H15－H002

# わが国における情報セキュリティの実態

## －「情報セキュリティに関する調査」集計結果－

平成16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、605 事業体から回答をいただき、信頼できる調査データを収集することができました。ご回答いただいた事業体、および調査項目の検討、調査結果取りまとめ等にご協力いただいたリスク対策検討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 16 年 3 月

財団法人日本情報処理開発協会

# 平成１５年度リスク対策検討委員会

（敬称略／五十音順）

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

# 目　　次

# 1．調査の概要

## 1.1　調査の概要

### 1.1.1　調査の目的

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

### 1.1.2　調査の対象

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

### 1.1.3　調査時期

調査票発送　　平成15年10月29日
回収締切　　平成16年1月9日

### 1.1.4　回収状況

発送数　　4,000件
回収数（回収率）　　605件（15.1%）

これまでの調査における回収率は、平成5年度33.9%、7年度29.3%、9年度23.3%、11年度18.4%、13年度18.0%であった。回収の割合は調査のたびに減少している。こうした傾向にはいくつかの理由が考えられる。たとえば、質問票の留置期間が約2か月と長かったこと、公的機関を含め情報セキュリティ関連の調査依頼が増えてきたこと、雇用環境の変化の中で一段と多忙となり回答者にとって時間的に余裕がなくなってきたこと、1.1.6に示すように質問項目数が多いこと等をあげることができるかもしれない。しかしながら、調査結果には情報リスクマネジメントに関わる実態を認識するための重要な側面が示されており、今後の情報セキュリティのあり方を考える手掛かりになるものと思われる。

### 1.1.5　回答事業体の平均従業員数

2,256人

### 1.1.6　調査項目（計75項目）

1．経済産業省の安全対策の施策について（6項目）
2．情報リスクマネジメントについて（4項目）
3．情報リスク分析について（11項目）
4．情報セキュリティポリシー・管理・対策について（8項目）
5．災害対策・障害対策について（15項目）
6．不正アクセス対策・不正侵入対策・情報漏洩対策について（8項目）
7．コンピュータウイルス対策について（4項目）

8．アウトソーシングについて（３項目）
9．システム監査・情報セキュリティ監査について（５項目）
10．個人情報保護について（11 項目）

今回の質問構成は全体で 75 項目からなっており、平成 13 年度調査（89 項目）と比べ若干質問数が減少している。今回の調査実施にあたり、これまでの継続調査項目の見直し・整理を行い、また、情報技術の進歩による情報システム環境の変化を考慮した新たな質問項目や選択肢を加味した内容となっている。さらに、リスクマネジメントの視点から情報リスクマネジメント関連、個人情報保護に関連する項目を見直し、これまで以上に現状の解明に役立つ調査を目指した。

### 1.1.7　調査対象業種および回収状況

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

表１－１．回収状況

| 業務ｸﾞﾙｰﾌﾟ | 業　種 | 回収数 | 平均従業員数(小数点以下切捨) | 業務ｸﾞﾙｰﾌﾟ | 業　種 | 回収数 | 平均従業員数(小数点以下切捨) |
|---|---|---|---|---|---|---|---|
| 食品・紙・パルプ・繊維・印刷 | 食品製造業 | 16 | 960 | 情報処理サービス業 | 情報処理サービス業・ソフトウェア業 | 74 | 755 |
| | 繊維工業 | 6 | 5,225 | その他対事業所サービス | 農・林・漁・狩・水産養殖業 | 2 | 620 |
| | 紙・ﾊﾟﾙﾌﾟ・紙加工品製造業 | 5 | 1,121 | | 鉱業 | 1 | 177 |
| | 印刷業・同関連産業 | 2 | 147 | | 建設業 | 37 | 2,579 |
| 石油・化学・鉄鋼・非鉄・金属 | 化学工業 | 26 | 3,201 | | 新聞業・出版業 | 3 | 3,670 |
| | 石油製品製造業 | 4 | 1,540 | | 不動産業 | 2 | 203 |
| | 鉄鋼業 | 9 | 5,901 | | 運輸・通信・倉庫業 | 27 | 1,617 |
| | 非鉄金属製造業・金属製品製造業 | 16 | 1,251 | | 電力・ガス業 | 9 | 12,669 |
| 電気・一般・輸送・精密機械 | 一般機械器具製造業 | 22 | 1,524 | | 放送業 | 4 | 167 |
| | 電気機械器具製造業 | 27 | 4,580 | | 広告・調査・情報提供サービス業 | 4 | 1,814 |
| | 輸送用機械器具製造業 | 24 | 5,232 | | その他のサービス業 | 14 | 1,102 |
| | 精密機械器具製造業 | 9 | 1,614 | 公共サービス | 医療業 | 5 | 522 |
| その他製造業 | 窯業・土石製品製造業 | 10 | 1,130 | | 宗教法人 | 0 | - |
| | その他製造業 | 35 | 1,901 | | 高校 | 2 | 69 |
| 商　業 | 卸業・商社 | 31 | 566 | | 大学 | 17 | 602 |
| | 小売業 | 12 | 3,795 | | その他の教育機関 | 5 | 299 |
| 金融・保険業 | 金融業 | 54 | 1,469 | | 学術研究機関 | 4 | 231 |
| | 証券業・商品取引業 | 3 | 4,280 | | 法人団体・農協 | 13 | 587 |
| | 生命保険業 | 10 | 4,786 | 政府・地方公共団体 | 政府 | 3 | 1,250 |
| | 損害保険業 | 7 | 4,428 | | 地方公共団体 | 51 | 3,271 |
| 小　計 | | 328 | - | 小　計 | | 277 | - |
| 合　計 | | | | | | 605 | 平均　2,256 |

## 1.2 調査結果の要約

本調査は、今日の情報システム環境に鑑みて、情報リスクマネジメントに重点を置き、10領域の調査項目について構成を修正した。しかし、これまでの調査結果との比較が必要な項目については時系列分析ができるよう項目を残している。また、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。

### 1.2.1 経済産業省の安全対策の施策について

経済産業省の情報システムの安全対策に関する諸施策には、各種対策における指針を示す『情報システム安全対策基準』、『コンピュータウイルス対策基準』、『コンピュータ不正アクセス対策基準』ならびに『システム監査基準』がある。さらに、被害の実態を把握して改善措置を図るための『コンピュータウイルス被害届出制度』、『コンピュータ不正アクセス被害届出制度』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『JPCERT/CC（JPCERTコーディネーションセンター）』の設置、システム監査企業を登録し一般に紹介する『システム監査企業台帳制度』がある。また、平成15年4月からは『情報セキュリティ監査制度』および情報セキュリティ監査企業を一般に紹介する『情報セキュリティ監査企業台帳制度』の運用が開始された。

こうした情報セキュリティ関連の基準について、「利用している」、「知っている」とする回答はいずれも7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、情報システム環境の変化に鑑みて、どれだけの事業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14.9%が「利用」しており、「知っている」のは60.8%であった。『コンピュータウイルス対策基準』の場合は14.2%が「利用」しており、「知っている」は62.8%である。『コンピュータ不正アクセス対策基準』については11.9%が「利用」しており、「知っている」は64.8%である。『システム監査基準』については「利用している」が他の基準に比べ低く、1割にも満たない（8.4%）という結果となった。知っていながらもなぜ利用率が低いのか、その理由を分析する必要があるかもしれない。『システム監査企業台帳制度』については「知っている」が44.5%であるが、「利用している」は2.3%と非常に低い。

『情報セキュリティ監査制度』については、運用開始後あまり時間が経過していないが、半数を超える54.5%が「知っている」と回答した。『情報セキュリティ監査企業台帳制度』については、システム監査企業台帳の利用率とほぼ同じ割合となった。（「知っている」41.0%、「利用している」3.3%）（Ｑ1）。

平成7年8月に阪神・淡路大震災での被害状況を反映して改訂された『情報システム安全対策基準』は、情報処理サービス業情報システム安全対策実施事業所認定制度がISMS適合性評価制度に移行したことにより、平成16年3月末をもって廃止することとなった。本基準の廃止を「知っている」と回答したのは36.2%である（Ｑ2）。

『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（現：独立行政法人情報処理推進機構、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78.7%で、平成13年度調査（以下、「前回調査」という。）（76.7%）から２ポイント増加した。コンピュータ不正アクセス被害の届出機関としては72.1%（H13：71.0%）が「知っている」と回答しており、前回調査とあまり変化はない（Ｑ３）。

平成８年に制定された不正アクセス被害届出制度と同じ年に活動を開始した『JPCERT/CC（JPCERTコーディネーションセンター；旧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35.9%（H13：42.6%）であり、届出制度と比べるとかなり低く、また、前回調査に比べ約７ポイント減少した（Ｑ４）。

『JIS X 5080 規格：情報技術－情報セキュリティマネジメントの実践のための規範』（平成14年２月制定）の認知度は、「利用している」が10.1%、「知っている」が34.4%である。

『JIS Q 2001規格　リスクマネジメントシステム構築のための指針』（平成13年３月制定）については「利用している」が3.3%、前回調査の0.7%から2.6ポイント増、「知っている」との回答は32.2%と、前回調査21.3%から約10ポイントの増加となった。

『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』（平成11年４月制定）の認知度について、「知っている」との回答は37.5%（H13：26.0%）、「利用している」は8.6%（H13:5.6%）となった（Ｑ５）。

平成13年秋期から情報処理技術者試験に「情報セキュリティアドミニストレータ試験」が実施されているが、同試験については「実際、社員を受験させている」11.4%（H13:7.1%）と試験自体を「知っている」63.0%（H13：57.5%）との回答から、回答事業体の約４分の３がこの試験を認知していることがわかる（Ｑ６）。

### 1.2.2　情報リスクマネジメントについて

現在の情報システム環境におけるリスク対応の実態を把握するため新たに設けたのがこの情報リスクマネジメントについての質問であった。この点について９割以上が重視しているが、その中でリスクマネジメントを「実践している」との回答（26.3%）と「重要と考えている」（63.8%）との差は大きい（Ｑ７）。リスクマネジメントの視点からみると、実際に「実践している」ことと「考えている」との間には、問題が生じた場合の対応コストに大きな違いがあり、この点について過去の事例から判断する必要がある。

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」とする回答は37.0%と前回調査（26.0%）から11ポイントの増加となり、逆に「低い」との回答は22.4%から15.2%に減少した。また、「わからない」は前回調査（15.3%）から7.6%へと、約半数になった（Ｑ８）。この点に関して、情報システム環境の変化に対する経営者層の認識に顕著な変化が生じていることが確認できる。

JIPDECでは、平成４年にリスク分析手法（JRAM）を開発した。その後の情報環境を踏まえ、平成12年度からリスクマネジメントのあり方について調査研究を開始し、リスクマネジメント手法としてJIPDECリスクマネジメントシステム（JRMS）を開発した。調査研究の成果については協会ホームページ等で情報を提供してきたが、今回の認識度調査では「知っている」との回答が27.3%であった。残念ながら、「利用したことがある」との回答はわずか1.7%であったが、今後、JRMS

の利用率が増えていくことが望まれる（Q９）。

情報のマネジメントにあたっては、情報リスクマネジメント方針の明確化、リスク分析、情報セキュリティ対策に係るポリシー類の策定・整備、システム監査の実施等が重要視されるべきである。今回の調査によれば、最も多く実施されているのは「情報セキュリティ対策」（55.7%）、次いで、「情報セキュリティポリシー」の策定（52.2%）、「システム監査」（30.1%）、「情報リスクマネジメント方針」（19.3%）であった。一方で「特に実施していない」とする回答は 24.8%となった（Q10）。事業体の４分の１は特に行っていないことになり、情報システムへの依存度の高まりから、問題視したいところである。

### 1.2.3　情報リスク分析について

リスクマネジメントにおいて重要なのはリスク分析にある。この点から、基幹システムの停止をどう分析しているのか、きわめて重要と考えられる。この点について、基幹システムが１時間以上停止した場合の経営に与える影響（被害額）について、「想定していない」との回答は 77.0%と前回調査（75.9%）よりわずかであるが増大している（Q11）。これまで情報システム関係で問題が生じているにもかかわらず想定していないのが事業体の４分の３であることは、システムへの信頼度が高いのか、いまだに事後的な対応に重点が置かれているのか、考察の余地がある。なお、「想定している」場合の１日における被害想定額は、「１千万円未満」（41.2%）が前回調査（47.1%）同様、最も高い結果となった。次いで高かったのは「１千万円以上～５千万円未満」の 25.2%（前回 18.5%）であった。また、「10 億円以上」も 10.7%あり、利用しているシステム環境によりかなりの違いが把握できる（Q12）。

リスクマネジメントの出発点はリスク分析にあるのが常識である。情報システムに関わるリスク分析の実施状況について、「行っている」は 29.9%と前回調査の 18.8%から 11 ポイント以上の増加となった。「実施していない」は 79.5%から 54.2%と 25.3 ポイント減少したが、これは前回調査で「実施する予定がある」という選択肢がなかったことも関係している（Q13）。

リスク分析実施事業体のうち、８割以上が「ハードウェア障害」、「ソフトウェア障害」、「ネットワーク障害」、「事故」、「コンピュータウイルスのリスク」をリスク分析の対象とした（Q14）。

リスク分析を実施した際の問題点として最も高い割合を示したのは「リスクの定量化が測れない」（61.3%）、次いで「確立した手法がない」（47.5%←H13:62.2%）、「専門家がいない」（38.7%←H13:34.1%）、「分析のためのデータが乏しい」（30.9%←H13:38.5%）という結果となった（Q15）。

リスク分析を実施しない理由については、「手法がわからない」が最も多く 50.6%（H13：47.8%）、「予算がない」（38.1%←H13:26.4%）、「発生被害額が算出できない」（32.9%）、「効果がわからない」（31.7%←H13:31.2%）となった。「重要性を感じていない」は前回調査の 13.3%から 8.5%に減少し、「効果があるとは思えない」（4.9%←H13：6.1%）、「リスク分析の意味がわからない」（4.3%←H13:9.5%）をあわせると、リスク分析に対して 17.7%（H13：28.9%、11.2 ポイント減少）が否定的な見解を示したといえる（Q16）。

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 7.8%と、前回調査の 9.1%とあまり変化はない。前回まで増加傾向にあった「部分的なダウン」は 39.8%（H13：45.0%）

と、前回を約５ポイント下回っている（Q17）。

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「ハードウェア障害」（53.1%←H13:56.7%）、「ネットワーク機器などの障害」（38.5%←H13:41.5%）、「ソフトウェア障害」（25.3%←H13:33.0%）であるが、いずれも前回調査に比べ、減少傾向にある。これらの結果は情報システムの信頼性が上昇したからなのか、以下の質問への回答等との関係からも検討を加える必要がある。

一方、増加傾向にあるのは「コンピュータウイルス」（24.0%←H13:15.7%）、「通信事業者に起因する障害」（14.6%←H13:12.4%）、「ISP 等の社外のインターネットに起因する障害」（8.7%←H13:5.2%）で、特にコンピュータウイルスによるダウンは 8.3 ポイントの増加となった（Q18）。

基幹システムにおける平均故障間隔（MTBF）は 2,773.3 時間で、前回調査の 2,938.7 時間より若干短くなった。また、平均修理時間（MTTR）は 120.0 分で、前回調査の 145.7 分より短くなっている（Q19、Q20）。

コンピュータ犯罪意識に関する質問では次のような結果が得られた。●『市販のソフトをコピーして使う』場合、それが「犯罪行為である（刑法上の処罰の対象となる）」という認識については 59.8%（H13：69.9%、H11：54.2%、H９：50.7%）となり、前回調査に比べ約 10 ポイント減少した。かわりに『企業内で戒告・訓告・注意処分等の対象』が 9.3%から 16.2%へと 6.9 ポイント増加した。●『データ、プログラムを無断で使う』行為が「問題であると思う」との意識は増加している（27.3%←H13:20.8%）が、「企業内でも戒告等の処分の対象となる」（31.9%←H13:27.6%）、「犯罪行為である」（26.6%←H13:38.6%）との意識は減少傾向にある。●『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」割合は増加（37.0%←H13:32.5%）したが、「犯罪行為である」という認識は前回の 25.5%から 16.5%に減少した。●『就業時間内に会社のコンピュータを私用に使う』行為に対しては「問題であると思う」割合は 44.6%（H13：47.1%）であり、「企業内で戒告等の処分の対象になる」が 39.1%から 44.0%に増加した。●『WWW を仕事以外（個人目的での発注、アンケート回答等）で利用する』、『私用の電子メールを送・受信する』という行為は事業体のコンピュータの私的な利用に関する質問であるが、それぞれ 50.1%（H13:46.2%）、52.7%（H13:49.6%）の事業体が「問題であると思う」としている。●『他人の ID を無断借用する』行為については、「企業内で戒告等の処分の対象となる」が 41.0%（H13:34.3%）、「犯罪行為である」が 23.1%（H13:34.4%）、「問題であると思う」が 21.8%（H13:16.6%）となった。●『業務上入手した顧客情報を正当な理由なしに第三者に売却する』という項目では 72.7%が「犯罪行為である」としている（H13:79.5%）。これに「企業内で懲戒免職の対象となる」（16.2%）を加えると約９割が厳しい認識を示している（Q21）。

### 1.2.4 情報セキュリティポリシー・管理・対策について

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 85.5%（H13:77.9%、7.6 ポイント増）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守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」71.2%（H13：53.3%、17.9 ポイント増）で、「管理者の理解」は 39.7%（H13:32.7%）であった。管理者よりも経営者の理解が重要とする回答が多かったのは、経営資源を投入するには経営

サイドの関与が必要と考えた結果であろう（Q22）。

事業体における情報システム関連支出のうち、情報セキュリティ対策にかける支出割合がどれぐらいかを調査したところ、平均6.1%と、前回調査（4.1%）に比べ2ポイント増加した。なお、無回答が3割以上を占めているが、これは対策費用がどれぐらいか把握できないケースが多いものと考えられる（Q23）。

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

情報セキュリティポリシーは事業体における経営理念を反映して構成されるのが一般的と思われる。経営理念に基づいてセキュリティポリシーを「定めている」のは46.1%と、前回調査の24.0%に比べ大幅に増加した。一方、「定めていない」は23.6%で前回調査（32.9%）より9.3ポイント減少した。なお、「作成を検討している」は16.2%と前回調査（28.8%）から12.6ポイント減少した。

実施手続・規程類の策定状況については、「定めている」が34.9%（H13：22.1%、12.8ポイント増）となった。一方「定めていない」は24.1%（H13：32.5%、8.4ポイント減）であった。

セキュリティポリシー、実施手続・規程類ともに「策定済」、「作成中」の事業体をあわせると過半数を越えることになる（Q24）。

Q24で調査したセキュリティポリシーおよび実施手続・規程類の見直しについて、「定期的に見直しをしている」と回答したのが情報セキュリティポリシーで65.9%（H13：66.9%）、実施手続・規程類が82.9%（H13:79.9%）と、いずれも高い値となった（Q25）。

Q24で情報セキュリティポリシーを策定／作成中の事業体（357件）に対し、何を参考にしたかを調査した。最も多かったのは「BS7799やISO/IEC17799、情報セキュリティポリシーに関するガイドライン」で46.5%が参考にしている。次いで「自社で独自に開発している」が39.2%となった（Q26）。

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

ネットワーク管理者については「定めている」のは83.3%（H13:79.2%）である。

情報システムの管理者については、「定めている」のは80.5%（H13:79.1%）である。

情報セキュリティ管理者の設置については、「定めている」が65.5%と前回調査（52.8%）より約13ポイント増加した。いずれの責任者についても、「設置の必要はない」との意見は0件であった。（Q27）。

システム災害／障害、不正アクセス、ウイルスを含む情報セキュリティ管理に関する問題点について調査したところ、「組織の従業員に対する教育・訓練がいきとどかない」が最も多く54.5%（H13:61.1%）、「コストがかかりすぎる」53.6%（H13:51.9%）、「専門要員がいない」43.0%、「どこまでやればよいのか基準が定められていない」38.2%（H13:42.1%）、「ノウハウ不足」34.4%（H13:46.1%）が高い割合を示している。「コストがかかりすぎる」および新設の「専門要員がいない」以外では、前回調査と比べ減少傾向にある（Q28）。

情報セキュリティを実現するために重要と思われる要素を10項目とりあげ、それに対する優先順位（1～3位）を調査した。最も重要（1位を選択）と思われているのは「情報セキュリティ

ポリシー（経営者の積極的な関与）」32.9%（H13:36.3%）で、経営者のコミットメントが重視されている。次いで「人的セキュリティ（役職員への教育訓練や内部規則の策定など）」15.4%（H13:11.8%）である。次に「通信および運用管理（ネットワークの管理、ウイルス対策、ログ管理など）」11.1%（H13:12.3%）、「情報セキュリティ組織（情報セキュリティの推進組織の構築と活動）」10.4%（H13:12.1%）という結果となった。なお、「人的セキュリティ」は前回調査で４番目に多かったが、今回２番目となった。

また、優先順位をつけずに選択のみをしたケースの結果については、「人的セキュリティ」（51.4%←H13:41.3%、10.1ポイント増）、「情報セキュリティポリシー」（47.4%←H13:49.6%）、「通信および運用管理」（42.1%←H13:51.4%、9.3 ポイント減）、「情報セキュリティ組織」（35.5%←H13:38.7%）の順となった（Q29）。

### 1.2.5 災害対策・障害対策について

情報セキュリティポリシー、実施手続・規程類に基づいた災害・障害対策が明確になっているかとの質問に対し、44.1%が「特に定めていない」という結果となったが、前回調査（53.6%）に比べると 9.5 ポイント減少し、「情報セキュリティポリシー、実施手続・規程類の中で明確になっている」との回答は前回調査の 19.1%から 27.4%へと増加した（Q30）。

『JIS X 5080 規格』の事業継続性管理で定められている事業継続性計画の作成状況について、「作成していない」との回答が過半数を大幅に越える 64.8%となった（Q31）。

Q31 で事業継続性計画を「作成している／作成中である」と回答した 102 の事業体に対し、何を対象としているかを調査した。もっとも多いのは「事故・災害」で 95.1%、次いで「障害」（78.4%）である。前回調査では、質問を「危機管理マニュアルの項目」としていたが、上記２項目については前回同様、高い回答率であった。なお、「外部からの悪意による緊急事態（サイバーテロ、ウイルス等）」が前回調査の 11.7%から 43.1%へと 31.4 ポイントと大幅な増加となった（Q32）。

さて、情報システムの災害に対する復旧対策の実施状況について、「データのバックアップを定期的に実施」（80.7%）が最も多く、「サーバのバックアップ用ファイルを自社内保管」（38.0%）、「PC 中の業務用ファイルのバックアップ」（34.0%←H13:55.2%、21.2 ポイント減）、「ネットワークのバックアップ」（32.4%←H13:36.2%）、「手作業への復帰」（31.7%←H13:29.4%）となった。なお、「特に対策を講じていない」は 2.5%と前回調査の 8.4%から 5.9 ポイント減少した。なお、「対策を講じていない」理由で回答率が最も高いのは「コストがかかりすぎる」で 53.3%（H13：46.7%）であった（Q33、34）。

情報システムの障害対策のために設置している機能について調査した。基幹システムがメインフレームの場合、最も高い回答率を示したのは「ホットスタンバイシステム」（23.5%←H13:16.4%）で、クライアントサーバシステムの場合は「ミラリング」の 50.1%（H13:42.5%）であった。一方、「特に設けていない」は前回調査の回答率 28.3%から 17.4%へと 10.9 ポイント減少した（Q35）。

サーバ設置場所およびデータ保管場所の火災対策について調査した。サーバ設置場所では「自動火災報知設備」（76.0%）、「消火器」（63.0%）、「消火・排煙等の防災機器の定期的点検」（56.5%）の順となった。データ保管場所では「自動火災報知設備の設置」（69.3%）、「消火器」

(57.4%)、「消火・排煙等の防災機器の定期的点検」(53.4%) と、両者とも同じ順位となった。(Q36)。

地震対策に関しては、結果はほぼ前回調査と同じく、サーバ保管場所で最も多い回答は「転倒防止措置」(56.0%) で、次いで「機器の移動防止措置」(39.5%)、「建物が耐震構造」(36.4%) であった。データ保管場所では「転倒防止措置」(40.5%)、「建物が耐震構造」(35.9%)、「機器の移動防止措置」(27.1%) と両者とも同じ順位となった。「特に対策を講じていない」との回答については、サーバ設置場所が22.3%、データ保管場所は24.3%と、火災対策 (ともに6.8%) に比べ、地震対策の実施率は低くなっている。Q29で『重要と思われる情報セキュリティ要素』の調査を行った。この中で「物理的および環境的セキュリティ」の複数回答結果が 12.1%で 10項目中第8位と評価が低かったが、地震国日本において果たしてこのままでよいか、再考する必要がある。(Q37)。

電源設備についての対策では、前回調査同様、圧倒的に「CVCF/UPS」86.8% (H13:80.4%) が多く、次いで「自家発電装置」が36.9% (H13:30.5%) となった (Q38)。

水冷の空調設備を使用している場合、何らかの災害が発生した場合に電源設備の予備が完備していても水冷用の水の供給がなければコンピュータが作動できない。そこで、どれぐらいの水を確保しているかを調査した。約半数が水冷の空調設備を使用していないが、使用している事業体のうち、「まったく確保していない」が8.8%という結果となった (Q39)。

情報システム、サーバ設置場所、機器の災害・障害対策で今後強化すべきこととして最も多かったのは「回線障害対策」(46.0%)、「ハードウェア障害対策」(42.8%)、「自然災害対策」(39.0%)、「人の悪意による事故等への対策」(35.7%) となった (Q40)。

ネットワーク環境下での問題状況として、どのようなネットワーク機器・サービス障害を想定しているか調査を行った。特に回答率の高かったのは「ルータ、サーバ (機器) 障害」が80.3% (H13:74.7%)、次いで「LAN (配線) の障害」64.0% (H13:64.5%) であった。いずれも自事業体内での障害を中心に想定している(Q41)。

ネットワーク障害に対する対策については、「重要回線を部分的に二重化」31.9% (H13:25.8%)、「通信機器の二重化」24.6% (H13:21.6%)、「異なる種別回線を利用」23.1% (H13:21.2%)、「専用のバックアップ回線を常時設定」18.2% (H13:17.8%) 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28.3% (H13:34.5%、H11:48.6%、H9:51.9%) と傾向としては対策を講じていない割合は減少している(Q42)。

### 1.2.6 不正アクセス対策・不正侵入対策・情報漏洩対策について

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、翌年2月に施行された。この法律を「知っている」との回答は81.3%と、前回調査 (76.7%) から4.6ポイント増加した (Q45)。

不正アクセスの被害状況については、「物理的アクセス被害 (コンピュータ室等への侵入)」が0.2%、「論理的アクセス被害 (ネットワーク経由の侵入)」は8.9% (H13:14.6%) と、それほどの被害は受けていない (Q46)。

不正アクセス被害を受けた事業体がIPAに被害届を出したかどうかを調査したところ、18.2%が「出した」と回答している。Q2で72.1%が「IPAが被害届出機関であることを知っている」

と回答しているが、「知っている」のであればなぜ届け出ないのか。前回調査に引き続き「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、その原因を究明することも必要かもしれない（Q47）。

不正アクセス対策の実施状況を調査した。まずサーバ設置場所またはデータ保管室での物理的不正アクセス対策として、最も多く実施されている対策としては、「室の出入口で入室管理／退室管理を行っている」（57.5%／42.1%）、「室の管理責任者を定めている」（46.6%）、「入退室についてカード、パスワードを使用している」（45.5%）となった。最も増減が大きかったのは「出入口での入室管理」で、前回調査の45.3%から57.5%へ12.2ポイントの増加となった。一方、「特に対策を講じていない」は前回調査の25.6%から18.3%へ7.3ポイント減少した（Q48）。

次にネットワークを介しての論理的不正アクセス対策について、最も多く行われているのは「ファイアウォールの利用」（83.3%）で、前回調査の69.1%から14.2ポイント増となった。次いで「パスワードの活用」（67.9%←H13:66.3%）、「セキュリティパッチの適用」（61.0%）、「ネットワーク機器の運用者（アクセス範囲）の限定」（51.4%←H13:49.0%）、「ネットワーク管理者がサーバ、ルータ、ファイアウォールのログを定期的にチェック」（42.6%←H13:41.5%）と続いている（Q49）。

情報についての機密度のランク設定に関しては「設定していない」が前回調査の68.2%から56.7%へ大きく減少した（Q50）。

基幹システムのパスワード変更設定のレベルについては、「パスワードの変更を推奨しているが、変更期間は利用者に任せている」が最も多く、27.9%（H13:35.8%、7.9ポイント減）であった（Q51）。

今回調査で新たに設けた情報漏洩対策について、「入退室（館）管理」（54.5%）、「アクセス管理」（53.1%）、「セキュリティポリシー、規程類の整備」（52.7%）、「ハードディスク、CD、FD等記録媒体の返却、廃棄時の破壊、溶解」（50.9%）が過半数を越えている（Q52）。

### 1.2.7　コンピュータウイルス対策について

過去1年間でコンピュータウイルスに感染したか否かの調査では、70.1%（H13:68.8%）がウイルスに感染したことが「ある」と回答している。このうち、コンピュータウイルスの被害に遇った場合の届出状況については、IPAに被害を届け出たのは13.9%と、前回調査（19.8%）よりも5.9ポイント減少した（Q53、Q54）。

主な感染原因（経路）については、電子メール自動感染型ウイルスによる被害が拡大しているが、「電子メールの添付書類で」（47.6%）が前回調査（67.0%）と比べ19.4ポイント減少した。また、「インターネット経由」による被害が前回調査の42.1%から45.8%へと微増した（Q55）。

コンピュータウイルス対策の実施状況を調査した。もっとも多く行われている対策としては「ワクチンソフトの利用」で86.6%（H13:84.8%）、次いで「ワクチンソフト・パラメータファイルの定期的更新」75.0%（H13:67.1%、7.9ポイント増）、「サーバ機でのワクチンソフトの利用」（71.6%←H13:61.6%、10ポイント増）となっている。実施率は低いながらも前回調査と比べ増加が著しかったのは「メール用ゲートウェイ／サーバでのワクチンソフトの利用」で、前回調査の44.3%から62.3%へと18ポイント増加した（Q56）。

### 1.2.8 アウトソーシングについて

昨今の事業体の経営実体から、アウトソーシングの利用についてリスクの面からも考慮すべきである。システム運用にあたり、アウトソーシングを利用している事業体は、49.6%である。アウトソーシング先選定時の観点としては、「コスト」(67.0%)、「専門性」(62.7%)、「品質(サービスレベル)」(61.0%)が重視されている(Q57、Q58)。

アウトソーシング先との契約について情報セキュリティ関係で重視している項目としては「守秘義務契約」(72.0%)が圧倒的に多く、次いで「サービスレベル」(47.3%)、「事故後の早期復旧対策」(36.7%)と続いている(Q59)。

### 1.2.9 システム監査・情報セキュリティ監査について

情報システムを利用する事業体において、監査の視点は不可欠である。システム監査の実施状況について、「実施している」との回答は35.9%(H13:34.8%)とほとんど変化はなかった。実施している事業体217件に対し、どのような効果があったかを調査した。「担当者がリスクを考慮しながら業務を実行するようになった」と「要員が規定・ルール等を意識して業務を実行するようになった」がともに38.7%と最も多かった(Q60、Q61)。

Q60でシステム監査を実施しない事業体(315件)の理由として最も多いのは前回同様、「システム監査実施のためのコンセンサス、組織風土が十分に備わっていない」(39.0%)で、全体の約4割を占めた(Q62)。

平成15年4月より情報セキュリティ監査制度の運用が開始されたが、情報セキュリティ監査の実施状況について、「実施した」との回答は18.2%、「実施しない」が59.3%となった。システム監査の実施状況(35.9%)と比べ、約半数の結果となった(Q63)。

情報セキュリティ監査を実施しない理由としては、システム監査同様「情報セキュリティ監査実施のためのコンセンサス、組織風土が十分に備わっていない」が42.6%ともっとも多い(Q64)。

### 1.2.10 個人情報保護について

個人情報の取扱い状況について、「従業員情報」が当然ながら最も多く82.5%、次いで「顧客サポート」(40.5%)、「売買等契約の履行」(32.2%)、「代金等の回収」(31.4%)となった(Q65)。

平成15年に公布された『個人情報保護法』の認知度については、「内容を知っている」(46.9%)および「制定されたことを知っている」(43.6%)から、9割が法律の存在を認知していることがわかる。この個人情報保護法が具体的に施行されるのは平成17年4月からであるが、公布から施行までの2年間の間に行う対策については「現状の管理体制で十分なため、特に対応策を講じない」(26.9%)が「個人情報保護のための規程の整備」(26.8%)をわずか0.1ポイント上回った(Q66、67)。

個人情報の管理状況に対するリスクの認識度について、「いつ問題が発生してもおかしくない状況であると認識している」との回答が27.9%と最も多く、次いで「何度かヒヤリ・ハッとした経験があり、リスクがある認識している」(20.0%)となった(Q68)。

現在行っている個人情報保護対策および今後実施を予定している対策について調査した。現在行っている対策のうち、最も多いのは「管理責任者の設置」(36.0%)、「個人情報保護に関する規程の策定および運用」(34.7%)である。今後の予定している対策としては「社員教育に個人情報

保護に関するカリキュラムを追加し、定期的に教育を実施」(25.0%)、「個人情報保護規程の策定・運用」(24.0%) となっている (Q69)。

従業員情報を除く個人情報の収集方法としては「営業活動により情報主体から直接入手」が最も多く 74.5% (H13:76.7%)、かなりの差をもって「業務委託契約等に基づき提供を受ける」が 18.1% (H13:12.5%) である (Q70)

Q70 で「直接収集している」と回答した事業体のうち、収集・利用目的について同意をとっているかとの質問に対しては「同意をとっている」が 46.1%と前回調査の 59.1%から 13 ポイント減少した。また、直接収集する場合、情報主体に対し利用目的を通知して同意を得ることについて、「当然必要である」との回答が 66.0%と最も多い (Q71)。

Q70 で「間接的に収集している」と回答した事業体のうち、収集・利用目的についてきちんと対応しているかの調査に対し、「情報主体が他社への提供について同意していることを情報提供者 (入手先) に確認している」が 35.7%、その一方で、「何もしていない」との回答が3割弱もあるのは問題である (Q72)。

個人情報を外部委託する際に委託先と取り交わす条項として、「秘密保持義務」を条項に入れる事業体が圧倒的に多く 56.0% (H13:41.4%、14.6 ポイント増)、次いで「目的外使用・再委託禁止」(41.8%)、「個人情報の適切な管理」(39.8%←H13:24.7%、15.1 ポイント増) となった (Q74)。

JIPDEC では個人情報保護対策の一環として平成 10 年4月から『プライバシーマーク制度』を運用している。このプライバシーマークの認定を受けることに対し、4分の3の事業体が有効視しつつも、そのうちの 44.8%は「有効ではあるが、事業者への負担が重い」と感じている (Q75)。

上記を総括すると、個人情報の必要性の認識が十分ではなく、また対策の実施も不十分である。残念ながら過去1年間においても以下のような大規模な個人情報漏洩・紛失事件が発生した。

| 会社名 | 漏洩・紛失情報 | 件数(推測) | 被害による影響 |
|---|---|---|---|
| アプラス | クレジットカード分割払いのお客様情報の一部 | 80,000 人分 | DM会社への流出 |
| JCB、UFJカード、ららぽーと | スヌーピータウンメンバーズ JCB カード 会員登録情報 | 7,000 人分 | 対象者へ 1,000 円のギフトカード送付 |
| ファミリーマート | ファミマクラブ メールマガジン配信希望会員情報 | 18 万 3,000 人分 | 二次災害(架空請求詐欺)が発生 |
| ローソン | ローソンパスの会員情報 | 56 万件 | 500 円のお見舞金支払い |
| 三洋信販 | 顧客情報 | 32 万人分 | 二次災害(騙り・詐欺)が発生 |
| NTTデータ | 不動産情報サイト HOME4U(ホームフォーユー) 査定依頼情報 | 4,300 人分 | |
| ソフトバンク | ソフトバンク BB 加入者情報 | 470 万人分 | 恐喝、500 円のお見舞金支払い |
| ジャパネットたかた | 顧客情報 | 数十万人分 | 営業自粛 |
| シティバンク | 国内顧客に向けた取引明細書のバックアップデータ | 12 万口座分 | |

今後このような事件を未然に防ぐため、現代社会において個人情報の保護対策についてより一層の強化を図る必要がある。

# 2．調査結果の詳細

## 2.1　経済産業省の安全対策の施策について

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

（左欄：件数／右欄：%，以下同じ）

| 施策 | 利用している | | 知っている | | 知らない | | 無回答 | | 計 | |
|---|---|---|---|---|---|---|---|---|---|---|
| 情報システム安全対策基準（平成7年8月改訂） | 90 | 14.9 | 368 | 60.8 | 140 | 23.1 | 7 | 1.2 | 605 | 100.0 |
| コンピュータウイルス対策基準（平成7年7月改訂） | 86 | 14.2 | 380 | 62.8 | 133 | 22.0 | 6 | 1.0 | 605 | 100.0 |
| コンピュータ不正アクセス対策基準　（平成8年8月制定） | 72 | 11.9 | 392 | 64.8 | 135 | 22.3 | 6 | 1.0 | 605 | 100.0 |
| システム監査基準（平成8年1月改訂） | 51 | 8.4 | 391 | 64.6 | 154 | 25.5 | 9 | 1.5 | 605 | 100.0 |
| システム監査企業台帳制度（平成3年3月制定） | 14 | 2.3 | 269 | 44.5 | 312 | 51.6 | 10 | 1.7 | 605 | 100.0 |
| 情報セキュリティ監査制度（平成15年4月運用開始） | 24 | 4.0 | 330 | 54.5 | 243 | 40.2 | 8 | 1.3 | 605 | 100.0 |
| 情報セキュリティ監査企業台帳制度　（平成15年3月制定） | 20 | 3.3 | 248 | 41.0 | 328 | 54.2 | 9 | 1.5 | 605 | 100.0 |

（注）システム監査企業台帳／情報セキュリティ監査企業台帳を利用している場合は「1」を回答。

経済産業省（以下、「METI」という。）が策定している情報セキュリティ関連基準の認知度合いについて、「すでに利用している」に対して「知っている」事業体の回答数・割合は相対的に高く、両者を合算すればいずれも７割前後が認知（「すでに利用している」、「知っている」）している。しかしながら、「すでに利用している」のと「知っている」との意味の違いが重要であり、この点に関しては後述の指摘を重視されたい。平成 13 年度調査（以下、「前回調査」という。）と比べ、認知度の増減に差があったのは「システム監査企業台帳制度」（46.8%）で、前回調査（33.9%）に比べ 12.9 ポイント増加した。しかし制度開始からすでに 10 年以上が経過しているにも関わらず相変わらず認識度は高くない。

一方、平成 15 年３月に制定され、同年４月から運用が開始された情報セキュリティ監査制度の認知度については、制度開始から半年ほどしか経っていないにも関わらず、約６割が同制度を認識している。業種グループ別にみると、政府・地方公共団体の認知度が 87.1%と最も高く、次いで情報処理サービス業（85.1%）、電気・一般・輸送用機械製造業（58.5%）と続いている。しかし、同台帳制度の認知度についてはシステム監査企業台帳に近い結果となった。

情報システム安全対策基準の認知度については、前回調査の 68.0%に対し、今回調査では 75.7%と 7.7 ポイントの増加となった。

コンピュータウイルス対策基準の認知度については、前回調査の 69.3%から 77.0%へ 7.7 ポイントの増加となった。

コンピュータ不正アクセス対策基準は、前回調査の 68.7%から 76.7%と８ポイントの増加と

なった。

システム監査基準は、前回調査の 68.2%から 73.0%と、4.8 ポイントの増加となった。

システム監査企業台帳については、前述のとおり 12.9 ポイントの増加となった。前回調査では減少傾向にあったが、今回大幅に増加した。しかし、特に「利用している」割合が 2.3%と低いのが他の基準に比べ目立っている。

情報セキュリティ監査企業台帳は制度開始初年度ということから、6 月の申告後、特例により第 2 回目の登録申告期間が設けられ、翌 16 年 1 月に台帳の更新版が公開された。

上記の基準類、各監査企業台帳は下記のページで公開されている。特にシステム監査企業台帳および情報セキュリティ監査企業台帳は、最新の情報を公開しているので、各監査を外部へ依頼しようとする事業体は、それぞれの台帳を活用してもらいたい。

・METI「情報セキュリティに関する政策、緊急情報」のページ

http://www.meti.go.jp/policy/netsecurity/index.html

・JIPDEC「システム監査企業台帳制度支援」のページ

http://www.jipdec.jp/security/daityo/gaiyo.htm

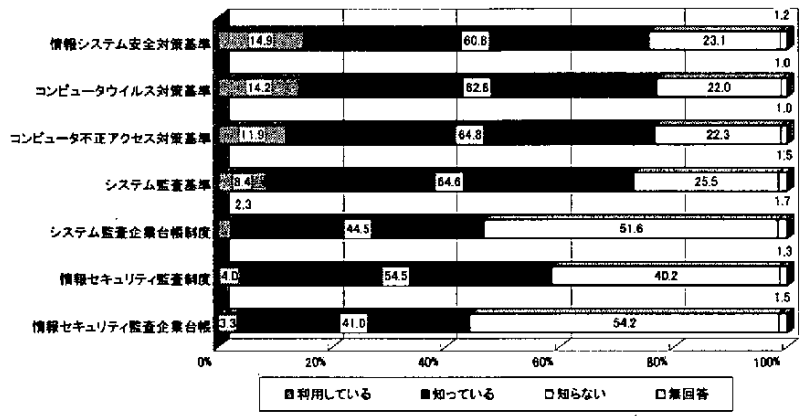
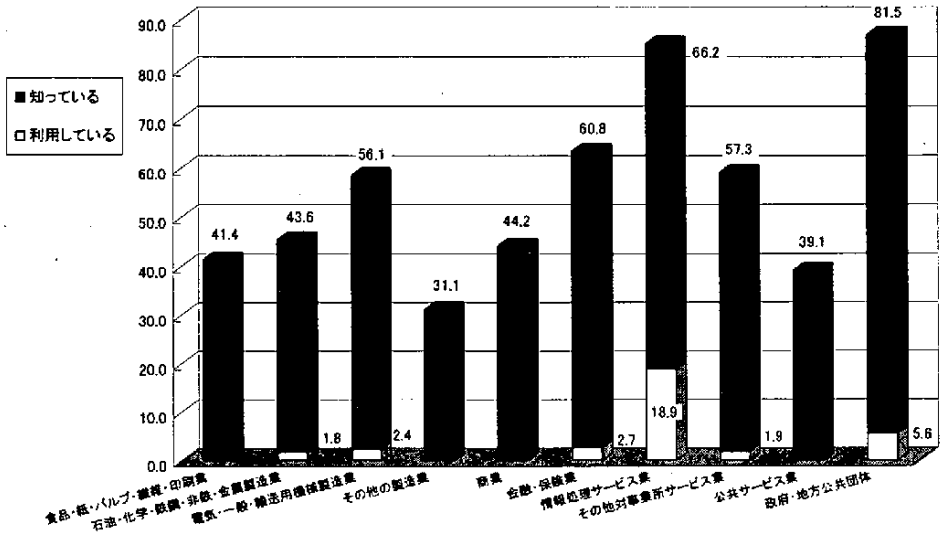



図2－1－1. 経済産業省策定の安全対策関連施策の認知度




2－1－2. 情報セキュリティ監査制度の認知度（業種グループ別）

Q２．（Q1 で「情報システム安全対策基準を利用している／知っている」と回答した場合）情報処理サービス業情報システム安全対策実施事業所認定制度が、情報セキュリティマネジメントシステム(ISMS)適合性評価制度に移行したことに伴い、「情報システム安全対策基準」が平成16年３月末をもって廃止されることを知っていますか。

| | | | |
|---|---|---|---|
| 1 | 知っている | 166 | 36.2 |
| 2 | 知らない | 285 | 62.2 |
| 無回答 | | 7 | 1.5 |
| 計 | | 458 | 100.0 |

情報処理サービス業システム安全対策事業所認定制度が平成13年３月末で廃止（平成12年度経済産業省告示第471号）され、ISMS適合性評価制度に移行されたことに伴い、情報システム安全対策基準も平成16年３月末で廃止されることになっている。本基準の廃止を認知している事業体は４割に満たない。なお、基準自体は廃止されるが、（財）金融情報システムセンター（FISC）や（社）電子情報技術産業協会（JEITA）などが策定するガイドライン等には安全対策基準内容が反映されているので、それぞれ参考にしてもらいたい。

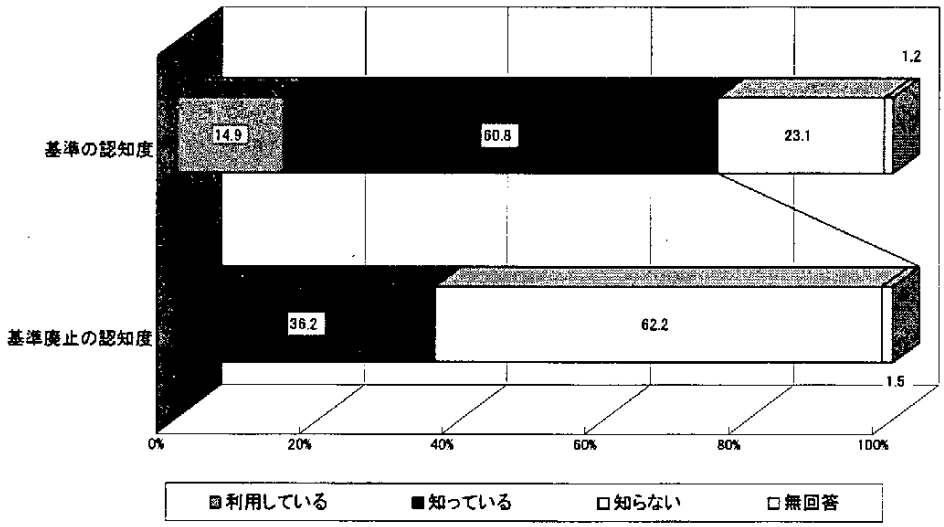



図2－1－3. 情報システム安全対策基準廃止の認知度

Q３．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) | 476 | 78.7 | 128 | 21.2 | 1 | 0.2 | 605 | 100.0 |
| コンピュータ不正アクセス被害(届出機関) | 436 | 72.1 | 167 | 27.6 | 2 | 0.3 | 605 | 100.0 |

METIは、コンピュータウイルス対策基準およびコンピュータ不正アクセス対策基準の策定に合わせて、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）[1]を指定している。これ

[1]（特）情報処理振興事業協会は、平成16年１月５日より独立行政法人情報処理推進機構に組織変更し、新たな活動を開始した。

は、被害の状況を把握することによって被害内容の分析と的確な対応策の検討を行い、被害の減少化に役立てようとするものである。

いずれも、被害届出機関としての存在は、回答の７割以上が認知している。

コンピュータウイルス被害届出機関に関しては、前回の 76.7%から 78.7%と、２ポイント増加した。業種グループ別では大きな差異は特に認められないが、情報処理サービス（90.5%）、石油・化学・鉄鋼・非鉄・金属製造業（85.5%）、政府・地方公共団体（85.2%）、金融・保険業（81.1%）が高い認知度を示している。また、資本金規模別、従業員数別にみると、大規模になるほど、認知率が高くなっている。

不正アクセス被害届出機関に関しては、前回調査の 71.0%から、72.1%と２ポイント増となった。業種グループ別、規模別でみてもウイルス被害届出機関と同様の傾向を示している。

・IPA セキュリティセンター（IPA/ISEC）の URL：http://www.ipa.go.jp/security/)

Ｑ４．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（JPCERT コーディネーションセンター)」を知っていますか。

| | | | |
|---|---|---|---|
| 1 | 知っている | 217 | 35.9 |
| 2 | 知らない | 380 | 62.8 |
| 無回答 | | 8 | 1.3 |
| 計 | | 605 | 100.0 |

JPCERT/CC は、平成８年８月に任意団体コンピュータ緊急対応センターとして設立、同年 10 月から本格的な業務を開始し、平成 15 年３月に有限責任中間法人 JPCERT コーディネーションセンターと名称を変えて活動を続けている。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、当該事業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事業体においては、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、存在については前回調査（42.6%）と比べ、約７ポイント減少した。

業種グループ別にみると、「知っている」と回答した業種のうち、５割以上を占めたのは、情報処理サービス（60.8%）のみであった。Ｑ３のウイルス／不正アクセス被害届出機関である IPA が７割以上の認知度を持っているのに対し、JPCERT/CC の認知度はかなり低いものとなった。

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

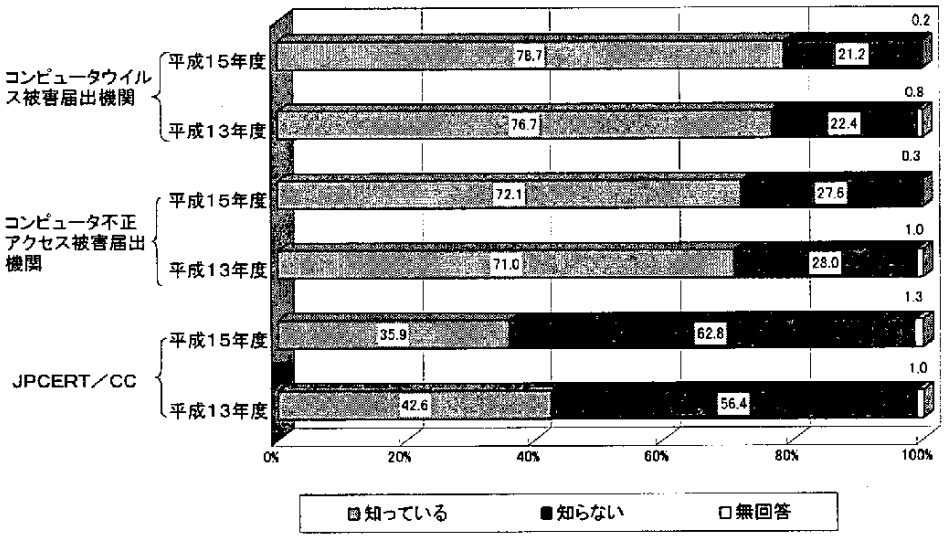



図2－1－4．被害届出機関(IPA)とJPCERT/CCの周知度

Q５．以下のJIS規格を知っていますか。

| 規格名 | 利用している | | 知っている | | 知らない | | 無回答 | | 計 | |
|---|---|---|---|---|---|---|---|---|---|---|
| JIS X 5080:情報技術－情報セキュリティマネジメントの実践のための規範(平成14年2月制定) | 61 | 10.1 | 208 | 34.4 | 329 | 54.4 | 7 | 1.2 | 605 | 100.0 |
| JIS Q 2001:リスクマネジメントシステム構築のための指針(平成13年3月制定) | 20 | 3.3 | 195 | 32.2 | 382 | 63.1 | 8 | 1.3 | 605 | 100.0 |
| JIS Q 15001:個人情報保護に関するコンプライアンス・プログラムの要求事項(平成11年4月制定) | 52 | 8.6 | 227 | 37.5 | 319 | 52.7 | 7 | 1.2 | 605 | 100.0 |

平成７年に英国規格協会（BSI）が制定した情報セキュリティマネジメント規格「BS7799のパート１」を国際標準化した規格「ISO/IEC17799：2000」に準拠した「JIS X 5080：2002 情報技術－情報セキュリティマネジメントの実践のための規範」が平成14年２月に制定されたが、本規格を「利用している」のが10.1％で、これは回答事業体の10分の１しか利用していないことになる。また、「知っている」という34.4％の回答をあわせた認知度は、44.5％である。

業種グループ別にみると、情報処理サービス業（77.0％）、政府・地方公共団体（59.3％）の認知度は高いが、他の業種での認知度は２～４割程度とかなり低い結果となった。

なお、後述Q29の選択肢である情報セキュリティ要素10項目は本規格で定められている情報セキュリティに対する要求事項を用いている。

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

わが国では阪神・淡路大震災を契機に、国際標準化機構（ISO）に対して日本発の国際規格提案

を行うことを目的の一つとして、平成13年3月に「JIS Q 2001：2001　リスクマネジメントシステムの構築に関する指針」を公表した。同規格の場合、「利用している」のがわずか3.3%と低い回答となっている。低さの原因は、同規格の場合、あらゆる事業体を視野に入れているため、現場での利用にはかなりの理解力と適応力が求められるため、やむをえないのかもしれない。しかし、「知っている」32.2%をあわせた認知度は前回調査（22.0%）から35.5%と、13.5ポイントの増加となっている。

業種グループ別にみると、「情報処理サービス業」（70.3%←H13:40.5%）、「その他対事業所サービス」（38.8%←H13:18.4%）については前回調査に比べ大幅の増加がみられた。

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 15001:1999　個人情報保護に関するコンプライアンス・プログラムの要求事項」）を制定した。

「JIS Q 15001」を「利用している」事業体は8.6%と低い。「知っている」という回答37.5%をあわせた認知度は46.1%と、前回調査（31.6%）から14.5ポイントの増加となった。

業種グループ別に認知度の高い順にあげると、情報処理サービス（85.2%←H13:71.6%）、その他対事業所サービス（53.4%←H13:28.7%）、金融・保険業（48.7%←H1345.1%）、公共サービス（47.9%←H13:21.6%）、政府・地方公共団体（46.3%←H13:26.3%）となっている。他の業種はまだ「JIS Q 15001」の認知度合いが低いといえる。

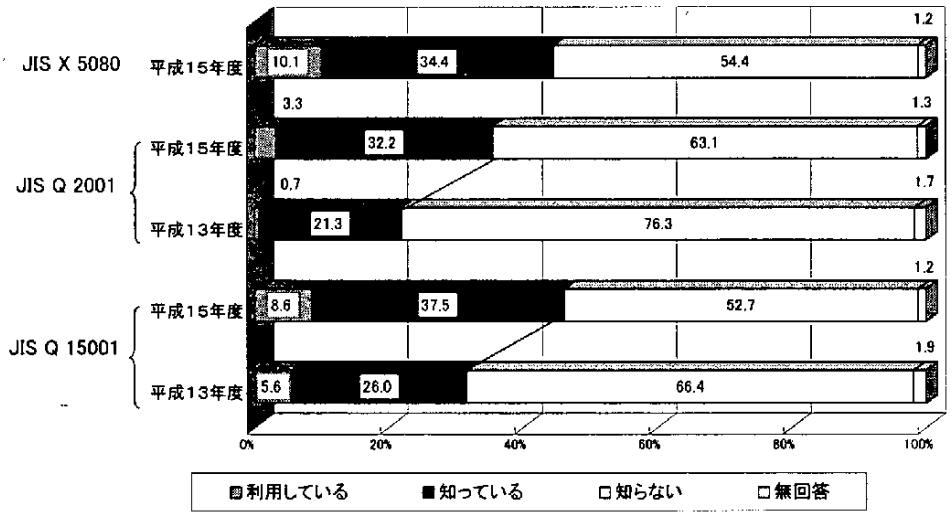



図2－1－5. JIS規格の認知度

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

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

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

・METI の安全対策の施策として該当するものがあることは知っている。内容についても、詳細

に把握している。

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

ところで、上記の回答結果に限定せず、重要なのは、「利用している」と「知っている」との意味の違いである。「知っている」だけでは、現場において情報リスクが実際に発生した場合の対応上、有効性を発揮することにはならない。したがって、情報リスクへの対応は事後的となり、これまでの情報リスク対応の不手際から生じたコスト負担の影響から判断し、あらためて両者の意味の違いを確認する必要があると思われる。

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

| | | | |
|---|---|---|---|
| 1 | 情報セキュリティ担当者をSS試験に受験させている | 69 | 11.4 |
| 2 | 知っている | 381 | 63.0 |
| 3 | 知らない | 154 | 25.5 |
| 無回答 | | 1 | 0.2 |
| 計 | | 605 | 100.0 |

情報セキュリティアドミニストレータ試験は、平成12年度に新設され、平成13年度の10月からこれまでに3回実施され、年々受験者数も増加している。

SS 試験の知名度は、この3年間に64.6%から74.4%と増加しており、受験させている事業体数も4.3ポイント向上している。これは、事業体にとって情報セキュリティが重要な要素と考え、積極的に人材開発を行っていることがわかる。これからは、日本の多くの企業にとって情報セキュリティに対する高レベルの技術者が必要となっていることがわかる。

・情報処理技術者試験センターのURL：http://www.jitec.jp/

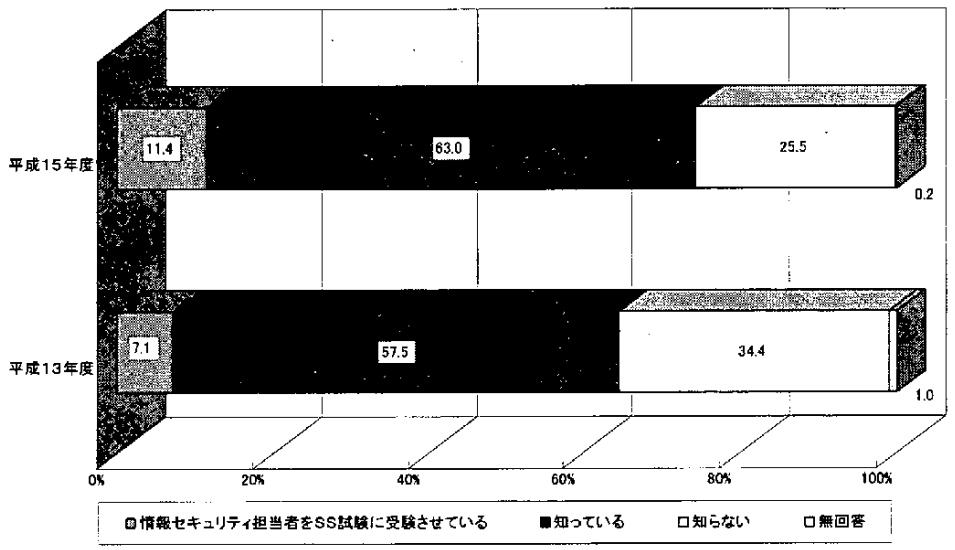



図2－1－6．情報セキュリティアドミニストレータ試験の周知度

## 2.2 情報リスクマネジメントについて

Q７．現代の情報システム環境から、情報リスクマネジメントについてどう考えていますか。

| | | | |
|---|---|---|---|
| 1 | 重要と考え、実践している | 159 | 26.3 |
| 2 | 重要と考えている | 386 | 63.8 |
| 3 | さらに強化する予定がある | 35 | 5.8 |
| 4 | 考えていない | 10 | 1.7 |
| 5 | わからない | 15 | 2.5 |
| 計 | | 605 | 100.0 |

現代の情報システム環境の変化、とりわけシステム利用の高度化、機器の性能の飛躍的な進歩やインターネットの進展等によりリスクに対する脆弱性が高まってきている。それゆえ、METI においても情報システムに関する各種の安全対策関連の基準を実施してきている。環境変化によるリスク対応の基本となるのは情報リスクマネジメントである。この点に関して新たに設けた質問がＱ７である。

回答結果は、図 2-2-1 のように、約 64％が「重要と考えている」と回答している。現実に「重要と考え、実践している」のは約 26％で、「さらに強化する予定」の 5.8％の回答を含めると、約 32％が現実に行っていることになる。いわば、回答者の約 96％が情報リスクマネジメントを重視しており、組織として情報システム環境の脆弱性を十分に認識しているといえる。

しかし、「重要と考えている」と、実際に「実践している」とではリスクマネジメントの視点からみるときに非常に大きな差異がある。それは事業体を脅かす問題が発生した場合の影響に違いが生じるからである。ましてや問題が具体化してからの対応コストは直接的な対応コストに加えて、間接的な信頼性の減少や復旧の時間的コスト等を加味せざるを得ないため、事前的なコストの比ではないといえる。対応を「重要と考えている」だけでは問題の解決にはならないということをあらためて考慮する必要がある。

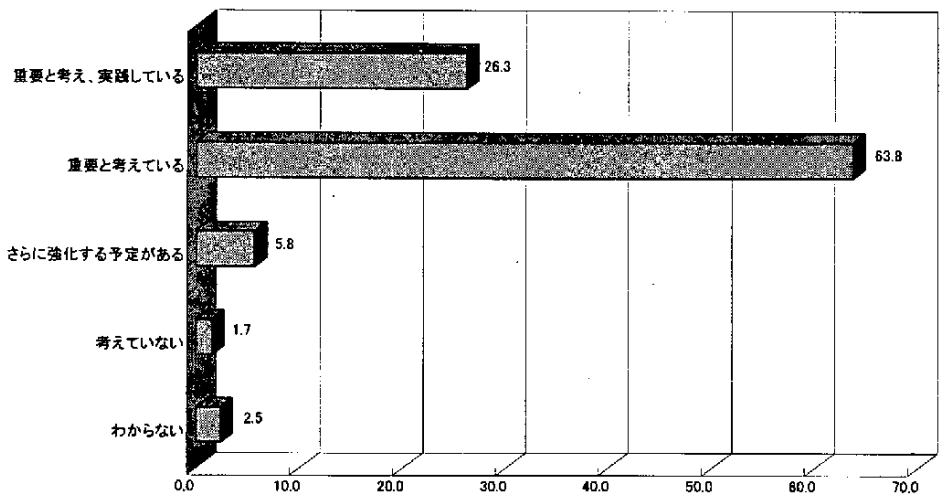



図2－2－1．情報リスクマネジメントに対する考え方

| 情報リスクマネジメントに対する考え方 / 業種グループ | 重要と考え、実践 | 重要と考えている | さらに強化する | 考えていない | わからない |
|---|---|---|---|---|---|
| 食品・紙・パルプ・繊維・印刷 | 10.3 | 75.9 | 3.5 | 3.5 | 6.9 |
| 石油・化学・鉄鋼・非鉄・金属 | 18.2 | 74.6 | 5.5 | 0.0 | 1.8 |
| 電気・一般・輸送用機械 | 26.8 | 69.5 | 1.2 | 1.2 | 1.2 |
| その他製造業 | 11.1 | 64.4 | 15.6 | 6.7 | 2.2 |
| 商業 | 14.0 | 72.1 | 7.0 | 2.3 | 4.7 |
| 金融・保険業 | 56.8 | 39.2 | 2.7 | 0.0 | 1.4 |
| 情報処理サービス | 51.4 | 43.2 | 2.7 | 1.4 | 1.4 |
| その他対事業所サービス | 17.5 | 67.0 | 9.7 | 2.9 | 2.9 |
| 公共サービス | 13.0 | 73.9 | 6.5 | 0.0 | 6.5 |
| 政府・地方公共団体 | 16.7 | 77.8 | 5.6 | 0.0 | 0.0 |

上記の点を業種グループ別にみると、業種による差異が顕著となっている。特に、金融・保険業ならびに情報処理サービス業において実施している割合が高い。相対的に「実践を考えている」という回答が低いのが製造業であるが、情報システムへの依存度は製造業でも高まっているはずであり、実践への取組みを再検討すべきであろう。ただ、「さらに強化する」とする回答が高いのは「その他製造業」であり、製造業の範疇においても、組織の受け止め方の差異を反映していると思われる。

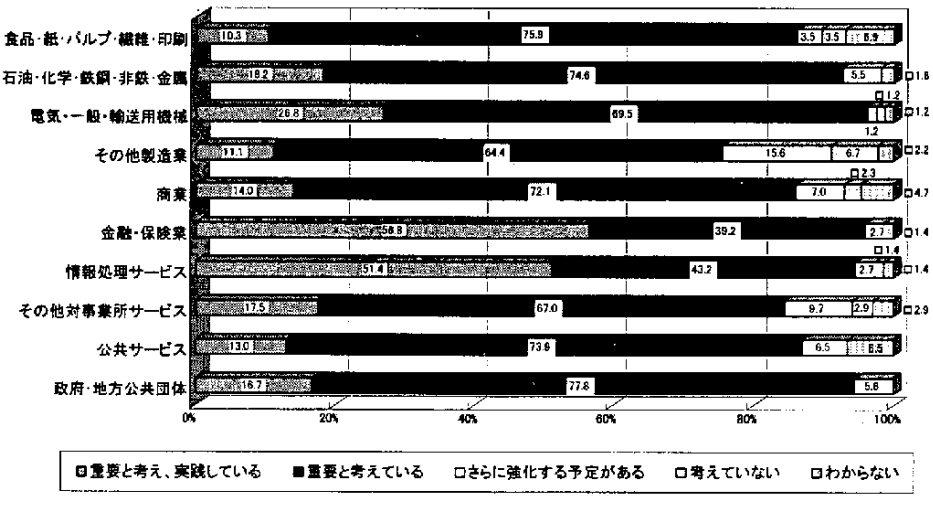



図2－2－2. 情報リスクマネジメントに対する考え方（業種グループ別）

| 情報リスクマネジメントに対する考え方 / 資本金規模 | 重要と考え実践 | 重要と考えている | さらに強化する予定 | 考えていない | わからない |
|---|---|---|---|---|---|
| 500億円以上 | 73.0 | 24.3 | 2.7 | 0.0 | 0.0 |
| 100億円以上500億円未満 | 42.1 | 42.1 | 15.8 | 0.0 | 0.0 |
| 50億円以上100億円未満 | 33.9 | 63.5 | 1.7 | 0.0 | 0.9 |
| 10億円以上50億円未満 | 17.7 | 74.5 | 3.9 | 0.0 | 3.9 |
| 1億円以上10億円未満 | 24.8 | 66.1 | 7.4 | 0.8 | 0.8 |
| 5千万円以上1億円未満 | 16.7 | 63.9 | 10.2 | 7.4 | 1.9 |
| 5千万円未満 | 20.6 | 67.7 | 2.9 | 0.0 | 8.8 |
| 資本金なし | 20.7 | 62.1 | 3.5 | 3.5 | 10.3 |

資本金規模別でみると、情報リスクマネジメントに対する考え方は、実践については規模を反映した傾向がある程度見られる（特に500億円以上）ものの、「重要と考えている」という側面では、50億円未満で相対的に高い割合を示している。

Q８．経営者層はコンピュータ関連の事件・事故に対するリスクについて関心が高いですか。

| | | | |
|---|---|---|---|
| 1 | 高い | 224 | 37.0 |
| 2 | 中位 | 241 | 39.8 |
| 3 | 低い | 92 | 15.2 |
| 4 | わからない | 46 | 7.6 |
| 無回答 | | 2 | 0.3 |
| 計 | | 605 | 100.0 |

経営者が抱いている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の度合いにはかなりの変化が確認できる。今回の調査では「高い」が37.0%となり、前回調査の26.0%（H11：25.5%）に比べて10ポイント以上高まっており、コンピュータ関連の事故・事件に対するリスクについて経営者の関心の度合いにかなりの変化が確認できる。「中位」についても今回は39.8%と前回の35.2%（H11： 33.2%）より高い割合となっており、これに反して「低い」という回答が15.2%と前回調査の22.4%（H11：18.3%）に比べかなり減少してきている。これらの結果は、情報システム環境に関する経営者層の意識がかなり変化してきたことを物語っていると思われる。

業種グループ別にみると、「高い」と回答した割合が高い業種は、金融・保険業（71.6%←H13:56.1%；H11：48.4%）、情報処理サービス業（73.0%←H13:50.0%；H11：50.6%）の２業種であり、増加の割合が顕著である。それぞれ前回に比べて、15.5ポイント、23.0ポイント増と著しい変化が見られる。ところで、政府・地方公共団体では前回調査に比べ約15ポイント高まったものの、いまだ40%以下となっている。しかし、相対的に低いと思われてきた業種においても、前回調査に比べ関心の度合いが高まってきている。たとえば、公共サービスでは15.2%

(H13:5.9%；H11：12.9%)、商業 18.6%（H13:14.5%；H11：14.1%)、その他製造業 17.8%（H13:11.3%；H11：19.7%）であった。これらは現在の情報リスク環境の変化をそれなりに受け止めてきている結果といえる。

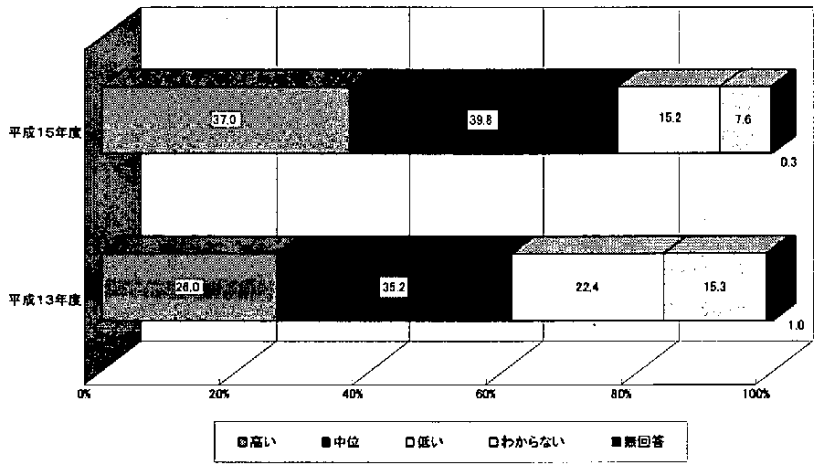



図2－2－3. 経営者のコンピュータ関連の事故・事件に対する関心度合い

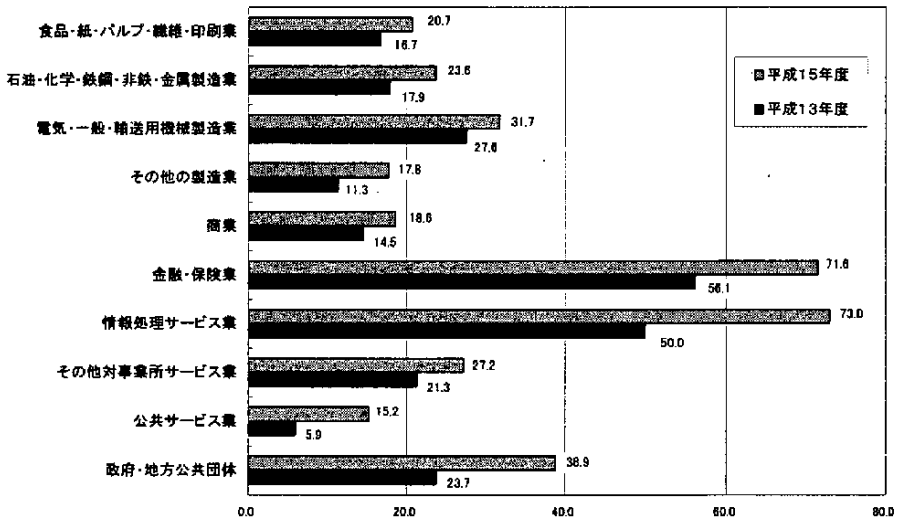



図2－2－4. 経営者のコンピュータ関連の事故・事件に対する関心度合い
（業種グループ別）

| リスクに対する意識 / 資本金規模 | 高い | 中位 | 低い | わからない | 無回答 |
|---|---|---|---|---|---|
| 500億円以上 | 70.3 | 24.3 | 2.7 | 2.7 | 0.0 |
| 100億円以上500億円未満 | 47.4 | 47.4 | 5.3 | 0.0 | 0.0 |
| 50億円以上100億円未満 | 49.6 | 36.5 | 9.6 | 4.4 | 0.0 |
| 10億円以上50億円未満 | 25.5 | 64.7 | 7.8 | 2.0 | 0.0 |
| 1億円以上10億円未満 | 29.8 | 38.0 | 23.1 | 9.1 | 0.0 |
| 5千万円以上1億円未満 | 31.5 | 40.7 | 21.3 | 6.5 | 0.0 |
| 5千万円未満 | 23.5 | 50.0 | 17.7 | 5.9 | 2.9 |
| 資本金なし | 34.5 | 31.0 | 24.1 | 10.3 | 0.0 |

資本金規模別でみると、経営者の関心の度合いが「高い」回答は50億円以上の事業体に多く、「中位」については50億円未満での割合が多くなっており、規模を反映した傾向がみられる。

Q9. 日本情報処理開発協会が開発した「JRMS（JIPDEC リスクマネジメントシステム)」という、リスク分析を含めたリスクマネジメント手法があることを知っていますか。

| | | | |
|---|---|---|---|
| 1 | 利用したことがある | 10 | 1.7 |
| 2 | 知っている | 165 | 27.3 |
| 3 | 知らない | 425 | 70.3 |
| 無回答 | | 5 | 0.8 |
| 計 | | 605 | 100.0 |

JIPDEC は平成４年に『コンピュータセキュリティに関するリスク分析－JRAM によるアプローチ』(以下、「JRAM」という)を発表し、その後の情報環境の著しい変容に鑑みて、平成16年１月に『JIPDEC リスクマネジメントシステム（JRMS）(以下、「JRMS 解説書」という。)』[1] を発刊した。これは、情報リスクについても経営者層、リスクマネジメント部門の認識が不可欠であることを前提に、経営リスク・情報リスクの分析・対策を含め、JIPDEC が開発したリスクマネジメント手法である。

