第４章　サイバーセキュリティサービスの課題

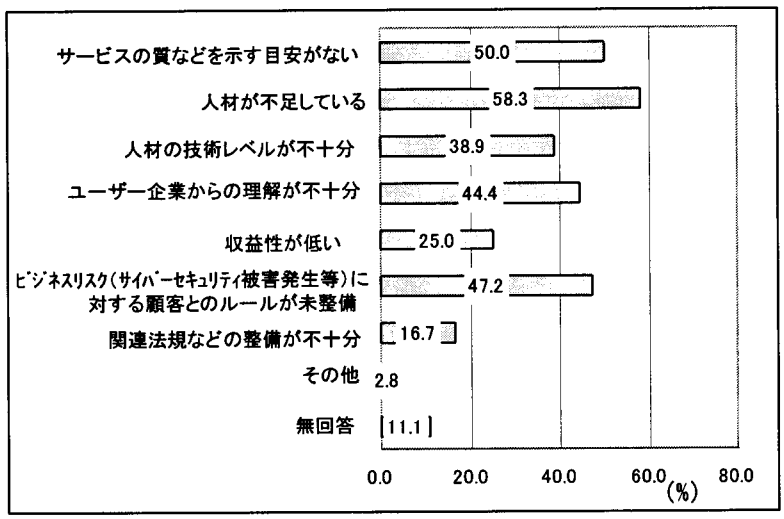
１．サイバーセキュリティサービス業界の抱える課題

ここでは、サイバーセキュリティサービス業界が抱えている課題について、整理する。

事業を行っていく上で、サイバーセキュリティサービス事業者が抱える課題には、「人材不足（量、技術）」、「ユーザ企業のセキュリティへの理解不足」、「サービス品質のばらつき」、「社内管理体制の整備」、「関連法制度の整備」、「顧客とのルールが未整備」がある。

「サイバーセキュリティサービスに関する実態調査」においても、多くの事業者が人材不足、ルールの未整備、サービスの質を示す目安がない、ユーザ企業の業界への理解の不足といった問題を課題に挙げている。

図表4-1　サービス事業者における事業環境の問題点（事業者、複数回答、N=36）



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）

(1)人材不足

事業者のほぼ全てが人材不足の問題を指摘している。

①人材の供給不足

サイバーセキュリティは新しい分野であることから、世界的にセキュリティ技術者が不足している。現在、大学などにおいてもサイバーセキュリティに関する専門的な教育は行われておらず、サイバーセキュリティ技術者の供給が非常に少ない。

また、サイバーセキュリティに関する社会的な認知が不十分であることも人材が集まりにくい要因の一つになっている。

②人材育成の負担大

セキュリティに関する知識を持った人材は少ないため、サービス事業者の多くは、ネットワーク等に関する専門的な知識を持った人材を採用し、セキュリティに関する教育を行うなど、社内で人材を育成している。事業者は一からセキュリティ技術者を育成する必要があり、特に事業規模の小さい事業者においては人材育成の負担は大きなものとなっている。

また、セキュリティ技術者には膨大な知識を要する。ネットワーク等に素養のある人材でも一定レベルに達するまでには数ヶ月の教育が必要になると指摘する事業者もある。さらに、不正アクセス手法やセキュリティホールは増える一方であり、常に最新情報を入手し、対策技術のアップデートを図っていかなくてはならない。情報収集コストや、テストを行うための模擬環境整備など、セキュリティ技術者の育成には多くのコストを要している。

③人材の流出

セキュリティ技術者の引き抜きが多く行われている。そのため、ストックオプション制度の導入や処遇面の見直しなどの取り組みを通じて、技術者の離職防止を図っている事業者も少なくない。

他の IT 業界に人材が流出することも懸念される。サイバーセキュリティに携わる人材にもっと注目があたるようにならないと、負担の大きいサイバーセキュリティ分野から、電子商取引などのより脚光を浴びる分野へと人材が流出する恐れが高まる。

