2．サイバーセキュリティサービスの提供状況

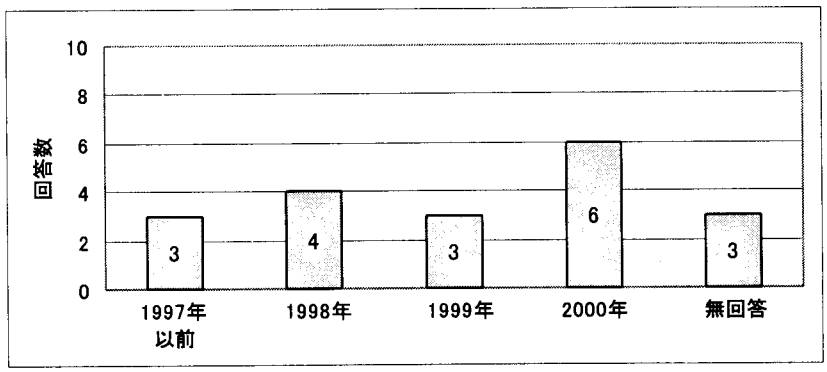
(1) セキュリティポリシー関連サービス

情報セキュリティ対策やセキュアなシステム構築に当たって、組織内で適用される考え方及び方針を体系化したものをセキュリティポリシーと呼ぶ。セキュリティポリシーは、会社などの組織が保有している情報及びシステムのセキュリティを確保するための方針である。

従来、不正アクセスやコンピュータウィルスなどの不正行為に対して、ファイアウォールやワクチンソフトの導入など対処療法的に対応策がとられてきたが、企業活動におけるリスク管理の重要性が認識されるなか、トップダウン方式のセキュリティについての理念であるセキュリティポリシーを策定する企業が増えている。セキュリティポリシーを策定することにより、セキュリティ確保のための対策が体系的に検討でき、実効性もあがるため、安全対策に不可欠なものとして、その重要性が高まっている。

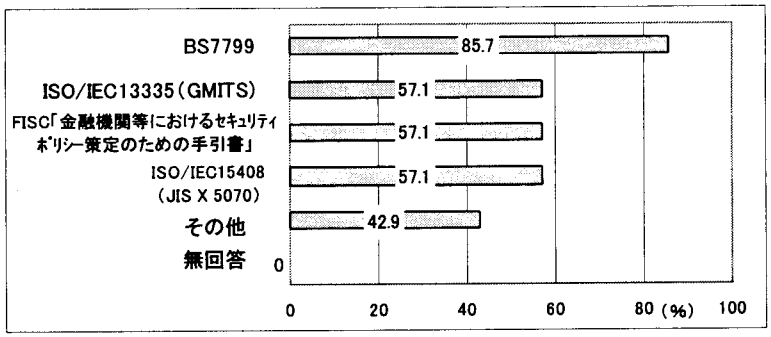
セキュリティポリシーの策定はリスク評価などのノウハウが必要となるため、セキュリティポリシー策定サービスを行っている事業者がでてきている。アンケートでは、全体の5割以上の19社がセキュリティポリシー関連サービスを提供している。サービスの提供開始時期は、1998年以降がほとんどであり、2000年にはいってからサービスを開始した会社も多い（図表2-15）。19社のうち14社が、セキュリティポリシー関連サービスで参照にしている基準等があるとしており、なかでも、BS7799が最も多くなっている（図表2-16）。また、7割にあたる会社（13社）は、市販ツールを利用していない。あるメーカー系の会社では、原子力分野などで蓄積したリスク解析などのセキュリティ手法を適用するといったことも行われている。

図表2-15　セキュリティポリシー関連サービス開始時期（N=19）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