この JRMS について約27%の事業体が「知っている」と回答してくれた。『JIPDEC リスクマネジメントシステムのあり方に関する研究（JRAM2002)』が平成15年３月に公刊され、その「第Ⅳ部 JRMS 質問項目」に今回の JRMS 解説書の試案的な項目が示されている。JRMS について 1.7%が利用したことがあるという回答は、こうした質問項目の利用によるものかもしれない。

しかしながら、JRMS 解説書の発刊前の段階で本調査が実施されたことを考慮に入れれば、７割が「知らない」と回答されたことも当然の結果かもしれない。

今後の情報システム環境におけるリスクマネジメントの重要性を考慮するとき、JRMS に対する理解度が上昇し、社会的な認知を受けるものと確信したい。

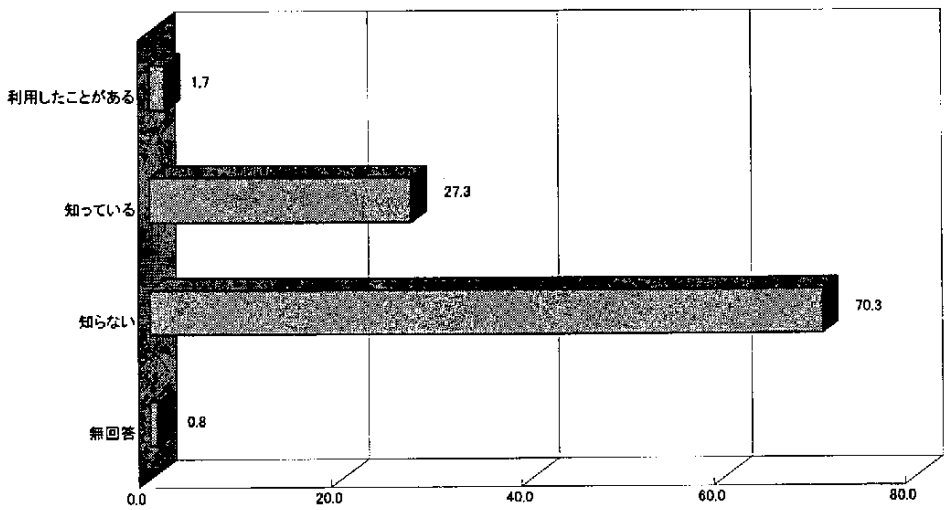



図2－2－5. JRMSの認知度

[1] 「JIPDEC リスクマネジメントシステム（JRMS）解説書」(分析ツール CD-ROM 付) JIPDEC、平成16年１月発行、詳細は http://www.jipdec.jp/chosa/jrms/top.html を参照。

Q10. 情報のマネジメントにおいては、情報リスクマネジメント方針の明確化、情報リスクの分析、情報セキュリティポリシー、情報セキュリティ対策の規程、システム監査等が重要です。これらのうち、貴事業体において実施しているものはどれですか。(複数回答)

| 回答件数 | | 605 | - |
|---|---|---|---|
| 1 | 情報リスクマネジメント方針 | 117 | 19.3 |
| 2 | 情報リスク分析 | 135 | 22.3 |
| 3 | 情報セキュリティポリシー | 316 | 52.2 |
| 4 | 情報セキュリティ対策 | 337 | 55.7 |
| 5 | 情報セキュリティ監査 | 117 | 19.3 |
| 6 | システム監査 | 182 | 30.1 |
| 7 | その他 | 24 | 4.0 |
| 8 | 特に実施していない | 150 | 24.8 |
| 無回答 | | 4 | 0.7 |

情報に関わるリスクマネジメントについて理論的には情報リスクマネジメントの方針が明確化され、その方針に従って情報リスクの分析を行い、その結果の評価を踏まえ情報セキュリティポリシーの立案ならびに情報セキュリティ対策の規程が整備され、システム監査等が実践されることになる。こうした側面は理念的に理解できていても、実践の場では時間とコスト、組織の陣容等の関係もあり、かなりの差異が生じてくるきらいがある。今回の調査では、「情報セキュリティ対策」については55.7%、「情報セキュリティポリシー」には52.2%と、両者について50%以上の回答が得られた。しかし、リスクマネジメントの視点からすれば、情報リスクマネジメント方針に従い、情報リスクにアプローチするという側面はかなり低い結果となった。「情報リスクマネジメント方針」への回答は20%を下回る回答であった。また、「情報リスク分析」についても22.3%の回答となっている。

なお、「情報セキュリティ監査」については、情報リスクマネジメント方針と同じ回答割合であるが、「システム監査」の場合は30.1%であり、システム監査の認識の高まりを指摘できると思われる。ただし、ここで問題なのは約25%が「特に実施していない」という結果となったことである。現在の情報環境は過去と比較にならないほど組織の脆弱性を高めており、知らず知らずのうちに情報リスクを被ったり、また他者に送り込む可能性もあり、リスク認識に関して注意を喚起する必要がある。

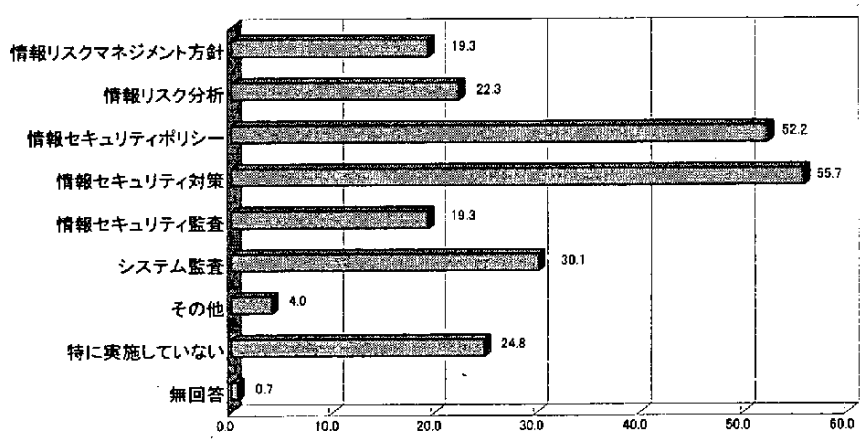



図2－2－6. 情報マネジメント上の実施対策

| 実施対策 / 資本金規模 | 情報リスクマネジメント方針 | 情報リスク分析 | 情報セキュリティポリシー | 情報セキュリティ対策 | 情報セキュリティ監査 | システム監査 | その他 | 特に実施していない | 無回答 |
|---|---|---|---|---|---|---|---|---|---|
| 500億円以上 | 51.4 | 59.5 | 97.3 | 89.2 | 43.2 | 62.2 | 0.0 | 0.0 | 0.0 |
| 100億円以上500億円未満 | 21.1 | 26.3 | 89.5 | 89.5 | 31.6 | 63.2 | 5.3 | 5.3 | 0.0 |
| 50億円以上100億円未満 | 21.7 | 27.0 | 64.4 | 66.1 | 25.2 | 49.6 | 2.6 | 9.6 | 0.0 |
| 10億円以上50億円未満 | 11.8 | 7.8 | 35.3 | 45.1 | 19.6 | 47.1 | 5.9 | 27.5 | 0.0 |
| 1億円以上10億円未満 | 20.7 | 22.3 | 43.8 | 52.9 | 15.7 | 27.3 | 4.1 | 29.8 | 0.0 |
| 5千万円以上1億円未満 | 14.8 | 16.7 | 31.5 | 44.4 | 13.9 | 15.7 | 4.6 | 38.9 | 0.0 |
| 5千万円未満 | 8.8 | 11.8 | 29.4 | 29.4 | 11.8 | 11.8 | 2.9 | 55.9 | 5.9 |
| 資本金なし | 31.0 | 24.1 | 41.4 | 34.5 | 20.7 | 13.8 | 3.5 | 44.8 | 3.5 |

上記の点を業種グループ別にみると、相対的に「高い」割合を示した業種は、Q7、Q8の場合と同様、情報処理サービス業、金融・保険業の順であった。また、業種間において若干の差異がみられるが、製造業と非製造業については製造業の方が相対的に低い回答を示している（「特に実施していない」では逆の回答割合となっており、その根拠については調査結果からは明らかではない）。

とりわけ政府・地方公共団体では「情報セキュリティポリシー」と「情報セキュリティ対策」に関して高い反面、情報セキュリティ監査においては逆の割合となっている。システム監査については7.4%と最低であるが、政府・地方公共団体こそ第三者の目を特に留意すべき組織であり、回答結果からこの点についてあらためて見つめ直す必要がありそうである。

## 2.3 情報リスク分析について

Q11. 基幹システム[注1)]が1時間以上停止した場合、経営に与える影響（被害額）[注2)]がどれ位になるか想定していますか。

| | | | |
|---|---|---|---|
| 1 | はい | 131 | 21.7 |
| 2 | いいえ　⇒Q13へ | 466 | 77.0 |
| 無回答 | | 8 | 1.3 |
| 計 | | 605 | 100.0 |

(注1)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(運用の型は図 2-3-1 参照)。本調査では、その中で最も重要なシステム1つに限定して回答。

(注2)被害額には売上の逸失額、賠償金額、原状回復費用を含む。

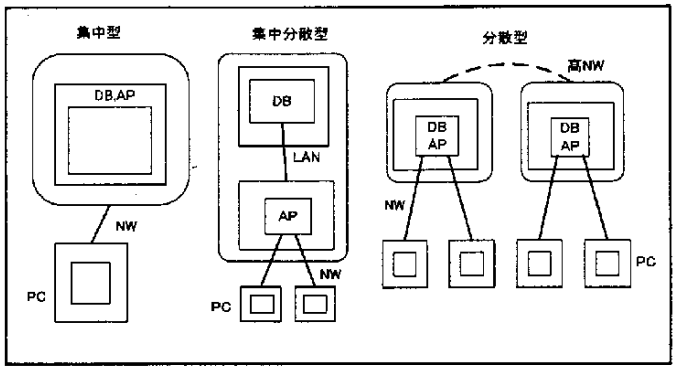



図2－3－1. 基幹システムの運用形態

基幹システムは経営の成果を左右する重要なシステムである。

被害額の想定の有無に関する調査は前回に引き続き2度目であるが、「いいえ」の回答が77.0%（前回75.9%）と圧倒的に高いのが気になる。

基幹システムにかかる費用と経営上の影響を明確にしておかないと、よい基幹システムを持っているにもかかわらず会社は倒産した、という結果になりかねない。

情報システムに対する投資の是非、情報セキュリティにかける費用の目安などを考える基礎を固めるためにも、経営に与える影響は把握しておく必要がある。

ただし、無回答が1.3%（前回2.2%）と低かったことにより、この問題に対する関心が高いことがうかがえる。

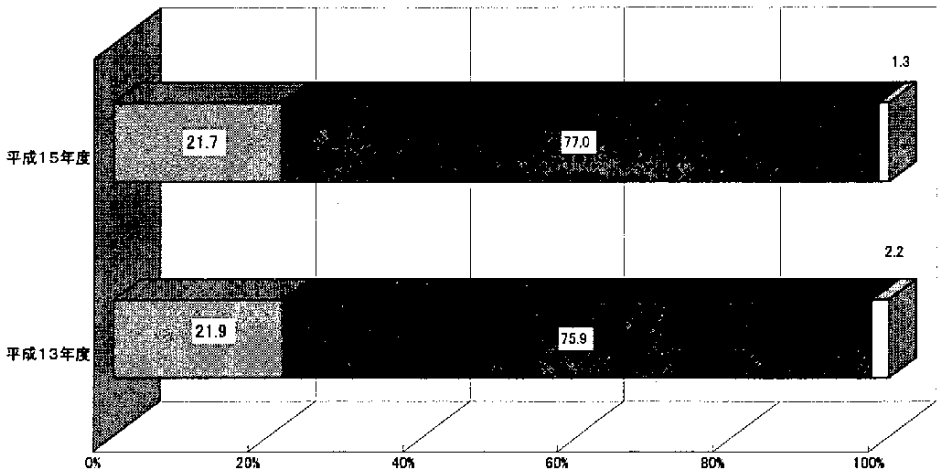



図2－3－2. 基幹システムの停止に伴う経営に与える影響度の想定

| 産業別 | はい | いいえ |
|---|---|---|
| 第二次産業 | 20.3% | 79.3% |
| 第三次産業 | 24.9% | 73.1% |

産業別にみた場合、第二次産業より、第三次産業の方が経営に与える影響を想定している割合が高いといえる。

Q12.（Q11で「1」と回答した場合）被害の推定額は1日あたりどれ位ですか。

| | | | |
|---|---|---|---|
| 1 | 10億円以上 | 14 | 10.7 |
| 2 | 5億円以上～10億円未満 | 1 | 0.8 |
| 3 | 1億円以上～5億円未満 | 14 | 10.7 |
| 4 | 5千万円以上～1億円未満 | 7 | 5.3 |
| 5 | 1千万円以上～5千万円未満 | 33 | 25.2 |
| 6 | 1千万円未満 | 54 | 41.2 |
| 無回答 | | 8 | 6.1 |
| 計 | | 131 | 100.0 |

被害の推定額は1千万円未満が41.2%（前回47.1%）と最も高く、1千万円以上～5千万円未満が25.2%（前回18.5%）が続いている。

基幹システムの停止による1日あたりの被害の推定額は、1時間以上停止した時間をどの程度としたかによって変わってくるが、被害の範囲を直接的被害に抑えた結果として考えると妥当なものであるといえよう。

また、「無回答」が6.1%と前回（3.8%）を上回っているが、影響（被害額）を想定している以上は被害の推定額は把握しておく必要があるだろう。

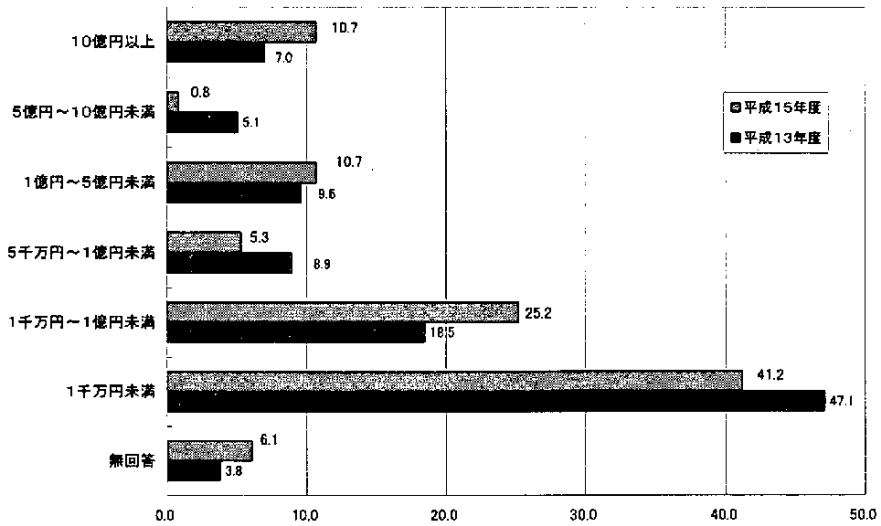



図2－3－3．1日あたりの被害損失額

Q13. 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 | 実施している | 181 | 29.9 |
| 2 | 実施していない ⇒Q16へ | 328 | 54.2 |
| 3 | 実施する予定がある ⇒Q17へ | 91 | 15.0 |
| 無回答 | ⇒Q17へ | 5 | 0.8 |
| 計 | | 605 | 100.0 |

リスク分析はリスクマネジメントの実践にあたり出発点をなすステップである。情報システムの昨今の脆弱性に鑑みれば、リスク分析は不可欠と思われるが、回答結果によれば「実施している」が約30%、「実施する予定がある」としているのは15.0%であった。前述のQ7において、リスクマネジメントの実施について「予定がある」、「実施していない」と「実施している」とではリスクマネジメントにおいて実際的な差に大きな違いがあることについて触れたが、リスク分析を「実施していない」事業体が54.2%を占めた。

この点に関して前回調査と比較すると、リスク分析を「行っている」が18.8%(H11調査12.0%)、「行っていない」が79.5%という点から、情報システム環境におけるリスク分析に対する重要性について顕著な変化が生じてきているといえる。

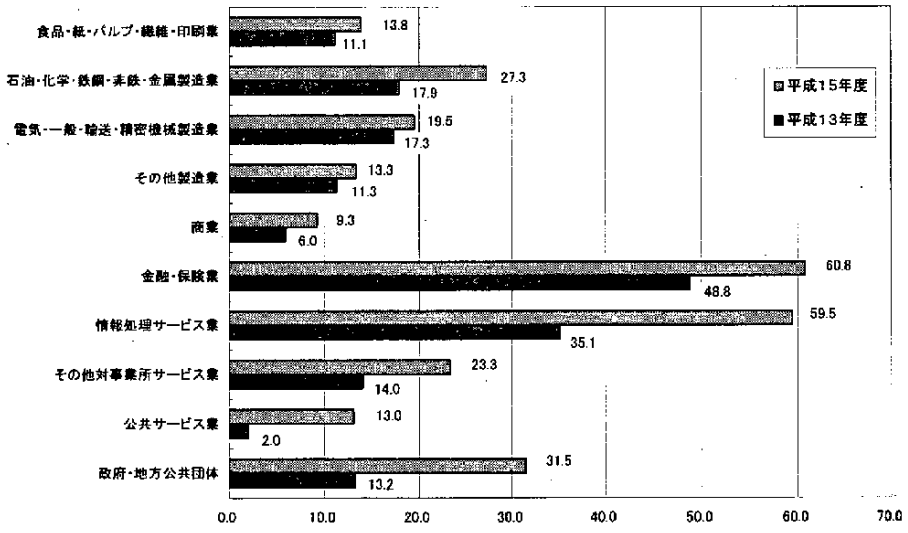



図2－3－4. リスク分析の実施状況(業種グループ別)

業種グループ別にみると、リスク分析の実施割合が高いのは、業種の特性を反映してか、金融・保険業と情報処理サービス業であった。たとえば、金融・保険業で60.8%と前回調査(48.8%)、H11度調査(29.7%)から大幅に増加している。次いで情報処理サービス業で59.5%(H13:35.1%;H11:21.3%)である。これらの業種については前回調査の分析結果報告書で「情報システムの業務への浸透度とともにリスクに対する敏感な業種で・・・その他の業種ではリスクへの関心は低く、合理的な安全対策をすすめるうえでの今後の重要課題といえる。」[1]と指摘したが、情報システムを業務に利用する度合いは、前回に比較して格段の変化があるはずである。この点、いずれの業種についても増加傾向が確認できるが、実施割合が低い業種については今回の調査でもその

1)『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－』JIPDEC、平成14年3月、p82

傾向がうかがえる。ちなみに、「実施していない」業種としては商業(81.4%)、公共サービス(80.4%)、その他製造業（77.8%）となっており、その理由が気になるところである。

| リスク分析 / 業種グループ | 実施している | 実施していない | 実施する予定がある | 無回答 |
|---|---|---|---|---|
| 食品・紙・パルプ・繊維・印刷 | 13.8 | 72.4 | 13.8 | 0.0 |
| 石油・化学・鉄鋼・非鉄・金属 | 27.3 | 58.2 | 14.5 | 0.0 |
| 電気・一般・輸送用機械 | 19.5 | 62.2 | 18.3 | 0.0 |
| その他製造業 | 13.3 | 77.8 | 8.9 | 0.0 |
| 商業 | 9.3 | 81.4 | 9.3 | 0.0 |
| 金融・保険業 | 60.8 | 20.3 | 16.2 | 2.7 |
| 情報処理サービス | 59.5 | 21.6 | 17.6 | 1.4 |
| その他対事業所サービス | 23.3 | 60.2 | 15.5 | 1.0 |
| 公共サービス | 13.0 | 80.4 | 6.5 | 0.0 |
| 政府・地方公共団体 | 31.5 | 44.4 | 22.2 | 1.9 |

次に規模でリスク分析の実施状況を比較すると、資本金別では 500 億円以上が 70.3%（前回 43.1%）、100 億円以上～500 億円未満が 36.8%（前回 34.2%）、50 億円～100 億円未満が 38.3%（前回 21.5%）、10 億円～50 億円未満 17.6%（前回 14.3%）、１億円～10 億円未満 28.9%（前回 13.3%）、５千万円～１億円未満 21.3%（前回 8.3%）、５千万円未満 20.6%（前回 10.9%）となっている。特に、500 億円以上の事業体ではリスク分析実施の割合の増加が著しく、それだけ情報システムに対する問題状況への対応のためのリスク分析の意義を重視している結果と思われる。

| リスク分析 / 資本金規模 | 実施している | 実施していない | 実施する予定がある | 無回答 |
|---|---|---|---|---|
| 500 億円以上 | 70.3 | 10.8 | 16.2 | 2.7 |
| 100 億円以上 500 億円未満 | 36.8 | 42.1 | 21.1 | 0.0 |
| 50 億円以上 100 億円未満 | 38.3 | 41.7 | 19.1 | 0.9 |
| 10 億円以上 50 億円未満 | 17.6 | 58.8 | 23.5 | 0.0 |
| 1億円以上 10 億円未満 | 28.9 | 55.4 | 14.9 | 0.8 |
| 5千万円以上1億円未満 | 21.3 | 68.5 | 10.2 | 0.0 |
| 5千万円未満 | 20.6 | 67.6 | 8.8 | 2.9 |
| 資本金なし | 27.6 | 69.0 | 3.4 | 0.0 |

ところで、従業員別にみると、若干興味深い傾向がうかがえる。１万人以上では 31.7%（H13:37.1%）、５千人～１万人未満では 52.4%（H13:40.0%）、３千人～５千人未満 40.4%（H13:30.8%）、１千人～３千人未満36.4%（前回27.2%）、500人から千人未満22.5%（H13:16.8%）、300～500 人未満 20.6%（H13:14.3%）、100～300 人未満 21.6%（H13:6.6%）、100 人未満 16.7%（H13:8.2%）となっており、1 万人以上の規模の事業体を除いて、すべてにおいてリスク分析の実施率が上昇している。この点は、情報機器の浸透度の広がりを反映していると思われるが、「実施していない」割合は相対的に従業員数が少ない事業体ほど高くなっている。

Q14.（Q13 で「1」と回答した場合）情報関連のどのようなリスクを対象としましたか？（複数回答）

| 回答件数 | | 181 | - |
|---|---|---|---|
| 1 | アウトソーシングリスク | 72 | 39.8 |
| 2 | コンピュータ犯罪(故意を含む)のリスク | 99 | 54.7 |
| 3 | 運用障害(操作ミス、入力ミス等) | 133 | 73.5 |
| 4 | 人的災害(テロ、労働争議等) | 68 | 37.6 |
| 5 | 自然災害 | 133 | 73.5 |
| 6 | 事故(火災、爆発、停電、漏水等) | 146 | 80.7 |
| 7 | ハードウェア障害 | 162 | 89.5 |
| 8 | ソフトウェア障害 | 149 | 82.3 |
| 9 | ネットワーク障害 | 147 | 81.2 |
| 10 | 電子メールのリスク(誤送信等) | 68 | 37.6 |
| 11 | コンピュータウイルスのリスク | 145 | 80.1 |
| 12 | 不正アクセスのリスク | 127 | 70.2 |
| 13 | その他 | 3 | 1.7 |
| 無回答 | | 1 | 0.6 |

Q13 でリスク分析を「実施している」と回答した事業体において 80%を超えていたのは、高い順からみると「ハードウェア障害」89.5%、「ソフトウェア障害」82.3%、「ネットワーク障害」81.2%、また従来から基本的な対象とされてきた「事故（火災、爆発、停電、漏水等）」80.7%、最近特に重視されている「コンピュータウイルスのリスク」は 80.1%であった。また、自然災害も無視しがたい対象であり、運用障害（操作ミス、入力ミス等）と並んで 73.5%となっている。「不正アクセスのリスク」も 70.2%と相対的に高い割合を示している。

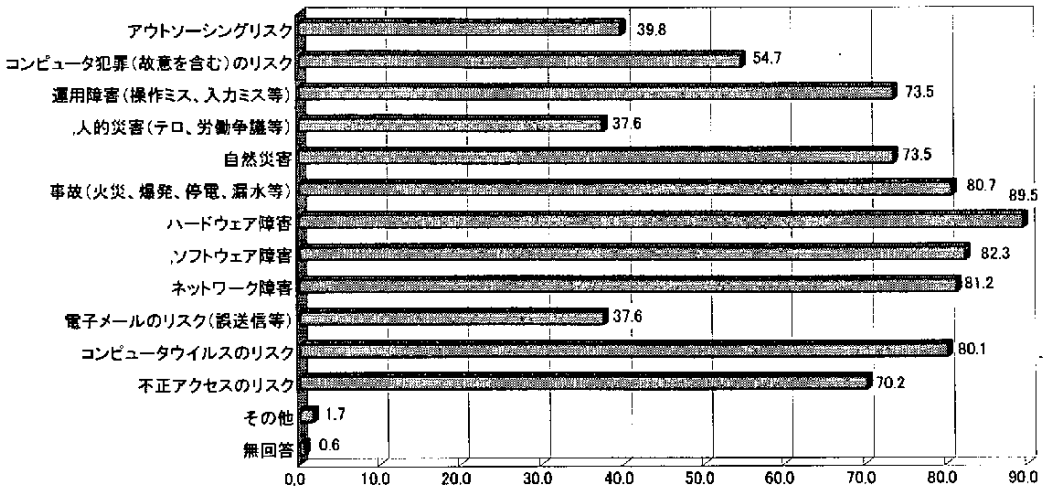



図2－3－5. リスク分析の対象

Q15. リスク分析を実施した際の問題点は何ですか。（複数回答）

| 回答件数 | | 181 | - |
|---|---|---|---|
| 1 | 経営との関係がわからない | 12 | 6.6 |
| 2 | 確立した手法がない | 86 | 47.5 |
| 3 | 分析のためのデータが乏しい | 56 | 30.9 |
| 4 | 専門家がいない | 70 | 38.7 |
| 5 | 組織ができていない | 30 | 16.6 |
| 6 | リスクの定量化が測れない | 111 | 61.3 |
| 7 | その他 | 11 | 6.1 |
| 8 | 問題点は特にない | 10 | 5.5 |
| 無回答 | | 3 | 1.7 |

リスク分析については、これまでもいかなる方法を用いて、どこまでやればよいのかがわからないといった指摘が一般的であった。たとえば、実施する際の問題点として「確立した手法がない」という回答結果は今回 47.5％と前回の 62.2％（H11 調査 58.7％）より減少したが、それでも 50％近い事業体にとっては確立したリスク分析の手法がないという。すでに言及したように、10 年以上前に JIPDEC は「JRAM」を公表しており、まがりなりにも手法はあったといえる。回答における問題は「確立した」という表現の受け止め方にあるのかもしれない。今回の JRMS 解説書により、こうした側面を払拭できれば幸いである。

ところで、今回の質問の選択肢にいれた「リスクの定量化が測れない」は 61.3％という高い回答結果となった。定量化にはどのような尺度を設定すればよいのかといった問題があるため、一般化が困難な面がある。たとえば、脆弱性に関しては、JRMS 解説書における「評価基準」なり、COBIT の「マチュリティモデル」などが参考になるかもしれない。実態を把握するには、JRAM における実態分析の手法が役に立つといえる。

なお、他の回答に関しては「分析のためのデータが乏しい」30.9%（前回38.5%）、「専門家がいない」38.7%（前回49.0%）、「組織ができていない」16.6%（前回26.7%）など、問題点に関わる回答が徐々にではあるが、減少傾向にあり、リスク分析の意味が理解されてきた結果と考えられる。

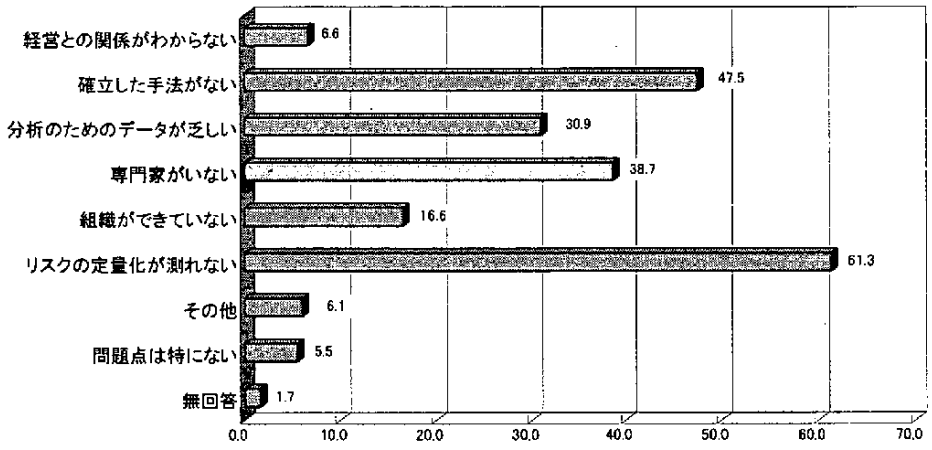



図2－3－6. リスク分析実施上の問題点

Q16.（Q13で「2」と回答した場合）リスク分析を実施しない理由は何ですか。（複数回答）

| 回答件数 | | 328 | - |
|---|---|---|---|
| 1 | 重要性を感じていない | 28 | 8.5 |
| 2 | 手法がわからない | 166 | 50.6 |
| 3 | 予算がない | 125 | 38.1 |
| 4 | 発生被害額が算出できない | 108 | 32.9 |
| 5 | リスク分析の意味がわからない | 14 | 4.3 |
| 6 | 効果がわからない | 104 | 31.7 |
| 7 | 効果があるとは思えない | 16 | 4.9 |
| 無回答 | | 6 | 1.8 |

「リスク分析を実施しない理由」については、「手法がわからない」が相変わらず多く、50.6%（前回47.8%；H11調査 44.7%）と過半数となった。Q15のリスク分析を実施した際の問題点における「確立された手法がない」のは、前回の報告書でも指摘した公的機関、コンサルティング会社等で手法が認知されていないことによるのかもしれない。次いで多いのは「予算がない」(38.1%←H13：26.4%）で、前回調査より10ポイント以上高まっている。同様に「発生被害額が算出できない」という回答も32.9%と前回（24.0%）より高くなっている。また、「効果がわからない」は31.7%と前回調査の 31.2%とほぼ同様である。この点については、実際に分析を行い、継続的にリスクマネジメントシステムを行い経営に生かす、というリスクマネジメントの実践によるといえる。したがって、『JRMS解説書』を通して理解を深め、回答結果にみる回答者のリスク認識のバラツキについてギャップ分析を行い、リスク対応の効果を把握すれば、この問題をかなり解決することができると思われる。

また、「重要性を感じていない」は8.5%（13.3%；H11：19.3%）、「効果があるとは思えない」4.9%（H13：6.1%；H11：6.6%）はいずれも減少傾向にあり、リスク分析に価値を見出す方向が感じられる。

| リスク分析未実施の理由 / 資本金規模 | 重要性を感じていない | 手法がわからない | 予算がない | 発生被害額が算出できない | リスク分析の意味がわからない | 効果がわからない | 効果があるとは思えない | 無回答 |
|---|---|---|---|---|---|---|---|---|
| 500億円以上 | 0.0 | 25.0 | 0.0 | 50.0 | 0.0 | 25.0 | 0.0 | 25.0 |
| 100億円以上500億円未満 | 12.5 | 0.0 | 62.5 | 62.5 | 0.0 | 50.0 | 0.0 | 0.0 |
| 50億円以上100億円未満 | 12.5 | 58.3 | 27.1 | 41.7 | 2.1 | 27.1 | 6.3 | 0.0 |
| 10億円以上50億円未満 | 6.7 | 60.0 | 23.3 | 33.3 | 6.7 | 40.0 | 3.3 | 0.0 |
| 1億円以上10億円未満 | 10.4 | 53.7 | 44.8 | 28.4 | 6.0 | 28.4 | 0.0 | 3.0 |
| 5千万円以上1億円未満 | 8.1 | 52.7 | 29.7 | 31.1 | 4.1 | 36.5 | 10.8 | 1.4 |
| 5千万円未満 | 13.0 | 52.2 | 39.1 | 21.7 | 4.3 | 60.9 | 4.3 | 0.0 |
| 資本金なし | 0.0 | 55.0 | 50.0 | 15.0 | 5.0 | 35.0 | 5.0 | 5.0 |

業種別にみると、リスク分析の実施率の高い金融・保険業ではリスク分析を実施していない理由について、「重要性を感じていない」は0.0%であるが、「手法がわからない」は80.0%と高く、前回の76.2%より高い割合を示し、しかも「リスク分析の意味がわからない」についても他の業種より高い13.3%となっている。情報処理サービス業でもリスク分析の「手法がわからない」が43.8%、さらに「効果がわからない」が37.5%となっており、質問の仕方に問題があったのか、または事業体としてリスクの影響をどう理解してきているのか、再検討の余地がありそうである。

また、リスク分析について「効果がわからない」については食品・紙・パルプ・繊維・印刷業では57.1%と高く（「手法がわからない」では第二位で66.7%、「予算がない」が47.6%）、石油･化学･鉄鋼･非鉄･金属業においても46.9%となっており、あらためて事業体経営におけるリスクマネジメントについての認識を重視する必要があるといえる。

Q17. 貴事業体の基幹システムは、過去1年間にシステムの運用に影響を与えるシステムダウン[注)]が発生しましたか。

| | | | |
|---|---|---|---|
| 1 | 全体的にダウンした | 47 | 7.8 |
| 2 | 部分的にダウンした | 241 | 39.8 |
| 3 | しない　⇒Q21へ | 315 | 52.1 |
| 無回答 | | 2 | 0.3 |
| 計 | | 605 | 100.0 |

システムダウンの発生率は平成９年度 52.7%、11 年度 51.7%、前回調査 54.1%と、これまではあまり大きな変化がみられなかったが、今回調査では 47.6%に減少している。また、「全体的にダウンした」も９年度 13.2%、11 年度 11.4%、前回 9.1%、今回 7.8%と減少してきている。これは、基幹システムの障害対策に力を入れているというよりは、分散システムの増加によって大規模な障害が発生しにくくなっていることを意味していると解釈すべきであろう。

Q18. 過去１年間に発生したシステムダウンの原因の中から該当するものを選んで下さい。(複数回答)

| | | | |
|---|---|---|---|
| 回答件数 | | 288 | - |
| 1 | 自然災害 | 12 | 4.2 |
| 2 | 停電(電力会社に起因する障害) | 28 | 9.7 |
| 3 | 電源機器・設備障害 | 32 | 11.1 |
| 4 | 空調等障害 | 14 | 4.9 |
| 5 | 通信事業者に起因する障害 | 42 | 14.6 |
| 6 | ISP(インターネットサービスプロバイダ)等、社外のインターネットに起因する障害 | 25 | 8.7 |
| 7 | ネットワーク機器などの障害 | 111 | 38.5 |
| 8 | ハードウェア障害 | 153 | 53.1 |
| 9 | OS障害 | 32 | 11.1 |
| 10 | ソフトウェア障害 | 73 | 25.3 |
| 11 | コンピュータウイルス(ウイルスによる不正侵入・ネットワーク障害を含む) | 69 | 24.0 |
| 12 | 火災による事故・障害 | 1 | 0.3 |
| 13 | 人の悪意(たとえば内部犯罪、不正侵入)による事故等 | 0 | 0.0 |
| 14 | オペミス等、人の過失による事故等 | 51 | 17.7 |
| 15 | その他 | 4 | 1.4 |
| 無回答 | | 5 | 1.7 |

システムダウンの原因について、全体の中で「ハードウェア障害」と「ネットワーク機器障害」が突出している。この両者をあわせると前回調査の 98.2%ほど大きくないものの 91.6%と全体の中で突出している。ネットワーク機器を含むハードウェア障害が依然として大きな問題であることがわかる。これは、オフィス内におけるサーバやパソコン、ルータ、ハブなどのネットワーク機器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。

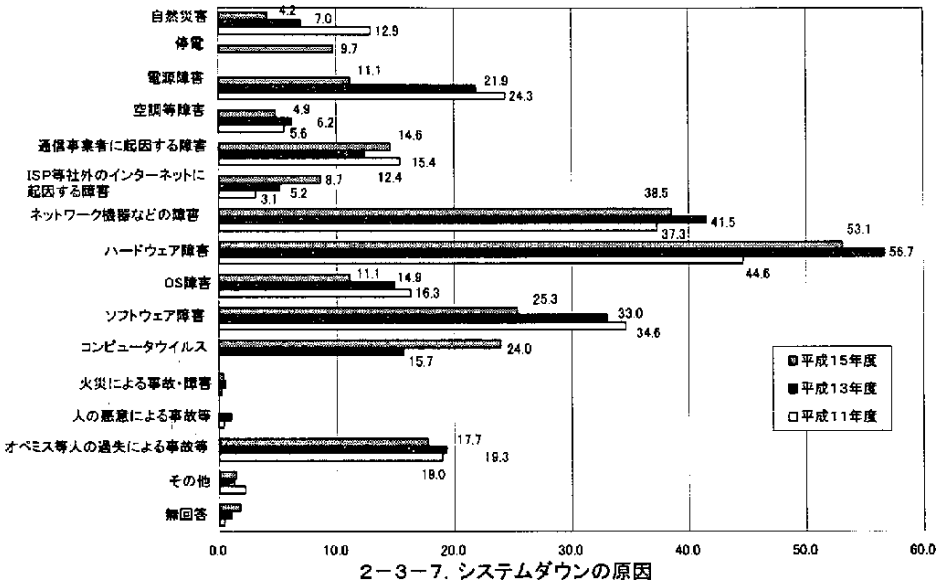
特に増加している障害は、コンピュータウイルスである。前回調査の 15.7%が 24.0%となり、今回調査のトップ４となっている。これは、事業体においてインターネットや電子メールの利用が進むことによって、無視できない脅威となっていることがわかる。ウイルス対策が緊急な課題といえよう。

一方、「OS 障害」や「ソフトウェア障害」の比率が減少してきているが、「OS 障害」が前回に比べ減少したことについては、Windows2000 や XP など OS の動作が比較的安定してきたことが起因していると考えられる。

通信事業者に起因する障害については大きな変化がないものの、「ISP 等社外のインターネットに起因する障害」が、平成 11 年度の 3.1%、前回 5.2%、今回 8.7%と増加してきている。これは、

事業体のインターネット利用が増大しているためと考えられる。今後はISP等についても二重化するなどの対策が必要になると考えられる。

なお、その他の原因として、「自然災害」が平成11年度の12.9%、前回7.0%、今回4.2%と連続して減少している。しかし、自然災害に対する障害を軽視することは難しく、この減少傾向から直ちに対策を緩和できるとはいえない。



2－3－7. システムダウンの原因

Q19. 基幹システムにおけるＭＴＢＦ（平均故障間隔）は何時間ですか。（少数点以下は四捨五入して下さい）

| | |
|---|---|
| 2773.3時間 | （回答件数219件/無回答69件） |

（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

MTBFについては前回調査の2,938.7時間に比べ、若干MTBFは短くなっており、故障の頻度が大きくなっている。この傾向はQ18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、事業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。

分布をみると2,000時間から3,000時間が最も大きくなっている。次のピークは3,000時間から5,000時間であり、おおむね指数分布に従っているといえよう。この結果からは、日本の情報システムは平均的に１年間に２回以下のダウンが発生しているといえよう。ただし、これは、結果であって、システムの要求条件と比較する必要がある。

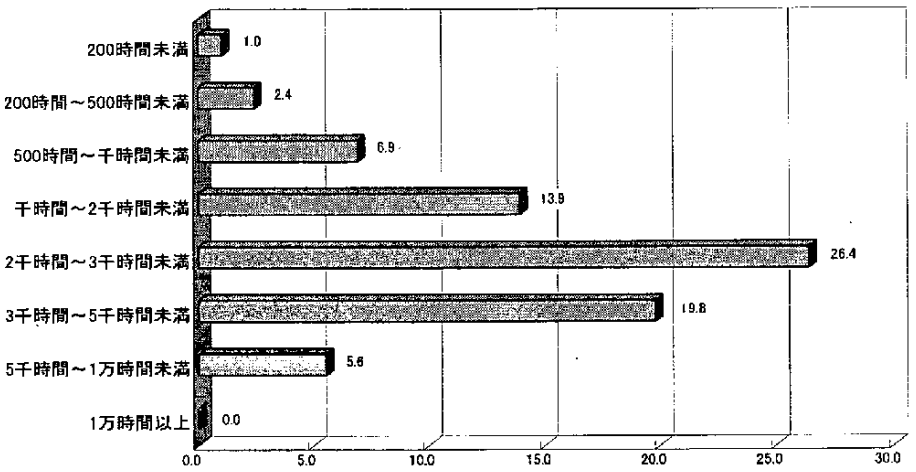



図2－3－8. 基幹システムにおけるMTBF

なお、資本金規模との関係について、資本金の大きい事業体の方がMTBFが長く、資本金の小さい事業体はMTBFが短いことがわかる。資本金の大きい事業体ほど信頼性対策が実施されていることを示している。今後、インターネットの普及により、よりシステムのオンライン化が要求される。これに応えるには、一層の信頼性対策が必要となる。

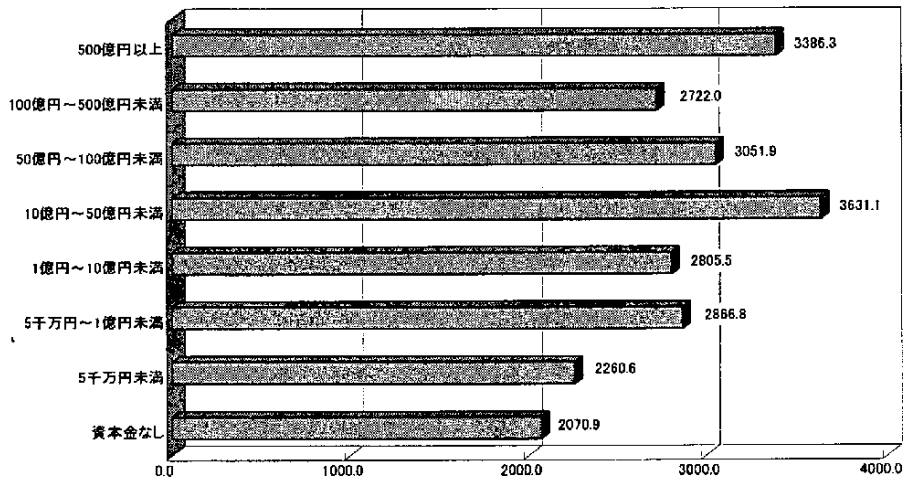



図2－3－9. 基幹システムにおけるMTBF(資本金規模別平均時間)

Q20. 基幹システムにおけるＭＴＴＲ（平均修理時間）は何分ですか。（少数点以下は四捨五入して下さい）

| | |
|---|---|
| 120.0分 | （回答件数206件／無回答82件） |

（参考：平成13年度）

| | |
|---|---|
| 145.7分 | （回答件数388件／無回答90件） |

故障修理に時間を示すMTTR（短いものがよい）は前回調査の145.7分に比べ、さらに短くなっている。この傾向は平成９年度の調査以来、連続して短くなってきている。

MTTRが短くなった原因としては、前回調査でも述べたように、コンピュータのモジュール化の進歩や装置自体のチップ化が進み、修理がより簡単になったものと考えられる。すなわち、修理の

場合、コンポーネットごとに取り替える形態の修理が増えてきたことが原因といえよう。さらにはパソコンやルータなどのネットワーク関係の設備は年々能力が向上していることから、償却の時間間隔がより短くなるとともに、機器への能力（パソコンの処理能力やルータなどの単位時間における処理パケット数）の増加のために機器を耐用年数以下で取り替える傾向にあること、すなわち、バスタブ曲線の修理が必要となるところまで稼働させないことなども原因と考えられる。

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

次に資本金規模との関係について、資本金の大きい事業体ほどMTTRが短く60分程度であり、資本金の小さい事業体ほどMTTRが長くなる傾向がわかる。MTBFと同様、資本金の大きい事業体ほど、信頼性対策が実施されていることを示している。なお、資本金5億以上に限れば、MTTRは100分程度となっている。この100分は、今後、各事業体が信頼性対策を考える上での一つの目安になると思われる。

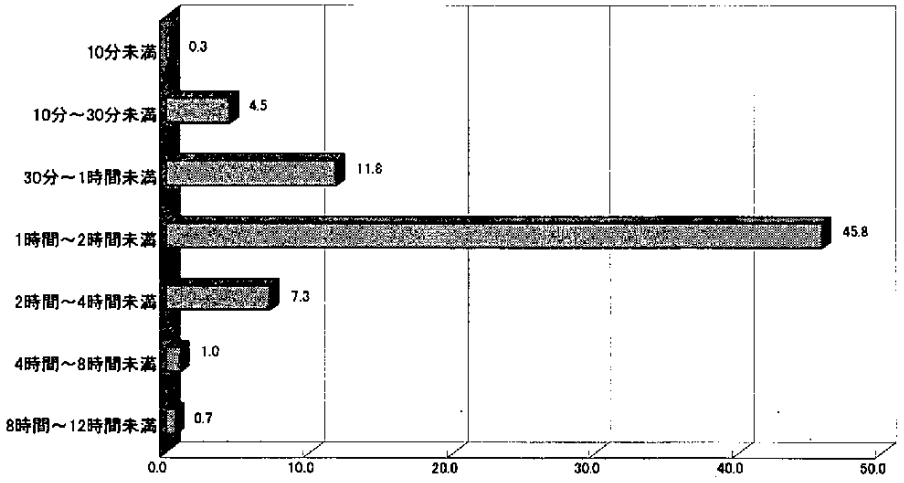



図2－3－10．基幹システムにおけるMTTR(平均修理時間)

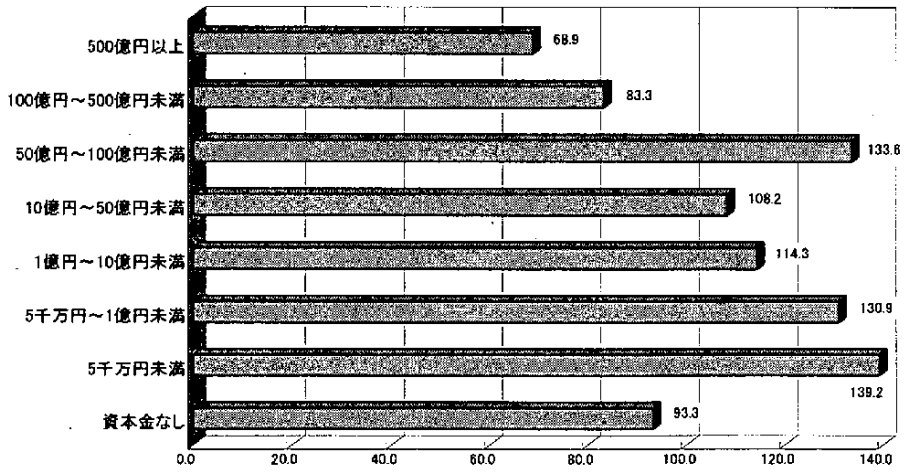



図2－3－11．基幹システムにおけるMTTR(資本金規模別　平均時間)

Q21. 次の各行為をリスクの視点からコンピュータ利用に関わる犯罪と想定し、貴事業体における認識の度合いを示すことができますか。各項目別に犯罪度欄の該当する番号に○をつけて下さい。

| 行為 / 犯罪度 | 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 | 2 | 0.3 | 7 | 1.2 | 12 | 2.0 |
| 問題であると思う | 115 | 19.0 | 165 | 27.3 | 224 | 37.0 |
| 企業内で戒告・訓告・注意処分等の対象となる | 98 | 16.2 | 193 | 31.9 | 188 | 31.1 |
| 企業内で懲戒免職の対象となる | 14 | 2.3 | 54 | 8.9 | 48 | 7.9 |
| 犯罪行為である(刑法上の処罰の対象となる) | 362 | 59.8 | 161 | 26.6 | 100 | 16.5 |
| わからない | 6 | 1.0 | 12 | 2.0 | 20 | 3.3 |
| 無回答 | 5 | 0.8 | 10 | 1.7 | 10 | 1.7 |
| 複数回答 | 3 | 0.5 | 3 | 0.5 | 3 | 0.5 |
| 計 | 605 | 100.0 | 605 | 100.0 | 605 | 100.0 |

『市販のソフトのコピー』に対してはこの２年間で急速に「犯罪行為である」との見方が増えてきている。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%、前回調査では69.9%に急増した。今回調査では59.8%と前回調査に比べ減少したが、「企業内で戒告・訓告・注意処分等の対象となる」と「企業内で懲戒免職の対象となる」が今までの調査で12%程度であったのに対し、今回調査では 18.5%にまで増加している。今までは、企業として犯罪行為であるとして注意はするが黙認する、という姿勢から、厳罰に処する姿勢をとり始めたともいえよう。今までの、ソフトのコピーが犯罪であるとの認識から企業のコンプライアンスが定着し始めた成果ともいえよう。

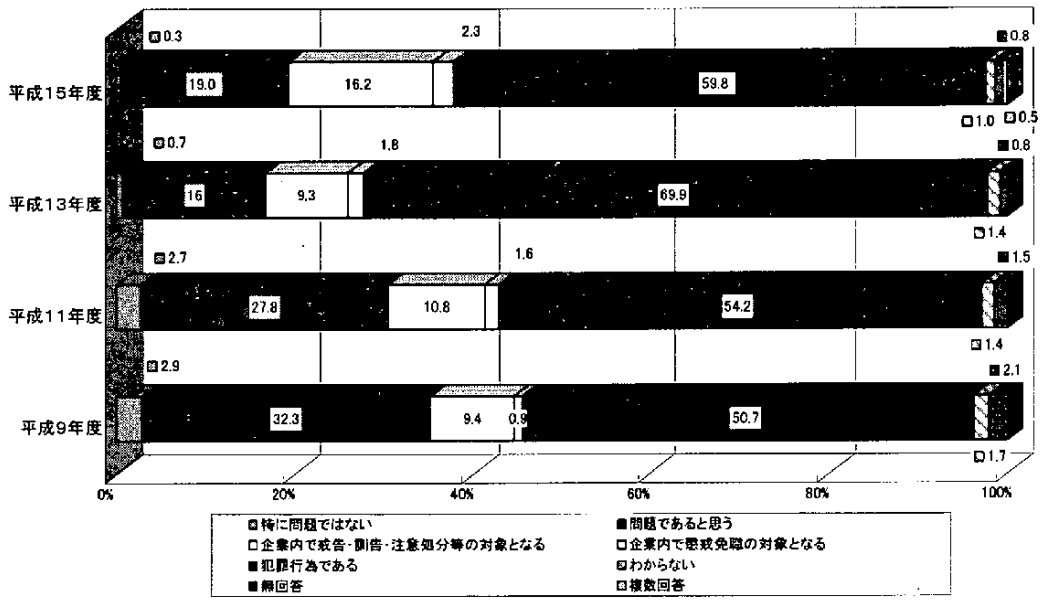



図2－3－12. 市販のソフトをコピーして使用

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

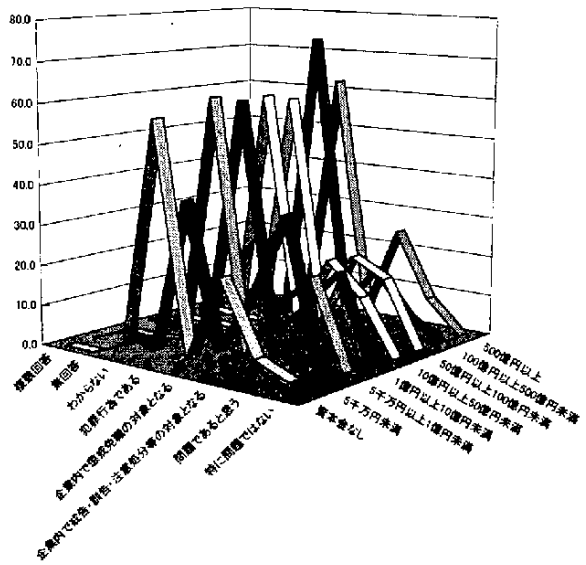



図2－3－13. 市販のソフトをコピーして使う(資本金との関係)

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

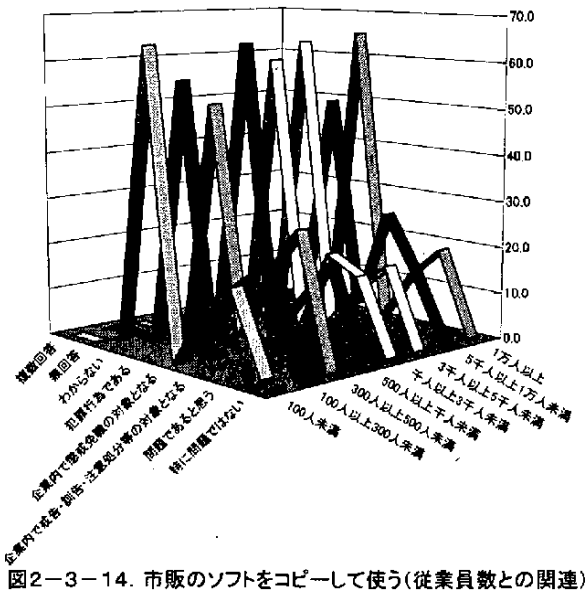



図2－3－14. 市販のソフトをコピーして使う(従業員数との関連)

『データ、プログラムの無断使用』については、『市販ソフトのコピー』に比べるとまだ犯罪との意識は低いが、前回調査と比べても「問題である」との認識を持ち、「企業内でも戒告・訓告・注意処分・懲戒免職の対象」との見方が増加してきている。

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

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

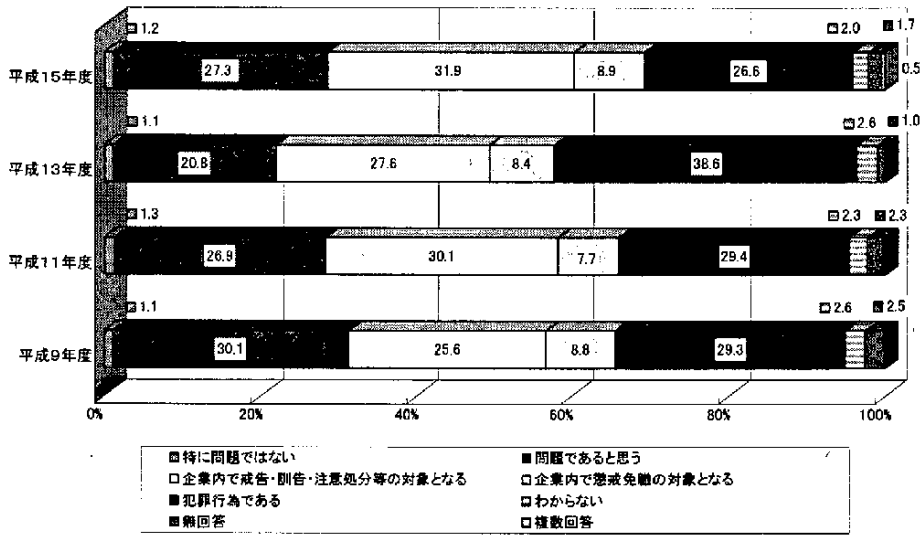



図2－3－15. データ、プログラムの無断使用

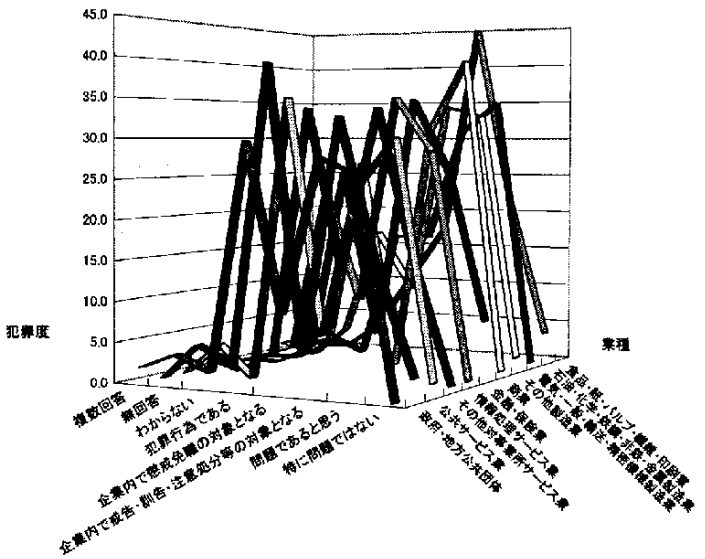



図2－3－16. データ、プログラムの無断使用（業種グループとの関連）

『データ、プログラムを覗き見る』行為について、前回調査と比べて「犯罪行為」との認識から、「問題である」、「企業内で戒告・訓告・注意処分等の対象となる」との認識に移行してきている。前回「犯罪行為である」は25.5％であったが、今回は9ポイント減少して16.5％となっており、市販ソフトのコピーやデータ、プログラムの無断使用に比べると処罰の対象や犯罪行為であるとの認識は依然として低い水準にある。

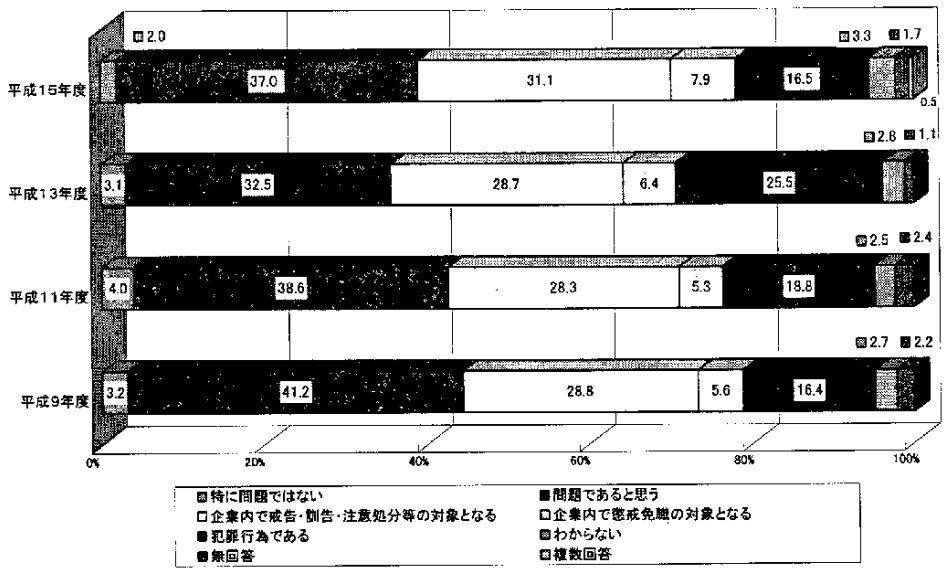



図2－3－17. データ、プログラムを覗き見る

業種グループ別にみると、前回 18.9%が「犯罪行為」と認識していた情報処理サービス業が21.6%へと 2.7 ポイント増加したのに対し、政府・地方公共団体では 42.1%から 22.2%へと約半分に減少した。

事業体規模との関係は、市販ソフトのコピー、データ・プログラムの無断使用と同様に、規模の大小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一層の啓蒙化活動が望まれる。

| 行為 / 犯罪度 | 就業時間内に会社のコンピュータを私用に使う | | WWWを仕事以外(個人目的での発注、アンケート回答等)で利用する | | 私的な目的のための電子メールを送・受信する | |
|---|---|---|---|---|---|---|
| 特に問題ではない | 13 | 2.1 | 19 | 3.1 | 28 | 4.6 |
| 問題であると思う | 270 | 44.6 | 303 | 50.1 | 319 | 52.7 |
| 企業内で戒告・訓告・注意処分等の対象となる | 266 | 44.0 | 240 | 39.7 | 217 | 35.9 |
| 企業内で懲戒免職の対象となる | 31 | 5.1 | 23 | 3.8 | 19 | 3.1 |
| 犯罪行為である(刑法上の処罰の対象となる) | 9 | 1.5 | 7 | 1.2 | 4 | 0.7 |
| わからない | 4 | 0.7 | 2 | 0.3 | 6 | 1.0 |
| 無回答 | 7 | 1.2 | 7 | 1.2 | 8 | 1.3 |
| 複数回答 | 5 | 0.8 | 4 | 0.7 | 4 | 0.7 |
| 計 | 605 | 100.0 | 605 | 100.0 | 605 | 100.0 |

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

『会社のコンピュータを私用に使う』行為に対して、「問題である」との認識は過去の調査結果とほとんど大きな差がみられない。一方、「犯罪である」との認識は 1.8%から 1.5%とほとんど変化がなく、「企業内での戒告・訓告・注意処分等の対象となる」が 39.1%から 44.0%へと増加した。刑罰対象まで厳しくはないが、会社の資産を使用しているという意識が高まってきたものと思われる。今後とも組織内での教育が重要と考えられる。

事業体規模別（資本金、従業員数別）にみると、やはり規模が大きくなるほど会社のコンピュータの私的な利用に関しては厳しい状況にあることがわかる。これは、従業員に対して情報化を率先させているため、また、私的利用で自組織の重要な情報が漏れる可能性もあり、管理が厳重になっているためと考えられる。

業種グループ別にみると、あまり大きな差はみられないが、情報処理サービス業、金融・保険業、政府・地方公共団体での意識改革が進んでいる。情報を活用する業種では私的な利用は組織内では処分されるようになってきているといえよう。

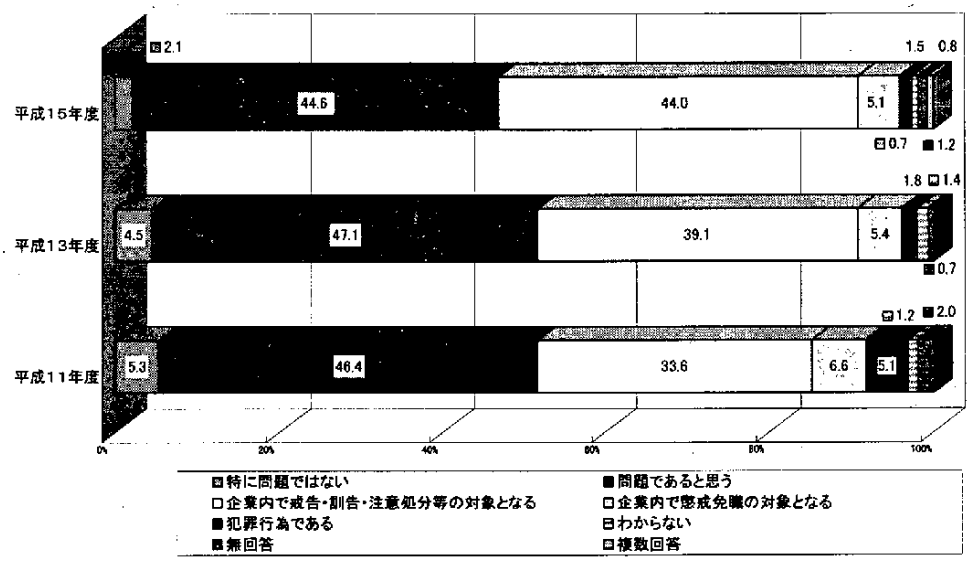



図2－3－18. 就業時間内にコンピュータを私的な目的で使う

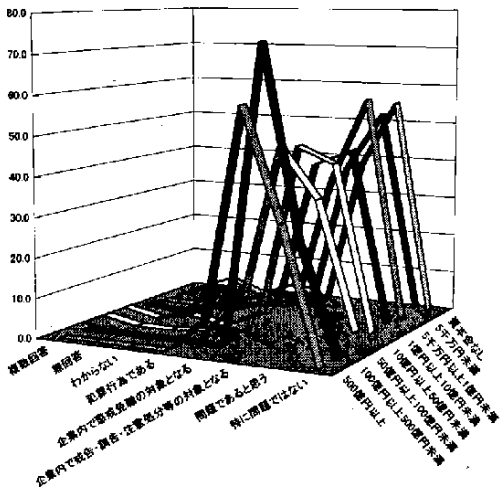



図2－3－19. 就業時間内に会社のコンピュータを私的目的に使う
（資本金との関連）

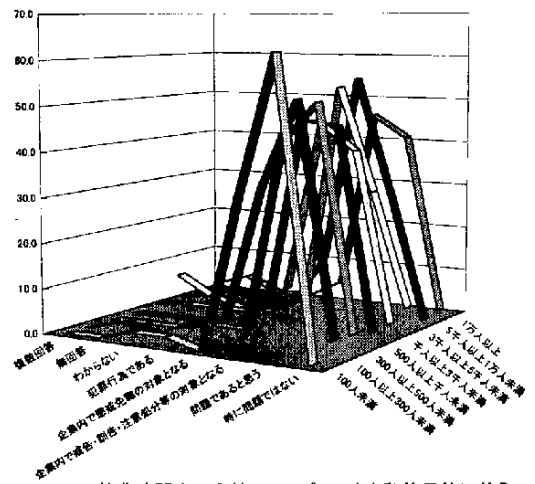



図2－3－20. 就業時間内に会社のコンピュータを私的目的に使う
（従業員数との相関）

『WWWを仕事以外（個人目的での発注、アンケート回答等）で利用する』行為について「特に問題ではない」との認識は6.3%から3.1%に約3ポイント減少し、「問題がある」との認識が46.2%から50.1%へと約4ポイント増加した。徐々にではあるが、問題視されつつあることがわかる。ただ、「企業内での懲戒免職の対象となる」および「犯罪行為である」については前回同様5%を下回る結果となった。

特に、WWWを利用して従業員が勤務時間内にショッピングや株式売買、ピンク系サイトを覗き見

たりすることが増加してきており、多くの事業体が問題視している。これに対しては、ファイアウォールで特にこれらのサイトへのアクセスを制限するフィルタを入れる事業体が増えてきている。

ただ、事業体としてもWWWが組織内のIT上必須となっており、WWWの利用をむやみに制限できず、結局は個人使用について厳格な態度をとりながらもコンピュータリテラシィ教育のためにはある程度の個人利用はやむを得ないと黙認している現状が推察できる。

事業体規模別にみると、事業体規模が大きくなるほど、犯罪度の意識が高まっている。なお、業種グループ別ではそれほどの差は出ていない。

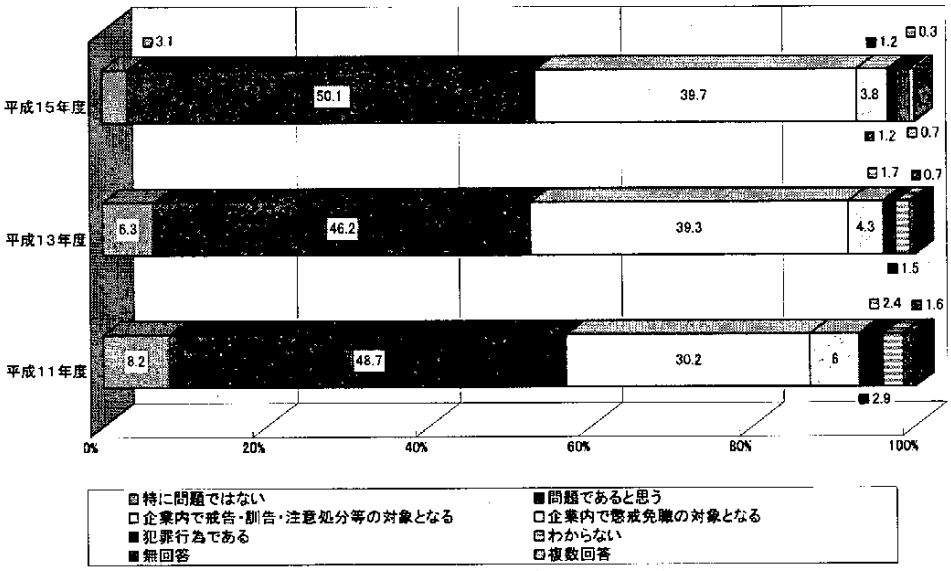



図2－3－21. WWWを仕事以外で利用する

『私用の電子メールを送・受信する』については、前回調査では「問題ではない」と考える事業体が10.6%であったのが4.6%に半減した一方で、「企業内で戒告・訓告」または「懲戒免職」との対象とみなしていることについては、前回の35.5%から39.0%に若干増えており、事業体にとって私的電子メールは禁止の方向に向かっていることがわかる。私的メールは、組織の重要な情報漏洩を引き起こしたり、また、労働生産性を低下させることにもつながることから、多くの事業体が制限するようになると考えられる。

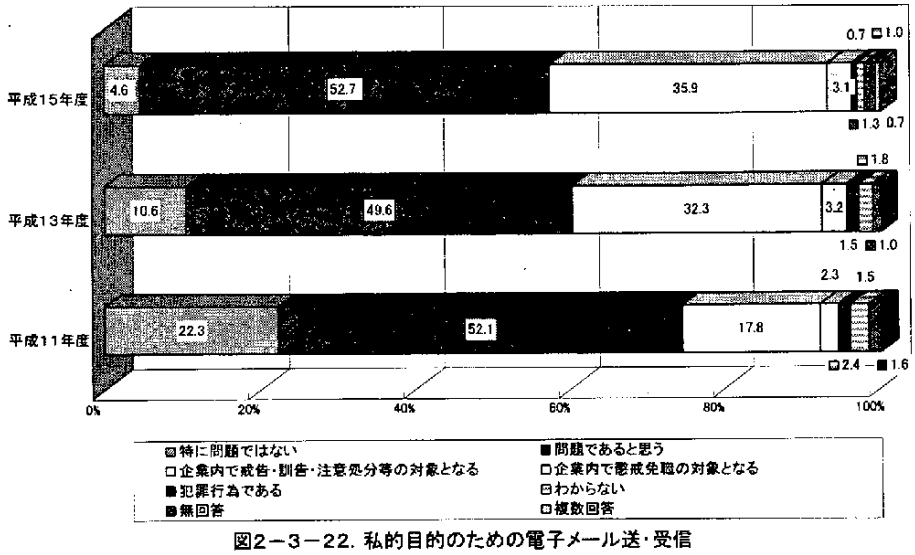



図2－3－22. 私的目的のための電子メール送・受信

図 2-3-22 からわかるように事業体の多くが WWW も電子メールも個人利用を厳しく取り締まり始めたといえよう。すでに、事業体は IT を従業員レベルにまで拡大させており、電子メール、WWW は事業体のホワイトカラーの重要な仕事のツールとなっていることがわかる。これは、ホームページの検索やネットサーフィンが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。

| 行為 / 犯罪度 | 他人のIDを無断借用する | | 業務上入手した顧客情報を正当な理由なしに第三者に売却する | |
|---|---|---|---|---|
| 特に問題ではない | 2 | 0.3 | 0 | 0.0 |
| 問題であると思う | 132 | 21.8 | 15 | 2.5 |
| 企業内で戒告・訓告・注意処分等の対象となる | 248 | 41.0 | 30 | 5.0 |
| 企業内で懲戒免職の対象となる | 65 | 10.7 | 98 | 16.2 |
| 犯罪行為である(刑法上の処罰の対象となる) | 140 | 23.1 | 440 | 72.7 |
| わからない | 8 | 1.3 | 9 | 1.5 |
| 無回答 | 6 | 1.0 | 7 | 1.2 |
| 複数回答 | 4 | 0.7 | 6 | 1.0 |
| 計 | 605 | 100.0 | 605 | 100.0 |

『他人の ID の無断使用』に対しては事業体としては問題であるが、「企業内で戒告・訓告・注意処分等の対象となる」との認識が前回調査の 34.3%から 41.0%に増加した。一方、「犯罪行為である」との認識については、前回の 34.3%から 23.1%に約 10 ポイント減少したが、無断使用行為を問題視していることには違いない。

しかし、市販ソフトの不正コピーに対する認識と比べると犯罪という認識は少ないように思われる。これは企業ではグループで仕事をしていることが多く、緊急な場合に他人の ID で仕事を行うなどの実態があり、問題があると認識しながらも犯罪という認識が低いものと考えられる。今後は企業も成果主義に変わりつつあり、従業員同士がライバルとなることもあり、この問題は避けて通れなくなるだろう。

