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12年3月

JIPDEC

財団法人　日本情報処理開発協会

KEIRIN

この資料は、競輪の補助金を受けて作成したものです。

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、867組織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。ご回答いただいた組織体、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12年3月

財団法人日本情報処理開発協会

平成11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	(株)CRC総合研究所　公共システム事業部　本部長役
	笠間誠一	(株)日立製作所　金融・流通システムグループ エンジニアリングサポート統括センタ　システム企画部　技師
	指田朝久	東京海上リスクコンサルティング株式会社 第二事業部主席研究員
	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　情報流通研究グループ 情報流通ネットワーク研究担当エグゼクティブ・リサーチャー
	松原榮一	日本ガートナーグループ(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。

1.2 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4，714事業体の情報システム部門を対象としている。

1.3 調査時期

調査表発送	平成11年10月29日
回収締切	平成11年12月24日

1.4 回収状況

発送数	4,714件
回収数	867件
回収率	18．4%

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%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が多くなった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。

1.5 回答組織体の平均従業員数

2,192人

1.6 調査項目

1．通商産業省の安全対策の施策について（4項目）
2．情報システム資産について（7項目）
3．過去の障害等の実績について（4項目）
4．セキュリティ管理一般について（14項目）
5．災害対策・障害対策について（18項目）
6．不正アクセス対策・不正侵入対策について（13項目）
7．コンピュータウイルス対策について（6項目）
8．情報リスクマネジメント関連について（15項目）
9．個人情報保護について（6項目）

今回の質問構成は全体で87項目からなっており、平成9年度調査に比べ25項目増加した。この増加は単に項目数を増やしたにとどまらない。たとえば、通商産業省の安全対策について前回は8項目であった。今回は4項目となっているが、質問項目数が減少したのではない。前回と異なり、質問の仕方を変え、合成することが可能な場合には1項目にまとめることにした。その他の領域においても、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、新たな質問項目を加味している。

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、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。

1．7　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。

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	25	2,277	情報処理サービス	情報処理サービス業・ソフトウェア業	89	577
	繊維工業	14	1,167	その他対事業所ｻｰﾋﾞｽ	農・林・漁・狩・水産養殖業	2	492
	紙・ﾊﾟﾙﾌﾟ・紙加工品製造業	8	1,251		鉱業	2	449
	印刷業・同関連産業	4	1,164		建設業	50	1,612
石油・化学・鉄鋼・非鉄・金属	化学工業	36	1,987		新聞業・出版業	7	1,764
	石油製品製造業	6	1,449		不動産業	6	518
	鉄鋼業	16	2,534		運輸・通信・倉庫業	32	3,358
	非鉄金属製造業・金属製品製造業	32	1,176		電力・ガス業	7	8,400
電気・一般・輸送・精密機械	一般機械器具製造業	34	921		放送業	9	1,881
	電気機械器具製造業	44	5,237		広告・調査・情報提供サービス業	5	1,015
	輸送用機械器具製造業	24	5,020		その他のサービス業	24	1,213
	精密機械器具製造業	23	1,304	公共ｻｰﾋﾞｽ	医療業	8	755
その他製造業	窯業・土石製品製造業	14	1,239		宗教法人	1	600
	その他製造業	57	1,824		高校	6	94
商　業	卸業・商社	66	743		大学	14	476
	小売業	33	1,999		その他の教育機関	11	88
金融・保険業	金融業	78	1,091		学術研究機関	5	289
	証券業・商品取引業	3	444		法人団体・農協	17	802
	生命保険業	3	5,767	政府・地方公共団体	政府	5	16,471
	損害保険業	7	2,988		地方公共団体	40	10,056
小　計		527	-	小　計		340	-
合　計						867	平均　2,192

1．8　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9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、「3．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. 通商産業省の安全対策施策について

通商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14．1%が「利用」しており、「知っている」のは49．5%であった。『コンピュータウイルス対策基準』の場合は12．0%が「利用」しており、「知っている」のは54．3%である。『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』については「利用している」のは若干低く10%台で、それぞれ、10．0%、10．6%である。また、「知っている」はそれぞれ51．6%、56．3%であった。知っていながらなぜ利用する割合が低いのか、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35．8%であるが、「利用している」のは1．6%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64．0%(H9:57．3%)で、前回調査の回答より6．7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57．1%(H9:44．7%)が「知っている」と回答しており、前回よりも12．4ポイントと大幅に増加している。これは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32．8%であり、届出制度と比べてかなり低くなっている(Q3)。

今回、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』に関して新たに質問を設けた。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、JIS Q 15001について「知っている」と回答したのは14．0%であった。事業者が広く個人情報に関わっている状況に鑑みてかなり低い割合であった(Q4)。

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総投資金額、ハードウェア、ソフトウェア、データの割合、資産価値評価の有無、重要情報価値の比較、基幹システムの運用形態等について考察してみた。

情報システムへの総投資金額は、前回調査とさほど変化はみられないが、パソコンの占める割合は平均で27．9%(H9:24．4%)と前回よりも3．5ポイント増加している。関連ソフトの充実やインターネットの普及等によりパソコンが組織体において重視されてきている表れといえる(Q5)。

総投資金額に対するハードウェア、ソフトウェア、データの割合は、ハードウェア54．6%(H9:57．5%)、ソフトウェア37．1%(H9:35．0%)、データ8．2%(H9:7．5%)となっている。前回調査と比べて、ハードウェアの割合は減少し、ソフトウェア、データがわずかながら増加している(Q6)。

全情報システムへの総投資金額の動向について、「上昇傾向」と回答したのは30．9%（H9：35．6%）、「ほぼ横ばい」は44．5%（H9：45．8%）、「下降傾向」は20．1%（H9：14．6%）となっている（Q7）。業種により差異があるが、該して景気を反映してか「上昇傾向」は前回調査より減少し、「下降傾向」が増加している。

資産価値評価の有無については（どのような評価方法を用いて評価したかは明らかではないが）、評価したことが「ある」のは7．8%（H9：5．8%）、「ない」は89．2%（H9：91．0%）であった（Q8）。前回と比べて評価実施の割合は若干高まっており、肯定的に考えれば、経営上、評価する意味が理解されてきていると思われる。だが、「ない」という89．2%の回答が気になるところである。

重要情報価値の比較については今回初めて取り上げた質問項目である。何が重要情報かは組織体の判断によるが、この点について比較したことが「ある」と回答したのは3．7%と低い割合であった（Q10）。しかし、「意味がない」という回答は1．5%ときわめて低く、問題は比較の意味がどこにあるのか明確でないところにありそうである。

基幹システムの運用形態について（Q11）は、前回調査と異なり選択肢を3つとした。運用形態として47．8%は依然としてメインフレーム等を中心とする集中型であった。この集中型に分散型の機能を有している集中分散型が38．2%で、ほとんどの組織体はメインフレームをベースにシステムを運用している。この点は、経済環境と情報システムへの投資が関係していると思われる。なお、分散型は12．2%となっている。

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11．4%であり、前回調査の13．2%に比べて1．8ポイント低い。「部分的なダウン」は40．3%（H9：39．5%）と、前回を若干上回っている。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（Q12）。

さて、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44．6%で、「ソフトウェア障害」の34．6%を10．0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37．3%となっており、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（H9は回線障害で回答：33．7%）より15．4%と大幅に減少している。なお、「自然災害」、「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（Q13）。

基幹システムにおける平均故障間隔（MTBF）は2，784．9時間で、前回調査の3，286．0時間よりかなり短縮されている。平均修理時間（MTTR）は128．0分と前回調査の101．8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（Q14、Q15）。

4．セキュリティ管理一般について

セキュリティ管理に関するベースとしてセキュリティポリシーは組織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18．9%と前回調査の27．0%から8．1ポイント減少している。「定めていない」は43．5%であり、

前回の38．5%より5．0ポイント増加している。回答結果については、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という今回調査の視点から、質問の表現を変えたことに関係があるかもしれない。しかし、「現在作成中」が9．3%と前回の6．0%より3．3ポイント増加している(Q16)。

セキュリティガイドラインとしての操作および業務処理手順の策定状況については、それを「定めている」のは27．9%で、前回調査の『セキュリティポリシーを定めている』とした回答の27．0%に近似している。なお、「定めていない」とする回答も39．2%で、前回調査の38．5%にかなり近い。「現在作成中である」が8．2%、「作成を検討している」は23．1%となっており、両者を合計すると31．3%となり、前回のセキュリティポリシーについての回答(32．4%)に近い割合となっている。ところで、「必要ない」は0．6%であった。回答結果については、今回「セキュリティガイドライン」として質問を明確にしたことが関係しているかもしれない(Q17)。

現在のIT環境を考えれば、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。そこで今回セキュリティガイドラインとして操作および業務処理手順を定めているか否か、新たに質問したわけであるが、この点についてセキュリティガイドラインを有しているのは26．0%であった(Q18)。

セキュリティガイドラインについては、現代の情報リスク環境に鑑みればガイドラインの見直しは不可欠と思われる。そこで、新たに設けたのがQ19である。この点、「定期的に見直しをしている」と回答したのは54．1%で、回答組織体の半数以上が見直しを行っている。しかし、見直しを「行っていない」組織体も38．8%に上っている。

基幹システムのネットワーク管理者についての質問は新たに設けたものであるが、「定めている」のは76．4%であった。これに「現在検討中」(5．0%)、「定めるか検討している」(3．8%)を加えると、約85%の組織体がネットワーク管理者を必要としていることが把握できる。基幹システムがネットワーク環境下で用いられ、パソコンも同様の環境において利用されていることが関係していると思われる。なお、「定めていない」は13．1%、「必要ない」は1．2%となっている(Q20)。

さて、情報システムの管理者については、「定めている」のは87．0%であった。これに「現在検討中」(3．3%)を加えると90%を超え、前回調査より高い割合となっている(Q21)。

また、専任のセキュリティ管理者ないし担当者の設置については、「いる」と回答したのが23．8%であった。「設置を検討している」のが12．5%である。なお、「いない」のは62．2%と高かったが、「必要ない」とする否定的な回答の割合はわずか1．0%であり、ほとんどの組織体は専任の管理者なり担当者を必要と考えている(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」のは75．4%と、組織体4に対して3が有していることとなる。「検討中」は9．6%、「持っていない」は13．5%であったが、「必要ない」は0．7%と非常に低い割合であった(Q23)。

データの使用・保管等の管理に関しては、「管理を行っている」という回答(90．0%)は前回調査に比して1．6ポイント高かった(Q24)。

ネットワーク化が進んでいると思われる今日、基幹システムを国際的に展開・利用している実態について新たな質問(Q25)を設けたわけであるが、国際的な展開に基幹システムを利用しているのは6．7%とかなり低く、「実施していない」割合は92．8%であった。しかしこの点は、わが国の次のような事情によるのかもしれない。すなわち、既存の基幹システムをそのまま国際的な展開に利用するのは稀で、国際的な展開が必要な場合には、必要に応じて情報システムを構築するといわれている。したがって、上記の基幹システムに関して情報システムのセキュリティ対策を講じているかという質問(Q26)に対する回答にも注意が必要かもしれない。基幹システムを国際展開に利用しているとの回答について情報システムのセキュリティ対策を「講じている」のは72．4%であった。「講じる予定」は13．8%であったが、国際的な展開の場でありながら「まったく考えていない」のが8．6%という結果であった。

そこで、セキュリティ対策を講じている場合、セキュリティ対策は何に準拠して策定したか(Q27)

については「独自の対策」によるのが76．2%で、「展開国先の法規制」のためが7．1%であった。なお、「取引先企業の要請」という自主性のない回答は「ゼロ」であった。

情報システムのセキュリティ対策を講じていない理由を明らかにするため、情報セキュリティ管理についての問題点を求めた質問（Q28）に対しては次のような回答結果であった。「組織の従業員に対する教育・訓練がいきとどかない」48．6%（H9：37．1%）、「コストがかかりすぎる」47．9%（H9：44．1%）、「どこまでやればよいのか基準が示されていない」47．2%（H9：47．3%））、「対策を構築するノウハウが不足している」44．8%（H9：39．4%）という回答がそれぞれ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」という選択肢以外、今回の回答はいずれも前回の割合を上回っている。したがって、問題状況の認識が明らかになりつつあるとみることもできる。だが、「どこまでやればよいのか」といった基準の提示の困難さは相変わらずのことなのかもしれない。「コストがかかりすぎる」ため講じないとする側面については、Q35のバックアップ対策（65．6%）、Q37の代替運転機能（71．8%）、Q45のシステム・障害対策（80．6%）への回答に比べるとかなり低い割合となっている。しかし、Q60の不正アクセス対策（40．3%）と比較すると若干高い割合を示している。

コンピュータ犯罪意識に関する質問（Q29）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54．2%（H9：50．7%、H7：38．4%）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、「企業内でも戒告等の処分の対象となる」（30．1%）、「犯罪行為である」（29．4%）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」割合は平成7年度、9年度に比べて減少傾向にあるが、「犯罪行為である」（18．8%）という認識は高まってきている。●『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46．4%であり、「企業内で戒告等の処分の対象になる」のが33．6%であった。「犯罪」という認識は5．1%と低い。ところが、●『コンピュータウイルスを伝染させる』行為については60．6%が「犯罪行為である」と回答し、18．3%は「企業内でも訓告等の処分の対象になる」としており、犯罪という理解は定着したといえる。●『他社のシステムへ侵入する』場合も、それが「犯罪行為である」とする割合は80．0%と高く、「企業内での処分の対象になる」側面を加えると90%を超え、コンピュータウイルスの場合と同様の理解が定着している。●『他人のパスワードを解読し、使用する』場合も調査のたびごとに「犯罪行為である」との認識が高まっている。今回調査では58．6%となり、「企業内での処分対象」との回答を加えると86%を超える。●『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34．8%、「犯罪行為である」が26．2%、「問題であると思う」のが25．4%と、犯罪という認識では他人のパスワードを解読し、使用する場合より低い。この点は、仕事にかかわるシステム利用実態が関係しているものと思われる。●『メール、ブラウザ等接続されたままの他人のマシンを操作する』行為については、「問題であると思う」（54．0%）としながらも、「犯罪行為」とみなす割合は9．9%と相対的に低い。この点はネットワークに接続された状態で他人のマシンもグループで使用する実態もあり、こうした状況に対する教育なり対応が必要と思われる。●『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受信する』、『時間外に会社のコンピュータでゲームを行う』という行為は組織体のコンピュータの私的な利用に関する質問であるが、いずれも48．4%～52．1%の組織体が「問題であると思う」としている。しかし、『私用の電子メールを受信する』と『時間外に会社のコンピュータでゲームを行う』については「特に問題ではない」とする回答が20%を超えている。組織体としてやむをえないと黙認している現状がありそうである。この点、「特に問題ではない」とする割合はWWWについては8．2%と低く、電子メール等の場合と厳しさに違いがみられる。●『ネットワークにログインしている他人のマシンのファイルを見る』というアクセスに関するこの項目は平成11年度の新規項目で、43．7%が「問題であると思う」としている。しかし、「特に問題ではない」とする割合は10．1%で、「犯罪行為である」（10．0%）とほぼ

同じ割合となっている。●『共有サーバにある仕事に関係していないファイルを見る』のは47．5%が「問題であると思う」とし、他人のマシンのファイルを見る場合より高い割合となっている。しかし、「特に問題ではない」とする割合は17．8%と7．7ポイント高い。その反面、「犯罪行為である」割合は3．3%と低く、認識に差異がみられる。●『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』という項目では84．7%が「犯罪行為である」としている。これに「企業内で懲戒免職の対象となる」(7．8%)を加えると90%以上が厳しい認識を示している。平成11年度には業務上入手した顧客情報を第三者に売却するという事件が発生し問題視された。事件に対する認識が回答結果に反映されていると思われる。

5. 災害対策・障害対策について

災害対策・障害対策に関して多くの質問項目を用意した。この点は情報システムのセキュリティにとり重要性が高いことによっている。特に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(Q30)は、前回調査より4．6ポイント増え、33．0%が「作成している」と回答している。しかしながら、「作成していない」とする割合の方が35．6%と多いが、前回調査の41．9%に比べて6．3ポイント減少している。

ところで、非常事態に備えて従業員に対する訓練の実施状況について、今回、情報セキュリティの訓練について新たに質問を設けたところ、「危機管理マニュアルに従って定期的に実施している」のはわずか5．2%であった。「時々実施している」のは9．7%で、「マニュアルに従って訓練している」のは14．9%と低かった。マニュアルは作るが訓練には消極的であるという側面が浮き彫りにされたといえる。ただ、「マニュアルはないが実施している」のが6．8%と、訓練の重要性を窺わせている。しかしながら、訓練を「特に実施していない」とする割合が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(Q32)。

さて、情報システムのセキュリティにおけるバックアップ体制はどうであろうか。実施対策の内容に関して回答率が高いのは「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)」で36．6%(H9:25．3%)、次いで新規選択項目の「ネットワークのバックアップ」が31．5%、「バックアップ用のコンピュータを設置」が24．3%(H9:14．8%)といった回答結果で、前回調査時に比べてバックアップへの重要性に対する認識の高まりが感じられる。しかし、「特に対策を講じていない」が25．5%であった。情報セキュリティの点でも事後的な対応が感じられるものの、平成7年度の62．7%、9年度の45．0%に比べ大幅な改善が認められる(Q34)。なお、「対策を講じない」理由で回答率が最も高いのは「コストがかかりすぎる」の65．6%(H9:72．9%)であった(Q35)。

情報システムでは情報セキュリティの観点から代替運転機能を設けていると思われるが、この点に関して前回の調査項目に新たな機能を加味して質問を構成した(Q36)。その結果、前回調査で「その他」の回答が4．0%であったが、今回最も高い回答率を示したのは新たに選択項目とした「ミラリング」の32．2%であった。デュアルシステム、デュプレックスシステム、ホットスタンバイシステム等については前回とさほど変化はみられない。ただ、「特に設けていない」とした前回の回答率66．5%に対して、今回調査では46．3%と約20ポイント減少している。なお、代替運転機能を設けない理由は、バックアップ対策と同様に「コストがかかりすぎる」(71．8%)ことにあった(Q37)。

ファイルに限定したバックアップ対策については前回調査に比べてさほど顕著な変化は認められなかった(Q38)。しかしながら、「対策を講じない」理由に関して「コストがかかりすぎる」が前回調査では37．2%であったが、今回は66．7%と大幅に増加した(Q39)。基幹システムにおけるファイルのバックアップ頻度については、「1日に1回程度」という回答が66．4%(H9:55．6%)と、頻度の高いバックアップの必要性が感じられる(Q40)。

火災対策については、前回調査にネットワーク設備室とコンピュータ設置場所を加え、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」70．0％（H9：71．2％）、「ハロン消火設備」48．4％（H9：56．0％）の順で高く、前回同様の結果となった。またデータ保管室では「自動火災報知設備の設置」57．4％（H9：58．9％）、新規選択項目である「消火・排煙等の防災機器の定期的点検」41．3％、「耐火金庫の設置」37．4％（H9：43．2％）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はデータ保管場所と同様の結果であった(Q41)。

地震対策に関しては、前回同様のコンピュータ室、データ保管場所にコンピュータ設置場所を加えて調査を行った。結果はほぼ前回と同じく、コンピュータ室で最も多い回答は「転倒防止措置」36．1％（H9：36．8％）で、次いで「フリーアクセス床は耐震構造」29．3％（H9：33．5％）であった。データ保管場所では「転倒防止措置」24．9％（H9：25．7％）で、次いで「媒体の落下防止措置」15．7％（H9：15．9％）であった。前回との大きな相違点は「特に対策を講じていない」と「無回答」についてであった。たとえば、コンピュータ室については、「特に対策を講じていない」37．0％（H9：0．9％）、「無回答」2．4％（H9：42．8％）であった。コンピュータ設置場所についての割合はそれぞれの選択項目についてコンピュータ室とデータ保管場所との中間くらいであった(Q42)。

電源設備についての対策では、今回調査では圧倒的に「CVCF/UPS」76．7％（H9：48．7％）が多く、「自家発電装置」でも24．8％（H9：7．5％）と前回調査をかなり上回る充実ぶりを示している(Q43)。

情報システム、ネットワーク室、機器の災害・障害対策の今後の方向性における今後の考え方(Q44)として次のような傾向が選択項目への回答から得られた。すなわち、「自然災害」、「電源障害」、「空調等障害」、「ハードウェア」、「OS障害」、「ソフトウェア障害」、「火災による事故・障害」については「現在のままでよい」とする回答が低くて45％台、高くて71％台であった。これらに対して「回線障害」、「人の悪意による事故等」、それに「オペミス等人の過失による事故等」はいずれも「強化する」が「現在のままでよい」を上回っていた。この点は現在の情報環境における問題状況を明確に物語っているといえる。

システム災害・障害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80．6％（H9：81．5％）と高い回答率となっている。次いで「どこまでやればよいのか基準が示されていない」42．3％（H9：42．8％）、「対策を構築するノウハウが不足」31．8％（H9：36．5％）となり、コスト、基準、それにノウハウが前回調査の場合と同様、問題であることが理解できる(Q45)。

ところで、ネットワーク環境下での問題状況として、今回若干表現を改め、ネットワーク機器・サービス障害について質問を行った。特に回答率の高かったのは「ルータ、DSNサーバなどのLAN機器の障害」66．0％、次いで「基幹LANの障害」62．3％であった。ネットワーク障害としてこれまでの調査結果では平成7年度、9年度ともに通信ケーブル切断といった物理的な障害がトップであったが、今回調査では、新たに設けた選択項目である「LAN関連」の項目（「ルータ、DSNサーバなどのLAN機器の障害」、「基幹LANの障害」）が高く、ネットワーク障害が業務に与える影響を問題にしていることが理解できる(Q46)。

ネットワーク障害に対する対策については、「異なる種別回線を利用」19．6％（H9：20．7％）、「重要回線を部分的に二重化」19．5％（H9：19．7％）、「専用のバックアップ回線を常時設定」16．0％（H9：15．4％）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48．6％（H9：51．9％;H7：56．3％）と傾向的には対策を講じていない割合は減少しているが、ネットワーク時代における業務との関連から、種々の対策を考慮する必要がありそうである(Q47)。

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47．4%であり、半数を少々下回った(Q48)。

不正アクセスの被害状況についての質問では、6．1%(H9：2．9%)が被害にあったことがあるとしている。前回調査と比べて増加しているのは、インターネットの普及と関係がありそうである(Q49)。では、不正アクセスの被害を被った組織体に対しIPAに被害届を出したかどうか質問したところ、20．8%(H9：15．6%)が「出した」と回答している。Q2では57．1%(H9：44．7%)がIPA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。また、不正アクセスにより被害を被った際、JPCERT/CCに相談したのであろうか。「相談した」という回答率は13．2%と低い(Q51)。Q3ではJPCERT/CCを32．8%が「知っている」と回答しており、IPAの場合と同様、乖離が認められる。なぜ相談しないのか、検討することが重要である。

情報システム機器、コンピュータ室、データ保管室、ネットワーク室等における不正アクセス対策として実施している対策はどうであろうか。最も高い割合は「室の管理責任者を定めている」44．2%(H9：19．3%)、「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」38．2%(H9：18．9%)、「室の出入口で入室管理を行っている」37．9%(H9：17．8%)と、いずれも前回の回答率を大幅に上回った(Q52)。ところで、前回設けていなかった新選択項目として「室の出入口で退室管理を行っている」かについては26．2%が「行っている」と回答し、入室の場合と10ポイント以上の差がみられた。

リモートアクセスについては、53．9%が「行っている」と回答しており、これは前回調査(53．8%)とほぼ同じである(Q53)。情報についての機密度のランク設定に関しては26．5%(H9：29．5%)と、前回を若干下回っている(Q54)。

ネットワークを介してなされる不正アクセスへの対応については、前回と比べて若干選択項目を増やし回答を求めた(Q55)。最も回答の多い「パスワードの活用」は83．4%(H9：72．8%)と前回を10ポイント以上も上回っている。次いで多いのが「ファイアウォールの利用」50．7%(H9：31．8%)で、前回調査より18．9ポイント増えている。新たに設けた「ネットワーク機器の運用者を限定」することについては40．9%、「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」することについては33．6%となっており、不正アクセス対応が複合的になってきていることを物語っている。

ところで、不正アクセス対策の問題点に関しては、「対策を構築するノウハウが不足」が40．9%(H9：39．0%)、「コストがかかりすぎる」が40．3%(H9：31．2%)と前回調査を上回り40%台となった。「どこまでやればよいのかの基準」は36．2%(H9：36．7%)と前回とほぼ同様であった。「従業員に対する教育訓練がいきとどかない」は37．0%(H9：29．9%)となり、Q59での教育訓練を「特に実施していない」(81．5%)実態と何らかの関連があるのかもしれない(Q60)。

7. コンピュータウイルス対策について

平成11年3月には新たな感染メカニズムをもち、従来型のウイルスに比べて感染力の強い「メリッサウイルス」が発生し話題となった。こうした状況下、コンピュータウイルス対策は重要な意味を有している。コンピュータウイルスに感染したか否か(Q61)については、54．6%が「ある」としており、

しかも前回の36．2%を18．4ポイントと大幅に上回っている。

それではコンピュータウイルスの被害に遇った場合の届出はどうなっているのであろうか。IPAに被害を届け出たのは13．5%(H9:19．9%)と前回調査を下回った。しかもQ2ではIPAについて64．0%が届出機関として指定されていることを「知っている」と回答していた(Q62)。こうした実態は、不正アクセスの場合と同様、何を物語っているのか、検討の必要性がある。

さて、主な感染経路であるが、この点については「外部から入手した記録媒体から」というのが多く59．2%で、前回の45．7%に比べて13．5ポイント増加した。今回新たに選択項目とした「電子メールの添付書類で」は52．6%で、マクロウイルスの影響が大きくなっている(Q63)。

コンピュータウイルス対策に関しては「ワクチンソフトの利用およびパラメータファイルの配布」が76．0%と多く、前回の「ワクチンソフトの利用」(59．1%)に鑑みて、今回新たに設けた選択項目を「ワクチン」と「パラメータファイルの配布」とに分けたほうがよかったかもしれない。新規の選択項目である「ウイルス検出時や緊急対応と連絡体制の整備」は37．1%で、「ソフトウェアの出所の確認」は25．6%(H9:24．9%)と前回とほぼ同様であった。なお、「特に対策を講じていない」は13．5%で前回の30．4%に比べて16．9ポイント減少しており、対策の必要性が高まってきている状況を示している(Q64)。

コンピュータウイルス対策の問題点に関しては、「コスト」(39．6%)、「どこまでやればよいのかの基準」(30．8%)に比べ、「従業員に対する教育訓練」の問題が41．1%と増加した(Q66)。この点は、Q65の教育訓練を「特に実施していない」が70．0%(H9:63．4%)であったが、この回答と何らかの関連が(不正アクセス対策での問題点の場合と同様に)あるのであろうか。

8．情報リスクマネジメント関連について

情報リスクへの対応においてはリスクマネジメントの視点が重要である。そこで新たに質問項目を設けた。リスクマネジメントの任務領域にはこれまで触れてきたセキュリティ管理、災害対策・障害対策等々が属している。隔年に行われてきた「情報セキュリティに関する調査」における構成との関係から、従来の項目と独立させてリスクマネジメント関連の項目をここに置くことにした。

さて、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」53．7%で、「管理者の理解」は30．4%であった。管理者より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。「担当者の理解」と「法規制の整備」は同じ割合で19．7%であった(Q67)。

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」25．5%、「中位」33．2%、「低い」18．3%といった結果であった。ただ、「わからない」が21．8%もあり、この認識はいかがなものであろうか(Q68)。

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」のはわずか12．0%で、86．3%は「行っていない」と回答している(Q69)。「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」(44．7%)と高く、次いで「効果がわからない」(33．2%)となっている。ただ、「重要性を感じていない」が19．3%もあり、「効果があるとは思えない」6．6%、「「リスク分析の意味がわからない」10．4%をあわせると、リスク分析に対して36．3%が否定的な見解を示したといえる(Q70)。

それでは「リスク分析を実施する際の問題点」は何なのであろうか。最も高い割合を示したのは「確立した手法がない」58．7%であった。かつてJIPDECが示した『リスク分析手法－JRAM－』は「手法」としてどうであったのか。情報環境の変化からすればすでに「古く役に立たない」と判断され

たのであろうか。いずれにせよ、リスク分析手法の確立が必要といえる。次いで多かったのは、「専門家がいない」49．0%、そして「分析のためのデータが乏しい」、「組織ができていない」がともに26．0%という結果であった(Q71)。

ところで、Q69でリスク分析を「行っている」と回答した104組織体においてリスク分析を行ったのは「情報システム部門内の要員」が63．5%であった。次いで、「関係部門を含めたプロジェクトチーム」12．5%、「外部のコンサルタント」8．7%という結果であった(Q72)。

情報にかかわるリスクについて昨今問題とされているのはシステミックリスクである。Q73においてシステミックリスクについて「システムを通して連鎖的に影響を及ぼすリスク」と解説しておいたが、このリスクを「重大と考える」のは55．6%であった。「さほど重大だと思わない」10．8%、「重大だと思わない」2．3%といった回答結果もみられ、業種差が認められる。ちなみに、金融・保険業では「重大と考える」が89．0%と高くなっている。

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」(12．3%)と「重大な影響は受けると思う」(48．2%)をあわせると6割以上の組織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(Q74)。

さて、システム監査の重要性についてであるが、53．9%(467組織体)が「重要と考える」と回答している(Q75)。Q1のシステム監査基準の認知度に関しては10．6%(92組織体)が「利用している」と回答した。システム監査を重視している467組織体がシステム監査を重要としながら実際にシステム監査基準を「利用している」のが92組織体という回答結果をどのように判断したらよいのか。この点の分析も今後の課題と思われる。しかもシステム監査を重大と思わない理由に関しては、「これまで重大なリスクなど起こらなかったため」が56．5%と半数を越えている。これまでリスクが起こらなければ今後も起こらないという考え方自体が問題である。ただ「システム監査の限界」が30．5%、「システム監査の理解が不十分」というのが28．0%であった(Q76)。

従業員に対する情報セキュリティの教育に関しては、85．0%が「実施していない」と回答している。「実施している」のはわずか12．9%であり、こうした状況は情報システムの安全対策の面から問題といえる(Q79)。

9．個人情報保護について

個人情報を利用している組織体が増え、プライバシー問題についての関心の高まりを受け、今回調査で新たに質問項目を設けた。顧客等の個人情報の利用については、42．1%が「はい」と回答している(Q82)。個人情報の利用目的では「顧客サポート」55．6%、「マーケティング」45．5%、「情報提供」36．2%といった結果であった(Q83)。

ところで、JIPDECが平成10年4月から運用している『プライバシーマーク制度』について、「知っている」のは20．0%であった(Q86)。Q4で触れた『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』に関しては14．0%が「知っている」と回答していた。これらの点を想起すれば、個人情報保護に対する公的な取組みについての認識度の低さが気になるところである。
(Q86)

2．調査結果の詳細

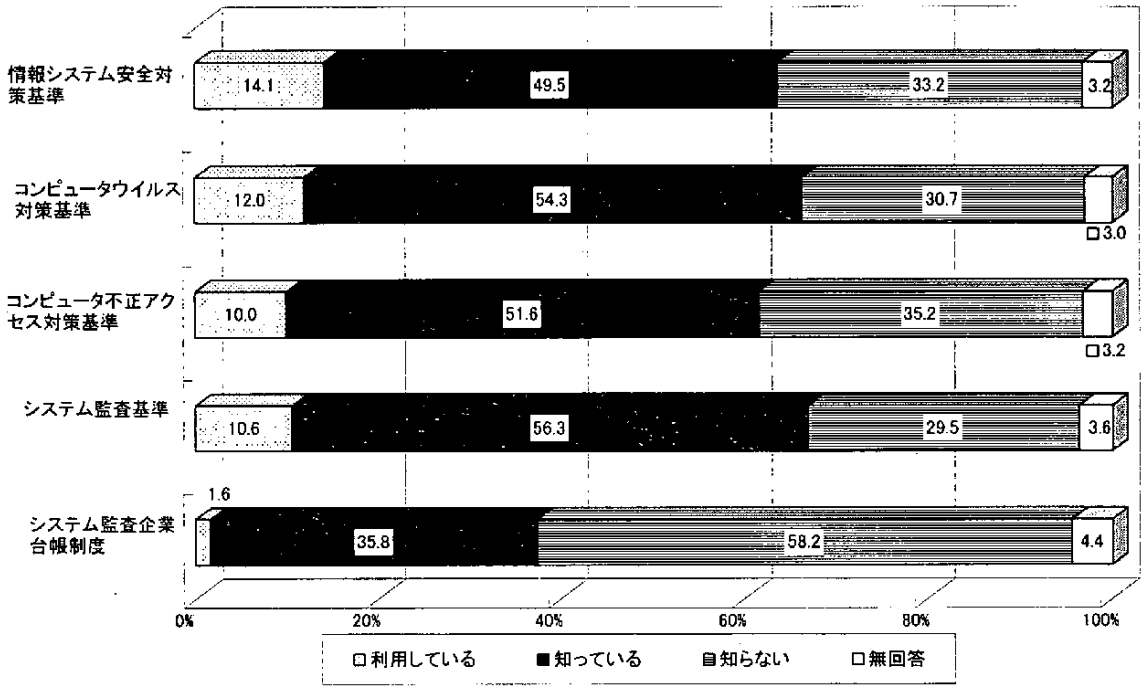
2．1　通商産業省の安全対策の施策について

Q1．通商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	122	14.1	429	49.5	288	33.2	28	3.2	867	100.0
コンピュータウイルス対策基準	104	12.0	471	54.3	266	30.7	26	3.0	867	100.0
コンピュータ不正アクセス対策基準	87	10.0	447	51.6	305	35.2	28	3.2	867	100.0
システム監査基準	92	10.6	488	56.3	256	29.5	31	3.6	867	100.0
システム監査企業台帳制度	14	1.6	310	35.8	505	58.2	38	4.4	867	100.0

Q1G1．通産省制定の安全対策関連施策の周知度



通商産業省が制定している情報セキュリティ関連基準の周知度合いについては、いずれも6割強が周知（「すでに利用している」、「知っている」）している。しかし、システム監査企業を一般の企業等に紹介することを目的に登録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37．4%と半数を下回っている。

情報システム安全対策基準は、電子計算機システム安全対策基準として昭和52年に制定、その後何度か改訂され、以来多くの組織体の安全対策策定の手本として活用されてきたことから、当然のことながら63．6%と高い周知度を示している。過去の調査結果をみると、平成5年度68．1%、7年度65．9%、9年度66．9%（7年度以外は、「利用している」と「知っている」の合計）と、若干低くなっているが、周知度が低くなったと捉える程度ではない。

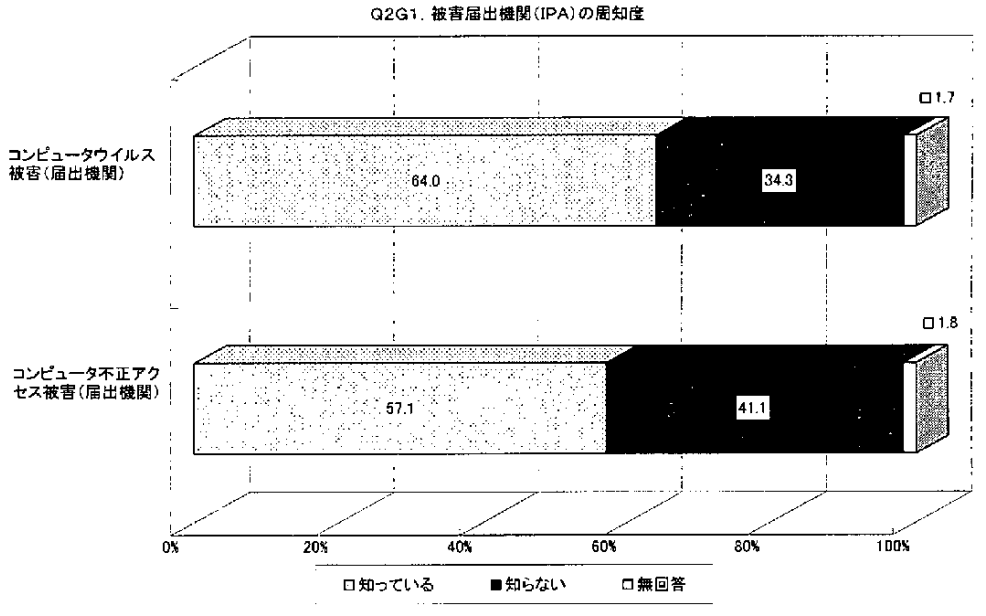
コンピュータウイルス対策基準（平成2年制定、7年改訂）の周知度については、5年度38．7%、7年度55．6%、9年度59．9%（5年度以外は「利用している」と「知っている」の合計）であり、今回の66．3%は着実に同基準が定着していることをうかがわせる結果となっている。なお、「利用している」との回答も7年度の6．3%、9年度の8．0%から12．0%へと徐々に増加しており、コンピュータウイルス被害の増加を反映している。

コンピュータ不正アクセス対策基準(平成8年制定)は、9年度の44．7%から大幅に増加して61．6%となっている。これは、基幹システムの形態が分散型に移行している傾向を反映しているためと考えられる。

システム監査基準(昭和60年制定)は、5年度は73．6%、7年度は72．8%、9年度は69．4%であったが、今回もほぼ同率(66．9%)で推移しているものの、少ない割合ながら減少傾向が続いている。

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)	555	64.0	297	34.3	15	1.7	867	100.0
コンピュータ不正アクセス被害(届出機関)	495	57.1	356	41.1	16	1.8	867	100.0



通商産業省は、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、回答の過半数が認めている。

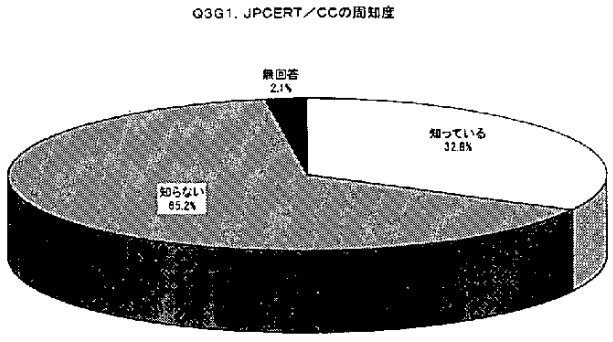
コンピュータウイルス被害届出機関に関しては、平成5年度33．0%、7年度45．2%、9年度57．3%であり、毎回周知の程度が増加している。業種別では大きな差異は特に認められないが、情報処理サービス(84．3%)、公共サービス(71．0%)等が高い周知度を示している。

また、情報システム資産の情報化投資額別(Q5で算出)では、「100億円以上」91．1%、「50～100億円未満」90．7%、「30～50億円未満」79．2%、「10～30億円未満」75．2%、「1～10億円未満」57．8%、「5千～1億円未満」41．3%、「5千万円未満」29．0%と、投資金額が多いほど周知度が高くなっている。

不正アクセス被害届出機関に関しては、前回調査では44．7%であったが、今回57．1%と大きく増加している。この場合も業種別、情報化投資額別ではウイルス被害届出機関と同様の傾向を示している。

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	284	32.8
2	知らない	565	65.2
無回答		18	2.1
計		867	100.0



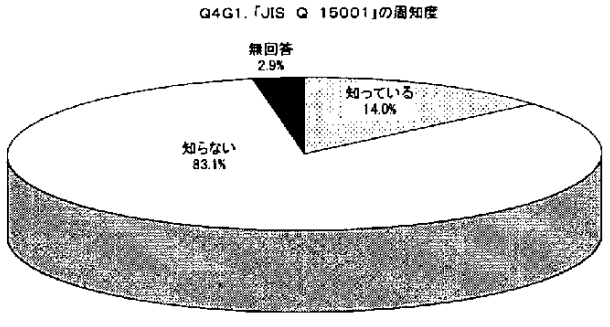
コンピュータ緊急対応センター(JPCERT／CC)は、平成8年8月に設立され、同年10月から本格的な業務を開始している。その目的は、特にインターネットに接続された組織体の情報システムが不正アクセスの被害を受けた場合、当該組織体からの依頼を受けて被害の実態調査、被害状況の侵入手口の分析、再発防止策の検討と助言を行うこと、さらにはサーバ関連ソフトのセキュリティホールに関する技術・警告等の情報提供を行うことにある。

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、32．8%の周知度にとどまっている。

業種別にみると、情報処理サービスが51．7%と高い割合を示しており、公共サービス(48．4%)、電気・一般・輸送・精密機械(36．8%)、政府・地方公共団体(35．6%)が続いている。情報化投資額別では、投資金額の多い組織体が高い周知度を示している。

Q4.「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	知っている	121	14.0
2	知らない	721	83.2
無回答		25	2.9
計		867	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)を制定した。

「JIS Q 15001」の周知度は、14．0%と低く、42．1%の組織体が顧客等の個人情報を取り扱っている(Q82参照)ことと、大きく乖離している。

業種別に周知度の高い順にあげると、情報処理サービス(46．1%)、その他対事業所サービス(14．6%)、公共サービス(14．5%)、金融・保険業(14．3%)となっている。これらの業種が個人情報を「取り扱っている」と回答した状況(Q82)は、情報処理サービス(48．3%)、その他対事業所サービス(44．4%)、公共サービス(38．7%)、金融・保険業(86．8%)となっており、情報処理サービス業の周知度合いと個人情報取扱い状況がほぼ一致しているものの、他の業種は「JIS Q 15001」の周知度合いが低いといえる。

ところで、「Q1」、「Q2」、「Q3」、「Q4」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:

・通商産業省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。

・通商産業省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。

・通商産業省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。

2．2　情報システム資産について

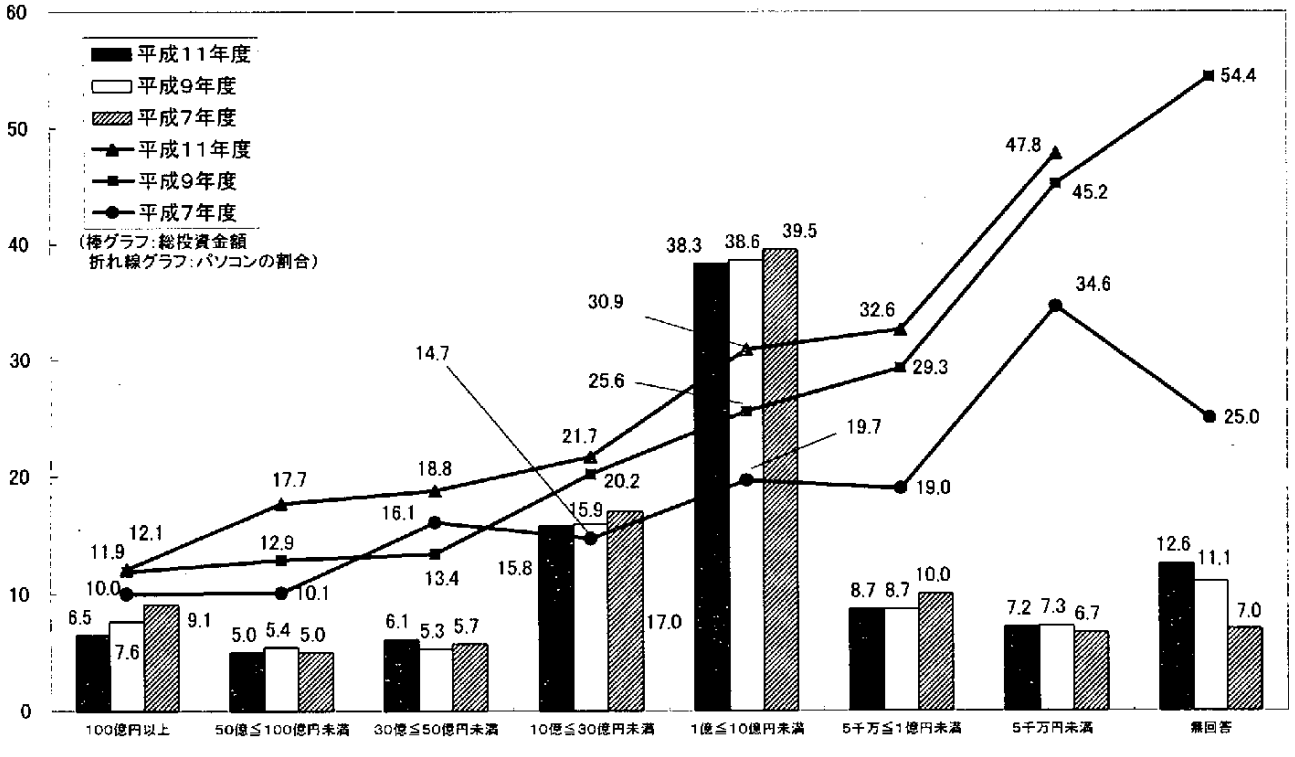
Q5．①ハードウェア、ソフトウェア、データを含む、現在稼働中の全情報システムへの総投資金額の概算を教えて下さい。

②また、パソコンの総投資金額に対する割合についても横の欄にご記入下さい。

		総投資金額の概算		パソコンの割合
1	100億円以上	56	6.5	12.1
2	50億円以上～100億円未満	43	5.0	17.7
3	30億円以上～50億円未満	53	6.1	18.8
4	10億円以上～30億円未満	137	15.8	21.7
5	1億円以上～10億円未満	332	38.3	30.9
6	5千万円以上～1億円未満	75	8.7	32.6
7	5千万円未満	62	7.2	47.8
無回答		109	12.6	－
計		867	100.0	平均　27.9

（注）総投資金額は、購入価格換算、レンタルはレンタル月額の45倍：全CPU，全周辺機器、全端末、全ソフトウェア、保有している全データの開発・購入費を含んだもの

Q5G1．コンピュータシステムの総投資金額とパソコンの割合



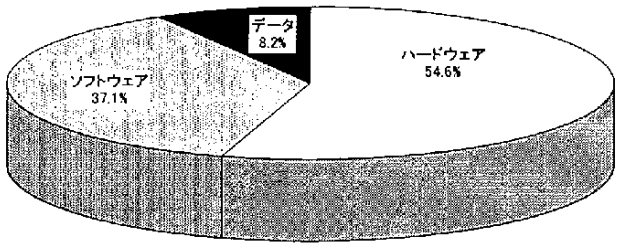
コンピュータシステムの総投資金額については前回調査と比べそれほどの差はでていないが、パソコンの占める割合は、平均で平成7年度18．1%、9年度24．4%、11年度27．9%と増加傾向にある。これは関連ソフトの充実、インターネットの普及などでパソコンが各組織体で不可欠のものとなりつつあることを意味している。

また、資本金別にみると、資本金500億円以上の組織体の42．2%が総投資金額を100億円以上としているが、総投資金額1～10億と見積もっている組織体が圧倒的に多い。

Q6. 全情報システムへの総投資金額(上記)に対するハードウェア、ソフトウェア、データの割合はどの程度ですか。(回答件数 715 件)

ハードウェア (平均)	54.6
ソフトウェア (平均)	37.1
データ (平均)	8.2

Q6G1. 全情報システムへの総投資金額の割合

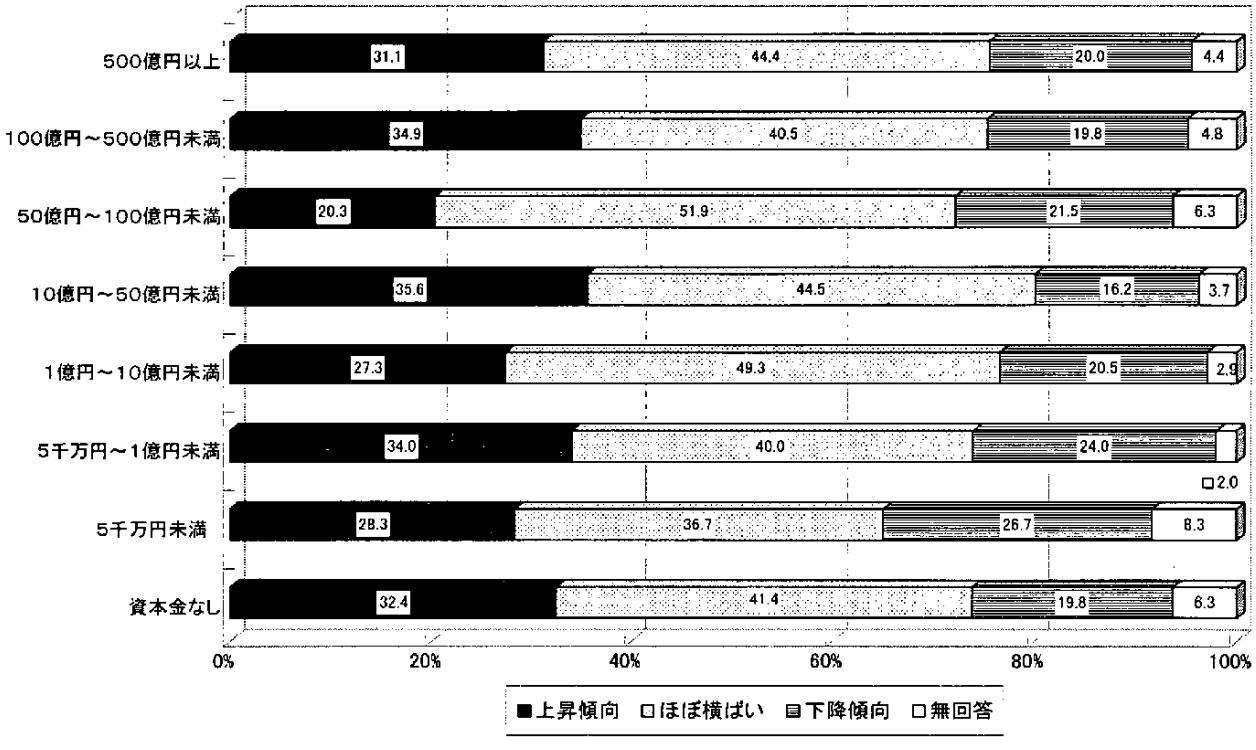


全情報システムへの総投資金額のうち、ソフトウェアの占める割合は平成7年度32.9%、9年度35.0%、11年度37.1%と増加傾向にある。これは、情報化社会への対応上高度な情報処理が必要となってきているからであろう。

Q7. 全情報システムへの総投資金額は、どのような傾向を示していますか。

1	上昇傾向	268	30.9
2	ほぼ横ばい	386	44.5
3	下降傾向	174	20.1
無回答		39	4.5
計		867	100.0

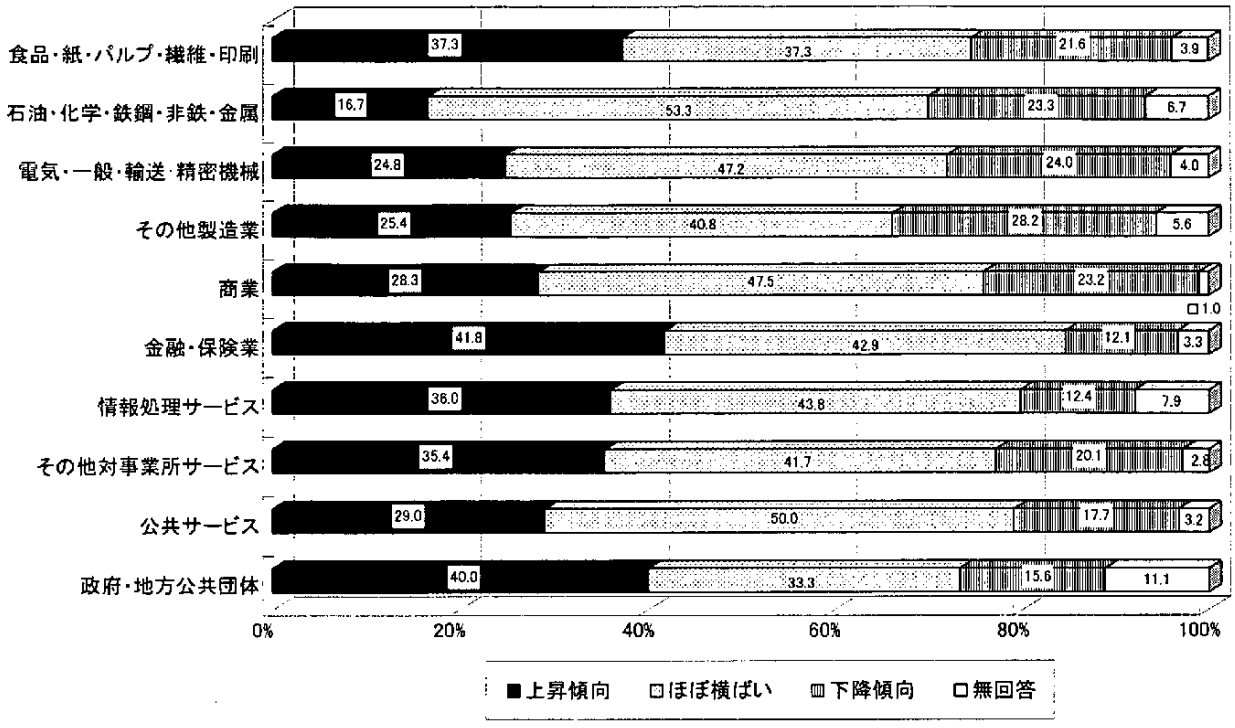
Q7G1. 全情報システムへの総投資金額の傾向



「上昇傾向」については前回調査(35.6%)より減少しており、「下降傾向」については増加(前回は14.6%)している。

全体的にみて全情報システムへの総投資金額も景気の動向に影響を受けているようである。

Q7G2. 全情報システムへの総投資金額の傾向(業種別)



業種別にみると、「上昇傾向」では金融・保険業(41.8%)が高く、次いで食品・紙・パルプ・繊維・印刷(37.3%)、情報処理サービス(36.0%)となっている。また、「下降傾向」ではその他製造業(28.2%)が高く、次いで電気・一般・輸送・精密機械(24.0%)、石油・化学・鉄鋼・非鉄・金属(23.3%)、商業(23.2%)となっている。

Q8. 情報システムの資産価値を評価したことがありますか。

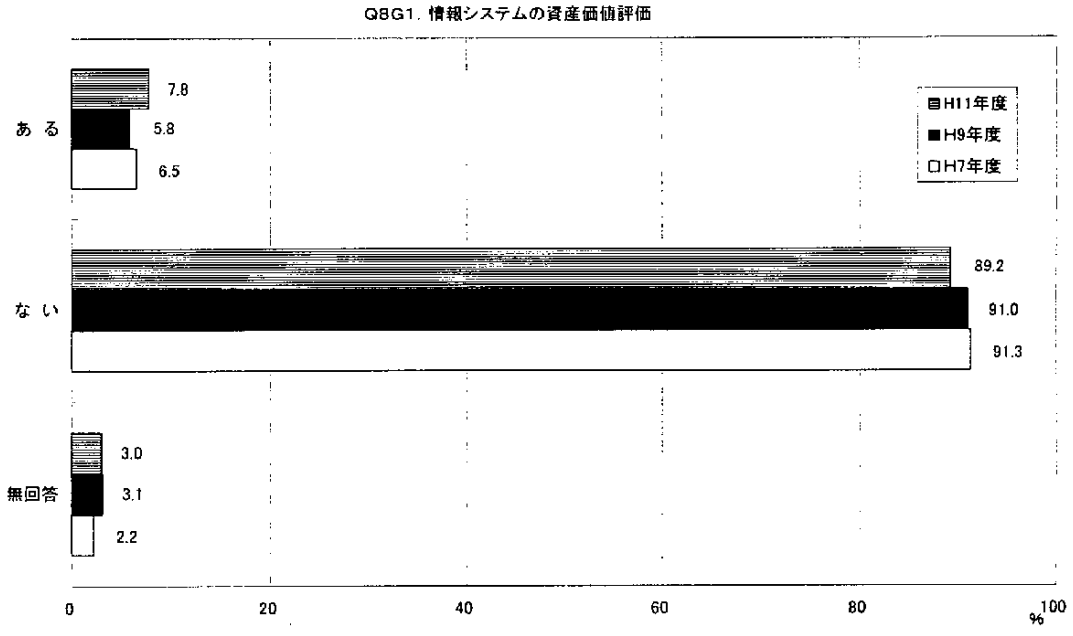
1	ある	68	7.8
2	ない	773	89.2
無回答		26	3.0
計		867	100.0

情報システムの資産評価の実施については前回調査結果(「ある」5.8%、「ない」91.0%)をいずれも上回っており、傾向的には当該項目にはあまり熱心ではないようである。

業種別にみると、非製造業の評価はやや高く、なかでも情報処理サービスは前回調査よりかなり高くなっている。同じことは商業(今回調査では12.1%が「ある」と回答)についてもいえるが、経営管理の視点として重要な項目であるが、現実には資産評価活用方法がわからないところに問題がある。

企業規模(資本金、従業員数)別にみても同じ傾向にある。資本金、従業員数のいずれも小さい方が資産価値評価が高いのは当然である。

なお、評価したことが「ある」(7.8%)と回答した組織体がどのような評価方法で資産価値を評価したかは不明である。資産価値を評価する方法としては再製造価格法、市価規準法等いろいろ考えられるが、今後の調査の際には評価方法を把握できる質問の仕方を考慮する必要があろう。



Q9. 情報システムの現在の資産価値は、どの程度と見積っていますか。(Q8の「1」を回答－68件)

平均	1,629.8	百万円

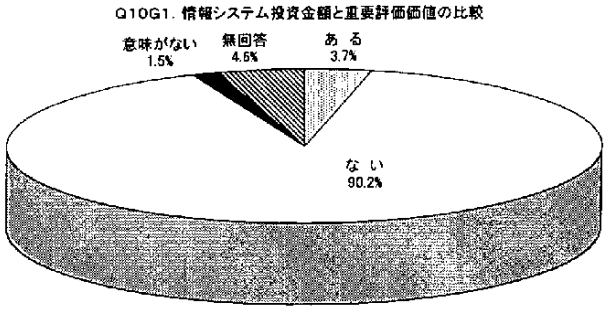
情報システムの資産価値は平均1，629．8百万円である。

資本金別にみると、資本金50億円～100億円未満が5，425．0百万円、500億円以上が4，717．5百万円となっている。

有効回答数は68件と少ないが、情報システムの資産価値を評価することは情報セキュリティ上からも大切なことである。

Q10. 情報システム投資金額と重要情報価値を比較したことがありますか。

1	ある	32	3.7
2	ない	782	90.2
3	意味がない	13	1.5
無回答		40	4.6
計		867	100.0



今回初めての質問であるが、無回答の割合が少なく、また「比較しても意味がない」もきわめて少ない。すなわち、評価の意味について否定的なものはないがまだ実施していない組織体がほとんどである。これは情報資産評価のための簡易、効果的な手法が見当たらないことに主な原因があると思われる。

ところで、情報システム投資金額は何らかの方法で経済価値換算が可能であるが、重要情報価値については必ずしも経済価値換算が可能とは限らず、定性的価値評価とならざるを得ない場合もある(たとえば信頼性・満足度等)。情報システム投資金額、重要情報価値双方とも経済価値換算可能であればそれぞれの比較は容易であろうが、片方が経済価値換算不能であり定性的評価にならざるを得ない場合があっても、投資資源に対する成果(入手する価値)に関してはバランス感覚で評価する必要があろう。

Q11. 貴社の基幹システムはどのように運用されていますか。

1	集中型	414	47.8
2	集中分散型	331	38.2
3	分散型	106	12.2
無回答		16	1.8
計		867	100.0

(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を指し、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、47.8%と半数近くの組織体が依然としてメインフレーム等を中心とした集中型の形態をとっている。これに一部の機能を分散システムにおいている形態を加えると86.0%となり、ほとんどの組織体がメインフレーム等を中心においている。これは、基幹システムは規模が大きく、システムの再構築にも大きな投資が必要なので、昨今の経済状況から再構築が進んでいないことや、Y2K対応でシステム再構築の要員が不足していたためと考えられる。

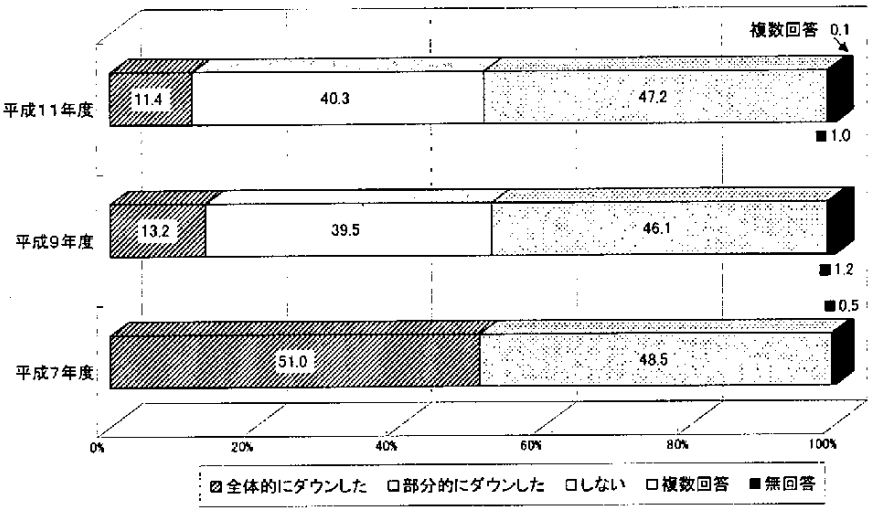
2．3　過去の障害等の実績について

Q12．貴社の基幹システムは過去1年間（平成10年1月～12月）に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	99	11.4
2	部分的にダウンした	349	40.3
3	しない	409	47.2
複数回答		1	0.1
無回答		9	1.0
計		867	100.0

システムダウンの発生率は平成7年度51．0%、9年度52．7%、11年度51．7%とあまり変化はみられない。しかし、「全体的にダウンした」は9年度13．2%、11年度11．4%と1．8ポイント減少している。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を意味している。

Q12G1．基幹システムのシステムダウンの状況

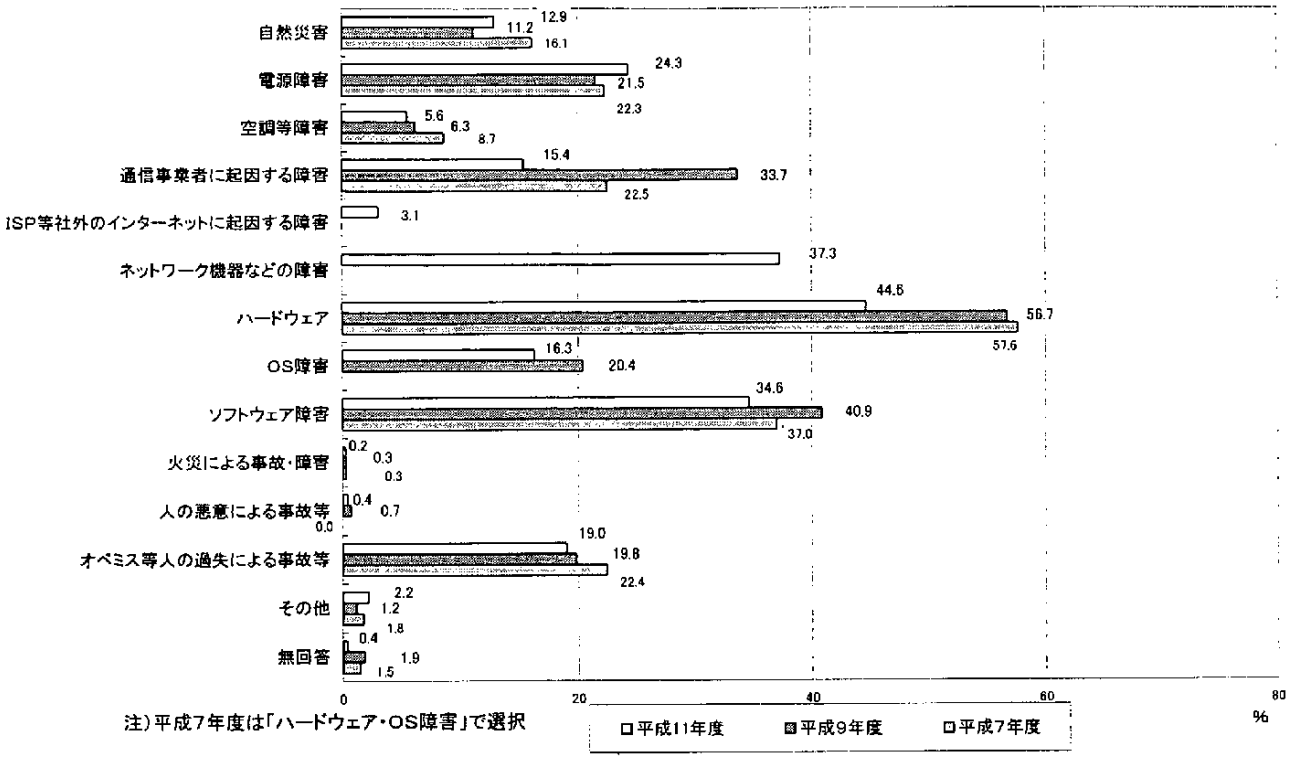


Q13．過去1年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。（複数回答）
（Q12の「1」、「2」を回答）

