13－H002

わが国における情報セキュリティの実態
「情報セキュリティに関する調査」集計結果

平成14年3月

財団法人 日本情報処理開発協会

KEIRIN

この資料は競輪の補助金を受けて作成したものです。

序

当協会では、この度わが国における情報システムのセキュリティ対策の状況を把握するため、「情報セキュリティに関する調査」を実施いたしました。

調査は、企業等の情報システム部門を対象として行い、セキュリティ対策の現状と問題点を把握するとともに、今後のセキュリティ対策の傾向を把握することをねらいとしています。

調査にあたっては、718 事業体から回答をいただき、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、調査結果取りまとめ等にご協力いただいたリスクマネジメント委員会委員をはじめとする各位に心から謝意を表します。

平成 14 年 3 月

財団法人日本情報処理開発協会

平成１３年度リスクマネジメント委員会

（敬称略／五十音順）

委員長	森宮　康	明治大学　商学部教授
委　員	池内　正英	安全工学（株）　代表取締役社長
	笠間　誠一	（株）日立製作所　金融システム事業部金融ソリューションシステム本部　第一部
	指田　朝久	東京海上リスクコンサルティング(株)危機管理・情報グループ主席研究員
	花香　俊明	ハナカリサーチセンター　代表
	原田　要之助	（株）情報通信総合研究所　情報流通プラットフォーム研究グループ　グループリーダー／エグゼクティブリサーチャー
	松原　榮一	ガートナージャパン（株）ジャパンリサーチセンター　マネージングディレクター

目　　次

1．調査の概要

1.1　調査の概要 1
1.1.1　調査の目的 1
1.1.2　調査の対象 1
1.1.3　調査時期 1
1.1.4　回収状況 1
1.1.5　回答事業体の平均従業員数 1
1.1.6　調査項目 1
1.1.7　調査対象業種および回収状況 2
1.2　調査結果の要約 3
1.2.1　経済産業省の安全対策施策について 3
1.2.2　情報システム資産について 4
1.2.3　過去の障害等の実績について 4
1.2.4　情報セキュリティ管理一般について 5
1.2.5　災害対策・障害対策について 6
1.2.6　不正アクセス対策・不正侵入対策について 8
1.2.7　コンピュータウイルス対策について 9
1.2.8　情報リスクマネジメント関連について 10
1.2.9　情報セキュリティマネジメントシステム（ISMS）について 11
1.2.10　個人情報保護について 12

2．調査結果の詳細

2.1　経済産業省の安全対策の施策について 13
2.2　情報システム資産について 19
2.3　過去の障害等の実績について 23
2.4　セキュリティ管理一般について 26
2.5　災害対策・障害対策について 47
2.6　不正アクセス対策・不正侵入対策について 59
2.7　コンピュータウイルス対策について 68
2.8　情報リスクマネジメント関連について 76
2.9　情報セキュリティマネジメントシステム（ISMS）について 87
2.10　個人情報保護について 91
2.11　その他 97

3．クロス集計結果の分析

3.1　クロス集計の概要 98
3.2　Ｑ２のクロス集計 104
3.3　Ｑ５のクロス集計 106
3.4　Ｑ８のクロス集計 107
3.5　Q24 のクロス集計 113
3.6　Q44 のクロス集計 115
3.7　Q60 のクロス集計 116
3.8　Q62 のクロス集計 117
3.9　Q63 のクロス集計 137
3.10　Q69 のクロス集計 145

付属資料　　「情報セキュリティに関する調査」アンケート調査票

1．調査の概要

1.1　調査の概要

1.1.1　調査の目的

わが国における情報セキュリティの現状および意識を把握するとともに、今後の情報セキュリティの促進に役立てることを目的としている。

1.1.2　調査の対象

財団法人日本情報処理開発協会（JIPDEC）が隔年で実施している「情報セキュリティに関する調査」の母集団4,000事業体の情報システム部門を対象としている。

1.1.3　調査時期

調査票発送　　平成13年10月29日
回収締切　　平成13年12月26日

1.1.4　回収状況

発送数　　4,000件
回収数（回収率）　　718件（18.0%）

これまでの調査における回収率は、平成5年度33.9%、7年度29.3%、9年度23.3%、11年度18.4%であった。回収の割合は調査のたびに減少している。この点、質問票の留置期間が約2か月と長かったこと、調査依頼が多く、多忙な回答者にとり時間的に余裕がなかったこと、1.6に示すように質問項目数が多いこと等の理由があるかもしれないが、調査結果の活かし方に工夫が必要と思われる。

1.1.5　回答組織体の平均従業員数

2,198人

1.1.6　調査項目

1．経済産業省の安全対策の施策について（7項目）
2．情報システム資産・費用について（5項目）
3．過去の障害等の実績について（4項目）
4．情報セキュリティ管理一般について（9項目）
5．災害対策・障害対策について（16項目）
6．不正アクセス対策・不正侵入対策について（12項目）
7．コンピュータウイルス対策について（8項目）
8．情報リスクマネジメント関連について（9項目）
9．情報セキュリティマネジメントシステム（ISMS）について（8項目）
10．個人情報保護について（11項目）

今回の質問構成は全体で89項目からなっており、平成11年度調査（87項目）とほぼ同じ質問数となっているが、今回の調査実施にあたり、これまでの継続調査項目の見直し・整理を行い、また、情報技術の進歩による情報システム環境の変化を考慮した新たな質問項目や選択肢を加味した内容となっている。

さらに、リスクマネジメントの視点から情報リスクマネジメント関連、情報セキュリティマネジメントシステム（ISMS）、個人情報保護に関連する項目を増やし、これまで以上に現状の解明に役立つ調査を目指した。

1.1.7 調査対象業種および回収状況

調査対象の業種は下表の40の業種に分類しているが、さらに10の「業種グループ」に再分類している。本報告書においては、主に「業種グループ別」のデータを取り上げて論じている。

表1－1．回収状況

業務ｸﾞﾙｰﾌﾟ	業　種	回収数	平均従業員数	業務ｸﾞﾙｰﾌﾟ	業　種	回収数	平均従業員数
食品・紙・パルプ・繊維・印刷	食品製造業	14	1,031	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	74	606
	繊維工業	11	895	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	5	1,096		鉱業	2	110
	印刷業・同関連産業	6	2,256		建設業	36	2,228
石油・化学・鉄鋼・非鉄・金属	化学工業	30	2,157		新聞業・出版業	8	1,716
	石油製品製造業	4	1,507		不動産業	2	73
	鉄鋼業	8	3,193		運輸・通信・倉庫業	41	2,957
	非鉄金属製造業・金属製品製造業	25	1,040		電力・ガス業	6	6,964
電気・一般・輸送・精密機械	一般機械器具製造業	19	807		放送業	9	234
	電気機械器具製造業	41	6,674		広告・調査・情報提供サービス業	9	1,905
	輸送用機械器具製造業	17	4,176		その他のサービス業	23	923
	精密機械器具製造業	21	1,075	公共サービス	医療業	6	625
その他製造業	窯業・土石製品製造業	11	1,470		宗教法人	0	-
	その他製造業	42	1,800		高校	2	83
商　業	卸業・商社	58	1,054		大学	20	719
	小売業	25	3,117		その他の教育機関	9	111
金融・保険業	金融業	71	1,563		学術研究機関	1	116
	証券業・商品取引業	6	1,864		法人団体・農協	13	739
	生命保険業	3	6,312	政府・地方公共団体	政府	3	3,866
	損害保険業	2	5,046		地方公共団体	35	7,575
小　計		419	-	小　計		299	-
合　計						718	平均　2,198

1.2 調査結果の要約

本調査は、今日の情報システム環境に鑑みて 10 領域の調査項目から構成されている。さらに調査結果について仮説を立て、それを検証するためクロス集計結果を用いて分析を行った。クロス集計結果については、「第３部　クロス集計結果の分析」において分析結果を示している。ここでは、「1.6　調査項目」に示されている各項目についてその概要を示す。

なお、文中における「ＱＸＸ」は調査票の質問番号を、また、（H×：○○%）は各年度の調査結果を表している。

1.2.1 経済産業省の安全対策施策について

経済産業省の情報システムの安全対策に関する諸施策には、各種対策における指針を示す『情報システム安全対策基準』、『コンピュータウイルス対策基準』、『コンピュータ不正アクセス対策基準』ならびに『システム監査基準』がある。さらに、被害の実態を把握して改善措置を図るための『コンピュータウイルス被害届出制度』、『コンピュータ不正アクセス届出制度』のほか、不正アクセスによる被害の実態調査、被害に関する侵入手口の分析、再発防止の検討・助言等を行う『コンピュータ緊急対応センター（JPCERT/CC)』の設置ならびにシステム監査企業を登録し一般企業に紹介する『システム監査企業台帳制度』がある。

こうした情報セキュリティ関連の基準については、「利用している」、「知っている」とする回答はいずれも６割を超えており、各基準が社会に浸透している実態を表している。問題は、どれだけの組織体が現実にそれぞれの基準を利用しているかにある。

たとえば、『情報システム安全対策基準』は 14.8%が「利用」しており、「知っている」のは 53.2%であった。『コンピュータウイルス対策基準』の場合は 14.8%が「利用」しており、「知っている」のは 54.5%である。『コンピュータ不正アクセス対策基準』については 13.1%が「利用」しており、「知っている」との回答は 55.6%である。『システム監査基準』については「利用している」が他の基準に比べ低く、１割にも満たない 8.9%と結果となった。知っていながらもなぜ利用率が低いのか、その理由を分析する必要があるかもしれない。『システム監査企業台帳制度』については「知っている」のは 32.2%であるが、「利用している」のは 1.7%と非常に低い（Ｑ１）。

『コンピュータウイルス被害届出制度』ならびに『コンピュータ不正アクセス被害届出制度』のもとで情報処理振興事業協会（IPA）が被害届出機関として指定されている。特にコンピュータウイルス被害の届出について「知っている」と回答したのは 76.7%（H11：64.0%）で、前回調査の回答より 12.7 ポイント増加している。コンピュータ不正アクセスの被害の届出機関としては 71.0%（H11：57.1%）が「知っている」と回答しており、前回調査よりも 13.9 ポイントと大幅に増加している。これは昨今の被害実態の深刻さを反映したものと考えられる（Ｑ２）。

平成８年に制定された不正アクセス届出制度と並んで同じ年に活動を開始した『コンピュータ緊急対応センター（JPCERT/CC)』については、「知っている」と回答した割合は 42.6%（H11：32.8%）であり、届出制度と比べるとかなり低くなっているが、前回調査よりも約 10 ポイントの増加となった（Ｑ３）。

今回、平成 13 年３月に制定された『JIS Q 2001 規格　リスクマネジメントシステム構築のための指針』の認知度について新たに質問を設けた。阪神・淡路大震災を契機として、ISO に対する日本発の国際規格提案を目的の１つとして作られた JIS 規格であるが、制定されてからまだあ

まり時間が経っていないこともあり、「知っている」との回答は22.0%、「利用している」との回答はわずかに0.7%という低い結果となった（Q４）。

情報環境が変化するなかで個人情報の保護が重視されてきているが、平成 11 年４月に制定された『JIS Q 15001 規格　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』について「利用している」、「知っている」と回答したのは31.6%（H11:14.0）と、前回に比べ17.6ポイント増加し、ようやく浸透してきたことがわかる（Q５）。

平成13年秋期の情報処理技術者試験において、「情報セキュリティアドミニストレータ試験」が新設された。同試験については「実際、社員を受験させている」（7.1%）と試験自体を「知っている」（57.5%）との回答から、回答事業体の約 65%がこの試験を認知していることがわかる（Q６）。

事業体における情報セキュリティアドミニストレータの意義について、73.0%が人材として必要であるとの意識をもっている（Q７）。

1.2.2　情報システム資産について

情報システム資産については基幹システムの運用形態、基幹システム停止が経営にもたらす影響度合い（被害額）、開発・運用にかかる年間総費用等について考察した。

基幹システムの運用形態については、前回調査同様、メインフレーム等を衷心とする集中型が49.4%となった。この集中型に分散型の機能を有している集中分散型が31.8%で、前回調査と比べ、大きく減少し、逆に分散型が12.2%から17.0%へと増加した（Q８）。

基幹システムが１時間以上停止した場合の経営に与える影響（被害額）について、「想定していない」との回答は約８割を占めている（Q９）。また、想定している場合、１日あたりの被害額を１千万円未満と想定している事業体が47.1%と最も高い（Q10）。

現在稼働中の全情報システムの開発・運用にかかる年間総費用（過去１年間に支出した金額）として「１億円以上10億円未満」とする事業体が36.4%。次いで「５千万円未満」が23.5%であった（Q11）。

Q11に対する、アウトソーシング、システム部門の人件費、リース／レンタル、ネットワーク・回線使用料、減価償却費、その他の割合として最も多くを占めたのは、リース／レンタルで平均27.5%、次いで人件費（24.7%）となった。現在はアウトソーシングに関しては21.2%と前記の２つと比べ若干低い結果となったが、人件費、諸経費の削減目的から、今後アウトソーシングにかかる費用が増加することが予想される（Q12）。

1.2.3　過去の障害等の実績について

基幹システムのシステムダウン（過去１年間）について、平成７年度以降の結果をみてもさほど顕著な変化はみられない。今回調査では「全面的にダウンした」のが 9.1%であり、前回調査の11.4%に比べて2.3ポイント低くなった。「部分的なダウン」は45.0%（H11：40.3%）と、前回を約５ポイント上回っている。したがって、システムダウンに関する傾向は前回調査と同様、全面的には減少しているが部分的には増加となっている（Q13）。

システムダウンの原因について、回答の割合が高かったのは「ハードウェア」の 56.7%（H11：44.6%）で、「ソフトウェア障害」の 33.0%を 23.7 ポイント上回っている。また「ネットワーク機器などの障害」は 41.5%と前回調査（37.3%）よりも 4.2 ポイント増加しており、ネットワーク利用が重要となっている現状のなかで障害がかなり発生していることを物語っている。インターネット接続関連では「通信事業者に起因する障害」は前回調査（15.4%）から 12.4%と減少している。なお、「電源障害」、「空調障害」、「オペレーションミス」などについては過去の調査結果と比べてさほど大きな変化はみられない（Q14）。

基幹システムにおける平均故障間隔（MTBF）は 2,938.7 時間で、前回の 2,784.9 時間より若干長くなった。平均修理時間（MTTR）は 145.7 分と前回調査の 128.0 分より長くなっている。これは、ハードウェアの故障の種類やタイプが増えてきており、LAN やインターネット接続に関わるネットワーク機器の故障に対する修理が関係していると思われる（Q15、Q16）。

1.2.4 情報セキュリティ管理一般について

事業体における情報システム関連支出のうち、情報セキュリティ対策にかける支出割合がどれぐらいかを調査したところ、平均 4.1%という結果となった。なお、無回答が約３割を占めているが、これは対策費用がどれぐらいか把握できないケースが多いものと考えられる（Q17）。

平成 12 年７月に内閣の情報セキュリティ対策推進会議が「情報セキュリティポリシーに関するガイドライン」を策定した。本調査では、同ガイドラインで定義されている情報セキュリティポリシー構造（３階層構造）を想定して、情報セキュリティポリシーの策定状況等について調査した。

情報セキュリティポリシーは事業体における経営理念を反映して構成されるのが一般的と思われる。経営理念に基づいてセキュリティポリシーを「定めている」のは 24.0%と前回調査（18.9%）から 5.1 ポイント増加している。「定めていない」は 32.9%で前回（43.5%）より 10.6 ポイントも減少した。なお、「現在作成中」は 12.7%と前回（9.3%）より 3.4 ポイント増加している。

実施手続・規程類の策定状況については、「定めている」が 22.1%となった。一方「定めていない」は 32.5%となった（Q18）。

Q18 で調査したポリシーおよび実施手続・規程類の見直しについて、「定期的に見直しをしている」と回答したのが情報セキュリティポリシーで 66.9%、実施手続・規程類が 79.9%と、いずれも高い値となった（Q19）。

Q18 で情報セキュリティポリシーを策定／作成中の事業体に対し、何を参考にしたかを調査した。最も多かったのは BS7799 や ISO/IEC17799、前述の「情報セキュリティポリシーに関するガイドライン」で約半数が参考にしている。次いで「自社で独自に開発している」が 36.5%となった（Q20）。

現在の IT 環境において、出張や移動中に携帯端末や携帯電話を利用する頻度が高まっており、それゆえに移動中における情報セキュリティ対策は重視しておかなければならない。そこで、Q18 で実施手続・規程類を策定／作成中の事業体に対し、出張中や移動中の環境について規程類を定めているかを調査したところ、39.2%が「策定している」となった（Q21）。

基幹システムのネットワーク、情報システム、情報セキュリティの管理を担当する責任者の設置状況について調査した。

ネットワーク管理者については「定めている」のは 79.2%、「設置を検討している」(8.9%)をあわせると、88.1%がネットワーク管理者を重視していることがわかる。

情報システムの管理者については、「定めている」のは 79.1%で前回調査よりも約８ポイント減少した。

情報セキュリティ管理者の設置については、「定めている」が 52.8%、「設置を検討している」が 22.8%であり、両者をあわせると、前回調査 (23.8%＋12.5%＝36.3%) と比べ倍増した。(Q22)。

緊急時についての連絡手段は情報化社会では重要である。そうした時の連絡手段を持っている(「複数持っている 13.1%)」、「持っている 64.5%」) のが 77.6%と前回調査 (75.4%) に比べ微増した (Q23)。

情報セキュリティ管理についての問題点について調査したところ、「従業員に対する教育・訓練がいきとどかない」が最も多く 61.1% (H11：48.6%)、「コストがかかりすぎる」51.9% (H11：47.9%)、「ノウハウ不足」46.1% (H11:44.8%)、「どこまでやればよいのか基準が示されていない」42.1% (47.2%) がそれぞれ 40%以上という高い割合を示している。これらの項目については「どこまでやればよいのか基準が示されていない」以外はいずれも前回の割合を上回っている。特に「教育・訓練がいきとどかない」は 12.5 ポイントの増加となった (Q24)。

コンピュータ犯罪意識に関する質問では次のような結果が得られた。●『市販のソフトをコピーして使う』場合、それが「犯罪行為である (刑法上の処罰の対象となる)」という認識については 69.9% (H11：54.2%、H９：50.7%) となり、調査のたびごとに高まっている。●『データ、プログラムを無断で使う』のは「問題であると思う」割合は減少してきており (H11:26.9%→20.8%)、「企業内でも戒告等の処分の対象となる」(H11:30.1%→27.6%)、「犯罪行為である」(H11：29.4%→38.6%) という認識が定着しつつある。●『データ、プログラムを覗き見る』行為に関しては「問題であると思う」割合は減少傾向 (H11:38.6%→32.5%) にあるが、「犯罪行為である」(H11:18.8%→25.5%) という認識は高まってきている。●『就業時間内に会社のコンピュータを私用に使う』行為に対しては「問題であると思う」割合は 47.1% (H11:46.4%) であり、「企業内で戒告等の処分の対象になる」のが 39.1% (H11:33.6%) であった。「犯罪」という認識は 1.8% (H11:5.1%) と前回と比べてかなり低くなった。●『WWW を仕事以外 (個人目的での発注、アンケート回答等) で利用する』、『私用の電子メールを送・受信する』という行為は事業体のコンピュータの私的な利用に関する質問であるが、それぞれ 46.2% (H11:48.7%)、49.6% (H11:52.1%) の事業体が「問題であると思う」としている。●『他人のＩＤを無断借用する』行為については、「企業内で戒告等の処分の対象となる」のが 34.3 (H11:34.8%)、「犯罪行為である」が 34.4% (H11:26.2%)、「問題であると思う」のが 16.6% (25.4%) となった。●『業務上入手した顧客情報を正当な理由なしに第三者に売却する』という項目では 79.5%が「犯罪行為である」としている (H11:84.7%)。これに「企業内で懲戒免職の対象となる」(11.8%) を加えると 90%以上が厳しい認識を示している (Q25)。

1.2.5　災害対策・障害対策について

情報セキュリティポリシー、実施手続・規程類の基づいた災害・障害対策が明確になっているかとの質問に対し、53.6%が「特に定めていない」という結果となった（Q26)。

非常事態に対する危機管理マニュアル類の策定については、前回調査（44.0%）より2.5ポイント減少し41.5%が「作成している」、「作成中」と回答している（Q27)。

危機管理マニュアルで取り上げられている項目として、「事故・災害」（86.6%)、「障害」（78.5%）などの防災災害が中心となっており、ウイルスや不正アクセスに対する緊急対応を含むサイバーテロを取り上げている事業体は全体の11.7%と低い結果となった。

ところで、非常事態に備えて従業員に対する情報セキュリティの面からの訓練の実施状況については、「定期的に実施している」のはわずか6.0%（H11:5.2%）であった。「時々実施している」のは10.7%（H11:9.7%）と前回同様、あまり実施されていない。しかしながら、訓練を「特に実施していない」とする割合が82.6%(H11:76.7%)と圧倒的に多いのが気になるところである。この点、非常事態とは何を指しているのか、訓練の方法とは何かといった点を明確にすることが重要かもしれない(Q29)。

さて、情報システムの災害に対する復旧対策の実施状況について、「PC中の業務用ファイルのバックアップ」が最も多く、55.2%であった。次に多かったのは「ネットワークのバックアップ」（36.2%)、「手作業への復帰」（29.4%）となった(Q30)。なお、「特に対策を講じていない」（60件）理由で回答率が最も高いのは「コストがかかりすぎる」の46.7%（H11：65.6%）であった（Q31)。

情報システムの障害対策のために設置している機能について調査した。最も高い回答率を示したのは前回調査同様「ミラリング」の42.5%（H11:32.2%）であった。設置の割合は低いながら、前回に比べ増加が目立ったのは、「クラスタリング」（H11：5.5%→12.1%)、「コールドスタンバイシステム」（H11:9.8%→14.8%）である。一方、「特に設けていない」は前回の回答率46.3%から28.3%へと18ポイント減少している（Q32)。なお、障害対策機能を設けない理由は、復旧対策と同様に「コストがかかりすぎる」（65.5%）ことにあった（Q33)。

火災対策については、コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所について質問を行った。コンピュータ室では「自動火災報知設備」74.0%（H11:70.0%)、「消火・排煙等の防災機器の定期的点検」58.2%（H11:47.2%)、「ハロン消火設備」50.3%（H11：48.4%）の順となった。データ保管場所では「自動火災報知設備の設置」61.4%（H11：57.4%)、「消火・排煙等の防災機器の定期的点検」47.9%（H11:41.3%)、「耐火金庫の設置」36.8%（H11:37.4%）の順であった。ネットワーク設備室、コンピュータ設置場所についてもコンピュータ室、データ保管場所と同様の結果であった。なお、「特に対策を講じていない」についてはいずれも前回調査よりも割合が高くなっている。(Q34)。

地震対策に関しては、結果はほぼ前回調査と同じく、コンピュータ室で最も多い回答は「転倒防止措置」43.6%（H11:36.1%）で、次いで「フリーアクセス床は耐震構造」34.0%（H11:29.3%）であった。データ保管場所では「転倒防止措置」29.9%（H11：24.9%)、次いで「機器の移動防止措置」19.6%（H11:13.4%）であった。「特に対策を講じていない」との回答については、コンピュータ室は33.7%、データ保管場所、コンピュータ設置場所ともに48.9%といずれも高い割合となっており、火災対策と比べ、地震対策の実施率は低くなっている。(Q35)。

電源設備についての対策では、前回調査同様、圧倒的に「CVCF/UPS」80.4%（H11:76.7%）が

多く、「自家発電装置」が30.5%（H11:24.8%）となった（Q36）。

水冷の空調設備を使用している場合、何らかの災害が発生した場合、電源設備の予備が完備していても水冷用の水の供給がなければコンピュータが作動できない。そこで、どれぐらいの水を確保しているかを調査した。約半数が水冷の空調設備を使用していない。使用している事業体のうち、「まったく確保していない」が9.7%という結果となった（Q37）。

情報システム、ネットワーク室、機器の災害・障害対策で今後強化すべきこととして最も多かったのは「回線障害」（47.5%）、「ハードウェア障害」（37.6%）、「人の悪意による事故等」（36.6%）となった（Q38）。

システム災害・障害対策に関する問題点として最も多かったのは前回同様「コストがかかりすぎる」で72.1%となった（Q39）。

ネットワーク環境下での問題状況として、どのようなネットワーク機器・サービス障害を想定しているか、調査を行った。特に回答率の高かったのは「ルータ、サーバ（機器）障害」が74.7%、次いで「LAN（配線）の障害」64.5%であった。いずれも自事業体内での障害を中心に想定している（Q40）。

ネットワーク障害に対する対策については、「重要回線を部分的に二重化」25.8%（H11:19.5%）、「通信機器の二重化」（21.6%）、「異なる種別回線を利用」21.2%（H11:19.6%）、「専用のバックアップ回線を常時設定」17.8%（H11:16.0%）といった順位となっている。しかし「特に対策を講じていない」が34.5%と過去の調査（H11:48.6%、H9：51.9%）と傾向的には対策を講じていない割合は減少している（Q41）。

1.2.6 不正アクセス対策・不正侵入対策について

平成11年8月に「不正アクセス行為の禁止等に関する法律」が公布され、平成12年2月に施行された。この法律を「知っている」との回答は76.7%と前回（47.4%）と比べ大幅に増加した（Q42）。

不正アクセスの被害状況については、「物理的アクセス被害（コンピュータ室等への侵入）」が0.7%、「論理的アクセス被害（ネットワーク経由の侵入）」は14.6%と、それほどの被害は受けていない。とはいえ、前回調査の6.1%（物理的／論理的被害の区別なし）と比べると、今回調査では被害の率が倍増しており、これはインターネットの普及と論理的アクセス被害の増加に関係があると思われる（Q43）。

不正アクセス被害を受けた事業体がIPAに被害届を出したかどうかを調査したところ、22.7%（H11：20.8%が「出した」と回答している。Q2では71.0%（H11：57.1%）がIPAが被害届出機関であることを「知っている」と回答しているが、「知っている」のであればなぜ届け出ないのか。今回の調査で「知っている」ことと実際に届け出るという行動との乖離が明らかになったといえるが、問題はその原因を究明することも必要かもしれない（Q44）。

全回答者ならびにQ43で不正アクセス被害を受けた事業体に対して不正アクセス対策の実施状況を調査した。まず、ネットワーク室、機器、コンピュータ室、データ保管室での物理的不正アクセス対策として、最も多く実施されている対策としては、「室の管理責任者を定めている」で49.7%、「室の出入口で入室管理／退室管理を行っている」（45.3%／34.0%）、「入退室について

カード、パスワードを使用している」(37.7%) となった。一方、物理的不正アクセス被害を契機に講じた対策としては、「IPA や JPCERT/CC への相談」、「室の入室管理」があげられた(Q45)。

次にネットワークを介しての論理的不正アクセス対策について、最も多く行われているのは「ファイアウォールの利用」で 69.1%である。前回調査 (50.7%) から 18.4 ポイント増加した。次いで「パスワードの活用」(H11:83.4%→66.3%で 17.1 ポイント減)、「ネットワーク機器の運用者(アクセス範囲)の限定」(49.0%)、「ネットワーク管理者がサーバ、ルータ、ファイアウォールのログを定期的にチェック」(41.5%) と続いている。一方、論理的不正アクセス被害を契機に講じた対策としては、「アクセス制御ソフトウェアの使用」および「ネットワーク管理者によるログチェック」がともに 14.3%、次いで「ファイアウォールの利用」10.5%となっている (Q46)。

情報についての機密度のランク設定に関しては 28.4% (H11 : 26.5%) と、前回を若干下回っている (Q47)。

基幹システムのパスワードの変更設定のレベルについては、「パスワードの変更を推奨しているが、変更期間は利用者に任せている」が最も多く、35.8%であった (Q48)。

暗号の採用状況について、前回調査ではほとんどの事業体で暗号を採用していなかったが、今回調査では約3割が何らかの暗号を採用している。特に「市販の暗号ソフト購入」および「利用しているアプリケーションに付随している暗号機能」はともに 12.7%であり、手軽に暗号化を達成するツールの利用が可能となったことが、暗号の採用の普及につながったと考えられる(Q49)。どのような情報を暗号化しているかについては、「伝送するデータのうち重要なもの」が最も多く、46.0%、次いで「認証情報」(23.8%)、「記録媒体上の重要なもの」(22.3%) の順となった (Q50)。

PKI (公開鍵基盤) についての方針について今回初めて調査を行った。約7割の事業体が「検討をしていない」という結果となった (Q51)。

不正アクセス対策について、従業員に対する教育・訓練の実施状況については、27.6%の事業体が何らかの形により対応している。一方、69.8%が「特に実施していない」という結果となった。前回調査 (81.5%) と比べれば 11.7 ポイントの減少はしているが、早急に対応を図るべきである。

不正アクセス対策に関する問題点としては、「コストがかかりすぎる」(49.0%、H11:40.3%)、「ノウハウ不足」(42.5%、H11:40.9%)、「従業員に対する教育訓練がいきとどかない」(40.3%、H11 : 37.0%) がいずれも 40%台と高い割合となった (Q53)。

1.2.7 コンピュータウイルス対策について

過去1年間でコンピュータウイルスに感染したか否か(Q54)の調査では、68.8%がウイルスに感染したことが「ある」と回答しており前回(54.6%)から 14.2 ポイントと大幅に上回っている。

コンピュータウイルスの被害に遇った場合の届出状況については。情報処理振興事業協会 (IPA) に被害を届け出たのは 19.8% (H11:13.5%) と前回よりも増加した (Q55)。

何台のコンピュータが感染したかについて調査した結果、約半数は 10 台未満となっているが、一方で残りの半数は10台以上であり、最も多くて1,000台以上に感染したとの回答も6件(1.2%)あった (Q56)。

さて、主な感染原因（経路）であるが、電子メール自動感染型ウイルスによる被害が拡大しているが、その影響からか、「電子メールの添付書類で」（67.0%）が前回調査（52.6%）と比べ14.4ポイント増加した。また、「インターネット経由」による被害が22.0%から42.1%へと約倍増した（Q57）。

ウイルス被害を受けた場合、外部にその感染メールや感染ファイルを送ってしまったことがあるかを調査したところ、26.9%が「ある」と回答した。なお、「把握していない」との回答は19.8%となった（Q58）。

全回答者ならびにQ54 でコンピュータウイルス感染した事業体に対してコンピュータウイルス対策の実施状況を調査した。もっとも多く行われている対策としては「ワクチンソフトの利用」で84.8%であり、前回調査（76.0%）と比べ、8.8ポイント増加した。次いで「ワクチンソフト・パラメータファイルの定期的更新」（67.1%）、「サーバ機でのワクチンソフトの利用」（61.6%）となっている。一方、感染を契機として行った対策としては、「ワクチンソフト・パラメータファイルの定期的更新」（14.4%）、「ワクチンソフトの利用」（14.0%）、「緊急時の社員への連絡」（11.9%）、「サーバ機でのワクチンソフトの利用」（11.5%）となった（Q59）。

コンピュータウイルス対策に関する従業員の教育・訓練については、約6割が「特に実施していない」としている。前述の不正アクセス対策同様、従業員に対する教育・訓練の実施を重視していない傾向にある（Q60）。

コンピュータウイルス対策の問題点については、「コスト」43.3%（H11：39.6%）、「従業員に対する教育訓練」39.0%（H11：41.1%）、「ノウハウ不足」25.3%（H11:26.0%）の順となった。（Q61）。

1.2.8 情報リスクマネジメント関連について

情報セキュリティを実現するために重用と思われる要素を10項目とりあげ、それに対する優先順位（1～3位）を調査した。最も重要と思われているのは「情報セキュリティポリシー」（36.3%）、次いで「通信および運用管理」（12.3%）、「情報セキュリティ組織」（12.1%）という結果となった。なお、優先順位をつけずに選択のみをしたケースもあり、その結果については、「通信および運用管理」（51.4%）、「情報セキュリティポリシー」（49.6%）、「人的セキュリティ」（41.3%）の順となった（Q62）。

情報セキュリティの確保にとって重要な視点については、「社内全体の理解」が77.9%（H11：74.9%）と最も高い回答率を示している。定められた規則等を全員が理解し護ることは情報セキュリティにとり非常に重要といえる。次いで多かったのは「経営者の理解」53.3%（H11：53.7%）で、「管理者の理解」は32.7%（H11：30.4%）であった。管理者よりも経営者の理解が重要とする回答が多かったのは、経営資源を投入するには経営サイドの関与が必要と考えた結果であろう（Q63）。

情報リスクについては経営者の認識が重要であるが、コンピュータ関連の事件・事故に対するリスクへの関心度については、「高い」26.0%と前回とあまり変化はない。「中位」35.2%、「低い」22.4%という結果となった。ただ、「わからない」は前回（21.8%）から若干減少し、15.3%となった（Q64）。

リスクマネジメントの出発点はリスクの分析にあるのが常識である。情報システムにかかわるリスク分析の実施状況については、「行っている」は 18.8%と前回（12.0%）からは若干増加したが、いまだ約８割の事業体が「行っていない」と回答している（Q65）。

リスク分析を実施した際の問題点として最も高い割合を示したのは「確立した手法がない」で 62.2%（H11:58.7%）であった。次いで多かったのは、「分析のためのデータが乏しい」（38.5%、H11:26.0）、「専門家がいない」（34.1%、H11:49.0%）という結果となった（Q66）。

リスク分析を実施しない理由については、「手法がわからない」が最も多く 47.8%、次いで、「効果がわからない」（31.2%）、「予算がない」（26.4%）となった。ただ、「重要性を感じていない」が 13.3%もあり、「効果があるとは思えない」6.1%、「リスク分析の意味がわからない」9.5%をあわせると、リスク分析に対して 28.9%が否定的な見解を示したといえる（Q67）。

システム監査の実施状況について、「実施している」との回答は 34.8%となった（Q68）。システム監査を実施しない理由として最も多いのは「システム監査実施のためのコンセンサス、組織風土が備わっていない」で 39.1%と全体の約４割を占めた（Q69）。

今日のように情報システムが経営のあらゆる領域で利用されている現状に鑑みて情報システム関連のリスクが倒産に結びつくか否かについて質問したところ、「思う」（12.0%）と「重大な影響は受けると思う」（56.0%）をあわせると約７割の事業体が倒産との関係でかなり重大視していることが理解できる（Q70）。

1.2.9 情報セキュリティマネジメントシステム（ISMS）について

平成 13 年度よりパイロット事業として運用を開始した「ISMS 適合性制度」の認知度について、６割弱の事業体は制度自体を「知らない」という結果となった（Q71）。この ISMS 制度については「国際規格であり望ましい」とする意見が 51.7%と最も多く、逆に「国際基準よりも厳しい日本独自のものを追加して作成すべきである」との意見は 11.7%であった（Q72）。

ISMS 適合性制度が ISO9000 や ISO14000 などと同様に取引条件や安全性に関する評価基準として利用できるか、との質問に対して「一定の目安となる」との回答が最も多く 55.7%となった。「客観的な評価として利用できる」（18.5%）とあわせると、約７割が評価基準として利用できると評価している（Q73）。

ISMS 適合性制度の認証取得を「予定している」事業体は 16.8%となった。このうち、業種別にみると、情報サービス業が６割以上を占めている（Q74）。認証の取得目的としては「外部への一般的な情報セキュリティ保証として」が 44.0%、次いで「自社内部の情報セキュリティ目標として」が 20.0%となった（Q75）。認証にかかるコスト負担の程度については、「大きい」が 68.0%、「非常に大きい」が 14.0%と、約８割はコスト負担が大きいと考えている（Q76）。

ISMS 適合性制度の認証取得により期待する効果としては、「取引先からの信用を得られる」が 84.0%、「自社のイメージアップ」66.0%、「他社との差別化」が 42.0%となり、いずれも対外的な効果を期待していることがわかる（Q77）。

海外取引において ISMS 適合性制度の基準が役立つか、との質問に対し、「わからない」との回答が 44.0%「海外との取引に極めて有効」との意見が 32.0%となった（Q78）。

1.2.10　個人情報保護について

個人情報の利用目的では「従業員の管理（インハウス情報）」が57.1％と最も多く、次いで「顧客サポート」38.3％、「マーケティング」25.6％、「情報提供」22.3％といった結果となった（Q79）。その収集方法としては、「申込書等により情報主体から直接入手」が最も多く76.7％、かなりの差をもって「業務委託契約等に基づき提供を受ける」が12.5％である（Q80）。直接収集をする場合、収集・利用目的について同意をとっているかとの質問に対しては「同意をとっている」が59.1％と約6割がきちんと対応しているが、その一方で、本人の同意なしに利用している事業体が約2割もあるのは問題である（Q81）。また、間接的に収集する場合、「情報主体から同意を取っている」および「入手先が情報主体の同意をとっていることを確認している」をあわせると35.9％は同意のもとに利用していることがわかる（Q82）。

個人情報をコンピュータ処理する際の内部規程類の策定状況については、「定めている」（25.2％）および「作成中である」（6.1％）をあわせると3割程度が内部規程により管理をしていることがわかる（Q83）。個人情報の廃棄方法については、64.9％が規程で定めており、「作成中である」（14.7％）をあわせると約8割が廃棄について規程により管理していることがわかる（Q84）。

個人情報取扱いに関して責任・権限をもった管理者を「定めている」（33.8％）、「定めていない」は37.0％となり、若干「定めていない」方が多くなった（Q85）。

個人情報も取扱いに関する苦情処理窓口の設置状況について、窓口が「ある」との回答は39.3％、「ない」が48.2％と、窓口を設置していない事業体の方が10ポイント程度多い。（Q86）。

情報主体からの自己情報の開示・訂正・削除に応じる体制になっているかとの質問に対しては、「なっている」が50.3％、「なっていない」は31.1％となった（Q87）

個人情報を外部委託する際に委託先と取り交わす条項として、「秘密保持義務」を条項に入れる事業体が圧倒的に多く41.4％、次に「個人情報の適切な管理」24.7％となった（Q88）。

平成10年4月から運用している『プライバシーマーク制度』の認知度については、「知っている」が40.4％と、前回調査（20.0％）と比べると倍増した。とはいえ、いまだ約5割の事業体には知られておらず、もっとPRが必要である（Q89）。

2．調査結果の詳細

2.1 経済産業省の安全対策の施策について

Q１．経済産業省で制定している安全対策の各施策を知っていますか。施策ごとに回答して下さい。

（左欄：件数／右欄：%，以下同じ）

施　　策	利用している		知っている		知らない		無回答		計	
情報システム安全対策基準（平成7年8月改訂）	106	14.8	382	53.2	213	29.7	17	2.4	718	100.0
コンピュータウイルス対策基準（平成7年7月改訂）	106	14.8	391	54.5	203	28.3	18	2.5	718	100.0
コンピュータ不正アクセス対策基準(平成8年8月制定)	94	13.1	399	55.6	207	28.8	18	2.5	718	100.0
システム監査基準（平成8年1月改訂）	64	8.9	426	59.3	208	29.0	20	2.8	718	100.0
システム監査企業台帳制度（平成3年3月制定）	12	1.7	231	32.2	448	62.4	27	3.8	718	100.0

経済産業省（METI)が制定している情報セキュリティ関連基準の認知度合いについては、いずれも７割前後が認知（「すでに利用している」、「知っている」）している。しかし、システム監査を業として行っている企業を一般の企業等に紹介することを目的としているシステム監査企業台帳制度（平成３年制定）については、回答組織体の 33.9％と半数を下回っている。

情報システム安全対策基準の認知度については、平成 11 年度調査（以下、「前回調査」という。）の 63.6％に対し、今回調査では 68.0％と 4.4 ポイントの増加となった。

コンピュータウイルス対策基準の認知度については、69.3％と前回調査の 66.3％から３ポイントの増加となった。

コンピュータ不正アクセス対策基準（平成８年制定）は、前回調査の 61.6％から 68.7％と 7.1 ポイントの増加となった。

システム監査基準は、前回調査（66.9％）までは減少傾向にあったが今回調査では若干増加し、68.2％となった。

システム監査企業台帳については、前回の 37.4％から 33.9％と 3.5 ポイント減少した。他の基準に比べ、特に「利用している」割合が 1.7％と低いのが目立っている。これまで台帳（製本版）は全国の中央図書館、商工会議所等で閲覧する形をとっていたが、現在では METI および JIPDEC の Web でも公開ししているので、システム監査を外部へ依頼しようとする事業体は、本台帳を利用してもらいたい。

上記の各基準類、システム監査企業台帳は下記ののページで公開されている。

・METI「情報セキュリティ政策、書名認証、プライバシー」のページ
　http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
・JIPDEC「システム監査企業台帳」のページ
　http://www.jipdec.jp/security/daityo/list.html

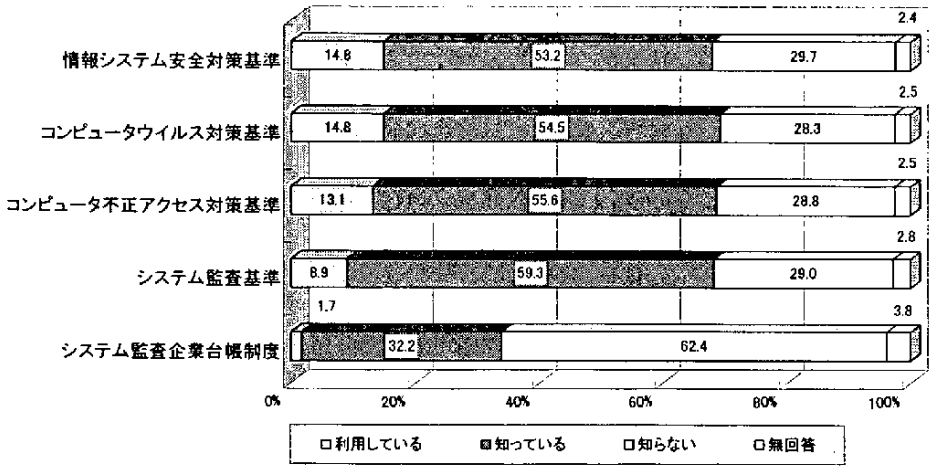


図2－1－1．経済産業省策定の安全対策関連施策の認知度

Q２．情報処理振興事業協会（IPA）がコンピュータウイルスおよびコンピュータ不正アクセス被害の届出機関として指定されていることを知っていますか。

被　害	知っている		知らない		無回答		計	
コンピュータウイルス被害(届出機関)	551	76.7	161	22.4	6	0.8	718	100.0
コンピュータ不正アクセス被害(届出機関)	510	71.0	201	28.0	7	1.0	718	100.0

METI は、コンピュータウイルス対策基準およびコンピュータ不正アクセス対策基準の制定に合わせて、各々の被害を届け出る機関として情報処理振興事業協会（IPA）を指定している。これは、被害の状況を把握することによって被害内容の分析と的確な対応策の検討を行い、被害の減少化に役立てようとするものである。

いずれも、被害届出機関としての存在は、回答の７割以上が認めている。

コンピュータウイルス被害届出機関に関しては、前回の 64.0％から 76.7％と、12.7 ポイントの大幅な増加となった。業種グループ別では大きな差異は特に認められないが、政府・地方公共団体（94.7％）、情報処理サービス（90.5％）、電気・一般・輸送機械製造業（83.7％）等が高い認知度を示している。

また、全情報システムの年間総費用（Q11 で算出）では、「100 億円以上」96.3％、「50～100 億円未満」100.0％、「30～50 億円未満」92.0％、「10～30 億円未満」94.7％、「1～10 億円未満」78.5％、「５千～１億円未満」73.8％、「５千万円未満」59.8％と、投資金額が多いほど認知度が高いことがわかる。

不正アクセス被害届出機関に関しては、前回調査では 57.1％であったが、今回は 71.0％と 13.9 ポイント増となった。業種グループ別、年間総費用別でみてもウイルス被害届出機関と同様の傾向を示している。

いずれも昨今のウイルスや不正アクセス被害の拡大に合わせて、マスコミ等を介して被害届出機関である IPA の知名度が上がったものと思われる。

・IPA の URL：http://www.ipa.go.jp/security/

Q３．不正アクセスの被害を受けた組織等からの依頼を受けて、被害の実態調査、被害状況の侵入手口の分析、再発防止策の検討と助言を行う「ＪＰＣＥＲＴ／ＣＣ（コンピュータ緊急対応センター）」を知っていますか。

1	知っている	306	42.6
2	知らない	405	56.4
無回答		7	1.0
計		718	100.0

コンピュータ緊急対応センター（JPCERT/CC）は、平成８年８月に設立され、同年 10 月から格的な業務を開始している。その目的は、特にインターネットに接続された組織体の情報システムが不正アクセスの被害を受けた場合、当該組織体からの依頼を受けて被害の実態調査、被害状況の侵入手口の分析、再発防止策の検討と助言を行うこと、さらにはサーバ関連ソフトのセキュリティホールに関する技術・警告等の情報提供を行うことにある。

したがって、インターネットを活用している組織体においては、自社のシステムを安全に運用管理するために JPCERT/CC の提供する情報を活用することが有効であるが、前回調査（32.8％）と比べ、約 10 ポイントの増加となった。

業種グループ別にみると、５割以上を占めたのは、政府・地方公共団体（63.2％）、情報処理サービス（55.4％）、公共サービス（54.9％）、電気・一般・輸送用機械製造業（50.0％）である。年間総費用別では、投資金額の多い組織体が高い認知度を示している。

・JPCERT/CC の URL：http://www.jpcert.or.jp/

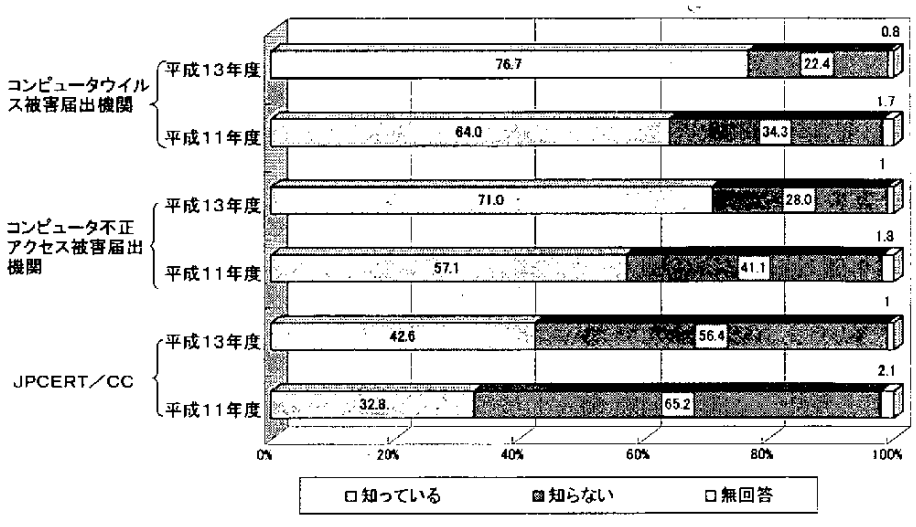


図2－1－2．被害届出機関(IPA)とJPCERT/CCの周知度

Q４．「JIS Q 2001 規格　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）を知っていますか。

1	利用している	5	0.7
2	知っている	153	21.3
3	知らない	548	76.3
無回答		12	1.7
計		718	100.0

自然災害、人為的事故、経済事件など、組織にかかわるさまざまなリスクの顕在化により、組織の運営、または存続をも揺るがしかねない事態を招く可能性が高くなってきている。併せてIT環境の高度化により自組織に限らず、関係者、さらには社会的損失までにも悪影響を与えかねない状況となっている。このような状況に対し、組織は経営をリスクマネジメントから捉え、リスクの影響を明らかにし、リスクに対応することがますます重要になっている。

わが国では阪神・淡路大震災を契機に、国際標準化機構（ISO）に対して日本発の国際規格提案を行うことを目的の一つとして、平成13年3月に「JIS Q 2001 リスクマネジメントシステムの構築に関する指針」を公表したが、同規格の認知度は22.0%という低い結果となった。

業種グループ別にみると、「情報処理サービス業」が40.5%、「金融・保険業」が24.4%、「商業」が24.1%、「政府・地方公共団体」が23.7%と、いずれも低い結果となった。

Q５．「JIS Q 15001 規格　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）を知っていますか。

1	利用している	40	5.6
2	知っている	187	26.0
3	知らない	477	66.4
無回答		14	1.9
計		718	100.0

情報化の高度化、ネットワーク化の推進等、情報環境のグローバル化が進むなか、個人情報の活用と個人情報保護の調和を図ることが強く求められるようになってきた。そのため、わが国では事業者が個人情報の保護を図るための基準として、国際ルールに適合した日本工業標準（「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」）を制定した。

「JIS Q 15001」の認知度は、31.6%と前回（14.0%）から２倍以上の増加となり、ようやく浸透してきたことがわかる。

業種グループ別に認知度の高い順にあげると、情報処理サービス（71.6%、前回46.1%）、金融・保険業（45.1%、前回14.3%）その他対事業所サービス（28.7%、前回14.6%）、石油・科学・鉄鋼・非鉄・金属製造業（26.9%、前回6.7%）、政府・地方公共団体（(26.3%、前回6.7%）となっている。他の業種は「JIS Q 15001」の認知度合いが低いといえる。

ところで、「Q１」、「Q２」、「Q３」、「Q４」、「Q５」のいずれもが「知っていますか」と設問されているが、「知っていますか」の捉え方としては概ね次のような解釈が考えられる：

・METIの安全対策の施策として該当するものがあることは知っている。しかし、内容については、全く把握していない。
・METIの安全対策の施策として該当するものがあることは知っている。内容については、概要程度は把握している。
・METIの安全対策の施策として該当するものがあることは知っている。内容についても、詳細に把握している。

したがって、回答結果は上記のような解釈にかかわらず、回答者が判断し回答した結果の表れと理解されたい。

Q６．情報処理技術者試験制度で新設された「情報セキュリティアドミニストレータ試験（SS 試験）」（平成１３年秋期より試験開始）を知っていますか。

1	情報セキュリティ担当者をSS試験に受験させている	51	7.1
2	知っている	413	57.5
3	知らない	247	34.4
無回答		7	1.0
計		718	100.0

「情報セキュリティアドミニストレータ試験（SS 試験）」は、平成 12 年度の情報処理技術者試験制度の見直しの中で、産業界を始め、情報セキュリティに詳しい人材が必須とのことで、新設された。試験は平成 13 年度の 10 月に実施され 23,778 名が受験を申し込み、実際に 15,988 名が受験し、2,111 名が合格した（情報処理技術者試験センター、http://www.jitec.jipdec.or.jp/）。

実際に試験に受験させたのは 7.1％であり、資格が重要と考えている企業が多いことがわかる。さらに、試験自体については「知っている」の 57.5％を合わせると企業の約 65％が認知していることがわかる。これからは、日本の多くの企業にとって、情報セキュリティに対する高レベルの技術者が必要となっていることがわかる。

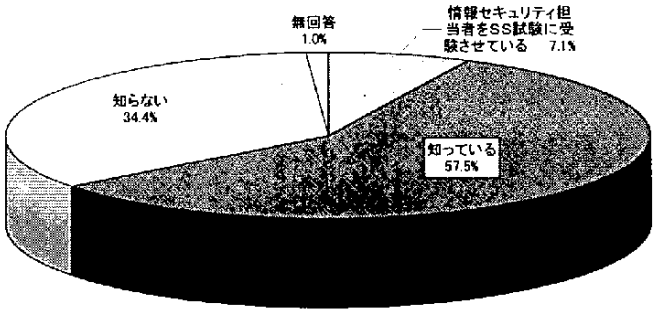


図2－1－3. 情報セキュリティアドミニストレータ試験の周知度

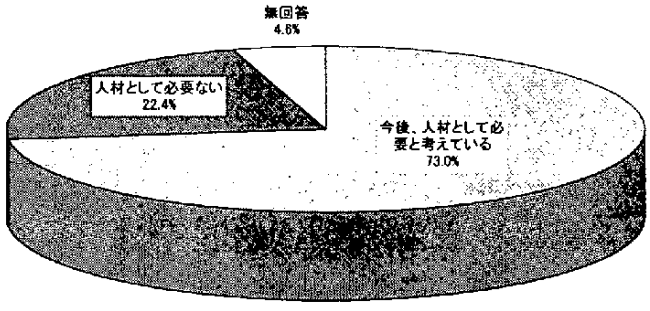
Q７．貴事業体での情報セキュリティアドミニストレータの意義についてお答え下さい。

1	今後、人材として必要と考えている	524	73.0
2	人材として必要ない	161	22.4
無回答		33	4.6
計		718	100.0

企業は、情報セキュリティが、企業の経営上重要となってきていることを自覚しており、その人材には情報セキュリティアドミニストレータを志向しているようだ。73.0％の企業が今後、情報セキュリティアドミニストレータを人材として必要としていることがわかる。これは、日常業務で利用するパソコン、インターネットを利用した電子メールや Web 情報の検索など、ユーザー

としての自社のコンピュータシステムを適正に運用するにはアドミニストレータが必要であること、さらに、このアドミニストレータには、情報セキュリティの高度な知識も身に付けていてほしいと企業側が考えていることがわかる。

企業は、基幹システムについてはセキュリティも含めて外部の企業にアウトソーシングすることで自社にセキュリティの人材を配置しなくても企業経営ができる。しかし、日常のパソコンやインターネットをほとんどの従業員が用いて業務を進めるようになった今日、日常業務のツールとしての情報システムのセキュリティが重要となっていることがわかる。今後の、企業の人材育成の一つのプログラムとして、情報セキュリティを組み込んでいく必要があることがわかる。



Q2－1－4. 情報セキュリティアドミニストレータ試験の意義

2.2 情報システム資産について

Q８．貴事業体の基幹システム(注)はどのように運用されていますか。(単一回答)

1	集中型	355	49.4
2	集中分散型	228	31.8
3	分散型	122	17.0
無回答		13	1.8
計		718	100.0

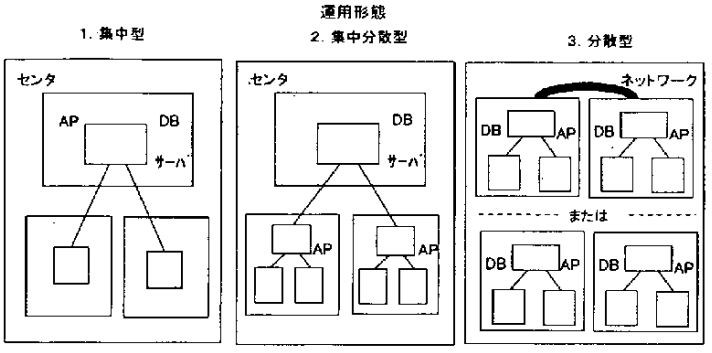


図2－1－1. 基幹システムの運用形態例

(注)基幹システムとは貴事業体が事業継続上必要とされる主要業務の遂行に欠くことのできない日常業務および決算業務の情報システムの総称ですが、ここではその中で最も重要なシステム1つに限定して回答

基幹システムの形態では、集中型をとる事業体の割合が前回の 47.8%から 49.4%へとわずかではあるが増加している。また、分散型も前回の 12.2%から 17.0%へと、非常に大きな伸び率を示した。一方、集中分散型は、前回の 38.2%から 31.8%へと大きく減少している。そして、その減少分のほとんどは分散型へ移行したと考えられる。これは、インターネットテクノロジをベースとする分散コンピューティングへ向かう大きなトレンドによるものと考えられる。一方、非常に高い稼働率が要求されるシステムについては、集中分散型の複雑性に起因した TCO が高いことに対する反省として、シンプルな集中型のシステムに移ったことの結果と考えられる。

Q９．基幹システムが１時間以上停止した場合、経営に与える影響（被害額注）がどれぐらいになるか想定していますか。

1	はい	157	21.9
2	いいえ ⇒Q11 へ	545	75.9
無回答		16	2.2
計		718	100.0

注)被害額には売上の逸失額、賠償金額、原状回復費用を含む。

情報システムは、すべて経営の成果を高めるために整備されるものである。

この調査は今回は初めてであるが、「いいえ」の回答が圧倒的に多いのが気になる(75.9%)。

経営に与える影響を概算でも想定しておかないと、今後、情報システムへの投資をどの程度にするかの判断の目安がはっきりしなくなるおそれがある。

また、情報セキュリティ対策にどの程度

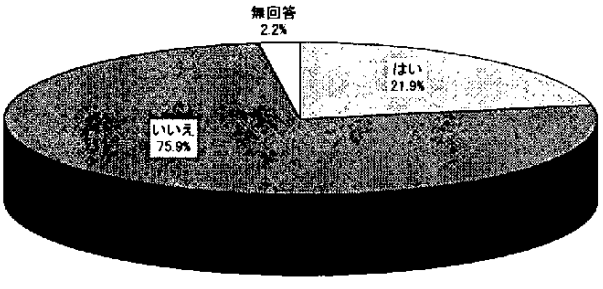


図2－2－2. 基幹システムの停止に伴う経営に与える影響度の想定

費用をかけたらよいかの判断が難しくなることも考えられる。ただし、今回「無回答」が2.2%であったことは、この問題に対する関心が高いことを示しているといえる。

また、産業別にみた場合、特に大きな差はなかったが、「はい」は第三次産業（23.9%）が第二次産業（21.8%）を若干上回っていた。

Q10. その場合の被害の推定額は1日あたりどれぐらいですか。

1	10億円以上	11	7.0
2	5億円以上～10億円未満	8	5.1
3	1億円以上～5億円未満	15	9.6
4	5千万円以上～1億円未満	14	8.9
5	1千万円以上～5千万円未満	29	18.5
6	1千万円未満	74	47.1
無回答		6	3.8
計		157	100.0

被害推定額は1千万未満が最も高く、47.1%であった。

情報システムが1時間以上停止した場合との質問（Q9）で、停止時間の長さをどの程度と想定したかによって、被害の推定額は違ってくることを考えると、これは妥当なものであろう。

また、「無回答」の3.8%は、基幹システムが1時間以上停止した場合、経営に与える影響はあると想定してはいるが、具体的な被害の推定額の把握までには至っていないものと考えられる。

