(3)その他のセキュリティ対策

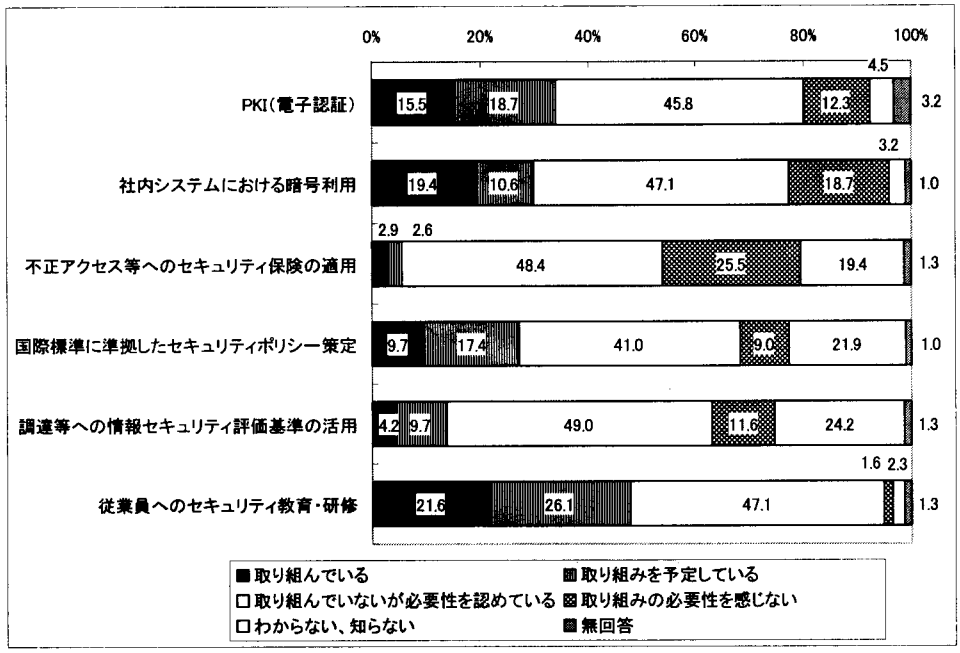
ウィルス対策、不正アクセス対策以外のサイバーセキュリティ対策は、まだ本格的に取り組まれている状況に至っていない。その中で従業員へのセキュリティ教育は、最も取り組みが進んでおり、多くの企業において必要性が認識されている。既に21.6%の企業が取り組みを行っている。

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

直接的な損害だけではなく、ウィルスに感染したメールを他社へ送ることや、他社に対する不正アクセスの踏み台として自社のシステムが利用されるといったことを通じて、企業の社会的な信用を損なうといった大きなビジネスリスクにも通じる。

一方で、不正アクセス技術の高度化や多様化に伴い、ユーザ企業単独で適切なセキュリティ対策を実現していくことは難しくなってきている。多くの企業は、「どこまで取り組めばいいのかわからない」、あるいは「専門的なノウハウや知識が不足している」、「対策を講じる人材が不足している」といった問題を抱えている。

このような背景の中で、専門的な技術や体制を持つサイバーセキュリティサービス事業者に不正アクセス対策に関するアウトソーシングを行う企業が増えてきている。

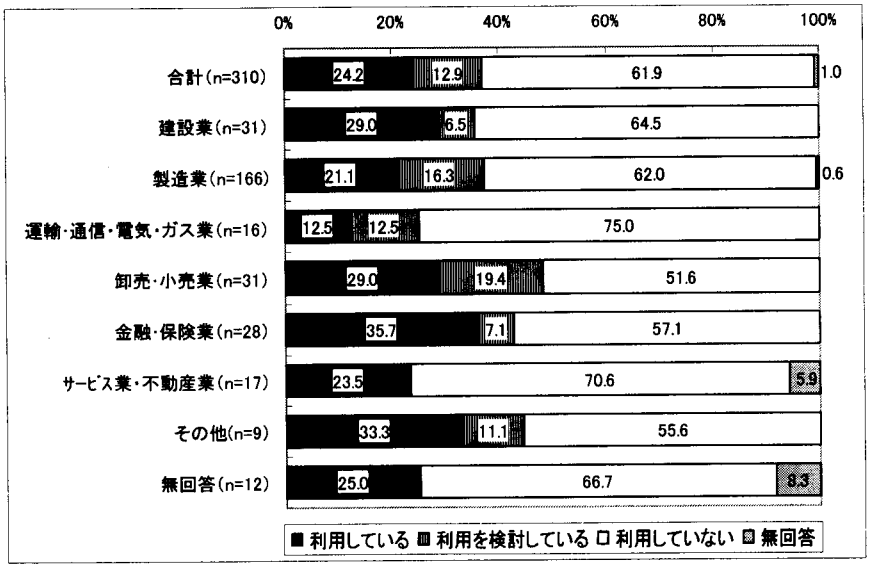
ここでは、企業におけるサイバーセキュリティサービスの利用状況、利用にあたっての課題について整理する。

