特定非営利活動法人
NPO情報セキュリティフォーラム

情報セキュリティに関するアンケート調査

調査報告書

平成 18 年 3 月

特定非営利活動法人　NPO 情報セキュリティフォーラム

目　次

Ⅰ．調査概要

- 調査目的
  本調査は、企業における情報セキュリティ対策の現状、情報セキュリティに対する意識、情報セキュリティに関する問題点、情報セキュリティに関する企業の要望等を把握し、今後、地域に情報セキュリティを普及・推進・発展させていくための基礎資料とすることを目的とした。

- 調査名
  「情報セキュリティに関するアンケート調査」

- 調査方法
  郵送留置法

- 調査地域
  神奈川県内

- 調査対象
  県内の企業 2,000 社（無作為抽出）

- 実施期間
  平成 18 年 1 月 23 日から平成 18 年 2 月 10 日まで

- 回収数
  103 社（回収率 5.2%）

- 調査項目
  ①回答企業の概要
  ②企業におけるシステム利用環境
  ③システム環境における情報セキュリティ対策
  ④情報セキュリティ業務を担当する人材
  ⑤企業内での情報セキュリティに対する意識・教育
  ⑥個人情報保護に対する対策・体制
  ⑦情報セキュリティポリシー策定・評価制度
  ⑧情報セキュリティ監査の実施
  ⑨事業継続計画の策定（災害や障害への対応方法）
  ⑩情報セキュリティ対策の今後の取り組み

Ⅱ．調査結果

１．回答企業の概要

（１）回答企業の従業員数、業種、年間売上

従業員数は「1～9 人」が 26.2%、「10～29 人」と「50～99 人」が 19.4%の順に多く、合わせて 65.0%と 7 割近くを占めている。

業種は「製造」30.1%、「サービス」17.5%の順に多く、合わせて 47.6%と半数近くを占めており、「エネルギー」、「飲食」からの回答は得られていない。

年間売上は「5 億円以上～30 億円未満」が 37.9%と最も多く、次いで「1 億円以上～5 億円未満」18.4%となった。

設問 1(1) 貴社の従業員数をお答えください。

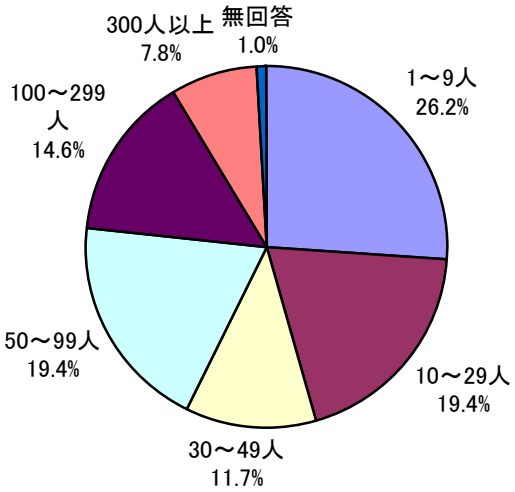

図　従業員数　(n=103)

設問 1(3) 貴社の年間売上をお答えください。

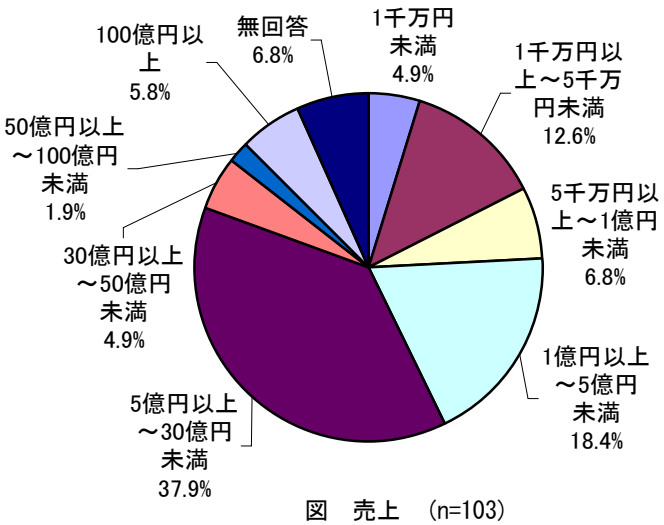

図　売上　(n=103)

設問 1(2) 貴社の業種をお答えください。

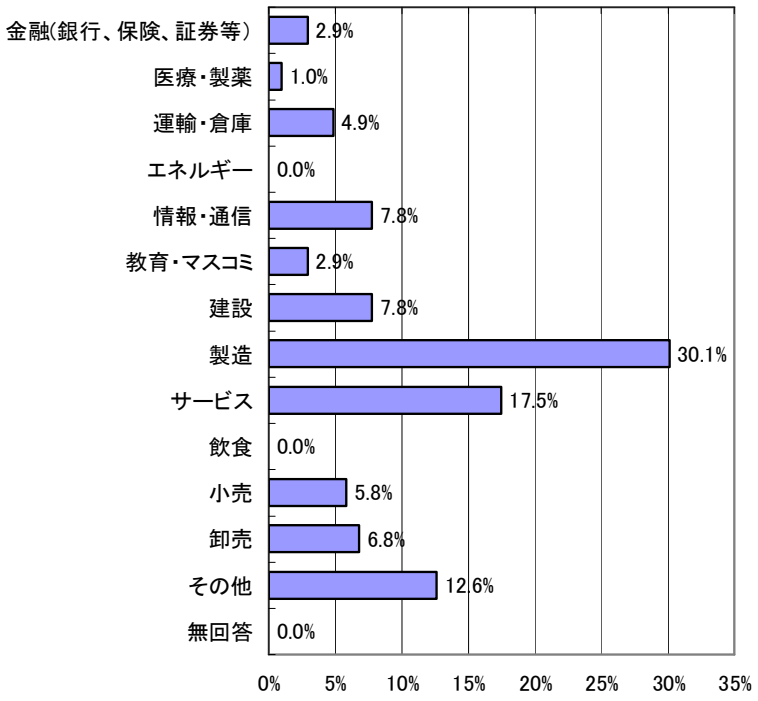

図　業種　(n=103)

２．企業におけるシステム利用環境

（１）パソコン・OS の利用状況

パソコンの利用状況については、「1 人 1 台以上で利用している」との回答が 54.4%と最も多く、次いで「数人で 1 台利用している」23.3%、「部課単位で数台利用している」19.4%となった。

社内で最も利用されている OS では、「WindowsXP」との回答が 64.1%と 6 割以上を占めているものの、OS のサポート期間の終了（2006 年 6 月）が予定されている「Windows98,Me」は 11.7%残っており、サポート期間終了後の問題が懸念される。

設問 2(1) 貴社のパソコンの利用状況についてお答えください。

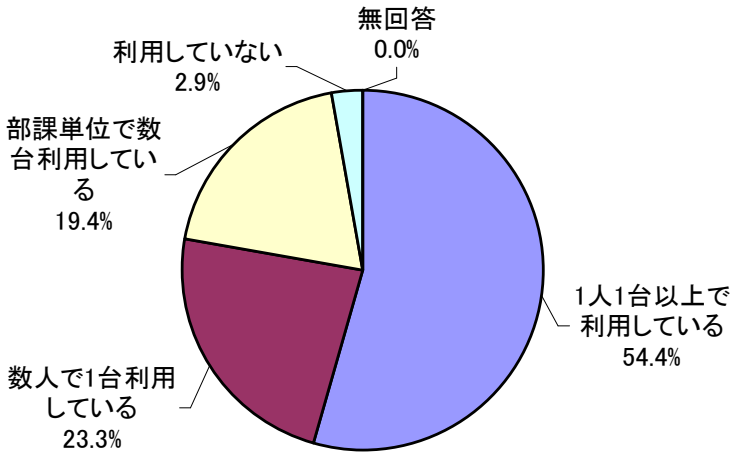

図　パソコンの利用　(n=103)

設問 2(2) 社内でもっとも利用されている OS についてお答えください。

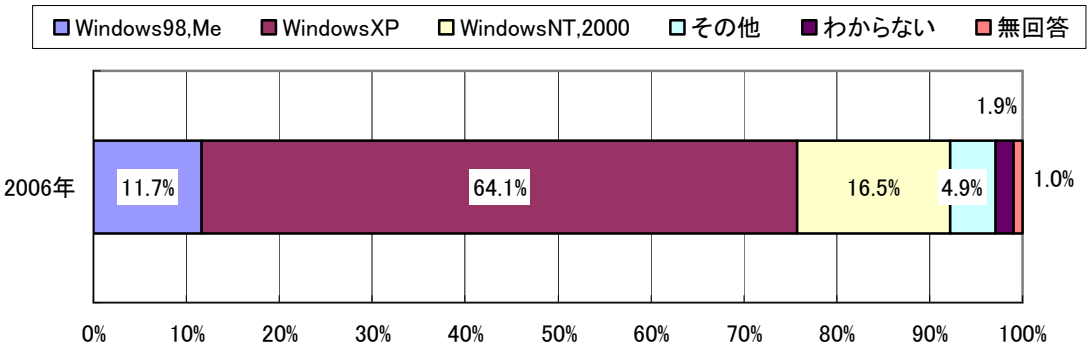

図　社内でもっとも利用されている OS　(n=103)

（２）社内 LAN の導入状況

LAN を導入している企業は全体の 81.5%で、企業内ネットワークの定着が見られる。

また、LAN にパソコンが接続されている企業は、「ほとんどすべてのパソコンが接続されている」、「半分程度のパソコンが接続されている」との回答を合わせると 78.6%となり、パソコン単体での利用から、ネットワークを利用して業務を行う企業が多くなっている。

設問 2(3) 社内 LAN の導入状況およびパソコンの接続状況についてお答えください。

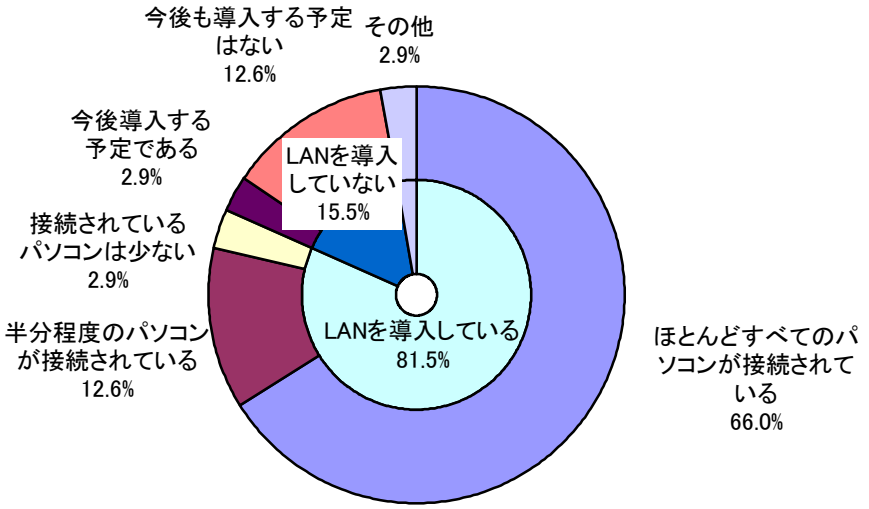

図　社内 LAN の導入状況　(n=103)

（３）企業におけるサーバの利用状況

Web サーバとメールサーバについては、「自社にサーバを設置して利用している」、「アウトソーシングでサーバを利用している」との回答を合わせると、それぞれ 66.0%、68.0%と利用率が高い。

Web サーバやメールサーバを利用していると回答した企業の利用形態としては、ホスティングサービスの充実などを背景に、Web サーバでは 35.9%、メールサーバでは 37.9%がアウトソーシングで利用しており、一方で秘匿性が高く、社内におくべきファイルサーバ（自社内 52.4%、アウトソーシング 2.9%）や DB サーバ（自社内 37.9%、アウトソーシング 0.0%）については自社での運用が圧倒的に多くなっている。

設問 2(4) 次の５つのサーバについて、貴社で利用されているサーバの管理方法をそれぞれお答えください。

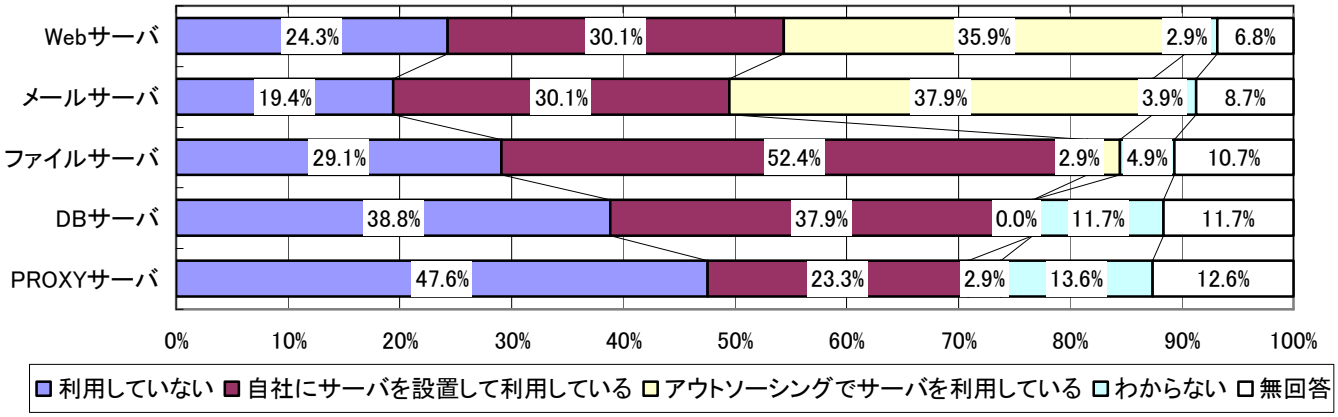

図　企業におけるサーバの利用状況　(n=103)

