした回答に対し、「2001年度に実施したか」（Q15）の２項目の調査を行った。「過去にシステム監査を実施したことがある」との回答は、被監査部門では39.3%であった。監査担当部門に対する調査では38.4%であり（Q17)、ほぼ同様の回答となっている。(監査担当部門に関する分析は、「3.1.2」を参照のこと。)

Q15. 平成１３年度にシステム監査を受けましたか。

1	受けた	178	69.8	
2	受けない	77	30.2	→Q34へ
計		255	100.0	

過去にシステム監査を実施した事業体に対しての平成13年度のシステム監査実施状況について、「実施した」とする回答は69.8%である。同一の質問に対する監査担当部門の回答は、75.8%であり、回答値は近似している（Q31)。(監査担当部門に関する分析は、「3.1.3」を参照のこと。)

平成13年度に実施した状況を業種別にみると、過去のシステム監査の状況と同様、生命保険業（100.0%)、情報処理サービス業・ソフトウェア業（88.6%)、金融業（77.3%)、輸送用機械器

具製造業（72.7%）、電気機械器具製造業（60.9%）となっており、これらの業種でシステム監査を継続的に実施している傾向が強いといえる。

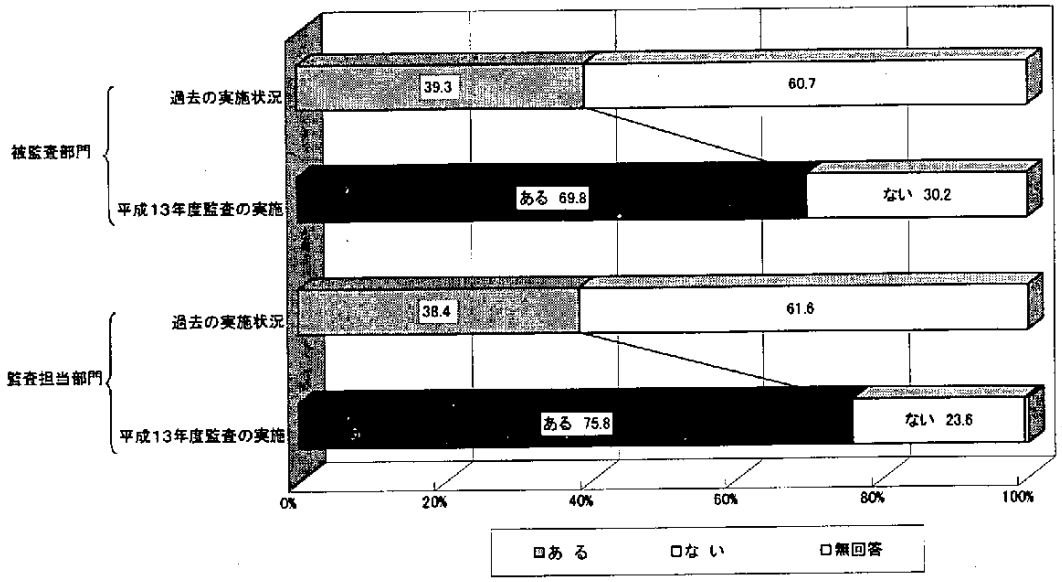

図3－2－4. システム監査実施状況

Q16. システム監査を受けたのはどの業務でしたか。（複数回答）

回答件数		178	-
1	企画業務	76	42.7
2	開発業務	124	69.7
3	運用業務	159	89.3
4	保守業務	95	53.4
無回答		3	1.7

平成13年度にシステム監査を受けた被監査部門に、システム監査実施業務を調査した。調査はシステム監査基準の区分に準じて、「企画業務」、「開発業務」、「運用業務」、「保守業務」に対して実施した。

システム監査の実施業務は、「企画業務」が42.7%（前回調査35.4%）、「開発業務」が69.7%（前回調査66.3%）、「運用業務」が89.3%（前回調査86.3%）、「保守業務」が53.4%（前回調査54.9%）であった。業務別で調査した結果は、これまでも実施率の高い順から「運用業務」、「開発業務」、「保守業務」、「企画業務」であり、その傾向は変わらない。監査を実施した効果が大きい「企画業務」における監査の実施が7.3ポイント増加したことが注目される。

Q17. システム監査では、どのテーマを実施しましたか。(複数回答)

回答件数		178	-
1	ドキュメント管理	115	64.6
2	進捗管理	65	36.5
3	品質管理	76	42.7
4	コスト管理	37	20.8
5	要員管理	65	36.5
6	外部委託(開発の委託)	78	43.8
7	外部委託(アウトソーシング)	61	34.3
8	セキュリティ対策	140	78.7
9	ネットワーク管理	74	41.6
10	ソフトウェアの適正利用(ライセンス管理)	41	23.0
11	個人情報保護対策	59	33.1
12	PC管理、モバイル機器管理	52	29.2
13	コンピュータウイルス対策	77	43.3
14	情報システム関連のリスク管理	86	48.3
15	災害対策	84	47.2
16	その他	17	9.6
無回答		3	1.7

今回調査では、監査対象分野ごとの実施状況の調査を実施した。その結果、最も多かったのは「セキュリティ対策」78.7%(監査担当部門に対する調査(Q36)では84.8%)であり、情報システムの安全性に対する関心度の向上がうかがえる。安全性の観点からのシステム監査としては、「個人情報保護対策」33.1%(同60.1%)、「コンピュータウイルス対策」43.3%(同59.4%)、「情報システム関連のリスク管理」48.3%(同58.0%)、「災害対策」47.2%(同55.8%)も多くなっている。(監査担当部門に関する分析は、「3.1.3」を参照のこと。)

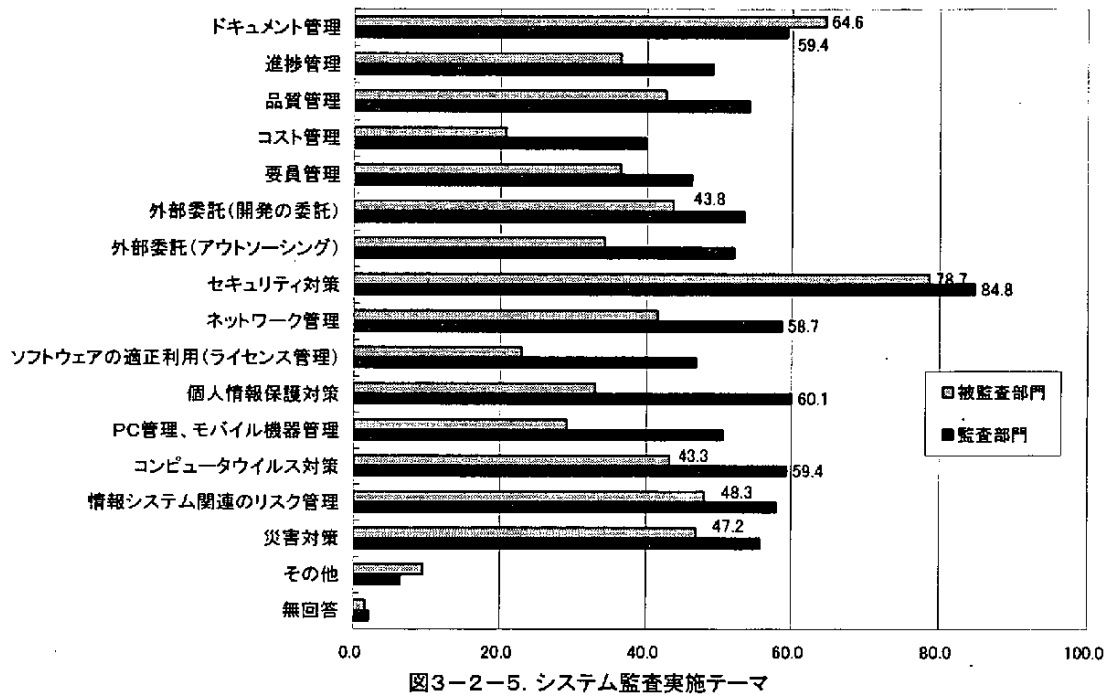

図3−2−5. システム監査実施テーマ

Q18. システム監査は次のどの方式で実施されましたか。(複数回答)

回答件数		178	-
1	内部監査部門型（監査部、検査部等が実施）	106	59.6
2	外部委託型（システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託）	98	55.1
無回答		3	1.7

（「1　内部監査部門型」のみ該当する場合はQ21へ、2つとも該当する場合はQ19へ）

平成 13 年度にシステム監査を実施した事業体の被監査部門に対する実施方式の調査（複数回答）では、59.6%が「内部監査部門型（監査部、検査部等が実施）」となっており、「外部委託型（システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託）」は 55.1%となっている。「内部監査部門型」と「外部委託型」の差は僅かであり、予想以上に外部監査型が多くなっているといえよう。

監査担当部門に対する調査では、「内部監査部門型」が 70.3%であり「外部監査部門型」は 33.3%であった（Q32）。監査担当部門の回答は、すべて監査部門を設置している事業体からの回答であり、一方、被監査部門からの回答は必ずしも監査部門がある事業体からの回答ではないため、回答の母集団が異なることが、ある程度影響していると想定される。(監査担当部門に関する分析は、「3.1.3」を参照のこと。)

Q19. (Q18で「2」を回答した場合) 外部委託企業は、システム監査企業台帳登録企業ですか。

1	はい	43	43.9
2	いいえ	1	1.0
3	わからない	50	51.0
無回答		4	4.1
計		98	100.0

この調査項目は今回新たに設けたものであるが、システム監査を委託している場合の委託先企業は、その委託先がわかる場合の回答は、1件を除きすべてがシステム監査企業台帳登録企業であった。また、登録企業か否かが不明の回答も多かった。この回答の状況は、監査担当部門からの回答と同様である。

Q20. 外部委託の場合、どこが実施しましたか。

1	監査法人（公認会計士を含む）	88	89.8
2	コンサルタント（個人／企業）	4	4.1
3	情報処理サービス業者	3	3.1
4	その他	1	1.0
無回答		2	2.0
計		98	100.0

この調査項目も今回新たに設定したものである。回答は、圧倒的に「監査法人（公認会計士を含む）」（89.8%）が多かった。この回答の状況も、監査担当部門からの回答と同様である。

Q21. システム監査を受けた結果、監査人に対してどのような印象をもちましたか。（単一回答）

1	問題があった	18	10.1	
2	十分満足できた	17	9.6	→Q23へ
3	特に問題はなかった	133	74.7	→Q23へ
4	わからない	7	3.9	→Q23へ
無回答		3	1.7	
計		178	100.0	

システム監査を受けた被監査部門が、システム監査人に対して持った印象を調査した。「十分に満足できた」（9.6%）、「特に問題はなかった」（74.7%）と、被監査部門としては監査人の活動に対して問題視してはいないことがわかった。

なお、今回調査では回答の選択肢を変更しており、前回調査ではシステム監査人の活動に対する肯定的な選択肢は「特に問題はなかった」だけであり、その回答は72.6%であった。今回調査では「十分に満足できた」の選択肢の分だけ、肯定的な評価が増えたといえる。

Q22. どのような点で問題があったと思いますか。最も問題と思った点を1つ選んで下さい。（単一回答）

1	監査人の権限および役割分担が不明確であった	3	16.7
2	現場（被監査部門）とのコミュニケーション能力が不足していた	2	11.1
3	監査人の監査対象業務に関する知識が不足していた	3	16.7
4	監査人の情報システムに関する知識が不足していた	5	27.8
5	監査人の洞察力・判断力に問題があった	1	5.6
6	その他	1	5.6
複数回答		3	17.0
計		18	100.0

Q21の回答で明らかになったように、全体的にはシステム監査人の活動に対しての問題点があるとした回答は少ない。「問題があった」とした回答に対する具体的な問題点は、上記のとおりである。「監査人の情報システムに関する知識が不足していた」（27.8%）の回答が最も多かったが、回答数の絶対値が少ないため、回答結果の評価に対しては、十分な考慮が必要である。

Q23. システム監査を受けた時、現場の負担はありましたか。

1	負担はなかった	15	8.4
2	負担は多少あったが、通常業務に支障をきたすほどではなかった	146	82.0
3	通常業務に支障をきたした	12	6.7
4	その他	1	0.6
無回答		4	2.2
計		178	100.0

システム監査の実施時には、被監査部門に準備、対応などの負担がかかる場合がある。被監査部門に対しシステム監査を受けた際の現場での負担状況について調査した。

8.4%が「負担はなかった」、82.0%が「負担はあったが通常業務に支障をきたすほどではなかった」とし、「通常業務に支障をきたした」はわずか6.7%となっている。

Q24. システム監査を受けた結果どのような点が問題だと感じましたか。最も問題と感じたものを1つ選んで下さい。(単一回答)

1	システム監査計画に無理があった	4	2.2
2	システム監査方法が現場を無視したものであった	2	1.1
3	システム監査人へ提出すべき資料を整理していなかった	24	13.5
4	資料提出や意見聴取の指示が不明確であった	11	6.2
5	資料要求が多すぎた	14	7.9
6	現場の説明がシステム監査人に理解されなかった	8	4.5
7	監査プログラムの使用のために現場に負担がかかった	3	1.7
8	実地調査が多すぎた	1	0.6
9	その他	3	1.7
10	特に問題は感じなかった	96	53.9
無回答		7	3.9
複数回答		5	3.0
計		178	100.0

「システム監査を受けた結果、問題点があったか」の調査では、「特に問題を感じなかった」が過半数の53.9%(前回調査51.4%)であったが、「何らかの問題点を感じた」も39.4%あった。「Q21. システム監査人の問題点」、あるいは「Q23. システム監査を受けた時の現場の負担」に関してはシステム監査に対する肯定的な意見が多かったが、この調査ではいくつかの問題点が提起されている。

問題点で最も多かったのは「システム監査人へ提出すべき資料を整理していなかった」(13.5%)であり、システム監査を受ける側の準備として、資料の作成、収集の時間が必要なことを挙げている。またこの回答についで多かった「資料要求が多すぎた」(7.9%)、「資料提出や意見聴取の指示が不明確であった」(6.2%)をみると、監査時の資料に関する問題が多かったことを示している。

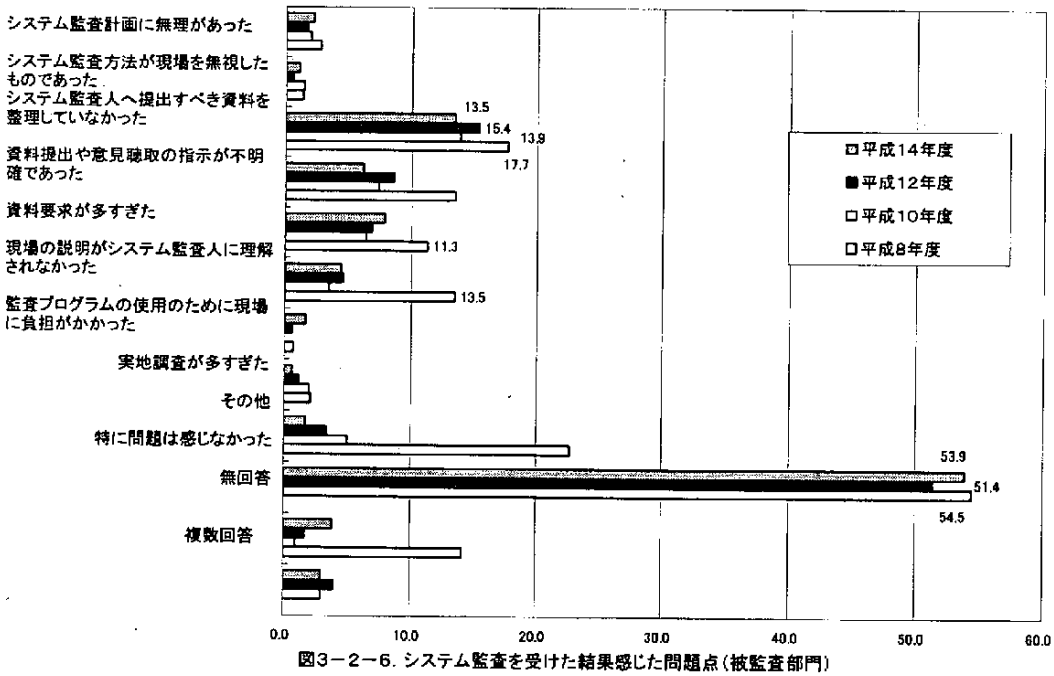

図3－2－6. システム監査を受けた結果感じた問題点（被監査部門）

Q25. 監査結果について、システム監査人と貴部門との間で講評会（監査報告書を作成する前に意見交換、確認等を行うことをいう）が行われましたか。

1	行われた	150	84.3
2	行われなかった	23	12.9
無回答		5	2.8
計		178	100.0

講評会は、監査報告書の作成前に監査担当部門と被監査部門との間で開催されるものであり、システム監査実施時の事実誤認を排除するとともに、被監査部門のシステム監査結果に対する理解を深めることを目的とするものである。システム監査の実効性、効果を高めるために、可能な限り講評会を開催することが推奨されているが、調査結果では84.3%と高い割合で実施していることがわかった。この質問は監査担当部門に対しても行われており、90.6%であった（Q50）。被監査部門と監査担当部門の回答の傾向は一致している。

Q26. 監査報告書の作成後に関係者を含めた監査報告会が行われましたか。

1	行われた	123	69.1	
2	行われなかった	50	28.1	→Q28へ
無回答		5	2.8	
計		178	100.0	

監査結果の報告を監査に関係する関係者を集めて実施する監査報告会の開催状況は 69.1%であった。監査講評会に比べて低い値であるが、監査報告書を関係部署に対して提出／送付することで監査終了としている場合が、約3割程度あるためと思われる。

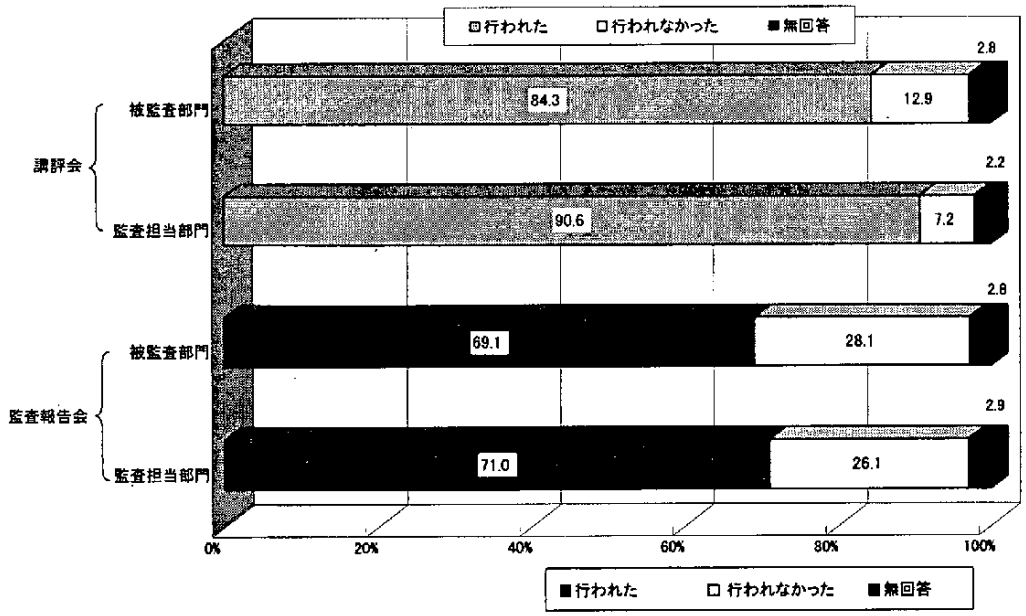

図3－2－7. 講評会／監査報告会の実施状況

Q27. 監査報告会に情報システム部門から出席しましたか。

1	し　た	110	89.4
2	しない	12	9.8
無回答		1	0.8
計		123	100.0

監査報告会を実施した場合に、監査報告会に対する情報システム部門からの出席は89.4%であった。比較的、効率であるといえる。なお、監査報告会の出席者の状況の調査は監査担当部門に対して調査している。その結果は、監査担当部門のQ52に分析されている。

Q28. 監査報告書の指摘事項や改善勧告の内容について妥当だと思いますか。

1	妥当だと思う	117	65.7
2	一部妥当だと思う	54	30.3
3	妥当だと思わない	2	1.1
無回答		5	2.8
計		178	100.0

監査報告書の指摘事項や改善勧告に対する被監査部門の評価をみると、65.7%が「妥当だと思う」と評価している。残りのほとんどが「一部妥当だと思う」(30.3%) と回答しており、「妥当だと思わない」はきわめて僅少であった。先述のシステム監査の実施上の問題点、現場の負荷などの調査項目の回答と合わせ、システム監査の実施、結果に対して、被監査部門はおおむね妥当と評価しているといえよう。

Q29. 改善命令を受けましたか。

1	受けた	119	66.9	
2	受けない	56	31.5	→Q31へ
無回答		3	1.7	
計		178	100.0	

平成13年度にシステム監査を実施した事業体のうち、改善命令を受けた被監査部門は66.9%（前回調査70.9%）である。約7割が改善命令を受けているが、「改善命令を受けた」回答の割合は過去最低であり、徐々に値は低くなっている。

Q30. 改善命令を受けて対策を実施しましたか。

1	実施した	64	53.8
2	一部実施した	54	45.4
3	実施していない	1	0.8
計		119	100.0

改善命令に対し対策を「実施した」が53.8%、「一部実施した」が45.4%となっており、ほとんどの被監査部門で何らかの形でシステム監査の結果が情報システムの改善に反映されていることとなる。前回調査では「実施した」が42.7%であり、今回は11.1ポイント増加した。「一部実施」を含め「実施」の割合が高く、システム監査は情報システムの改善に役立っているといえる。

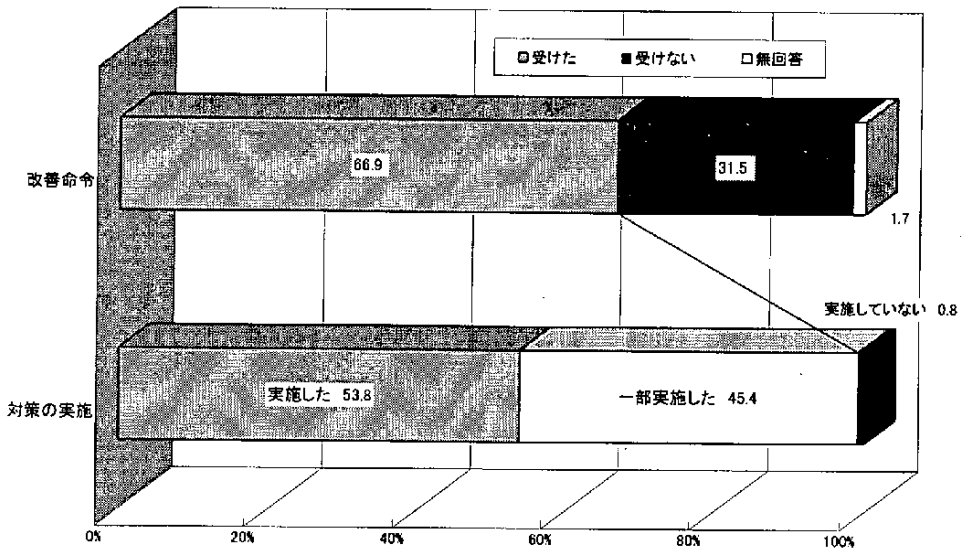

図3－2－8. 改善命令の発令／対策の実施（被監査部門）

Q31. システム監査を受けた結果、被監査部門としては効果があったと思いますか。

1	効果があったと思う	129	72.5
2	効果はなかったと思う	7	3.9
3	どちらともいえない	37	20.8
4	わからない	2	1.1
無回答		3	1.7
計		178	100.0

