平成１６年度 マスターセンター補助事業

中小企業の情報セキュリティ

東海地区における中小企業の現状とその対策

平成１７年１月

社団法人 中小企業診断協会愛知県支部

目　次

はじめに

近年の情報技術革新の進展はすさまじく産業構造や企業経営のあり方に大きな変化をもたらしている。特にインターネットに代表されるネットワークシステムは、社会にとって不可欠なインフラとなっている。こうした状況は、高度情報化社会を目指す我が国にとっては好ましいことではある。しかし、利用者が増えるに従い、特にセキュリティや倫理の面からさまざまな問題が発生している。報道されているようにコンピュータウィルス、迷惑メール、不正アクセスなどの被害、そして企業からの情報漏洩事故などが相次いでおり、大きな関心をよんでいる。

こうした社会の流れを背景に、企業の情報セキュリティについてのレポートは多くでているが、そのほとんどは大企業もしくはそれに準ずる中堅企業についてのものである。事業所数では圧倒的に多い中小企業に関する情報セキュリティの実態は、殆ど明らかにされていないのが実情である。

そこで、中小企業における情報セキュリティの実情を明らかにして、今後のあるべきセキュリティ対策の指針を示すべく今回の調査を実施したものである。調査実施に際して、東海地方を中心に活動する私達は、当地区の中小企業に対象を絞って、情報セキュリティの実態を把握することとした。

今回の調査を通じて、中小企業の情報セキュリティの実態を明らかにし、セキュリティのあり方の方向性を多少なりとも示すことができたのではないかと考えている。

なお調査報告書作成に当たって、ご協力いただいた方々に誌面を借りて謝意を表する。

社団法人 中小企業診断協会 愛知県支部

第１章　調査実施概要

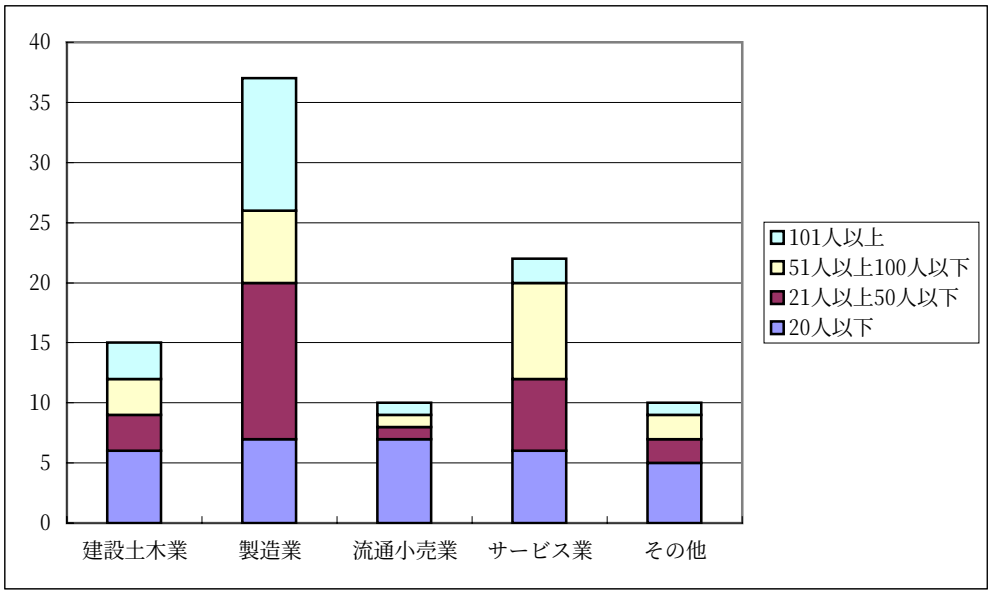
本調査は正確性を確保するために次の様式で実施した。アンケートの質問項目一覧は、巻末に資料として添付してあるので本報告書を読み進むにあたり参考にしていただきたい。

(1) アンケート実施方法

① 対象企業

平成１５年秋から平成１６年夏にかけて、メンバーの一部が東海地区の中小企業を対象に複数回セミナー・講演などを実施する機会があり、都度、参加企業にアンケートへの協力を依頼した。最終的に９４社から回答を得ることが出来た。

回答企業全体(母集団)の業種および従業員規模をあらわしたものが下のグラフである。



② ブラウザによるＷＥＢへ回答入力

企業担当者の簡便な回答を可能にするとともに、回答集計の簡素化をねらいとしてブラウザでインターネット上に回答する方式を採用した。

紙ベースではなくシステム化することで、全ての質問項目に回答しないとアンケートが完了しない仕組みとしたため、無回答(空白回答)を無くしデータの信頼性が高まった。

③ 無記名回答

回答企業のプライバシーを尊重し正確な実情を収集するために、無記名回答とした。ただし、回答企業の業種等の最低限の基本情報は収集した。

④ 対面回答

情報セキュリティに関するアンケート内容は、質問項目に専門的用語が使われることが多いため、ＩＴやセキュリティに関する知識が無いと正しく回答できない場合がある。このため、今回は企業

が回答する間、メンバーが傍らで待機し、質問があれば全て詳細に説明をすることで、正しい回答が得られるように努めた。

回答企業が質問に疑念を持つことなく回答できる環境を提供することで、より正確なデータ収集が可能になったと考える。

(2) アンケート質問項目

全３６項目を用意した。各質問項目の目的は以下のとおりである。

① 企業属性　(問１～問4)

回答企業の業種・規模などを把握する。

② 情報化の現状　(問５～問８)

現在の情報化の度合いを把握する。

③ 情報セキュリティに対する現状認識　(問９～問１３)

企業のセキュリティに対する意識を調査する。

④ ウイルス感染の実態　(問１４～問１９)

もっともオーソドックスなＰＣウイルスの感染有無と被害の実態を調査する。

⑤ 制度的(人的)対策の実態　(問２０～問２４)

セキュリティ対策の一環としての教育やルール制定の現状を調査する。

⑥ 物理的対策の実態　(問２５～問２７)

建物や機器の設置方法など物理的対策の現状を調査する。

⑦ 技術的対策の実態　(問２８～問３３)

システム上の対策の現状を調査する。

⑧ 今後の取り組み姿勢　(問３４～問３６)

将来への情報セキュリティ対策の展望を調査する。

アンケートの実施風景

第２章　アンケート結果の考察

１．情報セキュリティに対する現状認識（アンケート問９～１３）

(1) セキュリティに対する意識

情報セキュリティが重要である、と回答した企業は９６％と、大半の企業がその必要性を十分に認識している。企業規模の大小にかかわらず日常的にＩＴを活用する場面が多くなり、情報セキュリティ対策は避けて通れない、という意識が幅広く浸透している事実を示している。

問９　ＩＴの利用が進む中で、情報セキュリティ(安全対策)は重要だとお考えですか

重要である	それほど重要とは思わない	よくわからない
９０(96%)	２ (2%)	２ (2%)

ところで、情報セキュリテイが重要だと回答した企業のうち、なぜ必要と考えるかについての回答は、「ウイルスに感染すると困る」が９０社中５９社と最も多く、次いで「取引先などに迷惑がかかるから」が４７社となっている。コンピュータウイルス被害がマスコミなどで取り上げられる機会が多くなり、「感染したくない」という単純な動機で安全対策を必要と感じている、ととらえることもできる。本来、企業が最も意識しなければならない「取引先などに迷惑がかかるから」が２番目であったのは残念であるし、今後中小企業に対してこうした点を重点に意識の啓蒙を行う必要があるかもしれない。

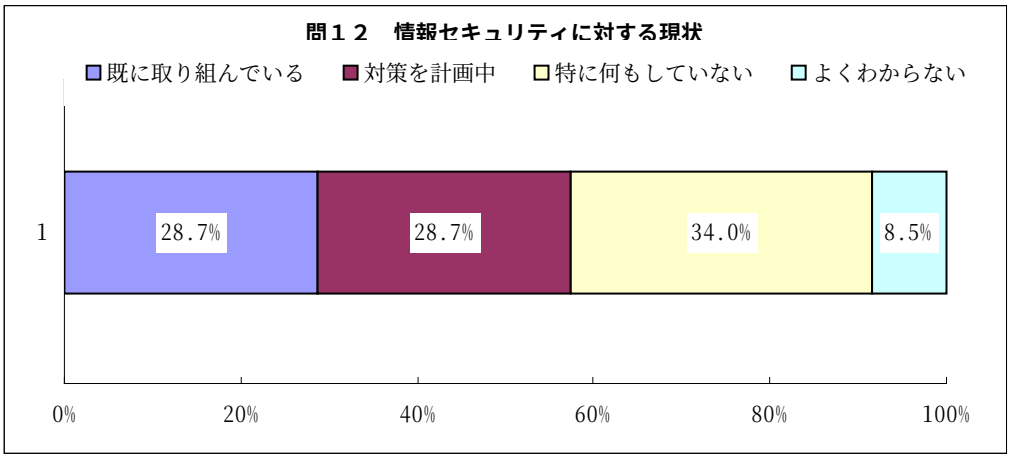
問１０　情報セキュリティはなぜ必要だと思いますか(２つまで)

ウイルスに感染すると困るから	取引先などに迷惑がかかるから	自社が多額の経済的損失を被るから
59	47	41

(2) 情報セキュリティ取り組みの現状

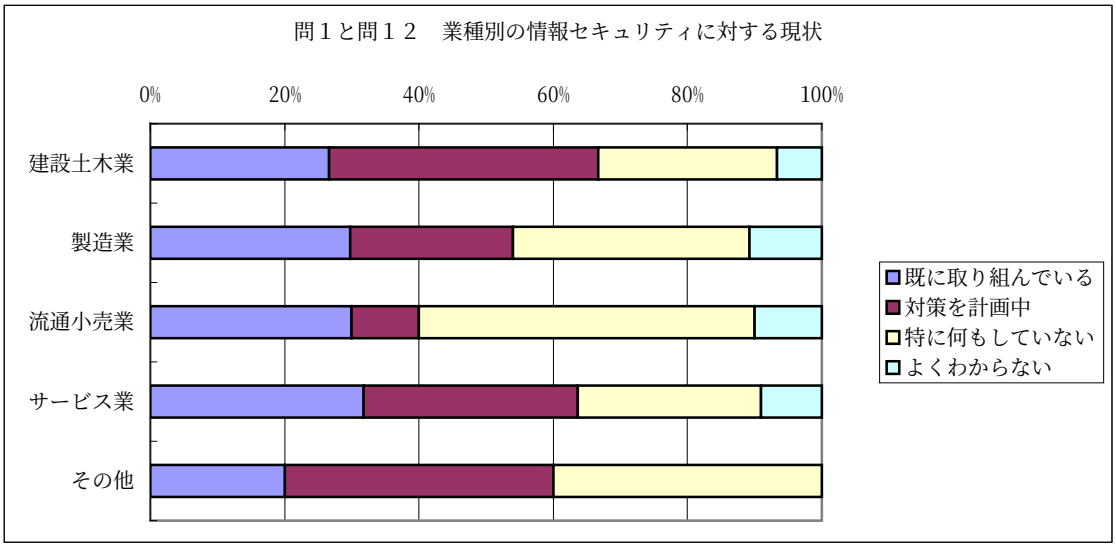
① 全体

実際の情報セキュリティ対策に対する取り組み状況は、「既に取り組んでいる」(２９%)、「対策を計画中」(２９%)と合わせると６割近くの企業が前向きな姿勢であることがわかる。



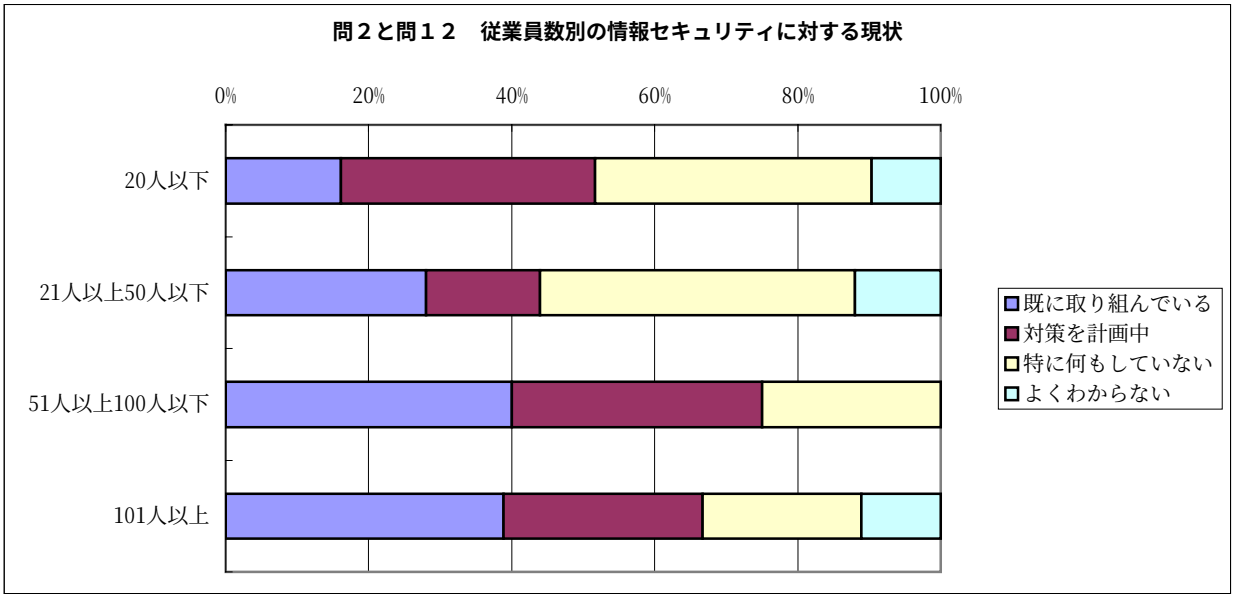
② 業種別

業種別に取り組み状況を見ると業種間では大きな差は無いものの、流通小売業が若干低め(40%)なのは、従業員数が少ない事業所が多いこと、すなわち小規模な事業所が多いことと関連がありそうである。



③ 従業員数別

次に従業員数別に取り組み状況を見てみると、「既に取り組んでいる」企業の比率は従業員数の大小と関連性がありそうである。企業規模が大きくなるにつれ、具体的な対策を既に行っている傾向があると言える。



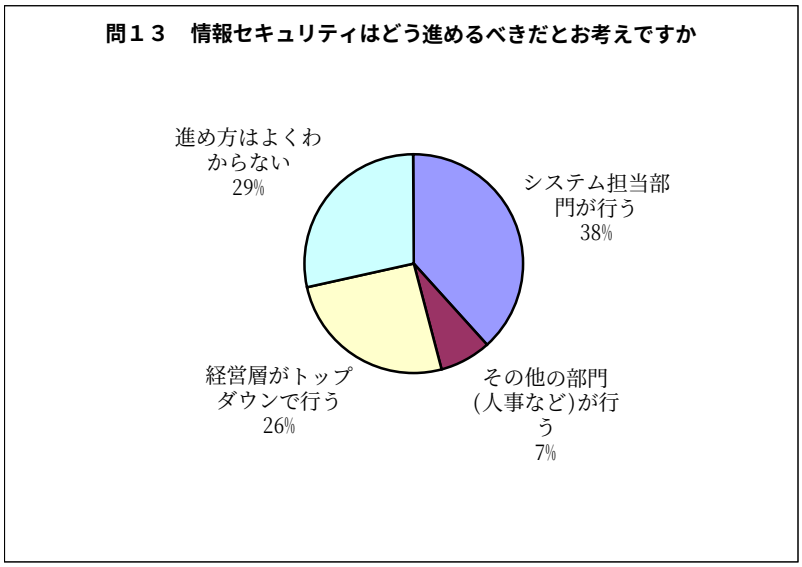
以上から、情報セキュリテイの重要性に関しては企業規模の大小を問わず、広く認識されているにもかかわらず、具体的な取り組みとなると小規模な企業ほど立ち遅れているという現状が見てとれる。

(3) どのように進めるのか

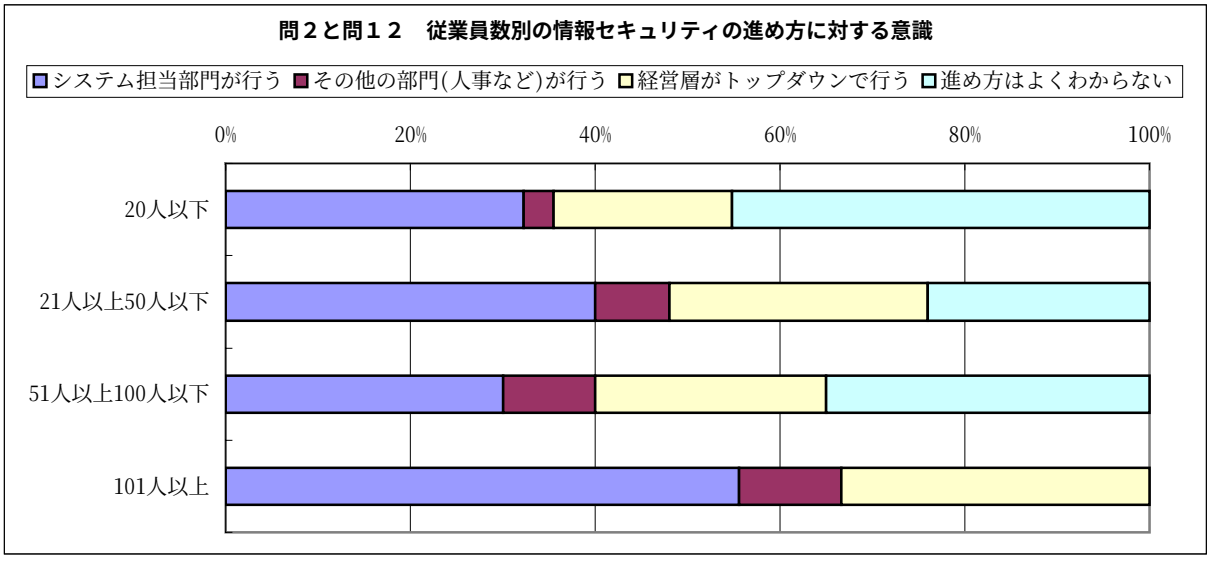
情報セキュリティはどう進めるべきかという問いに対しては、「システム部門が行う」(３８%)と最も多く、次いで「経営層がトップダウンで行う」(２６%)であった。

