

# 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18年3月



財団法人 日本情報処理開発協会



この資料は、競輪の補助金を受けて作成したものです。





## 序

この報告書は、財団法人日本情報処理開発協会が日本自転車振興会の補助金を受けて実施した平成 17 年度情報化の進展に関する補助事業「情報セキュリティ基盤の強化に関する調査研究」事業の一環としてとりまとめたものです。

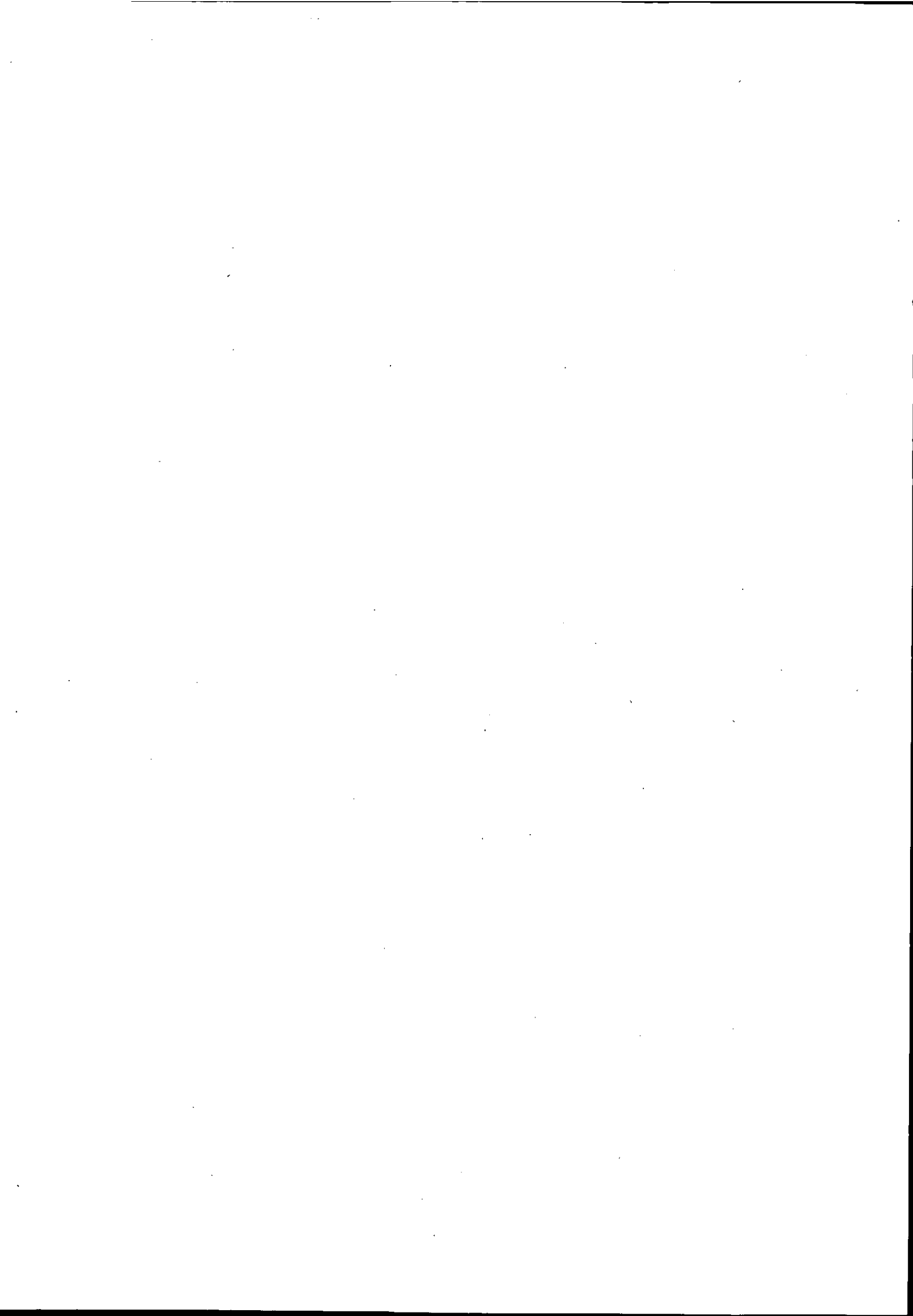
当協会では、この度わが国における情報システムのセキュリティ対策の状況を把握するため、「情報セキュリティに関する調査」を実施いたしました。

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狙いとしています。

調査にあたっては、514 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、調査結果とりまとめ等にご協力いただいた情報セキュリティ調査 WG の委員をはじめとする各位に心から謝意を表します。

平成 18 年 3 月

財団法人日本情報処理開発協会



平成17年度情報セキュリティ調査WG

(敬称略／五十音順)

|     |        |                                                     |
|-----|--------|-----------------------------------------------------|
| 委員長 | 森宮 康   | 明治大学 商学部教授                                          |
| 委員  | 指田 朝久  | 東京海上日動リスクコンサルティング(株)<br>リスクコンサルティング室情報グループ グループリーダー |
|     | 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<br>マーケティングソリューション研究グループ 主席研究員          |
|     | 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   |
| 1.1 調査の概要 .....                         | 1   |
| 1.1.1 調査の目的 .....                       | 1   |
| 1.1.2 調査の対象 .....                       | 1   |
| 1.1.3 調査時期 .....                        | 1   |
| 1.1.4 回収状況 .....                        | 1   |
| 1.1.5 回答事業体の平均従業員数 .....                | 1   |
| 1.1.6 調査項目 .....                        | 1   |
| 1.1.7 調査対象業種および回収状況 .....               | 2   |
| 1.2 調査結果の要約 .....                       | 3   |
| 1.2.1 経済産業省の安全対策の施策について .....           | 3   |
| 1.2.2 情報リスクマネジメントについて .....             | 4   |
| 1.2.3 情報セキュリティポリシー・管理・対策について .....      | 7   |
| 1.2.4 災害対策・障害対策について .....               | 8   |
| 1.2.5 不正アクセス対策・不正侵入対策・情報漏えい対策について ..... | 9   |
| 1.2.6 コンピュータウイルス対策について .....            | 10  |
| 1.2.7 システム監査・情報セキュリティ監査について .....       | 10  |
| 1.2.8 個人情報保護について .....                  | 11  |
| 2. 調査結果の詳細 .....                        | 15  |
| 2.1 経済産業省の安全対策の施策について .....             | 15  |
| 2.2 情報リスクマネジメントについて .....               | 20  |
| 2.3 情報セキュリティポリシー・管理・対策について .....        | 66  |
| 2.4 災害対策・障害対策について .....                 | 83  |
| 2.5 不正アクセス対策・不正侵入対策・情報漏えい対策について .....   | 97  |
| 2.6 コンピュータウイルス対策について .....              | 105 |
| 2.7 システム監査・情報セキュリティ監査について .....         | 110 |
| 2.8 個人情報保護について .....                    | 119 |
| 2.9 その他 .....                           | 129 |

|                 |     |
|-----------------|-----|
| 3. クロス集計結果の分析   | 130 |
| 3.1 Q 3 のクロス集計  | 132 |
| 3.2 Q 4 のクロス集計  | 135 |
| 3.3 Q 6 のクロス集計  | 140 |
| 3.4 Q 8 のクロス集計  | 145 |
| 3.5 Q13-①のクロス集計 | 156 |
| 3.6 Q13-②のクロス集計 | 161 |
| 3.7 Q14-①のクロス集計 | 164 |
| 3.8 Q18 のクロス集計  | 167 |
| 3.9 Q22 のクロス集計  | 176 |
| 3.10 Q24 のクロス集計 | 184 |
| 3.11 Q25 のクロス集計 | 187 |
| 3.12 Q41 のクロス集計 | 194 |
| 3.13 Q46 のクロス集計 | 196 |

|                                |     |
|--------------------------------|-----|
| 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 | 203 |
|--------------------------------|-----|

## 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（以下、「JIPDEC」という。）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 17 年 11 月 22 日 |
| 回収締切  | 平成 18 年 1 月 16 日  |

#### 1.1.4 回収状況（表 1-1 参照）

|          |              |
|----------|--------------|
| 発送数      | 4,000 件      |
| 回収数（回収率） | 514 件（12.9%） |

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%、15 年度 15.1%と、回収率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、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、調査結果には情報セキュリティ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

2,191 人

#### 1.1.6 調査項目（計 56 項目）

1. 経済産業省の安全対策の施策について（2 項目）
2. 情報リスクマネジメントについて（15 項目）
3. 情報セキュリティポリシー・管理・対策について（5 項目）
4. 災害対策・障害対策について（9 項目）
5. 不正アクセス対策・不正侵入対策・情報漏えい対策について（5 項目）
6. コンピュータウイルス対策について（3 項目）
7. システム監査・情報セキュリティ監査について（5 項目）
8. 個人情報保護について（12 項目）

今回の質問構成は全体で56項目からなっており、平成15年度調査(75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

調査対象の業種は表1-1の40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

| 業務グループ         | 業 種             | 回収数 | 平均従業員数 | 業務グループ    | 業 種               | 回収数             | 平均従業員数 |       |
|----------------|-----------------|-----|--------|-----------|-------------------|-----------------|--------|-------|
| 食品・紙・パルプ・繊維・印刷 | 食品製造業           | 14  | 911    | 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 | 81              | 618    |       |
|                | 繊維工業            | 10  | 1,291  |           | 農・林・漁・狩・水産養殖業     | 0               | -      |       |
|                | 紙・パルプ・紙加工品製造業   | 1   | 1,277  |           | 鉱業                | 1               | 171    |       |
|                | 印刷業・同関連産業       | 2   | 6,567  |           | 建設業               | 26              | 2,507  |       |
| 石油・化学・鉄鋼・非鉄・金属 | 化学工業            | 15  | 3,597  |           | 所以对事業所サービス        | 新聞業・出版業         | 3      | 884   |
|                | 石油製品製造業         | 1   | 2,500  |           |                   | 不動産業            | 0      | -     |
|                | 鉄鋼業             | 5   | 1,056  |           |                   | 運輸・通信・倉庫業       | 31     | 976   |
|                | 非鉄金属製造業・金属製品製造業 | 15  | 430    |           |                   | 電力・ガス業          | 4      | 6,258 |
| 電気・一般・輸送・精密機械  | 一般機械器具製造業       | 17  | 1,589  |           |                   | 放送業             | 2      | 112   |
|                | 電気機械器具製造業       | 26  | 7,913  |           |                   | 広告・調査・情報提供サービス業 | 3      | 1,842 |
|                | 輸送用機械器具製造業      | 10  | 4,025  |           |                   | その他のサービス業       | 6      | 1,000 |
|                | 精密機械器具製造業       | 7   | 1,717  | 公共サービス    |                   | 医療業             | 2      | 3,407 |
| その他製造業         | 窯業・土石製品製造業      | 4   | 2,111  |           |                   | 宗教法人            | 0      | -     |
|                | その他製造業          | 27  | 1,004  |           |                   | 高校              | 1      | 115   |
| 商 業            | 卸業・商社           | 24  | 871    |           |                   | 大学              | 18     | 729   |
|                | 小売業             | 13  | 4,252  |           | その他の教育機関          | 2               | 1,134  |       |
| 金融・保険業         | 金融業             | 46  | 1,663  |           | 政府・地方公共団体         | 学術研究機関          | 2      | 1,931 |
|                | 証券業・商品取引業       | 4   | 1,020  |           |                   | 法人団体・農協         | 13     | 842   |
|                | 生命保険業           | 7   | 13,304 | 政府        |                   | 3               | 5,768  |       |
|                | 損害保険業           | 7   | 3,453  | 地方公共団体    |                   | 61              | 3,015  |       |
| 小 計            |                 | 255 | -      | 小 計       |                   | 259             | -      |       |
| 合 計            |                 |     |        |           |                   | 514             | 2,191  |       |

## 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、8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に項目を残している。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、今年度の調査結果については「今回調査」、15年度調査結果については「前回調査」、それ以前の調査結果については、それぞれ年号を用いている。また、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』、『システム監査基準』、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』、平成15年4月から運用が開始されている『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』がある。このうち『システム監査基準』については、平成16年に改訂され、従来の『システム監査基準』と新設された『システム管理基準』の2本立てとなった。

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」とする回答は新設の『システム管理基準』以外が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19.8%が「利用」しており、「知っている」のは57.6%であった。『コンピュータウイルス対策基準』は20.8%が「利用」しており、「知っている」は59.3%である。『コンピュータ不正アクセス対策基準』については19.3%が「利用」しており、「知っている」は60.5%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12.5%であった。また、旧システム監査基準から独立した『システム管理基準』は「利用している」が10.1%、「知っている」は58.0%と、現行のシステム監査基準の認知度に比べ、若干低い結果となった。

『情報セキュリティ監査制度』については、運用開始半年後の前回調査時点ですでに約6割の認知度であったが、今回調査では「利用している」が9.5%、「知っている」が61.1%と、システム監査基準の認知度とほぼ同じとなった。

いずれの基準についても、基準の存在を知りつつも利用率がなぜ低いのか、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』の運用開始からすでに10年以上が経過しているが、「知っている」は51.8%と過半数を超えたものの、実際に台帳を「利用している」事業体の数は3.1%と非常に低い。

『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認知度とほぼ同じ結果となった（「知っている」47.9%、「利用している」7.8%）。（Q1）。

『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18.7%、「知っている」が41.2%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6.4%と前回調査の3.3%から3.1ポイント増、「知っている」は45.1%と、前回調査の32.7%から約13ポイント増加となった。

『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」は42.4%（H15：37.5%）、「利用している」は24.9%（H15：8.6%、16.3ポイント増）となった。

今回調査で新たに『事業継続計画（BCP）策定ガイドライン』（平成17年3月策定）、『事業継続ガイドライン（第1版）』（平成17年8月策定）の認知度を調査した。

両ガイドラインともに策定直後の調査であったが、「利用している」がそれぞれ4.3%、3.7%、「知っている」が40.5%、38.3%と、認知度はいずれも4割を超えている（44.8%、42.0%）。

情報セキュリティ適合性評価制度（ISMS 認証制度）の認証基準とされている『ISMS 認証基準（Ver. 2.0）』（平成17年）は、「利用している」が22.0%、「知っている」が51.9%と、73.9%の認知度となった。（Q2）。

### 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、前回調査から情報リスクマネジメントに対する意識調査を行っている。この点について、前回調査同様、9割程度が情報リスクマネジメントを重視しているが、具体的には「重要と考え実践している」が前回調査の26.3%から40.9%へと約15ポイント増加し、「重要と考えている」が63.8%から49.6%に減少した。前回調査からの増減がそのまま単に「考えている」ことから「実践」に動いたことになる（Q3）。

情報リスクについては経営者の認識が重要であるが、今回調査では以下の4点について認識度を調査した。（前回調査では①のみを調査）

①「情報システム関連の事件・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63.2%と前回調査（37.0%）から26.2ポイントの増加となり、逆に「低い」は15.2%から8.9%に減少した。また、「わからない」は前回調査（7.6%）から3.9%へと約半数になった。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。

②「個人情報などの情報漏えいに対するリスク」については、関心が「高い」は69.3%、逆に「低い」は7.6%となった。

③「情報セキュリティガバナンス」への関心度合いはまだ低く、「高い」（19.5%）と「低い」（15.2%）であまり差はみられない。なお、「わからない」との回答が3割を若干超えた。

④「情報セキュリティ対策ベンチマーク」についても情報セキュリティガバナンス同様、「わからない」との回答が37.0%と最も多い。（Q4）

情報システム関連、情報セキュリティ関連、個人情報漏えいのリスクが事業体の経営に重大な

影響を与えるかとの調査については、約9割が何らかの影響を受けると感じている。(Q5)

「情報セキュリティガバナンス」の観点から、どのような関係者を考慮しているかとの調査を行った。最も多いのは、「顧客・消費者等」が70.8%、次いで「従業員」(57.4%)、「取引先」(56.0%)の順となっている。(Q6)

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いるが、リスク分析手法の認識度調査において、利用したことがあるリスク分析手法で最も多かったのは『JRMS』で、43.0%が「知っている」または「利用したことがある」と回答した。前回調査での利用度合いはわずか1.7%であったのに対し、今回調査では若干利用率が増えた。しかしながら、いずれの分析手法についても半数以上が「知らない」と回答しており、今後、JRMSを含め、公開されているリスク分析手法が活用されることが望まれる(Q7)。

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、情報リスクの分析、情報セキュリティポリシー・規程類の策定、システム監査の実施等が重要視されるべきである。今回調査で最も多く策定／実施されているのは「情報セキュリティポリシーの策定」(68.5%≡H15:52.2%)、次いで「情報セキュリティ対策の実施手順、規程類の策定」(56.0%)、「情報リスクマネジメント方針の明確化」(45.7%≡H15:19.3%)、「情報セキュリティ監査の実施」(35.2%≡H15:19.3%)、「システム監査」(34.8%≡H15:30.1%)、「情報リスク分析の実施」(32.3%≡H15:22.3%)であった。いずれも前回調査よりも実施率は上がっている。一方で「策定／実施の予定がない」とする回答で最も多かったのは「システム監査の実施」(32.1%)、次いで「情報リスク分析の実施」(26.5%)、情報セキュリティ監査の実施(25.3%)であった(Q8)。

今回調査では、Q8のリスク分析を実施している事業体に対するリスク分析対象について調査を行った。8割以上が「地震」、「コンピュータ犯罪のリスク」、「事故」、「自社従業員などによる故意による情報漏えい」、「不注意・過失による情報漏えい」、「ハードウェア障害」、「ソフトウェア障害」、「ネットワーク障害」、「コンピュータウイルス、スパイウェアによるシステム停止」をリスク分析の対象とした。

リスク分析が経営に影響を与えたもので7割を超えたのは「地震」、「コンピュータ犯罪」、「事故」、「故意による情報漏えい」、「不注意・過失による情報漏えい」である(Q9)。

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かがきわめて重要と考えられる。リスク分析を実施した際の問題点として最も高い割合を示したのは「確立した手法がない」(62.7%≡H15:47.5%)、次いで「リスクの定量化が測れない」(51.2%≡H15:61.3%)、「専門家がない」(26.5%≡H15:38.7%)、「分析のためのデータが乏しい」(24.7%≡H15:30.9%)という結果となった(Q10)。

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30.0%で、前回調査の77.0%から大幅に減少した。(Q11)。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」(36.6%)が前回調査(41.2%)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13.8%(H15:25.2%、約11ポイント減)であった。また、「10億円以上」は6.5%(H15:10.7%)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)。

過去1年間における基幹システムのシステムダウンについて、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「全体的にダウンした」が8.0%と、前回(7.8%)とほとんど変化はない。一方、前回一旦減少した「部分的なダウン」は41.8%と若干増加した(H15:39.8%、H13:45.0%)。(Q13-①)。

なお、今回調査ではさらにシステムダウンの影響についても調査を行った。全体的にダウンした場合、「システム運用への悪影響をもたらす」は80.5%、「事業中断につながる」は26.8%となった。一方、部分的なダウンの場合は、それぞれ88.4%、13.5%と、ダウンの規模にかかわらず、システム運用に悪影響をおよぼすとの回答が大半であった。(Q13-②)

過去1年間の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「ネットワーク機器などの障害」(48.6%↖H15:38.5%↙H13:41.5%)、「サーバなどのハードウェア障害」(48.2%↙H15:53.1%↙H13:56.7%)、「アプリケーションソフトウェア障害」(41.7%↖H15:25.3%↙H13:33.0%)である。

ほとんどの原因が前回調査から増加傾向にあるが、その中で大幅に変化があったのは「オペミス等、人の過失による事故等」で、前回の17.7%から32.0%へと約14ポイント増加した。(Q14)。

基幹システムにおける平均故障間隔(MTBF)は4,273.4時間で、前回調査の2773.3時間からかなり故障間隔が長くなっており、システムの信頼性の向上がみられる。また、平均修理時間(MTTR)は130分で、前回調査の120分より若干長くなっている(Q15、Q16)。

コンピュータ犯罪意識に関する6つの質問では次のような結果が得られた。なお、前回調査までは選択肢として「問題であると思う」を設定していたが、今回調査からは外しているため、数値の増減に大きな差が生じている。

①『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56.0%(↙H15:59.8%↙H13:69.9%)となり、前回調査に比べ約3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16.2%から28.8%へと12.6ポイント増加した。

②『データ、プログラムを無断で使う』行為については、「企業内で戒告等の対象」が42.0%(H15:31.9%、10.1ポイント減)、「犯罪行為」が前回の26.6%から31.3%へと増加した。

③『データ、プログラムを覗き見る』行為に対しては、「企業内で戒告等の対象」が46.3%(H15:31.1%、15.2ポイント増)である。

④『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、「企業内で戒告等の処分の対象」が前回調査の44.0%から71.6%へと27.6ポイント、大幅に増加した。

⑤『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68.5%(H15:39.7%)、64.2%(H15:35.9%)の事業体が「企業内で戒告等の処分の対象」と判断している。

⑥『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50.2%(H15:41.0%)、「犯罪行為である」が19.3%(H15:23.1%)となった。

いずれの設問においても、「企業内で戒告等の処分の対象となる」が増加したのは、前述のとおり、今回調査で「問題があると思う」の選択肢がなかったことによるものと思われる。(Q17)

### 1.2.3 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 83.5% (H15:85.5%←H13:77.9%、2ポイント減)と最も高い割合を示している。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って非常に重要といえる。次いで多かったのは「経営者の理解」76.1% (H15:71.2%←H13:53.3%、4.9ポイント増)で、「管理者の理解」は47.1% (H15:39.7%、7.4ポイント増)であった。管理者よりも経営者の理解が重要であるという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。なお、前回調査の「法規制の整備」(14.4%)に替えて新設した「社内規定やルールの整備」は58.9%と、「経営者層の理解」の次に位置した。(Q18)

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7.7%と前回調査(6.1%)に比べ1.6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を把握できないケースが多いものと考えられる(Q19)。

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」が88.9%(H15:83.3%、5.6ポイント増)、情報システムの管理者については「定めている」が88.5%(H15:80.5%、8ポイント増)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80.4%と前回調査(65.5%)より約15ポイント増加した。なお、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1%未満であった(前回調査ではいずれも回答数は0件であった)。(Q20)。

システム災害/障害、不正アクセス、コンピュータ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、「コストがかかりすぎる」(62.6%←H15:53.6%、前回第2位)、「組織の従業員に対する教育・訓練がいきとどかない」(52.1%←H15:54.5%、前回第1位)、「専門要員がない」(44.0%←H15:43.0%)、「どこまでやればよいのか基準が定められていない」(42.0%←H15:38.2%)、「ノウハウ不足」(29.4%←H15:34.4%)が高い割合を示している。

なお、「組織の従業員に対する教育・訓練がいきとどかない」、「ノウハウ不足」、「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」は、過去2回の調査ごとに減少傾向にある。(Q21)。

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)」(30.5%←H15:32.9%←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)」(19.8%←H15:15.4%←H13:11.8%)である。次に「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)」(8.2%←H15:10.4%←H13:12.1%)、「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)」(8.0%←H15:7.1%←H13:7.1%)と続いている。

なお、前回3位であった「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)」(6.8%←H15:11.1%←H13:12.3%)は第5位となった。

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、第1位「人的セキュリ

ティ」(58.6%↖H15:52.7%↖H13:41.3%)、第2位「情報セキュリティポリシー」(45.5%↖H15:48.6%↖H13:49.6%)、第3位「通信および運用管理」(35.0%↖H15:43.2%↖H13:51.4%)、第4位「情報資産の分類および管理」(34.4%↖H15:32.7%)、第5位「アクセス制御」(30.8%↖H15:29.0%)の順となった。なお、前回4位だった「情報セキュリティ組織」は6位に順位を下げた(Q22)。

#### 1.2.4 災害対策・障害対策について

情報セキュリティポリシーや実施手続・規程類等に基づいた災害対策・障害対策が明確になっているかとの調査では、「ポリシー、規程類の中で明確になっている」との回答が約半数の48.1%(H15:27.4%、約20ポイント増)となった。「他の基準で扱っている」の21.8%とあわせ、約7割が対策を明確にしていることになる。なお、前回調査で44.1%であった「特に定めていない」は28.2%となり、約16ポイント減少した(Q23)。

『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」は48.8%と約半数となっているが、前回調査(64.8%)からは16ポイント減少した。なお、「作成している」は16.5%、「作成中である」(4.7%)をあわせても約2割にしかなっていない(Q24)。

Q24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109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96.3%(H15:95.1%)、次いで「障害」(85.3%↖H15:78.4%)である。なお、前回調査と比較し、全選択肢が増加傾向にあるが、その中で一番差があったのは、「外部からの悪意による緊急事態」(52.3%↖H15:43.1%、9.2ポイント増)であった(Q25)。

災害に対する情報システムのバックアップ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」(82.5%)が最も多く、次いで「対象システムを決めている」(58.8%)、「バックアップの頻度、バックアップ先を決定している」(56.0%)、「バックアップに関する規程や手順を決めている」(51.4%)が過半数を超えた。なお、「特に対策を講じていない」は5.6%であった(Q27)。

情報システムの障害対策のために設置している機能について調査した。最も高い回答率を示したのは今回調査から選択肢に追加した「RAID (Redundant Arrays of Inexpensive Disks) 1～5」(82.3%)で、他と比べ圧倒的な割合を占めている。次いで「コールドスタンバイシステム」(38.1%↖H15:21.5%)、「ホットスタンバイシステム」(37.4%↖H15:23.5%)、「クラスタリング」(36.8%↖H15:19.5%)となっている。一方、「特に設けていない」(6.8%)は、前回調査の17.4%から10.6ポイント減少した(Q28)。

地震対策に関しては、前回調査まではサーバ保管場所とデータ保管場所に分けて調査を行ってきたが、今回調査では特に設置場所を区別していない。最も多く行われている対策は「転倒防止措置」(65.0%)、次いで「建物が耐震構造」(44.4%)。「機器の移動防止措置」(34.6%)となった。「特に対策を講じていない」は14.8%となり、前回調査の「サーバ設置場所」22.3%、「データ保管場所」24.3%に対し、地震対策の未実施率は低くなっている。Q22で行った『重要と思われる情報セキュリティ要素』の調査では「物理的および環境的セキュリティ」の複数回答結果が16.5%(H15:12.1%)で10項目中第9位(前回は第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（Q28）。

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」（86.0%←H15:86.8%）が多く、次いで「自家発電装置」が45.9%（H15:36.9%）となった（Q29）。

事業体における情報セキュリティ教育の実態を調査した。定期的を実施している項目として最も多いのは「個人情報保護」（42.2%）で、次いで「コンピュータウイルス対策」（33.5%）、「情報セキュリティの一般知識」（33.1%）であった。定期的にはないにしろ、「時々実施している」場合、最も多いのは「コンピュータウイルス対策」（38.9%）で、次いで「情報セキュリティの一般知識」（33.9%）、「個人情報保護」（33.5%）である。この3項目について、「実施を予定している」をあわせると、「個人情報保護」が84.6%、「コンピュータウイルス対策」が79.2%、「情報セキュリティの一般知識」が79.8%と、8割前後の事業体が教育を実施（予定）しており、昨今多発している個人情報保護の漏えいやコンピュータウイルス被害を未然に防ぐため、従業員に対する教育の重要性をほとんどの事業体が認知していることとなる。なお「実施していない」で最も多かったのは「災害対策」（40.9%）、次いで「障害対策」（38.3%）となった。突発的に起こる災害・障害に対しては発生を予知することが難しいとはいえ、予防策を講じ、それを従業員に周知・徹底させるには、やはり定期的に教育・訓練を実施すべきであると思われる（Q30）。

情報セキュリティ人材の養成にあたっては、過半数の55.1%が「特に行っていない」と回答であったが、前回調査（76.5%）からは21.4ポイント減少した。一方、実施している場合の手段としては、回答率は低いながらも「民間資格の利用」が前回調査の4.8%から21.6%へ、約4倍となった（Q31）。

#### 1.2.5 不正アクセス対策・不正侵入対策・情報漏えい対策について

不正アクセス対策については、前回調査まで物理的／論理的不正アクセス対策の実施状況についてそれぞれ調査を行っていたが、今回は、管理面／技術面における不正アクセス対策について調査を行った。

管理面における不正アクセス対策として最も多く実施されているのは、「室の出入口での入・退室管理」（72.6%）、「個人情報・機密情報の担当者の限定（アクセス制限）」（70.0%）、「ネットワーク機器の運用者（アクセス範囲）の限定」（69.8%）である。

次に技術面における不正アクセス対策として多いのは、「ファイアウォールの利用」（87.7%）、「セキュリティパッチの適用」（74.7%）、「室への入退室についてカード、パスワードを使用」（60.7%）である（Q33）。

なお、Q32およびQ33と前回調査で共通の選択肢について結果を比較すると、すべて前回調査よりも増加しているが、特に増加ポイントが大きかったのは、「情報セキュリティ管理者やネットワーク管理者によるサーバやルータ、ファイアウォールのログの定期的なチェック」（論理的アクセス対策）で前回調査の20.5%から57.2%へと36.7ポイントの増加となった。次いで多かったのは「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」で前回調査（論理的アクセス対策）では36.4%であったが、今回調査では62.5%と、26.1ポイント増加した。

個人情報や機密情報に対する機密区分の設定に関しては、「機密区分を設定しているが暗号化はしていない」が40.9%であった。なお、「機密区分を設定しておらず、暗号化もしていない」

(33.3%で)については、前回調査(「暗号化していない」)で56.7%と過半数を超えていたのに対し、今回調査では20ポイント以上減少した(Q34)。

基幹システム、重要サーバ、シングルサインオン等の一般ユーザのパスワード変更設定のレベルについて最も多かったのは、「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28.0%(H15:27.9%)であった。全体的に大幅な変化はみられなかったが、「パスワードの変更に関して特に定めていない」(16.0%←H15:26.0%、10ポイント減)、「パスワードによる管理を実施していない」(2.9%←H15:6.6、3.7ポイント減)と、前回調査に比べパスワード管理が強化されてきていることがわかる(Q35)。

情報漏えい対策については今回提示した対策12項目中、半分の6項目が過半数を超えた。その中で8割以上の事業体が講じている対策が「アクセス制限」で、前回調査の53.1%から80.9%へ27.8ポイント増加した。次いで多かったのは「セキュリティポリシー、個人情報保護ポリシー、規程類の整備」で77.4%(H15:52.7%、24.7ポイント増)、「従業員に対する教育」68.3%(H15:45.6%、22.7ポイント増)となった。前回調査で1割強の事業体が「特に対策を行っていない」としていたが、今回調査では4.3%へと7.6ポイント減少した(Q36)。

#### 1.2.6 コンピュータウイルス対策について

過去1年間におけるコンピュータウイルス(以下、「ウイルス」という。)、スパイウェア、スパムメール、フィッシングの被害状況に関する調査では、44.2%がウイルス被害があったと回答している。またスパムメールについては24.5%が被害にあったとの回答であった。一方で「被害はない」との回答は45.3%となっている。前回調査で70.1%がウイルス感染したと回答していたことに比べ、25.9ポイント減少した(Q37)。

ここ数年来、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、Q37の被害のうち、ウイルスおよびスパイウェアの主な感染原因(経路)については、「電子メールの添付書類で」が最も多く64.3%(H15:47.6%、16.7ポイント増)、次いで「インターネット経由」が45.1%(H15:45.8%、0.7ポイント減)となった(Q38)。

ウイルス、スパイウェア、フィッシング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は「PCでのワクチンソフトの利用」で86.0%(H15:86.6%)、次いで「PCのワクチンソフト・パラメータファイルの定期的な更新」(79.6%←H15:75.0%)、そして、今回新たに追加した「従業員の教育」(74.5%)の順となった。

なお、前回調査と比較して全体的には順位の変動があまりみられなかったが、この中で大幅な変動があったのは「記録媒体利用時のチェックの実施」で、前回の7位(45.6%)から15位(28.2%、17.4ポイント減)に下降した。逆に「出所確認」は前回の17位(15.7%)から12位(32.1%、16.4ポイント増)に、「パスワードの変更等、アクセスコントロールの強化」は18位(15.2%)から13位(30.9%、15.7ポイント増)に上昇した(Q39)。

#### 1.2.7 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。過去2年以内のシステム監査の実施状況について、「実施している」は40.7%となり、前回調査の35.9%から若干増加した。「これから実施する予定がある」(17.1%)をあわせると、前回調査よりも11ポイント増加し

たことになる（Q40）。

Q40 でシステム監査を実施している事業体 209 件に対し、どのような効果があったかを調査した。最も多かったのは「要員が規定・ルール等を意識して業務を実行するようになった」で 50.2%、次いで「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」が 47.4%であった。前回調査ではこの 2 項目が同率の 1 位（38.7%）であった（Q41）。

Q40 でシステム監査を実施しない事業体（204 件）の未実施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」（41.7%）で、全体の約 4 割を占めた（Q42）。

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 35.2%で、前回調査（18.2%）から倍増し、「実施しない」は 36.0%（H15:59.3%、23.3 ポイント減）となった。Q40 のシステム監査の実施状況と比較すると、「予定」を含んだ場合では情報セキュリティ監査（63.0%）の方がシステム監査（57.8%）を上回った。なお、実施した情報セキュリティ監査は助言型監査が 85.9%、保証型監査が 59.6%であった（Q43）。

Q43 で情報セキュリティ監査を実施しない 185 事業体の未実施の理由としては、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 44.9%と最も多い（Q44）。

#### 1.2.8 個人情報保護について

平成 15 年に公布、平成 17 年 4 月から完全施行されている『個人情報保護法』（以下、『保護法』という。）の認知度については、「内容を知っている」（87.9%）および「公表されたことを知っている」（10.5%）の回答率から、ほとんどがその存在を認知していることがわかる。一方、16 年 10 月に策定された経済産業省の『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』（以下、『METI ガイドライン』という。）についても、約 9 割が認知している（Q45）。

『保護法』で定められている個人情報取扱事業者に該当するかの調査については、今回の回答事業者の 66.1%がそれに該当する（Q46）。

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 82.9%（H15:82.5%）、次いで「顧客サポート」（48.4%↖H15:40.5%）、「売買等契約の履行」（40.7%↖H15:32.2%）、「委託（受託）処理」（33.3%↖H15:18.2%、15.1 ポイント増）となった（Q47）。

個人情報の収集方法としては直接収集と間接収集があるが、「情報主体からの直接収集」（73.0%）、「従業者から直接収集」（72.6%）、「営業活動による情報主体からの直接収集」（54.3%）と、直接収集が上位を占めている（Q48）。

Q48 で直接収集する場合の情報主体からの収集・利用目的の同意確認の有無については、「すべて同意を取っている」が 63.1%、「重要な変更の場合のみ、個別に同意を取る」が 20.6%と、8 割以上がきちんと対応している（Q49）。

また、グループ企業や業務委託による預託などによる間接収集の場合、「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に確認する」が 68.0%、「情報主体から利用に関し、改めて同意を取る」が 20.0%と、9 割弱の事業者が対応しているという結果となった（Q50）。

個人情報の漏えいとその事業体にもたらす影響は大きく、業務停止や損害賠償問題、さらには事業体の存続にまで影響を及ぼしかねない。最も深刻な被害を及ぼすと考えられているのは「社会的な信用の低下」(89.5%)、次いで「情報が漏えいした情報主体からの損害賠償請求」(69.8%)、「親会社や関連会社側、企業グループの社会的信用低下」(45.1%)、「顧客や取引先、官公庁からの取引での指名停止」(43.6%)となっている(Q51)。

個人情報保護対策の実施状況を調査した。『保護法』施行以前から実施している対策としては「管理責任者の設置」が最も多く36.4%、次いで「個人情報保護に関する規程を定め運用する」(35.8%)、となっている。

なお、保護法施行前後を含め、現在行っている対策について前回調査と比較すると、最も多いのは「個人情報保護に関する規程を定め運用する」で83.1%(H15:34.7%、48.4ポイント増)、「管理責任者の設置」(81.9%↖H15:36.0%、45.9ポイント増)、「苦情相談窓口を設置し、個人からの問題意識を吸い上げ、対応する」(65.4%↖H15:24.3%、41.1ポイント増)となっている。

一方、今後予定している対策としては、「リスク分析を実施して必要な安全対策を構築する」(30.2%↖H15:22.3%、7.9ポイント増)、「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る」(25.1%↖H15:17.9%、7.2ポイント増)である。一方、現在も今後もあり実施されない対策としては「個人情報漏えい保険に加入する」で、「実施の予定がない」が約7割を占めた。(Q52)。

個人情報の管理状況に対するリスクの認識度について、「対策を講じているが、リスクはあると認識している」が他を圧倒的に引き離し、73.3%であった。なお、対策実施の有無にかかわらず、88.8%が「リスクがある」と認識している(前回調査でリスクがあると認識していたのは47.9%)。(Q53)。

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80.5%、(H15:56.0%、24.5ポイント増)、次いで「個人情報の適切な管理」(66.9%↖H15:39.8%、27.1ポイント増)、「目的外使用・再委託禁止」(65.0%↖H15:41.8%、23.2ポイント増)となった(Q54)。

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』を運用しているが、このプライバシーマークの認定状況について調査を行った。回答事業体の約4分の1が取得済み(または取組中)となっている。(Q55)。

Q55でプライバシーマーク取得(または取組中)の134事業体に対するプライバシーマークの取得目的を調査した。最も多いのは「社内の管理体制が構築でき、信頼性を確保できる」で96.3%であった。Q51で情報漏えいをもたらす被害として「社会的な信用低下」があげられていたが、社内体制を強化し、信頼性を確保することが信用低下を防ぐ一助となると思われる。

(参考)

過去1年間において発生した10万件以上の大規模な個人情報漏えい・流出・紛失事件は以下のとおり。

| 事業体名                    | 漏えい・紛失情報               | 媒体・原因等             | 件数(推測)                  |
|-------------------------|------------------------|--------------------|-------------------------|
| みちのく銀行                  | 顧客情報                   | CDデータ紛失            | 131万件                   |
| 大阪市                     | 花博記念公園の寄付者情報           | データ入りパソコン盗難        | 30万7,000件               |
| 福井銀行                    | 顧客情報                   | マイクロフィルム、記録文書紛失    | 17万件                    |
| UFJ信託銀行                 | 顧客情報                   | マイクロフィルム紛失         | 11万6,000件               |
| りそなグループ(4行)             | 顧客情報                   | マイクロフィルム紛失         | 30万件                    |
| 静岡銀行                    | 顧客情報                   | マイクロフィルム、記録文書廃棄・紛失 | 12万2,347件廃棄<br>4,470件紛失 |
| 大阪信用金庫                  | 顧客情報                   | CD-ROM紛失           | 57万件紛失                  |
| 中国銀行                    | 顧客情報                   | (店舗統廃合等に伴う)誤廃棄     | 10万6,000件               |
| トマト銀行                   | 顧客情報                   | 誤廃棄                | 11万1,780件               |
| 琉球銀行                    | 顧客情報                   | マイクロフィルム、文書誤廃棄     | 10万件                    |
| 東京国税局                   | 納税者情報                  | ノート型PC盗難           | 47万件                    |
| NTTドコモ中国<br>(ドコモサービス中国) | 取引先・契約者情報              | 外付けハードディスク紛失       | 13万4,782件               |
| JR西日本                   | 会員制旅行サービス「ジパング倶楽部」会員情報 | 不明<br>仏具電話セールスに利用  | 12万6,680件<br>(43万件か)    |

(平成18年3月16日作成)

なお、このほか、件数は少ないが、ファイル交換ソフト「Winny (ウィニー)」を介しての情報漏えい事件が頻発している。ほとんどが事業体の従業員が社内情報を外部に持ち出し、私用パソコンでWinnyを使用した結果、暴露ウイルスに感染し、ネットワーク上に事業体の保有する各種情報が流出した、というケースである。中でも政府機関による情報漏えいの多発を受け、政府は2006年3月中に省庁ごとに情報管理の基準を策定させる方針を決めた。

#### Winny ウイルス感染被害による漏えい (一例)

| 事業体名              | 漏えい・紛失情報              | 件数<br>(推測) | 再発防止策                                                                              |
|-------------------|-----------------------|------------|------------------------------------------------------------------------------------|
| 北海道庁              | 道職員／退職者／法人情報          | 3,544件     | ・文書によるセキュリティ対策の徹底通知<br>・情報セキュリティに係るガイドライン、指針の策定、道職員向けハンドブックの作成により、情報セキュリティ対策の徹底を図る |
| 近畿コンピュータサービス      | 養父市営CATV加入者情報         | 6,770件     |                                                                                    |
| 富士通               | コールセンターへの問い合わせ者情報     | 1,950件     | 顧客情報の持出禁止を強化                                                                       |
| 北海道電力・関西電力・九州電力 他 | 原子力・火力・水力発電所関係資料／社員情報 | 1,300件     | ・企業機密管理宣言<br>・管理体制の強化                                                              |
| NTT 東日本           | 顧客情報・社員情報             | 1,600件     | ・業務関連情報を自宅等社外持出禁止<br>・自宅PCでのWinny使用禁止<br>・個人情報の取扱いに関する全社員への周知・教育の徹底<br>・情報管理体制の強化  |

| 事業体名                       | 漏えい・紛失情報                                  | 件数<br>(推測)         | 再発防止策                                                                        |
|----------------------------|-------------------------------------------|--------------------|------------------------------------------------------------------------------|
| 防衛庁                        | 陸上・海上・航空自衛隊の内部資料(「秘」情報を含む)                | FD290 枚<br>分のデータ 他 | ・ファイル交換ソフトの削除<br>・私物 PC での秘密情報の取扱全面禁止                                        |
| 岡山県警                       | 捜査情報(被害者情報を含む)                            | 1,600 件            | 私物パソコンを含みウィニーの使用禁止                                                           |
| NTT 東西                     | 顧客情報および NTT グループ社員情報                      | 2,000 件            | ・私用 PC の持込み禁止、<br>・従業員への周知徹底<br>・情報管理の強化                                     |
| 法務省                        | 刑務所受刑者情報を含む内部情報                           | 10,000 件<br>以上     |                                                                              |
| 富士宮信用金庫<br>日本電気<br>NEC ソフト | 顧客の手形決済情報                                 | 13,619 件           | 委託先企業の管理徹底                                                                   |
| 住友生命保険                     | 米国子会社の取引先企業情報／現地役職員情報                     | 8,000 件            | ・情報の社外持出し禁止の再徹底<br>・個人所有 PC の安全管理の注意喚起                                       |
| 読売理工学院                     | 卒業生情報                                     | 1,036 件            | ・個人情報の学外持出し禁止<br>・ウイルス感染しやすいソフトの使用禁止                                         |
| 京橋通郵便局                     | 顧客リスト                                     | 2,838 件            | 顧客情報の管理徹底を指導                                                                 |
| アイティービー                    | ケーブルテレビ加入者および工事情報                         | (最大)<br>1,378 件    | ・私用 PC の業務用データ取扱禁止<br>・社内ルールの再徹底を指導                                          |
| 富山 長谷川病院                   | 手術室利用履歴情報                                 | 2,873 件            | ・外部ネットワーク遮断<br>・患者情報持ち出し登録許可制<br>・私用 PC 持込禁止                                 |
| 愛媛県警                       | 捜査資料<br>「Nシステム」(自動車ナンバー自動読取りシステム)で収集したデータ | 延 10 万台の車の<br>ナンバー | 全職員に対し、以下の誓約書を出させる<br>①公務 PC や FD 等を許可なく外部に持ち出さない<br>②公私に限らず、ファイル交換ソフトを使用しない |

(平成 18 年 3 月 16 日作成)

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。

| 施 策                             | 利用している |      | 知っている |      | 知らない |      | 無回答 |     | 計   |       |
|---------------------------------|--------|------|-------|------|------|------|-----|-----|-----|-------|
| ①情報システム安全対策基準<br>(平成7年8月改訂)     | 102    | 19.8 | 296   | 57.6 | 104  | 20.2 | 12  | 2.3 | 514 | 100.0 |
| ②コンピュータウイルス対策基準<br>(平成7年7月改訂)   | 107    | 20.8 | 305   | 59.3 | 90   | 17.5 | 12  | 2.3 | 514 | 100.0 |
| ③コンピュータ不正アクセス対策基準<br>(平成8年8月制定) | 99     | 19.3 | 311   | 60.5 | 92   | 17.9 | 12  | 2.3 | 514 | 100.0 |
| ④システム監査基準<br>(平成16年10月改訂)       | 64     | 12.5 | 316   | 61.5 | 118  | 23.0 | 16  | 3.1 | 514 | 100.0 |
| ⑤システム管理基準<br>(平成16年10月策定)       | 52     | 10.1 | 298   | 58.0 | 149  | 29.0 | 15  | 2.9 | 514 | 100.0 |
| ⑥システム監査企業台帳制度<br>(平成3年3月制定)     | 16     | 3.1  | 266   | 51.8 | 216  | 42.0 | 16  | 3.1 | 514 | 100.0 |
| ⑦情報セキュリティ監査制度<br>(平成15年3月運用開始)  | 49     | 9.5  | 314   | 61.1 | 138  | 26.8 | 13  | 2.5 | 514 | 100.0 |
| ⑧情報セキュリティ監査企業台帳制度<br>(成15年3月制定) | 40     | 7.8  | 246   | 47.9 | 213  | 41.4 | 15  | 2.9 | 514 | 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」を選択

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」事業体の割合は相対的に高く、両者をあわせればいずれも7割前後が認知している。しかしながら、「すでに利用している」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15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「情報セキュリティ監査制度」（70.6％）で、前回調査（58.5％）に比べ12.1ポイント増加した。前回調査時点では同制度の運用が開始されてからまだ半年も経っていなかったにも関わらず、すでに6割近い認知度であったが、わずか運用開始2年で他の基準に近い認知度となった。

業種グループ別にみると、「政府・地方公共団体」の認知度が92.2％と最も高く、次いで「情報処理サービス業」（85.2％）となっている。

また、同制度の一環として運用されている「情報セキュリティ監査企業台帳制度」の認知度も前回調査の44.3％から11.4ポイント増加し、55.7％となった。これはすでに制度が開始されて10年以上が経過している「システム監査企業台帳制度」よりも1.6ポイント高い結果となった。

システム監査基準が平成16年10月に約8年ぶりに改訂され、「システム監査基準」と「システム管理基準」の二本立てとなった。改訂版「システム監査基準」の認知度は74.0％、前回調査の73.0％とほとんど変わりなかった。また、新設された「システム管理基準」は68.1％と、他の基準との差もさほどみられない。

システム監査企業台帳については、前回調査の46.8％から54.9％と、認知度は8.1ポイント増加したが、「利用している」割合がわずか3.1％と、利用率の低さが他の基準に比べ目立っている。

その他の基準については、前回調査からの増減はほとんどみられなかった。

「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75.7％に対し、今回調査では

77.4%と1.7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77.0%から80.1%へ3.1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76.7%から79.8%と3.1ポイントの増加となった。

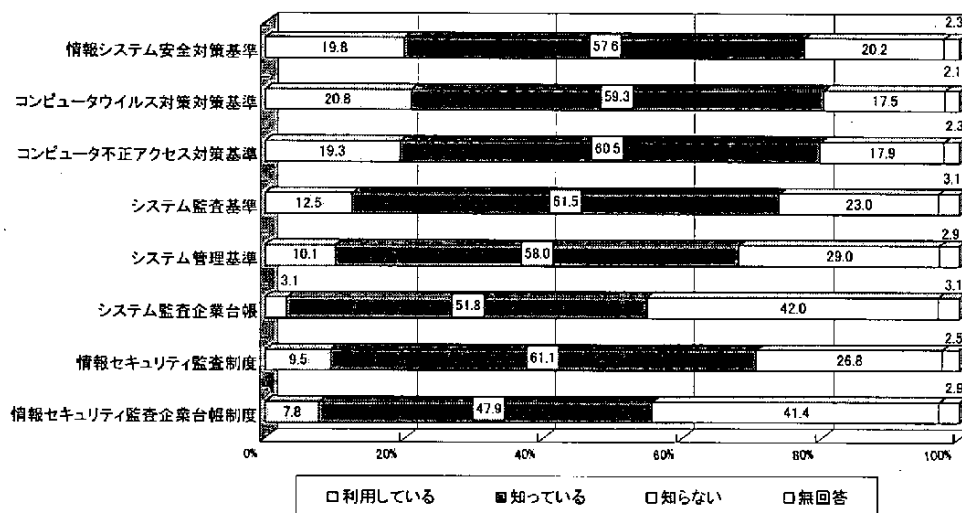


図2-1-1. 経済産業省策定の安全対策関連施策の認知度

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/daicho/gaiyo.htm>

Q2. 以下のJIS規格等を知っていますか。

| 規格名                                                   | 利用している |      | 知っている |      | 知らない |      | 無回答 |     | 計   |       |
|-------------------------------------------------------|--------|------|-------|------|------|------|-----|-----|-----|-------|
| ①JIS 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)   | 96     | 18.7 | 212   | 41.2 | 194  | 37.7 | 12  | 2.3 | 514 | 100.0 |
| ②JIS 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)          | 33     | 6.4  | 232   | 45.1 | 236  | 45.9 | 13  | 2.5 | 514 | 100.0 |
| ③JIS 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) | 128    | 24.9 | 218   | 42.4 | 156  | 30.4 | 12  | 2.3 | 514 | 100.0 |
| ④事業継続計画(BCP)策定ガイドライン(平成17年3月策定)                       | 22     | 4.3  | 208   | 40.5 | 270  | 52.5 | 14  | 2.7 | 514 | 100.0 |
| ⑤事業継続ガイドライン第1版(平成17年8月策定)                             | 19     | 3.7  | 197   | 38.3 | 283  | 55.1 | 15  | 2.9 | 514 | 100.0 |
| ⑥ISMS認証基準(Ver.2.0)                                    | 113    | 22.0 | 267   | 51.9 | 122  | 23.7 | 12  | 2.3 | 514 | 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」のは18.7%と、前回調査の10.1%から約8ポイント増加した。また、「知っている」の41.2%をあわせた認知度は59.9%と、前回調査から15.4ポイント増加した。

業種グループ別にみると、「情報処理サービス業」（81.5%）、「政府・地方公共団体」（75.0%）の認知度が前回同様高い。しかし、前回調査では他の業種での認知度が2～4割程度と低かったが、今回調査ではいずれも5～7割程度にまで増加してきている。

なお、後述Q22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きている。

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。同規格を「利用している」割合は6.4%と低い。この低さの原因は、同規格が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ことも一因と思われる。しかし、「知っている」（45.1%）をあわせた認知度は前回調査（35.5%）から51.5%へと、16ポイントの増加となった。

業種グループ別にみると、「情報処理サービス業」（77.8%へH15：70.3%）、「その他対事業所サービス」（54.0%へH15：38.8%）については前回調査に比べると比較的大幅な増加がみられた。

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、前回調査の8.6%から24.9%へと16.3ポイント増加した。「知っている」の42.4%をあわせた認知度67.3%は、前回調査（46.1%）から21.2ポイントの増加となった。

業種グループ別にみると、業務で直接／間接的に個人情報を取り扱う機会が多い「情報処理サービス業」（92.6%へH15：85.2%）、「その他対事業所サービス」（72.4%へH15：53.4%）、「政府・地方公共団体」（68.8%へH15：46.3%）、「金融・保険業」（67.2%へH15：48.7%）の認知度がいずれも過半数を超えている。その他の業種についても、数値は低いが4割以上の認知度である。

なお、JIS規格は工業標準化法に基づき、策定後5年に1回の見直しが必要とされているが、「JIS Q 15001」については平成18年1月にMETIが改訂（案）を提示し、パブリックコメント募集を行っており、近い将来、改訂が予定されている。

METI は平成 17 年 3 月に、商務情報政策局長の私的研究会である「企業における情報セキュリティガバナンスのあり方に関する研究会」の研究成果をとりまとめ、「企業における情報セキュリティガバナンスのあり方に関する研究会」報告書を公表した。そして、セキュリティガバナンスの実現手段ツールとして「情報セキュリティ対策ベンチマーク」、「情報セキュリティ報告書モデル」、「事業継続計画策定ガイドライン」を策定し、それらの普及方策について提言を行った。これら実現手段ツールのうち、今回調査では、IT 事故を想定した事業継続計画（BCP）策定ガイドラインの認知度について調査を行った。策定から約半年が経過していた時点での調査であったが、同ガイドラインを「利用している」のは 4.3%、「知っている」（40.5%）をあわせると 44.8%の認知度となった。

平成 17 年 8 月に内閣府中央防災会議「民間と市場の力を活かした防災力向上に関する専門調査会」がとりまとめた「事業継続ガイドライン（第 1 版）」の認知度は、BCP 策定ガイドライン同様の結果となり、「利用している」（3.7%）と「知っている」（38.3%）をあわせると 42.0%の認知度となった。ガイドラインの策定から実態調査までが約 2 か月しかなかったことも結果に影響しているものと思われる。

なお、中小企業庁では、中小企業の BCP 普及促進を目的として、平成 18 年 2 月に「中小企業 BCP 策定運用指針」を策定しているので、そちらも参照されたい。

情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証審査の基準とされている ISMS 認証基準（平成 15 年策定）の認知度は、「利用している」22.0%、「知っている」51.9%と、7 割強の割合を占めている。

なお、ISMS 認証基準の国際規格が ISO/IEC 27001:2005 として平成 17 年 10 月に発行され、今後 JIS Q 27001 として発行されることとなったため、これにあわせて ISMS 認証基準(Ver. 2.0)も JIS Q 27001(ISO/IEC 27001)に移行することとなった。

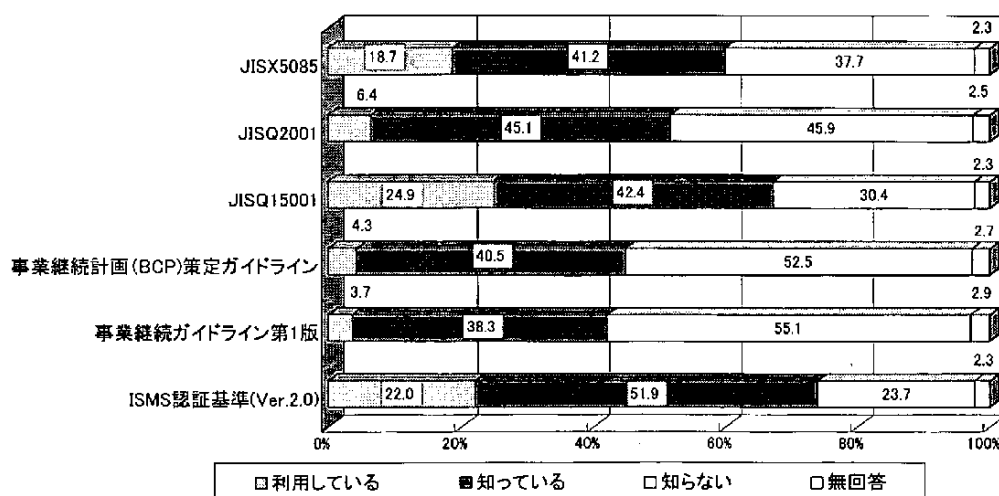


図2-1-2. JIS規格等の認知度

ところで、「Q1」、「Q2」とも設問が「〇〇を知っていますか」という形になっているが、この「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。

(参考)

○事業継続計画策定ガイドライン（経済産業省）

<http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf>

○事業継続ガイドライン（内閣府）

<http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf>

○中小企業 BCP 策定運用指針

<http://www.chusho.meti.go.jp/bcp/>

○ISMS 認証基準の移行について

<http://www.isms.jipdec.jp/ISO27001.html>

## 2.2 情報リスクマネジメントについて

Q3. 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 | 210 | 40.9  |
| 2   | 重要と考えている     | 255 | 49.6  |
| 3   | さらに強化する予定がある | 30  | 5.8   |
| 4   | 考えていない       | 7   | 1.4   |
| 5   | わからない        | 7   | 1.4   |
| 無回答 |              | 5   | 1.0   |
| 計   |              | 514 | 100.0 |

現代の情報システム環境の変化はこれまでになく著しいといえる。システム関連のハード・ソフト面での著しい進展、さらにインターネットの利用の高度化等はたしかに事業展開に便利さをもたらしたが、リスクに対する脆弱性を露呈させてきた。この点は、平成17年度に生じた金融機関でのシステム障害、さらに証券取引所のシステムの一時機能停止等における状況からうかがい知ることができる。こうした事態に備え、METIから情報システムに関する各種の安全対策関連基準が策定され、各種対策が講じられてきているものの、システム利用の頻度と影響の大きさからすれば、かなり「イタチゴッコ」的な側面がみられ、想定範囲を超えていたという見方もやむをえないかもしれない。それだけに、情報システム環境変化を先取りするリスク対応が求められ、情報リスクマネジメントの実践は喫緊の課題である。

この点に関して前回調査において新たに情報リスクマネジメントに関する質問を設けた。今回調査においては情報リスクマネジメントを「重要と考え、実践している」が40.9%、「重要と考えている」が49.6%であった。前回調査ではそれぞれが26.3%、63.8%であったが、情報リスクマネジメントの「実践」において大幅な増加が確認できた。これは、情報システムリスクに対応する必要性を実感してのことであると思われる。

また、「さらに強化する予定」(5.8%)をあわせると、約47%が情報リスクマネジメントを現実に行っており、さらに「重要と考えている」をあわせると、96.3%が情報リスクに対する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。

しかし再度強調しておきたい点は、「重要と考えている」と、実際に「実践している」とでは現実の情報リスクマネジメントからいえば非常に大きな差異があることである。事業体を脅かす事態が発生した場合、問題が具体化してからの対応コスト（直接的な対応コストの他に、信頼性の欠如という間接的なコスト、さらに重視すべき時間的コスト等）は事前的な対応コストの比ではないという点である。システム機能停止等の場合、その影響の範囲によるが、情報リスク対応を「重要と考えている」だけでは問題の解決にはならないのである。

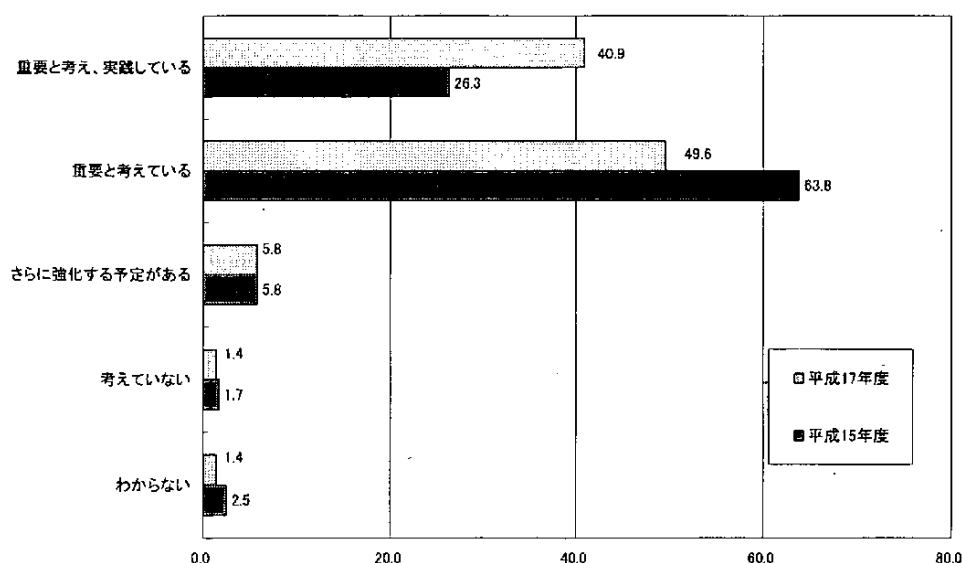


図2-2-1. 情報リスクマネジメントに対する考え方

| 情報リスクマネジメントに対する考え方 | 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 |
|--------------------|----------|----------|---------|--------|-------|
| 業種グループ             |          |          |         |        |       |
| 食品・紙・パルプ・繊維・印刷     | 29.6     | 48.1     | 14.8    | 3.7    | 3.7   |
| 石油・化学・鉄鋼・非鉄・金属     | 22.2     | 66.7     | 5.6     | 2.8    | 0.0   |
| 電気・一般・輸送用機械        | 41.7     | 45.0     | 10.0    | 1.7    | 0.0   |
| その他製造業             | 12.9     | 58.1     | 9.7     | 6.5    | 6.5   |
| 商業                 | 21.6     | 75.7     | 0.0     | 0.0    | 2.7   |
| 金融・保険業             | 56.3     | 35.9     | 6.3     | 0.0    | 0.0   |
| 情報処理サービス業          | 71.6     | 22.2     | 4.9     | 1.2    | 0.0   |
| その他対事業所サービス        | 36.8     | 56.6     | 3.9     | 1.3    | 1.3   |
| 公共サービス             | 28.9     | 63.2     | 5.3     | 0.0    | 2.6   |
| 政府・地方公共団体          | 37.5     | 57.8     | 3.1     | 0.0    | 1.6   |

ところで、情報リスクマネジメントについては現状において各業種とも情報システムへの依存度を増しているとはいえ、業種による差異も考察対象としておきたい。そこで上記の点を業種グループ別にみると業種による差異がかなり顕著となっている。「情報処理サービス業」においては、「重要と考え実践している」と「さらに強化を考えている」を合計した割合が76.5%と高い。この点は、前回調査（54.1%＝51.4%+2.7%）と比較すると22ポイントほど高くなっている。

なお、近年の金融業界における状況を想定すれば、情報システムの完全統合のため、時期を先送りしたケースもある他、保険業においても情報端末への依存度が高まっている現状から、実践の度合いがかなり高いと想定できたが、「金融・保険業」は結果として62.6%となっている。前回調査（59.5%＝56.8%+2.7%）と比較すると3ポイントほどの増加にすぎない。「製造業」全

般においても情報システムは不可欠であると思われ、「重要と考えている」割合が高いものの、「実践している」という回答は相対的に低い。製造業という範疇においても、組織の受け止め方に差異があるが、情報リスクマネジメント実践への取組みを検討すべきといえる。

| 情報リスクマネジメントに<br>対する考え方 | 重要と<br>考え実践 | 重要と<br>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 |
|------------------------|-------------|--------------|-----------|--------|-------|
| 資本金規模                  |             |              |           |        |       |
| 500 億円以上               | 72.7        | 22.7         | 4.5       | 0.0    | 0.0   |
| 100 億円以上 500 億円未満      | 58.5        | 33.0         | 6.4       | 0.0    | 0.0   |
| 50 億円以上 100 億円未満       | 31.4        | 68.6         | 0.0       | 0.0    | 0.0   |
| 10 億円以上 50 億円未満        | 32.6        | 59.8         | 5.4       | 0.0    | 0.0   |
| 1 億円以上 10 億円未満         | 33.0        | 50.0         | 10.6      | 4.3    | 1.1   |
| 5 千万円以上 1 億円未満         | 28.1        | 50.0         | 9.4       | 6.3    | 6.3   |
| 5 千万円未満(資本金なしを含む)      | 34.1        | 58.5         | 3.3       | 0.8    | 3.3   |

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大規模な組織（特に 500 億円以上）ほど「実践している」と回答し、情報リスク対応の実態を反映した傾向がみられるものの、「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。前回調査に比較すると「重要と考え実践している」割合が「50 億円未満」の規模で高まっている。

Q4. 経営者層は次の事項について関心が高いですか。

| 関心事項                   | 高い  |      | 中位  |      | 低い  |      |
|------------------------|-----|------|-----|------|-----|------|
| ①情報システム関連の事件・事故に対するリスク | 325 | 63.2 | 119 | 23.2 | 46  | 8.9  |
| ②個人情報などの情報漏えいに対するリスク   | 356 | 69.3 | 102 | 19.8 | 39  | 7.6  |
| ③情報セキュリティガバナンス(注1)     | 100 | 19.5 | 173 | 33.7 | 78  | 15.2 |
| ④情報セキュリティ対策ベンチマーク(注2)  | 44  | 8.6  | 153 | 29.8 | 121 | 23.5 |

| 関心事項                   | わからない |      | 無回答 |     | 計   |       |
|------------------------|-------|------|-----|-----|-----|-------|
| ①情報システム関連の事件・事故に対するリスク | 20    | 3.9  | 4   | 0.8 | 514 | 100.0 |
| ②個人情報などの情報漏えいに対するリスク   | 13    | 2.5  | 4   | 0.8 | 514 | 100.0 |
| ③情報セキュリティガバナンス(注1)     | 158   | 30.7 | 5   | 1.0 | 514 | 100.0 |
| ④情報セキュリティ対策ベンチマーク(注2)  | 190   | 37.0 | 6   | 1.2 | 514 | 100.0 |

注1) 情報セキュリティガバナンスは、経済産業省が進めている情報セキュリティ対策の新しい枠組みで、企業の株主などの利害関係者に対して情報セキュリティに関する報告書を発行するなどが盛り込まれている。

注2) 情報セキュリティ対策ベンチマークは、経済産業省が進めている情報セキュリティの対策の総合評価方法で、数値化された結果が得られる

経営者にとって関心が高いと思われる「①情報システム関連の事件・事故に対するリスク」、「②個人情報などの情報漏えいに対するリスク」、「③情報セキュリティガバナンス」、「④情報セキュリティ対策ベンチマーク」に対する意識調査を行った。これらに対する経営者層の関心度合いにはかなりの差がみられた。

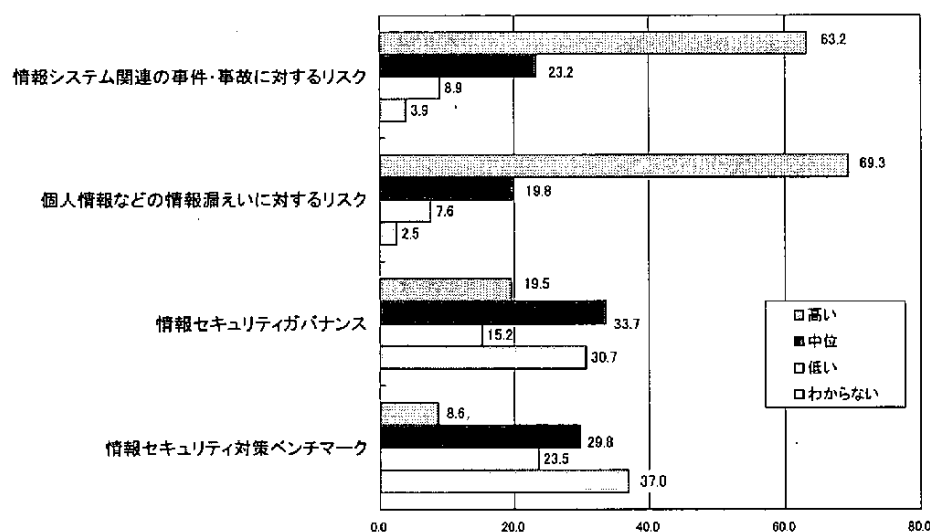


図2-2-2. 経営者の情報システム関連の事故・事件に対する関心度合い

「①情報システム関連の事件・事故に対するリスク」については前回調査、平成13年度調査では「コンピュータ関連の事件・事故に対するリスク」という表現で質問を設定した。厳密には同じとは言いがたいが、今回調査では関心が「高い」という回答が63.2%と、かなり高い割合となり、前回調査の37.0%に比べ26ポイント増加した。ちなみに、13年度調査（26.0%）から比べて関心度合いの高まりは著しいといえる。この点からコンピュータのみならずネットワーク等を含めた情報システム関連の事故・事件に対するリスクについて経営者の関心にかんがりの変化が生じてきたことが確認できる。その反面、「中位」について今回は23.2%となり、前回の39.8%と13年度の35.2%に比較し、低い割合となっている。同様に「低い」という回答が8.9%と前回の15.2%、13年度調査の22.4%に比べ著しく減少してきている。これらの結果は、情報システム環境における情報システムリスクに関する経営者層の意識の高まりを示しているといえる。

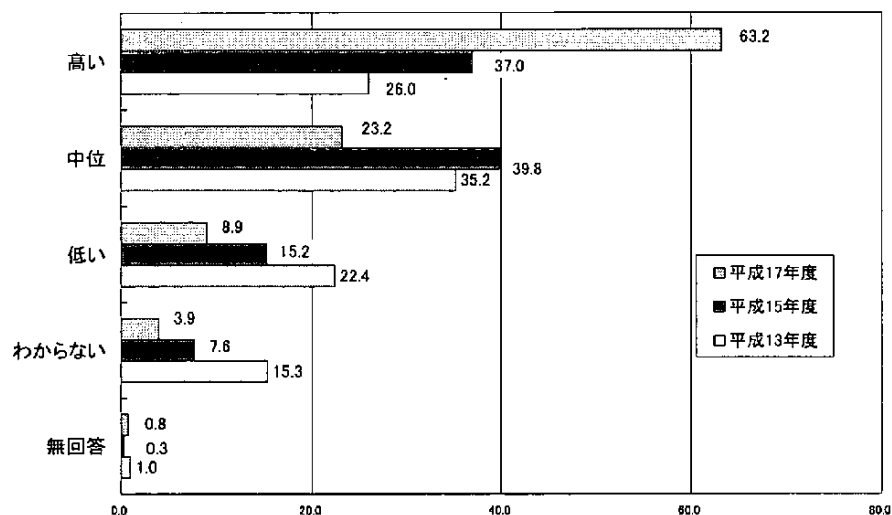


図2-2-3. 経営者の情報システム関連の事故・事件に対する関心度合い

| 業種グループ \ 情報システム関連の事件・事故関連<br>リスクに対する意識 | 高い   | 中位   | 低い   | わからない | 無回答 |
|----------------------------------------|------|------|------|-------|-----|
| 食品・紙・パルプ・繊維・印刷                         | 48.1 | 33.3 | 11.1 | 7.4   | 0.0 |
| 石油・化学・鉄鋼・非鉄・金属                         | 30.6 | 41.7 | 16.7 | 11.1  | 0.0 |
| 電気・一般・輸送用機械                            | 56.7 | 30.0 | 11.7 | 0.0   | 1.7 |
| その他製造業                                 | 41.9 | 29.0 | 22.6 | 3.2   | 3.2 |
| 商業                                     | 48.6 | 27.0 | 18.9 | 5.4   | 0.0 |
| 金融・保険業                                 | 81.3 | 15.6 | 1.6  | 0.0   | 1.6 |
| 情報処理サービス業                              | 91.4 | 8.6  | 0.0  | 0.0   | 0.0 |
| その他対事業所サービス                            | 63.2 | 22.4 | 9.2  | 5.3   | 0.0 |
| 公共サービス                                 | 44.7 | 23.7 | 18.4 | 13.2  | 0.0 |
| 政府・地方公共団体                              | 70.3 | 23.4 | 1.6  | 3.1   | 1.6 |
| 計                                      | 63.2 | 23.2 | 8.9  | 3.9   | 0.8 |

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（70%以上）は「情報処理サービス業」（91.4%）、「金融・保険業」（81.3%）、「政府・地方公共団体」（70.3%）の3業種であった。ただし全業種で増加傾向が確認できる。特に前回調査に比べ関心の度合いが高まっているのは「その他対事業所サービス」（63.2%⇨H15：27.2%、36.0ポイント増）、「政府・地方公共団体」（70.3%⇨H15：38.9%、31.4ポイント増）、「商業」（48.6%⇨18.6%、30ポイント増）、「公共サービス」（44.7%⇨15.2%、29.5ポイント増）、「食品・紙・パルプ・繊維・印刷」（48.1%⇨20.7%、27.4ポイント増）である。これらは現在の経営環境を考慮に入れ、情報リスクを判断した上での関心度合いといえるのであろう。

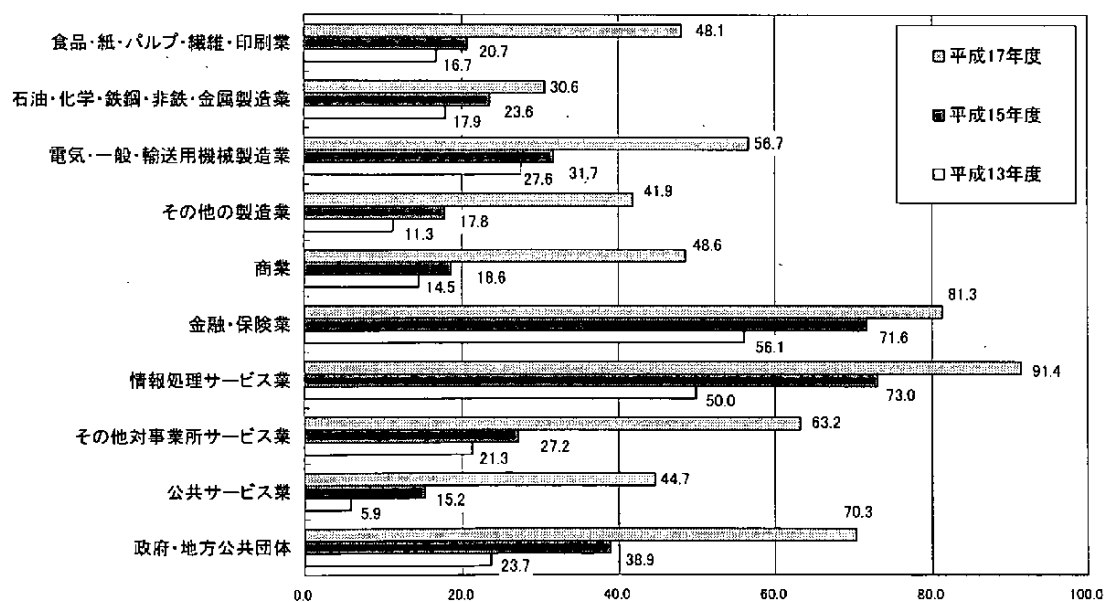


図2-2-4. 経営者の情報システム関連の事件・事故に対するリスクへの関心度合い（選択肢「高い」のみ）（業種グループ別）

| 情報システム関連の事件・事故<br>関連リスクに対する意識 | 高い   | 中位   | 低い   | わから<br>ない | 無回答 |
|-------------------------------|------|------|------|-----------|-----|
| 資本金規模                         |      |      |      |           |     |
| 500 億円以上                      | 81.8 | 15.9 | 2.3  | 0.0       | 0.0 |
| 100 億円以上 500 億円未満             | 70.2 | 19.1 | 7.4  | 2.1       | 1.1 |
| 50 億円以上 100 億円未満              | 65.7 | 31.4 | 2.9  | 0.0       | 0.0 |
| 10 億円以上 50 億円未満               | 55.4 | 31.5 | 8.7  | 3.3       | 1.1 |
| 1 億円以上 10 億円未満                | 59.6 | 21.3 | 12.8 | 5.3       | 1.1 |
| 5 千万円以上 1 億円未満                | 56.3 | 21.9 | 15.6 | 6.3       | 0.0 |
| 5 千万円未満 (資本金なしを含む)            | 61.0 | 22.0 | 9.8  | 6.5       | 0.8 |

資本金規模別にみると、経営者層の関心の高さは資本金規模に応じた結果となっており、規模を反映した傾向がみられる。

「②個人情報などの情報漏えいに対するリスク」については、経営者層として次のような回答を示している。関心度合いが「高い」(69.3%)は、「情報システム関連の事件・事故関連のリスク」に比べわずかではあるが高い割合となっており、その分、「中位」の割合が減少している。

| 個人情報などの情報漏えいリスクに<br>対する意識 | 高い   | 中位   | 低い   | わから<br>ない | 無回答 |
|---------------------------|------|------|------|-----------|-----|
| 業種グループ                    |      |      |      |           |     |
| 食品・紙・パルプ・繊維・印刷            | 44.4 | 40.7 | 11.1 | 3.7       | 0.0 |
| 石油・化学・鉄鋼・非鉄・金属            | 38.9 | 36.1 | 16.7 | 8.3       | 0.0 |
| 電気・一般・輸送用機械               | 61.7 | 23.3 | 13.3 | 0.0       | 1.7 |
| その他製造業                    | 48.4 | 25.8 | 19.4 | 3.2       | 3.2 |
| 商業                        | 54.1 | 27.0 | 16.2 | 2.7       | 0.0 |
| 金融・保険業                    | 92.2 | 6.3  | 0.0  | 0.0       | 1.6 |
| 情報処理サービス業                 | 92.6 | 6.2  | 1.2  | 0.0       | 0.0 |
| その他対事業所サービス               | 65.8 | 23.7 | 6.6  | 3.9       | 0.0 |
| 公共サービス                    | 63.2 | 23.7 | 7.9  | 5.3       | 0.0 |
| 政府・地方公共団体                 | 78.1 | 15.6 | 1.6  | 3.1       | 1.6 |
| 計                         | 69.3 | 19.8 | 7.6  | 2.5       | 0.8 |

業種グループ別にみると、「金融・保険業」ならびに「情報処理サービス業」では9割を超えており、いかに情報漏れがビジネス展開上重要なリスクであるかを物語っている。

| 個人情報などの情報漏えいリスクに対する意識 | 高い   | 中位   | 低い   | わからない | 無回答 |
|-----------------------|------|------|------|-------|-----|
| 資本金規模                 |      |      |      |       |     |
| 500 億円以上              | 86.4 | 13.6 | 0.0  | 0.0   | 0.0 |
| 100 億円以上 500 億円未満     | 76.6 | 13.8 | 6.4  | 2.1   | 1.1 |
| 50 億円以上 100 億円未満      | 74.3 | 22.9 | 2.9  | 0.0   | 0.0 |
| 10 億円以上 50 億円未満       | 65.2 | 22.8 | 8.7  | 2.2   | 1.1 |
| 1 億円以上 10 億円未満        | 61.7 | 22.3 | 12.8 | 2.1   | 1.1 |
| 5 千万円以上 1 億円未満        | 56.3 | 21.9 | 15.6 | 6.3   | 0.0 |
| 5 千万円未満(資本金なしを含む)     | 68.3 | 21.1 | 5.7  | 4.1   | 0.8 |

資本金規模別にみても、規模の大小にかかわらず、経営者層の関心が高いことがわかる。

「③情報セキュリティガバナンス」については、経営者層の関心度合いが「高い」が 19.5%であり、前述の情報システム関連事件・事故リスクおよび情報漏えいリスク関連に対する経営者の関心度合いと比べ、かなり低い結果となった。METI の情報セキュリティ対策上の新しい枠組みとして、利害関係者に情報セキュリティに関する情報開示を求めているわけであるが、調査結果からは「中位」が 33.7%と「わからない」の 30.7%を若干上回っている程度であり、さらに注意喚起が必要かもしれない。

| 情報セキュリティガバナンスに対する意識 | 高い   | 中位   | 低い   | わからない | 無回答 |
|---------------------|------|------|------|-------|-----|
| 業種グループ              |      |      |      |       |     |
| 食品・紙・パルプ・繊維・印刷      | 18.5 | 29.6 | 14.8 | 37.0  | 0.0 |
| 石油・化学・鉄鋼・非鉄・金属      | 5.6  | 30.6 | 25.0 | 38.9  | 0.0 |
| 電気・一般・輸送用機械         | 15.0 | 35.0 | 21.7 | 26.7  | 1.7 |
| その他製造業              | 6.5  | 19.4 | 25.8 | 45.2  | 3.2 |
| 商業                  | 13.5 | 43.2 | 27.0 | 16.2  | 0.0 |
| 金融・保険業              | 29.7 | 35.9 | 6.3  | 25.0  | 3.1 |
| 情報処理サービス業           | 25.9 | 46.9 | 6.2  | 21.0  | 0.0 |
| その他対事業所サービス         | 26.3 | 39.5 | 10.5 | 23.7  | 0.0 |
| 公共サービス              | 13.2 | 23.7 | 21.1 | 42.1  | 0.0 |
| 政府・地方公共団体           | 18.8 | 17.2 | 14.1 | 48.4  | 1.6 |
| 計                   | 19.5 | 33.7 | 15.2 | 30.7  | 1.0 |

業種グループ別にみると、「金融・保険業」および「情報処理サービス業」で「高い」がそれぞれ 29.7%、25.9%と「中位」より低い割合となっている。「政府・地方公共団体」では「高い」が「中位」を上回っているが、それでも 20%以下である。

| 情報セキュリティガバナンス<br>に対する意識 | 高い   | 中位   | 低い   | わからない | 無回答 |
|-------------------------|------|------|------|-------|-----|
| 資本金規模                   |      |      |      |       |     |
| 500 億円以上                | 38.6 | 40.9 | 9.1  | 9.1   | 2.3 |
| 100 億円以上 500 億円未満       | 23.4 | 40.4 | 9.6  | 25.5  | 1.1 |
| 50 億円以上 100 億円未満        | 17.1 | 54.3 | 14.3 | 14.3  | 0.0 |
| 10 億円以上 50 億円未満         | 25.0 | 30.4 | 14.1 | 29.3  | 1.1 |
| 1 億円以上 10 億円未満          | 10.6 | 36.2 | 17.0 | 35.1  | 1.1 |
| 5 千万円以上 1 億円未満          | 3.1  | 37.5 | 21.9 | 37.5  | 0.0 |
| 5 千万円未満(資本金なしを含む)       | 17.1 | 19.5 | 19.5 | 43.1  | 0.8 |

資本金規模別にみると、規模が大きくなるにつれて、関心度合いは高くなっている。

「④情報セキュリティ対策ベンチマーク」については、注2に示されているように、METI が進めている情報セキュリティ対策についての総合評価方法で数値化された結果が得られるものであるが、これに関する経営者の関心度合いに関し、「高い」という回答は8.6%と1割を下回っている。また、「中位」が29.8%、「低い」は23.5%と関心度合いは低い。

| 情報セキュリティ対策ベンチマーク<br>に対する意識 | 高い   | 中位   | 低い   | わからない | 無回答 |
|----------------------------|------|------|------|-------|-----|
| 業種グループ                     |      |      |      |       |     |
| 食品・紙・パルプ・繊維・印刷             | 7.4  | 22.2 | 29.6 | 40.7  | 0.0 |
| 石油・化学・鉄鋼・非鉄・金属             | 0.0  | 22.2 | 30.6 | 47.2  | 0.0 |
| 電気・一般・輸送用機械                | 5.0  | 23.3 | 38.3 | 30.0  | 3.3 |
| その他製造業                     | 3.2  | 3.2  | 35.5 | 54.8  | 3.2 |
| 商業                         | 2.7  | 40.5 | 32.4 | 24.3  | 0.0 |
| 金融・保険業                     | 17.2 | 31.3 | 23.4 | 25.0  | 3.1 |
| 情報処理サービス業                  | 11.1 | 48.1 | 11.1 | 29.6  | 0.0 |
| その他対事業所サービス                | 14.5 | 42.1 | 15.8 | 27.6  | 0.0 |
| 公共サービス                     | 5.3  | 18.4 | 31.6 | 44.7  | 0.0 |
| 政府・地方公共団体                  | 6.3  | 17.2 | 12.5 | 62.5  | 1.6 |
| 計                          | 8.6  | 29.8 | 23.5 | 37.0  | 1.2 |

業種グループ別にみると、「金融・保険業」で「高い」が17.2%、「中位」の31.3%とあわせれば48.5%となるが、「低い」、「わからない」の合計48.4%とほぼ同じ割合となっている。

「情報処理サービス業」では「高い」が11.1%、「中位」が48.1%である。「政府・地方公共団体」でも「高い」が6.3%、「中位」が17.2%であり、こうした状況に鑑みて、さらなる注意喚起が必要であろう。

| 情報セキュリティ対策ベンチマーク<br>に対する意識 | 高い   | 中位   | 低い   | わからない | 無回答 |
|----------------------------|------|------|------|-------|-----|
| 資本金規模                      |      |      |      |       |     |
| 500 億円以上                   | 25.0 | 36.4 | 20.5 | 15.9  | 2.3 |
| 100 億円以上 500 億円未満          | 6.4  | 36.2 | 22.3 | 34.0  | 1.1 |
| 50 億円以上 100 億円未満           | 5.7  | 40.0 | 28.6 | 25.7  | 0.0 |
| 10 億円以上 50 億円未満            | 9.8  | 32.6 | 21.7 | 34.8  | 1.1 |
| 1億円以上 10 億円未満              | 8.5  | 26.6 | 26.6 | 37.2  | 1.1 |
| 5千万円以上1億円未満                | 3.1  | 25.0 | 28.1 | 43.8  | 0.0 |
| 5千万円未満(資本金なしを含む)           | 5.7  | 21.1 | 22.0 | 49.6  | 1.6 |

資本金規模別にみると、「500 億円以上」の事業体で4社に1社の割合で関心が「高い」という結果となった。

Q5. 情報システム関連、情報セキュリティ関連、個人情報漏えいのリスクが貴事業体の経営に重大な影響(経営危機、倒産等)を与えますか。(単一回答)

|     |              |     |       |
|-----|--------------|-----|-------|
| 1   | 思う           | 259 | 50.4  |
| 2   | 重大な影響は受けると思う | 196 | 38.1  |
| 3   | 重大な影響は受けない   | 46  | 8.9   |
| 4   | わからない        | 10  | 1.9   |
| 無回答 |              | 3   | 0.6   |
| 計   |              | 514 | 100.0 |

情報システム関連、情報セキュリティ関連、個人情報漏えいのリスクが事業体の経営に重大な影響を与えると思うか、という質問に対し、「思う」、「重大な影響は受けると思う」の合計は88.5%であり、「重大な影響は受けない」が8.9%であった。このように情報セキュリティ関連のリスクが経営問題であるという認識は広まっているといえる。

業種グループ別にみると、「金融・保険業」で「思う」が70.3%、「重大な影響は受けると思う」が28.1%で合計98.4%、しかも「重大な影響は受けない」という回答が0件であった。また、「情報処理サービス業」は「思う」が80.2%、「重大な影響は受けると思う」が18.5%、「重大な影響は受けない」が1.2%であり、「金融・保険業」と「情報処理サービス業」が情報セキュリティなどのリスクが経営に大きな打撃を与える重大なリスクと認識している。一方、「製造業」全般は「重大な影響を受けない」が20.1%であり、業種による差異が明確に表れている。

事業体規模別で比較すると、資本金規模別では「10 億円以上 50 億円未満」、「1 億円以上 10 億円未満」の事業体で「重大な影響は受けない」という回答が10%を超えている。また、従業員数別では「500 人以上 1,000 人未満」、「300 人以上 500 人未満」、「100 人未満」で「重大な影響は受けない」が10%を超えている。一般に規模が小さいところほど経営への影響が小さいと認識しているところが増えている。これは小規模製造業を中心に情報リスクが小さいと認識されていると推定される。

Q6. 情報セキュリティガバナンス(Q4の「注1」参照)の観点から、情報セキュリティ対策にあたり、どの関係者を考慮に入れていますか。(複数回答)

| 回答件数      | 514 | —    |
|-----------|-----|------|
| 1 株主・投資家等 | 200 | 38.9 |
| 2 顧客・消費者  | 364 | 70.8 |
| 3 取引先     | 288 | 56.0 |
| 4 格付け機関   | 26  | 5.1  |
| 5 従業員     | 295 | 57.4 |
| 6 その他     | 51  | 9.9  |
| 無回答       | 18  | 3.5  |

ここでは情報セキュリティガバナンスの関係者について調査した。調査結果からはコーポレートガバナンスで重視されているものとほぼ同様に重視されていることがわかる。これらは、事業体の利益と密接に関係していることから、情報セキュリティガバナンスでも基本となる構造であろう。関心の高い順では、「顧客・消費者」70.8%、「取引先」56.0%、「従業員」57.4%、「株主・投資家」38.9%となっている。ただし、コーポレートガバナンスの場合、株主がより高い位置に来るのに対し、「顧客・消費者」が高い位置づけにあるのは、個人情報漏えいなどの場合、最も影響が大きいのが顧客・消費者であるためと考えられる。また、「格付け機関」が5.1%と少ないのは、株主・投資家が少ないことにも関係がある。今まで、個人情報漏えいで倒産した企業がないことや、株価が暴落したというような事例がないためと考えられる。以上の結果からは、事業体にとって情報セキュリティガバナンスが重要なテーマとなってきたことがわかる。

その他の記述回答では、地方公共団体から「住民」、教育機関からは「学生」との回答が多く出された。

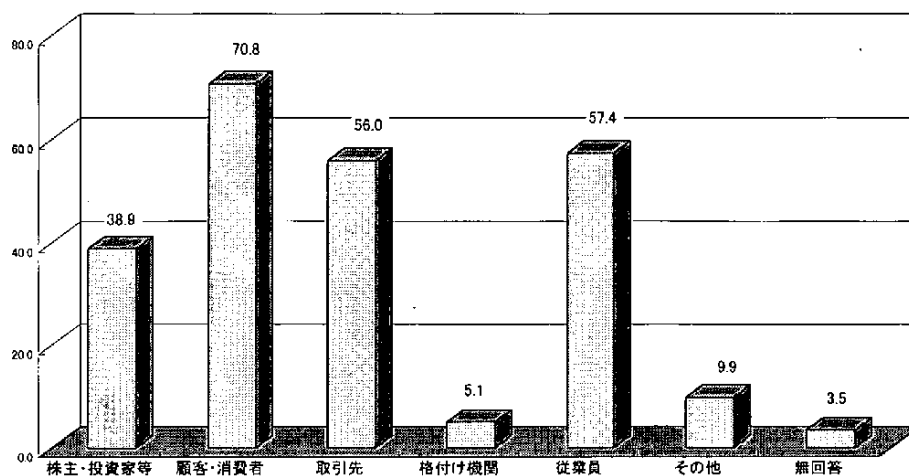


図2-2-5. 情報セキュリティガバナンスの関係者

従業員数別にみると、規模によって「株主・投資家等」、「顧客・消費者」、「取引先」の割合が異なっている。規模が中規模以下の場合には「顧客・消費者」を重視しており、「株主・投資家等」の占める割合はあまり大きくない。規模が大きい事業体では「顧客・消費者」を偏重していない。