→Q34へ

システム監査を受けた結果、被監査部門として「効果があったと思うか」という質問に対し、「効果があったと思う」という回答が72.5%であり、前回調査の69.1%を3.4ポイント上回った。一方、「効果はなかったと思う」(3.9%) は前回調査 (3.4%) とほとんど変わらなかった。

被監査部門に対するQ28、Q30およびQ31の調査結果から、システム監査実施の効果は上がっていると判断できる。今後、システム監査の効果をさらに高めるため、講評会や監査報告会での議論を深め、改善勧告が全面実施されるよう工夫することが必要である。

Q32. どのような点に効果があったと思いますか。最も効果があったと思うものを1つ選んで下さい。(単一回答)

1	システムに起因する事故・障害が未然に防止できた	6	4.7
2	リスク対策をどこまで考慮すればよいかが明らかになった	23	17.8
3	担当者がリスクを考慮しながら業務を実行するようになった	14	10.9
4	システム部門に対する過大な要求がなくなった	0	0.0
5	システムの安全性向上対策のレベルが明らかになった	23	17.8
6	システムの有効利用が促進された	3	2.3
7	有効なシステムの開発設計が可能になった	2	1.6
8	業務の継続性の確保が図られた	6	4.7
9	要員が規定・ルール等を意識して業務を実行するようになった	35	27.1
10	その他	4	3.1
無回答		2	1.6
複数回答		11	9.0
計		129	100.0

システム監査実施による効果があったとした被監査部門に対する「最も効果のあった点は何か」という設問については「要員が規定・ルール等を意識して業務を実行するようになった」(27.1%)、「リスク対策をどこまで考慮すればよいかが明らかになった」、「システムの安全性向上対策のレベルが明らかになった」(ともに 17.8%)、「担当者がリスクを考慮しながら業務を実行するようになった」(10.9%) を指摘する回答が多かった。この結果から、システム監査は、安全性向上やリスク対策など、取るべき対策の目標設定を明確にする効果が大きいことがわかる。

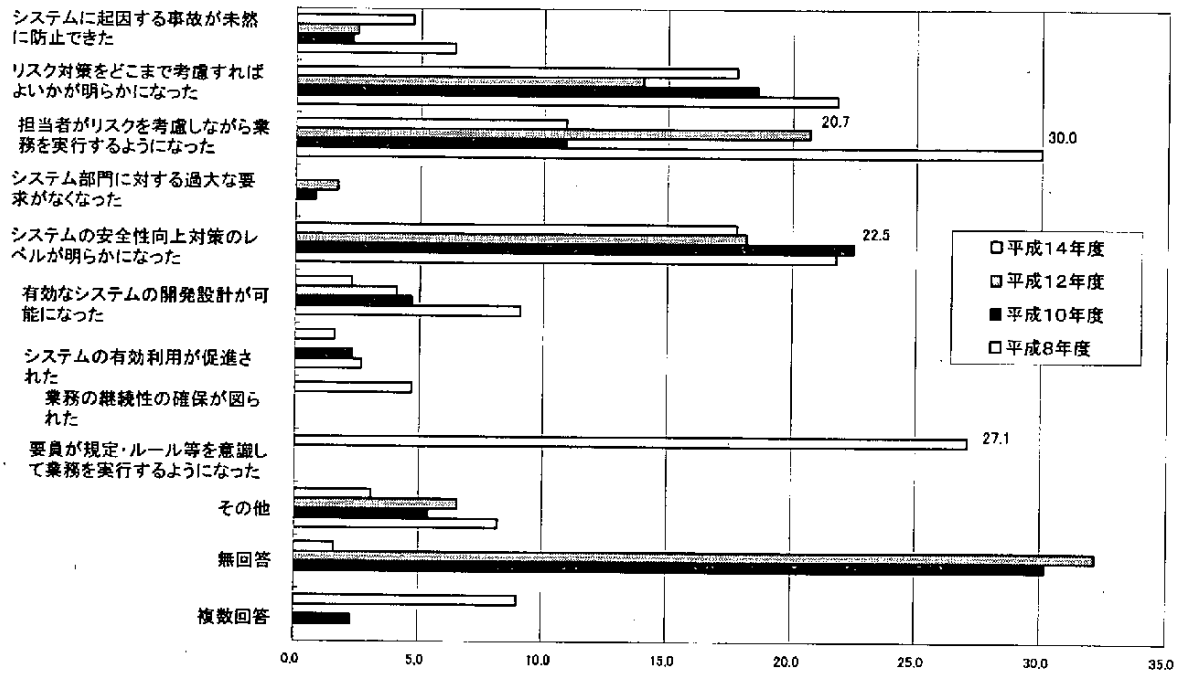

図3－2－9. システム監査の効果(被監査部門)

Q33. どのような点で最も改善が図れたと思いますか。最も改善が図れたと思うものを１つ選んで下さい。(単一回答)

1	スケジュール管理の適正化	0	0.0
2	コストの削減	1	0.8
3	情報の保護対策の向上	12	9.3
4	セキュリティ対策の向上	41	31.8
5	生産性の向上	2	1.6
6	品質管理の向上	12	9.3
7	規則・手続き等の遵守	30	23.3
8	ドキュメント類の整備	13	10.1
9	作業環境の改善	3	2.3
10	要員管理の適正化	1	0.8
11	その他	2	1.6
無回答		3	2.3
複数回答		9	7.0
計		129	100.0

システム監査の実施により最も改善された点としては、「セキュリティ対策の向上」(31.8%)、「規則・手続き等の遵守」(23.3%)が多い。セキュリティ対策はシステム監査の対象テーマとしても増えており、その結果として前回調査(26.4%)に比べ5.4ポイントの増加となった。前回

調査との比較では、「規則・手続き等の遵守」が7.6ポイントの増加となっている。

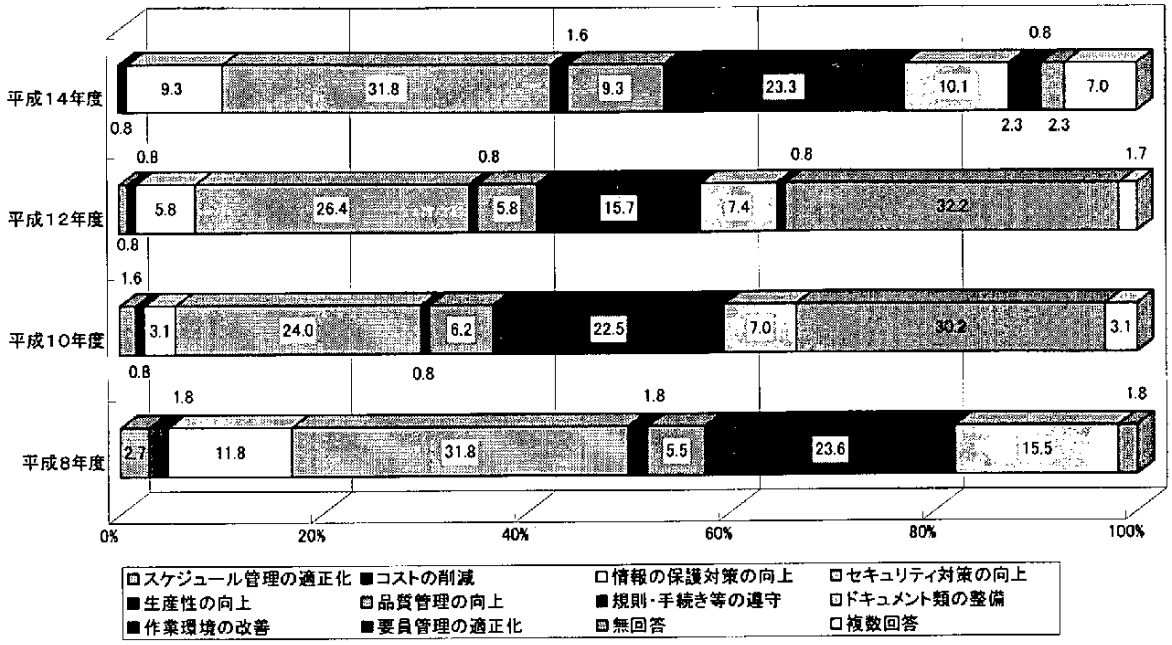

図3－2－10. システム監査による改善点(被監査部門)

3.2.3　システム監査のあり方について

Q34. 各業務の監査で重視すべき着眼点は何ですか。各業務ごとにそれぞれ１つ選んで下さい。

着眼点 / 業務	安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性	無回答	複数回答	計
企画業務	18	50	89	52	151	180	30	49	26	4	649
	2.8	7.7	13.7	8.0	23.3	27.7	4.6	7.6	4.0	0.6	100.0
開発業務	15	160	58	33	66	32	183	78	21	3	649
	2.3	24.7	8.9	5.1	10.2	4.9	28.2	12.0	3.2	0.5	100.0
運用業務	202	240	60	26	14	9	13	68	12	5	649
	31.1	37.0	9.2	4.0	2.2	1.4	2.0	10.5	1.8	0.8	100.0
保守業務	181	279	37	11	17	50	5	48	17	4	649
	27.9	43.0	5.7	1.7	2.6	7.7	0.8	7.4	2.6	0.6	100.0

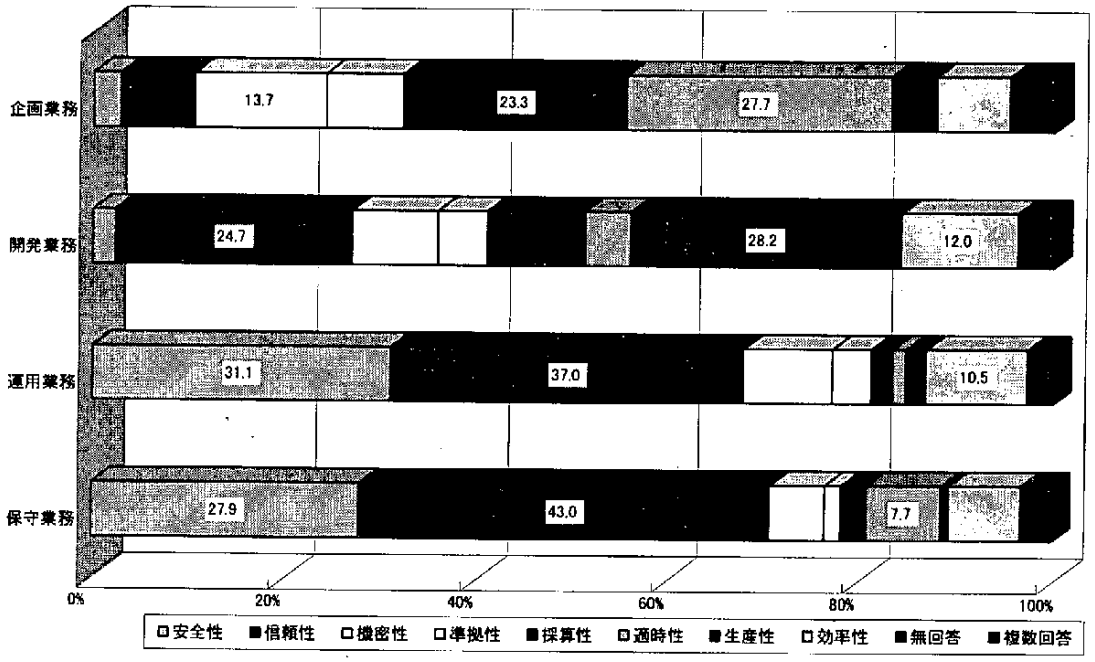

図3－2－11. 監査の重視すべき着眼点(業務別)

被監査部門で最も重視すべきと考えている着眼点は、システム監査を実施した事業体のみならず、システム監査を実施していない事業体を含めて、システム監査のあり方として調査した。

企画業務では、「適時性」が 27.7%であり、進展の早い経営環境、情報技術の変化に対応することの重要性が増してきている現れと思われる。次に多かったのが、「採算性」(23.3%)、「機密性」(13.7%) であり、この順番は前回調査と変わらない。

開発業務で多かったのが「生産性」(28.2%) で、システム開発に責任を持つ被監査部門の意識が現われている。生産性に続いて「信頼性」が 24.7%、ついで「効率性」が 12.0%となっている。「効率性」は、情報システムの稼働時の効率性と、開発時の開発効率性が考えられるが、多くの回答が開発効率性をさしていると想定される。

運用業務で最も重視すべきと考えている着眼点は「信頼性」が 37.0%、「安全性」が 31.1%、「効率性」が 10.5%と、この３項目で８割弱となっている。

保守業務でも「信頼性」が43.0%、「安全性」が27.9%となっており、監査担当部門に対する調査同様、運用業務と同じ傾向となっている。

Q35. 各テーマの監査で重視すべき着眼点は何ですか。各テーマごとにそれぞれ1つ選んで下さい。

着眼点 / テーマ	安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性	無回答	複数回答	計
ドキュメント管理	29	170	133	162	2	70	17	43	23	0	649
	4.5	26.2	20.5	25.0	0.3	10.8	2.6	6.6	3.5	0.0	100.0
進捗管理	18	76	7	42	22	211	143	103	27	0	649
	2.8	11.7	1.1	6.5	3.4	32.5	22.0	15.9	4.2	0.0	100.0
品質管理	71	419	13	43	12	12	31	18	29	1	649
	10.9	64.6	2.0	6.6	1.8	1.8	4.8	2.8	4.5	0.2	100.0
コスト管理	7	30	12	10	391	17	69	86	25	2	649
	1.1	4.6	1.8	1.5	60.2	2.6	10.6	13.3	3.9	0.3	100.0
要員管理	27	53	43	23	43	90	175	165	29	1	649
	4.2	8.2	6.6	3.5	6.6	13.9	27.0	25.4	4.5	0.2	100.0
外部委託（開発の委託）	29	199	113	12	110	10	93	57	26	0	649
	4.5	30.7	17.4	1.8	16.9	1.5	14.3	8.8	4.0	0.0	100.0
外部委託（アウトソーシング）	61	210	123	5	124	6	37	54	28	1	649
	9.4	32.4	19.0	0.8	19.1	0.9	5.7	8.3	4.3	0.2	100.0
セキュリティ対策	320	102	179	13	6	7	0	2	20	0	649
	49.3	15.7	27.6	2.0	0.9	1.1	0.0	0.3	3.1	0.0	100.0
ネットワーク管理	193	304	99	5	4	5	1	14	23	1	649
	29.7	46.8	15.3	0.8	0.6	0.8	0.2	2.2	3.5	0.2	100.0
ｿﾌﾄｳｪｱの適正利用（ﾗｲｾﾝｽ管理）	56	138	32	267	42	50	6	29	28	1	649
	8.6	21.3	4.9	41.1	6.5	7.7	0.9	4.5	4.3	0.2	100.0
個人情報保護対策	125	74	372	47	1	3	1	3	23	0	649
	19.3	11.4	57.3	7.2	0.2	0.5	0.2	0.5	3.5	0.0	100.0
PC管理、モバイル機器管理	131	115	108	62	34	63	19	85	32	0	649
	20.2	17.7	16.6	9.6	5.2	9.7	2.9	13.1	4.9	0.0	100.0
コンピュータウイルス対策	424	116	28	9	4	40	0	7	21	0	649
	65.3	17.9	4.3	1.4	0.6	6.2	0.0	1.1	3.2	0.0	100.0
情報システム関連のリスク管理	310	171	36	26	35	31	2	14	24	0	649
	47.8	26.3	5.5	4.0	5.4	4.8	0.3	2.2	3.7	0.0	100.0
災害対策	466	67	3	16	27	37	0	9	24	0	649
	71.8	10.3	0.5	2.5	4.2	5.7	0.0	1.4	3.7	0.0	100.0
その他	4	5	2	1	3	1	0	1	632	0	649
	0.6	0.8	0.3	0.2	0.5	0.2	0.0	0.2	97.4	0.0	100.0

被監査部門に対し、監査テーマ別に最も重視すべき着眼点を調査した。

ドキュメント管理では、トップが「信頼性」（26.2%）、ついで「準拠性」（25.0%）、「機密性」（20.5%）となっている。

進捗管理では、「適時性」(32.5%)、「生産性」22.0%が多くなっている。ついで「効率性」(15.9%) と並んでおり、コストに関連した事項が高くなっている。

要員管理では、「生産性」(27.0%)、「効率性」(25.4%) となっている。

外部委託は、開発の外部委託とアウトソーシングに分けて調査がなされた。開発の外部委託では、「信頼性」(30.7%) と高く、ついで「機密性」(17.4%) と「採算性」(16.9%) が並んでいる。一方、アウトソーシングでも開発の外部委託と同様である。最も多かったのは、「信頼性」(32.4%) であり、「採算性」(19.1%) と「機密性」(19.0%) が並んでいる。

セキュリティ関連のセキュリティ対策、個人情報保護対策、コンピュータウイルス対策、情報システムのリスク管理などは、当然ながらそれぞれ「安全性」、「信頼性」あるいは「機密性」が圧倒的に高くなっている。

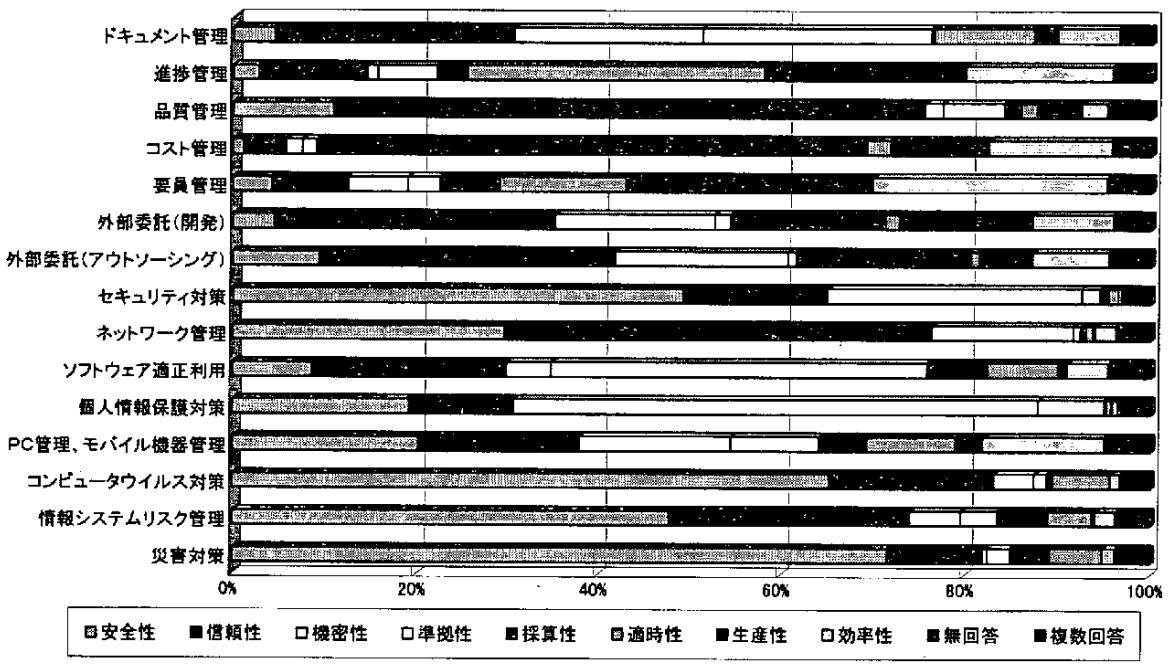

図3−2−12. 監査で重視すべき着眼点(テーマ別−被監査部門)

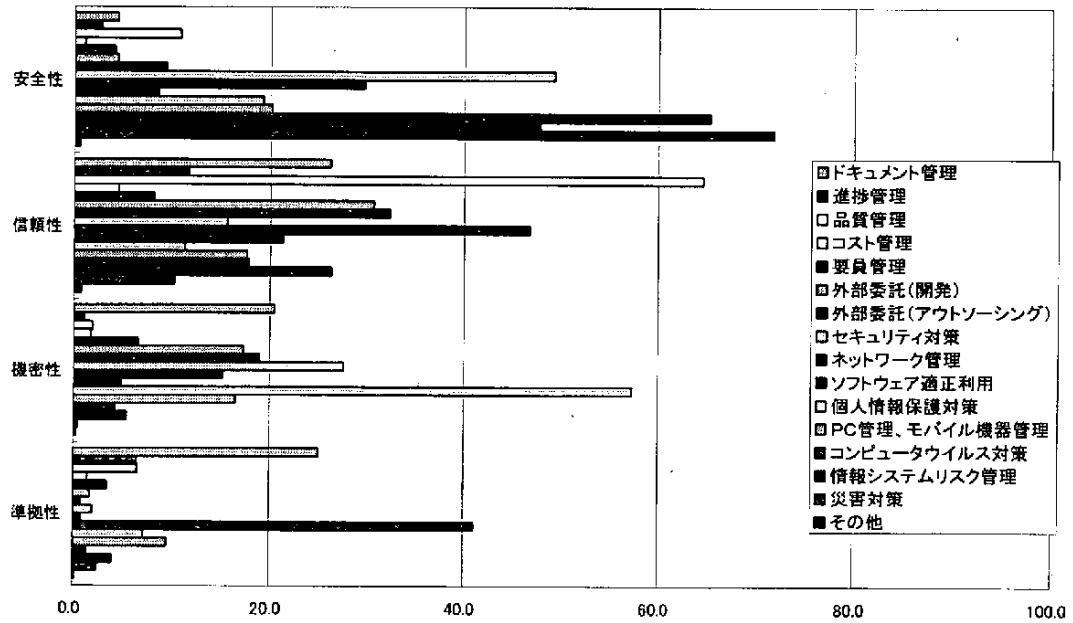

図3−2−13−1. 監査で重視すべき着眼点(テーマ別−被監査部門)

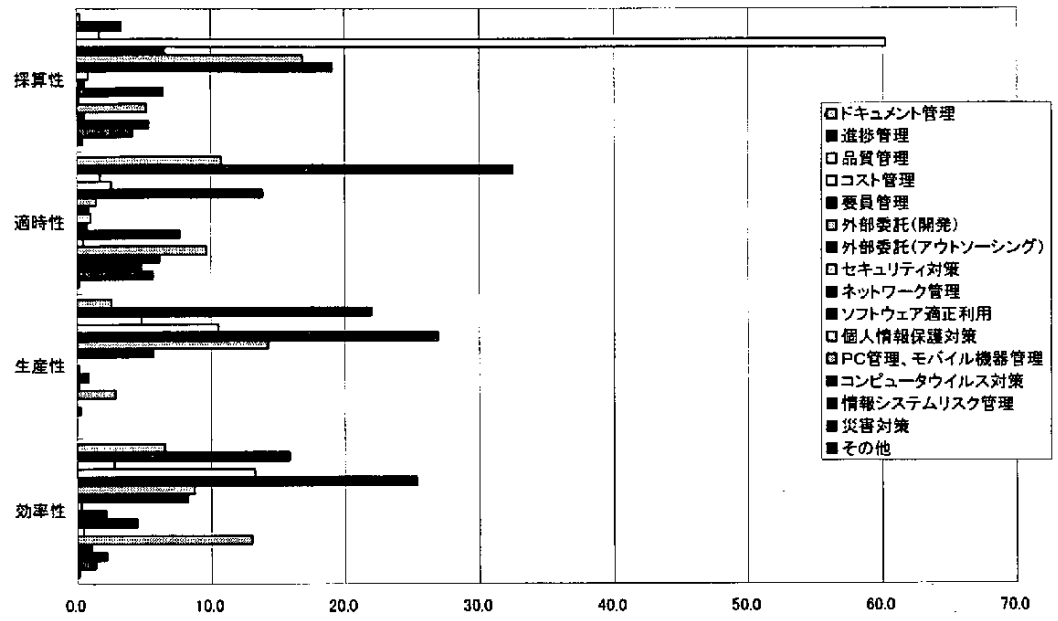

図3－2－13－2. 監査で重視すべき着眼点（着眼点別－被監査部門）

Q36. コンピュータ犯罪防止、ヒューマンエラー防止、事故防止、災害対策、個人情報保護の５項目について、防止ならびに早期発見の観点から、システム監査において特に重視すべき分野はどこだと思いますか。各項目ごとに最も重要と思われる分野（１～１２）を１つだけ選んで下さい。