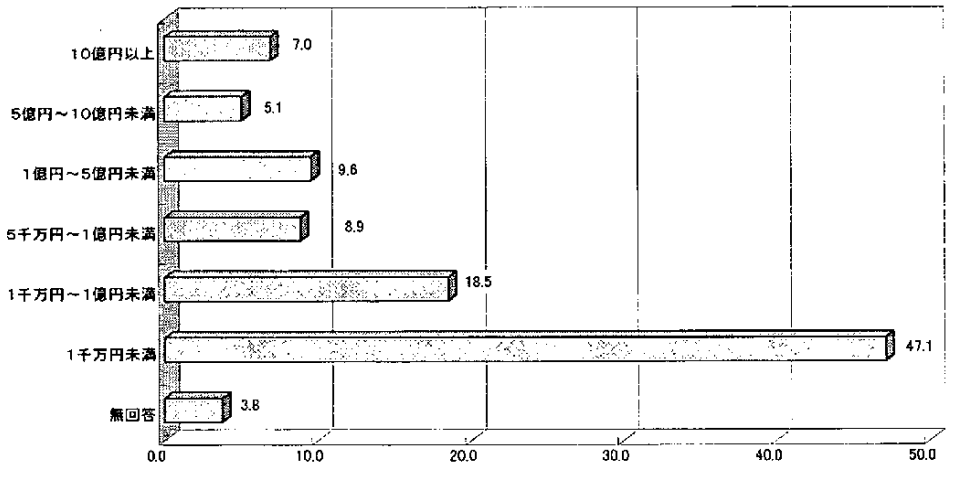


図2－2－3. 1日あたりの被害損失額

Q11. アウトソーシング、サービスを含む、現在稼働中の全情報システムの開発・運用に関する年間総費用[注]の概算を教えて下さい。

1	100億円以上	27	3.8
2	50億円以上～100億円未満	30	4.2
3	30億円以上～50億円未満	25	3.5
4	10億円以上～30億円未満	76	10.6
5	1億円以上～10億円未満	261	36.4
6	5千万円以上～1億円未満	80	11.1
7	5千万円未満	169	23.5
無回答		50	7.0
計		718	100.0

注）年間総費用は、情報システムの開発・運用のために、アウトソーシング、サービス、リース、レンタル、回線使用料等、費用として過去1年間に支出した金額

最もポイントの高い「1億円以上～10 億円未満」を産業別にみると次のようになる。第二次産業が 38.6%、第三次産業が 32.9%、政府・地方公共団体が 55.3%である。次にポイントの高い「5千万未満」は、第二次産業が 24.8%、第三次産業が 24.2%、政府・地方公共団体が 2.6%である。

政府・地方公共団体で「1億円以上～10 億円未満」の次に高いポイントを示したのは、「10 億円～30 億円未満」の（31.6%）であった。

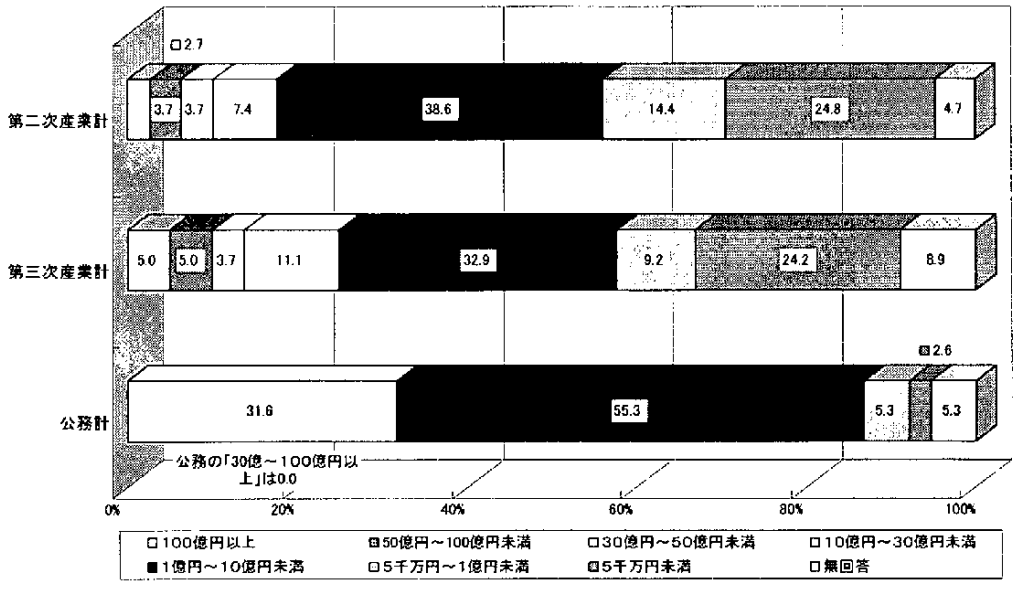


図2－2－4. 開発・運用に関する年間総費用の概算

Q12. 全情報システムへの年間総費用（上記）に対する下記の項目の割合は概算でどの程度ですか。

回答件数	557
アウトソーシング（開発・運用・保守）	平均 21.2%
自社情報システム部門の人件費	平均 24.7%
リース／レンタル	平均 27.5%
ネットワーク・回線使用料など	平均 10.6%
減価償却費	平均 9.0%
その他	平均 7.0%
無回答	161

全情報システムにかかる費用の割合としては、リース／レンタルにかかる費用が最も高く（27.5%）である。次いで自社情報システム部門の人件費（24.7%）が続いている。アウトソーシング関連費用は21.2%であったが、今後は、自社の人件費削減を含む諸経費の削減の目的から、アウトソーシングは増加アウトソーシングは増加の傾向にある。したがって、アウトソーシング関連費用の全体に占める割合は、徐々に増加していくものと考えられる。

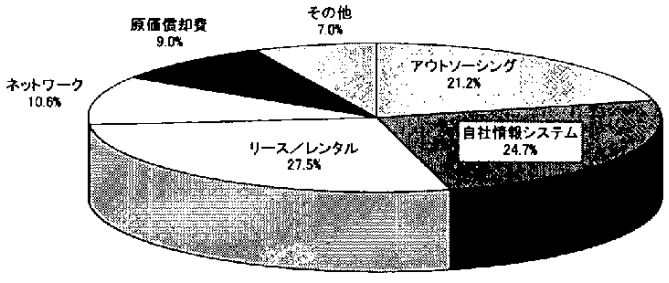


図2－2－5. 年間総費用に対する割合

2.3 過去の障害等の実績について

Q13. 貴事業体の基幹システムは過去１年間にシステムの運用に影響を与えるシステムダウンが発生しましたか。

1	全体的にダウンした	65	9.1
2	部分的にダウンした	323	45.0
3	しない ⇒Q17 へ	327	45.5
無回答		3	0.4
計		718	100.0

システムダウンの発生率は平成９年度 52.7%、11 年度 51.7%、13 年度 54.1%とあまり大きな変化はみられない。しかし、「全体的にダウンした」は９年度 13.2%、11 年度 11.4%、13 年度は 9.1%に徐々に減少している。これは障害対策に力を入れている組織体が増えつつあること、分散システムの増加によって大規模な障害が発生しにくくなっていることを意味している。

Q14. 過去１年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。（複数回答）

回答件数		388	
1	自然災害	27	7.0
2	電源障害	85	21.9
3	空調等障害	24	6.2
4	通信事業者に起因する障害	48	12.4
5	ISP(インターネットサービスプロバイダ)等、社外のインターネットに起因する障害	20	5.2
6	ネットワーク機器などの障害	161	41.5
7	ハードウェア障害	220	56.7
8	OS障害	58	14.9
9	ソフトウェア障害	128	33.0
10	コンピュータウイルス	61	15.7
11	火災による事故・障害	2	0.5
12	人の悪意(たとえば内部犯罪、不正侵入)による事故等	4	1.0
13	オペミス等人の過失による事故等	75	19.3
14	その他	5	1.3
無回答		4	1.0

(注1)システムダウンとは、システムの全面ストップもしくはそれに準じる障害と定義する。
(注2)1回の事故について原因が複数考えられる場合は、主要原因のみの回答。

前回調査から「ハードウェア障害」と「ネットワーク機器障害を区別しているが、両者を併せると前回の 81.9%から 98.2%と 100%に近い数値となった。ネットワーク機器を含むハードウェア障害が以前にもまして増えていることがわかる。これは、オフィス内におけるネットワーク機器やパソコンなどが増加したことによるものと考えられる。今後、オフィス内でのネットワーク利用が重要となるなかで、より障害の少ないネットワーク機器の開発が望まれる。

「通信事業者に起因する障害」（12.4%）は、前回調査（15.4%）から３ポイント減少した。

一方、「社外のインターネットに起因する障害」については前回調査（3.1％）から若干増加して5.2％となったが、両者を併せても２割に満たない状況であり、より通信環境が改善しているといえよう。

なお、その他の原因として、前回調査と比べて大きく変化があったのは、「自然災害」で、12.9％から 7.0％と 5.9 ポイントの減少となった。それ以外の原因についてはあまり大きな変化はみられない。

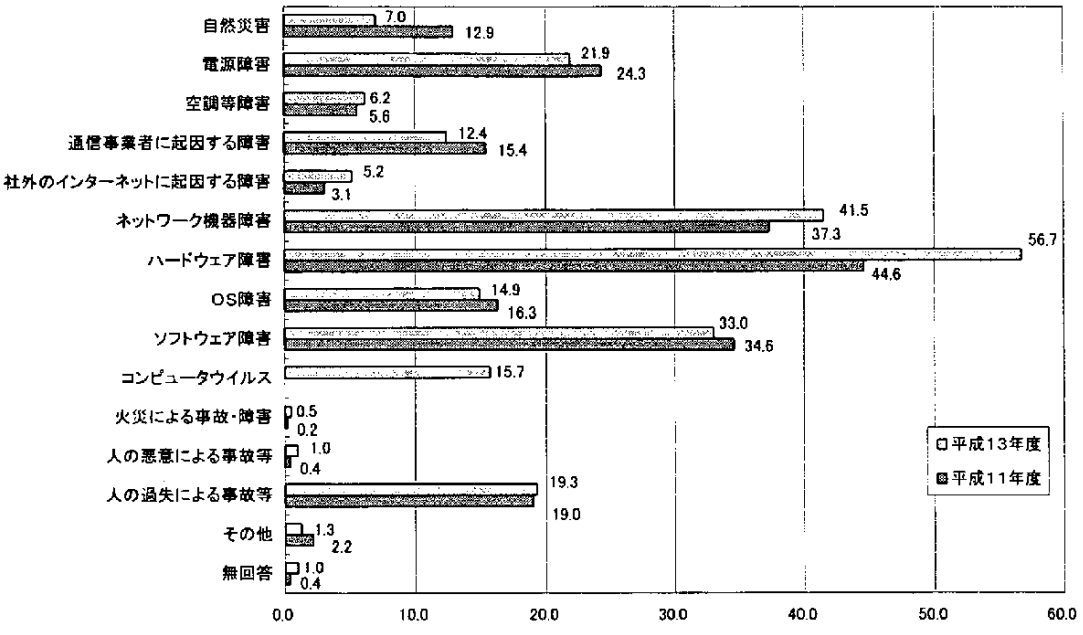


図2－3－1．システムダウンの原因

Q15．基幹システムにおけるＭＴＢＦ（平均故障間隔）は何時間ですか。

平均　2,938.7 時間

（回答件数 388 件／無回答 99 件）

（注）MTBFは、特定期間をとり、次の計算式で算出しています。
（システム稼働時間）／（ダウン回数＋1）

前回調査に比べ、若干 MTBF が長くなってはいるが、９年度調査時と比べると、相変わらず MTBF は短く、頻繁に故障が起きていることがわかる。この傾向はQ14 で述べたように、パソコンやサーバなどがより多く用いられるようになったためハードウェア故障が増えていることや、組織体内のネットワーク化やインターネットへの接続に用いるネットワーク機器の故障が起きているためと考えられる。この減少傾向がより進行しているのは、インターネットを通じた受発注、顧客へのダイレクト販売などが増加し、基幹システムへの改造とインターネットとの接続のためのシステムの複雑化によって故障の頻度が増していることも原因と考えられる。

Q16. 基幹システムにおけるMTTR（平均修理時間）は何分ですか。

平均　　145.7分	（回答件数388件／無回答90件）

平成13年度の調査では、9年度、11年度に比べて、故障修理に時間を示すMTTR（短いものがよい）が、短くなっている。平成11年度の調査では、企業の組織、パソコンやサーバーなどがより多く用いられるためハードウェア故障の種類が増えていることや、組織体内のLANやインターネットとの接続に用いるネットワーク機器の故障の修理に手間取っているためと考え、今後も長期化するような傾向にあると分析した。

MTTRが短くなった原因としては、コンピュータのモジュール化の進歩や装置自体のチップ化が進み、修理がより簡単になったものと考えられる。さらには、パソコンやルーターなどの設備は償却の時間間隔がより短くなるとともに、機器への能力（パソコンの処理能力やルーターなどの単位時間における処理パケット数）の増加のために機器を取り替える傾向にあることなども原因と考えられる。

なお、調査年ごとに回答件数が減少していることも短くなっている原因とも考えられる。

2.4 情報セキュリティ管理一般について

Q17. 貴事業体では、情報セキュリティ対策に情報システム関連支出の何パーセントを使っていますか。

平均　4.1%

（回答件数 718 件／無回答 197 件）

今回はじめて行った調査である。産業別に情報システム関連支出のうち、情報セキュリティ対策に占める割合で、ポイントの高い順からみると次のようになる。

業種	1%	5%	7%以上	無回答
第二次産業	22.1%	17.1%	11.4%	19.1%
第三次産業	18.4%	15.0%	12.9%	31.3%
政府・地方公共団体	18.4%	10.5%	2.6%	50.0%
計	19.9%	15.6%	11.7%	27.4%

無回答の理由としては、情報セキュリティ対策費が、情報システム関連支出の何パーセントを占めているか、把握できないケースが多いのではないかと考えられる。

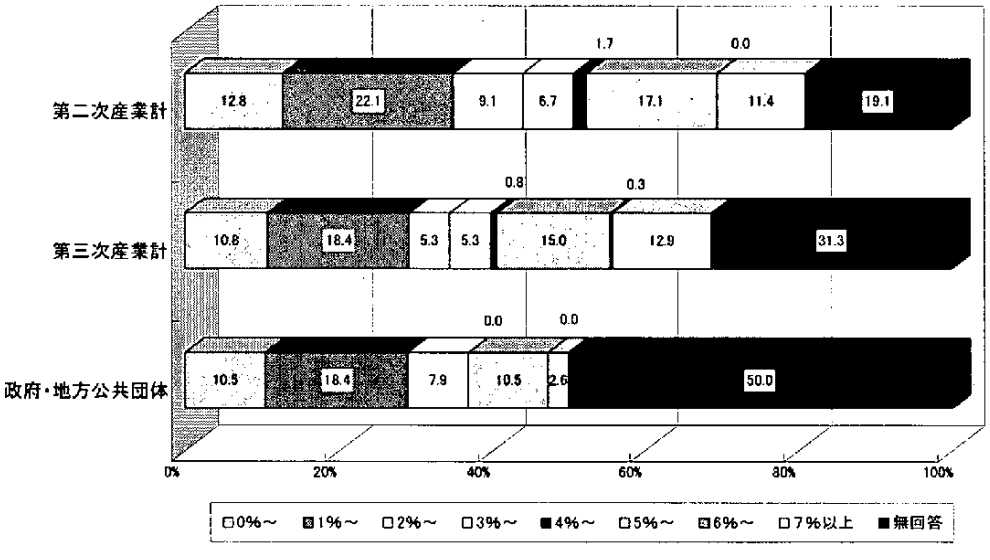


図2－4－1. 情報セキュリティ対策への情報システム関連支出の割合

以下の質問は、情報セキュリティポリシーについての質問である。ここでは、平成 12 年７月に内閣　情報セキュリティ対策推進会議が定義した情報セキュリティの３階層をベースにした構造（図 2-4-2）を想定している。

なお、図の詳細については、下記の「情報セキュリティポリシーに関するガイドライン」を参照していただきたい。

URL:http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

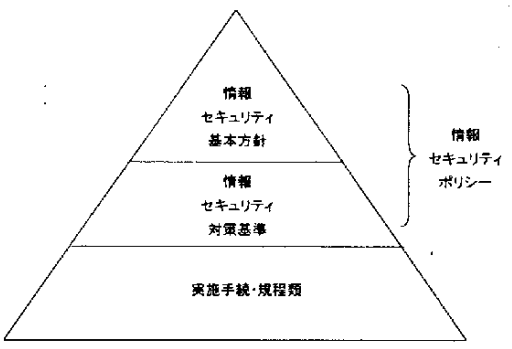


図２－４－２．情報セキュリティポリシー構造

Q18. 貴事業体では経営理念に基づく情報セキュリティポリシー、実施手続・規程類を定めていますか。

			情報セキュリティポリシー		実施手続・規程類	
1	定めている	⇒Q19 へ	172	24.0	159	22.1
2	現在作成中である	⇒Q20 へ	91	12.7	104	14.5
3	作成を検討している	⇒Q21 へ	207	28.8	204	28.4
4	定めていない		236	32.9	233	32.5
5	必要ない		5	0.7	6	0.8
無回答			7	1.0	12	1.7
計			718	100.0	718	100.0

情報セキュリティポリシーについては、平成12年7月に内閣　情報セキュリティ対策推進会議が主導で政府関係の組織体に向けて「情報セキュリティポリシーに関するガイドライン」を定めた。これが大きなトリガーとなって多くの組織体で情報セキュリティポリシーが定められたり、作成されつつある。平成13年度の調査では、情報セキュリティポリシーを「定めている」のは24.0%と、前回調査（18.9%）から5.1ポイント増加している。また、「定めていない」が32.9%であり、前回（43.5%）より10.6ポイントも減少した。

ただ、平成９年度調査に比べるとまだ、情報セキュリティポリシーの作成状況は低い（平成９年度の策定状況は 27.0%）。ただし、平成９年度の調査時点での情報セキュリティポリシーの意味するものの理解が組織体によって異なっていたことも理由として考えられる。これは、平成11年度と平成９年とで情報セキュリティポリシーと経営理念との関係を明確にするために、質問の表現を変えたことによるものと思われる。なお、「現在作成中」が12.7%と前回（9.3%）より3.4ポイント増加している。現在「作成を検討している」のは28.8%で３ポイント増加している。

情報セキュリティの実施手続・規程類を「定めている」のは22.1%で、前回調査で「定めている」とした回答の27.9%に比べて低い値となっている。また「定めていない」は32.5%で、前回調査（39.2%）よりも6.7ポイント減少した。一方、「現在作成中である」

(14.5%)、「作成を検討している」(28.4%)はいずれも前回調査の値に比べて増加している。これは、前回の調査では、情報セキュリティポリシーや情報セキュリティガイドラインという質問であったため、また、図 2-4-2 の情報セキュリティポリシーに対する用語の説明が不十分であったことにより、回答者の用語に対する認識が異なっていたためと考えられる。したがって、平成 11 年の調査結果と単純な比較だけで結論づけるのは危険であろう。しかし、「定めていない」と何らかの検討をしている差については比較の意味があり、実施手順や規程類についての認識が高まっているといえよう。

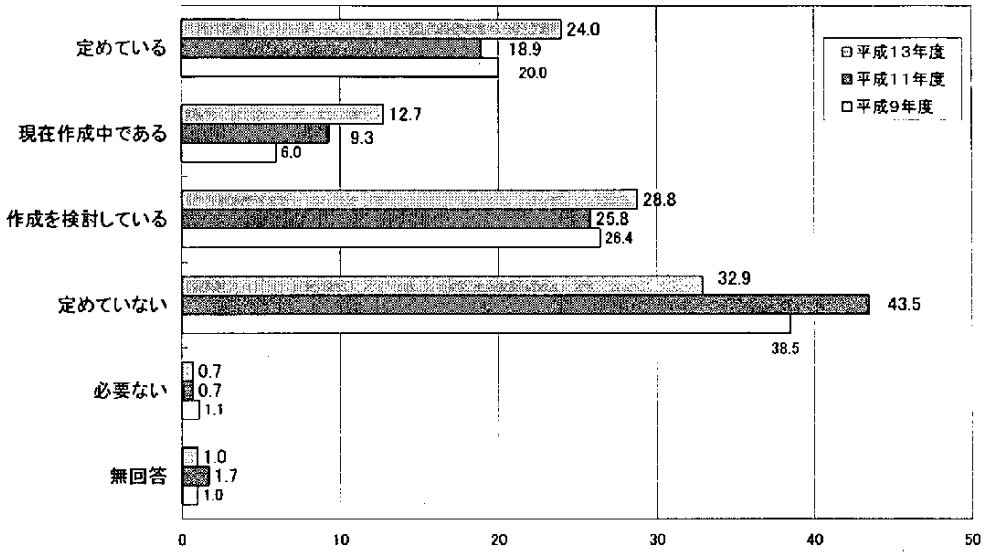


図2－4－3. 情報セキュリティポリシーの策定状況

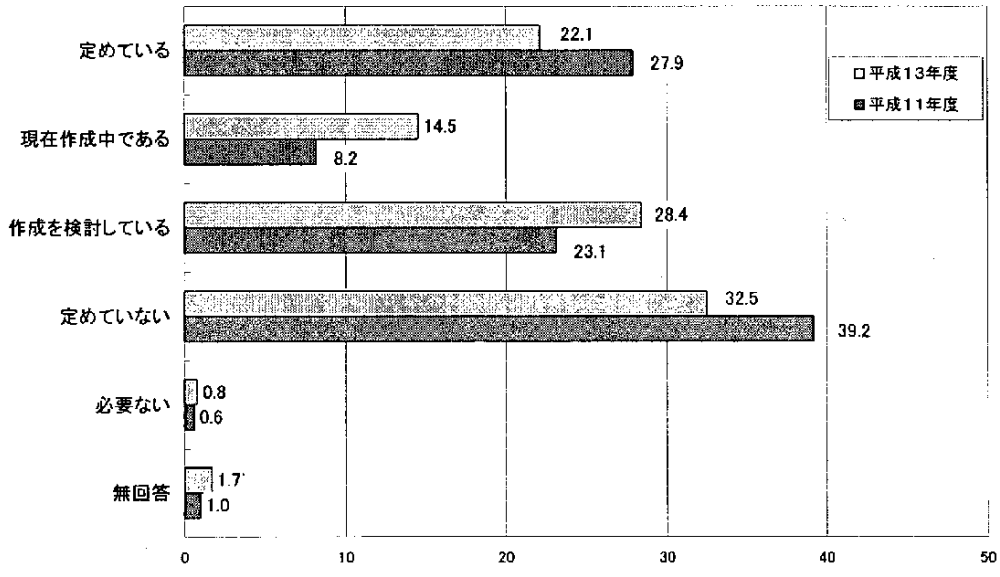


図2－4－4. 実施手順・規程類の策定状況

なお、情報セキュリティポリシーの作成状況と実施手順・規程類の作成状況の傾向は大変よく似ている。これを図 2-4-5 に示す。これは、図 2-4-2 に示す両者の関係が、情

報セキュリティポリシーを作成してからこれをベースにして実施手順・規程類を作成するようになっているためであり、平成 12 年に内閣が策定した「情報セキュリティポリシーに関するガイドライン」が強く意識されているためと考えられる。日本でも、情報セキュリティに対する認知度が高まってきているといえよう。

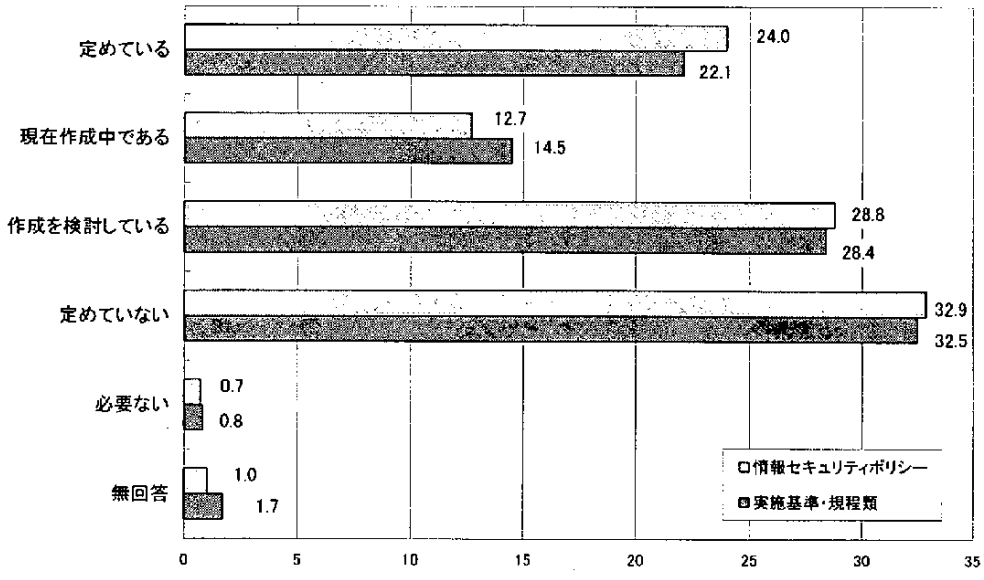


図2－4－5. セキュリティポリシーと実施基準・規程類との関係

Q19. 情報セキュリティポリシー、実施手続・規程類は定期的に見直していますか。
（「Q18 の「1」、「2」を回答」

		情報セキュリティポリシー		実施手続・規程類	
1	いる	115	66.9	127	79.9
2	いない	38	22.1	27	17.0
無回答		19	11.0	5	3.1
計		172	100.0	159	100.0

現代の情報環境は、平成 11 年度の調査時に比べてコンピュータウイルスやインターネットのサイトへの不正侵入が相継いでおり悪化している。そのため、情報セキュリティポリシーや実施手続・規程類の定期的な見直しが不可欠となっている。

前回調査ではガイドラインの見直しについて調査しているため、単純な比較はできないが、情報セキュリティポリシーを「定期的に見直しをしている」と回答したのは 66.9%、実施手続・規程類の見直しにあたっては、約８割の事業体が行っている。これは、内閣が情報セキュリティポリシーの重要性を宣伝したことや ISO17799 に定期的な見直しについて触れられていることが一因と考えられる。さらには、環境の激変を組織体が自覚しており、自主的に見直さざるをえなくなっているものと考えられる。

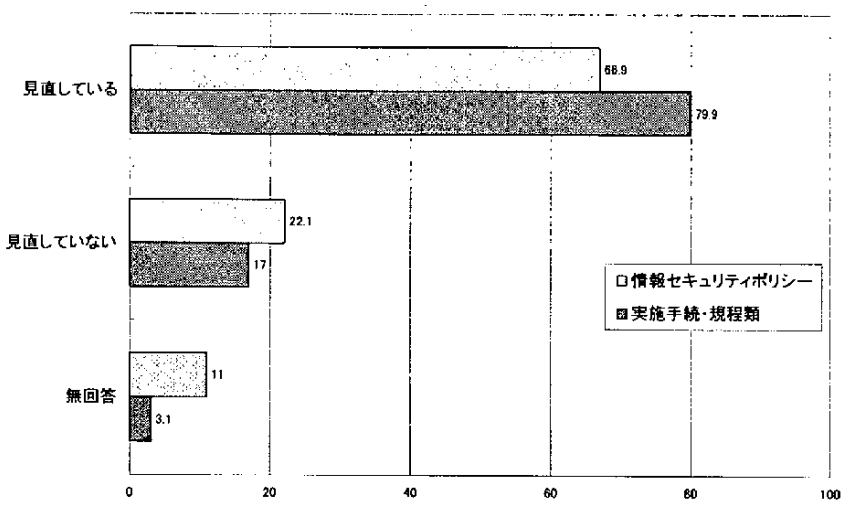


図2－4－6. 情報セキュリティポリシー／実施手続・規程類の見直しについて

Q20.（Q18で情報セキュリティポリシーを定めている／作成中の場合）貴事業体の情報セキュリティポリシーは次のどれを参照していますか。（複数回答）

回答件数		263	
1	BS7799、ISO/IEC17799、情報セキュリティポリシーに関するガイドライン(内閣)	132	50.2
2	日本銀行や金融情報システムセンター(FISC)のポリシー	68	25.9
3	COBIT(Control Objective for Information and related Technology)などのデファクト標準	5	1.9
4	自社で独自に開発	96	36.5
無回答		13	4.9

今回の調査では情報セキュリティポリシーを作成している事業体が増えたことから、何をベースにしてポリシーを作成したのかを調査した。結果としては、平成11年にはあまり知られていなかったBS7799やISO17799の比率が高く50.2%となっている。これは、平成12年に内閣が主導して政府関係組織に対し情報セキュリティポリシー策定を促したことによる影響が大きいと思われる。なお、この基準が出るまでは、情報セキュリティ対策が進んでいた金融機関では、日本銀行や金融情報システムセンター（FISC）のポリシー類が主に用いられていた。今後、金融機関以外の事業体での情報セキュリティポリシーの採用が広がるにつれて、この比率は減少していくと考えられる。

デファクト標準を利用したり、自主的に開発した組織体は、38.4%（101件）となっている。一方、平成11年には18.9%の組織体（164件）が情報セキュリティポリシーを持っている（図2-4-3参照）。これらの事業体では情報セキュリティの重要性に気づいて先行したため、デファクト標準を採用したり、自主的に開発したと考えられる。事業体は、個々にビジネスモデルが違っており、たとえISO17799を採用しても、そのままあてはまるとは限らない。標準などの利用できる範囲を知ってカスタマイズすることが重要である。

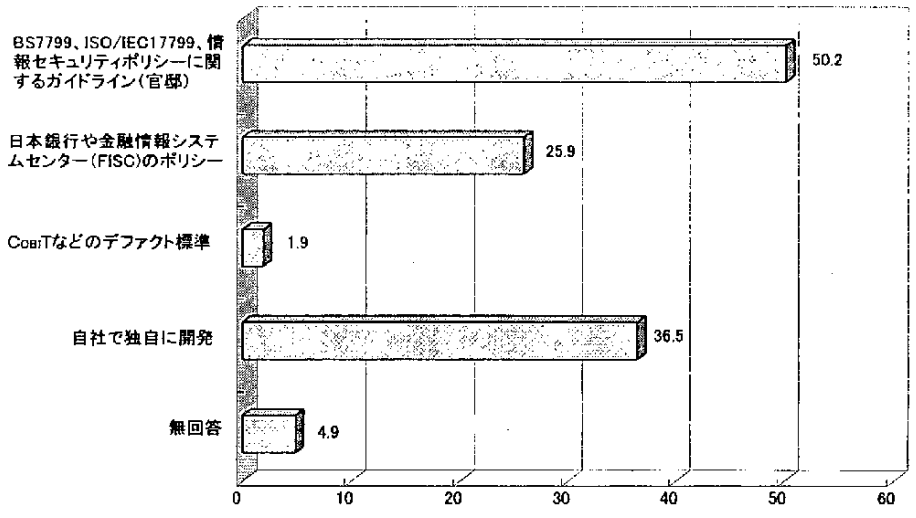


図2－4－7. 情報セキュリティポリシー策定時の参照項目

Q21.（Q18で実施手続・規程類を定めている／作成中の場合）情報セキュリティに関する実施手続・規程類には出張中、移動中の環境について定めていますか。

1	いる	103	39.2
2	いない	141	53.6
無回答		19	7.2
計		263	100.0

現在のIT環境における情報セキュリティに関しては出張中、移動中を問わず考慮すべきである。この設問は前回調査から設けた質問である。その時は、「移動中の情報セキュリティガイドラインを有している」という形で調査した。今回は、実施手続・規程類を持っている事業体の中で、移動中の情報セキュリティという設問で調査した。そのため、必ずしも内容は一致していないが比較をしてみた。

平成13年度の「出張中、移動中の環境について定めている」事業体の比率は39.2%で、平成11年度の「移動中の情報セキュリティガイドラインを有している」事業体の26.0%とに比べて約13ポイント増加している。これは営業担当が出先でパソコンや携帯情報端末、携帯電話を利用する頻度が高まっており、移動中の情報セキュリティを考慮している事業体が増加していることがわかる。

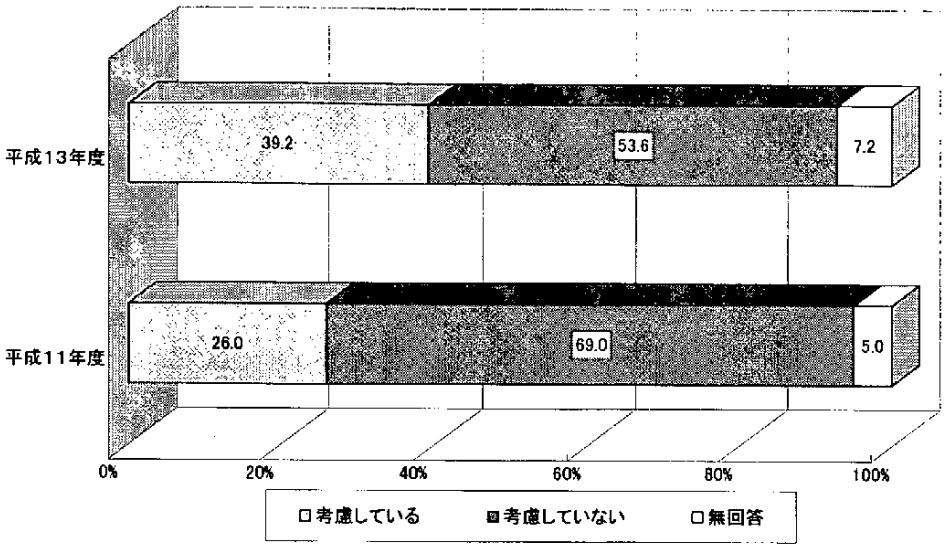


図2－4－8. 移動中のセキュリティに対する考慮の有無

Q22. 以下の管理について、責任を有する担当者を定めていますか。

管理項目 / 設置状況	ネットワークの管理		情報システムの管理		情報セキュリティの管理	
定めている	569	79.2	568	79.1	379	52.8
設置を検討している	64	8.9	70	9.7	164	22.8
定めていない	73	10.2	69	9.6	162	22.6
必要ない	3	0.4	1	0.1	2	0.3
無回答	9	1.3	10	1.4	11	1.5
計	718	100.0	718	100.0	718	100.0

今回、基幹システムのネットワーク、情報システムの管理、情報セキュリティの管理を担当する責任者の設置について質問した。前回調査では管理者について質問したが、管理に関しての責任の有無が重要とのことで、平成13年の調査では、担当者＋責任者という形で質問した。

ネットワーク管理者を「定めている」のは平成13年は79.2%で平成11年の76.4%に比べて2.8ポイントの微増であり、「検討している」8.9%（約4ポイント増加）をあわせると、実に88.1%の事業体がネットワーク管理者を重視していることがわかる。これは、ほとんどの事業体で基幹システムがネットワーク環境下で用いられることとともに、パソコンもインターネットに接続されて利用されていることがわかる。なお、「定めていない」は10.2%と、「必要ない」は0.4%となっており、両者を併せても10.6%と低い割合となった。

一方、情報システムの管理者については、「定めている」、「検討中である」ともにネットワーク管理者とほぼ同様の趨勢となった。これは、情報システムの管理とネットワークの管理がともに情報システムにとって同意語となりつつあることを示していると考えられる。「定めている」、「検討中である」をあわせると88.8%となり、平成11年調査の

90.3%と比べると、1.5 ポイント減少している。これは、今回の設問が責任者について聞いたためと考えられ、ほとんどの事業体において情報システム管理者が定められているといえよう。

なお、情報システム管理者を「定めていない（「定めていない」＋「必要ない」）は、まだ 9.7%近くある。この内訳は、その他対事業所サービス業や公共サービス業に多くみられる。これは、コンピュータを利用しているものの、外部サービスを利用していて組織内部に情報システムの責任者をおく必要がないと判断しているためと考えられる。

専任の情報セキュリティ管理者または担当者の有無については、「定めている」、「検討している」の肯定的な回答をしたのは、75.6%と平成 11 年の 36.3%から倍増した。一方、「いない」、「必要ない」という否定的な回答は 22.9%と平成 11 年度の 63.2%から激減した。これは、今まで以上にネットワークやコンピュータを利用する事業体が増え、不正侵入やウイルスなどの被害を受ける頻度が高くなったためと考えられ、平成 11 年度当時とくらべて様変わりしたといえよう。今後、どの事業体にとっても情報セキュリティ管理は無視できない状況と考えられる。

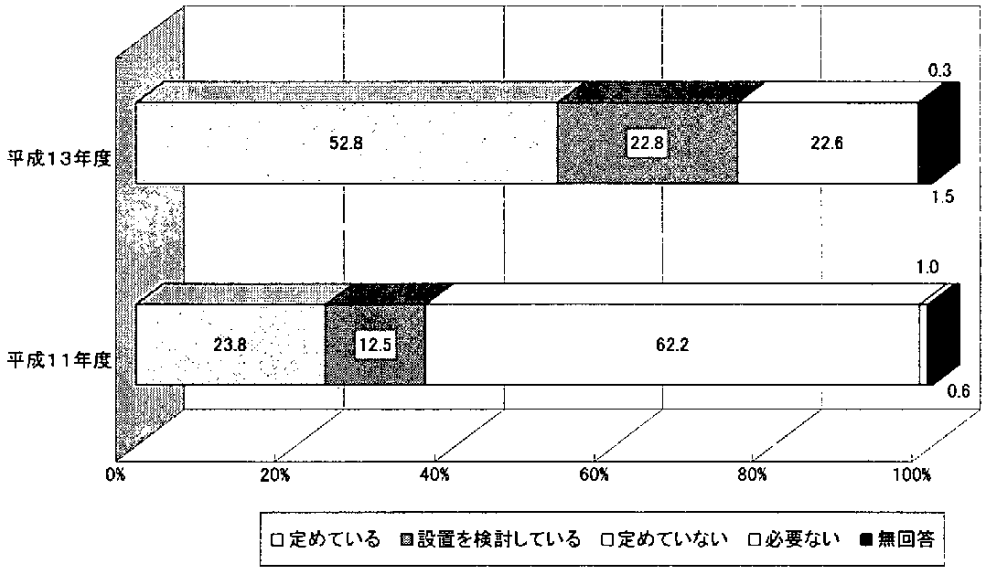


図2－4－9．情報セキュリティ管理責任者の設置の比較

専任の情報セキュリティ管理者または担当者の設置とシステム管理者、ネットワーク管理者の設置状況を比較すると、情報システム管理者、ネットワーク管理者、情報セキュリティ管理者の順であり、この傾向は平成 11 年と変わっていない。しかし、システム管理者とネットワーク管理者がほとんど差がなくなったこと、さらには、情報セキュリティ管理者についても急増しており、Q７では 73.0%の事業体が情報セキュリティアドミニストレータの必要性を述べていることから、いずれこの３つが同様な数字に落ち着くと考えられる。

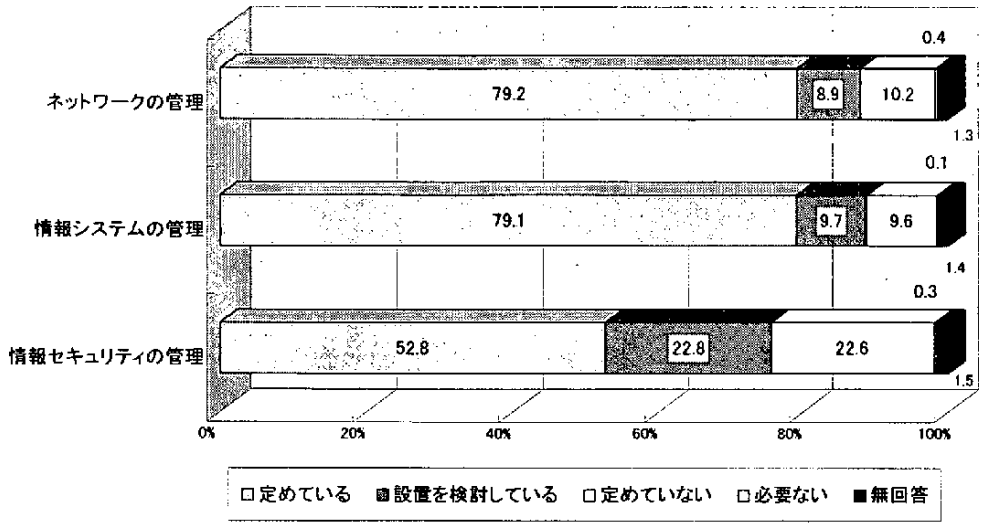


図2－4－10. 管理責任者の設置について

なお、各管理者の設置状況と事業体の企業規模（資本金、従業員数）、年間総費用との明確な相関はみられない。

Q23. 緊急時のための連絡手段を持っていますか。

1	複数の連絡手段を持っている	94	13.1
2	持っている	463	64.5
3	検討中である	72	10.0
4	持っていない	77	10.7
5	必要ない	4	0.6
無回答		8	1.1
計		718	100.0

全体傾向では前回とほとんど変わっていないが、わずかながら好転しており、緊急連絡手段を持っている（複数の手段＋持っている）比率は今回 77.6%、前回 75.4%と微増し、持っていない比率は今回 10.7%、前回 13.5%と減少している。必要ないとの回答はきわめて低く（今回 0.6%、前回 0.7%）好ましい傾向といえる。問題は「複数の連絡手段を持っている」の回答がまだまだ低く、業種グループ別にみると、最も高い回答でも金融・保険業の 18.3%にとどまっている。

Q24. 情報セキュリティ管理についての問題点は何ですか。(複数回答)

回答件数		718	
1	経営者層の理解が得られない	111	15.5
2	コストがかかりすぎる	373	51.9
3	組織の従業員に対する教育・訓練がいきとどかない	439	61.1
4	組織の従業員に対する負担がかかりすぎる	129	18.0
5	ノウハウが不足している	331	46.1
6	どこまでやればよいのか基準が示されていない	302	42.1
7	要求に合致するもの(サービス)がない	27	3.8
8	組織の従業員に倫理観が乏しく、情報を財産と認識する風土がない	139	19.4
9	情報セキュリティ管理が事業の国際化に見合っていない	9	1.3
10	その他	19	2.6
11	特に問題はない	23	3.2
無回答		11	1.5

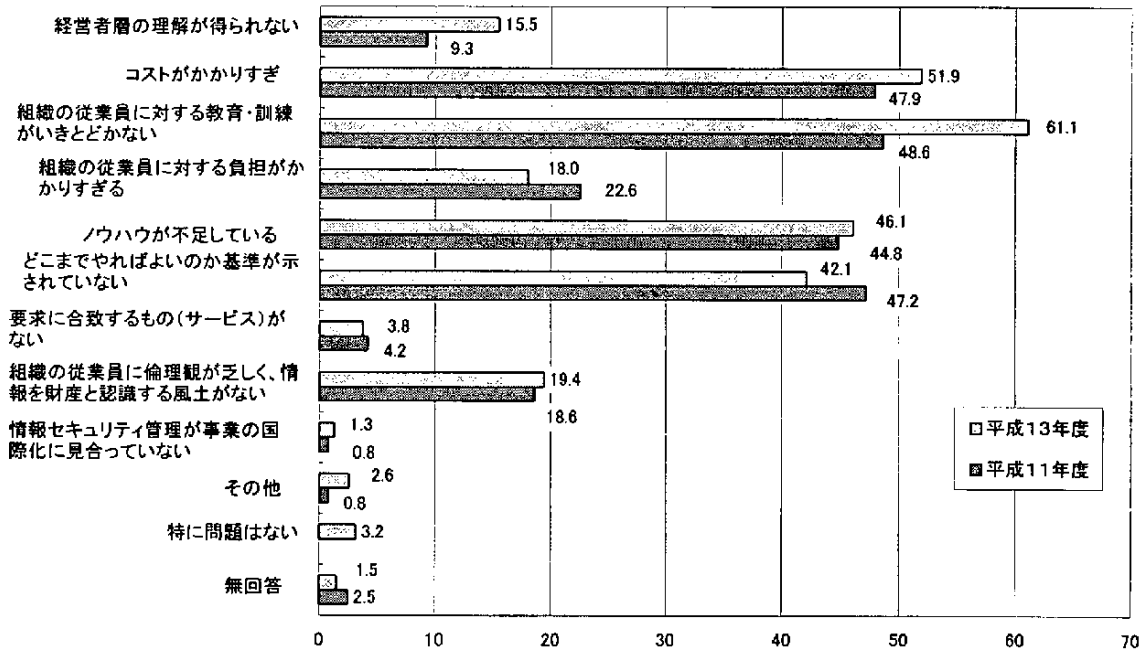


図2−4−11. 情報セキュリティ管理の問題点

Q17以降では「情報セキュリティ管理一般」について設問したが、情報セキュリティポリシーを定めているのが24.0%と、回答全体の4分の1以下であり、実施手続・規程類では22.1%とさらに低い傾向がみられた。こうした中、情報セキュリティ管理についての問題点については上記のような結果が得られた。最も高い回答は「組織の従業員に対する教育・訓練がいきとどかない」の61.1%であった。この割合は前回の48.6%を12.5ポイントも上回っている。情報セキュリティでは組織の構成員に対する教育・訓練が非常に重要であるにもかかわらず、それらが行き届かないのは、経営者層の認識というよりも現在の経営環境下、費用の負担能力に原因があるのかもしれない。次いで多い理由は前回トップであった「コストがかかりすぎる」(51.9%、前回47.9%)で、この

点を裏づけていると言えるかもしれない。前回の調査では、いずれも50%を超える回答がなかったが、今回、上記の２つの面で顕著な傾向がみられた。

また第３位には「対策を構築するノウハウが不足している」が46.1%と前回（44.8%）を1.3ポイント上回った。第４位に「どこまでやればよいのか基準が示されていない」が入り、42.1%と前回（47.2%）より5.1ポイント低いものの、それぞれ40%以上という高い割合を示している。第５位に「組織の従業員に倫理観が乏しく、情報を財産と認識する風土がない」の19.4%であった。

ところで、他の質問との関連から考察すると、第１位の「組織の従業員に対する教育・訓練がいきとどかない」について他の質問と比較してみると、次のような傾向がみられた。Q39「システム災害・障害対策についての問題点」の場合、「要員に対する教育訓練がいきとどかない」が23.3%と低く、情報セキュリティ管理一般に比べ、災害・障害といった個別課題においては問題が少ないのかもしれない。しかし、この点は、前回でも23.5%であり、同様の傾向を示している。

また、Q53 の「不正アクセス対策についての問題点」に関しては、「組織の従業員に対する教育訓練がいきとどかない」が40.3%と、かなり低めであった。この点に関する前回の回答は37.0%で、３ポイントほど高い割合となっている。全体的な課題と個別の課題との間に、若干受け止め方なり取り組み姿勢に違いがあるといえる。

特に、情報セキュリティ管理における問題点について２番目に高い回答であった「コストがかかりすぎる」（51.9%）に関しては、Q39 の「システム災害・障害対策についての問題点」では「コストがかかりすぎる」が最も高く、72.1%（前回80.6%）に比べると低い割合となっている。だが、「要員に対して負担がかかりすぎる」は24.0%であり、いずれにせよコストが問題となっている。

なお、「災害対策・障害対策について」の設問「情報システムの災害に対する復旧対策を講じない理由」（Q31）に関しては「コストがかかりすぎる」への回答が46.7%、「障害対策を講じない理由」（Q33）のうち「コストがかかりすぎる」への回答が65.5%と、それぞれ最も高い割合を示し、対応上コスト面の理由を重視している。

また、Q53 の「不正アクセス対策についての問題点」に関しては、「コストがかかりすぎる」が最も高かったが、回答は49.0%と上記に比べ若干低めであった。しかし、前回調査（40.3%）と比較すると９ポイントほど高い割合となっている。

次に回答数の比較的多い（10件以上の）業種別の結果についてみていくことにする。

回答の最も多かった「組織の従業員に対する教育・訓練がいきとどかない」で全体の割合である61.1%を超えているのは、第二次産業（60.7%：全体298件中181件回答）では建設業（61.1%）、化学工業（66.7%）、電気機械器具製造業（68.3%）、輸送用機械器具製造業（64.7%）、その他の製造業（64.3%）、第三次産業（59.7%：全体380件中227件回答）では小売業（64.0%）、金融業（67.6%）、大学（65.0%）、そして地方公共団体の77.1%であった。

「コストがかかりすぎる」で51.9%を超えていたのは、第二次産業（54.7%：全体298

件中 181 件回答）では建設業（52.8%）、非鉄金属製造業・金属製品製造業（68.0%）、一般機械器具製造業（57.9%）、電気機械器具製造業（56.1%）、輸送用機械器具製造業（58.8%）、精密機械器具製造業（71.4%）、その他の製造業（64.3%）であった。第三次産業（50.3%：全体 380 件中 191 件回答）では卸業・商社（55.2%）、運輸・通信・倉庫業（58.5%）、大学（55.0%）、そして地方公共団体（54.3%）であった。

「ノウハウが不足している」で 46.1%を越えていたのは、第二次産業（46.6%：全体 298 件中 139 件回答）では化学工業（46.7%）、非鉄金属製造業・金属製品製造業（60.0%）、一般機械器具製造業（52.6%）、電気機械器具製造業（48.8%）、第三次産業（43.7%：全体 380 件中 166 件回答）では（43.7%）、小売業（52.0%）、運輸・通信・倉庫業（46.3%）、情報処理サービス業・ソフトウェア業（48.6%）、そして地方公共団体（68.6%）であった。

「どこまでやればよいのか基準が示されていない」について、42.1%を超えていたのは、第二次産業（48.0%：全体 298 件中 143 件回答）では化学工業（43.3%）、一般機械器具製造業（63.2%）、電気機械器具製造業（46.3%）、輸送用機械器具製造業（64.7%）、精密機械器具製造業（47.6%）、その他の製造業（64.3%）、第三次産業（38.9%：全体 380 件中 148 件回答）では卸業・商社（56.9%）、小売業（44.0%）であった。

なお、前回の調査から設けた「組織の従業員に倫理観が乏しく、情報を財産と認識する風土がない」という質問に対しては 19.4%の回答率であったが、業種別にみると次のような結果が得られた。第二次産業（21.5%：全体 298 件中 64 件回答）では、その他の製造業（23.8%）が、第三次産業（18.4%：全体 380 件中 70 件回答）における卸業・商社（29.3%）であった。

「経営者層の理解が得られない」という回答は今回 15.5%であった。平成 11 年度では「トップの理解が得られない」という表現であったが、回答は 9.3%、平成９年度は 5.8%と、経営者層の理解が得られない割合が回を追って増えている理由はいかなることであろうか。

他の項目と比べて相対的に低い割合と思われるものの、情報システムの情報セキュリティについて経営者層に対する認識の点で、これはかなり問題といえる。ちなみに、業種別にみると全体の割合 15.5%を超えているのは、第二次産業（20.5%：全体 298 件中 61 件回答）のうち、電気機械器具製造業が 29.3%、その他の製造業が 26.2%、第三次産業総体では 12.1%であった。

なお、その他の意見としては、「要員不足」、「職員の情報セキュリティに対する意識不足」、「管理職層の倫理観の欠如」等があげられた。

Q25. 次の各行為をコンピュータ犯罪だと思いますか。各項目ごとに犯罪度欄の該当する番号に○をつけて下さい。

犯罪度＼行為	市販のソフトをコピーして使う		データ、プログラムを無断で使う		データ、プログラムを覗き見る	
特に問題ではない	5	0.7	8	1.1	22	3.1
問題であると思う	115	16.0	149	20.8	233	32.5
企業内で戒告・訓告・注意処分等の対象とな	67	9.3	198	27.6	206	28.7
企業内で懲戒免職の対象となる	13	1.8	60	8.4	46	6.4
犯罪行為である(刑法上の処罰の対象とな	502	69.9	277	38.6	183	25.5
わからない	10	1.4	19	2.6	20	2.8
無回答	6	0.8	7	1.0	8	1.1
計	718	100.0	718	100.0	718	100.0

『市販のソフトのコピー』に対してはこの２年間で急速に「犯罪行為である」との見方が増えてきた。平成７年度調査では 38.4%しかなかったものが９年度には 50.7%、前回調査では 54.2%、そして今回調査では 69.9%と急増した。ソフトのコピーが犯罪であるとの認識が定着したという、長年かけて教育してきた成果ともいえよう。

業種グループ別にみても明確な差異はみられないが、特に政府・地方公共団体、情報処理サービス業、金融・保険業、電気・一般・輸送用機械器具製造業の意識改革が進んでいる。今後は、せっかく定着した知識財産に関する行動が後退しないよう継続して教育していくことが必要であろう。

事業体規模別（資本金、従業員数）にみると、大規模なところほど刑法上の犯罪という認識が高く、資本金が小さくなるにつれて、犯罪という認識が小さくなり、一方では「問題である」が増えていた。この傾向は前回調査と比べ多少その差が狭まってきたが、引き続き中小企業に対して市販ソフトウェアのコピー問題をアピールしていくことが必要と考えられる。

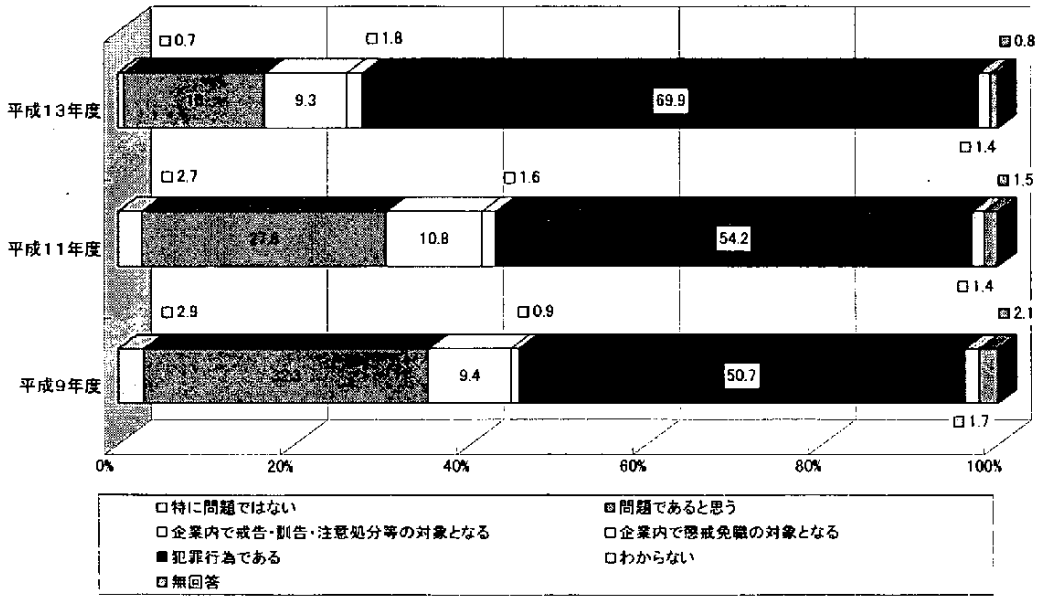


図2－4－12. 市販のソフトをコピーして使用

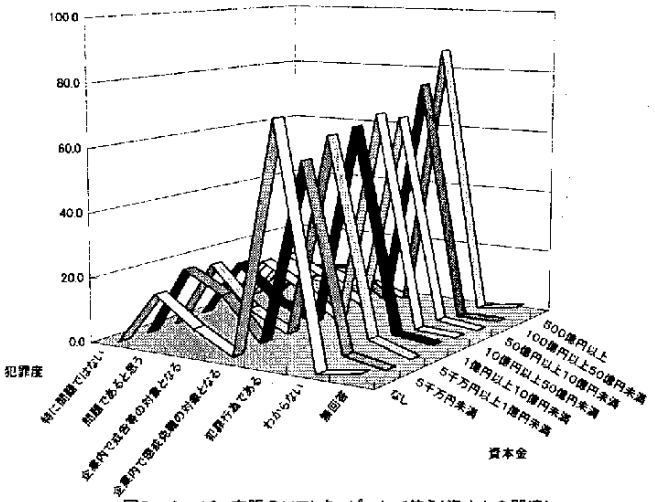


図2－4－13. 市販のソフトをコピーして使う(資本との関連)

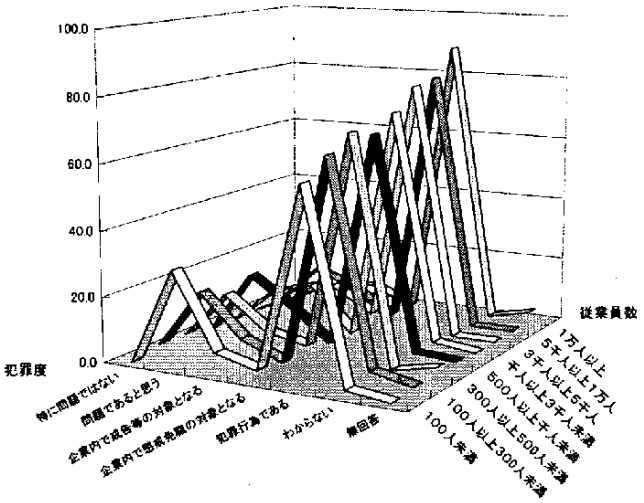


図2－4－14. 市販のソフトをコピーして使う(従業員数との関連)

『データ・プログラムの無断使用』については、市販ソフトのコピーに比べるとまだ犯罪との意識は低いが、前回調査と比較すると増加している（H11：29.4%→38.6%）。市販ソフトに比べると、単に問題であるとの認識から、企業内でも懲戒免職になったり、刑法上の犯罪行為であるとの見方が増加しており、犯罪という考えが広がりつつあるといえよう。

業種グループ別にみると、情報処理サービス業、金融・保険業、政府・地方公共団体が犯罪行為という点で意識改革が進んでいる。今後、この傾向が全産業に広がっていくものと考えられる。