回答件数		448	
1	自然災害	58	12.9
2	電源障害	109	24.3
3	空調等障害	25	5.6
4	通信事業者に起因する障害	69	15.4
5	ISP(ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ)等社外のインターネットに起因する障害	14	3.1
6	ネットワーク機器などの障害	167	37.3
7	ハードウェア	200	44.6
8	OS障害	73	16.3
9	ソフトウェア障害	155	34.6
10	火災による事故・障害	1	0.2
11	人の悪意による事故等	2	0.4
12	オペミス等人の過失による事故等	85	19.0
13	その他	10	2.2
無回答		2	0.4

（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

13G1. システムダウンの原因



注)平成7年度は「ハードウェア・OS障害」で選択

平成9年度調査と比較して「ハードウェア」の障害が減少しているが、これは11年度から「ネットワーク機器」を別に設けたため少なくなったようにみえているだけで、両者を合計すると81．9%となっており、ネットワーク機器を含むハードウェアの障害が増加しているといえよう。これは、情報化投資額が増え、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。

9年度以降急増したと考えられるインターネット接続については、今回新たに追加した項目であるが、障害件数は多くない。すなわち、障害という面からみてインターネットは十分にビジネスに利用できるものといえよう。また、「インターネットに起因する障害」と「通信事業者に起因する障害」をあわせた割合は、9年度の「回線障害」より減少しており、通信環境が改善しているといえよう。

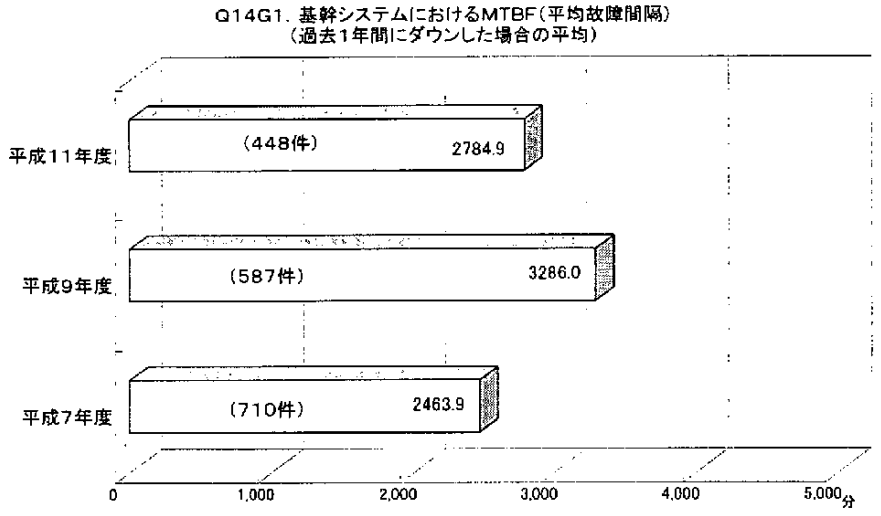
7年度、9年度調査との比較で、「自然」、「電源」、「空調」、「オペレーションミス」などによる障害発生にはあまり大きな変化がみられない。この結果からは、オフィス内でのコンピュータ利用環境には大きな変化があまりないものと考えられる。

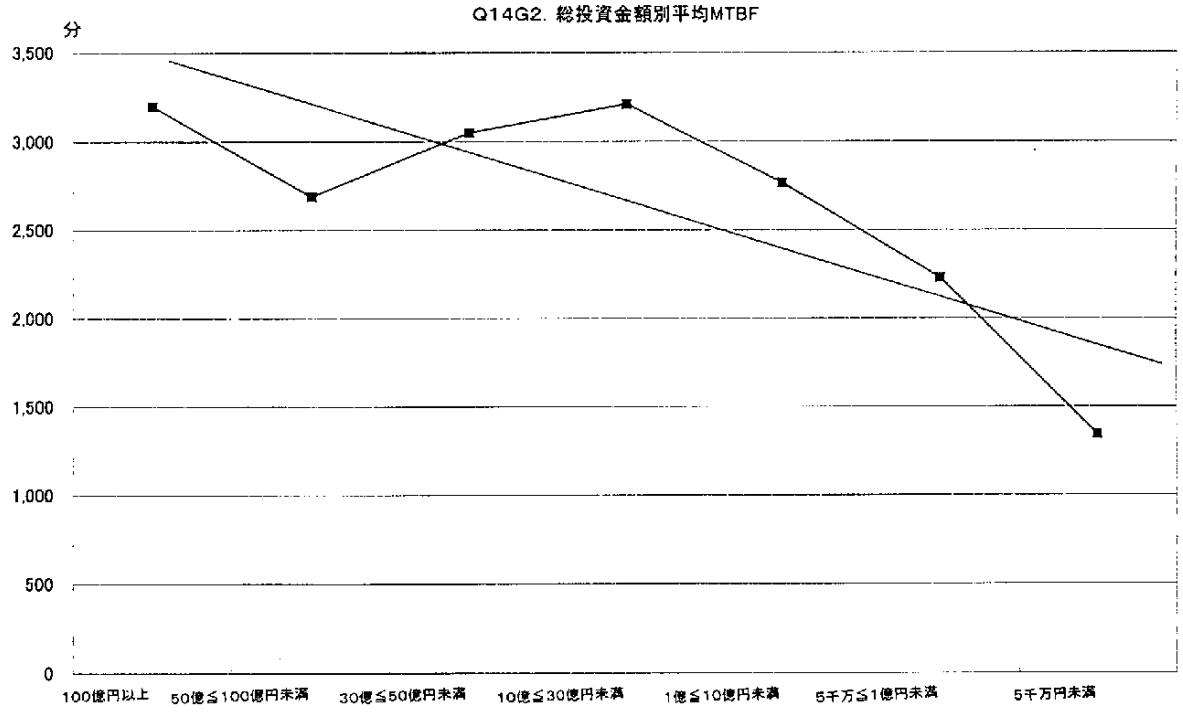
Q14. 基幹システムにおけるMTBF(平均故障間隔)は何時間ですか。(Q12 の「1」、「2」を回答－448件)

平均	2,784.9	時間

(注)MTBFは、特定期間をとり、次の計算式で算出されている
(システム稼働時間)／(ダウン回数＋1)

平成7年度、9年度、11年度調査とMTBFが徐々に短く(悪く)なる傾向がみられ、より頻繁に故障が起きていることがわかる。これはQ13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。

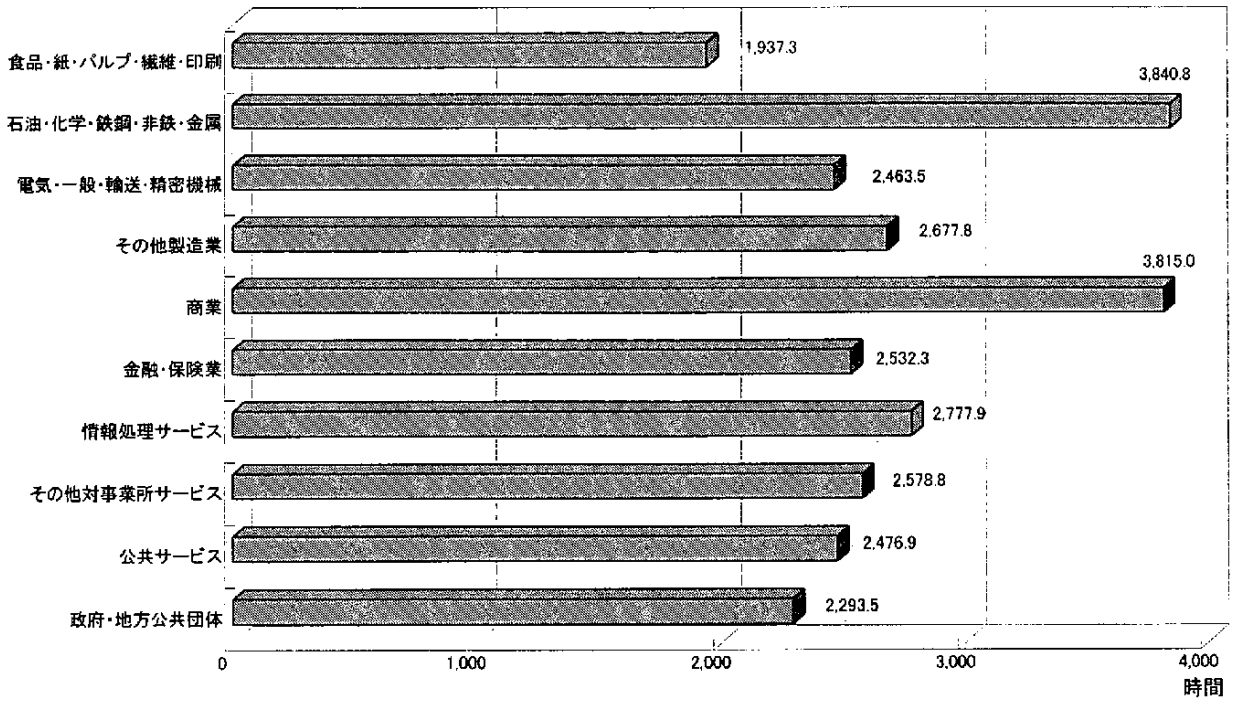




なお、11年度調査では、MTBFと組織体の資本金との相関はあまりみられないが、情報化投資額との相関は大きい。情報化投資額が大きいほどMTBFが小さい傾向にある。これは、情報化投資額の多い組織体では信頼性対策が十分になされていると考えられる。

業種別にみると、商業、石油・化学・鉄鋼・非鉄・金属でのMTBF(大きい方がよい)がよい。一方、食品・紙・パルプ・繊維・印刷のMTBFが極端に悪い点を除くと、他の業種ではあまり差がない。9年度調査時にMTBFがよかった金融・保険業、情報処理サービスは、11年度調査では他業種と比べて差がなくなっている。これは、情報通信ネットワークの急激な変化のなかでネットワーク機器を導入しながら信頼性を維持・向上するのが難しくなってきているためと考えられる。

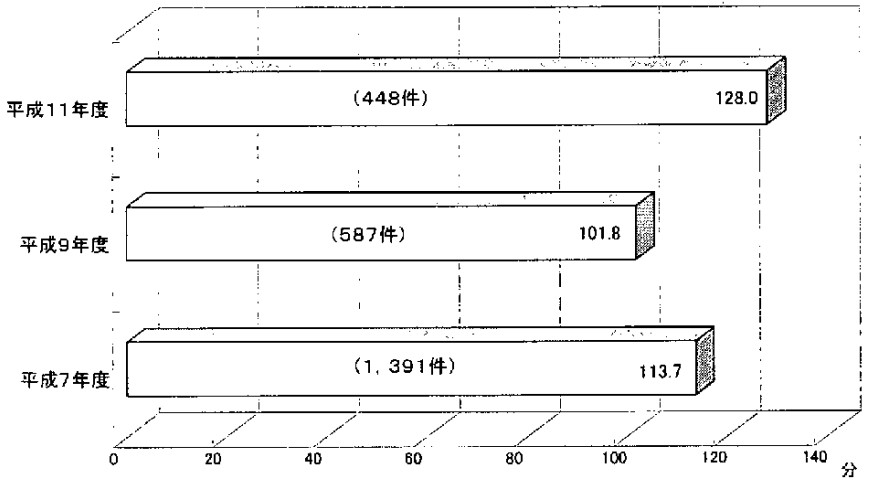
Q14G3. 業種別MTBF



Q15. 基幹システムにおけるMTTR(平均修理時間)は何分ですか。(Q12の「1」、「2」を回答－448件)

平均	128.0	分

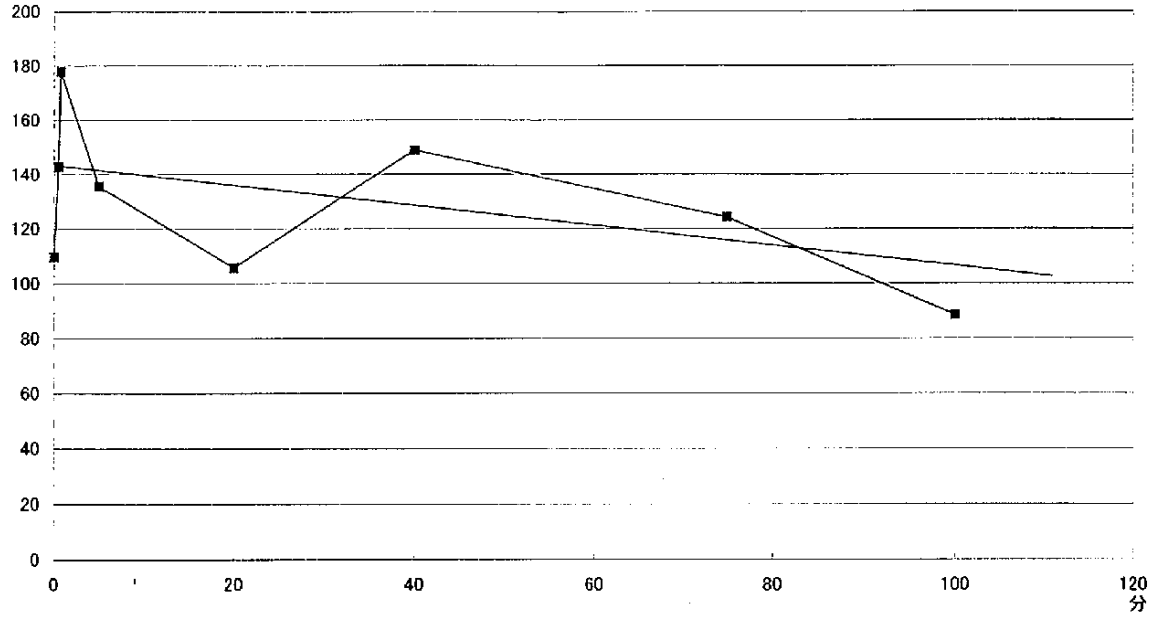
Q15G1. 基幹システムにおけるMTTR(平均修理時間)



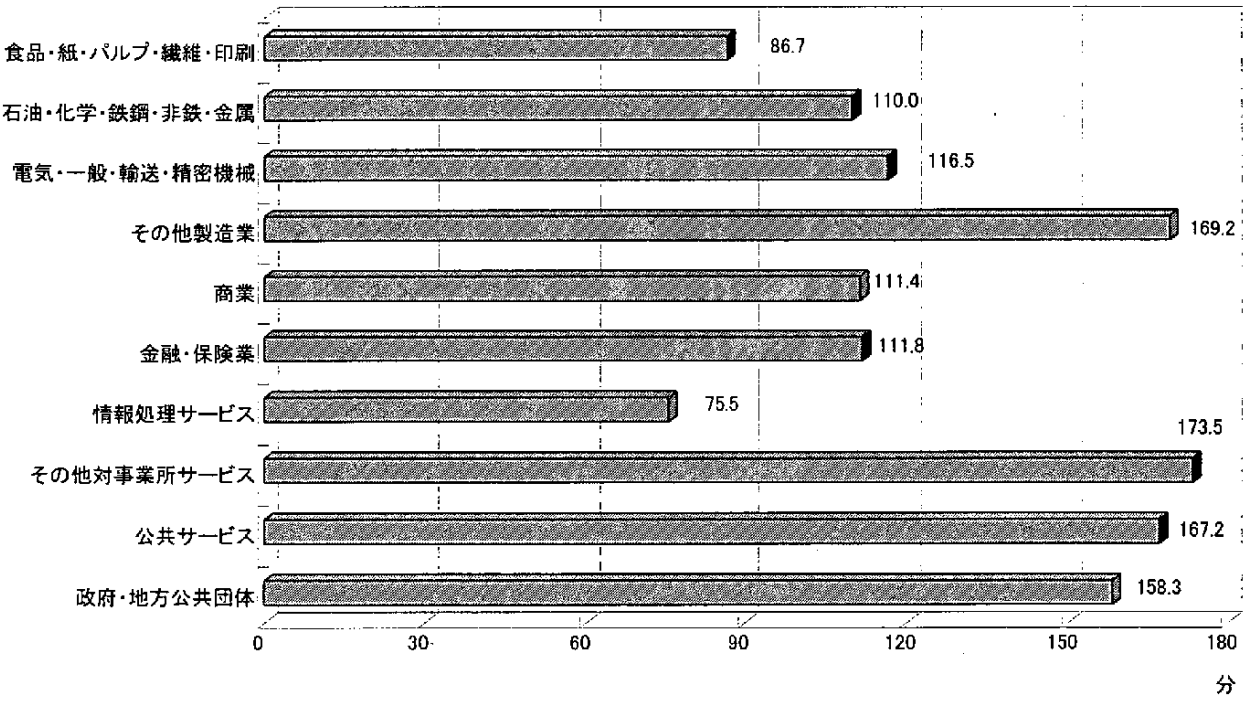
平成9年度調査では7年度に比べて短くなったMTTR(短いものがよい)が、11年度では長くなっている。これは、パソコンやサーバなどがより多く用いられるためハードウェア故障の種類が増えていることや、組織体内のLANやインターネットとの接続に用いるネットワーク機器の故障の修理に手間取っているためと考えられる。

なお、11年度調査では、MTBFは情報化投資額との相関は大きかった。同様にMTTRも情報化投資額の大小と相関がみられる。しかし、MTBFほど大きくはない。このことからも情報化投資額の多い組織体では信頼性対策が考慮されているとみられる。

Q15G2情報投資資金とMTTRの関係



Q15G3. 業種別MTTR



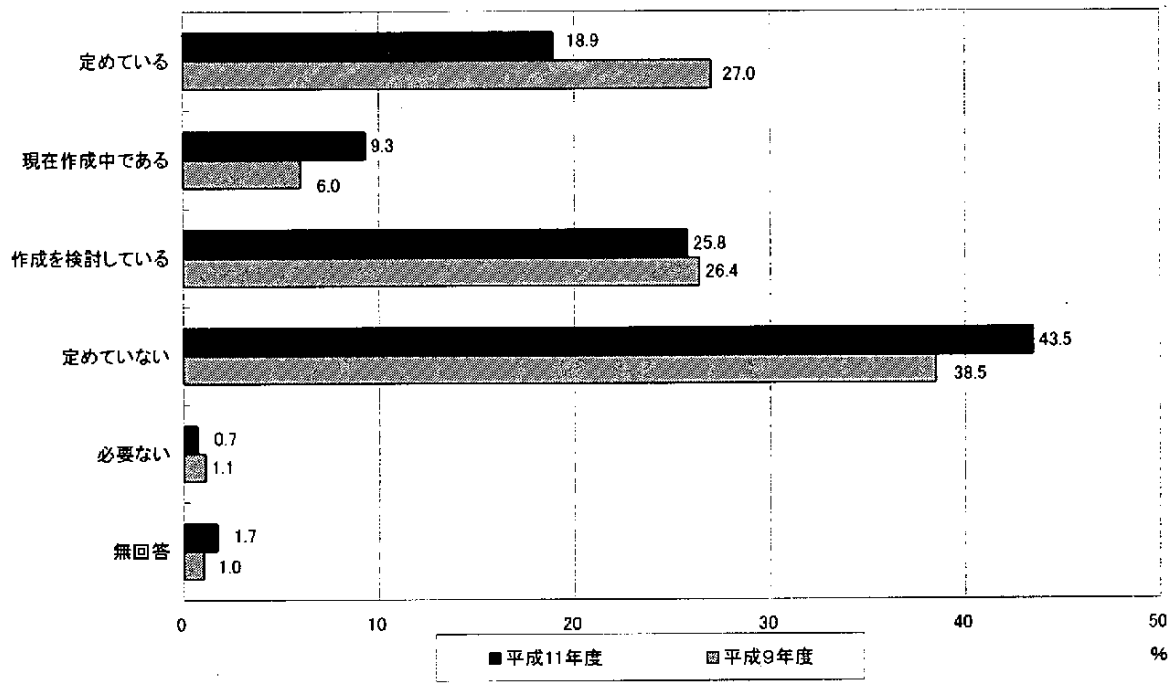
業種別にみると、その他製造業、その他事業所サービス、公共サービスのMTTRが悪く、長期故障が増えていることがうかがえる。一方、情報処理サービスは9年度と同様に短い。これは、新規の情報機器の導入に伴って情報処理サービス関連企業以外では十分に維持管理できていないためと考えられる。今後、情報機器の保守・運用を行う情報処理サービス業などの専門業者にアウトソーシングするなどの対応が考えられる。9年度調査時にMTTRが短かった金融・保険業は他業種との差がなくなった。

2．4　セキュリティ管理一般について

Q16．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。

1	定めている	164	18.9
2	現在作成中である	81	9.3
3	作成を検討している	224	25.8
4	定めていない	377	43.5
5	必要ない	6	0.7
無回答		15	1.7
計		867	100.0

Q16G1．セキュリティポリシーの策定状況



セキュリティポリシーは組織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18．9%と、前回調査（27．0%）から8．1ポイント減少している。「定めていない」が43．5%であり、前回（38．5%）より5ポイントも増加している。調査時点の組織体の回答者に差異があるとしても、現在のIT時代におけるセキュリティに対する認識として疑問と思われる。

ところで、今回は前回調査と異なり、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意図があり、質問の表現を変えたことに関係があるかもしれない。しかし、「現在作成中」が9．3%と前回（6．0%）より3．3ポイント増加している。現在「作成を検討している」のは25．8%で、0．6ポイント減少している。「必要ない」は0．7%と前回（0．3%）より0．4ポイント増加している。

なお、すでに定めている割合を業種別にみると、非製造業では情報処理サービス（37．1%）、金融・保険業（24．2%）、公共サービス（21．0%）、製造業では、電気・一般・輸送・精密機械（21．6%）となっている。ちなみに、前回調査では、情報処理サービスが45．5%、金融・保険業が42．0%と、セキュリティポリシーを定めている割合が高かったのが、今回調査では相対的に低くなっている。この点は、設問についての理解に拠ると思われる。

ただし、資本金別にみると、資本金が多いほど定めている割合が高いとは必ずしもいえない（50億円以上20．3%；100億円以上26．2%；500億円以上17．8%）。

Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。

1	定めている	242	27.9
2	現在作成中である	71	8.2
3	作成を検討している	200	23.1
4	定めていない	340	39.2
5	必要ない	5	0.6
無回答		9	1.0
計		867	100.0

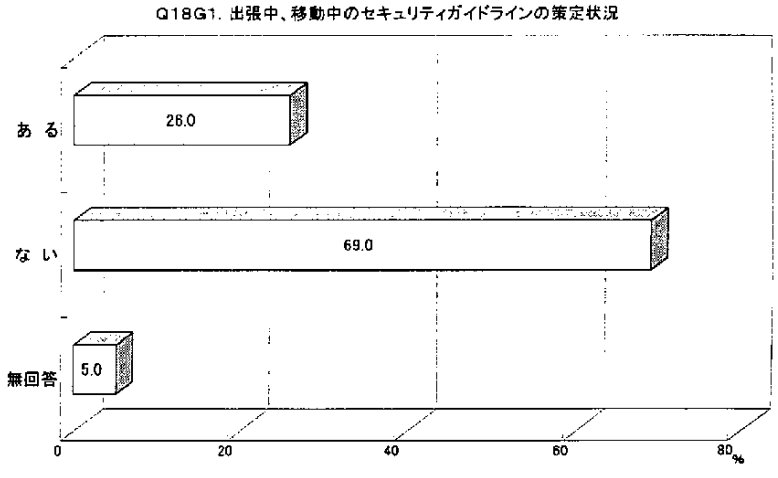
セキュリティガイドラインとして操作および業務処理手順を「定めている」のは27．9%で、前回調査で「セキュリティポリシーを定めている」とした回答の27．0%に非常に近い結果となっている。なお、「定めていない」とする回答も39．2%と約4割にのぼり、上記同様、前回調査の38．5%に近い。なお、「現在作成中である」が8．2%、「作成を検討している」は23．1%で、両者をあわせると31．3%となり、前回のセキュリティポリシーについての回答である32．4%に近似している。

ところで、「必要ない」は0．6%であった。しかしながら『操作および業務処理手順を定めていますか』と質問した前回調査(「定めている」71．1%、「定めていない」12．9%)と比較すると、かなりの差異が生じている。この点も、今回「セキュリティガイドライン」として質問を明確化したことに拠っているものと思われる。

なお、すでに定めている割合を業種別にみると、非製造業では金融・保険業(47．3%)、情報処理サービス(41．6%)、公共サービス(22．6%)が、また製造業では、電気・一般・輸送・精密機械(27．2%)となっている。

Q18. 出張中、移動中の環境についてのセキュリティガイドラインがありますか。(Q17 の「1」を回答)

1	ある	63	26.0
2	ない	167	69.0
無回答		12	5.0
計		242	100.0

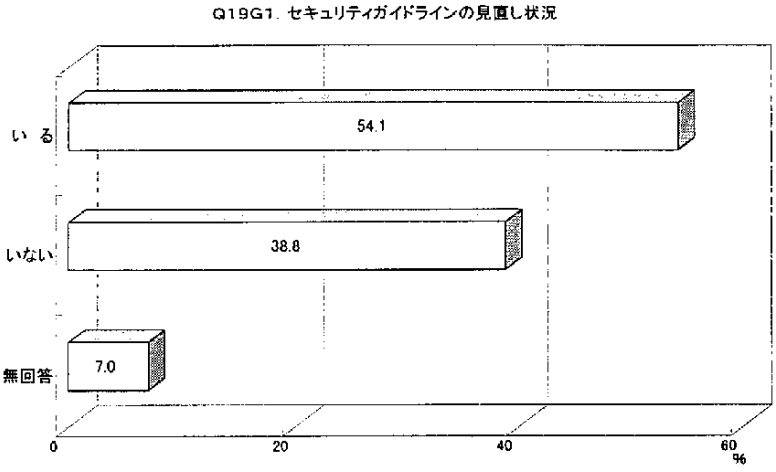


現在のIT環境におけるセキュリティに関しては出張中、移動中を問わず考慮すべきである。そこで今回新たに設けた質問であるが、この点についてセキュリティガイドラインを有しているのは26．0%と、約4社に1社の割合であった。

出張中、移動中のガイドラインを有している業種別にみると、非製造業では、その他対事業所サービス(38．7%)が高く、情報処理サービス(35．1%)、公共サービス(21．4%)、金融・保険業(11．6%)と業種差を明確に表している。また、製造業では、電気・一般・輸送・精密機械(32．4%)が相対的に高いといえる。

Q19. セキュリティガイドラインを定期的に見直していますか。(Q17 の「1」を回答)

1	い る	131	54.1
2	いない	94	38.8
無回答		17	7.0
計		242	100.0

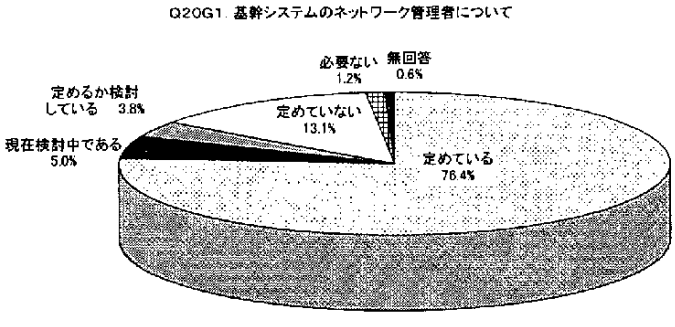


現代の情報リスク環境はまさに変化と隣り合わせであり、セキュリティガイドラインの見直しが不可欠と思われ、今回新たに質問を設けてみた。この点、「定期的に見直しをしている」と回答したのは54. 1%で、回答の半数以上が見直しを行っている。しかし、「見直しをしていない」組織体も38. 8%にあがっている。

定期的に見直しを行っている回答を業種別にみると、非製造業では、情報処理サービス(64. 9%)、その他対事業所サービス(61. 3%)が高く、公共サービス(50. 0%)、金融・保険業(55. 8%)、商業(30. 0%)との業種差を反映している。また、製造業では、食品・紙・パルプ・繊維・印刷(58. 3%)、石油・化学・鉄鋼・非鉄・金属(54. 5%)、電気・一般・輸送・精密機械(52. 9%)が相対的に高い回答となっている。

Q20. 基幹システムのネットワーク管理者を定めていますか。

1	定めている	662	76.4
2	現在検討中である	43	5.0
3	定めるか検討している	33	3.8
4	定めていない	114	13.1
5	必要ない	10	1.2
無回答		5	0.6
計		867	100.0

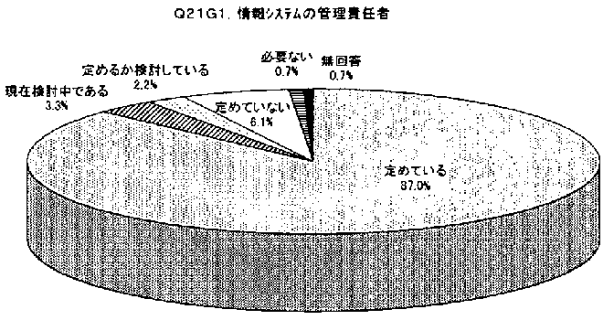


今回、基幹システムのネットワークに特定した形で管理者について新たに質問を設けた。ネットワーク管理者を「定めている」のは76. 4%であり、「現在検討中」(5. 0%)、「定めるか検討している」(3. 8%)をあわせると、85. 2%の組織体がネットワーク管理者を必要としていることが確認できる。これは、基幹システムがネットワーク環境下で用いられることとともに、パソコンもそうした環境において利用されていることが関係している。なお、「定めていない」は13. 1%、「必要ない」は1. 2%となっている。

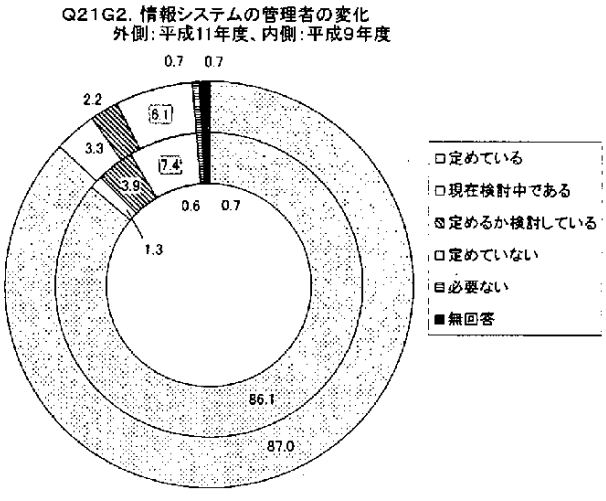
業種別に「定めている」割合をみると、非製造業では、情報処理サービス(91. 0%)、その他対事業所サービス(77. 1%)、公共サービス(74. 2%)、金融・保険業(72. 5%)、商業(66. 7%)が、また、製造業では、電気・一般・輸送・精密機械(84. 8%)、石油・化学・鉄鋼・非鉄・金属(78. 9%)、食品・紙・パルプ・繊維・印刷(76. 5%)と全体的に高い割合となっている。

Q21. 情報システムの管理責任者を定めていますか。

1	定めている	754	87.0
2	現在検討中である	29	3.3
3	定めるか検討している	19	2.2
4	定めていない	53	6.1
5	必要ない	6	0.7
無回答		6	0.7
計		867	100.0



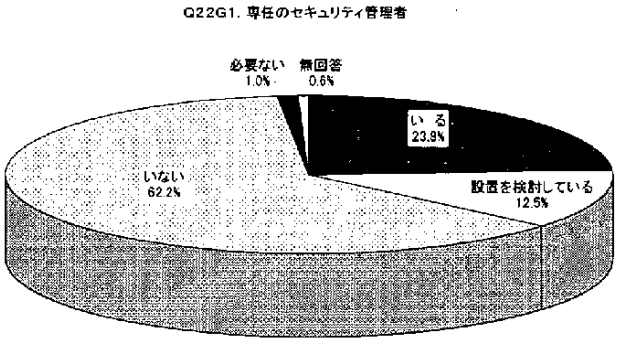
情報システムの管理者については、「定めている」、「検討中である」をあわせた場合、前回調査よりも若干増加して90%を越える高い数字となった。すなわち、ほとんどの組織体において情報システム管理者が定められているといえよう。



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7%近くある。この内訳は、その他対事業所サービスや公共サービスに多くみられる。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。

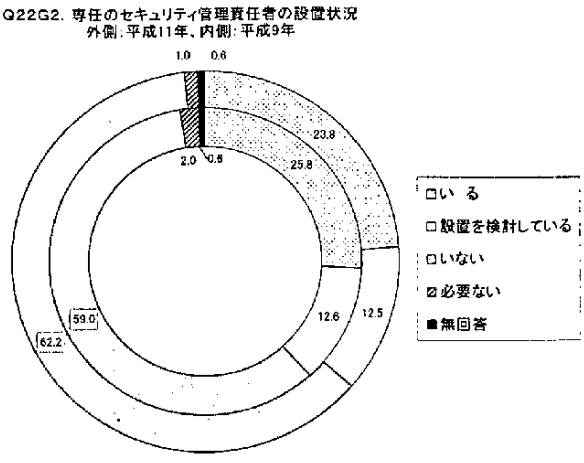
Q22. 貴社には専任のセキュリティ管理者または担当者がいますか。

1	い る	206	23.8
2	設置を検討している	108	12.5
3	いない	539	62.2
4	必要ない	9	1.0
無回答		5	0.6
計		867	100.0

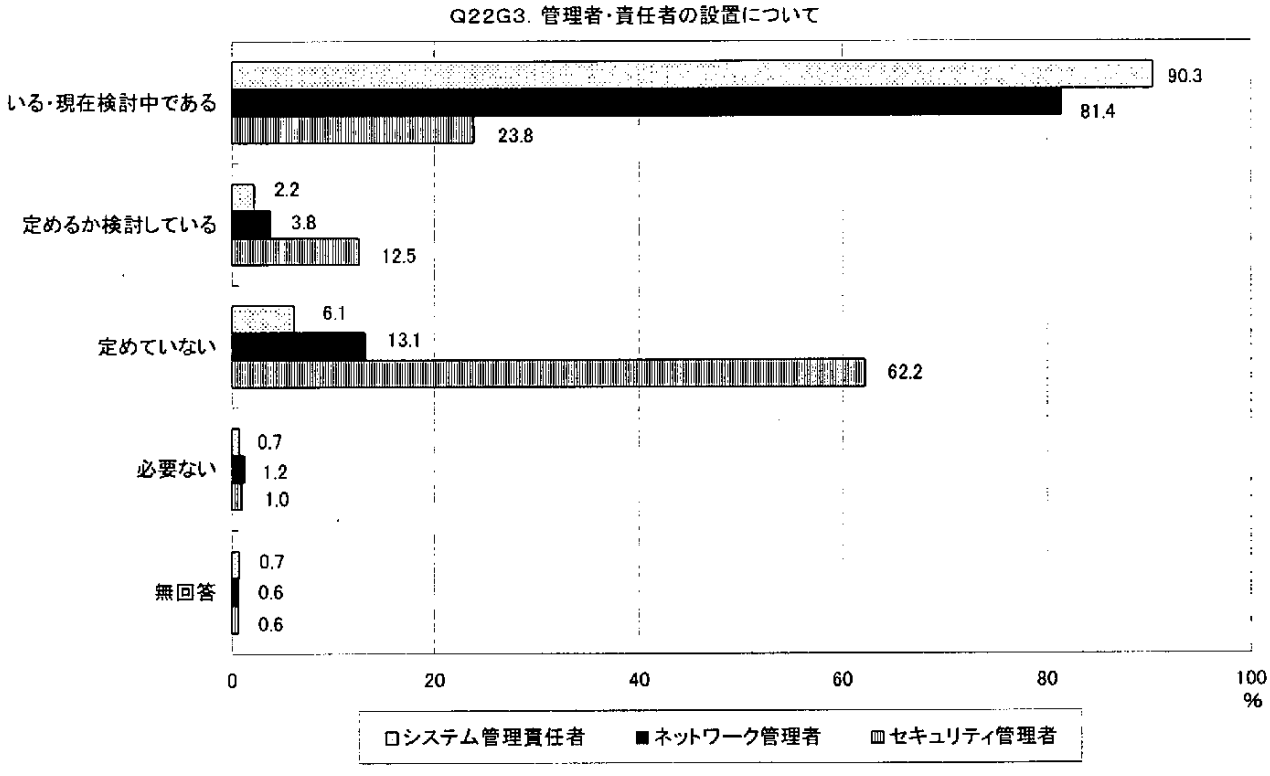


専任のセキュリティ管理者または担当者の有無については、「いる」、「検討している」の肯定的な回答をしたのが36. 3%で、平成9年度調査の38. 4%に比べて減少している。一方、「いない」、「必要ない」という否定的な回答は61. 0%から63. 2%と増加している。セキュリティポリシーの認識度の減少と同様に、セキュリティに対する認識度が減少したといえよう。これは、今まで以上にネットワークやコンピュータを利用する組織体が増えたものの、セキュリティ管理にまで十分に手が回っていない状況と考えられる。

専任の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、システム管理者、ネットワーク管理者、セキュリティ管理者の順となり、システム管理者とネットワーク管理者は同様な傾向を示している。一方、セキュリティ管理者については「いない」、「必要ない」が多い。また、各管理者の設置状況と組織体の企業規模（資本金、従業員数）、情報化投資額との明確な相関はみられない。



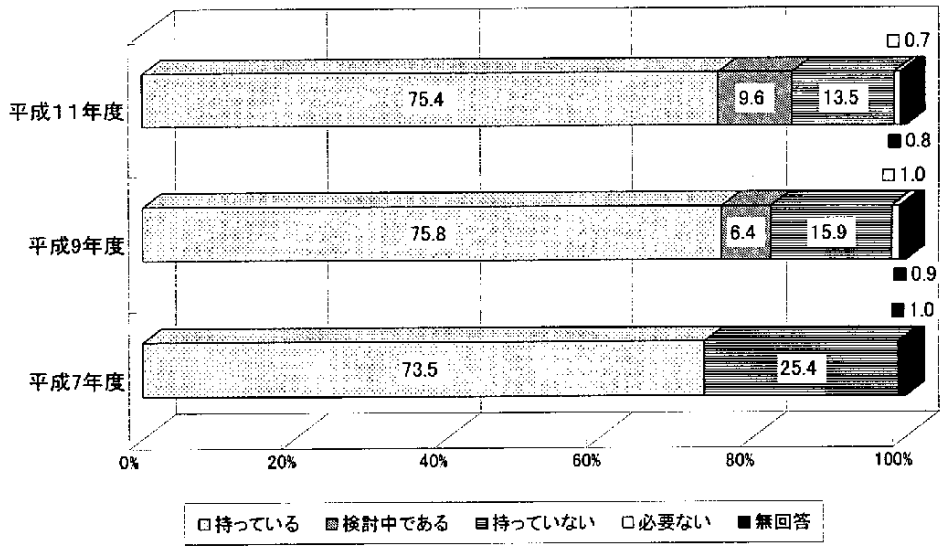
業種別にみると、情報処理サービスでセキュリティ管理者設置の割合が、全体の36．3%に比べ64．1%と飛び抜けて高い。しかし、他の業種では全体的に低く、まだまだ組織体におけるセキュリティへの認識度が低いことがわかる。



Q23. 緊急時の連絡手段を持っていますか。

1	持っている	654	75.4
2	検討中である	83	9.6
3	持っていない	117	13.5
4	必要ない	6	0.7
無回答		7	0.8
計		867	100.0

Q23G1. 緊急時の連絡手段



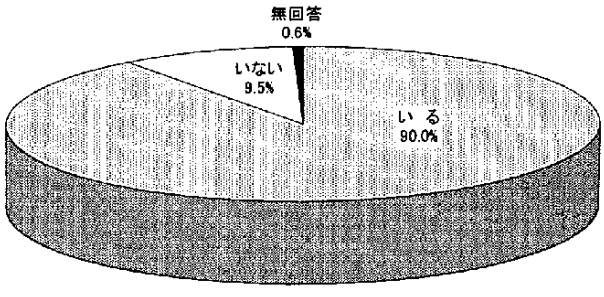
全体傾向は前回調査とほとんど変わらず、「検討中」がやや増え、「持っていない」、「必要ない」がやや減少してはいるが、全体として何らかの方法での緊急連絡システムがすでにあると考えられる。重要性の認識度もさらに高まっているといえるので、今後の問題は緊急連絡手段のレベル、質がパニック下で有効かどうかの継続的改善がなされる必要がある。

業種別にみると、前回調査に比べ、特に公共サービス(67.7%)、商業(77.8%)，金融・保険業(87・9%)の割合が高くなっており、逆に製造業の割合は減っている。この傾向は単純には評価できないが、社会的にも当該業種での認識の高まりが読み取れる。

Q24. データの使用・保管等の管理を行っていますか。

1	い る	780	90.0
2	いない	82	9.5
無回答		5	0.6
計		867	100.0

Q24G1. データの使用・保管等の管理状況



データの使用・保管等の管理に関しては、管理を「行っている」という回答(90.0%)は、前回(88.4%)に比べ1.6ポイント上昇している。

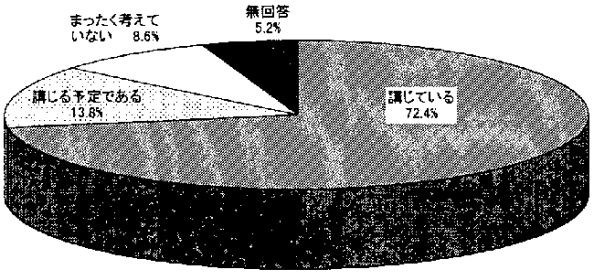
管理を行っている割合を業種別にみると、非製造業では、商業(96.0%)、その他対事業所サービス(91.7%)、公共サービス(85.5%)、金融・保険業(91.2%)、情報処理サービス(89.9%)が、また製造業では、電気・一般・輸送・精密機械(92.0%)、食品・紙・パルプ・繊維・印刷(90.2%)、石油・化学・鉄鋼・非鉄・金属(87.8%)と、全体的に高く、かつ順位に差異がみられる。

ただ、資本金別にみると、資本金が多いほど行っている割合は高くなっている(50億円以上92.4%;100億円以上94.4%;500億円以上97.8%)が、前回調査の「100億円以上の企業はほぼ100%の実施率であった」とは若干の違いが感じられる。

Q25. 基幹システムを国際的に展開・利用していますか。

1	実施している	58	6.7
2	実施していない	805	92.8
無回答		4	0.5
計		867	100.0

Q25G1. 国際展開している基幹システムのセキュリティ対策の策定状況



情報化・国際化の波が喧しかった時代から実質的にネットワーク化が進んでいると思われる今日、基幹システムを国際的に展開・利用している実態について新たな質問を設けてみた。この点、Q11の(注)において基幹システムについて一応の限定がされており、主要業務に関連づけた情報システムの総称となっていた。したがって、システムが国内向けに構築されていれば、当然国際的な展開について「実施していない」といった回答になる。また、国際的な展開にはそのためのシステムを有している組織体も考えられ、回答に誤差が生じるおそれがある。そうしたことが関係しているかもしれないが、国際的な展開に基幹システムを「利用している」のは6．7%とかなり低く、「実施していない」割合は92．8%であった。

実施している割合を業種別にみると、非製造業では、公共サービス(11．3%)、情報処理サービス(11．2%)、その他対事業所サービス(5．6%)、商業(2．0%)が、また製造業では、電気・一般・輸送・精密機械(18．4%)、石油・化学・鉄鋼・非鉄・金属(4．4%)と、メーカの国際的な展開が相対的に高い。この点、資本金別にみると、資本金100億円以上で13．5%、500億円以上で22．2%と規模の大きさが関係しているといえる。

ところで、日本における各組織体既存の基幹システムをそのまま国際的に展開するケースは稀であり、各組織体は国際的に適用できる情報システムを必要に応じてそれぞれ構築し、展開しているケースが多いことも考えられる。今回調査では基幹システムを「貴組織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」と定義づけている。したがって、国際的な展開をするうえで、その都度必要に応じて構築するシステムも「組織体の基幹システム」と捉えることもできる。

Q26. 上記の基幹システムについて、情報システムのセキュリティ対策を講じていますか。(Q25 の「1」を回答)

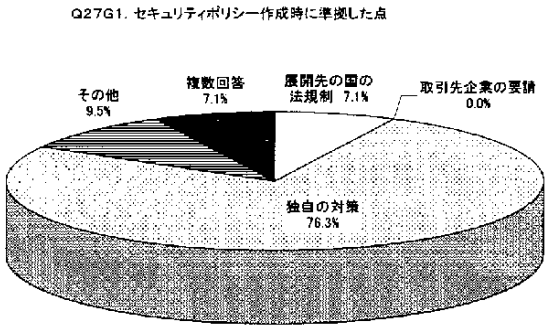
1	講じている	42	72.4
2	講じる予定である	8	13.8
3	まったく考えていない	5	8.6
無回答		3	5.2
計		58	100.0

上記の基幹システムを国際展開に利用している58件についてみると、情報システムのセキュリティ対策を「講じている」のは、72．4%の組織体であった。「講じる予定」は13．8%であったが、国際的な展開の場でありながら「まったく講じていない」のが8．6%という結果となった。「まったく講じていない」のは情報環境下のリスクを考えていないからなのか、どのようにリスク認識しているのか問題である。

講じている割合を業種別にみると、非製造業では、商業1/2(50.0%)、その他対事業所サービス8/8(100.0%)、公共サービス5/7(71.4%)、情報処理サービス8/10(80.0%)、また、製造業では、電気・一般・輸送・精密機械15/23(65.2%)、石油・化学・鉄鋼・非鉄・金属2/4(50.0%)であった。資本金別にみると、資本金100億円以上で76.5%、500億円以上で70.0%といった状況である。

Q27. 講じている場合、セキュリティ対策は何に準拠して策定しましたか。(Q26の「1」を回答)

1	展開先の国の法規制	3	7.1
2	取引先企業の要請	0	0.0
3	独自の対策	32	76.2
4	その他	4	9.5
複数回答		3	7.1
無回答		0	0.0
計		42	100.0



Q26でセキュリティ対策を「講じている」とした42件の場合、セキュリティ対策は何に準拠して策定したのかが問題となる。この点「展開国先の法規制」によるのが7.1%であった。「独自の対策」によるのが76.2%(32社)という状況である。なお、「取引先企業の要請」といった自主性のない回答は「ゼロ」であった。

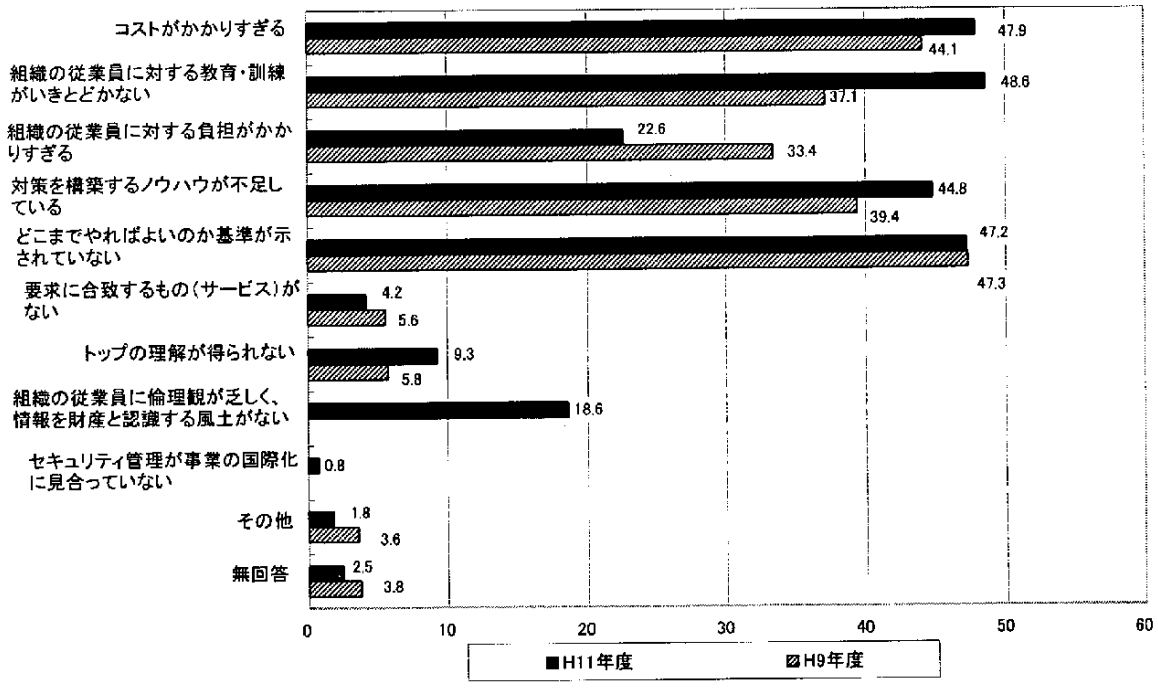
独自の対策の割合を業種別にみると、「、非製造業では、その他対事業所サービス(75.0%)、公共サービス(80.0%)、情報処理サービス(75.0%)、また、製造業では、電気・一般・輸送・精密機械(93.3%)であった。この点、資本金別にみると、資本金50億円以上で75.0%、100億円以上で61.5%、500億円以上で100.0%と、必ずしも規模の大きさが関係しているとはいえない結果となっている。

Q28. 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		867	
1	コストがかかりすぎる	415	47.9
2	組織の従業員に対する教育・訓練がいきとどかない	421	48.6
3	組織の従業員に対する負担がかかりすぎる	196	22.6
4	対策を構築するノウハウが不足している	388	44.8
5	どこまでやればよいのか基準が示されていない	409	47.2
6	要求に合致するもの(サービス)がない	36	4.2
7	トップの理解が得られない	81	9.3
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	161	18.6
9	セキュリティ管理が事業の国際化に見合っていない	7	0.8
10	その他	16	1.8
無回答		22	2.5

Q26の質問に対して情報システムのセキュリティ対策を講じていない理由を明らかにするため、情報セキュリティ管理についての問題点について質問したところ、上記のような結果が得られた。「組織の従業員に対する教育・訓練がいきとどかない」48．6%、「コストがかかりすぎる」47．9%、「どこまでやればよいのか基準が示されていない」47．2%、「対策を構築するノウハウが不足している」44．8%という回答がそれぞれ40%以上という高い割合を示している。これらの項目に関しては、「基準の提示」以外、今回の回答はいずれも前回の結果を上回っている。どこまでやればよいのかといった基準の提示の困難さは相変わらずのことなのかもしれない。

Q28G1．情報セキュリティの問題点



なお、「コストがかかりすぎるため講じない」（47．9%）とする側面については、Q35のバックアップ対策（65．6%）、Q37の代替運転機能（71．8%）、Q45のシステム災害・障害対策（80．6%）への回答に比べると、かなり低い割合となっている。しかし、Q60の不正アクセス対策（40．3%）と比較すると高い割合を示している。

「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、平均値48．6%を超えているのは、製造業で、石油・化学・鉄鋼・非鉄・金属（54．4%）、その他製造業（52．1%）、非製造業では公共サービス（56．5%）、その他対事業所サービス（51．4%）であった。

「コストがかかりすぎる」について平均値47．9%を超えているのは、製造業で石油・化学・鉄鋼・非鉄・金属（56．7%）、電気・一般・輸送・精密機械（55．2%）、その他製造業（56．3%）で、非製造業では、商業の52．5%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」について平均値47．2%を超えているのは、製造業では、その他製造業（53．5%）、電気・一般・輸送・精密機械（52．8%）、食品・紙・パルプ・繊維・印刷（51．0%）、石油・化学・鉄鋼・非鉄・金属（48．9%）で、非製造業では、商業（54．5%）であった。この点、最も割合の高かったのは政府・地方公共団体（55．6%）であった。

「対策を構築するノウハウが不足している」について平均値44．8%を超えているのは、製造業では食品・紙・パルプ・繊維・印刷（58．8%）、電気・一般・輸送・精密機械（46．4%）で、非製造業では、金融・保険業（50．5%）、商業（45．5%）、その他対事業所サービス（45．1%）であった。

なお、新たに設けた「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」という項目については18．6%であったが、業種別にみると次のような結果が得られた。製造業では石

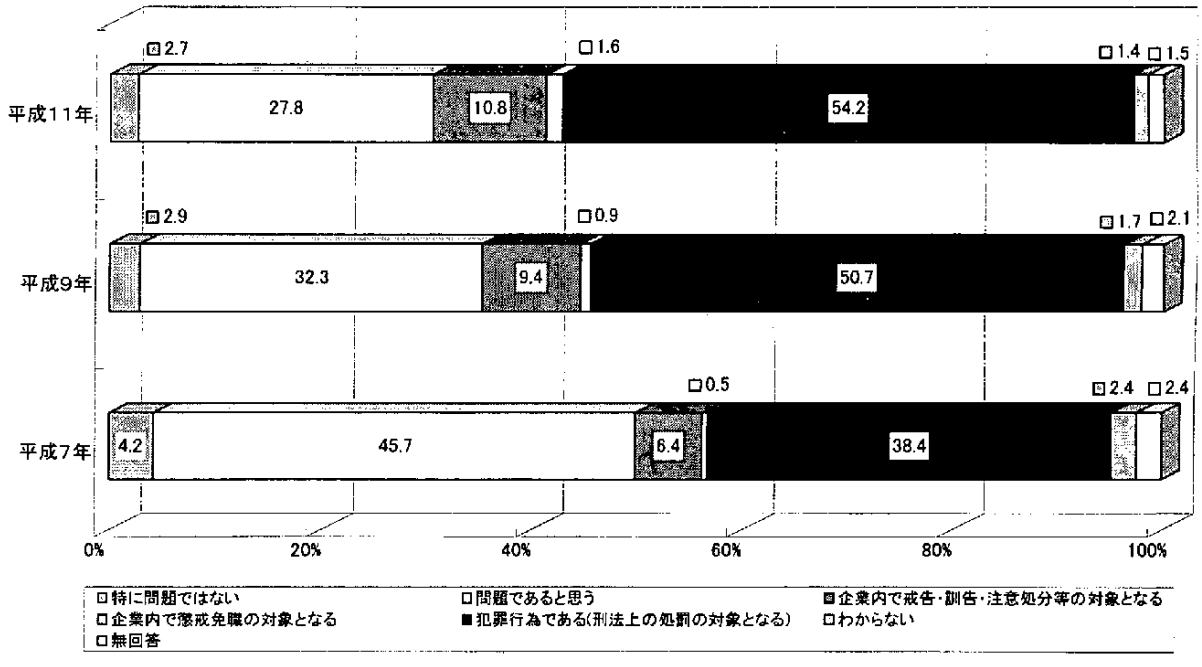
油・化学・鉄鋼・非鉄・金属（24．4%）、その他製造業（22．5%）で、非製造業では、商業（28．3%）、その他対事業所サービス（26．4%）であった。

ところで、前回「トップの理解が得られない」は5．8%であったが、今回は9．3%とかなり高くなっている。他の項目と比べて相対的に低いとはいえ、情報システムのセキュリティについてトップにまだこうした認識がみられることが把握できたといえる。ちなみに、業種別にみると、平均値9．3%を超えているのは、製造業ではその他製造業（12．7%）、電気・一般・輸送・精密機械（12．0%）、非製造業では商業（14．1%）、政府・地方公共団体（13．3%）、その他対事業所サービス（12．5%）であった。

Q29．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	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	23	2.7	11	1.3	35	4.0
問題であると思う	241	27.8	233	26.9	335	38.6
企業内で戒告・訓告・注意処分等の対象となる	94	10.8	261	30.1	245	28.3
企業内で懲戒免職の対象となる	14	1.6	67	7.7	46	5.3
犯罪行為である(刑法上の処罰の対象となる)	470	54.2	255	29.4	163	18.8
わからない	12	1.4	20	2.3	22	2.5
無回答	13	1.5	20	2.3	21	2.4
計	867	100.0	867	100.0	867	100.0

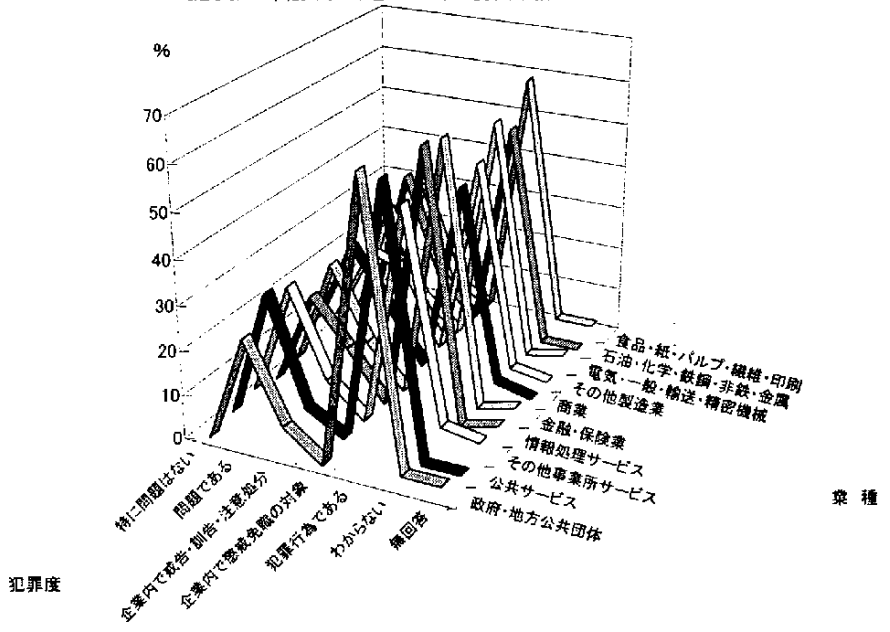
Q29G1．市販のソフトをコピーして使用



市販のソフトのコピーに対してはQ29G1にみるように急速に「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%、11年度には54．2%と増加してきており、ソフトのコピーが犯罪であるとの認識が普及してきているといえよう。9年度調査では、小規模の企業ほど問題視していないという分析がなされていたが、11年度調査では、この相関は小さくなっており、意識改革が進んでいるといえよう。

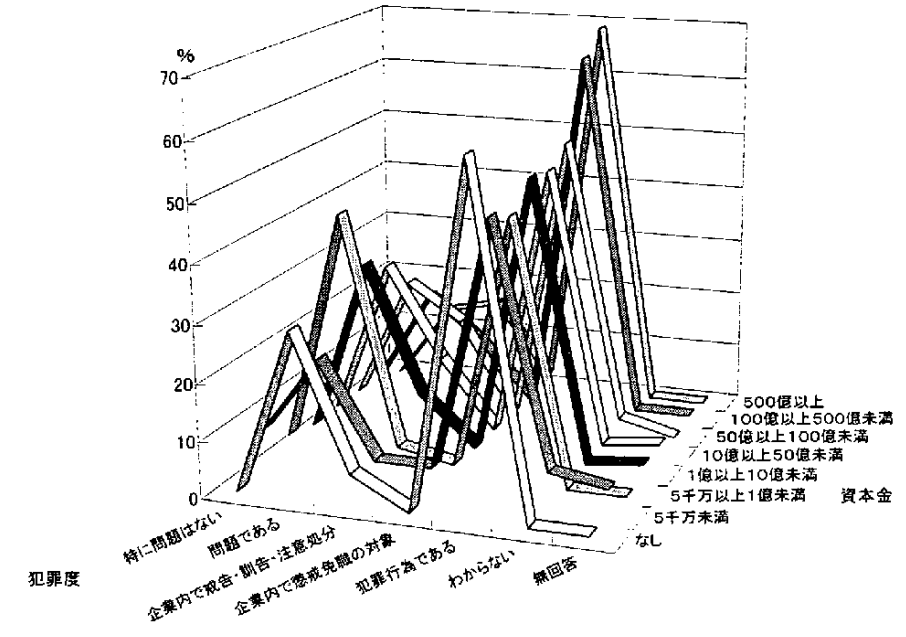
業種別にみるとあまり明確な差異はみられないが、政府・地方公共団体、情報処理サービス、公共サービス、金融・保険業の意識改革が進んでいる。今後、この傾向が全産業に広がっていくものと考えられる。

Q29G2. 市販のソフトをコピーして使う(業種との関連)

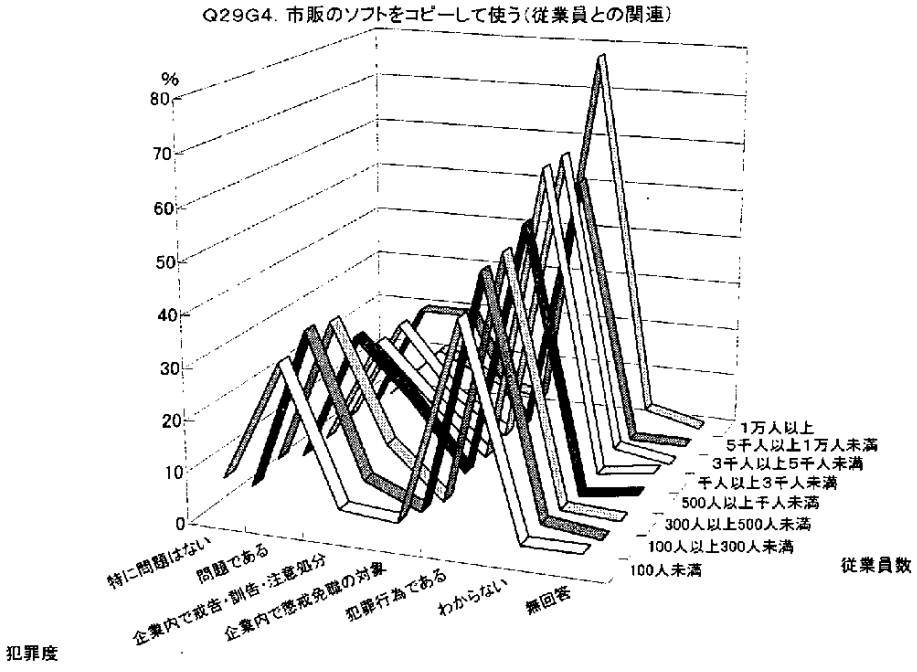


一方、企業規模(資本金、従業員数)との比較では大企業ほど刑法上の犯罪という認識が高く、資本金が小さくなるにつれて、犯罪という認識が小さくなり、一方では「問題である」が増えていく。今後、中小企業に対しての市販ソフトウェアのコピー問題をアピールしていくことが必要と考えられる。

Q29G3. 市販ソフトをコピーして使う(資本との関連)



Q29G4. 市販のソフトをコピーして使う(従業員との関連)

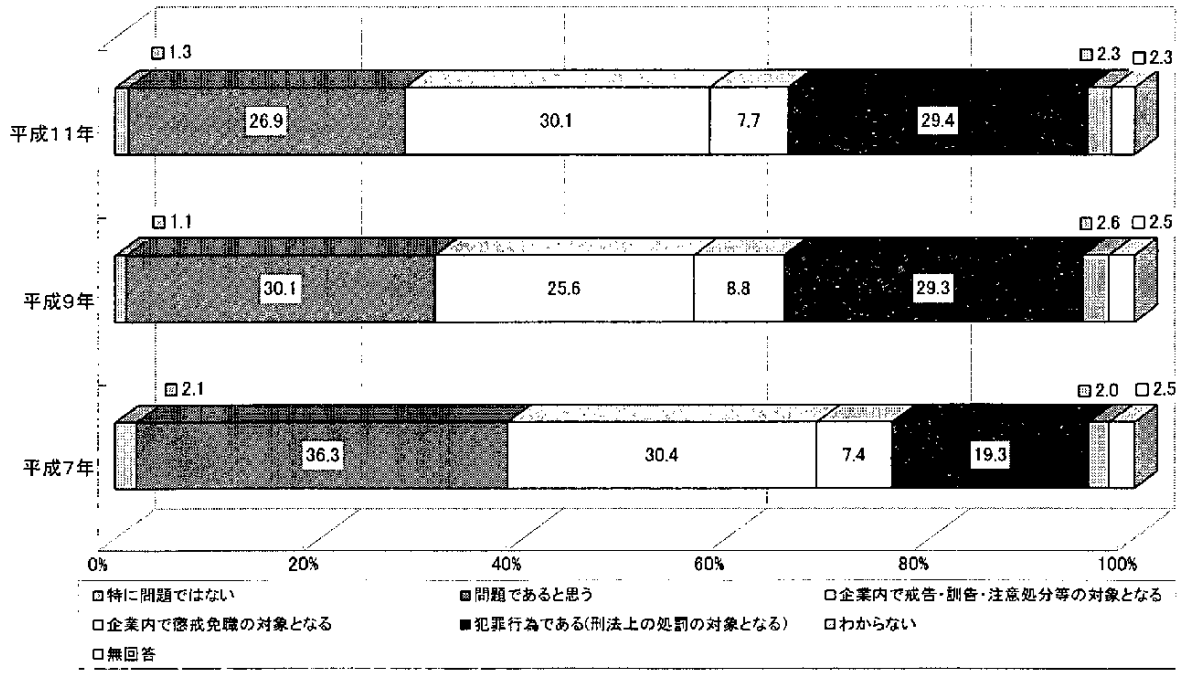


『データ、プログラムの無断使用』に対しては図Q29G5にみるように、単に「問題である」との認識から、「企業内で懲戒免職」になったり、「刑法上の犯罪行為である」との見方が増加しており、犯罪という考えが定着したといえよう。

