3．サイバーセキュリティサービス事業者における人材

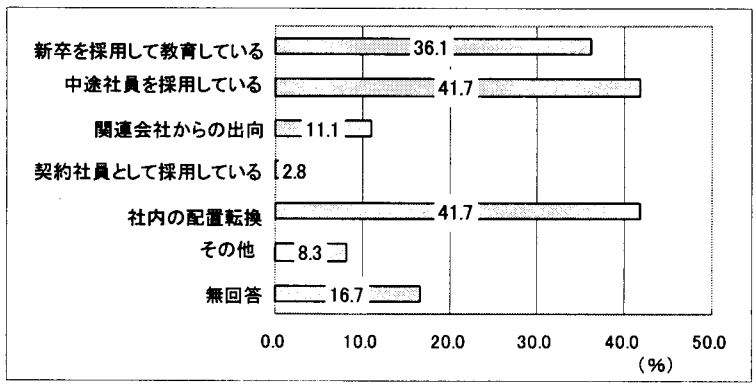
セキュリティサービスを提供していくにあたって、技術力をもった人材確保は不可欠であるが、後に示すように、セキュリティサービス事業者における課題でもっとも多く指摘されているのが人材の不足である。ここでは、採用と教育の面からセキュリティサービス事業者がどのように人材確保を行っているかみていく。

(1)人材採用

即戦力となるノウハウをもった人材を中途採用したいという意向が各社とも強い。ただ、情報通信分野の中でも新しい分野であるためセキュリティ分野に精通した技術者が少ないこともあって、TCP/IP などネットワーク関連の技量を有した人材を確保し、セキュリティ技術者に育成するという会社が多い。各社人材確保にあたっては、様々なアプローチを行っている。ベンダーを中心に社内の配置転換により人材確保をしている会社、また、中途採用を行っている会社が多い。アンケートでも、「経験のある中途社員を採用している」と「社内の配置転換によって行っている」が最も多くなっている（図表 2-35）。

サイバーセキュリティサービスを実施する過程で顧客情報にふれる機会も多いため、従業員にモラルが要求され、頻繁に転職している人などが敬遠されるなど人物に対する評価が非常に重視されている。そのため、社員の知人といったかたちでの採用が多いとする会社もある。このように、人材採用では技量のみならず人物評価も重視されており、適した人材が少ないのが現状である。

図表2-35　人材の確保形態（N=36、複数回答）



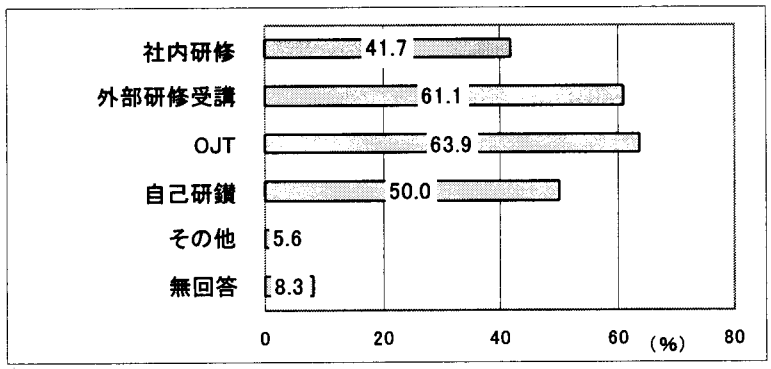
資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

(2)人材教育

セキュリティ分野での技量が少ない人に対して教育を行っていくケースが多いため、従業員教育は外部研修が多くなる。また、ノウハウに依存して業務を行っていくという面があるため、OJT が重視される。アンケートでも「外部研修の受講」と「OJT」が多くなっている（図表 2-36）。また、自己研鑽とする企業も多い。

