16－H003

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集計結果－

平成17年3月

JIPDEC

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。

16-H003　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集計結果

（平成17年3月発行）

正誤表

ページ	該当箇所
116	Q58のグラフ(図3－2－32)

（正）

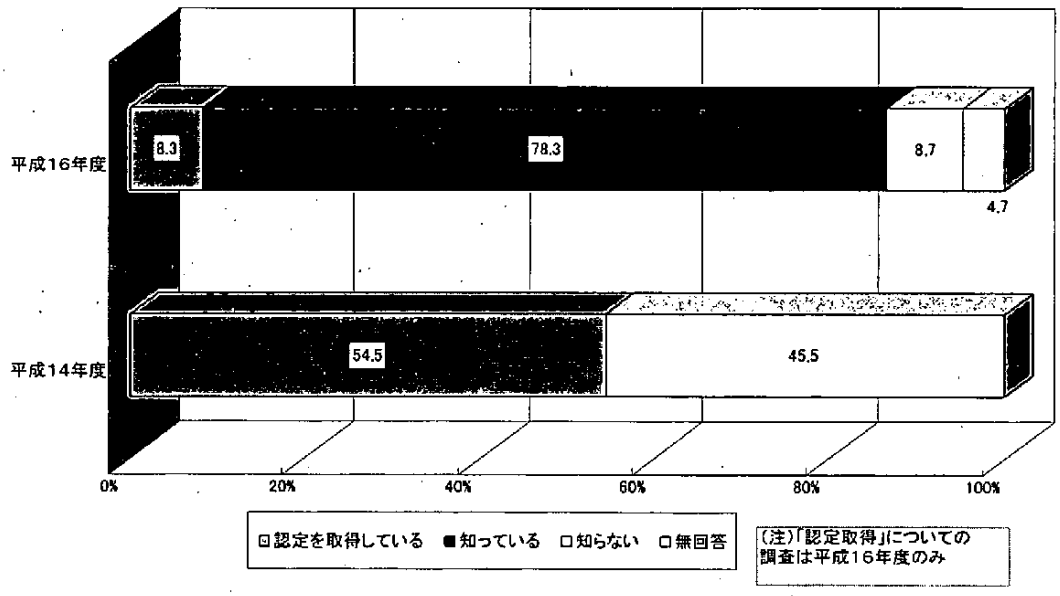

図3－2－32. プライバシーマーク制度の認知状況(被監査部門)

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、421 事業体の監査担当部門、507 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１７年３月

財団法人　日本情報処理開発協会

平成16年度システム監査基準普及検討委員会　委員名簿

（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	市村　典男	(社)情報サービス産業協会　システム監査研究会 副座長
	稲垣　隆一	日本弁護士連合会　弁護士
	江藤　友保	(株)シーイーシー 管理本部
	岡崎　洋治	(財)金融情報システムセンター 監査安全部　主任研究員
	小田　浩史	富士通エフ・アイ・ピー(株) アウトソーシング事業部オンサイトサービス部
	川辺　良和	(有)インターギデオン　代表取締役
	喜入　　博	KPMGビジネスアシュアランス(株)　常勤顧問
	橘和　尚道	NPO法人日本システム監査人協会　副会長
	清水　惠子	日本公認会計士協会 監査対応IT委員会　専門委員
	千枝　和行	(社)日本情報システム・ユーザー協会 ビジネスシステム定義研究プロジェクト 委員
	新田　　稔	IBMビジネスコンサルティング サービス(株) 公共事業本部 ISリスクマネジメント　マネージング・コンサルタント
	原田　要之助	情報システム・コントロール協会　東京支部
	本田　　実	システム監査学会　理事
	丸山　満彦	監査法人トーマツ　エンタープライズリスクサービス部 シニアマネジャー

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 16 年 11 月 19 日
回収締切　　平成 17 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　　421 件（回収率：10.5%）
被監査部門　　507 件（回収率：12.7%）

1.1.5　回答事業体の平均従業員数

監査担当部門　　2,751 人
被監査部門　　2,244 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．貴事業体の監査体制について
Ⅲ．システム監査の実施について
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．個人情報保護について

（2）被監査部門対象

Ⅰ．システム監査一般について
Ⅱ．システム監査の実施について
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．個人情報保護について

表１－１－１．回収状況（監査担当部門）

業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数（小数点以下切捨）	業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数（小数点以下切捨）
食品・紙・パルプ・繊維・印刷	食品製造業	12	2,170	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	66	956
	繊維工業	5	2,127	その他対事業所サービス	農・林・漁・狩・水産養殖業	0	-
	紙・ﾊﾟﾙﾌﾟ・紙加工品製造業	3	2,142		鉱業	1	776
	印刷業・同関連産業	1	2,500		建設業	15	1,524
石油・化学・鉄鋼・非鉄・金属	化学工業	16	2,772		新聞業・出版業	1	6,500
	石油製品製造業	1	136		不動産業	3	1,716
	鉄鋼業	4	8,286		運輸・通信・倉庫業	17	1,570
	非鉄金属製造業・金属製品製造業	3	713		電力・ガス業	8	12,249
電気・一般・輸送・精密機械	一般機械器具製造業	13	2,102		放送業	2	129
	電気機械器具製造業	21	6,065		広告・調査・情報提供サービス業	2	3,109
	輸送用機械器具製造業	11	3,574		その他のサービス業	9	819
	精密機械器具製造業	9	2,718	公共サービス	医療業	2	784
その他製造業	窯業・土石製品製造業	6	2,049		宗教法人	0	-
	その他製造業	18	2,828		高校	3	238
商　　業	卸業・商社	23	1,175		大学	12	1,065
	小売業	6	1,720		その他の教育機関	1	120
金融・保険業	金融業	58	1,879		学術研究機関	2	406
	証券業・商品取引業	4	302		法人団体・農協	7	2,296
	生命保険業	7	23,420	政府・地方公共団体	政府	1	800
	損害保険業	3	6,278		地方公共団体	45	3,074
小　　計		224	-	小　　計		197	-
合　　計						421	平均　2,751

表１－１－２．回収状況（被監査部門）

業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数（小数点以下切捨）	業務ｸﾞﾙｰﾌﾟ	業　　種	回収数	平均従業員数（小数点以下切捨）
食品・紙・パルプ・繊維・印刷	食品製造業	14	1,189	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	66	787
	繊維工業	5	2,660	その他対事業所サービス	農・林・漁・狩・水産養殖業	0	-
	紙・ﾊﾟﾙﾌﾟ・紙加工品製造業	1	1,441		鉱業	2	542
	印刷業・同関連産業	1	1,498		建設業	27	2,171
石油・化学・鉄鋼・非鉄・金属	化学工業	19	1,167		新聞業・出版業	0	-
	石油製品製造業	0	4,386		不動産業	2	247
	鉄鋼業	6	846		運輸・通信・倉庫業	22	3,247
	非鉄金属製造業・金属製品製造業	7	1,442		電力・ガス業	4	19,124
電気・一般・輸送・精密機械	一般機械器具製造業	16	4,417		放送業	6	154
	電気機械器具製造業	25	5,111		広告・調査・情報提供サービス業	2	3,705
	輸送用機械器具製造業	20	1,105		その他のサービス業	10	1,142
	精密機械器具製造業	8	1,105	公共サービス	医療業	6	1,469
その他製造業	窯業・土石製品製造業	7	3,128		宗教法人	0	-
	その他製造業	28	1,173		高校	3	79
商　　業	卸業・商社	28	742		大学	18	912
	小売業	10	2,238		その他の教育機関	2	1,092
金融・保険業	金融業	62	1,371		学術研究機関	2	406
	証券業・商品取引業	4	270		法人団体・農協	6	1,514
	生命保険業	9	10,186	政府・地方公共団体	政府	2	3,600
	損害保険業	4	4,792		地方公共団体	53	3,516
小　　計		274	-	小　　計		233	-
合　　計						507	平均　2,244

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８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 12 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している。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ものがあるため、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

経済産業省のシステム監査基準（昭和 60 年策定、平成８年改訂）が平成 16 年 10 月に改訂された。その前年には「情報セキュリティ監査制度」が発足されたが、これらセキュリティ関連基準、制度等の認知度について両部門に対し調査を行った。

システム監査関連基準の認知度について、平成８年版システム監査基準は両部門ともに［監：86.9%、被：88.5%］であった。同基準は改訂によりシステム監査基準とシステム管理基準に分かれた。公表から本調査実施まであまり時間がたっていなかったため、新基準の認知度についてはあまり高い結果は得られないだろうと予想していたが、結果として、新システム監査基準は［監：61.1%、被：57.8%］、システム管理基準は［監：63.5%、被：63.9%］と半数以上が「知っている」と回答した。また、平成 15 年に策定された情報セキュリティ監査基準は［監：76.7%、被：80.9%］、情報セキュリティ管理基準は［監：71.0%、被：78.7%］と、策定・公表から２年あまりでありながら、高い認知度となった。その他、情報システム安全対策基準［監：72.8%、被：75.2%］、コンピュータウイルス対策基準［監：75.1%、被：79.1%］、コンピュータ不正アクセス対策基準［監：71.3%、被：76.5%］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。

システム監査企業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前回調査ではあまり差が見られなかったが、今回は［監：48.7%、被：39.3%］と監査担当部門の方が約９ポイント高い。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、監査担当部門の方が被監査部門を 2.2 ポイント上回っている。（前回調査では、被監査担当部門の方が 9.4 ポイント高。）

同様に情報セキュリティ監査企業台帳制度の認知度についてもシステム監査企業台帳と同様、監査担当部門の方が被監査部門より認知度が高いが、「参考にしたい」との意見は、被監査部門の方が若干高い。

JIS X 5080 の認知度は［監：47.8%、被：53.6%］、JIS Q 15001 は［監：53.5%、被：58.2%］と 50～60%前後となったが、JIS Q 2001 の認知度［監：40.6%、被：42.2%］は他の規格に比べ

かなり低い。【監／被Q１～17】

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76.0%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9.7人、平均年齢47.3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 25.4%であり、システム監査人の人数は平均3.0人、平均年齢46.4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Q18～19】

システム監査技術者試験合格者数は平均5.6人で、所属部署については、「情報システム部門」が最も多く67.4%、「内部監査部門」は27.9%となった。【監Q20～21】

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 46.3%が、また被監査部門では44.4%の事業体が監査を実施している。初めて本調査を行った平成２年度調査（監：24.3%、被：22.2%）と比べ実施率は両部門ともに倍増しており、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Q22、被Q19】

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Q24、26】

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。【監Q28、29】

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Q31～32】

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」（42.6%）について被監査部門では 15.2%、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」（35.5%）について監査部門では 13.3%であり、両者の意見にかなり大きな差がみられる。【監：Q25、被：Q44】

2.3 システム監査の実施について

過去に監査を実施したことがある回答事業体に対し、過去２年以内での監査実施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。

過去２年以内に監査を「実施した」との回答は監査担当部門が87.8%、被監査部門が90.2%である。監査担当部門では「内部監査部門型」（60.8%）、被監査部門では、「外部委託型」（73.4%）による監査が多い。【監Q36～37、被Q20、23】

監査実施業務で多いのは「運用業務」（監：91.8%、被：90.1%）、「開発業務」（監：70.8%、被：67.5%）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Q40、被Q21】

また、監査対象テーマ別の実施状況については、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：84.2%、被：82.3%）。【監Q41、被Q22】

監査担当部門からみた自社の情報システムの状態は、33.9%が「満足」しているが、「なんともいえない」（34.5%）、「多少不満」（25.1%）との意見も多い。【監Q54】

被監査部門が監査を受けた結果の効果について、73.4%の事業体が「効果があったと思う」と回答しており、どのような効果があったかについては、「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」を挙げている事業体が25.5%と最も多い。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」（38.3%）、「規則・手続き等の遵守」（14.1%）である。【被Q36～38】

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過去２年以内の監査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調査した。結果は次のとおりである。なお、今回調査から、着眼点として「有効性」を追加した【監／被Q40～41】

（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「有効性」（36.7%）、被監査部門が「有効性」（37.9%）
- 開発業務で重視すべき着眼点は、監査担当部門が「信頼性」（27.8%）、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「信頼性」（監：37.9%）
- 保守業務で重視すべき着眼点は「信頼性」（監：38.5%、被：40.2%）

（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：65.7%、被：59.2%）
- 信頼性を重視すべきテーマは「品質管理」（監：62.5%、被：58.2%）
- 機密性を重視すべきテーマは「個人情報保護対策」（監：58.6%、被：51.5%）
- 準拠性を重視すべきテーマは「ソフトウェア適正利用」（監61.3%、被：42.8%）
- 採算性を重視すべきテーマは「コスト管理」（監：49.3%、被：59.4%）
- 適時性を重視すべきテーマは「進捗管理」（監：26.6%、被：31.6%）
- 生産性を重視すべきテーマは「要員管理」（監：20.9%、被：25.6%）
- 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」（17.9%）、被監査部門が「要員管理」（22.1%）
- 有効性を重視すべきテーマは監査担当部門が「進捗管理」（17.7%）、被監査部門が「災害対策」（16.4%）

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：37.4%、被：40.2%）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：38.0%、被：44.2%）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」（監：23.4%、被：17.8%）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「電源管理」（24.0%）、被監査部門が「情報保管（データ管理）」（29.4%）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:71.3%、被：69.2%）である。【監／被Q42】

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「システム監査を実施する担当者（部門）の確保が難しい」（22.1%）。前回調査では「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」が最も多かったが、今回調査では、「担当者の確保」と順位が逆転した。

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Q62～64】。

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、両部門とも「策定／策定中」の事業体が７割を超えている（監：73.2%、被：70.3%）【監：Q65、被：Q45】

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：50.4%、被：47.3%）。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：51.1%、被：49.3%）。

情報セキュリティに関し優先的に実施しているのは「情報セキュリティ体制の確立」（監:46.6%、被：43.0%）、「情報セキュリティ教育の実施」（監：43.5%、被：43.2%）である。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10～15%、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２～３割を占めている。【監：Q65～Q69、被：Q45～49】

情報セキュリティ監査の実施状況については、「実施／予定」の事業体はまだ少なく、過半数に満たない（監：43.2%、被：28.2%）。また、セキュリティ監査の実施については被監査部門の方

が外部委託による監査を望んでいる。(監：38.2%、被：52.5%)【監：Q69～70、被：Q50～Q51】

ISMS適合性評価制度(平成13年にパイロット運用、本格運用は平成14年)の認知度について、両部門とも「認証取得済／知っている」が前回調査と比べ30ポイント程度増加した(監:62.5%、被：74.6%)。【監：Q72、被：Q52】

2.7 個人情報保護について

平成17年4月に全面施行される個人情報保護法の認知度について、ほとんどの事業体が認知している(監：94.5%、被：94.1%)。保護法の施行を受け、各省庁が分野別にガイドライン等の整備を行ってきたが、このうち、経済産業省が策定した「経済産業分野を対象とするガイドライン」の認知度については、法律の認知度に比べると低いとはいえ、8割前後が知っている。(監:78.0%、被：82.6%)【監：Q73～74、被：Q53～54】

個人情報の管理状況に対するリスク認識については、両部門ともに何らかのリスクを認識している事業体の方が多い。【監：Q75、被：Q55】

現在実施している個人情報保護対策について、最も多いのは「管理責任者の設置」(監:42.5%、被：40.0%)である。一方で「特に対策を講じていない」事業体も3割前後を占めている(監：29.5%、被：33.1%)。また、今後実施を予定している対策については、両部門ともに「管理責任者の設置」(監：37.1%、被 40.8%)である。なお、現在実施している対策については、今後の実施対策には含めていない。【監：Q76、被：Q56】

個人情報保護の監査について、被監査部門の方が外部委託による監査を望んでいる。(監:38.2%、被：41.0%)【監：Q77、被：Q57】

プライバシーマーク制度(平成10年運用開始)の認知度について、両部門とも「認証取得済／知っている」が前回調査と比べ30ポイント程度増加した(監:78.2%、被:86.6%)。【監：Q78、被：Q58】

3．調査結果の詳細

システム監査基準（昭和 60 年策定、平成８年改訂）のシステム監査基準は改訂されて、システム監査基準とシステム管理基準の二本立てとなり、平成 16 年 10 月に公表されたが、今回（平成 16 年度）の調査は新基準公表後まもなく実施されたものである。

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～Q17 の質問については被監査部門に対しても同一の調査を行っているので、「3.2.1」を参照のこと。）

Q１．経済産業省の「システム監査基準」（平成８年改訂）を知っていますか。

1	利用したことがある	83	19.7
2	内容は知っているが、利用したことはない	144	34.2
3	存在だけは知っている	139	33.0
4	知らない	52	12.4
無回答		3	0.7
計		421	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、「前回調査」という。）と平成 16 年度調査（以下、「今回調査」という。）を比較してみると、システム監査を知っているのは、全体で前回調査の 78.1%から今回調査 86.9%と、8.8 ポイント増加しており、システム監査が着実に浸透していることを示す数字となっている。

個別の項目をながめると、まず、基準を「利用したことがある」のは、前回調査が 19.8%で、今回調査が 19.7%であるから、ほぼ同じとみてよい。すなわち、この数字で見る限り、システム監査基準の利用に関しては進展がみられないといえる。いいかえれば、この２年間に、システム監査基準を利用して新たにシステム監査の実施に踏み切った事業体はほとんどなかったのではないかと思われる。

つぎに、基準の「内容は知っているが利用したことがない」のは、前回調査の 24.5%から、今回調査では 34.2%と 9.7 ポイント増加している。これは、システム監査基準を使ってシステム監査を実施したことはないが、この２年間にシステム監査基準の内容は知ることになった事業体が大幅に増加しているのであるから、システム監査が言葉だけの広がりだけではなく内容的に浸透していることを物語っている。

また、システム監査基準の「存在だけは知っている」のは、前回調査 33.8%であり、今回調査が 33.0%であるから、ほとんど変化はみられない。逆に、システム監査基準を「知らない」というのは、前回調査の 20.9%から、今回調査は 12.4%と 8.5 ポイントの大幅な減少を示していることが注目される。

以上のことから、一方で「内容は知っているが、利用したことはない」が9.7ポイントと大幅な増加を示し、他方で「知らない」が8.5ポイントと大幅に減少していることは、次のように解釈できよう。すなわち、システム監査基準を「知らない」が大幅に減少した分は、その分が「存在だけは知っている」の方に移行し、従来の「存在だけは知っている」の中から「内容は知っているが、利用したことはない」へ大幅に移行しているものと思われる。

このように分析すると、システム監査基準の「存在だけは知っている」が、前回調査が33.8%で今回調査が33.0%とほとんど変化はみられないが、その中身は相当に異なっているといえよう。このような見方をすると、この2年間に新たにシステム監査の実施に踏み切った事業体はあまり見られないが、システム監査基準の内容について理解を深めた事業体は増加しているといえよう。

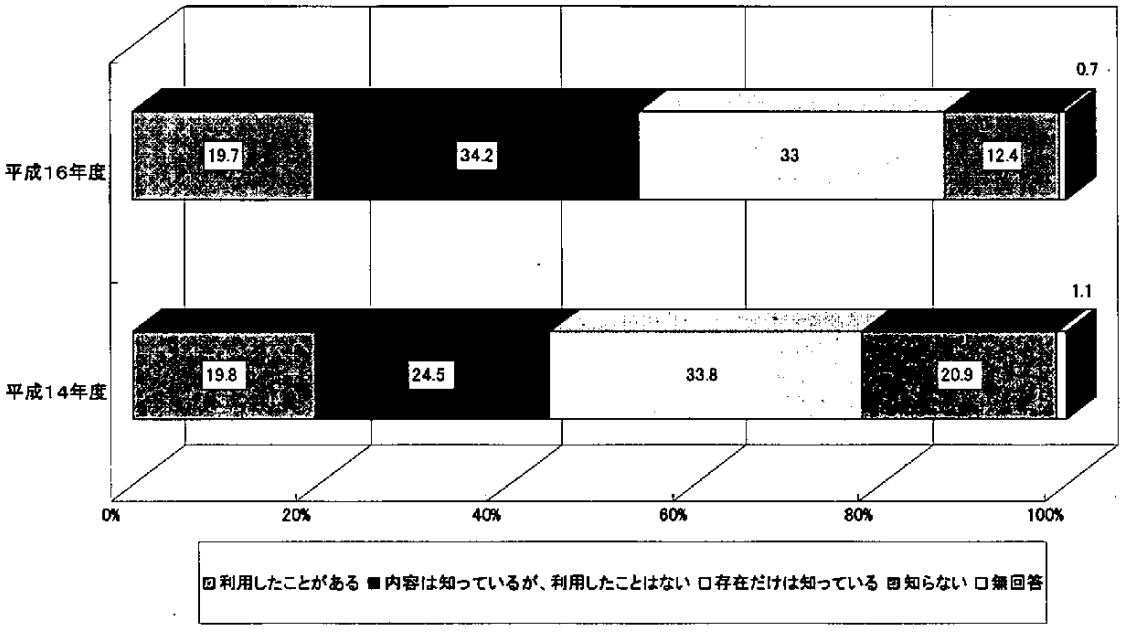

図3－1－1. システム監査基準の認知度(監査担当部門)

Q2.「システム監査基準」が平成16年10月に改訂されたことを知っていますか。

1	利用したことがある	29	6.9
2	内容は知っているが、利用したことはない	128	30.4
3	存在だけは知っている	100	23.8
4	知らない	161	38.2
無回答		3	0.7
計		421	100.0

改訂システム監査基準を「利用したことがある」のは6.9%に過ぎず、「知らない」は38.2%に達している。これは、システム監査基準が改訂された直後に実施された調査であることを考慮すれば、仕方のないことであろう。しかし、改訂システム監査基準を利用した事業体は少ないが、改訂直後の調査でさえ、「内容は知っているが利用したことはない」が30.4%、「存在だけは知っている」が23.8%あり、改訂されたシステム監査基準を知っている事業体は全体で61.1%に達していることは高く評価してよい。

Q３．経済産業省から「システム管理基準」（平成 16 年 10 月）が策定・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	31	7.4
2	内容は知っているが、利用したことはない	127	30.2
3	存在だけは知っている	109	25.9
4	知らない	150	35.6
無回答		4	1.0
計		421	100.0

システム監査基準が改訂されるとともに、新たに姉妹編としてシステム管理基準が公表されたが、システム管理基準についてもシステム監査基準と同様の傾向が表れている。何らかの形でシステム管理基準を知っているのは、63.5%に上っている。このような傾向は、システム管理基準がシステム監査基準の姉妹編として位置づけられ、システム監査にも活用される基準として作成されていることから当然のことといえよう。

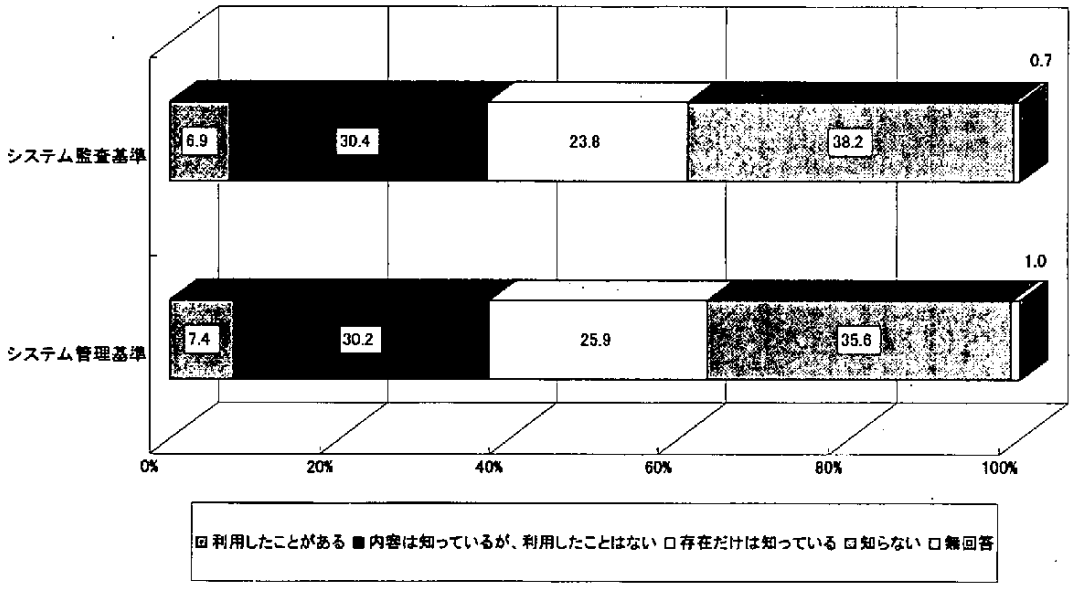

図3－1－2. 新システム監査基準／システム管理基準の認知度（監査担当部門）

Q４．経済産業省の「システム監査企業台帳」（平成３年）を知っていますか。

1	知っている	205	48.7
2	知らない	213	50.6
無回答		3	0.7
計		421	100.0

→Q６へ

システム監査企業台帳を「知っている」のは、前回調査の 33.8%から、今回調査は 48.7%と約 15 ポイント増加している。逆に、「知らない」は、前回調査の 65.4%から、今回調査は 50.6%と約 15 ポイント減少している。システム監査企業台帳の認知度が、この２年間に約 15 ポイントも向上していることは、最近におけるシステム監査への関心の高まりと理解してよいと思われる。

Q５．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	18	8.8
2	今後参考にしたいと思う	153	74.6
3	参考にしたいと思わない	28	13.7
無回答		6	2.9
計		205	100.0

これは、システム監査企業台帳制度を知っている事業体に対する質問である。これまでにシステム監査企業台帳を「参考にしたことがある」のは、前回調査が9.4%で、今回調査が8.8%と、いずれも10%に達していない。しかし、「今後参考にしたいと思う」事業体は、前回調査の64.4%から、今回調査は74.6%へと約10ポイントの増加を示している。システム監査の実施に伴って、この台帳が重視されるようになるであろうことを予感させる数字となっている。

Q６．経済産業省の「情報セキュリティ監査基準」（平成15年４月策定）を知っていますか。

1	利用したことがある	65	15.4
2	内容は知っているが、利用したことはない	131	31.1
3	存在だけは知っている	127	30.2
4	知らない	94	22.3
無回答		4	1.0
計		421	100.0

経済産業省は平成15年４月、情報セキュリティ監査基準と情報セキュリティ管理基準を告示した。情報セキュリティ監査基準を知っているのは、全体で76.7%であり、告示から約１年半後の調査であることを考慮すると、認知度は高いといえる。

認知度が高いとはいえ「利用したことがある」のは15.4%に過ぎない。しかし、「内容は知っているが、利用したことはない」が31.1%に達しており、内容を知っている事業体がかなりあることがわかる。問題は「知らない」という22.3%の事業体をいかにして減らしていくかであろう。

Q７．経済産業省の「情報セキュリティ管理基準」（平成15年４月策定）を知っていますか。

1	利用したことがある	63	15.0
2	内容は知っているが、利用したことはない	129	30.6
3	存在だけは知っている	107	25.4
4	知らない	117	27.8
無回答		5	1.2
計		421	100.0

情報セキュリティ管理基準を知っているのは、全体で71.0%と情報セキュリティ監査基準より認知度が5.7ポイント低くなっている。これは、この調査が監査担当部門対象の調査であることを考慮すれば、仕方のないことであろうか。

個別項目のうち、「存在だけは知っている」が情報セキュリティ監査基準が 30.2%であるのに対して、情報セキュリティ管理基準は25.4%であり、4.8ポイント低くなっている。また、「知らない」については、情報セキュリティ監査基準が22.3%であるのに対して、情報セキュリティ管理基準は27.8%であり、5.5ポイント高くなっている。

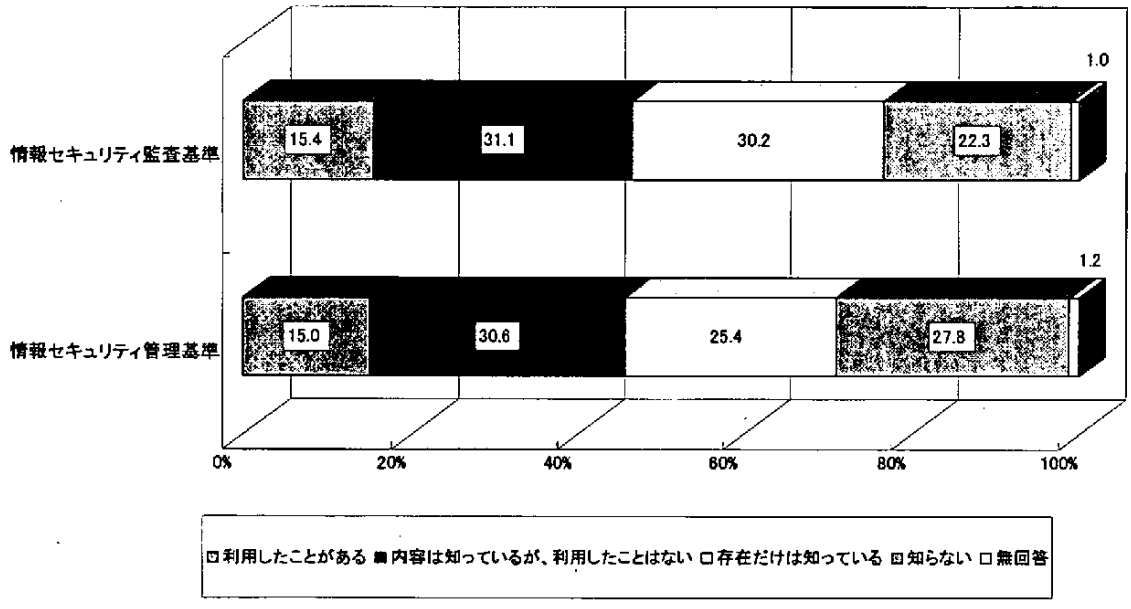

図3－1－3. 情報セキュリティ監査基準／情報セキュリティ管理基準の認知度（監査担当部門）

Q8．経済産業省の「情報セキュリティ監査企業台帳」（平成１５年）を知っていますか。

1	知っている	193	45.8
2	知らない	225	53.4
無回答		3	0.7
計		421	100.0

→Q10へ

情報セキュリティ監査企業台帳を「知っている」のは、45.8%であり、創設されて１年半程度での認知率としては高いといえる。とくに、平成３年に創設されたシステム監査企業台帳の認知率が48.7%であることを考えると、情報セキュリティ監査企業台帳の浸透の仕方は非常に速いということができる。

Q９．情報セキュリティ監査を外部の企業に委託する場合、「情報セキュリティ監査企業台帳」を参考にしたいと思いますか。

1	参考にしたことがある	21	10.9
2	今後参考にしたいと思う	146	75.6
3	参考にしたいと思わない	22	11.4
無回答		4	2.1
計		193	100.0

情報セキュリティ監査を外部に委託する場合に、情報セキュリティ監査企業台帳を「参考にしたことがある」のは10.9%で、システム監査企業台帳を参考にした8.8%を上回っている。つまり、外部に委託するのは、システム監査より情報セキュリティ監査の方が多くなるのではないかと推測される。いいかえれば、システム監査より情報セキュリティ監査の方が、より高い専門能力を必要とすることから、外部へ委託する可能性がより高いのではないかと思われる。

Q10．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	323	76.7
2	知らない	94	22.3
無回答		4	1.0
計		421	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、本年度で20年目を迎える。この間、システム監査技術者試験の存在はよく知られるようになり、今日ではすっかり情報社会に定着した試験となっている。システム監査技術者試験を「知っている」のは、今回調査では76.7%であり、このまま認知度が上がっていけば、次回の調査では認知率が80%を超えることになる可能性がある。

Q11．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	84	20.0	
2	内容は知っているが、利用したことはない	119	28.3	
3	存在だけは知っている	103	24.5	
4	知らない	112	26.6	→Q13へ
無回答		3	0.7	→Q13へ
計		421	100.0	

情報システム安全対策基準を知っているのは、全体で前回調査の 67.6%から、今回調査は 72.8%へと 5.2 ポイント増加している。70%を超える事業体が知っているということは、基準として認知度が高いといってよいだろう。

「利用したことがある」のは、前回調査の 22.2%から、今回調査は 20.0%と若干減少している。これは、前回調査より今回調査の母集団が約 50 事業体少ないことが影響しているものと思われる。しかし、「内容は知っているが、利用したことはない」については、前回調査の 18.4%から、今回調査は 28.3%であり、9.9 ポイントと大幅な増加を示していることが注目される。

情報システム安全対策基準に限ったことではないが、単に名称を知っているだけではなく、利用したことがなくても基準の内容は知っているという事業体が大幅に増えるということは、それだけニーズが高まっていることを意味するものであり、よい傾向であるといえる。

Q12.「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	243	79.4
2	知らない	63	20.6
計		306	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」、運用基準で「システム監査」という項目が位置づけられている。このことを「知っている」のは、前回調査が 78.4%で、今回調査は 79.4%であり、約 80%の事業体がこのことを知っていることになり、認知度が高いといえる。

Q13. 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	71	16.9	
2	内容は知っているが、利用したことはない	117	27.8	
3	存在だけは知っている	128	30.4	
4	知らない	100	23.8	→Q15 へ
無回答		5	1.2	
計		421	100.0	

コンピュータウイルス対策基準を知っているのは、全体で前回調査の 66.9%から、今回調査は 75.1%と 8.2 ポイント増加している。コンピュータウイルス対策基準の認知度が、情報システム安全対策基準の 72.8%を上回り、75.1%に達していることは、最近のコンピュータウイルス被害状況を反映しているものと思われる。

コンピュータウイルス対策基準を「利用したことがある」のは、前回調査が 17.5%で、今回調査が 16.9%となっており、若干低下しているが、これは母集団の関係であろうと思われ、ほとんど同じ傾向とみてよい。これに対して、「内容は知っているが、利用したことはない」は、前回調

査が18.4%であるのに対して今回調査は27.8%であり、9.4ポイントと大幅に増加している。これも、最近の事情を反映して、内容を知る必要がある事業体が増えているものと解釈できる。

Q14.「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	219	69.3
2	知らない	95	30.1
無回答		2	0.6
計		316	100.0

コンピュータウイルス対策基準にシステム監査が位置づけられているが、このことを「知っている」のは、前回調査65.9%、今回調査が69.3%であり、3.4ポイント増加している。約70%がコンピュータウイルス対策基準にシステム監査が位置づけられていることを知っていることは、コンピュータウイルス対策におけるシステム監査の役割の重要性が認識されてきていることを物語っている。

Q15. 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	69	16.4
2	内容は知っているが、利用したことはない	116	27.6
3	存在だけは知っている	115	27.3
4	知らない	117	27.8
無回答		4	1.0
計		421	100.0

→Q17へ

コンピュータ不正アクセス対策基準を知っているのは、全体で前回調査の63.9%から、今回調査では71.3%と7.4ポイント増加している。コンピュータ不正アクセス対策基準の認知度が70%を超えていることは、最近のホームページの改変などをはじめ、不正アクセス事件が発生していることなどに対して敏感になっているものと思われる。

しかし、同基準を「利用したことがある」のは、前回調査が16.7%、今回調査が16.4%であり、あまり利用されていない。「内容は知っているが、利用したことはない」は、前回調査の20.0%から、今回調査では27.6%へと7.6ポイント増加している。これは、この２年間に「知らない」事業体が７ポイント減少し、その分が「存在だけは知っている」へ移動し、「存在だけは知っている」の中から約７ポイントが「内容は知っているが、利用したことはない」へと動いたものと思われる。このため、「存在だけは知っている」の数字は約7%でほとんど変わらないが、その中の事業体は入れ替わっているものと思われる。

Q16.「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	206	68.7
2	知らない	92	30.7
無回答		2	0.7
計		300	100.0

コンピュータ不正アクセス基準にもシステム監査が位置づけられている。このことを「知っている」のは、前回調査が 69.0%、今回調査が 68.7%である。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を知っているのは、70%に達しておらず他の基準と比較して若干低くなっている。問題は、そのことよりも、この２年間ほとんど変化が見られないことであろう。

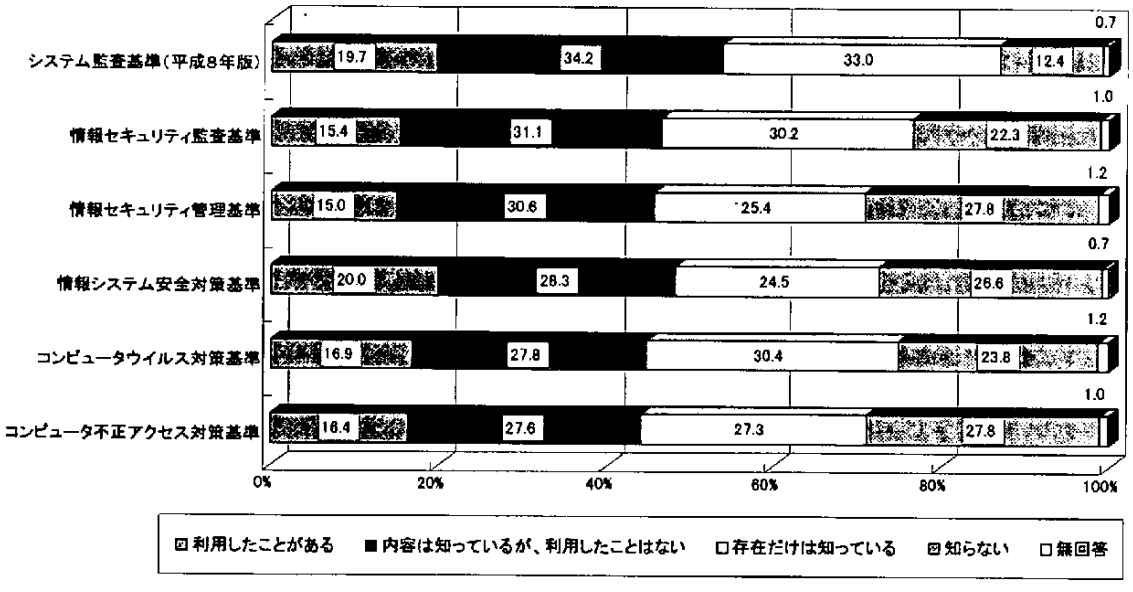

図3－1－4. セキュリティ関連基準の認知度(監査担当部門)

Q17. 以下の JIS 規格を知っていますか。

規格名	利用している		知っている		知らない		無回答		計	
JIS X 5080 ： 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 (平成 14 年2月制定)	52	12.4	149	35.4	215	51.1	5	1.2	421	100.0
JIS Q 2001 ： リスクマネジメントシステム構築のための指針 (平成 13 年3月制定)	21	5.0	150	35.6	244	58.0	6	1.4	421	100.0
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 (平成 11 年4月制定)	77	18.3	148	35.2	190	45.1	6	1.4	421	100.0

JIS 規格については、「利用している」のは JIS Q 15001 が最も多くて 18.3%を示している。これは、プライバシーマーク制度の影響であると思われる。したがって、プライバシーマークを取得する事業体が増えれば、この認知度も上昇すると思われる。

次に利用が多いのが JIS X 5080 で 12.4%を示している。これは、ISMS 適合性評価制度の影響であると思われる。プライバシーマーク制度と同様に、認証を取得する事業体が増加すれば、この認知度も上昇することであろう。

最も利用率が低いのは JIS Q 2001 で 5.0%にすぎない。他の２つの規格に対して、これには認証制度などがないため、あまり利用されていないものと思われる。つまり、必要に迫られないと利用されないことを物語っている。

この３つの規格については、利用率が最も高い JIS Q 15001 のみは「知っている」が「知らない」を上回っているが、JIS X 5080 と JIS Q 2001 については「知らない」が過半数を超えている。これらの規格が存在することくらいは、もっと知られてもよいのではないかと思われる。

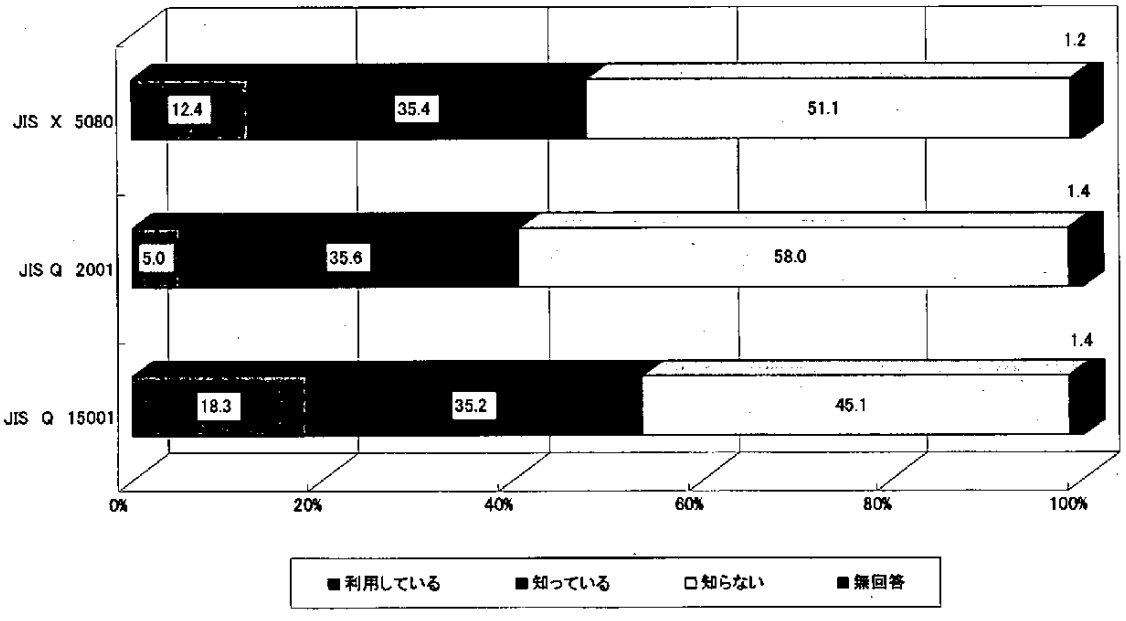

図3－1－5. JIS規格の認知度(監査担当部門)

3.1.2　貴事業体の監査体制について

Q18. 貴事業体には内部監査部門（監査部、検査部等）が設置されていますか。

1	いる	320	76.0
2	いない	99	23.5
無回答		2	0.5
計		421	100.0

→Q19へ

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、検査部等）を設置している状況は、全回答の76.0%が「設置している」となっている。設置状況は、これまで平成10年63.4%、平成12年68.5%、前回調査69.0%で微増であったが、今回調査では、前回調査に比較して7.0ポイント増と、大きく増加した。これは近年、企業等における内部統制の強化の表れとみることができる。

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（100.0%）、電力・ガス事業(100.0%)、金融業（98.3%）、建設業（93.3%）、運輸・通信業・倉庫業（76.5%）、電気機械機具製造業（76.2%）、化学工業（75.0%）、卸売・商社（73.9%）、地方公共団体（71.1%）、情報処理サービス業・ソフトウェア業（68.2%）が特に高くなっている。

Q18-1. 内部監査人は何人いますか。

平均	9.7人	
1人	36	11.3
2人	45	14.1
3人	38	11.9
4人	49	15.3
5人	23	7.2
6～10人	45	14.1
11～15人	17	5.3
16～20人	19	5.9
21人以上	38	11.9
無回答	10	3.1
計	320	100.0

Q18-2. 内部監査人は平均何歳ですか。
（端数切捨て）

平均	47.3歳	
～35歳	7	2.2
36～40歳	17	5.3
41～45歳	35	10.9
46～50歳	86	27.5
51～55歳	85	26.6
56～60歳	44	13.8
61～65歳	19	5.9
66歳以上	2	0.6
無回答	23	7.2
計	320	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9.7人であり、前回調査の13.3人に対して3.6人減少している。特に「21人以上がいる」とした回答が、前回調査では15.0%であったのに対し今回は11.9%であったことが減少の理由の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59.8%となっている。全体平均を高くしているのは金融関係で、「21人以上」の内部監査人がいると回答した11.9%の多くは金融業であった。

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47.3歳である。前回調査の平均年齢は51.1歳であり、２年経過したにもかかわらず、この間で3.8歳も若返りとなっている。これまでの調査では内部監査人の平均年齢は上昇しており、前回調査で初めて若干の若返りとなった

が、今回調査では、大きく若返った。前回調査で平均年齢帯で最も多かったのは、「51 歳～55 歳」であったが、全体の平均年齢の若返りを反映し今回調査では、「46 歳～50 歳」となり、回答全体の27.5%であった。

若返ったとはいえ平均年齢 47.3 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。

Q19. 貴事業体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	107	25.4
2	いない	312	74.1
無回答		2	0.5
計		421	100.0

→Q20 へ

Q19-1. システム監査人は何人ですか。

平均	3.0人	
1人	35	32.7
2人	36	33.6
3人	14	13.1
4人	5	4.7
5人	2	1.9
6～10人	8	7.5
11～15人	1	0.9
16～20人	1	0.9
21人以上	2	1.9
無回答	3	2.8
計	107	100.0

Q19-2. システム監査人は平均何歳ですか。（端数切り捨て）

平均	46.4歳	
～35歳	3	2.8
36～40歳	7	6.5
41～45歳	16	15.0
46～50歳	32	29.9
51～55歳	26	24.3
56～60歳	16	15.0
61～65歳	0	0.0
66歳以上	0	0.0
無回答	7	6.5
計	107	100.0

Q19-3. 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）

1990年以前	22	20.6	1998年	5	4.7
1991年	0	0.0	1999年	4	3.7
1992年	3	2.8	2000年	7	6.5
1993年	0	0.0	2001年	9	8.4
1994年	6	5.6	2002年	16	15.0
1995年	4	3.7	2003年	9	8.4
1996年	0	0.0	2004年	6	5.6
1997年	3	2.8	無回答	13	12.1
計				107	100.0

内部監査部門は回答の76.0%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25.4%となっている。これは、前回調査の23.6%に比べ、1.8ポイントの増加となっている。一般の業務監査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、金融業が63.8%、生命保険業が57.1%、情報処理サービス業・ソフトウェア業が43.9%となっている。金融業は前回調査が60.9%であり、2.9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、今回調査では、3.0 人である。過去の調査では、平成 10 年 3.3 人、平成 12 年 4.8 人、前回調査が 4.0 人であった。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 32.7%、２人が 33.6%となっており、約２／３の事業所が２名までとなっている。

システム監査人の平均年齢は、前回調査で 48.9 歳であったが、２年経過したにもかかわらず今回調査では、2.5 歳若い 46.4 歳となった。従来の調査ではシステム監査人の平均年齢は増加する一方であり、初めて前回調査で 0.2 歳の僅かながらの若返りであったが、今回の調査では大幅な若返りとなった。「Q18-2 内部監査人の平均年齢」の大幅な若返りと合わせて、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47.3歳より0.9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 20.6%、「1991 年以降」が 67.3%となっている。最近の 2001 年以降の数字が高く、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 12.1%と他の調査項目に比較して多くなっているが、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。

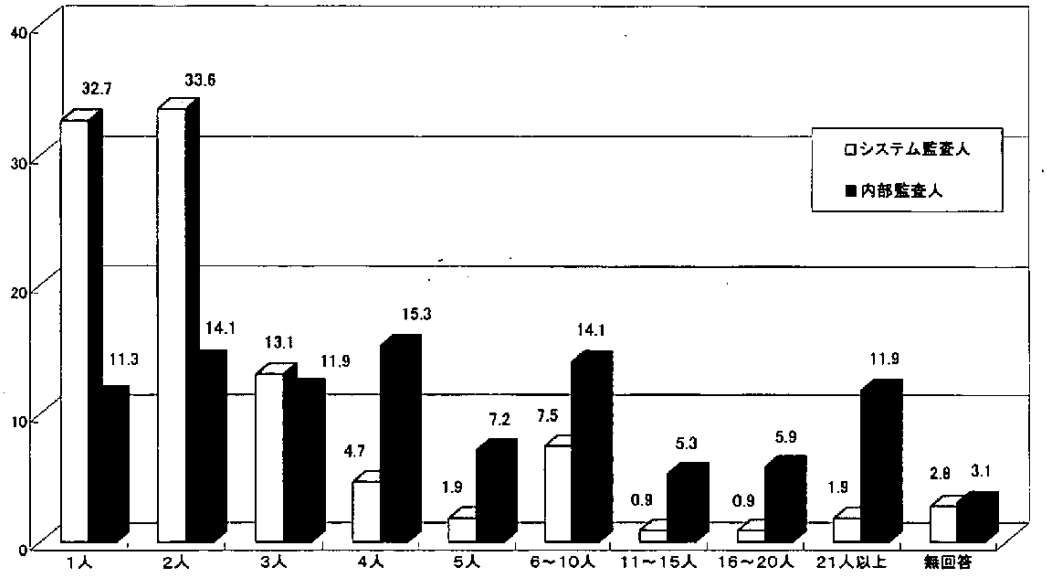

図3－1－6. システム監査人と内部監査人の配置状況(監査担当部門)

Q20. 貴事業体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	86	20.4
2	いない	227	53.9
3	把握していない	101	24.0
無回答		7	1.7
計		421	100.0

→Q22 へ

Q20-1. 何人の合格者がいますか。

回答件数	86	-	平均	5.6 人	
1人	31	36.0	6～10人	9	10.5
2人	14	16.3	11～15人	3	3.5
3人	7	8.1	16～20人	1	1.2
4人	3	3.5	21人以上	7	8.1
5人	4	4.7	無回答	7	8.1

情報処理技術者試験が実施されて 18 年が経過（調査時点）した。全回答者に対する試験合格者の有無の調査では、「合格者がいる」は、平成 10 年調査 19.4%、平成 12 年調査 19.3%、前回調査では 19.6%であったが、今回調査でも 20.4%と前回調査に比較して 0.8 ポイントの増加となった。業種別では、生命保険業が 57.1%、情報処理サービス業・ソフトウェア業が 56.1%と高く、次いで電力・ガス事業が 37.5%、電気機械器具製造業が 23.8%、金融業は 19.0%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 5.6 人であり、前回調査の 9.3 人に対し 3.7 人の大幅減となった。内訳は、1 人が 36.0%、2 人が 16.3%であるが、一方、21 名以上の回答は、8.1%となっている。大幅減となった理由は、16 名以上と回答した事業体の回答数が減少したためである。21 名以上の合格者がいると回答した業種では情報処理サービス業・ソフトウェア業が多い。

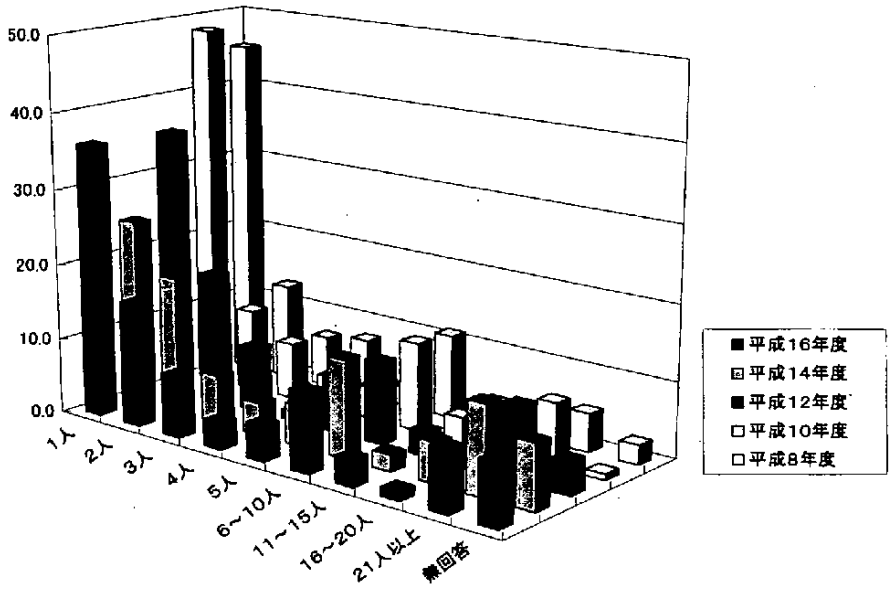

図3-1-7. システム監査技術者試験 合格者分布(監査担当部門)

Q21. 合格者はどこに所属していますか。(複数回答)

回答件数		86	-
1	監査担当部門	24	27.9
2	情報システム部門	58	67.4
3	その他	39	45.3

合格者が所属する部門（複数回答）は、「情報システム部門」が 67.4%（前回調査 69.9%）であり、「内部監査部門」に所属するのは 27.9%（前回調査では 31.2%）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。

回答は複数回答であるが、「その他」の回答も 45.3%となっており、合格者のいる事業体の半分近くが、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。

Q22. 貴事業体ではシステム監査を実施したことがありますか。

1	ある	195	46.3	
2	ない	226	53.7	→Q62へ
計		421	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「過去のシステム監査実施状況」（監査Q22、被監査Q19）、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、「過去２年以内の監査実施状況」（監査Q36、被監査Q20）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 46.3%、被監査部門では 44.4%となっている。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 12 年調査では、監査担当部門は 36.7%、被監査部門は 35.4%、前回調査では監査担当部門 38.4%、被監査部門 39.3%となっている。（被監査部門に関する分析（Q19）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。これまでは前回調査に対して約 2～3%の増加であったが、今回調査では、監査担当部門は 7.9 ポイント、被監査部門は 5.1 ポイントの大幅な増加となっている。