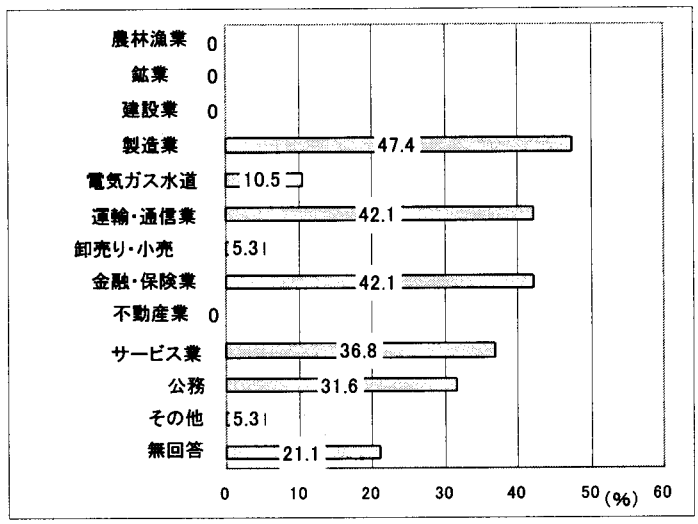
図表2-16　セキュリティポリシー関連サービスで参照している基準（N=14、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

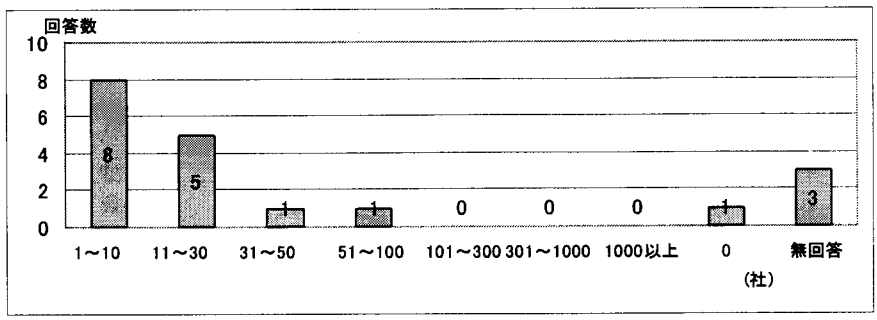
セキュリティポリシー関連サービスの顧客で多いのは、「製造業」で最も多く、次いで「運輸・通信業」「金融･保険業」である（図表 2-17）。また顧客数は、「１～10 社」が最も多く、次いで「11～30 社」である（図表 2-18）。

図表2-17 セキュリティポリシー関連サービスにおける顧客の業種（N=19、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

図表2-18 セキュリティポリシー関連サービスにおける顧客数（N=14）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

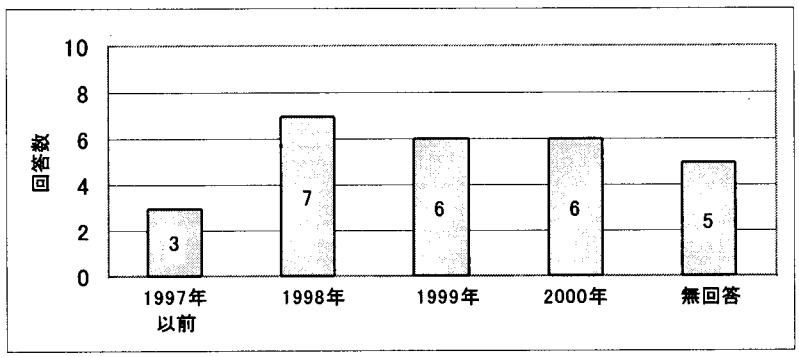
(2) セキュリティチェックサービス

セキュリティチェックは、顧客のネットワークにセキュリティホールがないか、また、各種機器の設定が正しいものになっているか検査するもので、セキュリティ検査ツールを使用するものが多いが、例えば新しいセキュリティホールなどツールで不十分なところについては技術者が検査を行う。また、実際に外部から顧客のネットワークに侵入を試みるペネトレーションサービスも行われている。これは、外部から侵入を試み、重要情報が漏れる可能性があるかどうかを検査するサービスで、クラッカと同じ手口により、セキュリティ・ホールを見つけるものである。