業種別にみると、公共サービス、情報処理サービス、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、資本金規模との強い相関がみられる。資本金の少ない小規模な組織体ほど犯罪行為という認識に欠けている。

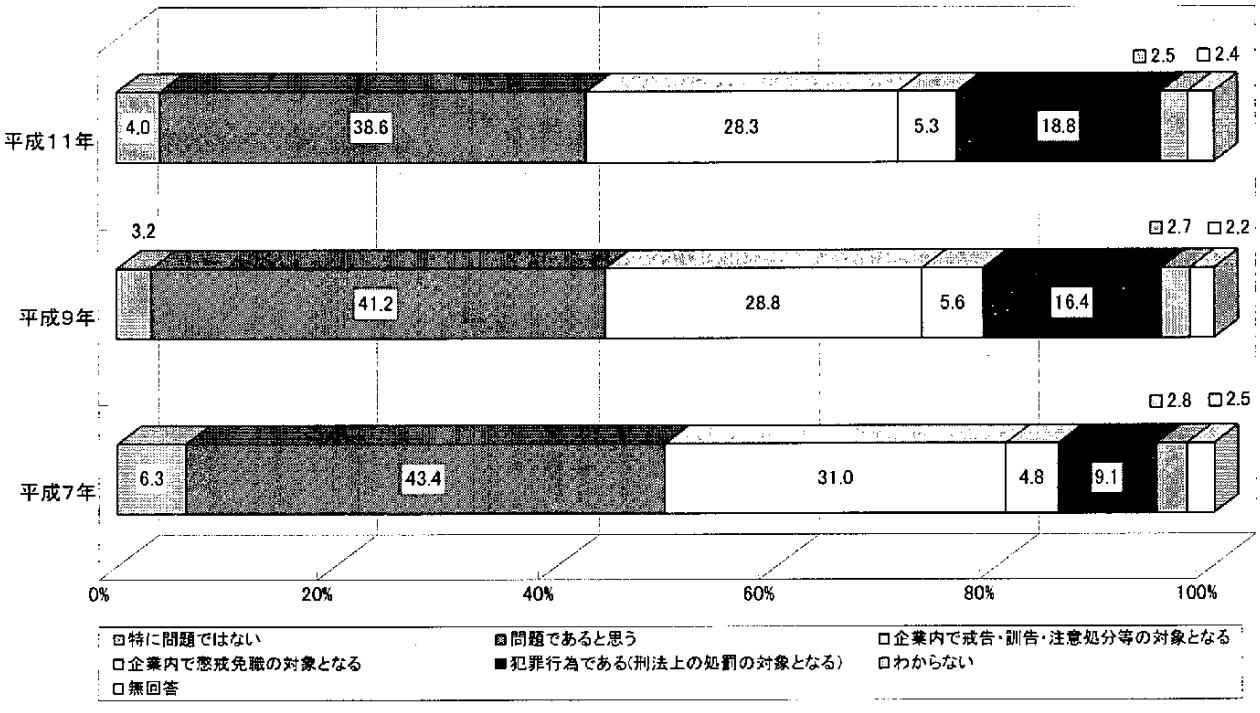
Q29G5. データ、プログラムの無断使用



『データ、プログラムを覗き見る』行為に対しては図Q29G6にみるように、「問題である」との認識は平成9年度と比べて大きな差はみられないが、「犯罪行為である」との認識は増加して18．8%となっている。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。

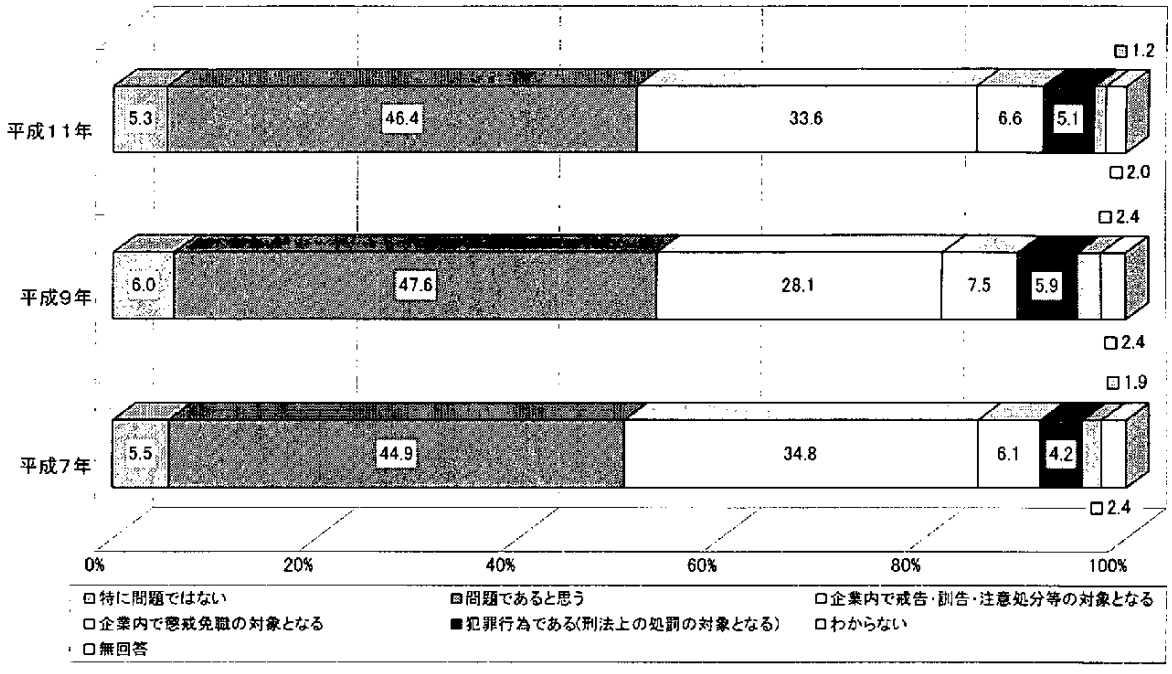
業種別にみると、情報処理サービスの刑法上の犯罪という意識が27．0%となっており、二番手である金融・保険業を6．1ポイントリードしている。すなわち、情報処理サービスでの意識改革が進んでいるといえよう。資本金規模との関係は、市販ソフトのコピー、データ・プログラムの無断使用と同様に、資本金との強い相関がみられる。今後、中小企業における情報処理でのいっそうの啓蒙化活動が望まれる。

Q29G6. データ、プログラムを覗き見る



行　為　項　目	会社のコンピュータを私用に使う		コンピュータウイルスを伝染させる		他社のシステムへ侵入する	
特に問題ではない	46	5.3	1	0.1	1	0.1
問題であると思う	402	46.4	89	10.3	44	5.1
企業内で戒告・訓告・注意処分等の対象となる	291	33.6	159	18.3	46	5.3
企業内で懲戒免職の対象となる	57	6.6	65	7.5	50	5.8
犯罪行為である(刑法上の処罰の対象となる)	44	5.1	525	60.6	694	80.0
わからない	10	1.2	17	2.0	20	2.3
無回答	17	2.0	11	1.3	12	1.4
計	867	100.0	867	100.0	867	100.0

Q29G7. 会社のコンピュータを私用に使う

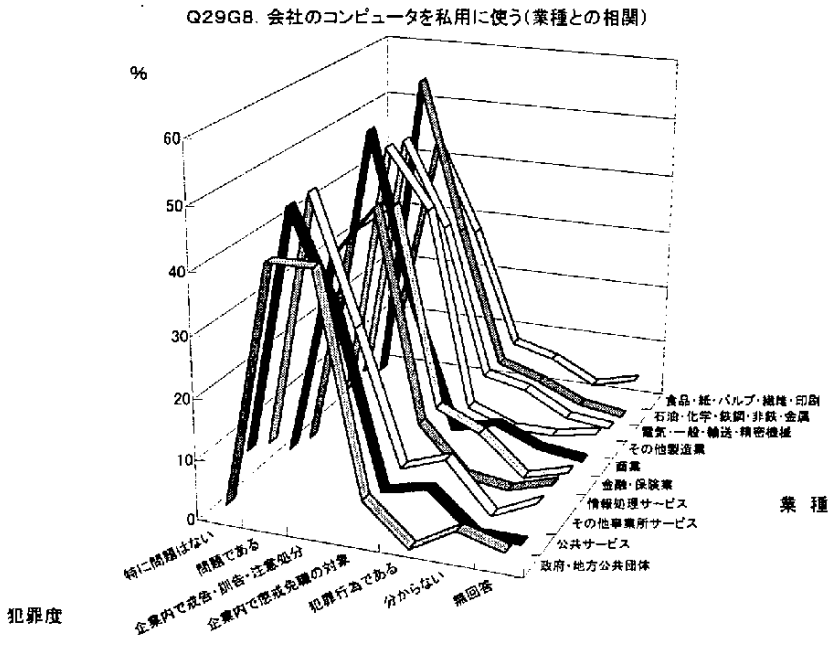


『会社のコンピュータを私的に使う』行為に対しては図Q29G7にみるように、「問題である」との認識は平成7年度、9年度調査とほとんど大きな差がみられない。まだまだ犯罪という認識は希薄といえよう。会社の資産を使っているという組織体内での教育が今後ともに重要と考えられる。

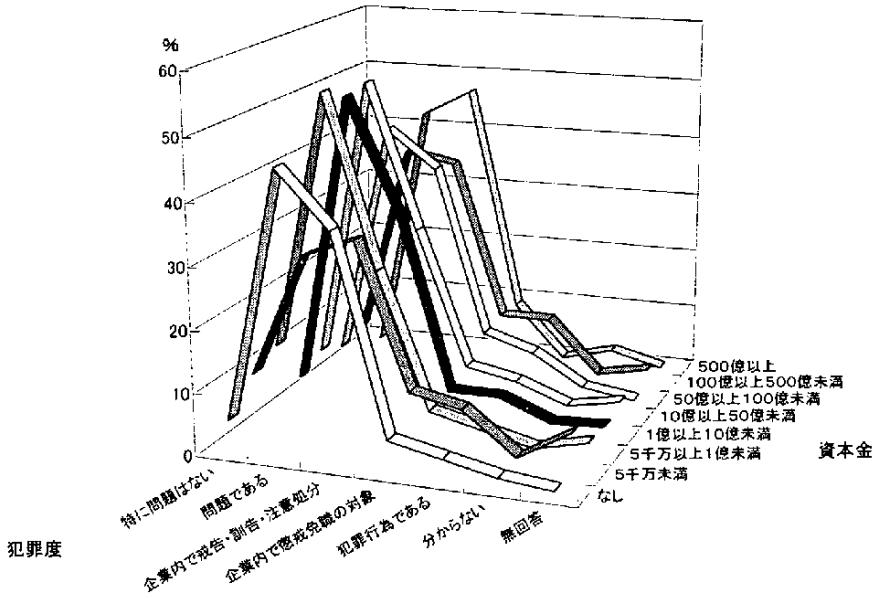
業種別にみると、あまり大きな差はみられないが、その他対事業所サービス、公共サービスでの意識改革が進んでいる。情報を活用する業種では私的な利用は組織内では処分されるようになってきているといえよう。

次に、情報化投資額が大きい組織体ほど、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、情報化投資額が大きいほど情報のもつ価値を重視しており、いきおい、従業員に対しても情報化を率先させているため、また、私的利用で組織体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。

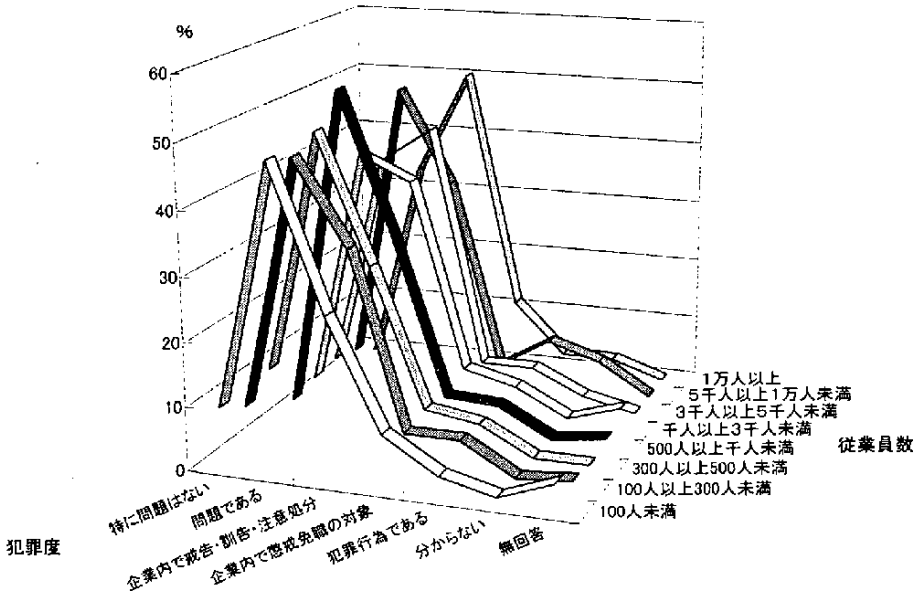
Q29G8. 会社のコンピュータを私用に使う(業種との相関)



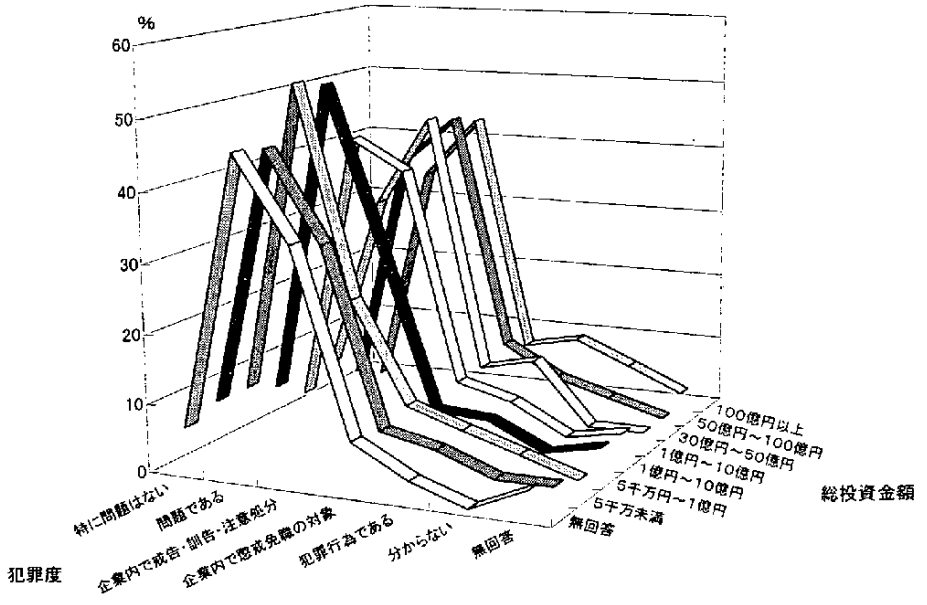
Q29G9. 会社のコンピュータを私用に使う(資本金との相関)



Q29G10. 会社のコンピュータを私用に使う(従業員との相関)

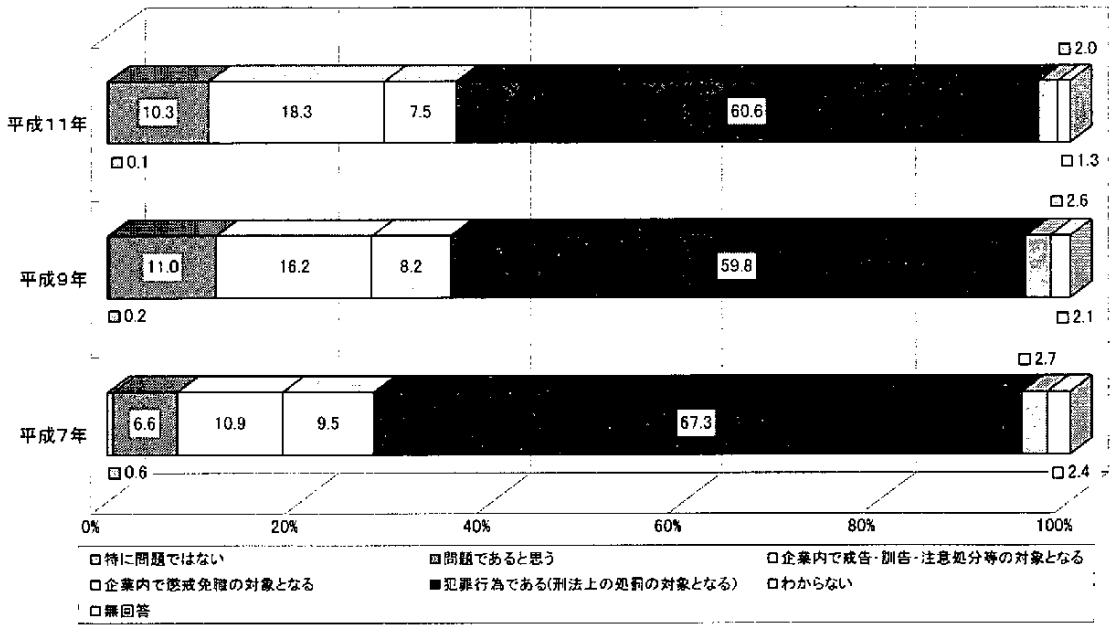


Q29G11. 会社のコンピュータを私用に使う(情報化投資額との相関)



『コンピュータウイルスを伝染させる』行為に対しては図Q29G12にみるように、「問題ではない」との回答は1件しかなく、「企業内での処分対象」と「犯罪行為」をあわせると86．4%となり、犯罪という考えが定着したといえよう。

Q29G12. コンピュータウイルスを伝染させる

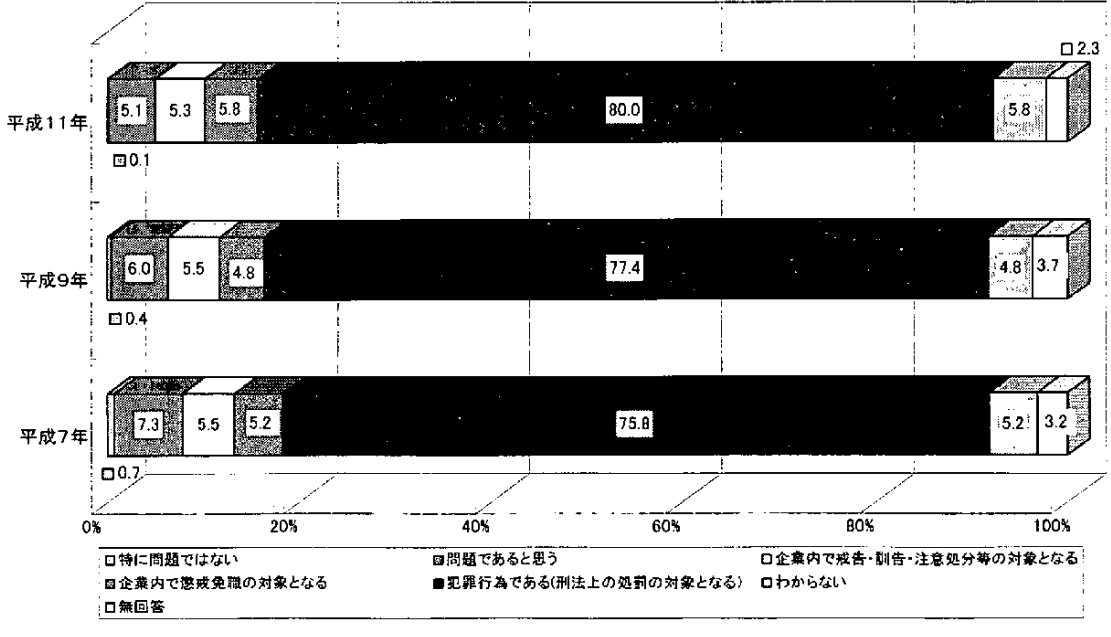


昨今の組織体におけるウイルスによる被害の増大、IPAによる啓蒙活動などによって、ウイルスを伝染させることが重大な被害につながるということが浸透したといえよう。

なお、この傾向は、業種別、企業規模(資本金、従業員数)の大小、情報化投資額の大小であまり差異がなかった。

『他社のシステムに侵入する』行為に対しては図Q29G13にみるように、「犯罪行為である」との回答が平成9年度の77．4%からさらに増えて80．0%となっている。「企業内での処分対象」をあわせると90%以上となり、ウイルス同様犯罪という認識が定着したといえよう。今後も、企業や教育機関においてコンピュータに関する犯罪として教育を進めていくことが重要である。

Q29G13. 他社のシステムへ侵入する

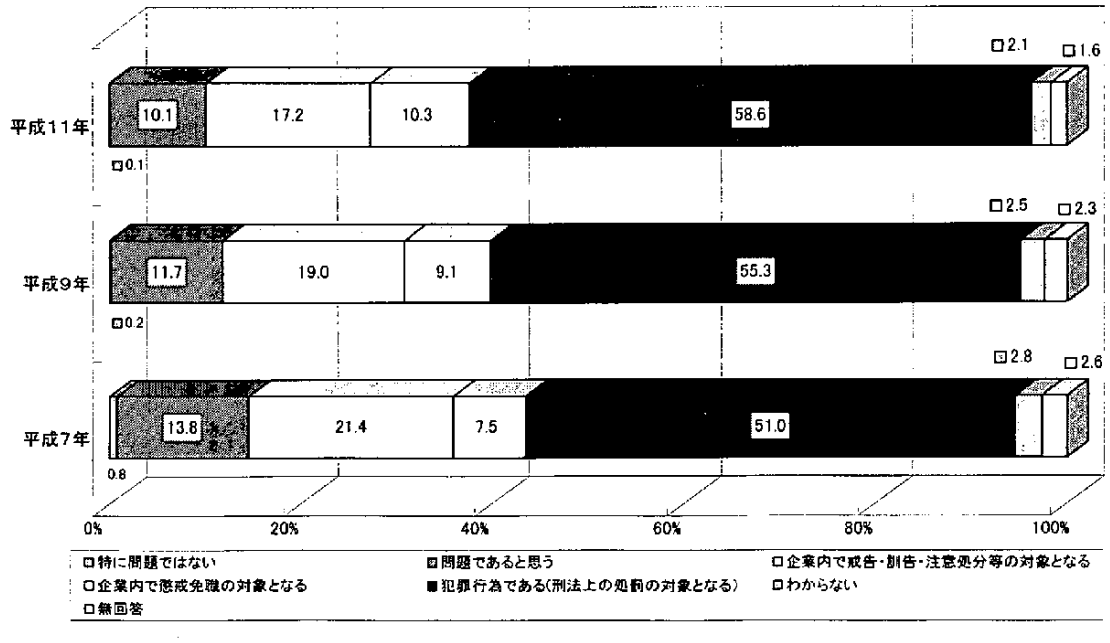


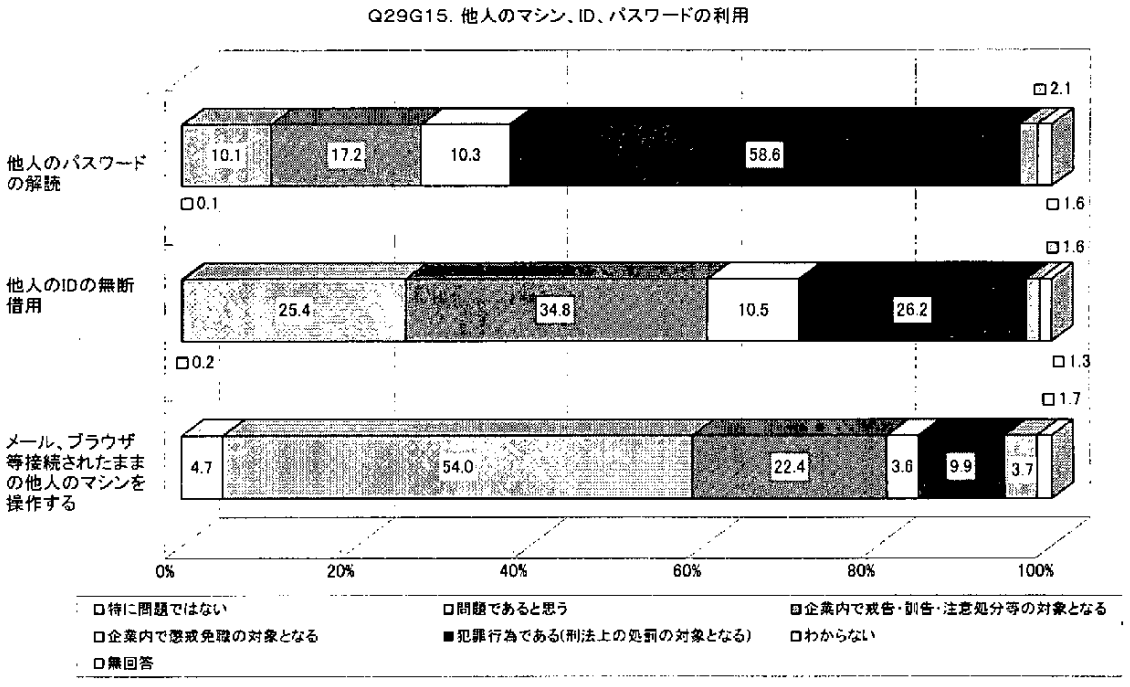
なお、この傾向は業種別にはあまり大きな差がみられなかった。ほとんどの組織体で犯罪という考えが一般化してきていると考えられる。これには本年2月から施行された「不正アクセス行為の禁止等に関する法律」によるものとも考えられる。ただ、政府・地方公共団体が刑法上の犯罪と考える割合が平均より若干下回っている。これは設問が「他社」とあり、政府関係の組織が含まれていないと考えた可能性がある。

行　為　項　目	他人のパスワードを解読し、使用する		他人のIDを無断借用する		メール、ブラウザ等接続されたままの他人のマシンを操作する	
特に問題ではない	1	0.1	2	0.2	41	4.7
問題であると思う	88	10.1	220	25.4	468	54.0
企業内で戒告・訓告・注意処分等の対象となる	149	17.2	302	34.8	194	22.4
企業内で懲戒免職の対象となる	89	10.3	91	10.5	31	3.6
犯罪行為である(刑法上の処罰の対象となる)	508	58.6	227	26.2	86	9.9
わからない	18	2.1	14	1.6	32	3.7
無回答	14	1.6	11	1.3	15	1.7
計	867	100.0	867	100.0	867	100.0

『他人のパスワードを解読し、使用する』行為に対しては図Q29G14にみるように、「犯罪行為である」との回答が平成7年度調査の51．0%、9年度の55．3%から増えて58．6%となっている。すなわち、犯罪という認識が定着しつつあるといえよう。この行為（58．6%が刑法上の犯罪と回答）は前問の『他社のシステムに侵入する』行為（80．0%が「刑法上の犯罪」と回答）に比べると犯罪という認識が薄い。組織体内での不正行為があった場合には、被疑者のパスワードを解読する必要があるので問題ではあるが、必要との見方をしているためと考えられる。前問とあわせて、今後も、企業や教育機関において犯罪として教育を進めていくことが重要である。

Q29G14．他人のパスワードを解読し、使用する





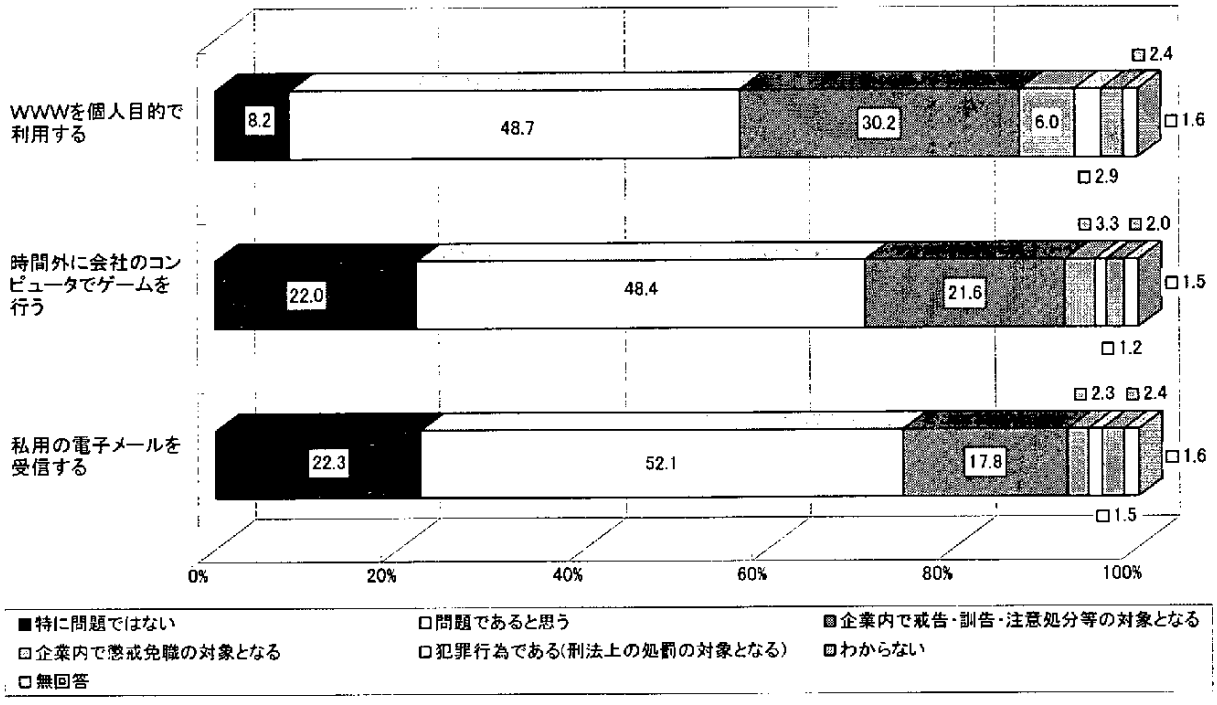
『他人のIDの無断使用』に対しては「問題がある」との認識はパスワードの解読の場合と同様であるが、『他人のパスワードを解読し、使用する行為』の方が、より犯罪度が高いと考えていることがわかる。これは、各組織体ではグループで仕事をしていることが多く、緊急な場合などで他人のIDで仕事を行うなどの実態があり、問題があるとは認識しながらも犯罪であるという認識が低いものと考えられる。これは、『メール、ブラウザ等接続されたままの他人のマシンを操作する行為』に対する回答をみると顕著である。ネットワークに接続された状態の他人のマシンでもグループで使うという実態が少なからずあり、これに対して「問題である」という意識が希薄である。今後、ネットワークに接続されたままでマシンを放置しないこと、他人のマシンの利用には問題があるという教育、組織体内での厳重な処分という姿勢が望まれる。

行　為　項　目	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受信する		時間外に会社のコンピュータでゲームを行う	
特に問題ではない	71	8.2	193	22.3	191	22.0
問題であると思う	422	48.7	452	52.1	420	48.4
企業内で戒告・訓告・注意処分等の対象となる	262	30.2	154	17.8	187	21.6
企業内で懲戒免職の対象となる	52	6.0	20	2.3	29	3.3
犯罪行為である(刑法上の処罰の対象となる)	25	2.9	13	1.5	10	1.2
わからない	21	2.4	21	2.4	17	2.0
無回答	14	1.6	14	1.6	13	1.5
計	867	100.0	867	100.0	867	100.0

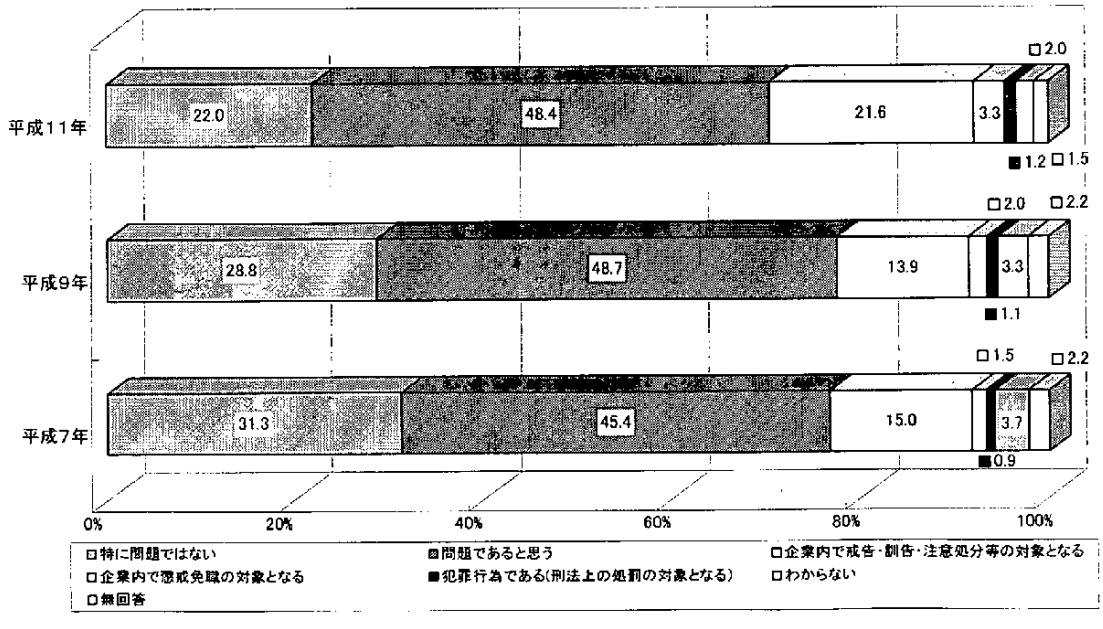
『WWWを仕事以外で利用する』、『私用の電子メールを受信する』、『時間外に会社のコンピュータでゲームを行う』の3つの項目は、いずれも組織体のコンピュータの私的な利用についての設問である。私用の電子メール、時間外のコンピュータゲームについて、約50%もの組織体は「問題がある」と認識している。一方、約20%が「特に問題ではない」と回答しており、組織体としても、コンピュータリテラシィ教育のためにはある程度の個人利用はやむを得ないと黙認している現状が推察できる。『WWWの個人利用』と『電子メールの個人利用』を比べると、「問題がない」という返答がWWWについては少なく、電子メールに比べるとより厳しい対応がなされている。これは、ホームページの検索やネット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。

業種別、企業規模(資本金、従業員数)、情報化投資額との関係については、ほとんど差はみられなかった。

Q29G16. パソコンの個人使用についての比較



Q29G17. 時間外に会社のコンピュータでゲームをする



米国で求人関連ポータルサイトである Vault.com(旧称 VaultReports.com)が1999年9月に電子メールやWWWの個人利用に関してアンケートを行った。従業員1，244人、雇用者1，438人から回答を得て、その結果をホームページ上(http://www. Vault.com)で公開している。

これによると、『職場で1日に仕事に無関係なメールを何通受け取るか』という質問に対しては、「1日に1～5通」が31．7%、「1日に10～20通」が28．3%という結果である。また、『職場で仕事に無関係なWWWのサイトを見てもよいと思うか。どのくらいの時間だったら許されるか』という質問に対し、従業員からは「30分までならよい」が31．2%、「15分まで」が24．4%、「絶対ダメ」は12．5%という回答であった。また頻度については、「定期的に」が37．1%、「1日に数回」が31．9%と答えている。同様の質問に対し雇用者側からは、『従業員が仕事に無関係なメールを送ってもよいと思うか。どのくらいの頻度だったら許されるか』という質問に対しては、「1日に1～5回」が61．0%、「1日に5～10回」が14．5%程度を容認している。「絶対ダメ」と回答したのは14．2%であった。また、『従業員が仕事に無関係なWWWサイトを見てもよいと思うか』との質問に対し、「15分までならよい」が31．3%、「30分まで」が26．6%。「絶対ダメ」は17．8%であった。

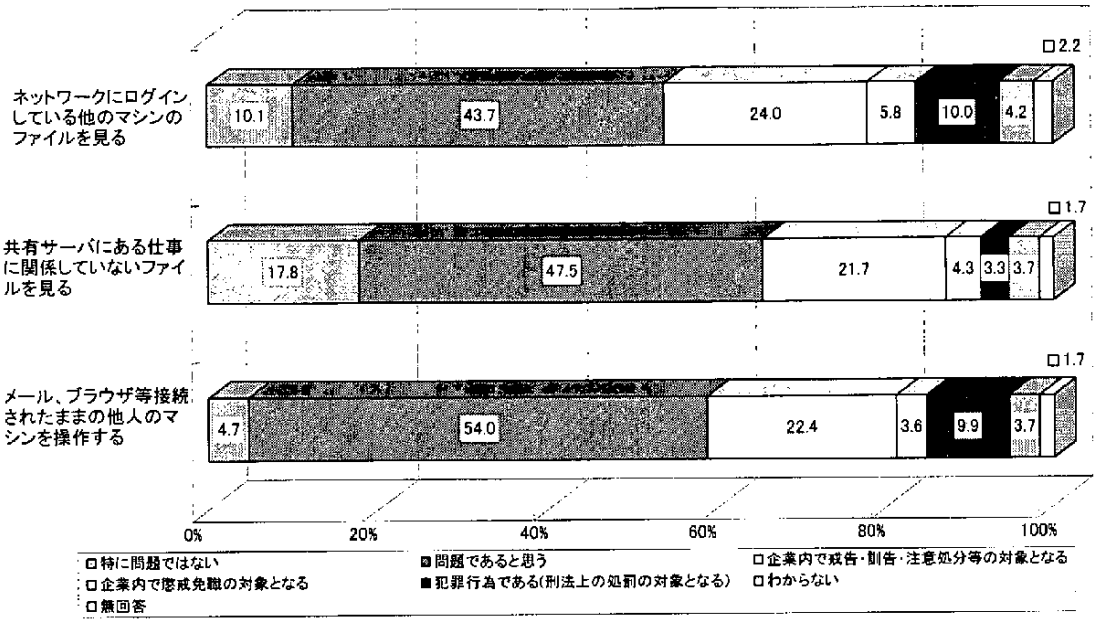
今回のJIPDECの調査結果は、同一の質問内容ではないので単純に比較はできないが、雇用者側の見解を比べると日本の方が厳しいようだ。これは、米国では電子メールが一般化してきており、また、企業の社会的責任という形でのボランティア活動などで電子メールやWWWのホームページへのアクセスを許容していると考えられる。日本においても、企業間のつながり、個人のネットワークなど個人領域の活動と企業の利益活動を切り分けられないところがあり、電子メールがこのような目的で使われているところもあり、電子メールの利用を100%制限するのではなく、むしろ、従業員に適切な使い方を学ばせ、自主規制させるように仕向けるのがよいのではないだろうか。

なお、『時間外に会社のコンピュータでゲームを行う』行為については、平成7年度、9年度調査と比較すると、「特に問題がない」という回答が減ってきており、30%近くが注意や処分対象と考えるようになってきている。最近のパソコンは機能も高く、ローカルのハードディスクも大容量となりつつあり、汎用のコンピュータ端末としての利用から、インターネットやイントラネットのクライアントマシンと位置づけられるようになっている。また、大量の情報処理を行うため、ウイルスなどを持ち込む危険性のあるコンピュータゲームを行う風潮が改善されつつあるともいえよう。

今後、組織体内でのパソコン利用が進み、コンピュータリテラシィ教育が一段落するにつれ、ある程度の個人利用が制限されていくと考えられる。

行　為　項　目	ネットワークにログインしている他のマシンのファイルを見る		共有サーバにある仕事に関係していないファイルを見る		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	88	10.1	154	17.8	1	0.1
問題であると思う	379	43.7	412	47.5	15	1.7
企業内で戒告・訓告・注意処分等の対象となる	208	24.0	188	21.7	26	3.0
企業内で懲戒免職の対象となる	50	5.8	37	4.3	68	7.8
犯罪行為である(刑法上の処罰の対象となる)	87	10.0	29	3.3	734	84.7
わからない	36	4.2	32	3.7	15	1.7
無回答	19	2.2	15	1.7	8	0.9
計	867	100.0	867	100.0	867	100.0

Q29G18. 他のマシンやファイルへのアクセスに関して



各組織体ではファイルの共有やデータベース化を進めている。このなかで、個人のファイルや自分の仕事に関係のないものへのアクセスをどのように考えているかを調査した。平成11年度の新規項目である『ネットワークにログインしている他のマシンのファイルを見ること』、『仕事に関係しないファイルへのアクセス』については、通常はアクセス制御でコントロールすべきものである。特に、ネットワークにログインしている他のマシンのファイルを見ることが「問題ではない」という回答が10%を上回っており、ただ、漠然と「問題である」と考えている様子がわかる。これは、ネットワークに接続されたマシンを利用する場合のケースと比べても割合が高い。今後、個人の意識改革を進め、ネットワークで見えるからファイルにアクセスしてもかまわないという風潮を変え、個々のファイルにアクセス制御を行うこと、他のファイルが見える状態であっても仕事に関係がない限りアクセスしないという利用マナーを身につけることが望まれる。

業種別、企業規模(資本金、従業員数)、情報化投資額との関係では、大きな差はみられなかった。ただし、情報処理サービスが他の業種と比べるとより厳しいものとなっている。

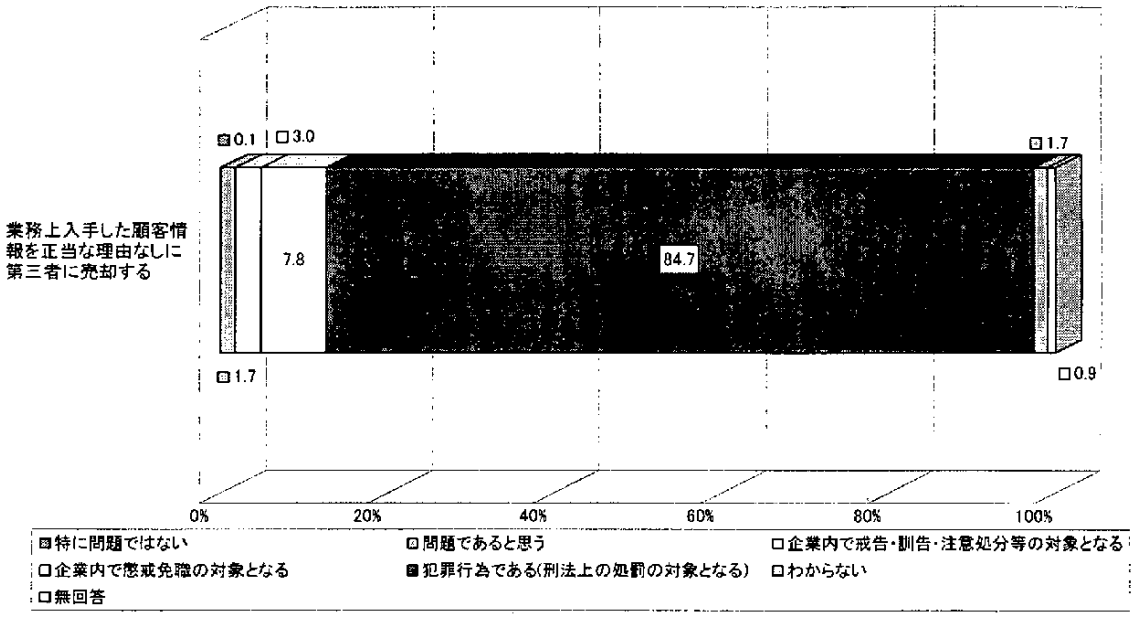
『共有サーバにある仕事に関係していないファイルを見る』行為に関しては、その他製造業、公共サービスで若干、甘い傾向がみられた。

平成11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が多発した。そのため、この問題に対しては84.7%が「犯罪行為」と認識しており、「企業内の処分」を含めると95.5%が厳格な対応をすると回答している。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くる。しかし、ネットワーク社会では個人のプライバシーを保護することが国際的なコンセンサスとなっており、今後、組織体において顧客情報の管理の徹底が重要となる。プライバシーマークの利用を含め、積極的に取り組むことが必要である。

業種別にみると、「犯罪行為」とみなす割合は、政府・地方公共団体(93.3%)、情報処理サービス(91.0%)、金融・保険業(87.9%)が他の業種と比べ高く厳しいものとなっている。

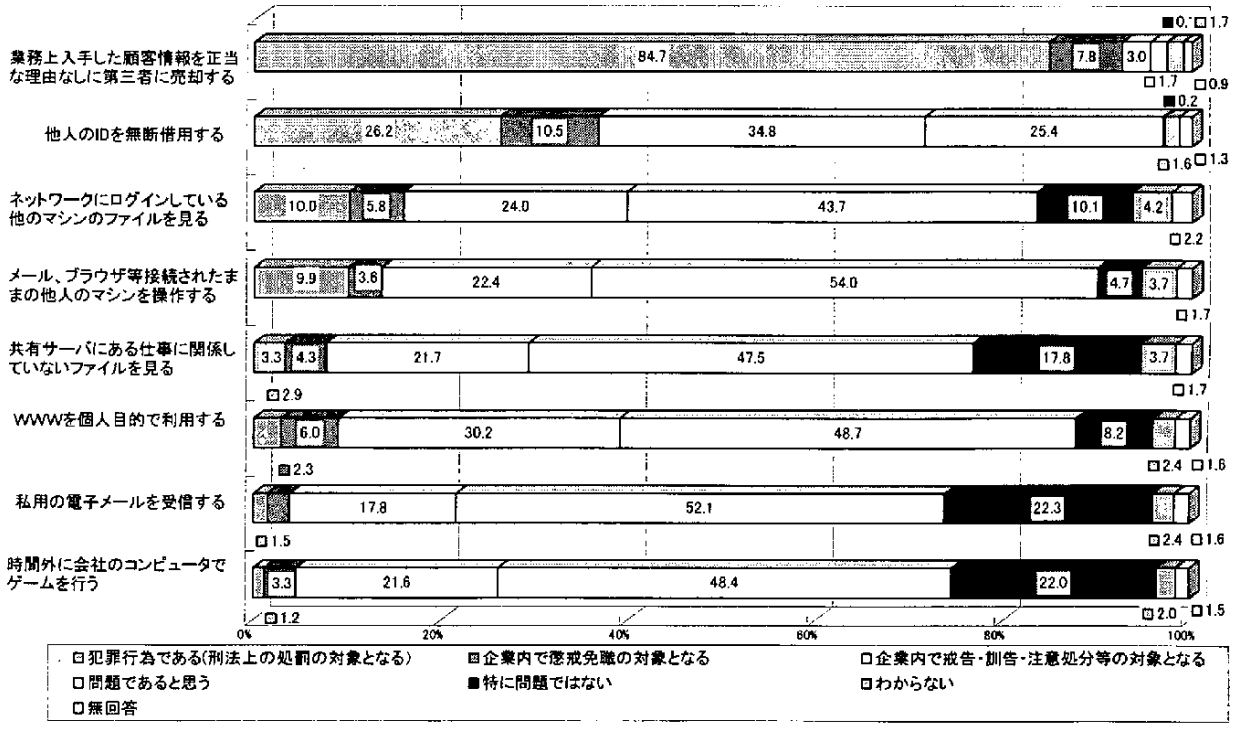
企業規模(資本金、従業員数)、情報化投資額の点では、小規模企業ほど犯罪とみなす割合が低い。今後、中小企業などに対して顧客情報の管理を徹底させることが必要であろう。電子商取引では企業規模にかかわらず競争できる点がメリットであるが、企業規模によって管理がルーズであると、電子商取引自体の信用をなくすことにもつながりかねない。

Q29G19. 顧客情報の漏洩について



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、Q29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。

Q29G20. さまざまなコンピュータ利用での犯罪認識度



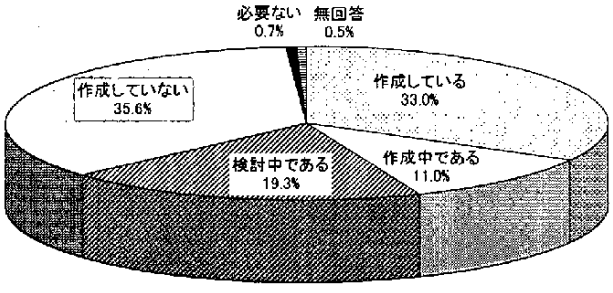
この結果では、『業務上入手した顧客情報を正当な理由なしに第三者に売却する』行為が、最も犯罪としての認識度合いが高く84．7%となっている。次いで、『他人のIDを無断借用する』、『ネットワークにログインしている他のマシンのファイルを見る』が10%を超えている。『メール、ブラウザ等接続されたままの他人のマシンを操作する』が、僅差の9．9%であるが、『共有サーバにある仕事に関係しないファイルを見る』、『WWWを個人目的で使用する』、『私用の電子メールを受信する』、『時間外の会社のコンピュータでゲームを行う』は、組織体内での懲戒免職を含めても数パーセントであり、ほとんど犯罪行為という認識が少ない。企業や組織内の仕事において「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。企業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。

2．5　災害対策・障害対策について

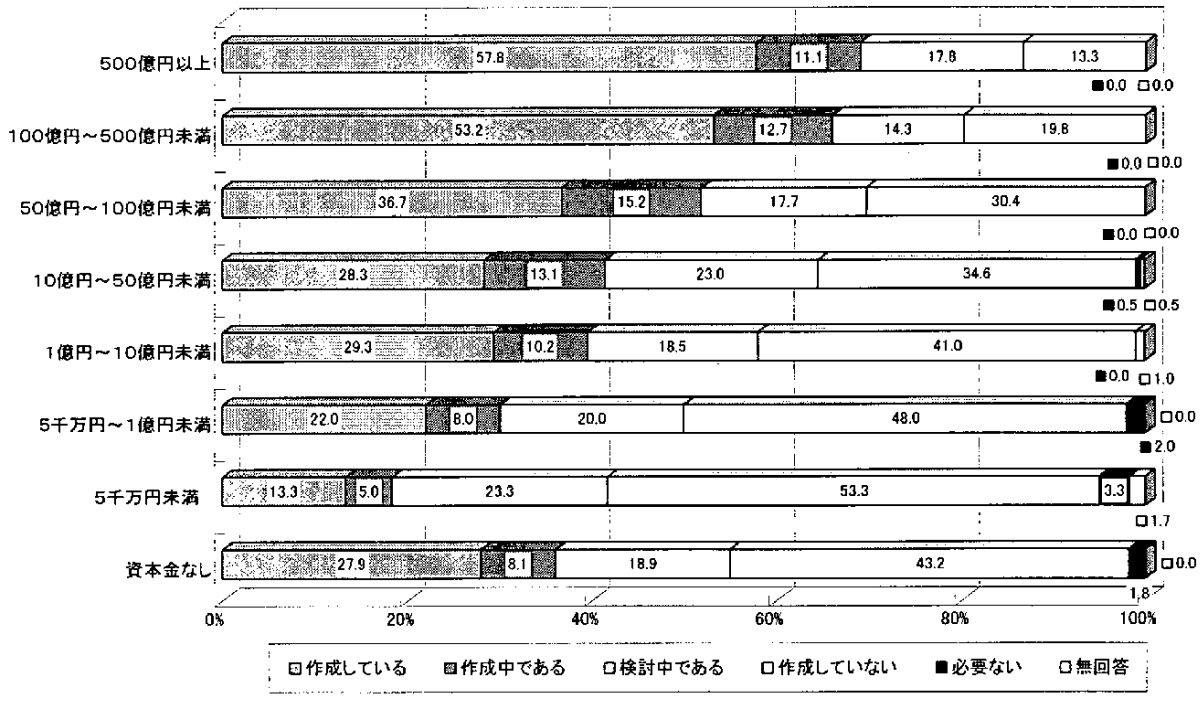
Q30．非常事態の発生を想定して危機管理に関する全社的なマニュアル類を作成していますか。

1	作成している	286	33.0
2	作成中である	95	11.0
3	検討中である	167	19.3
4	作成していない	309	35.6
5	必要ない	6	0.7
無回答		4	0.5
計		867	100.0

Q30G1．災害復旧に関する計画書、マニュアル類の作成状況



Q30G2．危機管理マニュアルの作成状況



マニュアル類を「作成していない」は前回調査（41．9%）に比べ大幅に減っている。また、「作成している」、「作成中」をあわせる（44．0%）とこれも前回調査の33．9%を大幅に上回っている。

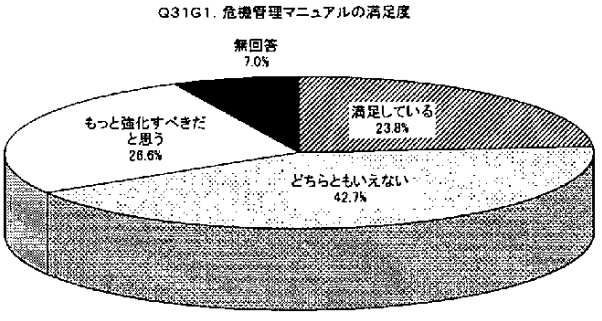
業種別にみると、金融・保険業が特に大きく89．0%、次いで情報処理サービスが49．5%と、前回調査と傾向としては変わらないが、特に金融・保険業での「作成している」は前回調査の57．3%に対し、今回調査では78．0%と同業界の中で積極的な準備が進められていることが読み取れる。

企業規模（資本金、従業員数）別では、当然小さくなればなるほど「作成していない」割合が高くなるが、それが30%を上回るボーダーラインは前回、今回調査とも資本金50億円前後である。この割合が前回調査に比べ特に減少が激しかったのは10億円～50億円未満までのゾーンで、今後ベンチャー企業を中心にますます小規模企業が活発化することを考えると、これは好ましい傾向といえる。

Q31.（作成している場合）貴社でとられている危機管理マニュアルは、全体的にみて満足できるものですか。（Q30の「1」を回答）

1	満足している	68	23.8
2	どちらともいえない	122	42.7
3	もっと強化すべきだと思う	76	26.6
無回答		20	7.0
計		286	100.0

今回初めての質問であるが、この数字とQ30の分析を関連させると、マニュアルの整備はかなりの組織体で進んでいるが、今後とも継続的改善の余地があることを物語っており（2および3の合計が69．3%）、特に商業でこの傾向は顕著である（88．2%）。すなわち、満足の基準が求められているということである。

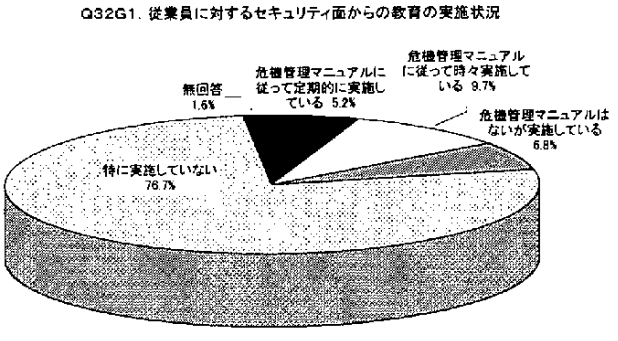


Q32. 非常事態に備えて従業員に対してセキュリティの面から訓練を実施していますか。

1	危機管理マニュアルに従って定期的に実施している	45	5.2
2	危機管理マニュアルに従って時々実施している	84	9.7
3	危機管理マニュアルはないが実施している	59	6.8
4	特に実施していない	665	76.7
無回答		14	1.6
計		867	100.0

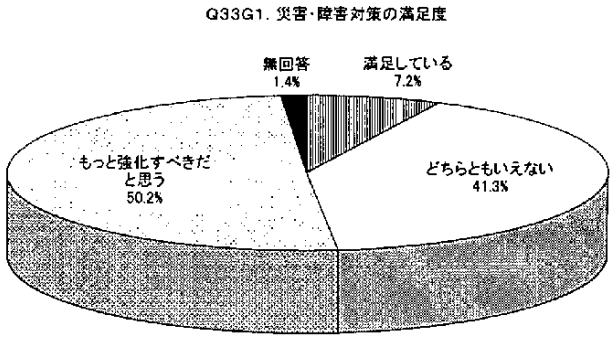
情報セキュリテイ面の訓練に特化した質問は今回初めてであるが、コンピュータウイルスに絞り込んだ前回、今回調査の回答を含め、訓練としては「特に実施していない」が圧倒的に多い。

業種別にどの業種ということはいえないが、情報処理サービスにおいても68．5%が実施していない。これはわが国で情報セキュリテイ面での「非常事態とは何か」の定義がなく狭義に受け取られていること、訓練の意味と方法がみえないこと等によるもので、今後のサイバーセキュリティ時代での重要な検討課題の1つとして取りあげていかなければならない。



Q33. 貴社でとられている災害・障害対策は、全体的にみて満足できるものですか。

1	満足している	62	7.2
2	どちらともいえない	358	41.3
3	もっと強化すべきだと思う	435	50.2
無回答		12	1.4
計		867	100.0



全体として満足していないのは明らかであるが、前回調査に比べ「どちらともいえない」がかなり増加し、「強化すべき」がやや減っている。これはQ31同様、組織体として「満足」の基準だということを意味している。満足の基準は復旧の対応時間、回復のレベル、迅速な報告と情報開示等、業種によって、また組織体固有の経営判断によっても異なるが、今後は満足の基準の作成手法の開発にも力を入れる必要がある。

業種別にみると、情報処理サービスが「もっと強化すべき」の割合が高いのは当然であるが、特筆すべきは商業で、「強化」の割合が高く、対策をより強化すべきと感じられていると判断される。

Q34. ①情報システムのバックアップ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)

②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

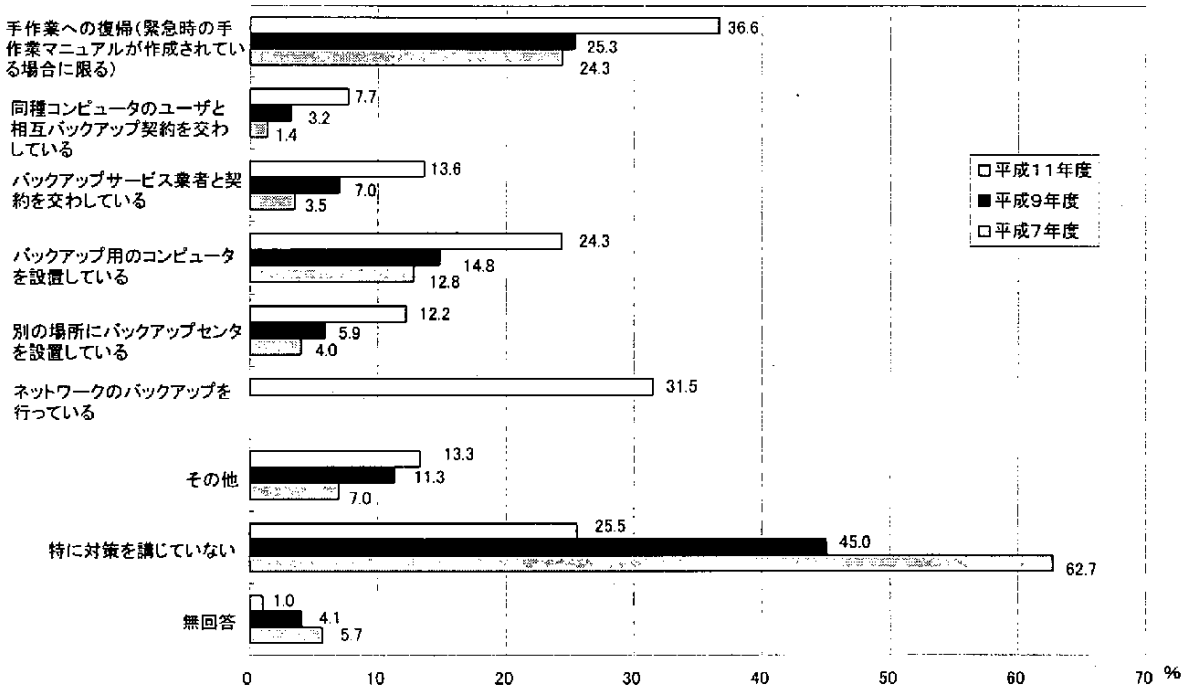
回答件数 867		実施対策		満足している		問題がある		どちらともいえない		無回答	
1	手作業への復帰(緊急時の手作業マニュアルが作成されている場合に限る)	317	36.6	81	25.6	139	43.8	97	30.6	0	0.0
2	同種コンピュータのユーザと相互バックアップ契約を交わしている	67	7.7	18	26.9	28	41.8	20	29.9	1	1.5
3	バックアップサービス業者と契約を交わしている	118	13.6	53	44.9	31	26.3	32	27.1	2	1.7
4	バックアップ用のコンピュータを設置している	211	24.3	103	48.8	57	27.0	49	23.2	2	0.9
5	別の場所にバックアップセンタを設置している	106	12.2	46	43.4	37	34.9	22	20.8	1	0.9
6	ネットワークのバックアップを行っている	273	31.5	112	41.0	81	29.7	77	28.2	3	1.1
7	その他	115	13.3	36	31.3	42	36.5	32	27.8	5	4.3
8	特に対策を講じていない	221	25.5								
無回答		9	1.0								

バックアップ対策として多く利用されている機能は、「手作業への復帰」(36．6%)が多く、次いで「バックアップ用コンピュータ設置」(24．3%)である。

特に「対策を講じていない」と回答した組織体は、平成7年度(62．7%)、9年度(45．0%)、11年度(25．5%)と大幅に減少している。

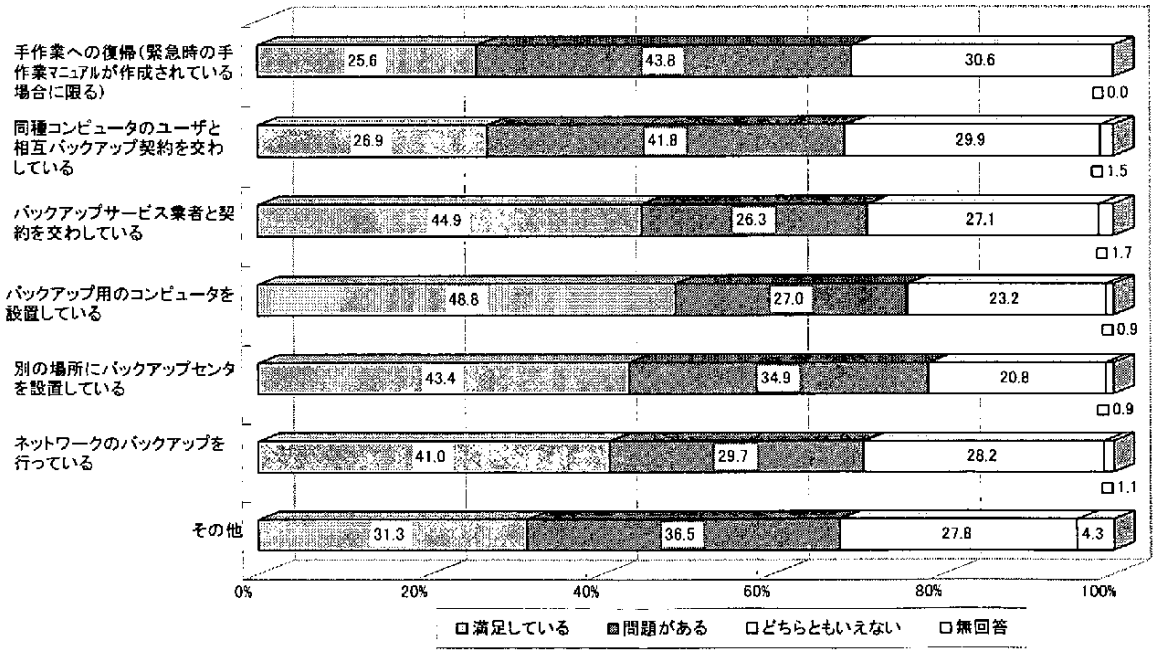
また、「ネットワークのバックアップ」については今回初めてあげた項目であるが、組織体の31．5%がバックアップを行っている。

