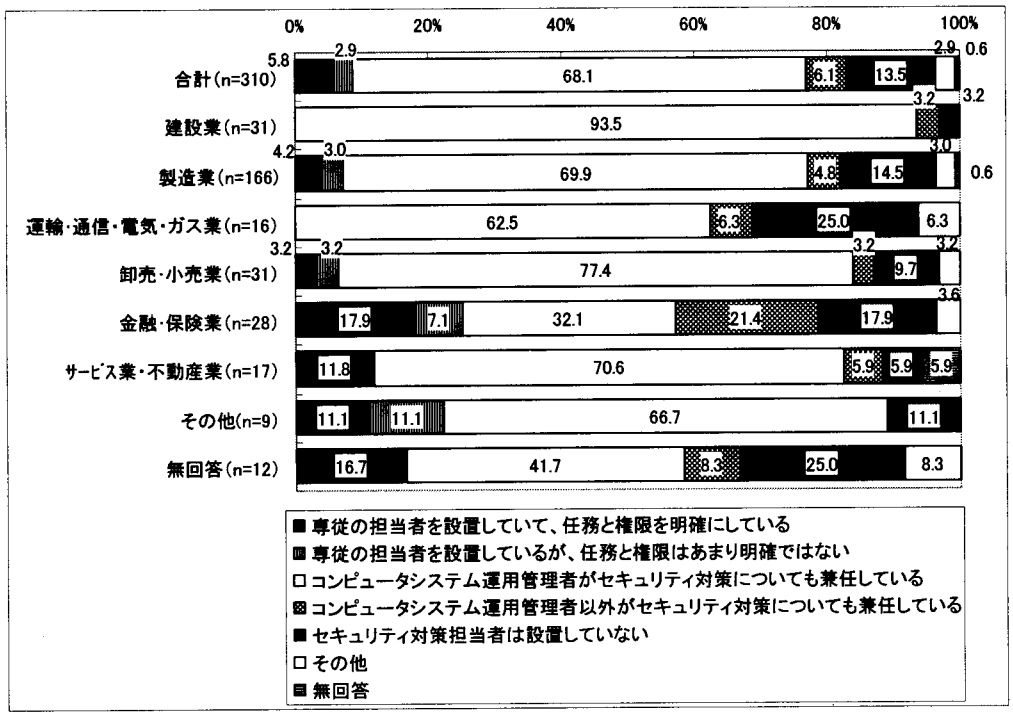
(2)セキュリティ管理体制

企業におけるセキュリティ担当者は、大半の企業ではコンピュータシステム運用管理者が兼任して担当している。専従のセキュリティ担当者を設置している企業は8.7%にとどまる。一方でセキュリティ担当者を設置していない企業も 13.5%あるなど、体制面でのばらつきがみられる。業種別にみると金融・保険業では 25.0%の企業が専従担当者を設置している。

図表3-8　セキュリティ対策担当者の設置状況



資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

不正アクセスに使われる技術やツールが進歩していく中で、サイバーセキュリティ対策には専門的な技術や知識が要求されるようになってきている。今後は、コンピュータシステムの運用管理と兼任してセキュリティ対策を行う体制では、十分な情報収集や対策を施していくことが難しくなっていくことが考えられる。

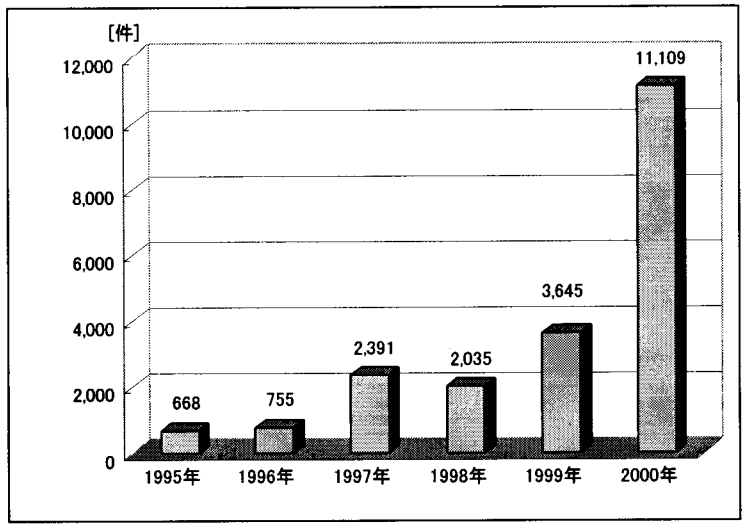
3．サイバーセキュリティ対策への取り組み状況

(1)コンピュータウィルス対策

近年、マクロウィルスやメール悪用ウィルスといった、広範な感染力をもつコンピュータウィルスが増えたことなどから、情報処理振興事業協会（IPA）に届けられたコンピュータウィルスの発見件数は大幅に増加している。特に、2000 年 5 月に広