分野／項目	データの入力プロセス	データ処理プロセス	出力プロセス	プログラム変更	オペレーション	情報保管（データ管理）	入退室（館）管理	システム開発	ハードウエア *1	ソフトウエア *2	ネットワーク	電源設備	無回答	複数回答	計
コンピュータ犯罪防止	29	20	20	13	24	223	53	12	0	14	211	0	25	5	649
	4.5	3.1	3.1	2.0	3.7	34.4	8.2	1.8	0.0	2.2	32.5	0.0	3.9	0.8	100.0
ヒューマンエラー防止	132	50	4	56	278	24	17	30	1	19	5	1	23	9	649
	20.3	7.7	0.6	8.6	42.8	3.7	2.6	4.6	0.2	2.9	0.8	0.2	3.5	1.4	100.0
事故防止	7	44	4	39	106	62	73	39	108	12	49	59	42	5	649
	1.1	6.8	0.6	6.0	16.3	9.6	11.2	6.0	16.6	1.8	7.6	9.1	6.5	0.8	100.0
災害対策	2	5	3	1	11	180	13	3	142	11	60	179	26	13	649
	0.3	0.8	0.5	0.2	1.7	27.7	2.0	0.5	21.9	1.7	9.2	27.6	4.0	2.0	100.0
個人情報保護	8	18	62	1	20	403	28	9	0	11	60	0	23	6	649
	1.2	2.8	9.6	0.2	3.1	62.1	4.3	1.4	0.0	1.7	9.2	0.0	3.5	0.9	100.0

＊1　CPU と周辺機器／＊2　基本ソフトとアプリケーションソフト

コンピュータ犯罪、ヒューマンエラー、事故、災害対策、個人情報保護に対してトラブル防止および発生時の早期発見の観点から、システム監査を実施する場合の最も重視すべき分野を情報システムを構成する要素、行為に分けて調査した。

コンピュータ犯罪防止では、「情報保管（データ管理）」（34.4%）、「ネットワーク」（32.5%）が圧倒的に多かった。監査担当部門に対する調査では、「情報保管（データ管理）」（40.6%）が圧倒的であり、ついで「ネットワーク」（15.2%）であった（Q37）。被監査部門と比べてその差は大きく、監査担当部門と被監査部門の間で認識の違いが出ている。ヒューマンエラー防止では、「オペレーション」（42.8%）、「データの入力プロセス」（20.3%）が高く、事故防止では回答は分散しているものの、比較的、「ハードウェア」（16.6%）、「オペレーション」（16.3%）、「入退室（館）管理」（11.2%）が高くなっている。

災害対策では「情報保管（データ管理）」（27.7%）、「電源設備」（27.6%）、「ハードウェア」（21.9%）が多くなっている。

個人情報保護については、監査担当部門同様、やはり「情報保管（データ管理）」（62.1%）と圧倒的に多い。（監査担当部門に関する分析は、「3.1.3」を参照のこと。）

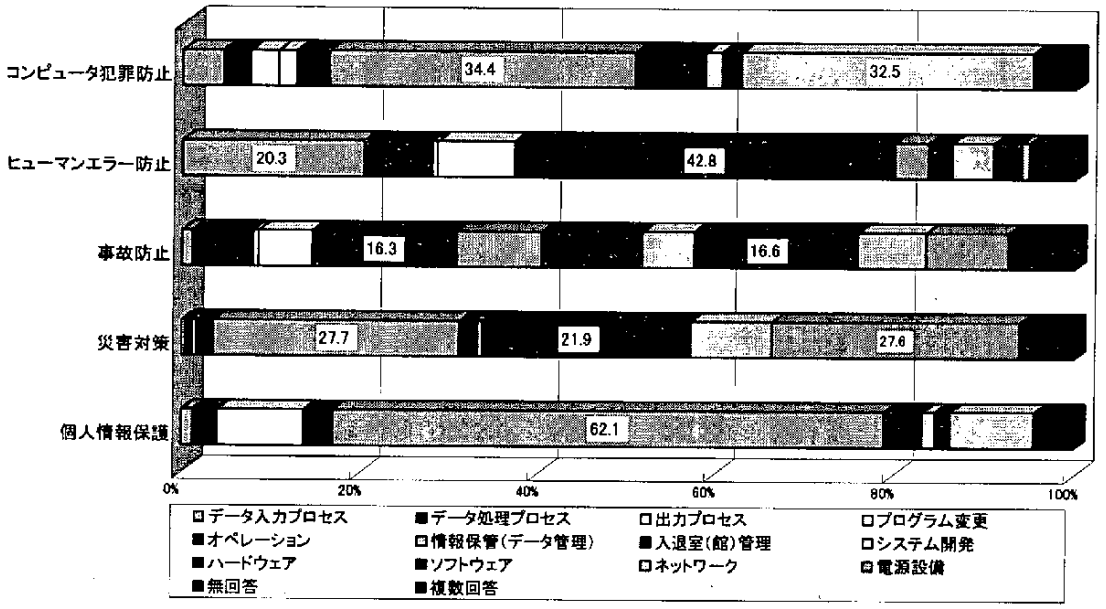

図3－2－14. コンピュータ犯罪防止、ヒューマンエラー防止、事故防止、災害対策、個人情報保護の観点から最も重視すべき分野（被監査部門）

Q37. システム監査を実施する場合、どのような点を充実させなければならないと思いますか。最も重要だと思われるものを1つ選んで下さい。

1	監査計画	126	19.4
2	事前調査	55	8.5
3	実地調査	135	20.8
4	改善勧告内容	161	24.8
5	監査報告会	41	6.3
6	チェックリスト	99	15.3
7	その他	9	1.4
無回答		22	3.4
複数回答		1	0.2
計		649	100.0

システム監査の実施過程でどのような点を充実しなくてはならないか、最も充実すべきと考えている点について調査した。

「改善勧告内容」(24.8%)が高く、ついで「実地調査」(20.8%)、「監査計画」(19.4%)となっている。

Q38. システム監査は誰が実施するのが効果的だと思いますか。最も効果的と思われるものを1つ選んで下さい。

1	監査役(団体等は監事、自治体は監査委員)	33	5.1
2	内部の監査人	108	16.6
3	情報システム部門の要員	14	2.2
4	システム監査技術者試験合格者	74	11.4
5	監査法人・公認会計士	146	22.5
6	システム監査企業台帳に基づくシステム監査企業	242	37.3
7	その他	11	1.7
無回答		21	3.2
計		649	100.0

システム監査は内部監査として実施されている割合が最も高い。しかしながら監査を受ける被監査部門では、最も効果的な監査主体として、内部監査部門ではなく「システム監査企業台帳に基づくシステム監査企業」(37.3%)を挙げている。ついで「監査法人・公認会計士」(22.5%)であり、「内部の監査人」(16.6%)は第3番目となっている。監査担当部門に対する同一の調査では、「内部の監査人」(47.8%)で圧倒的なトップである(Q20)。被監査部門と監査担当部門の意識に大きな差が出ている。(監査担当部門に関する分析は、「3.1.3」を参照のこと。)

その他の意見としては、「内部監査人の報告を外部の専門家がレビュー評価してフィードバックさせる」、「業務内容を理解しているシステム監査人(システム監査技術者)」等が挙げられた。

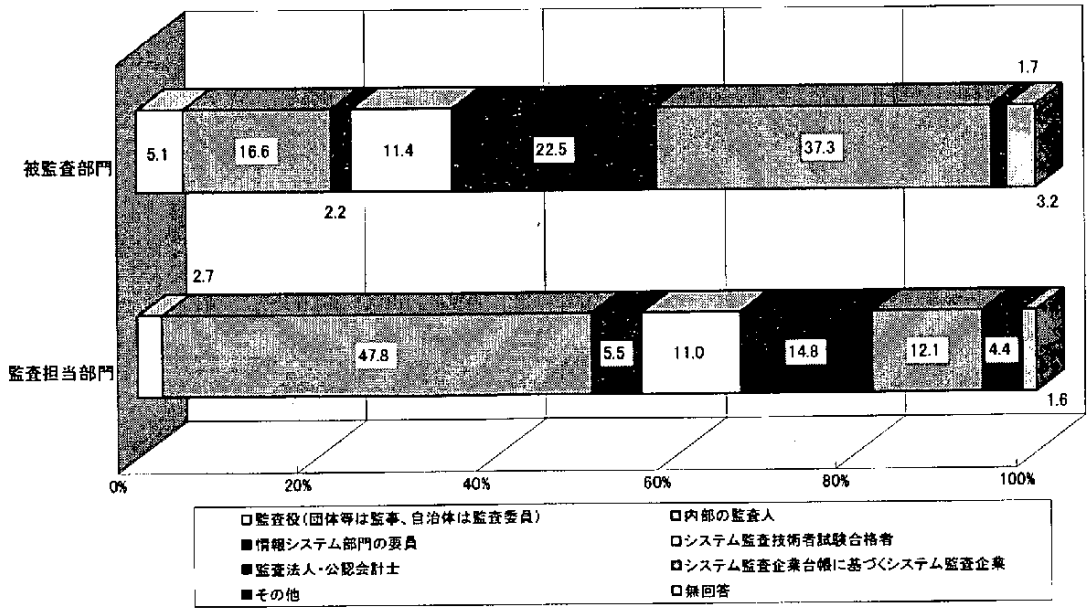

図3−2−15. 最も効果的と思われるシステム監査実施者

3.2.4　情報セキュリティの推進について

JIPDEC では、本調査の他、同じ母集団の情報システム部門（今回調査の被監査部門に該当）を対象とした「情報セキュリティに関する調査」（以下、「情報セキュリティ調査」という。）をそれぞれ隔年で実施している。

今回調査と平成 13 年度に実施した「情報セキュリティ調査」で共通する情報セキュリティ関連項目について、比較分析を併せて行っている。

なお、平成 13 年度「情報セキュリティに関する調査」結果については、JIPDEC ホームページで公開しているので、参照のこと。

○http://www.jipdec.jp/security/01sec.html

Q39. 貴社では情報セキュリティポリシーを策定していますか。

1	定めている	223	34.4
2	現在作成中である	141	21.7
3	作成を検討している	167	25.7
4	現在、定める予定がない	108	16.6
無回答		10	1.5
計		649	100.0

情報セキュリティポリシーの策定状況について、被監査部門では「定めている」が 34.4％であり、「現在作成中」を含めると 56.1％、さらに、「作成を検討している」を含めると 76.4％の事業体が情報セキュリティに対して積極的な姿勢であることがわかる。しかし監査担当部門と比較すると、「定めている」（43.7％）との回答については 10 ポイント近く差がでており、監査担当部門の方がセキュリティポリシーに対する認識が高く、情報セキュリティに対する取組みが進んでいることがわかる。

（Q39～Q43 の質問については監査担当部門でも同一の調査を行っているので、「3.1.5」を参照のこと。）

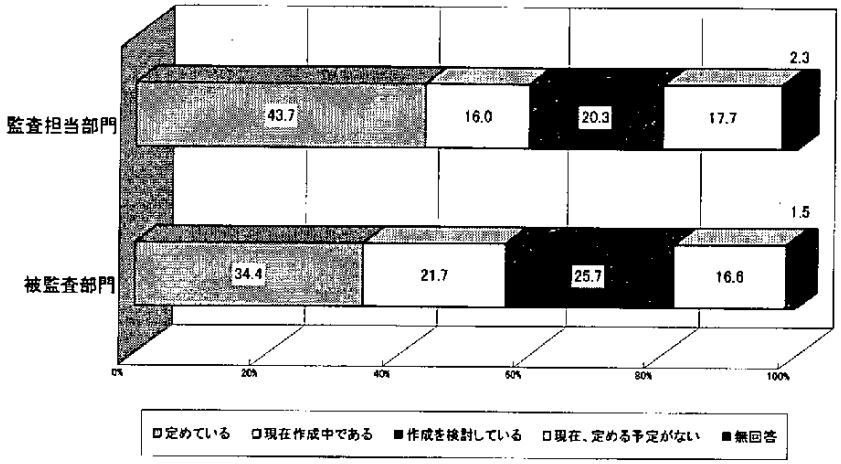

図3－2－16. 情報セキュリティポリシー策定状況

情報セキュリティポリシー策定状況		システム監査普及状況調査		情報セキュリティ調査	
1	定めている	223	34.4	172	24.0
2	現在作成中である	141	21.7	91	12.7
3	作成を検討している	167	25.7	207	28.8
4	現在、定める予定がない*)	108	16.6	241	33.6
無回答		10	1.5	7	1.0
計		649	100.0	718	100.0

*)「情報セキュリティ調査」では選択肢として「必要ない」が設けられているが、ここではこの回答を「予定がない」に加えている（なお、「必要ない」の回答数は「5」である）

（出典：JIPDEC　平成13年度「情報セキュリティに関する調査」Q18）

今回調査と「情報セキュリティ調査」を比較すると、セキュリティポリシーの策定率は10.4ポイント増加している。また、「現在作成中」を含めると19.4ポイント、さらに、「作成を検討している」を含めた場合も16.3ポイント増加しており（情報セキュリティ調査：65.5%）、この1年の間に情報セキュリティポリシーへの取組みが進んでいることがわかる。これは平成14年2月に情報セキュリティの基準である「ISO17799:2000」が「JIS X 5080:2002」となったことも背景にあると考えられる。今後、多くの事業体が情報セキュリティポリシーを採用し、日本の情報処理環境の改善が進むと考えられる。このような状況の中で、監査担当部門は情報セキュリティポリシーに基づく組織、教育、実態の改善などを進めていく推進役としての立場が要求されるであろう。

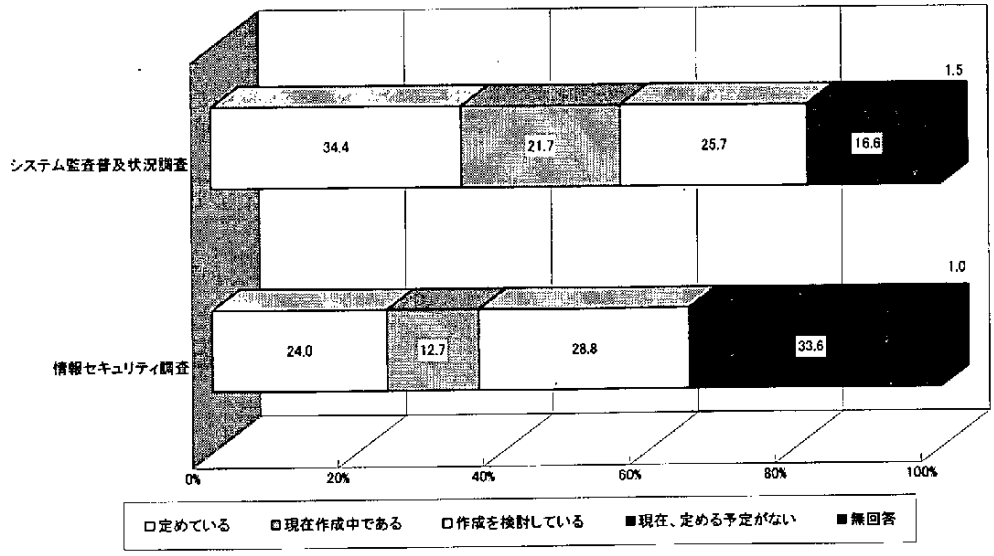

図3－2－17. 情報セキュリティポリシー策定状況（情報セキュリティ調査との比較）

Q40. 貴社では情報セキュリティをどのような体制で推進していますか。(複数回答)

回答件数		649	-
1	情報セキュリティ担当役員を設置している	101	15.6
2	情報セキュリティ委員会を設置している	134	20.6
3	情報システム部門主導で実施している	340	52.4
4	情報セキュリティ専任者を設置している	67	10.3
5	各部門・拠点にセキュリティ担当者を設置している	115	17.7
6	外部のセキュリティコンサルタントを活用している	41	6.3
7	特に実施していない	158	24.3
8	その他	12	1.8
無回答		10	1.5

情報セキュリティ推進体制について、「情報セキュリティ担当役員の設置」は15.6%、「情報セキュリティ委員会の設置」は 20.6%であった。なお、「情報セキュリティ専任者」については10.3%と、監査担当部門（13.7%）同様、低い結果となった。

「各部門・拠点ごとのセキュリティ担当者の設置」については 17.7%（監：21.5%）であり、「情報システム部門主導で実施」（監：50.6%、被：52.4%）と比較すると、情報セキュリティの推進は、情報システム部門の仕事となっているケースが多い。一方、「外部セキュリティコンサルタントの活用」（6.3%）については、監査担当部門同様に低い結果となった。

全体としては、わが国における情報セキュリティの推進が進みつつある状況ではあるが、いまだに情報システム部門に依存しており、今後、情報システムを利用するユーザ側のより一層の関与が望まれるところである。

今後、システム監査や平成15年4月から制度化される情報セキュリティ監査などをきっかけにして情報セキュリティの実効的な推進が望まれる。

また、「JIS X 5080:2000」、ＩＳＭＳ、情報セキュリティ管理基準などでは、情報セキュリティに対する組織化、体制など詳しく述べており、これを活用して、情報セキュリティの推進が望まれる。

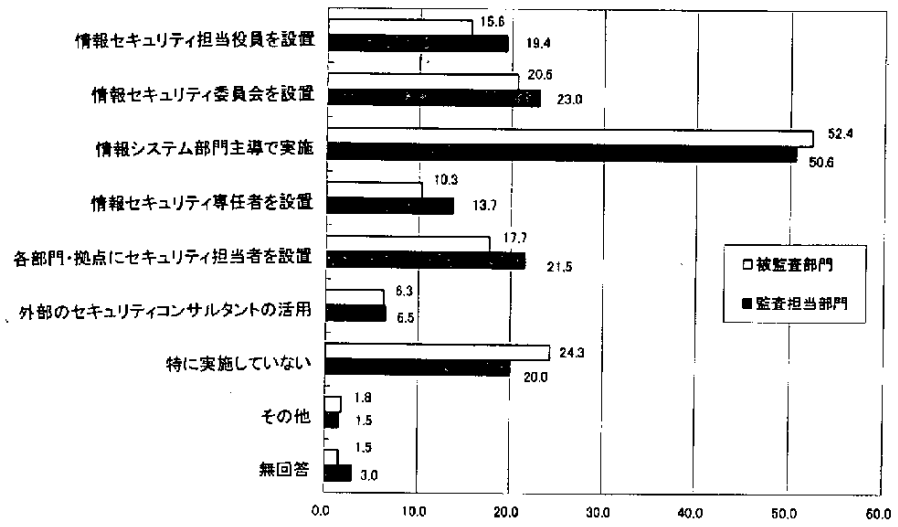

図3－2－18. 情報セキュリティ推進体制

管理者の設置状況		情報セキュリティの管理者		情報システムの管理者	
1	定めている	379	52.8	568	79.1
2	設置を検討している	164	22.8	70	9.7
3	定めていない	162	22.6	69	9.6
4	必要ない	2	0.3	1	0.1
無回答		11	1.5	10	1.4
計		718	100.0	718	100.0

（出典：JIPDEC　平成13年度「情報セキュリティに関する調査」Q22）

「情報セキュリティ調査」では情報システムならびに情報セキュリティに関する管理者の設置状況について調査を行ったが、このうち「情報セキュリティ管理者」は52.8%であった。この結果と今回調査の「情報セキュリティ専任者を設置」および「各部門・拠点にセキュリティ担当者を設置」の合計（28.0%）を比較すると、24.8ポイントという大きな差がみられる。今回調査では、セキュリティ推進体制に関する調査であったため、体制というほどきちんと確立していないという現状を示していると考えるのがよいのではないだろうか。一方、これらの数字に「情報システム部門の関与」を加えると、今回調査では 80.4%となり、「情報セキュリティ調査」の情報システム管理者の79.1%とほぼ同じ結果となる。両方の調査結果からは、情報セキュリティの推進は情報システム部門の関与なしには進めるのが難しいことがいえよう。

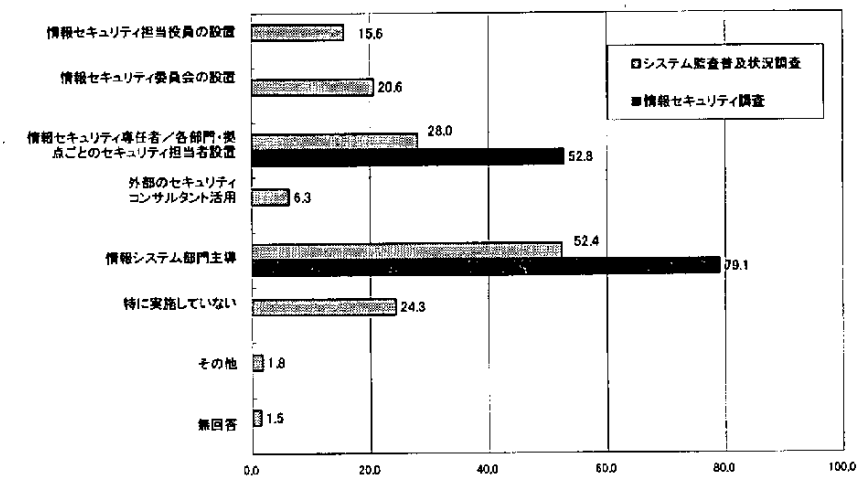

図3－2－19. 情報セキュリティ推進体制（情報セキュリティ調査との比較）

Q41. 情報セキュリティ推進体制で最も重要と思われることを1つ選んで下さい。（単一回答）

1	経営者のリーダーシップ	140	21.6
2	全社的な推進体制	313	48.2
3	情報システム部門の推進体制	34	5.2
4	利用部門の理解・協力	146	22.5
5	その他	4	0.6
無回答		11	1.7
複数回答		1	0.2
計		649	100.0

事業体としての情報セキュリティの推進にあたっての意識について、「経営者のリーダシップ」が21.6%、「全社的な推進体制」が48.2%であった。合計すると、約70%が経営者や全社的な体制を希望していることがわかる。

わが国では、経営者のリーダシップや全社的な推進体制を作ってトップダウン型に情報セキュリティを推進するよりも、利用部門からのボトムアップで進めていく方が効率がよい場合もある。監査担当部門同様、「利用部門の理解・協力」について、22.5%（約5分の1）がボトムアップ型で情報セキュリティを進めている。情報セキュリティは最も情報セキュリティの弱いところから破綻することもある。したがって、事業体として一致して情報セキュリティ対策をとらなければならないことも多い。ただし、トップダウンで命令しただけでは、たとえば、ユーザにＩＤやパスワードの管理を徹底するのは難しいことも指摘されており、今後、事業体の中でどのように情報セキュリティを推進するか、今後より重要となるであろう。

情報セキュリティ確保上の基本的に重要な視点（複数回答）			
1	経営者層の理解	383	53.3
2	管理者の理解	235	32.7
3	担当者の理解	145	20.2
4	社内全体の理解	559	77.9
5	法規制の整備	106	14.8
6	その他	1	0.1
無回答		18	2.5
計		718	-