Q34G1．情報システムのバックアップ対策



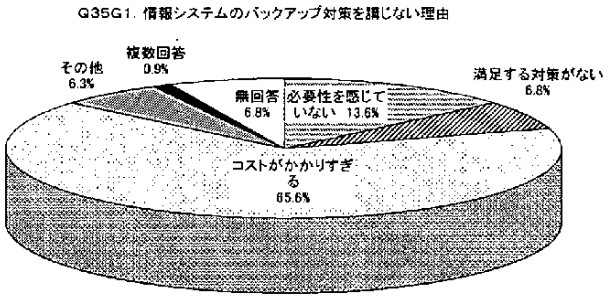
しかし、バックアップ対策の方法についての満足度については、たとえば、「手作業への復帰」についていえば、「満足している」(25．6%)より「問題がある」(43．8%)との回答が18．2ポイント多く、「問題がある」と「どちらともいえない」(30．6%)をあわせると74．4%とかなり高い割合となり、バックアップ対策はまだまだ十分とはいえない。

Q34G2．情報システムのバックアップ方法に対する満足度



Q35. 対策を講じない理由は何ですか。主なもの1つを選んで下さい。(Q34 の「8」を回答)

1	必要性を感じていない	30	13.6
2	満足する対策がない	15	6.8
3	コストがかかりすぎる	145	65.6
4	その他	14	6.3
複数回答		2	0.9
無回答		15	6.8
計		221	100.0



バックアップ対策を講じない理由としては、
「コストがかかりすぎる」が65．6%と多く、
バックアップ対策の必要性は認識しているが
コスト上の理由から対策を講じない組織体が多い。

バックアップ対策にどの程度のコストをかけるかは情報システムの資産価値とのバランスで考えるべきであり、「コストがかかりすぎる」問題は、Q8の『情報システムの資産価値評価』との関係と無縁ではない。

Q36. ①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。(複数回答)

②また、その機能に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

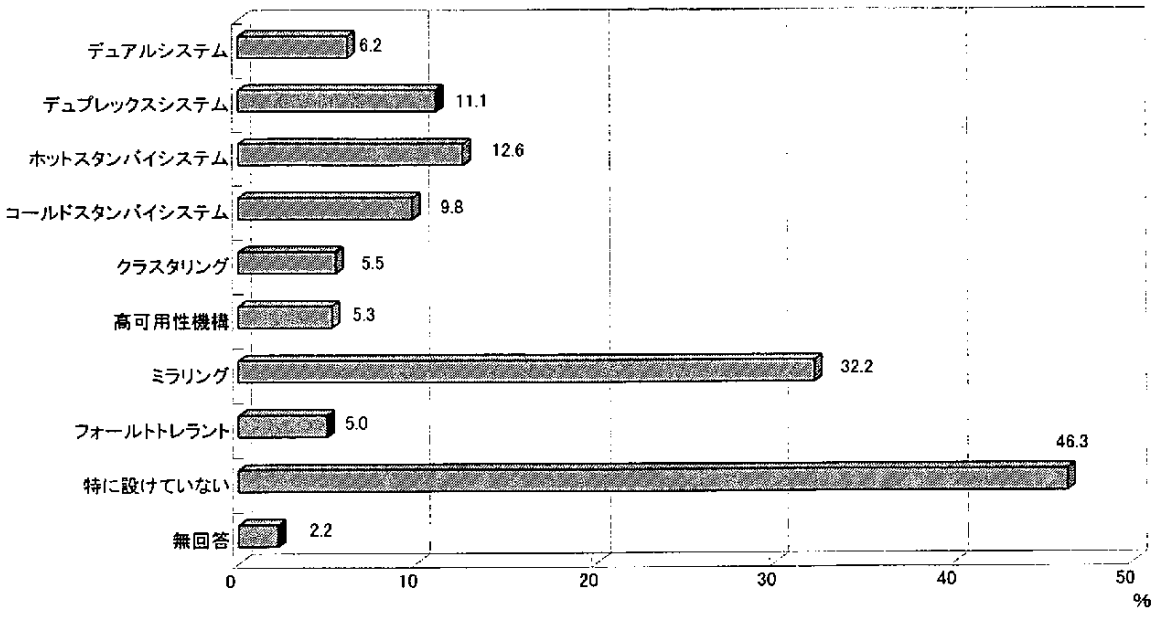
回答件数 867		設置機能		満足している		問題がある		どちらともいえない		無回答	
1	デュアルシステム	54	6.2	23	42.6	14	25.9	17	31.5	0	0.0
2	デュプレックスシステム	96	11.1	53	55.2	21	21.9	21	21.9	1	1.0
3	ホットスタンバイシステム	109	12.6	70	64.2	19	17.4	17	15.6	3	2.8
4	コールドスタンバイシステム	85	9.8	34	40.0	24	28.2	26	30.6	1	1.2
5	クラスタリング	48	5.5	29	60.4	9	18.8	10	20.8	0	0.0
6	高可用性機構	46	5.3	24	52.2	6	13.0	16	34.8	0	0.0
7	ミラリング	279	32.2	155	55.6	47	16.8	71	25.4	6	2.2
8	フォールトトレラント	43	5.0	21	48.8	4	9.3	16	37.2	2	4.7
9	特に設けていない	401	46.3								
無回答		19	2.2								

代替運転機能を「設置していない」(46．3%)は前回調査(66．5%)からみると20．2ポイント減少している。

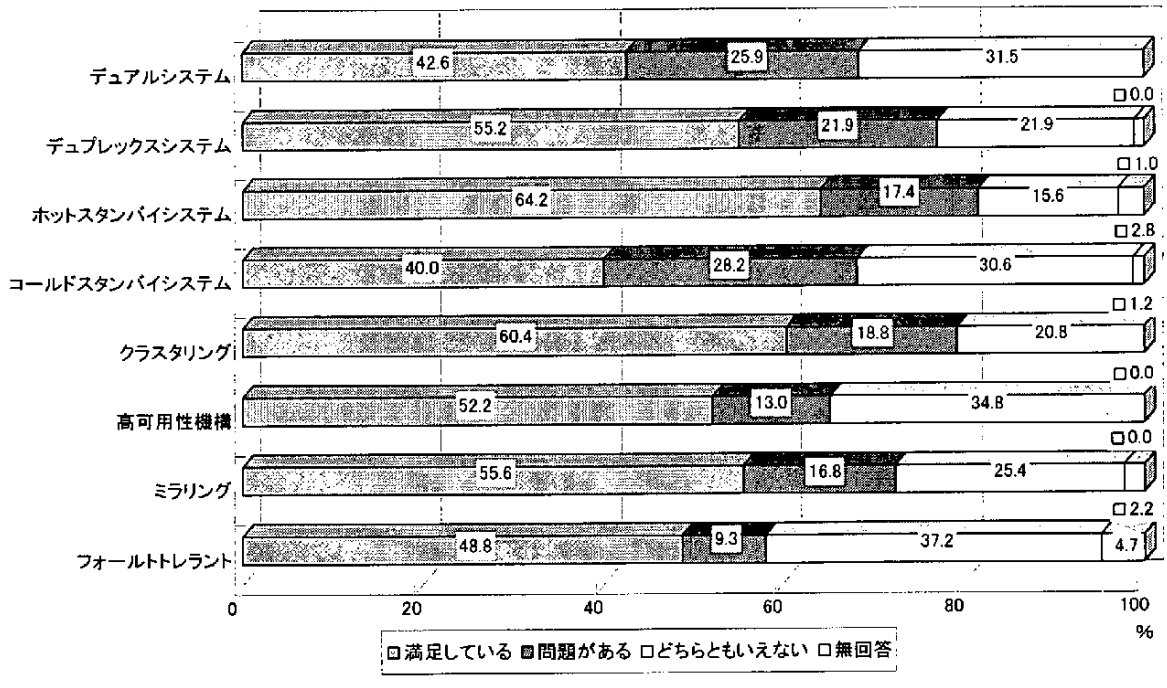
また、全体的にみると「満足している」との回答は「問題がある」との回答を上回っており、代替運転機能設置の現状は満足されているといえる。

ただし、デュアルシステム(「満足している」(42．6%)、「問題がある」+「どちらともいえない」(57．4%))、コールドスタンバイシステム(「満足している」(40．0%)、「問題がある」+「どちらともいえない」(58．8%))は代替運転機能としてかならずしも十分とはいえないようである。

Q36G1. 情報システムの代替運転機能の設置状況



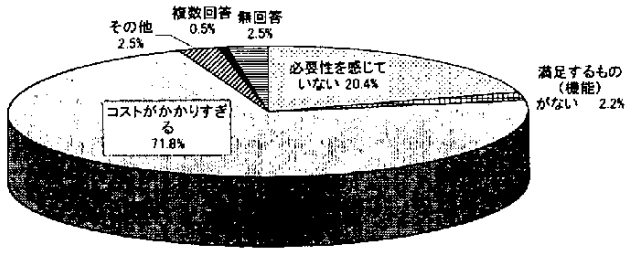
Q36G2. 代替運転機能方法の満足度



Q37. 代替運転機能を設けない理由は何ですか。主なものを1つ選んで下さい。(Q36 の「9」を回答)

1	必要性を感じていない	82	20.4
2	満足するもの(機能)がない	9	2.2
3	コストがかかりすぎる	288	71.8
4	その他	10	2.5
複数回答		2	0.5
無回答		10	2.5
計		401	100.0

Q37G1. 代替運転機能を講じない理由



代替運転機能を設置しない理由としては「コストがかかりすぎる」が71．8%と、ここでもコストの問題を理由に代替運転機能を設置していない組織体が多い。また、「必要性を感じていない」が20．4%であった。

業種別、企業規模（資本金別、従業員数別）、総投資金額別にみても、「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。

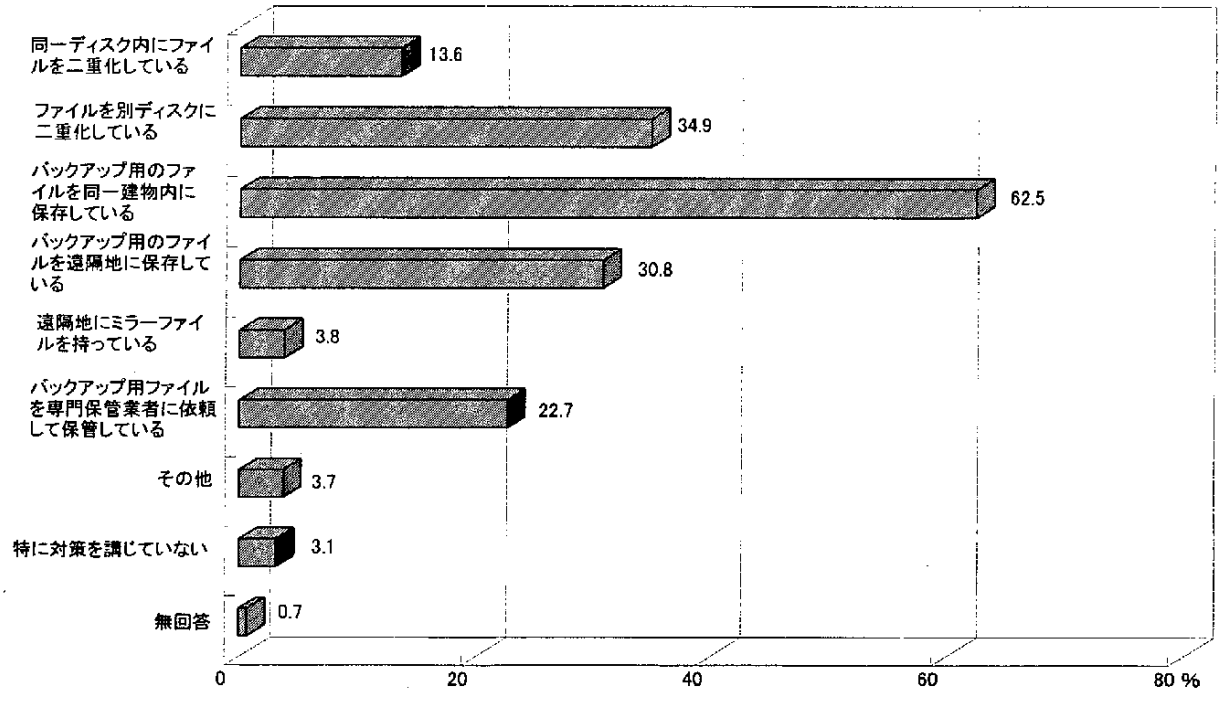
必要性を感じていない組織体を資本金別でみると、資本金50億円未満の規模にその傾向がみられる。 やはり、代替運転機能にかかるコストの問題などを考慮しての結果であろう。

Q38. ①ファイルのバックアップ対策はどのようなものですか。実施している対策項目を選んで下さい。（複数回答）

②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

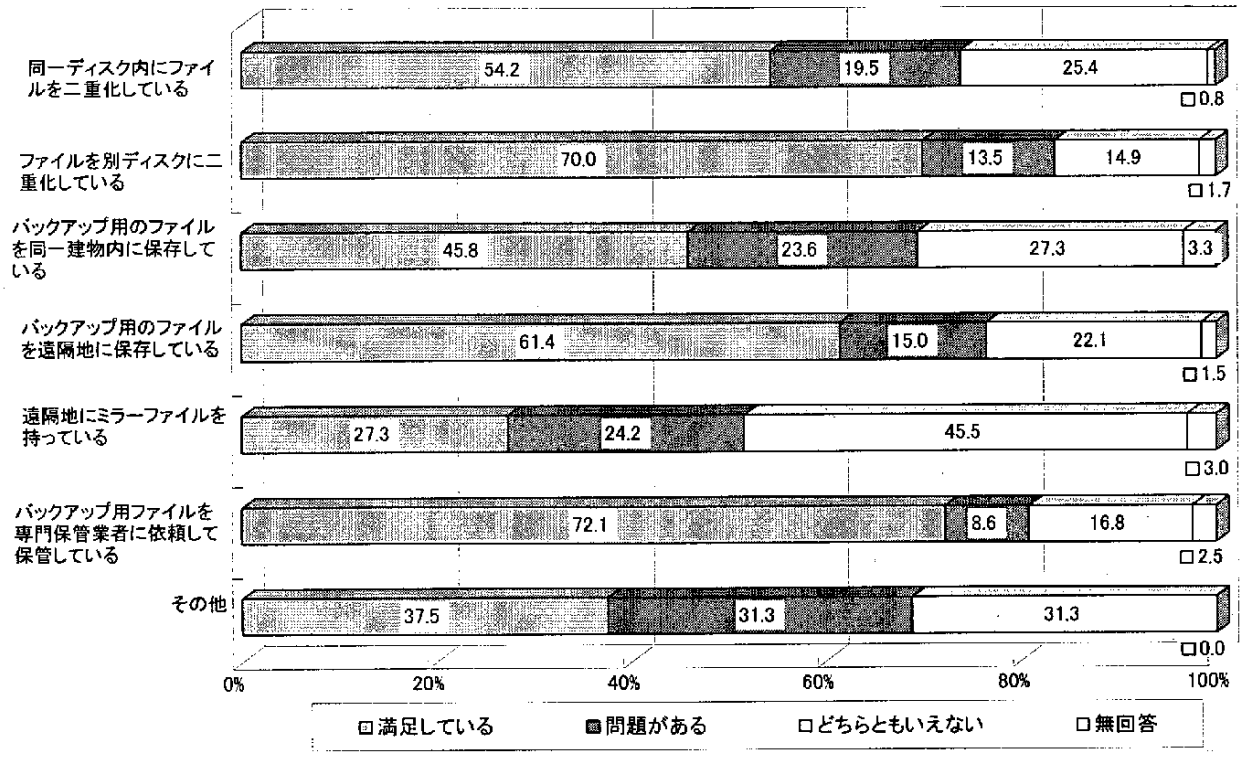
回答件数　867		実施対策		満足している		問題がある		どちらともいえない		無回答	
1	同一ディスク内にファイルを二重化している	118	13.6	64	54.2	23	19.5	30	25.4	1	0.8
2	ファイルを別ディスクに二重化している	303	34.9	212	70.0	41	13.5	45	14.9	5	1.7
3	バックアップ用のファイルを同一建物内に保存している	542	62.5	248	45.8	128	23.6	148	27.3	18	3.3
4	バックアップ用のファイルを遠隔地に保存している	267	30.8	164	61.4	40	15.0	59	22.1	4	1.5
5	遠隔地にミラーファイルを持っている	33	3.8	9	27.3	8	24.2	15	45.5	1	3.0
6	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	197	22.7	142	72.1	17	8.6	33	16.8	5	2.5
7	その他	32	3.7	12	37.5	10	31.3	10	31.3	0	0.0
8	特に対策を講じていない	27	3.1								
無回答		6	0.7								

Q38G1. ファイルのバックアップ方法



ファイルのバックアップ方法については、過去の調査結果同様、「バックアップ用のファイルを同一建物内に保存している」組織体が多く62．5%、次いで「ファイルを別ディスクに二重化している」が34．9%、「バックアップ用のファイルを遠隔地に保存している」が30．8%であった。

Q38G2. ファイルのバックアップ対策の満足度



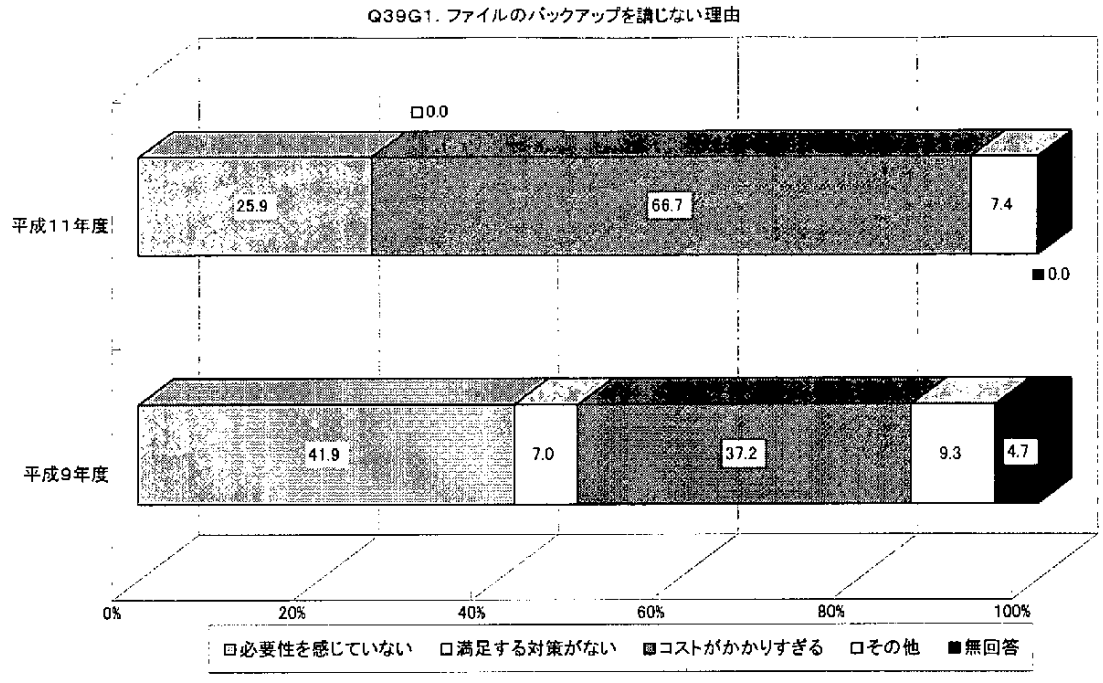
現在行っている対策の満足度については、「遠隔地でのミラーファイル」を除くすべてで「満足している」との回答が「問題がある」、「どちらともいえない」を大幅に上回っており、相対的には自社で行っている対策に満足していることがわかる。

Q39. 対策を講じない理由は何ですか。主なもの1つを選んで下さい。(Q38 の「8」を回答)

1	必要性を感じていない	7	25.9
2	満足する対策がない	0	0.0
3	コストがかかりすぎる	18	66.7
4	その他	2	7.4
無回答		0	0.0
計		27	100.0

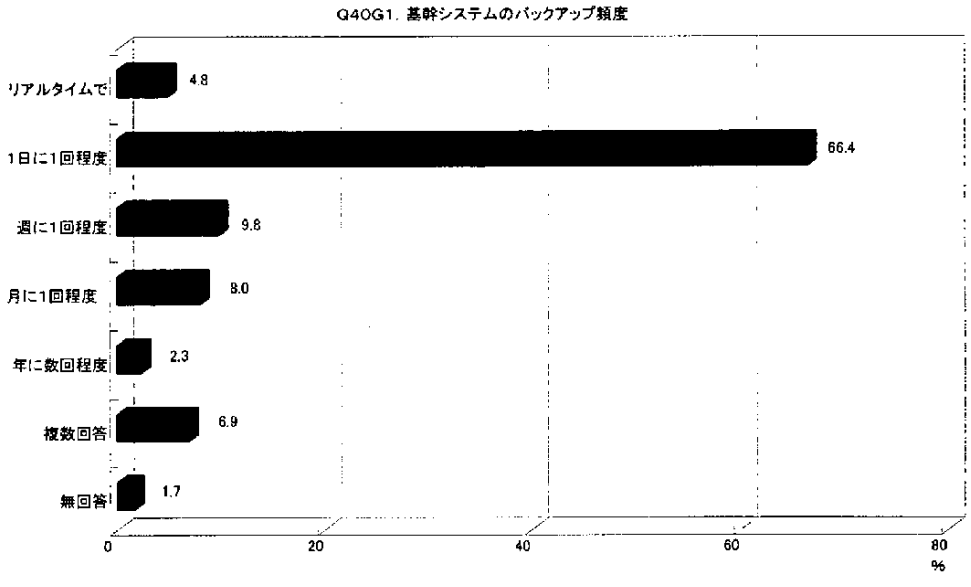
ファイルのバックアップについて対策を講じない理由としては「コストがかかりすぎる」が66．7%と多い。また、「必要性を感じない」は前回調査では41．9%であったが、今回調査では25．9%と16．0ポイント減少している。

ファイルのバックアップの必要性については認識が強まりつつあるようだ。



Q40. 貴社の基幹システムはどれぐらいの頻度でファイル等のバックアップを実施していますか。

1	リアルタイムで	42	4.8
2	1日に1回程度	576	66.4
3	週に1回程度	85	9.8
4	月に1回程度	69	8.0
5	年に数回程度	20	2.3
複数回答		60	6.9
無回答		15	1.7
計		867	100.0



前回調査同様、「毎日バックアップする」組織体が66．4%と多い。これは、ファイル等のバックアップの必要性、コストおよび情報システム運用上の関係からの結果であろう。

Q41. 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)

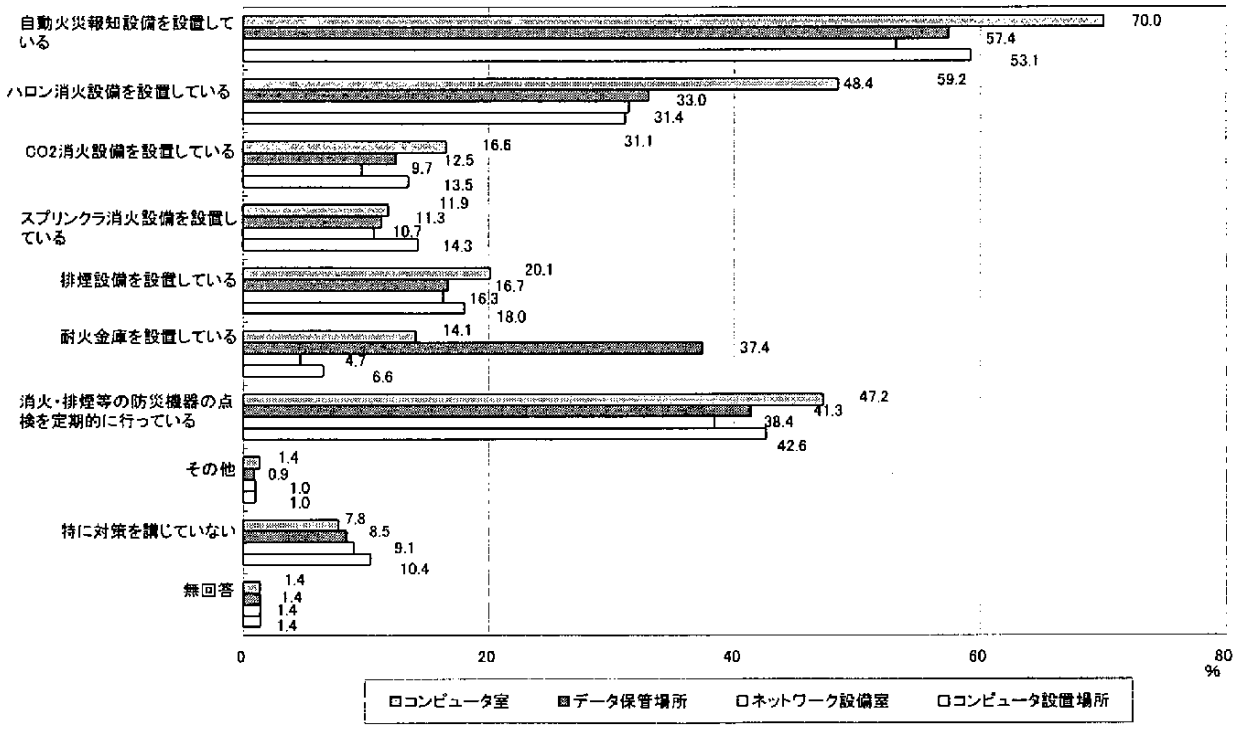
回答件数　867	コンピュータ室		データ保管場所		ネットワーク設備室		コンピュータ設置場所	
自動火災報知設備を設置している	607	70.0	498	57.4	460	53.1	513	59.2
ハロン消火設備を設置している	420	48.4	286	33.0	272	31.4	270	31.1
CO_2消火設備を設置している	144	16.6	108	12.5	84	9.7	117	13.5
スプリンクラ消火設備を設置している	103	11.9	98	11.3	93	10.7	124	14.3
排煙設備を設置している	174	20.1	145	16.7	141	16.3	156	18.0
耐火金庫を設置している	122	14.1	324	37.4	41	4.7	57	6.6
消火・排煙等の防災機器の点検を定期的に行っている	409	47.2	358	41.3	333	38.4	369	42.6
その他	12	1.4	8	0.9	9	1.0	9	1.0
特に対策を講じていない	68	7.8	74	8.5	79	9.1	90	10.4
無回答	12	1.4	12	1.4	12	1.4	12	1.4

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」であったが、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」組織体は少なく、各組織体とも何らかの対策を講じている。

災害対策としては、第一に火災対策であるとの認識が強く感じられる。

Q41G1. 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

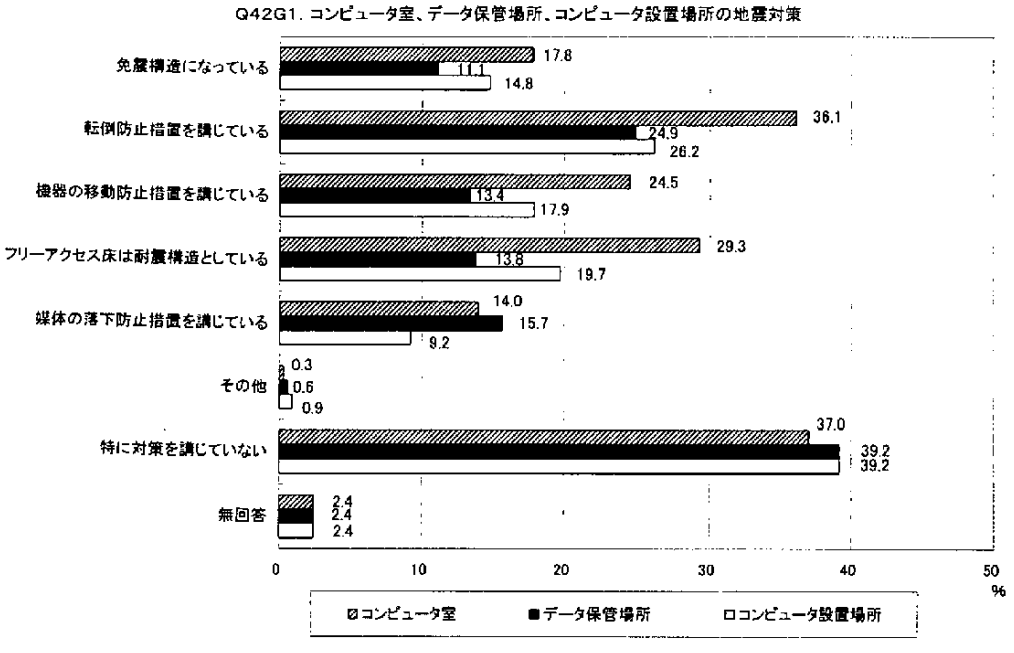


Q42. コンピュータ室、データ保管場所、コンピュータ設置場所ではどのような地震対策をとっていますか。各場所ごとに実施している対策を選んで下さい。(複数回答)

回答件数　867	コンピュータ室		データ保管場所		コンピュータ設置場所	
免震構造になっている	154	17.8	96	11.1	128	14.8
転倒防止措置を講じている	313	36.1	216	24.9	227	26.2
機器の移動防止措置を講じている	212	24.5	116	13.4	155	17.9
フリーアクセス床は耐震構造としている	254	29.3	120	13.8	171	19.7
媒体の落下防止措置を講じている	121	14.0	136	15.7	80	9.2
その他	3	0.3	5	0.6	8	0.9
特に対策を講じていない	321	37.0	340	39.2	340	39.2
無回答	21	2.4	21	2.4	21	2.4

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」を講じている組織体が多い。

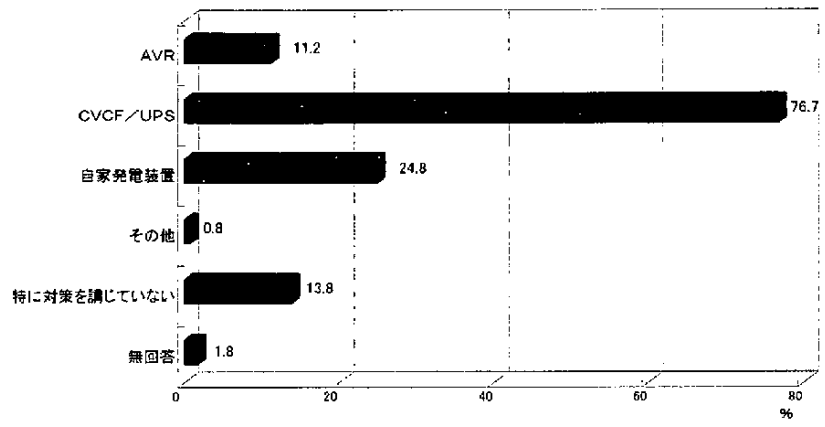
一方、「対策を講じていない」組織体は、コンピュータ室37．0%、データ保管場所39．2%、コンピュータ設置場所39．2%といずれも多く、火災対策から比べると地震対策はまだまだである。大規模な地震が各地で起こっているが、火災ほど身近には感じられていないようだ。



Q43. 電源設備の災害対策として、次のどの対策をとっていますか。(複数回答)

回答件数		867	
1	AVR	97	11.2
2	CVCF／UPS	665	76.7
3	自家発電装置	215	24.8
4	その他	7	0.8
5	特に対策を講じていない	120	13.8
無回答		16	1.8

Q43G1. 電源設備の災害対策



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」(76．7%)が多く、前回(48．7%)より28．0ポイント増加している。

また、「対策を講じていない」組織体は前回調査(23．7%)から比べると9．9ポイント減少して13．8%となっている。電源設備の災害対策の必要性は高まりつつある。

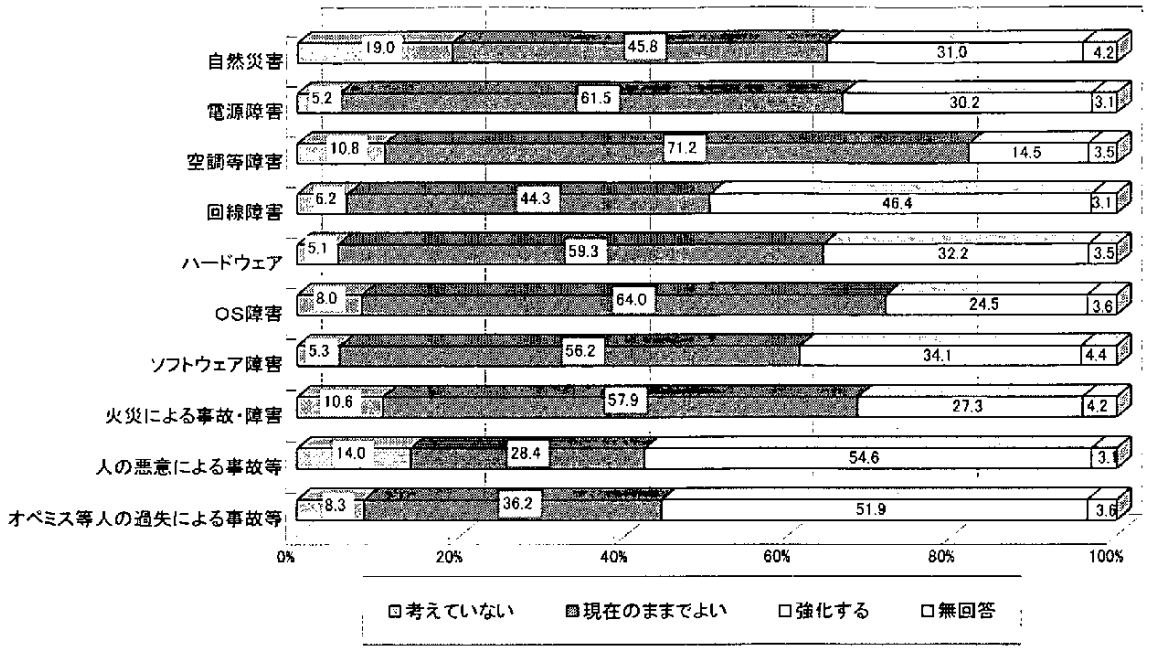
Q44. 情報システム、ネットワーク室、機器の災害・障害等の対策について、今後の方向性を原因別にみた場合、今後の考え方欄の該当する番号に○印をつけて下さい。

原　因	自然災害		電源障害		空調等障害		回線障害	
考えていない	165	19.0	45	5.2	94	10.8	54	6.2
現在のままでよい	397	45.8	533	61.5	617	71.2	384	44.3
強化する	269	31.0	262	30.2	126	14.5	402	46.4
無回答	36	4.2	27	3.1	30	3.5	27	3.1
計	867	100.0	867	100.0	867	100.0	867	100.0

原　因	ハードウェア		OS障害		ソフトウェア障害		火災による事故・障害	
考えていない	44	5.1	69	8.0	46	5.3	92	10.6
現在のままでよい	514	59.3	555	64.0	487	56.2	502	57.9
強化する	279	32.2	212	24.5	296	34.1	237	27.3
無回答	30	3.5	31	3.6	38	4.4	36	4.2
計	867	100.0	867	100.0	867	100.0	867	100.0

原　因	人の悪意による事故等		オペミス等人の過失による事故等	
考えていない	121	14.0	72	8.3
現在のままでよい	246	28.4	314	36.2
強化する	473	54.6	450	51.9
無回答	27	3.1	31	3.6
計	867	100.0	867	100.0

Q44G1. 情報システム、ネットワーク室、機器の災害・障害対策に関する今後の方向性.



全体的にみて、現状で満足している傾向にあるが、「回線障害」についてはさらに対策の「強化」を考えている組織体が若干ではあるが増加している。

また、「人による悪意」、「過失対策」については、さらに「強化」を考えている組織体が50%を超えているが、これらは回線障害、人為的な障害が災害・障害対策上無視できないものになっているからである。

Q45. 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		867	
1	コストがかかりすぎる	699	80.6
2	要員に対する教育訓練がいきとどかない	204	23.5
3	要員に対して負担がかかりすぎる	244	28.1
4	対策を構築するノウハウが不足している	276	31.8
5	どこまでやれば良いのか基準が示されていない	367	42.3
6	要求に合致するもの(製品)がない	34	3.9
7	トップの理解が得られない	81	9.3
8	その他	6	0.7
9	特に問題はない	25	2.9
無回答		12	1.4

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」(80. 6%)である。

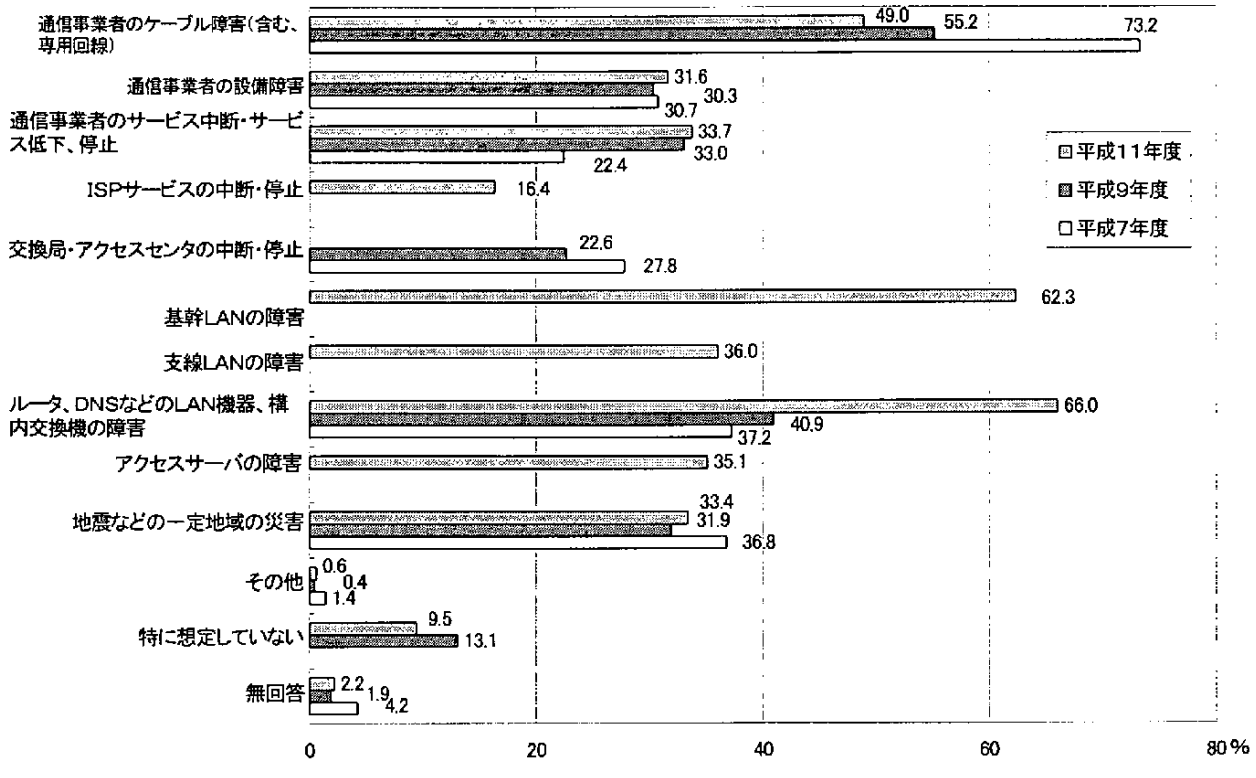
また、システム災害・障害対策はどこまでやればよいのか、基本線を設定することが難しく、その悩みが浮き彫りにされている。

この問題はQ35で述べたように、情報システムの資産価値をとらえ、また、不幸にして災害・障害が現実のものとなった場合の経営に与える影響を予測しておかなければ、組織体はシステム災害・障害にどの程度のコストをかけたらよいかの意思決定はなかなかできなくなる。

Q46. 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		867	
1	通信事業者のケーブル障害(含む、専用回線)	425	49.0
2	通信事業者の設備障害	274	31.6
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	292	33.7
4	ISP(ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ)サービスの中断・停止	142	16.4
5	基幹LANの障害	540	62.3
6	支線LANの障害	312	36.0
7	ルータ、DNSサーバなどのLAN機器(構内交換機を含む)の障害	572	66.0
8	アクセスサーバの障害	304	35.1
9	地震などの一定地域の災害	290	33.4
10	その他	5	0.6
11	特に想定していない	82	9.5
無回答		19	2.2

Q46G1. 想定するネットワーク障害の内訳



想定されるネットワーク障害としては、平成7年度、9年度調査ともに「通信ケーブル障害」がトップとなっていた。しかし、11年度調査では、新たに設置した「LAN関連の項目」、「ルータ、DNSサーバなどのLAN機器」(平成7、9年度は「構内交換機」と比較)、「基幹LANの障害」が飛び抜けている。すなわち、組織体内のネットワーク化が進み、外部との接続にもまして、内部のネットワーク障害が業務に与える影響が大きくなってきたものといえよう。また、通信ケーブル障害の割合が平成7年度、9年度、11年度と年々減少している。これは、通信事業者が競争の中で通信ケーブル関係の信頼度

を重視しているためと考えられる。「地震などの一定地域の災害」、「通信事業者の設備障害」などには大きな変化はない。

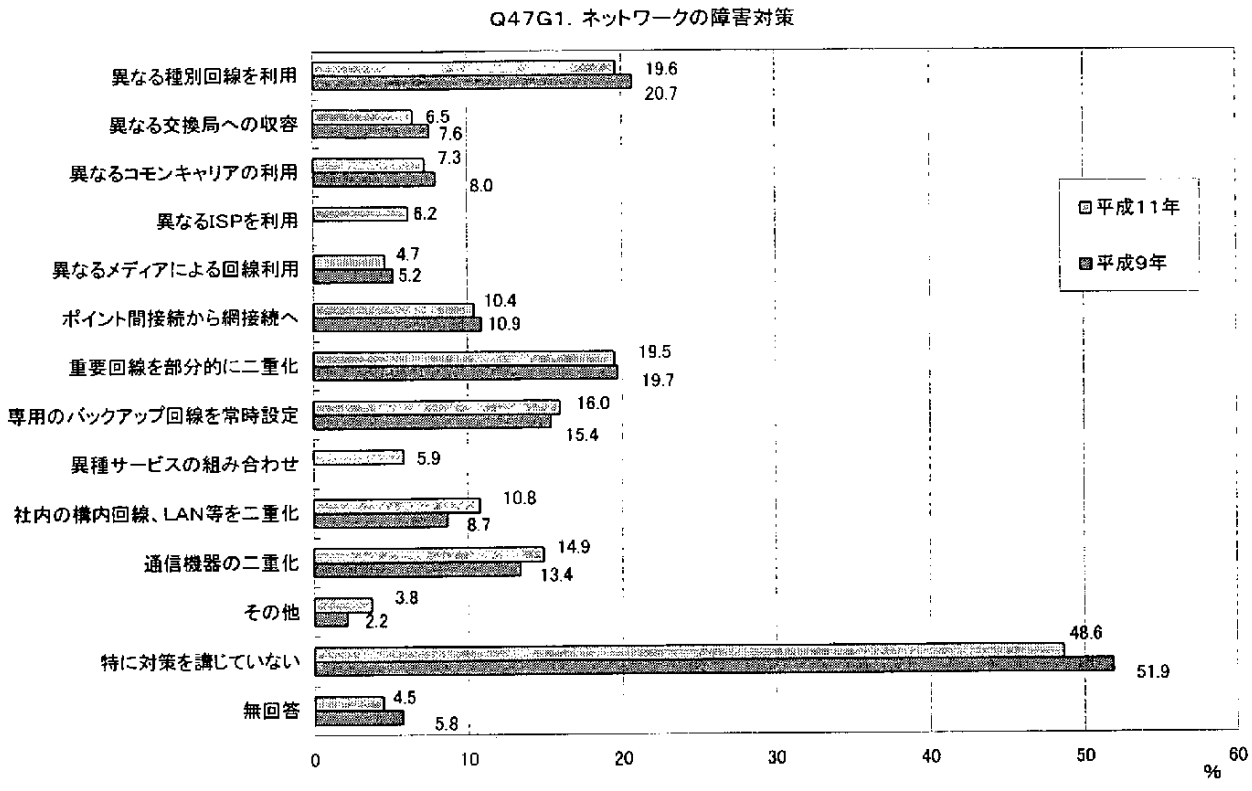
業種別にみると、金融・保険業では「通信事業者のケーブル障害」(78．0%)、「通信事業者の設備障害」(53．8%)、「通信事業者のサービス中断」(52．7%)による広域通信での障害想定の割合が大きく、「ルータ・DNSなどのLAN機器の障害」(54．9%)、「基幹LANの障害」(52．7%)などLANや構内のネットワークの障害想定の割合は小さい。一方、情報処理サービスでは「通信事業者のケーブル障害」(44．9%)、「通信事業者の設備障害」(25．8%)、「通信事業者のサービス中断」(27．0%)と広域通信の障害想定の割合は小さいが、「ルータ・DNSなどのLAN機器の障害」(70．8%)、「基幹LANの障害」(59．6%)などLANや構内のネットワークの障害想定は大きい。また、「ISPのサービスの中断」の想定がもっとも高く(20．2%)、いち早くインターネットを活用している状況がうかがえる。情報処理サービスほどではないものの、電気・一般・輸送・精密機械や公共サービスでも同様の傾向を示している。

また、企業規模(資本金、従業員数)や情報化投資額との比較でみると、大企業ほどケーブル災害などの広域通信の災害を想定する割合が高くなっている。

Q47. ①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。(複数回答)

②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

回答件数　867		実施対策		満足している		問題がある		どちらともいえない		無回答	
1	異なる種別回線を利用	170	19.6	81	47.6	31	18.2	53	31.2	5	2.9
2	異なる交換局への収容	56	6.5	24	42.9	12	21.4	18	32.1	2	3.6
3	異なるコモンキャリアの利用	63	7.3	26	41.3	12	19.0	25	39.7	0	0.0
4	異なるISP(ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ)を利用	54	6.2	17	31.5	14	25.9	23	42.6	0	0.0
5	異なるメディアによる回線利用(例:衛星回線等)	41	4.7	13	31.7	8	19.5	19	46.3	1	2.4
6	ポイント間接続から網接続へ	90	10.4	49	54.4	13	14.4	25	27.8	3	3.3
7	重要回線を部分的に二重化	169	19.5	80	47.3	36	21.3	45	26.6	8	4.7
8	専用のバックアップ回線を常時設定	139	16.0	73	52.5	28	20.1	27	19.4	11	7.9
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	51	5.9	17	33.3	10	19.6	22	43.1	2	3.9
10	社内の構内回線、LAN等を二重化	94	10.8	34	36.2	25	26.6	33	35.1	2	2.1
11	通信機器(CCU、ルータ、DNSサーバ、アクセスサーバ等)の二重化	129	14.9	43	33.3	38	29.5	41	31.8	7	5.4
12	その他	33	3.8	8	24.2	11	33.3	11	33.3	3	9.1
13	特に対策を講じていない	421	48.6								
無回答		39	4.5								

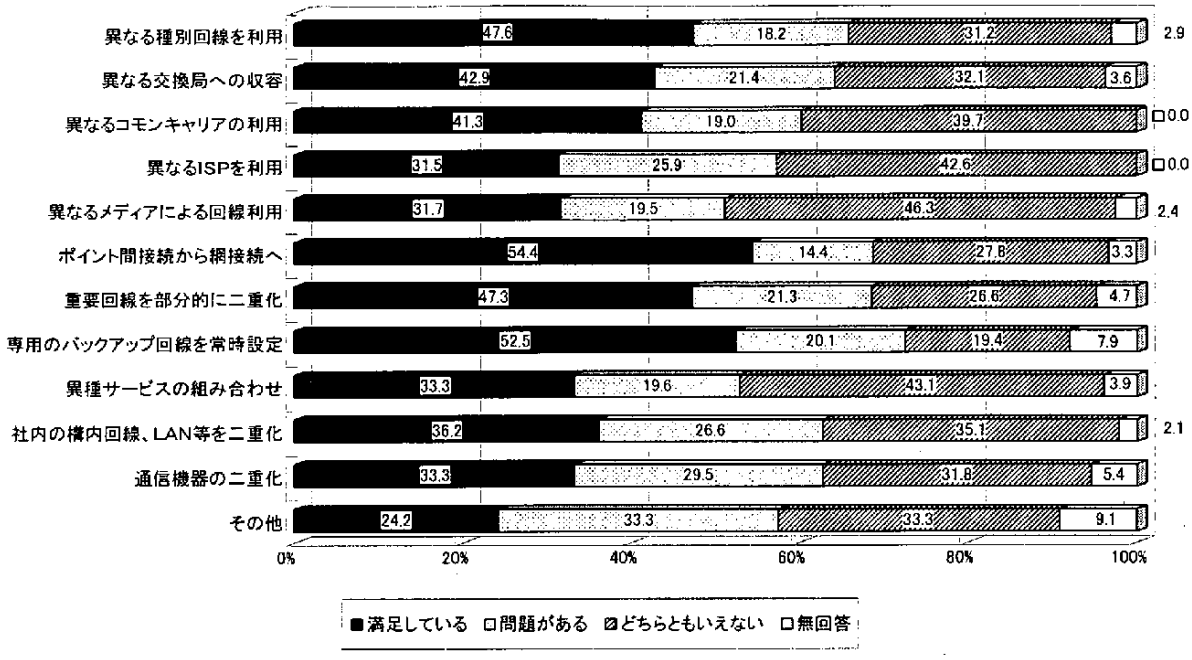


全体的な傾向は前回調査とほぼ同様である。ネットワーク障害対策については、前回調査の51．9%に比べて3．3ポイント減少したものの、依然として半数に近い組織体が対策を立てていない。対策としては、「異なる種別回線を利用」、「重要回線を部分的に二重化」、「専用のバックアップ回線を常時設定」を約15%～20%の組織体が採用している。また、組織体内の「通信機器の二重化」が前回調査と比べて増加している。これは、組織体のネットワーク化が進んでいるため、組織体内のネットワーク障害に対しても対策が必要となっているためと考えられる。また、インターネットの利用が進んだことから、「複数ISPを利用」する割合が、「異なるコモンキャリアの利用」、「異なる交換局の収容」とほぼ同程度となっている。今後、組織体のインターネット利用が進むにつれ、複数のISPとの接続が重要になると考えられる。

ネットワーク障害対策への満足度は、「ポイント間接続から網接続」と「専用のバックアップ回線を常時設定」が50%を超えて強く支持されている。「異なる種別回線を利用」、「重要回線を部分的に二重化」、「異なる交換局への収容」、「異なるコモンキャリアへの収容」の満足度が40%を超えているが、それ以外の項目については、前回調査に比べると満足度は低下している。各組織体ともさまざまな対策を行っているものの、「コストがかかる」、「専門家が必要」などまだまだ問題が大きいことがわかる。通信事業者やインターネットのサービスプロバイダは、今後インターネットの利用が進むなかで、ユーザに支持されるコスト、使い勝手のよさの点から新しいサービスの提供などを考えていく必要がある。

業種別にみると、満足度の高い障害対策がそれぞれ異なっているが、概ね、大企業（資本金、情報化投資額別）ほど満足度は高い。これは、必要に応じてリスクを低減するために投資を行っているものと考えられる。なお、「通信機器（CCU、ルータ、DNSなど）のLAN機器の二重化」に関する満足度では、企業規模との相関関係はあまりみられない。すなわち、これはLAN機器などの障害が多く、通信事業者の高信頼なネットワークに慣れた大企業でも投資という形でのリスク軽減が難しく、戸惑いがみられるように思う。今後、LAN機器などの通信機器の高信頼化が望まれる。

Q47G2. ネットワーク障害対策への満足度

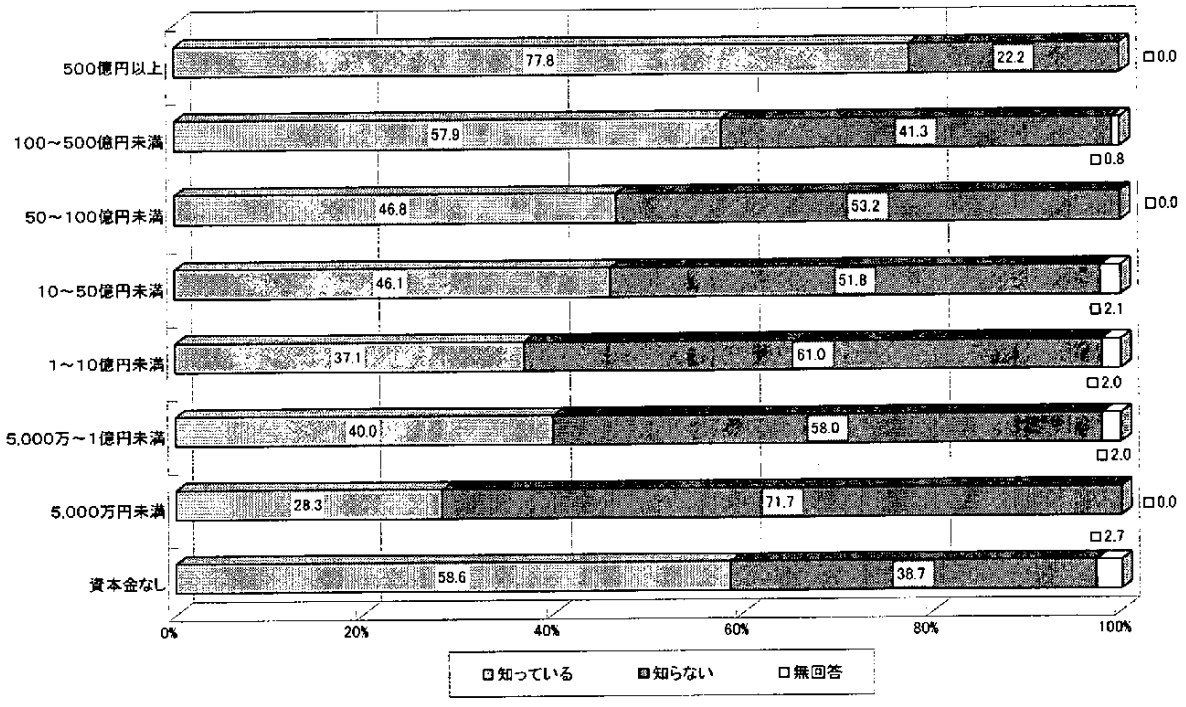


2．6　不正アクセス対策・不正侵入対策について

Q48．平成 12 年2月施行予定の「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	411	47.4
2	知らない	443	51.1
無回答		13	1.5
計		867	100.0

Q48G1．不正アクセス禁止法の認知度（資本金別）



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」のは約半数にとどまっている。

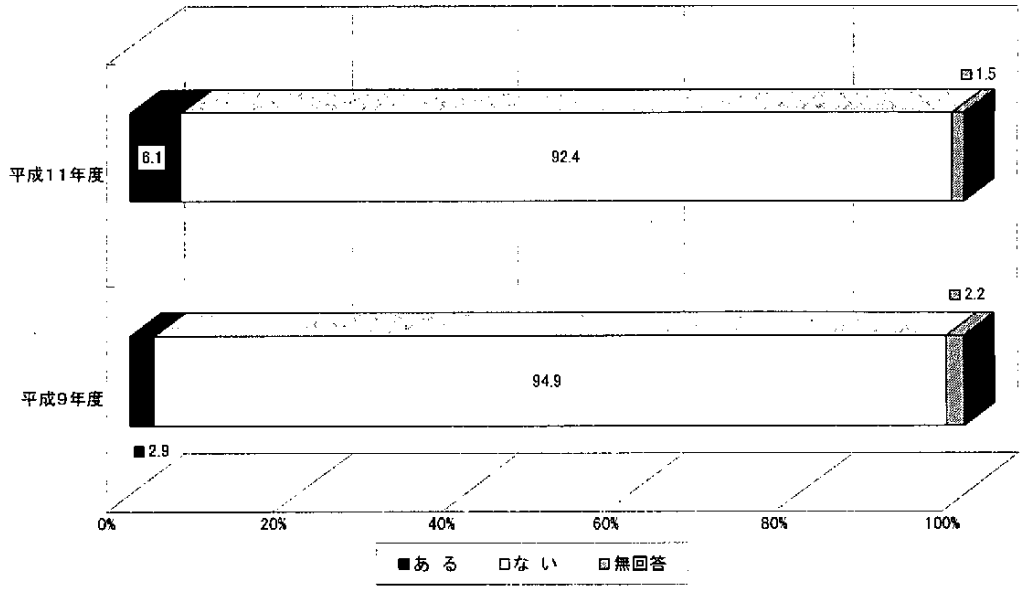
企業規模（資本金、従業員数）などでみると、規模の大きな組織体ほど存在を「知っている」とする割合が増加する傾向にある。

Q49．貴社では過去1年間（平成10年1月～12月）に不正アクセスの被害に遇われたことがありますか。

1	あ る	53	6.1
2	な い	801	92.4
無回答		13	1.5
計		867	100.0

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、前回調査時点と比較すると、2．9%から6．1%へと3．2ポイント増加しており、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る。

Q49G1. 過去1年間の不正アクセス被害状況



Q50. 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。(Q49の「1」を回答)

1	出した	11	20.8
2	出さない	40	75.5
無回答		2	3.8
計		53	100.0

IPAに被害届を出す組織体は約2割にとどまり、前回調査(15.6%)と比較して若干増加したものの、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57.1%あることと比べると、やや少ない回答率である。

Q51. 不正アクセスの被害にあたり、JPCERT/CC(コンピュータ緊急対応センター)に相談しましたか。(Q49の「1」を回答)

1	した	7	13.2
2	しない	44	83.0
無回答		2	3.8
計		53	100.0

不正アクセスの被害にあった組織体のうち、JPCERT/CCに相談したのは13.2%にとどまっている。Q3において、不正アクセスに関するJPCERT/CCの活動を「知っている」という回答が全体の約3割にとどまっていることも影響していると思われる。

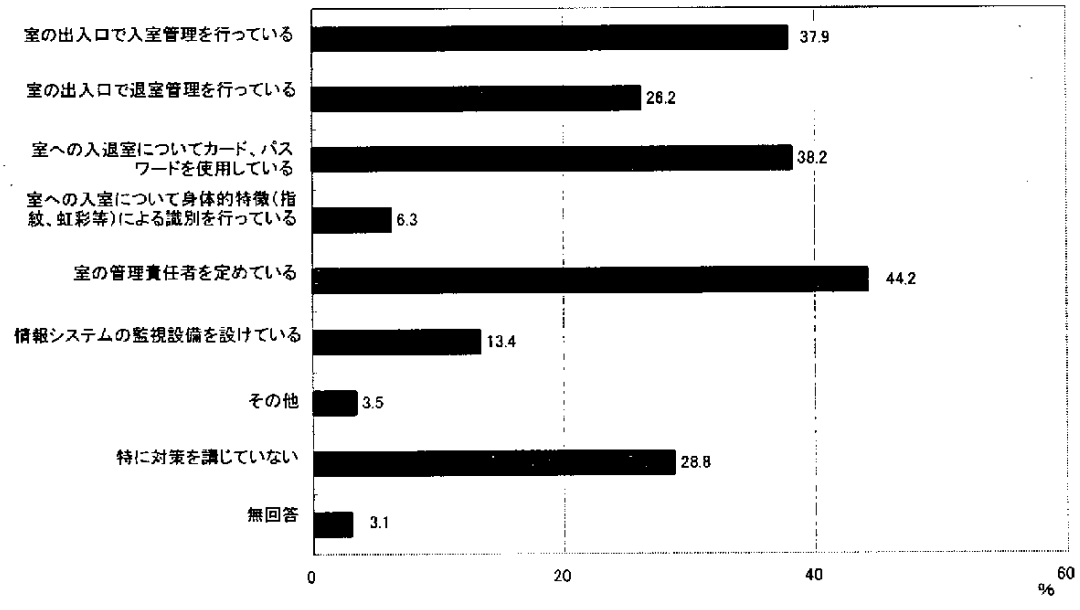
Q52. ①主要なネットワーク室や機器、コンピュータ室またはデータ保管室での不正アクセス対策はどのようなものですか。実施している対策を選んで下さい。(複数回答)

②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

回答件数　867		実施対策		満足している		問題がある		どちらともいえない		無回答	
1	室の出入口で入室管理を行っている	329	37.9	183	55.6	54	16.4	86	26.1	6	1.8
2	室の出入口で退室管理を行っている	227	26.2	132	58.1	32	14.1	59	26.0	4	1.8
3	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	331	38.2	205	61.9	49	14.8	69	20.8	8	2.4
4	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	55	6.3	16	29.1	9	16.4	30	54.5	0	0.0
5	室の管理責任者を定めている	383	44.2	193	50.4	55	14.4	115	30.0	20	5.2
6	情報システムの監視設備を設けている	116	13.4	63	54.3	21	18.1	32	27.6	0	0.0
7	その他	30	3.5	7	23.3	3	10.0	15	50.0	5	16.7
8	特に対策を講じていない	250	28.8								
無回答		27	3.1								

(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。

Q52G1. 不正アクセス対策の実施状況

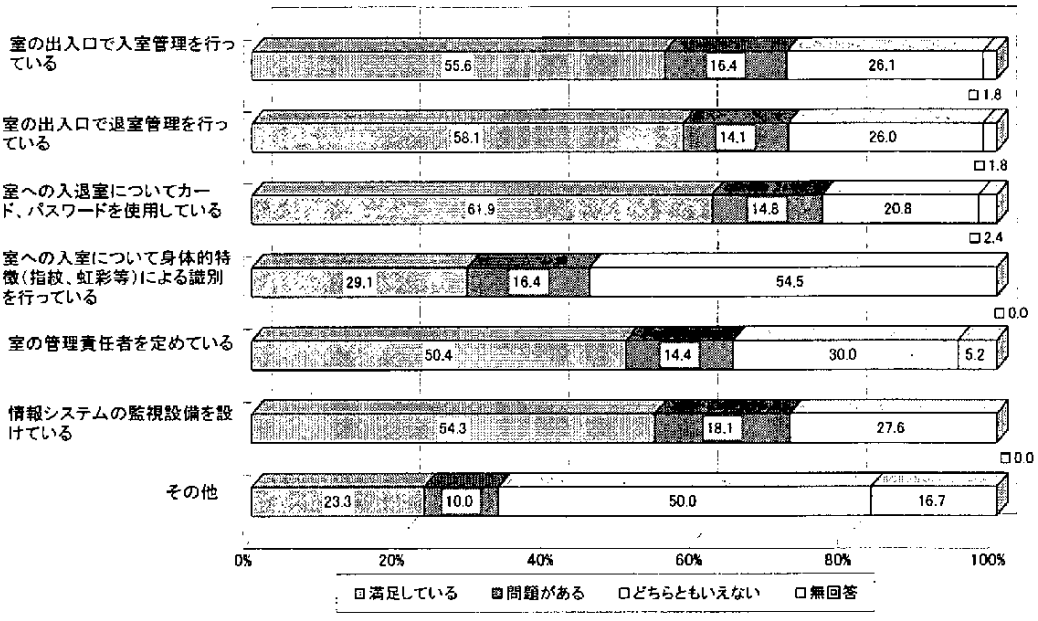


不正アクセス対策として、約4割の組織体が「管理責任者の設置」、「入室管理」、「カード・パスワードの利用」を実施している。

「入室管理」を実施していると回答した組織体は37．9%であるのに比べ、「退室管理」を実施していると回答したのは26．2%にとどまっている。また、「監視設備の設置」や「身体的特徴による識別」を行っている組織体は、全体の中でも1割前後であり、より高度な不正アクセス対策を実施している組織体は現時点では少数である。

満足度に関しては、おおむね「満足している」という回答が多い。ただし、「身体的特徴による識別」に関しては「どちらともいえない」という回答が半数を超え、「満足している」という回答は約3割にとどまっている。