市販コピーと同様に、事業体規模との強い相関がみられる。資本金の少ない小規模な事業体ほど犯罪行為という認識に欠けている。

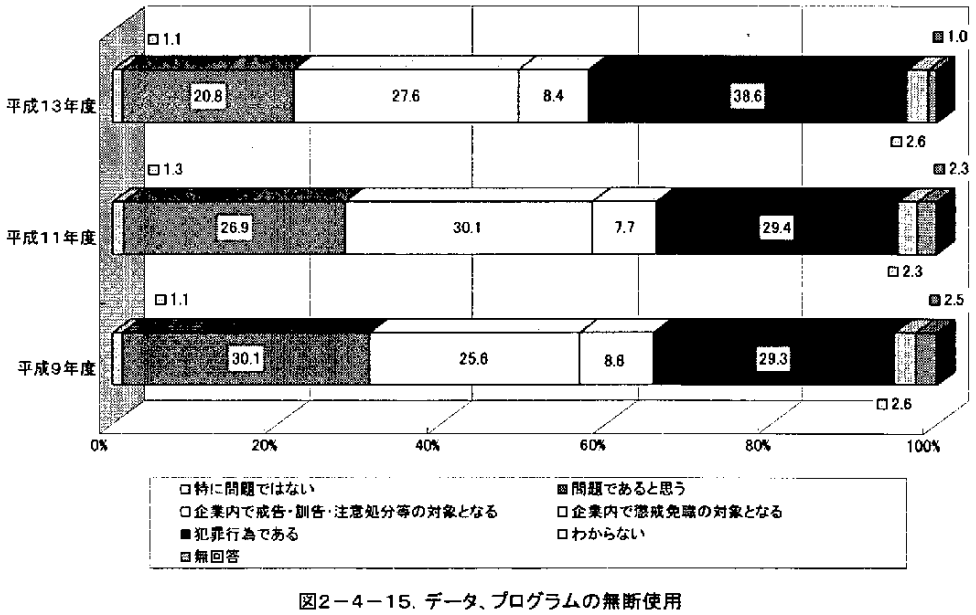


図2－4－15. データ、プログラムの無断使用

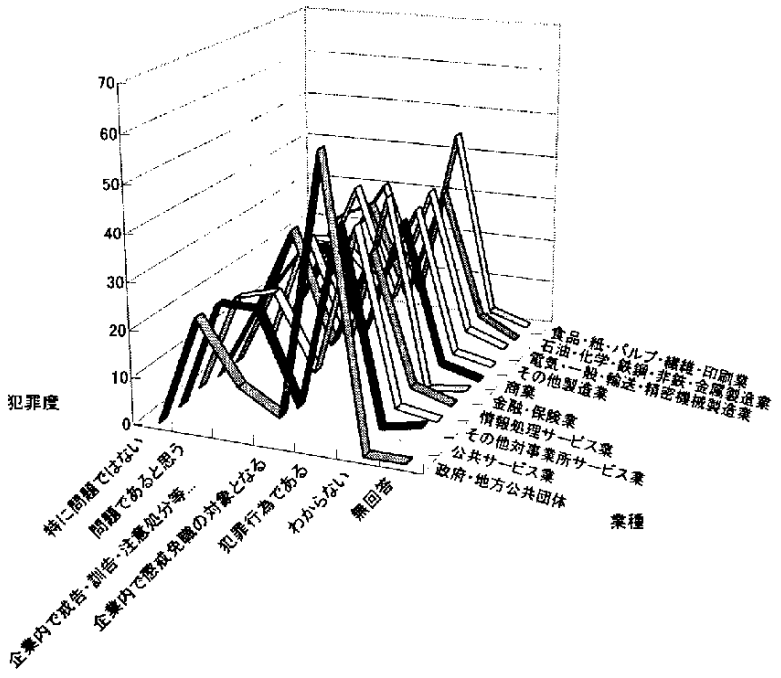


図2－4－16. データ、プログラムの無断使用(業種グループとの関連)

『データ、プログラムを覗き見る』行為について、前回調査と比べて「問題であると思う」という消極的な反応から、「犯罪行為である」との認識にシフトしている。特に「犯罪行為である」との認識が18.8%から6.7ポイント増加して25.5%となっている。しかし、市販ソフトのコピーやデータプログラムの無断使用に比べると処罰の対象や犯罪行為であるとの認識は依然として低い水準にある。

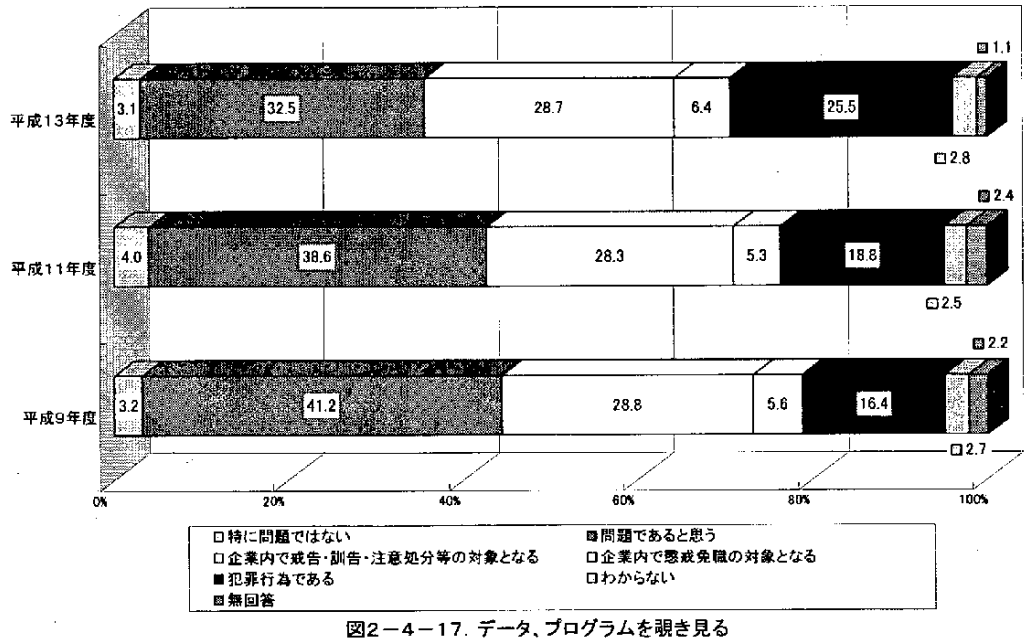


図2－4－17. データ、プログラムを覗き見る

業種グループ別にみると、前回、27.0%が「犯罪行為」と認識していた情報処理サービス業が18.9%に8.1ポイント減少したのに対し、政府・地方公共団体が20.0%から42.1%へと倍増した。

事業体規模との関係は、市販ソフトのコピー、データ・プログラムを無断で使うと同様に、規模の大小との強い相関が見られる。今後、中小企業における情報処理での一層の啓蒙化活動が望まれる。

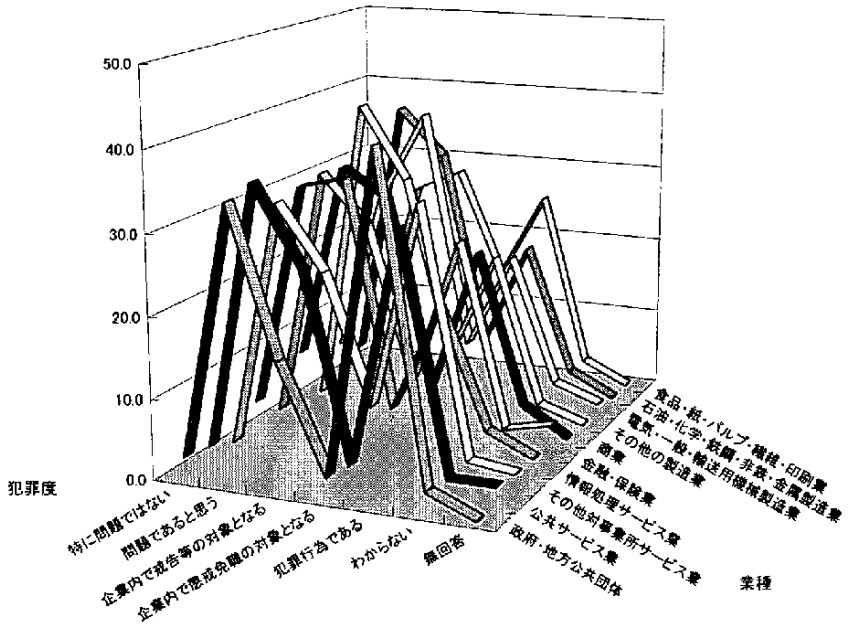


図2－4－18. データ、プログラムを覗き見る(業種グループとの関連)

行為 / 犯罪度	就業時間内に会社のコンピュータを私用に使う		WWW を仕事以外(個人目的での発注、アンケート回答等)で利用する		私用の電子メールを送・受信する	
特に問題ではない	32	4.5	45	6.3	76	10.6
問題であると思う	338	47.1	332	46.2	356	49.6
企業内で戒告・訓告・注意処分等の対象となる	281	39.1	282	39.3	232	32.3
企業内で懲戒免職の対象となる	39	5.4	31	4.3	23	3.2
犯罪行為である(刑法上の処罰の対象となる)	13	1.8	11	1.5	11	1.5
わからない	10	1.4	12	1.7	13	1.8
無回答	5	0.7	5	0.7	7	1.0
計	718	100.0	718	100.0	718	100.0

『会社のコンピュータを私用に使う』、『WWW を仕事以外で利用する』、『私用の電子メールを送・受信する』の３項目はいずれも事業体のコンピュータの私的な利用についての設問である。

『会社のコンピュータを私用に使う』行為に対して、「問題である」との認識は９年度、前回調査とほとんど大きな差がみられない。一方、「犯罪である」との認識は 5.1％から 1.8％に減少し、「企業内での戒告・訓告・注意処分等の対象となる」が 33.6％から 39.1％へと増加した。刑罰対象まで厳しくはないが、会社の資産を使用しているという意識が高まってきたものと思われる。今後とも組織内での教育が重要と考えられる。

事業体規模別にみると、やはり規模が大きくなるほど会社のコンピュータの私的な利用に関しては厳しい状況にあることがわかる。これは、従業員に対して情報化を率先させているため、また、私的利用で自組織の重要な情報が漏れる可能性もあり、管理が厳重になっているためと考えられる。
業種グループ別にみると、あまり大きな差は見られないが、情報処理サービス業、金融・保険業、政府・地方公共団体での意識改革が進んでいる。情報を活用する業種では私的な利用は組織内では処分されるようになってきているといえよう。

『WWW を仕事以外（個人目的での発注、アンケート回答等）で利用する』行為について「問題がある」との認識は前回調査とあまり差は出ていない。しかしながら、『コンピュータの私用での利用』同様、「企業内での戒告・訓告・注意処分等の対象」との意識が高まってきており、前回調査の 30.2％から 39.3％へと約 7 ポイント増加した。
特に、WWW を利用して従業員が勤務時間内にショッピングをしたり、株式を売買したり、ピンク系サイトを覗き見たりすることが増加してきており、多くの事業体が問題視している。これに対しては、ファィアウォールで、特にこれらのサイトへのアクセスを制限するフィルタを入れる事業体が増えてきている。
ただ、企業としても、WWW が企業の IT 上必須となっており、WWW をむやみに制限できず、結局は個人使用について厳格な態度をとりながらも、ある程度はコンピュータリテラシィ教育のためにはある程度の個人利用はやむを得ないと黙認している現状が推察できる。
事業体規模別にみると、事業体規模が大きくなるほど、犯罪度の意識が高まっている。なお、業種グループ別ではさほどの差は出ていない。

『私用の電子メールを送・受信する』については、前回調査では「問題ではない」と考える企業が 20％を超えていた。しかし、今回調査では 10.6％と半減している。一方、「企業内で戒告・訓告」または「懲戒免職」との対象とみなしていることについては、前回約 20％であったものが、35.5％に増えており、事業体にとって私的電子メールは禁止の方向に向かっていることがわかる。私的メールは、組織の重要な情報漏洩を引き起こしたり、また、労働生産性を低下させることにもつながることから、多くの事業体が制限するようになると考えられる。

事業体の多くが、WWW も電子メールも個人利用を厳しく取り締まり始めたといえよう。すでに、企業は IT を授業員レベルにまで拡大させており、電子メール、WWW は企業のホワイトカラーの重要な仕事のツールとなっていることがわかる。これは、ホームページの検索やサーフィンは電子メールに比べて時間を要するため、また、他の従業員が模倣しないためにも、厳しい対応となっていると考えられる。

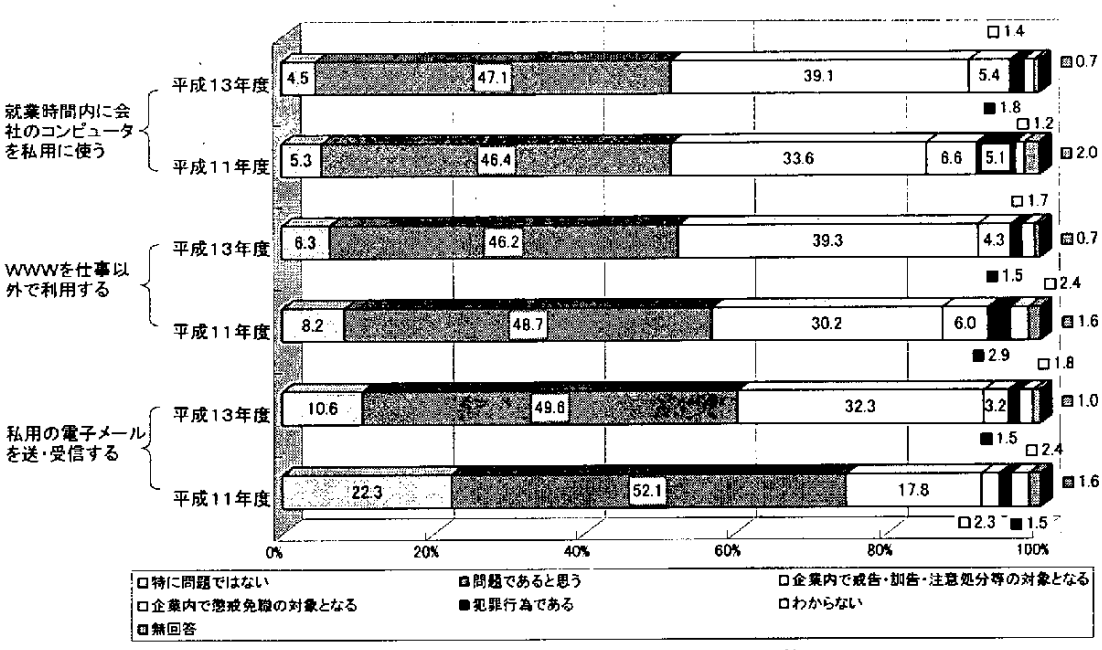


図2－4－19. コンピュータの個人私用についての比較

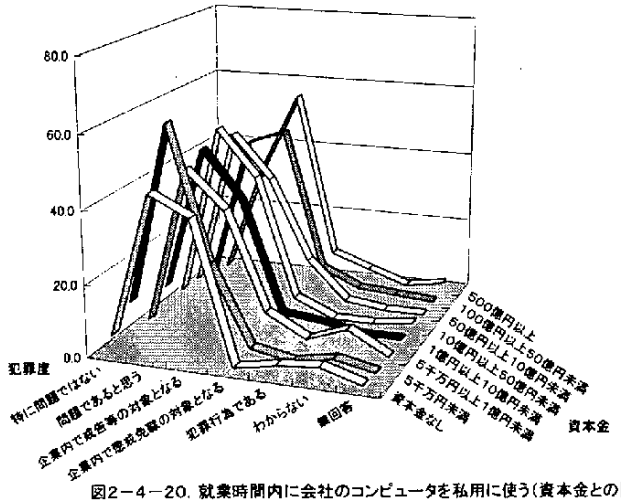


図2－4－20. 就業時間内に会社のコンピュータを私用に使う(資本金との関連)

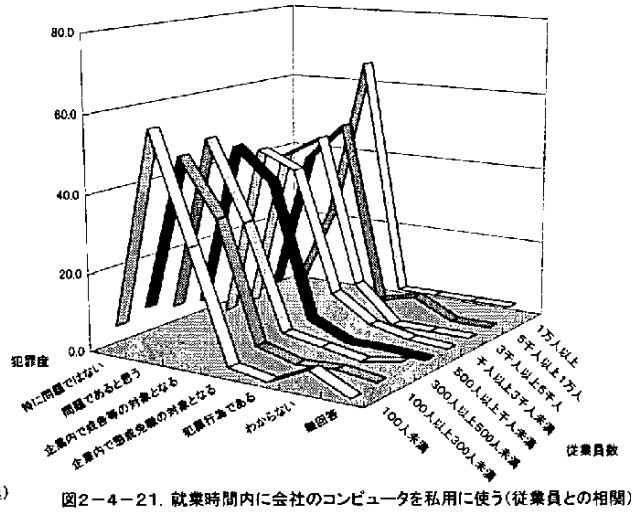


図2－4－21. 就業時間内に会社のコンピュータを私用に使う(従業員との相関)

犯罪度＼行為	他人のIDを無断借用する		業務上入手した顧客情報を正当な理由なしに第三者に売却する	
特に問題ではない	3	0.4	1	0.1
問題であると思う	119	16.6	13	1.8
企業内で戒告・訓告・注意処分等の対象となる	246	34.3	22	3.1
企業内で懲戒免職の対象となる	88	12.3	85	11.8
犯罪行為である(刑法上の処罰の対象となる)	247	34.4	571	79.5
わからない	8	1.1	15	2.1
無回答	7	1.0	11	1.5
計	718	100.0	718	100.0

他人のIDの無断使用に対しては事業体としては問題であり、犯罪行為であるとの見方が進んできている。特に、「犯罪行為である」については、前回調査の26.1%が34.3%となっており、犯罪行為であるとの考えが進んできているまだ、市販ソフトの不正コピーに対する認識と比べると、犯罪という認識は少ないように思われる。これは、企業ではグループで仕事をしていることが多く、緊急な場合などで他人のIDで仕事を行うなどの実態があり、問題があると認識しながらも犯罪という認識が低いものと考えられる。今後、企業も成果主義に変わりつつあり、従業員同士がライバルとなり、この問題は避けて通れないであろう。

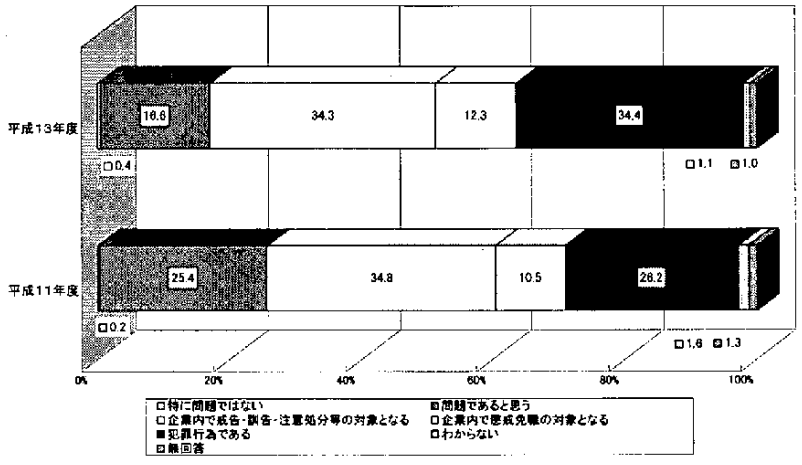


図2－4－22. 他人のIDを無断借用する

従業員数別にみると、従業員数1万人以上の事業体と100人以下の小規模のところで「犯罪行為」との意識が高いのに対し、中規模の事業体では、「企業内での戒告・訓告・注意処分等の対象」という見方が高くなっている。これは前回調査結果と比較すると相当意識度に変化がみられる。

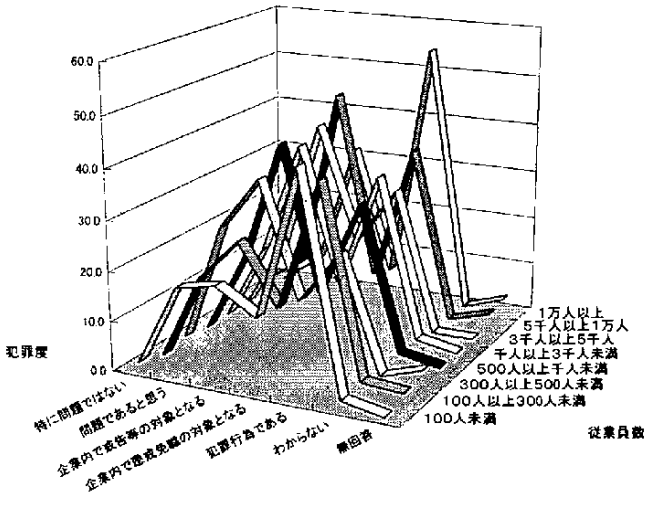


図2－4－23. 他人のIDを無断借用する(従業員数との関連－平成13年度)

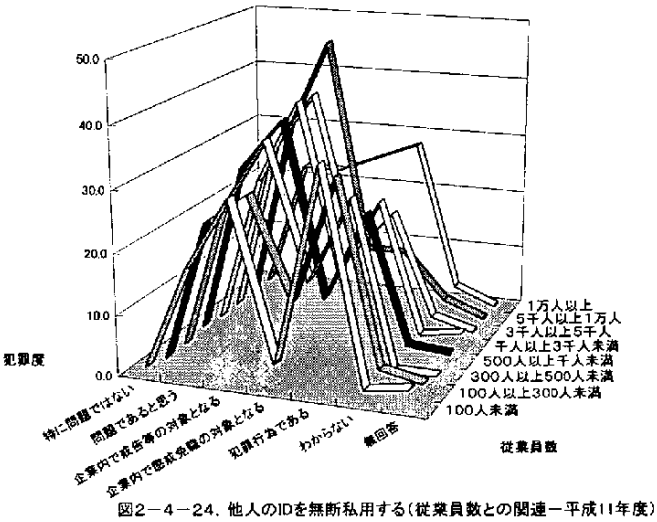


図2－4－24. 他人のIDを無断私用する(従業員数との関連－平成11年度)

平成 13 年度には、業務上入手した顧客情報を第三者に販売する事件や漏洩事件が多発した。また、個人情報保護法が検討されており、この問題に対する認識度合いは高い。とくに、前回調査では「犯罪行為である」が、84.7%であった。今回もこの傾向は同様であり、企業内の処分を含めると 90%以上が厳格な対応をすると答えている。今後、ネットワークでの情報共有が進むにつれてマーケティングで顧客情報がより重要となっている。しかし、ネットワーク社会では個人情報を保護することが国際的なコンセンサスとなっており、企業は今後、顧客情報のより徹底した管理が重要となる。プライバシーマークの利用を含め、積極的に取組むことが必要である。

業種グループ別との関係では、犯罪行為とみなす割合は、政府・地方公共団体（H11:93.3%→94.7%）、公共サービス業（H11:83.9%→86.3%）情報処理サービス業（H11：91.0%→83.8%）、金融・保険業（H11:87.9%→84.1%）と、他の業種と比べる高く厳しいものとなっている。

事業体規模（資本金、従業員数）の点では、小規模企業ほど犯罪とみなす比率が低い。今後、中小企業などに対して顧客情報の管理を徹底させることが必要であろう。電子商取引では、企業規模にかかわらず競争できる点がメリットであるが、企業規模によって管理がルーズであると、電子商取引自体の信用をなくすことにもつながりかねない。

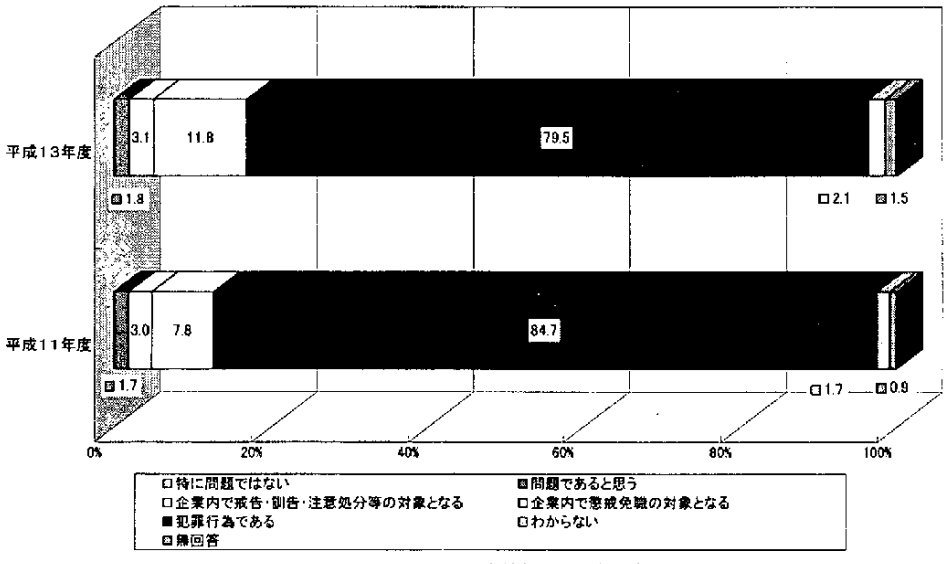


図2－4－25. 顧客情報を第三者に売却する

最後に、さまざまなコンピュータ利用での犯罪の認識度合いを比較してみた。すなわち、Q25 の各質問項目を「犯罪行為である」、「企業内で懲戒免職の対象となる」、「企業内で戒告・訓告・注意処分等の対象となる」の順に比較した。

この結果では、『業務上入手した顧客情報を正当な理由なしに第三者に売却する』行為が、最も「犯罪」としての認識度合いが高く、79.5%となる。次いで、『他人の ID を無断借用する』が 30%を越えており、いずれも、「犯罪」、「懲戒免職の対象」との認識が高い。一方、『WWW を個人目的で使用する』、『私用の電子メールを送・受信する』、『就業時間内でコンピュータを私用に使う』については、「犯罪」行為との認識は少なく、「問

題である」、「企業内で戒告・訓告・注意処分等の対象」程度の認識はありつつも、犯罪との認識は低い。業務上において「コンピュータを使っている」というモラルの向上が望まれる。経営者層側も今後情報化を進めていくなかで、従業員に対するこれらの点での教育によるモラル向上を図っていく必要があると考えられる。

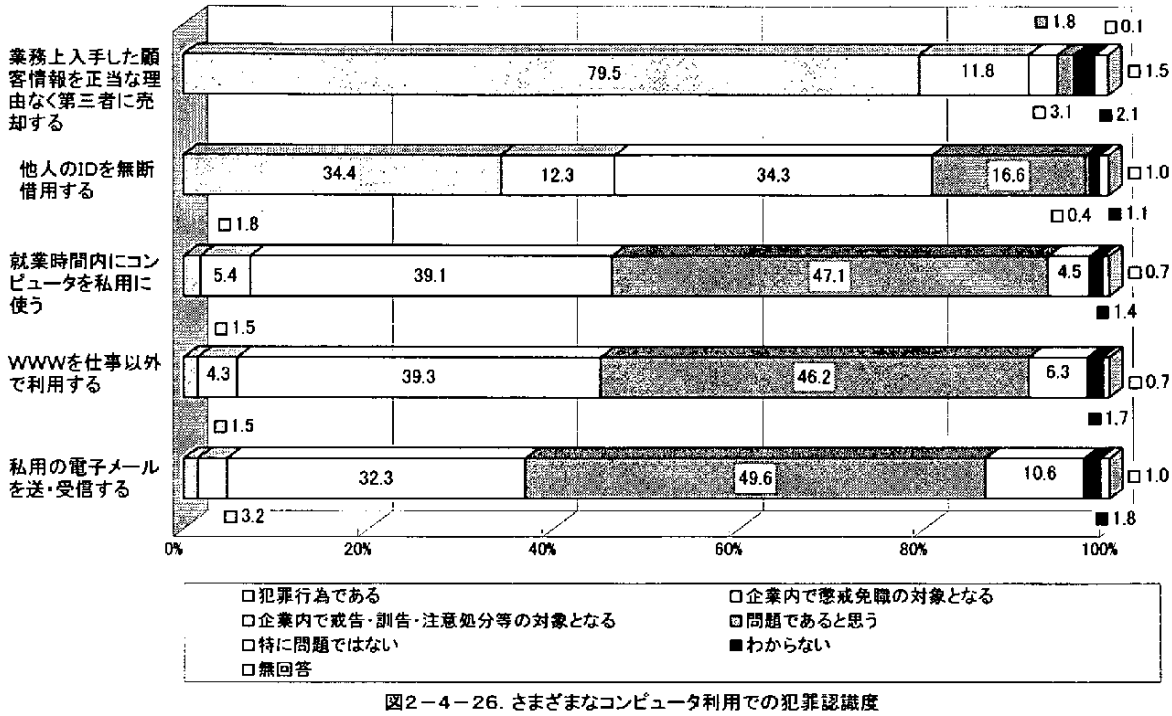


図2－4－26. さまざまなコンピュータ利用での犯罪認識度

2.5 災害対策・障害対策について

Q26. 情報セキュリティポリシー、実施手続・規程類に基づき災害・障害対策が明確にされていますか。

1	情報セキュリティポリシーや実施手続・規程類の中で明確になっている	137	19.1
2	他の基準で扱っている	188	26.2
3	特に定めていない(情報セキュリティポリシーがない場合も含む)	385	53.6
無回答		8	1.1
計		718	100.0

災害、障害手続に関する新規の設問であり情報セキュリティポリシーの重要性、有用性について確認する目的のものである。全体数値からは情報セキュリティポリシーがあらゆる基準、規定の基礎として定着するにはまだかなりの時間を要すると判断される。全体数値からさらに気になることは手続、規定を定めるにあたって基本となるべき方針は“特に定められていない”ことである。つまり現在ほとんどの事業体で災害、障害に関する手続、規定は特別な基本思想、方針なくして作られているということである。従来はそれでもよかったが、万一の事態おける社会に対するアカウンタビリティが問われる時代にあっては基本思想の表明が重要となる。情報セキュリティポリシーに基づいて再度見直しを行うことが強調される必要がある。

Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。

1	作成している		196	27.3
2	作成中である		102	14.2
3	作成を含め検討中である	⇒Q29 へ	149	20.8
4	作成していない		261	36.4
5	必要ない		6	0.8
無回答			4	0.6
計			718	100.0

前回調査と比べ、「作成している・作成中である」(41.5%) と「作成していない」(36.4%) の比率が微妙に変化している。

40%を境にしたこの変化を無視できるものかどうかに議論はあるが、母集団が小さいこと、サイバーテロその他テロ的行為の増加傾向、東海大地震の見直し等の環境変化を考えれば減少傾向として問題にすべきであろう。

業種グループ別にみると、金融・保険業でのマニュアル作成状況は 87.8% (「作成中」を含む) と高いことは好ましいことであり、また当然である。一方、「作成していない」比率が商業(49.4%)、公共サービス業 (56.9%) で特に高いことは母集団が小さいことを考慮しても憂慮すべきことと言える。実情把握のためさらに精査が必要である。

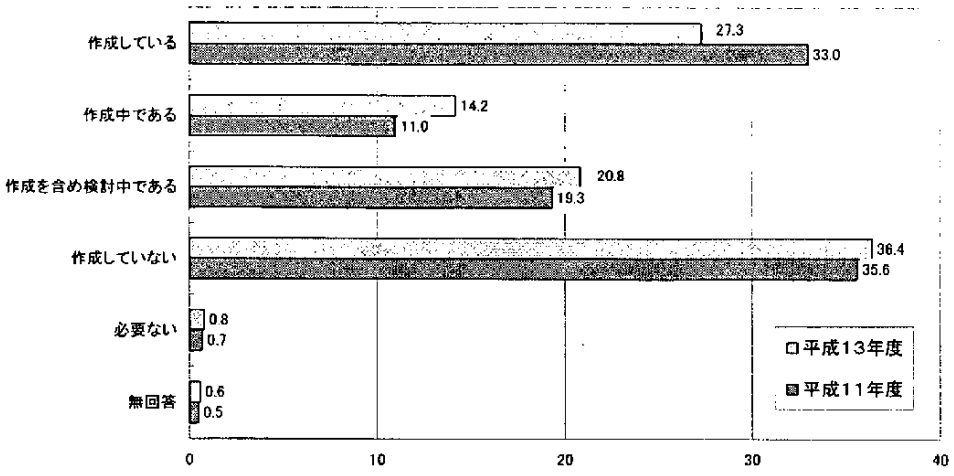


図2－5－1. 危機管理マニュアルの作成状況

28. （Q27 の）危機管理マニュアルには以下の項目を含んでいますか。含まれている項目を選んで下さい。（複数回答）

回答件数		298	
1	サイバーテロ	35	11.7
2	ネットワークセキュリティ上の緊急事態	136	45.6
3	事故・災害（火災、地震、風水害等）	258	86.6
4	障害（機械故障、回線障害等）	234	78.5
5	プログラムミス、オペレーションミス等のシステムの誤り	133	44.6
6	その他	9	3.0
無回答		8	2.7

ここでのパーセンテージは質問項目間の比率ではなく、Q27 の有効回答件数のうち、何％が当該項目を取り上げているかの比率である。質問の定義が明瞭でなかったきらいがあるものの数字から判断する限り、危機管理マニュアルとしては防災災害が中心であり、項目としてサイバーテロ（ウイルス、ハッカーによる緊急対応も含む）を取り上げているところは少なく、11.7％という低い結果となった。おそらく「プログラムミス、オペレーションミス等のシステムの誤り」に含まれているとも考えられる（金融・保険業においてもサイバーテロはほとんどとりあげられていない）が、災害、障害項目とそれ以外の項目の数字にこれだけ大きな隔たりがあるのは情報セキュリティは危機管理マニュアルとは別物と認識されていることによるものであろう。

この認識はリスクマネジメントという包括的なリスク認識に立つ新たな時代においては妥当ではない。あらゆる危機を含む全社的な危機管理マニュアルにはこれらの項目が一切含められるべきである。

Q29. 非常事態に備えて従業員に対して情報セキュリティの面から訓練を実施していますか。

1	定期的に実施している	43	6.0
2	時々実施している	77	10.7
3	特に実施していない	593	82.6
無回答		5	0.7
計		718	100.0

前回調査同様の結果で情報セキュリティとしての緊急事態対応訓練はわずかに実施されているだけで、ほとんど実施されていない。これはQ28に通じるもので、情報セキュリティにおける危機認識が防災、災害などとは別扱いとしており、したがってサイバー危機訓練も俎上に上がらないと考えられる。前回調査でのコメントとしてあげた「サイバーセキュリティ時代の重要な検討課題の一つとして取り上げるべき」の具現化の手立てができていないことを意味する。

業種グループ別にみても、金融・保険業、情報処理サービス業が多少訓練を実施していると考えられるが、ほとんどの業種で訓練は行われていない。情報セキュリティの危機対応にはかなり遅れをとっていることは明白である。

Q30. 情報システムの災害に対する復旧対策としてどのようなことを実施していますか。実施している対策を選んで下さい。(複数回答)

回答件数		718	
1	手作業への復帰(緊急時の手作業マニュアルが作成されている場合に限る)	211	29.4
2	同種コンピュータのユーザと相互バックアップ契約を交わしている	18	2.5
3	バックアップサービス業者と契約を交わしている	53	7.4
4	別の場所にバックアップセンタを設置している	66	9.2
5	ネットワークのバックアップを行っている	260	36.2
6	サーバのバックアップ用ファイルを専門保管業者に依頼して保管している	145	20.2
7	サーバのバックアップ用ファイルを遠隔地の自社施設に保管している	136	18.9
8	サーバのファイルは、遠隔地にミラーファイルを持っている	34	4.7
9	PC中の業務用ファイルは、バックアップを取っている	396	55.2
10	PC中の業務用ファイルのバックアップは、遠隔地に保管している	19	2.6
11	その他	35	4.9
12	特に対策を講じていない ⇒Q31へ	60	8.4
無回答		4	0.6

今回は分析方法を単純化し、回答件数のうち何パーセントがそれぞれのバックアップ方法をとっているか、それによって方法の普遍度を検証したものである。

全体的にまだバックアアップの意識が高いとはいえない。「PC 中の業務用ファイルはバックアップを取っている」(55.2%) が最も高く、これに次いで「ネットワークのバックアップ」(36.2%)、「手作業への復帰 (つまりシステムによるバックアップがない)」は 29.4%である。サーバのバックアップについては、43.8%が何等か対策を行っているが、遠隔地でミラーファイルを持っている事業体はほとんどない (4.7%)。ただし母集団が極端に小さい (34 件) ためパーセンテージの数値は問題とならないが、金融・保険業においてもこの傾向は変わらず、わずか 2.4%である。「別な場所にバックアアップセンタを設置している」が 9.2%ということは注目に値するが、サーバその他のファイルに関し、自組織外でのバックアップは少ない。

その他の意見としては、「必要に応じてバックアップ実施」、「バックアップファイルを耐火金庫で保管」等があげられた。

Q31. 対策を講じない理由は何ですか。主な理由を1つだけ選んで下さい。

1	経営者層の理解が得られない	4	6.7
2	コストがかかりすぎる	28	46.7
3	必要性を感じていない	13	21.7
4	満足する対策がない	6	10.0
5	その他	6	10.0
無回答		3	5.0
計		60	100.0

母集団が小さいので厳密なことは言えないが、バックアップを取り入れない理由の傾向は把握できる。今回、回答項目として新たに「経営者の理解が得られない」を加えたが、この比率は意外に低かった。そして前回調査同様、「コストがかかりすぎる」が大半の理由である（46.7%）。気になることは「必要性を感じていない」（21.7%）の比率が前回（13.6%）よりもかなり高くなっている点であるが、母集団が前回の有効回答数221件に対し、今回わずか60件であることから比率の意味はあまり大きなものではないと考える。

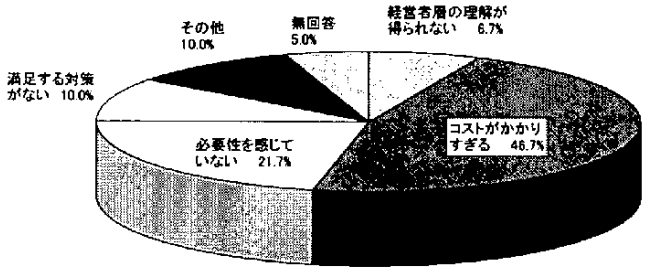


図2－5－2. 情報システムの災害対策を講じない理由

Q32. 情報システムの障害対策として次の機能を設けていますか。現在設置している機能を選んで下さい。（複数回答）

回答件数		718	
1	デュアルシステム	47	6.5
2	デュプレックスシステム	49	6.8
3	ホットスタンバイシステム	118	16.4
4	コールドスタンバイシステム	106	14.8
5	クラスタリング	87	12.1
6	高可用性機構	52	7.2
7	ミラリング	305	42.5
8	フォールトトレラント	41	5.7
9	特に設けていない ⇒Q33へ	203	28.3
無回答		24	3.3

注）基幹システムがメインフレームの場合は、1～4を、クライアントサーバシステムの場合は5～8から選択。

情報システムの障害対策として、「特に設けていない」は（28.3%）で、前回調査（46.3%）からみると18ポイント減少している。とはいえ、各事業体にとって情報システムの障害対策は関心

の高いものの一つであると考えられるが、障害対策機能を特に設けていない事業体が４分の１強と、高いポイントを占めている。

業種別に「特に設けていない」の回答率をみると次のようになる。

第二次産業	34.9%
第三次産業	23.4%
政府・地方公共団体	26.3%

また、設置している機能として、ミラリングが42.5%と最も高く、ホットスタンバイシステム（16.4%）、コールドスタンバイシステム（14.8%）が続いている。

これは、基幹システムがメインフレームの場合はホットスタンバイシステム、コールドスタンバイシステムのポイントが高く、クライアントサーバシステムの場合は、ミラリングのポイントが高いことを示している。

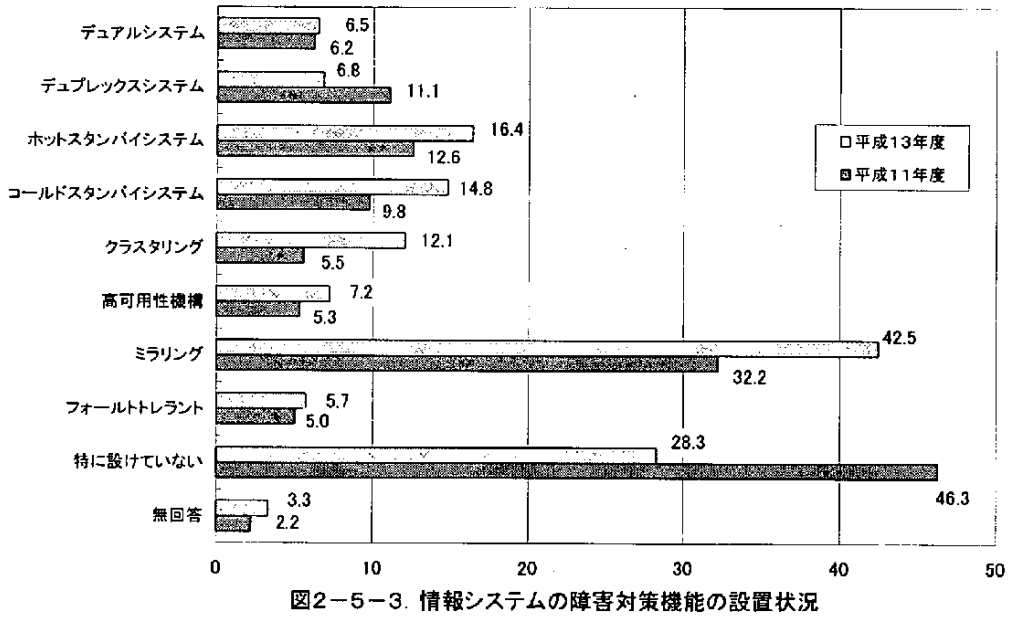


図2－5－3. 情報システムの障害対策機能の設置状況

Q33.（Q32で）対策を講じない理由は何ですか。主な理由を<u>１つだけ</u>選んで下さい。

1	経営者層の理解が得られない	4	2.0
2	コストがかかりすぎる	133	65.5
3	必要性を感じていない	37	18.2
4	満足するもの(機能)がない	10	4.9
5	その他	10	4.9
無回答		9	4.4
計		203	100.0

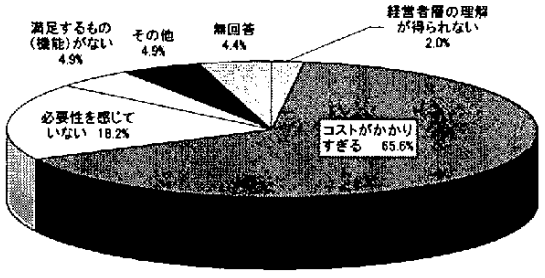


図2－5－4. 情報システムの障害対策を講じない理由

対策を講じない理由としては「コストがかかりすぎる」（65.5%）が最も多く、かなりの差があるが「必要性を感じていない」（18.2%）が続いている。業種別、企業規模（資本金別、従業員数別）、年間総費用別にみても、「コストがかかりすぎる」を第一の理由としている傾向は変わらない。

Q34. コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所ではそれぞれどのような火災対策をとっていますか。各場所ごとに実施している対策を選んで下さい。（複数回答）

回答件数 718	コンピュータ室		データ保管場所		ネットワーク設備室		コンピュータ設置場所	
自動火災報知設備を設置している	531	74.0	441	61.4	436	60.7	453	63.1
ハロン消火設備を設置している	361	50.3	247	34.4	227	31.6	210	29.2
CO_2消火設備を設置している	106	14.8	73	10.2	81	11.3	85	11.8
スプリンクラ消火設備を設置している	100	13.9	82	11.4	85	11.8	122	17.0
排煙設備を設置している	175	24.4	130	18.1	134	18.7	143	19.9
耐火金庫を設置している	118	16.4	264	36.8	39	5.4	42	5.8
消火・排煙等の防災機器の点検を定期的に行っている	418	58.2	344	47.9	337	46.9	337	46.9
その他	11	1.5	9	1.3	8	1.1	8	1.1
特に対策を講じていない	62	8.6	113	15.7	174	24.2	139	19.4
無回答	12	1.7	12	1.7	12	1.7	12	1.7

コンピュータ室、データ保管場所、ネットワーク設置室、コンピュータ設置場所ともに設備面で火災対策として最も多いのは、「自動火災報知器の設置」、次いで「ハロン消火設備の設置」であるが、データ保管場所については、「ハロン消火設備の設置」より「耐火金庫の設置」が多くなっている。また、「特に対策を講じていない」はコンピュータ室（8.6%）が最も低く、データ保管室（15.7%）、ネットワーク設備室（24.2%）、コンピュータ設置場所（19.4%）は高いポイントとなっており、コンピュータ室重視の傾向があるようだ。

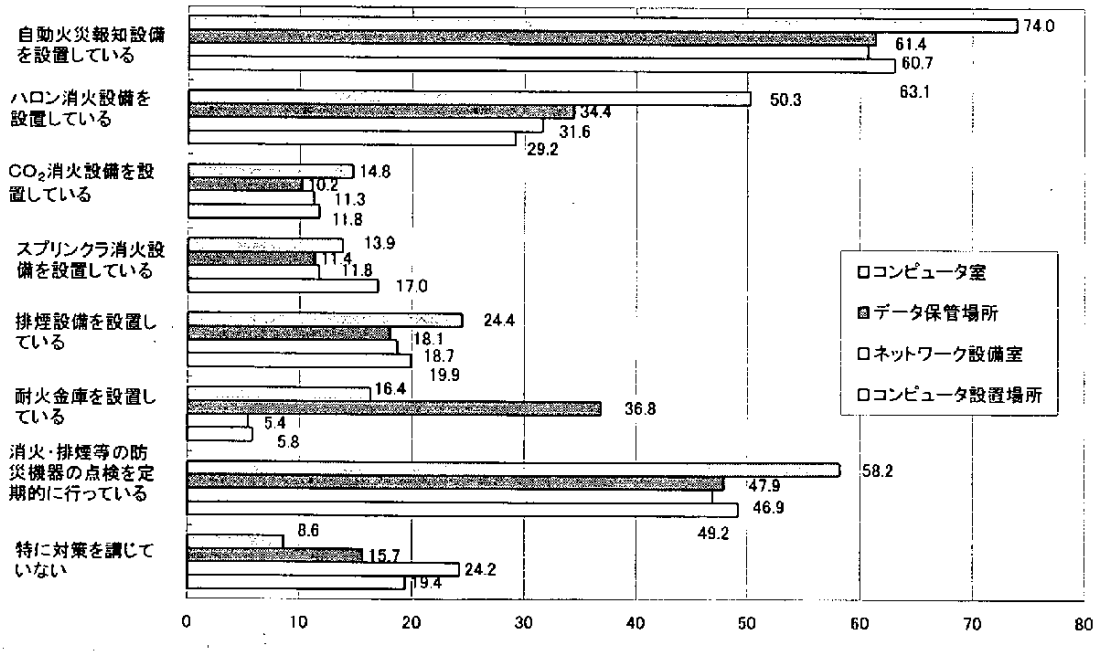


図2－5－5. コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所の火災対策

「特に対策を講じていない」は前回調査よりもすべてポイントは高くなっているが、「消火・排煙等の防災機器の点検を定期的に行っている」も前回調査よりもすべてポイントが高くなっている。火災対策について関心の高い事業体と、あまり高くない事業体の差が開きつつあるようだ。

Q35. コンピュータ室、データ保管場所、コンピュータ設置場所ではどのような地震対策をとっていますか。各場所ごとに実施している対策を選んで下さい。(複数回答)

回答件数 718	コンピュータ室		データ保管場所		コンピュータ設置場所	
建物が免震構造になっている	166	23.1	139	19.4	131	18.2
転倒防止措置を講じている	313	43.6	215	29.9	221	30.8
機器の移動防止措置を講じている	225	31.3	141	19.6	147	20.5
フリーアクセス床は耐震構造としている	244	34.0	128	17.8	149	20.8
媒体の落下防止措置を講じている	119	16.6	136	18.9	81	11.3
その他	8	1.1	9	1.3	10	1.4
特に対策を講じていない	242	33.7	351	48.9	351	48.9
無回答	19	2.6	19	2.6	19	2.6

地震対策としては、コンピュータ室、データ保管場所、コンピュータ設置場所とも、「転倒防止措置」を講じている事業体が多い。

地震対策としての各項目(「その他」以外の項目)はそれぞれ高いポイントを示している。

一方、「対策を講じていない」事業体は、コンピュータ室(33.7%)、データ保管場所(48.9%)、コンピュータ設置場所(48.9%)といずれも多く、火災対策から比べると地震対策はまだまだである。

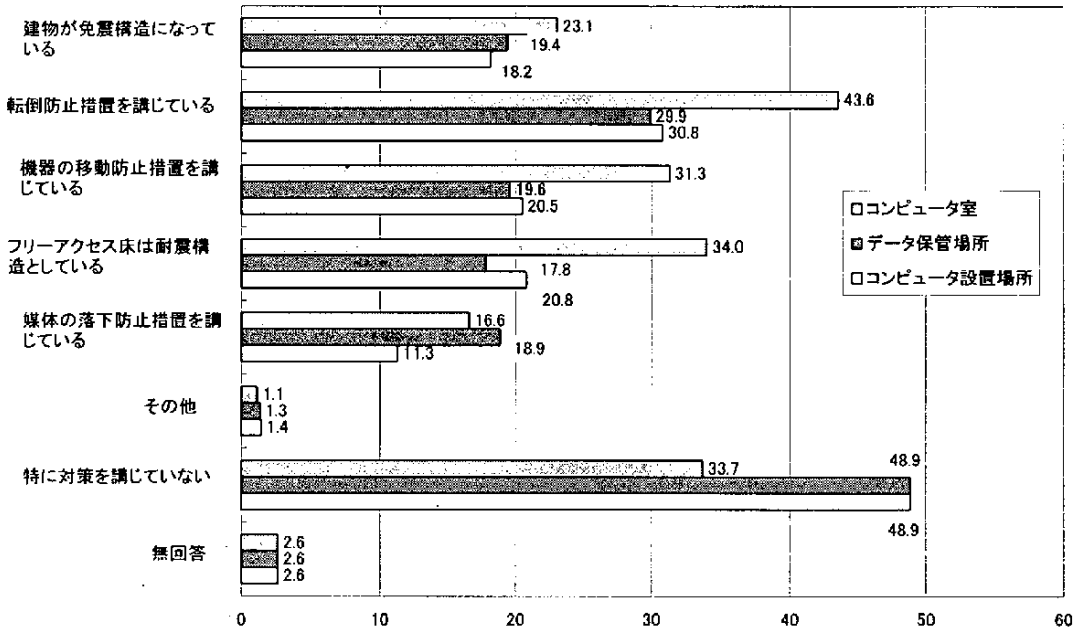


図2−5−6. コンピュータ室、データ保管場所、コンピュータ設置場所の地震対策

「対策を講じていない」を産業別にみると次のようになる。

	コンピュータ室	データ保管場所	コンピュータ設置場所
第二次産業	41.6%	60.1%	57.7%
第三次産業	29.2%	42.6%	44.2%
政府・地方公共団体	15.8%	23.7%	26.3%

大規模な地震が各地で起こっているが、火災ほど身近には感じられていないようだ。

Q36. 電源設備の災害対策として、どのような対策をとっていますか。実施している対策を選んで下さい。(複数回答)

回答件数		718	
1	AVR	56	7.8
2	CVCF／UPS	577	80.4
3	自家発電装置	219	30.5
4	電力供給経路の複数化	107	14.9
5	その他	9	1.3
6	特に対策を講じていない	76	10.6
無回答		10	1.4

電源設備の災害対策としては、前回調査と同様、「CVCF/UPS が使われている」(80.4%)が多く、前回調査の(76.7%)より 3.7 ポイント増加している。

また、「対策を講じていない」事業体は前回調査(13.8%)から比べると 3.2 ポイント減少して 10.6%となっている。

今回初めて「電力供給経路の複数化」について調査したが、14.9%であった。「電力供給経路の複数化」を産業別にみると次のようになる。

第二次産業	11.1%
第三次産業	18.4%
政府・地方公共団体	10.5%

電源設備の災害対策の必要性は高まりつつある。

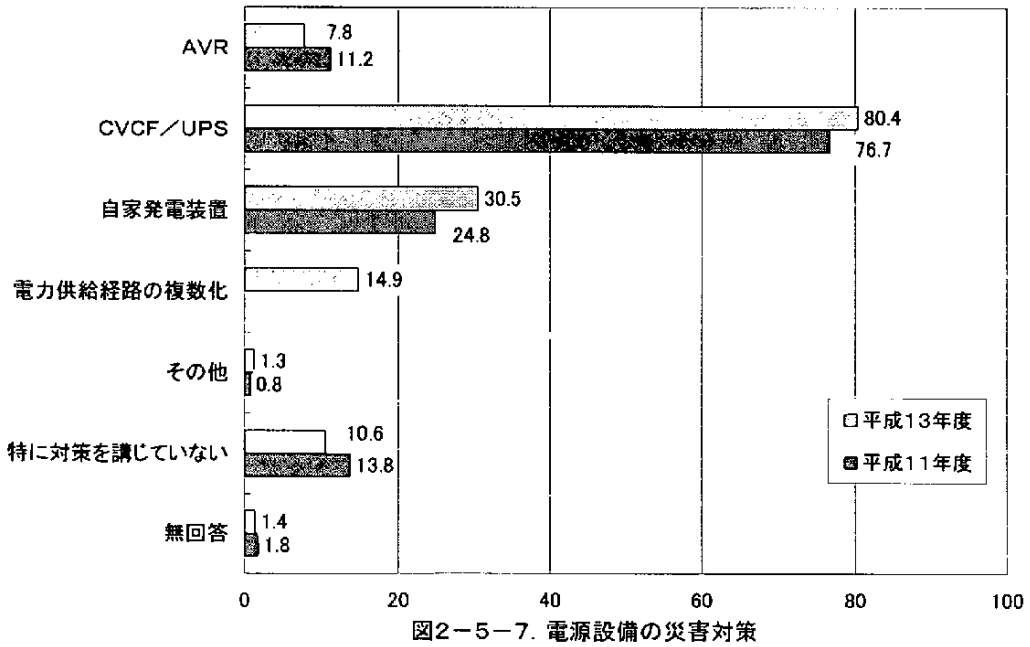


図2－5－7. 電源設備の災害対策

Q37. 水冷の空調設備を使っている場合、空調用の水は何日分確保していますか。

1	1日分～3日分	51	7.1
2	4日分～6日分	15	2.1
3	7日分以上	39	5.4
4	まったく確保していない	70	9.7
5	水冷の空調設備を使用していない	347	48.3
無回答		196	27.3
計		'718	100.0

今回初めて行った調査である。

水冷の空調設備を使用している施設で何らかの災害が発生した場合、電源設備の予備が完備していても、水冷用の水が供給されなければコンピュータを作動させることはできない。

「まったく確保していない」(9.7%) はポイントとしては少し高い。情報システムの年間総費用が 30 億円未満の事業体でポイントが高く、30 億円以上の事業体ではポイントが低い。

特に情報システムの年間総費用が 100 億円以上の事業体では、7 日分以上の確保が 33.3%と高いポイントを示している。

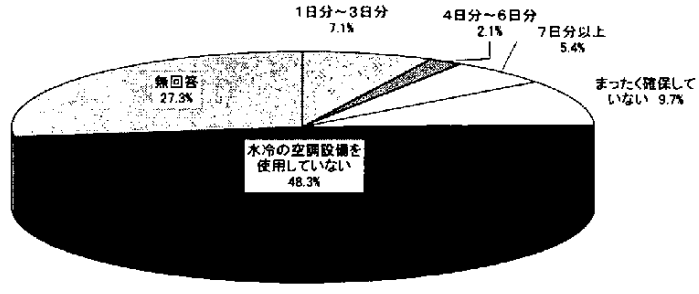


図2－5－8. 水冷空調設備用の水の確保について

Q38. 情報システム、ネットワーク室、機器の災害・障害等で今後強化しなければならないと思うものは何ですか。(複数回答)

回答件数		718	
1	自然災害	217	30.2
2	電源障害	240	33.4
3	空調等障害	82	11.4
4	回線障害	341	47.5
5	ハードウェア障害	270	37.6
6	OS障害	110	15.3
7	ソフトウェア障害	166	23.1
8	火災による事故・障害	150	20.9
9	人の悪意による事故等	263	36.6
10	オペミス等、人の過失による事故等	212	29.5
11	テロによる機器の運用停止(DDOS:DOSアタックを含む)	197	27.4
12	取引先システムの停止や異常処理	64	8.9
無回答		17	2.4

「回線障害」（47.5％）が最も高く、「ハードウェア障害」（37.6％）、「人の悪意による事故等」（36.6％）と続いている。

高度情報化に伴い、今後、回線トラブル、コンピュータ犯罪などの対策に力を入れていこうとする傾向がみられる。

特に、「テロによる機器の運用停止（DDOS：DOSアタックを含む）」が27.4％であることは、最近の社会情勢が影響しているものと考えられる。

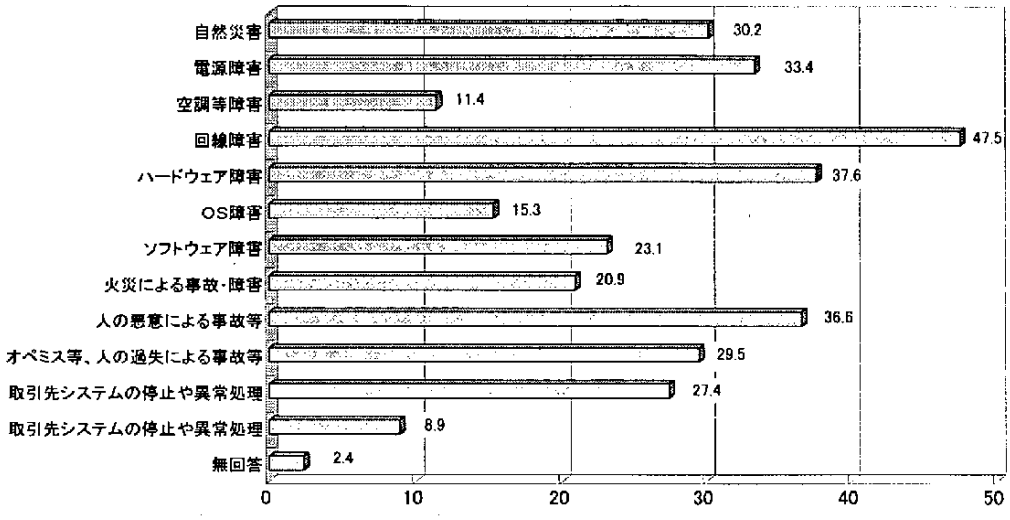


図2－5－9. 情報システム、ネットワーク室、機器の災害対策で強化すべき点

Q39. システム災害・障害対策についての問題点は何ですか。（複数回答）

回答件数		718	
1	経営者層の理解が得られない	86	12.0
2	コストがかかりすぎる	518	72.1
3	要員に対する教育訓練がいきとどかない	167	23.3
4	要員に対して負担がかかりすぎる	172	24.0
5	ノウハウが不足している	228	31.8
6	どこまでやれば良いのか基準が示されていない	277	38.6
7	要求に合致するもの(製品)がない	16	2.2
8	その他	6	0.8
9	特に問題はない	26	3.6
無回答		14	1.9

システム災害・障害対策の問題は、やはり「コストがかかりすぎる」（72.1％）となっている。前回調査（80.6％）からみると、8.5ポイント減少しているが、システム災害・障害対策はどこまでやればよいのか、基本線を設定することが難しく、その悩みが浮き彫りにされている。

