明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ事故対応に関わるアンケート調査
調査報告書

2011年3月

情報セキュリティ大学院大学

目次

１．調査概要

１．１．調査目的

本調査は、情報セキュリティ大学院大学と神奈川県が協働で行う「情報セキュリティ事故の対応技術に関する教材の作成事業」の一環として行ったもので、事業全体の目的は、中・小規模の組織に対して情報セキュリティ事故発生時の対応技術を普及・促進することである。そのために、事故発生時の対応手順を具体的に示す教材を作成して無償配布し、中・小規模の組織において個人情報漏えいなどの情報セキュリティ事故が発生した際に、的確な対応ができる準備を行えるようにすることを事業での主な実施内容としている。

今回、本調査により、神奈川県内の中小企業における情報セキュリティ事故対応への準備状況やその他の情報セキュリティ対策の実施状況を把握し、本事業にて作成する教材の内容を現場の状況に即した実用的な内容とすることを目的として実施した。

１．２．調査対象

本調査は、神奈川県内の中小企業 539 件を調査対象として実施した。その内訳は、平成 17 年 7 月から平成 22 年 6 月までの神奈川県における中小企業新事業活動促進法に基づく経営革新計画の承認企業 608 件のうち所在不明や重複を除く 539 件となっている。

	内容
標本数	539 件
標本台帳	神奈川県における中小企業新事業活動促進法に基づく経営革新計画の承認企業 ※平成 17 年 7 月から平成 22 年 6 月までに承認された企業 608 件のうち、所在不明、県外移転や重複を除く 539 件が対象

１．３．調査実施期間

2010 年 7 月下旬～8 月上旬

１．４．調査方法

郵送調査法

１．５．回収結果

発送総数 539 件に対して、101 件の有効回収があり、有効回収率は 18.7%であった。

発送数	回収数	回収率
539	101	18.7%

１．６．調査項目

調査の主な設問項目は下記の通りである。

（1）組織・回答者の属性

（2）情報資産の保有状況

（3）システム環境

（4）情報セキュリティ対策の実施状況

（5）情報セキュリティ事故対応への準備状況

（6）情報セキュリティ事故の発生状況

（7）情報セキュリティ事故発生時の対応状況

２．調査結果

２．１．回答企業・回答者の概要

2.1.1. 従業員数（アルバイトなどを含む）

回答を得た企業の従業員数は、30 人未満の企業が 53.5%、100 人未満の企業が 89.1%であり、比較的小規模な企業が多い結果となった。

中小企業基本法第２条第１項による中小企業の法令上の定義では、業種によって異なる資本金規模や従業員規模が定義されているが、従業員規模が最大の業種でも 300 人以下とされている。今回、回答を得た企業の従業員数は全て 300 人未満となっており、概ねこの定義に当てはまるであろうことがわかる。

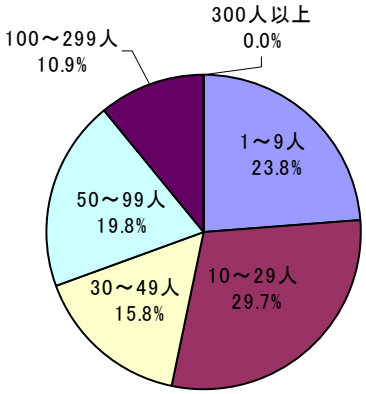

図　従業員数（n=101）

2.1.2. 売上高

回答を得た企業の売上高は１億円未満が 24.8%で、全体の約４分の１程度であり、5 億円未満が 60.4%、5 億円以上が 37.7%となった。中小企業庁が 2010 年７月に公表した中小企業実態基本調査では、中小企業の平成 20 年度決算実績において、１企業当たりの売上高は１億 4,291 万円（前年比 1.8%減）であるが、回答を得た企業の１企業当たりの売上高はこの値より大きい可能性があることが伺える。

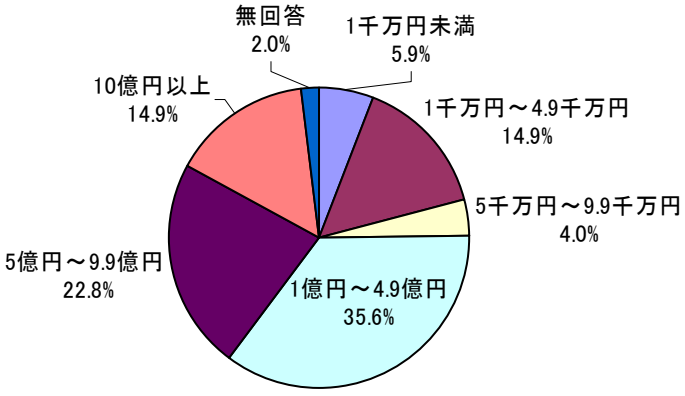

図　売上高（n=101）

2.1.3. 回答企業の主要業種

回答を得た企業の主要な業種は、製造業が最も多く 41.6%、次いで建設業の 11.9%であり、この 2 業種で 53.5%となった。製造業の割合が多くなった理由としては、今回調査対象とした企業が、神奈川県における中小企業新事業活動促進法に基づく経営革新計画の承認企業であり、この調査対象とした母集団における製造業の割合が約 48%であったことによるものである。なお、中小企業庁が全国の中小企業新事業活動促進法に基づく経営革新計画の承認企業を対象に平成 21 年に実施した「経営革新の評価・実態調査」においても回答を得た企業の多くは製造業であり 48.0%という結果となっている。

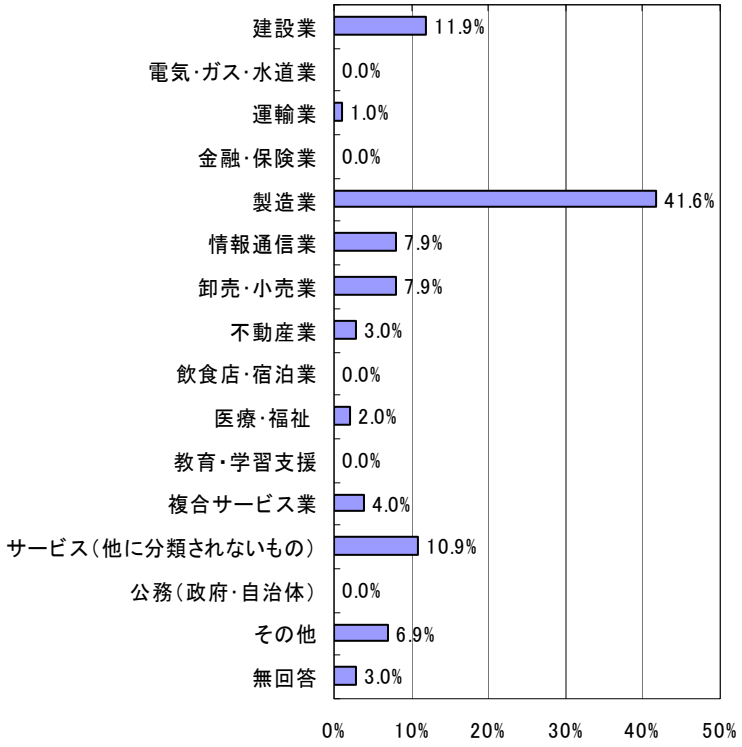

図　主要業種（n=101）

2.1.4. 回答者の所属

回答者の所属は、総務が 32.7%で全体の約 3 分の 1 程度を占め、次いで「その他」が 27.7%、社長室が 15.8%となっている。「その他」を選択した企業の大半が 2.1.5 の回答者の役職についての調査で「会長・社長・役員」を選択しており、回答者は中小企業において管理する立場にいる人が多いことが伺える。

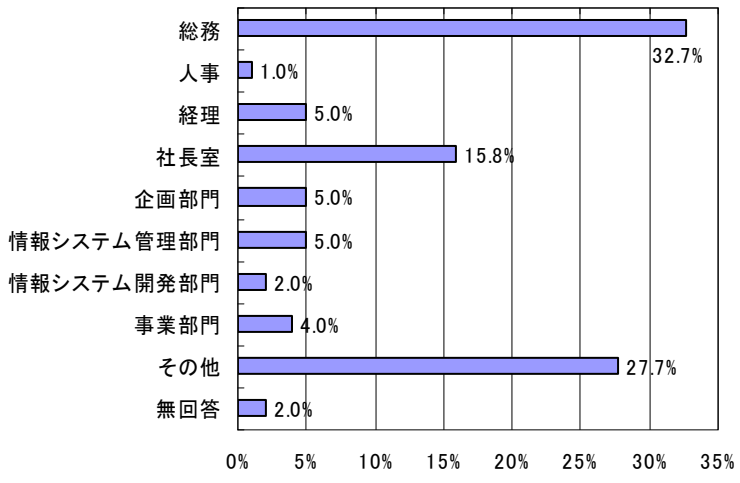

図　回答者所属（n=101）

2.1.5. 回答者の役職

回答者の役職は、「会長・社長・役員」が 51.5%となった。今回、回答を得た企業は、従業員数が 30 名以下の比較的小規模な企業が 53.5%となっており、小規模な企業の社長が回答者となったケースが多いことが伺える。

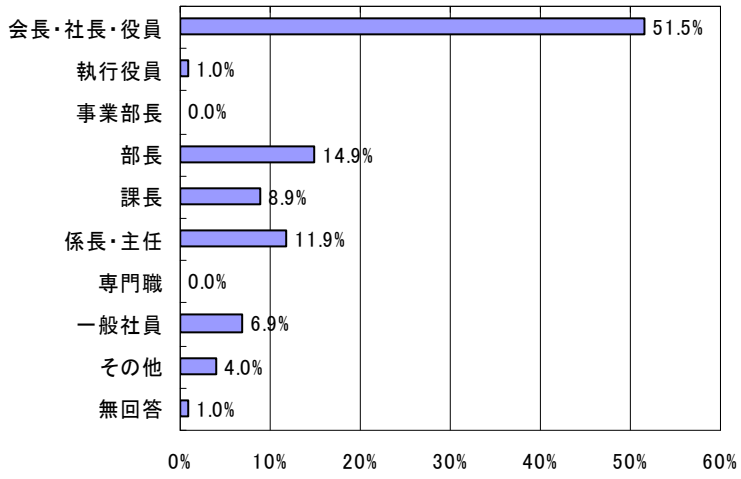

図 回答者役職(n=101)

2.1.6. 主要な業務における情報システム（社外のシステム含む）への依存度

主要な業務における情報システムへの依存度は、「一部にとどまる」または「若干依存している」と回答した企業、すなわち情報システムに依存している割合が 50%以下の企業が 47.6%であり、「多くの部分が依存している」または「ほとんどの部分が依存している」と回答した企業、すなわち依存している割合が 50%以上の企業が 51.5%となり、ほぼ同様な割合となった。中小企業において、LAN の構築が進んでいると言われているが、情報システムの使い方は、メールや Web といった主要な業務をサポートする役割で使用するにとどまっている企業も多く、必ずしも主要な業務自体に情報システムを構築している状況ではないことが伺える。