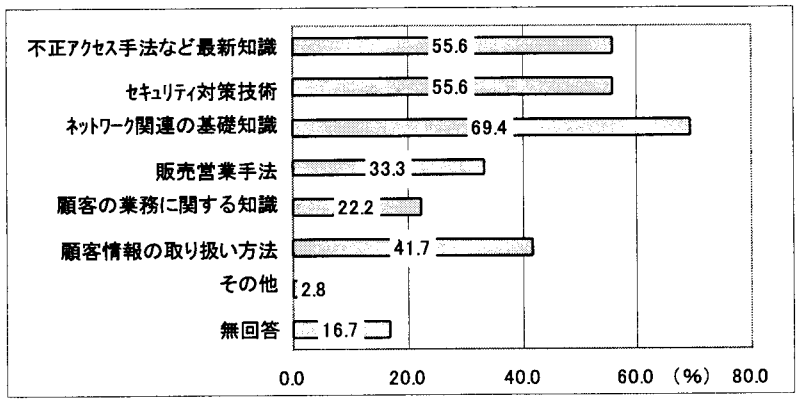
また、従業員教育の内容は、「ﾈｯﾄﾜｰｸ関連の基礎知識」が最も多く、次いで「不正ｱｸｾｽ手法やｾｷｭﾘﾃｨﾎｰﾙ等の最新知識」と「ｾｷｭﾘﾃｨ対策技術」である。このように技術的な内容をあげた企業が多い（図表 2-37）。「顧客情報の取り扱い方法」という社内のセキュリティ体制のための教育内容をあげた企業も 4 割あった。

図表2-36　従業員教育の手法（N=36、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2-37　従業員教育の内容（N=36、複数回答）



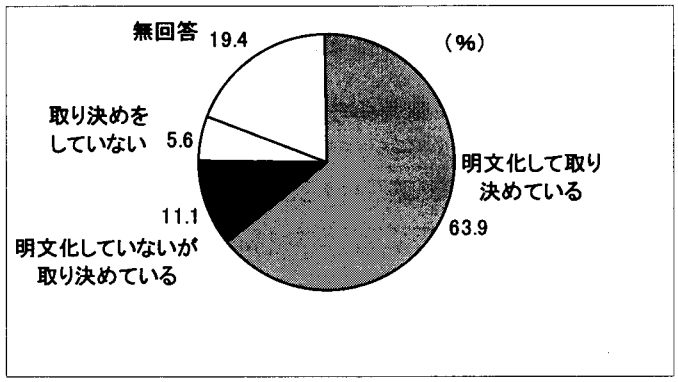
資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

4．顧客情報の漏洩防止

(1)顧客情報の漏洩防止の対策

サービス提供の過程で顧客情報にふれるため、顧客にとって、安全に顧客情報が管理されることは非常に重要なことである。アンケートで顧客情報保護を顧客との間で「明文化して取り決めている」という会社が過半数を占めたように（図表 2-38）、顧客との間では顧客情報保護を契約でうたっているケースが多い。

図表2-38　顧客情報保護を明文化して定めている企業（N=36、複数回答）



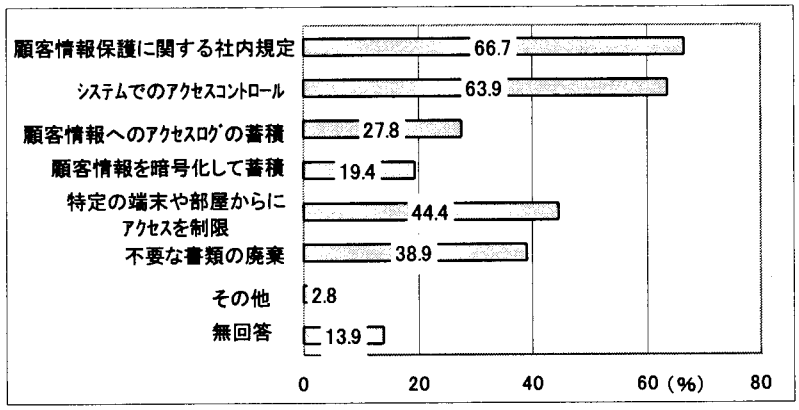
資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

こうした顧客情報保護をうたった契約を結ぶ一方で、顧客情報の漏洩防止に留意することはサイバーセキュリティサービス事業者が顧客の信用を得るために非常に重要なことである。

漏洩防止策としては、人の管理とシステムでの管理の両面があるが、どちらかがより重要ということはなく、多くの場合両面で対策がとられている。アンケートでも、

漏洩防止策として「顧客情報保護に関する社内規定の制定」、「顧客情報を管理しているシステムへのアクセスコントロール」の 2 点をあげた会社が最も多くなっている（図表 2-39）。その他、特定の部屋からのみ顧客情報にアクセスできるといった物理的な防止策やそもそも必要のなくなった書類は全て破棄するといったことも多くの会社で行われている。