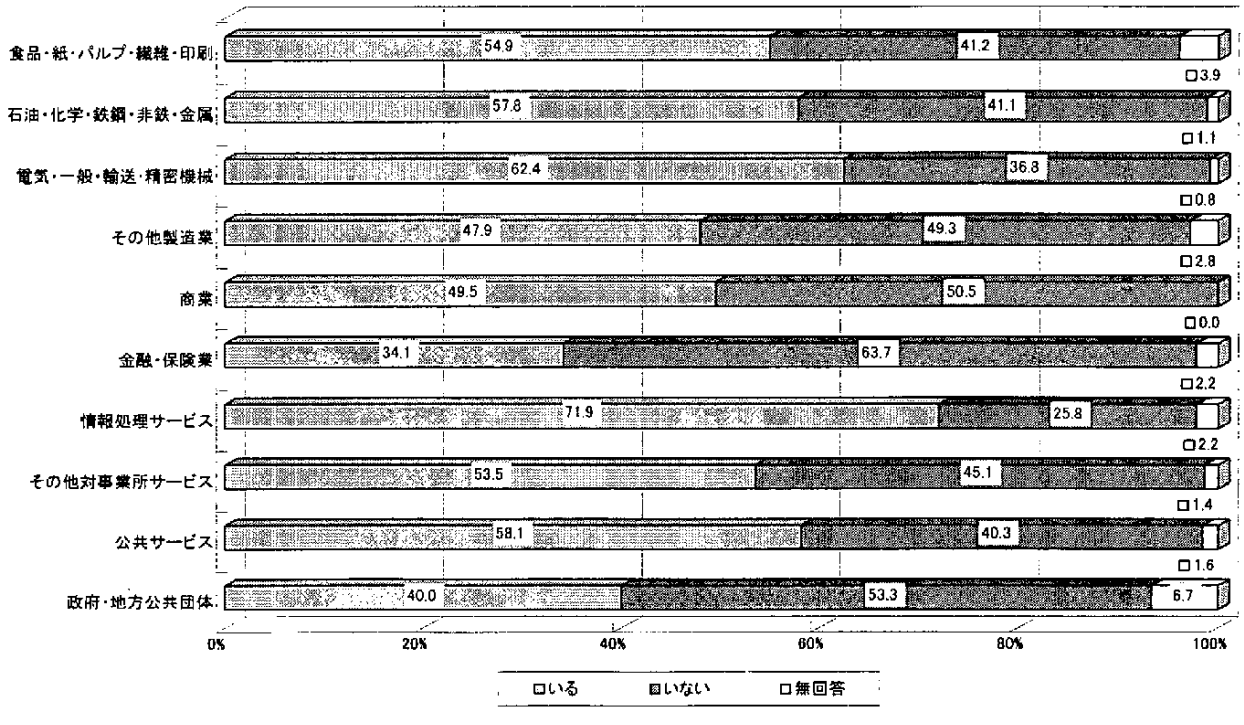
Q52G2. 不正アクセス対策の満足度



Q53. 貴社ではリモートアクセスを行っていますか。

1	い る	467	53.9
2	いない	384	44.3
無回答		16	1.8
計		867	100.0

Q53G1. リモートアクセスの実施状況(業種別)



約半数の組織体がリモートアクセスを実施していると回答している。

業種別にみると、情報処理サービスにおいて高い実施率（71．9%）がみられたが、金融・保険業（34．1%）、政府・地方公共団体（40．0%）においては比較的低い実施率であった。

Q54. 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	230	26.5
2	いない	619	71.4
無回答		18	2.1
計		867	100.0

機密度のランクを「設定している」という割合は26．5%であり、平成9年度調査（29．5%）が7年度（10．5%）から大きな伸びをみせたのと比べるとほぼ横ばいとなっている。

業種別にみると、情報処理サービスが44．9%と平均を大きく上回る割合を示している。また、資本金別では、資本金500億円を超える組織体の割合が44．4%と高い。

Q55. ①ネットワークを介しての不正アクセスに対して講じている対策は何ですか。実施している対策を選んで下さい。（複数回答）

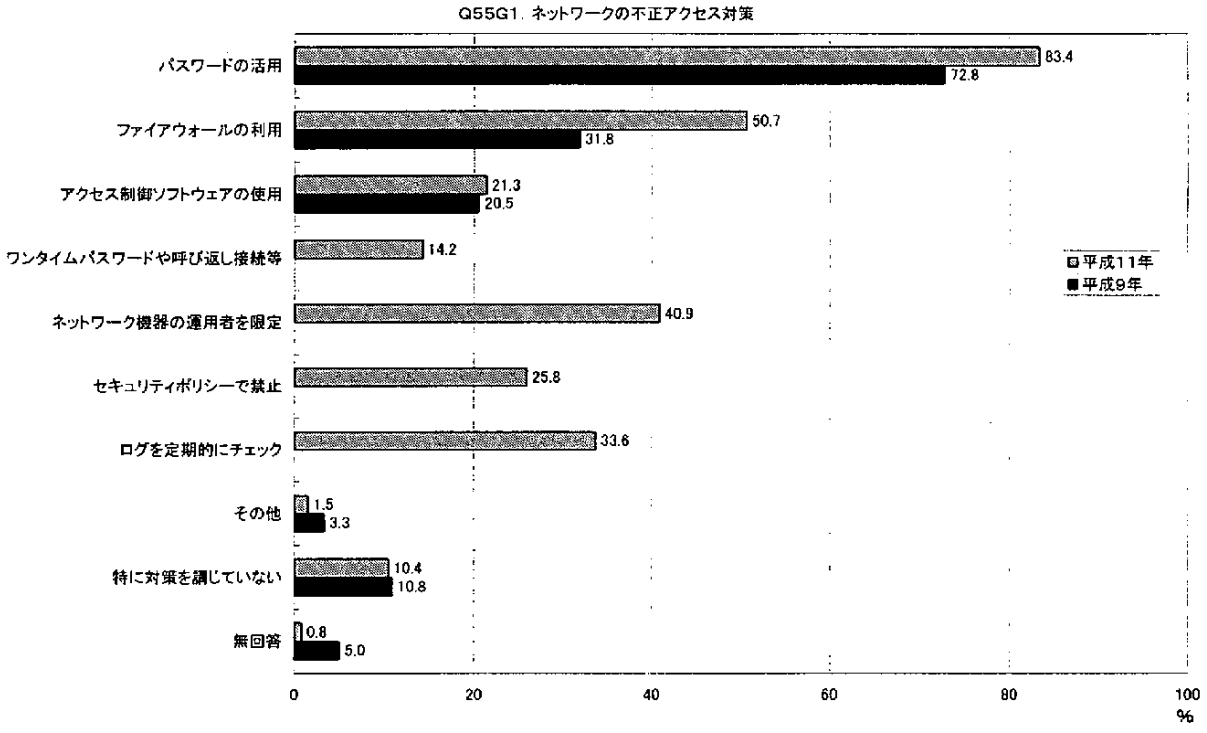
②また、その対策で不正アクセスは防止できると思いますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

回答件数 867		実施体制		満足している		問題がある		どちらともいえない		無回答	
1	パスワードの活用	723	83.4	249	34.4	215	29.7	231	32.0	28	3.9
2	ファイアウォールの利用	440	50.7	248	56.4	61	13.9	109	24.8	22	5.0
3	アクセス制御ソフトウェアの使用	185	21.3	114	61.6	21	11.4	43	23.2	7	3.8
4	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	123	14.2	83	67.5	10	8.1	27	22.0	3	2.4
5	ネットワーク機器の運用者（アクセス範囲）を限定	355	40.9	196	55.2	51	14.4	99	27.9	9	2.5
6	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	224	25.8	96	42.9	54	24.1	70	31.3	4	1.8
7	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	291	33.6	134	46.0	62	21.3	86	29.6	9	3.1
8	その他	13	1.5	7	53.8	1	7.7	2	15.4	3	23.1
9	特に対策を講じていない	90	10.4								
無回答		7	0.8								

ネットワークを介して不正アクセスに講じている対策としては、平成9年度調査に比べて「パスワードの活用」が特に増加し、83．4%に達している。しかし、まだ約16%がパスワードを利用しておらず、不正アクセスに対するガードが甘いといえよう。また、組織体のインターネット利用が増加し、「ファイ

アウォールの利用」が9年度調査に比べて18．9ポイント向上し、50．7%となっている。今後、組織体がインターネットを用いた電子商取引やイントラネット、エクストラネットを用いた調達などオープンなネットワークにかかわる機会がますます増えると考えられ、「ファイアウォール」の採用が今後も増加すると考えられる。11年度調査で加えた新しい調査項目については、「ネットワーク機器の運用者の限定」や、「ログの定期的なチェック」など、30%を超える組織体が採用しており、不正アクセスに対する対策が複合的に行われていることがわかる。

一方、パスワードによる強固なものとする「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に対しては他の対策に比べて採用は低い。今後、企業外から企業のサーバなどにアクセスするアプリケーションが増加するのに伴い、これらの対策も増加するものと考えられる。

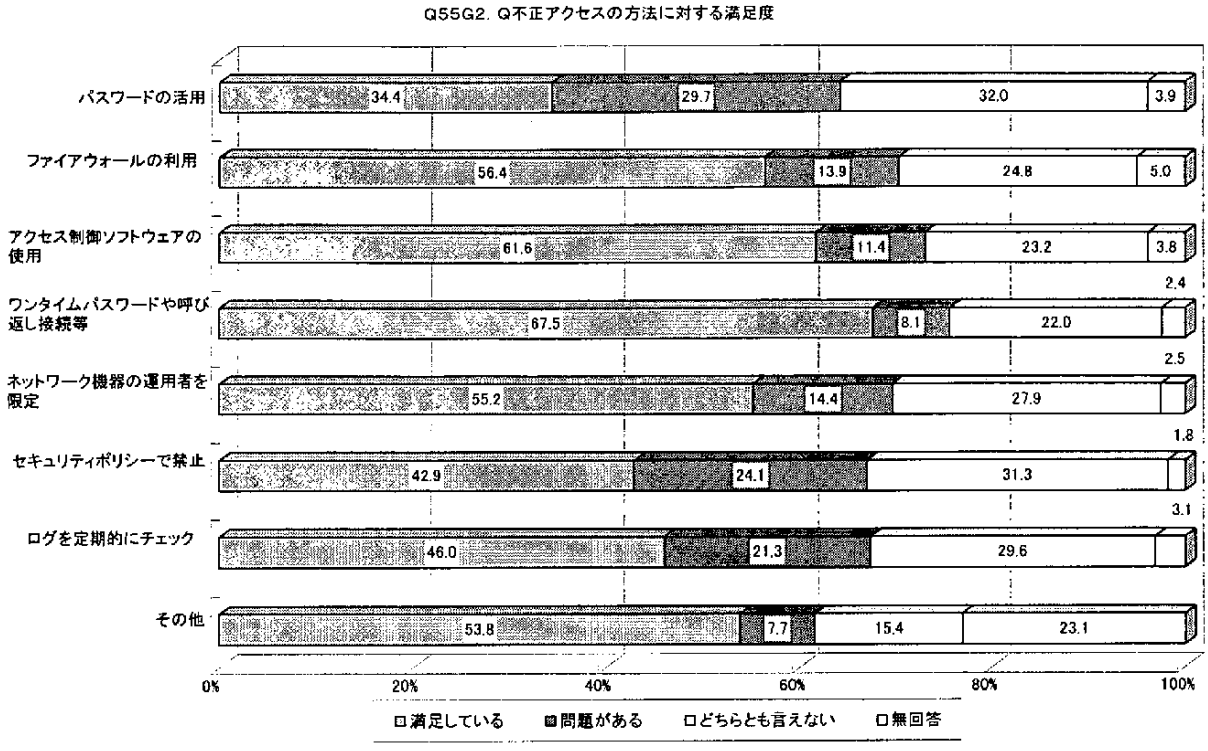


業種別にみると、情報処理サービス(92．1%)、公共サービス(90．3%)、金融・保険業(87．9%)が「パスワード」を活用している。「ファイアーウォール」は、情報処理サービスが71．9%と飛びぬけている。「ネットワーク機器の運用者の限定」では、情報処理サービス58．4%、その他対事業所サービス44．4%、公共サービス43．5%となっている。

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よくない。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。

セキュリティポリシーでの制限については、全業種ともに採用されていない。しかし、セキュリティポリシーでアクセスや配線などLANにかかわる事項を管理するので、全業種とも今後重点的に取り組むテーマである。

パスワードは企業規模(資本金、従業員数)や情報化投資額が大きいほど採用が多く、1万人規模の従業員数の組織体では97．2%が採用している。同様の傾向が「ファイアウォール」、「ワンタイムパスワード」、「ネットワーク機器の運用者の限定」、「セキュリティポリシーによる禁止」にもみられる。



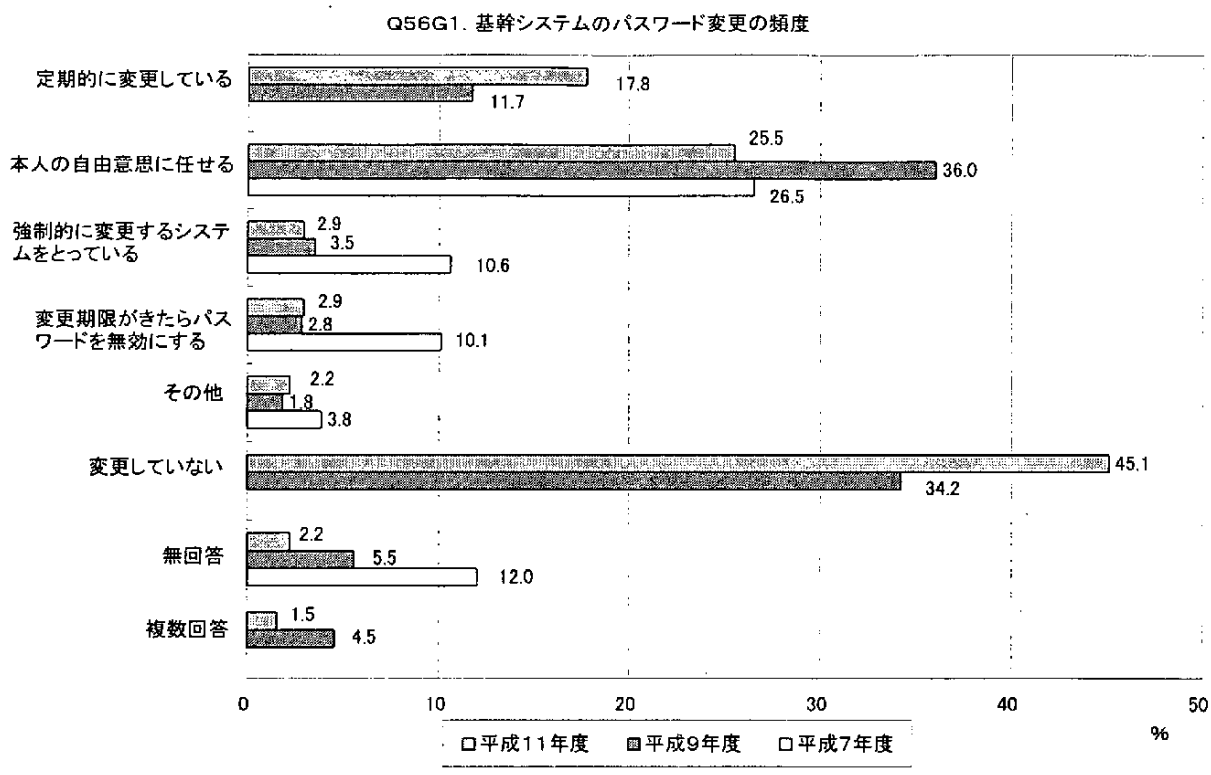
ネットワーク障害対策への満足度は、「ワンタイムパスワードや呼び返し接続等」の追加的コントロールがもっとも高く67．5%となっている。また、「アクセス制御ソフトの利用」、「ネットワーク機器の運用者の限定」、「ファイアウォールの利用」が50%を越えている。

一方、「パスワードの活用」、「ログの定期的なチェック」、「セキュリティポリシーでの禁止」などは50%以下となっており、使いやすいものとする工夫やツールなどが必要といえよう。

現在、パスワードに対しては、マシンごとに変えることや簡単に推察されないこと、定期的な変更などが義務づけられる一方で、ID＋パスワードによる認証の頻度が増えている。そのため、パスワードを覚えやすくしたり、同じものを使ったりと弊害が指摘されているが、これに十分に応えるものがない。今後、コンピュータ利用者が増えるなかで一般の人がより簡単に間違いなく使え、問題を起こさないサービスや技術開発が必要であろう。

Q56. 貴社では基幹システムのパスワードを変更していますか。

1	定期的に変更している	154	17.8
2	本人の自由意思に任せる	221	25.5
3	強制的に変更するシステムをとっている	25	2.9
4	変更期限がきたらパスワードを無効にする	25	2.9
5	その他	19	2.2
6	変更していない	391	45.1
複数回答		13	1.5
無回答		19	2.2
計		867	100.0



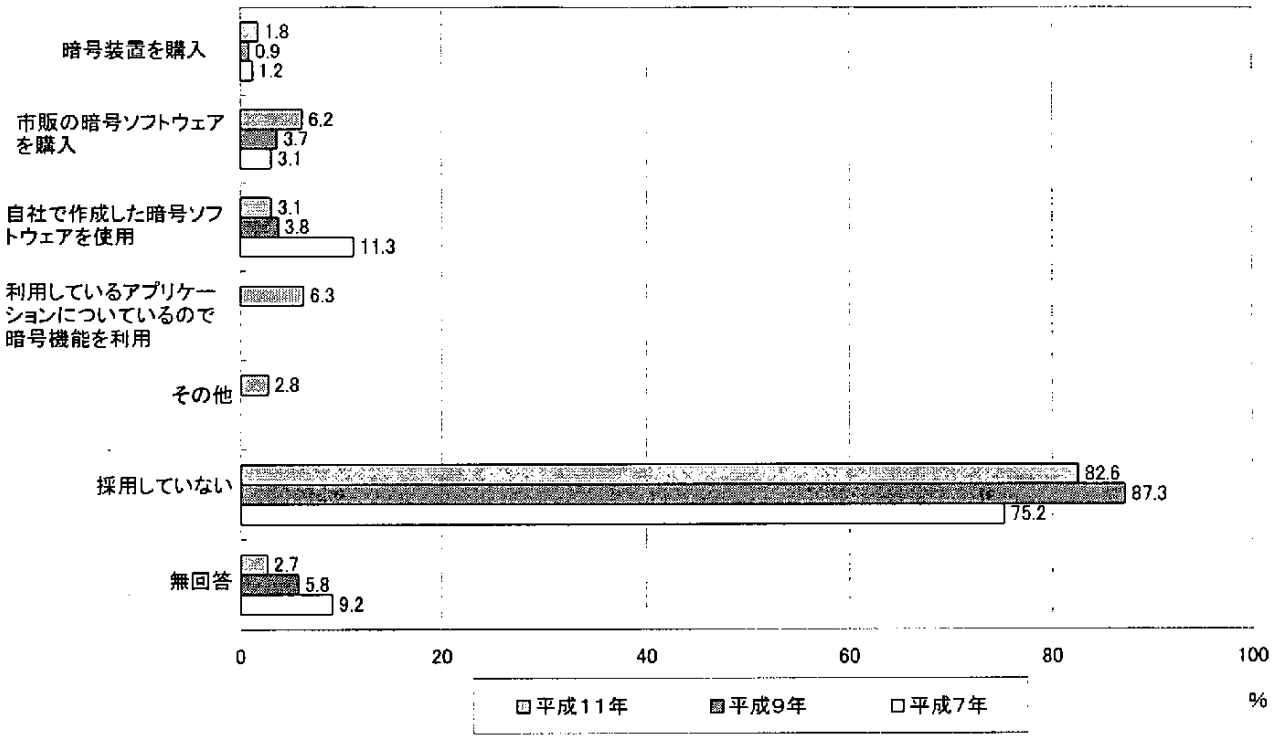
パスワード管理については、「変更していない」という回答が最も多く45．1%を占め、次いで「本人の自由意思に任せる」(25．5%)、「定期的に変更している」(17．8%)の順となっている。

平成9年度調査と比較して、「定期的に変更している」が、11．7%から17．8%に増加し、「本人の自由意思に任せる」が36．0%から25．5%に減少している。その一方で、「変更していない」は前回調査の34．2%から45．1%に増加している。「本人の自由意思に任せる」と「変更していない」をあわせた約7割の組織体においては、基幹システムにおけるパスワードの変更に関して明確なガイドラインを持たず、パスワードによる不正アクセス対策の有効性に関して問題を投げかける結果となった。

Q57. ①貴社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)
②また、現在採用している暗号に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

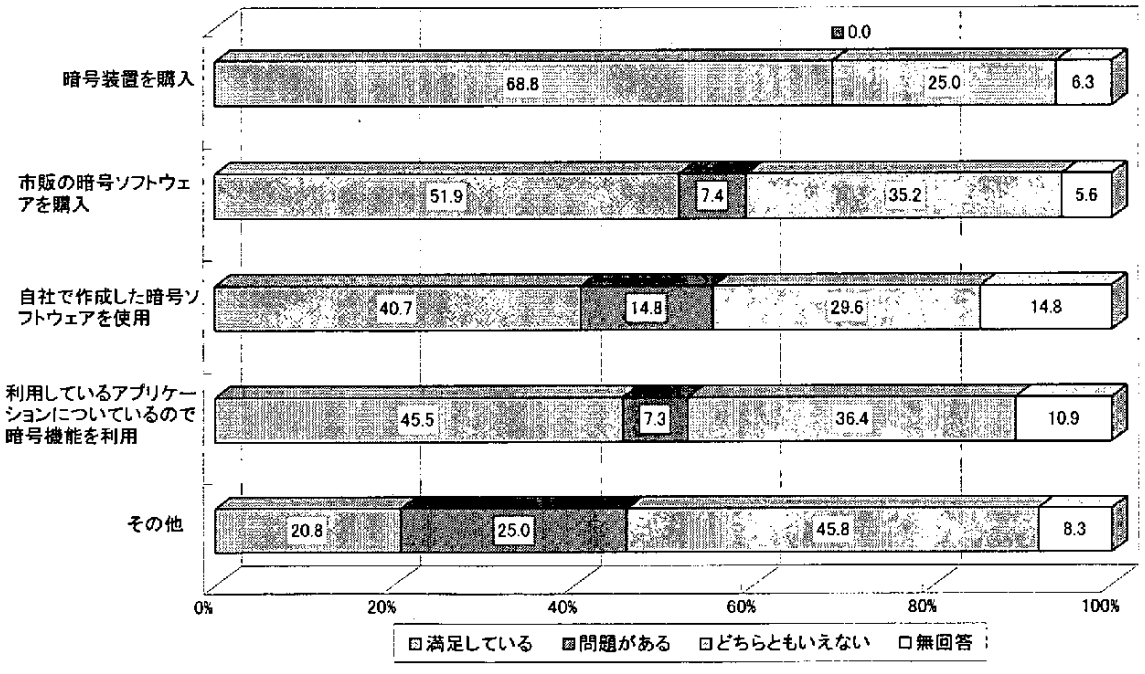
回答件数　867		暗号		満足している		問題がある		どちらともいえない		無回答	
1	暗号装置を購入	16	1.8	11	68.8	0	0.0	4	25.0	1	6.3
2	市販の暗号ソフトウェアを購入	54	6.2	28	51.9	4	7.4	19	35.2	3	5.6
3	自社で作成した暗号ソフトウェアを使用	27	3.1	11	40.7	4	14.8	8	29.6	4	14.8
4	利用しているアプリケーションについているので暗号機能を利用	55	6.3	25	45.5	4	7.3	20	36.4	6	10.9
5	その他	24	2.8	5	20.8	6	25.0	11	45.8	2	8.3
6	採用していない	716	82.6								
無回答		23	2.7								

Q57G1. 暗号の採用状況



暗号の採用については、まだほとんどの組織体で採用していないといえよう。これは、平成7年度、9年度調査と比べても変化しておらず、ネットワーク化が急速に進んでいるなかで、データ自体の保護を行うことが十分に考えられていない。そのなかでも、「市販の暗号化ソフトを利用」したり、「購入したソフトに組み込まれた形での暗号の利用」がみられる。今後、市販製品を中心に暗号の採用が進んでいくと考えられる。

Q57G2. 採用している暗号に対する満足度

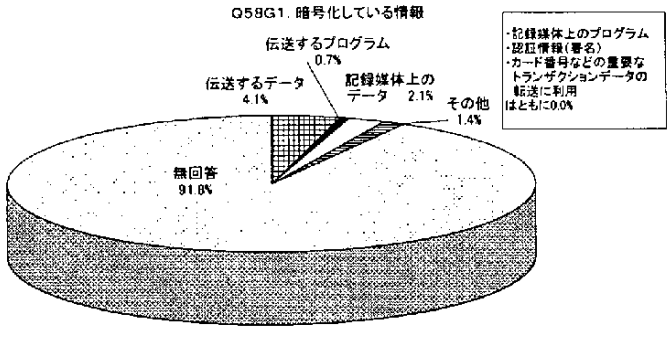


採用している暗号に対する満足度は、「暗号装置の購入」、「自社で作成した暗号ソフトウェアを使用」に関してはサンプル数が少ない。一方、「利用しているアプリケーションについているので暗号機能を利用」と「市販の暗号ソフトウェアを購入」に関してはサンプル数があるので、この2つについてのみコメントする。この2つともに45%～50%が満足しており、暗号によって安全が保証されていることがうかがえる。米国からの128ビットの暗号を採用した製品が輸入解禁されたのをきっかけに、今後暗号の採用を進めていく必要があるだろう。

Q58. 暗号化している情報は次のどれですか。(複数回答)(Q57 の「1」～「5」を回答)

回答件数		145	
1	伝送するデータ	6	4.1
2	伝送するプログラム	1	0.7
3	記録媒体上のデータ	3	2.1
4	記録媒体上のプログラム	0	0.0
5	認証情報(署名)	0	0.0
6	カード番号などの重要なトランザクションデータの転送に利用	0	0.0
7	その他	2	1.4
無回答		134	92.4

暗号化している情報の種類に関する質問であるが、有効回答数が12件と少なく、このままでは判断ができない。前回調査では、77件中71件の採用がみられたが、今回調査では上記のような結果となり、無回答が大勢を占めた。12件の内訳としてはデータ伝送で利用するのが多いようである。



Q59. 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。

1	定期的に実施している	14	1.6
2	社内教育用のセキュリティ教育カリキュラムを策定して実施している	26	3.0
3	計画書またはマニュアル類に従って実施している	70	8.1
4	その他	33	3.8
5	特に実施していない	707	81.5
複数回答		3	0.3
無回答		14	1.6
計		867	100.0

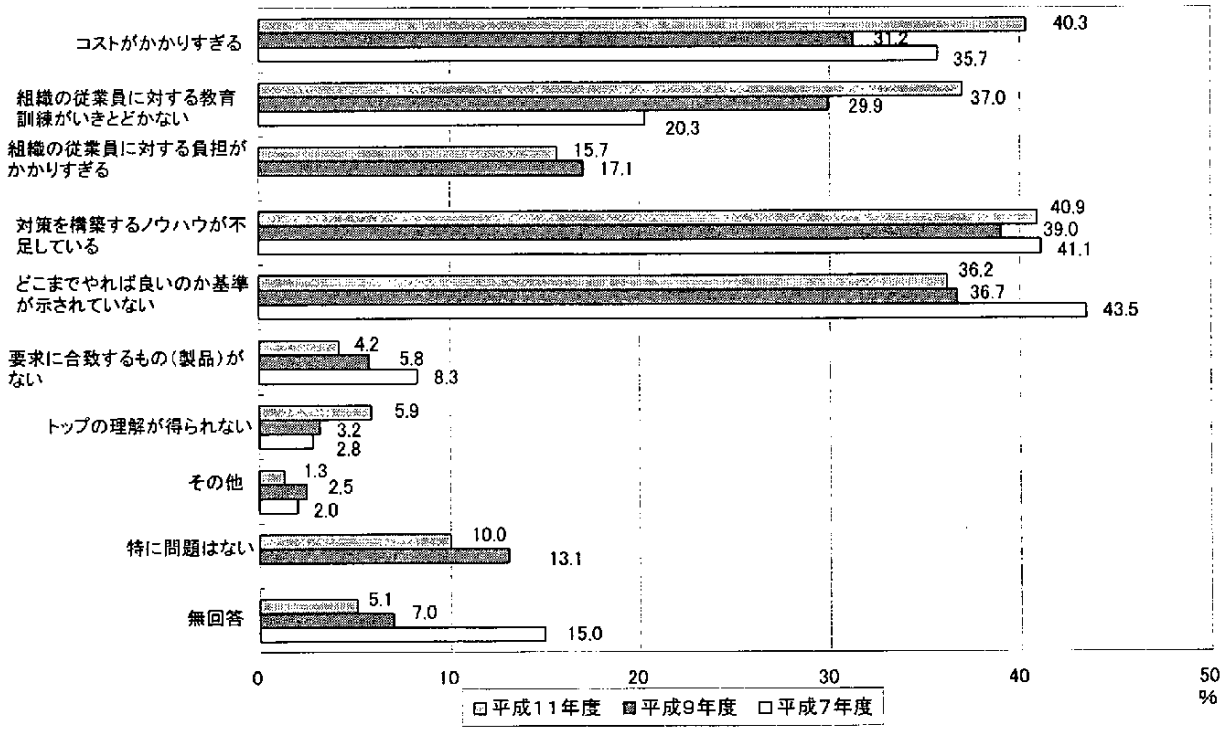
不正アクセスに対する教育・訓練については81．5%が「まったく行っていない」と回答している。Q17において「セキュリティガイドラインを定めている」という回答が27．9%であるのに比べ、何らかの「教育・訓練を実施している」という回答が16．5%にとどまっており、セキュリティガイドラインを定めている組織体においても、その実効性に関して疑問の残る結果となった。

Q60. 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		867	
1	コストがかかりすぎる	349	40.3
2	組織の従業員に対する教育訓練がいきとどかない	321	37.0
3	組織の従業員に対する負担がかかりすぎる	136	15.7
4	対策を構築するノウハウが不足している	355	40.9
5	どこまでやれば良いのか基準が示されていない	314	36.2
6	要求に合致するもの(製品)がない	36	4.2
7	トップの理解が得られない	51	5.9
8	その他	11	1.3
9	特に問題はない	87	10.0
無回答		44	5.1

不正アクセス対策に関しては、8割を超える回答者が何らかの問題の存在を指摘している。問題点として、「コストがかかりすぎる」(40. 3%)、「対策を構築するノウハウの不足」(40. 9%)、「教育訓練」(37. 0%)、「どこまでやればよいかの基準」(36. 2%)があげられる。前回調査と比較すると「教育訓練が行き届かない」が29. 9%から37. 0%に増加しているが、これは不正アクセス対策に力を入れ始めている組織体が増加している結果であると思われる。

Q60G1. 不正アクセス対策の問題点

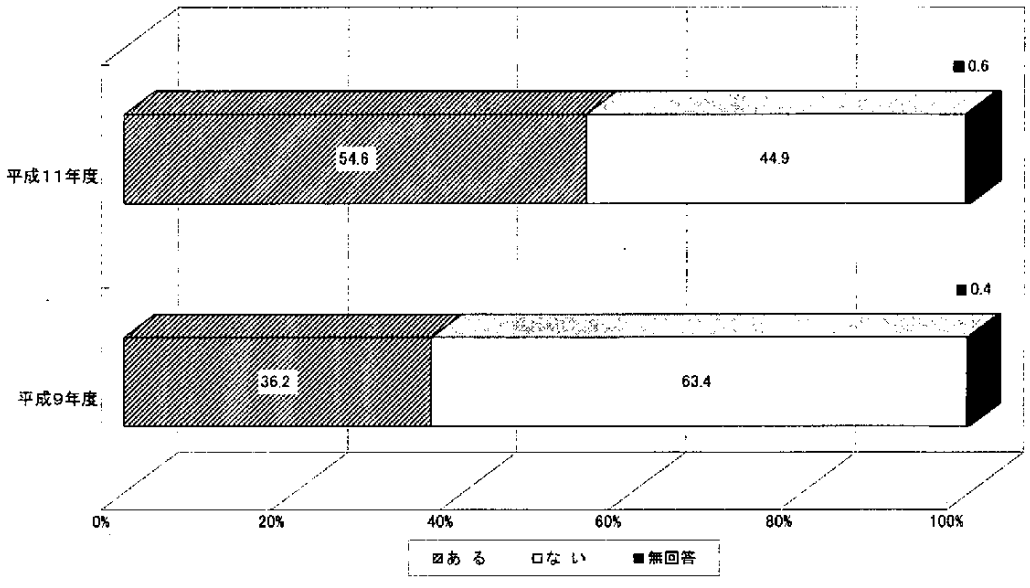


2．7　コンピュータウイルス対策について

Q61．貴社では過去1年間（平成10年1月～12月）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	473	54.6
2	な い	389	44.9
無回答		5	0.6
計		867	100.0

Q61G1．過去1年間のコンピュータウイルス被害状況



コンピュータウイルス被害については過半数の組織体が感染被害を受けている。前回調査と比べると18．4ポイントの増加であり、5割以上の増加率となった。この率でいくと、次回調査（平成13年度実施予定）では、80%以上の組織体が被害を受けることになると予想される。しかし、平成11年3月に発生した「メリッサウイルス」は、ウイルスがメールを自動的に発信して感染を広げるという新しい感染メカニズムを持ち、従来のファイル感染型ウイルスやマクロウイルスに比べ、非常に強い感染力を持っていた。このため、次回調査においては、被害を受けた組織体の割合は100%に近づくことが予想される。

Q62．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。
（Q61 の「1」を回答）

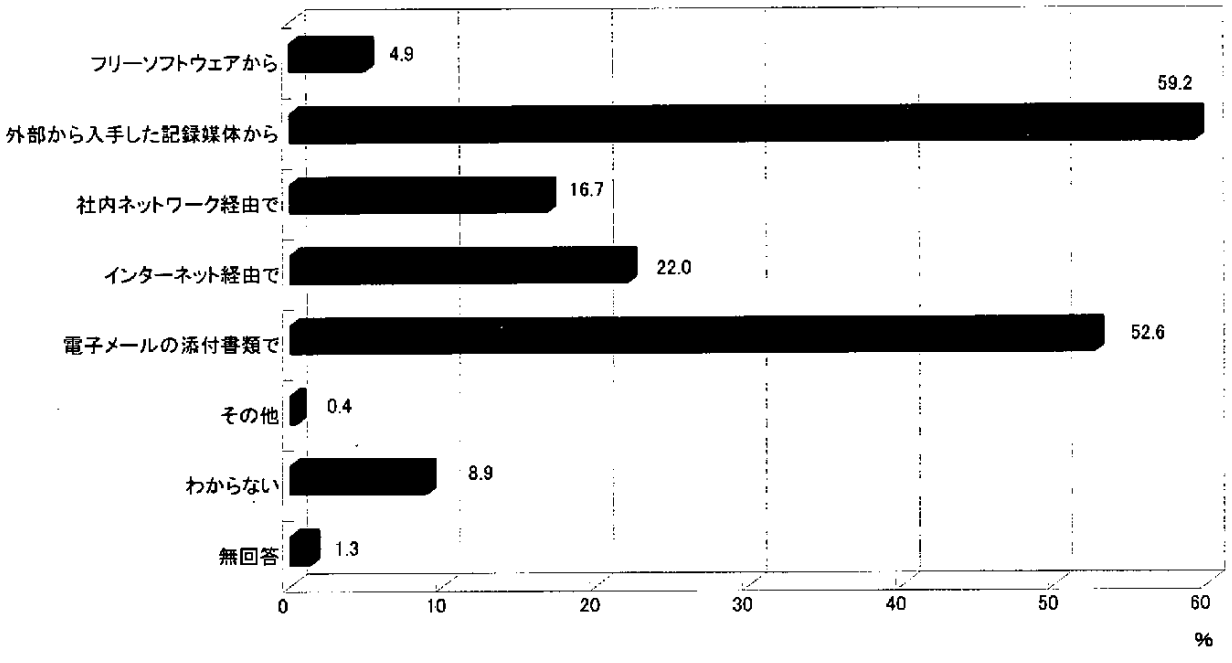
1	出した	64	13.5
2	出さない	389	82.2
無回答		20	4.2
計		473	100.0

通商産業省告示第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が、実際にコンピュータウイルスの被害を受けても届け出を出さない組織体が多い。前回調査に比べて届け出率が下がっているのは、昨今ウイルス感染の被害が急増し、またこの仕組みを知らない組織体が被害を受けたためと考えられる。

Q63. 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)(Q61 の「1」を回答)

回答件数		473	
1	フリーソフトウェアから	23	4.9
2	外部から入手した記録媒体から	280	59.2
3	社内ネットワーク経由で	79	16.7
4	インターネット経由で	104	22.0
5	電子メールの添付書類で	249	52.6
6	その他	2	0.4
7	わからない	42	8.9
無回答		6	1.3

Q63G1. コンピュータウイルスの主要感染原因(経路)



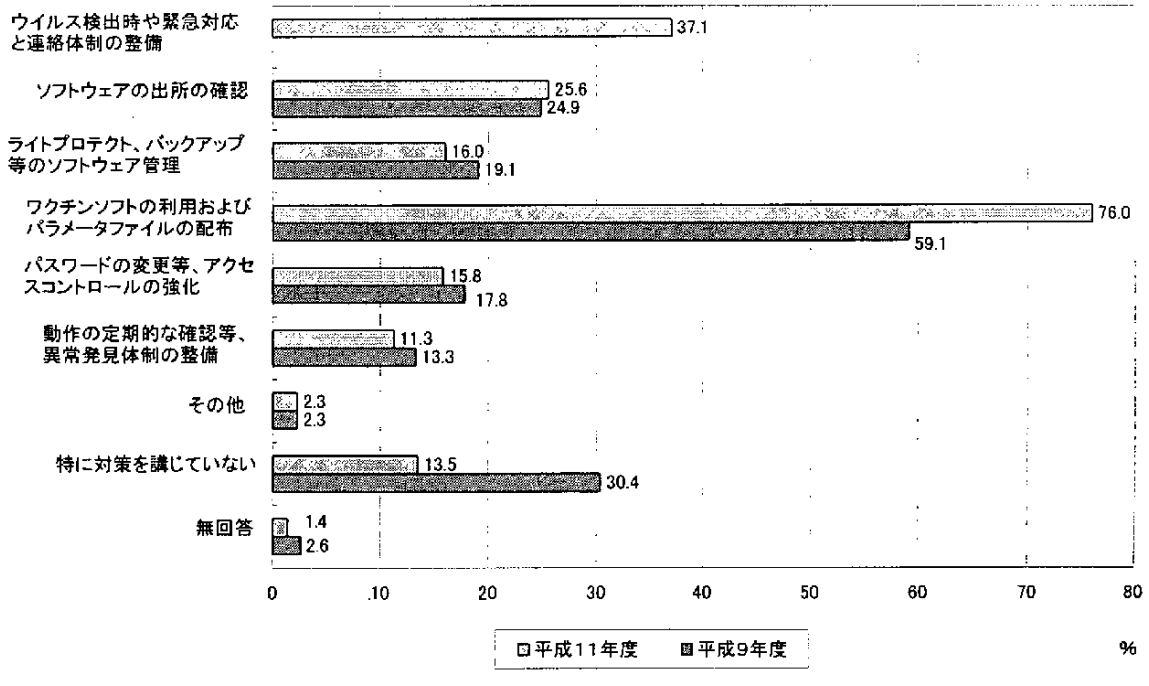
コンピュータウイルスの感染経路としては、前回調査に引き続き「外部から入手した記録媒体経由」によるものが多い。一方、「電子メールの添付書類で感染するマクロウイルス」の伸びが非常に大きいのが今回調査で明らかになった。この傾向は、メリッサウイルスのような電子メール自動感染型のウイルスが増えたことにより、今後一層強まっていくと考えられる。

Q64. ①貴社ではコンピュータウイルス対策を講じていますか。実施している対策を選んで下さい。(複数回答)

②また、その対策で満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。

回答件数 867		実施体制		満足している		問題がある		どちらともいえない		無回答	
1	ウイルス検出時や緊急対応と連絡体制の整備	322	37.1	160	49.7	67	20.8	84	26.1	11	3.4
2	ソフトウェアの出所の確認	222	25.6	85	38.3	48	21.6	81	36.5	8	3.6
3	ライトプロテクト、バックアップ等のソフトウェア管理	139	16.0	52	37.4	29	20.9	50	36.0	8	5.8
4	ワクチンソフトの利用およびパラメータファイルの配布	659	76.0	287	43.6	135	20.5	194	29.4	43	6.5
5	パスワードの変更等、アクセスコントロールの強化	137	15.8	46	33.6	35	25.5	50	36.5	6	4.4
6	動作の定期的な確認等、異常発見体制の整備	98	11.3	36	36.7	22	22.4	33	33.7	7	7.1
7	その他	20	2.3	8	40.0	6	30.0	5	25.0	1	5.0
8	特に対策を講じていない	117	13.5								
無回答		12	1.4								

Q64G1. コンピュータウイルス対策の実施状況



コンピュータウイルス対策として、「ワクチンソフトの利用」が前回調査の59．1%から76．0%へ大きく増加した。これは、電子メール感染型のウイルスが増えた結果、ソフトウェアの出所の確認といった手続き面での対策ではウイルス被害防止に対応できないことが認識された結果と思われる。

しかし、一方では、調査時点でワクチンソフトを導入していない組織体が24．0%もあり、これらの組織体が電子メールを使用していた場合、非常に大きな被害を受けることとなる。ワクチンソフトの利用は急速に100%に近づくことが予想される。また、ワクチンソフトも定期的にウイルスパターン

ファイルの更新を行う必要があるが、こういった管理を行うための体制を整備した組織体は37．1%と少なく、ワクチンソフトを導入後、きちんとした管理体制がとられていない組織体が多いことも危惧される。

Q65．貴社では従業員に対し、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	定期的に実施している	25	2.9
2	社内教育用のセキュリティ教育カリキュラムを策定して実施している	35	4.0
3	計画書またはマニュアル類に従って実施している	125	14.4
4	その他	61	7.0
5	特に実施していない	607	70.0
複数回答		4	0.5
無回答		10	1.2
計		867	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17．2%から21．3%へと大きく増加している。しかし、「実施していない」組織体が依然として70．0%と大きいことは、利用者のウイルス感染に対する意識が不十分のままで、組織内にウイルス感染が広がる前に発見し、適切な対応を取ることを難しくしている。これは、最近のウイルス感染拡大の1つの原因とすらなっている。今後、各組織体がいろいろな業務でネットワークを活用するようになると、利用者のコンピュータウイルスやセキュリティに関する意識を高めるために教育・訓練の実施は必須となる。

Q66．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）

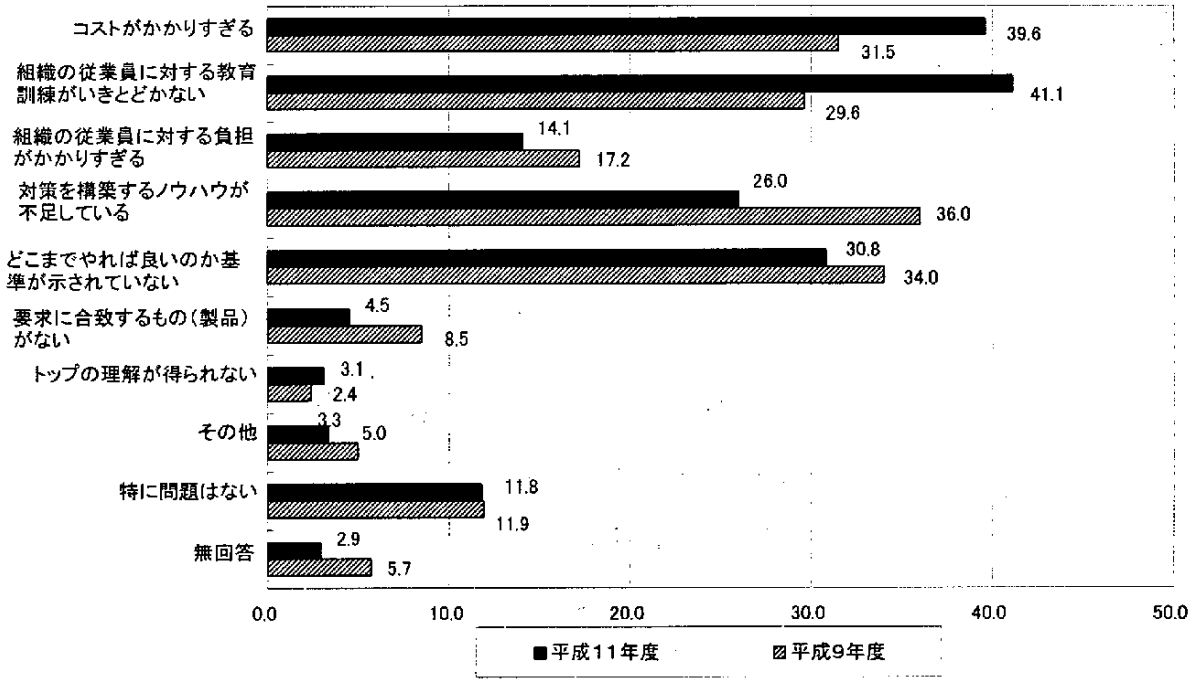
回答件数		867	
1	コストがかかりすぎる	343	39.6
2	組織の従業員に対する教育訓練がいきとどかない	356	41.1
3	組織の従業員に対する負何がかかりすぎる	122	14.1
4	対策を構築するノウハウが不足している	225	26.0
5	どこまでやれば良いのか基準が示されていない	267	30.8
6	要求に合致するもの（製品）がない	39	4.5
7	トップの理解が得られない	27	3.1
8	その他	29	3.3
9	特に問題はない	102	11.8
無回答		25	2.9

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「従業員に対する教育訓練の徹底」と「コスト」の問題をあげた組織体が多かった。Q65で教育・訓練未実施の組織体が70．0%と多かったことと、教育・訓練の必要性を認識している結果、この問題をあげた組織体が多かったと思われる。

今後の対策としては、ウイルス対策用の教育・訓練の雛形をWebで公開したり、情報処理技術者試験のなかで積極的に取り上げるといった対策が必要である。

一方、「対策を構築するノウハウの不足」や「どこまでやればよいかの基準」については、前回調査に比べて問題点としてあげた組織体が少なくなっており、ウイルス対策についてアウトソーシングを受託する会社等が増え、必要ならば外部のノウハウを活用できるようになったためと考えられる。

Q66G1. コンピュータウイルス対策の問題点

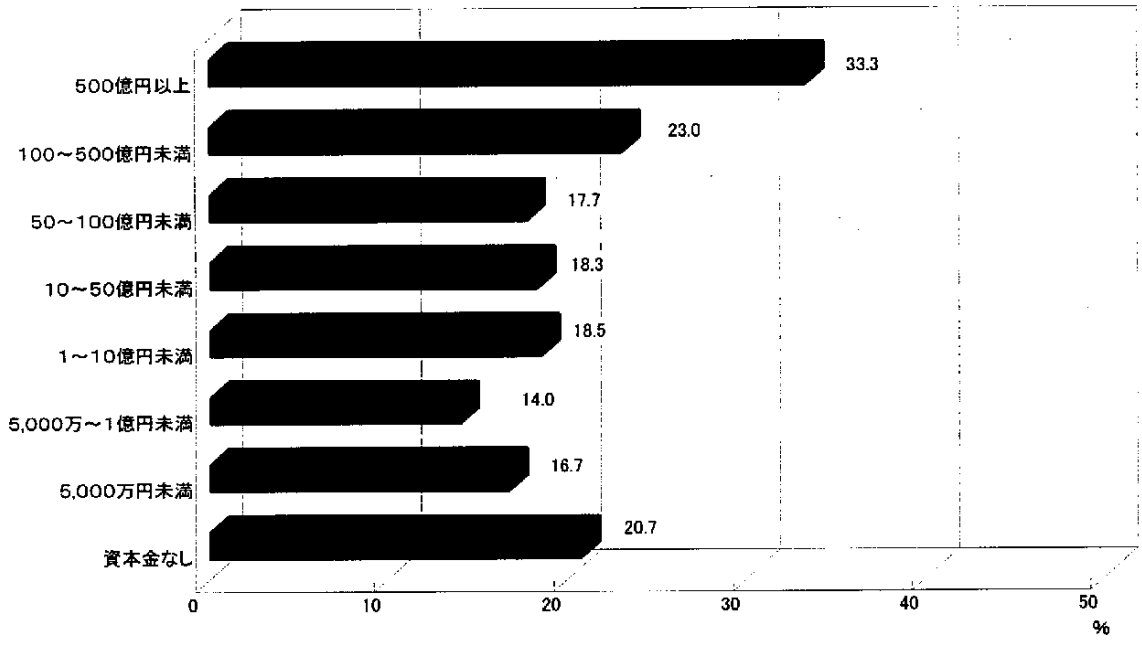


2．8　情報リスクマネジメント関連について

Q67．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		867	
1	経営者の理解	466	53.7
2	管理者の理解	264	30.4
3	担当者の理解	171	19.7
4	社内全体の理解	649	74.9
5	法規制の整備	171	19.7
6	その他	9	1.0
無回答		21	2.4

Q67G1．法規制の整備(資本金別)



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74．9%に達したが、これは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、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「経営者の理解」が重要との意見が53．7%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が必要としていると考えられる。

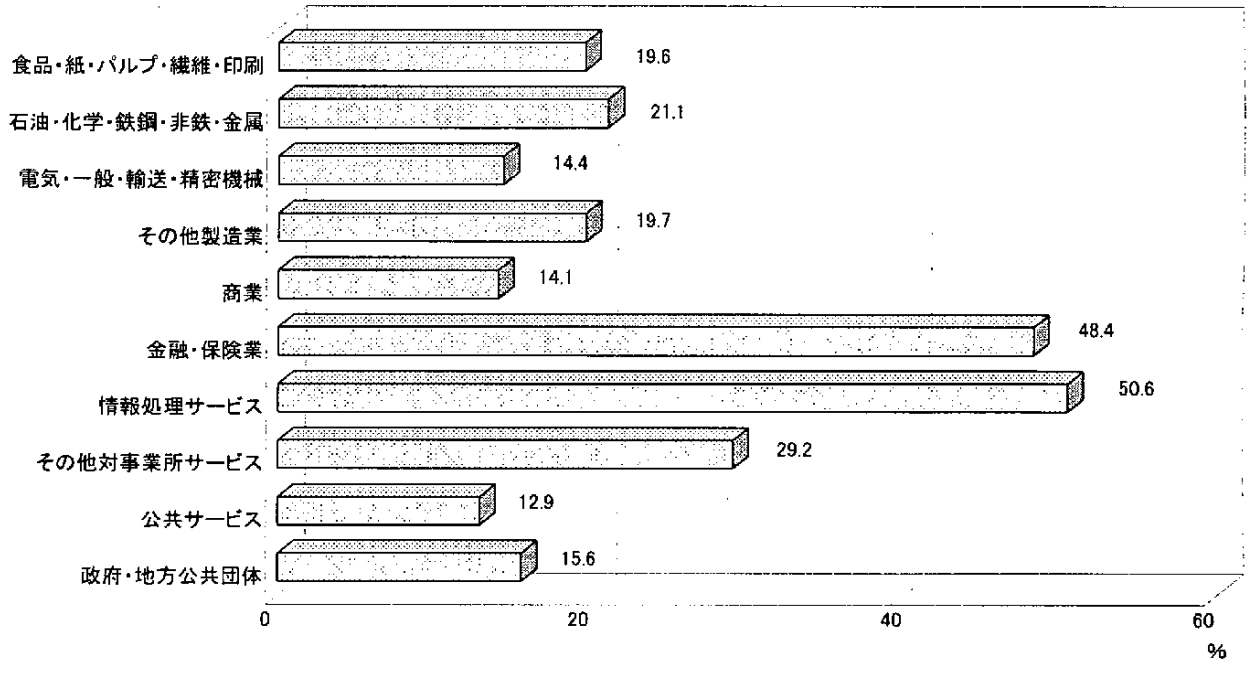
業種別や企業規模(資本金、従業員数)による違いを考察すると、各回答に大きな差はなかったが、その中で「法規制の整備」の必要性については、企業規模の大きい組織体ほどその必要性を訴えている。なお、この「法規制の整備」という選択項目の場合、情報セキュリティについて何らかの形で各組織体に情報セキュリティの実施を義務づける法規制の整備なのか、情報セキュリティに関する関連法による規制(たとえば『不正アクセス行為の禁止等に関する法律』)の整備等なのか、解釈の仕方を明確にしておくことも必要であった。

その他の意見としては、セキュリティ技術の向上と普及およびコストの低下、社内規定の教育などがあげられた。

Q68. 経営者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	221	25.5
2	中 位	288	33.2
3	低 い	159	18.3
4	わからない	189	21.8
無回答		10	1.2
計		867	100.0

Q68G1. リスクに関する関心度(業種グループ別)



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は分散した評価となっている。

業種別にみると、「高い」と回答した割合が高い業種は情報処理サービス(50.6%)、金融保険業(48.4%)の2業種である。一方低い業種は、公共サービス(12.9%)、商業(14.1%)、電気・一般・輸送・精密機械(14.4%)であった。

Q69. 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	104	12.0
2	行っていない	748	86.3
無回答		15	1.7
計		867	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わずか12.0%と低い値にとどまっている。

業種別にみると、金融・保険業(29.7%)、情報処理サービス(21.3%)が実施率の高い業種であるが、それでも30%に達しておらず、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。

Q70. リスク分析を実施しない理由は何ですか。(複数回答)(Q69 の「2」を回答)

回答件数		748	
1	重要性を感じていない	144	19.3
2	手法がわからない	334	44.7
3	予算がない	164	21.9
4	発生被害額が算出できない	152	20.3
5	リスク分析の意味がわからない	78	10.4
6	効果がわからない	248	33.2
7	効果があるとは思えない	49	6.6
無回答		52	7.0

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44．7%で一番多く、公的機関やベンダ、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」(19．3%)、「効果があるとは思えない」(6．6%)の2つの合計が25．9%であり、約4分の1がリスク分析の実施そのものに疑問を抱いている。

Q71. リスク分析を実施する際の問題点は何ですか。(複数回答)(Q69 の「1」を回答)

回答件数		104	
1	経営との関係がわからない	5	4.8
2	確立した手法がない	61	58.7
3	分析のためのデータが乏しい	27	26.0
4	専門家がいない	51	49.0
5	組織ができていない	27	26.0
6	問題点は特にない	10	9.6
7	その他	3	2.9
無回答		8	7.7

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」(58．7%)、「専門家がいない」(49．0%)となっており、実践的な手法の提供が望まれている。

その他の意見としては、リスク管理と情報セキュリティ管理の同期が一致しない、との意見があげられた。

Q72. リスク分析は誰が実施しましたか。(Q69 の「1」を回答)

1	情報システム部門内の要員	66	63.5
2	関係部門を含めたプロジェクトチーム	13	12.5
3	外部のコンサルタント	9	8.7
4	その他	4	3.8
複数回答		5	4.8
無回答		7	6.7
計		104	100.0

リスク分析は「情報システム部門内の要員」が実施するという回答が63．5%であり一番多かった。その他の意見として「リスク管理担当者のもとに実施する」、「各情報システムの管理責任者」、「管理部門等」、「社内のユーザ部門が実施する」との意見もあった。

Q73．貴社にとり、システミックリスク(注)をどう認識していますか。

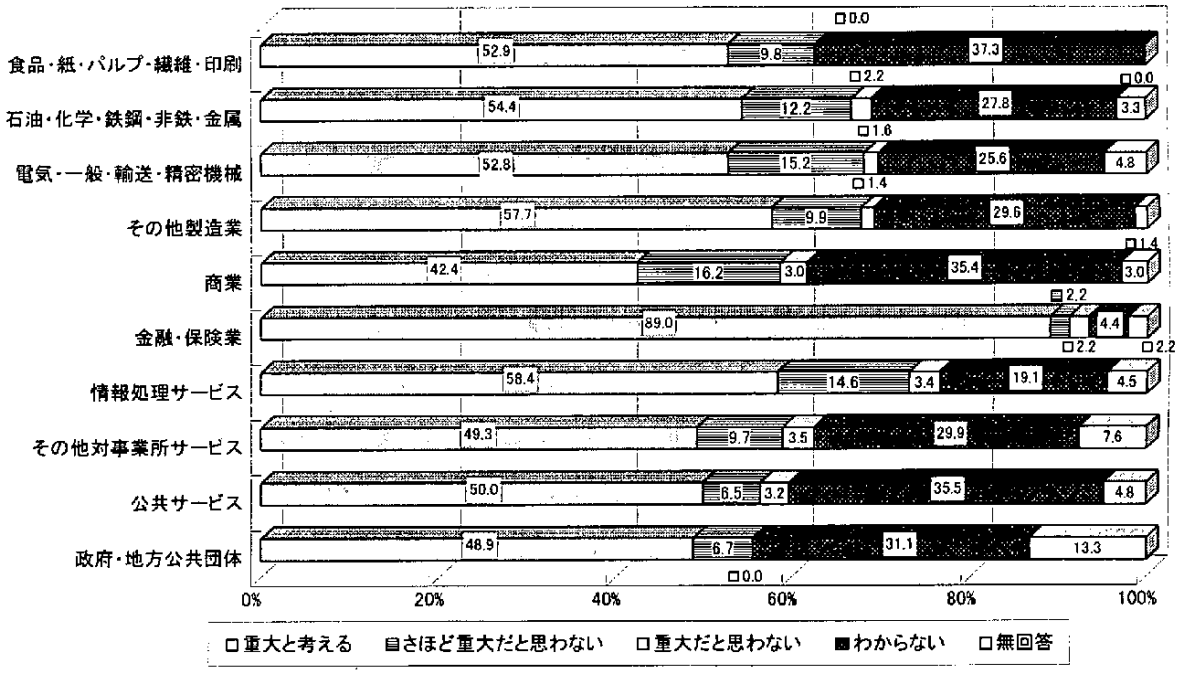
1	重大と考える	482	55.6
2	さほど重大だと思わない	94	10.8
3	重大だと思わない	20	2.3
4	わからない	232	26.8
無回答		39	4.5
計		867	100.0

（注）システミックリスクとはシステムを通して連鎖的に影響を及ぼすリスクをいいます。

システミックリスクを「重大と認識している」割合が55．6%と過半数を超えている。

業種別にみると、金融・保険業が「重大と認識している」割合が89．0%とかなり高いが、その他のほとんどの業種でも50%以上が「重大」と認識しており、情報化社会における組織体間のシステム的な結合度が大きいことがうかがえる。

Q73G1．システミックリスクに対する認識度（業種グループ別）



Q74．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。

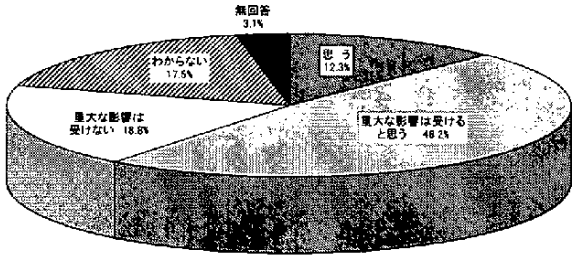
1	思 う	107	12.3
2	重大な影響は受けると思う	418	48.2
3	重大な影響は受けない	163	18.8
4	わからない	152	17.5
無回答		27	3.1
計		867	100.0

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12．3%である。倒産にいたらなくとも「重大な影響を受けると思う」が48．2%に達し、あわせて60．5%が相当程度の影響を受けると感じている。

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、金融・保険業23．1%、商業20．2%となっている。

一方、「重大な影響を受けない」としているところの意見として、「受託業務のケースでは倒産に該当するが、自社業務では重大な影響は受けない」としているものがあった。

Q74G1．情報システム関連リスクが与える倒産への影響度



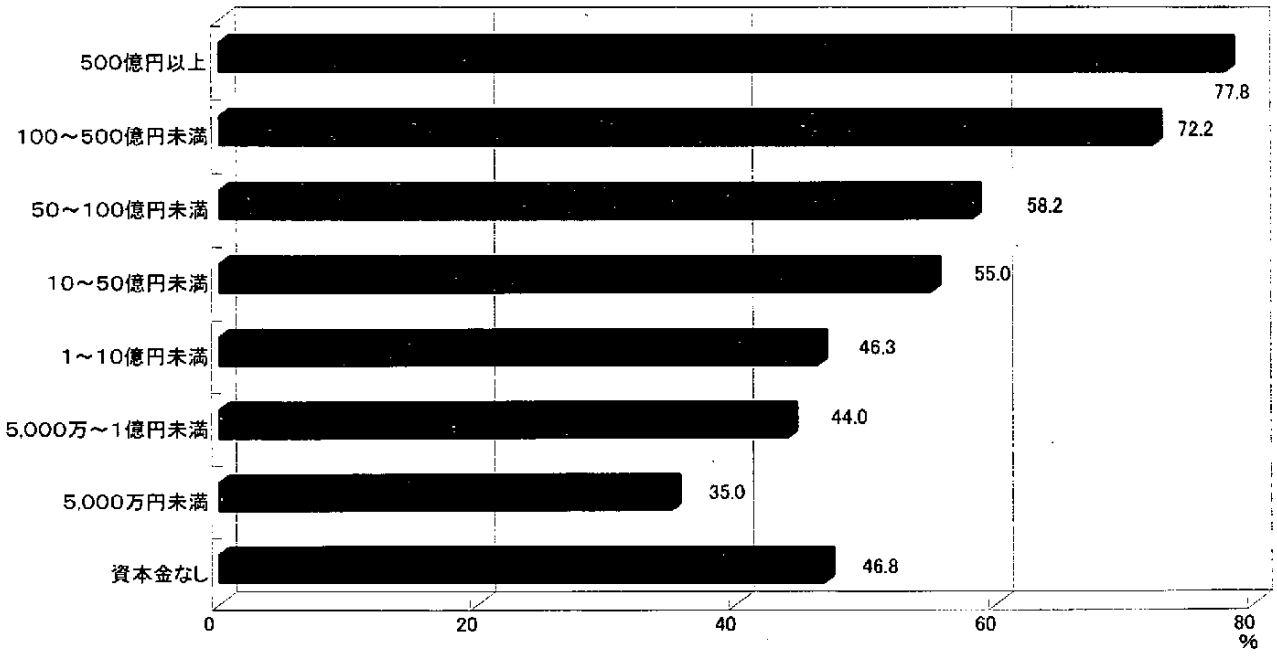
Q75．経営上、システム監査をどう考えていますか。

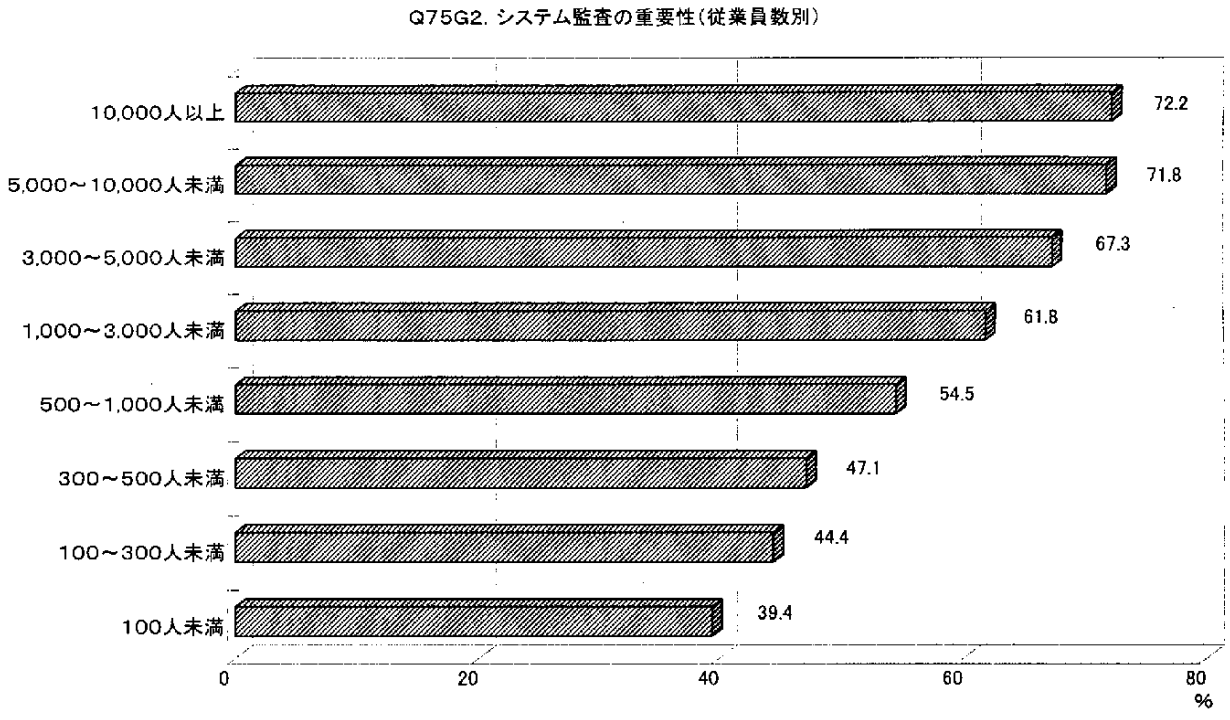
1	重要と考える	467	53.9
2	さほど重要だと思わない	175	20.2
3	重要だと思わない	25	2.9
4	わからない	177	20.4
無回答		23	2.7
計		867	100.0