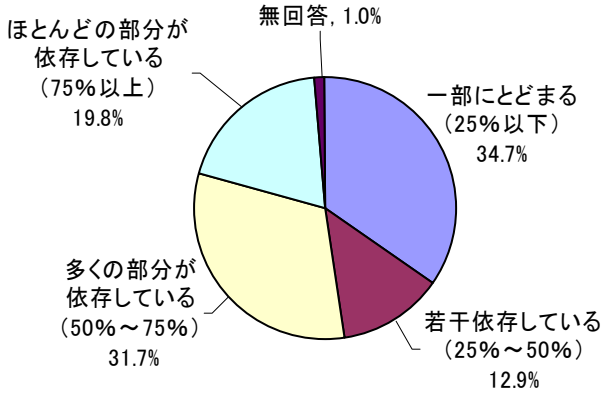

図 情報システムへの依存度(n=101)

2.1.7. 元請や代理店、フランチャイジー等のビジネスパートナーへの依存度

ビジネスパートナーへの依存度は、「ほとんど依存していない」と回答した企業が 49.5%であり、「部分的に依存している」、「大きく依存している」、「元請や代理店なしでは事業成り立たない」のいずれかを回答企業は 49.5%となり、ビジネスパートナーにほとんど依存していない企業とある程度以上依存している企業の割合が同じになった。中小企業庁が 2010 年 7 月 30 日に公表した中小企業実態基本調査では、中小企業の平成 20 年度決算実績において受託のあった法人企業の割合が 13.4%、委託を実施した法人企業の割合が 18.1%、フランチャイズ・チェーンへの加盟率は 2.4%となっており、これと比較すると依存度が高い結果となったといえる。

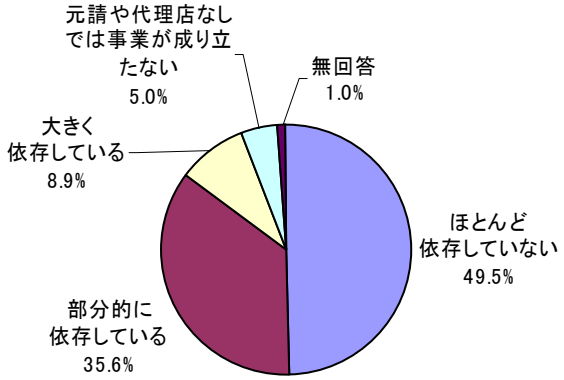

図 ビジネスパートナーへの依存度（n=101）

2.1.8. 情報システム部門の有無

情報セキュリティ部門が「無い」と回答した企業が 79.2%となった。「有る」と回答した企業は、従業員数が必ずしも多い企業というわけではなく、2.1.1 の従業員数の調査で「1～9 人」、「10～29 人」、「30～49 人」、「50～99 人」、「100～299 人」のそれぞれを回答した企業が偏りなく含まれていた。

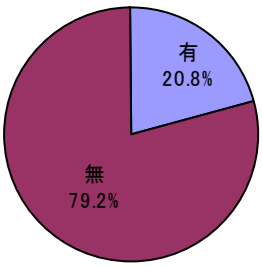

図 情報システム部門の有無（n=101）

2.1.9. 情報システム担当者数

情報システム担当者数についての設問は、記述式のため無回答（未記入）であった企業は、0 名を意図している可能性が高いと考えられる。情報システム担当者は、1 名の兼任者を持つ企業が最も多く 34.7%であり、次いで 2 名の兼任者を持つ企業が 20.8%となった。中小企業においては、兼任者として 1、2 名の情報システム担当者を置く企業が多いことが伺える。

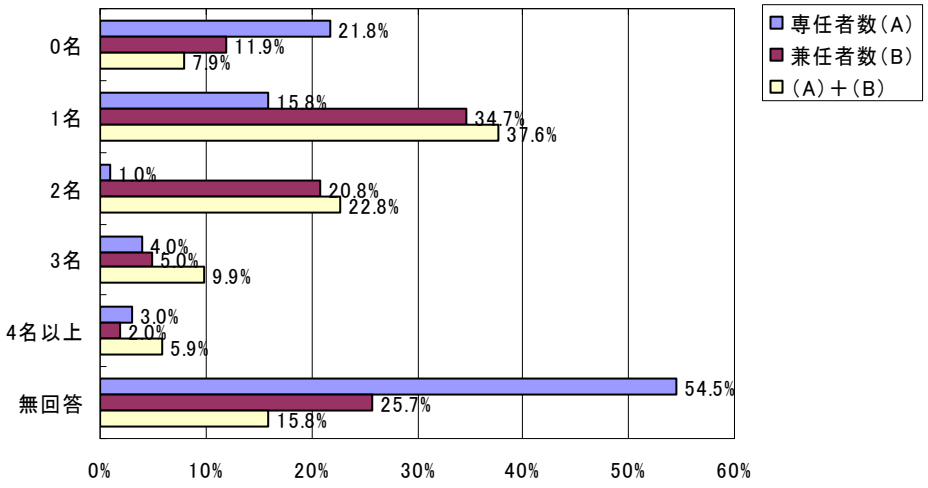

図 情報システム担当者数(n=101)

2.1.10. 情報セキュリティ担当者数

情報セキュリティ担当者数についての設問も、記述式のため無回答（未記入）であった企業は、0 名である可能性が高いと考えられる。情報セキュリティ担当者は、1 名の兼任者を持つ企業が最も多く 41.6%であり、2 名以上の専任者または兼任者を持つ企業は 24.9%となった。中小企業においては、兼任者として 1 名の情報セキュリティ担当者を置く企業が多いということが伺える。また、情報システム担当者数と比較すると、若干ではあるが情報セキュリティ担当者数の方が少ない傾向がある。

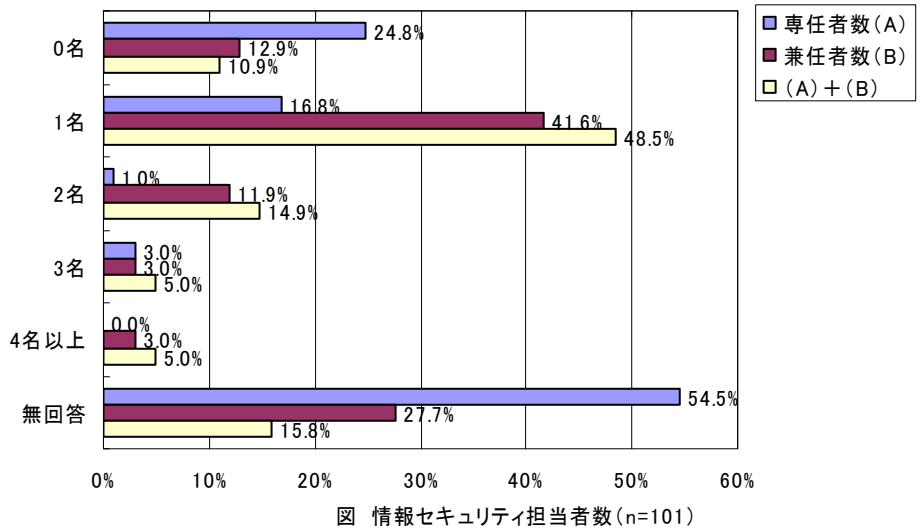

図 情報セキュリティ担当者数(n=101)

２．２．情報資産の保有状況

2.2.1. 重要情報（個人情報、機密情報など）の保有状況

重要情報の保有状況は、「ほとんどない」または「少ない」と回答した企業が 49.5%、「全体の半分程度」または「ほとんどがその種の情報である」と回答した企業が 48.5%であり、ほぼ同じぐらいの割合となった。

「ほとんどない」と回答した企業の多くは、2.1.7 のビジネスパートナーへの依存度の調査で「ほとんど依存していない」と回答した企業であった。これらの企業では、保有している重要情報は「従業員に関する個人情報」や「経営に関する情報」であり、漏洩したとしても自社の情報であるために事業に深刻な影響は生じないと考えていると推測される。

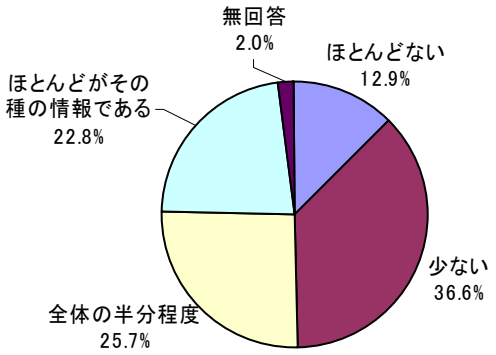

図　重要情報の保有状況（n=101）

2.2.2. 個人情報の保有数（データの延べ数）

個人情報の保有数についての設問は記述式であったが、「1～100 名」の範囲の回答が 27.7%、「101～1000 名」の範囲の回答が 23.8%、「1001～5000 名」の範囲の回答が 11.9%となった。

個人情報保護法では、5001 件以上の個人情報を個人情報データベース等として所持し事業に用いている事業者は個人情報取扱事業者とされ、個人情報取扱事業者が主務大臣への報告やそれに伴う改善措置に従わない等の適切な対処を行わなかった場合は、事業者に対して刑事罰が科される。この定義と照らし合わせると、今回回答を得た企業においてはわずか 10%しか個人情報取扱事業者に該当しないという結果になった。

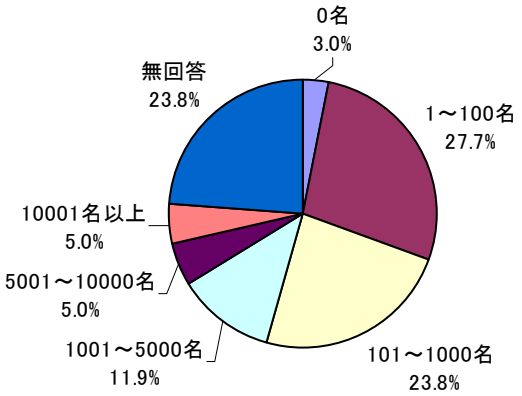

図　個人情報保有数（n=101）

2.2.3. 保有している重要情報（個人情報、機密情報など）の内容 ［複数回答可］

保有している重要情報として認識している情報は、「従業員に関する個人情報」と「顧客に関する個人情報」が最も多く、ともに 69.3%となった。

「従業員に関する個人情報」を選択していない 30.7%の企業のうちの約 39%は、2.1.1 の従業員数についての調査で「1～9 人」と回答している企業であるため、「従業員に関する個人情報」をほとんど保有・管理していない可能性はあるが、企業において全く「従業員に関する個人情報」を保有していないという状況は考えにくい。そのため、約 30%の企業が「従業員に関する個人情報」を重要情報として認識していない可能性が高いということが伺える。