図表2-39　顧客情報漏洩の防止策（N=36、複数回答）

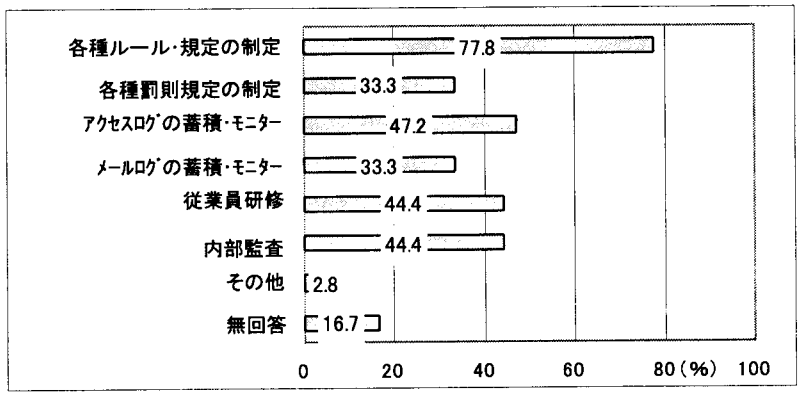


資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

また、従業員からの顧客情報漏洩の防止策に絞ってみると、守秘義務契約を結ぶといったことや、就業規則に守秘義務を盛り込むといった各種社内規定を設けている会社が多い（図表 2-40）。こうした規定は、退職した従業員にも適用されている。（図表 2-41）。離職率を下げるために、就業環境の充実を図っている企業も多い。一方、アクセスログの蓄積及びモニターや内部監査を行うなど不正行為を抑える具体的な防止策をとっている会社も多い。セキュリティチェックなどの業務を 2 名で行いクロスチェックすること（バディシステム）なども多くの会社で行われている。

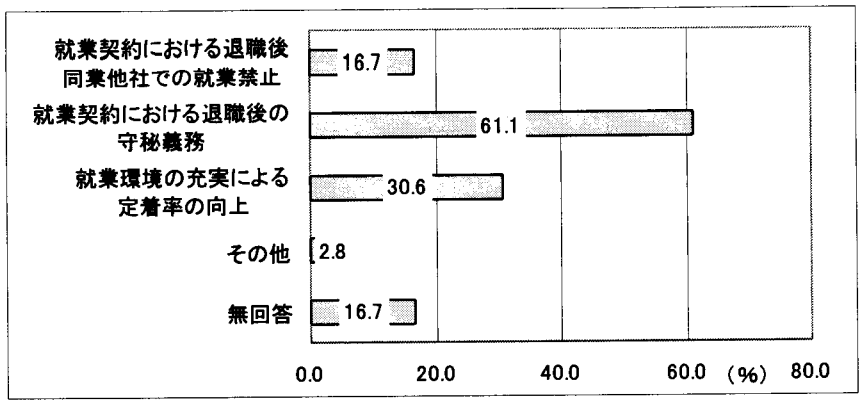
顧客情報管理に関連しては、個人情報保護法案が 2001 年 3 月 27 日に閣議決定され、今国会で審議が予定されている。個人情報保護法では、個人情報の取得や利用などに関する「基本原則」が示されている。特に、体系化された個人情報データベース等を保有する民間企業については、情報の管理等に関する義務を定めている。

図表2-40　従業員からの顧客情報漏洩の防止策（N=36、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2-41　退職した従業員に対する顧客情報漏洩防止策（N=36、複数回答）

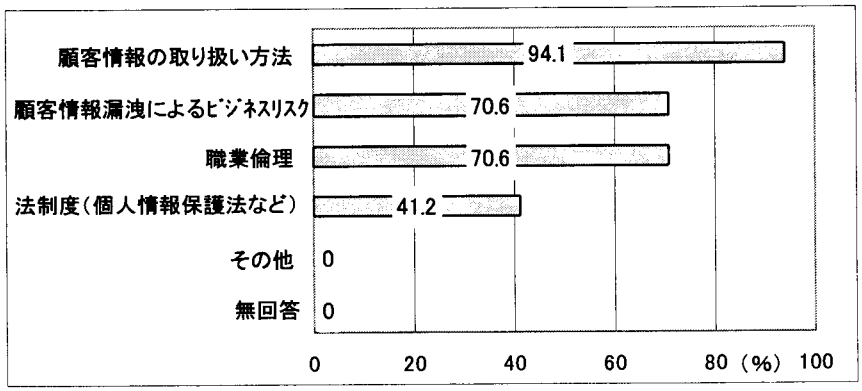


資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

こうして、各社は顧客情報漏洩への対策を講じているが、根本的には従業員のモラルが重要であると指摘する会社が多い。そのため、給与などの処遇を向上させるなど従業員のモチベーションを保つための取り組みが行われている。また、従業員教育にも力が入れられている。アンケートでは、従業員研修を漏洩防止策として全体の4割以上の会社があげており（図表 2-40）、顧客情報の取り扱い方法や顧客情報漏洩によるビジネスリスク、職業倫理などの研修が行われている（図表 2-42）。