（出典：JIPDEC　平成13年度「情報セキュリティに関する調査」Q63）

「情報セキュリティ調査」では、「Q63. 情報セキュリティの確保にとり、基本的に重要な視点は何だと思いますか。」という内容で経営者の理解などについて調査した。この調査結果では、「経営者の理解」、「社内全体の理解」を求めるものが、それぞれ、53.3%、77.9%と高い割合を占めている。これは、今回調査の結果とも共通することであり、今後、事業体の中で、経営者および同僚からの理解・支援を推進することが重要である。

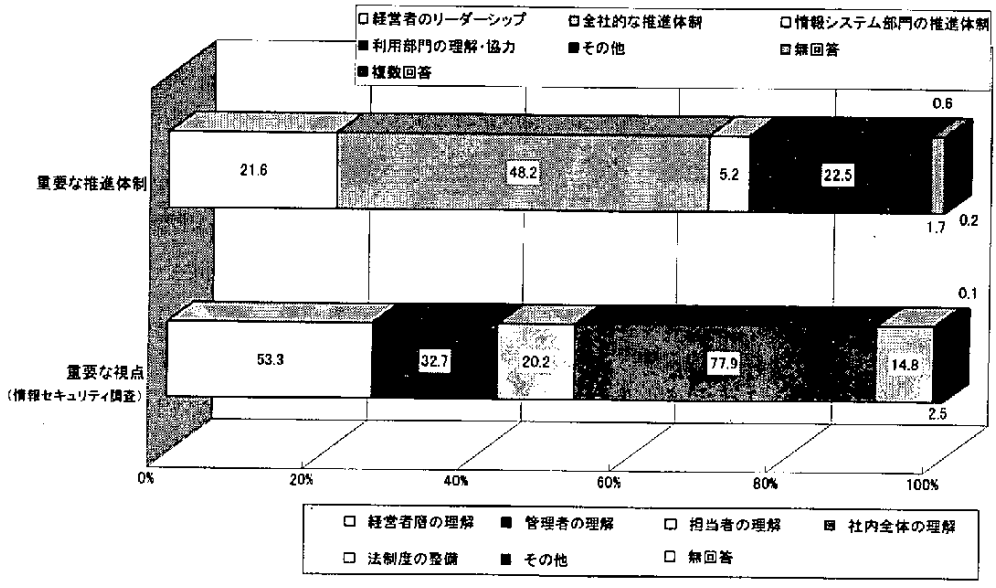

図3－2－20. 最も重要な情報セキュリティ推進体制／重要な視点

Q42.貴社では情報セキュリティについて、優先的に実施しているものを３つまで選んで下さい。

（複数回答）

回答件数		649	－
1	情報セキュリティ対策コストの確保	151	23.3
2	リスク分析の実施	169	26.0
3	システム監査の実施	98	15.1
4	情報セキュリティ教育	251	38.7
5	情報セキュリティ体制の確立	315	48.5
6	情報セキュリティアドミニストレータの確保	20	3.1
7	情報資産の洗い出し	151	23.3
8	ＩＳＭＳの取得	24	3.7
9	プライバシーマークの取得	23	3.5
10	その他	19	2.9
11	特に実施していない	139	21.4
無回答		13	2.0
複数回答（４つ以上選択）		2	0.3

事業体が情報セキュリティを推進する場合、さまざまな対策項目を行わなければならないが、その一方で戦略と整合性が必要であり、また、情報セキュリティ対策には費用が発生するため、全体の中でバランスをとりながら進めていかなければならない。ここでは、このような背景の中で具体的にどのような項目を優先して進めているかの実態を調査した。

回答の高いものから挙げると、「情報セキュリティ体制の確立」、「情報セキュリティ教育」、「リスク分析」、「情報セキュリティ対策コスト」、「情報資産の洗い出し」となっており、きわめて妥当なものであり、情報セキュリティの重要性が認識されつつあることを意味しているといえよう。重要度の順番については、監査部門、被監査部門ともにほとんど同じであり、多くの項目で同様な傾向を示している。

しかし、「情報セキュリティ対策コストの確保」（監査：18.6%、被：23.3%）と「情報資産の洗い出し」（監査：16.5%、被：23.3%）については両部門での回答に差がでている。監査担当部門の場合、前述のQ61などの質問では、情報セキュリティについて被監査部門よりも高い数値を示しているのに対し、これら２つの項目については数値が約５～６ポイントも低いという結果となった。ただ、この調査では優先課題についてベスト３を聞いたため、監査担当部門では、対策コストが相対的に他の項目よりも優先度としてベスト３に入らなかったと考えるのが妥当であろう。一方、被監査部門への調査では、情報システム部門などへの調査であり、コストの面やデータなどの情報資産についてはオーナーでないために重要性の評価ができないことから、これらの項目が高いとみるのが妥当であろう。

なお、今回の調査では、ＩＳＭＳやプライバシーマーク、情報セキュリティアドミニストレータについても選択肢に含んでいるが、重要度という点ではかなり低い結果となった。しかしこれは、事業体にとって認定や資格よりも情報セキュリティの組織、制度、リスク分析等、さらに重要な要素があるということで、単純にこの結果から事業体での重要度がないということは判断できない。しかし、３～６％の事業体ではベスト３に入ると考えているため、それだけ事業体が注

目していると考えられる。

ただ、残念なのは、「特に実施していない」が両部門ともに20％を越えているのは残念である。これには、より一層の情報セキュリティに対するＰＲが重要といえる。

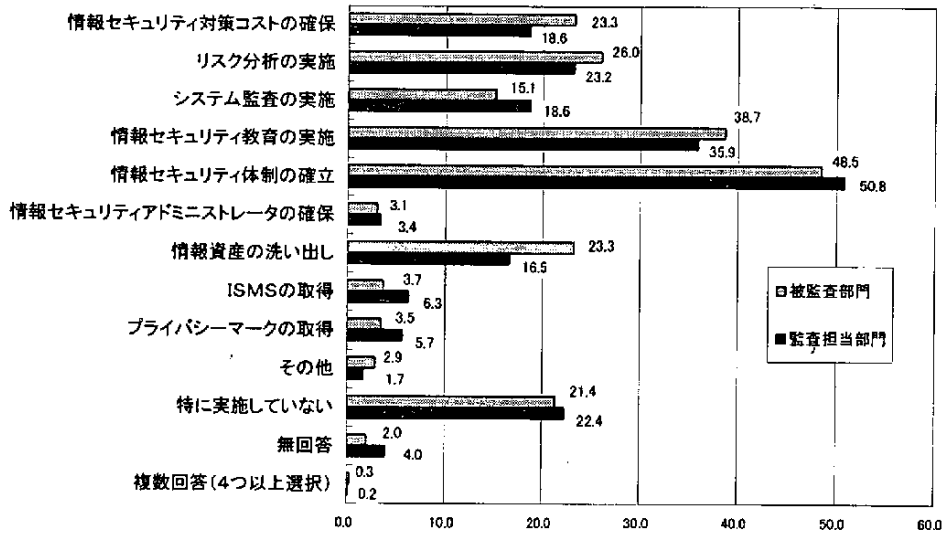

図3－2－21．優先的に実施している情報セキュリティ項目

期密度ランクの設定状況			
1	設定している	204	28.4
2	設定していない	490	68.2
無回答		24	3.3
計		718	100.0

（出典：JIPDEC　平成13年度「情報セキュリティに関する調査」Q47）

「情報セキュリティ調査」では、情報資産に対する機密度ランクの設定状況を調査しているが、「ランクを定めている」との回答は28.4％であった。この結果と今回調査の「情報資産の洗い出し」（23.3％）を比較すると、約５ポイントの差があるが、調査内容の違いを考慮すると、「情報資産に対しての管理」という点でみれば、わが国の事業体にはまだこの点での管理面の甘さがあることがわかる。

リスク分析の実施状況			
1	行っている	135	18.8
2	行っていない	571	79.5
無回答		12	1.7
計		718	100.0

（出典：JIPDEC　平成13年度「情報セキュリティに関する調査」Q65）

一方、リスク分析について、「情報セキュリティ調査」では「行っている」が18.8％であった。この結果と今回調査の「情報資産の洗い出し」（23.3％）を比較すると、今回調査の方が4.5ポイント高い。調査内容の違いを考慮すると、「リスク分析が重要」という点でみると、体制が十分で

ないという点からは、あまり大きな差ではない。両方の調査結果からは、リスク分析の重要性を認識させることが重要といえよう。

Q43. 貴社では情報セキュリティについてどのような教育を実施していますか。(複数回答)

回答件数		649	-
1	新入社員教育を実施している	166	25.6
2	一般社員向け教育を実施している	229	35.3
3	管理職教育を実施している	90	13.9
4	役員教育を実施している	23	3.5
5	派遣要員向け教育を実施している	36	5.5
6	情報セキュリティ担当者の専門教育を実施している	74	11.4
7	その他	39	6.0
8	特に実施していない	269	41.4
無回答		14	2.2

「情報セキュリティ調査」では、「Q24.情報セキュリティ管理についての問題点は何ですか。(複数回答)」の選択肢として「組織の従業員に対する教育・訓練がいきとどかない」を挙げていたが、結果として61.1%(718件中439の回答)、最も重要な問題として挙げられた。今回調査ではこの結果を受け、情報セキュリティ教育の実状を詳しく調査した。

今回の調査結果から、教育の実態について監査担当部門と被監査部門で大変よく似た傾向にあることがわかる。しかし「役員教育の実施」および「派遣要員向け教育の実施」の2項目については両部門ともに3～7%とかなり低く、また、「特に実施していない」は監査担当部門が41.1%、被監査部門が41.4%という結果となった。

「3.1.5」ですでに示しているが、インターネットのウイルス、DoS攻撃、不正侵入などに対処するためにも、新入社員や一般社員向けの教育に限らず、管理職、派遣要員、専門家への再教育、より高度な情報セキュリティ教育を全社的に行う必要がある。

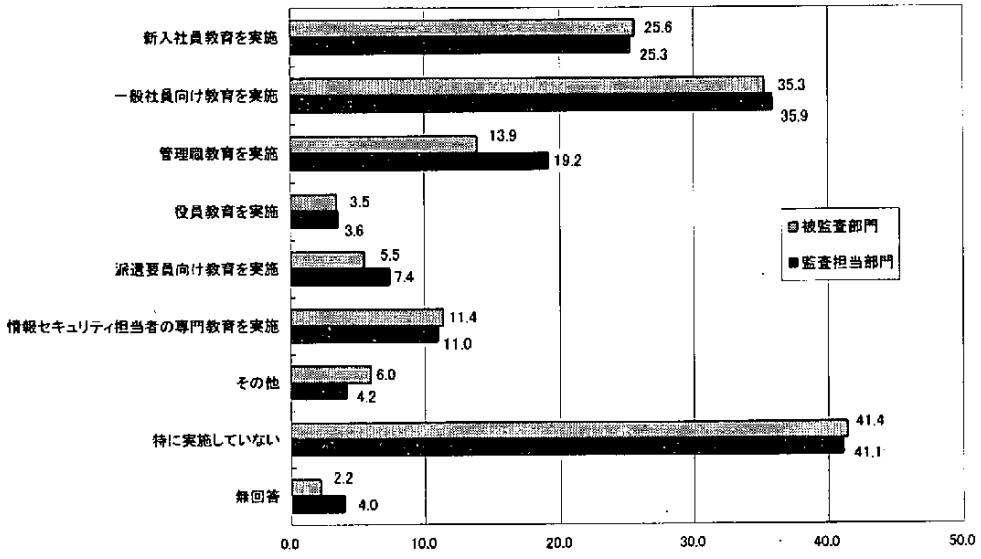

図3－2－22. 情報セキュリティ教育の実施状況

3.2.5　電子メールの利用について

（Q44～48 の質問については被監査部門での同一の調査を行っているので、「3.2.5」を参照のこと。）

Q44. 電子メール利用のルールを定めていますか。

1	定めている	384	59.2	
2	現在作成中である	39	6.0	
3	作成を検討している	95	14.6	
4	現在、定める予定がない	101	15.6	
5	わからない	6	0.9	
6	電子メールを利用していない	13	2.0	→終了
無回答		11	1.7	
計		649	100.0	

電子メールの利用が一般化している中で、79.8%の事業体が利用のルールを作成もしくは作成の必要性を感じている。この傾向は特定の業種に偏ったものではない。従業員数が少ない事業体ほど、ルール作成率が高い。

Q45. 要員の電子メールの利用状況を監視していますか。

1	監視している	235	37.6	
2	今後、監視する予定がある	98	15.7	
3	監視していない	285	45.6	→Q47 へ
4	わからない	6	1.0	→Q47 へ
無回答		1	0.2	
計		625	100.0	

電子メールを利用している事業体のうち、53.3%が利用状況を監視または監視を予定している。業種別では金融業・電気機械器具製造業の実施率が高いが、政府・地方公共団体の実施率が低い。

Q46.（Q45 で「1」、「2」を回答した場合）電子メール利用状況の監視について、ルールを定めていますか。

1	ルールを定め、社員に周知している	162	48.6
2	ルールは定めているが、社員に周知していない	46	13.8
3	現在作成中である	38	11.4
4	作成を検討している	62	18.6
5	現在、定める予定がない	19	5.7
6	わからない	1	0.3
無回答		5	1.5
計		333	100.0

電子メールの利用状況を監視または監視を予定している事業体のうち、48.6%がそのルールを定め、社員に周知している。

Q47. 自宅や出張先からメールサーバへのリモートアクセスを認めていますか。

1	認めている	128	20.5
2	許可制で認めている	196	31.4
3	認めていない	286	45.8
4	わからない	11	1.8
無回答		4	0.6
計		625	100.0

電子メールを利用している事業体のうち、45.8%がリモートアクセスを認めておらず、その中において、政府・地方公共団体で「認めていない」とする割合が高い。

Q48. 自宅の個人アドレスへの社内メールの転送を認めていますか。

1	認めている	196	31.4
2	許可制で認めている	97	15.5
3	認めていない	286	45.8
4	わからない	43	6.9
無回答		3	0.5
計		625	100.0

電子メールを利用している事業体のうち、45.8%が自宅の個人アドレスへ転送を認めておらず、Q47同様、政府・地方公共団体で「認めていない」とする割合が高い。

3.3 クロス集計結果分析

3.3.1 クロス集計対象項目

今年度は、システム監査の実態についてより深い分析を行うため、個々の質問に対する分析とは別にクロス集計による分析を行った。

クロス集計の対象とした項目および集計目的は次のとおりである。

1．監査担当部門対象

質問項目	クロス集計対象項目	クロス集計目的
Q20. システム監査は誰が実施するのが効果的だと思いますか。最も効果的と思うものを１つ選んで下さい。	Q23. システム監査人に最も不足していると思われる知識は何ですか。次の中から１つ選んで下さい。	システム監査人の実施者と必要スキルおよび解決策（教育方法）
	Q24. システム監査人に最も不足していると思われる能力は何ですか。次の中から１つ選んで下さい。	
	Q25. システム監査人に対してどのような教育方法をとっていますか。主に行っているものを１つ選んで下さい。	
Q32. システム監査は次のどの方式で実施しましたか。（複数回答） 項番６．外部委託型（システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託）	Q62. 貴社では情報セキュリティをどのような体制で推進していますか。（複数回答） 項番６．外部のセキュリティコンサルタントを活用している	情報システムの保全における推進体制（内部推進型および外部委託型の傾向分析）
Q52. 監査報告会に出席したのは誰ですか。（複数回答）	Q63. 情報セキュリティ推進体制で最も重要と思われることを１つだけ選んで下さい。	情報システムの保全に関する経営者の関与
Q61. 貴社では情報セキュリティポリシーを策定していますか。	Q12. ＩＳＭＳ（情報セキュリティマネジメントシステム）適合性評価制度を知っていますか。	情報セキュリティポリシー策定企業におけるＩＳＭＳの活用状況
	Q17. 貴社ではシステム監査を実施したことがありますか。	情報セキュリティポリシー策定後の実効性確認実施の有無
	Q66. 貴社では情報セキュリティポリシー監査を実施したことがありますか。	
Q64. 貴社では情報セキュリティについて、優先的に実施しているものを３つまで選んで下さい。（複数回答） 項番１．情報セキュリティ対策コストの確保	Q42. 貴社の情報システムの信頼性を高めるためにもっと投資すべきだと思いますか。	経営環境が厳しい状況での投資状況（予定を含む）
	Q45. 貴社の情報システムの安全性を高めるためにもっと投資すべきだと思いますか。	
	Q48. 貴社の情報システムの効率性を高めるためにもっと投資すべきだと思いますか。	
Q67. 電子メール利用のルールを定めていますか。	Ｑ７．経済産業省から「コンピュータウイルス対策基準」（平成７年改訂）が公表されていることを知っていますか。	電子メール利用ルール策定企業の経済産業書の関連基準の認知

質問項目	クロス集計対象項目	クロス集計目的
	Q10.「コンピュータ不正アクセス対策基準」の中でシステム監査が位置づけられていることを知っていますか。	度
Q72. 電子メールの利用に関して、監査を実施したことがありますか。	Q17. 貴社ではシステム監査を実施したことがありますか。	システム監査実施企業の内、電子メール利用の監査を行った企業の割合
Q63. 情報セキュリティ推進体制で最も重要と思われることを１つだけ選んで下さい。	Q57. システム監査を実施していない理由はどのような点ですか。次の中から主な理由を１つ選んで下さい。	監査人（監査担当部門）における監査阻害要因と解決すべき機能の分析

２．被監査部門対象

質問項目	クロス集計対象質問	クロス集計目的
Q18. システム監査は次のどの方式で実施されましたか。(複数回答)	Q38. システム監査は誰が実施するのが効果的だと思いますか。最も効果的と思われるものを１つ選んで下さい。（貴社の実態とは別にお答えいただいて結構です）	被監査部門が想定するあるべき監査人と現実の監査人との差異の有無。
Q28. 監査報告書の指摘事項や改善勧告の内容について妥当だと思いますか。 項番３．妥当だと思わない	Q22. どのような点で問題があったと思いますか。最も問題と思った点を１つ選んで下さい。(単一回答)	被監査部門が監査結果に不満を持った原因の分析
	Q23. システム監査を受けた時、現場の負担はありましたか。	
	Q24. システム監査を受けた結果どのような点が問題だと感じましたか。最も問題と感じたものを１つ選んで下さい。(単一回答)	
	Q25. 監査結果について、システム監査人と貴部門との間で講評会（監査報告書を作成する前に意見交換、確認等を行うことをいう)が行われましたか。	
Q37. システム監査を実施する場合、どのような点を充実させなければならないと思いますか。最も重要だと思われるものを１つ選んで下さい。 項番４．改善勧告内容 項番５．監査報告会	Q22. どのような点で問題があったと思いますか。最も問題と思った点を１つ選んで下さい。(単一回答)	被監査部門に対する監査結果通知方法の妥当性検証
	Q26. 監査報告書の作成後に関係者を含めた監査報告会が行われましたか。	
	Q27. 監査報告会に情報システム部門から出席しましたか。	
Q39. 貴社では情報セキュリティポリシーを策定していますか。	Q44. 電子メール利用のルールを定めていますか。	電子メールによるリスクの認知度の分析
Q40. 貴社では情報セキュリティをどのような体制で推進していますか。(複数回答) 項番６．外部のセキュリティコンサルタントを活用している	Q18. システム監査は次のどの方式で実施されましたか。(複数回答) 項番２．外部委託型（システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託）	情報システムの保全におけるアウトソーサの利用度

3.3.2　監査担当部門対象

1．『Q20. 効果的と思うシステム監査実施者』のクロス集計

×Q23. システム監査人に不足していると思われる知識

不足している知識 / システム監査実施者	回答件数	経営に関する知識		業務知識		法律知識		監査知識	
監査役（団体等は監事、自治体は監査委員）	5	0	0.0	1	20.0	0	0.0	0	0.0
内部の監査人	87	10	11.5	26	29.9	14	16.1	11	12.6
情報システム部門の要員	10	3	30.0	2	20.0	0	0.0	1	10.0
システム監査技術者試験の合格者	20	3	15.0	3	15.0	1	5.0	5	25.0
監査法人・公認会計士	27	0	0.0	8	29.6	0	0.0	8	29.6
システム監査企業台帳に基づくシステム監査企業	22	1	4.5	5	22.7	0	0.0	1	4.5
その他	8	0	0.0	0	0.0	2	25.0	1	12.5
無回答	3	0	0.0	0	0.0	0	0.0	0	0.0
計	182	17	9.3	45	24.7	17	9.3	27	14.8

不足している知識 / システム監査実施者	情報システムの知識		その他		わからない		無回答		複数回答	
監査役（団体等は監事、自治体は監査委員）	4	80.0	0	0.0	0	0.0	0	0.0	0	0.0
内部の監査人	16	18.4	5	5.7	4	4.6	1	1.1	0	0.0
情報システム部門の要員	4	40.0	0	0.0	0	0.0	0	0.0	0	0.0
システム監査技術者試験の合格者	5	25.0	0	0.0	3	15.0	0	0.0	0	0.0
監査法人・公認会計士	4	14.8	0	0.0	4	14.8	2	7.4	1	3.7
システム監査企業台帳に基づくシステム監査企業	7	31.8	1	4.5	2	9.1	5	22.7	0	0.0
その他	2	25.0	2	25.0	1	12.5	0	0.0	0	0.0
無回答	0	0.0	0	0.0	0	0.0	3	100.0	0	0.0
計	42	23.1	8	4.4	14	7.7	11	6.0	1	0.5

このクロス分析では、監査担当部門が何に不満を感じ、『効果的と思うシステム監査実施者』を選択したかを考察したい。監査担当部門は、システム監査人が最も不足している知識として『業務知識』を挙げている。そのため、最も効果的なシステム監査人として自社業務に精通している『内部監査人』に回答が集中している傾向にある。監査人の業務知識不足により、監査時間の多くが業務説明に費やされたり、業務内容の誤解から監査結果にも誤認を生じたケースが経験上あったのではないかと推察される。次に多いのが『情報システムの知識不足』であるが、これは、情報システム部門からみれば、内部監査人にも、公認会計士、システム監査企業などの外部監査法人のすべてにもあてはまっている。特筆すべきは、本来情報システムにある程度習熟していると思われる『システム監査技術者試験の合格者』や『システム監査企業台帳に基づくシステム監

査企業』でこの回答が最多の意見となっている事実である。資格取得者や情報システムの専門家といえども、昨今の技術進歩や新しい業務形態に十分についていけない現状がある。監査担当部門としては、情報システムに熟知しているはずの『システム監査技術者試験の合格者』や『システム監査企業台帳に基づくシステム監査企業』が、想定以下のスキルしかなかったことがこの回答を選ばせたと考えられる。また、『監査法人・公認会計士』に対する監査知識不足を主張する意見も意外に多かった。前述の『システム監査技術者試験の合格者』や『システム監査企業台帳に基づくシステム監査企業』に対する情報システム知識と同様、委託している監査担当部門としては、本来プロとして期待している結果を十分出していないという判断であろうと考えられる。委託先に対する監査担当部門も目は厳しいが、それだけアウトソーサに対する期待度が大きいということであろう。

×Q24. システム監査人に不足していると思われる能力

不足している能力 / システム監査実施者	回答件数	インタビュー能力		分析能力		判断能力		報告書作成能力	
監査役（団体等は監事、自治体は監査委員）	5	1	20.0	3	60.0	1	20.0	0	0.0
内部の監査人	87	9	10.3	32	36.8	14	16.1	11	12.6
情報システム部門の要員	10	1	10.0	4	40.0	2	20.0	1	10.0
システム監査技術者試験の合格者	20	5	25.0	5	25.0	3	15.0	0	0.0
監査法人・公認会計士	27	0	0.0	10	37.0	3	11.1	1	3.7
システム監査企業台帳に基づくシステム監査企業	22	4	18.2	5	22.7	1	4.5	1	4.5
その他	8	0	0.0	1	12.5	1	12.5	0	0.0
無回答	3	0	0.0	0	0.0	0	0.0	0	0.0
計	182	20	11.0	60	33.0	25	13.7	14	7.7