むしろ全体をバランスして扱っていることがわかる。すなわち、大規模な事業体ほど情報セキュリティは全体の関係者に共通するテーマとなっていることがわかる。これは、情報セキュリティの観点からは、大規模な事業体は、たとえば ISMS 認証取得など、情報セキュリティに対する対策がすでに採られていて、特に顧客や取引先の目を気にしていないと考えられる。一方、従業員が3,000人未満の事業体では「顧客・消費者」と「取引先」がほぼ同じレベルとなっている。これは、個人情報の取扱いなどで顧客や取引先から厳しい条件が課せられるためと考えるのが妥当であろう。情報セキュリティガバナンスは、事業体にとって重要な問題となっていることがわかる。

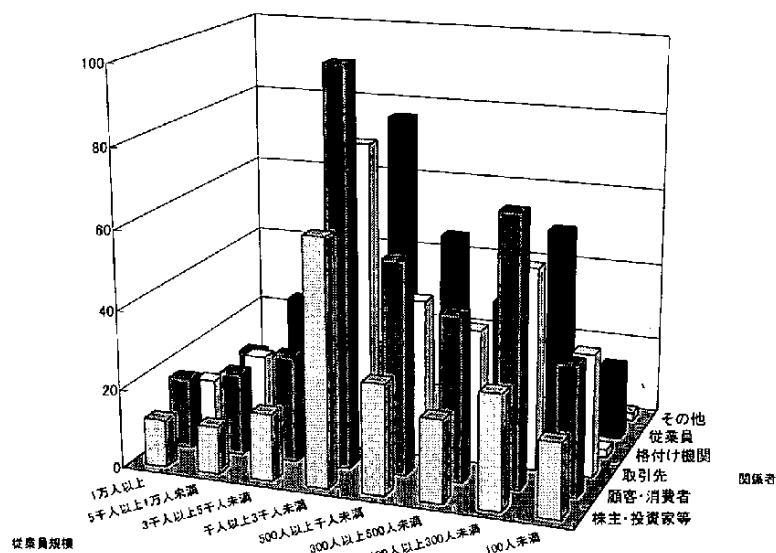


図2-2-6. 情報セキュリティガバナンスの関係者(従業員規模)

業種別グラフ(図2-2-6)をみると、「顧客・消費者」、「取引先」、「従業員」、「株主・投資家等」の割合順序は従業員数別とほぼ同じであることがわかる。ただし、「金融・保険業」、「公共サービス」、「政府・地方公共団体」では、「顧客・消費者」の割合が他の業種よりも高い。一方、「情報処理サービス業」では、「顧客・消費者」と「取引先」の差が最も小さい。

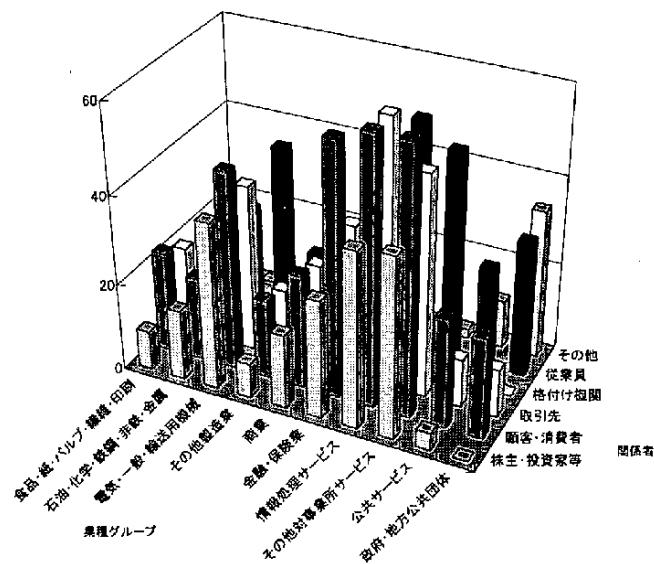


図2-2-7. 情報セキュリティガバナンスの関係者(業種グループ別)

なお、情報セキュリティガバナンスが企業における重要な経営問題になっている。METI から平成 17 年 3 月に「企業における情報セキュリティガバナンスのあり方に関する研究会」の研究成果が発表された。政府は、報告資料で①情報セキュリティ対策ベンチマーク、②情報セキュリティ報告書モデル、③事業継続計画策定ガイドラインを提言した。

①は企業が業界や扱っている情報、リスクなどを考慮して、自社が他の企業と比べてどのような立ち位置にいるのか、同業種と比べてどのような対策が進んでいるのか、または遅れているのかを評価できる。このツールは独立行政法人情報処理推進機構（以下、「IPA」という。）のホームページで公開されており、多くの企業が自社のレベルを測定できるようになっている。

②は今後、企業が有価証券報告書などで自社の情報セキュリティのレベルを報告する際のベースとなるものである。平成 17 年 12 月には政府の統一基準が策定され、政府の仕事を委託される企業には情報セキュリティ対策が要求されるようになる。このような調達の場合に、企業の情報セキュリティについて報告する際の報告書のガイドである。

③は METI が平成 16 年以来進めている「しなやかな事故前提社会システム」を実現する上で、事故への対応、事故からの復旧などをまとめた事業継続のガイドラインとなっている。

一方、経済団体連合会は、METI の情報セキュリティガバナンスの施策について、「経済界としては、情報セキュリティの確保をコーポレートガバナンスや企業の社会的責任の一環と捉え、各企業の自主的取組みによって情報セキュリティを確保することが原則であると考えている。」（「企業における情報セキュリティガバナンスのあり方に関する研究会報告書(案)」に対する意見、平成 17 年 3 月 11 日、<http://www.keidanren.or.jp/japanese/policy/2005/012.html>）と一応の評価をしている。しかし、「企業の情報セキュリティ確保に関する政府の役割は、自らの情報セキュリティ確保の取組みを通じて企業等に範を示すことや、広報、啓蒙活動を通じたセキュリティ文化の醸成、税制的優遇措置の付与など、各企業の自主的取組みを促すための環境整備であることを銘記すべきである。」（同上）とも述べている。

また、米国では、平成 15 年に官民をあげて情報セキュリティガバナンスについて会合を開催し、方向性をまとめた。特に、ビジネス・ソフトウェア・アライアンス (Business Software Alliance: BSA) は、「情報セキュリティガバナンス：行動のためのフレームワーク (Information Security Governance: Toward a Framework for Action)」で、情報セキュリティについては以下の 4 点についてのフレームワークを構築することを提案している。①政府による情報セキュリティに関する規制枠組み整備が重要、②情報セキュリティ問題は、技術的問題ではなく、企業のコーポレートガバナンス問題として扱う必要がある、③情報セキュリティ問題を解決するために共通に行動できることが必要、その結果、④情報セキュリティ対策が遅々として進まないのは情報セキュリティガバナンスのフレームワークが機能していないからであり、官民を挙げた対応が必要、としている。米国の情報セキュリティガバナンスは、経営者に向けた情報セキュリティ問題が経営問題であることを認知することを主張し、そのための企業の弱みを知るためのツールを開発した。

○METI 「企業における情報セキュリティガバナンスのあり方に関する研究会」のページ

[http://www.meti.go.jp/policy/netsecurity/sec\\_gov\\_report.html](http://www.meti.go.jp/policy/netsecurity/sec_gov_report.html)

○IPA 「情報セキュリティ対策ベンチマーク」のページ

<https://isec.ipa.go.jp/benchmark-new/member/>

Q7. 次のリスク分析手法を知っていますか。

| リスク分析手法                                                                     | 利用したことがある |     | 知っている |      | 知らない |      | 無回答 |      | 計   |       |
|-----------------------------------------------------------------------------|-----------|-----|-------|------|------|------|-----|------|-----|-------|
| ①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)における脆弱性分析                        | 20        | 3.9 | 201   | 39.1 | 285  | 55.4 | 8   | 1.6  | 514 | 100.0 |
| ②日本情報処理開発協会が開発した JRAM における定量分析                                              | 6         | 1.2 | 164   | 31.9 | 335  | 65.2 | 9   | 1.8  | 514 | 100.0 |
| ③GMITS (GMITS Guidelines for the Management for IT Security (ISO/IEC13335)) | 26        | 5.1 | 153   | 29.8 | 328  | 63.8 | 7   | 1.4  | 514 | 100.0 |
| ④その他                                                                        | 7         | 1.4 | 4     | 0.8  | 0    | 0.0  | 503 | 97.9 | 514 | 100.0 |

JIPDEC は平成4年にリスク分析手法『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。)を発表した。その後の著しい情報環境の変化に対応するため、平成16年1月に『JIPDEC リスクマネジメントシステム (J RMS) 解説書 (以下、「J RMS」という。)]<sup>1</sup>を発売した。J RMS 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、情報システム部門、ユーザ部門におけるリスクマネジメント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 が開発した手法である。

この J RMS の認知度について、前回調査では 27.3%の事業体が「知っている」、1.7%が「利用したことがある」と回答してくれた。この点は、すでに『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)』報告書が平成15年3月に発行されており、その「第IV部 J RMS 質問項目」に J RMS 解説書における項目案が示されていることから、1.7%の「利用がある」と回答したのではないかと解説しておいた。今回の調査結果では「利用したことがある」が 3.9%、「知っている」が 39.1%であった。

業種別にみると、「情報処理サービス業」ではある程度の認知度があることが理解できる。

| 業種グループ         | J RMS の認知度 | 利用したことがある | 知っている | 知らない | 無回答 |
|----------------|------------|-----------|-------|------|-----|
| 食品・紙・パルプ・繊維・印刷 |            | 0.0       | 18.5  | 81.5 | 0.0 |
| 石油・化学・鉄鋼・非鉄・金属 |            | 0.0       | 36.1  | 63.9 | 0.0 |
| 電気・一般・輸送用機械    |            | 1.7       | 25.0  | 70.0 | 3.3 |
| その他製造業         |            | 3.2       | 16.1  | 77.4 | 3.2 |
| 商業             |            | 0.0       | 32.4  | 64.9 | 2.7 |
| 金融・保険業         |            | 3.1       | 43.8  | 46.9 | 6.3 |
| 情報処理サービス業      |            | 16.0      | 56.8  | 27.2 | 0.0 |
| その他対事業所サービス    |            | 2.6       | 42.1  | 55.3 | 0.0 |
| 公共サービス         |            | 0.0       | 36.8  | 63.2 | 0.0 |
| 政府・地方公共団体      |            | 1.6       | 48.4  | 50.0 | 0.0 |
| 計              |            | 3.9       | 39.1  | 55.4 | 1.6 |

<sup>1</sup>「JIPDEC リスクマネジメントシステム (J RMS) 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。

「②JRAM」については「利用」が1.2%、「知っている」が31.9%と、JRMSの方に軍配を上げることができる。しかしながら、残念なことに55.4%の事業体がJRMSを「知らない」という。また、JRAMについても65.2%が「知らない」という回答であった。

「③GMITS (ISO/IEC13335)」については5.1%が「利用したことがある」という反面、「知っている」が29.8%、「知らない」が63.8%とJRMSより認知度が低い結果となっている。

重要なことは、情報リスクマネジメントに対する組織の対応の実態がどうなのか、その点を把握するための方法論を知らずに質問Q3、Q8、Q10等を回答した結果（たとえば、情報リスクマネジメントの実践等についての回答結果）をどのように理解すべきなのか、あらためて検討の余地があるかもしれない。

Q8. 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、情報セキュリティポリシー、情報リスクの分析、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。これらの対策を実施していますか。  
注)③「情報リスク分析」で「1」を回答した場合のみQ9を回答。それ以外はQ11に進む。

| 実施対策                    | 策定／実施<br>している |      | 策定／実施を<br>予定している |      | 策定／実施の<br>予定はない |      |
|-------------------------|---------------|------|------------------|------|-----------------|------|
| ①情報リスクマネジメント方針の明確化      | 235           | 45.7 | 154              | 30.0 | 116             | 22.6 |
| ②情報セキュリティポリシーの策定        | 352           | 68.5 | 111              | 21.6 | 45              | 8.8  |
| ③情報リスク分析の実施 ⇒Q9へ        | 166           | 32.3 | 206              | 40.1 | 136             | 26.5 |
| ④情報セキュリティ対策の実施手順、規程類の策定 | 288           | 56.0 | 150              | 29.2 | 65              | 12.6 |
| ⑤情報セキュリティ監査の実施          | 181           | 35.2 | 194              | 37.7 | 130             | 25.3 |
| ⑥システム監査の実施              | 179           | 34.8 | 158              | 30.7 | 165             | 32.1 |

| 実施対策                    | 無回答 |     | 計   |       |
|-------------------------|-----|-----|-----|-------|
| ①情報リスクマネジメント方針の明確化      | 9   | 1.8 | 514 | 100.0 |
| ②情報セキュリティポリシーの策定        | 6   | 1.2 | 514 | 100.0 |
| ③情報リスク分析の実施 ⇒Q9へ        | 6   | 1.2 | 514 | 100.0 |
| ④情報セキュリティ対策の実施手順、規程類の策定 | 11  | 2.1 | 514 | 100.0 |
| ⑤情報セキュリティ監査の実施          | 9   | 1.8 | 514 | 100.0 |
| ⑥システム監査の実施              | 12  | 2.3 | 514 | 100.0 |

情報リスクマネジメントを理論的・実践的に示せば、情報リスクマネジメントの方針を明確にし、情報セキュリティポリシーを策定し、その方針に従って情報リスクの分析を行い、また情報セキュリティ対策の実施手順・規程類を整備し、さらに情報セキュリティ監査なりシステム監査を実施することである。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、組織体制等の関係もあり、それぞれの事業体において若干差異が生じてこよう。前回調査では、「情報リスクマネジメント方針」19.3%、「情報リスク分析」22.3%、「情報セキュリティポリシー」52.2%、「情報セキュリティ対策」55.7%、「情報セキュリティ監査」19.3%、「システム監査」30.1%という回答結果が得られた。

今回調査においては、「①情報リスクマネジメント方針の明確化」45.7%、「②情報セキュリティポリシーの策定」68.5%、「④情報セキュリティ対策の実施手順、規程類の策定」56.0%という比

較的高い割合であるのに対し、「③情報リスク分析の実施」32.3%、「⑤情報セキュリティ監査の実施」35.2%、「⑥システム監査の実施」34.8%と、3割程度となった。

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の明確化」に従い、情報リスクにアプローチするという側面に前回以上の高い割合の回答がみられ、それなりに評価したいところであるが、情報セキュリティ対策の面ではさほどの改善は表れていないと思われる。ただ、「情報リスク分析」についても10ポイントほどのアップ（前回では22.3%）があった他、「情報セキュリティ監査」で15ポイントほど高い回答がみられたが、「システム監査」の場合は5ポイント弱のアップであった。監査の視点について、ともに30%を上回っていることは評価できるが、これらの回答結果から、情報セキュリティ監査なりシステム監査について認識が高まってきたといえるのかどうか（前回、システム監査の割合から認識の高まりを素直に表現したが）、実態についての客観的な観察が必要と思われる。こうした側面について他の質問項目とのクロス集計分析から異なる傾向が把握できるかもしれない。

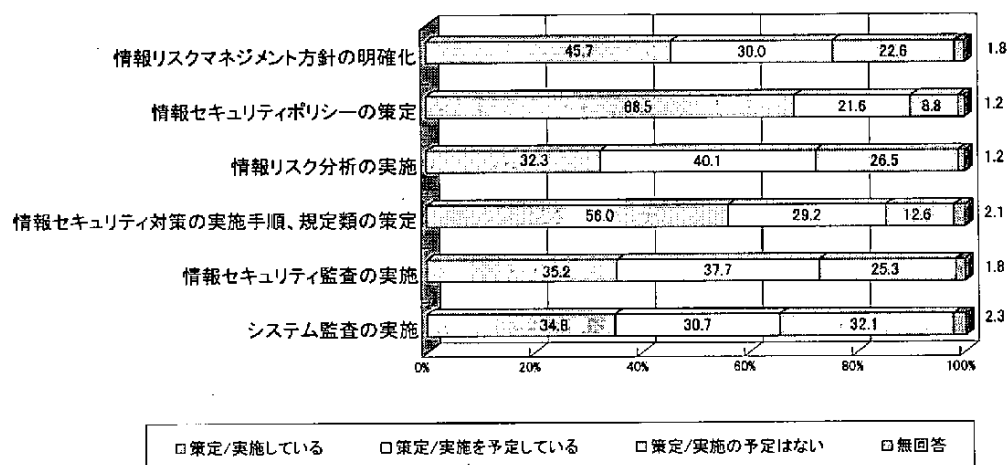


図2-2-8. 情報マネジメント上の実施対策

Q8-①情報リスクマネジメント方針の明確化

| 業種グループ         | 実施状況 | 策定／実施している | 策定／実施を予定している | 策定／実施の予定はない | 無回答 |
|----------------|------|-----------|--------------|-------------|-----|
| 食品・紙・パルプ・繊維・印刷 |      | 40.7      | 25.9         | 29.6        | 3.7 |
| 石油・化学・鉄鋼・非鉄・金属 |      | 19.4      | 41.7         | 38.9        | 0.0 |
| 電気・一般・輸送用機械    |      | 46.7      | 31.7         | 20.0        | 1.7 |
| その他製造業         |      | 19.4      | 29.0         | 48.4        | 3.2 |
| 商業             |      | 32.4      | 29.7         | 32.4        | 5.4 |
| 金融・保険業         |      | 75.0      | 17.2         | 6.3         | 1.6 |
| 情報処理サービス業      |      | 72.8      | 19.8         | 7.4         | 0.0 |
| その他対事業所サービス    |      | 35.5      | 46.1         | 17.1        | 1.3 |
| 公共サービス         |      | 28.9      | 31.6         | 36.8        | 2.6 |
| 政府・地方公共団体      |      | 40.6      | 29.7         | 28.1        | 1.6 |
| 計              |      | 45.7      | 30.0         | 22.6        | 1.8 |

Q8-②情報セキュリティポリシーの策定

| 業種グループ         | 実施状況 | 策定／実施<br>している | 策定／実施を<br>予定している | 策定／実施の<br>予定はない | 無回答 |
|----------------|------|---------------|------------------|-----------------|-----|
| 食品・紙・パルプ・繊維・印刷 |      | 55.6          | 25.9             | 14.8            | 3.7 |
| 石油・化学・鉄鋼・非鉄・金属 |      | 36.1          | 38.9             | 25.0            | 0.0 |
| 電気・一般・輸送用機械    |      | 63.3          | 30.0             | 6.7             | 0.0 |
| その他製造業         |      | 41.9          | 29.0             | 25.8            | 3.2 |
| 商業             |      | 40.5          | 35.1             | 21.6            | 2.7 |
| 金融・保険業         |      | 93.8          | 4.7              | 0.0             | 1.6 |
| 情報処理サービス業      |      | 82.7          | 13.6             | 2.5             | 1.2 |
| その他対事業所サービス    |      | 63.2          | 26.3             | 10.5            | 0.0 |
| 公共サービス         |      | 60.5          | 34.2             | 5.3             | 0.0 |
| 政府・地方公共団体      |      | 93.8          | 4.7              | 0.0             | 1.6 |
| 計              |      | 68.5          | 21.6             | 8.8             | 1.2 |

Q8-③情報リスク分析の実施

| 業種グループ         | 実施状況 | 策定／実施<br>している | 策定／実施を<br>予定している | 策定／実施の<br>予定はない | 無回答 |
|----------------|------|---------------|------------------|-----------------|-----|
| 食品・紙・パルプ・繊維・印刷 |      | 11.1          | 66.7             | 18.5            | 3.7 |
| 石油・化学・鉄鋼・非鉄・金属 |      | 5.6           | 55.6             | 38.9            | 0.0 |
| 電気・一般・輸送用機械    |      | 28.3          | 55.0             | 16.7            | 0.0 |
| その他製造業         |      | 12.9          | 25.8             | 58.1            | 3.2 |
| 商業             |      | 10.8          | 45.9             | 40.5            | 2.7 |
| 金融・保険業         |      | 54.7          | 31.3             | 12.5            | 1.6 |
| 情報処理サービス業      |      | 70.4          | 23.5             | 6.2             | 0.0 |
| その他対事業所サービス    |      | 27.6          | 42.1             | 30.3            | 0.0 |
| 公共サービス         |      | 15.8          | 39.5             | 42.1            | 2.6 |
| 政府・地方公共団体      |      | 26.6          | 37.5             | 34.4            | 1.6 |
| 計              |      | 32.3          | 40.1             | 26.5            | 1.2 |

Q8-④情報セキュリティ対策の実施手順、規程類の策定

| 業種グループ         | 実施状況 | 策定／実施<br>している | 策定／実施を<br>予定している | 策定／実施の<br>予定はない | 無回答 |
|----------------|------|---------------|------------------|-----------------|-----|
| 食品・紙・パルプ・繊維・印刷 |      | 48.1          | 25.9             | 22.2            | 3.7 |
| 石油・化学・鉄鋼・非鉄・金属 |      | 27.8          | 52.8             | 19.4            | 0.0 |
| 電気・一般・輸送用機械    |      | 55.0          | 35.0             | 8.3             | 1.7 |
| その他製造業         |      | 25.8          | 35.5             | 35.5            | 3.2 |
| 商業             |      | 24.3          | 45.9             | 27.0            | 2.7 |
| 金融・保険業         |      | 85.9          | 9.4              | 1.6             | 3.1 |
| 情報処理サービス業      |      | 77.8          | 17.3             | 2.5             | 2.5 |
| その他対事業所サービス    |      | 56.6          | 28.9             | 14.5            | 0.0 |
| 公共サービス         |      | 44.7          | 28.9             | 23.7            | 2.6 |
| 政府・地方公共団体      |      | 57.8          | 34.4             | 4.7             | 3.1 |
| 計              |      | 56.0          | 29.2             | 12.6            | 2.1 |

## Q8-⑤情報セキュリティ監査の実施

| 業種グループ         | 実施状況 | 策定／実施<br>している | 策定／実施を<br>予定している | 策定／実施の<br>予定はない | 無回答 |
|----------------|------|---------------|------------------|-----------------|-----|
| 食品・紙・パルプ・繊維・印刷 |      | 25.9          | 33.3             | 37.0            | 3.7 |
| 石油・化学・鉄鋼・非鉄・金属 |      | 8.3           | 47.2             | 44.4            | 0.0 |
| 電気・一般・輸送用機械    |      | 26.7          | 48.3             | 25.0            | 0.0 |
| その他製造業         |      | 12.9          | 32.3             | 51.6            | 3.2 |
| 商業             |      | 16.2          | 40.5             | 40.5            | 2.7 |
| 金融・保険業         |      | 46.9          | 26.6             | 23.4            | 3.1 |
| 情報処理サービス業      |      | 70.4          | 24.7             | 3.7             | 1.2 |
| その他対事業所サービス    |      | 34.2          | 39.5             | 26.3            | 0.0 |
| 公共サービス         |      | 18.4          | 39.5             | 36.8            | 5.3 |
| 政府・地方公共団体      |      | 39.1          | 50.0             | 9.4             | 1.6 |
| 計              |      | 35.2          | 37.7             | 25.3            | 1.8 |

## Q8-⑥システム監査の実施

| 業種グループ         | 実施状況 | 策定／実施<br>している | 策定／実施を<br>予定している | 策定／実施の<br>予定はない | 無回答 |
|----------------|------|---------------|------------------|-----------------|-----|
| 食品・紙・パルプ・繊維・印刷 |      | 29.6          | 29.6             | 37.0            | 3.7 |
| 石油・化学・鉄鋼・非鉄・金属 |      | 19.4          | 33.3             | 47.2            | 0.0 |
| 電気・一般・輸送用機械    |      | 36.7          | 35.0             | 26.7            | 1.7 |
| その他製造業         |      | 22.6          | 19.4             | 54.8            | 3.2 |
| 商業             |      | 24.3          | 32.4             | 40.5            | 2.7 |
| 金融・保険業         |      | 70.3          | 20.3             | 6.3             | 3.1 |
| 情報処理サービス業      |      | 43.2          | 33.3             | 22.2            | 1.2 |
| その他対事業所サービス    |      | 32.9          | 32.9             | 32.9            | 1.3 |
| 公共サービス         |      | 21.1          | 34.2             | 36.8            | 7.9 |
| 政府・地方公共団体      |      | 20.3          | 32.8             | 45.3            | 1.6 |
| 計              |      | 34.8          | 30.7             | 32.1            | 2.3 |

業種グループ別に実施状況を見ると、「①情報リスクマネジメント方針の明確化」の場合、相対的に「高い」割合を示した業種は、「金融・保険業」および「情報処理サービス業」であった。

「②情報セキュリティポリシーの策定」については、「政府・地方公共団体」が「金融・保険業」と同様に90%以上の回答を示している。

「③情報リスク分析の実施」に関しては「情報処理サービス業」のみが70.4%の回答を示したが、「金融・保険業」では50%台と低くなっている。

「④情報セキュリティ対策の実施手順、規程類の策定」となると、70%以上の回答があったのは「金融・保険業」および「情報処理サービス業」であり、金融・保険業では80%を超えている。

なお、「⑤情報セキュリティ監査の実施」の場合、70%を超える実施状況を示したのは「情報処理サービス業」のみであり、「⑥システム監査の実施」については「金融・保険業」だけが70%以上の回答を示している。監査の重要性はいずれの業種においても指摘できることであるが、「金融・保険業」および「情報処理サービス業」が他業種に比べ相対的に高い割合を示している。

たしかに業種間においてそれぞれの質問項目について回答結果に差異がみられるが、製造業と非製造業を比較すれば、製造業が相対的に低い回答を示している、その理由については分析の必

要があるかもしれない。特に、「政府・地方公共団体」については前回調査で「情報セキュリティポリシー」と「情報セキュリティ対策」の回答が高かったが、今回調査では「情報セキュリティポリシー」への回答が高かった反面、「情報リスク分析」、「システム監査」については20%台となっている。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みつめ直す必要があるとみられる。

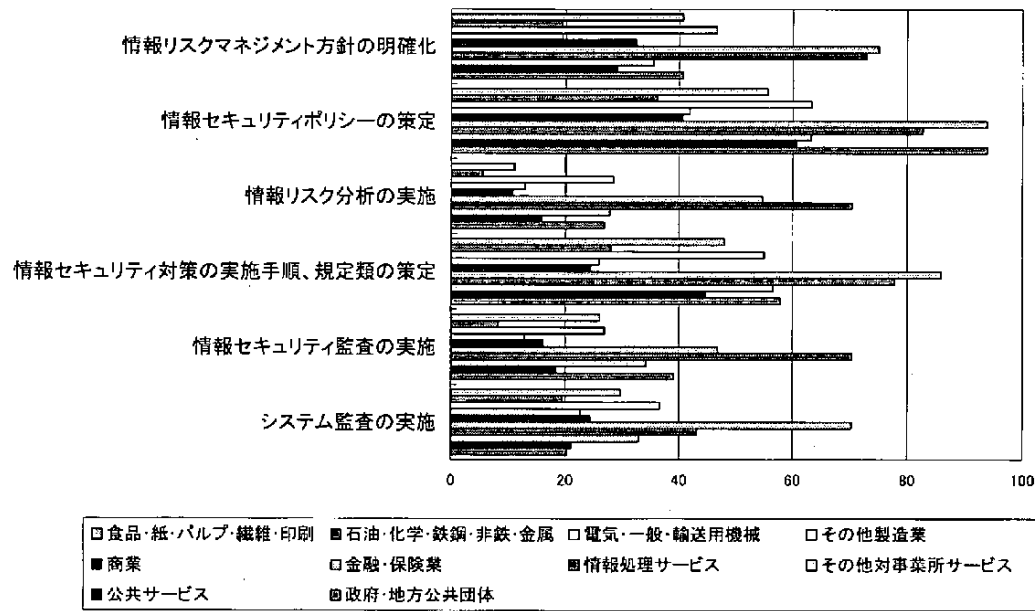


図2-2-9. 情報マネジメント上の実施対策(業種別)(選択肢「策定／実施のみ」)

| 策定／実施対策          | 情報リスクマネジメント方針 | 情報セキュリティポリシー | 情報リスク分析 | 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 |
|------------------|---------------|--------------|---------|------------|------------|--------|
| 資本金規模            |               |              |         |            |            |        |
| 500億円以上          | 65.9          | 88.6         | 45.5    | 90.9       | 59.1       | 68.2   |
| 100億円以上500億円未満   | 54.3          | 77.7         | 42.6    | 70.2       | 40.4       | 47.9   |
| 50億円以上100億円未満    | 48.6          | 54.3         | 31.4    | 40.0       | 25.7       | 48.6   |
| 10億円以上50億円未満     | 42.4          | 63.0         | 26.1    | 51.1       | 30.4       | 40.2   |
| 1億円以上10億円未満      | 42.6          | 58.5         | 34.0    | 47.9       | 34.0       | 25.5   |
| 5千万円以上1億円未満      | 34.4          | 40.6         | 25.0    | 40.6       | 25.0       | 6.3    |
| 5千万円未満(資本金なしを含む) | 39.0          | 77.2         | 25.2    | 51.2       | 32.5       | 19.5   |

資本金規模別でみると、「500億円以上」の事業体がすべての策定／実施対策で高い割合を示している。ただ、規模別のなかでも「情報セキュリティポリシー」が他に比較して策定／実施の面で高い割合となっているが、この点は情報リスクマネジメントにおける論理的なプロセスより、対外的な形式重視の結果といえるかもしれない。

さて、Q8で「情報リスク分析を実施している」と回答したケースについて、さらに分析を進めることにしたい。これまで一般的といえるのは、「はじめにリスク分析ありき」というより、「はじめに対策ありき」といったアプローチを採用する傾向であった。そうした実態について、リスクマネジメントにおけるマネジメントサイクル（PDCA）の意義を強調したいため、あらためてここで考察することにした。

Q9. Q8で「③情報リスク分析を実施している」と回答した場合、

①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）

②対象リスクを分析した結果、経営に与える影響が大きかったのは何ですか。（単一回答）

| ①対象リスク<br>回答件数:514 件 |                                             |      | ②リスク分析の結果、経営に与える影響 |           |           |      |       |
|----------------------|---------------------------------------------|------|--------------------|-----------|-----------|------|-------|
|                      |                                             |      | 影響が<br>あった         | 影響は<br>ない | わから<br>ない | 無回答  | 計     |
| 1                    | 自然災害(地震を除く水害等)                              | 131  | 81                 | 29        | 7         | 14   | 131   |
|                      |                                             | 78.9 | 61.8               | 22.1      | 5.3       | 10.7 | 100.0 |
| 2                    | 地震                                          | 140  | 108                | 15        | 7         | 10   | 140   |
|                      |                                             | 84.3 | 77.1               | 10.7      | 5.0       | 7.1  | 100.0 |
| 3                    | 人的災害(テロ 等)                                  | 110  | 68                 | 17        | 18        | 7    | 110   |
|                      |                                             | 66.3 | 61.8               | 15.5      | 16.4      | 6.4  | 100.0 |
| 4                    | コンピュータ犯罪(不正アクセス、<br>サーバ乗っ取り、故意等を含む)<br>のリスク | 146  | 109                | 18        | 8         | 11   | 146   |
|                      |                                             | 88.0 | 74.7               | 12.3      | 5.5       | 7.5  | 100.0 |
| 5                    | 運用障害(操作ミス、入力ミス等)                            | 145  | 99                 | 26        | 8         | 12   | 145   |
|                      |                                             | 87.3 | 68.3               | 17.9      | 5.5       | 8.3  | 100.0 |
| 6                    | 事故(火災、爆発、停電、漏水等)                            | 146  | 110                | 18        | 8         | 10   | 146   |
|                      |                                             | 88.0 | 75.3               | 12.3      | 5.5       | 6.8  | 100.0 |
| 7                    | 不正侵入で起きるサーバの乗っ<br>取り                        | 131  | 85                 | 27        | 8         | 11   | 131   |
|                      |                                             | 78.9 | 64.9               | 20.6      | 6.1       | 8.4  | 100.0 |
| 8                    | 自社従業員などによる故意による<br>情報漏えい                    | 145  | 111                | 17        | 8         | 9    | 145   |
|                      |                                             | 87.3 | 76.6               | 11.7      | 5.5       | 6.2  | 100.0 |
| 9                    | 不注意・過失による情報漏えい<br>(電子メールやファックスの誤送信<br>を含む)  | 144  | 103                | 19        | 8         | 14   | 144   |
|                      |                                             | 86.7 | 71.5               | 13.2      | 5.6       | 9.7  | 100.0 |
| 10                   | 盗難・車上荒らしなどによる情報<br>漏えい                      | 125  | 81                 | 28        | 7         | 9    | 125   |
|                      |                                             | 75.3 | 64.8               | 22.4      | 5.6       | 7.2  | 100.0 |
| 11                   | システムの統合リスク                                  | 81   | 35                 | 27        | 19        | 0    | 81    |
|                      |                                             | 48.8 | 43.2               | 33.3      | 23.5      | 0.0  | 100.0 |
| 12                   | システムの改良・容量増に伴う<br>トラブル                      | 108  | 61                 | 31        | 11        | 5    | 108   |
|                      |                                             | 65.1 | 56.5               | 28.7      | 10.2      | 4.6  | 100.0 |
| 13                   | 過負荷によるシステムダウン                               | 110  | 69                 | 28        | 8         | 5    | 110   |
|                      |                                             | 66.3 | 62.7               | 25.5      | 7.3       | 4.5  | 100.0 |
| 14                   | ハードウェア障害                                    | 144  | 92                 | 30        | 8         | 14   | 144   |
|                      |                                             | 86.7 | 63.9               | 20.8      | 5.6       | 9.7  | 100.0 |

| ①対象リスク<br>回答件数:514 件 |                                                               |      | ②リスク分析の結果、経営に与える影響 |           |           |      |       |
|----------------------|---------------------------------------------------------------|------|--------------------|-----------|-----------|------|-------|
|                      |                                                               |      | 影響が<br>あった         | 影響は<br>ない | わから<br>ない | 無回答  | 計     |
| 15                   | ソフトウェア障害                                                      | 138  | 87                 | 31        | 9         | 11   | 138   |
|                      |                                                               | 83.1 | 63.0               | 22.5      | 6.5       | 8.0  | 100.0 |
| 16                   | ネットワーク障害                                                      | 145  | 100                | 24        | 7         | 14   | 145   |
|                      |                                                               | 87.3 | 69.0               | 16.6      | 4.8       | 9.7  | 100.0 |
| 17                   | コンピュータウイルス、スパイウェアによるシステムの停止                                   | 150  | 99                 | 14        | 19        | 18   | 150   |
|                      |                                                               | 90.4 | 66.0               | 9.3       | 12.7      | 12.0 | 100.0 |
| 18                   | (コンピュータウイルスパラメータなどの)信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止 | 112  | 64                 | 23        | 18        | 7    | 112   |
|                      |                                                               | 67.5 | 57.1               | 20.5      | 16.1      | 6.3  | 100.0 |
| 19                   | フィッシングなどで自社サイトが模倣され、自社ユーザに被害がでる                               | 91   | 36                 | 29        | 25        | 1    | 91    |
|                      |                                                               | 54.8 | 39.6               | 31.9      | 27.5      | 1.1  | 100.0 |
| 20                   | ボットなどを利用した DOC 攻撃                                             | 96   | 44                 | 26        | 20        | 6    | 96    |
|                      |                                                               | 57.8 | 45.8               | 27.1      | 20.8      | 6.3  | 100.0 |
| 21                   | その他                                                           | 14   | 5                  | 3         | 6         | 0    | 14    |
|                      |                                                               | 8.4  | 35.7               | 21.4      | 42.9      | 0.0  | 100.0 |
| 22                   | 無回答                                                           | 2    |                    |           |           |      |       |
|                      |                                                               | 1.2  |                    |           |           |      |       |

Q8で情報リスク分析を「実施している」と回答した事業体の現状をより具体的に把握するため、対象リスクを大幅に増やした。そのうち、上表に従い、回答の割合が80%を超えた結果について高い順から示すと、「コンピュータウイルス、スパイウェアによるシステムの停止」90.4%、「コンピュータ犯罪」・「事故（火災、爆発、停電、漏水等）」88.0%、「運用障害（操作ミス、入力ミス等）」、「自社従業員などによる故意による情報漏えい」・「ネットワーク障害」87.3%、「不注意・過失による情報漏えい」・「ハードウェア障害」86.7%、「地震」84.3%、「ソフトウェア障害」83.1%となっている。ネットワーク時代におけるリスクを明示している反面、火災・爆発等の事故ならびに地震国日本といった伝統的な部分に対する考慮がみられる。

ちなみに前回調査結果をみると、「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%、「コンピュータウイルスのリスク」80.1%、「自然災害」・「運用障害（操作ミス、入力ミス等）」73.5%、「不正アクセスのリスク」70.2%であり、順位に大きな変動がみられる。今回調査で対象リスクを変更したことも影響しているが、それよりもこの2年間にコンピュータウイルス、コンピュータ犯罪、情報漏えいといった「人間のモラルハザード」に関わる側面がクローズアップされてきたためと思われる。

| 調査年度<br>順位 | 平成17年度                     | 平成15年度         |      |
|------------|----------------------------|----------------|------|
| 第1位        | コンピュータウイルス、スパイウェアによるシステム停止 | ハードウェア障害       | 第1位  |
| 第2位        | コンピュータ犯罪                   | ソフトウェア障害       | 第2位  |
|            | 事故                         | ネットワーク障害       | 第3位  |
| 第4位        | 運用障害                       | 事故             | 第4位  |
|            | 故意による情報漏えい                 | コンピュータウイルスのリスク | 第5位  |
|            | ネットワーク障害                   | 運用障害           | 第6位  |
| 第7位        | 不注意・過失による情報漏えい             | 自然災害           | 第8位  |
|            | ハードウェア障害                   | 不正アクセスのリスク     |      |
| 第9位        | 地震                         | コンピュータ犯罪のリスク   | 第9位  |
| 第10位       | ソフトウェア障害                   | アウトソーシングリスク    | 第10位 |

ところで、情報リスク分析の結果、「経営に与える影響があった」について、70%以上の回答をみると、高い順から「地震」77.1%、「自社従業員などによる故意による情報漏えい」76.6%、「コンピュータ犯罪」74.7%、「不注意・過失による情報漏えい」71.5%となっている。これを50%まで広げると上記の特徴がより明確に浮かび上がってくる。すなわち、「ネットワーク障害」69.0%、「運用障害（操作ミス、入力ミス等）」68.3%、「コンピュータウイルス、スパイウェアによるシステムの停止」66.0%、「不正侵入で起きるサーバの乗っ取り」64.9%、「盗難・車上荒らしなどによる情報漏えい」64.8%、「ハードウェア障害」63.9%、「ソフトウェア障害」63%、「過負荷によるシステムダウン」62.7%、「自然災害（地震を除く水害等）」61.8%、「（コンピュータウイルスパラメータなどの）信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止」57.1%等が重要な問題となっていることが理解できる。なお、「システムの改良・容量増に伴うトラブル」56.5%（「金融・保険業」では63.6%）、「システムの統合リスク」43.2%（「金融・保険業」では66.7%）といった結果も昨今の動向を物語っているといえよう。

Q10. Q8で「③情報リスク分析を実施している」と回答した場合、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                           | 166 | —    |
|--------------------------------|-----|------|
| 1 経営との関係がわからない                 | 10  | 6.0  |
| 2 確立した手法がない(被害想定額・被害頻度が算出できない) | 104 | 62.7 |
| 3 分析のためのデータが乏しい                | 41  | 24.7 |
| 4 専門家がない                       | 44  | 26.5 |
| 5 組織ができていない                    | 15  | 9.0  |
| 6 リスクの定量化が測れない                 | 85  | 51.2 |
| 7 その他                          | 9   | 5.4  |
| 8 特に問題はない                      | 16  | 9.6  |
| 9 無回答                          | 3   | 1.8  |

過去の調査でリスク分析実施上の問題点としてあげられたのは「確立した手法がない」、「リスクの定量化が測れない」であった。今回調査においても同様の回答結果が示されている。「確立した手法がない」(62.7%)は前回調査の47.5%を上回ったが、平成13年度の62.2%と同様の結果となった。平成15年度調査報告書でも指摘したが、「確立した手法」とは何を指すのかが問われることになるが、10年以上前にJIPDECは「JRAM」を開発しており、さらに平成15年には「JRMS解説書」を公にしている。しかも、Q7-①において「JRMS」を55.4%が「知らない」と回答している。事業体は分析手法を与えられるものという考え方でいるのか、JIPDECの広報活動に問題があるのか、いずれかであろう。しかし、事業体に対するリスクの影響に鑑みれば、進んで分析手法を求めるものと思われる。事業体がリスク分析手法を求めるにあたっては、たとえばインターネット等を用いて検索すれば容易に把握できると思われる。ただ、リスクの定量化となると、事業体としてのそれなりの体制が必要になる。

ちなみに、「リスクの定量化が測れない」(51.2%)は、前回調査の61.3%より減少した。いずれにせよ50%以上の事業体にとって「リスクの定量化」が課題となっている。定量化のアプローチについてはJRAMにおける実態分析の手法を用いれば可能であるが、その場合、上述のように組織内において事故データ(業務日報に基づく事故の発生から事業体への影響(障害報告書)等のリスク分析シートによる事故発生頻度分析・強度分析による事故結果による評価分析を実行できる)を集積・分析する体制が必要となる。さらに、定量化にはどのような尺度を設定すればよいのか、といった問題もある。考え方としては、JRMS解説書の「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。

なお、他の回答に関しては「専門家がいない」26.5%( $\searrow$ H15:38.7% $\searrow$ H13:34.1%)、「分析のためのデータが乏しい」24.7%( $\searrow$ H15:30.9% $\searrow$ H13:38.5%)、「組織ができていない」9.0%( $\searrow$ H15:16.6% $\searrow$ H13:26.7%)など、問題点に関わる割合が徐々に減少してきており、リスク分析の意義が認識されてきた傾向がうかがえる。

しかしながら、「特に問題はない」は9.6%と前回の5.5%を上回った。10%以下とはいえ、この状況をどう理解すべきか、これまで何事もなく経過してきたという楽観によるリスクセンスの欠如なのか、検討の余地がありそうである。

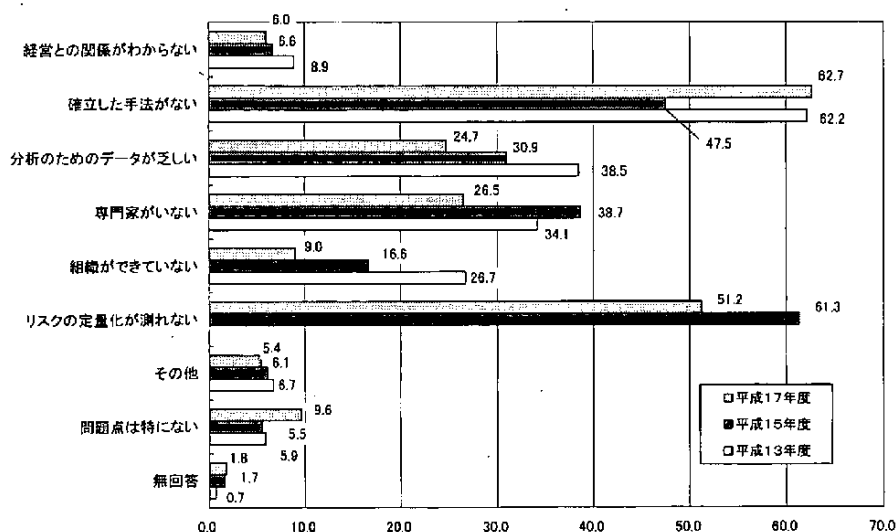


図2-2-10. リスク分析実施上の問題点

| 業種グループ \ 実施状況  | 経営との関係が<br>わからない | 確立した<br>手法がない | 分析のための<br>データが乏しい | 専門家が<br>いない | 組織ができて<br>いない |
|----------------|------------------|---------------|-------------------|-------------|---------------|
| 食品・紙・パルプ・繊維・印刷 | 0.0              | 50.0          | 0.0               | 25.0        | 25.0          |
| 石油・化学・鉄鋼・非鉄・金属 | 0.0              | 100.0         | 0.0               | 0.0         | 0.0           |
| 電気・一般・輸送用機械    | 11.8             | 70.6          | 17.6              | 17.6        | 5.9           |
| その他製造業         | 33.3             | 33.3          | 33.3              | 33.3        | 0.0           |
| 商業             | 25.0             | 25.0          | 50.0              | 0.0         | 0.0           |
| 金融・保険業         | 2.9              | 60.0          | 28.6              | 25.7        | 5.7           |
| 情報処理サービス業      | 3.5              | 59.6          | 17.5              | 19.3        | 3.5           |
| その他対事業所サービス    | 4.8              | 57.1          | 33.3              | 47.6        | 14.3          |
| 公共サービス         | 0.0              | 100.0         | 16.7              | 50.0        | 16.7          |
| 政府・地方公共団体      | 11.8             | 76.5          | 41.2              | 35.3        | 29.4          |
| 計              | 6.0              | 62.7          | 24.7              | 26.5        | 9.0           |

| 業種グループ \ 実施状況  | リスクの定量化<br>が測れない | その他  | 特に問題は<br>ない | 無回答 |
|----------------|------------------|------|-------------|-----|
| 食品・紙・パルプ・繊維・印刷 | 75.0             | 0.0  | 0.0         | 0.0 |
| 石油・化学・鉄鋼・非鉄・金属 | 50.0             | 0.0  | 0.0         | 0.0 |
| 電気・一般・輸送用機械    | 70.6             | 11.8 | 0.0         | 5.9 |
| その他製造業         | 66.7             | 0.0  | 0.0         | 0.0 |
| 商業             | 75.0             | 0.0  | 25.0        | 0.0 |
| 金融・保険業         | 60.0             | 0.0  | 8.6         | 0.0 |
| 情報処理サービス業      | 38.6             | 8.8  | 15.8        | 1.8 |
| その他対事業所サービス    | 52.4             | 4.8  | 9.5         | 0.0 |
| 公共サービス         | 16.7             | 0.0  | 0.0         | 0.0 |
| 政府・地方公共団体      | 52.9             | 5.9  | 5.9         | 5.9 |
| 計              | 51.2             | 5.4  | 9.6         | 1.8 |

ところで、業種グループ別にみると、実際の回答数を考慮すべきであるが<sup>2)</sup>、それなりの業種において約60%が「確立した手法がない」としている。

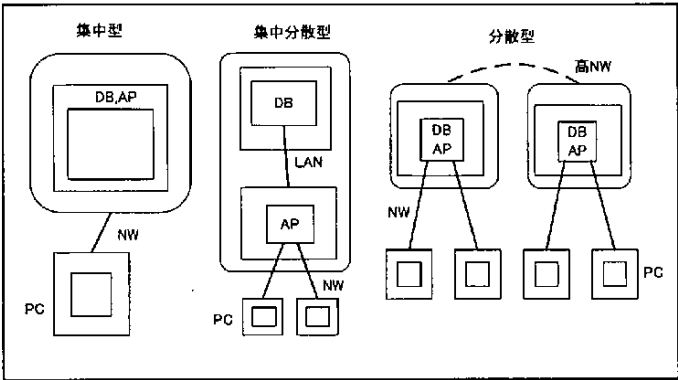
また、「リスクの定量化」については、製造業に比して非製造業でのバラツキがみられる。

<sup>2)</sup> 「石油・化学・鉄鋼・非鉄・金属」では2事業者、「公共サービス」では6事業者がすべて「確立した手法がない」としているため100%に、また「その他製造業」では3事業者うち1で33.3%、「商業」では4事業者うち1で25%となっている。

Q11. 基幹システム<sup>注1)</sup>が1時間以上停止した場合、経営に与える影響があると思いますか。

|     |     |       |     |       |
|-----|-----|-------|-----|-------|
| 1   | はい  | ⇒Q12へ | 355 | 69.1  |
| 2   | いいえ | ⇒Q13へ | 154 | 30.0  |
| 無回答 |     |       | 5   | 1.0   |
| 計   |     |       | 514 | 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(運用の型は下図参照)。本調査では、その中で**最も重要なシステム1つに限定して回答**。



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。事業体を人間に例えれば、基幹システムは体内に流れる血液の役割を果たしているといえる。人間にとって体内の血液の流れが止まると即、死に至るように、基幹システムが1時間以上停止した場合、事業体の経営に何らかの影響を与えることは当然のことと考えられる。

前回調査では、「いいえ」の回答が 77.0% (H13 : 75.9%) と圧倒的に高かったが、今回調査では「影響があると考えている事業体」が 69.1% と高くなり、「はい」と「いいえ」のポイントが逆転したことが特徴といえる。基幹システムに対する経営の依存度が高まり、重要な役割を果たしているとの認識が強まってきたことの表れであろう。

ただし、「いいえ」の回答が 30.0% あることは、まだシステムはシステム、経営とは別と考えて、基幹システムの経営に関わる影響を十分認識していない事業体があることを示しているのではないかと。「いいえ」と回答した事業体はもう一度基幹システムの経営における役割を確認し、その影響を明確にしておかないと、基幹システムへの投資が適切か否かを判断することが難しくなり、基幹システムの維持管理に悪影響を与えることが考えられる。

| 産業 \ 影響   | はい   | いいえ  |
|-----------|------|------|
| 第二次産業     | 62.8 | 37.2 |
| 第三次産業     | 69.9 | 28.6 |
| 政府・地方公共団体 | 84.4 | 14.1 |

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が、第二次産業も「はい」が「いいえ」を上回っており、基

幹システムの重要性を認識する傾向が強まってきているといえる。

また、「政府・地方公共団体」の「はい」のポイントが高く、基幹システムへの依存度がきわめて高い状況にあるものと思われる。

| 調査年度 \ 影響  | はい   | いいえ  |
|------------|------|------|
| 平成17年度調査結果 | 69.1 | 30.0 |
| 平成15年度調査結果 | 21.7 | 77.0 |
| 平成13年度調査結果 | 21.9 | 75.9 |

過去の調査結果と比較すると、前回、平成13年度調査と今回では「はい」と「いいえ」の回答が逆転しているが、これは第二次産業も第三次産業も同じである。

その原因として考えられるのは、基幹システムのトラブルおよび停止の影響などが新聞・テレビなどで大きく報道され、その影響の大きさや深刻さ、経営に与える打撃の強さなどが認識されてきた結果と思われる。

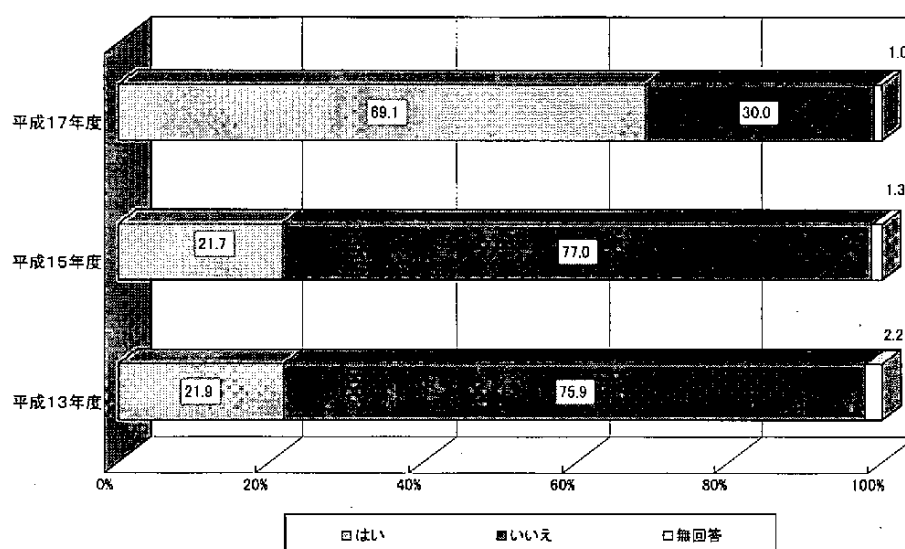


図2-2-11. 基幹システムの停止に伴う経営に与える影響度の想定

Q12. Q11 で「1」と回答した場合、被害の推定額<sup>(注)</sup>は1日あたりどれ位ですか。

|     |               |     |       |
|-----|---------------|-----|-------|
| 1   | 10億円以上        | 23  | 6.5   |
| 2   | 5億円以上～10億円未満  | 11  | 3.1   |
| 3   | 1億円以上～5億円未満   | 33  | 9.3   |
| 4   | 5千万円以上～1億円未満  | 48  | 13.5  |
| 5   | 1千万円以上～5千万円未満 | 49  | 13.8  |
| 6   | 1千万円未満        | 130 | 36.6  |
| 無回答 |               | 61  | 17.2  |
| 計   |               | 355 | 100.0 |

(注)被害額には売上の逸失額、賠償金額、原状回復費用を含みます。

基幹システムが1時間以上停止した場合、経営に与える被害の推定額は「1千万円未満」が36.6% (H15:41.2%)と最も高く、「1千万円以上～5千万円未満」が13.8% (H15:25.2%)、「5千万円以上～1億円未満」が13.5% (H15:5.3%)となっている。

被害の推定額は「1千万円未満」、「1千万円以上～5千万円未満」の割合がそれぞれ減少し、「5千万円以上～1億円未満」は増加している。しかし、前回調査では10億円以上の損害を想定した事業体が10.7%あったが、今回は6.5%と減少している。

ここでは被害推定額を「(注)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。」と注釈しているが、結果からみると被害の範囲は前回同様、直接的被害に抑えて想定したものと思われる。被害の範囲を注釈に示した内容まで拡大して想定しないと実際の被害額が過少に見積もられ、基幹システムの経営に与える位置づけが不明確になり、基幹システム改善の方向性を見失う結果となることが考えられる。

被害の推定額が低めに見積もられていることと、無回答の大幅な増加が気になるところである。今回調査では「無回答」が17.2%と前回の6.1%を大幅に上回っているが、影響ありと想定している以上は被害の想定を金額換算して推定額を把握しておく必要がある。

平成17年度に起きた証券取引関連システムトラブルなどの情報システムのトラブル被害の大きさと影響範囲の大きさを改めて確認する必要がある。

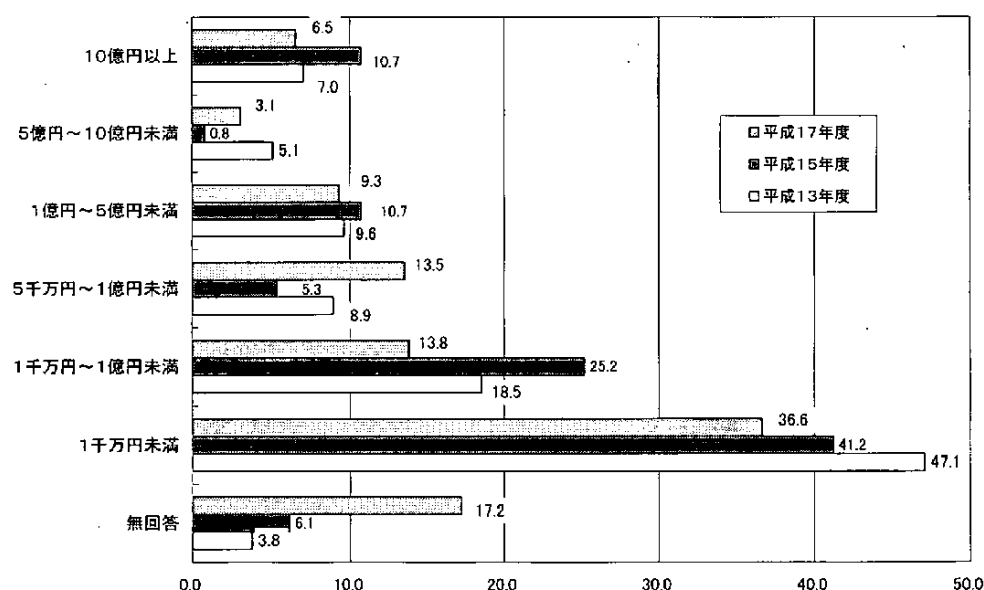


図2-2-12. 1日あたりの被害損失額

Q13-①貴事業体の基幹システムは、過去1年間に、システムの運用に悪影響を与えたか、または事業中断につながるシステムダウン<sup>(注1)</sup>が発生しましたか。

| 回答件数 |             | 514 | —    |
|------|-------------|-----|------|
| 1    | 全体的にダウンした   | 41  | 8.0  |
| 2    | 部分的にダウンした   | 215 | 41.8 |
| 3    | ダウンしない⇒Q15へ | 249 | 48.4 |
| 無回答  |             | 23  | 4.5  |

システムダウンの発生率は平成 11 年度 51.7%、13 年度 54.1%とあまり大きな変化はみられなかったが、前回調査で 47.6%に減少した。今回調査では 49.8%と前回とほとんど変化はみられなかった。また、「全体的にダウンした」は、11 年度 11.4%、13 年度 9.1%、前回 7.8%と一貫して減少していた。今回調査でも 8.0%と前回調査とほぼ同様であった。

前回調査時に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コメントした。今回調査でシステムダウンの発生率および全体的なダウンについて、どちらも変化がなかったことから、分散システムによる大規模な障害の減少というメリットは、ほぼ限界に近づいたともいえよう。

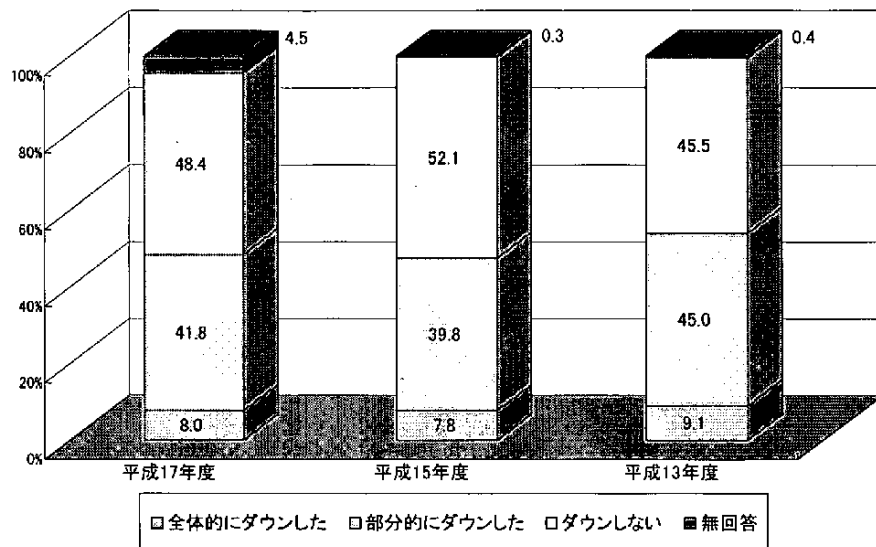


図2-2-13. システムダウンの発生率

資本金規模別にみるとほとんど差がないことがわかる。ホストコンピュータを利用していた時代には、事業規模に応じて大型コンピュータ、中型（ミニコンを含む）、オフィスコンピュータという使い分けがあった。現在は、PC やネットワーク機器の価格が安くなったおかげで、ほとんどの事業で導入されているため、事業の規模によるシステムのダウンは差がなくなったといえよう。

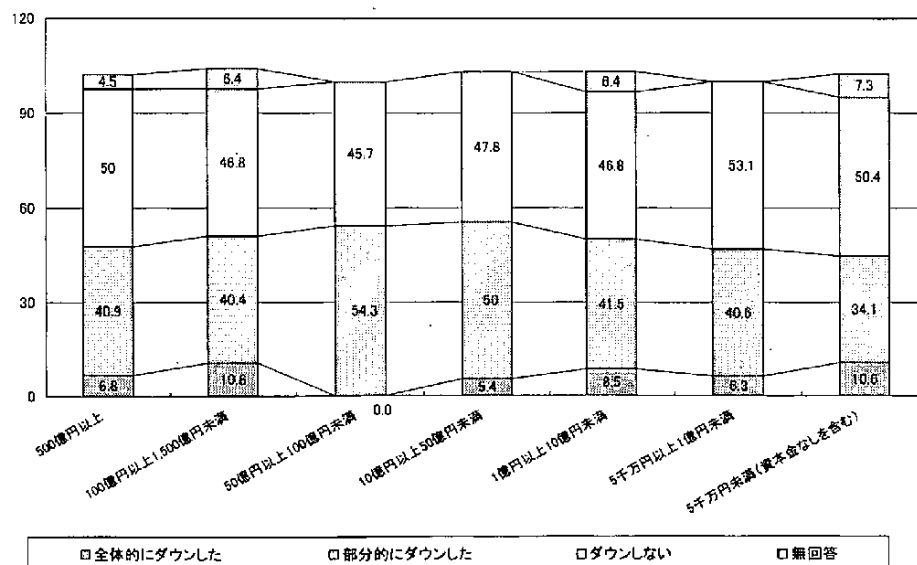


図2-2-14. システムダウンの発生率(資本金規模別)

業種別にみると、ダウンの割合が小さいのは「商業」、「情報処理サービス業」、「政府・地方公共団体」で、「金融・保険業」がこれに続いている。一方、ダウンの割合が多いのは、「食品・紙・パルプ・繊維・印刷」と「その他対事業所サービス」となっている。いずれも、情報処理が重要な業種においてはダウン対策が採られていると考えられる。

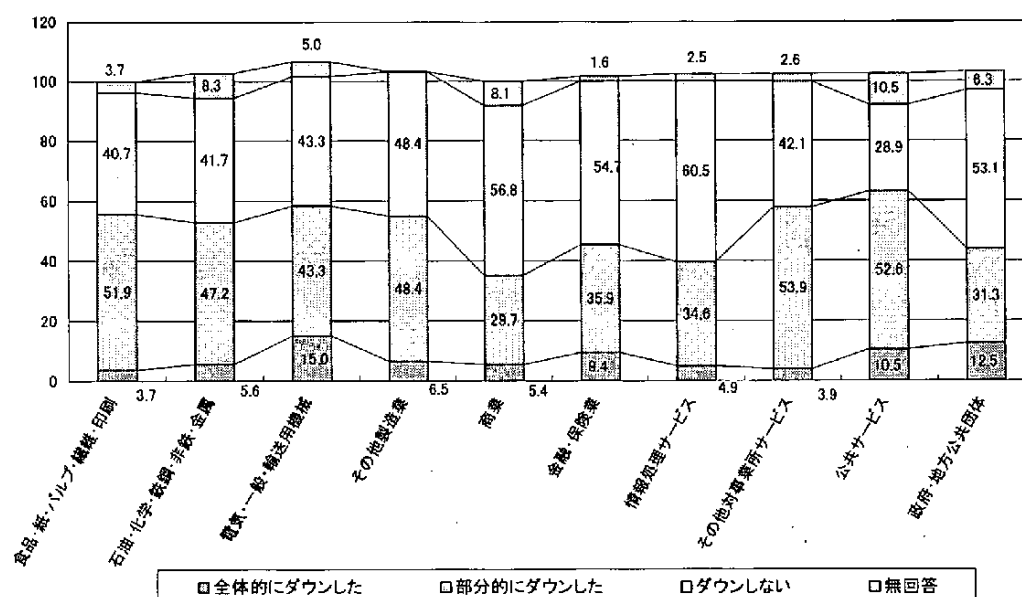


図2-2-15. システムダウンの発生率(業種別)

Q13-②システムダウンはシステムの運用に悪影響を与えたか、さらに事業中断につながるもの<sup>(注2)</sup>でしたか。

| ②システムダウンの影響 |           |     | システム運用<br>への悪影響 <sup>(注2)</sup> |      | 事業中断 |      | 無回答 |     |
|-------------|-----------|-----|---------------------------------|------|------|------|-----|-----|
| 1           | 全体的にダウンした | 41  | 33                              | 80.5 | 11   | 26.8 | 0   | 0.0 |
| 2           | 部分的にダウンした | 215 | 190                             | 88.4 | 29   | 13.5 | 4   | 1.9 |

(注1)システムダウンとは、システムの全面ストップもしくはそれに準じる障害と定義します。

(注2)「システム運用への悪影響」は、事業中断に至らなかったシステム障害を指します。

システムダウンによる運用への影響について、「全体的にダウンした」事業体 41 件 (8.0%) のうち、11 件 (26.8%) が「事業中断があった」、また、33 件 (80.5%) が「システム運用への悪影響があった」、また、「部分的にダウンした」事業体の 215 件 (48.4%) のうち、29 件 (13.5%) が「事業中断があった」、190 件 (88.4%) が「システム運用への悪影響があった」と回答している。これらの結果から、システムの障害は、組織や企業にとって重要な項目となっていることがわかる。

平成 16 年以降、METI が「しなやかな事故前提社会システム」を提唱している。今回調査において大規模な障害は減ってきているものの、部分的な問題を 40% 近くの事業体が経験していることにもみられるように、事故を減少させるのは難しい問題といえよう。したがって、事故が起きることを前提にして、企業や組織では対応を十分に考慮して対処することが望ましいといえよう。

ちなみに、平成 16 年 4 月 8 日に発生した航空路レーダー情報処理システム障害や、14 年 4 月のみずほ銀行合併時の大混乱、また、16 年度には東証、大証などで情報システムの大規模な問題が多発した。これらの情報システムでは、大型ホスト型のアーキテクチャから分散システムへの移行が検討され、その途上であった。事業体からの要請でさまざまな機能を追加しているため、デバックや改良には十分な注意が必要であったが、予算的な面も含め、十分ではなく、結果として事業中断に陥ったとみられる。今後とも、情報システムをめぐる外部条件は、ターゲットとするユーザニーズの多様化、対応までの時間的な制約、関係するシステムやハードウェアの多様化など、ますます厳しくなると考えられる。したがって、情報システムの設計、改良には、事業を中断させるリスクを十分に考慮した対応が求められている。高度な事業を支援しながら、情報システムの信頼性を落とさずに運用しつつ、新しいシステムに移行する技術やノウハウを確立することが求められている。

資本金規模別にみた部分的なダウンが与える影響には顕著な差はみられない。ただし、資本金規模が大きいほど、事業中断につながる割合は小さくなっている。一方、資本金が小さい事業体では、部分的なダウンが事業中断につながる割合が高いことがわかる。これは、事業規模が大きいほど、複数のシステムを導入していたり、二重化などの対策が採られていることから、事業に与える影響が限定されているためと考えられる。

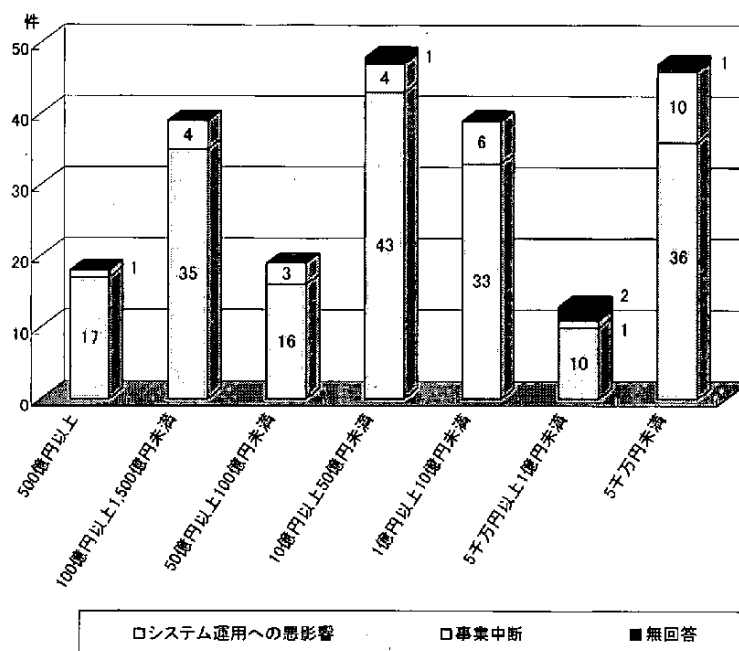


図2-2-16. 資本金規模別にみた部分的なシステムダウンの影響

Q14-①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)

(△:増加/▼:減少)

| 原因 |                                                 | H17 年度 | H15 年度 | 増減 |
|----|-------------------------------------------------|--------|--------|----|
| 1  | 自然災害(地震を除く水害等)                                  | 15     | 12     | △  |
|    |                                                 | 6.1    | 4.2    |    |
| 2  | 地震                                              | 9      | -      |    |
|    |                                                 | 3.6    |        |    |
| 3  | 火災による事故・障害                                      | 5      | 1      | △  |
|    |                                                 | 2.0    | 0.3    |    |
| 4  | 停電(電力会社に起因する障害)                                 | 35     | 28     | △  |
|    |                                                 | 14.2   | 9.7    |    |
| 5  | 電源機器・設備障害                                       | 55     | 32     | △  |
|    |                                                 | 22.3   | 11.1   |    |
| 6  | 空調等障害                                           | 17     | 14     | △  |
|    |                                                 | 6.9    | 4.9    |    |
| 7  | 通信障害(通信事業者、ISPの障害を含む)                           | 65     | 42     | △  |
|    |                                                 | 26.3   | 14.6   |    |
| 8  | ネットワーク機器などの障害                                   | 120    | 111    | △  |
|    |                                                 | 48.6   | 38.5   |    |
| 9  | サーバなどのハードウェア障害                                  | 119    | 153    | ▼  |
|    |                                                 | 48.2   | 53.1   |    |
| 10 | OS障害                                            | 40     | 32     | △  |
|    |                                                 | 16.2   | 11.1   |    |
| 11 | アプリケーションソフトウェア障害                                | 103    | 73     | △  |
|    |                                                 | 41.7   | 25.3   |    |
| 12 | コンピュータウイルス、スパイウェア(ウイルスによる不正侵入・ネットワーク障害を含む)による障害 | 29     | 69     | ▼  |
|    |                                                 | 11.7   | 24.0   |    |
| 13 | 不正アクセスや DOS 攻撃によるサービス中断                         | 9      | -      |    |
|    |                                                 | 3.6    |        |    |
| 14 | 人の悪意(たとえば内部犯罪、不正侵入)による事故等                       | 4      | 0      | △  |
|    |                                                 | 1.6    | 0.0    |    |
| 15 | オペミス等、人の過失による事故等                                | 79     | 51     | △  |
|    |                                                 | 32.0   | 17.7   |    |
| 16 | その他                                             | 6      | 4      | △  |
|    |                                                 | 2.4    | 1.4    |    |
| 17 | 無回答                                             | 3      | 5      |    |
|    |                                                 | 1.2    | 1.7    |    |

今回調査では、前回調査に比べ一部選択項目を詳細にした。前回調査に比べると、ほとんどの項目でシステムダウンが増加している。

項目別にみると、特に「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、平成 13 年調査では 98.2%、前回調査では 91.6%、今回調査でも 96.8%と全体の中で突出しており、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と考えられ、ネットワークやシステム全体としての信頼性の向上が依然として難しいことがわかる。

ただし、前回調査では「ハードウェア障害」は 38.5%、「ネットワーク機器障害」は 53.1%と、ネットワーク機器の方が多かったのに対し、今回調査では、それぞれ 48.2%、48.6%となっており、ほとんど差がみられなかった。ネットワーク機器の信頼性が上がったとは言いきれないが、改善されていると考えられる。いずれにしても、今後、事業体ではオフィス内でのネットワーク利用がより重要となるなかで、障害の少ないネットワーク機器やシステムの開発が望まれるといえよう。

前回調査との大きな違いはコンピュータウイルス関連である。「コンピュータウイルス、スパイウェア障害」については、平成 13 年度 15.7%、前回調査 24.0%とトップ 4 に入っていたものが、今回調査では 11.7%と大きく減少し、順位を下げた（第 9 位）。これまでは事業体においてインターネットや電子メール、Web 等の利用が進むことによって、ウイルス対策が無視できない脅威となってきたからである。今回調査では、この項目にはウイルスのみならず、スパイウェアなども含めている。また、平成 17 年 5 月には、有力なウイルス対策ソフトウェアベンダが誤った対策ソフトを配布したため、多くの事業者のパソコンが動作不能となる事件が発生したことが報道されている。

このような背景から、分析者らは、ウイルス関連が大きくなるのではと予測していた。しかし、調査結果からは前回、13 年度調査に比べ、システムダウンなどの大きな問題に繋がるケースはむしろ減っていることがわかる。すなわち、ウイルスについてはユーザ側の認識が高まり、また、対策ソフトウェアも一般的となっているため、ウイルスなどが事業体の大きなシステムダウンに繋がるリスクは少なくなっていると考えられる。

一方、「OS 障害」は、前回調査では 11.1%であったものが、今回調査では 16.2%と増加している。また、「ソフトウェア障害」については、今回調査では「アプリケーションソフトウェア障害」と内容を限定したにもかかわらず、前回調査（25.3%）から 41.7%に増加し、トップ 4 となった。

「OS 障害」、「アプリケーションソフトウェア障害」ともに、この数年ソフトウェアバグに起因する問題があり、OS では Windows 2000 や XP などのパッチが定期的に配布されている。同様に、Web 関係のソフトウェアパッケージでもソフトウェアバグが不正侵入に繋がるなどの脆弱性が指摘されている。すなわち、OS やソフトウェアは、平成 15 年以降、セキュリティホールを攻撃するウイルスや不正侵入が注目され、ベンダも対策としてソフトウェア修正パッチを配布するようになった。ところが、このパッチを適用するとソフトウェアが動作しないという問題がクローズアップされるようになった。最悪の場合、パッチを適用するとシステムが動作しないということも起きており、パッチをあてなければウイルス障害の脅威がある、という状況になった。この部分の本質的な解決策はないが、今後、OS や Web

などのプラットフォームの機能とアプリケーションの境界をできる限り分け、お互いに影響しなくなるような工夫が問われよう。

「通信事業者に起因する障害」については、前回調査が4.6%であったのに対し、今回調査では26.3%に倍増している。この理由として考えられるのは、前回調査では「ISP等社外のインターネットに起因する障害」を個別の項目として集計していたことである。この項目が前回調査では8.7%であったので、合計すると23.3%となる。したがって、前回調査の数値としては23.3%が今回調査の26.3%に相当すると考えられる。したがって、3ポイント増加したことになる。この増加の原因としては、事業体の多くが今までの専用回線からIP-VPNや広域イーサなどの付加価値の高いサービスにシフトしていることである。これらのサービスは、既存の専用回線に比べると大容量で安価であるが、高度になった分、信頼性などの懸念がある。その反映として今回の調査結果にみられるシステムダウンが数ポイント増加したと考えられる。今後、通信はより広帯域、高速性が望まれ、ますますイーサなどのプロトコルを利用するようになり、レイヤ1のみの専用線に比べると信頼性に対するユーザ側の工夫も必要になる。

なお、その他の原因として「自然災害」が平成11年度の12.9%、13年度の7.0%、前回調査4.2%と連続して減少した。今回調査では9.7%（「地震を除く風水害」が6.1%、「地震」が3.6%）であり、平成16年に台風、地震、雪害など自然災害の発生が多かったことを考えると、妥当な数字と考えられる。今後とも自然災害に対する障害を軽視することは難しく、十分な対策は必須である。

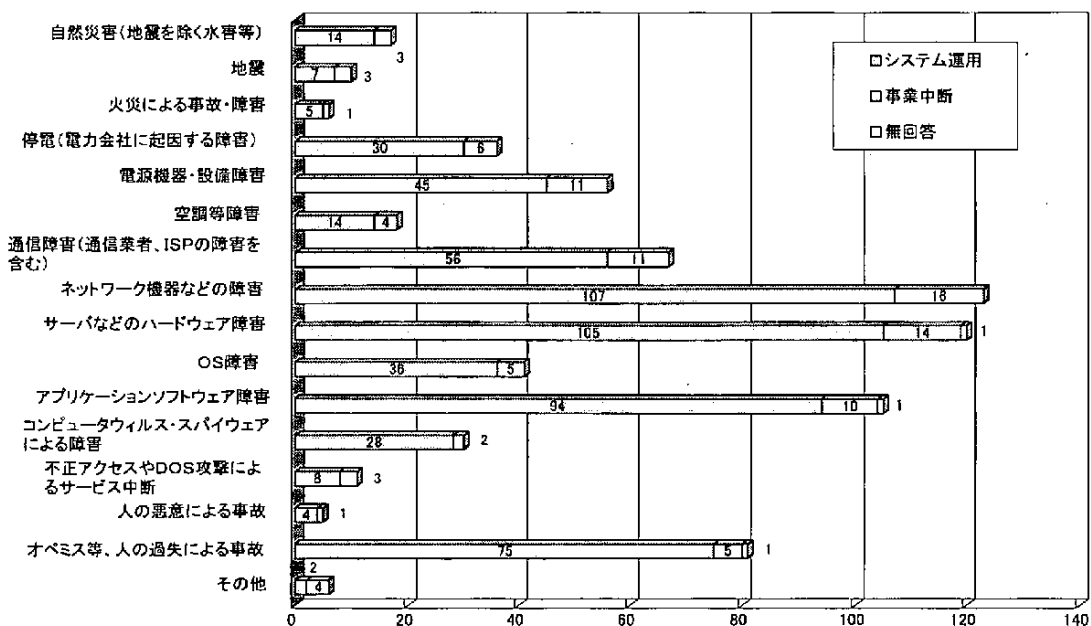
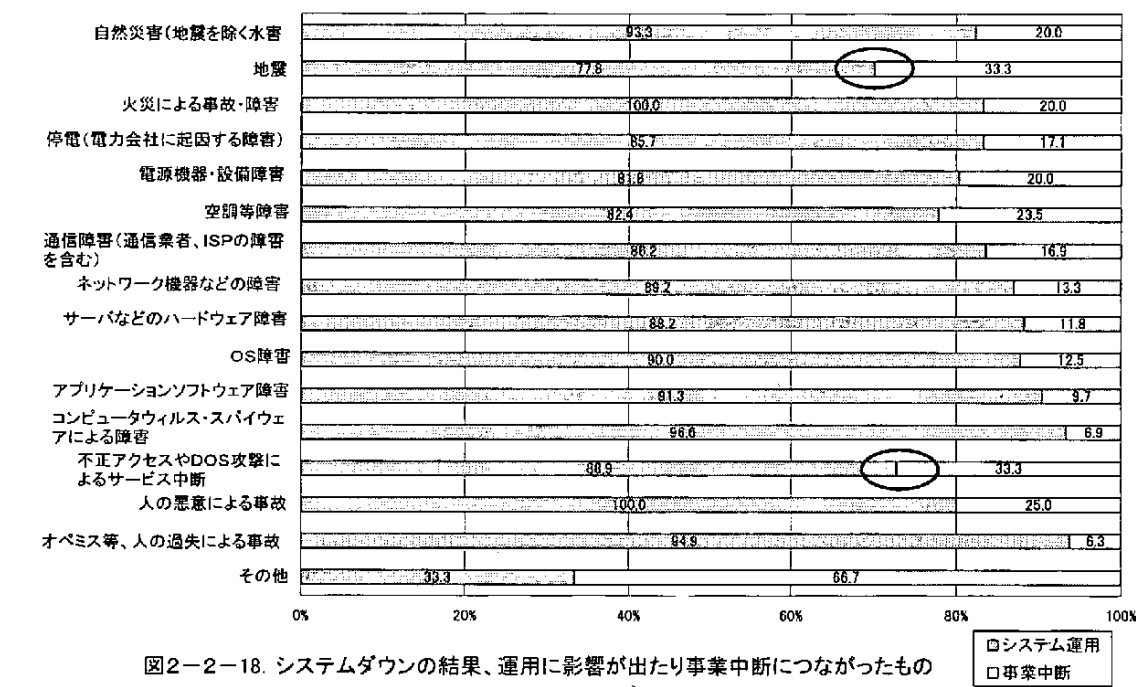


図2-2-17. システムへの影響度合い

Q14-②システムダウンの結果、「システム運用への悪影響」(事業中断には至っていない)、または「事業中断」にまで至りましたか。(複数回答)

| ①システムダウンの原因<br>回答件数:247 件 |                                                 |      | ②システムへの影響度合い |      |     |
|---------------------------|-------------------------------------------------|------|--------------|------|-----|
|                           |                                                 |      | システム<br>運用   | 事業中断 | 無回答 |
| 1                         | 自然災害(地震を除く水害等)                                  | 15   | 14           | 3    | 0   |
|                           |                                                 | 6.1  | 93.3         | 20.0 | 0.0 |
| 2                         | 地震                                              | 9    | 7            | 3    | 0   |
|                           |                                                 | 3.6  | 77.8         | 33.3 | 0.0 |
| 3                         | 火災による事故・障害                                      | 5    | 5            | 1    | 0   |
|                           |                                                 | 2.0  | 100.0        | 20.0 | 0.0 |
| 4                         | 停電(電力会社に起因する障害)                                 | 35   | 30           | 6    | 0   |
|                           |                                                 | 14.2 | 85.7         | 17.1 | 0.0 |
| 5                         | 電源機器・設備障害                                       | 55   | 45           | 11   | 0   |
|                           |                                                 | 22.3 | 81.8         | 20.0 | 0.0 |
| 6                         | 空調等障害                                           | 17   | 14           | 4    | 0   |
|                           |                                                 | 6.9  | 82.4         | 23.5 | 0.0 |
| 7                         | 通信障害(通信事業者、ISPの障害を含む)                           | 65   | 56           | 11   | 0   |
|                           |                                                 | 26.3 | 86.2         | 16.9 | 0.0 |
| 8                         | ネットワーク機器などの障害                                   | 120  | 107          | 16   | 0   |
|                           |                                                 | 48.6 | 89.2         | 13.3 | 0.0 |
| 9                         | サーバなどのハードウェア障害                                  | 119  | 105          | 14   | 1   |
|                           |                                                 | 48.2 | 88.2         | 11.8 | 0.8 |
| 10                        | OS障害                                            | 40   | 36           | 5    | 0   |
|                           |                                                 | 16.2 | 90.0         | 12.5 | 0.0 |
| 11                        | アプリケーションソフトウェア障害                                | 103  | 94           | 10   | 1   |
|                           |                                                 | 41.7 | 91.3         | 9.7  | 1.0 |
| 12                        | コンピュータウイルス、スパイウェア(ウイルスによる不正侵入・ネットワーク障害を含む)による障害 | 29   | 28           | 2    | 0   |
|                           |                                                 | 11.7 | 96.6         | 6.9  | 0.0 |
| 13                        | 不正アクセスや DOS 攻撃によるサービス中断                         | 9    | 8            | 3    | 0   |
|                           |                                                 | 3.6  | 88.9         | 33.3 | 0.0 |
| 14                        | 人の悪意(たとえば内部犯罪、不正侵入)による事故等                       | 4    | 4            | 1    | 0   |
|                           |                                                 | 1.6  | 100.0        | 25.0 | 0.0 |
| 15                        | オペミス等、人の過失による事故等                                | 79   | 75           | 5    | 1   |
|                           |                                                 | 32.0 | 94.9         | 6.3  | 1.3 |
| 16                        | その他                                             | 6    | 2            | 4    | 0   |
|                           |                                                 | 2.4  | 33.3         | 66.7 | 0.0 |
| 17                        | 無回答                                             | 3    |              |      |     |
|                           |                                                 | 1.2  |              |      |     |

システムダウンの結果、「システム運用への悪影響」（事業中断には至っていない）、または「事業中断」にまで至るかをみると、今回調査でとりあげた原因のほとんどで「事業中断」につながる割合が2割前後となっている。割合が高いのは「地震」や「不正アクセスやDOS 攻撃によるサービス中断」で、33.3%である。「不正アクセスやDOS 攻撃によるサービス中断」で事業中断する場合、たとえば、平成17年5月の価格比較サイト大手「価格.com」のWeb サイトが不正アクセスにより一時閉鎖に追い込まれた事件が例にあげられる。この事件は「価格.com」サイトにSQL インジェクション攻撃などで不正侵入して、ウイルス「trojandownloader.small.AAO」「PSW.Delf.FZ」をインストールしてしまう Web サイトに誘導する仕掛けがなされた。そのため、「価格.com」では、原因究明が終わるまで事業を中断させられた。このような新しいリスクが顕著になってきている。



Q15. 基幹システムにおけるMTBF(平均故障間隔)は何時間ですか。

(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 時間稼働中に 1 回ダウンした場合 ⇒ (365 日 × 24H) / (1 回 + 1) = 4,380 時間

|          |                        |
|----------|------------------------|
| 4,273 時間 | (回答件数 514 件/無回答 153 件) |
|----------|------------------------|

平成13年調査の2,938.7時間、前回調査の2,773.3時間に比べ、MTBFは若干長くなっており、信頼性の向上がみられる。この傾向はQ14で述べたハードウェア故障やネットワーク機器などの障害でシステムダウンが増えていることと矛盾するように思える。今回のMTBFの数値から、日本の情報システムは平均的に1年間に1回程度のダウンが発生しているといえよう。

ただし、分布をみると3,000時間から5,000時間が最も大きくなっている。次のピークは5,000時間から10,000時間と2,000時間から3,000時間であり、隣り合っている。前回

調査では典型的な指数分布であったが、今回調査では 200 時間未満の分布があり、指数分布とは必ずしもいえない。すなわち、図中の 200 時間未満に大きな出現があることから、短時間でダウンしている不安定なシステムと、MTBF が 4,400 時間以上の比較的安定しているシステムに二分化されているといえよう。

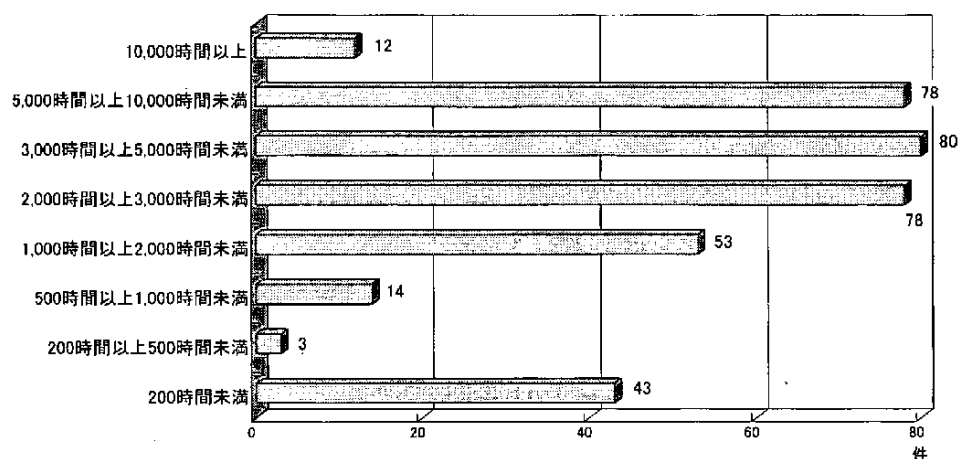


図2-2-19. 基幹システムにおけるMTBF

資本金規模と MTBF の関係をみると、前回調査の分析では、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、という結果が出ていた。今回調査でも、資本金が大きくなるにつれて MTBF が長くなる特徴がみられる。すなわち、規模の大きい事業体ほど信頼性対策が実施されていることがわかる。ただし、「500 億超」の大企業は「100 億円以上 500 億円未満」より高くない。また、「5,000 万未満」の事業体も MTBF が 4,000 時間を超えているなど、資本金との関係が明確でなくなりつつある。すなわち、インターネットやブロードバンドの普及によって情報システムの依存度が事業体規模によらないケース（中小規模の事業体でもインターネットによる売買を中心とする場合は、高信頼なサーバやネットワーク機器などの設備投資をするなど）が増えてきていると考えられる。

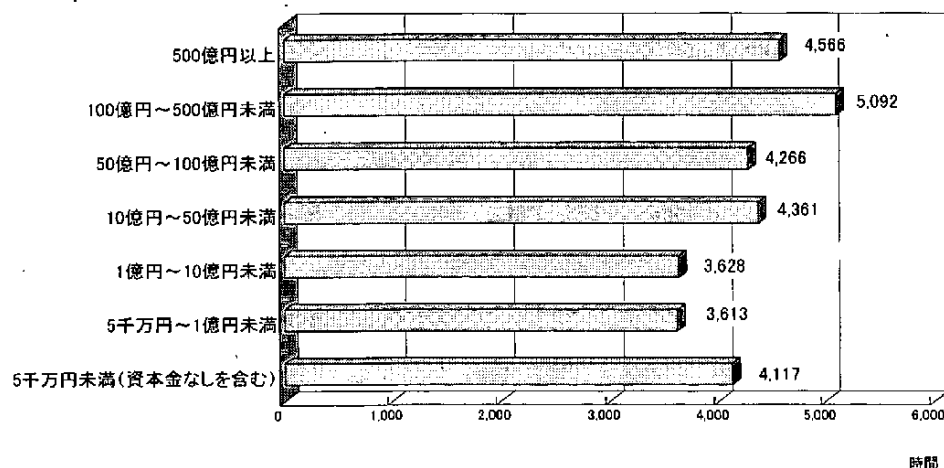


図2-2-20. 基幹システムMTBF(資本金規模別 平均時間)