一般に企業の情報セキュリティ対策は、システム部門任せにすることなく、リスクマネジメントの一環として全社的に取り組むことが重要であると言われている。この一般論にしたがえば、回答企業群の４割近くは誤った意識であることがわかる。

また、約３割の企業が「進め方はよくわからない」と回答している。情報セキュリティの重要性は認識していても、具体的に取り組むためのノウハウが乏しいなどの理由で対策の実施に足踏みをしてしまっている現状を見ることができる。



この「進め方はよくわからない」と回答した企業を従業員数別に見ると、２０人以下の企業では実に６割超なのに対し、１０１人以上の企業ではゼロであった。単純に企業規模の大小に比例しているわけではないが、従業員数が少ない経営規模の小さな企業ほど、関連する情報やノウハウが乏しいため、進め方がわからず手をこまねいている現状があらわれている。



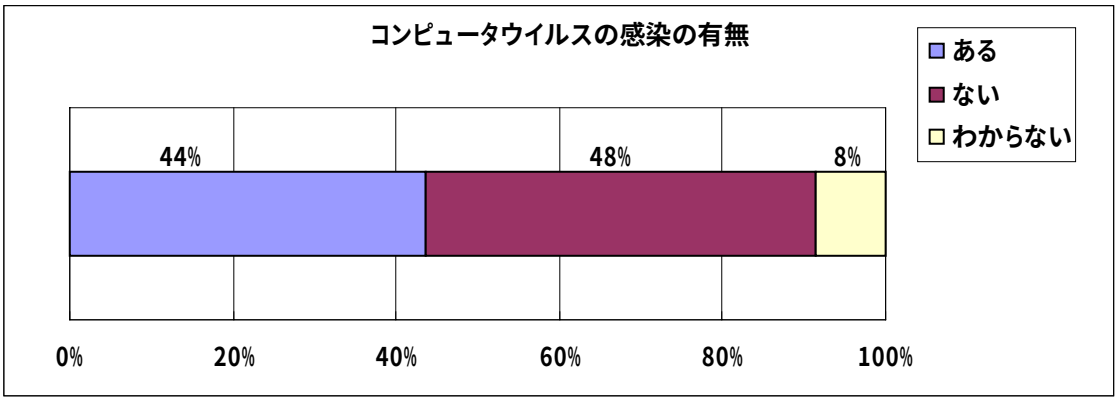
２． 被害の実態（アンケート問１４～１８）

(1) コンピュータウイルスの感染

中小企業だからウイルス感染はないとか大丈夫というのは絶対にありえない。また毎年進化したウイルスが世界中でつくられ、多くの種類が発見されている。

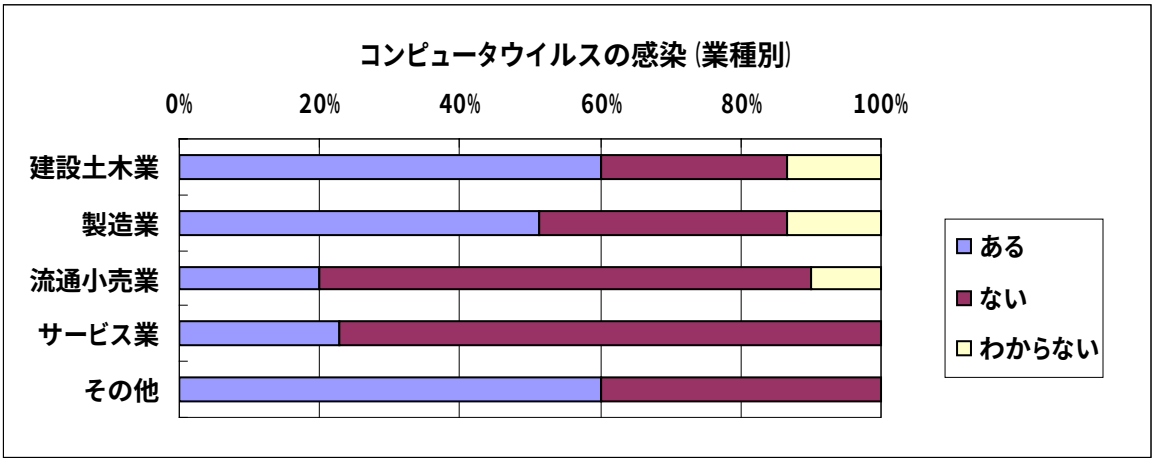
中小企業ではコンピュータウイルス被害の程度がどれほどか、実態を調べてみた。

まず、「コンピュータウイルスの感染の有無」では、「ある」が４４%、「ない」が４８%であり４割以上が感染を経験しており、感染をしていない企業がわずかに多い結果となった。



上記のアンケートの結果をもう少し詳しく内容分析してみた。

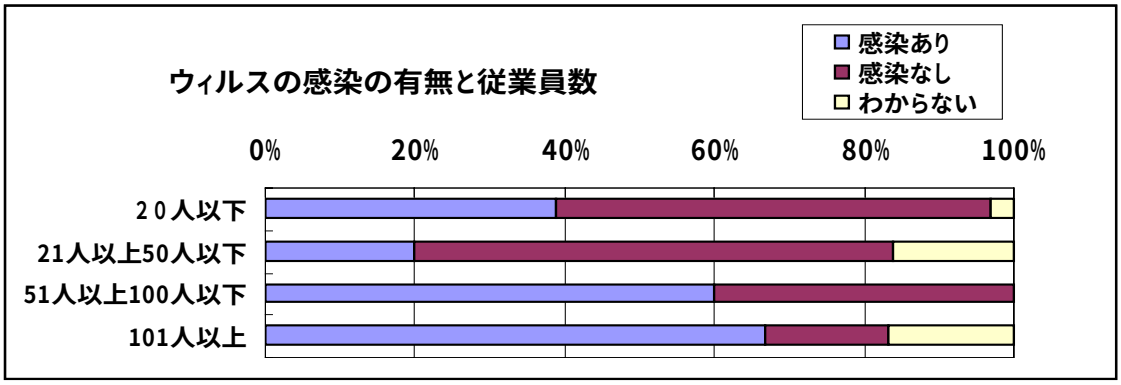
ウイルス感染の有無を業種別で調べたが、建設土木業・その他の業種で６０%と全業種平均（４４%）をかなり上回っている。次に製造業が全業種平均より少し高めとなっているが、逆に流通小売業・サービス業ではかなり低い数値となっている。しかし、感染の程度が高い、低いはあってもすべての業種が感染しており業種別の例外はない。



また、ウイルスの感染の有無と従業員数の関係についても調べてみた。

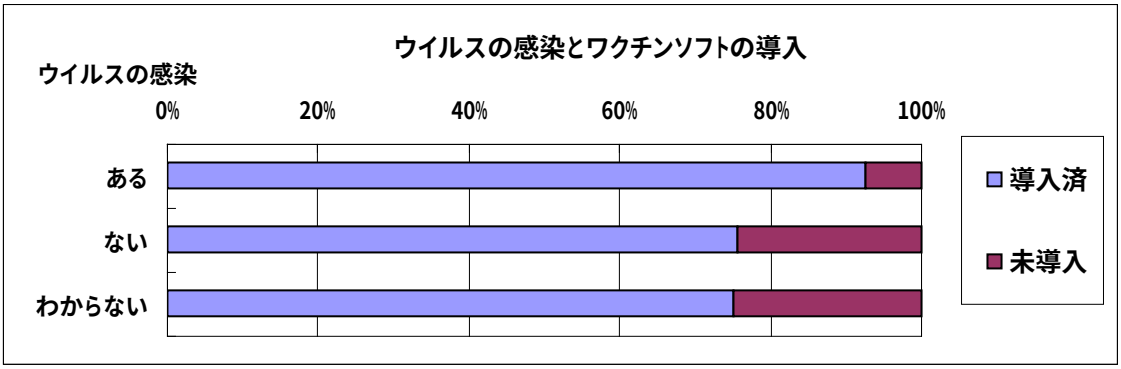
従業員数が増えれば（一般的には従業員数に比例して保有コンピュータ数も増えることになる）感染の程度に違いがあるかどうか調べたが、従業員数が多いほど感染の割合が増えてくるという結果になった。しかし、感染の程度が最も低かったのは２１～５０人の従業員規模であった。後述の「従業

員数と復旧に要した期間」の表でも２１～５０人規模は５１～１００人および２０人以下の従業員規模と比較すると、“一日で復旧した期間”という最短期で復旧した比率が高くなっている。この規模は組織として管理しやすいのかもしれない（但し、これだけの情報ではもちろん断定できない）。



最後に、ウイルスの感染の有無とワクチンソフトの導入の関係を調べたのが次表である。

ウイルス感染を経験したところは 9 割以上の企業がワクチンソフトを導入済であるが、「感染がない」、「わからない」と答えた企業では約４分の１がワクチンソフトをまだ導入していない。かなり導入企業は増えてきていると思うが、ウイルスの感染の有無によってワクチンソフトの導入に対する認識の差がでている。しかし、感染を経験していても約１割の企業はワクチンソフトをいまだ未導入としている。ウイルスに感染して被害が発生してからでは遅いと思われるが（もちろん「感染がない」・「わからない」の未導入企業も含めて）。

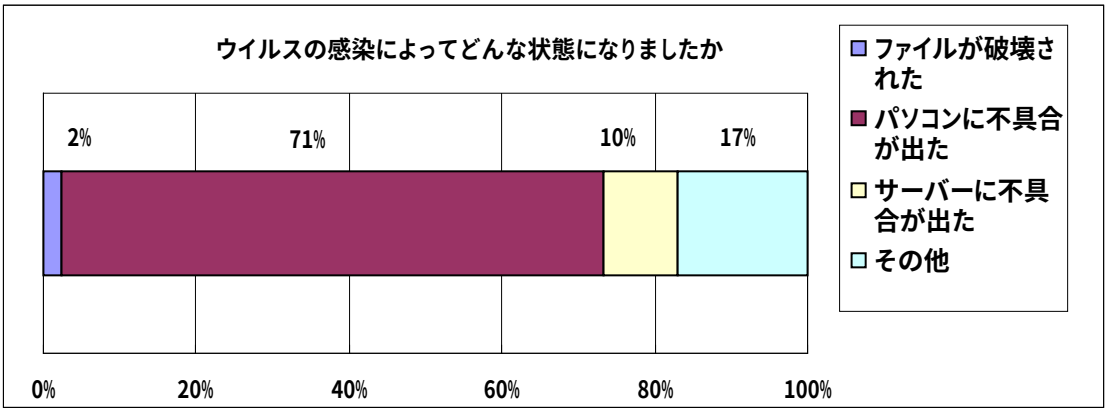


(2) ウイルスの感染およびその被害の程度

ウイルスの感染率は４割以上となったが、ではウイルスに感染した企業では「どのような状態」になっただろうか。

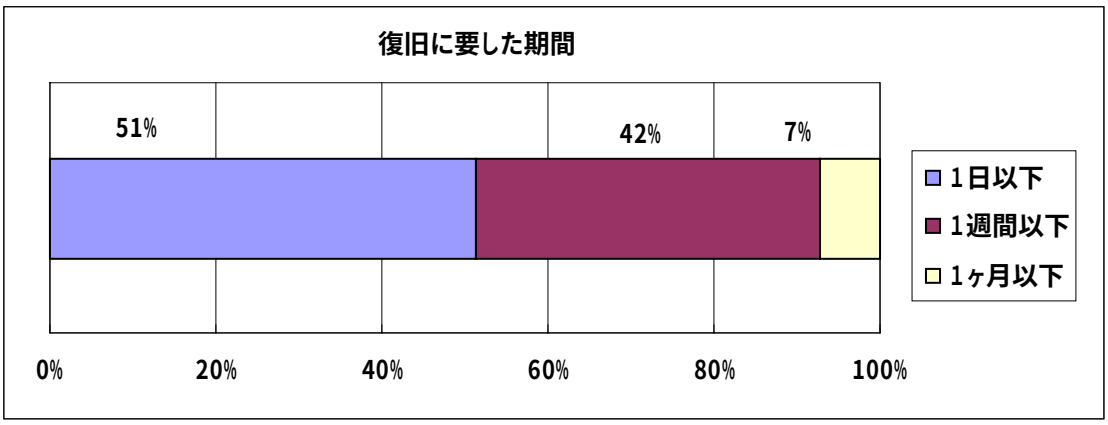
「パソコンに不具合が出た」が最も多く７１%でトップである。個々のパソコンにワクチンソフトがインストールされていなかったか、ワクチンソフトが最新のパターンファイルに更新されていなかったのが原因と考えられる。次に「その他」、「サーバに不具合が出た」、「ファイルが破壊された」と

続く。ここでは「その他」が１７％と多くなったが、当初こちらで想定していた以外の事例が発生している。

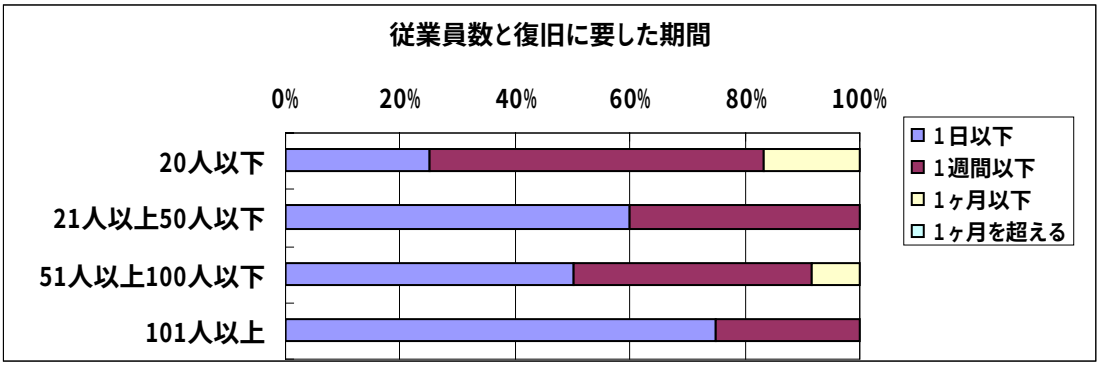


次に、ウイルスの被害をうけた企業が復旧までどのくらい要したかを質問した。

「１日以内」が５１％、「１週間以内」が４２％となっている。１週間以内（合計９３％）でほとんど復旧していると考えてもいいだろう。しかし、１ヶ月以内（１週間以上）が 7%ある。つまり、ウイルスには多様な種類があり、ウイルスの種類・その後の対応によっては復旧まで時間が長くかかることがあると考えたほうがよい。

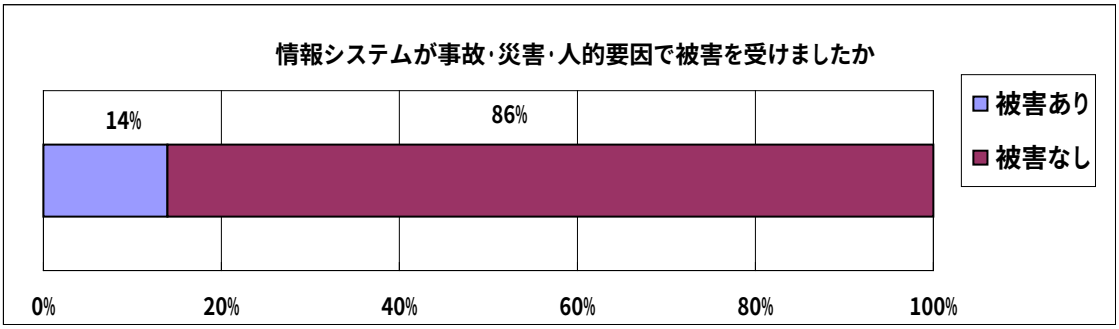


また、従業員規模で復旧期間をみると１０１人以上の規模の企業ではウイルスに感染しても短い期間で復旧しているが、逆に２０人以下の規模ではウイルスに感染すると復旧するまで長くかかっている。