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（79.3%）、情報処理サービス業・ソフトウェア業（59.1%）、電気機械器具製造業（57.1%）の順となっている。前回調査で金融業は 70.3%であり、今回は 9.0 ポイント増加した。

回答数は少ないものの、生命保険業（100.0%）、鉄鋼業および電力・ガス事業（75.0%）、建設業（53.3%）、一般機械器具製造業（46.2%）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 41.0%、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 56.6%となっている。前回調査に比較し、第二次産業では 10.0 ポイント、第三次産業では 7.2 ポイントの増加となっている。

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 36.0%、1,000 人以上 5,000 人未満では 52.0%、5,000 人以上 10,000 人未満では 65.7%、10,000 人以上では 84.2%が監査を実施している。10,000 人以上では前回調査では 83.9%であり、前回と同様である。

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。

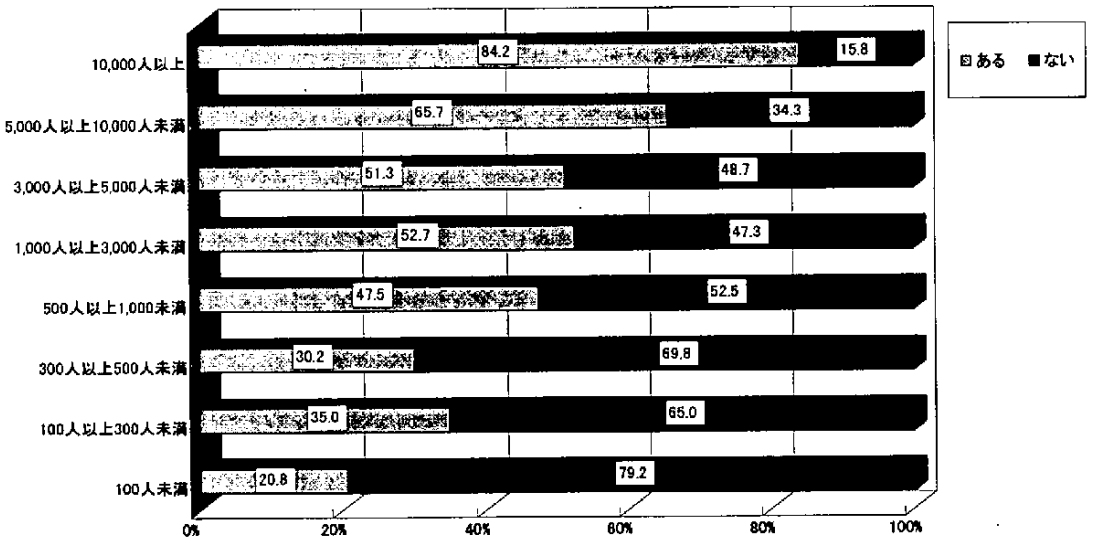

図3－1－8. システム監査実施状況(従業員数別－監査担当部門)

Q23. 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	74	37.9
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	39	20.0
3	定められていない	79	40.5
無回答		3	1.5
計		195	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の策定状況については、監査担当部門では、「定められている」が 37.9%、「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 20.0%であり、合計が 57.9%である。これまでの調査では、平成 10 年調査が合計 54.7%、平成 12 年調査が 58.7%、前回調査が 65.9%となっており、前回調査まで徐々に増加してきたが、今回は 8.0 ポイントの減少となった。今回は、「他の社内規定でシステム監査の実施が明記されている」が前回調査とほぼ同様であったのに対し、「定められている」が 8.8 ポイント減少したことが影響している。「定められている」割合が高い業種は、情報処理サービス業・ソフトウェア業の 61.5%、金融業の 56.5%、化学工業の 40.0%である。

Q24. 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	3	1.5
2	システム監査人が不足している	77	39.5
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	22	11.3
4	システム監査のチェックリストが整備されていない	11	5.6
5	利用できるシステム監査技法が少ない	13	6.7
6	被監査部門の協力が得られない	3	1.5
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	1	0.5
8	その他	13	6.7
9	実施上の問題点はない	46	23.6
無回答		1	0.5
複数回答		5	2.6
計		195	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割弱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 39.5%が「システム監査人の不足」と回答している。「システム監査人の不足」は、前回調査では 33.5%であったのに対し 6.0 ポイントと大きく増加し、より大きな問題点となっている。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」（11.3%）、「利用できるシステム監査技法が少ない」（6.7%）、「システム監査チェックリストが整備されていない」（5.6%）となっている。

「その他」（6.7%）の意見としては、「対象部門が多く網羅的にできない」、「システムの専門家ではないため、一部のセキュリティ監査（可能な範囲は全て）に限られてしまう」、「システム監査の実施体制がシステム部門に依拠している」等が挙げられた。

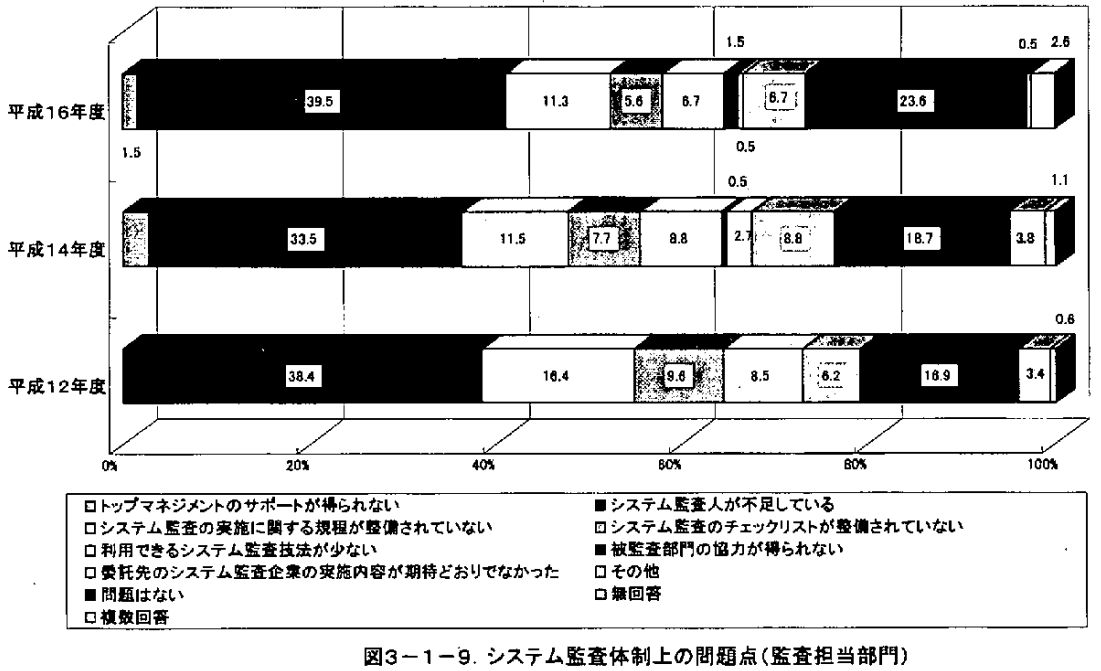

図3－1－9. システム監査体制上の問題点（監査担当部門）

Q25. 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)	3	1.5
2	内部の監査人	83	42.6
3	情報システム部門の要員	7	3.6
4	システム監査技術者試験の合格者	27	13.8
5	監査法人・公認会計士	44	22.6
6	システム監査企業台帳に基づくシステム監査企業	26	13.3
7	その他	4	2.1
無回答		1	0.5
計		195	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」(42.6%) が高く、約４割となっている。平成 10 年 45.3%、平成 12 年 42.9%、前回調査では 47.8%であったが、今回調査では前回調査に比較して 5.2 ポイントの減少となっている。「内部の監査人」の回答が約４割との値は、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による実施率が高かったのと符合している。

「内部の監査人」に次いで高いのが、「監査法人・公認会計士」(22.6%)、「システム監査技術者試験合格者」(13.8%)、「システム監査企業台帳に基づくシステム監査企業」(13.3%)となった。前回調査では、「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%) の順であった。

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」(35.5%)、「監査法人・公認会計士」(25.8%)、「内部の監査人」(15.2%)、「システム監査技術者試験合格者」(11.0%) となっている (被監査部門に関する分析 (Q44) は、「3.2.3」を参照のこと)。

その他の意見としては、「監査部門に専門知識を持つスタッフを配置して行うのが望ましい」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。

Q26. 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	34	17.4
2	事前調査	46	23.6
3	実地調査	43	22.1
4	改善勧告内容	40	20.5
5	監査報告会	4	2.1
6	チェックリスト	19	9.7
7	その他	8	4.1
無回答		1	0.5
計		195	100.0

システム監査は、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である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」(23.6%)、「実地調査」(22.1%)、「改善勧告内容」(20.5%)の３項目がほぼ並び、次いで「監査計画」(17.4%)、「チェックリスト」(9.7%)の順となった。「事前調査」は、前回調査では26.9%であり、やや減少した。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。

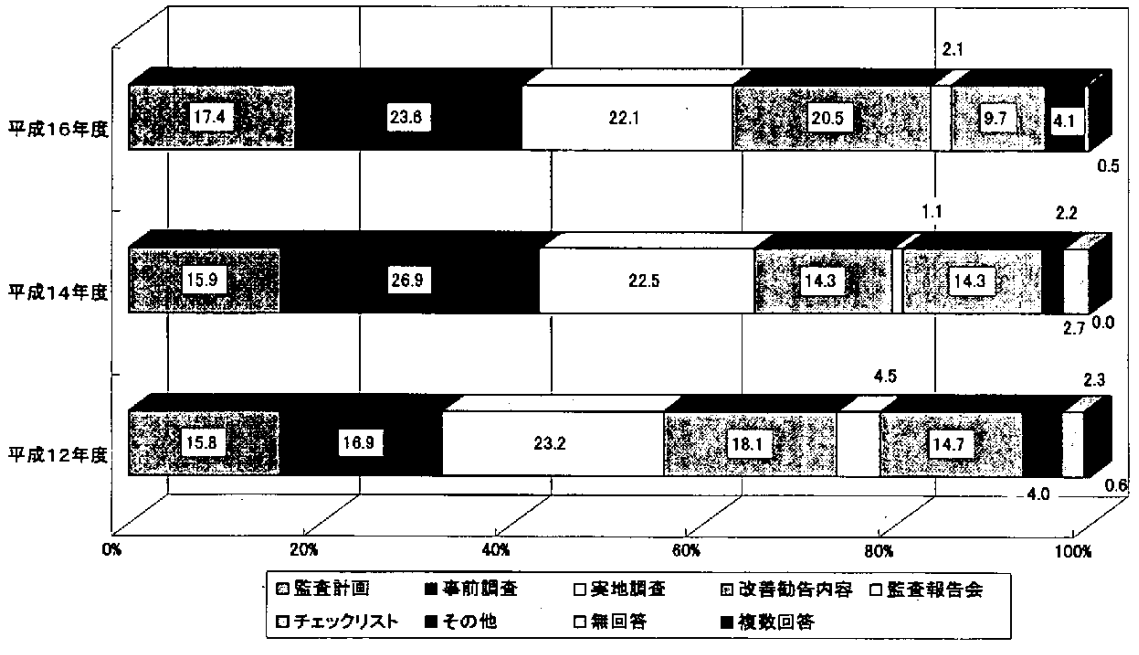

図3－1－10. システム監査で充実すべき点(監査担当部門)

Q27. 貴事業体ではシステム監査人は何人位必要だと思いますか。

平均	3.4人	
1人	26	13.3
2人	67	34.4
3人	36	18.5
4人	9	4.6
5人	21	10.8
6～10人	13	6.7
11～15人	2	1.0
16～20人	1	0.5
21人以上	3	1.5
無回答	17	8.7
計	195	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10年で平均3.7人、平成12年では平均5.5人、前回調査では3.9人であったが、今回調査では3.4人となった。3.4人必要との値は、「Q19-1. システム監査人の人数」の平均であった3.0人とほぼ同じであり、必要数と現状はほぼ一致していることになる。しかし、Q24におけるシステム監査の実施における問題点で最も回答数が多かった「システム監査人が不足している」(39.5%) との回答とは、やや乖離がある。

Q28. 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	20	10.3
2	業務知識	52	26.7
3	法律知識	15	7.7
4	監査知識	25	12.8
5	情報システムの知識	48	24.6
6	その他	3	1.5
7	わからない	22	11.3
無回答		8	4.1
複数回答		2	1.0
計		195	100.0

Q28、Q29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。回答は、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」(26.7%) と「情報システムの知識」(24.6%) 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。前回調査から選択肢として加えた「わからない」は、11.3%となっている。

Q29. 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	32	16.4
2	分析能力	70	35.9
3	判断能力	24	12.3
4	報告書作成能力	12	6.2
5	その他	6	3.1
6	わからない	39	20.0
無回答		12	6.2
計		195	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、前回調査同様、「分析能力」（35.9%）が圧倒的に高く、トップとなり、次いで「インタビュー能力」（16.4%）、「判断能力」（12.3%）となっている。「わからない」（20.0%）も多かった。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、分析ができていないことを示している。

Q30. 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	63	32.3
2	社内教育	9	4.6
3	OJT	27	13.8
4	通信教育	2	1.0
5	その他	5	2.6
6	特に教育は実施していない	41	21.0
7	監査を外部委託しているため該当しない	37	19.0
無回答		11	5.6
計		195	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行っている教育方法に関する調査では、前回調査と同様「外部セミナーを利用」（32.3%）がトップとなり、次いで「OJT」（13.8%）であった。次いで「特に教育は実施していない」（21.0%）であり、「監査を外部委託しているため該当しない」は、19.0%であった。

Q31. 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		195	-
1	トップマネジメントの要求に基づいて決定	56	28.7
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	9.7
3	内部監査部門長の判断に基づいて決定	100	51.3
4	システム監査人の独自の判断で決定	57	29.2
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	8	4.1
6	プライバシーマーク制度の要求事項に基づいて決定	25	12.8
7	ISMS制度の要求事項に基づいて決定	26	13.3
8	その他	20	10.3
無回答		10	5.1

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」(51.3%)、次いで「システム監査人の独自の判断で決定」(29.2%)、「トップマネジメントの要求に基づいて決定」(28.7%) となっている。これに続いているのが「ISMS 制度の要求事項に基づいて決定」(13.3%)、「プライバシーマーク制度の要求事項に基づいて決定」(12.8%) と制度による監査の実施も多くなっている。「ISNS 制度の要求事項に基づいて決定」は前回調査の 6.6% から倍増し、「プライバシーマーク制度の要求事項に基づいて決定」は前回の 9.3%から 3.5 ポイント増加となっている。「内部監査部門長の判断に基づく決定」は前回調査で 54.4%であり、今回調査もほぼ同様である。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。

「トップマネジメントの要求に基づいて決定」(28.7%) は、平成 12 年調査では 16.4%であったものが前回調査で 29.1%と大幅に増加したが、今回調査でも同様の回答となった。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。

その他の意見としては、「アプリケーションシステムのリスク評価に基づいて決定」、「監査法人の方針に基づいて決定する」等が多かった。

Q32. 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		195	-
1	トップマネジメントの要求に基づいて決定	56	28.7
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	23	11.8
3	内部監査部門の判断で決定	107	54.9
4	システム監査人の独自の判断で決定	57	29.2
5	各種認定制度等の要求事項に基づいて決定	29	14.9
6	その他	15	7.7
無回答		11	5.6

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54.9%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29.2%、「トップマネジメントの要求に基づいて決定」は28.7%であり、「各種認定制度等の要求事項に基づいて決定」は14.9%、「監査役の要求に基づいて決定」は11.8%となっている。これらの値は、いずれも前間のシステム監査対象の決定と近似している。

その他の意見は「Q31. 監査対象の決定」とほとんど同じ内容であった。

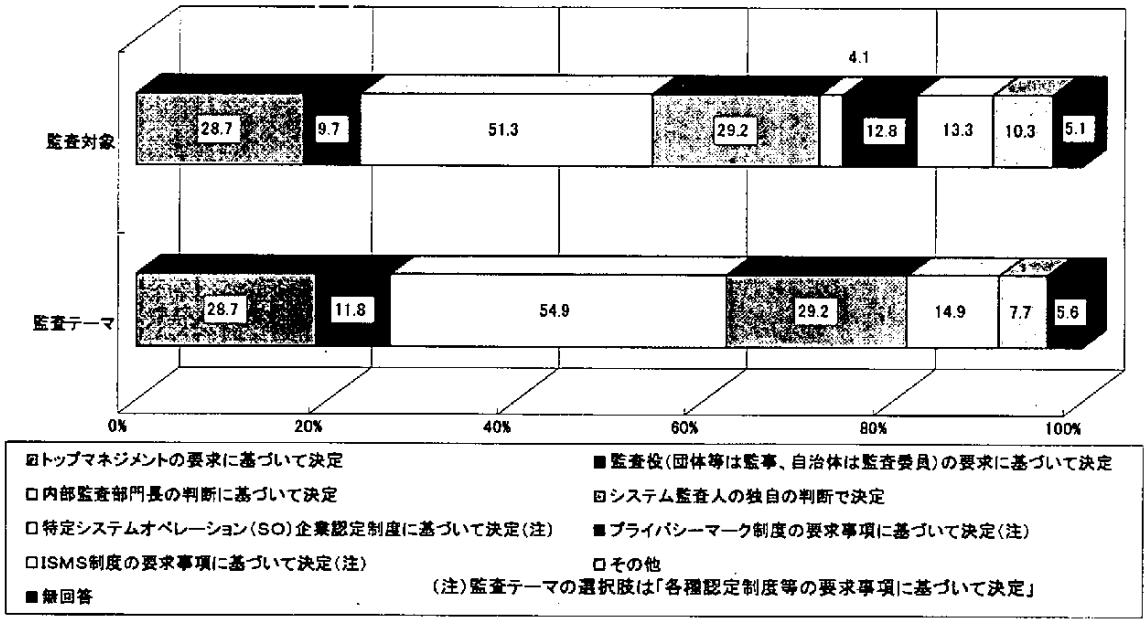

図3－1－11. システム監査対象／テーマの決定要件(監査担当部門)

Q33. 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	88	45.1	→Q35へ
2	いない	99	50.8	
無回答		8	4.1	→Q35へ
計		195	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45.1%が策定している。前回調査では50.0%であり、若干の減少となった。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、事業体における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。

Q34. 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		99	-
1	必要性がない	2	2.0
2	個別計画書だけで十分である	3	3.0
3	内部監査計画に含まれている	31	31.3
4	システム監査基本計画書作成のルールがない	20	20.2
5	外部に委託しているので作成していない	24	24.2
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	25	25.3
7	その他	3	3.0
無回答		3	3.0

システム監査の基本(年度)計画書を策定していない事業体に対して、その理由を調査した。その結果、「内部監査計画に含まれる」(31.3%)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。

Q35. 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	172	88.2
2	いない	13	6.7
無回答		10	5.1
計		195	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。88.2%が「通知している」とし、「通知していない」の6.7%を大きく上回っている。前回調査では、「通知している」が90.1%であり、1.9ポイント減少した。前々回調査まで、通知をしていない回答(約30%前後)の割合が高かった業種である金融業は、前回調査で15.6%であったが、今回調査も17.4%と低かった。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表れていたが、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　システム監査の実施について

Q36. 過去２年以内にシステム監査を実施しましたか。

1	した(実施中を含む)	171	87.7	
2	しない	23	11.8	→Q65へ
無回答		1	0.5	
計		195	100.0	

Q22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46.3%であったが、このうち、過去２年以内にシステム監査を実施した事業体は87.7%と、９割近くが監査を実施している。

過去２年以内に監査を実施した状況を業種別にみると、２年以内に限定しない過去の実施状況と同様、金融業（95.7%）、情報処理サービス業・ソフトウェア業（92.3%）、電気機械器具製造業（91.7%）、生命保険業（85.7%）、化学工業（80.0%）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。

Q37. 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		171	-	
1	内部監査部門型(監査部、検査部等が実施)	104	60.8	
2	部門監査型(情報システム部門が実施)	13	7.6	
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	2.9	→Q40へ
4	委員会方式(システム監査委員会を設置して実施)	6	3.5	
5	チームアプローチ(システム監査プロジェクトチームを編成して実施)	12	7.0	
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)	68	39.8	→Q38へ
7	その他	7	4.1	→Q40へ
無回答		4	2.3	

過去２年以内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、60.8%が「内部監査部門型（監査部、検査部等が実施)」となっており、次いで「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)」（39.8%）となっている。前回調査に比較して外部委託型が6.5ポイント増（前回調査33.3%)、内部監査部門型は9.5ポイント減（前回調査70.3%）となっている。

一方、「部門監査型（情報システム部門で実施)」（7.6%)、「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編成して実施)」（7.0%)、「委員会方式(システム監査委員会を設置して実施)」（3.5%)、「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)」（2.9%）の各方式は少ない。

その他の意見として、「会計監査の一環として実施」等が多かった。

Q38.（Q37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	32	47.1
2	いいえ	3	4.4
3	わからない	32	47.1
無回答		1	1.5
計		68	100.0

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、ほとんどがシステム監査企業台帳登録企業であった。また、台帳登録企業か否かが不明の回答も約半数と多かった。

Q39. 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)	57	83.8
2	コンサルタント(個人／企業)	5	7.4
3	情報処理サービス業者	4	5.9
4	その他	0	0.0
無回答		1	1.5
複数回答		1	1.5
計		68	100.0

外部委託の場合の委託先の調査に関しては、圧倒的に「監査法人(公認会計士を含む)」(83.8%)が多かった。それ以外としては、「コンサルタント（個人／企業)」が7.4%、「情報処理サービス業者」が5.9%であった

Q40. 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（1～9）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	有効性	無回答	複数回答	計
企画業務	98	6	8	5	10	7	14	0	6	36	1	5	98
	57.3	6.1	8.2	5.1	10.2	7.1	14.3	0.0	6.1	36.7	1.0	5.1	100.0
開発業務	121	9	50	14	6	5	4	8	5	9	1	10	121
	70.8	7.4	41.3	11.6	5.0	4.1	3.3	6.6	4.1	7.4	0.8	8.3	100.0
運用業務	157	50	39	31	9	1	1	1	5	2	3	15	157
	91.8	31.8	24.8	19.7	5.7	0.6	0.6	0.6	3.2	1.3	1.9	9.6	100.0
保守業務	109	31	42	9	6	1	2	2	2	4	1	9	109
	63.7	28.4	38.5	8.3	5.5	0.9	1.8	1.8	1.8	3.7	0.9	8.3	100.0
無回答	5												
	2.9												
回答件数	171												
	－												

過去２年以内にシステム監査を実施した監査担当部門に、Q40、Q41 でシステム監査実施業務を調査した。Q40 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」の各業務の実施状況、および実施業務に対し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 57.3%（前回調査 54.3%）、「開発業務」が 70.8%（前回調査 70.3%）、「運用業務」が 91.8%（前回調査 89.1%）、「保守業務」が 63.7%（前回調査 61.6%）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いずれの業務もシステム監査の実施率が増加している。

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、今回調査から新たな選択肢とした「有効性」が 36.7%と圧倒的に高く、次いで「適時性」が 14.3%、「準拠性」が 10.2%であった。前回調査で 24.0%の回答と最も高かった「採算性」は今回調査では 7.1%と低く、全体の５番目であった。前回調査で「採算性」として回答した中に、今回調査では新設された選択肢「有効性」に回答した割合が多かったと見られる。「有効性」、「適時性」、「準拠性」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」（41.3%）で回答の約４割を占めている。前回の調査でもトップであったが、そのときの 39.2%よりさらに高い割合を占めている。次いで前回調査で 5.2%で６位であった「機密性」（11.6%）となっている。３番目である「安全性」の 7.4%とともに、これは個人情報保護を始めとする情報システムのセキュリティの重要視の現われと見られる。前回調査で開発業務で重要視する項目として高かった「準拠性」は 12.4%から 5.0%へ、「生産性」は 11.3%から 6.6%と低くなっている。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」（31.8%）、「信頼性」（24.8%）、「機密性」（19.7%）の順となった。前回調査ではトップが「安全性」（42.3%）、「信頼性」（19.5%）であり、次いで「機密性」（13.8%）と、今回調査では安全性が 10.5 ポイントも減少したのに対し、信頼性が 5.3 ポイント増、同じく機密性が 5.9 ポイント増となった。安全性が低くなったもののデータの保護を主体とした機密性が増加していることは運用業務では情報セキュリティ対策の必要性が強くなっていることの表れであるといえよう。

保守業務では、「信頼性」が最も多く 38.5%である。次いで「安全性」が 28.4%であり、ここでは前回調査より信頼性が 2.7 ポイント減少したのに対し、安全性が 1.2 ポイント増加した。

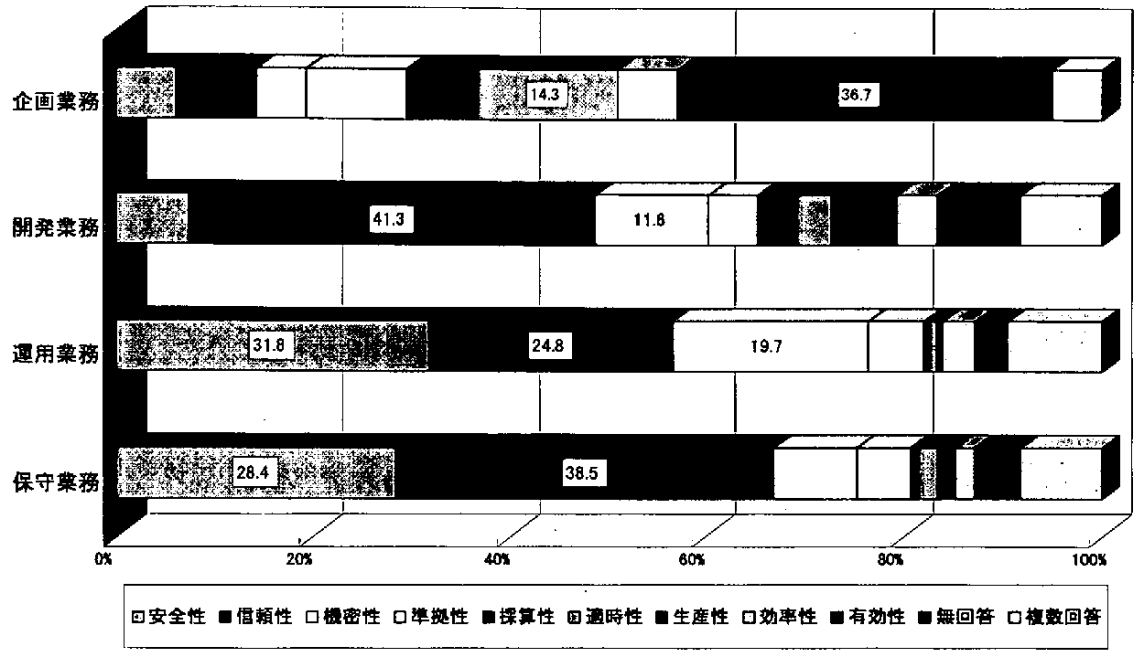

図3－1－12. システム監査で重視した着眼点(業務別－監査担当部門)

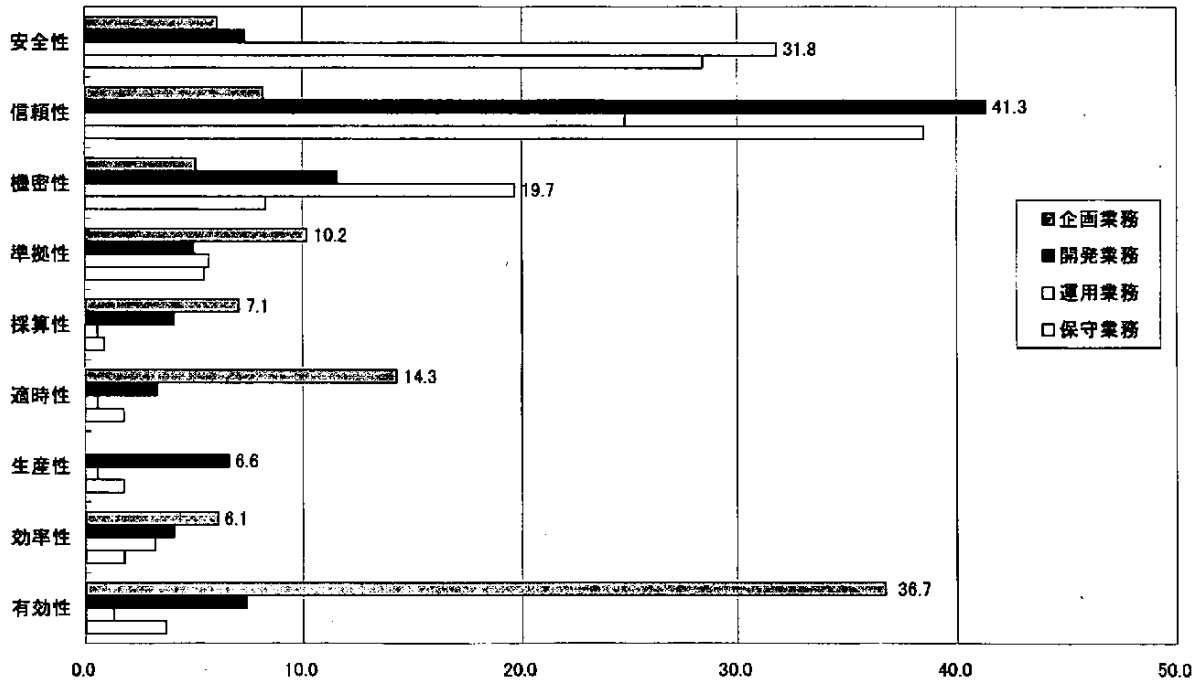

図3－1－13. システム監査で重視した着眼点(監査担当部門)

Q41. 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（1～9）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	171	-
ドキュメント管理	100	58.5
進捗管理	79	46.2
品質管理	88	51.5
コスト管理	67	39.2
要員管理	67	39.2
外部委託(開発の委託)	89	52.0
外部委託(アウトソーシング)	91	53.2
セキュリティ対策	144	84.2
ネットワーク管理	100	58.5
ソフトウェアの適正利用(ライセンス管理)	80	46.8
個人情報保護対策	99	57.9
PC管理、モバイル機器管理	94	55.0
コンピュータウイルス対策	106	62.0
情報システム関連のリスク管理	99	57.9
災害対策	99	57.9
無回答	7	4.1

今回調査も、「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」(84.2%)の監査であり、情報システムの機密性、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、「コンピュータウイルス対策」(62.0%)、「個人情報保護対策」(57.9%)、「情報システム関連のリスク管理」(57.9%)、「災害対策」(57.9%)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	有効性	無回答	複数回答	計
ドキュメント管理	5	25	12	38	1	1	1	5	9	1	2	100
	5.0	25.0	12.0	38.0	1.0	1.0	1.0	5.0	9.0	1.0	2.0	100.0
進捗管理	2	10	0	7	0	21	9	13	14	2	1	79
	2.5	12.7	0.0	8.9	0.0	26.6	11.4	16.5	17.7	2.5	1.3	100.0
品質管理	11	55	0	7	1	0	2	0	10	1	1	88
	12.5	62.5	0.0	8.0	1.1	0.0	2.3	0.0	11.4	1.1	1.1	100.0
コスト管理	0	2	0	2	33	0	6	12	10	1	1	67
	0.0	3.0	0.0	3.0	49.3	0.0	9.0	17.9	14.9	1.5	1.5	100.0

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	有効性	無回答	複数回答	計
要員管理	6	11	4	2	4	4	14	10	11	1	0	67
	9.0	16.4	6.0	3.0	6.0	6.0	20.9	14.9	16.4	1.5	0.0	100.0
外部委託(開発の委託)	8	32	24	5	5	2	2	7	1	2	1	89
	9.0	36.0	27.0	5.6	5.6	2.2	2.2	7.9	1.1	2.2	1.1	100.0
外部委託(ｱｳﾄｿｰｼﾝｸﾞ)	21	22	26	6	5	0	1	4	1	2	3	91
	23.1	24.2	28.6	6.6	5.5	0.0	1.1	4.4	1.1	2.2	3.3	100.0
セキュリティ対策	56	15	51	3	0	0	0	1	10	1	7	144
	38.9	10.4	35.4	2.1	0.0	0.0	0.0	0.7	6.9	0.7	4.9	100.0
ネットワーク管理	39	28	20	1	0	2	0	4	2	1	3	100
	39.0	28.0	20.0	1.0	0.0	2.0	0.0	4.0	2.0	1.0	3.0	100.0
ｿﾌﾄｳｪｱの適正利用(ﾗｲｾﾝｽ管理)	8	7	4	49	0	3	0	0	7	1	1	80
	10.0	8.8	5.0	61.3	0.0	3.8	0.0	0.0	8.8	1.3	1.3	100.0
個人情報保護対策	14	4	58	14	0	0	0	0	4	1	4	99
	14.1	4.0	58.6	14.1	0.0.	0.0	0.0	0.0	4.0	1.0	4.0	100.0
PC管理、モバイル機器管理	29	8	34	11	0	3	0	2	2	1	4	94
	30.9	8.5	36.2	11.7	0.0	3.2	0.0	2.1	2.1	1.1	4.3	100.0
コンピュータウイルス対策	65	12	8	4	0	3	0	0	10	1	3	106
	61.3	11.3	7.5	3.8	0.0	2.8	0.0	0.0	9.4	0.9	2.8	100.0
情報システム関連のリスク管理	39	22	8	7	0	3	0	1	13	1	5	99
	39.4	22.2	8.1	7.1	0.0	3.0	0.0	1.0	13.1	1.0	5.1	100.0
災害対策	65	7	0	2	0	6	0	0	14	1	4	99
	65.7	7.1	0.0	2.0	0.0	6.1	0.0	0.0	14.1	1.0	4.0	100.0

過去２年以内にシステム監査を実施した監査担当部門に、監査実施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 38.0%とトップであった。前回調査でも「準拠性」が 50.0%と圧倒的に高かったが、今回は 12.0 ポイント減少し、「信頼性」が 25.0%となっている。準拠性重視は、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 26.6%でトップであり、次いで「有効性」(17.7%)、「効率性」(16.5%)、「信頼性」(12.7%)、「生産性」(11.4%) 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」が最も重要視され 36.0%、アウトソーシングでは「機密性」(28.6%) 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。

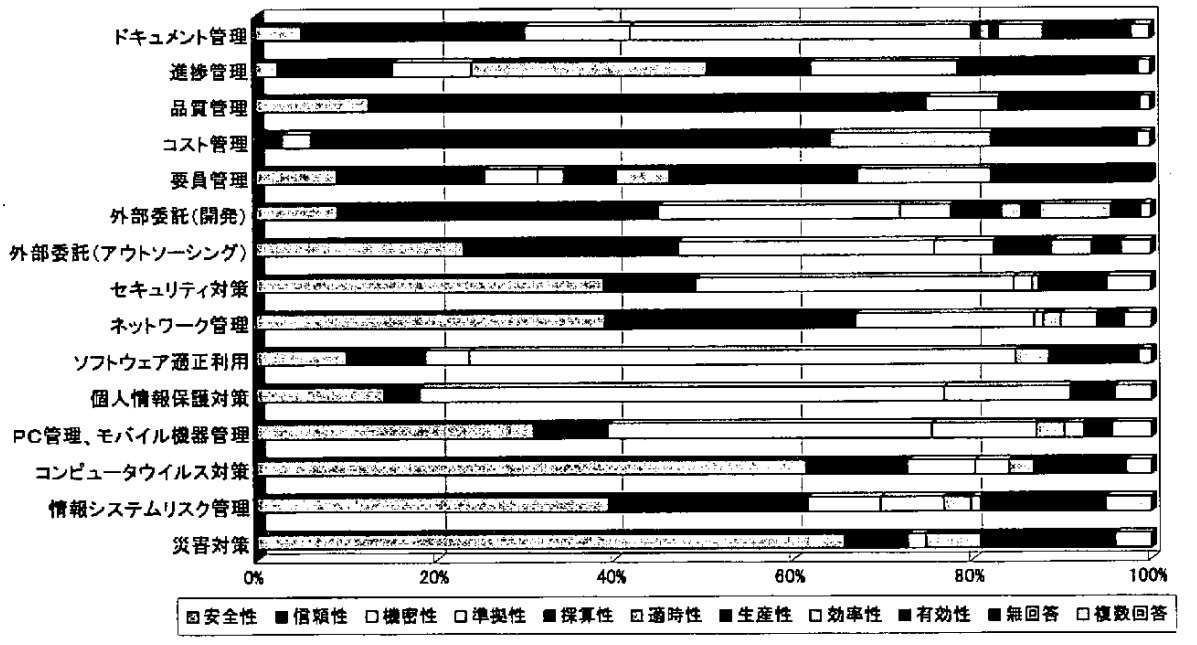

図3－1－13. システム監査で重視した着眼点(テーマ別－監査担当部門)

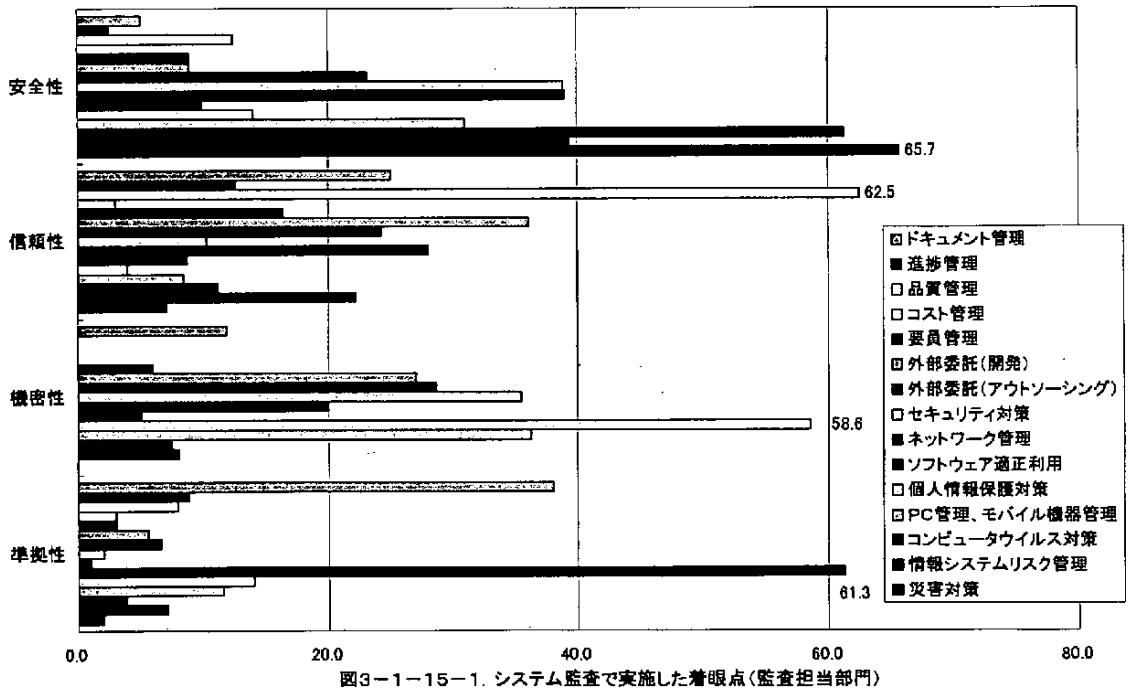

図3－1－15－1. システム監査で実施した着眼点(監査担当部門)

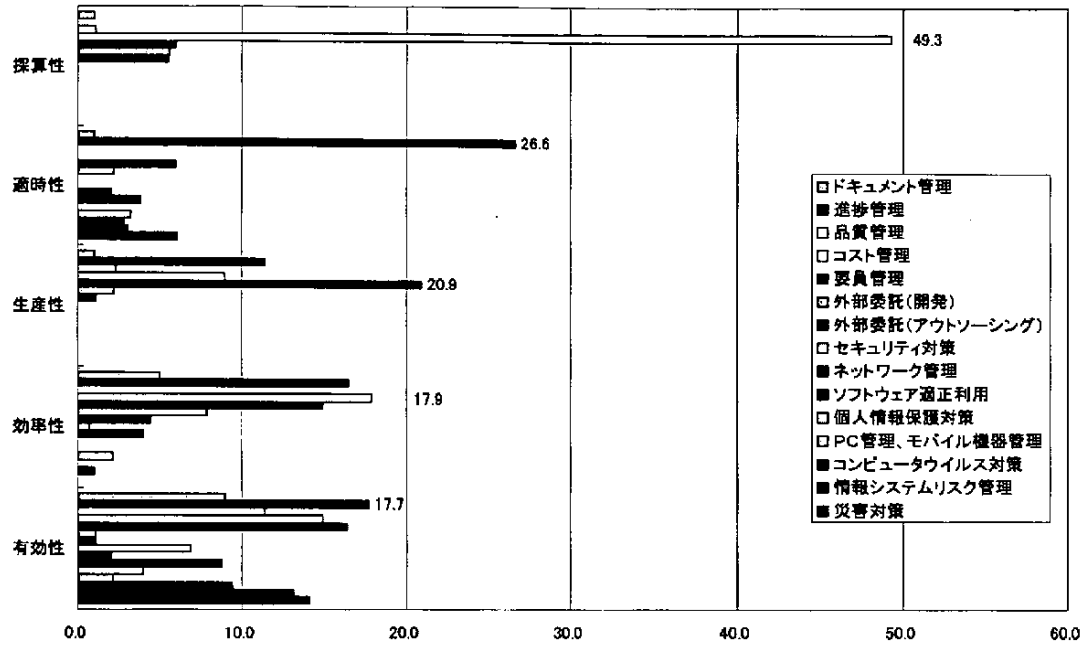

図3－1－15－2. システム監査で重視した着眼点(監査担当部門)

Q42. 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。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(注1)	ソフトウエア(注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	17	6	4	7	11	64	23	6	0	10	13	0	7	3	171
	9.9	3.5	2.3	4.1	6.4	37.4	13.5	3.5	0.0	5.8	7.6	0.0	4.1	1.8	100.0
ヒューマンエラー防止	40	14	4	9	65	5	2	18	0	4	0	0	7	3	171
	23.4	8.2	2.3	5.3	38.0	2.9	1.2	10.5	0.0	2.3	0.0	0.0	4.1	1.8	100.0
事故防止	3	10	1	17	40	11	9	23	17	9	10	10	9	2	177
	1.8	5.8	0.6	9.9	23.4	6.4	5.3	13.5	9.9	5.3	5.8	5.8	5.3	1.2	100.0
災害対策	0	4	0	1	9	35	1	2	38	4	25	41	9	2	177
	0.0	2.3	0.0	0.6	5.3	20.5	0.6	1.2	22.2	2.3	14.6	24.0	5.3	1.2	100.0
個人情報保護	2	2	9	0	9	122	10	3	1	2	3	0	6	2	177
	1.2	1.2	5.3	0.0	5.3	71.3	5.8	1.8	0.6	1.2	1.8	0.0	3.5	1.2	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、事故防止、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、行為に関して調査した。

コンピュータ犯罪防止では、「情報保管（データ管理）」（37.4%）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71.3%と高かった。

ヒューマンエラー防止では、「オペレーション」（38.0%）、「データの入力プロセス」（23.4%）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」（23.4%）、「システム開発」（13.5%）が高くなっている。

災害対策では「電源設備」（24.0%）、「ハードウェア」（22.2%）、「情報保管（データ管理）」（20.5%）、「ネットワーク」（14.6%）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。

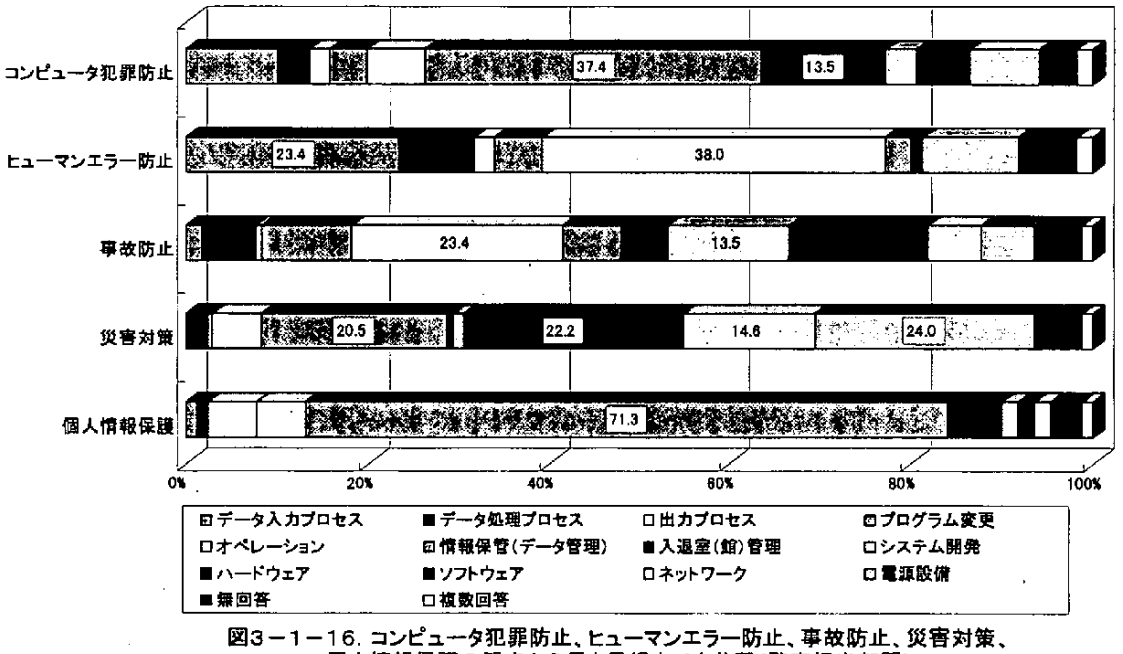

図3－1－16. コンピュータ犯罪防止、ヒューマンエラー防止、事故防止、災害対策、個人情報保護の観点から最も重視すべき分野（監査担当部門）

Q43. システム監査を実施する際に、どのような基準類を利用しましたか。(複数回答)

回答件数		171	-
1	システム監査基準	92	53.8
2	システム管理基準	39	22.8
3	情報セキュリティ監査基準	60	35.1
4	情報セキュリティ管理基準	48	28.1
5	情報システム安全対策基準	55	32.2
6	コンピュータウイルス対策基準	45	26.3
7	コンピュータ不正アクセス対策基準	41	24.0
8	プライバシーマーク監査ガイドライン	33	19.3
9	ISMSガイド	44	25.7
10	その他	46	26.9
無回答		13	7.6

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。

従来までシステム監査の分野では経済産業省の「システム監査基準」が策定されていたが、平成16年10月にこれまでの基準が「システム監査基準」と「システム管理基準」に分割された。その結果、前回調査では72.5%であった「システム監査基準」が53.8%となり、新たな選択肢「システム管理基準」が22.8%との回答となった。

「システム監査基準」と「システム管理基準」の合計に次いで多いのが平成15年4月に公表された「情報セキュリティ監査基準」(35.1%)となっている。この「情報セキュリティ監査基準」と対をなすのが「情報セキュリティ管理基準」で28.1%であった。

前回調査まで「システム監査基準」に次いで活用されていた「情報システム安全対策基準」は32.2%であった。同基準は前回調査では61.6%であり、29.4ポイントと大きく減少した。これは前出の「情報セキュリティ管理基準」の公表の影響と思われる。

「コンピュータウイルス対策基準」(26.3%)や「コンピュータ不正アクセス対策基準」(24.0%)も前回調査に比較して大きく減少している。

一方、「ISMS ガイド」(25.7%)、「プライバシーマーク監査ガイドライン」(19.3%)は、特定の分野(セキュリティ全般およびプライバシー保護)を対象としたものであり、他の基準に比較して活用度はやや低くなっている。

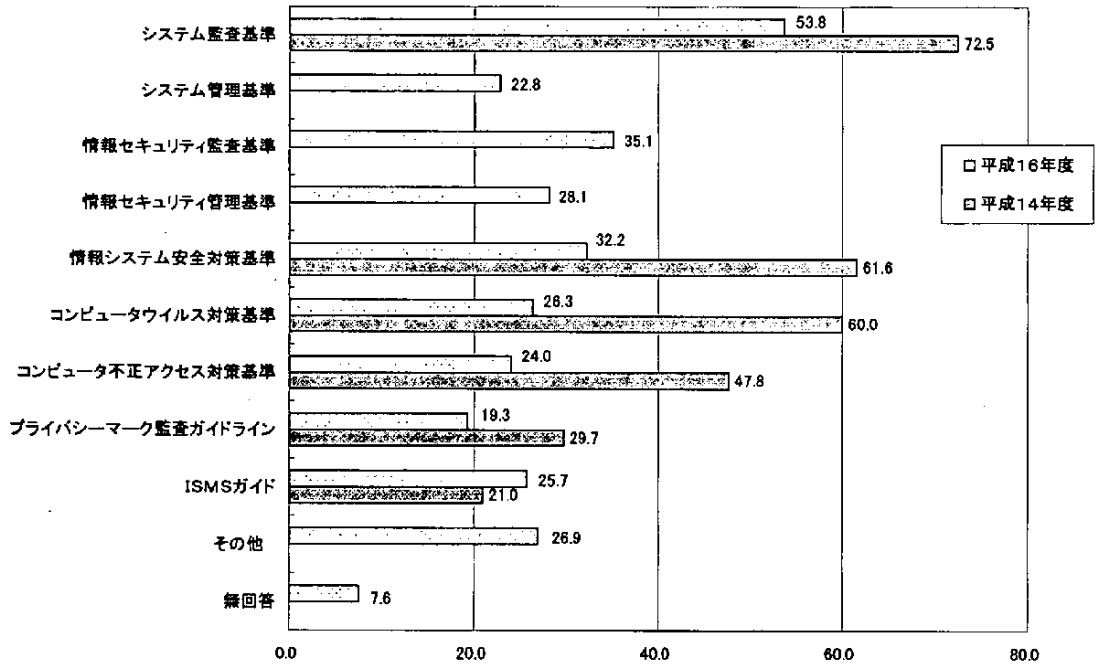

図3－1－17. システム監査実施時の利用基準類(監査担当部門)

Q44. 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	108	63.2
2	いない	59	34.5
無回答		4	2.3
計		171	100.0

システム監査の実施では何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作成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。

「作成している」は63.2%と高く、「作成していない」は34.5%であった。これは前回調査に対して、「作成している（前回調査77.5%)」が14.3ポイント減少したのに対し、「作成していない」（前回調査21.0%）は13.5ポイント増加した。

Q45からQ54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。

Q45. 貴事業体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	13	7.6
2	やや十分だと思う	54	31.6
3	普通だと思う	65	38.0
4	やや不十分だと思う	25	14.6
5	不十分だと思う	11	6.4
6	わからない	2	1.2
無回答		1	0.6
計		171	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である信頼性は、「十分だと思う」(7.6%)、「やや十分だと思う」(31.6%)の回答で約4割を占めた。一方、「やや不十分である」(14.6%)、「不十分と思う」(6.4%) は合計約2割となっており、信頼性を評価する割合が多くなっている。

Q46. 貴事業体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	157	91.8
2	思わない	4	2.3
3	わからない	9	5.3
無回答		1	0.6
計		171	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91.8%ときわめて高い。

Q45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」と監査担当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。

Q47. 貴事業体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	109	63.7
2	思わない	26	15.2
3	わからない	35	20.5
無回答		1	0.6
計		171	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63.7%と高くなっている。

Q45 からQ47 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４割が信頼性は十分、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。

Q48. 貴事業体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	8	4.7
2	やや十分だと思う	53	31.0
3	普通だと思う	58	33.9
4	やや不十分だと思う	39	22.8
5	不十分だと思う	9	5.3
6	わからない	3	1.8
無回答		1	0.6
計		171	100.0

自然災害、不正アクセスおよび破壊行為等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」(4.7%)、「やや十分だと思う」(31.0%) をあわせると、信頼性と同様、約４割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 1.8 ポイントの減少(前回調査 6.5%)、「やや十分だと思う」は 10.3 ポイントの減少(前回調査 41.3%)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、辛い評価が増加している。

Q49. 貴事業体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	154	90.1
2	思わない	8	4.7
3	わからない	8	4.7
無回答		1	0.6
計		171	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。

Q50. 貴事業体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	118	69.0
2	思わない	24	14.0
3	わからない	28	16.4
無回答		1	0.6
計		171	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割がその必要性を考慮している。

Q51. 貴事業体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	5	2.9
2	やや十分だと思う	33	19.3
3	普通だと思う	73	42.7
4	やや不十分だと思う	41	24.0
5	不十分だと思う	14	8.2
6	わからない	4	2.3
無回答		1	0.6
計		171	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、監査担当部門は「十分だと思う」(2.9%)、「やや十分だと思う」(19.3%) とプラス面を評価する回答は全体の２割である。一方「やや不十分だと思う」(24.0%) と「不十分だと思う」(8.2%) は約３割であり、効率性に関しては、やや辛い評価となっている。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」(0.7%)、「やや十分であると思う」(29.7%) であり、今回は「やや十分であると思う」が減少し、全体的により厳しい見方となった。

Q52. 貴事業体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	148	86.5
2	思わない	9	5.3
3	わからない	13	7.6
無回答		1	0.6
計		171	100.0