３．システム環境における情報セキュリティ対策

（１）パソコンの OS のアップデートチェックの状況

OS のアップデートは、「自動更新を利用している」との回答が 55.3%と最も多く、「担当者の指示により手動で更新している」、「個人の判断により手動で更新している」との回答を合わせた更新状況は 86.4%となり、一面ではアップデートへの意識が浸透しているとも言えるが、別の見方をすれば個人の判断による対応の遅れも懸念される結果となった。

設問 3(1)貴社が利用しているパソコンの OS のセキュリティパッチの適用は主としてどのように行っていますか。

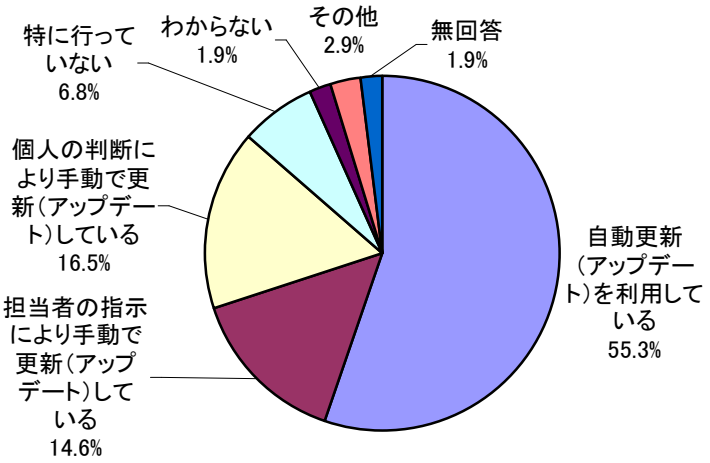

図　OS のアップデートチェック状況　(n=103)

（２）ウイルス対策ソフトの導入状況

ウイルス対策ソフトの導入状況は、「すべてのパソコンに導入している」との回答が 53.4%と半数を超えるものの、「あまり導入していない」、「導入していない」との回答を合わせると 18.4%となり、ウイルス感染の危険性が高い状態での運用が窺える結果となった。

設問 3(2)貴社のパソコンにウイルス対策ソフトウェアは導入されていますか。

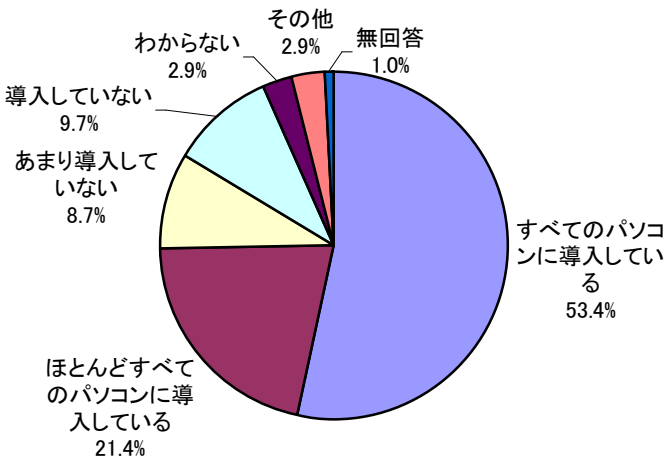

図　ウイルス対策ソフトの導入状況　(n=103)

（３）ウイルス対策ソフトのパターンファイルの更新方法

ウイルス対策ソフトのパターンファイルの更新方法については、「自動更新を利用している」との回答が 83.7%となり、「担当者の指示により手動で更新している」、「個人の判断により手動で更新している」を合わせると 100.0%更新をしている結果となった。

自動更新が８割を超えていることから、ウイルス対策ソフト導入後の適切な運用方法がほぼ浸透したとも言えるであろう。

設問 3(3) 貴社ではウイルス対策ソフトウェアのパターンファイルの更新（アップデート）は主としてどのように行っていますか。

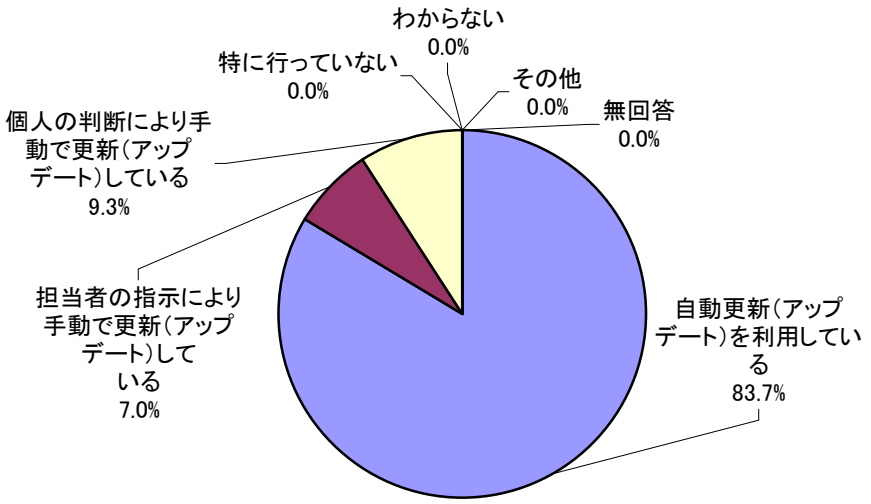

図　パターンファイルのアップデート方法　(n=86)

※設問 3(2) で以下の回答をした企業への設問	
1. すべてのパソコンに導入している	53.4%
2. ほとんどすべてのパソコンに導入している	21.4%
3. あまり導入していない	8.7%

（４）セキュリティ事故の発生状況と事故内容

過去１年間における情報セキュリティ関連の事故または事件が「ある」と回答した企業は 32.0%となった。

事故内容としては、「ウイルス・ワームの感染」が 25 票（回答企業の 75.8%）と圧倒的に多い。

設問 3(4) 貴社では過去１年間に情報セキュリティ関連の事故または事件が発生しましたか。
発生した場合には、事故または事件内容をお答えください。

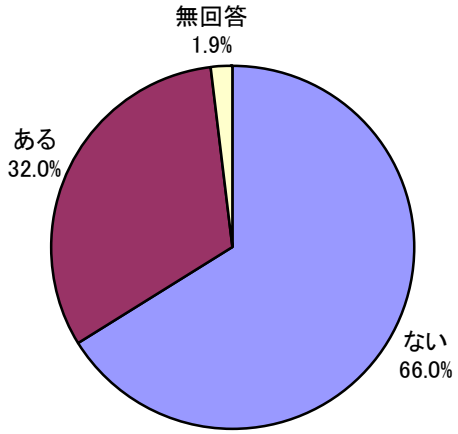

図　過去１年間のセキュリティ事故発生状況　(n=103)

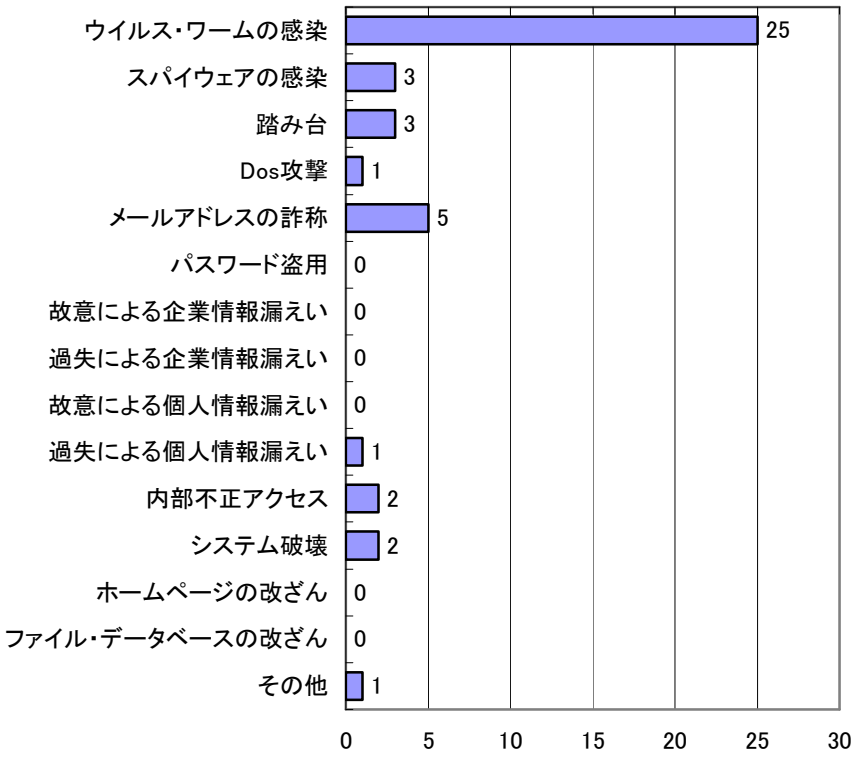

図　過去１年間の事故内容　(複数回答：43)　(n=33)

（５）導入している情報システム、サービスの実施利用状況

情報システム、サービスの実施状況については、「電子メール」の利用率が 85.4%と最も高く、次いで「Web による情報発信」が 53.4%となった。

一方、「VPN」、「無線 LAN」、「電子商取引」は 20～30%にとどまっている。

また、情報システム、サービスを実施していない理由については、総じて「必要がない」ためとの回答が多く、「導入するための予算化が難しい」との回答は少ない。

「電子メール」、「VPN」、「電子商取引」では「知識やノウハウがない」、「Web による情報発信」では「運用できる人材がいない」といった回答が多く、人材面での問題が窺える結果となった。

「無線 LAN」については、サービスの特性もあって「セキュリティ面が心配」が 28.2%を占めた。

設問 3(5) 貴社で実施している情報システム、サービスをお答えください。実施していない場合、その理由は何ですか。

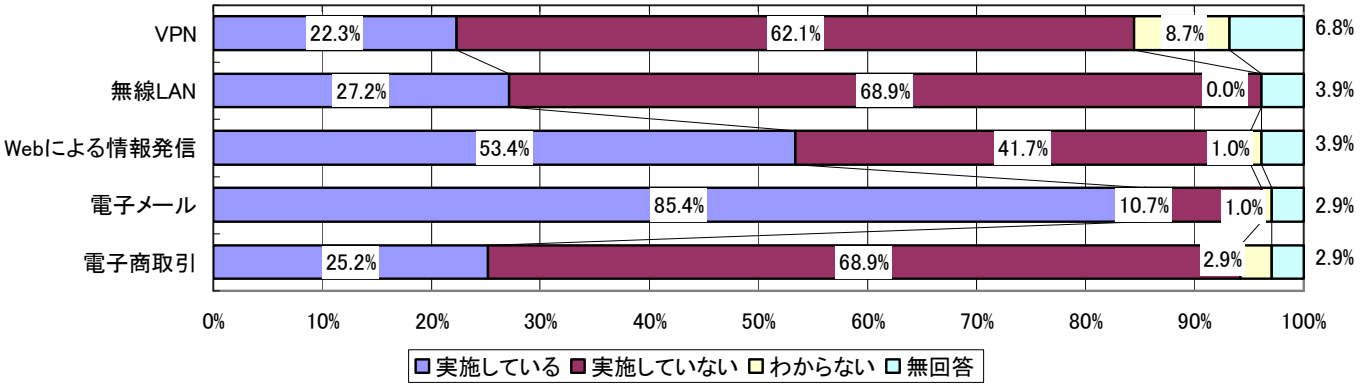

図　情報システム、サービスの実施利用状況　(n=103)

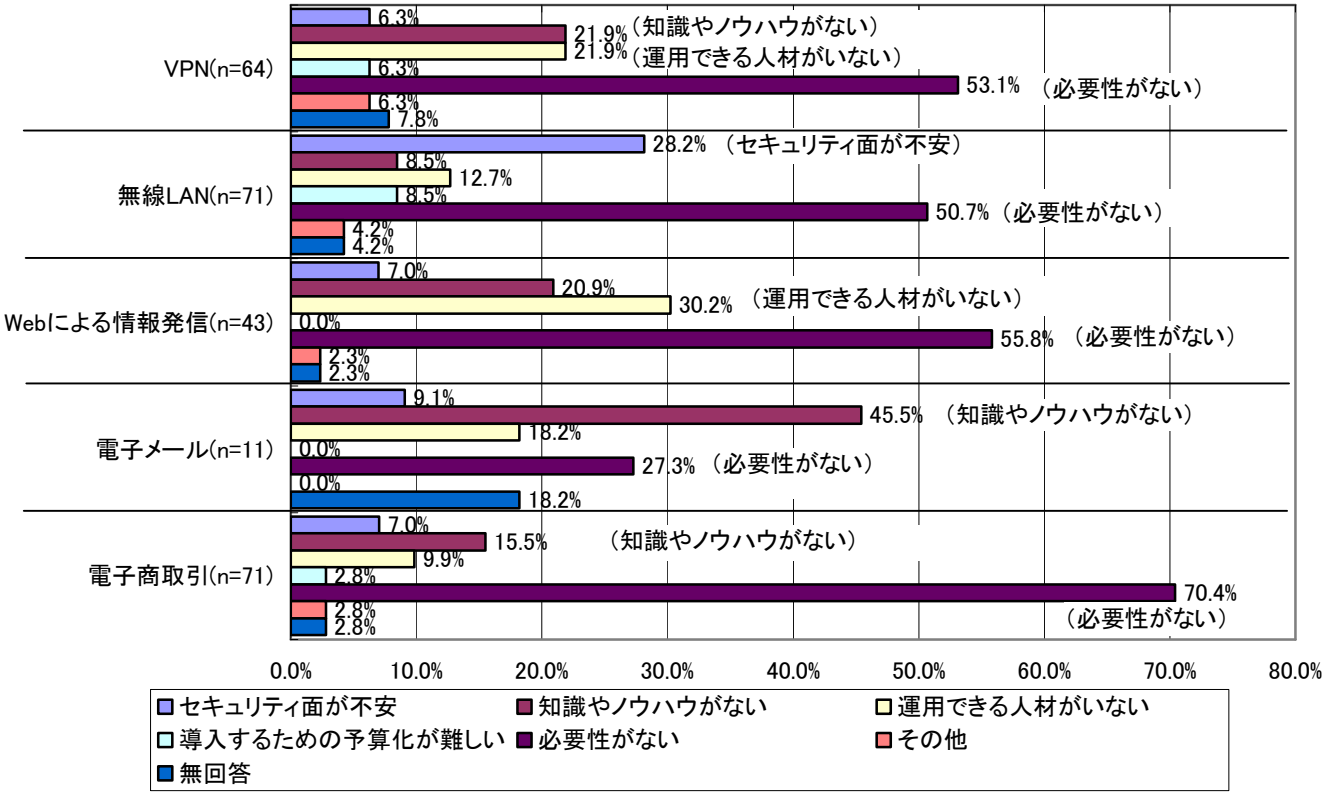

図　情報システム、サービスを実施利用していない理由(複数回答)

