第５章　サイバーセキュリティサービスの発展のために必要な取り組み

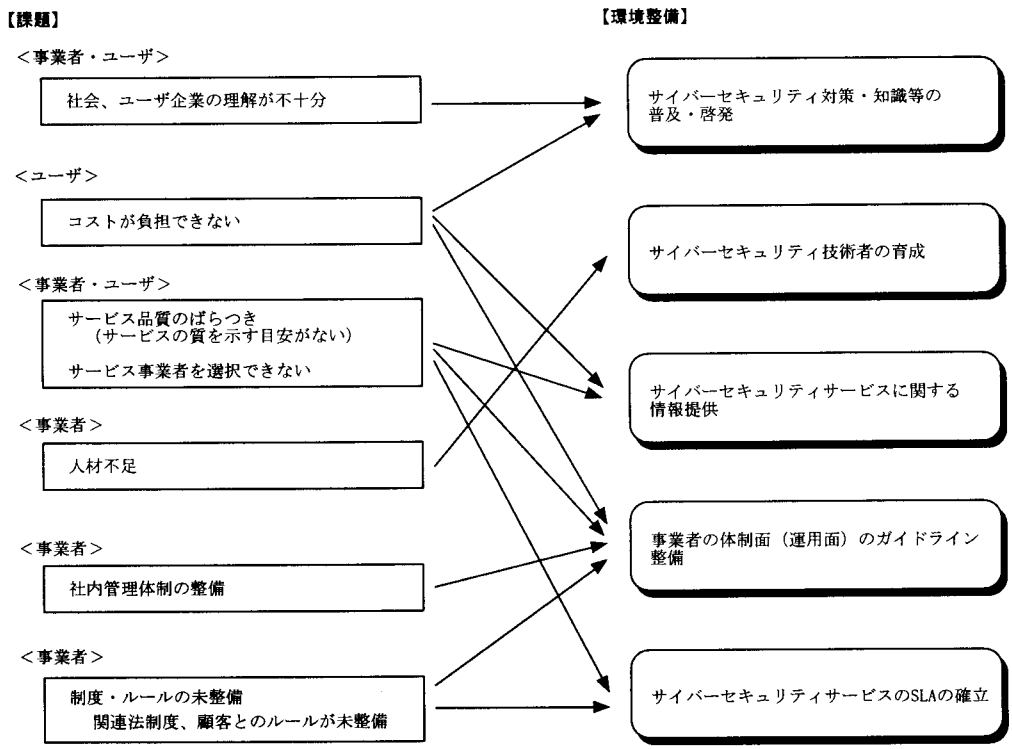
ネットワークの利用の広がりに伴い、情報システムに対する不正アクセスやコンピュータウィルスといった新たな脅威が生じている。高度化するネットワーク上の脅威に対抗していくためには、ファイアウォールといったハードウェアを導入するだけではなく、運用段階においても、設定等を適切に更新していくといった継続的な取り組みが必要となる。

しかし、技術の高度化に伴い、ユーザである企業等がこれらの継続的な取り組みを単独で進めていくことが難しくなってきている。適切なサイバーセキュリティ対策を行う上で、サイバーセキュリティに関する専門的な知識やノウハウを持った事業者のサービスを活用することが有望となってきている。

一方、第４章でみたようにサイバーセキュリティサービスの事業を展開する上で、様々な課題が存在する。これらの課題に対応するとともに、サイバーセキュリティサービスの健全な発展を促していくために、普及・啓発をはじめとした様々な取り組みが求められている。

これらの課題に対応し、さらにサイバーセキュリティサービスの発展を促していくためには、以下のような取り組みが求められる。

図表5-1　課題とサービス発展に向けて求められる取り組み



資料：三和総合研究所作成

1．サイバーセキュリティ対策・知識等の普及・啓発

サイバーセキュリティに対する社会やユーザ企業の意識は、2000年1月の官公庁ホームページ改竄事件などを契機として、高まってきているものの、未だ十分な状況にはなっていない。サービス事業者、ユーザ企業ともにサイバーセキュリティに関する知識の普及・啓発の必要性を指摘している。

社会のあらゆる分野でネットワーク利用が広がる中で、その基盤を支える取り組みとしてサイバーセキュリティの重要性は、今後、ますます高まっていく。さらに、ネットワークが国際的に広がっていく中で、サイバーセキュリティへの取り組みが不十分であることのビジネスリスクは大きなものとなってきている。安全なネットワーク社会を実現し、その利便性を享受するためには、サイバーセキュリティの重要性や対策に関する知識等の普及・啓発を行っていくことが必要である。

具体的には、以下のような取り組みが求められる。

(1)サイバーセキュリティの全体像の理解

現状、ユーザ企業のサイバーセキュリティに関する知識が不足している。そのため、どのような取り組みが必要なのか、あるいは提供されるサービスの質や内容は妥当であるのかといった判断が行えていない。

サイバーセキュリティ対策に取り組むにあたっては、ユーザ企業においてもその要素技術を俯瞰し、サイバーセキュリティの全体像を理解した上で、サービスを利用していく必要がある。