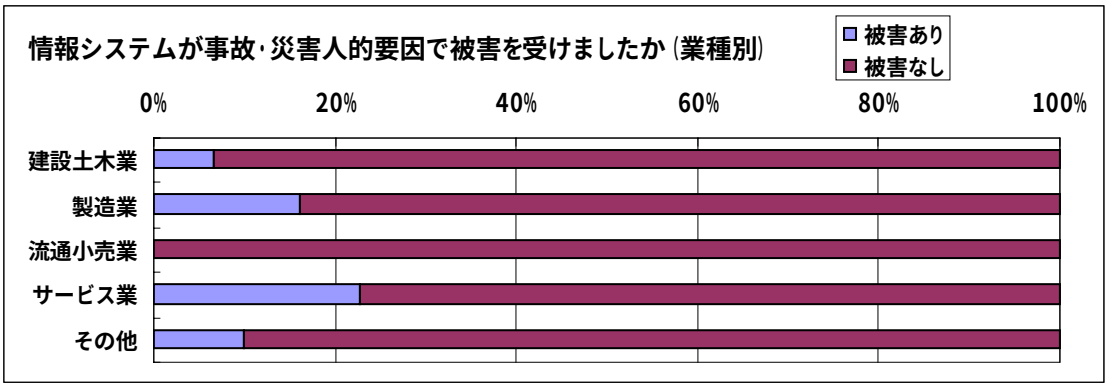


(3) コンピュータウイルス以外の情報システム被害（事故・災害・人的要因による被害）

ウイルスの感染以外で情報機器、システムが何らかの原因で事故を発生し被害を受けたことがあるかきいた。「被害あり」が１４%、「被害なし」が８６%とかなり多くの企業が“被害がない”と回答した。ちなみに、ウイルスの感染では「ある」が４４%、「ない」が４８%と回答しているので、被害の比率を単純に比較すると情報機器、システムの安全確保のほうが事故発生率は低い。ウイルスの感染よりも自社で管理しやすいか、または単純に事故発生が少ないと考えられる。

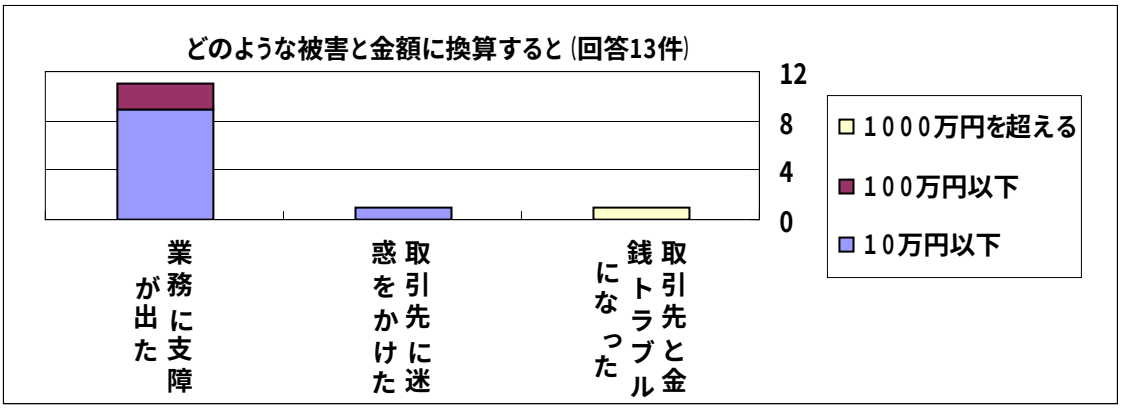


被害を受けた企業を業種別でみるとサービス業・製造業が全体を比較して高く、その他の業種・建設土木業では低めとなった。しかし、流通小売業では被害はゼロであり業種間でかなりばらつきが認められる。



次に、情報機器・システムに災害・人的要因等で物理的な事故があったと回答した企業でどのような被害を受け、また被害の種類とその程度を金額概算で回答してもらった。

「業務に支障が出た」が１１件、「取引先に迷惑をかけた」が１件、そして「金銭的トラブル」は１件であった。業務になんらかの支障が出たというのがほとんどで、とりあえず社内で被害がおさまっており、業務に支障が出たケースは被害が１０万円以下で多数となっている。しかし、取引先と金銭的なトラブルになったケースは１０００万円以上と金額がかなり大きくなっていることに注目したい。



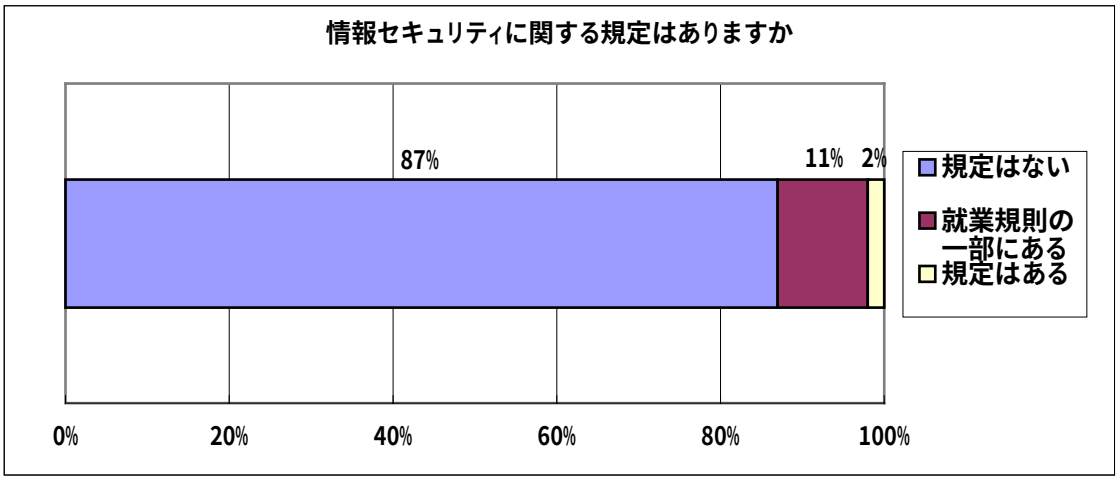
３．制度的対策の状況（アンケート問２０～２４）

情報セキュリティにおける制度的取り組みについて、その実施状況を質問した。

(1) 情報セキュリティに関する規定（問２０）

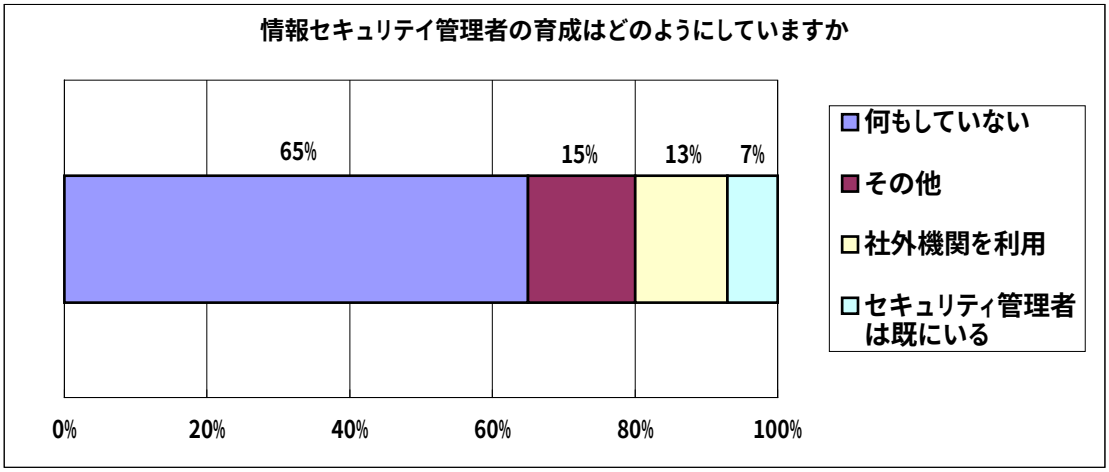
情報セキュリテイに間する規定が制定されているかについて質問した。情報セキュリテイに対する現状（問１２）において既に取り組んでいる企業が２９%あるとの回答を得ているため、ほぼ同様の結果が得られるものと期待していたが、８７%が「ない」、１１%が「就業規則の一部にある」と回答し、「ある」と回答した企業はわずかに２%であった。

このことは、個々の対策は実施しているものの、ほとんどの企業では、どのような方針の下、どのような対策を、どのような手順で実施するのか、をまとめたセキュリティポリシーは策定していないことを示している。しかし、今後の取り組み（問３４）として、１７%の企業が「セキュリティポリシーの策定」を挙げていることから、今後、情報セキュリテイに関する規定を制定する企業が増えてくる事が期待できる。



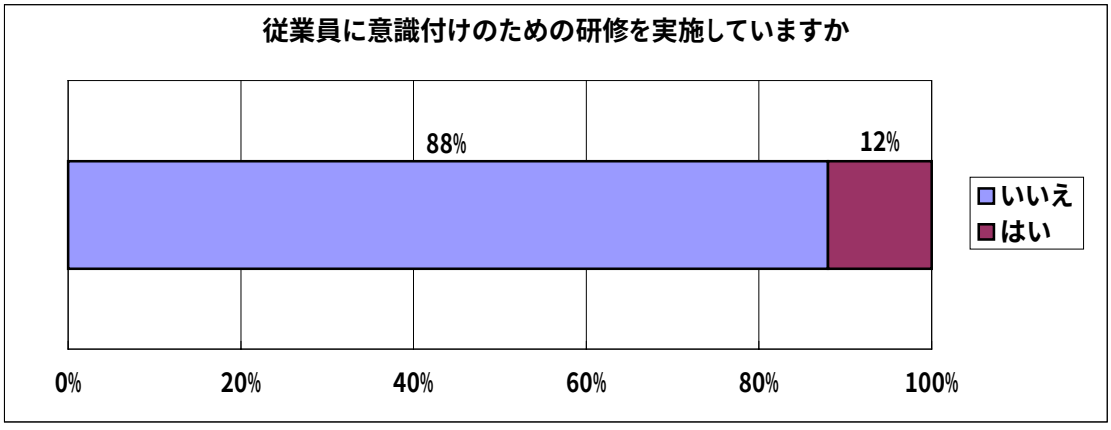
(2) 情報セキュリティ管理者の育成方法（問２１）

情報セキュリティ活動のリーダーとして管理者の育成をどのようにしているのかを質問した。回答企業のうち、「社外機関を利用」と回答した企業が１３%、「セキュリティ管理者は既にいる」と回答した企業は７%という結果だった。２０%の企業が育成のため何らかの対応を実施している事になる。一方「何もしていない」企業が６５%もあり、情報セキュリティの組織的推進の中心人物である管理者の育成について実際の行動を起こしていない企業が多い事がわかった。



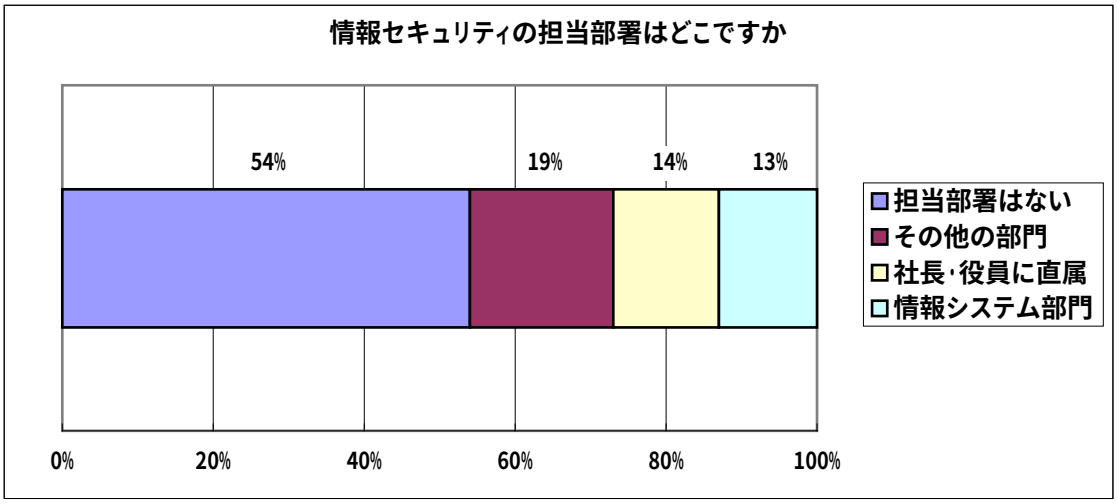
(3) 従業員のための研修実施の有無（問２２）

従業員に情報セキュリテイの意識付けのために研修を実施しているか質問した。「はい」と回答した企業が１２%と、問２１での情報セキュリティの管理者の育成のためなんらかの対応をしている企業より少ない結果を示した。

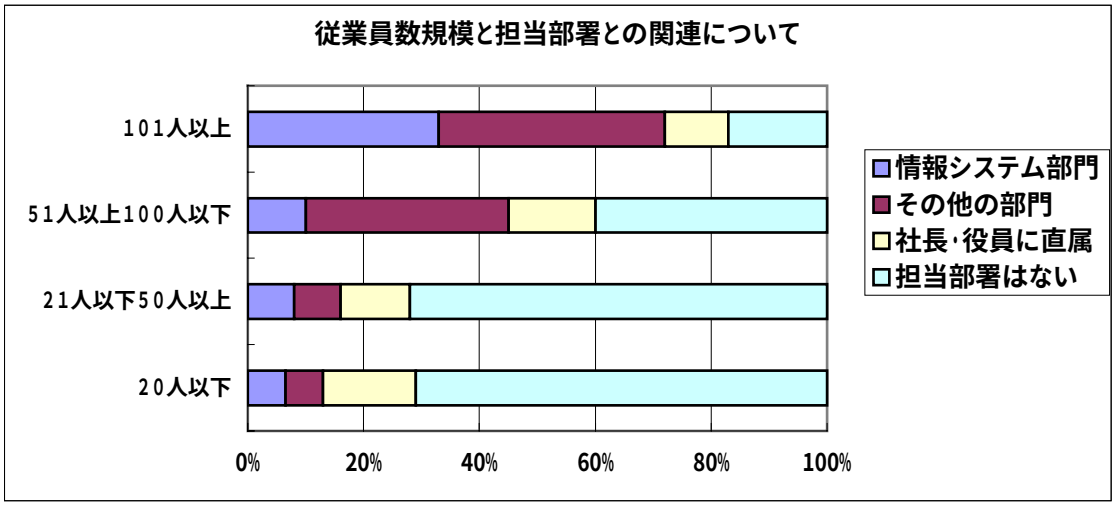


(4) 情報セキュリティの担当部署（問２３）

情報セキュリティを担当している部署がどこかについて質問した。回答企業の１４%が「社長・役員に直属」、１３%が「情報システム部門」と回答し、組織的に情報セキュリテイに対処している企業が４６%であることがわかる。しかし、情報セキュリテイの取り組み状況に関する質問（問１２）において、計画中も含め取り組んでいる企業が５８%であることから個人単位で情報セキュリテイに対処している企業が少なからず存在することがわかった。

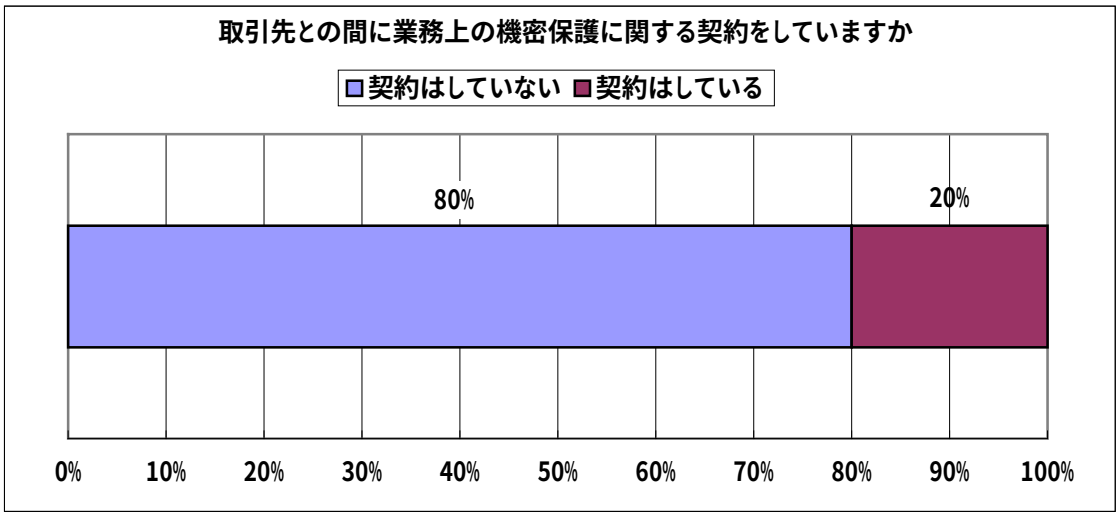


また、下図は従業員数規模との関連を見たものだが、従業員数が多い企業ほど情報セキュリティの担当部署が決まっていると回答した企業が多く、従業員数が少ないほど「担当部署はない」と回答した企業が多いことがわかる。従業員数の少ない企業においては、情報セキュリティ担当の部署での組織的な活動ではなく、個人単位での活動が主となっていると考えられる。