４．情報セキュリティ業務を担当する人材

（１）情報セキュリティ業務に対応する状況

情報セキュリティ業務について、「情報システム関連の担当者が兼任している」との回答が 36 票（回答企業の 35.0%）と多いが、「特に決まっていない」との回答も 34 票（回答企業の 33.0%）と次いで多い。

一方で、専門的な人材・企業が対応しているという回答は、「専門部署を設置して対応している」、「専門部署は設置していないが、専従の担当者がいる」、「一部または全部をアウトソーシングしている」を合わせた 34 票（回答企業の 33.0%）であり、全体の 3 分の 1 程度にすぎない結果となった。

設問 4(1) 貴社の情報セキュリティに対応する状況についてお答えください。（複数回答可）

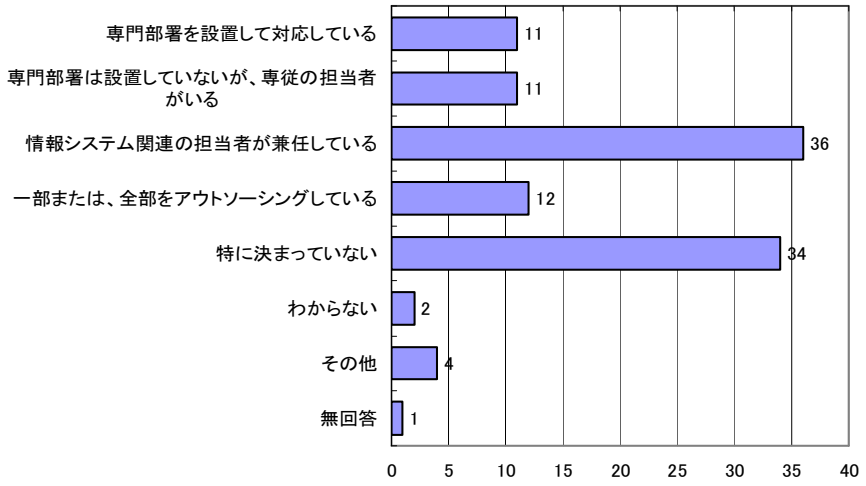

図　情報セキュリティ業務に対応する状況　（複数回答:111）（n=103）

（２）情報セキュリティに携わる人員数

情報セキュリティに携わる人員数は「1 人」との回答が 42 社（40.8%）で全回答の半数近くとなり最も多くなっている。

理想とする人員数についても「1 人」との回答が 31 社（30.1%）と多くなっているが、「2 人」または「3 人」の回答を合わせると 34 社（33.0%）となり、2 人以上の人員を必要と考えている企業も多いという結果になった。

「理想－現実の人員数差」は 0.99 人と 1 人近くとなり、企業におけるセキュリティ担当者の不足が推察される結果となった。

設問 4(2) 貴社では、情報セキュリティ業務に何人携わっていますか。また、情報セキュリティを維持するためには何人位必要と思いますか。具体的な人数をご記入ください。

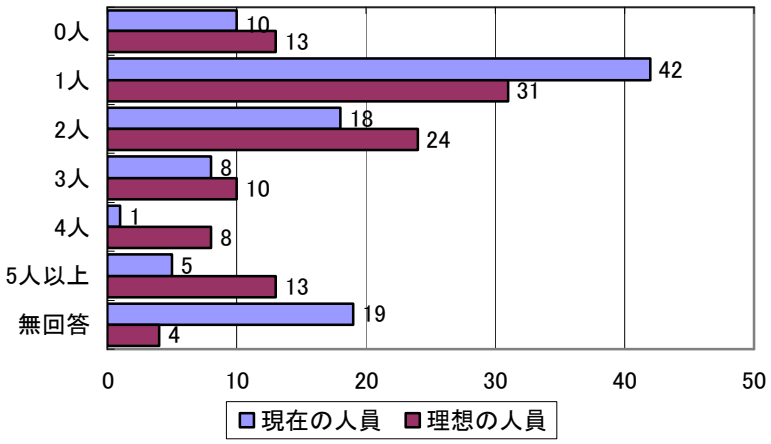

図　情報セキュリティに携わる人員数　(n=103)

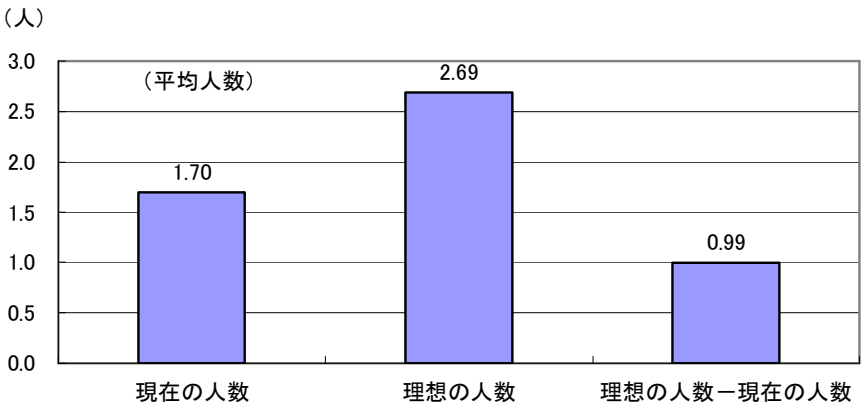

図　情報セキュリティに携わる人員数　（平均）

（３）情報セキュリティの人材に対する問題点

情報セキュリティに携わる人材に対する問題点として「社内に必要な知識を持つ人材が少ない」との回答が 60 票（回答企業の 58.3%）で最も多く、次いで「技術の変化が早く、担当者の知識を保つのが難しい」が 34 票（回答企業の 33.0%）、「人材の育成が難しい」が 30 票（回答企業の 29.1%）となり、社内において適切な人材を確保する難しさが窺える結果となった。

設問 4(3) 情報セキュリティに関する業務を担当する人材に関しての問題点は何ですか。(複数回答可)

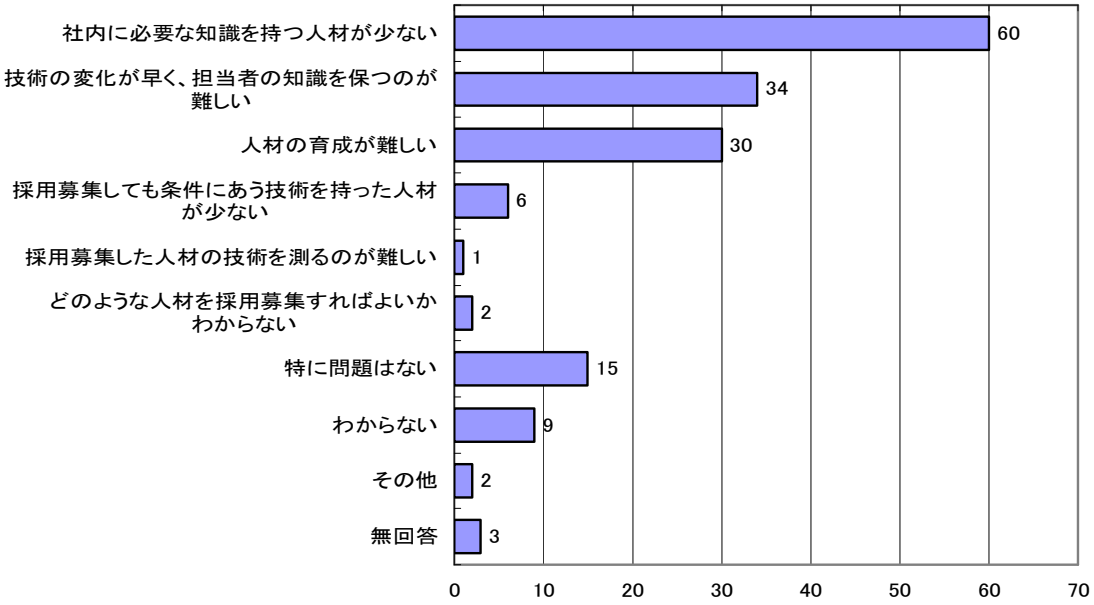

図　情報セキュリティの人材に対する問題点　（複数回答:162）　(n=103)

（４）情報セキュリティ担当者が持っていることが望ましい知識・技術

情報セキュリティの担当者が持つことが望ましい知識や技術については、「ネットワークセキュリティ技術」との回答が 59 票（回答企業の 57.3%）と最も多く、「OS セキュリティの知識」34 票（回答企業の 33.0%）、「セキュアサーバの構築技術」26 票（回答企業の 25.2%）と上位にきており、ネットワークの構築に必要な知識が重要と考えていることが窺える。

また、「セキュリティ事故の対応技術」との回答も 43 票（回答企業の 41.7%）と多く、事故が発生した場合に対処のできる人材を求める企業の姿も窺える。

(4)情報セキュリティに携わる社員が持っていることが望ましい知識・技術等について優先度の高いものを３つまでお答えください。

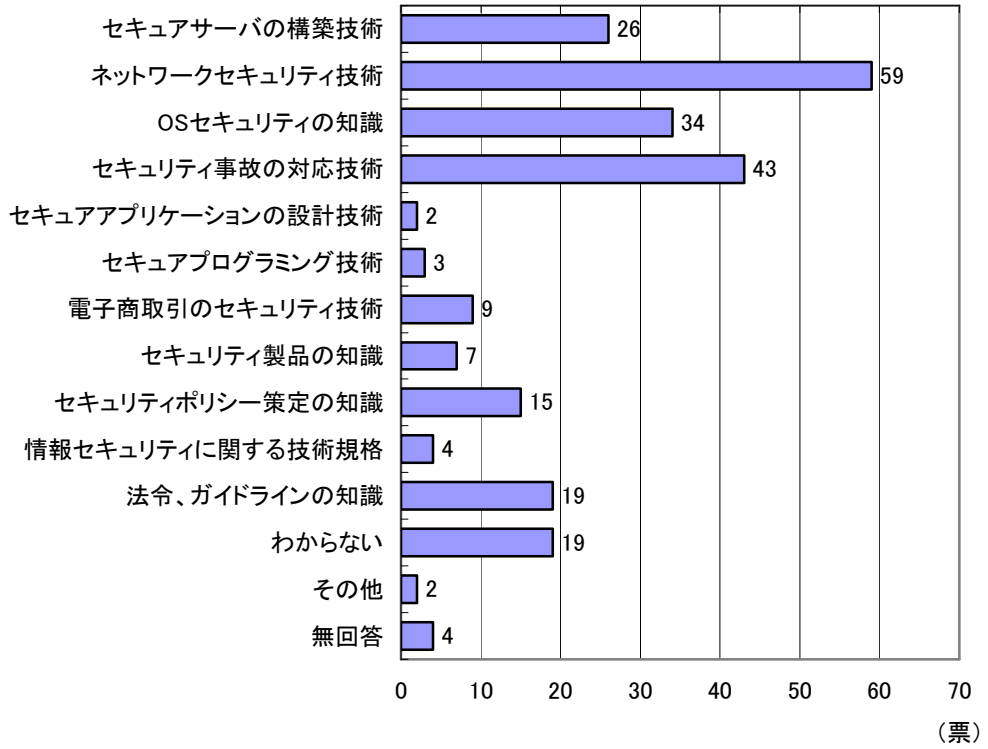

図　社員が持っていることが望ましい知識・技術等　（複数回答:246）　(n=103)

５．企業内での情報セキュリティに対する意識・教育

（１）社員の情報セキュリティに対する意識

情報セキュリティに対して「ほとんどすべての社員が意識している」との回答が 19.4%にとどまり、「あまり意識していない」との回答が 44.7%と約 5 割となった。情報セキュリティに対する意識の低さが窺われ、事故が懸念される結果となった。