(1)サイバーセキュリティサービスの利用状況

企業の24.2%は、既にサイバーセキュリティサービスの利用を行っている。さらに12.9%の企業がサイバーセキュリティサービスの利用を検討している。業種的には、金融・保険業、建設業、卸売・小売業による利用が進んでいる。

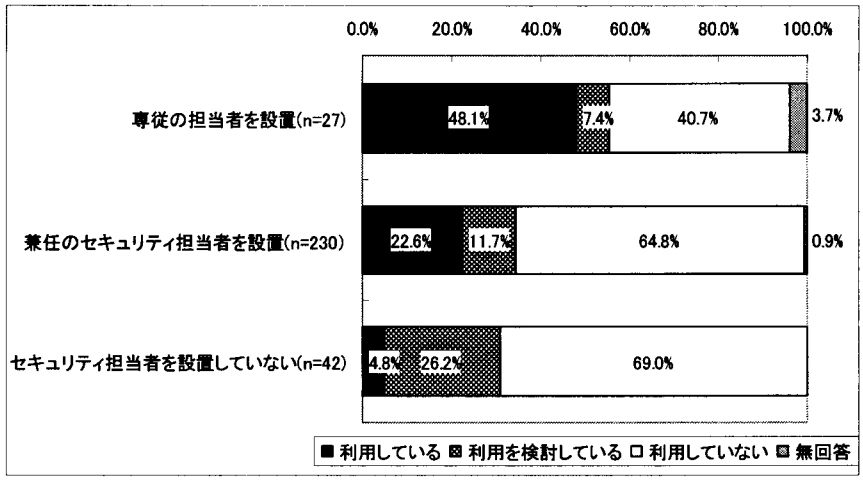
社内に専従のセキュリティ担当者を設置している企業の方がサイバーセキュリティサービスを利用している比率が高くなっている。企業として、サイバーセキュリティへの意識が高く、社内での取り組みが進んでいる企業の方がサイバーセキュリティサービスの必要性や有用性を認めて利用しているケースが多くなっているものと考えられる。

図表3-23　サイバーセキュリティサービスの利用状況



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)