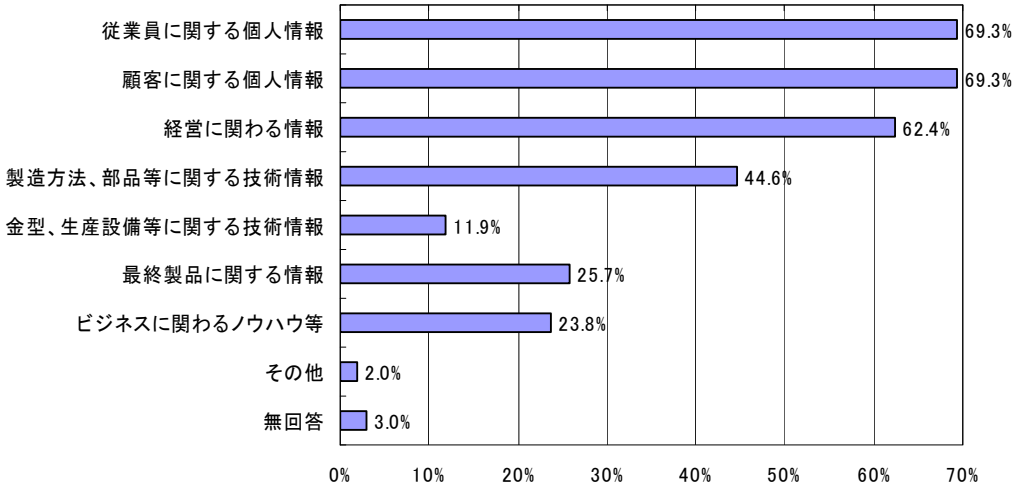

図 保有している重要情報の種類（n=101）

【「その他」の回答内容】

- 開発案件情報
- 委託業務における受取資料

2．3．システム環境

2.3.1. パソコン（オフコンも含む）の利用状況

パソコンの利用状況は、「1 人 1 台、もしくはそれ以上で利用している」と回答した企業が 75.2%であり、「数人で 1 台利用している」が 21.8%、「部課単位で数台利用している」が 9.9%という結果になった。

1 人 1 台の環境にない企業が 21.8%あるが、「利用していない」と回答した企業は 0%であり、パソコンを全く利用していない企業はほとんど無い状況であることが伺える。

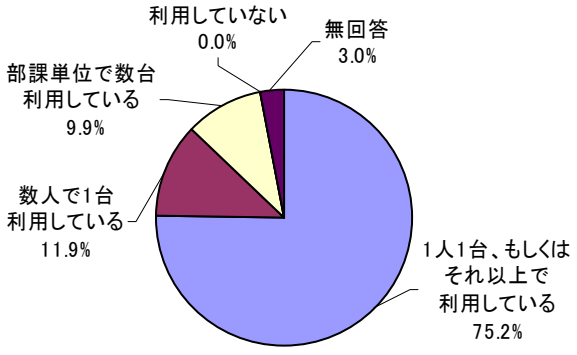

図 パソコンの利用状況（n=101）

2.3.2. サーバの保有台数とクライアントの保有台数

サーバの保有台数は、1 台以下の企業が 53.5%という結果になった。これらの企業の多くは、2.3.7 のサーバの管理方法についての調査において、Web サーバやメールサーバは「全ての管理を外部委託している」または「一部の管理を外部委託している」と回答しており、自社内で Web サーバやメールサーバを構築して運用しているという企業は少ない状況にあることが伺える。

サーバを 2 台以上保有している 37.6%の企業についても、2.3.7 のサーバの管理方法についての調査において、Web サーバやメールサーバは「全ての管理を外部委託している」または「一部の管理を外部委託している」と回答している企業が多い状況となっているが、前述の 1 台以下の企業とは異なりファイルサーバやデータベースサーバは「自社で管理している」と回答した企業が多い結果となった。

クライアントの保有台数は、2.3.1 のパソコンの利用状況についての調査で「1 人 1 台、もしくはそれ以上で利用している」と回答した企業が 75.2%という結果から、2.1.1 の従業員数についての調査結果よりも少ない数となることが予想されるが、概ねそのとおりとなっていることが確認できる。

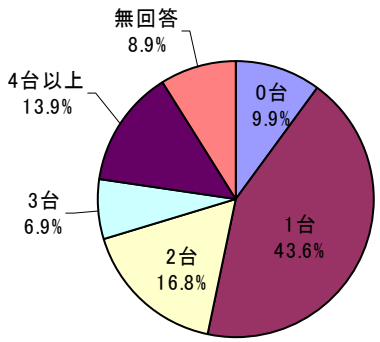

図　サーバ保有台数(n=101)

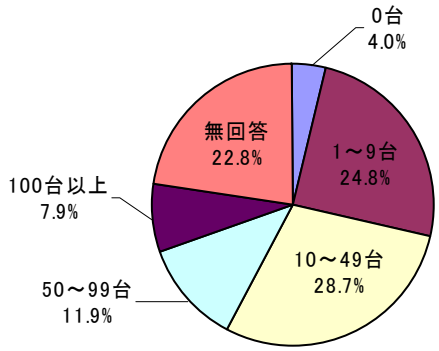

図　クライアント保有台数(n=101)

2.3.3. 最も多く利用している OS

社内で最も多く利用されている OS は、「WindowsXP」が最も多く 87.1%であった。サポートの終了している OS である「Windows98,Me」や「WindowsNT,2000」を最も多く利用している企業もわずかではあるが、5%存在した。

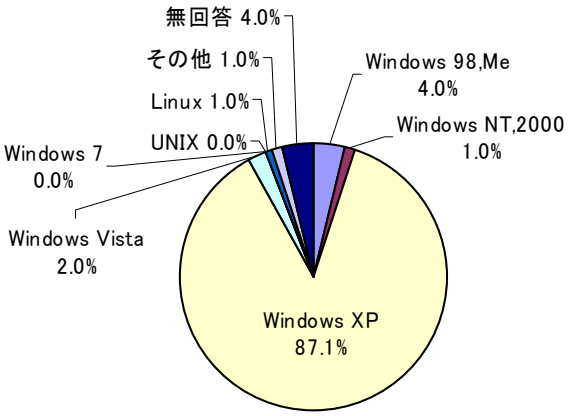

図　最も多く利用しているOS(n=101)

【「その他」の回答内容】

・Mac OS

2.3.4. サポートの終了しているOS（Windows 98 / Windows Me など）の利用状況

社内でサポートが終了しているOSをインストールしているパソコンの利用状況は、「ない」と回答した企業が69.3%であり、次いで「数台程度」と回答した企業が22.8%となった。

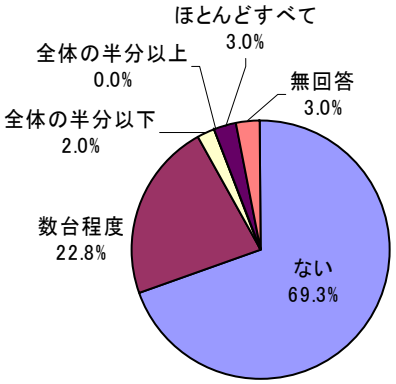

図　サポートが終了したOSの利用状況（n=101）

2.3.5. セキュリティパッチ（脆弱性の修正）の適用状況

セキュリティパッチの適用状況は、「常に適用し、適用状況も把握している」と回答した企業、すなわち、セキュリティパッチを確実に適用している企業は、25.7%であった。

「各ユーザに適用を任せている」、「ほとんど適用していない」、「分からない」のいずれかを選択した企業、すなわち、セキュリティパッチの適用が組織として推進されていない企業が、40.6%となった。パソコンの基本的な情報セキュリティ対策ができていない企業がまだまだ存在する状況にあることが伺える。

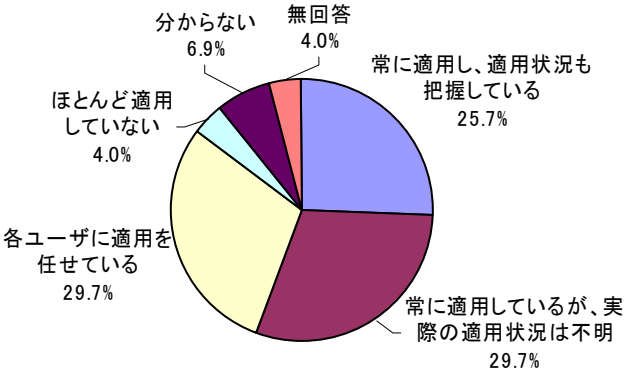

図　セキュリティパッチの適用状況

2.3.6. LANの導入状況およびパソコンの接続状況

LANの導入状況およびパソコンの接続状況は、「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」と回答した企業が83.2%であり、「半分程度のパソコンがこれに接続されている」を含めると89.1%となった。中小企業においてもパソコン単体での利用形態はほとんどなくネットワークを含めた情報セキュリティ対策や事故対応への準備が必要であることがわかる。

LANが導入されている企業は、合計すると92.1%であり、LANを導入していないが今後導入する予定である企業が1.0%であることから、中小企業においてLANの導入はほぼ完了している状況にあることが伺える。

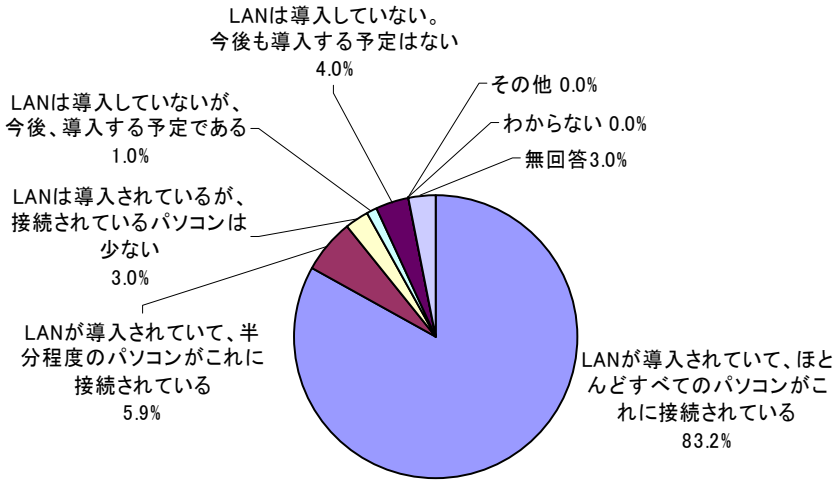

図　LANの導入状況（n=101）

2.3.7. 情報システムやネットワーク機器の管理方法

Webサーバやメールサーバについては、「全ての管理を外部委託している」と回答した企業がそれぞれ44.6%、51.5%となり、外部委託している企業が多いことがわかる。ホスティングサービスが充実している現状において、資金や人的資源の限られた中小企業では、わざわざ自社でサーバを構築して運用するよりも容易に利用できるホスティングサービスの利用を選択する企業が多いという状況が伺える。