効率性に関しても、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。

Q53. 貴事業体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	101	59.1
2	思わない	34	19.9
3	わからない	34	19.9
無回答		2	1.2
計		171	100.0

投資に関しても、信頼性と同様、効率性に対しても約８割がその必要性を回答している。

Q54. 貴事業体の情報システムは、総合的に見て満足できる状態ですか。

1	十分満足	0	0.0
2	満足	58	33.9
3	なんともいえない	59	34.5
4	多少不満	43	25.1
5	大いに不満	8	4.7
6	わからない	2	1.2
無回答		1	0.6
計		171	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。

前回調査で1.4%だった「十分に満足」は回答が１件もなく0%となった。「満足」(33.9%)と評価する割合が回答の約３分の１となっている。監査担当部門が評価した情報システムは、やや辛い評価になっている。

一方、「多少不満」(25.1%)、「大いに不満」(4.7%)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」(34.5%)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、何ともいえない。

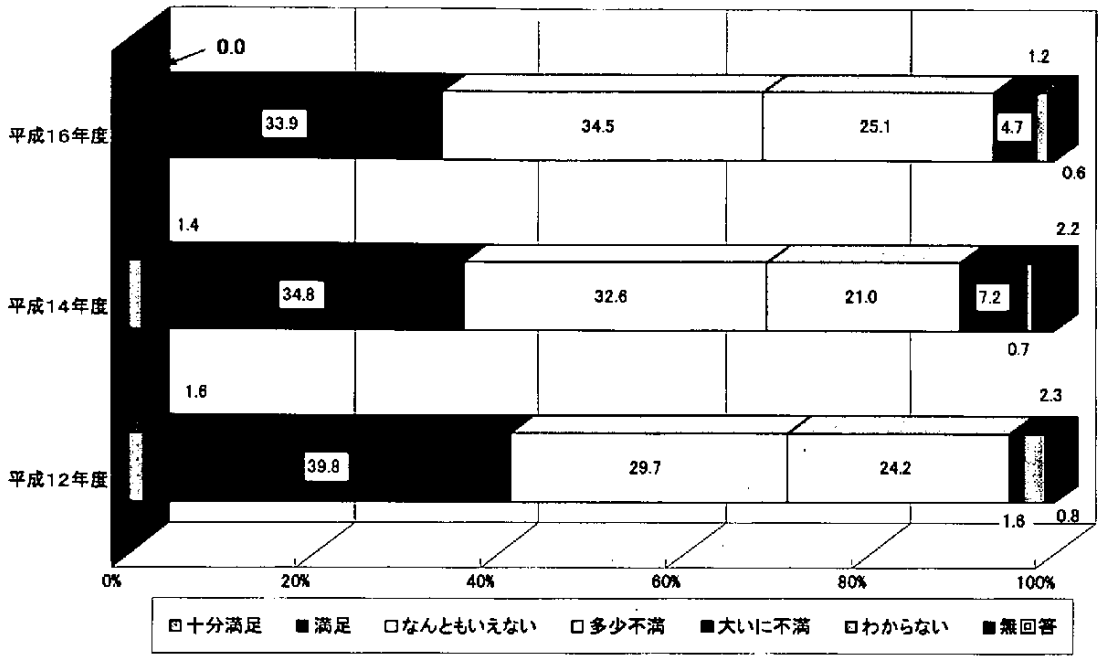

図3－1－18. 情報システムに対する評価(監査担当部門)

今回の調査ではQ55で講評会の開催状況を、Q56で監査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。

Q55. 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	138	80.7
2	行わなかった	30	17.5
無回答		3	1.8
計		171	100.0

講評会はシステム監査実施事業体の80.7%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84.2%であり、同様な値となっている。(被監査部門に関する分析（Q30）は、「3.2.2」を参照のこと)。

Q56. 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	113	66.1	
2	行わなかった	56	32.7	→Q58へ
無回答		2	1.2	
計		171	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3分の2の66.1%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66.0%であった（。被監査部門に関する分析（Q31）は、「3.2.2」を参照のこと）。この実施率は、過去の調査結果と大きな違いはない。

Q57. 監査報告会に出席したのは誰ですか。（複数回答）

回答件数		113	-
1	最高経営者(会長、社長、知事、市長等)	49	43.4
2	財務担当役員	18	15.9
3	情報システム担当役員	53	46.9
4	監査役	43	38.1
5	情報システム部門の管理者	75	66.4
6	内部監査人	66	58.4
7	ユーザ部門の管理者	41	36.3
8	外部のシステム監査人	11	9.7
9	その他	6	5.3
無回答		1	0.9

監査報告会への出席者は、「情報システム部門の管理者」（66.4%）、「内部監査人」（58.4%）、「情報システム担当役員」（46.9%）、「最高経営者」（43.4%）、「監査役」（38.1%）、「ユーザ部門の管理者」（36.3%）、「財務担当役員」（15.9%）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（73.5%）に比べ7.1ポイント減少している。また「最高経営者」も前回調査（45.9%）に対し、今回調査では43.4%と僅かではあるが減少した。

その他の回答としては、「監査報告はメールで代替している」、「(内部)監査部門の担当役員」、「公認会計士」等が挙げられた。

Q58. 監査報告書（原本）は誰に提出（報告書の宛先）しましたか。（単一回答）

注）複数部署に配布している場合は、その中での最高権限者を回答

1	最高意思決定機関(取締役会、理事会、議会等)	25	14.6
2	最高経営者(社長、理事長、首長等)	91	53.2
3	担当役員	30	17.5
4	監査役(団体等は監事、自治体は監査委員)	4	2.3
5	内部監査部門長	6	3.5
6	その他	8	4.7
無回答		6	3.5
複数回答		1	0.6
計		171	100.0

監査報告書の提出先については、「最高経営者」が 53.2%となっており、「担当役員」が 17.5%、「最高意思決定機関」が 14.6%である。この三者で約８割強となっている。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Q59～Q61 で調査した。

Q59. 監査報告書の写を被監査部門に配布しましたか。

1	し た	143	83.6
2	しない	24	14.0
無回答		4	2.3
計		171	100.0

「被監査部門への配布」について、前回調査では 94.2%とほとんどの事業体が配布していたのに対し、今回調査では 83.6%と約 10 ポイント減少した。とはいえ、こ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。

Q60. 監査報告書の写を監査役に配布しましたか。

1	し た	116	67.8
2	しない	49	28.7
無回答		6	3.5
計		171	100.0

「監査役への配布」（67.8%）となっており、前回調査の 71.7%と大きな変化はない。

Q61. 監査報告書の写を貴事業体の会計監査人に配布しましたか。

1	した	48	28.1
2	しない	117	68.4
無回答		6	3.5
計		171	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28.1%となっている。

3.1.4. 未実施および実施可能性について

Q62 からQ64 までは、Q22 でシステム監査を実施したことが「ない」と回答した 226 事業体からの回答結果を分析したものである。

Q62. 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	7	3.1
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	42	18.6
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	35	15.5
4	システム監査を実施する担当者(部門)の確保が難しい	50	22.1
5	システム監査の方法、制度、手続きなどが十分でない	37	16.4
6	システム監査の効果が明確でない	7	3.1
7	システム監査の必要性を感じない	15	6.6
8	アウトソーシングしているため	6	2.7
9	その他	15	6.6
無回答		6	2.7
複数回答		6	2.7
計		226	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、前回調査では「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」が 21.6%で回答のトップであったが、今回は 15.5%で４番目となった。代わってトップは「システム監査を実施する担当者（部門）の確保が難しい」(22.1%)、次いで「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」(18.6%)、「システム監査の方法、制度、手続き等が十分でない」(16.4%) となっている。しかしこれらの選択肢で、大きな差はない。

その他の回答としては、「システム監査よりも情報セキュリティ監査を優先している」、「監査部門を設置したばかりであり、これから実施予定である」といった意見が出された。

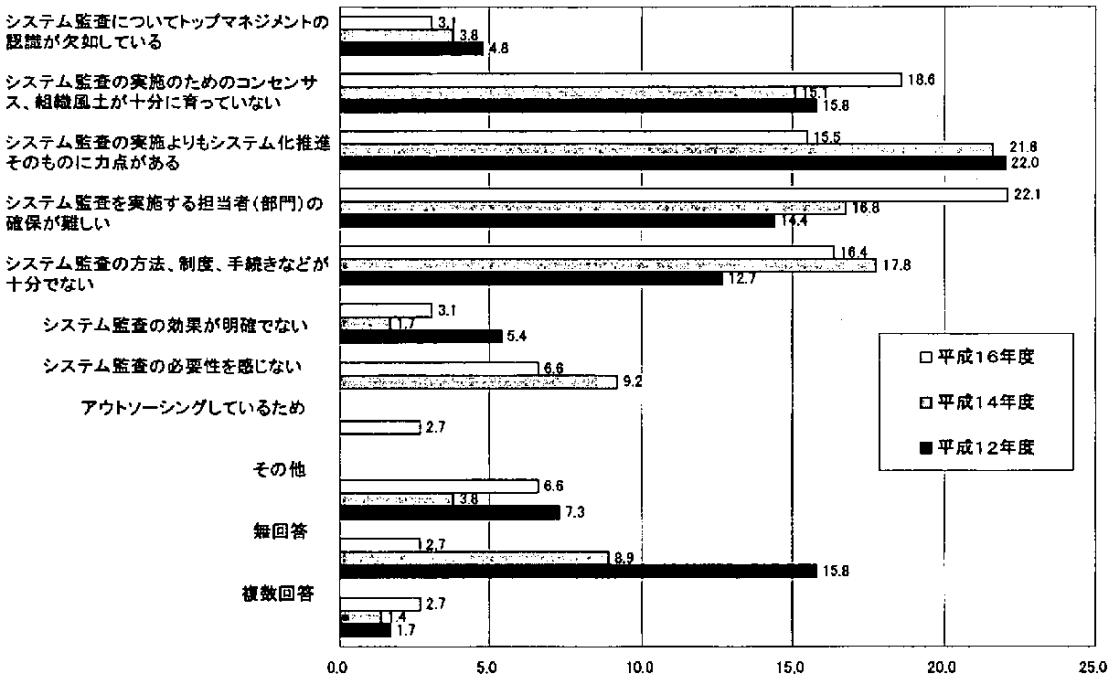

図3－1－19. システム監査未実施の理由(監査担当部門)

Q63. 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	25	11.1	
2	2～3年以内には導入の予定	48	21.2	
3	当面導入の予定はない	120	53.1	
4	将来とも導入の予定はない	9	4.0	→Q65へ
5	その他	17	7.5	
無回答		7	3.1	
計		226	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については、「現在、システム監査の導入を計画中」が11.1%（前回調査9.9%）、「2～3年以内には導入予定」が21.2%（前回調査16.8%）と、前回調査と比べそれぞれ1.2ポイント、4.4ポイント増加している。

一方、「当面導入の予定はない」は53.1%（前回調査55.8%）、「将来とも導入の予定はない」は4.0%（前回調査6.2%）と、あわせて57.1%の事業体がシステム監査導入を予定していない。

Q64. 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		90	-
1	内部監査部門型(監査部、検査部等が実施)	32	35.6
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)	17	18.9
3	決まっていない	45	50.0
無回答		2	2.2

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の予定は、「内部監査部門型」(35.6%)が多く、「外部委託型」(18.9%)となっている。また、半数が未定となっている。

3.1.5　情報セキュリティの推進について

Q65～Q72の質問については被監査部門に対しても同一の調査を行っているので、「3.2.4」を参照のこと。

Q65. 貴事業体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	255	60.6
2	現在作成中である	53	12.6
3	作成を検討している	69	16.4
4	現在、定める予定がない	34	8.1
無回答		10	2.4
計		421	100.0

情報セキュリティポリシーの策定状況について、今回調査では「定めている」が60.6%であり、「現在作成中」を含めると73.2%が、さらに、「作成を検討している」を含めると89.6%と9割近い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。なお、前回調査では、「定めている」が43.7%、「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%であった。すなわち、この2年間で10ポイント近く増えたことになる。同一の質問を被監査部門にも行っている（Q45）が、同様の結果が得られた。業種別に見ると、製造業では、「現在、定める予定がない」は16.3%であり、全体（8.1%）の2倍近い結果となった。とくに、食品・紙・パルプ・繊維・印刷や石油・化学・鉄鋼・非鉄・金属の業種では、20%以上が「定める予定がない」となっている。これらのインフラ型製造業では、個人情報の扱いやインターネット利用の必要がないことなどによるものと考えられる。

なお、前回調査では、監査部門と被監査部門の回答で大きく結果が違っており、監査部門の方が、意識が高いと論じた。しかし、今回は両部門ともに「策定している（検討中を含む）」が89.6%となり、両部門での認識の差は解消されつつあるといえよう。

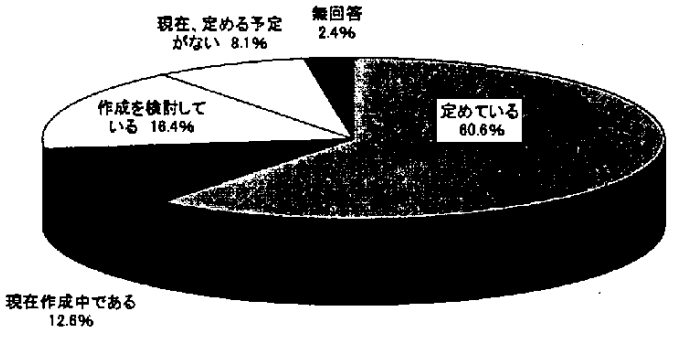

図3－1－20. 情報セキュリティポリシーの策定状況
（平成16年度－監査担当部門）

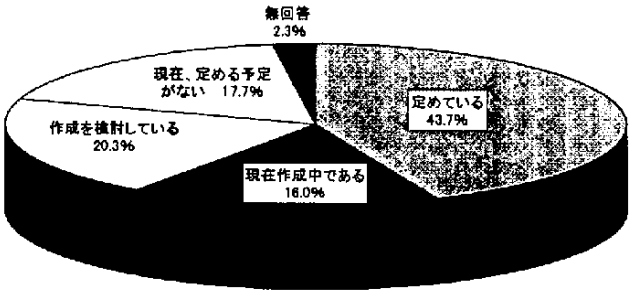

図3－1－21. 情報セキュリティポリシー策定状況
（平成14年度－監査担当部門）

Q66. 貴事業体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		421	-
1	情報セキュリティ担当役員を設置している	125	29.7
2	情報セキュリティ委員会を設置している	144	34.2
3	情報システム部門主導で実施している	212	50.4
4	情報セキュリティ専任者を設置している	64	15.2
5	各部門・拠点にセキュリティ担当者を設置している	129	30.6
6	外部のセキュリティコンサルタントを活用している	30	7.1
7	特に実施していない	54	12.8
8	その他	13	3.1
無回答		15	3.6

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。

情報セキュリティ推進体制について、「情報セキュリティ担当役員の設置」は前回調査の19.4%から29.7%へ、「情報セキュリティ委員会の設置」は前回調査の23.0%から34.2%へ、両者ともに10ポイント増加している。

一方、「情報システム部門主導で実施している」(50.4%)は、前回調査(50.6%)とほぼ横ばいの状況である。これらの結果から、平成14年度調査時には、「情報セキュリティ担当役員」や「情報セキュリティ委員会」の設置状況が低い状況にあると述べた。しかし、この2年で大きく変わったといえよう。事業体が情報セキュリティの重要性をより強く認識するようになり、情報セキュリティ対策が情報システム部門から経営陣に移りつつあることがわかる。

なお、「情報セキュリティ専任者」(今回:15.2%、前回:13.7%)、「外部セキュリティコンサルタントの活用」(今回:7.1%、前回:6.5%)はあまり変化がみられない。一方、「各部門・拠点ごとのセキュリティ担当者の設置」については前回調査の21.5%から30.6%と約9ポイント増加している。これは、被監査部門の「情報セキュリティ専任者」(16.8%)、「各部門・拠点ごとのセキュリティ担当者の設置」(30.8%)とほぼ同様の傾向であった。

全体としては、長い間、情報システム部門に依存してきた流れが大きく変わろうとしている転機点に差しかかっていることがわかる。すなわち、情報セキュリティは、情報システム部門の所掌するものではなく、全社的なものとなった。今後は、経営者が関与するようになり、より、ガバナンス面からの情報セキュリティ対策が進むことは望ましいと考えられる。監査担当部門も、これからは、情報セキュリティについて経営者により強く実施を求める時代になってきたといえ

よう。米国の経営者は、SOX(企業改革法)への準拠で内部統制の観点から、経営者に情報セキュリティ対策を求めている。日本でも、今後、同様な動きが出てくると考えられており、経営者が情報セキュリティについてより関与するようになるのは自然な動向なのかもしれない。

この傾向は、被監査部門ではより鮮明にみられる。(被監査部門に関する分析（Q46）は、「3.2.4」を参照のこと)。

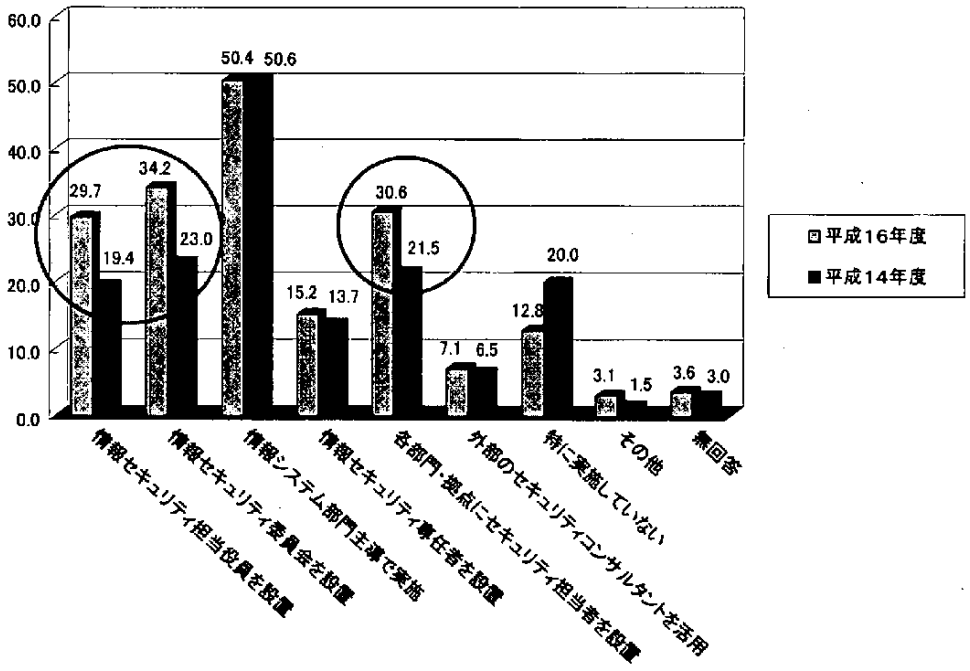

図3－1－22. 情報セキュリティ推進体制(監査担当部門)

Q67. 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	89	21.1
2	全社的な推進体制	215	51.1
3	情報システム部門の推進体制	20	4.8
4	利用部門の理解･協力	75	17.8
5	その他	3	0.7
無回答		4	1.0
複数回答		15	3.6
計		421	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51.1%と最も多く、「経営者のリーダーシップ」(21.1%）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。なお、この傾向は前回調査のそれぞれ、51.3%、17.3%と比べてほとんど変化していない。

わが国では経営者のリーダー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17.8%（前回調査19.8%、２ポイント減少)、被監査部門19.9%と、「情報システム部門の推進体制」は4.8%（前回調査は7.4%で2.6ポイント減少）しており、情報システム部門主導が少しずつ変わりつつあることがわかる。

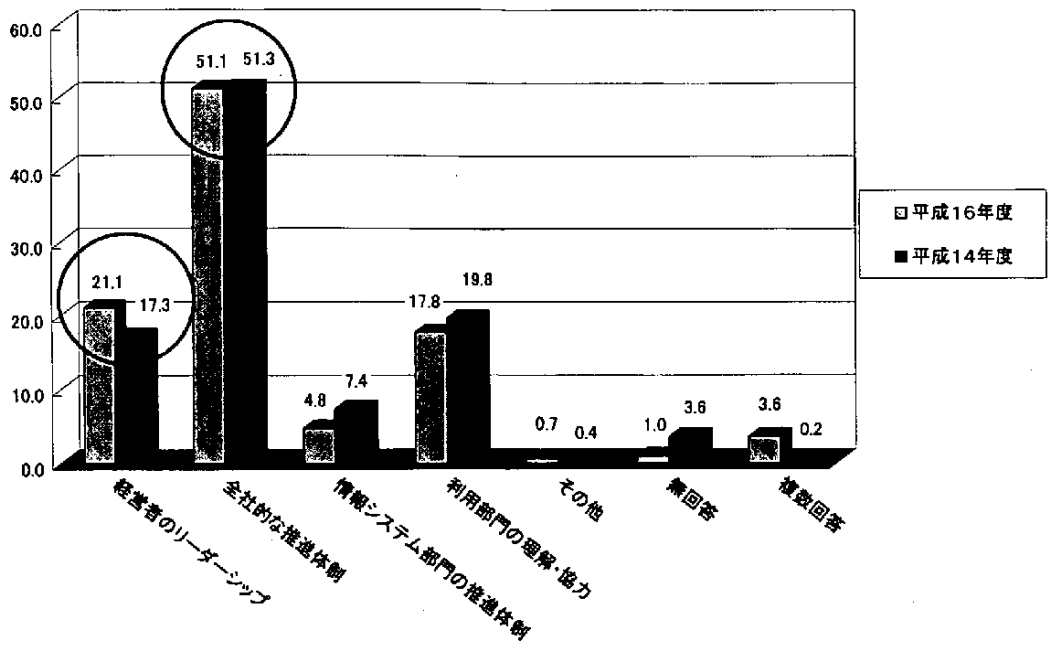

図3－1－23. 情報セキュリティ推進にあたっての意識(被監査部門)

Q68. 貴事業体で情報セキュリティについて、優先的に実施していることを３つまで選んで下さい。(複数回答)

回答件数		421	
1	情報セキュリティ対策コストの確保	67	15.9
2	リスク分析の実施	118	28.0
3	システム監査の実施	53	12.6
4	情報セキュリティ監査の実施	68	16.2
5	情報セキュリティ教育の実施	183	43.5
6	情報セキュリティ体制の確立	196	46.6
7	情報セキュリティアドミニストレータの確保	9	2.1
8	情報資産の洗い出し	123	29.2
9	ISMS の取得	33	7.8
10	プライバシーマークの取得	54	12.8
11	その他	10	2.4
12	特に実施していない	44	10.5
無回答		15	3.6
複数回答(4つ以上を選択)		4	1.0

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。

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」(46.6%)、「情報セキュリティ教育」(43,5%)、「情報資産の洗い出し」(29.2%)、「リスク分析」(28.0%)、「情報セキュリティ監査の実施」(16.2%)、「情報セキュリティ対策コストの確保」(15.9%)、「システム監査」(12.6%)の順となっている。前回調査との大きな違いは、「特に実施していない」が前回調査の22.4%から10.5%と半減しており、情報セキュリティに対する関心が高まっていることがわかる。

前回調査と比較すると、大きく増加したのは「情報セキュリティ教育の実施」(前回:35.9%、7.6ポイント増)、「情報資産の洗い出し」(前回:16.5%、12.7ポイント増)、「リスク分析」(前回:23.2%、4.8ポイント増)、「プライバシーマークの取得」(前回:5.7%、7.1ポイント増)である。一方、「情報セキュリティ対策コストの確保」(前回:18.6%、2.7 ポイント減)、「システム監査の実施」(前回:18.6%、6.0ポイント減少)、「情報セキュリティ体制の確立」(前回:50.8%、4.2ポイント減)となった。

この変化は、この2年間に情報セキュリティ監査制度が確立したこと、これに伴ってシステム監査の位置づけも変わったためである(今回調査では、「情報セキュリティ監査の実施」(16.2%)が「システム監査の実施」(12.6%)よりも3.6ポイント高い。これは、インターネットの利用が企業の95%を超えた現在、どの企業にとっても情報セキュリティ対策が必須のものとなったためであり、きわめて妥当なものである。

なお、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:15.9%、被:24.1%)と「情報セキュリティ監査」(監査:16.2%、被:10.1%)については回答に差がでている。これは、監査担当部門の場合、情報セキュリティ監査実施という立場から、コントロールを高める必然性を強く認識しているものと思われる。

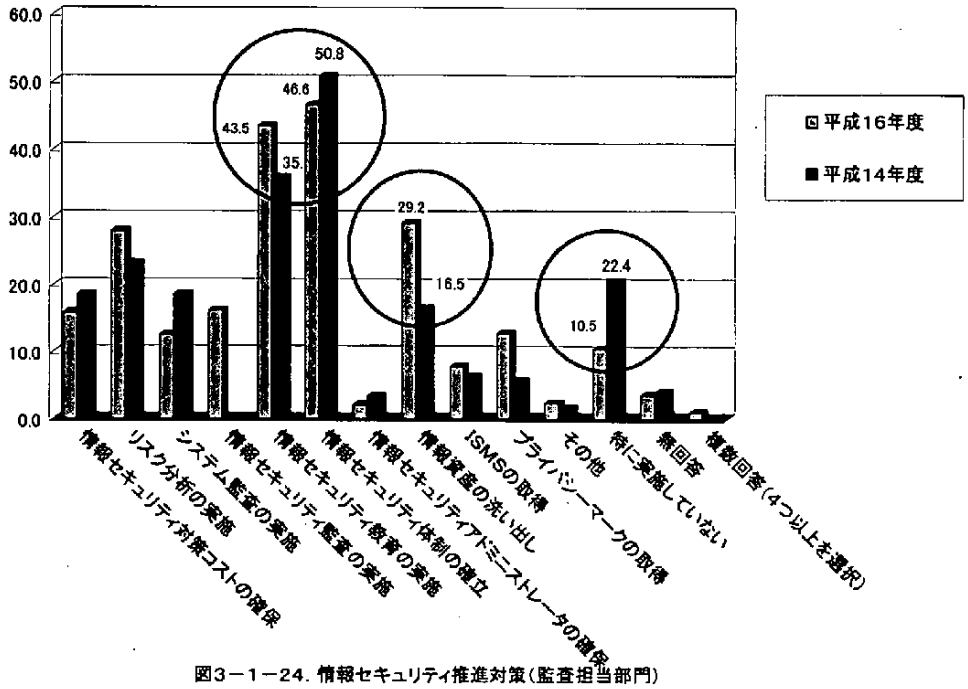

図3－1－24. 情報セキュリティ推進対策(監査担当部門)

Q69. 貴事業体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		421	-
1	新入社員教育を実施している	137	32.5
2	一般社員向け教育を実施している	231	54.9
3	管理職教育を実施している	139	33.0
4	役員教育を実施している	37	8.8
5	派遣要員向け教育を実施している	57	13.5
6	情報セキュリティ担当者の専門教育を実施している	50	11.9
7	その他	24	5.7
8	特に実施していない	102	24.2
無回答		15	3.6

今回の調査結果を前回調査と比べると、「新入社員教育を実施している」が、25.3%から 32.5%へと 7.2 ポイント増加し、「一般社員向け教育を実施している」が、35.9%から 54.9%へと 19 ポイント増加した点である。同様に、数値的には大きくはないが、「管理職教育を実施している」が、19.2%から 33.0%へと 13.8 ポイント増、「役員教育を実施している」が、3.6%から 8.8%へと 5.2 ポイント増となっている。すなわち、情報セキュリティ教育は、新人、社員、管理職、役員など、すべての事業体構成員向けの教育が重視されてきているといえよう。一方、専門家向けの「情報セキュリティ担当者の専門教育を実施している」では、前回調査の 11.0%から 11.9%へとほとんど増えていない。これは、情報セキュリティについては、専門家よりも、一般社員、経営者、管理職などがより知ることが重視されていることがわかる。すなわち、事業体で一人一台のパソコン環境が実現され、またインターネット接続が企業の 95%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、すべての従業員や事業体の構成員の守るべきことになったといえよう。

以上のことから、より、一般がわかる情報セキュリティの教材が必要になっている。情報セキュリティの監査でも、全従業員を対象にした情報セキュリティマネジメントを大きなターゲットとする必要がある。

その他の回答としては、「一般、管理職向け教育は部分的に実施しているため、全社展開を必要と感じている」、「勉強会の実施」、「各部門のシステム担当者向け教育の実施」等があげられた。

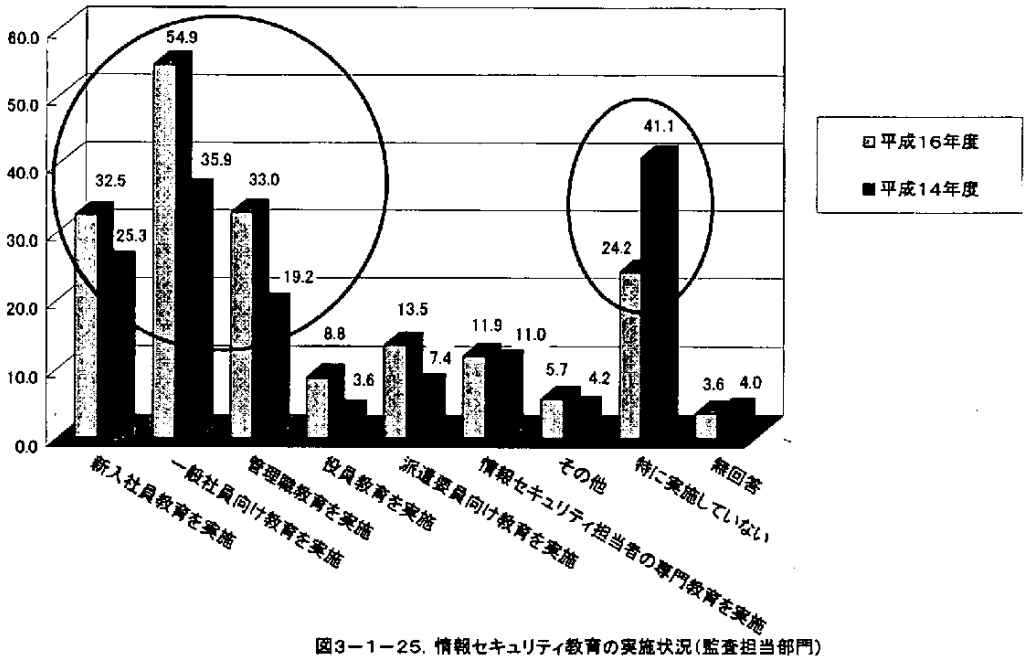

図3－1－25. 情報セキュリティ教育の実施状況(監査担当部門)

Q70. 貴事業体では情報セキュリティ監査を実施したことがありますか。

1	ある	121	28.7
2	これから実施する予定がある	61	14.5
3	ない	224	53.2
無回答		15	3.6
計		421	100.0

今回調査では、「情報セキュリティ監査の実施」について調査した。情報セキュリティ監査制度は平成15年度に導入されており、2年目となる16年度にどの程度の事業体が実施したかについて調査した。その結果からは、28.7%の事業体が「ある」と答えており、また、「これから実施する予定がある」の14.5%を合計すると、43.2%が監査実施の意向を示している。情報セキュリティ監査制度は各事業体に好意的に受け入れられているといえよう。ただし、被監査部門の28.2%と比べると高く、この違いは監査部門という特殊性を考慮する必要があるかもしれない。

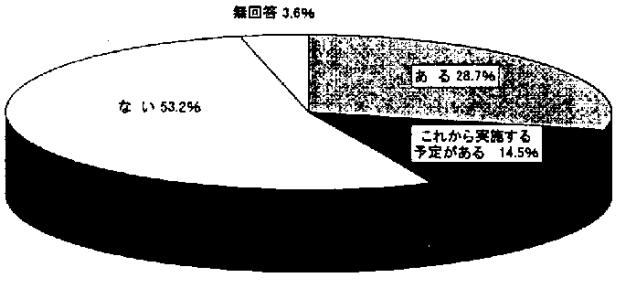

図3－1－26. 情報セキュリティ監査の実施状況(監査担当部門)

Q71. 貴事業体では情報セキュリティ監査を外部に委託したいと思いますか。

1	思 う	161	38.2
2	思わない	237	56.3
無回答		23	5.5
計		421	100.0

情報セキュリティ監査では外部の目でその実施状況を監査するのが重要である。そこで、今回調査では、情報セキュリティ監査に関して外部に委託したいかを調査した。その結果からは、38.2%の事業体が「思う」と答えており、また、「思わない」が56.3%となっている。まだまだ、外部監査が増えてきたものの、事業体の多くは内部監査ですませたいというのが本音であることがわかる。

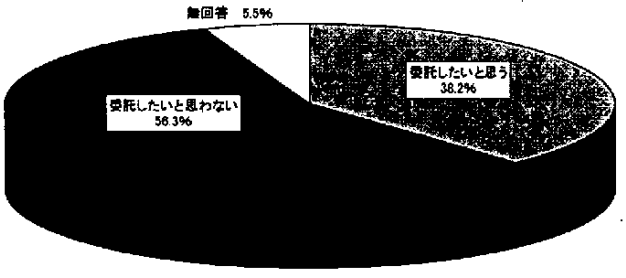

図3－1－27. 情報セキュリティ監査の外部への委託(監査担当部門)

Q72. 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	認定を取得している	39	9.3
2	知っている	224	53.2
3	知らない	143	34.0
無回答		15	3.6
計		421	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、前回調査では36.3%であったが、今回調査では、「認定を取得している」が9.3%、「知っている」が53.2%とあわせて62.5%の事業体が認知しており、一般的にも多くの事業体には認知されていると考えられる。今後は、取得企業が増えることが望まれる。

ただし、ISMSとQ71の情報セキュリティ監査とは、一見両立するように見えるが、企業が両方を実施することは必要な経費の面からもあり得ないといえよう。今後、２つの制度が、お互い切磋琢磨しながら、進んでいくことを望む。

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

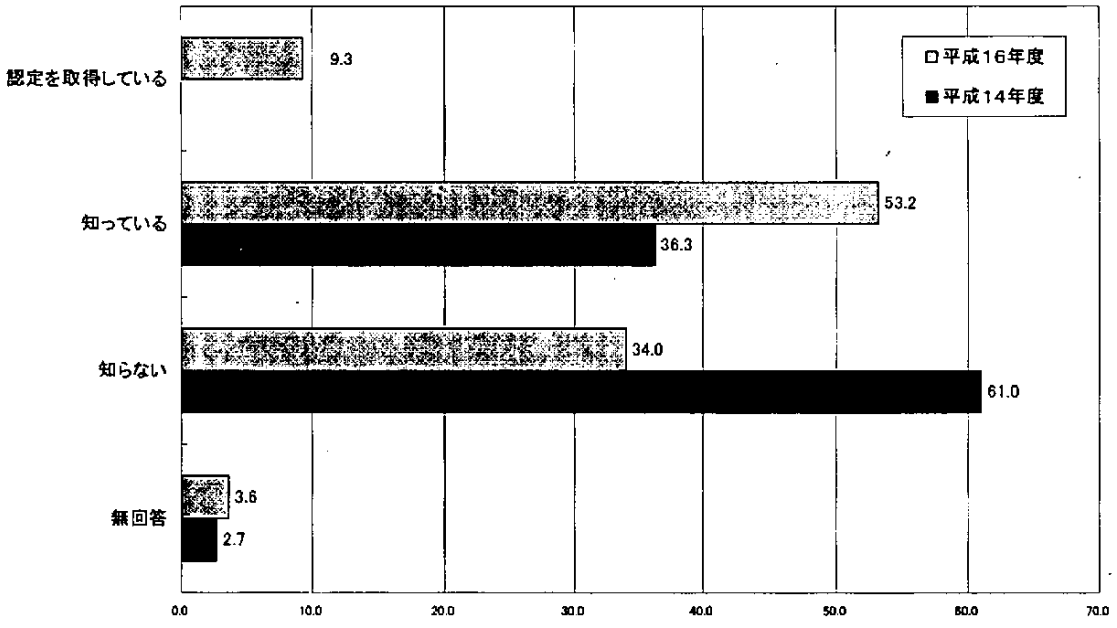

図3－1－28. ISMS適合性評価制度の認知度(被監査部門)

3.1.6　個人情報保護について

Q73～Q78 の質問については被監査部門に対しても同一の調査を行っているので、「3.2.5」を参照のこと。

Q73.「個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）」を知っていますか。

1	内容を知っている	280	66.5
2	制定されたことを知っている	118	28.0
3	知らない	11	2.6
無回答		12	2.9
計		421	100.0

平成 17 年 4 月の「個人情報の保護に関する法律」全面施行の影響もあり、認知度（「内容を知っている」、「制定されたことを知っている」の合計）は 94.5%と高い。個人情報の漏洩が多発する中、罰則を伴う法律の施行は、企業活動に大きな影響を及ぼすこともあり、そのことが、「内容を知っている」66.5%の高い値に現れていると見ることができる。

特に、従業員 1 万人を超える企業では、「内容を知っている」が 100%であり、5 千人を超える従業員数の企業でも、「内容を知っている」が 82.9%、「制定されたことを知っている」17.1%と認知度は 100%を示している。

業種別では、情報処理サービス業が「内容を知っている」81.8%、「制定されたことを知っている」13.6%であり、認知度は 95.4%と最も高い値となっている。

Q74. 経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成 16 年 10 月公表）を知っていますか。

1	内容を知っている	204	48.5
2	公表されたことを知っている	124	29.5
3	知らない	80	19.0
無回答		13	3.1
計		421	100.0

経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の認知度は、「個人情報の保護に関する法律」の値には、及ばないものの、「内容を知っている」48.5%、「制定されたことを知っている」29.5%で合計は 78.0%と高い。

特に、本調査がガイドラインの公表平成 16 年 10 月から間もないことを考慮すると、認知度は非常に高いといえる。特に、情報処理サービス業では、「内容を知っている」77.3%、「制定されたことを知っている」15.2%であり、認知度は 92.5%と所管省庁であることもあって非常に高い値を示している。

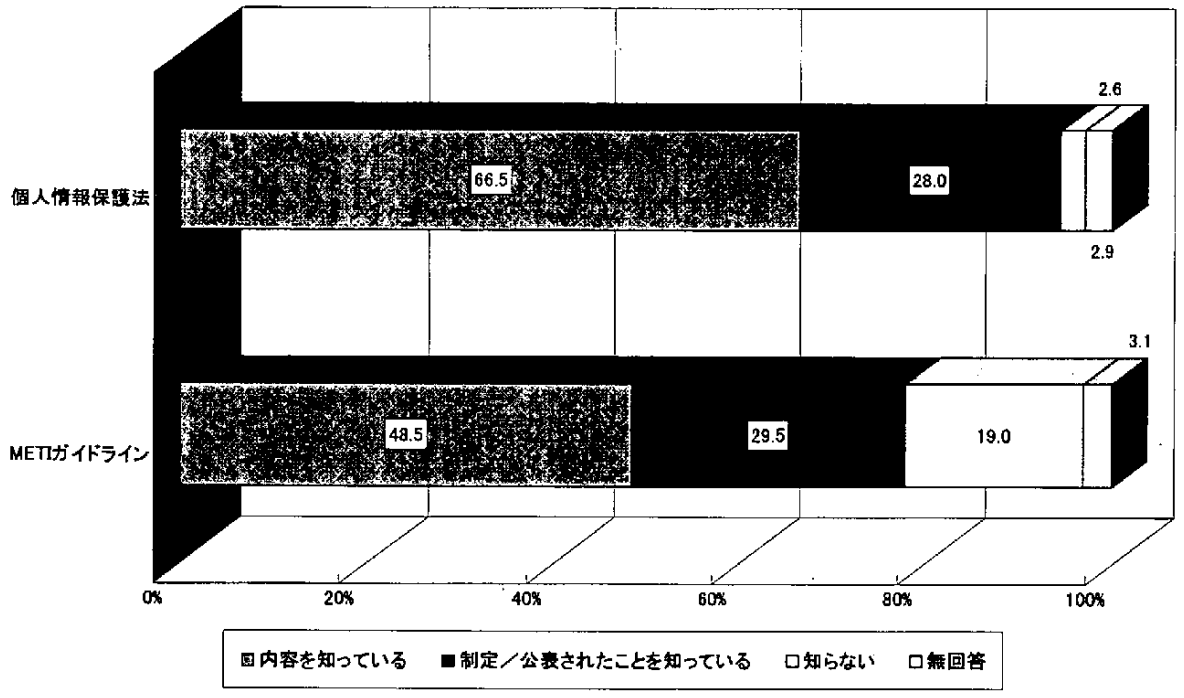

図3－1－29. 法律、ガイドラインの認知状況(監査担当部門)

Q75. 現在の個人情報の管理状況についてリスクをどのように認識していますか。

1	対応策を講じているので、リスクはないと認識している	35	8.3
2	現状の管理方法で何も問題が発生していないので、リスクはないと認識している	45	10.7
3	何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	140	33.3
4	いつ問題が発生してもおかしくない状況であると認識している	120	28.5
5	その他	39	9.3
6	特に認識していない	24	5.7
無回答		18	4.3
計		421	100.0

個人情報の管理状況についてリスクについて、リスクの有無を以下のように集計してみた。

・「リスクはない」・・・・24.7%（上記１、２、６の合計）

・「リスクはある」・・・・61.8%（上記３、４の合計）

「リスクはある」との認識は、61.8%と高い反面、認識していないも含めた「リスクはない」も24.7%となっている。約４分の１が「個人情報に関するリスクはない」と認識している点は、注目に値する。業種別では、金融・保険業の「何度かヒヤリ・ハッとした経験があり、リスクがあると認識している」51.4%、「いつ問題が発生してもおかしくない状況であると認識している」29.2%で「リスクはある」としては合計80.6%と最も高い値となっている。

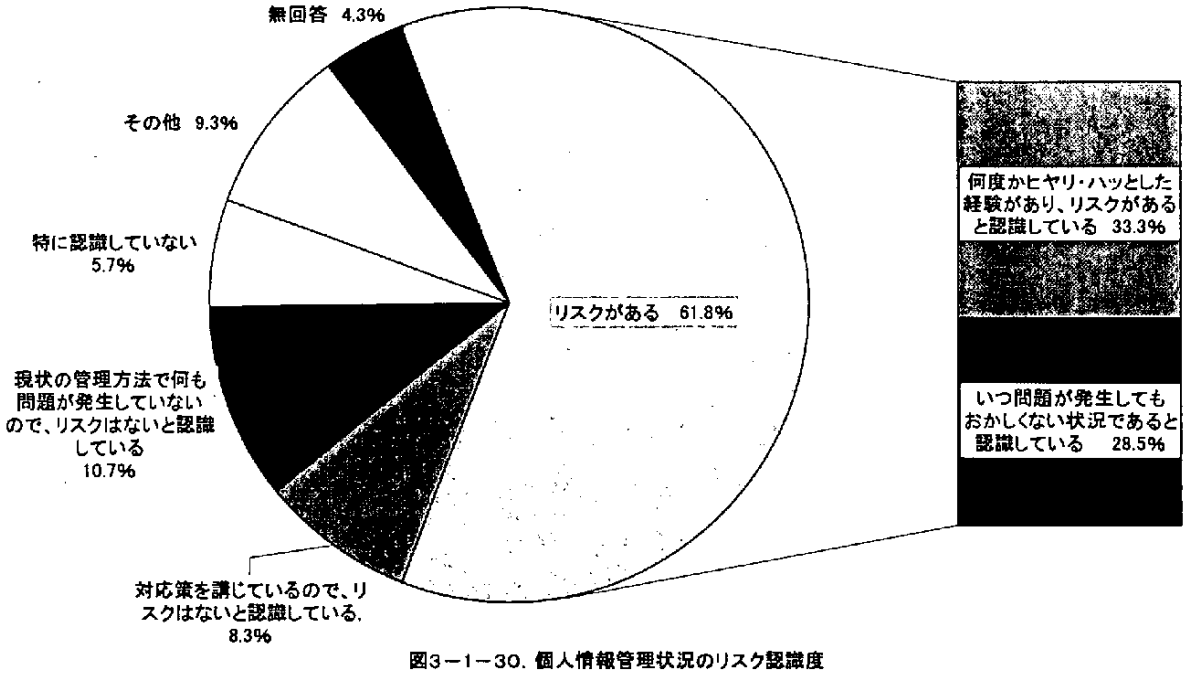

図3－1－30. 個人情報管理状況のリスク認識度

Q76. 個人情報保護対策として、①現在何を実施していますか。 ②また、今後どういうことを実施する予定ですか。(複数回答)

対　策	①現在実施している対策		②今後実施を予定している対策	
回答件数	421	－	421	－
プライバシーポリシーを策定している	138	32.8	133	31.6
管理責任者を置いている(保護体制(役割、責任、権限)を確立する)	179	42.5	126	29.9
個人情報保護に関する規程を定め運用している	167	39.7	156	37.1
個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している	66	15.7	108	25.7
社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している	123	29.2	149	35.4
定期的に監査を実施している	93	22.1	144	34.2
リスク分析を実施して必要な安全対策を構築している	113	26.8	146	34.7
苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している	166	39.4	99	23.5
仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている	132	31.4	120	28.5
その他	6	1.4	10	2.4
特に対策を講じない	124	29.5	16	3.8
無回答	21	5.0	121	28.7

注) ①ですでに導入している対策については、②の集計の対象外とし、「無回答」に含んでいる。

現在、実施している対策として上位３つは、「管理責任者の設置 42.5%」、「個人情報保護規程制定・運用 39.7%」、「苦情相談窓口設置 39.4%」であり、個人情報取扱事業者の義務として掲げられる「プライバシーポリシー策定 32.8%」、「個人情報保護教育の実施」は 29.2%に止まっている。

その一方、「特に対策を講じない」も 29.5%あり、個人情報保護法全面施行を控えた現状として遅れている状況が窺える。

今後実施予定の対策は、個人情報保護規程の制定・運用 37.1%、個人情報保護教育の実施 35.4%、リスク分析の実施と安全対策 34.7%、監査の実施 34.2%となっており、３社に１社がルールを策定し、周知徹底のための教育を実施し、監査を実施するマネジメントシステムの構築を予定している。そのことは、「プライバシーマーク取得の認定を受ける 25.7%」にも現れている。

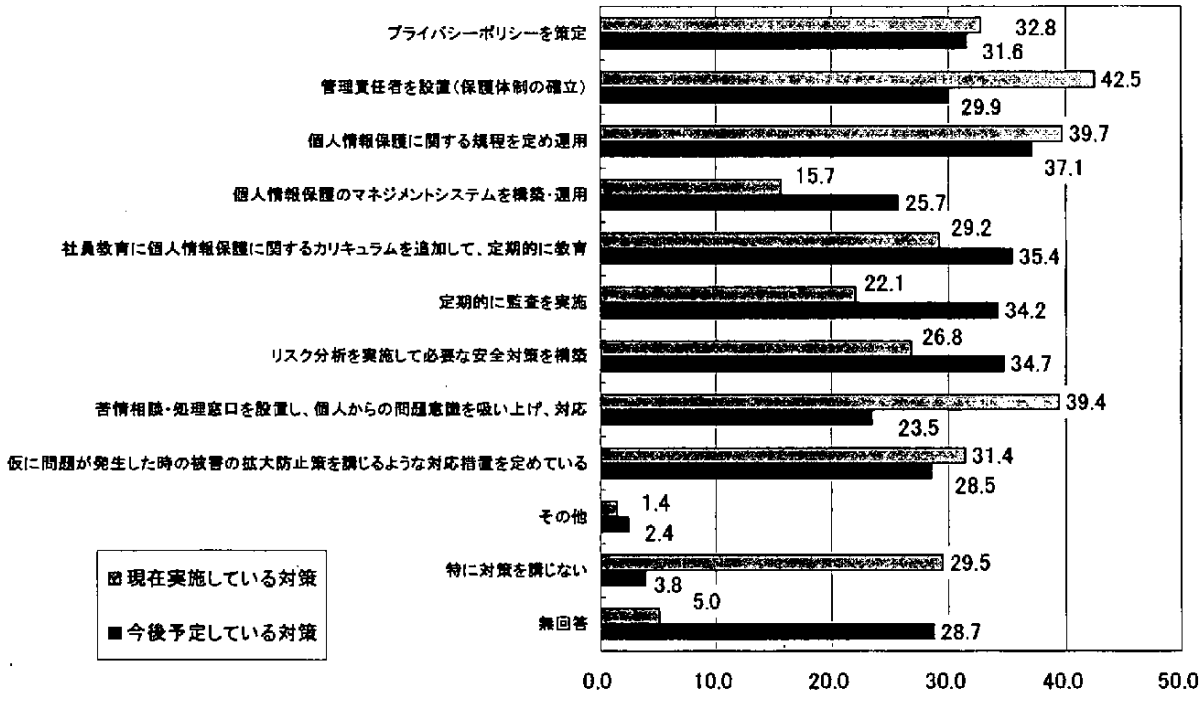

図3－1－31. 個人情報保護対策(監査担当部門)

Q77. 貴事業体では個人情報保護の監査を外部に委託したいと思いますか。

1	思う	116	27.6
2	思わない	280	66.5
無回答		25	5.9
計		421	100.0

個人情報保護の監査の外部委託については、委託したいと「思わない 66.5%」が、「思う 27.6%」を大きく上回った。このことは、監査所管部門への質問であり、委託への厳しい結果となって現れたと想定される。同じ質問について、情報システム部門は、「思わない 52.1%」が、「思う 41.0%」の結果であり、委託したいと「思う」は監査部門の結果より約 14 ポイント高くなっている。

業種については、公共サービスが、「思う 40.7%」で最も高い値であった。

Q78. プライバシーマーク制度を知っていますか。

1	認定を取得している	44	10.5
2	知っている	285	67.7
3	知らない	77	18.3
無回答		15	3.6
計		421	100.0

日本情報処理開発協会(JIPDEC)が運用す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。

平成14年度の調査では、プライバシーマークの認知度は、「知っている43.5%」よりも「知らない54.9%」の方が高い値を示す状況であった。

今回の調査では、平成17年4月の個人情報保護法全面施行への対策としても注目を集めていることもあり、プライバシーマーク制度の認知度は、「知っている 67.7%」に「認定を取得している10.5%」も加えて78.2%と前回よりも34.7ポイントもアップし、「知らない18.3%」を大きく上回った。業種別では、情報サービス業では、「認定を取得している53%」が過半数を超え、「知っている42.4%」との合計は95.4%と高い値となっている。

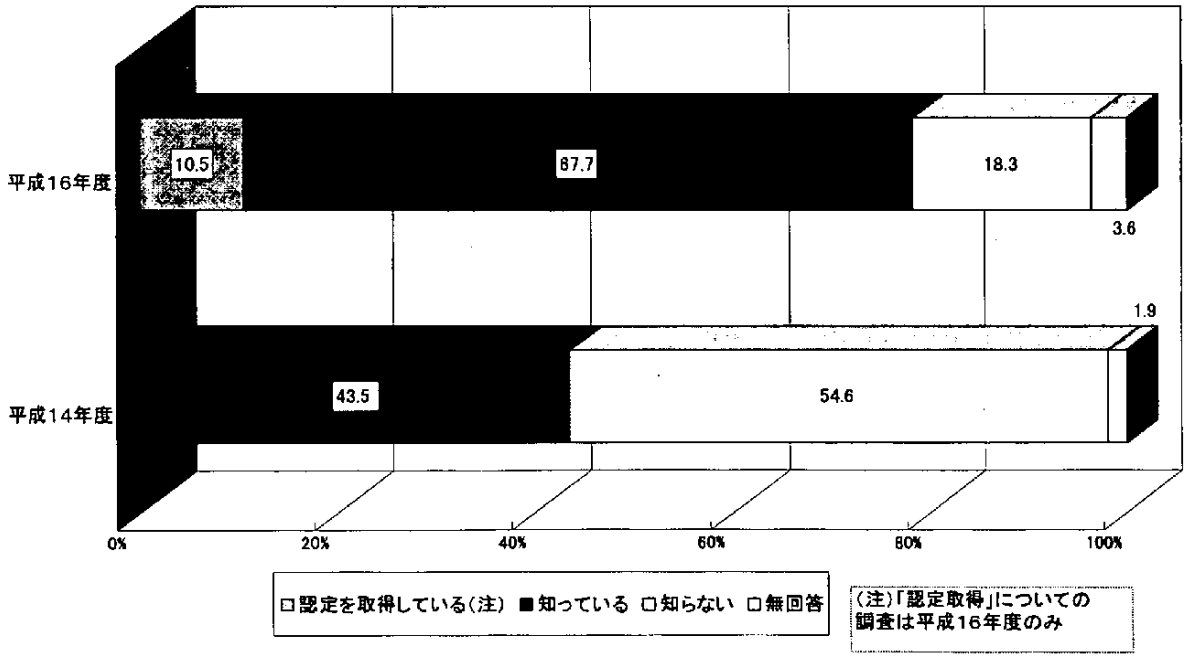

図3－1－32. プライバシーマーク制度の認知状況(監査担当部門)

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～Q17の質問については監査担当部門に対しても同一の調査を行っているので、「3.1.1」を参照のこと。