設問 5(1) 貴社の社員は情報セキュリティに関して意識していますか。

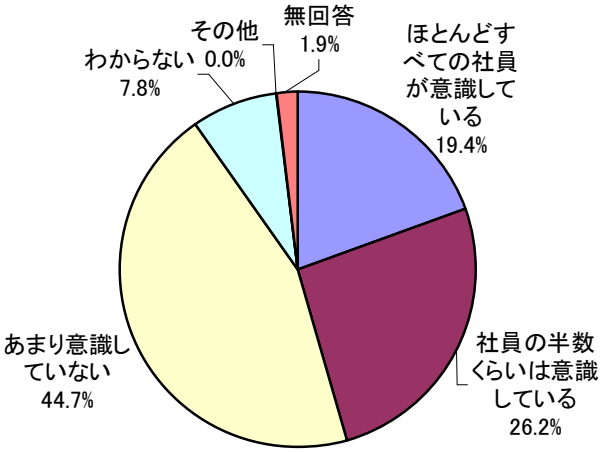

図　社員の情報セキュリティに関する意識　(n=103)

（２）社員への情報セキュリティの教育状況について

社員への教育状況は「特に行っていない」との回答が 68 票（回答企業の 66.0%）と圧倒的に多く、社員の情報セキュリティ意識の低さの一因とも考えられる結果となった。

設問 5(2) 貴社では、社員に対して情報セキュリティの教育を実施していますか。(複数回答可)

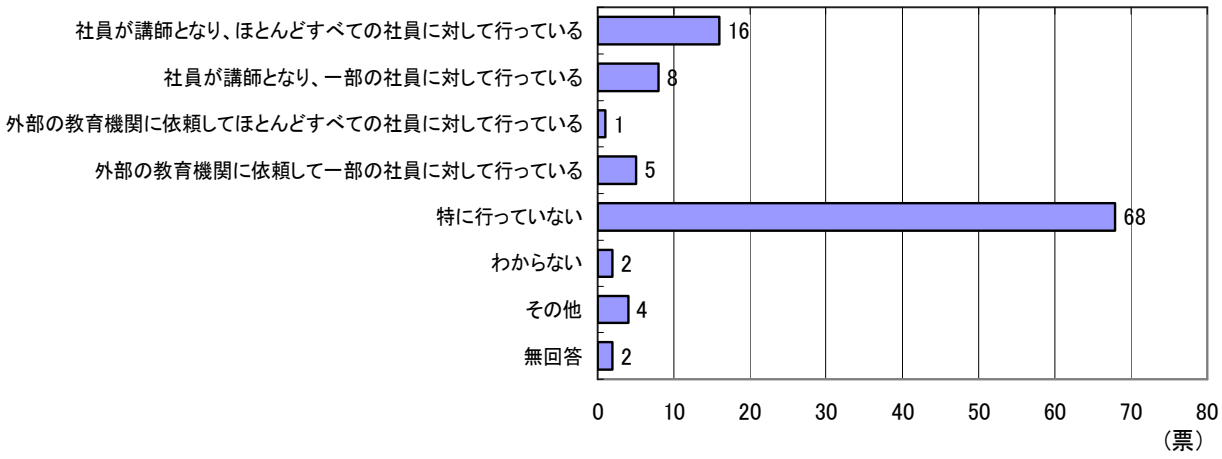

図　社員の情報セキュリティの教育状況　(複数回答:106)　(n=103)

（３）情報セキュリティ教育実施の問題点

情報セキュリティ教育実施にあたっての問題点は「ノウハウ・知識がない」との回答が 41 票（回答企業の 39.8%）と最も多く、また「教育を実施する適任者がいない」との回答が 39 票（回答企業の 37.9%）となっており、企業内でのノウハウ不足からの人材教育実施の難しさが窺える。

また、「教育する時間がない」との回答が 35 票（回答企業の 34.0%）あり、ノウハウ・人材不足に加え、業務時間内における教育時間の確保も課題となっている。

設問 5(3)情報セキュリティ教育に関しての問題点は何ですか。（複数回答可）

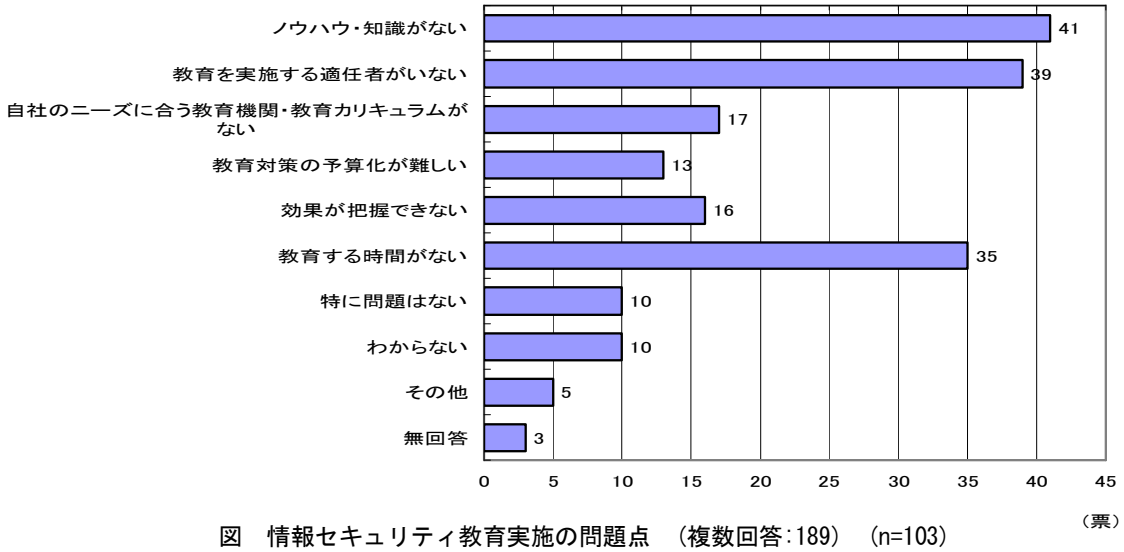

図　情報セキュリティ教育実施の問題点　（複数回答:189）（n=103）

６．個人情報保護に対する対策・体制

（１）個人情報保護法への対応状況

「個人情報の保護に関する法律」が施行（2005 年 4 月）されて約 1 年が経過しているものの、法に「対応済」との回答は 35.9%にすぎず、「法を把握している」との回答についても 6 割（60.2%）にとどまった。

設問 6(1) 貴社は個人情報保護法への対応を実施していますか。

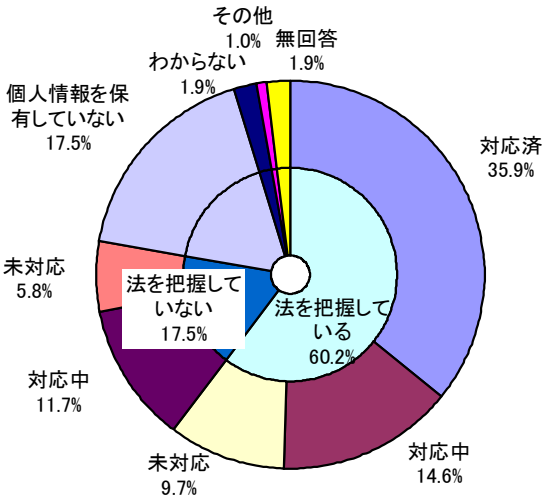

図　個人情報管理対策状況　(n=103)

（２）社内管理規定の策定状況

社内管理規定については、半数の企業が何らかの形で策定を済ませており、策定中の企業も含めて 7 割近くの企業が策定に取り組んでいる。

設問 6(2) 個人情報保護法に対応した社内管理規定を策定していますか。

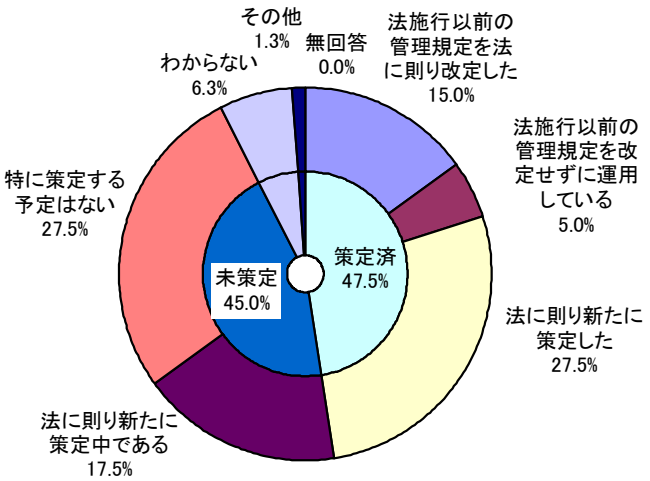

図　社内管理規定の策定状況　(n=80)

※設問 6(1) で以下の回答をした企業への設問	
1. 法を把握している、対応が完了している	35. 9%
2. 法を把握している、現在対応中である	14. 6%
3. 法を把握している、まだ対応していない	9. 7%
4. 法を把握しきれていない、現在対応中である	11. 7%
5. 法を把握しきれていない、まだ対応していない	5. 8%

（３）個人情報に関する認定マーク等の取得済、取得検討状況

個人情報保護に関する認定マークの取得等については、「特に取得したいマークはない」との回答が 47 票（回答企業の 58.8%）と最も多く、認定マーク等による個人情報保護の対策を考えている企業はまだ少ないことが窺える。

取得を検討している認定マークとしては「プライバシーマーク（P マーク）」が 13 票（回答企業の 16.3%）と多い。

設問 6(3) 貴社で、取得を検討している個人情報保護に関する認定マークをお答えください。また、取得している認定マーク（取得中を含む）がある場合、お答えください。（複数回答可）

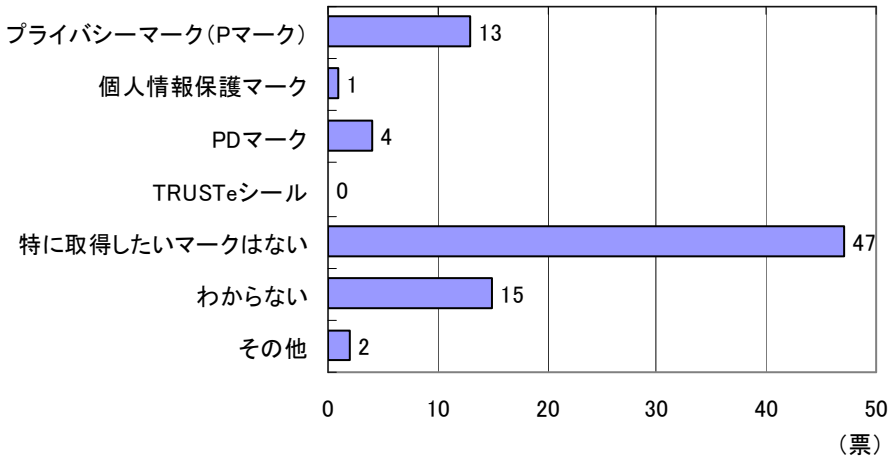

図　取得したい認定マーク　（複数回答:82）　(n=80)

※設問 6(1) で以下の回答をした企業への設問	
1. 法を把握している、対応が完了している	35.9%
2. 法を把握している、現在対応中である	14.6%
3. 法を把握している、まだ対応していない	9.7%
4. 法を把握しきれていない、現在対応中である	11.7%
5. 法を把握しきれていない、まだ対応していない	5.8%

7．情報セキュリティポリシー策定・評価制度

（1）情報セキュリティポリシー

情報セキュリティポリシーについては、「策定していない。今後も策定する予定はない」との回答が 35 票（34.0%）と高い数値になっているが、「策定済み」、「現在策定中」、「策定していないが、今後策定する予定はある」を合わせた策定を望むとする回答は 53 票（51.5%）と全体の約半数を占めている。

情報セキュリティポリシーを策定する際の問題点としては、「人材に余裕がない」38 票（回答企業の 36.9%）、「知識やノウハウがない」34 票（回答企業の 33.0%）の回答が多い。

設問 7(1)情報セキュリティポリシーについてお伺いします。
①貴社では、情報セキュリティポリシーを策定されていますか。

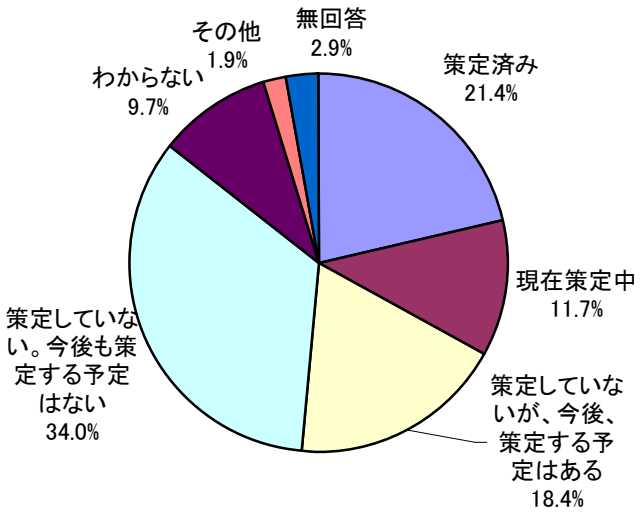

図　セキュリティポリシーの策定状況　(n=103)