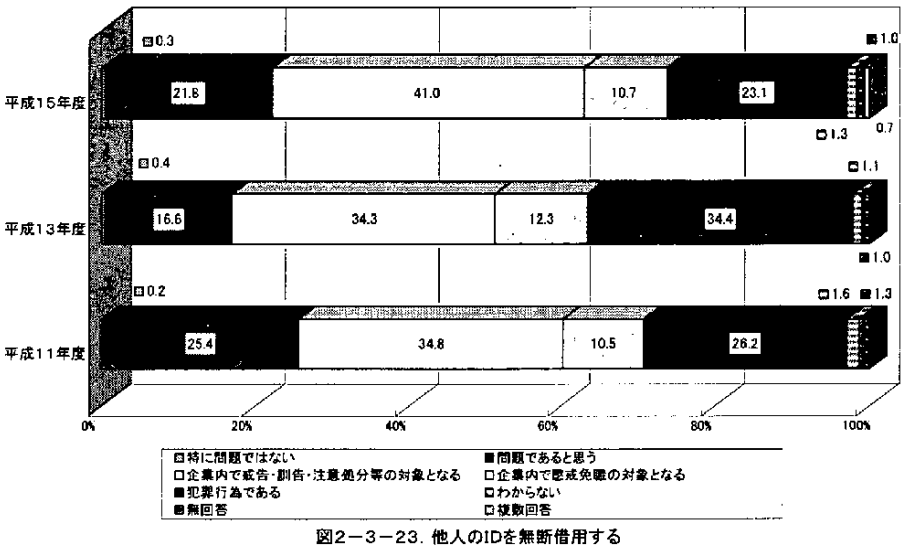


図2－3－23. 他人のIDを無断借用する

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

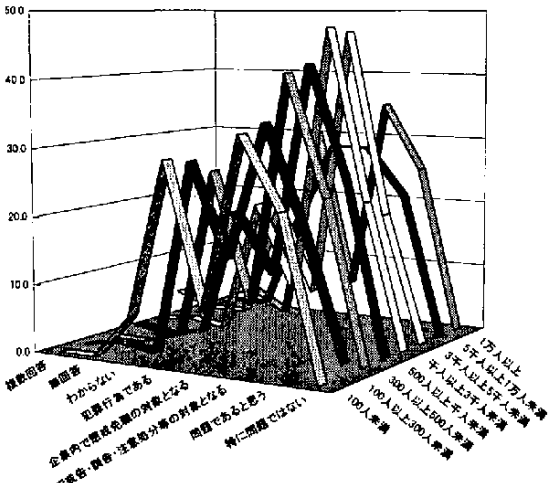



図2－3－24. 他人のIDを無断借用する
（従業員数との相関－15年度）

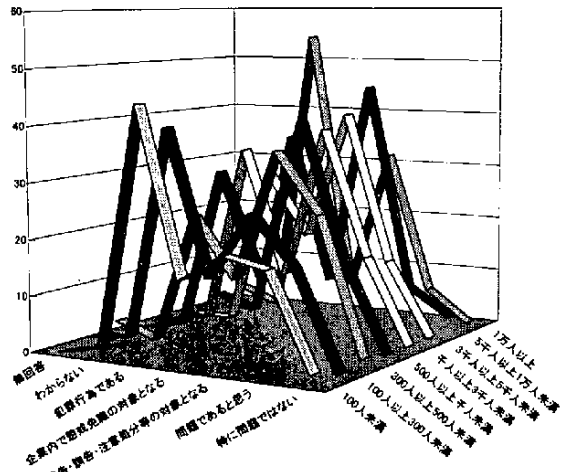



図2－3－25. 他人のIDを無断借用する
（従業員数との相関－平成13年度）

ここ数年、『業務上入手した顧客情報を理由なしに第三者に売却する行為』や漏洩事件が多発している。また、平成15年に個人情報保護法が制定されたことから、これらの問題に対する認識度合いは高い。特に、前回調査では「犯罪行為である」が79.5%であったが、今回もこの傾向は同様であり、企業内の処分を含めると90%以上が厳格な対応をとる、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情報を保護することが国際的なコンセンサスとなっており、事業体は今後、顧客情報のより徹底した管理が重要となる。プライバシーマークの利用を含め、積極的に取り組むことが必要である。

業種グループ別との関係では、「犯罪行為」とみなす割合は、情報処理サービス業（79.7%←H13:83.8%）、金融・保険業（78.4%←H13:84.1%）、公共サービス業（78.3%←H13:86.3%）、政府・地方公共団体（74.1%←H13:94.7%）は他の業種と比べると高く、厳しいものとなっている。

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

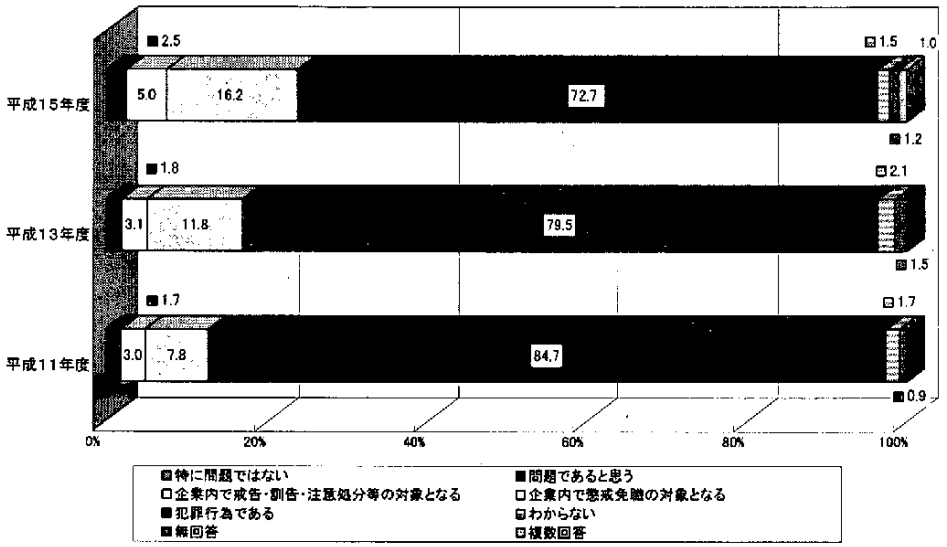



図2－3－26. 顧客情報を第三者に売却する

最後に、Q21 の各質問項目のうち、さまざまなコンピュータ利用での犯罪の認識度合いについて、「犯罪行為である」、「企業内で懲戒免職の対象となる」、「企業内で戒告・訓告・注意処分等の対象となる」の順に比較した。

この結果では、『業務上入手した顧客情報を正当な理由なしに第三者に売却する』行為が最も「犯罪」としての認識度合いが高く、72.7%である。次いで、『他人の ID を無断借用する』が 20%を越えており、いずれも「犯罪」、「懲戒免職の対象」との認識が高い。一方、『WWW を個人目的で使用する』、『私用の電子メールを送・受信する』、『就業時間内でコンピュータを私用に使う』については「問題である」、「企業内で戒告・訓告・注意処分等の対象」程度の認識はありつつも、犯罪との認識は低い。業務上において「会社のコンピュータを使っている」というモラルの向上が望まれる。経営者層側も今後情報化を進めていくなかで、従業員に対するこれらの点での教育によるモラル向上を図っていく必要があると考えられる。

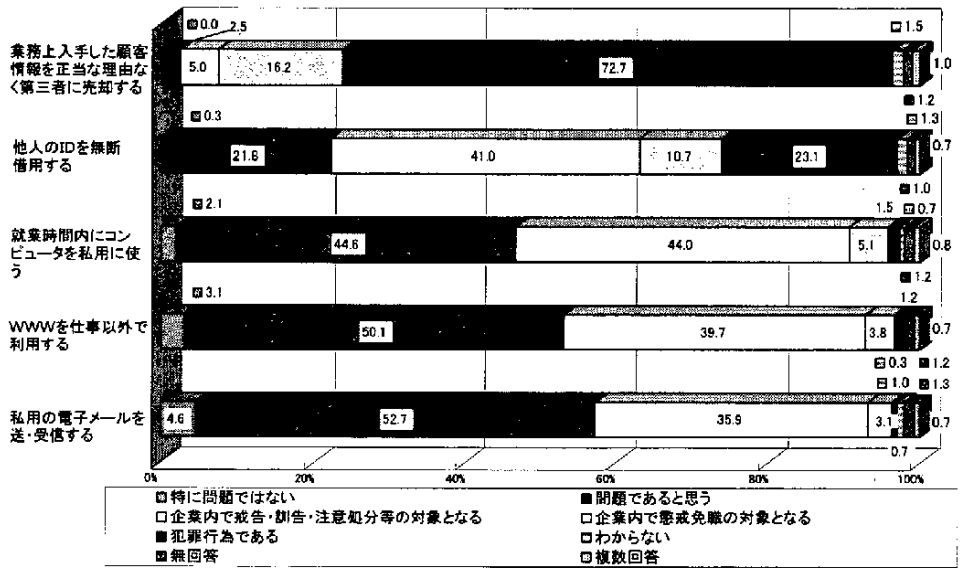



図2－3－27. さまざまなコンピュータ利用での犯罪認識度

## 2.4 情報セキュリティポリシー・管理・対策について

Q22. 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 | | 605 | － |
|---|---|---|---|
| 1 | 経営者層の理解 | 431 | 71.2 |
| 2 | 管理者の理解 | 240 | 39.7 |
| 3 | 担当者の理解 | 187 | 30.9 |
| 4 | 社内全体の理解(エンドユーザを含む) | 517 | 85.5 |
| 5 | 法規制の整備 | 87 | 14.4 |
| 6 | その他 | 2 | 0.3 |
| 無回答 | | 5 | 0.8 |

情報セキュリティの確保にとり、「社内全体の理解（エンドユーザを含む）」が85.5%（前回77.9%）と最も高いポイントとなっている。情報セキュリティの確保には全社員の共通認識と協力が必要であるとの認識であり、これはごくあたり前のことであるが、実際には、思うようにはいっていないことの結果であろう。

次に高いポイントは「経営者層の理解」71.2%（前回53.3%）であるが、やはり、経営者を巻き込んだ全社的な活動に持っていかないと効果が現れないことを表していると同時に、情報セキュリティに関する投資の意思決定者として経営者の役割が大きいと考えられている結果である。

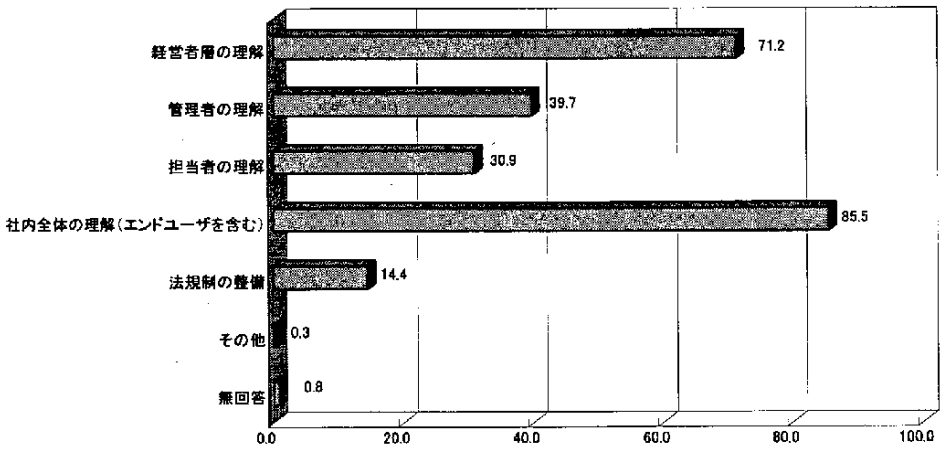



図2－4－1. 情報セキュリティ確保のための基本的重要な視点

産業別の「社内全体の理解」の回答率は政府・地方公共団体が高いポイントとなっている。

| | |
|---|---|
| 第二次産業 | 85.7% |
| 第三次産業 | 83.5% |
| 政府・地方公共団体 | 94.4% |

資本金規模と回答率との関係は以下のとおりである。

| 資本金 | 社内全体の理解 | 経営者層の理解 |
|---|---|---|
| 500 億円以上 | 91.9% | 89.2% |
| 100 億円以上 500 億円未満 | 94.7% | 63.2% |
| 50 億円以上 100 億円未満 | 87.8% | 71.3% |
| 10 億円以上 50 億円未満 | 78.4% | 64.7% |
| 1億円以上 10 億円未満 | 88.4% | 76.9% |
| 5千万円以上1億円未満 | 80.6% | 75.0% |
| 5千万円未満 | 64.7% | 58.8% |
| 資本金なし | 89.9% | 75.9% |

資本金規模に関わらず「社内全体の理解」が高いポイントとなっており、次いで「経営者層の理解」が続いている。

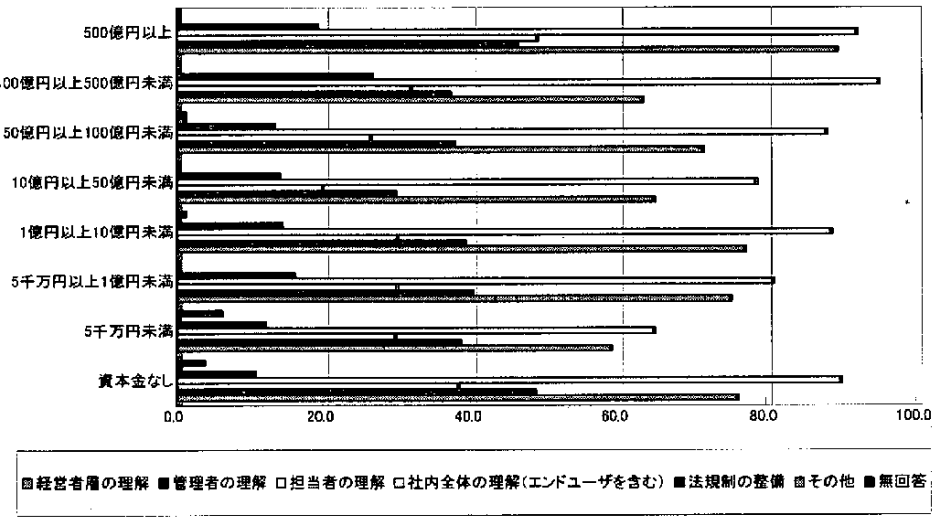



図2－4－2. 情報セキュリティ確保のための基本的重要な視点(資本金別)

また、従業員規模と回答率の関係は以下のとおりである。

| 従業員数 | 社内全体の理解 | 経営者層の理解 | 管理者の理解 |
|---|---|---|---|
| 1万人以上 | 91.7% | 66.7% | |
| 5千人以上1万人未満 | 90.5% | | 57.1% |
| 3千人以上5千人未満 | 87.2% | 74.5% | |
| 千人以上3千人未満 | 86.0% | 74.1% | |
| 500 人以上千人未満 | 90.1% | 74.8% | |
| 300 人以上500 人未満 | 77.9% | 67.6% | |
| 100 人以上300 人未満 | 80.2% | 73.3% | |
| 100 人未満 | 83.3% | 56.3% | |

従業員数規模別に比較しても「社内全体の理解」が最も高く、ほとんどの規模で「経営者層の理解」が続いているが、従業員数５千人以上１万人未満の事業体のみ「管理者の理解」が２番目に高いポイントとなっている。

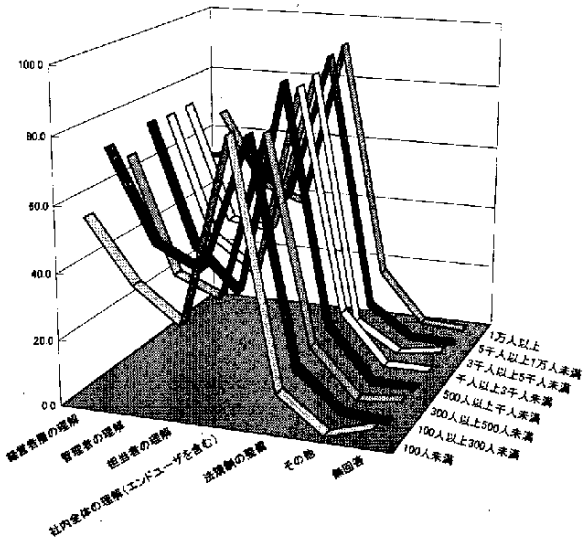



図2－4－3. 情報セキュリティ確保のための基本的重要な視点（従業員規模別）

Q23. 貴事業体では、情報セキュリティ対策（不正アクセス対策、ウイルス対策、信頼性対策、個人情報保護対策等）に情報システム関連支出の何パーセントを使っていますか。（小数点第1位まで）

| | | |
|---|---|---|
| 6.1 | % | （回答件数: 387件） |

情報システム関連支出に対する情報セキュリティ対策費の割合は 6.1%と前回調査の 4.1%を上回っており、情報セキュリティ対策にかける費用が年々多くなる傾向を表しているものと思われる。

| 業種 | 平均 |
|---|---|
| 第二次産業 | 5.4% |
| 第三次産業 | 6.8% |
| 政府・地方公共団体 | 6.1% |

第三次産業が最も高く、政府・地方公共団体がこれに続いている。情報システムの位置づけが不特定多数の人々との関わりを多くしている結果であろう。

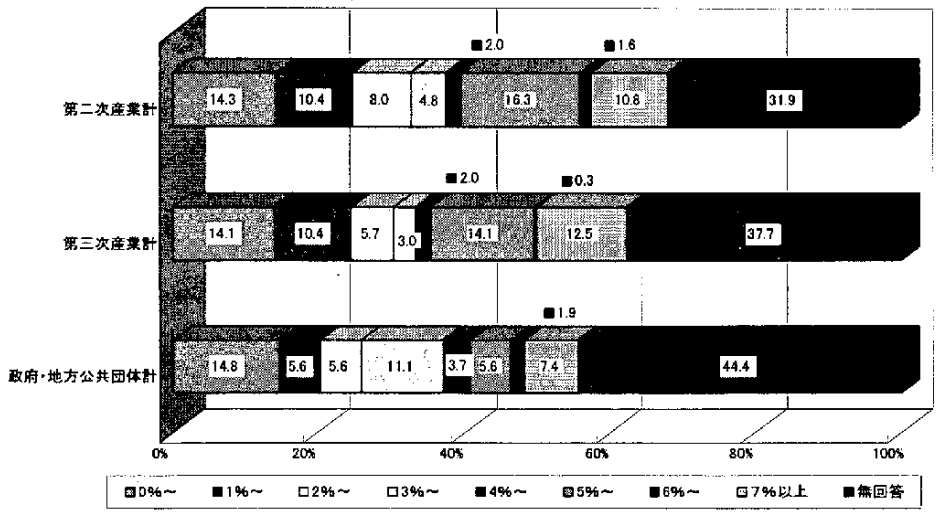



図2－4－4. 情報セキュリティ対策への情報システム関連支出の割合

以下の質問は、情報セキュリティポリシーについての質問である。ここでは、平成12年7月に内閣　情報セキュリティ対策推進会議が定義した情報セキュリティの3階層をベースにした構造（図2-4-5）を想定している。

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

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

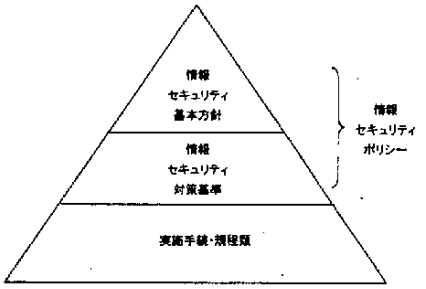



**図２－４－５．情報セキュリティポリシー構造**

Q24. 貴事業体では経営理念に基づく情報セキュリティポリシー、実施手続・規程類を定めていますか。

| 策定状況 | | 情報セキュリティポリシー | | 実施手続・規程類 | |
|---|---|---|---|---|---|
| 1 | 定めている | 279 | 46.1 | 211 | 34.9 |
| 2 | 現在作成中である | 78 | 12.9 | 125 | 20.7 |
| 3 | 作成を検討している | 98 | 16.2 | 111 | 18.3 |
| 4 | 定めていない | 143 | 23.6 | 146 | 24.1 |
| 5 | 必要ない | 4 | 0.7 | 4 | 0.7 |
| 無回答 | | 3 | 0.5 | 8 | 1.3 |
| 計 | | 605 | 100.0 | 605 | 100.0 |

情報セキュリティポリシーについては、平成12年7月に内閣官房の情報セキュリティ対策推進会議が主導で政府関係の組織体に向けて『情報セキュリティポリシーに関するガイドライン』を定めた。これが大きなトリガーとなって多くの事業体で情報セキュリティポリシーが定められたり、作成されつつある。特に、今回調査では、情報セキュリティポリシーを「定めている」のは46.1%と、前回調査（24.0%）から約22ポイント増加している。また、「定めていない」が23.6%と、前回（32.9%）より9ポイントも減少した。この結果、情報セキュリティポリシーを「定めている」、「現在作成中」を合わせると59.0%となり、初めて過半数を超えた。さらに「作成を検討中」を加えると75.2%となり、事業体においては、すでに情報セキュリティポリシーが必須のものとなっているといえよう。これは、平成14年のISO17799の国内標準化（JIS X 5080）、ISMS制度の拡充、情報セキュリティ監査基準の策定によるところが大きいと考えられる。

以上の結果から情報セキュリティポリシーがこの5年間に着実に浸透していることがわかる。また、平成9年や11年に情報セキュリティポリシーを作成した事業体にとっては、見直しの時期となっており、今後の事業体における情報セキュリティポリシーの定着を考える時期にきているともいえよう。

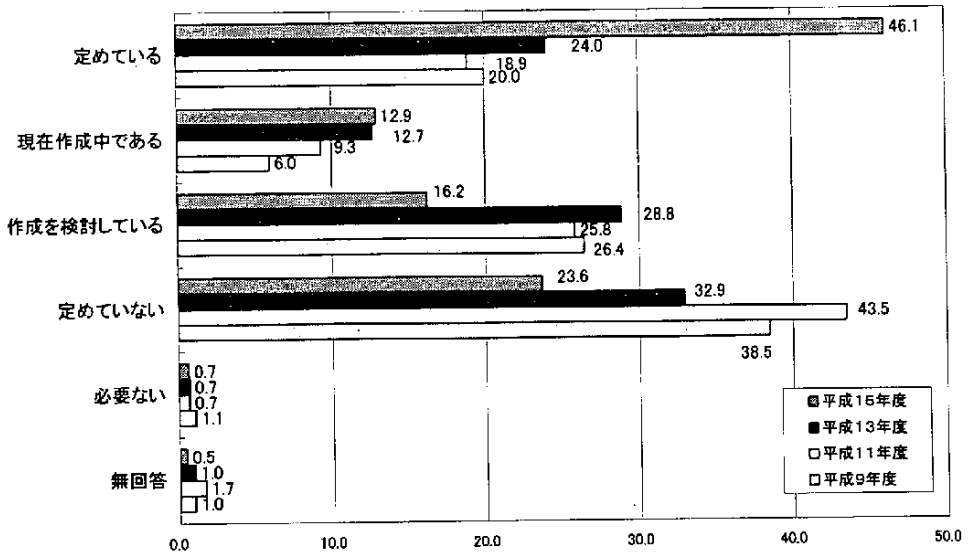



図2－4－6. 情報セキュリティポリシーの策定状況

情報セキュリティの実施手続・規程類を「定めている」のは34.9%で、前回調査で「定めている」とした回答の22.1%に比べ、10ポイント以上の増加となっている。また「定めていない」は24.1%で、前回調査（32.5%）よりも8.4ポイント減少した。一方、「現在作成中である」（20.7%）は前回調査（14.5%）に比べ増加している。

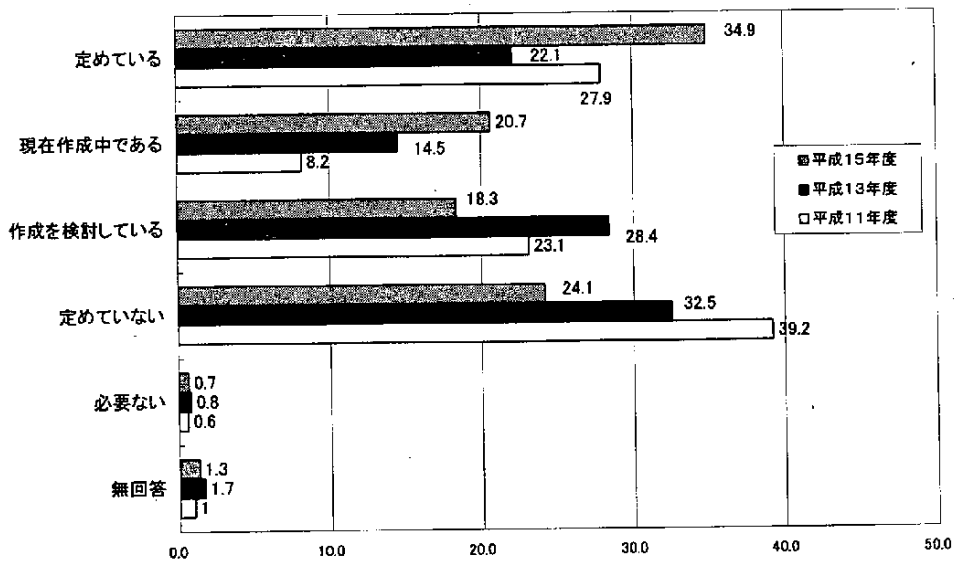



図2－4－7. 実施手続･規程類の策定状況

なお、情報セキュリティポリシーの作成状況と実施手続・規程類の作成状況の傾向は大変よく似ている。これは、図2-4-5の情報セキュリティポリシー構造に示す両者の関係が、情報セキュリティポリシーを作成してからこれをベースにして実施手続・規程類を作成するようになっているためであり、平成12年に内閣が策定した「情報セキュリティポリシーに関するガイドライン」が強く意識されているためと考えられる。日本でも、情報セキュリティに対する認知度が高まってきているといえよう。

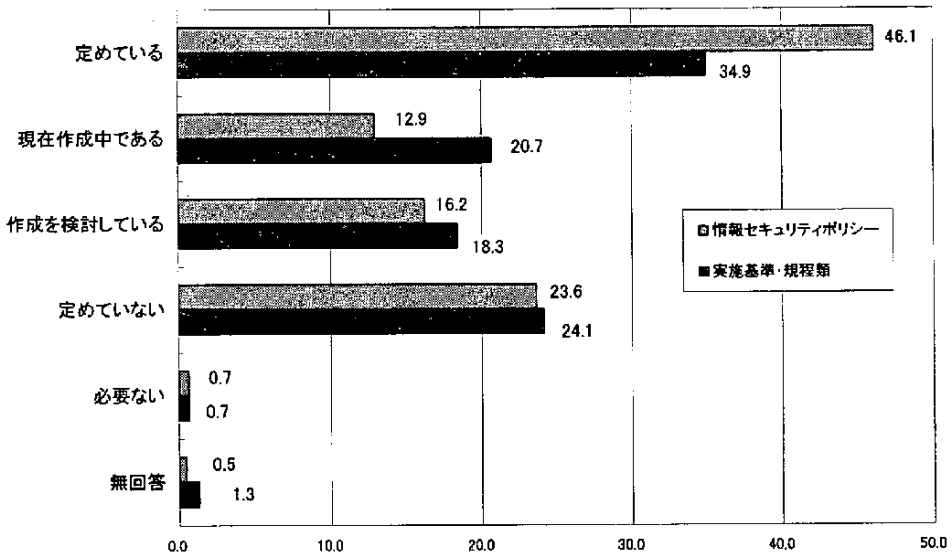



図2－4－8. セキュリティポリシーと実施手続・規程類との関係

Q25. （Q24 で「ポリシー／規程類を定めている」と回答した場合）情報セキュリティポリシー、実施手続・規程類は定期的に見直していますか。

| 策定項目 | いる | | いない | | 無回答 | | 計 | |
|---|---|---|---|---|---|---|---|---|
| 情報セキュリティポリシー | 184 | 65.9 | 62 | 22.2 | 33 | 11.8 | 279 | 100.0 |
| 実施手続・規程類 | 175 | 82.9 | 32 | 15.2 | 4 | 1.9 | 211 | 100.0 |

現代の情報環境はコンピュータウイルスやインターネットのサイトへの不正侵入が相継いでおり、悪化している。また、個人情報保護法の成立や住民基本台帳制度の施行など、情報処理に関する法的な制度が進展しており、情報処理そのものに対する情報セキュリティの意味合いが大きく変わってきている。そのため、情報セキュリティポリシーや実施手続・規程類の定期的な見直しが不可欠となっている。

前回調査では情報セキュリティポリシーを「定期的に見直している」と回答したのは 66.9%、実施手続・規程類の見直しにあたっては 79.9%の事業体が行っていた。今回の調査では「セキュリティポリシー」が 65.9%、「実施手続・規程類」が 82.9%となっており、依然として多くの事業体が見直しを行っている。これは、ISO/IEC17799（JIS X 5080）の制定などが一因と考えられる。今後もそれぞれの事業体が定期的に見直し、情報環境の激変に対応できるような制度的な支援も必要と考える。

特に「JIS X 5080」では定期的に情報セキュリティポリシーを見直すことが示されており、今後、ISMS 認証や情報セキュリティ監査制度が進展する中で、見直しが広がることが期待される。

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

（JIS X 5080:2002 の 3.1.2 から抜粋）

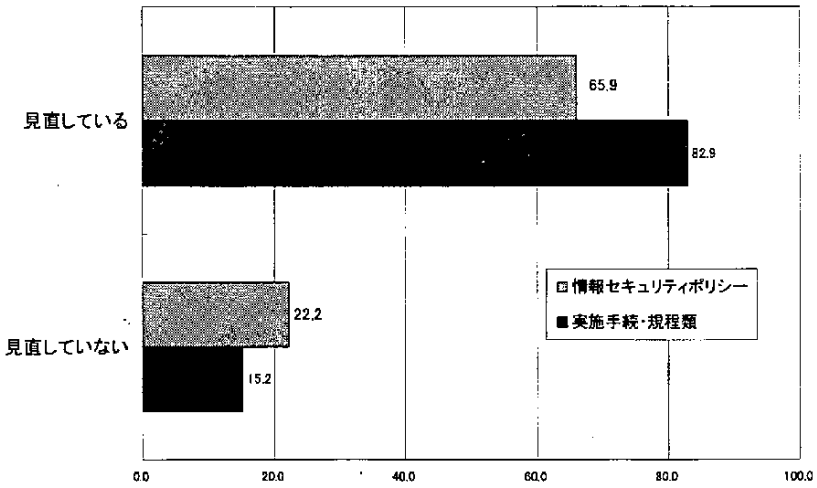



図2－4－9. 情報セキュリティポリシー／実施手続・規程類の見直しについて

ここで重要なのは、情報セキュリティの環境が技術の進歩や社会へのインターネットの広がりに合わせて大きく変化することに情報セキュリティ基本方針が対応していかなければならないことである。そのためには、情報セキュリティポリシーを定期的に見直し、その環境に対応して重要な情報資産を保護する必要がある。この観点から、情報セキュリティポリシーに対する監査も重要な要素である。これについて「JIS X 5080」では下記のように監査や第三者によるレビューを示唆している。

> 4.1.7　情報セキュリティの他者によるレビュー　情報セキュリティ基本方針文書(3.1 参照)には，情報セキュリティの基本方針及び責任を記述する。組織の行動が基本方針を適切に反映し，基本方針が実行可能及び有効であることを保証するために，情報セキュリティ基本方針の実施を他者がレビューすることが望ましい(12.2 参照)。
>
> このようなレビューは，内部監査部門，他部門の管理者又はそのようなレビューを専門とする第三者組織が実施してもよい。ただし，その場合，レビューを実施する者は，適切な技能及び経験をもつものとする。

(JIS X 5080:2002 の 3.1.2 から抜粋)

Q26.（Q24 で「情報セキュリティポリシーを定めている／作成中」と回答した場合）情報セキュリティポリシーは次のどれを参照して作成していますか。(複数回答)

| | | | |
|---|---|---|---|
| 回答件数 | | 357 | - |
| 1 | JIS X 5080、情報セキュリティポリシーに関するガイドライン(官邸) | 166 | 46.5 |
| 2 | 日本銀行や金融情報システムセンター(FISC)のポリシー | 65 | 18.2 |
| 3 | COBITなどのデファクト標準 | 19 | 5.3 |
| 4 | 自社で独自に開発 | 140 | 39.2 |
| 無回答 | | 43 | 12.0 |

今回の調査では情報セキュリティポリシーを作成している事業体が増えたことから、何をベースにポリシーを作成したかを調査した。結果としては、「BS7799」や「ISO/IEC17799」の比率が前回調査の 50.2%から 46.5%に低下した。一方、日本銀行や金融情報システムセンター（FISC）のポリシーの比率が７ポイント近く増加している。

COBITなど、デファクト基準の採用の比率は、前回調査（1.9%）と比較すると3.4ポイント増加している。一方、自主的に開発した事業体も前回の36.5%から39.2%へと若干増加している。これは、「JIS X 5080」が広まったものの、事業体は個々にビジネスモデルが違っており、自社への適用にあたっては、自分の業種にあったものを選んでいると考えられる。今後、標準に従う部分とカスタマイズする部分をどのように選択するか、また、自社の部分をどのように維持・管理するかが重要になるといえよう。

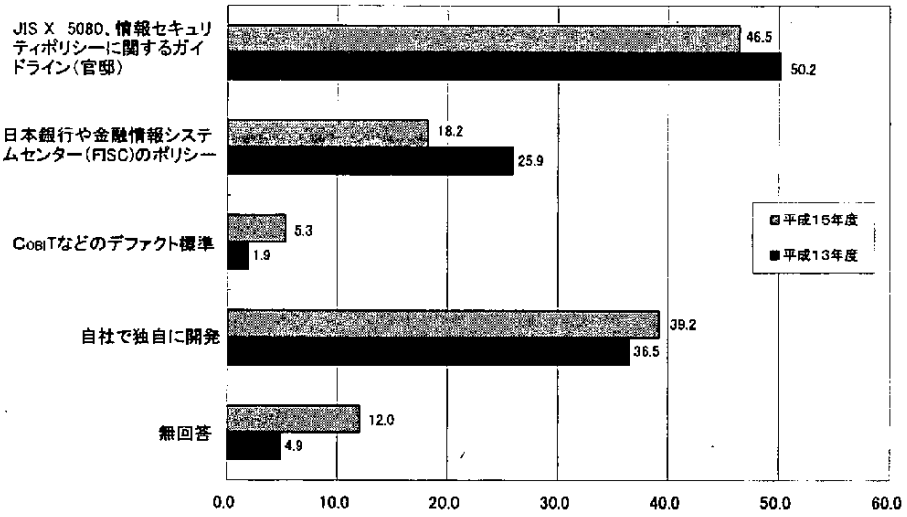



図2－4－10. 情報セキュリティポリシー策定時の参照項目

Q27. 以下の管理について、責任を有する担当者を定めていますか。

| 管理項目 | 定めている | | 設置を検討している | | 定めていない | | 必要ない | | 無回答 | | 計 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ネットワークの管理 | 504 | 83.3 | 37 | 6.1 | 59 | 9.8 | 0 | 0.0 | 5 | 0.8 | 605 | 100.0 |
| 情報システムの管理 | 487 | 80.5 | 45 | 7.4 | 67 | 11.1 | 0 | 0.0 | 6 | 1.0 | 605 | 100.0 |
| 情報セキュリティの管理 | 396 | 65.5 | 88 | 14.5 | 116 | 19.2 | 0 | 0.0 | 5 | 0.8 | 605 | 100.0 |

基幹システムのネットワーク、情報システムの管理、情報セキュリティの管理に対する責任を有する担当者の設置状況について調査を行った。前回調査では、管理者と責任者について質問したが、今回は区別していない。

ネットワーク管理者を「定めている」が83.3%で、前回調査の79.2%、11年の76.4%に比べて増加している。これに「検討している」（6.1%←H13:8.9%、約3ポイント減）をあわせると、89.4%の事業体がネットワーク管理者を重視していることがわかる。なお、「定めていない」は9.8%、「必要ない」は0.0%となっており、両者をあわせても10.0%以下となった。やはり、ほとんどの事業体で基幹システムがネットワーク環境下で用いられているとともに、インターネットを利用したり、電子メールを利用していることから、ネットワーク管理の必要性を重視していると考えられる。

一方、情報システムの管理者については、「定めている」、「検討中である」ともにネットワーク管理者とほぼ同様の趨勢となった。これは、情報システムの管理とネットワークの管理がともに情報システムにとって同意語となりつつあることを示していると考えられる。「定めている」と「検討中である」をあわせると87.9%となり、平成11年度以来、数ポイントではあるが減少傾向に

ある。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、いまだ11%を超えて増加傾向にある。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（アウトソーシング）していて組織内部に情報システムの責任者をおく必要がないと判断しているためと考えられる。

情報セキュリティ管理者または責任者の有無については、「定めている」、「検討している」の肯定的な回答をしたのは80.0%と、前回調査の75.6%、11年の36.3%から増加傾向にある。一方、「定めていない」および「必要ない」という否定的な回答は19.2%と前回調査の22.9%から減少した。ただし、この調査項目は11年度と前回調査において大きく情勢が変わったが、今回は前回のような劇的な変動はなかった。このことから、今まで以上にネットワークやコンピュータを利用する事業体が増え、不正侵入やウイルスなどの被害を受ける頻度が高くなったため、どの事業体にとっても情報セキュリティの管理が重要な要素となっていることが考えられる。

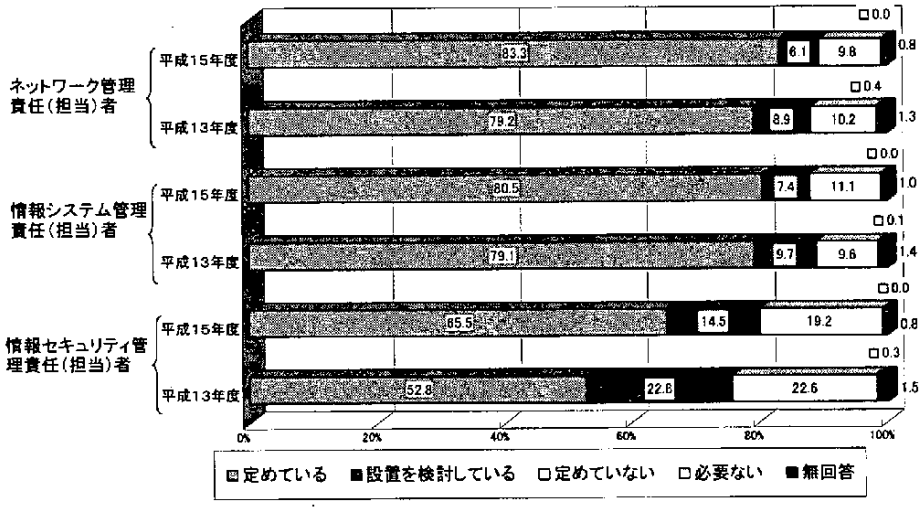



図2－4－11. 管理責任者の設置について

Q28. 情報セキュリティ（システム災害/障害、不正アクセス、ウイルスを含む）管理についての問題点は何ですか。（複数回答）

| 回答件数 | | 605 | － |
|---|---|---|---|
| 1 | 経営者層の理解が得られない | 92 | 15.2 |
| 2 | コストがかかりすぎる | 324 | 53.6 |
| 3 | 専門要員がいない | 260 | 43.0 |
| 4 | 組織の従業員に対する負担がかかりすぎる | 158 | 26.1 |
| 5 | 組織の従業員に対する教育・訓練がいきとどかない | 330 | 54.5 |
| 6 | ノウハウが不足している | 208 | 34.4 |
| 7 | どこまでやればよいのか基準が示されていない | 231 | 38.2 |
| 8 | 要求に合致するもの(サービス／製品)がない | 25 | 4.1 |
| 9 | 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 | 117 | 19.3 |
| 10 | 情報セキュリティ管理が事業の国際化に見合っていない | 3 | 0.5 |
| 11 | その他 | 8 | 1.3 |
| 12 | 特に問題はない | 20 | 3.3 |
| 無回答 | | 6 | 1.0 |

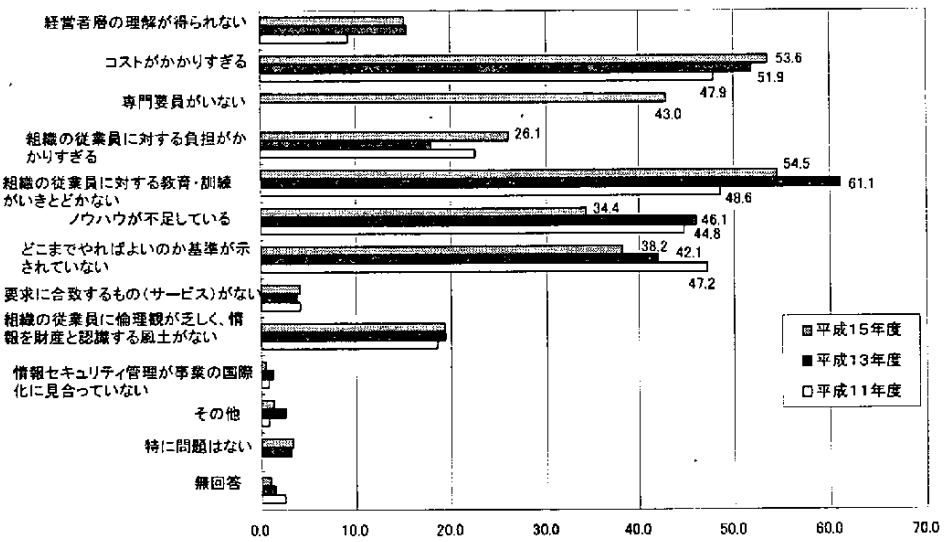



図2－4－12. 情報セキュリティ管理の問題点

情報セキュリティ管理についての問題点は第１位が「組織の従業員に対する教育・訓練がいきとどかない」（54.5%）であった。第２位が「コストがかかりすぎる」（53.6%）、第３位が「専門要員がいない」（43.0%）であった。「専門要員がいない」の選択肢は今年度新設した項目であったが、上位２つは平成 11 年度、前回調査同様、傾向は変わっていない。情報セキュリティの最新の考えでは、情報セキュリティは従業員が守るものであり、そのためには従業員の教育が重要であるという認識であるが、この結果がそれを裏付けているものといえる。また専門要員については、従業員の教育のほか、ウイルス対策やアクセス管理など情報セキュリティを強化維持するためのさまざまな日常業務をシステムの保守作業の一環として実施しなければならず、突発的なウイルス対策などを講じる負担が大きく、専門の知識を持ちロードを本来業務として割り当てることができる専門要員の確保を切望しているのではないかということで新たに選択肢を設けたが、結果として第３位の回答数を得ており、保守要員の負担のある状況が現れている。

各々の回答の傾向をみると、２つの回答で特徴が現れている。一つは第２位にあげられた「コストがかかりすぎる」であり、平成 11 年度が 47.9%、前回調査 51.9%、今回が 53.6%と上昇傾向にある。これはウイルス対策や不正アクセス対策などの発生頻度が高くなってきており、もはやウイルス対策ソフトなどは常備しなければならないことが一般化するなど、コストをかけなければならない状況を示している。また 11 年と現在を比較すると、11 年ではサーバ／クライアント方式の端末展開は展開途上であったが、現在はほぼすべての事務部門の標準となってきており、それに比例するようにウイルスや不正アクセス対応などの情報セキュリティ関係の費用も増加していることの反映と考えられる。

もう一つは「どこまでやればよいのか基準が示されていない」で、これは 11 年度 47.2%、前回調査 42.1%、今回 38.2%と下降傾向にある。これもクライアント、サーバ方式による端末展開が一段落し、またウイルス対策ソフトなどが標準化されたこと、また JIS X 5080 が ISMS 制度として普及するなどにより、どの程度のことを実施すればよいかが共通認識となってきたことの現れと考えられる。

なお、「経営者層の理解が得られない」は前回とほぼ同様の15.2%である。情報セキュリティを実施する現場としては、一定程度のセキュリティ対策を行うことはすでに予算化されるなど経営者の了解を得ており、それよりも回答者が直面しているのは教育の負担や予算の問題という日常的な対象に焦点があたっているといえる。

Q29. 以下の情報セキュリティ要素（1－10）のうち、貴事業体にとって重要と思われる要素を3つ選び、下の回答欄に優先順位をつけて記入して下さい。

| 回答件数　605件 | | 優先順位別集計(注) | | | | | | 複数回答としての集計 | |
|---|---|---|---|---|---|---|---|---|---|
| 情報セキュリティ要素 | | 1位 | | 2位 | | 3位 | | | |
| 1 | 情報セキュリティポリシー(経営者の積極的な関与) | 199 | 32.9 | 37 | 6.1 | 48 | 7.9 | 287 | 47.4 |
| 2 | 情報セキュリティ組織(情報セキュリティの推進組織の構築と活動) | 63 | 10.4 | 102 | 16.9 | 50 | 8.3 | 215 | 35.5 |
| 3 | 情報資産の分類および管理(情報資産のリスク評価とそれによる重要度の分類) | 43 | 7.1 | 73 | 12.1 | 77 | 12.7 | 193 | 31.9 |
| 4 | 人的セキュリティ(役職員への教育訓練や内部規則の策定など) | 93 | 15.4 | 106 | 17.5 | 111 | 18.3 | 311 | 51.4 |
| 5 | 物理的および環境的セキュリティ(入退室管理や安全区画の構築など) | 13 | 2.1 | 28 | 4.6 | 31 | 5.1 | 73 | 12.1 |
| 6 | 通信および運用管理(ネットワークの管理、ウイルス対策、ログ管理など) | 67 | 11.1 | 97 | 16.0 | 89 | 14.7 | 255 | 42.1 |
| 7 | アクセス制御(IDとパスワード管理、不正アクセス対策など) | 22 | 3.6 | 65 | 10.7 | 81 | 13.4 | 171 | 28.3 |
| 8 | システム開発およびメンテナンス(開発環境のセキュリティ、ライブラリ管理運用など) | 6 | 1.0 | 14 | 2.3 | 23 | 3.8 | 46 | 7.6 |
| 9 | 事業継続管理(災害対策、障害対策など) | 58 | 9.6 | 49 | 8.1 | 53 | 8.8 | 161 | 26.6 |
| 10 | 準拠(法律遵守、システム監査など) | 21 | 3.5 | 12 | 2.0 | 20 | 3.3 | 54 | 8.9 |
| 無回答 | | 20 | 3.3 | 21 | 3.5 | 22 | 3.6 | 15 | 2.5 |
| 複数回答 | | | | 1 | 0.2 | | | | |

(注)優先順位をつけていない回答(5件)は集計対象外として、無回答に含んでいる。ただし、複数回答集計には含んでいる。

情報セキュリティを実現するために必要な要素をJIS X 5080の大項目に合わせて10分類し、それについて優先順位を第3位までつけてもらった。前回は優先順位をつけずに回答した割合も相当多く、分析に手間がかかったが、今回はほとんどが優先順位をつけた回答となった。これは回答方法に慣れたことも考えられるが、一方で、ISMSや情報セキュリティの浸透やリスクマネジメントの手法などがリスクの大きさに応じて対策をつけることや優先順位をつけて対応することを求めていることから、優先順位をつけることに抵抗が少なくなってきたとも考えられる。

（1）第1位の分析

第1位にあげた項目をみると「情報セキュリティポリシー（経営者の積極的な関与）」が605件中199件、32.9%とトップの選択であり、しかも2位の「人的セキュリティ（役職員への教育訓練や内部規則の策定など）」93件（15.4%）を大きく引き離している。これは前回調査でも同様で「情報セキュリティポリシー」（36.3%）が1位であった。情報セキュリティの推進には要員の配備、予算の確保など経営資源を必要とするため、当然ながら経営者の理解や関心の高さおよび責任体制の強化が必要であり、それを裏付けるものである。また昔のホストコンピュータ時

代と異なり、クライアントサーバが多くなっている今日では、情報システム部門だけでは情報セキュリティを構築するには限界があり、第一線の一般ユーザの理解と協力がないと情報セキュリティは構築維持ができない。このため情報システム部門を越えて全社的な推進運動を行うためにはやはり経営者の関与が不可欠である。

第３位以下は「通信および運用管理（ネットワークの管理、ウイルス対策、ログ管理など）」67 件（11.1%）、４位「情報セキュリティ組織（情報セキュリティの推進組織の構築と活動）」63 件（10.4%）である。前回調査では２位が「通信および運用管理」（12.3%）、３位「情報セキュリティ組織」（12.1%）、４位「人的セキュリティ」（11.8%）であった。２位から４位までは僅差ではあるが、「通信および運用管理」が少しウエイトが下がり、そのかわり従業員教育や規則の作成などの従業員に関係する実務的な要素に重きが置かれるようになっている。この解釈はいろいろあると考えられるが、ウイルス対策などは対応ソフトなどの標準手法が出揃ったことにより不安感が減少しているが、より企業ごとの風土体質をあらわす従業員教育の重要性がますます高まってきていることの現れと思われ、対策が全社的なレベルのより実践的なものを求めているのではないかと推測される。

５位以下は、５位「事業継続管理（災害対策、障害対策）」58 件（9.6%）、６位「情報資産の分類および管理（情報資産のリスク評価とそれによる重要度の分類）」43 件（7.1%）、７位「アクセス制御（ID とパスワード管理、不正アクセス対策など）」22 件（3.6%）、８位「準拠（法令遵守、システム監査など）」21 件（3.5%）、９位「物理的および環境的セキュリティ（入退室管理や安全区画の構築など）」13 件（2.1%）、10 位「システム開発およびメンテナンス（開発環境のセキュリティ、ライブラリ運用管理など）」６件（1.0%）となっている。

前回調査の順番を参考までに掲げると、５位「事業継続管理」（8.6%）、６位「情報資産の分類および管理」（7.1%）、７位「アクセス制御」（5.8%）、８位「システム開発およびメンテナンス」（2.3%）、９位「物理的および環境的セキュリティ」（2.0%）、10 位「準拠」（1.8%）であった。

５位以下を比較すると前回調査に比べて「事業継続管理」、「情報資産の分類および管理」、「アクセス制御」の３つはともに５位、６位、７位で順位に変化がなかった。今回調査の特徴としては前回 10 位の「準拠」が８位に若干順位を上げたことである。物理的環境的セキュリティや開発環境などと比較して法律遵守、監査などが重要と位置づけられた結果である。

（２）上位３位までの分析

第２位の選択状況を分析してみると、第２位は第１位の比較では２位であった「人的セキュリティ」が 106 件（17.5%）で１位になっている。続いて「情報セキュリティ組織」102 件（16.9%）、と組織や従業員教育など情報セキュリティの推進に欠かせない人的な対応要素が上位にあげられている。３位以下は「通信および運用管理」97 件（16.0%）、「情報資産の分類および管理」73 件（12.1%）、「アクセス制御」65 件（10.7%）となり、情報セキュリティポリシーを除きほぼ上位の要素が並んでいる。またアクセス制御が５位に上昇してきており、ハッカー対策をはじめパスワード管理などの実務が重要視されていることがわかる。

第３位の選択状況では、１位「人的セキュリティ」111 件（18.3%）、２位「通信および運用管理」89 件（14.7%）、３位「アクセス制御」81 件（13.4%）、４位「情報資産の分類および管

理」77件（12.7%）、5位「事業継続管理」53件（8.8%）となっており、徐々にウイルス対策や不正アクセス対策、バックアップ対策など実務的な項目に重みを増していることがわかる。

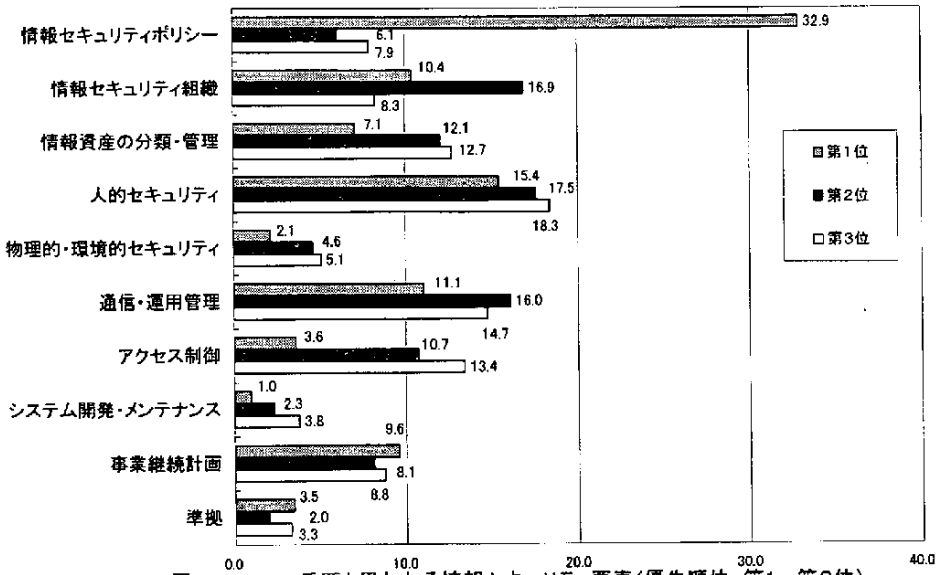


図2－4－13. 重要と思われる情報セキュリティ要素（優先順位 第1～第3位）

（3）上位3位までを総合した評価

上位3位までを合計した結果を順位でみると次のようになる。1位は「人的セキュリティ」311件（51.4%）であり、役職員への教育や内部規制の策定など、まさに情報セキュリティの根幹が人の知識と意識にあることをそのまま裏付けるものといえる。2位は「情報セキュリティポリシー」287件（47.4%）で、総数では「人的セキュリティ」に譲るものの、第1位では他の項目に大きな差をつけて重要視されており、経営者の関与が重要であることが示されている。3位は「通信および運用管理」255件（42.1%）であり、ウイルス対策などに手間を取られている実態が現れている。4位以下は次のとおりである。4位「情報セキュリティ組織」215件（35.5%）、5位「情報資産の分類および管理」193件（31.9%）、6位「アクセス制御」171件（28.3%）、7位「事業継続管理」161件（26.6%）、8位「物理的および環境的セキュリティ」73件（12.1%）、9位「準拠」54件（8.9%）、10位「システム開発およびメンテナンス」46件（7.6%）である。得票数字の分布からみると4つのグループに分けられ、A群「人的セキュリティ」（51.4%）、「情報セキュリティポリシー」（48.4%）、B群「通信および運用管理」（42.1%）、「情報セキュリティ組織」（35.5%）、C群「情報資産の分類および管理」（31.9%）、「アクセス制御」（28.3%）、「事業継続管理」（26.6%）、D群「物理的および環境的セキュリティ」（12.1%）、「準拠」（8.9%）、「システム開発およびメンテナンス」（7.6%）となる。

前回調査での順番は、A群1位「通信および運用管理」（51.4%）、2位「情報セキュリティポリシー」（49.6%）、B群3位「人的セキュリティ」（41.3%）、4位「情報セキュリティ組織」（38.7%）、5位「アクセス制御」（34.7%）、C群6位「情報資産の分類および管理」（28.2%）、7位「事業継続管理」（24.5%）、D群8位「物理的および環境的セキュリティ」（12.3%）、9位「システム開発およびメンテナンス」（10.5%）、10位「準拠」（7.0%）である。

前回調査と今回を比較すると、全体の大きな傾向は変わっていないが、順位が上昇したのはB群からA群に昇格し、しかも第1位となった「人的セキュリティ」である。一方、A群からB群

に下降したものが「通信および運用管理」である。前回に比べてウイルス対策などの通信および運用管理が標準手法などが浸透しロードはあるものの、ある程度落ち着いて評価されたのに対し、かわって従業員教育や規定の作成がトップとなったのは、すべての従業員が定められた対応行動を実施しなければ情報セキュリティが構築できないという現状を現しているものと思われる。同様にB群の「アクセス制御」がC群に下降しており、これも不正アクセス対策も以前に比較して標準手法が確立されつつあり、切迫度が減少していることと関連していると推察される。最後に同じD群の「準拠（法律遵守、監査）」が最下位から一つ順番を上げたが、法律の遵守および監査はマネジメントシステムでは重要であり、またコンプライアンスは経営の基礎であるものの、その評価が決して高くないことが何に起因するのか、考える必要がある。

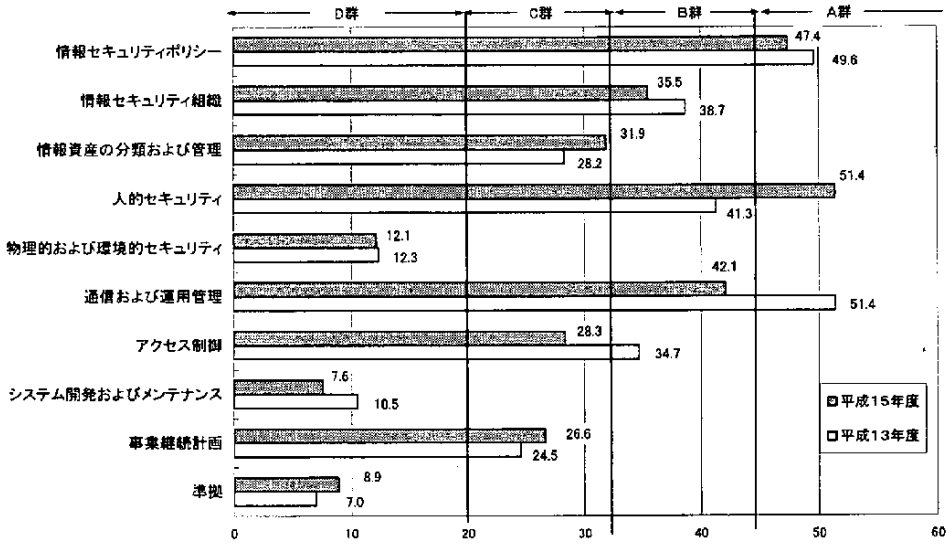



図2－4－14. 重要と思われるセキュリティ要素（優先順位付けなし）

（4）業種別の特徴

ここでは25件以上の回答がある8つの業種について特徴をみることとする。8業種とは、建設業、化学工業、電気機械器具製造業、卸業・商社、金融業、運輸・通信・倉庫業、情報処理サービス業、地方公共団体である。

セキュリティ要素それぞれのカテゴリの割合を順位づけると、建設業では「アクセス制御」が10.8%とその他の業種に比較して高い割合を占めている。化学工業は「情報資産の分類および管理」が15.4%で第1位である。電気機械器具製造業は「通信および運用管理」が25.9%と飛びぬけて高い値を示している。卸業・商社では「事業継続管理」が19.4%で第1位である。この「事業継続管理」については金融業および運輸・通信・倉庫業の回答が18.5%となっており、卸業・商社を合わせたこの3業種は情報システムの停止による影響が大きいことが予想されるが、そのとおりの評価となっている。情報処理サービス業では「人的セキュリティ」が17.6%と高く、また「物理的および環境的セキュリティ」は選択肢がもともと少ないが重要視している。

地方公共団体は一般の企業とは異なる大きな特徴がある。「情報セキュリティポリシー」が19.6%と他の事業体が30%程度あるいはそれ以上の選択をしているのに対し、地方公共団体ではわずか19.6%でしかない。一方で「人的セキュリティ」が45.1%と他の業種に比べ圧倒的な高さをほこり、地方自治体のガバナンス構造が一般企業とは大きく異なることを表していると考えられる。

回答25件以上の業種　第1位

| 情報セキュリティ要素 / 業種 | 情報セキュリティポリシー | 情報セキュリティ組織 | 情報資産の分類・管理 | 人的セキュリティ | 物理的・環境的セキュリティ | 通信・運用管理 | アクセス制御 | システム開発・メンテナンス | 事業継続計画 | 準拠 |
|---|---|---|---|---|---|---|---|---|---|---|
| 建設業 | 29.7 | 16.2 | 10.8 | 5.4 | 0.0 | 10.8 | 10.8 | 0.0 | 8.1 | 2.7 |
| 化学工業 | 34.6 | 11.5 | 15.4 | 15.4 | 0.0 | 7.7 | 3.8 | 0.0 | 0.0 | 7.7 |
| 電気機械器具製造業 | 37.0 | 3.7 | 3.7 | 11.1 | 0.0 | 25.9 | 3.7 | 3.7 | 3.7 | 7.4 |
| その他の製造業 | 34.3 | 14.3 | 14.3 | 11.4 | 0.0 | 14.3 | 0.0 | 0.0 | 8.6 | 0.0 |
| 卸業・商社 | 32.3 | 12.9 | 9.7 | 6.5 | 3.2 | 12.9 | 0.0 | 0.0 | 19.4 | 3.2 |
| 金融業 | 37.0 | 11.1 | 3.7 | 9.3 | 1.9 | 5.6 | 3.7 | 5.6 | 18.5 | 1.9 |
| 運輸・通信・倉庫業 | 33.3 | 11.1 | 7.4 | 11.1 | 0.0 | 7.4 | 3.7 | 0.0 | 18.5 | 7.4 |
| 情報処理サービス業 | 36.5 | 10.8 | 8.1 | 17.6 | 4.1 | 6.8 | 2.7 | 0.0 | 6.8 | 1.4 |
| 地方公共団体 | 19.6 | 5.9 | 2.0 | 45.1 | 0.0 | 13.7 | 2.0 | 0.0 | 2.0 | 2.0 |

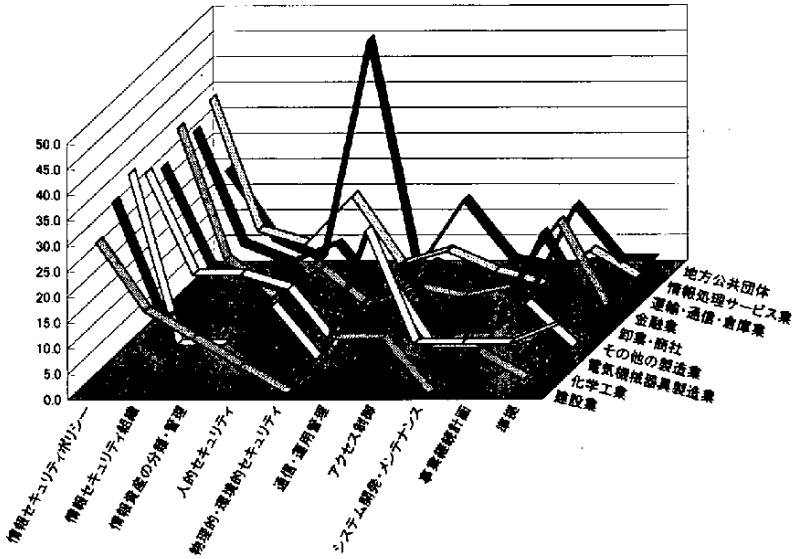



図2－4－15. 業種別にみた重要セキュリティ要素（第1位　回答件数25件以上）

## 2.5 災害対策・障害対策について

Q30. 情報セキュリティポリシー、実施手続・規程類に基づき、災害・障害対策が明確にされていますか。

| | | | |
|---|---|---|---|
| 1 | 情報セキュリティポリシーや実施手続・規程類の中で明確になっている | 166 | 27.4 |
| 2 | 他の基準で扱っている | 164 | 27.1 |
| 3 | 特に定めていない(情報セキュリティポリシーがない場合も含む) | 267 | 44.1 |
| 無回答 | | 8 | 1.3 |
| 計 | | 605 | 100.0 |

情報セキュリティポリシーや実施手続などに災害対策や障害対策を定めているかという質問については、「情報セキュリティポリシーや実施手続・規程類の中で明確になっている」が 27.4%であり、前回の 19.1%と比較して 8.3 ポイント増加している。また「他の基準で扱っている」が 27.1%と前回の 26.2%に比べて微増している。そのため「特に定めていない(情報セキュリティポリシーがない場合も含む)」が 44.1%となり、前回の 53.6%から 9.5 ポイント減少し 50%を下回った。まだまだ道半ばという感はあるものの認識度が向上していることがうかがえる。

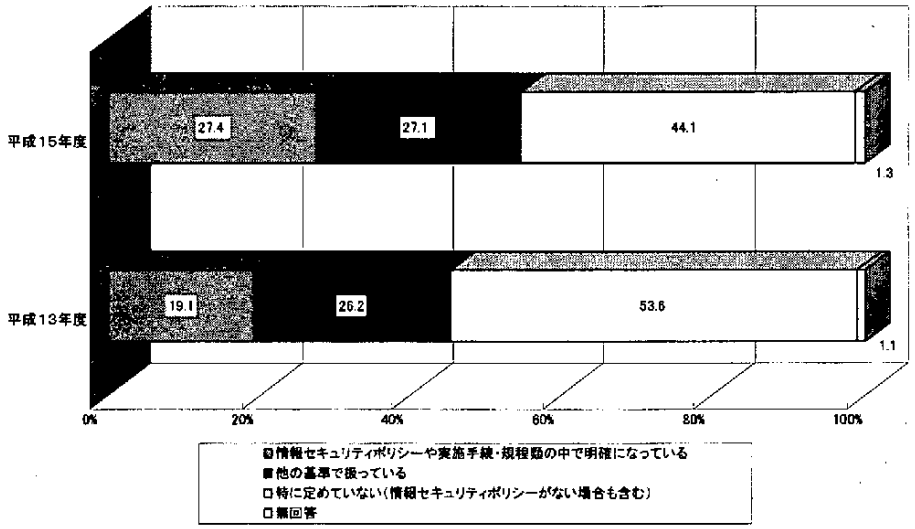



図2－5－1. 情報セキュリティポリシー、規定類における災害対策・障害対策の明確化

Q31.「JIS X 5080 規格」の事業継続性管理に定められている事業継続性計画を作成していますか。(オフィススペースの確保等も含む)。

| | | | | |
|---|---|---|---|---|
| 1 | 作成している | | 62 | 10.2 |
| 2 | 作成中である | | 40 | 6.6 |
| 3 | 作成を含め検討中である | ⇒Q33へ | 82 | 13.6 |
| 4 | 作成していない | ⇒Q33へ | 392 | 64.8 |
| 5 | 必要ない | ⇒Q33へ | 12 | 2.0 |
| 無回答 | | ⇒Q33へ | 17 | 2.8 |
| 計 | | | 605 | 100.0 |

事業継続性管理計画の作成については、64.8%が「作成していない」という回答となった。今回初めての質問であるが、ニューヨークの同時多発テロ(2001.9.11)の後で業務継続計画や業務

復旧計画の必要性がいわれているとはいえ、現実には作成が難しいことが現れており、実際に計画を「作成している」のは10.2%にすぎない。

なお、前回調査では類似の内容として「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を作成していますか」との質問があったが、ここではマニュアルを「作成している」(27.3%)、「作成していない」(36.4%)であり、この質問のニュアンスの差があるものの、「JIS X 5080」に定める事業継続性管理計画は単にマニュアルがあるだけでは完成されているとはいえず、訓練をはじめ、きちんと機能することが求められるため、ハードルが高いともいえる。

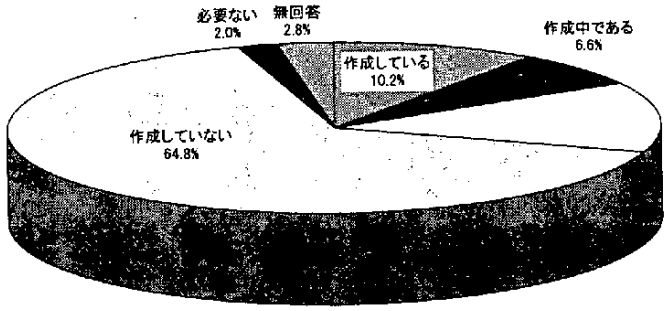



図2－5－2. 事業計測性計画の作成状況

Q32. (Q31で「1」、「2」と回答した場合) 事業継続性計画には以下の項目を含んでいますか。含まれている項目を選んで下さい。(複数回答)

| 回答件数 | | 102 | - |
|---|---|---|---|
| 1 | 外部からの悪意による緊急事態(サイバーテロ、ウイルス等) | 44 | 43.1 |
| 2 | ネットワークセキュリティ上の緊急事態(重大なセキュリティホール等) | 39 | 38.2 |
| 3 | 事故・災害(火災、地震、風水害、停電等) | 97 | 95.1 |
| 4 | 障害(ハードウェア障害、システムソフトウェア障害、回線障害等) | 80 | 78.4 |
| 5 | 人的なミスに起因する障害・誤処理(プログラムミス、オペレーションミス等) | 48 | 47.1 |
| 6 | 内部犯罪による緊急事態 | 22 | 21.6 |
| 7 | その他 | 3 | 2.9 |
| 無回答 | | 3 | 2.9 |

事業継続性計画を策定するためには対象とするリスクを明らかにする必要がある。そのため、事業継続性計画を作成(作成中を含む)している事業体に対し、どのようなリスクを対象としているか調査を行った。一番多いリスクは事故・災害(火災、地震、風水害、停電)などで実に95.1%の高い値を示した。これは前回調査の86.6%をさらに上回り、ほとんどの事業体が対象としていることを表している。次に多いのが「障害(ハードウェア障害、システムソフトウェア障害、回線障害など)」(78.4%)で、これは前回の78.5%とほぼ同様の値を示している。この2つがいわばAランクのリスクである。第3番目はやや採用割合の水準が下がってBランクに3つのリスクが想定されている。「人的ミスに起因する障害・誤処理(プログラムミス、オペレーションミス等)」(47.1%)で、前回の44.6%とほぼ同じである。また「ネットワークセキュリティ上の緊急事態(重大なセキュリティホール等)」は38.2%と、これは前回の45.6%に比較すると下がっている。一方、「外部からの悪意による緊急事態(サイバーテロ、ウイルス)」については43.1%と前回の

11.7%から31.4ポイントも増加している。これはウイルスやハッカーまがいのポートスキャンが日常となっているという情報ネットワーク環境の悪化を表していると想定される。またこの外部からの悪意による緊急事態にネットワークセキュリティ上の緊急事態が吸収されて認識されていることも考えられる。これはネットワーク上のセキュリティホール等が発見されるとすぐに世界中でそれを狙ったハッキングが横行しているからである。

なお、今回新たに追加した「内部犯罪による緊急事態」は21.6%であり、従来日本で行われてきた性善説を基にした対応策では不十分、という考え方がまだ主流ではないが一定程度存在していることがうかがえる。これは自治体などを中心に預かった情報資産を守っていることを証明する必要性が認識されてきたとも考えられる。

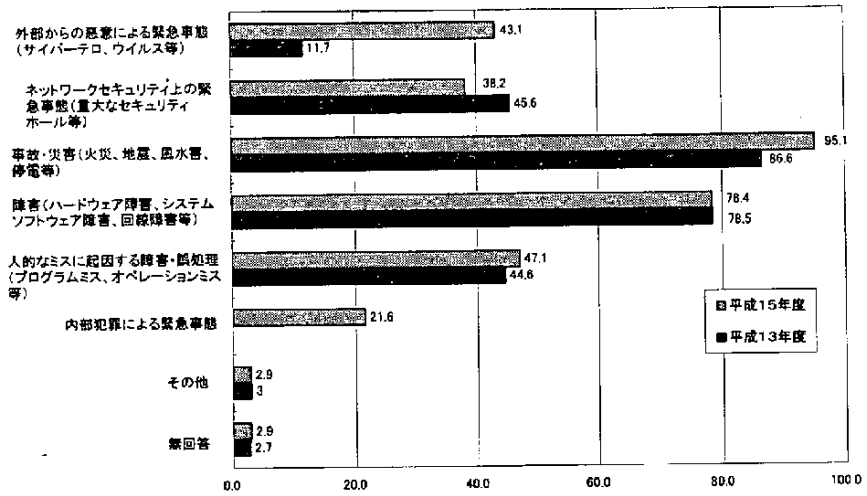



図2－5－3. 事業継続性計画での策定項目

Q33. 情報システムの災害に対する復旧対策としてどのようなことを実施していますか。実施している対策を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。（複数回答）

| 回答件数 | | 605 | － |
|---|---|---|---|
| 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） | 192 | 31.7 |
| 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 | 13 | 2.1 |
| 3 | バックアップサービス業者と契約を交わしている | 32 | 5.3 |
| 4 | 別の場所にバックアップセンタを設置している | 58 | 9.6 |
| 5 | ネットワークのバックアップを行っている | 196 | 32.4 |
| 6 | サーバのバックアップ用ファイルを専門保管業者に依頼して保管している | 145 | 24.0 |
| 7 | サーバのバックアップ用ファイルを遠隔地の自社施設に保管している | 105 | 17.4 |
| 8 | サーバのバックアップ用ファイルを自社内（耐火金庫等）に保管している | 230 | 38.0 |
| 9 | サーバのファイルは、遠隔地にミラーファイルを持っている | 23 | 3.8 |
| 10 | PC中の業務用ファイルのバックアップを取っている | 206 | 34.0 |
| 11 | PC中の業務用ファイルのバックアップを遠隔地に保管している | 16 | 2.6 |
| 12 | データのバックアップを定期的に行っている | 488 | 80.7 |
| 13 | その他 | 8 | 1.3 |
| 14 | アウトソーシング先の対策は把握していない | 8 | 1.3 |
| 15 | 特に対策を講じていない　⇒Q34へ | 15 | 2.5 |
| 無回答 | | 15 | 2.5 |

情報システムの災害に対する復旧対策の策定状況について調査した。サーバ関連対策で一番実施されているのが「データのバックアップを定期的に行っている」(80.7%) であり、ランクAの選択率である。続いて30%台のBランクのものはサーバに関するバックアップに関するものが多い。「サーバのバックアップ用ファイルを自社内 (耐火金庫等) に保管している」(38.0%)、「サーバのバックアップ用ファイルを専門保管業者に依頼して保管している」(24.0%)、「サーバのバックアップ用ファイルを遠隔地の自社施設に保管している」(17.4%) があげられる。複数回答のため、この3つを並行して実施している事業体があるとも考えられるが、38%から最大80%までの間でサーバのバックアップが行われていると考えられる。

次にネットワーク関連対策で実施されているのが、「ネットワークのバックアップを行っている」(32.4%)、「PC 中の業務用ファイルのバックアップを取っている」(34.0%)、が対策として挙げられている。一方、機械での作業がうまくいかないことを想定して、「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)」(31.7%) もある。ここまでがランクBの対策といえる。

上記以外はどちらかというと対策が実施されないという部類に入るものとなる。「同種の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」(2.1%)、「バックアップサービス業者と契約を交わしている」(5.3%)、「別の場所にバックアップセンタを設置している。」(9.6%)、「サーバのファイルは遠隔地にミラーファイルを持っている」(2.6%) などいずれも10%を下回っている。