Q1．経済産業省の「システム監査基準」（平成8年改訂）を知っていますか。

1	利用したことがある	55	10.8
2	内容は知っているが、利用したことはない	174	34.3
3	存在だけは知っている	220	43.4
4	知らない	50	9.9
無回答		8	1.6
計		507	100.0

システム監査基準の認知度は、前回調査が 86.7%、今回調査が 88.5%である。若干ではあるが、監査担当部門より被監査部門の方がシステム監査基準を知っているという現象が表れている（被監査：88.5%、監査：86.9%）。これは日本的な特徴であるかもしれないが、被監査部門が積極的にシステム監査に取り組む傾向がみられるのも事実である。

システム監査基準を「利用したことがある」のは前回調査が 14.2%、今回調査は 10.8%であり、この2年間で 3.4 ポイント減少した理由はわからないが、この調査の母集団の影響であろう。ただし、この「利用したことがある」ということの理解が「システム監査を受けたことがある」と混同されている部分があるとすれば問題があるが、被監査部門としてシステム監査基準を使って点検・調査しているのであれば、マネジメントの強化に寄与していると理解してよい。ただし、あくまでもシステム監査を受ける側に対する調査である点を明確にした上で評価しなければならない。

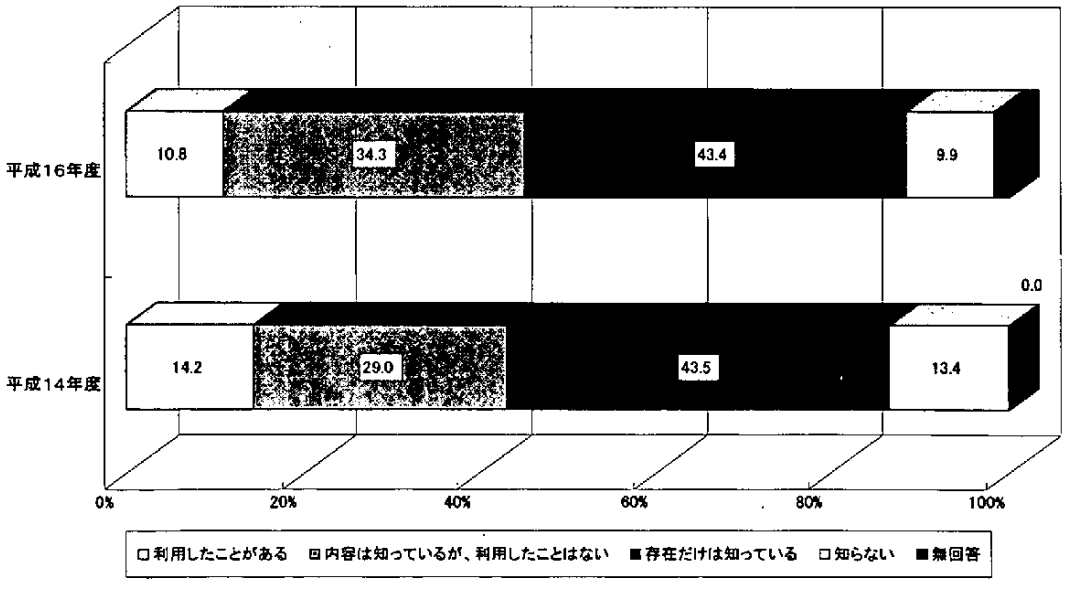

図3－2－1．システム監査基準の認知度（被監査部門）

Q２．「システム監査基準」が平成 16 年 10 月に改訂されたことを知っていますか。

1	利用したことがある	18	3.6
2	内容は知っているが、利用したことはない	131	25.8
3	存在だけは知っている	144	28.4
4	知らない	207	40.8
無回答		7	1.4
計		507	100.0

改訂システム監査基準を知っているのは、全体で 57.8%に上っている。これも、被監査部門における認知度で、しかも改訂直後の調査で優に過半数を超える事業体が基準の改訂を知っているというのは、システム監査に対する期待の盛り上がりが相当なものと評価してよいであろう。

改訂システム監査基準を「利用したことがある」のは 3.6%に過ぎないが、被監査部門であることを考えればあまり問題はないであろう。システム監査を受ける側が、どのような監査をするのかを勉強することは有意義なことであるといえる。

「内容は知っているが、利用したことはない」が 25.8%で、つまり被監査部門の４分の１が改訂基準の内容を把握していることになり、高く評価してよい。問題は、「知らない」の 40.8%を放置しておいてよいかどうかであろう。何らかの形で、これらの事業体に対して、システム監査およびシステム監査基準の意味合いを理解してもらうことがシステム監査の普及を図る上で必要であろう。

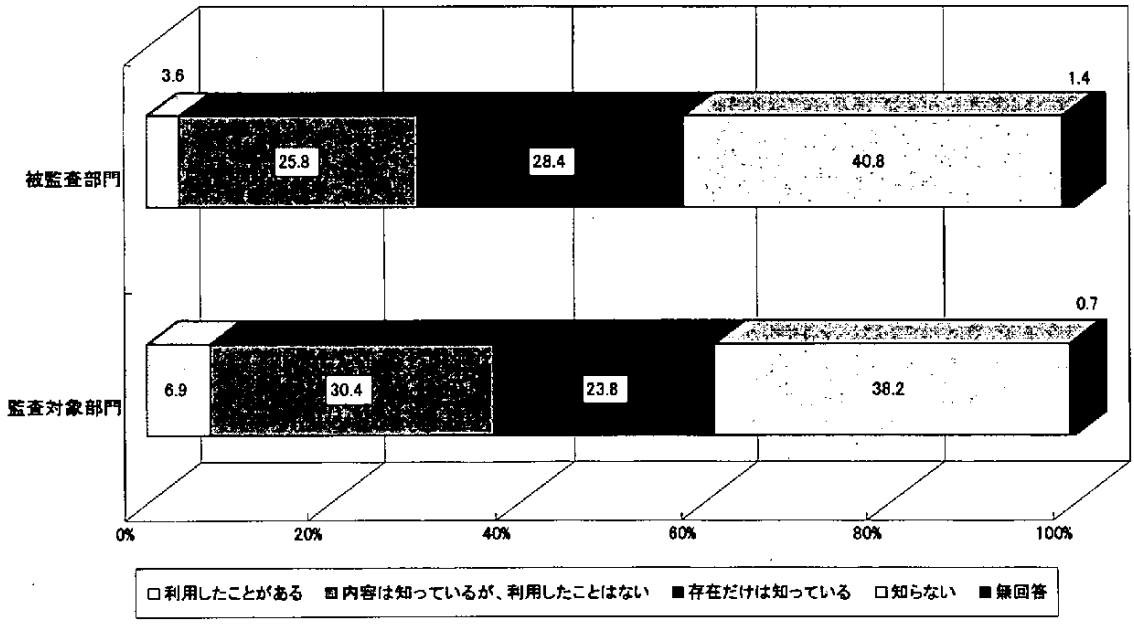

図3－2－2. 新システム監査基準の認知度(被監査部門／監査担当部門の比較)

Q３．経済産業省から「システム管理基準」（平成 16 年 10 月）が策定・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	24	4.7
2	内容は知っているが、利用したことはない	125	24.7
3	存在だけは知っている	175	34.5
4	知らない	176	34.7
無回答		7	1.4
計		507	100.0

今回のシステム監査基準の改訂では、同時にシステム管理基準も公表され、二本立てとなった。システム管理基準は、第一義的には情報システム部門で利用するものであり、それをシステム監査の際にも利用するという位置づけである。このシステム管理基準を「知っている」のは、全体で 63.9%に上り、システム監査基準の認知度（57.8%）よりも高い。被監査部門であるから、システム管理基準の認知度の方が高いのは、ある意味では当然である。

システム管理基準を「利用したことがある」のは、4.7%とまだ低い。これは、システム管理基準が公表されて間もないためであり、時間が経過すれば利用する事業体が大幅に増加するものと思われる。

全体の傾向は、システム監査基準とよく似ている。しかし、システム管理基準は、システム監査基準よりも、「存在だけは知っている」が 6.1 ポイント高く、逆に「知らない」が 6.1 ポイント低くなっている。被監査部門としては、多少ではあるがシステム監査基準よりもシステム管理基準の方に興味を示している向きが多いといえよう。

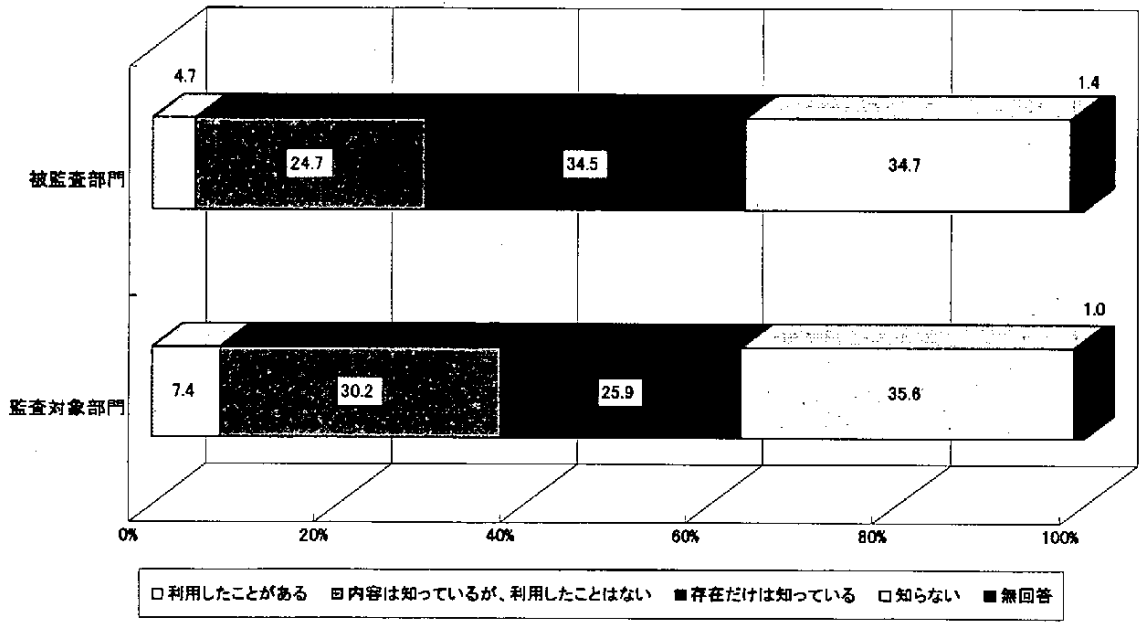

図3－2－3．システム管理基準の認知度（被監査部門／監査担当部門の比較）

Q４．経済産業省の「システム監査企業台帳」（平成３年）を知っていますか。

1	知っている	199	39.3
2	知らない	300	59.2
無回答		8	1.6
計		507	100.0

システム監査企業台帳制度は平成３年に創設された。この台帳を「知っている」のは、39.3%である。この数字を高いと評価するか、低いと評価するかは難しい判断である。それは、この制度が基本的には被監査部門が利用するものではなく、あくまでも経営者や監査担当部門が利用する制度だからである。しかし、この数字からは、被監査部門においてこの制度が着実に知られるようになっていることもみてとれる。それは、この２年間で「知っている」が約 40%に達していることと、「知らない」が 60%を割り込んでいることから明らかである。

Q５．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	19	9.5
2	今後参考にしたいと思う	144	72.4
3	参考にしたいと思わない	28	14.1
無回答		8	4.0
計		199	100.0

この質問は、あくまでも被監査部門に対するものであることを念頭に置いておく必要がある。この台帳を「参考にしたことがある」のは、前回調査が 7.0%で、今回調査が 9.5%である。１割に満たない数字ではあるが、この調査からは、どのようなことに参考にしたかはわからない。また、「今後参考にしたいと思う」は、前回調査が 73.8%、今回調査が 72.4%とほぼ同等の高い数字を示している。これも、この調査からは、どのようなことに参考にしたいのかの詳細はわからない。ただ、どのようなことに参考にされるかは別として、マネジメントの強化に役立つように参考にされれば、この制度としては役に立っていることになる。

Q６．経済産業省の「情報セキュリティ監査基準」（平成 15 年４月策定）を知っていますか。

1	利用したことがある	43	8.5
2	内容は知っているが、利用したことはない	177	34.9
3	存在だけは知っている	190	37.5
4	知らない	89	17.6
無回答		8	1.6
計		507	100.0

情報セキュリティ監査基準を知っているのは、全体で80.9%に達している。今日の情報社会を反映してか、短期間で急速に知られるようになっている。被監査部門の認知度が80.9%で、監査担当部門の認知度76.7%を上回っていることは、情報システム部門における情報セキュリティへの関心の高さを物語っている。

情報セキュリティ監査基準を「利用したことがある」のは、8.5%であるが、被監査部門での利用がどのようなものであるかは、この調査からはわからない。ただし、情報セキュリティ監査を受ける側としてこの基準を利用したのであれば、その試みは評価しなければならない。

監査担当部門と被監査部門を比較してみると、「利用したことがある」は監査担当部門(15.4%)の方が6.9ポイント高くなっているが、これは当然といえば当然の話である。問題は、「内容は知っているが、利用したことはない」は監査担当部門（31.1%）の方が3.8ポイント低くなっているし、「存在だけは知っている」は監査担当部門（30.2%）の方が7.3ポイント低くなっており、その結果「知らない」が監査担当部門（22.3%）の方が4.7ポイント高くなっていることである。情報セキュリティ監査基準は、あくまでも情報セキュリティに関する監査の基準であるから、監査担当部門はほとんどが知っていてしかるべきであろうと思われる。

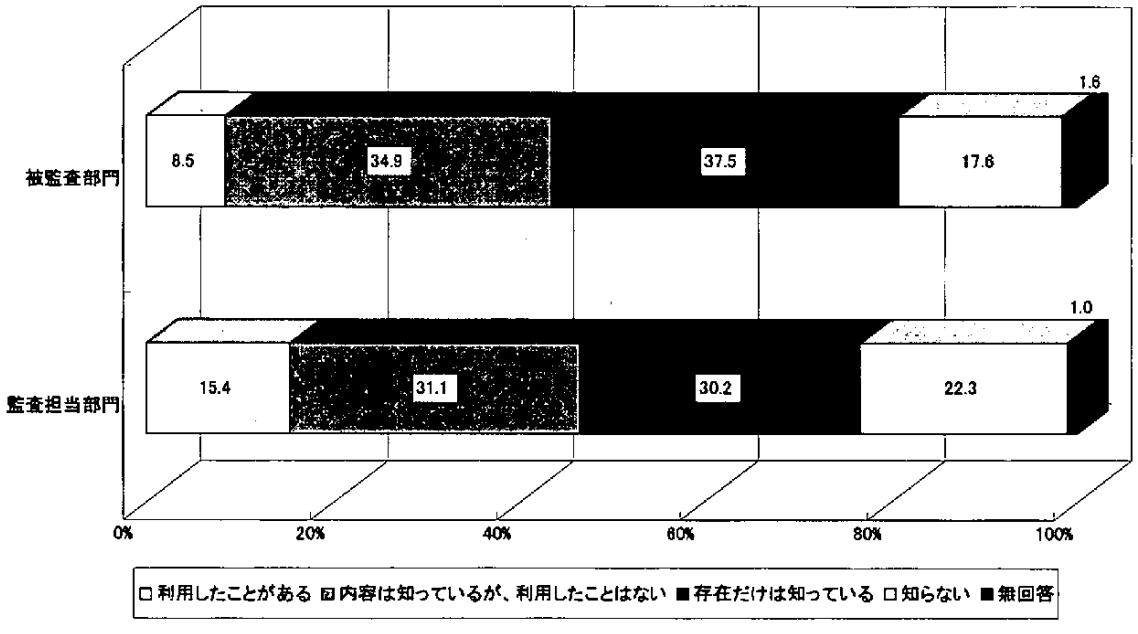

図3－2－4．情報セキュリティ監査基準の認知度(被監査部門／監査担当部門の比較)

Q7．経済産業省の「情報セキュリティ管理基準」（平成15年4月策定）を知っていますか。

1	利用したことがある	50	9.9
2	内容は知っているが、利用したことはない	168	33.1
3	存在だけは知っている	181	35.7
4	知らない	100	19.7
無回答		8	1.6
計		507	100.0

情報セキュリティ管理基準を知っているのは、全体で 78.7%となっており、監査担当部門の71.0%よりも高くなっている。これも、情報セキュリティ監査基準の場合と同じような傾向を示している。つまり、被監査部門の方が利用経験こそ少ないが、基準の「内容は知っているが、利用したことはない」(被監査:33.1%、監査:30.6%)や「存在だけは知っている」(被監査:35.7%、監査:25.4%)は高くなっている。そして、「知らない」は監査担当部門の方が 8.1 ポイント高いという結果が表れている。

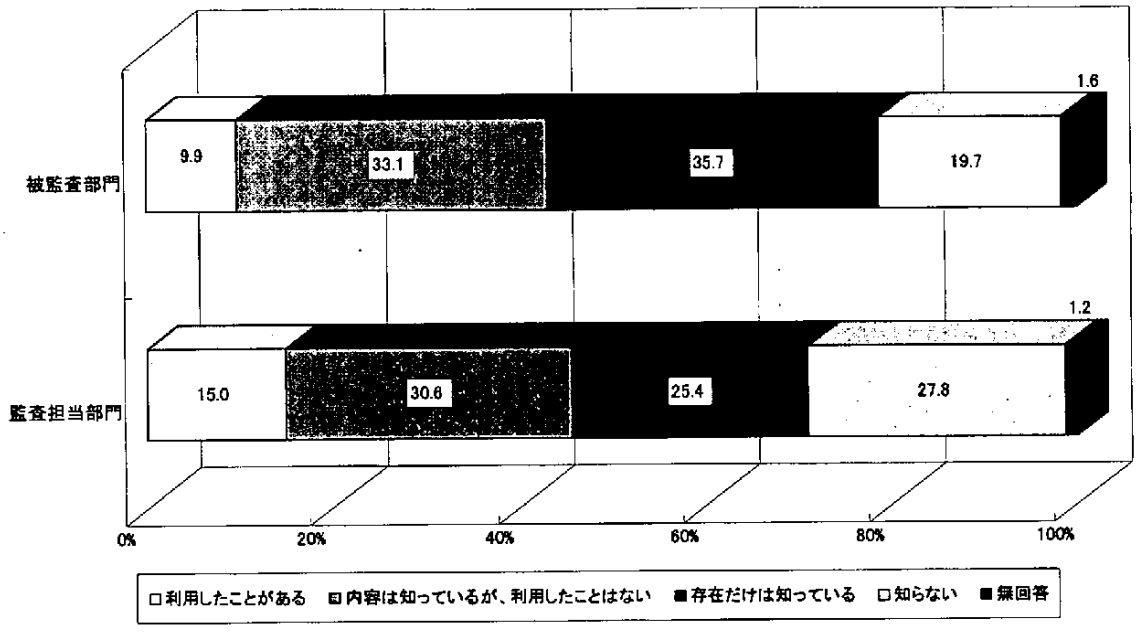

図3－2－5. 情報セキュリティ管理基準の認知度(被監査部門／監査担当部門の比較)

Q８．経済産業省の「情報セキュリティ監査企業台帳」(平成 15 年)を知っていますか。

1	知っている	188	37.1
2	知らない	308	60.7
無回答		11	2.2
計		507	100.0

情報セキュリティ監査企業台帳について「知っている」のは、被監査部門は 37.1%で、監査担当部門(45.8%)より 8.7 ポイント低くなっている。これは、事業体で監査を外部に委託する責任者は誰かということが日本では明確になっていないため、この数字をどのように評価するかは難しい。一般論としては、監査担当部門の認知度が高くてしかるべきであろう。

Q９．情報セキュリティ監査を外部の企業に委託する場合、「情報セキュリティ監査企業台帳」を参考にしたいと思いますか。

1	参考にしたことがある	17	9.0
2	今後参考にしたいと思う	143	76.1
3	参考にしたいと思わない	20	10.6
無回答		8	4.3
計		188	100.0

この質問については、被監査部門と監査担当部門とが同じような傾向を示している。しかし、被監査部門が情報セキュリティ監査企業台帳を参考にするという場合、この調査からはどのように参考にするのかは不明である。

Q10. 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	417	82.2
2	知らない	82	16.2
無回答		8	1.6
計		507	100.0

システム監査技術者試験の認知度は、監査担当部門が76.7%であるのに対して、被監査部門が82.2%と5.5ポイント高くなっている。本来、監査人の試験であるから、監査担当部門の認知度の方が高いのではないかと思われがちであるが、実際には情報システム側の方がよく知っているという結果になっている。その１つの理由は、情報処理技術者試験のなかの一区分として実施されていることが影響しているのではないかと思われる。

Q11. 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	89	17.6
2	内容は知っているが、利用したことはない	140	27.6
3	存在だけは知っている	152	30.0
4	知らない	119	23.5
無回答		7	1.4
計		507	100.0

情報システム安全対策基準を知っているのは、全体で前回調査が 80.8%、今回調査が 75.2%となっており、この２年間で5.6ポイント減少している。すなわち、情報システム安全対策基準の認知度が低下する傾向にあるといえる。とくに気になる点は、「知らない」が前回調査には19.3%と２割以下であったものが、今回調査には23.5%と20%を突破して4.2ポイントも増えて

いることである。情報セキュリティがこれだけ声高に叫ばれているとき、この基準の認知度低下に歯止めを掛ける必要性はないのか気がかりである。

Q12.「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	286	75.1
2	知らない	94	24.7
無回答		1	0.3
計		381	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。このことを「知っている」のは前回調査が 73.9%で、今回調査が 75.1%と若干増えているが、全体的には同じような傾向となっている。情報システム安全対策基準の中にシステム監査が位置づけられていることはよく知られていると評価してよいだろう。

Q13. 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	90	17.8
2	内容は知っているが、利用したことはない	144	28.4
3	存在だけは知っている	167	32.9
4	知らない	99	19.5
無回答		7	1.4
計		507	100.0

コンピュータウイルス対策基準を知っているのは、全体で前回調査が 80.0%、今回調査が 79.1%となっている。若干今回の方が低くなっているが、これは母集団の違いからくる誤差の範囲であろう。まずは、よく知られていると評価してよいが、「利用したことがある」のが 20%以下と低いのが気がかりである。これは、ワクチンソフトの普及や、問題が発見された場合の OS の更新など、きめの細かい対応策がとられていることが功を奏しているのであろうと思われる。

Q14.「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	246	61.3
2	知らない	147	36.7
無回答		8	2.0
計		401	10.0

コンピュータウイルス対策基準のなかにシステム監査が位置づけられている。これを知っているのは、前回調査が 63.0%、今回調査が 61.3%と若干低くなっているが、傾向は同じである。この 60%を超える認知度を、高いとみるか、低いとみるかは、意見の分かれるところかもしれないが、やはりよく知られていると評価してよいと思われる。

Q15. 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	77	15.2
2	内容は知っているが、利用したことはない	145	28.6
3	存在だけは知っている	166	32.7
4	知らない	111	21.9
無回答		8	1.6
計		507	100.0

コンピュータ不正アクセス対策基準を知っているのは、全体で前回調査が 76.2%、今回調査が 76.5%とほとんど同じ傾向である。全体としては４分の３以上が知っているのでよく知られているともいえるが、個別の項目をみていくと問題がある。

コンピュータ不正アクセス対策基準を「利用したことがある」のは、前回調査が 15.1%で、今回調査が 15.2%とほとんど同じである。この種の基準は、利用しなければ意味がないのではないかと思われるが、「利用したことがある」が約 15%にすぎないのは、今日のように不正アクセスが問題視されているときには低いと評価せざるを得ない。

Q16. 「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	242	62.4
2	知らない	140	36.1
無回答		6	1.5
計		388	100.0

コンピュータ不正アクセス基準のなかにシステム監査が位置づけられている。このことを「知っている」のは、前回調査は 64.8%であるが、今回調査は 62.4%と若干低くなっている。不正アクセスに対してもシステム監査が効果的であることを世の中に広めるためには、もっと知ってもらうための努力が必要である。

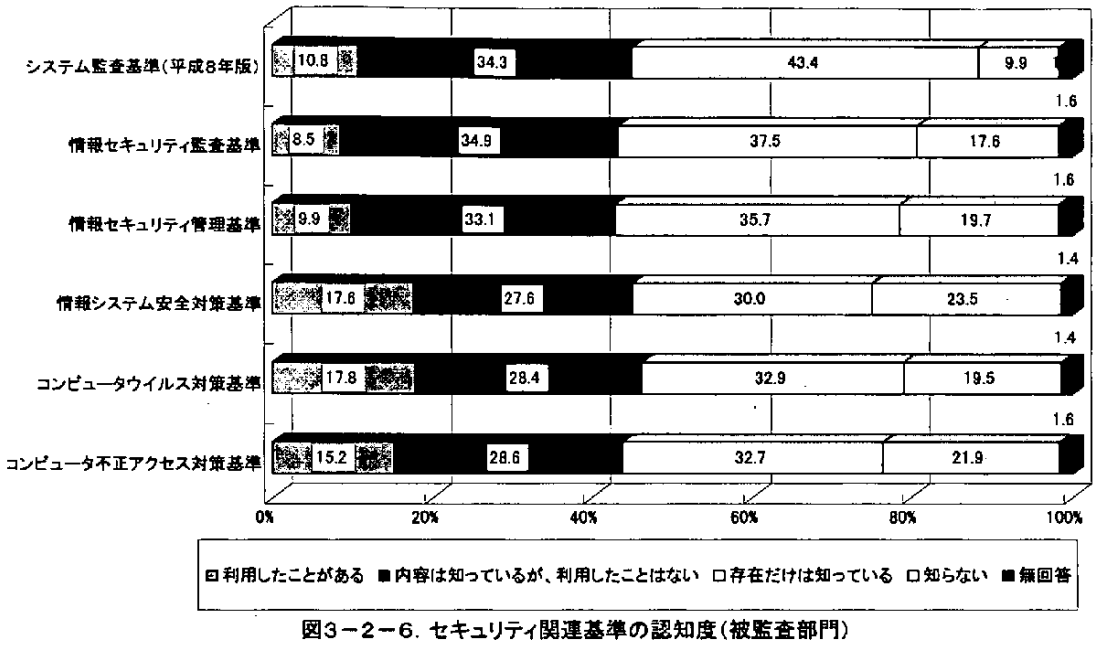

図3－2－6. セキュリティ関連基準の認知度(被監査部門)

Q17. 以下のJIS規格を知っていますか。

規格名	利用している		知っている		知らない		無回答		計	
JIS X 5080 : 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(平成14年2月制定)	63	12.4	209	41.2	226	44.6	9	1.8	507	100.0
JIS Q 2001 : リスクマネジメントシステム構築のための指針(平成13年3月制定)	19	3.7	195	38.5	284	56.0	9	1.8	507	100.0
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(平成11年4月制定)	66	13.0	229	45.2	203	40.0	9	1.8	507	100.0

監査担当部門は「知っている」が全ての規格において35%台であるが、被監査部門では40%台前後となっている。すなわち、これらの規格は、被監査部門の方でよく知られていることになる。ただし、監査担当部門同様、認定制度に関連する規格のJIS Q 15001およびJIS X 5080については「利用している」のは12～13%であり、JIS Q 2001はわずか4%にも満たない。まず、規格をもっと知ってもらうことから始める必要性がありそうである。

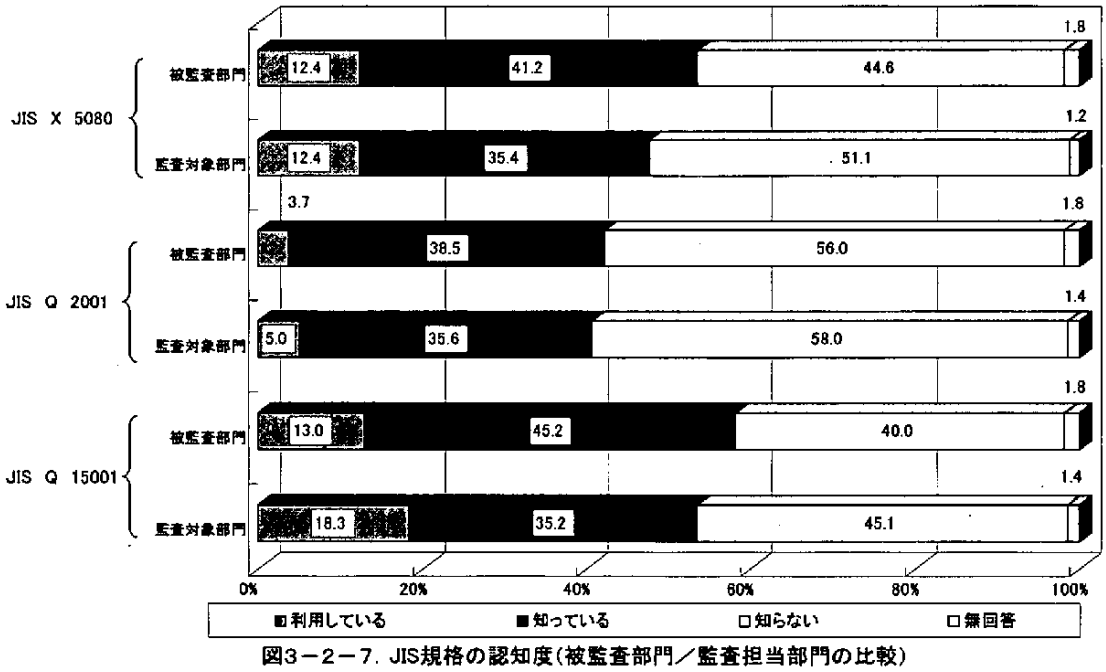

図3－2－7. JIS規格の認知度(被監査部門／監査担当部門の比較)

3.2.2　システム監査の実施について

Q18. 貴事業体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	125	24.7
2	いない	377	74.4
無回答		5	1.0
計		507	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、24.7%が「いる」と回答している。これは前回調査と比較して7.1ポイントの大幅な増加である。同一の質問を監査担当部門に対して実施しているが（Q19)、その回答では25.4%であり、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、生命保険業が66.7%、金融業が59.7%、情報処理サービス業・ソフトウェア業が43.9%となっている。金融業は、監査担当部門に対する調査では63.8%となっており、被監査部門に対する回答値とほぼ一致している。(監査担当部門に関する分析（Q19）は、「3.1.2」を参照のこと。)

Q19. 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	225	44.4	
2	受ける予定がある	22	4.3	→Q40へ
3	な い	258	50.9	→Q40へ
無回答		2	0.4	
計		507	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／受けたことがあるか」（被監査Q19、監査Q22)、さらにシステム監査を実施したことがある、あるいは受けたことがあるとした回答に対し、「過去２年間に実施したか／受けたことがあるか」の２項目の調査を行った。「過去にシステム監査を受けたことがあるか」（被監査Q20、監査Q36）に対しての回答は、被監査部門では前回調査（39.3%）に対して5.1ポイント増の44.4%であった。監査担当部門に対する調査では46.3%（前回調査：38.4%）であり（Q22)、ほぼ同様の回答となっている。何れの部門に対する調査でも前回調査に比較して５ポイント以上の増加となったことが注目される。(監査担当部門に関する分析（Q22）は、「3.1.2」を参照のこと。)

Q20. 過去２年間にシステム監査を受けましたか。

1	受けた(実施中を含む)	203	90.2	
2	受けない	22	9.8	→Q40へ
計		225	100.0	

過去にシステム監査を実施した事業体に対しての過去２年間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90.2%である。同一の質問に対する監査担当部門の回答は、87.7%であり、回答値は近似している（Q36)。

被監査部門からの回答で、過去２年間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、金融業（97.9%)、情報処理サービス業・ソフトウェア業（94.3%)、輸送用機械器具製造業および化学工業（90.9%)、電気機械器具製造業（81.8%)、生命保険業（77.8%）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。

（監査担当部門に関する分析（Q36）は、「3.1.3」を参照のこと。）

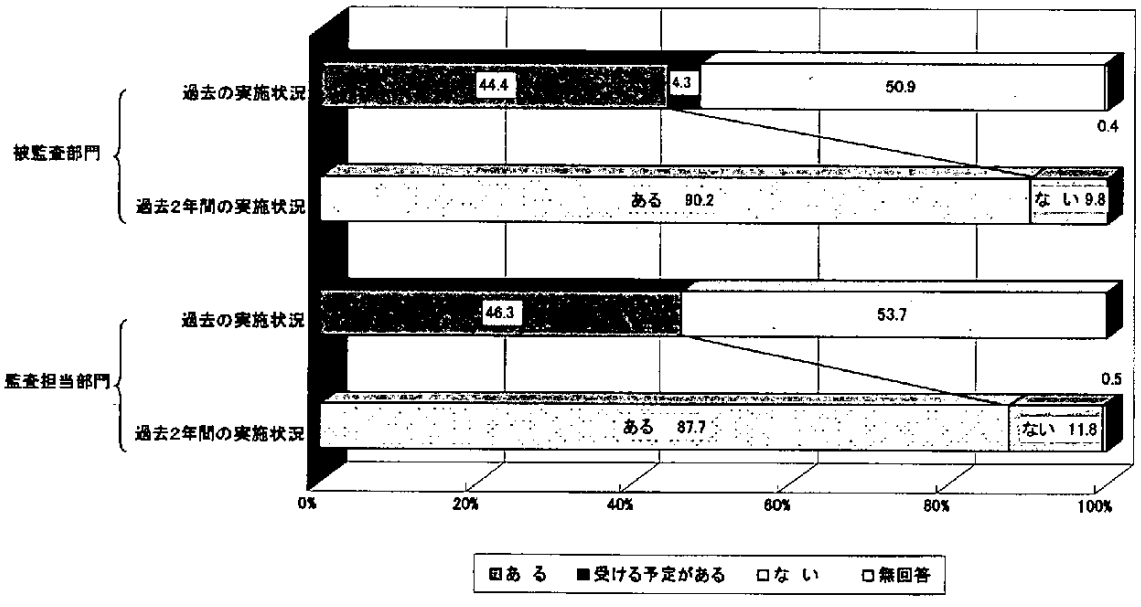

図3－2－8. システム監査実施状況

Q21. システム監査を受けたのはどの業務でしたか。(複数回答)

1	企画業務	87	42.9
2	開発業務	137	67.5
3	運用業務	183	90.1
4	保守業務	115	56.7
無回答		2	1.0
計		203	100.0

過去２年間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」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42.9%（前回調査42.7%)、「開発業務」が67.5%（前回調査69.7%)、「運用業務」が90.1%（前回調査89.3%)、「保守業務」が56.7%（前回調査53.4%）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率が依然として他の業務に比べ低いのは今後の課題である。

Q22. 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		203	-
1	ドキュメント管理	122	60.1
2	進捗管理	61	30.0
3	品質管理	86	42.4
4	コスト管理	34	16.7
5	要員管理	68	33.5
6	外部委託(開発の委託)	95	46.8
7	外部委託(運用の委託)	111	54.7
8	セキュリティ対策	167	82.3
9	ネットワーク管理	105	51.7
10	ソフトウェアの適正利用(ライセンス管理)	65	32.0
11	個人情報保護対策	62	30.5
12	PC管理、モバイル機器管理	84	41.4
13	コンピュータウイルス対策	92	45.3
14	情報システム関連のリスク管理	119	58.6
15	災害対策	88	43.3
16	その他	11	5.4
無回答		2	1.0

監査対象分野ごとの実施状況の調査では、最も多かったのは「セキュリティ対策」82.3%(監査担当部門に対する調査(Q41)では84.2%)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」30.5%(同57.9%)、「コンピュータウイルス対策」45.3%(同62.0%)、「情報システム関連のリスク管理」58.6%(同57.9%)、「災害対策」43.3%(同57.9%)も多くなっている。(監査担当部門に関する分析(Q41)は、「3.1.3」を参照のこと。)

個人情報保護法の本格施行が平成17年4月になされるが、「個人情報保護法対策」の監査の実施率が監査担当部門と被監査部門とで27.4ポイントの開きがあるのは、監査部門の監査において情報システム部門を対象にしない一般の個人情報保護の業務監査の場合の回答が含まれていることが想定される。

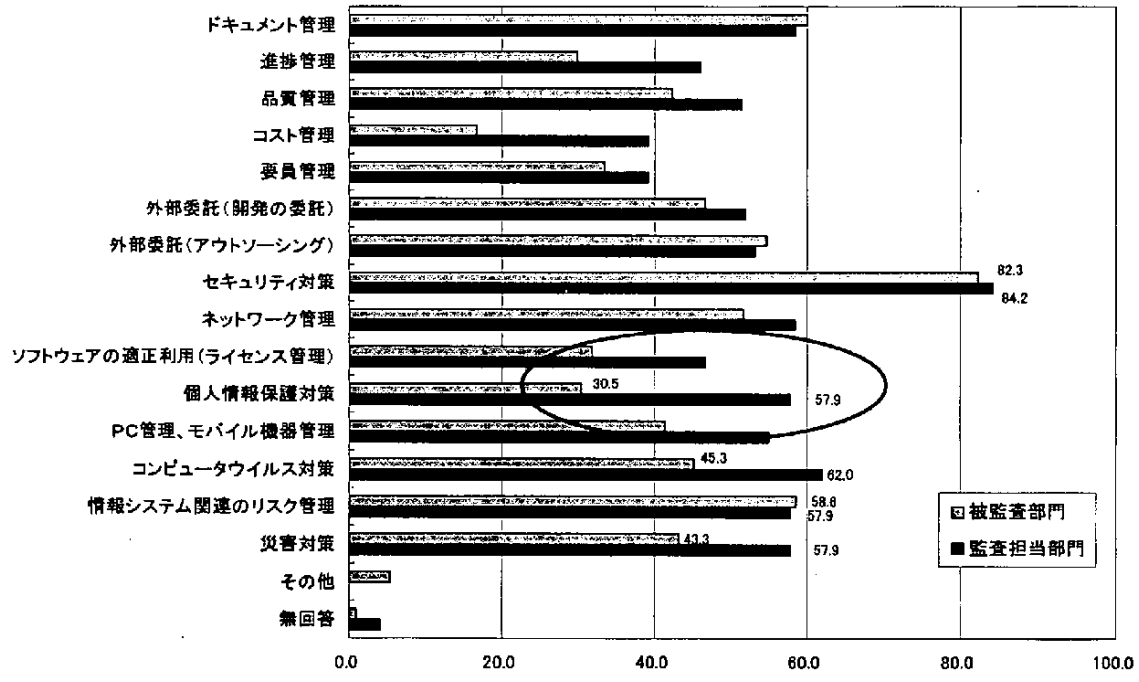

図3－2－9. システム監査実施テーマ

Q23. 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		203	－
1	内部監査部門型(監査部、検査部等が実施)	106	52.2
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)	149	73.4
無回答		1	0.5

(注)「1　内部監査部門型」のみ該当する場合はQ26へ、2つとも該当する場合はQ24を回答。

過去2年間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、52.2%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73.4%となっている。前回調査に比較して「内部監査部門型」が7.4ポイント減少した反面、「外部委託型」が18.3ポイントの大幅な増加となっている。

監査担当部門に対する調査では、「内部監査部門型」が60.8%であり「外部委託型」は39.8%であった（Q37)。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だけの回答とはいえないため、監査担当部門と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（Q37）は、「3.1.3」を参照のこと。)

Q24.（Q23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の登録企業ですか。

1	はい	63	42.3
2	いいえ	10	6.7
3	わからない	74	49.7
無回答		2	1.3
計		149	100.0

システム監査を委託している場合の委託先企業が「システム監査企業台帳の登録企業であるかの調査では、「はい（委託先企業）」が42.3%、「いいえ（委託先業ではない）」が6.7%であった。また、登録企業か否かが不明の回答も多かった（49.7%）。それぞれの選択肢の回答状況は、監査担当部門からの回答と同様であった（Q38）。（監査担当部門に関する分析（Q38）は、「3.1.3」を参照のこと。）

Q25.（Q23で「2」を回答した場合）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)	116	77.9
2	コンサルタント(個人／企業)	7	4.7
3	情報処理サービス業者	4	2.7
4	その他	2	1.3
無回答		20	13.4
計		149	100.0

この調査項目は前回調査から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）」が77.9%と多かったが、前回調査に比較して11.9ポイントの減少となった。減少となった分は、他の選択肢の回答が増加したのではなく、「無回答」が増加した。

Q26. 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	17	8.4	
2	十分満足できた	29	14.3	→Q28へ
3	特に問題はなかった	146	71.9	
4	わからない	9	4.4	
無回答		2	1.0	
計		203	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」（14.3%）、「特に問題はなかった」（71.9%）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。

特に「十分満足できた」は、前回調査の9.6%から、4.7ポイント増加した。

Q27. どのような点で問題があったと思いますか。最も問題だと思った点を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	17.6
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	11.8
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	23.5
4	監査人の情報システムに関する知識が不足していた	4	23.5
5	監査人の洞察力・判断力に問題があった	2	11.8
6	その他	2	11.8
計		17	100.0

Q26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かったが、「問題があった」とした回答に対する具体的な問題点は、表のとおりである。「監査人の監査対象業務に関する知識が不足していた」、「監査人の情報システムに関する知識が不足していた」（23.5%）と「知識」に関する回答が最も多かった。しかし、回答数の絶対数が少ないため、回答結果の評価に対しては、十分な考慮が必要である。

Q28. 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	18	8.9
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	165	81.3
3	通常業務に支障をきたした	17	8.4
4	その他	0	0.0
無回答		3	1.5
計		203	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。

8.9%が「負担はなかった」、81.3%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8.4%となっている。

Q29. 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。最も問題だと感じた点を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	1	0.5
2	システム監査方法が現場を無視したものであった	1	0.5
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	32	15.8
4	資料提出や意見聴取の指示が不明確であった	12	5.9
5	資料要求が多すぎた	19	9.4
6	現場の説明がシステム監査人に理解されなかった	13	6.4
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	3.9
8	実地調査が多すぎた	3	1.5
9	その他	4	2.0
10	特に問題は感じなかった	98	48.3
無回答		5	2.5
複数回答		7	3.4
計		203	100.0

システム監査を受けた結果の問題点についての調査では、「特に問題を感じなかった」が半数近い48.3%（前回調査53.9%）であったが、何らかの問題点があったとの回答（選択肢１～９）の合計は45.9%あった。被監査部門に対する調査の「Q27. システム監査を受けた時の監査人に対する問題点」、あるいは「Q28. 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」（15.8%）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」（9.4%）、「現場の説明がシステム監査人に理解されなかった」（6.4%）をみると、監査時の資料、説明に関する問題が多かったことを示している。

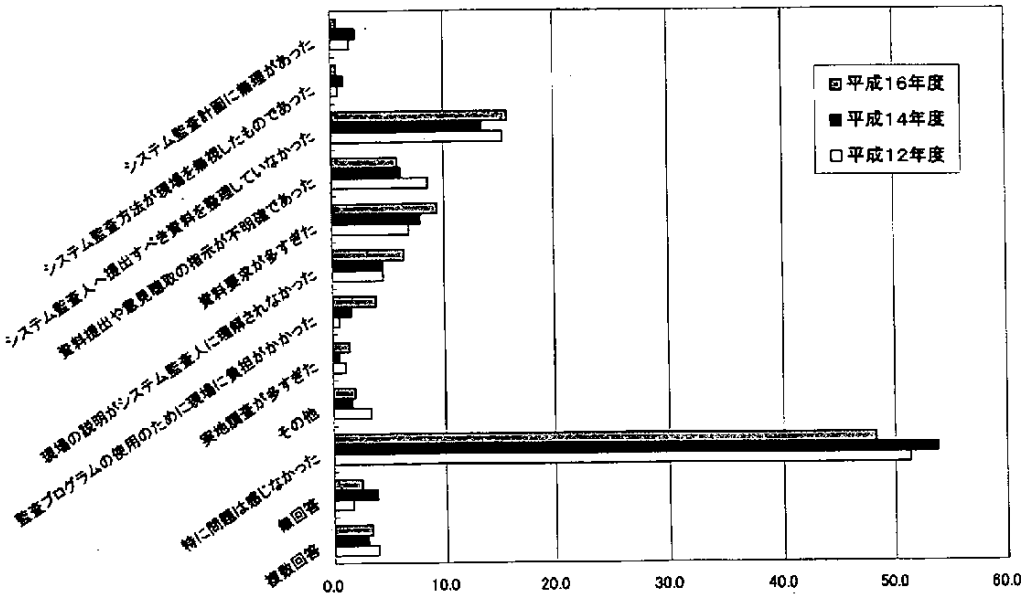

図3－2－10. システム監査を受けて感じた問題点

Q30. 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	171	84.2
2	行われなかった	27	13.3
無回答		5	2.5
計		203	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84.2%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、80.7%であった（Q55）。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。（監査担当部門に関する分析（Q55）は、「3.1.3」を参照のこと。）

Q31. 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	134	66.0	
2	行われなかった	62	30.5	→Q33へ
無回答		7	3.4	
計		203	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 66.0%であった。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。

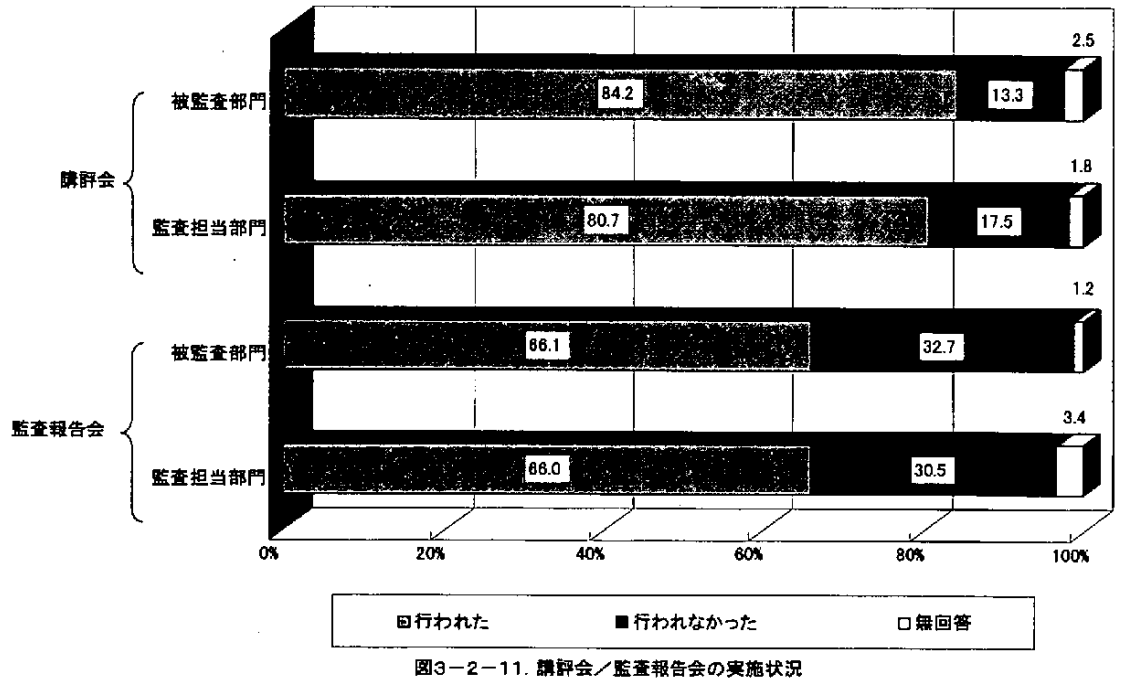

図3－2－11. 講評会／監査報告会の実施状況

Q32. 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	114	85.1
2	しない	17	12.7
無回答		3	2.2
計		134	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85.1%であった。比較的、高率であるといえる。なお、監査報告会の出席者の状況については監査担当部門に対しても調査しており、その結果は、監査担当部門のQ57 で分析されている。(監査担当部門に関する分析 (Q57) は、「3.1.3」を参照のこと。)

Q33. 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	134	66.0
2	一部妥当だと思う	58	28.6
3	妥当だと思わない	3	1.5
無回答		8	3.9
計		203	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、66.0%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」(28.6%) と回答しており、「妥当だと思わない」は僅少であった。先述のシステム監査の実施上の問題点 (Q29)、現場の負荷 (Q28) 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。

Q34. 改善命令を受けましたか。

1	受けた	119	58.6	
2	受けない	79	38.9	→Q36へ
無回答		5	2.5	
計		203	100.0	

過去2年間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 58.6% (前回調査 66.9%) である。約6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。

Q35. 改善命令を受けて対策を実施しましたか。

1	実施した	70	58.8
2	一部実施した	45	37.8
3	実施していない	2	1.7
無回答		2	1.7
計		119	100.0

改善命令に対し対策を「実施した」が58.8%、「一部実施した」が37.8%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53.8%であり、今回は5.0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。

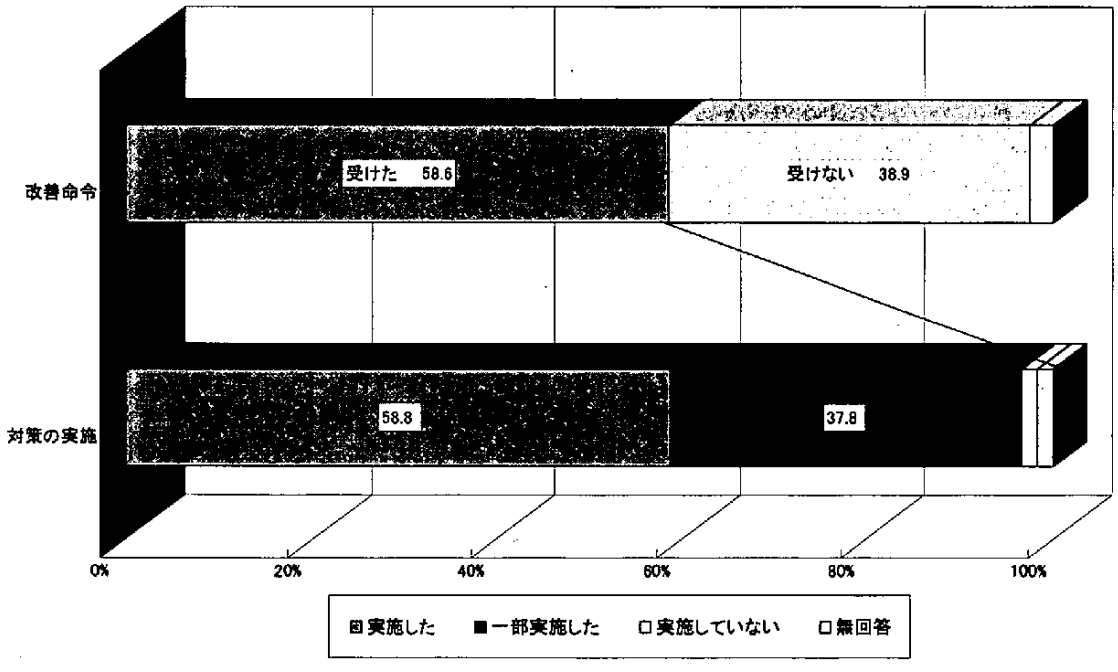

図3－2－12. 改善命令の発令／対策の実施(被監査部門)

Q36. 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	149	73.4	
2	効果はなかったと思う	2	1.0	→Q39へ
3	どちらともいえない	42	20.7	→Q39へ
4	わからない	5	2.5	→Q39へ
無回答		5	2.5	
計		203	100.0	

システム監査を受けた結果、被監査部門として、効果があったかを問うた質問に対し、「効果があったと思う」という回答は73.4%であり、前回調査の72.5%とほぼ同様である。一方、「効果はなかったと思う」(1.0%) は前回調査 (3.9%) 同様、低い値となっている。

被監査部門に対するQ33、Q35およびQ36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。

Q37. 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点を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	4	2.7
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	38	25.5
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	18	12.1
4	システム部門に対する過大な要求がなくなった	1	0.7
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	24	16.1
6	システムの有効利用が促進された	3	2.0
7	有効なシステムの開発設計が可能になった	3	2.0
8	業務の継続性の確保が図られた	3	2.0
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	30	20.1
10	その他	7	4.7
無回答		2	1.3
複数回答		16	10.7
計		149	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、前回調査では「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」が27.1%とトップであったが、今回調査では7.0ポイント減の20.1%で2位となり、「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」が前回調査が17.8%から7.7ポイント増の25.5%でトップとなった。情報システムや情報資産のリスク管理の重要性がITガバナンスの充実と共に唱えられている現状を反映している。

ついで「システムの安全性向上対策のレベルが明らかになった」(16.1%)、「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」(12.1%)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。