最近の傾向として、企業の社内システムが大規模になってきており、検査の対象となるサーバー等が急速に増加していることがある。

こうしたセキュリティチェックサービスを全体の 3/4 にあたる 27 社が提供している。サービスの提供開始時期は、1998 年以降がほとんどであり、1997 年以前は 3 社にすぎない（図表 2-19）。セキュリティチェックサービスを提供している会社の 7 割の会社（回答があった 26 社中 19 社）がセキュリティチェックにて市販ツールを利用している。

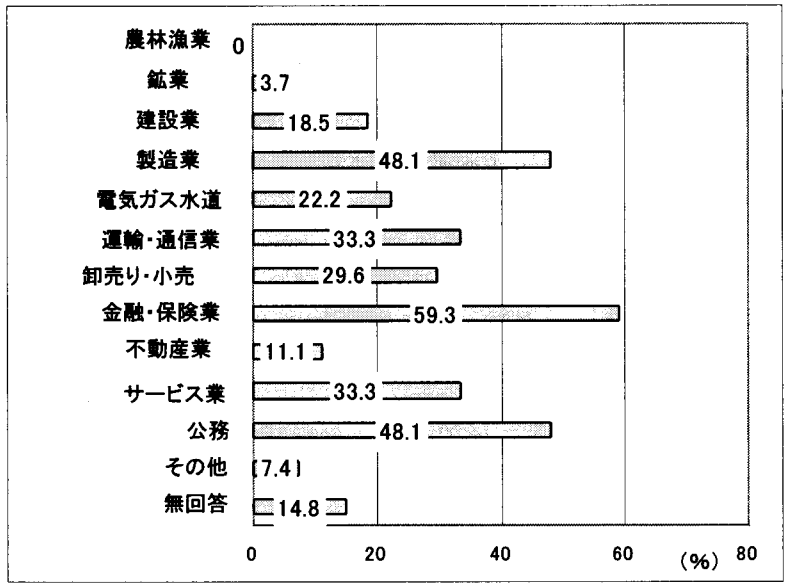
図表2-19　セキュリティチェックサービス提供時期（N=27）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

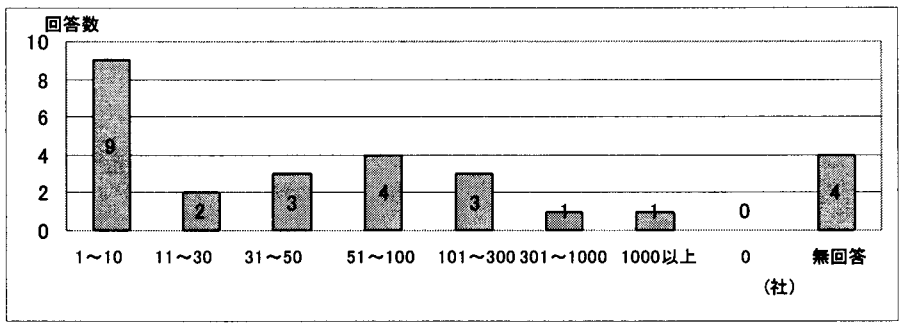
セキュリティチェックサービスの顧客の業種は、「金融・保険業」が最も多く、次いで「製造業」である（図表 2-20）。また、顧客数は「1～10 社」が最も多く、次いで「51 社～100 社」である（図表 2-21）。

図表2-20　セキュリティチェックサービスにおける顧客の業種（N=27、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

図表2-21　セキュリティチェックサービスにおける顧客数（N=27）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