一方で、秘匿性が高い情報を保存する可能性があるファイルサーバやデータベースサーバについては、「自社で管理している」と回答した企業が多く、それぞれ59.4%、49.5%となっている。

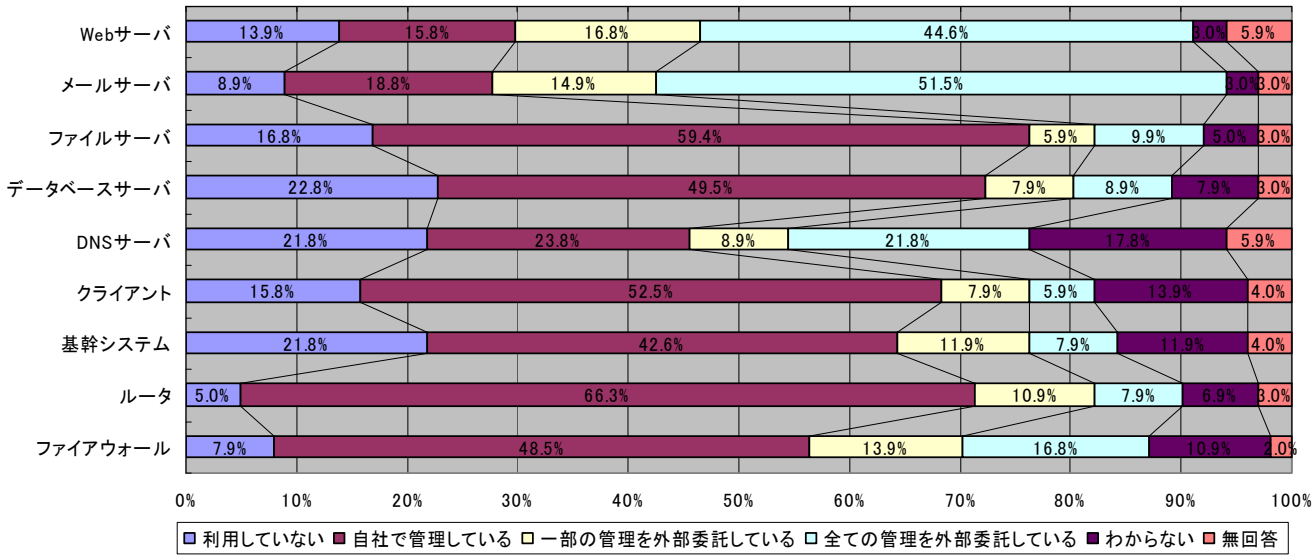

図　情報システム・ネットワークの管理体制（N=101）

２．４．情報セキュリティ対策の実施状況

2.4.1. 個人所有のパソコンを業務使用することの是非の明確化状況

個人所有のパソコンを業務使用することの是非については、「明確にしていない」と回答した企業の方が多く、64.4%であった。

「明確にしている」と回答した企業のうち、2.4.2 の個人所有のパソコンを業務使用している人の有無についての調査で「いる」と回答した企業、すなわち、個人所有のパソコンの業務使用を許可制にしている企業は、全体の約 10%であった。

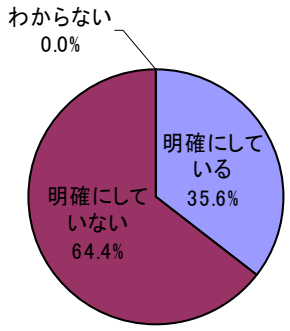

図　個人所有パソコンの使用是非（n=101）

2.4.2. 個人所有のパソコンを業務使用している人の有無

個人所有のパソコンを業務使用している人がいるかどうかについて「わからない」と回答した企業は、わずか 1%であり、ほとんどの企業がパソコンの使用状況を把握できているという結果になった。

個人所有のパソコンを業務使用している人が「いる」と回答した企業は 38.6%であり、そのなかで、個人所有のパソコンを業務使用することの是非を「明確にしていない」と回答した企業は全体の 28.7%であった。中小企業において、自宅でウイルス感染した個人所有のパソコンを社内 LAN に接続したことによりウイルスが蔓延してしまうといったリスクを持つ企業が全体の 4 分の 1 以上存在するという結果になった。

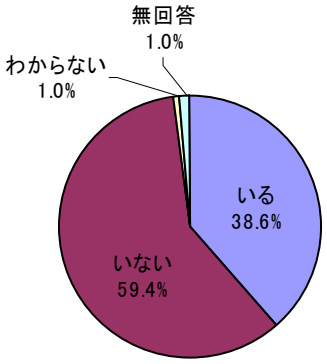

図　個人所有パソコンの業務使用者有無（n=101）

2.4.3. パソコンのログイン管理状況

パソコンのログイン管理については、「行っている」と回答した企業が 46.5%であるのに対して、「行っていない」または「一部行っている」と回答した企業が 53.5%であり、ログイン管理が行われていないパソコンがある企業が多いことがわかった。

ログイン管理を「行っていない」と回答した企業のうち、2.3.1 のパソコンの利用状況についての調査で「1 人 1 台もしくはそれ以上で利用している」と回答した企業は約 70%であった。このことから、1 台のパソコンを複数の人が使用する環境にあり、利便性が損なわれるためにログイン管理を行っていないというケースが多いわけではなく、1 人 1 台のパソコンを使用できる環境にあるが、リスクを認識していないためにログイン管理を行っていないケースが多くあることが推察される。

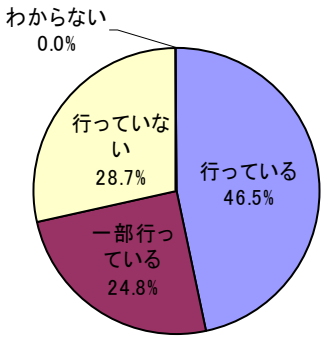

図 パソコンのログイン管理状況(n=101)

2.4.4. 情報セキュリティポリシーの策定状況

情報セキュリティポリシーは、「ない」と回答した企業が最も多く 54.5%であり、情報セキュリティポリシーを定めていない企業が多いことがわかった。

企業規模に関わらず「公式なポリシーを定めている」または「非公式なポリシーを定めている」を回答した企業は存在したが、「公式なポリシーを定めている」と回答した企業の業種としては、「情報通信業」や「サービス（他には分類されないもの)」の割合が多い結果となった。「サービス（他には分類されないもの)」の業種の企業について調査したところ、複数のサービスのうちの一つに情報通信業を含んでいるという共通点があることがわかった。このことから、IT に関連した業務を行っている企業ほど組織として情報セキュリティ対策を実施することの必要性あるいは、実施していることを対外的に示す必要性を感じているということが伺える。

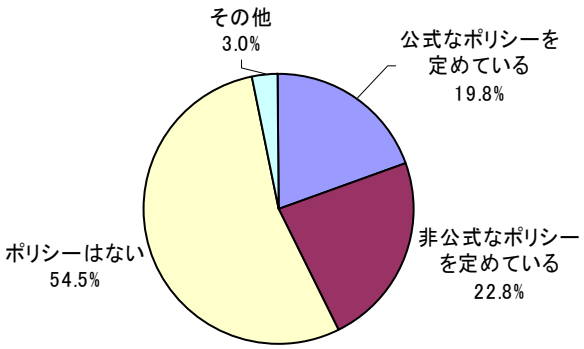

図 情報セキュリティポリシーの策定状況

2.4.5. 重要情報（個人情報、機密情報など）についての認識の共有状況

保有している重要情報が何かを社内で「共有している」と回答した企業は、27.7%で全体の 4 分の 1 程度であり、多くの企業が組織として守るべき重要情報についての認識が社内で共有されていない状態にあることがわかった。

「共有していない」と回答した企業のうちの 70%は、2.2.1 の重要情報の保有状況についての調査で重要情報は「ほとんどない」または「少ない」と回答しており、共有すべき対象そのものが存在しないという認識をもっているケースが多いことが伺える。

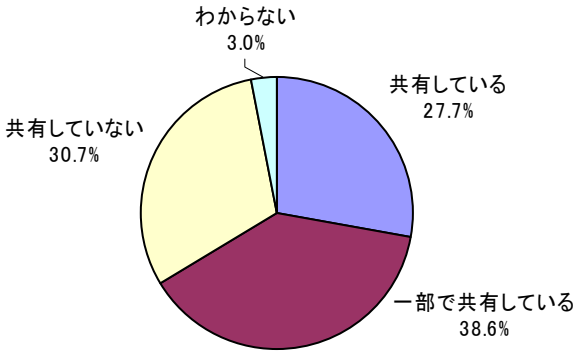

図　重要情報についての認識の共有状況（n=101）

2.4.6. 重要情報の取り扱いに関する具体的なルールの策定状況

重要情報の取り扱いに関する具体的なルールは、「定めていない」と回答した企業が最も多く 39.6%であり、2.4.5 の設問で重要情報が何かを社内で「共有していない」と回答した企業の割合よりも多い結果となった。このことから、重要情報が何かを認識できていてもそれに関するルールが整備されていないという企業があることが推察されたため、重要情報が何かを社内で「共有している」または「一部で共有している」と回答した企業のうち、重要情報の取り扱いに関する具体的なルールを「定めていない」と回答した企業の割合を調べたところ、約 28%であることがわかった。

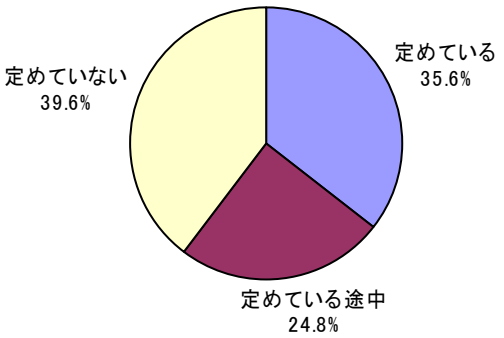

図　重要情報の取り扱いに関するルールの策定状況（n=101）

2.4.7. 重要情報の取り扱いに関するルールは遵守可能か

※「2.4.6」の設問で「1. 定めている」を選択した方のみ回答。

重要情報の取り扱いに関するルールは、守ることができるルールに「なっている」と回答した企業が最も多く 63.9%であり、次いで「一部なっていない」が 19.4%で、「なっていない」と回答した企業はなかった。重要情報の取り扱いに関するルールを定めている企業においては、比較的多くの企業で守ることができるルールが整備されていることがわかった。