不足している能力 / システム監査実施者	その他		わからない		無回答		複数回答	
監査役（団体等は監事、自治体は監査委員）	0	0.0	0	0.0	0	0.0	0	0.0
内部の監査人	3	3.4	17	19.5	1	1.1	0	0.0
情報システム部門の要員	0	0.0	2	20.0	0	0.0	0	0.0
システム監査技術者試験の合格者	1	5.0	6	30.0	0	0.0	0	0.0
監査法人・公認会計士	2	7.4	7	25.9	3	11.1	1	3.7
システム監査企業台帳に基づくシステム監査企業	0	0.0	5	22.7	6	27.3	0	0.0
その他	2	25.0	4	50.0	0	0.0	0	0.0
無回答	0	0.0	0	0.0	3	100.0	0	0.0
計	8	4.4	41	22.5	13	7.1	1	0.5

このクロス分析では、監査担当部門がどの能力不足に不満を感じ、『効果的と思うシステム監査実施者』を選択したかを考察したい。各システム監査人とも最も多く選ばれているのは、『分析能力』である。分析能力の不足は、どのシステム監査実施者でも解決困難な問題であると監査担当部門は認識している。『効果的と思うシステム監査実施者』に『内部監査人』を選択した事業体が『分析能力』に次いで比較的多く選択したのが、『判断能力』と『報告書作成能力』である。監査の分析結果に基づき一定の方向で結論づけ、報告書を作成する上で、やはり業務知識や社内状況の認識不足から監査の分析結果を十分活かし切れず、報告書の内容も通り一片な内容となってしまうことから、監査担当部門として被監査部門に対し、有効な提言ができていないジレンマを感じているためと思われる。内部の監査人であれば、少なくとも業務知識や社内状況を考慮した報告が可能である、との思いがあるためであろう。

逆に『効果的と思うシステム監査実施者』に『監査法人・公認会計士』を選択した回答者が、不足している能力として『インタビュー能力』を上げている回答者が一人もいないのは、特徴的である。監査法人や公認会計士が被監査部門に対するインタビューを的確に行い、監査担当部門に対し、一定の成果ある報告を行っているためであろう。職業上のスキルとはいえ、他の分野の監査人は大いに見習う必要がある。

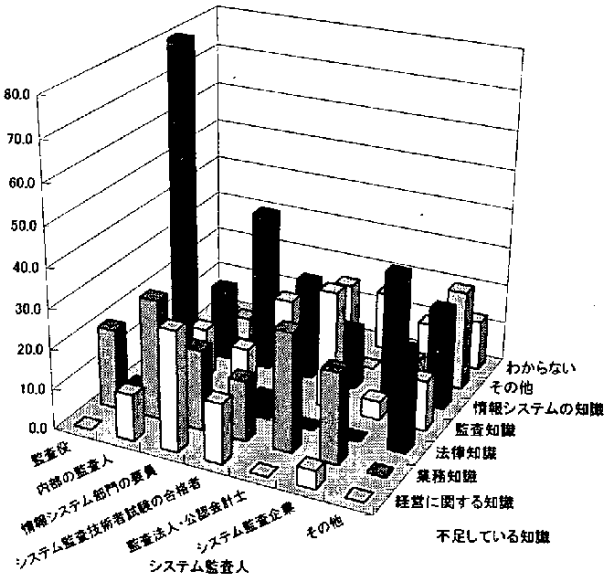

図3－3－1. システム監査人に不足している知識(監査担当部門)

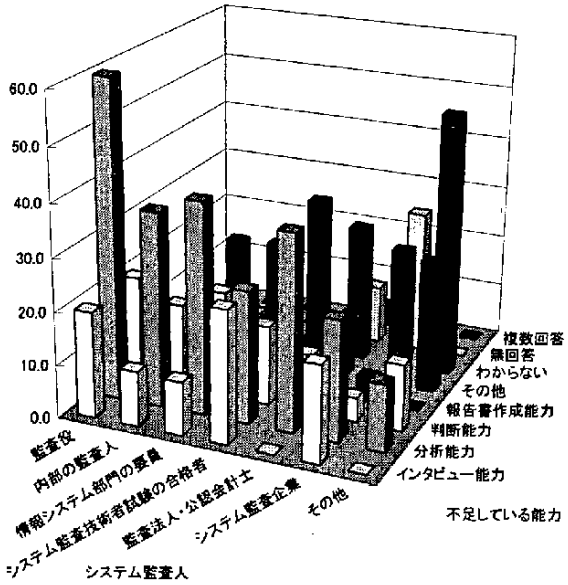

図3－3－2. システム監査人に不足している能力(監査担当部門)

Q25. システム監査人に対する教育方法

教育方法 / システム監査実施者	回答件数	外部セミナーを利用		社内教育		ＯＪＴ		通信教育	
監査役（団体等は監事、自治体は監査委員）	5	1	20.0	0	0.0	0	0.0	0	0.0
内部の監査人	87	38	43.7	2	2.3	21	24.1	0	0.0
情報システム部門の要員	10	1	10.0	0	0.0	3	30.0	0	0.0
システム監査技術者試験の合格者	20	8	40.0	1	5.0	0	0.0	0	0.0
監査法人・公認会計士	27	5	18.5	1	3.7	1	3.7	0	0.0
システム監査企業台帳に基づくシステム監査企業	22	5	22.7	0	0.0	3	13.6	1	4.5
その他	8	3	37.5	0	0.0	1	12.5	0	0.0
無回答	3	0	0.0	0	0.0	0	0.0	0	0.0
計	182	61	33.5	4	2.2	29	15.9	1	0.5

教育方法 / システム監査実施者	その他		特に教育は実施していない		監査を外部委託しているため該当しない		無回答		複数回答	
監査役（団体等は監事、自治体は監査委員）	1	20.0	3	60.0	0	0.0	0	0.0	0	0.0
内部の監査人	1	1.1	17	19.5	6	6.9	2	2.3	0	0.0
情報システム部門の要員	0	0.0	3	30.0	2	20.0	1	10.0	0	0.0
システム監査技術者試験の合格者	0	0.0	10	50.0	1	5.0	0	0.0	0	0.0
監査法人・公認会計士	0	0.0	8	29.6	6	22.2	5	18.5	1	3.7
システム監査企業台帳に基づくシステム監査企業	0	0.0	5	22.7	3	13.6	5	22.7	0	0.0
その他	1	12.5	1	12.5	2	25.0	0	0.0	0	0.0
無回答	0	0.0	0	0.0	0	0.0	3	100.0	0	0.0
計	3	1.6	47	25.8	20	11.0	16	8.8	1	0.5

このクロス分析では、効果的な監査実施者全体を通じ、『外部での教育』に期待する傾向が強いことがわかる。これは、自社内に監査人教育を行う教育カリキュラムがなく、全社的なニーズもないことから、外部教育機関での育成が最も効果的と考えての回答と思われる。『内部の監査人』を効果的な監査実施者として選択しているグループが次に多く選んでいるのが、『自社内でのＯＪＴ』である。これは、社内で行う監査について、社内の監査スキル保有者の下で実監査を行いながら監査スキルを習得していく社内システムが確立している事業体と、監査スキルの確立を個人の努力にのみ期待している事業体の二者に大別される。このクロス分析からは、どちらのケースが多いのかは判別できないが、前者の事業体が多くあることを期待したい。『内部監査人』を効果的な監査実施者として挙げている事業体のうち、17社は特に教育を行っていない。これらの事

業体では監査スキルの向上が望めないので、ぜひ何らかの教育を行うことをお勧めしたい。デフレ不況のため、経営環境が厳しく、教育予算など十分に確保できない現状は認識しているが、監査スキルの高い監査人が監査を行うことで、業務の合理化や情報システムにかかる経費が削減できることもあり、その場合の費用対効果が大きい。監査担当部門は教育予算の獲得への努力をお願いしたい。

2.『Q32 システム監査実施方式』のクロス集計

×Q62. 情報セキュリティの推進体制

監査実施方式＼推進体制	回答件数	情報ｾｷｭﾘﾃｨ担当役員の設置		情報ｾｷｭﾘﾃｨ委員会の設置		情報ｼｽﾃﾑ部門主導で実施		情報ｾｷｭﾘﾃｨ専任者を設置		各部門・拠点にｾｷｭﾘﾃｨ担当者を設置	
内部監査部門型	97	33	34.0	43	44.3	51	52.6	27	27.8	43	44.3
部門監査型	14	4	28.6	5	35.7	7	50.0	1	7.1	8	57.1
指名方式	5	2	40.0	2	40.0	2	40.0	0	0.0	2	40.0
委員会方式	5	4	80.0	4	80.0	1	20.0	0	0.0	1	20.0
チームアプローチ	4	1	25.0	1	25.0	2	50.0	1	25.0	1	25.0
外部委託型	46	16	34.8	14	30.4	23	50.0	8	17.4	18	39.1
その他	8	2	25.0	1	12.5	6	75.0	1	12.5	1	12.5
無回答	1	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
計	180	62	34.4	70	38.9	92	51.1	38	21.1	74	41.1

監査実施方式＼推進体制	外部のｾｷｭﾘﾃｨｺﾝｻﾙﾀﾝﾄを活用		特に実施していない		その他		無回答	
内部監査部門型	11	11.3	3	3.1	1	1.0	1	1.0
部門監査型	3	21.4	0	0.0	0	0.0	0	0.0
指名方式	0	0.0	0	0.0	0	0.0	0	0.0
委員会方式	1	20.0	0	0.0	0	0.0	0	0.0
チームアプローチ	0	0.0	0	0.0	0	0.0	0	0.0
外部委託型	7	15.2	1	2.2	0	0.0	2	4.3
その他	0	0.0	0	0.0	0	0.0	0	0.0
無回答	0	0.0	1	100.0	0	0.0	0	0.0
計	22	12.2	5	2.8	1	0.6	3	1.7

ここでは、情報セキュリティの推進体制とシステム監査の推進体制を分析している。最も多いパターンは、『情報セキュリティの専任者』を置き、『内部監査部門による監査推進』を行う方式である。事業体活動における情報システムの重要性を鑑み、内部で専任者を養成、設置するようになってきている。これとは逆に、すべてをアウトソーサへ依存している事業体を分析すると、情報システムの保全に関わるアウトソーサは多くのサービスメニューを掲げているが、情報セキュリティの推進とシステム監査の推進の両方をアウトソーサに委ねている事業体は７社と全体の約3.9%にすぎない。

3．『Q52. 監査報告会への出席者』のクロス集計

×Q63. 情報セキュリティ推進体制で最な重要なこと

セキュリティ推進体制 / 監査報告会出席者	回答件数	経営者のリーダーシップ		全社的な推進体制		情報ｼｽﾃﾑ部門の推進体制		利用部門の理解・協力	
最高経営者（会長、社長、知事、市長等）	45	10	22.2	24	53.3	0	0.0	9	20.0
財務担当役員	20	3	15.0	9	45.0	1	5.0	7	35.0
情報システム担当役員	47	10	21.3	25	53.2	0	0.0	11	23.4
監査役	38	7	18.4	20	52.6	0	0.0	10	26.3
情報システム部門の管理者	72	12	16.7	44	61.1	2	2.8	13	18.1
内部監査人	59	11	18.6	35	59.3	1	1.7	11	18.6
ユーザ部門の管理者	42	8	19.0	24	57.1	2	4.8	8	19.0
外部のシステム監査人	11	1	9.1	7	63.6	1	9.1	2	18.2
その他	9	1	11.1	4	44.4	0	0.0	3	33.3
計	343	63	18.4	192	56.0	7	2.0	74	21.6

セキュリティ推進体制 / 監査報告会出席者	その他		無回答	
最高経営者（会長、社長、知事、市長等）	0	0.0	2	4.4
財務担当役員	0	0.0	0	0.0
情報システム担当役員	0	0.0	1	2.1
監査役	0	0.0	1	2.6
情報システム部門の管理者	0	0.0	1	1.4
内部監査人	0	0.0	1	1.7
ユーザ部門の管理者	0	0.0	0	0.0
外部のシステム監査人	0	0.0	0	0.0
その他	0	0.0	1	11.1
計	0	0.0	7	2.0

情報セキュリティの推進における理想と現実を分析した。情報セキュリティの推進体制として、経営者のトップダウンによる体制が本来あるべき推進体制である。そのため、社長または情報システム担当役員（ＣＩＯ）が情報システムの安全に関して推進していく体制の有無と監査担当部門としてトップダウンの重要性の意識の有無を分析する。

結論からいうと、監査報告会の出席者が『情報システム部門の管理者』、『内部監査人』、『ユーザ部門の管理者』に留まっており、情報セキュリティの推進体制も『全社的な体制』との漠然とした回答が多い。これでは監査結果のフィードバックが経営に反映されることはなく、監査担当部門の自己満足に終わる可能性がある。まず、監査担当部門は監査結果を必ず最高経営者またはＣＩＯにフィードバックし、トップダウンで問題点の解決にあたる事業体内の体制を構築する努力が必要である。

4．『Q61．情報セキュリティポリシー策定状況』のクロス集計

×Q12．ＩＳＭＳ適合性評価制度の認知度

ISMS適合性評価制度 / ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定状況	回答件数	知っている		知らない		無回答	
定めている	207	109	52.7	95	45.9	3	1.4
現在作成中である	76	35	46.1	41	53.9	0	0.0
作成を検討している	96	20	20.8	73	76.0	3	3.1
現在、定める予定がない	84	5	6.0	74	88.1	5	6.0
無回答	11	3	27.3	6	54.5	2	18.2
計	474	172	36.3	289	61.0	13	2.7

当クロス分析では、情報セキュリティポリシーを策定した、または策定中の事業体に対するＩＳＭＳ適合性評価制度の認知度を分析している。やはり傾向として情報セキュリティポリシーを策定済み企業の半数以上（52.7%）、および現在策定中の企業の約半数（46.1%）が、ＩＳＭＳ適合性評価制度を知っており、作成時に何らかの参考にしたものと推測できる。これに対し情報セキュリティポリシー策定にあまり関心のない企業では、ＩＳＭＳの制度自体を知らない企業が多い。ＩＳＭＳ適合性評価制度に関する広報活動を強化するとともに、認定取得を公的機関への入札条件にするなどの、認定所得企業への優遇策を推進し、当制度を拡大していく必要性がある。

×Q17．システム監査の実施状況

システム監査の実施 / ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定状況	回答件数	ある		ない	
定めている	207	121	58.5	86	41.5
現在作成中である	76	26	34.2	50	65.8
作成を検討している	96	24	25.0	72	75.0
現在、定める予定がない	84	9	10.7	75	89.3
無回答	11	2	18.2	9	81.8
計	474	182	38.4	292	61.6

結果をみると、情報セキュリティポリシーを定めている事業体のうち、41.5%がシステム監査を実施していないことに驚かされる。情報セキュリティポリシーは多くの事業体で定められているが、システム監査は比較的実施されていない。これには以下のような理由が考えられる。

①ベンダ企業から情報システムを購入し、利用のみを行うユーザ事業体

②自社で情報システムの開発や維持を行っており、情報セキュリティポリシーを制定した事業体

①の事業体では、システム監査は行われないことが多い。特にサーバを中心に構築されたシステムを利用している事業体では、情報セキュリティポリシー監査を実施していればシステム監査

に代替でき、問題はないと思われる。

②の事業体は、情報セキュリティポリシーとシステム監査項目に多くの関連性があることから、システム監査も併せて実施することをお勧めしたい。情報システム全体をチェックすることで、当該事業体の情報システムがより強固なものになる。情報システムの利用者に対して万全な体制を確立しても、肝心なシステム構築段階で問題があるようでは、簡単にセキュリティが破られる可能性が高い。必ずシステム構築段階にも目を向けていただきたい。

×Q66. 情報セキュリティポリシー監査の実施状況

セキュリティポリシー監査の実施 / セキュリティポリシー策定状況	回答件数	ある		ない		無回答	
定めている	207	53	25.6	152	73.4	2	1.0
現在作成中である	76	3	3.9	73	96.1	0	0.0
作成を検討している	96	3	3.1	93	96.9	0	0.0
現在、定める予定がない	84	0	0.0	80	95.2	4	4.8
無回答	11	0	0.0	4	36.4	7	63.6
計	474	59	12.4	402	84.8	13	2.7

情報セキュリティポリシー監査を実施した事業体がセキュリティポリシー策定事業体の４分の１（25.6%）しかないのは、大きな問題である。これでは、実際に策定されたセキュリティポリシーが遵守されているかどうかわからず、セキュリティポリシーを策定していない事業体と結果としては、大して変わらないことになる。おそらく策定されたセキュリティポリシーに監査などの内部チェック機能が欠落しているのが原因と考えられる。基本的にはセキュリティポリシー策定後、そのポリシーに基づく監査を行い、セキュリティポリシーの遵守状況と問題点を把握し、改善を行う必要がある。Plan⇒Do⇒Check⇒Action（ＰＤＣＡ）のサイクルをまわしながらセキュリティポリシーをより良く昇華していく活動が重要であり、このことについてもっと啓蒙していく必要性を感じた。このような考え方はＩＳＯ9001やプライバシーマークでの認定取得と共通であり、国際的にも確立された手法であることから、セキュリティポリシーを策定したすべての事業体に必ずＰＤＣＡサイクルが反映されるように期待したい。

最後に、情報セキュリティポリシーの策定に着手していない事業体については必ず何らかのルールを作ることを提言したい。情報システムはどの事業体にとっても現在の業務になくてはならないものであり、その情報システムがトラブルやウイルスなどにより失われた場合の損失は事業体活動に大きな影響を及ぼすものである。ポリシー策定の時間や策定に関わる要員の確保など困難な問題はあるが、情報システムの損失に比べれば費用対効果として十分に有用である。簡単なものから策定し、時間をかけて内容を充実していけばよいものである。とりあえずできる範囲で策定されることをお勧めする。

5．『Q63. 情報セキュリティ推進体制』のクロス集計

×Q57. システム監査を実施していない理由

システム監査未実施の理由 / セキュリティ推進体制	回答件数	トップマネジメントの認識が欠如		コンセンサス、組織風土が十分に育っていない		システム監査の実施よりもシステム化推進		実施する担当者（部門）の確保が難しい		方法、制度、手続きなどが十分でない	
経営者のリーダーシップ	45	3	6.7	10	22.2	11	24.4	5	11.1	6	13.3
全社的な推進体制	140	3	2.1	23	16.4	33	23.6	26	18.6	30	21.4
情報システム部門の推進体制	26	1	3.8	4	15.4	5	19.2	4	15.4	4	15.4
利用部門の理解・協力	65	4	6.2	7	10.8	13	20.0	13	20.0	10	15.4
その他	2	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
無回答	14	0	0.0	0	0.0	1	7.1	1	7.1	2	14.3
計	292	11	3.8	44	15.1	63	21.6	49	16.8	52	17.8

システム監査未実施の理由 / セキュリティ推進体制	効果が明確でない		必要性を感じない		その他		無回答		複数回答	
経営者のリーダーシップ	0	0.0	4	8.9	2	4.4	4	8.9	0	0.0
全社的な推進体制	3	2.1	10	7.1	4	2.9	8	5.7	0	0.0
情報システム部門の推進体制	2	7.7	2	7.7	1	3.8	2	7.7	1	3.8
利用部門の理解・協力	0	0.0	7	10.8	1	1.5	8	12.3	2	3.1
その他	0	0.0	0	0.0	2	100.0	0	0.0	0	0.0
無回答	0	0.0	4	28.6	1	7.1	4	28.6	1	7.1
計	5	1.7	27	9.2	11	3.8	26	8.9	4	1.4

ここでは、システム監査が行われない原因について考察した。監査が行われていない事業体では、システム監査を実施するよりもシステム化推進を優先して考えている事業体が多いことがわかる。これは、利用部門からの情報システム部門に対する要求が多く、監査に裂く時間がない場合が多い。『実施する担当者（部門）の確保が難しい』を選択した企業もこれに該当するケースが多い。この状況を改めるのは、最高経営者またはＣＩＯによりトップダウンによるシステム監査の実施以外に方法がない。システム監査を行うには、監査担当部門も被監査部門も既存業務以外に監査のための時間が取られるだけでなく、被監査部門では自らの問題点を指摘されるなどのデメリットもあり、社内に相当な抵抗感がある。しかし、企業経営からみると、情報システムが抱えるリスクからの保護に役立ち、問題点を明確にできることで、業務の合理化や無駄の撲滅による経費削減に繋がるケースが多い。全社的な推進体制を確立し、システム監査を実施するかしないかは、経営者の判断にかかっていることを監査担当部門も見失いがちである。監査担当部門としても、最高経営者もしくはＣＩＯに対して、システム監査を行うことの有意性を説き、ぜひ実施させてほしい。

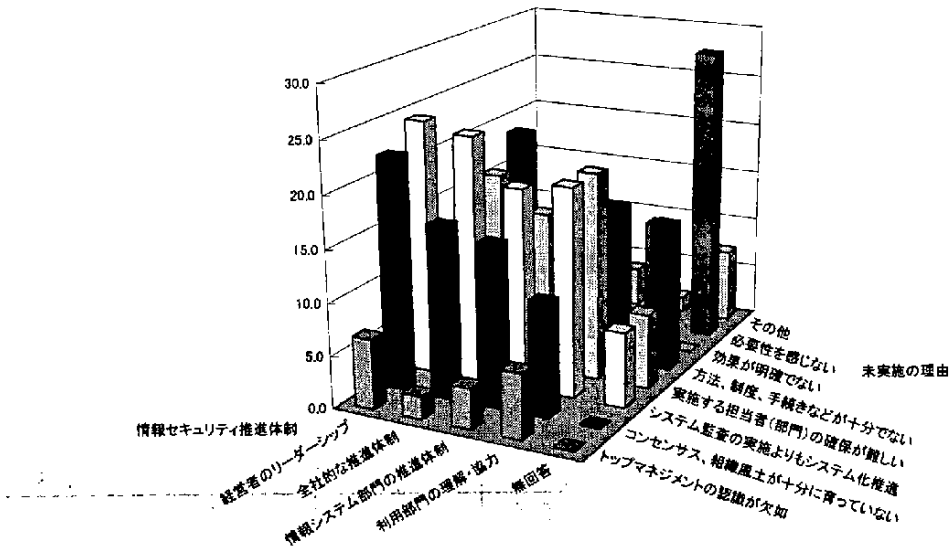

図3－3－3. システム監査未実施の理由(監査担当部門)

6．『Q64. 優先的に行っている情報セキュリティ対策』のクロス集計

×Q42. 情報システムの信頼性を高めるための投資の必要性

信頼性のための投資の必要性 / 情報セキュリティ対策	回答件数	思う		思わない		わからない		無回答	
情報セキュリティ対策コストの確保	26	21	80.8	3	11.5	2	7.7	0	0.0
リスク分析の実施	45	31	68.9	10	22.2	3	6.7	1	2.2
システム監査の実施	69	43	62.3	16	23.2	9	13.0	1	1.4
情報セキュリティ教育の実施	55	36	65.5	13	23.6	6	10.9	0	0.0
情報セキュリティ体制の確立	94	64	68.1	19	20.2	10	10.6	1	1.1
情報ｾｷｭﾘﾃｨｱﾄﾞﾐﾆｽﾄﾚｰﾀの確保	3	2	66.7	1	33.3	0	0.0	0	0.0
情報資産の洗い出し	26	19	73.1	5	19.2	2	7.7	0	0.0
ＩＳＭＳの取得	18	13	72.2	3	16.7	2	11.1	0	0.0
プライバシーマークの取得	19	14	73.7	3	15.8	2	10.5	0	0.0
その他	4	4	100.0	0	0.0	0	0.0	0	0.0
特に実施していない	2	1	50.0	0	0.0	1	50.0	0	0.0
無回答	2	1	50.0	0	0.0	1	50.0	0	0.0
計	363	249	68.6	73	20.1	38	10.5	3	0.8