(2)社会、ユーザ企業の理解が不十分

多くの事業者は、社会やユーザ企業のサイバーセキュリティに対する理解が不足していることを課題として挙げている。理解が不足していることから、サイバーセキュリティ対策に取り組むことの必要性が理解されにくく、サービスの利用が進まない。そのため、現状ではサービスを利用しているのは、大手企業などセキュリティへの意識の高い企業が中心であり、市場の広がりが進んでいない。また、サービスに対して対価を支払うという意識が低く、製品導入を伴わないサービスへの理解が不足している。こうした問題は、事業者の事業性や収益性の問題にも繋がっている。

①サイバーセキュリティ対策を自社の問題と捉えていない

企業においては、未だ不正アクセスなどは他人事といった意識をしている企業が多い。特に地方の企業においてその傾向は顕著である。概して首都圏に所在する企業においては、サイバーセキュリティ対策の必要性についての理解が高まってきているが、地方ではまだシステム構築やネットワークの利用が進んでいないこともあり、セキュリティに対する意識が低い状況にある。

②不正アクセスによるビジネスリスクを過小評価

不正アクセスによるビジネスリスクが過小評価されることも多く、サイバーセキュリティへの取り組みが進んでいない。

自社は本格的なネットワーク利用をしていないから、万一、不正アクセスが行われても大きな損害が生じないと考えても、自社のサーバが他社への不正アクセスの踏み台に利用され、社会的な信用を失うことや他社から損害賠償請求を受けるといった大きなビジネスリスクに発展する可能性は低くない。

③経営層の理解が得られない

サイバーセキュリティ対策は、情報システム部門が対応すべき問題であり経営問題として捉えられていない。そのためサイバーセキュリティ対策にコストをかけることへの経営層の理解が得られにくい状況にある。

④サイバーセキュリティ対策に対する知識の不足

サイバーセキュリティ対策を行っていく上で、ユーザ企業も、ある程度サイバーセキュリティ対策に関する知識を持つ必要がある。サイバーセキュリティの要素技術を俯瞰し、その全体像を理解した上でなければ、必要となる対策を判断できず、サイバーセキュリティサービスの選択も行えない。

(3)サービス品質のばらつき

同じサイバーセキュリティサービスでも、事業者によってサービスの品質にばらつきがある。十分な品質のサービスを提供しないと不正アクセスを防ぐことができない可能性がある。

また、サービスは利用してみないとその優劣を判断することは難しい。サービスの

品質を判断する上で何らかの目安となる指標が求められているが、一方でサービスの品質を評価することは容易ではない。サービスの品質は、技術力やスキルだけではなく、品質管理に対するサービス業としての企業の体制に依存する部分が大きい。

事業者としても、サービスの品質を顧客に対して十分に示すことは難しく、現状では、実績をもとにサービスの評価が行われているケースが多い。

(4)社内管理体制の整備

セキュリティサービスに従事する社員の倫理が問題となる可能性がある。海外では、セキュリティ検査を行う際に顧客企業のシステムにバックドアをしかけ、あとから不正アクセス行為を行うといった事件も起きている。

サイバーセキュリティ事業者に対して、ユーザ企業からこうした事故が生じないように、どのような対策を行っているのか説明を求められるといったことが、今後増えていくものと考えられる。その際に、社会に対して説明が行えるだけの管理体制を整えておく必要がある。

(5)顧客との取り決め

サイバーセキュリティサービスのカバーする範囲について、顧客であるユーザ企業と事業者との間で十分な取り決めが行われていないことがある。そのため、ユーザ企業とサービス事業者との間で、サービスの適用範囲について考え方に齟齬が生じるといった恐れがある。

そのため、サイバーセキュリティサービスの提供にあたっては、サービス事業者と顧客との間で、サービスがどこまでをカバーしているものなのか、取り決めを行っていく必要がある。