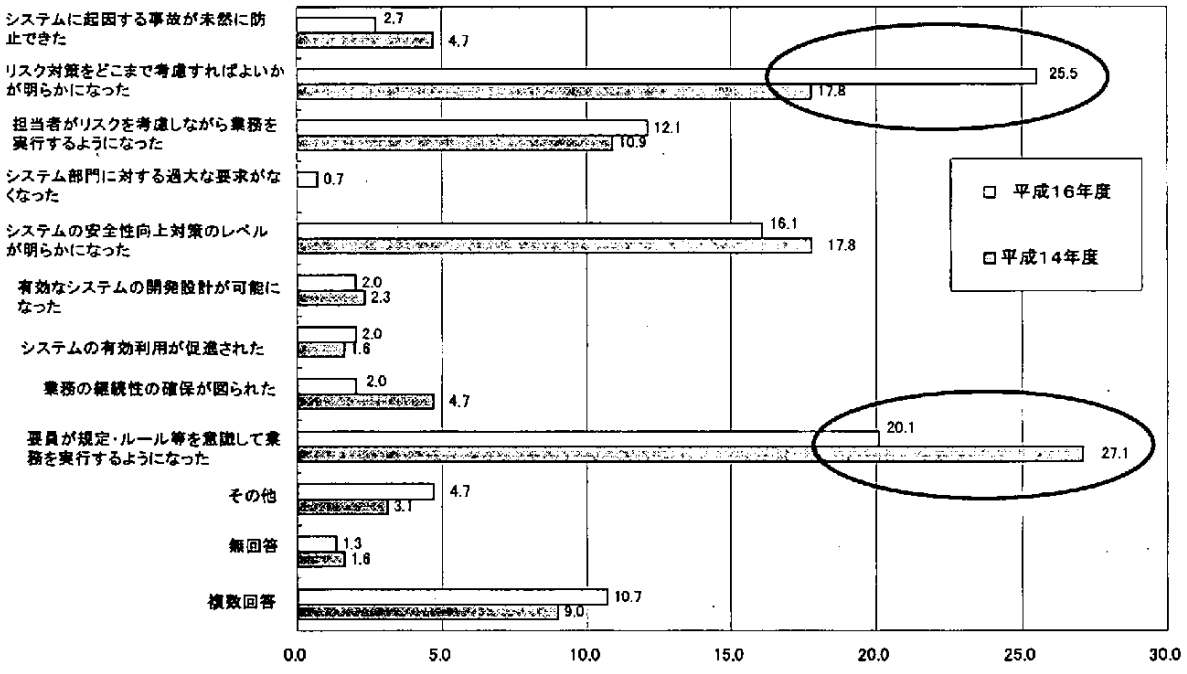

図3－2－13. システム監査の効果(被監査部門)

Q38. 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点を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	0	0.0
3	情報の保護対策の向上	14	9.4
4	セキュリティ対策の向上	57	38.3
5	生産性の向上	0	0.0
6	品質管理の向上	17	11.4
7	規則・手続き等の遵守	21	14.1
8	ドキュメント類の整備	20	13.4
9	作業環境の改善	2	1.3
10	要員管理の適正化	1	0.7
11	その他	2	1.3
無回答		3	2.0
複数回答		12	8.1
計		149	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」(38.3%)、「規則・手続き等の遵守」(14.1%)、「ドキュメント類の整備」(13.4%)が多い。「セキュリティ対策の向上」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(31.8%)に比べ6.5ポイントの増加となった。

平成17年4月の個人情報保護法の本格施行に伴い、「情報の保護対策の向上」の回答が注目されたが、9.4%であり前回調査の 9.3%と同様であった。これは個人情報保護の対応として回答選

択肢の「セキュリティ対策の向上」を回答されたケースが多かったと思われる。

前回調査で平成12年度調査との比較で7.6ポイント増加した「規則・手続き等の遵守」（前回調査23.3%）は、今回調査では前回調査に比較し、9.2ポイント減少した。

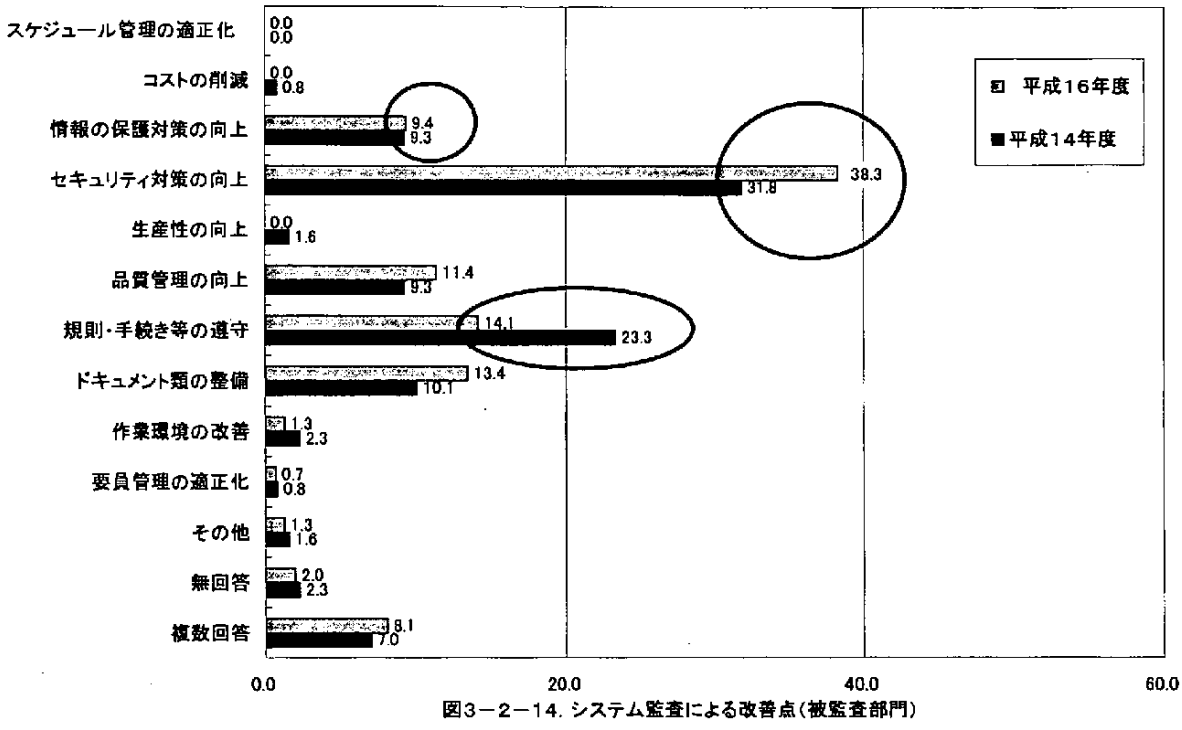

図3－2－14. システム監査による改善点（被監査部門）

Q39. 貴事業体ではシステム監査の結果をどのように活用していますか。

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	173	85.2
2	取引先に対する自社システムの信頼性・安全性・効率性の説明責任	10	4.9
3	わからない	10	4.9
無回答		8	3.9
複数回答		2	1.0
計		203	100.0

今回の調査では、新たな調査項目としてシステム監査の結果の活用を加えた。その回答では、「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」が 85.2%と圧倒的に多かった。事業体活動全体においてステークホルダーに対する「説明責任」が求められてきているが、システム監査においてはその活用に関して、まだ少数であった。

3.2.3 システム監査のあり方について

Q40. 各業務の監査で重視すべき着眼点は何ですか。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	有効性	無回答	複数回答	計
企画業務	12	34	54	16	76	69	6	22	192	18	8	507
	2.4	6.7	10.7	3.2	15.0	13.6	1.2	4.3	37.9	3.6	1.6	100.0
開発業務	14	141	47	22	46	11	131	47	23	18	7	507
	2.8	27.8	9.3	4.3	9.1	2.2	25.8	9.3	4.5	3.6	1.4	100.0
運用業務	144	192	55	18	11	3	7	53	4	12	8	507
	28.4	37.9	10.8	3.6	2.2	0.6	1.4	10.5	0.8	2.4	1.6	100.0
保守業務	141	204	21	16	15	37	11	21	17	16	8	507
	27.8	40.2	4.1	3.2	3.0	7.3	2.2	4.1	3.4	3.2	1.6	100.0

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、被監査部門で最も重視すべきと考えている着眼点を調査した。この調査の選択肢として今回より新たに「有効性」を加えた。

企画業務では、新たな選択肢「有効性」が37.9%でトップであった。その影響で前回調査において27.7%でトップであった「適時性」は13.6%となった。「適時性」より多かったのは「採算性」（15.0%）であり、「有効性」が高かったことで情報システムの効果を重要視する傾向がわかった。

開発業務で多かったのが「信頼性」（27.8%）、「生産性」（25.8%）で、システム開発に責任を持つ被監査部門の意識が表れている。生産性に続いて「機密性」と「効率性」がともに9.3%であった。「効率性」は、情報システムの稼働時の処理の効率性と、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指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37.9%、「安全性」が28.4%と多くなっており、ついで「機密性」が10.8%、「効率性」が10.5%で、この４項目で８割強となっている。

保守業務でも「信頼性」が40.2%、「安全性」が27.8%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。

（監査担当部門の調査対象は、過去２年以内の監査実施事業体が実施した業務に対する着眼点を調査している。分析（Q40）は、「3.1.3」を参照のこと。）

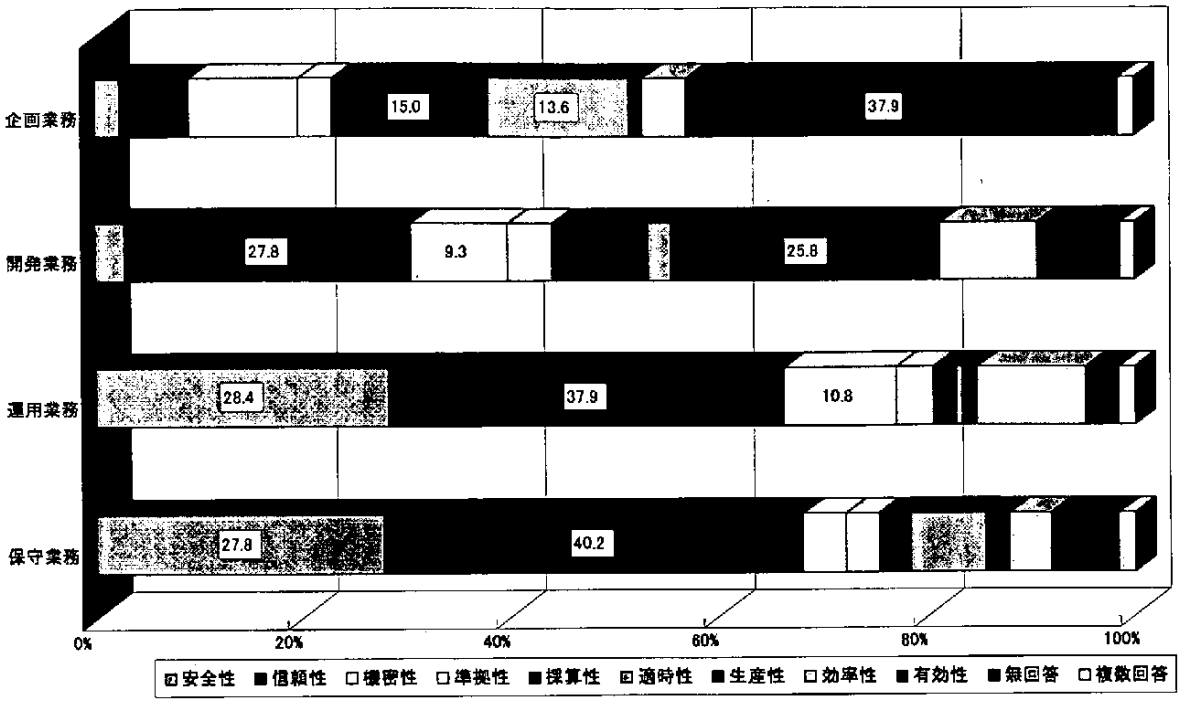

図3－2－15. システム監査で重視すべき着眼点(業務別－被監査部門)

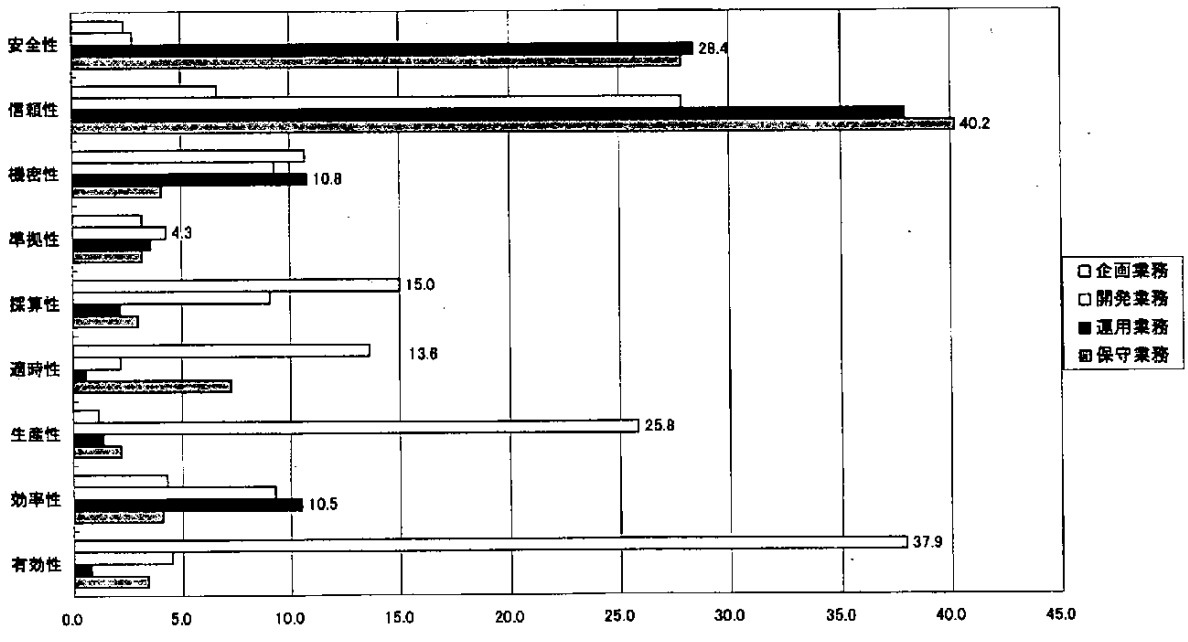

図3－2－16. システム監査で重視すべき着眼点(被監査部門)

Q41. 各テーマの監査で重視すべき着眼点は何ですか。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	有効性	無回答	複数回答	計
ドキュメント管理	22	115	99	105	0	47	7	27	58	24	3	507
	4.3	22.7	19.5	20.7	0.0	9.3	1.4	5.3	11.4	4.7	0.6	100.0
進捗管理	11	62	5	26	6	160	93	81	35	23	5	507
	2.2	12.2	1.0	5.1	1.2	31.6	18.3	16.0	6.9	4.5	1.0	100.0
品質管理	62	295	3	29	7	4	26	11	40	23	7	507
	12.2	58.2	0.6	5.7	1.4	0.8	5.1	2.2	7.9	4.5	1.4	100.0
コスト管理	4	21	4	5	301	6	52	57	31	22	4	507
	0.8	4.1	0.8	1.0	59.4	1.2	10.3	11.2	6.1	4.3	0.8	100.0
要員管理	17	51	24	14	31	61	130	112	38	25	4	507
	3.4	10.1	4.7	2.8	6.1	12.0	25.6	22.1	7.5	4.9	0.8	100.0
外部委託（開発の委託）	25	160	70	15	66	6	52	52	32	24	5	507
	4.9	31.6	13.8	3.0	13.0	1.2	10.3	10.3	6.3	4.7	1.0	100.0
外部委託（ｱｳﾄｿｰｼﾝｸﾞ）	96	163	97	14	44	4	10	33	19	22	5	507
	18.9	32.1	19.1	2.8	8.7	0.8	2.0	6.5	3.7	4.3	1.0	100.0
セキュリティ対策	222	63	143	9	4	7	0	1	35	17	6	507
	43.8	12.4	28.2	1.8	0.8	1.4	0.0	0.2	6.9	3.4	1.2	100.0
ネットワーク管理	150	243	55	6	5	5	1	11	8	18	5	507
	29.6	47.9	10.8	1.2	1.0	1.0	0.2	2.2	1.6	3.6	1.0	100.0
ソフトウェアの適正利用（ライセンス管理）	35	92	19	217	22	25	4	20	45	24	4	507
	6.9	18.1	3.7	42.8	4.3	4.9	0.8	3.9	8.9	4.7	0.8	100.0
個人情報保護対策	104	38	261	54	0	2	0	1	23	20	4	507
	20.5	7.5	51.5	10.7	0.0	0.4	0.0	0.2	4.5	3.9	0.8	100.0
PC管理、モバイル機器管理	123	75	114	34	16	27	10	42	37	25	4	507
	24.3	14.8	22.5	6.7	3.2	5.3	2.0	8.3	7.3	4.9	0.8	100.0
コンピュータウイルス対策	288	71	31	15	1	28	1	3	45	18	6	507
	56.8	14.0	6.1	3.0	0.2	5.5	0.2	0.6	8.9	3.6	1.2	100.0
情報システム関連のリスク管理	211	115	35	18	15	18	0	6	66	19	4	507
	41.6	22.7	6.9	3.6	3.0	3.6	0.0	1.2	13.0	3.7	0.8	100.0
災害対策	300	41	1	7	19	27	0	4	83	20	5	507
	59.2	8.1	0.2	1.4	3.7	5.3	0.0	0.8	16.4	3.9	1.0	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。今回の調査では、回答の選択肢に新たに「有効性」を加えた。

ドキュメント管理では、トップが「信頼性」（22.7%）、ついで「準拠性」（20.7%）、「機密性」（19.5%）となっている。

進捗管理では、「適時性」(31.6%)、「生産性」(18.3%)、「効率性」(16.0%) が多くなっており、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」(25.6%)、「効率性」(22.1%) 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」(31.6%) と高く、ついで「機密性」(13.8%) と「採算性」(13.0%) 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、「信頼性」が最も多く 32.1%であり、ついで「機密性」が 19.1%、「安全性」が 18.9%であり、情報セキュリティを重視する傾向がある。

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。

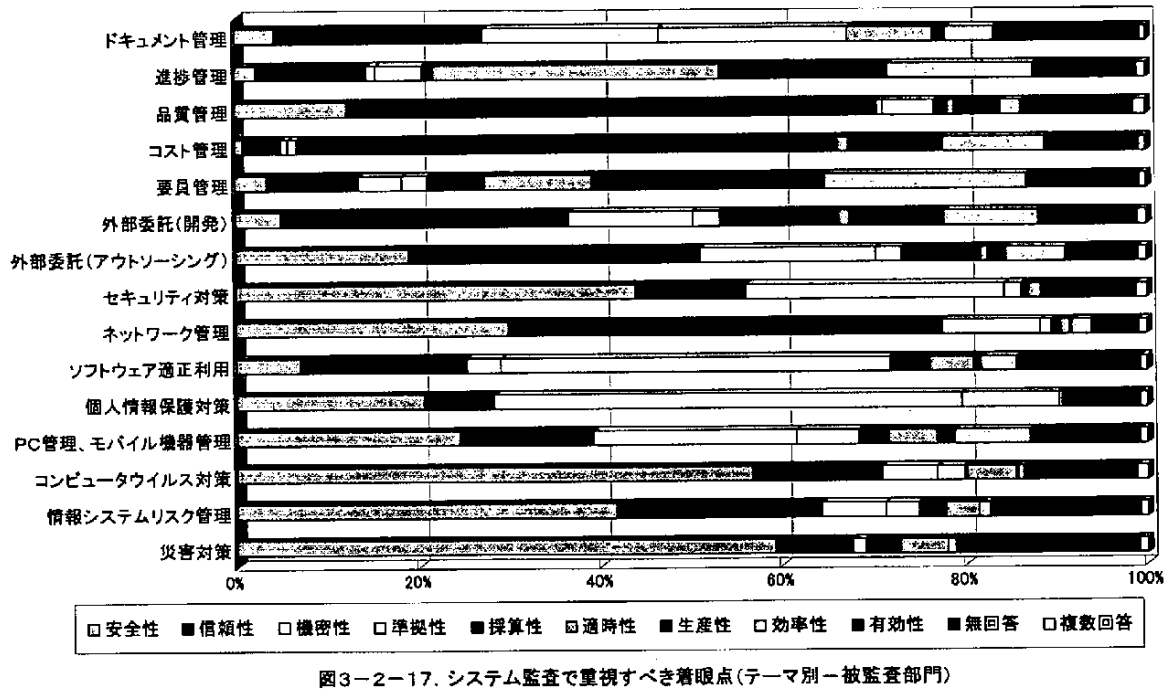

図3－2－17. システム監査で重視すべき着眼点(テーマ別－被監査部門)

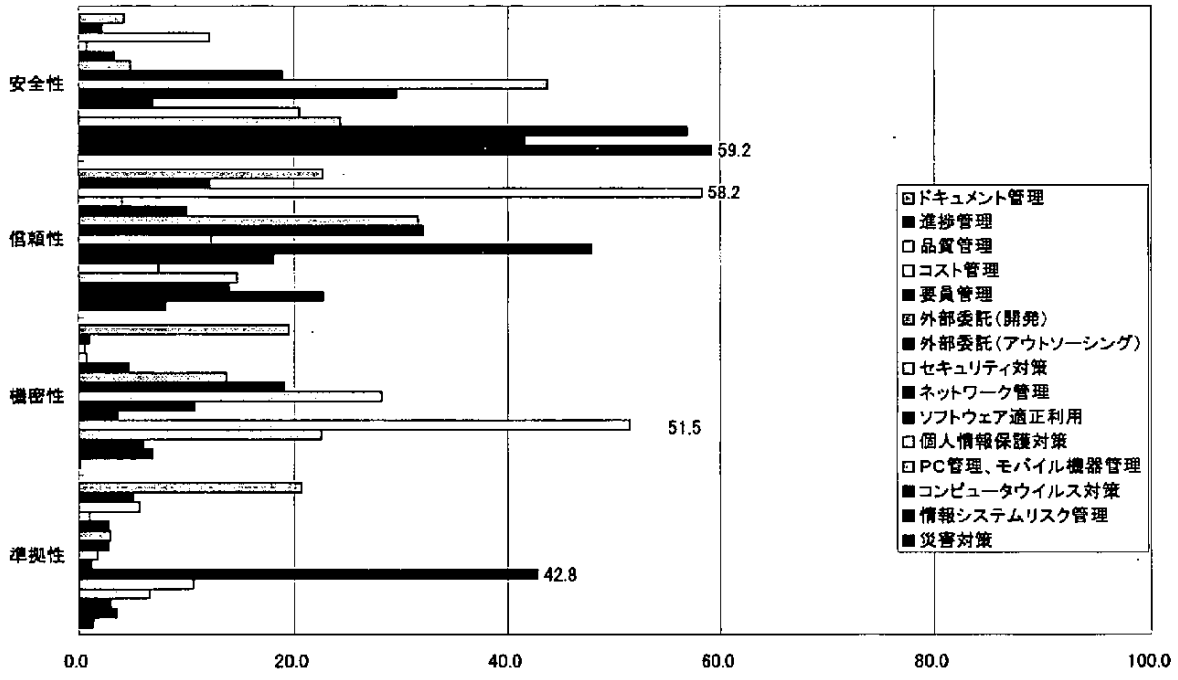

図3－2－18－1. システム監査で重視すべき着眼点(被監査部門)

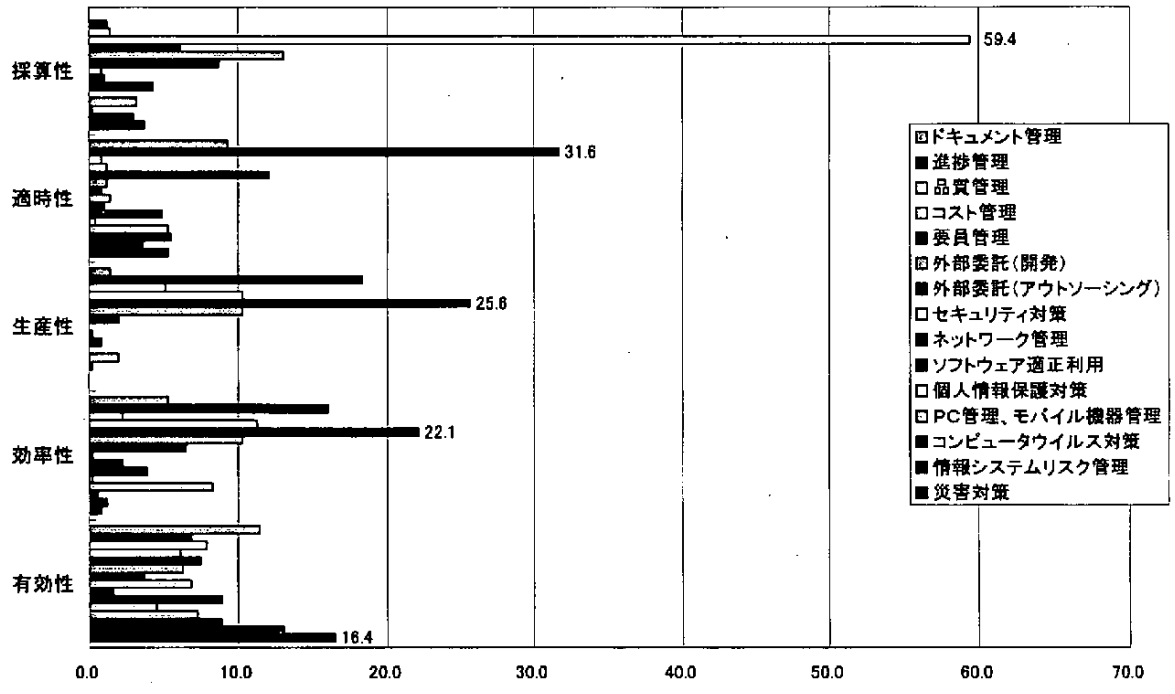

図3－2－18－2. システム監査で重視すべき着眼点(被監査部門)

Q42. 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。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	ハードウエア(注1)	ソフトウエア(注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	12	13	18	8	32	204	45	9	3	7	134	0	18	4	507
	2.4	2.6	3.6	1.6	6.3	40.2	8.9	1.8	0.6	1.4	26.4	0.0	3.6	0.8	100.0
ヒューマンエラー防止	87	38	6	31	224	27	20	35	0	13	1	0	19	6	507
	17.2	7.5	1.2	6.1	44.2	5.3	3.9	6.9	0.0	2.6	0.2	0.0	3.7	1.2	100.0
事故防止	5	36	3	33	90	64	49	32	88	8	33	35	25	6	507
	1.0	7.1	0.6	6.5	17.8	12.6	9.7	6.3	17.4	1.6	6.5	6.9	4.9	1.2	100.0
災害対策	3	3	1	0	6	149	5	5	100	6	64	138	24	3	507
	0.6	0.6	0.2	0.0	1.2	29.4	1.0	1.0	19.7	1.2	12.6	27.2	4.7	0.6	100.0
個人情報保護	2	11	46	0	21	351	24	6	2	3	22	0	16	3	507
	0.4	2.2	9.1	0.0	4.1	69.2	4.7	1.2	0.4	0.6	4.3	0.0	3.2	0.6	100.0

注１）CPUと周辺機器／注）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について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）」（40.2%）、「ネットワーク」（26.4%）が圧倒的に多かった。監査担当部門に対する調査（Q42）では、「情報保管(データ管理)」（37.4%）が圧倒的であり、ついで「入退出（館）管理」（13.5%）であった。監査担当部門の「ネットワーク」は 7.6%であり、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」（44.2%）、「データの入力プロセス」（17.2%）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」（17.8%）、「ハードウェア」（17.4%）が高くなっている。

災害対策では「情報保管（データ管理）」（29.4%）、「電源設備」（27.2%）、「ハードウェア」（19.7%）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）」（69.2%）と圧倒的に多い。（監査担当部門に関する分析（Q42）は、「3.1.3」を参照のこと。）

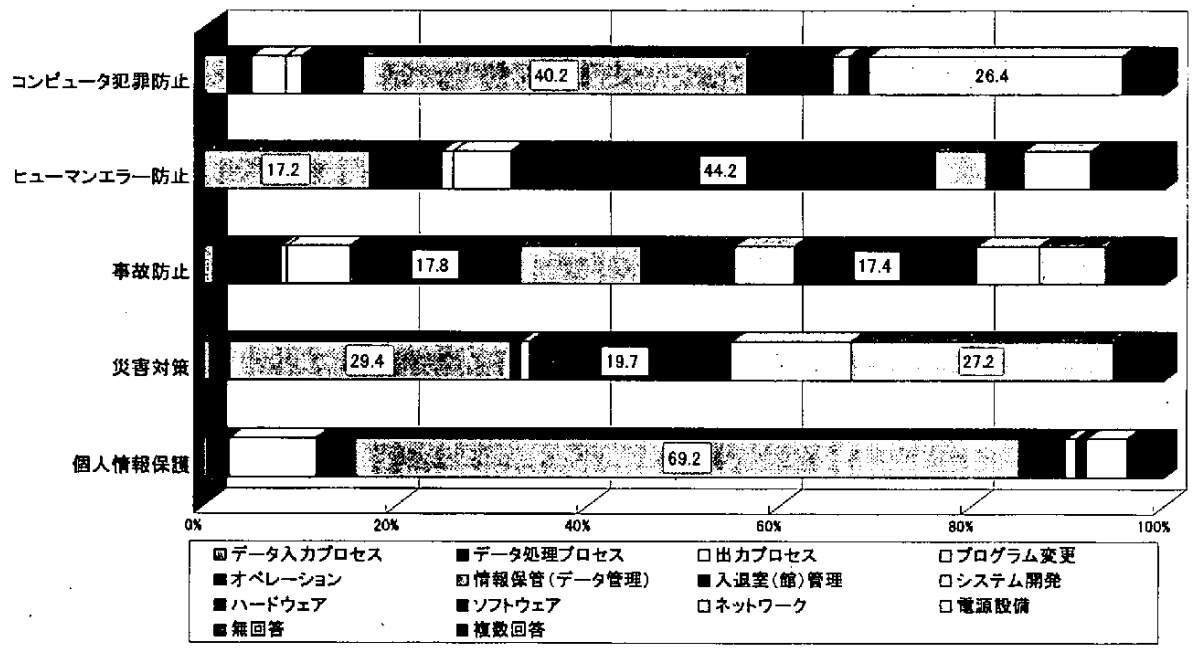

図3－2－19. コンピュータ犯罪防止、ヒューマンエラー防止、事故防止、災害対策、個人情報保護の観点から最も重視すべき分野(被監査部門)

Q43. 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点を１つ選んで下さい。

1	監査計画	98	19.3
2	事前調査	50	9.9
3	実地調査	102	20.1
4	改善勧告内容	117	23.1
5	監査報告会	28	5.5
6	チェックリスト	93	18.3
7	その他	3	0.6
無回答		16	3.2
計		507	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」(23.1%) が高く、ついで「実地調査」(20.1%)、「監査計画」(19.3%) となっている。

Q44. 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。最も効果的だと思われる者を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)	28	5.5
2	内部の監査人	77	15.2
3	情報システム部門の要員	12	2.4
4	システム監査技術者試験合格者	56	11.0
5	監査法人・公認会計士	131	25.8
6	システム監査企業台帳に基づくシステム監査企業	180	35.5
7	その他	7	1.4
無回答		16	3.2
計		507	100.0

被監査部門のQ23、監査担当部門のQ37の調査結果でもわかるように、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」(35.5%)を挙げている。ついで「監査法人・公認会計士」(25.8%)であり、「内部の監査人」(15.2%)は3番目となっている。監査担当部門に対する同一の調査(Q25)では、「内部の監査人」(42.6%)と圧倒的に高く、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(Q25)は、「3.1.2」を参照のこと。)

その他の意見としては、「システム経験のある内部の監査人」、「経営的視点から見る監査人と技術的視点から見る監査人のチーム」、「自社基準に基づき、育成と判定により監査人を育てる」等が挙げられた。

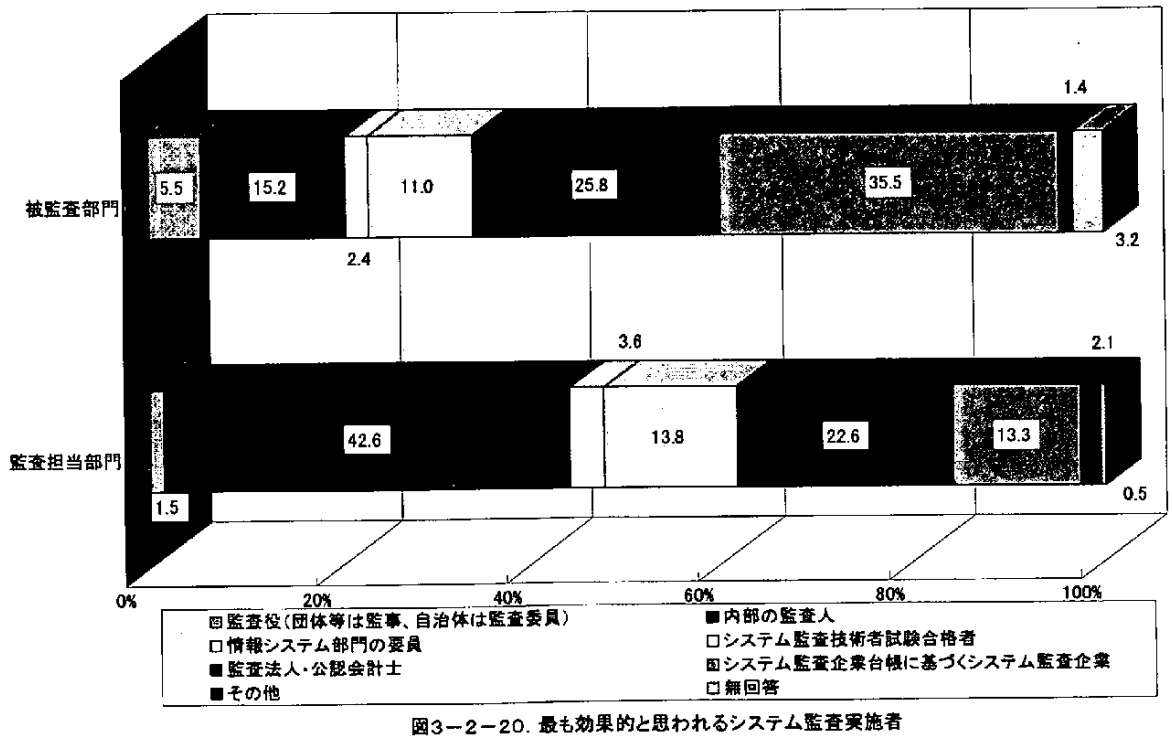

図3−2−20. 最も効果的と思われるシステム監査実施者

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15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15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/03sec.htm

（Q45～Q52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。）

Q45. 貴事業体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	269	53.1
2	現在作成中である	87	17.2
3	作成を検討している	98	19.3
4	現在、定める予定がない	47	9.3
無回答		6	1.2
計		507	10.0

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53.1%であり、「現在作成中」を含めると70.3%、さらに、「作成を検討している」を含めると89.6%とほぼ9割の事業体が情報セキュリティポリシーについて積極的な姿勢であることがわかる。これは、前回調査の「定めている」が34.4%、「現在作成中」を含めると56.1%であったことと比較すると、大きく変革したことがわかる。この傾向は、監査担当部門でもほぼ同様であり、日本の情報セキュリティがこの数年で大きく変化し始めたことが見て取れる。なお、前回調査では、監査部門と被監査部門で大きく結果が違っており、監査担当部門の方が、意識が高いと論じた。しかし、今回は、両部門とも同率の89.6%となり、両部門での認識の差は解消されつつあるといえよう。

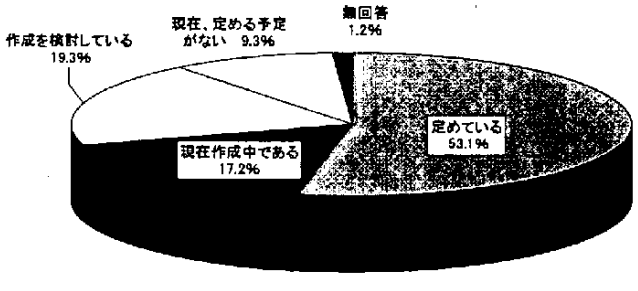

図3－2－21. 情報セキュリティポリシーの策定状況
（平成16年度－被監査部門）

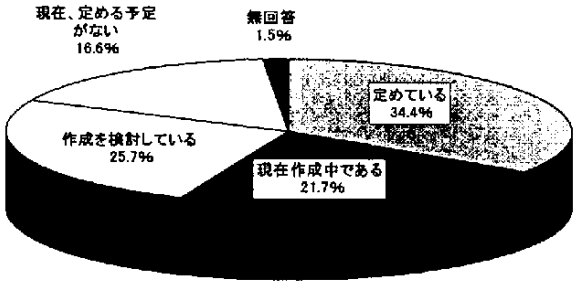

図3－2－22. 情報セキュリティポリシー策定状況
（平成14年度－被監査部門）

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	269	53.1	279	46.1
2	現在作成中である	87	17.2	78	12.9
3	作成を検討している	98	19.3	98	16.2
4	現在、定める予定がない*)	47	9.3	147	24.3
無回答		6	1.2	3	0.5
計		507	10.0	605	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【4】である）

（出典：JIPDEC　平成15年度「情報セキュリティに関する調査」Q24）

今回調査と平成15年度「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7ポイント増加している。また、「現在作成中」を含めると11.3ポイント、さらに「作成を検討している」を含めた場合も14.4ポイント増加しており（情報セキュリティ調査：75.2%）、この1年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15年の情報セキュリティ監査制度の発足、また、平成17年4月の個人情報保護法の完全施行に向けて情報セキュリティ対策の重要性が高く認知されるに至ったことが挙げられる。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、さらには、情報セキュリティ監査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。

資本金と情報セキュリティポリシーの策定状況をみると、やはり企業規模と策定に大きな相関が見られる。資本金が大きいほど情報セキュリティポリシーを「策定している」比率が高く、資本金が小さいほど「定める予定がない」が高くなっている。今後は、このような企業規模として小規模事業者に対する情報セキュリティに関する取組みをどのように進めるかが重要となると考えられる。

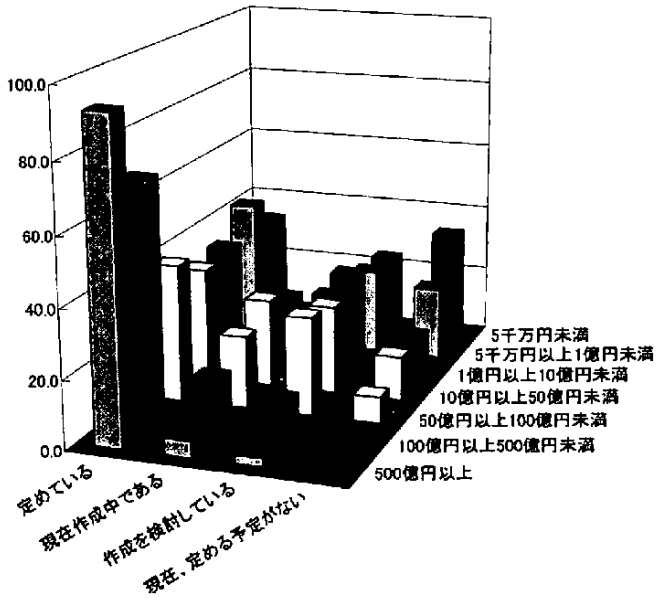

図3－2－23. セキュリティポリシー策定状況（資本金規模別－被監査部門）

Q46. 貴事業体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		507	-
1	情報セキュリティ担当役員を設置している	150	29.6
2	情報セキュリティ委員会を設置している	187	36.9
3	情報システム部門主導で実施している	240	47.3
4	情報セキュリティ専任者を設置している	85	16.8
5	各部門・拠点にセキュリティ担当者を設置している	156	30.8
6	外部のセキュリティコンサルタントを活用している	44	8.7
7	特に実施していない	79	15.6
8	その他	9	1.8
無回答		9	1.8

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」は前回調査の15.6%から29.6%に14ポイント増、「情報セキュリティ委員会の設置」は前回調査の20.6%が36.9%に16.3ポイント増と、両者ともに倍以上となっている。逆に、「情報システム部門主導で実施している」は、前回調査が52.4%であったものが47.3%と5.1ポイント減少している。これは、情報セキュリティ対策が情報システム部門から経営陣に移ったことがわかる。すなわち、情報セキュリティは情報システム部門のものではなく、全社的なものとなったことが伺える。

なお、「情報セキュリティ専任者」については前回調査の10.3%が16.8%に6.5ポイント増、「各部門・拠点ごとのセキュリティ担当者の設置」については前回調査の17.7%が30.8%へと13.1ポイント増加している。これは、監査担当部門の「情報セキュリティ専任者」(15.2%)、「各部門・拠点ごとのセキュリティ担当者の設置」(30.6%)とほぼ同様の傾向となり、企業は情報セキュリティ対策に人的な面でも力をいれていることがわかる(Q66)。

「外部セキュリティコンサルタントの活用」(8.7%)については、前回の6.3%と比べあまり増加していない。一方、担当役員や専任者・担当者が大きく増加していることから、企業は外部のリソースで対応するよりも、内部のリソースで、長期的に対応しようとしていることがわかる。

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、長い間、情報システム部門に依存してきた流れが大きく変わろうとしている転機であることがわかる。日本も今後、経営者が関与するようになり、より、ガバナンス面からの情報セキュリティ対策が進むと考えられる。

管理者の設置状況		情報システムの管理者		情報セキュリティの管理者	
1	定めている	487	80.5	396	65.5
2	設置を検討している	45	7.4	88	14.5
3	定めていない	67	11.1	116	19.2
4	必要ない	0	0.0	0	0.0
無回答		6	1.0	5	0.8
計		605	100.0	605	100.0

(出典:JIPDEC 平成15年度「情報セキュリティに関する調査」Q27)

「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。

「情報セキュリティ管理者」について、平成15年度情報セキュリティ調査では「定めている」が65.5%と、13年度（セキュリティ調査）の52.8%の1.24倍であった。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」の合計は47.6%と前回調査（システム監査調査）の28.0%の1.7倍となった。今回調査では、セキュリティ推進体制に関する調査であり、具体的な担当者の増加よりも、より、組織面での体制から捉えられた結果であり、単純に比較はできないが、この数字からも、情報セキュリティが経営面への課題と変わりつつあることがわかる。

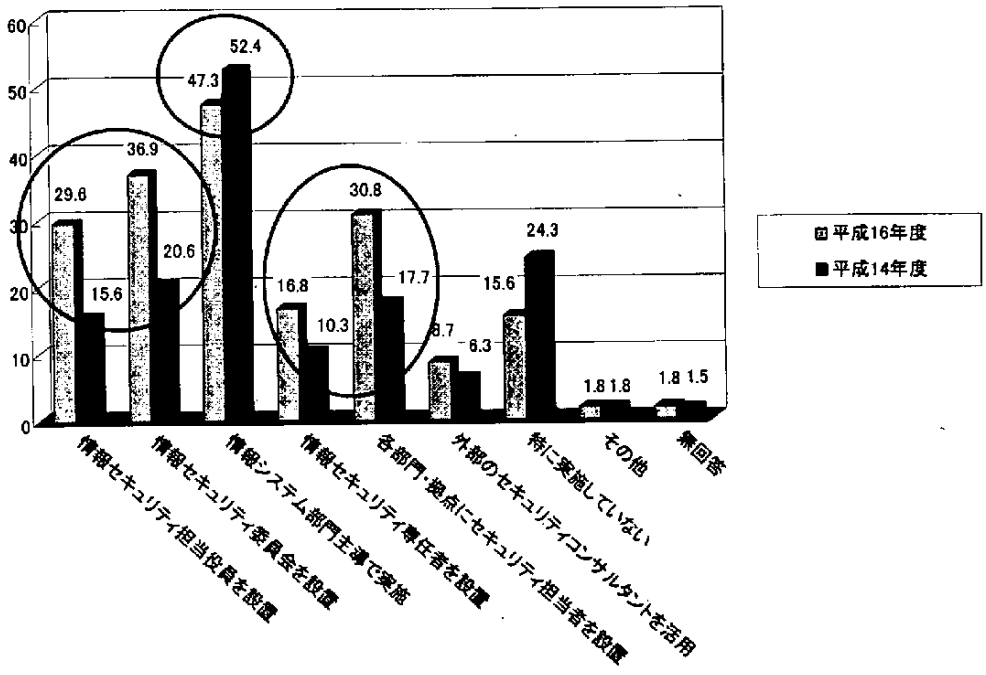

図3－2－24. 情報セキュリティ推進体制（被監査部門）

Q47. 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	119	23.5
2	全社的な推進体制	250	49.3
3	情報システム部門の推進体制	25	4.9
4	利用部門の理解・協力	101	19.9
5	その他	1	0.2
無回答		2	0.4
複数回答		9	1.8
計		507	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、「経営者のリーダーシップ」が23.5%（前回調査21.6%）、「全社的な推進体制」が49.3%（前回調査48.2%）であり、両者をあわせると72.8%となり、前回調査（69.8%）ともあまり変化はなく、経営者や全社的な体制に対する希望には大きな変化はないと考えられる。Q46での情報セキュリティ担当役員の設置が前回調査の15.6%から29.6%へと急増したことと比べると、経営者のリーダーシップへの希

望はそれほど大きくない。経営陣の関与が増えてきたわりには経営者自体の関わりが明確なトップダウン型になりきっていないことがみてとれる。

この結果からは、情報セキュリティの推進には、利用部門からのボトムアップで進めていく方がよいというようにみえる。一方、「利用部門の理解・協力」について、前回調査では 22.5%とボトムアップ型が明確であったが、今回調査では 19.9%と 20%を割り込んでいて、ボトムアップにもそれほど期待されていないことがわかる。ただし、全社的な推進体制については高いままであることを考えると、トップダウン、ボトムアップを組み合わせた折衷形による新しい推進モデルが必要になってきているといえよう。

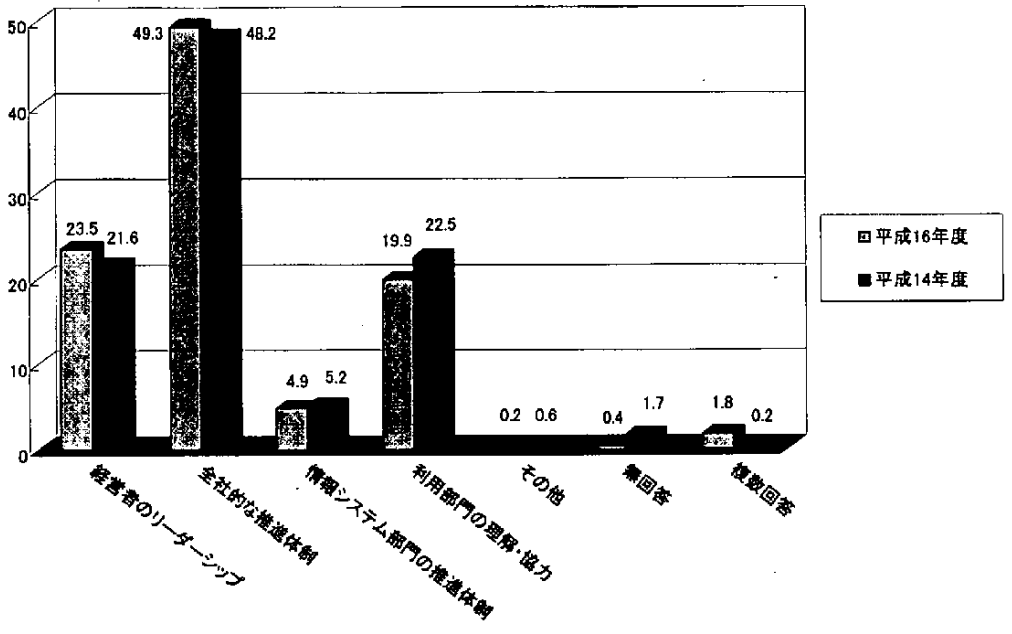

図3－2－25. 情報セキュリティ推進にあたっての意識(被監査部門)

Q48. 貴事業体で情報セキュリティについて、優先的に実施していることを３つまで選んで下さい。(複数回答)

1	情報セキュリティ対策コストの確保	122	24.1
2	リスク分析の実施	148	29.2
3	システム監査の実施	57	11.2
4	情報セキュリティ監査の実施＊	51	10.1
5	情報セキュリティ教育の実施	219	43.2
6	情報セキュリティ体制の確立	218	43.0
7	情報セキュリティアドミニストレータの確保	10	2.0
8	情報資産の洗い出し	176	34.7
9	ISMS の取得	42	8.3
10	プライバシーマークの取得	52	10.3
11	その他	8	1.6
12	特に実施していない	78	15.4
無回答		9	1.8
複数回答(4つ以上を選択)		2	0.4

事業体が情報セキュリティを推進する場合、さまざまな対策を行わなければならないが、その一方で新システム管理基準の冒頭で述べている全体最適化、さらには、コーポレートガバナンスとの整合をとる必要がある。また、情報セキュリティ対策には費用（新しい設備の導入や運用費用）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。この質問では、企業や組織が、どのような情報セキュリティ対策を優先し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、「情報セキュリティ教育」（今回：43.2%、前回：38.7%）、「情報セキュリティ体制の確立」（今回：43.0%、前回：48.5%）、「情報資産の洗い出し」（今回：34.7%、前回：23.3%）、「リスク分析の実施」（今回：29.2%、前回：26.0%）、「情報セキュリティ対策コストの確保」（今回：24.1%、前回：23.3%）となっており、きわめて妥当なものである。ただし、今回調査の特徴としては、情報セキュリティ教育が前回調査から4.5ポイント増え、全体のトップとなったことである。また、「情報資産の洗い出し」が11.4ポイント、「ISMSの取得」（今回：8.3%、前回：3.7%）が4.6ポイント、「プライバシーマークの取得」（今回：10.3%、前回：3.5%）が6.8ポイント増加した。これは、個人情報漏洩の対策としての情報セキュリティの重要性が認識され、認知度が高まったことによると考えられる。なお、重要度の順番については、監査担当部門、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：15.9%、被監査：24.1%）と「情報セキュリティ監査」（監査：16.2%、被監査：10.1%）については回答に差がでている。これは、監査担当部門の場合、情報セキュリティ監査実施という立場から、コントロールを高める必然性を強く認識しているものと思われる。なお、対策コストが相対的に低いのは、監査担当部門はコストに対する責任がないため、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。被監査担当部門にとっては、情報システムのコスト要素を重視していると考えるのが妥当であろう。（監査担当部門に関する分析（Q69）は、「3.1.5」を参照のこと。）

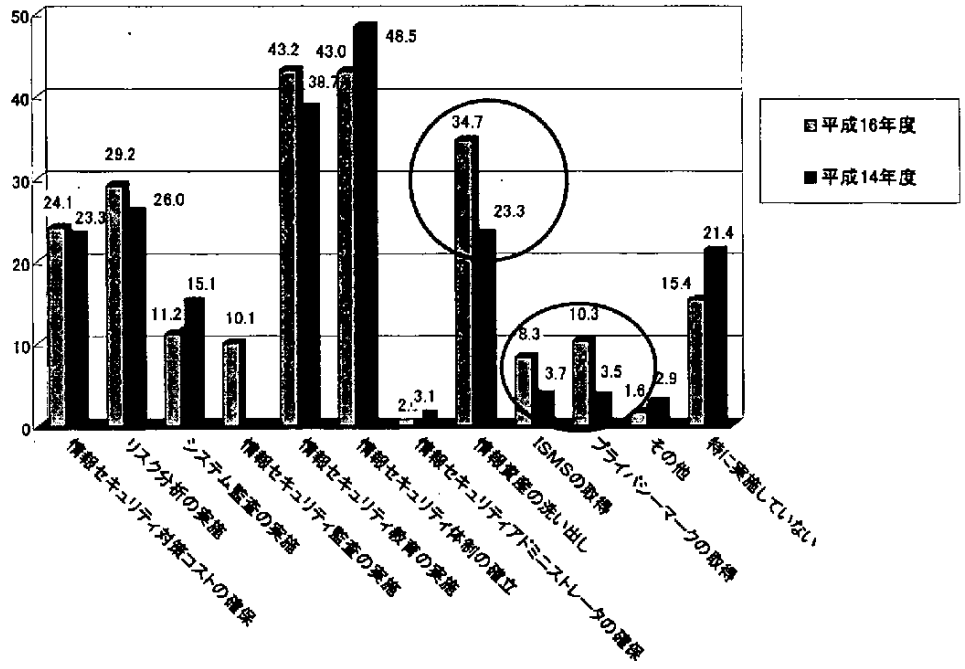

図3－2－26. 情報セキュリティ推進対策（被監査部門）

なお、図 3-2-27 は、「システム監査の実施」と「情報セキュリティ監査の実施」とを優先している対外事業者を業種別にみたものである。これをみると、内部統制が重要視される商業や金融・保険業では、システム監査が優先されている。一方、政府・地方公共団体や情報処理サービス産業、製造業では、情報セキュリティ監査が優先されていることがわかる。すなわち、サービス産業では、内部統制よりも、サービス提供に関わる不正やサービス妨害などの対策が重視されていると考えられる。情報セキュリティが重要となってきていることが伺える。