まったラブレター・ワームは、添付ファイルを開くことによりウィルス感染し、メールソフトに登録されているアドレスに対して、感染ファイルを自動送信することから、世界的な規模で被害を拡大させた。

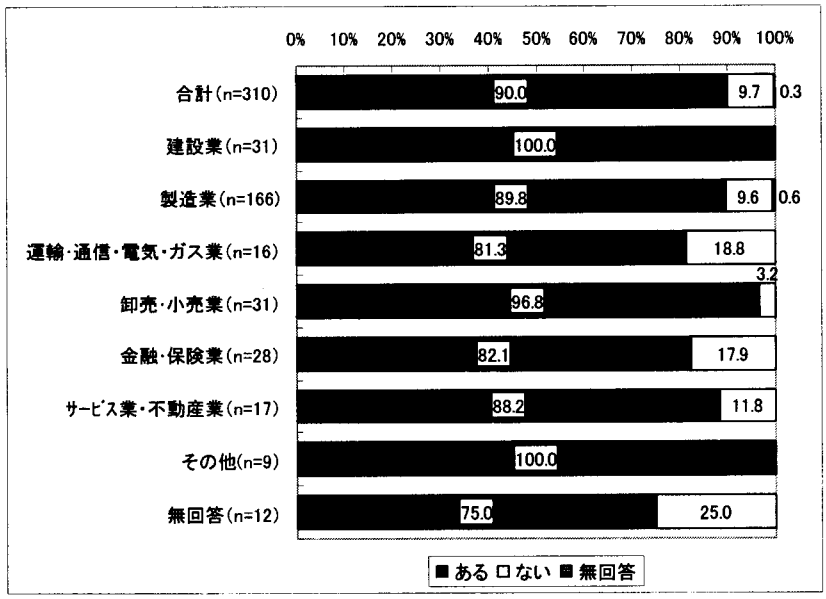
図表3-9　コンピュータウィルス届出件数の推移



資料：情報処理振興事業協会（http://www.ipa.go.jp）

実際、企業の90.0%はコンピュータウィルスに感染した経験を持っており、ネットワークを利用する上で、コンピュータウィルスへの対策を行うことは必須となっている状況が伺える。