2001 年のニューヨークワールドトレードセンタービルへのテロを契機に業務復旧および業務継続計画の必要性が問われ、何らかの対策がとられてきている。これは「特に対策を講じていない」(2.5%) と少ないことからも明らかである。しかし、離れた場所にデータやプログラムのバックアップを持ち、あるいは本格的なバックアップセンタの保有かバックアップサービス業の利用の必要性がいわれているが、実際にはそれらの対策の実施率は低く、具体的な動きとしてはまだ障害対策などですぐにでもバックアップデータから復旧できるように、手元にバックアップデータを保存しているレベルの対応策が多い状況であることがうかがえる。

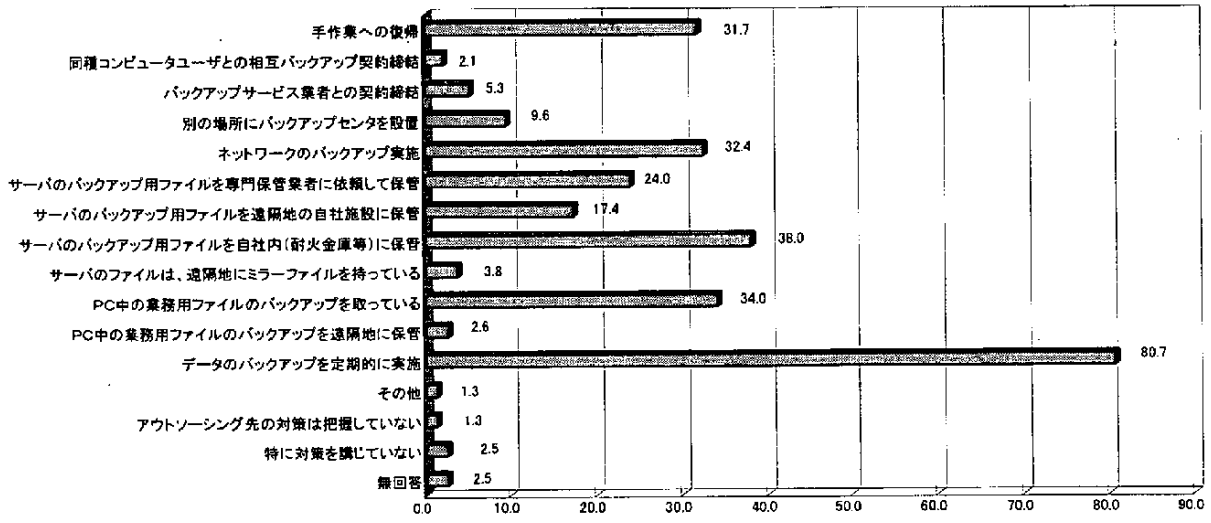



図2−5−4. 情報システムの災害復旧対策の実施状況

Q34.（Q33 で「15」と回答した場合）復旧対策を講じない理由は何ですか。主な理由を1つだけ選んで下さい。

| | | | |
|---|---|---|---|
| 1 | 経営者層の理解が得られない | 2 | 13.3 |
| 2 | コストがかかりすぎる | 8 | 53.3 |
| 3 | バックアップに対する必要性を感じていない | 1 | 6.7 |
| 4 | 満足する対策がない | 2 | 13.3 |
| 5 | その他 | 1 | 6.7 |
| 複数回答 | | 1 | 6.7 |
| 計 | | 15 | 100.0 |

Q33 で復旧対策を講じないという回答が少なかったため、統計上意味がある数字までにはいたっていないが、「コストがかかりすぎる」（53.3%）が過半数をしめた。その他は「経営者層の理解が得られない」、「バックアップに対する必要性を感じていない」、「満足する対策がない」、「その他」などが1、2件の回答となっている。

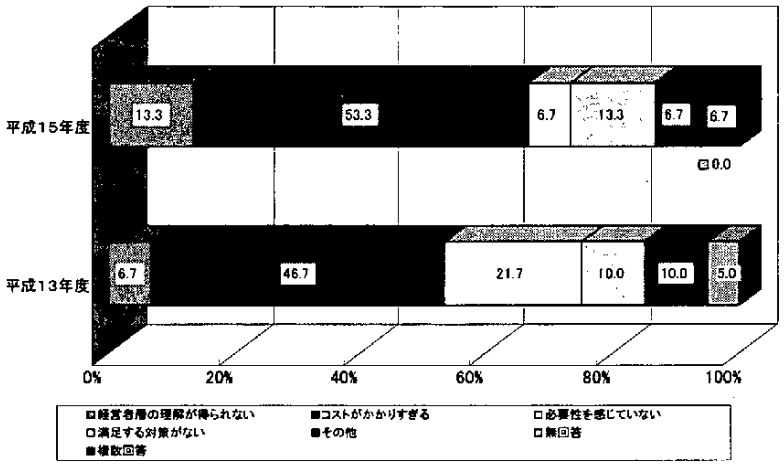



図2－5－5. 情報システムの障害対策を講じない理由

Q35. 情報システムの障害対策として次の機能を設けていますか。現在設置している機能を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。（複数回答）

| | | | |
|---|---|---|---|
| 回答件数 | | 605 | - |
| 1 | デュアルシステム | 61 | 10.1 |
| 2 | デュプレックスシステム | 69 | 11.4 |
| 3 | ホットスタンバイシステム | 142 | 23.5 |
| 4 | コールドスタンバイシステム | 130 | 21.5 |
| 5 | クラスタリング | 118 | 19.5 |
| 6 | 高可用性機構 | 59 | 9.8 |
| 7 | ミラリング | 303 | 50.1 |
| 8 | フォールトトレラント | 62 | 10.2 |
| 9 | アウトソーシング先の対策は把握していない | 13 | 2.1 |
| 10 | 特に設けていない | 105 | 17.4 |
| 無回答 | | 30 | 5.0 |

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

基幹システムがメインフレームの場合は「ホットスタンバイシステム」が23.5%（前回16.4%）と最も高く、コールドスタンバイシステム」が21.5%（前回14.8%）とこれに続いているが、それほど大きな差はみられない。

基幹システムがクライアントサーバシステムの場合は、「ミラリング」が50.1%（前回42.5%）と高いポイントとなっている。

また、「特に設けていない」は17.4%で、前回の28.3%からみると10.9ポイント低くなっているが、これは情報システムの障害対策の重要性が認識されてきている結果と思われる。

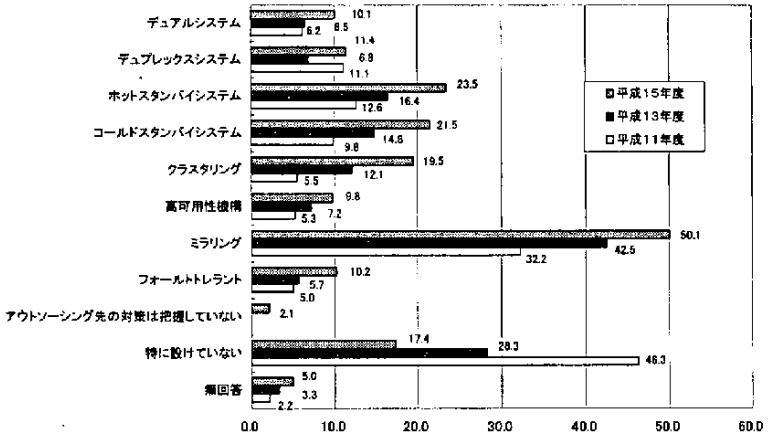


図2－5－6. 情報システムの障害対策機能の設置状況

業種別の「特に設けていない」の回答率は以下のとおりであるが、各業種別の割合の高さは、基幹システムに障害が発生した場合の事業体に与える影響度の大きさによる結果と思われる。

| | |
|---|---|
| 第二次産業 | 21.9% |
| 第三次産業 | 15.8% |
| 政府・地方公共団体 | 5.6% |

Q36. サーバ設置場所、データ保管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。各場所別に実施している対策を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。（複数回答）

| 対策項目 | サーバ設置場所 | | データ保管場所 | |
|---|---|---|---|---|
| 回答件数 | 605 | - | 605 | - |
| 自動火災報知設備を設置している | 460 | 76.0 | 419 | 69.3 |
| ガス式の消火設備を設置している | 288 | 47.6 | 237 | 39.2 |
| 消火器を設置している | 381 | 63.0 | 347 | 57.4 |
| スプリンクラ消火設備を設置している | 110 | 18.2 | 112 | 18.5 |
| 排煙設備を設置している | 179 | 29.6 | 161 | 26.6 |
| 耐火金庫を設置している | 132 | 21.8 | 276 | 45.6 |
| 消火・排煙等の防災機器の点検を定期的に行っている | 342 | 56.5 | 323 | 53.4 |
| その他 | 11 | 1.8 | 11 | 1.8 |
| アウトソーシング先の対策は把握していない | 18 | 3.0 | 28 | 4.6 |
| 特に対策を講じていない | 41 | 6.8 | 41 | 6.8 |
| 無回答 | 18 | 3.0 | 37 | 6.1 |

| 火災対策 | サーバ設置場所 | データ保管場所 |
|---|---|---|
| 自動火災報知設備を設置している | 76.0% | 69.3% |
| 消火器を設置している | 63.0% | 57.4% |

自動火災報知設備を設置し、かつ消火器を設置している火災対策が多いようである。

データ保管場所よりサーバ設置場所の方が割合が高いが、これはデータ保管場所よりサーバ設置場所の方が一般的に重視されている結果であろう。

データ保管場所もサーバ設置場所と同様、情報システムの運用上不可欠であることを認識して対策の強化を図る必要がある。

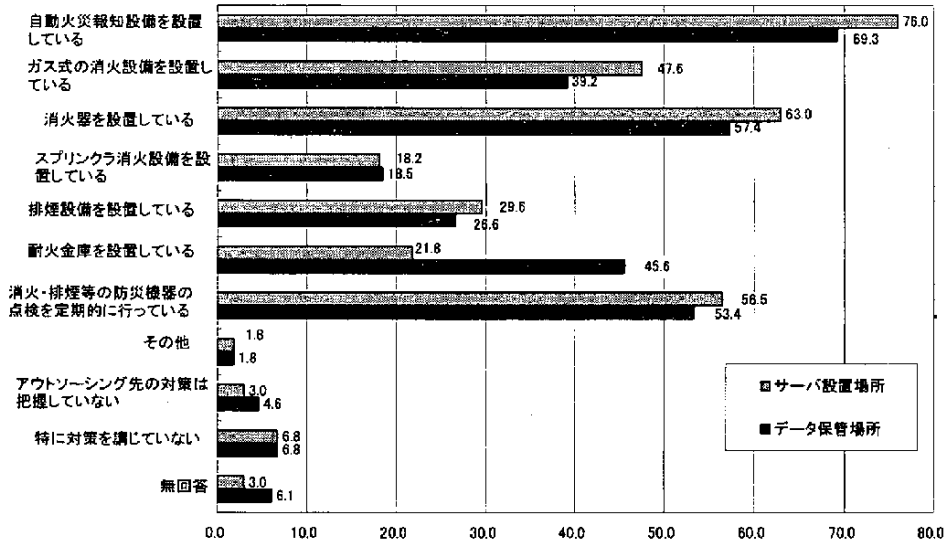



図2－5－7. サーバ設置場所、データ保管場所の火災対策

業種別の「アウトソーシング先の対策は把握していない」の回答率は以下のとおりであるが、アウトソーシング先の対策は自事業体と同様に重要であるので、把握すると同時に契約上明記する必要がある。

| | |
|---|---|
| 第二次産業 | 3.2% |
| 第三次産業 | 5.1% |
| 政府・地方公共団体 | 9.3% |

業種別に「特に対策を講じていない」の回答率は以下のとおりである。

| | |
|---|---|
| 第二次産業 | 6.8% |
| 第三次産業 | 7.4% |
| 政府・地方公共団体 | 1.9% |

Q37. サーバ設置場所、データ保管場所ではどのような地震対策をとっていますか。各場所別に実施している対策を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。(複数回答)

| 対策項目 | サーバ設置場所 | | データ保管場所 | |
|---|---|---|---|---|
| 回答件数 | 605 | - | 605 | - |
| 建物が免震構造になっている | 90 | 14.9 | 82 | 13.6 |
| 建物が耐震構造になっている | 220 | 36.4 | 217 | 35.9 |
| 転倒防止措置を講じている | 339 | 56.0 | 245 | 40.5 |
| 機器の移動防止措置を講じている | 239 | 39.5 | 164 | 27.1 |
| フリーアクセス床は耐震構造としている | 180 | 29.8 | 133 | 22.0 |
| フリーアクセス床は免震構造としている | 84 | 13.9 | 54 | 8.9 |
| 媒体の落下防止措置を講じている | 136 | 22.5 | 155 | 25.6 |
| その他 | 12 | 2.0 | 7 | 1.2 |
| アウトソーシング先の対策は把握していない | 18 | 3.0 | 31 | 5.1 |
| 特に対策を講じていない | 135 | 22.3 | 147 | 24.3 |
| 無回答 | 27 | 4.5 | 79 | 13.1 |

| 対策 | サーバ設置場所 | データ保管場所 |
|---|---|---|
| 転倒防止措置を講じている | 56.0% | 40.5% |

地震対策としては「転倒防止措置を講じている」がサーバ設置場所、データ保管場所共に高い割合となっている。

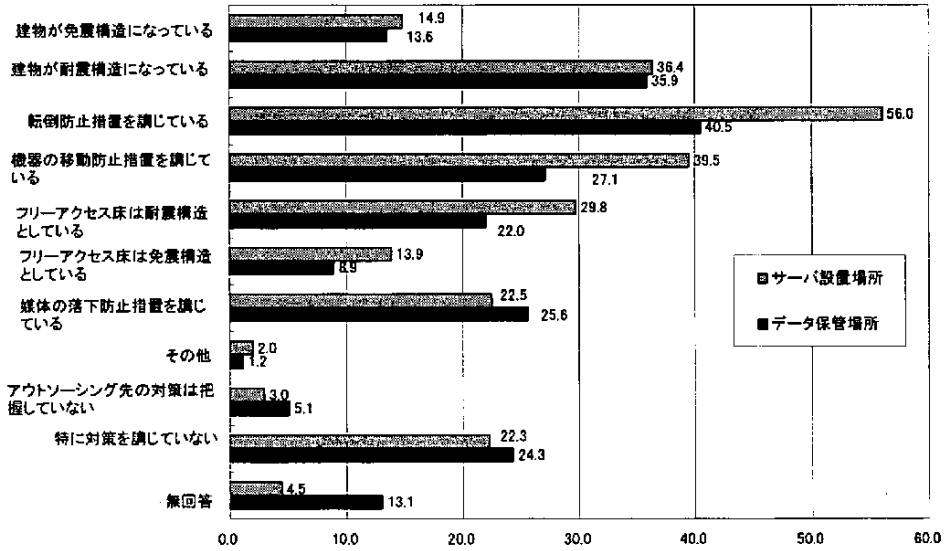



図2−5−8. サーバ設置場所、データ保管場所の地震対策

業種別の「アウトソーシング先の対策は把握していない」の回答率は以下のとおりである。

| | |
|---|---|
| 第二次産業 | 4.8% |
| 第三次産業 | 5.4% |
| 政府・地方公共団体 | 5.6% |

災害と同様にアウトソーシング先の地震対策を把握しておく必要があるだろう。

業種別の「特に対策は講じていない」の回答率は以下のとおりである。

| | |
|---|---|
| 第二次産業 | 29.5% |
| 第三次産業 | 22.6% |
| 政府・地方公共団体 | 9.3% |

火災対策に比べると、「特に対策は講じていない」の割合が高く、火災については対策を講じているが、地震についてはまだ対策が軽視されているように思われる。

Q38. 電源設備の災害対策としてどのような対策をとっていますか。実施している対策を選んで下さい。(複数回答)

| | | | |
|---|---|---|---|
| 回答件数 | | 605 | - |
| 1 | AVR | 51 | 8.4 |
| 2 | CVCF／UPS | 525 | 86.8 |
| 3 | 自家発電装置 | 223 | 36.9 |
| 4 | 電力供給経路の複数化 | 104 | 17.2 |
| 5 | その他 | 4 | 0.7 |
| 6 | 特に対策を講じていない | 38 | 6.3 |
| 無回答 | | 8 | 1.3 |

電源設備の災害対策としては「CVCF/UPS」が86.8%（前回80.4%）と高くなっている。

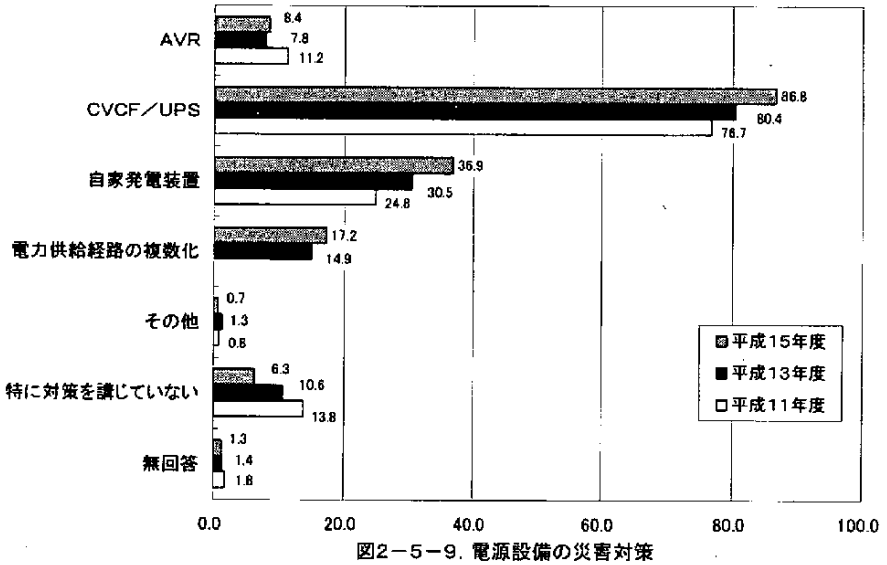


図2－5－9. 電源設備の災害対策

業種別の「特に対策を講じていない」の回答率は以下のとおりである。

| | |
|---|---|
| 第二次産業 | 10.4% |
| 第三次産業 | 3.7% |
| 政府・地方公共団体 | 1.9% |

第二次産業が「特に対策を講じていない」の割合が高いのが気になる。

業種別の「電力供給経路の複数化」の回答率は以下のとおりである。

| | |
|---|---|
| 第二次産業 | 14.7% |
| 第三次産業 | 20.5% |
| 政府・地方公共団体 | 11.1% |

第三次産業の「電力供給の複数化」の割合が高いのは、電力の供給停止による被害額の大きさを考慮してのことであろう。

Q39. 水冷の空調設備（室外機にクーリングタワーを使っている等）を使っている場合、空調用の水は何日分確保していますか。

| | | | |
|---|---|---|---|
| 1 | 1日分～3日分 | 67 | 11.1 |
| 2 | 4日分～6日分 | 16 | 2.6 |
| 3 | 7日分以上 | 38 | 6.3 |
| 4 | まったく確保していない | 53 | 8.8 |
| 5 | 水冷の空調設備を使用していない | 293 | 48.4 |
| 無回答 | | 138 | 22.8 |
| 計 | | 605 | 100.0 |

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

「まったく確保していない」8.8%（前回 9.7%）は割合としては少し高いが、前回から比べると、やや改善されているように思われる。

資本金規模別にみると、規模が大きいほど、空調用水７日分以上の確保の割合が高いことがわかる。

| 資本金規模 | 空調用の水7日分以上確保 |
|---|---|
| 500 億以上 | 25.6% |
| 100 億以上 500 億未満 | 21.1% |
| 100 億円未満 | 14.1% |
| 資本金なし | 3.4% |

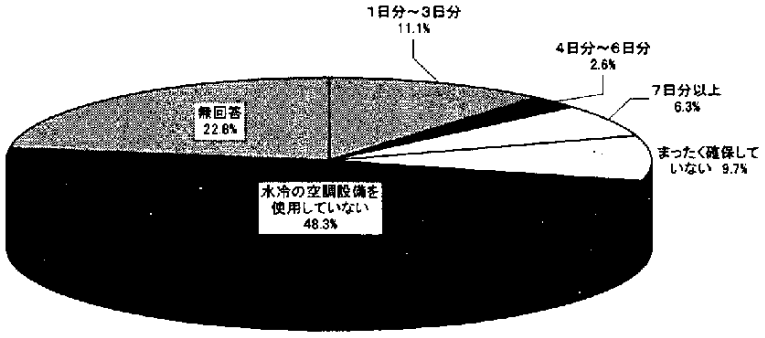



図2－5－10. 水冷空調設備用の水の確保について

Q40. 情報システム、サーバ設置場所、機器の災害・障害等で今後強化しなければならないと思う対策は何ですか。(複数回答)

| 回答件数 | | 605 | - |
|---|---|---|---|
| 1 | 自然災害対策 | 236 | 39.0 |
| 2 | 電源障害対策 | 162 | 26.8 |
| 3 | 空調等障害対策 | 82 | 13.6 |
| 4 | 回線障害対策 | 278 | 46.0 |
| 5 | ハードウェア障害対策 | 259 | 42.8 |
| 6 | OS障害対策 | 135 | 22.3 |
| 7 | ソフトウェア障害対策 | 154 | 25.5 |
| 8 | 火災による事故・障害対策 | 144 | 23.8 |
| 9 | 人の悪意による事故等への対策 | 216 | 35.7 |
| 10 | オペミス等、人の過失による事故等への対策 | 198 | 32.7 |
| 11 | テロによる機器の運用停止(DDOS:DOSアタックを含む)対策 | 97 | 16.0 |
| 12 | 取引先システムの停止や異常処理対策 | 43 | 7.1 |
| 無回答 | | 19 | 3.1 |

「回線障害対策」46.0%（前回 47.5%）が最も高く、「ハードウェア障害対策」42.8%（前回 37.6%）がこれに続いている。

前回は「人の悪意による事故等への対策」(36.6%)が三番目に高い割合であったが、今回は「自然災害対策」(39.0%、前回 30.2%)が三番目に高くなっており、自然災害への脅威を重視する傾向がみられる。

また、「テロによる機器の運用停止（DDOS：DOS アタックを含む）対策」が 16.0%と、前回の 27.4%より約 11 ポイント低くなったが、これはすでにテロの脅威が薄れてしまったと考えている結果であろうか。

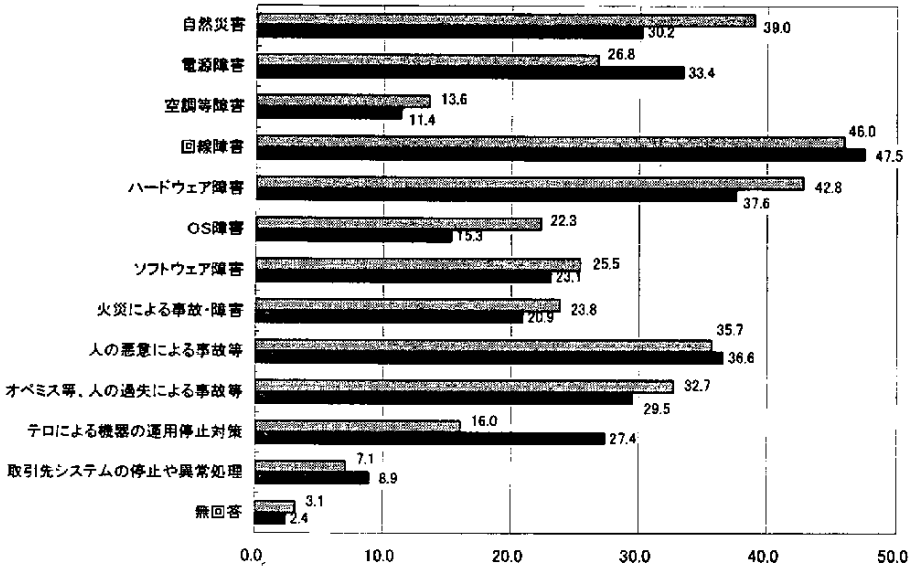



図2－5－11. 情報システム、サーバ設置場所、機器の災害対策で強化すべき点

Q41. 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 | | 605 | - |
|---|---|---|---|
| 1 | 通信事業者のケーブル障害(専用回線を含む) | 283 | 46.8 |
| 2 | 通信事業者の設備障害 | 241 | 39.8 |
| 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 | 244 | 40.3 |
| 4 | ISP(インターネットサービスプロバイダ)サービスの中断・停止 | 188 | 31.1 |
| 5 | LAN(配線)の障害 | 387 | 64.0 |
| 6 | ルータ・サーバ(機器)の障害 | 486 | 80.3 |
| 7 | 地震などの一定地域の災害 | 250 | 41.3 |
| 8 | その他 | 31 | 5.1 |
| 9 | 特に想定していない | 56 | 9.3 |

ネットワーク機器サービスの障害として最も多く想定されているのは「ルータ・サーバ機器の障害」(80.3%) で、前回調査の 74.7%よりも 5.6 ポイント増加している。次いで「LAN (配線) 障害」が 64.0%で、前回 (64.5%) とほぼ同様の結果となった。いずれも自事業体内での障害を中心とした想定である。実に５社のうち３～４社までが構内に IP ベースのネットワークを構築しており、これらの機器に対する不安を感じていることがわかる。しかし、MTBF (平均故障間隔) の分析 (Q19 参照) では全体的に大きな数値にはなっておらず、不安が先行しているとも考えられる。

これに続くのが「通信事業者のケーブル障害」(46.8%←H13:45.4%)、「通信事業者のサービス中断・サービス低下」(40.3%←H13:35.1%)、「通信事業者の設備障害」(39.8%←H13:34.7%)、「ISP サービスの中断・停止」(31.1%←H13:20.3%) で、通信業者関連の障害も依然としてかなり高い割合となっており、いずれも前回調査よりも増加傾向にある。企業ユーザは、自己のネットワーク、そのネットワークを外部と接続する通信事業者の順でサービスの障害を想定している。

また、「地震などの一定地域の災害」(41.3%) は前回調査の 30.2%と比べると 10 ポイント以上高くなっている。平成 15 年には、東南海地震や東海地震の対策が広く考えられており、これが一因となっているかと思われる。地域災害との関連も無視できない要素となっているのであろう。

最後に「特に想定していない」は前回調査の 6.4%から 2.9 ポイント上昇し、9.3%となっており、障害に対する関心は全体的に高くなっているといえよう。

業種別にみると、各業種とも共通した結果となった。

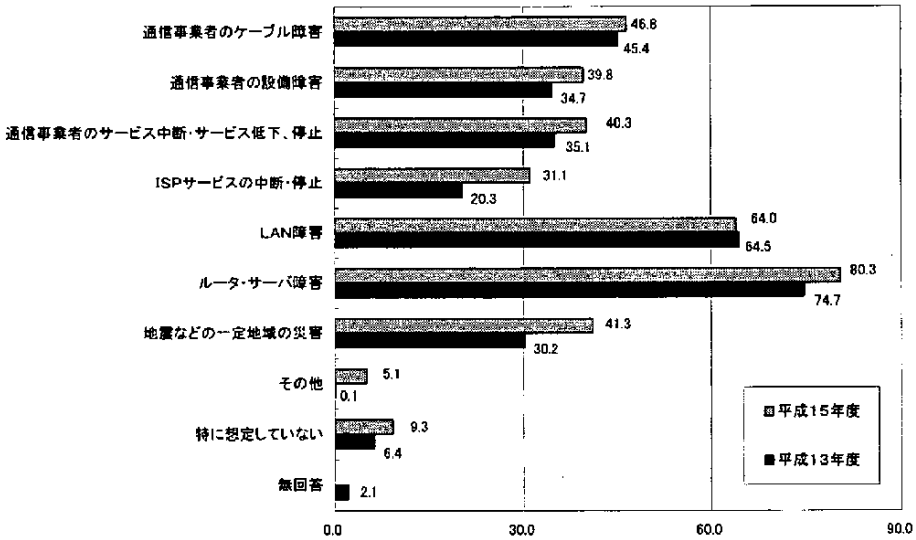



図2－5－12. 想定されるネットワーク機器、サービス障害

Q42. どのようなネットワーク障害対策を実施していますか。実施している対策を選んで下さい。（複数回答）

| | | | |
|---|---|---|---|
| 回答件数 | | 605 | - |
| 1 | 異なる種別回線を利用 | 140 | 23.1 |
| 2 | 異なる交換局への収容 | 40 | 6.6 |
| 3 | 異なるコモンキャリアの利用 | 61 | 10.1 |
| 4 | 異なるISPを利用 | 55 | 9.1 |
| 5 | 異なるメディアによる回線利用（例：衛星回線等） | 16 | 2.6 |
| 6 | ポイント間接続から網接続へ | 105 | 17.4 |
| 7 | 重要回線を部分的に二重化 | 193 | 31.9 |
| 8 | 専用のバックアップ回線を常時設定 | 110 | 18.2 |
| 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 | 96 | 15.9 |
| 10 | 社内の構内回線、LAN等を二重化 | 102 | 16.9 |
| 11 | 通信機器（CCU、ルータ、社外 WWW サーバ、DNS サーバ、アクセスサーバ等）の二重化 | 149 | 24.6 |
| 12 | インターネットに接続したサーバの分散（負荷分散、地域分散） | 82 | 13.6 |
| 13 | その他 | 8 | 1.3 |
| 14 | 特に対策を講じていない | 171 | 28.3 |
| 無回答 | | 14 | 2.3 |

Q41 のネットワーク障害の想定に関する調査では各事業体とも何らかの障害を想定し、それにあわせ何らかの対策を行っている。「特に対策を講じていない」が前回調査の 34.5%から 28.3%に減少したが、これは、障害の想定が高くなった分、各事業体が対策を実施していることの表れとみることができる。

特に前回との比較で大きく変わったのは、企業や組織がネットワークの信頼性の向上を目指す傾向が顕著になってきたことである。特に、図中に赤丸をした「重要回線を部分的に二重化」（31.9%←H13:25.8%）、「ポイント間接続から網接続へ」（17.4%←H13:11.0%）、「異なるコモンキャリアの利用」（10.1%←H13:6.8%）、「異なる ISP を利用」（9.1%←H13:5.0%）がいずれも大きく増加している。中でも「重要回線を部分的に二重化」は６ポイントも増加している。現在、

企業は経済の低成長、リストラと投資をかなり抑制してきている。しかし、今回の結果からはネットワークへの必要な投資については積極的であることがわかる。これは、もはや企業にとってネットワークは将来への投資ではなく、現在のビジネスの維持に必要な要素となっているためと考えられる。

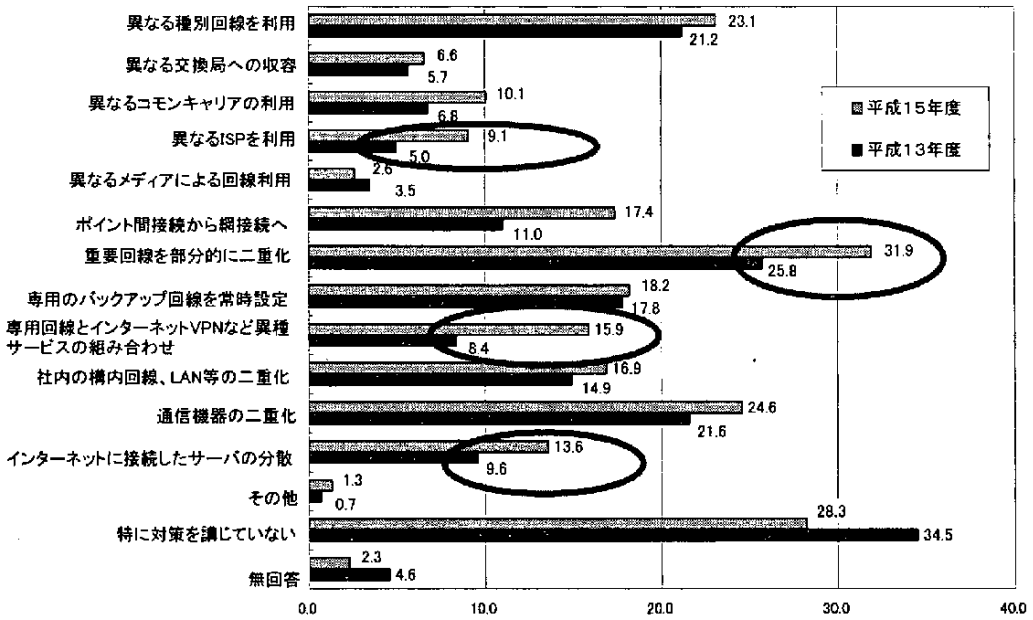



図2－5－13. ネットワーク障害対策の実施状況

Q43. 貴事業体では従業員に対し、情報セキュリティの面（災害／障害、不正アクセス、ウイルスを含む）から教育・訓練を実施していますか？

| | | | |
|---|---|---|---|
| 1 | 定期的に実施している | 101 | 16.7 |
| 2 | 時々実施している | 155 | 25.6 |
| 3 | 実施を予定している | 85 | 14.0 |
| 4 | 特に実施していない | 254 | 42.0 |
| 無回答 | | 10 | 1.7 |
| 計 | | 605 | 100.0 |

従業員に対する教育・訓練に関しては「時々実施している」（25.6%）が最も高い。情報セキュリティの問題は事業体全体の問題であり、また、経営上の影響も大きい問題でもあるため、事業体として従業員全員の理解と協力を得るためにも、教育・訓練に力を入れることの重要性を認識し、計画的な教育・訓練を実施すべきである。また、教育・訓練の対象として経営者層も入れる必要がある。

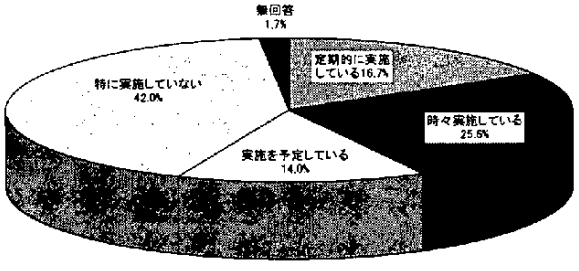



図2－5－14. 従業員に対する情報セキュリティ教育・訓練の実施状況

業種別にみると「特に実施していない」の回答率は以下のとおりである。

| | |
|---|---|
| 第二次産業 | 51.0% |
| 第三次産業 | 39.1% |
| 政府・地方公共団体 | 14.8% |

政府・地方公共団体は個人情報保護の点からも関係者の教育・訓練を重視していると思われる。

Q44. 貴事業体では情報セキュリティの人材をどのように養成していますか。

| | | | |
|---|---|---|---|
| 1 | 自社育成プログラムにより高度な人材育成を行っている | 47 | 7.8 |
| 2 | 民間資格を利用して育成している | 29 | 4.8 |
| 3 | 情報セキュリティアドミニストレータ試験を活用している | 38 | 6.3 |
| 4 | 特に行っていない | 463 | 76.5 |
| 5 | 必要ない | 2 | 0.3 |
| 無回答 | | 15 | 2.5 |
| 複数回答 | | 11 | 1.8 |
| 計 | | 605 | 100.0 |

情報セキュリティ人材の育成について「特に行っていない」との回答が76.5%と非常に高いポイントとなっている。情報セキュリティの人材育成には時間がかかることを考え、できるだけ早期に計画的に人材育成を強化する必要がある。

情報セキュリティに関する対策に費用をかけ、いくら強化しても、肝心の適任者が不足していては効果的な対策とならず無駄の多い内容となるケースが多い。

また、事件・事故・災害などが現実のものとなった場合は、適任者の迅速な指揮と行動が被害の拡大を防ぐ重要な要素であることを認識すべきである。情報セキュリティの人材育成の重要性をもっと認識する必要がある。

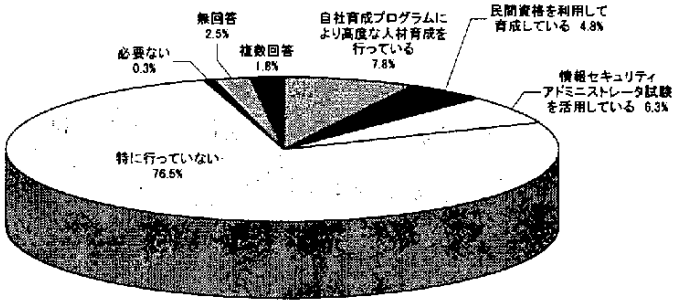



図2－5－15. 情報セキュリティ人材の養成状況

## 2.6 不正アクセス対策・不正侵入対策・情報漏洩対策について

Q45.「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 | 492 | 81.3 |
| 2 | 知らない | 105 | 17.4 |
| 無回答 | | 8 | 1.3 |
| 計 | | 605 | 100.0 |

「不正アクセス行為の禁止等に関する法律」が公布された平成11年度時点においては、法律の存在を「知っている」との回答は47.4%であったが、前回調査では76.7%、今回は81.3%となり、同法の認知度は大幅に高まった。

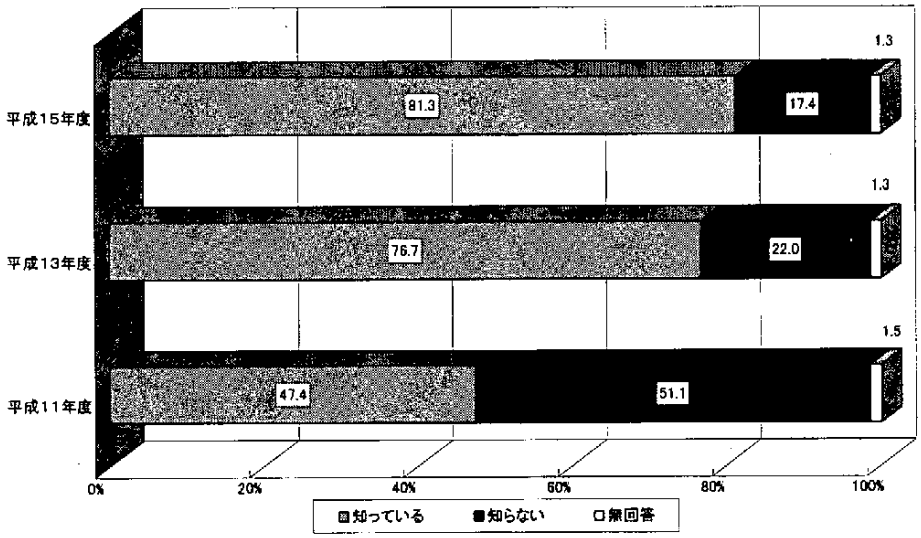



図2－6－1. 不正アクセス禁止法の認知度

Q46. 貴事業体では過去1年間に不正アクセスの被害に遇われたことがありますか。（複数回答）

| | | | |
|---|---|---|---|
| 1 | 物理的なアクセス被害（コンピュータ室等への侵入）に遭った | 1 | 0.2 |
| 2 | 論理的アクセス被害（ネットワーク経由による侵入）に遭った | 54 | 8.9 |
| 3 | な い ⇒Q48へ | 543 | 89.8 |
| 無回答 | ⇒Q48へ | 7 | 1.2 |
| 計 | | 605 | 100.0 |

大多数の事業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。また、論理的な不正アクセスは平成9年度が2.9%、11年度が6.1%、前回調査が14.6%と大幅に増加していたものの、今回調査では8.9%と少なくなっており、ファイアウォールの設置等をはじめとした不正アクセス対策の進展を示したものと考えられる。それでも、8.9%の事業体が論理的な不正アクセスの被害を受けていることは、これへの対策のさらなる徹底が必要なことを示している。

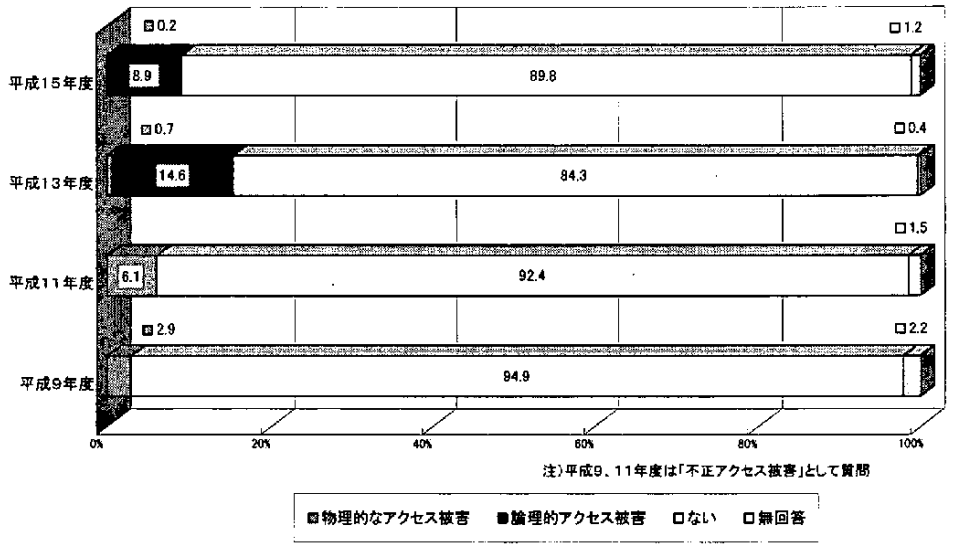



図2－6－2. 過去1年間の不正アクセス被害状況

Q47. 不正アクセス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

| | | | |
|---|---|---|---|
| 1 | 出した | 10 | 18.2 |
| 2 | 出さない | 44 | 80.0 |
| 無回答 | | 1 | 1.8 |
| 計 | | 55 | 100.0 |

IPA に被害届を出す事業体は前回調査同様約２割にとどまり、やはり少数である。Ｑ３においてIPAがコンピュータウイルスと不正アクセス被害の届出機関であることを「知っている」という回答がともに７割を越えていることと比べると、非常に少ない回答率である。

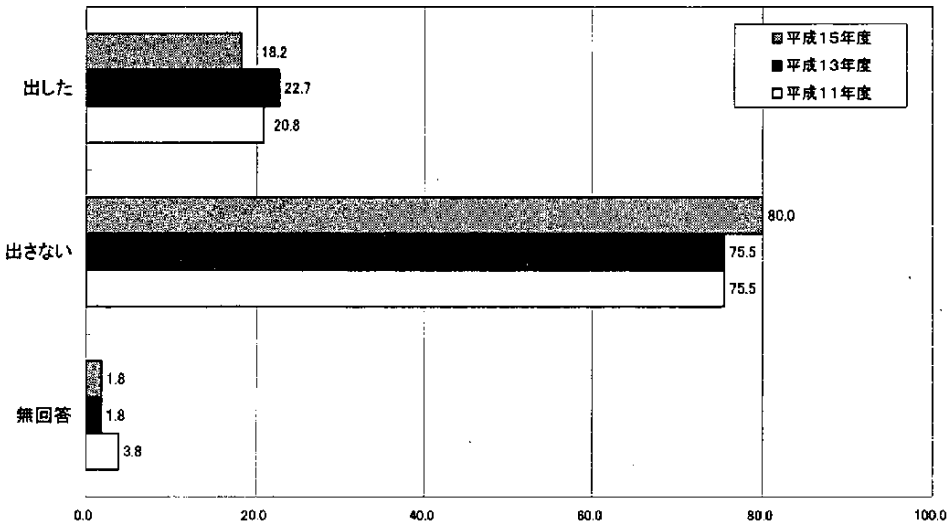



図2－6－4. 不正アクセス被害届出状況

Q48. 主要なサーバ設置場所、データ保管場所での物理的な不正アクセスに対してどのような対策を実施していますか。現在実施している対策を選んで下さい。(複数回答)

| | | | |
|---|---|---|---|
| 回答件数 | | 605 | - |
| 1 | 不正アクセスを受けた場合のIPAやJPCERT／CCへの相談 | 22 | 3.6 |
| 2 | 室の出入口での入室管理 | 348 | 57.5 |
| 3 | 室の出入口での退室管理 | 255 | 42.1 |
| 4 | 室への入退室についてカード、パスワードを使用 | 275 | 45.5 |
| 5 | 入退室のときにアンチパスバック(定期券のように二度連続して入れないような仕組み)を持っている | 21 | 3.5 |
| 6 | 室への入室について身体的特徴(指紋、虹彩等)により識別 | 51 | 8.4 |
| 7 | 室の管理責任者を定めている | 282 | 46.6 |
| 8 | 情報システムの監視設備を設けている | 99 | 16.4 |
| 9 | 定期的にリスク分析や情報セキュリティ監査を実施 | 81 | 13.4 |
| 10 | その他 | 17 | 2.8 |
| 11 | アウトソーシングのため、自社では特に対策を講じていない | 20 | 3.3 |
| 12 | 特に対策を講じていない | 111 | 18.3 |
| 無回答 | | 6 | 1.0 |

物理的な不正アクセスに対する対策は、大きな傾向は平成 11 年度、前回とほぼ同様である。ただし、「特に対策を講じていない」事業体が平成 11 年以降大きく減少してきており、物理的なアクセス対策が進んでいることがわかる。なお、約４～５割の事業体が「管理責任者の設置」、「入退室管理」、入退室における追加的な処置としての「カード・パスワードの利用」を実施している。

特に「入室管理」は 11 年度の 37.9%が前回調査では 45.3%、今回調査では 12.2 ポイント増加して 57.5%になった。また、「退室管理」では、11 年度の 26.2%が前回調査では 34.0%、今回は 8.1 ポイント増加して 42.1%になった。さらに、「カード・パスワードの利用」では、11 年度の 38.2%が、前回 37.7%、今回 7.8 ポイント増加して 45.5%になった。データにアクセスした者の管理のために入退室管理、さらに、無人の場合の追加的処置としてのカード・パスワードの利用が重要とみなされるようになった。この結果から、昨今の情報セキュリティ対策でデータを保存しているサーバなどの機器を隔離し、物理的に保護することが重要とみなされるようになったことがわかる。

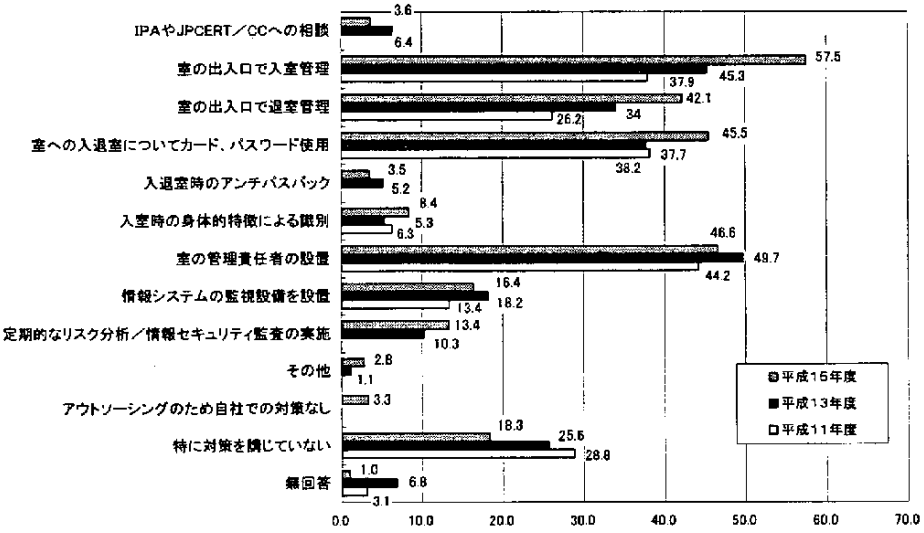



図2－6－4. 物理的不正アクセスの実施状況

Q49. ネットワークを介しての論理的な不正アクセスに対してどのような対策を実施していますか。現在実施している対策を選んで下さい。(複数回答)

| 回答件数 | | 605 | - |
|---|---|---|---|
| 1 | 不正アクセスを受けた場合のIPAやJPCERT／CCへの相談 | 21 | 3.5 |
| 2 | パスワードの活用 | 411 | 67.9 |
| 3 | ファイアウォールの利用 | 504 | 83.3 |
| 4 | セキュリティパッチの適用 | 369 | 61.0 |
| 5 | アクセス制御ソフトウェアの使用 | 171 | 28.3 |
| 6 | 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の実施 | 106 | 17.5 |
| 7 | ネットワーク機器の運用者(アクセス範囲)の限定 | 311 | 51.4 |
| 8 | 情報セキュリティポリシーで勝手にLANの配線を触ったり、個人のPCを接続することの禁止 | 220 | 36.4 |
| 9 | 情報セキュリティ管理者がサーバやルータ、ファイアウォールのログの定期的にチェック | 124 | 20.5 |
| 10 | 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 | 258 | 42.6 |
| 11 | 情報セキュリティ監査の実施 | 75 | 12.4 |
| 12 | システム監査の実施 | 71 | 11.7 |
| 13 | その他 | 11 | 1.8 |
| 14 | 特に対策を講じていない | 31 | 5.1 |
| 無回答 | | 4 | 0.7 |

論理的不正アクセス対策について、今回の調査では、前回調査の内容を見直し、選択肢に「セキュリティパッチの適用」、「システム監査の実施」を追加した。特に、OSのパッチがバッファーオーバフロー問題で注目されていること、このパッチを適用しないユーザを狙ったウイルス攻撃が問題となっているが、結果として61.0%がセキュリティパッチを適用していることがわかり、きわめて注目されていることがわかった。しかし、40%近くが適用していない可能性もあり、これが一度攻撃されると大きな問題となることが懸念される。より積極的な広報が望まれる。

ネットワークからの不正アクセスに講じている対策について、今回の調査では、「パスワードの活用」が67.9%と、平成11年度の83.4%、前回の66.3%と比べても低いレベルである。現在のネットワーク環境を考えた場合、ユーザIDとパスワードによる認証の実施率は100%に達していると思われるので、回答者が質問の「活用」という言葉を厳密に解釈しすぎた結果ではないかと思われる。また、ネットワーク機器などほとんどがIDとパスワードで管理されている中で、管理対象が多すぎて、特にきちんとしたパスワード管理を怠っているのであれば問題である。ネットワーク管理者や情報セキュリティ管理者は、再度、すべての機器やユーザなどのパスワードについて再検討する必要がある。

次に、「ファイアウォールの利用」については11年度の50.7%から前回は18.4ポイント増加して69.1%であったが、今回調査ではさらに20ポイント増加し、83.3%となった。これは、企業や組織にとって、インターネットが必須のものとなったことと、不正アクセス事件などの増加で、ファイアウォールの利用の重要性が認識されたためと考えられる。

一方、1,000万加入を超えたブロードバンドの進展によって、一般家庭や小規模事業者が不正侵入や踏み台攻撃の対象になっており、パーソナルファイアウォール等を含めた対策がより必要となっている。資本金規模とファイアウォールの設置との関係を図2-6-6でみると、事業規模が

小さくなるとファイアウォールの設置の割合が下がっている。今後、このようなブロードバンドを利用するようになった小規模事業者の不正アクセス問題が懸念される。このような事業者へのファイアウォールの導入にあたって支援政策が望まれる。

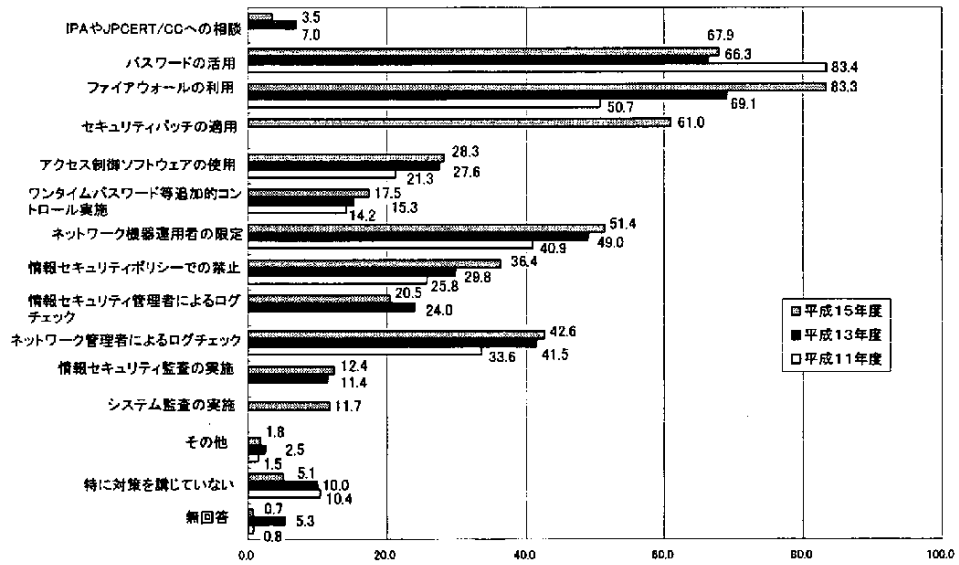



図2－6－5. 論理的不正アクセス対策の実施状況

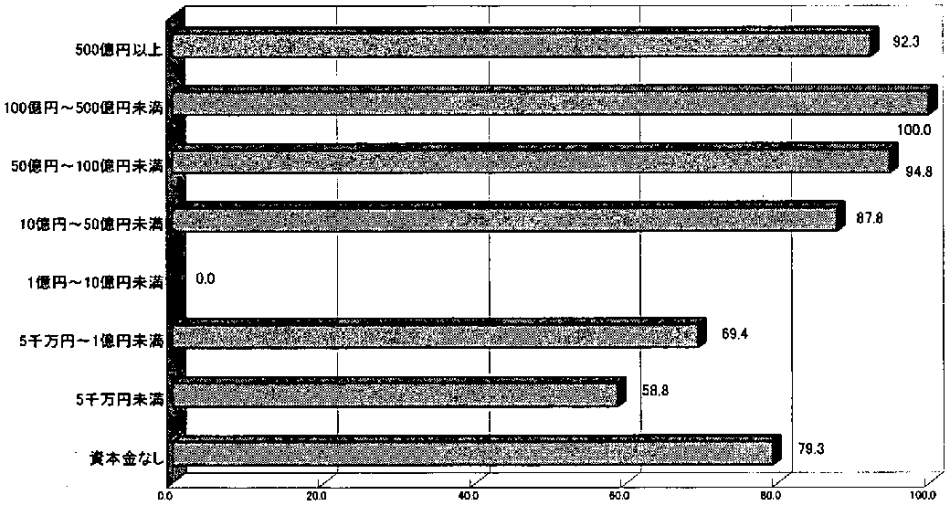



図2－6－6. ファイアウォールの設置と資本金規模との関係

業種別にファイアウォールの設置状況をみると、政府・地方公共団体が92.6％と高い。これは、住民基本台帳制度で安全性が議論されていることから意識が高いことがわかる。一方、保険業（生保・損保）が100％であるのに対し、金融業は72.2％と同類の業種でも事業の性質によって異なっており、一方、情報処理サービス業は90％近い。すなわち、個々の企業のさまざまな要因によってファイアウォールの採用が異なっている。

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前回調査から大きくは改善されていない。今後、営業の情報化が進むなかで、どの事業体も外部からネットワークにアクセスする機会が増えてくると想定される。この場合には、「ワンタイムパスワード」などの利用が必須である。

「情報セキュリティポリシーで勝手にLANの配線を触ったり、個人のPCを接続することを禁止」については、実施している事業体の比率が前回調査の29.8%から36.4%に大きく増加した。セキュリティポリシーを定めている事業体ではほとんどが制限を含めていると考えられる。また、セキュリティポリシーの浸透と比例して、今後、セキュリティポリシーを定めるときに、アクセスや配線などLANにかかわる事項は、必ず含むべき項目である。

「情報セキュリティ管理者やネットワーク管理者による定期的なログのチェック」は、情報セキュリティ管理者によるものが前回調査と比べて減少した、一方、ネットワーク管理者によるものは、前回調査より増加している。特にファイアウォールの設置率が80%を超えたことを考えると、未だ多くの事業体で十分な監視が実施されているとはいえない。これには情報セキュリティ管理者とネットワーク管理者の業務の切分けなども必要となる。

最後に、Q48とQ49に共通していることとして、IPAやJPCERT/CCの活用が平成13年度から増加してきているが、その頻度はきわめて低いことがあげられる。これは、両者の組織が専門的であるため、本当に必要とする機会が少ないことが原因であるが、ウイルスや不正侵入に関する情報収集力や広報をもっと簡単に活用できるような工夫も必要と考える。

Q50. 情報についての機密度のランクを設定していますか。

| | | | |
|---|---|---|---|
| 1 | ランクを設定し、暗号化している | 37 | 6.1 |
| 2 | ランクは設定していないが、暗号化はしている | 59 | 9.8 |
| 3 | ランクを設定しているが、暗号化はしていない | 143 | 23.6 |
| 4 | 暗号化していない | 343 | 56.7 |
| 無回答 | | 22 | 3.6 |
| 複数回答 | | 1 | 0.2 |
| 計 | | 605 | 100.0 |

暗号化の有無に関わらず、機密度のランクを「設定している」という割合は29.7%であり、前回調査の28.4%と比較するとほぼ横ばいとなっている。各情報について機密度のランク付けを行うことは、その情報のセキュリティをコスト効率よく高めようとした時に必須の作業であり、この数字が上がらないことは、総花的な非常にコストの高いセキュリティ対策を行っているか、このあたりの対策があまり進んでいないことの表れと考えられる。

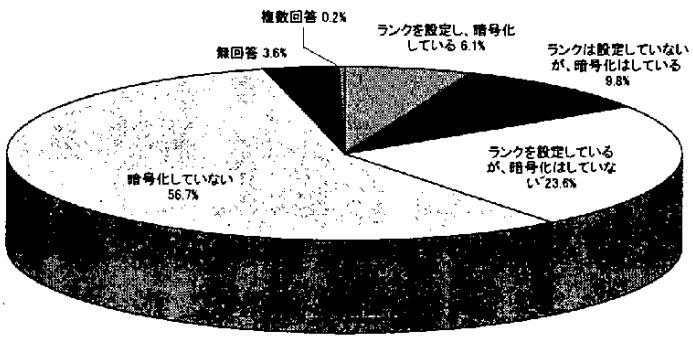



図2－6－7. 機密度ランクの設定状況

Q51. 貴事業体では基幹システム[注)]のパスワード変更をどのレベルに設定していますか。

| | | | |
|---|---|---|---|
| 1 | ワンタイムパスワードを設定している | 10 | 1.7 |
| 2 | 変更期限がきたらパスワードを無効にする | 40 | 6.6 |
| 3 | 定期的に新しいパスワードを配布する | 37 | 6.1 |
| 4 | 変更期限を定めて利用者が変更している | 100 | 16.5 |
| 5 | パスワードの変更を推奨しているが、変更期間は利用者に任せている | 169 | 27.9 |
| 6 | パスワードの変更に関して特に定めていない | 157 | 26.0 |
| 7 | パスワードによる管理を実施していない | 40 | 6.6 |
| 8 | その他 | 11 | 1.8 |
| 無回答 | | 7 | 1.2 |
| 複数回答 | | 34 | 5.6 |
| 計 | | 605 | 100.0 |

注)最も重要なシステム1つに限定して回答。基幹システムについては「2.3 図 2-3-1」を参照のこと)

パスワード管理については、前回調査に比べて管理水準の向上を示す数値が得られた。つまり、「変更期限がきたらパスワードを無効にする」(6.6%←H13:4.0%)、「定期的に新しいパスワードを配布する。」(6.1%←H13:5.4%)、「変更期限を定めて利用者が変更している。」(16.5%←H13:10.9%)といったパスワード管理を強化する回答が増加した。一方、「パスワードの変更を推奨しているが、変更期間は利用者に任せている。」(27.9%←H13:35.8%)、「パスワードの変更に関して特に定めていない」(26.0%←H13:29.7%)といった、弱いパスワード管理を実施している回答が減少した。これにより、パスワード管理は徐々にではあるが強化される方向に向かっていることを示している。しかし、パスワードの変更に関して「特に定めていない」という回答も 26%あり、より一層の改善の余地もあることを示している。

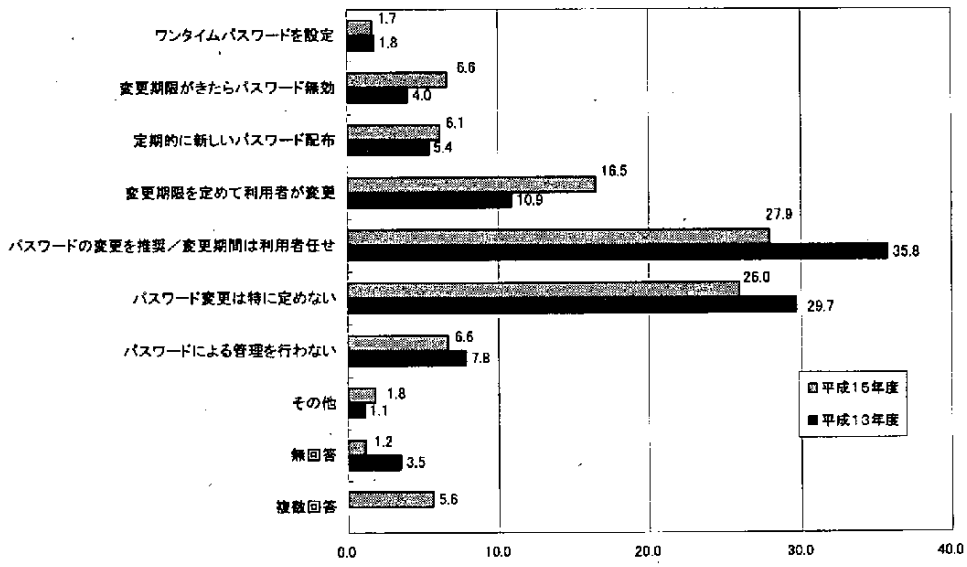



図2－6－8. 基幹システムのパスワード変更レベルの設定

Q52. 情報漏洩対策として行っていることは何ですか。(複数回答)

| 回答件数 | | 605 | - |
|---|---|---|---|
| 1 | セキュリティポリシー、規程類の整備 | 319 | 52.7 |
| 2 | 従業員に対する教育 | 276 | 45.6 |
| 3 | 入退室(館)管理 | 330 | 54.5 |
| 4 | アクセス管理 | 321 | 53.1 |
| 5 | 機密情報の管理 | 178 | 29.4 |
| 6 | 情報媒体(PC、携帯電話、PDA、記録媒体等)の持出し・持込みの禁止 | 194 | 32.1 |
| 7 | ハードディスク、CD、FD等記録媒体の返却、廃棄時の破壊、溶解 | 308 | 50.9 |
| 8 | 暗号化機能の採用 | 85 | 14.0 |
| 9 | 輸送体制強化 | 30 | 5.0 |
| 10 | 電子メールのモニタリング | 109 | 18.0 |
| 11 | ログチェックの追跡機能 | 130 | 21.5 |
| 12 | その他 | 4 | 0.7 |
| 13 | 特に対策を行っていない | 72 | 11.9 |
| 無回答 | | 6 | 1.0 |

情報漏洩に対する対策として、どのよう対策を実施しているかについて今回新たに質問を追加した。この結果、「セキュリティポリシーを定めている」事業体は前回調査の 24.0%から半数を超える 52.7%へと 28.7 ポイント増加した。これは、セキュリティポリシーの重要性がいろいろなところで訴えられ、これを反映した結果と考えられる。また、「従業員に対する教育」が 45.6%、「入退室管理」が 54.5%、「アクセス管理」が 53.1%と、ほぼ半数の事業体が実施している。一方、「機密情報の管理」については 29.4%と意外と低い数値になった。これは、Q50 で情報の機密度を設定している事業体の割合である 29.7%とほぼ同じであり、情報を機密と分類していない事業体は機密情報という認識がないためと思われる。

「ハードディスク等の情報記録媒体のライフサイクル管理」については、中古 PC のハードディスクから顧客情報が漏洩した等の事例があり、一般の認識が高まって廃棄時に破壊等の対策をとる事業体が増えたためと考えられる。しかし、セキュリティポリシーを定めることを初め、媒体のライフサイクル管理についても実施している事業体は約半数であり、これらが当然実施されるべき項目であることを考慮すると、残りの事業体は情報セキュリティ面で大きな課題を抱えていると考えられる。

暗号化の利用も Q50 とほぼ近い 14.0%となった。最近のハードウェアの性能向上により、データの暗号化に対する CPU リソースの問題は小さくなったが、鍵管理の作業は依然として大きな課題であり、その作業負荷を考えるとデータの機密度に応じて暗号化を適用するのが妥当な解決策である。

内部者による情報漏洩の大きな割合が電子メールによるものと思われるが、この「モニタリング」を実施している事業体は 18.0%と少なかった。この数字は、個人情報保護法の施行と共に今後増加していくと考えられる。

「システムログ等のチェック」は情報漏洩のみならず、不正アクセスの兆しを発見する手段でもあり、今回の 21.5%という数字は今後増加させていく必要がある。

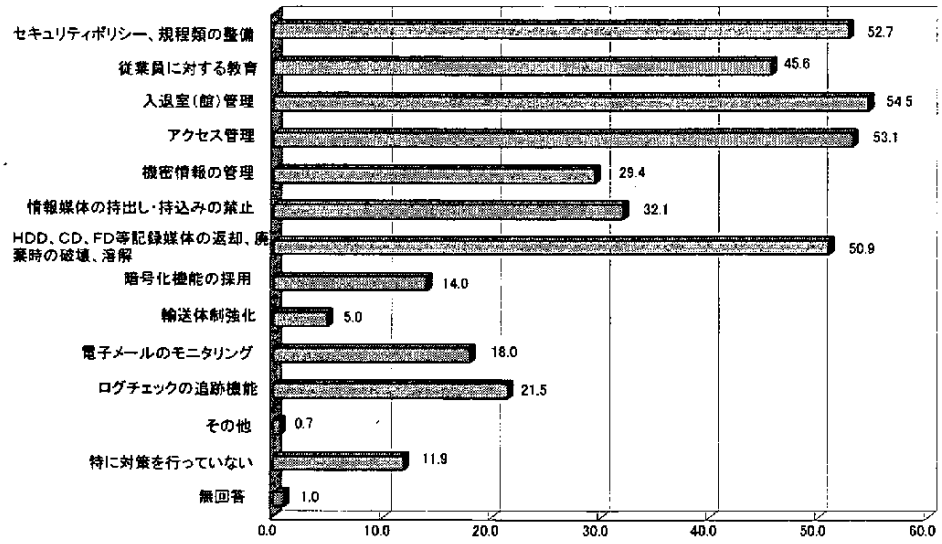



図2－6－9. 情報漏洩対策の実施状況

## 2.7 コンピュータウイルス対策について

Q53. 貴事業体では過去１年間にコンピュータウイルスに感染したことがありますか。

| | | | |
|---|---|---|---|
| 1 | ある | 424 | 70.1 |
| 2 | ない　⇒Q56へ | 179 | 29.6 |
| 無回答 | | 2 | 0.3 |
| 計 | | 605 | 100.0 |

コンピュータウイルスの被害は前回調査（68.8%）とほとんど変らず、感染率が 70.1%となった。これは、パソコンでのウイルス対策のワクチン利用率が 86.6%と、前回調査の 84.8%とあまり変っていないことがその原因と考えられる（Q56 の「PC でのワクチンソフトの利用」を参照）。しかし、パソコンにワクチンソフトを導入し、パラメータファイルの更新を行っていた事業体が 75.0%あったにも関わらず（Q59 の「パラメータファイル更新」を参照）、29.9%の事業体はウイルスに感染している。これは、平成-15 年１月に発生した SQL Slammer や同年８月に発生した MS Blaster のように、OS のセキュリティホールを悪用して、非常に感染の速い強いウイルスが発生したためと考えられる。

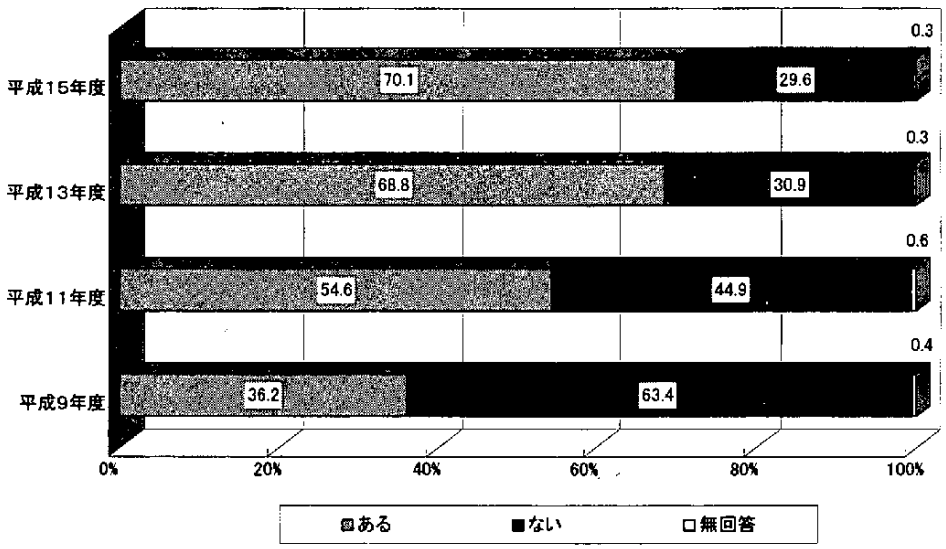



図2－7－1. 過去1年間のコンピュータウイルス被害状況

Q54.（Q53 で「１」と回答した場合）コンピュータウイルス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか。

| | | | |
|---|---|---|---|
| 1 | 出した | 59 | 13.9 |
| 2 | 出さない | 353 | 83.3 |
| 無回答 | | 12 | 2.8 |
| 計 | | 424 | 100.0 |

ウイルス被害にあった場合、経済産業省告示第 429 号で IPA に届け出ることになっている。今回の調査では届出を出した割合が 13.9%と、前回調査の 19.8%から大きく減少した。平成 11 年度調査では 13.5%だったので、ほぼその水準まで下がってしまったと考えられる。Q３で IPA が

ウイルス被害の届出機関であることを知っているとの回答が78.7%であることを考えると、この数字を上げるためには、届出を出したことに対する何らかの見返りの仕組みを構築する必要があると考えられる。

Q55. 主要な感染原因（経路）は判明していますか。主な原因を選んで下さい。（複数回答）

| 回答件数 | | 424 | - |
|---|---|---|---|
| 1 | フリーソフトウェアから | 5 | 1.2 |
| 2 | 外部から入手した記録媒体(FD、パソコン等)から | 162 | 38.2 |
| 3 | 社内ネットワーク経由で | 84 | 19.8 |
| 4 | インターネット経由で | 194 | 45.8 |
| 5 | 電子メールの添付書類で | 202 | 47.6 |
| 6 | 外部のホームページの閲覧で | 68 | 16.0 |
| 7 | その他 | 22 | 5.2 |
| 8 | わからない | 30 | 7.1 |
| 無回答 | | 6 | 1.4 |

コンピュータウイルスの感染経路は前回調査から大きな変化があった。つまり、前回調査で圧倒的に多かった電子メールの添付書類によるものが67.0%から47.6%へと大きく減少し、外部のホームページの閲覧によるものも25.1%から16.0%に大きく減少した。これは、これらの感染経路に対するワクチンソフトの対応が進み、これらの感染経路を使うウイルスのブロックに成功したためと考えられる。一方、外部から入手した記録媒体によるものが32.0%から38.2%に増加した。また、社内ネットワーク経由のものが15.2%から19.8%に、インターネット経由のものも42.1%から45.8%に増加した。こういったネットワーク経由で直接増加するウイルスは、平成14年から翌年にかけていろいろな種類が発生した結果として、感染経路に占める割合が増加したと考えられる。

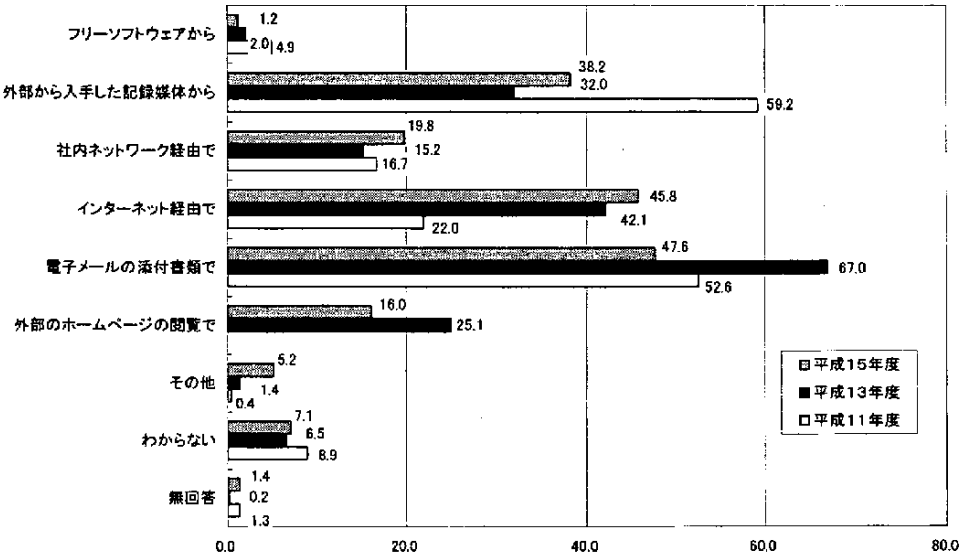



図2－7－2. 主要なウイルス感染原因(経路)