経営上システム監査を重要と考えている割合は53．9%に達し過半数を超えた。

業種別にみると、「重要と考えている」割合が高い業種は、金融・保険業（84．6%）、情報処理サービス（70．8%）である。

Q75G1．システム監査の重要性（資本金別）





また、企業規模(資本金、従業員数)が大きくなるほど「重要」との回答が高く、株主や取引先、顧客等のステークホルダー・関係者の増加に伴う業務の透明性や情報公開が求められていることへの表れと考えられる。

Q76. 重要だと思わない理由は何ですか。(複数回答)(Q75 の「2」、「3」を回答)

回答件数		200	
1	経営者の認識が低いため	19	9.5
2	これまで重大なリスクなど起こらなかったため	113	56.5
3	システム監査の理解が不十分	56	28.0
4	システム監査の限界	61	30.5
5	その他	8	4.0
無回答		11	5.5

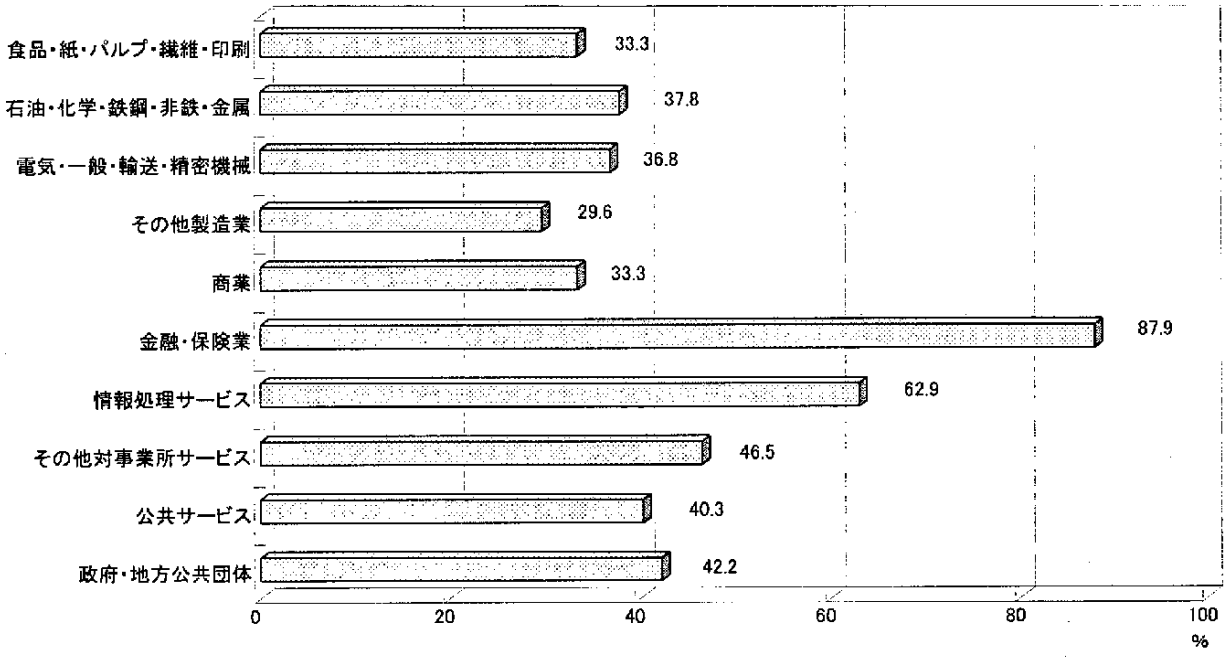
システム監査を重要と思わない理由として、「これまで重大なリスクなど起こらなかったため」が56.5%となっており、リスクマネジメントの立場からすると好ましくない状況である。一方、「システム監査の限界」とする意見も30.5%あり、その他の意見としては、「システム監査結果をフィードバックする体制が整っていない」、「重要なデータの取扱いが少ない」、「システム監査基準の規定項目が現状と合致しない」、「会計士とシステム監査人とが互いに責任逃れをする」などの厳しい指摘がある。

この他、「システム活用度が低い」、「自社の基幹システムは手作業でカバーできる範囲」、「重要な仕事をさせていない」などの意見があげられた。

Q77. 緊急時の役割はあらかじめ決められていますか。

1	い る	398	45.9
2	いない	441	50.9
無回答		28	3.2
計		867	100.0

Q77G1. 緊急時の役割の決定(業種グループ別)



緊急時の役割をあらかじめ「決めている」のは45．9%と半数を若干下回った。

業種別にみると、高いところでは金融・保険業(87．9%)、情報処理サービス(62．9%)がある。一方、食品・紙・パルプ・繊維・印刷／商業(33．3%)、その他製造業(29．6%)等低いところもあり、業種による差が大きい。

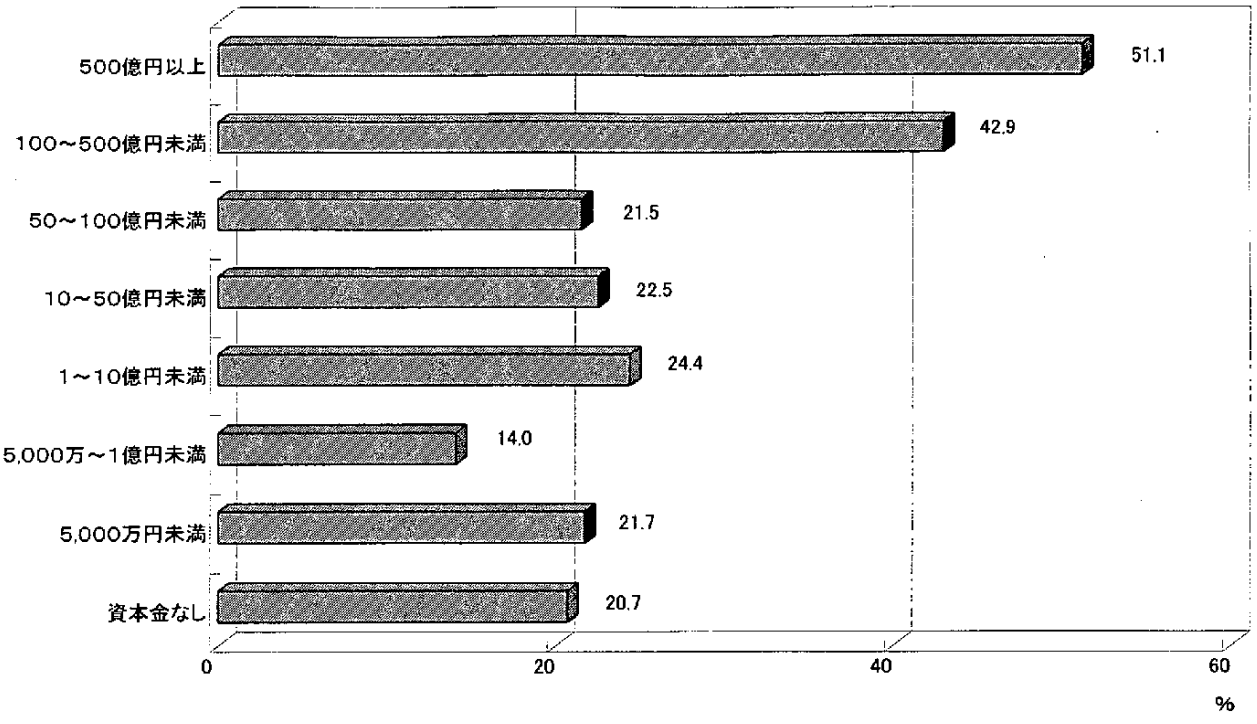
Q78. 災害復旧のレベル(事業再開のための最低限、災害以前の水準、等)をあらかじめ段階的に決めていますか。

1	い る	230	26.5
2	いない	612	70.6
無回答		25	2.9
計		867	100.0

災害復旧のレベルを「定めている」のは26．5%と約4分の1にとどまった。

業種別にみると、一番高い金融・保険業では58．2%であるが、その他の業種には大きな差はない。一方、資本金別にみると、資本金100億円以上では42．9%から51．1%となったが、100億円未満では高くても24．4%と100億円を境に差が生じている。

Q78G1. 災害復旧レベルの決定(資本金別)



Q79. 全社の従業員に対し、情報セキュリティ教育を実施していますか。

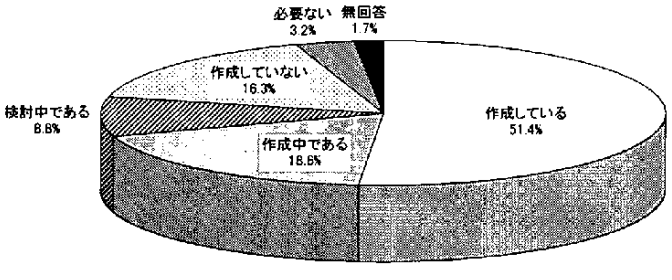
1	い る	112	12.9
2	いない	737	85.0
無回答		18	2.1
計		867	100.0

情報セキュリティ教育を「実施している」割合は12．9%と低い状況にとどまった。実施率の高い業種でも情報処理サービス(36．0%)、金融・保険業(23．1%)と総じて低い状況であり、安全対策上の大きな課題といえる。

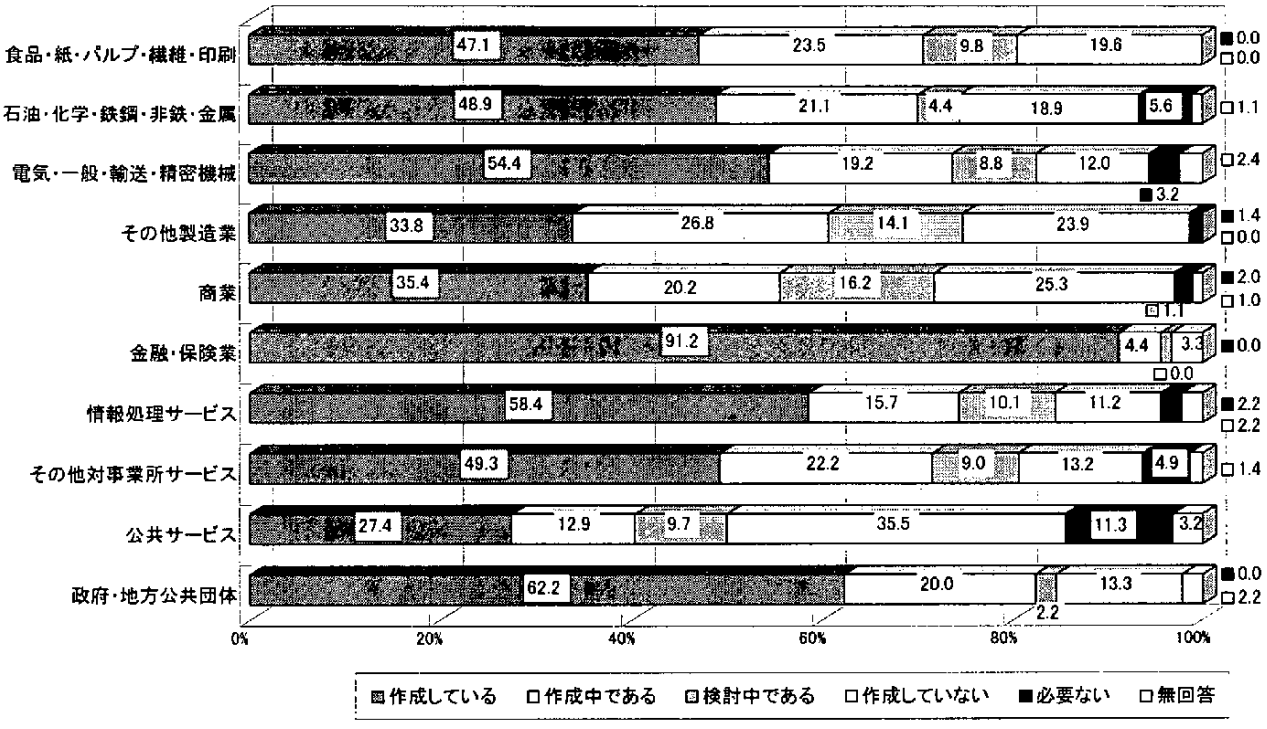
Q80. 西暦2000年問題の発生を想定して危機管理マニュアルを作成していますか。

1	作成している	446	51.4
2	作成中である	161	18.6
3	検討中である	76	8.8
4	作成していない	141	16.3
5	必要ない	28	3.2
無回答		15	1.7
計		867	100.0

Q80G1. 西暦2000年問題対応の危機管理マニュアルの作成



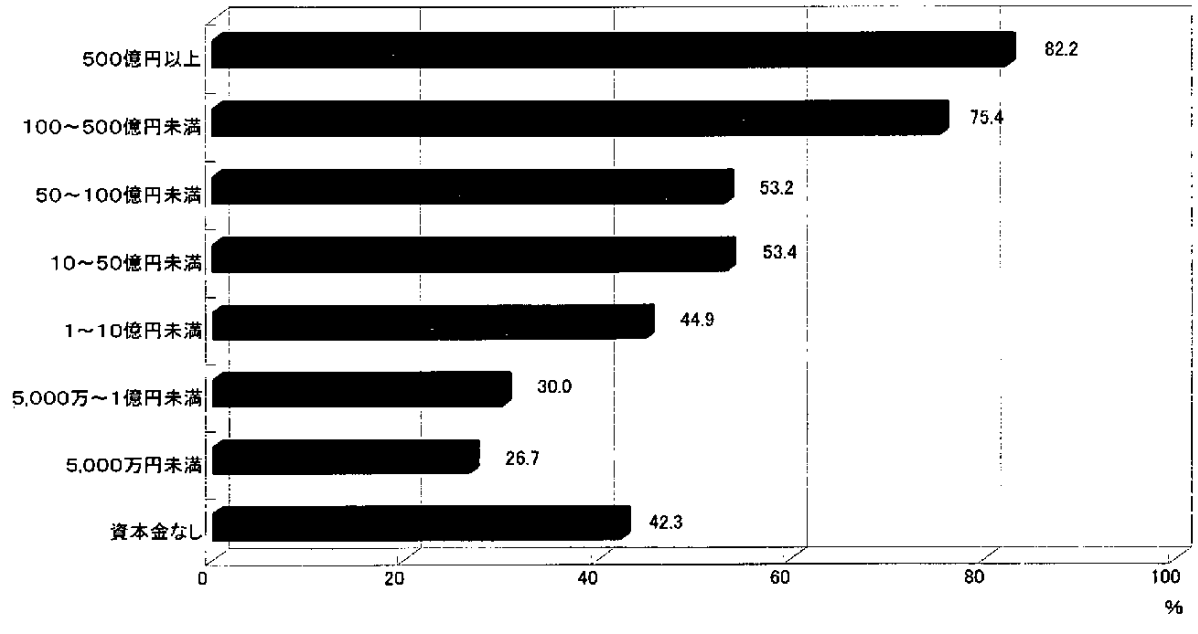
Q80G2. 西暦2000年問題を想定した危機管理マニュアルの作成（業種グループ別）



西暦2000年問題は大きな社会的混乱もなく、軽微なトラブルの発生にとどめることができた。しかし、万一のための危機管理マニュアルについては調査時点（1999年10月）で「作成している」との回答は51．4%であった。「作成していない」（16．3%）と「必要ない」（3．2%）をあわせると19．5%と、約5分の1が危機管理マニュアルを作成しないで2000年を迎えようとしていた。

業種別にみると、すでに危機管理マニュアルを「作成していた」のは金融・保険業が91．2%と群を抜いて高く、次いで政府・地方公共団体（62．2%）、情報処理サービス（58．4%）と続く。資本金別にみると資本金が大きいところほど危機管理マニュアルを作成している割合が高い。

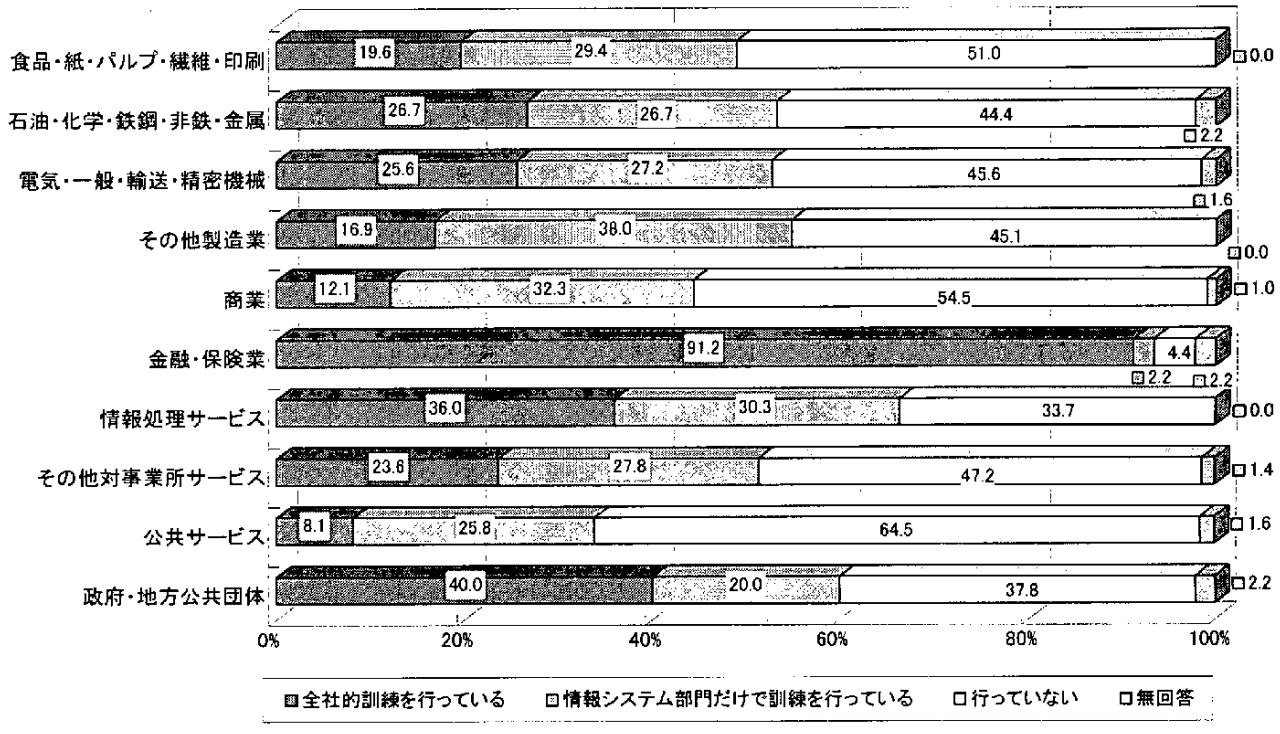
Q80G3. 西暦2000年問題を想定した危機管理マニュアルの作成（資本金別）



Q81. 西暦 2000 年問題に対し、従業員に対し訓練を行っていますか。

1	全社的訓練を行っている	262	30.2
2	情報システム部門だけで訓練を行っている	226	26.1
3	行っていない	368	42.4
無回答		11	1.3
計		867	100.0

Q81G1. 西暦2000年問題に対する従業員の訓練



2000年問題に対して「全社的に訓練を行っている」のは30．2%と約3分の1を下回った。危機管理マニュアルの作成を視野に入れている割合（Q80の回答1～3の合計）が78．8%であるのに対し、訓練実施の割合は「情報システム部門だけで訓練を行っている」もあわせて56．3%であり、マニュアル作成の割合に比べて71．4%の状況となっている。

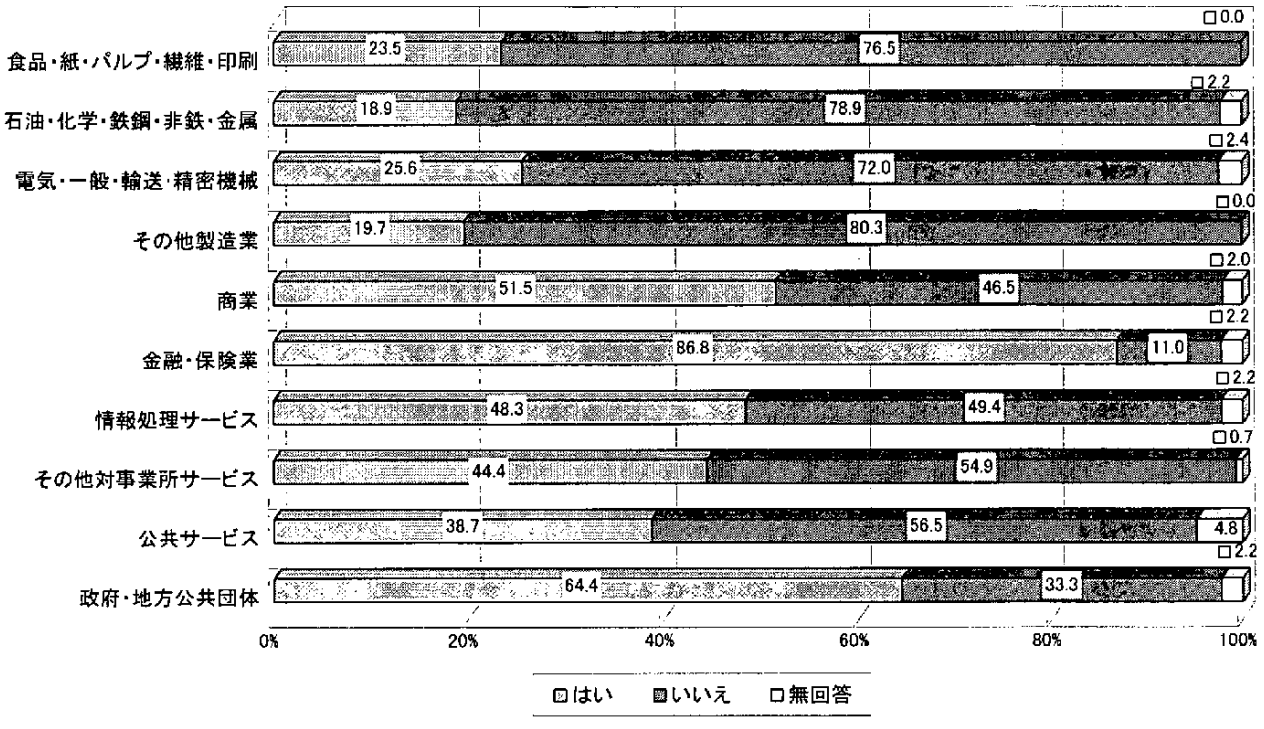
業種別にみると、金融・保険業での全社的訓練の実施率が91．2%と極めて高いのが目立っている。

2．9　個人情報保護について

Q82.顧客等の個人情報を利用していますか。

1	はい	365	42.1
2	いいえ	486	56.1
無回答		16	1.8
計		867	100.0

Q82G1．個人情報の利用状況（業種グループ別）

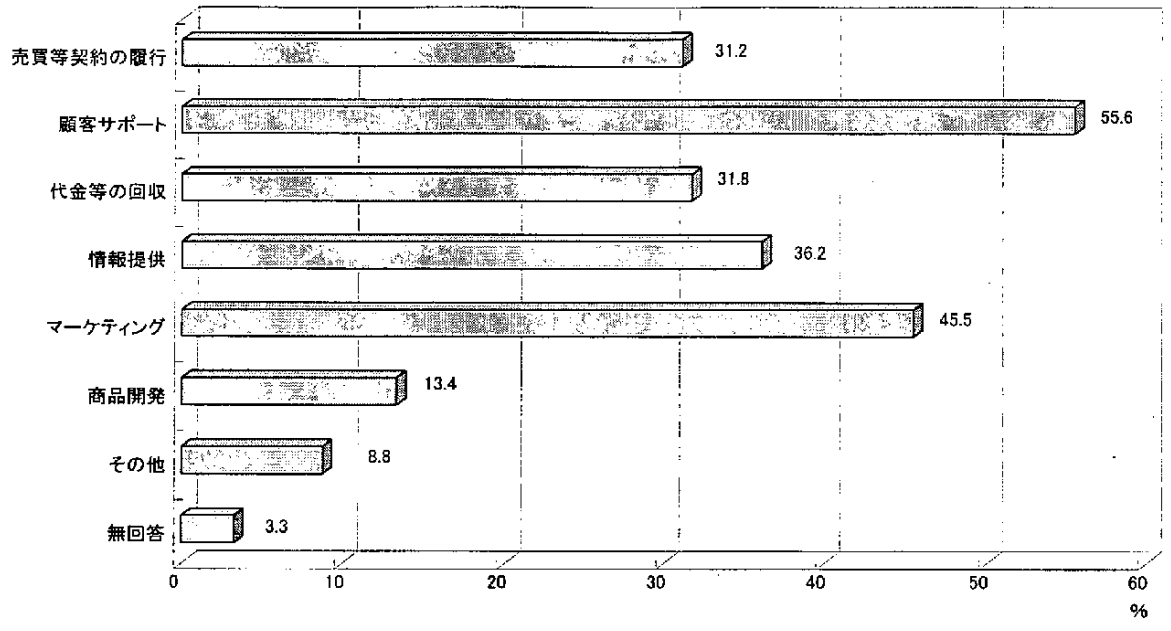


プライバシー問題に対する関心の高まりをうけ、個人情報保護に関する調査項目を今回新たに設けた。個人情報の利用に関しては、約4割の組織体が「利用している」と回答しているが、特に金融・保険業（86．8%）において高い利用率がみられる。逆に製造業全体では22．3%が利用しているにとどまり、業種別における個人向けへの事業展開の度合いが反映されていると思われる。

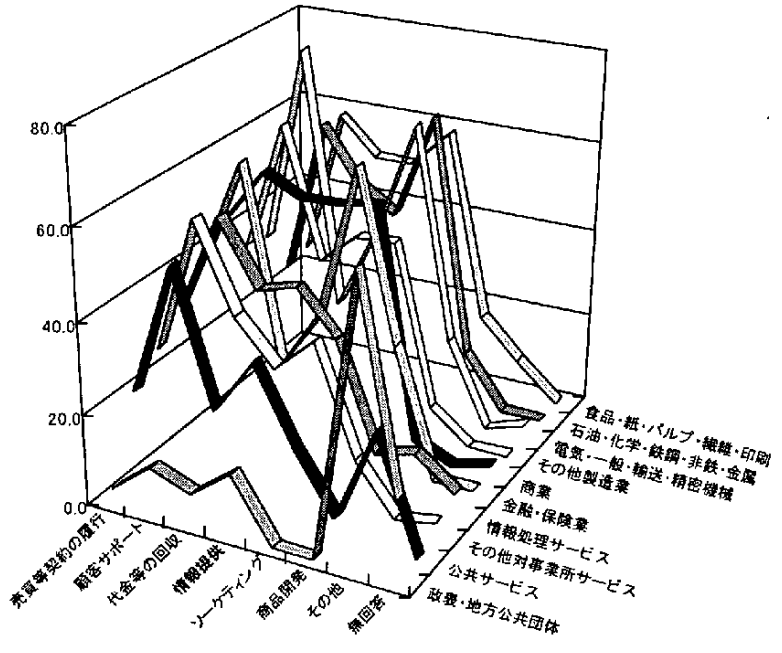
Q83.利用目的は何ですか。（複数回答）（Q82 の「1」を回答）

回答件数		365	
1	売買等契約の履行	114	31.2
2	顧客サポート	203	55.6
3	代金等の回収	116	31.8
4	情報提供	132	36.2
5	マーケティング	166	45.5
6	商品開発	49	13.4
7	その他	32	8.8
無回答		12	3.3

Q83G1. 個人情報の利用目的



Q83G2. 個人情報の利用目的(業種別)



Q82で個人情報を利用しているとの回答のうち、その利用目的としては「顧客サポート」が最も多く55.6%の回答があり、次いで「マーケティング」(45.5%)である。

「顧客サポートでの利用」はほとんどの業種においてもっとも高い回答率を示しているが、特に電気・一般・輸送・精密機器が高く(78.1%)、次いで金融・保険業(62.0%)である。

「マーケティング目的の利用」では、公共サービス(16.7%)が平均を下回る回答率となっており、情報処理サービス(32.6%)、その他対事業所サービス(35.9%)もやや低めの結果となった。

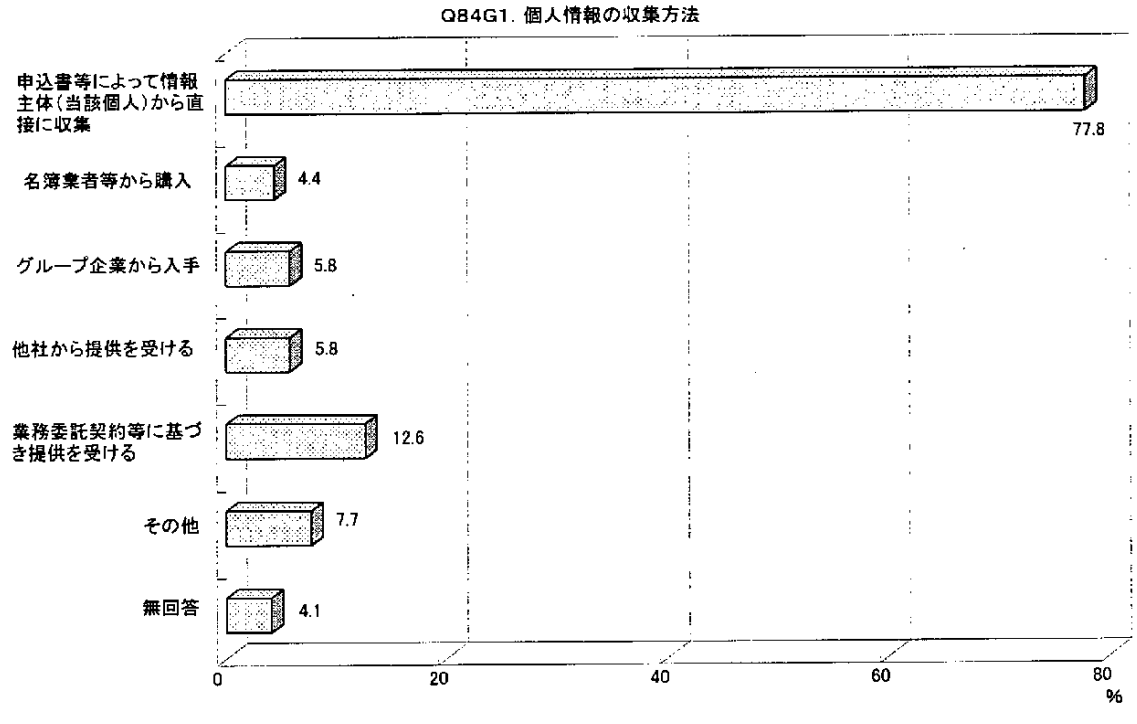
政府・地方公共団体は他の業種区分と回答の傾向が大きく異なり、「契約の履行」から「商品開発」までの回答率が比較的低く、「その他」の回答が62.1%となっているが、これは行政の特殊性によるものと思われる。

Q84. 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)(Q82 の「1」を回答)

回答件数		365	
1	申込書等によって情報主体(当該個人)から直接に収集	284	77.8
2	名簿業者等から購入	16	4.4
3	グループ企業から入手	21	5.8
4	他社から提供を受ける	21	5.8
5	業務委託契約等に基づき提供を受ける	46	12.6
6	その他	28	7.7
無回答		15	4.1

個人情報の収集方法としては、「当該個人から直接に収集する」との回答が8割弱と最も高く、次に回答数の大きい「業務委託契約等によるもの」では12．6%と大幅に差が出ている。

業種別にみると、金融・保険業(89．9%)、公共サービス(83．3%)、商業(82．4%)においては、個人から直接に収集する回答が多い。逆に、情報処理サービスでは、「業務委託契約等に基づく提供」(44．2%)や「グループ企業から入手」(16．3%)という回答が多く、個人情報の入手方法に関して、事業形態の影響がみられる。

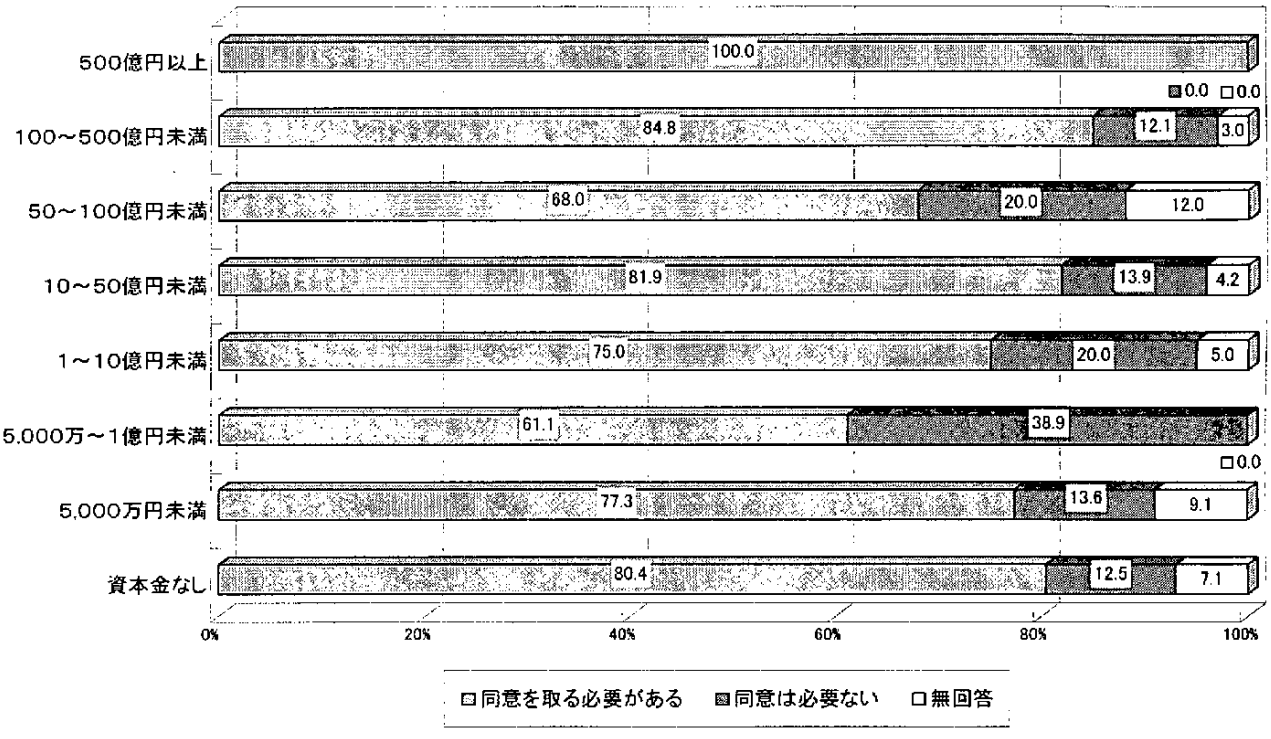


Q85. 情報主体から直接に収集する場合、利用目的等を明示して同意を取る必要があると思いますか。
(Q82 の「1」を回答)

1	同意を取る必要がある	291	79.7
2	同意は必要ない	56	15.3
無回答		18	4.9
計		365	100.0

個人情報の収集に関しては、個人情報を利用していると回答した組織体のうち、約8割が「同意を取る必要がある」と回答しており、個人情報保護に対する意識の高まりを反映している結果となった。資本金500億円以上の組織体では100%の組織体が「同意を取る必要がある」と回答しており、従業員数や情報化投資額でもっとも大きなカテゴリにおいて高率の回答が得られている。

Q85G1. 情報主体からの同意の必要性(資本金別)



Q86. (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)

回答件数		867	
1	知っている	173	20.0
2	知らない	670	77.3
3	プライバシーマークを利用したい	19	2.2
4	利用したいと思わない	2	0.2
無回答		18	2.1

(財)日本情報処理開発協会の『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2割にとどまっている。

本質問に関連して、Q4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』の周知度に対する回答でも「知っている」という回答は14.0%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。

Q82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57.3%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。86.8%が個人情報の利用をあげた金融・保険業においては、25.3%が「知っている」と回答するにとどまり、また51.5%が個人情報を利用していると回答した商業においては、「知っている」という回答は12.1%である。

Q87. 今後必要と思われるセキュリティ制度・機能・製品等がありましたら、具体的にお書き下さい。

本設問に対する意見は次のとおりである（抜粋）

（セキュリティ全般）

・電子商取引を行うにあたっての法整備とセキュリティ確保のための基盤技術の標準化。
・セキュリティモデルの制定
・会社全体のセキュリティポリシー策定・整備。
・不正アクセス、ウイルス、監査基準等、個別のセキュリティ関連ドキュメントは入手できるが、リスク対策の範囲、コスト、影響度等の事例が不足している。安全対策認定のための活動を実施しているが、全体のセキュリティガイドラインやセキュリティポリシー確立の案内書が必要と思われる。
・BS7799に類するISO（JIS）規準（認定制度）、PKI製品、アクセス制御、認証
・ISO15408の具体化等、情報システムセキュリティの評価基準の明確化が必要と考えられる。また、犯罪的行為に対する厳正な対応による抑止力の発揮が期待される。
・セキュリティ対策を講じている企業などに対して税制上の優遇措置を充実させ、そのコスト面でのバックアップを計ってほしい。
・法律や制度ができた時、確実に関係先に伝わる形をとってもらいたい。たとえばウイルス被害を受けた場合に連絡先、連絡方法がわからない。
・ISO等のセキュリティ認証制度
・インターネット接続にて、海外のオフィスの集中管理を可能にする製品、および設置サービス（特にアジア）
・モバイルアクセスでセキュリティを確保する安価な製品。現在ではセキュリティツール自体がマシンの価格と同時またはこえる場合もある。

（不正アクセス・コンピュータウイルス対策）

・不正アクセスまたはウイルスによる障害を防ぐ機能、製品の充実

（ネットワーク関連）

・ネットワークコンピューティングを拡大するためのロ―コストな製品の発売。

（暗号・認証）

・データの暗号化
・暗号化メール、ディジタル署名
・認証
・個人を特定するためのICカード

（アクセスコントロール）

・パスワードの強制的変更
・アクセスログを自動分析、自動整理保管するユーティリティ

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として指定されてい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への届け出率は低く、施策の周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実施した。

・Q62. 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。

クロス集計をみると、届け出ない組織体の71．2%がIPAが届出機関であることを知っており、届け出ない理由が施策の周知度以外にあることが推測される。

Q2-2. IPAが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。

組織体が不正アクセス被害を受けたときにIPAに届け出る率は低く、施策の周知度との関係を分析するため、以下の質問とのクロス集計を実施した。

・Q50. 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、届け出ない組織体の72．5%が IPA が届出機関であることを知っており、届け出ない理由が施策の周知度以外にあることが推測される。

Q3. 不正アクセスの被害を受けた組織等から依頼を受けて、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。

不正アクセス被害を受けたときにJPCERT／CCに相談する組織体は13．2%と少数にとどまるが、施策の周知度との関係を以下の質問とのクロス集計により行った。

・Q51. 不正アクセスの被害にあたり、JPCERT/CC(コンピュータ緊急対応センター)に相談しましたか。

クロス集計では、不正アクセス被害にあった組織体でJPCERT／CCに相談をしたのは16．7%にとどまっている。

Q4.「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。

『プライバシーマーク制度』の周知度が、個人情報保護施策に対する周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うことにより検証を試みた。

・Q86.（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』に対する周知度と、プライバシーマーク制度に対する周知度との間には関連がみられ、個人情報保護に関する周知度がプライバシーマーク制度に対する周知度に影響しているものと思われる。

Q5. ①ハードウェア、ソフトウェア、データを含む、現在稼働中の全情報システムへの総投資金額の概算を教えて下さい。

情報システムへの投資金額が大きい、すなわち守るべき情報資産が大きい組織体ほど、情報システムのセキュリティに対して組織的な対応を図っているのではないかという仮説をたて、以下の質問に対する回答との間でクロス集計を行った。

・Q16. 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。
・Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。
・Q19. セキュリティガイドラインを定期的に見直していますか。
・Q20. 基幹システムのネットワーク管理者を定めていますか。
・Q21. 情報システムの管理責任者を定めていますか。
・Q22. 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。

クロス集計の結果、セキュリティポリシーの制定(Q16)、セキュリティガイドラインの作成(Q17)、セキュリティガイドラインの定期的見直し(Q19)、ネットワーク管理者の設置(Q20)、情報システム管理者の設置(Q21)に関しては、情報システムの総投資金額が多いほど、「定めている」と回答した率が高い傾向がみられた。専任のセキュリティ管理者の設置(Q22)に関しては、他の質問の傾向と異なり、総投資金額の間で明確な傾向はみられなかった。

逆に「定めている」とした回答に対する総投資金額別では、はっきりした傾向はみられなかった。それに対して、「定めていない」との回答に対しては、総投資金額が小さい組織体ほど高い傾向がみられた。

Q11. 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、組織体の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いう仮説を立て、次の質問との間でクロス集計を行うことにより検証を試みた。

・Q13. 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。
・Q14. 基幹システムにおけるMTBF(平均故障間隔)は何時間ですか。
・Q15. 基幹システムにおけるMTTR(平均修理時間)は何分ですか。
・Q16. 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。
・Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。
・Q19. セキュリティガイドラインを定期的に見直していますか。
・Q20. 基幹システムのネットワーク管理者を定めていますか。
・Q21. 情報システムの管理責任者を定めていますか。
・Q22. 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。
・Q32. 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。
・Q34. ①情報システムのバックアップ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。

・Q36. ①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。
・Q38. ①ファイルのバックアップ対策はどのようなものですか。実施している対策項目を選んで下さい。
・Q45. システム災害・障害対策についての問題点は何ですか。
・Q46. 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。
・Q59. 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。

システムダウンの原因(Q13)では、運用実績の長い集中型が全体的にもっともよい傾向があり、一部の項目を除き、分散型や集中分散型はほぼ同じ傾向となった。「OS障害」では構成が複雑な集中分散型が悪く、「ソフトウェア障害」では要求される品質の影響か、分散型がもっとも悪い結果となった。

セキュリティポリシーの制定(Q16)、専任のセキュリティ管理者の設置(Q22)に関しては、集中型よりも集中分散型、分散型の方が「定められている」、「作成中である」、「現在検討中である」との回答率が高い。

バックアップ対策(Q34)、ファイルのバックアップ対策(Q38)においては、集中型、集中分散型では、広域災害に対応できる対策を実施している組織体が分散型と比較して多い。分散型でのバックアップ対策は、同一施設内で実施する対策をあげた回答が中心となる。

Q16. 記者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？

経営理念に基づくセキュリティポリシーを定めている組織体では、セキュリティ管理に関する取組みも進んでいるという仮説を立て、セキュリティ管理に関連する回答との間でクロス集計を実施することにより検証した。

・Q11. 貴社の基幹システムはどのように運用されていますか。
・Q20. 基幹システムのネットワーク管理者を定めていますか。
・Q21. 情報システムの管理責任者を定めていますか。
・Q23. 緊急時の連絡手段を持っていますか。
・Q24. データの使用・保管等の管理を行っていますか。
・Q25. 基幹システムを国際的に展開・利用していますか。
・Q28. 情報セキュリティ管理についての問題点は何ですか。
・Q30. 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。
・Q33. 貴社でとられている災害・障害対策は、全体的にみて満足できるものですか。
・Q38. ①ファイルのバックアップ対策はどのようなものですか。実施している対策項目を選んで下さい。
・Q40. 貴社の基幹システムはどれぐらいの頻度でファイル等のバックアップを実施していますか。
・Q60. 不正アクセス対策についての問題点は何ですか。
・Q66. 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。
・Q68. 経営者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。
・Q75. 経営上、システム監査をどう考えていますか。

セキュリティ管理の体制整備(Q20、Q21、Q23、Q24)に関しては、セキュリティポリシーを定めている組織体では、セキュリティ管理体制が充実している傾向がある。ただし、セキュリティポリシーを定めていない組織体でも、その多くは管理体制を整備しているが、非常事態の発生時における責任範囲の明確化のためにも、セキュリティポリシーの制定が望まれる。

国際展開(Q25)に関しては、 国際的な展開を行っていない組織体においてセキュリティポリシーを定めている割合は小さい傾向がある。

リスク対策の実施（Q30、Q33、Q38、Q40、Q66）に関しては、セキュリティポリシーの有無と、リスク対策の実施度合いの間には、はっきりした相関はみられない。現時点では、リスクマネジメントが組織体の経営全体の問題という認識が薄く、特定部門において個別のリスク対策が実施されている状況にあるものと思われる。

経営者の関与（Q68、Q75）に関しては、経営理念に基づくセキュリティポリシーの有無と、経営者の関与の間では、大きな相関がみられた。

Q67. 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）

情報セキュリティの捉え方（「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」、「法規制の理解」）の違いが、情報セキュリティの確保への取組み度合いに影響があることを想定し、以下の質問との間でクロス集計を行った。

・Q5. ①ハードウェア、ソフトウェア、データを含む、現在稼働中の全情報システムへの総投資金額の概算を教えて下さい。
・Q8. 情報システムの資産価値を評価したことがありますか。
・Q20. 基幹システムのネットワーク管理者を定めていますか。
・Q21. 情報システムの管理責任者を定めていますか。
・Q22. 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。
・Q25. 基幹システムを国際的に展開・利用していますか。
・Q30. 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。
・Q32. 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。
・Q33. 貴社でとられている災害・障害対策は、全体的にみて満足できるものですか。
・Q69. 情報システムに係わるリスク分析を実施していますか。
・Q74. 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。

特に、「経営者の理解」が重要であると回答した組織体ほど、情報セキュリティ確保に向けた取組みが進んでいるとの仮説を立てた。Q67の各項目（「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」、「法規制の理解」）それぞれの回答に対してクロス集計による分析を行い、上記仮説の検証を試みたが、「経営者の理解」を重要な視点として認識している組織体ほど情報セキュリティの確保に向けた取組みが実施されているとの仮説を裏づける分析結果は得られなかった。しかし、情報セキュリティ確保に向けた諸施策を実施している組織体ほど、情報セキュリティへの認識が高い傾向がみられた。全体的な傾向としては、経営者と従業員が一体となった取組みを重視する回答（「社内全体の理解」）の方が、経営者のイニシアチブを重視する項目（「経営者の理解」）より高い回答率となる傾向がみられ、日本的な経営観の影響がみられる。

Q69. 情報システムに係わるリスク分析を実施していますか。

情報システムのセキュリティ確保にとって、リスク分析は出発点となる。情報システムのリスク分析を実施している組織体では、当然以下の質問との間で何らかの関連性が想定される。このため、以下の質問との間でクロス集計によりリスク分析の実態について検証を試みた。

・Q8. 情報システムの資産価値を評価したことがありますか。
・Q11. 貴社の基幹システムはどのように運用されていますか。

・Q12. 貴社の基幹システムは過去1年間(平成10年1月～12月)にシステムダウンが発生しましたか。
・Q25. 基幹システムを国際的に展開・利用していますか。
・Q46. 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。
・Q61. 貴社では過去1年間(平成10年1月～12月)にコンピュータウイルスに感染したことがありますか。
・Q73. 貴社にとり、システミックリスクをどう認識していますか。

リスク分析を行っていると回答した組織体でも、Q8において資産価値の評価を行った組織体は11．5%にとどまり、また資産価値の評価を行ったと回答した組織体でも、リスク分析を実施した組織体は17．6%にとどまり、リスク分析とは何か、何に対して分析するのかが確定していないことが見受けられる。

基幹システムの形態別では、リスク分析を行っていると回答した組織体のうち、システム形態として分散型をあげた組織体が、集中型、集中分散型をあげた組織体と比べて少なく、分散型システムでのリスク分析が未確立である等の影響が推測される。

基幹システムを国際的に展開・利用している組織体ではリスクに対する認識が高いと推測されたが、Q25とのクロス集計でも国際的に展開している組織体の方がそうでない場合と比べてリスク分析の実施率が高く、上記推測はある程度実証された。また、Q73とのクロス集計において、システミックリスクに対する認識とリスク分析との関係が強く認識できた。

リスク分析の実施がシステムダウンの発生(Q12)やコンピュータウイルスの感染(Q61)の低減に対して効果があるのでないかという仮説に対しては、それを裏づける明確な結果は今回のクロス集計からは得られなかったが、リスク分析を「行っていない」という回答に対するクロス集計の結果から、リスク分析の意味を指摘することができる。

Q46とのクロス集計では、ネットワーク障害に対するリスク分析においては、「LAN機器の障害」、「基幹LANの障害」、「通信事業者のケーブル障害」を重視しているのは、組織体のおかれた環境が反映していると思われる。

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。

コンピュータウイルスの被害にあった場合、被害届出機関である情報処理振興事業協会（IPA）に被害を届け出る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組織体であれば、被害を受けた際、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組織体がどれだけIPAのことを知っているのか、クロス集計を行った。

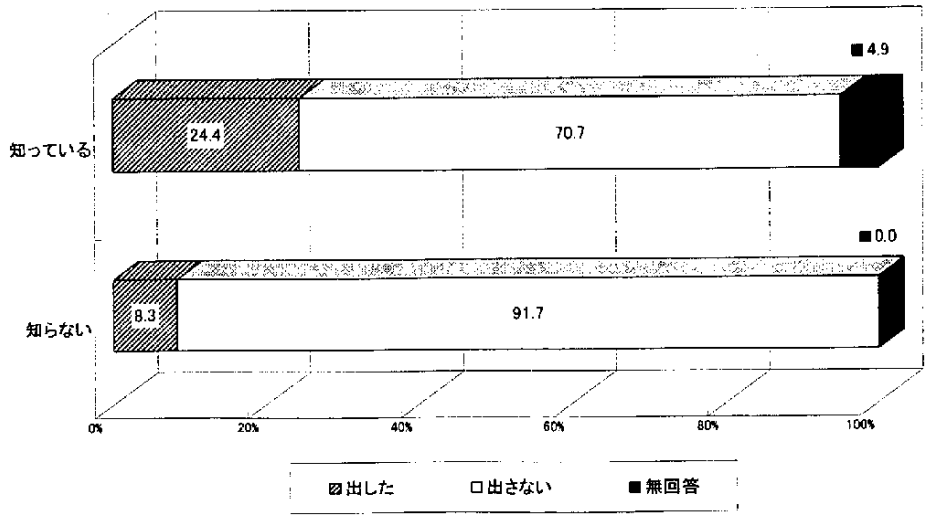
Q62. コンピュータウイルス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

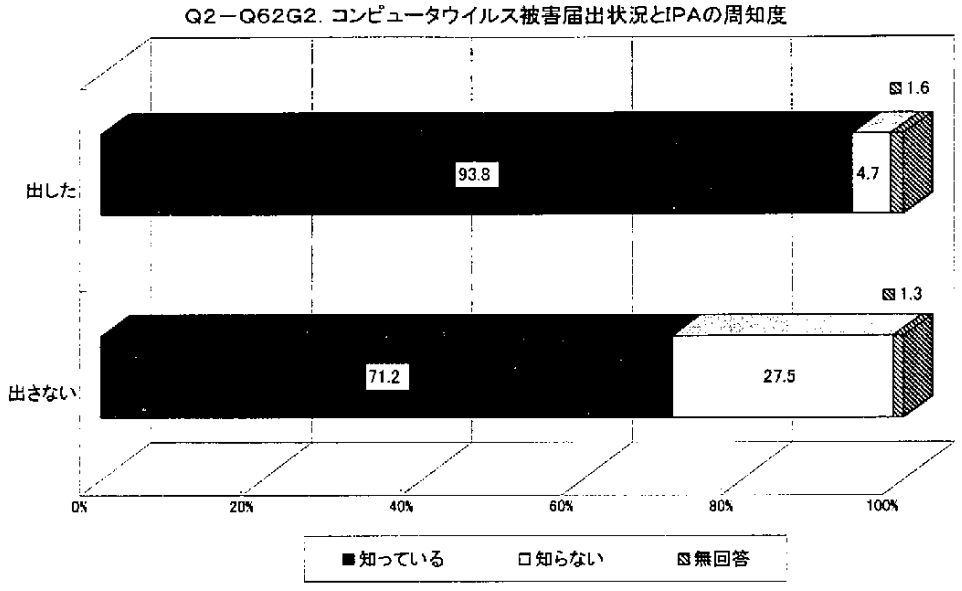
届出 / IPA	回答数	出した		出さない		無回答	
知っている	356件	60件	16.9%	277件	77.8%	19件	5.3%
知らない	111	3	2.7	107	96.4	1	0.9
無回答	6	1	16.7	5	83.3	0	0.0
計	473	64	13.5	389	82.2	20	4.2

IPA / 届出	回答数	知っている		知らない		無回答	
出した	64件	60件	93.8%	3件	4.7%	1件	1.6%
出さない	389	277	71.2	107	27.5	5	1.3
無回答	414	218	52.7	187	45.2	9	2.2
計	867	555	64.0	297	34.3	15	1.7

Q61でコンピュータウイルスの被害にあったと回答した473組織体のうち、IPAに被害を届け出たのは13．5%に過ぎない。Q2においてIPAがコンピュータウイルス被害届出機関と指定されていることに関してその周知度を調査した結果、「知っている」との回答が64．0%であるが、「知らない」と回答した組織体も34．3%存在した。IPAが被害届出機関であることが知られていないことが、被害届を出す組織体が少数にとどまる主な要因となっているならば、「知っている」と回答した組織体は「出した」と回答する傾向が強くなるはずである。

Q2−Q62G1. IPAの周知度に対するウイルス被害届出状況





クロス集計の結果、被害届を出していない組織体の71．2%がIPAが届出機関であることを知っており、届け出ない理由がPR不足以外にあることがわかる。

Q2-2. 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ますか。

コンピュータ不正アクセスの被害にあった場合、被害届出機関である情報処理振興事業協会(IPA)に被害を届け出る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組織体であれば、被害を受けた際、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組織体がどれだけIPAのことを知っているのか、クロス集計を行った。

Q50. 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。

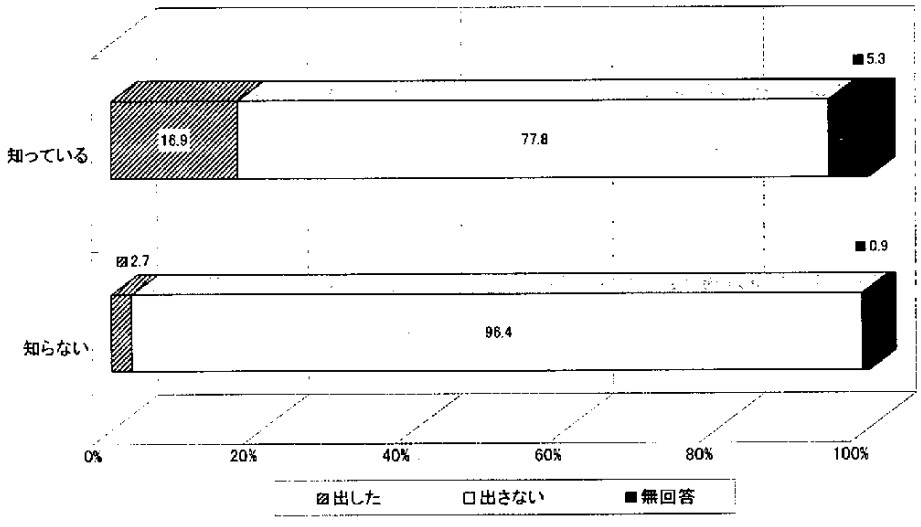
届出 / IPA	回答数	出した		出さない		無回答	
知っている	41件	10件	24.4%	29件	70.7%	2件	4.9%
知らない	12	1	8.3	11	91.7	0	0.0
無回答	0	0	0.0	0	0.0	0	0.0
計	53	11	20.8	40	75.5	2	3.8

IPA / 届出	回答数	知っている		知らない		無回答	
出した	11件	10件	90.9%	1	9.1%	0	0.0%
出さない	40	29	72.5	11	27.5	0	0.0
無回答	816	456	55.9	344	42.2	16	2.0
計	867	495	57.1	356	41.1	16	1.8

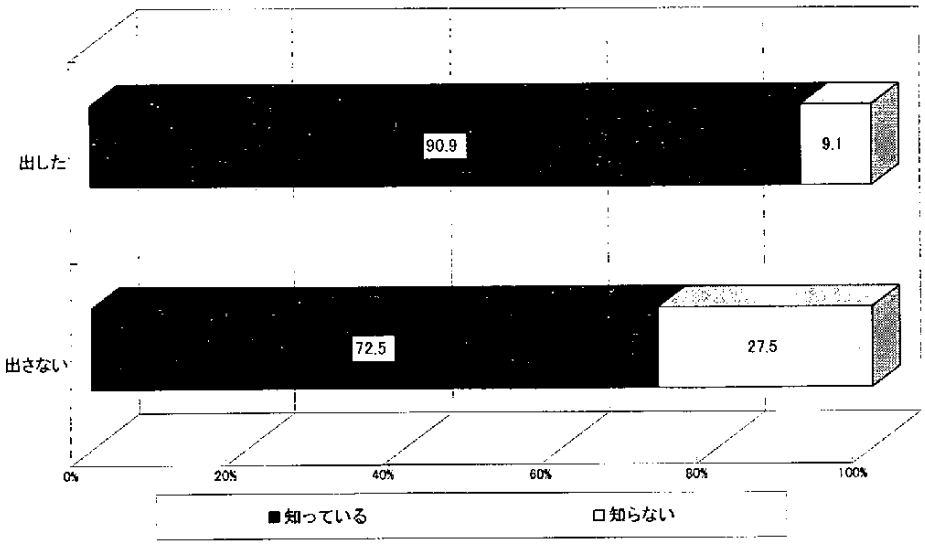
Q49で不正アクセスの被害にあったと回答した53組織体のうち、IPAに被害を届け出たのは20.8%に過ぎない。Q2において、IPAが不正アクセス被害届出機関と指定されていることに関してその周知度を調査した結果、「知っている」との回答が57.1%であるが、「知らない」と回答した組織体も41.1%存在した。IPAが不正アクセス被害届出機関であることが知られていないことが、被害届を出す組織体が少数にとどまる主な要因となっているならば、「知っている」と回答した組織体は「出した」と回答する傾向が強くなるはずである。

クロス集計の結果、「知っている」と回答した組織体においても「出した」と回答した組織体は24.4%にとどまり、被害を届け出る機関が少ない原因は、施策の周知度以外のところにある可能性が高い。

Q2－Q50G1. IPAの周知度に対する不正アクセス被害届出状況



Q2－Q50G2. 不正アクセス被害届出状況とIPAの周知度



3．3　Q3のクロス集計

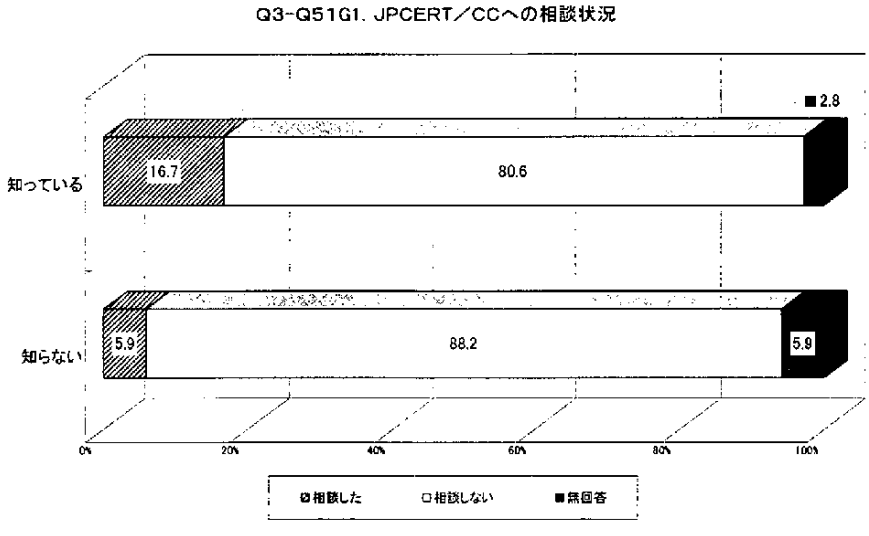
Q3. 不正アクセスの被害を受けた組織等から依頼を受けて、被害の実態調査、被害状況の侵入手口の分析、再発防止策の検討と助言を行う「JPCERT/CC(コンピュータ緊急対応センター)」を知っていますか。

コンピュータ不正アクセスの被害にあった場合、被害に対する相談、助言等を行う組織としてコンピュータ緊急対応センタ(JPCERT／CC)が平成8年から活動を行っている。JPCERT／CCの存在を知っている組織体であれば、被害を受けた際には相談、助言等を受けていると仮定した。そこで、JPCERT／CCの活動の周知度と、不正アクセスの被害にあったときに相談する割合についてクロス集計を行った。

Q51. 不正アクセスの被害にあたり、JPCERT/CC(コンピュータ緊急対応センタ)に相談しましたか。

相談 / JPCERT／CC	回答数	した		しない		無回答	
知っている	36件	6	16.7%	29	80.6%	1	2.8%
知らない	17	1	5.9	15	88.2	1	5.9
無回答	0	0	0.0	0	0.0	0	0.0
計	53	7	13.2	44	83.0	2	3.8

JPCERT／CC / 相談	回答数	知っている		知らない		無回答	
した	7件	6	85.7%	1	80.6%	0	0.0%
しない	4	29	65.9	15	88.2	0	0.0
無回答	816	249	30.5	549	0.0	18	2.2
計	867	284	32.8	565	83.0	18	2.1



Q3においてJPCERT／CCを知っていると回答した組織体は32．8%にとどまり、周知度が低いことが不正アクセス被害に遭ったときにJPCERT／CCに相談する割合が低いことに影響している可能性も考えられた。

クロス集計の結果、JPCERT／CCを知っていると回答した組織体においても、不正アクセス被害にあったときに相談した組織体は16．7%にとどまった。

3．4　Q4のクロス集計

Q4.「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。

Q86において、JIPDECの『プライバシーマーク制度』を「知っている」と回答した組織体は20．0%であり、77．3%が「知らない」と回答した要因について、『JIS Q 15001』の周知度との関連を分析した。

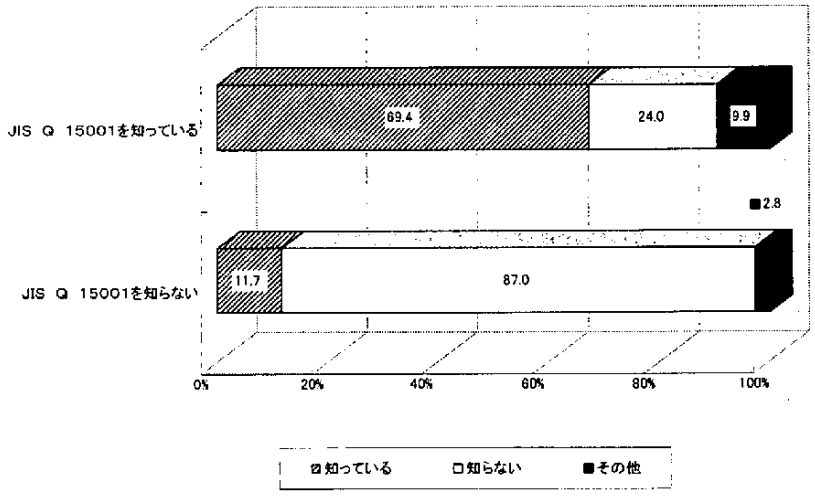
Q86.(財)日本情報処理開発協会の「プライバシーマーク制度(平成10年4月開始)」を知っていますか。(複数回答)

制度 / JIS Q 15001	回答数	知っている		知らない		その他	
知っている	121件	84件	69.4%	29件	24.0%	12件	9.9%
知らない	721	84	11.7	627	87.0	20	2.8
無回答	25	5	20.0	14	56.0	7	28.0
計	867	173	20.0	670	77.3	39	4.5

JIS Q 15001 / 制度	回答数	知っている		知らない		その他	
知っている	173件	84件	48.6%	84件	48.6%	5件	2.9%
知らない	670	29	4.3	627	93.6	14	2.1
その他	39	12	30.8	20	51.3	7	17.9
計	867	121	14.0	721	83.2	25	2.9