②情報セキュリティポリシーを策定する際の問題点は何ですか。（複数回答可）

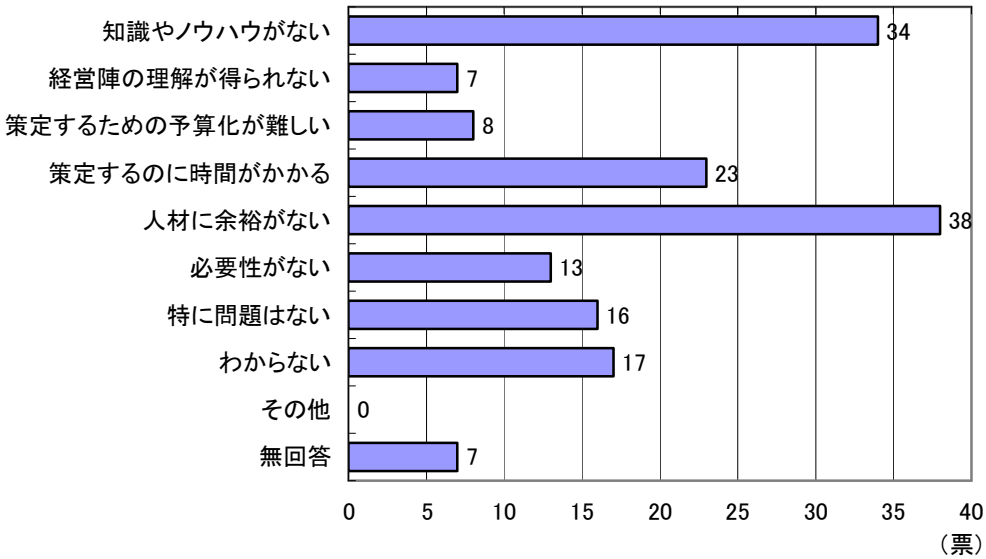

図　情報セキュリティポリシーを策定する際の問題点　（複数回答：163）　(n=103)

（２）ISMS 適合性評価制度

①企業での ISMS 適合性評価制度の認証取得状況

ISMS 適合性評価制度の認証については、「取得済み」、「現在申請中」との回答がそれぞれ 1.9%にとどまった。

意向としても「取得していないが、今後、取得を予定している」との回答が 9.7%であり、「取得していない。今後も取得予定はない」が 40.8%、「ISMS 適合性評価制度を知らない」が 25.2%となった。

設問 7(2)「情報セキュリティマネジメントシステム(ISMS)適合性評価制度」についてお伺いします。
①貴社では、ISMS 適合性評価制度の認証を取得されていますか。

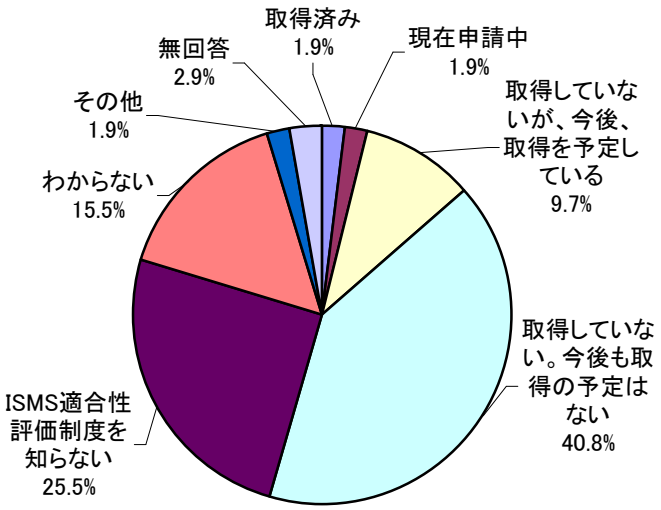

図　ISMS 適合性評価制度の認証取得状況　(n=103)

（２）ISMS 適合性評価制度

②ISMS 適合性評価制度のメリットと問題点

ISMS 適合性評価制度の認証取得のメリットとして、「顧客満足の向上・信頼度向上」との回答が 10 票（回答企業の 71.4%）と最も多く、次いで「社員のセキュリティ意識の向上」の 9 票（回答企業の 64.3%）となった。取得によって、顧客満足・信頼性や社員のセキュリティに関する意識の向上を期待する企業が多い。

問題点については、「人材に余裕がない」との回答が 9 票（回答企業の 36.0%）、次いで「知識やノウハウがない」、「認証取得に時間がかかる」の 7 票（回答企業の 28.0%）となった。

②ISMS 適合性評価制度の認証を取得することのメリットは何ですか。（複数回答可）

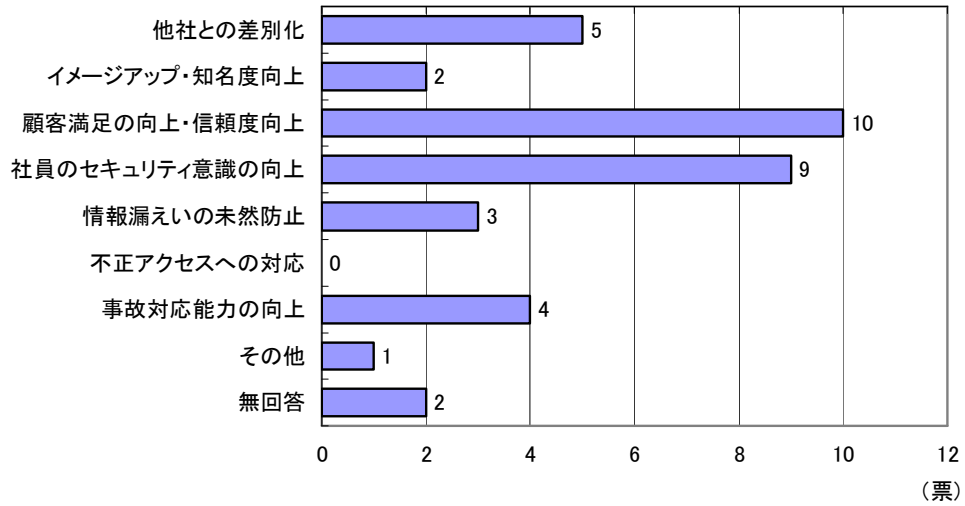

図　ISMS 適合性評価制度の認証取得のメリット　（複数回答:50）　(n=14)

※設問 7(2)①で以下の回答をした企業への設問

1. 取得済み	1.9%
2. 現在申請中	1.9%
3. 取得していないが、今後取得を予定している	9.7%

③ISMS 適合性評価制度の認証を取得する際の問題点は何ですか。（複数回答可）

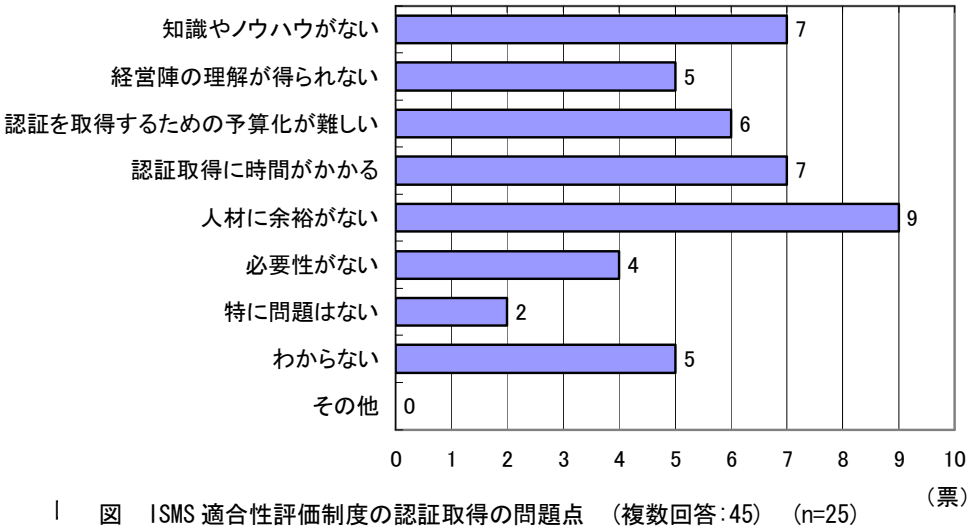

図　ISMS 適合性評価制度の認証取得の問題点　（複数回答:45）　(n=25)

８．情報セキュリティ監査の実施

（１）情報セキュリティ監査の実施状況

情報セキュリティ監査を「実施している」との回答は 8.7%となり、「現在計画中」3.9%と「いずれ実施したい」17.5%と実施意向を含めても、30.1%にとどまった。一方、「実施する予定はない」との回答が 58.3%と約 6 割となった。

設問 8(1) 貴社では、情報セキュリティ監査を実施していますか。

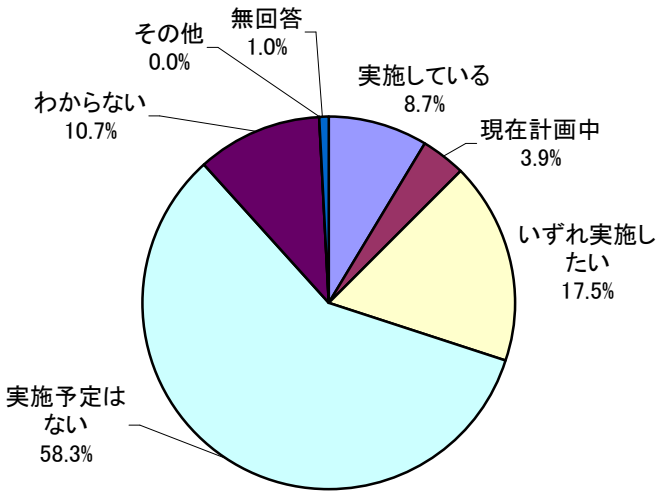

図　セキュリティ監査実施状況　(n=103)

（２）情報セキュリティ監査の実施方法

回答総数は 14 票と少ないが、情報セキュリティ監査の実施方法は、外部や監査部門など、監査を主とした部署や企業であることが窺える。

設問 8(2) 貴社での監査の実施方法は何ですか。(複数回答可)

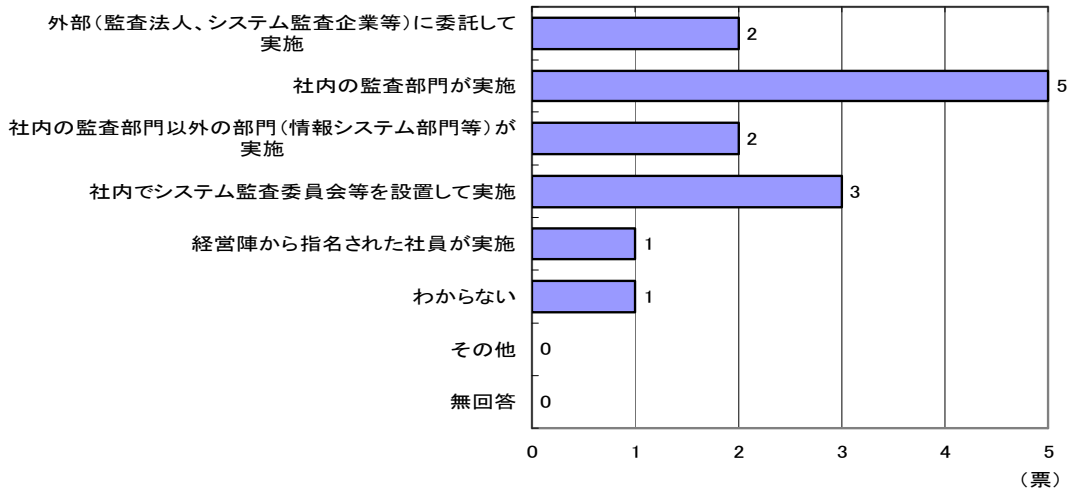

図　情報セキュリティ監査の実施方法　(複数回答:14)　(n=13)

※設問 8(1) で以下の回答をした企業への設問

1. 実施している	8. 7%
2. 現在計画中	3. 9%

（３）情報セキュリティ監査実施の問題点

情報セキュリティ監査を実施する場合の問題点では、「知識やノウハウがない」との回答が 13 票(回答企業の 37.1%)と最も多く、「人材に余裕がない」との回答も 11 票(回答企業の 31.4%)となった。

設問 8(3)情報セキュリティ監査を実施する場合の問題点は何ですか。(複数回答可)

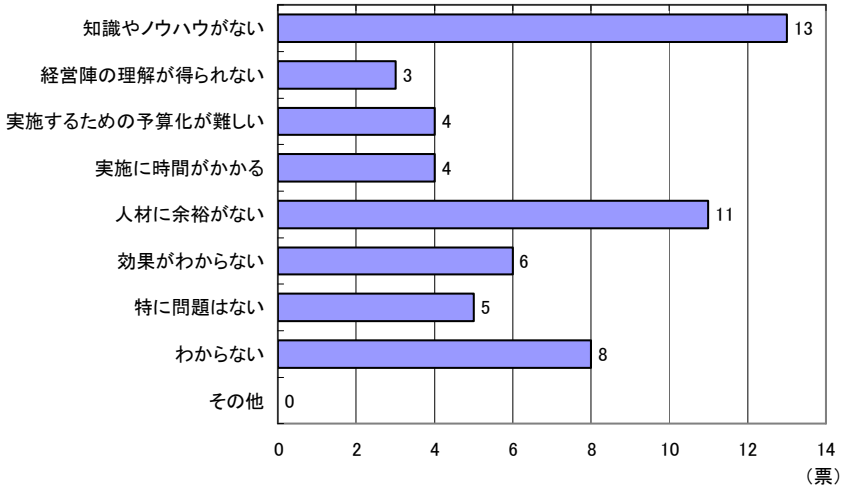

図　情報セキュリティ監査を実施する場合の問題点　(複数回答:54)　(n=35)

９．事業継続計画の策定（災害や障害への対応方法）

（１）災害や情報システムの障害発生時の事業を継続するための対応策

事業継続のための対応策については、「対応策を策定し、いつでも対応できる状態になっている」との回答は 13.6%にとどまったものの、「対応策を策定中である」、「策定していないが、今後、策定する予定である」の回答を合わせると、51.5%と半数を超える結果となった。