(3) セキュリティ監視サービス

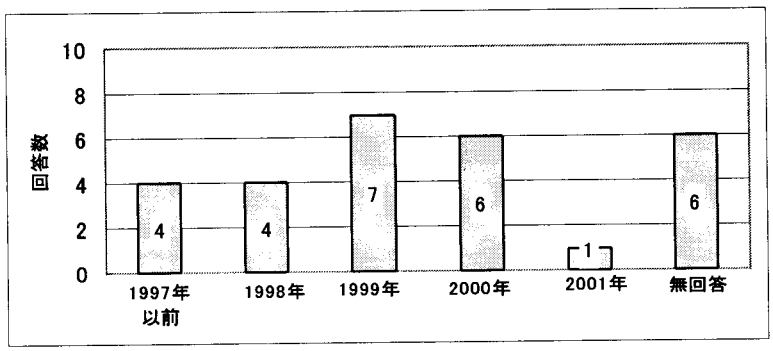
セキュリティ監視サービスは、顧客のネットワークに不正アクセスを検知するシステムを導入し、サービス事業者が監視するサービスである。ログを監視するシステムを設置することで不正アクセス等を監視するサービスもある。また、顧客企業に入り、内部サーバーへの不正アクセスやセキュリティポリシーの違反を監視することも行われている。米国では、不正アクセスの多くが内部からのものであると言われており、損害も大きくなるため、大きな留意が払われている。

一旦、不正アクセスが発生すると、リモートで可能な対策を講じるとともに、顧客側のシステム担当者への連絡、対処方法の指示等を行う。

こうしたセキュリティ監視サービスを全体の 8 割近い会社（28 社）が提供している。

サービスの提供開始時期は、1999 年以降が多く、1997 年以前は 4 社にすぎない（図表 2-22）。セキュリティ監視サービスを提供している会社の 3/4 にあたる 21 社が市販ツールを利用しているとしている。

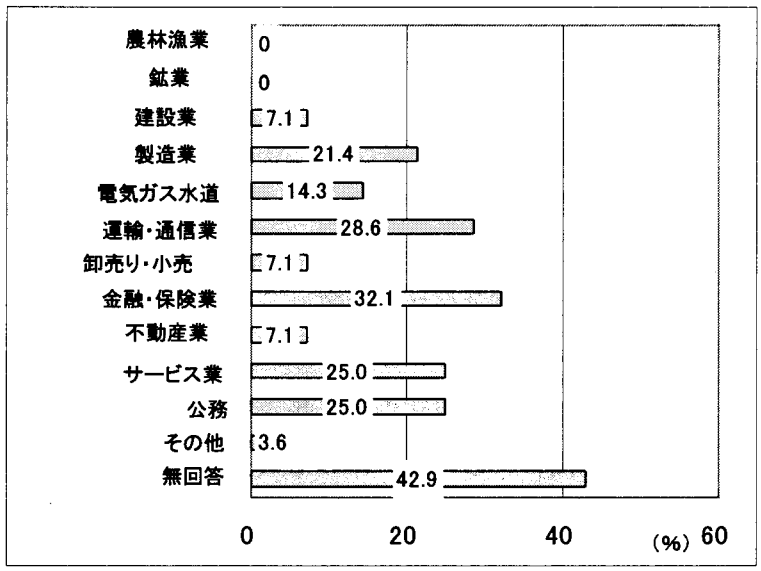
図表2-22　セキュリティ監視サービス提供時期（N＝28）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

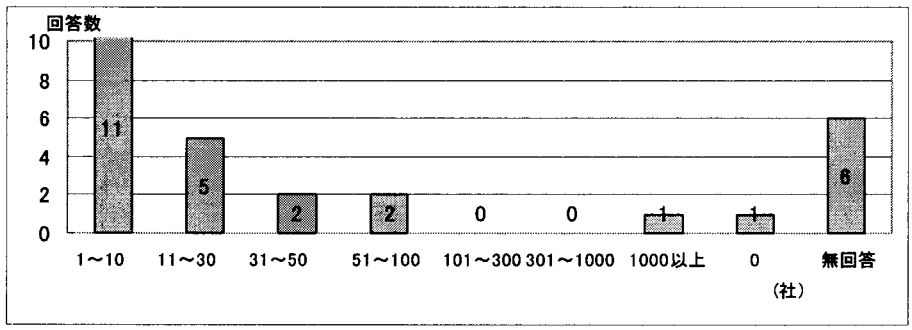
監視サービスの顧客の業種は、「運輸・通信業」と「金融・保険業」が最も多くなっている（図表 2-23）。また、顧客数は「１～10 社」が最も多く、次いで「11～30 社」である（図表 2-24）。