情報システムの信頼性を高めるための投資の必要性について、必要性を認識している事業体においては、『情報セキュリティ体制の確立』を選択した事業体がもっとも多く（64社、68.1%）、次に『「システム監査の実施』となっている（43社、62.3%）。なお、信頼性投資を不必要とした事業体についてもこれらの項目を選択したところが最も多く、体制確立や監査の実施だけでは目に見える費用はかからないとの認識で、投資不要と判断したのではないかと推定した。実際、これらの事業体の従業員が行う活動にも経費がかかるため、予算を計上するのが一般的である。

×Q45. 情報システムの安全性を高めるための投資の必要性

安全性のための投資の必要性 / 情報セキュリティ対策	回答件数	思う		思わない		わからない		無回答	
情報セキュリティ対策コストの確保	26	20	76.9	4	15.4	2	7.7	0	0.0
リスク分析の実施	45	31	68.9	11	24.4	2	4.4	1	2.2
システム監査の実施	69	45	65.2	14	20.3	9	13.0	1	1.4
情報セキュリティ教育の実施	55	43	78.2	9	16.4	3	5.5	0	0.0
情報セキュリティ体制の確立	94	66	70.2	18	19.1	9	9.6	1	1.1
情報ｾｷｭﾘﾃｨｱﾄﾞﾐﾆｽﾄﾚｰﾀの確保	3	2	66.7	1	33.3	0	0.0	0	0.0
情報資産の洗い出し	26	19	73.1	5	19.2	2	7.7	0	0.0
ＩＳＭＳの取得	18	14	77.8	2	11.1	2	11.1	0	0.0
プライバシーマークの取得	19	15	78.9	3	15.8	1	5.3	0	0.0
その他	4	3	75.0	1	25.0	0	0.0	0	0.0
特に実施していない	2	0	0.0	1	50.0	1	50.0	0	0.0
無回答	2	1	50.0	0	0.0	1	50.0	0	0.0
計	363	259	71.3	69	19.0	32	8.8	3	0.8

情報システムの安全性に対する投資も、前述の信頼性とほぼ同様の結果となった。今回気がつくのは、『情報セキュリティ教育の実施』の項目の回答数が前述の『Q42. 情報システムの信頼性を高めるためにもっと投資』よりも増えていることである。安全性に対しては、教育も有効な手段であり、そのためには投資すべきであるという監査担当部門の考え方が現れている。

×Q48. 情報システムの効率性を高めるための投資の必要性

効率性のための投資の必要性 / 情報セキュリティ対策	回答件数	思う		思わない		わからない		無回答	
情報セキュリティ対策コストの確保	26	22	84.6	1	3.8	3	11.5	0	0.0
リスク分析の実施	45	30	66.7	9	20.0	5	11.1	1	2.2
システム監査の実施	69	44	63.8	14	20.3	10	14.5	1	1.4
情報セキュリティ教育の実施	55	37	67.3	12	21.8	6	10.9	0	0.0
情報セキュリティ体制の確立	94	71	75.5	13	13.8	9	9.6	1	1.1
情報ｾｷｭﾘﾃｨｱﾄﾞﾐﾆｽﾄﾚｰﾀの確保	3	1	33.3	1	33.3	1	33.3	0	0.0
情報資産の洗い出し	26	20	76.9	3	11.5	3	11.5	0	0.0
ＩＳＭＳの取得	18	14	77.8	2	11.1	2	11.1	0	0.0
プライバシーマークの取得	19	15	78.9	4	21.1	0	0.0	0	0.0
その他	4	4	100.0	0	0.0	0	0.0	0	0.0
特に実施していない	2	1	50.0	0	0.0	1	50.0	0	0.0
無回答	2	0	0.0	0	0.0	2	100.0	0	0.0
計	363	259	71.3	59	16.3	42	11.6	3	0.8

信頼性・安全性・効率性の３つについて投資意欲を見てきたが、この効率性の項目が一番投資意欲が高かった。効率性は各事業体が追求する重要なファクタであり、そのための投資意欲も高い。傾向的には、前述の『Q42. 情報システムの信頼性を高めるためにもっと投資』とほぼ同様の回答結果となった。

7.『Q67. 電子メール利用ルールの策定状況』のクロス集計

×Q10. コンピュータ不正アクセス対策基準でのシステム監査の位置づけの認知度

システム監査の位置づけ / 電子メール利用ルールの策定状況	回答件数	知っている		知らない		無回答	
定めている	193	146	75.6	44	22.8	3	1.6
現在作成中である	17	12	70.6	5	29.4	0	0.0
作成を検討している	46	27	58.7	19	41.3	0	0.0
現在、定める予定がない	33	17	51.5	16	48.5	0	0.0
わからない	10	5	50.0	5	50.0	0	0.0
電子メールを利用していない	3	1	33.3	2	66.7	0	0.0
無回答	1	1	100.0	0	0.0	0	0.0
計	303	209	69.0	91	30.0	3	1.0

ここでは、『電子メール利用ルールの策定状況』と『コンピュータ不正アクセス対策基準』にシステム監査が位置づけられていることの認知度を比較した。やはり、電子メールルールを作成する際にこの対策基準を参考にした事業体も多く、認知度は高かった。特に、ルールを定める予定のない事業体でも、半数以上が「コンピュータ不正アクセス対策基準」にシステム監査が位置づけられることを知っており、コンピュータの不正アクセスやコンピュータウイルスなどに対する関心の高さを伺い知ることができる。

×Q７.「コンピュータウイルス対策基準」の認知度

コンピュータウイルス対策基準の認知度 / 電子メール利用ルールの策定状況	回答件数	利用したことがある		内容は知っているが利用したことはない		存在だけは知っている		知らない		無回答	
定めている	280	70	25.0	60	21.4	71	25.4	76	27.1	3	1.1
現在作成中である	23	1	4.3	8	34.8	9	39.1	5	21.7	0	0.0
作成を検討している	63	7	11.1	8	12.7	33	52.4	15	23.8	0	0.0
現在、定める予定がない	64	4	6.3	7	10.9	26	40.6	26	40.6	1	1.6
わからない	29	0	0.0	3	10.3	7	24.1	18	62.1	1	3.4
電子メールを利用していない	6	0	0.0	1	16.7	1	16.7	4	66.7	0	0.0
無回答	9	1	11.1	0	0.0	0	0.0	7	77.8	1	11.1
計	474	83	17.5	87	18.4	147	31.0	151	31.9	6	1.3

コンピュータウイルス対策基準は前述の不正アクセスに比べ、認知度（特に利用度）が低いように感じる。これは、コンピュータウイルス対策がウイルスソフトの導入と新規ウイルスへの対策に主眼が置かれているためである。対策基準は、どちらかといえば注意すべき留意事項が記述されており、事業体としては、新規ウイルス対策ソフトのアップデートやクライアントへの配布方法などもっと実践的な内容を欲している。それが全体として対策基準の利用状況を低下させている（20%以下）理由となっている。

8.『Q72. 電子メール利用の監査の実施状況』のクロス集計

Q17. システム監査の実施状況

システム監査の実施 / 電子メール利用監査の実施	回答件数	ある		ない	
ある	41	33	80.5	8	19.5
ない	417	146	35.0	271	65.0
無回答	1	0	0.0	1	100.0
計	459	179	39.0	280	61.0

電子メールが正しく使用されているかどうかを監査している事業体が意外に少ないことがこの結果からわかる。システム監査を実施した179事業体に対し、電子メールの利用状況を確認した事業体は33企業（18.4%）にすぎない。この原因として想定できるのは、電子メールを重要な情報システムとして位置づけていないか、または電子メール管轄部署が情報システム部門以外の部門である場合が想定される。

電子メールは、実業務ではなくてはならないツールであり、ウイルスの混入や事業体もしくは個人情報の漏洩は重大な問題となる。電子メールシステムを情報システム部門で管理している場合は、ぜひとも監査項目に加えるべきである。

また、電子メールの管轄部署が総務部などの情報システム部門以外である場合は、監査項目から抜け落ちやすい。しかし、メールで外部とデータのやりとりを行い、そこで使用した媒体をそのまま情報システムで使用しているケースが見受けられる。いくら情報システムでさまざまな対策を講じていても、簡単にウイルスが情報システムに混入したり、機密データが社外に漏洩することになる。情報システム部門の管轄外であっても、管理部門と協力しながら電子メール監査を行うことをお勧めする。組織防衛には全社一丸となった協力体制が必要である。

3.3.3　被監査部門対象

1．『Q18. システム監査実施方式』のクロス集計

×Q38. 最も効果的と思われるシステム監査実施者

システム監査実施者 / 監査実施方式	回答件数	監査役		内部の監査人		情報システム部門の要員		システム監査技術者試験合格者		監査法人・公認会計士	
内部監査部門型	106	8	7.5	27	25.5	1	0.9	12	11.3	25	23.6
外部委託型	98	2	2.0	13	13.3	1	1.0	10	10.2	28	28.6
無回答	3	0	0.0	1	33.3	0	0.0	0	0.0	1	33.3
計	207	10	4.8	41	19.8	2	1.0	22	10.6	54	26.1

システム監査実施者 / 監査実施方式	システム監査企業台帳に基づくシステム監査企業		その他		無回答	
内部監査部門型	28	26.4	4	3.8	1	0.9
外部委託型	40	40.8	1	1.0	3	3.1
無回答	1	33.3	0	0.0	0	0.0
計	69	33.3	5	2.4	4	1.9

被監査部門が理想とする監査人と実際との差異について考察してみた。最も効果的と思われるシステム監査実施者として『システム監査企業台帳に基づくシステム監査企業』の回答が多く、実際、『外部委託型』による40事業体が回答していることから、現状にも満足している様子がわかる。

『内部の監査人』を効果的とした事業体のうち、27事業体が『内部監査型』でシステム監査を行っていることから、内部の監査人もかなり効果をあげている状況が見受けられる。一方、内部監査型の事業体のうち、有効な監査人を『システム監査企業台帳に基づくシステム監査企業』および『監査法人・公認会計士』を選択した事業体の被監査部門は、内部監査での限界を感じていると推察される。内部監査人の監査技術の向上が必要であり、外部セミナーの参加などによるスキルアップも一つの手段である。

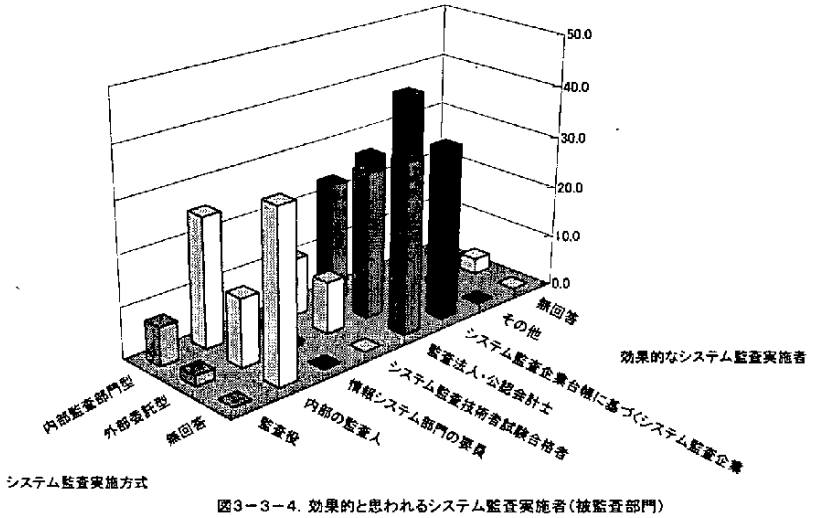

図3－3－4. 効果的と思われるシステム監査実施者（被監査部門）

2．『Q28. 監査報告書の指摘事項・改善勧告内容の妥当性』のクロス集計

×Q22. システム監査人の問題点

システム監査人の問題点 / 指摘事項・改善勧告内容	回答件数	監査人の権限および役割分担が不明確		現場（被監査部門）とのｺﾐｭﾆｹｰｼｮﾝ能力不足		監査人の監査対象業務に関する知識不足		監査人の情報システムに関する知識不足		監査人の洞察力・判断力の問題	
妥当だと思う	5	1	20.0	0	0.0	1	20.0	2	40.0	0	0.0
一部妥当だと思う	13	2	15.4	2	15.4	2	15.4	3	23.1	1	7.7
妥当だと思わない	0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
計	18	3	16.7	2	11.1	3	16.7	5	27.8	1	5.6

システム監査人の問題点 / 指摘事項・改善勧告内容	その他		複数回答	
妥当だと思う	0	0.0	1	20.0
一部妥当だと思う	1	7.7	2	15.0
妥当だと思わない	0	0.0	0	0.0
計	1	5.6	3	17.0

監査人に対する問題点を指摘した被監査部門の監査結果に対する評価を分析してみた。数は少ないが、やはり監査報告書の指摘事項／改善勧告内容に対し、同意し得ない結果を残している。これは原因が等分化されており、問題点を指摘できないが、監査人の業務知識とスキルの不足や被監査部門の説明不足に原因があると推察される。監査人と被監査部門が指摘事項／改善勧告の内容をよく話しあい、お互い合意した上で報告書に記述する必要がある。

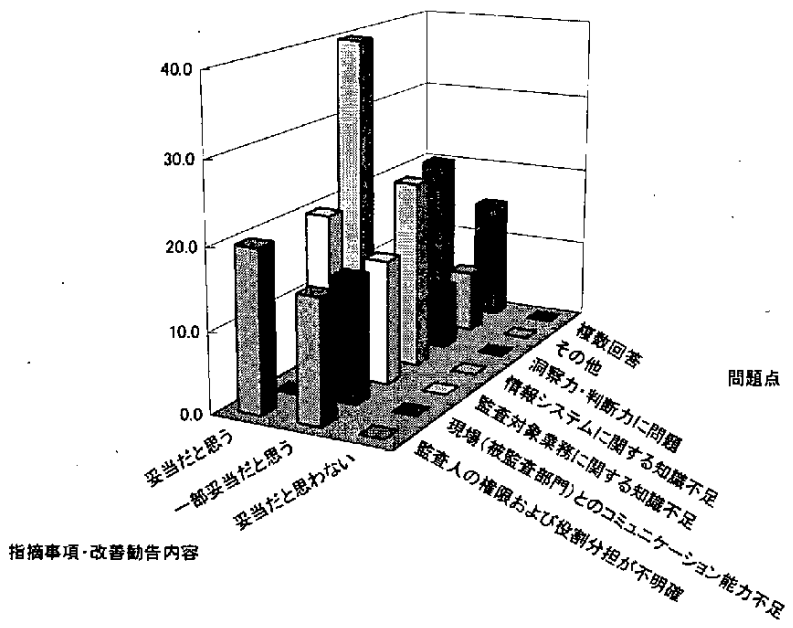

図3－3－5. システム監査人の問題点（被監査部門）

×Q23. システム監査を受けた時の現場の負担

現場の負担 / 指摘事項・改善勧告内容	回答件数	負担はなかった		負担は多少あったが、通常業務に支障をきたすほどではなかった		通常業務に支障をきたした		その他		無回答	
妥当だと思う	117	11	9.4	96	82.1	9	7.7	0	0.0	1	0.9
一部妥当だと思う	54	4	7.4	44	81.5	3	5.6	1	1.9	2	3.7
妥当だと思わない	2	0	0.0	2	100.0	0	0.0	0	0.0	0	0.0
無回答	5	0	0.0	4	80.0	0	0.0	0	0.0	1	20.0
計	178	15	8.4	146	82.0	12	6.7	1	0.6	4	2.2

このクロス分析では、被監査部門が業務の忙しさとの兼ね合いで十分監査人と意思疎通ができたかを分析した。結果としては、ほとんどの事業体の被監査部門（60.1%）が業務に支障をきたすことなく監査報告書の指摘事項／改善勧告の内容を受け入れている。被監査部門がシステム監査を何度も経験し、余裕を持って対応している状況にあると考えられる。通常業務に支障をきたした被監査部門は、システム監査をあまり経験していないか、監査方法が変わった（たとえば内部監査型から外部監査型に方式が変更になった）ことなどが理由として考えられる。これも経験を積むことにより解消されていくと考えられる。

×Q24. システム監査実施上の問題点

実施上の問題点 / 指摘事項・改善勧告内容	回答件数	システム監査計画に無理があった		システム監査方法が現場を無視したものであった		ｼｽﾃﾑ監査人へ提出すべき資料を整理していなかった		資料提出や意見聴取の指示が不明確		資料要求が多すぎた		現場の説明がｼｽﾃﾑ監査人に理解されなかった	
妥当だと思う	117	2	1.7	0	0.0	14	12.0	6	5.1	10	8.5	3	2.6
一部妥当だと思う	54	2	3.7	2	3.7	10	18.5	3	5.6	4	7.4	5	9.3
妥当だと思わない	2	0	0.0	0	0.0	0	0.0	1	50.0	0	0.0	0	0.0
無回答	5	0	0.0	0	0.0	0	0.0	1	20.0	0	0.0	0	0.0.
計	178	4	2.2	2	1.1	24	13.5	11	6.2	14	7.9	8	4.5

実施上の問題点 / 指摘事項・改善勧告内容	監査プログラムの使用のために現場に負担がかかった		実地調査が多すぎた		その他		特に問題は感じなかった		無回答		複数回答	
妥当だと思う	2	1.7	1	0.9	1	0.9	70	59.8	3	2.6	5	4.0
一部妥当だと思う	1	1.9	0	0.0	2	3.7	22	40.7	3	5.6	0	0.0
妥当だと思わない	0	0.0	0	0.0	0	0.0	1	50.0	0	0.0	0	0.0
無回答	0	0.0	0	0.0	0	0.0	3	60.0	1	20.0	0	0.0
計	3	1.7	1	0.6	3	1.7	96	53.9	7	3.9	5	3.0

当分析では、システム監査実施時の問題点とこの問題点が被監査部門に監査報告書の指摘事項／改善勧告内容が受け入れられない起因となっているかどうかの状況を分析を行った。監査報告の一部もしくは大部分に異議を唱えた被監査部門のうち、監査時の状況についての問題点については『特に問題は感じなかった』と回答したのは23社あり、システム監査の進行そのものは問題なく進められている事業体が多いことがわかる。また、選択肢第2位の『システム監査人へ提出すべき資料を整理していなかった』の10社についても自らの反省点を述べているものであり、監査人側に問題はなかったと思われる。一部回答に監査計画や推進方法に問題を残した事業体もあったが、全体を通してうまく監査されている。

×Q25. システム監査人と被監査部門による講評会の実施

講評会の実施 / 指摘事項・改善勧告内容	回答件数	行われた		行われなかった		無回答	
妥当だと思う	117	104	88.9	12	10.3	1	0.9
一部妥当だと思う	54	42	77.8	10	18.5	2	3.7
妥当だと思わない	2	1	50.0	1	50.0	0	0.0
無回答	5	3	60.0	0	0.0	2	40.0
計	178	150	84.3	23	12.9	5	2.8

システム監査における講評会は、監査人と被監査部門が出席し、指摘事項および改善勧告について両者が合意の上、監査報告書に記載するのが原則である。この分析では、被監査部門出席の下での講評会が開催されなかった場合に、監査報告書の内容を受諾に差異が発生するかを分析した。全体の84.3%の企業において被監査部門との講評会が行なわれており、講評会が行なわれた事業体において監査結果に対し、不満を持った被監査部門は43社、28.7%であった。

一方、講評会が開かれず、監査結果に不満を持った被監査部門は11社、47.8%にも及んだ。やはり講評会において監査人と被監査部門が問題点について、お互いに意識を共有することが、被監査部門に改善を促し、システム監査をより有効なものとすることができることが、この結果から明確となった。

3．『Q37．システム監査で充実すべき点』のクロス集計

×Q22．システム監査人の問題点

システム監査人の問題点 / 充実すべき点	回答件数	監査人の権限および役割分担が不明確		現場（被監査部門）とのコミュニケーション能力不足		監査人の監査対象業務に関する知識不足		監査人の情報システムに関する知識不足		監査人の洞察力・判断力の問題	
監査計画	5	1	20.0	0	0.0	0	0.0	3	60.0	0	0.0
事前調査	1	0	0.0	1	100.0	0	0.0	0	0.0	0	0.0
実地調査	2	0	0.0	0	0.0	1	50.0	1	50.0	0	0.0
改善勧告内容	3	1	33.3	1	33.3	0	0.0	0	0.0	0	0.0
監査報告会	4	1	25.0	0	0.0	2	50.0	1	25.0	0	0.0
チェックリスト	2	0	0.0	0	0.0	0	0.0	0	0.0	1	50.0
その他	1	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
無回答	0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
複数回答	0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
計	18	3	16.7	2	11.1	3	16.7	5	27.8	1	5.6

システム監査人の問題点 / 充実すべき点	その他		複数回答	
監査計画	0	0.0	1	20.0
事前調査	0	0.0	0	0.0
実地調査	0	0.0	0	0.0
改善勧告内容	0	0.0	1	33.0
監査報告会	0	0.0	0	0.0
チェックリスト	0	0.0	1	50.0
その他	1	100.0	0	0.0
無回答	0	0.0	0	0.0
複数回答	0	0.0	0	0.0
計	1	5.6	3	17.0

受審したシステム監査に問題ありとした被監査部門が、システム監査のどの部分を充実すべきと考えているかを分析した。喜ばしいことに、『問題あり』とした被監査部門が少ないため、十分な分析には至らなかった。重複回答があった問題点として『監査人の情報システムに関する知識不足』を挙げている被監査部門が充実すべきと考えているのは、『監査計画』３件、『実地調査』１件、『監査報告会』１件の計５件であった。また、『監査人の監査対象業務に関する知識不足』を挙げている被監査部門では、『実地調査』１件、『監査報告会』２件の計３件であった。『問題あり』とした被監査部門のうち、『実地調査』、『監査報告会』を充実すべきとの意見が出た理由として、監査人が業務や情報システムを十分理解していなかったために、被監査部門として監査結果に十分満足できなかったことが推定できる。また、『監査計画』を充実すべきと回答した被監査部門は、該当情報システムに対する監査人の認識誤りが監査計画の時点に遡ると考えているためと推定できる。

×Q26. 監査報告書の作成後に関係者を含めた監査報告会の実施状況

監査報告会の実施 / 充実すべき点	回答件数	行われた		行われなかった		無回答	
監査計画	42	31	73.8	10	23.8	1	2.4
事前調査	19	15	78.9	4	21.1	0	0.0
実地調査	32	20	62.5	12	37.5	0	0.0
改善勧告内容	32	24	75.0	7	21.9	1	3.1
監査報告会	14	9	64.3	5	35.7	0	0.0
チェックリスト	32	21	65.6	9	28.1	2	6.3
その他	1	1	100.0	0	0.0	0	0.0
無回答	5	2	40.0	2	40.0	1	20.0
複数回答	1	0	0.0	1	100.0	0	0.0
計	178	123	69.1	50	28.1	5	2.8

ここでは、監査報告会開催の有無と被監査部門がシステム監査で充実すべきと考えている点との相関関係を分析した。想定どおり監査報告会の充実では、監査報告会開催の有無により意見が分かれた。報告会が実施された被監査部門では、監査報告会の充実を求める意見が、7.3%に過ぎなかったが、報告会未開催の被監査部門では、全体の 10 に増加して 10.0%に増加しており、監査報告会のあり方が被監査部門におけるシステム監査の充実に結びつくと思われる。