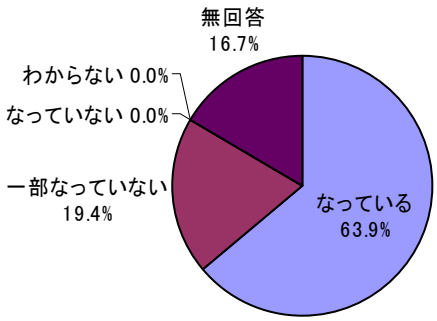

図 重要情報の取り扱いに関するルールは遵守可能なものとなっているか（n=36）

2.4.8. 情報セキュリティ教育の実施状況

情報セキュリティの教育は、「特に行っていない」と回答した企業が最も多く 53.5%という結果になった。「特に行っていない」と回答した企業のうちの約 80%が 2.4.1 の設問で個人所有のパソコンの業務使用の是非を「明確にしていない」と回答しており、約 74%が 2.4.4 の設問で公式な情報セキュリティポリシーを「定めていない」と回答している。このことから、情報セキュリティ教育を行っていない企業は、組織として情報セキュリティ対策を実施していく意識が低い傾向があることがわかり、中小企業においてはまだまだ情報セキュリティ対策に対する意識が低い企業が多いことが確認された。

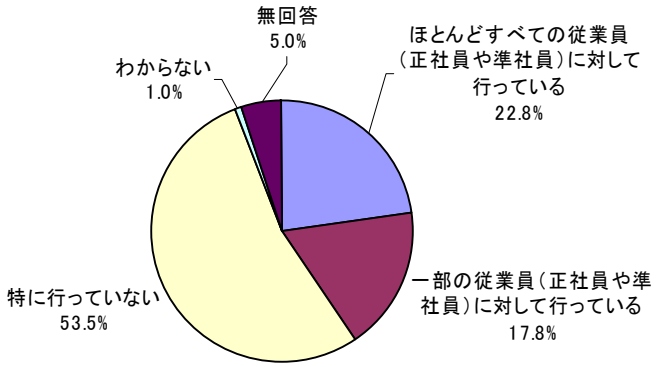

図 情報セキュリティ教育の実施状況（n=101）

2.4.9. 情報セキュリティの教育の実施形式［複数回答可］

※「2.4.8」の設問で「1.ほとんどすべての従業員に対して行っている」または「2.一部の従業員に対して行っている」を選択した方のみ回答。

情報セキュリティ教育の形式は、「ミーティング」と回答した企業が 39.0%と最も多く、次いで「集合型研修」が 31.7%、「メール」が 29.3%となった。「e ラーニング」と回答した企業はなく、「社外講師による研修」は 7.3%であった。中小企業においては、情報セキュリティ教育に対して e ラーニングシステムを導入するほどのコストをかけている企業はほとんどなく、必要に応じて容易に実施できる形式を採用している状況が多いことが伺える。

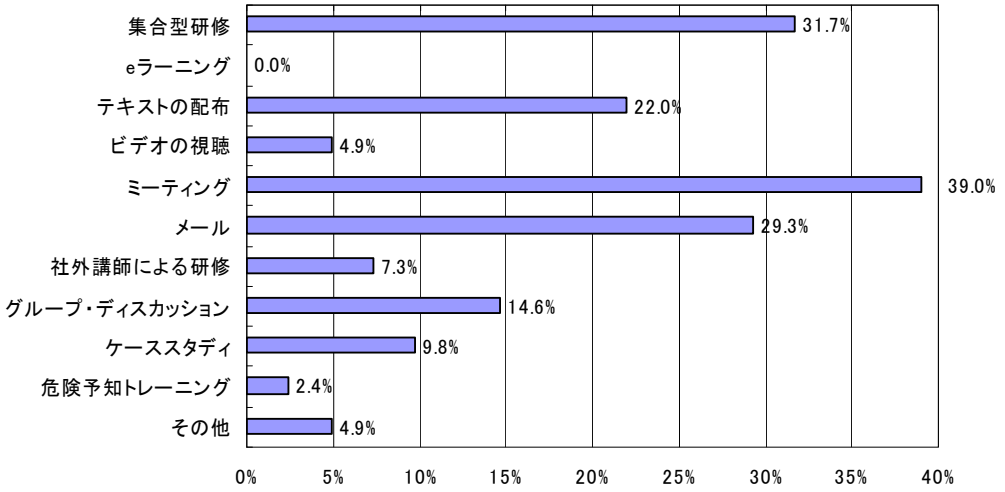

図　情報セキュリティ教育の実施形式（n=41）

2.4.10. 情報セキュリティ教育の実施内容［複数回答可］

※「2.4.8」の設問で「1.ほとんどすべての従業員に対して行っている」または「2.一部の従業員に対して行っている」を選択した方のみ回答。

情報セキュリティ教育の内容は、「ウイルスや不正アクセス等のネットワークセキュリティ」と回答した企業が 58.5%と最も多い結果となった。2.6.1 の過去に発生したことのある情報セキュリティ事故についての調査で最も多かった回答がウイルス感染であることからも、ウイルスをより身近な脅威として感じている状況であることが伺える。

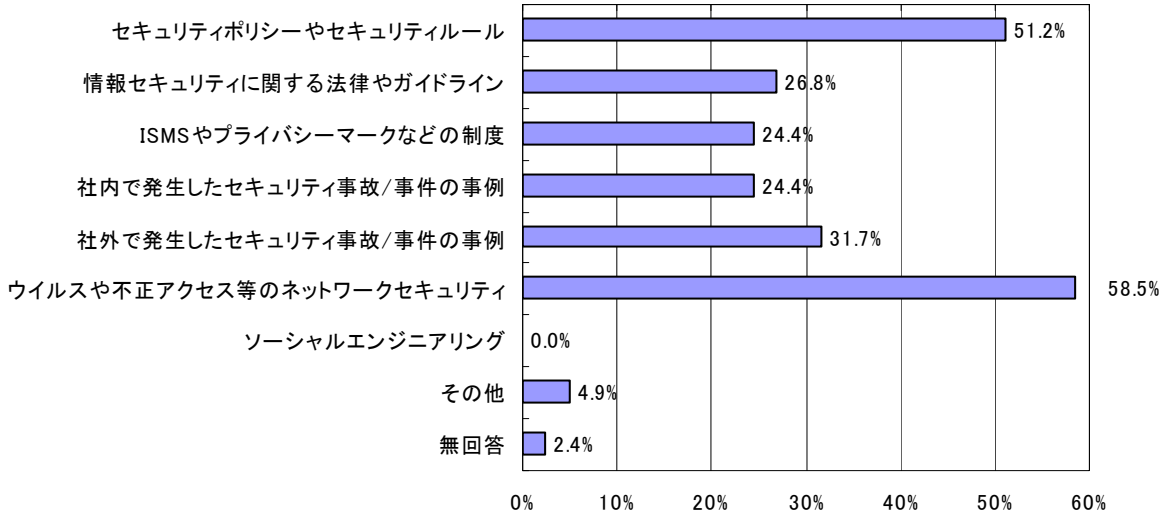

図　情報セキュリティ教育の実施内容（n=41）

２．５．情報セキュリティ事故対応への準備状況

2.5.1. 情報セキュリティ事故対応への準備状況

情報セキュリティ事故対応への準備を「実施している」と回答した企業は、25.7%で全体の 4 分の 1 程度であり、多くの企業において事故対応への準備を実施していない状況にあることがわかった。

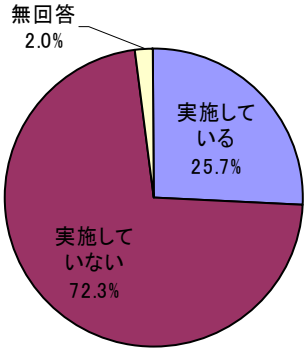

図　情報セキュリティ事故対応の準備実施状況（n=101）

2.5.2. 実施している情報セキュリティ事故対応準備の内容［複数回答可］

※「2.5.1」の設問で「1. 実施している」を選択した方のみ回答。

情報セキュリティ事故対応への準備として実施されている内容としては、「重要情報のバックアップ」が最も多く 80.8%、次いで「連絡窓口（担当者）の設置」が 65.4%となり、コストがかからず知識やノウハウもあまり必要としないものが実施されている傾向があることが伺える。バックアップについては、大容量の外付けハードディスクが比較的安価に入手できることもあり、中小企業においても導入が進んでいると推察される。

逆に実施されていない内容としては、「証拠保全の手順書の作成」や「重要サーバの構築手順書の作成」であり、専門的な知識を必要とする対策については、自社で行わずに情報システムの管理委託先に任せているというような状況にあることが伺える。

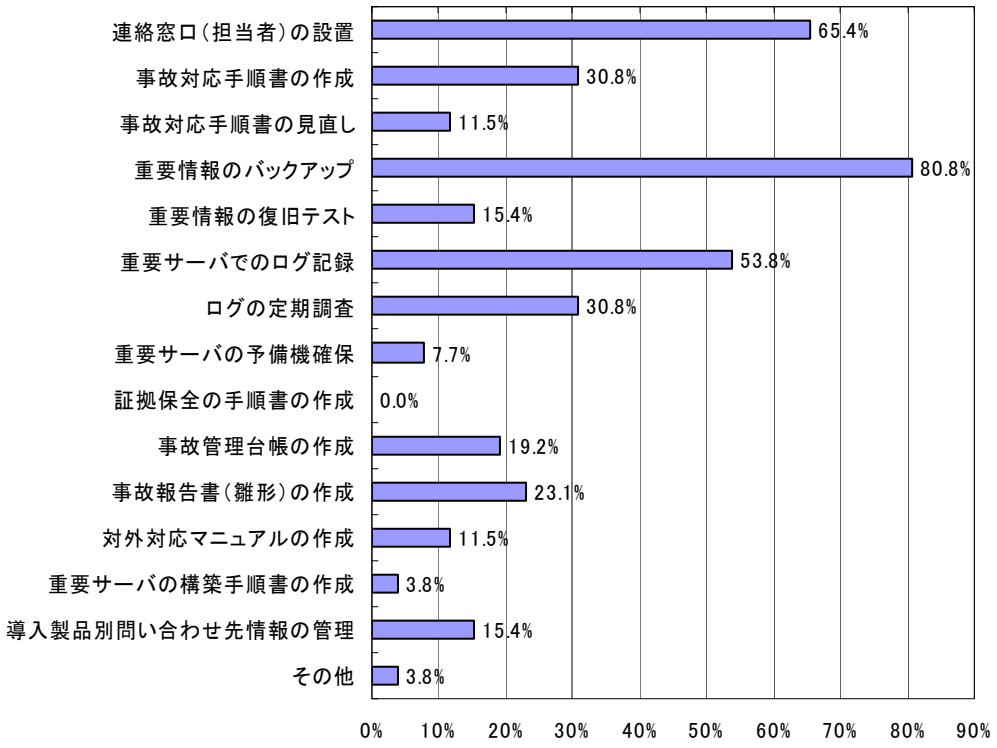

図　情報セキュリティ事故対応の準備内容（n=26）

2.5.3. 情報セキュリティ事故対応への準備を行う際に参考にした情報

※「2.5.1」の設問で「1. 実施している」を選択した方のみ回答。

【回答内容】

- ISO/IEC27001 関連の HP、ISMS ユーザーズガイド等
- ISO27001（ISMS）
- ISMS 及び 27001
- インターネット
- 各種セミナー、WEB 情報、受信メール情報
- プライバシーマークの PMS
- Ｐマーク取得の際のコンサルタントから
- 個人情報保護法