(6)関連法制度の整備

サイバーセキュリティは新しい分野であることもあり、関連法規の整備がまだ十分ではない。

例えば、米国では故意にコンピュータ・ウィルスを配布する行為を犯罪であるとする州法[1]が成立しているが、国内ではまた取り決めがなされていない。

---

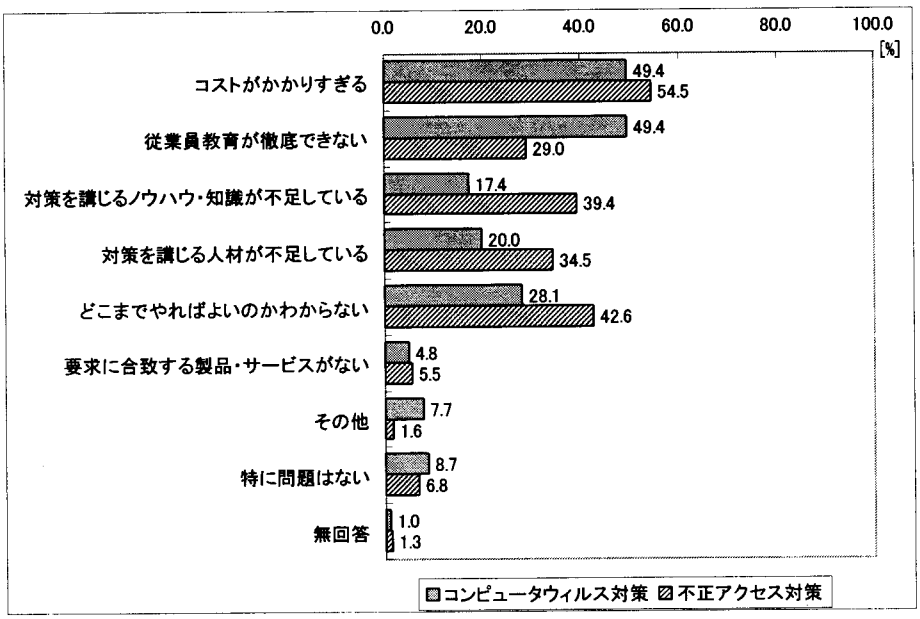
[1] ペンシルバニア州では故意によるコンピュータウィルスの配布を犯罪であるとする法案を可決、2000年7月末から施行。

2．ユーザ企業が抱える課題

サイバーセキュリティ対策を行うにあたって、ユーザ企業は、コストの問題やノウハウや知識の不足、人材の不足といった問題を抱えている。

コストはセキュリティ対策全般にわたる課題となっているが、不正アクセス対策では、そもそもどのような対策をどこまで行う必要があるのかを判断できない企業も多い。その理由としては、サイバーセキュリティに関する知識不足も一つの要因となっている。

図表4-2　ウィルス・不正アクセス対策に関する問題点（ユーザ企業、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）

一方で、不正アクセス手法の高度化や多様化が急速に進展しており、もはや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い状況になってきている。そこで、専門的な知識を持ったサイバーセキュリティサービスの利用を検討する企業が増えてきている。

サイバーセキュリティサービスの利用にあたって、ユーザ企業が感じる問題も少なくない。事業者の技術力や信用などを示す指標がなく評価・選定を行うことができない。また、サービスの品質や価格体系・相場がわからないといった問題がある。

これらのことから、ユーザ企業におけるサイバーセキュリティサービスの利用にあたっての課題として、「サイバーセキュリティに関する理解の不足」、「コストが負担できない」、「サイバーセキュリティサービスの質（技術力、信用）が判断できない」といったことが挙げられる。

(1)サイバーセキュリティに関する理解の不足

ユーザ企業の特に経営層をはじめとする従業員におけるサイバーセキュリティに関する理解の不足により、自社がサイバーセキュリティに対して、どの程度取り組む必要があるのか、どのくらいのコストが必要となるのか判断することが難しい。そのため、サイバーセキュリティサービスを利用するにあたって、サービスの評価やコストの妥当性の判断が行えない。

(2)コストが負担できない

サイバーセキュリティ対策を行うためには、相応のコストが必要になるが、ユーザ企業においては、セキュリティ対策にコストがかかりすぎるという認識がされている。サイバーセキュリティサービスの利用を行わない理由としても大きなウェイトを占めている。

サービス事業者の増加などに伴って、サービスの相場の形成が行われつつあるが、ユーザ企業にとっては価格の相場がわからないことも大きな課題となっている。

(3)サービス事業者を選択できない

ユーザ企業は、自社にない高度な技術やノウハウ、専門性の高い人材を得るためにサイバーセキュリティサービスの利用するのだが、事業者が提供するサービスの質を判断するための目安や指標がない。サービスや価格の妥当性等について評価・判断することが難しい。

ユーザ企業においては、総じてサイバーセキュリティサービスに関する情報が不足しているとの認識が強い。