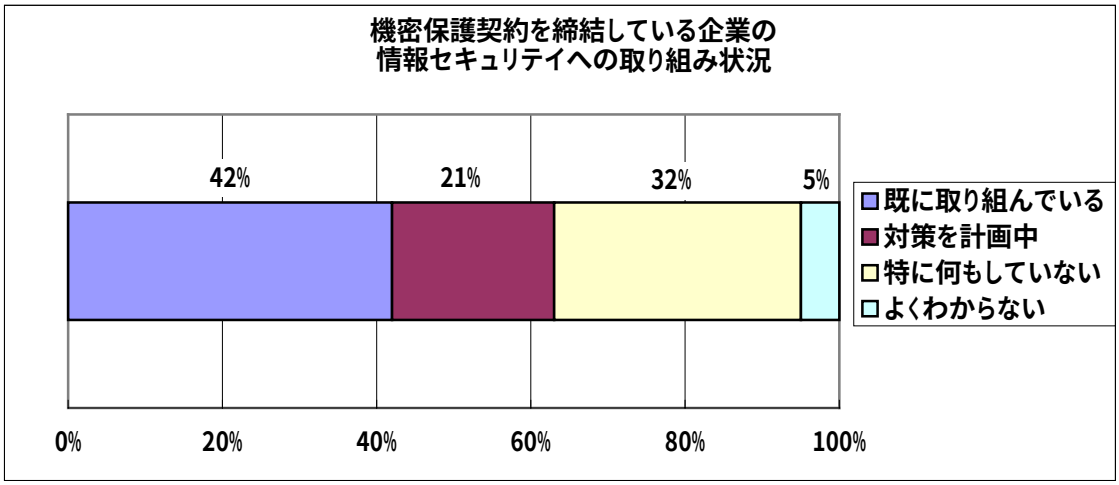


(5) 取引先との機密保護の契約（問２４）

取引先と業務上、機密保護に関する契約をしているかを質問した。回答企業の８０%が「いいえ」、２０%が「はい」と回答した。この質問は、企業の情報セキュリテイの対応状況とは直接関係はないが、知的財産権の保護、個人情報保護などの無形の資産や財産を保護しようとする気運が高まっている現在、注目すべき問題である。つまり、機密保護契約を締結している企業は、取引上知り得た機密を第三者に漏らすことを禁じられているわけであるが、同時に第三者に漏らさないよう対策をすることを要求されているともいえる。質問の回答から見ると、２０%の企業が情報セキュリテイの対策を実施することを要求されている事を示している。



さらに、下図は機密保護契約を締結している企業の、情報セキュリテイの取り組み状況を示したものである。「特に何もしていない」、「よくわからない」と答えた３７%の企業は、どのように機密保護契約を遵守しようとしているのか非常に心配である。

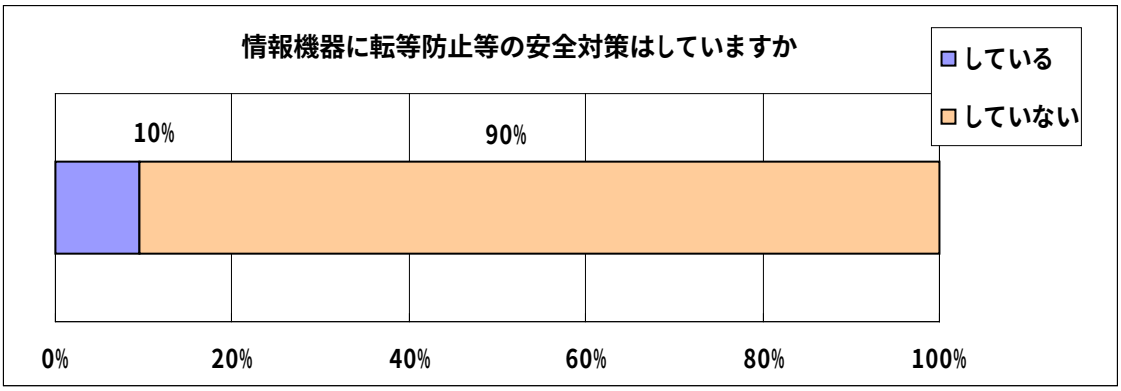


また、機密保護契約を締結している企業割合は、現在２０%であるが、将来、ＩＳＭＳ（Information Security Management System）の認証を取得した企業が増加し、認証を取得した取引先から業務上の機密保護に関する契約を要請される事が多くなると予想されるため、この割合は増えていくことが推測できる。ここで注意すべきことは、当該企業の情報セキュリティに関する社内体制が整わない状態で契約を結び、自社の責任により契約に違反した場合、契約の内容にもよるが損害賠償を要求される可能性がある。賠償額にもよるが、資本力が比較的脆弱な中小企業にとっては命取りにもなりかねない。また、何よりも信用の失墜が企業経営上致命的な打撃となる。機密保護契約を締結する場合は、それなりのリスクが生じることがあることも心しなければならない。

４．物理的対策の状況（アンケート問２５～２７）

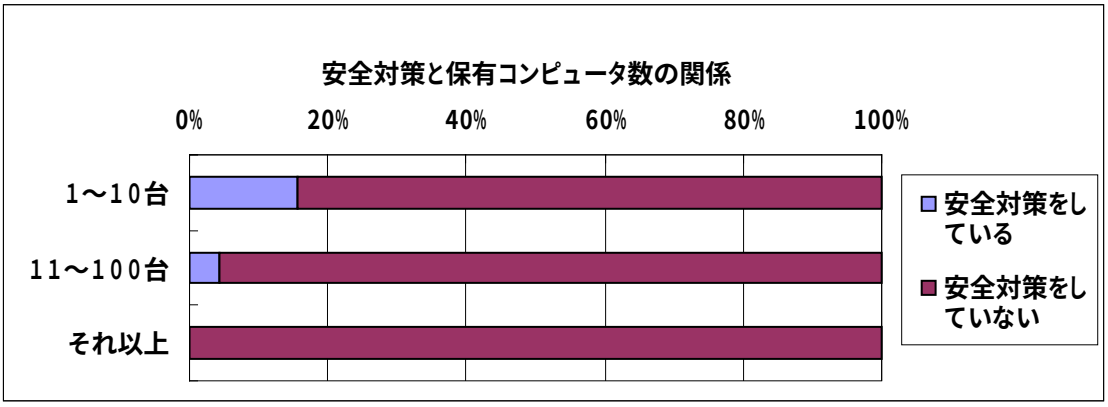
(1) 情報機器の保全状況

台風・地震等の自然災害、火災・停電等の事故に対して情報機器の転倒防止策・水害等の安全対策がどの程度実施されているかをみてみると、ウイルスの被害の実態(アンケート問17～19)ほど多くない。ご当地東海地区にまもなく発生するといわれている東海地震のために何か対策を実施しているのではないかという希望も含めてきいたが、「している」が１０%、「していない」が９０%と残念ながら安全対策はそれほど施されていない状況であった。

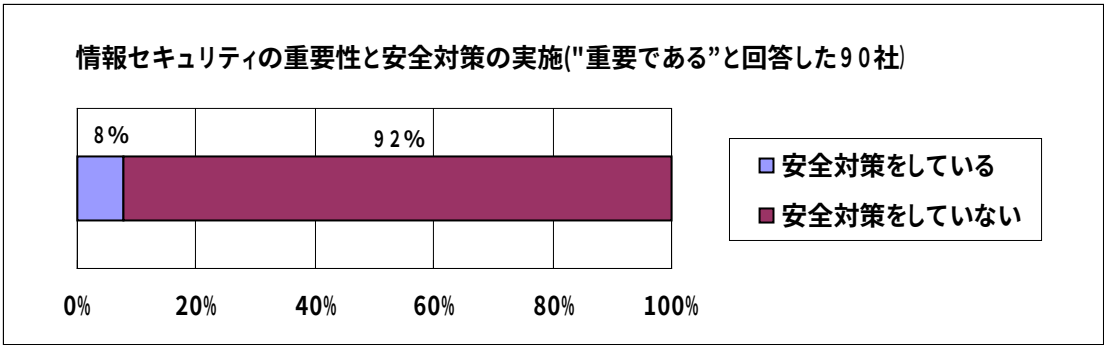


そして、安全対策と保有コンピュータ数に関係があるか調べたのが次表である。

保有コンピュータ数が多くなるほど安全対策をしていない企業の割合が増え、１０１台以上（それ以上）保有する企業では全企業が安全対策はしていない結果となった。コンピュータが増えれば費用が台数に比例でなく級数的に増大すること、および専門的な人材が社内にいないか不足しているのが原因と考えられる。

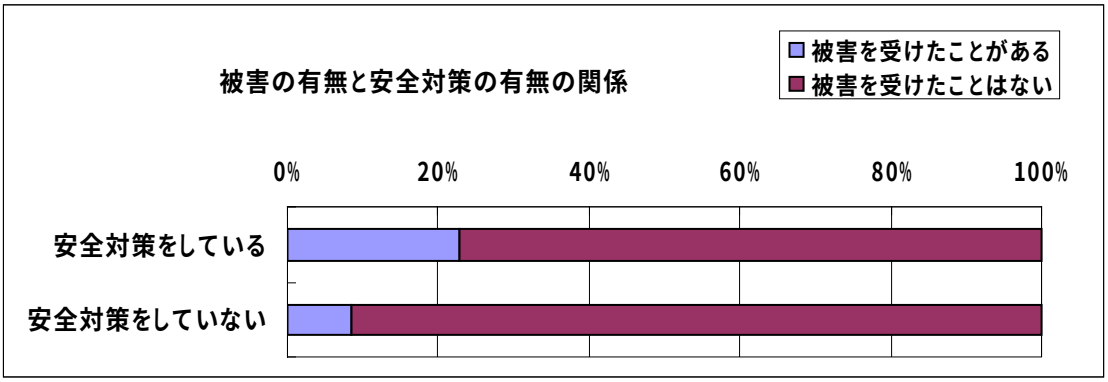


それでは、“情報セキュリティが重要”と考えている企業（アンケート問９で９４社中９０社）のうち、この安全対策がどれほど実施されているのか調べてみると、８%しか実際に安全対策は施されていない。認識はされていても実施するのは大変という現状が見てとれる。



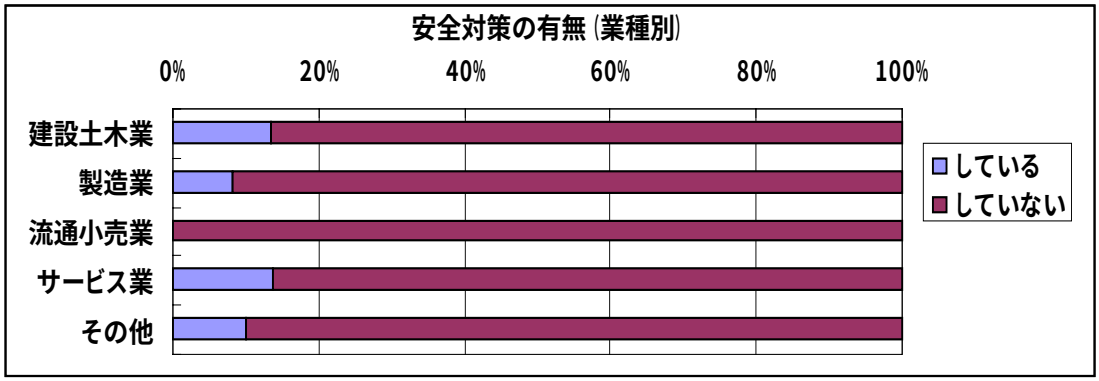
また、安全対策の実施の有無と安全対策で事故が発生したかの有無の関係を調べた。

安全対策をしている企業の方が被害を受けた比率が高い。被害を受けてしまったから安全対策をしたのではないかとも考えられる。



最後に、安全対策について業種別で特徴があるか調べた。

安全対策を「している」が多い業種は建設土木業・サービス業で１３%前後、次にその他の業種・製造業と続くが流通小売業では安全対策がゼロという結果であり、業種間で差がでている。

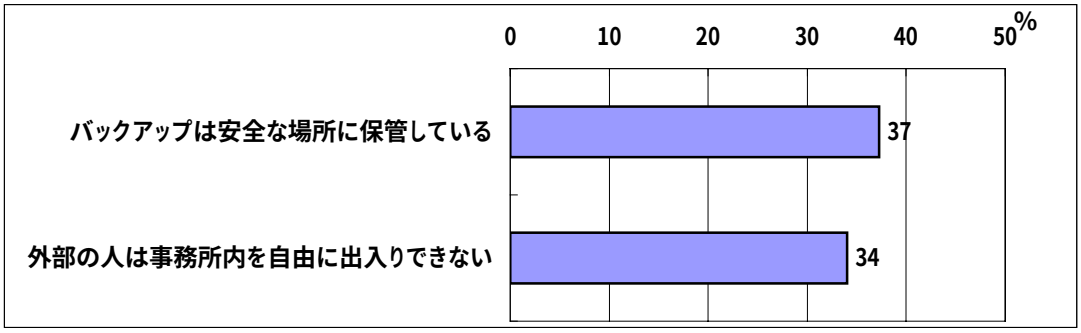


(2) 安全なバックアップデータの保管、事務所の出入り規制

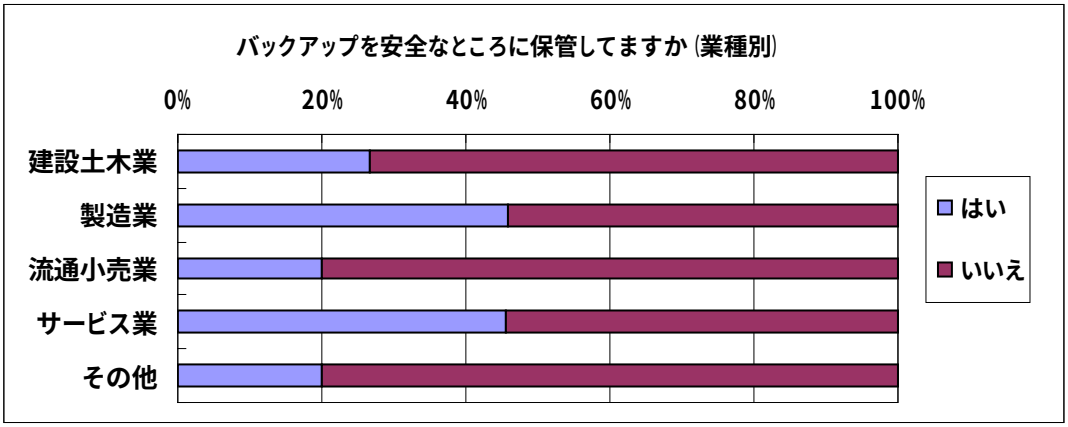
「もしものときにリストアできるバックアップデータがどのような状態で保管されているか」、および「部外者が事務所内を自由に出入りできるか」をきいた。

「バックアップは安全な場所に保管している」が３７%、「外部の人は事務所内を自由に出入りで

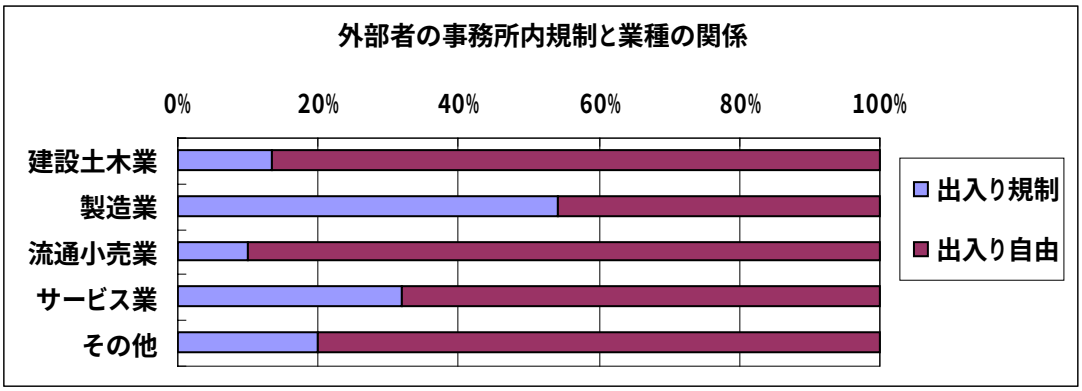
きない」が３４％であった。裏返せばバックアップは６割以上が安全でない場所に保管されていること、及び６割以上の事務所は外部者が自由に出入り可能であることを企業が認めていることである。企業にとって重要な情報機器・データを守るという認識が低いと感じられる。



バックアップデータの保管を業種別でみると製造業とサービス業では“安全な場所に保管”は高い比率となっているが、建設土木業・流通小売業・その他の業種は平均より低くなっている。