設問 9(1) 貴社では、災害や情報システムの障害などが発生した場合、事業を継続するための対応策を策定していますか。

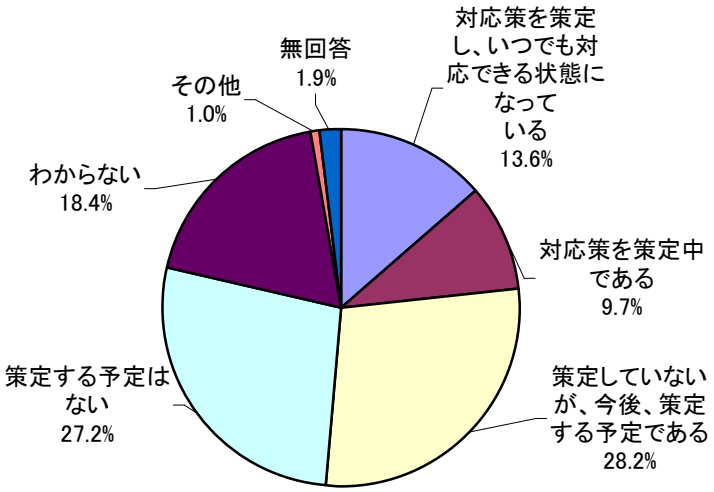

図　事業継続のための対応策の策定状況　(n=103)

（２）策定した対応策の見直し

策定した対応策は、定期的な見直しを行っていく必要がある。回答総数は 14 票と少ないが、策定された対応策は適宜見直しが行われている。

設問 9(2) 貴社では、策定した対策の見直しを行っていますか。

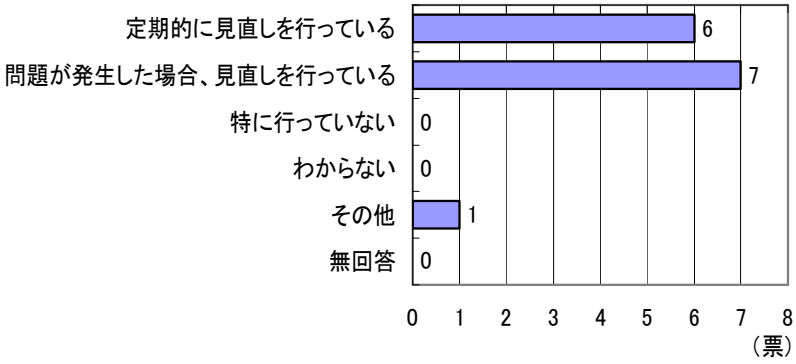

図　策定した対策の見直し　(n=14)

※設問 9(1) で以下の回答をした企業への設問
1. 対応策を策定し、いつでも対応できる状態になっている　13.6%

（３）対応策を策定する上での問題点

「対応策を策定する予定はない」と回答した企業に対して質問した策定しない理由は、「知識やノウハウがない」、「必要性を感じない」が 10 票(回答企業の 35.7%)、次いで「人材に余裕がない」が 9 票(回答企業の 32.1%)となった。

正しい知識やノウハウを持った人材育成の啓発普及が必要と言える。

設問 9(3)策定しない理由は何ですか。(複数回答可)

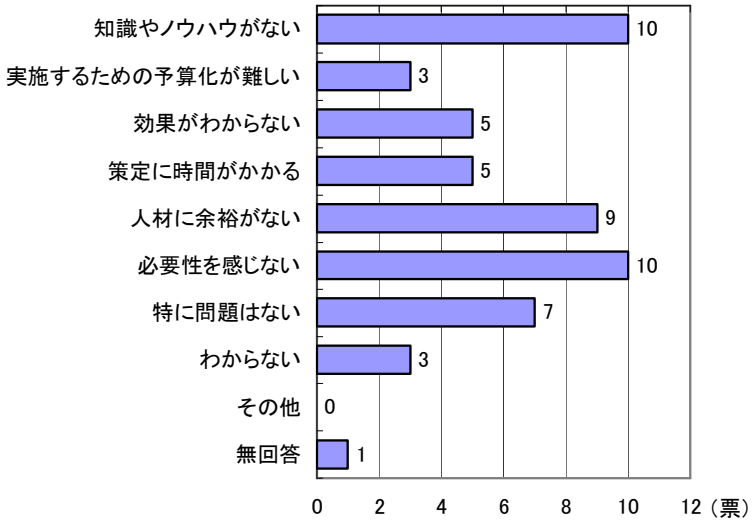

図　事業継続のための対応策策定上の問題点　(複数回答:53)　(n=28)

※設問 9(1)で以下の回答をした企業への設問
4. 策定する予定はない　27.2%

１０．情報セキュリティ対策の今後の取り組み

（１）今後実施や導入を検討する情報セキュリティ対策

今後の情報セキュリティ対策については､｢社員教育の実施｣との回答が 41 票(回答企業の 39.8%)と最も多く、次いで「データ・電子メール暗号化」30 票（回答企業の 29.1%)、「ウイルス対策ソフトウェアの導入」23 票（回答企業の 22.3%）となり、現状の対策不足の認識と合致する結果となった。

設問 10(1) 今後、実施や導入を検討しているセキュリティ対策について優先度の高いものを 3 つまでお答えください。

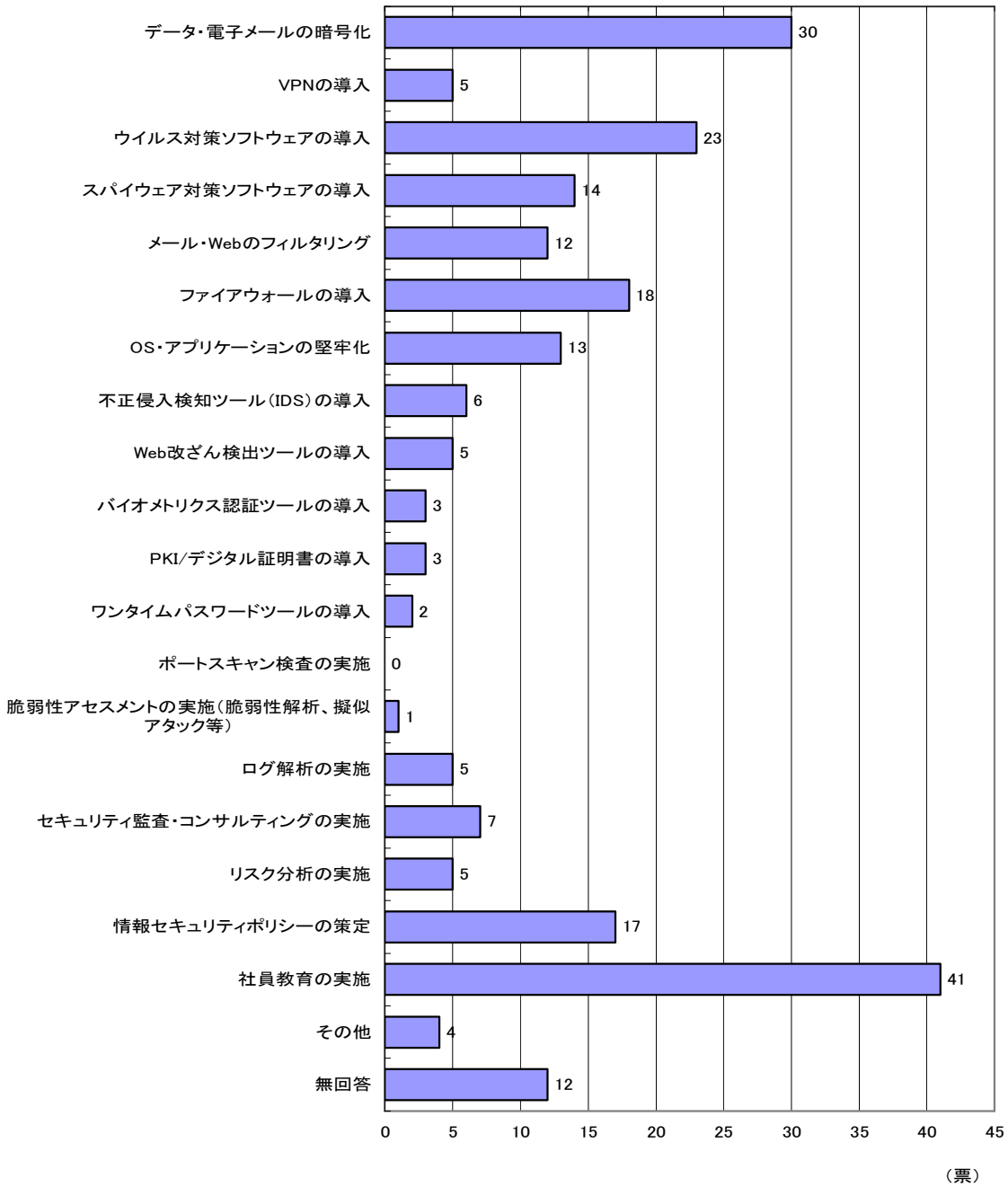

図　導入を検討しているセキュリティ対策　(複数回答:226)　(n=103)

（２）情報セキュリティに対する投資の重要度

情報セキュリティに対する投資については、「他の投資案件と比べて最重要案件と考えている」との回答が 6.8%にとどまり、逆に「他の投資案件と比べて重要度は低いと考えている」が 42.7%と半数近くとなった。

設問 10(2) 貴社の情報セキュリティに対する投資についてのお考えをお答えください。

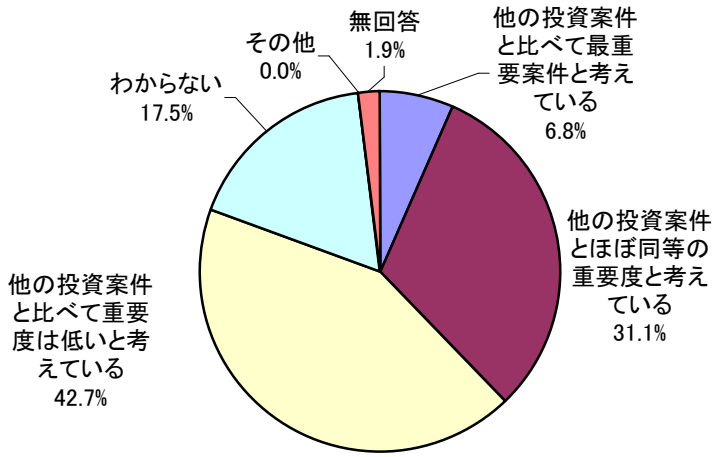

図　情報セキュリティに対する投資についての考え　(n=103)

（３）情報セキュリティに対する投資額

2006 年度の情報セキュリティ投資額については、「2005 年度とほぼ同等の計画」との回答が 43.7%と最も多く、「2005 年度と比較して増やす計画」との回答は 6.8%にとどまった。

なお、「わからない」との回答も 41.7%となっている。

設問 10(3) 貴社の 2006 年度の情報セキュリティ投資額は、2005 年度と比較してどのようになる見通しかお答えください。

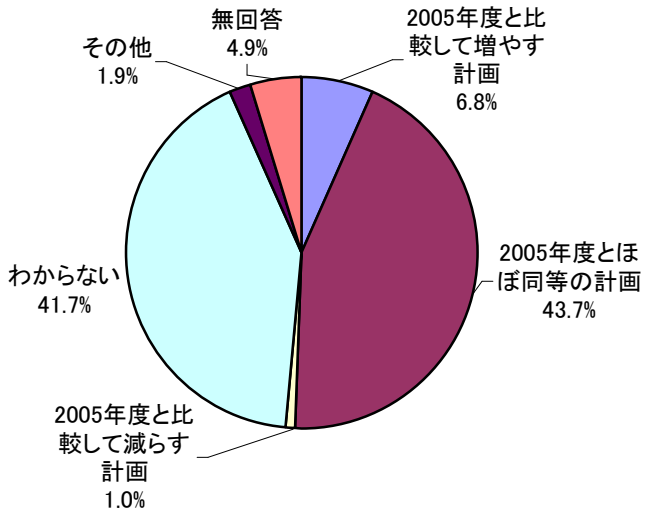

図　情報セキュリティに対する投資額の見通し　(n=103)

（４）自治体に希望する情報セキュリティに関する施策

自治体に希望する施策として「侵害行為を取り締まる法制度の整備」との回答が 39 票（回答企業の 37.9%）と最も多い。また、「機器・ソフトウェア購入への助成」33 票（回答企業の 32.0%）、「セキュリティサービス利用への助成」25 票（回答企業の 24.3%）との回答も多く、費用面での施策を求める企業が多い。