図表3-24　セキュリティ担当者設置状況によるサイバーセキュリティサービスの利用状況

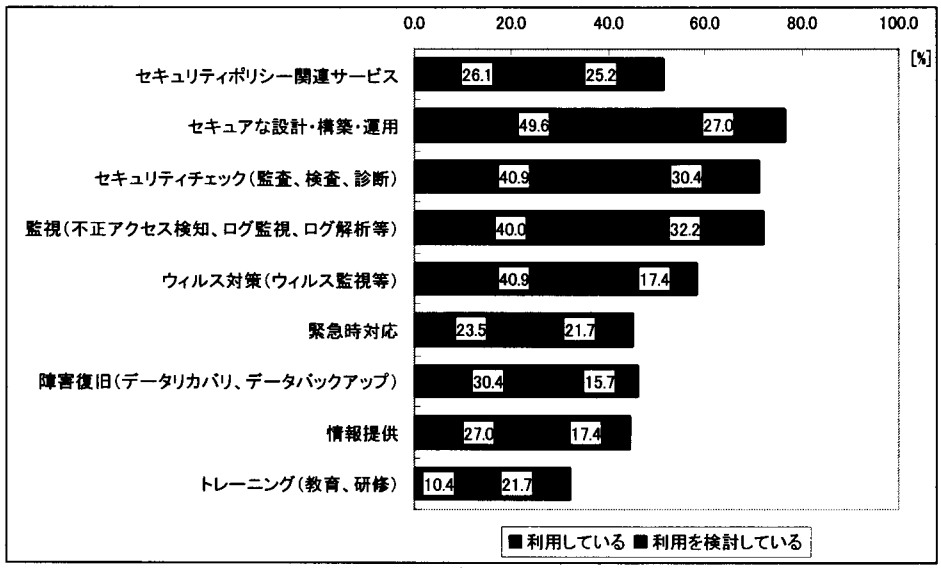


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

企業が具体的に利用しているサイバーセキュリティサービスは、「セキュアなシステム設計・構築・運用」、「セキュリティチェック（監査、検査、診断）」、「ウィルス対策」、「監視（不正アクセス検知、ログ監視、ログ解析）」が多くなっている。

利用を検討している企業も、現在多く利用されているサービスについて利用を検討しているケースが多い。

図表3-25　利用しているサイバーセキュリティサービス（複数回答、n=115）



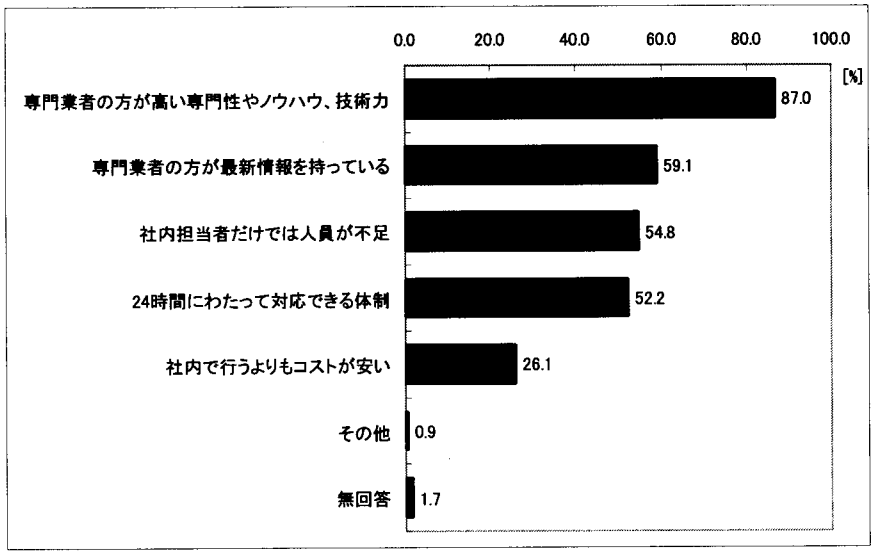
資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

サイバーセキュリティサービスを利用している企業は、専門業者の持つ高い専門性・ノウハウ・最新情報といった自社にない技術力を評価して利用を行っている。

また、自社のセキュリティ体制の要員面での不足を補うために、サイバーセキュリティサービスが利用されているケースも多い。24 時間対応体制を整えるためにサイ

バーセキュリティサービスを利用するケースも多い。自社で24時間の対応体制を行おうとするとセキュリティの素養のある人材を複数名用意して、さらにシフト勤務を行わせることが必要となり、要員面、コスト面から実現は難しい。サイバーセキュリティサービスを利用することにより、専門性の高い体制で効率よく24時間体制の実現が行える。