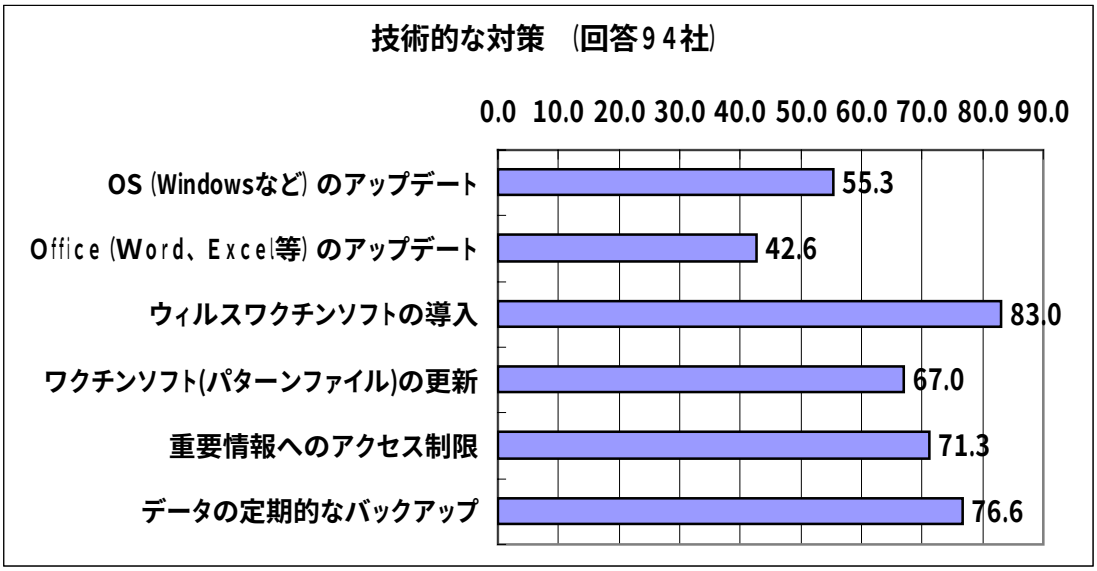
部外者の事務所内への出入り規制を業種別でみると製造業の割合が他と比べてかなり多いが、以前から製造業では工場全体を入場規制する場合が多く、情報セキュリティだけでなく安全面・衛生面を含めて対策が取られているためと考えられる。建設土木業・流通小売業・その他の業種は低くなっている。



５．技術的対策の状況（アンケート問２８～３３）

(1) 概要

情報セキュリティに対する技術的な対策として、OS（Windows など）のアップデート、Ｏｆｆｉｃｅ（Ｗｏｒｄ、Ｅｘｃｅｌ等）のアップデート、ウィルスワクチンソフトの導入、ワクチンソフト(パターンファイル)の更新、重要情報へのアクセス制限、データの定期的なバックアップの６項目についてその実施状況を質問した。下図は各対策の実施率を示すグラフである。



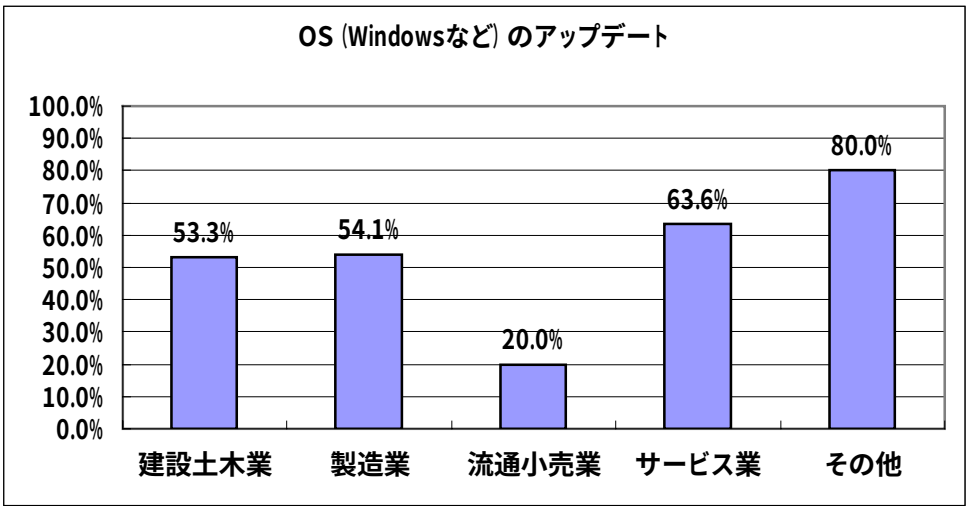
技術的対策として中小企業が実施しているもので、最も普及しているものは「ウィルスワクチンソフトの導入」であり、全体の８３%が実施している。しかしまだ２割弱はウィルスに対して無防備状態にあるとも言える。またウィルスワクチンソフトを導入しても、パターンファイルを更新していない企業も１６%程度あり、それも含めれば全体の３３%すなわち３社のうち１社がウィルスに感染する恐れがあるといえる。

次に実施率の高い対策は「データのバックアップ」で、全体の７７%が実施しているという回答であった。また、「重要情報へのアクセス制限」も７１%となっており、この対策については当初想定したよりも意識が高い結果となっている。

「Ｗｉｎｄｏｗｓのアップデート」は５５%、「Ｏｆｆｉｃｅのアップデート」は４３%という実施率であった。Ｏｆｆｉｃｅのアップデートがあまりなされていないことはある程度予想されたが、Ｗｉｎｄｏｗｓのアップデートについては意外と低い結果であった。この辺はウィルス感染と、ＷＥＢ環境下での脆弱性との違いが識別されていないことによるものと思われる。「ウィルスワクチンソフトを入れてあるから大丈夫」という安易な認識を、ＩＴ活用を支援する立場にある者は是正していく必要があろう。

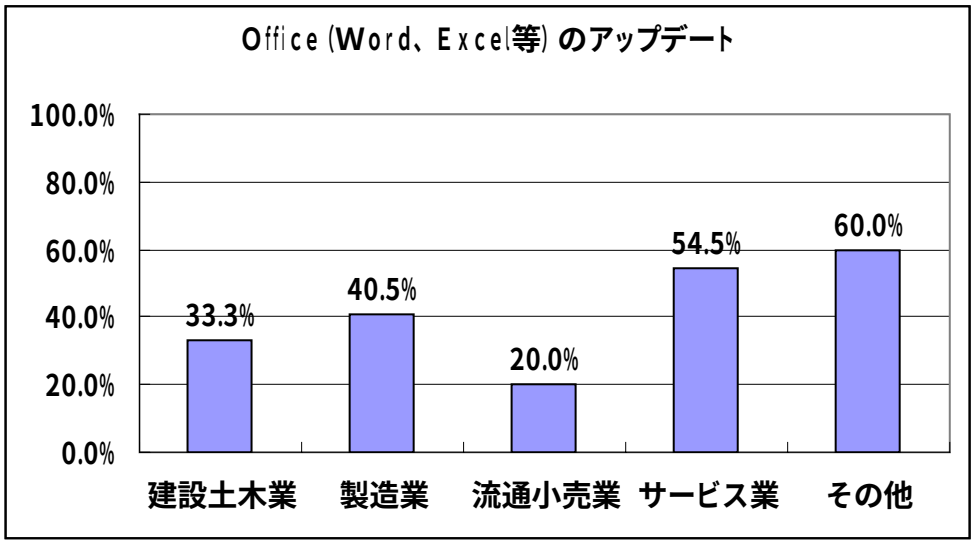
(2) ＯＳのアップデート

下のグラフは、Ｗｉｎｄｏｗｓのアップデートについてその実施状況を業種別に比較したものである。これを見ると、サービス業やその他ではやや高めで、流通小売業ではかなり低くなっている。製造業や建設土木業では平均的となっている。



(3) Ｏｆｆｉｃｅのアップデート

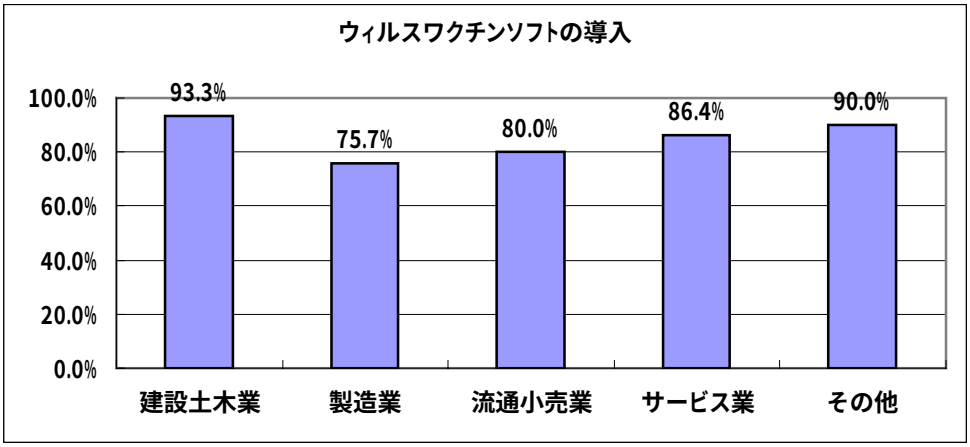
下のグラフは、Ｏｆｆｉｃｅのアップデートについてその実施状況を業種別に比較したものである。これを見ると、全体的には低いもののＷｉｎｄｏｗｓの状況と同様の傾向で、サービス業やその他ではやや高め、流通小売業ではかなり低い、製造業や建設土木業では平均的となっている。

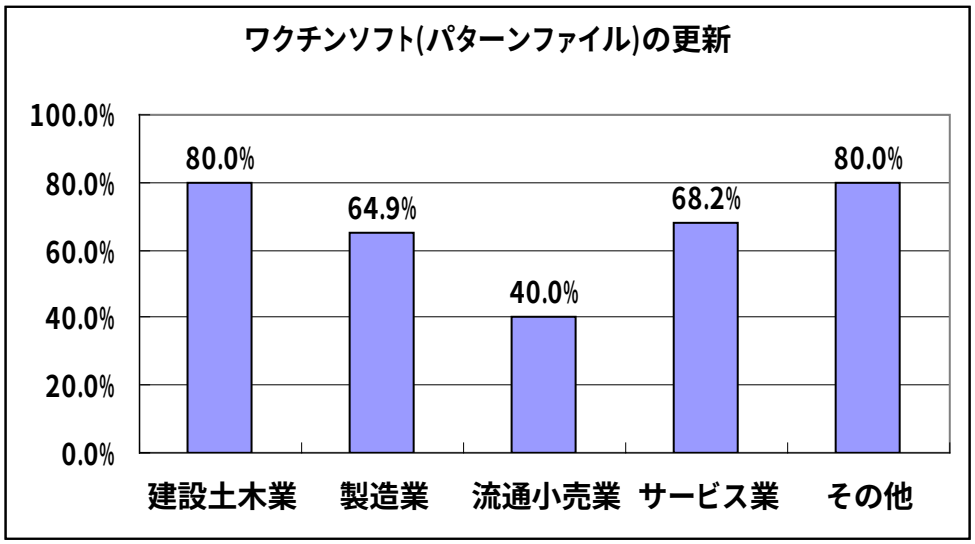


(4) ウィルス対策ソフトとパターンファイル更新

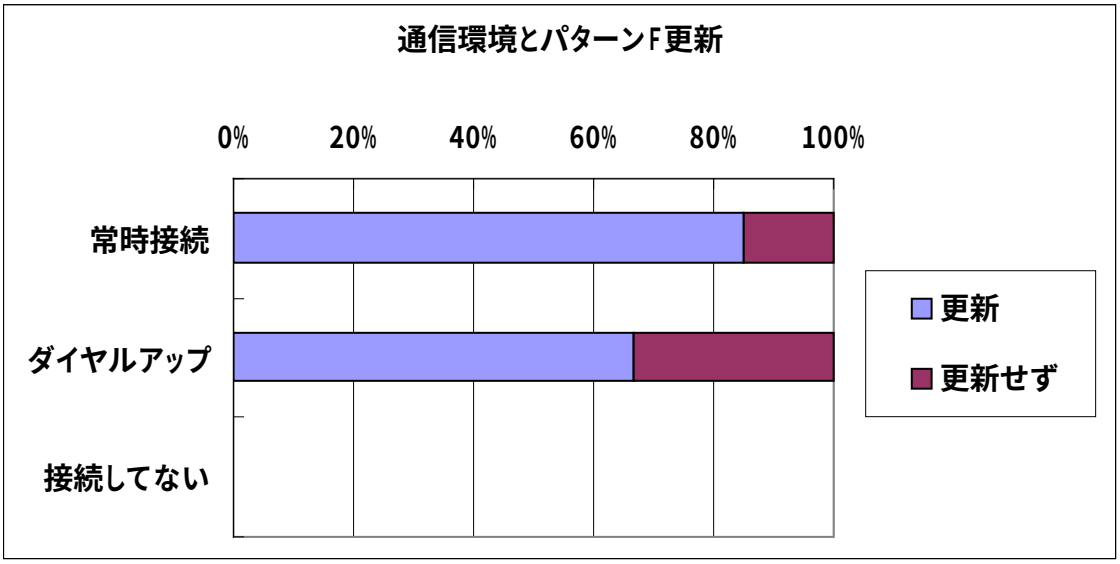
下のグラフは、ウィルス対策ソフトとパターンファイル更新についてその実施状況を業種別に比較

したものである。これを見ると、製造業で若干低めとなっているが、概ね同じ程度に実施していると見ることが出来る。しかし、パターンファイル更新について見てみると、流通小売業ではかなり低くなっている。流通小売業では導入企業の約半分が、パターンファイルの更新を行っていないということになる。

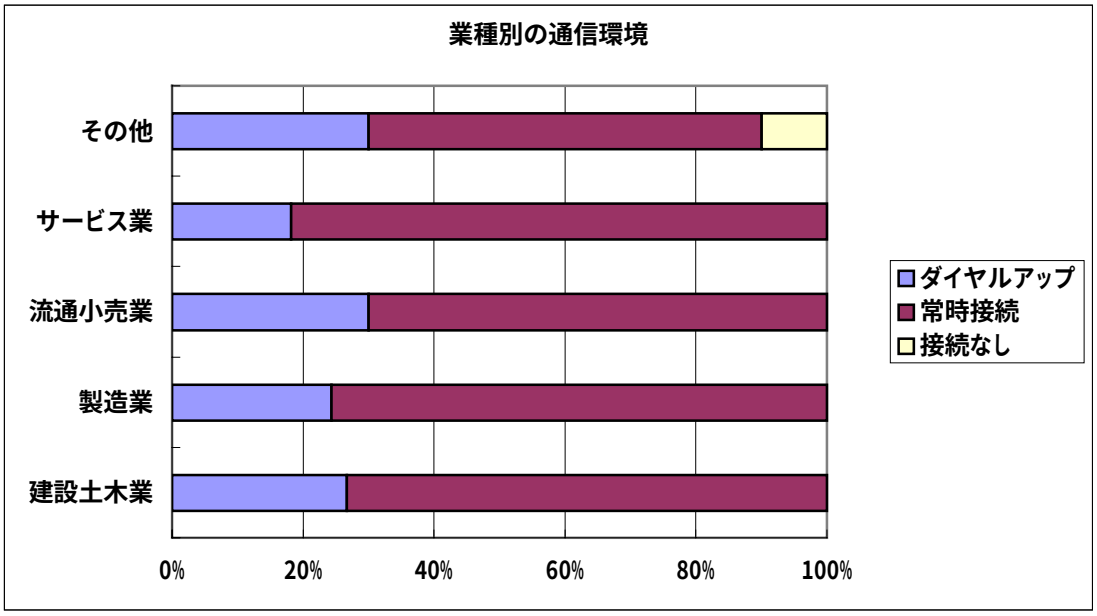




次ページのグラフは、ウィルスワクチンソフトを導入済みの７８社において、各社の通信環境（常時接続、ダイヤルアップ、通信環境なし）とパターンファイル更新の関係を示したものである。すなわち、昨今のウィルスワクチンソフトには自動更新機能が付いているのでその設定さえしておけばよいはずであるが、それは通信環境にも依存するものである。すなわち通信環境の影響による差があるのではないかという仮説を検証するためのものであるが、結果としてはやはり、常時接続環境にある企業はダイヤルアップ接続の企業よりもパターンファイル更新の実施率が高いといえる。また、ウィルスワクチンソフト導入企業７８社においてはＷＥＢ接続環境にない企業は一社も無かった。



下のグラフは業種別の通信環境であるが、これを見ると特に流通業の常時接続の比率が極端に低いというわけではない。すなわち流通小売のパターンファイル更新の実施率が低いのは、通信環境による差ではなく、単に意識の問題であると考えられる。

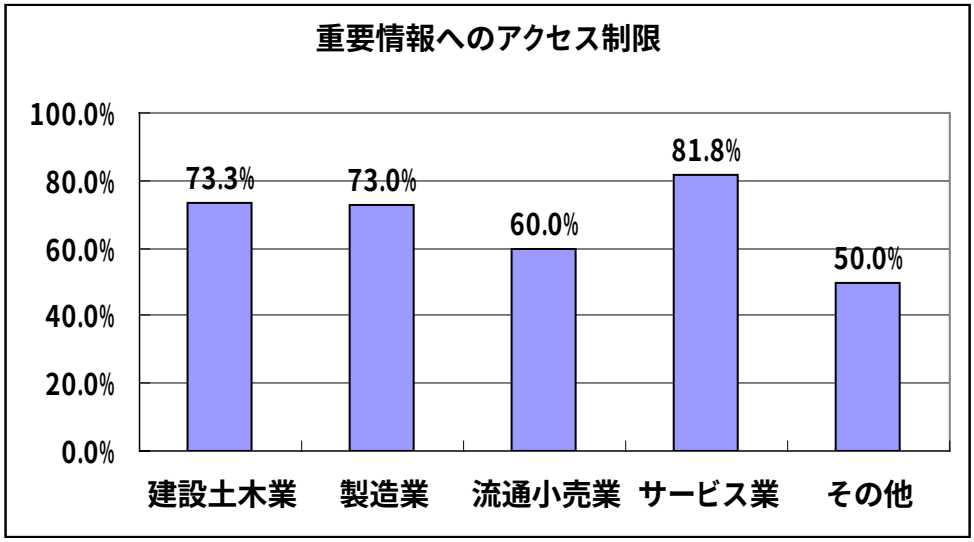


以上の結果より、ウィルスワクチンソフトの導入に関しては業種による差はないが、パターンファイル更新については、企業の通信環境に左右されること、また業種別では流通小売業での実施率が低いということが言えよう。