図表2-23　セキュリティ監視サービスにおける顧客の業種（N=28、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

図表2-24　セキュリティ監視サービスにおける顧客数（N=28）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

(4) トレーニングサービス

サイバーセキュリティの分野が新しいこともあり、セキュリティの分かる人材は少なく、サイバーセキュリティ事業者、ベンダー（システム構築者）、ユーザー企業といった各方面で人材が必要とされている。すなわち、人材需要が供給を大幅に上回っている状況である。

こうしたことから様々なトレーニングサービスが行われている。例えば、財団法人日本情報処理開発協会中央情報教育研究所（CAIT）では、経営管理層や情報システム部門の責任者、情報システムの運用管理者等を対象として、情報システムにおけるリスク、セキュリティ対策、システム監査とその考え方などについての研修を行って

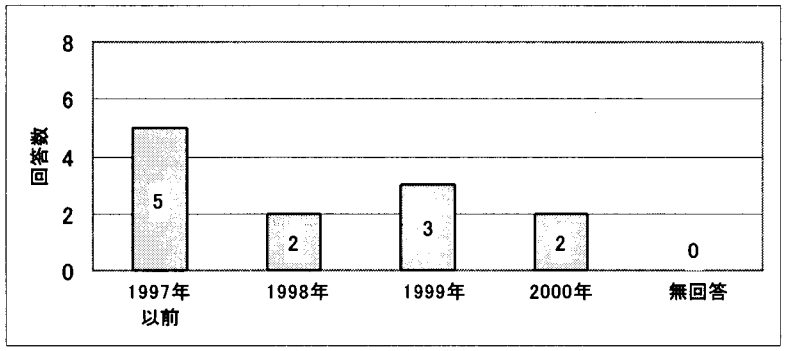
いる。また、ベンダーと一緒にセキュリティ技術者の研修事業を手掛ける人材派遣会社も出てきている。

セキュリティサービス事業者では、ユーザー企業のセキュリティに対する理解を深めるため、無料セミナーなどを開催している会社も多い。また、顧客企業のシステム運用者に対する研修が行われている。

アンケートでも、1/3 の 12 社がセキュリティ関連のトレーニングサービスを提供している。サービスの提供開始時期は、1997 年以前が多い（図表 2-25）。

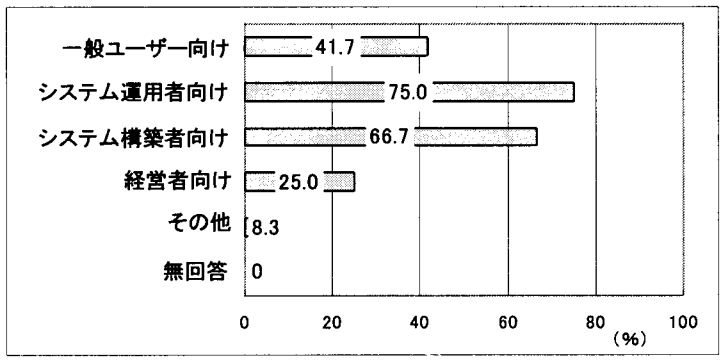
セキュリティ関連のトレーニングの対象者としては、一般ユーザー、システム運用者、システム構築者それぞれに対して行われている（図表 2-26）。トレーニングにおける修了認定制度を有している会社が 6 社ある。

図表2-25　セキュリティトレーニングサービス提供時期（N＝12）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