Q16. 基幹システムにおけるMTTR(平均修理時間)は何分ですか。

|         |                        |
|---------|------------------------|
| 130.0 分 | (回答件数 514 件/無回答 174 件) |
|---------|------------------------|

基幹システムの故障修理に時間を示す MTTR (短いものがよい) は平成 13 年度の 145.7 分に比べると短い、前回調査の 120.0 分に比べると 10 分長くなっている。前回調査まで短くなる傾向が続いてきたが、今回でこの傾向が止まった。

MTTR が一貫して短くなってきた原因としては、今まで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。すなわち、修理の場合、コンポーネントごとに取り替える形態の修理が増えてきたこと、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と説明してきた。しかし、今回調査でこの数値が上昇したことから、修理の際に時間がかかる新しい要因が発生したと考えるべきである。(前回までは回答数が 100 件を下回っていたが、今回は有効回答数が 170 件と増加したのもこの傾向が止まった原因かもしれない。)

MTTR の分布は、1 時間以上 2 時間未満にピークがあり、2 時間以上 4 時間未満がこれに続いている。また、10 分以下の頻度も高い。すなわち、10 分程度の簡単な修理の場合と数時間程度の修理の場合に二分化している。

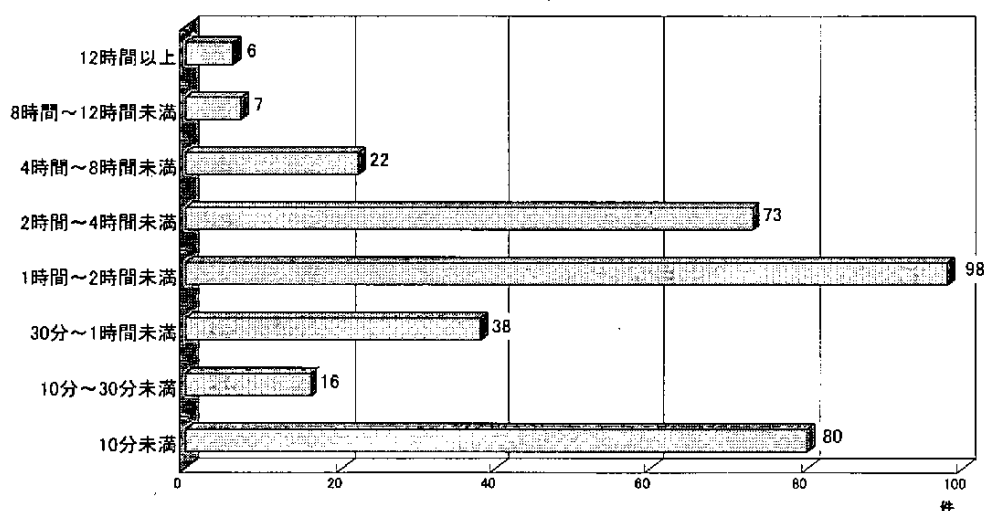


図2-2-21. 基幹システムにおけるMTTR(平均修理時間)

MTTR が減少した理由として考えられるのは、最近の情報システムでは OS 障害などのときには、復旧には OS の再インストールのみならず、セキュリティなどのシステム的环境設定や OS のパッチ適用などが必要になっていることである。また、システムのディスク要領が大規模化 (最近のパソコンでも 100 ギガバイトを越えるディスクを内蔵している) しているので、バックアップからのデータリカバリを行う場合に数時間を要するようになっている。すなわち、ハードウェア、ソフトウェアの大規模化の進展が、部品化やコンポーネント化の効果を打ち消しつつあることが原因と考えられる。

次に事業規模と MTTR の関係を見ると、前回調査では事業規模として資本金規模で MTTR の関係を分析し、資本金の大きい事業体ほど MTTR が短く、資本金の小さい事業体ほど MTTR が長い傾向であることを述べた。しかし、今回調査では資本金規模と MTTR に大きな関係性は認められないことがわかった。前述の MTBF の分析で述べたように、資本金の大きい事業体ほど故障復旧に対して対応できるとは言い切れないことがわかる。すなわち、技術的な制約などで、修理については資本とは無関係な要因によっていることがわかる。

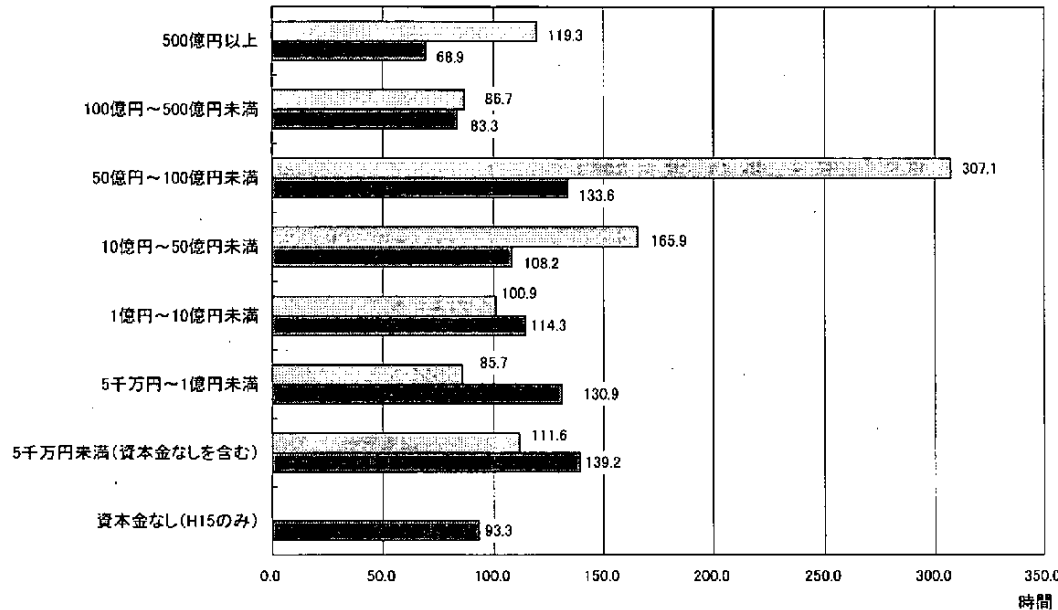


図2-2-22. 基幹システムにおけるMTTR(資本金規模別 平均時間)

Q17. 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               | 市販のソフトを<br>コピーして使う |       | データ、プログラ<br>ムを無断で使う |       | データを<br>盗み見る |       |
|-----------------------|--------------------|-------|---------------------|-------|--------------|-------|
|                       | 11                 | 2.1   | 17                  | 3.3   | 14           | 2.7   |
| 特に問題ではない              | 11                 | 2.1   | 17                  | 3.3   | 14           | 2.7   |
| 企業内で戒告・訓告・注意処分等の対象となる | 148                | 28.8  | 216                 | 42.0  | 238          | 46.3  |
| 企業内で懲戒免職の対象となる        | 25                 | 4.9   | 73                  | 14.2  | 85           | 16.5  |
| 犯罪行為である(刑法上の処罰の対象となる) | 288                | 56.0  | 161                 | 31.3  | 123          | 23.9  |
| わからない                 | 28                 | 5.4   | 30                  | 5.8   | 39           | 7.6   |
| 無回答                   | 10                 | 1.9   | 12                  | 2.3   | 11           | 2.1   |
| 複数回答                  | 4                  | 0.8   | 5                   | 1.0   | 4            | 0.8   |
| 計                     | 514                | 100.0 | 514                 | 100.0 | 514          | 100.0 |

『市販のソフトのコピー使用』に対しては、この数年で急速に「犯罪である」との見方が定着してきている。平成11年度には、「犯罪である」が54.2%、13年度は69.9%、前回調査では59.8%となった。今回は、「犯罪行為である(刑法上の処罰の対象となる)」が56.0%となっており、前回調査とほぼ同様の割合となった。また、「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」が前回調査で18.5%であったのに対し、今回調査では33.7%にまで増加している。なお、今回調査では、犯罪性の認識が高まってきたことから、前回までの「問題である」という中途半端な設問項目を削除している。すなわち、事業体も犯罪行為であるとして、厳罰に処する姿勢が定着したといえよう。これは、最近の事業体のコンプライアンス重視による成果ともいえよう。

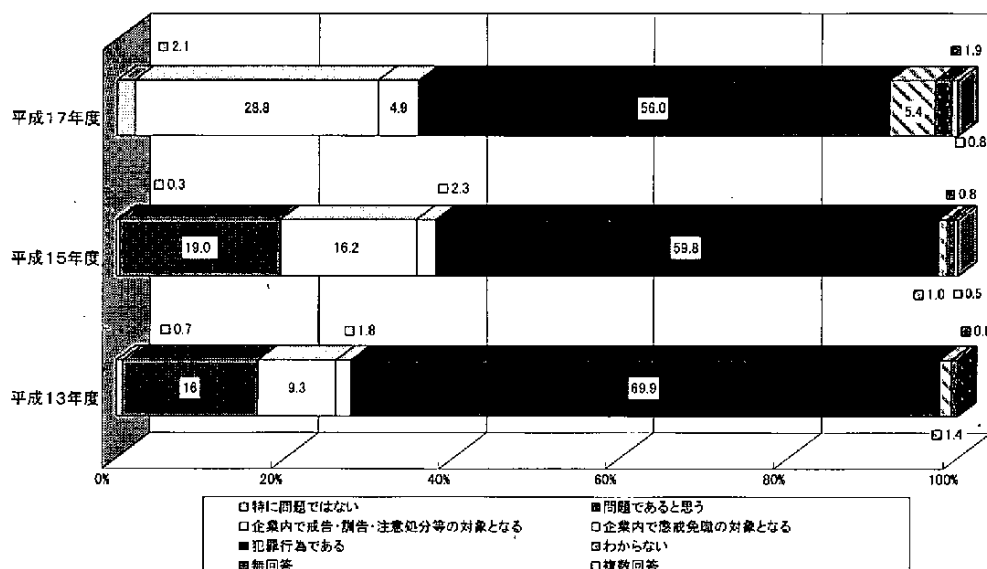


図2-2-23. 市販のソフトをコピーして使用

業種グループ別にみると、前回調査まで業種による明確な差異はみられなかった。今回調査では、「犯罪行為である」のみにピークがある業種と、「犯罪行為である」と「企業内で戒告・訓告・注意処分等の対象となる」の2つにピークがある業種とが分かれた。前者では、「商業」、「政府・地方公共団体」、「公共サービス業」であり、後者では、「食品・紙・パルプ・繊維・印刷」、「金融・保険業」、「情報処理サービス業」となっている。これは、事業体のおかれた性格にもよるが、コンプライアンスが厳しく問われている現実がわかる。

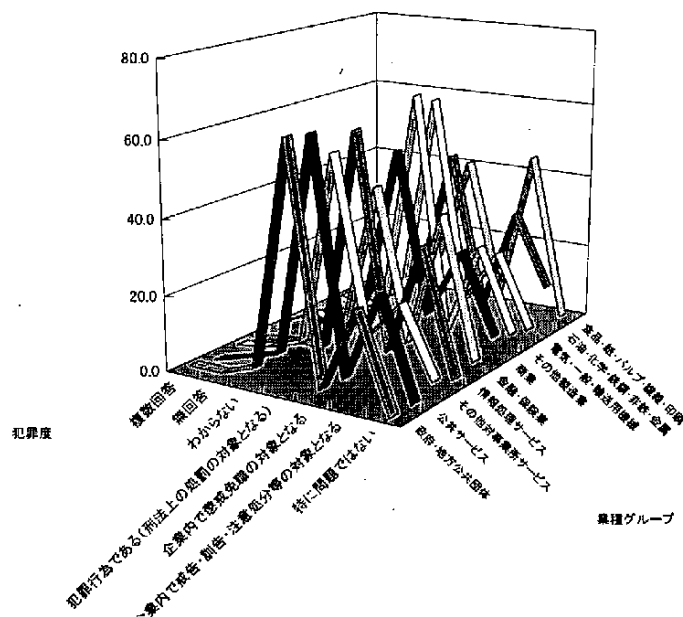


図2-2-24. 市販のソフトをコピーして使う(業種グループとの関連)

事業体規模別（資本金、従業員数別）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、「企業内で戒告・訓告・注意処分等の対象となる」が増えている。この傾向は前回調査とあまり変わっていない。事業体として従業員を犯罪者扱いしたくないとの考えであろう。一方、大規模な事業体では、犯罪として扱うことで襟を正していると考えられる。

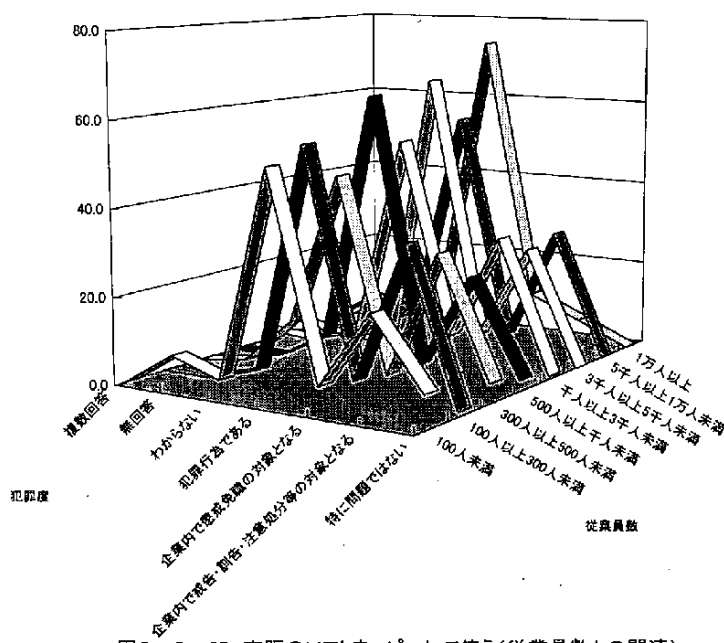


図2-2-25. 市販のソフトをコピーして使う(従業員数との関連)

『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使用』に比べるとまだ犯罪との意識は低く「問題ない」が3.3%である。しかし、「企業内でも戒告・訓告・注意処分」が42.0%、「企業内で懲戒免職の対象となる」14.2%、「犯罪行為である」が31.3%となっており、これらを合計すると87.5%となり、違反行為との認識が定着してきている。

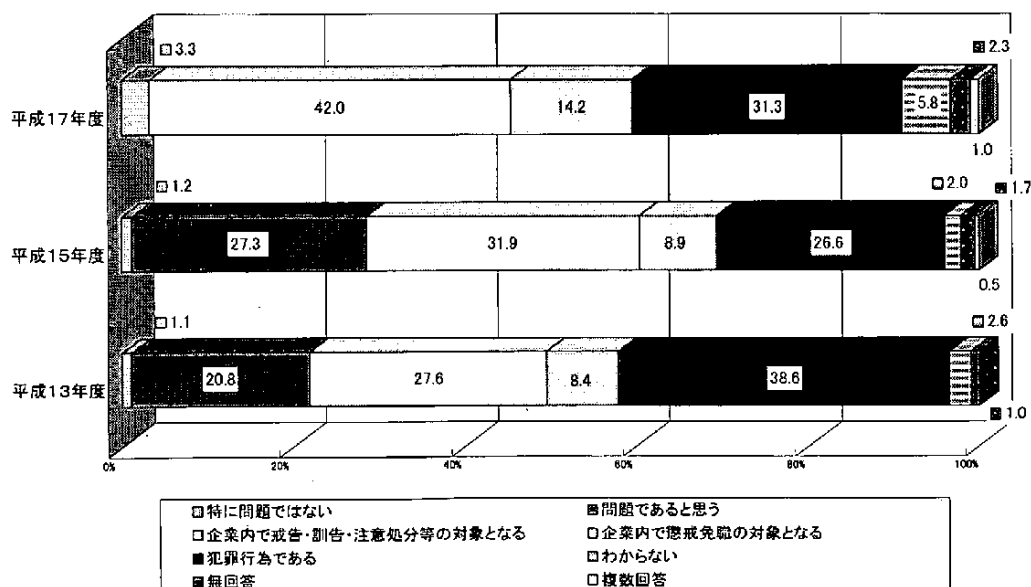


図2-2-26. データ、プログラムの無断使用

業種グループ別にみると「公共サービス業」、「政府・地方公共団体」、「情報処理サービス業」が「犯罪行為」という点で意識改革が進んでいる。その他の産業では「企業内でも戒告・訓告・注意処分」が多い。今後、個人情報保護法や会社法の改正などで情報の管理が厳しくなる中で、「犯罪行為」という認識が全産業に広がっていくものと考えられる。

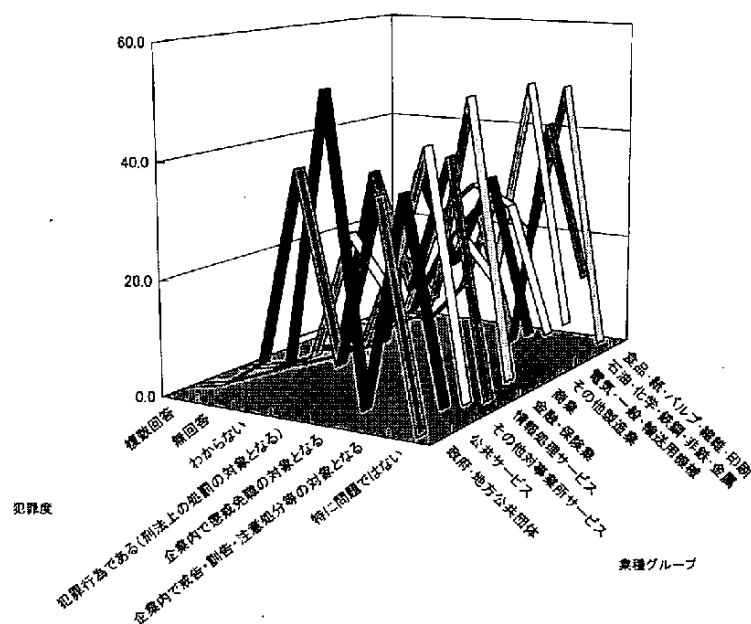


図2-2-27. データ、プログラムを無断で使う(業種グループとの関連)

事業体規模別にみると、『市販ソフトのコピー使用』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よりも企業内の懲戒の法が強いことがわかる。すなわち、犯罪という認識に欠けている。

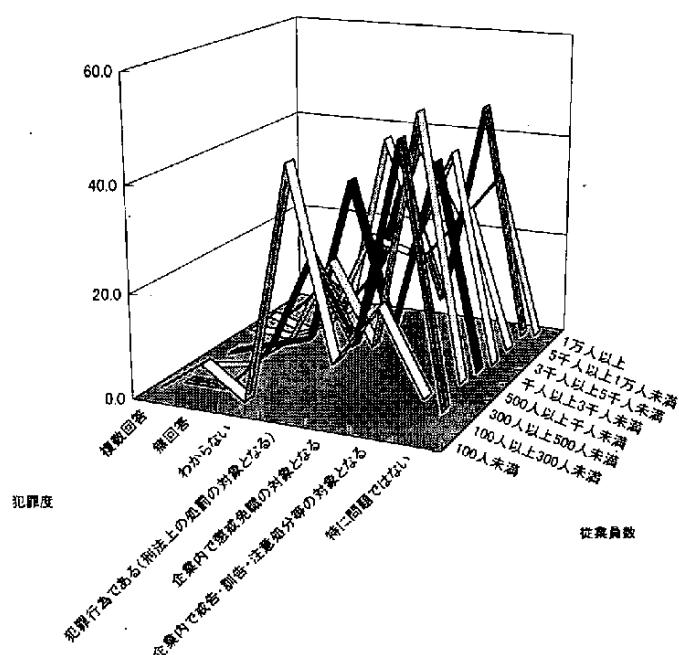


図2-2-28. データ、プログラムを無断で使う(従業員数との関連)

『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16.5%であったが、今回は約7ポイント増えて23.9%となったが、『市販ソフトのコピー使用』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高くない。

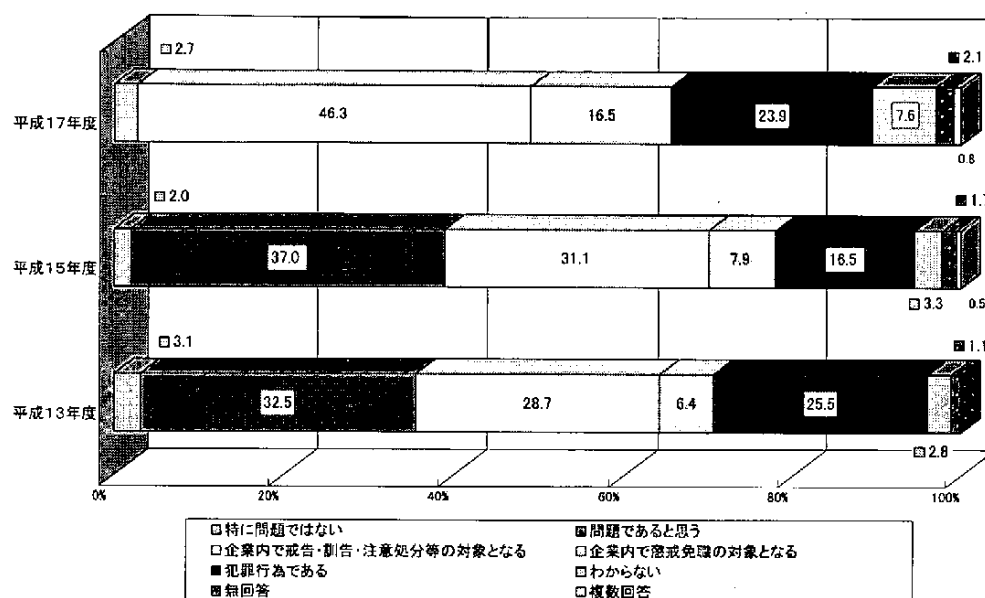


図2-2-29. データ、プログラムを覗き見る

業種グループ別にみると、ほとんどの業種で「企業内で戒告・訓告・注意処分等の対象となる」が高い。前回「情報処理サービス業」では「犯罪行為」としていたのは21.6%であったが、今回調査では32.1%に増加している。また、「政府・地方公共団体」は22.2%から31.3%に増加している。

事業体規模との関係は、『市販ソフトのコピー使用』、『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。

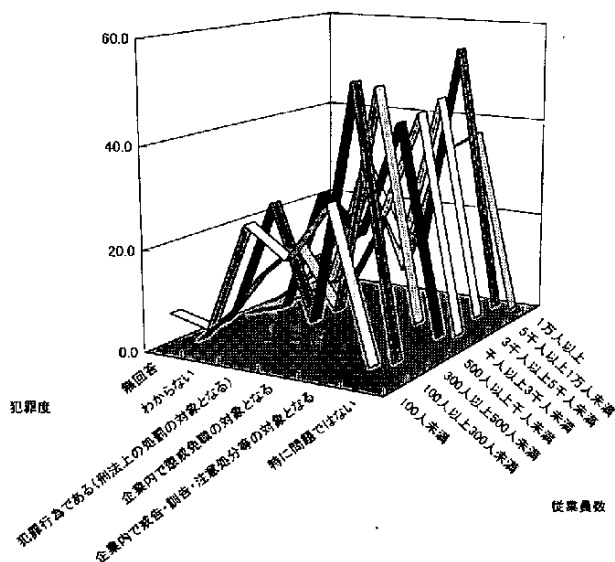


図2-2-30. データを盗み見る(従業員数との関連)

| 行 為 項 目               | 就業時間内に会社のコンピュータを私的な目的に使う |       | 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 |       | 私的な電子メールを送受信する |       |
|-----------------------|--------------------------|-------|-----------------------------------|-------|----------------|-------|
| 特に問題ではない              | 52                       | 10.1  | 70                                | 13.6  | 96             | 18.7  |
| 企業内で戒告・訓告・注意処分等の対象となる | 368                      | 71.6  | 352                               | 68.5  | 330            | 64.2  |
| 企業内で懲戒免職の対象となる        | 45                       | 8.8   | 41                                | 8.0   | 29             | 5.6   |
| 犯罪行為である（刑法上の処罰の対象となる） | 12                       | 2.3   | 8                                 | 1.6   | 7              | 1.4   |
| わからない                 | 23                       | 4.5   | 28                                | 5.4   | 37             | 7.2   |
| 無回答                   | 12                       | 2.3   | 13                                | 2.5   | 12             | 2.3   |
| 複数回答                  | 2                        | 0.4   | 2                                 | 0.4   | 3              | 0.6   |
| 計                     | 514                      | 100.0 | 514                               | 100.0 | 514            | 100.0 |

『就業時間内に会社のコンピュータを私的な目的に使う』、『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』、『私的な電子メールを送受信する』の3項目はいずれも事業体でのコンピュータの私的な利用についての設問である。なお、今回調査では前述のとおり、「問題である」という中途半端な設問項目を削除しているため、前回よりも「問題ではない」との回答が増えている。したがって、今回の調査では前回までの「問題ではない」とは違う意味合いで回答している可能性もあることから、単純な差異の比較に止める。

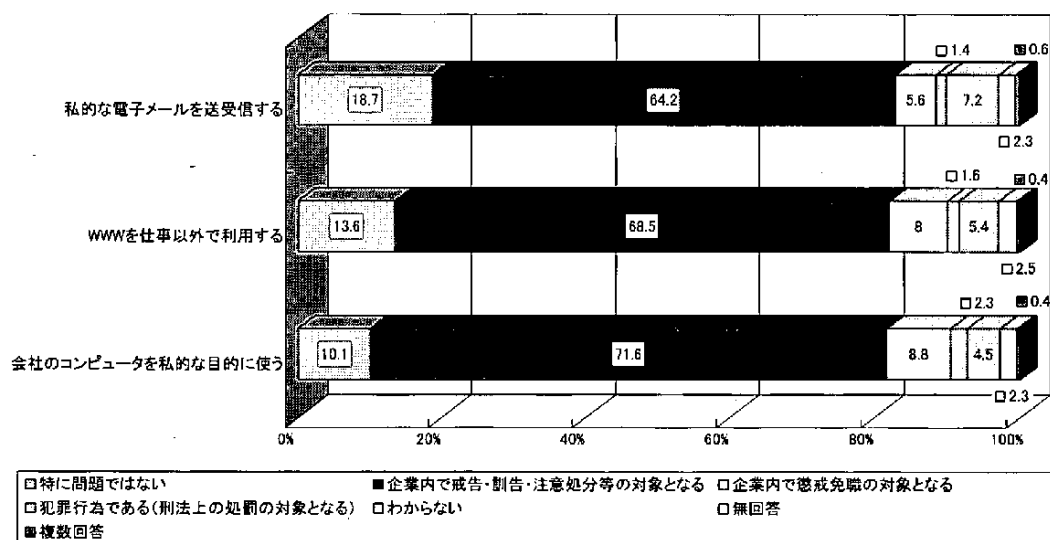


図2-2-31. コンピュータの私的な利用について

『会社のコンピュータを私用に使う』行為に対して、「問題ではない」が10.1%となっており、「企業内で戒告・訓告・注意処分等の対象となる」、「企業内で懲戒免職の対象となる」、「犯罪行為である」を合計した認識は82.7%となっている。「企業内での戒告・訓告・注意処分等の対象となる」が44.0%から71.6%へと大幅に増加した。ただし、前回調査で「問題である」に答えた層（44.6%）がすべて「懲戒」に答えたと考えると、88.6%となり、今回調査の71.6%と比べるとそれほど増加したともいえない。いずれにせよ、会社のコンピュー

タを使用に使うことは、「会社の資産の不正使用」という意識が高まってきたものと思われる。この点で、今後とも組織内での教育が重要と考えられる。

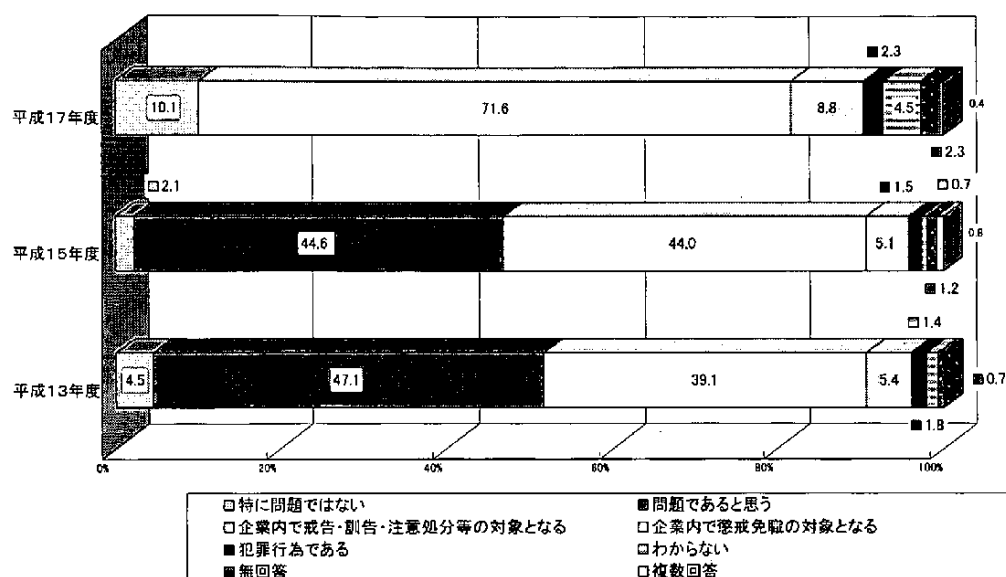


図2-2-32. 就業時間内にコンピュータを私的な目的で使う

業種グループ別にみると、ほとんどの業種で「企業内で戒告・訓告・注意処分等の対象となる」が最も高くなっている。情報処理サービス業では、コンピュータそのものが付加価値創造のツールであるためか、「企業内で戒告・訓告・注意処分等の対象となる」が75.3%となっており、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。

事業体規模別（資本金、従業員数）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。この傾向は前回調査と共通した点でもある。今後とも組織内での教育が重要と考えられる。

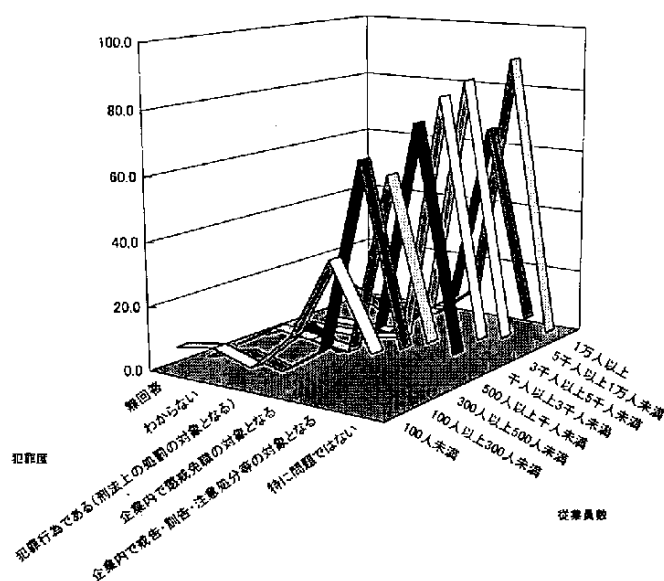


図2-2-33. 就業時間内に会社のコンピュータを私的な目的に使う(従業員数との関連)

『WWWを仕事以外（個人目的での発注、アンケート回答等）で利用する』行為について、「問題ではない」が13.6%となっており、「企業内で戒告・訓告・注意処分等の対象となる」、「企業内で懲戒免職の対象となる」、「犯罪行為である」を合計した認識は78.1%（H15:44.7%）となっている。ただし、前回調査の「問題である」に答えた層（50.1%）がすべて「懲戒」に答えたと考え、前回の合計値は94.8%となり、今回調査（78.1%）よりも高い。すなわち、前回調査で「問題がある」と考えた層は、一部が「問題がない」と答えているものと考えられる。いずれにせよ、7割近くが、会社のコンピュータを使用に使うことは「会社の資産の不正使用」と考える意識が高まってきたものと思われる。この点で、今後とも組織内での教育が重要と考えられる。

特にWWWを利用して従業員が勤務時間内にネット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、多くの事業体が勤務怠慢と問題視している。これに対しては、ファイアウォールなどで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ー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。

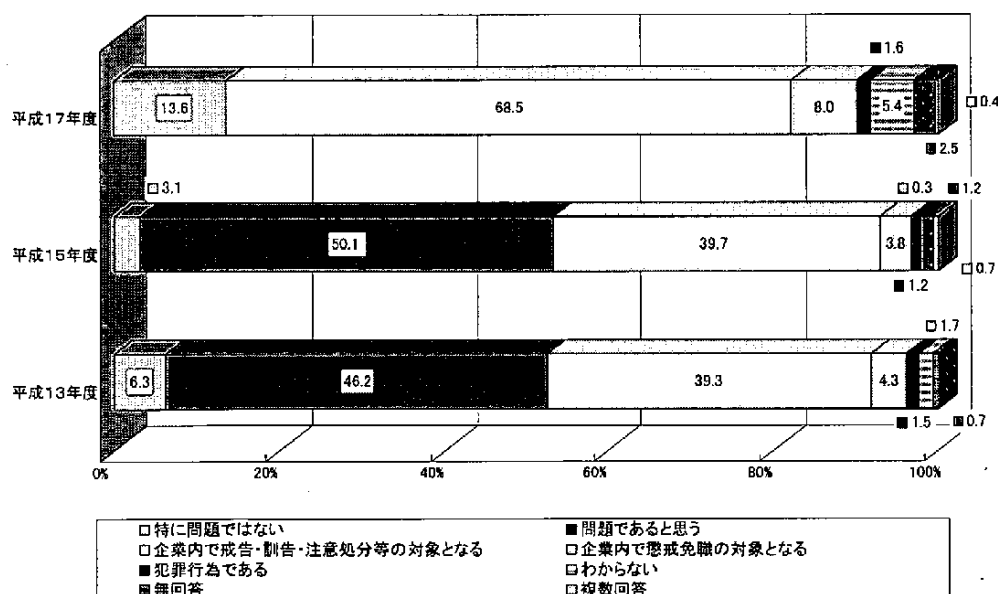


図2-2-34. WWWを仕事以外で利用する

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差は出ていない。

『私的な電子メールを送受信する』行為について、「問題ではない」と考える事業体が18.7%となっており、「企業内で戒告・訓告・注意処分等の対象となる」、「企業内で懲戒免職の対象となる」、「犯罪行為である（刑法上の処罰の対象となる）」を合計した認識は71.2%となっている。ただし、前回調査で「問題である」に答えた層（52.7%）がすべて「懲戒」に答えたと考え、前回の合計値は92.4%となり、今回調査よりも高い。すなわち、前回調

査で「問題がある」と考えた層は、一部が「問題がない」と答えているものと考えられる。いずれにせよ、7割近くが私的な電子メールを仕事以外に使うことは「会社の資産の不正使用」と考える意識が高まってきたものと思われる。私的メールは組織の重要な情報漏えいを引き起こしたり、また、労働生産性を低下させたりすることから、多くの事業体が制限するようになって考えられる。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も考えられる。

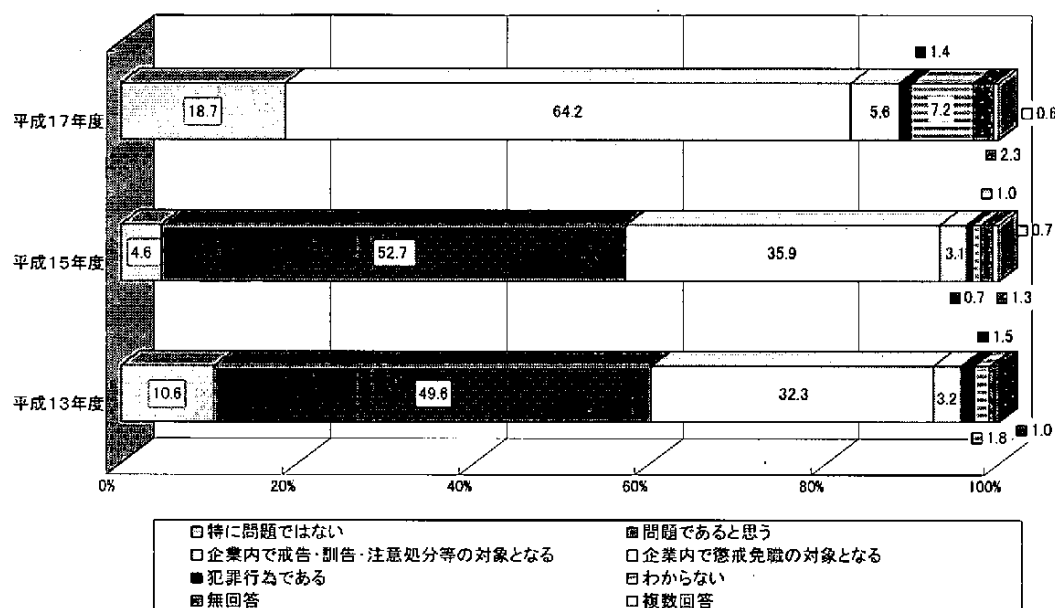


図2-2-35. 私的目的のための電子メール送・受信

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。

| 行 為 項 目               | 他人の ID を無断借用する |       |
|-----------------------|----------------|-------|
| 特に問題ではない              | 12             | 2.3   |
| 企業内で戒告・訓告・注意処分等の対象となる | 258            | 50.2  |
| 企業内で懲戒免職の対象となる        | 103            | 20.0  |
| 犯罪行為である(刑法上の処罰の対象となる) | 99             | 19.3  |
| わからない                 | 29             | 5.6   |
| 無回答                   | 10             | 1.9   |
| 複数回答                  | 3              | 0.6   |
| 計                     | 514            | 100.0 |

『他人の ID の無断使用』に対しては「問題ではない」と考える事業体が 2.3%であり、前回調査の 0.3%から若干増加した。「企業内で戒告・訓告・注意処分等の対象となる」、「企業内で懲戒免職の対象となる」、「犯罪行為である」を合計した認識は 89.5%となっている。ただ

し、前回調査で「問題である」に答えた層（21.8%）がすべて「懲戒」に答えたと考えると、前回調査の合計値は 96.6% となり、今回調査よりも高い。すなわち、前回調査で「問題がある」と考えた層は、一部が「問題がない」と答えているものと考えられる。いずれにせよ、9割近くが他人のIDの無断使用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使用』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。これは事業体ではグループで仕事をしていることが多く、グループでIDを利用するなどの実態があり、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。今後は事業体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。

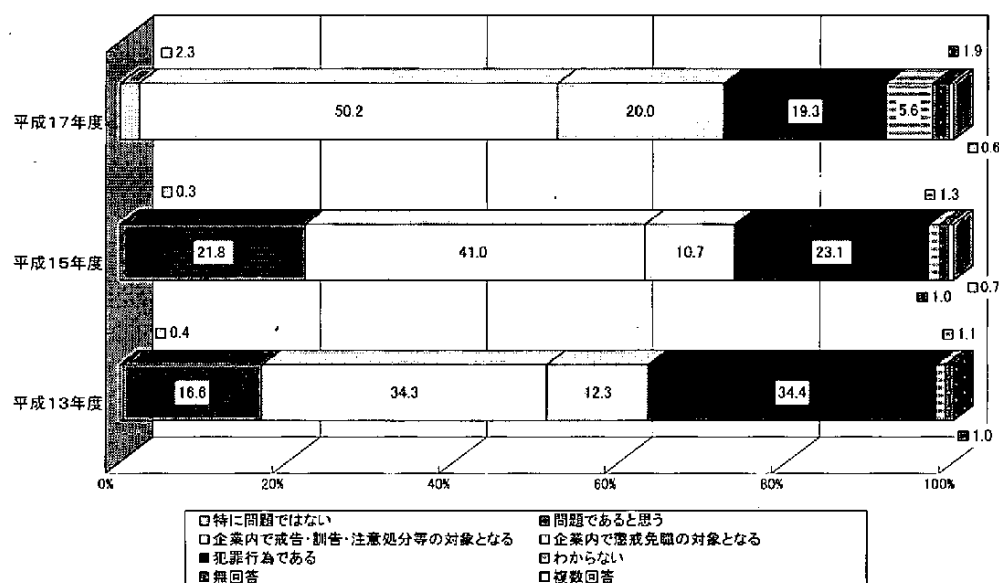


図2-2-36. 他人のIDを無断借用する

従業員数別にみると、従業員数1万人以上の事業体と3,000人以上5,000人未満の規模の事業体で「犯罪行為」との意識が高い（31.7%）。その他の事業体では、「企業内での戒告・訓告・注意処分等の対象」が50%以上となっている。

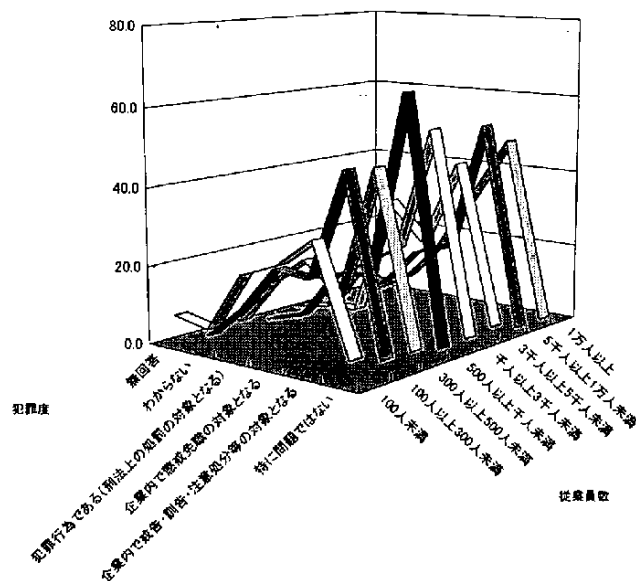


図2-2-37. 他人のIDを無断借用する(従業員数との関連)

## 2.3 情報セキュリティポリシー・管理・対策について

Q18. 情報セキュリティの確保にとり、基本的に重要な要素は何だと思いますか。(複数回答)

| 回答件数                 | 514 | —    |
|----------------------|-----|------|
| 1 経営者層の理解            | 391 | 76.1 |
| 2 管理者の理解             | 242 | 47.1 |
| 3 担当者の理解             | 205 | 39.9 |
| 4 社内全体の理解(エンドユーザを含む) | 429 | 83.5 |
| 5 社内規定やルールの整備        | 303 | 58.9 |
| 6 その他                | 13  | 2.5  |
| 無回答                  | 2   | 0.4  |

情報セキュリティの確保にとり基本的に重要な要素として、「社内全体の理解(エンドユーザを含む)」(83.5%)が最も高い割合で、前回調査(85.5%)と同様の結果となった。しかし、前回は若干下回っており、「経営者層の理解」が76.1%と前回の71.2%を若干上回っている。

産業別にみると、「第二次産業」、「第三次産業」も同様の傾向で、「社内全体の理解」が高い割合を示している。

これは、実際の問題として、情報セキュリティの確保には全従業員の共通認識と協力が必要なことはあるが、直接的に全従業員の共通認識と協力を得ることはなかなか難しく、やはり経営者層の理解を得て経営者層の積極的なリーダーシップにより、社内の情報セキュリティを確保することが一番効果的であるとの考え方が強くなってきている結果であろう。

また、昨今のさまざまなシステムトラブルなどをみても、情報セキュリティに関して経営者層の役割の重要性が認識されてきているものと思われる。

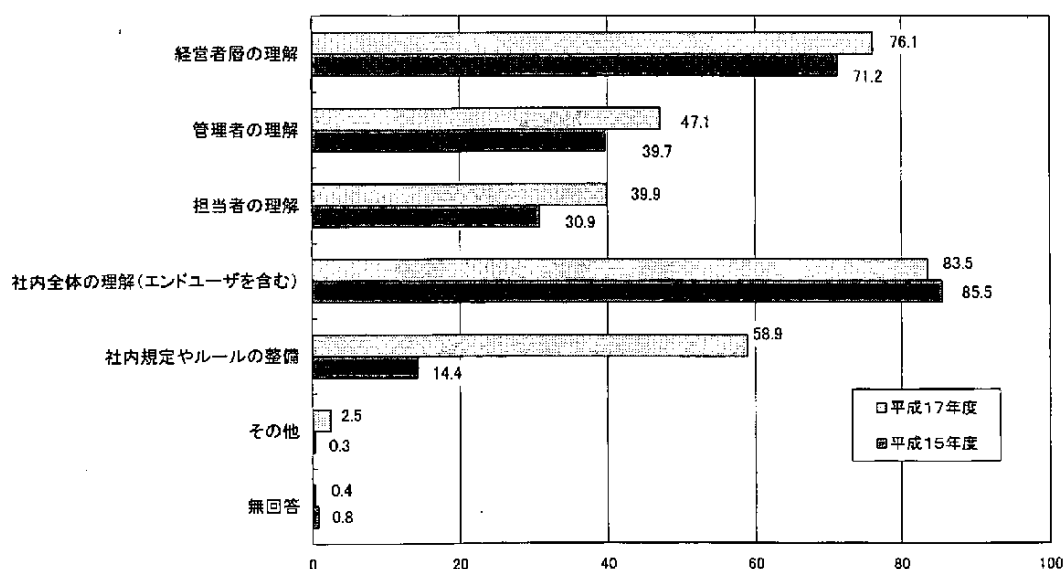


図2-3-1. 情報セキュリティ確保のための基本的重要な視点

| 産業        | 重要要素 | 経営者の理解 | 管理者の理解 | 担当者の理解 | 社内全体の理解 | 社内規定の整備 | その他 |
|-----------|------|--------|--------|--------|---------|---------|-----|
| 第二次産業     |      | 73.8   | 41.5   | 32.2   | 81.4    | 56.3    | 2.7 |
| 第三次産業     |      | 80.5   | 46.2   | 40.2   | 82.7    | 59.0    | 2.3 |
| 政府・地方公共団体 |      | 64.1   | 65.6   | 59.4   | 92.2    | 65.6    | 3.1 |

産業別でみると「社内全体の理解」の回答は「政府・地方公共団体」が高い割合を占めている。

「第二次産業」、「第三次産業」とも「社内全体の理解」、「経営者の理解」の割合が高く、他の要素との差が大きい、「政府・地方公共団体」は「社内全体の理解」のみが高く、それ以外の要素に大きな差はみられない。

| 資本金               | 社内全体の理解 | 経営者層の理解 |
|-------------------|---------|---------|
| 500 億円以上          | 86.4    | 84.1    |
| 100 億円以上 500 億円未満 | 85.1    | 83.0    |
| 50 億円以上 100 億円未満  | 88.6    | 74.3    |
| 10 億円以上 50 億円未満   | 77.2    | 72.8    |
| 1 億円以上 10 億円未満    | 87.2    | 74.5    |
| 5 千万円以上 1 億円未満    | 68.8    | 78.1    |
| 5 千万円未満(資本金なしを含む) | 85.4    | 71.5    |

資本金規模別にみると、規模の大小に関わらず「社内全体の理解」が高い割合となっている。次いで「経営者層の理解」が続いているが、その差はあまり大きくなく、経営者層の理解に対する期待がますます強くなってきているものと思われ、経営者層のリーダーシップに期待したいところである。

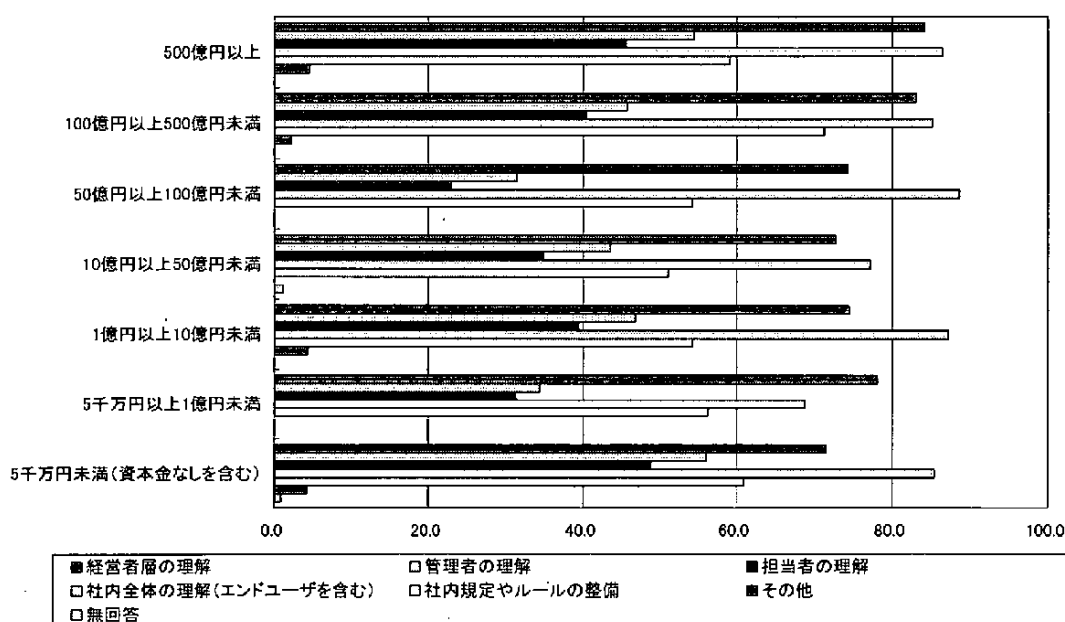


図2-3-2. 情報セキュリティ確保のための基本的重要な視点(資本金規模別)

| 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        | 84.2    | 94.7    | 42.1   |
| 5千人以上1万人未満   | 97.4    | 78.9    | 52.6   |
| 3千人以上5千人未満   | 87.8    | 70.7    | 56.1   |
| 千人以上3千人未満    | 85.2    | 77.3    | 51.6   |
| 500人以上千人未満   | 82.1    | 74.4    | 48.7   |
| 300人以上500人未満 | 86.4    | 72.7    | 40.9   |
| 100人以上300人未満 | 83.7    | 77.2    | 40.2   |
| 100人未満       | 63.5    | 73.1    | 44.2   |

従業員数別にみても「社内全体の理解」が高い割合であるが、従業員「1万人以上」の事業体では「経営者層の理解」が「社内全体の理解」を上回っている。組織が大きくなると経営者層の強力なリーダーシップなくしては全社的な問題は解決しないということであろう。

「100人未満」の事業体も「社内全体の理解」より「経営者層の理解」が上回っているが、これは従業員数の規模が小さい事業体では経営者層の考え方が全従業員に浸透しやすく、経営者層の認識に影響される度合いが強い結果であろう。

一方、「管理者の理解」に対する割合が比較的低いが、これは情報セキュリティの確保について管理者層への役割・期待が明確でなく、重要性が低いとの認識であると考えられるが、やはり管理者層は組織の要であり、組織全体への影響が大きいため、経営者層と同じように管理者層の理解も十分高める必要があるだろう。

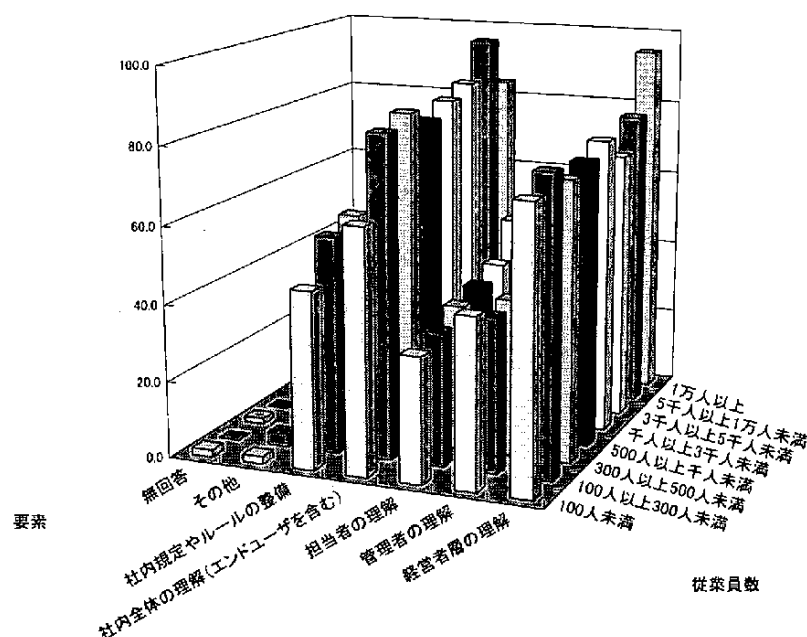


図2-3-3. 情報セキュリティ確保のための基本的な重要要素(従業員規模別)

Q19. 貴事業体では、情報セキュリティ対策(不正アクセス対策、コンピュータウイルス対策、信頼性対策、個人情報保護対策、情報セキュリティ監査、システム監査等)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)

|      |                        |
|------|------------------------|
| 7.7% | (回答件数:514 件/無回答:167 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7.7%と前回調査の6.1%を上回り、情報セキュリティ対策にかかる費用が年々増加傾向を表しているものと思われる。

| 産業        | 情報セキュリティ対策費 平均(%) |      |
|-----------|-------------------|------|
|           | 今回調査              | 前回調査 |
| 第二次産業     | 6.5               | 5.4  |
| 第三次産業     | 9.4               | 6.8  |
| 政府・地方公共団体 | 4.1               | 6.1  |

産業別にみると、「第三次産業」が最も高く、「第二次産業」がこれに続いている。前回調査では「政府・地方公共団体」が6.1%、「第二次産業」が5.4%であったが、今回調査では「第二次産業」が「政府・地方公共団体」を2.4ポイント上回っている。

第二次産業も情報セキュリティ対策に投資することが事業体の発展にとって必要との認識が強まった結果であると同時に、情報セキュリティ対策費をきちんと把握する傾向が増えてきているものと思われる。

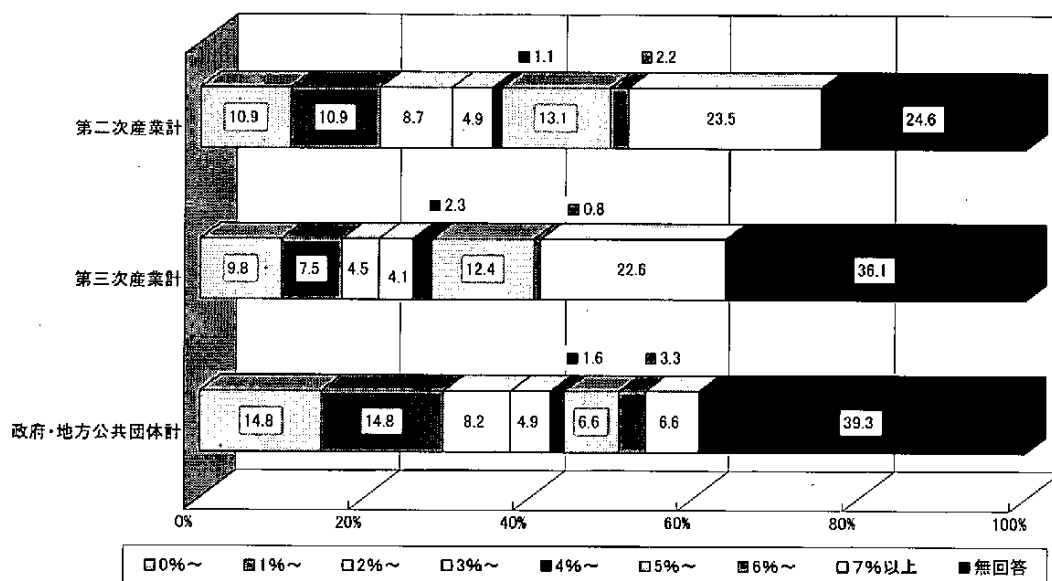


図2-3-4. 情報セキュリティ対策への情報システム関連支出の割合

情報システム関連支出のなかでの情報セキュリティ対策に対する支出の割合は年々増加傾向にあるが、今回調査で「無回答」が32.5%と比較的高いのが気にかかる。どのような支出が情報セキュリティ対策の費用かを明確に判断することは難しいことであり、また、事業体にとって情報システム全体に対する情報セキュリティ対策費が何パーセントが適切かの判断に苦しむ面もあるが、情報セキュリティ対策費としてどの程度支出されているか、その内容は適切かを把握しておくことが情報セキュリティを強化していくうえでも必要であろう。

情報セキュリティ対策費は「護り」のための費用と考えがちであるが、これは、むしろ「攻め」のための費用として捉えるべきと考える。

| 産業        | 無回答  |
|-----------|------|
| 第二次産業     | 24.6 |
| 第三次産業     | 36.1 |
| 政府・地方公共団体 | 40.6 |

産業別にみると、「無回答」は、「政府・地方公共団体」の割合が高く、「第三次産業」がこれに続いている、情報セキュリティ対策費の把握が難しい現状であろうか。

| 資本金               | 無回答  | 情報セキュリティ対策費 平均(%) |
|-------------------|------|-------------------|
| 500 億円以上          | 45.5 | 6.3               |
| 100 億円以上 500 億円未満 | 33.0 | 5.3               |
| 50 億円以上 100 億円未満  | 25.7 | 7.6               |
| 10 億円以上 50 億円未満   | 25.0 | 9.3               |
| 1億円以上 10 億円未満     | 29.8 | 9.8               |
| 5 千万円以上 1億円未満     | 21.9 | 12.6              |
| 5 千万円未満           | 39.8 | 5.0               |

資本金規模別でみると、「500 億円以上」の事業体の無回答率が一番高い。また、情報セキュリティ対策費の割合は「5 千万円以上 1 億円未満」の事業体が高くなっており、情報セキュリティ対策費の割合が高いポイントを示している事業体は無回答の割合が低い傾向にある。

Q20. 以下の管理について、責任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   |       |
|--------------|-------|------|-----------|-----|--------|-----|------|-----|-----|-----|-----|-------|
| ①ネットワークの管理   | 457   | 88.9 | 22        | 4.3 | 30     | 5.8 | 2    | 0.4 | 3   | 0.6 | 514 | 100.0 |
| ②情報システムの管理   | 455   | 88.5 | 19        | 3.7 | 33     | 6.4 | 2    | 0.4 | 5   | 1.0 | 514 | 100.0 |
| ③情報セキュリティの管理 | 413   | 80.4 | 49        | 9.5 | 45     | 8.8 | 4    | 0.8 | 3   | 0.6 | 514 | 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、“責任を有する担当者”について質問したが、今回は単に“責任者”とした。

ネットワーク管理者について、「定めている」が88.9%で、平成11年の76.4%、平成13年の79.2%、前回調査の83.3%から増加傾向にある。これに「検討している」(4.3%↙H15:6.1%、約1.8ポイント減)をあわせると、93.2%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5.8%であり、前回調査の9.8%から4ポイント減となっている。ほとんどの事業体では、パソコンや情報システムをネットワーク環境下で用いるとともに、電子メールやグループウェアを利用したり、インターネットによる電子取引やWebによる情報収

集などに利用したりしている。これらの環境を適切に運用するために、ネットワーク管理を重視していることがわかる。

情報システムの管理者については、「定めている」、「検討している」ともにネットワーク管理者とほぼ同様の趨勢となっている。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92.2%となる。平成11年度から前回調査までは減少傾向にあったが、今回は増加した。これは、ネットワーク管理が広くなる中で、情報システムの管理を分けないと十分に管理しきれないことから増加していると考えられる。

情報セキュリティ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89.9%と、11年度の36.3%、13年度の75.6%、前回調査の80.0%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9.6%と、前回調査の19.2%から大きく減少した。前回調査からの変動の理由として、個人情報保護法で管理者を決めることが謳われていることも一因と考えられる。また、企業会計審議会が検討している“日本版SOX法”への対応などで情報セキュリティに対する専門家が必要になってきていること、さらに、昨今のインターネットでの不正侵入やウイルス対策、Winnyによる情報漏えい対策など、どの事業体にとっても情報セキュリティ管理が重要な要素となっていることから、今後も情報セキュリティ責任者を設置する事業体が増加するものと考えられる。

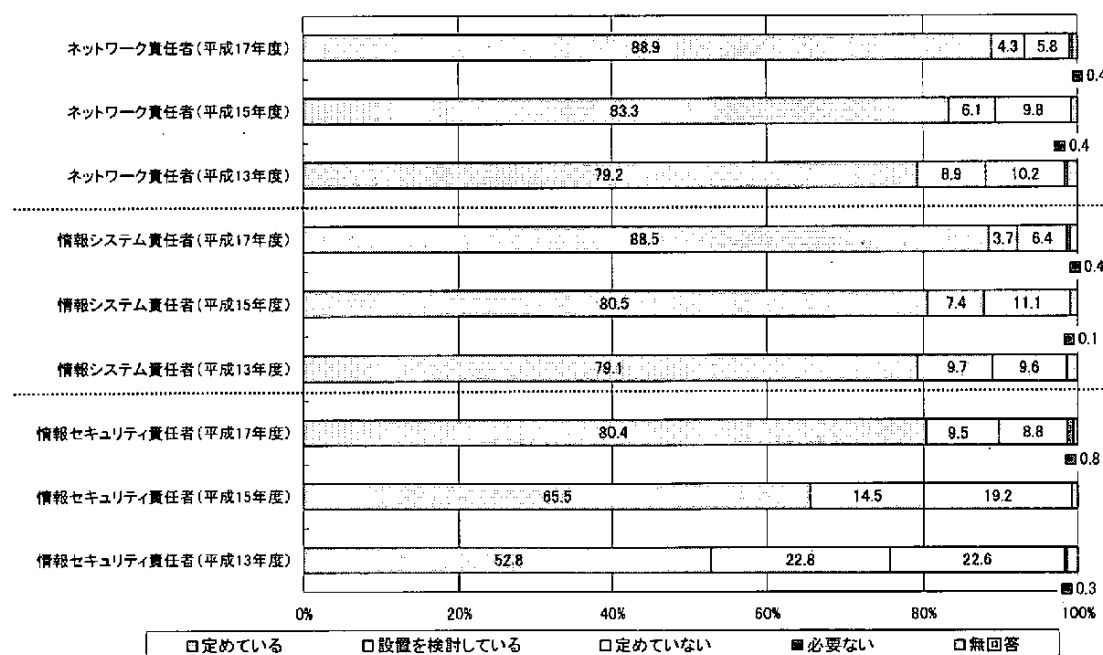


図2-3-5. 責任者の設置状況

ネットワーク責任者、情報システム責任者、情報セキュリティ責任者の有無について、資本規模別にみると、規模が大きい事業体は肯定的な回答が高く、規模が小さくなるにつれ「定めている」、「検討している」の割合が低くなっていく。「500億円以上」では「定めている」、「検討している」の合計が100%となっている。なお、「5,000万円以上1億未満」と「5,000万円未満」

で責任者の設置状況が逆となっている。これは、IT を利用するベンチャーなどの企業は、企業規模よりも事業を適切に進めるため、責任者を設置しているためと考えられる。

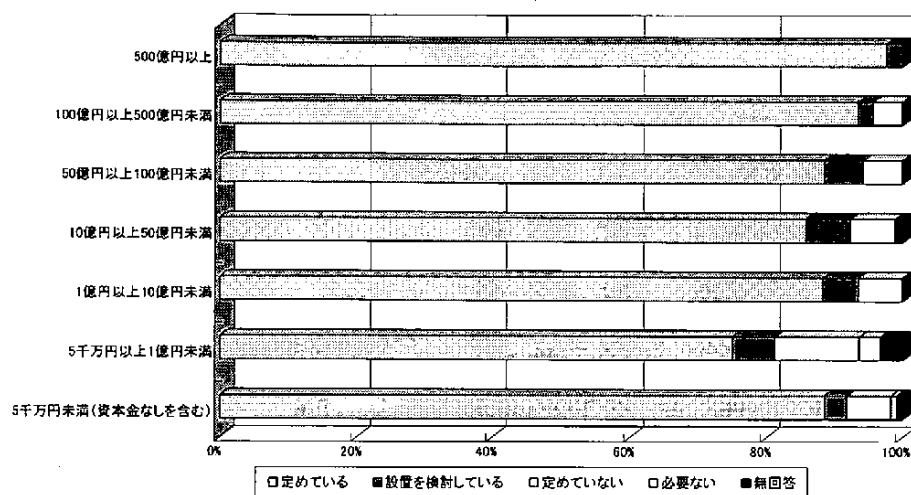


図2-3-6. ネットワーク管理者と資本金規模の関係

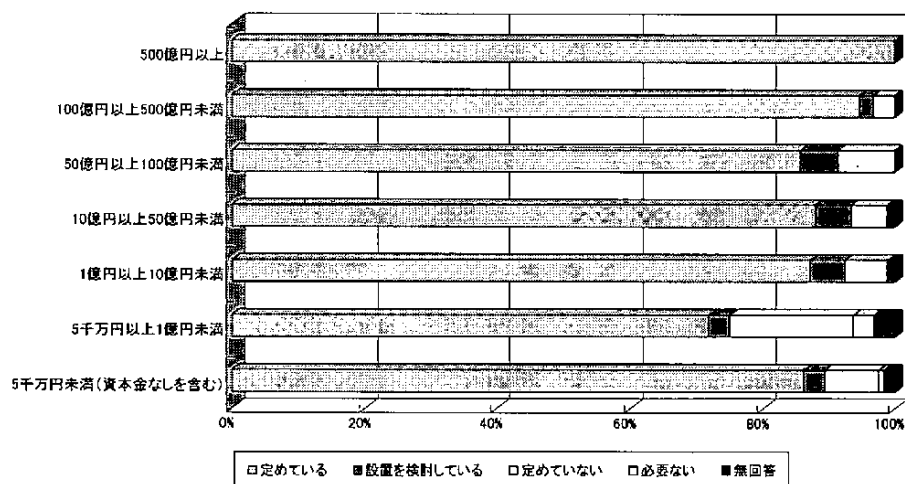


図2-3-7. 情報システム管理者と資本金規模の関係

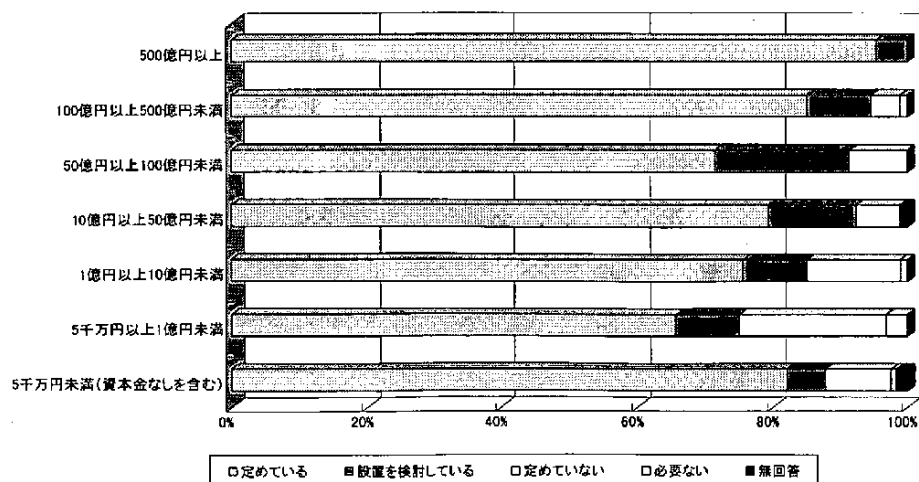


図2-3-8. 情報セキュリティ責任者と資本金規模の関係

Q21. 情報セキュリティ(システム災害／障害、不正アクセス、コンピュータウイルスを含む)管理についての問題点は何ですか。(複数回答)

| 回答件数 |                                | 514 | -    |
|------|--------------------------------|-----|------|
| 1    | 経営者層の理解が得られない                  | 86  | 16.7 |
| 2    | コストがかかりすぎる                     | 322 | 62.6 |
| 3    | 専門要員がない(要員が確保できない)             | 226 | 44.0 |
| 4    | 組織の従業員に対する負担がかかりすぎる            | 139 | 27.0 |
| 5    | 組織の従業員に対する教育・訓練がいきとどかない        | 268 | 52.1 |
| 6    | ノウハウが不足している                    | 151 | 29.4 |
| 7    | どこまでやればよいのか基準が示されていない          | 216 | 42.0 |
| 8    | 要求に合致するもの(サービス／製品)がない          | 27  | 5.3  |
| 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 | 97  | 18.9 |
| 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      | 7   | 1.4  |
| 11   | その他                            | 6   | 1.2  |
| 12   | 特に問題はない                        | 10  | 1.9  |
| 無回答  |                                | 2   | 0.4  |

情報セキュリティ管理の問題点について、「コストがかかりすぎる」(62.6%)が前回調査の53.6%から9.0ポイント増加し、第1位となった。前回1位の「組織の従業員に対する教育・訓練がいきとどかない」(52.1%)は前回の54.5%から2.4ポイント減少して2位となったが、以前高い問題意識として認識されている。この2点は平成11年度調査から常に上位2つの地位を占めている。第3位は前回同様「専門要員がない」(44.0%→H15:43.0%)である。

今回第1位となった「コストがかかりすぎる」は、平成11年度が47.9%、13年度51.9%、前回53.6%、そして今回が62.6%と増加傾向にある。これはウイルスや不正アクセスなどの被害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に加え、平成17年4月に施行された個人情報保護法対応として物理的セキュリティの導入や従業員教育、規程類の作成など、総合的に対応策を導入するためにコストをかけなければならない状況であったことを示している。

一方、「ノウハウが不足している」は34.4%から29.4%→5.0ポイント減少している。これは個人情報保護法対応については各省庁がガイドラインを示したこと、またガイドラインの普及にあわせてISMSやプライバシーマークなどの認証制度などが普及することにより、ある程度網羅的に対応策が普及したことが考えられる。

なお、「経営者層の理解が得られない」は今回16.7%で、前回調査の15.2%とほぼ同じであった。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の実施はすでに予算化などで経営者の了解を得ており、それよりも事業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。

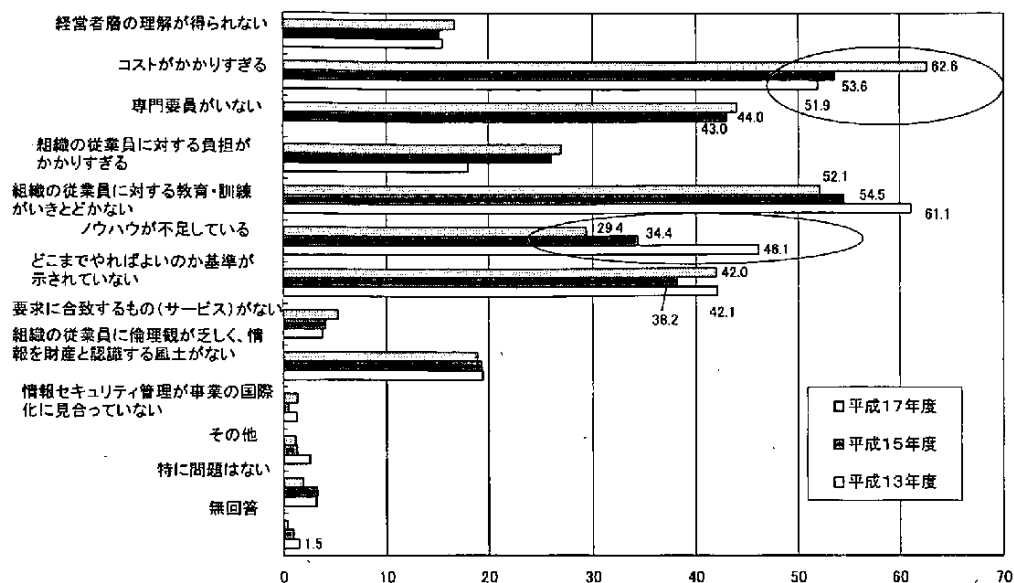


図2-3-9. 情報セキュリティ管理の問題点

業種グループ別にみると、「金融・保険業」では「経営者の理解が得られない」は7.8%と圧倒的に低く、経営者の理解は得られているものの、「どこまでやればよいのか基準が示されていない」(51.6%)ことを問題視している。「情報処理サービス業」は金融・保険業同様、「経営者の理解が得られない」は6.2%と低い、「組織の従業員に対する負担がかかりすぎる」(39.5%)ことを問題視している。「公共サービス」では「専門要員がいない(要員が確保できない)」(65.8%)と要員面で大きな課題を抱えている。また「政府・地方公共団体」では「組織の従業員に対する教育・訓練がいきとどかない」(71.9%)と教育の問題を一番の課題としている。この他、「その他製造業」では「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」(45.2%)が特異な選択として表れている。実際の理由はわからないが、背景に製造に関して情報システムへの依存度が低い、また個人情報を取り扱っていないなどの業種の特徴があるのかもしれない。このように業種によって問題となる課題に大きな特徴が表れていることがわかる。

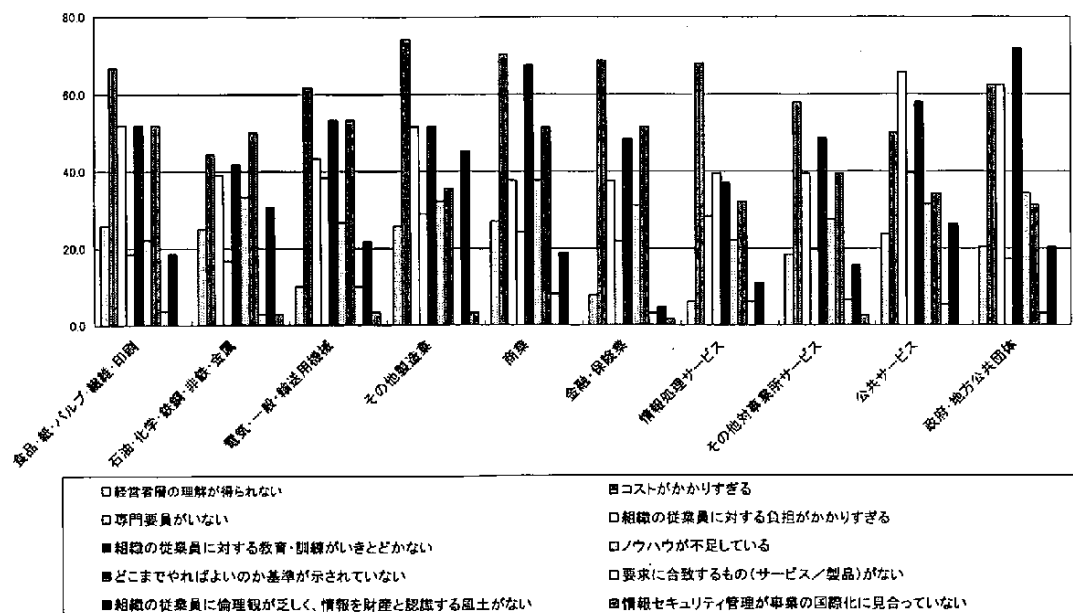


図2-3-10. 情報セキュリティ管理の問題点(業種グループ別)

資本金規模別にみると、「500億円以上」の事業体で「経営者の理解が得られない」(9.1%)が「コストがかかりすぎる」(47.7%)とともに全体の平均値よりも少なく、経営者の理解が進んでいる。「専門要員がいない」については規模が小さくなるほど問題視する割合が高くなっており、規模が小さくなるほど専門家を確保できていない状況がわかる。逆に「組織の従業員に対する負荷がかかりすぎる」は事業体規模が多いほど選択する割合が高くなり、人数が多いほど対応策に苦慮している様子がうかがえる。

Q22. 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 514 件 |                                         | 優先順位別集計 |      |     |      |    |      | 複合回答<br>としての集計<br>(503 件) |      |
|------------|-----------------------------------------|---------|------|-----|------|----|------|---------------------------|------|
| 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)                | 157     | 30.5 | 42  | 8.2  | 20 | 3.9  | 229                       | 45.5 |
| 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)         | 42      | 8.2  | 72  | 14.0 | 31 | 6.0  | 149                       | 29.6 |
| 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)    | 41      | 8.0  | 56  | 10.9 | 67 | 13.0 | 173                       | 34.4 |
| 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等)            | 102     | 19.8 | 100 | 19.5 | 85 | 16.5 | 295                       | 58.6 |
| 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等)         | 13      | 2.5  | 34  | 6.6  | 34 | 6.6  | 83                        | 16.5 |
| 6          | 通信および運用管理(ネットワークの管理、コンピュータウイルス対策、ログ管理等) | 35      | 6.8  | 61  | 11.9 | 74 | 14.4 | 176                       | 35.0 |
| 7          | アクセス制御(IDとパスワード管理、不正アクセス対策等)            | 21      | 4.1  | 53  | 10.3 | 75 | 14.6 | 155                       | 30.8 |
| 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等) | 0       | 0.0  | 8   | 1.6  | 14 | 2.7  | 23                        | 4.6  |
| 9          | 事業継続管理(災害対策、障害対策等)                      | 41      | 8.0  | 34  | 6.6  | 56 | 10.9 | 134                       | 26.6 |
| 10         | 準拠(法律遵守、システム監査等)                        | 34      | 6.6  | 25  | 4.9  | 27 | 5.3  | 87                        | 17.3 |
| 無回答        |                                         | 28      | 5.4  | 29  | 5.6  | 31 | 6.0  | -                         | -    |

(注)優先順位をつけていない回答(17件)は対象外として、無回答に含んでいる。ただし、複数回答集計には含み、有効回答件数(503件)で割合を算出している

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 項目に分類し、それについて優先順位を第3位までつけてもらった。

#### (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514件中157件、30.5%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)」103件(19.8%)を大きく引き離している。これは前回調査でも同様に「情報セキュリティポリシー」(32.9%)が1位であった。しかし過去3回の調査結果を比較すると、「情報セキュリティポリシー」は36.3%(平成11年度)から32.9%(13年度)、そして今回の30.5%とその割合がだんだん下がってきている。逆に人的セキュリティは13年度11.8%、前回の15.4%からさらに4.4ポイント増加しており、両者の差が縮小してきている。

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るが、事業体によっては経営者の理解を求める段階が過ぎ去り、予防面の実務をどう実施していくのかという点に焦点が移動してきている可能性がある。

3位以下は、「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)」42件(8.2%)、4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)」41件(8.0%)および「事業継続管理(災害対策、障害対策)」41件(8.0%)、6位「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)」35件(6.8%)となっている。

前回調査では3位が「通信および運用管理」67件(11.1%)、4位「情報セキュリティ組織」63件(10.4%)である。13年度調査では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位と3位の差が大きく開き、3位から6位までは僅差ではあるが、「通信および運用管理」が13年度12.3%、前回11.1%、そして今回が6.8%と大幅にウエイトが下がっている。従業員教育や規則の作成、リスク分析などの組織や人を中心とした実務的な要素に重きが置かれるようになっている一方で、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重要度が大幅に減少したと考えられる。また、前回6位であった「情報資産の分類および管理」が4位に入っているなど、ウイルスなどの技術的問題より、セキュリティには事業体ごとの風土体質を表す組織や従業員教育の重要性がますます高まってきているといえる。

7位以下は、7位「準拠(法令遵守、システム監査など)」34件(6.6%)、8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)」21件(4.6%)、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(2.5%)、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)」0件(0.0%)となっている。

前回調査の順番は、7位「アクセス制御」(3.6%)、8位「準拠」(3.5%)、9位「物理的および環境的セキュリティ」(2.1%)、10位「システム開発およびメンテナンス」(1.0%)であった。13年度調査の順番を参考までに掲げると、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。

7位以下を比較すると、「準拠」が前回調査でも10位から8位に順位を上げていたが、今回調査ではさらに順位を上げ7位となっており、6位の「通信および運用管理」と0.2ポイント差になっている。これは個人情報保護法の観点で法令遵守などがいわれ始めたり、また全般的に内部統制とリスクマネジメントなど日本版SOX法への対応が求められるなど、監査の重要性が少しずつ浸透してきた可能性がある。また「システム開発およびメンテナンス」の選択が初めてゼロとなった。

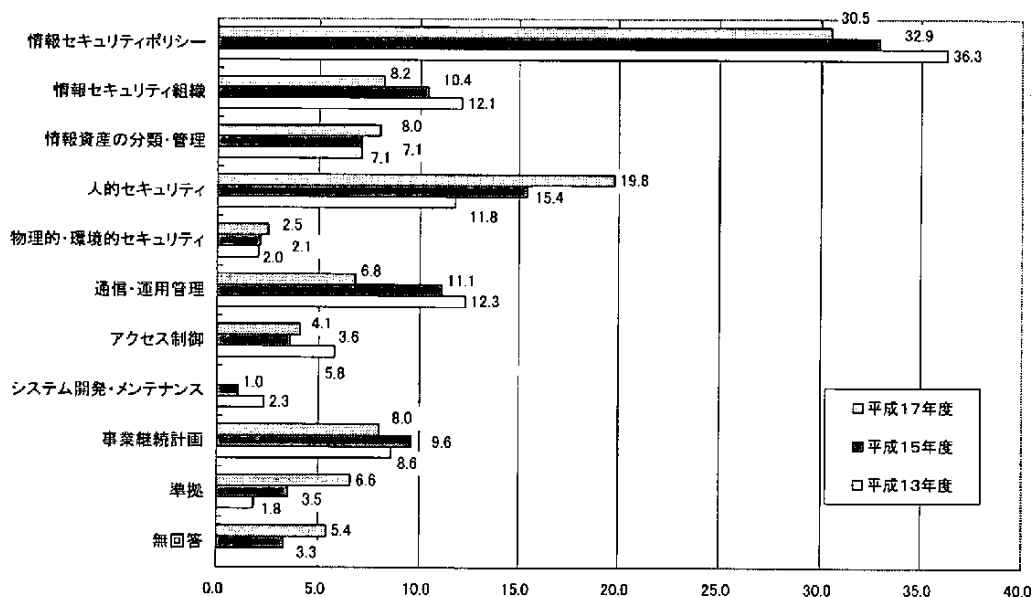


図2-3-11. 重要と思われるセキュリティ要素(1位)

重要要素順位の動向(優先順位 1位)

| 調査年度<br>順位 | 平成17年度                 | 平成15年度          | 平成13年度          |
|------------|------------------------|-----------------|-----------------|
| 第1位        | 情報セキュリティポリシー           | 情報セキュリティポリシー    | 情報セキュリティポリシー    |
| 第2位        | 人的セキュリティ               | 人的セキュリティ        | 通信および運用管理       |
| 第3位        | 情報セキュリティ組織             | 通信および運用管理       | 情報セキュリティ組織      |
| 第4位        | 情報資産の分類および管理<br>事業継続計画 | 情報セキュリティ組織      | 人的セキュリティ        |
| 第5位        | -                      | 事業継続計画          | 事業継続計画          |
| 第6位        | 通信および運用管理              | 情報資産の分類および管理    | 情報資産の分類および管理    |
| 第7位        | 準拠                     | アクセス制御          | アクセス制御          |
| 第8位        | アクセス制御                 | 準拠              | システム開発およびメンテナンス |
| 第9位        | 物理的および環境的セキュリティ        | 物理的および環境的セキュリティ | 物理的および環境的セキュリティ |
| 第10位       | システム開発およびメンテナンス        | システム開発およびメンテナンス | 準拠              |

## (2) 上位3位までの分析

第2位の選択状況を分析すると、前述の「(1) 第1位の分析」では2位であった「人的セキュリティ」が100件(19.5%)で1位になっている。次いで「情報セキュリティ組織」72件(14.0%)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前回同様、上位にあげられている。3位以下は「通信および運用管理」61件(11.9%)、「情報資産の分類および管理」56件(10.9%)、「アクセス制御」53件(10.3%)となり、前回の順位とまったく同

じであった。1位では順位を落とした「通信および運用管理」が3位を保ち、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技術的な実務がまだまだ重要視されていることがわかる。

第3位の選択状況は、1位「人的セキュリティ」85件（16.5%）、2位「アクセス制御」75件（14.5%）、3位「通信および運用管理」74件（14.4%）、4位「情報資産の分類および管理」67件（13.0%）、5位「事業継続管理」56件（10.9%）となっており、ほとんど前回と同様の順位であった。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が重みを増していることがわかる。

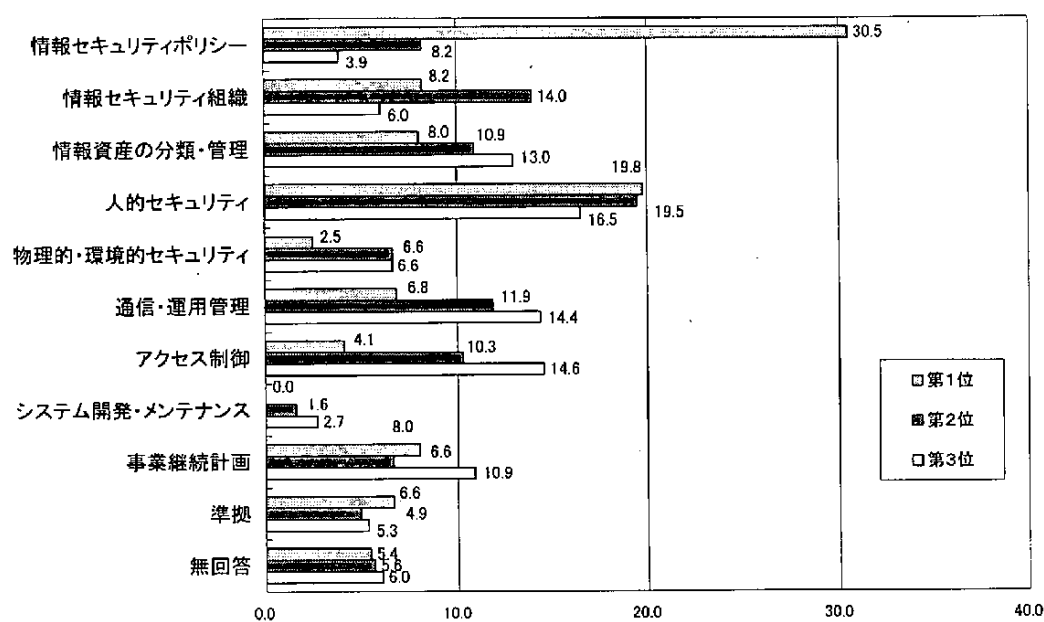


図2-3-12. 重要と思われる情報セキュリティ要素（優先順位 第1～第3位）

### (3) 上位3位までを総合した評価

#### 複合回答としての集計

| 情報セキュリティ要素 |                     | 平成17年度<br>(503件) |      | 平成15年度<br>(590件) |      | 平成13年度<br>(698件) |      |
|------------|---------------------|------------------|------|------------------|------|------------------|------|
| 1          | 情報セキュリティポリシー        | 229              | 45.5 | 287              | 48.6 | 346              | 49.6 |
| 2          | 情報セキュリティ組織          | 149              | 29.6 | 215              | 36.4 | 270              | 38.7 |
| 3          | 情報資産の分類および管理        | 173              | 34.4 | 193              | 32.7 | 197              | 28.2 |
| 4          | 人的セキュリティ            | 295              | 58.6 | 311              | 52.7 | 288              | 41.3 |
| 5          | 物理的および環境的セキュリティ     | 83               | 16.5 | 73               | 12.4 | 86               | 12.3 |
| 6          | 通信および運用管理           | 176              | 35.0 | 255              | 43.2 | 359              | 51.4 |
| 7          | アクセス制御              | 155              | 30.8 | 171              | 29.0 | 242              | 34.7 |
| 8          | システム開発およびメンテナンス     | 23               | 4.6  | 46               | 7.8  | 73               | 10.5 |
| 9          | 事業継続管理(災害対策、障害対策など) | 134              | 26.6 | 161              | 27.3 | 171              | 24.5 |
| 10         | 準拠                  | 87               | 17.3 | 54               | 9.2  | 49               | 7.0  |

### ①順位の分析

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」295件(58.6%)であり、前回(52.7%)から5.9ポイント増加している。前回以上に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」229件(45.5%)で、前回(48.6%)よりも3.1ポイント減少した。ただし総数では「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」176件(34.9%)で、前回(43.2%)から8.3ポイントの減少と大きく評価が下がった。第2位や第3位の選択では従来と同じ位置付けであることが多いことも判明しているため、実務レベルでは依然ウイルス対策などに手間を取られている実態が表れている。ただし、ある程度標準手法も実装されてきており、第1位に挙げるほどではなくなっているものと考えられる。

4位以下は次のとおりである。4位「情報資産の分類および管理」173件(34.3%⇨H15:32.7%、1.6ポイント増)、5位「アクセス制御」155件(30.8%⇨H15:29.0%、1.8ポイント増)、6位「情報セキュリティ組織」149件(29.6%⇨H15:36.4%、6.8%減)、7位「事業継続管理」134件(26.6%⇨H15:27.3%、0.7ポイント減)、8位「準拠」87件(17.3%⇨H15:9.2%、8.1ポイント増)、9位「物理的および環境的セキュリティ」83件(16.5%⇨H15:12.4%、4.1ポイント増)、10位「システム開発およびメンテナンス」23件(4.6%⇨H15:7.8%、3.2ポイント減)となった。このなかで、第6位の「情報セキュリティ組織」が前回から6.8ポイント減少したことにより、順位も2つ降下した。