「社員教育」や「講習会・セミナー開催」など、教育機会の提供を望む企業も多くなっている。

設問 10(4)情報セキュリティに関して、自治体に行ってほしい施策はありますか。（複数回答可）

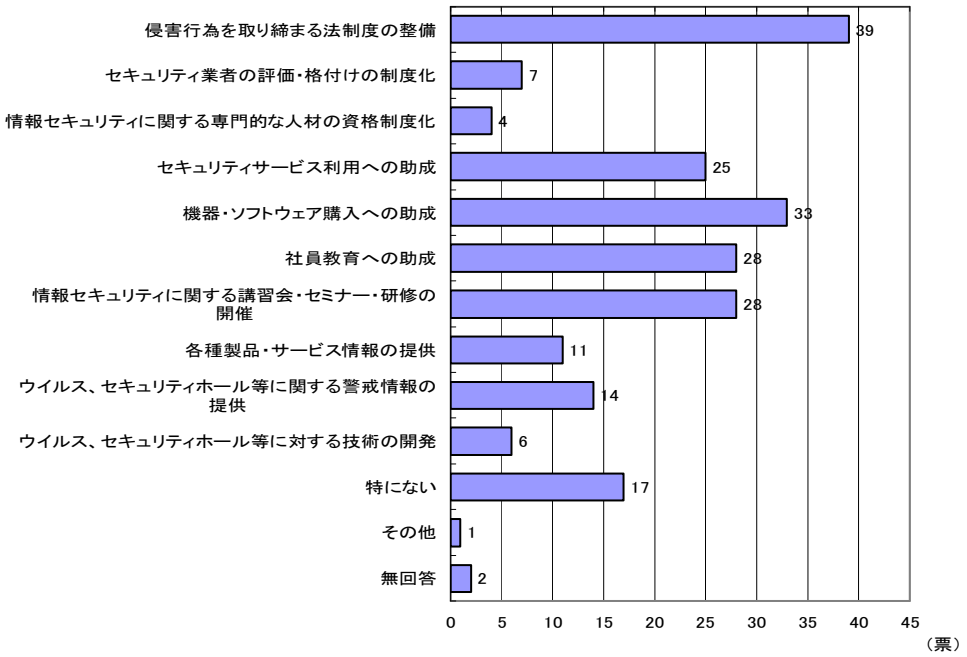

図　自治体に行ってほしい施策　（複数回答:215）　(n=103)

（５）情報セキュリティフォーラムの活動

本フォーラムの活動については、「企業向けの情報セキュリティの普及活動」34 票（回答企業の 33.0%）と最も多く、次いで「情報セキュリティに関する情報提供」33 票（回答企業の 32.0%）、「情報セキュリティ技術者を育成するセミナー活動」31 票（回答企業の 30.1%）となった。

自治体に望む施策同様、教育機会の提供を望む企業も多くなっている。

設問 10(5)本フォーラムでは以下のような活動を予定しております。興味をお持ちの活動をお答えください。（複数回答可）

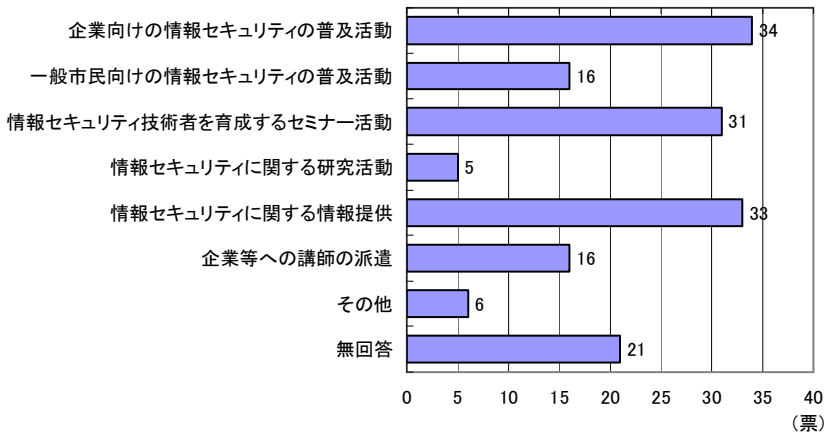

図　情報セキュリティフォーラムの活動　（複数回答:162）　(n=103)

（６）関心のある情報セキュリティセミナー

セミナーについては、「情報セキュリティ全般的な基礎知識」との回答が 46 票（回答企業の 44.7%）と最も多く、全般的な情報セキュリティ情報を求めていることが窺える。また、次に「ネットワークセキュリティ」30 票（回答企業の 29.1%）、「コンピュータウイルス対策」22 票（回答企業の 21.4%）とあり、技術面でのセキュリティの対策方法についての関心は高いことが窺える。

設問 10(6) 本フォーラムでは今後、情報セキュリティに関連する各種セミナーを実施していく予定です。企画する際の参考にさせていただきたいので、関心のあるテーマをお答えください。（複数回答可）

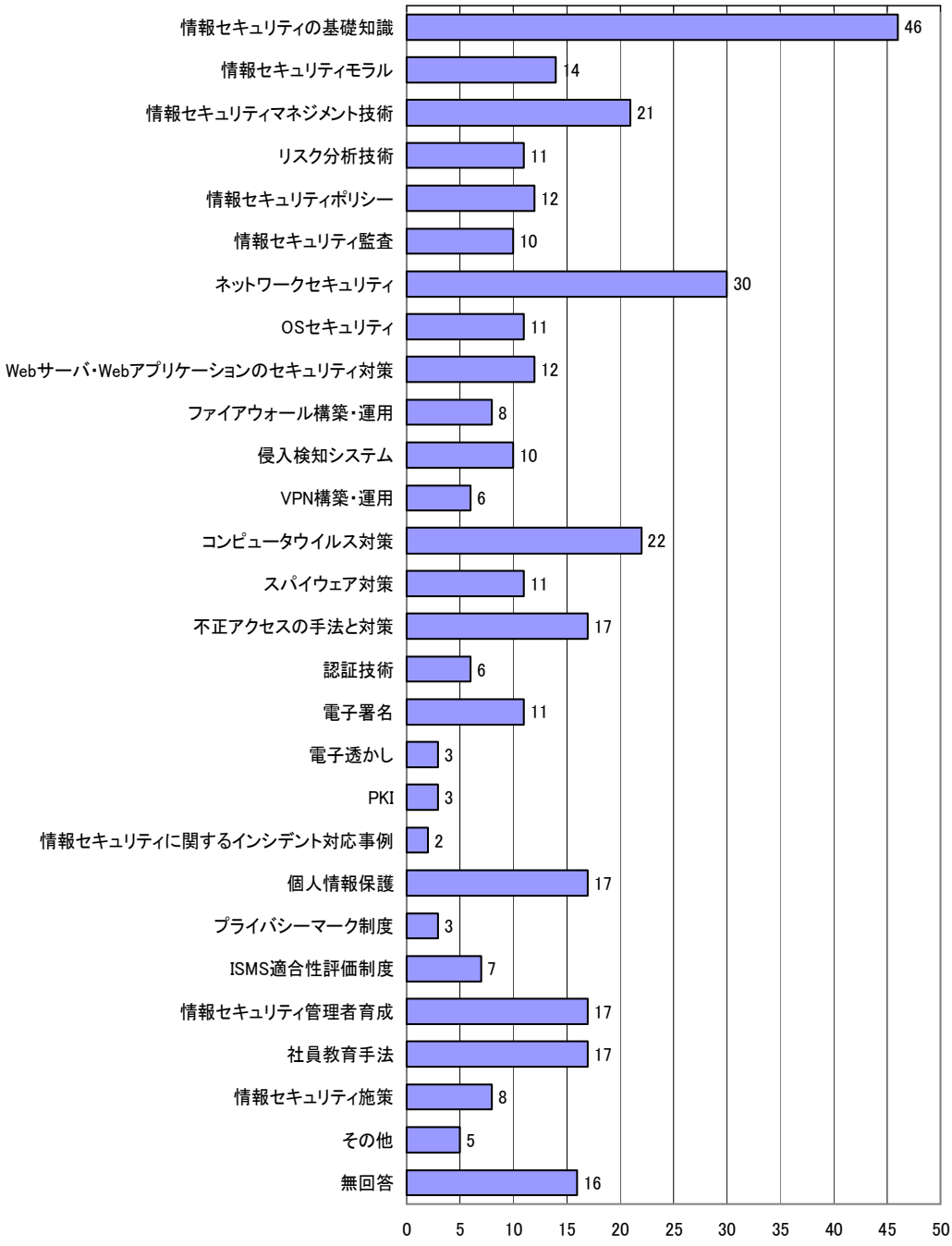

図　関心のある情報セキュリティセミナー　（複数回答:356）　(n=103)

情報セキュリティに関するアンケート調査
調査票

特定非営利活動法人　NPO 情報セキュリティフォーラム

この調査は、神奈川県内の企業における企業情報、個人情報などをはじめとする情報資産を守るための情報セキュリティ対策の現況を把握し、集計結果を公表することにより安全で安心できる社会を目指した情報セキュリティ対策の取組みを促進するために実施いたします。また今後情報セキュリティの分野で本フォーラムが実施する事業の基礎資料とさせていただきます。

なお、回答いただきました内容は、集計結果のみを公表することとし、ご記入者が特定できる個票レベルでの公表はありません。

ご多忙のところ誠に恐縮ではございますが、ご協力くださいますようよろしくお願いいたします。

本調査票については、大変お手数をおかけいたしますが、2006 年 2 月 10 日（金）までに同封の返信用封筒に本調査票を入れて投函してください。

集計した調査結果は 3 月中旬ごろに、本フォーラム Web サイト上(http://www.isef.or.jp/)で公表いたします。

【ご回答をお願いしたい方】

本調査は以下の部門の方にご回答をお願いいたします。

①情報セキュリティ部門又は担当

②①に準ずる部門又は担当（例えば、情報部門、総務部門など）

【返送先・お問合わせ先】
〒221－0835　横浜市神奈川区鶴屋町2-17 相鉄岩崎学園ビル
特定非営利活動法人NPO情報セキュリティフォーラム　（担当：今野、増田）
TEL(045)311-8777　FAX(045)311-8747
URL http://www.isef.or.jp/　E-Mail:isef@isef.or.jp

差し支えない範囲で以下の項目をご記入ください。

企業名：	
所在地：〒	
電話番号：	記入者の部署名および氏名：
FAX：	
E-Mail：	

※ご記入いただきました回答者情報（個人情報）は、アンケート結果発送のためのみに利用いたします。

※ご回答いただける設問について該当する番号に○印をお付けください

設問１　貴社の概要についてお伺いします。

(1) 貴社の従業員数をお答えください。

1. 1～9人　2. 10～29人　3. 30～49人
4. 50～99人　5. 100～299人　6. 300人以上

(2) 貴社の業種をお答えください。

1. 金融(銀行、保険、証券等)　2. 医療・製薬　3. 運輸・倉庫
4. エネルギー　5. 情報・通信　6. 教育・マスコミ
7. 建設　8. 製造　9. サービス
10. 飲食　11. 小売　12. 卸売
13. その他(　　)

(3) 貴社の年間売上をお答えください。

1. 1千万円未満　2. 1千万円以上～5千万円未満　3. 5千万円以上～1億円未満
4. 1億円以上～5億円未満　5. 5億円以上～30億円未満　6. 30億円以上～50億円未満
7. 50億円以上～100億円未満　8. 100億円以上

設問２　貴社のシステム環境についてお伺いします。

(1) 貴社のパソコンの利用状況についてお答えください。

1. 1人1台以上で利用している　2. 数人で1台利用している
3. 部課単位で数台利用している　4. 利用していない

(2) 社内でもっとも利用されている OS についてお答えください。

1. Windows98,Me　2. WindowsXP　3. WindowsNT,2000
4. UNIX　5. Linux　6. わからない
7. その他(　　)

(3) 社内 LAN の導入状況およびパソコンの接続状況についてお答えください。

1. LAN が導入されていて、ほとんどすべてのパソコンがこれに接続されている
2. LAN が導入されていて、半分程度のパソコンがこれに接続されている
3. LAN は導入されているが、接続されているパソコンは少ない
4. LAN は導入していないが、今後、導入する予定である
5. LAN は導入していない。今後も導入する予定はない
6. わからない
7. その他(　　)

(4) ①～⑤のサーバについて、貴社で利用されているサーバの管理方法をそれぞれお答えください。

	利用していない	自社にｻｰﾊﾞを設置して利用している	ｱｳﾄｿｰｼﾝｸﾞでｻｰﾊﾞを利用してる	わからない
①Web サーバ	1	2	3	4
②メールサーバ	1	2	3	4
③ファイルサーバ	1	2	3	4
④DB サーバ	1	2	3	4
⑤PROXY サーバ	1	2	3	4

設問３　貴社のシステム環境における情報セキュリティ対策についてお伺いします。

(1) 貴社が利用しているパソコンの OS のセキュリティパッチの適用は主としてどのように行っていますか。
1. 自動更新(アップデート)を利用している　2. 担当者の指示により手動で更新(アップデート)している
3. 個人の判断により手動で更新(アップデート)している　4. 特に行っていない
5. わからない
6. その他(　　)

(2) 貴社のパソコンにウイルス対策ソフトウェアは導入されていますか。
1. すべてのパソコンに導入している
2. ほとんどすべてのパソコンに導入している　} (3)をお答えください
3. あまり導入していない
4. 導入していない
5. わからない
6. その他(　　)

(2)で 1～3 とお答えいただいた方にお伺いします。

(3) 貴社ではウイルス対策ソフトウェアのパターンファイルの更新(アップデート)は主としてどのように行っていますか。
1. 自動更新(アップデート)を利用している　2. 担当者の指示により手動で更新(アップデート)している
3. 個人の判断により手動で更新(アップデート)している　4. 特に行っていない
5. わからない
6. その他(　　)

(4) 貴社では過去1年間に情報セキュリティ関連の事故または事件が発生しましたか。発生した場合には、事故または事件内容をお答えください。
1. ない
2. ある(複数回答可)

A. ウイルス・ワームの感染　B. スパイウェアの感染　C. 踏み台（不正アクセスや迷惑メールの中継点として利用されること）
D. DoS 攻撃（サーバに負荷をかけてサービス提供をできなくしてしまう攻撃）　E. メールアドレスの詐称　F. パスワード盗用
G. 故意による企業情報漏えい　H. 過失による企業情報漏えい　I. 故意による個人情報漏えい
J. 過失による個人情報漏えい　K. 内部不正アクセス　L. システム破壊
M. ホームページの改ざん　N. ファイル・データベースの改ざん
O. その他(　　)