Q56. コンピュータウイルスに対してどのような対策を実施していますか。現在実施している対策を選んで下さい。(複数回答)

| 回答件数 | | 605 | - |
|---|---|---|---|
| 1 | コンピュータウイルス被害を受けた場合のIPAへの相談 | 28 | 4.6 |
| 2 | ウイルス対策用のマニュアル(セキュリティ対策基準に入れた場合も含む)の作成 | 188 | 31.1 |
| 3 | ウイルス対策チーム(社内でウイルスが検出された時の対応を行うチーム)の設置 | 141 | 23.3 |
| 4 | ウイルス検出時や緊急対応と連絡体制の整備 | 277 | 45.8 |
| 5 | ソフトウェアの出所の確認 | 95 | 15.7 |
| 6 | 記録媒体のウイルスチェックの実施 | 276 | 45.6 |
| 7 | ライトプロテクト、バックアップ等のソフトウェア管理 | 65 | 10.7 |
| 8 | PCでのワクチンソフト(ウイルス検出ソフトを含む)の利用 | 524 | 86.6 |
| 9 | PCのワクチンソフト・パラメータファイルを定期的に更新 | 454 | 75.0 |
| 10 | サーバ機でのワクチンソフトの利用 | 433 | 71.6 |
| 11 | メール用ゲートウェイ／サーバでのワクチンソフトの利用 | 377 | 62.3 |
| 12 | メール用ゲートウェイ／サーバでの添付ファイルの制限(例:実行ファイル削除) | 138 | 22.8 |
| 13 | ワクチンソフトの集中監視 | 273 | 45.1 |
| 14 | 定期的な集中監視ログの解析 | 103 | 17.0 |
| 15 | パスワードの変更等、アクセスコントロールの強化 | 92 | 15.2 |
| 16 | 動作の定期的な確認等、異常発見体制の整備 | 66 | 10.9 |
| 17 | 緊急時の電子メールサーバの停止 | 134 | 22.1 |
| 18 | 緊急時の社員への連絡(ウイルス警告の放送／送付) | 263 | 43.5 |
| 19 | OSの修正プログラムの適用(アップデートを含む) | 346 | 57.2 |
| 20 | アプリケーションの修正プログラムの適用(アップデートを含む) | 230 | 38.0 |
| 21 | ウイルス対策サービスの利用 | 108 | 17.9 |
| 22 | その他 | 3 | 0.5 |
| 23 | 特に対策を講じていない | 13 | 2.1 |
| 無回答 | | 6 | 1.0 |

コンピュータウイルスへの有効な対策として、PC への「ワクチンソフトの導入」がある。この数値は、前回調査の 84.8%から今回の 86.6%とほとんど変っていない。導入していない 13.4%の事業体は、早急に導入を行うべきである。

また、メール経由で感染するウイルスが依然として多い現状を反映して、「メール用ゲートウェイ／サーバでのワクチンソフトの利用」は、前回調査の 44.3%から 62.3%へと大きく増加した。PC へのワクチンソフトの導入を行っていない事業体は、このメール用ゲートウェイ／サーバでの集中チェックを行っていると思われるが、メール以外の感染メカニズムを持ったウイルスも多いので、PC への導入も必須である。

ワクチンソフトがウイルスを検出するために使用するパラメータファイル（ワクチンベンダによりパターンファイル、シグニチャファイルとも呼ばれる。）は、最新のものを使用しないと新しいウイルスを検出することができない。この重要性は、近年のネットワーク経由で感染速度の非常に早いウイルスが発生した時に大きくクローズアップされた。そして、パラメータファイルを「定期的に更新している」割合は、前回調査の 67.1%から 75.0%へと増加した。この結果、「ワクチンソフトを利用しているが定期的に更新していない」事業体が 17.7%から 11.6%と大きく減

少した。また、このパラメータファイルの更新を確実に行うにはワクチンソフトを集中管理しないと難しいが、「ワクチンソフトの集中管理を実施している」事業体は、前回調査の 29.1%から 45.1%へと大幅に増加した。しかし、依然として 29.9%の事業体がパラメータファイルの定期的な更新は行っているが集中管理を行っていない。集中管理を行わないと定期的な更新の洩れや新種ウイルスに対する緊急時対応に問題が残る。最近の OS やアプリケーションのセキュリティホールを悪用するウイルスの発生を反映して今回追加した「OS／アプリケーションの修正プログラムの適用」は、それぞれ 57.2%、38.0%と高い数値となった。

コンピュータウイルスの被害を防ぐためには、ワクチンの利用といった技術面と共にウイルス対策についての組織的な対応が重要である。たとえば、自社のウイルス対策用マニュアルの作成、ウイルス対策チームの設置、緊急対応と連絡体制の整備が必要となる。しかし、これらの対応の実施率は低く、今回調査では「マニュアルの作成」が 31.1%（前回 27.6%）、「対策チームの設置」が 23.3%（前回 23.4%）、「緊急対応と連絡体制の整備」が 45.8%（前回 40.7%）と前回調査とあまり変らなかった。この大きな原因の一つにこういった対策を実施する要員が不足していることがあり、「外部のウイルス対策サービスの利用」も前回調査の 14.8%から 17.9%へと大きく増加した。この傾向は、今後も継続していくと考えられる。

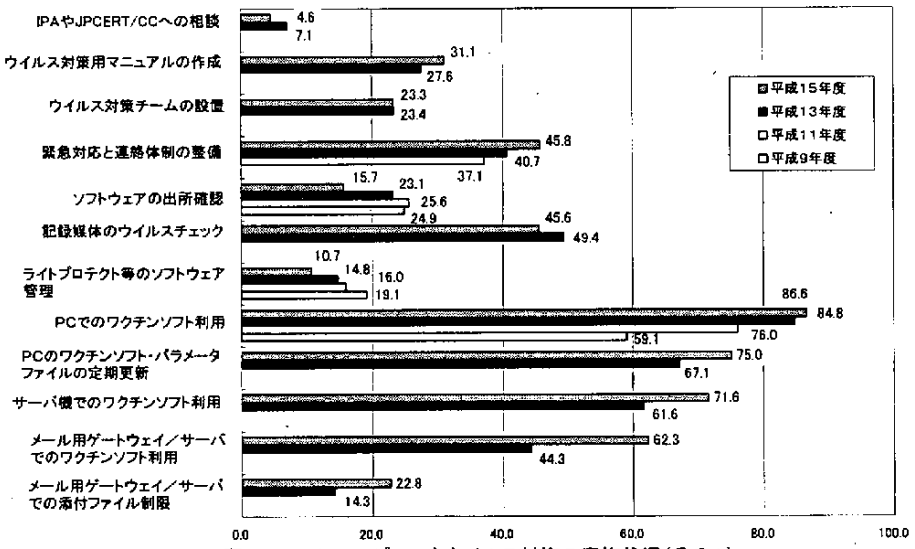



図2－7－3. コンピュータウイルス対策の実施状況（その1）

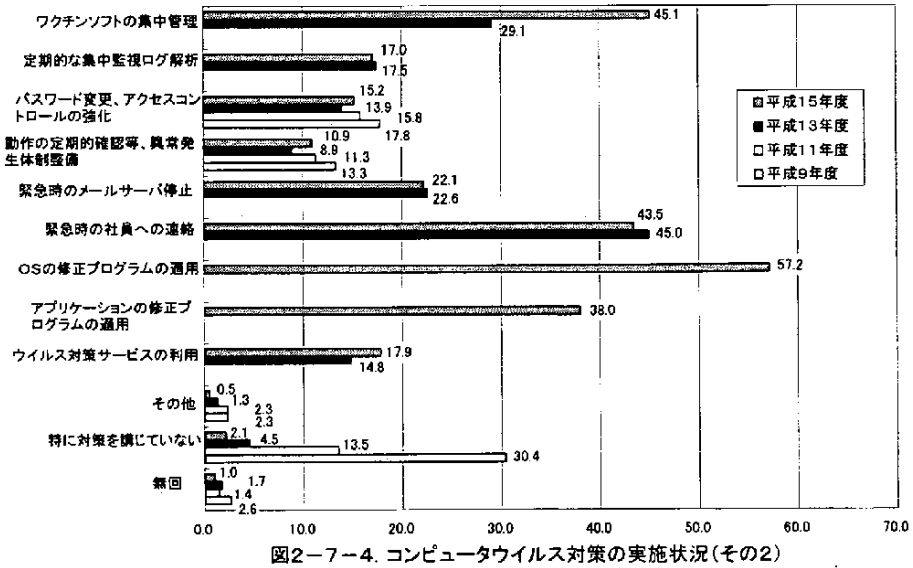



図2－7－4. コンピュータウイルス対策の実施状況（その2）

## 2.8 アウトソーシングについて

Q57. 貴事業体では運用に関し、アウトソーシングを利用していますか。

| | | | |
|---|---|---|---|
| 1 | 利用している | 300 | 49.6 |
| 2 | 利用していない　⇒Q60 へ | 300 | 49.6 |
| 無回答 | | 5 | 0.8 |
| 計 | | 605 | 100.0 |

今回調査では初めて運用のアウトソーシングについての質問を行った。各事業体のアウトソーシング利用率は 49.6%となり、半数の事業体が運用のアウトソーシングを利用している。もちろん、この割合は資本金が大きくなるにつれて急上昇し、資本金 100 億円以上となると 80%以上の企業がアウトソーシングを利用している。

なお、業種グループ別にみると、最も利用率が高いのは金融・保険業で 74.3%、次いで政府・地方公共団体で 64.8%がアウトソーシングを利用している。

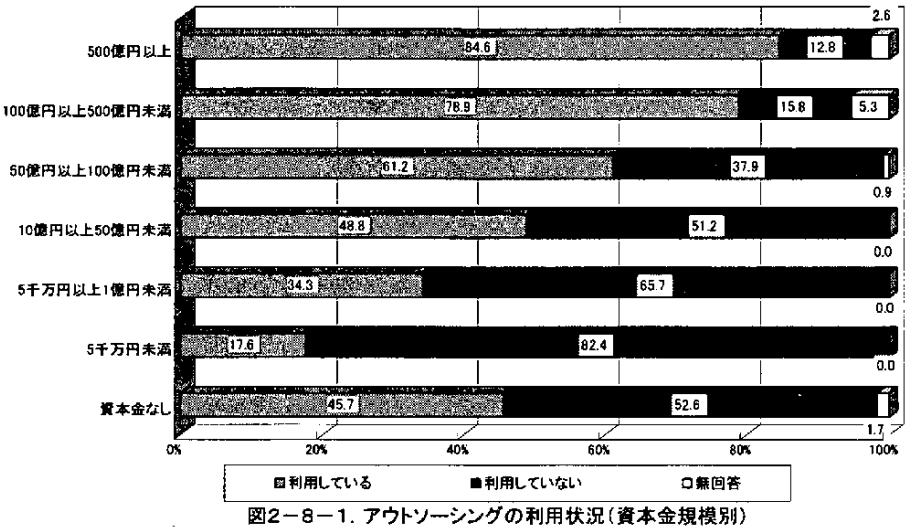



図2－8－1. アウトソーシングの利用状況（資本金規模別）

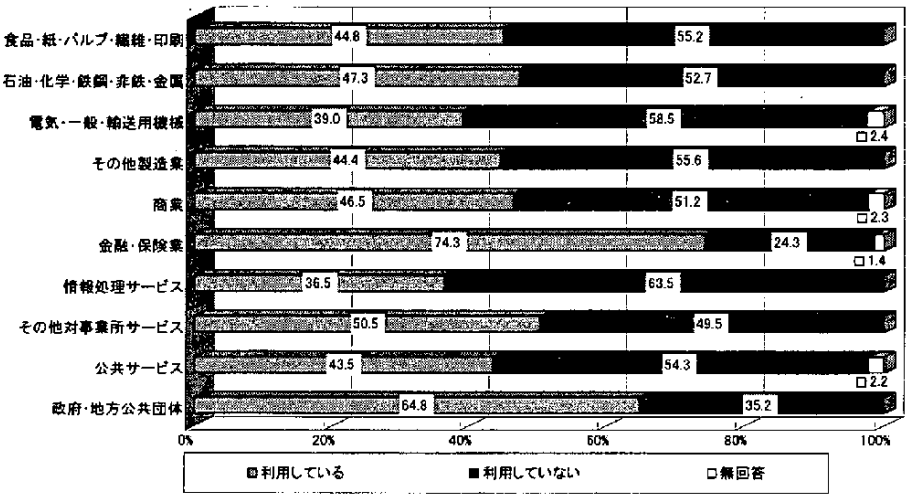



図2－8－2. アウトソーシングの利用状況（業種グループ別）

Q58. （Q57で「1」と回答した場合）アウトソーシング先を選定する場合、どのような観点から選定していますか。（複数回答）

| 回答件数 | | 300 | - |
|---|---|---|---|
| 1 | コスト | 201 | 67.0 |
| 2 | 専門性 | 188 | 62.7 |
| 3 | セキュリティ | 126 | 42.0 |
| 4 | 品質（サービスレベル） | 183 | 61.0 |
| 5 | 開発を依頼した会社をそのままメンテナンス先に選定 | 53 | 17.7 |
| 6 | その他 | 13 | 4.3 |
| 無回答 | | 11 | 3.7 |

運用のアウトソーシング先を選定する時に重視している評価項目については、コスト、専門性、品質の3項目が重視されているというあたり前のことが確認された。しかし、「セキュリティ」についても42.0%と高い数字となり、情報システム子会社を含むアウトソーサもセキュリティへの対応が必要なことを示している。

Q59. アウトソーシング先との契約において情報セキュリティ関係で重視している項目はどれですか。（複数回答）

| 回答件数 | | 300 | - |
|---|---|---|---|
| 1 | セキュリティポリシー | 73 | 24.3 |
| 2 | 社員の教育体制 | 69 | 23.0 |
| 3 | 守秘義務契約 | 216 | 72.0 |
| 4 | サービスレベル（業務中断時間） | 142 | 47.3 |
| 5 | ウイルス対策 | 77 | 25.7 |
| 6 | 不正アクセス対策 | 94 | 31.3 |
| 7 | 火災、災害対策 | 75 | 25.0 |
| 8 | 入退室、侵入対策 | 94 | 31.3 |
| 9 | 機械事故対策 | 63 | 21.0 |
| 10 | オペレーションミス対策 | 77 | 25.7 |
| 11 | 事故後の早期復旧対策 | 110 | 36.7 |
| 12 | 認証制度の取得 | 24 | 8.0 |
| 13 | 監査など内部統制対策 | 28 | 9.3 |
| 14 | 委託元による監査の実施 | 26 | 8.7 |
| 15 | 賠償責任 | 39 | 13.0 |
| 16 | その他 | 2 | 0.7 |
| 無回答 | | 10 | 3.3 |

運用のアウトソーシングを行う場合、アウトソーサとの契約において情報セキュリティ関連で重視している項目について質問した。この質問では『契約において』としたために、方針や原則といった包括的な項目に回答が集中した傾向があると考えられるが、一番高かったのは「守秘義務契約」の72.0%であった。この質問は運用のアウトソーシングを行っている事業体のみが答えているので、28.0%の事業体は守秘義務契約を行わずに運用のアウトソーシングを行っていることに

なり、早急な改善が必要である。

次に重視しているのは「サービスレベル」で47.3%であった。これは発注者とアウトソーサ間で、サービスレベルアグリーメント(SLA)を結び、提供されたサービスの可視化をはかる動きが一般化しつつあることを示している。ITコーディネータ協会をはじめ、各団体もSLAの雛型を作り、公開しているので、今後各事業体はSLAをあたり前のものとして結んでいくと考えられる。また、このSLAが守れなかった時の「賠償責任」も13.0%の事業体が定めており、これまでの曖昧な契約関係が欧米型の権利義務関係を明確にし、それに応じた結果責任を負う欧米型の契約に近づきつつあることを示している。

運用をアウトソーシングする場合、情報システム部門が経営者やユーザ部門から念を押されるのは、万が一の事故があった場合に適切な対応が取れるか否かである。これを反映して、アウトソーサとの契約においても「事故後の早期復旧対策」について36.7%の事業体が定めている。

一方、「セキュリティポリシー」が24.3%、「社員の教育体制」が23.0%といったように、セキュリティ管理の関わるところはあまり高くない数値である。これらの項目は、契約にはあまり盛り込まれていないが、少なくともセキュリティポリシーについては自社のセキュリティポリシーに従ったシステム運用を担保するのが発注者側の情報システム部門の責任であり、Q10でセキュリティポリシーを定めている割合が52.2%であることを考慮しても、半数近くの事業体が自社のセキュリティポリシーが適用される保証を得ていないことは問題である。

ウイルス対策等のセキュリティに関する一連の対策は、その内容によっては発注者側が提供している場合も多いので、アウトソーサとの作業内容定義に包含される場合も多く、アウトソーシング契約の内容としては重視されなかったと考えられる。

また、「認証の取得」や「監査等のモニタリング」に関わる項目は、8.0%～9.3%と低かった。通常、これらの項目も契約よりはSLA等に含まれる場合が多いことも影響していると考えられる。特に、日本企業ではQ10のシステム監査の実施率が30.1%と低いことも、これらの数字を低くしている原因であろう。

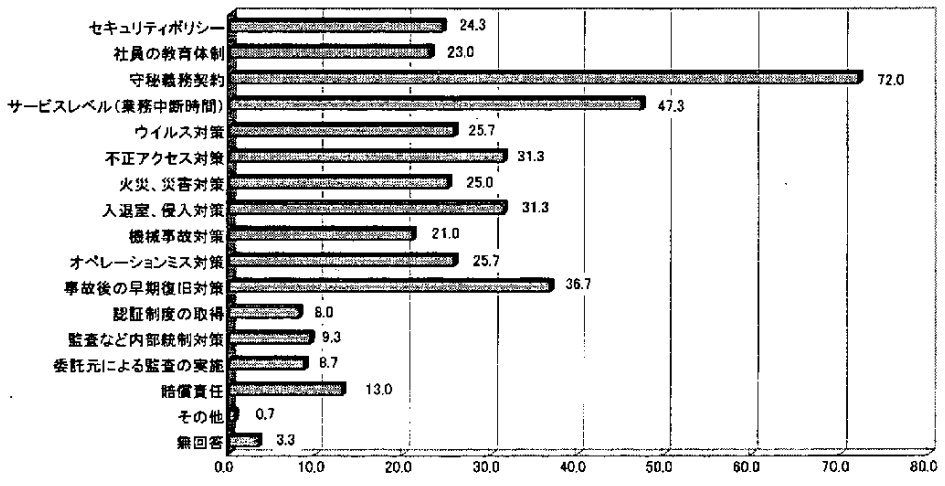



図2－8－3. アウトソーシング契約でのセキュリティ重視項目

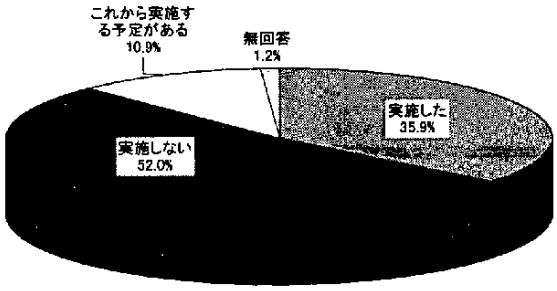
## 2.9 システム監査・情報セキュリティ監査について

Q60. 過去2年以内にシステム監査を実施したことがありますか。（業務監査に含まれている場合を含む）

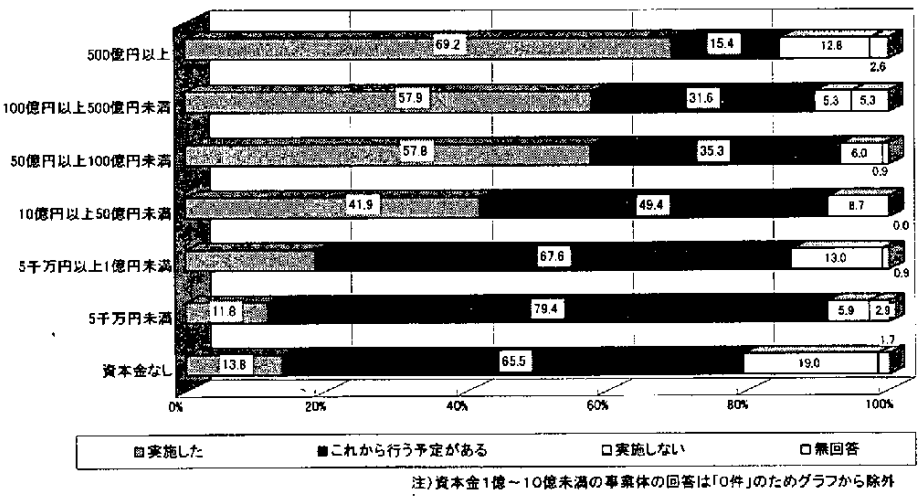
| | | | |
|---|---|---|---|
| 1 | 実施した(実施中を含む) | 217 | 35.9 |
| 2 | 実施しない ⇒Q62 へ | 315 | 52.1 |
| 3 | これから実施する予定がある ⇒Q63 へ | 66 | 10.9 |
| 無回答 | | 7 | 1.2 |
| 計 | | 605 | 100.0 |

システム監査の実施率は35.9%で、前回調査の34.8%と比べてもほとんど増えておらず、依然として3分の1を超えた程度であり、企業などへの浸透が十分でないことがわかる。ただし、資本金規模でみると、100億円以上の企業では60%近くの実施率である。しかし1億円未満では実施率は20%以下と大きく二極分化していることがわかる。

業種グループ別にみると金融・保険業がシステム監査を実施している割合が前回調査（65.9%）同様62.2%と一番高く、次に情報処理サービス業で45.9%（前回56.8%）となっている。その他の設問同様、この二つの業種が情報システムに関するリスクへの関心度が高い。一方、システム監査の実施率が低い業種は公共サービスの15.2%（前回5.9%）、政府・地方公共団体の13.0%（前回5.3%）であり、前回と比べると改善したものの、依然として低いレベルにある。公共性を求められるこの二つの業種できわめて低いのは問題であり、早急の改善が必要と考えられる。




2-9-1. システム監査の実施状況




注）資本金1億～10億未満の事業体の回答は「0件」のためグラフから除外

図2-9-2. システム監査の実施状況（資本金別）

Q61. （Q60 で「1」と回答した場合）システム監査を実施した結果、どのような点に効果があったと思いますか。（複数回答）

| 回答件数 | | 217 | - |
|---|---|---|---|
| 1 | システムに起因する事故・障害が未然に防止できた | 22 | 10.1 |
| 2 | リスク対策をどこまで考慮すればよいかが明らかになった | 77 | 35.5 |
| 3 | 担当者がリスクを考慮しながら業務を実行するようになった | 84 | 38.7 |
| 4 | システム部門に対する過大な要求がなくなった | 1 | 0.5 |
| 5 | システムの信頼性向上対策のレベルが明らかになった | 72 | 33.2 |
| 6 | システムの有効利用が促進された | 23 | 10.6 |
| 7 | システムの効率性が確保できた | 21 | 9.7 |
| 8 | 有効なシステムの開発設計が可能になった | 4 | 1.8 |
| 9 | 業務の継続性の確保が図られた | 25 | 11.5 |
| 10 | 要員が規定・ルール等を意識して業務を実行するようになった | 84 | 38.7 |
| 11 | その他 | 9 | 4.1 |
| 12 | 効果は得られなかった | 21 | 9.7 |

システム監査を実施した事業体に対しシステム監査の効果について調査した。この質問は今年度初めて行ったものであり、効果としては「担当者がリスクを考慮しながら業務を実行するようになった」および「要員が規定・ルール等を意識して業務を実行するようになった」が 38.7%で同率であった。さらに、「リスク対策をどこまで考慮すればよいかが明らかになった」が 35.5%、「システムの信頼性向上対策のレベルが明らかになった」が 33.2%であった。共通する点としては、リスクへの認識、対策、信頼性などの従業員の意識改革につながる点が大きいことがわかる。しかし、リスクに対する意識改革は情報セキュリティ監査とも共通するものであり、システム監査ならではの点としては信頼性対策など限られている。今後は情報セキュリティ監査とシステム監査が並行することになるので、両者の監査の視点の違いを明確にする必要がある。

システム監査基準では特に情報システムの構築の企画・開発・運用・保守のライフサイクルでの信頼性・効率性・有効性の点で情報セキュリティ監査と一線を画しており、この観点からは「システムの効率性が確保できた」、「有効なシステムの開発設計が可能になった」での効果が低い点が危惧される。今後、システム監査として情報セキュリティ監査との違いを明確にしながら進めていくことが重要であろう。

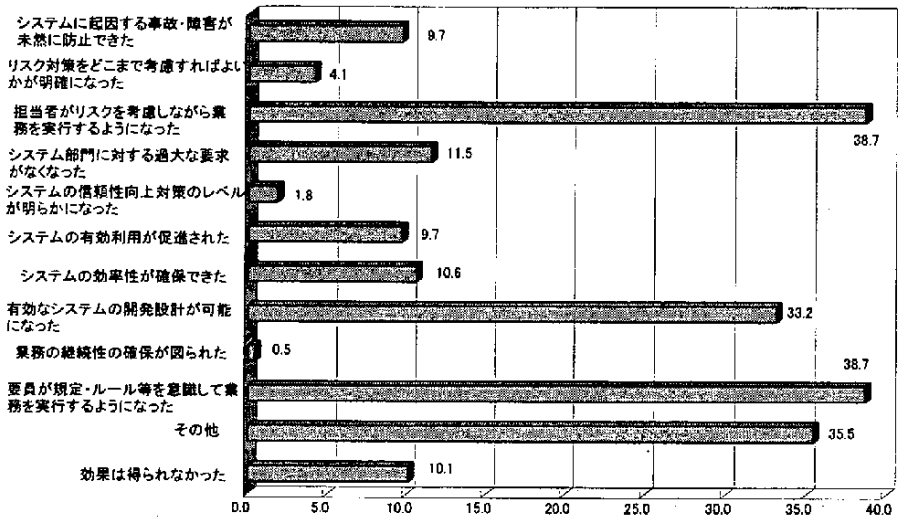



図2－9－3. システム監査実施による効果

Q62.（Q60で「2」と回答した場合）システム監査を実施していない理由は何ですか。（複数回答）

| 回答件数 | | 315 | - |
|---|---|---|---|
| 1 | 経営者層が重要性を認識していないため | 45 | 14.3 |
| 2 | システム監査実施のためのコンセンサス、組織風土が十分に備わっていない | 123 | 39.0 |
| 3 | システム監査の実施よりもシステム化推進そのものに力点がある | 92 | 29.2 |
| 4 | システム監査の方法、制度、手続きなどが十分ではない | 110 | 34.9 |
| 5 | 効果が明確でない | 98 | 31.1 |
| 6 | 適切なシステム監査人が見つからない | 48 | 15.2 |
| 7 | アウトソーシングしているため | 16 | 5.1 |
| 8 | その他 | 15 | 4.8 |
| 無回答 | | 15 | 4.8 |

システム監査を実施していない理由として、「システム監査実施のコンセンサス、組織風土が十分に備わっていない」が前回調査（39.1%）とほぼ同様の39.0%であり、全体の約4割を占めている。金融・保険業、情報処理サービス業などを除く一般の業種では、情報システムの企業経営への影響度が企業の中で比較的小さい場合は、なかなかその重要性が理解されないものと思われる。そのため、情報システムの枠のなかでも「システム監査の実施よりもシステム化推進そのものに力点がある」29.2%（前回30.5%）、「効果が明確でない」31.1%（前回27.0%）などの意見が生じ、開発優先の一般的な風潮のなかに埋没していると考えられる。今後、システム監査基準が改定され、情報セキュリティ監査制度とあいまって、発展することが望まれる。

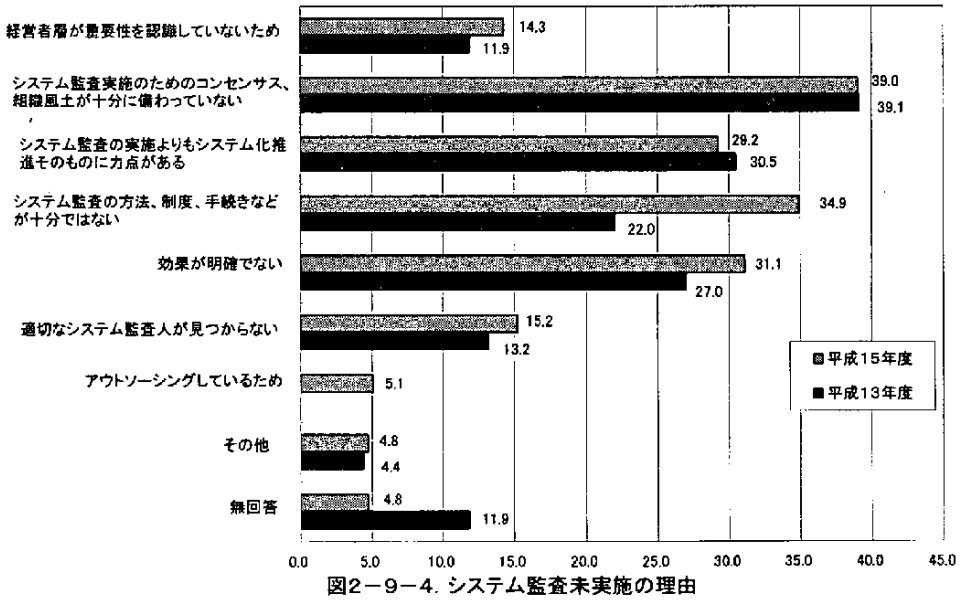


図2－9－4. システム監査未実施の理由

Q63. 情報セキュリティ監査を実施したことがありますか。（業務監査に含まれている場合を含む）

| 1 | 実施した | 110 | 18.2 |
|---|---|---|---|
| 2 | これから行う予定がある | 122 | 20.2 |
| 3 | 実施しない | 359 | 59.3 |
| 無回答 | | 14 | 2.3 |
| 計 | | 605 | 100.0 |

情報セキュリティ監査は平成 15 年４月に制度が告示された新しい制度である。今まではシステム監査の一部として実施されていたり、侵入検査（ペネトレーションテスト）として実施されてきた内容である。今回の調査では、システム監査の実施比率である 35.9%よりも高いと考えてきた。しかし、実態は 18.2%と約半分であった。「これから行う予定がある」を含めても 38.4%と低い。さらに、「実施しない」との回答が 59.3%となっている。せっかく制度ができたのに、実施率が低いことや「実施しない」との回答がこの比率となっているのは問題である。

なお、資本金別にみた実施率では、資本金が 300 億円を超える大企業が 48.7%となっているほかは実施率がきわめて低い。資本金が 30 億円の以下の事業体では「実施しない」が 50%を超えている。今後、情報システム監査の実施にあたって何らかの促進策が必要と考えられる。

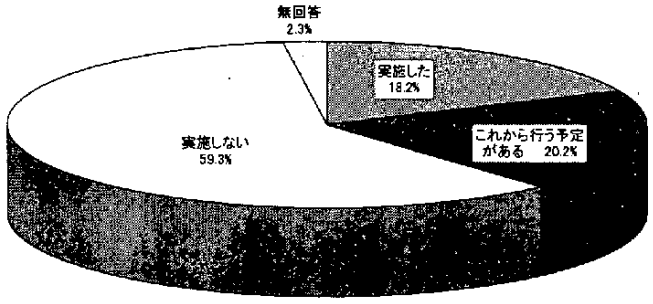
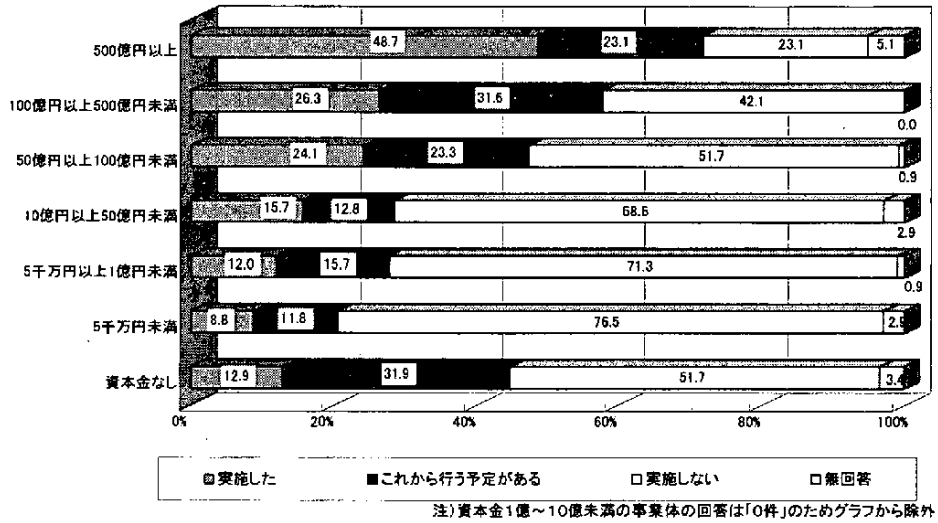



図2－9－5. 情報セキュリティ監査の実施状況




注）資本金1億～10億未満の事業体の回答は「0件」のためグラフから除外

図2－9－6. 情報セキュリティ監査の実施状況（資本金別）

なお、システム監査と情報セキュリティ監査の実施状況を比較すると、実施した事業体の比率ではシステム監査が 35.9%と情報セキュリティ監査の 18.2%を大きく引き離している。これは、情報セキュリティ監査制度が発足してからまだ日が浅いこと、また、監査を実施する主体が十分に機能していないためと考えられる。しかし、情報セキュリティ監査は多くの事業体にとってシステム監査よりも希求の課題となっていることから、近くシステム監査と情報セキュリティ監査の立場が変わるのも時間の問題と考えられる。今後、システム監査と情報セキュリティ監査の違いを明確にしていく必要がある。

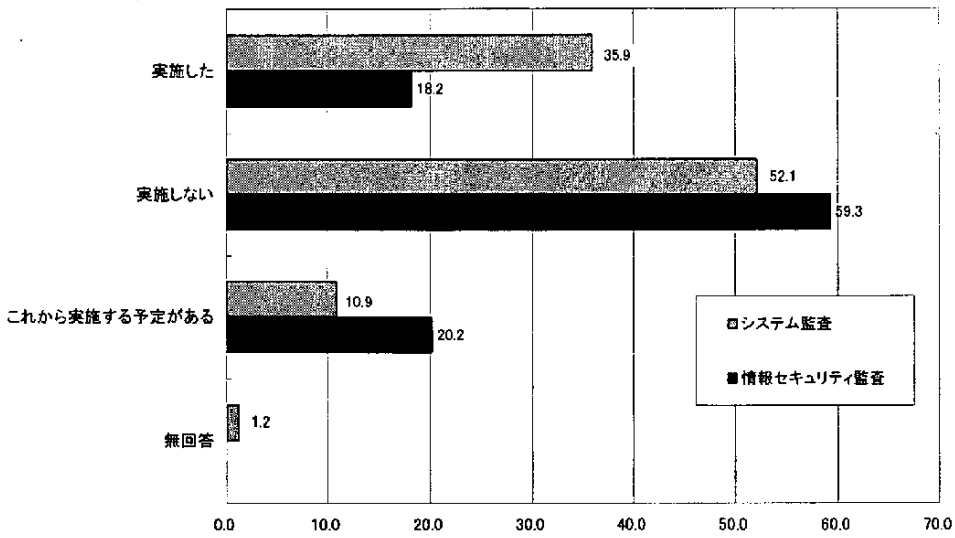



図2－9－7. システム監査および情報セキュリティ監査の実施状況

Q64. （Q63で「3」と回答した場合）情報セキュリティ監査を実施していない理由は何ですか。（複数回答）

| 回答件数 | | 359 | － |
|---|---|---|---|
| 1 | 経営者層が重要性を認識していないため | 42 | 11.7 |
| 2 | 情報セキュリティ監査実施のためのコンセンサス、組織風土が十分に備わっていない | 153 | 42.6 |
| 3 | 情報セキュリティ監査制度をよく知らない | 92 | 25.6 |
| 4 | 情報セキュリティ監査の方法、手続きなどが十分ではない | 108 | 30.1 |
| 5 | 効果が明確でない | 98 | 27.3 |
| 6 | 適切な情報セキュリティ監査企業・監査人が見つからない | 25 | 7.0 |
| 7 | 情報セキュリティマネジメントシステム(ISMS)の認証を取得しているため、不要である | 4 | 1.1 |
| 8 | その他 | 16 | 4.5 |
| 無回答 | | 35 | 9.7 |

情報セキュリティ監査を実施していない理由として、「情報セキュリティ監査実施のためのコンセンサス、組織風土が十分に備わっていない」が42.6%と高い。これは、システム監査を実施していない理由の「システム監査実施のコンセンサス、組織風土が十分に備わっていない」（39.1%）とほぼ共通する傾向である。これに続く理由としては、「情報セキュリティ監査の方法、手続きなどが十分ではない」が30.1%である。これは、情報セキュリティ監査制度が平成15年4月に運用を開始したばかりであり、一般の事業体にとってはどのように実施してよいのか不明な点が多いという不安によるものであろう。これは、監査制度が完備しても事業体にとってはシステム監査制度との違いが不明であり、「効果が明確でない」と27.3%が答えていることにみられるようにコストがかかる方向でしかないという後ろ向きの姿勢も読みとれる。今後、情報セキュリティ監査制度の内容、効果などについて一層のPR、啓蒙活動が必要であると考える。

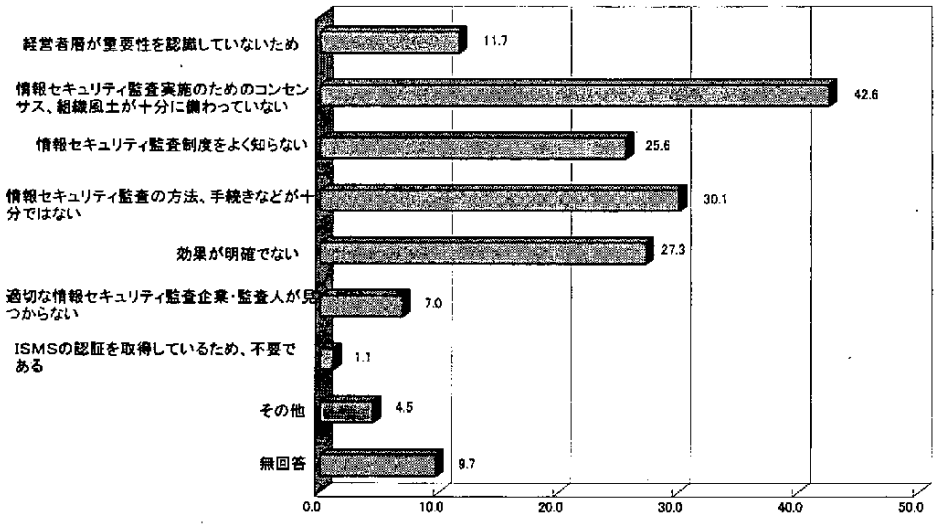



図2－9－8. 情報セキュリティ監査を実施しない理由

## 2.10 個人情報保護について

Q65. 貴事業体ではどのような個人情報を取り扱っていますか。(複数回答)

| 回答件数 | | 605 | - |
|---|---|---|---|
| 1 | 売買等契約の履行 | 195 | 32.2 |
| 2 | 顧客サポート | 245 | 40.5 |
| 3 | 代金等の回収 | 190 | 31.4 |
| 4 | 情報提供 | 127 | 21.0 |
| 5 | マーケティング | 120 | 19.8 |
| 6 | 商品開発 | 77 | 12.7 |
| 7 | 行政サービスの履行 | 66 | 10.9 |
| 8 | 委託(受託)処理 | 110 | 18.2 |
| 9 | 従業員情報(雇用に関わる届出情報(採用時を含む)、給与、保険関係、健康診断結果、退職者情報等) | 499 | 82.5 |
| 10 | その他 | 34 | 5.6 |
| 無回答 | | 17 | 2.8 |

各事業体の個人情報の取扱いについては、「従業員情報の管理」(82.5%)が最も多く、次いで「顧客サポート」(40.5%)、「売買契約の履行」(32.2%)、「代金等の回収」(31.4%)となった。

前回調査では、個人情報の利用目的についての質問であり、事業体が保有する情報を二次的に「利用」する場合と、管理から利用までの「取扱い」の意味合いの違いから、単純に比較はできないが、「従業員情報」(前回調査では「従業員の管理(インハウス情報)」で、前回調査の57.1%から82.5%へと、25.4ポイント増加した。しかし、「従業員情報の管理」は本来100%になるはずであり、約2割の事業体が必ずしも従業員情報が個人情報であることを認識していないことがわかる。

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

業種グループ別にみると、金融業・保険業はいずれも高い割合を占めしているが、その中で特に高いのは「顧客等サポート」(68.9%)、「売買等契約の履行」(66.2%)となっている。業務の性質上、情報処理サービス業は「委託(受託)処理」(77.0%)、政府・地方公共団体は「行政サービスの履行」(88.9%)の割合が他の業種と比べ圧倒的に高い。

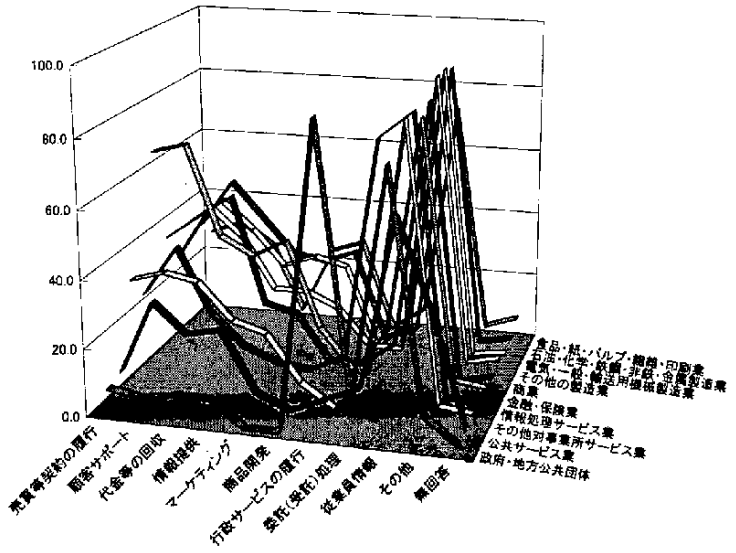


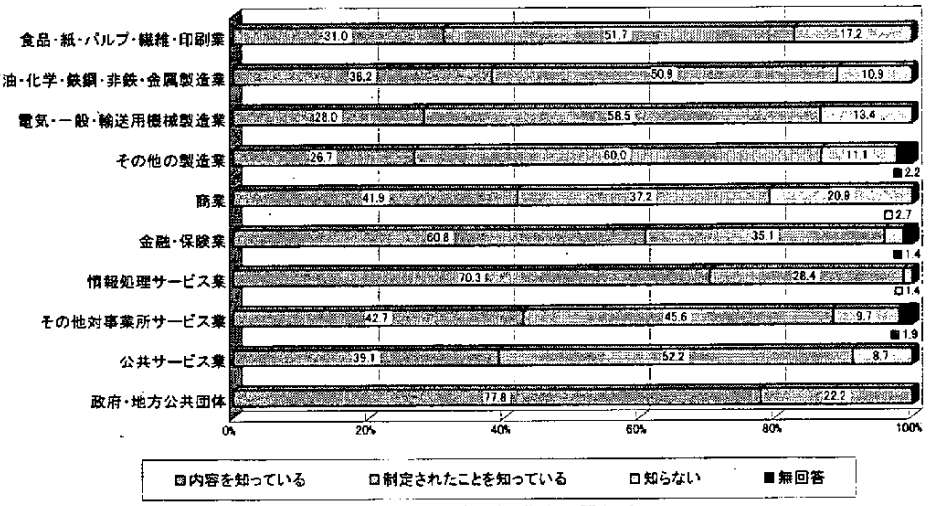

図2－10－1. 個人情報の利用目的(業種グループ別)

Q66.「個人情報の保護に関する法律（平成15年5月30日法律第57号)」を知っていますか。

| | | | |
|---|---|---|---|
| 1 | 内容を知っている | 284 | 46.9 |
| 2 | 制定されたことを知っている | 264 | 43.6 |
| 3 | 知らない | 53 | 8.8 |
| 無回答 | | 4 | 0.7 |
| 計 | | 605 | 100.0 |

個人情報保護法は平成15年5月に公布され、「第4章　個人情報取扱事業者の義務等」～「第6章　罰則」を除く他の規程は同日から施行されているが、約9割が法律の存在を認知している。

業種グループ別にみると、業務上、個人情報の取扱いが多い第三次産業（サービス業）が製造業グループに比べ、認知度が高い。特に、政府・地方公共団体は「知らない」との回答は0件、情報処理サービス業、金融・保険業でも1～2割であった。




2-10-2. 個人情報保護法の認知度

Q67. 個人情報保護法が施行されるまでに、どのような対応策を講じますか。

| | | | |
|---|---|---|---|
| 1 | 社内にプロジェクトを立ち上げて管理体制を見直し、必要な対策を講じる予定であ | 64 | 10.6 |
| 2 | 外部コンサルタントに委託して管理体制を見直し、必要な対策を講じる予定である | 13 | 2.1 |
| 3 | すでに対応策を講じる準備を開始している | 45 | 7.4 |
| 4 | プライバシーマークの認証を受けて対応を済ませている | 40 | 6.6 |
| 5 | 個人情報保護のための規程を整備している | 162 | 26.8 |
| 6 | その他 | 64 | 10.6 |
| 7 | 現状の管理体制で十分なので、特に何も対応策を講じない | 163 | 26.9 |
| 無回答 | | 34 | 5.6 |
| 複数回答 | | 20 | 3.3 |
| 計 | | 605 | 100.0 |

個人情報保護法は平成17年4月から施行が予定されているが、「特に対策を講じない」との意見が最も多く、26.8%であった。僅差で、「個人情報保護の規程の整備」が26.8%である。

その他の意見としては、「対策を検討中」、「プライバシーマークの取得準備（申請）中」、「個人情報保護条例の改定」（地方公共団体に限定）などの意見があげられた。

Q68. 現在の個人情報の管理状況についてリスクをどのように認識していますか。

| | | | |
|---|---|---|---|
| 1 | 対応策を講じているので、リスクはないと認識している | 39 | 6.4 |
| 2 | 現状の管理方法で何も問題が発生していないので、リスクはないと認識してい | 108 | 17.9 |
| 3 | 何度かヒヤリ・ハッとした経験があり、リスクがあると認識している | 121 | 20.0 |
| 4 | いつ問題が発生してもおかしくない状況であると認識している | 169 | 27.9 |
| 5 | その他 | 51 | 8.4 |
| 6 | 特に認識していない | 93 | 15.4 |
| 無回答 | | 21 | 3.5 |
| 複数回答 | | 3 | 0.5 |
| 計 | | 605 | 100.0 |

個人情報の管理状況について、「現状で問題がない」、「対応策を講じているためリスクはない」と認識しているのは24.3%である。その一方で、「何らかの問題が発生してもおかしくない」（27.9%）、「ヒヤリとした経験があり、リスクを認識している」（20.0%）との意見が約半数を占めている。昨今、個人情報漏洩事件が多発しているが、窃盗など、悪意による事件のほか、個人情報が入っているPCや搬送時の荷物の紛失など、人的な管理ミスが原因となっているケースも多発している。今後、このようなミスが起こらないよう、個人情報の管理体制を強化すべきである。

Q69. 個人情報保護対策として、現在何を実施していますか。また、今後どういうことを実施する予定ですか。(複数回答)

| 対策 | 現在実施している対策 | | 今後実施を予定している対策 | |
|---|---|---|---|---|
| 回答件数 | 605 | - | 605 | - |
| 管理責任者を置いている(保護体制(役割、責任、権限)を確立する | 218 | 36.0 | 110 | 18.2 |
| 個人情報保護に関する規程を定め運用している | 210 | 34.7 | 145 | 24.0 |
| 個人情報保護のマネジメントシステムを構築して(プライバシーマークの認定を受ける)運用している | 62 | 10.2 | 85 | 14.0 |
| 社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している | 111 | 18.3 | 151 | 25.0 |
| 定期的に監査(内部監査／外部監査)を実施している | 130 | 21.5 | 109 | 18.0 |
| リスク分析を実施して必要な安全対策を構築している | 81 | 13.4 | 135 | 22.3 |
| 苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している | 147 | 24.3 | 64 | 10.6 |
| 仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている | 96 | 15.9 | 108 | 17.9 |
| その他 | 16 | 2.6 | 21 | 3.5 |
| 特に対策を講じない | 178 | 29.4 | 86 | 14.2 |
| 無回答 | 111 | 18.3 | 219 | 36.2 |

現段階で行っている個人情報保護対策として最も多いのは「管理責任者の設置の確立」で36.0%、次いで「個人情報保護規程の策定および運用」が34.7%となっている。一方で、「特に対策を講じない」とする回答が29.4%、と約3割を占めている。

また、今後実施を予定している対策としては、「社員に対する個人情報保護カリキュラムを含めた定期的な教育」(25.0%)、「個人情報保護規程の策定および運用」(24.0%)となった。

●以下、Q70～Q73についてはQ65で「9」のみを選択した事業体は集計の対象外としている。

Q70. 取り扱っている個人情報の収集方法はどのように行っていますか。(複数回答)

| | | | |
|---|---|---|---|
| 回答件数 | | 486 | - |
| 1 | 営業活動(名刺交換、Web、メール、申込書等)により情報主体(当該個人)から直接収集 | 362 | 74.5 |
| 2 | 名簿業者等から購入 | 9 | 1.9 |
| 3 | グループ企業から入手 | 34 | 7.0 |
| 4 | 他社から提供を受ける | 30 | 6.2 |
| 5 | 業務委託契約等に基づき提供を受ける | 88 | 18.1 |
| 6 | 新聞、雑誌等メディアからの収集 | 34 | 7.0 |
| 7 | その他 | 65 | 13.4 |
| 無回答 | | 34 | 7.0 |

「情報主体から直接収集」は前回調査(76.7%)同様、最も多く、74.5%となった。次に多いのは「業務委託契約等による提供」(18.1%←12.5%)であり、前回とほとんど同じ結果となった。

これら直接収集や業務委託による提供については事業形態の影響がみられる。

なお、わずかではあるが「グループ企業からの入手」（7.0%←H13:4.3%）、「他社からの提供」（6.2%←H13:3.8%）というケースが見られる。また、「名簿業者からの購入」（1.9%）については、前回の 2.2%から若干減少した。これらの事業体が個人情報の扱いをどのように行っているのか、立ち入ってみていく必要がある。

Q71.（Q70 で「1」と回答した場合）情報主体から直接に収集する場合、収集・利用目的について同意を取っていますか。

| | | | |
|---|---|---|---|
| 1 | はい | 167 | 46.1 |
| 2 | いいえ | 44 | 12.2 |
| 3 | わからない | 107 | 29.6 |
| 無回答 | | 44 | 12.2 |
| 計 | | 362 | 100.0 |

個人情報の収集に関しては、46.1%が同意をとっているが、前回調査（59.1%）に比べ、13 ポイント減少した。「取っていない」との回答は 21.6%から 12.2%と、9ポイント減少した。

Q72.（Q70 で「1」と回答した場合）個人情報を個人から直接に収集する場合、利用目的を通知して同意を取ることについてどう考えますか。

| | | | |
|---|---|---|---|
| 1 | 当然必要である | 239 | 66.0 |
| 2 | 同意を取る手続きが困難で、業務遂行に大きな影響を及ぼすために対応できな | 19 | 5.2 |
| 3 | 個人と取引を遂行するうえで、暗黙のうちに個人が同意しているはずであるから必要ない | 30 | 8.3 |
| 4 | 個人が積極的に提供しているのだから、改めて同意を取る必要性を感じない | 14 | 3.9 |
| 5 | もともと意識のない個人に改めて同意を取ることの意味がない | 2 | 0.6 |
| 6 | 個人から苦情を申し立てられるような利用をしていないので、必要と思わない | 12 | 3.3 |
| 無回答 | | 43 | 11.9 |
| 複数回答 | | 12 | 3.3 |
| 計 | | 362 | 100.0 |

個人情報を情報主体から直接収集する場合に同意をとっているかを調査したところ、「当然必要である」との回答が圧倒的に多く、66.0%であった。一方で、「暗黙のうちに個人が同意しているから必要ない」（8.3%）と「個人が積極的に提供しているから改めて同意をとる必要がない」（3.9%）をあわせると、約1割が同意を必要としないと考えている。

Q73.（Q70で「2」～「6」と回答した場合）間接的に収集する場合、収集・利用目的についてどのような対応を行っていますか。

| | | | |
|---|---|---|---|
| 1 | 情報主体から利用に関し、改めて同意を取っている | 20 | 14.0 |
| 2 | 情報主体が他社への提供について同意していることを情報提供者(入手先)に確認している | 51 | 35.7 |
| 3 | 何もしていない | 40 | 28.0 |
| 無回答 | | 30 | 21.0 |
| 複数回答 | | 2 | 1.4 |
| 計 | | 143 | 100.0 |

間接収集の際に情報主体から同意を取り直しているとの回答は14.0%と前回調査（17.4%）とあまり変化はみられなかった。

一方、「入手先に提供について同意しているかを確認している」との回答は前回調査（18.5%）から35.7%と12.7ポイントと大幅に増加した。しかしながら、「何もしていない」が28.0%（前回27.4%）あるのは問題である。情報主体の関知しないところで情報が一人歩きすることのないよう、間接収集であってもきちんと情報主体の同意を得るべきである。「個人情報保護法　第4章（5）第三者提供の制限（23条））では、「本人の同意を得ない個人データの第三者提供の原則禁止」がうたわれていることから、事業者はきちんとした対応をとる義務が生じることになる。

Q74. 個人情報を外部委託する場合に交わす契約条項には何がありますか。(複数回答)

| | | | |
|---|---|---|---|
| 回答件数 | | 605 | - |
| 1 | 秘密保持義務 | 339 | 56.0 |
| 2 | 責任分担(漏洩事故発生時の損害賠償　等) | 153 | 25.3 |
| 3 | 個人情報の適正な管理(廃棄、返却、授受等) | 241 | 39.8 |
| 4 | 目的外使用・再委託禁止 | 253 | 41.8 |
| 5 | その他 | 9 | 1.5 |
| 6 | 外部委託を行っていない | 199 | 32.9 |
| 無回答 | | 45 | 7.4 |

回答について特に問題と考えられることはない。「秘密保持義務」(56.0%←H13:41.7%)、「個人情報の適切な管理」(39.8%←H13:24.7%)など、いずれも前回調査と比べ約15ポイントの増加となった。今回選択肢に追加した「目的外使用・再委託禁止」も41.8%と高い割合を示しており、外部委託先の個人情報の取扱いには十分な配慮がなされていると考えられる。

外部委託を行っていない事業体は前回の42.2%から32.9%と約10ポイントの減少となった。

業種グループ別にみると、製造業では約4割が外部委託を行っていないのに対し、政府・地方公共団体（3.7%）や金融・保険業（12.2%）では個人情報の管理を外部委託している。

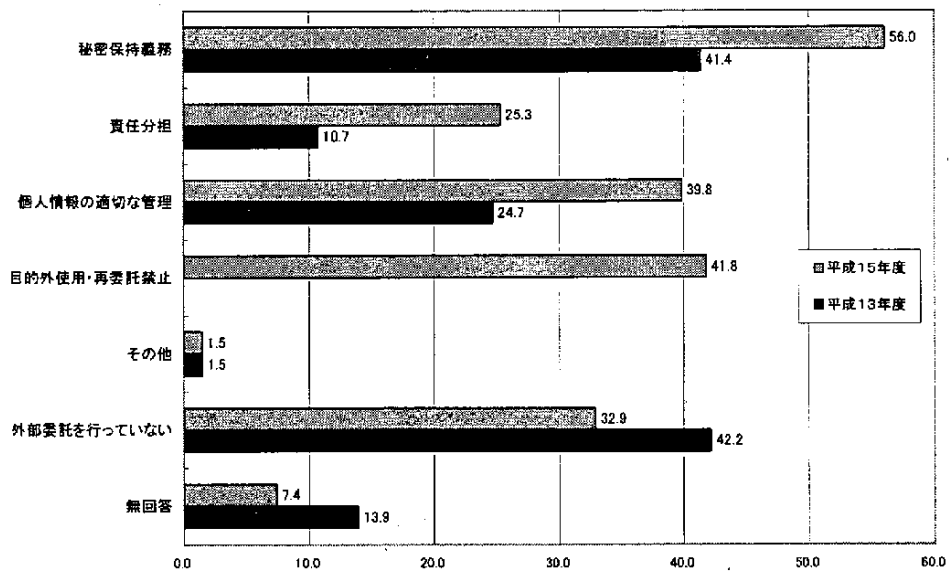



図2－10－3. 個人情報を外部委託する際の契約条項

Q75. 個人情報保護への対応策としてプライバシーマークの認定を受けることが有効だと思いますか。

| | | | |
|---|---|---|---|
| 1 | 社内の管理体制(コンプライアンス・プログラム)が構築できて有効である | 190 | 31.4 |
| 2 | 有効であるが事業者にとっては負担が重い | 271 | 44.8 |
| 3 | 有効とは思わない | 56 | 9.3 |
| 無回答 | | 87 | 14.4 |
| 複数回答 | | 1 | 0.2 |
| 計 | | 605 | 100.0 |

JIPDEC が運用しているの『プライバシーマーク』の認定を受けることについては約７割が「有効」と認識しているが、そのうちの約４割が「事業者にとって負担」であるとの印象を持っている。

業種別にみると、サービス業など個人情報を直接扱う機会が多い業種が「有効」と認識している。特に情報処理サービス業、金融・保険業の約９割が「有効」と見ている。ただし、マーク取得にあたっては、コンプライアンス・プログラムの策定やセキュリティ対策、監査の実施、継続教育の実施など、体制の整備を十分に行っておく必要があり、事業者にとっての負担はかなりのものである、との意見が多い。

## 2.11 その他

ここでは、「今後必要と思われる情報セキュリティ制度・機能・製品等」ならびに「各事業体で実施している情報セキュリティ対策の問題点」についての意見を一部抜粋、要約して紹介する。

（必要と思われる制度・機能・製品等）

・個人情報保護法対策、情報漏洩対策に関わるシステムの導入
・ネットワーク管理。資産管理
・公営によるウイルス対策ソフト・定義ファイルのサービス提供
・ＩＤＰ、セキュリティパッチ（ＯＳアプリケーション）の自動 Update 機能
・個人情報提供サービスの廃止
・セキュリティ監査制度の法的実権
・コンピュータ自体の安全性（セキュリティ）の向上
・海外拠点との連携のためのグローバルな制度。法制度国の方針の異なる部分の調整機能
・セキュリティチェックツール、セキュリティ教育ツール（e-learning 等）
・セキュリティレベルの認証制度、（企業）規模の小さい組織や個人への情報セキュリティ対策の徹底化（特にコスト、時間、技術レベルの問題のクリア）　　等。

（情報セキュリティ対策の問題点）

・セキュリティ対策の重要性および費用対効果を経営者層が理解していない
・専門要員の不足
・従業員のセキュリティに対する意識の向上が必要
・セキュリティ対策費用がかかりすぎる
・関係する法律・制度・基準・ガイド等に対しどこまで対応すればよいかの判断がつきにくい
・関連会社間での運用管理、使用ツール等の統一が図れない
・どのような対策を実施しても十分ということはなく、どの程度にとどめておけばよいか、担当レベルの判断になる　　等。

# 3．クロス集計結果の分析

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以下のクロス集計による分析を行った。質問項目に対するクロスを考慮したのは、関連質問に対する情報リスクマネジメントならびに情報セキュリティの視点から仮説を設け、それを検証することにより、事業体の実態に迫り、情報リスクに曝されている事業体にとり対応のための方策を策定する意味を示唆することにある。今回の報告書においても、前回調査同様、上記の視点に立ち、クロス分析を行うことにした。

クロス集計を行った項目は以下のとおりである。

| | 質問項目 | クロス集計対象項目 |
|---|---|---|
| 3.1 | Q6. 情報処理技術者試験制度の「情報セキュリティアドミニストレータ試験（SS 試験）」を知っていますか。 | Q27－③情報セキュリティの管理について、責任を有する担当者を定めていますか。 |
| | | Q63. 情報セキュリティ監査を実施したことがありますか。 |
| 3.2 | Q10. 情報リスクマネジメントにおいては、情報リスクマネジメント方針の明確化、情報リスクの分析、情報セキュリティポリシー、情報セキュリティ対策の規程、システム監査等が重要です。これらのうち、貴事業体において実施しているものはどれですか。 | Q22. 情報セキュリティ確保にとり、基本的に重要な視点は何だと思いますか。（複数回答） |
| | | Q24. 貴事業体では経営理念に基づく①情報セキュリティポリシー、②実施手続・規程類を定めていますか。 |
| | | Q60.過去2年以内にシステム監査を実施したことがありますか。 |
| | | Q63. 情報セキュリティ監査を実施したことがありますか。 |
| 3.3 | Q12. 基幹システムが1時間以上停止した場合、経営に与える影響（被害額）がどれ位になるか想定していますか。 | Q43. 貴事業体では従業員に対し、情報セキュリティの面（災害／障害、不正アクセス、ウイルスを含む）から教育・訓練を実施していますか。 |
| 3.4 | Q22. 情報セキュリティ確保にとり、基本的に重要な視点は何だと思いますか。 | Q28. 情報セキュリティ（システム災害／障害、不正アクセス、ウイルスを含む）管理についての問題点は何ですか。 |
| | | Q43. 貴事業体では従業員に対し、情報セキュリティの面（災害／障害、不正アクセス、ウイルスを含む）から教育・訓練を実施していますか。 |
| | | Q44. 貴事業体では情報セキュリティの人材をどのように養成していますか。 |
| 3.5 | Q24. 貴事業体では経営理念に基づく情報セキュリティポリシー、実施手続・規程類を定めていますか。 | Q46. 貴事業体では過去1年間に不正アクセスの被害に遭われたことがありますか。 |
| | | Q50. 情報についての機密度のランクを設定していますか。 |
| | | Q53. 貴事業体では過去1年間にコンピュータウイルスに感染したことがありますか。 |
| | | Q58. 運用に関しアウトソーシングを利用している場合、アウトソーシング先を選定する場合、どのような観点から選定していますか。（複数回答） |
| 3.6 | Q27. ネットワークの管理、情報システムの管理、情報セキュリティの管理について、責任を有する担当者を定めていますか。 | Q24. 貴事業体では経営理念に基づく①情報セキュリティポリシー、②実施手続・規程類を定めていますか。 |
| 3.7 | Q29. 情報セキュリティ要素のうち、貴事業体にとって重要と思われる要素を3つ選び、優先順位をつけて記入してください。 | Q29 の優先順位（1位×2位　他） |
| | | Q24. 貴事業体では経営理念に基づく①情報セキュリティポリシー、②実施手続・規程類を定めていますか。 |

| | 質問項目 | クロス集計対象項目 |
|---|---|---|
| 3.8 | Q31.「JIS X 5080 規格」の事業継続性管理に定められている事業継続性計画を作成していますか。 | Q13. 情報システムに係わるリスク分析を実施していますか。 |
| 3.9 | Q32. 事業継続性計画を作成／作成中の場合、事業継続性計画には以下の項目を含んでいますか。 | Q14. リスク分析を実施している場合、情報関連のどのようなリスクを対象としましたか。(複数回答) |
| 3.10 | Q42. どのようなネットワーク障害対策を実施していますか。実施している対策を選んでください。 | Q19. 基幹システムにおける MTBF(平均故障間隔)は何時間ですか。 |
| 3.11 | Q43. 貴事業体では従業員に対し、情報セキュリティの面(災害／障害、不正アクセス、ウイルスを含む)から教育・訓練を実施していますか。 | Q44. 貴事業体では情報セキュリティの人材をどのように養成していますか |
| 3.12 | Q60. 過去2年以内にシステム監査を実施したことがありますか。 | Q24. 貴事業体では経営理念に基づく①情報セキュリティポリシー、②実施手続・規程類を定めていますか。 |
| 3.13 | Q61. システム監査を実施した場合、その結果、どのような点に効果があったと思いますか。 | Q19. 基幹システムにおける MTBF(平均故障間隔)は何時間ですか。 |
| 3.14 | Q63. 情報セキュリティ監査を実施したことがありますか。 | Q24. 貴事業体では経営理念に基づく①情報セキュリティポリシー、②実施手続・規程類を定めていますか。 |

## 3．1　Q6のクロス集計

Q6.情報処理技術者試験制度の「情報セキュリティアドニミストレータ試験（SS試験）を知っていますか。

×Q27－③情報セキュリティの管理について、責任を有する担当者を定めていますか。
×Q63. 情報セキュリティ監査を実施したことがありますか。

### 3.1.1　Q27－③とのクロス集計

×Q27－③情報セキュリティの管理について、責任を有する担当者を定めていますか。

情報セキュリティアドミニストレータ試験の認知状況と情報セキュリティ管理者の関係を調べるため、クロス分析を実施した。

| Q27-③セキュリティ管理者 / Q6 アドミニストレータ試験 | 回答件数 | 定めている | | 設置を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 情報セキュリティ担当者をSS試験に受験させている | 69 | 60 | 15.2 | 6 | 6.8 | 2 | 1.7 | 0 | 0.0 | 1 | 20.0 |
| 知っている | 381 | 250 | 63.1 | 62 | 70.5 | 68 | 58.6 | 0 | 0.0 | 1 | 20.0 |
| 知らない | 154 | 85 | 21.5 | 20 | 22.7 | 46 | 39.7 | 0 | 0.0 | 3 | 60.0 |
| 無回答 | 1 | 1 | 0.3 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 計 | 605 | 396 | 100.0 | 88 | 100.0 | 116 | 100.0 | 0 | 0.0 | 5 | 100.0 |

情報セキュリティ管理者を「定めている」、または「設置を検討している」事業体では、情報セキュリティアドミニストレータ試験の認知度がきわめて高いことがわかる。

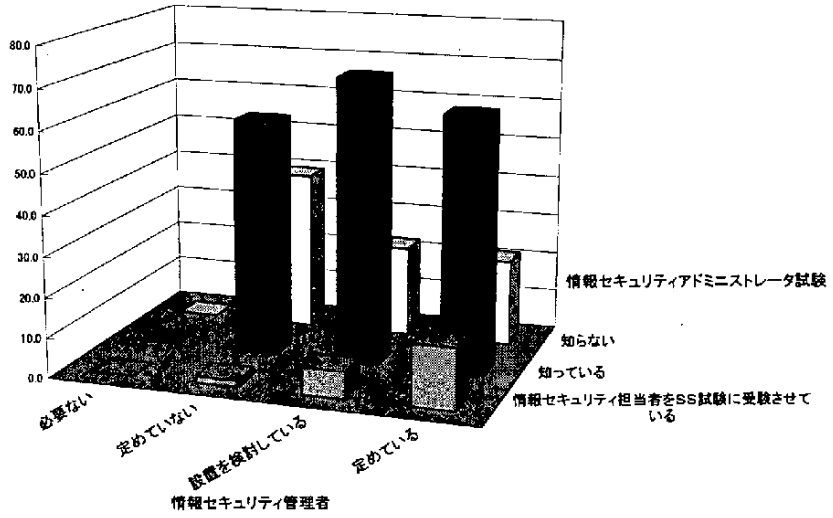



図3－1－1. 情報セキュリティアドミニストレータ試験の認知度と情報セキュリティ管理者の設置状況の関係

### 3.1.2　Q63 とのクロス集計

**Q63. 情報セキュリティ監査を実施したことがありますか。**

| Q63 情報セキュリティ監査 / Q6 アドミニストレータ試験 | 回答件数 | 実施している | | これから行う予定がある | | 実施しない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 情報セキュリティ担当者をSS試験に受験させている | 69 | 27 | 24.5 | 19 | 15.6 | 22 | 6.1 | 1 | 7.1 |
| 知っている | 381 | 71 | 64.5 | 84 | 68.9 | 216 | 60.2 | 10 | 71.4 |
| 知らない | 154 | 12 | 10.9 | 19 | 15.6 | 121 | 33.7 | 2 | 14.3 |
| 無回答 | 1 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 1 | 7.1 |
| 計 | 605 | 110 | 100.0 | 122 | 100.0 | 359 | 100.0 | 14 | 100.0 |

情報セキュリティ監査の実施状況と情報セキュリティアドミニストレータ試験との関係が大きいことがわかった。特に、情報セキュリティ監査を実施または実施予定の事業体では、情報セキュリティアドミニストレータ試験への認知度がきわめて高いことがわかる。ただし、受験との関係はあまり大きくないことがわかる。

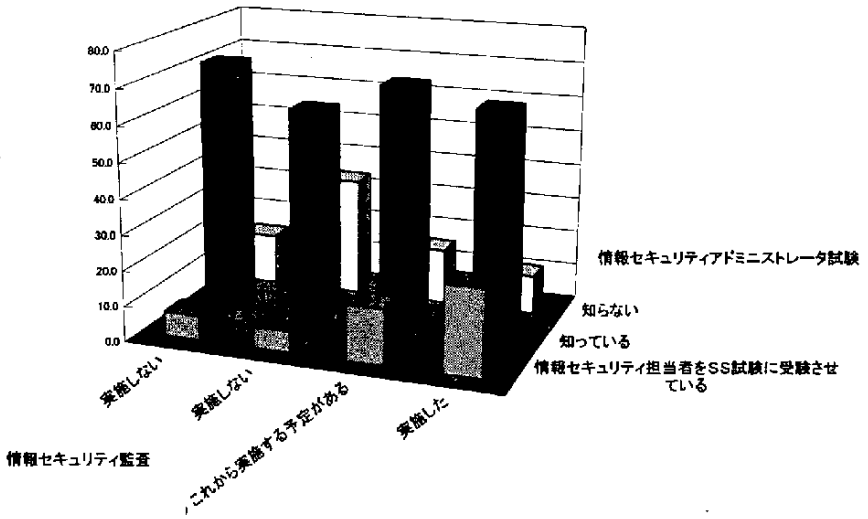



図3－1－2. 情報セキュリティアドミニストレータ試験と情報セキュリティ監査実施状況との関係

## 3．2　Q10のクロス集計

Q10. 情報のマネジメントにおいては情報リスクマネジメント方針の明確化、情報リスクの分析、情報セキュリティポリシー、情報セキュリティ対策の規程、システム監査等が重要です。これらのうち、貴事業体において実施しているものはどれですか。

×Q22. 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。
×Q24-①. 貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。
×Q24-②. 貴事業体では経営理念に基づく実施手続・規程類を定めていますか。
×Q60. 過去２年以内にシステム監査を実施したことがありますか。
×Q63. 情報セキュリティ監査を実施したことがありますか。

### 3.2.1　Q22とのクロス集計

**Q22.情報セキュリティの確保にとり、基本的に重要な視点は何だと思いますか。**

情報リスクマネジメントを実施している事業体としては、情報セキュリティの確保に関わる基本的な視点が明確であると考えられる。情報セキュリティ上重要な視点については「社内全体の理解（エンドユーザを含む）の理解」（85.5%）、次いで「経営者の理解」（71.2%）であったが、これらの視点から情報リスクマネジメント上の重要対策の実施状況との相関について分析を行った。

①Q10からみたQ22（情報リスクマネジメント上の重要対策に対するセキュリティ上の視点）

| Q22 視点 / Q10 対策 | 回答件数 | 経営者層の理解 | | 管理者の理解 | | 担当者の理解 | | 社内全体の理解 | | 法規制の整備 | | その他 | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 94 | 80.3 | 57 | 48.7 | 49 | 41.9 | 110 | 94.0 | 28 | 23.9 | 0 | 0.0 | 1 | 0.9 |
| 情報リスク分析 | 135 | 112 | 83.0 | 69 | 51.1 | 61 | 45.2 | 123 | 91.1 | 31 | 23.0 | 0 | 0.0 | 1 | 0.7 |
| 情報セキュリティポリシー | 316 | 230 | 72.8 | 141 | 44.6 | 116 | 36.7 | 288 | 91.1 | 50 | 15.8 | 0 | 0.0 | 1 | 0.3 |
| 情報セキュリティ対策 | 337 | 254 | 75.4 | 150 | 44.5 | 123 | 36.5 | 310 | 92.0 | 57 | 16.9 | 0 | 0.0 | 2 | 0.6 |
| 情報セキュリティ監査 | 117 | 84 | 71.8 | 50 | 42.7 | 38 | 32.5 | 112 | 95.7 | 24 | 20.5 | 0 | 0.0 | 0 | 0.0 |
| システム監査 | 182 | 137 | 75.3 | 76 | 41.8 | 55 | 30.2 | 165 | 90.7 | 36 | 19.8 | 0 | 0.0 | 1 | 0.5 |
| その他 | 24 | 17 | 70.8 | 11 | 45.8 | 10 | 41.7 | 24 | 100.0 | 6 | 25.0 | 1 | 4.2 | 0 | 0.0 |
| 特に実施していない | 150 | 99 | 66.0 | 54 | 36.0 | 36 | 24.0 | 110 | 73.3 | 16 | 10.7 | 1 | 0.7 | 1 | 0.7 |
| 無回答 | 4 | 1 | 25.0 | 0 | 0.0 | 0 | 0.0 | 3 | 75.0 | 0 | 0.0 | 0 | 0.0 | 1 | 25.0 |
| 計 | 605 | 431 | 74.4 | 240 | 44.0 | 187 | 35.3 | 517 | 90.1 | 87 | 17.9 | 2 | 0.1 | 5 | 0.6 |

「社内全体の理解（エンドユーザを含む）」では、情報リスクマネジメント方針(94.0%)、情報リスク分析（91.1%）を始め、いずれも90%を超える高い割合を示している。