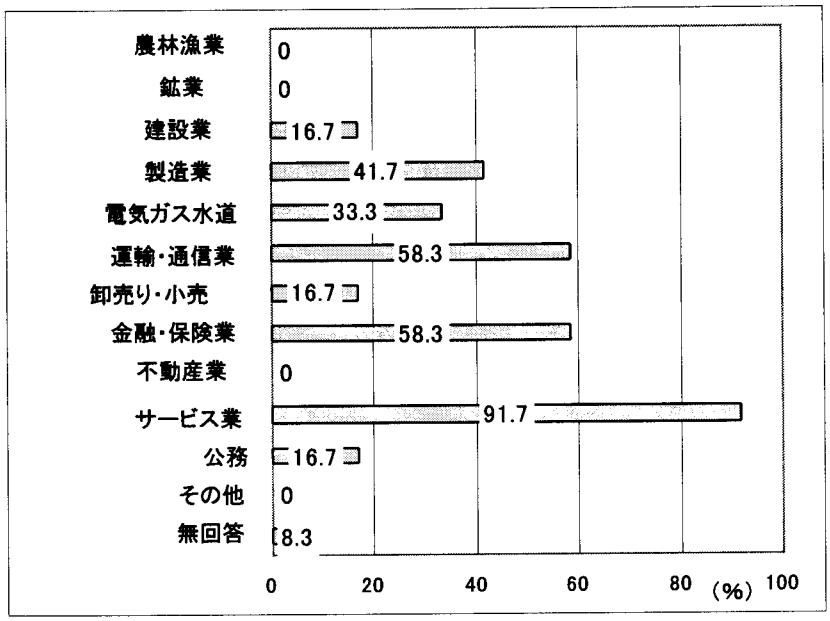
図表2-26　セキュリティトレーニングサービス対象者（N=12、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

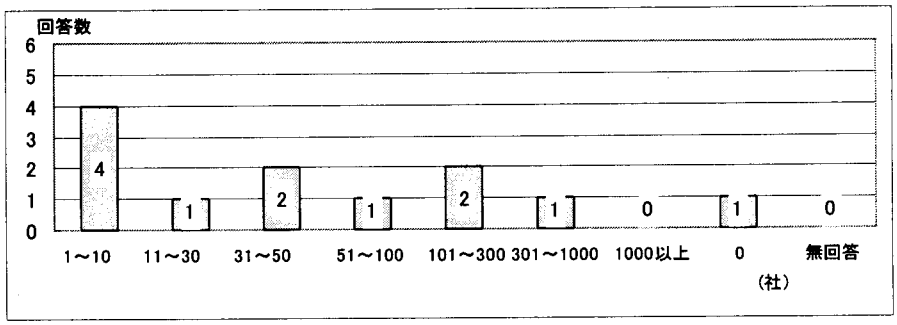
トレーニングサービスの顧客の業種は、「サービス業」が最も多くなっている。「運輸・通信業」と「金融・保険業」も多い（図表 2-27）。また、顧客数は「1～10 社」が最も多い（図表 2-28）。

図表2-27　セキュリティトレーニングサービスにおける顧客の業種（N=12、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

図表2-28　セキュリティトレーニングサービスにおける顧客数（N＝12）



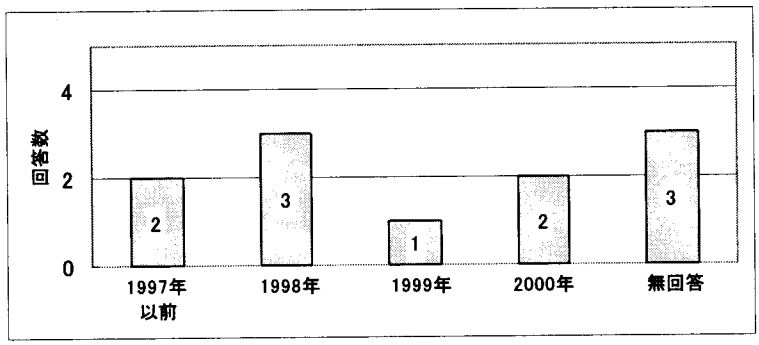
資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

(5) 緊急時対応サービス

緊急時対応サービスは、顧客のネットワークに対してなんらかの被害を受けた、あるいはその疑いがある場合に、顧客企業に出向いて対策を講じるサービスで、顧客システムの停止、被害範囲の特定、不正アクセス手段の解明、再発防止のための対策等を実施する。