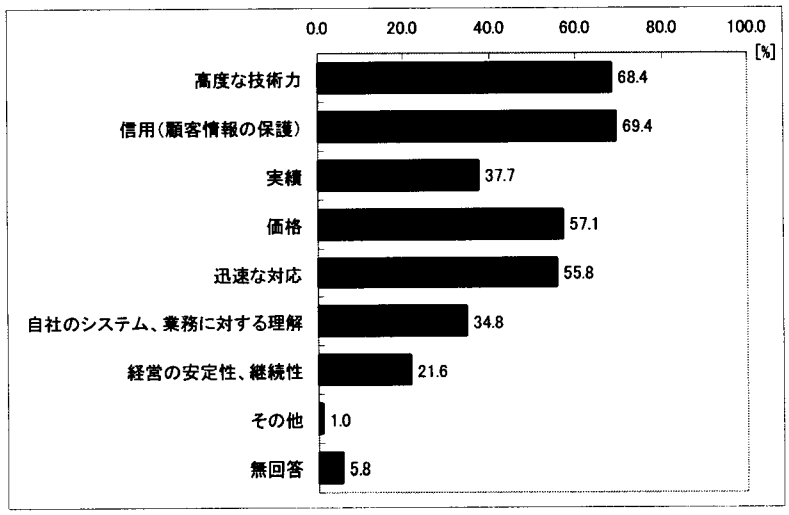
図表3-26　サイバーセキュリティサービスを利用する理由（複数回答、n=115）



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）

企業がサイバーセキュリティサービス事業者を選定する際には、高度な技術力とともに、事業者の信用が重視されている。また、価格も事業者選定にあたって大きな判断材料となっている。

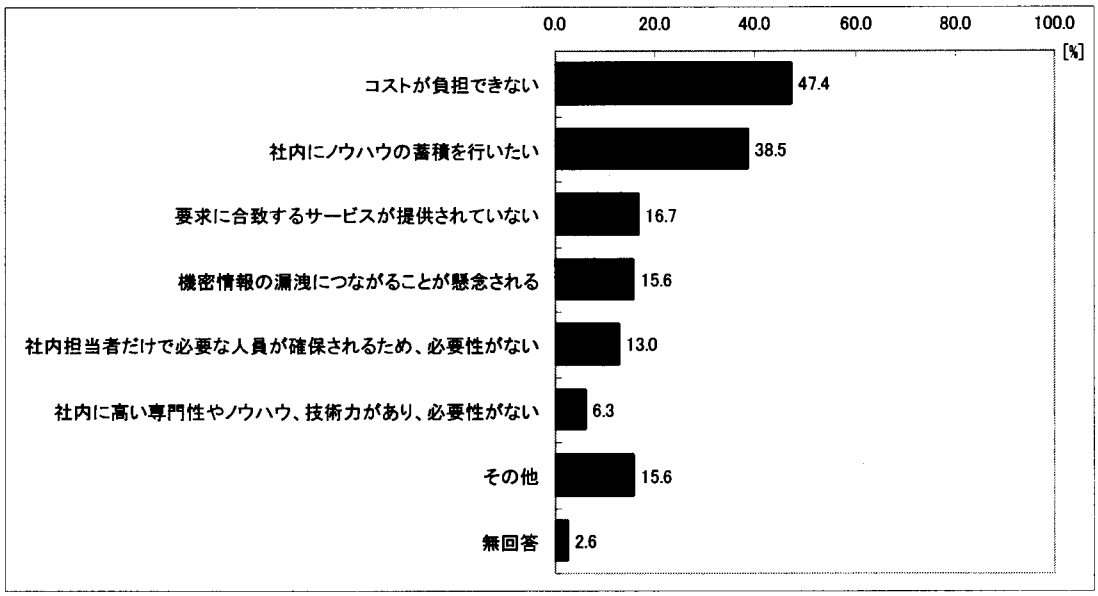
図表3-27　サイバーセキュリティ事業者選定で重視する点（複数回答、n=310）