(5) 貴社で実施している情報システム、サービスをお答えください。実施していない場合、その理由は何ですか。

	実施している	実施していない	わからない	【実施していない理由(複数回答可)】 セキュリティ面が不安	知識やノウハウがない	運用できる人材がいない	導入するための予算化が難しい	必要性がない	その他
＜記入例＞	1	(2)	3	(A)	B	C	(D)	E	F
①VPN(ﾊﾞｰﾁｬﾙﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ)	1	2	3	A	B	C	D	E	F
②無線 LAN	1	2	3	A	B	C	D	E	F
③Web による情報配信	1	2	3	A	B	C	D	E	F
④電子メール	1	2	3	A	B	C	D	E	F
⑤電子商取引	1	2	3	A	B	C	D	E	F

設問４　情報セキュリティを担当する人材についてお伺いします。

(1) 貴社の情報セキュリティに対応する状況についてお答えください。(複数回答可)

1. 専門部署を設置して対応している
2. 専門部署は設置していないが、専従の担当者がいる
3. 情報システム関連の担当者が兼任している
4. 一部または、全部をアウトソーシングしている
5. 特に決まっていない
6. わからない
7. その他(　　)

(2) 貴社では、情報セキュリティ業務に何人携わっていますか。また、情報セキュリティを維持するためには何人位必要と思いますか。具体的な人数をご記入ください。

・現在の人数　　人　　・理想とする人数　　人

(3) 情報セキュリティに関する業務を担当する人材に関しての問題点は何ですか。(複数回答可)

1. 社内に必要な知識を持つ人材が少ない
2. 技術の変化が早く、担当者の知識を保つのが難しい
3. 人材の育成が難しい
4. 採用募集しても条件にあう技術を持った人材が少ない
5. 採用募集した人材の技術を測るのが難しい
6. どのような人材を採用募集すればよいかわからない
7. 特に問題はない
8. わからない
9. その他(　　)

(4) 情報セキュリティに携わる社員が持っていることが望ましい知識・技術等について優先度の高いものを3つまでお答えください。

1. セキュアサーバの構築技術
2. ネットワークセキュリティ技術
3. OS セキュリティの知識
4. セキュリティ事故の対応技術
5. セキュアアプリケーションの設計技術
6. セキュアプログラミング技術
7. 電子商取引のセキュリティ技術
8. セキュリティ製品の知識
9. セキュリティポリシー策定の知識
10. 情報セキュリティに関連する技術規格
11. 法令、ガイドラインの知識
12. わからない
13. その他(　　)

設問５　社内での情報セキュリティに関する社員の意識・教育についてお伺いします。

(1) 貴社の社員は情報セキュリティに関して意識していますか。

1. ほとんどすべての社員が意識している
2. 社員の半数位は意識している
3. あまり意識していない
4. わからない
5. その他(　　)

(2) 貴社では、社員に対して情報セキュリティの教育を実施していますか。(複数回答可)

1. 社員が講師となり、ほとんどすべての社員に対して行っている
2. 社員が講師となり、一部の社員に対して行っている
3. 外部の教育機関に依頼してほとんどすべての社員に対して行っている
4. 外部の教育機関に依頼して一部の社員に対して行っている
5. 特に行っていない
6. わからない
7. その他(　　)

(3)　情報セキュリティ教育に関しての問題点は何ですか。(複数回答可)

1. ノウハウ・知識がない
2. 教育を実施する適任者がいない
3. 自社のニーズに合う教育機関・教育カリキュラムがない
4. 教育対策の予算化が難しい
5. 効果が把握できない
6. 教育する時間がない
7. 特に問題はない
8. わからない
9. その他(　　)

設問６　個人情報に関する対策、体制等についてお伺いします。

(1)　貴社は個人情報保護法への対応を実施していますか。

1. 個人情報保護法の内容を把握し、一通りの対応が完了している
2. 個人情報保護法の内容を把握しているが、現在対応中である
3. 個人情報保護法の内容を把握しているが、まだ対応していない
4. 個人情報保護法の内容を把握しきれていないが、現在対応中である
5. 個人情報保護法の内容を把握しきれていないため、まだ対応していない
6. 個人情報を保有していないので、対応の必要はない
7. わからない
8. その他(　　)

(2)～(3)を
お答えください。

(1)で 1～5 とお答えいただいた方は、以下の(2)～(3)をお答えください

(2)　個人情報保護法に対応した社内管理規定を策定していますか。

1. 法施行以前の管理規定を法に則り改定した
2. 法施行以前の管理規定を改定せずに運用している
3. 法に則り新たに策定した
4. 法に則り新たに策定中である
5. 特に策定する予定はない
6. わからない
7. その他(　　)

(3)　貴社で、取得を検討している個人情報保護に関する認定マークをお答えください。また、取得している認定マーク(取得中を含む)がある場合、お答えください。(複数回答可)

1. プライバシーマーク　(P マーク)
2. 個人情報保護マーク　(通信事業関連企業向けの認定)
　※個人情報保護マーク制度は平成 17 年 9 月で終了
3. PD マーク
　(神奈川県が実施する個人情報取扱業務登録制度)
4. TRUSTeシール
　(オンライン、ネットワーク上のプライバシー保護に関する認定)
5. 特に取得したいマークはない
6. わからない
7. その他(　　)

設問７　情報セキュリティポリシー、評価制度についてお伺いします。

(1)　情報セキュリティポリシーについてお伺いします。

※　情報セキュリティポリシーとは、事業者が所有する情報資産の情報セキュリティ対策について、情報セキュリティの基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定としてとりまとめたもの。

①貴社では、情報セキュリティポリシーを策定されていますか。

1. 策定済み
2. 現在策定中
3. 策定していないが、今後、策定する予定はある
4. 策定していない。今後も策定する予定はない
5. わからない
6. その他(　　)

②情報セキュリティポリシーを策定する際の問題点は何ですか。(複数回答可)

1. 知識やノウハウがない
2. 経営陣の理解が得られない
3. 策定するための予算化が難しい
4. 策定するのに時間がかかる
5. 人材に余裕がない
6. 必要性がない
7. 特に問題はない
8. わからない
9. その他(　　)

(2) 「情報セキュリティマネジメントシステム(ISMS)適合性評価制度」についてお伺いします。

※ ISMS 適合性評価制度は、事業者の情報セキュリティマネジメントシステムが財団法人日本情報処理開発協会の定める ISMS 認証基準に準拠していることを認定する制度のこと。

① 貴社では、ISMS 適合性評価制度の認証を取得されていますか。

1. 取得済み
2. 現在申請中
3. 取得していないが、今後、取得を予定している

→ ②をお答えください

4. 取得していない。今後も取得予定はない
5. ISMS 適合性評価制度を知らない
6. わからない
7. その他(　　)

①で 1～3 とお答えいただいた方にお伺いします。

②ISMS 適合性評価制度の認証を取得することのメリットは何ですか。(複数回答可)

1. 他社との差別化
2. イメージアップ・知名度向上
3. 顧客満足の向上・信頼度向上
4. 社員のセキュリティ意識の向上
5. 情報漏えいの未然防止
6. 不正アクセスへの対応
7. 事故対応能力の向上
8. その他(　　)

③ISMS 適合性評価制度の認証を取得する際の問題点は何ですか。(複数回答可)

1. 知識やノウハウがない
2. 経営陣の理解が得られない
3. 認証を取得するための予算化が難しい
4. 認証取得に時間がかかる
5. 人材に余裕がない
6. 必要性がない
7. 特に問題はない
8. わからない
9. その他(　　)

設問８　情報セキュリティ監査についてお伺いします。

(1) 貴社では、情報セキュリティ監査を実施していますか。

1. 実施している
2. 現在計画中

→ (2)をお答えください

3. いずれ実施したい
4. 実施予定はない
5. わからない
6. その他(　　)

(1)で 1, 2 とお答えいただいた方にお伺いします。

(2) 貴社での監査の実施方法は何ですか。(複数回答可)

1. 外部(監査法人、システム監査企業等)に委託して実施
2. 社内の監査部門が実施
3. 社内の監査部門以外の部門(情報システム部門等)が実施
4. 社内でシステム監査委員会等を設置して実施
5. 経営陣から指名された社員が実施
6. わからない
7. その他(　　)

(3) 情報セキュリティ監査を実施する場合の問題点は何ですか。(複数回答可)

1. 知識やノウハウがない
2. 経営陣の理解が得られない
3. 実施するための予算化が難しい
4. 実施に時間がかかる
5. 人材に余裕がない
6. 効果がわからない
7. 特に問題はない
8. わからない
9. その他(　　)

設問９　災害や障害への対応方法についてお伺いします。

(1) 貴社では、災害や情報システムの障害などが発生した場合、事業を継続するための対応策を策定していますか。

1. 対応策を策定し、いつでも対応できる状態になっている → (2)をお答えください
2. 対応策を策定中である
3. 策定していないが、今後、策定する予定である
4. 策定する予定はない → (3)をお答えください
5. わからない
6. その他(　　)

(1)で 1 とお答えいただいた方にお伺いします。

(2) 貴社では、策定した対策の見直しを行っていますか。

1. 定期的に見直しを行っている
2. 問題が発生した場合、見直しを行っている
3. 特に行っていない
4. わからない
5. その他(　　)

(1)で 4 とお答えいただいた方にお伺いします。

(3) 策定しない理由は何ですか。(複数回答可)

1. 知識やノウハウがない
2. 実施するための予算化が難しい
3. 効果がわからない
4. 策定に時間がかかる
5. 人材に余裕がない
6. 必要性を感じない
7. 特に問題はない
8. わからない
9. その他(　　)

設問１０　情報セキュリティ対策の今後の取り組みについてお伺いします。

(1) 今後、実施や導入を検討しているセキュリティ対策について**優先度の高いものを 3 つまで**お答えください。

1. データ・電子メールの暗号化
2. VPN の導入
3. ウイルス対策ソフトウェアの導入
4. スパイウェア対策ソフトウェアの導入
5. メール・Web のフィルタリング
6. ファイアウォールの導入
7. OS・アプリケーションの堅牢化
8. 不正侵入検知ツール(IDS)の導入
9. Web 改ざん検出ツールの導入
10. バイオメトリクス認証ツールの導入
11. PKI/デジタル証明書の導入
12. ワンタイムパスワードツールの導入
13. ポートスキャン検査の実施
14. 脆弱性アセスメントの実施(脆弱性解析、擬似アタック等)
15. ログ解析の実施
16. セキュリティ監査・コンサルティングの実施
17. リスク分析の実施
18. 情報セキュリティポリシーの策定
19. 社員教育の実施
20. その他(　　)

(2) 貴社の情報セキュリティに対する投資についてのお考えをお答えください。

1. 他の投資案件と比べて最重要案件と考えている
2. 他の投資案件とほぼ同等の重要度と考えている
3. 他の投資案件と比べて重要度は低いと考えている
4. わからない
5. その他(　　)

(3) 貴社の 2006 年度の情報セキュリティ投資額は、2005 年度と比較してどのようになる見通しかお答えください。

1. 2005 年度と比較して増やす計画 ⟶ ＋　　％程度
2. 2005 年度とほぼ同等の計画
3. 2005 年度と比較して減らす計画 ⟶ －　　％程度
4. わからない
5. その他(　　)

(4) 情報セキュリティに関して、自治体に行ってほしい施策はありますか。(複数回答可)

1. 侵害行為を取り締まる法制度の整備
2. セキュリティ業者の評価・格付けの制度化
3. 情報セキュリティに関する専門的な人材の資格制度化
4. セキュリティサービス利用への助成
5. 機器・ソフトウェア購入への助成
6. 社員教育への助成
7. 情報セキュリティに関する講習会・セミナー・研修の開催
8. 各種製品・サービス情報の提供
9. ウイルス、セキュリティホール等に関する警戒情報の提供
10. ウイルス、セキュリティホール等に対する技術の開発
11. 特にない
12. その他(　　)

(5) 本フォーラムでは以下のような活動を予定しております。興味をお持ちの活動をお答えください。(複数回答可)

1. 企業向けの情報セキュリティの普及活動
2. 一般市民向けの情報セキュリティの普及活動
3. 情報セキュリティ技術者を育成するセミナー活動
4. 情報セキュリティに関する研究活動
5. 情報セキュリティに関する情報提供
6. 企業等への講師の派遣
7. その他(　　)

(6) 本フォーラムでは今後、情報セキュリティに関連する各種セミナーを実施していく予定です。企画する際の参考にさせていただきたいので、関心のあるテーマをお答えください。(複数回答可)

1. 情報セキュリティ基礎知識
2. 情報セキュリティモラル
3. 情報セキュリティマネジメント技術
4. リスク分析技術
5. 情報セキュリティポリシー
6. 情報セキュリティ監査
7. ネットワークセキュリティ
8. OS セキュリティ
9. Web サーバ・Web アプリケーションのセキュリティ対策
10. ファイアウォール構築・運用
11. 侵入検知システム
12. VPN 構築・運用
13. コンピュータウイルス対策
14. スパイウェア対策
15. 不正アクセスの手法と対策
16. 認証技術
17. 電子署名
18. 電子透かし
19. PKI
20. 情報セキュリティに関するインシデント対応事例
21. 個人情報保護
22. プライバシーマーク制度
23. ISMS 適合性評価制度
24. 情報セキュリティ管理者育成
25. 社員教育手法
26. 情報セキュリティ施策
27. その他(　　)

以上です。ご協力ありがとうございました。

特定非営利活動法人　NPO 情報セキュリティフォーラム
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-17　総鉄岩崎学園ビル
TEL(045)311-8777　　FAX(045)311-8747
E-Mail:isef@isef.or.jp　　URL:http://www.isef.or.jp