「経営者層の理解が得られない」（12.0％）も前回調査（9.3％）と比べ、2.7ポイント増加している。

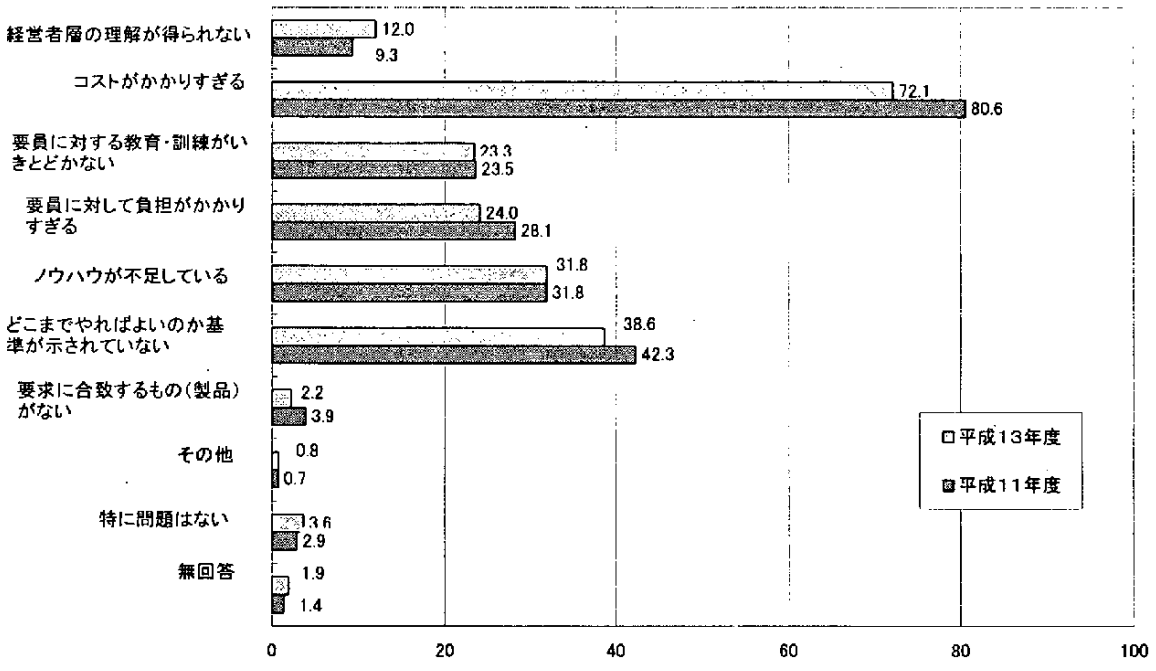


図2－5－10. システム災害・障害対策の問題点

Q40. どのようなネットワーク機器、サービスの障害を想定していますか。(複数回答)

回答件数		718	
1	通信事業者のケーブル障害(含む、専用回線)	326	45.4
2	通信事業者の設備障害	249	34.7
3	通信事業者のサービス(電話、パケット交換など)中断・サービス低下、停止	252	35.1
4	ISP(インターネットサービスプロバイダ)サービスの中断・停止	146	20.3
5	LAN(配線)の障害	463	64.5
6	ルータ・サーバ(機器)の障害	536	74.7
7	地震などの一定地域の災害	217	30.2
8	その他	1	0.1
9	特に想定していない	46	6.4
無回答		15	2.1

ネットワーク機器サービスの障害として想定しているのは「ルータ・サーバ機器の障害」(74.7%)が最も高いポイントであり、次に「LAN(配線)障害」(64.5%)がこれに続いている。いずれも自事業体内での障害を中心とした想定である。

通信業者関連の障害もかなり高いポイントではあるが、意識としては自事業体内の障害をまず念頭に置いている。

また、「地震などの一定地域の災害」(30.2%)もかなり高いポイントを示している。地域災害との関連も無視できない要素となっているのであろう。

最後に「特に想定していない」は 6.4%と低い結果となっており、障害に対する関心は全体的に高いといえるであろう。

業種別にみると、各業種とも共通した結果となった。

Q41. どのようなネットワーク障害対策を実施していますか。実施している対策を選んで下さい。
(複数回答)

回答件数		718	
1	異なる種別回線を利用	152	21.2
2	異なる交換局への収容	41	5.7
3	異なるコモンキャリアの利用	49	6.8
4	異なるISPを利用	36	5.0
5	異なるメディアによる回線利用(例:衛星回線等)	25	3.5
6	ポイント間接続から網接続へ	79	11.0
7	重要回線を部分的に二重化	185	25.8
8	専用のバックアップ回線を常時設定	128	17.8
9	専用回線とインターネットVPNなどの異種サービスの組み合わせ	60	8.4
10	社内の構内回線、LAN等を二重化	107	14.9
11	通信機器(CCU、ルータ、社外 WWW サーバ、DNS サーバ、アクセスサーバ等)の二重化	155	21.6
12	インターネットに接続したサーバの分散(負荷分散、地域分散)	69	9.6
13	その他	5	0.7
14	特に対策を講じていない	248	34.5
無回答		33	4.6

Q40 の障害の想定に関する調査では各事業体とも何らかの障害を想定しているものの、「特に対策を講じていない」(34.5%) と実際の対策に関してはあまり進んでいないようだ。

自事業体内での障害を想定している事業体が比較的多く、高いポイントを示している以上、やはり対策は自事業体内で必要なことを十分に実施する必要があるだろう。

ネットワーク障害対策としては、回線、通信機器等の二重化対策が高いポイントを示している。

重要回線を部分的に二重化	25.8
社内の構内回線、LAN等を二重化	14.9
通信機器(CCU、ルータ、社外 WWW サーバ、DNS サーバ、アクセスサーバ等)の二重化	21.6

「特に対策を講じていない」を業種別にみると、第二次産業 (43.3%) がこれに従っている。

2.6 不正アクセス対策・不正侵入対策について

Q42.「不正アクセス行為の禁止等に関する法律」（平成11年8月公布）を知っていますか。

1	知っている	551	76.7
2	知らない	158	22.0
無回答		9	1.3
計		718	100.0

前回の調査時点においては、「不正アクセス行為の禁止等に関する法律」の存在を「知っている」との回答は47.4%であったが、今回調査では76.7%となり、同法の認知度は大幅に高まった。

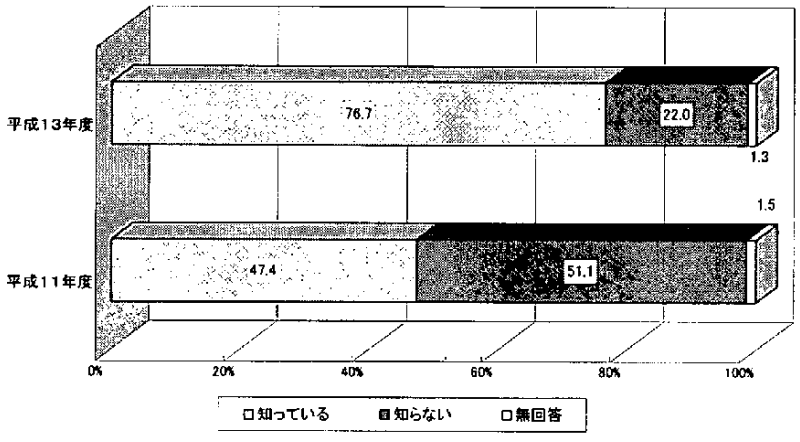


図2－6－1. 不正アクセス禁止法の認知度

Q43. 貴事業体では過去1年間に不正アクセスの被害に遇われたことがありますか。（複数回答）

回答件数		718	
1	物理的なアクセス被害（コンピュータ室等への侵入）に遭った	5	0.7
2	論理的アクセス被害（ネットワーク経由による侵入）に遭った	105	14.6
3	な い ⇒Q45へ	605	84.3
無回答		3	0.4

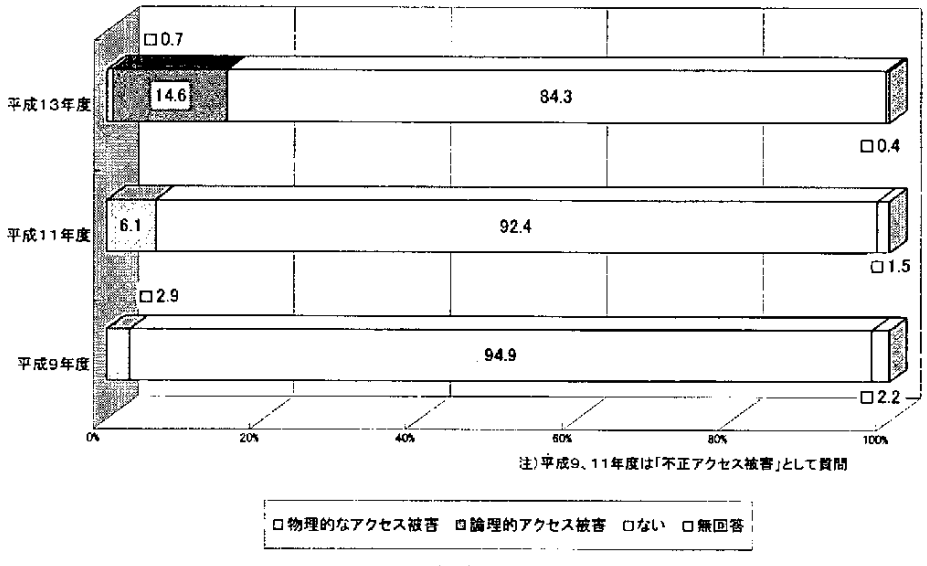


図2－6－2. 過去1年間の不正アクセス被害状況

大多数の組織体においては不正アクセスの被害は「ない」という結果が出ているが、平成９年度および前回調査と比較すると、2.9%から6.1%、さらに14.6%へと大幅に増加しており、インターネットの普及に伴うと思われる不正アクセス被害の増大がみられ、無視できない状況となってきている。

また、件数は５件と少数ではあるが、コンピュータ室等に侵入されたという物理的な被害が起きており、物理的な侵入対策も決して忘れてはならないことを警告している。

Q44. 不正アクセス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

1	出した	25	22.7
2	出さない	83	75.5
無回答		2	1.8
計		110	100.0

IPAに被害届を出す組織体は前回調査同様約２割にとどまり、やはり少数である。Q２においてIPAがコンピュータ不正アクセス被害の届出機関であることを「知っている」という回答が71.0%あることと比べると、非常に少ない回答率である。

Q45. ①主要なネットワーク室や機器、コンピュータ室またはデータ保管室での物理的な不正アクセス対策はどのようなものですか。現在実施している対策を選んで下さい。(複数回答)
②(Q43で「１」と答えた場合のみ)このうち、不正アクセスの**被害を契機として**実施した対策を選んで下さい。(複数回答)

不正アクセス対策	①実施対策		②不正アクセス被害後の対策	
回答件数	718		5	
不正アクセスを受けた場合の、IPAやJPCERT／CC(コンピュータ緊急対応センター)への相談	46	6.4	1	20.0
室の出入口で入室管理を行っている	325	45.3	1	20.0
室の出入口で退室管理を行っている	244	34.0	0	0.0
室への入退室についてカード、パスワードを使用している	271	37.7	0	0.0
入退室のときにアンチパスバック(定期券のように二度連続して入れないような仕組み)を持っている	37	5.2	0	0.0
室への入室について身体的特徴(指紋、虹彩等)による識別を行っている	38	5.3	0	0.0
室の管理責任者を定めている	357	49.7	0	0.0
情報システムの監視設備を設けている	131	18.2	0	0.0
定期的にリスク分析や情報セキュリティ監査を実施	74	10.3	0	0.0
その他	8	1.1	0	0.0
特に対策を講じていない	184	25.6	1	20.0
無回答	49	6.8	2	40.0

(注)データ保管室とは、データ、プログラム等を含む記録媒体およびドキュメントを保管する「独立した室」であり、室内に置かれるデータ保管庫は含みません。

物理的な不正アクセスに対する対策は、前回調査に比べてほとんど変動がない。約４～５割の事業体が「管理責任者の設置」、「入室管理」、「カード・パスワードの利用」を実施している。これは、メインフレームを設置していたデータセンターでは、物理的なアクセスに対するセキュリティを伝統的に確保してきたので、その施設を継続的に使用している事業体では、継続して物理的なセキュリティが確保され、サーバの設置場所として一般の事務室環境を選んだ企業では、物理的セキュリティにあまり着目しなかったためと考えられる。

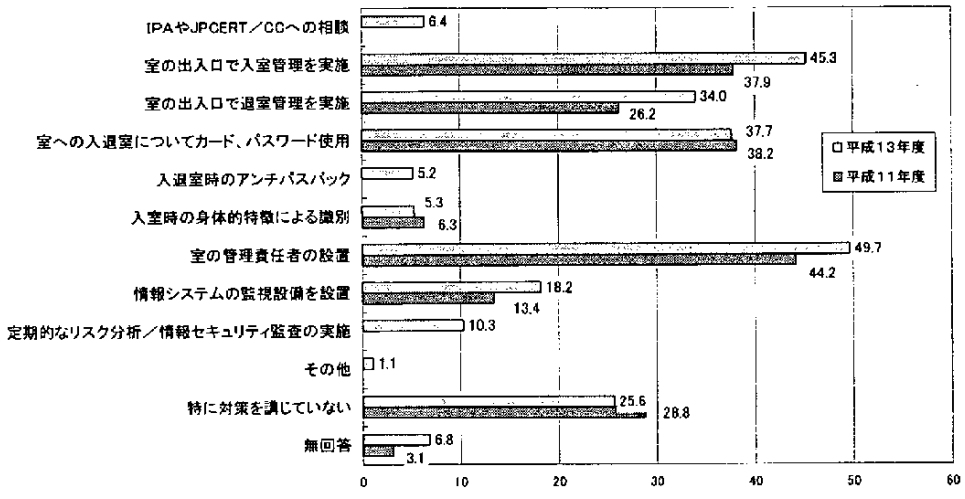


図2－6－3. 物理的不正アクセスの実施状況

Q46. ①ネットワークを介しての論理的な不正アクセスに対して講じている対策は何ですか。現在実施している対策を選んで下さい。(複数回答)
②(Q43 で「2」と答えた場合のみ)このうち、不正アクセスの被害を契機として実施した対策を選んで下さい。(複数回答)

不正アクセス対策	①実施対策		②不正アクセス被害後の対策	
回答件数	718		105	
不正アクセスを受けた場合の、IPAやJPCERT／CCへの相談	50	7.0	9	8.6
パスワードの活用	476	66.3	4	3.8
ファイアウォールの利用	496	69.1	11	10.5
アクセス制御ソフトウェアの使用	198	27.6	15	14.3
社外からのアクセスのために設置しているアクセスサーバへのアクセスにワンタイムパスワードや呼び返し接続等の追加的コントロールを実施	110	15.3	2	1.9
ネットワーク機器の運用者(アクセス範囲)を限定	352	49.0	4	3.8
情報セキュリティポリシーで勝手にLANの配線を触ったり、個人のPCを接続することを禁止	214	29.8	3	2.9
情報セキュリティ管理者がサーバやルータ、ファイアウォールのログを定期的にチェック	172	24.0	8	7.6
ネットワーク管理者がサーバやルータ、ファイアウォールのログを定期的にチェック	298	41.5	15	14.3
定期的にリスク分析や情報セキュリティ監査を実施	82	11.4	4	3.8
その他	18	2.5	8	7.6
特に対策を講じていない	72	10.0	5	4.8
無回答	38	5.3	56	53.3

ネットワークからの不正アクセスに講じている対策について、今回の調査と前回調査を比較すると、「パスワードの活用」が、83.4%から 66.3%と 17.1 ポイント低下している。現在のネットワーク環境を考えた場合、ユーザ ID とパスワードによる認証の実施率は、100%に達していると思われるので、回答者が質問の「活用」という言葉を厳密に解釈しすぎた結果ではないかと思われる。次に、「ファイアウォールの利用」については、50.7%から 69.1%と 18.4 ポイント増加した。これは、一連のホームページ改ざん事件の被害から、ファイアウォールの利用の重要性が認識されたためと考えられる。しかし、30.9%がファイアウォールを設置しておらず、インターネットとの接続を実施しているとしたら、セキュリティ上大きな問題である。ファイアウォールの利用は、インターネット接続の前提条件と考えるべきである。さらに、今後ブロードバンドの一般家庭や小規模事業者への普及と共に、こういったところが不正アクセスの被害の対象となることが考えられ、パーソナルファイアウォール等の対策が必要となる。

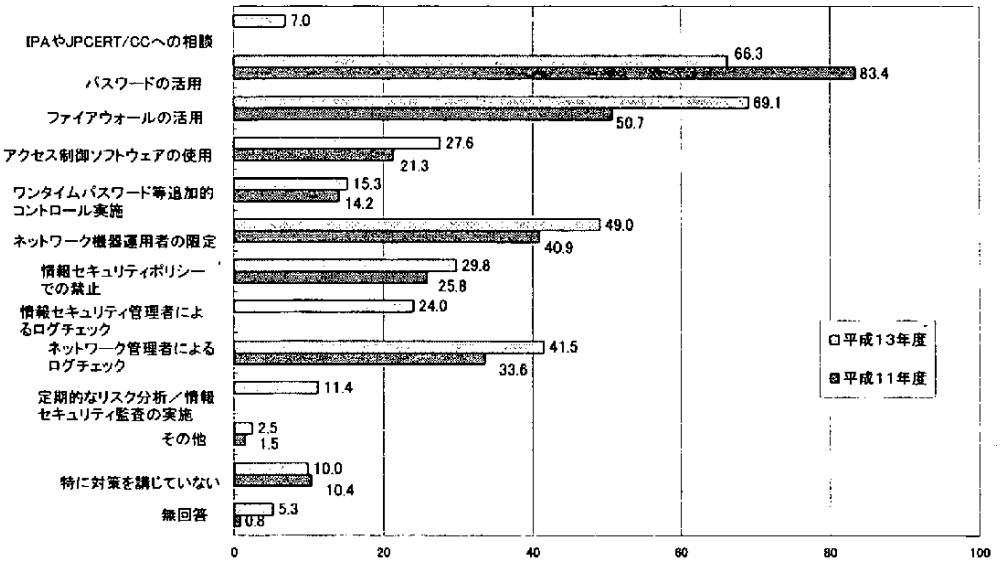


図2－6－4. 論理的不正アクセス対策の実施状況

業種別にファイアウォールの設置状況をみると、証券・商品取引業と保険業では 100%になっており、新聞・出版の 87.5%、電力・ガス事業の 83.3%が続いている。

社外からのアクセスに関しては、「ワンタイムパスワード」などの追加的コントロールが必要であるが、全業種とも取組み状況は進んでいない。今後、営業の情報化が進むなかで SFA(Sales Force Administration) の採用を行う組織体も増えてくると想定される。この場合には、「ワンタイムパスワード」などの利用が必須である。

「情報セキュリティポリシーで勝手に LAN の配線を触ったり、個人の PC を接続することを禁止」については、セキュリティポリシーを定めている事業体では、ほとんどが制限を含めていると考えられる。今後、セキュリティポリシーを定めるときに、アクセスや配線など LAN にかかわる事項は、必ず含むべき項目である。

「情報セキュリティ管理者やネットワーク管理者による定期的なログのチェック」は、それぞれ 24.0%、41.5%であり、前回調査でネットワーク管理者によるチェックが 33.6%だったのに比べて大きく向上している。特にファイアウォールの設置率が 69.1%であることを考えると、設置してある組織体では 6 割の企業がログの監視を実施していることになる。

Q47. 情報についての機密度のランクを設定していますか。

1	い る	204	28.4
2	いない	490	68.2
無回答		24	3.3
計		718	100.0

機密度のランクを「設定している」という割合は 28.4%であり、平成９年度（29.5%）、前回調査（26.5%）と比較するとほぼ横ばいとなっている。

今後、情報セキュリティポリシーを作成し導入する事業体が一般的とならなければ機密度のランクの設定は浸透しないと考えられる。

Q48. 貴事業体では基幹システムのパスワード変更をどのレベルに設定していますか。（単一回答）

1	ワンタイムパスワードを設定している	13	1.8
2	変更期限がきたらパスワードを無効にする	29	4.0
3	定期的に新しいパスワードを配布する	39	5.4
4	変更期限を定めて利用者が変更している	78	10.9
5	パスワードの変更を推奨しているが、変更期間は利用者に任せている	257	35.8
6	パスワードの変更に関して特に定めていない	213	29.7
7	パスワードによる管理を実施していない	56	7.8
8	その他	8	1.1
無回答		25	3.5
計		718	100.0

平成９年度、前回調査と質問構成を変更しているため一概にはいえないが、前回調査では「変更していない」が 45.1%であったが、今回は「パスワードの管理を実施していない」は 7.8%、「パスワードの変更に関して特に定めていない」が 29.7%であり、多少、パスワードへの認識は高まったと考えられる。

しかしながら、「パスワードの変更を推奨しているが、変更期間は利用者に任せている」が 35.8%となっており、前回の「本人の自由意思に任せる」（25.5%）と比べても、むしろ多くなっており、組織全体で最後まで徹底している状況には至っていない。なお、前回の「定期的に変更している」（17.8%）に該当する回答は「ワンタイムパスワードの設定」（1.8%）、「変更期限がきたらパスワードを無効にする」（4.0%）、「定期的に新しいパスワードの配布」（5.4%）、「変更期限を定めて利用者が変更」（10.9%）であるが、合計すると 22.1%であり、前回から 4.3 ポイント増加している。

パスワード管理は不正アクセス対策の中心であるため、なお一層の向上が求められる。

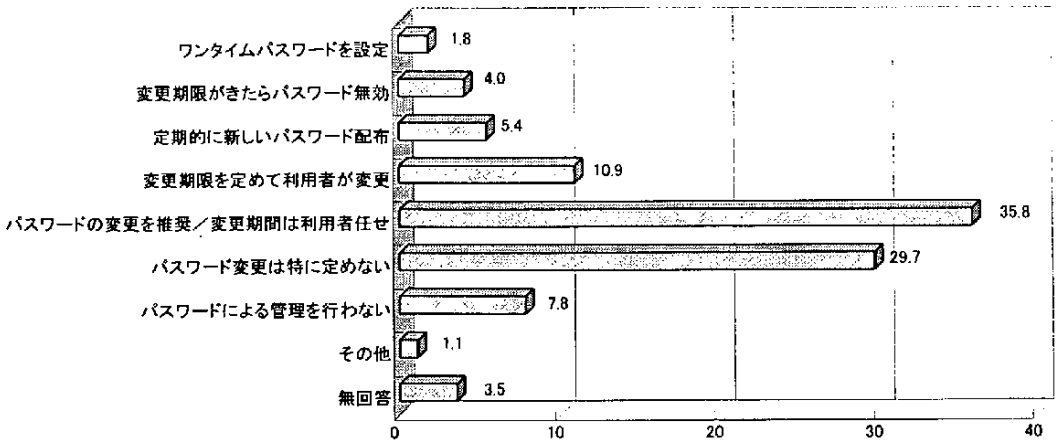


図2－6－5. 基幹システムのパスワード変更レベルの設定

Q49. 貴事業体では暗号を採用していますか。採用している暗号を選んで下さい。(複数回答)

回答件数		718	
1	暗号装置を購入	26	3.6
2	市販の暗号ソフトウェアを購入	91	12.7
3	自社で作成した暗号ソフトウェアを使用	22	3.1
4	利用しているアプリケーションに付随しているので、暗号機能を利用	91	12.7
5	その他	10	1.4
6	採用していない　⇒Q51へ	506	70.5
無回答		10	1.4

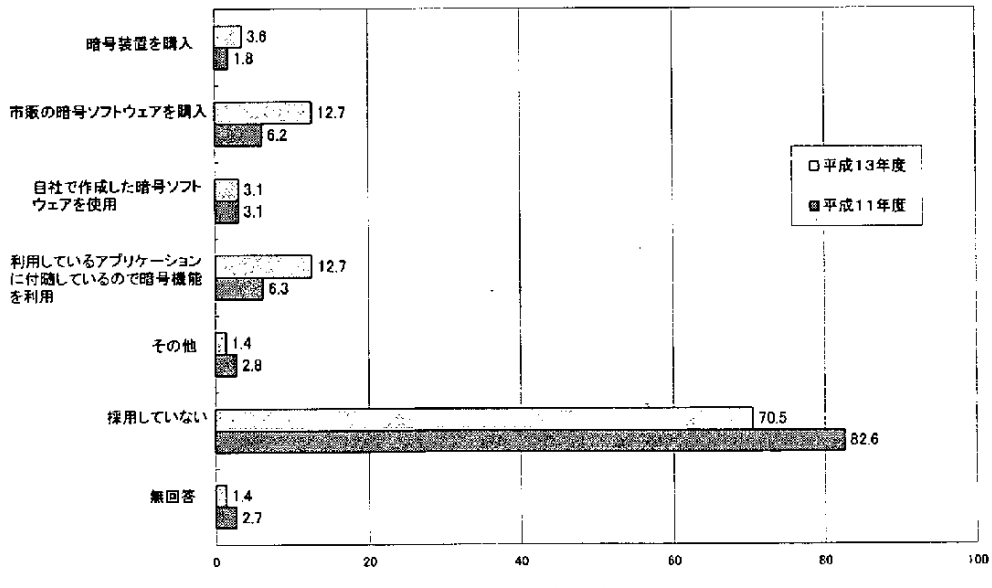


図2－6－6. 暗号の採用状況

暗号の採用について、前回調査では採用している事業体が 17.4％であったのに比べ、今回調査では 28.1％の事業体が採用しており、普及率が大きく向上した。この中には、インターネットのホームページでも SSL に対応したものが多くなっており、暗号ソフトウェアを導入したという意

識を持たずに、サーバーで暗号を利用しているユーザも多いことが予想される。ブラウザ側でも、ほとんどの利用者がSSLを使用しており、実際の暗号の普及率は高いことが予想される。(ホームバンキング等では、SSLが必須になっている。)

Q50. 暗号化している情報は次のどれですか。(複数回答)

回答件数		202	
1	伝送するデータすべて	26	12.9
2	伝送するデータのうち重要なもの(プログラムなど)	93	46.0
3	記録媒体上のデータすべて	1	0.5
4	記録媒体上の重要なもの(プログラムなど)	45	22.3
5	認証情報(署名)	48	23.8
6	重要なトランザクションデータ(カード番号などの)の転送に利用	39	19.3
7	その他	19	9.4
無回答		8	4.0

暗号化している情報の種類に関する質問であるが、前回調査では有効回答数が12件であったのに対し、今回は202件となった。回答数の増加は特筆すべきものであり、暗号が一般的になる兆しと考えられる。

暗号化を利用している情報を見ると、一番多かったのは「伝送するデータのうち重要なもの」(46.0%)であり、ディスク等の記憶媒体保管時の暗号化は、その半分程度であることがわかる。今後電子商取引の普及と共に、伝送されるデータの暗号化の利用は、SSLを中心に増えていくことが予想される。

Q51. ＰＫＩ(公開鍵基盤)について貴事業体はどのような方針をお持ちですか。

1	導入済み	47	6.5
2	導入を前提に評価中	111	15.5
3	検討の結果、当面導入の予定はない	46	6.4
4	検討していない	492	68.5
無回答		22	3.1
計		718	100.0

「電子署名及び認証業務に関する法律」が、平成13年4月より施行されたのに対応して、電子商取引を実際の業務に使うための法的な枠組みが整備された。これを実施するには、電子署名の仕組みが必要となるので、今後PKIの必要性は急速に高まることが予想される。現在は、評価中の事業体を含めて22%の組織がPKIに取り組んでいるが、現在検討していない68.5%の事業体は、早急に検討を進めるべきである。

Q52. 貴事業体では不正アクセス対策について従業員に教育・訓練の場を設けていますか。

1	情報セキュリティ教育に関して定期的に実施している	24	3.3
2	社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している	57	7.9
3	情報セキュリティポリシーや対策基準類に従って実施している	80	11.1
4	その他	38	5.3
5	特に実施していない	501	69.8
無回答		18	2.5
計		718	100.0

不正アクセスに対する教育・訓練については27.6%の事業体が何らかの形で行っており、前回調査で16.5%だったのに比べると大幅に上昇している。しかし、セキュリティに関しては、技術的な対策だけでは不十分であり、従業員のセキュリティリテラシーを高める方が、効果的でありかつ投資も少ないことから、投資効率としては一番良い対策といわれている。この視点からは27.6%という数字は依然過小であり、実施していない事業体は早急に検討を開始すべきである。

その他の意見としては、「入社時の研修時に」、「社内ホームページ、掲示板、電子メール等での情報提供・注意喚起」等があげられた。

Q53. 不正アクセス対策についての問題点は何ですか。(複数回答)

回答件数		718	
1	経営者層の理解が得られない	75	10.4
2	コストがかかりすぎる	352	49.0
3	不正アクセス侵害事件や対策に関するタイムリーな情報収集ができていない	126	17.5
4	組織の従業員に対する教育訓練がいきとどかない	289	40.3
5	組織の従業員に対する負担がかかりすぎる	126	17.5
6	ノウハウが不足している	305	42.5
7	どこまでやれば良いのか基準が示されていない	249	34.7
8	要求に合致するもの(製品)がない	21	2.9
9	その他	11	1.5
10	特に問題はない	46	6.4
無回答		20	2.8

不正アクセス対策に関しては、90.8%以上の回答者が何らかの問題点を指摘している。主要な問題点としては、「コストがかかりすぎる」(49.0%)、「対策を構築するノウハウの不足」(42.5%)、「教育訓練」(40.3%)、「どこまでやればよいかの基準」(34.7%)があげられ、これらの項目は、前回の調査でも同様に高い割合であった。しかし、「コストがかかりすぎる」については、前回の40.3%が49.0%へと大きく増加しており、実際にセキュリティ対策を実施しようとすると、そのコストが大きな壁になっていると考えられる。これに対して、「経営者の理解が得られない」は、10.4%に止まった。この数字は、決して経営者がセキュリティに十分に理解を示しているからではなく、未だ経営者にセキュリティ対策の必要性を訴えるまでに至っていないと考えるべきである。

なお、その他の意見としては、「管理者層の倫理観の欠如」、「人材不足」、「ツール不足」等があげられた。

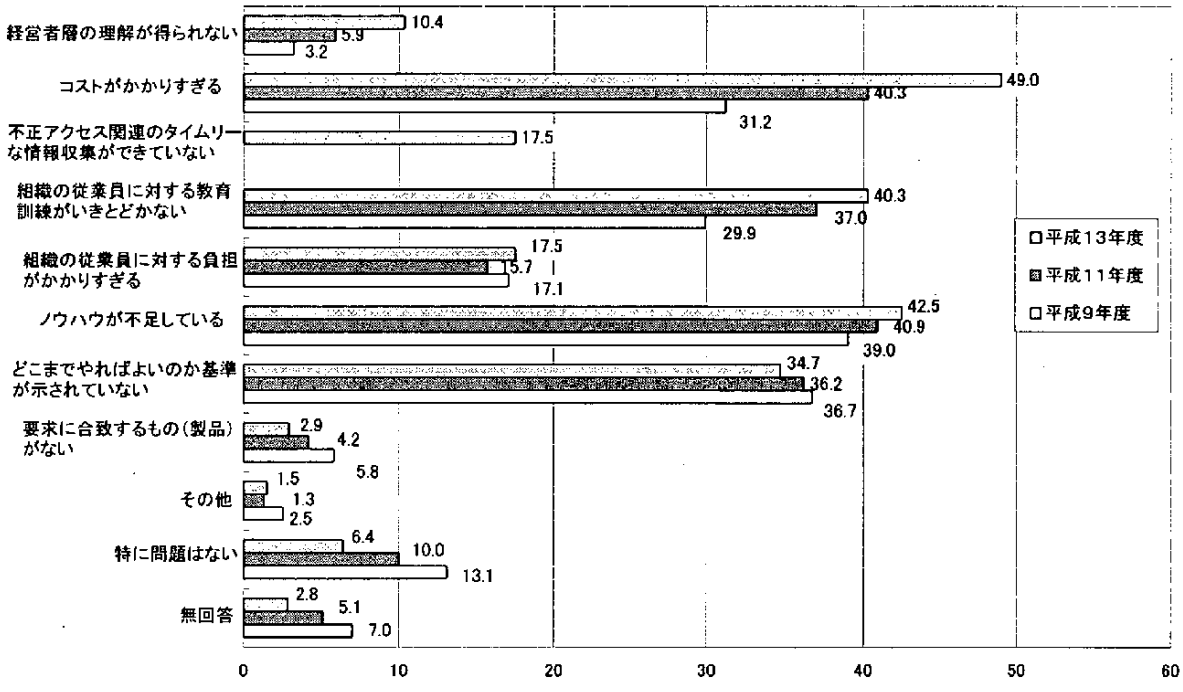


図2－6－7. 不正アクセス対策の問題点

2.7 コンピュータウイルス対策について

Q54. 貴事業体では過去１年間にコンピュータウイルスに感染したことがありますか。

1	ある	494	68.8
2	ない ⇒Q59へ	222	30.9
無回答		2	0.3
計		718	100.0

コンピュータウイルスの被害は、100%に達することを危惧していたが、意外にも前回の 54.6%から 68.8%と、14.2 ポイントの増加に留まった。これは、パソコンにはウイルス対策のワクチンを入れるのが当たり前になり、被害を受ける前にすでに 70.8%の事業体がワクチンソフトを導入していた結果、ウイルス感染を事前に防止できた成果と考えられる。(Q59 の「PC でのワクチンソフトの利用」を参照)。しかし、ワクチンソフトを導入し、パラメータファイルを更新していた事業体が 52.7%であったにもかかわらず（Q59 の「パラメータファイル更新」を参照)、ウイルスに感染しなかった事業体は 30.9%であり、残りの 21.8%はウイルスに感染している。これは、今回の調査の直前、９月 19 日に発生した Nimda のように非常に感染力の強いウイルスが出現し、ワクチンベンダーのパラメータファイル作成が間に合わなかったり、パラメータファイルの配布に時間がかかったためと考えられる。

なお、Nimda はこれまでのメールによる感染に加え、Web サーバのセキュリティホールを使って Web サーバを探して感染させたり、Web にアクセスすると感染したり、ファイル共有の機能を使って感染させるといった複数の感染手段を持ち、非常に感染力の強いウイルスである。

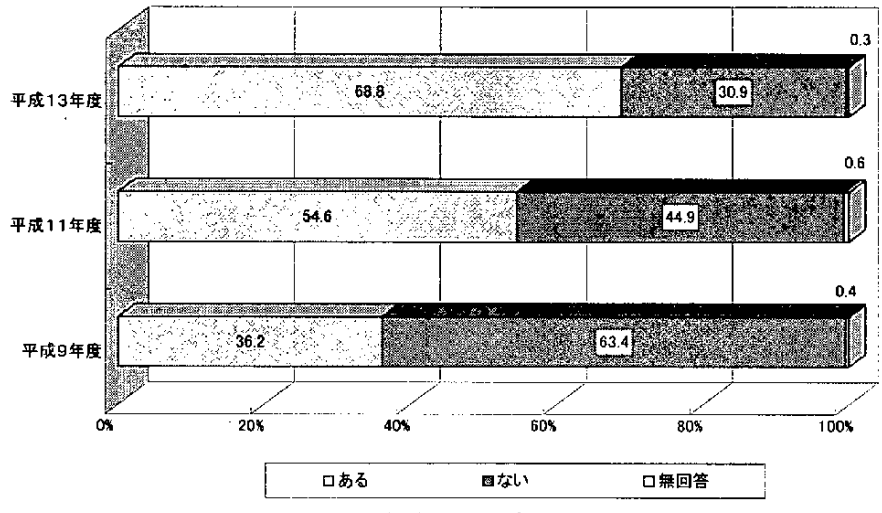


図2－7－1. 過去1年間のコンピュータウイルス被害状況

Q55. コンピュータウイルス被害届出機関である情報処理振興事業協会（ＩＰＡ）に被害を届け出ましたか。

1	出した	98	19.8
2	出さない	387	78.3
無回答		9	1.8
計		494	100.0

経済産業省告示第429号では、ウイルス被害にあったらIPAに届け出ることになっている。前回の調査では、届け出を出した割合が13.5%（8社に1社）と低かったが、今回の調査では、19.8%（5社に1社）へと大きく向上した。ウイルス感染の被害が広がったことと、マスコミでもウイルス関連でIAPの発表が引用されるケースが増え、知名度が向上したためと考えられる。

Q56. 感染したコンピュータは何台ですか。

1	10台未満	248	50.2
2	10台以上～20台未満	84	17.0
3	20台以上～50台未満	78	15.8
4	50台以上～100台未満	29	5.9
5	100台以上～200台未満	24	4.9
6	200台以上～500台未満	13	2.6
7	500台以上～1,000台未満	6	1.2
8	1,000台以上	6	1.2
無回答		6	1.2
計		494	100.0

何台のコンピュータがコンピュータウイルスに感染したかを回答してもらったところ、約5割の感染事例が10台以上であり、平均すると60台程度のコンピュータがウイルスに感染している。ウイルスに感染した場合、そのウイルスがどの程度悪性かによるが、駆除作業は一台ごとの対応となるので作業負荷が大きく、非常に大きなコストとなる。さらに、そのコンピュータの利用者は、駆除作業が終了するまでコンピュータが使えないので、仕事が全く進まないとか、データが失われた場合の被害を含めて考えれば、1件の感染で何百万円の被害となる。回答の中には、1,000台以上の感染事例が6件あり、この場合では億単位の被害が想定される。

Q57. 主要な感染原因（経路）は判明していますか。主な原因を選んで下さい。（複数回答）

回答件数		494	
1	フリーソフトウェアから	10	2.0
2	外部から入手した記録媒体から	158	32.0
3	社内ネットワーク経由で	75	15.2
4	インターネット経由で	208	42.1
5	電子メールの添付書類で	331	67.0
6	外部のホームページの閲覧で	124	25.1
7	その他	7	1.4
8	わからない	32	6.5
無回答		1	0.2

コンピュータウイルスの感染経路としては、電子メールの添付書類によるものが67.0%と最大になった。これは、電子メール自動感染型のウイルスが主流となった状況を反映している。また、インターネット経由の感染も前回の22.0%から42.1%へと倍増している。

注目すべきは、外部から入手した記録媒体からの感染が 32.0％と依然として多いことである。この感染手法を使うウイルスは、最近では新種が発生していないので、ワクチンソフトをインストールしていればまず感染しないはずである。感染した 158 件のケースは、ワクチンソフトをインストールしていなかったケースがほとんどと考えられる。（感染後にインストールした場合を考慮すると、178 件がインストールしていなかったことになる。）

一方、新型の感染手法として、Web サーバーソフト、ブラウザ、電子メールソフトのセキュリティホールを利用してホームページを見ると感染する Nimda が 9 月に発生した。これによる感染の事例も 25.1％あり、今後の感染経路として注目すべきである。

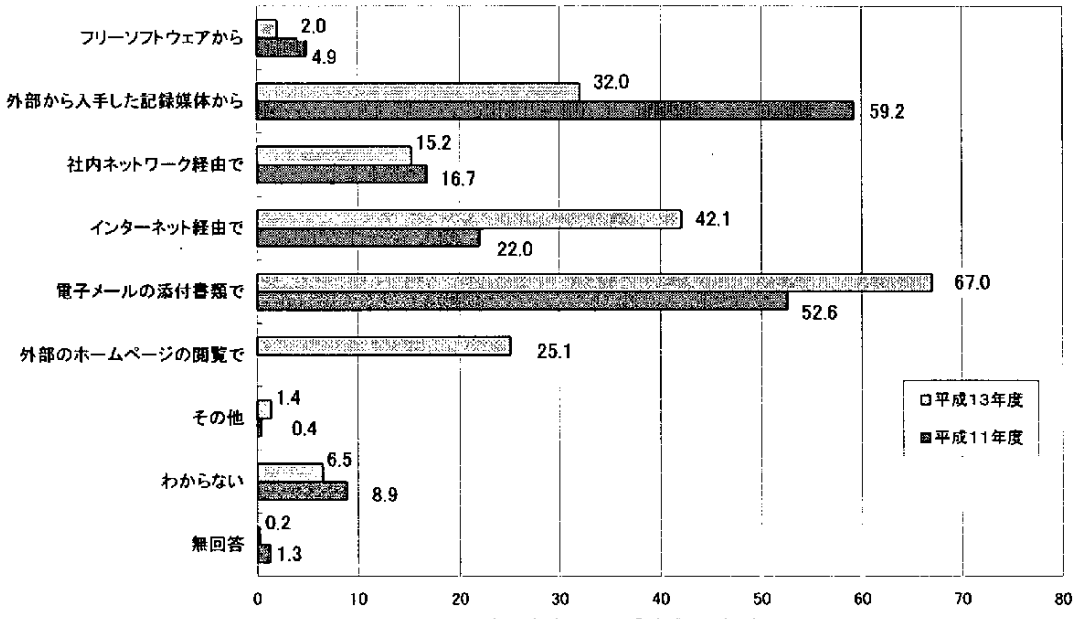


図2－7－2. 主要なウイルス感染原因（経路）

Q58. 貴事業体では、過去１年間に、外部に対してコンピュータウイルスに感染したメールを送ったり、感染したファイルを送ってしまったことがありますか。

1	あ る	133	26.9
2	な い	256	51.8
3	把握していない	98	19.8
無回答		7	1.4
計		494	100.0

最近の電子メールを感染経路とするウイルスは、感染したパソコンが次は他のパソコンにウイルス付き電子メールを送り感染を広げていく。つまり、ウイルスの被害者が次は加害者になるわけである。今回始めてこの項目を調査したが、26.9％の事業体が加害者になっている。一方、この数字が電子メールの添付書類で感染した事業体数の 331 件に比べて少ないのは、Hybris ウイルスのように電子メールの発信元を改ざんして送るので、被害者側で発信元を特定できなかったり、同時期にいろいろなところからウイルスが送られてきたために発信元を特定できなかったためと考えられる。いずれにしろ、自社からウイルス付きのメールを送ってしまった場合、社内のセキュリティ管理に対して外部からの信用を失うことになり、ビジネス面での悪影響も考えられる。

Q59.. ①コンピュータウイルスに対して講じている対策は何ですか。現在実施している対策を選んで下さい。(複数回答)

②(Q54で「1」と答えた場合のみ)このうち、ウイルス被害を契機として実施した対策を選んで下さい。(複数回答)

コンピュータウイルス対策	①実施対策		②ウイルス被害後の対策	
回答件数	718		494	
コンピュータウイルス被害を受けた場合のIPAへの相談	51	7.1	15	3.0
ウイルス対策用のマニュアル(セキュリティ対策基準に入れた場合も含む)の作成	198	27.6	26	5.3
ウイルス対策チーム(社内でウイルスが検出された時の対応を行うチーム)の設置	168	23.4	37	7.5
ウイルス検出時や緊急対応と連絡体制の整備	292	40.7	48	9.7
ソフトウェアの出所の確認	166	23.1	32	6.5
記録媒体のウイルスチェックの実施	355	49.4	42	8.5
ライトプロテクト、バックアップ等のソフトウェア管理	106	14.8	9	1.8
PCでのワクチンソフト(ウイルス検出ソフトを含む)の利用	609	84.8	69	14.0
PCのワクチンソフト・パラメータファイルを定期的に更新	482	67.1	71	14.4
サーバ機でのワクチンソフトの利用	442	61.6	57	11.5
メール用ゲートウェイ／サーバでのワクチンソフトの利用	318	44.3	34	6.9
メール用ゲートウェイ／サーバでの添付ファイルの制限(例:実行ファイル削除)	103	14.3	20	4.0
ワクチンソフトの集中監視	209	29.1	31	6.3
定期的な集中監視ログの解析	126	17.5	27	5.5
パスワードの変更等、アクセスコントロールの強化	100	13.9	8	1.6
動作の定期的な確認等、異常発見体制の整備	64	8.9	11	2.2
緊急時の電子メールサーバの停止	162	22.6	30	6.1
緊急時の社員への連絡(ウイルス警告の放送／送付)	323	45.0	59	11.9
ウイルス対策サービスの利用	106	14.8	12	2.4
その他	9	1.3	6	1.2
特に対策を講じていない	32	4.5	9	1.8
無回答	12	1.7	295	59.7

コンピュータウイルスへの有効な対策として、PCへのワクチンソフトの導入がある。最近のウイルス感染被害の状況を考えれば、この割合が100%になることを期待していたが、意外にも84.8%に止まった。また、ウイルス被害を受けて導入した事業体が14.0%あることから、それ以前の導入率は70.8%に止まっており、前回調査の76.0%を下回っている。

一方、今回初めて調査したメール用ゲートウェイでのワクチンソフトの利用は44.3%に達し、電子メールで感染するウイルスの対策をメールサーバで集中的に行う事業体も多いことを示している。PCへのワクチンソフトの導入率が下がった原因の一つは、このメールサーバでの集中チェックによるものと考えられる。しかし、最近のウイルス感染の状況を考えると、PCへのワクチンソフトの導入率とメール用ゲートウェイへの導入率ともに実施することが必要である。

ワクチンソフトがウイルスを検出するために使用するパラメータファイル(ワクチンベンダーによりパターンファイル、シグニチャファイルとも呼ばれる。)は、最新の物を使用しないと新し

いウイルスを検出することができない。各ベンダーは、現在毎週パラメータファイルを更新し、新種のウイルスが発生した時には、対応するパラメータファイルを直ちに作成している。これをタイムリーに各PCに配布することが必要である。しかし、今回の調査ではパラメータファイルを定期的に更新しているのは67.1%であり、ワクチンを導入していてもウイルス防御に役立っていないケースが17.7%ある。このパラメータファイルの更新を確実に行うにはワクチンソフトを集中管理しないと難しいが、ワクチンソフトの集中管理を実施している事業体は、29.1%に止まっており、残りの38.0%の事業体は、すべてのPCについて毎週パラメータファイルを更新することは難しいと考えられる。

コンピュータウイルスの被害を防ぐためには、ワクチンの利用といった技術面と共に、ウイルス対策についての組織的な対応が重要である。たとえば、自社のウイルス対策基準の作成、緊急時対応の体制の整備、ウイルスについての教育等について、それを実施する組織とその権限・役割を明確に、それに必要な資源をアサインする必要がある。しかし、この対応は実施率が低く、ウイルス対策用マニュアルを作成している事業体が27.6%、ウイルス対策チームを定めている事業体が23.4%と不十分な状況である。

ウイルス対策について、対策を実行していくためのスキルを自社要員に習得・維持させていくのが困難であり、外部のウイルス対策サービスも今後有効な選択肢の一つとなっていくと思われる。すでに、こういったサービスを利用している事業体が14.8%あり、数字は今後急上昇することが予想される。

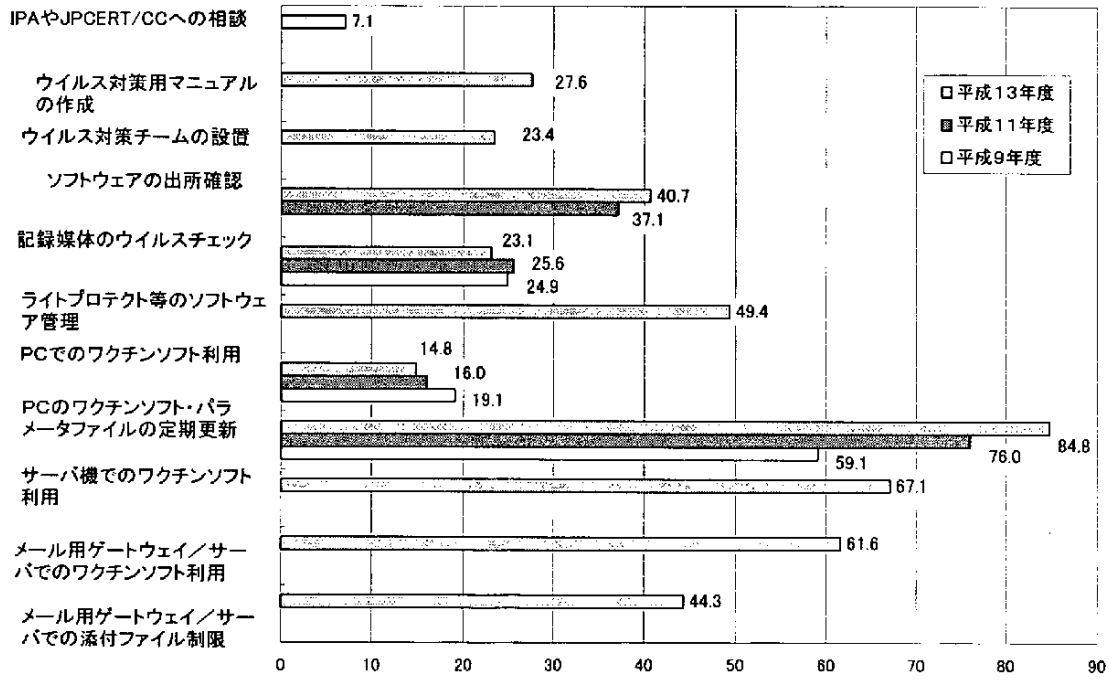


図2－7－3．コンピュータウイルス対策の実施状況（その1）

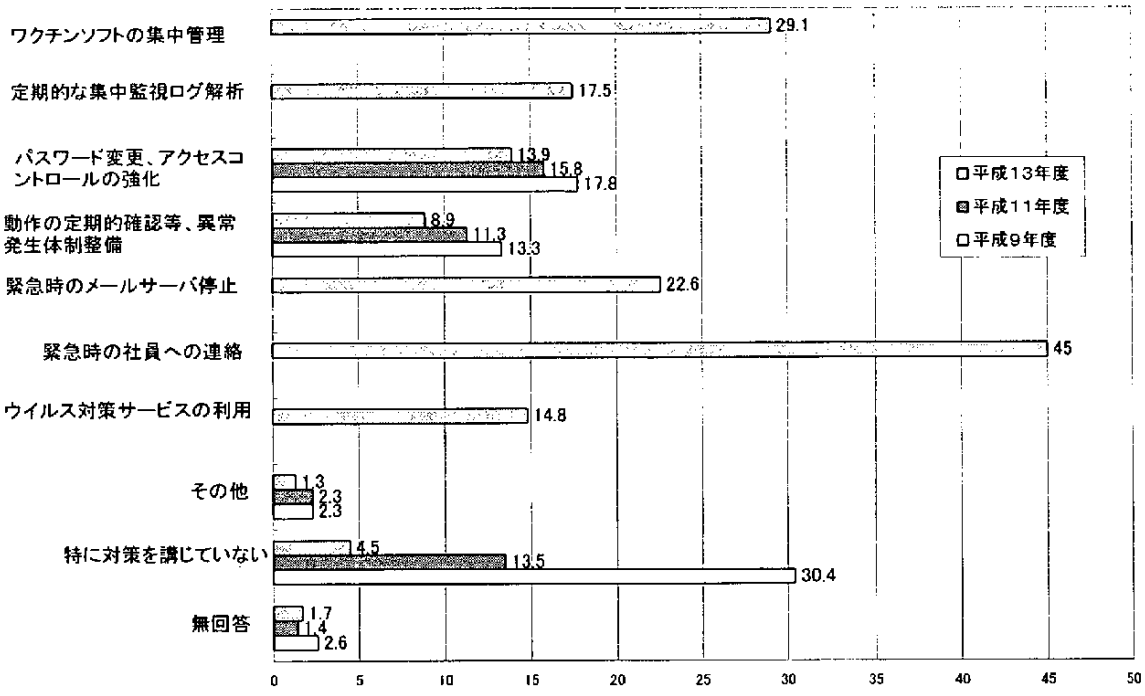


図2－7－4．コンピュータウイルス対策の実施状況（その2）

Q60．貴事業体では従業員に対し、コンピュータウイルス対策に関する教育・訓練の場を設けていますか。

1	情報セキュリティ教育に関して定期的に実施している	30	4.2
2	社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している	62	8.6
3	情報セキュリティポリシーや実施手順、規定類に従って実施している	97	13.5
4	その他	70	9.7
5	特に実施していない	439	61.1
無回答		20	2.8
計		718	100.0

コンピュータウイルス対策に関する教育・訓練の実施率は、前回調査の28.3%から36.0%へと大きく増加したが、一方、特に実施していない事業体も61.1%ある。コンピュータウイルス対策について、適切な教育・訓練を実施することは、一番費用対効果の高いウイルス対策であるといわれており、この実施率が低いことは、Q59におけるウイルス対策についての組織的対応が不十分なことと合わせて、現在のウイルス対策が技術面に偏りすぎていることを示唆している。しかし、外部ネットワークとの接続を遮断するといったユーザー部門の業務にも大きな影響を与える対策が必要な場合もあり、技術面の対策のみでは適切な対応が難しい。ユーザー部門の責任者にウイルス対策について教育し、ユーザー部門に対する影響があっても対策を行う必要性を理解させる下地を作っておくべきである。

その他の意見としては、「社内ホームページ、電子掲示板、電子メール等による情報提供・注意喚起」、「担当者に一任」等があげられた。

Q61. コンピュータウイルス対策についての問題点は何ですか。(複数回答)

回答件数		718	
1	経営者層の理解が得られない	40	5.6
2	コストがかかりすぎる	311	43.3
3	コンピュータウイルス情報や対策に関するタイムリーな情報収集ができていない	137	19.1
4	組織の従業員に対する教育訓練がいきとどかない	280	39.0
5	組織の従業員に対する負何がかかりすぎる	135	18.8
6	ノウハウが不足している	182	25.3
7	どこまでやれば良いのか基準が示されていない	179	24.9
8	要求に合致するもの(製品)がない	23	3.2
9	適切な委託先がない	9	1.3
10	その他	20	2.8
11	特に問題はない	73	10.2
無回答		14	1.9

コンピュータウイルス対策についての問題点として、今回の調査では前回第2位の「コストがかかりすぎる」が第1位となり、前回1位だった「従業員に対する教育訓練の徹底」が第2位になった。第3位には「ノウハウが不足している」ことがあげられている。

ウイルス対策のコストについては、ワクチンソフトでは他のソフトウェアで通常購入価格の15%程度の保守料金が2倍以上する場合もあり、このことが一つの理由と考えられる。また、最近のウイルスの発生状況からパラメータファイルの更新も通常の状態で毎週行われており、前回調査の時には、月に一回程度の更新だった状況から、大幅に頻度が上がっている。そして、70.9%の事業体がワクチンの集中監視を行っておらず、各PCのパラメータファイル更新に人手がかかることから、大きなコストになるためと考えられる。

次にウイルス対策についての教育・訓練は、Q60で教育訓練を実施した事業体が28.3%から36.0%へと大きく増加したにもかかわらず、問題点と考えている事業体が前回調査の41.1%から39.0%と微減に留まった。これは、教育・訓練の重要性がより理解され、教育を実施していないことを問題点と考えている事業体が増えたためと考えられる。

今後、平成13年秋季より情報処理技術者試験が開始された情報セキュリティアドミニストレータを中核に、これらの問題点を解決し、わが国の事業体がコンピュータウイルスへの適切な対応がとれるようにすることは、e-ジャパン実現の必要条件の一つである。

その他の意見としては「新種ウイルスに対するワクチンソフト対応までのタイムラグ」、「クライアントの利用ブラウザの種類、バージョンが把握できない」、「ユーザがパッチ処理をしているかの確認ができない」等があげられた。

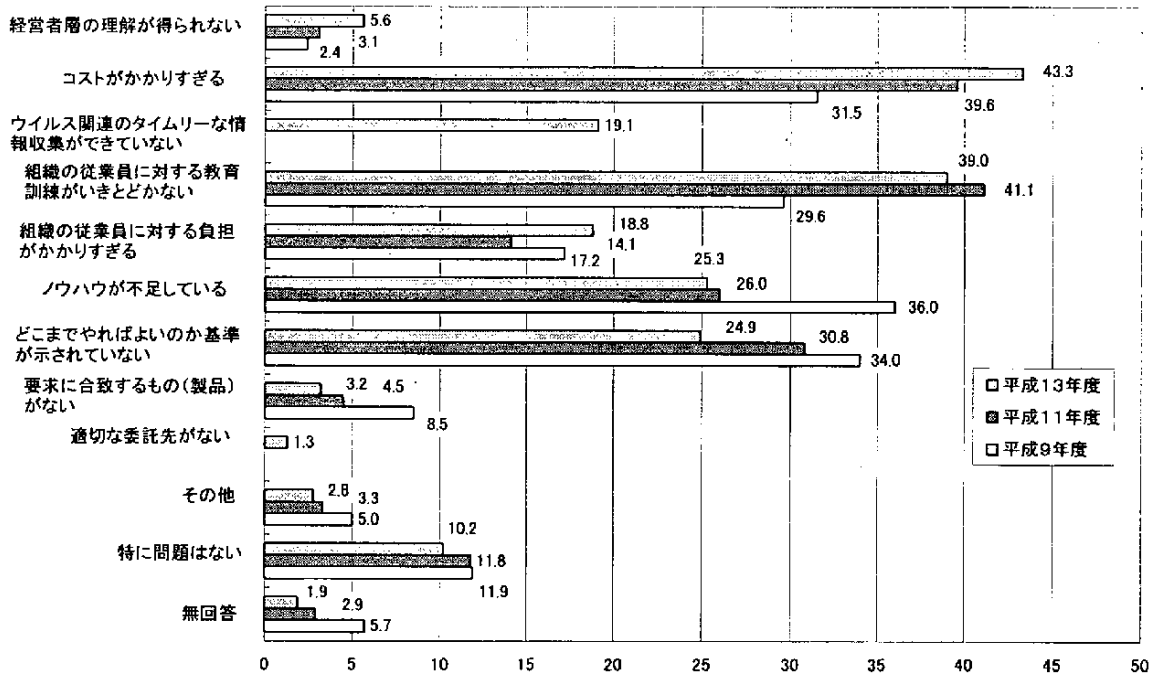


図2－7－5. コンピュータウイルス対策の問題点

2.8 情報リスクマネジメント関連について

Q62. 情報セキュリティ要素1～10のうち、貴事業体にとって重要と思われる要素を**3つ選び**、下の回答欄に優先順位をつけて記入して下さい。

情報セキュリティ要素(回答件数718件)		1位 有効回答数604件		2位 有効回答数600件		3位 有効回答数598件	
1	情報セキュリティポリシー(経営者の積極的な関与)	219	36.3	47	7.8	37	6.2
2	情報セキュリティ組織(情報セキュリティの推進組織の構築と活動)	73	12.1	99	16.5	60	10.0
3	情報資産の分類および管理(情報資産のリスク評価とそれによる重要度の分類)	43	7.1	61	10.2	65	10.9
4	人的セキュリティ(役職員への教育訓練や内部規則の策定など)	71	11.8	93	15.5	92	15.4
5	物理的および環境的セキュリティ(入退室管理や安全区画の構築など)	12	2.0	27	4.5	37	6.2
6	通信および運用管理(ネットワークの管理、ウイルス対策、ログ管理など)	74	12.3	122	20.3	111	18.6
7	アクセス制御(IDとパスワード管理、不正アクセス対策など)	35	5.8	81	13.5	92	15.4
8	システム開発およびメンテナンス(開発環境のセキュリティ、ライブラリ管理運用など)	14	2.3	26	4.3	21	3.5
9	事業継続計画(災害対策、障害対策など)	52	8.6	33	5.5	61	10.2
10	準拠(法律遵守、システム監査など)	11	1.8	11	1.8	22	3.7
無回答(注)		114	-	118	-	120	-