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）

一方、サイバーセキュリティサービスを利用していない理由には、コストが負担できない、ノウハウを社内に蓄積したいということが多く挙げられている。

図表3-28　サイバーセキュリティサービスを利用しない理由（複数回答、n=192）



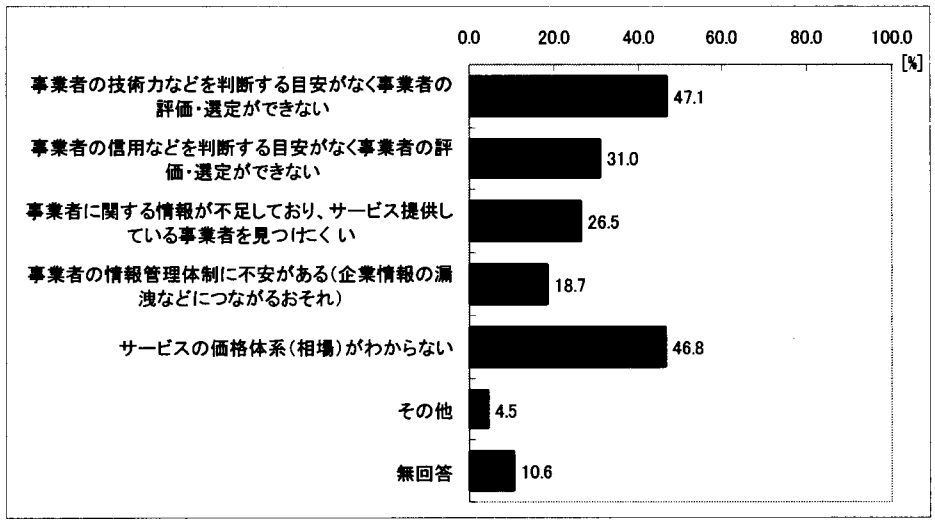
資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

(2)サイバーセキュリティサービス利用にあたっての課題

企業がサイバーセキュリティサービスを利用する上では、事業者の提供するサイバーセキュリティサービスの品質を評価・選定することが難しい点が課題として多く挙げられている。サービスの品質や事業者の信用などは、製品などと比較すると判断することが難しく、利用してみないとわからないという問題がある。また、サービスの価格体系や相場がわからないことも課題として挙げられている。

全般的には、事業者に関する情報が不足しているために、自社のニーズに対してどの事業者のサービスが適しており、そのコストはどれくらいが妥当であるのかがわからないことが問題となっている。

図表3-29　サイバーセキュリティサービス利用上の課題

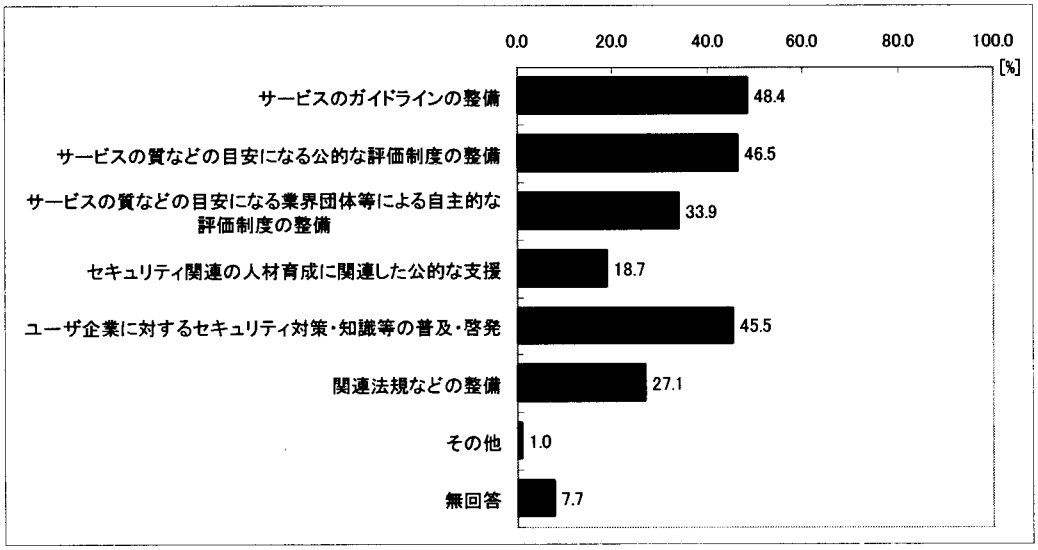


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

サイバーセキュリティサービスの利用を促進していく上で、サービスのガイドラインの整備やサービスの質などの目安になる公的評価制度の整備等の環境整備を進めていくことが望まれている。

また、ユーザ企業においてはサイバーセキュリティ対策の全体像を必ずしも理解していないなど、サイバーセキュリティに関する知識や理解が不足している。そのため、必要となる対策を判断・選択することなどが難しい状況にある。サイバーセキュリティに関する知識等の普及・啓発が望まれている。

図表3-30　サイバーセキュリティサービスの利用にあたって必要となる環境整備



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）