×Q27. 監査報告会への情報システム部門からの出席状況

監査報告会への出席 / 充実すべき点	回答件数	した		しない		無回答	
監査計画	31	27	87.1	3	9.7	1	3.2
事前調査	15	12	80.0	3	20.0	0	0.0
実地調査	20	18	90.0	2	10.0	0	0.0
改善勧告内容	24	22	91.7	2	8.3	0	0.0
監査報告会	9	8	88.9	1	11.1	0	0.0
チェックリスト	21	20	95.2	1	4.8	0	0.0
その他	1	1	100.0	0	0.0	0	0.0
無回答	2	2	100.0	0	0.0	0	0.0
計	123	110	89.4	12	9.8	1	0.8

この分析では、情報システム部門の監査報告会への出席の有無とシステム監査で充実すべき項目の差異について考察した。特徴的な事象として情報システム部門が監査報告会に出席した場合は、チェックリストを充実すべき項目として挙げている被監査部門が多くなっている（出席時：

18.1%、未出席時：8.3%)。これは、おそらく監査報告会で監査人の報告を聞き、初めて監査時の質問の意味を理解したケースがあったことを意味していると推察した。監査時に監査人からの質問意図を誤って捉え、正しく回答ができなかったことへの不満の現れである。被監査部門や関係部門が監査報告会に出席することは、誤認に対する弁明を認め、正しい監査結果を導くことに多いに役立つ。被監査部門や関係部門出席の下での監査報告会開催を推奨したい。

4.『Q39. 情報セキュリティポリシー策定状況』のクロス集計

×Q44. 電子メール利用のルールの策定状況

セキュリティポリシー策定状況＼電子メール利用ルール策定状況	回答件数	定めている		現在作成中である		作成を検討している		現在、定める予定がない		わからない	
定めている	223	174	78.0	8	3.6	18	8.1	15	6.7	0	0.0
現在作成中である	141	88	62.4	22	15.6	21	14.9	7	5.0	1	0.7
作成を検討している	167	84	50.3	9	5.4	41	24.6	27	16.2	1	0.6
現在、定める予定がない	108	35	32.4	0	0.0	13	12.0	49	45.4	4	3.7
無回答	10	3	30.0	0	0.0	2	20.0	3	30.0	0	0.0
計	649	384	59.2	39	6.0	95	14.6	101	15.6	6	0.9

セキュリティポリシー策定状況＼電子メール利用ルール策定状況	電子メールを利用していない		無回答	
定めている	3	1.3	5	2.2
現在作成中である	2	1.4	0	0.0
作成を検討している	3	1.8	2	1.2
現在、定める予定がない	5	4.6	2	1.9
無回答	0	0.0	2	20.0
計	13	2.0	11	1.7

ここでは『電子メール利用ルールの策定状況』と『情報セキュリティポリシーの策定状況』を分析している。回答した被監査部門では、電子メール利用ルールと情報セキュリティポリシーの両方を定めている事業体が多く、現在作成中のところも含めると実に 45.0%の事業体が両方のルールを制定している。自事業体の情報システムや電子メール保全に対する意識の高さの現れである。

なお、情報セキュリティポリシーは制定せず、電子メール利用ルールのみを定めている事業体（制定中も含む）は、128 件、19.7%となる。一方、情報セキュリティポリシーのみを定めている事業体は、策定中も含め 61 件、9.4%であり、電子メール利用ルールのみを定めた事業体の約半数となる。この傾向の違いは、事業体における電子メールの利用がより身近なものとなり、利用事業体がルールを定める必要に迫られたためと推察できる。

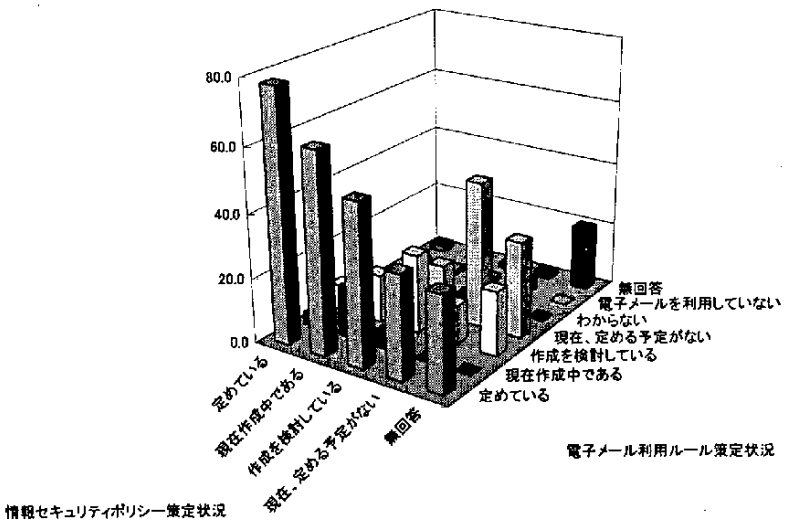

図3－3－6. 電子メール利用ルールの策定状況(被監査部門)

5.『Q40. 情報セキュリティ体制の推進』のクロス集計

×Q18. システム監査の実施方式

システム監査実施方式 / 情報セキュリティ体制	回答件数	内部監査部門型		外部委託型		無回答	
情報セキュリティ担当役員の設置	49	39	79.6	23	46.9	0	0.0
情報セキュリティ委員会の設置	60	51	85.0	24	40.0	1	1.7
情報システム部門主導で実施	98	50	51.0	58	59.2	2	2.0
情報セキュリティ専任者を設置	38	32	84.2	15	39.5	1	2.6
各部門・拠点にセキュリティ担当者を設置	58	47	81.0	28	48.3	0	0.0
外部のセキュリティコンサルタントを活用	17	10	58.8	12	70.6	0	0.0
特に実施していない	13	4	30.8	9	69.2	0	0.0
その他	5	4	80.0	3	60.0	0	0.0
無回答	3	1	33.3	2	66.7	0	0.0
計	341	238	69.8	174	51.0	4	1.2

ここでは、監査と情報セキュリティの体制について考察した。各事業体からの回答のとして、情報セキュリティは『情報システム部門主導で実施』あるいは『各部門・拠点にセキュリティ担当者を設置』し、システム監査は外部に委託するタイプが最も多かった（25.2%）。この回答を含め、情報セキュリティ体制を事業体内部で実施し、システム監査を外部委託している事業体は、148 社、43.4%に及ぶ。システム監査は監査結果の客観性や事業体内部で十分に準備工数や監査人が確保できないために外部委託とし、自らの情報を守る体制は自らで構築するという傾向が強いことがわかる。一方、情報セキュリティ体制に外部コンサルタントを活用し、システム監査を内部監査部門型にしているのは、10 社、2.9%にすぎない。

付属資料

「システム監査普及状況調査」アンケート様式

監査担当部門対象

5

(財)日本情報処理開発協会

2003-2004年版　システム監査白書資料

「システム監査」普及状況調査（Ⅰ）

貴社名（または団体名）			
所　在　地	〒　Tel　－　－ 内線		6
ご回答者役職名		ご芳名	
資本金（非営利法人においては、基金、出資金等）	7 千億 百億 十億 億 千万 百万 12 円		
従業員数（学校の場合は常勤教員数、病院の場合は病床数、官庁の場合は関係庁部所の定員数をご記入下さい。）	13 十万 万 千 百 十 18 人		

◇　本調査におきましては、機密を厳守し、個別データは絶対に公表いたしません。

◇　ご回答者に関する事項（氏名、所属等）については、本調査に関わる目的外では使用いたしません。

◇　ご回答賜りました事業体には、全体の集計結果を後日お送り申し上げます。

◇　なお、ご回答は、当該項目の番号に○印をお付けいただくか、もしくは記入欄にご記入いただく方式です。選択肢に「その他」とある場合は、具体的に記述して下さい。

◇　ご回答は平成14年12月10日までにお願いいたします。

業　種 19,20　**複数業種に関連する場合は、主力業種1つのみ○印をつけて下さい。**

1	農・林・漁・狩猟・水産養殖業	16	電気機械器具製造業	31	広告・調査・情報提供サービス業
2	鉱業	17	輸送用機械器具製造業	32	情報処理サービス業・ソフトウェア業（注1）
4	建設業	18	精密機械器具製造業	33	医療業（注2）
5	食品製造業	19	その他の製造業	34	宗教法人
6	繊維工業	21	卸業・商社	35	高校
7	紙・パルプ・紙加工品製造業	22	小売業	36	大学
8	新聞業・出版業	23	金融業	37	その他の教育機関
9	印刷業・同関連産業	24	証券業・商品取引業	38	学術研究機関
10	化学工業	25	生命保険業（含代理業・サービス業）	39	法人団体・農協
11	石油製品製造業	26	損害保険業（含代理業・サービス業）	40	その他のサービス業
12	窯業・土石製品製造業	27	不動産業	42	政府
13	鉄鋼業	28	運輸・通信・倉庫業	43	地方公共団体
14	非鉄金属製造業・金属製品製造業	29	電力・ガス事業		
15	一般機械器具製造業	30	放送業		

（注1）「情報処理サービス業・ソフトウェア業」では、コンピュータを利用して、情報の処理、加工等のサービスを行なうものおよびコンピュータのソフトウェア開発を行なうものをいいますが、本調査ではこれらの業務量が年間事業収入の50%以上あるもののみに限定します。

（注2）「医療業」：病院などで、その管轄が政府、地方公共団体、大学、組合などであっても、その管轄主体の分類に入れず、この医療業に入れて下さい。

21 A

本調査に関するお問い合わせ

財団法人　日本情報処理開発協会　情報セキュリティ部
（システム監査普及状況調査担当）

〒105-0011　東京都港区芝公園3－5－8　機械振興会館
TEL：03-3432-9387

Ⅰ システム監査一般について

Q1. 経済産業省から「システム監査基準」(平成8年改訂)が公表されていることを知っていますか。

22		
	1	利用したことがある
	2	内容は知っているが、利用したことはない
	3	存在だけは知っている
	4	知らない

Q2. 経済産業省の「システム監査企業台帳制度」(平成3年)を知っていますか。

23		
	1	知っている
	2	知らない →Q4へ

Q3. システム監査を外部の企業に委託する場合「システム監査企業台帳」を参考にしたいと思いますか。

24		
	1	参考にしたことがある
	2	今後参考にしたいと思う
	3	参考にしたいと思わない

Q4. 経済産業省の情報処理技術者試験制度で行われている「システム監査技術者試験」を知っていますか。

25		
	1	知っている
	2	知らない

Q5. 経済産業省から「情報システム安全対策基準」(平成7年改訂)が公表されていることを知っていますか。

26		
	1	利用したことがある
	2	内容は知っているが、利用したことはない
	3	存在だけは知っている
	4	知らない →Q7へ

Q6. 「情報システム安全対策基準」の中でシステム監査が位置づけられていることを知っていますか。

27		
	1	知っている
	2	知らない

Q7. 経済産業省から「コンピュータウイルス対策基準」(平成7年改訂)が公表されていることを知っていますか。

28		
	1	利用したことがある
	2	内容は知っているが、利用したことはない
	3	存在だけは知っている
	4	知らない →Q9へ

Q8. 「コンピュータウイルス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

29		
	1	知っている
	2	知らない

Q9. 経済産業省から「コンピュータ不正アクセス対策基準」(平成8年)が公表されていることを知っていますか。

30		
	1	利用したことがある
	2	内容は知っているが、利用したことはない
	3	存在だけは知っている
	4	知らない →Q11へ

(注)システム監査とは次のように定義します。
監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検および評価し、組織体の長に助言および勧告するとともにフォローアップする一連の活動

Q10.「コンピュータ不正アクセス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

31

1	知っている
2	知らない

Q11. プライバシーマーク制度を知っていますか。

32

1	知っている
2	知らない

Q12. ISMS(情報セキュリティマネジメントシステム)適合性評価制度を知っていますか。

33

1	知っている
2	知らない

34 B

Ⅱ 貴事業体の監査体制について

Q13. 貴社には内部監査部門(監査部、検査部等)が設置されていますか。

35

1	い る
2	いない

Q13-1. 内部監査人は何人いますか。

36 [　　] 人

Q13-2. 内部監査人は平均何歳ですか。(端数切捨て)

39 [　　] 歳

Q14. 貴社にはシステム監査人(システム監査の担当者)がいますか。

41

1	い る
2	いない

Q14-1. システム監査人は何人ですか。

42 [　　] 人

Q14-2. システム監査人は平均何歳ですか。(端数切り捨て)

45 [　　] 歳

Q14-3. システム監査人を置いたのはいつですか。(西暦でお答え下さい)

47 [　　] 年

Q15. 貴社にはシステム監査技術者試験の合格者がいますか。(所属部門は問いません)

51

1	い る
2	いない

→Q17へ

Q15-1. 何人の合格者がいますか。

52 [　　] 人

Q16. 合格者はどこに所属していますか。(複数回答)

55	1	内部監査部門
56	2	情報システム部門
57	3	その他

Q17. 貴社ではシステム監査を実施したことがありますか。

58

1	あ る
2	な い

→Q57へ

59 C

Q18. システム監査の実施に関する規程が定められていますか。

60	1	定められている
	2	他の社内規程でシステム監査の実施が明記されている
	3	定められていない

Q19. システム監査の実施において問題がありましたか。最も問題だと思われるものを1つ選んで下さい。

61	1	トップマネジメントのサポートが得られない
	2	システム監査人が不足している
	3	システム監査の実施に関する規程が整備されていない
	4	システム監査のチェックリストが整備されていない
	5	利用できるシステム監査技法が少ない
	6	被監査部門の協力が得られない
	7	委託先のシステム監査企業の実施内容が期待どおりでなかった
	8	その他(具体的に書いて下さい:　　)
	9	問題はない

Q20. システム監査は誰が実施するのが効果的だと思いますか。最も効果的と思うものを1つ選んで下さい。

62	1	監査役(団体等は監事、自治体は監査委員)
	2	内部の監査人
	3	情報システム部門の要員
	4	システム監査技術者試験の合格者
	5	監査法人・公認会計士
	6	システム監査企業台帳に基づくシステム監査企業
	7	その他(具体的に書いて下さい:　　)

Q21. システム監査を実施する際、どのような点を充実させなければならないと思いますか。最も重要と思うものを1つ選んで下さい。

63	1	監査計画
	2	事前調査
	3	実地調査
	4	改善勧告内容
	5	監査報告会
	6	チェックリスト
	7	その他(具体的に書いて下さい:　　)

Q22. 貴社ではシステム監査人は何人位必要だと思いますか。

64		人

Q23. システム監査人に最も不足していると思われる知識は何ですか。次の中から1つ選んで下さい。

67	1	経営に関する知識
	2	業務知識
	3	法律知識
	4	監査知識
	5	情報システムの知識
	6	その他(具体的に書いて下さい:　　)
	7	わからない

Q24. システム監査人に最も不足していると思われる能力は何ですか。次の中から1つ選んで下さい。

68	1	インタビュー能力
	2	分析能力
	3	判断能力
	4	報告書作成能力
	5	その他(具体的に書いて下さい:　　)
	6	わからない

Q25. システム監査人に対してどのような教育方法をとっていますか。主に行っているものを1つ選んで下さい。

69	1	外部セミナーを利用
	2	社内教育
	3	OJT
	4	通信教育
	5	その他(具体的に書いて下さい:　　)
	6	特に教育は実施していない
	7	監査を外部委託しているため該当しない

Q26. システム監査の対象はどのようにして決定していますか。(複数回答)

70	1	トップマネジメントの要求に基づいて決定
71	2	監査役(団体等は監事、自治体は監査委員)の要求に基づいて決定
72	3	内部監査部門長の判断に基づいて決定
73	4	システム監査人の独自の判断で決定
74	5	特定システムオペレーション(SO)企業認定制度に基づいて決定
75	6	プライバシーマーク制度の要求事項に基づいて決定
76	7	ISMS制度の要求事項に基づいて決定
77	8	その他(具体的に書いて下さい:　　)

Q27. 監査テーマはどのようにして決定していますか。(複数回答)

78	1	トップマネジメントの要求に基づいて決定
79	2	監査役(団体等は監事、自治体は監査委員)の要求に基づいて決定
80	3	内部監査部門の判断で決定
81	4	システム監査人の独自の判断で決定
82	5	各種認定制度等の要求事項に基づいて決定
83	6	その他(具体的に書いて下さい:　　)

Q28. システム監査の基本(年度)計画書を策定していますか。

84	1	い る	→Q30へ
	2	いない	

Q29. システム監査基本計画書を作成していない理由はなぜですか。(複数回答)

85	1	必要性がない
86	2	個別計画書だけで十分である
87	3	内部監査計画に含まれている
88	4	システム監査基本計画書作成のルールがない
89	5	外部に委託しているので作成していない
90	6	必要に応じてシステム監査を実施しているため、作成していない
91	7	その他(具体的に書いて下さい:　　)

Q30. システム監査を実施する場合、事前に被監査部門へ通知していますか。

92	1	い る
	2	いない

93 D

Ⅲ 平成13年度のシステム監査実施について

Q31. 平成13年度にシステム監査を実施しましたか。

94	1	し た	
	2	しない	→Q61へ

Q32. システム監査は次のどの方式で実施しましたか。(複数回答)

95	1	内部監査部門型(監査部、検査部等が実施)	→Q35へ
96	2	部門監査型(情報システム部門が実施)	
97	3	指名方式(トップから指名された者がシステム監査人となって実施)	
98	4	委員会方式(システム監査委員会を設置して実施)	
99	5	チームアプローチ(システム監査プロジェクチームを編成して実施)	
100	6	外部委託型(システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託)	→Q33へ
101	7	その他(具体的に書いて下さい:　　)	→Q35へ

Q33. (Q32で「6」を回答した場合)外部委託企業は、システム監査企業台帳登録企業ですか。

102	1	はい
	2	いいえ
	3	わからない

Q34. 外部委託の場合、どこが実施しましたか。

103	1	監査法人(公認会計士を含む)
	2	コンサルタント(個人／企業)
	3	情報処理サービス業者
	4	その他(具体的に書いて下さい:　　)

Q35. システム監査を実施した業務欄の数字に○をつけ、その業務について右欄の着眼点で最も重視した項目を1つ選んで下さい。(業務は複数回答)

	業務＼着眼点		安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性	
104	1	企画業務	1	2	3	4	5	6	7	8	108
105	2	開発業務	1	2	3	4	5	6	7	8	109
106	3	運用業務	1	2	3	4	5	6	7	8	110
107	4	保守業務	1	2	3	4	5	6	7	8	111

112 E

Q36. システム監査を実施したテーマ欄の数字に○をつけ、その業務について右欄の着眼点で最も重視した項目を1つ選んで下さい。(テーマは複数回答)

	テーマ＼着眼点		安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性	
113	1	ドキュメント管理	1	2	3	4	5	6	7	8	129
114	2	進捗管理	1	2	3	4	5	6	7	8	130
115	3	品質管理	1	2	3	4	5	6	7	8	131
116	4	コスト管理	1	2	3	4	5	6	7	8	132
117	5	要員管理	1	2	3	4	5	6	7	8	133
118	6	外部委託(開発の委託)	1	2	3	4	5	6	7	8	134
119	7	外部委託(アウトソーシング)	1	2	3	4	5	6	7	8	135
120	8	セキュリティ対策	1	2	3	4	5	6	7	8	136
121	9	ネットワーク管理	1	2	3	4	5	6	7	8	137
122	10	ソフトウェアの適正利用(ライセンス管理)	1	2	3	4	5	6	7	8	138
123	11	個人情報保護対策	1	2	3	4	5	6	7	8	139
124	12	PC管理、モバイル機器管理	1	2	3	4	5	6	7	8	140
125	13	コンピュータウイルス対策	1	2	3	4	5	6	7	8	141
126	14	情報システム関連のリスク管理	1	2	3	4	5	6	7	8	142
127	15	災害対策	1	2	3	4	5	6	7	8	143
128	16	その他(　　)	1	2	3	4	5	6	7	8	144

Q37. コンピュータ犯罪、ヒューマンエラー、事故、災害対策、個人情報保護の5項目について、防止ならびに早期発見の観点から、システム監査において特に重視すべき分野はどこだと思いますか。各項目ごとに最も重要と思われる分野(1～12)を1つだけ選んで下さい。

	分野＼項目	データの入力プロセス	データ処理プロセス	出力プロセス	プログラム変更	オペレーション	情報保管(データ管理)	入退室(館)管理	システム開発	ハードウェア *1	ソフトウェア *2	通信回線	電源設備
145	コンピュータ犯罪防止	1	2	3	4	5	6	7	8	9	10	11	12
147	ヒューマンエラー防止	1	2	3	4	5	6	7	8	9	10	11	12
149	事故防止	1	2	3	4	5	6	7	8	9	10	11	12
151	災害対策	1	2	3	4	5	6	7	8	9	10	11	12
153	個人情報保護	1	2	3	4	5	6	7	8	9	10	11	12

*1　CPUと周辺機器／*2　基本ソフトとアプリケーションソフト

155 F

Q38. システム監査を実施する際に、以下の基準等を利用しましたか。

		利用した	利用しない
156	システム監査基準	1	2
157	情報システム安全対策基準	1	2
158	コンピュータウイルス対策基準	1	2
159	コンピュータ不正アクセス対策基準	1	2
160	プライバシーマーク監査ガイドライン	1	2
161	ISMSガイド	1	2

Q39. システム監査において自社用のチェックリストを作成していますか。

162

1	い る
2	いない

Q40. 貴社の情報システムの信頼性は十分だと思いますか。

163

1	十分だと思う
2	やや十分だと思う
3	普通だと思う
4	やや不十分だと思う
5	不十分だと思う
6	わからない

Q41. 貴社の情報システムの信頼性を高めるために改善の余地があると思いますか。

164

1	思 う
2	思わない
3	わからない

Q42. 貴社の情報システムの信頼性を高めるためにもっと投資すべきだと思いますか。

165

1	思 う
2	思わない
3	わからない

Q43. 貴社の情報システムの安全性は十分だと思いますか。

166

1	十分だと思う
2	やや十分だと思う
3	普通だと思う
4	やや不十分だと思う
5	不十分だと思う
6	わからない

Q44. 貴社の情報システムの安全性を高めるために改善の余地があると思いますか。

167

1	思 う
2	思わない
3	わからない

Q45. 貴社の情報システムの安全性を高めるためにもっと投資すべきだと思いますか。

168

1	思 う
2	思わない
3	わからない

Q46. 貴社の情報システムの効率性は十分だと思いますか。

169

1	十分だと思う
2	やや十分だと思う
3	普通だと思う
4	やや不十分だと思う
5	不十分だと思う
6	わからない

Q47. 貴社の情報システムの効率性を高めるために改善の余地があると思いますか。

170	1	思 う
	2	思わない
	3	わからない

Q48. 貴社の情報システムの効率性を高めるためにもっと投資すべきだと思いますか。

171	1	思 う
	2	思わない
	3	わからない

Q49. 貴社の情報システムは、総合的に見て満足できる状態ですか。

172	1	十分満足
	2	満足
	3	なんともいえない
	4	多少不満
	5	大いに不満
	6	わからない

Q50. 監査結果について、情報システム部門との間での講評会(監査報告書を作成する前に意見交換、確認等を行うことをいう)を行いましたか。

173	1	行った
	2	行わなかった

Q51. 監査報告書の作成後に関係者を含めた監査報告会を行いましたか。

174	1	行った
	2	行わなかった

Q52. 監査報告会に出席したのは誰ですか。(複数回答)

175	1	最高経営者(会長、社長、知事、市長等)
176	2	財務担当役員
177	3	情報システム担当役員
178	4	監査役
179	5	情報システム部門の管理者
180	6	内部監査人
181	7	ユーザ部門の管理者
182	8	外部のシステム監査人
183	9	その他(具体的に書いて下さい:　　)