### ②数字の変動による分析

数字の変動からみると大きく増加したのが「準拠」8.1ポイント、「人的セキュリティ」5.9ポイント、「物理的および環境的セキュリティ」4.1ポイントであり、また大きく減少したのが「通信および運用管理」8.3ポイント、「情報セキュリティ組織」6.8ポイント、「情報セキュリティポリシー」3.1ポイントである。個人情報保護法などの対応などから監査やコンプライアンスの重要性、従業員教育、そして事務所の入退室管理、キャビネットの鍵管理などが注目をあびた一方で、ウイルス対策が標準的になったこと、組織作りやポリシー作成などが一段落したか、あるいは同じ分野の「人的セキュリティ」に注目度が移ったのではないかと推測される。

### ③支持率の分布による分析

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」(58.6%)、B群「情報セキュリティポリシー」(45.5%)、C群「通信および運用管理」(35.0%)、「情報資産の分類および管理」(34.4%)、「アクセス制御」(30.8%)、「情報セキュリティ組織」(29.6%)、「事業継続管理」(26.6%)、D群「準拠」(17.3%)、「物理的および環境的セキュリティ」(16.5%)、「システム開発およびメンテナンス」(4.6%)となる。

前回調査ではA群「人的セキュリティ」(52.7%)、「情報セキュリティポリシー」(48.6%)、B群「通信および運用管理」(43.2%)、「情報セキュリティ組織」(36.4%)、C群「情報資産の分類および管理」(32.7%)、「アクセス制御」(29.0%)、「事業継続管理」(27.3%)、

D群「物理的および環境的セキュリティ」(12.4%)、「準拠」(9.2%)、「システム開発およびメンテナンス」(7.8%)であった。

13年度調査での順番は、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%)、C群5位「アクセス制御」(34.7%)、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%)であった。

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、A群は「人的セキュリティ」の一つのみとなった。一方、A群からB群に下降したものが「情報セキュリティポリシー」であるが、B群もこの一つとなり、前回B群であった「情報セキュリティ組織」と「通信および運用管理」などは支持率が下がり、C群に分類するところが妥当となった。前回、13年度をあわせて検討すると、「人的セキュリティ」の重要性がますます高まり、情報セキュリティは従業員の教育が焦点であるといっても過言ではない状況にある。一方、今回調査では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ためかC群に位置づけられた。また「アクセス制御」も前回同様C群にあり、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。つまりウイルス対策や不正アクセス対策など技術的対応はひととおり必要とツールなどの手法が出揃ってきて安定してきたと推察される。「情報セキュリティ組織」の支持率が下がったのは原因が不明である。最後に同じD群の「準拠(法律遵守、監査)」が13年度調査には10位であったが、順位をひとつずつ上げてきている。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ことがまだ支持率が低位ながらもようやく評価が高まってきたといえる。

重要要素順位の動向(複合回答集計分)

| グループ | 調査年度<br>順位 | 平成17年度          | 平成15年度          | 平成13年度          |
|------|------------|-----------------|-----------------|-----------------|
| A    | 第1位        | 人的セキュリティ        | 人的セキュリティ        | 通信および運用管理       |
| B    | 第2位        | 情報セキュリティポリシー    | 情報セキュリティポリシー    | 情報セキュリティポリシー    |
| C    | 第3位        | 通信および運用管理       | 通信および運用管理       | 人的セキュリティ        |
|      | 第4位        | 情報資産の分類および管理    | 情報セキュリティ組織      | 情報セキュリティ組織      |
|      | 第5位        | アクセス制御          | 情報資産の分類および管理    | アクセス制御          |
|      | 第6位        | 情報セキュリティ組織      | アクセス制御          | 情報資産の分類および管理    |
|      | 第7位        | 事業継続管理          | 事業継続管理          | 事業継続計画          |
| D    | 第8位        | 準拠              | 物理的および環境的セキュリティ | 物理的および環境的セキュリティ |
|      | 第9位        | 物理的および環境的セキュリティ | 準拠              | システム開発およびメンテナンス |
|      | 第10位       | システム開発およびメンテナンス | システム開発およびメンテナンス | 準拠              |

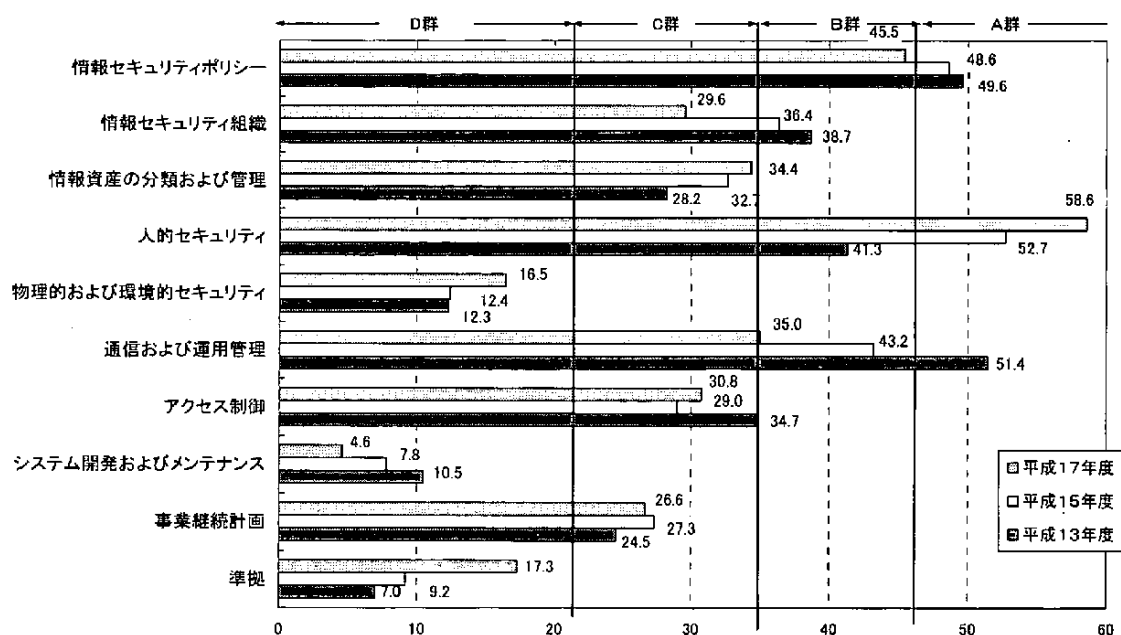


図2-3-13. 重要と思われるセキュリティ要素(優先順位付けなし)

#### (4) 業種グループ別の特徴

ここでは業種グループ別にどのような特色があるかをみる。セキュリティ要素それぞれのカテゴリで平均からの乖離状況を把握するため、それぞれ順位をつけて眺めてみると、「食品・紙・パルプ・繊維・印刷」では「情報セキュリティポリシー」が40.7%とその他の業種に比較して高い割合を占めている。また、「アクセス制御」も11.1%と高い数字を示している。「石油・化学・鉄鋼・非鉄・金属」は「通信および運用管理」が11.1%である。「電気・一般・輸送用機械」では「事業継続管理」が11.7%とやや高い値を示している。「その他製造業」では「情報資産の分類および管理」が16.1%で1位である。「商業」は「情報セキュリティポリシー」が40.5%と高い。「金融・保険業」では「情報セキュリティ組織」が12.5%と高いほか、「事業継続管理」14.1%、「準拠」10.9%と高い特徴がある。「情報処理サービス業」は平均から大きな差は少ないが「情報セキュリティポリシー」37.0%と高い値を示している。「その他事業所サービス」では「人的セキュリティ」が23.7%と高く、また「準拠」が10.5%と高い値を示している。

「公共サービス」は一般の事業体とは異なる大きな特徴がみられる。「情報セキュリティポリシー」が23.7%と大きく平均値を下回っている。一方で「情報セキュリティ組織」(21.2%)、「情報資産の分類」(13.2%)、「人的セキュリティ」(21.1%)と高くなっている。また「政府・地方公共団体」も「情報セキュリティポリシー」(21.9%)が大きく平均を下回っている一方、「人的セキュリティ」(37.5%)と前回の(45.1%)ではないにしろ、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。

業種グループ別にみた第1位選択項目

| 情報セキュリティ要素     | 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   |
|----------------|--------------|------------|------------|----------|---------------|---------|--------|---------------|--------|------|
| 業種             |              |            |            |          |               |         |        |               |        |      |
| 食品・紙・パルプ・繊維・印刷 | 40.7         | 7.4        | 7.4        | 11.1     | 0.0           | 7.4     | 11.1   | 0.0           | 3.7    | 7.4  |
| 石油・化学・鉄鋼・非鉄・金属 | 38.9         | 5.6        | 5.6        | 16.7     | 2.8           | 11.1    | 8.3    | 0.0           | 5.6    | 2.8  |
| 電気・一般・輸送・精密機器  | 28.3         | 3.3        | 10.0       | 18.3     | 0.0           | 5.0     | 3.3    | 0.0           | 11.7   | 10.0 |
| その他の製造業        | 29.0         | 6.5        | 16.1       | 16.1     | 12.9          | 3.2     | 6.5    | 0.0           | 9.7    | 0.0  |
| 商業             | 40.5         | 2.7        | 2.7        | 18.9     | 2.7           | 8.1     | 5.4    | 0.0           | 10.8   | 8.1  |
| 金融・保険業         | 29.7         | 12.5       | 6.3        | 7.8      | 0.0           | 1.6     | 9.4    | 0.0           | 14.1   | 10.9 |
| 情報処理サービス業      | 37.0         | 7.4        | 6.2        | 18.5     | 2.5           | 8.6     | 1.2    | 0.0           | 4.9    | 6.2  |
| その他対事業所サービス    | 25.0         | 10.5       | 5.3        | 23.7     | 2.6           | 5.3     | 2.6    | 0.0           | 10.5   | 10.5 |
| 公共サービス         | 23.7         | 21.1       | 13.2       | 21.1     | 7.9           | 2.6     | 0.0    | 0.0           | 5.3    | 2.6  |
| 政府・地方公共団体      | 21.9         | 4.7        | 10.9       | 37.5     | 0.0           | 14.1    | 0.0    | 0.0           | 1.6    | 1.6  |

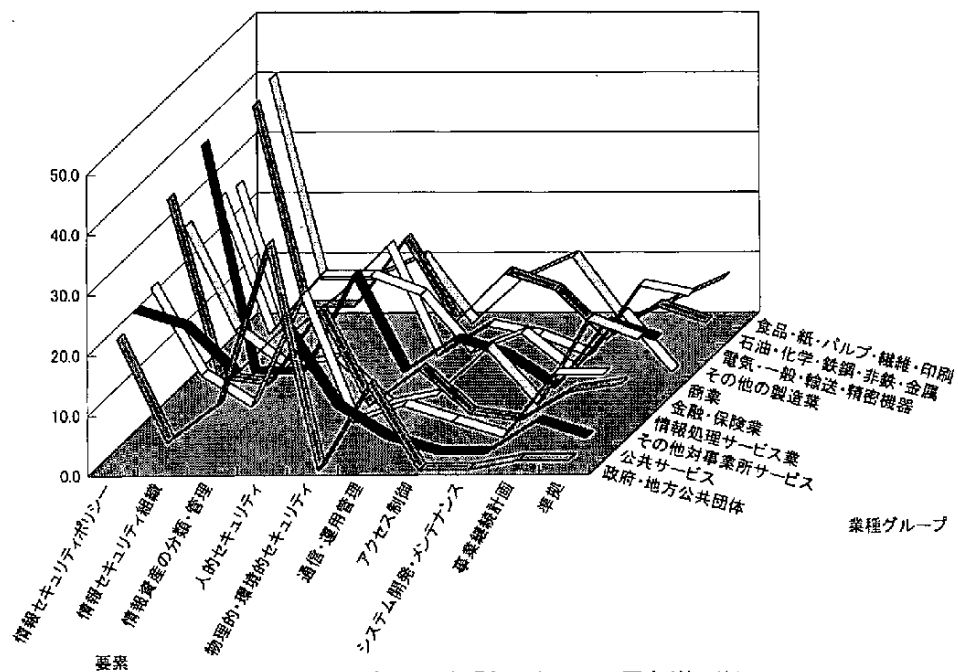


図2-3-14. 業種別にみた重要セキュリティ要素(第1位)

## 2.4 災害対策・障害対策について

Q23. 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 | 247 | 48.1  |
| 2 | 他の基準で扱っている                       | 112 | 21.8  |
| 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)   | 145 | 28.2  |
|   | 無回答                              | 10  | 1.9   |
|   | 計                                | 514 | 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について、「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48.1%で、前回調査の27.4%に比べ20.7ポイント増加した。また、平成13年度調査の19.1%からは29.0ポイント増という大きな変化がみられた。また「他の基準で扱っている」が21.8%と前回調査(27.1%)から減少している。また「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28.2%で3割を下回った。前回調査(44.1%)からは15.9ポイント減少、13年度調査(53.6%)からは25.4ポイント減少した。情報セキュリティポリシーなどによる災害・障害対策の明確化は3分の2を超え、ようやくここに至り認識度が向上していることがうかがえる。

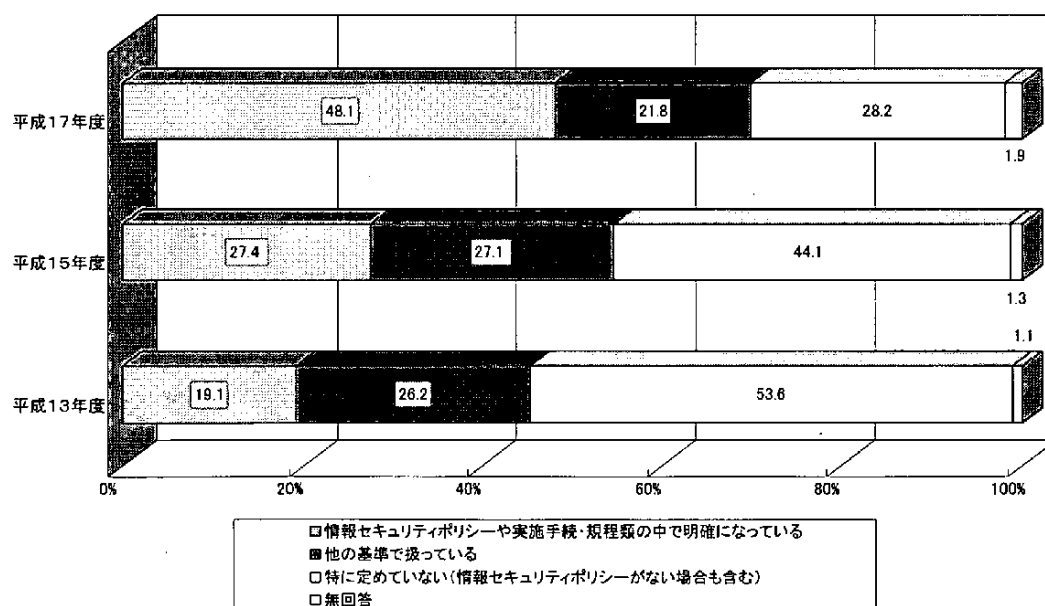


図2-4-1. 情報セキュリティポリシー、規定類における災害対策・障害対策の明確化

業種グループ別にみると大きな差異がみられる。「金融・保険業」では「特に定めていない」がゼロ、「情報処理サービス業」も9.9%と低い。一方、「定めていない」が50%を超えるのは「石油・化学・鉄鋼・非鉄・金属」(50.0%)、「その他製造業」(67.7%)、「商業」(51.4%)、「公共サービス」(52.6%)である。このようにみれば認識度が向上しているといえるが、情報システムの依存度合いにその普及率が大きく左右されており、その意味で今後これらの「定めていない」方が多い業種の取組みの浸透が課題になると考えられる。

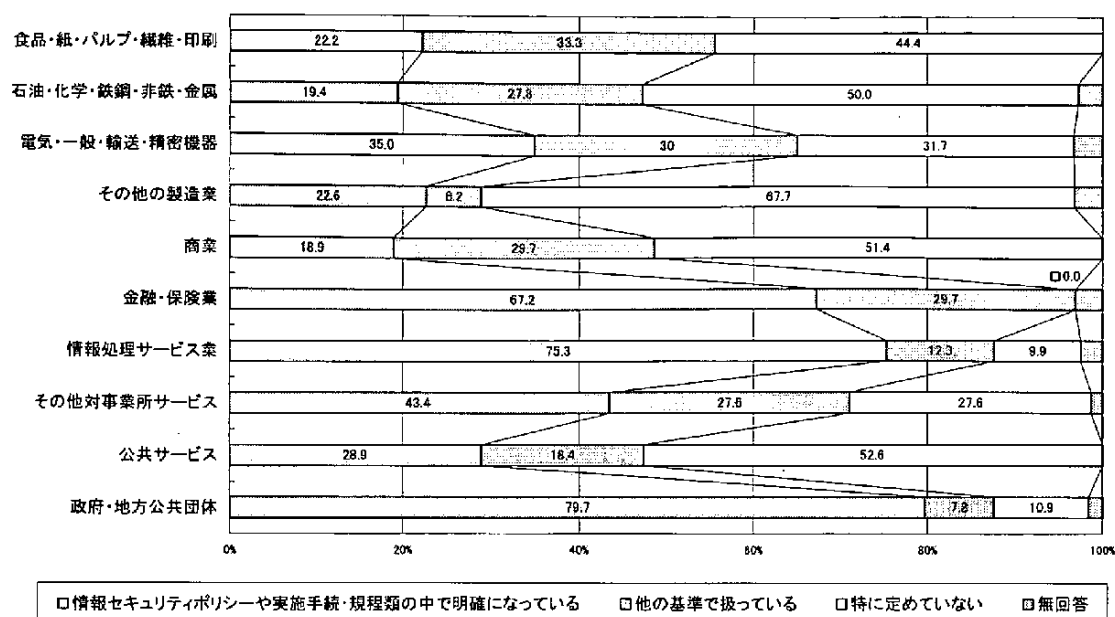


図2-4-2. 情報セキュリティポリシー、規定類における災害対策・障害対策の明確化  
(業種グループ別)

Q24. 「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      | ⇒Q25へ | 85  | 16.5  |
| 2   | 作成中である      | ⇒Q25へ | 24  | 4.7   |
| 3   | 作成を含め検討中である | ⇒Q26へ | 128 | 24.9  |
| 4   | 作成していない     | ⇒Q26へ | 251 | 48.8  |
| 5   | 必要ない        | ⇒Q26へ | 9   | 1.8   |
| 無回答 |             |       | 17  | 3.3   |
| 計   |             |       | 514 | 100.0 |

事業継続性計画については、「作成している」が16.5%であり、前回調査(10.2%)から6.3ポイント増加した。また「作成中」(4.7%)は前回(6.6%)から1.9ポイント減少、「作成を含め検討中である」(24.9%)は前回(13.6%)から11.3ポイント増加した。一方、「作成していない」(48.8%)は前回(64.8%)から16.0ポイント減少した。また、「必要ない」(1.8%)は前回(2.0%)とほぼ同じである。本調査は前回から始めたものであるが、ニューヨーク同時多発テロ(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表れており、実際に計画を「作成している」のは2割に満たない。ただし、「作成していない」が50%を下回るなど、少しずつ浸透してきていることがわかる。

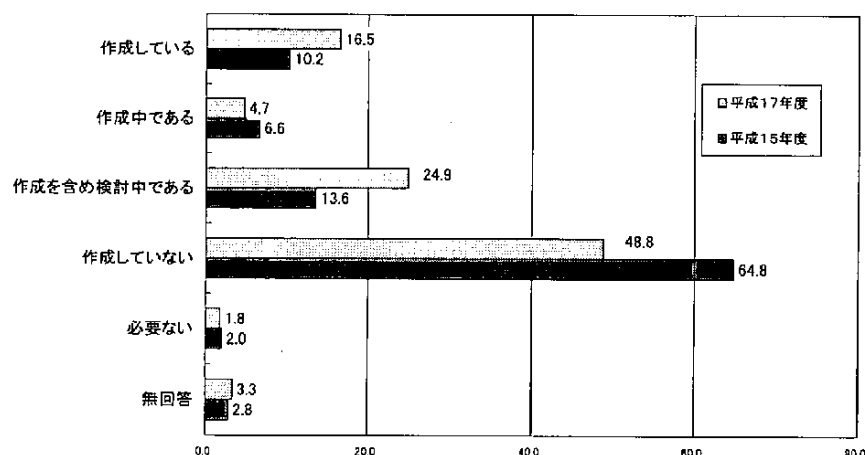


図2-4-3. 事業継続性計画の作成状況

業種グループ別にみると、ここでも業種の差異が明確である。「作成している」で割合が高いのは「金融・保険業」(42.2%) および「情報処理サービス業」(42.0%) で、この2業種は他と比べ抜きん出ている。

一方、「作成していない」割合が高い業種は「石油・化学・鉄鋼・非鉄・金属」(66.7%) で、3分の2が作成していない。そのほか、「その他製造業」(80.6%)、「商業」(59.5%)、「公共サービス」(73.7%)、「政府・地方公共団体」(60.9%) も高い。今後事業継続を浸透させるためには製造業や商業なども含めて考えている内閣府の「事業継続ガイドライン」や中小企業庁が2月に発表した「中小企業BCP策定運用指針」などの活用が必要と考えられる。

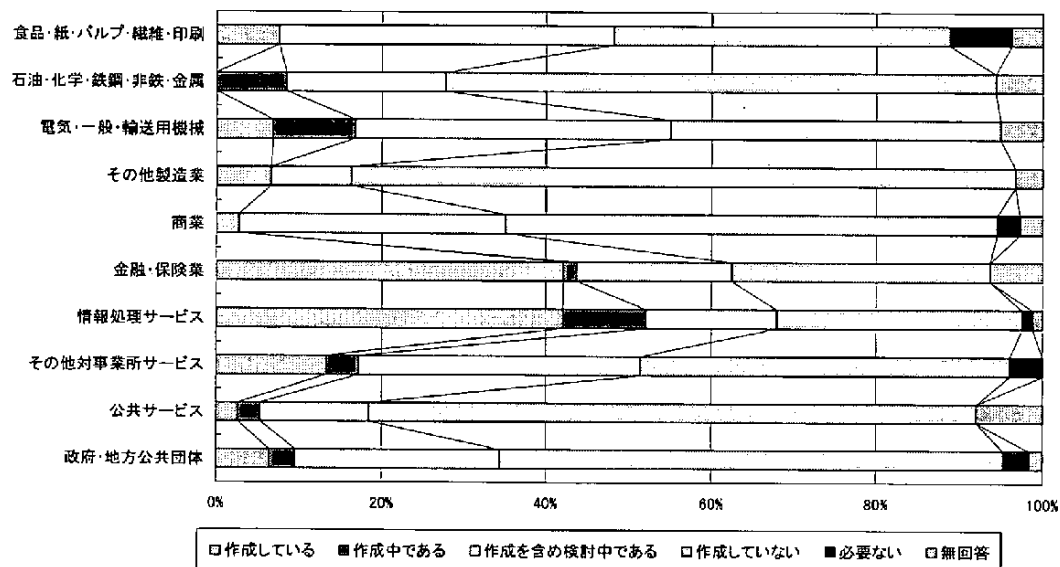


図2-4-4. 事業継続計画の作成状況(業種グループ別)

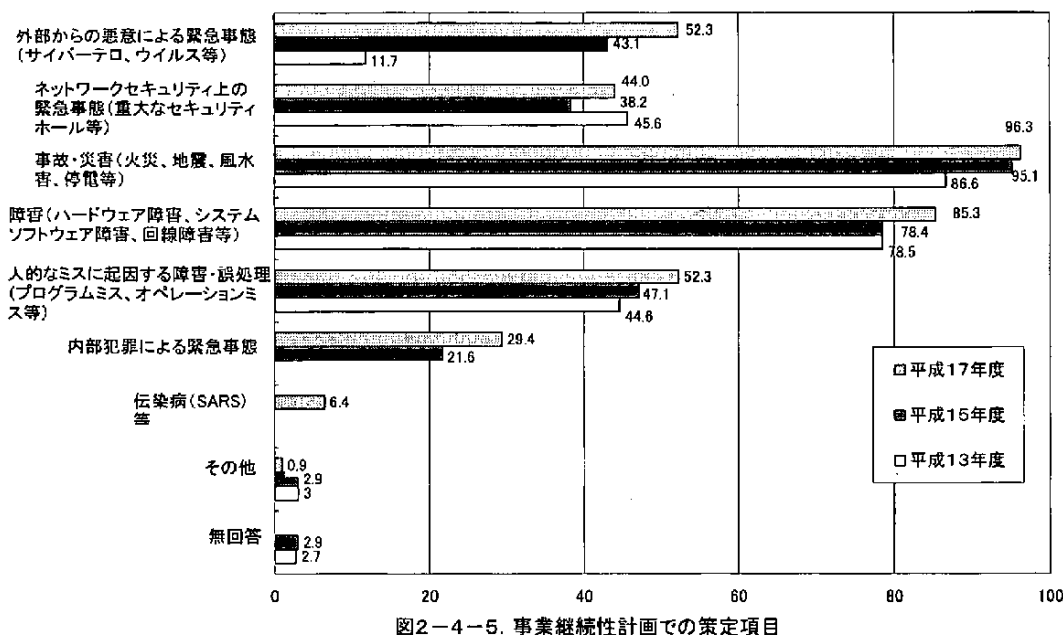
Q25. (Q24 で「1」、「2」と回答した場合)事業継続性計画には以下の項目を含んでいますか。含まれている項目を選んで下さい。(複数回答)

| 回答件数                                   | 109 | —    |
|----------------------------------------|-----|------|
| 1 外部からの悪意による緊急事態(サイバーテロ、コンピュータウイルス等)   | 57  | 52.3 |
| 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)    | 48  | 44.0 |
| 3 事故・災害(火災、地震、風水害、停電等)                 | 105 | 96.3 |
| 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)      | 93  | 85.3 |
| 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) | 57  | 52.3 |
| 6 内部犯罪による緊急事態                          | 32  | 29.4 |
| 7 伝染病(SARS等)                           | 7   | 6.4  |
| 8 その他                                  | 1   | 0.9  |

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、Q24 で「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、停電等)」(96.3%)で、前回調査の95.1%同様の高い値を示した。これは13年度調査の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、回線障害等)」(85.3%)で、これは前回(78.4%)より6.9ポイント増加し、また13年度調査の78.5%を上回っている。この2つがいわば事業継続の対象とするリスクではAランクとなる。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)」(52.3%)は前回(47.1%)から5.2ポイント増加している。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)」(44.0%)は前回の38.2%から5.8ポイント増加し、13年度の45.6%に匹敵する。一方、「外部からの悪意による緊急事態(サイバーテロ、コンピュータウイルス等)」については52.3%と前回の43.1%から9.2ポイント増加し、13年度の11.7%から実に40.6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的になっているという、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、「内部犯罪による緊急事態」は29.4%で、前回の21.6%から7.8ポイント増加した。今回は対象とするリスクについての変動はないが、すべてのリスクについて対象としているポイントが増加しており、マルチハザードによる対策へと進化していることがうかがえる。



Q26. 災害に対する情報システムのバックアップ対策を講じていますか。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 |                            | 514 | —    |
|------|----------------------------|-----|------|
| 1    | 対象システムを決めている               | 302 | 58.8 |
| 2    | バックアップに関する規程や手順を決めている      | 264 | 51.4 |
| 3    | バックアップの頻度、バックアップ先を決定している   | 288 | 56.0 |
| 4    | バックアップを定期的に実施している          | 424 | 82.5 |
| 5    | バックアップの実施状況を定期的にチェックしている   | 207 | 40.3 |
| 6    | 回復手順を決めている                 | 219 | 42.6 |
| 7    | バックアップを業者に委託するときはSLAを結んでいる | 34  | 6.6  |
| 8    | バックアップシステムの稼働状況を確認している     | 136 | 26.5 |
| 9    | アウトソーシング先の対策は把握していない       | 9   | 1.8  |
| 10   | 特に講じていない                   | 29  | 5.6  |
| 無回答  |                            | 12  | 2.3  |

情報システムの災害に対するバックアップ対策の策定状況について調査した。前回調査まではサーバ関連対策としての設問であったが、今回はサーバクライアント方式が一般化されたとの状況把握のもと、サーバに限定しない聞き方とし、また設問も変更している。

バックアップ対策として、最も多く行われているのは「データのバックアップを定期的に行っている」が82.5%で最も割合が高い。これはシステムのバックアップはなかなかシステム構築が難しいと考えられるが、最低限データの保全を実施したい、という考えの表れと考えられる。

次に多いのは「バックアップの対象システムを決めている」が58.8%、「バックアップの頻度やバックアップ先を決定している」が56.0%、「バックアップに関する規程や手順を定めている」が51.4%である。一方、「バックアップの状況を定期的にチェックしている」は40.3%と5割を

下回っており、「回復手順を定めている」は42.6%、「バックアップシステムの稼働状況を確認している」は26.5%と急速に実施しているところが少なくなってくる。なお、「バックアップ業者に委託する時はSLAを結んでいる」事業体は6.6%であり、「アウトソーシング先の対策は把握していない」事業体も1.8%存在している状況である。

一般にデータのバックアップを取得するところまでは実施しているが、バックアップを構築するところは半分程度である。またバックアップ体制を構築していても、その後の稼働確認などのチェックが全体的に弱いことがうかがえる。

Q27. 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。設置(予定)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                   | 514 | —    |
|------------------------|-----|------|
| 1 ホットスタンバイシステム         | 192 | 37.4 |
| 2 コールドスタンバイシステム        | 196 | 38.1 |
| 3 クラスタリング              | 189 | 36.8 |
| 4 RAID(RAID1～5)        | 423 | 82.3 |
| 5 フォールトトレラント           | 91  | 17.7 |
| 6 アウトソーシング先の対策は把握していない | 9   | 1.8  |
| 7 特に設けていない             | 35  | 6.8  |
| 無回答                    | 14  | 2.7  |

前回調査までは基幹システムがメインフレームの場合とクライアントサーバシステムの場合に分けて障害対策機能の設置状況を調査したが、今回調査では特に分けることはしなかった。したがって、前回の調査結果はあまり参考にできない。

今回調査では「RAID (RAID1～5)」が82.3%と圧倒的に割合が高く、次いで「コールドスタンバイシステム」(38.1%)、「ホットスタンバイシステム」(34.7%)、「クラスタリング」(36.8%)が続いている。この結果から、RAID (RAID1～5) が情報システムの障害対策として一般的に普及しているといえるのではないかな。また、次に続くコールドスタンバイシステム、ホットスタンバイシステム、クラスタリングの各機能の設置については特に差がないものと考ええる。

「特に設けていない」は前回17.4%であったが、今回は6.8%と大幅に減少している。これは昨今の情報システムのトラブルが関係各所に大きな影響を与えていることから、情報システムの障害対策の重要性が認識されてきた結果と思われる。

また、「アウトソーシング先の対策は把握していない」が前は2.1%であったが、今回は1.8%とわずかながら減少している。アウトソーシングの利用率が増加する状況で、アウトソーシング先の問題は自組織内の問題であるとの認識が強まった結果であろう。

産業別にみると「特に設けていない」の回答は以下のとおりである。産業区分に関わらず前回調査より減少していることは、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を考慮しての結果と思われる。

| 産業        | 平成 17 年度 | 平成 15 年度 |
|-----------|----------|----------|
| 第二次産業     | 11.5     | 21.9     |
| 第三次産業     | 4.9      | 15.8     |
| 政府・地方公共団体 | 1.6      | 5.6      |

Q28. 貴事業体ではどのような地震対策をとっていますか。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 |                      | 514 | —    |
|------|----------------------|-----|------|
| 1    | 建物が免震構造になっている        | 89  | 17.3 |
| 2    | 建物が耐震構造になっている        | 228 | 44.4 |
| 3    | 転倒防止措置を講じている         | 344 | 65.0 |
| 4    | 機器の移動防止措置を講じている      | 178 | 34.6 |
| 5    | フリーアクセス床は耐震構造としている   | 155 | 30.2 |
| 6    | フリーアクセス床は免震構造としている   | 70  | 13.6 |
| 7    | 媒体の落下防止措置を講じている      | 130 | 25.3 |
| 8    | その他                  | 11  | 2.1  |
| 9    | アウトソーシング先の対策は把握していない | 13  | 2.5  |
| 10   | 特に対策を講じていない          | 76  | 14.8 |
| 無回答  |                      | 10  | 1.9  |

災害には、その発生を未然に防止できるものと防止できないものがあるが、地震はその発生を未然に防止することのできない災害の代表的なものである。したがって、地震対策は発生を未然に防止することではなく、発生した場合の被害を最小限に食い止め、また、被害の復旧が短時間で終わるような対策が必要となる。

前回までの調査では、「サーバ設置場所」・「データ保管場所」と分けて調査したが、今回は特に分けずに行った。

| 調査年度<br>地震対策項目  | 平成 17 年度 | 平成 15 年度 |         |
|-----------------|----------|----------|---------|
|                 |          | 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    | 65.0     | 56.0     | 40.5    |
| 機器の移動防止措置を講じている | 34.6     | 39.5     | 27.1    |
| 建物が耐震構造になっている   | 44.4     | 36.4     | 35.9    |

今回、前回調査とも「転倒防止措置を講じている」割合が高い。地震対策としてはそれぞれの建物の環境条件の違いもあり、一言で結論づけることはできないが、「転倒防止措置を講じている」が一般的といえるのではないかな。

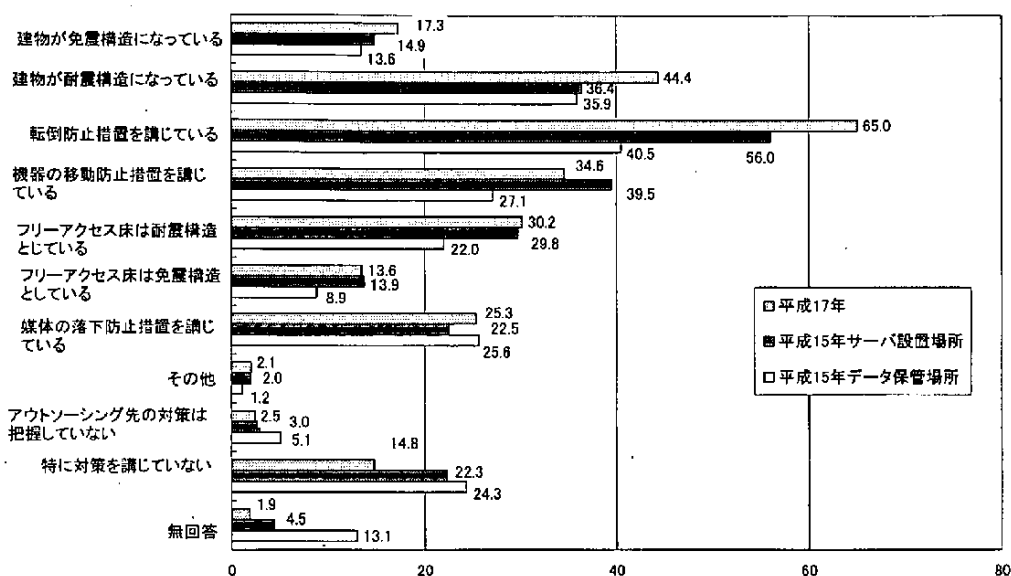


図2-4-6. 地震対策の実施状況

産業別にみると、「アウトソーシング先の対策は把握していない」および「特に対策は実施していない」の割合は以下のとおりである。

| 調査項目<br>産業 | アウトソーシング先の対策は<br>把握していない |        | 特に対策は講じていない |        |
|------------|--------------------------|--------|-------------|--------|
|            | 平成17年度                   | 平成15年度 | 平成17年度      | 平成15年度 |
| 第二次産業      | 1.6                      | 4.8    | 21.9        | 29.5   |
| 第三次産業      | 3.4                      | 5.4    | 12.8        | 22.6   |
| 政府・地方公共団体  | 1.6                      | 5.6    | 3.1         | 9.3    |

情報システム障害同様、アウトソーシング先の地震対策を把握しておくことが大切であるが、前回と比較すると各産業とも割合が減少しており、対策の把握が進んでいるものと思われる。これは、アウトソーシング先の地震対策まで把握することの必要性の認識を強めている結果と思われる。

また、「特に対策は実施していない」については、前回調査と比較すると割合が大きく減少している。災害対策のうち、地震対策の必要性を認識してきた結果であろう。

Q29. 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          | 514 | —    |
|---------------|-----|------|
| 1 AVR         | 42  | 8.2  |
| 2 CVCF/UPS    | 442 | 86.0 |
| 3 自家発電装置      | 236 | 45.9 |
| 4 電力供給経路の複数化  | 105 | 20.4 |
| 5 その他         | 3   | 0.6  |
| 6 特に対策を講じていない | 34  | 6.6  |
| 無回答           | 7   | 1.4  |

電源設備の災害対策としては「CVCF/UPS」が 86.0% (H15 : 86.8%) と一番高い。次に高いのは「自家発電装置」で 45.9% (H15 : 36.9%) であるが、前回調査と比較してみると、「CVCF/UPS」が 0.8 ポイント減少し、「自家発電装置」が 9 ポイント増加している。これらをみると、電源設備の災害対策の主流はやはり「CVCF/UPS」ではあるが、「自家発電装置」の重要性が高まりつつあるようだ。また、「電力供給経路の複数化」は 20.4% (H15:17.2%) で、3.2 ポイント増加している。

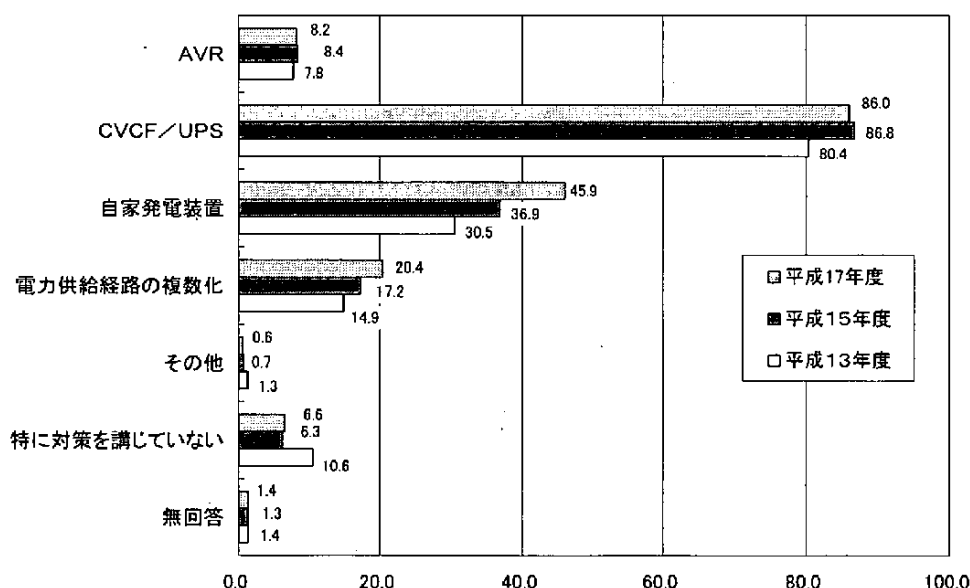


図2-4-7. 電源設備の災害対策

産業別にみると、「電力供給経路の複数化」の回答は以下のとおりである。

|           | 平成 17 年度 | 平成 15 年度 |
|-----------|----------|----------|
| 第二次産業     | 14.2     | 14.7     |
| 第三次産業     | 24.4     | 20.5     |
| 政府・地方公共団体 | 21.9     | 11.1     |

「第三次産業」が 3.9 ポイント、「政府・地方公共団体」が 10.8 ポイント増加しているが、電源設備の災害対策としての方策を複数化しておくことの必要性を考慮してのことであろう。

産業別の「特に対策を講じていない」の回答は以下のとおりである。

|           | 平成 17 年度 | 平成 15 年度 |
|-----------|----------|----------|
| 第二次産業     | 9.3      | 10.4     |
| 第三次産業     | 6.4      | 3.7      |
| 政府・地方公共団体 | 0.0      | 1.9      |

前回調査と比較すると、「第二次産業」および「政府・地方公共団体」がわずかではあるが減少している。一方、「第三次産業」が 2.7 ポイント増加しており、未実施率の増加が気にかかる。

Q30. 貴事業体では従業員に対し、情報セキュリティのどの教育・訓練を実施していますか。

| 管理項目           | 定期的実施<br>している |      | 時々実施している |      | 実施を予定<br>している |      |
|----------------|---------------|------|----------|------|---------------|------|
| ①災害対策          | 106           | 20.6 | 89       | 17.3 | 73            | 14.2 |
| ②障害対策          | 94            | 18.3 | 122      | 23.7 | 64            | 12.5 |
| ③不正アクセス対策      | 130           | 25.3 | 145      | 28.2 | 60            | 11.7 |
| ④コンピュータウイルス対策  | 172           | 33.5 | 200      | 38.9 | 35            | 6.8  |
| ⑤ポリシー類         | 155           | 30.2 | 141      | 27.4 | 87            | 16.9 |
| ⑥アクセス制限の実施     | 156           | 30.4 | 151      | 29.4 | 63            | 12.3 |
| ⑦個人情報保護        | 217           | 42.2 | 172      | 33.5 | 46            | 8.9  |
| ⑧情報セキュリティの一般知識 | 170           | 33.1 | 174      | 33.9 | 66            | 12.8 |

| 管理項目           | 実施していない |      | 無回答 |     | 計   |       |
|----------------|---------|------|-----|-----|-----|-------|
| ①災害対策          | 210     | 40.9 | 36  | 7.0 | 514 | 100.0 |
| ②障害対策          | 197     | 38.3 | 37  | 7.2 | 514 | 100.0 |
| ③不正アクセス対策      | 157     | 30.5 | 22  | 4.3 | 514 | 100.0 |
| ④コンピュータウイルス対策  | 88      | 17.1 | 19  | 3.7 | 514 | 100.0 |
| ⑤ポリシー類         | 110     | 21.4 | 21  | 4.1 | 514 | 100.0 |
| ⑥アクセス制限の実施     | 117     | 22.8 | 27  | 5.3 | 514 | 100.0 |
| ⑦個人情報保護        | 66      | 12.8 | 13  | 2.5 | 514 | 100.0 |
| ⑧情報セキュリティの一般知識 | 89      | 17.3 | 15  | 2.9 | 514 | 100.0 |

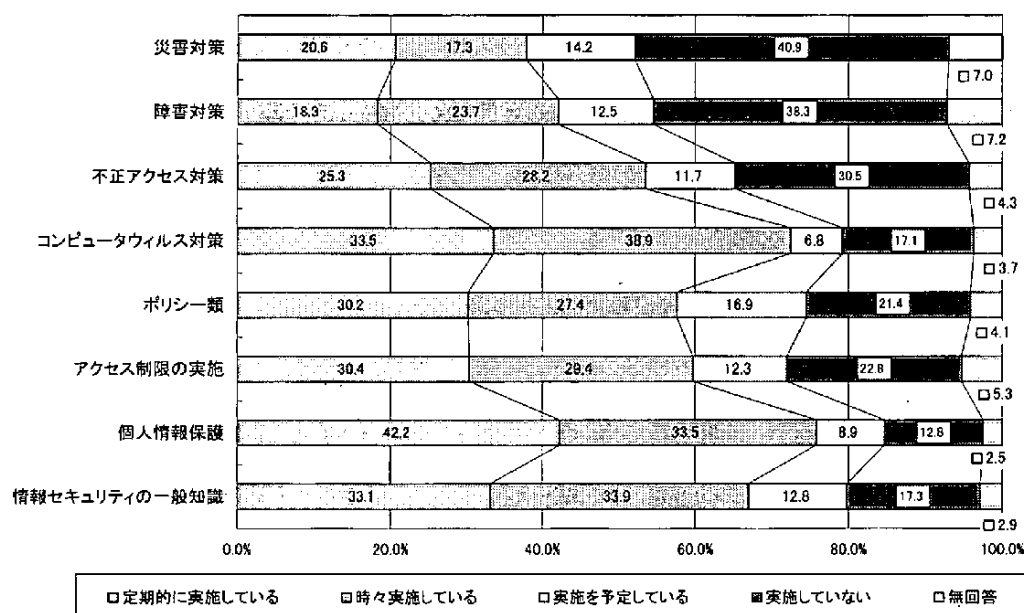
従業員に対する教育・訓練に関しては「個人情報保護」が最も高く、実施頻度にかかわらず75.7%が実施している。これは個人情報保護法（平成15年制定）の影響が大きく、また、高い関心の表れと思われる。次いで「コンピュータウイルス対策」（72.4%）、「情報セキュリティの一般知識」（67.0%）がこれに続いているが、各事業体の情報セキュリティ関連の関心のポイントがこの辺にあるのではないかと。

「実施している」および「実施を予定している」の合計と、「実施していない」を比較した結果は以下のとおりである。

| 実施項目 \ 実施状況   | ・定期的実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|---------------|---------------------------------------|---------|
| 災害対策          | 52.1                                  | 40.9    |
| 障害対策          | 54.5                                  | 38.3    |
| 不正アクセス        | 65.2                                  | 30.5    |
| コンピュータウイルス対策  | 79.2                                  | 17.1    |
| ポリシー類         | 74.5                                  | 21.4    |
| アクセス制限の実施     | 72.1                                  | 22.8    |
| 個人情報保護        | 84.6                                  | 12.8    |
| 情報セキュリティの一般知識 | 79.8                                  | 17.3    |

「災害対策」、「障害対策」、「不正アクセス」の割合がやや低い、これは従業員一般に対する教育・訓練より、専門的な担当者に対する教育・訓練が中心に行われている結果と思われる。

情報セキュリティの問題は事業体全体の問題であり、担当者のみが理解していればよいということではなく、経営上の影響も大きい問題であるため、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、できるだけ広い範囲の情報セキュリティ教育・訓練（災害対策・障害対策・不正アクセスも含め）を計画的に実施すべきであろう。また、教育・訓練の対象として経営者層、管理者層も入れる必要がある。



2-4-7. 従業員に対する情報セキュリティ教育の実施状況

産業別の「情報セキュリティの一般知識」に関する教育を「特に実施していない」の割合は以下のとおりである。

|           |       |
|-----------|-------|
| 第二次産業     | 26.2% |
| 第三次産業     | 14.3% |
| 政府・地方公共団体 | 4.7%  |

「政府・地方公共団体」の割合が低い、これは常に多くの人々がいろいろな情報を求めて政府・地方公共団体の事業所を訪れる関係から、その対応に配慮してのことと思われる。

情報セキュリティの教育・訓練の実施状況について、産業別の割合は以下のとおりである。

#### ①災害対策

| 産業        | 実施状況                                   | 実施していない |
|-----------|----------------------------------------|---------|
|           | ・定期的に実施している<br>・時々実施している<br>・実施を予定している |         |
| 第二次産業     | 40.5                                   | 53.0    |
| 第三次産業     | 62.7                                   | 30.5    |
| 政府・地方公共団体 | 40.7                                   | 50.0    |

災害対策に関する教育・訓練については、「第三次産業」の「実施している」、または「実施を予定している」の割合が一番高い。

## ②障害対策

| 産業 \ 実施状況 | ・定期的に実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|-----------|----------------------------------------|---------|
| 第二次産業     | 37.7                                   | 55.2    |
| 第三次産業     | 65.4                                   | 27.8    |
| 政府・地方公共団体 | 56.3                                   | 34.4    |

障害対策に関する教育・訓練については、「第二次産業」の「実施している」、または「実施を予定している」の割合が低い。

## ③不正アクセス対策

| 産業 \ 実施状況 | ・定期的に実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|-----------|----------------------------------------|---------|
| 第二次産業     | 54.7                                   | 39.9    |
| 第三次産業     | 70.3                                   | 26.3    |
| 政府・地方公共団体 | 73.5                                   | 21.9    |

不正アクセス対策に関する教育・訓練については、「第二次産業」の「実施している」、または「実施を予定している」の割合が低い。

## ④コンピュータウイルス対策

| 産業 \ 実施状況 | ・定期的に実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|-----------|----------------------------------------|---------|
| 第二次産業     | 77.0                                   | 19.1    |
| 第三次産業     | 80.1                                   | 16.5    |
| 政府・地方公共団体 | 81.3                                   | 14.1    |

コンピュータウイルス対策に関する教育・訓練については、各産業とも「実施している」または「実施を予定している」の割合が高い。

## ⑤ポリシー類

| 産業 \ 実施状況 | ・定期的に実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|-----------|----------------------------------------|---------|
| 第二次産業     | 62.8                                   | 32.2    |
| 第三次産業     | 79.3                                   | 17.7    |
| 政府・地方公共団体 | 87.5                                   | 6.3     |

ポリシー類に関する教育・訓練については「第二次産業」の「実施している」または「実施を予定している」の割合が低く、「政府・地方公共団体」の割合が高い。

#### ⑥アクセス制限の実施

| 産業 \ 実施状況 | ・定期的に実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|-----------|----------------------------------------|---------|
| 第二次産業     | 65.5                                   | 29.5    |
| 第三次産業     | 78.6                                   | 16.9    |
| 政府・地方公共団体 | 62.5                                   | 28.1    |

アクセス制限の実施に関する教育・訓練については「第三次産業」の「実施している」、または、「実施を予定している」の割合が高い。

#### ⑦個人情報保護

| 産業 \ 実施状況 | ・定期的に実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|-----------|----------------------------------------|---------|
| 第二次産業     | 74.3                                   | 23.0    |
| 第三次産業     | 90.9                                   | 7.5     |
| 政府・地方公共団体 | 87.4                                   | 6.3     |

個人情報保護に関する教育・訓練については、各産業とも「実施している」または「実施を予定している」の割合が高い。

#### ⑧情報セキュリティの一般知識

| 産業 \ 実施状況 | ・定期的に実施している<br>・時々実施している<br>・実施を予定している | 実施していない |
|-----------|----------------------------------------|---------|
| 第二次産業     | 70.5                                   | 26.2    |
| 第三次産業     | 83.1                                   | 14.3    |
| 政府・地方公共団体 | 92.2                                   | 4.7     |

情報セキュリティの一般知識に関する教育・訓練については、各産業とも「実施している」または「実施を予定している」の割合が高いが、「政府・地方公共団体」の割合が最も高い。

Q31. 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。(単一回答)

|      |                                 |     |       |
|------|---------------------------------|-----|-------|
| 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       | 56  | 10.9  |
| 2    | 民間の教育機関を利用して育成している              | 111 | 21.6  |
| 3    | 情報セキュリティアドミニストレータなどの資格試験を活用している | 42  | 8.2   |
| 4    | 特に行っていない                        | 283 | 55.1  |
| 5    | 必要ない                            | 2   | 0.4   |
| 複数回答 |                                 | 20  | 3.9   |
| 計    |                                 | 514 | 100.0 |

情報セキュリティ人材の育成については、「民間の教育機関を利用して育成している」(21.6%  
→H15:4.8%)の割合が高い。

今回と前回調査を比較した結果は以下のとおりである。

|                                 | 平成 17 年度 | 平成 15 年度 |
|---------------------------------|----------|----------|
| 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       | 10.9     | 7.8      |
| 民間の教育機関を利用して育成している              | 21.6     | 4.8      |
| 情報セキュリティアドミニストレータなどの資格試験を活用している | 8.2      | 6.3      |
| 人材教育を行っている(合計)                  | 40.7     | 18.9     |
| 特に行っていない                        | 55.1     | 76.5     |

前回調査で最も割合が低かった「民間の教育機関を利用して育成している」が今回調査では最も高くなったが、これは費用的には負担が大きい内容の充実している民間の教育機関を選択することの効果を期待してのことであろう。なお、前回調査の選択肢は「民間資格を利用して育成している」であったが、今回調査では「民間の教育機関を利用して育成している」と内容を変えたため、そのニュアンスの違いが割合の変化に影響を与えているとも考えられる。

また、全体的に何らかの方法で、「人材育成を行っている(合計)」は40.7%と、前回の18.9%より21.8ポイント高くなった。一方で「特に行っていない」は55.1%とやや高い結果ではあるが、前回調査の76.7%に比べると割合はかなり減少している。これは情報セキュリティ教育の必要性が理解されてきた結果であろう。

産業別の情報セキュリティ関連の人材育成状況は以下のとおりである。

| 育成状況<br>産業 | 自社育成プログラムによる | 民間の教育機関を利用 | 資格試験などを活用 | 人材育成を行っている(合計) | 特に行っていない |
|------------|--------------|------------|-----------|----------------|----------|
| 第二次産業      | 8.2          | 14.8       | 5.5       | 28.5           | 68.3     |
| 第三次産業      | 12.4         | 22.2       | 11.3      | 45.9           | 48.9     |
| 政府・地方公共団体  | 12.5         | 39.1       | 3.1       | 54.7           | 42.2     |

情報セキュリティ関連の人材育成については、「第二次産業」が全般的に実施率が低く、「特に行っていない」が高い。第二次産業は情報セキュリティ関連の人材育成の関心が薄いようである。

## 2.5 不正アクセス対策・不正侵入対策・情報漏えい対策について

Q32. 管理面における不正アクセス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                                                   | 514 | —    |
|--------------------------------------------------------|-----|------|
| 1 不正アクセスを受けた場合のIPAやJPCERT/CCへの相談                       | 63  | 12.3 |
| 2 室の出入口での入・退室管理                                        | 373 | 72.6 |
| 3 室の管理責任者の設置                                           | 285 | 55.4 |
| 4 パソコン・記録媒体の持込み・持出しの管理                                 | 282 | 54.9 |
| 5 重要情報を扱うシステムを隔離し、他のシステムと接続させない                        | 230 | 44.7 |
| 6 個人情報・機密情報の担当者の限定(アクセス制限)                             | 360 | 70.0 |
| 7 ネットワーク機器の運用者(アクセス範囲)の限定                              | 359 | 69.8 |
| 8 情報セキュリティポリシーで勝手にLANの配線に触ったり、個人のPCを接続することの禁止          | 321 | 62.5 |
| 9 情報セキュリティ管理者やネットワーク管理者によるサーバやルータ、ファイアウォールのログの定期的なチェック | 294 | 57.2 |
| 10 定期的にリスク分析や情報セキュリティ監査を実施                             | 162 | 31.5 |
| 11 その他                                                 | 7   | 1.4  |
| 12 アウトソーサ側の実施対策を確認している                                 | 54  | 10.5 |
| 13 特に対策を講じていない                                         | 28  | 5.4  |
| 無回答                                                    | 8   | 1.6  |

管理面における不正アクセス対策は、前回調査から大きな前進がみられた。この原動力になっているのは、もちろん個人情報保護法の施行であろう。

「IPA や JPCERT/CC への相談」は、前回調査の 3.6%から 12.6%と 3.5 倍に増加した。これは、実際に不正アクセス被害が増加したことと、IPA や JPCERT/CC が相談を受けていることが周知された結果と考えられる。

「入・退室管理」や「管理責任者の設置」といった物理的な不正アクセスに対する対策は、今回調査では前回に比べて大きく改善された。しかし、紙等の物理的な媒体に対する不正アクセスを防ぐためには、入・退室管理は基本であり、これを実施していない3割近くの事業体は、早急に何らかの対策を実施すべきである。

「パソコン・記録媒体の持込み・持出しの管理」は、ノートパソコンの紛失による HDD 内のデータ漏えいや、1GB 以上の USB メモリが安価になり簡単に大量のファイルを持ち出せるようになった現状から、不正アクセス対策として重要な項目の一つになった。しかし、業務効率の観点からはノートパソコンを持ち運ぶ必要もあり、パソコンや記録媒体に入っている情報の重要性和とのバランスを考慮した管理が必要である。もし、管理が行われていなければ、最も機密度の高いデータも持ち歩かれている可能性があると考えべきである。

「重要情報を扱うシステムを隔離し、他のシステムと接続させない」ことは、システム連携等での不便さよりも、情報が漏えいした場合の影響度が非常に大きい場合にとられる対策である。すべての事業体にこのようなシステムがあるとは限らないが、不正アクセスを受けて情報が漏えいした場合の被害を自社で算定した結果により考慮する価値がある。実例としては、社内の人事システムを人事部門内の隔離した環境で運営している例がある。

「情報に対するアクセス権を個人別に限定する」ことは、情報保護の基本であり、すべての事業体が実施すべき事項である。また、ユーザ ID としてグループ用の ID を設け、複数の社員が使い回している状況は、アクセス権管理をしていないのと同じであり、日本版 SOX 法で求められる内部統制上からも重要な欠陥になりうる。

「ネットワーク機器の運用管理者の限定」は、前回調査の 51.4% から 69.8% へ向上した（18.4 ポイント増）。ネットワーク用のアナライザ等の使用は、ネットワーク上をユーザ ID やパスワードが流れていることを考えると、大きなリスクになりうる。

「物理的な LAN 配線を触ることや個人 PC の接続禁止」は、前回調査の 36.4% から 62.5% へと大きく向上した（26.1 ポイント増）。持ち込まれた個人用パソコンからのウイルス感染により社内のネットワークが大きな被害を受けた、という事件も発生しており、この禁止措置はぜひ実施する必要がある。

「ログの定期的なチェック」は、前回調査の 20.4% から 57.2% と三倍近くになった（36.8 ポイント増）。これは、不正アクセスを実際に受けるケースが増えたことと、ログデータからフィルタリングするツールが普及したことが追い風となっている。自組織がどれぐらいの不正アクセスを受けているかはぜひ知っておくべきであり、それに対応できる技術者が組織内にいない場合は、アウトソーシングすることも検討すべきである。

不正アクセスのリスクは、日々新しい手口が出てきているため、定期的なリスク分析やセキュリティ監査を実施することが望ましい。事業体の規模が小さい場合は、相対的な負担が大きくなるが、一旦被害を受けた場合のことを考えると、規模に係らず対策を講じることが望ましい。

アウトソーシングを利用している場合は、自組織内での対策に加え、アウトソーサでも同等の対策がとられていないと自組織内の対策も意味がなくなってしまう。特に、システム開発においては重層的な下請関係がとられることもあり、主契約者が実質的に目を光らせていない状況で個人情報流出した事例もある。アウトソーシングを利用している事業体は、アウトソーサの監督責任が自組織に残ることに留意すべきである。

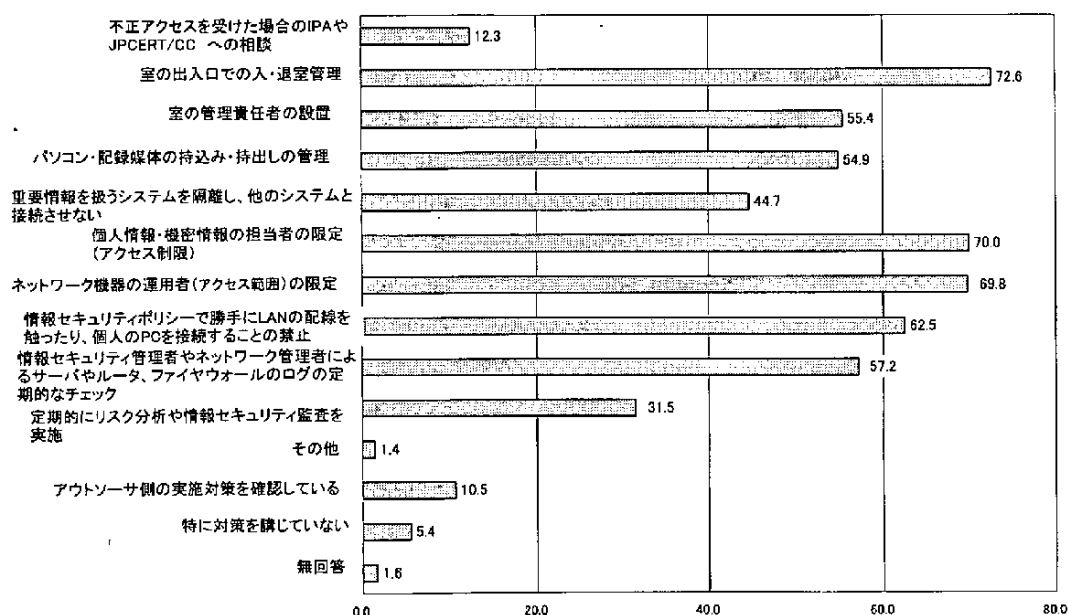


図2-5-1. 管理面における不正アクセス対策の実施状況

Q33. 技術面における不正アクセス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 |                                                                   | 514 | —    |
|------|-------------------------------------------------------------------|-----|------|
| 1    | 室への入退室についてカード、パスワードを使用                                            | 312 | 60.7 |
| 2    | 入退室のときにアンチパスバック(定期券のように二度連続して入れないような仕組み)を持っている                    | 39  | 7.6  |
| 3    | 室への入室について身体的特徴(指紋、虹彩等)により識別                                       | 95  | 18.5 |
| 4    | 情報システムの監視設備を設けている                                                 | 159 | 30.9 |
| 5    | ファイアウォールの利用                                                       | 451 | 87.7 |
| 6    | セキュリティパッチの適用                                                      | 384 | 74.7 |
| 7    | アクセス制御ソフトウェアの使用                                                   | 208 | 40.5 |
| 8    | 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 | 109 | 21.2 |
| 9    | その他                                                               | 7   | 1.4  |
| 10   | 特に対策を講じていない                                                       | 24  | 4.7  |
| 無回答  |                                                                   | 7   | 1.4  |

技術面における不正アクセス対策は、投資の効果がみえやすいこともあり、大きく前進した。

「入退室管理でのカード等の使用」、「アンチパスバックの使用」、「生体認証による識別」、「監視設備の設置」等の物理的な不正アクセス対策は、前回調査が 45.5%と高かったカード等の使用を除くと、軒並み 2 倍程度の数字になっており、大きな進展がみられた。もちろん、事業体規模によりすべてを実施することは現実的ではないが、外部からの侵入よりも内部での物理的なアクセスを適切に管理するという視点に立つと、カード等の使用は最低限実施すべきである。カードや生体認証等を使っている事業体に重なりがないとしても、約 2 割の事業体が物理的な不正アクセス対策を実施していないことになる。

論理的な不正アクセス対策としての「ファイアウォールの利用」は、前回調査 (83.3%) から 87.7%へとわずかながら増加した。また、「セキュリティパッチの適用」も前回調査 (61.0%) から 74.7%への増加に留まった。これらの項目は、論理的な不正アクセス対策の基本的なところであり、ぜひ実施すべきである。

「アクセス制御ソフトウェアの使用」は、前回調査 (28.3%) から 40.5%へと大きく増加した。しかし、Q32 で「個人情報・機密情報の担当者の限定 (アクセス制限)」を実施しているという回答が 70.0%であったことを考慮すると、約 3 割の事業体は OS の基本機能を使ってアクセス管理を実施していると考えられ、今後、アクセス管理対象が細分化されるにつれ、作業が困難になると考えられる。

「社外からのアクセスに対して追加的なコントロールを実施している」については、前回調査 (17.5%) から 21.2%へと約 2 割増加した。これは、個人情報保護法の施行に伴い、社外からのアクセス自体を禁止した事業体があることや、ブロードバンドの普及により社外からのアクセスに VPN が使われ、追加的なコントロールの必要性が下がったことが影響し、もっと大きな増加にならなかったためと考えられる。しかし、今後予測される新型の鳥インフルエンザの大流行により、基幹要員が自宅で業務を遂行することが必要になった場合の対策としても、各事業体は社外からの安全なアクセスを整備しておくべきであり、非常に高度の機密を扱うシステムでは、VPN に加えてワンタイムパスワードを使うことも考慮すべきである。

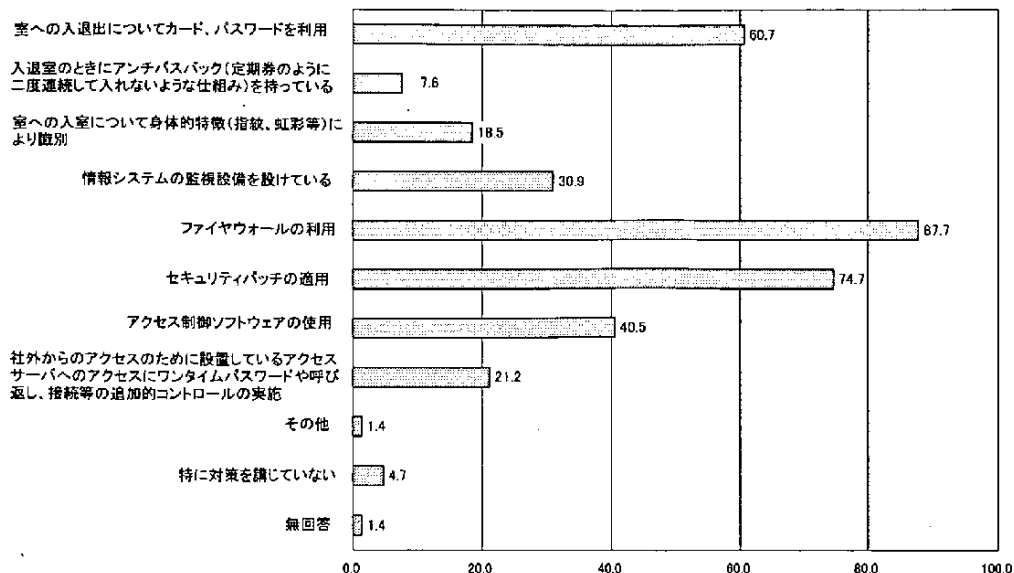


図2-5-2. 技術面における不正アクセスの実施状況

なお、今回Q32で「管理面」の、Q33で「技術面」における不正アクセス対策の実施状況を調査したが、前回までは「物理的」および「論理的」不正アクセス対策の切り口で調査を行っており、質問項目も若干異なっている。過去2回のそれぞれの実施状況は以下のとおりである。

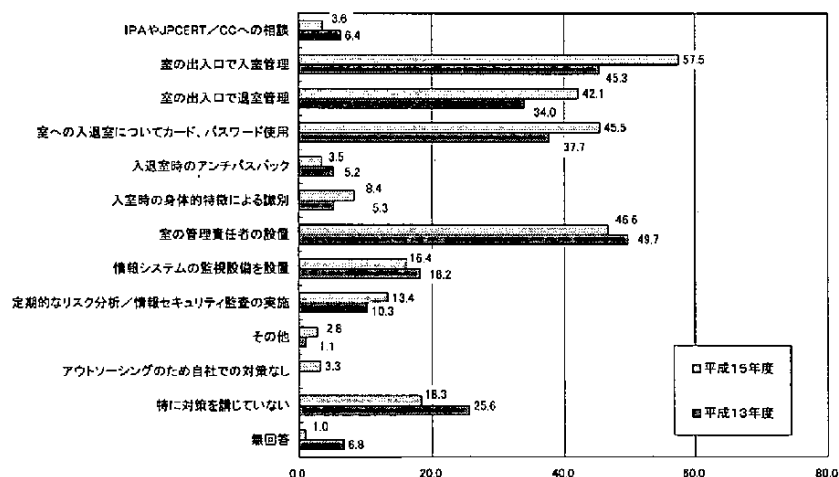


図2-5-3. 物理的不正アクセスの実施状況(参考)

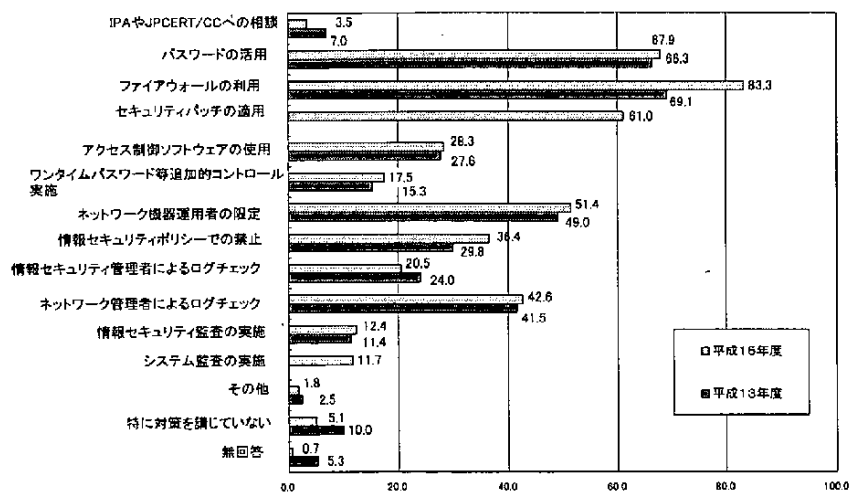


図2-5-4. 論理的不正アクセス対策の実施状況(参考)

Q34. 情報価値の観点から、個人情報や機密情報等に対し機密度区分を設定していますか。(単一回答)

|     |                        |     |       |
|-----|------------------------|-----|-------|
| 1   | 機密区分を設定し、暗号化している       | 71  | 13.8  |
| 2   | 機密区分を設定しているが、暗号化はしていない | 210 | 40.9  |
| 3   | 機密区分を設定していないが、暗号化をしている | 41  | 8.0   |
| 4   | 機密区分を設定しておらず、暗号化もしていない | 171 | 33.3  |
| 無回答 |                        | 21  | 4.1   |
| 計   |                        | 514 | 100.0 |

機密度区分を設定している割合は、前回調査では29.7%であったが、今回は54.7%と1.84倍になった。機密度区分を行わない場合、本来厳重に保護すべき情報が不十分な管理のままにされ、不正アクセスがあった場合のリスクを非常に高くしてしまう。実際に機密度の区分を行うと、非常に厳重に保護すべき情報は、一般的には1割から2割の間であり、そこにリソースを集中して、必要な保護対策を実施すべきである。このためにも、機密度区分の設定はぜひ実施すべきである。

また、暗号化についても、ハードウェアの能力拡大とともに、PCにおいても実用的な時間で可能となり、以前に比べ技術的なハードルは低くなっている。対象とする情報の機密度と、持ち運ぶノートPCといったリスクの両面から検討し、必要な場合はHDDの暗号化等を実施すべきである。

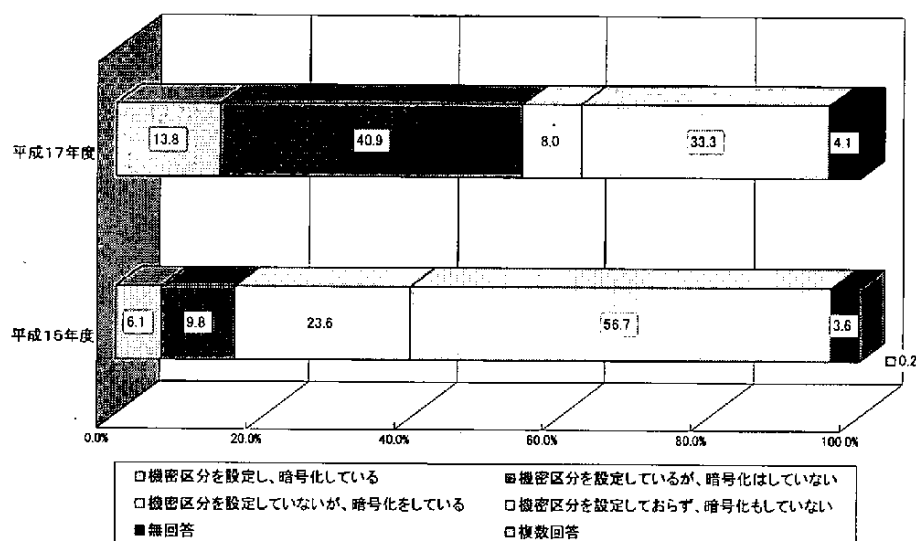


図2-5-5. 機密度ランクの設定状況

Q35. 貴事業体では基幹システム・重要なサーバ、シングルサインオン等<sup>(注)</sup>の一般ユーザのパスワード変更をどのレベルに設定していますか。(単一回答)

|     |                                 |     |       |
|-----|---------------------------------|-----|-------|
| 1   | ワンタイムパスワードを設定している               | 9   | 1.8   |
| 2   | 変更期限がきたらパスワードを無効にする             | 53  | 10.3  |
| 3   | 定期的に新しいパスワードを配布する               | 44  | 8.6   |
| 4   | 変更期限を定めて利用者が変更している              | 132 | 25.7  |
| 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 | 144 | 28.0  |
| 6   | パスワードの変更に関して特に定めていない            | 82  | 16.0  |
| 7   | パスワードによる管理を実施していない              | 15  | 2.9   |
| 8   | その他                             | 5   | 1.0   |
| 無回答 |                                 | 30  | 5.8   |
| 計   |                                 | 514 | 100.0 |

(注) 最も重要なシステム1つに限定して回答。(p3「基幹システムの説明」を参照のこと)

ユーザ認証に最もよく使われているのは、ユーザ ID とパスワードである。しかし、パスワードについては、パスワード管理をどの程度実施するかでその信頼性は大きく変わってくる。パスワード管理に重要な要素である一定のパスワードの使用期間について、前回調査に比べ管理水準の向上がみられた。まず、ノート PC 等を公衆ネットワーク経由で使用する場合は、ワンタイムパスワードが不正アクセス阻止の有力な対策であるが、「ワンタイムパスワード利用」は 1.8%、前回調査 (1.7%) とほとんど変化はなかった。これは、非常にセキュリティが要求されるシステムについては、公衆ネットワークを使わないようにした事業者が多いためと考えられる。次いで「変更期限がきたらパスワードを無効にする」が前回調査の 6.6% から 10.3% へ、「定期的に新しいパスワードを配布」が前回調査の 6.1% から 8.6% へ、「変更期限を定めて利用者が変更している」が前回調査の 16.5% から 25.7% へと、パスワード管理の強化につながる施策の割合が増加した。

一方、パスワード管理が不十分になることが多い「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」はほぼ横ばいに、「パスワードの変更に関して特に定めていない」は前回調査の 26.0% から 16.0% に大きく減少した。これは、パスワードの管理に対する意識が大きく向上したことの表れと考えられる。

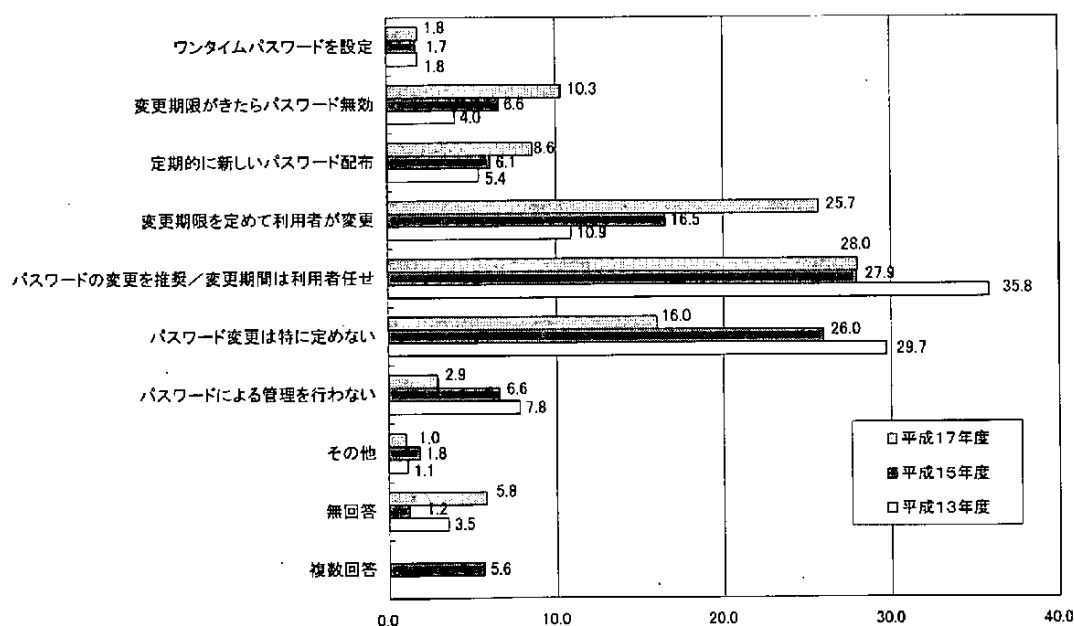


図2-5-6. 基幹システム等のパスワード変更レベルの設定状況

Q36. 情報漏えい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 |                                                            | 514 | —    |
|------|------------------------------------------------------------|-----|------|
| 1    | セキュリティポリシー、個人情報保護ポリシー、規程類の整備                               | 398 | 77.4 |
| 2    | 従業者に対する教育                                                  | 351 | 68.3 |
| 3    | 入退室(館)管理                                                   | 343 | 66.7 |
| 4    | アクセス制限                                                     | 416 | 80.9 |
| 5    | 機密情報の管理                                                    | 248 | 48.2 |
| 6    | 不正プログラムの侵入防止(コンピュータウイルス等でキーロガーやデータの不正送信プログラムが持ち込まれないようにする) | 298 | 58.0 |
| 7    | 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                         | 239 | 46.5 |
| 8    | ハードディスク、CD、FD等記録媒体や不要となった印刷物の返却、廃棄時の破壊、溶解                  | 343 | 66.7 |
| 9    | 暗号化機能の採用                                                   | 198 | 38.5 |
| 10   | 輸送体制強化                                                     | 90  | 17.5 |
| 11   | 電子メールの送信時モニタリング                                            | 119 | 23.2 |
| 12   | ログチェックの追跡機能                                                | 167 | 32.5 |
| 13   | その他                                                        | 7   | 1.4  |
| 14   | 特に対策を行っていない                                                | 22  | 4.3  |
| 無回答  |                                                            | 4   | 0.8  |

事業体として情報漏えい対策を実施していくうえで最も重要なのは、その組織としてセキュリティ対策にどう取り組んでいくかの基本となるセキュリティポリシーの裏づけである。この点から、「セキュリティポリシー、個人情報保護ポリシー、規程類の整備」が前回調査の 52.7% から 77.4%へと大幅に増加し、4分の3を越えたことは非常に大きな意味がある。つまり、情報漏えい事件が起きた場合に、その事業体がセキュリティポリシーを定めていなかった場合、管理不備を指摘される可能性が非常に高くなるからである。現在、ポリシー類を整備していない事業体は早急に対応すべきである。

次に、個別の対策をみると、「従業者に対する教育」が前回調査の 45.6%から 68.3%へ、「入退室(館)管理」が前回調査の 54.5%から 66.7%へ、「アクセス制限」が前回調査の 53.1%から 80.9%に増加している。しかし、これらの項目は、情報漏えい対策としては基本的な項目であるため、未実施の事業体は早急を実施すべきである。

「機密情報の管理」は、前回調査の 29.4%から 48.2%に増加した。機密情報を管理する前提として、社内の情報に機密区分が設定されていることが必要であり、Q34 で「機密区分を設定している」という回答が前回調査の 29.7%から 54.7%に増加したことの効果がでていと考えられる。しかし、機密区分を設定してもそれに見合った管理をしていない事業体も 6.5%(54.7%－48.2%(Q36の「機密情報の管理」))あり、一層の管理レベルの向上が望まれる。

「不正プログラムの侵入防止」は新しく設けた質問であるが、58.0%の実施率となった。最近の情報漏えいの原因の一つに、ファイル交換ソフトウェアとウイルス感染による事例が多くみられ、不正プログラムの侵入防止対策は、ぜひ実施・強化すべきである。

「情報媒体の持出し・持込みの禁止」が前回調査の 32.1%から 46.5%へ、「記録媒体や文書の返却・廃棄」が前回調査の 50.9%から 66.7%に増加した。情報媒体の持出し・持込みの禁止

は、USB等の小型大容量メモリが安価になり誰でも持っている現状を考えると、今後の大きな漏えいルートと考えられる。特に、情報の機密区分が未設定の場合は、データのコピー等が野放しになる危険が高く、対策として考慮すべきである。また、記憶媒体や文書の返却・廃棄は外部委託を実施している場合のみならず、社内においても適切なルール化が必要な項目である。

「暗号化機能の採用」が前回調査の14.0%から38.5%になった。これは、Q34の回答で「暗号化している」という回答の合計(21.8%)とはギャップがあり、解釈が難しいところである。しかし、暗号化の採用が増加していることはたしかであり、取り扱う情報により適切な暗号化の採用をぜひ検討すべきである。たとえば、ノートPCのHDD全体を暗号化することや、インターネットで個人情報を入力する時にSSLを使用するといったことは、実施すべき項目である。

「輸送体制強化」が前回調査の5.0%から17.5%へ、「電子メールの送信時モニタリング」が前回調査の18.0%から23.2%へ、「ログチェックの追跡機能」が前回調査の21.5%から32.5%に増加している。「輸送体制強化」は、ブロードバンドネットワークの普及により、物理媒体を輸送するよりもネットワークでデータを送ることが一般的になったので、実施率が低く出ていると考えられる。また、「電子メールの送信時モニタリング」は、実際に行う場合の作業負荷とセキュリティポリシー等で実施を規定し、あらかじめ従業員からの了承を取る必要性があり、これらの点から実施率があまり上がっていないと考えられる。「ログチェックの追跡機能」は、Q32での「ログの定期的なチェック」の実施率が57.2%であることを考えると、25%程度の事業体が手作業でログをチェックしていることになり、作業負荷を考えると、何らかのツールの導入が必要となる。これらの3項目とも情報漏えいを防ぐためには必要な項目であり、自社の状況に応じた検討を今後行うべきである。

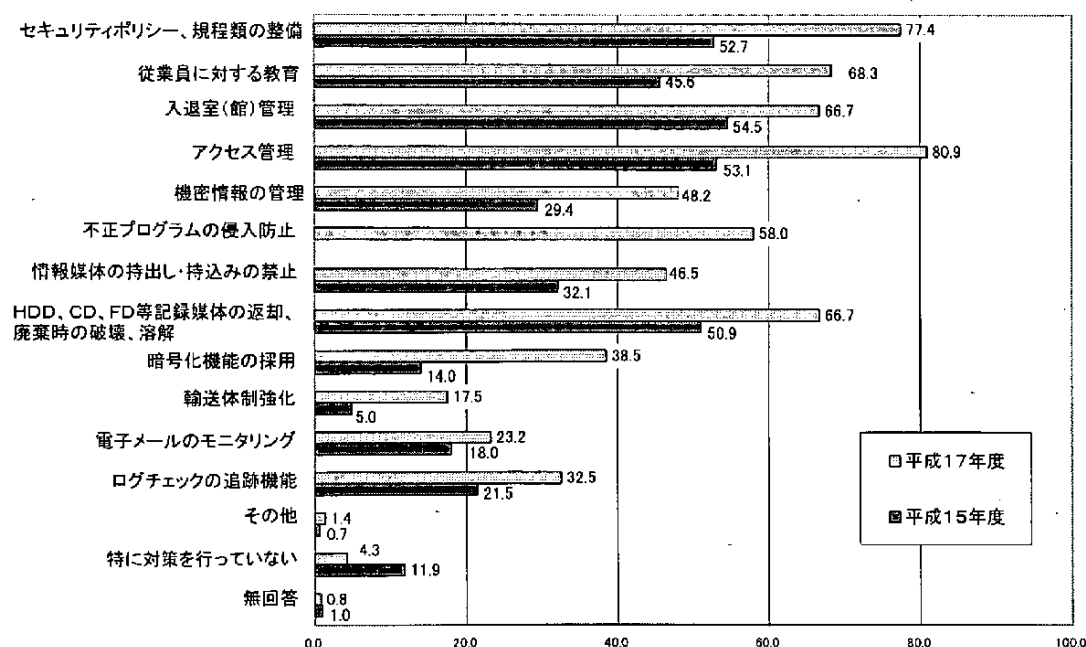


図2-5-7. 情報漏洩対策の実施状況

## 2.6 コンピュータウイルス対策について

Q37. 貴事業体では過去1年間にコンピュータウイルス、スパイウェア、スパムメール、フィッシングの被害にあったことがありますか。(複数回答)

| 回答件数 |                         |       | 514 | —    |
|------|-------------------------|-------|-----|------|
| 1    | コンピュータウイルス              | ⇒Q38へ | 227 | 44.2 |
| 2    | スパイウェア                  | ⇒Q38へ | 47  | 9.1  |
| 3    | スパムメール                  | ⇒Q39へ | 126 | 24.5 |
| 4    | フィッシング(自社のWebを模倣・悪用された) | ⇒Q39へ | 5   | 1.0  |
| 5    | 被害はない                   | ⇒Q39へ | 233 | 45.3 |
| 6    | 被害を把握していない              | ⇒Q39へ | 13  | 2.5  |
| 無回答  |                         |       | 7   | 1.4  |

今回調査から、コンピュータウイルスに加え、スパイウェア、スパムメール、フィッシング被害状況を調査した。前回までは広くコンピュータウイルスとして回答されていたと考えられるが、全体としては、感染被害を受けたという割合が前回調査の70.1%から54.7%へと大きく低下した。これは、ウイルス対策用の「ワクチンソフトの利用率」が86.0%、「パラメータファイルの定期的な更新」が79.6%の率で実施されていることを考えると（Q39のウイルス対策の実施状況参照）、ワクチンソフトの機能向上や、パラメータファイルの自動更新の実施が進んだためではないかと考えられる。しかし、パラメータファイルの定期的な更新を行っていても、約4分の1の事業体が感染被害にあっていることになり、自動更新の実施をより高める必要がある。

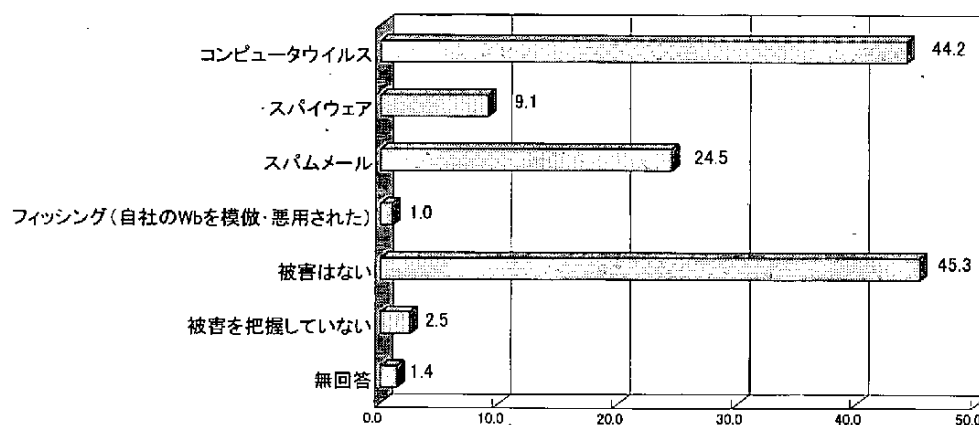


図2-6-1. 過去1年間のコンピュータウイルス等の被害状況

Q38. Q37 で「1」、「2」を回答した場合、コンピュータウイルス、スパイウェアの主要な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                             | 514 | -    |
|----------------------------------|-----|------|
| 1 フリーソフトウェアから                    | 12  | 5.1  |
| 2 社内ネットワーク経由で                    | 34  | 14.5 |
| 3 インターネット経由で                     | 106 | 45.1 |
| 4 電子メールの添付書類で                    | 151 | 64.3 |
| 5 外部のホームページの閲覧で                  | 63  | 26.8 |
| 6 ネットワーク経由の不正アクセス                | 4   | 1.7  |
| 7 スпамメールのリンク先                   | 10  | 4.3  |
| 8 バックドア                          | 4   | 1.7  |
| 9 ファイル交換ソフト                      | 3   | 1.3  |
| 10 インスタントメッセージサービス               | 3   | 1.3  |
| 11 外部との情報交換のために持ち込んだ PC や記録媒体経由で | 36  | 15.3 |
| 12 個人が持ち込んだPCや記録媒体経由で            | 48  | 20.4 |
| 13 その他                           | 2   | 0.9  |
| 14 わからない                         | 5   | 2.1  |
| 無回答                              | 2   | 0.9  |

Q37 でコンピュータウイルスに加え、スパイウェア、スパムメール、フィッシングを対象に追加したのに合わせ、その経路についても項目を追加した。全般的な傾向は前回調査で上位を占めた「電子メールの添付書類で」(64.3%→H15: 47.6%、16.7ポイント増)、「インターネット経由で」(45.1%→H15: 45.8%、0.7ポイント減)、「外部のホームページの閲覧で」(26.8%が前回の16.0%→H15: 26.8%、10.8ポイント増)と、主要な感染経路は同じである。

一方、「外部との情報交換のために持ち込んだPCや記録媒体経由で」は前回の38.2%から15.3%に減少しており、外部との情報交換の経路がフロッピーディスク等の記録媒体からブロードバンドの普及に伴い、急速にネットワークに変わったためと考えられる。また、社員が自分のPCに業務用のデータをコピーして自宅で仕事をする事が多くなっており、事業体はセキュリティポリシーで業務の効率を下げる覚悟でこれを禁止するか、仕事に使う社員のPCについても会社のセキュリティポリシーを適用して、会社でセキュリティ対策を実施するかを選択を迫られている。