同様に「経営者層の理解」では情報リスクマネジメント方針（80.3%）および情報リスク分析（83.0%）について80%台の回答であり、情報セキュリティポリシー以下、システム監査（75.3%）を含め、70%台の結果となっている。「管理者の理解」ならびに「担当者の理解」

についても、情報リスクマネジメントにおける重要な方針・情報リスク分析に 40～50％台の回答を示している。「法規制の整備」からみるとそれぞれの項目の割合が相対的に低い。現在の情報システム環境では従来のような法規制の整備を待つといった時間的な猶予がないことの理解と共に、事業体としてのアカウンタビリティについての認識の高まりを期待したい。

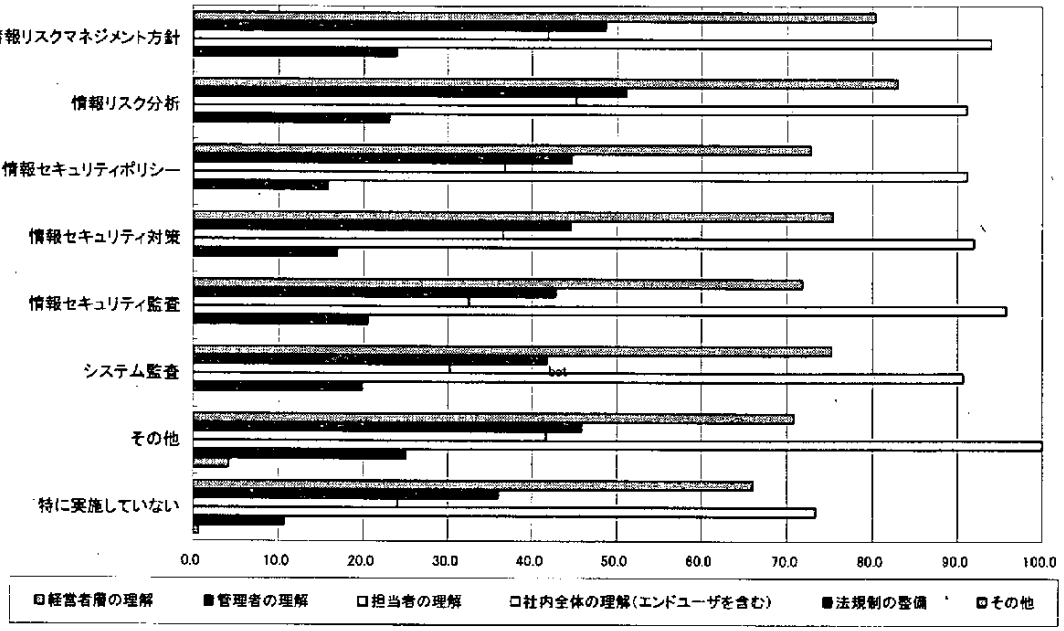



図3－2－1. 情報リスクマネジメント上の重要対策に対するセキュリティ上の視点

②Q22 からみたQ10 （セキュリティ上の視点からみた情報リスクマネジメント上の重要対策）

| Q22 視点 / Q10 対策 | 回答件数 | 経営者層の理解 | | 管理者の理解 | | 担当者の理解 | | 社内全体の理解 | | 法規制の整備 | | その他 | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 94 | 21.8 | 57 | 23.8 | 49 | 26.2 | 110 | 21.3 | 28 | 32.2 | 0 | 0.0 | 1 | 20.0 |
| 情報リスク分析 | 135 | 112 | 26.0 | 69 | 28.8 | 61 | 32.6 | 123 | 23.8 | 31 | 35.6 | 0 | 0.0 | 1 | 20.0 |
| 情報セキュリティポリシー | 316 | 230 | 53.4 | 141 | 58.8 | 116 | 62.0 | 288 | 55.7 | 50 | 57.5 | 0 | 0.0 | 1 | 20.0 |
| 情報セキュリティ対策 | 337 | 254 | 58.9 | 150 | 62.5 | 123 | 65.8 | 310 | 60.0 | 57 | 65.5 | 0 | 0.0 | 2 | 40.0 |
| 情報セキュリティ監査 | 117 | 84 | 19.5 | 50 | 20.8 | 38 | 20.3 | 112 | 21.7 | 24 | 27.6 | 0 | 0.0 | 0 | 0.0 |
| システム監査 | 182 | 137 | 31.8 | 76 | 31.7 | 55 | 29.4 | 165 | 31.9 | 36 | 41.4 | 0 | 0.0 | 1 | 20.0 |
| その他 | 24 | 17 | 3.9 | 11 | 4.6 | 10 | 5.3 | 24 | 4.6 | 6 | 6.9 | 1 | 50.0 | 0 | 0.0 |
| 特に実施していない | 150 | 99 | 23.0 | 54 | 22.5 | 36 | 19.3 | 110 | 21.3 | 16 | 18.4 | 1 | 50.0 | 1 | 20.0 |
| 無回答 | 4 | 1 | 0.2 | 0 | 0.0 | 0 | 0.0 | 3 | 0.6 | 0 | 0.0 | 0 | 0.0 | 1 | 20.0 |
| 計 | 605 | 431 | 100.0 | 240 | 100.0 | 187 | 100.0 | 517 | 100.0 | 87 | 100.0 | 2 | 100.0 | 5 | 100.0 |

一方、情報セキュリティの確保の視点のうち、経営者層の理解からみた場合、「情報セキュリティ対策」が 58.9％と高く、次いで「情報セキュリティポリシー」の 53.4％と、情報セキュリティ対策に関わる面に比較的高い割合が多く見られた。一方「情報リスクマネジメント方針」は 21.8％、「情報リスク分析」は 26.0％という結果となった。客観的な視点からのチェック機能を果たすシステム監査については、「経営者・管理者それぞれの理解」ならびに「社内全体の理解」では、情報リスクマネジメント方針や情報リスク分析より回答の割合が高くなっている。

こうした傾向からすれば、「はじめに手段ありき」的な考え方の存在が確認できる。この点は、Q22 の情報セキュリティに関する質問の性格からやむをえない結果とも思われるが、管理者、担当者等、いずれの場合にも共通の傾向であり、リスクマネジメントにおけるプロセスについて理解が十分ではないといえるかもしれない。

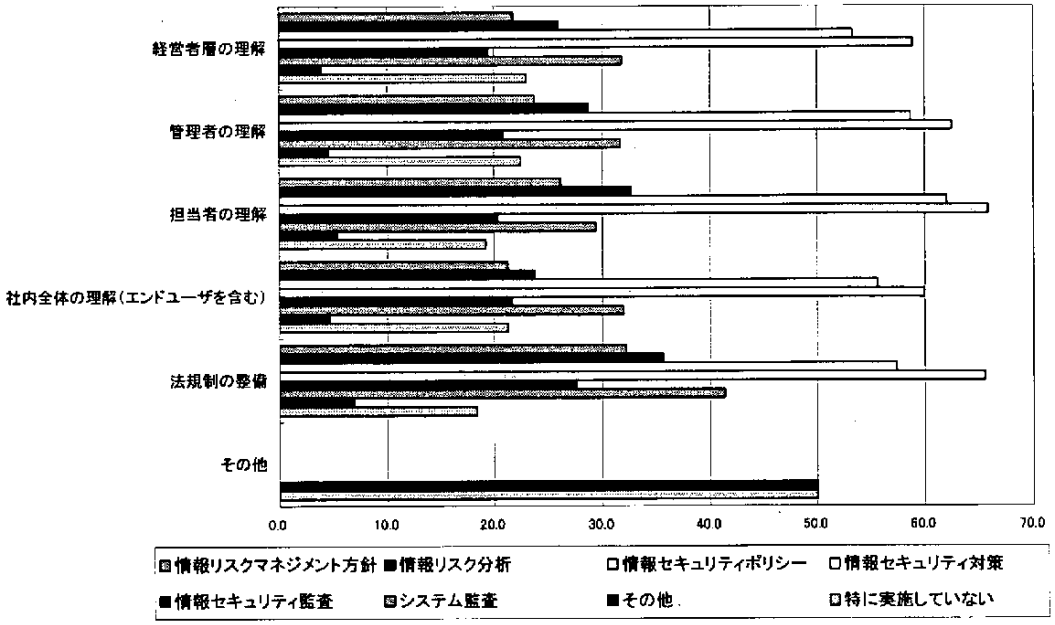



図3－2－2. セキュリティ上の視点に対する情報リスクマネジメント上の重要対策

### 3.2.2 Q24-①とのクロス集計

**Q24-①貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。**

情報リスクマネジメントを理解し、実施している事業体であれば、経営理念のもとで情報セキュリティポリシーや実施手続・規程類を定めているのが妥当と考えられる。したがって、情報セキュリティポリシーが策定されているのが当然であるといえる。

①Q10 からみたQ24-①

（情報リスクマネジメント上の重要対策に対するセキュリティポリシーの策定状況）

| Q24 ポリシー / Q10 対策 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 100 | 85.5 | 8 | 6.8 | 4 | 3.4 | 5 | 4.3 | 0 | 0.0 | 0 | 0.0 |
| 情報リスク分析 | 135 | 118 | 87.4 | 10 | 7.4 | 3 | 2.2 | 4 | 3.0 | 0 | 0.0 | 0 | 0.0 |
| 情報セキュリティポリシー | 316 | 258 | 81.6 | 39 | 12.3 | 11 | 3.5 | 8 | 2.5 | 0 | 0.0 | 0 | 0.0 |
| 情報セキュリティ対策 | 337 | 234 | 69.4 | 38 | 11.3 | 37 | 11.0 | 26 | 7.7 | 0 | 0.0 | 2 | 0.6 |
| 情報セキュリティ監査 | 117 | 97 | 82.9 | 10 | 8.5 | 7 | 6.0 | 3 | 2.6 | 0 | 0.0 | 0 | 0.0 |
| システム監査 | 182 | 119 | 65.4 | 19 | 10.4 | 28 | 15.4 | 15 | 8.2 | 0 | 0.0 | 1 | 0.5 |
| その他 | 24 | 6 | 25.0 | 11 | 45.8 | 5 | 20.8 | 2 | 8.3 | 0 | 0.0 | 0 | 0.0 |
| 特に実施していない | 150 | 3 | 2.0 | 11 | 7.3 | 31 | 20.7 | 101 | 67.3 | 4 | 2.7 | 0 | 0.0 |
| 無回答 | 4 | 2 | 50.0 | 0 | 0.0 | 1 | 25.0 | 1 | 25.0 | 0 | 0.0 | 0 | 0.0 |
| 計 | 605 | 279 | 67.8 | 78 | 10.6 | 98 | 9.2 | 143 | 11.9 | 4 | 0.3 | 3 | 0.2 |

情報セキュリティポリシーの策定状況との相関について、情報リスクマネジメントに関わる要素として「情報セキュリティポリシー」と回答した 316 事業体のうち、Q24 において情報セキュリティポリシーを「定めている」と回答したのは 81.6%であった。事業体数および割合の両回答の差異はどこにあるのであろうか。また、「現在作成中」および「作成を検討している」を回答した事業体はあわせても 15.8%にすぎず、「定めていない」は 2.5%であった。

回答に関して重要な点は、何らかの情報関連の事故・事件が生じた場合の結果である。たとえ「作成中」であっても事故・事件が発生した場合の影響は「定めていない」場合と同じといえる。実際に情報セキュリティポリシーを「定めている」事業体では、当該ポリシーに従って情報リスク対策を用意しているケースが一般的であり、そうした事業体の被るインパクトとそうでない事業体の受ける影響の違いはどうなのであろうか。この点の認識が情報リスクマネジメントなり情報セキュリティにとってきわめて重視すべき側面である。

②Q24-①からみたQ10

（セキュリティポリシーの策定状況からみた情報リスクマネジメント上の重要対策の実施状況）

| Q24 ポリシー / Q10 対策 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 100 | 35.8 | 8 | 10.3 | 4 | 4.1 | 5 | 3.5 | 0 | 0.0 | 0 | 0.0 |
| 情報リスク分析 | 135 | 118 | 42.3 | 10 | 12.8 | 3 | 3.1 | 4 | 2.8 | 0 | 0.0 | 0 | 0.0 |
| 情報セキュリティポリシー | 316 | 258 | 92.5 | 39 | 50.0 | 11 | 11.2 | 8 | 5.6 | 0 | 0.0 | 0 | 0.0 |
| 情報セキュリティ対策 | 337 | 234 | 83.9 | 38 | 48.7 | 37 | 37.8 | 26 | 18.2 | 0 | 0.0 | 2 | 66.7 |
| 情報セキュリティ監査 | 117 | 97 | 34.8 | 10 | 12.8 | 7 | 7.1 | 3 | 2.1 | 0 | 0.0 | 0 | 0.0 |
| システム監査 | 182 | 119 | 42.7 | 19 | 24.4 | 28 | 28.6 | 15 | 10.5 | 0 | 0.0 | 1 | 33.3 |
| その他 | 24 | 6 | 2.2 | 11 | 14.1 | 5 | 5.1 | 2 | 1.4 | 0 | 0.0 | 0 | 0.0 |
| 特に実施していない | 150 | 3 | 1.1 | 11 | 14.1 | 31 | 31.6 | 101 | 70.6 | 4 | 100.0 | 0 | 0.0 |
| 無回答 | 4 | 2 | 0.7 | 0 | 0.0 | 1 | 1.0 | 1 | 0.7 | 0 | 0.0 | 0 | 0.0 |
| 計 | 605 | 279 | 100.0 | 78 | 100.0 | 98 | 100.0 | 143 | 100.0 | 4 | 100.0 | 3 | 100.0 |

一方、Q24 において情報セキュリティポリシーを「定めている」と回答した 279 事業体について、Q10 で情報セキュリティポリシーに関して 92.5%が策定しているという結果となった。Q24 でセキュリティポリシーを「現在作成中」の事業体は 50.0%、情報セキュリティ対策に関しては 48.7%であった。なお、他の項目に関しては、情報リスクマネジメント方針（35.8%）、情報リスク分析（42.3%）、システム監査については 42.7%、情報セキュリティ監査（34.8%）と相対的に低い割合であったが、情報セキュリティ対策については 83.9%と高く、重点がセキュリティ対策に置かれる傾向が感じられる。

また、「作成を検討している」という 98 事業体のうち、11.2%が情報セキュリティポリシーと回答している。「定めていない」143 の事業体においても 5.6%が「情報セキュリティポリシー」をあげているという回答結果がみられる。

クロス集計でみた場合の回答の不一致をどう理解すべきについては、回答者側の組織内における実態把握がどの程度正確なのか、検討の余地がここでも確認できる。いずれにしても、それぞれの項目に関し、情報セキュリティポリシーとの関連なり対応がどうなのか、確認の必要がありそうである。

### 3.2.3 Q24-②とのクロス集計

**Q24-②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。**

事業体において、実施手続・規程類の策定に関しては、策定された情報セキュリティポリシーに従って定めるのが一般的であると仮定することができる。この点に関しては、以下のような結果が把握できた。

①Q10からみたQ24-②

（情報リスクマネジメント上の重要対策に対する実施手続・規程類の策定状況）

| Q24 実施手続・規程類 / Q10 対策 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 83 | 70.9 | 23 | 19.7 | 6 | 5.1 | 5 | 4.3 | 0 | 0.0 | 0 | 0.0 |
| 情報リスク分析 | 135 | 99 | 73.3 | 29 | 21.5 | 3 | 2.2 | 4 | 3.0 | 0 | 0.0 | 0 | 0.0 |
| 情報セキュリティポリシー | 316 | 183 | 57.9 | 86 | 27.2 | 31 | 9.8 | 14 | 4.4 | 0 | 0.0 | 2 | 0.6 |
| 情報セキュリティ対策 | 337 | 189 | 56.1 | 83 | 24.6 | 41 | 12.2 | 22 | 6.5 | 0 | 0.0 | 2 | 0.6 |
| 情報セキュリティ監査 | 117 | 85 | 72.6 | 19 | 16.2 | 10 | 8.5 | 3 | 2.6 | 0 | 0.0 | 0 | 0.0 |
| システム監査 | 182 | 104 | 57.1 | 34 | 18.7 | 30 | 16.5 | 12 | 6.6 | 0 | 0.0 | 2 | 1.1 |
| その他 | 24 | 4 | 16.7 | 12 | 50.0 | 6 | 25.0 | 2 | 8.3 | 0 | 0.0 | 0 | 0.0 |
| 特に実施していない | 150 | 5 | 3.3 | 10 | 6.7 | 29 | 19.3 | 101 | 67.3 | 4 | 2.7 | 1 | 0.7 |
| 無回答 | 4 | 1 | 25.0 | 0 | 0.0 | 1 | 25.0 | 1 | 25.0 | 0 | 0.0 | 1 | 25.0 |
| 計 | 605 | 211 | 54.5 | 125 | 21.4 | 111 | 11.4 | 146 | 11.9 | 4 | 0.3 | 8 | 0.6 |

Q10への回答である316事業体のうち、実施手続・規程類を定めているのは57.9%にすぎない。この点、情報セキュリティポリシーを持っていながら実施手続・規程類を定めていない約4割の事業体は、いかに情報リスクへの具体的な対応を考えているのであろうか。現在作成中の割合も27.2%であり、必ずしも高いはいえない。

情報リスクマネジメント方針を持つ117事業体では、上記規程類を定めているのが70.9%であった。また、情報セキュリティ対策では337事業体のうち「定めている」としているのが56.1%となっている。

Q10において「実施している」と回答したその結果との齟齬をどのように理解すべきなのであろうか。

②Q10 からみたQ24-②

（実施手続・規程類の策定状況に対する情報リスクマネジメント上の重要対策）

| Q24 実施手続・規程類 / Q10 対策 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 83 | 39.3 | 23 | 18.4 | 6 | 5.4 | 5 | 3.4 | 0 | 0.0 | 0 | 0.0 |
| 情報リスク分析 | 135 | 99 | 46.9 | 29 | 23.2 | 3 | 2.7 | 4 | 2.7 | 0 | 0.0 | 0 | 0.0 |
| 情報セキュリティポリシー | 316 | 183 | 86.7 | 86 | 68.8 | 31 | 27.9 | 14 | 9.6 | 0 | 0.0 | 2 | 25.0 |
| 情報セキュリティ対策 | 337 | 189 | 89.6 | 83 | 66.4 | 41 | 36.9 | 22 | 15.1 | 0 | 0.0 | 2 | 25.0 |
| 情報セキュリティ監査 | 117 | 85 | 40.3 | 19 | 15.2 | 10 | 9.0 | 3 | 2.1 | 0 | 0.0 | 0 | 0.0 |
| システム監査 | 182 | 104 | 49.3 | 34 | 27.2 | 30 | 27.0 | 12 | 8.2 | 0 | 0.0 | 2 | 25.0 |
| その他 | 24 | 4 | 1.9 | 12 | 9.6 | 6 | 5.4 | 2 | 1.4 | 0 | 0.0 | 0 | 0.0 |
| 特に実施していない | 150 | 5 | 2.4 | 10 | 8.0 | 29 | 26.1 | 101 | 69.2 | 4 | 100.0 | 1 | 12.5 |
| 無回答 | 4 | 1 | 0.5 | 0 | 0.0 | 1 | 0.9 | 1 | 0.7 | 0 | 0.0 | 1 | 12.5 |
| 計 | 605 | 211 | 100.0 | 125 | 100.0 | 111 | 100.0 | 146 | 100.0 | 4 | 100.0 | 8 | 100.0 |

実施手続・規程類を定めている 211 事業体について情報リスクマネジメント上の重要対策の実施状況をみると、86.7％の事業体が情報セキュリティポリシーと回答している。ヨリ高い割合を示しているのは「情報セキュリティ対策」であり、情報セキュリティポリシーに基づき情報セキュリティ対策、実施手続・規程類が策定されるという、論理的な行動が事業体において必ずしも採択されているといえない実態が確認できる。

### 3.2.4 Q60 とのクロス集計

**Q60. 過去２年以内にシステム監査を実施したことがありますか。**

情報リスクマネジメントにおいては、客観的な視点から行うシステム監査は非常に重要である。特に、情報リスクマネジメントについて認識のある事業体であれば、システム監査を実施することが理論的のみならず実体的にも妥当のはずである。少なくとも、Q10 で「実施している」と回答した事業体であればQ60 も同様の回答結果がみられるという仮説を立てても当然といえる。そこで、実施対策とシステム監査の実施状況との相関について焦点をあて、その上で他の重要な項目についても取りあげることとした。

①Q10 からみたQ60（情報リスクマネジメント上の重要対策に対するシステム監査の実施状況）

| Q60 システム監査 / Q10 対策 | 回答件数 | 実施した（実施中を含む） | | 実施しない | | これから実施する予定がある | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 56 | 47.9 | 43 | 36.8 | 15 | 12.8 | 3 | 2.6 |
| 情報リスク分析 | 135 | 67 | 49.6 | 44 | 32.6 | 21 | 15.6 | 3 | 2.2 |
| 情報セキュリティポリシー | 316 | 124 | 39.2 | 148 | 46.8 | 39 | 12.3 | 5 | 1.6 |
| 情報セキュリティ対策 | 337 | 135 | 40.1 | 154 | 45.7 | 43 | 12.8 | 5 | 1.5 |
| 情報セキュリティ監査 | 117 | 63 | 53.9 | 37 | 31.6 | 14 | 12.0 | 3 | 2.6 |
| システム監査 | 182 | 106 | 58.2 | 62 | 34.1 | 12 | 6.6 | 2 | 1.1 |
| その他 | 24 | 7 | 29.2 | 15 | 62.5 | 2 | 8.3 | 0 | 0.0 |
| 特に実施していない | 150 | 42 | 28.0 | 96 | 64.0 | 11 | 7.3 | 1 | 0.7 |
| 無回答 | 4 | 1 | 25.0 | 2 | 50.0 | 0 | 0.0 | 1 | 25.0 |
| 計 | 605 | 217 | 43.5 | 315 | 43.5 | 66 | 11.4 | 7 | 1.7 |

情報リスクマネジメントに関しては、システム監査について 182 事業体が「実施している」と回答しているが、これに対し、過去２年におけるシステム監査の実施状況をみると、「実施した（実施中を含む）」は残念ながら 58.2%であった。しかも、34.1%は「実施しない」と回答している。

情報リスクマネジメントに関わる他の側面について、システム監査における監査対象の面から考慮するとき、情報セキュリティ対策では 40.1%、情報セキュリティポリシーでは 39.2%という状況であり、システム監査の実施状況から他の項目との関連についても着目する必要がある。

②Q60 からみたQ10（システム監査の実施状況に対する情報リスクマネジメント上の重要対策）

| Q60 システム監査 / Q10 対策 | 回答件数 | 実施した(実施中を含む) | | 実施しない | | これから実施する予定がある | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 56 | 25.8 | 43 | 13.7 | 15 | 22.7 | 3 | 42.9 |
| 情報リスク分析 | 135 | 67 | 30.9 | 44 | 14.0 | 21 | 31.8 | 3 | 42.9 |
| 情報セキュリティポリシー | 316 | 124 | 57.1 | 148 | 47.0 | 39 | 59.1 | 5 | 71.4 |
| 情報セキュリティ対策 | 337 | 135 | 62.2 | 154 | 48.9 | 43 | 65.2 | 5 | 71.4 |
| 情報セキュリティ監査 | 117 | 63 | 29.0 | 37 | 11.7 | 14 | 21.2 | 3 | 42.9 |
| システム監査 | 182 | 106 | 48.8 | 62 | 19.7 | 12 | 18.2 | 2 | 28.6 |
| その他 | 24 | 7 | 3.2 | 15 | 4.8 | 2 | 3.0 | 0 | 0.0 |
| 特に実施していない | 150 | 42 | 19.4 | 96 | 30.5 | 11 | 16.7 | 1 | 14.3 |
| 無回答 | 4 | 1 | 0.5 | 2 | 0.6 | 0 | 0.0 | 1 | 14.3 |
| 計 | 605 | 217 | 100.0 | 315 | 100.0 | 66 | 100.0 | 7 | 100.0 |

一方、システム監査を「実施した（実施中を含む）」事業体の数は 217 であった。これに対し、Q10 で「システム監査」と回答したのは 48.8%である。この差異の原因が何であったかについて、回答者によっては実態の把握が明確でなかったことに問題があったのかもしれない。

他の項目、たとえば、情報セキュリティ対策については 62.2%と相対的に高い割合であり、対策重視の側面が垣間みられる。

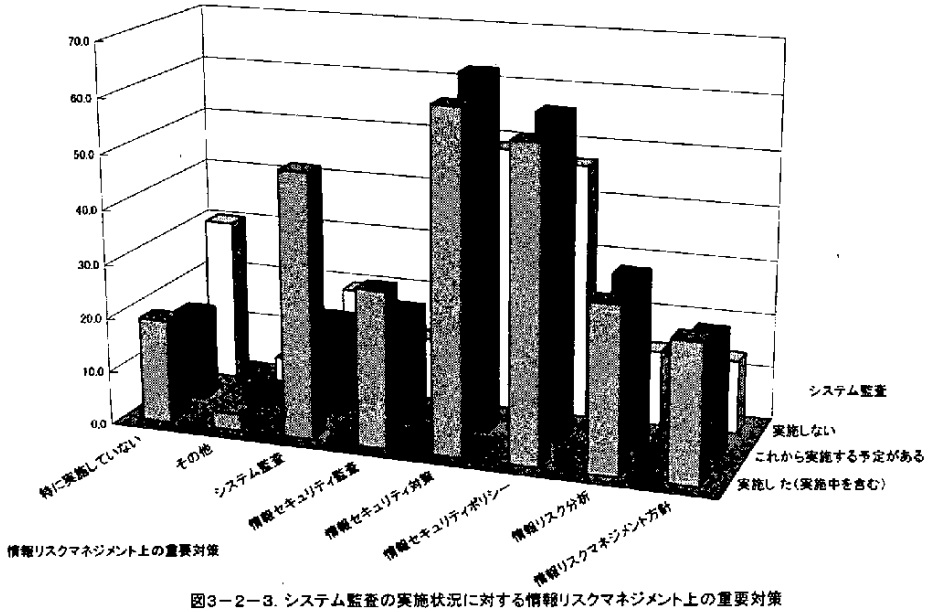



図3－2－3. システム監査の実施状況に対する情報リスクマネジメント上の重要対策

いずれにしても、こうした数値を考慮する際、回答者がいかなる視点から質問への回答に臨んだのか、問題によって回答者（複数の回答者）が異なったのか、単独の回答者の場合、回答の時間差があったのか、認識に差異があったのか、こうしたクロスによる対応の結果については、すでに触れてきたように、組織の実態について回答時の理解なり認識にギャップが存在していたことになる。思い込みや不正確な情報等、理由は何であれ、リスクマネジメントに関する認識の共有ができていない結果といえる。事業体にとって対処すべき重要なリスクに関わる問題だけに、検討の余地が残されている。

### 3.2.5 Q63 とのクロス集計

**Q63. 情報セキュリティ監査を実施したことがありますか。**

情報セキュリティ監査との関係では、情報セキュリティに特化しているとはいえ、システム監査の場合と類似の視点からアプローチすることが可能である。Q63 に対する回答数は 110 であり、Q10 に対する回答 117 の事業体と異なっている。

情報セキュリティ監査との関係では、情報セキュリティに特化しているとはいえ、システム監査の場合と類似の仮説からアプローチすることができる。

①Q10 からみたQ63

（情報リスクマネジメント上の重要対策に対する情報セキュリティ監査の実施状況）

| Q63 情報セキュリティ監査 / Q10 対策 | 回答件数 | 実施した（実施中を含む） | | これから実施する予定がある | | 実施しない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 40 | 34.2 | 22 | 18.8 | 52 | 44.4 | 3 | 2.6 |
| 情報リスク分析 | 135 | 47 | 34.8 | 28 | 20.7 | 57 | 42.2 | 3 | 2.2 |
| 情報セキュリティポリシー | 316 | 82 | 25.9 | 74 | 23.4 | 151 | 47.8 | 9 | 2.8 |
| 情報セキュリティ対策 | 337 | 85 | 25.2 | 74 | 22.0 | 167 | 49.6 | 11 | 3.3 |
| 情報セキュリティ監査 | 117 | 58 | 49.6 | 20 | 17.1 | 35 | 29.9 | 4 | 3.4 |
| システム監査 | 182 | 60 | 33.0 | 26 | 14.3 | 94 | 51.6 | 2 | 1.1 |
| その他 | 24 | 3 | 12.5 | 10 | 41.7 | 11 | 45.8 | 0 | 0.0 |
| 特に実施していない | 150 | 16 | 10.7 | 21 | 14.0 | 112 | 74.7 | 1 | 0.7 |
| 無回答 | 4 | 1 | 25.0 | 0 | 0.0 | 2 | 50.0 | 1 | 25.0 |
| 計 | 605 | 110 | 28.4 | 122 | 19.9 | 359 | 49.3 | 14 | 2.5 |

回答数については、Q10 に対する情報セキュリティ監査に対する回答 117 事業体のうち、Q63 でセキュリティ監査を「実施した」とする回答は 49.6％であり、システム監査への回答事業体数の 33.0％より割合が高くなっている。一方、「実施しない」事業体が 29.9％である。

②Q63 からみたQ10（情報セキュリティ監査の実施状況に対する情報リスクマネジメント上の重要対策）

| Q63 情報セキュリティ監査 / Q10 対策 | 回答件数 | 実施した（実施中を含む） | | これから実施する予定がある | | 実施しない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 情報リスクマネジメント方針 | 117 | 40 | 36.4 | 22 | 18.0 | 52 | 14.5 | 3 | 21.4 |
| 情報リスク分析 | 135 | 47 | 42.7 | 28 | 23.0 | 57 | 15.9 | 3 | 21.4 |
| 情報セキュリティポリシー | 316 | 82 | 74.5 | 74 | 60.7 | 151 | 42.1 | 9 | 64.3 |
| 情報セキュリティ対策 | 337 | 85 | 77.3 | 74 | 60.7 | 167 | 46.5 | 11 | 78.6 |
| 情報セキュリティ監査 | 117 | 58 | 52.7 | 20 | 16.4 | 35 | 9.7 | 4 | 28.6 |
| システム監査 | 182 | 60 | 54.5 | 26 | 21.3 | 94 | 26.2 | 2 | 14.3 |
| その他 | 24 | 3 | 2.7 | 10 | 8.2 | 11 | 3.1 | 0 | 0.0 |
| 特に実施していない | 150 | 16 | 14.5 | 21 | 17.2 | 112 | 31.2 | 1 | 7.1 |
| 無回答 | 4 | 1 | 0.9 | 0 | 0.0 | 2 | 0.6 | 1 | 7.1 |
| 計 | 605 | 110 | 100.0 | 122 | 100.0 | 359 | 100.0 | 14 | 100.0 |

一方、Q63 の情報セキュリティ監査について「実施した」事業体は 52.7%である。なお、システム監査の方が 54.5%とわずかながら多い割合となっている。また、情報セキュリティ対策（77.3%）ならびに情報セキュリティポリシー（74.5%）については７割を超えている。それに対し、情報リスクマネジメントは 36.4%、情報リスク分析は 42.7%と相対的に低く、こうした側面からすれば、リスクマネジメントにおけるプロセス観なりリスク分析の視点の比重が低く、「はじめに対策ありき」といった視点の存在が読み取れよう。

回答間における齟齬の存在については、あらためて言及することはしないが、回答結果の読み方には注意が必要といえる。ただ、繰り返し強調しておきたい点は、「含み益」に依存しえた過去と異なり、調査項目について「実施した」と「実施しない」、「実施の予定」との事業体の間に、問題状況発生後の結果に大きな違い（復旧・回復の投入時間・発生費用の違い等）が出てくることが考えられ、そうした認識に基づくリスクマネジメント実践が必要である。

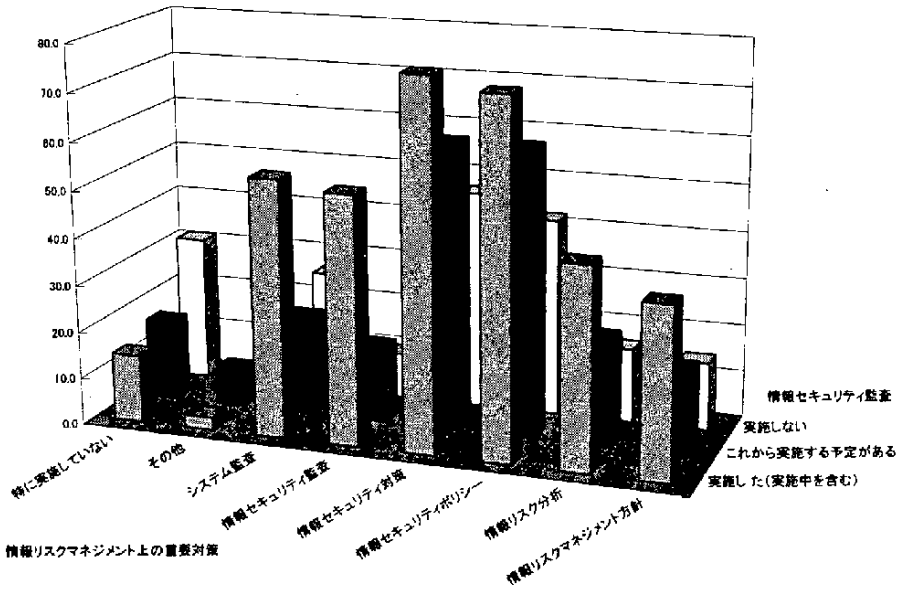



図3－2－4. 情報セキュリティ監査の実施状況に対する情報リスクマネジメント上の重要対策

## 3．3　Q12のクロス集計

Q12.（基幹システムが1時間以上停止した場合、経営に与える影響がどれぐらいになるか想定している場合）被害の推定額は1日あたりどれぐらいですか。

×Q43. 貴事業体では従業員に対し、情報セキュリティの面（災害／障害、不正アクセス、ウイルスを含む）から教育・訓練を実施していますか。

基幹システムの停止に対する経営に与える影響被害の推定額は「1千万円未満」41.2%が最も高く、「1千万円～5千万円未満」25.2%がこれに続いていた。これに対し、従業員に対する情報セキュリティ関連教育・訓練の実施状況との関係についてクロス分析を行った。

| Q43 教育・訓練 / Q12 被害推定額 | 回答件数 | 定期的に実施している | | 時々実施している | | 実施を予定している | | 特に実施していない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10億円以上 | 14 | 3 | 21.4 | 3 | 21.4 | 2 | 14.3 | 6 | 42.9 | 0 | 14 |
| 5億円以上～10億円未満 | 1 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 1 | 100. | 0 | 1 |
| 1億円以上～5億円未満 | 14 | 5 | 35.7 | 1 | 7.1 | 4 | 28.6 | 4 | 28.6 | 0 | 14 |
| 5千万円以上～1億円未満 | 7 | 1 | 14.3 | 1 | 14.3 | 1 | 14.3 | 4 | 57.1 | 0 | 7 |
| 1千万円以上～5千万円未満 | 33 | 3 | 9.1 | 7 | 21.2 | 5 | 15.2 | 18 | 54.5 | 0 | 33 |
| 1千万円未満 | 54 | 9 | 16.7 | 11 | 20.4 | 11 | 20.4 | 22 | 40.7 | 1 | 54 |
| 無回答 | 8 | 2 | 25.0 | 2 | 25.0 | 0 | 0.0 | 4 | 50.0 | 0 | 8 |
| 計 | 131 | 23 | 17.6 | 25 | 19.1 | 23 | 17.6 | 59 | 45.0 | 1 | 131 |

Q43の回答結果としては、「特に実施していない」42.0%が最も高いポイントで、「時々実施している」（25.6%）がこれに続いているが、被害推定額との関係をみると以下のとおりであった。

| 被害推定額 | 1位 | % |
|---|---|---|
| 10億円以上 | 特に実施していない | 42.9 |
| 5億円以上～10億円未満 | 特に実施していない | 100.0 |
| 1億円以上～5億円未満 | 定期的に実施している | 35.7 |
| 5千万円以上～1億円未満 | 特に実施していない | 57.1 |
| 1千万円以上～5千万円未満 | 特に実施していない | 54.5 |
| 1千万円未満 | 特に実施していない | 40.7 |

被害推定額を1億円以上～5億円未満とした事業体は「定期的に実施している」が35.7%と比較的高い割合であったが、その他の被害額を推定している事業体は「特に実施していない」が高い割合であった。

推定した被害額に基づき実際の被害額をできるだけ少なくしようと考えた場合、情報セキュリティに関する従業員教育の充実が必要であるが、「特に実施していない」が高い割合となっている。

また、「定期的に実施している」と「時々実施している」の回答率を被害推定額からみると以下のような結果となった。

| 被害推定額 | 定期的に実施している | 時々実施している | 合計 |
|---|---|---|---|
| 10億円以上 | 21.4 | 21.4 | 42.8 |
| 5億円以上～10億円未満 | 0.0 | 0.0 | 0.0 |
| 1億円以上～5億円未満 | 35.7 | 7.1 | 42.8 |
| 5千万円以上～1億円未満 | 14.3 | 14.3 | 28.6 |
| 1千万円以上～5千万円未満 | 9.1 | 21.2 | 30.3 |
| 1千万円未満 | 16.7 | 20.4 | 37.1 |

「定期的に実施している」と「時々実施している」を合わせると、28.6%～42.8%の事業体が教育・訓練を実施している。

ただし、被害推定額を「5億円以上～10億円未満」とした事業体の情報セキュリティに関する従業員の教育・訓練は0.0%という結果となった。

相対的にみると、被害推定額を多く見積もっている事業体は、情報セキュリティに関する従業員の教育・訓練に力を入れていると考えていたが、ここでは特に顕著な関係はみられなかった。

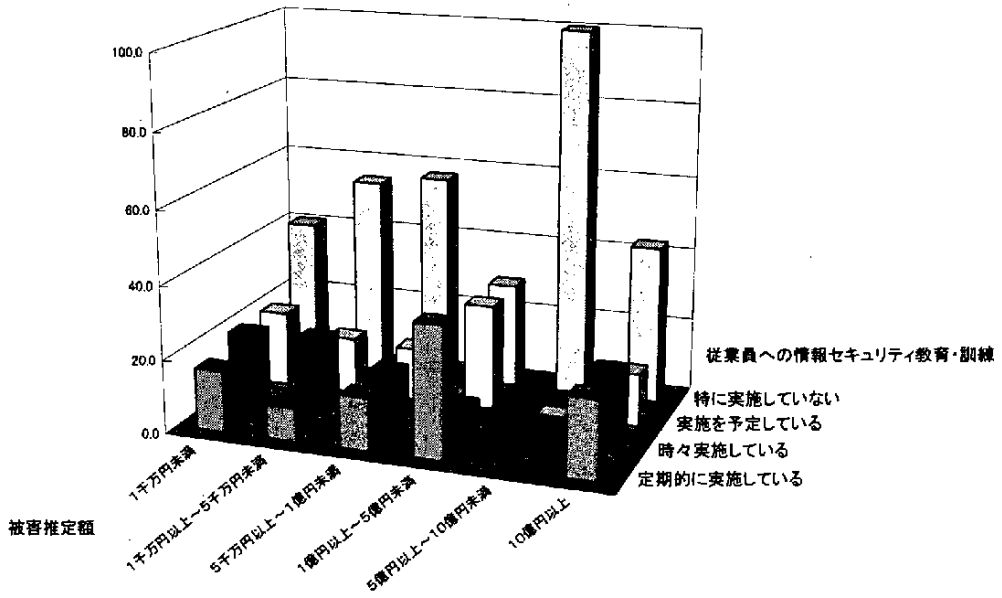



図3－3－1. 被害推定額と従業員のセキュリティ教育・訓練の実施状況の関係

## 3．4　Q22のクロス集計

Q22. 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

×Q28. 情報セキュリティ管理についての問題点は何ですか。
×Q43. 貴事業体では従業員に対し、情報セキュリティの面（災害／障害、不正アクセス、ウイルスを含む）から教育・訓練を実施していますか。
×Q44. 貴事業体では情報セキュリティの人材をどのように養成していますか。

### 3.4.1　Q28とのクロス集計

**Q28. 情報セキュリティ管理についての問題点は何ですか。**

情報セキュリティの管理についての問題点を選択した回答者が情報セキュリティの確保には何が重要であると考えているか、クロス集計により分析した。なお、ここでは回答数に差があるため20件以上の回答があるもののみ分析を行った。

| Q22 セキュリティ確保上の視点 / Q28 情報セキュリティ管理の問題点 | 回答件数 | 経営者層の理解 | | 管理者の理解 | | 担当者の理解 | | 社内全体の理解（ｴﾝﾄﾞﾕｰｻﾞを含む） | | 法規制の整備 | | その他 | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 経営者層の理解が得られない | 92 | 81 | 88.0 | 32 | 34.8 | 18 | 19.6 | 73 | 79.3 | 11 | 12.0 | 0 | 0.0 | 0 | 0.0 |
| コストがかかりすぎる | 324 | 252 | 77.8 | 138 | 42.6 | 105 | 32.4 | 285 | 88.0 | 58 | 17.9 | 1 | 0.3 | 0 | 0.0 |
| 専門要員がいない | 260 | 185 | 71.2 | 116 | 44.6 | 85 | 32.7 | 224 | 86.2 | 38 | 14.6 | 1 | 0.4 | 0 | 0.0 |
| 組織の従業員に対する負担がかかりすぎる | 158 | 114 | 72.2 | 83 | 52.5 | 60 | 38.0 | 142 | 89.9 | 35 | 22.2 | 0 | 0.0 | 1 | 0.6 |
| 組織の従業員に対する教育・訓練がいきとどかない | 330 | 248 | 75.2 | 149 | 45.2 | 108 | 32.7 | 293 | 88.8 | 43 | 13.0 | 1 | 0.3 | 0 | 0.0 |
| ノウハウが不足している | 208 | 149 | 71.6 | 97 | 46.6 | 70 | 33.7 | 171 | 82.2 | 30 | 14.4 | 1 | 0.5 | 1 | 0.5 |
| どこまでやればよいのか基準が示されていない | 231 | 179 | 77.5 | 102 | 44.2 | 78 | 33.8 | 196 | 84.8 | 34 | 14.7 | 0 | 0.0 | 0 | 0.0 |
| 要求に合致するもの（サービス／製品）がない | 25 | 22 | 88.0 | 7 | 28.0 | 6 | 24.0 | 23 | 92.0 | 5 | 20.0 | 0 | 0.0 | 0 | 0.0 |
| 組織の従業員に倫理観が乏しく、情報を財産と認識する風土がない | 117 | 87 | 74.4 | 48 | 41.0 | 33 | 28.2 | 103 | 88.0 | 12 | 10.3 | 0 | 0.0 | 0 | 0.0 |
| 情報セキュリティ管理が事業の国際化に見合っていない | 3 | 3 | 100.0 | 2 | 66.7 | 2 | 66.7 | 3 | 100.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| その他 | 8 | 6 | 75.0 | 5 | 62.5 | 4 | 50.0 | 8 | 100.0 | 3 | 37.5 | 0 | 0.0 | 0 | 0.0 |
| 特に問題はない | 20 | 10 | 50.0 | 6 | 30.0 | 8 | 40.0 | 18 | 90.0 | 4 | 20.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 6 | 1 | 16.7 | 0 | 0.0 | 0 | 0.0 | 2 | 33.3 | 0 | 0.0 | 0 | 0.0 | 4 | 66.7 |
| 計 | 605 | 431 | 71.2 | 240 | 39.7 | 187 | 30.9 | 517 | 85.5 | 87 | 14.4 | 2 | 0.3 | 5 | 0.8 |

問題点として「経営者層の理解が得られない」を選択した92事業体は情報セキュリティの確保にとり基本的に重要な視点として「経営者の理解」88.0%、「管理者の理解」34.8%、「担当者の理解」19.6%、「社内全体の理解（エンドユーザを含む）」79.3%、「法規制の整備」12.0%となっ

ている。この傾向は全体の平均である「経営者の理解」71.2%、「管理者の理解」39.7%、「担当者の理解」30.9%、「社内全体の理解」85.5%、「法規制の整備」14.4%とほぼ同じである。ただしそれぞれを平均と比べると、「経営者層の理解」が16.8ポイントと非常に高く、「管理者の理解」が4.9ポイント低く、「担当者の理解」が11.3ポイント低く、「社内全体の理解」が6.2ポイント低く、「法規制の整備」が2.4ポイント低い結果となっている。

その他の選択肢と傾向を比較した場合、「経営者層の理解」が平均値より大幅に高く、その他の項目がすべて平均値より下回ったものはこの選択肢しかなく、このように「経営者層の理解が得られない」を選択した事業体は重要な視点として「経営者の理解」を相当意識してあげており、重要視しているがゆえにその理解が得られないことが問題である、と認識していることを意味しており、結果としても妥当と考えられる。

以下、このように選択肢ごとに平均と比較するなかで、特徴のあるものについて分析する。「コストがかかりすぎる」を選択した324事業体の傾向をみると、「経営者層の理解」77.8%と平均より6.6ポイント高く、「管理者の理解」42.6%と2.9ポイント、「担当者の理解」32.4%と1.5ポイント、「社内全体の理解」88.0%と2.5ポイント、「法規制の整備」17.9%と3.5ポイント高くすべての項目で高い結果となった。「経営者層の理解」を選択した割合は全体で3番目の高さであり、コスト負担の承認が経営者の判断によるためと考えられる。

「専門要員がいない」の260事業体の回答では「経営者層の理解」71.2%で平均と同じであり、「管理者の理解」44.6%と4.9ポイント高く、「担当者の理解」32.7%と1.8ポイント、「社内全体の理解」86.2%と0.7ポイント、「法規制の整備」は14.6%と0.2ポイント高い結果となった。平均と比べ大きな差はみられないが、「管理者の理解」を選択した割合は3番目と高く、「経営者層の理解」が平均であることを考慮すると、専門要員の確保には現場の管理者の理解が一番必要と捉えられていると考えられる。

「組織の従業員に対する負担がかかりすぎる」158事業体の回答では、「経営者層の理解」72.7%、と1.0ポイント高く、「管理者の理解」52.5%と12.8ポイント高く、「担当者の理解」38.0%と7.1ポイント高く、「社内全体の理解」89.9%と4.4ポイント高く、「法規制の整備」22.2%と7.8ポイント高い。このうち「管理者の理解」と「法規制の整備」は全体で1番目の高さであり、「担当者の理解」は2番目、「社内全体の理解」は3番目の高さである。相対的にみれば、従業員への負荷については経営者の理解よりもどちらかというと各職場の現場の管理や従業員相互の協力などの必要性を強く意識していると考えられる。

「組織の従業員に対する教育・訓練がいきとどかない」を選択した330事業体の回答では「経営者層の理解」75.2%と4.0ポイント高く、「管理者の理解」45.2%と5.5%、「担当者の理解」32.7%と1.8ポイント、「社内全体の理解」88.8%と3.3ポイント高い。一方「法規制の整備」は13.0%と1.4ポイント低くなっている。訓練に関しては各事業体の取組みそのものであるため、訓練に対して法規制を求めることは少ないものと考えられる。

「ノウハウが不足している」を選択した208事業体の回答では「経営者層の理解」71.6%と0.4ポイント高く、「管理者の理解」46.6%と6.9ポイント高く、「担当者の理解」33.7%と2.8%高いが、一方「社内全体の理解」82.2%と3.3ポイント低く、「法規制の整備」14.4%と平均値であった。「管理者の理解」は2番目の高さであり、ノウハウを習得するためには社内全体の理解や法整備については重きがおかれず、現場の管理者の意識に大きく依存していることがわかる。

「どこまでやればよいのか基準が示されていない」を選択した231事業体の回答をみると「経営者層の理解」77.5%と4.3ポイント高く、「管理者の理解」44.2%と4.5ポイント高く、「担当者の理解」33.8%と2.9ポイント高く、「社内全体の理解」84.8%と0.7ポイント低く、「法規制の整備」14.7%と0.3ポイント高い。「担当者の理解」が3番目に高く、どこまで実施すればよいかという点については担当者の理解の問題が他の選択肢よりも高いこともうなずける。また「社内全体の理解」が平均より少ないのも、まず基準に応じてどこまで実施するかを決定するのが事務局部門であることからこれも理解できる。

「要求に合致するもの（サービス/製品）がない」を選択した25事業体の回答をみると、「経営者層の理解」88.0%と16.8ポイント高く、「管理者の理解」28.0%と11.7ポイント低く、「担当者の理解」24.0%と6.9ポイント低く、「社内全体の理解」92.0%と6.5ポイント高く、「法規制の整備」20.0%と5.6ポイント高い。「経営者層の理解」と「社内全体の理解」は1番目に高く、「法規制の整備」が2番目に高いが、回答者数の数が少ないため確実なことはいえない。経営者の夢のような要求に困惑したり、あるいは法律の規制などで望まれるサービスや製品が開発されることを願っていることの現われかもしれない。

「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」を選択した117事業体の回答をみると、「経営者層の理解」74.4%と3.2ポイント高く、「管理者の理解」41.0%と1.3ポイント高く、「担当者の理解」28.2%と2.7ポイント低く、「社内全体の理解」88.0%と2.5ポイント高く、「法規制の整備」10.3%と4.1ポイント低い。社内の価値観や倫理観の問題であるため経営者、管理者、社内全体というトップダウンからの強い指導を求めていることがわかる。

「特に問題はない」を選択した20事業体の回答をみると、「経営者層の理解」50.0%と21.2ポイント低く、「管理者の理解」30.0%と9.7ポイント低く、「担当者の理解」40.0%と9.1ポイント高く、「社内全体の理解」90.0%と4.5ポイント高く、「法規制の整備」20.0%と5.6ポイント高い。回答者が少ないがその他の選択と比較すると経営者や管理者の理解を求めることが少なく担当者の理解が一番多いなど現場のみで考えようとする傾向がうかがえる。

全体的にみると、「経営者層の理解」が重要と考えている場合、問題点として「経営者層の理解が得られない」を選択しており、この結果は妥当といえる。「管理者の理解」を求めているのは「専門要員がいない」、「組織の従業員に対する負荷がかかりすぎる」、「ノウハウが不足している」となっており、スキルのある要員の確保が事務局部門であるシステム部門の管理者の問題として捉えられている傾向がみられる。「担当者の理解」を選択しているのは「組織の従業員に対する負担がかかりすぎる」、「どこまでやればよいのか基準が示されない」という選択である。「社内全体の理解」を求めているのは「組織の従業員に対する負荷がかかりすぎる」であり、対策は従業員全員が行うべきものであり、この回答結果は妥当である。

「法規制の整備」については「組織の従業員に対する負荷がかかりすぎる」、「コストがかかりすぎる」が比較的選択が多く、何らかの規制により経営に認めさせたいという意識がある。また逆に選択が少ない「専門要員がいない」、「組織の従業員に対する教育・訓練がいきとどかない」、「ノウハウが不足している」などがあり、これらは社内問題として認識されていることを反映していると考えられる。

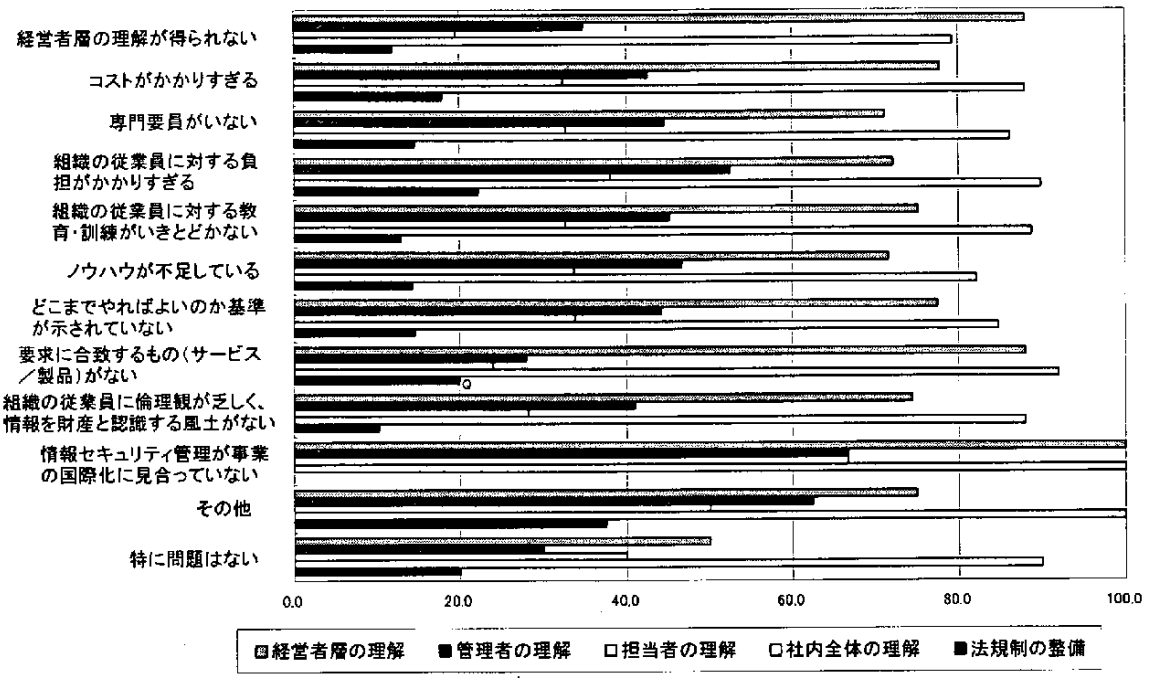



図3－4－1. セキュリティ確保のための重要な視点とセキュリティ管理上の問題点の関係

### 3.4.2 Q43 とのクロス集計

**Q43. 貴事業体では従業員に対し、情報セキュリティの面（災害／障害、不正アクセス、ウイルスを含む）から教育・訓練を実施していますか。**

Q22 の回答結果として、「社内全体の理解（エンドユーザを含む）」が 85.5%と最も高く、「経営者層の理解」が 71.2%とこれに続いている。

これに対し、従業員への情報セキュリティに関する教育・訓練の実施状況の関係についてクロス分析を行った。

| Q22 セキュリティ確保上の視点 ＼ Q43 教育・訓練 | 回答件数 | 定期的に実施している | | 時々実施している | | 実施を予定している | | 特に実施していない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 経営者層の理解 | 431 | 77 | 17.9 | 113 | 26.2 | 59 | 13.7 | 175 | 40.6 | 7 | 1.6 |
| 管理者の理解 | 240 | 53 | 22.1 | 58 | 24.2 | 30 | 12.5 | 97 | 40.4 | 2 | 0.8 |
| 担当者の理解 | 187 | 49 | 26.2 | 47 | 25.1 | 19 | 10.2 | 70 | 37.4 | 2 | 1.1 |
| 社内全体の理解 | 517 | 97 | 18.8 | 137 | 26.5 | 73 | 14.1 | 203 | 39.3 | 7 | 1.4 |
| 法規制の整備 | 87 | 28 | 32.2 | 21 | 24.1 | 10 | 11.5 | 27 | 31.0 | 1 | 1.1 |
| その他 | 2 | 0 | 0.0 | 0 | 0.0 | 1 | 50.0 | 1 | 50.0 | 0 | 0.0 |
| 無回答 | 5 | 0 | 0.0 | 0 | 0.0 | 2 | 40.0 | 2 | 40.0 | 1 | 20.0 |
| 計 | 605 | 101 | 16.7 | 155 | 25.6 | 85 | 14.0 | 254 | 42.0 | 10 | 1.7 |

Q43 の回答結果として、最も高いポイントが「特に実施していない」(42.0%) で、これに「時々実施している」(25.6%) が続いているが、Q22 との関係は以下のとおりであった。

| 重要な視点 | 1位<br>(特に実施していない) | 2位<br>(時々実施している) |
|---|---|---|
| 経営者層の理解 | 40.6 | 26.2 |
| 管理者の理解 | 40.4 | 24.2 |
| 担当者の理解 | 37.4 | 25.1 |
| 社内全体の理解 | 39.3 | 26.5 |
| 法規制の整備 | 31.0 | 24.1 |
| その他 | 50.0 | 0.0 |

「その他」を除くと、「時々実施している」が24.1%～26.5%であった。

社内各層の理解度を高めるために必要と思われる情報セキュリティの面からの教育・訓練については「特に実施していない」が高い割合となっている。

ただし、2番目に高い「時々実施している」と「定期的に実施している」の回答率をQ22からみると以下のような結果であった。

| 重要な視点 | 定期的に実施している | 時々実施している | 計 |
|---|---|---|---|
| 経営者層の理解 | 17.9 | 26.2 | 44.1 |
| 管理者の理解 | 22.1 | 24.2 | 46.3 |
| 担当者の理解 | 26.2 | 25.1 | 51.3 |
| 社内全体の理解 | 18.8 | 26.5 | 45.1 |
| 法規制の整備 | 32.2 | 24.1 | 56.3 |
| その他 | 0.0 | 0.0 | 0.0 |

「その他」を除いた「定期的に実施している」と「時々実施している」の合計からみると、いずれの重要な視点も「特に実施していない」を上回っていた。

### 3.4.3 Q44とのクロス集計

**Q44. 貴事業体では情報セキュリティの人材をどのように養成していますか。**

セキュリティ確保に重要な視点と情報セキュリティ人材養成の実施方法の関係についてクロス分析を行った。

| Q44 人材育成 / Q22 セキュリティ確保上の視点 | 回答件数 | 自社育成プログラムにより高度な人材育成を実施 | | 民間資格を利用して育成 | | 情報セキュリティアドミニストレータ試験を活用 | | 特に行っていない | | 必要ない | | 無回答 | | 複数回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 経営者層の理解 | 431 | 37 | 8.6 | 22 | 5.1 | 30 | 7.0 | 321 | 74.5 | 1 | 0.2 | 11 | 2.6 | 9 | 2.1 |
| 管理者の理解 | 240 | 21 | 8.8 | 16 | 6.7 | 14 | 5.8 | 174 | 72.5 | 1 | 0.4 | 6 | 2.5 | 8 | 3.3 |
| 担当者の理解 | 187 | 22 | 11.8 | 12 | 6.4 | 7 | 3.7 | 134 | 71.7 | 0 | 0.0 | 4 | 2.1 | 8 | 4.3 |
| 社内全体の理解 | 517 | 45 | 8.7 | 24 | 4.6 | 32 | 6.2 | 394 | 76.2 | 0 | 0.0 | 11 | 2.1 | 11 | 2.1 |
| 法規制の整備 | 87 | 10 | 11.5 | 5 | 5.7 | 4 | 4.6 | 58 | 66.7 | 1 | 1.1 | 3 | 3.4 | 6 | 6.9 |
| その他 | 2 | 0 | 0.0 | 1 | 50.0 | 0 | 0.0 | 1 | 50.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 5 | 0 | 0.0 | 0 | 0.0 | 1 | 20.0 | 2 | 40.0 | 0 | 0.0 | 2 | 40.0 | 0 | 0.0 |
| 計 | 605 | 47 | 7.8 | 29 | 4.8 | 38 | 6.3 | 463 | 76.5 | 2 | 0.3 | 15 | 2.5 | 11 | 1.8 |

Q44の回答結果は「特に行っていない」(76.5%) が非常に高いが、Q22との関係は以下のとおりであった。

| 重要な視点 | 1位 (特に行っていない) |
|---|---|
| 経営者層の理解 | 74.5 |
| 管理者の理解 | 72.5 |
| 担当者の理解 | 71.7 |
| 社内全体の | 76.2 |
| 法規制の整備 | 66.7 |
| その他 | 50.0 |

この結果からみると、基本的に重要な視点からみた情報セキュリティの人材養成としては、「特に行っていない」が圧倒的である。

また、「自社育成プログラムにより高度な人材育成を行っている」、「民間資格を利用して育成している」、「情報セキュリティアドミニストレータ試験を活用している」の回答率を情報セキュリティの確保にとり、重要な視点からみると、以下のとおりの結果であった。

| 重要な視点 | 自社育成プログラムにより育成 | 民間資格を利用して育成 | 情報セキュリティアドミニストレータ試験の活用 | 合計 |
|---|---|---|---|---|
| 経営者層の理解 | 8.6 | 5.1 | 7.0 | 20.7 |
| 管理者の理解 | 8.8 | 6.7 | 5.8 | 21.3 |
| 担当者の理解 | 11.8 | 6.4 | 3.7 | 21.9 |
| 社内全体の理解 | 8.7 | 4.6 | 6.2 | 19.5 |
| 法規制の整備 | 11.5 | 5.7 | 4.6 | 21.8 |
| その他 | 0.0 | 50.0 | 0.0 | 50.0 |

この結果からみると、「その他」が 50.0%と高いが、何らかの方法で情報セキュリティの人材育成を行っているのは 19.5%～21.9%となっている。

情報セキュリティの確保にとり、基本的に重要とする視点と従業員に対する教育・訓練の充実および情報セキュリティの人材育成との関係は特にないようである。

## 3．5　Q24のクロス集計

Q24－①．貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。
Q24－②．貴事業体では経営理念に基づく実施手続・規程類を定めていますか。

×Q46．貴事業体では過去１年間に不正アクセスの被害に遭われたことがありますか。
×Q50．情報価値の視点から機密度のランクを設定していますか。
×Q53．貴事業体では過去１年間にコンピュータウイルスに感染したことがありますか。
×Q58．（運用に関しアウトソーシングを利用している場合）アウトソーシング先を選定する場合、どのような観点から選定していますか。

組織のセキュリティ管理を向上させるためには、セキュリティポリシーをまず定め、それに従って実施基準を作成し、それを遵守するというアプローチが効果的とされているが、実際の調査結果から、この仮説を検証した。

### 3.5.1　Q46とのクロス集計

**Q46．貴事業体では過去１年間に不正アクセスの被害に遭われたことがありますか。**

ここでは、情報セキュリティポリシー、実施手続・規程類の策定状況と、不正アクセスの被害状況について分析した。

| Q46 不正アクセス被害 / Q24-①ポリシー | 回答件数 | 物理的なアクセス被害に遭った | | 論理的アクセス被害に遭った | | ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 定めている | 279 | 1 | 0.4 | 25 | 9.0 | 249 | 89.2 | 4 | 1.4 |
| 現在作成中である | 78 | 0 | 0.0 | 13 | 16.7 | 65 | 83.3 | 0 | 0.0 |
| 作成を検討している | 98 | 0 | 0.0 | 6 | 6.1 | 90 | 91.8 | 2 | 2.0 |
| 定めていない | 143 | 0 | 0.0 | 9 | 6.3 | 133 | 93.0 | 1 | 0.7 |
| 必要ない | 4 | 0 | 0.0 | 1 | 25.0 | 3 | 75.0 | 0 | 0.0 |
| 無回答 | 3 | 0 | 0.0 | 0 | 0.0 | 3 | 100.0 | 0 | 0.0 |
| 計 | 605 | 1 | 0.2 | 54 | 8.9 | 543 | 89.8 | 7 | 1.2 |

| Q46 不正アクセス被害 / Q24-② 実施手続・規程類 | 回答件数 | 物理的なアクセス被害に遭った | | 論理的アクセス被害に遭った | | ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 定めている | 211 | 1 | 0.5 | 20 | 9.5 | 187 | 88.6 | 3 | 1.4 |
| 現在作成中である | 125 | 0 | 0.0 | 19 | 15.2 | 106 | 84.8 | 0 | 0.0 |
| 作成を検討している | 111 | 0 | 0.0 | 7 | 6.3 | 101 | 91.0 | 3 | 2.7 |
| 定めていない | 146 | 0 | 0.0 | 7 | 4.8 | 138 | 94.5 | 1 | 0.7 |
| 必要ない | 4 | 0 | 0.0 | 1 | 25.0 | 3 | 75.0 | 0 | 0.0 |
| 無回答 | 8 | 0 | 0.0 | 0 | 0.0 | 8 | 100.0 | 0 | 0.0 |
| 計 | 605 | 1 | 0.2 | 54 | 8.9 | 543 | 89.8 | 7 | 1.2 |

実施手続・規程類について「必要ない」および「無回答」の回答数が著しく少ないので、これによるバラツキが大きいと考えられ、分析の対象から外して考えるべきである。

一方、「セキュリティポリシーを定めている」と「現在作成中である」に比べ、「作成を検討している」と「定めていない」の方が、論理的アクセス被害に遭った割合が低くなっている。普通に考えれば、セキュリティポリシーがある方が対策のレベルが高いので、論理的不正アクセスに対しても防御が進んでいるはずである。この原因は、論理的不正アクセスの被害に遭っても、回答者が不正アクセスを受けたことを認識しておらず、「知らぬが仏」状態にあるのではないかと考えられる。

### 3.5.2 Q50 とのクロス集計

**Q50. 情報価値の視点から機密度のランクを設定していますか。**

情報を守るためには、社内のすべての情報を同じように守るのではなく、その情報の重要度に応じた機密度ランク付けを行い、それに対応した機密保護を実施する必要がある。このランク付けを行わないと、すべての情報に対して非常に高い機密保護を実施し、利用性が著しく悪くなるか、機密保護対策として実施されるレベルが低く、重要な顧客情報の漏洩といった事態を招く結果となる。情報セキュリティポリシーと実施手続・規程類の策定状況と機密度ランクの設定および暗号化の利用について相関を取った。

| Q50 機密度ランク / Q24-①ポリシー | 回答件数 | ランクを設定し、暗号化している | | ランクは設定していないが、暗号化はしている | | ランクを設定しているが、暗号化はしていない | | 暗号化していない | | 無回答 | | 複数回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 279 | 29 | 10.4 | 22 | 7.9 | 108 | 38.7 | 110 | 39.4 | 10 | 3.6 | 0 | 0.0 |
| 現在作成中である | 78 | 1 | 1.3 | 11 | 14.1 | 12 | 15.4 | 53 | 67.9 | 0 | 0.0 | 1 | 1.3 |
| 作成を検討している | 98 | 6 | 6.1 | 12 | 12.2 | 15 | 15.3 | 62 | 63.3 | 3 | 3.1 | 0 | 0.0 |
| 定めていない | 143 | 1 | 0.7 | 14 | 9.8 | 7 | 4.9 | 113 | 79.0 | 8 | 5.6 | 0 | 0.0 |
| 必要ない | 4 | 0 | 0.0 | 0 | 0.0 | 1 | 25.0 | 3 | 75.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 3 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 2 | 66.7 | 1 | 33.3 | 0 | 0.0 |
| 計 | 605 | 37 | 6.1 | 59 | 9.8 | 143 | 23.6 | 343 | 56.7 | 22 | 3.6 | 1 | 0.2 |

| Q50 機密度ランク / Q24-② 実施手続・規程類 | 回答件数 | ランクを設定し、暗号化している | | ランクは設定していないが、暗号化はしている | | ランクを設定しているが、暗号化はしていない | | 暗号化していない | | 無回答 | | 複数回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 211 | 23 | 10.9 | 21 | 10.0 | 80 | 37.9 | 79 | 37.4 | 8 | 3.8 | 0 | 0.0 |
| 現在作成中である | 125 | 6 | 4.8 | 15 | 12.0 | 36 | 28.8 | 64 | 51.2 | 3 | 2.4 | 1 | 0.8 |
| 作成を検討している | 111 | 5 | 4.5 | 10 | 9.0 | 16 | 14.4 | 77 | 69.4 | 3 | 2.7 | 0 | 0.0 |
| 定めていない | 146 | 3 | 2.1 | 11 | 7.5 | 10 | 6.8 | 115 | 78.8 | 7 | 4.8 | 0 | 0.0 |
| 必要ない | 4 | 0 | 0.0 | 0 | 0.0 | 1 | 25.0 | 3 | 75.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 8 | 0 | 0.0 | 2 | 25.0 | 0 | 0.0 | 5 | 62.5 | 1 | 12.5 | 0 | 0.0 |
| 計 | 605 | 37 | 6.1 | 59 | 9.8 | 143 | 23.6 | 343 | 56.7 | 22 | 3.6 | 1 | 0.2 |

情報の機密度ランク付けについては、セキュリティポリシーを「定めている」事業体が49.1%であるのに対し、それ以外では「作成中」が16.7%、「検討中」が21.4%、「定めていない」では5.6%と大きな差がみられた。実施手続・規程類の策定状況についても、多少の数字の違いはあるものの同様の結果となった。これらの結果は、情報セキュリティポリシーと実施手続・規程類を定めていなければ、情報のランク付けが行われず、適切な情報保護も実行されないことを示している。

一方、暗号化については、セキュリティポリシーを「定めている」事業体が18.3%に対し、それ以外では「作成中」が15.4%、「検討中」が18.3%、「定めていない」では10.5%となった。この場合は、「定めている」～「検討中」までのグループと「定めていない」グループで大きな差がみられた。いずれにしろ、情報セキュリティポリシーと実施手続・規程類の整備、機密度のランク付け、暗号化の利用では非常に高い相関がみられた。

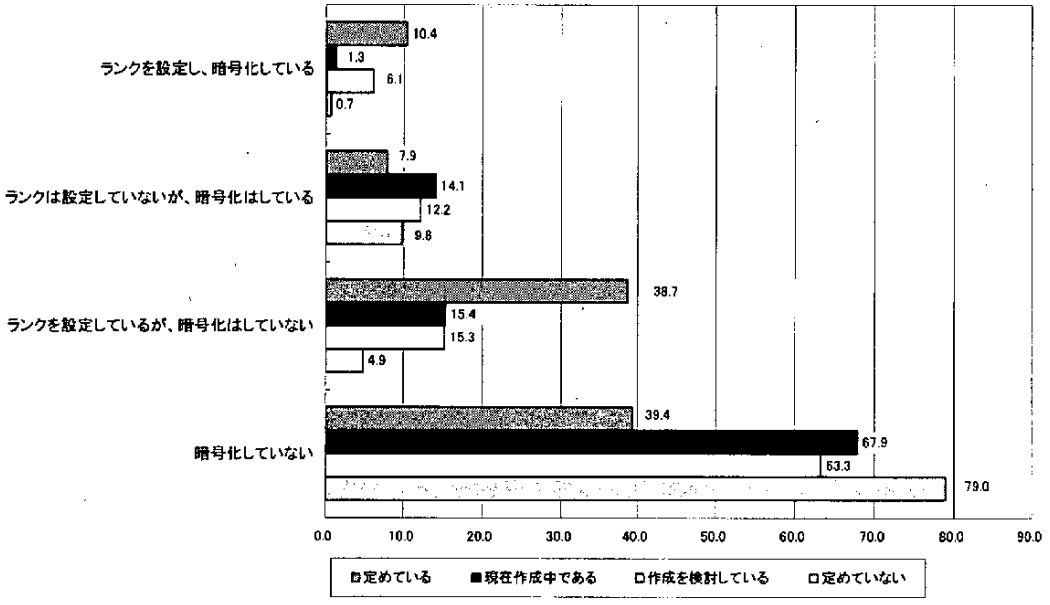



図3－5－1. 機密度ランク付けと情報セキュリティポリシーの策定状況の関係

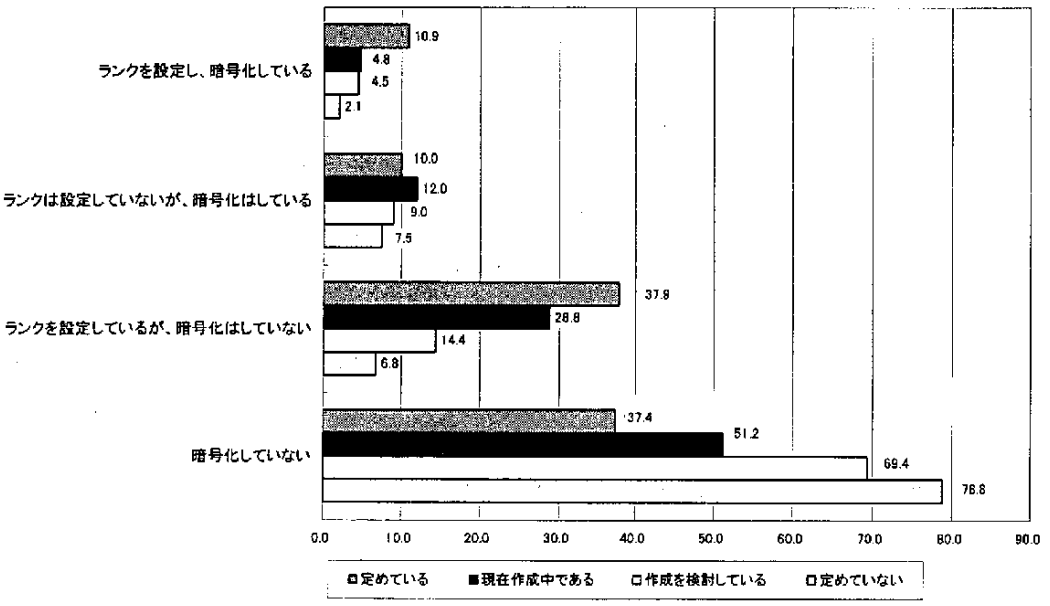



図3－5－2. 機密度ランク付けと実施手続・規程類の策定状況の関係

### 3.5.3 Q53 とのクロス集計

**Q53. 貴事業体では過去１年間にコンピュータウイルスに感染したことがありますか。**

コンピュータウイルスの被害についてはすでに一般にも広く知られているが、各事業体がそれをどの程度防御しているか、情報セキュリティポリシーと実施手続・規程類の策定状況との相関を取った。

| Q53 ウイルス被害 / Q24-①ポリシー | 回答件数 | ある | | ない | | 無回答 | |
|---|---|---|---|---|---|---|---|
| 定めている | 279 | 192 | 68.8 | 86 | 30.8 | 1 | 0.4 |
| 現在作成中である | 78 | 53 | 67.9 | 25 | 32.1 | 0 | 0.0 |
| 作成を検討している | 98 | 76 | 77.6 | 21 | 21.4 | 1 | 1.0 |
| 定めていない | 143 | 99 | 69.2 | 44 | 30.8 | 0 | 0.0 |
| 必要ない | 4 | 1 | 25.0 | 3 | 75.0 | 0 | 0.0 |
| 無回答 | 3 | 3 | 100.0 | 0 | 0.0 | 0 | 0.0 |
| 計 | 605 | 424 | 70.1 | 179 | 29.6 | 2 | 0.3 |

| Q53 ウイルス被害 / Q24-② 実施手続・規程類 | 回答件数 | ある | | ない | | 無回答 | |
|---|---|---|---|---|---|---|---|
| 定めている | 211 | 148 | 70.1 | 63 | 29.9 | 0 | 0.0 |
| 現在作成中である | 125 | 87 | 69.6 | 36 | 28.8 | 2 | 1.6 |
| 作成を検討している | 111 | 85 | 76.6 | 26 | 23.4 | 0 | 0.0 |
| 定めていない | 146 | 97 | 66.4 | 49 | 33.6 | 0 | 0.0 |
| 必要ない | 4 | 1 | 25.0 | 3 | 75.0 | 0 | 0.0 |
| 無回答 | 8 | 6 | 75.0 | 2 | 25.0 | 0 | 0.0 |
| 計 | 605 | 424 | 70.1 | 179 | 29.6 | 2 | 0.3 |