顧客情報漏洩に対してはシステム的な防止策を講じたとしても限度があり、最終的には従業員のモラルによるところが大きいため、前述のように人材採用にあたって、その点に非常に留意がされている。

図表2-42　顧客情報保護に関する従業員研修（N=36、複数回答）

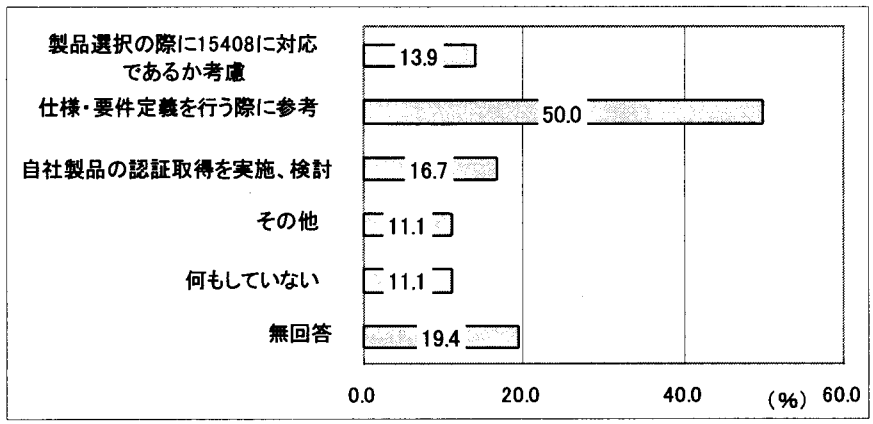


資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

また、顧客の信頼を確保するために、セキュリティ評価基準であるISO/IEC15408といった国際標準に準拠して、セキュリティポリシー策定やセキュアなシステムを設計することも行われている。アンケートでは、何らかの取り組みを行っている企業が

9割近くあり（無回答を除く）、ISO/IEC15408を仕様・要件定義を行う際の参考としている会社が多い（図表2-43）。

図表2-43　ISO/IEC15408への取り組み状況（N=36、複数回答）



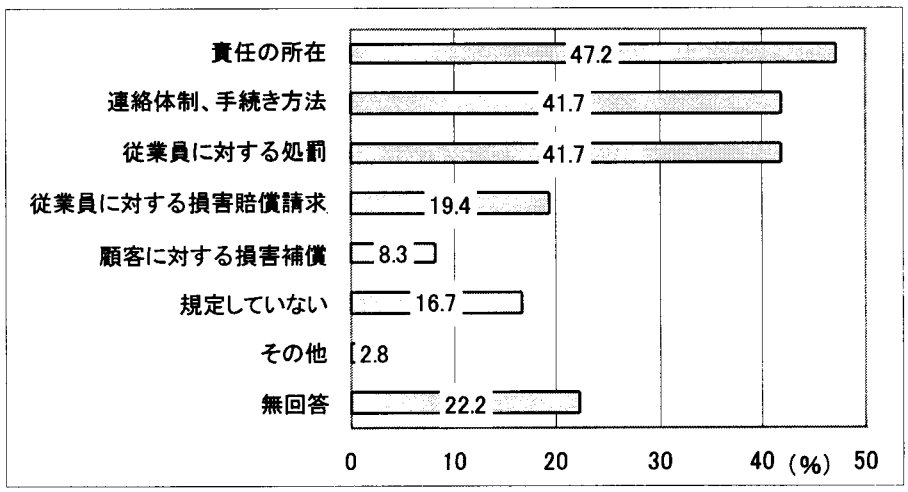
資料：社会安全研究財団「サイバーセキュリティサービスに関する実態調査」(2000.12)

(2)危機管理体制

会社としてのリスクマネジメントという観点から、顧客情報漏洩防止を積極的に行うことによって、何らかの顧客情報漏洩などが発生した場合の説明責任を果たすという側面がある。