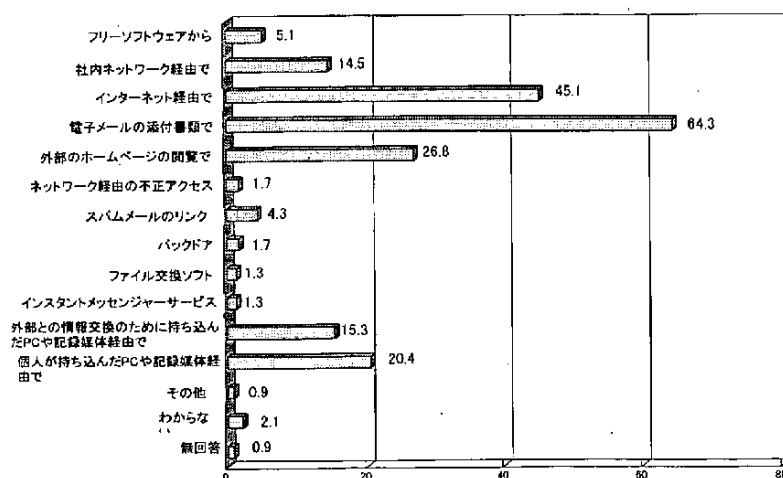


図2-6-2. 主要なウイルス等被害の感染経路(原因)

Q39. コンピュータウイルス、スパイウェア、スパムメール、フィッシング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                                                      | 514  | —    |
|-----------------------------------------------------------|------|------|
| 1 被害を受けた場合のIPAへの相談                                        | 41   | 8.0  |
| 2 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                       | 173  | 33.7 |
| 3 緊急対策チーム(社内でコンピュータウイルスが検出された時の対応を行うチーム)の設置               | 116  | 22.6 |
| 4 検出時や緊急対応と連絡体制の整備                                        | 217  | 42.2 |
| 5 従業員の教育(出所のわからないメール、疑わしいメールを開封しない等)                      | 38.3 | 74.5 |
| 6 出所の確認                                                   | 165  | 32.1 |
| 7 記録媒体利用時のチェックの実施                                         | 145  | 28.2 |
| 8 ライトプロテクト、バックアップ等のソフトウェア管理                               | 68   | 13.2 |
| 9 PCでのワクチンソフト(検出ソフトを含む)の利用                                | 442  | 86.0 |
| 10 PCのワクチンソフト・パラメータファイルの定期的な更新                            | 409  | 79.6 |
| 11 サーバ機でのワクチンソフトの利用(ISPの提供するサービス利用)                       | 296  | 57.6 |
| 12 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                             | 333  | 64.8 |
| 13 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)                  | 148  | 28.8 |
| 14 ワクチンソフトの集中監視                                           | 255  | 49.6 |
| 15 定期的な集中監視ログの解析                                          | 131  | 25.5 |
| 16 パスワードの変更等、アクセスコントロールの強化                                | 159  | 30.9 |
| 17 動作の定期的な確認等、異常発見体制の整備                                   | 87   | 16.9 |
| 18 緊急時の電子メールサーバの停止                                        | 114  | 22.2 |
| 19 緊急時の社員への連絡(コンピュータウイルス警告の放送/送付)                         | 212  | 41.2 |
| 20 OSの修正プログラムの適用(アップデートを含む)                               | 315  | 61.3 |
| 21 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)                         | 214  | 41.6 |
| 22 プロバイダが提供する対策サービスの利用                                    | 66   | 12.8 |
| 23 フィッシング防止のため、電子署名のついたメールを採用したり、自社 HP で真正性を確認できるツールを配布する | 11   | 2.1  |
| 24 その他                                                    | 2    | 0.4  |
| 25 特に対策を講じていない                                            | 4    | 0.8  |
| 無回答                                                       | 16   | 3.1  |

コンピュータウイルスやスパイウェアに感染して社内の PC が一日使用できなかった場合、その事業体としての被害はどの位と考えられるか。もちろん、業種や IT の活用度合いにより大きな違いはあるが、一度この状況を想定してユーザ部門にその被害について検討してもらえば、ウイルス等の被害に対する対策の重要性が判明するであろう。コンピュータウイルス等により、55% 程度の事業体が被害を受けている現状を考えれば、各事業体は、基本的な対策を実施していない理由について、再度吟味する必要がある。

「対策のマニュアル化」、「緊急対策チームの設置」、「対応と連絡体制の整備」といった管理面での対策については、前回とほぼ横ばいとなっており、セキュリティポリシーの設定と結び付けた全般的なアプローチが望まれるところである。一方、今回から調査項目に加えた「従業員

の教育」は、74.5%と比較的高い実施率であり、これによりマニュアル化、緊急対策チームの設置、対応と連絡体制の整備等の対策を補っていると考えられる。

コンピュータウイルスへの対策としては、「PCでのワクチンソフトの利用」(86.0%)があるが、前回調査(86.6%)とほぼ同じであった。これは実施率100%になってほしい対策であり、導入していない事業体は、ぜひ導入を検討すべきである。また、ワクチンソフトが入っていてもウイルスの検出に使うパラメータファイルが古ければ、ワクチンを入れていないのと同じであるため、実施率が49.6%に留まっている「ワクチンソフトの集中監視」は、ぜひ実施すべき対策である。

一方、「サーバ機でのワクチンソフトの利用」は、前回調査の71.6%から57.6%へと減少しているが、これは括弧内の「ISPの提供するサービス利用」を、自社で実施している場合を含まないと取ったためではないかと思われる。さらに「メール用ゲートウェイでのワクチンソフトの利用」(64.8%)も前回調査(62.3%)とほとんど横ばい状態にあり、改善の必要がある。

「メール用ゲートウェイでの添付ファイルの制限」は、社外とのデータのやり取りがメールで行われていることを考えると、常時禁止してしまうのは業務の効率性の点からは問題がある。ただし、新種のウイルスが発生してワクチンソフトのパラメータファイルの対応ができるまでの間、添付ファイルをブロックすることは感染拡大防止の有効な手段であり、緊急時のメールサーバの停止とともに、いざという時にその機能が使えるようにしておくべきである。

最後に、最近ウイルスやスパイウェアでは、OSやミドルウェアの脆弱性について感染を拡大させるものがある。これに対するワクチンソフトメーカーのパッチ適用は本番環境に悪影響を与える場合もあり、各事業体にとって頭の痛い問題である。根本的には、各メーカーが脆弱性を少なくすることが重要であるが、現実的な対応としては、脆弱性の大きさと本当に重要なシステムについて、テスト実施によりパッチを適用すべきである。

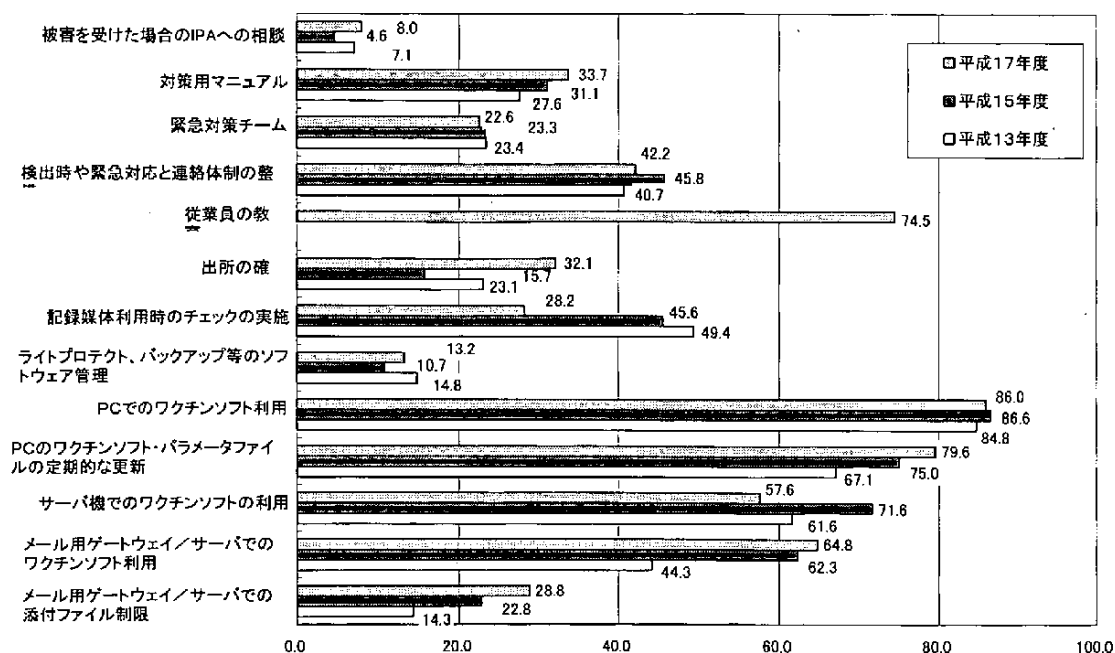


図2-6-3. コンピュータウイルス対策の実施状況(その1)

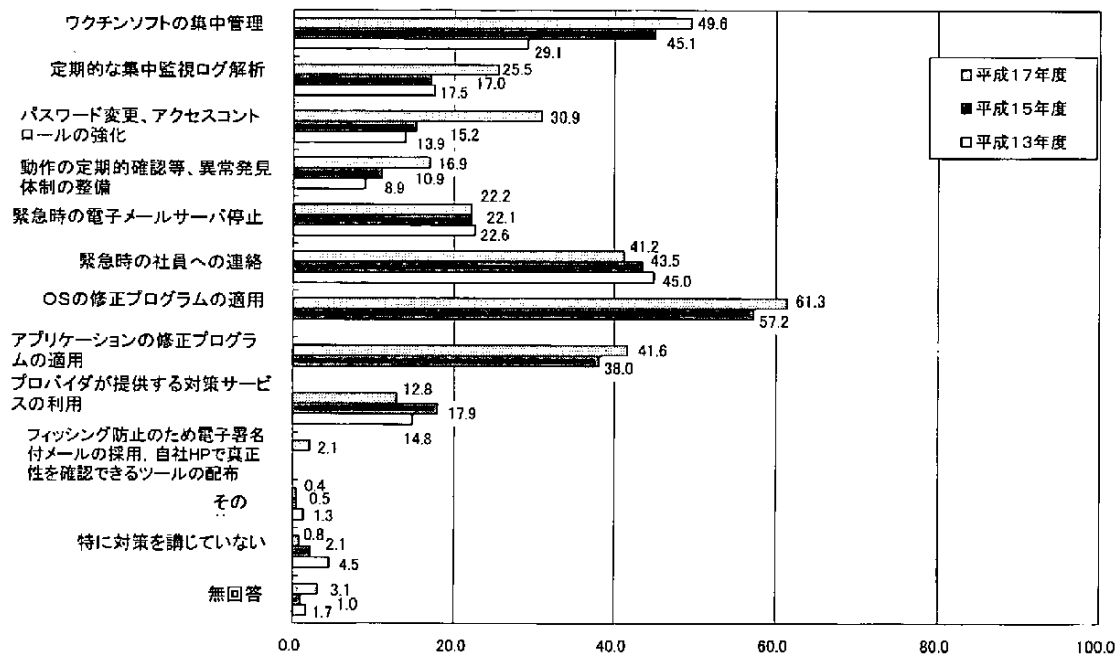


図2-6-4. コンピュータウイルス対策の実施状況(その2)

## 2.7 システム監査・情報セキュリティ監査について

Q40. 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) ⇒Q41へ  | 209 | 40.7  |
| 2   | これから実施する予定がある ⇒Q43へ | 88  | 17.1  |
| 3   | 実施しない ⇒Q42へ         | 204 | 39.7  |
| 無回答 |                     | 13  | 2.5   |
| 計   |                     | 514 | 100.0 |

システム監査を「実施した」事業体の割合は40.7%で、前回調査の35.9%、平成13年度の34.8%と比べると約5ポイント増加した。また、「これから実施する予定がある」を加えると57.8%となり、50%を超えている。これは、平成16年10月にシステム監査基準が改訂されたことや情報セキュリティ監査制度の広がりなどが背景にあると考えられる。

一方、システム監査を「実施しない」事業体は、39.7%となっており、「実施する」事業体とほぼ同率となっている。

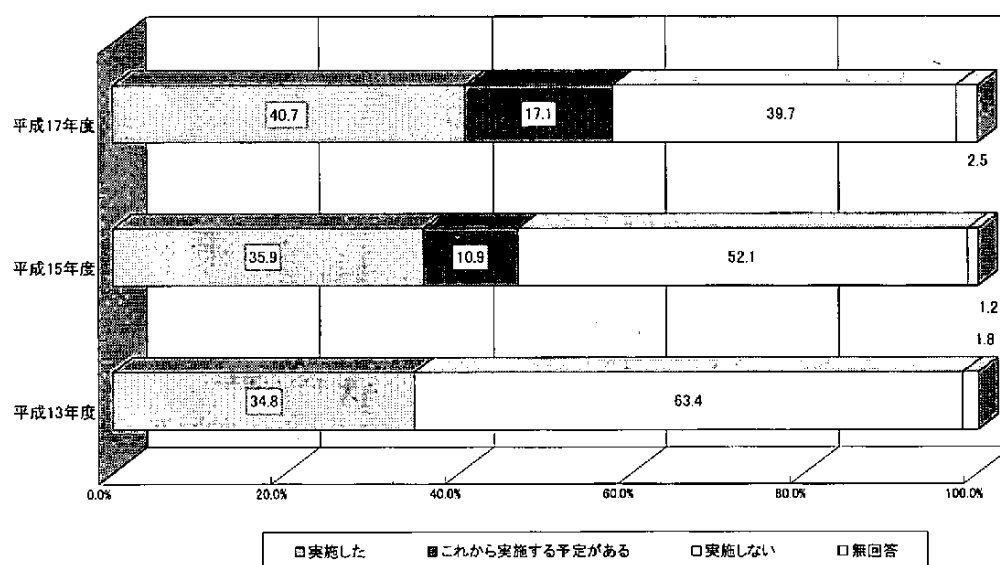


図2-7-1. システム監査の実施状況

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70.3%（≒H15:65.9%、4.4ポイント増）で一番高く、次いで「電気・一般・輸送用機械」53.3%、「情報処理サービス業」48.1%（≒H15:45.9%、2.2ポイント増）となっている。今までは「金融・保険業」と「情報処理サービス業」の二つの業種がシステム監査の実施率が高かったが、今回は、これに「製造業」が加わった。

一方、システム監査の実施率が低い業種は「公共サービス」15.8%（≒H15:15.2%、0.6ポイント増）、「政府・地方公共団体」20.3%（≒H15:13.0%、7.3ポイント増）であり、前回調査と比べると若干改善されてきてはいるが、他の業種や全体と比較してもまだ低い実施率である。公共性を求められるこの二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。

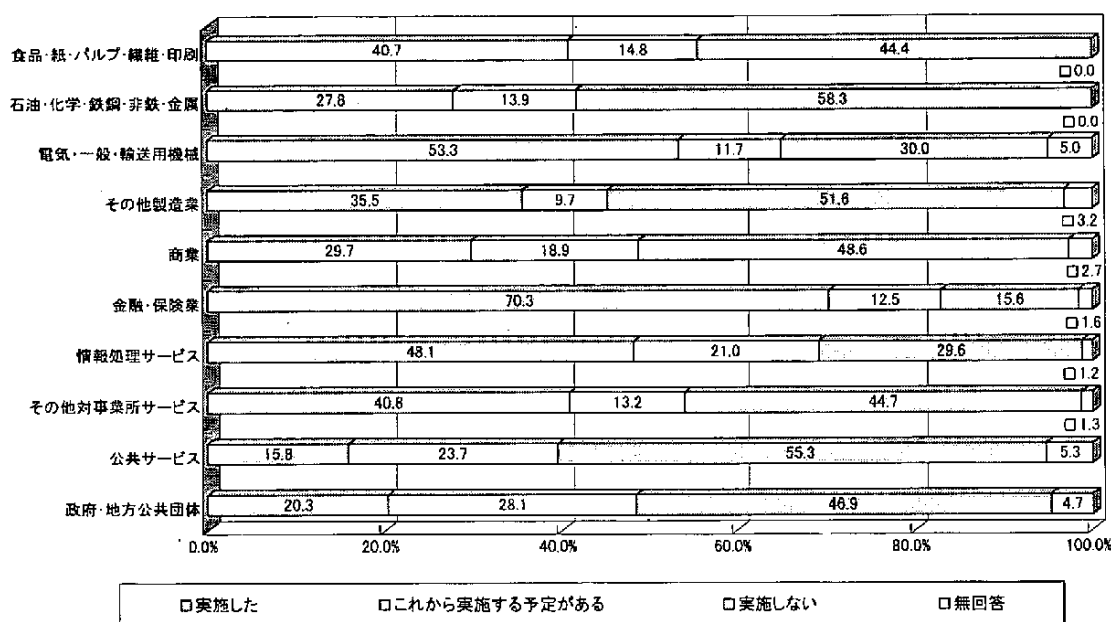


図2-7-2. システム監査の実施状況(業種グループ別)

資本金規模別にみると、規模の大きさとほぼ比例しており、前回調査と傾向は変わっていない。「資本金 500 億円以上」の事業体では「実施した」が 79.5%、「これから実施する予定がある」(15.9%)とあわせると 95.4%になる。なお、前回調査で実施率が 60%を超えていたのは「500 億円以上」の事業体のみであったが、今回調査では「50 億円以上」の事業体が 60%以上となっている。

一方、規模が小さくなるにつれて実施率は低くなっており、「1 億円未満」の事業体での実施率は 2 割に満たない状況にある。

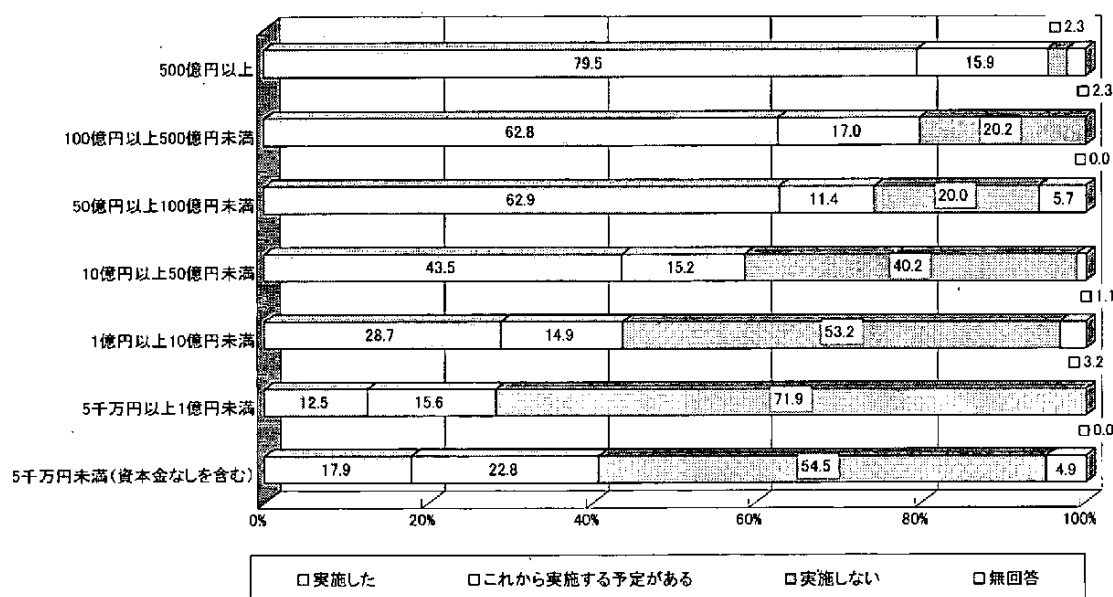


図2-7-3. システム監査の実施状況(資本金規模別)

Q41. Q40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 |                              | 209 | -    |
|------|------------------------------|-----|------|
| 1    | システムに起因する事故・障害が未然に防止できた      | 34  | 16.3 |
| 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   | 81  | 38.8 |
| 3    | 担当者がリスクを考慮しながら業務を実行するようになった  | 99  | 47.4 |
| 4    | システムの信頼性向上対策のレベルが明らかになった     | 89  | 42.6 |
| 5    | システムの有効利用が促進された              | 18  | 8.6  |
| 6    | システムの効率性が確保できた               | 13  | 6.2  |
| 7    | 業務の継続性の確保が図られた               | 37  | 17.7 |
| 8    | 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 | 105 | 50.2 |
| 9    | その他                          | 4   | 1.9  |
| 10   | 効果は得られなかった                   | 10  | 4.8  |
| 無回答  |                              | 2   | 1.0  |

Q40 で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。

システム監査の主な効果としては、「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」が 50.2%（≪H15：38.7%、11.5 ポイント増）、「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 47.4%（≪H15：38.7%、8.7 ポイント増）であった。次いで「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 42.6%（≪H15：35.5%、7.1 ポイント増）、「リスク対策をどこまで考慮すればよいか明らかになった」が 38.8%（≪H15：33.2%、5.6 ポイント増）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に限られている。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「システムの有効利用が促進された」が 8.6%（≪H15：10.6%、2 ポイント減）、「システムの効率性が確保できた」が 6.2%（≪H15：9.7%、3.5 ポイント減）と前回調査よりも減少しており、効果が低い点が危惧される。今後、システム監査と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。

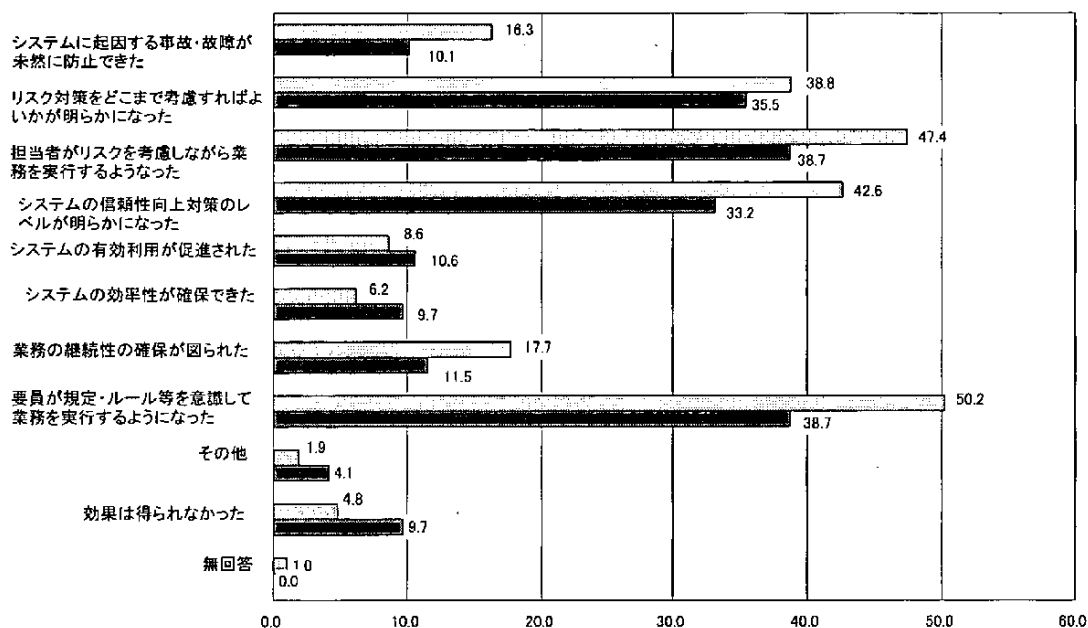


図2-7-4. システム監査実施による効果

Q42. Q40 で「3」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 |                                    | 204 | —    |
|------|------------------------------------|-----|------|
| 1    | 経営者層が重要性を認識していないため                 | 39  | 19.1 |
| 2    | 予算が確保できない                          | 52  | 25.5 |
| 3    | 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 | 85  | 41.7 |
| 4    | システム監査の実施よりもシステム化推進そのものに力点がある      | 52  | 25.5 |
| 5    | システム監査の方法、制度、手続きなどが十分ではない          | 73  | 35.8 |
| 6    | 効果が明確でない                           | 64  | 31.4 |
| 7    | 適切なシステム監査人が見つからない                  | 28  | 13.7 |
| 8    | アウトソーシングしているため                     | 9   | 4.4  |
| 9    | その他                                | 4   | 2.0  |
| 無回答  |                                    | 7   | 3.4  |

Q40 でシステム監査を実施していない事業体に対し、未実施の理由を調査した。

未実施の理由として、「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」が41.7%（ $\rightarrow$ H15:39.0%、2.7ポイント増）、「システム監査の方法、制度、手続きなどが十分ではない」が35.8%（ $\rightarrow$ H15:34.9%、0.9ポイント増）、「効果が明確でない」31.4%（ $\rightarrow$ H15:31.1%、0.3ポイント増）となっている。これは、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、事業体経営に対する情報システムの影響度が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」25.5%（ $\rightarrow$ H15:29.2%、3.7ポイント減）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。

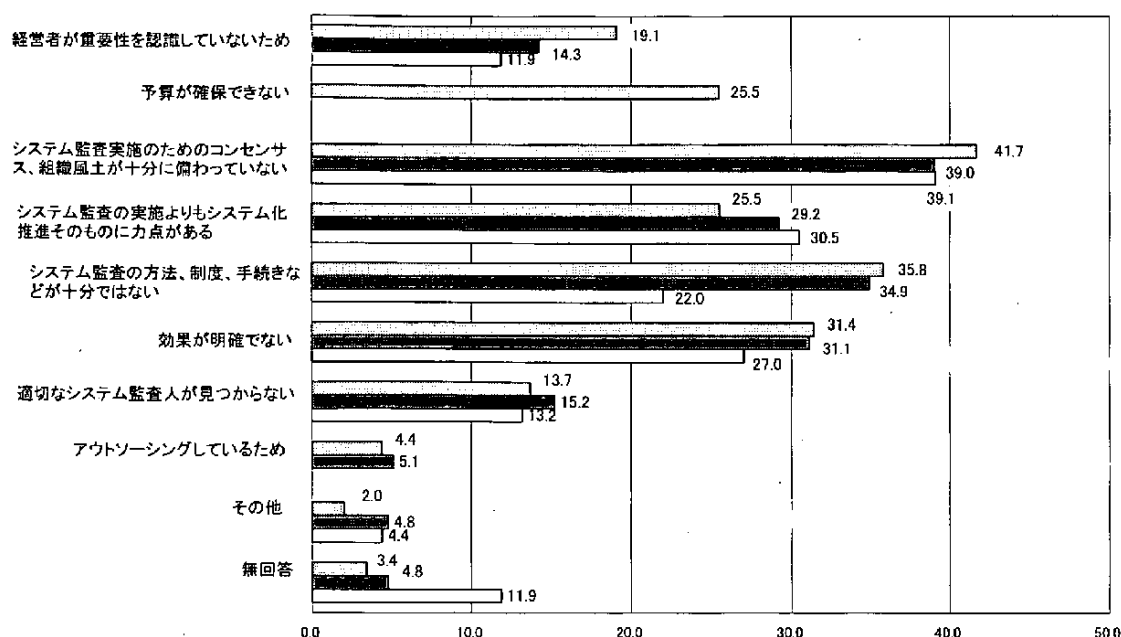


図2-7-5. システム監査未実施の理由

Q43-①過去2年以内に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)

②実施したことがある／予定している場合、それは助言型監査ですか、保証型監査ですか。(複数回答)

| ①情報セキュリティ監査の実施 |             | ①実施<br>状況 | ②監査の種類    |           |
|----------------|-------------|-----------|-----------|-----------|
|                |             |           | ②-1.助言型監査 | ②-2.保証型監査 |
| 1              | 実施した        | 181       | 158       | 87        |
|                |             | 35.2      | 85.9      | 59.6      |
| 2              | これから行う予定がある | 143       | 31        | 13        |
|                |             | 27.8      | 16.8      | 8.9       |
| 3              | 実施しない ⇒Q44へ | 185       |           |           |
|                |             | 36.0      |           |           |
| 無回答            |             | 5         | 1         | 49        |
|                |             | 1.0       | 0.5       | 33.6      |
| 計              |             | 514       |           |           |
|                |             | 100.0     |           |           |

⇒Q45へ

(注)監査の定義

助言型監査: 監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールの改善を目的として、監査対象の情報セキュリティ上の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を行う監査の形態をいう。

保証型監査: 監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールが監査手続を実施した限りにおいて適切である旨(または不適切である旨)を伝達する監査の形態をいう。

情報セキュリティ監査を「実施した」事業体の割合は 35.2%で、前回調査の 18.2%と比べると約2倍となっている。また、「これから実施する予定がある」の 14.3%を加えると 65.0%となり、前回調査の 38.4%を大きく上回る。

一方、情報セキュリティ監査を「実施しない」事業体は 36.0%で、前回調査の 59.3%と比べると 23.3ポイント減少しており、多くの事業体が情報セキュリティ監査制度について肯定的になったことがわかる。全体では、情報セキュリティ監査を「実施した」事業体の割合と「実施しない」事業体とほぼ同じ程度となっており、システム監査と同様の傾向を示している。

なお、前回調査時のセキュリティ監査の実施率が低かった要因には、調査の実施時期が情報セキュリティ監査制度が運用を開始して半年程度しか経過していなかったことなどから、情報セキュリティ監査についてほとんど知られていなかったためと考えられる。2年を経てようやく知名度が上がり、システム監査とほぼ同レベルに至ったといえよう。

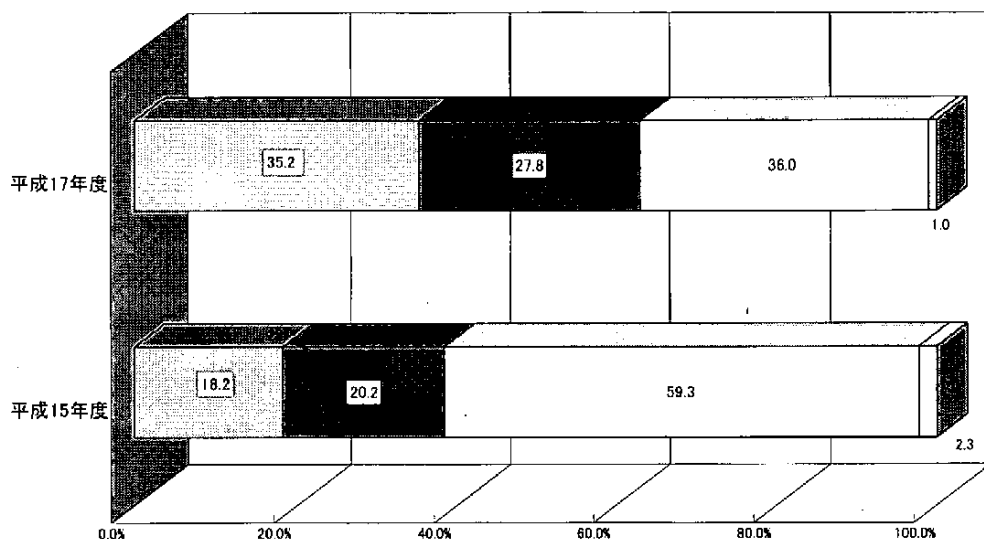


図2-7-6. 情報セキュリティ監査の実施状況

業種グループ別にみると、「政府・地方公共団体」が84.4%、「情報処理サービス業」が82.8%、「金融・保険業」が71.9%となっており、次いで「電気・一般・輸送用機械」が65.0%と続いている。システム監査と比べると、政府・地方公共団体と情報処理サービス業の二つが突出している。これは、平成16年の個人情報保護法の施行などで情報セキュリティを実施した事業体が多いためと考えられる。また、地方公共団体は総務省の方針でもあり、情報セキュリティ監査に積極的に取り組んでいる姿勢がうかがえる。今後は、政府の統一基準の導入もあり、監査実施率が増加すると考えられる。

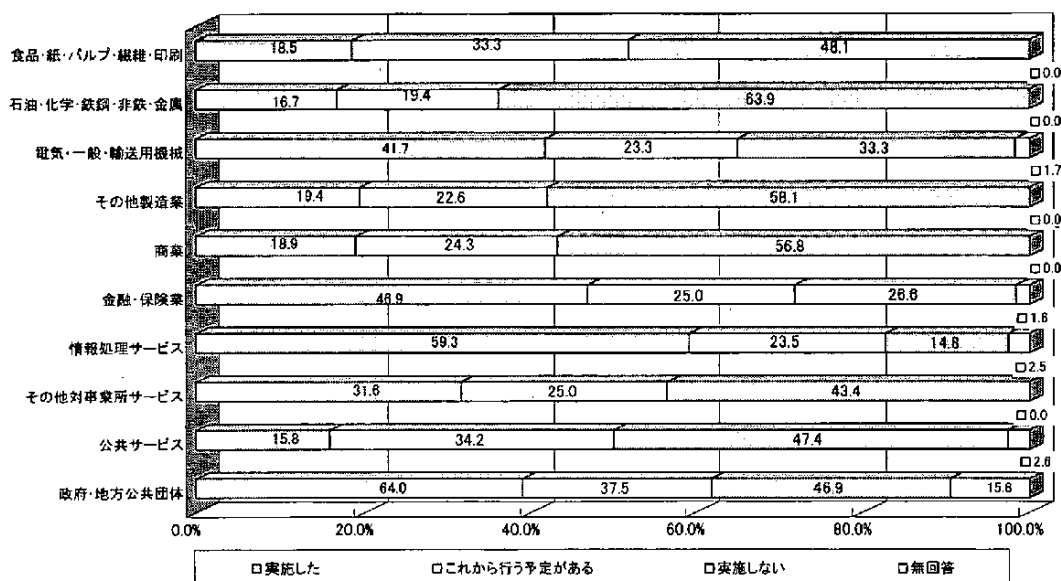


図2-7-7. 情報セキュリティ監査の実施状況(業種グループ別)

資本金規模別にみると、資本金の大きさとほぼ比例している。「10 億円以上 50 億円未満」および「5 千万円未満」の事業体以外は実施率が 30% を越えている。この傾向はシステム監査と共通している。また、資本金 500 億円以上の事業体では「実施した」が 59.1% であり、「これから実施する予定がある」(27.8%) をあわせると 86.4% となっている。

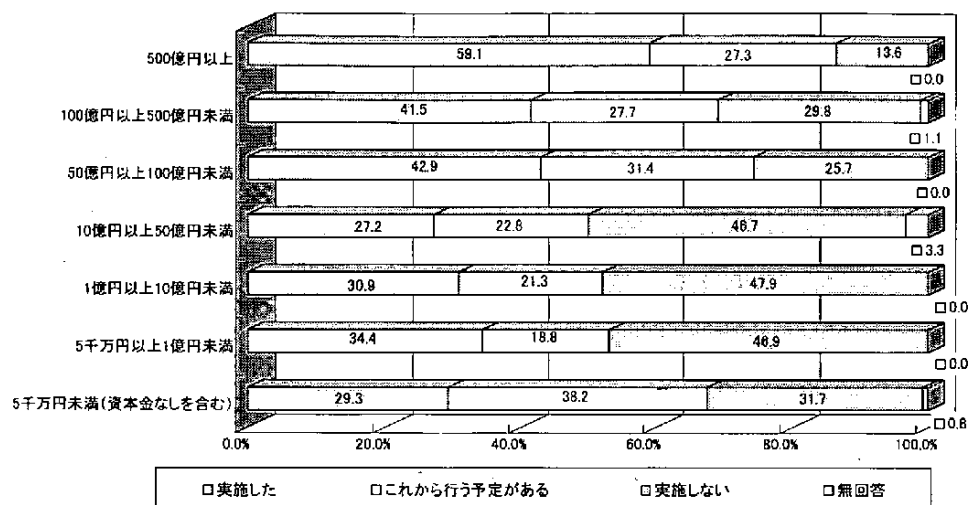


図2-7-8. 情報セキュリティ監査の実施状況(資本金規模別)

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、監査を「実施した」事業体の割合はシステム監査が 40.7% で、情報セキュリティ監査の 35.2% を若干上回る。一方、「これから実施する予定がある」をあわせると、システム監査は 57.8% となり、情報セキュリティ監査の 65.0% に比べると若干低い。また、監査を「実施しない」事業体は、システム監査では 39.7% であるのに対し、情報セキュリティ監査は 36.0% と下回っている。なお、システム監査、情報セキュリティ監査ともに「実施した」事業体の割合と「実施しない」事業体とほぼ同程度となっている。

今回の調査結果からは、情報セキュリティ監査の知名度はこの2年間に浸透しており、ほぼシステム監査と同程度になったことがわかる。今後、監査の場面に応じてどのように使い分けるかなどが重要となってくる。

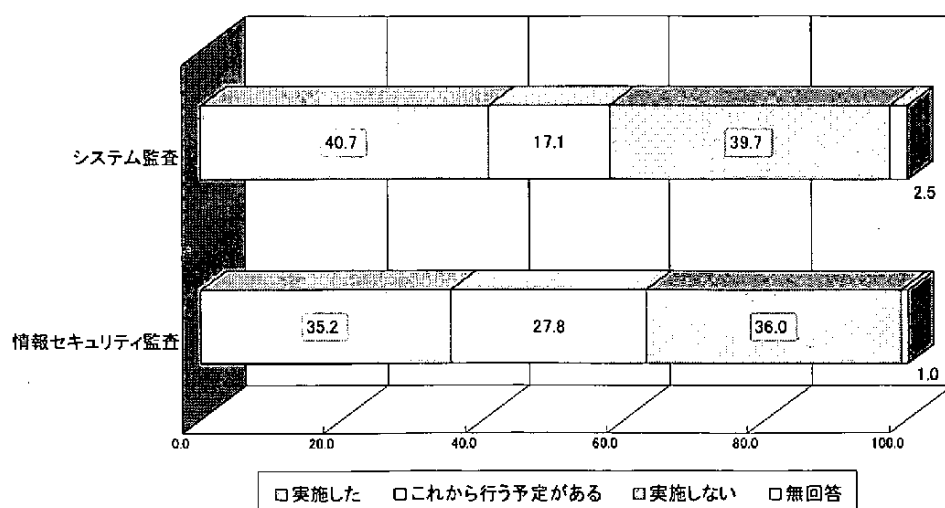


図2-7-9. システム監査および情報セキュリティ監査の実施状況

Q43-②実施したことがある／予定している場合、それは助言型監査ですか、保証型監査ですか。(複数回答)

| ①情報セキュリティ監査の実施 |             | ①実施<br>状況 | ②監査の種類    |           |
|----------------|-------------|-----------|-----------|-----------|
|                |             |           | ②-1.助言型監査 | ②-2.保証型監査 |
| 1              | 実施した        | 181       | 158       | 87        |
|                |             | 35.2      | 85.9      | 59.6      |
| 2              | これから行う予定がある | 143       | 31        | 13        |
|                |             | 27.8      | 16.8      | 8.9       |
|                |             | 36.0      |           |           |
|                |             |           |           |           |
| 無回答            |             | 5         | 1         | 49        |
|                |             | 1.0       | 0.5       | 33.6      |

⇒Q45へ

⇒Q45へ

情報セキュリティ監査は、情報セキュリティの欠陥に対して助言を行うことを目的とする助言型監査と、情報セキュリティに保証を与えることを目的とする保証型監査に分けられる。情報セキュリティ監査を実施した事業体 181 件のうち、「助言型監査」を実施したのは 158 件で全体の 85.9%にあたる。一方、「保証型監査」を実施したのは 87 件、59.6%となっている。なお、保証型監査は助言型監査を実施することもあるため、両者の数字を足すと 100%を越えることになる。この数字からは、助言型監査が多いものの保証型監査もかなり実施されていることがうかがえる。

なお、保証型監査については、定義どおりであれば、監査報告書が公開されたり、何らかの形で第三者が利用するものであるが、このような報告書の存在が知られていないので、この数値は自主的な判断や準規型の監査について述べているものと推測される。いずれにせよ、情報セキュリティ監査制度ができて、それなりに情報セキュリティ監査が実施されていることがうかがえる。なお、業種グループ別にみると、「政府・地方公共団体」で情報セキュリティ監査を実施した 24 団体すべてが助言型監査を実施している。

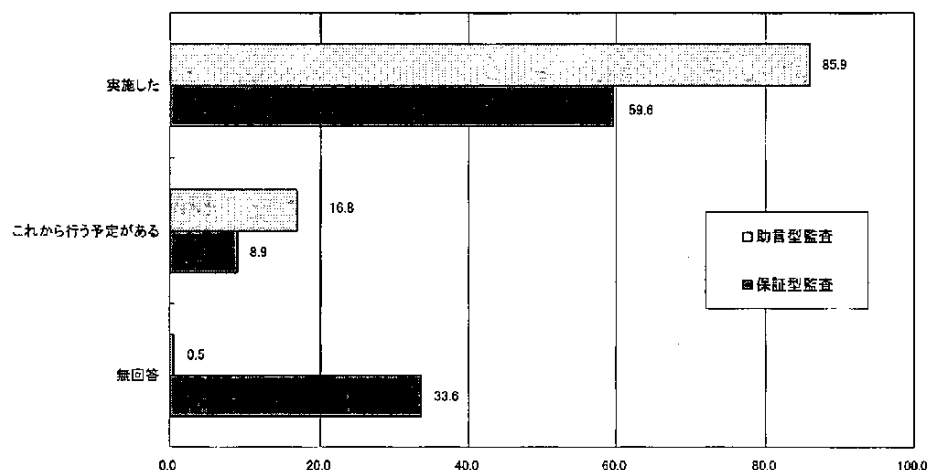


図2-7-10. 情報セキュリティ監査の実施状況

Q44. (Q43 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                                         | 185 | -    |
|----------------------------------------------|-----|------|
| 1 経営者層が重要性を認識していないため                         | 36  | 19.5 |
| 2 予算が確保できない                                  | 49  | 26.5 |
| 3 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     | 83  | 44.9 |
| 4 情報セキュリティ監査制度をよく知らない                        | 40  | 21.6 |
| 5 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                 | 52  | 28.1 |
| 6 効果が明確でない                                   | 55  | 29.7 |
| 7 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                 | 24  | 13.0 |
| 8 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 | 3   | 1.6  |
| 9 その他                                        | 10  | 5.4  |
| 無回答                                          | 5   | 2.7  |

Q43 で情報セキュリティ監査を実施していない事業体に対し、未実施の理由を調査した。

未実施の理由として、「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44.9%（←H15：42.6%、2.3ポイント増）と突出して高い。これは、Q42のシステム監査未実施の理由の「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」（41.7%）とほぼ共通する傾向である。次いで「効果が明確でない」29.7%、「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28.1%、「予算が確保できない」が26.5%と続いている。これは、情報セキュリティ監査制度が発足したものの専門家が少ないなど、まだ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。また、「効果が明確でない」にみられるように、コストがかかる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。

なお、その他の意見としては、「システム監査で代替する」、「監査を受けるまでの体制に達していない」等があげられた。

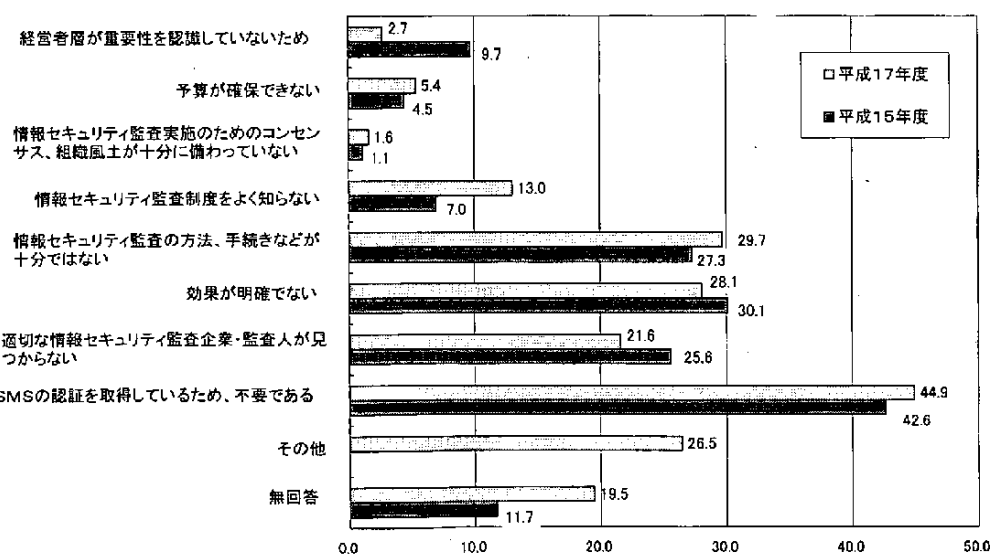


図2-7-11. 情報セキュリティ監査を実施しない理由

## 2.8 個人情報保護について

Q45. 「個人情報保護法」(平成 17 年 4 月 1 日完全施行)および、経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成16年10月公表)を知っていますか。

| 法律／ガイドライン                                                 | 内容を知っている |      | 公表されたことを知っている |      | 知らない |     | 無回答 |     | 計   |       |
|-----------------------------------------------------------|----------|------|---------------|------|------|-----|-----|-----|-----|-------|
| ①個人情報保護法<br>(平成 17 年4月1日完全施行)                             | 452      | 87.9 | 54            | 10.5 | 2    | 0.4 | 6   | 1.2 | 514 | 100.0 |
| ②個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン<br>(平成 16 年 10 月策定) | 361      | 70.2 | 107           | 20.8 | 37   | 7.2 | 9   | 1.8 | 514 | 100.0 |

個人情報保護法は、平成 17 年 4 月 1 日から完全施行されたが、法律の内容を知っている割合は、前回調査の 46.9%から 87.9%へと大幅に増加した。これは、法律が完全施行されたことと、一連の個人情報漏えい事件により各事業体の関心が高まったことの反映と考えられる。また、METI が策定したガイドラインについても、その内容を「知っている」割合が 70.2%と、非常に高い割合となった。これらの結果から、少なくとも個人情報保護として何をすべきかの知識は普及したと考えられる。

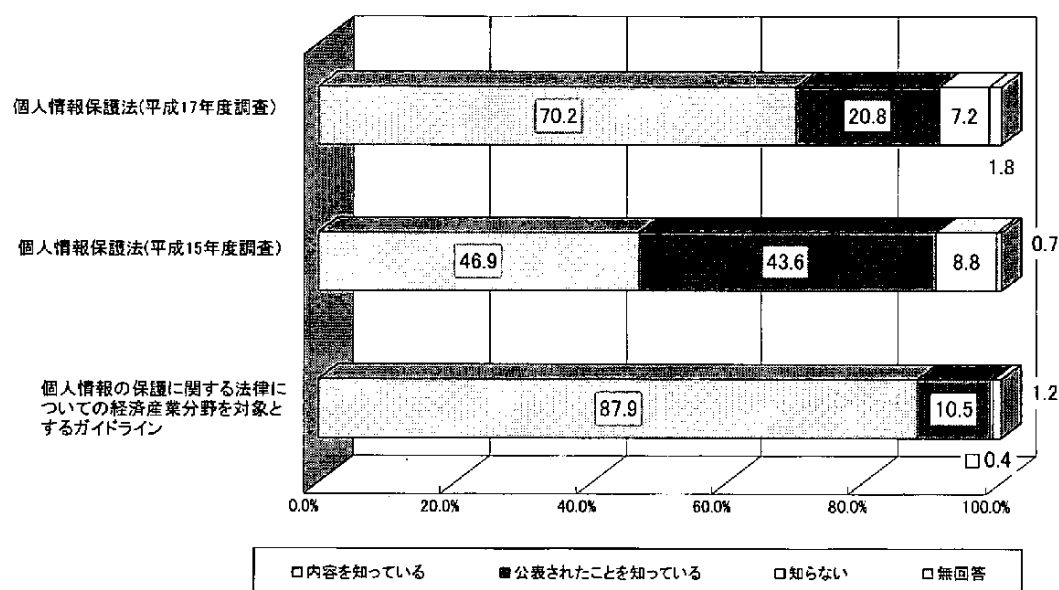


図2-8-1. 個人情報保護法／METIガイドラインの認知度

Q46. 貴事業体は個人情報取扱事業者(過去半年に 5,000 件以上の個人情報を取扱ったことがある)に該当しますか。なお、国の機関、地方公共団体、独立行政法人の場合は、「2」を選択して下さい。

|     |          |     |       |
|-----|----------|-----|-------|
| 1   | 該当する     | 340 | 66.1  |
| 2   | 該当しない(注) | 140 | 27.2  |
| 3   | わからない    | 28  | 5.4   |
| 無回答 |          | 6   | 1.2   |
| 計   |          | 514 | 100.0 |

(注:国の機関、地方公共団体、独立行政法人を含む)

個人情報取扱事業者（過去半年に5,000件以上の個人情報を取り扱ったことがある）に該当しない事業体が27.2%であったのは、国の機関、地方公共団体、独立行政法人が事業者には該当しないことと、従業員規模が小さい事業体で、直接消費者に販売をしていない所が該当しないためと考えられる。一方、従業員規模が5,000名以上の事業体で、該当しないと回答した所も14件あり、自社の従業員情報も個人情報になるという基本的な部分の理解不足も見受けられる。また、「わからない」という回答は、組織内の個人情報洗い出し等を実施していないことを示しており、ガイドラインの再徹底等の施策が必要と考えられる。

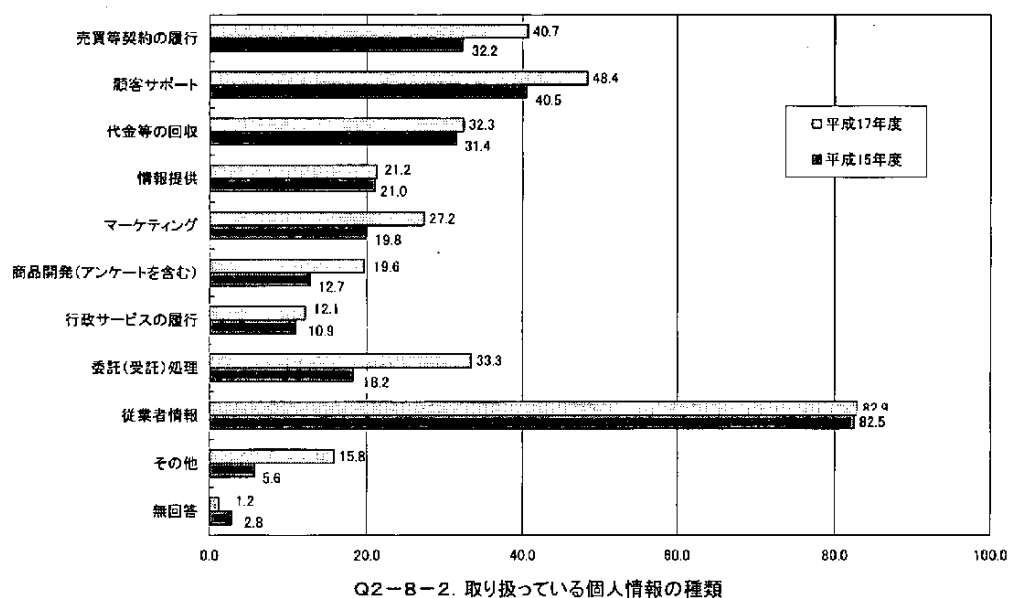
Q47. 貴事業体ではどのような個人情報を取り扱っていますか。(複数回答)

| 回答件数 |                                                                         | 514 | —    |
|------|-------------------------------------------------------------------------|-----|------|
| 1    | 売買等契約の履行                                                                | 209 | 40.7 |
| 2    | 顧客サポート                                                                  | 249 | 48.4 |
| 3    | 代金等の回収                                                                  | 166 | 32.3 |
| 4    | 情報提供                                                                    | 109 | 21.2 |
| 5    | マーケティング                                                                 | 140 | 27.2 |
| 6    | 商品開発(アンケートを含む)                                                          | 101 | 19.6 |
| 7    | 行政サービスの履行                                                               | 62  | 12.1 |
| 8    | 委託(受託)処理                                                                | 171 | 33.3 |
| 9    | 従業者情報(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)                         | 426 | 82.9 |
| 10   | その他<br>例) 学校などの教育機関では在学生・受験者・卒業生等の情報、病院<br>など医療機関では患者情報、公共団体などでは住民情報など。 | 81  | 15.8 |
| 無回答  |                                                                         | 6   | 1.2  |

ここでは個人情報取扱事業者に限定せず、事業体として取り扱っている個人情報について、その種類を回答してもらった。予想されたとおり「従業員情報」を回答した割合が82.9%と非常に高かった。しかし、従業員の情報は、すべての事業体が規模にかかわらず持っているはずであり、「5,000人以下の個人情報も含んで回答する」という質問の主旨が適切に伝わらなかったのか、従業員情報が個人情報に該当することの認識がまだ十分ではないことを示している。

従業員以外の個人情報については、「顧客サポート」48.4%、「売買等の契約の履行」40.7%、「代金等の回収」32.3%、「マーケティング」27.2%、「情報提供」21.2%、「商品開発」19.6%と続いている。これらの項目では、前回調査と比較し「顧客サポート」、「売買等の契約の履行」、「マーケティング」、「商品開発」が軒並み8ポイント程度伸びているのに対し、「代金等の回収」と「情報提供」は横ばいとなったのが対照的である。今回、個人情報を取り扱っているという割合が増えた要因としては、これまで取り扱っていなかった事業体が、新たに個人情報を利用するようになったというよりは、個人情報保護法の施行に伴い、組織内の個人情報を洗い出したところ、自組織で個人情報を使っている部署が新たに判明した結果と考えられる。

「その他」の記述回答には、公共団体による「住民情報」や教育機関による「在学生、卒業生、受験生」、医療機関の「患者情報」等があげられた。



Q48. 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 |                                            | 514             | —   |      |
| 1    | 情報主体(当該個人)から直接収集                           | ⇒Q49へ           | 375 | 73.0 |
| 2    | 従業者から直接収集                                  |                 | 373 | 72.6 |
| 3    | 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 |                 | 279 | 54.3 |
| 4    | 名簿業者等から購入                                  | ⇒Q50または<br>Q51へ | 20  | 3.9  |
| 5    | グループ企業から入手                                 |                 | 48  | 9.3  |
| 6    | 他社から提供を受ける                                 |                 | 39  | 7.6  |
| 7    | 業務委託契約等に基づき預託される                           |                 | 107 | 20.8 |
| 8    | 住民基本台帳から入手                                 |                 | 25  | 4.9  |
| 9    | 新聞、雑誌等メディアからの収集                            |                 | 17  | 3.3  |
| 10   | その他                                        |                 | 17  | 3.3  |
| 無回答  |                                            | 7               | 1.4 |      |

各事業体は取り扱っている個人情報をどのように収集しているのか。収集方法には大きく分けて、①情報主体から直接収集している場合(選択肢1～3)と、②間接的に収集している場合(4～9)があるが、直接収集の方が圧倒的に多い。これは、個人情報保護法の方針にも合致しており、よい傾向である。従業員情報については、Q47で82.9%の回答者が取り扱っていると回答しているが、入手方法として「従業員から直接収集」が72.6%に留まり、質問の主旨が適切に伝わらなかった可能性を残している。

一方、間接収集では、「業務委託契約等に基づき預託される」が前回調査の18.1%から20.8%に、「グループ企業から入手」が前回調査の7.0%から9.3%へと若干増加した。また、今回はじめて調査した「住民基本台帳から入手」は、4.9%と高い数字を示した。

Q49. Q48 で「1」から「3」を回答した場合、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。(単一回答)

|     |                                 |     |       |
|-----|---------------------------------|-----|-------|
| 1   | すべて同意を取っている                     | 306 | 63.1  |
| 2   | (第三者提供など)重要な変更の場合のみ、個別に同意を取っている | 100 | 20.6  |
| 3   | 何もしていない                         | 32  | 6.6   |
| 4   | わからない                           | 34  | 7.0   |
| 無回答 |                                 | 13  | 2.7   |
| 計   |                                 | 485 | 100.0 |

個人情報を直接収集している場合、収集・利用目的について「同意を取っている」割合は、前回調査の 46.1%から 63.1%へと大きく増加した。しかし、「同意を取っていない」が 6.6%、「わからない」が 7.0%もあり、個人情報保護法のコンプライアンスからは、問題を残している。

Q50. Q48 で「4」～「6」を回答した場合、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。(複数回答)

|      |                                           |         |
|------|-------------------------------------------|---------|
| 回答件数 | 75                                        | —       |
| 1    | 情報主体から利用に関し、改めて同意を取っている                   | 15 20.0 |
| 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 68.0 |
| 3    | 何もしていない                                   | 5 6.7   |
| 無回答  |                                           | 8 10.7  |

個人情報を間接収集している場合、「情報主体から改めて同意を取っている」は、前回調査の 14.0%から 20.0%に 6 ポイント増加、「情報提供者に他社提供の同意を確認している」は、前回調査の 35.7%から 68.0 ポイント増加し、68.0%となった。これは個人情報保護法の趣旨が徹底した成果と考えられる。しかし「何もしていない」事業体も 6.7%ある。個人情報保護法第 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禁止が定められており、情報主体から個人情報の開示請求があった場合にトラブルに巻き込まれる可能性を考慮し、未実施の事業体を含め、情報主体に対する利用目的の同意について、十分な注意が必要である。

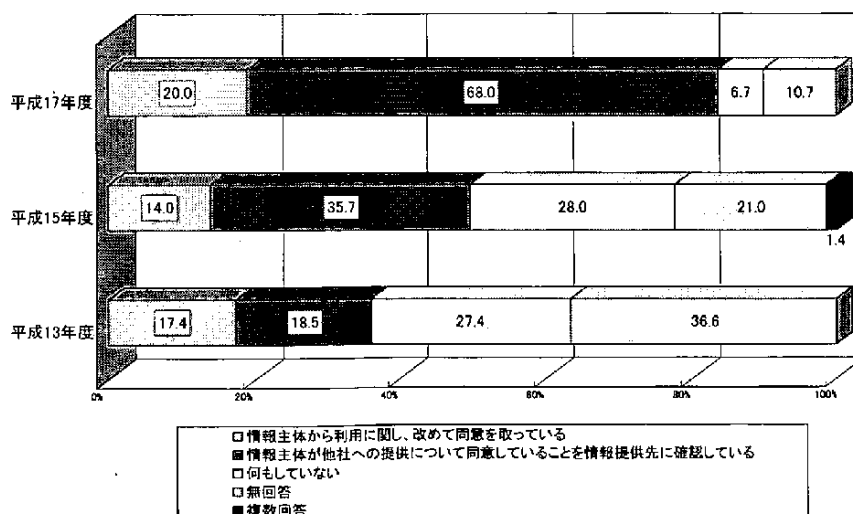


図2-8-3. 間接収集の際の情報主体への同意の有無

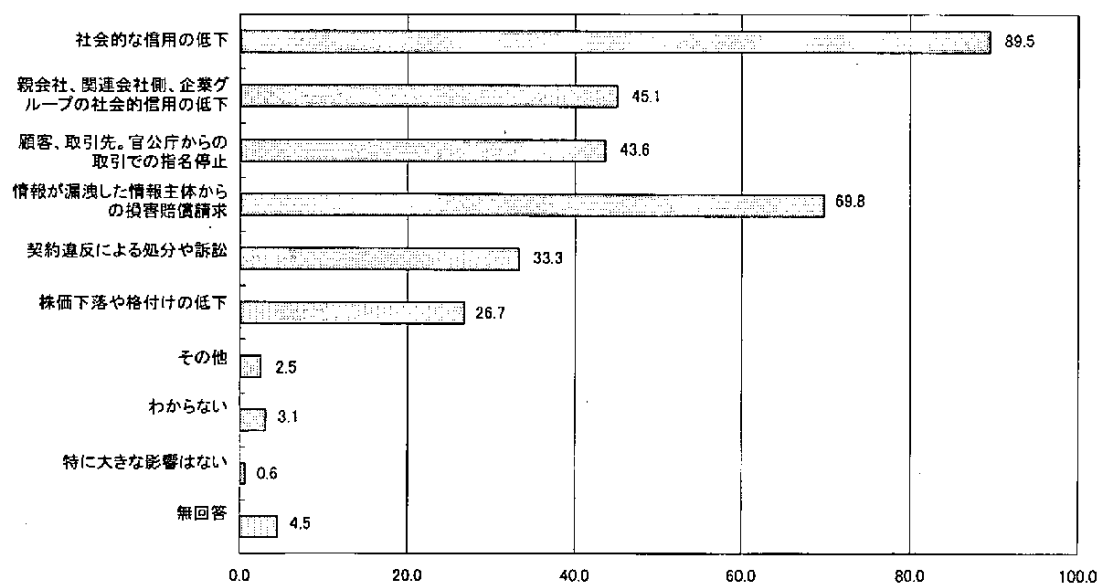
Q51. 個人情報の漏えいにより深刻な被害を及ぼす事項をどのように認識していますか。(複数回答)

| 回答件数                                | 514 | —    |
|-------------------------------------|-----|------|
| 1 社会的な信用の低下(マスメディアに対するイメージダウンを含む)   | 460 | 89.5 |
| 2 親会社や関連会社側、企業グループの社会的信用の低下         | 232 | 45.1 |
| 3 顧客や取引先、官公庁からの取引での指名停止             | 224 | 43.6 |
| 4 情報が漏えいした情報主体からの損害賠償請求(裁判費用、期間を含む) | 359 | 69.8 |
| 5 契約違反による処分や訴訟                      | 171 | 33.3 |
| 6 株価下落や格付けの低下                       | 137 | 26.7 |
| 7 その他                               | 13  | 2.5  |
| 8 わからない                             | 16  | 3.1  |
| 9 特に大きな影響はない                        | 3   | 0.6  |
| 無回答                                 | 23  | 4.5  |

個人情報に漏えいした場合の影響について、どう考えているかを調査した。

「社会的な信用の低下」が 89.5%、「情報主体からの損害賠償請求」が 69.8%、「親会社や関連会社、企業グループの社会的信用の低下」が 45.1%、「取引先での指名停止」が 43.6%、「契約違反による処分や訴訟」が 33.3%となった。基本的には、自社や親会社の社会的な信用が低下して売上の減少を招いたり、自主規制を含む業務停止による売上の減少、損害賠償や契約違反に対する訴訟による金銭的なダメージを受け、結果として株価の下落や格付けの低下につながると考えられる。金銭的なダメージを算出するのは容易ではないが、社内でコンセンサスを作っておくと、個人情報保護に対する経営者の意識向上にもつながるので、是非検討すべきである。

「その他」の記述回答としては、「漏洩した情報主体およびその家族への被害」、「行政全般の信用低下」、「住民への影響」等があげられた。



Q2-8-4. 個人情報漏えいが及ぼす被害の影響度合い

Q52. 個人情報保護対策として、以下の対策を実施していますか。

| 対 策                                          | 個人情報保護法<br>施行以前から実施<br>している |      | 現在対策を<br>実施している |      | 今後新たに実施を<br>予定している |      |
|----------------------------------------------|-----------------------------|------|-----------------|------|--------------------|------|
|                                              |                             |      |                 |      |                    |      |
| ①管理責任者を置く(保護体制(役割、責任、権限)を確立する                | 187                         | 36.4 | 234             | 45.5 | 36                 | 7.0  |
| ②個人情報保護に関する規程を定め運用する                         | 184                         | 35.8 | 243             | 47.3 | 44                 | 8.6  |
| ③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認定を受ける)運用する | 84                          | 16.3 | 49              | 9.5  | 77                 | 15.0 |
| ④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、定期的に教育する         | 133                         | 25.9 | 178             | 34.6 | 92                 | 17.9 |
| ⑤定期的に監査(内部監査／外部監査)を実施する                      | 121                         | 23.5 | 133             | 25.9 | 116                | 22.6 |
| ⑥リスク分析を実施して必要な安全対策を構築する                      | 110                         | 21.4 | 96              | 18.7 | 155                | 30.2 |
| ⑦苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応する           | 156                         | 30.4 | 180             | 35.0 | 63                 | 12.3 |
| ⑧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る          | 121                         | 23.5 | 137             | 26.7 | 129                | 25.1 |
| ⑨個人情報漏えい保険に加入する                              | 28                          | 5.4  | 40              | 7.8  | 54                 | 10.5 |

| 対 策                                          | 実施の予定はない |      | 無回答 |     | 計   |       |
|----------------------------------------------|----------|------|-----|-----|-----|-------|
|                                              |          |      |     |     |     |       |
| ①管理責任者を置く(保護体制(役割、責任、権限)を確立する                | 46       | 8.9  | 11  | 2.1 | 514 | 100.0 |
| ②個人情報保護に関する規程を定め運用する                         | 34       | 6.6  | 9   | 1.8 | 514 | 100.0 |
| ③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認定を受ける)運用する | 282      | 54.9 | 22  | 4.3 | 514 | 100.0 |
| ④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、定期的に教育する         | 96       | 18.7 | 15  | 2.9 | 514 | 100.0 |
| ⑤定期的に監査(内部監査／外部監査)を実施する                      | 126      | 24.5 | 18  | 3.5 | 514 | 100.0 |
| ⑥リスク分析を実施して必要な安全対策を構築する                      | 134      | 26.1 | 19  | 3.7 | 514 | 100.0 |
| ⑦苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応する           | 100      | 19.5 | 15  | 2.9 | 514 | 100.0 |
| ⑧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る          | 106      | 20.6 | 21  | 4.1 | 514 | 100.0 |
| ⑨個人情報漏えい保険に加入する                              | 351      | 68.3 | 41  | 8.0 | 514 | 100.0 |

現在行っている個人情報保護対策として、管理面を主にその実施率について調査した。この結果、「管理責任者を置き保護体制を確立する」が前回調査の 36.0%から 81.9%へ、「個人情報保護に関する規程の設定」が前回調査の 34.7%から 83.1%へ、「個人情報に関する社員教員」が前回調査の 25.0%から 60.5%と大幅に増加した。これらの項目は、個人情報の保護を組織として継続的に行っていくためには必須の項目であり、前回調査の後に個人情報保護法が施行されたためか、大きく改善されている。今後、実施率を 100%に近づける努力を、特に社員教育については一層の改善が望まれる。

次に PDCA の計画とチェックの部分では、「リスク分析の実施」が前回調査の 13.4%から 40.1%へ、「定期的な監査の実施」が 21.5%から 49.4%へ、「苦情相談・処理窓口の設置」が 24.3%から 65.4%へ、「対応処置の設定」が 15.9%から 50.2%へ増加している。また、領域が不足しているという認識は回答者も感じており、今後の実施予定では、「リスク分析の実施」と「定期的な監査

の実施」が高い数字になっており、これに対する支援策が望まれる。

なお、今回調査では「個人情報漏えい保険への加入」はまだ少なく13.2%、今後も「加入の予定はない」との回答が7割近くを占めているが、個人情報漏えい事故が多発している現状から、今後は保険加入率が増えてくることが予想される。

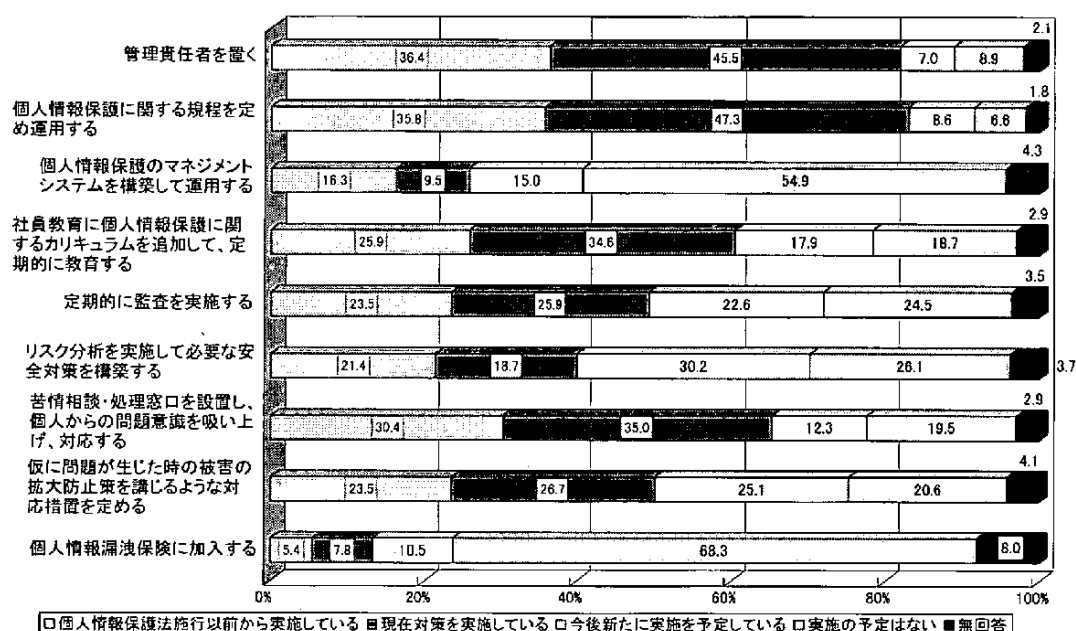


図2-8-5. 個人情報保護対策の実施状況

Q53. 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。(単一回答)

|     |                                      |     |       |
|-----|--------------------------------------|-----|-------|
| 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            | 5   | 1.0   |
| 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 | 18  | 3.5   |
| 3   | 対策を講じているが、リスクはあると認識している              | 377 | 73.3  |
| 4   | 何度がヒヤリ・ハットした経験があり、リスクがあると認識している      | 30  | 5.8   |
| 5   | 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         | 50  | 9.7   |
| 6   | その他                                  | 2   | 0.4   |
| 7   | 特に認識していない                            | 20  | 3.9   |
| 無回答 |                                      | 12  | 2.3   |
| 計   |                                      | 514 | 100.0 |

個人情報の管理状況に対するリスク認識を調査したが、前回調査に比べ大きく異なった結果となった。「対応策を講じているので、リスクはないと認識している」が前回調査の6.4%から1.0%へ5.4ポイント減、「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」が前回調査の17.9%から3.5%へ14.4ポイント減と、リスクがないと認識している割合が顕著に下がっている。一方、「何度がヒヤリ・ハットした経験があり、リスクがあると認識している」が前回調査の20.0%から5.8%へ14.2ポイント減、「いつ問題が発生してもおかしくない状況であると認識している」が前回調査の27.9%から9.7%へ18.2ポイント減少しており、保護対策が一定の成果を上げていると考えられる。

この結果、多くの回答が今回始めて設けた「対策を講じているが、リスクはあると認識している」に集中し、73.3%という結果になったと考えられる。

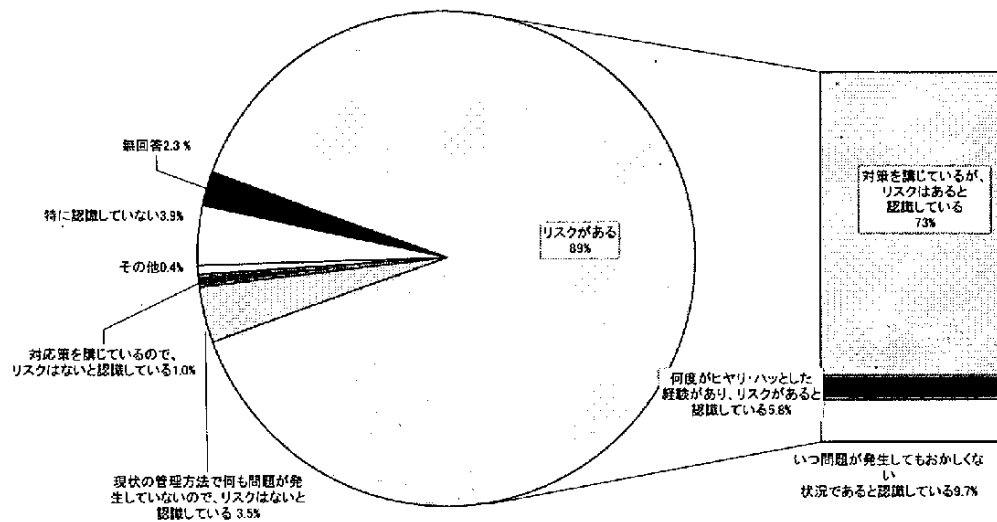


図2-8-6. 個人情報管理状況のリスク認識度

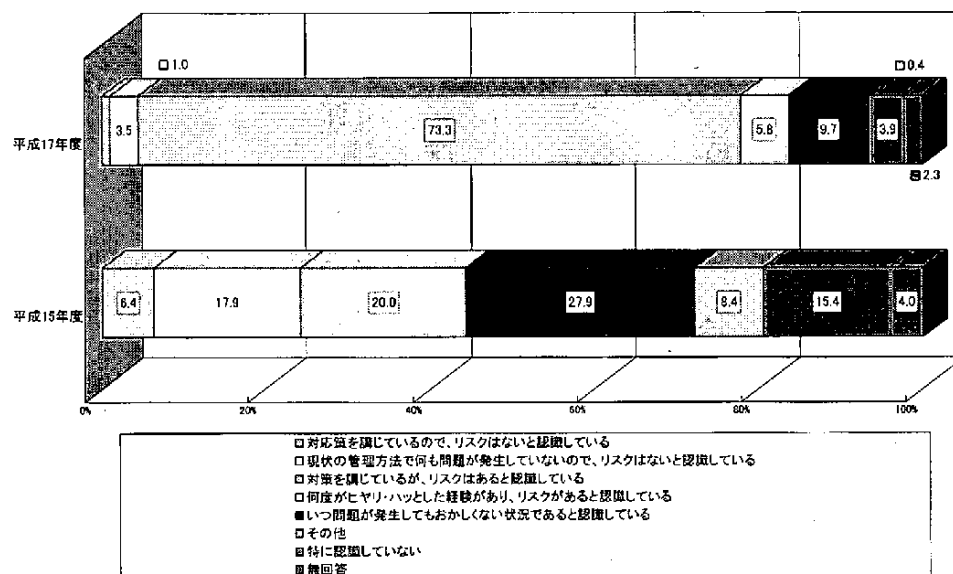


図2-8-7. 個人情報の管理状況に対するリスク認識

Q54. 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 |                       | 514 | -    |
|------|-----------------------|-----|------|
| 1    | 機密保持義務                | 414 | 80.5 |
| 2    | 責任分担(漏えい事故発生時の損害賠償 等) | 248 | 48.2 |
| 3    | 個人情報の適正な管理(廃棄、返却、授受等) | 344 | 66.9 |
| 4    | 目的外使用・再委託の制限          | 334 | 65.0 |
| 5    | 個人情報の取扱いに関する監査の実施     | 174 | 33.9 |
| 6    | その他                   | 12  | 2.3  |
| 7    | 外部委託を行っていない           | 75  | 14.6 |
| 無回答  |                       | 13  | 2.5  |

個人情報の処理を外部に委託する時には、委託する側が適切な監督を行う義務を持っていることが個人情報保護法第22条で定められている。METTが公表した「個人情報の保護に関する法律についての 経済産業分野を対象とするガイドライン」によれば、「機密保持義務」、「個人情報の適正な管理」、「目的外使用・再委託の制限」、「目的外使用・再委託の制限」、「個人情報の取扱いに関する監査の実施」については、実施が望ましい項目として定義されている。実施率が一番高い「機密保持義務」でも、外部委託を行っている426事業体（82.9%）の内、80.5%しか実施しておらず、今後、是非実施を検討すべきである。

その他の記述回答では、「事故発生時の報告義務」、「収集の制限」、「複写／複製の禁止」等があげられた。

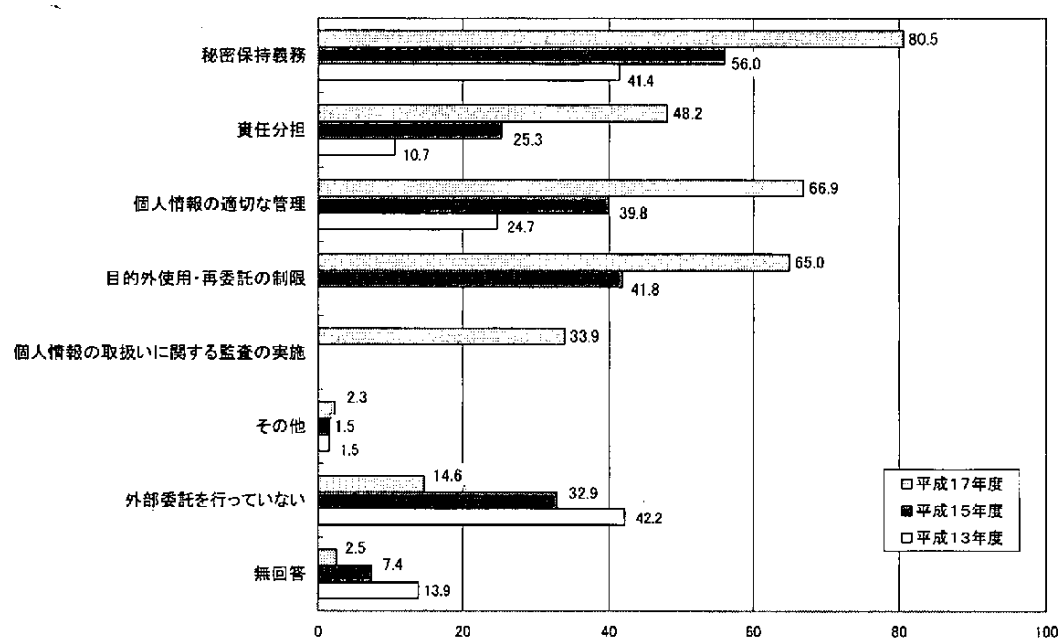


図2-8-9. 個人情報を外部委託する際の契約条項

Q55. プライバシーマーク制度を知っていますか。

|     |                |       |     |       |
|-----|----------------|-------|-----|-------|
| 1   | すでに認定されている     | ⇒Q56へ | 74  | 14.4  |
| 2   | 認定申請中である       | ⇒Q56へ | 22  | 4.3   |
| 3   | 取得のための準備を行っている | ⇒Q56へ | 38  | 7.4   |
| 4   | 認定を受ける予定はない    | ⇒終了   | 346 | 67.3  |
| 5   | 知らない           | ⇒終了   | 23  | 4.5   |
| 無回答 |                |       | 11  | 2.1   |
| 計   |                |       | 514 | 100.0 |

Q56. Q55 で「1」～「3」を回答した場合、プライバシーマークの取得目的は何ですか。（複数回答）

|      |                                        |     |      |
|------|----------------------------------------|-----|------|
| 回答件数 |                                        | 134 | —    |
| 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、信頼性を確保できる | 129 | 96.3 |
| 2    | 取引先からの要請による（入札条件となっている）                | 32  | 23.9 |
| 3    | その他                                    | 5   | 3.7  |
| 無回答  |                                        | 3   | 2.2  |

JIPDECが運用しているプライバシーマーク制度については、「すでに認定されている」が14.4%、「認定申請中」が4.3%、「取得のための準備を行っている」が7.4%となった。これらを合計すると、全体の約4分の1がプライバシーマークの認定を受けようとしており、非常に高い認知度を得ていると考えられる。一方、「認定を受ける予定はない」という回答も67.3%に上っており、自組織が扱っている個人情報の規模や、リスクを考慮して、自組織として手適切な判断が必要となる。

一方、プライバシーマークを取得したり、これからしようとしている事業体は、その目的として「システムや社内セキュリティ管理体制の構築」や、「取引先からの必須要件として指示」を取得の目的としている。今後は、個人情報の外部委託に際しても、委託先が機密を守れることが重要な選定要件になると考えられる。

## 2.9 その他（記述回答）

本調査では、「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」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に関する問題点」について、自由に記載していただいた意見を一部抜粋、要約して紹介する。

### （１）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

- ・日本版 SOX 法を視野にいたした対応
- ・ISO27001 への対応
- ・安全、安心なネットワーク環境。
- ・コンピュータウイルス、スパムメール対策
- ・スパイウェア等、Web にかかるセキュリティ強化と利便性を備えたサービスの提供。
- ・内部漏えいに対する有効な検知ツール
- ・人的対策の強化（法の整備、罰則強化、技術的・物理的対策の強化） 等

### （２）情報セキュリティ対策に関する問題点

- ・関連会社を含めた情報セキュリティ対策レベルの統一化
- ・指紋認証、IC カード、手のひら認証等、認証手段についての業界内での統一が図られていない
- ・教職員を含む従業員に対するセキュリティ対策（教育）の徹底
- ・経営者層の理解不足
- ・セキュリティ対策予算の確保
- ・要員不足
- ・どこまでやればよいのか、基準・指針が明確になっていない
- ・全社的な事業継続計画の策定 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 | Q3. 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。                                                                                   | Q40. 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。                                               |
|     |                                                                                                                               | Q43-①過去2年以内に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 | Q4. 経営者層は次の事項について関心が高いですか。                                                                                                    | Q3. 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。                                    |
|     |                                                                                                                               | Q5. 情報システム関連、情報セキュリティ関連、個人情報保護漏洩のリスクが貴事業体の経営に重大な影響(経営危機、倒産等)を与えenと思いますか。       |
| 3.3 | Q6. 情報セキュリティガバナンス(Q4の「注1」参照)の観点から、情報セキュリティ対策にあたり、どの関係者を考慮に入れていますか。                                                            | Q25. 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。                                   |
|     |                                                                                                                               | Q26. 災害に対する情報システムのバックアップ対策を講じていますか。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。 |
|     |                                                                                                                               | Q53. 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。                                        |
| 3.4 | Q8. 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、または実施を予定しているものはどれですか？ | Q18. 情報セキュリティの確保にとり、基本的に重要な要素は何だと思いますか。(複数回答)                                  |
|     |                                                                                                                               | Q30-8. 貴事業体では従業員に対し、情報セキュリティの一般知識に関する教育を実施していますか。                              |
|     |                                                                                                                               | Q40. 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。                                               |
|     |                                                                                                                               | Q43. 情報セキュリティ監査を実施したことがありますか。                                                  |
| 3.5 | Q13-①貴事業体の基幹システムは、過去1年間に、システムの運用に悪影響を与えたか、または事業中断につながるシステムダウンが発生しましたか。                                                        | Q22-9. 貴事業体として重要と思われる要素:事業継続管理(災害対策、障害対策など)                                    |
|     |                                                                                                                               | Q24. 「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)。        |
|     |                                                                                                                               | Q25. (Q24 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)        |
| 3.6 | Q13-②システムダウンはシステムの運用に悪影響を与えたか、さらに事業中断につながるものでしたか。(選択肢1～2)                                                                     | Q22-9. 貴事業体として重要と思われる要素:事業継続管理(災害対策、障害対策など)                                    |
|     |                                                                                                                               | Q24. 「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)。        |

|      | 質問項目                                                                   | クロス集計対象項目                                                              |
|------|------------------------------------------------------------------------|------------------------------------------------------------------------|
| 3.7  | Q14-①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)                      | Q24.「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)。 |
| 3.8  | Q18. 情報セキュリティの確保にとり、基本的に重要な要素は何だと思えますか。(複数回答)                          | Q21. 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)          |
|      |                                                                        | Q30-8. 貴事業体では従業員に対し、情報セキュリティの一般知識に関する教育を実施していますか。                      |
|      |                                                                        | Q31. 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。(単一回答)                            |
| 3.9  | Q22. 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下さい。(選択肢 1～10)   | Q22 の優先順位(1位×2位)                                                       |
| 3.10 | Q24.「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)。 | Q8-3. 情報システムに係わるリスク分析を実施していますか。                                        |
| 3.11 | Q25. 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。                         | Q9. 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)                       |
| 3.12 | Q41. 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えますか。                           | Q15. 基幹システムにおける MTBF(平均故障間隔)は何時間ですか。                                   |
| 3.13 | Q46. 貴事業体は個人情報取扱事業者(過去半年に 5,000 件以上の個人情報を取扱ったことがある)に該当しますか。            | Q47. 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。                                        |
|      |                                                                        | Q48. 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。                                    |
|      |                                                                        | Q49. Q48 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。   |
|      |                                                                        | Q51. 個人情報の漏洩により深刻な被害を及ぼす事項をどのように認識していますか。                              |
|      |                                                                        | Q53. 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。                                |
|      |                                                                        | Q54. 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。                                   |

なお、上記のクロス以外にも複数の設問に対しクロス集計を行ったが、回収数が少なかったことが影響し、設問間の明確な関係がみられなかったため、ここでは省略している。

### 3.1 Q3のクロス集計

Q3. 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。

クロス対象

Q40. 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。

Q43-①過去2年以内に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 Q40 とのクロス集計

Q40. 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。

| Q3. 情報<br>リスクマネジメント \ Q40. システム監査 | 回 答<br>件 数 | 1. 実施した |      | 2. これから実施<br>する予定がある |      | 3. 実施しない |      | 4. 無回答 |     |
|-----------------------------------|------------|---------|------|----------------------|------|----------|------|--------|-----|
| 1. 重要と考え、実践している                   | 210        | 120     | 57.1 | 34                   | 16.2 | 51       | 24.3 | 5      | 2.4 |
| 2. 重要と考えている                       | 255        | 78      | 30.6 | 45                   | 17.6 | 124      | 48.6 | 8      | 3.1 |
| 3. さらに強化する予定がある                   | 30         | 9       | 30.0 | 7                    | 23.3 | 14       | 46.7 | 0      | 0.0 |
| 4. 考えていない                         | 7          | 0       | 0.0  | 1                    | 14.3 | 6        | 85.7 | 0      | 0.0 |
| 5. わからない                          | 7          | 1       | 14.3 | 0                    | 0.0  | 6        | 85.7 | 0      | 0.0 |
| 6. 無回答                            | 5          | 1       | 20.0 | 1                    | 20.0 | 3        | 60.0 | 0      | 0.0 |
| 7. 計                              | 514        | 209     | 40.7 | 88                   | 17.1 | 204      | 39.7 | 13     | 2.5 |

情報リスクマネジメントを「重要と考え、実践している」事業体は 57.1%が、「重要と考えている」事業体は 30.6%がシステム監査を実施している。また、情報リスクマネジメントを「さらに強化する予定がある」事業体では、システム監査を「実施しない」（46.7%）が「実施した」（30.0%）を上回っている。一方、情報リスクマネジメントを「考えていない」および「わからない」事業体では、システム監査を「実施しない」（ともに 85.7%）と回答している。すなわち、情報リスクマネジメントは、システム監査の実施と強い相関があると考えられる。