図表3-10　コンピュータウィルスの感染経験

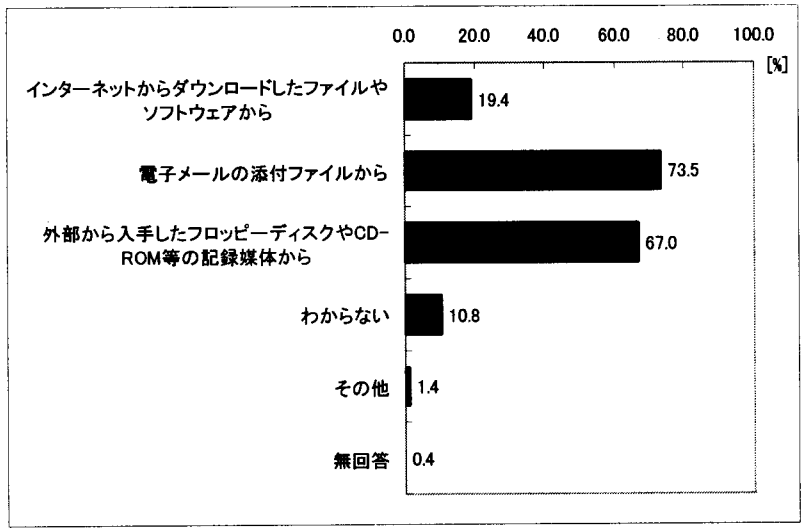


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

コンピュータウィルスの感染経路としては、ラブレター・ワーム等のように電子

メールの添付ファイルから感染しているケースが多い（73.5%）。また、外部から入手した記録媒体から感染するケースも多くなっている（67.0%）。

図表3-11　コンピュータウィルスの感染経路（複数回答、n=279）

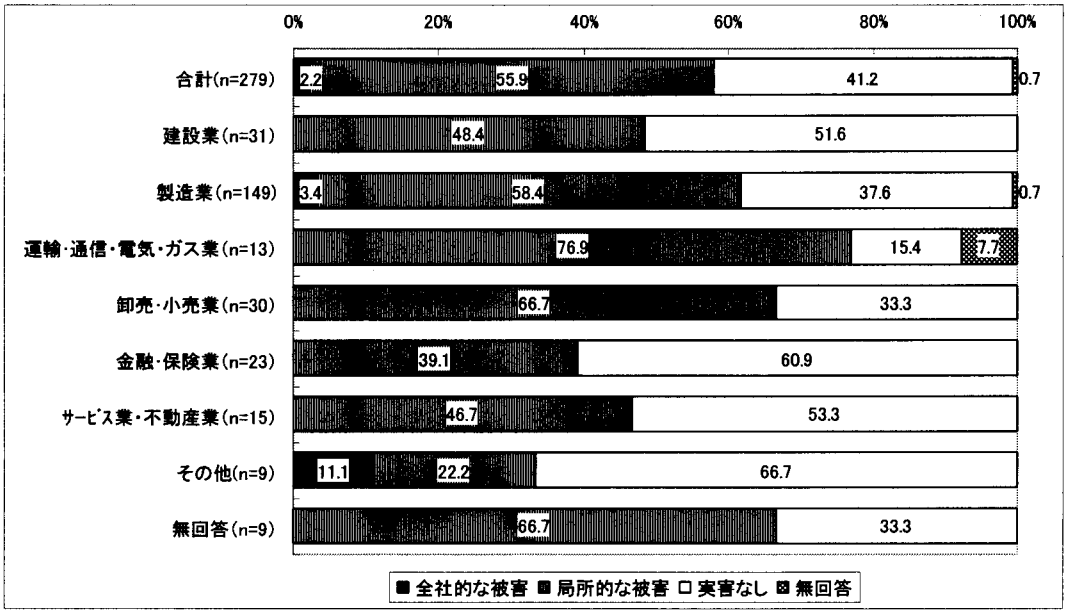


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

現在のところ、コンピュータウィルス感染による被害規模は、全社的な被害にまで及んでいるケースは少ない。しかしながら、感染した企業の約６割は、そのほとんどが局所的な被害ではあるが、実害を被っている。業種別には、運輸・通信・電気・ガス業、卸売・小売業、製造業において被害を受けた比率が高くなっている。

さらに、コンピュータウィルスの被害は、社内の情報資産が直接的に受ける被害にとどまらない。コンピュータウィルスに感染したファイルを、取引先企業や顧客に対して送ることにより、企業の社会的な信用が損なわれる恐れがある。コンピュータウィルスを経営上のビジネスリスクとしても認識していく必要性が指摘されている。

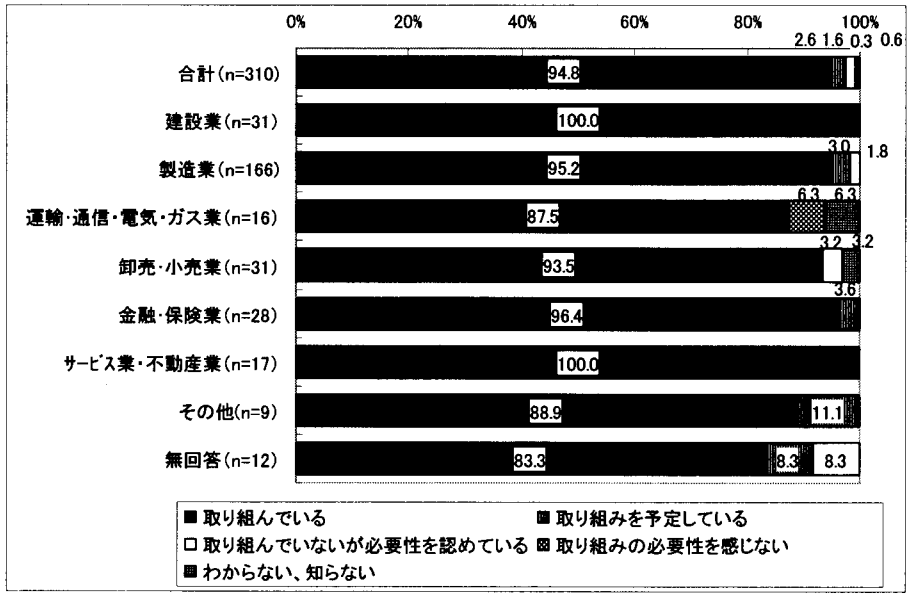
図表3-12　コンピュータウィルス感染によるの被害の規模



資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

既に多くの企業がコンピュータウィルスに感染した経験があることもあり、コンピュータウィルス対策の必要性は多くの企業で認識され、対策が実施されている。業種別にも取り組み状況に大きな違いはなく、幅広い企業が既にコンピュータウィルスへの対策に取り組んでいる。