2.5.4. 情報セキュリティ事故対応への準備を行う際に不足していた情報

※「2.5.1」の設問で「1. 実施している」を選択した方のみ回答。

【回答内容】

- 市販されている本など（全体的に専門用語が多すぎてわかりにくかった）

2.5.5. 情報セキュリティ事故対応への準備を行う必要性に対する認識

※「2.5.1」の設問で「2. 実施いない」を選択した方のみ回答。

情報セキュリティ事故対応への準備を実施していない企業のうち、実施することの「必要性を感じる」と回答した企業は 71.2%であり、実施していない企業の多くは何らかの問題があることで実施できていない状況であることが伺える。

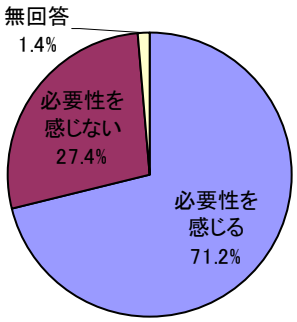

図 情報セキュリティ事故対応準備の必要性（n=73）

2.5.6. 情報セキュリティ事故対応への準備を実施する上での問題点［複数回答可］

※「2.5.1」の設問で「2. 実施していない」を選択した方のみ回答。

情報セキュリティ事故対応への準備をする上での問題点として、最も多かったのは「担当できる人材が不足している」で 61.6%、次いで「知識やノウハウが不足している」で 54.8%という結果になった。コストがかけられず実施できないという状況よりは、何をやればいいのかわからない、もしくは、どうやればいいのかわからないというように事故対応への準備に関する情報が不足している状況にあるということが伺える。

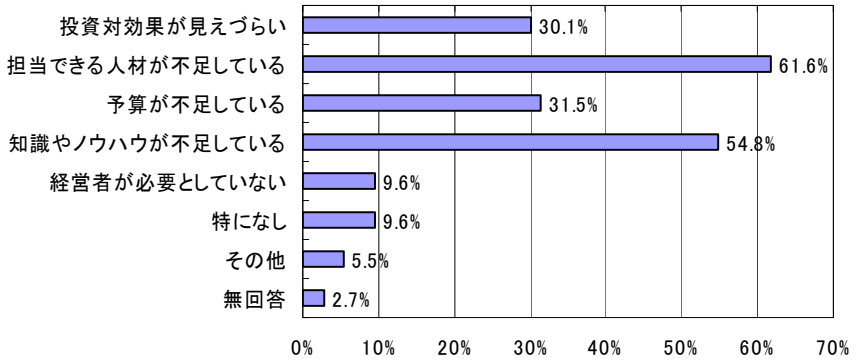

図 情報セキュリティ事故対応への準備を実施する上での問題点（n=73）

【「その他」の回答内容】

- 業務スピードが遅延したり複雑になる
- 重要情報の管理手法、設備、コストなど知識不足
- IT への関心か薄い

２．６．情報セキュリティ事故の発生状況

2.6.1. 過去に発生した情報セキュリティ事故［複数回答可］

過去に発生したことのある情報セキュリティ事故で最も回答が多かったのは、「ウイルス感染」で36.6%であり、「ウイルス感染」を含めて過去に何らかの情報セキュリティ事故が発生したことがあると回答した企業は43.5%という結果になった。

「ウイルス感染」以外の事故が発生した企業は少なく、対外的な対応が必要となる顧客情報の漏えいや復旧に時間を要するようなシステムへの被害を経験した企業は、ほとんどないという状況であることが伺える。

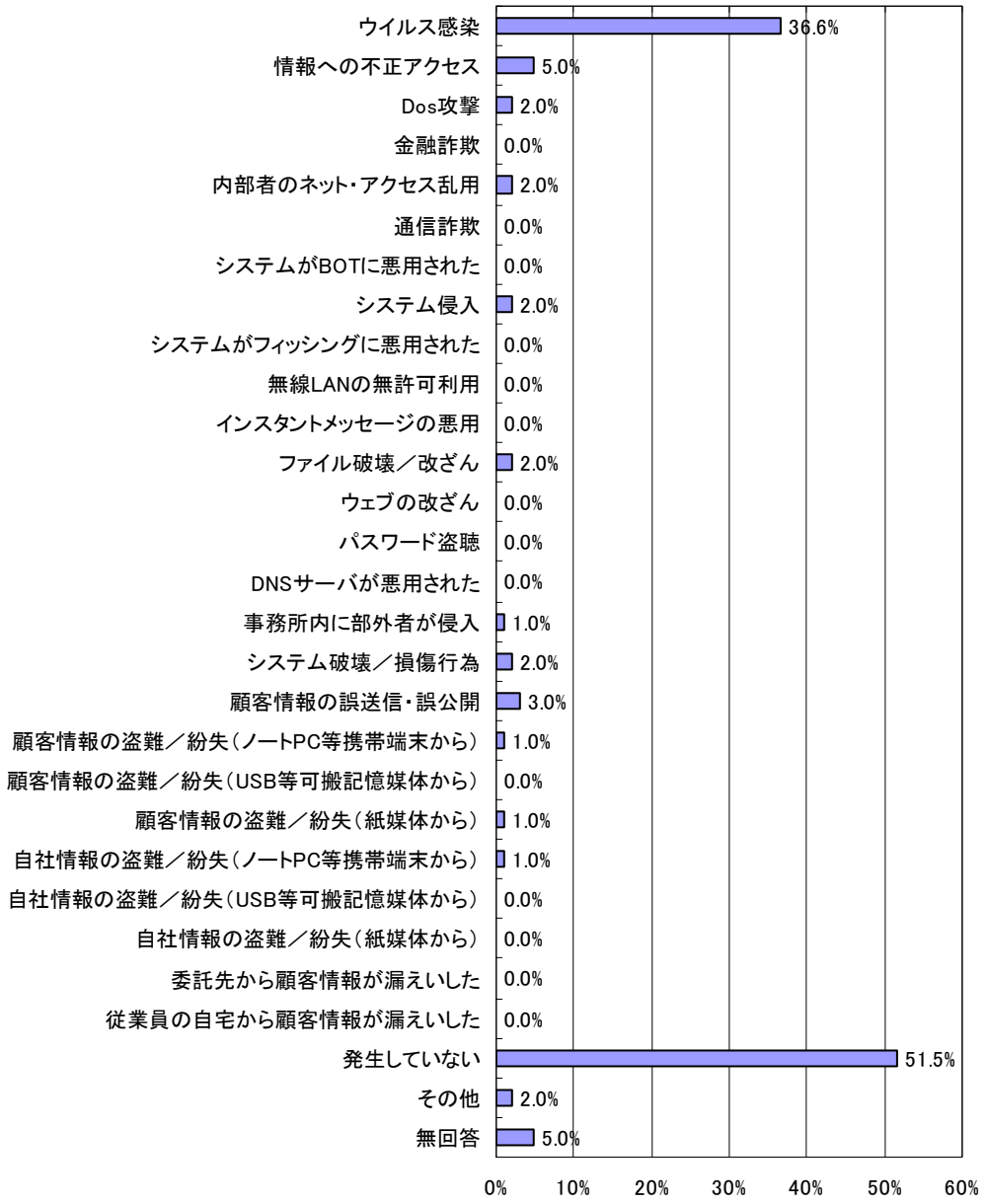

図 情報セキュリティ事故の発生状況（n=101）

【「その他」の回答内容】

・入管証等の紛失

2.6.2. 情報セキュリティ事故の過去１年間の発生回数

※「2.6.1」の設問で「27. 発生していない」以外を選択した方が回答。

過去１年間の情報セキュリティ事故発生回数は、無回答の企業が 50.0%となっているが、この調査の設問は記入式であるため、これらの企業は「発生なし」を意図している可能性が高いと思われる。（※下表の「発生なし」に集計した企業は、回答欄に 0 を記入した企業）

無回答を「発生なし」と判断した場合、2.6.1 で示した過去に情報セキュリティ事故が発生したことがあると回答した 43.5%の企業のうち過去１年間に情報セキュリティ事故が発生していない企業は、72.7%となった。すなわち、全体の約 13%の企業が過去１年間のうちに情報セキュリティ事故が発生したということがわかる。

選択肢		発生回数	回答数	構成比
外部要因	故意によるもの	－	－	－
	過失によるもの	1 回	1	2.3%
		3 回	1	2.3%
	その他	1 回	2	4.5%
		2 回	1	2.3%
内部要因	故意によるもの	－	－	－
	過失によるもの	1 回	5	11.4%
		2 回	1	2.3%
		6 回	1	2.3%
		10 回	1	2.3%
	その他	－	－	－
発生なし			10	22.7%
無回答			22	50.0%

２．７．情報セキュリティ事故発生時の対応状況

2.7.1. 情報セキュリティ事故発生時の対応状況［複数回答可］

※「2.6.1」の設問で「27. 発生していない」以外を選択した方が回答。

情報セキュリティ事故が発生した時の内部的な対応として最も多かった回答が、「セキュリティソフトをインストールした」で 38.6%となった。2.6.1 で示したとおり過去に発生した情報セキュリティ事故として最も多かったのがウイルス感染であるということから、この選択肢を回答した企業の多くは、パソコンがウイルスに感染したことをきっかけとしてウイルス対策ソフトを導入したというケースであることが伺える。