Q53. 監査報告書(原本)は誰に提出(報告書の宛先)しましたか。

注)複数部署に配布している場合は、その中で最高権限者を選んで下さい。

184	1	最高意思決定機関(取締役会、理事会、議会等)
	2	最高経営者(社長、理事長、首長等)
	3	担当役員
	4	監査役(団体等は監事、自治体は監査委員)
	5	内部監査部門長
	6	その他(具体的に書いて下さい:　　)

Q54. 監査報告書の写を被監査部門に配布しましたか。

185

1	した
2	しない

Q55. 監査報告書の写を監査役に配布しましたか。

186

1	した
2	しない

Q56. 監査報告書の写を貴社の会計監査人に配布しましたか。

187

1	した
2	しない

188 G

Ⅳ 未実施および実施可能性について

(Q57からQ60までは、Q17でシステム監査を実施していない企業のみお答え下さい)

Q57. システム監査を実施していない理由はどのような点ですか。次の中から主な理由を1つ選んで下さい。

189

1	システム監査についてトップマネジメントの認識が欠如している
2	システム監査の実施のためのコンセンサス、組織風土が十分に育っていない
3	システム監査の実施よりもシステム化推進そのものに力点がある
4	システム監査を実施する担当者(部門)の確保が難しい
5	システム監査の方法、制度、手続きなどが十分でない
6	システム監査の効果が明確でない
7	システム監査の必要性を感じない
8	その他(具体的に書いて下さい:　　)

Q58. 今後、システム監査についてどのように対応されますか。次の中から1つ選んで下さい。

190

1	現在、システム監査の導入を計画中
2	2～3年以内には導入の予定
3	当面導入の予定はない　→Q61へ
4	将来とも導入の予定はない　→Q61へ
5	その他(具体的に書いて下さい:　　)

Q59. どのような体制で進められる予定ですか。(複数回答)

191	1	内部監査部門型(監査部、検査部等が実施)
192	2	外部委託型(システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託)
193	3	決まっていない

Q60. 特にどのような観点から監査を進められる予定ですか。次の中から1つ選んで下さい。

194

1	安全性(システムの物理的安全性／不正防止)
2	信頼性(ハードウェア／ソフトウェアの正確さに基づく信頼性)
3	機密性(データの権限者以外への機密)
4	準拠性(法律、条例、規則等への準拠)
5	採算性(コスト面からの効率)
6	適時性(開発、導入、アウトプット作成等のタイミング)
7	生産性(リソース面からの効率)
8	効率性(システム目標の達成度合い)

195 H

V 情報セキュリティの推進について

Q61. 貴社では情報セキュリティポリシーを策定していますか。

196	1	定めている
	2	現在作成中である
	3	作成を検討している
	4	現在、定める予定がない

Q62. 貴社では情報セキュリティをどのような体制で推進していますか。(複数回答)

197	1	情報セキュリティ担当役員を設置している
198	2	情報セキュリティ委員会を設置している
199	3	情報システム部門主導で実施している
200	4	情報セキュリティ専任者を設置している
201	5	各部門・拠点にセキュリティ担当者を設置している
202	6	外部のセキュリティコンサルタントを活用している
203	7	特に実施していない
204	8	その他(具体的に書いて下さい:　　)

Q63. 情報セキュリティ推進体制で最も重要と思われることを1つだけ選んで下さい。

205	1	経営者のリーダーシップ
	2	全社的な推進体制
	3	情報システム部門の推進体制
	4	利用部門の理解・協力
	5	その他(具体的に書いて下さい:　　)

Q64. 貴社では情報セキュリティについて、優先的に実施しているものを3つまで選んで下さい。(複数回答)

206	1	情報セキュリティ対策コストの確保
208	2	リスク分析の実施
210	3	システム監査の実施
	4	情報セキュリティ教育の実施
	5	情報セキュリティ体制の確立
	6	情報セキュリティアドミニストレータの確保
	7	情報資産の洗い出し
	8	ISMSの取得
	9	プライバシーマークの取得
	10	その他(具体的に書いて下さい:　　)
	11	特に実施していない

Q65. 貴社では情報セキュリティについてどのような教育を実施していますか。(複数回答)

212	1	新入社員教育を実施している
213	2	一般社員向け教育を実施している
214	3	管理職教育を実施している
215	4	役員教育を実施している
216	5	派遣要員向け教育を実施している
217	6	情報セキュリティ担当者の専門教育を実施している
218	7	その他(具体的に書いて下さい:　　)
219	8	特に実施していない

Q66. 貴社では情報セキュリティポリシー監査を実施したことがありますか。

220

1	ある
2	ない

221 I

VI 電子メールの利用について

Q67. 電子メール利用のルールを定めていますか。

222

1	定めている	
2	現在作成中である	
3	作成を検討している	
4	現在、定める予定がない	
5	わからない	
6	電子メールを利用していない	→終了

Q68. 要員の電子メールの利用状況を監視していますか。

223

1	監視している	
2	今後、監視する予定がある	
3	監視していない	→Q70へ
4	わからない	→Q70へ

Q69. (Q68で「1」、「2」を回答した場合)電子メール利用状況の監視について、ルールを定めていますか。

224

1	ルールを定め、社員に周知している
2	ルールは定めているが、社員に周知していない
3	現在作成中である
4	作成を検討している
5	現在、定める予定がない
6	わからない

Q70. 自宅や出張先からメールサーバへのリモートアクセスを認めていますか。

225

1	認めている
2	許可制で認めている
3	認めていない
4	わからない

Q71. 自宅の個人アドレスへの社内メールの転送を認めていますか。

226

1	認めている
2	許可制で認めている
3	認めていない
4	わからない

Q72. 電子メールの利用に関して、監査を実施したことがありますか。

227

1	ある
2	ない

228 J

ご協力ありがとうございました

KEIRIN 00 このアンケートは競輪の補助を受けて実施しているものです。

被監査部門対象

5

(財)日本情報処理開発協会

2003-2004年版　システム監査白書資料

「システム監査」普及状況調査（II）

貴社名（または団体名）			
所　在　地	〒　　Tel　　－　　－ 内線		6
ご回答者役職名		ご芳名	
資本金（非営利法人においては、基金、出資金等）	7 千億 百億 十億 億 千万 百万 12 円		
従業員数（学校の場合は常勤教員数、病院の場合は病床数、官庁の場合は関係庁部所の定員数をご記入下さい。）	13 十万 万 千 百 十 18 人		

◇　本調査におきましては、機密を厳守し、個別データは絶対に公表いたしません。

◇　ご回答者に関する事項（氏名、所属等）については、本調査に関わる目的外では使用いたしません。

◇　ご回答賜りました事業体には、全体の集計結果を後日お送り申し上げます。

◇　なお、ご回答は、当該項目の番号に○印をお付けいただくか、もしくは記入欄にご記入いただく方式です。選択肢に「その他」とある場合は、具体的に記述して下さい。

◇　ご回答は平成14年12月10日までにお願いいたします。

業　種 19, 20　　複数業種に関連する場合は、主力業種1つのみ○印をつけて下さい。

1	農・林・漁・狩猟・水産養殖業	16	電気機械器具製造業	31	広告・調査・情報提供サービス業
2	鉱業	17	輸送用機械器具製造業	32	情報処理サービス業・ソフトウェア業（注1）
4	建設業	18	精密機械器具製造業	33	医療業（注2）
5	食品製造業	19	その他の製造業	34	宗教法人
6	繊維工業	21	卸業・商社	35	高校
7	紙・パルプ・紙加工品製造業	22	小売業	36	大学
8	新聞業・出版業	23	金融業	37	その他の教育機関
9	印刷業・同関連産業	24	証券業・商品取引業	38	学術研究機関
10	化学工業	25	生命保険業（含代理業・サービス業）	39	法人団体・農協
11	石油製品製造業	26	損害保険業（含代理業・サービス業）	40	その他のサービス業
12	窯業・土石製品製造業	27	不動産業	42	政府
13	鉄鋼業	28	運輸・通信・倉庫業	43	地方公共団体
14	非鉄金属製造業・金属製品製造業	29	電力・ガス事業		
15	一般機械器具製造業	30	放送業		

（注1）「情報処理サービス業・ソフトウェア業」では、コンピュータを利用して、情報の処理、加工等のサービスを行なうものおよびコンピュータのソフトウェア開発を行なうものをいいますが、本調査ではこれらの業務量が年間事業収入の50%以上あるもののみに限定します。

（注2）「医療業」：病院などで、その管轄が政府、地方公共団体、大学、組合などであっても、その管轄主体の分類に入れず、この医療業に入れて下さい。

21 A

本調査に関するお問い合わせ

財団法人．日本情報処理開発協会　情報セキュリティ部
（システム監査普及状況調査担当）

〒105-0011　東京都港区芝公園3-5-8　機械振興会館
TEL：03-3432-9387

I システム監査一般について

Q1. 経済産業省から「システム監査基準」(平成8年改訂)が公表されていることを知っていますか。

22

1	利用したことがある
2	内容は知っているが、利用したことはない
3	存在だけは知っている
4	知らない

Q2. 経済産業省の「システム監査企業台帳制度」(平成3年)を知っていますか。

23

1	知っている	
2	知らない	→Q4へ

Q3. システム監査を外部の企業に委託する場合「システム監査企業台帳」を参考にしたいと思いますか。

24

1	参考にしたことがある
2	今後参考にしたいと思う
3	参考にしたいと思わない

Q4. 経済産業省の情報処理技術者試験制度で行われている「システム監査技術者試験」を知っていますか。

25

1	知っている
2	知らない

Q5. 経済産業省から「情報システム安全対策基準」(平成7年改訂)が公表されていることを知っていますか。

26

1	利用したことがある	
2	内容は知っているが、利用したことはない	
3	存在だけは知っている	
4	知らない	→Q7へ

Q6. 「情報システム安全対策基準」の中でシステム監査が位置づけられていることを知っていますか。

27

1	知っている
2	知らない

Q7. 経済産業省から「コンピュータウイルス対策基準」(平成7年改訂)が公表されていることを知っていますか。

28

1	利用したことがある	
2	内容は知っているが、利用したことはない	
3	存在だけは知っている	
4	知らない	→Q9へ

(注)システム監査とは次のように定義します。
監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検および評価し、組織体の長に助言および勧告するとともにフォローアップする一連の活動

Q8.「コンピュータウイルス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

29

1	知っている
2	知らない

Q9. 経済産業省から「コンピュータ不正アクセス対策基準」(平成8年)が公表されていることを知っていますか。

30

1	利用したことがある
2	内容は知っているが、利用したことはない
3	存在だけは知っている
4	知らない

→Q11へ

Q10.「コンピュータ不正アクセス対策基準」の中でシステム監査が位置づけられていることを知っていますか。

31

1	知っている
2	知らない

Q11. プライバシーマーク制度を知っていますか。

32

1	知っている
2	知らない

Q12. ISMS(情報セキュリティマネジメントシステム)適合性評価制度を知っていますか。

33

1	知っている
2	知らない

34 B

Ⅱ　平成13年度のシステム監査実施について

Q13. 貴社にはシステム監査人がいますか。

35

1	い る
2	いない

Q14. 貴部門では、システム監査を受けたことがありますか。

36

1	あ る
2	な い

→Q34へ

Q15. 平成13年度にシステム監査を受けましたか。

37

1	受けた
2	受けない

→Q34へ

Q16. システム監査を受けたのはどの業務でしたか。(複数回答)

38	1	企画業務
39	2	開発業務
40	3	運用業務
41	4	保守業務

Q17. システム監査では、どのテーマを実施しましたか。(複数回答)

42	1	ドキュメント管理
43	2	進捗管理
44	3	品質管理
45	4	コスト管理
46	5	要員管理
47	6	外部委託(開発の委託)
48	7	外部委託(アウトソーシング)
49	8	セキュリティ対策
50	9	ネットワーク管理
51	10	ソフトウェアの適正利用(ライセンス管理)
52	11	個人情報保護対策
53	12	PC管理、モバイル機器管理
54	13	コンピュータウイルス対策
55	14	情報システム関連のリスク管理
56	15	災害対策
57	16	その他(具体的に書いて下さい:　　)

Q18. システム監査は次のどの方式で実施されましたか。(複数回答)

58	1	内部監査部門型(監査部、検査部等が実施)
59	2	外部委託型(システム監査企業台帳に基づくシステム監査企業やコンサルタント会社等へ委託)

(注)「1　内部監査部門型」のみ該当する場合はQ21へ、2つとも該当する場合はQ19に進んで下さい。

Q19. (Q18で「2」を回答した場合)外部委託企業は、システム監査企業台帳登録企業ですか。

60	1	はい
	2	いいえ
	3	わからない

Q20. 外部委託の場合、どこが実施しましたか。

61	1	監査法人(公認会計士を含む)
	2	コンサルタント(個人／企業)
	3	情報処理サービス業者
	4	その他(具体的に書いて下さい:　　)

Q21. システム監査を受けた結果、監査人に対してどのような印象をもちましたか。(単一回答)

62

1	問題があった	
2	十分満足できた	→Q23へ
3	特に問題はなかった	→Q23へ
4	わからない	→Q23へ

Q22. どのような点で問題があったと思いますか。最も問題と思った点を1つ選んで下さい。(単一回答)

63

1	監査人の権限および役割分担が不明確であった
2	現場(被監査部門)とのコミュニケーション能力が不足していた
3	監査人の監査対象業務に関する知識が不足していた
4	監査人の情報システムに関する知識が不足していた
5	監査人の洞察力・判断力に問題があった
6	その他(具体的に書いて下さい:　　)

Q23. システム監査を受けた時、現場の負担はありましたか。

64

1	負担はなかった
2	負担は多少あったが、通常業務に支障をきたすほどではなかった
3	通常業務に支障をきたした
4	その他(具体的に書いて下さい:　　)

Q24. システム監査を受けた結果どのような点が問題だと感じましたか。最も問題と感じたものを1つ選んで下さい。(単一回答)

65

1	システム監査計画に無理があった
2	システム監査方法が現場を無視したものであった
3	システム監査人へ提出すべき資料を整理していなかった
4	資料提出や意見聴取の指示が不明確であった
5	資料要求が多すぎた
6	現場の説明がシステム監査人に理解されなかった
7	監査プログラムの使用のために現場に負担がかかった
8	実地調査が多すぎた
9	その他(具体的に書いて下さい:　　)
10	特に問題は感じなかった

Q25. 監査結果について、システム監査人と貴部門との間で講評会(監査報告書を作成する前に意見交換、確認等を行うことをいう)が行われましたか。

67

1	行われた
2	行われなかった

Q26. 監査報告書の作成後に関係者を含めた監査報告会が行われましたか。

68	1	行われた
	2	行われなかった →Q28へ

Q27. 監査報告会に情報システム部門から出席しましたか。

69	1	した
	2	しない

Q28. 監査報告書の指摘事項や改善勧告の内容について妥当だと思いますか。

70	1	妥当だと思う
	2	一部妥当だと思う
	3	妥当だと思わない

Q29. 改善命令を受けましたか。

71	1	受けた
	2	受けない →Q31へ

Q30. 改善命令を受けて対策を実施しましたか。

72	1	実施した
	2	一部実施した
	3	実施していない

Q31. システム監査を受けた結果、被監査部門としては効果があったと思いますか。

73	1	効果があったと思う
	2	効果はなかったと思う →Q34へ
	3	どちらともいえない →Q34へ
	4	わからない →Q34へ

Q32. どのような点に効果があったと思いますか。最も効果があったと思うものを1つ選んで下さい。
（単一回答）

74	1	システムに起因する事故・障害が未然に防止できた
	2	リスク対策をどこまで考慮すればよいかが明らかになった
	3	担当者がリスクを考慮しながら業務を実行するようになった
	4	システム部門に対する過大な要求がなくなった
	5	システムの安全性向上対策のレベルが明らかになった
	6	システムの有効利用が促進された
	7	有効なシステムの開発設計が可能になった
	8	業務の継続性の確保が図られた
	9	要員が規定・ルール等を意識して業務を実行するようになった
	10	その他（具体的に書いて下さい：　　）

Q33. どのような点で最も改善が図れたと思いますか。最も改善が図れたと思うものを1つ選んで下さい。
（単一回答）

76	1	スケジュール管理の適正化
	2	コストの削減
	3	情報の保護対策の向上
	4	セキュリティ対策の向上
	5	生産性の向上
	6	品質管理の向上
	7	規則・手続き等の遵守
	8	ドキュメント類の整備
	9	作業環境の改善
	10	要員管理の適正化
	11	その他（具体的に書いて下さい：　　）

78 C

Ⅲ システム監査のあり方について

Q34. 各業務の監査で重視すべき着眼点は何ですか。各業務ごとにそれぞれ1つ選んで下さい。

業務＼着眼点	安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性
79 企画業務	1	2	3	4	5	6	7	8
80 開発業務	1	2	3	4	5	6	7	8
81 運用業務	1	2	3	4	5	6	7	8
82 保守業務	1	2	3	4	5	6	7	8

Q35. 各テーマの監査で重視すべき着眼点は何ですか。各テーマごとにそれぞれ1つ選んで下さい。

テーマ＼着眼点	安全性	信頼性	機密性	準拠性	採算性	適時性	生産性	効率性
83 ドキュメント管理	1	2	3	4	5	6	7	8
84 進捗管理	1	2	3	4	5	6	7	8
85 品質管理	1	2	3	4	5	6	7	8
86 コスト管理	1	2	3	4	5	6	7	8
87 要員管理	1	2	3	4	5	6	7	8
88 外部委託（開発の委託）	1	2	3	4	5	6	7	8
89 外部委託（アウトソーシング）	1	2	3	4	5	6	7	8
90 セキュリティ対策	1	2	3	4	5	6	7	8
91 ネットワーク管理	1	2	3	4	5	6	7	8
92 ソフトウェアの適正利用（ライセンス管理）	1	2	3	4	5	6	7	8
93 個人情報保護対策	1	2	3	4	5	6	7	8
94 PC管理、モバイル機器管理	1	2	3	4	5	6	7	8
95 コンピュータウイルス対策	1	2	3	4	5	6	7	8
96 情報システム関連のリスク管理	1	2	3	4	5	6	7	8
97 災害対策	1	2	3	4	5	6	7	8
98 その他（　　）	1	2	3	4	5	6	7	8

99 D

Q36. コンピュータ犯罪防止、ヒューマンエラー防止、事故防止、災害対策、個人情報保護の5項目について、防止ならびに早期発見の観点から、システム監査において特に重視すべき分野はどこだと思いますか。各項目ごとに最も重要と思われる分野(1～12)を1つだけ選んで下さい。

項目＼分野	データの入力プロセス	データ処理プロセス	出力プロセス	プログラム変更	オペレーション	情報保管(データ管理)	入退室(館)管理	システム開発	ハードウェア *1	ソフトウェア *2	ネットワーク	電源設備
100 コンピュータ犯罪防止	1	2	3	4	5	6	7	8	9	10	11	12
102 ヒューマンエラー防止	1	2	3	4	5	6	7	8	9	10	11	12
104 事故防止	1	2	3	4	5	6	7	8	9	10	11	12
106 災害対策	1	2	3	4	5	6	7	8	9	10	11	12
108 個人情報保護	1	2	3	4	5	6	7	8	9	10	11	12

*1 CPUと周辺機器／*2 基本ソフトとアプリケーションソフト

Q37. システム監査を実施する場合、どのような点を充実させなければならないと思いますか。最も重要だと思われるものを1つ選んで下さい。

110	1	監査計画
	2	事前調査
	3	実地調査
	4	改善勧告内容
	5	監査報告会
	6	チェックリスト
	7	その他(具体的に書いて下さい:　　)

Q38. システム監査は誰が実施するのが効果的だと思いますか。最も効果的と思われるものを1つ選んで下さい。(貴社の実態とは別にお答えいただいて結構です)

111	1	監査役(団体等は監事、自治体は監査委員)
	2	内部の監査人
	3	情報システム部門の要員
	4	システム監査技術者試験合格者
	5	監査法人・公認会計士
	6	システム監査企業台帳に基づくシステム監査企業
	7	その他(具体的に書いて下さい:　　)

112 E

Ⅳ 情報セキュリティの推進について

Q39. 貴社では情報セキュリティポリシーを策定していますか。

113	1	定めている
	2	現在作成中である
	3	作成を検討している
	4	現在、定める予定がない

Q40. 貴社では情報セキュリティをどのような体制で推進していますか。(複数回答)

114	1	情報セキュリティ担当役員を設置している
115	2	情報セキュリティ委員会を設置している
116	3	情報システム部門主導で実施している
117	4	情報セキュリティ専任者を設置している
118	5	各部門・拠点にセキュリティ担当者を設置している
119	6	外部のセキュリティコンサルタントを活用している
120	7	特に実施していない
121	8	その他(具体的に書いて下さい:　　)

Q41. 情報セキュリティ推進体制で最も重要と思われることを1つ選んで下さい。(単一回答)

122	1	経営者のリーダーシップ
	2	全社的な推進体制
	3	情報システム部門の推進体制
	4	利用部門の理解・協力
	5	その他(具体的に書いて下さい:　　)

Q42. 貴社では情報セキュリティについて、優先的に実施しているものを3つまで選んで下さい(複数回答)

123	1	情報セキュリティ対策コストの確保
125	2	リスク分析の実施
127	3	システム監査の実施
	4	情報セキュリティ教育
	5	情報セキュリティ体制の確立
	6	情報セキュリティアドミニストレータの確保
	7	情報資産の洗い出し
	8	ISMSの取得
	9	プライバシーマークの取得
	10	その他(具体的に書いて下さい:　　)
	11	特に実施していない

Q43. 貴社では情報セキュリティについてどのような教育を実施していますか。(複数回答)

129	1	新入社員教育を実施している
130	2	一般社員向け教育を実施している
131	3	管理職教育を実施している
132	4	役員教育を実施している
133	5	派遣要員向け教育を実施している
134	6	情報セキュリティ担当者の専門教育を実施している
135	7	その他(具体的に書いて下さい:　　)
136	8	特に実施していない

137 F

Ⅳ 電子メールの利用について

Q44. 電子メール利用のルールを定めていますか。

138	1	定めている	
	2	現在作成中である	
	3	作成を検討している	
	4	現在、定める予定がない	
	5	わからない	
	6	電子メールを利用していない	→終了

Q45. 要員の電子メールの利用状況を監視していますか。

139	1	監視している	
	2	今後、監視する予定がある	
	3	監視していない	→Q47へ
	4	わからない	→Q47へ

Q46. (Q45で「1」、「2」を回答した場合)電子メール利用状況の監視について、ルールを定めていますか。

140	1	ルールを定め、社員に周知している
	2	ルールは定めているが、社員に周知していない
	3	現在作成中である
	4	作成を検討している
	5	現在、定める予定がない
	6	わからない

Q47. 自宅や出張先からメールサーバへのリモートアクセスを認めていますか。

141	1	認めている
	2	許可制で認めている
	3	認めていない
	4	わからない

Q48. 自宅の個人アドレスへの社内メールの転送を認めていますか。

142

1	認めている
2	許可制で認めている
3	認めていない
4	わからない

ご協力ありがとうございました。

143 G

KEIRIN ○○ このアンケートは競輪の補助を受けて実施しているものです。

再生紙使用

平成15年3月発行

発行所　財団法人　日本情報処理開発協会
東京都港区芝公園3丁目5番8号
機械振興会館内
ＴＥＬ　03(3432)９３８７

印刷所　株式会社　美　行　企　画
東京都千代田区神田錦町2丁目5番地
鈴木第2ビル　2Ｆ
ＴＥＬ　03(3219)２９７１

H14-H004