図表3-13　コンピュータウィルス対策への取り組み状況

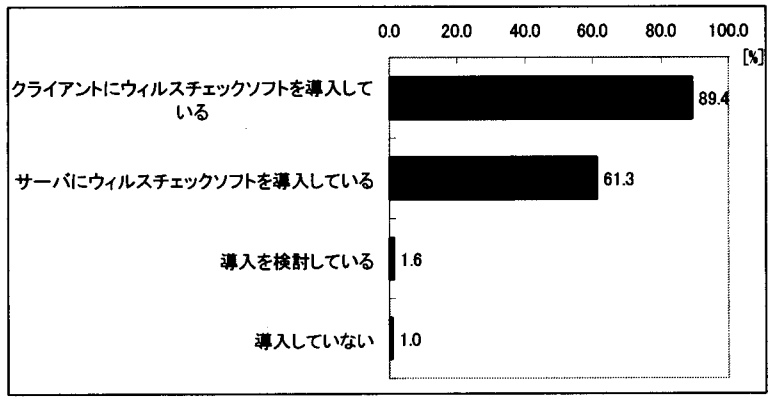


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

コンピュータウィルス対策として、ウィルスチェックソフトの導入は広く行われて

いる。導入していない企業は 1.0%に過ぎない。ウィルスチェックソフトをクライアントに導入している企業は 89.4%、サーバに導入している企業は 61.3%に達している。

図表3-14　ウィルスチェックソフトの導入状況（複数回答、n=310）

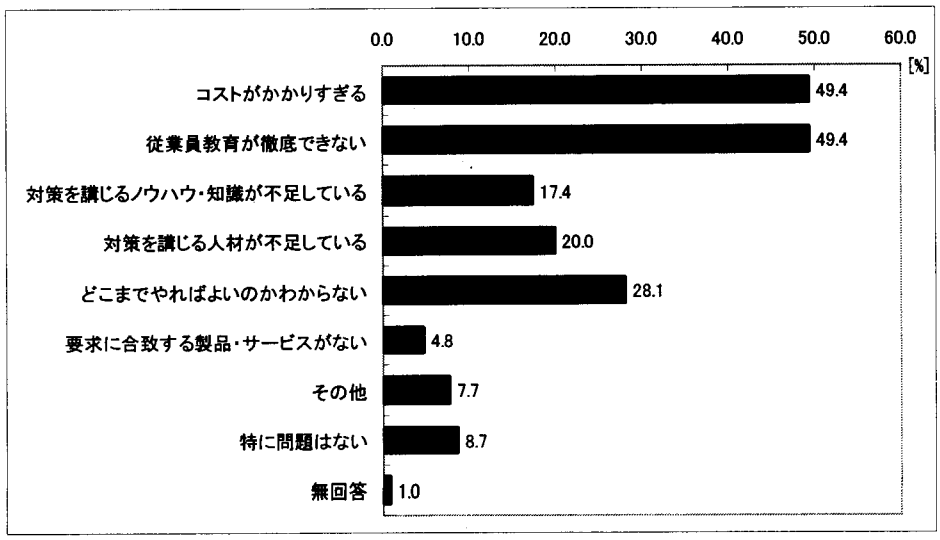


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

コンピュータウィルス対策を行っていく際の問題点としては、半数の企業がコストと従業員教育の徹底という問題を挙げている。ウィルスチェックソフトを導入したとしても社員が適切に利用しなければ、その効果は得られない。

後述する不正アクセス対策と比較すると、「どこまでやればよいのかわからない」、「対策を講じるノウハウ・知識が不足」、「対策を講じる人材が不足」といった問題を挙げる企業は少ない。ウィルス対策に関しては、ウィルスチェックソフトの導入といったシステム面での対応策が比較的わかりやすい。しかし、ウィルスソフトの導入だけでは不十分であり、従業員に対して利用を徹底することや、不審なファイルやメールを開かないよう教育するといった、運用面での取り組みが重要である。課題としても従業教育が徹底できないという問題が多く挙げられていることが特徴である。