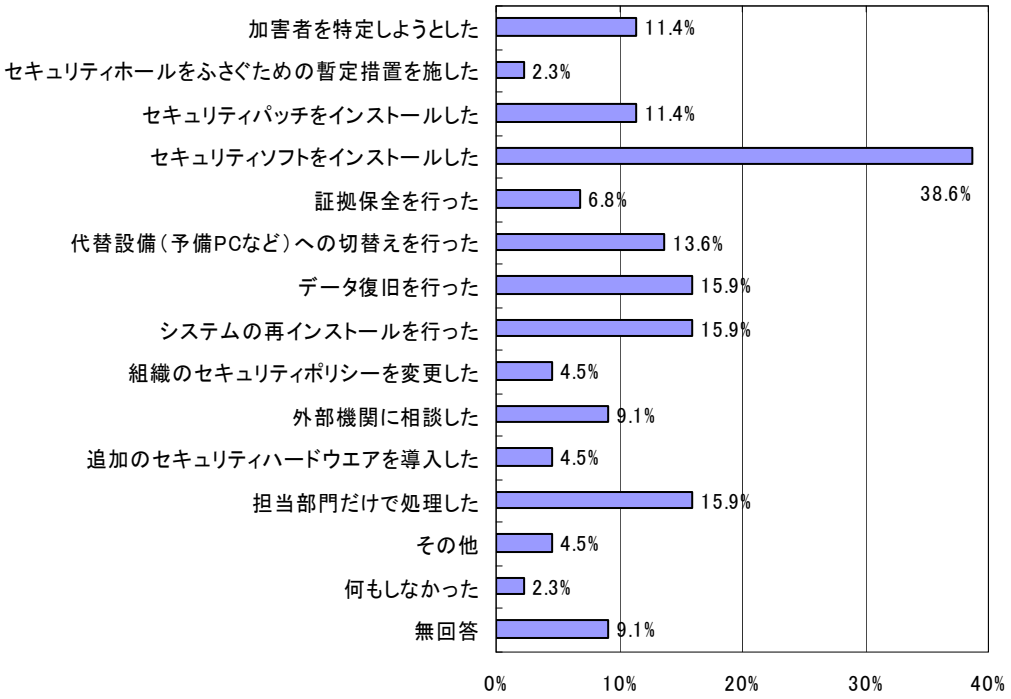

図 情報セキュリティ事故発生時の対応（n=44）

2.7.2. 届出を行った外部組織［複数回答可］

※「2.6.1」の設問で「27. 発生していない」以外を選択した方が回答。

過去に情報セキュリティ事故が発生したことがある企業のうち、77.3%の企業が「届出を行わなかった」と回答した結果となった。過去に発生した情報セキュリティ事故として多くの企業が「ウイルス感染」と回答していることから、「届出を行わなかった」と回答した企業の多くは、ウイルス感染したがウイルス対策ソフト等でウイルスを駆除して解決し、特に届出を行わなかったというケースであるということが伺える。

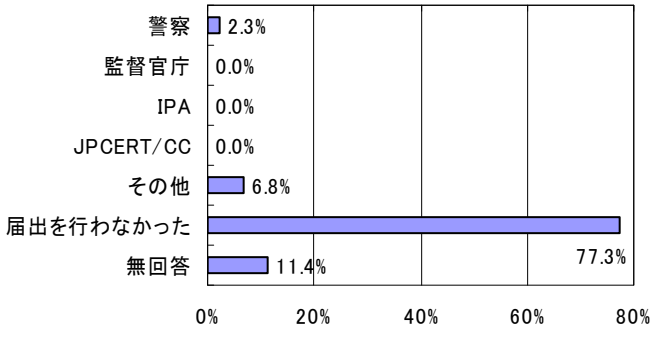

図 事故の届出を行った外部組織（n=44）

2.7.3. 届出を行わなかった理由［複数回答可］

※「2.7.2」の設問で「6. 届出を行わなかった」を選択した方のみ回答。

届出を行わなかった理由の多くは、「報告する程の事件ではなかったため」という結果となったが、これについても 2.7.2 で述べた内容と同様に、ウイルス感染したが対外的な影響を与えることなく解決したため報告する必要性を感じなかったケースが多いということが伺える。

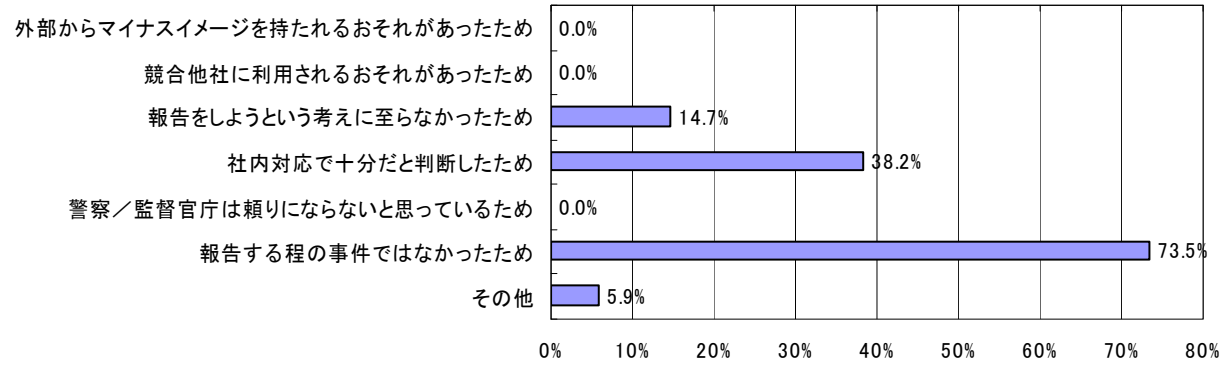

図 事故の届出を行わなかった理由（n=34）

【「その他」の回答内容】

・当時知識が少なく、報告する義務を知らなかった

参考資料：アンケート調査票

情報セキュリティ事故対応に関わるアンケート調査

【本調査にご協力いただくにあたって】

（1）本調査は、神奈川県が県政の課題解決のために実施している「大学発・政策提案制度」により、神奈川県と情報セキュリティ大学院大学が協働で行う「情報セキュリティ事故の対応技術に関する教材の作成事業」の一環として行うものです。

（2）本事業は、県内の企業や自治体において個人情報漏えいなどの情報セキュリティ事故が発生した際に、的確な対応ができる人材の育成を目的としており、作成した教材は本事業の成果として県内の企業や自治体に無償配布いたします。また、作成する教材を使用した無料講座も実施する予定です。

（3）このアンケートは、情報セキュリティ大学院大学が作成し、集計と分析を行います。ご回答いただいた情報は、本事業でのみ活用し、その結果を本事業にて作成する教材に反映いたします。なお、**個票データが会社名およびご回答者名とリンクして公表されることは一切ございません。**

（4）誠に勝手ながら、集計の都合上、調査票は以下の期日までに返信用封筒（切手不要）に入れ、ご投函いただきますようお願い申し上げます。

２０１０年８月６日（金）

（5）本調査に関してご不明な点がございましたら、以下までお問い合わせをお願い申し上げます。

情報セキュリティ大学院大学　担当：柿本
〒221-0835 神奈川県横浜市神奈川区鶴屋町 2－17　TEL 045-311-5581／FAX 045-311-8109

【ご回答をお願いしたい方】

貴社において、**情報セキュリティ担当者もしくは情報システム担当者の方**のご回答をお願い致します。

【ご回答者の情報】

ご記入いただいた個人情報は、本調査に関してお問い合わせをさせていただく際、または、本事業で作成した教材をお送りする際にのみ使用させていただきます。なお、ご希望の方には本事業にて実施する無料講座のご案内をお送りさせていただきますので、以下に○をご記入ください。

貴社名	
ご所属部署 お役職	
お名前	
ご住所	
TEL	
E-mail	
教材[注1]の無償配布 ○をご記入ください	1．希望する
	2．希望しない
無料講座[注2]のご案内 ○をご記入ください	1．希望する
	2．希望しない

注1）平成 23 年 3 月頃に配布予定。
注2）平成 22 年 10 月頃から全 10 回程度の講座を開講予定。

質問回答票	本用紙にご回答をご記入いただき、ご返送ください

選択式設問のご回答は、回答する選択肢の番号を〇で囲んでください。

記述式設問のご回答は、回答記入欄に具体的な数値や文章を記入してください。

1 貴組織･ご記入者について

1-1. 貴組織の従業員数（アルバイトなどを含む）を教えてください。［1つ選択］

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		

1-2. 貴組織の売上高（または予算額）を教えてください。［1つ選択］

1．1千万円未満	2．1千万円 ～ 4.9千万円	3．5千万円 ～ 9.9千万円
4．1億円 ～ 4.9億円	5．5億円 ～ 9.9億円	6．10億円以上

1-3. 貴組織の主要業種を教えてください。［1つ選択］

1．建設業	2．電気･ガス･水道業	3．運輸業
4．金融･保険業	5．製造業	6．情報通信業
7．卸売･小売業	8．不動産業	9．飲食店･宿泊業
10．医療･福祉	11．教育・学習支援	12．複合サービス業
13．サービス（他に分類されないもの）	14．公務（政府･自治体）	15．その他

1-4. ご記入者の所属を教えてください。［1つ選択］

1．総務	2．人事	3．経理
4．社長室	5．企画部門	6．情報システム管理部門
7．情報システム開発部門	8．事業部門	9．その他

1-5. ご記入者の役職を教えてください。［1つ選択］

1．会長・社長・役員	2．執行役員	3．事業部長
4．部長	5．課長	6．係長・主任
7．専門職	8．一般社員	9．その他

1-6. 貴組織の主要な業務に関して、情報システム（社外のシステム含む）に依存している割合はどの程度ですか。［1つ選択］

1．一部にとどまる（25%以下）	2．若干依存している（25%～50%）
3．多くの部分が依存している（50%～75%）	4．ほとんどの部分が依存している（75%以上）

1-7. 貴組織の業務は、元請や代理店、フランチャイジー等のビジネスパートナーにどの程度依存していますか。［1つ選択］

1．ほとんど依存していない	2．部分的に依存している
3．大きく依存している	4．元請や代理店なしでは事業が成り立たない

1-8. 貴組織に情報システム部門はありますか。［1つ選択］

1．有	2．無

1-9. 貴組織の情報システム担当者数を教えてください。

専任者数：（　　）人	兼任者数：（　　）人

1-10. 貴組織の情報セキュリティ担当者数を教えてください。

専任者数：（　　）人	兼任者数：（　　）人

2 情報資産について

2-1. 貴組織において、外部に漏洩すると事業に深刻な影響が生じる重要情報（個人情報、機密情報など）をどの程度保有、管理または使用していますか。［１つ選択］

１．ほとんどない	２．少ない
３．全体の半分程度	４．ほとんどがその種の情報である

2-2. 事業を実施する上で何名分程度の個人情報を取り扱っていますか。（データの延べ数でお答えください。）

おおよそ（　　）名分

2-3. 貴組織で保有している重要情報（個人情報、機密情報など）として把握されているものをお答えください。［該当するものすべて選択］

１．従業員に関する個人情報	２．顧客に関する個人情報
３．経営に関わる情報	４．製造方法、部品等に関する技術情報
５．金型、生産設備等に関する技術情報	６．最終製品に関する情報
７．ビジネスに関わるノウハウ等	
８．その他（具体的に） （　　）	