こうした緊急時対応サービスを、全体の2割にあたる11社が提供している。サービスの提供開始時期は、1998年以降が多い（図表2-29）。

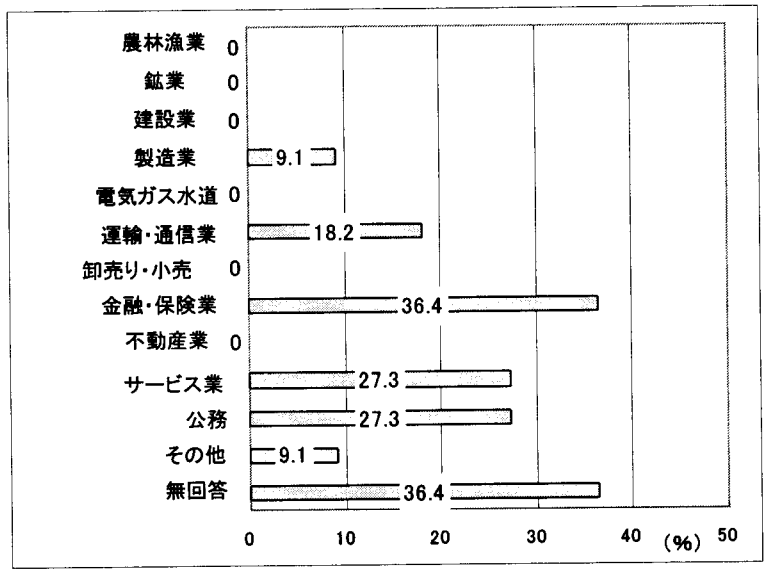
図表2-29　緊急時対応サービス提供時期（N=11）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

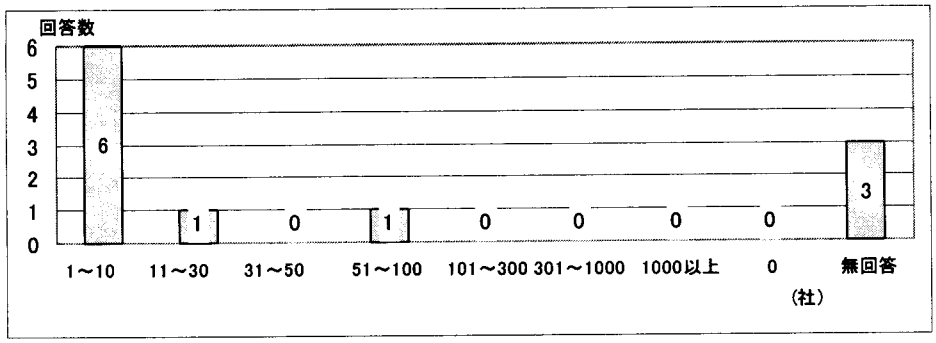
緊急時対応サービスの顧客は、「金融・保険業」、「ｻｰﾋﾞｽ業」、「公務」が多くなっている（図表2-30）。また、顧客数は、「1～10社」が最も多く、次いで「11～30社」と「51～100社」である（図表2-31）。

図表2-30　緊急時対応サービスにおける顧客の業種（N=11、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

図表2-31　緊急時対応サービスにおける顧客数（N=11）



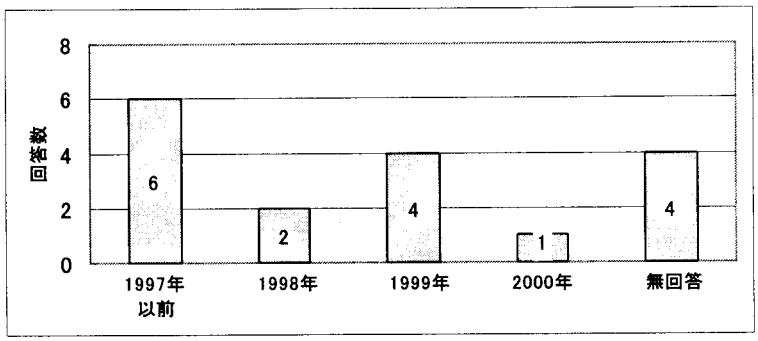
資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