注1)優先順位をつけなかった回答は「無回答」扱いとしている。
注2)それぞれの比率については、有効回答数を分母にして算出している

		1位－3位の総合計(①)		優先順位をつけなかった回答群(②)		総合合計(①+②)	
回答件数		604		94		698	
1	情報セキュリティポリシー	303	50.2	43	45.7	346	49.6
2	情報セキュリティ組織	232	38.4	38	40.4	270	38.7
3	情報資産の分類および管理	169	28.0	28	29.8	197	28.2
4	人的セキュリティ	256	42.4	32	34.0	288	41.3
5	物理的および環境的セキュリティ	76	12.6	10	10.6	86	12.3
6	通信および運用管理	307	50.8	52	55.3	359	51.4
7	アクセス制御	208	34.4	34	36.2	242	34.7
8	システム開発およびメンテナンス	61	10.1	12	12.8	73	10.5
9	事業継続計画	146	24.2	25	26.6	171	24.5
10	準拠	44	7.3	5	5.3	49	7.0

情報セキュリティを実現するための要素について10個の要素をISO17799を参考に例示し、その優先順位について調査を行った。1位から3位までを選択してもらう設問であったが、順位をつけずに3つを選択した回答もあったため、まず順位をつけたもので分析し、その3位までの合計と順位をつけずに3つ選択した回答を合計したものとで分析を行う。

なお、以下に示すパーセンテージは、有効回答数に対する比率を示している。

（1）第1位の分析

第1位には経営者の積極的な関与を代表とする「情報セキュリティポリシー」219件（36.3%）となった。その次に多かった「通信および運用管理」が74件であるように、大きな差をつけて重要な項目とされた。情報セキュリティの確保には要員や予算などの経営資源を必要とするため経営者の理解や関心の高さおよび責任体制の明確化が必要であり、それをある程度裏づけるものである。第2位はネットワークの管理やウイルス対策、ログ管理などの「通信および運用管理」が74件（12.3%）となり、ウイルスの被害に苦しめられその対策に追われている状況が反映されていると思われる。第2位、第3位、第4位はほとんど差がなく第3位には情報セキュリティの推進組織の構築とその活動である「情報セキュリティ組織」が73件（12.1%）、第4位には役職員への教育訓練や内部規則の策定などの「人的セキュリティ」が71件（11.8%）となった。ここでは情報セキュリティの構築にはやはり確固たる推進組織が構築され、従業員の教育や規則の策定徹底といったことが求められ、あらためて情報セキュリティに人間的な要素の占める割合が多いことが伺える。第5位以下は、次のとおりである。第5位－災害対策や障害対策など万一の事故に備える「事業継続計画」52件（8.6%）、第6位－情報資産のリスク評価とそれによる重要度の分類を中心とする「情報資産の分類および管理」43件（7.1%）、第7位－IDとパスワード管理、不正アクセス対策などの「アクセス制御」35件（5.8%）、第8位－開発環境のセキュリティ、ライブラリ管理などの「システム開発およびメンテナンス」14件（2.3%）、第9位－入退室管理や安全区画の構築など「物理的および環境的セキュリティ」12件（2.0%）、第10位－法律遵守やシステム監査など「準拠」11件（1.8%）となった。

（2）上位3位までの分析

第2位の選択状況をみると、「通信および運用管理」が122件、「情報セキュリティ組織」99件、「人的セキュリティ」93件、「アクセス制御」81件となり、情報セキュリティポリシーを確立したあとは、実際に情報セキュリティを確立し実現するための実践的な要素が求められていることがわかる。ここでは、情報セキュリティ組織の確立や人的セキュリティといった自らの組織の人間的な側面が重視されている。また猛威を振るい始めたウイルスへの対策や不正アクセス対策など、情報セキュリティ独特の実務で、また早急を要する対応に関心の高さが現れている。

第3位をみると第2位と同様の項目が多くあげられており、「通信および運用管理」111件、「人的セキュリティ」および「アクセス制御」92件、「情報資産の分類および管理」65件となっている。ここで特徴的なのは情報セキュリティの確立、特にISO17799などの情報セキュリティポリシーでは重要視されている情報資産の明確化や機密度合いに応じた分類などは第3位あたりの順位で4番目に評価されるなどあまり重要視されておらず、実際には個々の情報ごとに区分けしてセキュリティを組み込むよりも、情報システム全体を包括してウイルス対策や不正アクセスなどの対策をとっていることが憶測される。

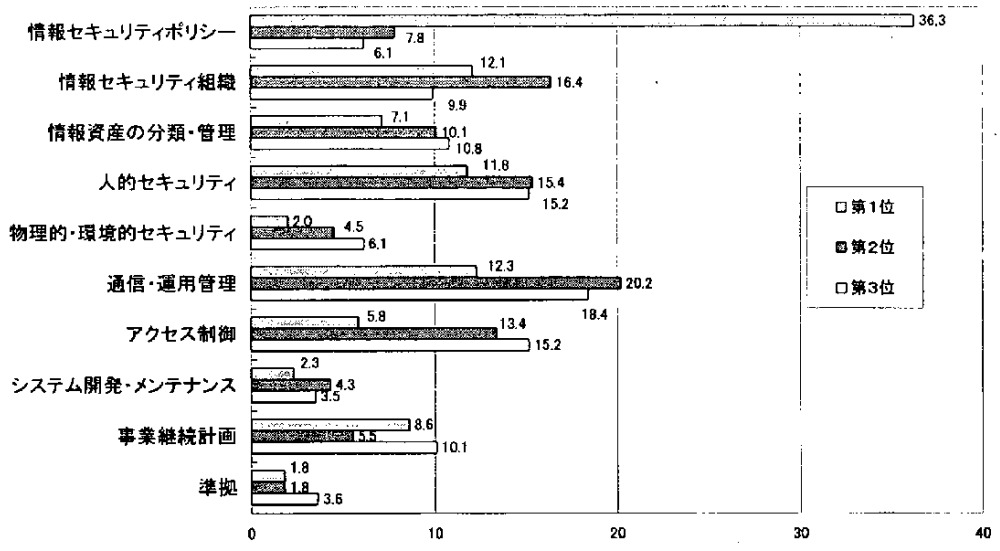


図2－8－1．重要と思われる情報セキュリティ要素（優先順位　第1～第3位）

（3）１位から３位の順位付けを元にした分析

これらを総合的に判断すると次のような現状といえる。

情報セキュリティの確立にはまず経営者の関与が必須であり、その経営者のリーダーシップにより情報セキュリティの推進組織をつくり、従業員の教育訓練や不正防止などの内部規範の策定など組織的な対応を重視している。実際の情報セキュリティの現場ではウイルス対策が現実の被害状況を反映してか重要とされている。パスワード管理や不正アクセス対策はウイルス対策の次とされている。予防対策は情報資産ごとに重要度をつけて選別して実施することはあまり重要視されておらず、情報システム全体を包括的に行うことが読み取られる。

大型コンピュータからサーバーパソコンに重点が移っている現状を反映し古典的なコンピュータルームの入退室管理や火災対策などの物理的な安全性は相対的に重要度が下がっている。また事故が発生した際の事業継続計画よりはネットワーク管理などの予防対策のほうが比較的重要視されている。システム監査や法律遵守については最重要視されていない。

（4）１位から３位まで優先順位を考慮しないで合計した集計の評価

優先順位をつけずに３つまでを選択した回答も94件あったため、それらを考慮し上位３つの合計で評価を行ってみる。

１位は「通信および運用管理」359 件（51.4%）となり、わずかの差ではあるが経営者の関与などの「情報セキュリティポリシー」を上回った。これは順位をつけた回答だけで３位まで合計した場合も同様に第一位となっており傾向は変わらない。第２位は「情報セキュリティポリシー」346 件（49.6%）となっており経営者の関与が必要であると認識されていることには変わりはない。第３位以下は、第３位「人的セキュリティ」288 件（41.3%）、第４位「情報セキュリティ組織」270 件（38.7%）、第５位「アクセス制御」242 件（34.7%）、第６位「情報資産の分類および管理」197 件（28.2%）、第７位「事業継続計画 171 件（24.5%）、第８位「物理的および環境的セキュリティ」86 件（12.3%）、第９位「システム開発およびメンテナンス」73 件（10.5%）、第10位「準拠」49 件（7.0%）となった。

全体の重要視している要素の順位は１位から３位の順位をつけた場合の評価とあまり差はない。３位までの総合順位で特筆すべき事項としては、経営者の関与を重要としながらも３位までの合計では経営者の関与は第２位に下がり、変わってウイルス対策に代表される通信および運用管理が第１位となることに端的にあらわれているように、情報セキュリティの確立を実現する実務部門がウイルス対策に追われている実態が垣間見えると考えられる。

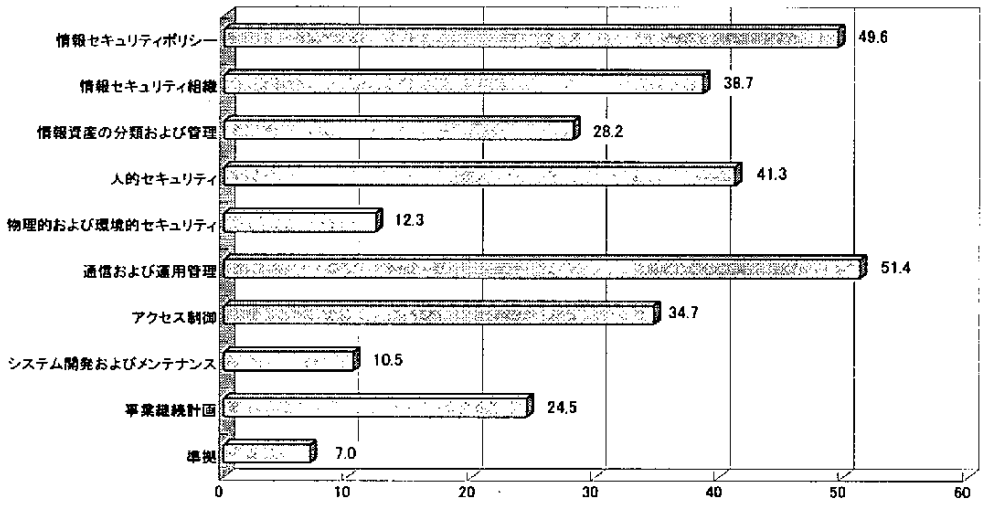


図2－8－2. 重要と思われるセキュリティ要素（優先順位付けなし）

（５）業種別の特徴

回答が 30 社以上あった業種、建設業、化学工業、電気機械器具製造業、その他の製造業、商社、金融業、運輸通信倉庫業、情報サービス業、地方公共団体の９つの業種について特徴を分析してみる。どの業種も第１位は「情報セキュリティポリシー」が多い。第２位は「情報セキュリティ組織」（建設業、情報処理サービス業、地方公共団体）、「人的セキュリティ」（電気機械機器製造業、その他製造業、商社、金融業）、「通信および運用管理」（建設業－（同点）、化学工業、運輸・通信・倉庫業）と分散している。１位の選定では最下位であった「準拠」を第１位に取り上げた企業が複数あった業種は金融業（３社）と情報処理サービス業（２社）であり、ＩＴ依存度が大きいこの２つの業種であることは興味深い。これは第２位に準拠を選択する業種も金融業と情報処理サービス業に偏っており同様の傾向を示している。

上位３位までの集計では平均からの差異をみてみる。この分析では回答は１位から３位までの順位をつけた回答を複数回答として集計した。業種は複数業種をくくった業種グループ別で行っている。

「情報セキュリティポリシー」を１位から３位までに選択した割合が全体平均（42.2％）より高かった業種は情報処理サービス（52.7％）、電気・一般・輸送用機械製造業（51.0％）、政府・地方公共団体（47.4％）である。また低い業種は食品・紙パルプ・繊維・印刷業（30.6％）、公共サービス（33.3％）であった。

「情報セキュリティ組織」で全体平均（32.3％）より高い業種は情報処理サービス（39.2％）、石油・化学・鉄鋼・非鉄金属製造業（37.3％）、政府・地方公共団体（36.8％）、金融・保険業（36.6％）

である。低い方ではその他製造業（26.4%）、電気・一般・輸送用機器製造業（26.5%）である。

「人的セキュリティ」で全体平均（35.7%）より高い業種は政府・地方公共団体が 60.5%と、きわめて高い選択をしている。その他では石油・化学・鉄鋼・非鉄金属製造業（44.8%）、金融・保険業（40.2%）がある。

「通信および運用管理」で全体平均（42.8%）より高い業種は政府・地方公共団体（60.5%）、石油・化学・鉄鋼・非鉄金属製造業（56.7%）ときわめて高い選択となっている。

一方選択の比率が低かった方での特徴は「事業継続計画」の全体平均（20.3%）に対して公共サービス（9.8%）、政府・地方公共団体（13.2%）の二つの業種は極端に低い選択となっている。

このように業種別には多少の差があるが全体的な傾向には大きな差はない。また規模別である資本金別、従業員別、年間総費用別の分析では大きな特徴は表れていない。

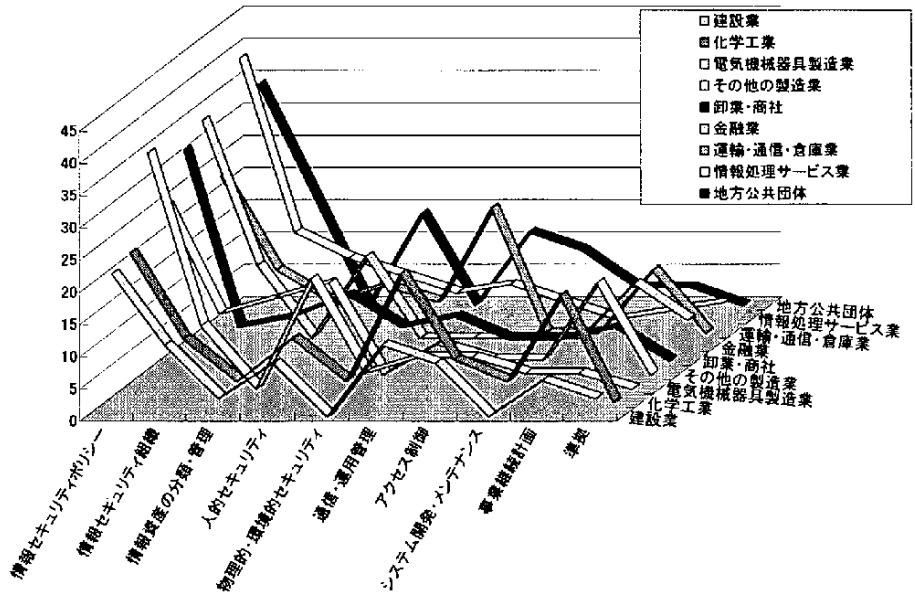


図2－8－3. 業種別にみた重要セキュリティ要素

Q63. 情報セキュリティの確保にとり、基本的に重要な視点は何だと思いますか。（複数回答）

回答件数		718	
1	経営者層の理解	383	53.3
2	管理者の理解	235	32.7
3	担当者の理解	145	20.2
4	社内全体の理解	559	77.9
5	法規制の整備	106	14.8
6	その他	1	0.1
無回答		18	2.5

情報セキュリティの確保にとり、「社内全体の理解」を重要視する回答が 77.9%（前回 74.9%）に達している。これは情報セキュリティの確保の実務にとって全社員が協力し、決められた規則や運用を守っていかなければならないが、依然現実にはなかなか守られていないことの表れと思われる。２番目に「経営者層の理解」が重要との意見が 53.3%（前回 53.7%）であるが、これは

情報セキュリティを進めるには経営資源を投入する必要があり、そのためには経営サイドの関与を必要としていると考えられる。これらの数字は前回の調査とほとんど変化がない。IT の進展がうたわれてはいるものの経営者層の意識には大きな変化がまだ表れていないと考えられる。

業種別や企業規模（資本金、従業員数）による違いを考察すると、各回答に大きな差はなかった。前回「法規制の整備」の必要性については、企業規模の大きい組織体ほどその必要性を訴えている割合が多かったが、今回、そのような傾向ははっきりとはみられていない。

Q64. 経営者層はコンピュータ関連の事件・事故に対するリスクについて関心が高いですか。

1	高 い	187	26.0
2	中 位	253	35.2
3	低 い	161	22.4
4	わからない	110	15.3
無回答		7	1.0
計		718	100.0

経営者のコンピュータ関連の事故・事件に対するリスクについての関心度合いについて、「高い」が 26.0%（前回調査 25.5%）、中位 35.2%（前回 33.2%）、低い 22.4%（前回 18.3%）と分散した評価となっている。また前回の調査と比べてもほとんど同じ傾向であり、Q63 同様、IT が声高にいわれていても経営者層の意識はあまり変わっていないと考えられる。

業種グループ別にみると、「高い」と回答した割合が高い業種は、金融・保険業の 56.1%（前回 48.4%）、情報処理サービス業の 50.0%（前回 50.6%）の 2 業種である。特に金融・保険業は大きく関心度を上げている。一方低い業種は、公共サービスの 5.9%（前回 12.9%）、商業の 14.5%（前回 14.1%）、その他製造業 11.3%（前回 19.7%）であった。

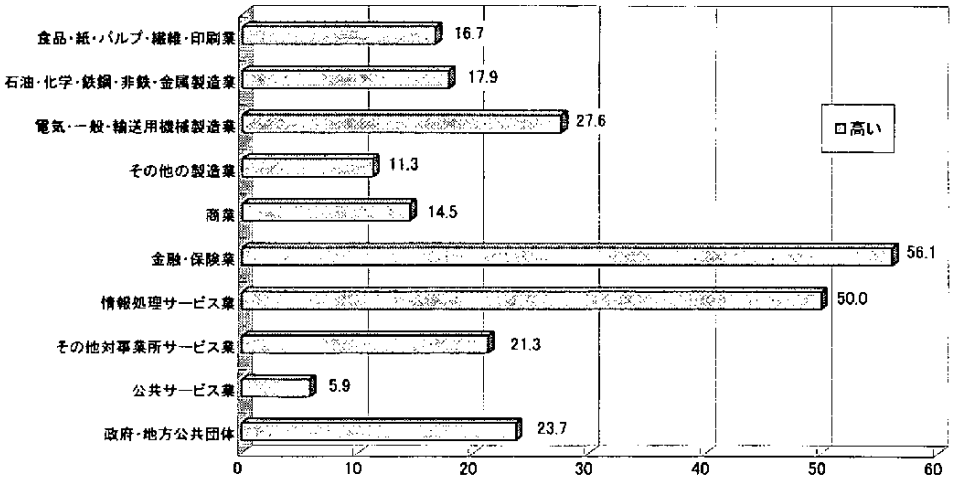


図2－8－4. 経営者のンピュータ関連の事故・事件に対する関心度合い（業種グループ別）

Q65. 情報システムに係わるリスク分析を実施していますか。

1	行っている	135	18.8
2	行っていない ⇒Q67へ	571	79.5
無回答		12	1.7
計		718	100.0

情報システムに関するリスク分析を実施しているのは 18.8%であり、前回の 12.0%と比較するとわずかながら増加しているが依然として低い値にとどまっている。そして 79.5%というほぼ全体の５分の４にあたる組織体がリスク分析を行っていない状況である。

業種グループ別にみると、金融・保険業で 48.8%と前回の 29.7%から大幅に増加していることが目立っている。次いで情報処理サービス業で 35.1%とこれも前回の 21.3%から増加している。この二つの業種が実施率の高い業種であり、情報システムのリスク分析の実施率を引き上げた大きな要因である。この二つの業種は情報システムの業務への浸透度とともにリスクに対する敏感な業種であるといえる。一方、その他の業種ではリスクへの関心は低く、合理的な安全対策をすすめるうえでの今後の重要課題といえる。

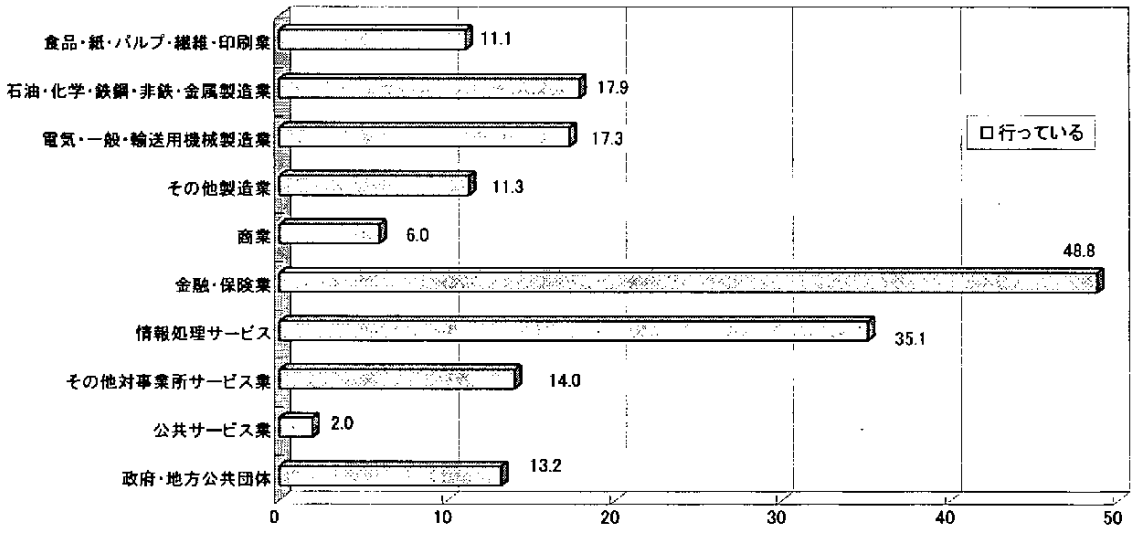


図2－8－5. リスク分析の実施状況(業種グループ別)

次に規模でリスク分析の実施状況を比較すると、資本金別では 500 億円以上 43.1%、100 億円以上～500 億円未満 34.2%、50 億円～100 億円未満 21.5%、10 億円～50 億円未満 14.3%、１億円～10 億円未満 13.3%、５千万円～１億円未満 8.3%、５千万円未満 10.9%とあきらかに資本金の大きな組織体ほどリスク分析を実施している。

また従業員別でも１万人以上 37.1%、５千人～１万人未満 40.0%、３千人～５千人未満 30.8%、千人～３千人未満 27.2%、500 人から千人未満 16.8%、300～500 人未満 14.3%、100～300 人未満 6.6%、100 人未満 8.2%と、規模による実施率の差が大きい。

さらに情報システムの年間総費用でみると、100 億円以上 66.7%、50 億円～100 億円未満 36.7%、30 億円～50 億円未満 48.0%、10 億円～30 億円未満 38.2%、１億円～10 億円未満 14.2%、５千万円～１億円 8.8%、５千万円未満 7.1%と差が大きい。10 億円を前後に 10 億円を超えると 40%近い実施率であるのに対して、10 億円を下回ると 15%以下と大きな差が生じている。

企業規模が大きくまたシステムに関する投資額が多いほど情報システムのリスクによる経営への影響もまた大きくなることが予想されるため、そのためのリスク分析の必要性を認識しているといえる。

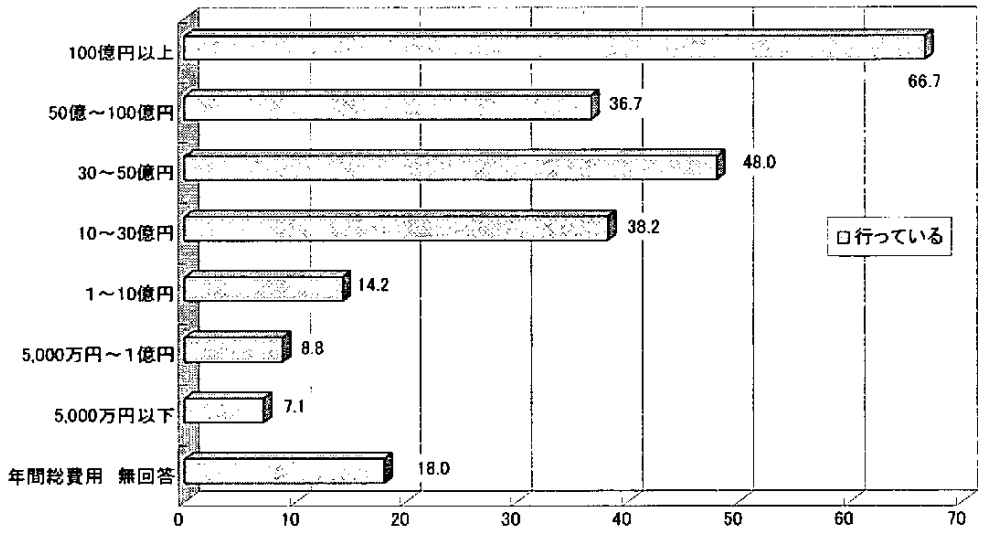


図2－8－6. リスク分析の実施状況(年間総費用別)

Q66. リスク分析を実施した際の問題点は何ですか。(複数回答)

回答件数		135	
1	経営との関係がわからない	12	8.9
2	確立した手法がない	84	62.2
3	分析のためのデータが乏しい	52	38.5
4	専門家がいない	46	34.1
5	組織ができていない	36	26.7
6	その他	9	6.7
7	問題点は特にない	8	5.9
無回答		1	0.7

今回のアンケートでは、リスク分析を実際に実施する際の問題点としては、「確立した手法がない」(62.2%)、「分析のためのデータが乏しい」(38.5%) となり、前回高い割合であった「確立した手法がない」(58.7%)、「専門家がいない」(49.0%) と比べると「専門家がいない」(34.1%) との回答が減少しているのが興味深い。これはリスク分析を実施しはじめた業種が一部に現れ始めたこと等により、専門家が少しずつ誕生してはいるが、まだ確立された手法がなく、実践的な手法の提供が望まれている状況を表している。リスク分析の手法は試行錯誤の時期であり、これからリスク分析を実施する組織体が増えるとともに手法も開発されて収斂されていくものと考えられる。

Q67. リスク分析を実施しない理由は何ですか。(複数回答)

回答件数		571	
1	重要性を感じていない	76	13.3
2	手法がわからない	273	47.8
3	予算がない	151	26.4
4	発生被害額が算出できない	137	24.0
5	リスク分析の意味がわからない	54	9.5
6	効果がわからない	178	31.2
7	効果があるとは思えない	35	6.1
無回答		27	4.7

リスク分析を実施しない理由としては、「手法がわからない」が47.8%（前回44.7%）で前回同様一番多く、前問同様、まだ確立された手法がなく公的機関やベンダー、コンサルティング会社、学会などが今まで適切な手法を提供および普及できていなかったと考えられる。その一方、「重要性を感じていない」は13.3%と前回の19.3%より減少したものの、「効果があるとは思えない」6.1%（前回6.6%）との2つの合計が19.4%（前回25.9%）であり、依然約5分の1がリスク分析の実施そのものに価値を見出していない。

業種別にみていくと、リスク分析の実施率の高い金融・保険業ではリスク分析を実施していない理由の第一位に「手法がわからない」76.2%をあげており、きわめて高い数値を示している。したがって、今金融・保険業で実施しているリスク分析の手法が水平展開されるとこれらの業種ではリスク分析の実施率が上昇することが期待できる。

Q68. システム監査を実施していますか。(業務監査に含まれている場合を含む)

1	い る ⇒Q70へ	250	34.8
2	いない	455	63.4
無回答		13	1.8
計		718	100.0

システム監査の実施は34.8%とやっと3分の1を超えた程度であり、依然として企業などへの浸透が十分でないことがわかる。業種別でみてみると金融・保険業がシステム監査を実施している割合が65.9%と一番高く、次に情報処理サービスで56.8%となっており、その他の設問同様、この二つの業種が情報システムに関するリスクに関心度が高い。

一方、システム監査の実施率が低い業種は公共サービスの5.9%、政府・地方公共団体5.3%であり、公共性を求められるこの二つの業種できわめて低く、改善が必要と考えられる。

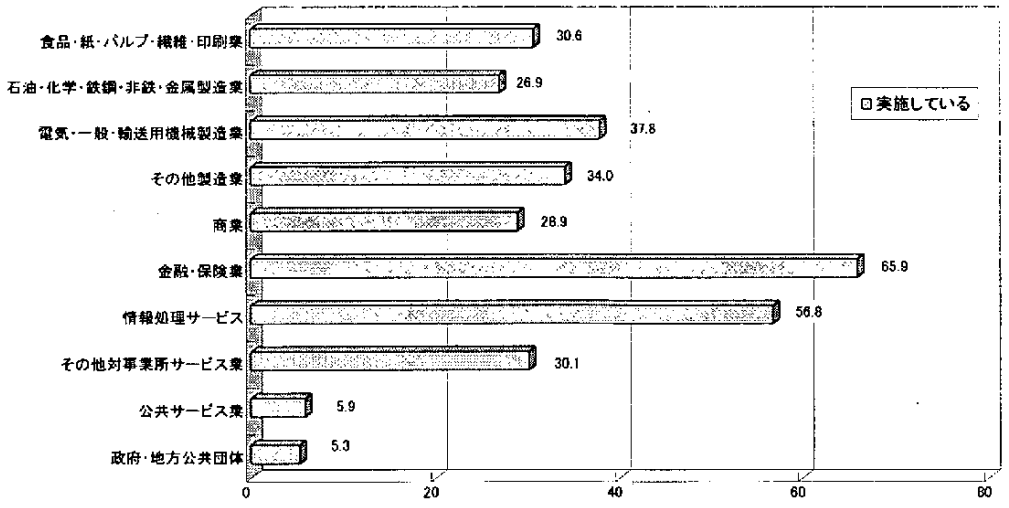


図2－8－7. システム監査の実施状況(業種グループ別)

Q69. システム監査を実施していない理由は何ですか。(複数回答)

回答件数		455	
1	経営者層が重要性を認識していないため	54	11.9
2	システム監査実施のためのコンセンサス、組織風土が十分に備わっていない	178	39.1
3	システム監査の実施よりもシステム化推進そのものに力点がある	139	30.5
4	システム監査の方法、制度、手続きなどが十分ではない	100	22.0
5	効果が明確でない	123	27.0
6	適切なシステム監査人が見つからない	60	13.2
7	その他	20	4.4
無回答		54	11.9

システム監査を実施していない理由として、「システム監査実施のコンセンサス、組織風土が十分に備わっていない」が39.1%と全体の約4割を占めている。金融・保険業、情報処理サービス業などを除く一般の業種では、情報システムの企業経営への影響度が企業の中で比較的小さい場合は、なかなかその重要性が理解されないものと思われる。そのため、情報システムの枠のなかでも「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」30.5%、「効果が明確でない」27.0%などの意見が生じ、開発優先の一般的な風潮のなかに埋没していると考えられる。

Q70. 情報システム関連のリスクが倒産に結びつくと思いますか。

1	思 う	86	12.0
2	重大な影響は受けると思う	402	56.0
3	重大な影響は受けない	99	13.8
4	わからない	102	14.2
無回答		29	4.0
計		718	100.0

情報システム関連のリスクが倒産に結びつくと「思う」割合は 12.0％（前回 12.3％）である。倒産に至らなくとも「重大な影響を受けると思う」が 56.0％（前回 48.2％）に達し、あわせて 68.0％（前回 60.5％）となり、全体の３分の２以上の企業や組織体が経営に重大な影響を受けると感じている。これらは IT の企業などへの浸透により依存度が高くなってきていることの表れと考えられる。

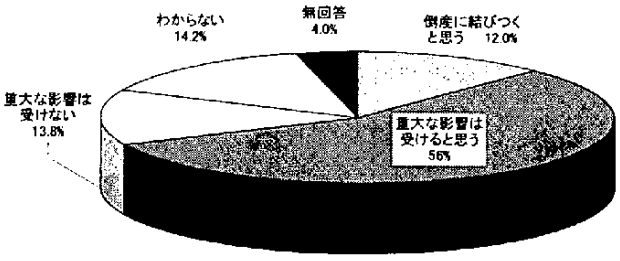


図2－8－8. 情報システム関連リスクがもたらす倒産への影響

業種別にみると、倒産に結びつくと考えている割合が高いのは、情報処理サービス業（24.3％）であり、前回（18.0％）より大きく関心度が高くなっており、まさに IT 推進の表裏一体と考えられる。一方金融・保険業は 17.1％（前回 23.1％）、商業 8.4％（前回 20.2％）と下がっており、IT の浸透度合いや情報システムリスクの見極めと対策の浸透などで、情報システムリスクの過大評価の時期が過ぎたとも考えられる。ただし「重大な影響は受けると思われる」という回答は金融・保険業 73.2％、商業 53.0％とリスクが大きいことは認識している。ちなみに情報処理サービス業は 58.1％となっており、全体でみると、「重大な影響は受けると思われる」と「倒産すると思う」をあわせると 82.4％となり、５分の４以上の企業が重大な経営問題になると考えていることがわかる。

一方、「重大な影響を受けない」としているところを規模別で分析すると、資本金や従業員数ではあまり差が生じていなかったが、年間総費用にみると「重大な影響を受けない」という回答が 100 億円以上 3.7％、50 億円～100 億円未満 3.3％、30 億円～50 億円 12.0％、10 億円～30 億円未満 6.6％、１億円～10 億円未満 14.6％、５千万円～１億円未満 16.3％、５千万円未満 20.1％となっており、年間総費用の低いところほど重大な影響は受けないと回答している。これはあきらかにその企業や組織体の IT への依存度を示すものであり、年間総費用が少なく IT に投資せず依存度が低いところでは、万一の情報システムのリスクが発生しても経営に影響が少ないことを表している。

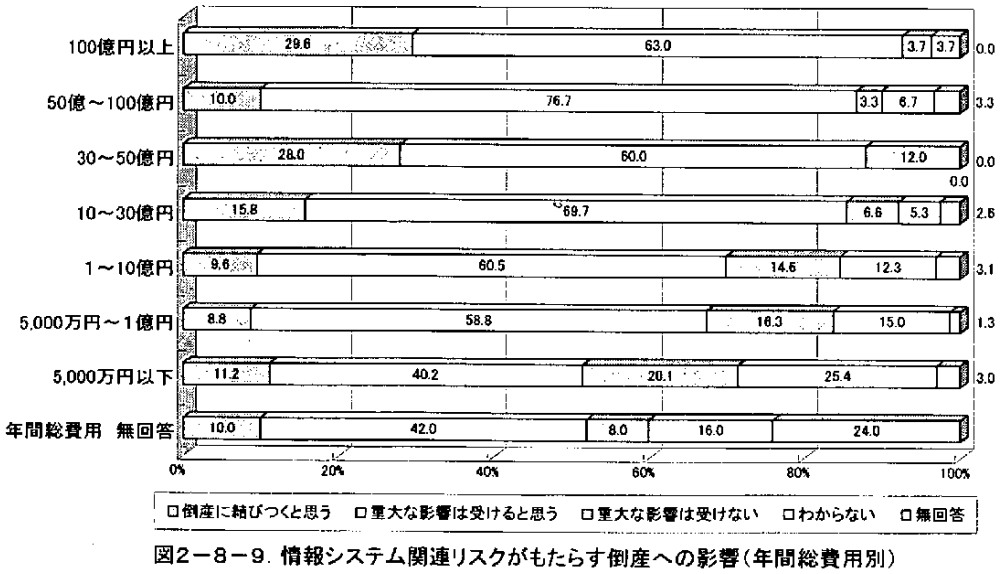


図2－8－9. 情報システム関連リスクがもたらす倒産への影響（年間総費用別）

2.9 情報セキュリティマネジメントシステム（ISMS）について

Q71.「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」を知っていますか。

1	よく知っている	34	4.7
2	知っている	96	13.4
3	存在だけ知っている	168	23.4
4	知らない ⇒Q79 へ	411	57.2
無回答		9	1.3
計		718	100.0

ISMS 適合性評価制度を「知らない」という回答が最も多く 57.2%である。「よく知っている」、「知っている」、「存在だけ知っている」という回答をあわせると 41.5%であり、「知らない」と同程度の割合である。

業種グループ別でみると、ISMS パイロット事業(平成 13 年 4 月～平成 14 年 3 月)の対象範囲である情報処理サービス業で「よく知っている」、「知っている」、「存在だけ知っている」をあわせると 74.4%となり、全体の回答である 41.5%と比較すると圧倒的に高い割合を占めている。なお、情報処理サービス業以外では、電気・一般・輸送用機械製造業（47.0%）、その他対事業所サービス業（46.2%）、金融・保険業（39.0%)が高い割合である。

（参考）ISMS 適合性評価制度の URL：http://isms.jipdec.or.jp

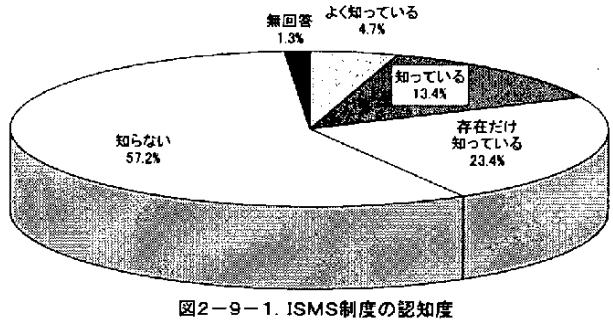


図2－9－1. ISMS制度の認知度

Q72. ISMS 適合性評価制度をどのように考えますか。

1	国際規格であり望ましい	154	51.7
2	国際規格よりも厳しい日本独自のものを追加して作成すべきである	35	11.7
3	旧安全対策基準等を活用すれば十分である	13	4.4
4	わからない	89	29.9
無回答		7	2.3
計		298	100.0

(注)ISMS適合性評価制度は ISO/IEC 17799 および BS 7799-2 を参考としたものです。

ISMS 適合性評価制度を「国際規格であり望ましい」との回答が最も多く、51.7%であり、一方、「国際規格よりも厳しい日本独自のものを追加して作成すべき」という回答は 11.7%である。

Q73. ISMS 適合性評価制度は ISO9000 や ISO14000 シリーズと同様に取引条件や安全性に関する評価基準として利用できると思いますか。

1	客観的な評価として利用できる	55	18.5
2	一定の目安となる	166	55.7
3	あまり利用できない	18	6.0
4	全く利用できない	0	0.0
5	わからない	56	18.8
無回答		3	1.0
計		298	100.0

ISMS 適合性評価制度を「ISO9000、ISO14000 シリーズ」と同様に取引条件や安全性に関する評価基準として「一定の目安となる」との回答が最も多く 55.7%である。なお、「客観的な評価として利用できる」という回答は 18.5%である。また、「一定の目安となる」と「客観的な評価として利用できる」という回答をあわせると 74.2%であることから、約7割が ISMS 適合性評価制度を取引条件や安全性に関する評価基準として利用できると評価している。

Q74. ISMS 適合性評価制度の認証取得を予定していますか。

1	予定している	50	16.8
2	予定していない ⇒Q79 へ	246	82.6
無回答		2	0.7
計		298	100.0

ISMS 適合性評価制度の認証取得を「予定している」と回答した割合は 16.8%である。業種グループ別にみると、制度の認知度同様、情報処理サービス業が最も多く 61.8%であるが、その他の業種については、約8割以上が「予定していない」との回答となった。

Q75. ISMS 適合性評価制度の認定取得の目的は何ですか。主な目的を<u>1つだけ</u>選んで下さい。

1	地方自治体等公的団体への入札条件として	7	14.0
2	民間企業との取引条件として	5	10.0
3	外部への一般的な情報セキュリティ保証として	22	44.0
4	自社内部の情報セキュリティ目標として	10	20.0
5	海外企業との取引条件として	0	0.0
6	その他	2	4.0
無回答		4	8.0
計		50	100.0

認証取得の主な目的は「外部への一般的な情報セキュリティ保証として」と回答した割合が最も高く 44.0%である。ついで「自社内部の情報セキュリティの目標として」が 20.0%である。また、「地方自治体等公的団体への入札条件として」、「民間企業との取引条件として」、「海外企業

との取引条件として」という取引条件を目的とする回答をあわせると 24.0%あり、外部への信頼性のアピールとなる「外部への一般的な情報セキュリティ保証として」とあわせた、対外的な目的をもった回答は 68.0%である。一方、「自社内部の情報セキュリティの目標として」という対内的な回答は 20.0%である。認証取得の目的は、対外的な目的の方が対内的と比較して高い割合である。

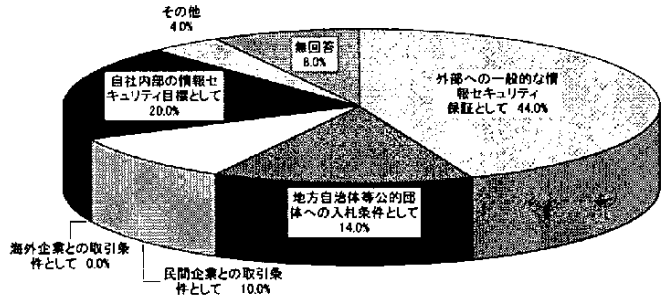


図2－9－2. ISMS適合性評価制度 認証取得目的

Q76. ISMS 適合性評価制度の認証取得のために必要となるコスト負担についてどのように考えますか。

1	非常に大きい	7	14.0
2	大きい	34	68.0
3	小さい	6	12.0
4	非常に小さい	0	0.0
5	新たなコストは発生しない	1	2.0
6	わからない	1	2.0
無回答		1	2.0
計		50	100.0

認証取得のために必要となるコスト負担については、「大きい」と回答した割合が最も高く 68.0%である。また、「非常に大きい」、「大きい」の回答をあわせると 82.0%あり、「小さい」、「非常に小さい」、「新たなコストは発生しない」の回答を合わせると 14.0%である。約8割が認証取得のために必要となるコスト負担が大きいと考えている。

Q77. ISMS 適合性評価制度の認証取得によって期待している効果はどのようなことですか。(複数回答)

回答件数		50	
1	経営陣の理解が得られる	4	8.0
2	取引先からの信用が得られる	42	84.0
3	投資する情報セキュリティ予算額の目標が得られる	3	6.0
4	自社のイメージがアップする	33	66.0
5	他社との差別化が図れる	21	42.0
6	わからない	0	0.0
無回答		1	2.0

ISMS 適合性評価制度の認証取得によって期待する効果は「取引先からの信用が得られる」と回答した割合が最も高く 84.0%であり、次いで「自社のイメージがアップする」が 66.0%である。ともに対外的な効果を期待しているといった回答である。

Q78. 海外との取引において、相互承認制度はまだありませんが、相互承認ができれば ISMS 適合性評価制度の基準が役に立つと感じますか。

1	海外企業との取引に極めて有効である	16	32.0
2	海外企業との取引にあまり意味があると思わない	4	8.0
3	他の基準の方が役に立つ	0	0.0
4	わからない	22	44.0
5	海外との取引を行わない	7	14.0
無回答		1	2.0
計		50	100.0

将来、海外との取引において相互承認ができた場合、ISMS 適合性評価制度の基準が役に立つか、という質問に対し「わからない」との回答が最も多く 44.0%である。次いで相互承認ができれば ISMS 適合性評価制度の基準が「極めて有効である」とする回答が 32.0%である。なお、「海外企業との取引にあまり意味があると思わない」という、相互承認ができても ISMS 適合性評価制度の基準は役に立たないといった回答は 8.0%と低い割合となった。

2.10 個人情報保護について

Q79. 個人情報の利用目的は何ですか。(複数回答)

回答件数		718	
1	売買等契約の履行	129	18.0
2	顧客サポート	275	38.3
3	代金等の回収	140	19.5
4	情報提供	160	22.3
5	マーケティング	184	25.6
6	商品開発	56	7.8
7	従業員の管理(インハウス情報)	410	57.1
8	行政サービスの履行	68	9.5
9	その他	28	3.9
無回答		74	10.3

個人情報保護の利用については、「従業員の管理」(57.1%) の利用が最も多く、次いで「顧客サポート」(38.3%)、「マーケティング」(25.6%) という結果となった。ただ、従業員に係わる情報を個人情報とみなしていれば、従業員管理での利用は 100%になるはずだが、約4割の事業体は必ずしも従業員情報が個人情報であるとの認識がないことがわかる。

一般的な情報提供や代金回収にもかなり使用されているが、いずれの場合も組織内部での利用が圧倒的に多いのが特徴である。

業種グループ別にみると、「金融業・保険業」はいずれも高い割合を占めしているが、その中で特に高いのは「顧客等サポート」で 76.8%、次に「マーケティング」(72.0%)、「売買等の契約の履行」(58.5%) となっている。

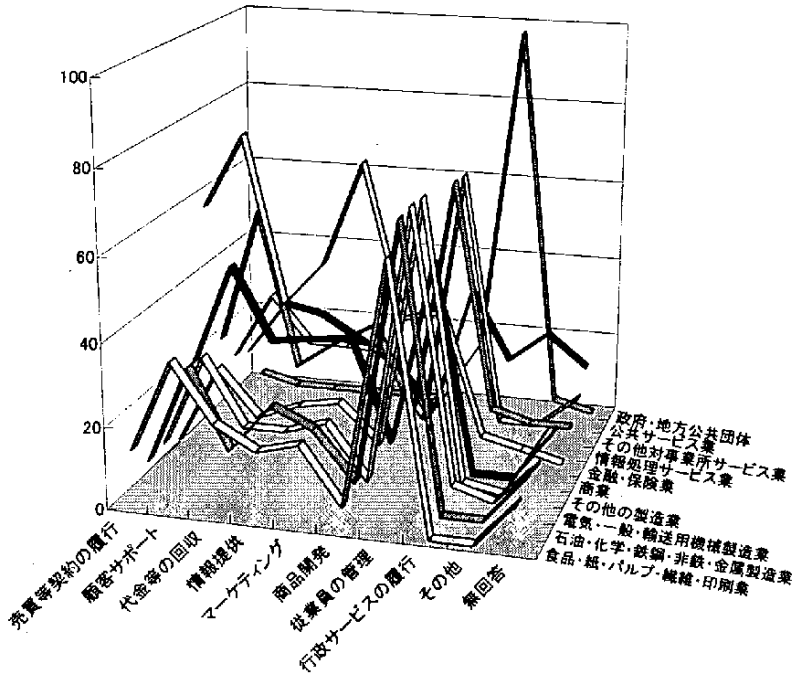


図2－10－1. 個人情報の利用目的(業種グループ別)

Q80. 利用している個人情報の収集方法はどのように行っていますか。(複数回答)

回答件数		718	
1	申込書等によって情報主体(当該個人)から直接に収集	551	76.7
2	名簿業者等から購入	16	2.2
3	グループ企業から入手	31	4.3
4	他社から提供を受ける	27	3.8
5	業務委託契約等に基づき提供を受ける	90	12.5
6	その他	52	7.2
無回答		89	12.4

「情報主体から直接収集」は前回調査（77.8%）同様、最も多く、76.7%となった。次に多いのは「業務委託契約等による提供」（12.5%）であり、前回とほとんど同じ結果となった。これら直接収集や業務委託による提供については事業形態の影響がみられる。

なお、わずかではあるが、「グループ企業からの入手」（4.3%）、「他社からの提供」（3.8%）というケースが見られる。また、「名簿業者からの購入」（2.2%）については、前回の4.4%から若干減少した。個人情報の取り扱いがどのように行われているか、立ち入ってみていく必要がある。

Q81. 情報主体から直接に収集する場合、収集・利用目的について同意を取っていますか。

1	はい	424	59.1
2	いいえ	155	21.6
無回答		139	19.4
計		718	100.0

個人情報の収集に関しては、約6割が同意を取っているが、「取っていない」との回答が約2割を占めており、本人の同意を得ずに収集・利用していることは問題と考えられる。

Q82. 間接的に収集する場合、収集・利用目的について情報主体から同意をとっていますか。

1	情報主体から同意をとっている	125	17.4
2	入手先が情報主体の同意をとっていることを確認している	133	18.5
3	何もしていない	197	27.4
無回答		263	36.6
計		718	100.0

無回答が36.6%と非常に多いのは、設問がわかりにくかった面があったと考えられる。おそらくこの無回答の中には、間接収集をしていない（直接収集のみ）の事業体が含まれているものと想定される。しかしながら、「何もしていない」が27.4%あるのは問題である。情報主体の関知しないところで情報が一人歩きすることのないよう、間接収集であってもきちんと情報主体の同意を得るべきである。

Q83. 貴事業体では顧客等の個人情報データをコンピュータ処理するに際して、個人情報保護の観点からの内部規程（たとえば、個人情報保護規程など）を定めていますか。

1	定めている	181	25.2
2	作成中である	44	6.1
3	検討中である } ⇒Q85へ	116	16.2
4	定めていない } ⇒Q85へ	290	40.4
無回答		87	12.1
計		718	100.0

コンピュータ処理上での個人情報の取り扱いに関しては、約３割が内部規程により管理をしていることがわかる。しかしながら、「定めていない」、「検討中である」を合わせると、56.6％が何の規制も設けていないのは問題である。個人情報の管理にあたっては内部規程により明確に保護されるべきである。

Q84. 個人情報の廃棄方法を個人情報保護規程に定めていますか。

1	定めている	146	64.9
2	作成中である	33	14.7
3	検討中である	15	6.7
4	定めていない	20	8.9
無回答		11	4.9
計		225	100.0

個人情報の廃棄方法について規程で「定められている」が64.9％となった。これに「作成中」を合わせると約８割が廃棄について規程を設けて処理しており、ほぼ満足する結果となった。ただし「定めていない」（8.9％）、「検討中」（6.7％）を合わせると約15％となるのは無視できない。

Q85. 個人情報の取扱いに関する責任と権限を持った管理者を定めていますか。

1	定めている	243	33.8
2	作成中である	124	17.3
3	定めていない	266	37.0
無回答		85	11.8
計		718	100.0

個人情報の取り扱いに関して管理者を「定めている」（33.8％）よりも「定めていない」（37.0％）方が若干多い結果となった。個人情報保護の扱いについていまだ不明瞭な点が多い証拠である。ただし「定めている」、「作成中」を合わせると51.1％となり、個人情報保護の重要性の認識の度合いは決して低くないといえる。

Q86. 個人情報の取扱いに関する情報主体からの苦情処理を行う窓口がありますか。

1	ある	282	39.3
2	ない	346	48.2
無回答		90	12.5
計		718	100.0

苦情処理窓口は非常に重要な機能であるが、48.2%は窓口を設置していない。おそらく現時点では取り扱いに対する問題があまりないこと、また、業種によっては、直接情報主体との接点をもたない業種も含まれていることと思われる。いずれにしても万一に備え、早急に窓口設置をしておくべきである。

Q87. 情報主体から、自己情報の開示や訂正または削除等を求められた場合、応じることになっていますか。

1	なっている	361	50.3
2	なっていない	223	31.1
無回答		134	18.7
計		718	100.0

情報主体からの自己情報の開示、削除等の要求への対応については、「なっていない」との回答が31.1%となった。個人情報の取り扱いはきわめて慎重を要するが、依頼に応じないということは問題である。

Q88. 個人情報を外部委託する場合に交わす条項には何がありますか。(複数回答)

回答件数		718	
1	秘密保持義務	297	41.4
2	責任分担	77	10.7
3	個人情報の適正な管理	177	24.7
4	その他	11	1.5
5	外部委託を行っていない	303	42.2
無回答		100	13.9

回答について特に問題と考えられることはない。「外部委託を行わない」が約4割あるのは正常なことと思われる。また秘密保持と個人情報の適正な管理を合わせると個人情報の取り扱いには十分な配慮がなされていると考えられる。

その他の意見としては「再委託の禁止」、「第三者への提供、目的外使用、複写等の禁止」、「返却・廃棄義務」等があげられた。

Q89.（財）日本情報処理開発協会の「プライバシーマーク制度」（平成10年4月運用開始）を知っていますか。（複数回答）

回答件数		718	
1	知っている	290	40.4
2	知らない	352	49.0
3	プライバシーマークを利用したい	24	3.3
4	利用したいと思わない	6	0.8
無回答		61	8.5

JIPDECが運用しているの『プライバシーマーク制度』を「知っている」との回答は全体の約4割と、前回調査から比べ倍増した。しかしながら、本質問に関連して、Q5で『JIS Q 15001 規格　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』の周知度に対する質問をしているが、その回答のうち、「知っている」は26.0%にとどまっており、個人情報保護に対する公的取組み自体に対する周知度はまだあまり高くないと思われる。

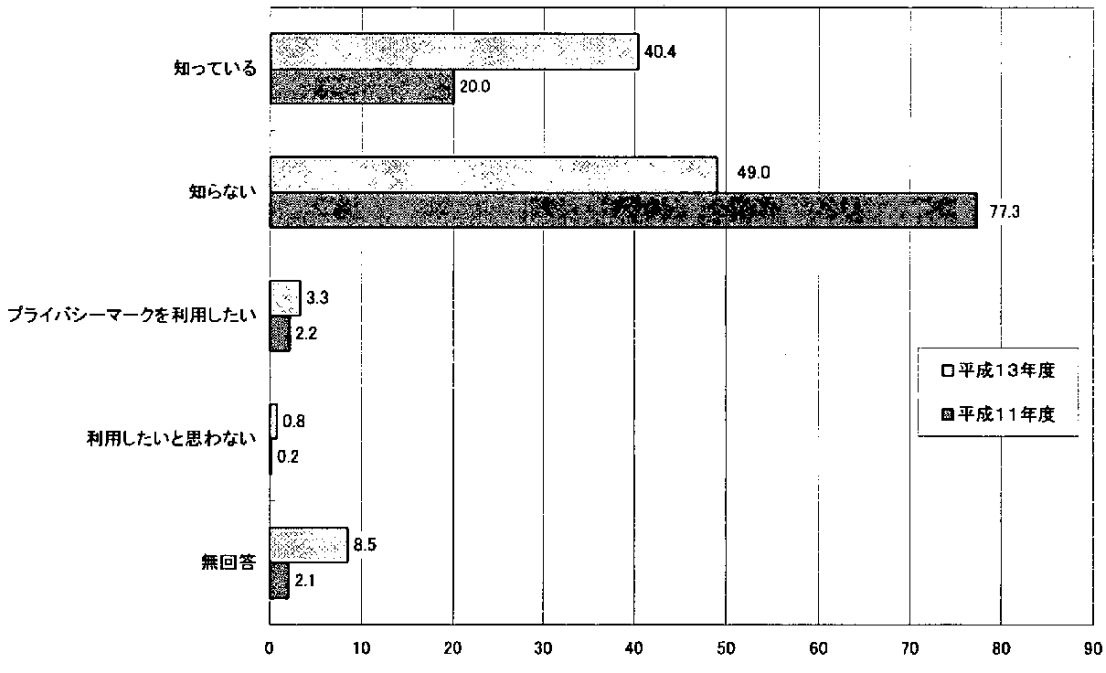


図2－10－2. プライバシーマーク制度の認知度

Q79において個人情報の利用に対し比較的高い回答率の得られた業種のうち、情報処理サービスで78.4%が「知っている」と回答したほかは、あまり高い回答率が得られていない。個人情報の利用がもっとも多い金融・保険業は48.8%、「商業」においては、32.5%という結果となった。

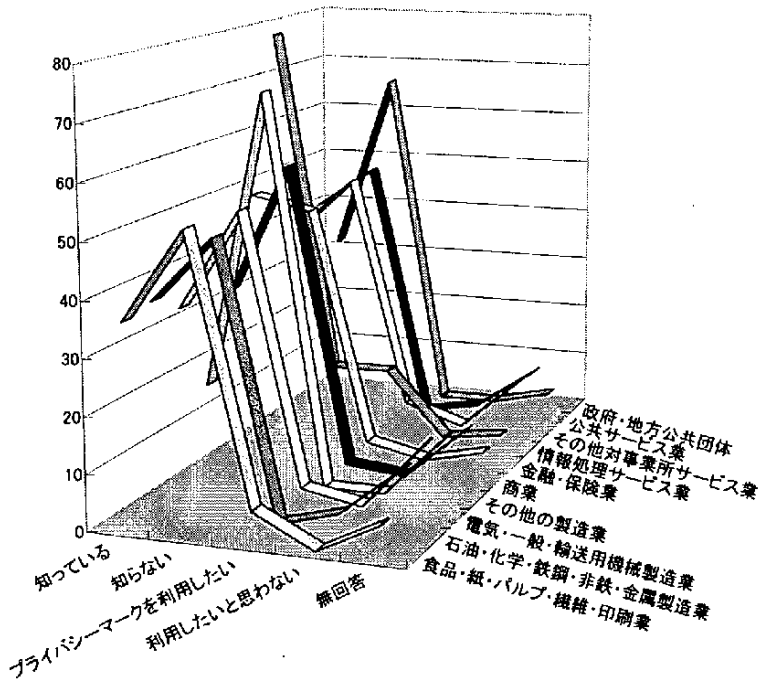


図2－10－3. プライバシーマーク制度の認知度（業種グループ別）

2.11 その他

ここでは、「今後必要と思われる情報セキュリティ制度・機能・製品等」ならびに「各事業体で実施している情報セキュリティ対策の問題点」についての意見を抜粋して紹介する。

（必要と思われる制度・機能、製品等）
・情報セキュリティ監査制度
・情報セキュリティ対策の実施基準と評価基準
・情報セキュリティにおける定量的かつ簡便なリスク分析手法、リスク分析ソフト
・LAN環境でのユーザ認識システム
・インターネットサイトと社内におけるセキュリティ診断サービス
・情報セキュリティポリシーチェックソフトの導入
・総合的に管理、監視できる改ざんチェックツール、ログ監視ツール、ウイルス検知ツール
・電子メール等で広まる恐れのあるウイルスに対するプロバイダ等による検知・駆除（プロバイダへの義務付け）　　等。

（情報セキュリティ対策の問題点）
・全社的な協力が得られない
・責任の所在が不明確である。緊急時の行動規程がなく、その都度対応しているため、万一の場合、被害甚大の恐れがある
・従業員の情報セキュリティに対する認識不足
・情報セキュリティポリシーが策定されていない
・体制が整っていない
・情報技術の急激な進展に対する人材の育成
・必要以上の対策に対するコスト増大　　等。

3．クロス集計結果の分析

3.1　クロス集計の概要

今年度は情報セキュリティに関し、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。

Q２－１．ＩＰＡがコンピュータウイルス被害の届出機関であることを知っていますか。

コンピュータウイルスの被害を受けたとき、IPA への届出率は低く、施策の認知度との関係を分析するため、以下の質問との間でクロス集計を行った。

×Q55. コンピュータウイルス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

クロス集計では、届け出を出さない事業体の 77.3%が IPA が届出機関であることを知っており、届け出を出さない理由として、施策の認知度以外にもあることが推測される。