(5) 重要情報へのアクセス管理

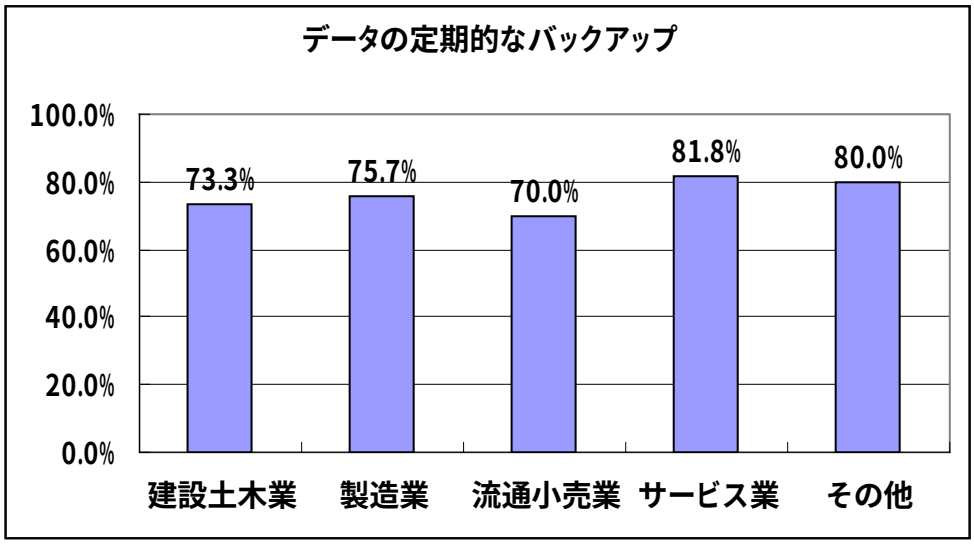
下のグラフは、重要情報へのアクセス制限についてその実施状況を業種別に比較したものである。これを見ると、流通小売業とその他でその実施率が若干低めとなっている。流通小売は、販売先（顧

客）も多いことから、特に昨今騒がれている顧客情報の取扱については十分な管理が望まれるところであるが、アクセス制限を設けていないところが４０%あるという結果になっている。



(6) 重要データのバックアップ

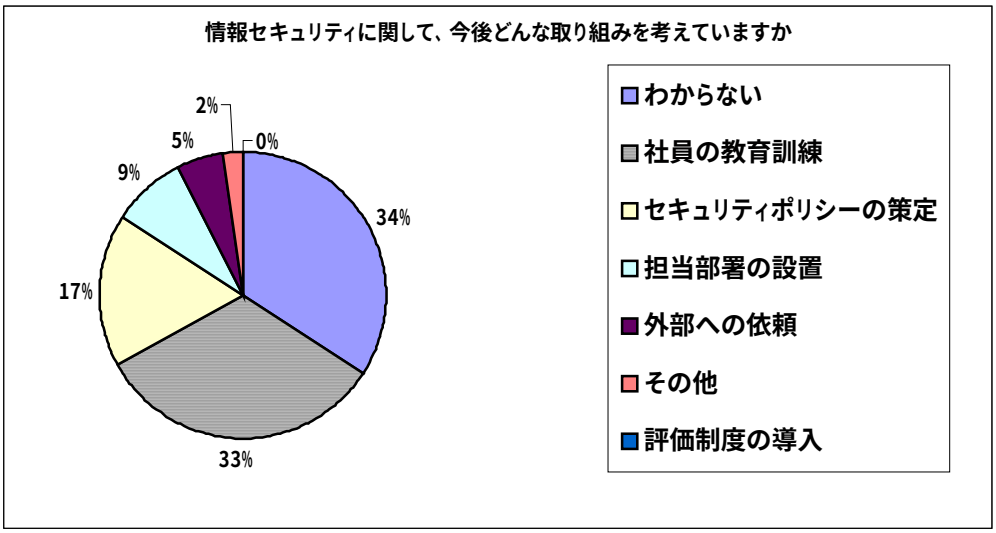
下のグラフは、重要データのバックアップについてその実施状況を業種別に比較したものである。これを見ると、やはり流通小売業でその実施率が若干低めとなっているものの、業種別の差異は無いといってよい。ただ、どの業種においても２～３割の企業が、突然のディスククラッシュに対応できない状況にあることは、憂慮すべき事柄である。



６．今後の取り組みに対する意識（アンケート問３４）

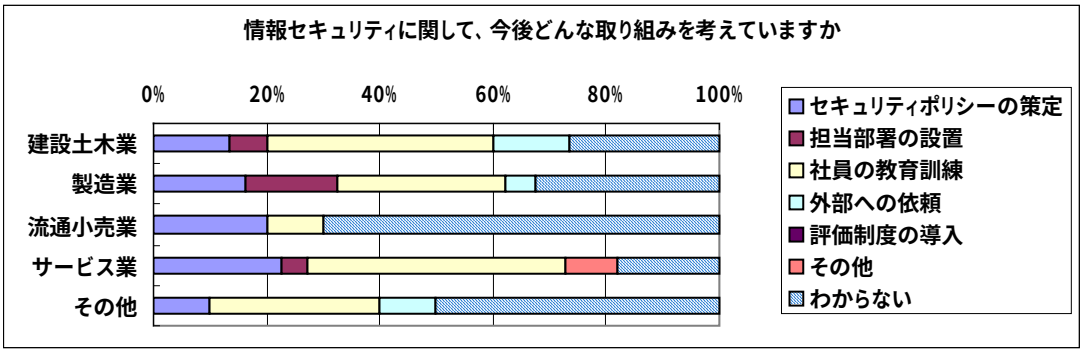
(1) 全体

情報セキュリティに関して今後どんな取り組みを考えているかについて聞いたところ、以下のような結果を得た。一番多かった回答は「わからない」３４％で、３分の１の企業がその対応の方針すらも待てない状況にある。２番目に多かった回答は「社員の教育訓練」３３％である。先ずは社員一人一人の意識とスキルをアップが重要であるという考え方が中心であることが分かる。次に多かったのは「セキュリティポリシーの策定」１７％である。「社員一人一人も重要であるが、その前にまず組織としてどう取り組むかが重要である」という意識を持っている企業は１７％ということになる。ついで、「担当部署の設置」９％や外部への依頼５％となっている。情報セキュリティは何処かに任せておけばよいという企業が１４％である、と捉えることができる。評価制度の導入については、まだまだ意識にないというのが現状であり、ＩＳＭＳ等の外部審査機関による認定制度については殆ど知られていない。



(2) 業種別

下のグラフは、情報セキュリティの今後の取り組みついて業種別に比較したものである。



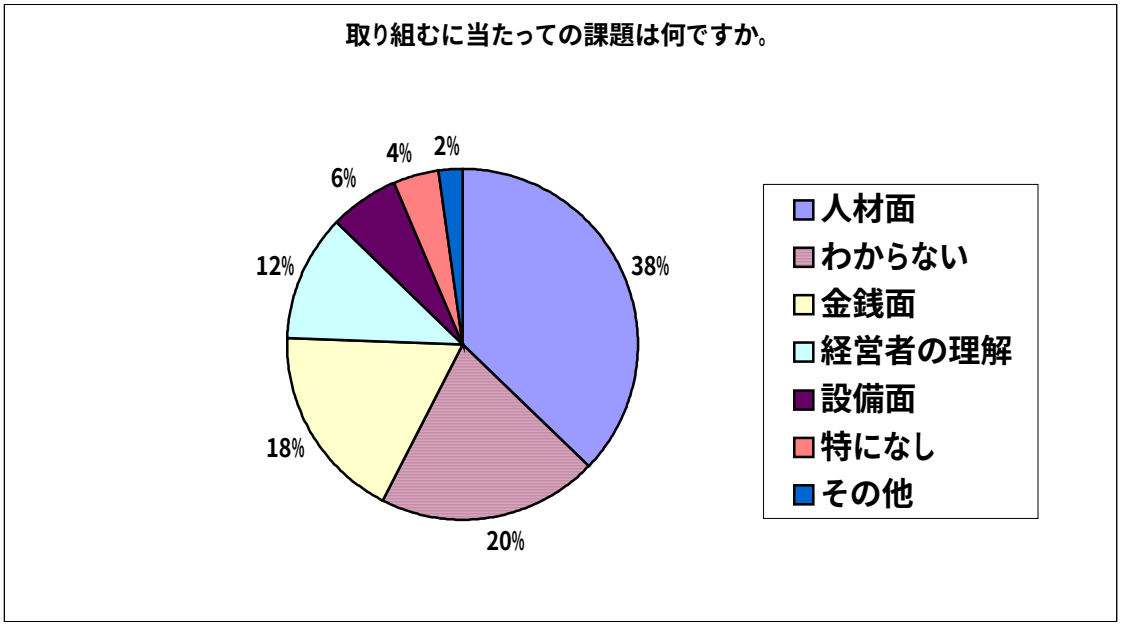
これを見ると、流通小売業とその他では「わからない」の比率が高くなっている。建築土木業、製造業、サービス業では、何らかの自助努力を行おうとする意向が強いことが伺える。サービス業では、「セキュリティポリシーの策定」や「社員の教育訓練」といった対応策が他の業種に比べ多くなっている。また、製造業では「担当部署の設置」といった対応策の比率が高くなっている。

７．取り組みにあたっての課題（アンケート問３５～３６）

(1) 取り組みにあたっての課題

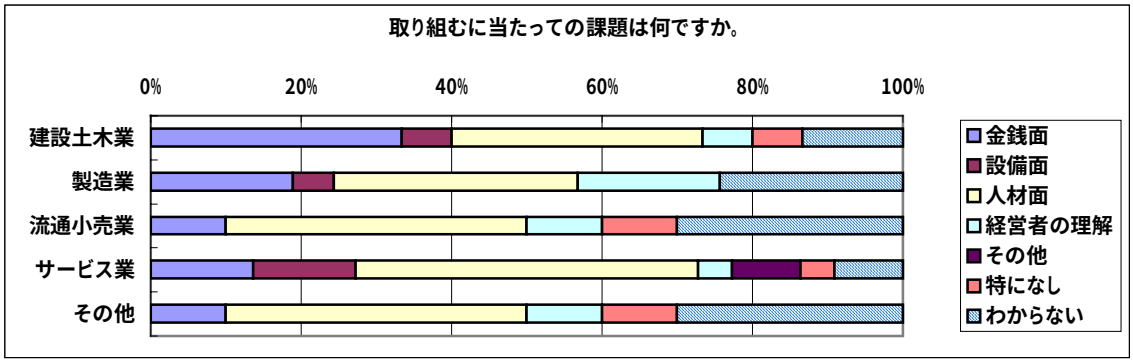
① 全体

情報セキュリティに取り組むにあたっての課題について聞いたところ、以下のような結果を得た。まず、取り組むにあたり具体的な課題が分からないところが２０％あるが、これではアクションにつながらないであろうことが見て取れる。一番多かった具体的課題は「人材面」３８％で、約４割の企業がキーとなる人材の育成と社員のリテラシィといったことを挙げている。次に多かった課題は「金銭面」１８％となっているが、具体的に何にコストがかかると思っているのかは不明である。多大なシステム投資がかかるという意識の現われかもしれない。３番目は「経営者の理解」１２％である。経営者が危機意識を持ちさえすればいいことなのであるが、それが薄弱だと嘆く情報担当者の嘆きが感じられる。（ここで注意しなければならないのは、「残りの８８％の企業の経営者は情報セキュリティに対して十分な意識をもって臨んでいる」ということではない。）



② 業種別

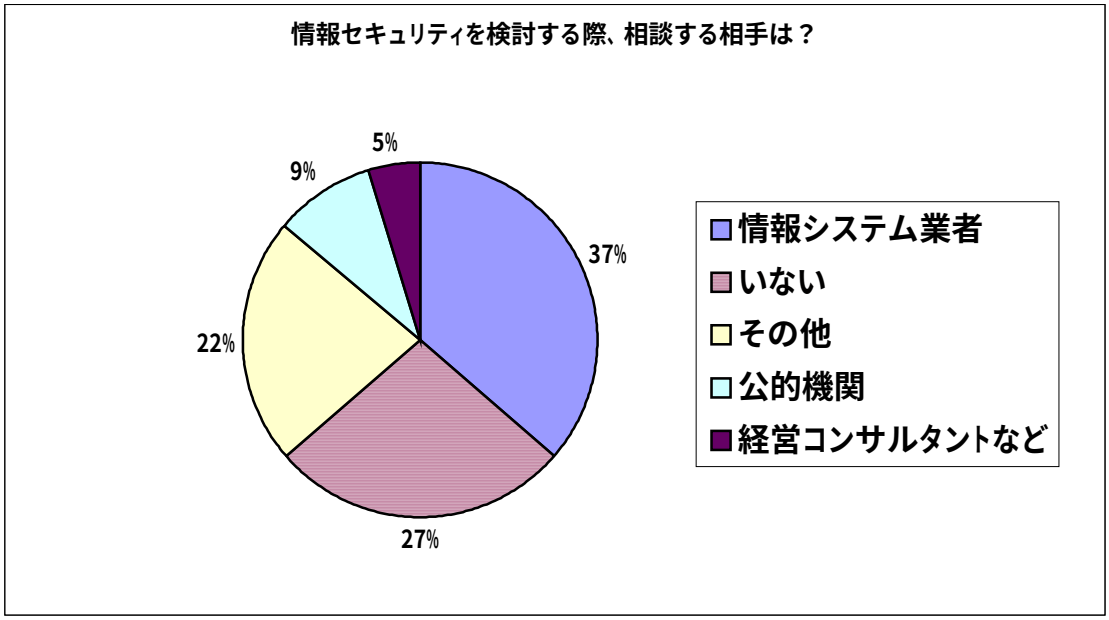
次ページのグラフは、情報セキュリティに取り組む場合の課題について業種別に比較したものである。建築土木業では「金銭面」の比率が相対的に高くなっており、製造業では「経営者の理解」の比率が相対的に高くなっている。



(2) 情報セキュリティの相談先

① 全体

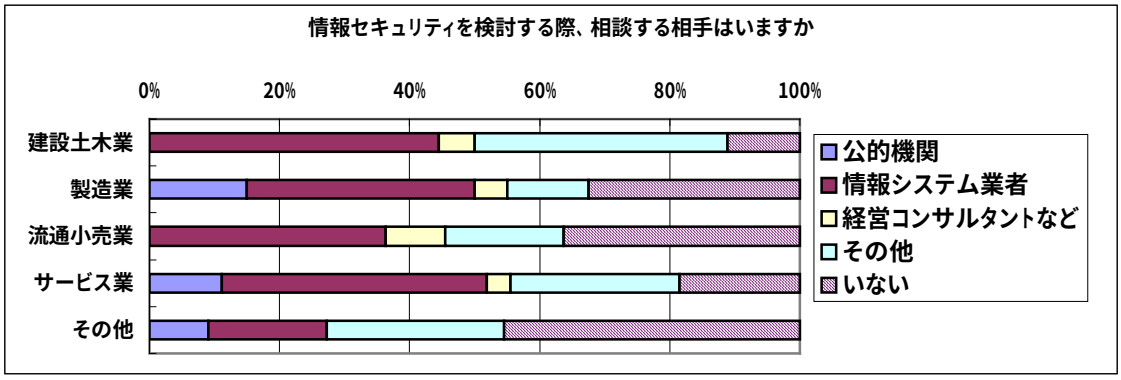
情報セキュリティに関する相談先について聞いたところ、以下のような結果を得た。一番多かった回答は「情報システム業者」３７%で、やはり外部の専門家を最初に想定するのであろう。次に具体的な相談先として想定されたところは「公的機関」９%、「経営コンサルタント」５%となっている。すなわち情報セキュリティにおいては、情報システム業者以外に頼る先はあまり思い浮かばないという状況にあるといえる。



② 業種別

次ページのグラフは、情報セキュリティに関する相談先について業種別に比較したものである。「情報システム業者」はどの業種においても大きなウェイトを占めていることがわかる。建築土木業や流通小売業では「公的機関」を想定するところはなかった。また製造業，流通小売業，その他では具体的な相談先が「いない」とする率が高く、公的機関からの更なる公告活動が望まれるとこ