現在は、個々の事業者によりサイバーセキュリティに関する教育や情報提供が行われている。しかしながら、こうした教育や情報提供では、自社の製品・サービスが中心となりやすく、サイバーセキュリティの全体像をつかむことが難しい。そのため、それぞれの技術やサービスがどのように異なり、また、どのような場面で利用していくべきなのかがわからず、ユーザ企業が混乱しやすい状況にある。

個々のベンダーによる普及・啓発では、自社のサービスへの誘導に繋がりやすい傾向があるため、サイバーセキュリティの全体像に関する情報提供を、公的な機関あるいは業界として行っていくことが求められる。

(2)ネットワーク上の脅威に対する理解

多くの企業では、まだ不正アクセスなどの被害は他人事であるという意識を持っている。サイバーセキュリティに取り組まないことへの危険性を意識していない企業が

多い。そのためサイバーセキュリティに多くのコストをかけることが理解されない。そのため、潜在的には大きな市場が見込まれながらも、顧客は未だ一部のセキュリティに対する意識の高い企業だけにとどまり、事業者の収益性の悪化にもつながっている。

現実の被害の数に近い統計データを示すといったことを通じて、不正アクセスの危険性や日常的に起こりうる脅威であることを示していく必要がある。

(3)サイバーセキュリティ対策への取り組みの意識付け

情報提供や教育を受けるだけではなく、自社の情報システムに対する脅威や内在する脆弱点について具体的に示されることにより、サイバーセキュリティ対策の必要性に対する意識が高まる。

そのために、例えば、ネットワーク上で大量の顧客情報を取り扱う事業者や電子商取引などを行っている事業者に対しては、セキュリティ検査やネットワーク監視等を受けることを推奨するといったことを検討していくことが必要であると考えられる。

また、ユーザ企業が自社のセキュリティ対策の水準について自己評価が行えるチェックリストを提示するといった取り組みについても考えられる。

(4)学校教育でのセキュリティ教育

社会におけるサイバーセキュリティに対する意識を高めていくために、学校教育においてセキュリティ教育を行っていくことが求められる。

不正アクセスやコンピュータウィルスの危険性といったサイバーセキュリティに関する知識に関する教育や、情報倫理面に関する教育を実施していくことが重要である。

2．サイバーセキュリティ技術者の育成

(1)サイバーセキュリティ技術者の資格認定制度

サイバーセキュリティ技術者の資格認定制度を通じて、サイバーセキュリティに関する社会的な認知を高め、サイバーセキュリティという職種を確立していくことが期待できる。資格認定制度の導入により、サイバーセキュリティ技術に興味を持つものが増え、技術者層の拡大につながることも期待される。また、セキュリティ技術者のやり甲斐の向上にもつながる。

サイバーセキュリティ事業者の技術力を評価することは難しいが、技術レベルを判

断する一つの指標として資格認定技術者数を利用していくことも考えられる。

実効ある資格認定制度とするためには、ある程度、実技試験を伴うような認定制度の導入についての検討が必要である。

また、技術革新が速い分野であることを考慮し、資格の有効期限や更新の仕組みについての検討が必要である。

資格の分類についての検討を行う必要がある。セキュリティ技術者という大きなとらえ方により、セキュリティに関する基本的な素養を示す資格制度が望ましいのか、あるいは細分化した資格が望ましいのか検討を行う必要がある。

(2)大学教育などにおけるサイバーセキュリティ技術教育

現状では、サイバーセキュリティ技術に関して教育を受ける場は、事業者が主催する教育セミナーなどに限定されており、十分に提供されているとはいえない。そのため、サイバーセキュリティ技術者は、事業者が一から育成していかなくてはならない状況にある。

大学教育などにおいて、サイバーセキュリティ技術者に必要な基礎的な事項に関する教育が受けられる場の提供や、必要な知識を修得できる仕組みを整えることが求められる。

3．サイバーセキュリティサービスに関する情報提供

ユーザ企業がサイバーセキュリティサービスの利用を行う場合に、現状ではサービスの実態や事業者に関する情報が不足しており、サービスを選定・評価することが難しい状況にある。

サイバーセキュリティサービスに関する情報提供を行うことにより、ユーザ企業が不安なくサービスの利用を可能にしていくことが必要である。

4．事業者の体制面（運用面）のガイドラインの整備

現状のサイバーセキュリティサービスにおいては、同じサービスであっても事業者によって、その品質にばらつきがある。サービスの品質は、事業者の技術力だけではなく、サービス業としての品質管理といった企業の体制面に依存するところが大きい。

サイバーセキュリティサービスに関する事業を行っていく上で必要となる、顧客情報の管理やサービス実施にあたっての責任範囲などといった、運用面での取り組みについてガイドラインとして整備していくことが考えられる。ガイドラインの整備により、事

業を行う上で必要な体制面の取り組みが明らかになりサイバーセキュリティ業界全体の信用向上にも繋がる。

５．サイバーセキュリティサービスの SLA（Service Level Agreement）の確立

サイバーセキュリティサービスは新しい分野であることもあり、顧客とサービス事業者との間でのリスク分担の考え方など、ルールが整っていない面がある。

セキュリティサービスに関して SLA のようなものが確立できることが望ましい。

事業者が提供するサイバーセキュリティサービスのレベルを規定できるようになれば、サービスの対価に対する理解も進み、市場の拡大にもつながり得る。