Q２－２．ＩＰＡが不正アクセス被害の届出機関であることを知っていますか。

不正アクセスの被害を受けたとき、IPA への届出率は低く、施策の認知度との関係を分析するため、以下の質問との間でクロス集計を行った。

×Q44. 不正アクセス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

クロス集計では、届けを出さない事業体の 72.3%が IPA が届出機関であることを知っており、届け出を出さない理由として、施策の認知度以外にもあることが推測される。

Q５．「JIS Q 15001 規格　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を知っていますか？

『プライバシーマーク制度』の認知度が個人情報保護施策に対する認知度の影響を受けていることが推測され、以下の質問との間でクロス集計を行った。

×Q87.（財）日本情報処理開発協会の「プライバシーマーク制度（平成 10 年４月開始）を知っていますか？

『JIS Q 15001』に対する認知度と『プライバシーマーク制度』に対する認知度との間には関連がみられ、個人情報保護施策に関する認知度がプライバシーマーク制度に対する認知度に影響しているものと思われる。

Q８．貴社の基幹システムはどのように運用されていますか。

基幹システムの形態が、事業体の情報セキュリティマネジメントに対して何らかの影響を与えるのではないか、との仮説から、以下の質問との間でクロス集計を行った。

×Q14．過去１年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。
×Q15．基幹システムにおけるMTBF（平均故障間隔）は何時間ですか。
×Q16．基幹システムにおけるMTTR（平均修理時間）は何分ですか。
×Q18-①貴社では経営理念に基づくセキュリティポリシーを定めていますか。
×Q18-②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。
×Q19-①セキュリティポリシーを定期的に見直していますか。
×Q19-②実施手続・規程類は定期的に見直していますか。
×Q22-①基幹システムのネットワーク管理者を定めていますか。
×Q22-②情報システムの管理責任者を定めていますか。
×Q22-③貴社には専任のセキュリティ管理者または担当者がいますか。
×Q29．非常事態に備えて従業員に対してセキュリティの面から訓練を実施していますか。
×Q30．情報システムの災害に対する復旧対策としてどのようなことを実施していますか。実施している対策を選んで下さい。
×Q32.情報システムには代替運転機能を設けていますか。現在設置している機能を選んで下さい。
×Q39．システム災害・障害対策についての問題点は何ですか。
×Q40．どのようなネットワーク機器、サービスの障害を想定していますか。
×Q52．貴社では不正アクセス対策について従業員に教育・訓練の場を設けていますか。

クロス集計の結果、Q14、Q15、Q16、Q18-①、Q18-②、Q19-①、Q22-②、Q30、Q32、Q39、Q52については、それぞれのシステム形態により有為の差が認められた。

Q24．情報セキュリティ管理についての問題点は何ですか。

情報セキュリティポリシーおよび実施手続・規程類を見直すにあたり、情報セキュリティ管理上の問題点を把握していることが前提にあるとの仮説を立て、以下の質問との間でクロス集計を行った。

×Q19-①情報セキュリティポリシーは定期的に見直していますか。
×Q19-②実施手続・規程類は定期的に見直していますか。

クロス集計の結果、情報セキュリティポリシーについて「見直しを行っている」事業体の場合、「経営者層の理解が得られない」、「情報セキュリティ管理が事業の国際化に見合っていない」がともに 75.0％と高い割合となった。また、実施手続・規程類の場合は、「見直しを行っている」

事業体の場合、「要求に合致するもの（サービス）がない」、「組織の従業員に対する教育・訓練がいきとどかない」、「コスト問題」が８割前後を占めている。

Q44. 不正アクセス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

不正アクセス被害にあった場合の被害届の状況と従業員に対する教育・訓練の実施状況との関連性についてクロス集計を行った。

×Q52. 貴事業体では、従業員に対し、不正アクセス対策に関する教育・訓練の場を設けていますか。

不正アクセス被害にあった事業体(110 件) のうち、IPA に届け出を出したのは 25 件である。このうち、「定期的に実施している」場合、8.0%、「時々実施している」が 12.0%、「情報セキュリティポリシー等に従って実施している」は 16.0%と、いずれも低い値となった。

Q60. 貴事業体では、従業員に対し、コンピュータウイルス対策に関する教育・訓練の場を設けていますか。

コンピュータウイルスに対し、従業員がその脅威を十分知らない場合にウイルス感染の割合が高くなるのではないか、との仮説を立て、従業員に対する教育・訓練の実施状況と感染被害の関連性について以下の質問との間でクロス集計を行った。

×Q54. コンピュータウイルスに感染したことがありますか。

感染経験のある 494 件のうち、教育・訓練を「実施していない」のが 57.7%と高く、教育・訓練の意味を明示しているといえる。

Q62. 情報セキュリティ要素 1～10 のうち、貴事業体にとって重要と思われる要素を３つ選び、下の回答欄に優先順位をつけて記入して下さい。

情報セキュリティ要素 10 のうち重要と思われる上位３つのうち、第１位と第２位との関連についてクロス集計を行った。ここでは、第１位と第２位の組み合わせからの分析、情報セキュリティポリシー選択の特異性、そのたの特徴についてとりまとめた。

第１位と第２位の組み合わせに関しては、第１位として最も多く選択された「情報セキュリティポリシー」(219 件) の場合、第２位には、「通信および運用管理」(122 件)、「情報セキュリティ組織」(99 件) が多く、上位３つまでが情報セキュリティ関連要素で占められた。

次に、Q62で情報セキュリティの要素の優先順位の選択と次の各質問についてのクロス集計分析を行った。

×Q18-①貴社では経営理念に基づくセキュリティポリシーを定めていますか。
×Q18-②貴社では経営理念に基づく実施手続き・規程類を定めていますか。
×Q22-①基幹システムのネットワークの管理について責任を有する担当者を定めていますか。
×Q22-②情報システムの管理について責任を有する担当者を定めていますか。
×Q22-③情報セキュリティの管理について責任を有する担当者を定めていますか。
×Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。
×Q29. 非常事態に備えて従業員に対し情報セキュリティの面から訓練を実施していますか。
×Q52. 貴事業体では不正アクセス対策について従業員に教育・訓練の場を設けていますか。
×Q60. 貴事業体ではコンピュータウイルス対策について従業員に教育・訓練の場を設けていますか。
×Q34. コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所ではそれぞれどのような火災対策をとっていますか。各場所ごとに実施している対策を選んで下さい。
×Q41. どのようなネットワーク障害対策を実施していますか。実施している対策項目を選んで下さい。
×Q48. 貴社では基幹システムのパスワード変更をどのレベルに設定していますか。
×Q65. 情報システムに係わるリスク分析を実施していますか。
×Q69. システム監査を実施していますか。

情報セキュリティポリシーや実施手続・規程類を「作成中」または「作成を検討中」の事業体は「情報セキュリティポリシー」を情報セキュリティ要素として第1位にあげている割合が高く、すでに「定めている」事業体よりも注目されていると思われる（Q18）。

ネットワーク管理、情報システム管理、情報セキュリティ管理の担当者を定めている場合、共通して「情報セキュリティポリシー」を第1位に、「情報セキュリティ組織」、「人的セキュリティ」、「通信および運用管理」を第2位に選択している事業体が多い（Q22）。

非常事態の発生を想定した危機管理マニュアルの策定と「事業継続計画」の選択状況については、マニュアルを作成している事業体ほど「事業継続計画」を選択する割合が高い（Q27）。

非常事態に備えた従業員に対する情報セキュリティ面からの訓練の実施と「人的セキュリティ」の選択状況については、現状では訓練の実施の有無と「人的セキュリティ」の選択に大差がない（Q29）。

不正アクセス対策に関する従業員の教育・訓練の実施状況と「人的セキュリティ」および「アクセス制御」との関係については、情報セキュリティポリシーや対策基準類に従って教育・訓練を実施している事業体では「人的セキュリティ」、「アクセス制御」を選択する割合が高い（Q52）。

コンピュータウイルス対策に関する従業員の教育・訓練の実施状況と「通信および運用管理」との関係については、教育を実施していないからこそ「通信および運用管理」を重視している事業体と、情報セキュリティポリシーや対策基準類に従って実施している事業体で高い割合となった（Q60）。

コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所での火災対策の実施状況に対し、重要要素ごとの平均を上回っている要素の比較を行った（Q34）。

コンピュータ室では、第１位に「情報セキュリティポリシー」を選択した場合、７項目の火災対策のうち５つで対策率が平均を上回っている。同様に、データ保管場所では４つ、ネットワーク設備室の場合は７つの火災対策すべて、コンピュータ設置場所では６つで対策率が平均を上回っている。

第１位の重要要素ごとにネットワーク障害対策の実施状況で平均を上回っているものを分析した。その結果、情報セキュリティポリシーを選択した場合、12 項目の対策のうち、平均を上回っていたのは 10 項目であり、次に多かったのは「物理的および環境的セキュリティ」、「準拠」がともに８項目であった（Q41）。

基幹システムのパスワード変更について、それぞれの選択肢と「情報セキュリティポリシー」および「アクセス制御」で平均を上回っているものを分析した。その結果、「アクセス制御」に関しては「パスワードに関して特に定めていない」とする回答が４割を超えており、関心が高い層と対応がとれていないことを認識している層が混在している（Q48）。

リスク分析の実施状況と各重要要素との関連について分析を行った。その結果、リスク分析を行っているとの平均回答（18.8％）を上回っている要素として、「情報資産の分類および管理」が最も多く、25.4％であった（Q65）。

システム監査の実施状況と各重要要素との関連について分析を行った結果、「準拠」が最も多く 54.5％、次いで「物理的および環境的セキュリティ」（50.0％）という結果となった（Q68）。

Q63. 情報セキュリティの確保にとり基本的に重要な視点は何だと思いますか？

前回調査において、情報セキュリティの確保にとり基本的に重要な視点として「経営者層の理解」、「管理者の理解」、「担当者の理解」、「社内全体の理解」、「法規制の整備」の５項目を挙げ、その中で「経営者層の理解」が重要と回答した事業体ほど、情報セキュリティ確保に向けた取り組みが進んでいるであろうと仮説の基、分析を行った。結果として各５項目の回答に差があまり見られなかったため、今年度も同様の分析を行った。

×Q22-①ネットワーク管理について、責任を有する担当者を定めていますか。
×Q22-②情報システムの管理について、責任を有する担当者を定めていますか。
×Q22-③情報セキュリティの管理について、責任を有する担当者を定めていますか。
×Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。
×Q29. 非常事態に備えて従業員に対してセキュリティの面から訓練をしていますか。
×Q65. 情報システムに係わるリスク分析を実施していますか。
×Q70. 情報システム関連のリスクが倒産に結びつくと思いますか。

全体的にみて、前回調査での傾向とあまり変わらず、各対策を実施している方が実施していない方よりも回答率が高い傾向にある。また、各対策とも「社内全体の理解」＞「経営者層の理解」＞「管理者の理解」＞「担当者の理解」＞「法規制の整備」の順で重視していることがわかる。

Q69. システム監査を実施していない理由は何ですか。

経営理念に基づき情報セキュリティポリシーを定める事業体であれば、システム監査に関して理解が深く、したがってシステム監査を実施する傾向が高いと思われる。また逆の傾向も考えられる。そこで、システム監査を実施していない回答について、その実態を考察してみた。

×Q18. 貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。

×Q65.情報システムに係わるリスク分析を実施していますか。

×Q70. 情報システム関連のリスクが倒産に結びつくと思いますか。

情報セキュリティポリシーを策定していない事業体がシステム監査を実施しない理由として、「経営者層が重要性を認識していない」(55.6%)、「効果が明確でない」(55.3%)、「適切なシステム監査人が見つからない」(51.7%) がそれぞれの回答数の半数以上となった (Q18)。

情報システムのリスク分析を行っていない事業体がシステム監査を実施しない理由として、「効果が明確でない」(93.5%)、「経営者層が重要性を認識していない」(92.6%)、「システム監査実施のためのコンセンサス、組織風土が十分に備わっていない」(90.4%) がそれぞれの回答数の９割を超えている (Q65)。

システム監査未実施の理由別に情報システム関連リスクが倒産に結びつくかの影響度をみた場合、「システム監査実施のためのコンセンサス、組織風土が十分備わっていない」に関しては、影響の有無による差がみられなかった (Q70)。

3.2 Q2のクロス集計

Q2－1．IPAがコンピュータウイルス被害の届出機関であることを知っていますか。

ウイルス対策の一環として、コンピュータウイルスの被害を受けた時に、IPA に届け出を出すことがコンピュータウイルス対策基準で定められている。したがって、このことを知っている事業体であれば、被害を受けた際に IPA に対し被害届を出していると仮定した。そこで実際に被害にあった事業体がどれだけ IPA のことを知っているか、クロス集計を行った。

×Q55．コンピュータウイルス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

（左欄：件数／右欄：%、以下同じ）

	回答数	出した		出さない		無回答	
知っている	401	93	23.2	299	74.6	9	2.2
知らない	87	4	4.6	83	95.4	0	0.0
無回答	6	1	16.7	5	83.3	0	0.0
計	494	98	81.2	389	78.3	9	1.8

	回答数	知っている		知らない		無回答	
出した	98	93	94.9	4	4.1	1	1.0
出さない	387	299	77.3	83	21.4	5	1.3
無回答	9	9	100.0	0	0.0	0	0.0
計	494	401	81.2	87	17.6	6	1.2

Q54 でコンピュータウイルスの被害にあったと回答した 494 事業体のうち、IPA に届け出たのは 19.8%にすぎない。Q2 において IPA がコンピュータウイルス被害届出機関に指定されていることに関して、その認知度を調査した結果、「知っている」との回答が 76.7%と高い数値となった。しかしながら、クロス集計の結果、実際の届け出率は低い。クロス集計を見ると、届け出を出さない事業体の 77.3%が IPA が届出機関であることを知っており、届け出を出さない理由が、PR 不足以外にあることがわかる。

Q2－2．IPAが不正アクセス被害の届出機関であることを知っていますか。

不正アクセス対策の一環として、不正アクセスの被害を受けた時に、IPA に届け出を出すことがコンピュータ不正アクセス対策基準で定められている。したがって、このことを知っている事業体であれば、被害を受けた際に IPA に対し被害届を出していると仮定した。そこで実際に被害にあった事業体がどれだけ IPA のことを知っているか、クロス集計を行った。

×Q44. 不正アクセス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

	回答数	出した		出さない		無回答	
知っている	87	25	28.7	60	69.0	2	2.3
知らない	22	0	0.0	22	26.5	0	0.0
無回答	1	0	100.0	1	100.0	0	0.0
計	110	25	22.7	83	75.5	2	1.8

	回答数	知っている		知らない		無回答	
出した	25	25	100.0	0	0.0	0	0.0
出さない	83	60	72.3	22	26.5	1	1.2
無回答	2	2	100.0	0	0.0	0	0.0
計	110	87	79.1	22	20.0	1	0.9

Q43で不正アクセスの被害にあったと回答した110事業体のうち、IPAに届け出たのは22.7%であった。Q2においてIPAが不正アクセス被害届出機関に指定されていることに関して、その認知度を調査した結果、「知っている」との回答が71.0%であったが、実際の届け出率は低い。クロス集計を見ると、届け出を出さない事業体の72.3%がIPAが届出機関であることを知っており、届け出を出さない理由が、PR不足以外にあることがわかる。

3.3 Q5のクロス集計

Q5．「JIS Q 15001 規格　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を知っていますか？

Q87 において、JIPDEC の『プライバシーマーク制度』を「知っている」と回答した事業体は40.4%であった。そこで、『JIS Q 15001』と『プライバシーマーク制度』の関連について分析した。

×Q87.（財）日本情報処理開発協会の「プライバシーマーク制度（平成10年4月開始）を知っていますか？（複数回答）

JIS ＼ 制度	回答数	知っている		知らない		その他	
利用している	40	36	90.0	2	5.0	6	15.0
知っている	187	125	66.8	44	23.5	24	12.8
知らない	477	124	26.0	298	62.5	60	12.6
無回答	14	5	35.7	8	57.1	1	7.1
計	718	290	40.4	352	49.0	91	12.7

制度 ＼ JIS	回答数	利用している		知っている		知らない		無回答	
知っている	290	36	12.4	125	43.1	124	42.8	5	1.7
知らない	352	2	0.6	44	12.5	298	84.7	8	2.3
その他	91	6	6.6	24	26.4	60	65.9	1	1.1
計	718	40	5.6	187	26.0	477	66.4	14	1.9

（注）その他には「プライバシーマークを利用したい」、「利用したいと思わない」「無回答」の合計値

『JIS Q 15001』を「利用している」と回答した事業体において、『プライバシーマーク制度』を「知っている」と回答した事業体は90.0%と高い割合となった。これは、プライバシーマーク取得にあたり『JIS Q 5001』に準拠したコンプライアンスプログラムの作成が義務づけられていることから、マークをすでに取得している、または取得の準備を行っている事業体がこの中に含まれていることが想定される。

3.4 Q８のクロス集計

Q８．貴社の基幹システムはどのように運用されていますか。

基幹システムの形態が異なった場合に、セキュリティ面での違いが見られるかを検証するために、Q８の集中型・集中分散型・分散型のシステム形態と、次の各質問についてのクロス集計分析を行った。

×Q14.過去１年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。（複数回答）
×Q15. 基幹システムにおけるMTBF（平均故障間隔）は何時間ですか。（回答件数388件）
×Q16. 基幹システムにおけるMTTR（平均修理時間）は何分ですか。（回答件数388件）
×Q18-①貴社では経営理念に基づくセキュリティポリシーを定めていますか。
×Q18-②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。
×Q19-①セキュリティポリシーを定期的に見直していますか。
×Q19-②実施手続・規程類は定期的に見直していますか。
×Q22-①基幹システムのネットワーク管理者を定めていますか。
×Q22-②情報システムの管理責任者を定めていますか。
×Q22-③貴社には専任のセキュリティ管理者または担当者がいますか。
×Q29. 非常事態に備えて従業員に対してセキュリティの面から訓練を実施していますか。
×Q30. 情報システムの災害に対する復旧対策としてどのようなことを実施していますか。実施している対策を選んで下さい。
×Q32.情報システムには代替運転機能を設けていますか。現在設置している機能を選んで下さい。
×Q39. システム災害・障害対策についての問題点は何ですか。（複数回答）
×Q40. どのようなネットワーク機器、サービスの障害を想定していますか。（複数回答）
×Q52. 貴社では不正アクセス対策について従業員に教育・訓練の場を設けていますか。

この結果、Q14、Q15、Q16、Q18-①、Q18-②、Q19-①、Q22-②、Q30、Q32、Q39、Q52については、それぞれのシステム形態により有為の差が認められた。しかし、集中型・集中分散型・分散型の順にセキュリティのレベルが低くなっているとは限らず、ある質問については集中型と集中分散型が一つのグループを作り、違う質問では集中分散型と分散型が一つのグループを作るといったことが見られた。

×Q14.過去１年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。（複数回答）

システムダウンの原因として多く上げられた主要項目で、システム形態により顕著な差が見られるのは、自然災害／電源障害／通信事業者／ネットワーク機器／ハードウェア／OS障害／ソフトウェア障害／コンピュータウイルス／オペミス等人の過失による事故等の９項目である。

(%)

	集中型	集中分散型	分散型
自然災害	1.7	5.7	5.7
電源障害	8.7	14.5	14.8
通信事業者	4.8	8.3	8.2
ネットワーク機器	16.1	25.4	35.2
ハードウェア	21.7	36.8	44.3
OS 障害	5.6	11.4	9.0
ソフトウェア障害	17.2	20.2	15.6
コンピュータウイルス	4.8	11.0	15.6
オペミス等人の過失による事故	9.9	13.2	7.4

まず、集中型は従来からのデータセンターでの運用が多く、ほとんどの項目で集中分散型や分散型に比べてシステムダウンの原因となった割合が小さかった。特に「自然災害」と「コンピュータウイルス」では３分の１、「電源障害」、「通信事業者」、「ネットワーク」、「ハードウェア」、「OS 障害」については、集中型が集中分散型や分散型に比べて２分の１の数字になっている。これは、従来からのデータセンターの建物が自然災害に対し堅牢に作られていることや、設備面でも電源障害に対する無停電装置の設置といった対策がとられている結果である。また複数の通信事業者を使ったり、ハードウェアやネットワーク機器に見られるように二重化等により信頼性の設計値が高いことが顕著に表れたものと考えられる。

また、「OS 障害」については複雑な構成になる集中分散型が高く、OS の種類が少ない分散型の方が少なくなっている。ここでも、使用実績が最もあり、基幹系での歴史が長い集中型が非常に障害が少なくなっている。「ソフトウェア障害」は、ユーザ側がどの程度の品質の作り込みをするかが結果として出てきており、集中型／分散型／集中分散型の順で多くなっている。「オペミス等」は運用の作業が少ない分散型が最もよく、集中分散型は構成が複雑になるためか一番悪い数字になっている。今後、集中分散型についても、集中型で使われている自動運用ツール等を導入することで、オペミス等を減らす必要がある。

×Q15. 基幹システムにおけるＭＴＢＦ（平均故障間隔）は何時間ですか。

	集中型	集中分散型	分散型
平均 MTBF	2,917 時間	3,244 時間	2,569 時間

システム形態別に MTBF の平均時間をとると、次の表のようになった。時間的には、集中分散型／集中型／分散型の順に短くなっており、前回の結果と比べると集中型と集中分散型の順位が逆転した。特に、MTBF が 10,000 時間を超える領域になると、集中分散型で１件しかなく、これが逆転を象徴している。

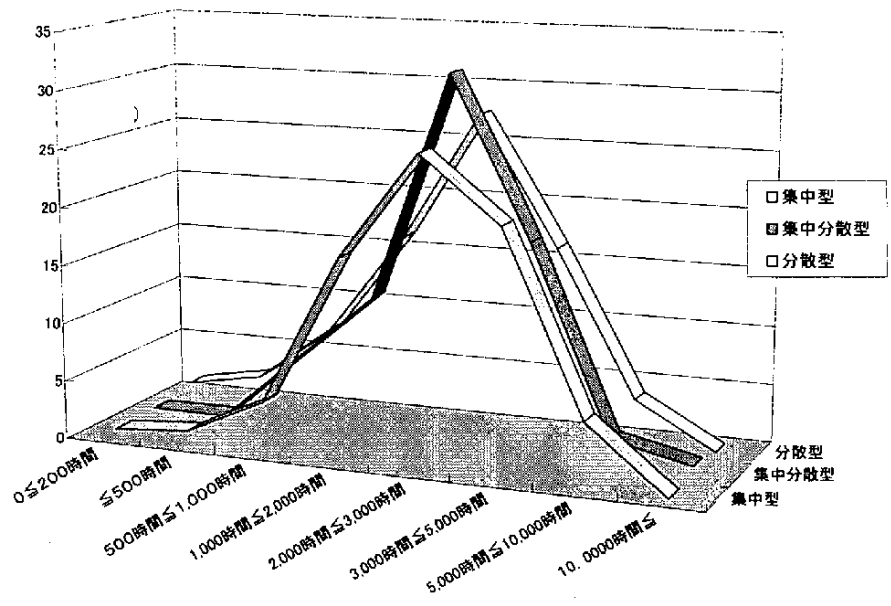


図3－4－1. 基幹システムの処理形態別MTBF

×Q16. 基幹システムにおけるMTTR（平均修理時間）は何分ですか。

	集中型	集中分散型	分散型
平均MTTR	135分	159分	151分

システム形態別にMTTRの平均時間を取ると、次の表のようになった。各形態とも平均すると2時間半程度と考えられる。これは、形態にかかわらず2時間程度を復旧の目処として設計した結果と思われる。

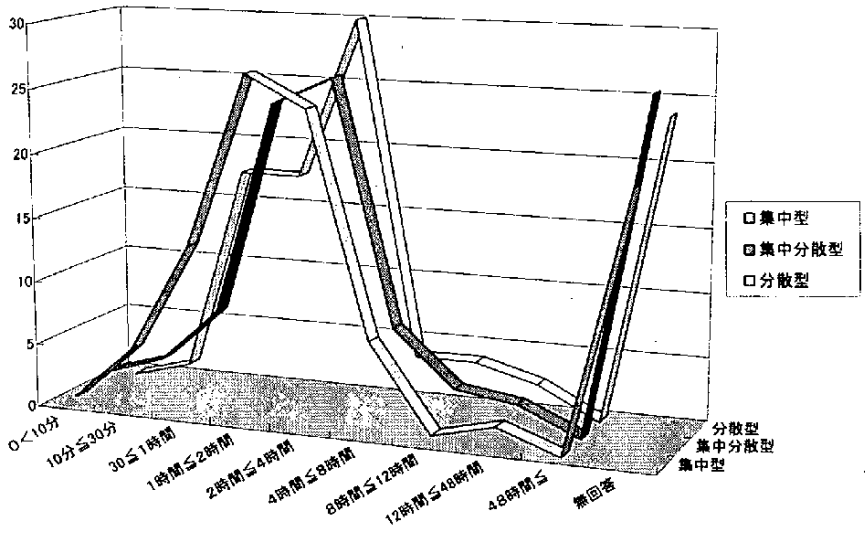


図3－4－2. 基幹システムの処理形態別MTTR

×Q18-①貴事業体では経営理念に基づくセキュリティポリシーを定めていますか。

（%、以下同じ）

	集中型	集中分散型	分散型
セキュリティポリシーが定められている。	25.4	22.8	20.5
セキュリティポリシーを作成中である。	11.0	14.0	14.8

システム形態別にセキュリティポリシーを定めているかを見ると、前回調査では集中型よりも集中分散型や分散型の方がセキュリティポリシーを「定めている」率が高かったが、今回は集中型が巻き返し定めている率が一番高くなった。これに、セキュリティポリシーを「作成中」の回答を加えると、どの処理形態も36%程度になり大きな差は見られなくなる。しかし「作成を検討中」が28.9%、「定めていない」が32.9%あり、セキュリティーポリシーの一層の普及に向けての努力が必要なことを示している。

×Q18-②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。

	集中型	集中分散型	分散型
実施手続・規程類を定めている	22.3	23.7	18.9
実施手続・規程類を作成中である	14.4	10.6	11.3

システム形態別に、セキュリティに関する実施手続・規程類を定めているかをみると、すでに「定めている」のは集中分散型／集中型がほぼ同じで割合で、分散型が少し少なくなっている。「作成中」と合わせた数字で考えても集中型／集中分散型が35%程度で、分散型の30%程度と差がある結果となった。セキュリティポリシーだけあっても、実施手続・規程類が整備されないと、セキュリティレベルの向上は望めないので、実施手続・規程類についても、普及に向けての努力が必要である。

×Q19-①セキュリティポリシーを定期的に見直していますか。

	集中型	集中分散型	分散型
定期的に見直している。	67.8	71.2	60.0

システム形態別に、セキュリティポリシーを定期的に見直しているかをみると、集中分散型／集中型／分散型の順になり、かつ分散型の数字が小さくなっている。新しい感染メカニズムを持ったウイルスの発生や不正侵入の新しい手口が毎日のように発生しているので、セキュリティポリシーも、定期的に見直すことが必要である。

×Q22-①基幹システムのネットワーク管理者を定めていますか。

	集中型	集中分散型	分散型
定めている	78.0	82.9	73.8
現在検討中である	8.7	7.5	13.1

基幹システムのネットワーク管理者を定めているかをみると、ネットワークに依存する率が高い集中分散型が一番高く、ついで集中型／分散型が高くなっている。しかし、検討中の数字を合わせると、すべて87%～90%となるので、次回にはほとんどの企業がネットワーク管理者を定めていると予想される。

×Q30. 情報システムの災害に対する復旧対策としてどのようなことを実施していますか。実施している対策を選んで下さい。

	集中型	集中分散型	分散型
手作業への復帰	30.1	31.1	22.13
バックアップサービス業者と契約	7.9	10.1	1.6
別の場所にバックアップセンタを設置	10.4	7.9	8.2
バックアップファイルを専門業者に委託して保管	21.7	21.1	14.8
サーバのファイルは、遠隔地にミラーファイルを保持	2.5	6.1	9.0
PC 中の業務用ファイルのバックアップを遠隔地に保管	3.1	2.6	1.6

情報システムのバックアップ対策として、「手作業での復帰」を採用しているのは、集中型と集中分散型に多く、分散型では約３分の２になっている。これは、集中型と集中分散型が規模の大きな組織で採用されており、内部統制のレベルも高いためと思われる。また、広域災害に対応できる「バックアップサービス業者との契約」、「バックアップセンターの設置」、「バックアップファイルの専門業者への委託保管」も、集中型と集中分散型で多く、分散型をとる組織での対応が遅れている。一方、「サーバのファイルを遠隔地にネットワークで保管する」、「リモートミラーリング」は、分散型での利用率が高くなっている。これは、データの容量が大きく影響していると思われる。

×Q32. 情報システムには代替運転機能を設けていますか。現在設置している機能を選んで下さい。

	集中型	集中分散型	分散型
ホットスタンバイシステム	20.8	14.5	8.2
クラスタリング	8.7	13.2	20.5
ミラリング	35.5	47.4	55.7
フォールトトレラント	5.6	5.3	7.4

情報システムの代替運転機能として何が使えるかは、ハードウェアやOSに依存するところが大きい。「ホットスタンバイシステム」が集中型、集中分散型、分散型の順で実施されているのは、ハードウェアとOSの機能性による。一方、「ディスクのミラリング」は、すべてのシステム形態

において採用が増加しており、集中分散型と分散型の方が集中型よりも多くなっているのは、RAID技術の採用が分散型で進んでいるためと思われる。（前回調査での「ミラリング」の利用は32.2%であったが、今回の調査では42.5%と大きく伸びている。）また、「フォールトトレラント」の利用率では、分散型が高かったが、これはハードウェアに依存した結果と考えられる。

×Q39. システム災害・障害対策についての問題点は何ですか。（複数回答）

	集中型	集中分散型	分散型
経営者の理解が得られない。	12.1	10.5	15.6
要員に対する教育・訓練が行き届かない	25.8	20.2	20.5
どこまでやるかの基準が示されていない	35.5	43.9	37.7
要求に合致する製品がない	1.4	2.2	4.1

この質問の回答率で高かったのは、「コスト」（72.1%）、「どこまでやるかの基準」（38.6%）、「ノウハウ不足」（31.8%）、「要員の作業負荷」（24.0%）、「要員の教育・訓練」（23.8%）の５項目である。これらのうち、「コスト」、「ノウハウ不足」、「要員の作業負荷」については各形態別の差が少なかった。一方、「どこまでやるかの基準」と「要員の教育・訓練」ではシステムの形態による差があるが、全体として特定の形態で問題点が多いという傾向は見られなかった。

×Q52. 貴社では不正アクセス対策について従業員に教育・訓練の場を設けていますか。

	集中型	集中分散型	分散型
セキュリティ教育を実施	18.3	31.1	18.1
セキュリティ教育を実施していない	82.7	68.9	82.9

不正アクセス対策についての教育・訓練は、集中分散型が集中型／分散型に比べて、1.5 倍の実施率となっている。しかし、最も実施率の高い集中分散型でも31.1%であり、残りの68.9%は実施していない。この数値は、コンピュータウイルス対策の教育実施率の 26%に比べても低く、早急な改善が必要である。特に今後の個人情報保護法の施行を考えると、従業員に対してセキュリティポリシーに基づいて教育を実施していかないと、個人情報の保護が不十分と判断されることも考えられる。

3.5 Q24 のクロス集計

Q24. 情報セキュリティ管理についての問題点は何ですか

情報セキュリティポリシーおよび実施手続・規程類を見直すという判断には情報セキュリティ管理についての問題点を十分見極めているといった仮説を立て、クロス回答からこの傾向を捉えてみることにする。

×Q19-①情報セキュリティポリシーは定期的に見直していますか。

	回答数	いる		いない	
経営者層の理解が得られない	12	9	75.0	2	16.7
コストがかかりすぎる	83	57	68.7	16	19.3
組織の従業員に対する教育・訓練がいきとどかない	114	77	67.5	23	20.2
組織の従業員に対する負担がかかりすぎる	33	18	54.5	10	30.3
ノウハウが不足している	56	30	53.6	18	32.1
どこまでやればよいのか基準が示されていない	58	38	65.5	14	24.1
要求に合致するもの(サービス)がない	4	2	50.0	1	25.0
組織の従業員に倫理観が乏しく、情報を財産と認識する風土がない	20	12	60.0	6	30.0
情報セキュリティ管理が事業の国際化に見合っていない	4	3	75.0	1	25.0
その他	10	4	40.0	5	50.0
特に問題はない	7	6	85.7	1	14.3
計	172	115	66.9	38	22.1

定期的に見直しているグループは見直していないグループに対していずれの項目においても高い割合を示している。見直しグループの回答数は 12 と少ないが、その 75.0%は「経営者層の理解が得られない」としている。「コストがかかりすぎる」(回答数 83) については、見直しグループでは 68.7%と高い割合となっている。特に回答数が 114 件と多かった「組織の従業員に対する教育・訓練がいきとどかない」では 67.5%、次いで回答の多かった「どこまでやればよいのか基準が示されていない」(回答数 58) については 65.5%という結果であった。「ノウハウが不足している」(回答数 56) としているのも見直しグループでは 53.6%と相対的に高く、回答数の少ない「情報セキュリティ管理が事業の国際化に見合っていない」(回答数４) では 75.0%であった。こうした回答は、上記の仮説を裏づけていると思われる。

×Q19-②実施手続・規程類は定期的に見直しを行っていますか。

	回答数	いる		いない	
経営者層の理解が得られない	12	9	75.0	3	25.0
コストがかかりすぎる	79	64	81.0	12	15.2
組織の従業員に対する教育・訓練がいきとどかない	105	87	82.9	16	15.2
組織の従業員に対する負担がかかりすぎる	27	20	74.1	6	22.2
ノウハウが不足している	51	35	68.6	13	25.5
どこまでやればよいのか基準が示されていない	54	42	77.8	9	16.7
要求に合致するもの(サービス)がない	6	5	83.3	1	16.7
組織の従業員に倫理観が乏しく、情報を財産と認識する風土がない	20	15	75.0	5	25.0
情報セキュリティ管理が事業の国際化に見合っていない	5	5	100.0	0	0.0
その他	10	6	60.0	3	30.0
特に問題はない	6	5	83.3	1	16.7
無回答	35	32	91.4	3	8.6
計	159	127	79.9	27	17.0

この点については、見直しグループの回答は「情報セキュリティポリシー」の場合より明確に上記の仮説が読みとれる。ちなみに、見直しグループの「経営者層の理解が得られない」(回答数 12) での 75.0%はポリシーと同じであるが、「コストがかかりすぎる」(回答数 79) については、見直しグループでは 81.0%と高い割合となっている。回答数が 105 件と多い「組織の従業員に対する教育・訓練がいきとどかない」では 82.9%、次いで回答の多かった「どこまでやればよいのか基準が示されていない」(回答数 54)については 77.8%という結果であった。「ノウハウが不足している」(回答数 51) では 68.6%と相対的に高く、5件と回答数の少ない「情報セキュリティ管理が事業の国際化に見合っていない」の場合は 100.0%が回答している。

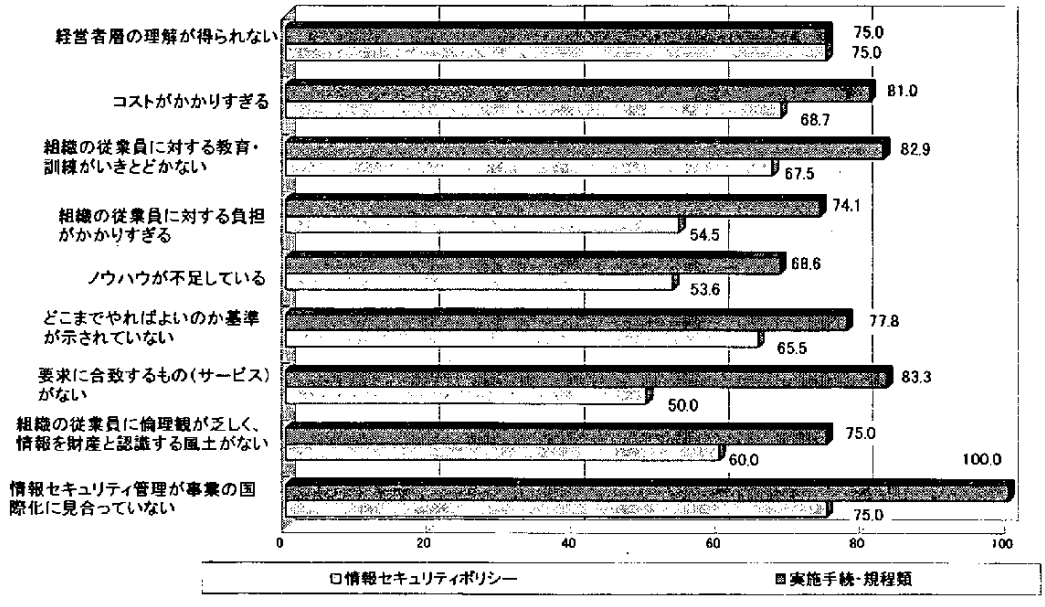


図3－5－1. 情報セキュリティ管理の問題点とポリシー類の見直し状況

3.6 Q44のクロス集計

Q44. 不正アクセス被害届機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

不正アクセスの被害にあった場合の対応は従業員の教育訓練に関係するものと思われる。この点から、IPAへの届け出の状況を考えてみることにする。

×Q52. 貴事業体では不正アクセス対策について従業員に教育・訓練の場を設けていますか。

教育・訓練 ＼ 被害届出	回答数	情報セキュリティ対策に関して定期的に実施している		社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している		情報セキュリティポリシーや対策基準類に従って実施している		その他		特に実施していない		無回答	
出した	25	2	8.0	3	12.0	4	16.0	5	20.0	11	44.0	0	0.0
出さない	83	4	4.8	8	9.6	9	10.8	5	6.0	55	66.3	2	2.4
無回答	610	18	3.0	46	7.5	67	11.0	28	4.6	435	71.3	16	2.6
計	718	24	3.3	57	7.9	80	11.1	38	5.3	501	69.8	18	2.5

教育・訓練 ＼ 被害届出	回答数	情報セキュリティ対策に関して定期的に実施している		社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している		情報セキュリティポリシーや対策基準類に従って実施している		その他		特に実施していない		無回答	
出した	25	2	8.3	3	5.3	4	5.0	5	13.2	11	2.2	0	0.0
出さない	83	4	16.7	8	14.0	9	11.3	5	13.2	55	11.0	2	11.1
無回答	610	18	75.0	46	80.7	67	83.7	28	73.6	435	86.8	16	88.9
計	718	24	3.3	57	7.9	80	11.1	38	5.3	501	69.8	18	2.5

IPAに届け出たのは25件であった。情報セキュリティ教育を「特に実施していない」が501件と圧倒的に多いが、実施していないグループの届け出件数は25件の44.0%（11件）であった。定期的に実施しているという24件の回答の場合、届け出たのは（25件中2件）8.0%、時々実施しているという回答57件については25件中3件（12.0%）、「情報セキュリティポリシーや対策基準に従って実施している」という80件のうちでは4件（16.0%）であった。

上記の結果から、届け出と従業員の教育訓練との関係は明らかではないように思われるが、「定期的に実施している」という24件については8.3%（2件）が届け出をし、「時々実施している」という回答57件については5.3%（3件）、「情報セキュリティポリシーや対策基準に従って実施している」という80件では5.0%（4件）であった。だが、「特に実施していない」501件の場合は他に比べて2.2%（11件）と低く、教育・訓練の意味を考えることが重要である。

3.7 Q60のクロス集計

Q60. 貴事業体では、従業員に対し、コンピュータウイルス対策に関する教育・訓練の場を設けていますか。

コンピュータウイルスに対し、従業員がその脅威を十分知らない場合にウイルス感染の割合が高くなるのではないか、との仮説を立て、従業員に対する教育・訓練の実施状況と感染被害の関連について、以下の質問との間でクロス集計を行った。

×Q54. コンピュータウイルスに感染したことがありますか。

教育 / 感染	回答数	情報セキュリティ教育に関し定期的に実施		社内教育用の情報セキュリティ教育カリキュラムに従って時々実施		情報セキュリティポリシーや実施手続、規程類に従って実施		その他		特に実施していない	
ある	494	23	4.7	54	10.9	62	12.6	57	11.5	285	57.7
ない	222	7	3.2	8	3.6	35	15.8	13	5.9	154	69.4
無回答	2	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
計	718	30	4.2	62	8.6	97	13.5	70	9.7	439	61.1

コンピュータウイルスに感染した経験がある回答494件について、対策に関する教育・訓練の関連をみると、「定期的に実施している」事業体では4.7%、「時々実施している」10.9%、「実施手順、規定類に従って実施している」12.6%であったが、これに対して、「実施していない」のが57.7%と高く、教育・訓練の意味を明示しているといえる。

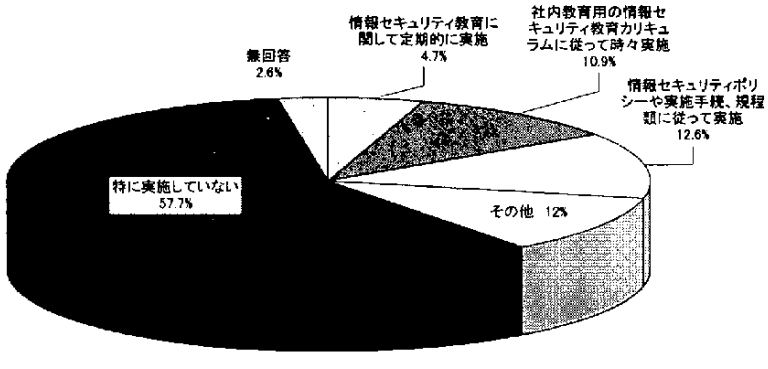


図3−7−1. ウイルス被害と従業員教育の実施状況

3.8 Q62 のクロス集計

Q62. 情報セキュリティ要素 1～10 のうち、貴事業体にとって重要と思われる要素を3つ選び、下の回答欄に優先順位をつけて記入して下さい。

3.8.1 Q62 のクロス集計

ここでは、情報リスクマネジメント関連について情報セキュリティ要素の 10 のうち重要なものと思われるものを上位３つ選択する質問について、第１位に選択した組織体が第２位に何を選択しているか、その関連について分析を行った。

表３－８－１．第１位と第２位の選択件数　（件）

情報セキュリティ要素		1位	2位
1	情報セキュリティポリシー(経営者の積極的な関与)	219	47
2	情報セキュリティ組織(情報セキュリティの推進組織の構築と活動)	73	99
3	情報資産の分類および管理(情報資産のリスク評価とそれによる重要度の分類)	43	61
4	人的セキュリティ(役職員への教育訓練や内部規則の策定など)	71	93
5	物理的および環境的セキュリティ(入退室管理や安全区画の構築など)	12	27
6	通信および運用管理(ネットワークの管理、ウイルス対策、ログ管理など)	74	122
7	アクセス制御(IDとパスワード管理、不正アクセス対策など)	35	81
8	システム開発およびメンテナンス(開発環境のセキュリティ、ライブラリ管理運用など)	14	26
9	事業継続計画(災害対策、障害対策など)	52	33
10	準拠(法律遵守、システム監査など)	11	11

（１）選択の組み合わせの上位５つからの分析

まず第１位の多い順にどのようであったかを洗ってみる。１番多い選択は「情報セキュリティポリシー（219 件)」であった。２番は「通信および運用管理（74 件)」、３番に「情報セキュリティ組織」である。

次に位第二位の選択をみると１番多数が「通信および運用管理（122 件)」、２番が「情報セキュリティ組織（99 件)」、３番が「人的セキュリティ（93 件)」であり「情報セキュリティポリシー」は 47 件と第二位での選択が少ない。

これら第一位および第二位の組み合わせの分析で何がわかるかみてみることとする。

一位－二位の選択で多かった組み合わせは次のものがある。一番多かった選択は第１位に「情報セキュリティポリシー」を選択し第２位に「情報セキュリティ組織」を選択したもので 70 件を数え、これは今回の分析の回答件数 604 件中、11.6％をしめる。次は第１位に「情報セキュリティポリシー」を選択し、第二位に「人的セキュリティ」を選択した組み合わせで 44 件、全体の 7.3％を占める。第三番目は「情報セキュリティポリシー」と「通信および運用管理」の 39 件でこれも全体の 6.5％を占める。第一位に情報セキュリティポリシーを選択する割合が多いため、上位３つまでが情報セキュリティポリシー関係であることは自然である。

ところが第四番目には情報セキュリティポリシーからの選択ではなく「通信および運用管理」と「アクセス制御」の組み合わせで 29 件、全体の 4.8％となっている。これは第１位、第２位、

第３位の単独での分析からも伺えるように、情報セキュリティポリシーなどの経営的概念からの選択をする群のほかに、実際のウイルス対策やパスワード管理、ハッカー対策などの実務を重視している選択者が一定程度存在していることを裏づけている。

第５番目は再び「情報セキュリティポリシー」と「情報資産の分類および管理」22 件、3.6％と、また情報セキュリティポリシーからの選択となっている。

表３－８－２.各要素別第２位選択項目

第1位「情報セキュリティポリシー」の場合

情報セキュリティ組織	70	32.0
情報資産の分類および管理	22	10.0
人的セキュリティ	44	20.1
物理的および環境的セキュリティ	9	4.1
通信および運用管理	39	17.8
アクセス制御	14	6.4
システム開発およびメンテナンス	5	2.3
事業継続計画	10	4.6
準拠	6	2.7

第1位「情報セキュリティ組織」の場合

情報セキュリティポリシー	12	16.4
情報資産の分類および管理	15	20.5
人的セキュリティ	18	24.7
物理的および環境的セキュリティ	4	5.5
通信および運用管理	12	16.4
アクセス制御	6	8.2
システム開発およびメンテナンス	1	1.4
事業継続計画	4	5.5
準拠	1	1.4

第1位「情報資産の分類および管理」の場合

情報セキュリティポリシー	6	14.0
情報セキュリティ組織	5	11.6
人的セキュリティ	9	20.9
物理的および環境的セキュリティ	4	9.3
通信および運用管理	9	20.9
アクセス制御	4	9.3
システム開発およびメンテナンス	2	4.7
事業継続計画	4	9.3
準拠	0	0.0

第1位「人的セキュリティ」の場合

情報セキュリティポリシー	9	12.7
情報セキュリティ組織	9	12.7
情報資産の分類および管理	7	9.9
物理的および環境的セキュリティ	4	5.6
通信および運用管理	18	25.4
アクセス制御	13	18.3
システム開発およびメンテナンス	5	7.0
事業継続計画	5	7.0
準拠	0	0.0

第1位「物理的および環境的セキュリティ」の場合

情報セキュリティポリシー	1	8.3
情報セキュリティ組織	1	8.3
情報資産の分類および管理	2	16.7
人的セキュリティ	1	8.3
通信および運用管理	3	25.0
アクセス制御	4	33.3
システム開発およびメンテナンス	0	0.0
事業継続計画	0	0.0
準拠	0	0.0

第1位「通信および環境的セキュリティ」の場合

情報セキュリティポリシー	8	10.8
情報セキュリティ組織	4	5.4
情報資産の分類および管理	5	6.8
人的セキュリティ	10	13.5
物理的および環境的セキュリティ	3	4.1
アクセス制御	29	39.2
システム開発およびメンテナンス	8	10.8
事業継続計画	5	6.8
準拠	0	0.0

第1位「アクセス制御」の場合

情報セキュリティポリシー	2	5.7
情報セキュリティ組織	1	2.9
情報資産の分類および管理	3	8.6
人的セキュリティ	2	5.7
物理的および環境的セキュリティ	1	2.9
通信および運用管理	17	48.6
システム開発およびメンテナンス	3	8.6
事業継続計画	5	14.3
準拠	0	0.0

第1位「システム開発およびメンテナンス」の場合

情報セキュリティポリシー	1	7.1
情報セキュリティ組織	3	21.4
情報資産の分類および管理	1	7.1
人的セキュリティ	0	0.0
物理的および環境的セキュリティ	0	0.0
通信および運用管理	5	35.7
アクセス制御	4	28.6
事業継続計画	0	0.0
準拠	0	0.0

第1位「事業継続計画」の場合

情報セキュリティポリシー	7	13.5
情報セキュリティ組織	5	9.6
情報資産の分類および管理	5	9.6
人的セキュリティ	5	9.6
物理的および環境的セキュリティ	2	3.8
通信および運用管理	17	32.7
アクセス制御	6	11.5
システム開発およびメンテナンス	1	1.9
準拠	4	7.7

第1位「準拠」の場合

情報セキュリティポリシー	1	9.1
情報セキュリティ組織	1	9.1
情報資産の分類および管理	1	9.1
人的セキュリティ	4	36.4
物理的および環境的セキュリティ	0	0.0
通信および運用管理	2	18.2
アクセス制御	1	9.1
システム開発およびメンテナンス	1	9.1
事業継続計画	0	0.0

第1位＼第2位	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類／管理	人的セキュリティ	物理的／環境的セキュリティ	通信／運用管理	アクセス制御	システム開発／メンテナンス	事業継続計画	準拠
1.情報セキュリティポリシー		70	22	44	9	39	14	5	10	6
2.情報セキュリティ組織	12		15	18	4	12	6	1	4	1
3.情報資産の分類および管理	6	5		9	4	9	4	2	4	0
4.人的セキュリティ	9	9	7		4	18	13	5	5	0
5.物理的および環境的セキュリティ	1	1	2	1		3	4	0	0	0
6.通信および運用管理	8	4	5	10	3		29	8	5	0
7.アクセス制御	2	1	3	2	1	17		3	5	0
8.システム開発およびメンテナンス	1	3	1	0	0	5	4		0	0
9.事業継続計画	7	5	5	5	2	17	6	1		4
10.準拠	1	1	1	4	0	2	1	1	0	

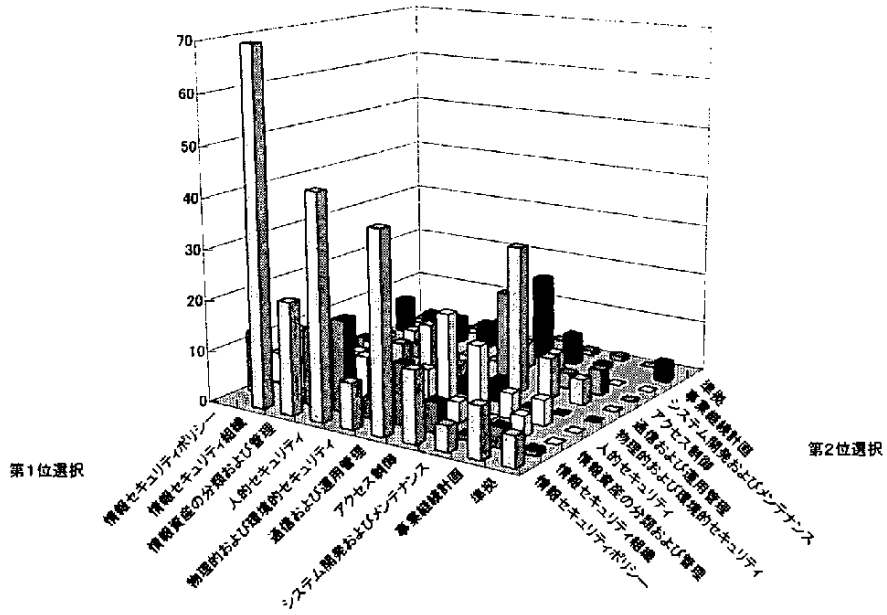


図3－8－1. 情報セキュリティ要素1位と2位の関係

（2）情報セキュリティポリシーの選択の特異性

第１位に圧倒的に指示されている「情報セキュリティポリシー」であるが、第２位での選択が意外と少ないという結果となった。「情報セキュリティ組織」から「準拠」までの各要素ごとに第２位に何を選択したかをみると、「情報資産の分類および管理」と「事業継続計画」で２番目に多い選択であったのを除いていずれも第１番目はおろか２番目にも選択されていないことがわかる。

表３－８－３．第１位、第２位を選択した要素の順番

第1位＼第2位	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類／管理	人的セキュリティ	物理的／環境的セキュリティ	通信／運用管理	アクセス制御	システム開発／メンテナンス	事業継続計画	準拠
1.情報セキュリティポリシー	■	1		2		3				
2.情報セキュリティ組織	3	■	2	1		3				
3.情報資産の分類および管理	3		■	1		1				
4.人的セキュリティ	3	3		■		1	2			
5.物理的および環境的セキュリティ			3	3	■	2	1			
6.通信および運用管理	3			2		■	1	3		
7.アクセス制御			3			1	■	3	2	
8.システム開発およびメンテナンス		3				1	2	■		
9.事業継続計画	2					1	3		■	
10.準拠				1		2				■

この表からいえることは、第一位には１位から３位までの総合計で50％を越す圧倒的な指示を得た「情報セキュリティポリシー」であるが、他の選択を選んだ群からは必ずしも多くの指示を得られていないことがわかる。一番多い選択は「通信および運用管理」であり「情報セキュリティポリシー」から「準拠」のどこからでもかならず上位３つ以内に選択されている。
これをみると、経営的には情報セキュリティなどの要素が重要としながらも実務的にはウイルス対策などに追われている様子が伺える。次に多い選択は「人的セキュリティ」である。これは「情報セキュリティ組織」、「情報資産の分類および管理」、「準拠」では１番多い選択であり、また「情報セキュリティポリシー」、「通信および運用管理」では２番目に多い選択である。

（３）選択の二つの塊

また、選択の様子をみると二つの塊があるように見える。一つは「情報セキュリティポリシー」、「情報セキュリティ組織」、「情報資産の分類および管理」、「人的セキュリティ」など経営的要素を選択する群である。（数は少ないが「事業継続計画」、「準拠」もこの群に含まれる可能性が高い）
もう一つは、「通信および運用管理」、「アクセス制御」、（数はすくないが「物理的および環境的セキュリティ」、「システム開発およびメンテナンス」もこちらに入ると考えられる）の群である。

一つ目の塊は、その中の多い組み合わせをみていくと、「情報セキュリティポリシーー情報セキュリティ組織」（70 件）、「情報セキュリティポリシーー人的セキュリティ」（44 件）、「情報セキュリティポリシーー情報資産の分類および管理」（22 件）、「情報セキュリティ組織－人的セキュリティ」（18 件）、「情報セキュリティ組織－情報資産の分類および管理」（15 件）、「情報セキュリティ組織－情報セキュリティポリシー」（12 件）などがあり、経営的な観点、組織、組織による資産管理、教育などの人的要素を重視している。

次の塊は「通信－アクセス制御」（29 件）、「アクセス制御－通信および運用管理」（17 件）の相互の組み合わせであり、実務的にウイルス対策、ハッカー対策などを重視している。

（４）その他の特徴

第２位の２番目に多い選択は「情報セキュリティ組織」であるが、これはその選択の大半が「情報セキュリティポリシー」を第一位に選択した群からの支持（70 件）であり、その他の選択をした群からはあまり支持が高くない。２番目に選択した群はなく、３番目に選択があったのが「人的セキュリティ」、「物理的および環境的セキュリティ」および「システム開発およびメンテナンス」の３つである。

一方「人的セキュリティ」は「情報セキュリティポリシー」からの選択も２番目に多い（44 件）が、その他の選択をしたところからも「通信および運用管理」と同じように選択されている。また数は少ないが「準拠」を選択した群からは「人的セキュリティ」を第２位に選択しているところが１番多く、準拠の実現には人的セキュリティが重要だと判断していることが伺える。

（５）まとめ

情報セキュリティに関する重要視する要素の選択について、経営的要素を重視する塊と実務を

重視する塊があるといえる。一般的には経営的な要素を重要視し、「情報セキュリティポリシー」を第１位にする傾向があり、そこでは「情報セキュリティポリシー」を作成し、「情報セキュリティ組織」、「人的セキュリティ」、「情報資産の分類および管理」などの要素を重視している。特に「情報セキュリティポリシー－情報セキュリティ組織」の組み合わせが 70 件と全体の 11.6％を占める。一方実務的にはウイルス対策やハッカー対策などの「通信および運用管理」、「アクセス制御」を重視する塊がある。

全体的には経営的な観点から重要な要素を選択する割合が高いが、経営的な視点を重視するところでも第２位には「通信および運用管理」を重視する傾向が強く、また「情報セキュリティポリシー」と「情報セキュリティ組織」はこの組み合わせこそ 11.6％を占め支持が多いが、その他を選択したところからは各々第２位の選択として高く支持されていないなど、経営的な観点を支持する群でも第２位は実務的な点から「通信および運用管理」を選択しているなど、理想の追求と現実への対応に苦慮しているという実態が伺える。

3.8.2　Q62 と各質問項目とのクロス集計

Q62 で情報セキュリティ要素の優先順位の選択と次の各質問の間でクロス集計を行った。

×Q18-①貴社では経営理念に基づくセキュリティポリシーを定めていますか。
×Q18-②貴社では経営理念に基づく実施手続き・規程類を定めていますか。
×Q22-①基幹システムのネットワークの管理について責任を有する担当者を定めていますか。
×Q22-②情報システムの管理について責任を有する担当者を定めていますか。
×Q22-③情報セキュリティの管理について責任を有する担当者を定めていますか。
×Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。
×Q29. 非常事態に備えて従業員に対し情報セキュリティの面から訓練を実施していますか。
×Q52. 貴事業体では不正アクセス対策について従業員に教育・訓練の場を設けていますか。
×Q60. 貴事業体ではコンピュータウイルス対策について従業員に教育・訓練の場を設けていますか。
×Q34. コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所ではそれぞれどのような火災対策をとっていますか。各場所ごとに実施している対策を選んで下さい。
×Q41. どのようなネットワーク障害対策を実施していますか。実施している対策項目を選んで下さい。
×Q48. 貴社では基幹システムのパスワード変更をどのレベルに設定していますか。
×Q65. 情報システムに係わるリスク分析を実施していますか。
×Q69. システム監査を実施していますか。