この結果からははっきりした相関はみられなかった。これは、平成 15 年に発生したウイルスが非常に感染力が強く、感染の広がるスピードが速かったために、ワクチンソフトのパターンファイルの対応が間に合わず、非常に進んだ対応をしていない事業体に感染が広がったためと考えられる。

### 3.5.4 Q58 とのクロス集計

**Q58. (運用に関しアウトソーシングを利用している場合) アウトソーシング先を選定する場合、どのような観点から選定していますか。**

情報システム業務におけるアウトソーシングの利用は多くの事業体がすでに実施しているが、アウトソーシング先を決定している時にどのような項目を重要視しているか、情報セキュリティポリシーと実施手続・規程類の策定状況との相関を取った。

| Q58 選定上の観点 / Q24-①ポリシー | 回答件数 | コスト | | 専門性 | | セキュリティ | | 品質 | | 開発した依頼会社をそのままメンテナンス先に選定 | | その他 | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 164 | 113 | 68.9 | 110 | 67.1 | 74 | 45.1 | 108 | 65.9 | 24 | 14.6 | 12 | 7.3 | 6 | 3.7 |
| 現在作成中である | 42 | 28 | 66.7 | 32 | 76.2 | 21 | 50.0 | 24 | 57.1 | 8 | 19.0 | 0 | 0.0 | 0 | 0.0 |
| 作成を検討している | 46 | 32 | 69.6 | 23 | 50.0 | 20 | 43.5 | 30 | 65.2 | 10 | 21.7 | 1 | 2.2 | 1 | 2.2 |
| 定めていない | 42 | 25 | 59.5 | 19 | 45.2 | 11 | 26.2 | 19 | 45.2 | 9 | 21.4 | 0 | 0.0 | 4 | 9.5 |
| 必要ない | 3 | 1 | 33.3 | 2 | 66.7 | 0 | 0.0 | 0 | 0.0 | 1 | 33.3 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 3 | 2 | 66.7 | 2 | 66.7 | 0 | 0.0 | 2 | 66.7 | 1 | 33.3 | 0 | 0.0 | 0 | 0.0 |
| 計 | 300 | 201 | 67.0 | 188 | 62.7 | 126 | 42.0 | 183 | 61.0 | 53 | 17.7 | 13 | 4.3 | 11 | 3.7 |

| Q58 選定上の観点 / Q24-② 実施手続・規程類 | 回答件数 | コスト | | 専門性 | | セキュリティ | | 品質 | | 開発した依頼会社をそのままメンテナンス先に選定 | | その他 | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 122 | 85 | 69.7 | 83 | 68.0 | 55 | 45.1 | 82 | 67.2 | 15 | 12.3 | 9 | 7.4 | 4 | 3.3 |
| 現在作成中である | 75 | 48 | 64.0 | 54 | 72.0 | 37 | 49.3 | 47 | 62.7 | 13 | 17.3 | 2 | 2.7 | 2 | 2.7 |
| 作成を検討している | 50 | 37 | 74.0 | 27 | 54.0 | 23 | 46.0 | 30 | 60.0 | 11 | 22.0 | 1 | 2.0 | 1 | 2.0 |
| 定めていない | 45 | 28 | 62.2 | 19 | 42.2 | 10 | 22.2 | 22 | 48.9 | 12 | 26.7 | 1 | 2.2 | 3 | 6.7 |
| 必要ない | 3 | 1 | 33.3 | 2 | 66.7 | 0 | 0.0 | 0 | 0.0 | 1 | 33.3 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 5 | 2 | 40.0 | 3 | 60.0 | 1 | 20.0 | 2 | 40.0 | 1 | 20.0 | 0 | 0.0 | 1 | 20.0 |
| 計 | 300 | 201 | 67.0 | 188 | 62.7 | 126 | 42.0 | 183 | 61.0 | 53 | 17.7 | 13 | 4.3 | 11 | 3.7 |

この結果、セキュリティについて、情報セキュリティポリシーを「定めている・作成中・検討中」のグループ（平均 46.2%）と、「定めていない」グループ（26.2%）では、非常に大きな差がみられた。同様に実施手続・規程類のセキュリティについても、「定めている・作成中・検討中」のグループ（平均 46.8%）と「定めていない」グループ（22.2%）で非常に大きな差がみられた。つまり、情報セキュリティポリシーと実施手続・規程類が整備されていない事業体では、アウトソーサを選ぶ基準としてセキュリティが重視されないので、アウトソーサからの情報漏洩のリスクが高いと考えられる。また、専門性や品質（サービスレベル）についてもこの２つのグループ間でセキュリティほど顕著ではないが、相関がみられる。これは、一般的に情報セキュリティポリシーと実施手続・規程類が整備されている事業体の方が、情報システムの内部管理の水準が高いためと考えられる。

## 3．6　Q27のクロス集計

Q27－①ネットワークの管理について、責任を有する担当者を定めていますか。
Q27－②情報システムの管理について、責任を有する担当者を定めていますか。
Q27－③情報セキュリティの管理について、責任を有する担当者を定めていますか。

×Q24－①貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。
×Q24－②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。

### 3.6.1　Q24-①とのクロス集計

**Q24－①貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。**

ネットワーク管理者、情報システム管理者、情報セキュリティ管理者の設置状況と情報セキュリティポリシー策定状況との関係を調べるためにクロス分析を実施した。

①ネットワーク管理者

| Q24-①ポリシー / Q27-① ネットワーク管理者 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 504 | 268 | 53.2 | 59 | 11.7 | 75 | 14.9 | 99 | 19.6 | 2 | 0.4 | 1 | 0.2 |
| 設置を検討している | 37 | 4 | 10.8 | 15 | 40.5 | 12 | 32.4 | 6 | 16.2 | 0 | 0.0 | 0 | 0.0 |
| 定めていない | 59 | 5 | 8.5 | 3 | 5.1 | 11 | 18.6 | 38 | 64.4 | 2 | 3.4 | 0 | 0.0 |
| 必要ない | 0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 5 | 2 | 40.0 | 1 | 20.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 2 | 40.0 |
| 計 | 605 | 279 | 46.1 | 78 | 12.9 | 98 | 16.2 | 143 | 23.6 | 4 | 0.7 | 3 | 0.5 |

ネットワーク管理者を定めている事業体では、情報セキュリティポリシーを「定めている」割合が53.2%、管理者の設置を検討している事業体では、情報セキュリティポリシーを「現在作成中」の割合が40.5%である。また、管理者を定めていない事業体では、情報セキュリティポリシーを「定めていない」割合が高く64.4%となっている。すなわち、情報セキュリティポリシーの作成とネットワーク管理者の設置には強い相関があることがわかる。

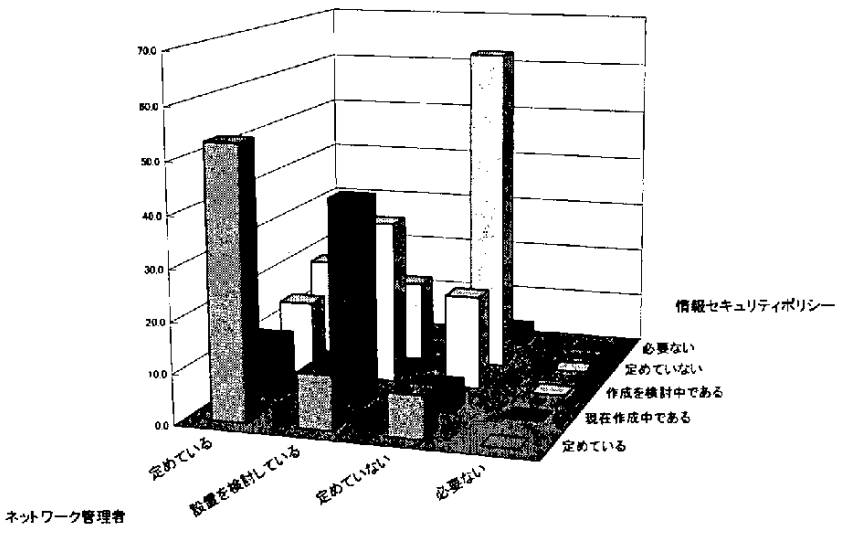



図3－6－1．ネットワーク管理者の設置状況と情報セキュリティポリシーの策定状況の関係

②情報システム管理者

| Q24-①ポリシー / Q27-② 情報システム管理者 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 487 | 263 | 54.0 | 55 | 11.3 | 69 | 14.2 | 97 | 19.9 | 2 | 0.4 | 1 | 0.2 |
| 設置を検討している | 45 | 6 | 13.3 | 17 | 37.8 | 16 | 35.6 | 6 | 13.3 | 0 | 0.0 | 0 | 0.0 |
| 定めていない | 67 | 7 | 10.4 | 5 | 7.5 | 13 | 19.4 | 40 | 59.7 | 2 | 3.0 | 0 | 0.0 |
| 必要ない | 0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 6 | 3 | 50.0 | 1 | 16.7 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 2 | 33.3 |
| 計 | 605 | 279 | 46.1 | 78 | 12.9 | 98 | 16.2 | 143 | 23.6 | 4 | 0.7 | 3 | 0.5 |

情報システム管理者を定めている事業体では、情報セキュリティポリシーを「定めている」割合が54.0%、管理者の設置を検討している事業体では、情報セキュリティポリシーを「現在作成中」である割合が37.8%である。また、管理者を定めていない事業体では、情報セキュリティポリシーを「定めていない」割合が高く、59.7%となっている。すなわち、情報セキュリティポリシーの作成と情報システム管理者の設置には強い相関があることがわかる。

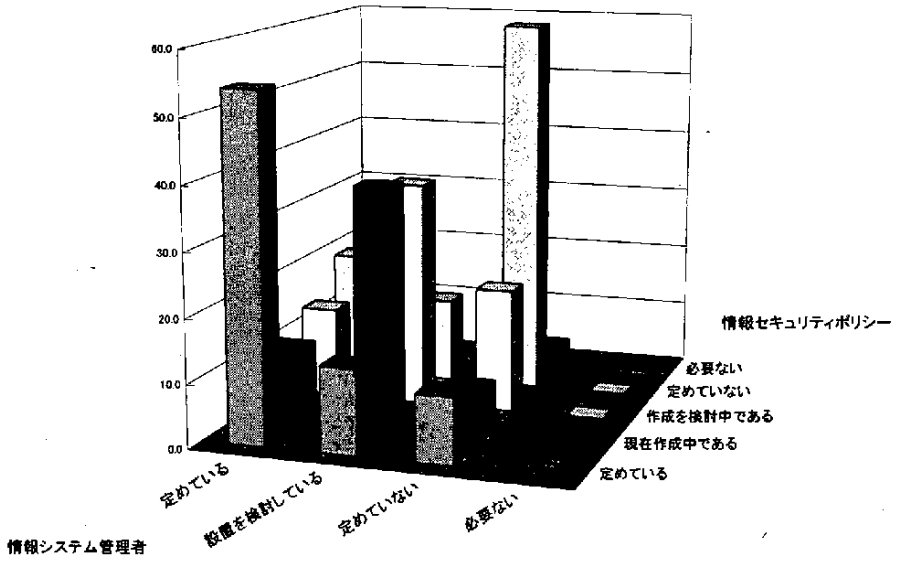



図3－6－2. 情報システム管理者の設置状況と情報セキュリティポリシーの策定状況の関係

③情報セキュリティ管理者

| Q24-①ポリシー / Q27-③ 情報セキュリティ管理者 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 396 | 255 | 64.4 | 41 | 10.4 | 46 | 11.6 | 52 | 13.1 | 1 | 0.3 | 1 | 0.3 |
| 設置を検討している | 88 | 12 | 13.6 | 30 | 34.1 | 30 | 34.1 | 16 | 18.2 | 0 | 0.0 | 0 | 0.0 |
| 定めていない | 116 | 10 | 8.6 | 6 | 5.2 | 22 | 19.0 | 75 | 64.7 | 3 | 2.6 | 0 | 0.0 |
| 必要ない | 0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 5 | 2 | 40.0 | 1 | 20.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 2 | 40.0 |
| 計 | 396 | 255 | 64.4 | 41 | 10.4 | 46 | 11.6 | 52 | 13.1 | 1 | 0.3 | 1 | 0.3 |

情報セキュリティ管理者を定めている事業体では、情報セキュリティポリシーを「定めている」割合が64.4%、管理者の設置を検討している事業体では、情報セキュリティポリシーを「現在作成中」、「作成を検討中」の割合がそれぞれ同率の34.1%である。また、管理者を定めていない事業体では、情報セキュリティポリシーを「定めていない」割合が高く64.7%となっている。すなわち、情報セキュリティポリシーの作成と情報セキュリティ管理者の設置には強い相関があることがわかる。

なお、各管理者を設置している場合のセキュリティポリシー策定率は、情報セキュリティ管理者（64.4%）がもっとも相関が大きいことがわかる。

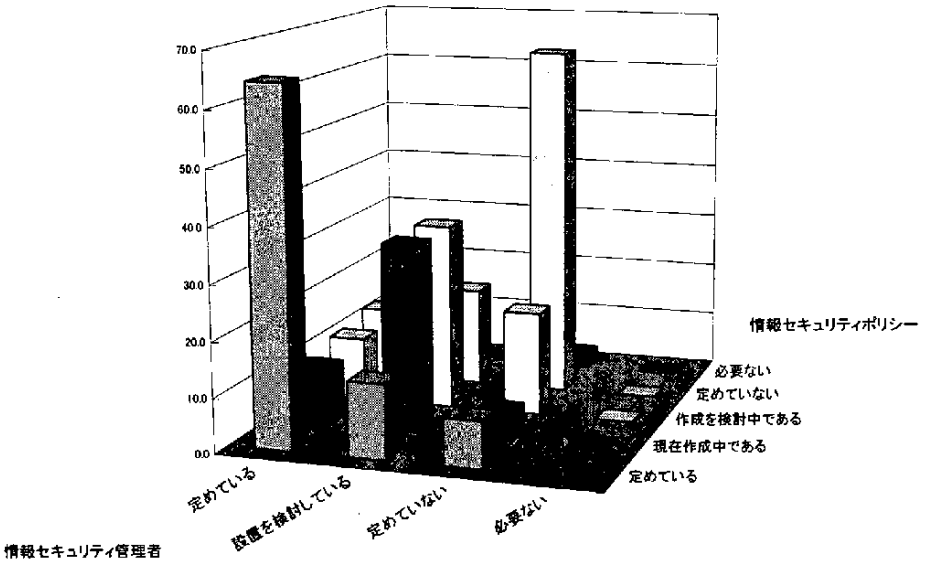



図3－6－3. 情報セキュリティ管理者の設置状況と情報セキュリティポリシーの策定状況の関係

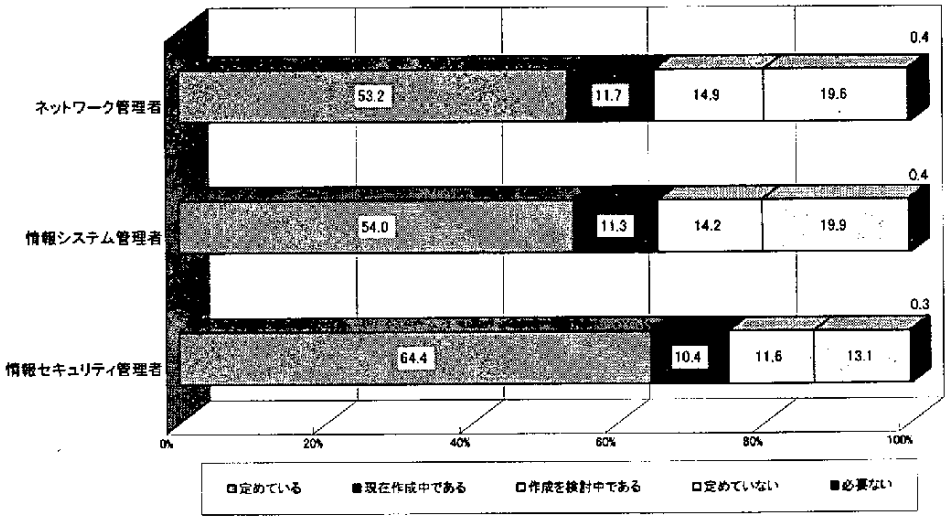



図3－6－4. 管理者の設置とセキュリティポリシー、実施手続・規程類の策定状況の関係

### 3.6.2 Q24-②とのクロス集計

**Q24－②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。**

ネットワーク管理者、情報システム管理者、情報セキュリティ管理者の設置状況と実施手続・規程類の策定状況との関係を調べるためにクロス分析を実施した。

①ネットワーク管理者

| Q24-②実施手続・規程類 / Q27-① ネットワーク管理者 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 504 | 199 | 39.5 | 109 | 21.6 | 89 | 17.7 | 99 | 19.6 | 2 | 0.4 | 6 | 1.2 |
| 設置を検討している | 37 | 4 | 10.8 | 14 | 37.8 | 12 | 32.4 | 7 | 18.9 | 0 | 0.0 | 0 | 0.0 |
| 定めていない | 59 | 5 | 8.5 | 2 | 3.4 | 10 | 16.9 | 40 | 67.8 | 2 | 3.4 | 0 | 0.0 |
| 必要ない | 0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 5 | 3 | 60.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 2 | 40.0 |
| 計 | 605 | 211 | 34.9 | 125 | 20.7 | 111 | 18.3 | 146 | 24.1 | 4 | 0.7 | 8 | 1.3 |

ネットワーク管理者を定めている事業体では、実施手続・規程類を「定めている」割合が39.5%、管理者の設置を検討している事業体では、実施手続・規程類を「現在作成中」の割合が37.8%である。また、管理者を定めていない事業体では、実施手続・規程類を「定めていない」割合が高く67.8%となっている。すなわち、実施手続・規程類の作成とネットワーク管理者の設置は、情報セキュリティポリシーの作成の場合と同様に相関があることがわかる。

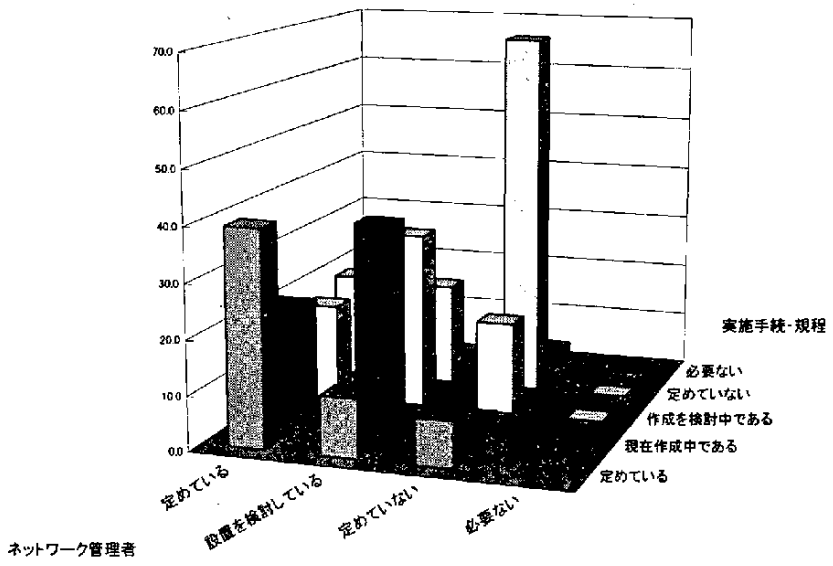



図3－6－5. ネットワーク管理者の設置状況と実施手続・規程類の策定状況の関係

②情報システム管理者

| Q24-②実施手続・規程類 / Q27-② 情報システム管理者 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 487 | 196 | 40.2 | 104 | 21.4 | 84 | 17.2 | 96 | 19.7 | 2 | 0.4 | 5 | 1.0 |
| 設置を検討している | 45 | 5 | 11.1 | 17 | 37.8 | 16 | 35.6 | 7 | 15.6 | 0 | 0.0 | 0 | 0.0 |
| 定めていない | 67 | 6 | 9.0 | 4 | 6.0 | 11 | 16.4 | 43 | 64.2 | 2 | 3.0 | 1 | 1.5 |
| 必要ない | 0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 6 | 4 | 66.7 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 2 | 33.3 |
| 計 | 605 | 211 | 34.9 | 125 | 20.7 | 111 | 18.3 | 146 | 24.1 | 4 | 0.7 | 8 | 1.3 |

情報システム管理者を定めている事業体では、実施手続・規程類を「定めている」割合が40.2%、管理者の設置を検討している事業体では、実施手続・規程類を「現在作成中」の割合が37.8%である。また、管理者を定めていない事業体では、実施手続・規程類を「定めていない」割合が高く64.2%となっている。すなわち、実施手続・規程類の作成と情報システム管理者の設置は、情報セキュリティポリシーの作成の場合と同様に相関があることがわかる。

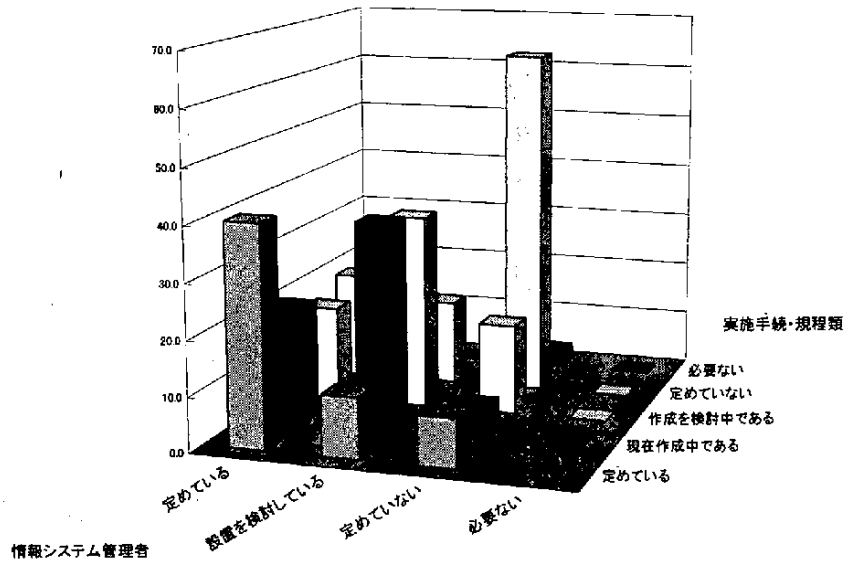



図3－6－6. 情報システム管理者の設置状況と実施手続・規程類の策定状況の関係

③情報セキュリティ管理者

| Q24-②実施手続・規程類 / Q27-③情報セキュリティ管理者 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定めている | 396 | 189 | 47.7 | 89 | 22.5 | 62 | 15.7 | 51 | 12.9 | 1 | 0.3 | 4 | 1.0 |
| 設置を検討している | 88 | 10 | 11.4 | 30 | 34.1 | 29 | 33.0 | 18 | 20.5 | 0 | 0.0 | 1 | 1.1 |
| 定めていない | 116 | 9 | 7.8 | 6 | 5.2 | 20 | 17.2 | 77 | 66.4 | 3 | 2.6 | 1 | 0.9 |
| 必要ない | 0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 5 | 3 | 60.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 2 | 40.0 |
| 計 | 605 | 211 | 34.9 | 125 | 20.7 | 111 | 18.3 | 146 | 24.1 | 4 | 0.7 | 8 | 1.3 |

情報セキュリティ管理者を定めている事業体では、実施手続・規程類を「定めていている」割合が47.7%、管理者の設置を検討している事業体では、実施手続・規程類を「現在作成中」の割合が34.1%である。また管理者を定めていない事業体では、実施手続・規程類を「定めていない」割合が高く66.4%となっている。すなわち、実施手続・規程類の作成と情報セキュリティ管理者の設置は、情報セキュリティポリシーの作成の場合と同様に相関があることがわかる。

なお、各管理者を設置している場合の実施手続・規程類の策定率は、情報セキュリティポリシー同様、情報セキュリティ管理者（47.7%）がもっとも相関が大きいことがわかる。

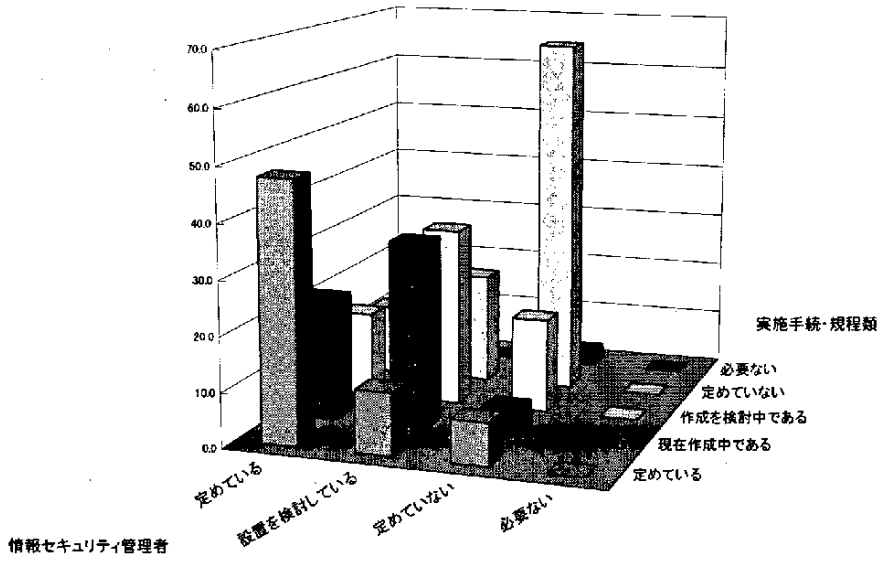



図3－6－7. 情報セキュリティ管理者の設置状況と実施手続・規程類の策定状況の関係

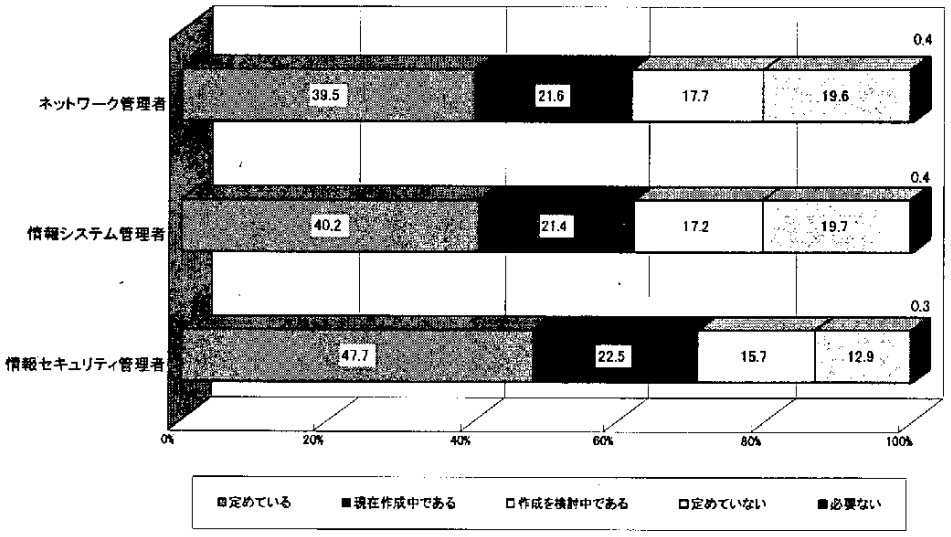



図3－6－8. 管理者の設置と実施手続・規程類の策定状況の関係

## 3．7　Q29のクロス集計

Q29. 情報セキュリティ要素 1～10 のうち、貴事業体にとって重要と思われる要素を3つ選び、下の回答欄に優先順位をつけて記入して下さい。

### 3.7.1　Q29のクロス集計

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

表３－７－１．第１位と第２位の選択件数　（件）

| 情報セキュリティ要素 | | 1位 | 2位 |
|---|---|---|---|
| 1 | 情報セキュリティポリシー（経営者の積極的な関与） | 199 | 37 |
| 2 | 情報セキュリティ組織（情報セキュリティの推進組織の構築と活動） | 63 | 102 |
| 3 | 情報資産の分類および管理（情報資産のリスク評価とそれによる重要度の分類） | 43 | 73 |
| 4 | 人的セキュリティ（役職員への教育訓練や内部規則の策定など） | 93 | 106 |
| 5 | 物理的および環境的セキュリティ（入退室管理や安全区画の構築など） | 13 | 28 |
| 6 | 通信および運用管理（ネットワークの管理、ウイルス対策、ログ管理など） | 67 | 97 |
| 7 | アクセス制御（IDとパスワード管理、不正アクセス対策など） | 22 | 65 |
| 8 | システム開発およびメンテナンス（開発環境のセキュリティ、ライブラリ管理運用など） | 6 | 14 |
| 9 | 事業継続計画（災害対策、障害対策など） | 58 | 49 |
| 10 | 準拠（法律遵守、システム監査など） | 21 | 12 |

表３－７－２．各要素別第２位選択項目

第1位「情報セキュリティポリシー」の場合

| | | |
|---|---|---|
| 情報セキュリティ組織 | 75 | 37.7 |
| 情報資産の分類および管理 | 33 | 16.6 |
| 人的セキュリティ | 47 | 23.6 |
| 物理的および環境的セキュリティ | 5 | 2.5 |
| 通信および運用管理 | 17 | 8.5 |
| アクセス制御 | 7 | 3.5 |
| システム開発およびメンテナンス | 3 | 1.5 |
| 事業継続計画 | 8 | 4.0 |
| 準拠 | 4 | 2.0 |

第1位「情報セキュリティ組織」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 4 | 6.3 |
| 情報資産の分類および管理 | 14 | 22.2 |
| 人的セキュリティ | 13 | 20.6 |
| 物理的および環境的セキュリティ | 2 | 3.2 |
| 通信および運用管理 | 17 | 27.0 |
| アクセス制御 | 4 | 6.3 |
| システム開発およびメンテナンス | 1 | 1.6 |
| 事業継続計画 | 8 | 12.7 |
| 準拠 | 0 | 0.0 |

第1位「情報資産の分類および管理」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 6 | 14.0 |
| 情報セキュリティ組織 | 6 | 14.0 |
| 人的セキュリティ | 12 | 27.9 |
| 物理的および環境的セキュリティ | 2 | 4.7 |
| 通信および運用管理 | 6 | 14.0 |
| アクセス制御 | 2 | 4.7 |
| システム開発およびメンテナンス | 2 | 4.7 |
| 事業継続計画 | 7 | 16.3 |
| 準拠 | 0 | 0.0 |

第1位「人的セキュリティ」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 13 | 14.0 |
| 情報セキュリティ組織 | 10 | 10.8 |
| 情報資産の分類および管理 | 9 | 9.7 |
| 物理的および環境的セキュリティ | 10 | 10.8 |
| 通信および運用管理 | 23 | 24.7 |
| アクセス制御 | 16 | 17.2 |
| システム開発およびメンテナンス | 1 | 1.1 |
| 事業継続計画 | 8 | 8.6 |
| 準拠 | 2 | 2.2 |

第1位「物理的および環境的セキュリティ」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 0 | 0.0 |
| 情報セキュリティ組織 | 1 | 7.7 |
| 情報資産の分類および管理 | 1 | 7.7 |
| 人的セキュリティ | 3 | 23.1 |
| 通信および運用管理 | 3 | 23.1 |
| アクセス制御 | 5 | 38.5 |
| システム開発およびメンテナンス | 0 | 0.0 |
| 事業継続計画 | 0 | 0.0 |
| 準拠 | 0 | 0.0 |

第1位「通信および環境的セキュリティ」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 2 | 3.0 |
| 情報セキュリティ組織 | 6 | 9.0 |
| 情報資産の分類および管理 | 3 | 4.5 |
| 人的セキュリティ | 16 | 23.9 |
| 物理的および環境的セキュリティ | 3 | 4.5 |
| アクセス制御 | 24 | 35.8 |
| システム開発およびメンテナンス | 2 | 3.0 |
| 事業継続計画 | 10 | 14.9 |
| 準拠 | 1 | 1.5 |

第1位「アクセス制御」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 0 | 0.0 |
| 情報セキュリティ組織 | 2 | 9.1 |
| 情報資産の分類および管理 | 2 | 9.1 |
| 人的セキュリティ | 4 | 18.2 |
| 物理的および環境的セキュリティ | 3 | 13.6 |
| 通信および運用管理 | 8 | 36.4 |
| システム開発およびメンテナンス | 1 | 4.5 |
| 事業継続計画 | 2 | 9.1 |
| 準拠 | 0 | 0.0 |

第1位「システム開発およびメンテナンス」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 0 | 0.0 |
| 情報セキュリティ組織 | 0 | 0.0 |
| 情報資産の分類および管理 | 0 | 0.0 |
| 人的セキュリティ | 0 | 0.0 |
| 物理的および環境的セキュリティ | 1 | 16.7 |
| 通信および運用管理 | 2 | 33.3 |
| アクセス制御 | 2 | 33.3 |
| 事業継続計画 | 1 | 16.7 |
| 準拠 | 0 | 0.0 |

第1位「事業継続計画」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 7 | 12.1 |
| 情報セキュリティ組織 | 2 | 3.4 |
| 情報資産の分類および管理 | 9 | 15.5 |
| 人的セキュリティ | 7 | 12.1 |
| 物理的および環境的セキュリティ | 0 | 0.0 |
| 通信および運用管理 | 19 | 32.8 |
| アクセス制御 | 5 | 8.6 |
| システム開発およびメンテナンス | 4 | 6.9 |
| 準拠 | 5 | 8.6 |

第1位「準拠」の場合

| | | |
|---|---|---|
| 情報セキュリティポリシー | 5 | 23.8 |
| 情報セキュリティ組織 | 0 | 0.0 |
| 情報資産の分類および管理 | 2 | 9.5 |
| 人的セキュリティ | 4 | 19.0 |
| 物理的および環境的セキュリティ | 2 | 9.5 |
| 通信および運用管理 | 2 | 9.5 |
| アクセス制御 | 0 | 0.0 |
| システム開発およびメンテナンス | 0 | 0.0 |
| 事業継続計画 | 5 | 23.8 |

| 第1位＼第2位 | 情報セキュリティポリシー | 情報セキュリティ組織 | 情報資産の分類／管理 | 人的セキュリティ | 物理的／環境的セキュリティ | 通信／運用管理 | アクセス制御 | システム開発／メンテナンス | 事業継続計画 | 準拠 |
|---|---|---|---|---|---|---|---|---|---|---|
| 情報セキュリティポリシー | | 75 | 33 | 47 | 5 | 17 | 7 | 3 | 8 | 4 |
| 情報セキュリティ組織 | 4 | | 14 | 13 | 2 | 17 | 4 | 1 | 8 | 0 |
| 情報資産の分類および管理 | 6 | 6 | | 12 | 2 | 6 | 2 | 2 | 7 | 0 |
| 人的セキュリティ | 13 | 10 | 9 | | 10 | 23 | 16 | 1 | 8 | 2 |
| 物理的および環境的セキュリティ | 0 | 1 | 1 | 3 | | 3 | 5 | 0 | 0 | 0 |
| 通信および運用管理 | 2 | 6 | 3 | 16 | 3 | | 24 | 2 | 10 | 1 |
| アクセス制御 | 0 | 2 | 2 | 4 | 3 | 8 | | 1 | 2 | 0 |
| システム開発およびメンテナンス | 0 | 0 | 0 | 0 | 1 | 2 | 2 | | 1 | 0 |
| 事業継続計画 | 7 | 2 | 9 | 7 | 0 | 19 | 5 | 4 | | 5 |
| 準拠 | 5 | 0 | 2 | 4 | 2 | 2 | 0 | 0 | 5 | |

（1）選択の組合せの上位からの分析

前回調査に引き続き、今回も第1位の多い順にどのようであったかを確認する。1番多い選択は「情報セキュリティポリシー（199件）」であった。2番は「人的セキュリティ（93件）」、3番に「通信および運用管理（67件）」である。

次に第2位の選択をみると、1番が「人的セキュリティ(106)件」、2番が「情報セキュリティ組織（102件）」、3番が「通信および運用管理（97件）」であり、「情報セキュリティポリシー」は前回同様37件と第2位での選択が少ない。ちなみに前回は1番多い選択は「情報セキュリティポリシー(219件)」であった。2番は「通信および運用管理（74件）」、3番に「情報セキュリティ組織」である。第2位の選択をみると1番多数が「通信および運用管理（122件）」、2番が「情報セキュリティ組織（99件）」、3番が「人的セキュリティ（93件）」であり、「情報セキュリティポリシー」は47件と第2位での選択が少なかった。

前回と比較して「通信および運用管理」はコンピュータウイルスがあたり前になったからか、順位が下がり、かわって「人的セキュリティ」が重要度を増していることがわかる。

これら第1位および第2位の組合せの分析で何がわかるかをみることとする。

1位－2位の選択で多かった組合せは次のものがある。一番多かった選択は第1位に「情報セキュリティポリシー」を選択し第2位に「情報セキュリティ組織」を選択したもので75件を数え、これは今回の分析の回答件数585件中、12.8%をしめる。次は第1位に「情報セキュリティポリシー」を選択し、第2位に「人的セキュリティ」を選択した組合せで47件、全体の8.0%を占める。3番目は「情報セキュリティポリシー」と「情報資産の分類および管理」の33件でこれも全体の5.6%を占める。第1位に情報セキュリティポリシーを選択する割合が多いため、上位3つまでが情報セキュリティポリシー関係であることは前回同様である。

前回は、一番多かった選択は第1位に「情報セキュリティポリシー」を選択し第2位に「情報セキ

ュリティ組織」を選択したもので70件を数え、これは今回の分析の回答件数604件中、11.6%をしめる。次は第1位に「情報セキュリティポリシー」を選択し、第2位に「人的セキュリティ」を選択した組合せで44件、全体の7.3%を占める。3番目は「情報セキュリティポリシー」と「通信および運用管理」の39件でこれも全体の6.5%を占める。

前回と比較すると、上位2つは同様であるが、「通信および運用管理」が減少しその代わりに「情報資産の分類および管理」が3位に入ってきている。ここでもウイルス対策などが一時に比較すると少し対応が標準化され落ち着いてきていることがうかがえる。

さらにみていくと、第四番目には情報セキュリティポリシーからの選択ではなく「通信および運用管理」と「アクセス制御」の組合せで24件、全体の4.1%（前回4.8%）となっている。これは第1位、第2位、第3位の単独での分析からもうかがえるように、情報セキュリティポリシーなどの経営的概念からの選択をするグループのほかに、実際のウイルス対策やパスワード管理、ハッカー対策などの実務を重視している選択者が一定程度存在していることを裏づけており、少なくなったとはいえ前回同様実務的な選択がされている状況がある。

5番目は「人的セキュリティ」と「通信および運用管理」23件、3.9%となっており、前回調査と異なり情報セキュリティポリシーからの選択はなく、今年重要視されている「人的セキュリティ」の項目が現れている。

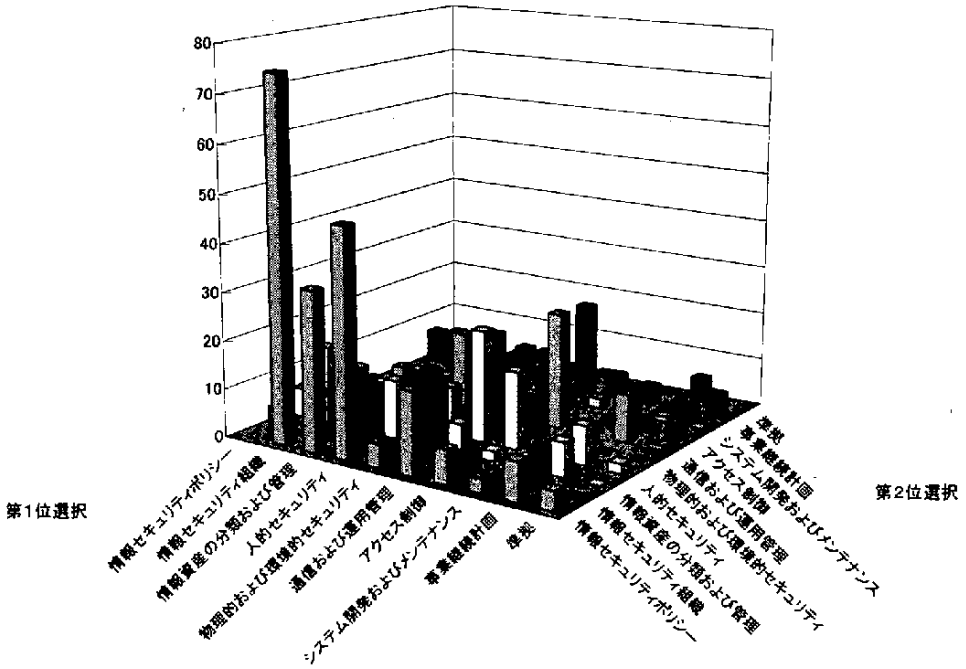



図3－7－1. 情報セキュリティ要素1位と2位の関係

（2）情報セキュリティポリシーの選択の特異性

第1位に圧倒的に指示されている「情報セキュリティポリシー」であるが、第2位での選択が少ないという結果は前回同様となった。「情報セキュリティ組織」から「準拠」までの要素ごとに第2位に何を選択したかをみると、「準拠」で第1位の選択となっているが、その他は第2位として選択されていない。「準拠」を第1位に選択したグループが第2位に「情報セキュリティポリシー」を選択することはガバナンスや内部統制を重んじることから望ましいと考えられるが、それ以外の選択を行ったところからは第2番がセキュリティポリシーではないことは改めて着目される。

表３－７－３．第１位、第２位を選択した要素の順番

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

表 3-7-3 からいえることは、前回同様第１位には１位から３位までの総合計で 50％を越す圧倒的な指示を得た「情報セキュリティポリシー」であるが、他の選択を選んだグループからは必ずしも多くの指示を得られていないことがわかる。一番多い選択は前回同様「通信および運用管理」であり、「情報セキュリティポリシー」と「準拠」を除き上位３つ以内に選択されている。

前回、経営的には情報セキュリティなどの要素が重要としながらも実務的にはウイルス対策などに追われている様子がうかがえるとしたが今年も同様である。次に多い選択は１位が多いか幅広く選択されているかの観点で評価が異なるが、「アクセス制御」と「人的セキュリティ」がある。「アクセス制御」は「通信および運用管理」、「物理的および環境的セキュリティ」、「システム開発およびメンテナンス」で第１位となっている。実務的な面からの評価がされている。一方、「人的セキュリティ」は「情報資産の分類および管理」では１番多い選択であり、また「情報セキュリティポリシー」、「物理的および環境的セキュリティ」、「通信および運用管理」、「アクセス制御」では２番目に多い選択である。前回と比較すると「人的セキュリティ」が３位までに選択されるところが増えている。これも実務的に規程を作成し教育を行うなどという、実務面で進捗していることの表れの可能性がある。

（３）選択の２つのグループ

前回同様選択の様子をみると、２つのグループがあるようにみえる。１つは「情報セキュリティポリシー」、「情報セキュリティ組織」、「情報資産の分類および管理」、「人的セキュリティ」など経営的要素を選択するグループである。（数は少ないが「事業継続計画」、「準拠」もこのグループに含まれる可能性が高い）

もう１つは、「通信および運用管理」、「アクセス制御」（数は少ないが「物理的および環境的セキュ

リティ」、「システム開発およびメンテナンス」もこちらに入ると考えられる）のグループである。

一つ目のグループは、その中の多い組合せをみていくと、「情報セキュリティポリシー－情報セキュリティ組織」（75 件）、「情報セキュリティポリシー－人的セキュリティ」（47 件）、「情報セキュリティポリシー－情報資産の分類および管理」（33 件）、「情報セキュリティ組織－人的セキュリティ」（13 件）、「情報セキュリティ組織－情報資産の分類および管理」（14 件）、「人的セキュリティー－情報セキュリティポリシー」（13 件）などがあり、経営的な観点、組織、組織による資産管理、教育などの人的要素を重視している。前回は「情報セキュリティポリシー－情報セキュリティ組織」、「情報セキュリティポリシー－人的セキュリティ」、「情報セキュリティポリシー－情報資産の分類および管理」、「情報セキュリティ組織－人的セキュリティ」、「情報セキュリティ組織－情報資産の分類および管理」、「情報セキュリティ組織－情報セキュリティポリシー」などがあった。

もう一つのグループは、これも前回同様「通信－アクセス制御」（24 件）、「アクセス制御－通信および運用管理」（８件）の相互の組合せであり、実務的にウイルス対策、ハッカー対策などを重視している。また「物理的および環境的セキュリティ」では「アクセス制御」と「通信および運用管理」が１位、２位であり。「システム開発およびメンテナンス」は「通信および運用管理」と「アクセス制御」が同率１位であり、これを含めたグループが実務者の対応状況を反映していると考えられる。

（４）その他の特徴

第２位の２番目に多い選択は「情報セキュリティ組織」であったが、前回調査ではその選択の大半が「情報セキュリティポリシー」を第１位に選択したグループからの支持であり、その他の選択をしたグループからはあまり支持が高くない。２番目に選択したグループはなく、３番目に選択があったのが「人的セキュリティ」、「物理的および環境的セキュリティ」および「システム開発およびメンテナンス」の３つである。今回も第２位の２番目に多い選択は「情報セキュリティ組織」であるが、これはその選択の大半が「情報セキュリティポリシー」を第一位に選択した群からの支持（75 件）であり、その他の選択をしたグループからはあまり支持が高くない。２番目に選択したグループはなく３番目に選択があったのが「情報資産の分類および管理」である。一方、今回２番目に多い選択となった「人的セキュリティ」は「情報セキュリティポリシー」からの選択も２番目に多い（47 件）が、「情報資産の分類および管理」からは１位に選択されているほか、多くのところから２位、３位に選択されているように、情報セキュリティを進める上で従業員の教育などの「人的セキュリティ」が重要だと判断していることがうかがえる。

（５）まとめ

概論として前回と今回では大きな違いはあまりなかった。情報セキュリティに関し重要視する要素の選択について、経営的要素を重視するグループと実務を重視するグループがあるといえる。一般的には経営的な要素を重要視し、「情報セキュリティポリシー」を第１位にする傾向があり、そこでは「情報セキュリティポリシー」を作成し、「情報セキュリティ組織」、「人的セキュリティ」、「情報資産の分類および管理」などの要素を重視している。特に「情報セキュリティポリシー－情報セキュリティ組織」の組合せが 75 件と全体の 12.8％を占める。一方実務的にはウイルス対策やハッカー対策などの「通信および運用管理」、「アクセス制御」を重視するグループがある。

全体的には経営的な観点から重要な要素を選択する割合が高いが、経営的な視点を重視するところ

でも、第２位には「通信および運用管理」を重視する傾向が強く、また「情報セキュリティポリシー」と「情報セキュリティ組織」はこの組合せこそ 11.6％を占め支持が多いながらも、その他を選択したところからは各々第２位の選択として高く支持されていない、また経営的な観点を支持するグループでも第２位は実務的な点から「通信および運用管理」を選択しているなど、理想の追求と現実への対応に苦慮しているという実態がうかがえる。

なお、経営的な視点を重視すること、および「通信及び運用管理」など実務を重視するところの双方とも「人的セキュリティ」の選択が増加しており、従来から情報セキュリティの定着には従業員教育が欠かせないとされてきたが、その従業員の教育などの重要性が増してきたことが判明したのが最大の特徴である。

### 3.7.2　Q24 とのクロス集計

**×Q24-①貴社では経営理念に基づくセキュリティポリシーを定めていますか。**

**×Q24-②貴社では経営理念に基づく実施手続き・規程類を定めていますか。**

**①×Q24-①貴社では経営理念に基づくセキュリティポリシーを定めていますか。**

| Q24-①ポリシー / Q29 セキュリティ要素 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | |
|---|---|---|---|---|---|---|---|---|---|---|
| 情報セキュリティポリシー | 91 | 32.6 | 29 | 37.2 | 41 | 41.8 | 38 | 26.6 | 0 | 0.0 |
| 情報セキュリティ組織 | 24 | 8.6 | 11 | 14.1 | 14 | 14.3 | 14 | 9.8 | 0 | 0.0 |
| 情報資産の分類および管理 | 21 | 7.5 | 7 | 9.0 | 8 | 8.2 | 7 | 4.9 | 0 | 0.0 |
| 人的セキュリティ | 57 | 20.4 | 14 | 17.9 | 8 | 8.2 | 14 | 9.8 | 0 | 0.0 |
| 物理的および環境的セキュリティ | 5 | 1.8 | 3 | 3.8 | 1 | 1.0 | 4 | 2.8 | 0 | 0.0 |
| 通信および運用管理 | 26 | 9.3 | 4 | 5.1 | 10 | 10.2 | 25 | 17.5 | 2 | 50.0 |
| アクセス制御 | 11 | 3.9 | 0 | 0.0 | 3 | 3.1 | 8 | 5.6 | 0 | 0.0 |
| システム開発およびメンテナンス | 2 | 0.7 | 0 | 0.0 | 1 | 1.0 | 3 | 2.1 | 0 | 0.0 |
| 事業継続計画 | 25 | 9.0 | 6 | 7.7 | 6 | 6.1 | 19 | 13.3 | 2 | 50.0 |
| 準拠 | 8 | 2.9 | 2 | 2.6 | 5 | 5.1 | 5 | 3.5 | 0 | 0.0 |
| 無回答 | 9 | 3.2 | 2 | 2.6 | 1 | 1.0 | 6 | 4.2 | 0 | 0.0 |
| 計 | 279 | 100.0 | 78 | 100.0 | 98 | 100.0 | 143 | 100.0 | 4 | 100.0 |

Q24-①で情報セキュリティポリシーを「定めている」事業体（回答数 279 件）では第１位に「情報セキュリティポリシー」を選択した割合は 91 件（32.6％）であった。「現在作成中である」（回答数 78 件）では 37.2％、「作成を検討している」（回答数 98 件）では 41.8％、「定めていない」（回答数 143 件）では 26.6％である。このように作成中、検討中で「情報セキュリティポリシー」を第一にあげる率が「定めている」ところよりも高く、実際にセキュリティポリシー作成活動を行っているところほど注目されている状況であることがわかった。一方、情報セキュリティポリシーを「定めていない」ところでは第１位の選択率は 26.6％と低かった。これは今回、情報セキュリティポリシーを「定めている」という回答が高くなっているが、前回と同様の傾向である。前回は情報セキュリティポリシーを「定めている」ところでは第１位に「情報セキュリティポリシー」を選択した割合は

30.2%であった。「現在作成中である」では35.2%、「作成を検討している」では39.6%、「定めていない」では21.6%であった。

情報セキュリティポリシーを「定めている」ところと「作成中」では第1位に「人的セキュリティ」をあげているところが2番目に多いが、「定めていない」では「通信および運用管理」が第2位にあがっており、経営的観点より実務的な要素を重視していることがうかがえ、意識の差があることがわかる。これも前回同様の傾向である。

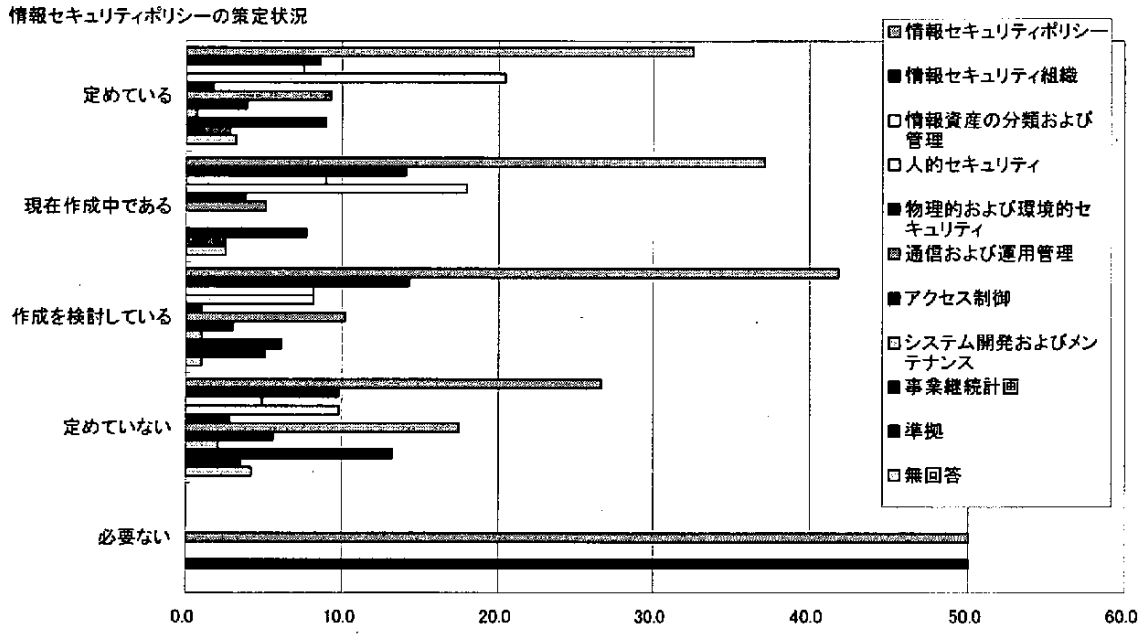



図3－7－2. 情報セキュリティポリシーの策定状況と情報セキュリティ要素との関係

×Q24-②貴社では経営理念に基づく実施手続・規程類を定めていますか。

| Q24－②実施手続・規程類 / Q29 セキュリティ要素 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | |
|---|---|---|---|---|---|---|---|---|---|---|
| 情報セキュリティポリシー | 71 | 33.6 | 40 | 32.0 | 43 | 38.7 | 45 | 30.8 | 0 | 0.0 |
| 情報セキュリティ組織 | 20 | 9.5 | 15 | 12.0 | 12 | 10.8 | 15 | 10.3 | 0 | 0.0 |
| 情報資産の分類および管理 | 16 | 7.6 | 11 | 8.8 | 10 | 9.0 | 6 | 4.1 | 0 | 0.0 |
| 人的セキュリティ | 34 | 16.1 | 31 | 24.8 | 12 | 10.8 | 14 | 9.6 | 0 | 0.0 |
| 物理的および環境的セキュリティ | 4 | 1.9 | 3 | 2.4 | 1 | 0.9 | 5 | 3.4 | 0 | 0.0 |
| 通信および運用管理 | 19 | 9.0 | 8 | 6.4 | 12 | 10.8 | 26 | 17.8 | 2 | 50.0 |
| アクセス制御 | 9 | 4.3 | 3 | 2.4 | 4 | 3.6 | 6 | 4.1 | 0 | 0.0 |
| システム開発およびメンテナンス | 2 | 0.9 | 0 | 0.0 | 1 | 0.9 | 3 | 2.1 | 0 | 0.0 |
| 事業継続計画 | 21 | 10.0 | 8 | 6.4 | 8 | 7.2 | 18 | 12.3 | 2 | 50.0 |
| 準拠 | 8 | 3.8 | 2 | 1.6 | 5 | 4.5 | 5 | 3.4 | 0 | 0.0 |
| 無回答 | 7 | 3.3 | 4 | 3.2 | 3 | 2.7 | 3 | 2.1 | 0 | 0.0 |
| 計 | 211 | 100.0 | 125 | 100.0 | 111 | 100.0 | 146 | 100.0 | 4 | 100.0 |

経営理念に基づき実施手続・規程類を「定めている」事業体（回答数 211 件）では、「情報セキュリティポリシー」の選択率は 33.6％であった。「現在作成中」（回答数 125 件）は 32.0％、「作成を検討中」（回答数 111 件）は 38.7％、「定めていない」（回答数 145 件）は 30.8％であった。これも全体の傾向としては、前問同様「検討中」が最も情報セキュリティポリシーを選択する割合が高く、「定めている」がその次に続いている。一方、「定めていない」は一番低い値を示しているが、前回と異なり意識の差が少なくなってきている。前回は「経営理念に基づき実施手続き・規程類を「定めている」」ところでは「情報セキュリティポリシー」の選択率は 25.8％であった。「現在作成中」では 38.5％、「作成を検討中」では 41.2％、「定めていない」21.9％であった。

特徴的なことは、現在実施手順・規程類を作成中のところで「人的セキュリティ」が 24.8％と割合が高くなっており、実務的に関心が高くなっている様子がうかがえる。前回同様、実施手順・規程類を定めていない事業体では「通信および運用管理」が 17.8％と第２番目に評価され、実務的な要素を重要視していることがわかる。

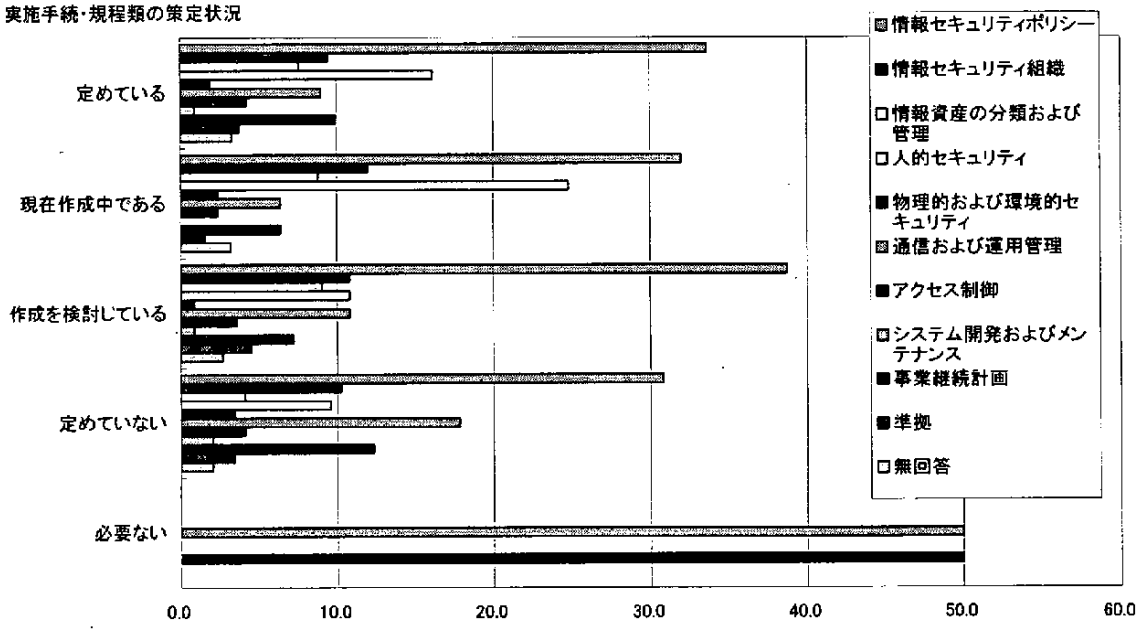



図３－７－３．実施手続・規程類の策定状況と情報セキュリティ要素との関係

## 3．8　Q31のクロス集計

Q31.「JIS X 5080 規格」の事業継続性管理に定められている事業継続性計画を作成していますか。

×Q13. 情報システムに係わるリスク分析を実施していますか。

| Q13 リスク分析 / Q31 事業継続性計画 | 回答件数 | 実施している | | 実施していない | | 実施する予定がある | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 作成している | 62 | 56 | 90.3 | 5 | 8.1 | 0 | 0.0 | 1 | 1.6 |
| 作成中である | 40 | 22 | 55.0 | 5 | 12.5 | 12 | 30.0 | 1 | 2.5 |
| 作成を含め検討中である | 82 | 26 | 31.7 | 22 | 26.8 | 33 | 40.2 | 1 | 1.2 |
| 作成していない | 392 | 70 | 17.9 | 275 | 70.2 | 46 | 11.7 | 1 | 0.3 |
| 必要ない | 12 | 0 | 0.0 | 12 | 100.0 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 17 | 7 | 41.2 | 9 | 52.9 | 0 | 0.0 | 1 | 5.9 |
| 計 | 605 | 181 | 29.9 | 328 | 54.2 | 91 | 15.0 | 5 | 0.8 |

事業継続性計画を作成している事業体ではリスク分析を「実施している」割合が 90.3％であるが、リスク分析を「実施していない」割合は 8.1％である。一方、事業継続性計画を作成中の事業体ではリスク分析を「実施している」ところが 55.0％である。「作成を含め検討中の事業体は 31.7％と、リスク分析を実施する割合が大きく下がっている。ただし作成していないところでも 17.9％とリスク分析を「実施」している。計画は「必要ない」と回答しているところではすべての事業体が「実施していない」と回答している。

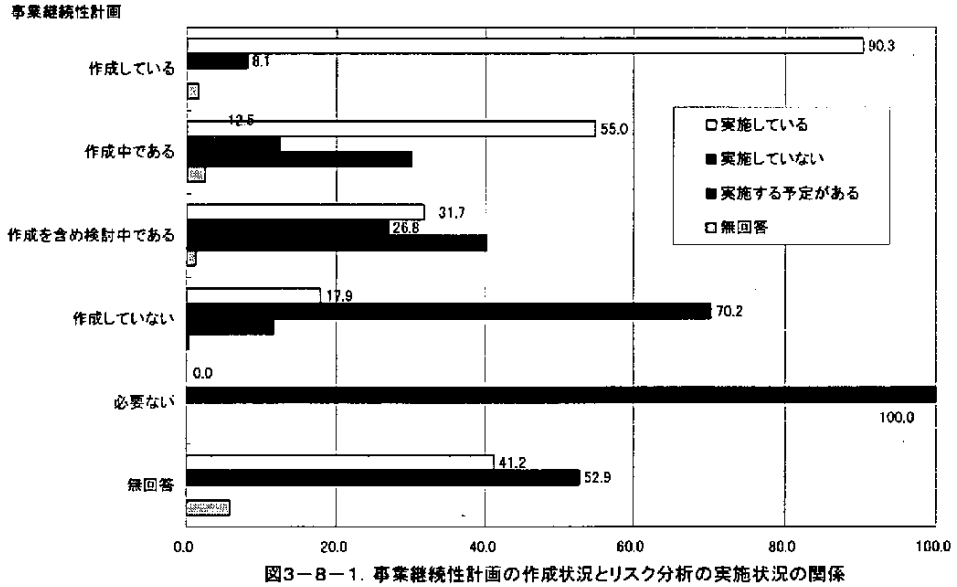



図3－8－1. 事業継続性計画の作成状況とリスク分析の実施状況の関係

| Q13 リスク分析 / Q31 事業継続性計画 | 回答件数 | 実施している | | 実施していない | | 実施する予定がある | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|
| 作成している | 62 | 56 | 30.9 | 5 | 1.5 | 0 | 0.0 | 1 | 20.0 |
| 作成中である | 40 | 22 | 12.2 | 5 | 1.5 | 12 | 13.2 | 1 | 20.0 |
| 作成を含め検討中である | 82 | 26 | 14.4 | 22 | 6.7 | 33 | 36.3 | 1 | 20.0 |
| 作成していない | 392 | 70 | 38.7 | 275 | 83.8 | 46 | 50.5 | 1 | 20.0 |
| 必要ない | 12 | 0 | 0.0 | 12 | 3.7 | 0 | 0.0 | 0 | 0.0 |
| 無回答 | 17 | 7 | 3.9 | 9 | 2.7 | 0 | 0.0 | 1 | 20.0 |
| 計 | 605 | 181 | 100.0 | 328 | 100.0 | 91 | 100.0 | 5 | 100.0 |

一方、リスク分析を実施した事業体がどのくらい事業継続性計画を作成したかをみると、リスク分析を「実施している」ところでも事業継続性計画を「作成している」のは 30.9%に過ぎず、「作成中」の 12.2%を含めても 43.1%と過半数に満たない。さすがにリスク分析を「実施している」ところでは業務継続計画や事業継続性計画が「必要ない」と回答したところは0件であったが、なかなか事業継続性計画を作成するには困難であることがわかる。

リスク分析を「実施していない」ところでは事業継続性計画を「作成している」は 1.5%と少なく「作成していない」が 83.8%であった。リスク分析を実施する意思があるかどうかが事業継続性計画の策定に大きな相関関係があると考えられるが、リスク分析を実施しても、なお事業継続性計画策定に至るにはもう一段の推進力が必要であるといえる。

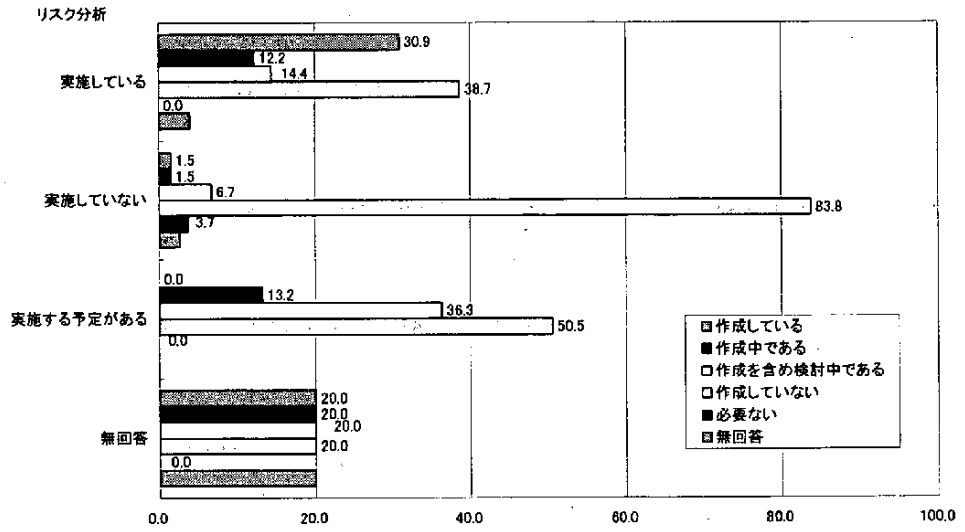



図3-8-2. リスク分析の実施状況と事業継続性計画の作成状況の関係

## 3．9　Q14のクロス集計

**Q32.（事業継続性計画を作成している場合）事業継続性計画には以下の項目を含んでいますか。**

**×Q14. リスク分析を実施している場合、情報関連のどのようなリスクを対象としましたか。**

事業継続性計画に網羅されている項目とリスク分析での対象リスクの関係について、クロス集計を行った。

| Q14 情報関連リスク / Q32 事業継続性計画 | 回答件数 | アウトソーシングリスク | コンピュータ犯罪 | 運用障害 | 人的災害 | 自然災害 | 事故 | ハードウエア障害 | ソフトウエア障害 | ネットワーク障害 | 電子メールのリスク | ウイルスのリスク | 不正アクセスのリスク | その他 | 無回答 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 外部からの悪意による緊急事態 | 37 | 40.5 | 70.3 | 81.1 | 40.5 | 75.7 | 86.5 | 94.6 | 94.6 | 91.9 | 40.5 | 83.8 | 86.5 | 0.0 | 0.0 |
| ネットワークセキュリティ上の緊急事態 | 30 | 36.7 | 76.7 | 80.0 | 40.0 | 76.7 | 86.7 | 93.3 | 93.3 | 90.0 | 50.0 | 86.7 | 83.3 | 0.0 | 0.0 |
| 事故・災害 | 76 | 44.7 | 65.8 | 84.2 | 48.7 | 85.5 | 89.5 | 94.7 | 88.2 | 88.2 | 46.1 | 84.2 | 80.3 | 0.0 | 0.0 |
| 障害 | 62 | 50.0 | 71.0 | 87.1 | 51.6 | 87.1 | 90.3 | 96.8 | 93.5 | 91.9 | 48.4 | 87.1 | 83.9 | 0.0 | 0.0 |
| 人的なミスに起因する障害・誤処理 | 41 | 46.3 | 80.5 | 90.2 | 51.2 | 85.4 | 87.8 | 95.1 | 95.1 | 90.2 | 48.8 | 92.7 | 87.8 | 0.0 | 0.0 |
| 内部犯罪による緊急事態 | 20 | 45.0 | 85.0 | 90.0 | 55.0 | 80.0 | 90.0 | 95.0 | 95.0 | 90.0 | 50.0 | 95.0 | 95.0 | 0.0 | 0.0 |
| その他 | 2 | 50.0 | 50.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 50.0 | 50.0 | 50.0 | 0.0 | 0.0 |
| 無回答 | 103 | 36.9 | 46.6 | 66.0 | 30.1 | 66.0 | 75.7 | 85.4 | 77.7 | 75.7 | 32.0 | 77.7 | 63.1 | 2.9 | 1.0 |
| 計 | 371 | 42.6 | 65.2 | 80.1 | 43.4 | 78.4 | 85.2 | 92.5 | 88.4 | 86.3 | 42.9 | 84.4 | 78.4 | 0.8 | 0.3 |

| Q14 情報関連リスク / Q32 事業継続性計画 | 回答件数 | アウトソーシングリスク | コンピュータ犯罪 | 運用障害 | 人的災害 | 自然災害 | 事故 | ハードウエア障害 | ソフトウエア障害 | ネットワーク障害 | 電子メールのリスク | ウイルスのリスク | 不正アクセスのリスク | その他 | 無回答 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 外部からの悪意による緊急事態 | 37 | 9.5 | 10.7 | 10.1 | 9.3 | 9.6 | 10.1 | 10.2 | 10.7 | 10.6 | 9.4 | 9.9 | 11.0 | 0.0 | 0.0 |
| ネットワークセキュリティ上の緊急事態 | 30 | 7.0 | 9.5 | 8.1 | 7.5 | 7.9 | 8.2 | 8.2 | 8.5 | 8.4 | 9.4 | 8.3 | 8.6 | 0.0 | 0.0 |
| 事故・災害 | 76 | 21.5 | 20.7 | 21.5 | 23.0 | 22.3 | 21.5 | 21.0 | 20.4 | 20.9 | 22.0 | 20.4 | 21.0 | 0.0 | 0.0 |
| 障害 | 62 | 19.6 | 18.2 | 18.2 | 19.9 | 18.6 | 17.7 | 17.5 | 17.7 | 17.8 | 18.9 | 17.3 | 17.9 | 0.0 | 0.0 |
| 人的なミスに起因する障害・誤処理 | 41 | 12.0 | 13.6 | 12.5 | 13.0 | 12.0 | 11.4 | 11.4 | 11.9 | 11.6 | 12.6 | 12.1 | 12.4 | 0.0 | 0.0 |
| 内部犯罪による緊急事態 | 20 | 5.7 | 7.0 | 6.1 | 6.8 | 5.5 | 5.7 | 5.5 | 5.8 | 5.6 | 6.3 | 6.1 | 6.5 | 0.0 | 0.0 |
| その他 | 2 | 0.6 | 0.4 | 0.7 | 1.2 | 0.7 | 0.6 | 0.6 | 0.6 | 0.6 | 0.6 | 0.3 | 0.3 | 0.0 | 0.0 |
| 無回答 | 103 | 24.1 | 19.8 | 22.9 | 19.3 | 23.4 | 24.7 | 25.7 | 24.4 | 24.4 | 20.8 | 25.6 | 22.3 | 0.0 | 0.0 |
| 計 | 605 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 | 100.0 |

筆者の期待としてはたとえばリスク分析の対象として事故災害を選択したところでは事業継続性計画でも高い相関が現れると期待したが、どちらも回答結果に大きな差異が得られなかった。