ろである。



(3) 今後の取り組み意識のまとめ

中小企業における今後の情報セキュリティの取り組みについて、以下に列挙する。

① 具体的な方針を持たない企業が約３分の１

② 社員の意識やスキルの向上が約３分の１

③ 全社的あるいは専任的な組織で取り組む仕組みをつくるが約３分の１

④ ＩＳＭＳ等の外部認証制度の活用についてはゼロ（認知すらされていない）

⑤ 取り組みにあたっての解消すべき課題（阻害要因）は、人材面、金銭面、経営者の理解の順である

⑥ 情報セキュリティの相談先は情報システム業者であって、他に相談するところは思い浮かばないのが現状である

第３章　あるべき中小企業のセキュリテイ対策

１．制度的な対策

制度的な取り組みにおける問題点を踏まえたうえで、組織化、人材育成、標準化の視点から制度的対策について以下に述べる。

(1) 組織化

情報セキュリティを担当する部署が決まっていない企業が多い。これは、どの様に進めたらよいのかわからないとする企業が多いことをあらわしている一面ともいえる。

ただここで強調したいことは、情報セキュリティを情報システム部門の技術的な一業務として捉え、情報システム部門に任せきりにせず、経営者が先頭切って行動しなければならない点である。さらに、情報システム部門が無い企業においては、パソコンに詳しい社員がいつの間にかボランティアで社内の情報システムを管理していることがある。そして、同じ情報のことだがらといって情報セキュリティの担当も任されることがある。個人的な活動だけで、企業の情報セキュリティに対応できるものではないという点である。

情報セキュリティは、あくまで経営課題のひとつとして経営者が認識すべきものである。もちろん、経営者が一人で対応できるものではないので、部下に任せることになるが、その場合、正式な業務として位置づけ、担当する者に十分な権限を与えた上で、実施させなければならない。また、どの部門に担当させるかは、各々の企業の判断するところであるが、経営者がバックアップして、行動できる環境を整えることが必要条件である。たとえ、担当者が新入社員であろうとも、情報セキュリティに関する指示に対しては、勤続３０年・４０年のベテラン社員も従うことが要求される。

(2) 人材育成

情報セキュリティ管理者の育成はぜひとも進めてほしいところだ。ほとんどの企業は、情報セキュリティは重要だとしているものの実際に育成している企業は少数派である。単に機械を買ってくれば後は機械がセキュリティを守ってくれるわけではない。情報セキュリティを担う人材がいてはじめて守られるものである。また、特定の人間の活動だけでは、情報セキュリティを十分守ることはできない。全従業員に企業の情報資産を守るのだという意識がなければ、水をザルですくうことになってしまう。従業員に対して行う情報セキュリティに関する教育も不可欠なものと考えてほしい。企業経営においても言えることだが、企業組織は人材によって成り立っており、その育成に取り組むべきことは自明の理である。

しかし、大企業においてでも、情報セキュリティ管理者の育成や従業員に対する研修等については、

本業の技術研修や接客教育等と比較すれば、ウエートはそれほど高くないようである。そこで、先ず社内で、自社における情報セキュリティとは何かなどの話し合いを定期的に開催したらどうだろうか。そして、商工会／商工会議所や自治体などで開かれるセミナー・講習会等に参加してみたらいいだろう。そこで身につけた情報セキュリテイの知識を社内に伝えることが、従業員への教育にもなるし、同じ悩みや疑問を持った仲間ができ、人脈を広げることにもなるであろう。

(3) 標準化

情報セキュリティに関する規定を持っている企業は、ごく少数である。しかし、ＩＴ化が進んだ現在、パソコン等に個々の対策を実施している企業は比較的多い。だが、個々の対策をバラバラに進めても、企業全体のセキュリティは守られない。そこには、企業全体を網羅する体系的な方針書（セキュリティポリシーという）、企業経営で言えば、経営理念・経営方針なるものが必要である。また、個々の対策についても、人によって実施する内容や手順が異なっていれば、十分な効果は期待できない。誰が実施しても同じ効果が期待できるように実施内容等を標準化すべきである。

しかし、最初から、ＩＳＭＳの認証取得レベルの立派なセキュリティポリシー等を策定しようとはせず、まず、「やっていいこと」と「やってはいけないこと」を挙げて身の丈にあったルールを作ることからはじめるべきである。もちろんルールを作る際は、身近な日常業務に関わるルールから作ることが大切である。そして、時間の経過とともに必要に応じて充実していけばよい。また、策定したルールは経営者の承認を得て、経営者の名前で社内に発表し遵守を徹底することも必要である。

以上、３つの視点から論じてみたが、これは、情報セキュリティに限らず企業内において行われる一般業務にも当てはまるもので、ごく基本的な対策といえる。

２． 物理的な対策

(1) アンケート結果から

情報セキュリティのひとつとして、情報機器類の保全など物理的な安全対策（情報の入れ物としての情報機器類・データファイルや事務所・建物の安全対策）があげられる。しかし、アンケート（問２５～２７）の結果からわかることは、

① 情報機器の転等防止等の安全対策は１０％しか実施されていない。

② バックアップデータが安全に保管されているのは３７％にとどまる。

③ 事務所の外部者規制は３４％しか実施されていない。

と十分な安全対策は実施されていないのが現状である。また、業種によってかなり認識に開きがあることもアンケート結果から確認されている。

情報機器は物理的な外形を有する「モノ」であり故障することを忘れてはならない。機器のフリーズや、ウイルス感染などのシステム的な被害の他に、外部からの不可抗力等により損傷したりする危険が常につきまとうのである。したがって、物理的な対策も情報セキュリティの重要な側面を持つという認識をもつ必要がある。

(2) 物理的対策の具体例

物理的対策は具体的にどうしたらよいか。アンケートの質問事項と回答結果から考察すると、①安全確保と事故の未然防止、②停電時の対応、③バックアップデータの保管とリストア、④部外者に対する事務所内規制、⑤ＰＣ廃棄時の処置、の５つの項目について対策を考える必要がある。

これらの具体例を以下に記したので、参考にしながら自社で早急に対応すべき事項から取り組んでいただきたい。

① 安全確保と事故の未然防止

事務所・工場内で作業や通行時にパソコン等と接触し、機器を倒壊したり損傷しないように安全柵等を設けて保護したり、また床にラインを描いて通路と区分し通行の妨げにならないように設置する。もちろん、情報機器を結ぶ電気配線・LAN ケーブルのコード類も引っ掛けたり踏んではずさないようにしておく。

さらに地震時の対策として、天井・壁等からの落下物で損傷しないように、またなるべく被害が最小限となるような場所に設置したりして予め機器等を保護しておくことである（最近はビジネス用の耐震グッズが出回っているので利用するとよい)。もし、情報機器の配置替えが即座には難しい場合には、今後のレイアウト変更や移転時には十分な安全対策を盛り込む必要がある。

② 停電時の対応

作業中に突然電源が切れたり、雷等で瞬間的に停電すると入力中のデータが消えたり、送信エラーが発生し復旧するのに大変な手間がかかることがある。その対策として無停電電源装置の導入が

必要となるが、いつでも稼動できる状態にしておく必要があるため、導入しただけで安心することなく、定期的な動作点検を怠らないにする。

③ バックアップデータの保管とリストア（データの復旧）

データ等のバックアップは定期的に行い、バックアップデータを定められた場所に整理して保管することが重要である。バックアップデータは内容の機密度、重要度にあわせ管理方法を決めておけば膨大なデータの保存期間・保存場所を決めるときに役に立つ。もちろん重要と指定したデータ・書類は鍵をかけ、その鍵の管理者を選任しきちんと管理していく必要がある。そしてトラブル時には保管してあるバックアップデータを使用してスムーズに復旧、起動等ができるようにテスト(訓練)を定期的に行う。

できれば地震・浸水等の被害を避けるため遠隔地にバックアップセンターを確保しておきたい（専門業者に依頼するのもよい）。

④ 部外者に対する事務所内規制

部外者が自由に出入りすると困る場所には、パーティションやロープ等で遮蔽するなど立ち入り規制をする。また、ＰＣ等の機器は、意図的か無意識かにかかわらず、部外者に画面を覗かれない位置に設置しておく（もちろん作業していないときは電源を切っておくかスクリーンセーバをかけロックする）。

携帯電話については近年、様々な機能が付加されており、カメラ・録音機能は情報漏えいのツールにもなり得るので、場所によっては制限することも必要である。

⑤ ＰＣ廃棄時の処置

意外と忘れがちであるが、破棄や下取りに出したPCから社内情報が漏れる場合がある。Windowsの「ごみ箱」からファイルを削除しただけではハードディスクの中のデータは完全に消えてはいない。完全にデータを消去できるアプリケーションソフトを使うか、ハードディスクを破壊するなど物理的に使用不能にしてから処分する。

(3) 対策を定着させる

前項①～⑤であげた物理的対策は、単に決めるだけでなく、社内にしっかりと根付かせることが重要である。

そのためには、バックアップはしているか、情報機器の設置は適正か等を定期的に点検する日または期間として、「パソコン防災の日」とか「パソコン防災週間」などを設けるのもよい。この日には、全員で対策の実施状況を点検するとともに、自社の情報資産にはどのようなリスクがあるのか、またそれらの情報資産のうち、何をどのように守るのか、などを話し合う場をつくるというのはどうだろうか。

３．技術的な対策

(1) 技術的課題のサマリー

前述したアンケート結果と重複するが、対策について検討する前にもう一度技術的なセキュリティ対策上の状況について確認しておく。以下はその実施状況の低い順に並べたものであるが、以降ではこの順にしたがってその対策案について述べる。

① Ｏｆｆｉｃｅのアップデート：４３％

② ＯＳのアップデート：５５％

③ ウィルスワクチンソフトのパターン更新：６７％

④ 重要情報へのアクセス制限：７１％

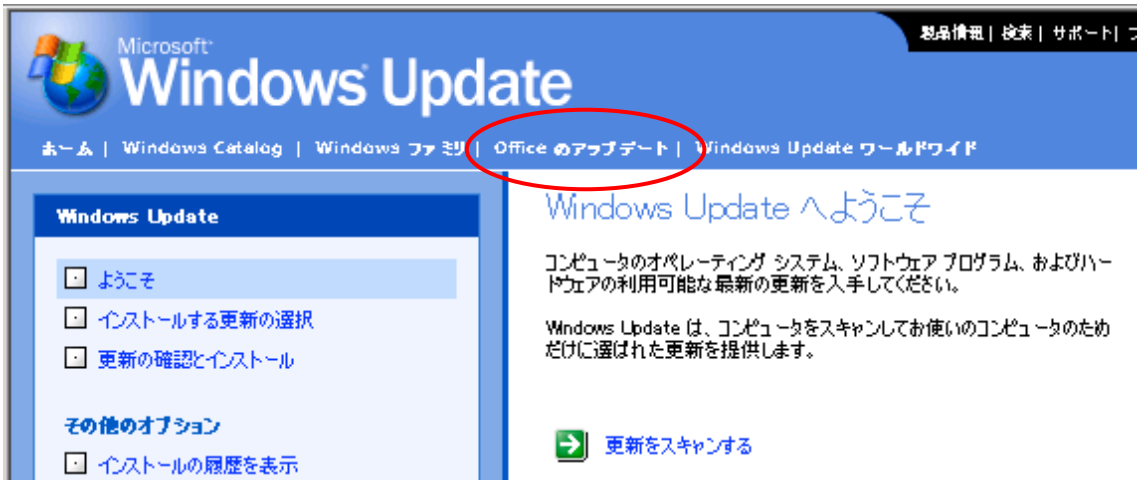
⑤ データの定期的なバックアップ：７７％

⑥ ウィルスワクチンソフトの導入：８３％

(2) Ｏｆｆｉｃｅ，ＯＳのアップデート

この課題については、個々人の意識づけでもできることではあるが、やはり組織的に行う為には担当を決めて「Windows を更新してください」と音頭を取らせたり、あるいは「毎週月曜日の朝一で更新スキャンを実行する」という具合に定期的に行わせるルールを徹底させるべきである。

下図は、よく見慣れている Windows のアップデート画面の一部である。注意されたいのは、Ｏｆｆｉｃｅについては、意識的に「Ｏｆｆｉｃｅのアップデート」をクリックしなければ、通常の「更新をスキャンする」だけではチェックできないということである。会社内あるいは外部取引先ともＯｆｆｉｃｅファイルのやり取りは少なくないので、かならずＯＳ更新とともにＯｆｆｉｃｅの更新も習慣づけることが大切である。



(3) ウィルスワクチンソフトのパターン更新

この課題についてはウィルスワクチンソフト導入企業の２０％が未対応であるが、調査からは、ダ

イヤルアップ接続の企業ではその比率が高くなることがわかった。したがってその対策の一つとしては、常時接続環境下へ移行することが考えられる。ダイヤルアップ接続であってももちろん問題はないが、接続時の待ち時間、通信速度、それらを換算したトータルのコスト等について考えた場合、果たしてメリットがあるといえるかどうか。当然外部からの侵入に対する備えも強固にする必要があろうが、基本的な設定をしっかりすれば良いだけのことであり、またその他のメリットも享受する点も考えれば常時接続に移行しない理由はない。

それ以外の原因として、ウィルスワクチンソフトのライセンス更新を行っていないということも想定される。しかしこれは技術的というよりは意識の問題なので、情報担当責任者（不在であれば経営者）の認識を改めるほかはない。

(4) 重要情報へのアクセス制限

昨今の、誰もが有益な情報にアクセスできる「情報共有」という流れからすると、この「情報へのアクセス制限」は相反する考えともとられる。ここで重要なことは（当然ではあるが）まず社内の情報資産の「機密性」を以下のような基準でそれぞれ評価し、整理することである。それにより相反するように思える上記課題を解決することが可能となる。

① 経営トップレベル
② 中間管理層レベル
③ 部門レベル
④ 一般社員レベル
⑤ 取引先、パートナーレベル
⑥ 一般公開レベル

情報の機密性を評価したら、それを物理的に何処に保管するかを整理する。物理的な単位としては以下のようなものが考えられ、必要に応じてその単位ごとにアクセスする権限を設定する。

① ネットワーク
② コンピュータ
③ ディスク
④ フォルダ
⑤ ファイル

(5) データの定期的なバックアップ

これについてもまず情報の「完全性」について評価を行うことから始められたい。完全性の基準とは例えば以下のようなものである。

① 情報が壊れたあるいは失われた場合に、経営に重大な影響がある

② 致命的ではないが、ある程度は業務に影響がある

③ 業務への影響はさほどない

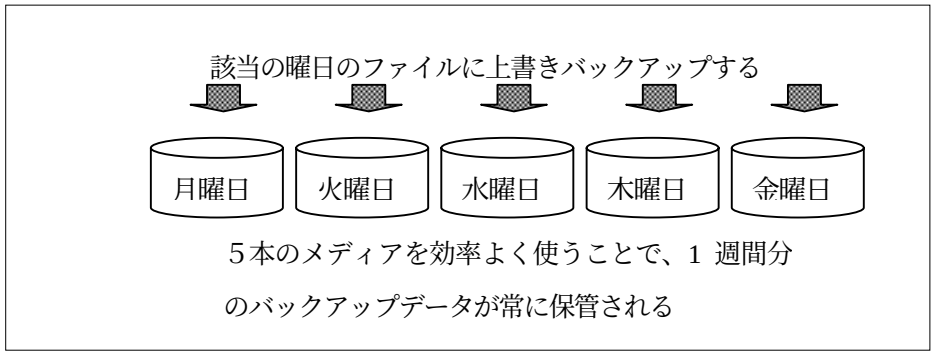
情報の整理が出来たら、次は具体的な手順として、誰が、いつ、どのようにバックアップをとるかをルールとして決める。もちろん自動バックアップソフトが利用できるようであればそれに越したことはない。またそれ以外に重要なことを以下に列挙する。

① バックアップが適正に行われているかどうか、必ず上位職者がチェックすること

② パッケージ系（テープやＤＶＤ）のメディアにも適宜コピーをとり、安全に保管すること

③ バックアップファイルをリストア（元に戻すこと）できるような練習をしておくこと。

④ バックアップファイルは上書きではなく、追加でおこなう（もし上書きする場合は、例えば、曜日毎にファイルを作成し、そのファイルに日々上書きしていく方式がよい）



(6) ウィルスワクチンソフトの導入

これについてはあえて言及するまでもないと思われる。未導入の企業が１７%あるが、その企業がとるべき方法は以下の３つである。

① すぐにウィルスワクチンソフトをインストールする

② 外部データの取り込みが出来ないように、ディスクドライブを取り外し、ネットワークから遮断する

③ コンピュータを使わない

４．まとめ

中小企業におけるセキュリティ対策のあるべき姿について検討してきたが、最も基本的なことは以下の３点であろう。

(1) 経営者の意識改革

情報セキュリティ対策に対しては、「手間やコストがかかるわりに、企業収益に直接貢献するわけでもない、ましてやうちは大企業じゃないから大丈夫」といった中小企業経営者の意識が少なからずある。そのような経営者の意識改革こそがまず求められる。

(2)「しくみ」と「しつけ」のバランス

次に重要なことは、情報セキュリティ対策に完全はありえないのであるから、できるところから着手することが肝心である。そのためには「当社が守るべき情報資産」を明確にして、セキュリティ対策を講ずるのであるが、その対策は大きく２つに分けられる。

① 装置系：ハードウェア、ソフトウェア、ネットワーク等における物理的・技術的なしくみ

② 運用系：従業員の動機付けやスキルアップといった人間系のしつけ

上記は、車のシートベルトに例えられる。すなわち衝突時に身を守る「シートベルト」という安全装置（しくみ）を、運転時には必ず着用する習慣（しつけ）があって初めてセキュリティが確立されるのである。これはセキュリティマネジメントの両輪、必要十分条件ともいえるものであるので、どちらに偏重しても機能しないことを経営者は認識すべきである。