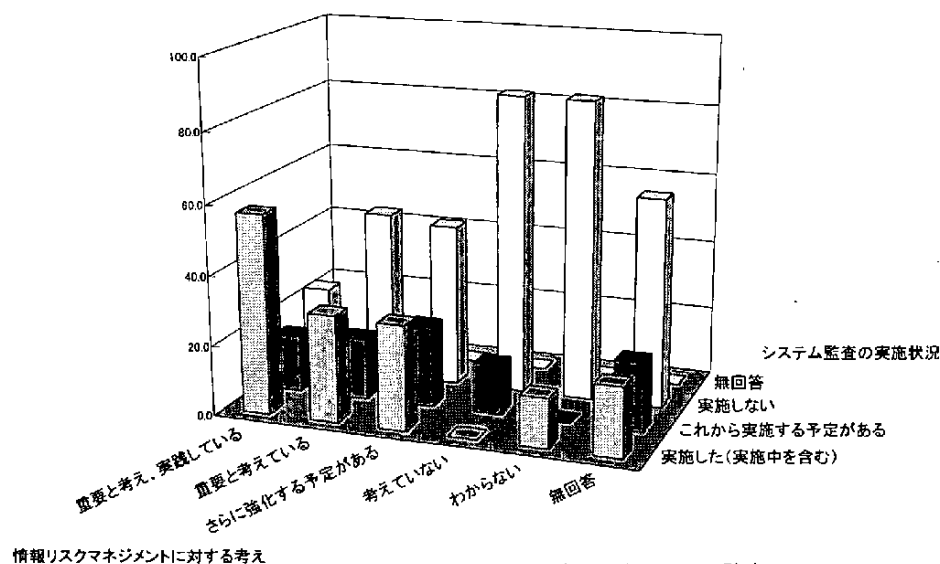


図3-1-1. 情報リスクマネジメントとシステム監査

### 3.1.2 Q43-①とのクロス集計

Q43-①過去2年以内に情報セキュリティ監査を実施したことがありますか。

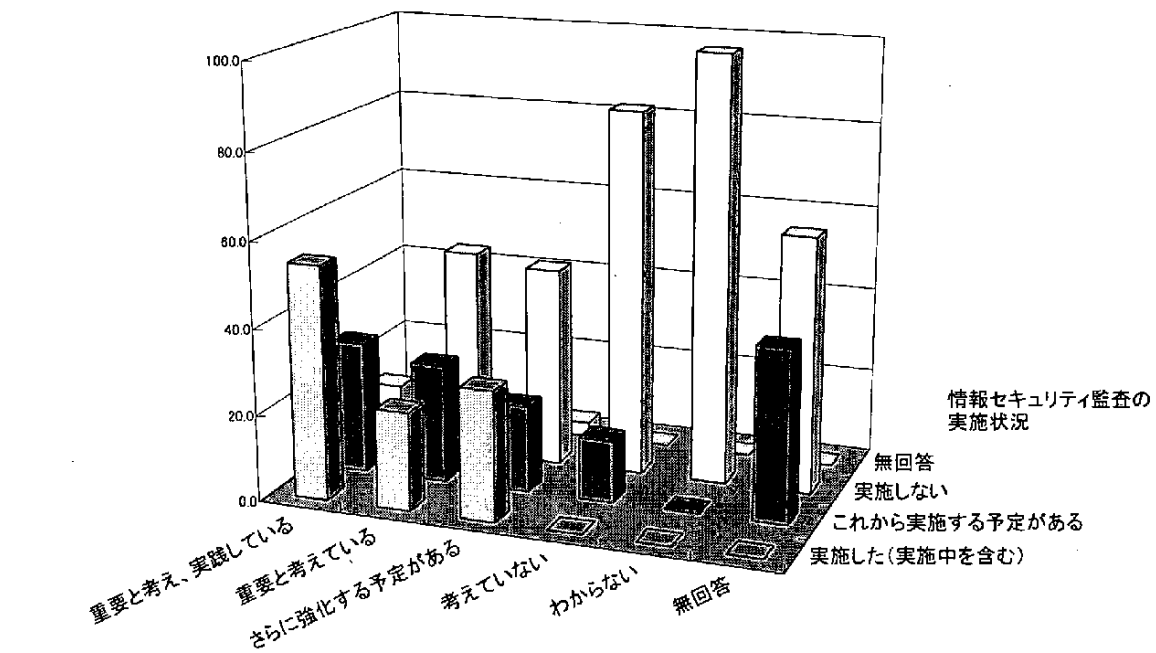
| Q43.情報セキュリティ監査<br>Q3. 情報リスクマネジメント | 回 答<br>件数 | 1. 実施した |      | 2. これから行<br>う予定が<br>ある |      | 3. 実施<br>しない |       | 4. 無回答 |     |
|-----------------------------------|-----------|---------|------|------------------------|------|--------------|-------|--------|-----|
| 1. 重要と考え、実践している                   | 210       | 114     | 54.3 | 64                     | 30.5 | 30           | 14.3  | 2      | 1.0 |
| 2. 重要と考えている                       | 255       | 58      | 22.7 | 70                     | 27.5 | 125          | 49.0  | 2      | 0.8 |
| 3. さらに強化する予定がある                   | 30        | 9       | 30.0 | 6                      | 20.0 | 14           | 46.7  | 1      | 3.3 |
| 4. 考えていない                         | 7         | 0       | 0.0  | 1                      | 14.3 | 6            | 85.7  | 0      | 0.0 |
| 5. わからない                          | 7         | 0       | 0.0  | 0                      | 0.0  | 7            | 100.0 | 0      | 0.0 |
| 6. 無回答                            | 5         | 0       | 0.0  | 2                      | 40.0 | 3            | 60.0  | 0      | 0.0 |
| 7. 計                              | 514       | 181     | 35.2 | 143                    | 27.8 | 185          | 36.0  | 5      | 1.0 |

情報リスクマネジメントを「重要と考え、実践している」事業体は、54.3%が情報セキュリティ監査を実施している。一方、情報リスクマネジメントを「重要と考えている」事業体は22.7%が情報セキュリティ監査を実施しており、「これから行う予定がある」事業体は27.5%である。しかし、「重要と考えて」いて「実施しない」事業体も49.0%となっており、情報セキュリティ監査を実施する事業体と実施しない事業体の割合はほぼ同じとなっている。

なお、情報リスクマネジメントを「さらに強化する予定がある」事業体では、情報セキュリティ監査を実施しない事業体（46.7%）が実施した事業体（30.0%）を16.7ポイント上回っている。一方、情報リスクマネジメントを「考えていない」および「わからない」事業体では、ほとんどが情報セキュリティ監査を「実施しない」と回答している。すなわち、情報リスクマネジメントは、情報セキュリティ監査の実施と強い相関があると考えられる。

情報リスクマネジメントの実施とシステム監査および情報セキュリティ監査の相関については、両者とも高い相関があるものの、システム監査の方がより相関が高い。これは、システム監査が今まで長い間内部監査で実施されてきた歴史があるためと考えられる。

本来的には、情報リスクマネジメントでは、PDCAの中でのチェックが必要となる。したがって、監査を行わないまでも内部監査やセルフチェックが望まれている。リスクマネジメントを実施している事業体では、マネジメントサイクルをまわしていくなかで、いずれ監査を実施する段階に至るものと考えられる。今後、リスクマネジメントの中で、情報セキュリティ監査やシステム監査の実施について広げていくことが必要であろう。



情報リスクマネジメントに対する考え

図3-1-2.情報リスクマネジメントと情報セキュリティ監査

## 3.2 Q4のクロス集計

Q4. 経営者層は次の事項について関心が高いですか。

- ①情報システム関連の事件・事故に対するリスク
- ②個人情報などの情報漏えいに対するリスク
- ③情報セキュリティガバナンス
- ④情報セキュリティ対策ベンチマーク

クロス対象

Q3. 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。

Q5. 情報システム関連、情報セキュリティ関連、個人情報保護漏洩のリスクが貴事業体の経営に重大な影響（経営危機、倒産等）を与えていると思いますか。

### 3.2.1 Q3とのクロス集計

Q3.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情報システム関連の事件・事故に対するリスク

| Q3. 情報リスク<br>マネジメント<br>Q4-①<br>情報システム<br>関連事件・事故 | 回答<br>件数 | 1. 重要と考<br>え実施して<br>いる |      | 2. 重要と<br>考えている |      | 3. さらに強<br>化する予定<br>がある |      | 4. 考えて<br>いない |     | 5. わからない |      | 6. 無回答 |      |
|--------------------------------------------------|----------|------------------------|------|-----------------|------|-------------------------|------|---------------|-----|----------|------|--------|------|
|                                                  |          |                        |      |                 |      |                         |      |               |     |          |      |        |      |
| 1. 高い                                            | 325      | 183                    | 56.3 | 126             | 38.8 | 14                      | 4.3  | 1             | 0.3 | 0        | 0.0  | 1      | 0.3  |
| 2. 中位                                            | 119      | 24                     | 20.2 | 83              | 69.7 | 8                       | 6.7  | 2             | 1.7 | 1        | 0.8  | 1      | 0.8  |
| 3. 低い                                            | 46       | 2                      | 4.3  | 32              | 69.6 | 4                       | 8.7  | 3             | 6.5 | 5        | 10.9 | 0      | 0.0  |
| 4. わからない                                         | 20       | 1                      | 5.0  | 13              | 65.0 | 4                       | 20.0 | 1             | 5.0 | 1        | 5.0  | 0      | 0.0  |
| 5. 無回答                                           | 4        | 0                      | 0.0  | 1               | 25.0 | 0                       | 0.0  | 0             | 0.0 | 0        | 0.0  | 3      | 75.0 |
| 6. 計                                             | 514      | 210                    | 40.9 | 255             | 49.6 | 30                      | 5.8  | 7             | 1.4 | 7        | 1.4  | 5      | 1.0  |

経営者層の情報システム関連の事故・事件（以下、「事件・事故リスク」という。）に対するリスクへの関心度合いと情報リスクマネジメントに対する意識の関係を項目ごとにみると、経営者が事件・事故リスクに対する関心が「高い」場合、情報リスクマネジメントについて「重要と考え実施している」が56.1%、「重要と考えている」が38.8%となっている。

一方、情報リスクマネジメントを「重要と考えている」経営者は、事件・事故リスクに対する関心が「中位」、「低い」、「わからない」の程度に関わらず、70%程度となっている。したがって、情報リスクマネジメントに対して「重要と考え実施している」経営者は、事件・事故リスクに対して関心が「高い」といえる。また、事件・事故リスクに対して関心が「高い」経営者は、情報リスクマネジメントを「重要と考え実施している」なり、「重要と考えている」ことがわかる。

②個人情報などの情報漏えいに対するリスク

| Q3. 情報リスク<br>マネジメント<br>Q4-②<br>情報漏えいリスク | 回<br>答<br>件<br>数 | 1. 重要と考<br>え実施して<br>いる |      | 2. 重要と考<br>えている |      | 3. さらに強化<br>する予定が<br>ある |      | 4. 考えて<br>いない |      | 5. わからない |      | 6. 無回答 |      |
|-----------------------------------------|------------------|------------------------|------|-----------------|------|-------------------------|------|---------------|------|----------|------|--------|------|
| 1. 高い                                   | 356              | 191                    | 53.7 | 146             | 41.0 | 17                      | 4.8  | 1             | 0.3  | 0        | 0.0  | 1      | 0.3  |
| 2. 中位                                   | 102              | 16                     | 15.7 | 76              | 74.5 | 6                       | 5.9  | 2             | 2.0  | 2        | 2.0  | 0      | 0.0  |
| 3. 低い                                   | 39               | 2                      | 5.1  | 25              | 64.1 | 3                       | 7.7  | 4             | 10.3 | 4        | 10.3 | 1      | 2.6  |
| 4. わからない                                | 13               | 1                      | 7.7  | 7               | 53.8 | 4                       | 30.8 | 0             | 0.0  | 1        | 7.7  | 0      | 0.0  |
| 5. 無回答                                  | 4                | 0                      | 0.0  | 1               | 25.0 | 0                       | 0.0  | 0             | 0.0  | 0        | 0.0  | 3      | 75.0 |
| 6. 計                                    | 514              | 210                    | 40.9 | 255             | 49.6 | 30                      | 5.8  | 7             | 1.4  | 7        | 1.4  | 5      | 1.0  |

経営者層の個人情報などの情報漏えいに対するリスク（以下、「情報漏えいリスク」という。）への関心度合いと情報リスクマネジメントに対する意識の関係を項目ごとにみると、経営者が情報漏えいリスクに対する関心が「高い」場合、情報リスクマネジメントについて「重要と考え実施している」が53.7%、「重要と考えている」が41.0%となっている。

一方、情報リスクマネジメントを「重要と考えている」経営者は、情報漏えいリスクについて「中位」、「低い」の程度に関わらず、70%程度となっている。したがって、情報リスクマネジメントに対して「重要と考え実施している」経営者は、情報漏えいリスクに対して関心が「高い」といえる。また、情報漏えいリスクに対して関心が「高い」経営者は、情報リスクマネジメントを「重要と考え実施している」なり「重要と考えている」ことがわかる。しかし、情報リスクマネジメントを「重要と考えている」経営者が、情報漏えいリスクに対して関心が「高い」とは必ずしも言い切れない。

③情報セキュリティガバナンス

| Q3. 情報リスクマ<br>ネジメント<br>Q4-③<br>セキュリティ<br>ガバナンスリスク | 回<br>答<br>件<br>数 | 1. 重要と考<br>え実施して<br>いる |      | 2. 重要と考<br>えている |      | 3. さらに強化<br>する予定が<br>ある |     | 4. 考えて<br>いない |     | 5. わからない |     | 6. 無回答 |      |
|---------------------------------------------------|------------------|------------------------|------|-----------------|------|-------------------------|-----|---------------|-----|----------|-----|--------|------|
| 1. 高い                                             | 100              | 64                     | 64.0 | 33              | 33.0 | 3                       | 3.0 | 0             | 0.0 | 0        | 0.0 | 0      | 0.0  |
| 2. 中位                                             | 173              | 85                     | 49.1 | 78              | 45.1 | 8                       | 4.6 | 1             | 0.6 | 0        | 0.0 | 1      | 0.6  |
| 3. 低い                                             | 78               | 18                     | 23.1 | 48              | 61.5 | 5                       | 6.4 | 4             | 5.1 | 3        | 3.8 | 0      | 0.0  |
| 4. わからない                                          | 158              | 42                     | 26.6 | 95              | 60.1 | 14                      | 8.9 | 2             | 1.3 | 4        | 2.5 | 1      | 0.6  |
| 5. 無回答                                            | 5                | 1                      | 20.0 | 1               | 20.0 | 0                       | 0.0 | 0             | 0.0 | 0        | 0.0 | 3      | 60.0 |
| 6. 計                                              | 514              | 210                    | 40.9 | 255             | 49.6 | 30                      | 5.8 | 7             | 1.4 | 7        | 1.4 | 5      | 1.0  |

経営者層の情報セキュリティガバナンスに対する関心度合いと情報リスクマネジメントに対する意識の関係を項目ごとにみると、経営者が情報セキュリティガバナンスに対し関心が「高い」場合、情報リスクマネジメントについて「重要と考え実施している」が64.0%、「重要と考えている」が33.0%となっている。

一方、情報リスクマネジメントを「重要と考えている」経営者は、情報セキュリティガバナンス

への関心は「中位」が 45.1%、「低い」が 61.5%、「わからない」が 60.1%となっていて、いずれとも言い切れない。したがって、情報セキュリティガバナンスに対し関心が「高い」経営者は、情報リスクマネジメントに対する意識が高いといえる。しかし、情報リスクマネジメントを「重要と考えている」経営者が、情報セキュリティガバナンスに対して関心があるとは必ずしも言い切れない。

#### ④情報セキュリティ対策ベンチマーク

| Q3. 情報リスクマネジメント<br>Q4-④<br>セキュリティ対策ベンチマーク | 回答<br>件数 | 1. 重要と考<br>え実施して<br>いる |      | 2. 重要と考<br>えている |      | 3. さらに強<br>化する予定<br>がある |     | 4. 考えて<br>いない |     | 5. わからない |     | 6. 無回答 |      |
|-------------------------------------------|----------|------------------------|------|-----------------|------|-------------------------|-----|---------------|-----|----------|-----|--------|------|
| 1. 高い                                     | 44       | 32                     | 72.7 | 10              | 22.7 | 1                       | 2.3 | 1             | 2.3 | 0        | 0.0 | 0      | 0.0  |
| 2. 中位                                     | 152      | 81                     | 53.3 | 64              | 42.1 | 7                       | 4.6 | 0             | 0.0 | 0        | 0.0 | 0      | 0.0  |
| 3. 低い                                     | 121      | 32                     | 26.4 | 71              | 58.7 | 8                       | 6.6 | 6             | 5.0 | 3        | 2.5 | 1      | 0.8  |
| 4. わからない                                  | 191      | 64                     | 33.5 | 108             | 56.5 | 14                      | 7.3 | 0             | 0.0 | 4        | 2.1 | 1      | 0.5  |
| 5. 無回答                                    | 6        | 1                      | 16.7 | 2               | 33.3 | 0                       | 0.0 | 0             | 0.0 | 0        | 0.0 | 3      | 50.0 |
| 6. 計                                      | 514      | 210                    | 40.9 | 255             | 49.6 | 30                      | 5.8 | 7             | 1.4 | 7        | 1.4 | 5      | 1.0  |

経営者層の情報セキュリティ対策ベンチマークに対する関心度合いと情報リスクマネジメントに対する意識の関係を項目ごとにみると、経営者が情報セキュリティ対策ベンチマークに関心が「高い」場合、情報リスクマネジメントについて「重要と考え実施している」が 72.7%、「重要と考えている」が 22.7%となっている。この両方で 95.4%となっている。一方、情報リスクマネジメントを「重要と考えている」経営者は、情報セキュリティ対策ベンチマークへの関心について「中位」が 42.1%、「低い」が 58.7%、「わからない」が 56.4%となっている。したがって、情報セキュリティ対策ベンチマークに対して関心が「高い」経営者は、情報リスクマネジメントへの意識が高いといえる。しかし、情報リスクマネジメントを「重要と考えている」経営者が、情報セキュリティ対策ベンチマークに関心があるとは必ずしも言い切れない。

以上のクロス分析からは、経営者の情報セキュリティに対してのリスク認識は、情報システム関連の事件・事故に対するリスク、個人情報などの情報漏えいリスク、情報セキュリティガバナンス、情報セキュリティ対策ベンチマークに関心の「高い」経営者は、情報リスクマネジメントを「重要と考え実施している」といえよう。すなわち、経営者はリスク認識が高く、これをコントロールするフレームワークや測定のツールに関心があることが望ましいといえよう。また、この4項目の中では、情報セキュリティ対策ベンチマーク、すなわち、自社の情報セキュリティを他社と比較するなどの評価ツールに関心が高いことが推測される。

### 3.2.2 Q5とのクロス集計

Q5.情報システム関連、情報セキュリティ関連、個人情報保護漏えいのリスクが貴事業体の経営に重大な影響(経営危機、倒産等)を与えますか。

#### ①情報システム関連の事件・事故に対するリスク

| Q5.経営への影響<br>Q4-①<br>情報システム<br>関連事件・事故 | 回答<br>件数 | 1. 思う |      | 2. 重大な影<br>響は受ける<br>と思う |      | 3. 重大な影響<br>は受けない |      | 4. わからない |      | 5. 無回答 |      |
|----------------------------------------|----------|-------|------|-------------------------|------|-------------------|------|----------|------|--------|------|
| 1. 高い                                  | 325      | 212   | 65.2 | 101                     | 31.1 | 11                | 3.4  | 1        | 0.3  | 0      | 0.0  |
| 2. 中位                                  | 119      | 26    | 21.8 | 70                      | 58.8 | 19                | 16.0 | 4        | 3.4  | 0      | 0.0  |
| 3. 低い                                  | 46       | 13    | 28.3 | 18                      | 39.1 | 13                | 28.3 | 2        | 4.3  | 0      | 0.0  |
| 4. わからない                               | 20       | 8     | 40.0 | 6                       | 30.0 | 3                 | 15.0 | 3        | 15.0 | 0      | 0.0  |
| 5. 無回答                                 | 4        | 0     | 0.0  | 1                       | 25.0 | 0                 | 0.0  | 0        | 0.0  | 3      | 75.0 |
| 6. 計                                   | 514      | 259   | 50.4 | 196                     | 38.1 | 46                | 8.9  | 10       | 1.9  | 3      | 0.6  |

経営者層の事故・事件リスクへの関心度合いと、情報システム関連、情報セキュリティ関連、個人情報保護漏えいのリスク（以下、「情報関連リスク」という。）が経営に与える影響の程度との関係を項目ごとにみると、経営者が事件・事故リスクに対する関心が「高い」場合は、65.2%が情報関連リスクが経営に重大な影響を与えると「思う」となっている。また、事件・事故リスクに対する関心が「中位」の場合は 58.8%が「重大な影響を受けると思う」、関心が「低い」場合は、39.1%が「重大な影響を受けると思う」、28.3%が「思う」と「重大な影響は受けない」となっており、重大な影響との深い関係はない。したがって、事件・事故リスクに対して関心の「高い」経営者は、情報関連リスクに対する意識が高いといえよう。

#### ②個人情報などの情報漏えいに対するリスク

| Q5.経営への影響<br>Q4-②<br>情報漏えい<br>リスク | 回答<br>件数 | 1. 思う |      | 2. 重大な影<br>響は受ける<br>と思う |      | 3. 重大な影響<br>は受けない |      | 4. わからない |      | 5. 無回答 |      |
|-----------------------------------|----------|-------|------|-------------------------|------|-------------------|------|----------|------|--------|------|
| 1. 高い                             | 356      | 215   | 60.4 | 128                     | 36.0 | 11                | 3.1  | 2        | 0.6  | 0      | 0.0  |
| 2. 中位                             | 102      | 29    | 28.4 | 48                      | 47.1 | 22                | 21.6 | 3        | 2.9  | 0      | 0.0  |
| 3. 低い                             | 39       | 9     | 23.1 | 15                      | 38.5 | 12                | 30.8 | 3        | 7.7  | 0      | 0.0  |
| 4. わからない                          | 13       | 6     | 46.2 | 4                       | 30.8 | 1                 | 7.7  | 2        | 15.4 | 0      | 0.0  |
| 5. 無回答                            | 4        | 0     | 0.0  | 1                       | 25.0 | 0                 | 0.0  | 0        | 0.0  | 3      | 75.0 |
| 6. 計                              | 514      | 259   | 50.4 | 196                     | 38.1 | 46                | 8.9  | 10       | 1.9  | 3      | 0.6  |

経営者層の漏えいリスクに対する関心度合いと情報関連リスクが経営に与える影響の程度との関係を項目ごとにみると、経営者が漏えいリスクに対する関心が「高い」場合は 60.4%が情報関連リスクが経営に重大な影響を与えると「思う」となっている。また、漏えいリスクに対する関心が「中位」の場合は 47.1%が「重大な影響を受けると思う」、関心が「低い」場合は 38.5%が「重大な影響を受けると思う」、30.8%が「重大な影響は受けない」となっており、重大な影響との深い

関係は特にはない。したがって、漏えいリスクに対して関心が「高い」経営者は、情報関連リスクに対する意識が高いといえよう。

### ③情報セキュリティガバナンス

| Q4-③<br>セキュリティ<br>ガバナンス | Q5.経営への影響 | 回答<br>件数 | 1. 思う |      | 2. 重大な影<br>響は受けると<br>思う |      | 3. 重大な影響<br>は受けない |      | 4. わからない |     | 5. 無回答 |      |
|-------------------------|-----------|----------|-------|------|-------------------------|------|-------------------|------|----------|-----|--------|------|
| 1. 高い                   |           | 100      | 64    | 64.0 | 32                      | 32.0 | 3                 | 3.0  | 1        | 1.0 | 0      | 0.0  |
| 2. 中位                   |           | 173      | 96    | 55.5 | 62                      | 35.8 | 14                | 8.1  | 1        | 0.6 | 0      | 0.0  |
| 3. 低い                   |           | 78       | 28    | 35.9 | 35                      | 44.9 | 12                | 15.4 | 3        | 3.8 | 0      | 0.0  |
| 4. わからない                |           | 158      | 70    | 44.3 | 66                      | 41.8 | 17                | 10.8 | 5        | 3.2 | 0      | 0.0  |
| 5. 無回答                  |           | 5        | 1     | 20.0 | 1                       | 20.0 | 0                 | 0.0  | 0        | 0.0 | 3      | 60.0 |
| 6. 計                    |           | 514      | 259   | 50.4 | 196                     | 38.1 | 46                | 8.9  | 10       | 1.9 | 3      | 0.6  |

経営者層の情報セキュリティガバナンスに対する関心度合いと情報関連リスクが経営に与える影響の程度との関係を項目ごとにみると、情報セキュリティガバナンスに対する関心が「高い」場合は 64.0%が情報関連リスクが経営に重大な影響を与えると「思う」となっている。また、情報セキュリティガバナンスに対する関心が「中位」の場合は 55.5%が「思う」、関心が「低い」場合は 44.9%が「重大な影響を受けると思う」、関心度合いが「わからない」場合は 44.3%が「思う」となっており、いずれの場合も「思う」が中心となる。すなわち、依存関係は特にはないといえよう。

### ④情報セキュリティ対策ベンチマーク

| Q4-④<br>セキュリティ<br>対策ベンチマーク | Q5.経営への影響 | 回答<br>件数 | 1. 思う |      | 2. 重大な影<br>響は受けると<br>思う |      | 3. 重大な影響<br>は受けない |      | 4. わからない |     | 5. 無回答 |      |
|----------------------------|-----------|----------|-------|------|-------------------------|------|-------------------|------|----------|-----|--------|------|
| 1. 高い                      |           | 44       | 29    | 65.9 | 13                      | 29.5 | 2                 | 4.5  | 0        | 0.0 | 0      | 0.0  |
| 2. 中位                      |           | 152      | 89    | 58.6 | 52                      | 34.2 | 10                | 6.6  | 1        | 0.7 | 0      | 0.0  |
| 3. 低い                      |           | 121      | 46    | 38.0 | 53                      | 43.8 | 18                | 14.9 | 4        | 3.3 | 0      | 0.0  |
| 4. わからない                   |           | 191      | 93    | 48.7 | 77                      | 40.3 | 16                | 8.4  | 5        | 2.6 | 0      | 0.0  |
| 5. 無回答                     |           | 6        | 2     | 33.3 | 1                       | 16.7 | 0                 | 0.0  | 0        | 0.0 | 3      | 50.0 |
| 6. 計                       |           | 514      | 259   | 50.4 | 196                     | 38.1 | 46                | 8.9  | 10       | 1.9 | 3      | 0.6  |

経営者層の情報セキュリティ対策ベンチマークに対する関心度合いと情報関連リスクが経営に与える影響の程度との関係を項目ごとにみると、経営者が情報セキュリティ対策ベンチマークに対して関心が「高い」場合は 65.9%が情報セキュリティ対策ベンチマークが経営に重大な影響を与えると「思う」となっている。また、関心が「中位」の場合は 58.6%が「思う」、関心が「低い」場合は 43.8%が「重大な影響を受けると思う」となっている。すなわち、情報セキュリティベンチマークに対する関心が高い経営者は、情報関連リスクが経営に与える影響が大きいと考えていることがわかる。

### 3.3 Q6のクロス集計

Q6. 情報セキュリティガバナンスの観点から、情報セキュリティ対策にあたり、どの関係者を考慮に入れていますか。

クロス対象

|                                                                                |
|--------------------------------------------------------------------------------|
| Q25. 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。                                   |
| Q26. 災害に対する情報システムのバックアップ対策を講じていますか。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。 |
| Q53. 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。                                        |

#### 3.3.1 Q25 とのクロス集計

Q25.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。

| Q25.事業継続計画<br>Q6.関係者 | 回答<br>件数 | 1. 外部からの悪意による緊急事態(サイバーテロ、コンピュータウイルス等) |       | 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) |       | 3. 事故・災害(火災、地震、風水害、停電等) |       | 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) |       | 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) |      |
|----------------------|----------|---------------------------------------|-------|--------------------------------------|-------|-------------------------|-------|------------------------------------|-------|-----------------------------------------|------|
| 1. 株主・投資家等           | 49       | 26                                    | 53.1  | 20                                   | 40.8  | 49                      | 100.0 | 41                                 | 83.7  | 23                                      | 46.9 |
| 2. 顧客・消費者            | 95       | 49                                    | 51.6  | 41                                   | 43.2  | 91                      | 95.8  | 82                                 | 86.3  | 50                                      | 52.6 |
| 3. 取引先               | 70       | 43                                    | 61.4  | 37                                   | 52.9  | 68                      | 97.1  | 56                                 | 80.0  | 37                                      | 52.9 |
| 4. 格付け機関             | 9        | 5                                     | 55.6  | 5                                    | 55.6  | 9                       | 100.0 | 7                                  | 77.8  | 4                                       | 44.4 |
| 5. 従業員               | 68       | 36                                    | 52.9  | 33                                   | 48.5  | 66                      | 97.1  | 56                                 | 82.4  | 38                                      | 55.9 |
| 6. その他               | 5        | 5                                     | 100.0 | 5                                    | 100.0 | 5                       | 100.0 | 5                                  | 100.0 | 4                                       | 80.0 |
| 7. 無回答               | 1        | 1                                     | 100.0 | 0                                    | 0.0   | 0                       | 0.0   | 1                                  | 100.0 | 0                                       | 0.0  |
| 8. 計                 | 110      | 58                                    | 52.7  | 48                                   | 43.6  | 105                     | 95.5  | 93                                 | 84.5  | 57                                      | 51.8 |

| Q25.事業継続計画<br>Q6.関係者 | 6. 内部犯罪による緊急事態 |       | 7. 伝染病(SARS等) |      | 8. その他 |     |
|----------------------|----------------|-------|---------------|------|--------|-----|
| 1. 株主・投資家等           | 11             | 22.4  | 3             | 6.1  | 0      | 0.0 |
| 2. 顧客・消費者            | 24             | 25.3  | 6             | 6.3  | 1      | 1.1 |
| 3. 取引先               | 23             | 32.9  | 5             | 7.1  | 1      | 1.4 |
| 4. 格付け機関             | 2              | 22.2  | 1             | 11.1 | 0      | 0.0 |
| 5. 従業員               | 22             | 32.4  | 3             | 4.4  | 1      | 1.5 |
| 6. その他               | 5              | 100.0 | 0             | 0.0  | 0      | 0.0 |
| 7. 無回答               | 0              | 0.0   | 0             | 0.0  | 0      | 0.0 |
| 8. 計                 | 32             | 29.1  | 7             | 6.4  | 1      | 0.9 |

情報セキュリティガバナンスと事業継続計画の関係を項目ごとにみると、すべての関係者にとって最も利害関係が大きいのは、「事故・災害（火災、地震、風水害、停電等）」および「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）」に集中している。「株主・投資家等」および「格付け機関」はすべて（100%）の関係者が「事故・災害」を重視している。また、「取引先」や「従業員」の97.1%、「顧客・消費者」の95.8%が重視している。

一方、「障害」については「株主・投資家等」は83.7%、「格付け機関」は77.8%が重視している。これは、事故・災害に比べると代替の手段などの対応が可能であるためと考えられる。

図3-3-1から、事故・災害および障害がどの関係者にとっても関心が高いことがわかる。この2つに着目すると、「顧客・消費者」についてのみ「障害」（82/93件=88.2%）の方が「事故・災害」（91/105件=86.7%）よりも割合が高い。これは顧客・消費者は日常のサービスを受けることを優先するため、事件・事故よりも障害の方が高くなっているものと考えられる。

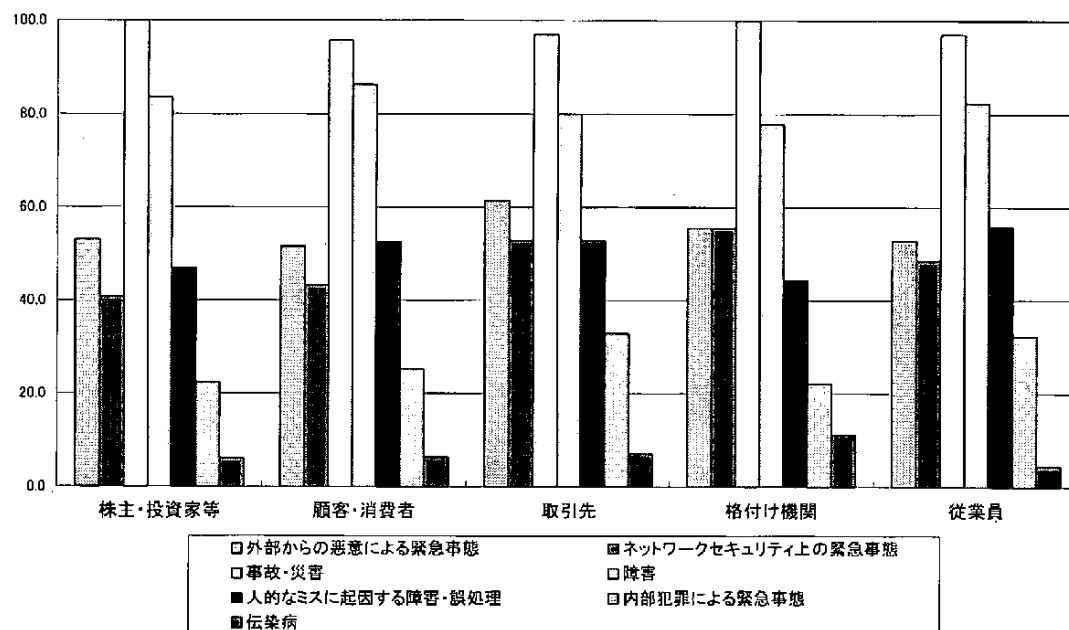


図3-3-1. 情報セキュリティガバナンスの関係者と事業継続計画項目の関係

### 3.3.2 Q26 とのクロス集計

Q26. 災害に対する情報システムのバックアップ対策を講じていますか。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。

| Q26. バックアップ対策<br>Q6. 関係者 | 回答件数 | 1. 対象システムを決めている |      | 2. バックアップに関する規程や手順を決めている |      | 3. バックアップの頻度、バックアップ先を決定している |      | 4. バックアップを定期的の実施している |      | 5. バックアップの実施状況を定期的にチェックしている |      |
|--------------------------|------|-----------------|------|--------------------------|------|-----------------------------|------|----------------------|------|-----------------------------|------|
| 1. 株主・投資家等               | 199  | 132             | 66.3 | 124                      | 62.3 | 119                         | 59.8 | 170                  | 85.4 | 92                          | 46.2 |
| 2. 顧客・消費者                | 364  | 220             | 60.4 | 203                      | 55.8 | 206                         | 56.6 | 304                  | 83.5 | 158                         | 43.4 |
| 3. 取引先                   | 287  | 174             | 60.6 | 165                      | 57.5 | 167                         | 58.2 | 239                  | 83.3 | 124                         | 43.2 |
| 4. 格付け機関                 | 25   | 19              | 76.0 | 19                       | 76.0 | 18                          | 72.0 | 21                   | 84.0 | 13                          | 52.0 |
| 5. 従業員                   | 295  | 179             | 60.7 | 171                      | 58.0 | 184                         | 62.4 | 258                  | 87.5 | 140                         | 47.5 |
| 6. その他                   | 51   | 28              | 54.9 | 19                       | 37.3 | 30                          | 58.8 | 44                   | 86.3 | 21                          | 41.2 |
| 7. 無回答                   | 18   | 6               | 33.3 | 5                        | 27.8 | 9                           | 50.0 | 13                   | 72.2 | 5                           | 27.8 |
| 8. 計                     | 514  | 301             | 58.6 | 263                      | 51.2 | 288                         | 56.0 | 424                  | 82.5 | 207                         | 40.3 |

| Q26. バックアップ対策<br>Q6. 関係者 | 6. 回復手順を決めている |      | 7. バックアップを業者に委託する時はSLAを結んでいる |      | 8. バックアップシステムの稼動状況を確認している |      | 9. アウトソーシング先の対策は把握していない |     | 10. 特に講じていない |      | 11. 無回答 |      |
|--------------------------|---------------|------|------------------------------|------|---------------------------|------|-------------------------|-----|--------------|------|---------|------|
| 1. 株主・投資家等               | 102           | 51.3 | 24                           | 12.1 | 61                        | 30.7 | 2                       | 1.0 | 5            | 2.5  | 6       | 3.0  |
| 2. 顧客・消費者                | 170           | 46.7 | 29                           | 8.0  | 101                       | 27.7 | 8                       | 2.2 | 19           | 5.2  | 8       | 2.2  |
| 3. 取引先                   | 142           | 49.5 | 23                           | 8.0  | 88                        | 30.7 | 5                       | 1.7 | 14           | 4.9  | 5       | 1.7  |
| 4. 格付け機関                 | 19            | 76.0 | 6                            | 24.0 | 10                        | 40.0 | 1                       | 4.0 | 1            | 4.0  | 0       | 0.0  |
| 5. 従業員                   | 143           | 48.5 | 23                           | 7.8  | 94                        | 31.9 | 4                       | 1.4 | 11           | 3.7  | 5       | 1.7  |
| 6. その他                   | 22            | 43.1 | 1                            | 2.0  | 19                        | 37.3 | 1                       | 2.0 | 2            | 3.9  | 0       | 0.0  |
| 7. 無回答                   | 1             | 5.6  | 1                            | 5.6  | 3                         | 16.7 | 0                       | 0.0 | 2            | 11.1 | 2       | 11.1 |
| 8. 計                     | 218           | 42.4 | 34                           | 6.6  | 135                       | 26.3 | 9                       | 1.8 | 29           | 5.6  | 12      | 2.3  |

情報セキュリティガバナンスと情報システムのバックアップ対策の関係を項目ごとにみると、すべての関係者にとって最も利害関係が大きいのは、「バックアップを定期的の実施している」であり、すべての関係者の8割以上がこの項目を選択している。これに続くのが「対象システムを決めている」となっており、6割以上がこの項目を選択している。従業員にとっては、「バックアップの頻度、バックアップ先を決定している」も重要な要素となっており、62.4%が選択している。

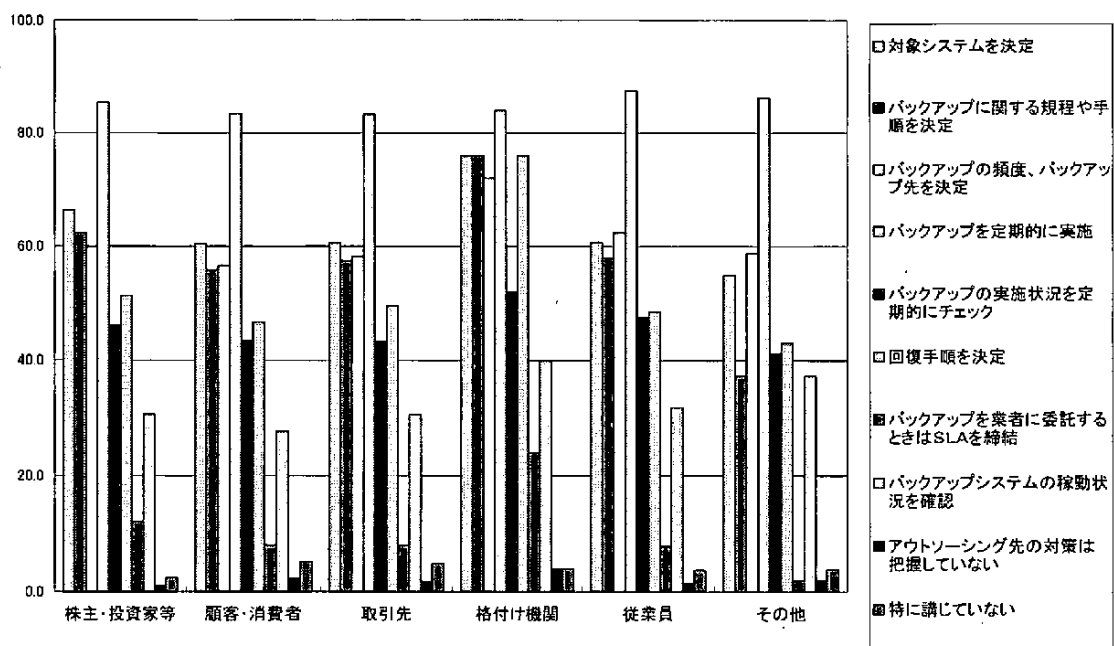


図3-3-2. 情報セキュリティガバナンスの関係者とバックアップ対策の実施状況との関係

### 3.3.3 Q53 とのクロス集計

Q53.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。

| Q53.個人情報の管理<br>状況のリスク<br>Q6.関係者 | 回<br>答<br>件<br>数 | 1. 対応策を講<br>じているので、<br>リスクはないと<br>認識している |     | 2. 現状の管理<br>方法で何も問<br>題が発生して<br>いないので、リ<br>スクはないと認<br>識している |     | 3. 対策を講じ<br>ているが、リス<br>クはあると認識<br>している |      | 4. 何度かヒヤ<br>リ・ハットした経<br>験があり、リス<br>クがあると認識し<br>ている |      | 5. いつ問題が<br>発生してもおか<br>しくない状況で<br>あると認識して<br>いる |      |
|---------------------------------|------------------|------------------------------------------|-----|-------------------------------------------------------------|-----|----------------------------------------|------|----------------------------------------------------|------|-------------------------------------------------|------|
| 1. 株主・投資家等                      | 199              | 2                                        | 1.0 | 4                                                           | 2.0 | 151                                    | 75.9 | 13                                                 | 6.5  | 17                                              | 8.5  |
| 2. 顧客・消費者                       | 364              | 5                                        | 1.4 | 8                                                           | 2.2 | 284                                    | 78.0 | 23                                                 | 6.3  | 27                                              | 7.4  |
| 3. 取引先                          | 287              | 3                                        | 1.0 | 9                                                           | 3.1 | 217                                    | 75.6 | 17                                                 | 5.9  | 19                                              | 6.6  |
| 4. 格付け機関                        | 25               | 0                                        | 0.0 | 0                                                           | 0.0 | 21                                     | 84.0 | 3                                                  | 12.0 | 1                                               | 4.0  |
| 5. 従業員                          | 295              | 2                                        | 0.7 | 9                                                           | 3.1 | 227                                    | 76.9 | 17                                                 | 5.8  | 25                                              | 8.5  |
| 6. その他                          | 51               | 1                                        | 2.0 | 1                                                           | 2.0 | 40                                     | 78.4 | 0                                                  | 0.0  | 7                                               | 13.7 |
| 7. 無回答                          | 18               | 0                                        | 0.0 | 0                                                           | 0.0 | 9                                      | 50.0 | 1                                                  | 5.6  | 4                                               | 22.2 |
| 8. 計                            | 514              | 5                                        | 1.0 | 18                                                          | 3.5 | 377                                    | 73.3 | 30                                                 | 5.8  | 50                                              | 9.7  |

| Q53.個人情報の管理<br>状況のリスク<br>Q6.関係者 | 6. その他 |     | 7. 特に認識して<br>いない |      | 8. 無回答 |     |
|---------------------------------|--------|-----|------------------|------|--------|-----|
| 1. 株主・投資家等                      | 1      | 0.5 | 5                | 2.5  | 6      | 3.0 |
| 2. 顧客・消費者                       | 2      | 0.5 | 8                | 2.2  | 7      | 1.9 |
| 3. 取引先                          | 1      | 0.3 | 14               | 4.9  | 7      | 2.4 |
| 4. 格付け機関                        | 0      | 0.0 | 0                | 0.0  | 0      | 0.0 |
| 5. 従業員                          | 0      | 0.0 | 6                | 2.0  | 9      | 3.1 |
| 6. その他                          | 0      | 0.0 | 1                | 2.0  | 1      | 2.0 |
| 7. 無回答                          | 0      | 0.0 | 3                | 16.7 | 1      | 5.6 |
| 8. 計                            | 2      | 0.4 | 20               | 3.9  | 12     | 2.3 |

情報セキュリティガバナンスと個人情報の管理状況に対するリスク認識との関係を項目ごとにみると、すべての関係者にとって利害関係が大きいのは、管理状況のリスクについて「対策を講じているが、リスクはあると認識している」に集中している。他の項目については、ほとんどが一桁台であり、すべての関係者が興味を持っていない。情報セキュリティガバナンスの観点と個人情報の管理状況についてリスクがあることが当然である、ということで選択はふれていない。

### 3.4 Q8のクロス集計

Q8. 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、または実施を予定しているものはどれですか。

クロス対象項目

|                                                   |
|---------------------------------------------------|
| Q18. 情報セキュリティの確保にとり、基本的に重要な要素は何だと思いますか。(複数回答)     |
| Q30-8. 貴事業体では従業員に対し、情報セキュリティの一般知識に関する教育を実施していますか。 |
| Q40. 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。                  |
| Q43. 情報セキュリティ監査を実施したことがありますか。                     |

#### 3.4.1 Q18 とのクロス集計

Q18. 情報セキュリティの確保にとり、基本的に重要な要素は何だと思いますか。(複数回答)

①Q8からみたQ18

| Q18. 重要要素<br>Q8. 実施対策      | 回答<br>件数 | 1. 経営者層の<br>理解 |      | 2. 管理者<br>の理解 |      | 3. 担当者<br>の理解 |      | 4. 社内全体<br>の理解 |      | 5. 社内規定<br>やルール<br>の整備 |      |
|----------------------------|----------|----------------|------|---------------|------|---------------|------|----------------|------|------------------------|------|
| 1. 情報リスクマネジメント方針           | 235      | 184            | 78.3 | 113           | 48.1 | 102           | 43.4 | 205            | 87.2 | 139                    | 59.1 |
| 2. 情報セキュリティポリシー            | 352      | 270            | 76.7 | 184           | 52.3 | 160           | 45.5 | 309            | 87.8 | 213                    | 60.5 |
| 3. 情報リスク分析                 | 165      | 133            | 80.6 | 84            | 50.9 | 81            | 49.1 | 146            | 88.5 | 93                     | 56.4 |
| 4. 情報セキュリティ対策の実施<br>手順、規定類 | 287      | 227            | 79.1 | 145           | 50.5 | 131           | 45.6 | 256            | 89.2 | 174                    | 60.6 |
| 5. 情報セキュリティ監査              | 180      | 145            | 80.6 | 100           | 55.6 | 91            | 50.6 | 158            | 87.8 | 102                    | 56.7 |
| 6. システム監査                  | 178      | 138            | 77.5 | 85            | 47.8 | 77            | 43.3 | 155            | 87.1 | 108                    | 60.7 |
| 無回答                        | 122      | 90             | 73.8 | 50            | 41.0 | 35            | 28.7 | 88             | 72.1 | 67                     | 54.9 |
| 計                          | 514      | 391            | 76.1 | 243           | 47.3 | 206           | 40.1 | 429            | 83.5 | 303                    | 58.9 |

| Q18. 重要要素<br>Q8. 実施対策      | 6. その他 |     | 無回答 |     |
|----------------------------|--------|-----|-----|-----|
| 1. 情報リスクマネジメント方針           | 4      | 1.7 | 0   | 0.0 |
| 2. 情報セキュリティポリシー            | 7      | 2.0 | 0   | 0.0 |
| 3. 情報リスク分析                 | 4      | 2.4 | 0   | 0.0 |
| 4. 情報セキュリティ対策の実施<br>手順、規定類 | 4      | 1.4 | 0   | 0.0 |
| 5. 情報セキュリティ監査              | 3      | 1.7 | 0   | 0.0 |
| 6. システム監査                  | 4      | 2.2 | 1   | 0.6 |
| 無回答                        | 6      | 4.9 | 1   | 0.8 |
| 計                          | 13     | 2.5 | 2   | 0.4 |

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当然のことながら明確なはずである。情報セキュリティ上基本的に重要な要素について、「情報リスクマネジメント方針」との関わりで最も高い回答は「社内全体の理解（エン

ドユーザを含む) の理解」87.2%であった。この割合は前回調査の94.0%に比べ6.8ポイント減少している。次いで「経営者層の理解」(78.3%)であるが、前回の80.3%から2ポイント減少した。

なお、前回調査では「法規制の整備」について質問を設けたが、今回調査では現状に鑑みて若干表現を変え、「社内規定やルールの整備」として回答を求めた。意味的には同じではないが、コンプライアンスの対象という点から比較してみると、前回の「法規制の整備」が23.9%であったのに対し、「社内規定やルールの整備」は59.1%と倍以上の回答結果が示された。たしかに「法規制の整備」と「社内規制・ルールの整備」には内容的に違いがあるが、コンプライアンスの重要性に鑑みると遵守対象の整備に対する取組み姿勢の変化が確認できると思われる。なお、「管理者の理解」については48.1%であり、前回とほぼ同様(48.7%)であった。

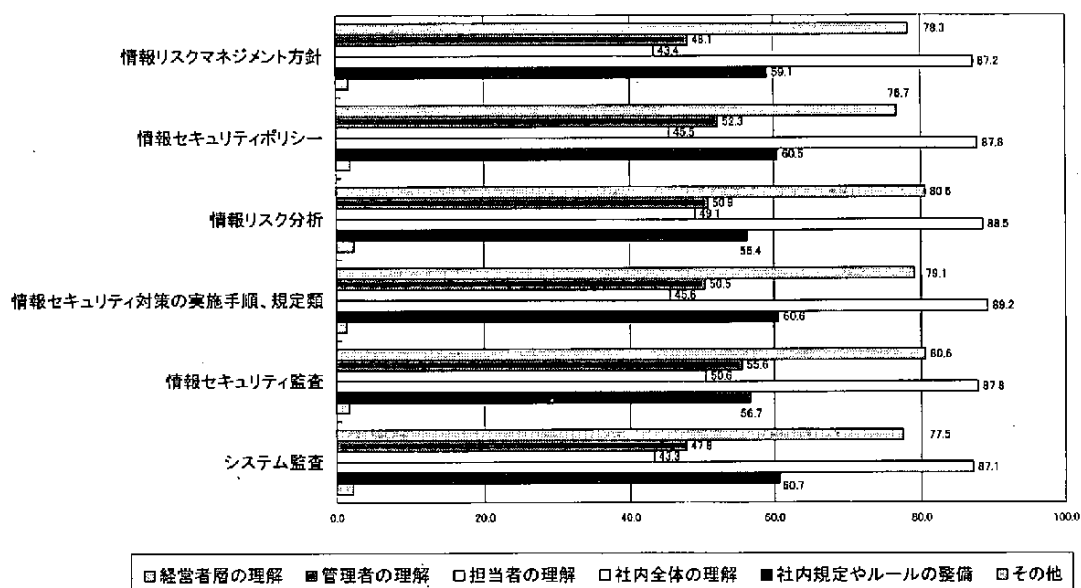


図3-4-1. 情報リスクマネジメント上の重要対策に対するセキュリティ上の視点

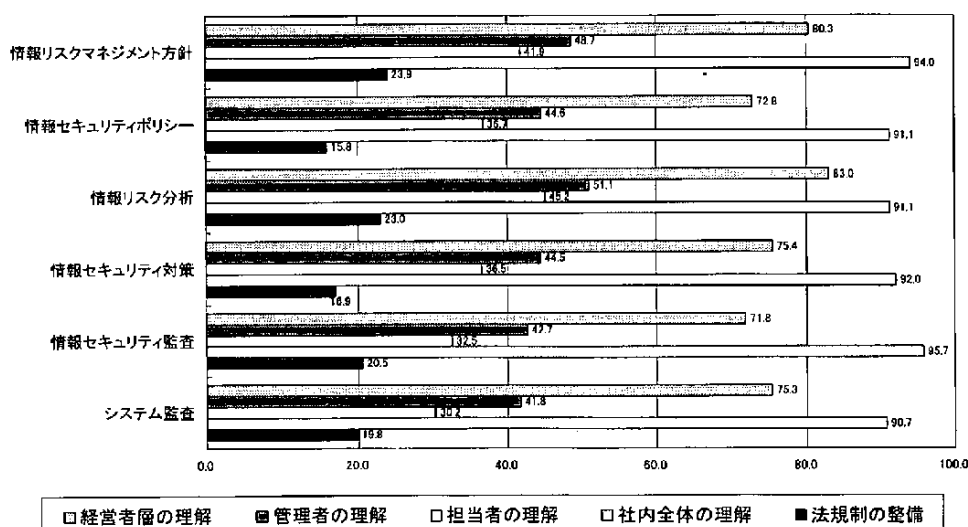


図3-4-2. (参考)情報リスクマネジメント上の重要対策に対するセキュリティ上の視点(平成15年度調査)

②Q18からみたQ8

| Q18.重要要素<br>Q8.実施対策        | 回答<br>件数 | 1. 経営者層の<br>理解 |       | 2. 管理者の<br>理解 |       | 3. 担当者の<br>理解 |       | 4. 社内全体の<br>理解 |       |
|----------------------------|----------|----------------|-------|---------------|-------|---------------|-------|----------------|-------|
| 1. 情報リスクマネジメント方針           | 235      | 184            | 47.1  | 113           | 46.5  | 102           | 49.5  | 205            | 47.8  |
| 2. 情報セキュリティポリシー            | 352      | 270            | 69.1  | 184           | 75.7  | 160           | 77.7  | 309            | 72.0  |
| 3. 情報リスク分析                 | 165      | 133            | 34.0  | 84            | 34.6  | 81            | 39.3  | 146            | 34.0  |
| 4. 情報セキュリティ対策の実<br>施手順、規定類 | 287      | 227            | 58.1  | 145           | 59.7  | 131           | 63.6  | 256            | 59.7  |
| 5. 情報セキュリティ監査              | 180      | 145            | 37.1  | 100           | 41.2  | 91            | 44.2  | 158            | 36.8  |
| 6. システム監査                  | 178      | 138            | 35.3  | 85            | 35.0  | 77            | 37.4  | 155            | 36.1  |
| 無回答                        | 122      | 90             | 23.0  | 50            | 20.6  | 35            | 17.0  | 88             | 20.5  |
| 計                          | 514      | 391            | 100.0 | 243           | 100.0 | 206           | 100.0 | 429            | 100.0 |

| Q18.重要要素<br>Q8.実施対策        | 5. 社内規定や<br>ルールを整備 |       | その他 |       | 無回答 |       |
|----------------------------|--------------------|-------|-----|-------|-----|-------|
| 1. 情報リスクマネジメント方針           | 139                | 45.9  | 4   | 30.8  | 0   | 0.0   |
| 2. 情報セキュリティポリシー            | 213                | 70.3  | 7   | 53.8  | 0   | 0.0   |
| 3. 情報リスク分析                 | 93                 | 30.7  | 4   | 30.8  | 0   | 0.0   |
| 4. 情報セキュリティ対策の実<br>施手順、規定類 | 174                | 57.4  | 4   | 30.8  | 0   | 0.0   |
| 5. 情報セキュリティ監査              | 102                | 33.7  | 3   | 23.1  | 0   | 0.0   |
| 6. システム監査                  | 108                | 35.6  | 4   | 30.8  | 1   | 50.0  |
| 無回答                        | 67                 | 22.1  | 6   | 46.2  | 1   | 50.0  |
| 計                          | 303                | 100.0 | 13  | 100.0 | 2   | 100.0 |

Q18 からみたクロスの回答結果から「経営者層の理解」をみると、「情報セキュリティ対策の実施手順、規定類」（58.1%／前回調査は「情報セキュリティ対策」で58.9%）を除く「情報リスクマネジメント方針」、「情報セキュリティポリシー」、「情報リスク分析」、「情報セキュリティ監査」、「システム監査」では、いずれにおいても前回調査よりも増加した。この傾向は「管理者の理解」、「担当者の理解」、「社内全体の理解」についても同様であった。

前回の回答結果からは「はじめに手段ありき」的な考え方の存在が確認できたが、今回の調査では、「経営者の理解」、「管理者の理解」、「担当者の理解」、「社内全体の理解」等において「情報リスクマネジメント方針」、「情報セキュリティポリシー」、「情報リスク分析」等リスクマネジメントプロセスに則った考え方がみられる。

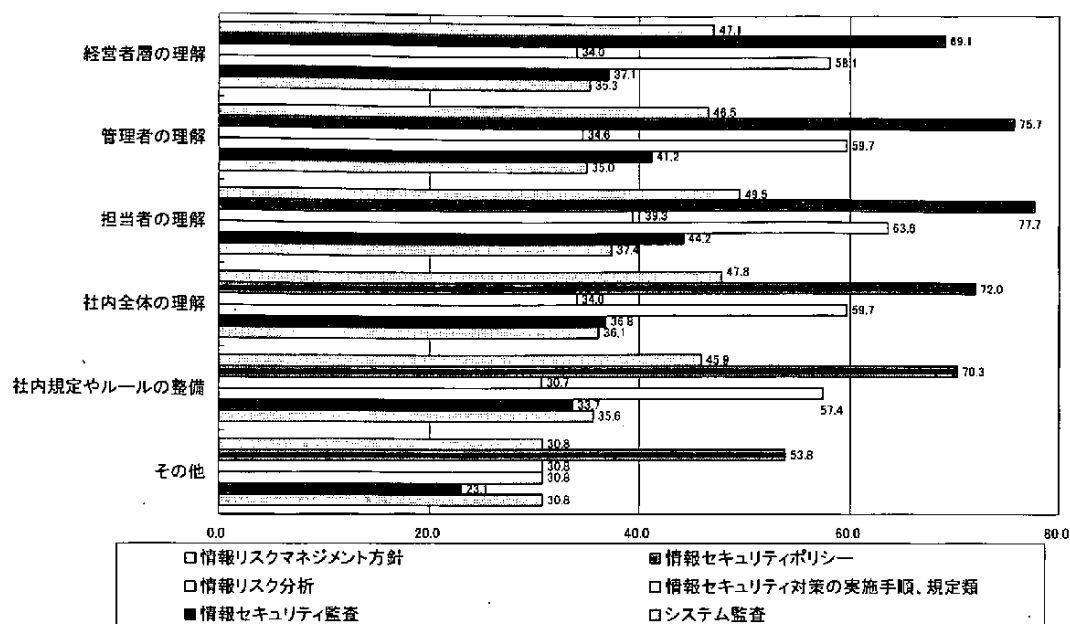


図3-4-3. セキュリティ上の視点に対する情報リスクマネジメント上の重要対策

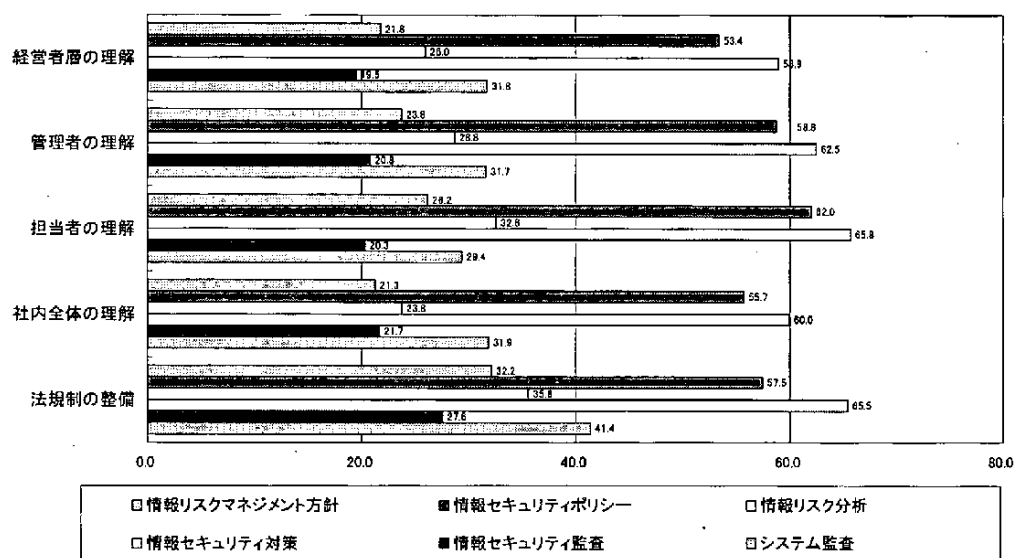


図3-4-4. (参考)セキュリティ上の視点に対する情報リスクマネジメント上の重要対策(平成15年度調査)

### 3.4.2 Q30-8 とのクロス集計

Q30-8. 貴事業体では従業員に対し、情報セキュリティの一般知識に関する教育を実施していますか。

#### ①Q8からみたQ30-8

| Q30-8.教育の実施状況<br>Q8. 実施対策  | 回答<br>件数 | 1. 定期的<br>に実施して<br>いる |      | 2. 時々実施<br>している |      | 3. 実施を予<br>定している |      | 4. 実施してい<br>ない |      | 無回答 |     |
|----------------------------|----------|-----------------------|------|-----------------|------|------------------|------|----------------|------|-----|-----|
| 1. 情報リスクマネジメント方針           | 235      | 126                   | 53.6 | 82              | 34.9 | 12               | 5.1  | 11             | 4.7  | 4   | 1.7 |
| 2. 情報セキュリティポリシー            | 352      | 152                   | 43.2 | 134             | 38.1 | 33               | 9.4  | 25             | 7.1  | 8   | 2.3 |
| 3. 情報リスク分析                 | 165      | 98                    | 59.4 | 52              | 31.5 | 4                | 2.4  | 8              | 4.8  | 3   | 1.8 |
| 4. 情報セキュリティ対策の実施<br>手順、規定類 | 287      | 141                   | 49.1 | 106             | 36.9 | 20               | 7.0  | 17             | 5.9  | 3   | 1.0 |
| 5. 情報セキュリティ監査              | 180      | 112                   | 62.2 | 49              | 27.2 | 11               | 6.1  | 5              | 2.8  | 3   | 1.7 |
| 6. システム監査                  | 178      | 85                    | 47.8 | 60              | 33.7 | 15               | 8.4  | 14             | 7.9  | 4   | 2.2 |
| 無回答                        | 122      | 11                    | 9.0  | 24              | 19.7 | 25               | 20.5 | 56             | 45.9 | 6   | 4.9 |
| 計                          | 514      | 170                   | 33.1 | 174             | 33.9 | 66               | 12.8 | 89             | 17.3 | 15  | 2.9 |

情報リスクマネジメントにおいては従業員に対する情報セキュリティの一般知識に関する教育はきわめて重要である。そこで、Q30-8 とのクロスから考察を進めてみた。

教育を「定期的に実施している」、「時々実施している」と回答した場合を教育重視している事業体であるとすれば、「情報リスクマネジメント方針」について教育を「定期的に実施」が 53.6%、「時々実施」が 34.9%と両者の関係が相対的に高いと思われる。「情報セキュリティポリシー」、「情報セキュリティ対策の実施手順、規定類」、「システム監査」でも同様の傾向が確認できるが、教育との関連から最も重視すべき「定期的に実施」は、「情報リスク分析」が 59.4%、「情報セキュリティ監査」が 62.2%と比較的高く、さらに「時々実施」をあわせると、両対策とも9割になる。

しかし、現在の情報環境の変化の著しい時代に約 13%の事業体がまだ「実施を予定している」としていることは、事業体に及ぼす情報リスクの意味をどう認識しているのか。また、それ以上に 17.3%の事業体が「実施していない」と回答している。情報リスクがこれまで顕在化しなかった、したがって今後とも健在化しない、と考えて従業員に対する教育を軽視しているのか、検討の余地がありそうである。

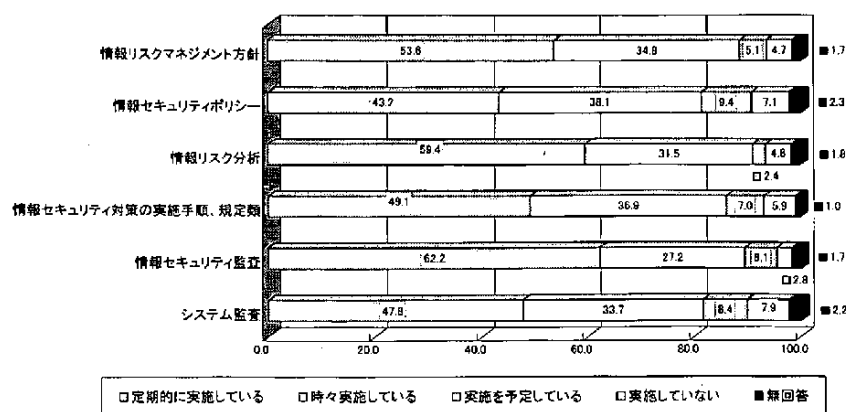


図3-4-5. 情報リスクマネジメント上の重要対策に対する情報セキュリティ教育の実施状況

### 3.4.3 Q40 とのクロス集計

Q40. 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も客観的な視点から行うシステム監査は重要である。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面的にも妥当なはずである。少なくとも、システム監査を通して、情報リスクマネジメントに関わる情報リスクマネジメント方針、情報セキュリティポリシー、情報リスク分析、情報セキュリティ対策の実施手順・規定類および情報セキュリティ監査との関係が把握できると思われる。この点は、情報リスクマネジメント実施の事業体であればシステム監査との明確な関係がみられるという前回調査の報告書での仮説に基づくものである<sup>り</sup>。そこで、情報リスクマネジメントに関わる項目について、Q8からシステム監査の実施状況（Q40）について考察してみることにする。

#### ①Q8からみたQ40

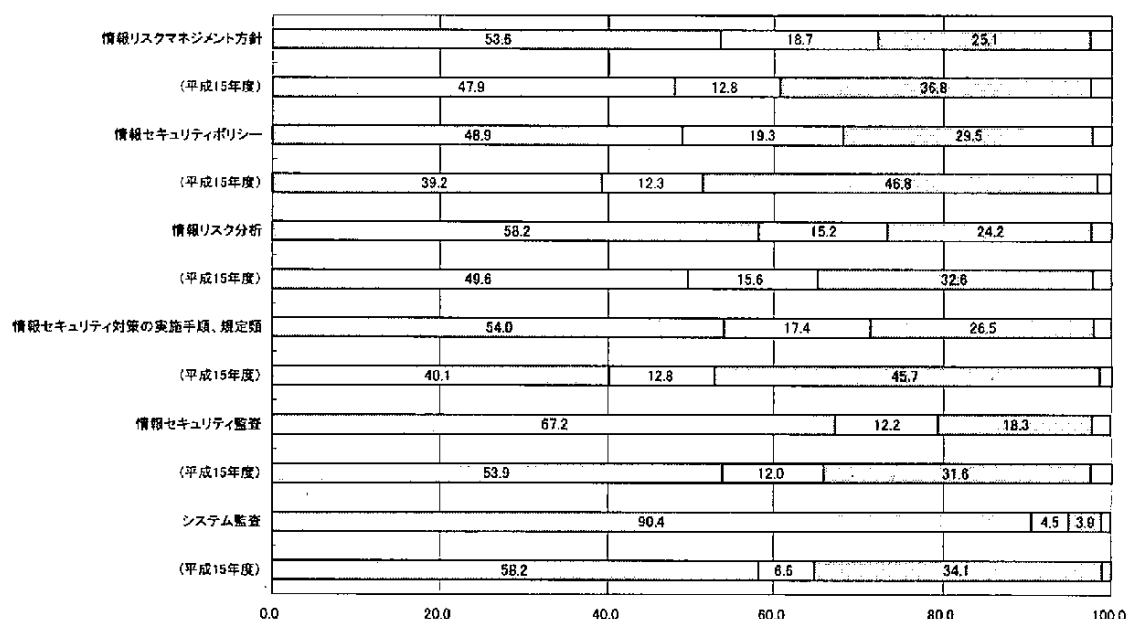
| Q8. 実施対策 \ Q40. システム監査の実施状況 | 回答件数 | 1. 実施した<br>(実施中を含む) |      | 2. これから実施する予定がある |      | 3. 実施しない |      | 無回答 |     |
|-----------------------------|------|---------------------|------|------------------|------|----------|------|-----|-----|
| 1. 情報リスクマネジメント方針            | 235  | 126                 | 53.6 | 44               | 18.7 | 59       | 25.1 | 6   | 2.6 |
| 2. 情報セキュリティポリシー             | 352  | 172                 | 48.9 | 68               | 19.3 | 104      | 29.5 | 8   | 2.3 |
| 3. 情報リスク分析                  | 165  | 96                  | 58.2 | 25               | 15.2 | 40       | 24.2 | 4   | 2.4 |
| 4. 情報セキュリティ対策の実施手順、規定類      | 287  | 155                 | 54.0 | 50               | 17.4 | 76       | 26.5 | 6   | 2.1 |
| 5. 情報セキュリティ監査               | 180  | 121                 | 67.2 | 22               | 12.2 | 33       | 18.3 | 4   | 2.2 |
| 6. システム監査                   | 178  | 161                 | 90.4 | 8                | 4.5  | 7        | 3.9  | 2   | 1.1 |
| 無回答                         | 122  | 12                  | 9.8  | 17               | 13.9 | 89       | 73.0 | 4   | 3.3 |
| 計                           | 514  | 209                 | 40.7 | 88               | 17.1 | 204      | 39.7 | 13  | 2.5 |

<sup>り</sup> 平成15年度版「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月発行） 3.2.4（p117～）参照。

Q 8 で調査した情報リスクマネジメントの実施対策のうち、システム監査を「実施している（実施中を含む）」事業体は 34.6%（178/514 件）である。これは前回調査（35.9%）に比べ 1.3 ポイントの減少ではあるが、ほぼ同程度の結果といえる。

「情報リスクマネジメント方針」については 53.6%（ $\rightarrow$ H15：47.9%、5.7 ポイント増）、「情報セキュリティポリシー」48.9%（ $\rightarrow$ H15：39.2%、9.7 ポイント増）、「情報リスク分析」58.2%（ $\rightarrow$ H15：49.6%、8.6 ポイント増）、「情報セキュリティ対策の実施手順・規定類」54.0%（ $\rightarrow$ H15：40.1%、13.9 ポイント増／「情報セキュリティ対策」で質問）、「情報セキュリティ監査」67.2%（ $\rightarrow$ H15：53.9%、13.3 ポイント増）といずれもが前回の割合を上回っている。特にシステム監査については、178 事業体のうち、「実施（中）」が 90.4%と前回調査の 58.2% に比べ 32.2 ポイント増となり、認識の高まりを感じとることができる。

しかし、「情報セキュリティ監査」の 67.2%に対し「システム監査」が 90.4%とかなり高い回答結果を示している。システム監査と情報セキュリティ監査との差異をどう認識すべきなのか。さらに、「情報セキュリティポリシー」の 48.9%等を考慮するとき、情報リスクマネジメントに関わる項目がそれぞれ独自であるのではなく、相互に関連した関係にあることを回答者はどのように考えているのか、さらに検討の余地がありそうである。



②Q40 からみたQ8

| Q40. システム監査の<br>実施状況<br>Q8. 実施対策 | 回 答<br>件数 | 1. 実施した<br>(実施中を<br>含む) |       | 2. これから実<br>施する予定が<br>ある |       | 3. 実施<br>しない |       | 無回答 |       |
|----------------------------------|-----------|-------------------------|-------|--------------------------|-------|--------------|-------|-----|-------|
| 1. 情報リスクマネジメント方針                 | 235       | 126                     | 60.3  | 44                       | 50.0  | 59           | 28.9  | 6   | 46.2  |
| 2. 情報セキュリティポリシー                  | 352       | 172                     | 82.3  | 68                       | 77.3  | 104          | 51.0  | 8   | 61.5  |
| 3. 情報リスク分析                       | 165       | 96                      | 45.9  | 25                       | 28.4  | 40           | 19.6  | 4   | 30.8  |
| 4. 情報セキュリティ対策の実施<br>手順、規定類       | 287       | 155                     | 74.2  | 50                       | 56.8  | 76           | 37.3  | 6   | 46.2  |
| 5. 情報セキュリティ監査                    | 180       | 121                     | 57.9  | 22                       | 25.0  | 33           | 16.2  | 4   | 30.8  |
| 6. システム監査                        | 178       | 161                     | 77.0  | 8                        | 9.1   | 7            | 3.4   | 2   | 15.4  |
| 無回答                              | 122       | 12                      | 5.7   | 17                       | 19.3  | 89           | 43.6  | 4   | 30.8  |
| 計                                | 514       | 209                     | 100.0 | 88                       | 100.0 | 204          | 100.0 | 13  | 100.0 |

次に、システム監査の実施状況から情報リスクマネジメント対策の実施状況をみると、「情報リスクマネジメント方針」60.3%（ $\nearrow$ H15:25.8%、34.5 ポイント増）、「情報セキュリティポリシー」82.3%（H15:57.1%、25.2 ポイント増）、「情報リスク分析」45.9%（ $\nearrow$ H15:30.9%、15.0 ポイント増、）、「情報セキュリティ対策の実施手順・規定類」74.2%（ $\nearrow$ H15:62.2%、12.0 ポイント増）、「情報セキュリティ監査」57.9%（ $\nearrow$ H15:29.0%、28.9 ポイント増）、「システム監査」77.0%（ $\nearrow$ H15:48.8%、28.2 ポイント増）であった。すべての項目において前回の割合を上回っているが、特筆すべき点は、「情報リスクマネジメント方針」、「情報セキュリティポリシー」に対する回答結果であり、さらに客観的な視点から情報リスクマネジメントの実際を監査するという「情報セキュリティ監査」ならびに「システム監査」への割合の増加である。

しかもこれからの「実施予定」についても、「情報セキュリティポリシー」、「情報セキュリティ対策関連の手順・規定類」に対する回答から、今後の対応に期待がもてそうである。

なお、「実施しない」という回答においても、「情報セキュリティポリシー」については49%（100%-51%）は実施しないわけではない、と捉えることができるわけであり、そうした視点に立てば、情報リスクマネジメントに関する理解は確実に広がってきていると思われる。

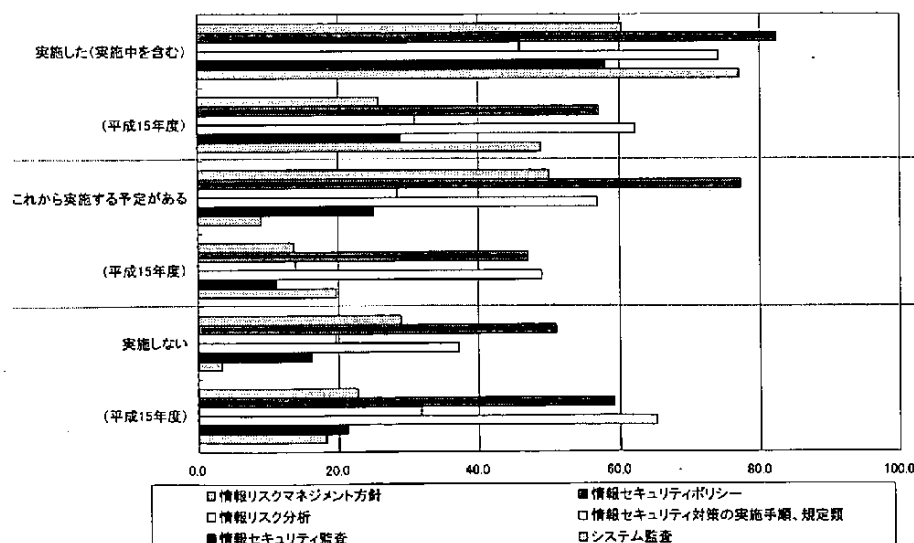


図3-4-7. システム監査の実施状況に対する情報リスクマネジメント上の実施対策

### 3.4.4 Q43 とのクロス集計

Q43.情報セキュリティ監査を実施したことがありますか。

#### ①Q8からみたQ43

| Q43. 情報セキュリティ<br>監査の実施状況   | 回答<br>件数 | 1. 実施した |      | 2. これから行う<br>予定がある |      | 3. 実施<br>しない |      | 無回答 |     |
|----------------------------|----------|---------|------|--------------------|------|--------------|------|-----|-----|
| Q8. 実施対策                   |          |         |      |                    |      |              |      |     |     |
| 1. 情報リスクマネジメント方針           | 235      | 121     | 51.5 | 67                 | 28.5 | 43           | 18.3 | 4   | 1.7 |
| 2. 情報セキュリティポリシー            | 352      | 159     | 45.2 | 109                | 31.0 | 80           | 22.7 | 4   | 1.1 |
| 3. 情報リスク分析                 | 165      | 105     | 63.6 | 37                 | 22.4 | 20           | 12.1 | 3   | 1.8 |
| 4. 情報セキュリティ対策の実施<br>手順、規定類 | 287      | 147     | 51.2 | 83                 | 28.9 | 53           | 18.5 | 4   | 1.4 |
| 5. 情報セキュリティ監査              | 180      | 138     | 76.7 | 31                 | 17.2 | 8            | 4.4  | 3   | 1.7 |
| 6. システム監査                  | 178      | 109     | 61.2 | 34                 | 19.1 | 33           | 18.5 | 2   | 1.1 |
| 無回答                        | 122      | 8       | 6.6  | 25                 | 20.5 | 88           | 72.1 | 1   | 0.8 |
| 計                          | 514      | 181     | 35.2 | 143                | 27.8 | 185          | 36.0 | 5   | 1.0 |

情報セキュリティ監査はシステム監査に比べ情報セキュリティに特化しているといえるが、システム監査の場合と同様の仮説からアプローチすることができる。情報セキュリティ監査を実施した事業体は181件（H15：110件）で、Q8に対する実施事業体（180件／H15：117件）とともに増加傾向にある。

Q8の回答事業体では「情報リスクマネジメント方針」51.5%（ $\nearrow$ H15:34.2%、17.3ポイント増）、「情報セキュリティポリシー」45.2%（ $\nearrow$ H15:25.9%、19.3ポイント増）、「情報リスク分析」63.6%（ $\nearrow$ H15:34.8%、28.8ポイント増）、「情報セキュリティ対策の実施手順・規定類」51.2%（ $\nearrow$ H15:25.2%、26.0ポイント増／「情報セキュリティ対策」で質問）、そして「システム監査」61.2%（ $\nearrow$ H15:33.0%、28.2ポイント増）と、いずれの項目も前回の回答を大幅に上回っている。

特に情報セキュリティ監査については、今回は180事業体のうち実施（実施中を含む）が138事業体で76.7%（約23.3%の回答がどうなのか）と、前回調査の49.6%（58／117件）に比べ、事業体の回答数から判断すれば、情報セキュリティ監査に対する認識の高まりが感じられる。なお、特に顕著な増加としては、情報リスク分析に対する回答結果にみられる。

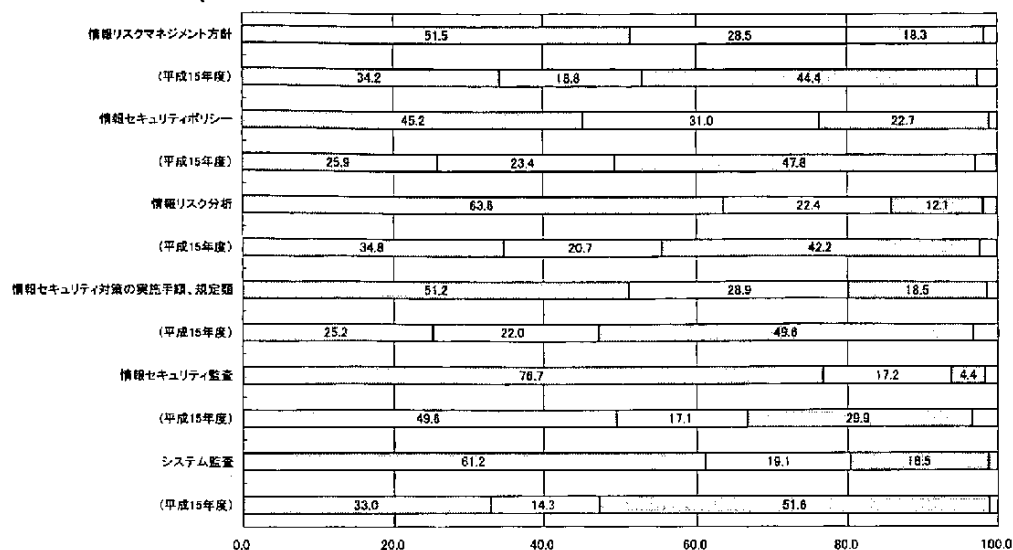


図3-4-8. 情報リスクマネジメント上の実施対策に対する情報セキュリティ監査の実施状況

## ②Q43 からみた Q 8

| Q43. 情報セキュリティ監査の実施状況<br>Q8. 実施対策 | 回答<br>件数 | 1. 実施した |       | 2. これから行う<br>予定がある |       | 3. 実施<br>しない |       | 無回答 |       |
|----------------------------------|----------|---------|-------|--------------------|-------|--------------|-------|-----|-------|
| 1. 情報リスクマネジメント方針                 | 235      | 121     | 66.9  | 67                 | 46.9  | 43           | 23.2  | 4   | 80.0  |
| 2. 情報セキュリティポリシー                  | 352      | 159     | 87.8  | 109                | 76.2  | 80           | 43.2  | 4   | 80.0  |
| 3. 情報リスク分析                       | 165      | 105     | 58.0  | 37                 | 25.9  | 20           | 10.8  | 3   | 60.0  |
| 4. 情報セキュリティ対策の実施<br>手順、規定類       | 287      | 147     | 81.2  | 83                 | 58.0  | 53           | 28.6  | 4   | 80.0  |
| 5. 情報セキュリティ監査                    | 180      | 138     | 76.2  | 31                 | 21.7  | 8            | 4.3   | 3   | 60.0  |
| 6. システム監査                        | 178      | 109     | 60.2  | 34                 | 23.8  | 33           | 17.8  | 2   | 40.0  |
| 無回答                              | 122      | 8       | 4.4   | 25                 | 17.5  | 88           | 47.6  | 1   | 20.0  |
| 計                                | 514      | 181     | 100.0 | 143                | 100.0 | 185          | 100.0 | 5   | 100.0 |

次にQ43 からQ8 への回答結果を考察する。「情報リスクマネジメント方針」66.9% (㊦H15 : 36.4%、30.5 ポイント増)、「情報セキュリティポリシー」87.8% (㊦H15 : 74.5%、13.3 ポイント増)、「情報リスク分析」58.0% (㊦H15 : 42.7%、15.3 ポイント増)、「情報セキュリティ対策の実施手順・規定類」81.2% (㊦H15 : 77.3%、3.9 ポイント増)／「情報セキュリティ対策」で質問、「システム監査」60.2% (㊦H15 : 54.5%、5.7 ポイント増)、「情報セキュリティ監査」76.2% (㊦H15 : 52.7%、23.5 ポイント増) という結果であった。前回調査ではシステム監査の方が情報セキュリティ監査を1.8 ポイント上回っていたが、今回は情報セキュリティ監査が7割を超え、システム監査を16 ポイント上回った。

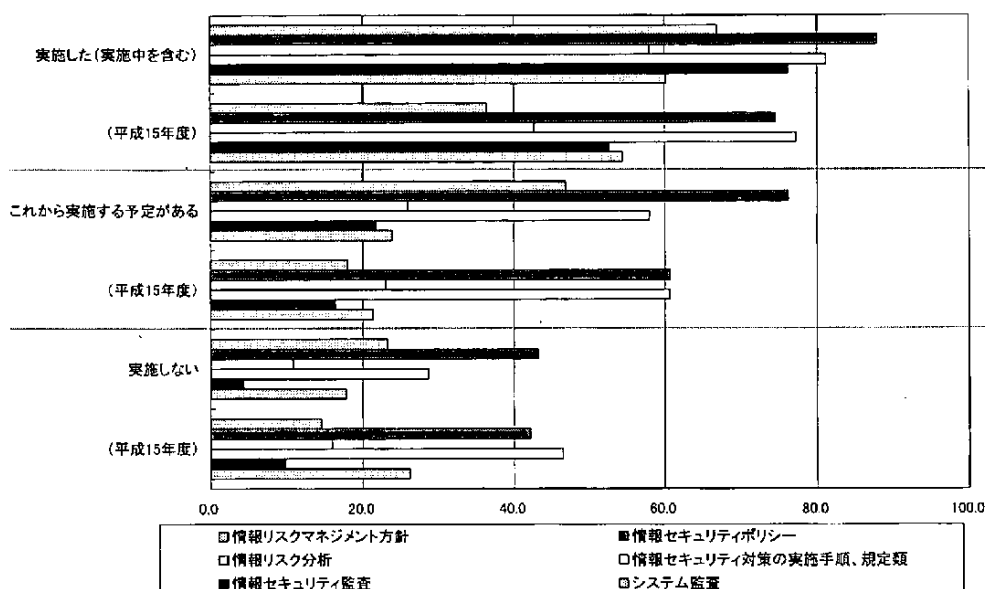


図3-4-9. 情報セキュリティ監査の実施状況に対する情報リスクマネジメント上の実施対策

これまでの回答結果に鑑みると、情報リスクマネジメントに関わるいずれの項目についても増加傾向にあるといえよう。

なお、システム監査および情報セキュリティ監査に対する回答結果の違いに関して、これらをどのように捉えるかは回答者の判断による、といわざるをえないが、概してこれらの監査をいかなる視点（コストと有効性、利便性等）から捉えるかにかかっている。

今回もクロス集計の結果、回答間における齟齬が見られるが、回答者の質問項目の理解なり認識に関係するかもしれない。いずれにせよ、回答結果の読み方には注意が必要といえる。ただ、今回も強調しておきたい点は、実施に関わる質問項目について、「実施した」、「実施の予定」、「実施しない」ことのそれぞれの結果には「復旧・回復のための投入時間」、それらのための要する「発生費用」の点で大きな差異が生じることである。情報リスクが顕在化した場合、事業体間にどれだけの差が生じるのか、あらためてリスクマネジメント実践の意義を確認しておくことが重要である。

### 3.5 Q13-①のクロス集計

Q13-①貴事業体の基幹システムは、過去1年間に、システムの運用に悪影響を与えたか、または事業中断につながるシステムダウンが発生しましたか。

クロス対象項目

|                                                                         |
|-------------------------------------------------------------------------|
| Q22-9. 貴事業体として重要と思われる要素:事業継続管理(災害対策、障害対策など)                             |
| Q24. 「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)。 |
| Q25. (Q24 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) |

事業継続管理とは、万一システムダウンなどの事故が発生した場合に重要業務を継続させるためにあらかじめ事前から備える仕組みである。ここではこの1年間で基幹システムのダウンによりシステムの運用に悪影響を被ったか、あるいは事業中断につながるような状況を経験した事業体と、部分的なダウンでそのような悪影響を経験しなかった、あるいはまったく影響を受けるようなシステムダウンを経験しなかった事業体で、事業継続管理に関する取組みや意識に何らかの差があるか、クロス集計を行った。

#### 3.5.1 Q22-9 とのクロス集計

Q22-9.貴事業体として重要と思われる要素:事業継続管理(災害対策、障害対策など)

| Q13-①<br>システムダウン<br>の発生状況 | Q22-9. 事業継続<br>管理Q13-① | 回答<br>件数 | 事業継続管理<br>(合計) |      |
|---------------------------|------------------------|----------|----------------|------|
| 1. 全体的にダウンした              |                        | 41       | 8              | 19.5 |
| 2. 部分的にダウンした              |                        | 215      | 57             | 26.5 |
| 3. ダウンしない                 |                        | 250      | 65             | 26.0 |
| 無回答                       |                        | 22       | 4              | 18.2 |
| 計                         |                        | 514      | 130            | 25.3 |

過去1年間に「全体的にダウンした」経験のある事業体は41件であるが、そのうち「事業継続管理」を重要な要素として取り上げた事業体は19.5%である。「部分的にダウンした」事業体は215社で、そのうち「事業継続管理」を重要とした事業体は26.5%である。「ダウンしない」事業体のうち、「事業継続管理」を重要とした事業体は26.0%となっている。

この数値からではダウンしていない事業体ではすべて対策が充実していたからダウンを起きなかった、ということはいえないが、「全体的にダウンした」事業体では「事業継続管理」を重要視する割合が19.5%であり、「部分的にダウンした」、「ダウンしなかった」の割合と比較すると低くなっている。事業継続管理を重要視することは一般にシステムダウンの予防策も充実

し、さらに万が一の被災を想定した備えを実施していると想定されるため、システムダウンも少ないことが期待されるが、このクロス分析では「備えあればシステムダウンなし」という傾向を若干ながら示しているといえる。

### 3.5.2 Q24 とのクロス集計

Q24. 「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)。

#### ①Q13-①からみたQ24

| Q24. 事業継続性計画<br>の作成状況<br>Q13-①<br>システムダウン<br>の発生状況 | 回<br>答<br>件<br>数 | 1. 作成し<br>ている |      | 2. 作成中<br>である |     | 3. 作成を<br>含め検討<br>中である |      | 4. 作成<br>していない |      | 5. 必要<br>ない |     | 無回答 |      |
|----------------------------------------------------|------------------|---------------|------|---------------|-----|------------------------|------|----------------|------|-------------|-----|-----|------|
| 1. 全体的にダウンした                                       | 41               | 7             | 17.1 | 0             | 0.0 | 8                      | 19.5 | 22             | 53.7 | 1           | 2.4 | 3   | 7.3  |
| 2. 部分的にダウンした                                       | 215              | 34            | 15.8 | 10            | 4.7 | 49                     | 22.8 | 114            | 53.0 | 3           | 1.4 | 5   | 2.3  |
| 3. ダウンしない                                          | 250              | 43            | 17.2 | 13            | 5.2 | 71                     | 28.4 | 113            | 45.2 | 4           | 1.6 | 6   | 2.4  |
| 4. 無回答                                             | 22               | 1             | 4.5  | 1             | 4.5 | 5                      | 22.7 | 11             | 50.0 | 1           | 4.5 | 3   | 13.6 |
| 5. 計                                               | 514              | 85            | 16.5 | 24            | 4.7 | 127                    | 24.7 | 252            | 49.0 | 9           | 1.8 | 17  | 3.3  |

『JIS X 5080』に求められる事業継続性計画を「作成している」事業体は全体で 16.5%、「作成中である」4.7%、「作成を含め検討中である」24.7%、「作成していない」49.0%、「必要ない」が 1.8%である。「全体的にダウンした」事業体では「作成している」が 17.1%と平均より若干高く、「作成中である」0.0%、「作成を含めて検討中である」19.5%は平均よりも低く、また「作成していない」は 53.7%と高い。したがって全体的にダウンした経験がある事業体は『JIS X 5080』に定められている事業継続性計画を作成していないところが多いことがわかる。

「部分的にダウンした」事業体の場合、「作成している」が 15.8%と低い。「作成中である」(4.7%)、「作成を含め検討中である」(22.8%)も低く、「作成していない」は 53.0%と高い。ダウンしていない事業体では「作成している」(17.2%)、「作成中である」(5.2%)、「作成を含め検討中である」(28.4%)が平均よりも高く、「作成していない」は 45.2%と低い。

これらの結果から、多少ではあるが、ダウンした事業体ほど『JIS X 5080』の中に定められる事業継続性計画を作成していない、またダウンしない事業体ほど事業継続性計画を作成している傾向にある。