3 システム環境について

3-1. 貴組織のパソコン（オフコンも含む）の利用状況についてお答えください。［１つ選択］

１．１人１台、もしくはそれ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

3-2. 貴組織で保有しているサーバの台数とクライアントの台数をお答えください。

サーバ台数：（　　）台	クライアント台数：（　　）台

3-3. 貴組織でもっとも多く利用されている OS についてお答えください。［１つ選択］

１．Windows 98,Me	２．Windows NT,2000	３．Windows XP
４．Windows Vista	５．Windows 7	６．UNIX
７．Linux		
８．その他（　　）		

3-4. 貴組織で現在使用しているパソコンのうち、Windows 98 / Windows Me などサポートの終了している OS がインストールされている台数は、貴組織全体のどれくらいの割合ですか。最も近いものをお答えください。［１つ選択］

１．ない	２．数台程度	３．全体の半分以下
４．全体の半分以上	５．ほとんどすべて	

3-5. 貴組織では、Windows Update などの手段で現在使用しているパソコンにセキュリティパッチ（脆弱性の修正）を適用していますか。最も近いものをお答えください。［1 つ選択］

１．常に適用し、適用状況も把握している	２．常に適用しているが、実際の適用状況は不明
３．各ユーザに適用を任せている	４．ほとんど適用していない
５．分からない	

3-6. 貴組織の 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つ選択］

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（　　）

3-7. 下記①～⑨について、貴組織で利用されている情報システムやネットワーク機器の管理方法をそれぞれお答えください。［1行につき1つずつ選択］

	利用していない	自社で管理している	一部の管理を外部委託している	全ての管理を外部委託している	わからない
①Web サーバ	1	2	3	4	5
②メールサーバ	1	2	3	4	5
③ファイルサーバ	1	2	3	4	5
④データベースサーバ	1	2	3	4	5
⑤DNS サーバ	1	2	3	4	5
⑥クライアント	1	2	3	4	5
⑦基幹システム	1	2	3	4	5
⑧ルータ	1	2	3	4	5
⑨ファイアウォール	1	2	3	4	5

4 情報セキュリティ対策の実施状況について

4-1. 貴組織において、個人所有のパソコンの業務使用を許可制にするなどのように、業務で個人所有のパソコンを使用することの是非を明確にしていますか。［1つ選択］

1．明確にしている	2．明確にしていない
3．わからない	

4-2. 貴組織において、個人所有のパソコンを業務使用している人はいますか。［1つ選択］

1．いる	2．いない
3．わからない	

4-3. 貴組織において、個人ごとのパソコンや共有パソコンのログイン ID、パスワードを個人ごとに発行して共有しないなどのように、ログイン管理を行っていますか。［1つ選択］

1．行っている	2．一部行っている
3．行っていない	4．わからない

4-4. 貴組織において、情報セキュリティポリシーを定めていますか。［1つ選択］

1．公式なポリシーを定めている	2．非公式なポリシーを定めている[注1]
3．ポリシーはない	4．その他

注1）非公式なポリシーとは、組織で正式に承認されたポリシーではないものを指します。

4-5. 貴組織において保有している重要情報（個人情報、機密情報など）が何かを定め、それを社内で共有していますか。［1つ選択］

1．共有している	2．一部で共有している
3．共有していない	4．わからない

4-6. 貴組織において、重要情報の取り扱いに関する具体的なルール（重要情報を持ち出さない、施錠できるところに保管するなど）を定めていますか。［1つ選択］

1．定めている	2．定めている途中
3．定めていない	

4-7. 重要情報の取り扱いに関するルールは、守ることができるルールとなっていますか。[１つ選択]

※「4-6」の設問で「2. 定めている途中」または「3. 定めていない」を選択した方は、ご回答いただく必要はありません。

１．なっている	２．一部なっていない
３．なっていない	４．わからない

4-8. 貴組織において、情報セキュリティの教育が行われていますか。[１つ選択]

１．ほとんどすべての従業員（正社員や準社員）に対して行っている
２．一部の従業員（正社員や準社員）に対して行っている
３．特に行っていない
４．わからない

※「4-8」の設問で「1. ほとんどすべての従業員（正社員や準社員）に対して行っている」または、「２．一部の従業員（正社員や準社員）に対して行っている」を選択した方は、以下の 4-9、4-10 をお答えください。

4-9. 情報セキュリティの教育はどのような形式で実施していますか。[該当するものすべて選択]

１．集合型研修	２．e ラーニング	３．テキストの配布
４．ビデオの視聴	５．ミーティング	６．メール
７．社外講師による研修	８．グループ・ディスカッション	９．ケーススタディ
10. 危険予知トレーニング		
11. その他（ ）		

4-10. 情報セキュリティの教育はどのような内容を実施していますか。[該当するものすべて選択]

１．セキュリティポリシーやセキュリティルール
２．情報セキュリティに関する法律やガイドライン
３．ISMS やプライバシーマークなどの制度
４．社内で発生したセキュリティ事故/事件の事例
５．社外で発生したセキュリティ事故/事件の事例
６．ウイルスや不正アクセス等のネットワークセキュリティ
７．ソーシャルエンジニアリング
８．その他（ ）

５ 情報セキュリティ事故対応への準備状況について

5-1. 貴組織において、重要情報の流出や紛失、盗難があった場合の対応手順書を作成するなどのように、情報セキュリティ事故が発生した場合に備えた準備をしていますか。[１つ選択]

１．実施している	２．実施していない

※「5-1」の設問で「1. 実施している」を選択した方は、以下の 5-2 ～ 5-4 をお答えください。

5-2. 貴組織で実施している情報セキュリティ事故対応への準備をお答えください。[該当するものすべて選択]

１．連絡窓口（担当者）の設置	２．事故対応手順書の作成	３．事故対応手順書の見直し
４．重要情報のバックアップ	５．重要情報の復旧テスト	６．重要サーバ[注2]でのログ記録
７．ログの定期調査	８．重要サーバの予備機確保	９．証拠保全の手順書の作成
10. 事故管理台帳の作成	11. 事故報告書（雛形）の作成	12. 対外対応マニュアルの作成
13. 重要サーバの構築手順書の作成		14. 導入製品別問い合わせ先情報の管理
15. その他		

注 2) 重要サーバとは、重要情報を保存しているサーバや停止すると業務に支障がでるサーバを指します。

5-3. 情報セキュリティ事故対応への準備を行う際に参考にした情報をお答えください。

5-4. 情報セキュリティ事故対応への準備を行う際に不足していた情報がございましたらお答えください。

※「5-1」の設問で「2. 実施していない」を選択した方は、以下の 5-5 、5-6 をお答えください。

5-5. 貴組織において、情報セキュリティ事故対応への準備を行う必要性を感じますか。［１つ選択］

１．必要性を感じる	２．必要性を感じない

5-6. 情報セキュリティ事故対応への準備を実施する上での問題点を教えてください。［該当するものすべて選択］

１．投資対効果が見えづらい	２．担当できる人材が不足している
３．予算が不足している	４．知識やノウハウが不足している
５．経営者が必要としていない	６．特になし
７．その他 （ ）	

６ 情報セキュリティ事故の発生について

6-1. 貴組織で発生したことのある情報セキュリティ事故を教えてください。［該当するものすべて選択］

１．ウイルス感染	２．情報への不正アクセス	３．Dos 攻撃
４．金融詐欺	５．内部者のネット・アクセス乱用[注3]	６．通信詐欺[注4]
７．システムが BOT に悪用された	８．システム侵入	９．システムがフィッシングに悪用された
10．無線 LAN の無許可利用	11．インスタントメッセージの悪用	12．ファイル破壊／改ざん
13．ウェブの改ざん	14．パスワード盗聴	15．DNS サーバが悪用された
16．事務所内に部外者が侵入	17．ｼｽﾃﾑ破壊/損傷行為	18．顧客情報の誤送信・誤公開
19．顧客情報[注5]の盗難／紛失（ﾉｰﾄ PC 等携帯端末から）		20．顧客情報の盗難／紛失（USB 等可搬記憶媒体から）
21．顧客情報の盗難／紛失（紙媒体から）		
22．自社情報[注6]の盗難／紛失（ﾉｰﾄ PC 等携帯端末から）		23．自社情報の盗難／紛失（USB 等可搬記憶媒体から）
24．自社情報の盗難／紛失（紙媒体から）		
25．委託先から顧客情報が漏えいした		26．従業員の自宅から顧客情報が漏えいした
27．発生していない		
28．その他（ ）		

注３）内部のネット・アクセス乱用とは、「わいせつな画像のダウンロード」、「プログラム等の違法コピー」、「私用メール利用等」、「セキュリティポリシー違反」などを指します。
注４）通信詐欺とは、「通信サービスを提供したように見せ、その費用を他人からだまし取る」、「通信サービスの費用を他人のクレジットカード、電話等に請求させる」などを指します。
注５）顧客情報とは、顧客の個人情報や顧客の機密情報（ビジネスに係るノウハウなど）を指します。
注６）自社情報とは、従業員の個人情報や自社の機密情報（経営に係る情報など）を指します。

6-2. 情報セキュリティ事故の過去１年間の発生回数を記入してください。

※「6-1」の設問で「27. 発生していない」を選択した方は、ご回答いただく必要はありません。

	故意によるもの	過失によるもの	その他
外部要因			
内部要因			

7 情報セキュリティ事故が発生した時の貴組織の対応について

※「6-1」の設問で「27. 発生していない」を選択した方は、ご回答いただく必要はありません。

7-1. 内部的な対応として、どのような行動を取りましたか。[該当するものすべて選択]

１．加害者を特定しようとした	２．セキュリティホールをふさぐための暫定措置を施した
３．セキュリティパッチをインストールした	４．セキュリティソフトをインストールした
５．証拠保全を行った	６．代替設備（予備 PC など）への切替えを行った
７．データ復旧を行った	８．システムの再インストールを行った
９．組織のセキュリティポリシーを変更した	10. 外部機関に相談した
11. 追加のセキュリティハードウエアを導入した	12. 担当部門だけで処理した
13. その他	14. 何もしなかった

7-2. 届出を行った外部組織を教えてください。[該当するものすべて選択]

１．警察	２．監督官庁	３．IPA	４．JPCERT/CC	５．その他
６．届出を行わなかった				

7-3. 「7-2」の設問で「６．届出を行わなかった」を選択した方にお聞きします。

届出を行わなかった理由について該当するものを選択してください。[該当するものすべて選択]

１．外部からマイナスイメージを持たれるおそれがあったため
２．競合他社に利用されるおそれがあったため
３．報告をしようという考えに至らなかったため
４．社内対応で十分だと判断したため
５．警察／監督官庁は頼りにならないと思っているため
６．報告する程の事件ではなかったため
７．その他

アンケートは以上です。ご協力ありがとうございました。

※ 2010 年 8 月 6 日（金）までに、同封の返信用封筒にて「本用紙」をご返送ください。

「情報セキュリティ事故対応に関わるアンケート調査　調査報告書」