×Q18-①貴社では経営理念に基づくセキュリティポリシーを定めていますか。

ポリシー / 要素	定めている		現在作成中である		作成を検討している		定めていない		必要ない	
情報セキュリティポリシー	52	30.2	32	35.2	82	39.6	51	21.6	2	40.0
情報セキュリティ組織	15	8.7	14	15.4	16	7.7	26	11.0	0	0.0
情報資産の分類および管理	9	5.2	4	4.4	9	4.3	21	8.9	0	0.0
人的セキュリティ	21	12.2	10	11.0	15	7.2	25	10.6	0	0.0
物理的および環境的セキュリティ	5	2.9	2	2.2	0	0.0	5	2.1	0	0.0
通信および運用管理	13	7.6	7	7.7	22	10.6	31	13.1	0	0.0
アクセス制御	6	3.5	2	2.2	9	4.3	17	7.2	1	20.0
システム開発およびメンテナンス	2	1.2	0	0.0	2	1.0	10	4.2	0	0.0
事業継続計画	17	9.9	7	7.7	14	6.8	14	5.9	0	0.0
準拠	3	1.7	1	1.1	3	1.4	3	1.3	1	20.0
無回答	29	16.9	12	13.2	35	16.9	33	14.0	1	20.0
計	172	100.0	91	100.0	207	99.8	236	100.0	5	100.0

Q18-①で情報セキュリティポリシーを「定めている」ところ（回答数172）では第1位に「情報セキュリティポリシー」を選択した割合は30.2%であった。「現在作成中である」（回答数91）では35.2%、「作成を検討している」（回答数207）では39.6%、「定めていない」（回答数236）では21.6%である。このように作成中、検討中で情報セキュリティポリシーを第一にあげる率が定めているところよりも高く、実際に活動しているところほど注目されている状況であることがわかった。一方情報セキュリティポリシーを「定めていない」ところでは第1位の選択率は21.6%と低かった。情報セキュリティポリシーを「定めている」ところと「作成中」では第1位に「人的セキュリティ」をあげているところ2番目に多いが、「作成を検討している」、「定めていない」では「通信および運用管理」があがっており、経営的観点より実務的な要素を重視していることがうかがえ、意識の差があることがわかる。

×Q18-②貴社では経営理念に基づく実施手続・規程類を定めていますか。

実施手続・規程類 / 要素	定めている		現在作成中である		作成を検討している		定めていない		必要ない	
情報セキュリティポリシー	41	25.8	40	38.5	84	41.2	51	21.9	2	33.3
情報セキュリティ組織	16	10.1	15	14.4	13	6.4	27	11.6	0	0.0
情報資産の分類および管理	12	7.5	4	3.8	6	2.9	20	8.6	0	0.0
人的セキュリティ	16	10.1	16	15.4	13	6.4	25	10.7	1	16.7
物理的および環境的セキュリティ	7	4.4	1	1.0	0	0.0	4	1.7	0	0.0
通信および運用管理	10	6.3	7	6.7	25	12.3	31	13.3	0	0.0
アクセス制御	7	4.4	1	1.0	11	5.4	15	6.4	1	16.7
システム開発およびメンテナンス	3	1.9	0	0.0	2	1.0	9	3.9	0	0.0
事業継続計画	17	10.7	6	5.8	13	6.4	16	6.9	0	0.0
準拠	4	2.5	0	0.0	3	1.5	3	1.3	1	16.7
無回答	26	16.4	14	13.5	34	16.7	32	13.7	1	16.7
計	159	100.0	104	100.0	204	100.0	233	100.0	6	100.0

経営理念に基づき実施手続き・規定類を「定めている」ところ（回答数 159）では「情報セキュリティポリシー」の選択率は 25.8%であった。「現在作成中」（回答数 104）では 38.5%、「作成を検討中」（回答数 204）では 41.2%、「定めていない」（回答数 233）21.9%であった。これも全体の傾向としては前問同様、「検討中」、「作成中」がもっとも「情報セキュリティポリシー」を選択する割合が高く、「定めている」がその次に続いている。一方、「定めていない」は一番低い値を示しており、意識の差が現れている。

×Q22-①ネットワークの管理について、責任を有する担当者を定めていますか。

担当者 / 要素	定めている		設置を検討している		定めていない		必要ない	
情報セキュリティポリシー	168	29.5	27	42.2	22	30.1	2	66.7
情報セキュリティ組織	64	11.2	4	6.3	4	5.5	0	0.0
情報資産の分類および管理	32	5.6	3	4.7	5	6.8	1	33.3
人的セキュリティ	56	9.8	7	10.9	7	9.6	0	0.0
物理的および環境的セキュリティ	11	1.9	0	0.0	1	1.4	0	0.0
通信および運用管理	63	11.1	6	9.4	4	5.5	0	0.0
アクセス制御	31	5.4	2	3.1	2	2.7	0	0.0
システム開発およびメンテナンス	10	1.8	0	0.0	4	5.5	0	0.0
事業継続計画	39	6.9	2	3.1	11	15.1	0	0.0
準拠	9	1.6	1	1.6	0	0.0	0	0.0
無回答	86	15.1	12	18.8	13	17.8	0	0.0
計	569	100.0	64	100.0	73	100.0	3	100.0

ネットワークの管理について責任を有する担当者を「定めている」場合（回答数 569）では情報セキュリティの重要な要素として「情報セキュリティポリシー」が第１位であり、続いて「情報セキュリティ組織」、「通信および運用管理」、「人的セキュリティ」となる。一方、「定めていない」ところ（回答数 73）では第１位は「情報セキュリティポリシー」であるものの、第２位は「事業継続計画」であり、定めている場合と違いが出ている。どのように解釈するかは難しいが、管理者を置かない状況では、万一の事故が発生した場合の対応計画を定めておき、事後の影響を最低限に止める所だけは確実にしようという意思の現れとも考えられる。

×Q22-②情報システムの管理について責任を有する担当者を定めていますか。

要素＼担当者	定めている		設置を検討している		定めていない		必要ない	
情報セキュリティポリシー	170	29.9	28	40.0	20	29.0	1	100.0
情報セキュリティ組織	61	10.7	4	5.7	7	10.1	0	0.0
情報資産の分類および管理	34	6.0	5	7.1	2	2.9	0	0.0
人的セキュリティ	59	10.4	6	8.6	5	7.2	0	0.0
物理的および環境的セキュリティ	11	1.9	0	0.0	1	1.4	0	0.0
通信および運用管理	60	10.6	7	10.0	6	8.7	0	0.0
アクセス制御	30	5.3	4	5.7	1	1.4	0	0.0
システム開発およびメンテナンス	11	1.9	0	0.0	3	4.3	0	0.0
事業継続計画	41	7.2	2	2.9	9	13.0	0	0.0
準拠	9	1.6	1	1.4	0	0.0	0	0.0
無回答	82	14.4	13	18.6	15	21.7	0	0.0
計	568	100.0	70	100.0	69	99.7	1	100.0

情報システムの管理について責任を有する担当者を「定めている」場合（回答数 568）では情報セキュリティの重要な要素として「情報セキュリティポリシー」が第１位であり、続いて「情報セキュリティ組織」、「通信および運用管理」、「人的セキュリティ」などが選択されている。一方、定めていないところ（回答数 69）では「情報セキュリティポリシー」の次に「事業継続計画」が選択されており、ほぼ前問同様の傾向となっている。

×Q22-③情報セキュリティ管理について、責任を有する担当者を定めていますか。

要素＼担当者	定めている		設置を検討している		定めていない		必要ない	
情報セキュリティポリシー	111	29.3	59	36.0	48	29.6	1	50.0
情報セキュリティ組織	35	9.2	17	10.4	20	12.3	0	0.0
情報資産の分類および管理	22	5.8	9	5.5	9	5.6	1	50.0
人的セキュリティ	38	10.0	18	11.0	14	8.6	0	0.0
物理的および環境的セキュリティ	10	2.6	0	0.0	2	1.2	0	0.0
通信および運用管理	40	10.6	18	11.0	15	9.3	0	0.0
アクセス制御	20	5.3	6	3.7	9	5.6	0	0.0
システム開発およびメンテナンス	8	2.1	0	0.0	6	3.7	0	0.0
事業継続計画	27	7.1	9	5.5	16	9.9	0	0.0
準拠	6	1.6	2	1.2	1	0.6	0	0.0
無回答	62	16.4	26	15.9	22	13.6	0	0.0
計	379	100.0	164	100.0	162	100.0	2	100.0

情報セキュリティの管理について責任を有する担当者を「定めている」場合（回答数 379）では、情報セキュリティの重要な要素として「情報セキュリティポリシー」を選択する割合が一番多いが、続いて「通信および運用管理」、「情報セキュリティ組織」、「人的セキュリティ」と続いている。一方「定めていない」（回答数 162）では、「情報セキュリティポリシー」が一番多いが、続いては「情報セキュリティ組織」、「事業継続計画」となっている。

×Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。

要素＼マニュアル	定めている		現在作成中である		作成を検討している		定めていない		必要ない	
情報セキュリティポリシー	66	33.7	28	27.5	63	42.3	59	22.6	3	50.0
情報セキュリティ組織	17	8.7	9	8.8	18	12.1	29	11.1	0	0.0
情報資産の分類および管理	13	6.6	6	5.9	9	6.0	15	5.7	0	0.0
人的セキュリティ	22	11.2	11	10.8	11	7.4	26	10.0	1	16.7
物理的および環境的セキュリティ	2	1.0	3	2.9	2	1.3	5	1.9	0	0.0
通信および運用管理	11	5.6	10	9.8	13	8.7	38	14.6	0	0.0
アクセス制御	8	4.1	2	2.0	4	2.7	20	7.7	1	16.7
システム開発およびメンテナンス	1	0.5	1	1.0	2	1.3	10	3.8	0	0.0
事業継続計画	18	9.2	11	10.8	8	5.4	15	5.7	0	0.0
準拠	7	3.6	0	0.0	0	0.0	4	1.5	0	0.0
無回答	31	15.8	21	20.6	19	12.8	40	15.3	1	16.7
計	196	100.0	102	100.0	149	100.0	261	99.9	6	100.0

ここでは、「事業継続計画」の選択状況について分析をした。危機管理マニュアルを「作成している」ところ（回答数196）では「事業継続計画」を選択した割合は9.2%である。「作成中」（回答数102）では10.8%、「作成中を含め検討中」（回答数149）5.4%、「作成していない」（回答数261）5.7%となっており、危機管理マニュアルを作成しているところほど事業継続計画を選択する割合が高い。

×Q29. 非常事態に備えて従業員に対して情報セキュリティの面から訓練をしていますか。

要素＼訓練	定期的に実施している		時々実施している		特に実施していない	
情報セキュリティポリシー	16	37.2	19	24.7	183	30.9
情報セキュリティ組織	6	14.0	9	11.7	58	9.8
情報資産の分類および管理	2	4.7	7	9.1	34	5.7
人的セキュリティ	3	7.0	9	11.7	59	9.9
物理的および環境的セキュリティ	1	2.3	2	2.6	9	1.5
通信および運用管理	3	7.0	9	11.7	61	10.3
アクセス制御	1	2.3	4	5.2	30	5.1
システム開発およびメンテナンス	0	0.0	1	1.3	13	2.2
事業継続計画	5	11.6	4	5.2	43	7.3
準拠	3	7.0	0	0.0	8	1.3
無回答	3	7.0	13	16.9	95	16.0
計	43	100.0	77	100.0	593	100.0

ここでは、「人的セキュリティ」の選択状況について分析をした。従業員に対して訓練を「行っている」ところ（回答数43）では人的セキュリティを選択した割合は7.0%、「時々実施している」（回答数77）では11.7%、「特に実施していない」（回答数593）では9.9%となっている。訓練を行っているところの回答数が少ないので優位性をすぐには評価できないが、期待される回答と

は反対の傾向である。これは一方では第１位の選択の割合では「情報セキュリティポリシー」の選択率が上がるとその他の分析に影響が生じている可能性がある。

そこで情報セキュリティの重要な要素の第１位から第３位まで合計したもので調査を行った。

訓練 / 要素	定期的に実施している		時々実施している		特に実施していない	
情報セキュリティポリシー	23	53.5	31	40.3	248	41.8
情報セキュリティ組織	20	46.5	30	39.0	182	30.7
情報資産の分類および管理	12	27.9	21	27.3	135	22.8
人的セキュリティ	15	34.9	29	37.7	211	35.6
物理的および環境的セキュリティ	5	11.6	6	7.8	64	10.8
通信および運用管理	12	27.9	33	42.9	260	43.8
アクセス制御	15	34.9	18	23.4	175	29.5
システム開発およびメンテナンス	1	2.3	7	9.1	53	8.9
事業継続計画	12	27.9	13	16.9	121	20.4
準拠	5	11.6	4	5.2	35	5.9
無回答	3	7.0	13	16.9	95	16.0
計	43	-	77	-	593	-

その結果、「実施している」は 34.9%、「時々実施している」37.7%、「特に実施していない」35.6%とあまり差がなかった。現状では訓練の実施状況と訓練を含む人的セキュリティの選択には大きな差がない。

×Q52. 貴事業体では不正アクセス対策について従業員に教育・訓練の場を設けていますか。

教育・訓練 / 要素	情報セキュリティ教育に関して定期的に実施している		社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している		情報セキュリティポリシーや対策基準類に従って実施している		その他		特に実施していない	
情報セキュリティポリシー	10	41.7	19	33.3	25	31.3	18	67.3	228	45.5
情報セキュリティ組織	9	37.5	29	50.9	21	26.3	20	74.7	147	29.3
情報資産の分類および管理	6	25.0	12	21.1	25	31.3	8	29.9	117	23.4
人的セキュリティ	6	25.0	22	38.6	27	33.8	18	67.3	177	35.3
物理的および環境的セキュリティ	3	12.5	3	5.3	16	20.0	4	14.9	45	9.0
通信および運用管理	7	29.2	20	35.1	37	46.3	13	48.6	226	45.1
アクセス制御	6	25.0	16	28.1	28	35.0	5	18.7	148	29.5
システム開発およびメンテナンス	4	16.7	5	8.8	2	2.5	2	7.5	48	9.6
事業継続計画	5	20.8	8	14.0	20	25.0	7	26.2	104	20.8
準拠	1	4.2	3	5.3	6	7.5	4	14.9	29	5.8
無回答	5	20.8	11	19.3	11	13.8	5	18.7	75	15.0
計	24	-	57	-	80	-	38	-	501	-

ここでは「人的セキュリティ」と「アクセス制御」について分析を行った。

情報セキュリティ教育に関して「定期的に実施している」(回答数 24) ところでは「人的セキュリティ」を第3位までに選択した割合は 25.0%である。「社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している」(回答数 57)では 38.6%、「情報セキュリティポリシーや対策基準類に従って実施している」(回答数 80) 33.8%、「特に実施していない」(回答数 501) 35.3%である。

また「アクセス制御」に関しては、情報セキュリティ教育に関して定期的に実施している (回答数 24) ところでは「アクセス制御」を第3位までに選択した割合は 25.0%である。「社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している」(回答数 57) では 28.1%、「情報セキュリティポリシーや対策基準類に従って実施している」(回答数 80) 35.0%、「特に実施していない」(回答数 501) 29.5%である。

このようにみると情報セキュリティポリシーや対策基準類に従って教育を実施している場合に、人的セキュリティやアクセス制御を選択する割合が高くなっており、情報セキュリティポリシーに関連した意識が多少ではあるが表れている。

一方、参考ではあるが、選択肢と教育の実施状況を見てみると (表略)、「情報セキュリティ組織」を上位3位までに選択したところ (複数回答合計 232) では、教育を「特に実施していない」割合が 63.4%であり、物理的環境的セキュリティを選択した (複数回答合計 76) 59.2%と並び、他に比べて教育がよくなされていることがわかる。特に「情報セキュリティ組織」を選択した場合、社内教育用の情報セキュリティカリキュラムに従って時々教育している割合が 12.5%と際立って高い特徴があった。

×Q60. 貴事業体では従業員に対しコンピュータウイルス対策に関する教育・訓練の場を設けていますか。

教育・訓練 / 要素	情報セキュリティ教育に関して定期的に実施している		社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している		情報セキュリティポリシーや対策基準類に従って実施している		その他		特に実施していない	
情報セキュリティポリシー	13	43.3	28	45.2	38	39.2	21	42.6	191	43.5
情報セキュリティ組織	9	30.0	30	48.4	29	29.9	30	60.9	126	28.7
情報資産の分類および管理	7	23.3	12	19.4	28	28.9	17	34.5	97	22.1
人的セキュリティ	8	26.7	28	45.2	33	34.0	25	50.7	156	35.5
物理的および環境的セキュリティ	3	10.0	7	11.3	11	11.3	4	8.1	49	11.2
通信および運用管理	10	33.3	18	29.0	44	45.4	39	79.1	191	43.5
アクセス制御	8	26.7	14	22.6	33	34.0	19	38.5	131	29.8
システム開発およびメンテナンス	1	3.3	6	9.7	3	3.1	7	14.2	44	10.0
事業継続計画	7	23.3	12	19.4	24	24.7	16	32.5	84	19.1
準拠	0	0.0	4	6.5	8	8.2	5	10.1	26	5.9
無回答	8	26.7	9	14.5	13	13.4	9	18.3	71	16.2
計	30	-	62	-	97	-	70	-	439	-

ここではウイルス対策を含む「通信および運用管理」との関係を分析した。

情報セキュリティに関して教育・訓練を「定期的に実施している」(回答数 30) 場合、「通信および運用管理」を上位３位までに選択した割合は 33.3%である。社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している (回答数 62) 場合では「通信および運用管理」を選択した割合は 29.0%である。「情報セキュリティポリシーや実施手順規定類に従って実施している」場合 (回答数 97) は 45.4%である。「特に実施していない」(回答数 439) では 43.5%である。したがって、これだけでみるとセキュリティポリシーに従って教育をしているところと、まったく実施していないがゆえに必要性を感じているところが「通信および運用管理」を重要要素として選択したことで高い割合となったと思われる。

参考までに重要要素の側から教育の実施状況をみると (表略)、「情報セキュリティ組織」を選択した場合 (複数回答合計 232) は「特に実施していない」割合が 54.3%と低い。同様に低いものは「情報資産の分類および管理」(合計 169) で 57.4%、「事業継続計画」(合計 146) で 57.5%である。一方、「システム開発およびメンテナンス」を挙げたところ (合計 61) では回答数が少ないが「教育を実施していない」が 72.1%と高かった。一般に開発分野では教育体制が甘くなるといわれているが、その現れである可能性もある。

×Q34. コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所ではどのような火災対策をとっていますか。各場所ごとに実施している対策を選んで下さい。

①コンピュータ室

要素 / 火災対策	平均	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類・管理	人的セキュリティ	物理的・環境的セキュリティ	通信・運用管理	アクセス制御	システム開発・メンテナンス	事業継続計画	準拠
自動火災報知設備を設置している	74.0	75.8	86.3	79.1	74.6	50.0	68.9	57.1	64.3	84.6	63.6
ハロン消火設備を設置している	50.3	59.4	56.2	55.8	50.7	58.3	32.4	37.1	14.3	44.2	54.5
CO2消火設備を設置している	14.8	14.6	21.9	9.3	11.3	25.0	14.9	11.4	28.6	11.5	18.2
スプリンクラ消火設備を設置している	13.9	14.2	6.8	7.0	16.9	0.0	20.3	14.3	14.3	11.5	0.0
排煙設備を設置している	24.4	24.7	30.1	16.3	29.6	25.0	20.3	8.6	14.3	23.1	27.3
耐火金庫を設置している	16.4	16.4	17.8	14.0	8.5	8.3	8.1	14.3	21.4	28.8	9.1
消火・排煙等の防災機器の点検を定期的に行っている	58.2	61.2	68.5	60.5	63.4	50.0	50.0	40.0	57.1	59.6	45.5
回答件数	-	219	73	43	71	12	74	35	14	52	11

コンピュータ室の火災対策の実施状況で各平均とそれぞれの重要要素ごとに平均を上回っている要素を数えて比較をした。その結果、第１位に「情報セキュリティポリシー」を選択した場合 (回答数 219)、７個の対策のうち５個で対策率が平均を上回っている。また対策を講じていない割合も 5.9%と少ない。以下「情報セキュリティ組織」が６個、「情報資産の分類および管理」３

個、「人的セキュリティ」5個、「物理的および環境的セキュリティ」3個、「通信および運用管理」2個、「アクセス制御」1個、「システム開発およびメンテナンス」3個、「事業継続計画」3個、「準拠」3個、「無回答」3個となった。この結果では火災対策などの「物理的および環境的セキュリティ」を第1位に選択したものは対象数が少ない（回答数12）が、対策をとっている割合は少ないといえる。「情報セキュリティポリシー」、「情報セキュリティ組織」、「人的セキュリティ」など経営的な観点から対策が必要であるとしているところほどコンピュータ室の火災対策が充実している。これは大型コンピュータセンターなどを構えるような大手企業ほど組織的な対応を必要としている状況が反映されている可能性もある。また、検討中であるときほど選択率が上昇するところから、物理的なセキュリティだけみると、できていないからこそ第1位に掲げているとも見ることができる。 また特徴的なものでは、「事業継続計画」を掲げた場合（回答数52）、「耐火金庫」の設置率が28.8%と高くなっている。

②データ保管場所

要素 / 火災対策	平均	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類・管理	人的セキュリティ	物理的・環境的セキュリティ	通信・運用管理	アクセス制御	システム開発・メンテナンス	事業継続計画	準拠
自動火災報知設備を設置している	61.4	**63.9**	**75.3**	**62.8**	**63.4**	33.3	58.1	48.6	42.9	**71.2**	45.5
ハロン消火設備を設置している	34.4	**40.2**	**45.2**	30.2	**42.3**	33.3	16.2	17.1	7.1	**34.6**	18.2
CO2消火設備を設置している	10.2	9.6	**16.4**	**11.6**	5.6	8.3	9.5	5.7	**14.3**	**11.5**	**18.2**
スプリンクラ消火設備を設置している	11.4	11.4	8.2	**11.6**	11.3	0.0	**14.9**	11.4	0.0	**11.5**	0.0
排煙設備を設置している	18.1	**18.7**	**23.3**	9.3	**18.3**	**25.0**	16.2	8.6	7.1	17.3	**27.3**
耐火金庫を設置している	36.8	36.1	**43.8**	34.9	**38.0**	16.7	21.6	25.7	35.7	**53.8**	**45.5**
消火・排煙等の防災機器の点検を定期的に行っている	47.9	**52.5**	**63.0**	44.2	**50.7**	41.7	36.5	31.4	35.7	**55.8**	36.4
回答件数	-	219	73	43	71	12	74	35	14	52	11

コンピュータ室同様に各選択の要素事に平均より高い設置割合がどのように分布しているか把握する。「情報セキュリティポリシー」を選択した場合（回答数219）7個のうち4個で対策率が平均を上回っている。以下「情報セキュリティ組織」6個、「情報資産の分類および管理」3個、「人的セキュリティ」5個、「物理的および環境的セキュリティ」1個、「通信および運用管理」1個、「アクセス制御」0個、「システム開発およびメンテナンス」1個、「事業継続計画」6個、「準拠」3個、「無回答」4個であった。「情報セキュリティポリシー」、「情報セキュリティ組織」、「人的セキュリティ」という経営的要素を重要視するところでこのような耐火対策が行われている率が高い。また「事業継続計画」を重要とするところも割合が高くなっており、なかでも「耐火金庫の設置」は53.8%と過半数を超えており、事業継続で特にデータのバックアップが需要であるが、その重要視していることと対策を取っていることが対応している。

③ネットワーク設備室

要素 / 火災対策	平均	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類・管理	人的セキュリティ	物理的・環境的セキュリティ	通信・運用管理	アクセス制御	システム開発・メンテナンス	事業継続計画	準拠
自動火災報知設備を設置している	60.7	**65.8**	**67.1**	53.5	**63.4**	41.7	59.5	48.6	50.0	**65.4**	36.4
ハロン消火設備を設置している	31.6	**38.4**	**34.2**	27.9	**42.3**	25.0	17.6	22.9	7.1	28.8	18.2
CO2消火設備を設置している	11.3	11.9	**19.2**	7.0	7.0	8.3	9.5	5.7	**28.6**	**11.5**	**18.2**
スプリンクラ消火設備を設置している	11.8	11.9	5.5	7.0	15.5	**16.7**	**16.2**	**14.3**	0.0	7.7	9.1
排煙設備を設置している	18.7	**19.6**	**19.2**	11.6	**25.4**	**25.0**	17.6	11.4	7.1	17.3	18.2
耐火金庫を設置している	5.4	**5.9**	1.4	**7.0**	**5.6**	0.0	2.7	**8.6**	0.0	**9.6**	0.0
消火・排煙等の防災機器の点検を定期的に行っている	46.9	**51.6**	**57.5**	41.9	**52.1**	41.7	39.2	31.4	42.9	**48.1**	36.4
回答件数	-	219	73	43	71	12	74	35	14	52	11

同様にネットワーク設備が設置されている室の対応状況をみる。「情報セキュリティポリシー」を選択した場合（回答数 219)、７個のうち７個ですべてについて平均を上回っている。以下「情報セキュリティ組織」５個、「情報資産の分類および管理」１個、「人的セキュリティ」６個、「物理的および環境的セキュリティ」２個、「通信および運用管理」１個、「アクセス制御」２個、「システム開発およびメンテナンス」１個、「事業継続計画」４個、「準拠」１個、「無回答」３個であった。ここではコンピュータ室やデータ保管と比較すると特に対策をしていないが 24.2%にものぼり、全体としては対策が進んでいない。そこで「情報セキュリティポリシー」がすべての７つの項目について平均を上回っており経営的な意識の高さが現れている。コンピュータ室、データ保管と同様、「情報セキュリティポリシー」、「情報セキュリティ組織」、「人的セキュリティ」を選択したところで実施率が高くなっている。

④コンピュータ設置場所

コンピュータ設置場所についても同様に評価する。「情報セキュリティポリシー」を選択した場合（回答数 219）７個のうち６個で対策率が平均を上回っている。以下「情報セキュリティ組織」５個、「情報資産の分類および管理」２個、「人的セキュリティ」５個、「物理的および環境的セキュリティ」１個、「通信および運用管理」２個、「アクセス制御」２個、「システム開発およびメンテナンス」１個、「事業継続計画」３個、「準拠」４個、「無回答」２個である。コンピュータ設置場所は現在では通常の事務室などに設置される場合も多くなっていると考えられる。ここでも「情報セキュリティポリシー」、「情報セキュリティ組織」、「人的セキュリティ」を掲げているところが今までの分析同様各要素で平均を上回っている個所が多い。また、準拠を掲げたところでも回答数が少ないが４か所で設置割合が高くなっている。

要素 / 火災対策	平均	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類・管理	人的セキュリティ	物理的・環境的セキュリティ	通信・運用管理	アクセス制御	システム開発・メンテナンス	事業継続計画	準拠
自動火災報知設備を設置している	63.1	**65.8**	**76.7**	62.8	**67.6**	33.3	**63.5**	54.3	50.0	**63.5**	54.5
ハロン消火設備を設置している	29.2	**36.5**	**38.4**	20.9	**36.6**	16.7	17.6	25.7	14.3	21.2	27.3
CO2消火設備を設置している	11.8	11.0	**19.2**	**16.3**	9.9	**16.7**	10.8	8.6	7.1	9.6	**18.2**
スプリンクラ消火設備を設置している	17.0	**17.8**	13.7	9.3	**19.7**	16.7	**17.6**	**22.9**	7.1	15.4	**18.2**
排煙設備を設置している	19.9	**22.8**	**20.5**	18.6	**26.8**	16.7	16.2	11.4	7.1	17.3	**27.3**
耐火金庫を設置している	5.8	**7.8**	4.1	4.7	4.2	0.0	1.4	**8.6**	0.0	**9.6**	**9.1**
消火・排煙等の防災機器の点検を定期的に行っている	49.2	**53.4**	**58.9**	51.2	**56.3**	41.7	40.5	31.4	**50.0**	**50.0**	45.5
回答件数	－	219	73	43	71	12	74	35	14	52	11

⑤まとめ

全体を通していえることは、耐火対策は設備投資を伴うため大企業など組織を重んじて活動する企業の方が設置率が高くなると考えられ、そのため、経営的観点や組織的な対応を重要視する「情報セキュリティポリシー」、「情報セキュリティ組織」、「人的セキュリティ」を選択したところが、耐火関係の実施率が高くなったものと考えられる。ちなみに従業員数と「情報セキュリティポリシー」の選択割合は1万人以上22.9%、5,000～1万人45.0%、3,000～5,000人42.3%、1,000～3,000人30.9%、500～1,000人33.6%、300～500人27.7%、100～300人29.1%、100人未満16.4%と規模が小さくなるに従い減少している。このような関係が物理的な対応では表れていると考えられる。

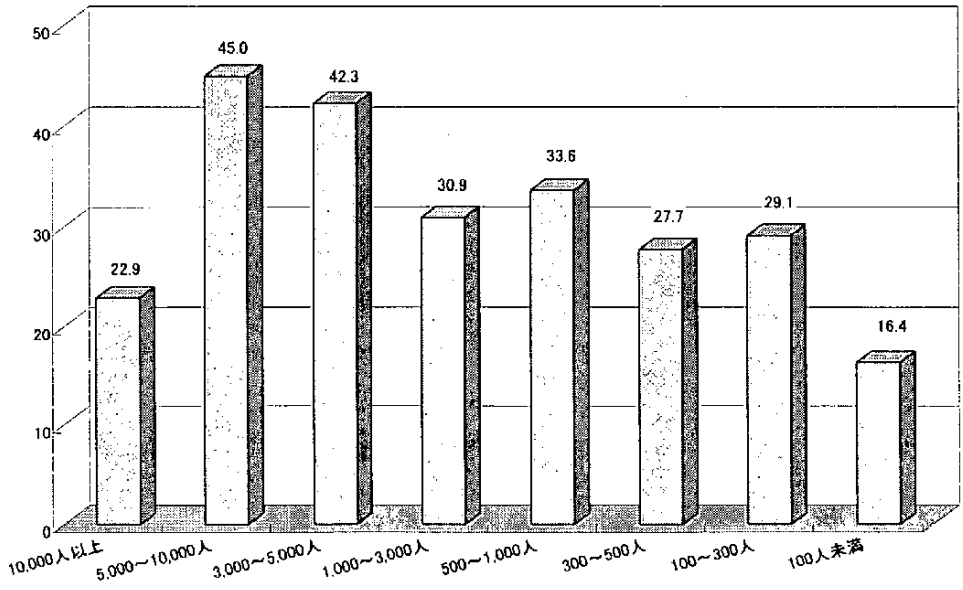


図3－8－2. 従業員規模と情報セキュリティポリシー選択

×Q41. どのようなネットワーク障害対策を実施していますか。

要素 / ネットワーク対策	平均	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類・管理	人的セキュリティ	物理的・環境的セキュリティ	通信・運用管理	アクセス制御	システム開発・メンテナンス	事業継続計画	準拠
異なる種別回線を利用	21.2	**25.6**	20.5	20.9	**25.4**	**33.3**	10.8	8.6	14.3	21.2	**36.4**
異なる交換局への収容	5.7	5.5	**9.6**	0.0	**8.5**	**16.7**	2.7	0.0	**7.1**	**11.5**	0.0
異なるコモンキャリアの利用	6.8	**7.8**	6.8	2.3	5.6	**8.3**	6.8	5.7	**7.1**	**15.4**	**18.2**
異なるISPを利用	5.0	**6.8**	2.7	2.3	2.8	**16.7**	**5.4**	2.9	0.0	3.8	0.0
異なるメディアによる回線利用	3.5	**3.7**	2.7	0.0	1.4	**8.3**	2.7	2.9	0.0	1.9	0.0
ポイント間接続から網接続へ	11.0	**12.8**	11.0	7.0	**14.1**	8.3	5.4	11.4	0.0	**15.4**	**18.2**
重要回線を部分的に二重化	25.8	**32.0**	20.5	7.0	**36.6**	25.0	16.2	**31.4**	**28.6**	**32.7**	**27.3**
専用のバックアップ回線を常時設定	17.8	**20.1**	**19.2**	**23.3**	14.1	**25.0**	16.2	11.4	**28.6**	**21.2**	9.1
専用回線とインターネットVPNなどの異種サービスと組み合わせ	8.4	8.2	**11.0**	7.0	**8.5**	8.3	**10.8**	5.7	0.0	**11.5**	**9.1**
社内の構内回線、LAN等を二重化	14.9	**15.5**	**19.2**	4.7	**19.7**	**33.3**	9.5	**14.3**	**14.3**	**17.3**	**18.2**
通信機器の二重化	21.6	**23.7**	**24.7**	**11.6**	19.7	**25.0**	16.2	8.6	**21.4**	**28.8**	**27.3**
インターネットに接続したサーバの分散	9.6	**10.0**	9.6	4.7	8.5	8.3	6.8	**11.4**	**21.4**	7.7	**18.2**
回答件数	-	219	73	43	71	12	74	35	14	52	11

情報セキュリティの重要な要素の第1位の選択ごとにそれぞれのネットワーク障害対策の実施率が平均より上回っている個数を数えた。その結果、「情報セキュリティポリシー」を選択した場合（回答数219）12個のうち10個で対策率が平均を上回っている。また対策を講じていない割合も29.7%であり全体の平均を下回っている。以下「情報セキュリティ組織」5個、「情報資産の分類および管理」1個、「人的セキュリティ」6個、「物理的および環境的セキュリティ」8個、「通信および運用管理」2個、「アクセス制御」3個、「システム開発およびメンテナンス」3個、「事業継続計画」8個、「準拠」8個、「無回答」4個であった。また実施していない割合が平均より低いのは、「情報セキュリティポリシー」、「情報セキュリティ組織」、「人的セキュリティ」、「無回答」である。この結果をみると、対策を実施している割合が高いのは「情報セキュリティポリシー」を選択した場合で12個のうち10と他を大きく引き離している。続いて「物理的および環境的セキュリティ」、「事業継続計画」、「準拠」と続いている。一方、この分野と関係ある「通信および運用管理」を掲げたところでは平均以上の実施率が「異なるISPの利用」と「専用回線とVPNなど異種サービスの組み合わせ」だけであり、この回答をみると実施率が低いという自覚から「通信および運用管理」が必要であるとの回答がされたものと考えられる。また「事業継続計画」や「準拠」で比較的高い実施率が得られたが、これらは実際に事業継続計画を立てている中で実施されているものと考えられる。

×Q48. 貴事業体では基幹システムのパスワードの変更をどのレベルに設定していますか。

要素 / パスワード変更レベル	情報セキュリティポリシー	情報セキュリティ組織	情報資産の分類・管理	人的セキュリティ	物理的・環境的セキュリティ	通信・運用管理	アクセス制御	システム開発・メンテナンス	事業継続計画	準拠
ワンタイムパスワードを設定している	1.8	0.0	0.0	2.8	0.0	2.7	0.0	0.0	1.9	0.0
変更期限がきたらパスワードを無効にする	5.9	1.4	0.0	2.8	8.3	1.4	5.7	0.0	1.9	0.0
定期的に新しいパスワードを配布する	7.8	8.2	4.7	4.2	8.3	4.1	2.9	0.0	3.8	0.0
変更期限を定めて利用者が変更している	12.3	15.1	11.6	5.6	16.7	10.8	0.0	28.6	15.4	9.1
パスワードの変更期限を推奨しているが、変更期間は利用者に任せている	37.0	41.1	30.2	39.4	8.3	43.2	37.1	0.0	25.0	45.5
パスワードの変更に関して特に定めていない	23.3	31.5	41.9	32.4	33.3	29.7	42.9	50.0	40.4	9.1
パスワードによる管理を実施していない	9.6	1.4	9.3	7.0	16.7	6.8	8.6	21.4	7.7	9.1
回答件数	219	73	43	71	12	74	35	14	52	11

分析結果から一番選択が多い「情報セキュリティポリシー」(回答数 219) では、「変更期限がきたらパスワードを無効にする」(5.9%) や「定期的に新しいパスワードを配布する」(7.8%)、「変更期限を定めて利用者が変更している」(12.3%) などが平均に比べて割合が高く、「パスワード変更に関して特に定めていない」(23.3%) が低くなっている。一方「アクセス制御」(回答数 35) では回答数が少ないが「変更期限がきたらパスワードを無効にする」が 5.7%と高くなっている、一方、「パスワードに関して特に定めていない」(42.9%)と対応がとられていない割合も高くなっている。ここでは関心が高い層と対応がとれていないことを認識している層が混在していることをうかがわせる。

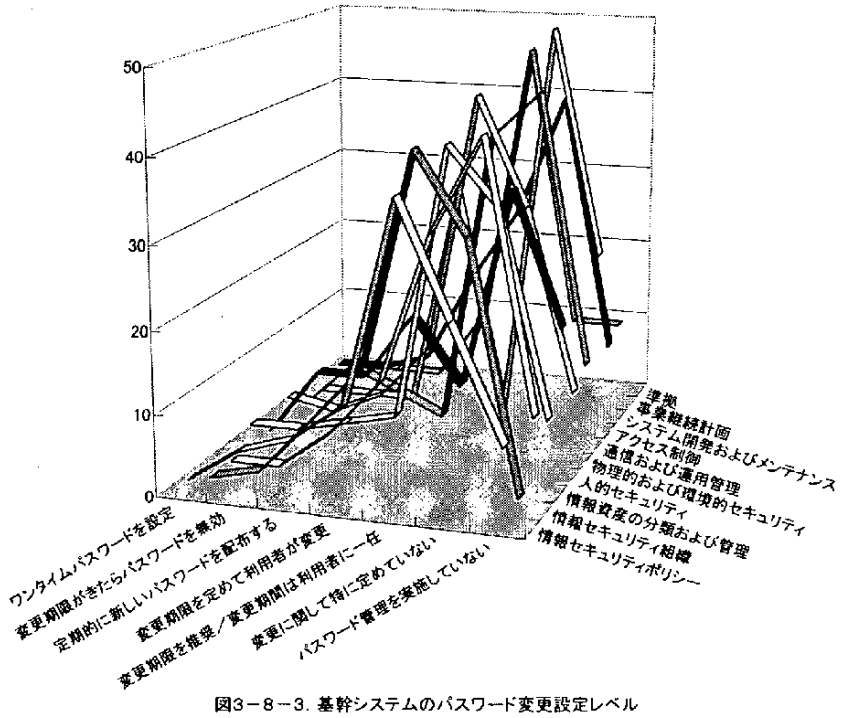


図3－8－3. 基幹システムのパスワード変更設定レベル

×Q65. 情報システムに係わるリスク分析を実施していますか。

	行っている		行っていない		無回答		計	
情報セキュリティポリシー	53	17.5	247	81.5	3	1.0	303	100.0
情報セキュリティ組織	50	21.6	181	78.0	1	0.4	232	100.0
情報資産の分類および管理	43	25.4	125	74.0	1	0.6	169	100.0
人的セキュリティ	55	21.5	200	78.1	1	0.4	256	100.0
物理的および環境的セキュリティ	18	23.7	6	7.9	0	0.0	76	100.0
通信および運用管理	42	13.7	262	85.3	3	1.0	307	100.0
アクセス制御	40	19.2	166	79.8	2	1.0	208	100.0
システム開発およびメンテナンス	6	9.8	54	88.5	1	1.6	61	100.0
事業継続計画	28	19.2	118	80.8	0	0.0	146	100.0
準拠	10	22.7	34	77.3	0	0.0	44	100.0
無回答	19	16.7	87	76.3	8	7.0	114	100.0

リスク分析の実施の有無による違いを分析した。情報セキュリティ要素別に実施の割合を比較すると、全体の平均では「行っている」が 18.8%であるが、「情報資産の分類および管理」を選択した場合（複数回答合計 169)、「行っている」が 25.4%と高く、この割合は全体で一番高い。

「情報資産の分類および管理」のなかで資産につきリスク分析を行うことが求められているが、そのとおり実施していることが伺える。行っているかいないかで重要要素の選択に違いがあるかをみると、「行っている」場合（回答数 135）では「人的セキュリティ」（55 件)、「情報セキュリティポリシー」（53 件)、「情報セキュリティ組織」（50 件)、「情報資産の分類および管理」（43 件と、４番目に選択されている。一方、「行っていない」（回答数 571）では「通信および運用管理」（262 件)、「情報セキュリティポリシー」（247 件)、「人的セキュリティ」（200 件)、「情報セキュリティ組織」（181 件)、「アクセス制御」（166 件）が上位にあり、「情報資産の分類および管理」（125 件）は６番目となる。このようにリスク分析の実施は実際の実施の状況により重要要素の選択にも大きな違いが生じている。リスク分析を実施するとその重要性を認識するようである。

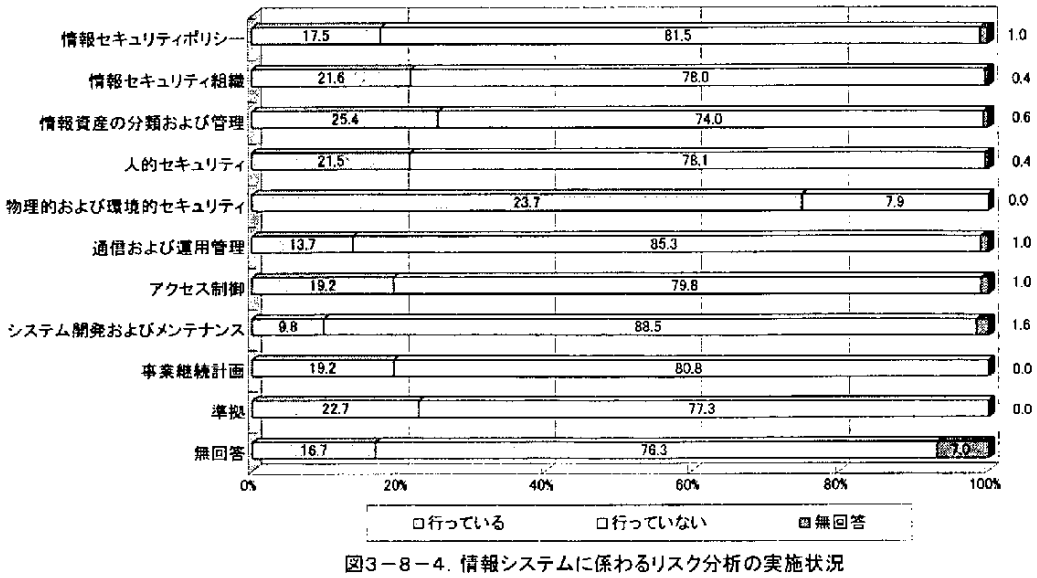


図3－8－4. 情報システムに係わるリスク分析の実施状況

×Q68. システム監査を実施していますか。

	いる		いない		無回答		計	
情報セキュリティポリシー	80	36.5	134	61.2	5	2.3	219	100.0
情報セキュリティ組織	24	32.9	49	67.1	0	0.0	73	100.0
情報資産の分類および管理	17	39.5	26	60.5	0	0.0	43	100.0
人的セキュリティ	24	33.8	47	66.2	0	0.0	71	100.0
物理的および環境的セキュリティ	6	50.0	6	50.0	0	0.0	12	100.0
通信および運用管理	23	31.1	50	67.6	1	1.4	74	100.0
アクセス制御	5	14.3	30	85.7	0	0.0	35	100.0
システム開発およびメンテナンス	1	7.1	13	92.9	0	0.0	14	100.0
事業継続計画	23	44.2	29	55.8	0	0.0	52	100.0
準拠	6	54.5	5	45.5	0	0.0	11	100.0
無回答	41	36.0	6	5.3	7	6.1	114	100.0

重要要素の選択とシステム監査の実施の可否について違いを分析した。各要素ごとにシステム監査を実施している割合をみると、多い順に「準拠」(回答数 11)、「物理的および環境的セキュリティ」(回答数 12)、「事業継続計画(回答数 52)、「情報資産の分類および管理(回答数 43)、「情報セキュリティポリシー」(回答数 219) となる。一方少ない方では「システム開発およびメンテナンス」(回答数 14)、「アクセス制御」(回答数 35)、「通信および運用管理」(回答数 74) となっている。回答数が少ないところは有意で判断できないが、監査を実施しているところは「準拠」や「事業継続計画」など経営的な観点で判断していることが伺える。一方、「アクセス制御」、「通信および運用管理」、また「システム開発およびメンテナンス」を重視する技術的実務的な判断を優先しているところでは監査については実施されていないことがわかる。

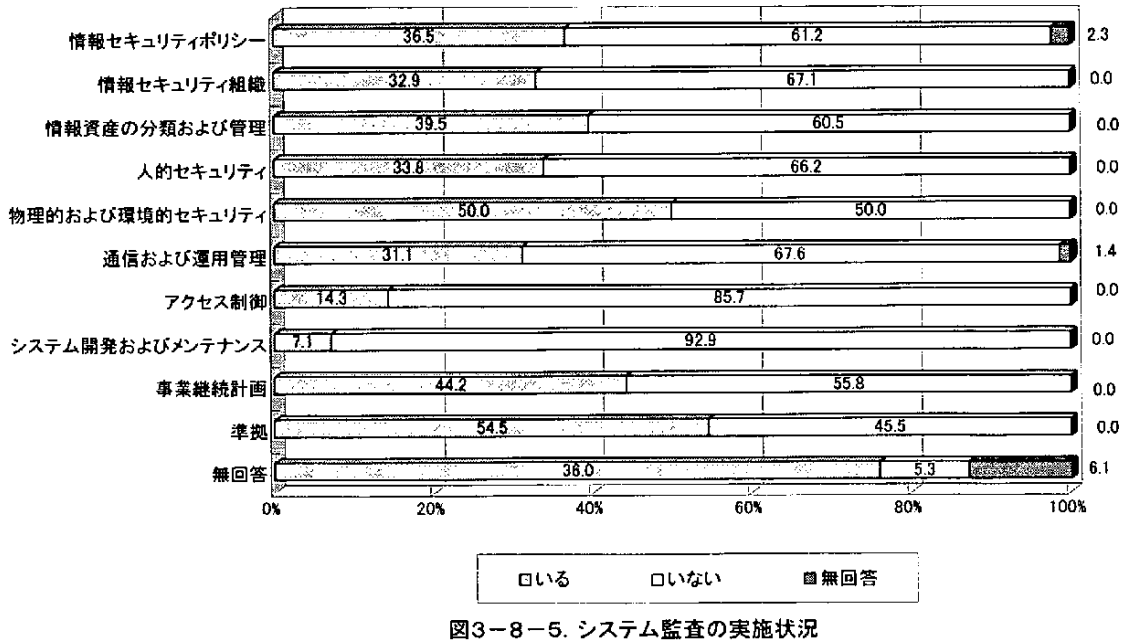


図3－8－5. システム監査の実施状況

3.9 Q63 のクロス分析

Q63. 情報セキュリティの確保にとり基本的に重要な視点は何だと思いますか？

情報セキュリティの確保にとり基本的に重要な視点について「経営者層の理解」、「管理者の理解」、「担当者の理解」、「社内全体の理解」、「法規制の整備」の各項目をあげ、複数回答を得る調査を行った。情報セキュリティの確保の現状とこれらの回答にどのような関係があるか、以下の質問との間でクロス集計を行った。

×Q22-①ネットワーク管理について、責任を有する担当者を定めていますか。
×Q22-②情報システムの管理について、責任を有する担当者を定めていますか。
×Q22-③情報セキュリティの管理について、責任を有する担当者を定めていますか。
×Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。
×Q29. 非常事態に備えて従業員に対してセキュリティの面から訓練をしていますか。
×Q65. 情報システムに係わるリスク分析を実施していますか。
×Q70. 情報システム関連のリスクが倒産に結びつくと思いますか。

前回の分析では「経営者の理解」をあげているところほど「情報セキュリティの確保」が進んでいるのではないかとの仮説をあげて分析を行った。その結果「経営者の理解」、「管理者の理解」、「担当者の理解」、「社内全体の理解」、「法規制の整備」の回答にあまり違いがなくこの仮説は確認できなかった。今回も前回同様の分析を実施することとした。

×Q22-①ネットワーク管理について、責任を有する担当者を定めていますか。

	経営者層の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
定めている	53.1	33.6	20.4	79.4	15.5
設置を検討している	59.4	42.2	20.3	73.4	14.1
定めていない	50.7	17.8	20.5	68.5	11.0
必要ない	33.3	33.3	0.0	100.0	0.0
無回答	55.6	33.3	11.1	77.8	11.1

ネットワーク管理者を定めているところ（回答数 569）では、「経営者の理解」53.1%、「管理者の理解」33.6%、「担当者の理解」20.4%、「社内全体の理解」79.4%、「法規制の整備」15.5%であった。一方、定めていないところ（回答数 73）では「経営者の理解」50.7%、「管理者の理解」17.8%、「担当者の理解」20.5%、「社内全体の理解」68.5%、「法規制の整備」11.0%であった。このようにこの２つを比較すると回答の選択率で前回同様、いずれも定めている方が割合は高かった。また定めていない事業体では「管理者の理解」が 17.8%と大幅に低い特徴がある。設置を検討している（回答数 64）では「経営者層の理解」59.4%、「管理者の理解」42.2%と高く、まさに検討中の事業体ほど経営者や管理者の関与が必要であり、その影響を受けると感じていることがわかる。なお、前回調査では「定めている」ところでは「経営者の理解」55.9%、「管理者の理解」30.4%、「担当者の理解」21.6%、「社内全体の理解」75.5%、「法規制の整備」21.0%であり、法規制の整備が今回大きく下がったのが目立つが、全体の回答傾向はほとんど変化がない。

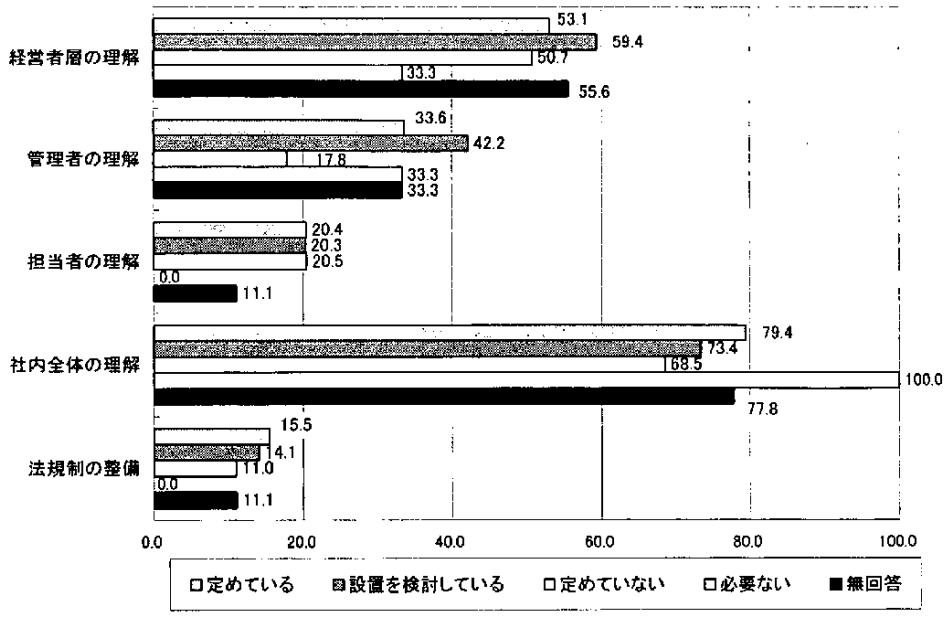


図3－9－1．ネットワーク管理担当者の設置状況

×Q22-②情報システムの管理について、責任を有する担当者を定めていますか。

	経営者層の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
定めている	53.2	34.2	20.6	78.7	15.3
設置を検討している	58.6	37.1	20.0	78.6	14.3
定めていない	47.8	17.4	18.8	69.6	10.1
必要ない	100.0	0.0	0.0	100.0	0.0
無回答	60.0	30.0	10.0	80.0	20.0

情報システムの管理者を「定めている」ところ（回答数568）では「経営者の理解」53.2%、「管理者の理解」34.2%、「担当者の理解」20.6%、「社内全体の理解」78.7%、「法規制の整備」15.3%であった。これは「Q22-①ネットワーク管理者」のクロス集計とほぼ同じ値である。一方、情報システムの管理者を「定めていない」（回答数69）では「経営者の理解」47.8%、「管理者の理解」17.4%、「担当者の理解」18.8%、「社内全体の理解」69.6%、「法規制の整備」10.1%であった。これもQ22-①同様に「定めている」と回答した方が「定めていない」と回答した群よりいずれも高い回答率を示している。また「定めていない」と回答したところでは前問同様、「管理者の理解」が17.4%と大きく下回っている。

「設置を検討している」ところ（回答数 70）では「経営者の理解」58.6%、「管理者の理解」37.1%でありこれもQ22-①同様、検討中の場合こそ経営者と管理者の理解が必要との現れである。なお、前回調査では「定めている」ところで「経営者の理解」55.0%、「管理者の理解」29.7%、「担当者の理解」20.7%、「社内全体の理解」74.7%、「法規制の整備」21.2%であり、全体の傾向は前問同様であまり大きな変化はなかった。

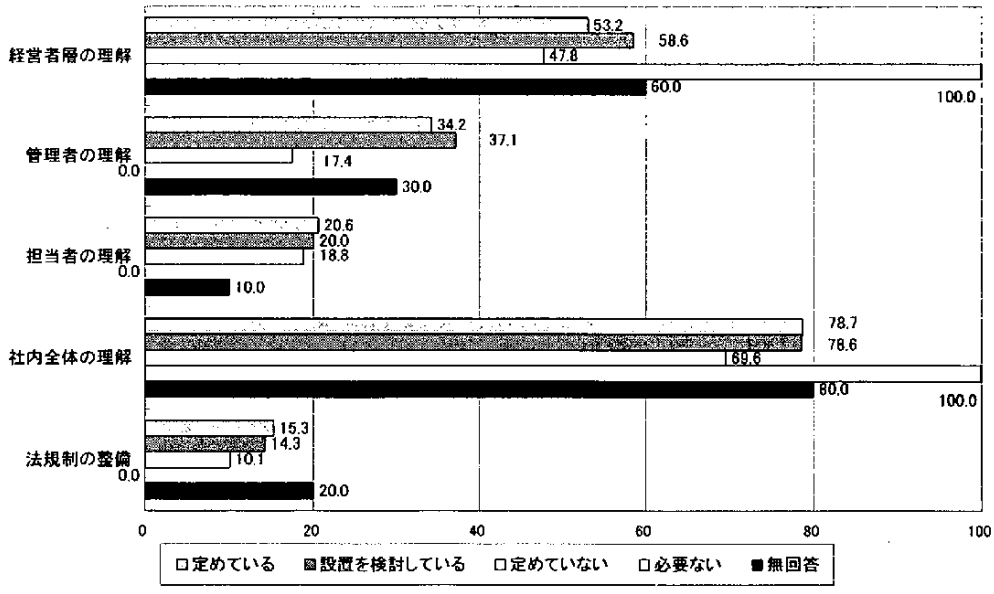


図3－9－2. 情報システム管理担当者の設置状況

×Q22-③情報セキュリティの管理について、責任を有する担当者を定めていますか。

	経営者層の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
定めている	51.5	33.8	21.6	80.5	19.0
設置を検討している	56.7	36.0	18.9	77.4	11.0
定めていない	53.7	27.2	19.1	72.2	8.6
必要ない	50.0	50.0	0.0	100.0	0.0
無回答	63.6	27.3	9.1	72.7	18.2

情報セキュリティに関する責任を有する担当者を「定めている」ところ（回答数379）では「経営者の理解」51.5%、「管理者の理解」33.8%、「担当者の理解」21.6%、「社内全体の理解」80.5%、「法規制の整備」19.0%であった。一方、「定めていない」ところ（回答数162）では「経営者の理解」53.7%、「管理者の理解」27.2%、「担当者の理解」18.9%、「社内全体の理解」72.2%、「法規制の整備」8.6%であった。これも前2つのクロス集計と同様の回答傾向である。

同様に「設置を検討している」ところ（回答数 164）では、「経営者の理解」56.7%、「管理者の理解」36.0%であり、他の回答より選択の割合が高くこれも前2問と同様の傾向である。

前回調査では「定めている」ところで「経営者の理解」53.4%、「管理者の理解」32.5%、「担当者の理解」22.8%、「社内全体の理解」75.2%、「法規制の整備」20.4%であり、前2つの分析同様ほとんど変化がない。

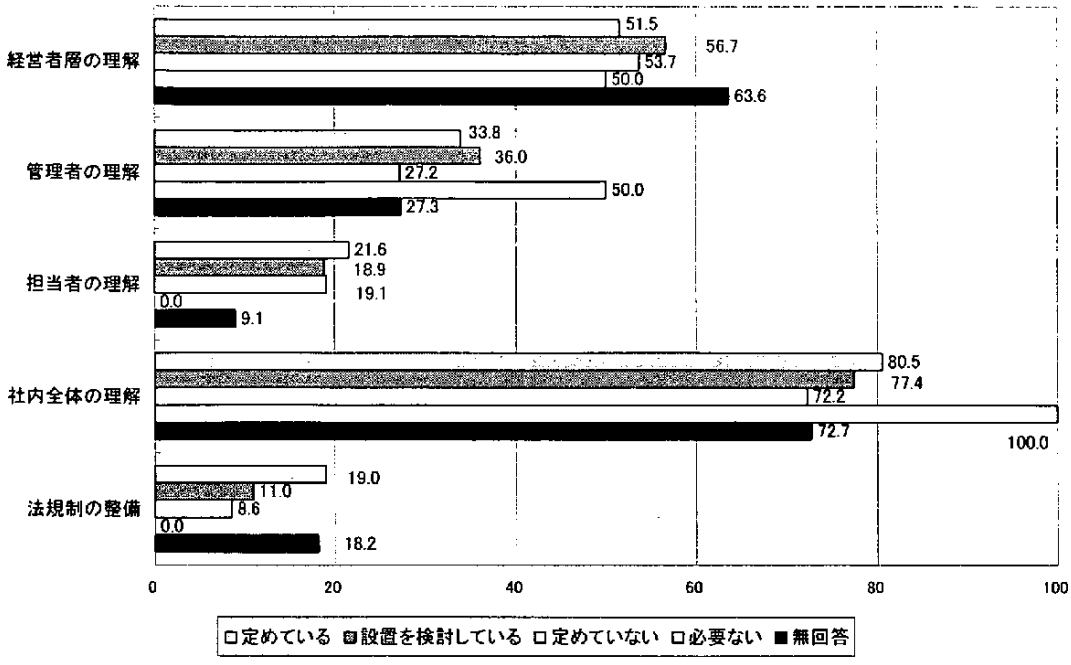


図3－9－3. 情報セキュリティ管理担当者の設置状況

×Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。

	経営者層の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
作成している	56.1	36.2	21.4	84.7	14.3
作成中である	56.9	31.4	22.5	83.3	13.7
作成を含め検討中である	57.7	34.9	17.4	79.9	19.5
作成していない	48.7	30.3	19.9	70.1	13.4
必要ない	33.3	16.7	0.0	66.7	0.0
無回答	0.0	0.0	50.0	50.0	0.0