アンケートでは、万一情報漏洩があった際の何らかの対処方法を定めている企業は8割（不明を除く）にのぼり、危機管理体制をとっている会社が多い。対処方法では、「責任の所在」が最も多く、次いで「従業員に対する処罰」である（図表2-44）。

図表2-44　情報漏洩の際の対処方法（N=36、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)

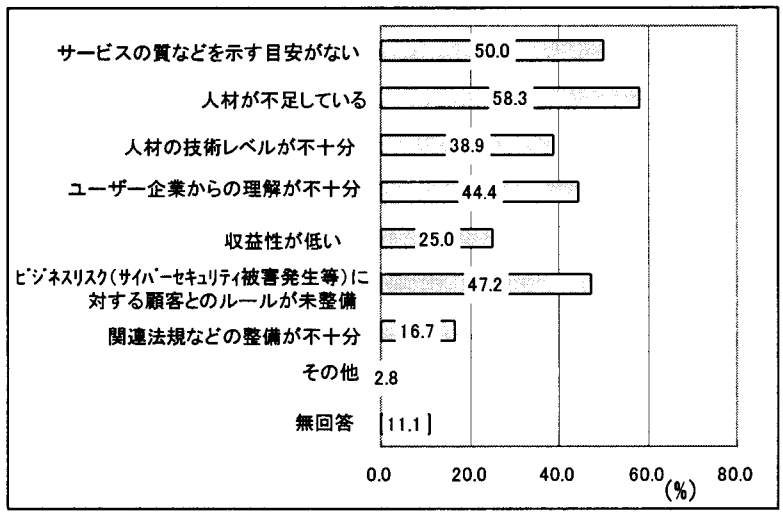
５．サイバーセキュリティサービス事業者の課題

サイバーセキュリティサービスの多くが、1998 年以降から開始されていることからも分かるように、サイバーセキュリティサービスは、近年、注目されるようになったサービスである。そのため、セキュリティ技術者が少なく、人材が不足している（図表 2-45）。また、顧客企業との契約が不十分なために、不正アクセスなどによる被害が発生した際のビジネスリスクが不透明であることが課題として挙げられている。

サービスという事業の特徴として、不正アクセスなどが実際に起きない限りサービス内容がユーザーにとって分かりにくいこと、また、ユーザー企業にセキュリティを理解する人材が少ないこともあり、サービスの質を示す目安がない。そのため、サービスの質の低下を懸念する声もある。

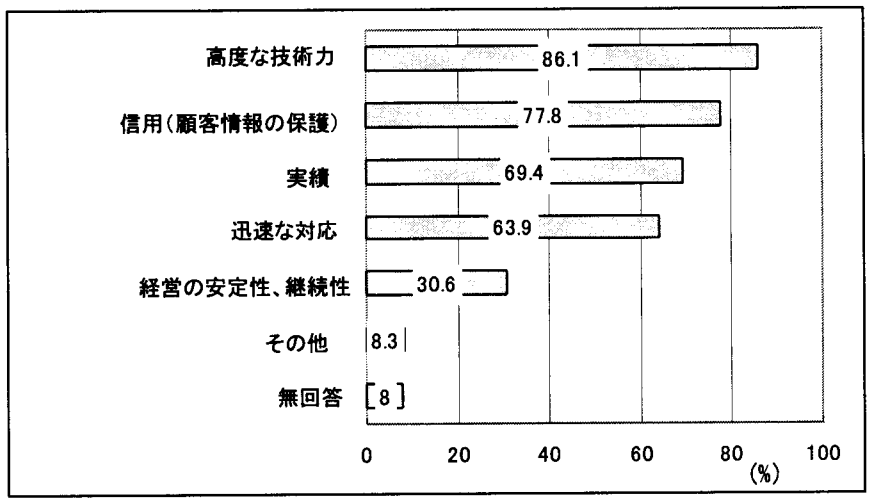
さらに、顧客企業もセキュリティに対する意識や理解がまだ十分ではなく、市場の立ち上げを各事業者が積極的に行っている状況である。そうしたなか、顧客企業からは、高度な技術力や顧客情報管理における信用、実績、迅速な対応などが求められている。

図表2-45　サイバーセキュリティサービスの事業環境の問題点（N=36、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2-46　サービス事業者に顧客から求められること（N=36、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)