## 3．10　Q42のクロス集計

Q42. どのようなネットワーク障害対策を実施していますか。

×Q19. 基幹システムにおけるMTBFは何時間ですか。

ネットワークの障害対策の効果を調べるために、基幹システムの MTBF（平均故障間隔)」とのクロス分析を実施した。

| Q42 ネットワーク障害対策 | Q19 MTBF平均時間 |
|---|---|
| 平均 | 2,961.9 |
| 異なる種別回線を利用 | 3,098.1 |
| 異なる交換局への収容 | 3,783.3 |
| 異なるコモンキャリアの利用 | 3,435.7 |
| 異なるISPを利用 | 2,575.4 |
| 異なるメディアによる回線利用(例:衛星回線等) | 3,154.0 |
| ポイント間接続から網接続へ | 3,053.6 |
| 重要回線を部分的に二重化 | 2,926.4 |
| 専用のバックアップ回線を常時設定 | 3;296.9 |
| 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 | 3,090.2 |
| 社内の構内回線、LAN等を二重化 | 2,895.2 |
| 通信機器の二重化 | 2,864.4 |
| インターネットに接続したサーバの分散 | 3,138.9 |
| その他 | 2,460.0 |
| 特に対策を講じていない | 2,402.3 |
| 無回答 | 3,102.5 |

MTBFの平均時間（2,961.9時間）よりも上回っているのは、「異なる交換局への収容」(3,783.3時間)、「異なるコモンキャリアの利用」（3,435.7時間）、「専用のバックアップ回線を常時設定」(3296.9時間)、[異なるメディアによる回線利用]（3,154.0時間)、「インターネットに接続したサーバの分散」(3,138.9時間)、「異なる種別回線を利用」(3,098.1時間)、「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」(3,090.2時間)、「ポイント間接続から網接続へ」(3,053.6時間）である。

一方、「特に対策を講じていない」および「その他」は約2,400時間足らずであった。このことから、異なる交換局などへの分散収容やバックアップ回線の設定といった二重化を行っている事業体では結果としてMTBFが長いことがわかる。

ただし、「異なるISPを利用」が2,500時間程度であり、対策としてあまり有効でない。ただしこれは、この方策をとっている総数が少ないこと、対策をとるためにはBGPなどの高度なプロトコルへの知識が要求されるためと考えられる。今回の調査で結論づけるのはまだ不十分と考えられる。

また、3次元グラフからは、異なる局や回線の二重化策を実施している事業体では、「2千時間

以上３千時間未満」および「３千時間以上４千時間未満」に集中している。このことから、多くの事業体これらの対策が役立っていることがわかる。

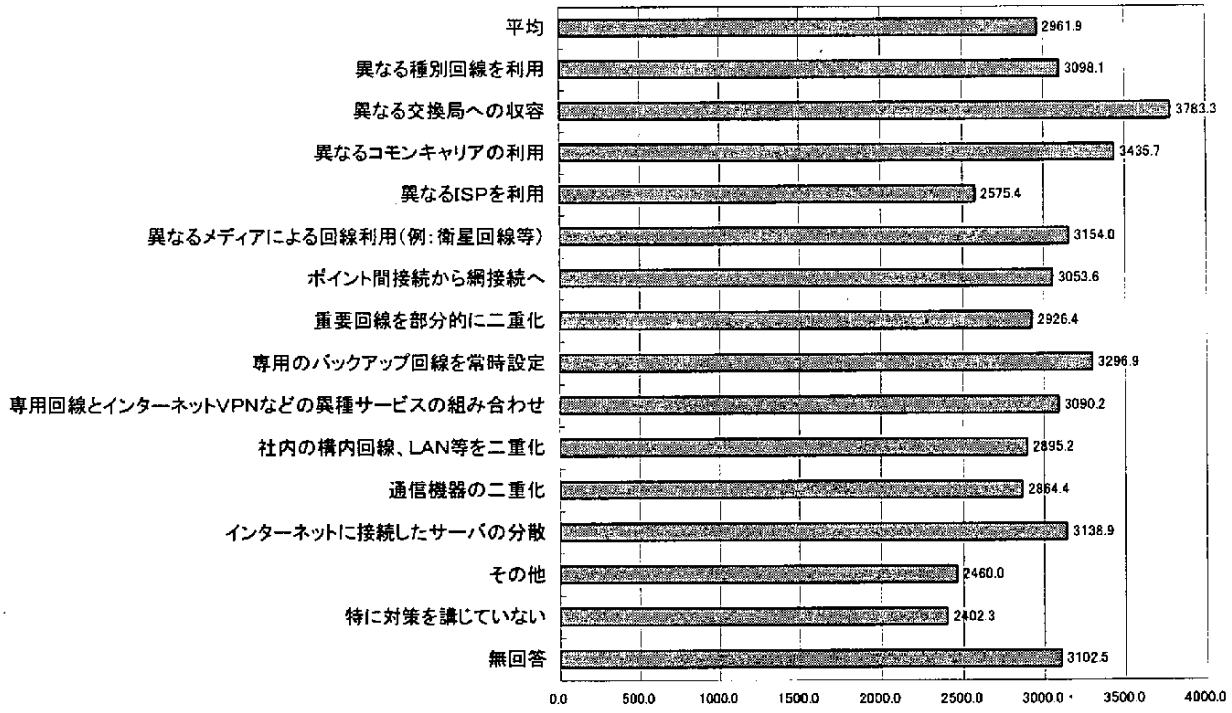



図3－10－1．ネットワーク障害対策とMTBF(平均故障間隔)の関係(平均)

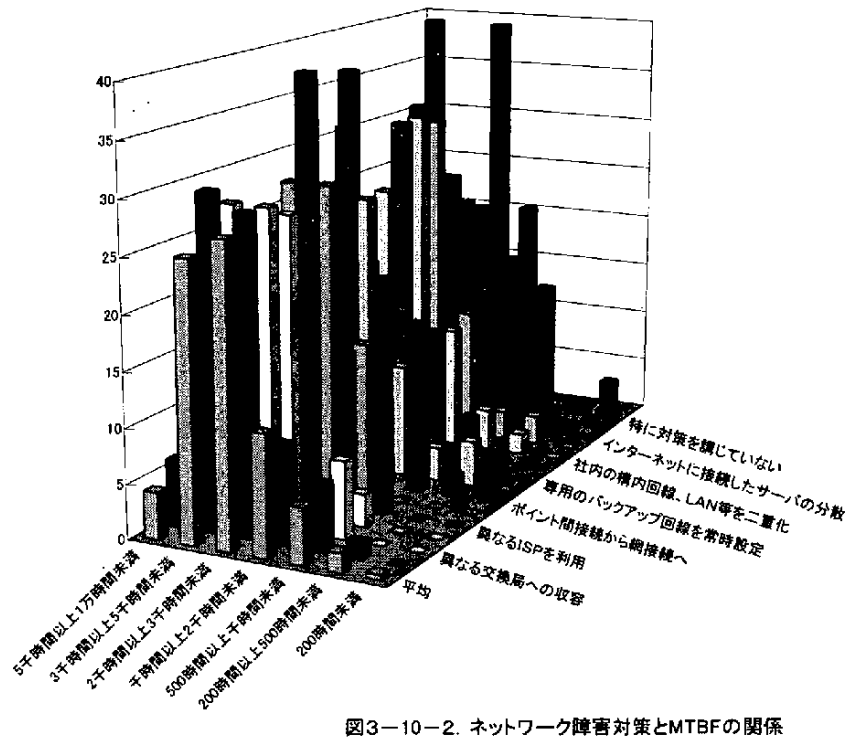



図3－10－2．ネットワーク障害対策とMTBFの関係

## 3．11　Q43 のクロス集計

**Q43. 貴事業体では従業員に対し、情報セキュリティの面から教育・訓練を実施していますか。**

**×Q44. 貴事業体では情報セキュリティの人材をどのように養成していますか。**

情報セキュリティ面での教育・訓練の実施状況として、特に実施していない」が 42.0％と最も高く、「時々実施している」が 25.6％とこれに続いている。これに対し情報セキュリティ人材養成の実施状況との関係についてクロス分析を行った。

| Q44 人材養成 / Q43 教育・訓練 | 回答件数 | 自社育成プログラムにより高度な人材育成を実施 | | 民間資格を利用して育成 | | 情報セキュリティアドミニストレータ試験を活用 | | 特に行っていない | | 必要ない | | 無回答 | | 複数回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 定期的に実施している | 101 | 26 | 25.7 | 9 | 8.9 | 11 | 10.9 | 45 | 44.6 | 0 | 0.0 | 2 | 2.0 | 8 | 7.9 |
| 時々実施している | 155 | 12 | 7.7 | 8 | 5.2 | 11 | 7.1 | 119 | 76.8 | 0 | 0.0 | 3 | 1.9 | 2 | 1.3 |
| 実施を予定している | 85 | 8 | 9.4 | 8 | 9.4 | 10 | 11.8 | 58 | 68.2 | 0 | 0.0 | 1 | 1.2 | 0 | 0.0 |
| 特に実施していない | 254 | 1 | 0.4 | 4 | 1.6 | 6 | 2.4 | 240 | 94.5 | 2 | 0.8 | 0 | 0.0 | 1 | 0.4 |
| 無回答 | 10 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 1 | 10.0 | 0 | 0.0 | 9 | 90.0 | 0 | 0.0 |
| 計 | 605 | 47 | 7.8 | 29 | 4.8 | 38 | 6.3 | 463 | 76.5 | 2 | 0.3 | 15 | 2.5 | 11 | 1.8 |

このうち、「定期的に実施している」、「時々実施している」、「実施を予定している」の関係をみると以下のような結果であった。

| Q44 人材 / Q43 教育・訓練 | 自社育成プログラムにより育成 | 民間資格を利用して育成 | 情報セキュリティアドミニストレータ試験を活用 | 合計 |
|---|---|---|---|---|
| 定期的に実施している | 25.7 | 8.9 | 10.9 | 45.5 |
| 時々実施している | 7.7 | 5.2 | 7.1 | 20.0 |
| 実施を予定している | 9.4 | 9.4 | 11.8 | 30.6 |

「定期的に実施している」が合計で 45.5％と最も高い割合であったが、その中で特に高い割合であったのは「自社育成プログラムにより高度な人材育成を行っている」（25.7％）であった。

## 3．12　Q60のクロス集計

Q60. 過去２年以内にシステム監査を実施したことがありますか。

×Q24－①貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。
×Q24－②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。

### 3.12.1　Q24－①とのクロス集計

**Q24-①貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。**

システム監査の実施状況と情報セキュリティポリシーの策定状況との関係について、クロス分析を実施した。

| Q24-①ポリシー / Q60 システム監査 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 実施した(実施中を含む) | 217 | 138 | 63.6 | 17 | 7.8 | 32 | 14.7 | 29 | 13.4 | 0 | 0.0 | 1 | 0.5 |
| これから実施する予定がある | 66 | 36 | 54.5 | 17 | 25.8 | 9 | 13.6 | 4 | 6.1 | 0 | 0.0 | 0 | 0.0 |
| 実施しない | 315 | 98 | 31.1 | 44 | 14.0 | 57 | 18.1 | 110 | 34.9 | 4 | 1.3 | 2 | 0.6 |
| 無回答 | 7 | 7 | 100.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 計 | 605 | 279 | 46.1 | 78 | 12.9 | 98 | 16.2 | 143 | 23.6 | 4 | 0.7 | 3 | 0.5 |

システム監査を実施した（実施中を含む）、および実施する予定がある事業体では、情報セキュリティポリシーを「定めている」割合が、それぞれ63.6%、54.5%と過半数を占めている。また、「現在作成中」を含めると、それぞれ71.4%、80.3%となる。一方、システム監査を実施しない事業体では情報セキュリティポリシーを「定めていない」割合が高く34.9%となっている。すなわち、情報セキュリティポリシーの作成とシステム監査の実施には強い相関があることがわかる。

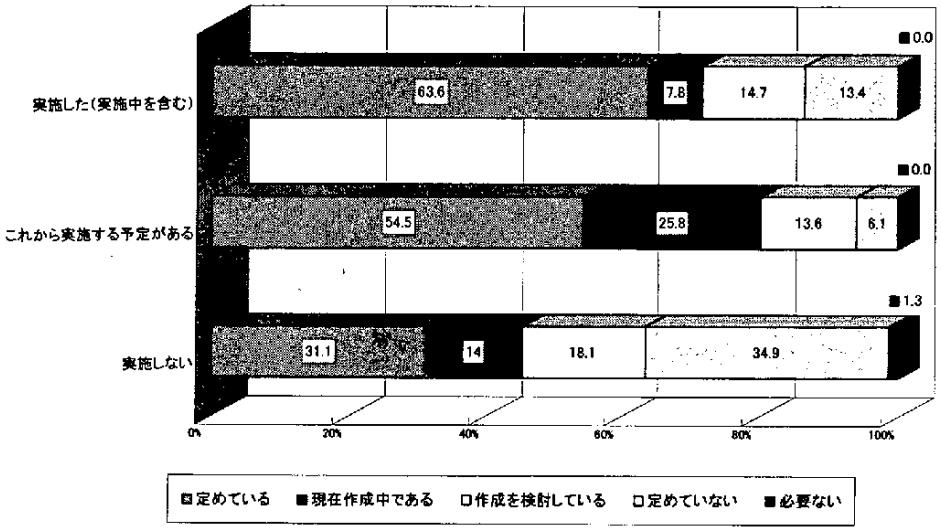



図3－12－1．システム監査の実施状況とセキュリティポリシーの策定状況の関係

### 3.12.2 Q24－②とのクロス集計

**Q24－②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。**

システム監査の実施状況と実施手続・規程類の策定状況との関係について、クロス分析を実施した。

| Q24-②実施手続・規程類 / Q60 システム監査 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 実施した(実施中を含む) | 217 | 116 | 53.5 | 41 | 18.9 | 33 | 15.2 | 25 | 11.5 | 0 | 0.0 | 2 | 0.9 |
| これから実施する予定がある | 66 | 26 | 39.4 | 24 | 36.4 | 11 | 16.7 | 5 | 7.6 | 0 | 0.0 | 0 | 0.0 |
| 実施しない | 315 | 64 | 20.3 | 59 | 18.7 | 67 | 21.3 | 116 | 36.8 | 4 | 1.3 | 5 | 1.6 |
| 無回答 | 7 | 5 | 71.4 | 1 | 14.3 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 1 | 14.3 |
| 計 | 605 | 211 | 34.9 | 125 | 20.7 | 111 | 18.3 | 146 | 24.1 | 4 | 0.7 | 8 | 1.3 |

システム監査を実施した（実施中を含む）、および実施する予定がある事業体では、実施手続・規程類を「定めている」割合が、それぞれ 53.5%、39.4%となっている。また、「現在作成中」を含めると、それぞれ 72.4%、75.8%となる。一方、システム監査を実施しない事業体では実施手続・規程類を「定めていない」割合が高く、36.8%となっている。すなわち、実施手続・規程類の有無とシステム監査の実施には強い相関があることがわかる。ただし、情報セキュリティポリシーと比較すると若干相関は低い。

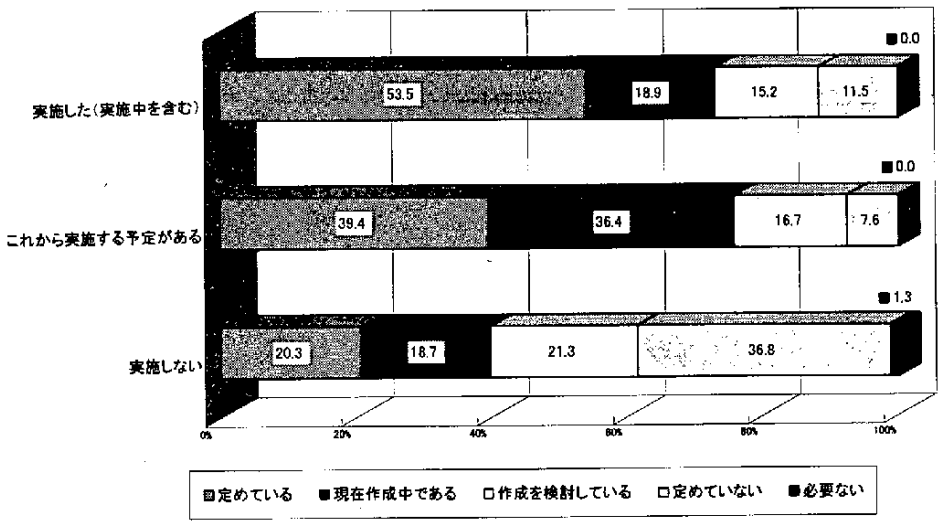



図3－12－2. システム監査の実施状況と実施手続・規程類の策定状況の関係

## 3．13　Q61のクロス集計

Q61.（システム監査を実施している場合）システム監査を実施した結果、どのような点に効果があったと思いますか。

×Q19. 基幹システムにおけるMTBFは何時間ですか。

システム監査の効果を調べるために、基幹システムのMTBF（平均故障間隔）とのクロス分析を実施した。

| Q61　システム監査の効果 | Q19　MTBF平均時間 |
|---|---|
| 平均 | 3,103.6 |
| システムに起因する事故・障害が未然に防止できた | 1,798.5 |
| リスク対策をどこまで考慮すればよいかが明らかになった | 3,187.5 |
| 担当者がリスクを考慮しながら業務を実行するようになった | 3,303.8 |
| システム部門に対する過大な要求がなくなった | 0.0 |
| システムの信頼性向上対策のレベルが明らかになった | 3,275.4 |
| システムの有効利用が促進された | 2,542.5 |
| システムの効率性が確保できた | 2,700.0 |
| 有効なシステムの開発設計が可能になった | 0.0 |
| 業務の継続性の確保が図られた | 3,,077.4 |
| 要員が規定・ルール等を意識して業務を実行するようになった | 3,014.2 |
| その他 | 4,922.0 |
| 効果は得られなかった | 2,593.9 |

「システムの信頼性向上対策のレベルが明らかになった」事業体のMTBFの平均値は3,275.4時間、「担当者がリスクを考慮しながら業務をするようになった」では3,303.8時間、「リスク対策をどこまで考慮すればよいかが明らかになった」では3,187.5時間と、平均の3,103.6時間を上回っており、システム監査がMTBFの向上に役立っていることがわかる。

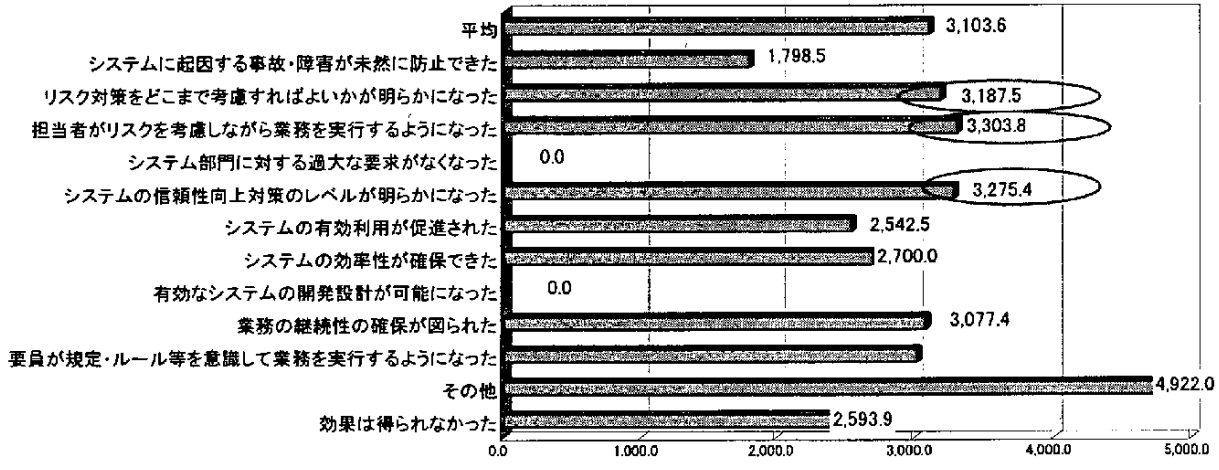



図3－13－1. システム監査の効果とMTBFの関係

## 3．14　Q63のクロス集計

Q63. 情報セキュリティ監査を実施したことがありますか。

×Q24－①貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。
×Q24－②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。

### 3.14.1　Q24－①とのクロス集計

**Q24-①貴事業体では経営理念に基づく情報セキュリティポリシーを定めていますか。**

情報セキュリティ監査の実施状況と情報セキュリティポリシーの策定状況との関係について、クロス分析を実施した。

| Q24-①ポリシー / Q63 情報セキュリティ監査 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 実施した | 110 | 49 | 44.5 | 15 | 13.6 | 19 | 17.3 | 27 | 24.5 | 0 | 0.0 | 0 | 0.0 |
| これから実施する予定がある | 122 | 39 | 32.0 | 21 | 17.2 | 29 | 23.8 | 31 | 25.4 | 2 | 1.6 | 0 | 0.0 |
| 実施しない | 359 | 184 | 51.3 | 41 | 11.4 | 45 | 12.5 | 85 | 23.7 | 2 | 0.6 | 2 | 0.6 |
| 無回答 | 14 | 7 | 50.0 | 1 | 7.1 | 5 | 35.7 | 0 | 0.0 | 0 | 0.0 | 1 | 7.1 |
| 計 | 605 | 279 | 46.1 | 78 | 12.9 | 98 | 16.2 | 143 | 23.6 | 4 | 0.7 | 3 | 0.5 |

情報セキュリティ監査を実施した、および実施する予定がある事業体では、情報セキュリティポリシーを「定めている」割合が、それぞれ44.5%、32.0%となっている。しかし、情報セキュリティ監査を実施しない事業体のうち、情報セキュリティポリシーを「定めている」割合は51.3%である。したがって、情報セキュリティポリシーを定めている事業体が必ずしも情報セキュリティ監査を実施したとはいえない。

また、情報セキュリティ監査を実施した事業体のうち、情報セキュリティポリシーを「定めていない」割合が24.5%であり、情報セキュリティ監査を実施しない事業体で情報セキュリティポリシーを「定めていない」割合（23.7%）とほとんど同じ結果となった。

すなわち、「情報セキュリティ監査の実施」と「情報セキュリティポリシーの作成」には相関がみられないことがわかる。これは、システム監査の場合に両者の相関が大きいことと比べると、大きな違いといえよう。なお、情報セキュリティ監査制度が平成15年4月から運用が開始されたばかりであり、実施している事業体も少ないこと、実施した内容が情報セキュリティ監査制度で述べている監査と必ずしも同じといえない点を考慮する必要がある。

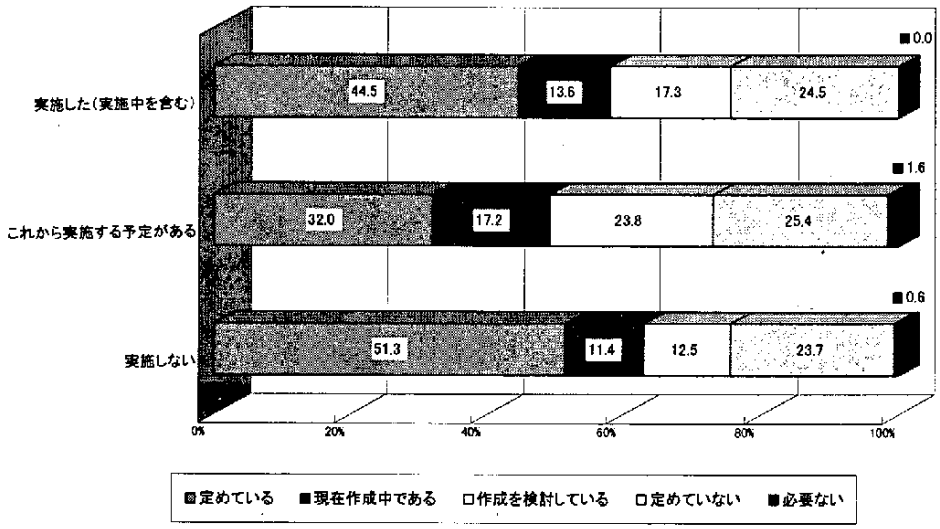



図3－14－1. 情報セキュリティ監査の実施状況とセキュリティポリシーの策定状況の関係

### 3.14.2 Q24－②とのクロス集計

**Q24-②貴事業体では経営理念に基づく実施手続・規程類を定めていますか。**

情報セキュリティ監査の実施状況と実施手続・規程類の策定状況との関係について、クロス分析を実施した。

| Q24-②実施手続・規程類 / Q63 情報セキュリティ監査 | 回答件数 | 定めている | | 現在作成中である | | 作成を検討している | | 定めていない | | 必要ない | | 無回答 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 実施した | 110 | 33 | 30.0 | 22 | 20.0 | 22 | 20.0 | 31 | 28.2 | 0 | 0.0 | 2 | 1.8 |
| これから実施する予定がある | 122 | 34 | 27.9 | 25 | 20.5 | 26 | 21.3 | 33 | 27.0 | 2 | 1.6 | 2 | 1.6 |
| 実施しない | 359 | 140 | 39.0 | 75 | 20.9 | 58 | 16.2 | 81 | 22.6 | 2 | 0.6 | 3 | 0.8 |
| 無回答 | 14 | 4 | 28.6 | 3 | 21.4 | 5 | 35.7 | 1 | 7.1 | 0 | 0.0 | 1 | 7.1 |
| 計 | 605 | 211 | 34.9 | 125 | 20.7 | 111 | 18.3 | 146 | 24.1 | 4 | 0.7 | 8 | 1.3 |

情報セキュリティ監査を実施した、および実施する予定がある事業体では、実施手続・規程類を「定めている」割合が、それぞれ30.0%、20.0%となっている。しかし、情報セキュリティ監査を実施しない事業体のうち、情報セキュリティポリシーを「定めている」割合は39.0%である。したがって、実施手続・規程類を定めている事業体が必ずしも情報セキュリティ監査を実施したとはいえない。したがって、情報セキュリティポリシーの場合とほとんど同様で、情報セキュリティ監査実施と実施手続・規程類の策定状況での相関はみられない。

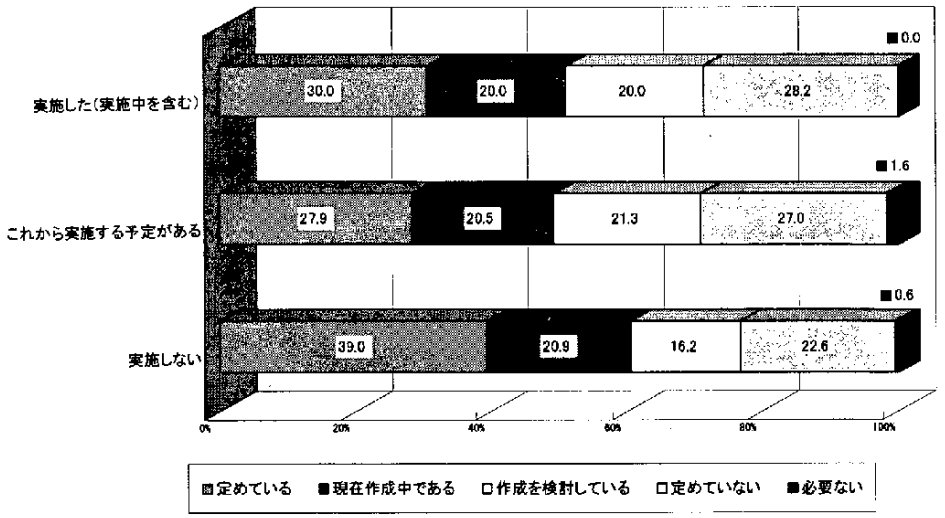



図3－14－2. 情報セキュリティ監査の実施状況と実施手続・規程類の策定状況の関係

付属資料

# 「情報セキュリティに関する調査」アンケート調査票

1

(財)日本情報処理開発協会

2003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　　－　　－<br>内線 | | |
| 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） | 6 兆 / 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。

◇　ご回答賜りました事業体には、全体の集計結果を後日お送り申し上げます。

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

| 業　種 19、20 | 複数業種に関連する場合は、主力業種1つのみ○印をつけて下さい。 | | | | |
|---|---|---|---|---|---|
| 1 | 農・林・漁・狩猟・水産養殖業 | 16 | 電気機械器具製造業 | 31 | 広告・調査・情報提供サービス業 |
| 2 | 鉱業 | 17 | 輸送用機械器具製造業 | 32 | 情報処理サービス業・ソフトウェア業（注1） |
| 4 | 建設業 | 18 | 精密機械器具製造業 | 33 | 医療業（注2） |
| 5 | 食品製造業 | 19 | その他の製造業 | 34 | 宗教法人 |
| 6 | 繊維工業 | 21 | 卸業・商社 | 35 | 高校 |
| 7 | 紙・パルプ・紙加工品製造業 | 22 | 小売業 | 36 | 大学 |
| 8 | 新聞業・出版業 | 23 | 金融業 | 37 | その他の教育機関 |
| 9 | 印刷業・同関連産業 | 24 | 証券業・商品取引業 | 38 | 学術研究機関 |
| 10 | 化学工業 | 25 | 生命保険業（含代理業・サービス業） | 39 | 法人団体・農協 |
| 11 | 石油製品製造業 | 26 | 損害保険業（含代理業・サービス業） | 40 | その他のサービス業 |
| 12 | 窯業・土石製品製造業 | 27 | 不動産業 | 42 | 政府 |
| 13 | 鉄鋼業 | 28 | 運輸・通信・倉庫業 | 43 | 地方公共団体 |
| 14 | 非鉄金属製造業・金属製品製造業 | 29 | 電力・ガス事業 | | |
| 15 | 一般機械器具製造業 | 30 | 放送業 | | |

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

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

21 A

| 1 | 経済産業省の安全対策の施策について |
|---|---|

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

| | 施　　策 | 利用している | 知っている | 知らない |
|---|---|---|---|---|
| 22 | 情報システム安全対策基準（平成７年８月改訂） | 1 | 2 | 3 |
| 23 | コンピュータウイルス対策基準（平成７年７月改訂） | 1 | 2 | 3 |
| 24 | コンピュータ不正アクセス対策基準（平成８年８月制定） | 1 | 2 | 3 |
| 25 | システム監査基準（平成８年１月改訂） | 1 | 2 | 3 |
| 26 | システム監査企業台帳制度（平成３年３月制定） | 1 (注) | 2 | 3 |
| 27 | 情報セキュリティ監査制度（平成１５年３月運用開始） | 1 | 2 | 3 |
| 28 | 情報セキュリティ監査企業台帳制度（平成１５年３月制定） | 1 (注) | 2 | 3 |

（注）システム監査企業台帳／情報セキュリティ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．（Q1 で「情報システム安全対策基準を利用している／知っている」と回答した場合）情報処理サービス業情報システム安全対策実施事業所認定制度が、情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度に移行したことに伴い、「情報システム安全対策基準」が平成１６年３月末をもって廃止されることを知っていますか。

29

| 1 | 知っている |
|---|---|
| 2 | 知らない |

Q３．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 |
|---|---|---|---|
| 30 | コンピュータウイルス被害（届出機関） | 1 | 2 |
| 31 | コンピュータ不正アクセス被害（届出機関） | 1 | 2 |

Q４．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（ＪＰＣＥＲＴコーディネーションセンター）」を知っていますか。

32

| 1 | 知っている |
|---|---|
| 2 | 知らない |

Q５．以下のＪＩＳ規格を知っていますか。

| | 規格名 | 利用している | 知っている | 知らない |
|---|---|---|---|---|
| 33 | ＪＩＳ Ｘ ５０８０：情報技術－情報セキュリティマネジメントの実践のための規範（平成１４年２月制定） | 1 | 2 | 3 |
| 34 | ＪＩＳ Ｑ ２００１：リスクマネジメントシステム構築のための指針（平成１３年３月制定） | 1 | 2 | 3 |
| 35 | ＪＩＳ Ｑ １５００１：個人情報保護に関するコンプライアンス・プログラムの要求事項（平成１１年４月制定） | 1 | 2 | 3 |

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

36

| 1 | 情報セキュリティ担当者をＳＳ試験に受験させている |
|---|---|
| 2 | 知っている |
| 3 | 知らない |

37 B

## 2 情報リスクマネジメントについて

Q７．現代の情報システム環境から、情報リスクマネジメントについてどう考えていますか。

38

| | |
|---|---|
| 1 | 重要と考え、実践している |
| 2 | 重要と考えている |
| 3 | さらに強化する予定がある |
| 4 | 考えていない |
| 5 | わからない |

Q８．経営者層はコンピュータ関連の事件・事故に対するリスクについて関心が高いですか。

39

| | |
|---|---|
| 1 | 高　い |
| 2 | 中　位 |
| 3 | 低　い |
| 4 | わからない |

Q９．日本情報処理開発協会が開発した「ＪＲＭＳ（JIPDECリスクマネジメントシステム）」という、リスク分析を含めたリスクマネジメント手法があることを知っていますか。

40

| | |
|---|---|
| 1 | 利用したことがある |
| 2 | 知っている |
| 3 | 知らない |

Q10．情報のマネジメントにおいては、情報リスクマネジメント方針の明確化、情報リスクの分析、情報セキュリティポリシー、情報セキュリティ対策の規程、システム監査等が重要です。これらのうち、貴事業体において実施しているものはどれですか？（複数回答）

| | | |
|---|---|---|
| 41 | 1 | 情報リスクマネジメント方針 |
| 42 | 2 | 情報リスク分析 |
| 43 | 3 | 情報セキュリティポリシー |
| 44 | 4 | 情報セキュリティ対策 |
| 45 | 5 | 情報セキュリティ監査 |
| 46 | 6 | システム監査 |
| 47 | 7 | その他<br>（　　） |
| 48 | 8 | 特に実施していない |

49 C

## 3 情報リスク分析について

Q11．基幹システム(注1)が１時間以上停止した場合、経営に与える影響（被害額）(注2)がどれ位になるか想定していますか。

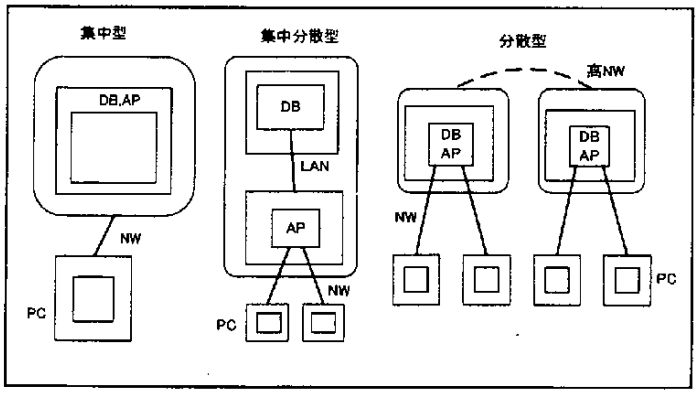
50

| | |
|---|---|
| 1 | は　い |
| 2 | いいえ |

⇒Ｑ１３へ

(注1)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（運用の型は右図参照）。本調査では、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。**

（注２）被害額には売上の逸失額、賠償金額、原状回復費用を含みます。



Q12. （Q11で「1」と回答した場合）被害の推定額は1日あたりどれ位ですか。

51

| | |
|---|---|
| 1 | １０億円以上 |
| 2 | ５億円以上～１０億円未満 |
| 3 | １億円以上～５億円未満 |
| 4 | ５千万円以上～１億円未満 |
| 5 | １千万円以上～５千万円未満 |
| 6 | １千万円未満 |

Q13. 情報システムに係わるリスク分析を実施していますか。

52

| | | |
|---|---|---|
| 1 | 実施している | |
| 2 | 実施していない | ⇒Ｑ１６へ |
| 3 | 実施する予定がある | ⇒Ｑ１７へ |

Q14. （Q13で「1」と回答した場合）情報関連のどのようなリスクを対象としましたか？（複数回答）

| | | |
|---|---|---|
| 53 | 1 | アウトソーシングリスク |
| 54 | 2 | コンピュータ犯罪（故意を含む）のリスク |
| 55 | 3 | 運用障害（操作ミス、入力ミス等） |
| 56 | 4 | 人的災害（テロ、労働争議等） |
| 57 | 5 | 自然災害 |
| 58 | 6 | 事故（火災、爆発、停電、漏水等） |
| 59 | 7 | ハードウェア障害 |
| 60 | 8 | ソフトウェア障害 |
| 61 | 9 | ネットワーク障害 |
| 62 | 10 | 電子メールのリスク（誤送信等） |
| 63 | 11 | コンピュータウイルスのリスク |
| 64 | 12 | 不正アクセスのリスク |
| 65 | 13 | その他（　　） |

Q15. リスク分析を実施した際の問題点は何ですか。（複数回答）

| | | |
|---|---|---|
| 66 | 1 | 経営との関係がわからない |
| 67 | 2 | 確立した手法がない |
| 68 | 3 | 分析のためのデータが乏しい |
| 69 | 4 | 専門家がいない |
| 70 | 5 | 組織ができていない |
| 71 | 6 | リスクの定量化が測れない |
| 72 | 7 | その他（　　） |
| 73 | 8 | 問題点は特にない |

⇒Ｑ１７へ

Q16. （Q13で「2」と回答した場合）リスク分析を実施しない理由は何ですか。（複数回答）

| | | |
|---|---|---|
| 74 | 1 | 重要性を感じていない |
| 75 | 2 | 手法がわからない |
| 76 | 3 | 予算がない |
| 77 | 4 | 発生被害額が算出できない |
| 78 | 5 | リスク分析の意味がわからない |
| 79 | 6 | 効果がわからない |
| 80 | 7 | 効果があるとは思えない |

81 D

Q17. 貴事業体の基幹システムは、過去１年間にシステムの運用に影響を与えるシステムダウン[注)]が発生しましたか。

82

| | |
|---|---|
| 1 | 全体的にダウンした |
| 2 | 部分的にダウンした |
| 3 | しない　⇒Ｑ２１へ |

（注）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。

Q18. （Q17 で「1」、「2」と回答した場合）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）

| | | |
|---|---|---|
| 83 | 1 | 自然災害 |
| 84 | 2 | 停電（電力会社に起因する障害） |
| 85 | 3 | 電源機器・設備障害 |
| 86 | 4 | 空調等障害 |
| 87 | 5 | 通信事業者に起因する障害 |
| 88 | 6 | ＩＳＰ（インターネットサービスプロバイダ）等、社外のインターネットに起因する障害 |
| 89 | 7 | ネットワーク機器などの障害 |
| 90 | 8 | ハードウェア障害 |
| 91 | 9 | ＯＳ障害 |
| 92 | 10 | ソフトウェア障害 |
| 93 | 11 | コンピュータウイルス（ウイルスによる不正侵入・ネットワーク障害を含む） |
| 94 | 12 | 火災による事故・障害 |
| 95 | 13 | 人の悪意（たとえば内部犯罪、不正侵入）による事故等 |
| 96 | 14 | オペミス等、人の過失による事故等 |
| 97 | 15 | その他（　　） |

Q19. 基幹システムにおけるＭＴＢＦ（平均故障間隔）は何時間ですか。（少数点以下は四捨五入して下さい）

（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

96 [　　] 時間 102

Q20. 基幹システムにおけるＭＴＴＲ（平均修理時間）は何分ですか。（少数点以下は四捨五入して下さい）

103 [　　] 分 106

Q21. 次の各行為をリスクの視点からコンピュータ利用に関わる犯罪と想定し、貴事業体における認識の度合いを示すことができますか。各項目別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 | | | | | |
|---|---|---|---|---|---|---|---|
| 107 | 市販のソフトをコピーして使う | 1 | 2 | 3 | 4 | 5 | 6 |
| 108 | データ、プログラムを無断で使う | 1 | 2 | 3 | 4 | 5 | 6 |
| 109 | データ、プログラムを覗き見る | 1 | 2 | 3 | 4 | 5 | 6 |
| 110 | 就業時間内に会社のコンピュータを私的な目的に使う | 1 | 2 | 3 | 4 | 5 | 6 |
| 111 | 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 |
| 112 | 私的な目的のための電子メールを送・受信する | 1 | 2 | 3 | 4 | 5 | 6 |
| 113 | 他人のＩＤを無断借用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 114 | 業務上入手した顧客情報を正当な理由なしに第三者に売却する | 1 | 2 | 3 | 4 | 5 | 6 |

犯罪度欄の回答群１～６は次のように定義します。

| | |
|---|---|
| １．特に問題ではない | ２．問題であると思う |
| ３．企業内で戒告・訓告・注意処分等の対象となる | ４．企業内で懲戒免職の対象となる |
| ５．犯罪行為である（刑法上の処罰の対象となる） | ６．わからない |

115 E

| 4 | 情報セキュリティポリシー・管理・対策について |
|---|---|

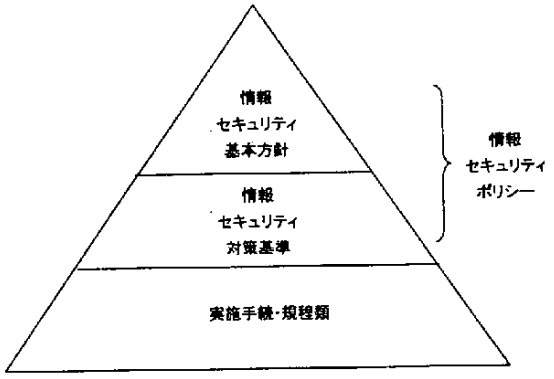
Q22. 情報セキュリティの確保にとり、基本的に重要な視点は何だと思いますか。（複数回答）

| | | |
|---|---|---|
| 116 | 1 | 経営者層の理解 |
| 117 | 2 | 管理者の理解 |
| 118 | 3 | 担当者の理解 |
| 119 | 4 | 社内全体の理解（エンドユーザを含む） |
| 120 | 5 | 法規制の整備 |
| 121 | 6 | その他（　　） |

Q23. 貴事業体では、情報セキュリティ対策（不正アクセス対策、ウイルス対策、信頼性対策、個人情報保護対策等）に情報システム関連支出の何パーセントを使っていますか。（小数点第１位まで）

122 [　　.　　%] 125

以下の質問では、情報セキュリティ対策との関連から情報セキュリティポリシーについてお尋ねします。ここでは、平成１２年７月に官邸が定義した情報セキュリティの３階層をベースにしたものを想定しています。
なお、図の詳細については、官邸の「情報セキュリティポリシーに関するガイドライン」をご参照下さい。
［ＵＲＬ］ http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html




Q24. 貴事業体では経営理念に基づく情報セキュリティポリシー、実施手続・規程類を定めていますか。

| | 策定項目 | 定めている | 現在作成中である | 作成を検討している | 定めていない | 必要ない |
|---|---|---|---|---|---|---|
| 126 | 情報セキュリティポリシー | 1 | 2 | 3 | 4 | 5 |
| 127 | 実施手続・規程類 | 1 | 2 | 3 | 4 | 5 |

⇩ Ｑ２６へ　　Ｑ２７へ

Q25. （Q24 で「ポリシー／規程類を定めている」と回答した場合）情報セキュリティポリシー、実施手続・規程類は定期的に見直していますか。

| | 策定項目 | い　る | いない |
|---|---|---|---|
| 128 | 情報セキュリティポリシー | 1 | 2 |
| 129 | 実施手続・規程類 | 1 | 2 |

Q26. （Q24 で「情報セキュリティポリシーを定めている／作成中」と回答した場合）情報セキュリティポリシーは次のどれを参照して作成していますか。（複数回答）

| | | |
|---|---|---|
| 130 | 1 | JIS X 5080、情報セキュリティポリシーに関するガイドライン（官邸） |
| 131 | 2 | 日本銀行や金融情報システムセンター（FISC）のポリシー |
| 132 | 3 | COBIT (Control Objective for Information and related Technology) などのデファクト標準 |
| 133 | 4 | 自社で独自に開発 |

Q27. 以下の管理について、責任を有する担当者を定めていますか。

| | 管理項目 | 定めている | 設置を検討している | 定めていない | 必要ない |
|---|---|---|---|---|---|
| 134 | ネットワークの管理 | 1 | 2 | 3 | 4 |
| 135 | 情報システムの管理 | 1 | 2 | 3 | 4 |
| 136 | 情報セキュリティの管理 | 1 | 2 | 3 | 4 |

Q28. 情報セキュリティ（システム災害／障害、不正アクセス、ウイルスを含む）管理についての問題点は何ですか。（複数回答）

| | | |
|---|---|---|
| 137 | 1 | 経営者層の理解が得られない |
| 138 | 2 | コストがかかりすぎる |
| 139 | 3 | 専門要員がいない |
| 140 | 4 | 組織の従業員に対する負担がかかりすぎる |
| 141 | 5 | 組織の従業員に対する教育・訓練がいきとどかない |
| 142 | 6 | ノウハウが不足している |
| 143 | 7 | どこまでやればよいのか基準が示されていない |
| 144 | 8 | 要求に合致するもの（サービス／製品）がない |
| 145 | 9 | 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 |
| 146 | 10 | 情報セキュリティ管理が事業の国際化に見合っていない |
| 147 | 11 | その他（　　） |
| 148 | 12 | 特に問題はない |

Q29. 以下の情報セキュリティ要素（1～10）のうち、貴事業体にとって重要と思われる要素を3つ選び、下の回答欄に優先順位をつけて記入して下さい。

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

| 回答欄 | 優先順位 | 第１位 149 | | 第２位 151 | | 第３位 153 | |
|---|---|---|---|---|---|---|---|

155 F

## 5 災害対策・障害対策について

Q30. 情報セキュリティポリシー、実施手続・規程類に基づき、災害・障害対策が明確にされていますか。

| 156 | | |
|---|---|---|
| | 1 | 情報セキュリティポリシーや実施手続・規程類の中で明確になっている |
| | 2 | 他の基準で扱っている |
| | 3 | 特に定めていない（情報セキュリティポリシーがない場合も含む） |

Q31. 「JIS X 5080 規格」の事業継続性管理に定められている事業継続性計画を作成していますか。（オフィススペースの確保等も含む）。

157

| | |
|---|---|
| 1 | 作成している |
| 2 | 作成中である |
| 3 | 作成を含め検討中である |
| 4 | 作成していない |
| 5 | 必要ない |

⇒Q３３へ

Q32. （Q31で「1」、「2」と回答した場合）事業継続性計画には以下の項目を含んでいますか。含まれている項目を選んで下さい。（複数回答）

| | | |
|---|---|---|
| 158 | 1 | 外部からの悪意による緊急事態（サイバーテロ、ウイルス等） |
| 159 | 2 | ネットワークセキュリティ上の緊急事態（重大なセキュリティホール等） |
| 160 | 3 | 事故・災害（火災、地震、風水害、停電等） |
| 161 | 4 | 障害（ハードウェア障害、システムソフトウェア障害、回線障害等） |
| 162 | 5 | 人的なミスに起因する障害・誤処理（プログラムミス、オペレーションミス等） |
| 163 | 6 | 内部犯罪による緊急事態 |
| 164 | 7 | その他（　　） |

Q33. 情報システムの災害に対する復旧対策としてどのようなことを実施していますか。実施している対策を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。（複数回答）

| | | | |
|---|---|---|---|
| 165 | 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） | ⇒Q３５へ |
| 166 | 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 | |
| 167 | 3 | バックアップサービス業者と契約を交わしている | |
| 168 | 4 | 別の場所にバックアップセンタを設置している | |
| 169 | 5 | ネットワークのバックアップを行っている | |
| 170 | 6 | サーバのバックアップ用ファイルを専門保管業者に依頼して保管している | |
| 171 | 7 | サーバのバックアップ用ファイルを遠隔地の自社施設に保管している | |
| 172 | 8 | サーバのバックアップ用ファイルを自社内（耐火金庫等）に保管している | |
| 173 | 9 | サーバのファイルは、遠隔地にミラーファイルを持っている | |
| 174 | 10 | ＰＣ中の業務用ファイルのバックアップを取っている | |
| 175 | 11 | ＰＣ中の業務用ファイルのバックアップを遠隔地に保管している | |
| 176 | 12 | データのバックアップを定期的に行っている | |
| 177 | 13 | その他（　　） | |
| 178 | 14 | アウトソーシング先の対策は把握していない | |
| 179 | 15 | 特に対策を講じていない | ⇒Q３４へ |

Q34. （Q33で「15」と回答した場合）復旧対策を講じない理由は何ですか。主な理由を1つだけ選んで下さい。

180

| | |
|---|---|
| 1 | 経営者層の理解が得られない |
| 2 | コストがかかりすぎる |
| 3 | バックアップに対する必要性を感じていない |
| 4 | 満足する対策がない |
| 5 | その他（　　） |

181 G

Q35. 情報システムの障害対策として次の機能を設けていますか。現在設置している機能を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。（複数回答）

| | |
|---|---|
| 1 | デュアルシステム |
| 2 | デュプレックスシステム |
| 3 | ホットスタンバイシステム |
| 4 | コールドスタンバイシステム |
| 5 | クラスタリング |
| 6 | 高可用性機構 |
| 7 | ミラリング |
| 8 | フォールトトレラント |
| 9 | アウトソーシング先の対策は把握していない |
| 10 | 特に設けていない |

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

Q36. サーバ設置場所、データ保管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。各場所別に実施している対策を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。（複数回答）

| 対策項目 | サーバ設置場所 | データ保管場所 |
|---|---|---|
| 自動火災報知設備を設置している | 192 1 | 202 2 |
| ガス式の消火設備を設置している | 193 1 | 203 2 |
| 消火器を設置している | 194 1 | 204 2 |
| スプリンクラ消火設備を設置している | 195 1 | 205 2 |
| 排煙設備を設置している | 196 1 | 206 2 |
| 耐火金庫を設置している | 197 1 | 207 2 |
| 消火・排煙等の防災機器の点検を定期的に行っている | 198 1 | 208 2 |
| その他<br>（右の欄に具体的に対策を書いて下さい） | 199 1 | 209 2 |
| アウトソーシング先の対策は把握していない | 200 1 | 210 2 |
| 特に対策を講じていない | 201 1 | 211 2 |

Q37. サーバ設置場所、データ保管場所ではどのような地震対策をとっていますか。各場所別に実施している対策を選んで下さい。なお、アウトソーシングしている場合は、アウトソース先が実施している対策を選んで下さい。（複数回答）

| 対策項目 | サーバ設置場所 | データ保管場所 |
|---|---|---|
| 建物が免震構造になっている | 212 1 | 222 2 |
| 建物が耐震構造になっている | 213 1 | 223 2 |
| 転倒防止措置を講じている | 214 1 | 224 2 |
| 機器の移動防止措置を講じている | 215 1 | 225 2 |
| フリーアクセス床は耐震構造としている | 216 1 | 226 2 |
| フリーアクセス床は免震構造としている | 217 1 | 227 2 |
| 媒体の落下防止措置を講じている | 218 1 | 228 2 |
| その他<br>（右の欄に具体的に対策を書いて下さい） | 219 1 | 229 2 |
| アウトソーシング先の対策は把握していない | 220 1 | 230 2 |
| 特に対策を講じていない | 221 1 | 231 2 |

232 H

Q38. 電源設備の災害対策としてどのような対策をとっていますか。実施している対策を選んで下さい。（複数回答）

| | | |
|---|---|---|
| 233 | 1 | ＡＶＲ |
| 234 | 2 | ＣＶＣＦ／ＵＰＳ |
| 235 | 3 | 自家発電装置 |
| 236 | 4 | 電力供給経路の複数化 |
| 237 | 5 | その他（　　） |
| 238 | 6 | 特に対策を講じていない |

Q39. 水冷の空調設備（室外機にクーリングタワーを使っている等）を使っている場合、空調用の水は何日分確保していますか。

| | | |
|---|---|---|
| 239 | 1 | １日分～３日分 |
| | 2 | ４日分～６日分 |
| | 3 | ７日分以上 |
| | 4 | まったく確保していない |
| | 5 | 水冷の空調設備を使用していない |

Q40. 情報システム、サーバ設置場所、機器の災害・障害等で今後強化しなければならないと思う対策は何ですか。（複数回答）

| | | |
|---|---|---|
| 240 | 1 | 自然災害対策 |
| 241 | 2 | 電源障害対策 |
| 242 | 3 | 空調等障害対策 |
| 243 | 4 | 回線障害対策 |
| 244 | 5 | ハードウェア障害対策 |
| 245 | 6 | ＯＳ障害対策 |
| 246 | 7 | ソフトウェア障害対策 |
| 247 | 8 | 火災による事故・障害対策 |
| 248 | 9 | 人の悪意による事故等への対策 |
| 249 | 10 | オペミス等、人の過失による事故等への対策 |
| 250 | 11 | テロによる機器の運用停止（ＤＤＯＳ：ＤＯＳアタックを含む）対策 |
| 251 | 12 | 取引先システムの停止や異常処理対策 |

Q41. 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）

| | | |
|---|---|---|
| 252 | 1 | 通信事業者のケーブル障害（専用回線を含む） |
| 253 | 2 | 通信事業者の設備障害 |
| 254 | 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 |
| 255 | 4 | ＩＳＰ（インターネットサービスプロバイダ）サービスの中断・停止 |
| 256 | 5 | ＬＡＮ（配線）の障害 |
| 257 | 6 | ルータ・サーバ（機器）の障害 |
| 258 | 7 | 地震などの一定地域の災害 |
| 259 | 8 | その他（　　） |
| 260 | 9 | 特に想定していない |

Q42. どのようなネットワーク障害対策を実施していますか。実施している対策を選んで下さい。（複数回答）

| | | |
|---|---|---|
| 261 | 1 | 異なる種別回線を利用 |
| 262 | 2 | 異なる交換局への収容 |
| 263 | 3 | 異なるコモンキャリアの利用 |
| 264 | 4 | 異なるＩＳＰを利用 |
| 265 | 5 | 異なるメディアによる回線利用（例：衛星回線等） |
| 266 | 6 | ポイント間接続から網接続へ |
| 267 | 7 | 重要回線を部分的に二重化 |
| 268 | 8 | 専用のバックアップ回線を常時設定 |
| 269 | 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 |
| 270 | 10 | 社内の構内回線、ＬＡＮ等を二重化 |
| 271 | 11 | 通信機器（ＣＣＵ、ルータ、社外WWWサーバ、ＤＮＳサーバ、アクセスサーバ等）の二重化 |
| 272 | 12 | インターネットに接続したサーバの分散（負荷分散、地域分散） |
| 273 | 13 | その他（　　） |
| 274 | 14 | 特に対策を講じていない |

Q43. 貴事業体では従業員に対し、情報セキュリティの面（災害／障害、不正アクセス、ウイルスを含む）から教育・訓練を実施していますか？

| | | |
|---|---|---|
| 275 | 1 | 定期的に実施している |
| | 2 | 時々実施している |
| | 3 | 実施を予定している |
| | 4 | 特に実施していない |

Q44. 貴事業体では情報セキュリティの人材をどのように養成していますか。

| | | |
|---|---|---|
| 276 | 1 | 自社育成プログラムにより高度な人材育成を行っている |
| | 2 | 民間資格を利用して育成している |
| | 3 | 情報セキュリティアドミニストレータ試験を活用している |
| | 4 | 特に行っていない |
| | 5 | 必要ない |

277 | 1 |

| | |
|---|---|
| 6 | 不正アクセス対策・不正侵入対策・情報漏洩対策について |

Q45. 「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。

| | | |
|---|---|---|
| 278 | 1 | 知っている |
| | 2 | 知らない |

Q46. 貴事業体では過去１年間に不正アクセスの被害に遇われたことがありますか。（複数回答）

| | | | |
|---|---|---|---|
| 279 | 1 | 物理的なアクセス被害（コンピュータ室等への侵入）に遭った | |
| 280 | 2 | 論理的アクセス被害（ネットワーク経由による侵入）に遭った | |
| 281 | 3 | な　い | ⇒Ｑ４８へ |

Q47. （Q47 で「１」、「２」と回答した場合）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。

| | | |
|---|---|---|
| 282 | 1 | 出した |
| | 2 | 出さない |

Q48. 主要なサーバ設置場所、データ保管場所での物理的な不正アクセスに対してどのような対策を実施していますか。現在実施している対策を選んで下さい。（複数回答）

| | | |
|---|---|---|
| 283 | 1 | 不正アクセスを受けた場合のＩＰＡやＪＰＣＥＲＴ／ＣＣへの相談 |
| 284 | 2 | 室の出入口での入室管理 |
| 285 | 3 | 室の出入口での退室管理 |
| 286 | 4 | 室への入退室についてカード、パスワードを使用 |
| 287 | 5 | 入退室のときにアンチパスバック（定期券のように二度連続して入れないような仕組み）を持っている |
| 288 | 6 | 室への入室について身体的特徴（指紋、虹彩等）により識別 |
| 289 | 7 | 室の管理責任者を定めている |
| 290 | 8 | 情報システムの監視設備を設けている |
| 291 | 9 | 定期的にリスク分析や情報セキュリティ監査を実施 |
| 292 | 10 | その他（　　） |
| 293 | 11 | アウトソーシングのため、自社では特に対策を講じていない |
| 294 | 12 | 特に対策を講じていない |

Q49. ネットワークを介しての論理的な不正アクセスに対してどのような対策を実施していますか。現在実施している対策を選んで下さい。（複数回答）

| | | |
|---|---|---|
| 295 | 1 | 不正アクセスを受けた場合のＩＰＡやＪＰＣＥＲＴ／ＣＣへの相談 |
| 296 | 2 | パスワードの活用 |
| 297 | 3 | ファイアウォールの利用 |
| 298 | 4 | セキュリティパッチの適用 |
| 299 | 5 | アクセス制御ソフトウェアの使用 |
| 300 | 6 | 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の実施 |
| 301 | 7 | ネットワーク機器の運用者（アクセス範囲）の限定 |
| 302 | 8 | 情報セキュリティポリシーで勝手にＬＡＮの配線を触ったり、個人のＰＣを接続することの禁止 |
| 303 | 9 | 情報セキュリティ管理者がサーバやルータ、ファイアウォールのログの定期的にチェック |
| 304 | 10 | 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 |
| 305 | 11 | 情報セキュリティ監査の実施 |
| 306 | 12 | システム監査の実施 |
| 307 | 13 | その他（　　） |
| 308 | 14 | 特に対策を講じていない |

Q50. 情報価値の視点から機密度のランクを設定していますか。

| | | |
|---|---|---|
| 309 | 1 | ランクを設定し、暗号化している |
| | 2 | ランクは設定していないが、暗号化はしている |
| | 3 | ランクを設定しているが、暗号化はしていない |
| | 4 | 暗号化していない |

Q51. 貴事業体では基幹システム(注) のパスワード変更をどのレベルに設定していますか。

| | | |
|---|---|---|
| 310 | 1 | ワンタイムパスワードを設定している |
| | 2 | 変更期限がきたらパスワードを無効にする |
| | 3 | 定期的に新しいパスワードを配布する |
| | 4 | 変更期限を定めて利用者が変更している |
| | 5 | パスワードの変更を推奨しているが、変更期間は利用者に任せている |
| | 6 | パスワードの変更に関して特に定めていない |
| | 7 | パスワードによる管理を実施していない |
| | 8 | その他（　　） |

（注）最も重要なシステム１つに限定してお答え下さい。（ｐ３「基幹システムの説明」を参照のこと）

Q52. 情報漏洩対策として行っていることは何ですか。（複数回答）

| | | |
|---|---|---|
| 311 | 1 | セキュリティポリシー、規程類の整備 |
| 312 | 2 | 従業員に対する教育 |
| 313 | 3 | 入退室（館）管理 |
| 314 | 4 | アクセス管理 |
| 315 | 5 | 機密情報の管理 |
| 316 | 6 | 情報媒体（ＰＣ、携帯電話、ＰＤＡ、記録媒体等）の持出し・持込みの禁止 |
| 317 | 7 | ハードディスク、ＣＤ、ＦＤ等記録媒体の返却、廃棄時の破壊、溶解 |
| 318 | 8 | 暗号化機能の採用 |
| 319 | 9 | 輸送体制強化 |
| 320 | 10 | 電子メールのモニタリング |
| 321 | 11 | ログチェックの追跡機能 |
| 322 | 12 | その他（　　） |
| 323 | 13 | 特に対策を行っていない |

324 J

| | |
|---|---|
| 7 | コンピュータウイルス対策について |

Q53. 貴事業体では過去１年間にコンピュータウイルスに感染したことがありますか。

| | | |
|---|---|---|
| 325 | 1 | あ　る |
| | 2 | な　い |

⇒Ｑ５６へ

Q54. （Q53 で「1」と回答した場合）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。

| | | |
|---|---|---|
| 326 | 1 | 出した |
| | 2 | 出さない |

Q55. 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）

| | | |
|---|---|---|
| 327 | 1 | フリーソフトウェアから |
| 328 | 2 | 外部から入手した記録媒体（ＦＤ、パソコン等）から |
| 329 | 3 | 社内ネットワーク経由で |
| 330 | 4 | インターネット経由で |
| 331 | 5 | 電子メールの添付書類で |
| 332 | 6 | 外部のホームページの閲覧で |
| 333 | 7 | その他（　　） |
| 334 | 8 | わからない |

Q56. コンピュータウイルスに対してどのような対策を実施していますか。現在実施している対策を選んで下さい。（複数回答）

| | | |
|---|---|---|
| 335 | 1 | コンピュータウイルス被害を受けた場合のＩＰＡへの相談 |
| 336 | 2 | ウイルス対策用のマニュアル（セキュリティ対策基準に入れた場合も含む）の作成 |
| 337 | 3 | ウイルス対策チーム（社内でウイルスが検出された時の対応を行うチーム）の設置 |
| 338 | 4 | ウイルス検出時や緊急対応と連絡体制の整備 |
| 339 | 5 | ソフトウェアの出所の確認 |
| 340 | 6 | 記録媒体のウイルスチェックの実施 |
| 341 | 7 | ライトプロテクト、バックアップ等のソフトウェア管理 |
| 342 | 8 | ＰＣでのワクチンソフト（ウイルス検出ソフトを含む）の利用 |
| 343 | 9 | ＰＣのワクチンソフト・パラメータファイルを定期的に更新 |
| 344 | 10 | サーバ機でのワクチンソフトの利用 |
| 345 | 11 | メール用ゲートウェイ／サーバでのワクチンソフトの利用 |
| 346 | 12 | メール用ゲートウェイ／サーバでの添付ファイルの制限（例：実行ファイル削除） |
| 347 | 13 | ワクチンソフトの集中監視 |
| 348 | 14 | 定期的な集中監視ログの解析 |
| 349 | 15 | パスワードの変更等、アクセスコントロールの強化 |
| 350 | 16 | 動作の定期的な確認等、異常発見体制の整備 |
| 351 | 17 | 緊急時の電子メールサーバの停止 |
| 352 | 18 | 緊急時の社員への連絡（ウイルス警告の放送／送付） |
| 353 | 19 | ＯＳの修正プログラムの適用（アップデートを含む） |
| 354 | 20 | アプリケーションの修正プログラムの適用（アップデートを含む） |
| 355 | 21 | ウイルス対策サービスの利用 |
| 356 | 22 | その他（　　） |
| 357 | 23 | 特に対策を講じていない |

358 K

| | |
|---|---|
| 8 | アウトソーシングについて |

Q57. 貴事業体では運用に関し、アウトソーシングを利用していますか。

| | | |
|---|---|---|
| 359 | 1 | 利用している |
| | 2 | 利用していない　⇒Ｑ６０へ |

Q58. （Q57で「1」と回答した場合）アウトソーシング先を選定する場合、どのような観点から選定していますか。（複数回答）

| | | |
|---|---|---|
| 360 | 1 | コスト |
| 361 | 2 | 専門性 |
| 362 | 3 | セキュリティ |
| 363 | 4 | 品質（サービスレベル） |
| 364 | 5 | 開発を依頼した会社をそのままメンテナンス先に選定 |
| 365 | 6 | その他（　　） |

Q59. アウトソーシング先との契約において情報セキュリティ関係で重視している項目はどれですか。（複数回答）

| | | |
|---|---|---|
| 366 | 1 | セキュリティポリシー |
| 367 | 2 | 社員の教育体制 |
| 368 | 3 | 守秘義務契約 |
| 369 | 4 | サービスレベル（業務中断時間） |
| 370 | 5 | ウイルス対策 |
| 371 | 6 | 不正アクセス対策 |
| 372 | 7 | 火災、災害対策 |
| 373 | 8 | 入退室、侵入対策 |
| 374 | 9 | 機械事故対策 |
| 375 | 10 | オペレーションミス対策 |
| 376 | 11 | 事故後の早期復旧対策 |
| 377 | 12 | 認証制度の取得 |
| 378 | 13 | 監査など内部統制対策 |
| 379 | 14 | 委託元による監査の実施 |
| 380 | 15 | 賠償責任 |
| 381 | 16 | その他（ ） |

382 L

| | |
|---|---|
| 9 | システム監査・情報セキュリティ監査について |

Q60. 過去２年以内にシステム監査を実施したことがありますか。（業務監査に含まれている場合を含む）

| | | | |
|---|---|---|---|
| 383 | 1 | 実施し た（実施中を含む） | |
| | 2 | 実施しない | ⇒Ｑ６２へ |
| | 3 | これから実施する予定がある | ⇒Ｑ６３へ |

Q61. （Q60で「1」と回答した場合）システム監査を実施した結果、どのような点に効果があったと思いますか。（複数回答）

| | | | |
|---|---|---|---|
| 384 | 1 | システムに起因する事故・障害が未然に防止できた | ⇒Ｑ６３へ |
| 385 | 2 | リスク対策をどこまで考慮すればよいかが明らかになった | |
| 386 | 3 | 担当者がリスクを考慮しながら業務を実行するようになった | |
| 387 | 4 | システム部門に対する過大な要求がなくなった | |
| 388 | 5 | システムの信頼性向上対策のレベルが明らかになった | |
| 389 | 6 | システムの有効利用が促進された | |
| 390 | 7 | システムの効率性が確保できた | |
| 391 | 8 | 有効なシステムの開発設計が可能になった | |
| 392 | 9 | 業務の継続性の確保が図られた | |
| 393 | 10 | 要員が規定・ルール等を意識して業務を実行するようになった | |
| 394 | 11 | その他（ ） | |
| 395 | 12 | 効果は得られなかった | |

Q62. （Q60で「2」と回答した場合）システム監査を実施していない理由は何ですか。（複数回答）

| | | |
|---|---|---|
| 395 | 1 | 経営者層が重要性を認識していないため |
| 397 | 2 | システム監査実施のためのコンセンサス、組織風土が十分に備わっていない |
| 398 | 3 | システム監査の実施よりもシステム化推進そのものに力点がある |
| 399 | 4 | システム監査の方法、制度、手続きなどが十分ではない |
| 400 | 5 | 効果が明確でない |
| 401 | 6 | 適切なシステム監査人が見つからない |
| 402 | 7 | アウトソーシングしているため |
| 403 | 8 | その他（　　） |

Q63. 情報セキュリティ監査を実施したことがありますか。（業務監査に含まれている場合を含む）

| | | |
|---|---|---|
| 404 | 1 | 実施した |
| | 2 | これから行う予定がある |
| | 3 | 実施しない |

⇒Q65へ

Q64. （Q63で「3」と回答した場合）情報セキュリティ監査を実施していない理由は何ですか。（複数回答）

| | | |
|---|---|---|
| 405 | 1 | 経営者層が重要性を認識していないため |
| 406 | 2 | 情報セキュリティ監査実施のためのコンセンサス、組織風土が十分に備わっていない |
| 407 | 3 | 情報セキュリティ監査制度をよく知らない |
| 408 | 4 | 情報セキュリティ監査の方法、手続きなどが十分ではない |
| 409 | 5 | 効果が明確でない |
| 410 | 6 | 適切な情報セキュリティ監査企業・監査人が見つからない |
| 411 | 7 | 情報セキュリティマネジメントシステム（ＩＳＭＳ）の認証を取得しているため、不要である |
| 412 | 8 | その他（　　） |

413 M

## 10 個人情報保護について

Q65. 貴事業体ではどのような個人情報を取り扱っていますか。（複数回答）

| | | |
|---|---|---|
| 414 | 1 | 売買等契約の履行 |
| 415 | 2 | 顧客サポート |
| 416 | 3 | 代金等の回収 |
| 417 | 4 | 情報提供 |
| 418 | 5 | マーケティング |
| 419 | 6 | 商品開発 |
| 420 | 7 | 行政サービスの履行 |
| 421 | 8 | 委託（受託）処理 |
| 422 | 9 | 従業員情報（雇用に関わる届出情報（採用時を含む）、給与、保険関係、健康診断結果、退職者情報等） |
| 423 | 10 | その他（　　） |

Q66. 「個人情報の保護に関する法律（平成１５年５月３０日法律第５７号）」を知っていますか。

| | | |
|---|---|---|
| 424 | 1 | 内容を知っている |
| | 2 | 制定されたことを知っている |
| | 3 | 知らない |

Q67. 個人情報保護法が施行されるまでに、どのような対応策を講じますか。

| | | |
|---|---|---|
| 425 | 1 | 社内にプロジェクトを立ち上げて管理体制を見直し、必要な対策を講じる予定である |
| | 2 | 外部コンサルタントに委託して管理体制を見直し、必要な対策を講じる予定である |
| | 3 | すでに対応策を講じる準備を開始している |
| | 4 | プライバシーマークの認証を受けて対応を済ませている |
| | 5 | 個人情報保護のための規程を整備している |
| | 6 | その他（　　） |
| | 7 | 現状の管理体制で十分なので、特に何も対応策を講じない |

Q68. 現在の個人情報の管理状況についてリスクをどのように認識していますか。

| | | |
|---|---|---|
| 426 | 1 | 対応策を講じているので、リスクはないと認識している |
| | 2 | 現状の管理方法で何も問題が発生していないので、リスクはないと認識している |
| | 3 | 何度かヒヤリ・ハッとした経験があり、リスクがあると認識している |
| | 4 | いつ問題が発生してもおかしくない状況であると認識している |
| | 5 | その他（　　） |
| | 6 | 特に認識していない |

Q69. 個人情報保護対策として、現在何を実施していますか。また、今後どういうことを実施する予定ですか。（複数回答）

| 対　策 | 現在実施している対策 | 今後実施を予定している対策 |
|---|---|---|
| 管理責任者を置いている（保護体制（役割、責任、権限）を確立する | 427 1 | 437 2 |
| 個人情報保護に関する規程を定め運用している | 428 1 | 438 2 |
| 個人情報保護のマネジメントシステムを構築して（プライバシーマークの認定を受ける）運用している | 429 1 | 439 2 |
| 社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している | 430 1 | 440 2 |
| 定期的に監査（内部監査／外部監査）を実施している | 431 1 | 441 2 |
| リスク分析を実施して必要な安全対策を構築している | 432 1 | 442 2 |
| 苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応している | 433 1 | 443 2 |
| 仮に問題が発生した時の被害の拡大防止策を講じるような対応措置を定めている | 434 1 | 444 2 |
| その他（　　） | 435 1 | 445 2 |
| 特に対策を講じない | 436 1 | 446 2 |

Q70. 取り扱っ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）

| | | | |
|---|---|---|---|
| 447 | 1 | 営業活動（名刺交換、Ｗｅｂ、メール、申込書等）により情報主体（当該個人）から直接収集 | |
| 448 | 2 | 名簿業者等から購入 | ⇒Ｑ７３へ |
| 449 | 3 | グループ企業から入手 | |
| 450 | 4 | 他社から提供を受ける | |
| 451 | 5 | 業務委託契約等に基づき提供を受ける | |
| 452 | 6 | 新聞、雑誌等メディアからの収集 | |
| 453 | 7 | その他（　　） | |

Q71. （Q70 で「1」と回答した場合）情報主体から直接に収集する場合、収集・利用目的について同意を取っていますか。

454

| | |
|---|---|
| 1 | は　い |
| 2 | いいえ |
| 3 | わからない |

Q72. 個人情報を個人から直接に収集する場合、利用目的を通知して同意を取ることについてどう考えますか。

455

| | | |
|---|---|---|
| 1 | 当然必要である | ⇒Q74へ |
| 2 | 同意を取る手続きが困難で、業務遂行に大きな影響を及ぼすために対応できない | |
| 3 | 個人と取引を遂行するうえで、暗黙のうちに個人が同意しているはずであるから必要ない | |
| 4 | 個人が積極的に提供しているのだから、改めて同意を取る必要性を感じない | |
| 5 | もともと意識のない個人に改めて同意を取ることの意味がない | |
| 6 | 個人から苦情を申し立てられるような利用をしていないので、必要と思わない | |

Q73. （Q70 で「2」～「6」と回答した場合）間接的に収集する場合、収集・利用目的についてどのような対応を行っていますか。

456

| | |
|---|---|
| 1 | 情報主体から利用に関し、改めて同意を取っている |
| 2 | 情報主体が他社への提供について同意していることを情報提供者（入手先）に確認している |
| 3 | 何もしていない |

Q74. 個人情報を外部委託する場合に交わす契約条項には何がありますか。（複数回答）

457

| | |
|---|---|
| 1 | 秘密保持義務 |
| 2 | 責任分担（漏洩事故発生時の損害賠償　等） |
| 3 | 個人情報の適正な管理（廃棄、返却、授受等） |
| 4 | 目的外使用・再委託禁止 |
| 5 | その他（　　） |
| 6 | 外部委託を行っていない |

Q75. 個人情報保護への対応策としてプライバシーマークの認定を受けることが有効だと思いますか。

463

| | |
|---|---|
| 1 | 社内の管理体制（コンプライアンス・プログラム）が構築できて有効である |
| 2 | 有効であるが事業者にとっては負担が重い |
| 3 | 有効とは思わない<br>（理由：　　） |

464 N

○今後必要と思われる情報セキュリティ制度・サービス・機能・製品等がありましたら、具体的にお書き下さい。

○貴事業体で実施している情報セキュリティ対策について、問題点があれば具体的に書いて下さい。

ご協力ありがとうございました。

KEIRIN

このアンケートは競輪の補助金を受けて実施するものです。

平成１６年３月発行

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

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

H15-H002