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

Q4−Q86G1. JIS Q 15001とプライバシーマーク制度の周知度



『JIS Q 15001』を「知っている」と回答した組織体において、『プライバシーマーク制度』を「知っている」と回答した組織体は69．4%、「知らない」と回答した組織体は24．0%である。また、『JIS Q 15001』を「知らない」と回答した組織体は、『プライバシーマーク制度』についても87．0%が「知らない」と回答しており、プライバシーに関する施策の周知度が『プライバシーマーク制度』の周知度に影響しているものと思われる。

3．5　Q5のクロス集計

Q5. ①ハードウェア、ソフトウェア、データを含む、現在稼働中の全情報システムへの総投資金額の概算を教えて下さい。

ハードウェア、ソフトウェア、データを含む全情報システムへの総投資金額はシステム利用に関する組織の脆弱性に関係し、情報セキュリティにかかわる方向性がみられると考えた。そこで、情報セキュリティの実態について、セキュリティポリシー・セキュリティガイドライン（業務処理手順、見直し等）の策定、ネットワーク管理者・管理責任者・セキュリティ担当者の設置状況を取り上げ、総投資金額との関係について以下の質問に関しそれぞれ仮説を立て、分析を行ってみることにした。

Q16. 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。
Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。
Q19. セキュリティガイドラインを定期的に見直していますか。
Q20. 基幹システムのネットワーク管理者を定めていますか。
Q21. 情報システムの管理責任者を定めていますか。
Q22. 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。

上記の質問とのクロス集計の結果から把握された傾向は以下のとおりである。

Q16. 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。

リスクマネジメントの視点からは、経営理念に基づいたセキュリティポリシーの存在は重要である。セキュリティポリシーにおいて利用している情報システムの脆弱性を確認することは不可欠な要素と考えられるからである。そこで、仮説として考えられたのは、情報システムへの投資金額が多いほどセキュリティポリシーを定めている割合が高いという特徴であった。

この点、セキュリティポリシーを「定めている」と回答した164件についてクロスをとったところ、次のような結果が得られた。

総投資金額	規模別回答数に対する割合		「定めている」(164 件)に対する割合(%)
	%	回答数／規模別回答数	
100億円以上	33.9	19/56	11.6
50億円以上～100億円未満	37.2	16/43	9.8
30億円以上～50億円未満	20.8	11/53	6.7
10億円以上～30億円未満	21.2	29/137	17.7
1億円以上～10億円未満	13.0	43/332	26.2
5千万円以上～1億円未満	12.0	9/75	5.5
5千万円未満	9.7	6/62	3.7

この点から、総投資金額によるクロスでみると、規模別回答数に対する割合からは総投資金額の多いところほどセキュリティポリシーを定めている割合が相対的に高いと思われる。しかし、「定めている」と回答した164件についてみると必ずしもそうした傾向がみられるとはいえないようであり、仮説が妥当であったとはいいがたい。

ところで、表に示していないが、「定めていない」とした回答については、総投資金額の低いところほど高い傾向がみられた。

Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。

総投資金額	規模別回答数に対する割合		「定めている」(242 件)に対する割合(%)
	%	回答数／規模別回答数	
100億円以上	48.2	27/56	11.2
50億円以上～100億円未満	60.5	26/43	10.7
30億円以上～50億円未満	35.8	19/53	7.9
10億円以上～30億円未満	29.9	41/137	16.9
1億円以上～10億円未満	22.0	73/332	30.2
5千万円以上～1億円未満	21.3	16/75	6.6
5千万円未満	11.3	7/62	2.9

セキュリティポリシーに基づいて規定されるセキュリティガイドラインとして操作および業務処理手順が示されているのが一般的である。そこで、上記と同様の仮説に立ち、情報システムへの総投資金額が多い組織体ほど操作および業務処理手順が定められていると考えた。

総投資金額によるクロスでは、「50億円以上～100億円未満」の組織体の割合が60．5%と高い。一般的には、総投資金額の多いところが相対的に操作および業務処理手順を「定めている」割合が高いといえる。「定めている」と回答した242件について総投資金額でみた場合、同様の傾向がみられるとはいいがたい。

しかしながら、「定めていない」とした回答については表で示していないが、総投資金額の低いところほど高い傾向がみられた。

Q19. セキュリティガイドラインを定期的に見直していますか。

総投資金額	規模別回答数に対する割合		「定めている」(131 件)に対する割合(%)
	%	回答数／規模別回答数	
100億円以上	70.4	19/27	14.5
50億円以上～100億円未満	61.5	16/26	12.2
30億円以上～50億円未満	47.4	9/19	6.9
10億円以上～30億円未満	65.9	27/41	20.6
1億円以上～10億円未満	42.5	31/73	23.7
5千万円以上～1億円未満	31.3	5/16	3.8
5千万円未満	57.1	4/7	3.1

既述のとおり、リスク環境の変化の著しい昨今、セキュリティポリシーに基づいて規定されるセキュリティガイドラインの定期的な見直しは不可欠といえる。前記同様の仮設に立ち、情報システムへの総投資金額が多い組織体ほどセキュリティガイドラインを定期的に見直していると考えた。

この点について、総投資金額でのクロスによると、「30億円以上～50億円未満」の回答の割合が相対的に47．4%と低く、総投資金額が低い「10億円以上～30億円未満」では逆に65．9%と高くなっている。だが、概して規模別回答数に対する割合からは総投資金額の多いところが相対的に高いといえる。しかし、「見直している」と回答した131件について総投資金額でみた場合、そのような傾向は確認できない。

しかしながら、「見直していない」とした回答については、「100億円以上」22．2%、「10億円以上～30億円未満」では29．3%と他に比べて低い結果となっているが、総投資金額の低いところほど相対的に高い傾向がみられた。

Q20．基幹システムのネットワーク管理者を定めていますか。

総投資金額	規模別回答数に対する割合		「定めている」(662 件)に対する割合(%)
	%	回答数／規模別回答数	
100億円以上	91.1	51/56	7.7
50億円以上～100億円未満	95.3	41/43	6.2
30億円以上～50億円未満	81.1	43/53	6.5
10億円以上～30億円未満	81.8	112/137	16.9
1億円以上～10億円未満	73.5	244/332	36.9
5千万円以上～1億円未満	68.0	51/75	7.7
5千万円未満	48.4	30/62	4.5

既述のとおり、ネットワーク環境に鑑みてネットワーク管理者を「定めている」のは全回答中76．4%の割合であり、「検討中」をあわせると約8割を超え、その存在は重要と思われる。そこで、上記同様に情報システムへの総投資金額が多い組織体ほどネットワーク管理者を定めている割合が高いと考えた。この点について全情報システムへの総投資金額でクロスをとったところ、「50億円以上～100億円未満」の規模別回答数に対する割合が95．3%と非常に高い割合を示している。全体的にみれば、総投資金額の規模に応じた割合になっていると思われ、仮説が検証されたように考えられた。しかし、ネットワーク管理者を「定めている」と回答した662件について捉えてみると、「1億円以上～10億円未満」の割合が36．9%と高く、総投資金額に応じた傾向とはなっていない。

しかしながら、「定めていない」とした114件の回答については、「1億円以上～10億円未満」が44．7%(回答数51件)と非常に高い割合となっていたが、総投資金額の低いところほど相対的に高い傾向がみられた。

Q21．情報システムの管理責任者を定めていますか。

総投資金額	規模別回答数に対する割合		「定めている」(754 件)に対する割合(%)
	%	回答数／規模別回答数	
100億円以上	91.1	51/56	6.8
50億円以上～100億円未満	97.7	42/43	5.6
30億円以上～50億円未満	88.7	47/53	6.2
10億円以上～30億円未満	88.3	121/137	16.0
1億円以上～10億円未満	85.5	284/332	37.7
5千万円以上～1億円未満	86.7	65/75	8.6
5千万円未満	67.7	42/62	5.6

ここでは、情報システムへの総投資金額が多い組織体ほど情報システムの管理責任者を定めている割合が高いという仮設を立ててみた。情報システムの管理者については、「定めている」のは全回答中87．0%と高く、「現在検討中」をあわせると9割を超えている。そこで、この点について、総投資金額でクロスをとり、規模別回答数に対する割合からみると、「50億円以上～100億円未満」の場合、97．7%と非常に高い割合を示しており、相対的に総投資金額に応じた割合となっている。しかし、「定めている」と回答した754件について総投資金額でみた場合、「1億円以上～10億円未満」の割合が前記同様に37．7%と高く、必ずしも総投資金額に応じた傾向はみられない。

しかしながら、「定めていない」とした53件の回答については、「1億円以上～10億円未満」が41．5%（回答数22件）と高い割合となっていた。

Q22．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。

総投資金額	規模別回答数に対する割合		「定めている」(206 件)に対する割合(%)
	%	回答数／規模別回総数	
100億円以上	28.6	16/56	7.8
50億円以上～100億円未満	34.9	15/43	7.3
30億円以上～50億円未満	15.1	8/53	3.9
10億円以上～30億円未満	19.7	27/137	13.1
1億円以上～10億円未満	23.2	77/332	37.4
5千万円以上～1億円未満	21.3	16/75	7.8
5千万円未満	19.4	12/62	5.8

当該質問に対しては、情報システムへの総投資金額が多い組織体ほど、当然専任のセキュリティ管理者または担当者がいるはずであるという推論に基づき仮設を立て、検証を試みようとした。しかし、専任のセキュリティ管理者なり担当者については、「定めている」と回答したのは23．8%と低く、「設置を検討している」をあわせても36．3%であった。この点について、総投資金額でクロスしたところ、相対的に高い割合を示しているのは「50億円以上～100億円未満」の組織体（34．9%）で、総投資金額に応じた傾向は必ずしもみられなかった。「定めている」と回答した206件について総投資金額でみた場合、「1億円以上～10億円未満」の割合が37．4%と高く、総投資金額に応じた傾向とはなっていない。

しかしながら、管理者または担当者が「いない」と回答した539件については、総投資金額の低い順で高い割合となっていた。

3．6　Q11のクロス集計

Q11. 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みられるかを検証するために、Q11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。

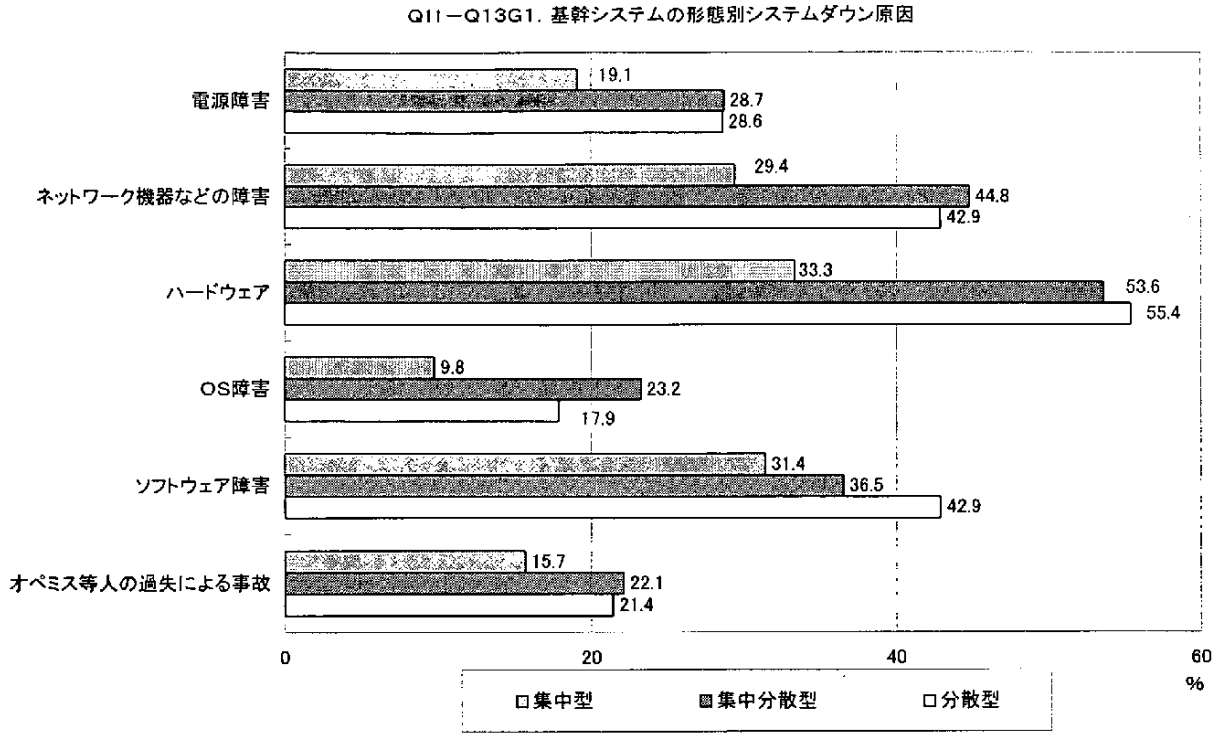
Q13. 過去1年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。
Q14. 基幹システムにおけるMTBF(平均故障間隔)は何時間ですか。
Q15. 基幹システムにおけるMTTR(平均修理時間)は何分ですか。
Q16. 貴社では経営理念に基づくセキュリティポリシーを定めていますか。
Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。
Q19. セキュリティガイドラインを定期的に見直していますか。
Q20. 基幹システムのネットワーク管理者を定めていますか。
Q21. 情報システムの管理責任者を定めていますか。
Q22. 貴社には専任のセキュリティ管理者または担当者がいますか。
Q32. 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。
Q34. ①情報システムのバックアップ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。
Q36. ①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。
Q38. ①ファイルのバックアップ対策はどのようなものですか。実施している対策項目を選んで下さい。
Q45. システム災害・障害対策についての問題点は何ですか。
Q46. 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。
Q59. 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、Q13、Q16、Q22、Q34、Q36、Q38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1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1つのグループを作るといったことがみられた。

Q13. 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)

	集中型	集中分散型	分散型
電源障害	19.1%	28.7%	28.6%
ネットワーク機器などの障害	29.4	44.8	42.9
ハードウェア	33.3	53.6	55.4
OS障害	9.8	23.2	17.9
ソフトウェア障害	31.4	36.5	42.9
オペミス等人の過失による事故	15.7	22.1	21.4

システムダウンの原因として多くあげられた主要項目で、システム形態により顕著な差がみられるのは、電源障害／ネットワーク機器などの障害／ハードウェア／OS障害／ソフトウェア障害／オペミス等人の過失による事故等の6項目である。



まず、集中型は従来からのデータセンタでの運用が多く、すべて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してあげられた数が少なかった。特に「電源障害」、「ネットワーク」、「ハードウェア」については、集中分散型と分散型がほぼ同じ数値なのに対し、3／5から3／4に少なくなっている。これは、たとえば「電源障害」に対する無停電装置の設置といった対策の実施や「ハードウェア」にみられるように、もともとの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込みをするかが結果として出てきており、集中型／集中分散型／分散型の順で多くなっている。「オペミス」等は運用の実績が長い集中型が最もよく、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、集中分散型や分散型についても、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。

Q14. 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（時間）	2,806.0	2,763.3	2,650.4

システム形態別にMTBFの平均時間をとると、上の表のようになった。時間的には、集中型／集中分散型／分散型の順に短くなっており、予想される結果である。特に、MTBFが10,000時間を超える領域になると、集中型で1件、集中分散型で1件、分散型ではゼロと大きな差になっている。しかし、平均値でみると集中型と分散型の差は5．6%であり、Q13の障害原因としてあげられた項目での数値よりは差が少なくなっている。これは、質問で障害の程度を特に限定しなかったため、比較的規模の大きい集中型での一部機能の障害も、全体障害もMTBFを計算するうえで同じように取り扱われてしまったためと考えられる。

Q15. 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448件)

	集中型	集中分散型	分散型
平均 MTTR(分)	124.5	133.6	125.4

システム形態別にMTTRの平均時間をとると、上の表のようになった。各形態とも平均すると2時間程度と考えられる。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。

Q16. 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。

	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	18.4%	18.7%	22.6%
セキュリティポリシーを作成中である	7.7	12.4	7.5

システム形態別にセキュリティポリシーの策定状況をみると、管理レベルが高いと思われる集中型よりも、ネットワークの利用が多い集中分散型や分散型の方がセキュリティーポリシーに積極的に取り組んでいる。「すでに定めている」と「現在作成中」をあわせると、集中分散型と分散型がほぼ同じ数字になるのに対して、集中型は約4%程度低くなっている。

Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。

	集中型	集中分散型	分散型
定めている	29.0%	27.8%	24.5%
作成中である	5.6	10.6	11.3

システム形態別に、セキュリティガイドラインとしての操作および業務処理手順の策定状況をみると、「すでに定めている」のは分散型／集中分散型／集中型の順に多くなっているが、「作成中」とあわせた割合で考えるとどのグループも約35%程度になり、大きな差はない。それよりも、Q16でセキュリティポリシーを定めている組織体が18．9%しかないのに、セキュリティガイドラインを定めている組織体が27．9%あり、この差の9%は、セキュリティポリシーなしでセキュリティガイドラインを定めていることになる。また、セキュリティポリシーがあってもセキュリティガイドラインがない組織体があれば、この差はもっと大きくなる。今後、セキュリティポリシーの検討を各組織体が行うように、雛形の作成等の推進策を実行すべきである。

Q19. セキュリティガイドライン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	55.0%	53.3%	57.7%

システム形態別に、セキュリティガイドラインを定期的に見直しているかをみると、各形態別に大きな差はみられなかった。

Q20. 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	73.4%	80.1%	76.4%
現在検討中である	4.3	5.1	6.6

基幹システムのネットワーク管理者の策定状況をみると、ネットワークに依存する率が高い集中分散型と分散型が高くなっている。しかし、集中型でもすでに73．4%が定めているので、顕著な差はない。運用管理者がネットワーク管理者を兼ねている場合等もあるので、質問で機能的な面をもっと詳しく規定しないと、回答者が適切な回答が出せない可能性がある。

Q21. 情報システムの管理責任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	86.5%	90.0%	80.2%
現在検討中である	3.6	2.7	3.8

情報システムの管理責任者の策定状況をみると、大半の組織体がすでに定めている。「定めていない」または「必要ない」と回答した組織体もあるが、質問で機能をもっと詳しく規定しないと、組織体の名称等により適切な回答ができなかった可能性がある。

Q22. 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。

	集中型	集中分散型	分散型
いる	21.0%	24.8%	31.1%
設置を検討している	8.7	16.6	13.2

専任のセキュリティ管理者または担当者の策定状況をみると、ネットワーク利用の多い分散型と集中分散型で設置されている数字が大きくなっている。その数字の絶対値は小さく、今後E－ビジネスの導入とともにセキュリティ管理者を配置する組織体が増えることが予想される。しかし企業規模によっては、専任のセキュリティ管理者を置くことが難しい場合もあるので、意思決定を自社で行い、実作業をアウトソーシングすることも検討すべきである。

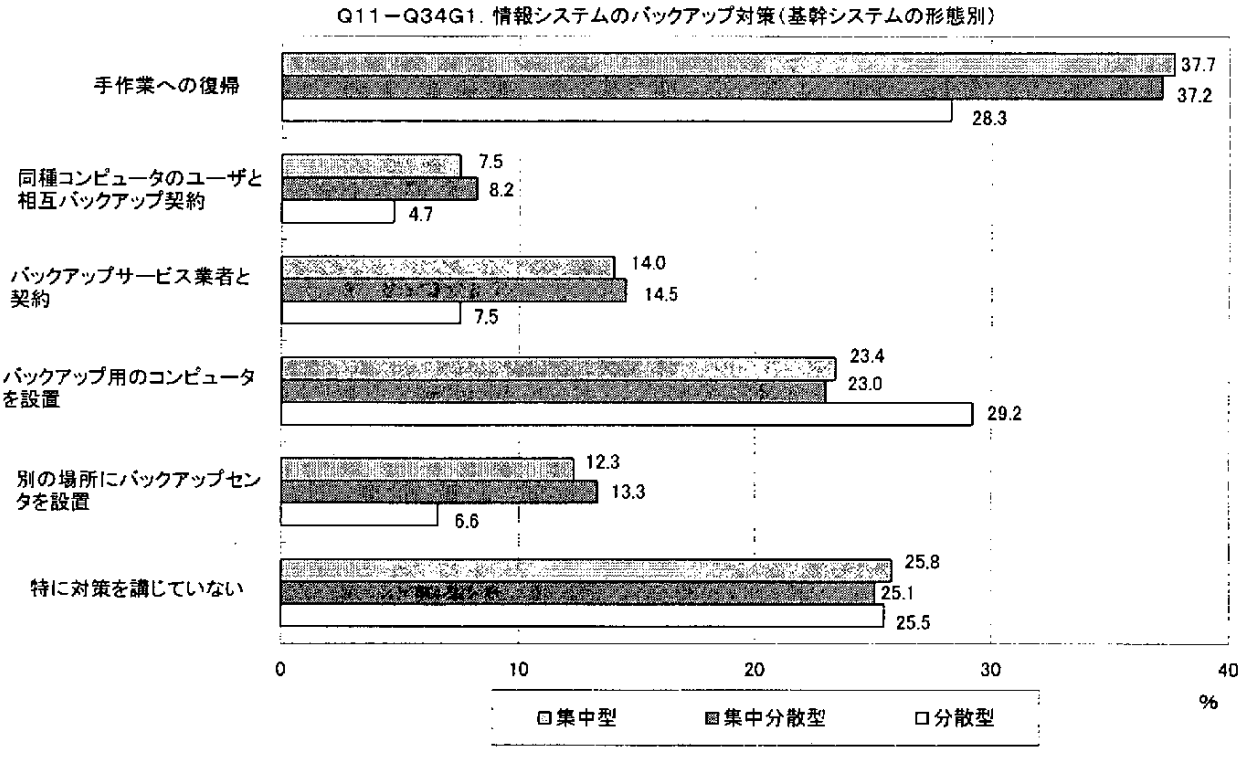
Q32. 非常事態に備えて従業員に対してセキュリティの面から訓練を実施していますか。

	集中型	集中分散型	分散型
危機管理マニュアルに従って定期的に実施	6.3%	5.4%	0.9%
危機管理マニュアルに従って時々実施	8.0	12.4	6.6
危機管理マニュアルはないが実施	6.5	7.3	7.5

非常事態に備えたコンティンジェンシー計画も、実際にテストを行っていないと絵に描いた餅になっている危険性がある。今回の調査では、危機管理マニュアルがある組織体の約45%しか訓練を実施していなかった。コンティンジェンシー計画を実施可能なものにするためには、定期的に訓練を実施してその結果を計画に反映していくことが必要である。

Q34. ①情報システムのバックアップ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	37.7%	37.2%	28.3%
同種コンピュータのユーザと相互バックアップ契約	7.5	8.2	4.7
バックアップサービス業者と契約	14.0	14.5	7.5
バックアップ用のコンピュータを設置	23.4	23.0	29.2
別の場所にバックアップセンタを設置	12.3	13.3	6.6
特に対策を講じていない	25.8	25.1	25.5



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3／4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体で採用されており、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ユーザ間の「相互バックアップ契約／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の設置」も、集中型と集中分散型で多く、分散型をとる組織体での対応が遅れている。分散型では、同一施設内にバックアップ用のコンピュータを持っている割合が集中型や集中分散型よりも多く、同一施設内でのバックアップでハードウェアの障害には対応しようとしている。

Q36. ①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
デュプレックスシステム	13.8%	9.1%	5.7%
ホットスタンバイシステム	12.6	14.5	5.7
ミラリング	24.9	39.0	39.6

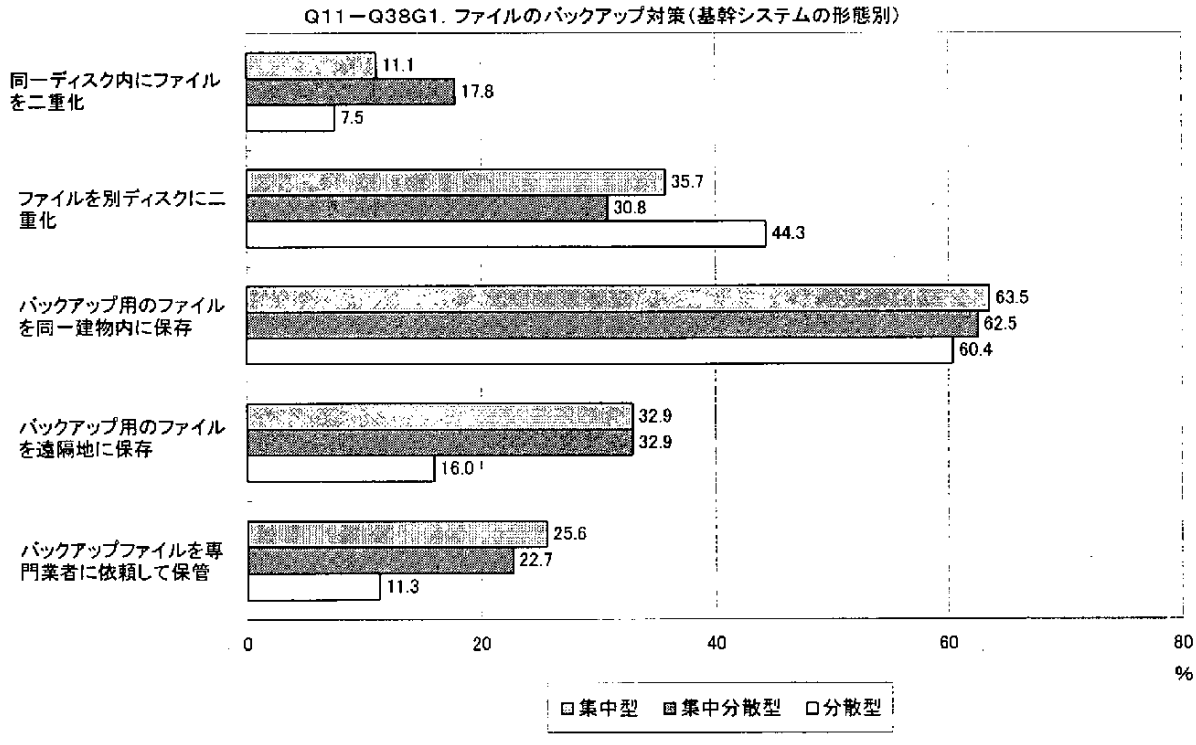
情報システムの代替運転機能として何が使えるかは、ハードウェアやOSに依存するところが大きい。「デュプレックスシステム」や「ホットスタンバイシステム」が、分散型よりも集中型／集中分散型で実施されている例が多いのは、ハードウェアとOSの機能性による。

一方、「ディスクのミラリング」については、集中分散型／分散型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。

（代替運転機能の用語定義をつけなかったため、デュアルシステム、高可用性機構、フォールトトレラントといった用語の定義が曖昧で、自社のシステム構成がどれに該当するのか戸惑った回答者が多かったことが懸念される。特に、商業的には非常に少ないデュアルシステムの回答が多かったのは、用語の定義の必要性を示唆している。）

Q38. ①ファイルのバックアップ対策はどのようなものですか。実施している対策項目を選んで下さい。

	集中型	集中分散型	分散型
同一ディスク内にファイルを二重化	11.1%	17.8%	7.5%
ファイルを別ディスクに二重化	35.7	30.8	44.3
バックアップ用のファイルを同一建物内に保存	63.5	62.5	60.4
バックアップ用のファイルを遠隔地に保存	32.9	32.9	16.0
バックアップファイルを専門業者に依頼して保管	25.6	22.7	11.3



ファイルのバックアップ対策として、ディスク装置の障害対策とディザスター対応の2種類を考える必要がある。ディスクの障害対策としては、ファイルの二重化やテープ等によるバックアップが考えられる。

「ファイルの二重化」については、同一ディスクか別ディスクかの違いはあるが、半数近くの組織体が実施している。分散型で別ディスクでの二重化が多いのは、ディスク装置の価格が集中型に比べて安いためと思われる。また、「バックアップ用ファイルを同一建物内に保存」も6割程度の組織体が実施しており、システム形態による差は少ない。

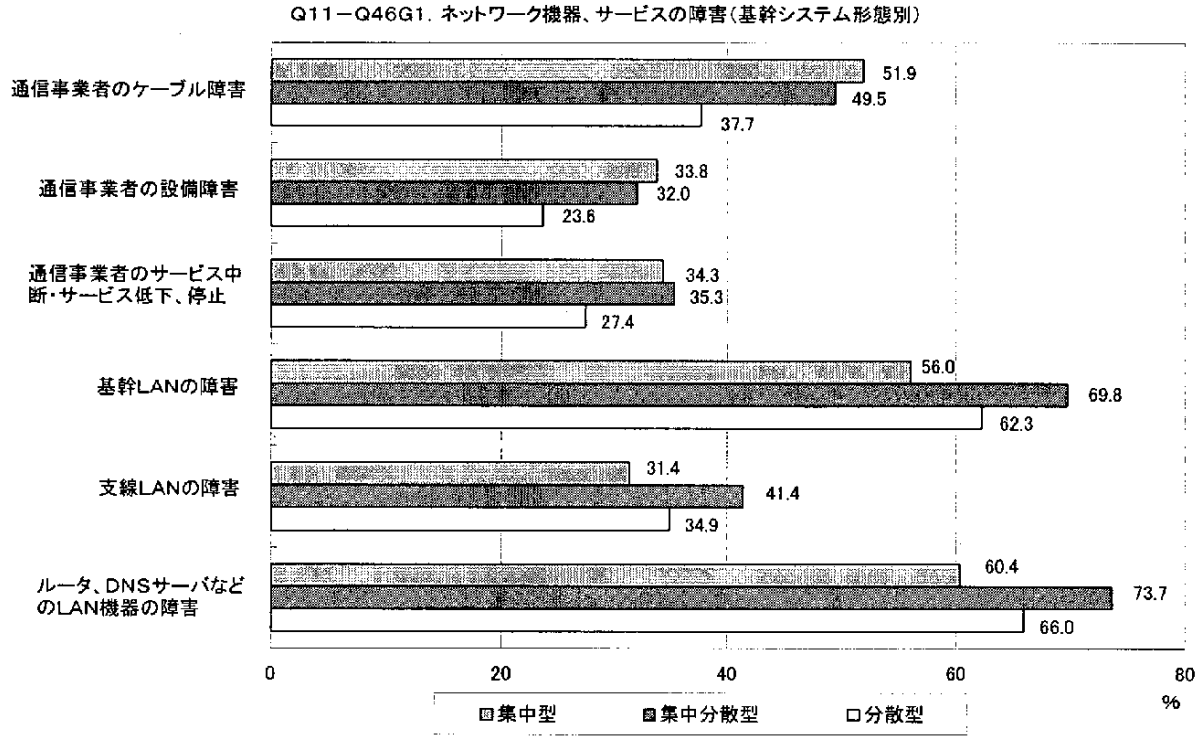
一方、集中型／集中分散型と分散型で顕著に差が出たのは、ディザスターへの対応である。「ファイルの遠隔地保管」や「専門業者への依頼」をみると、集中型／集中分散型と分散型で実施率に倍以上の開きがあり、ディザスターへの対応に大きな差があることがわかる。

Q45. 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)

この質問については、システムの形態による差がほとんどみられなかった。集中型／集中分散型／分散型のいずれにおいても「コスト」、「どこまでやるかの基準」、「ノウハウ不足」、「要員の作業負荷」、「教育訓練」が共通の問題となっている。

Q46. 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)

	集中型	集中分散型	分散型
通信事業者のケーブル障害	51.9%	49.5%	37.7%
通信事業者の設備障害	33.8	32.0	23.6
通信事業者のサービス中断・サービス低下、停止	34.3	35.3	27.4
基幹LANの障害	56.0	69.8	62.3
支線LANの障害	31.4	41.4	34.9
ルータ、DNSサーバなどのLAN機器の障害	60.4	73.7	66.0



ネットワーク関連の障害について何を想定するかでは、通信業者の障害を想定する割合が、集中型／集中分散型が分散型よりも高かった。一方LANや通信機器の障害については、集中分散型が集中型／分散型よりも高かった。これは、集中サーバと分散サーバ間の伝送料が大きく、障害発生時の影響が大きいためと思われる。

Q59. 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	13.7%	19.6%	21.7%
セキュリティ教育を実施していない	83.3	80.1	78.3

不正アクセス対策についての教育・訓練は、分散型／集中分散型／集中型の順に実施率が高い。しかし、最も実施率の高い分散型でも21．7%であり、残りの78．3%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30%に比べても低く、早急な改善が必要である（Q65参照）。特に、今後のグローバルなシステム接続を考えると、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、セキュリティが不足していることを理由に取引きが拒絶されることも考えられる。

3．7　Q16のクロス集計

Q16．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？

セキュリティポリシーを経営理念に基づいて定めている組織体では、たとえば、「トップの関心が高くセキュリティ管理について定めていない組織体よりは進んでいる」、というようなことがいえるであろうか？すなわち、ここでは以下の仮説を立て、クロス集計により検証してみた。

①セキュリティ管理者、情報システムの管理責任者を設置している（Q20、Q21）
②緊急時の連絡体制は十分に取られており、データの日常の使用管理などが十分に行われている（Q.23、Q24）
③基幹システムを国際的に展開・利用している（Q25）
④非常時の発生を想定して危機管理に関するマニュアル類を作成している（Q30）
⑤自社が採用している災害対策に対して満足している（Q.33）
⑥ファイルのバックアップ対策を十分に実施している（Q38,Q40）
⑦コンピュータウイルス対策の問題点を持っている（Q66）
⑧経営者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（Q68）
⑨経営者はシステム監査を重要視している（Q75）

さらに、セキュリティポリシーを定めている組織体では、
⑩どのような情報システム形態が多いか（Q11）
⑪情報セキュリティ管理に関して、どのような悩みを持っているのか。そしてそれは従業員なのか、コストなのか、範囲なのか。これらは、セキュリティポリシーを定めていない組織体と比べて進んでいるといえるのか（Q28）
⑫不正サクセス対策に関して、どのような悩みを持っているのか。そしてそれは従業員なのか、コストなのか、範囲なのか。これらは、セキュリティポリシーを定めていない組織体と比べて進んでいるといえるのか（Q60）

結論的には、⑧と⑨はセキュリティポリシーとの相関がきわめて大きいことがわかった。また、①と②は、セキュリティポリシーを定めている組織体では定めている割合が高いことがわかった。しかし、逆は成立しない。一方、④、⑤、⑥、⑦については、セキュリティポリシーとの関係はないことがわかった。

形態としての⑩では、集中型、集中分散型と分散型で大きく分かれ、分散型でのセキュリティポリシーの採用が少ないことがわかった。また、③の国際展開に関しては、国際展開していない組織体はセキュリティポリシーを定めていないことがわかった。

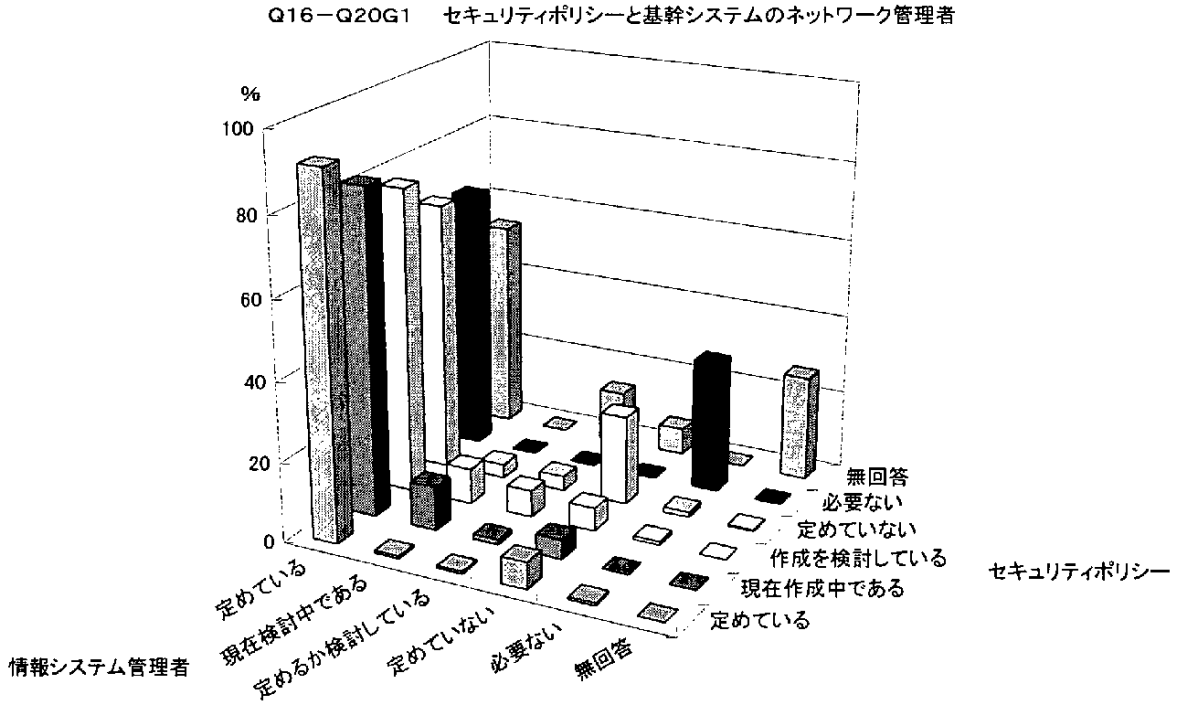
問題点では、情報セキュリティ管理、不正アクセス対策ともに、セキュリティポリシーを定めている組織体と定めていない組織体で大きく悩みの点が異なっていることがわかった。

以下に、分析の詳細を示す。

Q11．貴社の基幹システムはどのように運用されていますか。

セキュリティポリシーを「定めている」、「作成中」の割合と基幹システムの形態では、集中型では85．8%、集中分散型では88．4%と関連が高い。一方、分散型では24．5%と関連が低い。まだまだセキュリティポリシーに対しては集中型でのイメージが強いと考えられる。分散型では現場の管理に任せ、セキュリティポリシーと分けて考えているようにも見受けられる。ネットワークセキュリティがセキュリティポリシーの一部であることなどを今後PRしていく必要がある。

Q20. 基幹システムのネットワーク管理者を定めていますか。



セキュリティポリシーを定めている組織体では、91．5%が基幹システムのネットワーク管理者を定めている。これは、セキュリティポリシーでネットワーク管理者を定めているためと考えられる。一方、セキュリティポリシーを定めていない組織体でも68．7%が基幹システムのネットワーク管理者を定めている。したがって、セキュリティポリシーがなければ、組織体のネットワーク管理ができないというわけではない。

Q21. 情報システムの管理責任者を定めていますか。

セキュリティポリシーを定めている組織体では98．2%が情報システムの管理責任者を定めている。これは、セキュリティポリシーで情報システム管理責任者を定めているためと考えられる。一方、セキュリティポリシーを定めていない組織体でも84．1%が情報システムの管理責任者を定めている。したがって、セキュリティポリシーがなければ、組織体の情報システムの管理ができないというわけではない。ただし、管理責任者を定める以上、何らかのきまりや責任範囲の記述が必要であり、セキュリティポリシーが利用できる点を知ってもらう必要がある。

Q23. 緊急時の連絡手段を持っていますか。

セキュリティポリシーを定めている組織体では、89．6%が緊急時の連絡手段を定めている。これは、セキュリティポリシーで連絡手段を想定しているためと考えられる。一方、セキュリティポリシーを定めていない組織体でも69．8%が緊急時の連絡手段を定めている。したがって、セキュリティポリシーがなければ、緊急時連絡ができないわけではない。ただし、定める以上、セキュリティポリシーにまとめることを知ってもらう必要がある。

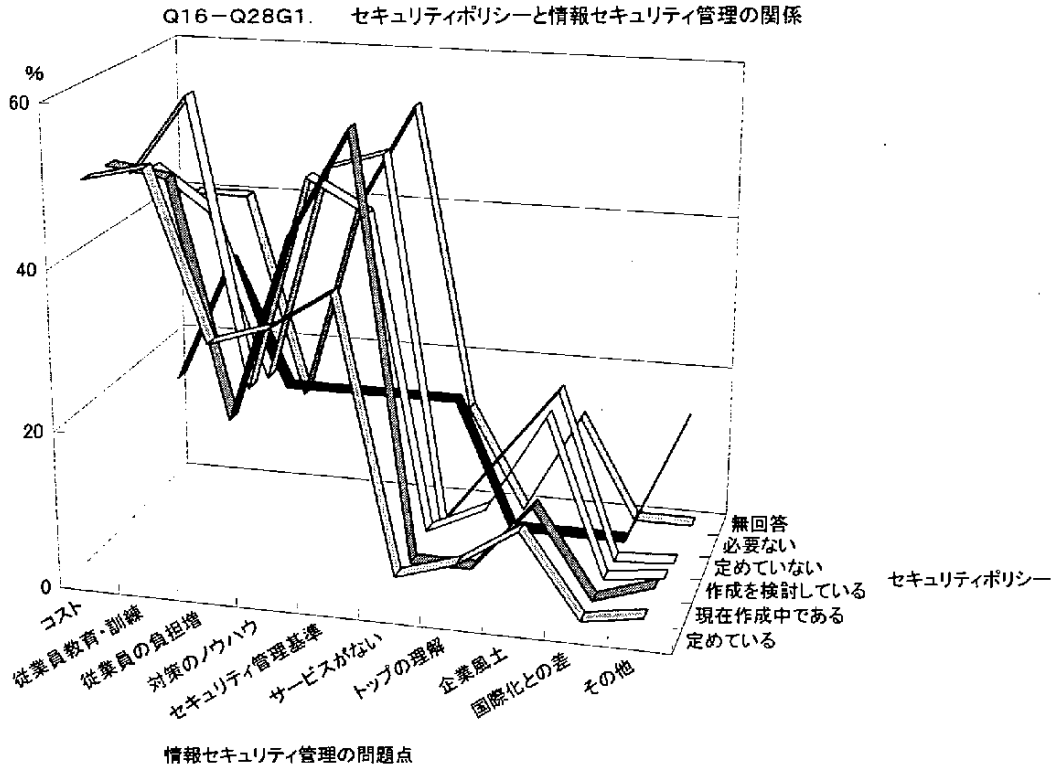
Q24. データの使用・保管等の管理を行っていますか。

セキュリティポリシーを定めている組織体では、95．7%がデータの使用・保管の管理を行っている。これは、セキュリティポリシーでデータの管理に関して規定しているためと考えられる。一方、セキュリティポリシーを定めていない組織体でも86．2%がデータの使用・保管等の管理を行っている。したがって、セキュリティポリシーがなければデータの使用・保管の管理が適切にできないというわけではない。ただし、データの使用・保管の管理をセキュリティポリシーの中に位置づけて、適切に管理することを知ってもらう必要がある。

Q25. 基幹システムを国際的に展開・利用していますか。

国際的に展開している組織体では、セキュリティポリシーを「定めている」、「作成中である」、「作成を検討している」をあわせると約30%となる。国際的に展開する以上、統一的なネットワークや情報システムを規定するポリシーが必要と考えられる。また、外国籍の社員に理解させるためにも都合がよい。ただし、国際展開していないところの96．8%がセキュリティポリシーを定めていない。今後、組織体のグローバル展開をきっかけに、セキュリティポリシーを制定するところが増えてくると考えられる。

Q28. 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)



セキュリティポリシーの有無に限らず共通する問題点として、「コストがかかりすぎる」、「従業員に対する教育・訓練が行き届かない」、「セキュリティ対策を構築するノウハウ不足」、「どこまでやるかの範囲に関する基準」の4つの点があげられる。ただし、セキュリティポリシーの制定状況によって、細かく順位が変わっている。

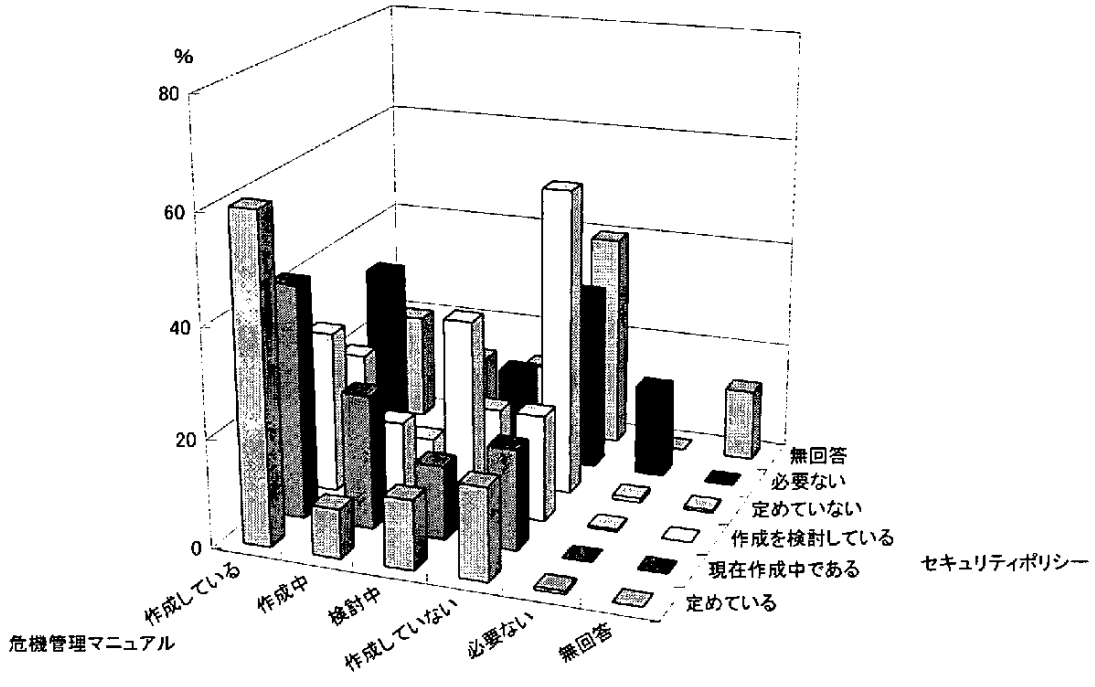
すなわち、セキュリティポリシーを定めている組織体では、①教育・訓練(52．4%)、②コスト(50．6%)、③範囲の基準(39%)の順となっている。一方、現在セキュリティポリシーを作成中の組織体では、①範囲の基準(56．8%)、②コスト(50．6%)、③教育・訓練(49．4%)となっている。さらに、作成を検討している組織体では、①教育・訓練(58%)、②ノウハウ不足(48．7%)、③コスト(47．8%)となっている。セキュリティポリシーを定めていない組織体では、①範囲の基準(50．4%)、②ノウハウ不足(48．0%)、③コスト(46．9%)、となっている。

セキュリティポリシーを「定めている」、「作成中」の組織体では、セキュリティ対策を講じるノウハウなどの蓄積があるものの、従業員にセキュリティポリシーを周知徹底すること、セキュリティポリシーの対象をどこまで広げていくか、が大きい問題となっている。一方、セキュリティポリシーを定めていない組織体では、情報セキュリティに関するノウハウ・範囲などで困っていることがわかる。したがって、これらの組織体では、今後、セキュリティ対策を実施していくなかで、情報セキュリティのノウハウを蓄積し、これが集大成された段階でセキュリティポリシーを定めるパスを考えると効率的ではないだろうか。

本質問のなかで注目に値するものとして、「トップの理解が得られない」ことを問題にしている組織体のなかでは、セキュリティポリシーを定めていないところがもっとも多い。すなわち、セキュリティポリシーが定められていることが情報セキュリティ管理に対するトップの理解にもつながっているといえよう。

Q30. 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。

Q16－Q30G1. セキュリティポリシーと危機管理マニュアル



セキュリティポリシーの作成状況と危機管理のマニュアル類の作成とは相関が強い。すなわち、セキュリティポリシーを定めている組織体では60．4%が危機管理のマニュアル類を作成している。一方、セキュリティポリシーを定めていない組織体では56．8%が危機管理のマニュアル類を作成していない。

多くの組織体が、セキュリティポリシーの中で危機管理に関しても検討している姿がうかがえる。

Q33. 貴社でとられている災害・障害対策は、全体的にみて満足できるものですか。

セキュリティポリシーと災害・障害対策の満足度とは相関がほとんどみられない。すなわち、セキュリティポリシーでは、災害対策の必要性、行動基準を示すが、具体的な対策を明記することが少なく、別途、災害・障害対策のマニュアルが必要となっているためと考えられる。

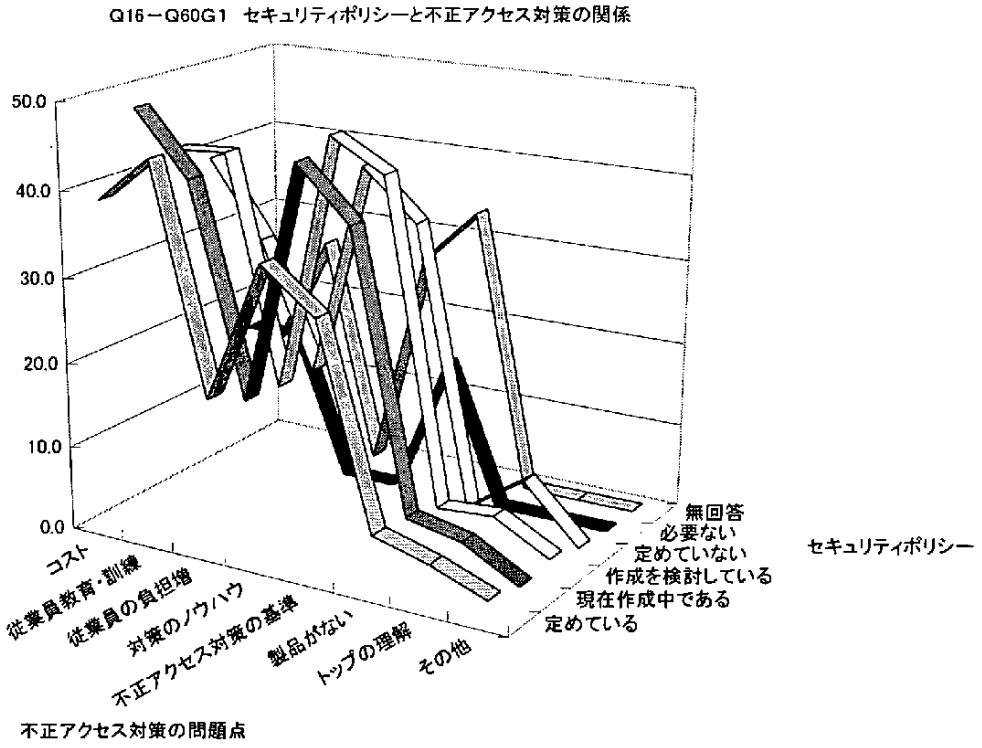
Q38. ①ファイルのバックアップ対策はどのようなものですか。実施している対策項目を選んで下さい。

セキュリティポリシーを「定めている」、「定めていない」に限らず、バックアップ対策には差異がみられない。すなわち、セキュリティポリシーとファイルのバックアップ対策には明確な相関がない。前項と同様に、セキュリティポリシーでは、バックアップ対策の必要性、行動基準を示すが、具体的な対策を明記することが少なく、別途、対策のマニュアルが必要となっているためと考えられる。

Q40. 貴社の基幹システムはどれぐらいの頻度でファイル等のバックアップを実施していますか。

セキュリティポリシーを「定めている」、「定めていない」に限らず、基幹システムのバックアップ頻度には差異がみられない。すなわち、セキュリティポリシーではバックアップ対策の必要性、行動基準を示すが、具体的な対策を明記することが少なく、別途、対策のマニュアルが必要となっているためと考えられる。これは、日本企業の多くが、現場のセキュリティ対策を積み上げた形でセキュリティポリシーを定めており、欧米にみられるトップダウン型でセキュリティポリシーを定め、これを核にして各対策を制定していく体制との文化的・歴史的（セキュリティポリシーが対策よりも後に導入された）経緯によるものと考えられる。

Q60. 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）



セキュリティポリシーの有無に限らず共通する問題点として、「コストがかかりすぎる」、「従業員に対する教育・訓練が行き届かない」、「不正アクセス対策を構築するノウハウ不足」、「どこまでやるかの範囲に関する基準」の4つの点があげられる。ただし、Q28の情報セキュリティ管理と比較すると、セキュリティポリシーを「定めている」、「定めていない」によって問題点に明確な差はみられない。

すなわち、セキュリティポリシーを定めている組織体では、①教育・訓練(44．5%)、②コスト(39%)、③ノウハウ不足(34．8%)となっている。一方、現在セキュリティポリシーを作成中の組織体では、①コスト(48．1%)、②ノウハウ不足(44．4%)、③教育・訓練(40．7%)、となっている。さらに、作成を検討している組織体では、①ノウハウ不足(46．0%)、②教育・訓練(42．4%)、範囲に関する基準(42．4%)となっている。セキュリティポリシーを定めていない組織体では、①ノウハウ不足(41．1%)、②コスト(39．5%)、③範囲に関する基準(35．3%)となっている。

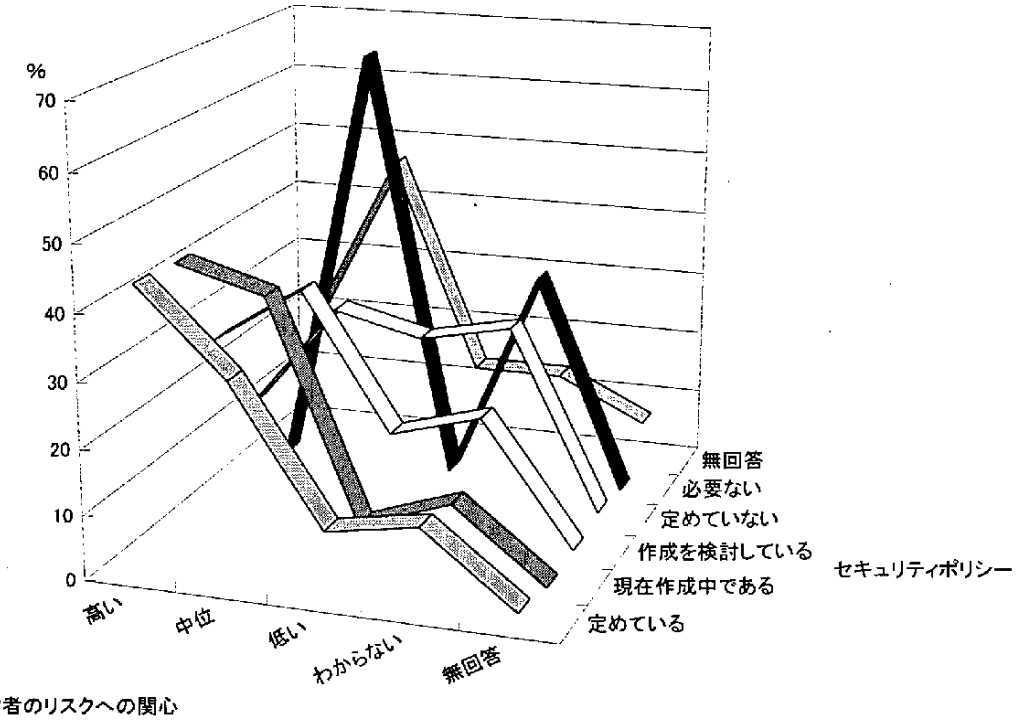
これは、不正対策がすばやく、具体的な対策をとることが重要であるので、各組織体とも、セキュリティポリシーのような概念ではなく、別途、具体的な対策のノウハウを必要とするためと考えられる。

Q66．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)

セキュリティポリシーを定めている、定めていないに限らず、コンピュータウイルス対策の問題点には差異がみられない。すべて「コストがかかること」、「従業員に対する教育・訓練」が問題点となっていて、割合にも差がみられない。すなわち、セキュリティポリシーとウイルス対策の問題点とは独立している。Q33、Q38と同様に、セキュリティポリシーではウイルス対策の必要性、行動基準を示すが、具体的な個々の対策、感染後の対策など明記することが少ないためと考えられる。Q33、Q38と同様に、別途の対策が必要になると考えられる。

Q68．経営者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。

Q16－Q68G1．セキュリティポリシーと経営者のリスクへの関心



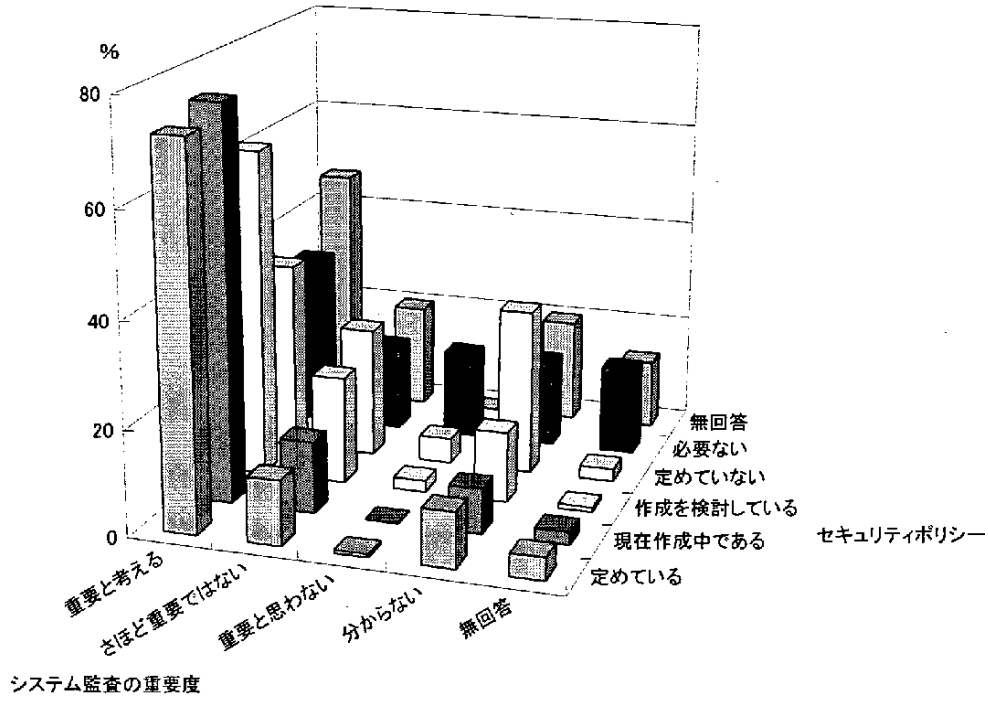
セキュリティポリシーが定められている組織体では、経営者のコンピュータ関連の事件・事故に対するリスクへの関心が高い(「定めている」43．9%、「作成中」43．2%)。一方、「作成を検討中」と「定めていない」と回答した組織体ではリスクへの関心は高くなく、中位となっている(「検討中」36．6%、「定めていない」29．7%)。すなわち、セキュリティポリシーが定められている組織体では、セキュリティポリシーが経営者のリスク判断に役立っているといえよう。

Q75．経営上、システム監査をどう考えていますか。

セキュリティポリシーを「定めている」と回答したうちの72．6%、「現在作成中」の75．3%、「作成を検討中」では62．9%の組織体がシステム監査を重要と考えている。以上のことから、セキュリティポリシーを定めている組織体では、システム監査を重要と考えていることがわかる。

一方、セキュリティポリシーを「定めていない」と回答した377組織体のうち36．3%しかシステム監査を重要とは考えず、また、31．6%は「わからない」と回答している。今後、セキュリティポリシーの重要性、リスク管理の必要性などとあわせて経営者を教育していく必要がある。

Q16－Q75G1．セキュリティポリシーとシステム監査の重要度



3．8　Q67のクロス集計

Q67. 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)

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」、「法規制の理解」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、これらの重要な視点の認識との間にどのような傾向があるか分析した。分析にあたっては下記の各項目とクロス集計を行った。

Q5.　①ハードウェア、ソフトウェア、データを含む、現在稼働中の全情報システムへの総投資金額の概算を教えて下さい。
Q8.　情報システムの資産評価をしたことがありますか。
Q20. 基幹システムのネットワーク管理者を定めていますか。
Q21. 情報システムの管理責任者を定めていますか。
Q22. 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。
Q25. 基幹システムを国際的に展開・利用していますか。
Q30. 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。
Q32. 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。
Q33. 貴社でとられている災害・障害対策は全社的にみて満足できるものですか
Q69. 情報システムに関わるリスク分析を実施していますか
Q74. 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。

仮説として「経営者の理解」をあげたところほど情報セキュリティの確保が実際に進んでいるのではないかと考えた。分析にあたっては、複数回答を得る設問であったため、各回答が全体の回答数の何パーセントを占めるかという割合を算出して行った。

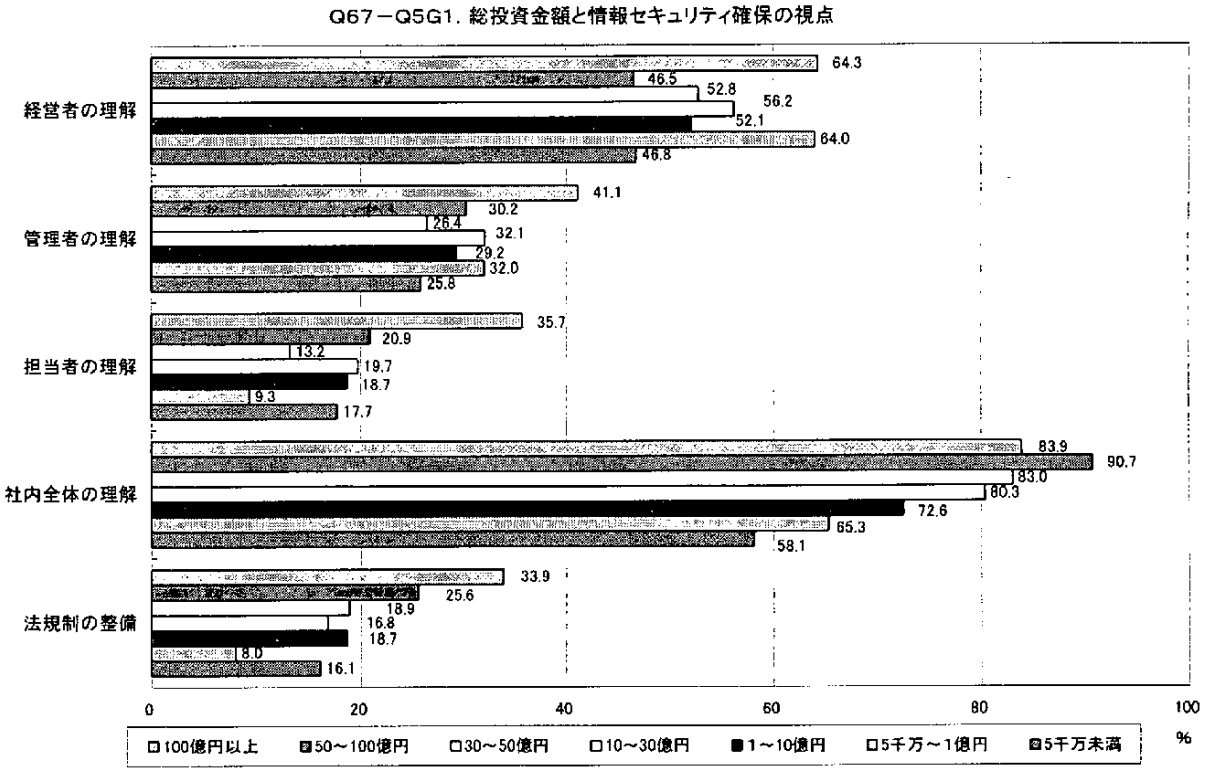
結論として、「経営者の理解」、「管理者の理解」、「担当者の理解」、「社内全体の理解」、「法規制の理解」のそれぞれの回答率の傾向は、クロス集計の各項目ごとに比較してもほとんど差がなかった。多くの場合、回答率の高い項目から「社内全体の理解」>「経営者の理解」>「管理者の理解」>「担当者の理解」=「法規制の整備」の順であった。

しかしながら、実際のセキュリティ確保のための諸施策の実施状況の有無での比較を行うと、各設問とも「管理者」を定めたり、「訓練を実施」したりなど具体的な対応を実施している組織体の方が実施していない組織体より、それぞれの回答率がいずれも高い傾向を示している。

結論として、仮説である「経営者の理解」を重要な視点として認識している組織体ほど情報セキュリティの確保が高いということはいえない。しかし実態として、情報セキュリティ確保の諸施策を実施している組織体ほど、全体として情報セキュリティへの認識度が高いことを表している。現状では「社内全体の理解が重要」という経営者と従業員が一体となって認識されている日本的経営観が情報セキュリティ面でもうかがわれ、経営者としての責任に対する認識度より、実際の情報セキュリティ確保の運用面での困難さの認識を反映した回答となっているものと思われる。