図表3-15　コンピュータウィルス対策に関する問題点（複数回答、n=310）



資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

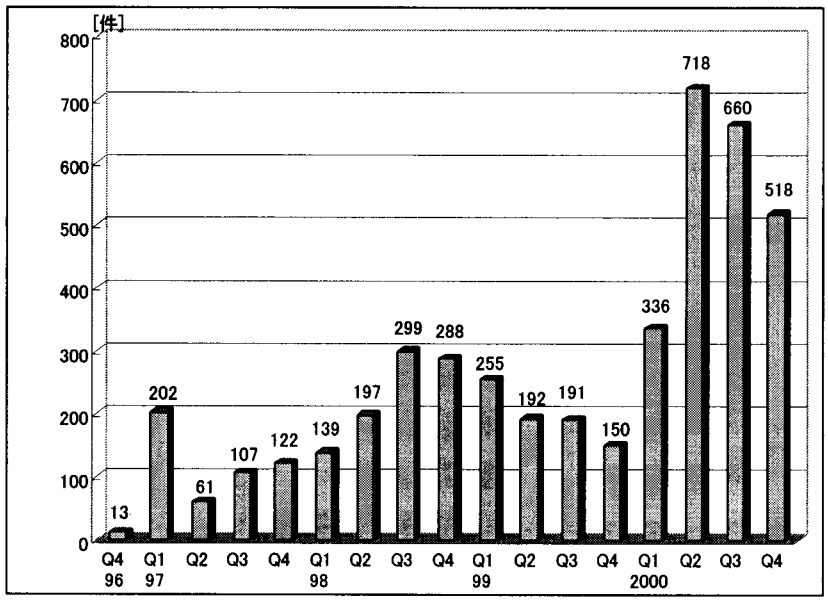
(2)不正アクセス対策

ネットワーク利用の拡大に伴い、近年、不正アクセス件数は大幅に増えてきている。2000年の省庁ホームページの改竄やECサイトへのDoS（Denial of Service）攻撃、2001年2月の日本企業等のホームページ書き換え等、多くの不正アクセス被害が起きており、不正アクセス対策は喫緊の課題となっている。

不正アクセス禁止法の施行日（2000年2月13日）から2000年12月31日までの間に、警察庁に106件の不正アクセス行為が報告され、そのうち25件は海外から不正アクセス行為が行われたことが判明している。また、この期間中に31件の不正アクセス行為が不正アクセス禁止法違反で検挙されている。

コンピュータ緊急対応センター（JPCERT/CC）が受理した不正アクセス件数の推移をみると、2000年に入って不正アクセス件数が急速に増えている状況が伺える。この件数はJPCERT/CCが受理した件数であり、実際の不正アクセスの発生件数や被害件数を表すものではない。不正アクセスの事前調査として行われるポートスキャンは、かなり頻繁に行われている状況になっている。また、手口の巧妙化に伴い、不正アクセスを受けたことに気が付かないことも少なくない。サイバーセキュリティサービス事業者によると、実数はこの100倍近いという認識もなされている。

図表3-16　JPCERTへの不正アクセス届出件数の推移

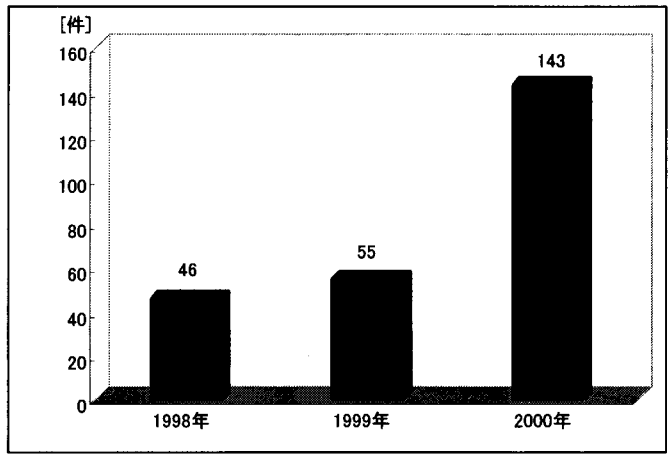


資料：JPCERT／CC資料（http://www.jpcert.or.jp）

その他、情報処理振興事業協会（IPA）に届出されたコンピュータ不正アクセス被害件数でみても2000年に入って増えている状況がわかる。2000年に届出された被害の内容には、メール中継への利用、ファイルやWebの改竄、トロイの木馬などの