(6) ウィルス対策サービス

通商産業省（現 経済産業省）「コンピュータウイルス対策基準」においては、コンピュータウイルスの定義を、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能といった機能を有するものとしている。コンピュータウイルスに感染すると、典型的な例として異常なメッセージ表示や音楽演奏等の症状がみられるが、ファイルを破壊されるなどの実害を被ることもある。さらに、感染に気付かずにコンピュータウィルスの発信元になり、取引先企業等に多大な被害を与える可能性もあるため、企業内で一定の対策をとっておくことが求められる。

ウィルス対策サービスを提供している会社は、全体の 5 割の 17 社である。サービスの提供開始時期は、1997 年以前が多いが、1999 年も多くなっている（図表 2-32）。

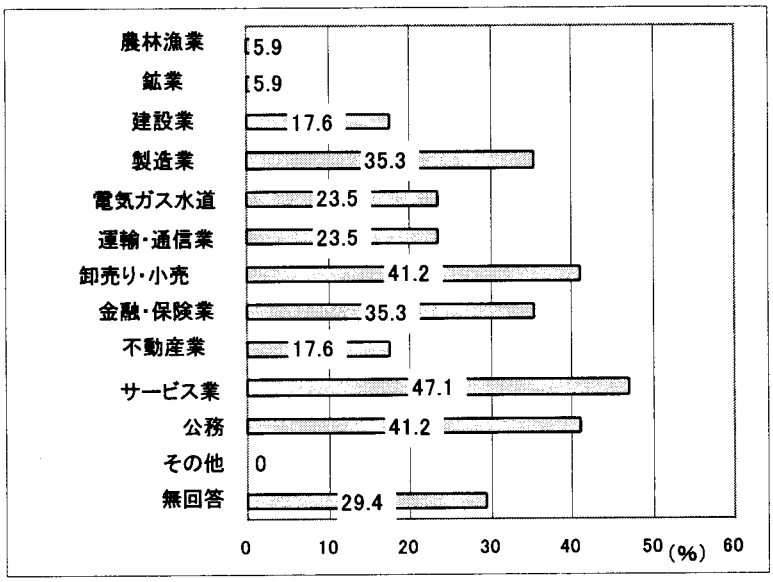
図表2-32　ウィルス対策サービス提供時期（N=17）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

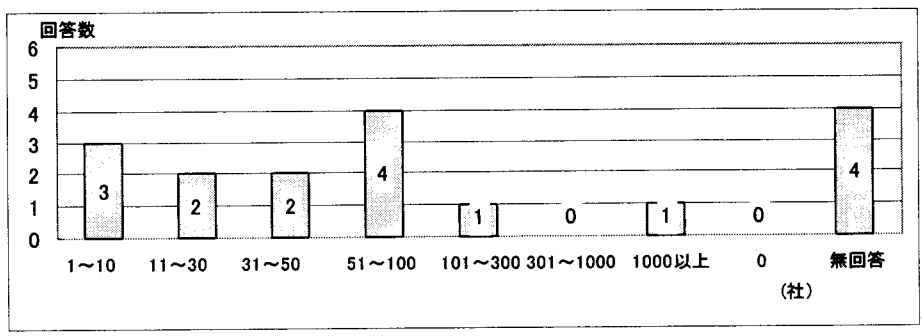
顧客の業種は「ｻｰﾋﾞｽ業」が最も多く、次いで「卸売・小売業、飲食店」と「公務」がである（図表 2-33）。顧客数は「51～100 社」が最も多く、次いで「１～10 社」であるが、なかには 1,000 社以上の顧客を抱える企業もある（図表 2-34）。

図表2-33　ウィルス対策サービスにおける顧客の業種（N=17、複数回答）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」（2000.12）

図表2-34　ウィルス対策サービスにおける顧客数（N=17）



資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」（2000.12）