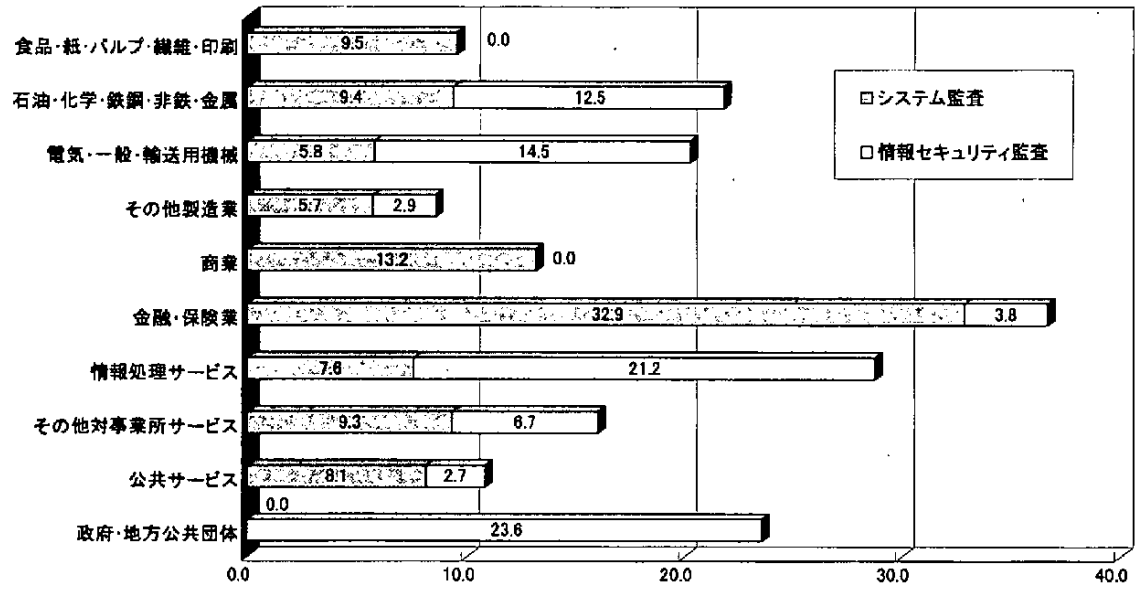

図3－2－27. 情報セキュリティ推進対策
（システム監査／セキュリティ監査－被監査部門）

リスク分析の実施状況			
1	実施している	181	29.9
2	実施していない	328	54.2
3	実施する予定がある	91	15.0
無回答		5	0.8
計		605	100.0

（出典：JIPDEC　平成 15 年度「情報セキュリティに関する調査」Q13）

今回の調査では「リスク分析の実施」が 29.2%であった。一方、平成 15 年度「情報セキュリティ調査」では 29.9%であった。両者でほぼ同様の結果が得られたのは興味深い。また、「情報資産の洗い出し」が 34.7%であることを考えると、今後 30%を超えて増加すると考えられる。ただし、「情報セキュリティ調査」では「実施していない」という回答が 50%を超えている。しかし、回答事業体の半数が実施していないという事実を理解し、日本の情報セキュリティの底上げには一層の情報資産の洗い出し、リスク分析、情報セキュリティ対策の流れを PR する必要がある。

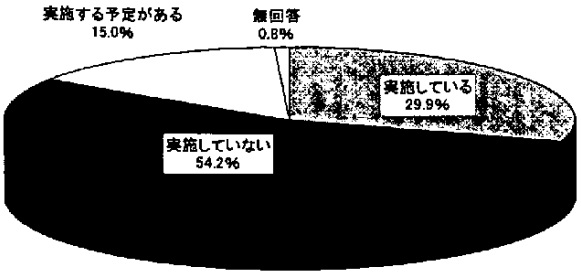

図3－2－28. リスク分析の実施状況
（平成15年度[情報セキュリティに関する調査]）

Q49. 貴事業体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		507	-
1	新入社員教育を実施している	172	33.9
2	一般社員向け教育を実施している	242	47.7
3	管理職教育を実施している	122	24.1
4	役員教育を実施している	37	7.3
5	派遣要員向け教育を実施している	60	11.8
6	情報セキュリティ担当者の専門教育を実施している	55	10.8
7	その他	22	4.3
8	特に実施していない	147	29.0
無回答		23	4.5

今回の調査結果を前回調査と比べると、大きく変わったのは情報セキュリティ教育を「特に実施していない」比率が前回の 41.4%から 29.0%へと大きく減少した点である。すなわち、情報セキュリティ教育を実施する企業や組織が増加したことがわかる。また、「新入社員教育を実施している」が、前回調査の 25.6%から 33.9%へと 8.3 ポイント増加し、「一般社員向け教育を実施している」が、前回調査の 35.3%から 47.7%へと 12.4 ポイント増加した点である。同様に、数値的には大きくはないが、「管理職教育を実施している」が、13.9%から 24.1%へと 10.2 ポイント増、「役員教育を実施している」が 3.5%から 7.3%へと倍増している。すなわち、情報セキュリティ教育は、新人、社員、管理職、役員などすべての企業構成員向けの教育が重視されてきているといえよう。

前回調査では、『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。』と述べていた。すなわち、今回調査時点で、個人情報漏洩関係で調査する中で、各社ともに全社的に情報セキュリティに対する認識（アウァネス）が低い点が問題の根底にあることがわかり、再教育を実施するようになった、と考えられる。

ただし、今回調査で気になるのは、「情報セキュリティ担当者の専門教育を実施している」が前回から減少した点である。一般社員向けの教育も重要であるが、専門家のスキルを高めることも引き続き重要な点であり、これを避けて通ることはできない。情報セキュリティに対する犯罪や攻撃が、16 年度でみても、フィッシング攻撃、コンピュータウイルスの増大、なりすまし犯罪、

個人情報漏洩など、ますますレベルの高いものとなっている中、専門家育成を怠ると、タイムリーな対策が打てず、大きな被害に繋がる危険性が高くなる。

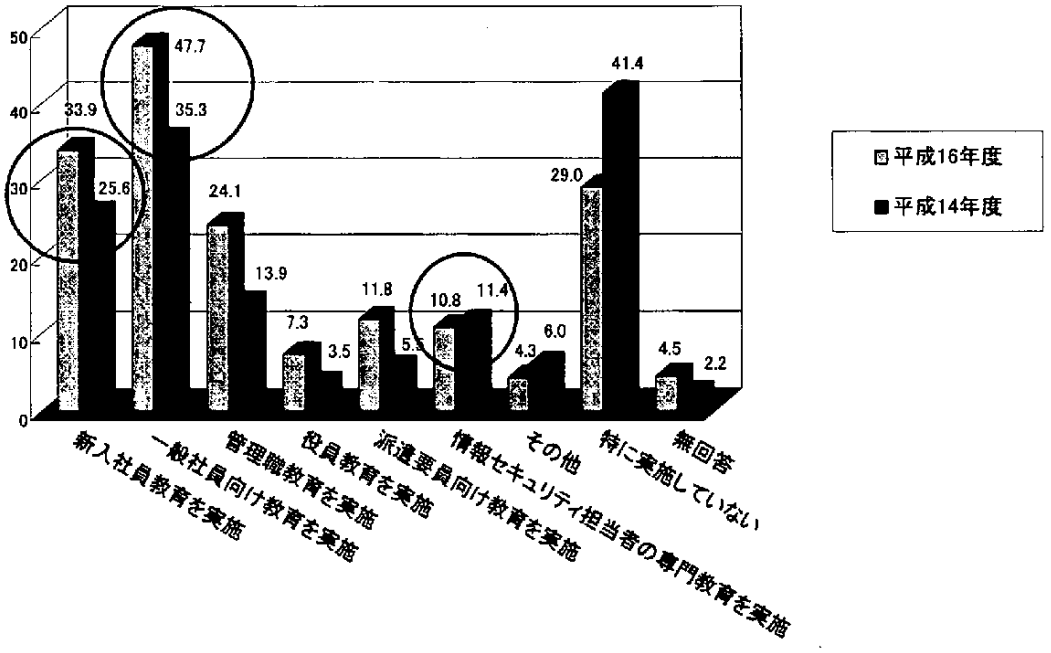

図3－2－29. 情報セキュリティ教育の実施状況（被監査部門）

なお、情報セキュリティ教育の実施状況を業種別にみると、情報処理サービス、政府・地方公共団体、公共サービス、その他対事業所サービスなどサービス産業では何らかの教育を実施しているのに対し、一次産業、製造業、商業での情報セキュリティ教育への意向は高くない。情報セキュリティ教育は、すべての産業に関係することから、産業を越えて広がるための支援策が必要といえよう。

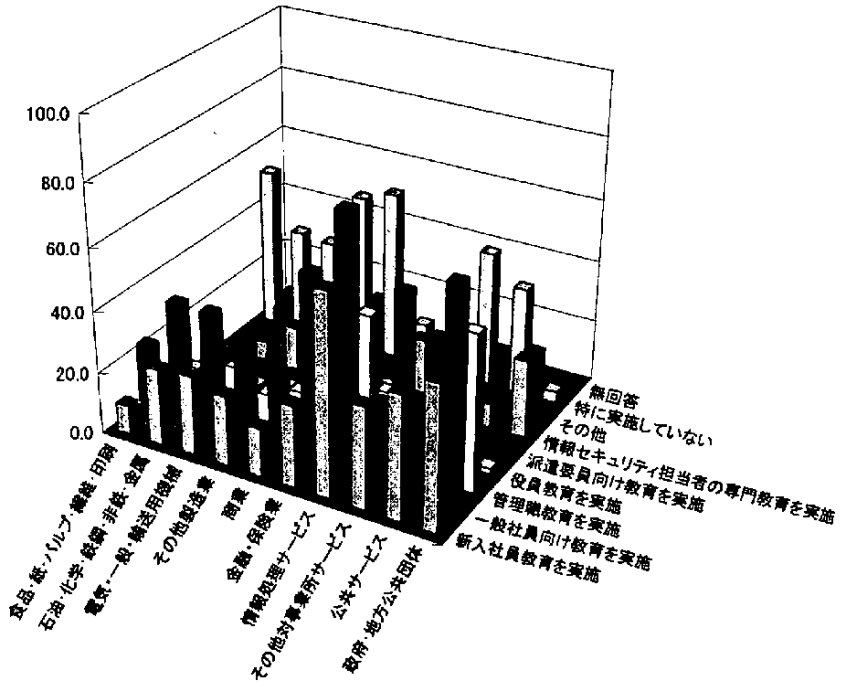

図3－2－30. 情報セキュリティ教育の実施状況（業種グループ別－被監査部門）

Q50. 貴事業体では情報セキュリティ監査を受けたことがありますか。

1	あ る	91	17.9
2	これから受ける予定がある	52	10.3
3	な い	341	67.3
無回答		23	4.5
計		507	100.0

今回調査では、情報セキュリティ監査の実施状況について調査した。情報セキュリティ監査制度は平成15年度に導入されており、２年目となる16年にどの程度の事業体が受診したかについて調査した。その結果からは、17.9%の事業体がすでに監査を受けており、システム監査の受診と比較すると、２年目としてはまずまずの数字といえよう。

なお、受診した事業体の特性と調べると、従業員数との相関が強いことがわかる。従業員規模が多いほど、情報セキュリティ監査を受診、またはこれから受ける予定があるといえよう。一方、規模が小さいほど、否定的な回答が多いことがわかる。

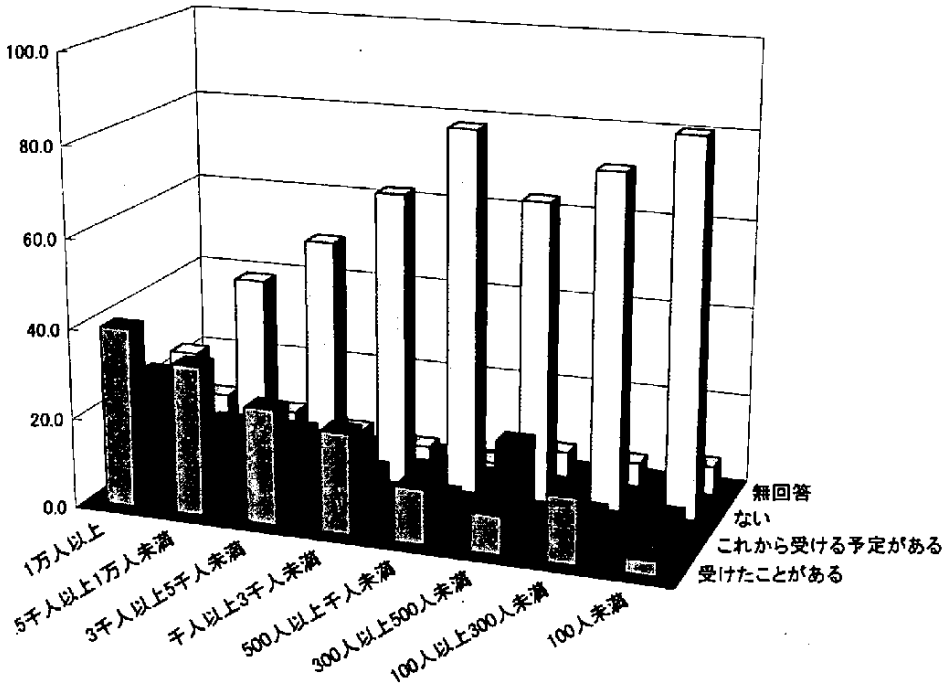

図3－2－31. 情報セキュリティ監査実施状況
（従業員数規模別－被監査部門）

Q51. 貴事業体では情報セキュリティ監査を外部に委託したいと思いますか。

1	思 う	266	52.5
2	思わない	205	40.4
無回答		36	7.1
計		507	100.0

情報セキュリティ監査制度は、外部監査、内部監査のどちらも可能となっているが、監査実施を外部に求めるかの調査を行ったところ、外部への委託要望が高いことがわかる。とくに、業種別では、政府・地方公共団体では、87.3%が外部への委託を希望している。

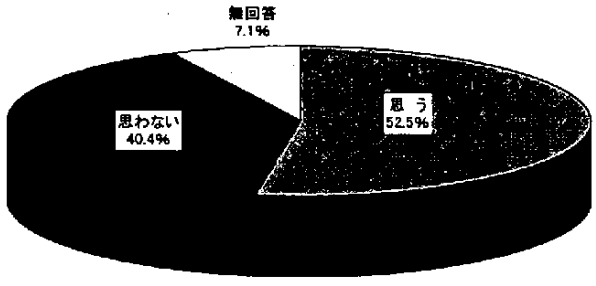

図3－2－32. 情報セキュリティの外部委託(被監査部門)

Q52. 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	認定を取得している	39	7.7
2	知っている	339	66.9
3	知らない	103	20.3
無回答		26	5.1
計		507	100.0

ISMS適合性認証制度の認知度は、前回調査の46.4%から、今回調査では「認定を取得している」の7.7%と「知っている」の66.9%を含めると74.6%にまで増加した。(前回調査では「認定取得」については調査を行っていない)。

業種別にみると、情報サービス産業は、今回調査では40.9%が認定を取得しており、48.5%が「知っている」となっている。一方、金融・保険では、3.8%が認定を取得、70.9%が「知っている」となっている。なお、認定を受けている事業体に関しては、資本金別や従業員との関連性はあまりなかったが、情報セキュリティが必要な事業体が取得していることがわかる。

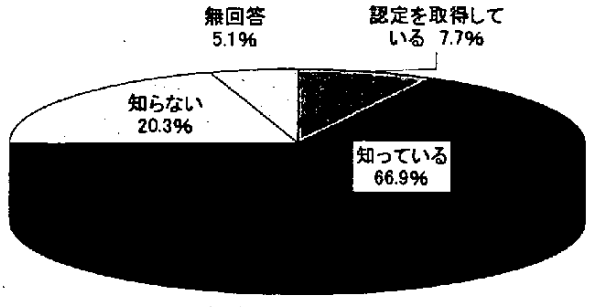

図3－2－33. ISMS適合性評価制度の認知度(被監査部門)

3.2.5　個人情報保護について

ここでは、今回調査と平成15年度に実施した「情報セキュリティ調査」で共通する個人情報保護関連項目について、比較分析を併せて行っている。

（Q53～Q58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、「3.1.6」を参照のこと。）

Q53.「個人情報の保護に関する法律（平成15年5月30日法律第57号）」を知っていますか。

1	内容を知っている	333	65.7
2	制定されたことを知っている	144	28.4
3	知らない	6	1.2
無回答		24	4.7
計		507	100.0

平成17年4月の「個人情報の保護に関する法律」全面施行の影響もあり、この法律の認知度（「内容を知っている」、「制定されたことを知っている」の合計）は監査担当部門の94.5%と同様、94.1%と高い。

個人情報漏洩の多発と罰則を伴う法律の施行は、企業活動に大きな影響を及ぼすこともあり、「内容を知っている」との回答自体、65.7%と高い値になっている。

平成15年度「情報セキュリティに関する調査」で情報システム部門に対して実施された同じ調査では、認知度が90.5%であり、今回の調査では3.6ポイント増加した。

業種別にみると、情報処理サービス業が「内容を知っている」87.9%、「制定されたことを知っている」10.6%で認知度が98.5%となっている他、金融・保険業も「内容を知っている」82.3%、「制定されたことを知っている」12.7%で認知度95.0%と高い値を示している。

Q54. 経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成16年10月公表）を知っていますか。

1	内容を知っている	249	49.1
2	公表されたことを知っている	170	33.5
3	知らない	65	12.8
無回答		23	4.5
計		507	100.0

経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」は、この調査の実施がガイドライン公表（平成16年10月）から間もない時期であったことを考慮すると、認知度（「内容を知っている」49.1%、「制定されたことを知っている」33.5%）82.6%は非常に高いといえる。また、監査担当部門の認知度78.0%より高くなっている。

特に情報処理サービス業では、「内容を知っている」80.3%、「制定されたことを知っている」が15.2%であり、合計の認知度は95.5%と非常に高い値を示し、情報処理サービス業の監査担当部門の認知度92.5%よりも高い。

個人情報の多くがデータベース化され、情報システムとして取り扱われていることから、情報システム部門での関心は高く、監査担当部門よりも認知度において高い値を示していると想定される。

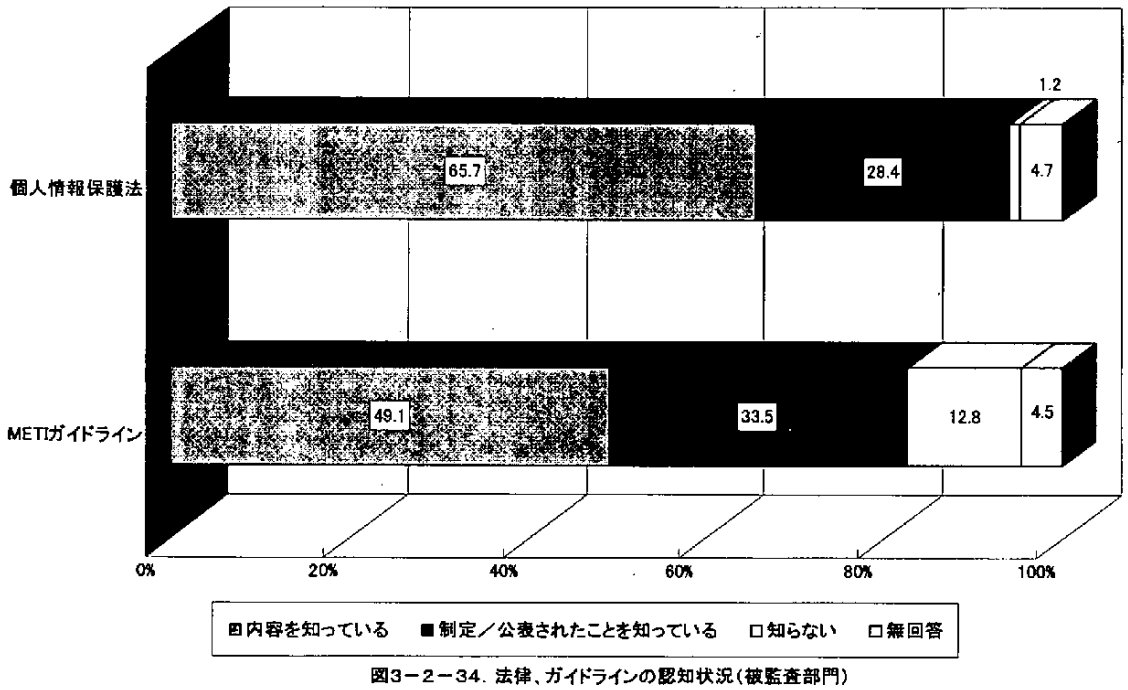

図3－2－34. 法律、ガイドラインの認知状況(被監査部門)

Q55. 現在の個人情報の管理状況についてリスクをどのように認識していますか。

1	対応策を講じているので、リスクはないと認識している	43	8.5
2	現状の管理方法で何も問題が発生していないので、リスクはないと認識している	62	12.2
3	何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	138	27.2
4	いつ問題が発生してもおかしくない状況であると認識している	155	30.6
5	その他	52	10.3
6	特に認識していない	30	5.9
無回答		27	5.3
計		507	100.0

個人情報の管理状況について、リスクの有無を監査担当部門と同様に以下のように集計した。

・「リスクはない」・・・・26.6%（上記１、２、６の合計）

・「リスクはある」・・・・57.8%（上記３、４の合計）

「リスクはある」との認識は57.8%と高い反面、認識していないも含めた「リスクはない」も26.6%と約４分の１以上が「個人情報に関するリスクはない」としている点は、注目に値する。

業種別にみると、金融・保険業の「何度かヒヤリ・ハッとした経験があり、リスクがあると認識している」が35.4%、「いつ問題が発生してもおかしくない状況であると認識している」が36.7%で、「リスクはある」が72.1%と最も高い値であるが、監査担当部門の80.6%よりも低い値となっている。

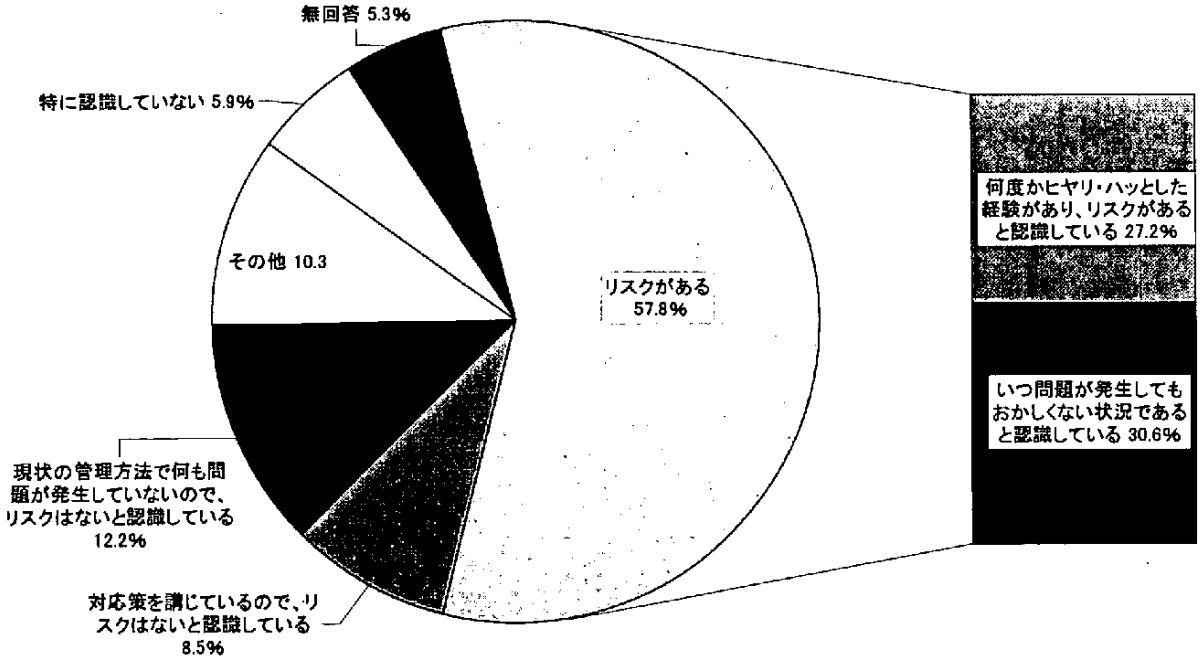

図3－2－35. 個人情報管理状況のリスク認識度(被監査部門)

Q56. 個人情報保護対策として、①現在何を実施していますか。②また、今後どういうことを実施する予定ですか。(複数回答)

対　策	①現在実施している対策		②今後実施を予定している対策	
回答件数	507	-	507	-
プライバシーポリシーを策定している	138	27.2	178	35.1
管理責任者を置いている(保護体制(役割、責任、権限)を確立する)	203	40.0	147	29.0
個人情報保護に関する規程を定め運用している	165	32.5	207	40.8
個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している	61	12.0	118	23.3
社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している	118	23.3	199	39.3
定期的に監査を実施している	99	19.5	143	28.2
リスク分析を実施して必要な安全対策を構築している	111	21.9	173	34.1
苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している	151	29.8	120	23.7
仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている	117	23.1	154	30.4
その他	7	1.4	9	1.8
特に対策を講じない	168	33.1	24	4.7
無回答	36	7.1	139	27.4

注) ①ですでに導入している対策については、②の集計の対象外とし、「無回答」に含んでいる。

現在実施している対策は、「管理責任者の設置」(40.0%) が最も高く、次いで「個人情報保護規程制定・運用」(32.5%) となっているが、この他に30%を超えて実施している対策はない。その一方で「特に対策を講じない」も33.1%もあり、3社に1社は何も実施していない状況といえる。

平成15年度「情報セキュリティ調査」で情報システム部門に行った同様の調査でも、今回調査同様、「管理責任者の設置」(36.0%)、「個人情報保護規程制定・運用」(34.7%) の他に30%を超える対策はなく、ほとんど昨年度と変わらない状況となっている。

今後実施予定の対策としては、「個人情報保護規程の制定・運用」40.8%、「個人情報保護教育の実施」39.3%、「プライバシーポリシー策定」35.1%、「リスク分析の実施と安全対策」34.1%という結果であった。平成15年度「情報セキュリティ調査」では、今後実施予定の30%を超える対策が存在しなかったことから、個人情報保護への取組みを急いでいる状況が読み取れる。

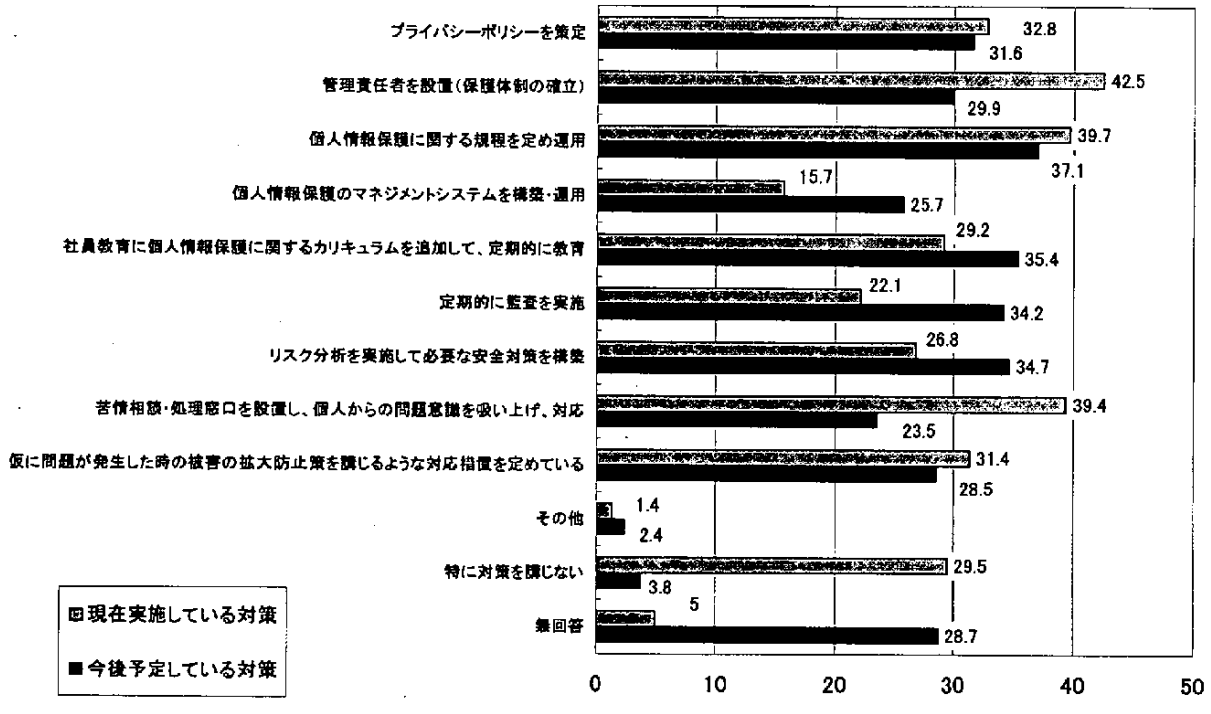

図3－2－36. 個人情報保護対策(被監査部門)

Q57. 貴事業体では個人情報保護の監査を外部に委託したいと思いますか。

1	思う	208	41.0
2	思わない	264	52.1
無回答		35	6.9
計		507	100.0

個人情報保護の監査の外部委託については、委託したいと「思わない」(52.1%) が、「思う」(41.0%) を上回ったが、業種別にみると、公共サービスは「思う」(62.2%) が「思わない」(27.0%) を、金融・保険業では「思う」(57.0%) が「思わない」(36.7%) を、情報処理サービスでは「思う」(50.0%) が「思わない」(48.5%) をそれぞれ上回っている。

監査担当部門では、外部に委託したいと「思う」が「思わない」を上回る業種はなかったが、

情報システム部門では、公共サービス、金融・保険業、情報処理サービスの３業種で上回る結果となった。

Q58. プライバシーマーク制度を知っていますか。

1	認定を取得している	42	8.3
2	知っている	397	78.3
3	知らない	44	8.7
無回答		24	4.7
計		507	100.0

前回調査では、プライバシーマークの認知度は、「知っている」(54.5%) が「知らない」(45.5%) を僅かに上回っている状況であった。

今回の調査では、プライバシーマーク制度が平成17年4月の個人情報保護法全面施行への対策としても注目を集めていることもあり、「知っている」(78.3%) に「認定を取得している」(8.3%) も加えた認知度は、86.6%と前回調査の54.5%よりも32.1ポイントも増加し、ほとんどが知る状況となった。また、情報システム部門の認知度は、監査部門の認知度78.2%よりも高くなっている。

業種別にみると、情報処理サービス業では、「認定を取得している」が51.5%と過半数を超え、「知っている」(45.5%) との合計は97.0%で、認知度は非常に高い値を示している。

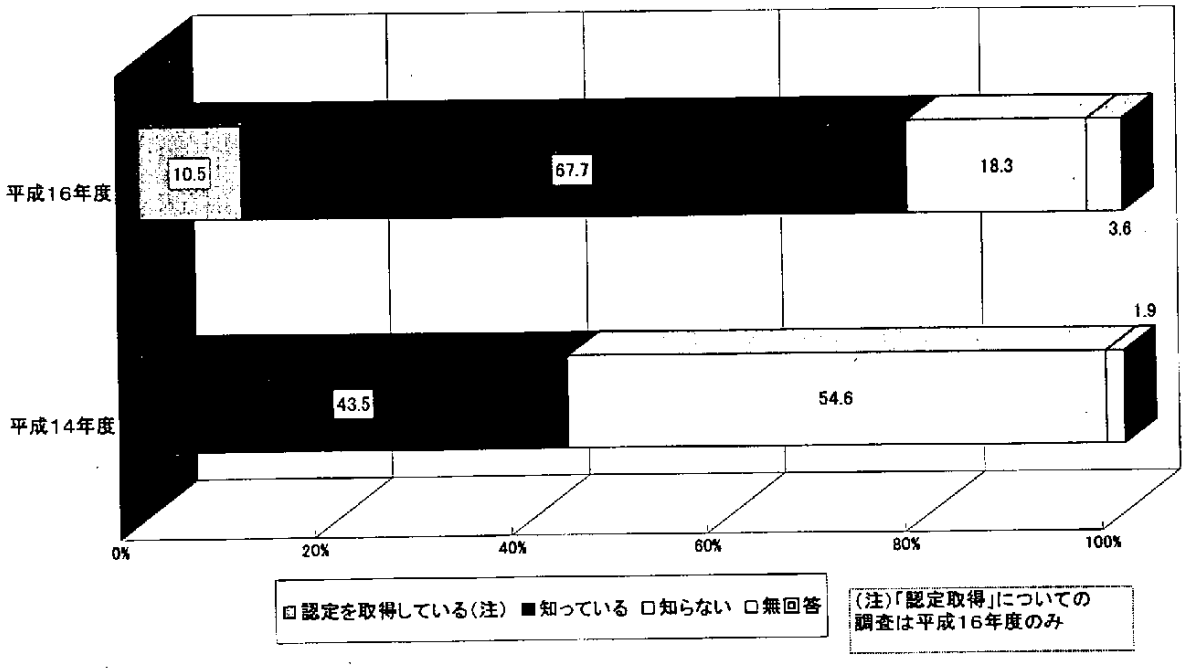

図3－2－32. プライバシーマーク制度の認知状況(被監査部門)

3.3 クロス集計結果分析

3.3.1 クロス集計対象項目

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
1	Q25. 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。	Q28. 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)
		Q29. 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。	
		Q30. 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。	
2	Q37. 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)	Q66. 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)	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)
3	Q57. 監査報告会に出席したのは誰ですか。(複数回答)	Q67. 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る経営者の関与
4	Q65. 貴事業体では情報セキュリティポリシーを策定していますか。	Q22. 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
		Q70. 貴事業体では情報セキュリティ監査を実施したことがありますか。	
		Q72. 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
5	Q68. 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)	Q47. 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)
		Q50. 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。	
		Q53. 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。	
6	Q67. 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。	Q62. 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
7	Q75. 現在の個人情報の管理状況についてリスクをどのように認識していますか。	Q76.個人情報保護対策として、 ①現在何を実施していますか。 ②今後実施を予定している対策	個人情報に対するリスク認識と対策実施の関係

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
1	Q23. 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)	Q44. 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
2	Q33. 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。	Q27. (システム監査人に対し)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
		Q28. システム監査を受けた時、現場の負担はありましたか。	
		Q29. 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)	
		Q30. 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。	
3	Q43. 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。	Q27. (監査人に対し)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
		Q31. 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。	
		Q32. 監査報告会に情報システム部門から出席しましたか。	
4	Q45.貴事業体では情報セキュリティポリシーを策定していますか。	Q19.貴部門では、システム監査を受け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
		Q50.貴事業体では情報セキュリティ監査を受けたことがありますか。	
		Q52.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
5	Q46. 貴事業体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	Q23. 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
6	Q55. 現在の個人情報の管理状況についてリスクをどのように認識していますか。	Q56.個人情報保護対策として、 ①現在何を実施していますか。 ②今後実施を予定している対策	個人情報に対するリスク認識と対策実施の関係

3.3.2 監査担当部門対象

1.「Q25. 効果的と思うシステム監査実施者」（有効回答件数：195 件）のクロス集計

×Q28. システム監査人に不足していると思われる知識

Q28 不足している知識 / Q25 効果的と思う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		情報システムの知識	
監査役	3	0	0.0	1	33.3	0	0.0	1	33.3	1	33.3
内部の監査人	83	12	14.5	20	24.1	8	9.6	12	14.5	22	26.5
情報システム部門の要員	7	1	14.3	1	14.3	1	14.3	0	0.0	3	42.9
システム監査技術者試験の合格者	27	4	14.8	8	29.6	4	14.8	2	7.4	5	18.5
監査法人・公認会計士	44	2	4.5	12	27.3	0	0.0	7	15.9	9	20.5
システム監査企業	26	1	3.8	9	34.6	2	7.7	3	11.5	7	26.9
その他	4	0	0.0	1	25.0	0	0.0	0	0.0	1	25.0
無回答	1	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
計	195	20	10.3	52	26.7	15	7.7	25	12.8	48	24.6

Q28 不足している知識 / Q25 効果的と思う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	0	0.0	0	0.0	0	0.0	0	0.0
内部の監査人	2	2.4	5	6.0	1	1.2	1	1.2
情報システム部門の要員	0	0.0	0	0.0	1	14.3	0	0.0
システム監査技術者試験の合格者	0	0.0	3	11.1	1	3.7	0	0.0
監査法人・公認会計士	1	2.3	10	22.7	2	4.5	1	2.3
システム監査企業	0	0.0	3	11.5	1	3.8	0	0.0
その他	0	0.0	0	0.0	2	50.0	0	0.0
無回答	0	0.0	1	100.0	0	0.0	0	0.0
計	3	1.5	22	11.3	8	4.1	2	1.0

このクロス分析では、前回調査同様、監査担当部門が『効果的と思うシステム監査実施者』に対して、何に対し不満を感じているか、を分析している。『効果的と思うシステム監査実施者』に『内部の監査人』に対する回答が最も多いのは前回と同様であるが、クロス集計した場合、『不足している知識』として「情報システムの知識」が第１位に挙がっていることが今回の調査結果の特徴である。前回調査では「業務知識」がトップであり、「情報システムの知識」は、今回調査ほどの比重を占めていなかったのである。第１位となった原因として考えられるのが、ここ数年来の情報システムの構成の変化である。現在の情報システムの技術進歩は、目覚しいものがあり、新しい技術が日々生み出されている現状がある。このような状況の中で、内部の監査人が現在の情報システムに対し、監査ができるだけのスキルを保有できておらず、十分な監査ができないという現状を問題視してい

ると考えられる。サーバの構成やネットワークの安全性について監査を行うには、専門的な知識が必要となる。また、実際、サーバやネットワークの構成上の不備により、コンピュータウイルスの情報システム全体への侵入や外部からのホームページの書換えや顧客情報を含んだ個人情報の流出などの事件も多く発生している。残念ながら、ネットワークやシステムに関する相当高い専門知識を有していなければ、これらの事件を監査で防ぐことはできない。システム監査の監査人として、さまざまな技術スキルを有する内部の技術者を参加させるだけでなく、情報セキュリティ監査や外部からのシステムへの侵入（アタック）テストなどを組み合わせるなど、情報システムの複雑化に伴い、監査もいくつかの手法を組み合わせる必要がある。

『内部の監査人』の不足している知識において、前回第１位であった「業務知識」は、今回「情報システムの知識」と僅差で２位となっている。事業体では自社の業務知識が外部の監査人より精通しており、より正確な監査を期待して監査人を内部から採用している場合が多い。調査では、この意図が期待はずれな結果となっていることを示している。今後は、内部の研修による業務知識の向上だけでなく、社内でも業務に精通していると認められている要員を監査人に当てるなど、監査人の任命に際しても考慮する必要がある。

『効果的と思うシステム監査実施者』として２番目に回答の多い『監査法人・公認会計士』での『不足している知識』は、前回同様「業務知識」がトップであった。これは予想された結果であったが、第２位が「わからない」と回答している点が注目できる。これは、監査法人や公認会計士にシステム監査を依頼したが、結果として満足できていないことを表わしている可能性がある。情報システムの多様化・複雑化のため、監査法人や公認会計士のシステム監査だけでは十分な効果が得ることは難しく、システム監査の実施にあたってはITガバナンスを中心に行い、その他は先の『内部の監査人』で述べたと同様、情報セキュリティ監査などの他の監査と組み合わせることにより効果を発揮する。

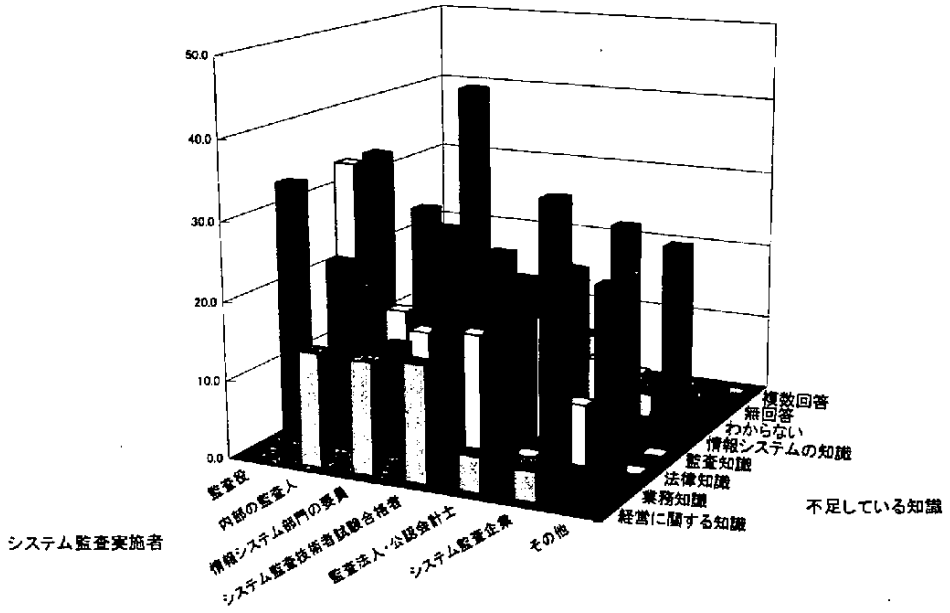

図３－３－１. 効果的と思うシステム監査実施者 × システム監査人に不足している知識
（監査担当部門）

×Q29. システム監査人に不足していると思われる能力

Q29.不足している能力 / Q25. 効果的と思う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	3	0	0.0	2	66.7	0	0.0	0	0.0
内部の監査人	83	17	20.5	30	36.1	14	16.9	6	7.2
情報システム部門の要員	7	1	14.3	5	71.4	0	0.0	0	0.0
システム監査技術者試験の合格者	27	3	11.1	12	44.4	2	7.4	1	3.7
監査法人・公認会計士	44	5	11.4	13	29.5	4	9.1	3	6.8
システム監査企業	26	5	19.2	7	26.9	4	15.4	2	7.7
その他	4	1	25.0	1	25.0	0	0.0	0	0.0
無回答	1	0	0.0	0	0.0	0	0.0	0	0.0
計	195	32	16.4	70	35.9	24	12.3	12	6.2

Q29.不足している能力 / Q25. 効果的と思うシステム監査実施者	その他		わからない		無回答	
監査役	0	0.0	1	33.3	0	0.0
内部の監査人	4	4.8	9	10.8	3	3.6
情報システム部門の要員	0	0.0	0	0.0	1	14.3
システム監査技術者試験の合格者	1	3.7	6	22.2	2	7.4
監査法人・公認会計士	1	2.3	15	34.1	3	6.8
システム監査企業	0	0.0	7	26.9	1	3.8
その他	0	0.0	0	0.0	2	50.0
無回答	0	0.0	1	100.0	0	0.0
計	6	3.1	39	20.0	12	6.2

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する。最も回答が多く寄せられた『内部の監査人』に対するクロス回答では、今回も「分析能力」の不足に多くの回答が寄せられた。次に多かったのは「インタビュー能力」であった。被監査部門から監査項目に対し的確なインタビューを行い、回答を分析する能力を身に付けるには、大変なスキルが必要であり、一長一短では育成できない。長期的な視野に立った監査人教育が必要といえる。また、前回と異なり、『内部の監査人』の項目で大きく減ったクロス回答が、「報告書作成能力」である。これは、おそらく監査担当部門が監査チェックシートや報告書のフォーマットを準備することにより、監査人の能力に係らず一定レベルの報告が可能になっていると想定される。内部の監査人の「分析能力」や「インタビュー能力」の不足を補い、効果的な監査を行うべく監査担当部門が努力したことが伺われる。

『監査法人・公認会計士』や『システム監査企業』など外部委託した場合のクロス回答で最も多いのが「わからない」である。これは、外部委託した場合は、①概ね満足しているという捉え方と、②不満は感じているが、何が問題か明確にわからないが何らかの能力が欠如していると考えている、の両方が考えられる。監査担当部門がシステム監査を外部委託し、監査結果に満足しているのであれば、外部委託が非常に有効な監査手段であるといえる。外部委託の場合でも、２番目に多いクロス回答はやはり「分析能力」であった。この分野では、外部委託者もスキルの底上げを期待したい。

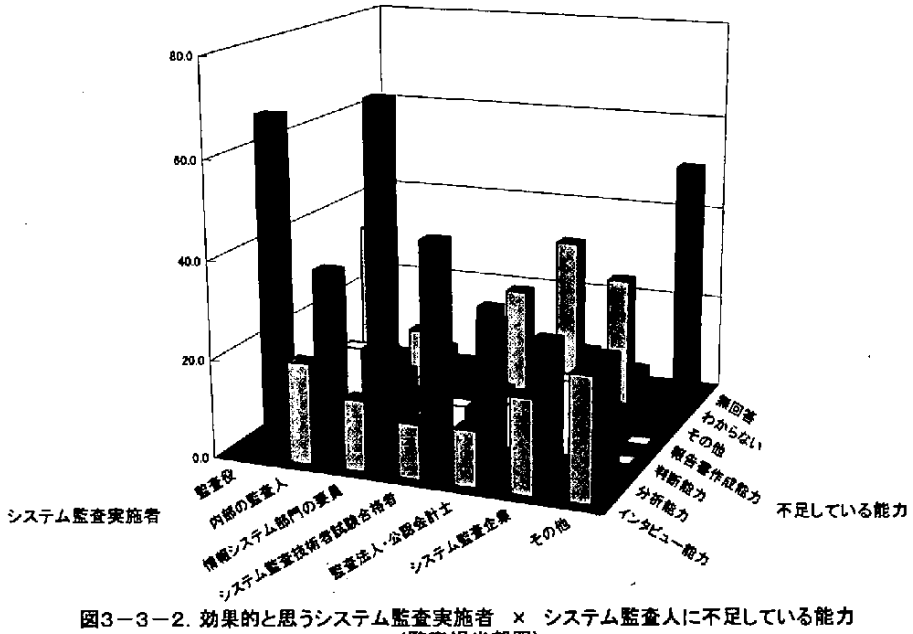

図3－3－2. 効果的と思うシステム監査実施者 × システム監査人に不足している能力
（監査担当部門）

×Q30. システム監査人に対する教育方法

Q30. システム監査人に対する教育方法 / Q25.効果的と思われる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	3	0	0.0	0	0.0	0	0.0	0	0.0
内部の監査人	83	36	43.4	3	3.6	18	21.7	1	1.2
情報システム部門の要員	7	2	28.6	1	14.3	2	28.6	0	0.0
システム監査技術者試験の合格者	27	12	44.4	2	7.4	3	11.1	1	3.7
監査法人・公認会計士	44	4	9.1	1	2.3	1	2.3	0	0.0
システム監査企業	26	8	30.8	2	7.7	2	7.7	0	0.0
その他	4	1	25.0	0	0.0	1	25.0	0	0.0
無回答	1	0	0.0	0	0.0	0	0.0	0	0.0
計	195	63	32.3	9	4.6	27	13.8	2	1.0

Q30. システム監査人に対する教育方法 / Q25.効果的と思われる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	
監査役	1	33.3	1	33.3	1	33.3	0	0.0
内部の監査人	2	2.4	15	18.1	5	6.0	3	3.6
情報システム部門の要員	0	0.0	1	14.3	0	0.0	1	14.3
システム監査技術者試験の合格者	2	7.4	4	14.8	1	3.7	2	7.4
監査法人・公認会計士	0	0.0	9	20.5	26	59.1	3	6.8
システム監査企業	0	0.0	10	38.5	4	15.4	0	0.0
その他	0	0.0	0	0.0	0	0.0	2	50.0
無回答	0	0.0	1	100.0	0	0.0	0	0.0
計	5	2.6	41	21.0	37	19.0	11	5.6

このクロス分析では、監査担当部門が監査人に対してどのような教育を行ったかを検証するものである。『監査法人・公認会計士』や『システム監査企業』などの外部委託の場合を除き、各項目とも最も多かったのは、「外部セミナーの利用」である。これは、自組織内に有効な育成カリキュラムを持たない場合や自組織内に監査人育成カリキュラムをもつ場合でも、より広い視野を持つのに有効な手段であり、予想どおり活用している監査担当部門が多かった。次に多い教育方法としては、OJT を挙げている事業体が多かった。問題は OJT の内容にある。経験の多い監査人の下で監査を行い、システム監査の勘所を体得する体制が整った事業体であれば特に問題はない。しかし、事業体の中には、本人任せで特に教育体制の整っていない場合も見受けられる。本人任せにせず、「外部セミナーの利用」や「OJT」により、監査人を育成するためのカリキュラムを作成し、教育を行った監査人には保有スキルを検証できるようにすることが肝要である。監査担当組織において、このような監査人育成のための体制を構築することは工数的にも金銭的にも大きな負担ではあるが、システム監査の質の低下により発生するトラブル（システム障害、個人情報漏洩など）による事業体の損失を考えれば、かえって短工数、低コストであることを考慮されたい。

2.『Q37. システム監査実施方式』（有効回答件数：171 件）のクロス集計

×Q66. 情報セキュリティの推進体制

Q66. 情報セキュリティ推進体制 / Q37. システム監査の実施方式	回答件数	情報セキュリティ担当役員を設置		情報セキュリティ委員会を設置		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	
内部監査部門型	104	53	51.0	50	48.1	51	49.0	29	27.9
部門監査型	13	8	61.5	7	53.8	9	69.2	2	15.4
指名方式	5	4	80.0	4	80.0	1	20.0	1	20.0
委員会方式	6	1	16.7	4	66.7	1	16.7	1	16.7
チームアプローチ	12	5	41.7	7	58.3	4	33.3	3	25.0
外部委託型	68	33	48.5	27	39.7	32	47.1	13	19.1
その他	7	3	42.9	0	0.0	3	42.9	1	14.3
無回答	4	1	25.0	0	0.0	1	25.0	0	0.0
計	171	79	46.2	72	42.1	79	46.2	39	22.8

Q66. 情報セキュリティ推進体制 / Q37. システム監査の実施方式	各部門・拠点にセキュリティ担当者を設置		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	
内部監査部門型	50	48.1	8	7.7	6	5.8	1	1.0
部門監査型	5	38.5	0	0.0	0	0.0	0	0.0
指名方式	3	60.0	0	0.0	0	0.0	0	0.0
委員会方式	2	33.3	1	16.7	0	0.0	0	0.0
チームアプローチ	7	58.3	2	16.7	0	0.0	0	0.0
外部委託型	27	39.7	13	19.1	7	10.3	2	2.9
その他	3	42.9	0	0.0	2	28.6	0	0.0
無回答	0	0.0	0	0.0	1	25.0	0	0.0
計	71	41.5	16	9.4	13	7.6	2	1.2

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。複数回答を許容しているため、実際的な監査推進組織の形態は推定の域を出ないが、情報システム担当役員（CIO）が中心となった委員会組織（事務局は情報システム担当部に設置）が監査担当部門として被監査部門を監査する形が多くなっていると考えられる。また、監査人は、監査部や検査部等の事業体内部の監査専門チームや外部の専門家チームが監査にあたる傾向がみられる。特に金融庁を監督官庁に持つ金融機関においてはこの形態をとる事業体が多く、そのことが前回調査と比較し、情報セキュリティ担当役員や情報セキュリティ委員会の設置と内部監査部門型や外部委託型とのクロス集計のポイントが高くなった理由と考えられる。情報セキュリティの推進体制としては、２年前に比べ向上がみられるといえる。