埋め込み、不正アカウントの作成、他のサイトへの踏み台、サービス妨害攻撃によるサーバダウン・サービス低下が挙げられている。

図表3-17　IPAへのコンピュータ不正アクセス被害の届出状況の推移

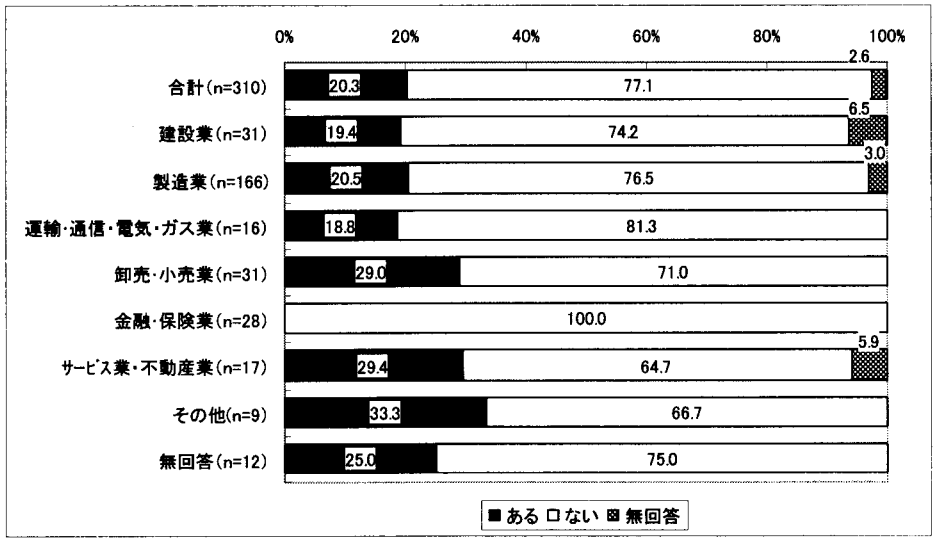


資料：情報処理振興事業協会資料（http://www.ipa.go.jp/）
（注）件数には未遂(実際の被害はなかったもの)も含まれる

企業の被害状況についてみると、ユーザ企業の20.3%がこれまで不正アクセスの被害を受けた経験がある。業種別には、金融・保険業で不正アクセスの被害を受けた企業が1社もないことが特徴である。また、卸売・小売業、サービス業は若干高くなっている。

但し、今後、企業におけるBtoC、BtoBなど、業務との密接なつながりのある分野でネットワーク利用が拡大するのに伴って、不正アクセスを万一受けた場合に受ける損害は多大なものとなる。

図表3-18　不正アクセス被害の経験

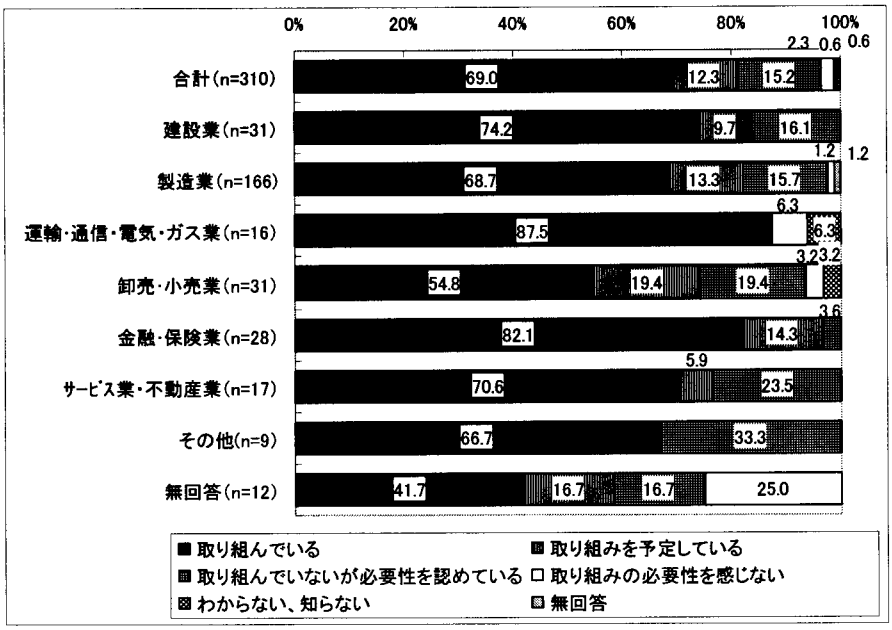


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

不正アクセス対策への取り組みは69.0%のユーザ企業が行っている。さらに取り組みを予定している企業を加えると 81.3%の企業が不正アクセス対策を行う状況となる。既に9割以上の企業が取り組みを行っているウィルス対策と比較すると、必要性は感じながらも実際の取り組みにまでは至っていない企業が多い状況が伺える。