Q5. ①ハードウェア、ソフトウェア、データを含む、現在稼働中の全情報システムへの総投資金額の概算を教えて下さい。

	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
100億円以上	64.3%	41.1%	35.7%	83.9%	33.9%
50～100億円	46.5	30.2	20.9	90.7	25.6
30～50億円	52.8	26.4	13.2	83.0	18.9
10～30億円	56.2	32.1	19.7	80.3	16.8
1～10億円	52.1	29.2	18.7	72.6	18.7
5千万～1億円	64.0	32.0	9.3	65.3	8.0
5千万未満	46.8	25.8	17.7	58.1	16.1
無回答	50.5	30.3	25.7	76.1	27.5

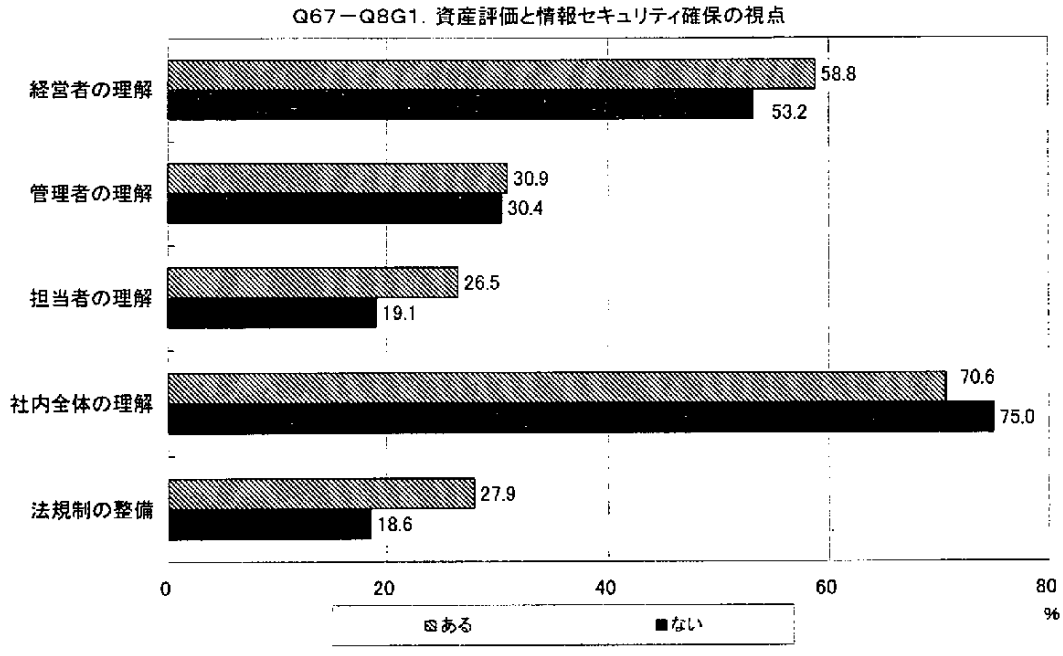


100億円以上の情報化投資を行っている組織体は、「経営者の理解」(64．3%)、「管理者の理解」(41．1%)、「担当者の理解」(35．7%)、「法規制の充実」(33．9%)の割合が100億円以下の組織体より高い。一般に総投資金額の高いほうが各項目の回答率が高く、セキュリティへの関心度合いも高いことがうかがえる。

Q8. 情報システムの資産価値を評価したことがありますか。

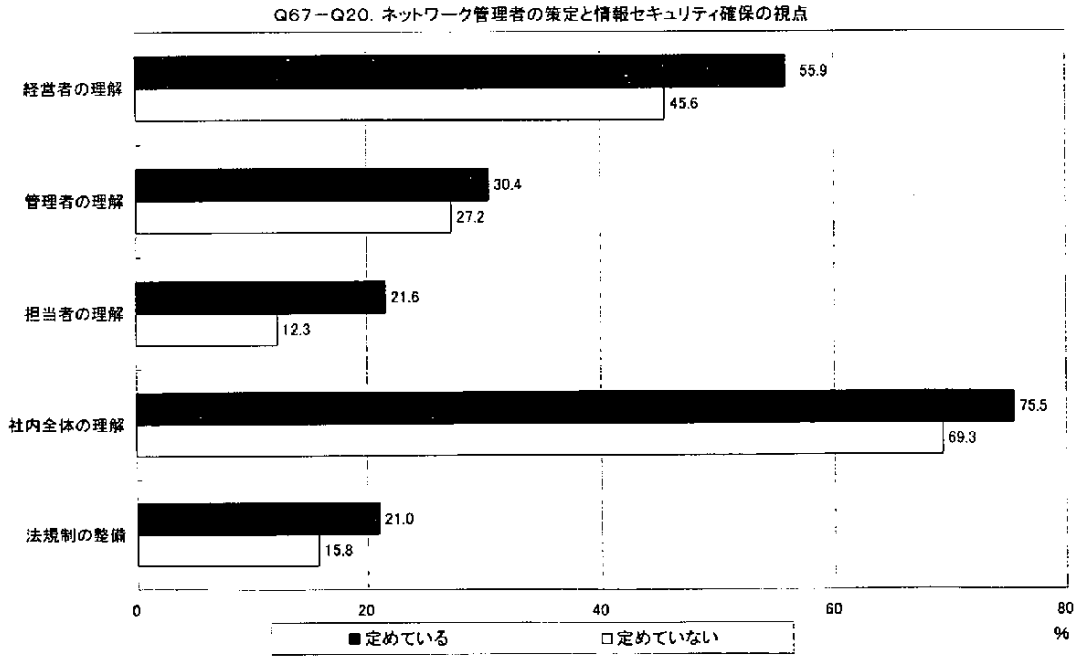
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
ある	58.8%	30.9%	26.5%	70.6%	27.9%
ない	53.2	30.4	19.1	75.0	18.6
無回答	57.7	30.8	19.2	80.8	30.8

資産価値評価の「ある」と「ない」のそれぞれの回答内容について全体的な傾向に大きな差はなかった。



Q20. 基幹システムのネットワーク管理者を定めていますか。

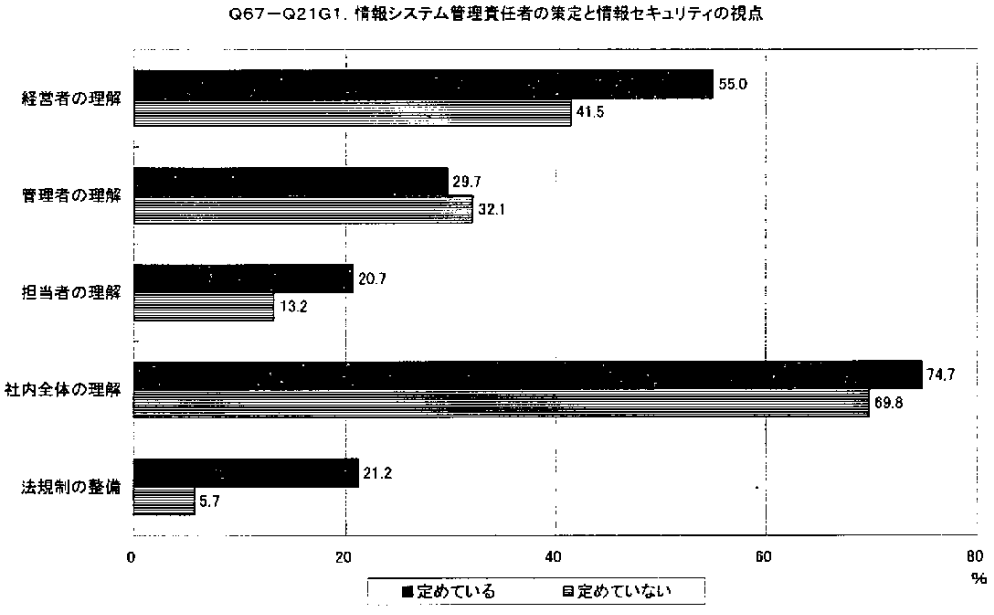
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
定めている	55.9%	30.4%	21.6%	75.5%	21.0%
定めていない	45.6	27.2	12.3	69.3	15.8
現在検討中である	48.8	25.6	7.0	86.0	14.0
定めるか検討している	51.5	51.5	24.2	69.7	15.2
必要ない	40.0	20.0	10.0	60.0	10.0
無回答	40.0	40.0	40.0	80.0	40.0



ネットワーク管理者を「定めている」方が「定めていない」と回答したところより、個別の割合がそれぞれ上回っている。したがって「定めている」組織体がリスクについての関心度が高いといえる。特に「経営者の理解」については「定めている」が55．9%、「定めていない」が45．6%と約10ポイントの差がある。

Q21．情報システムの管理責任者を定めていますか。

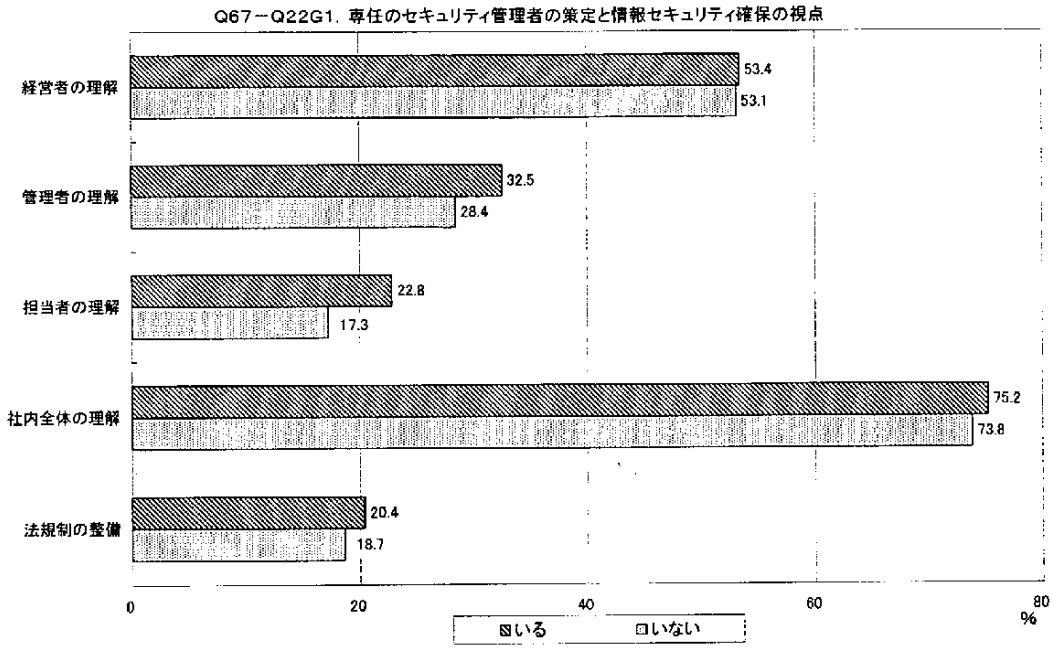
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
定めている	55.0%	29.7%	20.7%	74.7%	21.2%
定めていない	41.5	32.1	13.2	69.8	5.7
現在検討中である	55.2	31.0	6.9	89.7	13.8
定めるか検討している	42.1	57.9	15.8	73.7	10.5
必要ない	33.3	0.0	16.7	66.7	0.0
無回答	50.0	50.0	33.3	83.3	33.3



、Q20同様、情報システム管理責任者を「定めている」の方が、「定めていない」と回答したところより総じて割合が高く、管理責任者を定めている組織体がリスクに対する関心度が高いといえる。特に「経営者の理解」では「定めている」55．0%に対し「定めていない」41．5%と、また、「法規制の整備」では「定めている」21．2%に対し「定めていない」5．7%と差がある。

Q22．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。

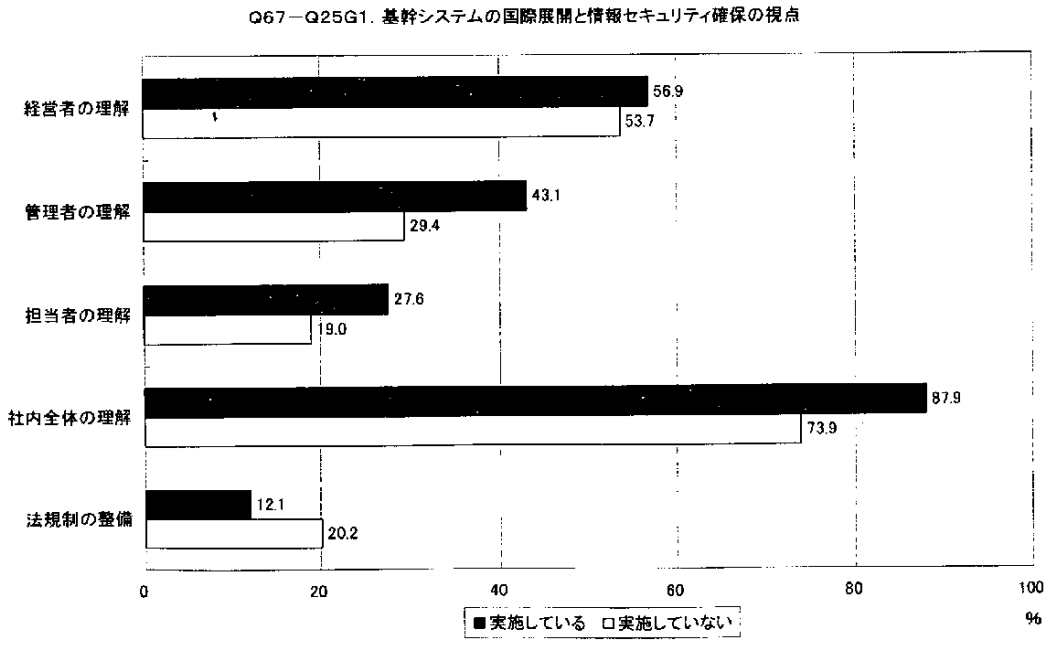
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
いる	53.4%	32.5%	22.8%	75.2%	20.4%
いない	53.1	28.4	17.3	73.8	18.7
設置を検討している	59.3	33.3	23.1	82.4	24.1
必要ない	33.3	55.6	33.3	44.4	0.0
無回答	60.0	60.0	60.0	60.0	40.0



専任のセキュリティ管理者／担当者については「いる」と「いない」で各項目の回答度合いについて大きな差はでなかった。これは専任か兼任かよりも設置そのものの方が重要な要素であるか、または小規模なところでは専任者を設置する余裕がなく、関心が高い組織体が「いない」に含まれているためと考えられる。

Q25．基幹システムを国際的に展開・利用していますか。

	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
実施している	56.9%	43.1%	27.6%	87.9%	12.1%
実施していない	53.7	29.4	19.0	73.9	20.2
無回答	25.0	50.0	50.0	75.0	25.0

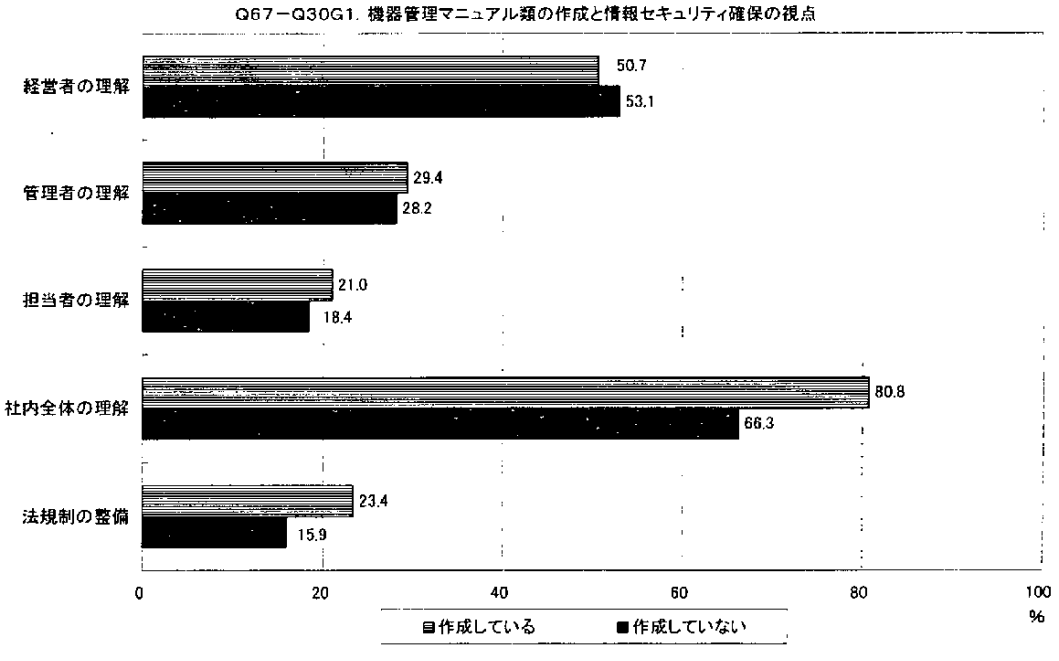


基幹システムを国際的に展開・利用しているところでは「管理者の理解」(43．1%)、「担当者の理解」(27．6%)、「社内全体の理解」(87．9%)が、国際的な利用を行っていないところでの「管理者の理解」(29．4%)、「担当者の理解」(19．0%)、「社内全体の理解」(73．9%)と比べ、大きく差が出ている。

一方、「法規制の整備」では、国際的に展開・利用している組織体が12．1%、展開・利用していない組織体が20．2%と逆転している。国際的企業の方が規模が大きく、また海外のリスクにさらされやすいためにセキュリティへの意識が高いことの表れと考えられる。法規制については情報セキュリティや個人情報保護の規格などは海外、特に欧州で先行しているため、すでに規制に即した対応を実施済みであると考えられる。

Q30．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。

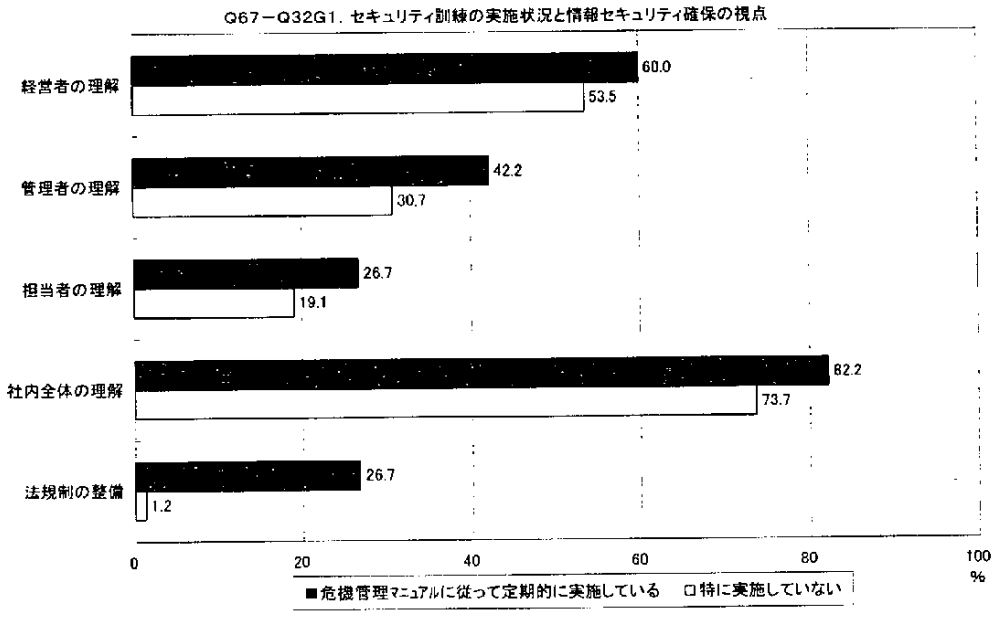
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
作成している	50.7%	29.4%	21.0%	80.8%	23.4%
作成していない	53.1	28.2	18.4	66.3	15.9
作成中である	61.1	38.9	25.3	76.8	18.9
検討中である	58.1	31.7	16.8	79.6	21.6
必要ない	33.3	33.3	33.3	83.3	16.7
無回答	0.0	25.0	0.0	50.0	0.0



全社的な危機管理マニュアルを作成している組織体で最も重要と考える視点として、「社内全体の理解」をあげた割合が80．8%と、「作成していない」組織体(66．3%)と比較して目立って高い。また、「法規制の整備」をあげている割合も23．4%であり、「作成していない」組織体の15．9%よりも高い。これは大企業であるほど全社的なマニュアルを作成していると思われること、および全社的なマニュアル作成には当然ながら全社の協力や理解がなければ作成できないことの表れと思われる。

Q32. 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。

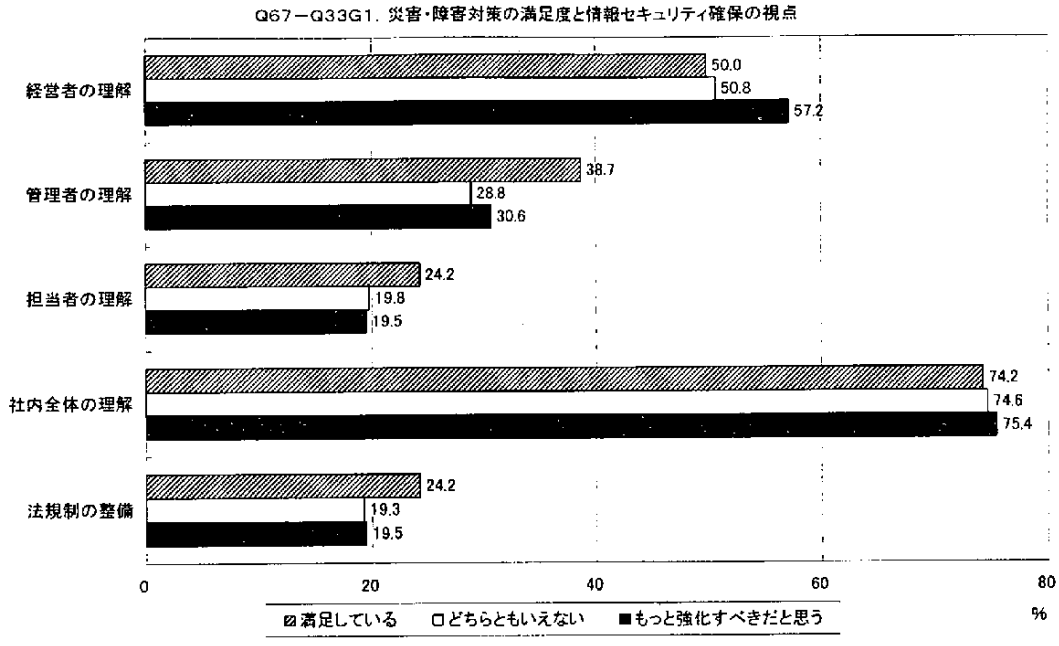
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
危機管理マニュアルに従って定期的に実施している	60.0%	42.2%	26.7%	82.2%	26.7%
特に実施していない	53.5	30.7	19.1	73.7	1.2
危機管理マニュアルに従って時々実施している	59.5	26.2	20.2	82.1	28.6
危機管理マニュアルはないが実施している	47.5	23.7	22.0	76.3	23.7
無回答	35.7	35.7	14.3	57.1	21.4



非常自体に対するセキュリティ訓練を「定期的に実施している」と「特に実施していない」を比較すると、「実施している」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%であり、「特に実施していない」の「経営者の理解」53．5%、「管理者の理解」30．7%、「担当者の理解」19．1%、「社内全体の理解」73．7%、「法規制の整備」1．2%に対していずれも高い。特に「法規制の整備」については回答度合いに大きな差があり、セキュリティに関しての意識の高低が現れていると思われる。

Q33. 貴社でとられている災害・障害対策は、全体的にみて満足できるものですか。

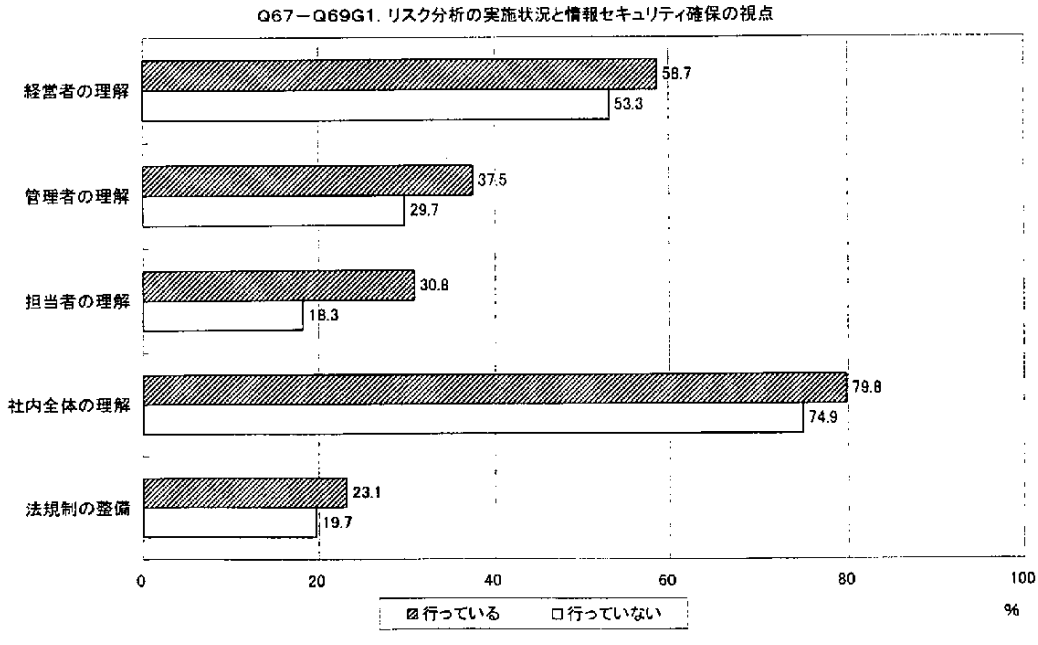
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
満足している	50.0%	38.7%	24.2%	74.2%	24.2%
どちらともいえない	50.8	28.8	19.8	74.6	19.3
もっと強化すべきだと思う	57.2	30.6	19.5	75.4	19.5
無回答	33.3	33.3	0.0	66.7	16.7



災害・障害対策の「満足している」、「どちらともいえない」、「もっと対策を強化しなくてはいけない」のそれぞれについて大きな差はない。多少の差としては「もっと対策を強化しなくてはいけない」で「経営者の理解」57．7%が「満足している」での「経営者の理解」50．0%、「どちらともいえない」50．8%に比べて割合が多い。差が大きく表れないのは、セキュリティレベルの満足度合いが求めるレベルと現状との相対的なものであるので、それぞれの捉え方によるものと考えられる。

Q69．情報システムに係わるリスク分析を実施していますか。

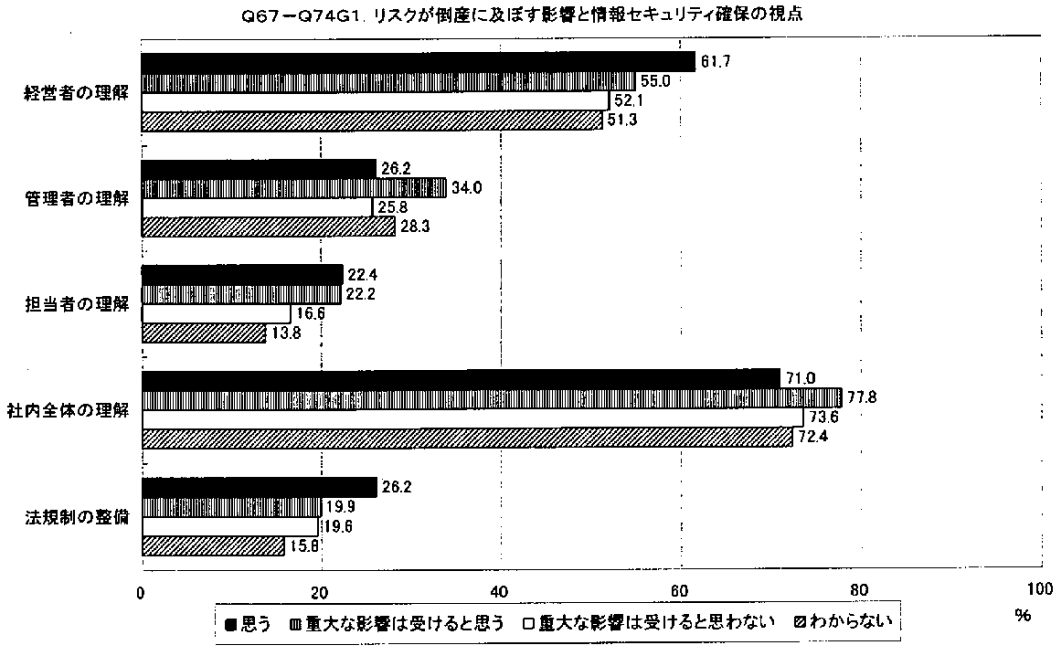
	経営者の理解	管理者の理解	担当者の理解	社内全体の理解	法規制の整備
行っている	58.7%	37.5%	30.8%	79.8%	23.1%
行っていない	53.3	29.7	18.3	74.9	19.7
無回答	40.0	20.0	13.3	40.0	0.0



リスク分析を「行っている」と「行っていない」とを比較するといずれの回答度合いも「行っている」が「行っていない」を上回っている。特に「管理者の理解」では「行っている」37．5%、「行っていない」29．7%と、また「担当者の理解」では「行っている」30．8%、「行っていない」18．3%と差がある。リスク分析を実際に実施する担当者の能力や理解力という実務の目からの回答となっていると思われる。

Q74. 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	61.7%	26.2%	22.4%	71.0%	26.2%
重大な影響は受けると思う	55.0	34.0	22.2	77.8	19.9
重大な影響は受けると思わない	52.1	25.8	16.6	73.6	19.6
わからない	51.3	28.3	13.8	72.4	15.8
無回答	25.9	33.3	22.2	66.7	14.8



情報システム関連リスクが倒産に結びつくと「思う」と回答した組織体では、「経営者の理解」が61．7%と「重大な影響を受けるとは思う」の「経営者の理解」55．0%、「重大な影響を受けるとは思わない」52．1%、「わからない」51．3%よりも高く、倒産は経営者の理解の問題との危機意識の表れを示していると思われる。また「管理者の理解」を高くあげたのは「重大な影響を受けると思う」が34．0%で「思う」26．2%、「思わない」25．8%、「わからない」28．3%より高い。これは倒産に至らないが重大な影響を受ける事態となると管理者が苦労することが予想されるため、その表れと考えられる。

3．9　Q69のクロス集計

Q69. 情報システムに係わるリスク分析を実施していますか。

情報システムのセキュリティに関して出発点はリスク分析にある。リスク分析の可否が組織の命運を握る場合もある。ここでは、情報システムに関してリスク分析を行っているような組織体であれば、当然、以下の質問と何らかの関係があると思われると仮説を立てた。

Q8. 情報システムの資産価値を評価したことがありますか。
Q11. 貴社の基幹システムはどのように運用されていますか。
Q12. 貴社の基幹システムは過去1年間にシステムダウンが発生しましたか。
Q25. 基幹システムを国際的に展開・利用していますか。
Q46. 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。
Q61. 貴社では過去1年間にコンサルティングウイルスに感染したことがありますか。
Q73. 貴社にとり、システミックリスクをどう認識していますか。

そこで、それぞれの質問とリスク分析の関連を検証するためクロスをとり、特徴を把握することにした。その結果は以下のとおりである。

Q8. 情報システムの資産価値を評価したことがありますか。

	ある		ない		無回答	
行っている	12件	11.5%	84件	80.8%	8件	7.7%
行っていない	52	7.0	680	90.9	16	2.1
無回答	4	26.7	9	60.0	2	13.3
計	68	7.8	773	89.2	26	3.0

リスク分析を行っている組織体であれば、仮説として、当然情報システムの資産価値を評価していると思われる。しかし、組織体として情報システムの資産価値を評価したことがあるのはわずかに68件（7．8%）と低かった。

ところで、リスク分析を「行っている」と回答した104件のうち、資産価値の評価を行ったのはわずかに12件（11．5%）で、仮説どおりとなっていない現実があった。「行っていない」のは748件中52件（7．0%）であった。しかし、資産評価を行った68件のうち、リスク分析を「行った」のは17．6%、「行わなかった」のは76．5%であった。この点は、リスク分析とは何であるのか、何に対して分析を行えばよいのかが確定していないことによると思われる。

Q11. 貴社の基幹システムはどのように運用されていますか。

	集中型		集中分散型		分散型		無回答	
行っている	46件	44.2%	45件	43.3%	12件	11.5%	1件	1.0%
行っていない	360	48.1	282	37.7	93	12.4	13	1.7
無回答	8	53.3	4	26.7	1	6.7	2	13.3
計	414	47.8	331	38.2	106	12.2	16	1.8

リスク分析を行っている組織体と基幹システムの運用との間には、何らかの関係があると思われる。基幹システムについては、ほとんどの組織体がメインフレーム等を中心においていることが示されたが、基幹システムの運用との関係では、リスク分析を「行っている」と回答した104件について、

集中型では46件（44．2%）、集中分散型では45件（43．3%）、分散型では12件（11．5%）であった。集中型／集中分散型に比べて、分散型の場合、リスク分析の方法が確立されていないといった困難さを物語っているのかもしれない。なお、各基幹システムにおいて、リスク分析を「行っていない」のはそれぞれ48．1%、37．7%、12．4%であった。なお、それぞれのシステム形態についてリスク分析を「行っていた」のは11．1～13．6%で、「行っていなかった」のはともに85%を超えていた。

Q12．貴社の基幹システムは過去1年間（平成10年1月～12月）にシステムダウンが発生しましたか。

リスク分析を行えばシステムダウンが回避できるとはいえない。しかし、リスク分析によって対応策を判断し、その方法を採用することにより、ダウンを減少させることは十分に考えられる。そこで、リスク分析とシステムダウンとの間に何らかの関係があるのか考察してみた。

基幹システムのシステムダウンについて、リスク分析を「行っている」と回答した104件のうち、全体的にダウンしたのが9件（8．7%）、部分的にダウンしたのが44件（42．3%）で、ダウンしなかったのが51件（49．0%）であった。この点、ダウンしなかったのがリスク分析により対策をとったためなのかは確定しがたい。ところでダウンしなかった409件中、リスク分析を「行っている」のが12．5%（51件）であり、「行っていない」のが85．8%（351件）であった。またリスク分析を「行っていない」という回答については、全体的にダウンしたのが89．9%（99件中89件）、部分的にダウンしたのが85．7%（349件中299件）であった。こうした側面から、リスク分析に基づいた対策の効果を考慮すべきといえるかもしれない。

Q25．基幹システムを国際的に展開・利用していますか。

近年のネットワーク化の進展から、基幹システムを国際的に展開・利用している実態が確認できる。（既述のように基幹システムが何であるのかの理解により差異があるかもしれないが）そうした展開を行っている組織体としてはリスクに対する認識は高いというのが一般的な推測であり、したがってリスク分析を行っているというのがここでの仮説である。この点、国際的に展開している組織体でリスク分析を行っているのは58件中17件（29．3%）、行っていないのは41件（70．7%）であった。国際的に基幹システムを利用していない805件中、リスク分析を行っていないのは705件（87．6%）で、上記の推測をある程度実証していると思われる。

Q46．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）

ネットワーク機器、サービス障害	リスク分析を行っている	
通信事業者のケーブル障害（含む、専用回線）	71件	68.3%
通信事業者の設備障害	55	52.9
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	55	52.9
ISP（ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ）サービスの中断・停止	31	29.8
基幹LANの障害	76	73.1
支線LANの障害	54	51.9
ルータ、DNSサーバなどのLAN機器（構内交換機を含む）の障害	79	76.0
アクセスサーバの障害	53	51.0
地震などの一定地域の災害	57	54.8

障害が発生するか、発生する場合どの部分なのか、といったことはリスク分析の課題である。この点については、リスク分析を「行っている」と回答した104件中、次のようなクロス集計の結果が得られた。読み方にもよるが、すでに平成11年度の特徴として指摘したとおり、「LAN関連の項目」、「ルータ、DNSサーバなどのLAN機器」、「基幹LANの障害」に相対的に高い割合がみられるのは、リスクに対する認識の表れと思われる。

Q61. 貴社では過去1年間(平成10年1月～12月)にコンピュータウイルスに感染したことがありますか。

すでにシステムダウンとの関係から考察したことと同様に、リスク分析を行えばウイルスに感染しないとはいえない。しかし、リスク分析によって感染経路を分析し、対応方法を用いることにより、ウイルスの感染を減少させることは期待できる。そこで両者の関係についてクロスをとり、検証してみた。その結果、リスク分析を「行っている」と回答した104件のうち、コンピュータウイルスに「感染した」のは68件(65.4%)、「感染したことがない」のは36件(34.6%)であった。リスク分析を行いながらもウイルスに感染したのが多いといった指摘がなされるかもしれないが、コンピュータウイルスに感染した473の組織体をみると、リスク分析を「行っている」のは14.4%で、「行っていない」とする400件(84.6%)に比べてかなりの差異がみられる。この点は少なくともリスク分析の意味が指摘できるといえよう。

Q73. 貴社にとり、システミックリスクをどう認識していますか。

	重大と考える		さほど重大と思わない		重大と思わない		わからない		無回答	
行っている	92件	88.5%	3件	2.9%	1件	1.0%	7件	6.7%	1件	1.0%
行っていない	388	51.9	91	12.2	19	2.5	224	29.9	26	3.5
無回答	2	13.3	0	0.0	0	0.0	1	6.7	12	80.0
計	482	55.6	94	10.8	20	2.3	232	26.8	39	4.5

ここでの認識も、システムダウン、ウイルスへの感染の場合と同様にアプローチすることができる。システミックリスクを重大だと認識している割合は全回答において55.6%と過半数を超えていた。ところで、リスク分析を行っている104件についてのクロスでは、システミックリスクを「重大と考える」のは88.5%、「さほど重大だと思わない」2.9%、「重大だと思わない」1.0%と顕著な差異が認められた。この点、「重大と考える」(482件)について「リスク分析を行っていない」のは80.5%とかなりの割合を示しているが、「さほど重大だと思わない」(94件)については96.8%、「重大だと思わない」(20件)については95.0%と比べて相対的に低い結果となっている。特に、システミックリスクについては、リスク分析との関係が強く認識できたと思われる。

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

1999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	
資本金（非営利法人においては、基金、出資金等）	7 千億 百億 十億 億 千万 百万 円		
従業員数（学校の場合は常勤教員数、病院の場合は病床数、官庁の場合は関係庁部所の定員数をご記入下さい。）	13 十万 万 千 百 十 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。

◇　ご回答賜りました企業には、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。

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 通商産業省の安全対策の施策について

Q１．通商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 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。

30		
	1	知っている
	2	知らない

31 B

2 情報システム資産について

Q５．①ハードウェア、ソフトウェア、データを含む、現在稼働中の全情報システムへの総投資金額の概算を教えて下さい。
②また、パソコンの総投資金額に対する割合についても横の欄にご記入下さい。

32	総投資金額の概算		33	パソコンの割合
1	１００億円以上			%
2	５０億円以上～１００億円未満		36	%
3	３０億円以上～５０億円未満		39	%
4	１０億円以上～３０億円未満		42	%
5	１億円以上～１０億円未満		45	%
6	５千万円以上～１億円未満		48	%
7	５千万円未満		51	%

(注) 総投資金額は、購入価格換算、レンタルはレンタル月額の 45 倍：全 CPU，全周辺機器、全端末、全ソフトウェア、保有している全データの開発・購入費を含んだもの。

Q６．全情報システムへの総投資金額（上記）に対するハードウェア、ソフトウェア、データの割合はどの程度ですか。

ハードウェア	54				%
ソフトウェア	57				%
データ	60				%
計		1	0	0	%

Q７．全情報システムへの総投資金額は、どのような傾向を示していますか。

63

1	上昇傾向
2	ほぼ横ばい
3	下降傾向

Q８．情報システムの資産価値を評価したことがありますか。

64

1	あ　る
2	な　い

⇒Q10 へ

Q９．情報システムの現在の資産価値は、どの程度と見積っていますか。

65

兆		百億		億				
								百万円

Q10．情報システム投資金額と重要情報価値を比較したことがありますか。

73

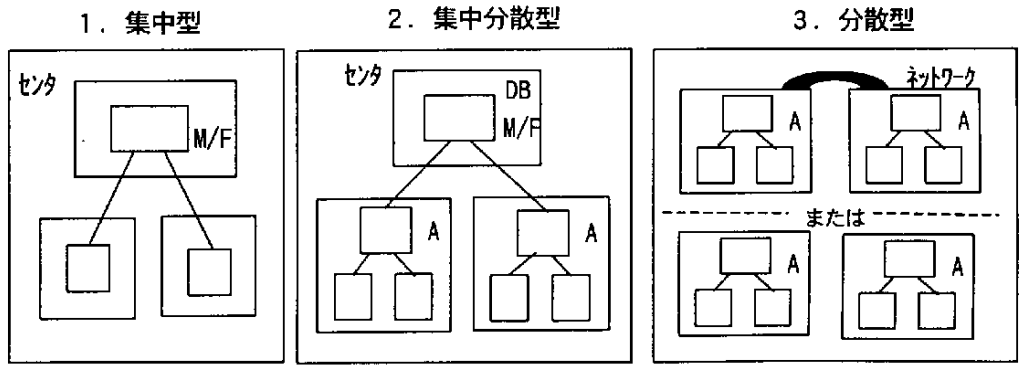
1	あ　る
2	な　い
3	意味がない（具体的に理由を書いて下さい：　　）

Q11．貴社の基幹システム(注)はどのように運用されていますか。

74

1	集中型
2	集中分散型
3	分散型

運用形態



(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。

75 C

これからの質問は貴社の基幹システムについてお答え下さい。

3	過去の障害等の実績について

Q12. 貴社の基幹システムは過去１年間（平成 10 年１月～12 月）にシステムダウンが発生しましたか。

76

1	全体的にダウンした
2	部分的にダウンした
3	しない ⇒Q16 へ

Q13. 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）

77	1	自然災害
78	2	電源障害
79	3	空調等障害
80	4	通信事業者に起因する障害
81	5	ＩＳＰ（ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ）等社外のインターネットに起因する障害
82	6	ネットワーク機器などの障害
83	7	ハードウェア
84	8	ＯＳ障害
85	9	ソフトウェア障害
86	10	火災による事故・障害
87	11	人の悪意による事故等
88	12	オペミス等人の過失による事故等
89	13	その他（具体的に書いて下さい：　　）

（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。

Q14. 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

90 | | | | | | 時間 |

Q15. 基幹システムにおけるＭＴＴＲ（平均修理時間）は何分ですか。

95 | | | | | 分 |

99 D

4	セキュリティ管理一般について

Q16. 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。

100

1	定めている
2	現在作成中である
3	作成を検討している
4	定めていない
5	必要ない

Q17. セキュリティガイドラインとして操作および業務処理手順を定めていますか。

101

1	定めている
2	現在作成中である
3	作成を検討している
4	定めていない
5	必要ない

⇒Q20 へ

Q18. 出張中、移動中の環境についてのセキュリティガイドラインがありますか。

102

1	あ る
2	な い

Q19. セキュリティガイドラインを定期的に見直していますか。

103

1	い る
2	いない

Q20. 基幹システムのネットワーク管理者を定めていますか。

104

1	定めている
2	現在検討中である
3	定めるか検討している
4	定めていない
5	必要ない

Q21. 情報システムの管理責任者を定めていますか。

105

1	定めている
2	現在検討中である
3	定めるか検討している
4	定めていない
5	必要ない

Q22. 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。

106

1	い る
2	設置を検討している
3	いない
4	必要ない

Q23. 緊急時の連絡手段を持っていますか。

107

1	持っている
2	検討中である
3	持っていない
4	必要ない

Q24. データの使用・保管等の管理を行っていますか。

108

1	い る
2	いない

Q25. 基幹システムを国際的に展開・利用していますか。

109

1	実施している
2	実施していない

⇒Q28 へ

Q26. 上記の基幹システムについて、情報システムのセキュリティ対策を講じていますか。

110

1	講じている
2	講じる予定である
3	まったく考えていない

⇒Q28 へ

Q27. 講じている場合、セキュリティ対策は何に準拠して策定しましたか。

111

1	展開先の国の法規制
2	取引先企業の要請
3	独自の対策
4	その他（具体的に書いて下さい：　　）

Q28. 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）

112	1	コストがかかりすぎる
113	2	組織の従業員に対する教育・訓練がいきとどかない
114	3	組織の従業員に対する負担がかかりすぎる
115	4	対策を構築するノウハウが不足している
116	5	どこまでやればよいのか基準が示されていない
117	6	要求に合致するもの（サービス）がない
118	7	トップの理解が得られない
119	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
120	9	セキュリティ管理が事業の国際化に見合っていない
121	10	その他（具体的に書いて下さい：　　）

Q29. 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					
122	市販のソフトをコピーして使う	1	2	3	4	5	6
123	データ、プログラムを無断で使う	1	2	3	4	5	6
124	データ、プログラムを覗き見る	1	2	3	4	5	6
125	会社のコンピュータを私用に使う	1	2	3	4	5	6
126	コンピュータウイルスを伝染させる	1	2	3	4	5	6
127	他社のシステムへ侵入する	1	2	3	4	5	6
128	他人のパスワードを解読し、使用する	1	2	3	4	5	6
129	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
130	私用の電子メールを受信する	1	2	3	4	5	6
131	ネットワークにログインしている他のマシンのファイルを見る	1	2	3	4	5	6
132	共有サーバにある仕事に関係していないファイルを見る	1	2	3	4	5	6
133	他人のＩＤを無断借用する	1	2	3	4	5	6
134	メール、ブラウザ等接続されたままの他人のマシンを操作する	1	2	3	4	5	6
135	時間外に会社のコンピュータでゲームを行う	1	2	3	4	5	6
136	業務上入手した顧客情報を正当な理由なしに第３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

137 E

5	災害対策・障害対策について

Q30. 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。

138		
	1	作成している
	2	作成中である
	3	検討中である
	4	作成していない
	5	必要ない

⇒Q32 へ

Q31. （作成している場合）貴社でとられている危機管理マニュアルは、全体的にみて満足できるものですか。

139		
	1	満足している
	2	どちらともいえない
	3	もっと強化すべきだと思う

Q32. 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。

140		
	1	危機管理マニュアルに従って定期的に実施している
	2	危機管理マニュアルに従って時々実施している
	3	危機管理マニュアルはないが実施している
	4	特に実施していない

Q33. 貴社でとられている災害・障害対策は、全体的にみて満足できるものですか。

141		
	1	満足している
	2	どちらともいえない
	3	もっと強化すべきだと思う

Q34. ①情報システムのバックアップ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。
②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。
（①、②ともに複数回答）

		対策項目		満足度		
142	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）	150	1	2	3
143	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	151	1	2	3
144	3	バックアップサービス業者と契約を交わしている	152	1	2	3
145	4	バックアップ用のコンピュータを設置している	153	1	2	3
146	5	別の場所にバックアップセンタを設置している	154	1	2	3
147	6	ネットワークのバックアップを行っている	155	1	2	3
148	7	その他（具体的に書いて下さい：　　）	156	1	2	3
149	8	特に対策を講じていない		⇒Q35 へ		

⇒Q36 へ

満足度１～３は次のように定義します。

1．満足している	2．問題がある	3．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

Q35. 対策を講じない理由は何ですか。主なもの１つを選んで下さい。

157	1	必要性を感じていない
	2	満足する対策がない
	3	コストがかかりすぎる
	4	その他（具体的に書いて下さい：　　）

Q36. ①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。
②また、その機能に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。
（①、②ともに複数回答）

		代替運転機能		満足度		
158	1	デュアルシステム	167	1	2	3
159	2	デュプレックスシステム	168	1	2	3
160	3	ホットスタンバイシステム	169	1	2	3
161	4	コールドスタンバイシステム	170	1	2	3
162	5	クラスタリング	171	1	2	3
163	6	高可用性機構	172	1	2	3
164	7	ミラリング	173	1	2	3
165	8	フォールトトレラント	174	1	2	3
166	9	特に設けていない		⇒Q37 へ		

⇒Q38 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を選択して下さい。

満足度１～３は次のように定義します。

１．満足している	２．問題がある	３．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

Q37. 代替運転機能を設けない理由は何ですか。主なものを１つ選んで下さい。

175	1	必要性を感じていない
	2	満足するもの（機能）がない
	3	コストがかかりすぎる
	4	その他（具体的に書いて下さい：　　）

Q38. ①ファイルのバックアップ対策はどのようなものですか。実施している対策項目を選んで下さい。
②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。
(①、②ともに複数回答)

		対策項目		満足度		
176	1	同一ディスク内にファイルを二重化している	184	1	2	3
177	2	ファイルを別ディスクに二重化している	185	1	2	3
178	3	バックアップ用のファイルを同一建物内に保存している	186	1	2	3
179	4	バックアップ用のファイルを遠隔地に保存している	187	1	2	3
180	5	遠隔地にミラーファイルを持っている	188	1	2	3
181	6	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	189	1	2	3
182	7	その他（具体的に書いて下さい：　　）	190	1	2	3
183	8	特に対策を講じていない		⇒Q39 へ		

⇒Q40 へ

満足度1～3は次のように定義します。

1．満足している	2．問題がある	3．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

Q39. 対策を講じない理由は何ですか。主なもの1つを選んで下さい。

191		
	1	必要性を感じていない
	2	満足する対策がない
	3	コストがかかりすぎる
	4	その他（具体的に書いて下さい：　　）

Q40. 貴社の基幹システムはどれぐらいの頻度でファイル等のバックアップを実施していますか。

192		
	1	リアルタイムで
	2	1日に1回程度
	3	週に1回程度
	4	月に1回程度
	5	年に数回程度

193 F

Q41. 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	ｺﾝﾋﾟｭｰﾀ室	データ保管場所	ﾈｯﾄﾜｰｸ設備室	ｺﾝﾋﾟｭｰﾀ設置場所
自動火災報知設備を設置している	194 1	195 2	196 3	197 4
ハロン消火設備を設置している	198 1	199 2	200 3	201 4
CO_2消火設備を設置している	202 1	203 2	204 3	205 4
スプリンクラ消火設備を設置している	206 1	207 2	208 3	209 4
排煙設備を設置している	210 1	211 2	212 3	213 4
耐火金庫を設置している	214 1	215 2	216 3	217 4
消火・排煙等の防災機器の点検を定期的に行っている	218 1	219 2	220 3	221 4
その他(右の欄に具体的に対策を書いて下さい)	222 1	223 2	224 3	225 4
特に対策を講じていない	226 1	227 2	228 3	229 4

Q42. 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
免震構造になっている	230 1	231 2	232 3
転倒防止措置を講じている	233 1	234 2	235 3
機器の移動防止措置を講じている	236 1	237 2	238 3
フリーアクセス床は耐震構造としている	239 1	240 2	241 3
媒体の落下防止措置を講じている	242 1	243 2	244 3
その他(右の欄に具体的に対策を書いて下さい)	245 1	246 2	247 3
特に対策を講じていない	248 1	249 2	250 3

Q43. 電源設備の災害対策として、次のどの対策をとっていますか。(複数回答)

251	1	ＡＶＲ
252	2	ＣＶＣＦ／ＵＰＳ
253	3	自家発電装置
254	4	その他(具体的に書いて下さい：　　)
255	5	特に対策を講じていない

Q44. 情報システム、ネットワーク室、機器の災害・障害等の対策について、今後の方向性を原因別にみた場合、今後の考え方欄の該当する番号に○印をつけて下さい。

	原　　因	今後の考え方		
256	自然災害	1	2	3
257	電源障害	1	2	3
258	空調等障害	1	2	3
259	回線障害	1	2	3
260	ハードウェア	1	2	3
261	ＯＳ障害	1	2	3
262	ソフトウェア障害	1	2	3
263	火災による事故・障害	1	2	3
264	人の悪意による事故等	1	2	3
265	オペミス等人の過失による事故等	1	2	3

今後の考え方欄の選択肢は次のとおり

1．考えていない	2．現在のままでよい	3．強化する

266 G

Q45. 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）

267	1	コストがかかりすぎる
268	2	要員に対する教育訓練がいきとどかない
269	3	要員に対して負担がかかりすぎる
270	4	対策を構築するノウハウが不足している
271	5	どこまでやれば良いのか基準が示されていない
272	6	要求に合致するもの（製品）がない
273	7	トップの理解が得られない
274	8	その他（具体的に書いて下さい：　　）
275	9	特に問題はない

Q46. 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）

276	1	通信事業者のケーブル障害（含む、専用回線）
277	2	通信事業者の設備障害
278	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
279	4	ＩＳＰ（ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ）サービスの中断・停止
280	5	基幹ＬＡＮの障害
281	6	支線ＬＡＮの障害
282	7	ルータ、ＤＮＳサーバなどのＬＡＮ機器（構内交換機を含む）の障害
283	8	アクセスサーバの障害
284	9	地震などの一定地域の災害
285	10	その他（具体的に書いて下さい：　　）
286	11	特に想定していない

Q47. ①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。
②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。
（①、②ともに複数回答）

	対策項目		満足度		
287	1 異なる種別回線を利用	300	1	2	3
288	2 異なる交換局への収容	301	1	2	3
289	3 異なるコモンキャリアの利用	302	1	2	3
290	4 異なるＩＳＰ（ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ）を利用	303	1	2	3
291	5 異なるメディアによる回線利用（例：衛星回線等）	304	1	2	3
292	6 ポイント間接続から網接続へ	305	1	2	3
293	7 重要回線を部分的に二重化	306	1	2	3
294	8 専用のバックアップ回線を常時設定	307	1	2	3
295	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	308	1	2	3
296	10 社内の構内回線、ＬＡＮ等を二重化	309	1	2	3
297	11 通信機器（CCU、ルータ、DNS サーバ、アクセスサーバ等）の二重化	310	1	2	3
298	12 その他（具体的に書いて下さい：　　）	311	1	2	3
299	13 特に対策を講じていない		-		

満足度１～３は次のように定義します。

１．満足している	２．問題がある	３．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

312 H

6 不正アクセス対策・不正侵入対策について

Q48. 平成 12 年２月施行予定の「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。

313

1	知っている
2	知らない

Q49. 貴社では過去１年間（平成 10 年１月～12 月）に不正アクセスの被害に遇われたことがありますか。

314

1	あ　る	
2	な　い	⇒Q52 へ

Q50. 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。

315

1	出した
2	出さない

Q51. 不正アクセスの被害にあたり、ＪＰＣＥＲＴ／ＣＣ（コンピュータ緊急対応センター）に相談しましたか。

316

1	し た
2	しない

Q52. 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不正アクセス対策はどのようなものですか。実施している対策を選んで下さい。
②また、その対策に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。
（①、②ともに複数回答）

	対策項目		満足度		
317 1	室の出入口で入室管理を行っている	325	1	2	3
318 2	室の出入口で退室管理を行っている	326	1	2	3
319 3	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	327	1	2	3
320 4	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	328	1	2	3
321 5	室の管理責任者を定めている	329	1	2	3
322 6	情報システムの監視設備を設けている	330	1	2	3
323 7	その他（具体的に書いて下さい：　　）	331	1	2	3
324 8	特に対策を講じていない		－		

（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。

満足度１～３は次のように定義します。

1．満足している	2．問題がある	3．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

Q53. 貴社ではリモートアクセスを行っていますか。

332

1	い る
2	いない

Q54. 情報についての機密度のランクを設定していますか。

333

1	い る
2	いない

Q55. ①ネットワークを介しての不正アクセスに対して講じている対策は何ですか。実施している対策を選んで下さい。
②また、その対策で不正アクセスは防止できると思いますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。(①、②ともに複数回答)

		対策項目		満足度		
334	1	パスワードの活用	343	1	2	3
335	2	ファイアウォールの利用	344	1	2	3
336	3	アクセス制御ソフトウェアの使用	345	1	2	3
337	4	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	346	1	2	3
338	5	ネットワーク機器の運用者（アクセス範囲）を限定	347	1	2	3
339	6	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	348	1	2	3
340	7	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	349	1	2	3
341	8	その他（具体的に書いて下さい：　　）	350	1	2	3
342	9	特に対策を講じていない		-		

満足度１～３は次のように定義します。

１．満足している	２．問題がある	３．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

Q56. 貴社では基幹システムのパスワードを変更していますか。

351	1	定期的に変更している
	2	本人の自由意思に任せる
	3	強制的に変更するシステムをとっている
	4	変更期限がきたらパスワードを無効にする
	5	その他（具体的に書いて下さい：　　）
	6	変更していない

Q57. ①貴社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。
②また、現在採用している暗号に満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。
(①、②ともに複数回答)

		採用方法		満足度			
352	1	暗号装置を購入	358	1	2	3	⇒Q58 へ
353	2	市販の暗号ソフトウェアを購入	359	1	2	3	
354	3	自社で作成した暗号ソフトウェアを使用	360	1	2	3	
355	4	利用しているアプリケーションについているので暗号機能を利用	361	1	2	3	
356	5	その他（具体的に書いて下さい：　　）	362	1	2	3	
357	6	採用していない		⇒Q59 へ			

満足度１～３は次のように定義します。

１．満足している	２．問題がある	３．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

Q58. 暗号化している情報は次のどれですか。(複数回答)

363	1	伝送するデータ
364	2	伝送するプログラム
365	3	記録媒体上のデータ
366	4	記録媒体上のプログラム
367	5	認証情報(署名)
368	6	カード番号などの重要なトランザクションデータの転送に利用
369	7	その他(具体的に書いて下さい:　　)

Q59. 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。

370	1	定期的に実施している
	2	社内教育用のセキュリティ教育カリキュラムを策定して実施している
	3	計画書またはマニュアル類に従って実施している
	4	その他(具体的に書いて下さい:　　)
	5	特に実施していない

Q60. 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)

371	1	コストがかかりすぎる
372	2	組織の従業員に対する教育訓練がいきとどかない
373	3	組織の従業員に対する負担がかかりすぎる
374	4	対策を構築するノウハウが不足している
375	5	どこまでやれば良いのか基準が示されていない
376	6	要求に合致するもの(製品)がない
377	7	トップの理解が得られない
378	8	その他(具体的に書いて下さい:　　)
379	9	特に問題はない

380 [1]

7	コンピュータウイルス対策について

Q61. 貴社では過去1年間(平成10年1月～12月)にコンピュータウイルスに感染したことがありますか。

381	1	あ　る
	2	な　い　⇒Q64へ

Q62. 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。

382

1	出した
2	出さない

Q63. 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）

383	1	フリーソフトウェアから
384	2	外部から入手した記録媒体から
385	3	社内ネットワーク経由で
386	4	インターネット経由で
387	5	電子メールの添付書類で
388	6	その他（具体的に書いて下さい：　　）
389	7	わからない

Q64. ①貴社ではコンピュータウイルス対策を講じていますか。実施している対策を選んで下さい。
②また、その対策で満足していますか。選択項目ごとに満足度欄の該当する番号に○をつけて下さい。
（①、②ともに複数回答）

		対策項目		満足度		
390	1	ウイルス検出時や緊急対応と連絡体制の整備	398	1	2	3
391	2	ソフトウェアの出所の確認	399	1	2	3
392	3	ライトプロテクト、バックアップ等のソフトウェア管理	400	1	2	3
393	4	ワクチンソフトの利用およびパラメータファイルの配布	401	1	2	3
394	5	パスワードの変更等、アクセスコントロールの強化	402	1	2	3
395	6	動作の定期的な確認等、異常発見体制の整備	403	1	2	3
396	7	その他（具体的に書いて下さい：　　）	404	1	2	3
397	8	特に対策を講じていない		-		

満足度１～３は次のように定義します。

１．満足している	２．問題がある	３．どちらともいえない

問題があると思われる場合、具体的に問題点をお書き下さい。

Q65. 貴社では従業員に対し、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。

405

1	定期的に実施している
2	社内教育用のセキュリティ教育カリキュラムを策定して実施している
3	計画書またはマニュアル類に従って実施している
4	その他（具体的に書いて下さい：　　）
5	特に実施していない

Q66. 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）

406	1	コストがかかりすぎる
407	2	組織の従業員に対する教育訓練がいきとどかない
408	3	組織の従業員に対する負何がかかりすぎる
409	4	対策を構築するノウハウが不足している
410	5	どこまでやれば良いのか基準が示されていない
411	6	要求に合致するもの（製品）がない
412	7	トップの理解が得られない
413	8	その他（具体的に書いて下さい：　　）
414	9	特に問題はない

415 J

8 情報リスクマネジメント関連について

Q67. 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）

416	1	経営者の理解
417	2	管理者の理解
418	3	担当者の理解
419	4	社内全体の理解
420	5	法規制の整備
421	6	その他（具体的に書いて下さい：　　）

Q68. 経営者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。

422	1	高　い
	2	中　位
	3	低　い
	4	わからない

Q69. 情報システムに係わるリスク分析を実施していますか。

423	1	行っている	⇒Q71 へ
	2	行っていない	

Q70. リスク分析を実施しない理由は何ですか。（複数回答）

424	1	重要性を感じていない	⇒Q73 へ
425	2	手法がわからない	
426	3	予算がない	
427	4	発生被害額が算出できない	
428	5	リスク分析の意味がわからない	
429	6	効果がわからない	
430	7	効果があるとは思えない	

Q71. リスク分析を実施する際の問題点は何ですか。（複数回答）

431	1	経営との関係がわからない
432	2	確立した手法がない
433	3	分析のためのデータが乏しい
434	4	専門家がいない
435	5	組織ができていない
436	6	問題点は特にない
437	7	その他（具体的に書いて下さい：　　）

Q72. リスク分析は誰が実施しましたか。

438	1	情報システム部門内の要員
	2	関係部門を含めたプロジェクトチーム
	3	外部のコンサルタント
	4	その他（具体的に書いて下さい：　　）

Q73. 貴社にとり、システミックリスク(注)をどう認識していますか。

439	1	重大と考える
	2	さほど重大だと思わない
	3	重大だと思わない
	4	わからない

(注) システミックリスクとはシステムを通して連鎖的に影響を及ぼすリスクをいいます。

Q74. 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。

440	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

Q75. 経営上、システム監査をどう考えていますか。

441	1	重要と考える	⇒Q77 へ
	2	さほど重要だと思わない	
	3	重要だと思わない	
	4	わからない	⇒Q77 へ

Q76. 重要だと思わない理由は何ですか。（複数回答）

442	1	経営者の認識が低いため
443	2	これまで重大なリスクなど起こらなかったため
444	3	システム監査の理解が不十分
445	4	システム監査の限界
446	5	その他（具体的に書いて下さい：　　）

Q77. 緊急時の役割はあらかじめ決められていますか。

447	1	い　る
	2	いない

Q78. 災害復旧のレベル（事業再開のための最低限、災害以前の水準、等）をあらかじめ段階的に決めていますか。

448

1	い る
2	いない

Q79. 全社の従業員に対し、情報セキュリティ教育を実施していますか。

449

1	い る
2	いない

Q80. 西暦2000年問題の発生を想定して危機管理マニュアルを作成していますか。

450

1	作成している
2	作成中である
3	検討中である
4	作成していない
5	必要ない

Q81. 西暦2000年問題に対し、従業員に対し訓練を行っていますか。

451

1	全社的訓練を行っている
2	情報システム部門だけで訓練を行っている
3	行っていない

452 K

9	個人情報保護について

Q82. 顧客等の個人情報を利用していますか。

453

1	は い	
2	いいえ	⇒Q86へ

Q83. 利用目的は何ですか。（複数回答）

454	1	売買等契約の履行
455	2	顧客サポート
456	3	代金等の回収
457	4	情報提供
458	5	マーケティング
459	6	商品開発
460	7	その他（具体的に書いて下さい：　　）

Q84. 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）

461	1	申込書等によって情報主体（当該個人）から直接に収集
462	2	名簿業者等から購入
463	3	グループ企業から入手
464	4	他社から提供を受ける
465	5	業務委託契約等に基づき提供を受ける
466	6	その他（具体的に書いて下さい：　　）

Q85. 情報主体から直接に収集する場合、利用目的等を明示して同意を取る必要があると思いますか。

467	1	同意を取る必要がある
	2	同意は必要ない

Q86. （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）

468	1	知っている
469	2	知らない
470	3	プライバシーマークを利用したい
471	4	利用したいと思わない（理由を書いて下さい：　　）

Q87. 今後必要と思われるセキュリティ制度・機能・製品等がありましたら、具体的にお書き下さい。

472 L

ご協力ありがとうございました。

KEIRIN 00　このアンケートは競輪の補助金を受けて実施するものです。

平成 12 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）９３８１

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
鈴木第二ビル　２Ｆ
ＴＥＬ　03（3219）２９７１