全社的なマニュアルを「作成している」ところ（回答数 196）では「経営者の理解」56.1%、「管理者の理解」36.2%、「担当者の理解」21.4%、「社内全体の理解」84.7%、「法規制の整備」14.3%であった。一方、「作成していない」ところ（回答数 261）では「経営者の理解」48.7%、「管理者の理解」30.3%、「担当者の理解」19.9%、「社内全体の理解」70.1%、「法規制の整備」13.4%であり、作成しているところと比較するといずれも作成している方が作成していないところよりも各々の回答率が高い。ここではこれまでのように「作成中」や「検討中」の場合でも「経営者の理解」56.9、57.7%、「管理者の理解」31.4、34.9%、と「作成している」とほぼ同じで突出して高くはない。

前回調査では「作成している」ところの回答は「経営者の理解」50.7%、「管理者の理解」29.4%、「担当者の理解」21.0%、「社内全体の理解」80.8%、「法規制の整備」23.4%と今法規制の整備が大きく下がった状況以外は回答の傾向は変わらない。

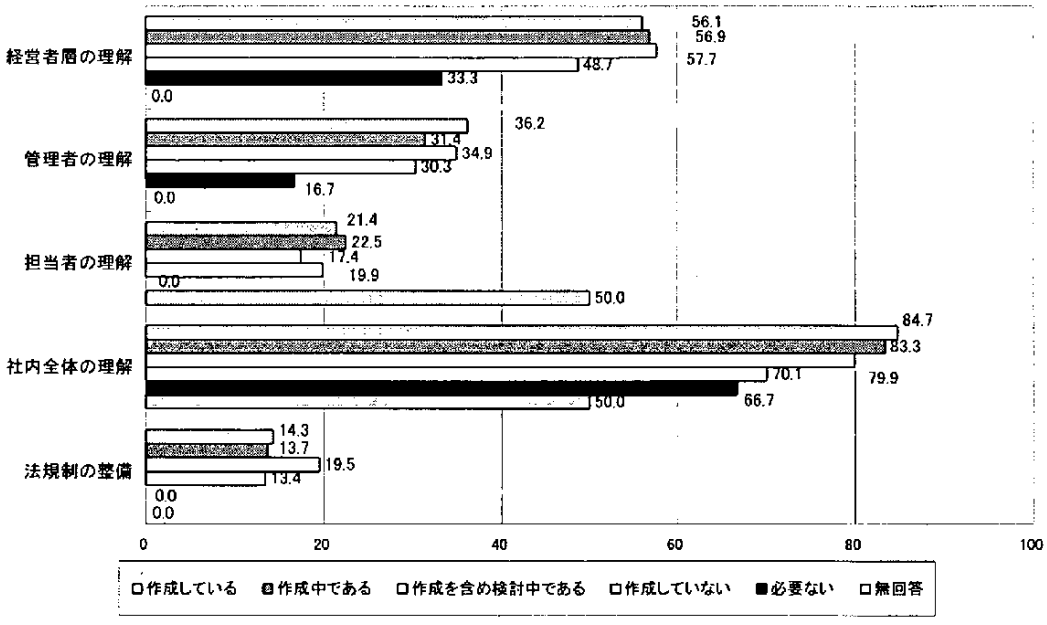


図3－9－4. 危機管理マニュアルの作成状況

×Q29. 非常事態に備えて従業員に対して情報セキュリティの面から訓練を実施していますか。

	経営者層の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
定期的に実施している	67.4	37.2	23.3	88.4	23.3
時々実施している	54.5	35.1	22.1	81.8	15.6
特に実施していない	52.4	32.4	19.7	76.9	14.2
無回答	20.0	0.0	20.0	40.0	0.0

非常事態に備えて情報セキュリティの面から訓練を「定期的に実施している」ところ（回答数43）では「経営者の理解」67.4%、「管理者の理解」37.2%、「担当者の理解」23.3%、「社内全体の理解」88.4%、「法規制の整備」23.3%となっている。一方、「特に実施していない」ところ（回答数593）では「経営者の理解」52.4%、「管理者の理解」32.4%、「担当者の理解」19.7%、「社内全体の理解」76.9%、「法規制の整備」14.2%となっている。「訓練を実施していない」ところが全体的に各回答率が低い傾向であるが、ここでは今までの分析と異なり、「担当者の理解」が「実施していない」方で回答率が高い。

前回調査では訓練を「定期的に実施している」ところでは「経営者の理解」60.0%、「管理者の理解」42.2%、「担当者の理解」26.7%、「社内全体の理解」82.2%、「法規制の整備」26.7%となっており、全体的な傾向は変わらない。また前回極端に低かった「実施していない」場合の法規制の整備（前回1.2%）は今回14.2%と、他に比べまだ大きな差があるものの、回答率は上昇している。

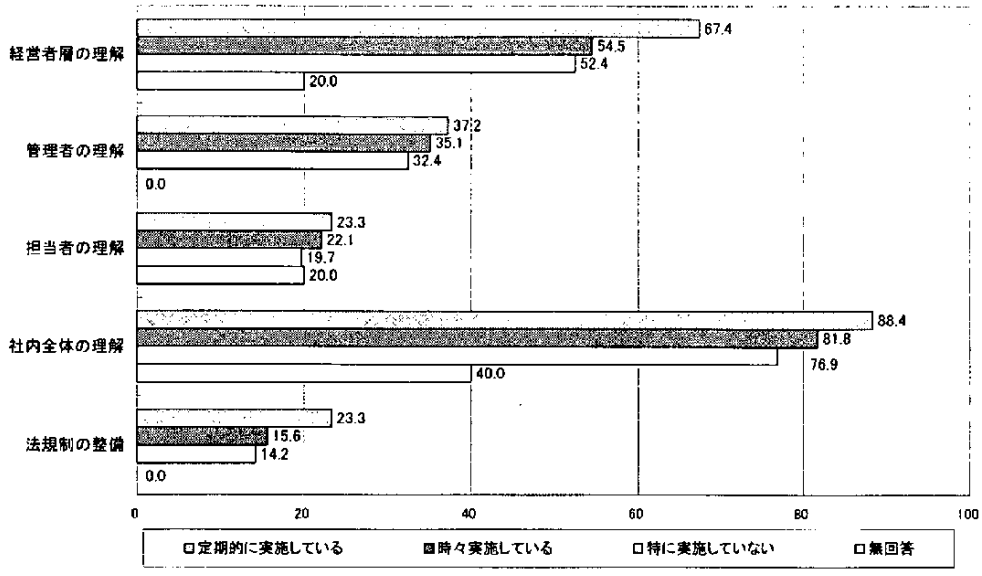


図3－9－5. 非常事態に備えた情報セキュリティ面の訓練の実施

×Q65. 情報システムに係わるリスク分析を実施していますか。

	経営者層の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
行っている	60.0	37.0	27.4	85.2	18.5
行っていない	52.2	31.9	18.4	76.5	13.8
無回答	33.3	25.0	25.0	58.3	16.7

情報システムに係わるリスク分析を「行っている」事業体（回答数 135）では「経営者の理解」60.0%、「管理者の理解」37.0%、「担当者の理解」27.4%、「社内全体の理解」85.2%、「法規制の整備」18.5%となっている。一方、「行っていない」ところ（回答数 571）では「経営者の理解」52.2%、「管理者の理解」31.9%、「担当者の理解」18.4%、「社内全体の理解」76.5%、「法規制の整備」13.8%となっており、他の分析と同様、「行っていない」方より「行っている」方が回答率が高い。

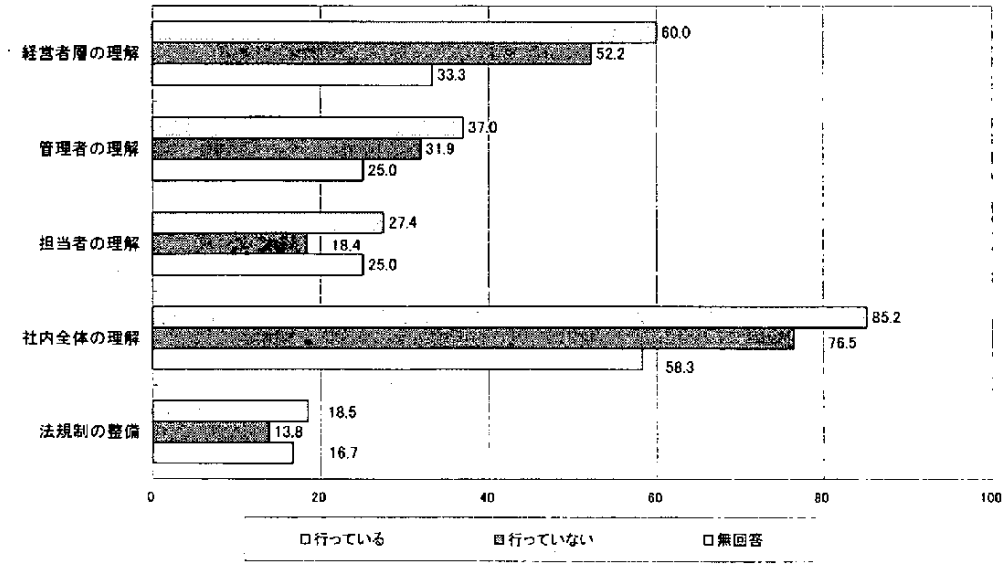


図3－9－6. 情報システムに係わるリスク分析の実施

また前回調査では「行っている」ところで「経営者の理解」58.7%、「管理者の理解」37.5%、「担当者の理解」30.8%、「社内全体の理解」79.8%、「法規制の整備」23.1%となっており、全体的な傾向は変わらない。

×Q70. 情報システム関連のリスクが倒産に結びつくと思いますか。

	経営者層の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
思う	62.8	34.9	22.1	87.2	22.1
重大な影響は受けると思う	55.2	35.3	21.6	79.4	14.2
重大な影響は受けないと思う	44.4	27.3	16.2	74.7	10.1
わからない	51.0	27.5	17.6	70.6	14.7
無回答	37.9	27.6	17.2	65.5	17.2

情報システム関連のリスクが倒産と「結びつく」と回答したところ（回答数86）では「経営者の理解」62.8%、「管理者の理解」34.9%、「担当者の理解」22.1%、「社内全体の理解」87.2%、「法規制の整備」22.1%となっている。「重大な影響は受けると思う」としたところ（回答数402）では「経営者の理解」55.2%、「管理者の理解」35.3%、「担当者の理解」21.6%、「社内全体の理解」79.4%、「法規制の整備」14.2%であった。一方、「重大な影響は受けない」としたところ（回答数99件）では「経営者の理解」44.4%、「管理者の理解」27.3%、「担当者の理解」16.2%、「社内全体の理解」74.7%、「法規制の整備」10.1%となっており、意識の差に応じて回答率が下がる傾向が顕著に表れている。

前回調査では「倒産すると思う」という回答では「経営者の理解」61.7%、「管理者の理解」26.2%、「担当者の理解」22.4%、「社内全体の理解」71.0%、「法規制の整備」26.2%であった。全体の傾向はほぼ同様である。「社内全体の理解」という回答が今回は87.2%と前回71.0%から大きく伸びているのが目立つ。

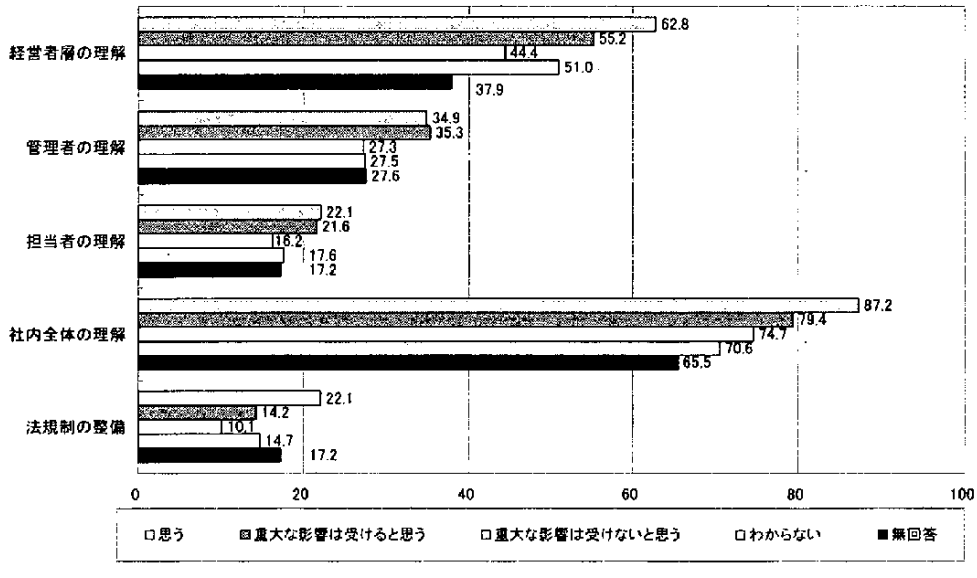


図3－9－7. 情報システム関連のリスクの倒産

全体の傾向分析

前回同様の傾向が引き続きみられる。全体の「経営者の理解」、「管理者の理解」、「担当者の理解」、「社内全体の理解」、「法規制の整備」の回答率の割合は「法規制の整備」の選択がやや減少しているのを除くと前回とほぼ同じ回答である。「法規制の整備」の割合が減少した詳しい理由はわからないが、国家として許認可を廃止する方向であること、それに代わってISO認証制度に切り替えていくこと、情報システムに関しても情報セキュリティポリシー、「ISO17799」、情報システム関連の製品にかかわる規格である「ISO15408」、個人情報保護に係わる「JIS Q 15001」などの規格が浸透してきていること、また金融関係では金融検査マニュアルが制定されたことなどが関係して法規制の整備の支持率が下がったと考えられる。

前回同様、各対策を実施している方が実施していない方より回答率が上回っており、回答率の差に意識の高さの差が伺える。

一方、回答傾向は実施の有無で同じ傾向を示しており、前回同様「社内全体の理解」＞「経営者の理解」＞「管理者の理解」＞「担当者の理解」＞「法規制の整備」となる。

経営者の理解よりも社内全体の理解を上げるという、経営者と従業員が、また情報システム部門と社内ユーザ部門の一体化が求められる、日本的な風土がここでもうかがえる。

3.10 Q69のクロス集計

Q69. システム監査を実施していない理由は何ですか。

経営理念に基づき情報セキュリティポリシーを定める事業体であれば、システム監査に関して理解が深く、したがってシステム監査を実施する傾向が高いと思われる。また逆の傾向も考えられる。そこで、システム監査を実施していない回答について、その実態を考察してみた。

×Q18. 貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。

ポリシー策定状況 / 監査未実施の理由	回答数	定めている		現在作成中である		作成を検討している		定めていない		必要ない	
経営者層が重要性を認識していないため	54	4	7.4	5	9.3	14	25.9	30	55.6	0	0.0
システム監査実施のためのコンセンサス、組織風土が十分に備わっていない	178	20	11.2	17	9.6	61	34.3	80	44.9	0	0.0
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	139	23	16.5	16	11.5	45	32.4	55	39.6	0	0.0
システム監査の方法、制度、手続きなどが十分でない	100	19	19.0	14	14.0	29	29.0	38	38.0	0	0.0
効果が明確でない	123	11	8.9	9	7.3	32	26.0	68	55.3	3	2.4
適切なシステム監査人が見つからない	60	5	8.3	7	11.7	16	26.7	31	51.7	0	0.0

Q18 に対する回答 455 件のうち、情報セキュリティポリシーを「定めている」のが 69 件（15.2%）、「定めていない」と回答した事業体は 200 件（44.0%）であった。

定めていない事業体がシステム監査を実施していない傾向についてみると、次のような結果が得られた。まず、システム監査について「経営者層が重要性を認識していない」では 55.6%と最も高く、次いで、「効果が明確でない」では 55.3%であった。さらに、「実施のためのコンセンサス、組織風土が十分に備わっていない」では 44.9%、「システム監査実施よりシステム化推進そのものに力点がある」の場合、39.6%という結果であった。これらは、「情報セキュリティポリシーを定めている」事業体に比べてに高い割合を示しており、経営理念に基づく情報セキュリティポリシーの存在がシステム監査の導入に関係があることを物語っているといえる。

×Q65. 情報システムに係わるリスク分析を実施していますか。

	回答数	行っている		行っていない	
経営者層が重要性を認識していないため	54	4	7.4	50	92.6
システム監査実施のためのコンセンサス、組織風土が十分に備わっていない	178	16	9.0	161	90.4
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	139	17	12.2	121	87.1
システム監査の方法、制度、手続きなどが十分でない	100	17	17.0	82	82.0
効果が明確でない	123	7	5.7	115	93.5
適切なシステム監査人が見つからない	60	8	13.3	52	86.7

リスク分析はシステム監査において重要な項目である。システム監査を実施していない455件の回答理由とリスク分析の関係について取り上げてみた。

システム監査を実施していない理由のうち「経営者層が重要性を認識していない」について、リスク分析を「行っている」7.4%に対して「行っていない」の回答は92.6%であった。「実施のためのコンセンサス、組織風土が十分に備わっていない」については「行っている」9.0%、「行っていない」90.4%、「システム監査実施よりシステム化推進そのものに力点がある」(回答数139)に関してはそれぞれ12.2%、87.1%、「システム監査の方法、制度、手続きなどが十分でない」(回答数100)の場合、17.0%、82.0%、システム監査の「効果が明確でない」についても、それぞれ5.7%、93.5%であった。いずれの理由についてもリスク分析を行っていない事業体の回答割合が高い。この点は、リスク分析ならびにシステム監査の機能に関する認識の度合いに拠っているものと思われる。

×Q70. 情報システム関連のリスクが倒産に結びつくと思いますか。

リスクの影響度 / 監査未実施の理由	思う		重大な影響は受ける		重大な影響は受けない		わからない	
経営者層が重要性を認識していないため	5	10.6	26	10.9	13	17.8	9	10.7
システム監査実施のためのコンセンサス、組織風土が十分に備わっていない	19	40.4	97	40.6	29	39.7	29	34.5
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	11	23.4	86	36.0	22	30.1	18	21.4
システム監査の方法、制度、手続きなどが十分でない	12	25.5	59	24.7	10	13.9	15	20.5
効果が明確でない	9	19.1	59	24.7	21	28.8	30	13.1
適切なシステム監査人が見つからない	3	6.4	31	13.0	14	19.2	11	7.1
計	47	-	239	-	73	-	84	-

システム監査との関係で455件の回答のうち、倒産に結びつくと「思う」10.3%(47件)、「重大な影響を受けると思う」52.5%(239件)であった。「重大な影響は受けない」は16.0%(73件)と低い割合であった。倒産に結びつくかどうかに対する認識をもとに、システム監査未実施に対する割合をみると、「経営者層が重要性を認識していない」について、「思う」(回答数47)では10.6%(5件)、「重大な影響を受けると思う」(回答数239)件では10.9%(26件)であったが、これらに対して「重大な影響を受けない」(回答数73)では17.8%(13件)と若干の違いがみられた。

しかし、「実施のためのコンセンサス、組織風土が十分に備わっていない」との理由については、それぞれ、40.4%(19/47件)、40.6%(97/239件)、39.7%(29/73件)とあまり差がない。システム監査の「効果が明確でない」についても、それぞれ19.1%(9/47件)、24.7%(59/239件)、28.8%(21/73件)であった。また、「システム監査実施よりシステム化推進そのものに力点がある」では、「重大な影響を受けると思う」36.0%(86/239件)、「重大な影響は受けない」30.1%(22/73件)といった結果であった。こうした結果から、情報システム関連のリスクが倒産に結びつくか否かに関して、システム監査未実施との関連は必ずしも明確ではない。

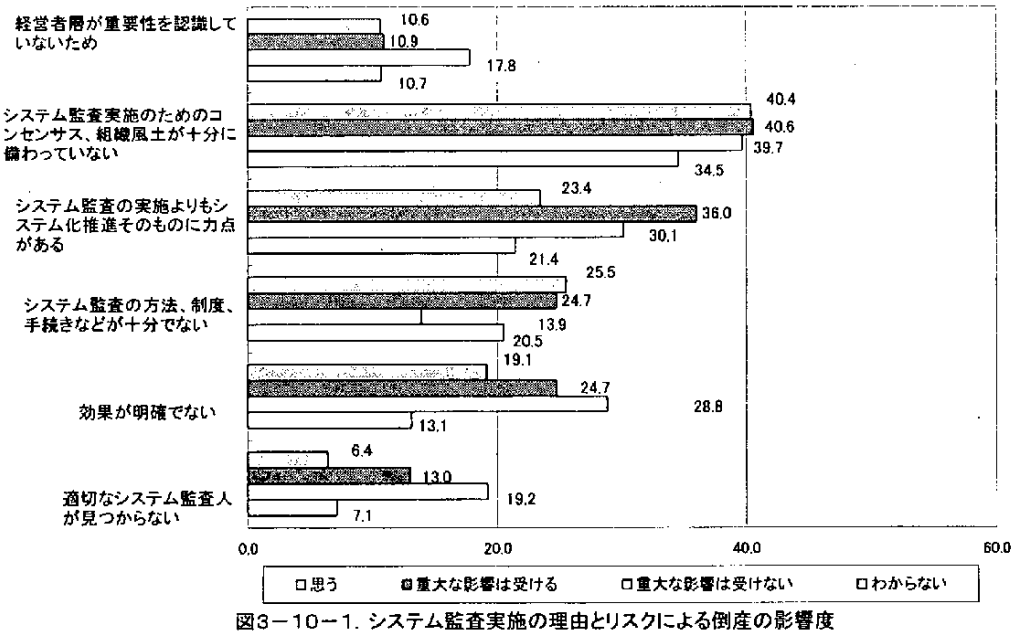


図3－10－1. システム監査実施の理由とリスクによる倒産の影響度

付属資料

「情報セキュリティに関する調査」
アンケート票

1 | | | | | |

(財)日本情報処理開発協会

2001年度

情報セキュリティに関する調査

貴社名（または団体名）		
所　在　地	〒　　Tel　　－　　－ 内線	6
ご回答者　所属/役職名		ご芳名

		千億	百億	十億	億	千万	百万	
資本金（非営利法人においては、基金、出資金等）	7							円

		十万	万	千	百	十		
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							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。

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

1	経済産業省の安全対策の施策について

Q１．経済産業省で制定している安全対策の各施策を知っていますか。施策ごとに回答して下さい。

	施　　策	利用している	知っている	知らない
22	情報システム安全対策基準（平成７年８月改訂）	1	2	3
23	コンピュータウイルス対策基準（平成７年７月改訂）	1	2	3
24	コンピュータ不正アクセス対策基準（平成８年８月制定）	1	2	3
25	システム監査基準（平成８年１月改訂）	1	2	3
26	システム監査企業台帳制度（平成３年３月制定）	1 (注)	2	3

（注）システム監査企業台帳を利用している場合は１を選択して下さい。

Q２．情報処理振興事業協会（ＩＰＡ）がコンピュータウイルスおよびコンピュータ不正アクセス被害の届出機関として指定されていることを知っていますか。

	被　　害	知っている	知らない
27	コンピュータウイルス被害（届出機関）	1	2
28	コンピュータ不正アクセス被害（届出機関）	1	2

Q３．不正アクセスの被害を受けた組織等からの依頼を受けて、被害の実態調査、被害状況の侵入手口の分析、再発防止策の検討と助言を行う「ＪPCERT／CC（コンピュータ緊急対応センター）」を知っていますか。

29

1	知っている
2	知らない

Q４．「ＪＩＳ Q2001 規格　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）を知っていますか。

30

1	利用している
2	知っている
3	知らない

Q５．「ＪＩＳ Q15001 規格　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）を知っていますか。

31

1	利用している
2	知っている
3	知らない

Q６．情報処理技術者試験制度で新設された「情報セキュリティアドミニストレータ試験（ＳＳ試験）」（平成１３年秋期より試験開始）を知っていますか。

32

1	情報セキュリティ担当者をＳＳ試験に受験させている
2	知っている
3	知らない

Q７．貴事業体での情報セキュリティアドミニストレータの意義についてお答え下さい。

33

1	今後、人材として必要と考えている
2	人材として必要ない

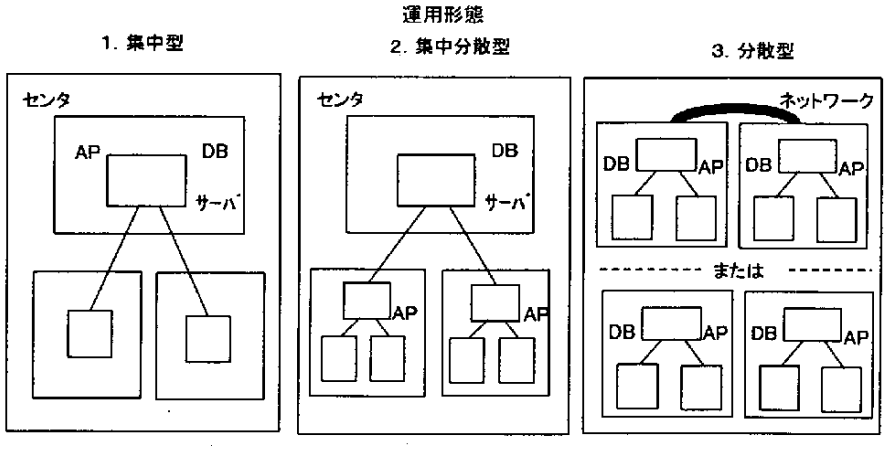
34 B

2 情報システム資産・費用について

Q８．貴事業体の基幹システム(注)はどのように運用されていますか。（単一回答）

35

1	集中型
2	集中分散型
3	分散型



（注）基幹システムとは貴事業体が事業継続上必要とされる主要業務の遂行に欠くことのできない日常業務および決算業務の情報システムの総称ですが、ここではその中で最も重要なシステム１つに限定してお答え下さい。

Q９．基幹システムが１時間以上停止した場合、経営に与える影響（被害額注）がどれぐらいになるか想定していますか。

36

1	は　い
2	いいえ

⇒Ｑ１１へ

注）被害額には売上の逸失額、賠償金額、原状回復費用を含む。

Q10．その場合の被害の推定額は１日あたりどれぐらいですか。

37

	影　響（被害額）
1	１０億円以上
2	５億円以上～１０億円未満
3	１億円以上～５億円未満
4	５千万円以上～１億円未満
5	１千万円以上～５千円未満
6	１千万円未満

Q11．アウトソーシング、サービスを含む、現在稼働中の全情報システムの開発・運用に関する年間総費用(注)の概算を教えて下さい。

38

1	１００億円以上
2	５０億円以上～１００億円未満
3	３０億円以上～５０億円未満
4	１０億円以上～３０億円未満
5	１億円以上～１０億円未満
6	５千万円以上～１億円未満
7	５千万円未満

注）年間総費用は、情報システムの開発・運用のために、アウトソーシング、サービス、リース、レンタル、回線使用料等、費用として過去１年間に支出した金額

Q12. 全情報システムへの年間総費用（上記）に対する下記の項目の割合は概算でどの程度ですか。

アウトソーシング（開発・運用・保守）	39				%
自社情報システム部門の人件費	42				%
リース／レンタル	45				%
ネットワーク・回線使用料など	48				%
減価償却費	51				%
その他	54				%
計		1	0	0	%

57 C

3 過去の障害等の実績について

Q13. 貴事業体の基幹システムは過去１年間にシステムの運用に影響を与えるシステムダウンが発生しましたか。

58

1	全体的にダウンした
2	部分的にダウンした
3	しない ⇒Ｑ１７へ

Q14. 過去１年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。（複数回答）

59	1	自然災害
60	2	電源障害
61	3	空調等障害
62	4	通信事業者に起因する障害
63	5	ＩＳＰ（インターネットサービスプロバイダ）等、社外のインターネットに起因する障害
64	6	ネットワーク機器などの障害
65	7	ハードウェア障害
66	8	ＯＳ障害
67	9	ソフトウェア障害
68	10	コンピュータウイルス
69	11	火災による事故・障害
70	12	人の悪意（たとえば内部犯罪、不正侵入）による事故等
71	13	オペミス等人の過失による事故等
72	14	その他（　　）

（注１）システムダウンとは、システムの全面ストップもしくはそれに準じる障害と定義します。
（注２）１回の事故について原因が複数考えられる場合は、主要原因のみご記入下さい。

Q15. 基幹システムにおけるＭＴＢＦ（平均故障間隔）は何時間ですか。
（注）ＭＴＢＦは、特定期間をとり、次の計算式で算出されます。
（システム稼働時間）／（ダウン回数＋１）
例）１年間 24 時間稼動中に２回ダウンした場合 →（365 日×24H）／（2 回+1）＝2,920 時間

73 | | | | | | 時間 | 77

Q16. 基幹システムにおけるＭＴＴＲ（平均修理時間）は何分ですか。

78 | | | | | 分 | 81

82 D

4 情報セキュリティ管理一般について

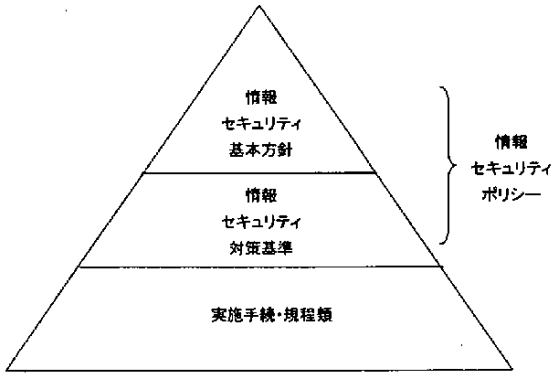
Q17. 貴事業体では、情報セキュリティ対策に情報システム関連支出の何パーセントを使っていますか。

83 [| | | %] 85

以下の質問では、情報セキュリティポリシーについてお尋ねします。ここでは、平成１２年７月に官邸が定義した情報セキュリティの３階層をベースにしたものを想定しております。

なお、図の詳細については、官邸の「情報セキュリティポリシーに関するガイドライン」をご参照下さい。

［ＵＲＬ］http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html



Q18. 貴事業体では経営理念に基づく情報セキュリティポリシー、実施手続・規程類を定めていますか。

	策定項目	定めている	現在作成中である	作成を検討している	定めていない	必要ない
86	情報セキュリティポリシー	1	2	3	4	5
87	実施手続・規程類	1	2	3	4	5

⇩ Q20へ　　Q22へ

Q19. 情報セキュリティポリシー、実施手続・規程類は定期的に見直していますか。

	策定項目	い る	いない
88	情報セキュリティポリシー	1	2
89	実施手続・規程類	1	2

Q20. （Q18で情報セキュリティポリシーを定めている／作成中の場合）貴事業体の情報セキュリティポリシーは次のどれを参照していますか。（複数回答）

90	1	BS7799、ISO/IEC17799、情報セキュリティポリシーに関するガイドライン（官邸）
91	2	日本銀行や金融情報システムセンター（FISC）のポリシー
92	3	COBIT（Control Objective for Information and related Technology）などのデファクト標準
93	4	自社で独自に開発

Q21. （Q18で実施手続・規程類を定めている／作成中の場合）情報セキュリティに関する実施手続・規程類には出張中、移動中の環境について定めていますか。

94	1	い る
	2	いない

Q22. 以下の管理について、責任を有する担当者を定めていますか。

	管理項目	定めている	設置を検討している	定めていない	必要ない
95	ネットワークの管理	1	2	3	4
96	情報システムの管理	1	2	3	4
97	情報セキュリティの管理	1	2	3	4

Q23. 緊急時のための連絡手段を持っていますか。

98	1	複数の連絡手段を持っている
	2	持っている
	3	検討中である
	4	持っていない
	5	必要ない

Q24. 情報セキュリティ管理についての問題点は何ですか。（複数回答）

99	1	経営者層の理解が得られない
100	2	コストがかかりすぎる
101	3	組織の従業員に対する教育・訓練がいきとどかない
102	4	組織の従業員に対する負担がかかりすぎる
103	5	ノウハウが不足している
104	6	どこまでやればよいのか基準が示されていない
105	7	要求に合致するもの（サービス）がない
106	8	組織の従業員に倫理観が乏しく、情報を財産と認識する風土がない
107	9	情報セキュリティ管理が事業の国際化に見合っていない
108	10	その他（　　）
109	11	特に問題はない

Q25. 次の各行為をコンピュータ犯罪だと思いますか。各項目ごとに犯罪度欄の該当する番号に○をつけて下さい。

	行　為　項　目	犯　罪　度					
110	市販のソフトをコピーして使う	1	2	3	4	5	6
111	データ、プログラムを無断で使う	1	2	3	4	5	6
112	データ、プログラムを覗き見る	1	2	3	4	5	6
113	就業時間内に会社のコンピュータを私用に使う	1	2	3	4	5	6
114	WWWを仕事以外（個人目的での発注、アンケート回答等）で利用する	1	2	3	4	5	6
115	私用の電子メールを送・受信する	1	2	3	4	5	6
116	他人のＩＤを無断借用する	1	2	3	4	5	6
117	業務上入手した顧客情報を正当な理由なしに第三者に売却する	1	2	3	4	5	6

犯罪度欄の回答群１～６は次のように定義します。

１．特に問題ではない	２．問題であると思う
３．企業内で戒告・訓告・注意処分等の対象となる	４．企業内で懲戒免職の対象となる
５．犯罪行為である（刑法上の処罰の対象となる）	６．わからない

118 E

5	災害対策・障害対策について

Q26. 情報セキュリティポリシー、実施手続・規程類に基づき災害・障害対策が明確にされていますか。

119	1	情報セキュリティポリシーや実施手続・規程類の中で明確になっている
	2	他の基準で扱っている
	3	特に定めていない（情報セキュリティポリシーがない場合も含む）

Q27. 非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。

120	1	作成している	
	2	作成中である	
	3	作成を含め検討中である	⇒Q２９へ
	4	作成していない	
	5	必要ない	

Q28. （Q27 の）危機管理マニュアルには以下の項目を含んでいますか。含まれている項目を選んで下さい。（複数回答）

121	1	サイバーテロ
122	2	ネットワークセキュリティ上の緊急事態
123	3	事故・災害（火災、地震、風水害等）
124	4	障害（機械故障、回線障害等）
125	5	プログラムミス、オペレーションミス等のシステムの誤り
126	6	その他（　　）

Q29. 非常事態に備えて従業員に対して情報セキュリティの面から訓練を実施していますか。

127	1	定期的に実施している
	2	時々実施している
	3	特に実施していない

Q30. 情報システムの災害に対する復旧対策としてどのようなことを実施していますか。実施している対策を選んで下さい。（複数回答）

128	1	手作業への復帰（緊急時の手作業マニュアルが作成されている場合に限る）	
129	2	同種コンピュータのユーザと相互バックアップ契約を交わしている	
130	3	バックアップサービス業者と契約を交わしている	
131	4	別の場所にバックアップセンタを設置している	
132	5	ネットワークのバックアップを行っている	
133	6	サーバのバックアップ用ファイルを専門保管業者に依頼して保管している	⇒Q３２へ
134	7	サーバのバックアップ用ファイルを遠隔地の自社施設に保管している	
135	8	サーバのファイルは、遠隔地にミラーファイルを持っている	
136	9	ＰＣ中の業務用ファイルは、バックアップを取っている	
137	10	ＰＣ中の業務用ファイルのバックアップは、遠隔地に保管している	
138	11	その他（　　）	
139	12	特に対策を講じていない	⇒Q３１へ

Q31. 対策を講じない理由は何ですか。主な理由を１つだけ選んで下さい。

140	1	経営者層の理解が得られない
	2	コストがかかりすぎる
	3	必要性を感じていない
	4	満足する対策がない
	5	その他（　　）

Q32. 情報システムの障害対策として次の機能を設けていますか。現在設置している機能を選んで下さい。（複数回答）

141	1	デュアルシステム	⇒Q３４へ
142	2	デュプレックスシステム	
143	3	ホットスタンバイシステム	
144	4	コールドスタンバイシステム	
145	5	クラスタリング	
146	6	高可用性機構	
147	7	ミラリング	
148	8	フォールトトレラント	
149	9	特に設けていない	⇒Q３３へ

注）基幹システムがメインフレームの場合は、１～４を、クライアントサーバシステムの場合は５～８から選択して下さい。

Q33. 対策を講じない理由は何ですか。主な理由を１つだけ選んで下さい。

150	1	経営者層の理解が得られない
	2	コストがかかりすぎる
	3	必要性を感じていない
	4	満足するもの（機能）がない
	5	その他（　　）

151 F

Q34. コンピュータ室、データ保管場所、ネットワーク設備室、コンピュータ設置場所ではそれぞれどのような火災対策をとっていますか。各場所ごとに実施している対策を選んで下さい。（複数回答）

対策項目	コンピュータ室	データ保管場所	ネットワーク設備室	コンピュータ設置場所
自動火災報知設備を設置している	152 1	153 2	154 3	155 4
ハロン消火設備を設置している	156 1	157 2	158 3	159 4
CO_2消火設備を設置している	160 1	161 2	162 3	163 4
スプリンクラ消火設備を設置している	164 1	165 2	166 3	167 4
排煙設備を設置している	168 1	169 2	170 3	171 4
耐火金庫を設置している	172 1	173 2	174 3	175 4
消火・排煙等の防災機器の点検を定期的に行っている	176 1	177 2	178 3	179 4
その他（右の欄に具体的に対策を書いて下さい）	180 1	181 2	182 3	183 4
特に対策を講じていない	184 1	185 2	186 3	187 4

Q35. コンピュータ室、データ保管場所、コンピュータ設置場所ではどのような地震対策をとっていますか。各場所ごとに実施している対策を選んで下さい。（複数回答）

対策項目	コンピュータ室	データ保管場所	コンピュータ設置場所
建物が免震構造になっている	188 1	189 2	190 3
転倒防止措置を講じている	191 1	192 2	193 3
機器の移動防止措置を講じている	194 1	195 2	196 3
フリーアクセス床は耐震構造としている	197 1	198 2	199 3
媒体の落下防止措置を講じている	200 1	201 2	202 3
その他（右の欄に具体的に対策を書いて下さい）	203 1	204 2	205 3
特に対策を講じていない	206 1	207 2	208 3

Q36. 電源設備の災害対策として、どのような対策をとっていますか。実施している対策を選んで下さい。（複数回答）

209	1	ＡＶＲ
210	2	ＣＶＣＦ／ＵＰＳ
211	3	自家発電装置
212	4	電力供給経路の複数化
213	5	その他（　　）
214	6	特に対策を講じていない

Q37. 水冷の空調設備を使っている場合、空調用の水は何日分確保していますか。

215	1	１日分～３日分
	2	４日分～６日分
	3	７日分以上
	4	まったく確保していない
	5	水冷の空調設備を使用していない

Q38. 情報システム、ネットワーク室、機器の災害・障害等で今後強化しなければならないと思うものは何ですか。（複数回答）

216	1	自然災害
217	2	電源障害
218	3	空調等障害
219	4	回線障害
220	5	ハードウェア障害
221	6	ＯＳ障害
222	7	ソフトウェア障害
223	8	火災による事故・障害
224	9	人の悪意による事故等
225	10	オペミス等、人の過失による事故等
226	11	テロによる機器の運用停止（ＤＤＯＳ：ＤＯＳアタックを含む）
227	12	取引先システムの停止や異常処理

Q39. システム災害・障害対策についての問題点は何ですか。（複数回答）

228	1	経営者層の理解が得られない
229	2	コストがかかりすぎる
230	3	要員に対する教育訓練がいきとどかない
231	4	要員に対して負担がかかりすぎる
232	5	ノウハウが不足している
233	6	どこまでやれば良いのか基準が示されていない
234	7	要求に合致するもの（製品）がない
235	8	その他（　　）
236	9	特に問題はない

Q40. どのようなネットワーク機器、サービスの障害を想定していますか。（複数回答）

237	1	通信事業者のケーブル障害（含む、専用回線）
238	2	通信事業者の設備障害
239	3	通信事業者のサービス（電話、パケット交換など）中断・サービス低下、停止
240	4	ＩＳＰ（インターネットサービスプロバイダ）サービスの中断・停止
241	5	ＬＡＮ（配線）の障害
242	6	ルータ・サーバ（機器）の障害
243	7	地震などの一定地域の災害
244	8	その他（　　）
245	9	特に想定していない

Q41. どのようなネットワーク障害対策を実施していますか。実施している対策を選んで下さい。（複数回答）

246	1	異なる種別回線を利用
247	2	異なる交換局への収容
248	3	異なるコモンキャリアの利用
249	4	異なるＩＳＰを利用
250	5	異なるメディアによる回線利用（例：衛星回線等）
251	6	ポイント間接続から網接続へ
252	7	重要回線を部分的に二重化
253	8	専用のバックアップ回線を常時設定
254	9	専用回線とインターネットＶＰＮなどの異種サービスの組み合わせ
255	10	社内の構内回線、ＬＡＮ等を二重化
256	11	通信機器（ＣＣＵ、ルータ、社外ＷＷＷサーバ、ＤＮＳサーバ、アクセスサーバ等）の二重化
257	12	インターネットに接続したサーバの分散（負荷分散、地域分散）
258	13	その他（　　）
259	14	特に対策を講じていない

260 G

6 不正アクセス対策・不正侵入対策について

Q42. 「不正アクセス行為の禁止等に関する法律」（平成１１年８月公布）を知っていますか。

261	1	知っている
	2	知らない

Q43. 貴事業体では過去１年間に不正アクセスの被害に遇われたことがありますか。（複数回答）

262	1	物理的なアクセス被害（コンピュータ室等への侵入）に遭った
263	2	論理的アクセス被害（ネットワーク経由による侵入）に遭った
264	3	な　い　⇒Ｑ４５へ

Q44. 不正アクセス被害届出機関である情報処理振興事業協会（ＩＰＡ）に被害を届け出ましたか。

265	1	出した
	2	出さない

Q45. ①主要なネットワーク室や機器、コンピュータ室またはデータ保管室での物理的な不正アクセス対策はどのようなものですか。現在実施している対策を選んで下さい。（複数回答）
②（Q45で「１」と答えた場合のみ）このうち、不正アクセスの被害を契機として実施した対策を選んで下さい。（複数回答）

不正アクセス対策	①実施対策	②不正アクセス被害後の対策
不正アクセスを受けた場合の、ＩＰＡやＪＰＣＥＲＴ／ＣＣ（コンピュータ緊急対応センター）への相談	266 1	277 2
室の出入口で入室管理を行っている	267 1	278 2
室の出入口で退室管理を行っている	268 1	279 2
室への入退室についてカード、パスワードを使用している	269 1	280 2
入退室のときにアンチパスバック（定期券のように二度連続して入れないような仕組み）を持っている	270 1	281 2
室への入室について身体的特徴（指紋、虹彩等）による識別を行っている	271 1	282 2
室の管理責任者を定めている	272 1	283 2
情報システムの監視設備を設けている	273 1	284 2
定期的にリスク分析や情報セキュリティ監査を実施	274 1	285 2
その他（　　）	275 1	286 2
特に対策を講じていない	276 1	287 2

（注）データ保管室とは、データ、プログラム等を含む記録媒体およびドキュメントを保管する「独立した室」であり、室内に置かれるデータ保管庫は含みません。

Q46. ①ネットワークを介しての論理的な不正アクセスに対して講じている対策は何ですか。現在実施している対策を選んで下さい。（複数回答）
②（Q43で「２」と答えた場合のみ）このうち、不正アクセスの被害を契機として実施した対策を選んで下さい。（複数回答）

不正アクセス対策	①実施対策	②不正アクセス被害後の対策
不正アクセスを受けた場合の、ＩＰＡやＪＰＣＥＲＴ／ＣＣへの相談	288 1	300 2
パスワードの活用	289 1	301 2
ファイアウォールの利用	290 1	302 2
アクセス制御ソフトウェアの使用	291 1	303 2
社外からのアクセスのために設置しているアクセスサーバへのアクセスにワンタイムパスワードや呼び返し接続等の追加的コントロールを実施	292 1	304 2
ネットワーク機器の運用者（アクセス範囲）を限定	293 1	305 2
情報セキュリティポリシーで勝手にＬＡＮの配線を触ったり、個人のＰＣを接続することを禁止	294 1	306 2
情報セキュリティ管理者がサーバやルータ、ファイアウォールのログを定期的にチェック	295 1	307 2
ネットワーク管理者がサーバやルータ、ファイアウォールのログを定期的にチェック	296 1	308 2
定期的にリスク分析や情報セキュリティ監査を実施	297 1	309 2
その他（　　）	298 1	310 2
特に対策を講じていない	299 1	311 2

Q47. 情報についての機密度のランクを設定していますか。

312	1	い る
	2	いない

Q48. 貴事業体では基幹システムのパスワード変更をどのレベルに設定していますか。(単一回答)

313	1	ワンタイムパスワードを設定している
	2	変更期限がきたらパスワードを無効にする
	3	定期的に新しいパスワードを配布する
	4	変更期限を定めて利用者が変更している
	5	パスワードの変更を推奨しているが、変更期間は利用者に任せている
	6	パスワードの変更に関して特に定めていない
	7	パスワードによる管理を実施していない
	8	その他 ( )

Q49. 貴事業体では暗号を採用していますか。採用している暗号を選んで下さい。(複数回答)

314	1	暗号装置を購入
315	2	市販の暗号ソフトウェアを購入
316	3	自社で作成した暗号ソフトウェアを使用
317	4	利用しているアプリケーションに付随しているので、暗号機能を利用
318	5	その他 ( )
319	6	採用していない ⇒Q51へ

Q50. 暗号化している情報は次のどれですか。(複数回答)

320	1	伝送するデータすべて
321	2	伝送するデータのうち重要なもの(プログラムなど)
322	3	記録媒体上のデータすべて
323	4	記録媒体上の重要なもの(プログラムなど)
324	5	認証情報(署名)
325	6	重要なトランザクションデータ(カード番号などの)の転送に利用
326	7	その他 ( )

Q51. PKI(公開鍵基盤)について貴事業体はどのような方針をお持ちですか。

327	1	導入済み
	2	導入を前提に評価中
	3	検討の結果、当面導入の予定はない
	4	検討していない

Q52. 貴事業体では不正アクセス対策について従業員に教育・訓練の場を設けていますか。

328	1	情報セキュリティ教育に関して定期的に実施している
	2	社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している
	3	情報セキュリティポリシーや対策基準類に従って実施している
	4	その他 ( )
	5	特に実施していない

Q53. 不正アクセス対策についての問題点は何ですか。（複数回答）

329	1	経営者層の理解が得られない
330	2	コストがかかりすぎる
331	3	不正アクセス侵害事件や対策に関するタイムリーな情報収集ができていない
332	4	組織の従業員に対する教育訓練がいきとどかない
333	5	組織の従業員に対する負担がかかりすぎる
334	6	ノウハウが不足している
335	7	どこまでやれば良いのか基準が示されていない
336	8	要求に合致するもの（製品）がない
337	9	その他（　　）
338	10	特に問題はない

339 H

7 コンピュータウイルス対策について

Q54. 貴事業体では過去１年間にコンピュータウイルスに感染したことがありますか。

340	1	あ　る
	2	な　い　⇒Ｑ５９へ

Q55. コンピュータウイルス被害届出機関である情報処理振興事業協会（ＩＰＡ）に被害を届け出ましたか。

341	1	出した
	2	出さない

Q56. 感染したコンピュータは何台ですか。

342	1	１０台未満
	2	１０台以上～２０台未満
	3	２０台以上～５０台未満
	4	５０台以上～１００台未満
	5	１００台以上～２００台未満
	6	２００台以上～５００台未満
	7	５００台以上～１，０００台未満
	8	１，０００台以上

Q57. 主要な感染原因（経路）は判明していますか。主な原因を選んで下さい。（複数回答）

343	1	フリーソフトウェアから
344	2	外部から入手した記録媒体から
345	3	社内ネットワーク経由で
346	4	インターネット経由で
347	5	電子メールの添付書類で
348	6	外部のホームページの閲覧で
349	7	その他（　　）
350	8	わからない

Q58. 貴事業体では、過去１年間に、外部に対してコンピュータウイルスに感染したメールを送ったり、感染したファイルを送ってしまったことがありますか。

357

1	あ る
2	な い
3	把握していない

Q59. ①コンピュータウイルスに対して講じている対策は何ですか。現在実施している対策を選んで下さい。(複数回答)
②(Q54で「１」と答えた場合のみ)このうち、ウイルス被害を契機として実施した対策を選んで下さい。(複数回答)

コンピュータウイルス対策	①実施対策	②ウイルス被害後の対策
コンピュータウイルス被害を受けた場合のＩＰＡへの相談	352 1	373 2
ウイルス対策用のマニュアル(セキュリティ対策基準に入れた場合も含む)の作成	353 1	374 2
ウイルス対策チーム(社内でウイルスが検出された時の対応を行うチーム)の設置	354 1	375 2
ウイルス検出時や緊急対応と連絡体制の整備	355 1	376 2
ソフトウェアの出所の確認	356 1	377 2
記録媒体のウイルスチェックの実施	357 1	378 2
ライトプロテクト、バックアップ等のソフトウェア管理	358 1	379 2
ＰＣでのワクチンソフト（ウイルス検出ソフトを含む）の利用	359 1	380 2
ＰＣのワクチンソフト・パラメータファイルを定期的に更新	360 1	381 2
サーバ機でのワクチンソフトの利用	361 1	382 2
メール用ゲートウェイ／サーバでのワクチンソフトの利用	362 1	383 2
メール用ゲートウェイ／サーバでの添付ファイルの制限（例：実行ファイル削除）	363 1	384 2
ワクチンソフトの集中監視	364 1	385 2
定期的な集中監視ログの解析	365 1	386 2
パスワードの変更等、アクセスコントロールの強化	366 1	387 2
動作の定期的な確認等、異常発見体制の整備	367 1	388 2
緊急時の電子メールサーバの停止	368 1	389 2
緊急時の社員への連絡（ウイルス警告の放送／送付）	369 1	390 2
ウイルス対策サービスの利用	370 1	391 2
その他（ ）	371 1	392 2
特に対策を講じていない	372 1	393 2

Q60. 貴事業体では従業員に対し、コンピュータウイルス対策に関する教育・訓練の場を設けていますか。

394

1	情報セキュリティ教育に関して定期的に実施している
2	社内教育用の情報セキュリティ教育カリキュラムに従って時々実施している
3	情報セキュリティポリシーや実施手順、規定類に従って実施している
4	その他（ ）
5	特に実施していない

Q61. コンピュータウイルス対策についての問題点は何ですか。(複数回答)

395	1	経営者層の理解が得られない
396	2	コストがかかりすぎる
397	3	コンピュータウイルス情報や対策に関するタイムリーな情報収集ができていない
398	4	組織の従業員に対する教育訓練がいきとどかない
399	5	組織の従業員に対する負何がかかりすぎる
400	6	ノウハウが不足している
401	7	どこまでやれば良いのか基準が示されていない
402	8	要求に合致するもの(製品)がない
403	9	適切な委託先がない
404	10	その他( )
405	11	特に問題はない

406 [ ]

8 情報リスクマネジメント関連について

Q62. 情報セキュリティ要素1~10のうち、貴事業体にとって重要と思われる要素を3つ選び、下の回答欄に優先順位をつけて記入して下さい。

	情報セキュリティ要素
1	情報セキュリティポリシー(経営者の積極的な関与)
2	情報セキュリティ組織(情報セキュリティの推進組織の構築と活動)
3	情報資産の分類および管理(情報資産のリスク評価とそれによる重要度の分類)
4	人的セキュリティ(役職員への教育訓練や内部規則の策定など)
5	物理的および環境的セキュリティ(入退室管理や安全区画の構築など)
6	通信および運用管理(ネットワークの管理、ウイルス対策、ログ管理など)
7	アクセス制御(IDとパスワード管理、不正アクセス対策など)
8	システム開発およびメンテナンス(開発環境のセキュリティ、ライブラリ管理運用など)
9	事業継続管理(災害対策、障害対策など)
10	準拠(法律遵守、システム監査など)

回答欄	優先順位	第1位 407		第2位 409		第3位 411	

Q63. 情報セキュリティの確保にとり、基本的に重要な視点は何だと思いますか。(複数回答)

413	1	経営者層の理解
414	2	管理者の理解
415	3	担当者の理解
416	4	社内全体の理解
417	5	法規制の整備
418	6	その他( )

Q64. 経営者層はコンピュータ関連の事件・事故に対するリスクについて関心が高いですか。

419	1	高 い
	2	中 位
	3	低 い
	4	わからない

Q65. 情報システムに係わるリスク分析を実施していますか。

420	1	行っている
	2	行っていない ⇒Q67へ

Q66. リスク分析を実施した際の問題点は何ですか。(複数回答)

421	1	経営との関係がわからない	⇒Q68へ
422	2	確立した手法がない	
423	3	分析のためのデータが乏しい	
424	4	専門家がいない	
425	5	組織ができていない	
426	6	その他 ( )	
427	7	問題点は特にない	

Q67. リスク分析を実施しない理由は何ですか。(複数回答)

428	1	重要性を感じていない
429	2	手法がわからない
430	3	予算がない
431	4	発生被害額が算出できない
432	5	リスク分析の意味がわからない
433	6	効果がわからない
434	7	効果があるとは思えない

Q68. システム監査を実施していますか。(業務監査に含まれている場合を含む)

435	1	い る	⇒Q70へ
	2	いない	

Q69. システム監査を実施していない理由は何ですか。(複数回答)

436	1	経営者層が重要性を認識していないため
437	2	システム監査実施のためのコンセンサス、組織風土が十分に備わっていない
438	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
439	4	システム監査の方法、制度、手続きなどが十分ではない
440	5	効果が明確でない
441	6	適切なシステム監査人が見つからない
442	7	その他 ( )

Q70. 情報システム関連のリスクが倒産に結びつくと思いますか。

443	1	思 う
	2	重大な影響は受けると思う
	3	重大な影響は受けない
	4	わからない

444 J

9	情報セキュリティマネジメントシステム（ＩＳＭＳ）について

Q71.「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」を知っていますか。

445

1	よく知っている
2	知っている
3	存在だけ知っている
4	知らない

⇒Ｑ７９へ

Q72. ＩＳＭＳ適合性評価制度をどのように考えますか。

446

1	国際規格であり望ましい
2	国際規格よりも厳しい日本独自のものを追加して作成すべきである
3	旧安全対策基準等を活用すれば十分である
4	わからない

（注）ＩＳＭＳ適合性評価制度はISO/IEC 17799およびBS 7799-2を参考としたものです。

Q73. ＩＳＭＳ適合性評価制度はISO9000やISO14000シリーズと同様に取引条件や安全性に関する評価基準として利用できると思いますか。

447

1	客観的な評価として利用できる
2	一定の目安となる
3	あまり利用できない
4	全く利用できない
5	わからない

Q74. ＩＳＭＳ適合性評価制度の認証取得を予定していますか。

448

1	予定している
2	予定していない

⇒Ｑ７９へ

Q75. ＩＳＭＳ適合性評価制度の認定取得の目的は何ですか。主な目的を１つだけ選んで下さい。

449

1	地方自治体等公的団体への入札条件として
2	民間企業との取引条件として
3	外部への一般的な情報セキュリティ保証として
4	自社内部の情報セキュリティ目標として
5	海外企業との取引条件として
6	その他（　　）

Q76. ＩＳＭＳ適合性評価制度の認証取得のために必要となるコスト負担についてどのように考えますか。

450

1	非常に大きい
2	大きい
3	小さい
4	非常に小さい
5	新たなコストは発生しない
6	わからない

Q77. ＩＳＭＳ適合性評価制度の認証取得によって期待している効果はどのようなことですか。（複数回答）

451	1	経営陣の理解が得られる
452	2	取引先からの信用が得られる
453	3	投資する情報セキュリティ予算額の目標が得られる
454	4	自社のイメージがアップする
455	5	他社との差別化が図れる
456	6	わからない

Q78. 海外との取引において、相互承認制度はまだありませんが、相互承認ができればＩＳＭＳ適合性評価制度の基準が役に立つと感じますか。

457	1	海外企業との取引に極めて有効である
	2	海外企業との取引にあまり意味があると思わない
	3	他の基準の方が役に立つ
	4	わからない
	5	海外との取引を行わない

458 K

10 個人情報保護について

貴事業体で取り扱っている個人情報（インハウス情報を含む）についてお答え下さい。

Q79. 個人情報の利用目的は何ですか。（複数回答）

459	1	売買等契約の履行
460	2	顧客サポート
461	3	代金等の回収
462	4	情報提供
463	5	マーケティング
464	6	商品開発
465	7	従業員の管理（インハウス情報）
466	8	行政サービスの履行
467	9	その他（　　）

Q80. 利用している個人情報の収集方法はどのように行っていますか。（複数回答）

468	1	申込書等によって情報主体（当該個人）から直接に収集
469	2	名簿業者等から購入
470	3	グループ企業から入手
471	4	他社から提供を受ける
472	5	業務委託契約等に基づき提供を受ける
473	6	その他（　　）

Q81. 情報主体から直接に収集する場合、収集・利用目的について同意を取っていますか。

474	1	は　い
	2	いいえ

Q82. 間接的に収集する場合、収集・利用目的について情報主体から同意をとっていますか。

475	1	情報主体から同意をとっている
	2	入手先が情報主体の同意をとっていることを確認している
	3	何もしていない

Q83. 貴事業体では顧客等の個人情報データをコンピュータ処理するに際して、個人情報保護の観点からの内部規程（たとえば、個人情報保護規程など）を定めていますか。

476	1	定めている	
	2	作成中である	
	3	検討中である	⇒Q85へ
	4	定めていない	

Q84. 個人情報の廃棄方法を個人情報保護規程に定めていますか。

477	1	定めている
	2	作成中である
	3	検討中である
	4	定めていない

Q85. 個人情報の取扱いに関する責任と権限を持った管理者を定めていますか。

478	1	定めている
	2	検討中である
	3	定めていない

Q86. 個人情報の取扱いに関する情報主体からの苦情処理を行う窓口がありますか。

479	1	あ　る
	2	な　い

Q87. 情報主体から、自己情報の開示や訂正または削除等を求められた場合、応じることになっていますか。

480	1	なっている
	2	なっていない

Q88. 個人情報を外部委託する場合に交わす条項には何がありますか。（複数回答）

481	1	秘密保持義務
482	2	責任分担
483	3	個人情報の適正な管理
484	4	その他（　　）
485	5	外部委託を行っていない

Q89. （財）日本情報処理開発協会の「プライバシーマーク制度」（平成１０年４月運用開始）を知っていますか。（複数回答）

486	1	知っている
487	2	知らない
488	3	プライバシーマークを利用したい
489	4	利用したいと思わない（理由を書いて下さい：　　）

○今後必要と思われる情報セキュリティ制度・サービス・機能・製品等がありましたら、具体的にお書き下さい。

○貴事業体で実施している情報セキュリティ対策について、問題点があれば具体的に書いて下さい。

ご協力ありがとうございました。

490 L

KEIRIN このアンケートは競輪の補助金を受けて実施するものです。

平成14年3月発行

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

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