業種別にみると金融・保険業、運輸・通信・電気・ガス業では80%以上の企業が不正アクセス対策に取り組んでいる一方で、卸売・小売業では54.8%にとどまるなど、現状では、業種により取り組み具合にばらつきがある。

図表3-19　不正アクセス対策への取り組み状況

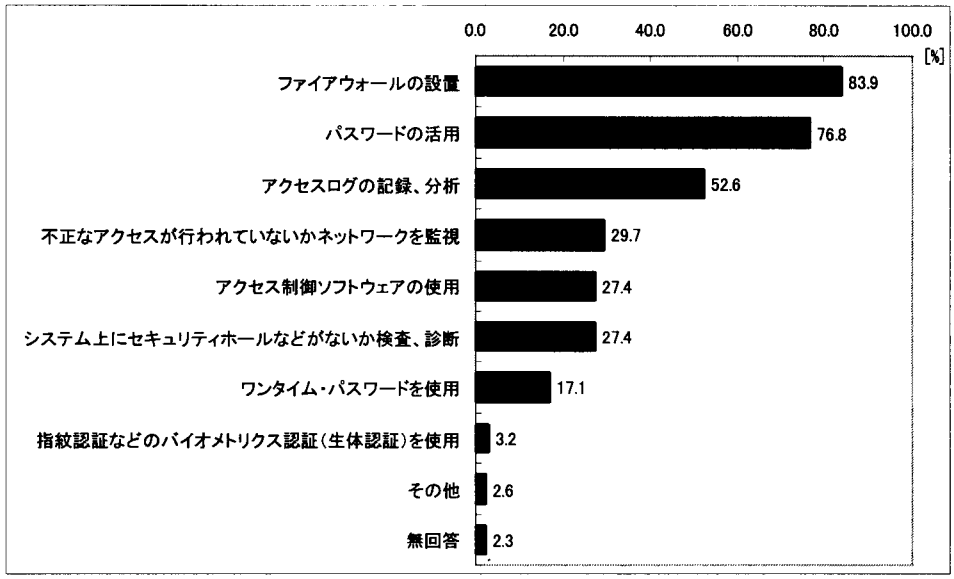


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

具体的な対策としては、ファイアウォールの設置やパスワードの活用が多くの企業で行われている。アクセスログの記録・分析についても半数以上の企業が実施している。ネットワーク監視、セキュリティ検査・診断については3割近い企業が実施している状況である。

但し、ファイアウォールを設置しただけでは不十分であり、適切な設定や修正といった運用面での取り組みを行うことの重要性がサイバーセキュリティ事業者から指摘されている。

図表3-20　不正アクセス対策の実施内容（n=310、複数回答）

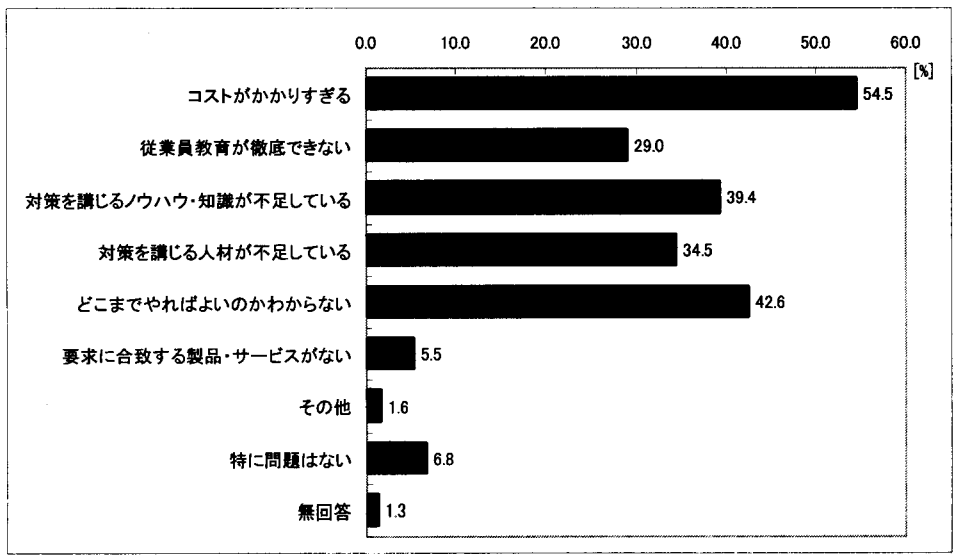


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

不正アクセス対策に関する問題点として、半数以上の企業がコストを挙げている。コストはウィルス対策においても多くの企業が問題としており、サイバーセキュリティ対策全般における問題になっている。