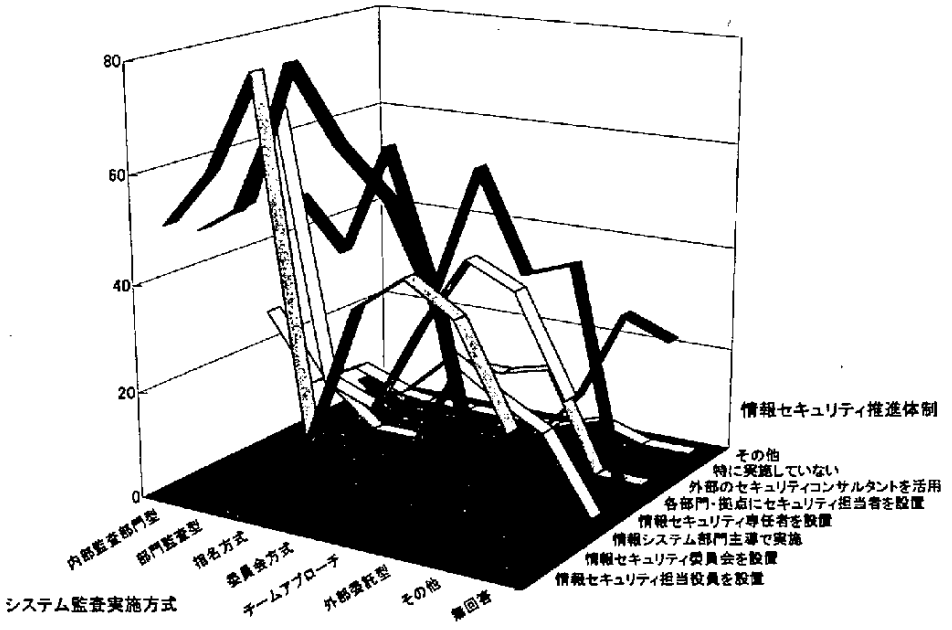

図3－3－3．システム監査実施体制 × 情報セキュリティ推進体制 平成16年度調査（監査担当部門）

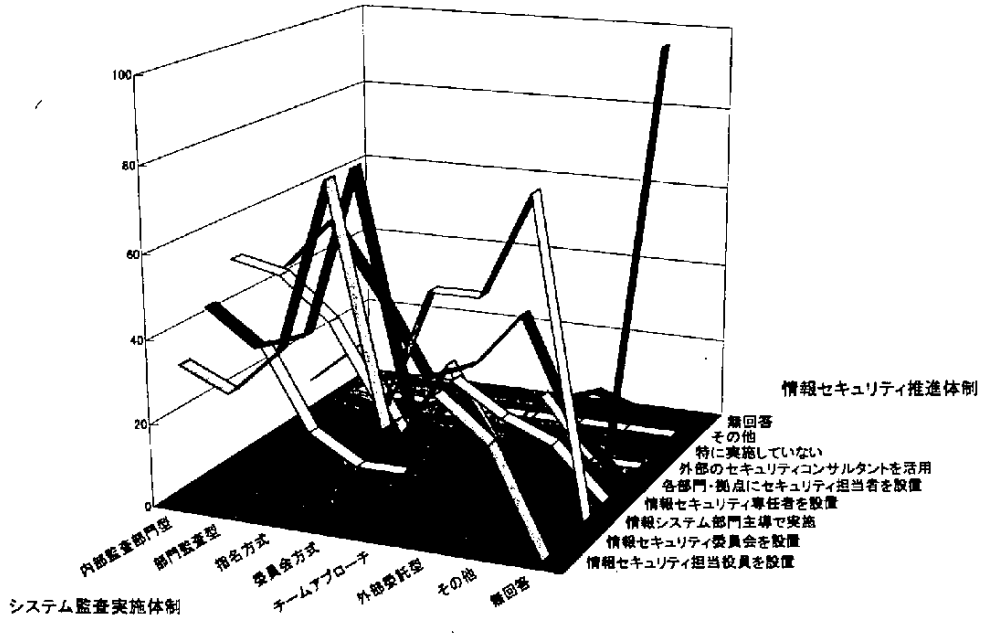

図3－3－4．システム監査実施体制 × 情報セキュリティ推進体制 平成14年度調査（監査担当部門）

3．『Q57. 監査報告会への出席者』（有効回答件数：113件）のクロス集計

×Q67. 情報セキュリティ推進体制で最な重要なこと

Q67. 情報セキュリティ推進体制 / Q57. 監査報告会への出席者	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	
最高経営者	49	13	26.5	26	53.1	0	0.0
財務担当役員	18	3	16.7	12	66.7	0	0.0
情報システム担当役員	53	15	28.3	27	50.9	1	1.9
監査役	43	9	20.9	23	53.5	1	2.3
情報システム部門の管理者	75	22	29.3	42	56.0	3	4.0
内部監査人	66	24	36.4	28	42.4	1	1.5
ユーザ部門の管理者	41	12	29.3	20	48.8	1	2.4
外部のシステム監査人	11	3	27.3	6	54.5	0	0.0
その他	6	2	33.3	1	16.7	0	0.0
無回答	1	0	0.0	1	100.0	0	0.0
計	113	34	30.1	55	48.7	3	2.7

Q67. 情報セキュリティ推進体制 / Q57. 監査報告会への出席者	利用部門の理解・協力		その他		無回答		複数回答	
最高経営者	5	10.2	1	2.0	3	6.1	1	2.0
財務担当役員	2	11.1	0	0.0	1	5.6	0	0.0
情報システム担当役員	6	11.3	0	0.0	3	5.7	1	1.9
監査役	7	16.3	0	0.0	2	4.7	1	2.3
情報システム部門の管理者	6	8.0	0	0.0	2	2.7	0	0.0
内部監査人	6	9.1	0	0.0	6	9.1	1	1.5
ユーザ部門の管理者	6	14.6	0	0.0	2	4.9	0	0.0
外部のシステム監査人	1	9.1	0	0.0	1	9.1	0	0.0
その他	2	33.3	0	0.0	0	0.0	1	16.7
無回答	0	0.0	0	0.0	0	0.0	0	0.0
計	12	10.6	1	0.9	6	5.3	2	1.8

ここでは、監査担当部門が理想とする監査推進体制と現実の監査推進状況のギャップを分析した。情報セキュリティの推進体制としては、経営者のトップダウンによる体制が本来は望ましい。最高経営者または 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。

今回調査では、『情報セキュリティ推進体制で最な重要なこと』として「全社的な推進体制」を挙げている監査担当部門が最も多い。しかし、今回調査で特徴的なことは、『経営者のリーダーシップ』を挙げている監査担当部門が大幅に増えたことにある（今回調査 30.1%←前回調査 18.4%、11.7ポイント増）。監査担当部門において、情報セキュリティの推進におけるトップマネジメントの重要性の認識が高くなってきていることがわかる。これに対し、実際の監査報告の出席者として最高経営者または CIO が出席しているケースが前回調査と比べ、若干しか増加していないのは残念である。監査結果は、必ず最高経営者または情報システム担当役員にフィードバックされ、トップダウンで解決を行う必要がある。監査担当部門は、これら経営陣に対し啓蒙活動を継続的に行う必要がある。

4．『Q65. 情報セキュリティポリシー策定状況』（有効回答件数：421件）のクロス集計

×Q22. システム監査の実施状況

Q65. 情報セキュリティポリシーの策定状況 ＼ Q22. システム監査の実施状況	回答件数	ある		ない	
定めている	255	146	57.3	109	42.7
現在作成中である	53	17	32.1	36	67.9
作成を検討している	69	19	27.5	50	72.5
現在、定める予定がない	34	7	20.6	27	79.4
無回答	10	6	60.0	4	40.0
計	421	195	46.3	226	53.7

平成17年4月からの個人情報保護法の施行や多発する個人情報の流出事件などの影響もあり、情報セキュリティポリシーを策定した事業体は前回調査と比較して圧倒的に多くなっている（今回調査60.6%←前回調査43.7%、16.9ポイント増）。特にセキュリティポリシーを全く定める予定のない事業体は回答数が84件から34件に激減しており、セキュリティポリシーが定着してきたといえる。しかし、残念なことにシステム監査の実施状況については、未実施の事業体が非常に多いことがわかる。セキュリティポリシーを策定した事業体のうち、システム監査を実施した事業体は58.5%から57.3%に減少している。セキュリティポリシーが事業体の中で本当に遵守されているかを確認する手段の一つとして監査がある。特に最近はシステム監査よりも情報セキュリティ監査が重要視される傾向にあるが、経営的視点から監査を行うことも重要であり、是非システム監査も実施してほしい。

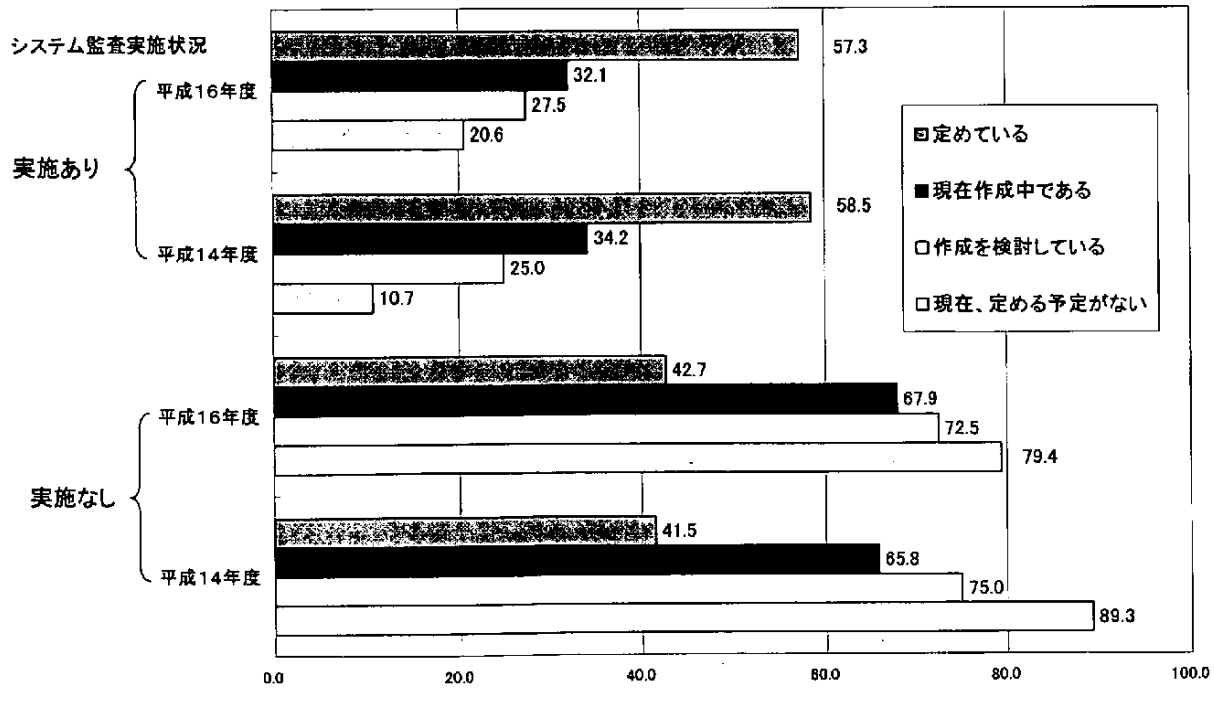

図3－3－5. 情報セキュリティポリシー策定状況 × システム監査の実施状況（監査担当部門）

×Q66. 情報セキュリティ監査の実施状況

Q70.情報セキュリティ監査の実施状況 / Q65.情報セキュリティポリシーの策定状況	回答件数	ある		これから実施する予定がある		ない		無回答	
定めている	255	107	42.0	45	17.6	101	39.6	2	0.8
現在作成中である	53	6	11.3	10	18.9	35	66.0	2	3.8
作成を検討している	69	5	7.2	4	5.8	58	84.1	2	2.9
現在、定める予定がない	34	1	2.9	2	5.9	28	82.4	3	8.8
無回答	10	2	20.0	0	0.0	2	20.0	6	60.0
計	421	121	28.7	61	14.5	224	53.2	15	3.6

このクロス分析では、情報セキュリティポリシーを策定した事業体が、情報セキュリティ監査を実施することにより情報セキュリティポリシーに実効性を持たせているかを検証している。今回は、前回調査と異なり、セキュリティポリシーを策定した事業体の約３分の２（実施予定を含む59.6%）がセキュリティ監査を実施している。前回は情報セキュリティポリシー監査の実施状況についての調査であったが、２年前にはポリシー策定済みの事業体のうち、約25%(注)しか監査を実施していなかったことを考えると大きな変化といえる。現在セキュリティポリシーを策定中または検討中の事業体では、情報セキュリティ監査の予定がないケースが多く、ポリシー策定後はぜひ監査を実施されたい。

（注）前回調査では、情報セキュリティポリシー監査の実施について、「実施予定」の選択肢を設けていない。

×Q72. ＩＳＭＳ適合性評価制度の認知度

Q72. ISMS適合性評価制度の認知度 / Q65.情報セキュリティポリシーの策定状況	回答件数	認定を取得している		知っている		知らない		無回答	
定めている	255	35	13.7	150	58.8	68	26.7	2	0.8
現在作成中である	53	0	0.0	33	62.3	18	34.0	2	3.8
作成を検討している	69	1	1.4	34	49.3	32	46.4	2	2.9
現在、定める予定がない	34	0	0.0	7	20.6	24	70.6	3	8.8
無回答	10	3	30.0	0	0.0	1	10.0	6	60.0
計	421	39	9.3	224	53.2	143	34.0	15	3.6

このクロス分析では、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。ISMS適合性評価制度の認知度が高まり、情報サービス業を中心に認証を取得しており、一部金融機関でも認証を取得するケースが出始めている。現在、736事業所（2005年３月末）が認証を受けており、制度そのものが定着してきている。そのため、今回のクロス集計では、セキュリティポリシーを策定済み、または作成中の事業体については前回

調査よりも回答総数が少ないにもかかわらず、ISMS 適合性評価制度を知っている（取得済みも含む）との回答が 218 件もあった（前回調査：144 件）。

また、逆にポリシーを策定済み、または作成中の事業体で制度を知らないと回答したものが、2 年前は 136 件もあったが、今回調査では 86 件と大幅に減っている。地方自治体や独立行政法人などでは、ISMS 認証取得済の事業体であることを入札条件としている例もあり、今後さらに認知度は高まると思われる。

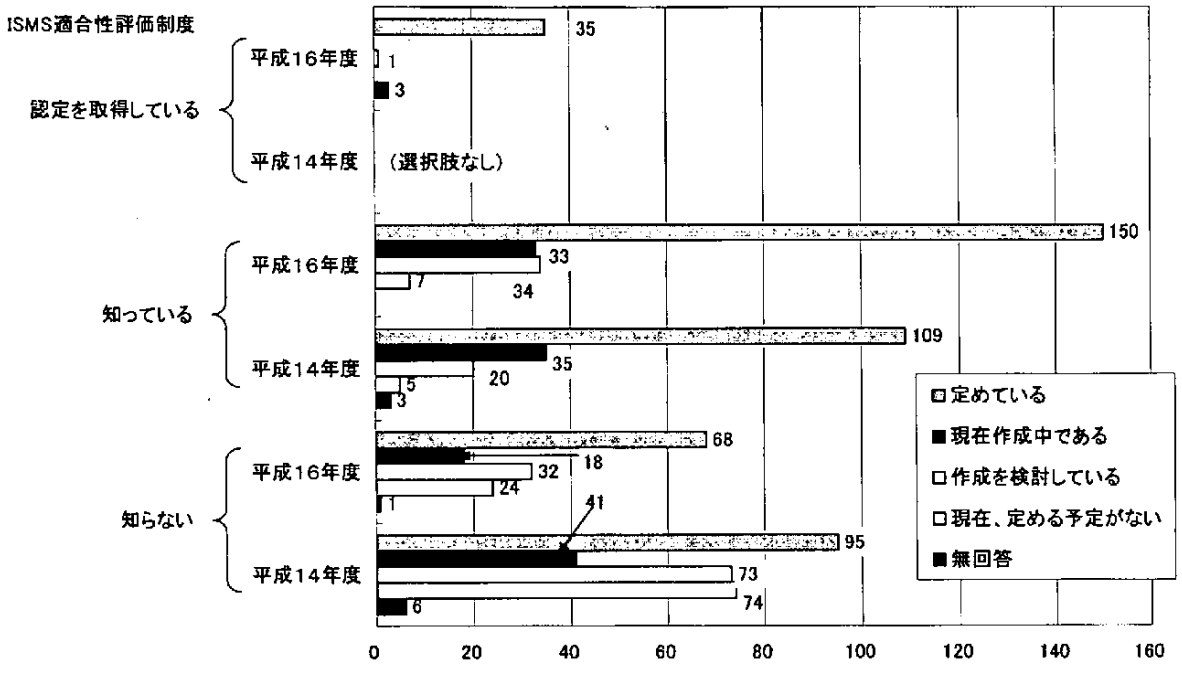

図3－3－6. 情報セキュリティポリシー策定状況 × ISMS認知状況（監査担当部門）

5．『Q67. 情報セキュリティ推進体制』（有効回答件数：421 件）のクロス集計

×Q62. システム監査を実施していない理由（有効回答件数：226 件）

Q62. システム監査未実施の理由 / Q67. 重視する情報セキュリティ推進体制	回答件数	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		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		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		システム監査を実施する担当者（部門）の確保が難しい		システム監査の方法、制度、手続きなどが十分でない	
経営者のリーダーシップ	39	2	5.1	12	30.8	4	10.3	11	28.2	4	10.3
全社的な推進体制	114	4	3.5	22	19.3	20	17.5	22	19.3	19	16.7
情報システム部門の推進体制	10	0	0.0	1	10.0	1	10.0	4	40.0	2	20.0
利用部門の理解・協力	50	1	2.0	7	14.0	8	16.0	11	22.0	12	24.0
その他	2	0	0.0	0	0.0	0	0.0	2	100.0	0	0.0
無回答	9	0	0.0	0	0.0	1	11.1	0	0.0	0	0.0
複数回答	2	0	0.0	0	0.0	1	50.0	0	0.0	0	0.0
計	226	7	3.1	42	18.6	35	15.5	50	22.1	37	16.4

Q62. システム監査未実施の理由 / Q67. 重視する情報セキュリティ推進体制	システム監査の効果が明確でない		システム監査の必要性を感じない		アウトソーシングしているため		その他		無回答		複数回答	
経営者のリーダーシップ	1	2.6	2	5.1	0	0.0	2	5.1	0	0.0	1	2.6
全社的な推進体制	5	4.4	5	4.4	5	4.4	11	9.6	0	0.0	1	0.9
情報システム部門の推進体制	0	0.0	1	10.0	0	0.0	0	0.0	0	0.0	1	10.0
利用部門の理解・協力	1	2.0	4	8.0	1	2.0	2	4.0	1	2.0	2	4.0
その他	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
無回答	0	0.0	3	33.3	0	0.0	0	0.0	5	55.6	0	0.0
複数回答	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	1	50.0
計	7	3.1	15	6.6	6	2.7	15	6.6	6	2.7	6	2.7

このクロス分析では、システム監査が行われていない原因とセキュリティ推進体制について考察した。前回調査では、システム監査が行われない理由として、システム化推進を優先していると回答した監査部門が最も多かったが、今回調査では、社内コンセンサスや監査人の調達など監査ができない理由を分析した回答が多くなっている（全体の 40%）。今回のクロス調査では、監査部門としては、情報セキュリティを推進する上で重要なのは全社的な推進体制であると考えているが、現実にはシステム監査を実施するためのコンセンサスや社内風土が醸成されておらず、システム監査人の確保も十分にできず、悩んでいる様子が伺える。情報セキュリティの推進やシステム監査の実施には、経営者のリーダーシップにより全社的な推進体制を構築し、実施していかなければならない。そのためには、被監査部門を含めた全社的な教育啓蒙活動や監査人の育成、または監査法人・公認会計士などに対するアウトソーシングの依頼など、『手間』と『費用』がかかる問題であり、経営者として情報システムをどのように捉えているかにより、対応が変わってくる。情報システムは、今日の経営になくてはならない経営資源であり、多くの経営者が情報システムの統制を大きな経営

課題の一つと捉え、積極的に取り組むことを期待したい。また、監査部門が情報システムのプロフェッショナルとして、これら経営者に啓蒙を行う役割を担うことも期待したい。

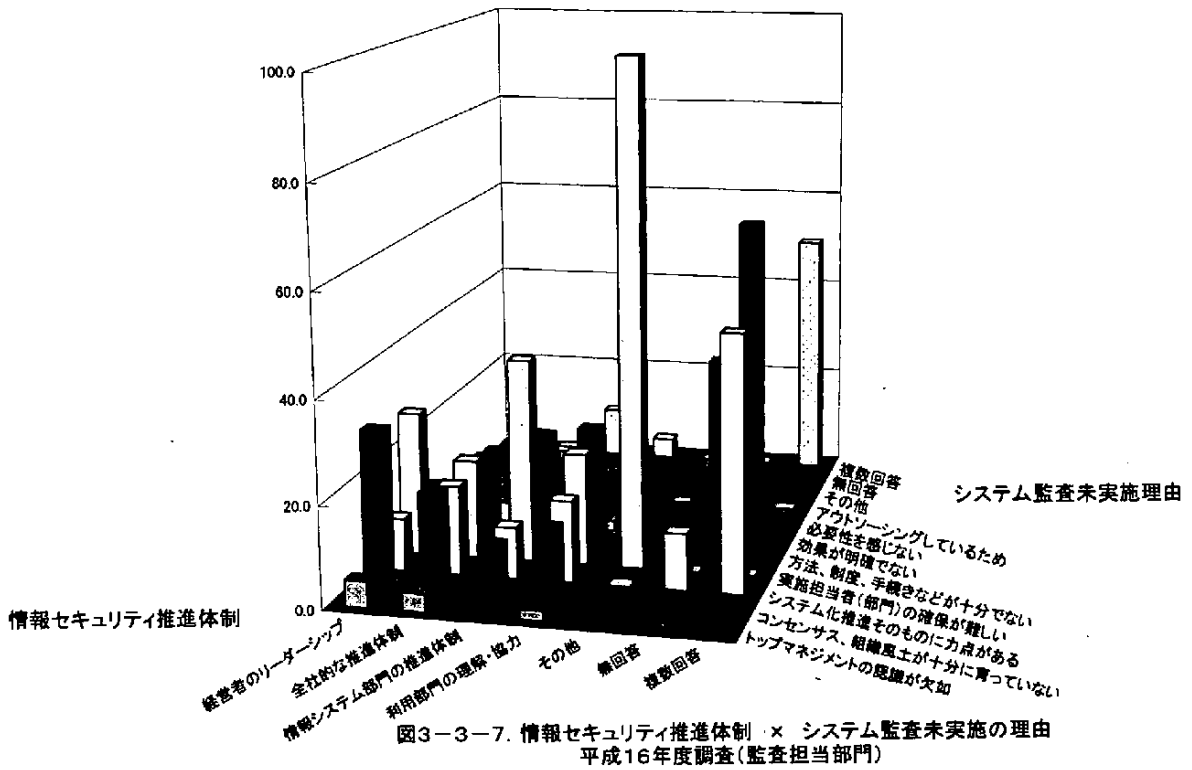

図3－3－7. 情報セキュリティ推進体制 × システム監査未実施の理由
平成16年度調査(監査担当部門)

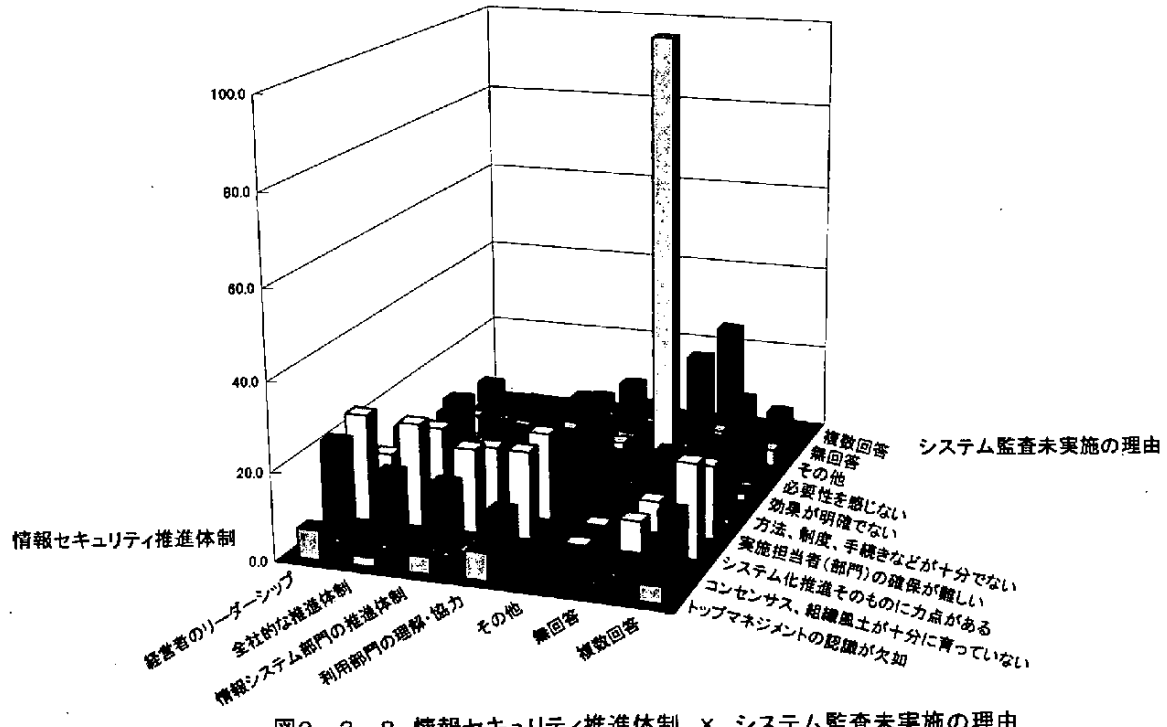

図3－3－8. 情報セキュリティ推進体制 × システム監査未実施の理由
平成14年度調査(監査担当部門)

6．『Q68. 優先的に行っている情報セキュリティ対策』（有効回答件数：421 件）のクロス集計

×Q47. 情報システムの信頼性を高めるための投資の必要性（有効回答件数：171 件）

Q47. 信頼性を高めるための投資の必要性 / Q68.優先的に実施している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	24	17	70.8	1	4.2	6	25.0	0	0.0
リスク分析の実施	59	37	62.7	10	16.9	12	20.3	0	0.0
システム監査の実施	44	24	54.5	11	25.0	8	18.2	1	2.3
情報セキュリティ監査の実施	46	32	69.6	4	8.7	10	21.7	0	0.0
情報セキュリティ教育の実施	82	57	69.5	8	9.8	17	20.7	0	0.0
情報セキュリティ体制の確立	84	54	64.3	11	13.1	19	22.6	0	0.0
情報セキュリティアドミニストレータの確保	2	2	100.0	0	0.0	0	0.0	0	0.0
情報資産の洗い出し	54	31	57.4	9	16.7	14	25.9	0	0.0
ISMSの取得	16	10	62.5	3	18.8	3	18.8	0	0.0
プライバシーマークの取得	27	16	59.3	7	25.9	3	11.1	1	3.7
その他	3	0	0.0	0	0.0	3	100.0	0	0.0
特に実施していない	1	0	0.0	1	100.0	0	0.0	0	0.0
無回答	66	43	65.2	12	18.2	10	15.2	1	1.5
複数回答	6	6	100.0	0	0.0	0	0.0	0	0.0
計	171	109	63.7	26	15.2	35	20.5	1	0.6

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前回調査同様『情報セキュリティ体制の確立』を選択した事業体が多かったが、今回最も多く回答が寄せられたのが、『情報セキュリティ教育の実施』であった（前回第３位、今回は第１位）。情報セキュリティ対策として教育が重要視されるようになってきたのは大きな変化であり、本来のあるべき姿に近づいていると考えてよい。

また、情報セキュリティを推進する上で必要な『リスク分析の実施』、『情報セキュリティ監査の実施』、『情報資産の洗い出し』などを選択する事業体が多く、次に『システム監査の実施』となっている。『システム監査の実施』については、前回調査では第２位であったが、今回調査では第６位と大きく後退した。

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。

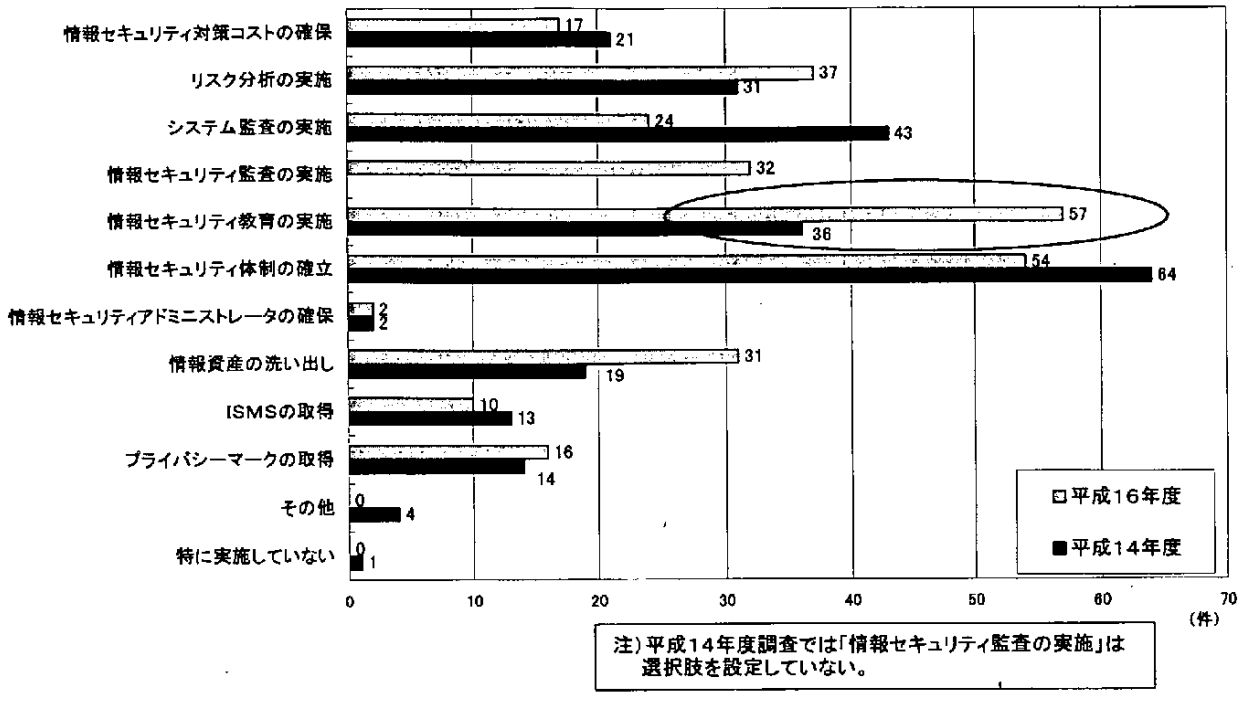

図3－3－9. 情報セキュリティ対策 × 信頼性を高めるための投資の必要性あり
(監査担当部門)

×Q50. 情報システムの安全性を高めるための投資の必要性

Q50. 安全性を高めるための投資の必要性 / Q68.優先的に実施している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	24	16	66.7	2	8.3	6	25.0	0	0.0
リスク分析の実施	59	37	62.7	11	18.6	11	18.6	0	0.0
システム監査の実施	44	29	65.9	8	18.2	6	13.6	1	2.3
情報セキュリティ監査の実施	46	33	71.7	7	15.2	6	13.0	0	0.0
情報セキュリティ教育の実施	82	59	72.0	9	11.0	14	17.1	0	0.0
情報セキュリティ体制の確立	84	57	67.9	11	13.1	16	19.0	0	0.0
情報セキュリティアドミニストレータの確保	2	2	100.0	0	0.0	0	0.0	0	0.0
情報資産の洗い出し	54	35	64.8	6	11.1	13	24.1	0	0.0
ISMSの取得	16	13	81.3	3	18.8	0	0.0	0	0.0
プライバシーマークの取得	27	19	70.4	5	18.5	2	7.4	1	3.7
その他	3	2	66.7	0	0.0	1	33.3	0	0.0
特に実施していない	1	0	0.0	1	100.0	0	0.0	0	0.0
無回答	67	48	71.6	9	13.4	9	13.4	1	1.5
複数回答	6	6	100.0	0	0.0	0	0.0	0	0.0
計	171	118	69.0	24	14.0	28	16.4	1	0.6

情報システムの安全性に対する投資についても前述の信頼性と同様、必要と考える監査担当部門では『情報セキュリティ教育の実施』および『情報セキュリティ体制の確立』の回答が多かった。次に多いのが、リスク分析、情報資産の洗い出し、情報セキュリティ監査、システム監査であった。

投資が必要と思わない監査担当部門でも、若干順位は異なるがほぼ同様の傾向がみられる。

一方、安全性に対する投資に必要性を感じない監査担当部門においても、情報セキュリティ対策としては同一の認識に立脚しており、広く共通認識となっている。

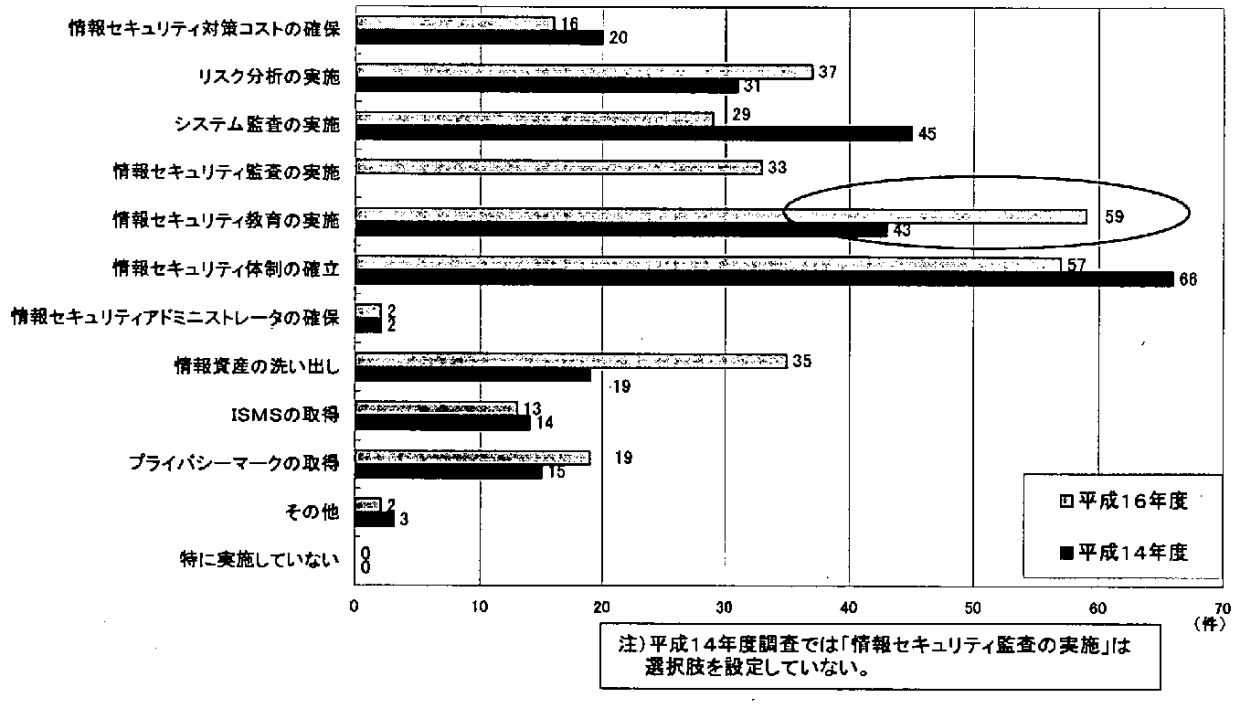

図3－3－10. 情報セキュリティ対策 × 安全性を高めるための投資の必要性あり（監査担当部門）

×Q53. 情報システムの効率性を高めるための投資の必要性

Q53. 効率性を高めるための投資の必要性 / Q68.優先的に実施している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	24	15	62.5	3	12.5	6	25.0	0	0.0
リスク分析の実施	59	36	61.0	13	22.0	10	16.9	0	0.0
システム監査の実施	44	25	56.8	12	27.3	6	13.6	1	2.3
情報セキュリティ監査の実施	46	27	58.7	9	19.6	10	21.7	0	0.0
情報セキュリティ教育の実施	82	52	63.4	15	18.3	15	18.3	0	0.0
情報セキュリティ体制の確立	84	47	56.0	17	20.2	20	23.8	0	0.0
情報セキュリティアドミニストレータの確保	2	2	100.0	0	0.0	0	0.0	0	0.0
情報資産の洗い出し	54	28	51.9	9	16.7	17	31.5	0	0.0
ISMSの取得	16	12	75.0	3	18.8	1	6.3	0	0.0
プライバシーマークの取得	27	18	66.7	6	22.2	2	7.4	1	3.7
その他	3	0	0.0	0	0.0	3	100.0	0	0.0
特に実施していない	1	0	0.0	1	100.0	0	0.0	0	0.0
無回答	67	37	55.2	14	20.9	12	17.9	4	6.0
複数回答	6	6	100.0	0	0.0	0	0.0	0	0.0
計	171	101	59.1	34	19.9	34	19.9	2	1.2

信頼性・安全性・効率性の３つの投資に対する考え方と情報セキュリティ対策を考察してきたが、効率性においてもほぼ同様の結論となっている。

情報セキュリティ対策として教育が最も優先的に実施されているという傾向は、投資の必要性の有無を超えて共通認識となっている。内部からの個人情報の流失や不用意な利用によるコンピュータウイルス感染などにより、情報システムおよび情報資産に対する脅威が散見されるようになり、場合によっては企業経営に大きな影響を及ぼすケースも珍しい話ではなくなった。そのため、投資に対する考え方の立場の違いがあろうとも、情報セキュリティ対策の重要性、特に情報セキュリティ教育の重要性が広く認識されるようになってきた。２年前の調査と比べ、情報セキュリティの考え方が進歩したといえる。

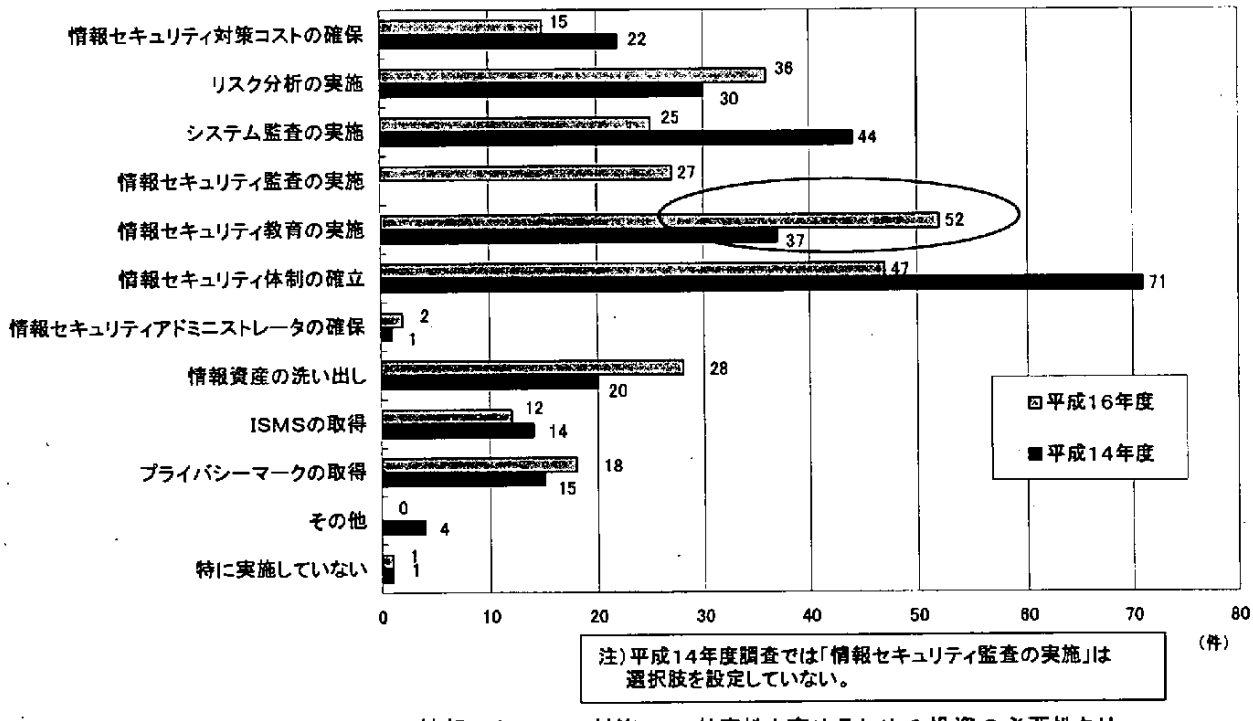

図3－3－11. 情報セキュリティ対策　×　効率性を高めるための投資の必要性あり
（監査担当部門）

7．『Q75.現在の個人情報の管理状況に対するリスク認識』(有効回答件数：421件) のクロス集計

×Q76-①　現在行っている個人情報保護対策

Q76-①現在実施している個人情報保護対策 / Q75.個人情報の管理状況に対するリスク認識度	回答件数	プライバシーポリシーを策定している		管理責任者を置いている(保護体制(役割、責任、権限)を確立する)		個人情報保護に関する規程を定め運用している		個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している		社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している		定期的に監査を実施している	
対応策を講じているので、リスクはないと認識している	35	23	65.7	27	77.1	26	74.3	16	45.7	25	71.4	19	54.3
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	45	10	22.2	16	35.6	14	31.1	6	13.3	11	24.4	8	17.8
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	140	58	41.4	78	55.7	72	51.4	30	21.4	54	38.6	39	27.9
いつ問題が発生してもおかしくない状況であると認識している	120	31	25.8	36	30.0	33	27.5	6	5.0	17	14.2	16	13.3
その他	39	15	38.5	19	48.7	19	48.7	8	20.5	14	35.9	10	25.6
特に認識していない	24	0	0.0	0	0.0	1	4.2	0	0.0	0	0.0	0	0.0
無回答	18	1	5.6	3	16.7	2	11.1	0	0.0	2	11.1	1	5.6
計	421	138	32.8	179	42.5	167	39.7	66	15.7	123	29.2	93	22.1

Q76-①現在実施している個人情報保護対策 / Q75.個人情報の管理状況に対するリスク認識度	リスク分析を実施して必要な安全対策を構築している		苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している		仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている		その他		特に対策を講じない	
対応策を講じているので、リスクはないと認識している	22	62.9	27	77.1	23	65.7	0	0.0	0	0.0
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	10	22.2	12	26.7	11	24.4	0	0.0	18	0.0
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	47	33.6	75	53.6	58	41.4	1	0.7	24	0.7
いつ問題が発生してもおかしくない状況であると認識している	20	16.7	29	24.2	24	20.0	4	3.3	50	3.3
その他	12	30.8	18	46.2	13	33.3	1	2.6	11	2.6
特に認識していない	2	8.3	2	8.3	0	0.0	0	0.0	20	0.0
無回答	0	0.0	3	16.7	3	16.7	0	0.0	1	0.0
計	113	26.8	166	39.4	132	31.4	6	1.4	124	29.5

当クロス集計では、当該監査担当部門が所属する事業体での個人情報保護対策と実際の個人情報のリスク認識について分析する。当クロス集計からわかることは、どのように個人情報保護対策を行っていようとも常にリスクは存在するということである。『ヒヤリ・ハッと』の経験者が 140 事業体もあり、また 120 事業体が『いつ問題が発生してもおかしくない』と回答している。特にプライバシーマークの認定を受けている事業体においてもリスク認識を持っているとの回答が 36 事業体もあり、プライバシーマーク認定企業でリスクがないと回答している事業体（22 事業体）と比べても、約 1.5 倍となっている。したがって、個人情報保護対策としてどのような対策を採ろうとも、万全ということはなく、継続的に対応を行っていく必要があることを当クロス集計は物語っている。なお、個人情報保護に対し、『対策を講じていない』と回答した 124 事業体について、半数以上の 74 事業体がリスク認識を持ちながら対応できていない現状がある。監査担当部門として問題意識はあるが、経営者の無関心や経営環境の悪化などのために組織としての動きとならないというジレンマが感じられる。監査担当部門として全社的な啓蒙活動を継続されることを期待したい。

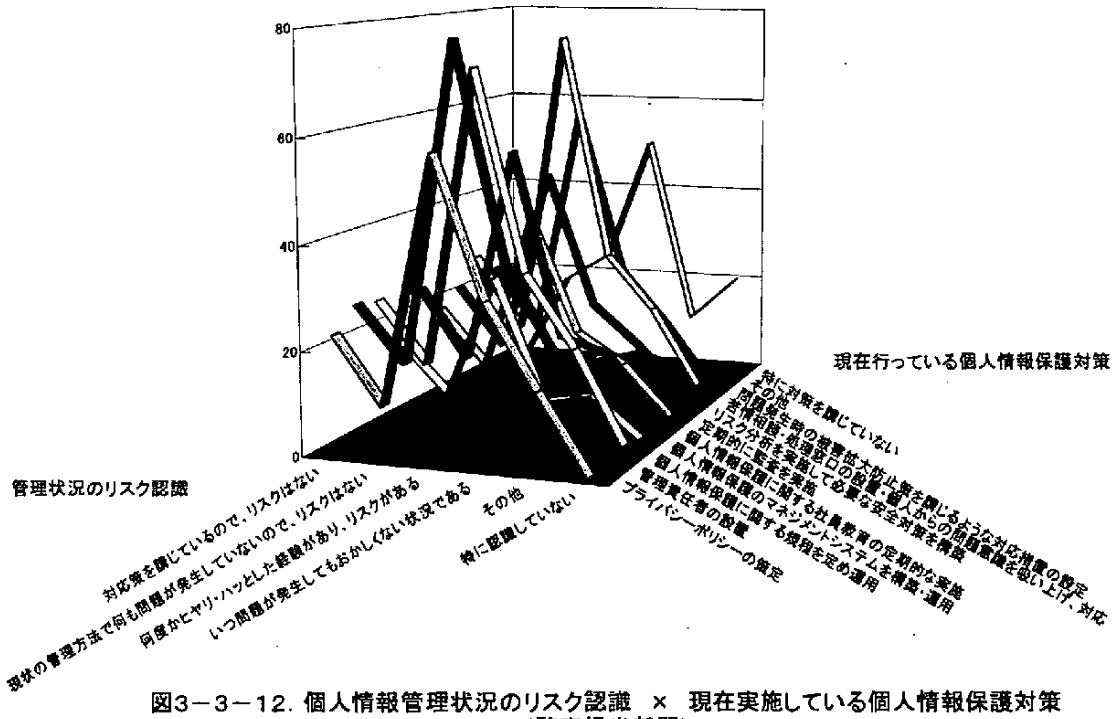

図3－3－12. 個人情報管理状況のリスク認識 × 現在実施している個人情報保護対策
（監査担当部門）

×Q76-②今後実施を予定している対策

Q76-②実施を予定している個人情報保護対策 / Q75.個人情報の管理状況に対するリスク認識度	回答件数	プライバシーポリシーを策定している		管理責任者を置いている(保護体制(役割、責任、権限)を確立する)		個人情報保護に関する規程を定め運用している		個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している		社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している		定期的に監査を実施している	
対応策を講じているので、リスクはないと認識している	35	10	28.6	12	34.3	12	34.3	12	34.3	10	28.6	12	34.3
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	45	22	48.9	20	44.4	28	62.2	14	31.1	26	57.8	18	40.0
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	140	100	71.4	82	58.6	100	71.4	100	71.4	112	80.0	118	84.3
いつ問題が発生してもおかしくない状況であると認識している	120	86	71.7	86	71.7	114	95.0	66	55.0	106	88.3	100	83.3
その他	39	26	66.7	32	82.1	32	82.1	12	30.8	26	66.7	28	71.8
特に認識していない	24	18	75.0	18	75.0	20	83.3	10	41.7	14	58.3	12	50.0
無回答	18	4	22.2	2	11.1	6	33.3	2	11.1	4	22.2	0	0.0
計	421	266	63.2	252	59.9	312	74.1	216	51.3	298	70.8	288	68.4

Q76-②実施を予定している個人情報保護対策 / Q75.個人情報の管理状況に対するリスク認識度	リスク分析を実施して必要な安全対策を構築している		苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している		仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている		その他		特に対策を講じない	
対応策を講じているので、リスクはないと認識している	16	45.7	4	11.4	8	22.9	0	0.0	0	0.0
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	24	53.3	18	40.0	16	35.6	2	4.4	4	4.4
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	112	80.0	72	51.4	94	67.1	6	4.3	2	4.3
いつ問題が発生してもおかしくない状況であると認識している	94	78.3	70	58.3	88	73.3	8	6.7	10	6.7
その他	30	76.9	22	56.4	24	61.5	2	5.1	0	5.1
特に認識していない	12	50.0	12	50.0	10	41.7	2	8.3	16	8.3
無回答	4	22.2	0	0.0	0	0.0	0	0.0	0	0.0
計	292	69.4	198	47.0	240	57.0	20	4.8	32	7.6

当クロス集計では回答事業体が、『実施を予定している個人情報保護対策』と『リスク認識度』との相関関係を分析している。リスク認識度の高い監査担当部門（『何度かヒヤリ・ハッとした経験があり、リスクがあると認識している』、『いつ問題が発生してもおかしくない状況であると認識している』と回答した事業体）、リスク認識度の低い監査担当部門（『対応策を講じているので、リスクはないと認識している』、『現状の管理方法で何も問題が発生していないので、リスクはないと認識している』と回答した事業体）共に実施予定の対策として、個人情報保護規程の策定、定期監査、リスク分析を挙げている。定期教育についてリスク認識の高い監査担当部門の方が若干重要視している傾向がみられるが、大きな差異となっていない。前述の実際に個人情報保護対策を行っている事業体でのクロス分析と同様、リスク認識度の差異による「実施を予定している個人情報保護対策」に大きな違いはみられなかった。

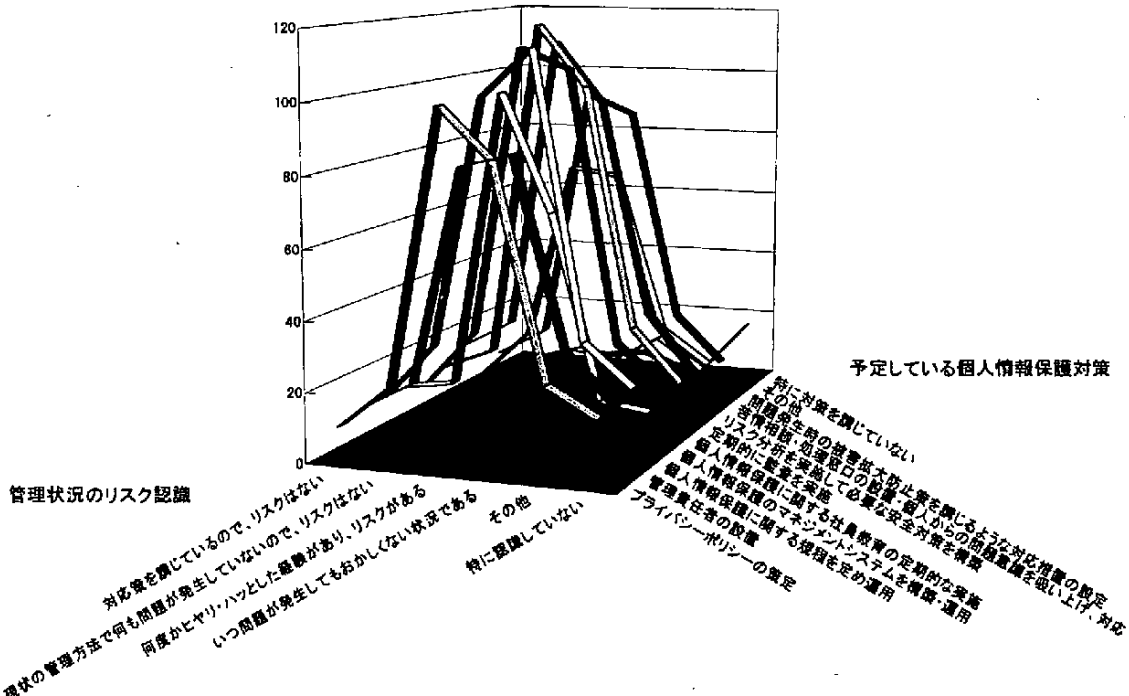

図3－3－13. 個人情報管理状況のリスク認識 × 今後予定している個人情報保護対策
（監査担当部門）

3.3.3 被監査部門対象

1.『Q21. システム監査実施方式』(有効回答件数：203件) のクロス集計

×Q44. 最も効果的と思われるシステム監査実施者

Q44. 効果的なシステム監査実施者 / Q23.システム監査の実施方法	回答件数	監査役(団体等は監事、自治体は監査委員)		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	
内部監査部門型(監査部、検査部等が実施)	106	2	1.9	35	33.0	5	4.7	6	5.7
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)	149	2	1.3	22	14.8	3	2.0	7	4.7
計	203	4	2.0	44	21.7	6	3.0	10	4.9

Q44. 効果的なシステム監査実施者 / Q23.システム監査の実施方法	監査法人・公認会計士		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(監査部、検査部等が実施)	32	30.2	23	21.7	1	0.9	2	0.0
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)	59	39.6	50	33.6	3	2.0	3	0.0
計	72	35.5	59	29.1	4	2.0	4	0.0

被監査部門が理想とする監査人と実際行われた監査との差異について考察した。『内部監査部門型』では、「組織内部の監査人（監査役、内部の監査人、情報システム部門要員)」を挙げた事業体が42事業体、「外部の監査人（監査法人、システム監査企業)」を挙げた事業体が55事業体と、若干外部の監査人が上回っている。これに対し、『外部委託型』では、「組織内部の監査人」は27事業体となっているが、外部の監査人は109事業体と圧倒的な差となっている。これは、監査を行う上で必要となるスキルが育たず、外部に委託した方が効果的な監査が行われると感じているからであろう。外部委託の場合は、監査のプロが行うため、内部監査型に比べ一般的には効率的でレベルの高い監査結果が得られる。しかし、外部委託をしてしまうと監査的な視点が事業体内部で育成されず、問題点の把握や改善が後手に回るケースが発生する。いわゆるトレードオフの関係となっており、事業体としての監査方針を検討する際に、内部型と外部委託型のどちらを選択するか、十分な考慮が必要となる。

2．『Q33. 監査報告書の指摘事項・改善勧告内容の妥当性』（有効回答件数：203 件）のクロス集計

×Q27. システム監査人の問題点（有効回答件数：17 件）

Q27. システム監査人の問題点 / Q33. 監査報告書の指摘事項・改善勧告の妥当性	回答件数	監査人の権限および役割分担が不明確であった		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		監査人の監査対象業務に関する知識が不足していた		監査人の情報システムに関する知識が不足していた	
妥当だと思う	5	1	20.0	1	20.0	1	20.0	0	0.0
一部妥当だと思う	10	2	20.0	1	10.0	2	20.0	3	30.0
妥当だと思わない	2	0	0.0	0	0.0	1	50.0	1	50.0
無回答	0	0	0.0	0	0.0	0	0.0	0	0.0
計	17	3	17.6	2	11.8	4	23.5	4	23.5