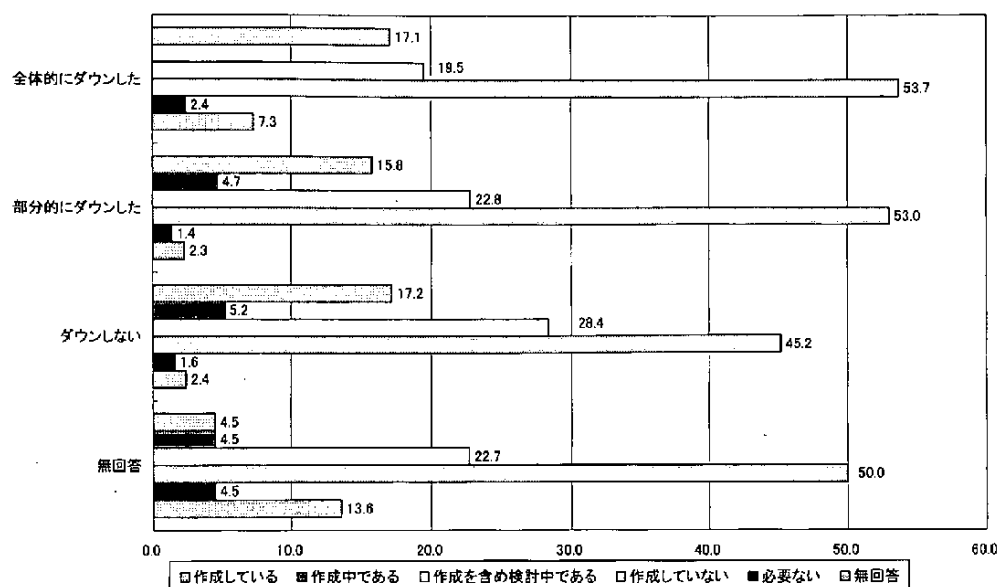


図3-5-1. システムダウンの発生状況に対する事業継続性計画の作成状況

②Q24からみたQ13-①

| Q24. 事業継続性計画<br>の作成状況<br>Q13-①<br>システムダウン<br>の発生状況 | 回 答<br>件数 | 1. 作成して<br>いる |       | 2. 作成中<br>である |       | 3. 作成を含め<br>検討中である |       | 4. 作成して<br>いない |       |
|----------------------------------------------------|-----------|---------------|-------|---------------|-------|--------------------|-------|----------------|-------|
|                                                    |           |               |       |               |       |                    |       |                |       |
| 1. 全面的にダウンした                                       | 41        | 7             | 8.2   | 0             | 0.0   | 8                  | 6.3   | 22             | 8.7   |
| 2. 部分的にダウンした                                       | 215       | 34            | 40.0  | 10            | 41.7  | 49                 | 38.6  | 114            | 45.2  |
| 3. ダウンしない                                          | 250       | 43            | 50.6  | 13            | 54.2  | 71                 | 55.9  | 113            | 44.8  |
| 無回答                                                | 22        | 1             | 1.2   | 1             | 4.2   | 5                  | 3.9   | 11             | 4.4   |
| 計                                                  | 514       | 85            | 100.0 | 24            | 100.0 | 127                | 100.0 | 252            | 100.0 |

| Q24. 事業継続性計画<br>の作成状況<br>Q13-①<br>システムダウン<br>の発生状況 | 5. 必要ない |       | 無回答 |       |
|----------------------------------------------------|---------|-------|-----|-------|
|                                                    |         |       |     |       |
| 1. 全面的にダウンした                                       | 1       | 11.1  | 3   | 17.6  |
| 2. 部分的にダウンした                                       | 3       | 33.3  | 5   | 29.4  |
| 3. ダウンしない                                          | 4       | 44.4  | 6   | 35.3  |
| 無回答                                                | 1       | 11.1  | 3   | 17.6  |
| 計                                                  | 9       | 100.0 | 17  | 100.0 |

事業継続性計画を「作成している」事業体では、「全面的にダウンした」が 8.2%、「部分的にダウンした」が 40.0%、「ダウンしない」が 50.6%である。一方、「作成していない」事業体の場合、「全面的にダウンした」8.7%、「部分的にダウンした」45.2%、「ダウンしない」が 44.8%であり、この結果を比較するとやはり計画を作成している事業体の方がダウンしていないことがわかる。

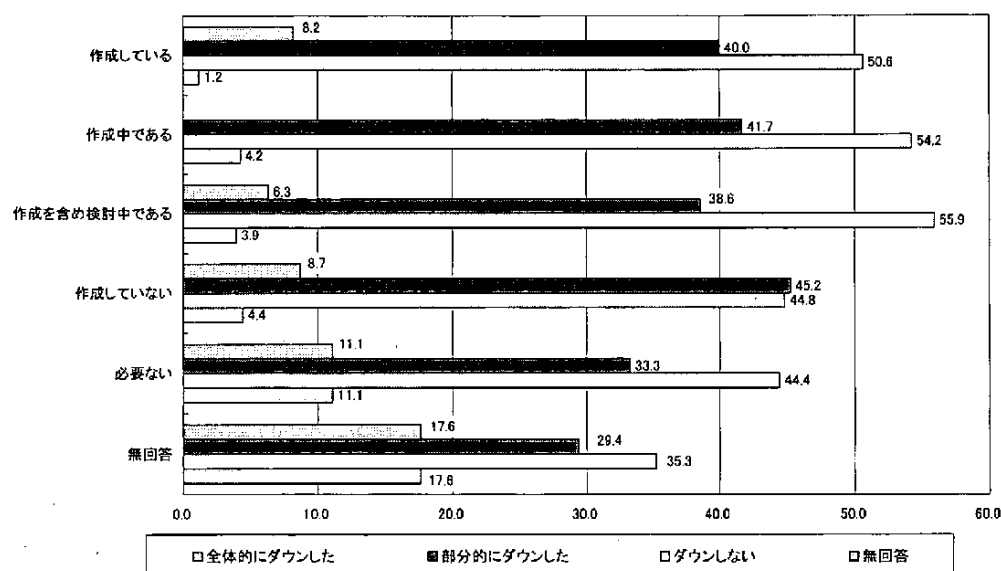


図3-5-2. 事業継続性計画の作成状況に対するシステムダウンの発生状況

### 3.5.3 Q25 とのクロス集計

Q25.(Q24 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)

| Q25. 事業継続性<br>計画項目<br>Q13-①<br>システムダウン<br>の発生状況 | 回答<br>件数 | 1. 外部からの<br>悪意による<br>緊急事態 |        | 2. ネットワーク<br>セキュリティ上<br>の緊急事態 |        | 3. 事故・災害 |        | 4. 障害 |        |
|-------------------------------------------------|----------|---------------------------|--------|-------------------------------|--------|----------|--------|-------|--------|
|                                                 |          | 件数                        | 割合 (%) | 件数                            | 割合 (%) | 件数       | 割合 (%) | 件数    | 割合 (%) |
| 1. 全体的にダウンした                                    | 7        | 3                         | 42.9   | 0                             | 0.0    | 7        | 100.0  | 7     | 100.0  |
| 2. 部分的にダウンした                                    | 44       | 23                        | 52.3   | 23                            | 52.3   | 41       | 93.2   | 37    | 84.1   |
| 3. ダウンしない                                       | 57       | 30                        | 52.6   | 24                            | 42.1   | 55       | 96.5   | 48    | 84.2   |
| 無回答                                             | 2        | 2                         | 100.0  | 1                             | 50.0   | 2        | 100.0  | 1     | 50.0   |
| 計                                               | 110      | 58                        | 52.7   | 48                            | 43.6   | 105      | 95.5   | 93    | 84.5   |

| Q25. 事業継続性<br>計画項目<br>Q13-①<br>システムダウン<br>の発生状況 | 5. 人的なミス<br>に起因する<br>障害・誤処理 |      | 6. 内部犯罪に<br>よる緊急事態 |      | 7. 伝染病 |      | 8. その他 |     |
|-------------------------------------------------|-----------------------------|------|--------------------|------|--------|------|--------|-----|
|                                                 |                             |      |                    |      |        |      |        |     |
| 1. 全体的にダウンした                                    | 5                           | 71.4 | 1                  | 14.3 | 1      | 14.3 | 0      | 0.0 |
| 2. 部分的にダウンした                                    | 21                          | 47.7 | 13                 | 29.5 | 3      | 6.8  | 1      | 2.3 |
| 3. ダウンしない                                       | 31                          | 54.4 | 17                 | 29.8 | 3      | 5.3  | 0      | 0.0 |
| 無回答                                             | 0                           | 0.0  | 1                  | 50.0 | 0      | 0.0  | 0      | 0.0 |
| 計                                               | 57                          | 51.8 | 32                 | 29.1 | 7      | 6.4  | 1      | 0.9 |

ここでは実際に事業継続性計画を「作成している」、または「作成中」の事業者がどのようなリスクを想定しているか、システムダウンを「経験した」事業者とダウンを「経験していな

い」事業者で内容に大きな差があるか、確認することとした。

結果として全体的にダウンした事業体が7社と少なかったため、そこを含めた検討はできなかった。全体平均と比較すると「部分的にダウンした」事業体では「ネットワーク上の緊急事態」が52.3%と多くなっている。「人的なミスに起因する障害・誤処理」は47.7%と平均の51.8%より低くなっている。

また「ダウンしない」事業体では、「ネットワーク上の緊急事態」が42.1%と低く、「人的なミスに起因する障害・誤処理」が54.4%と多くなっている。この理由については不明である。全体的な傾向としては、事業継続性計画を作成しているか作成中の事業体では、その対象とするリスクとシステムダウンの経験との間に大きな相違点がないと考えられる。

### 3.6 Q13-②のクロス集計

Q13-②システムダウンはシステムの運用に悪影響を与えたか、さらに事業中断につながるものでしたか。  
(選択肢 1、2)

クロス対象項目

Q22-9. 貴事業体として重要と思われる要素:事業継続管理(災害対策、障害対策など)

Q24. 「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)。

#### 3.6.1 Q22-9 とのクロス集計

Q22-9. 貴事業体として重要と思われる要素:事業継続管理(災害対策、障害対策など)

①全体的にダウンした場合(全体の8.0%)

| Q22-9. 事業継続管理<br>Q13-②<br>システムダウンの影響 | 回答<br>件数 | 事業継続<br>管理(合計) |      |
|--------------------------------------|----------|----------------|------|
| 1. システム運用への悪影響                       | 33       | 8              | 24.2 |
| 2. 事業中断                              | 11       | 1              | 9.1  |
| 無回答                                  | 473      | 122            | 25.8 |
| 計                                    | 514      | 130            | 25.3 |

②部分的にダウンした場合(全体の41.8%)

| Q22-9.事業継続管理<br>Q13-②<br>システムダウンの影響 | 回答<br>件数 | 事業継続<br>管理(合計) |      |
|-------------------------------------|----------|----------------|------|
| 1. システム運用への悪影響                      | 190      | 51             | 26.8 |
| 2. 事業中断                             | 29       | 9              | 31.0 |
| 無回答                                 | 303      | 74             | 24.4 |
| 計                                   | 514      | 130            | 25.3 |

ここでは、システムが「全体的にダウンした」場合と「部分的にダウンした」場合に2分割し、さらに「システム運用への悪影響を与えた」場合と最悪の状況である「事業中断に至った」ケースの合計4つに分けた場合、情報セキュリティに関わる10の大きな要素のうち、「事業継続管理」を重要視しているか否かでどのような状況の変化があるか、クロス集計を行った。

回答件数が少ないため断定的なことはいえないが、「全体的にダウンして事業中断に至った」ケースは11件あり、そのうち、事業継続管理を重要視した事業体はわずか1件(9.1%)であった。また「全社的にダウンしてシステム運用への悪影響まで至った」事業体は33件で、そのうち事業継続管理が重要であると回答した事業体は8件(24.2%)であった。

一方、「部分的にダウンして事業中断にまで至った」事業体は29件あり、そのうち事業継続管理を重要視した事業体は9件(31.0%)であった。また「部分的にダウンしてシステム運用への悪影響が生じた」事業体は190件あり、そのうち事業継続管理を重要視する事業体は51件(26.8%)である。

件数が少ないため詳しい分析には至らないが、事業継続管理を重要視している割合は、「部

部分的にダウンして事業中断に至った」事業体が 31.0%で一番高く、次に「部分的にダウンしシステム運用への悪影響が生じた」事業体が 26.8%であり、全体的にダウンした事業体の方が事業継続管理を重要視する割合が低い。

さらに「全体的にダウンした事業体でシステム運用の悪影響に留めて」いて事業継続管理を重要視する事業体は 24.2%、「全体的にダウンして事業中断に至った」事業体が事業継続管理を重要視する割合はわずか9.1%であった。

全体的にダウンして事業中断に至ったというケースで事業継続管理を重要視する割合が低いという傾向をみると、事件や事故を経験したために事業継続管理を重要視する、という方向性よりも、事業継続管理を重要視していなかったがために全体的なダウンや事業中断を招いたという解釈の方が成り立つ可能性が高いといえる。

断定的なことはいえないが、事業継続管理を重要視するところほど、事件や事故を発生させない予防の考え方もしっかりしているのではないかと期待できる。

### 3.6.2 Q24 とのクロス集計

Q24. 「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)。

| Q24. 事業継続性計画<br>の作成状況<br>Q13-②<br>システムダウンの影響 | 回答<br>件数 | 1. 作成して<br>いる |       | 2. 作成中<br>である |       | 3. 作成を含め<br>検討中<br>である |       | 4. 作成して<br>いない |       |
|----------------------------------------------|----------|---------------|-------|---------------|-------|------------------------|-------|----------------|-------|
| 1. システム運用への悪影響                               | 190      | 31            | 36.5  | 8             | 33.3  | 45                     | 35.4  | 101            | 40.1  |
| 2. 事業中断                                      | 29       | 4             | 4.7   | 1             | 4.2   | 5                      | 3.9   | 15             | 6.0   |
| 無回答                                          | 303      | 51            | 60.0  | 15            | 62.5  | 78                     | 61.4  | 141            | 56.0  |
| 計                                            | 514      | 85            | 100.0 | 24            | 100.0 | 127                    | 100.0 | 252            | 100.0 |

| Q24. 事業継続性計画<br>の作成状況<br>Q13-②<br>システムダウンの影響 | 5. 必要ない |       | 無回答 |       |
|----------------------------------------------|---------|-------|-----|-------|
| 1. システム運用への悪影響                               | 2       | 22.2  | 3   | 17.6  |
| 2. 事業中断                                      | 1       | 11.1  | 3   | 17.6  |
| 無回答                                          | 6       | 66.7  | 12  | 70.6  |
| 計                                            | 9       | 100.0 | 17  | 100.0 |

『JIS X 5080』の事業継続性管理に定められた事業継続性計画を作成しているか否かでシステム運用への悪影響や事業中断に影響があるか、クロス集計を行った。

「作成している」85 事業体の場合、「システム運用への悪影響」が生じたところは 31 件 (36.5%) である。また「事業中断」を経験したところは 4 件 (4.7%) である。あわせて 41.2%の事業体が『JIS X 5080』を作成しつつ、これらの悪影響を経験している。

「作成中である」24 事業体は「システム運用への悪影響」が 8 件 (33.3%)、「事業中断」

1 件 (4.2%) である。あわせて 37.5% が何らかの影響を受けている。

「作成中を含め検討中である」127 事業体は「システム運用への悪影響」を経験したところが 45 社 (35.4%)、「事業中断」5 社 (3.9%)、あわせて 39.3% が影響を受けている。

「作成していない」252 事業体は、「システム運用への悪影響」を経験したところが 101 件 (40.1%)、「事業中断」を経験したところが 15 件 (6.0%)、あわせて 46.1% が悪影響を受けている。

これらの結果から、『JIS X 5080』を作成している事業体より作成していない方がシステム運用への悪影響を被ったり、また事業継続に至ってしまう割合が大きいことがわかる。作成していない場合は結果として事故発生時に事業中断に至る割合も大きいといえる。したがって事業継続性計画を作成するまでに十分な取組みを行う、というセキュリティへの取組みの深さが結果的にシステム運用への悪影響や事業中断を回避しているといえる。

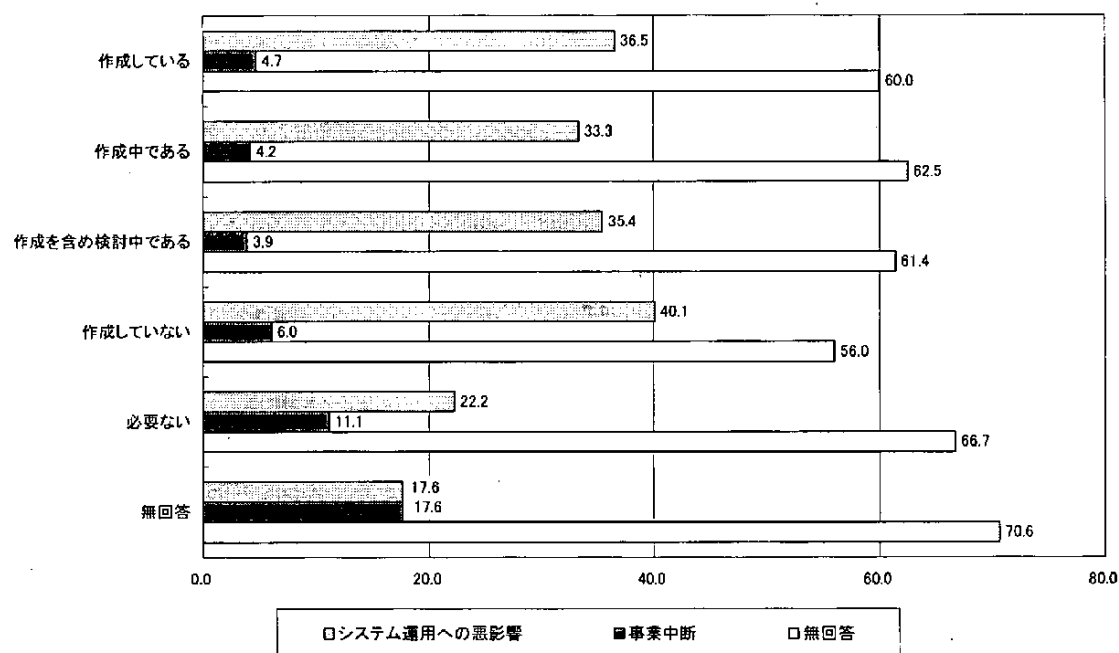


図3-6-1. システムダウンの影響度合いに対する事業継続性計画の作成状況

### 3.7 Q14 - ①のクロス集計

Q14-①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)

クロス対象項目

Q24.「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)。

| Q24. 事業継続性<br>計画の<br>作成状況<br><br>Q14-①<br>システムダウン<br>の原因 | 回<br>答<br>件<br>数 | 1. 作成して<br>いる |      | 2. 作成中で<br>ある |      | 3. 作成を含<br>め検討中<br>である |       | 4. 作成して<br>いない |      | 5. 必要<br>ない |     | 無回答 |      |
|----------------------------------------------------------|------------------|---------------|------|---------------|------|------------------------|-------|----------------|------|-------------|-----|-----|------|
| 1. 自然災害                                                  | 15               | 1             | 6.7  | 2             | 13.3 | 3                      | 20.0  | 7              | 46.7 | 1           | 6.7 | 1   | 6.7  |
| 2. 地震                                                    | 9                | 1             | 11.1 | 0             | 0.0  | 2                      | 22.2  | 6              | 66.7 | 0           | 0.0 | 0   | 0.0  |
| 3. 火災による事<br>故・障害                                        | 5                | 2             | 40.0 | 0             | 0.0  | 2                      | 40.0  | 0              | -    | 0           | 0.0 | 1   | 20.0 |
| 4. 停電                                                    | 35               | 4             | 11.4 | 1             | 2.9  | 7                      | 20.0  | 19             | 54.3 | 0           | 0.0 | 4   | 11.4 |
| 5. 電源機器・設備<br>障害                                         | 55               | 7             | 12.7 | 3             | 5.5  | 12                     | 21.8  | 30             | 54.5 | 0           | 0.0 | 3   | 5.5  |
| 6. 空調等障害                                                 | 17               | 1             | 5.9  | 2             | 11.8 | 4                      | 23.5  | 9              | 52.9 | 0           | 0.0 | 1   | 5.9  |
| 7. 通信障害                                                  | 65               | 9             | 13.8 | 6             | 9.2  | 13                     | 20.0  | 32             | 49.2 | 1           | 1.5 | 4   | 6.2  |
| 8. ネットワーク機<br>器などの障害                                     | 121              | 17            | 14.0 | 7             | 5.8  | 28                     | 23.1  | 65             | 53.7 | 1           | 0.8 | 3   | 2.5  |
| 9. サーバなどのハ<br>ードウェア障害                                    | 120              | 16            | 13.3 | 6             | 5.0  | 32                     | 26.7  | 62             | 51.7 | 2           | 1.7 | 2   | 1.7  |
| 10. OS障害                                                 | 40               | 3             | 7.5  | 1             | 2.5  | 13                     | 32.5  | 21             | 52.5 | 0           | 0.0 | 2   | 5.0  |
| 11. アプリケーショ<br>ンソフトウェア障害                                 | 104              | 22            | 21.2 | 2             | 1.9  | 28                     | 26.9  | 48             | 46.2 | 1           | 1.0 | 3   | 2.9  |
| 12. コンピュータウ<br>イルス、スパイウェ<br>アによる障害                       | 29               | 1             | 3.4  | 1             | 3.4  | 9                      | 31.0  | 16             | 55.2 | 0           | 0.0 | 2   | 6.9  |
| 13. 不正アクセス<br>や DOS 攻撃によ<br>るサービス中断                      | 9                | 1             | 11.1 | 0             | 0.0  | 3                      | 33.3  | 4              | 44.4 | 0           | 0.0 | 1   | 11.1 |
| 14. 人の悪意によ<br>る事故等                                       | 4                | 0             | 0.0  | 0             | 0.0  | 4                      | 100.0 | 0              | 0.0  | 0           | 0.0 | 0   | 0.0  |
| 15. オペミス等、人<br>の過失による事故<br>等                             | 79               | 10            | 12.7 | 3             | 3.8  | 22                     | 27.8  | 43             | 54.4 | 0           | 0.0 | 1   | 1.3  |
| 16. その他                                                  | 6                | 1             | 16.7 | 0             | 0.0  | 3                      | 50.0  | 1              | 16.7 | 0           | 0.0 | 1   | 16.7 |
| 無回答                                                      | 3                | 1             | 33.3 | 0             | 0.0  | 1                      | 33.3  | 1              | 33.3 | 0           | 0.0 | 0   | 0.0  |
| 計                                                        | 248              | 41            | 16.5 | 10            | 4.0  | 54                     | 21.8  | 131            | 52.8 | 4           | 1.6 | 8   | 3.2  |

過去1年間に発生したシステムダウンの原因別に、『JIS X 5080』に定められている事業継続性計画を作成しているか、クロス集計を行った。集計対象である248件のうち、分析はシステムダウンの原因について回答件数が30件以上のものに限定し、事業継続性計画については比較が明確になる「作成している」(41件/16.5%)、「作成していない」(131件/52.8%)の2つを対象とした。

過去1年間で発生したシステムダウンの原因のうち、「停電」を選択した35件の場合、事業継続性計画を「作成している」は4件(11.4%)、「作成していない」は19件(54.3%)であった。

「電源機器・設備障害」をあげた55件では「作成している」7件(12.7%)、「作成していない」30件(54.5%件)であった。

「通信障害」をあげた65件では「作成している」9件(13.8%)、「作成していない」32件(49.2%)であった。

「ネットワーク機器などの障害」を選択した121件では「作成している」17件(14.0%)、「作成していない」65件(53.7%)であった。

「サーバなどのハードウェア障害」をあげた120件では「作成している」16件(13.3%)、「作成していない」62件(51.7%)であった。

「OS障害」をあげた40件では「作成している」3件(7.5%)、「作成していない」21件(52.5%)であった。

「アプリケーションソフトウェア障害」を選択した104件では「作成している」22件(21.2%)、「作成していない」48件(46.2%)であった。

「オペミス等人の過失による事故等」を選択した79件では「作成している」10件(12.7%)、「作成していない」43件(54.4%)であった。

ここで「作成している」割合を評価する。全体平均よりも高い事業継続性計画の作成割合を示したものは「アプリケーションソフトウェア障害」である。平均が16.5%であるのに対して21.2%となっている。当然作成していない割合も46.2%と平均の52.8%よりも低い。一方、その他の原因はいずれも「作成している」割合が平均よりも低かった。

次に「作成していない」を評価すると、「作成していない」割合が高いシステムダウンの原因は「停電」、「電源機器・設備障害」、「ネットワーク機器などの障害」、「オペミス等・人の過失による事故等」がある。このようにみても、停電、電源系統は安心して不意打ちをくらったということが考えられる。ネットワーク機器などの障害も同様と思われる。つまり、これらは比較的日本では安定的なシステム構成要素であるため、万一の事業継続性計画を検討する際には想定リスクとして優先順位が下がるのではないかと考えられる。またオペミス等の人の過失による事故については最近の情報セキュリティが人的要素を重要視しているのに対して、各組織で実際にマニュアルを作成する場合には想定災害として人的ミス、特に同じ組織のメンバーの人的ミスを記載しにくい、という心理的な側面があるのではないと思われる。

これらを総合すると、アプリケーションソフトウェア障害を選択した事業体は事業継続性計画も比較的作成しているところが多い。一方不意打ちとなる原因は「停電」、「電源機器・設備障害」、「ネットワーク機器などの障害」という安定したインフラや機械まわりの原因と、「オペミス等人の過失による事故等」である。これらの要素に留意することにより、想定外の対応とならないことができる。

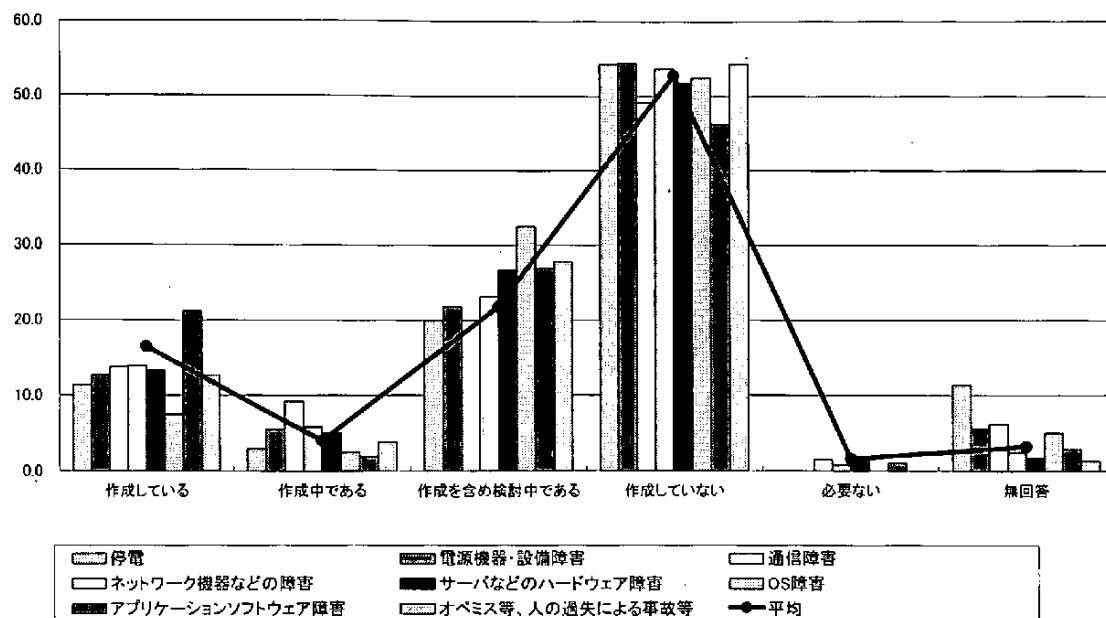


図3-7-1. システムダウンの原因と事業継続性計画の作成状況の関係

### 3.8 Q18のクロス集計

Q18.情報セキュリティの確保にとり、基本的に重要な要素は何だと思いますか。(複数回答)

クロス対象項目

Q21. 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)

Q30-8. 貴事業体では従業員に対し、情報セキュリティの一般知識に関する教育を実施していますか。

Q31. 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。(単一回答)

#### 3.8.1 Q21 とのクロス集計

Q21. 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)

Q21 からみたQ18

| Q21. 管理上の問題点<br>Q18. 重要要素 | 回答件数 |       | 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. 専門要員がいない(要員が確保できない) |      | 4. 組織の従業員に対する負担がかかりすぎる |      |
|---------------------------|------|-------|------------------|------|---------------|------|------------------------|------|------------------------|------|
| 1. 経営者層の理解                | 391  | 76.1  | 80               | 93.0 | 259           | 80.7 | 176                    | 77.9 | 124                    | 89.2 |
| 2. 管理者の理解                 | 243  | 47.3  | 43               | 50.0 | 158           | 49.2 | 120                    | 53.1 | 81                     | 58.3 |
| 3. 担当者の理解                 | 206  | 40.1  | 30               | 34.9 | 135           | 42.1 | 100                    | 44.2 | 74                     | 53.2 |
| 4. 社内全体の理解                | 429  | 83.5  | 67               | 77.9 | 271           | 84.4 | 193                    | 85.4 | 110                    | 79.1 |
| 5. 社内規定やルールの整備            | 303  | 58.9  | 49               | 57.0 | 199           | 62.0 | 143                    | 63.3 | 90                     | 64.7 |
| 6. その他                    | 13   | 2.5   | 2                | 2.3  | 9             | 2.8  | 6                      | 2.7  | 6                      | 4.3  |
| 無回答                       | 2    | 0.4   | 0                | 0.0  | 1             | 0.3  | 1                      | 0.4  | 0                      | 0.0  |
| 計                         | 514  | 100.0 | 86               | 16.7 | 321           | 62.5 | 226                    | 44.0 | 139                    | 27.0 |

| Q21. 管理上の問題点<br>Q18. 重要要素 | 5. 組織の従業員に対する教育・訓練がいきとどかない |      | 6. ノウハウが不足している |      | 7. どこまでやればよいのか基準が示されていない |      | 8. 要求に合致するもの(サービス/製品)がない |      | 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 |      |
|---------------------------|----------------------------|------|----------------|------|--------------------------|------|--------------------------|------|-----------------------------------|------|
| 1. 経営者層の理解                | 203                        | 75.5 | 110            | 72.8 | 166                      | 76.9 | 18                       | 66.7 | 76                                | 77.6 |
| 2. 管理者の理解                 | 136                        | 50.6 | 82             | 54.3 | 99                       | 45.8 | 13                       | 48.1 | 41                                | 41.8 |
| 3. 担当者の理解                 | 111                        | 41.3 | 71             | 47.0 | 77                       | 35.6 | 11                       | 40.7 | 31                                | 31.6 |
| 4. 社内全体の理解                | 237                        | 88.1 | 126            | 83.4 | 189                      | 87.5 | 24                       | 88.9 | 89                                | 90.8 |
| 5. 社内規定やルールの整備            | 176                        | 65.4 | 92             | 60.9 | 138                      | 63.9 | 17                       | 63.0 | 67                                | 68.4 |
| 6. その他                    | 8                          | 3.0  | 7              | 4.6  | 7                        | 3.2  | 1                        | 3.7  | 6                                 | 6.1  |
| 無回答                       | 1                          | 0.4  | 0              | 0.0  | 0                        | 0.0  | 0                        | 0.0  | 1                                 | 1.0  |
| 計                         | 269                        | 52.3 | 151            | 29.4 | 216                      | 42.0 | 27                       | 5.3  | 98                                | 19.1 |

| Q21. 管理上の<br>問題点<br>Q18. 重要要素 | 10. 情報セキュリティ管理が<br>事業の国際化<br>に見合っていない |       | 11. その他 |       | 12. 特に<br>問題はない |      | 無回答 |      |
|-------------------------------|---------------------------------------|-------|---------|-------|-----------------|------|-----|------|
| 1. 経営者層の理解                    | 7                                     | 100.0 | 5       | 83.3  | 8               | 80.0 | 1   | 50.0 |
| 2. 管理者の理解                     | 2                                     | 28.6  | 2       | 33.3  | 4               | 40.0 | 0   | 0.0  |
| 3. 担当者の理解                     | 2                                     | 28.6  | 1       | 16.7  | 5               | 50.0 | 0   | 0.0  |
| 4. 社内全体の理解                    | 5                                     | 71.4  | 6       | 100.0 | 7               | 70.0 | 0   | 0.0  |
| 5. 社内規定やルールの<br>整備            | 5                                     | 71.4  | 3       | 50.0  | 4               | 40.0 | 0   | 0.0  |
| 6. その他                        | 0                                     | 0.0   | 1       | 16.7  | 0               | 0.0  | 0   | 0.0  |
| 無回答                           | 0                                     | 0.0   | 0       | 0.0   | 0               | 0.0  | 1   | 50.0 |
| 計                             | 7                                     | 1.4   | 6       | 1.2   | 10              | 1.9  | 2   | 0.4  |

情報セキュリティの管理上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、クロス集計を行った。なお、ここでは回答数に差があるため 20 件以上の回答項目について分析を行った。

なお、前回調査での設問「法規制の整備」は、「社内規程とルールの整備」と自組織内の問題としての意識調査に変更しているが、複数回答のため、全体に大きな影響を与えないと考えるため、前回調査との比較は可能と判断している。

「経営者層の理解が得られない」の場合

| 調査年度<br>重要要素        | 平成 17 年度<br>(86 事業体) |       |       | 平成 15 年度<br>(92 事業体) |       |       |
|---------------------|----------------------|-------|-------|----------------------|-------|-------|
|                     | クロス                  | 平均    | 差     | クロス                  | 平均    | 差     |
| 経営者層の理解             | 93.0%                | 76.1% | +16.9 | 88.0%                | 71.2% | +16.8 |
| 管理者の理解              | 50.0%                | 47.3% | +2.7  | 34.8%                | 39.7% | -4.9  |
| 担当者の理解              | 34.9%                | 40.1% | -5.2  | 19.6%                | 30.9% | -11.3 |
| 社内全体の理解             | 77.9%                | 83.5% | -5.6  | 79.3%                | 85.5% | -6.2  |
| 社内規定やルールの整備(法規制の整備) | 57.0%                | 58.9% | -1.9  | 12.0%                | 14.4% | -2.4  |

「経営者層の理解が得られない」を選択した 86 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」93.0%、「管理者の理解」50.0%、「担当者の理解」34.9%、「社内全体の理解（エンドユーザを含む）」77.9%、「社内規程やルールの整備」57.0%となっている。この傾向は全体の平均とほぼ同じである。ただしそれぞれを平均と比べると、「経営者層の理解」が 16.9 ポイントと非常に高く、「管理者の理解」が 2.7 ポイント高、「担当者の理解」が 5.1 ポイント低、「社内全体の理解」が 5.6 ポイント低、「社内規程とルールの整備」が 1.9 ポイント低い結果となっている。

前回調査との比較でいくと、設問が「法規制の整備」から「社内規程とルールの整備」に変更になったところでは社外か社内の問題なので選択割合が大きく異なっている。

「経営者層の理解が得られない」と、Q21 のその他の選択肢との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、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。この傾向は前回調査と同様である。

以下、Q21 の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 321 事業体の傾向をみると、「経営者層の理解」80.7% (平均より 4.6 ポイント高)、「管理者の理解」49.2% (1.9 ポイント高)、「担当者の理解」42.1% (2.0 ポイント高)、「社内全体の理解」84.4% (0.9 ポイント高)、「社内規程とルールを整備」62.0% (3.1 ポイント高)と、すべての項目で平均よりも上回った。「経営者層の理解」を選択した割合は全体で3番目に高く、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。この傾向は前回も同様であった。

「専門要員がいない」の 226 事業体の回答は、「経営者層の理解」77.9% (平均より 1.8 ポイント高)、「管理者の理解」53.1% (5.8 ポイント高)、「担当者の理解」44.2% (4.1 ポイント高)、「社内全体の理解」85.4% (0.9 ポイント高)、「社内規程とルールを整備」は 63.3% (4.4 ポイント高)と、平均と比べ全体的に高い割合になっている。「管理者の理解」を選択した割合が高いことから、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。これも前回調査と同様の傾向である。

「組織の従業員に対する負担がかかりすぎる」139 事業体の回答は、「経営者層の理解」89.2% (平均より 13.1 ポイント高)、「管理者の理解」58.3% (11.0 ポイント高)、「担当者の理解」53.2% (13.2 ポイント高)、「社内全体の理解」79.1% (4.4 ポイント低)、「社内規程とルールを整備」64.7% (5.8 ポイント高)である。このうち「管理者の理解」と「担当者の理解」を選択した割合は全体で最も高く、「経営者層の理解」は2番目であった。相対的にみれば、従業員への負担については経営者の理解と各職場の現場の管理や情報セキュリティを推進する組織の担当者の理解を強く意識していると考えられる。一方「社内全体の理解」が一番低いのは意外であるが、これは推進する組織の責任感の大きさを表している可能性もある。

「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 269 事業体の回答は、「経営者層の理解」75.5% (平均より 0.6 ポイント低)、「管理者の理解」50.6% (3.3%高)、「担当者の理解」41.3% (1.2 ポイント高)、「社内全体の理解」88.1% (4.6 ポイント高)、「社内規程とルールを整備」65.4% (6.5 ポイント高)である。訓練に関しては訓練を受ける側の全社的理解と、教えるための社内規程やルールを整備がまず大切であると考えられている。

「ノウハウが不足している」を選択した 151 事業体の回答は、「経営者層の理解」72.8% (平均より 3.3 ポイント低)、「管理者の理解」54.3% (7.0 ポイント高)、「担当者の理解」47.0% (6.9%高)である。一方「社内全体の理解」83.4% (0.1 ポイント低)、「社内規程とルールを整備」60.9%

(2.0 ポイント高)である。前回調査同様「管理者の理解」は割合が2番目に高く、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216事業体の回答は、「経営者層の理解」76.9% (平均より0.8ポイント高)、「管理者の理解」45.8% (1.5ポイント低)、「担当者の理解」35.6% (4.5ポイント低)、「社内全体の理解」87.5% (4.0ポイント高)、「社内規程とルール整備」63.9% (5.0ポイント高)である。前回調査では担当者の理解の問題と捉えられていたが、今回は前回調査とは異なり、担当者の理解が減少し、社内全体の理解や社内規程とルールの整備が高くなっている。どこまでやるかについてはまず組織内での基準の作成が大きいとの意識の表れである。

「要求に合致するもの(サービス/製品)がない」を選択した27事業体の回答は、「経営者層の理解」66.7% (平均より9.4ポイント低)、「管理者の理解」48.1% (0.8ポイント高)、「担当者の理解」40.7% (0.6ポイント高)、「社内全体の理解」88.9% (5.4ポイント高)、「社内規程とルールの整備」63.0% (4.1ポイント高)である。前回同様に回答件数の数が少ないため確実なことはいえない。前は経営者の理解によるという割合が大変多かったが、今回調査では経営者の問題というより製品の購入にあたり、社内全体の理解やどこまで何を実施するのかを定める社内規程やルール作りが大切である、との認識に変化した可能性がある。

「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98事業体の回答は、「経営者層の理解」77.6% (平均より1.5ポイント高)、「管理者の理解」41.8% (5.5ポイント低)、「担当者の理解」31.6% (8.5ポイント低)、「社内全体の理解」90.8% (7.3ポイント高)、「社内規程とルールの整備」68.4% (9.5ポイント高)である。組織内での価値観や倫理観の問題であるため、管理者、担当者ベースの問題ではなく、経営者、組織内全体での社内規程やルールの整備という問題として捉えられている。

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、この結果は前回同様であり、また結果も妥当といえる。「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担がかかりすぎる」、「ノウハウが不足している」であり、これも前回同様である。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」、「コストがかかりすぎる」、「専門家がいない」であり、具体的に取り組む時に直面する問題を重視している。一方「どこまでやればよいのか基準が示されない」という選択は減少しており、情報セキュリティが抽象論から組織内に浸透しはじめ、具体的な取り組みが開始され始めている状況にあると考えられる。また、「社内全体の理解」を求めているのは「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潮がない」、「組織の従業員に対する教育・訓練がいき届かない」、「要求に合致するもの(サービス/製品)がない」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。

「社内規程やルールの整備」については「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潮がない」、「組織の従業員に対する教育・訓練が行き届かない」、「組織の従業員に対する負担がかかりすぎる」、が比較的選択が多く、倫理観を植え付けるためには規程やルールの整備を行ったうえで教育訓練を実施する必要があることを示しているが、一方、そのことが従業員に対しての負担となっていることを示すものと考えられる。

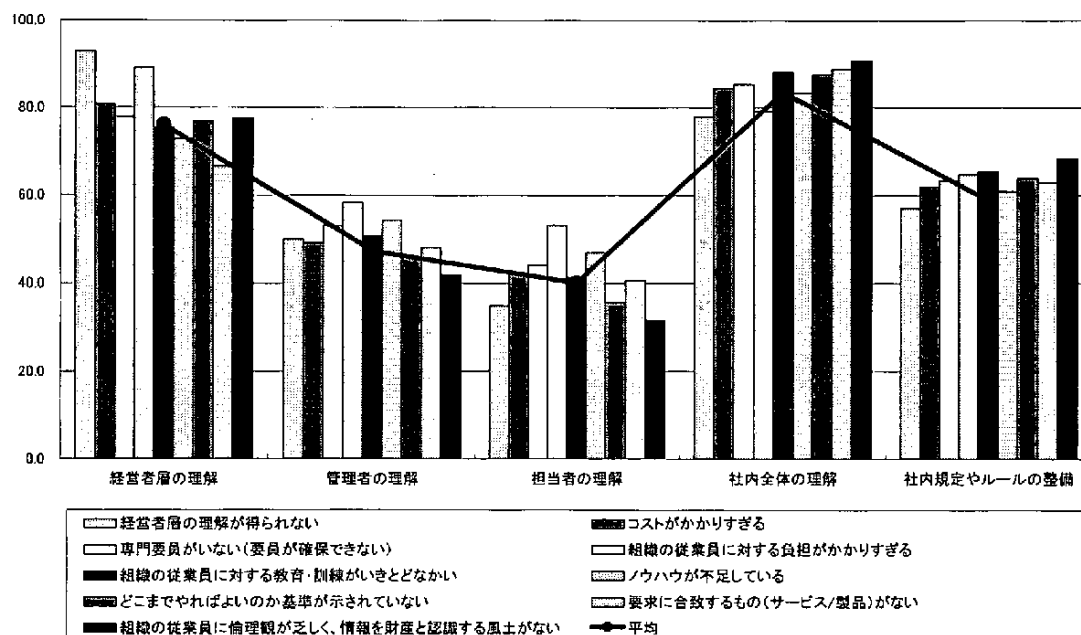


図3-8-1. 情報セキュリティの重要要素と情報セキュリティ管理上の問題点との関係

### 3.8.2 Q30-8 とのクロス集計

Q30-8. 貴事業体では従業員に対し、情報セキュリティの一般知識に関する教育を実施していますか。

Q18の結果としては、「社内全体の理解」が83.5%と最も高く、次いで「経営者層の理解」76.1%と続いている。ここでは情報セキュリティ確保上の重要要素と従業員への情報セキュリティに関する教育・訓練の実施状況との関係についてクロス分析を行った。

| Q30-8. 教育の実施状況<br>Q18. 重要要素 | 回答<br>件数 | 1. 定期的に<br>実施して<br>いる |      | 2. 時々実施<br>している |      | 3. 実施を予<br>定している |      | 4. 実施して<br>いない |      | 無回答 |     |
|-----------------------------|----------|-----------------------|------|-----------------|------|------------------|------|----------------|------|-----|-----|
| 1. 経営者層の理解                  | 391      | 141                   | 36.1 | 130             | 33.2 | 45               | 11.5 | 64             | 16.4 | 11  | 2.8 |
| 2. 管理者の理解                   | 243      | 93                    | 38.3 | 78              | 32.1 | 28               | 11.5 | 36             | 14.8 | 8   | 3.3 |
| 3. 担当者の理解                   | 206      | 87                    | 42.2 | 68              | 33.0 | 19               | 9.2  | 25             | 12.1 | 7   | 3.4 |
| 4. 社内全体の理解<br>(エンドユーザを含む)   | 429      | 150                   | 35.0 | 145             | 33.8 | 53               | 12.4 | 71             | 16.6 | 10  | 2.3 |
| 5. 社内規定やルールの整備              | 303      | 109                   | 36.0 | 99              | 32.7 | 40               | 13.2 | 45             | 14.9 | 10  | 3.3 |
| 6. その他                      | 13       | 5                     | 38.5 | 2               | 15.4 | 1                | 7.7  | 5              | 38.5 | 0   | 0.0 |
| 無回答                         | 2        | 0                     | 0.0  | 1               | 50.0 | 0                | 0.0  | 1              | 50.0 | 0   | 0.0 |
| 計                           | 514      | 170                   | 33.1 | 174             | 33.9 | 66               | 12.8 | 89             | 17.3 | 15  | 2.9 |

情報セキュリティ確保上の重要要素と情報セキュリティ教育の実施状況との関連について、それぞれの差をまとめた結果は以下のとおりである（（ ）内は前回調査結果）。

| Q30-8. 教育・訓練<br>Q18. 重要要素 | ・定期的実施している<br>・時々実施している<br>・実施を予定している | 実施していない     | 差           |
|---------------------------|---------------------------------------|-------------|-------------|
| 経営者層の理解                   | 80.8 (57.8)                           | 16.4 (40.6) | 64.4 (17.2) |
| 管理者の理解                    | 81.9 (58.8)                           | 14.8 (40.4) | 67.1 (18.4) |
| 担当者の理解                    | 84.4 (61.5)                           | 12.1 (37.4) | 72.3 (24.1) |
| 社内全体の理解                   | 81.2 (59.4)                           | 16.6 (39.3) | 64.6 (20.1) |
| 社内規定やルールを整備<br>(法規制の整備)   | 81.9 (67.8)                           | 14.9 (31.0) | 67.0 (36.8) |
| その他                       | 61.6 (50.0)                           | 38.5 (50.0) | 23.1 (0.0)  |

情報セキュリティの確保について、重要要素別に情報セキュリティに関する教育・訓練の実施状況を整理したが、「その他」以外についてはその差があまり感じられない。

「担当者の理解」では「実施している」、「実施を予定している」の合計値が7割を超えて他と比べ若干高くなっているが、特に差が出ていると考えるほどのものではない。

また、「その他」の「実施している」または「実施を予定している」の合計値が低い、これは「その他」の詳細な理由がまちまちであり、また、回答件数も13件で全体回答数の2.5%と低いため、あまり問題にすることはない。

なお、前回調査では、「実施（予定）」の合計値と「未実施」の差はあまりなく、最大で「法規制の整備」で36.8ポイントの差がみられた。しかし、今回調査では「実施（予定）」の合計値と「未実施」の差が大きく（最大は「担当者の理解」72.3ポイント）なっているのが最大の特徴である。今回の調査でみるかぎりでは、情報セキュリティの確保にとり、重要な視点に関わらず関連の教育・訓練の重要性を認識してその充実を図っているものと思われる。今後の教育・訓練には、経営者層、管理者層もその対象とする必要があると思われる。

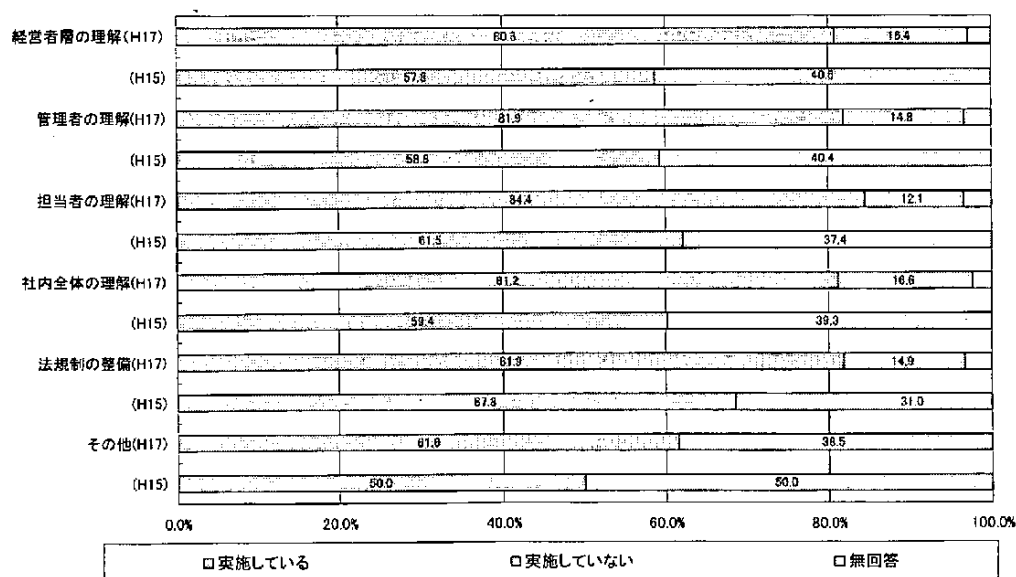


図3-8-2. 情報セキュリティの重要要素と情報セキュリティ教育実施状況との関係

### 3.8.3 Q31 とのクロス集計

Q31. 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。(単一回答)

| Q31. 人材養成<br>Q18. 重要要素 | 回 答<br>件数 | 1. 自社育成<br>プログラムに<br>より高度な人<br>材育成を行っ<br>ている | 2. 民間の教<br>育機関を利用<br>して育成して<br>いる | 3. 情報セキュ<br>リティアドミ<br>ニストレータな<br>どの資格試験を<br>活用している |
|------------------------|-----------|----------------------------------------------|-----------------------------------|----------------------------------------------------|
| 1. 経営者層の理解             | 391       | 47 12.0                                      | 85 21.7                           | 36 9.2                                             |
| 2. 管理者の理解              | 243       | 35 14.4                                      | 54 22.2                           | 21 8.6                                             |
| 3. 担当者の理解              | 206       | 32 15.5                                      | 51 24.8                           | 17 8.3                                             |
| 4. 社内全体の理解(エンドユーザを含む)  | 429       | 49 11.4                                      | 100 23.3                          | 30 7.0                                             |
| 5. 社内規定やルールの整備         | 303       | 33 10.9                                      | 71 23.4                           | 25 8.3                                             |
| 6. その他                 | 13        | 2 15.4                                       | 5 38.5                            | 0 0.0                                              |
| 無回答                    | 2         | 0 0.0                                        | 0 0.0                             | 0 0.0                                              |
| 計                      | 514       | 57 11.1                                      | 110 21.4                          | 42 8.2                                             |

| Q31. 人材養成<br>Q18. 重要要素 | 4. 特に行って<br>いない | 5. 必要ない | 無回答    |
|------------------------|-----------------|---------|--------|
| 1. 経営者層の理解             | 209 53.5        | 0 0.0   | 14 3.6 |
| 2. 管理者の理解              | 123 50.6        | 1 0.4   | 9 3.7  |
| 3. 担当者の理解              | 98 47.6         | 1 0.5   | 7 3.4  |
| 4. 社内全体の理解(エンドユーザを含む)  | 234 54.5        | 0 0.0   | 16 3.7 |
| 5. 社内規定やルールの整備         | 166 54.8        | 0 0.0   | 8 2.6  |
| 6. その他                 | 6 46.2          | 0 0.0   | 0 0.0  |
| 無回答                    | 2 100.0         | 0 0.0   | 0 0.0  |
| 計                      | 283 55.1        | 2 0.4   | 20 3.9 |

セキュリティ確保上の重要要素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。

前回調査との結果を比較すると以下のとおりである。(( ) 内が前回調査結果))

| Q31. 人材養成<br>Q18. 重要要素   | 自社育成<br>プログラム<br>により育成 | 民間の教育<br>機関を利用<br>して育成 | 情報セキュリティ<br>アドミニストレー<br>タ試験の活用 | 人材養成の<br>合計 | 特に行って<br>いない |
|--------------------------|------------------------|------------------------|--------------------------------|-------------|--------------|
| 経営者層の理解                  | 12.0 (8.6)             | 21.7 (5.1)             | 9.2 (7.0)                      | 42.9 (20.7) | 53.5 (74.5)  |
| 管理者の理解                   | 14.4 (8.8)             | 22.2 (6.7)             | 8.6 (5.8)                      | 45.2 (21.3) | 50.6 (72.5)  |
| 担当者の理解                   | 15.5 (11.8)            | 24.8 (6.4)             | 8.3 (3.7)                      | 48.6 (21.9) | 47.6 (71.7)  |
| 社内全体の理解                  | 11.4 (8.7)             | 23.3 (4.6)             | 7.0 (6.2)                      | 41.7 (19.5) | 54.5 (76.2)  |
| 社内規定やルールの整備<br>(法々規制の整備) | 10.9 (11.5)            | 23.4 (5.7)             | 8.3 (4.6)                      | 42.6 (21.8) | 54.8 (66.7)  |
| その他                      | 15.4 (0.0)             | 38.5 (50.0)            | 0.0 (0.0)                      | 53.9 (50.0) | 46.2 (50.0)  |

情報セキュリティの人材育成は、どの重要要素をとってみても「民間の教育機関を利用して育成」が高く、「自社育成プログラムにより育成」がこれに続いている。前回調査では「自社育成プログラムにより育成」の割合が高かったが、今回の調査では「民間の教育機関を利用して育成」が高い割合を示している。ただし、前回調査での質問「民間資格を利用して育成している」を「民間の教育機関を利用して育成している」と変更したことも影響していると思われる。

何らかの方法で人材育成を「行っている」割合の合計をみると、「その他」が 53.9% (△H15:50.0%、3.9 ポイント増)と最も高く、次いで「担当者の理解」48.6% (△H15:21.9%、26.7 ポイント増)、「管理者の理解」45.2%(△H15:21.3%、23.9 ポイント増)となっているが、いずれの要素においても「民間の教育機関を利用して育成」、「自社育成プログラムにより育成」が高いポイントとなっている。

重要要素別に「特に行っていない」の傾向をみると、前回調査では「社内全体の理解」が 76.2% (▽H17:54.5%、21.7 ポイント減)で第1位であったのに対し、今回調査では、前回第5位の「社内規定やルールの整備」が (54.8%▽H15:66.7%、11.9 ポイント減) 第1位となった。ただし、これは設問が「法規制の整備」から「社内規程やルールの整備」に変更したことも影響していると思われる。

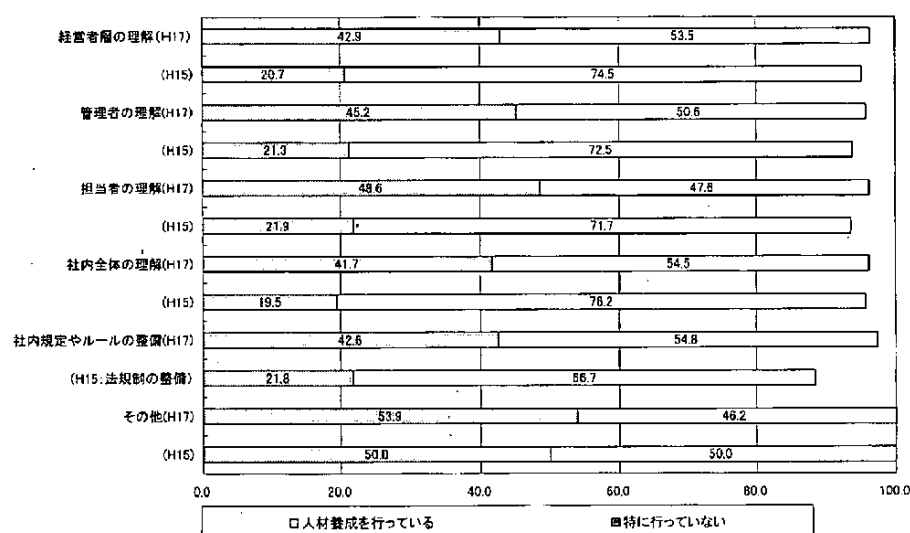


図3-8-3. 情報セキュリティの重要要素と情報セキュリティ人材養成の実施状況の関係

また、何らかの方法で「人材育成を行っている」の合計と、「特に行っていない」との差を整理した結果は以下のとおりである。( ( )内は前回の調査結果)

| Q31. 人材養成<br>Q18. 重要要素 | 人材養成合計      | 特に行っていない    | 差             |
|------------------------|-------------|-------------|---------------|
| 経営者層の理解                | 42.9 (20.7) | 53.5 (74.5) | -10.6 (-53.8) |
| 管理者の理解                 | 45.2 (21.3) | 50.6 (72.5) | -5.4 (-50.4)  |
| 担当者の理解                 | 48.6 (21.9) | 47.6 (71.7) | 1.0 (-49.8)   |
| 社内全体の理解                | 41.7 (19.5) | 54.5 (76.2) | -12.8 (-56.7) |
| 法規制の整備                 | 42.6 (21.8) | 54.8 (66.7) | -12.2 (-44.9) |
| その他                    | 53.9 (50.0) | 46.2 (50.0) | 7.7 (0.0)     |

何らかの人材養成を「行っている」と「特に行っていない」との差をみると、前回調査では「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」(7.8%)、「民間資格を利用して育成」(4.8%)、「情報セキュリティアドミニストレータ試験を活用」(6.3%)は、実施率がいずれも1割に満たなかったため、「特に行っていない」(76.5%)との差は大きかった。しかし、今回調査ではその差が小さくなっており、重要要素別にみると、「担当者の理解」では若干ではあるが「人材育成を行っている」(48.6%)が「特に行っていない」(47.6%)を上回っている。

いずれにしても、どの重要な要素をとってみても、何らかの方法で「人材育成を行っている」割合が高くなり、「特に行っていない」の割合が低くなっているのが特徴である。

各事業体とも情報セキュリティに関する人材養成を重視している傾向が強まっていると考えられる。

### 3.9 Q22 のクロス集計

Q22. 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。

クロス対象項目

Q22 の優先順位(第1位×第2位)

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3-9-1. 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)                 | 157 | 42  |
| 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)          | 42  | 72  |
| 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)     | 41  | 56  |
| 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)            | 102 | 100 |
| 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  | 34  |
| 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)       | 35  | 61  |
| 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)            | 21  | 53  |
| 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) | 0   | 8   |
| 9          | 事業継続計画(災害対策、障害対策など)                      | 41  | 34  |
| 10         | 準拠(法律遵守、システム監査など)                        | 34  | 25  |

表3-9-2. 各要素別第2位選択項目

| 第1位「①情報セキュリティポリシー」の場合 |    |      | 第1位「②情報セキュリティ組織」の場合 |    |      |
|-----------------------|----|------|---------------------|----|------|
| 情報セキュリティ組織            | 53 | 33.8 | 情報セキュリティポリシー        | 7  | 16.7 |
| 情報資産の分類および管理          | 21 | 13.4 | 情報資産の分類および管理        | 8  | 19.0 |
| 人的セキュリティ              | 40 | 25.5 | 人的セキュリティ            | 15 | 35.7 |
| 物理的および環境的セキュリティ       | 7  | 4.5  | 物理的および環境的セキュリティ     | 7  | 16.7 |
| 通信および運用管理             | 9  | 5.7  | 通信および運用管理           | 2  | 4.8  |
| アクセス制御                | 11 | 7.0  | アクセス制御              | 1  | 2.4  |
| システム開発およびメンテナンス       | 1  | 0.6  | システム開発およびメンテナンス     | 0  | 0.0  |
| 事業継続計画                | 8  | 5.1  | 事業継続計画              | 1  | 2.4  |
| 準拠                    | 7  | 4.5  | 準拠                  | 1  | 2.4  |

| 第1位「③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          | 4  | 9.8  |
| 情報セキュリティ組織            | 6  | 14.6 |
| 人的セキュリティ              | 14 | 34.1 |
| 物理的および環境的セキュリティ       | 3  | 7.3  |
| 通信および運用管理             | 5  | 12.2 |
| アクセス制御                | 4  | 9.8  |
| システム開発およびメンテナンス       | 1  | 2.4  |
| 事業継続計画                | 4  | 9.8  |
| 準拠                    | 0  | 0.0  |

| 第1位「④人的セキュリティ」の場合 |    |      |
|-------------------|----|------|
| 情報セキュリティポリシー      | 11 | 10.8 |
| 情報セキュリティ組織        | 9  | 8.8  |
| 情報資産の分類および管理      | 18 | 17.6 |
| 物理的および環境的セキュリティ   | 11 | 10.8 |
| 通信および運用管理         | 24 | 23.5 |
| アクセス制御            | 12 | 11.8 |
| システム開発およびメンテナンス   | 0  | 0.0  |
| 事業継続計画            | 9  | 8.8  |
| 準拠                | 8  | 7.8  |

| 第1位「⑤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             | 2 | 15.4 |
| 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                 | 4 | 30.8 |
| 物理的および環境的セキュリティ          | 3 | 23.1 |
| 通信および運用管理                | 3 | 23.1 |
| システム開発およびメンテナンス          | 0 | 0.0  |
| 事業継続計画                   | 1 | 7.7  |
| 準拠                       | 0 | 0.0  |

| 第1位「⑥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            | 1  | 2.9  |
| 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  | 5.7  |
| 人的セキュリティ                | 7  | 20.0 |
| 物理的および環境的セキュリティ         | 2  | 5.7  |
| アクセス制御                  | 18 | 51.4 |
| システム開発およびメンテナンス         | 2  | 5.7  |
| 事業継続計画                  | 3  | 8.6  |
| 準拠                      | 0  | 0.0  |

| 1位「⑦アクセス制御」の場合  |   |      |
|-----------------|---|------|
| 情報セキュリティポリシー    | 2 | 9.5  |
| 情報セキュリティ組織      | 1 | 4.8  |
| 情報資産の分類および管理    | 1 | 4.8  |
| 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       | 9 | 42.9 |
| システム開発およびメンテナンス | 1 | 4.8  |
| 事業継続計画          | 0 | 0.0  |
| 準拠              | 1 | 4.8  |

| 第1位「⑧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          | 0 | 0.0 |
| 通信および運用管理                | 0 | 0.0 |
| アクセス制御                   | 0 | 0.0 |
| 事業継続計画                   | 0 | 0.0 |
| 準拠                       | 0 | 0.0 |

| 第1位「⑨事業継続計画」の場合 |   |      |
|-----------------|---|------|
| 情報セキュリティポリシー    | 4 | 9.8  |
| 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    | 5 | 12.2 |
| 人的セキュリティ        | 9 | 22.0 |
| 物理的および環境的セキュリティ | 0 | 0.0  |
| 通信および運用管理       | 9 | 22.0 |
| アクセス制御          | 4 | 9.8  |
| システム開発およびメンテナンス | 2 | 4.9  |
| 準拠              | 8 | 19.5 |

| 第1位「⑩準拠」の場合     |    |      |
|-----------------|----|------|
| 情報セキュリティポリシー    | 11 | 32.4 |
| 情報セキュリティ組織      | 3  | 8.8  |
| 情報資産の分類および管理    | 1  | 2.9  |
| 人的セキュリティ        | 7  | 20.6 |
| 物理的および環境的セキュリティ | 2  | 5.9  |
| 通信および運用管理       | 0  | 0.0  |
| アクセス制御          | 0  | 0.0  |
| システム開発およびメンテナンス | 1  | 2.9  |
| 事業継続計画          | 8  | 23.5 |

| 第2位<br>第1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    |              | 53         | 21         | 40       | 7             | 9       | 11     | 1             | 8      | 7  |
| 情報セキュリティ組織      | 7            |            | 8          | 15       | 7             | 2       | 1      | 0             | 1      | 1  |
| 情報資産の分類および管理    | 4            | 6          |            | 14       | 3             | 5       | 4      | 1             | 4      | 0  |
| 人的セキュリティ        | 11           | 9          | 18         |          | 11            | 24      | 12     | 0             | 9      | 8  |
| 物理的および環境的セキュリティ | 2            | 0          | 0          | 4        |               | 3       | 3      | 0             | 1      | 0  |
| 通信および運用管理       | 1            | 0          | 2          | 7        | 2             |         | 18     | 2             | 3      | 0  |
| アクセス制御          | 2            | 1          | 1          | 4        | 2             | 9       |        | 1             | 0      | 1  |
| システム開発およびメンテナンス | 0            | 0          | 0          | 0        | 0             | 0       | 0      |               | 0      | 0  |
| 事業継続計画          | 4            | 0          | 5          | 9        | 0             | 9       | 4      | 2             |        | 8  |
| 準拠              | 11           | 3          | 1          | 7        | 2             | 0       | 0      | 1             | 8      |    |

#### (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位に選択した項目について確認する。一番多い選択は「情報セキュリティポリシー（157件）」であった。2番は「人的セキュリティ（102件）」、3番に「情報セキュリティ組織（42件）」である。前回調査では1番「情報セキュリティポリシー（199件）」、2番「人的セキュリティ（93件）」、3番「通信および運用管理（67件）」であり、上位2項目は同じであったが、第3番目が変更になった。

次に第2位の選択をみると、1番が「人的セキュリティ（100件）」、2番が「情報セキュリティ組織（72件）」、3番が「通信および運用管理（61件）」である。前回調査では、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）」であり順番に変更はなかった。「情報セキュリティポリシー」は前回、平成13年度調査同様6番目であり、第2位での選択は少ない。

参考までに13年度調査の第1位の中で多い選択は、1番「情報セキュリティポリシー（219件）」、2番「通信および運用管理（74件）」、3番「情報セキュリティ組織」である。第2位の選択をみると1番が「通信および運用管理（122件）」、2番「情報セキュリティ組織（99件）」、3番「人的セキュリティ（93件）」である。

前回、13年度調査との比較において、「人的セキュリティ」が重要度を増し、「通信および運用管理」が順位を下げていることがわかる。

#### (2) 第1位－第2位の組合せの選択傾向

これら第1位および第2位の組合せの選択の多いものを分析する。

第1位－第2位の選択で多かった組合せは次のものがある。今回調査で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53件を数え、これは今回の分析の回答件数514件中、10.3%を占める。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40件、全体の7.7%を占める。3番目は「人的セキュリティ」と「通信および運用管理」の24件で、これも全体の4.6%を占める。第1位と第2位は前回同様であったが、第3位は入れ替わっている。

前回調査で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」、第2位に「情報セキュリティ組織」を選択した組合せで75件を数え、これは前回の回答件数585件中、12.8%を占める。次は第1位に「情報セキュリティポリシー」、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」の組合せの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13年度調査と同様である。

13年度は、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」、第2位に「情報セキュリティ組織」を選択した組合せで70件を数え、回答件数604件中、11.6%を占める。次は第1位に「情報セキュリティポリシー」、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」の組合せの39件でこれも全体の6.5%を占める。

今回調査についてさらに分析すると、第4番目には再び情報セキュリティポリシーからの選択からで、「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」の組合せで21件、全体の4.1%、5番目は「人的セキュリティ」と「情報資産の分類および管理」と「通信および運用管理」と「アクセス制御」が同数で18件、3.5%となっている。

| 調査年度<br>順位 | 平成17年度                                             | 平成15年度                            | 平成13年度                            |
|------------|----------------------------------------------------|-----------------------------------|-----------------------------------|
| 第1位        | 情報セキュリティポリシー<br>&情報セキュリティ組織                        | 情報セキュリティポリシー<br>&情報セキュリティ組織       | 情報セキュリティポリシー<br>&情報セキュリティ組織       |
| 第2位        | 情報セキュリティポリシー<br>&人的セキュリティ                          | 情報セキュリティポリシー<br>&人的セキュリティ         | 情報セキュリティポリシー<br>&人的セキュリティ         |
| 第3位        | 人的セキュリティ&通信お<br>よび運用管理                             | 情報セキュリティポリシー<br>&情報資産の分類および<br>管理 | 情報セキュリティポリシー<br>&通信および運用管理        |
| 第4位        | 情報セキュリティポリシー<br>&情報資産の分類および<br>管理                  | 通信および運用管理 &<br>アクセス制御             | 通信および運用管理 &<br>アクセス制御             |
| 第5位        | 人的セキュリティ&情報資<br>産の分類および管理<br>通信および運用管理 &<br>アクセス制御 | 人的セキュリティ&通信お<br>よび運用管理            | 情報セキュリティポリシー<br>&情報資産の分類および<br>管理 |
| 第6位以下      | (略)                                                | (略)                               | (略)                               |

図3-9-1.セキュリティ要素 第1位&第2位の動向(上位5位までの推移)

## (2)「情報セキュリティポリシー」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、13年度同様となった。「情報セキュリティ組織」から「準拠」までの要素ごとに第2位に何を選擇したかをみると、「準拠」で第1位の選擇となっているが、その他は第2位として選擇されていない。これも前回同様である。「準拠」を第1位に選擇したグループが第2位に「情報セキュリティポリシー」を選擇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、それ以外の選擇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3-9-3. 第1位、第2位を選擇した要素の順番

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

表3-9-3からいえることは、前回同様第1位は「情報セキュリティポリシー」であるが、他の選擇を選んだグループからは必ずしも上位の支持を得られていないことがわかる。今回調査の上位3つの選擇として一番多いのは、前回、13年度調査と異なり「人的セキュリティ」であった。第1位選擇がなかった「システム開発およびメンテナンス」を除くすべてから上位3つまでの組合せに選擇されている。ちなみに前回、13年度調査では「通信および運用管理」が一番多かったが、今回は5つの要素で上位3つの選擇されている。

前回、13年度は第1位選擇に「通信および運用管理」が多かったため、経営的には情報セキュリティなどの要素を重要としながらも実務的にはウイルス対策などに迫られている様子が見えたと判断したが、今回も「人的セキュリティ」の次に1(位)の数が多いため、実務的には実情はあまり変化がないといえる。一方、「人的セキュリティ」は今回すべての選擇において上位3つまでに入ってきたが、13年度、前回と増加傾向であった。前は「情報資産の分類および管理」では1番多い選擇であり、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った。13年度から前回にかけては「人的セキュリティ」が3位までに選択される事業体が増えていた。

### (3) 選択の2つのグループ

前回、13年度同様に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」、「物理的および環境的セキュリティ」、のグループである。これらの2つのグループに変化はないといえる。

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」(53件)、「情報セキュリティポリシー&人的セキュリティ」(40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」(21件)、「人的セキュリティ&情報資産の分類および管理」(18件)、「情報セキュリティ組織&人的セキュリティ」(15件)、「情報資産の分類および管理&人的セキュリティ」(14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。

前回調査では「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&情報セキュリティポリシー」(13件)などであった。

13年度調査では「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」などがあつた。

このようにこれらの組合せは「人的セキュリティ」が存在感を増したが、全体的な枠組みは変わっていない。

もう一つのグループは、これも前回、13年度同様「通信および運用管理&アクセス制御」(18件)、「アクセス制御&通信および運用管理」(9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」がともに2番目であり、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。参考までに前回は「通信および運用管理&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位である。「通信および運用管理」「アクセス制御」の組合せが上位2つになるのは3回の調査とも同様である。

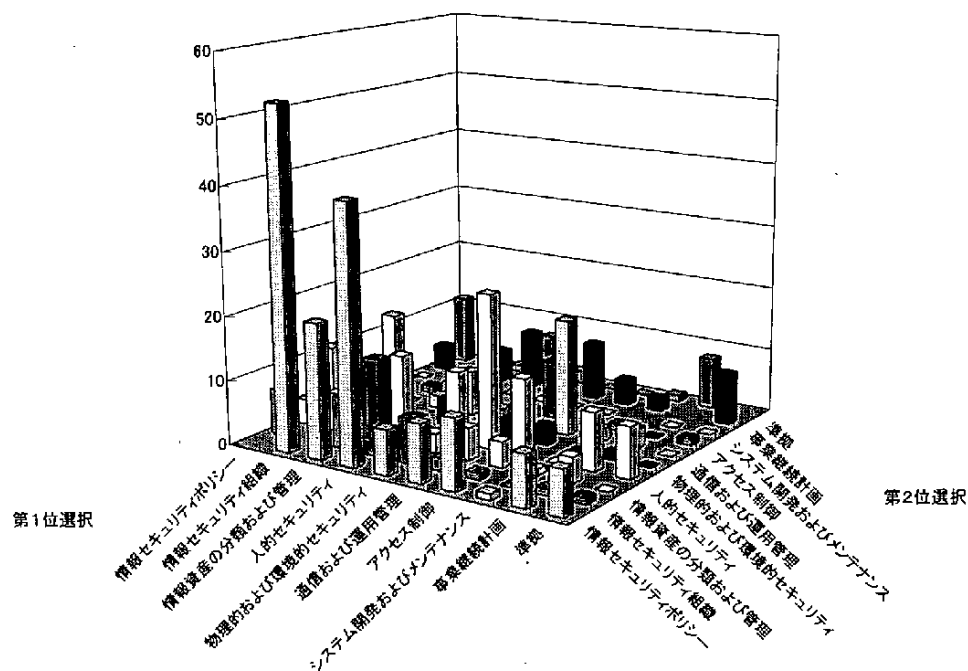


図3-9-2. 情報セキュリティ要素1位と2位の関係

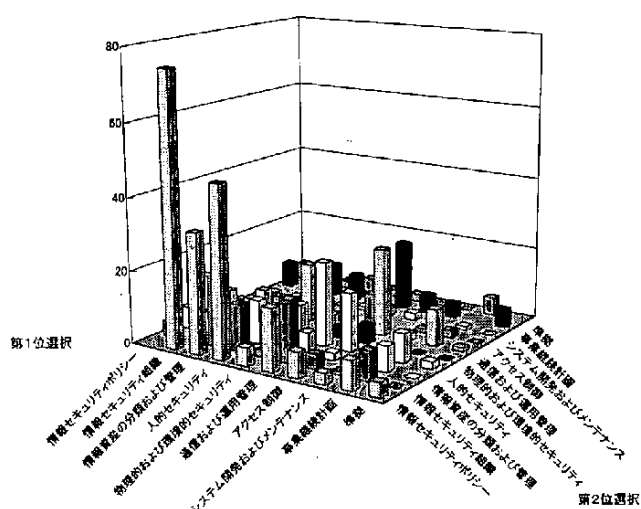


図3-9-3. 情報セキュリティ要素1位と2位の関係(平成15年度調査)

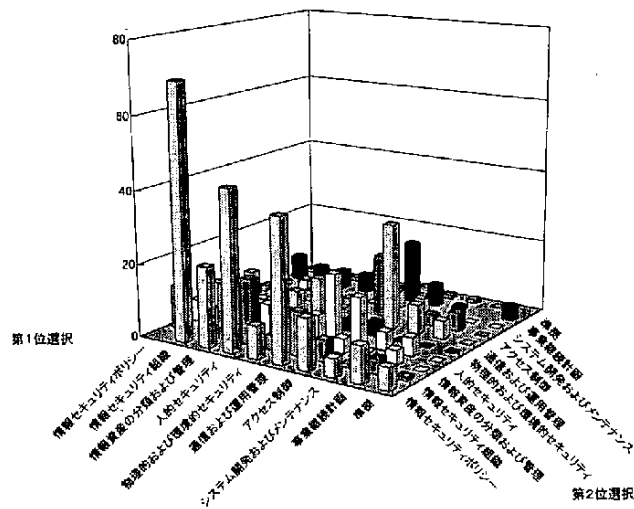


図3-9-4. 情報セキュリティ要素1位と2位の関係(平成13年度調査)

#### (4) その他の特徴

第2位の2番目に多い選択は前回、13年度と同様に「情報セキュリティ組織」であったが、今回調査でも選択の大半が「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「情報資産の分類および管理」である。今回1番目に多い選択となった「人的セキュリティ」は前回2番目に多い選択であった。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たことがここに来てより顕著になったといえる。「事業継続計画」と「準拠」がそれぞれ2位、3位にお互いを選択していることが特徴的である。

これらはリスク情報の開示や内部統制などの意識の高まりにつれ、コンプライアンスや監査などの必要性、あるいは取引先から事業継続計画を作成しているかについて問合せが増えてきていることにより、ステークホルダーである第三者の目を意識してきていることの表れともいえる。

#### (5) まとめ

概論として、前回調査と13年度とではほとんど同じで大きな違いがなかったのに対し、今回は大きな枠組みに変化はないものの、「人的セキュリティ」が重視されはじめたことが顕著になったといえる。一方、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は、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は前回、13年度同様であるといえる。

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53件でトップであり、この傾向は変わっていない。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り、これも前回、13年度と同様である。

このような中で「人的セキュリティ」は経営的要素を重視するグループからも実務を重視するグループからもともに重要視され、今回の調査では1位の支持がゼロであった「システム開発およびメンテナンス」を除くすべての8要素で上位3番目までに選択されている。

この傾向はすでに前回調査で表れており、前回は経営的な視点を重視すること、および「通信および運用管理」など実務を重視するところの双方ともが「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指摘していたが、個人情報保護法などの施行に伴い、実際の個人情報の取扱いや情報漏えい防止対策の実施についての取組みを企業などが行うことにより、情報セキュリティには、究極は従業員の教育などの「人的セキュリティ」が総合的にみて一番重要である、との認識が増大したといえる。

### 3.10 Q24 のクロス集計

Q24.「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。

クロス対象項目

Q8-3.情報システムに係わるリスク分析を実施していますか。

①Q24 からみたQ8-3

| Q24. 事業継続性計画 \ Q8-3. リスク分析 | 回答<br>件数 | 1. 策定／実<br>施している |      | 2. 策定／実<br>施を予定<br>している |      | 3. 策定／実<br>施の予定<br>はない |      | 無回答 |      |
|----------------------------|----------|------------------|------|-------------------------|------|------------------------|------|-----|------|
|                            |          |                  |      |                         |      |                        |      |     |      |
| 1. 作成している                  | 85       | 75               | 88.2 | 8                       | 9.4  | 2                      | 2.4  | 0   | 0.0  |
| 2. 作成中である                  | 24       | 11               | 45.8 | 11                      | 45.8 | 2                      | 8.3  | 0   | 0.0  |
| 3. 作成を含め検討中である             | 127      | 33               | 26.0 | 81                      | 63.8 | 11                     | 8.7  | 2   | 1.6  |
| 4. 作成していない                 | 252      | 40               | 15.9 | 99                      | 39.3 | 112                    | 44.4 | 1   | 0.4  |
| 5. 必要ない                    | 9        | 2                | 22.2 | 2                       | 22.2 | 5                      | 55.6 | 0   | 0.0  |
| 無回答                        | 17       | 4                | 23.5 | 6                       | 35.3 | 4                      | 23.5 | 3   | 17.6 |
| 計                          | 514      | 165              | 32.1 | 207                     | 40.3 | 136                    | 26.5 | 6   | 1.2  |

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88.2%（✓H15:90.3%、2.1ポイント減）であり、ほぼ前回調査と同様であるが、リスク分析を「実施していない」割合は2.4%（✓H15:8.1%、5.7ポイント減）と大きく下がった。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」割合が45.8%（✓H15:55.0%、9.2ポイント減）、また「作成を含め検討中」の事業体は26.0%（✓H15:31.7%、5.78ポイント減）と、リスク分析を実施する割合が作成しているところと比較して大きく下がっている。ただし「作成していない」事業体でも15.9%（✓H15:17.9%、2.0ポイント減）がリスク分析を「実施」している。なお、母数が少ないのであくまでも参考としてあげるが、「必要ない」と回答した事業体でも22.2%がリスク分析を「実施」している。

今回の特徴は「リスク分析」を「策定／実施の予定はない」（26.5%）が前回の54.2%から大幅に減少（27.7ポイント減）していることである。内訳では「作成している」、「作成中である」、「作成を含め検討中である」がそれぞれ2.4%、8.3%、8.7%と一桁台であるのに対し、「作成していない」、「必要ない」、「無回答」が44.4%、55.6%、23.5%であり、作成したり検討しているところではリスク分析は実施されているか予定されていることがわかる。

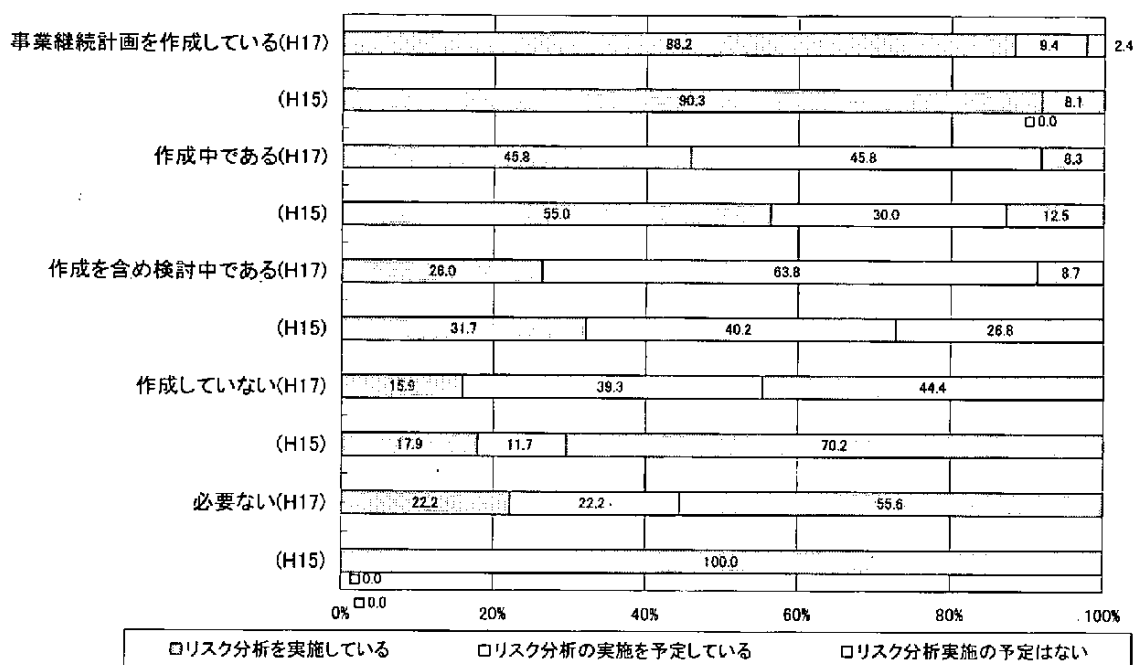


図3-10-1. 事業継続性計画の作成状況とリスク分析の実施状況の関係

②Q8-3からみたQ24

| Q24. 事業継続性計画   | Q8-3. リスク分析 |     | 1. 策定／実施している |     | 2. 策定／実施を予定している |     | 3. 策定／実施の予定はない |   | 無回答   |  |
|----------------|-------------|-----|--------------|-----|-----------------|-----|----------------|---|-------|--|
|                | 回答件数        |     |              |     |                 |     |                |   |       |  |
| 1. 作成している      | 85          | 75  | 45.5         | 8   | 3.9             | 2   | 1.5            | 0 | 0.0   |  |
| 2. 作成中である      | 24          | 11  | 6.7          | 11  | 5.3             | 2   | 1.5            | 0 | 0.0   |  |
| 3. 作成を含め検討中である | 127         | 33  | 20.0         | 81  | 39.1            | 11  | 8.1            | 2 | 33.3  |  |
| 4. 作成していない     | 252         | 40  | 24.2         | 99  | 47.8            | 112 | 82.4           | 1 | 16.7  |  |
| 5. 必要ない        | 9           | 2   | 1.2          | 2   | 1.0             | 5   | 3.7            | 0 | 0.0   |  |
| 無回答            | 17          | 4   | 2.4          | 6   | 2.9             | 4   | 2.9            | 3 | 50.0  |  |
| 計              | 514         | 165 | 100.0        | 207 | 100.0           | 136 | 100.0          | 6 | 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」事業体でも事業継続性計画を「作成している」のは165件中75件(45.5% ⇨ H15 : 30.9%、14.6 ポイント増)であり、割合は増加しているが、まだ過半数以下に過ぎず、「作成中」の11件を含めても52.1% (⇨ H15 : 43.1%、9.0 ポイント増)とようやく過半数に達した程度である。リスク分析を「実施している」事業体でも業務継続計画や事業継続性計画が「必要ない」との回答が2件あった。前回調査同様、事業継続性計画を作成するのは実際上困難であることがわかる。

リスク分析を「実施していない」場合で事業継続性計画を「作成している」との回答は136件中2件と、前回同様1.5%と少なく「作成していない」が112件82.4% (⇨ H15 : 83.8%、1.4 ポイント減)で、ここではあまり変化はなかった。

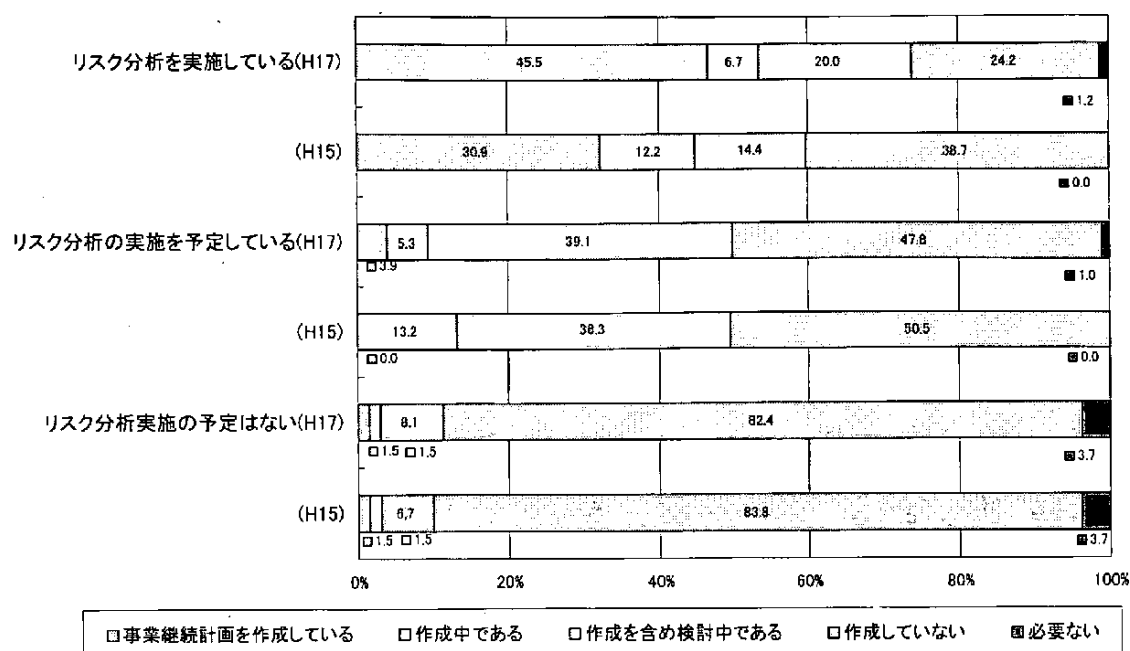


図3-10-2. リスク分析の実施状況と事業継続性計画の作成状況との関係

総括すると、前回調査と比較し、少しは事業継続性計画の作成が進んできており、事業継続性計画の策定にあたりリスク分析を実施する割合が増えている。

平成17年3月に経済産業省から、また8月に内閣府からそれぞれ事業継続計画（BCP）作成のためのガイドラインが発表されており、今後事業継続性計画を作成するところが増加することも期待される。またこれらガイドラインでは従来は明確に求められていなかったビジネスインパクトアナリシス（BIA）の実施や、リスク分析・被害想定を行わなければ本当の事業継続ではない、という欧米流の思想が明確にされた。このため、今後事業継続性計画を作成した場合はリスク分析が当然実施されるようになる、と考えられる。一方、リスク分析を実施してもそれだけでは事業継続性計画を作成することにはならないので、リスク分析から事業継続性計画の策定に至るようにより事業体や組織を動かしていくためには、何らかの推進力が必要である。