その他、不正アクセス対策では「どこまでやればよいのかわからない」という問題を42.6%の企業が挙げていることが特徴である。ウィルス対策とは異なり、不正アクセス対策では、どのような対策をどこまで行う必要があるのか判断できない企業が多く、専門的なノウハウや知識、人材に関する不足感が強い。

図表3-21　不正アクセス対策に関する問題点（複数回答、n=310）



資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

(3)その他のセキュリティ対策

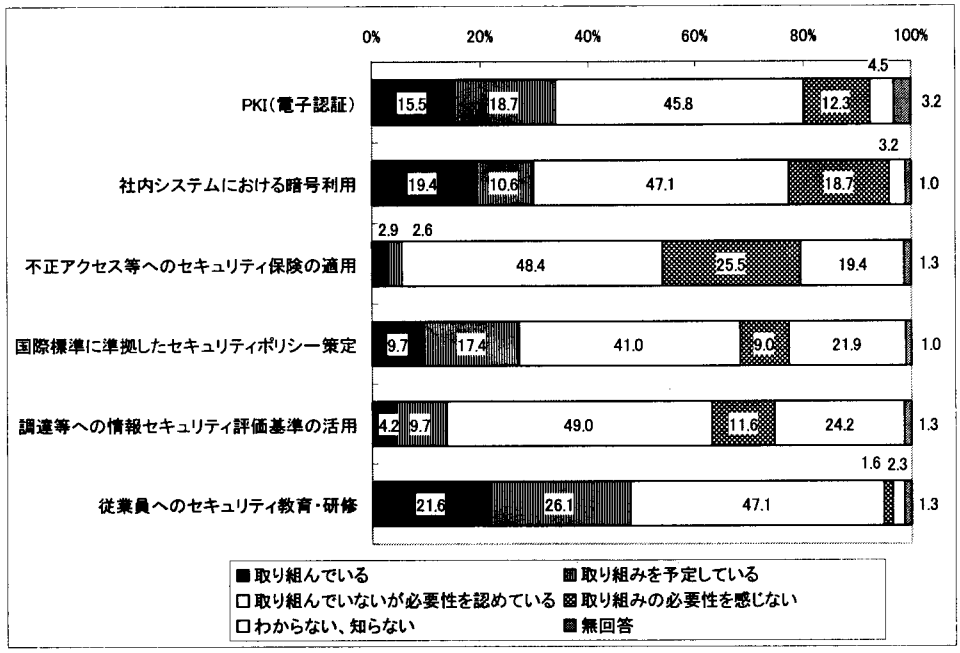
ウィルス対策、不正アクセス対策以外のサイバーセキュリティ対策は、まだ本格的に取り組まれている状況に至っていない。その中で従業員へのセキュリティ教育は、最も取り組みが進んでおり、多くの企業において必要性が認識されている。既に21.6%の企業が取り組みを行っている。

電子認証や社内システムでの暗号利用については一部の企業において取り組みが進められている。

セキュリティ保険は、「わからない、知らない」とする企業が19.4%あり認知が進んでいないとともに、「取り組みの必要性を感じない」とする企業が25.5%に達している。

また、BS7799やISO15408などの情報セキュリティ国際標準については、「わからない、知らない」とする企業が2割以上あり、認知が進んでいない。

図表3-22　各種セキュリティ対策への取り組み状況（n=310）



資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

4．サイバーセキュリティサービスの利用状況

1．でみたように企業におけるネットワーク利用は拡大している。利用の拡大に伴い、コンピュータウィルスや不正アクセスなどが、企業活動に対する大きな脅威となる可能性が高まっている。実際、企業の9割はコンピュータウィルスに感染した経験があり、企業の2割は不正アクセスの被害を受けている。

こうしたコンピュータウィルスや不正アクセスによる被害は、自社の情報資産への