Q27. システム監査人の問題点 / Q33. 監査報告書の指摘事項・改善勧告の妥当性	監査人の洞察力・判断力に問題があった		その他	
妥当だと思う	1	20.0	1	20.0
一部妥当だと思う	1	10.0	1	10.0
妥当だと思わない	0	0.0	0	0.0
無回答	0	0.0	0	0.0
計	2	11.8	2	11.8

当クロス集計では、監査結果の妥当性と監査人に対する問題点の相関関係を分析している。回答数が少ないため、十分な論拠とはならないが、傾向だけを述べておく。全体的に不満が多いのは、監査人の業務および情報システムの知識不足である。監査人を選ぶ際は、業務に詳しい監査人や情報システムに詳しい監査人など、監査人の特性を生かした選択が必要である。

×Q28. システム監査を受けた時の現場の負担

Q28. システム監査時の現場の負担 / Q33. 監査報告書の指摘事項・改善勧告の妥当性	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	
妥当だと思う	134	13	9.7	111	82.8	9	6.7	1	0.7
一部妥当だと思う	58	1	1.7	50	86.2	6	10.3	1	1.7
妥当だと思わない	3	1	33.3	0	0.0	2	66.7	0	0.0
無回答	8	3	37.5	4	50.0	0	0.0	1	12.5
計	203	18	8.9	165	81.3	17	8.4	3	1.5

ここでは、被監査部門が監査を受ける際の負担と監査後の指摘事項／改善勧告内容の妥当性の相関関係を分析する。回答事業体のほとんどが、「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」と考えており、監査日程の調整などを綿密に行ったうえで監査を実施している様子が伺える。また、「通常業務に支障をきたした」と回答した被監査部門においても、監査報告書の内容の妥当性をほぼ受け入れており、監査担当部門が受ける負担の差により監査後の指摘事項／改善勧告内容の妥当性が影響を受けることはないことがわかる。監査報告書の内容に疑義が持たれる要因は別の問題であるが、それは次のクロス分析で述べることとする。

×Q29. システム監査実施上の問題点

Q29. システム監査実施上の問題点 / Q33. 監査報告書の指摘事項・改善勧告の妥当性	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であった		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	134	0	0.0	0	0.0	22	16.4	6	4.5	14	10.4	5	3.7
一部妥当だと思う	58	1	1.7	0	0.0	7	12.1	6	10.3	5	8.6	7	12.1
妥当だと思わない	3	0	0.0	1	33.3	1	33.3	0	0.0	0	0.0	1	33.3
無回答	8	0	0.0	0	0.0	2	25.0	0	0.0	0	0.0	0	0.0
計	203	1	0.5	1	0.5	32	15.8	12	5.9	19	9.4	13	6.4

Q29. システム監査実施上の問題点 / Q33. 監査報告書の指摘事項・改善勧告の妥当性	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	4	3.0	2	1.5	2	1.5	72	53.7	3	2.2	4	3.0
一部妥当だと思う	4	6.9	1	1.7	2	3.4	21	36.2	1	1.7	3	5.2
妥当だと思わない	0	0.0	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	5	62.5	1	12.5	0	0.0
計	8	3.9	3	1.5	4	2.0	98	48.3	5	2.5	7	3.4

ここでは、システム監査実施上の問題点と監査後の指摘事項／改善勧告内容の妥当性の相関関係を分析する。このクロス集計からは、回答事業体においてはシステム監査がうまく行われていることがわかる。「特に問題は感じなかった」と回答している事業体が最も多く、「システム監査計画に無理があった」または「システム監査方法が現場を無視したものであった」など、システム監査そのものに問題ありとした回答は皆無に等しい状況となっている。そのため、被監査部門も監査報告書の内容を受け入れている傾向がみられる。したがって、結論としては、この集計でも特に相関関係はみられなかった、ということである。監査を行う上で問題となるのは、監査資料を分析し、被

監査部門に的確にヒアリングできるシステム監査人の能力の問題である。システム監査人の能力によって監査結果が異なり、被監査部門が監査報告書に疑問を呈したり、監査を行ったはずの項目でトラブルが発生するなどの状況が発生する。いかに適した監査人を調達できるかが、監査をうまく行うポイントである。

×Q30. システム監査人と被監査部門による講評会の実施

Q30. 講評会の実施の有無 / Q33. 監査報告書の指摘事項・改善勧告の妥当性	回答件数	行われた		行われなかった		無回答	
妥当だと思う	134	121	90.3	13	9.7	0	0.0
一部妥当だと思う	58	46	79.3	11	19.0	1	1.7
妥当だと思わない	3	2	66.7	1	33.3	0	0.0
無回答	8	2	25.0	2	25.0	4	50.0
計	203	171	84.2	27	13.3	5	2.5

当クロス集計では、システム監査後の講評会の実施状況と監査報告書の妥当性について分析を行う。システム監査では、監査終了後、監査担当部門と被監査部門とがクロージングミーティングを行い、指摘事項や改善勧告の内容を確認し、被監査部門が了承した上で監査報告書を作成する形態が望ましい。また、講評会も経営者、監査担当部門、被監査部門が出席し、行われるべきである。講評会が「行われた」と回答した被監査部門が84.2%にも上っている。講評会が行われなかった事業体の内、1事業体の被監査部門だけが監査報告書を妥当と思っておらず、24の被監査部門は監査報告書の妥当性を受け入れている。このことから、講評会が開催されていない事業体でも、監査担当部門と被監査部門が、指摘事項や改善勧告の内容を相互に確認できる何らかの機能を有していると考えられる。監査報告書の内容に被監査部門が同意できなければ、その後の改善活動が行われない可能性がある。講評会が開かれることが望ましいが、事情があり開催できない場合は、講評会に変わる機能を必ず有する必要がある。

3．『Q43. システム監査で充実すべき点』（有効回答件数：507件）のクロス集計

×Q27. システム監査人の問題点（有効回答件数：17件）

Q27. システム監査人の問題点 / Q43. システム監査で充実すべき点	回答件数	監査人の権限および役割分担が不明確であった		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		監査人の監査対象業務に関する知識が不足していた		監査人の情報システムに関する知識が不足していた	
監査計画	4	1	25.0	1	25.0	2	50.0	0	0.0
事前調査	1	0	0.0	0	0.0	1	100.0	0	0.0
実地調査	1	0	0.0	0	0.0	0	0.0	1	100.0
改善勧告内容	8	2	25.0	1	12.5	0	0.0	1	12.5
監査報告会	2	0	0.0	0	0.0	0	0.0	1	50.0
チェックリスト	3	0	0.0	0	0.0	1	33.3	1	33.3
その他	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
計	17	3	17.6	2	11.8	4	23.5	4	23.5

Q27. システム監査人の問題点 / Q43. システム監査で充実すべき点	監査人の洞察力・判断力に問題があった		その他	
監査計画	0	0.0	0	0.0
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	2	25.0
監査報告会	1	50.0	0	0.0
チェックリスト	1	33.3	0	0.0
その他	0	0.0	0	0.0
無回答	0	0.0	0	0.0
計	2	11.8	2	11.8

ここでは、被監査部門が監査人の問題としている項目とシステム監査で充実すべき点を分析した。当クロス集計も抽出できた件数が少ないため正しい分析ができないが、傾向として参照していただきたい。前述までの集計でも述べたが、被監査部門としては、対象業務および対象システムに関する知識不足が問題と感じているケースが多い。監査人の知識不足が原因で、事前調査、実地調査、チェックリスト、監査報告書などで充実すべきとの意見が出るのであろう。監査人を選ぶ際には、業務知識やシステム知識を保有し、監査に望む必要がある。また、事業体内部で要員の調達ができない場合は、外部の専門家へ依頼することも検討されたい。監査が不十分なために、トラブルが発生した場合のリカバリ費用は、外部の専門家への依頼費用の数倍となることを鑑みると、充実したシステム監査を行うことをお勧めしたい。

×Q31. 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

Q31. 監査報告会の実施状況 / Q43. システム監査で充実すべき点	回答件数	行われた		行われなかった		無回答	
監査計画	45	29	64.4	13	28.9	3	6.7
事前調査	23	19	82.6	4	17.4	0	0.0
実地調査	47	33	70.2	12	25.5	2	4.3
改善勧告内容	37	23	62.2	13	35.1	1	2.7
監査報告会	14	5	35.7	9	64.3	0	0.0
チェックリスト	32	22	68.8	9	28.1	1	3.1
その他	1	1	100.0	0	0.0	0	0.0
無回答	4	2	50.0	2	50.0	0	0.0
計	203	134	66.0	62	30.5	7	3.4

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。監査報告会の開催の有無によりシステム監査の充実すべき点で差異がでたのは『事前調査』であった（各回答計より「実施 14.2%（19/134 件）」、「未実施 6.5%（4/62 件）」）。監査報告会が実施された場合、『事前調査』で抽出された問題点と『実地調査』で抽出された問題点が、被監査部門で明確にわかり、被監査部門では、実地調査を行わなくても『事前調査』で判明する項目も多いと考えているために、『事前調査』の充実を求める声が大きくなっているのではないだろうか。今回調査でも、被監査部門の監査に対する負担を調査したが、「業務に影響は及ぼさなかったが、負担であった」と回答している被監査部門があり、『事前調査』の充実により解消できるケースもあるのではないだろうか。監査担当部門、被監査部門の両方の負担軽減のためにも『事前調査』の内容を見直すことも重要であろう。

×Q32. 監査報告会への情報システム部門からの出席状況（有効回答件数：134 件）

Q32. 監査報告会への出席状況 / Q43. システム監査で充実すべき点	回答件数	した		しない		無回答	
監査計画	29	24	82.8	5	17.2	0	0.0
事前調査	19	16	84.2	3	15.8	0	0.0
実地調査	33	31	93.9	1	3.0	1	3.0
改善勧告内容	23	19	82.6	4	17.4	0	0.0
監査報告会	5	4	80.0	1	20.0	0	0.0
チェックリスト	22	19	86.4	2	9.1	1	4.5
その他	1	0	0.0	1	100.0	0	0.0
無回答	2	1	50.0	0	0.0	1	50.0
計	134	114	85.1	17	12.7	3	2.2

このクロス集計では、監査報告会が開催された事業体での被監査部門の出席状況と監査の充実について取り上げている。ここで注目したいのは、出席の有無によって『実地調査』の項に差異が出てきている点である（「出席時 27.2%（31/114 件）」、「未出席時 5.9%（1/17 件）」）。これは『実地調査』に不満がなかったために監査報告会に出席しなかった可能性もある。出席した被監査部門が監査で充実すべき点のトップ項目として『実地調査』を上げていることと、未出席の被監査部門（1事業体のみ）の回答にあまりにも差異がありすぎるため、監査内容の充実度そのものに差異があり、出席状況が変化したと考えられる。

4.『Q39. 情報セキュリティポリシー策定状況』（有効回答件数：507 件）のクロス集計

Q19. システム監査の実施状況

Q19. システム監査の実施状況 / Q45.情報セキュリティの策定状況	回答件数	ある		これから実施する予定がある		ない		無回答	
定めている	269	153	56.9	13	4.8	103	38.3	0	0.0
現在作成中である	87	33	37.9	7	8.0	46	52.9	1	1.1
作成を検討している	98	30	30.6	2	2.0	66	67.3	0	0.0
現在、定める予定がない	47	6	12.8	0	0.0	41	87.2	0	0.0
無回答	6	3	50.0	0	0.0	2	33.3	1	16.7
計	507	225	44.4	22	4.3	258	50.9	2	0.4

情報セキュリティポリシーの策定状況とシステム監査の実施状況について考察したい。残念ながら、情報セキュリティポリシーを作成している事業体でもシステム監査を実施しない事業体が約4割もある。情報セキュリティの状況を判断するには情報セキュリティ監査が必須であり、システム監査そのものを絶対に行う必要はないが、是非システム監査を実施することをお勧めしたい。

×Q50. 情報セキュリティ監査の実施状況

Q50. 情報セキュリティ監査の実施状況 / Q45. 情報セキュリティポリシーの策定状況	回答件数	ある		これから実施する予定がある		ない		無回答	
定めている	269	81	30.1	36	13.4	140	52.0	12	4.5
現在作成中である	87	4	4.6	15	17.2	67	77.0	1	1.1
作成を検討している	98	3	3.1	1	1.0	87	88.8	7	7.1
現在、定める予定がない	47	2	4.3	0	0.0	43	91.5	2	4.3
無回答	6	1	16.7	0	0.0	4	66.7	1	16.7
計	507	91	17.9	52	10.3	341	67.3	23	4.5

情報セキュリティポリシーを策定している事業体のうち、52.0%が情報セキュリティ監査を行っていない現状がある。情報セキュリティポリシーを作成しても、それが遵守されているかどうかを判断する手段がなく、おそらく形だけを作成した事業体が多いのではないだろうか。また、情報セキュリティ監査を行いたいが方法がわからない事業体も多い。情報セキュリティ監査・管理基準やISMS策定のためのガイドラインなど、参考となる情報が経済産業省やJIPDEC等のホームページで公開されており、十分に有効活用できる内容となっている。情報セキュリティポリシーを定める予定のない事業体でも、是非一度、情報セキュリティ監査を行うことを推奨する。

Q52. ＩＳＭＳ適合性評価制度の認知度

Q52. ISMS適合性評価制度の認知度 / Q45. 情報セキュリティポリシーの策定状況	回答件数	認定を取得している		知っている		知らない		無回答	
定めている	269	37	13.8	191	71.0	28	10.4	13	4.8
現在作成中である	87	1	1.1	69	79.3	16	18.4	1	1.1
作成を検討している	98	1	1.0	59	60.2	29	29.6	9	9.2
現在、定める予定がない	47	0	0.0	15	31.9	30	63.8	2	4.3
無回答	6	0	0.0	5	83.3	0	0.0	1	16.7
計	507	39	7.7	339	66.9	103	20.3	26	5.1

ここでは、ISMS適合性評価制度の認知度と情報セキュリティポリシーの策定状況を分析する。ISMS適合性評価制度がおかれている状況もかなり変化してきている。監査担当部門の分析（Q65×Q72）でも述べたように、官公庁や民間企業において、アウトソーシング先を選択する場合に、ISMS認定が前提条件となる場合も珍しくなくなってきている。このような状況の中で、情報セキュリティポリシーをすでに策定している事業体の被監査部門では、認定取得済を含めて84.8%が『知っている』と回答している。一方、情報セキュリティポリシーに関心のない事業体では、『知らない』が63.8%に及んでいるが、全体としては、制度そのものが幅広く知られるようになってきた。今後は、各事業体ともに内容の充実を図るとともに、確実に定着するように期待したい。

5.『Q46. 情報セキュリティ体制の推進』(有効回答件数：507件) のクロス集計

×Q23. システム監査の実施方式 (有効回答件数：203件)

Q23. システム監査の実施方式 / Q46. 情報セキュリティの実施体制	回答件数	内部監査部門型(監査部、検査部等が実施)		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	
情報セキュリティ担当役員を設置している	111	58	52.3	53	47.7
情報セキュリティ委員会を設置している	116	58	50.0	58	50.0
情報システム部門主導で実施している	130	48	36.9	82	63.1
情報セキュリティ専任者を設置している	68	38	55.9	30	44.1
各部門・拠点にセキュリティ担当者を設置している	114	59	51.8	55	48.2
外部のセキュリティコンサルタントを活用している	29	15	51.7	14	48.3
特に実施していない	9	0	0.0	9	100.0
その他	3	1	33.3	2	66.7
無回答	3	1	33.3	2	66.7
計	203	106	52.2	149	73.4

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。「内部監査部門型」が情報セキュリティ担当役員や委員会の設置が主流なのに対し、「外部委託型」が情報システム部門主導としている事業体が多いことが特徴的である。外部委託型において、経営者の関与がどのように行われているのか気になるところである。内部監査型、外部委託型のどちらを選択するかは、事業体の考え方や費用、要員育成など幅広く考えていく必要があり、どちらが適しているかは一概にはいえないものである。しかしながら、監査結果に対する経営者の関与は必須であり、被監査部門としても必ず経営者を巻き込んだ体制を構築する必要がある。被監査部門が努力をしても、経営資源(ヒト・モノ・カネ)が不足していれば、改善効果に自ずと限界が出てくる。経営者の関与が低い被監査部門では、経営者への啓蒙活動を考慮されたい。

6．『Q55. 個人情報の管理状況』のクロス集計

×Q56-①現在行っている個人情報保護対策

Q56-①現在行っている個人情報保護対策 / Q55. 個人情報の管理状況	回答件数	プライバシーポリシーを策定している		管理責任者を置いている(保護体制(役割、責任、権限)を確立する)		個人情報保護に関する規程を定め運用している		個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している		社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している	
対応策を講じているので、リスクはないと認識している	43	26	60.5	34	79.1	34	79.1	21	48.8	29	67.4
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	62	8	12.9	18	29.0	13	21.0	4	6.5	9	14.5
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	138	50	36.2	69	50.0	60	43.5	23	16.7	39	28.3
いつ問題が発生してもおかしくない状況であると認識している	155	36	23.2	49	31.6	33	21.3	6	3.9	19	12.3
その他	52	16	30.8	29	55.8	23	44.2	7	13.5	19	36.5
特に認識していない	30	0	0.0	2	6.7	1	3.3	0	0.0	1	3.3
無回答	27	2	7.4	2	7.4	1	3.7	0	0.0	2	7.4
計	507	138	27.2	203	40.0	165	32.5	61	12.0	118	23.3

Q56-①現在行っている個人情報保護対策 / Q55. 個人情報の管理状況	定期的に監査を実施している		リスク分析を実施して必要な安全対策を構築している		苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している		仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている		その他		特に対策を講じない	
対応策を講じているので、リスクはないと認識している	23	53.5	29	67.4	31	72.1	29	67.4	1	2.3	3	2.3
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	9	14.5	11	17.7	12	19.4	10	16.1	2	3.2	28	3.2
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	36	26.1	36	26.1	52	37.7	36	26.1	1	0.7	40	0.7
いつ問題が発生してもおかしくない状況であると認識している	19	12.3	19	12.3	39	25.2	23	14.8	1	0.6	62	0.6
その他	12	23.1	15	28.8	16	30.8	17	32.7	2	3.8	12	3.8
特に認識していない	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	22	0.0
無回答	0	0.0	1	3.7	1	3.7	2	7.4	0	0.0	1	0.0
計	99	19.5	111	21.9	151	29.8	117	23.1	7	1.4	168	33.1

ここでは、現状の個人情報保護対策と個人情報の管理状況を分析している。多くの事業体が『何度かヒヤリ・ハッとした経験があり、リスクがあると認識している』および『いつ問題が発生してもおかしくない状況』と回答している。プライバシーマークを取得している事業体でも約47.5%（29/61件）がこの2項目に回答している。やはり完璧な対策はなく、改善を常に継続して行う必要がある。

なお、個人情報保護に対し『対策を講じていない』と回答した168事業体について、約6割の102事業体がリスク認識を持ちながら対応できていない現状がある。監査担当部門での分析（Q75×Q75-①）でも述べたように、被監査部門として管理状況に対する問題意識はありながらも、経営者の無関心や経営環境の悪化などのために組織としての動きとならないというジレンマが感じられる。

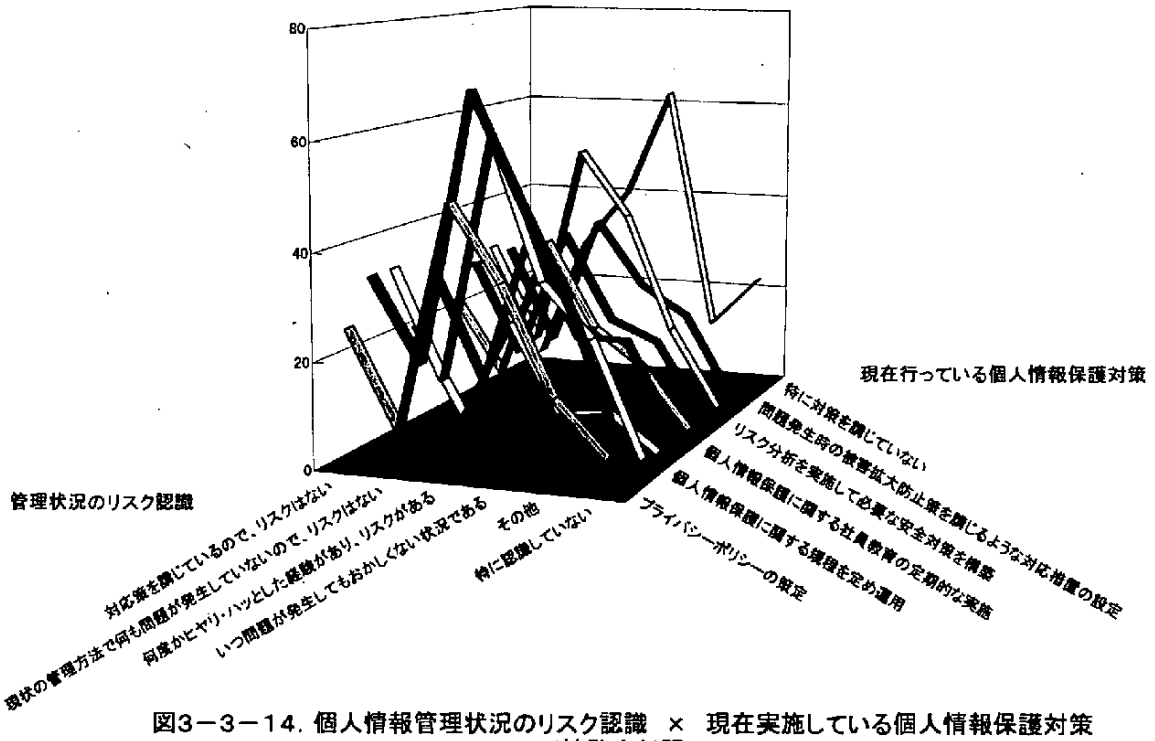

図3－3－14. 個人情報管理状況のリスク認識 × 現在実施している個人情報保護対策
（被監査部門）

Q56-②今後実施を予定している対策

Q56-②今後実施を予定している個人情報保護対策 / Q55. 現在の個人情報の管理状況	回答件数	プライバシーポリシーを策定している		管理責任者を置いている(保護体制(役割、責任、権限)を確立する)		個人情報保護に関する規程を定め運用している		個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している		社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している	
対応策を講じているので、リスクはないと認識している	43	8	18.6	6	14.0	7	16.3	9	20.9	10	23.3
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	62	21	33.9	15	24.2	24	38.7	13	21.0	23	37.1
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	138	60	43.5	49	35.5	66	47.8	35	25.4	66	47.8
いつ問題が発生してもおかしくない状況であると認識している	155	63	40.6	60	38.7	79	51.0	48	31.0	71	45.8
その他	52	20	38.5	14	26.9	20	38.5	10	19.2	22	42.3
特に認識していない	30	6	20.0	3	10.0	9	30.0	2	6.7	7	23.3
無回答	27	0	0.0	0	0.0	2	7.4	1	3.7	0	0.0
計	507	178	35.1	147	29.0	207	40.8	118	23.3	199	39.3

Q56-②今後実施を予定している個人情報保護対策 / Q55. 現在の個人情報の管理状況	定期的に監査を実施している		リスク分析を実施して必要な安全対策を構築している		苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している		仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている		その他		特に対策を講じない	
対応策を講じているので、リスクはないと認識している	9	20.9	6	14.0	4	9.3	6	14.0	1	2.3	0	2.3
現状の管理方法で何も問題が発生していないので、リスクはないと認識している	12	19.4	21	33.9	10	16.1	14	22.6	0	0.0	5	0.0
何度かヒヤリ・ハッとした経験があり、リスクがあると認識している	48	34.8	62	44.9	37	26.8	51	37.0	2	1.4	0	1.4
いつ問題が発生してもおかしくない状況であると認識している	53	34.2	62	40.0	51	32.9	62	40.0	3	1.9	7	1.9
その他	17	32.7	20	38.5	16	30.8	18	34.6	2	3.8	0	3.8
特に認識していない	3	10.0	2	6.7	2	6.7	3	10.0	1	3.3	11	3.3
無回答	1	3.7	0	0.0	0	0.0	0	0.0	0	0.0	1	0.0
計	143	28.2	173	34.1	120	23.7	154	30.4	9	1.8	24	4.7

今後予定している個人情報保護対策と現在の個人情報の管理状況について分析する。問題ありとした被監査組織（『何度かヒヤリ・ハッとした経験があり、リスクがあると認識している』または『いつ問題が発生してもおかしくない状況であると認識している』と回答した被監査部門）の今後の対策を分析すると、個人情報保護規程の策定、社員教育、リスク分析、ポリシー策定を回答している事業体が多い。特に意識に変化がみられるのは、社員教育の実施やリスク分析など個人情報保護対策では非常に重要な対策でありながら、今までおざなりにされてきた項目を今後の対策予定としている点である。個人情報保護が個人情報保護規程の策定やプライバシーポリシーの策定のような、形の策定から本質の対策へと変化している状況がみられる。

特に個人情報保護法の平成17年4月からの施行に伴い、各種のセミナーや対策本などの出版により、具体的な対策を考える上での情報が格段に得やすくなった。また、事業体の経営者も一定の費用負担を行うようになってきた。昨今の個人情報の流失による事業体の損失は公共団体、民間企業を問わず、大きなものになるという認識も共通のものとなってきている。今後もさらに本質的な対策への転換が図られるものと期待したい。

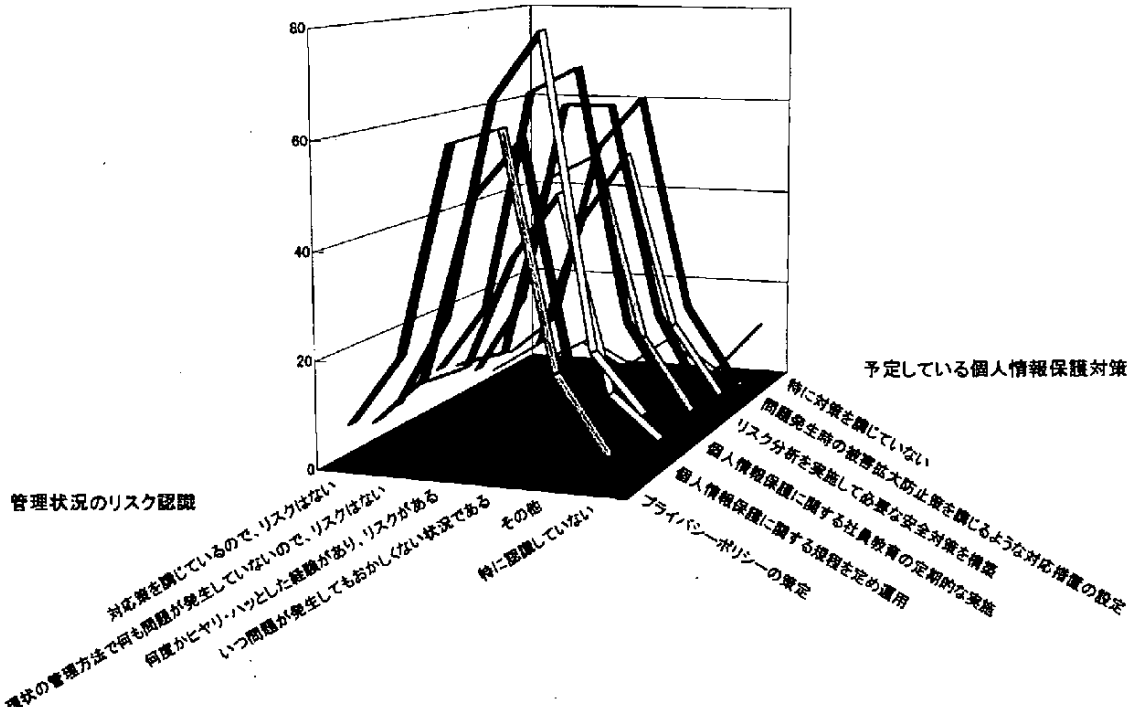

図3－3－15. 個人情報管理状況のリスク認識 × 今後予定している個人情報保護対策
（被監査部門）

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

2005-2006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16年12月17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　プライバシーマーク推進本部　情報セキュリティ対策課
（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：03-3432-3166

Ⅰ システム監査一般について

Q1. 経済産業省の「システム監査基準」(平成8年改訂)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. 「システム監査基準」が平成16年10月に改訂されたことを知っていますか。

23

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

Q3. 経済産業省から「システム管理基準」(平成16年10月)が策定・公表されていることを知っていますか。

24

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

Q4. 経済産業省の「システム監査企業台帳」(平成3年)を知っていますか。

25

1	知っている
2	知らない

→Q6へ

Q5. 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。

26

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

Q6. 経済産業省の「情報セキュリティ監査基準」(平成15年4月策定)を知っていますか。

27

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. 経済産業省の「情報セキュリティ管理基準」(平成15年4月策定)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

Q8. 経済産業省の「情報セキュリティ監査企業台帳」(平成15年)を知っていますか。

29

1	知っている
2	知らない

→Q10へ

Q9. 情報セキュリティ監査を外部の企業に委託する場合、「情報セキュリティ監査企業台帳」を参考にしたいと思いますか。

30	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

Q10. 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。

31	1	知っている
	2	知らない

Q11. 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。

32	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 →Q13へ

Q12. 「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。

33	1	知っている
	2	知らない

Q13. 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。

34	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 →Q15へ

Q14. 「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。

35	1	知っている
	2	知らない

Q15. 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。

36	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 →Q17へ

Q16. 「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。

37	1	知っている
	2	知らない

Q17. 以下のJIS規格を知っていますか。

	規格名	利用している	知っている	知らない
38	JIS X 5080 : 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(平成14年2月制定)	1	2	3
39	JIS Q 2001 : リスクマネジメントシステム構築のための指針(平成13年3月制定)	1	2	3
40	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(平成11年4月制定)	1	2	3

41 B

Ⅱ　貴事業体の監査体制について

Q18. 貴事業体には内部監査部門(監査部、検査部等)が設置されていますか。

42	1	い る
	2	いない

→Q19へ

Q18-1. 内部監査人は何人いますか。

43 [　　人] 45

Q18-2. 内部監査人は平均何歳ですか。(端数切捨て)

46 [　　歳] 47

Q19. 貴事業体にはシステム監査人(システム監査の担当者)がいますか。

48	1	い る
	2	いない

→Q20へ

Q19-1. システム監査人は何人ですか。

49 [　　人] 51

Q19-2. システム監査人は平均何歳ですか。(端数切り捨て)

52 [　　歳] 53

Q19-3. 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)

54 [　　年] 57

Q20. 貴事業体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)

58	1	い る
	2	いない
	3.	把握していない

→Q22へ

Q20-1. 何人の合格者がいますか。

59 [　　人] 61

Q21. 合格者はどこに所属していますか。(複数回答)

62	1	監査担当部門
63	2	情報システム部門
64	3	その他

Q22. 貴事業体ではシステム監査を実施したことがありますか。

65	1	あ る
	2	な い

→Q62へ

Q23. 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。

66	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

67 [C]

Q24. 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。

68		
	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	実施上の問題点はない

Q25. 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。

69		
	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:　　)

Q26. 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。

70		
	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:　　)

Q27. 貴事業体ではシステム監査人は何人位必要だと思いますか。

71 [　][　][　] 人 73

Q28. 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。

74		
	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

75 D

Q29. 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。

76	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

Q30. 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。

77	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

Q31. 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)

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	内部監査部門長の判断に基づいて決定
81	4	システム監査人の独自の判断で決定
82	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
83	6	プライバシーマーク制度の要求事項に基づいて決定
84	7	ISMS制度の要求事項に基づいて決定
85	8	その他(具体的に書いて下さい:　　)

Q32. 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)

86	1	トップマネジメントの要求に基づいて決定
87	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
88	3	内部監査部門の判断で決定
89	4	システム監査人の独自の判断で決定
90	5	各種認定制度等の要求事項に基づいて決定
91	6	その他(具体的に書いて下さい:　　)

Q33. システム監査の基本(年度)計画書を策定していますか。

92	1	い る　→Q35へ
	2	いない

Q34. 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)

93	1	必要性がない
94	2	個別計画書だけで十分である
95	3	内部監査計画に含まれている
96	4	システム監査基本計画書作成のルールがない
97	5	外部に委託しているので作成していない
98	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
99	7	その他(具体的に書いて下さい:　　)

Q35. 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。

100	1	い る
	2	いない

101 E

Ⅲ システム監査の実施について

Q36. 過去2年以内にシステム監査を実施しましたか。

102	1	し た(実施中を含む)
	2	しない →Q65へ

Q37. 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)

103	1	内部監査部門型(監査部、検査部等が実施)
104	2	部門監査型(情報システム部門が実施)
105	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)
106	4	委員会方式(システム監査委員会を設置して実施)
107	5	チームアプローチ(システム監査プロジェクトチームを編成して実施)
108	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) →Q38へ
109	7	その他(具体的に書いて下さい:　　) →Q40へ

(3,4,5 →Q40 へ)

Q38. (Q37 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。

110	1	は い
	2	いいえ
	3	わからない

Q39. 外部委託の場合、どこが実施しましたか。

111	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:　　)

112 F

Q40. 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(1～9)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	有効性	
113	1	企画業務 ➡	1	2	3	4	5	6	7	8	9	117
114	2	開発業務 ➡	1	2	3	4	5	6	7	8	9	118
115	3	運用業務 ➡	1	2	3	4	5	6	7	8	9	119
116	4	保守業務 ➡	1	2	3	4	5	6	7	8	9	120

Q41. 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(1～9)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	有効性	
121	1	ドキュメント管理 ➡	1	2	3	4	5	6	7	8	9	136
122	2	進捗管理 ➡	1	2	3	4	5	6	7	8	9	137
123	3	品質管理 ➡	1	2	3	4	5	6	7	8	9	138
124	4	コスト管理 ➡	1	2	3	4	5	6	7	8	9	139
125	5	要員管理 ➡	1	2	3	4	5	6	7	8	9	140
126	6	外部委託(開発の委託) ➡	1	2	3	4	5	6	7	8	9	141
127	7	外部委託(運用の委託) ➡	1	2	3	4	5	6	7	8	9	142
128	8	セキュリティ対策 ➡	1	2	3	4	5	6	7	8	9	143
129	9	ネットワーク管理 ➡	1	2	3	4	5	6	7	8	9	144
130	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	9	145
131	11	個人情報保護対策 ➡	1	2	3	4	5	6	7	8	9	146
132	12	PC管理、モバイル機器管理 ➡	1	2	3	4	5	6	7	8	9	147
133	13	コンピュータウイルス対策 ➡	1	2	3	4	5	6	7	8	9	148
134	14	情報システム関連のリスク管理 ➡	1	2	3	4	5	6	7	8	9	149
135	15	災害対策 ➡	1	2	3	4	5	6	7	8	9	150

Q42. 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。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(注1)	ソフトウェア(注2)	通信回線	電源設備
151	コンピュータ犯罪防止 ➡	1	2	3	4	5	6	7	8	9	10	11	12
153	ヒューマンエラー防止 ➡	1	2	3	4	5	6	7	8	9	10	11	12
155	事故防止 ➡	1	2	3	4	5	6	7	8	9	10	11	12
157	災害対策 ➡	1	2	3	4	5	6	7	8	9	10	11	12
159	個人情報保護 ➡	1	2	3	4	5	6	7	8	9	10	11	12

注1) CPUと周辺機器／注2) 基本ソフトとアプリケーションソフト

161 G

Q43. システム監査を実施する際に、どのような基準類を利用しましたか。(複数回答)

162	1	システム監査基準
163	2	システム管理基準
164	3	情報セキュリティ監査基準
165	4	情報セキュリティ管理基準
166	5	情報システム安全対策基準
167	6	コンピュータウイルス対策基準
168	7	コンピュータ不正アクセス対策基準
169	8	プライバシーマーク監査ガイドライン
170	9	ISMSガイド
171	10	その他(具体的に名称を書いて下さい:　　)

Q44. 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。

172	1	い る
	2	いない

Q45. 貴事業体の情報システムの信頼性は十分だと思いますか。

173	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

Q46. 貴事業体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。

174	1	思 う
	2	思わない
	3	わからない

Q47. 貴事業体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。

175	1	思 う
	2	思わない
	3	わからない

Q48. 貴事業体の情報システムの安全性は十分だと思いますか。

176	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

Q49. 貴事業体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。

177	1	思 う
	2	思わない
	3	わからない

Q50. 貴事業体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。

178

1	思 う
2	思わない
3	わからない

Q51. 貴事業体の情報システムの効率性は十分だと思いますか。

179

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

Q52. 貴事業体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。

180

1	思 う
2	思わない
3	わからない

Q53. 貴事業体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。

181

1	思 う
2	思わない
3	わからない

Q54. 貴事業体の情報システムは、総合的に見て満足できる状態ですか。

182

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

Q55. 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。

183

1	行った
2	行わなかった

Q56. 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。

184

1	行った
2	行わなかった

Q57. 監査報告会に出席したのは誰ですか。(複数回答)

185	1	最高経営者(会長、社長、知事、市長等)
186	2	財務担当役員
187	3	情報システム担当役員
188	4	監査役
189	5	情報システム部門の管理者
190	6	内部監査人
191	7	ユーザ部門の管理者
192	8	外部のシステム監査人
193	9	その他(具体的に書いて下さい:　　)

Q58. 監査報告書(原本)は誰に提出(報告書の宛先)しましたか。(単一回答)
注)複数部署に配布している場合は、その中での最高権限者に○をつけて下さい。

194	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:　　)

Q59. 監査報告書の写を被監査部門に配布しましたか。

195	1	し た
	2	しない

Q60. 監査報告書の写を監査役に配布しましたか。

196	1	し た
	2	しない

Q61. 監査報告書の写を貴事業体の会計監査人に配布しましたか。

197	1	し た
	2	しない

198 H

Ⅳ 未実施および実施可能性について

(Q62 からQ64 までは、Q22 でシステム監査を実施したことが「ない」と回答した事業体のみお答え下さい。)

Q62. 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。

199	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	アウトソーシングしているため
	9	その他(具体的に書いて下さい:　　)

Q63. 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。

200	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　→Q65へ
	4	将来とも導入の予定はない　→Q65へ
	5	その他(具体的に書いて下さい:　　)

Q64. どのような体制で進められる予定ですか。(複数回答)

201	1	内部監査部門型(監査部、検査部等が実施)
202	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)
203	3	決まっていない

204 I

V 情報セキュリティの推進について

Q65. 貴事業体では情報セキュリティポリシーを策定していますか。

205	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

Q66. 貴事業体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)

206	1	情報セキュリティ担当役員を設置している
207	2	情報セキュリティ委員会を設置している
208	3	情報システム部門主導で実施している
209	4	情報セキュリティ専任者を設置している
210	5	各部門・拠点にセキュリティ担当者を設置している
211	6	外部のセキュリティコンサルタントを活用している
212	7	特に実施していない
213	8	その他(具体的に書いて下さい:　　)

Q67. 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。

214	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:　　)

Q68. 貴事業体で情報セキュリティについて、優先的に実施していることを3つまで選んで下さい。(複数回答)

215	1	情報セキュリティ対策コストの確保
217	2	リスク分析の実施
219	3	システム監査の実施
	4	情報セキュリティ監査の実施
	5	情報セキュリティ教育の実施
	6	情報セキュリティ体制の確立
	7	情報セキュリティアドミニストレータの確保
	8	情報資産の洗い出し
	9	ISMSの取得
	10	プライバシーマークの取得
	11	その他(具体的に書いて下さい:　　)
	12	特に実施していない

Q69. 貴事業体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)

221	1	新入社員教育を実施している
222	2	一般社員向け教育を実施している
223	3	管理職教育を実施している
224	4	役員教育を実施している
225	5	派遣要員向け教育を実施している
226	6	情報セキュリティ担当者の専門教育を実施している
227	7	その他(具体的に書いて下さい:　　)
228	8	特に実施していない

Q70. 貴事業体では情報セキュリティ監査を実施したことがありますか。

229	1	あ る
	2	これから実施する予定がある
	3	な い

Q71. 貴事業体では情報セキュリティ監査を外部に委託したいと思いますか。

230	1	思 う
	2	思わない

Q72. 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。

231	1	認定を取得している
	2	知っている
	3	知らない

232 J

VI　個人情報保護について

Q73.「個人情報の保護に関する法律(平成15年5月30日法律第57号)」を知っていますか。

233	1	内容を知っている
	2	制定されたことを知っている
	3	知らない

Q74. 経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成16年10月公表)を知っていますか。

234	1	内容を知っている
	2	公表されたことを知っている
	3	知らない

Q75. 現在の個人情報の管理状況についてリスクをどのように認識していますか。

235	1	対応策を講じているので、リスクはないと認識している
	2	現状の管理方法で何も問題が発生していないので、リスクはないと認識している
	3	何度かヒヤリ・ハッとした経験があり、リスクがあると認識している
	4	いつ問題が発生してもおかしくない状況であると認識している
	5	その他(　　)
	6	特に認識していない

Q76. 個人情報保護対策として、①現在何を実施していますか。 ②また、今後どういうことを実施する予定ですか。
（複数回答）

対　策	①現在実施している対策	②今後実施を予定している対
プライバシーポリシーを策定している	236 1	247 2
管理責任者を置いている（保護体制（役割、責任、権限）を確立する）	237 1	248 2
個人情報保護に関する規程を定め運用している	238 1	249 2
個人情報保護のマネジメントシステムを構築して（プライバシーマークの認定を受ける）運用している	239 1	250 2
社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している	240 1	251 2
定期的に監査を実施している	241 1	252 2
リスク分析を実施して必要な安全対策を構築している	242 1	253 2
苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している	243 1	254 2
仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている	244 1	255 2
その他（　　）	245 1	256 2
特に対策を講じない	246 1	257 2

Q77. 貴事業体では個人情報保護の監査を外部に委託したいと思いますか。

258	
1	思う
2	思わない

Q78. プライバシーマーク制度を知っていますか。

259	
1	認定を取得している
2	知っている
3	知らない

260 K

ご協力ありがとうございました

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。

被監査部門対象

(財)日本情報処理開発協会

2005-2006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		
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）	千億	百億	十億	億	千万	百万	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。）	十万	万	千	百	十		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16年12月17日までにお願いいたします。

業種	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設定します。

（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。

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　プライバシーマーク推進本部　情報セキュリティ対策課
（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：03-3432-3166

Ⅰ システム監査一般について

Q1. 経済産業省の「システム監査基準」(平成8年改訂)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. 「システム監査基準」が平成16年10月に改訂されたことを知っていますか。

23	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

Q3. 経済産業省から「システム管理基準」(平成16年10月)が策定・公表されていることを知っていますか。

24	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

Q4. 経済産業省の「システム監査企業台帳」(平成3年)を知っていますか。

25	1	知っている
	2	知らない　→Q6へ

Q5. 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。

26	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

Q6. 経済産業省の「情報セキュリティ監査基準」(平成15年4月策定)を知っていますか。

27	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. 経済産業省の「情報セキュリティ管理基準」(平成15年4月策定)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

Q8. 経済産業省の「情報セキュリティ監査企業台帳」(平成15年)を知っていますか。

29	1	知っている
	2	知らない　→Q10へ

Q9. 情報セキュリティ監査を外部の企業に委託する場合、「情報セキュリティ監査企業台帳」を参考にしたいと思いますか。

30	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

Q10. 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。

31	1	知っている
	2	知らない

Q11. 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。

32	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 →Q13へ

Q12. 「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。

33	1	知っている
	2	知らない

Q13. 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。

34	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 →Q15へ

Q14. 「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。

35	1	知っている
	2	知らない

Q15. 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。

36	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 →Q17へ

Q16. 「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。

37	1	知っている
	2	知らない

Q17. 以下のJIS規格を知っていますか。

	規格名	利用している	知っている	知らない
38	JIS X 5080 : 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(平成14年2月制定)	1	2	3
39	JIS Q 2001 : リスクマネジメントシステム構築のための指針(平成13年3月制定)	1	2	3
40	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(平成11年4月制定)	1	2	3

41 B

Ⅱ　システム監査の実施について

Q18. 貴事業体にはシステム監査人(システム監査の担当者)がいますか。

42	1	い る
	2	いない

Q19. 貴部門では、システム監査を受けたことがありますか。

43	1	あ る	
	2	受ける予定がある	→Q40へ
	3	な い	→Q40へ

Q20. 過去2年間にシステム監査を受けましたか。

44	1	受けた(実施中を含む)	
	2	受けない	→Q40へ

Q21. システム監査を受けたのはどの業務でしたか。(複数回答)

45	1	企画業務
46	2	開発業務
47	3	運用業務
48	4	保守業務

Q22. 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)

49	1	ドキュメント管理
50	2	進捗管理
51	3	品質管理
52	4	コスト管理
53	5	要員管理
54	6	外部委託(開発の委託)
55	7	外部委託(運用の委託)
56	8	セキュリティ対策
57	9	ネットワーク管理
58	10	ソフトウェアの適正利用(ライセンス管理)
59	11	個人情報保護対策
60	12	PC管理、モバイル機器管理
61	13	コンピュータウイルス対策
62	14	情報システム関連のリスク管理
63	15	災害対策
64	16	その他(具体的に書いて下さい:　　)

Q23. 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)

65	1	内部監査部門型(監査部、検査部等が実施)
66	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Q26へ、2つとも該当する場合はQ24に進んで下さい。

67 C

Q24.（Q23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の登録企業ですか。

68	1	はい
	2	いいえ
	3	わからない

Q25.（Q23で「2」を回答した場合）外部委託の場合、どこが実施しましたか。

69	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：　　）

Q26. 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）

70	1	問題があった	
	2	十分満足できた	→Q28へ
	3	特に問題はなかった	→Q28へ
	4	わからない	→Q28へ

Q27. どのような点で問題があったと思いますか。最も問題だと思った点を1つ選んで下さい。（単一回答）

71	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：　　）

Q28. システム監査を受けた時、現場の負担はありましたか。

72	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：　　）

Q29. 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。最も問題だと感じた点を1つ選んで下さい。（単一回答）

73	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

Q30. 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。

75

1	行われた
2	行われなかった

Q31. 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。

76

1	行われた	
2	行われなかった	→Q33へ

Q32. 監査報告会に情報システム部門から出席しましたか。

77

1	した
2	しない

Q33. 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。

78

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

Q34. 改善命令を受けましたか。

79

1	受けた	
2	受けない	→Q36へ

Q35. 改善命令を受けて対策を実施しましたか。

80

1	実施した
2	一部実施した
3	実施していない

Q36. 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。

81

1	効果があったと思う	
2	効果はなかったと思う	→Q39へ
3	どちらともいえない	→Q39へ
4	わからない	→Q39へ

Q37. 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点を1つ選んで下さい。(単一回答)

82

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:　　)

Q38. 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点を1つ選んで下さい。**（単一回答）

84	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：　　）

Q39. 貴事業体ではシステム監査の結果をどのように活用していますか。

86	1	自社システムの信頼性・安全性・効率性の改善
	2	取引先に対する自社システムの信頼性・安全性・効率性の説明責任
	3	わからない

87 D

Ⅲ システム監査のあり方について

Q40. 各業務の監査で重視すべき着眼点は何ですか。**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	有効性
88	企画業務 ➡	1	2	3	4	5	6	7	8	9
89	開発業務 ➡	1	2	3	4	5	6	7	8	9
90	運用業務 ➡	1	2	3	4	5	6	7	8	9
91	保守業務 ➡	1	2	3	4	5	6	7	8	9

Q41. 各テーマの監査で重視すべき着眼点は何ですか。**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	有効性
92	ドキュメント管理 ➡	1	2	3	4	5	6	7	8	9
93	進捗管理 ➡	1	2	3	4	5	6	7	8	9
64	品質管理 ➡	1	2	3	4	5	6	7	8	9
95	コスト管理 ➡	1	2	3	4	5	6	7	8	9
96	要員管理 ➡	1	2	3	4	5	6	7	8	9
97	外部委託（開発の委託） ➡	1	2	3	4	5	6	7	8	9
98	外部委託（運用の委託） ➡	1	2	3	4	5	6	7	8	9
99	セキュリティ対策 ➡	1	2	3	4	5	6	7	8	9
100	ネットワーク管理 ➡	1	2	3	4	5	6	7	8	9
101	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	9
102	個人情報保護対策 ➡	1	2	3	4	5	6	7	8	9
103	PC管理、モバイル機器管理 ➡	1	2	3	4	5	6	7	8	9
104	コンピュータウイルス対策 ➡	1	2	3	4	5	6	7	8	9
105	情報システム関連のリスク管理 ➡	1	2	3	4	5	6	7	8	9
106	災害対策 ➡	1	2	3	4	5	6	7	8	9

107 E

Q42. 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。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(注1)	ソフトウエア(注2)	ネットワーク	電源設備
108	コンピュータ犯罪防止 ➡	1	2	3	4	5	6	7	8	9	10	11	12
110	ヒューマンエラー防止 ➡	1	2	3	4	5	6	7	8	9	10	11	12
112	事故防止 ➡	1	2	3	4	5	6	7	8	9	10	11	12
114	災害対策 ➡	1	2	3	4	5	6	7	8	9	10	11	12
116	個人情報保護 ➡	1	2	3	4	5	6	7	8	9	10	11	12

注1)CPUと周辺機器／注)基本ソフトとアプリケーションソフト

Q43. 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点を1つ選んで下さい。

118	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:　　)

Q44. 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。最も効果的だと思われる者を1つ選んで下さい。
(貴事業体の実態とは別にお答えいただいて結構です)

119	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:　　)

120 F

V 情報セキュリティの推進について

Q45. 貴事業体では情報セキュリティポリシーを策定していますか。

121	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

Q46. 貴事業体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)

122	1	情報セキュリティ担当役員を設置している
123	2	情報セキュリティ委員会を設置している
124	3	情報システム部門主導で実施している
125	4	情報セキュリティ専任者を設置している
126	5	各部門・拠点にセキュリティ担当者を設置している
127	6	外部のセキュリティコンサルタントを活用している
128	7	特に実施していない
129	8	その他(具体的に書いて下さい:　　)

Q47. 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。

130	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:　　)

Q48. 貴事業体で情報セキュリティについて、優先的に実施していることを3つまで選んで下さい。(複数回答)

131	1	情報セキュリティ対策コストの確保
133	2	リスク分析の実施
135	3	システム監査の実施
	4	情報セキュリティ監査の実施
	5	情報セキュリティ教育の実施
	6	情報セキュリティ体制の確立
	7	情報セキュリティアドミニストレータの確保
	8	情報資産の洗い出し
	9	ISMSの取得
	10	プライバシーマークの取得
	11	その他(具体的に書いて下さい:　　)
	12	特に実施していない

Q49. 貴事業体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)

137	1	新入社員教育を実施している
138	2	一般社員向け教育を実施している
139	3	管理職教育を実施している
140	4	役員教育を実施している
141	5	派遣要員向け教育を実施している
142	6	情報セキュリティ担当者の専門教育を実施している
143	7	その他(具体的に書いて下さい:　　)
144	8	特に実施していない

Q50. 貴事業体では情報セキュリティ監査を受けたことがありますか。

145	1	あ る
	2	これから受ける予定がある
	3	な い

Q51. 貴事業体では情報セキュリティ監査を外部に委託したいと思いますか。

146	1	思 う
	2	思わない

Q52. 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。

147	1	認定を取得している
	2	知っている
	3	知らない

148 G

Ⅵ　個人情報保護について

Q53.「個人情報の保護に関する法律(平成15年5月30日法律第57号)」を知っていますか。

149	1	内容を知っている
	2	制定されたことを知っている
	3	知らない

Q54. 経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成16年10月公表)を知っていますか。

150	1	内容を知っている
	2	公表されたことを知っている
	3	知らない

Q55. 現在の個人情報の管理状況についてリスクをどのように認識していますか。

151	1	対応策を講じているので、リスクはないと認識している
	2	現状の管理方法で何も問題が発生していないので、リスクはないと認識している
	3	何度かヒヤリ・ハッとした経験があり、リスクがあると認識している
	4	いつ問題が発生してもおかしくない状況であると認識している
	5	その他(　　)
	6	特に認識していない

Q56. 個人情報保護対策として、①現在何を実施していますか。②また、今後どういうことを実施する予定ですか。(複数回答)

対　策	①現在実施している対策		②今後実施を予定している対策	
プライバシーポリシーを策定している	152	1	163	2
管理責任者を置いている(保護体制(役割、責任、権限)を確立する)	153	1	164	2
個人情報保護に関する規程を定め運用している	154	1	165	2
個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している	155	1	166	2
社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している	156	1	167	2
定期的に監査を実施している	157	1	168	2
リスク分析を実施して必要な安全対策を構築している	158	1	169	2
苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している	159	1	170	2
仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている	160	1	171	2
その他(具体的に書いて下さい:　　)	161	1	172	2
特に対策を講じない	162	1	173	2

Q57. 貴事業体では個人情報保護の監査を外部に委託したいと思いますか。

174		
	1	思 う
	2	思わない

Q58. プライバシーマーク制度を知っていますか。

175		
	1	認定を取得している
	2	知っている
	3	知らない

176 H

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１７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
アシスト竹橋ビル　２Ｆ
ＴＥＬ　03(3219)２９７１

16-H003