(3) 小さな第１歩と継続的改善

小さな両輪でも良いので、まず経営者が「今年はこれをやる」と方針を出し、その運用状況をモニタリングし、悪いところを改善する（ＰＤＣＡサイクル）、達成できたら次のセキュリティ目標を明示しモニタリングする、これを継続的に繰り返していくことこそ中小企業における情報セキュリティ対策のあるべき姿であろう。

５．情報セキュリティをマネジメントとして取り組むために

情報化社会と言われている現在、物の価値より情報の価値が重要視される傾向が進んでおり、企業の経営資源の一つとして、人・物・金の次に情報と言われるほど、企業にとって情報は重要なものになっている。したがってその重要な経営資源である情報を保護する情報セキュリティは、現場だけで取り組む一業務ではなく、重要な経営戦略の一環として全社を挙げて取り組む必要があり、情報セキュリティをトップ自らが強力に推進する「マネジメント」に進化させなければならない。

「マネジメント」とは、①トップ自らが情報セキュリティの旗を振り、②守るべき領域や目標を明確にし、③適切な経営資源を投下し、④ＰＤＣＡサイクルにより継続的改善を図る仕組みを策定し、⑤実施状況をモニタリングしていくことに他ならない。

以下では、情報セキュリティをトップ自らが推進するマネジメントとして確立する為の要件を、人材、権限、コスト、時間という４つの視点から明らかにする。

(1) 人材

情報セキュリティという比較的新しい課題について対応できる人材が不可欠である。そのためには、教育・研修等を行い、情報セキュリティの課題を担える人材、リーダーを育てなければならない。また、日常業務の中で情報セキュリティの問題が発生するわけであるため、未然防止のため全ての従業員に対しての教育も必要で、全従業員のレベルアップが必要である。

(2) 権限

情報セキュリティを推進するリーダー・管理者に対し、適切な権限委譲が必要である。規定を制定する権限委譲、社内に対し遵守を要求できる権限委譲等、経営者の後ろ盾が不可欠である。制定される情報セキュリテイに関する規定は、経営者も含め全社員が遵守すべきもので、違反した場合は例外なく処罰されるものとしなければならない。さらには、取引先との間で締結される機密保護に関する契約についても契約違反の事態が社内において発生しないよう、全社員に対し契約内容を遵守した業務遂行を徹底することが必要となる。

(3) コスト

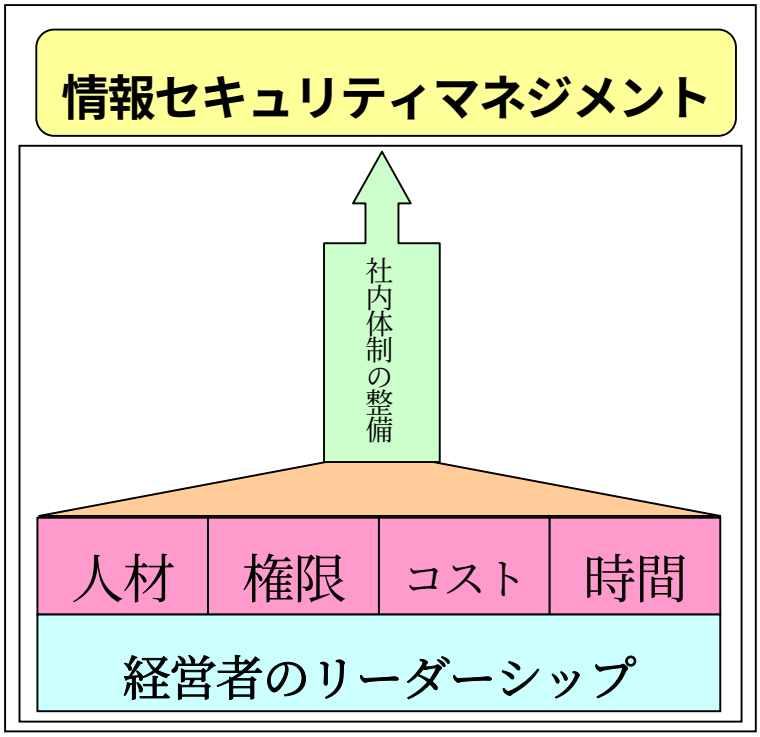
教育・研修等外部の研修機関を利用する際、その教育・研修費などは決して安くはない。しかし、これを人材育成の投資として、また、情報セキュリティのために必要な備品、機器やソフト等の調達費用についても必要経費として考えてほしい。もちろん無制限に経費をかけることはできないが、今後の企業経営に必要な、生き金として考えてほしい。

(4) 時間

中小企業では慢性的な人材不足という問題を抱えており、中小企業の従業員は、多能工的に業務に従事することを要求されている。その中で、情報セキュリティに関する業務が増えるわけだが、副次的な業務として片手間でする仕事としてではなく、重要な業務として位置付け、十分な時間を割り当てる必要がある。

以上４つの視点から必要となる要件を述べてきたが、中小企業に情報セキュリティというＤＮＡを組み込むためには、これら４つの要件は不可欠であり、それを経営者のリーダーシップのもと「マネジメントする枠組み」を構築する必要がある。

図　情報セキュリテイをマネジメントする枠組み



ＩＳＯ９００１の品質システムの認証取得が中小企業にも広がっているように、ＩＳＭＳ（Information Security Management System）の認証取得や、プライバシーマークの取得が、今後企業経営にとって無視できない存在になっていく可能性がある。情報セキュリティのマネジメント体制を短期間で確実に確立するために、これらの取得を目指すこともひとつの手段であろう。又それは同時に取引先や顧客への信頼性をアピールするというメリットも享受できるはずである。

第４章　セキュリティ対策チェックリスト

最低限これだけはおさえておきたい

最後に前章までの分析および考察を踏まえ、中小企業が情報セキュリティを確保するためにどういった点に留意すべきか、どのような予防策を施すべきかを、チェックリストの形でまとめてみた。

アンケート調査結果で判明したように、経営資源にさまざまな制約がある中小の事業所にとって、情報セキュリティに関していきなり万全の安全対策を求めることは、容易ではないし現実的でもないであろう。ここに挙げたチェック項目は「まず出来ることから始める」「企業規模にかかわらず最低限行うべき」ことを主旨として、盛り込んだものである。したがって、各種メディアなど世間一般に叫ばれている情報セキュリティ対策の内容と比較すると、やや敷居の低いものとなっているものの、取り組みやすい内容であるはずである。

それゆえに、規模の大小にかかわらず中小企業が情報システムを活用する限り、「最低限の対策」として全ての項目に関して対策を施す指針となることを期待するものである。

No.		対 策 内 容	チェック	
1	制度的対策	情報セキュリティの責任者がいるか	はい	いいえ
2		情報セキュリティの責任者がやるべきことは明確になっているか	はい	いいえ
3		情報セキュリティの責任者は、講習・セミナー等に出席する機会を与えられているか	はい	いいえ
4		社内で情報セキュリティに関する勉強会等を定期的に開催しているか	はい	いいえ
5		経営者は情報セキュリティの責任者の活動に積極的に関与しているか	はい	いいえ
6		情報セキュリティの責任者は経営者に、セキュリティの状況を定期的に報告しているか	はい	いいえ
7		経営情報や顧客情報等の重要資料は、施錠できる場所に保管しているか	はい	いいえ
8		経営情報や顧客情報等の重要資料を閲覧できる人を決めているか	はい	いいえ
9		職務上知り得た機密情報を、外部に漏らさないように周知しているか	はい	いいえ
10		情報機器の取り扱いや運用のルールは定めているか	はい	いいえ
11		ＰＣやＦＤ等の、持ち出し持ち込みのルールは決めてあるか	はい	いいえ
12		No.10～11 のルール内容は、社員全員が熟知しているか	はい	いいえ
13		No.10～11 のルールが守られているかを定期的にチェックしているか	はい	いいえ
14		外部に業務を委託する時は、委託先に守秘義務を課しているか	はい	いいえ
15	物理的対策	情報機器が通行する人と接触しないよう囲い等で保護をしているか	はい	いいえ
16		各種ケーブル類を引っ掛けたり、踏んだりしない対策はしているか	はい	いいえ
17		瞬電（瞬間的な停電）または停電対策はしているか	はい	いいえ
18	対策	無停電電源装置の稼動を定期的にチェックしているか	はい	いいえ
19		情報機器の耐用期間（老朽化）は管理しているか	はい	いいえ
20		バックアップデータは安全な場所に保管しているか	はい	いいえ
21		重要なデータ・書類を保管する鍵は責任者が管理しているか	はい	いいえ
22		PC を廃棄処分するとき、データは完全消去処理をしているか	はい	いいえ
23		部外者が自由に出入りできないようパーティションなどで遮蔽しているか	はい	いいえ
24		情報機器は部外者から画面を覗き込まれないような位置に設置しているか	はい	いいえ

25	技術的対策	会社のパソコンの OS（Windows）バージョンは社員が勝手に変更してはいけないというルールがあるか	はい	いいえ
26		会社のパソコンにソフトウエアなどを勝手にインストールしてはいけないというルールがあるか	はい	いいえ
27		OS（Windows）のアップデートが適切に行われているか管理しているか	はい	いいえ
28		ウィルスワクチンソフトのインストールやパターン更新が適切に行われているか定期的に確認しているか	はい	いいえ
29		ウィルスワクチンソフトのライセンスは毎年更新されているか	はい	いいえ
30		重要なデータにはアクセス権限が適切に設定されており、誰でも勝手に閲覧できないように管理されているか	はい	いいえ
31		パスワードが他者に知られないような管理・指導がなされているか	はい	いいえ
32		社内ネットワークへの外部からの不正アクセスに対する防御策は施されているか	はい	いいえ
33		無線 LAN を利用する場合には、暗号化等による盗聴対策をしているか	はい	いいえ
34		データのバックアップがルールどおり行われていることを定期的に確認しているか	はい	いいえ
35		システム管理が一人だけに集中せず、仮にその人がいなくなっても対応できるようになっているか	はい	いいえ
36		重要な情報を持っている人が転職や定年でいなくなることについて何らかの対処をしているか	はい	いいえ

資　料

アンケート質問項目一覧

	質問内容	回答選択肢
01	貴社の主たる業種は何ですか	□ 建設土木業 □ 製造業 □ 流通小売業 □ サービス業 □ その他
02	従業員数（パートを含む）についてお答えください	□ 20 人以下 □ 21 人以上 50 人以下 □ 51 人以上 100 人以下 □ 101 人以上
03	本社以外に支店、営業所などはありますか	□ ある □ ない
04	あなた(回答される方)についてお答えください	□ 一般社員(システム部門) □ 一般社員(システム部門以外) □ 管理職(システム部門) □ 管理職(システム部門以外) ◉ 経営者またはそれに準ずる
05	保有するコンピュータの台数はどのくらいですか	□ １～１０台 □ １１～１００台 □ それ以上
06	インターネットにはどのように接続していますか	□ ダイヤルアップ接続 □ 常時接続（ＡＤＳＬや光専用線等） □ 接続していない
07	電子商取引や業務連絡等で外部との交信に情報システムを利用していますか	□ 利用する □ たまに利用する □ 利用していない
08	情報システムの管理はどこの部門(誰)が行っていますか	□ システム部門 □ システム部門以外の部門 □ コンピュータに詳しい社員（部門は決まっていない） □ 経営者層
09	ＩＴの利用が進む中で、情報セキュリティ(安全対策)は重要だとお考えですか	□ 重要である □ それほど重要とは思わない □ よくわからない
10	問５で「重要である」と答えた方にお聞きします。情報セキュリティはなぜ必要だと思いますか(２つまで)	□ ウイルスに感染すると困るから □ 周囲が騒ぐから □ 取引先などに迷惑がかかるから □ 自社が多額の経済的損失を被るから
11	問５で「それほど重要とは思わない」と答えた方にお聞きします。なぜそう思うのですか	□ 当社のような中小企業では必要ない(大した被害はない) □ 実際に被害にあったら考えればいい □ その他
12	情報セキュリティに対する貴社の現状をお答えください	□ 既に取り組んでいる □ 対策を計画中 □ 特に何もしていない □ よくわからない

13	情報セキュリティはどう進めるべきだとお考えですか	□ システム担当部門が行う □ その他の部門(人事など)が行う □ 経営層がトップダウンで行う □ 進め方はよくわからない
14	貴社では、コンピュータウイルスの感染がありましたか	□ ある □ ない □ わからない
15	感染によって、どんな状態になりましたか（問１４で感染ありのみ）	□ ファイルが破壊された □ パソコンに不具合が出た □ サーバーに不具合が出た □ その他
16	復旧に要した時間は（問１４で感染ありのみ）	□ １日以下 □ １週間以下 □ １ヶ月以下 □ １ヶ月を超える
17	貴社の情報システムが、事故・災害・人的要因などによる被害を受けたことがありますか	□ ある □ ない
18	どんな被害がありましたか（問１７で被害ありのみ）	□ 取引先と金銭トラブルになった □ 取引先に迷惑をかけた □ 業務に支障が出た
19	被害を金額に換算すると、どれくらいになりますか（問１７で被害ありのみ）	□ １０万円以下 □ １００万円以下 □ １０００万円以下 □ １０００万円を超える
20	情報セキュリティに関する規定はありますか	□ ある □ 就業規則の一部にある □ ない
21	情報セキュリティ管理者の育成はどのようにしていますか	□ 社外機関を利用 □ セキュリティ管理者は既にいる □ その他 □ 何もしていない
22	従業員に意識付けのための研修を実施していますか	□ はい □ いいえ
23	情報セキュリティの担当部署はどこですか	□ 情報システム部門 □ その他の部門 □ 社長・役員に直属 □ 担当部署はない
24	取引先との間に業務上の機密保護に関する契約をしていますか。	□ はい □ いいえ
25	情報機器に囲いや転倒防止などの安全対策をしていますか	□ はい □ いいえ
26	バックアップした記憶媒体は、安全な場所に保管していますか	□ はい □ いいえ
27	取引先等の社外からの訪問者は、事務所内に自由に出入りできますか	□ はい □ いいえ
28	パソコンの基本ソフト（Windows2000、Windows	◉ はい □ いいえ

	ＸＰなど）に対し、Service Pack 等の修正プログラムを適用していますか	
29	Ｏｆｆｉｃｅ（Ｗｏｒｄ、Ｅｘｃｅｌ等）に対し、Service Pack 等の修正プログラムを適用していますか	☐ はい ☐ いいえ
30	コンピュータウィルスに対する、ワクチンソフトを導入していますか	☐ はい ☐ いいえ
31	ワクチンソフト(パターンファイル)は、常に最新の状態にしていますか	☐ はい ☐ いいえ
32	重要な情報（顧客情報、社員の個人情報等）へは、社員であれば誰でもアクセスできますか	☐ はい ☐ 決められた社員しかアクセスできない
33	パソコン内のデータは、定期的にバックアップしていますか	☐ はい ☐ いいえ
34	情報セキュリティに関して、今後どんな取り組みを考えていますか	☐ セキュリティポリシーの策定 ☐ 担当部署の設置 ◉ 社員の教育訓練 ☐ 外部への依頼 ☐ 評価制度の導入 ☐ その他 ☐ わからない
35	取り組むに当たっての課題は何ですか。	☐ 金銭面 ☐ 設備面 ☐ 人材面 ☐ 経営者の理解 ☐ その他 ☐ 特になし ☐ わからない
36	情報セキュリティを検討する際、相談する相手はいますか（複数解答可）	☐ 公的機関 ☐ 情報システム業者 ☐ 経営コンサルタントなど ☐ その他 ☐ いない

アンケート回答を送信する

おわりに

本研究に取り組んだメンバーは、経営や情報関連の仕事を主に行っているものの、こうした経営や情報の専門家といえども、情報セキュリティ対策の現状を把握するのは、なかなか難しいところである。しかし、この研究を通して東海地区における情報セキュリティの実情を明らかにすることができ、いくつかの点で再認識させられるところが多かった。その中でも主なものは次の３点である。

(1) 情報セキュリティに関する対応が遅れており、かなりの中小企業でコンピュータ・ウィルス被害などが発生している。

(2) 経営規模の小さな企業ほど、情報セキュリティに関する情報やノウハウが乏しく進め方が分からず手をこまねている。

(3) 情報セキュリティ対策を進める上での主な障害は、人材面と金銭面そして経営者の理解をあげている。特に、経営者の理解は非常に重要であり、経営者の意識改革が求められている。

更に中小企業が事業を展開していく上で、情報セキュリティに対する認識を一層深めることが重要であることが分かった。

最後に特筆すべきは、アンケートの回答の精度が高いことである。これまでの経験では、この種のアンケートは、企業に送っただけでなかなか精度の高い回答が得られない場合が多かった。そこで、今回は質問内容を的確に理解いただけるように、対面で直接説明したうえで回答を得ることとしたからである。

最後に繰り返しになるが、中小企業は最初からあまり大上段に構えず、企業として実施できることから実施して、セキュリティ対策の向上を図っていただきたい。そのために、この調査報告書が少しでもお役にたてば幸いである。

執筆者 中小企業診断協会 愛知県支部
榮　義紹
岩瀬　誠
神谷　龍司
酒井　隆司
安田　徹
E-mail secure@compass21.net