### 3.11 Q25 のクロス集計

Q25. 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。

クロス対象項目

Q9. 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)

| Q25. 策定項目 \ Q9. 対象リスク | 回答<br>件数 | 1. 自然災害 |       | 2. 地震 |       | 3. 人的災害 |       | 4. コンピュータ<br>犯罪のリスク |       |
|-----------------------|----------|---------|-------|-------|-------|---------|-------|---------------------|-------|
| 1. 外部からの悪意による緊急事態     | 49       | 43      | 87.8  | 44    | 89.8  | 38      | 77.6  | 45                  | 91.8  |
| 2. ネットワークセキュリティ上の緊急事態 | 37       | 32      | 86.5  | 33    | 89.2  | 31      | 83.8  | 33                  | 89.2  |
| 3. 事故・災害              | 83       | 72      | 86.7  | 75    | 90.4  | 63      | 75.9  | 73                  | 88.0  |
| 4. 障害                 | 78       | 66      | 84.6  | 69    | 88.5  | 57      | 73.1  | 67                  | 85.9  |
| 5. 人的なミスに起因する障害・誤処理   | 48       | 42      | 87.5  | 41    | 85.4  | 38      | 79.2  | 43                  | 89.6  |
| 6. 内部犯罪による緊急事態        | 28       | 25      | 89.3  | 25    | 89.3  | 23      | 82.1  | 25                  | 89.3  |
| 7. 伝染病                | 7        | 7       | 100.0 | 7     | 100.0 | 7       | 100.0 | 6                   | 85.7  |
| 8. その他                | 1        | 1       | 100.0 | 1     | 100.0 | 1       | 100.0 | 1                   | 100.0 |
| 計                     | 86       | 74      | 86.0  | 77    | 89.5  | 65      | 75.6  | 75                  | 87.2  |

| Q25. 策定項目 \ Q9. 対象リスク | 5. 運用障害 |       | 6. 事故 |       | 7. 不正侵入<br>で起きるサー<br>バの乗っ取り |       | 8. 自社従業員<br>などによる<br>故意による情<br>報漏えい |       |
|-----------------------|---------|-------|-------|-------|-----------------------------|-------|-------------------------------------|-------|
| 1. 外部からの悪意による緊急事態     | 46      | 93.9  | 45    | 91.8  | 43                          | 87.8  | 43                                  | 87.8  |
| 2. ネットワークセキュリティ上の緊急事態 | 36      | 97.3  | 35    | 94.6  | 33                          | 89.2  | 35                                  | 94.6  |
| 3. 事故・災害              | 75      | 90.4  | 76    | 91.6  | 65                          | 78.3  | 75                                  | 90.4  |
| 4. 障害                 | 70      | 89.7  | 71    | 91.0  | 60                          | 76.9  | 69                                  | 88.5  |
| 5. 人的なミスに起因する障害・誤処理   | 46      | 95.8  | 45    | 93.8  | 42                          | 87.5  | 44                                  | 91.7  |
| 6. 内部犯罪による緊急事態        | 25      | 89.3  | 25    | 89.3  | 24                          | 85.7  | 26                                  | 92.9  |
| 7. 伝染病                | 7       | 100.0 | 7     | 100.0 | 7                           | 100.0 | 7                                   | 100.0 |
| 8. その他                | 1       | 100.0 | 1     | 100.0 | 1                           | 100.0 | 1                                   | 100.0 |
| 計                     | 78      | 90.7  | 79    | 91.9  | 68                          | 79.1  | 77                                  | 89.5  |

| Q25. 策定項目 \ Q9. 対象リスク | 9. 不注意・過<br>失による情報<br>漏えい |       | 10. 盗難・車<br>上荒らしなど<br>による情報漏<br>えい |       | 11. システム<br>の統合リスク |       | 12. システム<br>の改良・容量<br>増に伴うトラ<br>ブル |       |
|-----------------------|---------------------------|-------|------------------------------------|-------|--------------------|-------|------------------------------------|-------|
| 1. 外部からの悪意による緊急事態     | 44                        | 89.8  | 39                                 | 79.6  | 32                 | 65.3  | 41                                 | 83.7  |
| 2. ネットワークセキュリティ上の緊急事態 | 35                        | 94.6  | 33                                 | 89.2  | 29                 | 78.4  | 31                                 | 83.8  |
| 3. 事故・災害              | 76                        | 91.6  | 67                                 | 80.7  | 51                 | 61.4  | 66                                 | 79.5  |
| 4. 障害                 | 70                        | 89.7  | 61                                 | 78.2  | 46                 | 59.0  | 60                                 | 76.9  |
| 5. 人的なミスに起因する障害・誤処理   | 44                        | 91.7  | 40                                 | 83.3  | 34                 | 70.8  | 40                                 | 83.3  |
| 6. 内部犯罪による緊急事態        | 25                        | 89.3  | 23                                 | 82.1  | 22                 | 78.6  | 23                                 | 82.1  |
| 7. 伝染病                | 7                         | 100.0 | 7                                  | 100.0 | 4                  | 57.1  | 6                                  | 85.7  |
| 8. その他                | 1                         | 100.0 | 1                                  | 100.0 | 1                  | 100.0 | 1                                  | 100.0 |
| 計                     | 78                        | 90.7  | 69                                 | 80.2  | 52                 | 60.5  | 68                                 | 79.1  |

| Q9. 対象リスク<br>Q25. 策定項目 | 13. 過負荷によるシステムダウン |       | 14. ハードウェア障害 |       | 15. ソフトウェア障害 |       | 16. ネットワーク障害 |       |
|------------------------|-------------------|-------|--------------|-------|--------------|-------|--------------|-------|
| 1. 外部からの悪意による緊急事態      | 38                | 77.6  | 46           | 93.9  | 46           | 93.9  | 46           | 93.9  |
| 2. ネットワークセキュリティ上の緊急事態  | 29                | 78.4  | 33           | 89.2  | 33           | 89.2  | 33           | 89.2  |
| 3. 事故・災害               | 65                | 78.3  | 77           | 92.8  | 75           | 90.4  | 76           | 91.6  |
| 4. 障害                  | 58                | 74.4  | 72           | 92.3  | 70           | 89.7  | 71           | 91.0  |
| 5. 人的なミスに起因する障害・誤処理    | 38                | 79.2  | 43           | 89.6  | 43           | 89.6  | 43           | 89.6  |
| 6. 内部犯罪による緊急事態         | 23                | 82.1  | 25           | 89.3  | 24           | 85.7  | 24           | 85.7  |
| 7. 伝染病                 | 7                 | 100.0 | 7            | 100.0 | 7            | 100.0 | 7            | 100.0 |
| 8. その他                 | 1                 | 100.0 | 1            | 100.0 | 1            | 100.0 | 1            | 100.0 |
| 計                      | 66                | 76.7  | 80           | 93.0  | 78           | 90.7  | 79           | 91.9  |

| Q9. 対象リスク<br>Q25. 策定項目 | 17. コンピュータウイルス、スパイウェアによるシステムの停止 |       | 18. 信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止 |       | 19. フィッシングなどで自社サイトが模倣され、自社ユーザに被害がでる |       | 20. ボットなどを利用したDOSやDDos攻撃 |       |
|------------------------|---------------------------------|-------|-----------------------------------------------|-------|-------------------------------------|-------|--------------------------|-------|
| 1. 外部からの悪意による緊急事態      | 47                              | 95.9  | 39                                            | 79.6  | 34                                  | 69.4  | 37                       | 75.5  |
| 2. ネットワークセキュリティ上の緊急事態  | 36                              | 97.3  | 31                                            | 83.8  | 28                                  | 75.7  | 31                       | 83.8  |
| 3. 事故・災害               | 76                              | 91.6  | 63                                            | 75.9  | 53                                  | 63.9  | 57                       | 68.7  |
| 4. 障害                  | 72                              | 92.3  | 57                                            | 73.1  | 47                                  | 60.3  | 52                       | 66.7  |
| 5. 人的なミスに起因する障害・誤処理    | 47                              | 97.9  | 40                                            | 83.3  | 35                                  | 72.9  | 38                       | 79.2  |
| 6. 内部犯罪による緊急事態         | 27                              | 96.4  | 24                                            | 85.7  | 23                                  | 82.1  | 23                       | 82.1  |
| 7. 伝染病                 | 7                               | 100.0 | 7                                             | 100.0 | 5                                   | 71.4  | 6                        | 85.7  |
| 8. その他                 | 1                               | 100.0 | 1                                             | 100.0 | 1                                   | 100.0 | 1                        | 100.0 |
| 計                      | 79                              | 91.9  | 65                                            | 75.6  | 54                                  | 62.8  | 59                       | 68.6  |

| Q9. 対象リスク<br>Q25. 策定項目 | 21. その他 |       | 無回答 |     |
|------------------------|---------|-------|-----|-----|
| 1. 外部からの悪意による緊急事態      | 7       | 14.3  | 0   | 0.0 |
| 2. ネットワークセキュリティ上の緊急事態  | 7       | 18.9  | 0   | 0.0 |
| 3. 事故・災害               | 9       | 10.8  | 1   | 1.2 |
| 4. 障害                  | 9       | 11.5  | 1   | 1.3 |
| 5. 人的なミスに起因する障害・誤処理    | 7       | 14.6  | 1   | 2.1 |
| 6. 内部犯罪による緊急事態         | 5       | 17.9  | 0   | 0.0 |
| 7. 伝染病                 | 1       | 14.3  | 0   | 0.0 |
| 8. その他                 | 1       | 100.0 | 0   | 0.0 |
| 計                      | 10      | 11.6  | 1   | 1.2 |

事業継続性計画を作成する場合、対象とするリスクを定めた後に計画を作成することが一般的であり、そのためにリスク分析を実施していると想定される。ここでは事業継続性計画の対象としているリスクと、リスク分析を実施する場合に想定するリスクの間の相関関係の有無について調査した。

# ①Q9からみたQ25

Q9でリスク分析を実施している場合に想定されたリスクごとに、それが事業継続性計画の対象リスクとして採用された割合が高いか否かを分析した。

Q9のリスク分析対象項目「自然災害」は合計で86.0%が事業継続性計画の対象とするリスクに選択されているが、その中で事業継続性計画策定項目のうち、「内部犯罪による緊急事態」が89.3%と高いが、概観すると大きな違いはない。

「地震」は合計で89.5%が選択されているが、「事故・災害」が90.4%と高い。母数が25件と統計的分析に意味がある30件に届かないケースを含めると、「人的なミスに起因する障害・誤処理」が85.4%と少ない。

「人的災害」については全体で75.6%が選択されているが、ここでは「ネットワークセキュリティ上の緊急事態」が83.8%と高い。一方で「障害」は73.1%と低い。多少ではあるがリスク分析の対象と事業継続性の対象とに関係がある場合があるといえる。

「コンピュータ犯罪のリスク」は合計87.2%が選択されているが、「外部からの悪意による緊急事態」が91.8%と高く、「障害」は85.9%とやや低い。

「運用障害」では全体で90.7%が採用されているが、「ネットワークセキュリティ上の緊急事態」が97.3%、「人的なミスに起因する障害・誤処理」が95.8%と高い値を示している。

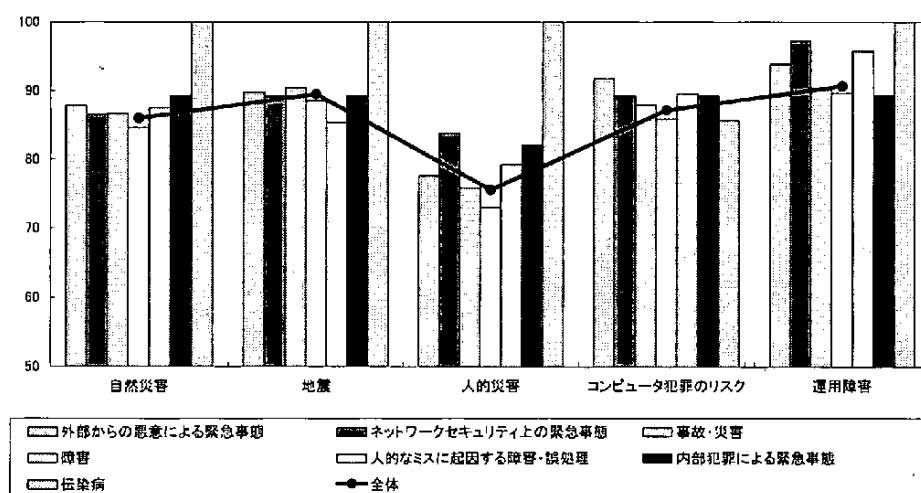


図3-11-1. リスク分析対象リスクと事業継続性計画策定項目との関係(その1)

「事故」は全体が91.9%となっているが、「ネットワークセキュリティ上の緊急事態」が94.6%と高く、「内部犯罪による緊急事態」は89.3%と低い。

「不正侵入で起きるサーバの乗っ取り」は全体では79.1%であるが、「ネットワークセキュリティ上の緊急事態」が89.2%、「外部からの悪意による緊急事態」が87.8%、「人的なミスに起因する障害・誤処理」が87.5%と高くなっている。逆に「障害」は76.9%と低い。

「自社従業員などによる故意による情報漏えい」では全体が89.5%であるが、「ネットワークセキュリティ上の緊急事態」が94.6%、「内部犯罪による緊急事態」が92.9%と高い。一方「外部からの悪意による緊急事態」は87.8%と低い。

「不注意・過失による情報漏えい」は全体では90.7%であるが、「ネットワークセキュリティ

上の緊急事態」が94.6%と高い。

「盗難・車上荒らしなどの情報漏えい」は合計で80.2%であるが、「ネットワークセキュリティ上の緊急事態」が89.2%と高く、「障害」は78.2%と低い。

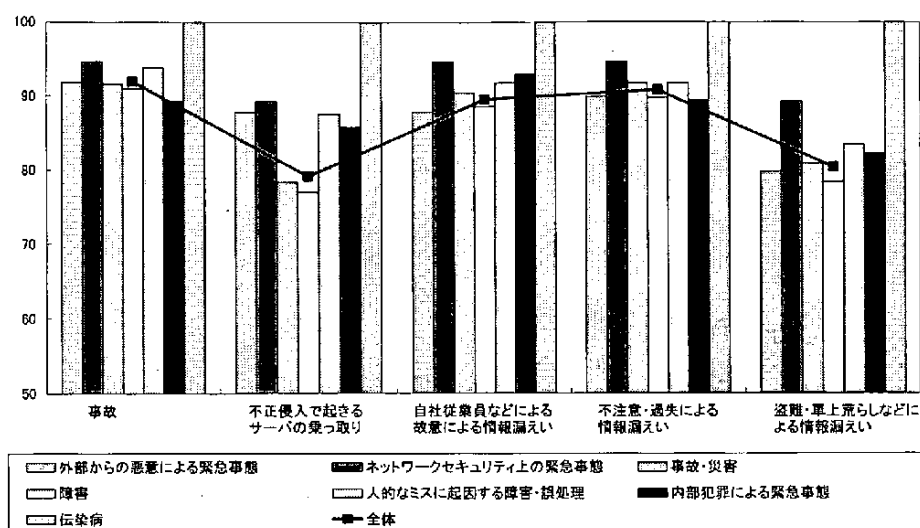


図3-11-2. リスク分析対象リスクと事業継続性計画策定項目との関係(その2)

「システムの統合リスク」は合計が60.5%であるが、「ネットワークセキュリティ上の緊急事態」が78.4%、「内部犯罪による緊急事態」が78.6%と高い。

「システム改良・容量増に伴うトラブル」は合計79.1%であるが、「ネットワークセキュリティ上の緊急事態」が83.8%、「外部からの悪意による緊急事態」が83.7%と高い。

「過負荷によるシステムダウン」は全体が76.7%であるが、「内部犯罪による緊急事態」が82.1%と高い。

「ハードウェア障害」は全体では93.0%であるが、ここでは「ネットワークセキュリティ上の緊急事態」が89.2%、「内部犯罪による緊急事態」が89.3%と低い。

「ソフトウェア障害」は全体では90.7%であるが、「外部からの悪意による緊急事態」93.9%と高く、「内部犯罪による緊急事態」は85.7%と低い。

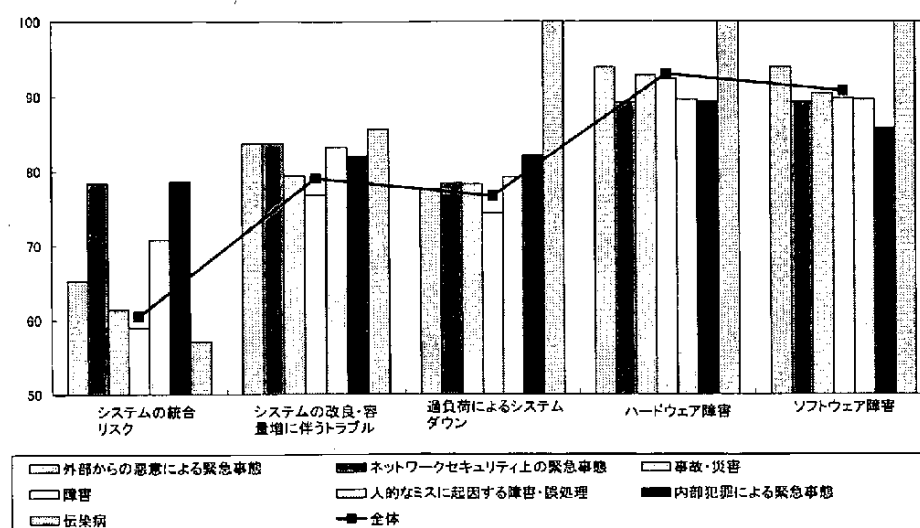


図3-11-3. リスク分析対象リスクと事業継続性計画策定項目との関係(その3)

「ネットワーク障害」は全体では91.9%であるが、「外部からの悪意による緊急事態」が93.9%と高く、「内部犯罪による緊急事態」は85.7%と低い。

「コンピュータウイルス、スパイウェアによるシステムの停止」は全体で91.9%であるが、「人的なミスに起因する障害・誤処理」が97.9%、「ネットワークセキュリティ上の緊急事態」が97.3%と高い。一方、「事故・災害」は91.6%と低い。

「信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止」は合計では75.6%が採用されているが、「内部犯罪による緊急事態」が85.7%、「ネットワークセキュリティ上の緊急事態」が83.8%と高く、「障害」は73.1%と低い。

「フィッシングなどで自社サイトが模倣され、自社ユーザに被害が出る」は全体では62.8%が採用されているが、「内部犯罪による緊急事態」が82.1%ときわめて高く、また「ネットワークセキュリティ上の緊急事態」も75.7%ときわめて高い。一方、「障害」は60.3%と低い。

「ボットなどを利用したDOSやDDos攻撃」は合計で68.6%であるが、「ネットワークセキュリティ上の緊急事態」が83.8%、「内部犯罪による緊急事態」が82.1%と高い。一方「障害」は66.7%と低い。

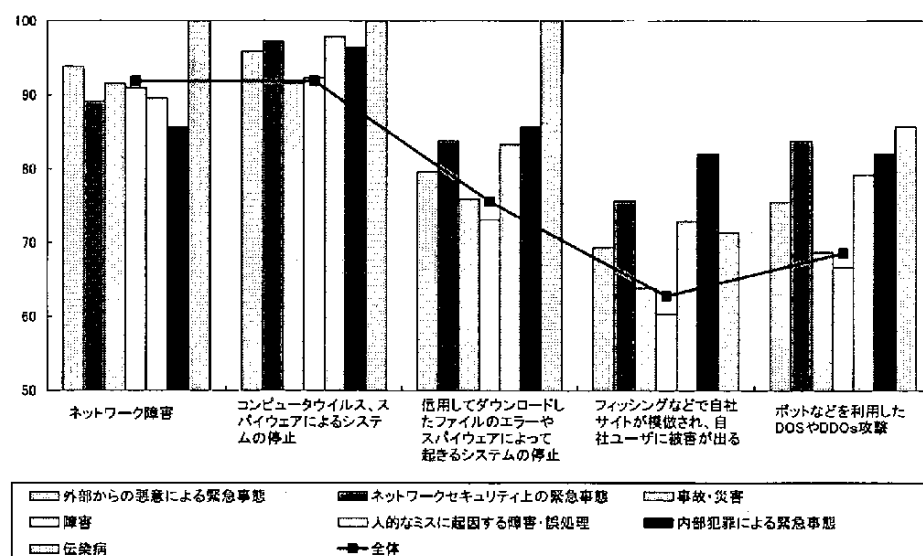


図3-11-4. リスク分析対象リスクと事業継続性計画策定項目との関係(その4)

このように全体をみると、「ネットワークセキュリティ上の緊急事態」、「内部犯罪による緊急事態」が比較的高かったり、低かったりという特徴的な選択となっている。

## ②Q25 からみたQ9

次にこれらの結果でQ25の各選択肢の特徴をみる。

ここでは、事業継続性計画での策定項目別に、対象リスクの割合に順位をつけ、それぞれの高順位（第1位および第2位）および低順位（第6位）にどの対象リスクが位置づけられるかを分析した。

なお、対象リスクのうち、「伝染病」および「その他」は回答件数が少ないため、今回の分析対象から外している。

(位)

| Q9. 対象<br>リスク<br>Q25. 策定項目 | 1. 自然<br>災害 | 2. 地震 | 3. 人的<br>災害 | 4. コン<br>ピュー<br>タ 犯 罪<br>のリスク | 5. 運用<br>障害 | 6. 事故 | 7. 不正<br>侵入で<br>起きる<br>サーバ<br>の乗っ<br>取り | 8. 自社<br>従業員<br>などによる故意による情報漏えい | 9. 不注意・過失による情報漏えい | 10. 盗<br>難・車<br>上 荒<br>らしなどによる情報漏えい |
|----------------------------|-------------|-------|-------------|-------------------------------|-------------|-------|-----------------------------------------|---------------------------------|-------------------|-------------------------------------|
| 1. 外部からの悪意による緊急事態          | 2           | 2     | 4           | 1                             | 3           | 3     | 2                                       | 6                               | 4                 | 5                                   |
| 2. ネットワークセキュリティ上の緊急事態      | 5           | 4     | 1           | 4                             | 1           | 1     | 1                                       | 1                               | 1                 | 1                                   |
| 3. 事故・災害                   | 4           | 1     | 5           | 5                             | 4           | 4     | 5                                       | 4                               | 3                 | 4                                   |
| 4. 障害                      | 6           | 5     | 6           | 6                             | 5           | 5     | 6                                       | 5                               | 5                 | 6                                   |
| 5. 人的なミスに起因する障害・誤処理        | 3           | 6     | 3           | 2                             | 2           | 2     | 3                                       | 3                               | 2                 | 2                                   |
| 6. 内部犯罪による緊急事態             | 1           | 3     | 2           | 3                             | 6           | 6     | 4                                       | 2                               | 6                 | 3                                   |

| Q9. 対象<br>リスク<br>Q25. 策定項目 | 11. シ<br>ステム<br>統 合<br>リスク | 12. シ<br>ステム<br>改 良・<br>容 量 増<br>に伴う<br>トラブル | 13. 過<br>負 荷 による<br>システム<br>ダウン | 14. ハ<br>ー ド<br>ウ ェ ア<br>障害 | 15. ソ<br>フ ト<br>ウ ェ ア<br>障害 | 16. ネ<br>ッ ト<br>ワ ー ク<br>障害 | 17. ウ<br>ィ ル<br>ス、ス<br>パ イ<br>ウ ェ ア<br>による<br>システム<br>停止 | 18. フ<br>ァ イ<br>ル エ<br>ラ ー や<br>ス パ<br>イ ウ<br>ェ ア<br>による<br>システム<br>停止 | 19. 自<br>社 サイト<br>が 模 倣<br>され、自<br>社 ユーザ<br>に被害が<br>でる | 20. ボ<br>ッ ト などを<br>利用した<br>DOS や<br>DDos 攻撃 |
|----------------------------|----------------------------|----------------------------------------------|---------------------------------|-----------------------------|-----------------------------|-----------------------------|----------------------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------|
| 1. 外部からの悪意による緊急事態          | 4                          | 2                                            | 5                               | 1                           | 1                           | 1                           | 4                                                        | 4                                                                      | 4                                                      | 4                                            |
| 2. ネットワークセキュリティ上の緊急事態      | 2                          | 1                                            | 3                               | 6                           | 5                           | 5                           | 2                                                        | 2                                                                      | 2                                                      | 1                                            |
| 3. 事故・災害                   | 5                          | 5                                            | 4                               | 2                           | 2                           | 2                           | 6                                                        | 5                                                                      | 5                                                      | 5                                            |
| 4. 障害                      | 6                          | 6                                            | 6                               | 3                           | 3                           | 3                           | 5                                                        | 6                                                                      | 6                                                      | 6                                            |
| 5. 人的なミスに起因する障害・誤処理        | 3                          | 3                                            | 2                               | 4                           | 4                           | 4                           | 1                                                        | 3                                                                      | 3                                                      | 3                                            |
| 6. 内部犯罪による緊急事態             | 1                          | 4                                            | 1                               | 5                           | 6                           | 6                           | 3                                                        | 1                                                                      | 1                                                      | 2                                            |

事業継続性計画で対象とするリスクで「外部からの悪意による緊急事態」を選んだ場合は「コンピュータ犯罪のリスク」、「ハードウェア障害」、「ソフトウェア障害」、「ネットワーク障害」（以上、第1位）、「自然災害」、「地震」、「不正侵入で起きるサーバの乗っ取り」、「システムの改良・容量増に伴うトラブル」（第2位）を選ぶ割合が高く、「自社従業員などによる故意による情報漏えい」が低い。

事業継続性計画で対象とするリスクで「ネットワークセキュリティ上の緊急事態」を選択した場合は、「人的災害」、「運用障害」、「事故」、「不正侵入で起きるサーバの乗っ取り」、「自社従業員な

どによる故意による情報漏えい」、「不注意・過失による情報漏えい」、「自社従業員などによる故意による情報漏えい」、「不注意・過失による情報漏えい」、「盗難・車上荒らしなどのによる情報漏えい」、「システムの改良・容量増に伴うトラブル」、「ボットなどを利用した DOS や DDos 攻撃」が第1位、「システムの統合リスク」、「コンピュータウイルス、スパイウェアによるシステム停止」、「信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止」、「フィッシングなどで自社サイトが模倣され、自社ユーザに被害が出る」（第2位）などが高い。また低いのは「ハードウェア障害」である。

「事故・災害」は特に特徴はないが、「地震」（第1位）は高い値を示した。一方「コンピュータウイルス、スパイウェアによるシステムの停止」は低い。

「障害」は全体的に低く、「自然災害」、「人的災害」、「コンピュータ犯罪のリスク」、「不正侵入で起きるサーバの乗っ取り」、「盗難・車上荒らしなどによる情報漏えい」、「システムの統合リスク」、「システムの改良・容量増に伴うトラブル」、「過負荷によるシステムダウン」、「信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止」、「フィッシングなどで自社サイトが模倣され、自社ユーザに被害が出る」、「ボットなどを利用した DOS や DDos 攻撃」は特に低い値を示している。

「人的なミスに起因する障害・誤処理」は「コンピュータウイルス、スパイウェアによるシステムの停止」（第1位）、「コンピュータ犯罪のリスク」、「運用障害」、「事故」、「不注意・過失による情報漏えい」、「盗難・車上荒らしなどによる情報漏えい」、「過負荷によるシステムダウン」（以上、第2位）が高く、一方「地震」が低い。

「内部犯罪による緊急事態」では「自然災害」、「システムの統合リスク」、「過負荷によるシステムダウン」、「信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止」、「フィッシングなどで自社サイトが模倣され、自社ユーザに被害が出る」が第1位、「人的災害」、「自社従業員などによる故意の情報漏えい」、「ボットなどを利用した DOS や DDos 攻撃」が第2位と高い。一方、「運用障害」、「事故」、「不注意・過失による情報漏えい」、「ソフトウェア障害」、「ネットワーク障害」が低い。

このように分析すると、多少の差異ではあるが、それぞれ事業継続性計画の対象としたリスクと情報関連のリスクの選択には関連性があるように見える。一般事業継続性計画の対象としたリスクと同じまたは類似のリスクはリスク分析の対象としている。一方、あまり関連性のないリスクは比較的对象としていない。事業継続性計画ではリスク分析によってその事業体の優先順位の高いリスクについて計画作成の対象としていると考えられる。

### 3.12 Q41 のクロス集計

Q41. 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。

クロス対象

Q15. 基幹システムにおけるMTBF(平均故障間隔)は何時間ですか。

| Q41. システム監査の効果                  | Q15.MTBF 平均時間 |
|---------------------------------|---------------|
| 平均                              | 4,273.4       |
| 1. システムに起因する事故・障害が未然に防止できた      | 3,674.3       |
| 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   | 4,750.0       |
| 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  | 5,979.9       |
| 4. システムの信頼性向上対策のレベルが明らかになった     | 4,538.4       |
| 5. システムの有効利用が促進された              | 4,362.3       |
| 6. システムの効率性が確保できた               | 4,271.5       |
| 7. 業務の継続性の確保が図られた               | 6,988.2       |
| 8. 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 | 5,968.2       |
| 9. その他                          | 665.0         |
| 10. 効果は得られなかった                  | 12,446.7      |
| 11. 無回答                         | 3,643.4       |

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。前回調査では、システム監査項目のうち MTBF を伸ばす要因は「システムの信頼性向上対策のレベルが明らかになった」、「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」と「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」の3点であった。今回調査では、「業務の継続性の確保が図られた」が6,988.2時間、「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」が5,979.9時間、「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5,968.2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」が4,750.0時間で、平均の4,273.4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。

前回、今回の2度の調査を通じて、「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」と「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」、「システムの信頼性向上対策のレベルが明らかになった」も平均よりは若干よいことがわかった。すなわち、これらの項目がシステム監査の効用として信頼性向上＝MTBFの数値を向上することにつながっていることがわかる。ただし、今回調査ではこれらに加えて「業務の継続性の確保が図られた」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」が新たに加わったと考えるべきであろう。

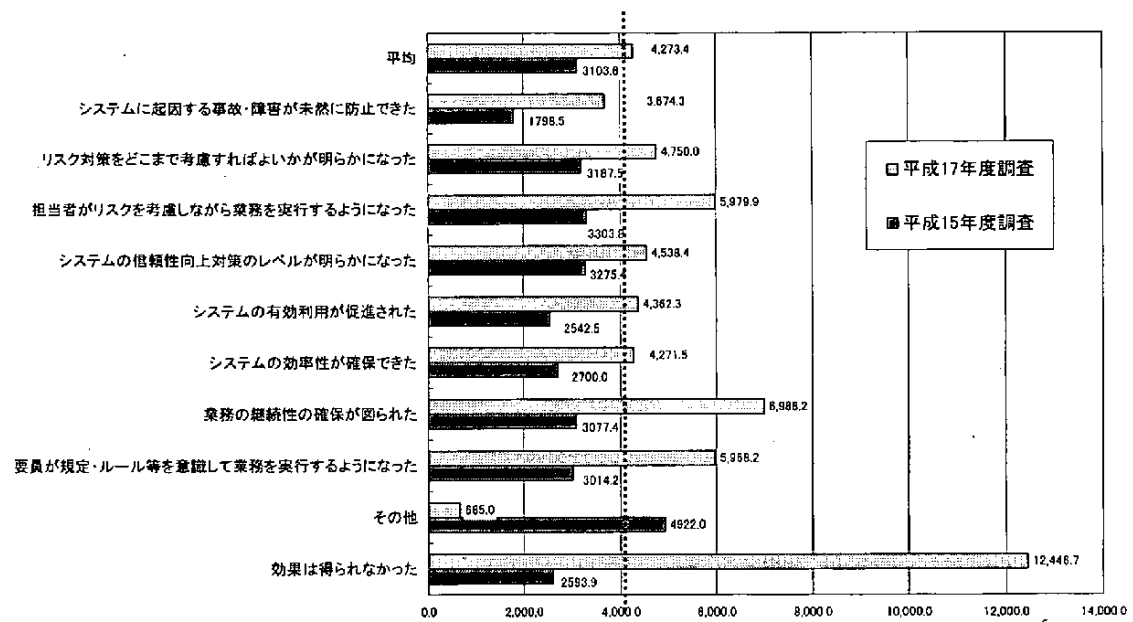


図3-12-1. システム監査の効果とMTBFの関係

### 3.13 Q46 のクロス集計

Q46. 貴事業体は個人情報取扱事業者(過去半年に 5,000 件以上の個人情報を取扱ったことがある)に該当しますか。

クロス対象

Q47. 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。

Q48. 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。

Q49. Q48 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についてどう考えますか。

Q51. 個人情報の漏洩により深刻な被害を及ぼす事項をどのように認識していますか。

Q53. 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。

Q54. 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。

#### 3.13.1 Q47 とのクロス集計

Q47. 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。

| Q47.取扱う個人情報<br>Q46.個人情報取扱事業者 | 回答件数 | 1. 売買等契約の履行 |      | 2. 顧客サポート |      | 3. 代金等の回収 |      | 4. 情報提供 |      | 5. マーケティング |      |
|------------------------------|------|-------------|------|-----------|------|-----------|------|---------|------|------------|------|
| 1. 該当する                      | 340  | 169         | 49.7 | 211       | 62.1 | 130       | 38.2 | 94      | 27.6 | 127        | 37.4 |
| 2. 該当しない                     | 140  | 30          | 21.4 | 28        | 20.0 | 25        | 17.9 | 13      | 9.3  | 11         | 7.9  |
| 3. わからない                     | 28   | 9           | 32.1 | 9         | 32.1 | 11        | 39.3 | 0       | 0.0  | 2          | 7.1  |
| 4. 無回答                       | 6    | 1           | 16.7 | 1         | 16.7 | 0         | 0.0  | 2       | 33.3 | 0          | 0.0  |
| 5. 計                         | 514  | 209         | 40.7 | 249       | 48.4 | 166       | 32.3 | 109     | 21.2 | 140        | 27.2 |

| Q47.取扱う個人情報<br>Q46.個人情報取扱事業者 | 6. 商品開発 |      | 7. 行政サービスの履行 |      | 8. 委託(受託)処理 |      | 9. 従業員情報 |      | 10. その他 |      | 11. 無回答 |      |
|------------------------------|---------|------|--------------|------|-------------|------|----------|------|---------|------|---------|------|
| 1. 該当する                      | 91      | 26.8 | 18           | 5.3  | 150         | 44.1 | 289      | 85.0 | 37      | 10.9 | 1       | 0.3  |
| 2. 該当しない                     | 8       | 5.7  | 43           | 30.7 | 20          | 14.3 | 108      | 77.1 | 43      | 30.7 | 2       | 1.4  |
| 3. わからない                     | 1       | 3.6  | 0            | 0.0  | 1           | 3.6  | 26       | 92.9 | 0       | 0.0  | 0       | 0.0  |
| 4. 無回答                       | 1       | 16.7 | 1            | 16.7 | 0           | 0.0  | 3        | 50.0 | 1       | 16.7 | 3       | 50.0 |
| 5. 計                         | 101     | 19.6 | 62           | 12.1 | 171         | 33.3 | 426      | 82.9 | 81      | 15.8 | 6       | 1.2  |

個人情報取扱事業者に該当する可能性のある事業体が扱っている個人情報にはどのようなものがあるか分析した。個人情報取扱事業者に「該当する」と回答した事業体では、62.1%が「顧客サポート」で個人情報を取り扱っていると答えている。また、85.0%が「従業員情報」を個人情報として取り扱っていると答えている。

一方、個人情報取扱事業者に「該当しない」、または該当するか「わからない」事業体でも、それぞれ 77.1%、92.9%が「従業員情報」を個人情報として取り扱っていると答えている。

「情報提供」、「マーケティング」、「商品開発」など、ほとんどの項目で個人情報を取り扱うことになるのは自明であるが、多くの事業者ではこれを認識していないように見える。また、個人情報取扱事業者であれば、半年以上保有する場合、厳しい管理が義務づけられているが、これを認知していないようにも見える。

### 3.13.2 Q48 とのクロス集計

Q48.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。

| Q48.収集方法<br>Q46.個人情報取扱事業者 | 回答<br>件数 | 1. 情報主体<br>から直接収<br>集 |      | 2. 従業者か<br>ら直接収集 |      | 3. 営業活動<br>により情報主<br>体から直接<br>収集 |      | 4. 名簿業者<br>等から購入 |     | 5. グループ<br>企業から入<br>手 |      |
|---------------------------|----------|-----------------------|------|------------------|------|----------------------------------|------|------------------|-----|-----------------------|------|
| 1. 該当する                   | 340      | 268                   | 78.8 | 262              | 77.1 | 221                              | 65.0 | 18               | 5.3 | 42                    | 12.4 |
| 2. 該当しない                  | 140      | 91                    | 65.0 | 92               | 65.7 | 46                               | 32.9 | 1                | 0.7 | 4                     | 2.9  |
| 3. わからない                  | 28       | 14                    | 50.0 | 17               | 60.7 | 9                                | 32.1 | 1                | 3.6 | 1                     | 3.6  |
| 4. 無回答                    | 6        | 2                     | 33.3 | 2                | 33.3 | 3                                | 50.0 | 0                | 0.0 | 1                     | 16.7 |
| 5. 計                      | 514      | 375                   | 73.0 | 373              | 72.6 | 279                              | 54.3 | 20               | 3.9 | 48                    | 9.3  |

| Q48.収集方法<br>Q46.個人情報取扱事業者 | 6. 他社から<br>提供を受け<br>る |      | 7. 業務委託<br>契約等に基づき<br>預託される |      | 8. 住民基<br>本台帳から<br>入手 |      | 9. 新聞、<br>雑誌等メデ<br>ィアからの<br>収集 |     | 10. その他 |     | 11. 無回答 |      |
|---------------------------|-----------------------|------|-----------------------------|------|-----------------------|------|--------------------------------|-----|---------|-----|---------|------|
| 1. 該当する                   | 35                    | 10.3 | 103                         | 30.3 | 4                     | 1.2  | 14                             | 4.1 | 4       | 1.2 | 1       | 0.3  |
| 2. 該当しない                  | 3                     | 2.1  | 3                           | 2.1  | 21                    | 15.0 | 3                              | 2.1 | 13      | 9.3 | 1       | 0.7  |
| 3. わからない                  | 1                     | 3.6  | 1                           | 3.6  | 0                     | 0.0  | 0                              | 0.0 | 0       | 0.0 | 2       | 7.1  |
| 4. 無回答                    | 0                     | 0.0  | 0                           | 0.0  | 0                     | 0.0  | 0                              | 0.0 | 0       | 0.0 | 3       | 50.0 |
| 5. 計                      | 39                    | 7.6  | 107                         | 20.8 | 25                    | 4.9  | 17                             | 3.3 | 17      | 3.3 | 7       | 1.4  |

個人情報取扱事業者に該当する可能性のある事業者では、取り扱っている個人情報の収集方法についてどのような収集方法を取っているか分析した。

個人情報取扱事業者に「該当する」事業者では、78.8%が「情報主体から直接収集」で、65.0%が「営業活動により情報主体から直接収集」で個人情報を取り扱っていると答えている。また、個人情報取扱事業者に「該当しない」事業者は 65.0%が「情報主体から直接収集」と答えている。

一方、個人情報の収集方法のうち、「従業者から直接収集」については、個人情報取扱事業者に「該当する」、「該当しない」、「わからない」が、それぞれ 77.1%、65.7%、60.7%となっており、個人情報取扱事業者の有無にかかわらず、個人情報として収集し、取り扱っていることがわかる。

なお、個人情報保護法で重視している「業務委託契約に基づき預託される」によって得られる個人情報については、30.3%に留まっている。これは、実際に業務委託で個人情報について処理しない限りありえないので、この数字に問題はない。以上の結果からは、個人情報取の取扱いに際して「情報主体から直接収集」、「従業者から直接収集」、「営業活動により情報主体から直接収集」、「業務委託契約に基づき預託される」については、個人情報取扱事業者を自認している事業体が多く、それなりに個人情報保護法が理解されつつあることがわかる。

### 3.13.3 Q49 とのクロス集計

Q49.Q48 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についてどう考えますか。

| Q49.直接収集時の<br>利用目的の<br>同意<br>Q46.個人<br>情報取扱事業者 | 回答<br>件数 | 1. すべて同<br>意を取っ<br>ている |      | 2. 重要な変<br>更の場合の<br>み、個別に同<br>意を取っ<br>ている |       | 3. 何もして<br>いない |      | 4. わから<br>ない |      | 5. 無回答 |     |
|------------------------------------------------|----------|------------------------|------|-------------------------------------------|-------|----------------|------|--------------|------|--------|-----|
| 1. 該当する                                        | 267      | 200                    | 74.9 | 50                                        | 18.7  | 7              | 2.6  | 9.0          | 3.4  | 1      | 0.4 |
| 2. 該当しない                                       | 91       | 44                     | 48.4 | 22                                        | 24.2  | 10             | 11.0 | 7.0          | 7.7  | 8      | 8.8 |
| 3. わからない                                       | 14       | 4                      | 28.6 | 2                                         | 14.3  | 5              | 35.7 | 3.0          | 21.4 | 0      | 0.0 |
| 4. 無回答                                         | 2        | 0                      | 0.0  | 2                                         | 100.0 | 0              | 0.0  | 0            | 0.0  | 0      | 0.0 |
| 5. 計                                           | 374      | 248                    | 66.3 | 76                                        | 20.3  | 22             | 5.9  | 19.0         | 5.1  | 9      | 2.4 |

個人情報取扱事業者に該当する可能性のある事業体では、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についてどのようにしているのか分析した。

個人情報取扱事業者に「該当する」事業体では、利用目的について「すべて同意を取っている」が74.9%であった。「重要な変更の場合のみ、個別に同意を取っている」は18.7%であり、「何もしていない」や「わからない」は6%程度となっている。

一方、個人情報取扱事業者に「該当しない」事業体では、利用目的について「すべて同意を取っている」が48.4%と、比較的同意を取っていることがわかる。また、「重要な変更の場合のみ、個別に同意を取っている」は24.2%と個人情報取扱事業者に「該当する」事業体よりも高いことがわかる。これは、個人情報取扱事業者でなくても、個人情報を収集する際には対象となる個人から事業者に対し、利用目的を質問されるためであろう。

### 3.13.4 Q51 とのクロス集計

Q51.個人情報の漏洩により深刻な被害を及ぼす事項をどのように認識していますか。

| Q51.漏えい被害<br>Q46.個人情報取扱事業者 | 回 答<br>件数 | 1. 社会的な<br>信用の低下 |      | 2. 親会社や<br>関連会社側、<br>企業グルー<br>プの社会的<br>信用の低下 |      | 3. 顧客や取<br>引先、官公庁<br>からの取引で<br>の指名停止 |      | 4. 情報が漏<br>洩した情報主<br>体からの損害<br>賠償請求 |      | 5. 契約違反<br>による処分や<br>訴訟 |      |
|----------------------------|-----------|------------------|------|----------------------------------------------|------|--------------------------------------|------|-------------------------------------|------|-------------------------|------|
| 1. 該当する                    | 340       | 320              | 94.1 | 189                                          | 55.6 | 195                                  | 57.4 | 255                                 | 75.0 | 139                     | 40.9 |
| 2. 該当しない                   | 140       | 120              | 85.7 | 31                                           | 22.1 | 22                                   | 15.7 | 92                                  | 65.7 | 27                      | 19.3 |
| 3. わからない                   | 28        | 17               | 60.7 | 11                                           | 39.3 | 6                                    | 21.4 | 11                                  | 39.3 | 4                       | 14.3 |
| 4. 無回答                     | 6         | 3                | 50.0 | 1                                            | 16.7 | 1                                    | 16.7 | 1                                   | 16.7 | 1                       | 16.7 |
| 5. 計                       | 514       | 460              | 89.5 | 232                                          | 45.1 | 224                                  | 43.6 | 359                                 | 69.8 | 171                     | 33.3 |

| Q51.漏えい被害<br>Q46.個人情報取扱事業者 | 6. 株価下落<br>や各付けの<br>低下 |      | 7. その他 |     | 8. わから<br>ない |      | 9. 特に大き<br>な影響は<br>ない |     | 10. 無回答 |      |
|----------------------------|------------------------|------|--------|-----|--------------|------|-----------------------|-----|---------|------|
| 1. 該当する                    | 115                    | 33.8 | 6      | 1.8 | 3            | 0.9  | 0                     | 0.0 | 9       | 2.6  |
| 2. 該当しない                   | 15                     | 10.7 | 7      | 5.0 | 3            | 2.1  | 3                     | 2.1 | 10      | 7.1  |
| 3. わからない                   | 7                      | 25.0 | 0      | 0.0 | 10           | 35.7 | 0                     | 0.0 | 1       | 3.6  |
| 4. 無回答                     | 0                      | 0.0  | 0      | 0.0 | 0            | 0.0  | 0                     | 0.0 | 3       | 50.0 |
| 5. 計                       | 137                    | 26.7 | 13     | 2.5 | 16           | 3.1  | 3                     | 0.6 | 23      | 4.5  |

個人情報取扱事業者に該当する可能性のある事業体では、個人情報の漏えいにより深刻な被害を及ぼす事項をどのように認識しているかについて分析した。

個人情報取扱事業者に「該当する」事業体では、個人情報の漏えいについて「社会的な信用の低下」が 94.1%であった。「顧客や取引先、官公庁からの取引での指名停止」が 57.4%、「親会社や関連会社側、企業グループの社会的信用の低下」が 55.6%と続いている。すなわち、個人情報取扱事業者に「該当する」事業体では、個人情報の漏えいにより深刻な被害を及ぼす事項について、「該当しない」や「わからない」に比べて有意差があることがわかる。

### 3.13.5 Q53 とのクロス集計

Q53. 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。

| Q53.個人情報管理<br>状況のリスク<br>Q46.個人<br>情報取扱事業者 | 回答<br>件数 | 1. 対応策を<br>講じている<br>ので、リスク<br>はないと認<br>識している |     | 2. 現状の管<br>理方法で何<br>も問題が発<br>生していな<br>いので、リス<br>クはないと認<br>識している |      | 3. 対策を講<br>じているが、<br>リスクはある<br>と認識してい<br>る |      | 4. 何度かヒ<br>ヤリ・ハツとし<br>た経験があ<br>り、リスクがあ<br>ると認識して<br>いる |      | 5. いつ問題<br>が発生して<br>もおかしくな<br>い状況であ<br>ると認識して<br>いる |      |
|-------------------------------------------|----------|----------------------------------------------|-----|-----------------------------------------------------------------|------|--------------------------------------------|------|--------------------------------------------------------|------|-----------------------------------------------------|------|
| 1. 該当する                                   | 340      | 4                                            | 1.2 | 6                                                               | 1.8  | 270                                        | 79.4 | 24                                                     | 7.1  | 25                                                  | 7.4  |
| 2. 該当しない                                  | 140      | 1                                            | 0.7 | 9                                                               | 6.4  | 95                                         | 67.9 | 3                                                      | 2.1  | 19                                                  | 13.6 |
| 3. わからない                                  | 28       | 0                                            | 0.0 | 3                                                               | 10.7 | 10                                         | 35.7 | 2                                                      | 7.1  | 6                                                   | 21.4 |
| 4. 無回答                                    | 6        | 0                                            | 0.0 | 0                                                               | 0.0  | 2                                          | 33.3 | 1                                                      | 16.7 | 0                                                   | 0.0  |
| 5. 計                                      | 514      | 5                                            | 1.0 | 18                                                              | 3.5  | 377                                        | 73.3 | 30                                                     | 5.8  | 50                                                  | 9.7  |

| Q53.個人情報管理<br>状況のリスク<br>Q46.個人<br>情報取扱事業者 | 6. その他 |     | 7. 特に認識<br>していない |      | 8. 無回答 |      |
|-------------------------------------------|--------|-----|------------------|------|--------|------|
| 1. 該当する                                   | 2      | 0.6 | 3                | 0.9  | 6      | 1.8  |
| 2. 該当しない                                  | 0      | 0.0 | 10               | 7.1  | 3      | 2.1  |
| 3. わからない                                  | 0      | 0.0 | 7                | 25.0 | 0      | 0.0  |
| 4. 無回答                                    | 0      | 0.0 | 0                | 0.0  | 3      | 50.0 |
| 5. 計                                      | 2      | 0.4 | 20               | 3.9  | 12     | 2.3  |

個人情報取扱事業者に該当する可能性のある事業体では、現在の個人情報の管理状況についてのリスクをどのように認識しているか分析した。

個人情報取扱事業者に「該当する」事業体では、個人情報の管理状況について「対策を講じているがリスクはあると認識している」が 79.4%であった。一方、個人情報取扱事業者に「該当しない」と述べている事業体でも、個人情報の管理状況について、「対策を講じているがリスクはあると認識している」が 67.9%となっている。すなわち、個人情報取扱事業者に「該当する」または「該当しない」事業体は、「わからない」と答えている事業者に比べ、個人情報の管理状況についてのリスクを認識していることがわかる。

### 3.13.6 Q54 とのクロス集計

Q54.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。

| Q54.外部委託時の契約条項<br>Q46.個人情報取扱事業者 | 回答件数 | 1. 機密保持義務 |      | 2. 責任分担 |      | 3. 個人情報の適正な管理 |      | 4. 目的外使用・再委託の制限 |      | 5. 個人情報の取扱いに関する監査の実施 |      |
|---------------------------------|------|-----------|------|---------|------|---------------|------|-----------------|------|----------------------|------|
| 1. 該当する                         | 340  | 302       | 88.8 | 186     | 54.7 | 249           | 73.2 | 239             | 70.3 | 134                  | 39.4 |
| 2. 該当しない                        | 140  | 97        | 69.3 | 55      | 39.3 | 84            | 60.0 | 83              | 59.3 | 35                   | 25.0 |
| 3. わからない                        | 28   | 12        | 42.9 | 5       | 17.9 | 9             | 32.1 | 9               | 32.1 | 4                    | 14.3 |
| 4. 無回答                          | 6    | 3         | 50.0 | 2       | 33.3 | 2             | 33.3 | 3               | 50.0 | 1                    | 16.7 |
| 5. 計                            | 514  | 414       | 80.5 | 248     | 48.2 | 344           | 66.9 | 334             | 65.0 | 174                  | 33.9 |

| Q54.外部委託時の契約条項<br>Q46.個人情報取扱事業者 | 6. その他 |     | 7. 外部委託を行っていない |      | 8. 無回答 |      |
|---------------------------------|--------|-----|----------------|------|--------|------|
| 1. 該当する                         | 7      | 2.1 | 25             | 7.4  | 7      | 2.1  |
| 2. 該当しない                        | 5      | 3.6 | 39             | 27.9 | 0      | 0.0  |
| 3. わからない                        | 0      | 0.0 | 11             | 39.3 | 3      | 10.7 |
| 4. 無回答                          | 0      | 0.0 | 0              | 0.0  | 3      | 50.0 |
| 5. 計                            | 12     | 2.3 | 75             | 14.6 | 13     | 2.5  |

個人情報取扱事業者に該当する可能性のある事業体では、取り扱っている個人情報を外部委託する場合に交わす契約条項に何があるか分析した。

個人情報取扱事業者に「該当する」事業体では、外部委託する場合に、88.8%が「機密保持義務」で、73.2%が「個人情報の適正な管理」、70.3%が「目的外使用・再委託の制限」を実施して個人情報を取り扱っていると回答している。また、個人情報取扱事業者に「該当しない」事業者でも 69.3%が「機密保持義務」で、60.0%が「個人情報の適正な管理」、59.3%が「目的外使用・再委託の制限」を実施して、個人情報を取り扱っていると回答している。

すなわち、個人情報取扱事業者に「該当する」、「該当しない」による違いは、外部委託する場合に交わす契約条項の遵守状況が異なることがわかる。「該当する」事業体の方が、10 ポイント以上、契約項目に注意を払っていることがわかる。



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



2005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 <span style="margin-left: 100px;">—</span> <span style="margin-left: 100px;">—</span><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）                              |                                                                                                 |
| 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定の定員数をご記入下さい。） |                                                                                                 |

- ◇ 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 <small>20, 21</small> |                      | 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。

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 |
|----|------------------------------|------------------|-------|------|
| 23 | ①情報システム安全対策基準(平成7年8月改訂)      | 1                | 2     | 3    |
| 24 | ②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    |
| 25 | ③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    |
| 26 | ④システム監査基準(平成16年10月改訂)        | 1                | 2     | 3    |
| 27 | ⑤システム管理基準(平成16年10月策定)        | 1                | 2     | 3    |
| 28 | ⑥システム監査企業台帳制度(平成3年3月制定)      | 1 <sup>(注)</sup> | 2     | 3    |
| 29 | ⑦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    |
| 30 | ⑧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 <sup>(注)</sup> | 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. 以下のJIS規格等を知っていますか。

|    | 規格名                                                   | 利用している | 知っている | 知らない |
|----|-------------------------------------------------------|--------|-------|------|
| 31 | ①JIS 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    |
| 32 | ②JIS 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    |
| 33 | ③JIS 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    |
| 34 | ④事業継続計画(BCP)策定ガイドライン<br>(平成17年3月策定)                   | 1      | 2     | 3    |
| 35 | ⑤事業継続ガイドライン第1版(平成17年8月策定)                             | 1      | 2     | 3    |
| 36 | ⑥ISMS認証基準(Ver.2.0)                                    | 1      | 2     | 3    |

37 B

2 情報リスクマネジメントについて

Q3. 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        |

Q4. 経営者層は次の事項について関心が高いですか。

|    | 関心事項                   | 高い | 中い | 低い | わからない |
|----|------------------------|----|----|----|-------|
| 39 | ①情報システム関連の事件・事故に対するリスク | 1  | 2  | 3  | 4     |
| 40 | ②個人情報などの情報漏えいに対するリスク   | 1  | 2  | 3  | 4     |
| 41 | ③情報セキュリティガバナンス(注1)     | 1  | 2  | 3  | 4     |
| 42 | ④情報セキュリティ対策ベンチマーク(注2)  | 1  | 2  | 3  | 4     |

注1) 情報セキュリティガバナンスは、経済産業省が進めている情報セキュリティ対策の新しい枠組みで、企業の株主などの利害関係者に対して情報セキュリティに関する報告書を発行するなどが盛り込まれている。

注2) 情報セキュリティ対策ベンチマークは、経済産業省が進めている情報セキュリティの対策の総合評価方法で、数値化された結果が得られる

Q5. 情報システム関連、情報セキュリティ関連、個人情報保護漏洩のリスクが貴事業体の経営に重大な影響(経営危機、倒産等)を与えますか。(単一回答)

|    |   |              |
|----|---|--------------|
| 43 | 1 | 思 う          |
|    | 2 | 重大な影響は受けると思う |
|    | 3 | 重大な影響は受けない   |
|    | 4 | わからない        |

Q6. 情報セキュリティガバナンス(Q4の「注1」参照)の観点から、情報セキュリティ対策にあたり、どの関係者を考慮に入れていますか。(複数回答)

|    |   |                  |
|----|---|------------------|
| 44 | 1 | 株主・投資家等          |
| 45 | 2 | 顧客・消費者           |
| 46 | 3 | 取引先              |
| 47 | 4 | 格付け機関            |
| 48 | 5 | 従業員              |
| 49 | 6 | その他(具体的に書いて下さい。) |

Q7. 次のリスク分析手法を知っていますか。

|    | リスク分析手法                                                                    | 利用したことがある | 知っている | 知らない |
|----|----------------------------------------------------------------------------|-----------|-------|------|
| 50 | ①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)における脆弱性分析                         | 1         | 2     | 3    |
| 51 | ②日本情報処理開発協会が開発したJRAMIにおける定量分析                                              | 1         | 2     | 3    |
| 52 | ③GMITS(GMITS Guidelines for the Management for IT Security (ISO/IEC13335)) | 1         | 2     | 3    |
| 53 | ④その他(具体的に書いて下さい。)                                                          | 1         | 2     |      |

Q8. 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、情報セキュリティポリシー、情報リスクの分析、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。これらの対策を実施していますか。

注) ③「情報リスク分析」で「1」を回答した場合のみQ9に、それ以外はQ11に進んで下さい。

|                            | 策定／実施<br>している | 策定／実施を<br>予定している | 策定／実施の<br>予定はない |
|----------------------------|---------------|------------------|-----------------|
| 54 ①情報リスクマネジメント方針の明確化      | 1             | 2                | 3               |
| 55 ②情報セキュリティポリシーの策定        | 1             | 2                | 3               |
| 56 ③情報リスク分析の実施             | 1 ⇒Q9へ        | 2                | 3               |
| 57 ④情報セキュリティ対策の実施手順、規程類の策定 | 1             | 2                | 3               |
| 58 ⑤情報セキュリティ監査の実施          | 1             | 2                | 3               |
| 59 ⑥システム監査の実施              | 1             | 2                | 3               |

Q9. Q8で「③情報リスク分析を実施している」と回答した場合、

①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)

②対象リスクを分析した結果、経営に与える影響が大きかったのは何ですか。(単一回答)

| ①対象リスク |                                                               | ②リスク分析の結果、経営に与える影響 |       |       |
|--------|---------------------------------------------------------------|--------------------|-------|-------|
|        |                                                               | 影響が<br>あった         | 影響はない | わからない |
| 60 1   | 自然災害(地震を除く水害等)                                                | 81 1               | 2     | 3     |
| 61 2   | 地震                                                            | 82 1               | 2     | 3     |
| 62 3   | 人的災害(テロ 等)                                                    | 83 1               | 2     | 3     |
| 63 4   | コンピュータ犯罪(不正アクセス、サーバ乗っ取り、故意等を含む)のリスク                           | 84 1               | 2     | 3     |
| 64 5   | 運用障害(操作ミス、入力ミス等)                                              | 85 1               | 2     | 3     |
| 65 6   | 事故(火災、爆発、停電、漏水等)                                              | 86 1               | 2     | 3     |
| 66 7   | 不正侵入で起きるサーバの乗っ取り                                              | 87 1               | 2     | 3     |
| 67 8   | 自社従業員などによる故意による情報漏えい                                          | 88 1               | 2     | 3     |
| 68 9   | 不注意・過失による情報漏えい(電子メールやファックスの誤送信を含む)                            | 89 1               | 2     | 3     |
| 69 10  | 盗難・車上荒らしなどによる情報漏えい                                            | 90 1               | 2     | 3     |
| 70 11  | システムの統合リスク                                                    | 91 1               | 2     | 3     |
| 71 12  | システムの改良・容量増に伴うトラブル                                            | 92 1               | 2     | 3     |
| 72 13  | 過負荷によるシステムダウン                                                 | 93 1               | 2     | 3     |
| 73 14  | ハードウェア障害                                                      | 94 1               | 2     | 3     |
| 74 15  | ソフトウェア障害                                                      | 95 1               | 2     | 3     |
| 75 16  | ネットワーク障害                                                      | 96 1               | 2     | 3     |
| 76 17  | コンピュータウイルス、スパイウェアによるシステムの停止                                   | 97 1               |       | 3     |
| 77 18  | (コンピュータウイルスパラメータなどの)信用してダウンロードしたファイルのエラーやスパイウェアによって起きるシステムの停止 | 98 1               | 2     | 3     |
| 78 19  | フィッシングなどで自社サイトが模倣され、自社ユーザに被害がでる                               | 99 1               | 2     | 3     |
| 79 20  | ボットなどを利用したDDoS攻撃                                              | 100 1              | 2     | 3     |
| 80 21  | その他(具体的に書いて下さい)                                               | 101 1              | 2     | 3     |

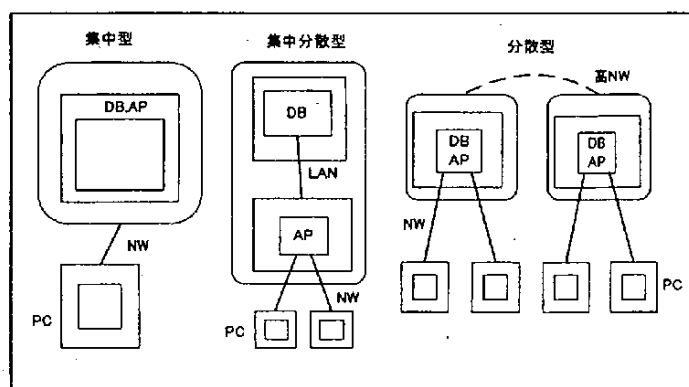
Q10. Q8で「③情報リスク分析を実施している」と回答した場合、リスク分析を実施した際の問題点は何ですか。(複数回答)

|     |   |                              |
|-----|---|------------------------------|
| 103 | 1 | 経営との関係がわからない                 |
| 104 | 2 | 確立した手法がない(被害想定額・被害頻度が算出できない) |
| 105 | 3 | 分析のためのデータが乏しい                |
| 106 | 4 | 専門家がない                       |
| 107 | 5 | 組織ができていない                    |
| 108 | 6 | リスクの定量化が測れない                 |
| 109 | 7 | その他(具体的に書いて下さい。)             |
| 110 | 8 | 特に問題はない                      |

Q11. 基幹システム<sup>注1)</sup>が1時間以上停止した場合、経営に与える影響があると思いますか。

|     |   |     |       |
|-----|---|-----|-------|
| 111 | 1 | はい  | ⇒Q12へ |
|     | 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。



Q12. Q11で「1」と回答した場合、被害の推定額<sup>(注)</sup>は1日あたりどれ位ですか。

|     |   |               |
|-----|---|---------------|
| 112 | 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        |

(注)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。

Q13. ①貴事業体の基幹システムは、過去1年間に、システムの運用に悪影響を与えたか、または事業中断につながるシステムダウン<sup>(注1)</sup>が発生しましたか。

②システムダウンはシステムの運用に悪影響を与えたか、さらに事業中断につながるものでしたか。

(①、②ともに複数回答)

| ①システムダウンの状況 |             | ②システムダウンの影響                 |       |
|-------------|-------------|-----------------------------|-------|
|             |             | システム運用への悪影響 <sup>(注2)</sup> | 事業中断  |
| 113         | 1 全体的にダウンした | 116 1                       | 118 2 |
| 114         | 2 部分的にダウンした | 117 1                       | 119 2 |
| 115         | 3 ダウンしない    | ⇒Q15へ                       |       |

(注1)システムダウンとは、システムの全面ストップもしくはそれに準じる障害と定義します。

(注2)「システム運用への悪影響」は、事業中断にまでは至らなかったシステム障害を指します。

- Q14. ①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)  
 ②システムダウンの結果、「システム運用への悪影響」(事業中断には至っていない)、または「事業中断」にまで至りましたか。(複数回答)

| ①原因 |                                                    | ②システムへの影響度合い |       |
|-----|----------------------------------------------------|--------------|-------|
|     |                                                    | システム運用       | 事業中断  |
| 120 | 1 自然災害(地震を除く水害等)                                   | 136 1        | 152 2 |
| 121 | 2 地震                                               | 137 1        | 153 2 |
| 122 | 3 火災による事故・障害                                       | 138 1        | 154 2 |
| 123 | 4 停電(電力会社に起因する障害)                                  | 139 1        | 155 2 |
| 124 | 5 電源機器・設備障害                                        | 140 1        | 156 2 |
| 125 | 6 空調等障害                                            | 141 1        | 157 2 |
| 126 | 7 通信障害(通信事業者、ISPの障害を含む)                            | 142 1        | 158 2 |
| 127 | 8 ネットワーク機器などの障害                                    | 143 1        | 159 2 |
| 128 | 9 サーバなどのハードウェア障害                                   | 144 1        | 160 2 |
| 129 | 10 OS障害                                            | 145 1        | 161 2 |
| 130 | 11 アプリケーションソフトウェア障害                                | 146 1        | 162 2 |
| 131 | 12 コンピュータウイルス、スパイウェア(ウイルスによる不正侵入・ネットワーク障害を含む)による障害 | 147 1        | 163 2 |
| 132 | 13 不正アクセスやDOS攻撃によるサービス中断                           | 148 1        | 164 2 |
| 133 | 14 人の悪意(たとえば内部犯罪、不正侵入)による事故等                       | 149 1        | 165 2 |
| 134 | 15 オペミス等、人の過失による事故等                                | 150 1        | 166 2 |
| 135 | 16 その他(具体的に書いて下さい)                                 | 151 1        | 167 2 |

- Q15. 基幹システムにおけるMTBF(平均故障間隔)は何時間ですか。(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 時間稼働中に 2 回ダウンした場合  $\Rightarrow (365 \text{ 日} \times 24 \text{ H}) / (2 \text{ 回} + 1) = 2,920 \text{ 時間}$

168       時間 172

(右詰めで記入して下さい)

- Q16. 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)

173      分 176

(右詰めで記入して下さい)

- Q17. 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 |   |   |   |   |
|---------|-----------------------------------|-------|---|---|---|---|
| 177     | ①市販のソフトをコピーして使う                   | 1     | 2 | 3 | 4 | 5 |
| 178     | ②データ、プログラムを無断で使う                  | 1     | 2 | 3 | 4 | 5 |
| 179     | ③データを盗み見る                         | 1     | 2 | 3 | 4 | 5 |
| 180     | ④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 |
| 181     | ⑤WWW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 |
| 182     | ⑥私的な電子メールを送・受信する                  | 1     | 2 | 3 | 4 | 5 |
| 183     | ⑦他人のIDを無断借用する                     | 1     | 2 | 3 | 4 | 5 |

犯罪度欄の回答群1～5は次のように定義します。

- |                   |                          |
|-------------------|--------------------------|
| 1. 特に問題ではない       | 2. 企業内で戒告・訓告・注意処分等の対象となる |
| 3. 企業内で懲戒免職の対象となる | 4. 犯罪行為である(刑法上の処罰の対象となる) |
| 5. わからない          |                          |

3 情報セキュリティポリシー・管理・対策について

Q18. 情報セキュリティの確保にとり、基本的に重要な要素は何だと思いますか。(複数回答)

|     |   |                    |
|-----|---|--------------------|
| 185 | 1 | 経営者層の理解            |
| 186 | 2 | 管理者の理解             |
| 187 | 3 | 担当者の理解             |
| 188 | 4 | 社内全体の理解(エンドユーザを含む) |
| 189 | 5 | 社内規定やルールの整備        |
| 190 | 6 | その他(具体的に書いて下さい。)   |

Q19. 貴事業体では、情報セキュリティ対策(不正アクセス対策、コンピュータウイルス対策、信頼性対策、個人情報保護対策、情報セキュリティ監査、システム監査等)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)

191   .   % 194

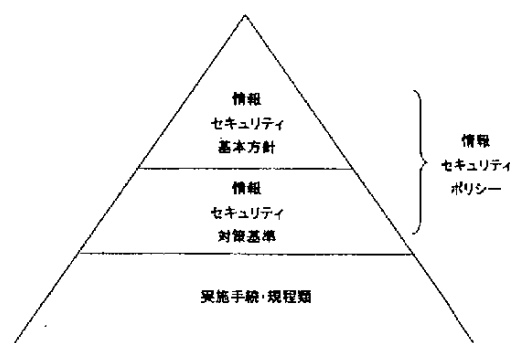
(右詰めで記入して下さい)

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>



Q20. 以下の管理について、責任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 |
|-----|--------------|-------|-----------|--------|------|
| 195 | ①ネットワークの管理   | 1     | 2         | 3      | 4    |
| 196 | ②情報システムの管理   | 1     | 2         | 3      | 4    |
| 197 | ③情報セキュリティの管理 | 1     | 2         | 3      | 4    |

Q21. 情報セキュリティ(システム災害/障害、不正アクセス、コンピュータウイルスを含む)管理についての問題点は何ですか。(複数回答)

|     |    |                                |
|-----|----|--------------------------------|
| 198 | 1  | 経営者層の理解が得られない                  |
| 199 | 2  | コストがかかりすぎる                     |
| 200 | 3  | 専門要員がいない(要員が確保できない)            |
| 201 | 4  | 組織の従業員に対する負担がかかりすぎる            |
| 202 | 5  | 組織の従業員に対する教育・訓練がいきとどかない        |
| 203 | 6  | ノウハウが不足している                    |
| 204 | 7  | どこまでやればよいのか基準が示されていない          |
| 205 | 8  | 要求に合致するもの(サービス/製品)がない          |
| 206 | 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 |
| 207 | 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      |
| 208 | 11 | その他(具体的に書いて下さい)                |
| 209 | 12 | 特に問題はない                        |

Q22. 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、コンピュータウイルス対策、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 <sup>210</sup> | 第2位 <sup>212</sup> | 第3位 <sup>214</sup> |
|-----|------|--------------------|--------------------|--------------------|

216 E

|   |               |
|---|---------------|
| 4 | 災害対策・障害対策について |
|---|---------------|

Q23. 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。

|                  |                                  |
|------------------|----------------------------------|
| <sup>217</sup> 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)   |

Q24. 「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)。

|                  |             |       |
|------------------|-------------|-------|
| <sup>218</sup> 1 | 作成している      | ⇒Q25へ |
| 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     | ⇒Q26へ |
| 5                | 必要ない        |       |

Q25. (Q24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)

|                  |                                      |
|------------------|--------------------------------------|
| <sup>219</sup> 1 | 外部からの悪意による緊急事態(サイバーテロ、コンピュータウイルス等)   |
| <sup>220</sup> 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)    |
| <sup>221</sup> 3 | 事故・災害(火災、地震、風水害、停電等)                 |
| <sup>222</sup> 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)      |
| <sup>223</sup> 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) |
| <sup>224</sup> 6 | 内部犯罪による緊急事態                          |
| <sup>225</sup> 7 | 伝染病(SARS等)                           |
| <sup>226</sup> 8 | その他(具体的に書いて下さい。)                     |

Q26. 災害に対する情報システムのバックアップ対策を講じていますか。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)

|     |    |                            |
|-----|----|----------------------------|
| 227 | 1  | 対象システムを決めている               |
| 228 | 2  | バックアップに関する規程や手順を決めている      |
| 229 | 3  | バックアップの頻度、バックアップ先を決定している   |
| 230 | 4  | バックアップを定期的の実施している          |
| 231 | 5  | バックアップの実施状況を定期的にチェックしている   |
| 232 | 6  | 回復手順を決めている                 |
| 233 | 7  | バックアップを業者に委託するときはSLAを結んでいる |
| 234 | 8  | バックアップシステムの稼働状況を確認している     |
| 235 | 9  | アウトソーシング先の対策は把握していない       |
| 236 | 10 | 特に講じていない                   |

Q27. 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。設置(予定)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)

|     |   |                      |
|-----|---|----------------------|
| 237 | 1 | ホットスタンバイシステム         |
| 238 | 2 | コールドスタンバイシステム        |
| 239 | 3 | クラスタリング              |
| 240 | 4 | RAID(RAID1~5)        |
| 241 | 5 | フォールトトレラント           |
| 242 | 6 | アウトソーシング先の対策は把握していない |
| 243 | 7 | 特に設けていない             |

Q28. 貴事業体ではどのような地震対策をとっていますか。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 |                      |
|-----|---------|----------------------|
| 244 | 1       | 建物が免震構造になっている        |
| 245 | 2       | 建物が耐震構造になっている        |
| 246 | 3       | 転倒防止措置を講じている         |
| 247 | 4       | 機器の移動防止措置を講じている      |
| 248 | 5       | フリーアクセス床は耐震構造としている   |
| 249 | 6       | フリーアクセス床は免震構造としている   |
| 250 | 7       | 媒体の落下防止措置を講じている      |
| 251 | 8       | その他(具体的に対策を書いて下さい)   |
| 252 | 9       | アウトソーシング先の対策は把握していない |
| 253 | 10      | 特に対策を講じていない          |

Q29. 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)

|     |   |                    |
|-----|---|--------------------|
| 254 | 1 | AVR                |
| 255 | 2 | CVCF/UPS           |
| 256 | 3 | 自家発電装置             |
| 257 | 4 | 電力供給経路の複数化         |
| 258 | 5 | その他(具体的に対策を書いて下さい) |
| 259 | 6 | 特に対策を講じていない        |

Q30. 貴事業体では従業員に対し、情報セキュリティのどの教育・訓練を実施していますか。

|     | 管理項目           | 定期的実施<br>している | 時々実施<br>している | 実施を予定<br>している | 実施していない |
|-----|----------------|---------------|--------------|---------------|---------|
| 260 | ①災害対策          | 1             | 2            | 3             | 4       |
| 261 | ②障害対策          | 1             | 2            | 3             | 4       |
| 262 | ③不正アクセス対策      | 1             | 2            | 3             | 4       |
| 263 | ④コンピュータウイルス対策  | 1             | 2            | 3             | 4       |
| 264 | ⑤ポリシー類         | 1             | 2            | 3             | 4       |
| 265 | ⑥アクセス制限の実施     | 1             | 2            | 3             | 4       |
| 266 | ⑦個人情報保護        | 1             | 2            | 3             | 4       |
| 267 | ⑧情報セキュリティの一般知識 | 1             | 2            | 3             | 4       |

Q31. 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。(単一回答)

|     |   |                                 |
|-----|---|---------------------------------|
| 268 | 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 | 民間の教育機関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などの資格試験を活用している |
|     | 4 | 特に行っていない                        |
|     | 5 | 必要ない                            |

269

F

5 不正アクセス対策・不正侵入対策・情報漏洩対策について

Q32. 管理面における不正アクセス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)

|     |    |                                                      |
|-----|----|------------------------------------------------------|
| 270 | 1  | 不正アクセスを受けた場合のIPAやJPCERT/CCへの相談                       |
| 271 | 2  | 室の出入口での入・退室管理                                        |
| 272 | 3  | 室の管理責任者の設置                                           |
| 273 | 4  | パソコン・記録媒体の持込み・持出しの管理                                 |
| 274 | 5  | 重要情報を扱うシステムを隔離し、他のシステムと接続させない                        |
| 275 | 6  | 個人情報・機密情報の担当者の限定(アクセス制限)                             |
| 276 | 7  | ネットワーク機器の運用者(アクセス範囲)の限定                              |
| 277 | 8  | 情報セキュリティポリシーで勝手にLANの配線に触ったり、個人のPCを接続することの禁止          |
| 278 | 9  | 情報セキュリティ管理者やネットワーク管理者によるサーバやルータ、ファイアウォールのログの定期的なチェック |
| 279 | 10 | 定期的なリスク分析や情報セキュリティ監査を実施                              |
| 280 | 11 | その他(具体的に書いて下さい。)                                     |
| 281 | 12 | アウトソーサ側の実施対策を確認している                                  |
| 282 | 13 | 特に対策を講じていない                                          |

Q33. 技術面における不正アクセス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  | 室への入退室についてカード、パスワードを使用                                            |
| 284 | 2  | 入退室のときにアンチパスバック(定期券のように二度連続して入れないような仕組み)を持っている                    |
| 285 | 3  | 室への入室について身体的特徴(指紋、虹彩等)により識別                                       |
| 286 | 4  | 情報システムの監視設備を設けている                                                 |
| 287 | 5  | ファイアウォールの利用                                                       |
| 288 | 6  | セキュリティパッチの適用                                                      |
| 289 | 7  | アクセス制御ソフトウェアの使用                                                   |
| 290 | 8  | 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 |
| 291 | 9  | その他(具体的に書いて下さい)                                                   |
| 292 | 10 | 特に対策を講じていない                                                       |

Q34. 情報価値の視点から、個人情報や機密情報等に対し機密度区分を設定していますか。(単一回答)

|     |   |                        |
|-----|---|------------------------|
| 293 | 1 | 機密区分を設定し、暗号化している       |
|     | 2 | 機密区分を設定しているが、暗号化はしていない |
|     | 3 | 機密区分を設定していないが、暗号化をしている |
|     | 4 | 機密区分を設定しておらず、暗号化もしていない |

Q35. 貴事業体では基幹システム・重要なサーバ、シングルサインオン等<sup>注)</sup>の一般ユーザのパスワード変更をどのレベルに設定していますか。(単一回答)

|     |   |                                 |
|-----|---|---------------------------------|
| 294 | 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(具体的に書いて下さい。)                |

(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)

Q36. 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)

|     |    |                                                            |
|-----|----|------------------------------------------------------------|
| 295 | 1  | セキュリティポリシー、個人情報保護ポリシー、規程類の整備                               |
| 296 | 2  | 従業者に対する教育                                                  |
| 297 | 3  | 入退室(館)管理                                                   |
| 298 | 4  | アクセス制限                                                     |
| 299 | 5  | 機密情報の管理                                                    |
| 300 | 6  | 不正プログラムの侵入防止(コンピュータウイルス等でキーロガーやデータの不正送信プログラムが持ち込まれないようにする) |
| 301 | 7  | 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                         |
| 302 | 8  | ハードディスク、CD、FD等記録媒体や不要となった印刷物の返却、廃棄時の破壊、溶解                  |
| 303 | 9  | 暗号化機能の採用                                                   |
| 304 | 10 | 輸送体制強化                                                     |
| 305 | 11 | 電子メールの送信時モニタリング                                            |
| 306 | 12 | ログチェックの追跡機能                                                |
| 307 | 13 | その他(具体的に書いて下さい。)                                           |
| 308 | 14 | 特に対策を行っていない                                                |

309

G

6 コンピュータウイルス対策について

Q37. 貴事業体では過去1年間にコンピュータウイルス、スパイウェア、スパムメール、フィッシングの被害にあったことがありますか。(複数回答)

|     |   |                         |       |
|-----|---|-------------------------|-------|
| 310 | 1 | コンピュータウイルス              | ⇒Q38へ |
| 311 | 2 | スパイウェア                  |       |
| 312 | 3 | スパムメール                  | ⇒Q39へ |
| 313 | 4 | フィッシング(自社のWebを模倣・悪用された) |       |
| 314 | 5 | 被害はない                   |       |
| 315 | 6 | 被害を把握していない              |       |

Q38. Q37で「1」、「2」を回答した場合、コンピュータウイルス、スパイウェアの主要な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)

|     |    |                             |
|-----|----|-----------------------------|
| 316 | 1  | フリーソフトウェアから                 |
| 317 | 2  | 社内ネットワーク経由で                 |
| 318 | 3  | インターネット経由で                  |
| 319 | 4  | 電子メールの添付書類で                 |
| 320 | 5  | 外部のホームページの閲覧で               |
| 321 | 6  | ネットワーク経由の不正アクセス             |
| 322 | 7  | スパムメールのリンク先                 |
| 323 | 8  | バックドア                       |
| 324 | 9  | ファイル交換ソフト                   |
| 325 | 10 | インスタントメッセージサービス             |
| 326 | 11 | 外部との情報交換のために持ち込んだPCや記録媒体経由で |
| 327 | 12 | 個人が持ち込んだPCや記録媒体経由で          |
| 328 | 13 | その他(具体的に書いて下さい。)            |
| 329 | 14 | わからない                       |

Q39. コンピュータウイルス、スパイウェア、スパムメール、フィッシング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)

|     |    |                                                        |
|-----|----|--------------------------------------------------------|
| 330 | 1  | 被害を受けた場合のIPAへの相談                                       |
| 331 | 2  | 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                      |
| 332 | 3  | 緊急対策チーム(社内でコンピュータウイルスが検出された時の対応を行うチーム)の設置              |
| 333 | 4  | 検出時や緊急対応と連絡体制の整備                                       |
| 334 | 5  | 従業員の教育(出所のわからないメール、疑わしいメールを開封しない 等)                    |
| 335 | 6  | 出所の確認                                                  |
| 336 | 7  | 記録媒体利用時のチェックの実施                                        |
| 337 | 8  | ライトプロテクト、バックアップ等のソフトウェア管理                              |
| 338 | 9  | PCでのワクチンソフト(検出ソフトを含む)の利用                               |
| 339 | 10 | PCのワクチンソフト・パラメータファイルの定期的な更新                            |
| 340 | 11 | サーバ機でのワクチンソフトの利用(ISPの提供するサービス利用)                       |
| 341 | 12 | 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                             |
| 342 | 13 | 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)                  |
| 343 | 14 | ワクチンソフトの集中監視                                           |
| 344 | 15 | 定期的な集中監視ログの解析                                          |
| 345 | 16 | パスワードの変更等、アクセスコントロールの強化                                |
| 346 | 17 | 動作の定期的な確認等、異常発見体制の整備                                   |
| 347 | 18 | 緊急時の電子メールサーバの停止                                        |
| 348 | 19 | 緊急時の社員への連絡(コンピュータウイルス警告の放送/送付)                         |
| 349 | 20 | OSの修正プログラムの適用(アップデートを含む)                               |
| 350 | 21 | 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)                         |
| 351 | 22 | プロバイダが提供する対策サービスの利用                                    |
| 352 | 23 | フィッシング防止のため、電子署名のついたメールを採用したり、自社 HP で真正性を確認できるツールを配布する |
| 353 | 24 | その他(具体的に書いて下さい。)                                       |
| 354 | 25 | 特に対策を講じていない                                            |

7 システム監査・情報セキュリティ監査について

Q40. 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)

|     |   |               |       |
|-----|---|---------------|-------|
| 356 | 1 | 実施した(実施中を含む)  | ⇒Q41へ |
|     | 2 | これから実施する予定がある | ⇒Q43へ |
|     | 3 | 実施しない         | ⇒Q42へ |

Q41. Q40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)

|     |    |                              |
|-----|----|------------------------------|
| 357 | 1  | システムに起因する事故・障害が未然に防止できた      |
| 358 | 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   |
| 359 | 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  |
| 360 | 4  | システムの信頼性向上対策のレベルが明らかになった     |
| 361 | 5  | システムの有効利用が促進された              |
| 362 | 6  | システムの効率性が確保できた               |
| 363 | 7  | 業務の継続性の確保が図られた               |
| 364 | 8  | 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 |
| 365 | 9  | その他(具体的に書いて下さい。)             |
| 366 | 10 | 効果は得られなかった                   |

Q42. Q40で「3」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)

|     |   |                                    |
|-----|---|------------------------------------|
| 367 | 1 | 経営者層が重要性を認識していないため                 |
| 368 | 2 | 予算が確保できない                          |
| 369 | 3 | 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 |
| 370 | 4 | システム監査の実施よりもシステム化推進そのものに力点がある      |
| 371 | 5 | システム監査の方法、制度、手続きなどが十分ではない          |
| 372 | 6 | 効果が明確でない                           |
| 373 | 7 | 適切なシステム監査人が見つからない                  |
| 374 | 8 | アウトソーシングしているため                     |
| 375 | 9 | その他(具体的に書いて下さい。)                   |

Q43. ①過去2年以内に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)

②実施したことがある／予定している場合、それは助言型監査ですか、保証型監査ですか。(複数回答)

| ①実施状況 |   |             | ②監査の種類    |           |       |
|-------|---|-------------|-----------|-----------|-------|
|       |   |             | ②-1.助言型監査 | ②-2.保証型監査 |       |
| 376   | 1 | 実施した        | 377 1     | 379 2     | ⇒Q45へ |
|       | 2 | これから行う予定がある | 378 1     | 380 2     |       |
|       | 3 | 実施しない       |           |           | ⇒Q44へ |

定義) 助言型監査: 監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールの改善を目的として、監査対象の情報セキュリティ上の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を行う監査の形態をいう。

保障型監査: 監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールが監査手続を実施した限りにおいて適切である旨(又は不適切である旨)を伝達する監査の形態をいう。

Q44. (Q43 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)

|     |   |                                            |
|-----|---|--------------------------------------------|
| 381 | 1 | 経営者層が重要性を認識していないため                         |
| 382 | 2 | 予算が確保できない                                  |
| 383 | 3 | 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     |
| 384 | 4 | 情報セキュリティ監査制度をよく知らない                        |
| 385 | 5 | 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                 |
| 386 | 6 | 効果が明確でない                                   |
| 387 | 7 | 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                 |
| 388 | 8 | 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 |
| 389 | 9 | その他(具体的に書いて下さい。)                           |

390

I

8 個人情報保護について

Q45. 「個人情報保護法」(平成 17 年 4 月 1 日完全施行)および、経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成 16 年 10 月公表)を知っていますか。

|     | 法律/ガイドライン                                                 | 内容を<br>知っている | 公表されたことを<br>知っている | 知らない |
|-----|-----------------------------------------------------------|--------------|-------------------|------|
| 391 | ①個人情報保護法(平成 17 年 4 月 1 日完全施行)                             | 1            | 2                 | 3    |
| 392 | ②個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン<br>(平成 16 年 10 月策定) | 1            | 2                 | 3    |

Q46. 貴事業体は個人情報取扱事業者(過去半年に 5,000 件以上の個人情報を取扱ったことがある)に該当しますか。  
なお、国の機関、地方公共団体、独立行政法人の場合は、「2」を選択して下さい。

|     |   |          |
|-----|---|----------|
| 393 | 1 | 該当する     |
|     | 2 | 該当しない(注) |
|     | 3 | わからない    |

(注: 国の機関、地方公共団体、独立行政法人を含む)

Q47. 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)

|     |    |                                                                                        |
|-----|----|----------------------------------------------------------------------------------------|
| 394 | 1  | 売買等契約の履行                                                                               |
| 395 | 2  | 顧客サポート                                                                                 |
| 396 | 3  | 代金等の回収                                                                                 |
| 397 | 4  | 情報提供                                                                                   |
| 398 | 5  | マーケティング                                                                                |
| 399 | 6  | 商品開発(アンケートを含む)                                                                         |
| 400 | 7  | 行政サービスの履行                                                                              |
| 401 | 8  | 委託(受託)処理                                                                               |
| 402 | 9  | 従業者情報(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)                                        |
| 403 | 10 | その他(具体的に書いて下さい。<br><br>例) 学校などの教育機関では在学学生・受験者・卒業生等の情報、 病院など医療機関では患者情報、 公共団体などでは住民情報など。 |

Q48. 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)

|     |    |                                            |             |
|-----|----|--------------------------------------------|-------------|
| 404 | 1  | 情報主体(当該個人)から直接収集                           | ⇒Q49へ       |
| 405 | 2  | 従業者から直接収集                                  |             |
| 406 | 3  | 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 |             |
| 407 | 4  | 名簿業者等から購入                                  | ⇒Q50またはQ51へ |
| 408 | 5  | グループ企業から入手                                 |             |
| 409 | 6  | 他社から提供を受ける                                 |             |
| 410 | 7  | 業務委託契約等に基づき預託される                           |             |
| 411 | 8  | 住民基本台帳から入手                                 |             |
| 412 | 9  | 新聞、雑誌等メディアからの収集                            |             |
| 413 | 10 | その他(具体的に書いて下さい。)                           |             |

Q49. Q48で「1」から「3」を回答した場合、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。(単一回答)

注)Q48で1～3を回答していない場合は、Q50 またはQ51 に進んで下さい。

|     |   |                                 |
|-----|---|---------------------------------|
| 414 | 1 | すべて同意を取っている                     |
|     | 2 | (第三者提供など)重要な変更の場合のみ、個別に同意を取っている |
|     | 3 | 何もしていない                         |
|     | 4 | わからない                           |

Q50. Q48で「4」～「6」を回答した場合、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。(複数回答)

注)Q48で「4」～「6」を回答していない場合は、Q51 に進んで下さい。

|     |   |                                           |
|-----|---|-------------------------------------------|
| 415 | 1 | 情報主体から利用に関し、改めて同意を取っている                   |
| 416 | 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 |
| 417 | 3 | 何もしていない                                   |

Q51. 個人情報の漏洩により深刻な被害を及ぼす事項をどのように認識していますか。(複数回答)

|     |   |                                  |
|-----|---|----------------------------------|
| 418 | 1 | 社会的な信用の低下(マスメディアに対するイメージダウンを含む)  |
| 419 | 2 | 親会社や関連会社側、企業グループの社会的信用の低下        |
| 420 | 3 | 顧客や取引先、官公庁からの取引での指名停止            |
| 421 | 4 | 情報が漏洩した情報主体からの損害賠償請求(裁判費用、期間を含む) |
| 422 | 5 | 契約違反による処分や訴訟                     |
| 423 | 6 | 株価下落や各付けの低下                      |
| 424 | 7 | その他(具体的に書いて下さい。)                 |
| 425 | 8 | わからない                            |
| 426 | 9 | 特に大きな影響はない                       |

427

J

Q52. 個人情報保護対策として、以下の対策を実施していますか。

|     | 対 策                                          | 個人情報保護<br>法施行以前か<br>ら実施している | 現在対策を<br>実施している | 今後新たに<br>実施を予定<br>している | 実施の予定<br>はない |
|-----|----------------------------------------------|-----------------------------|-----------------|------------------------|--------------|
| 428 | ①管理責任者を置く(保護体制(役割、責任、権限)を確立する                | 1                           | 2               | 3                      | 4            |
| 429 | ②個人情報保護に関する規程を定め運用する                         | 1                           | 2               | 3                      | 4            |
| 430 | ③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認定を受ける)運用する | 1                           | 2               | 3                      | 4            |
| 431 | ④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、定期的に教育する         | 1                           | 2               | 3                      | 4            |
| 432 | ⑤定期的に監査(内部監査／外部監査)を実施する                      | 1                           | 2               | 3                      | 4            |
| 433 | ⑥リスク分析を実施して必要な安全対策を構築する                      | 1                           | 2               | 3                      | 4            |
| 434 | ⑦苦情相談・処理窓口を設置し、個人からの問題意識を吸い上げ、対応する           | 1                           | 2               | 3                      | 4            |
| 435 | ⑧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る          | 1                           | 2               | 3                      | 4            |
| 436 | ⑨個人情報漏洩保険に加入する                               | 1                           | 2               | 3                      | 4            |

Q53. 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。(単一回答)

|     |   |                                      |
|-----|---|--------------------------------------|
| 437 | 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 | 対策を講じているが、リスクはあると認識している              |
|     | 4 | 何度かヒヤリ・ハツとした経験があり、リスクがあると認識している      |
|     | 5 | 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         |
|     | 6 | その他(具体的に書いて下さい。)                     |
|     | 7 | 特に認識していない                            |

Q54. 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)

|     |   |                       |
|-----|---|-----------------------|
| 438 | 1 | 機密保持義務                |
| 439 | 2 | 責任分担(漏洩事故発生時の損害賠償 等)  |
| 440 | 3 | 個人情報の適正な管理(廃棄、返却、授受等) |
| 441 | 4 | 目的外使用・再委託の制限          |
| 442 | 5 | 個人情報の取扱いに関する監査の実施     |
| 443 | 6 | その他(具体的に書いて下さい。)      |
| 444 | 7 | 外部委託を行っていない           |

Q55. プライバシーマーク制度を知っていますか。

|     |   |                |         |
|-----|---|----------------|---------|
| 445 | 1 | すでに認定されている     | ⇒Q56へ   |
|     | 2 | 認定申請中である       |         |
|     | 3 | 取得のための準備を行っている |         |
|     | 4 | 認定を受ける予定はない    | ⇒19ページへ |
|     | 5 | 知らない           |         |

Q56. Q55 で「1」～「3」を回答した場合、プライバシーマークの取得目的は何ですか。(複数回答)

|     |   |                                        |
|-----|---|----------------------------------------|
| 446 | 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、信頼性を確保できる |
| 447 | 2 | 取引先からの要請による(入札条件となっている)                |
| 448 | 3 | その他(具体的に書いて下さい。)                       |

449

K

○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

00

このアンケートは競輪の補助金を受けて実施するものです。

— 禁 無 断 転 載 —

平成18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 サンワ  
東京都千代田区飯田橋2丁目11番8号  
TEL 03(3265)1816





