第３章　ユーザ企業におけるサイバーセキュリティへの取り組みの現状

ここでは、主に今回実施したアンケート調査並びにユーザ企業へのインタビューをもとに、ユーザ企業におけるサイバーセキュリティへの取り組みについてまとめる。

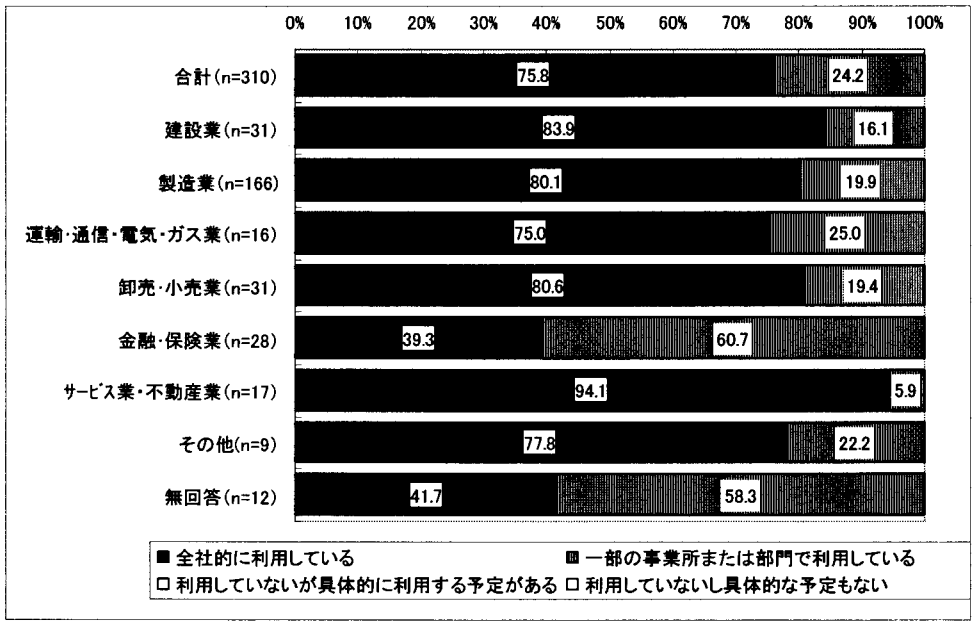
１．ネットワークの利用状況

(1)インターネット

現在、ユーザ企業の全てがインターネットの利用を行っており、その内の 3/4 は全社的な利用となっている。業種別には、金融・保険業においてインターネットを「一部の事業所または部門で利用している」割合が高いことが特徴である。

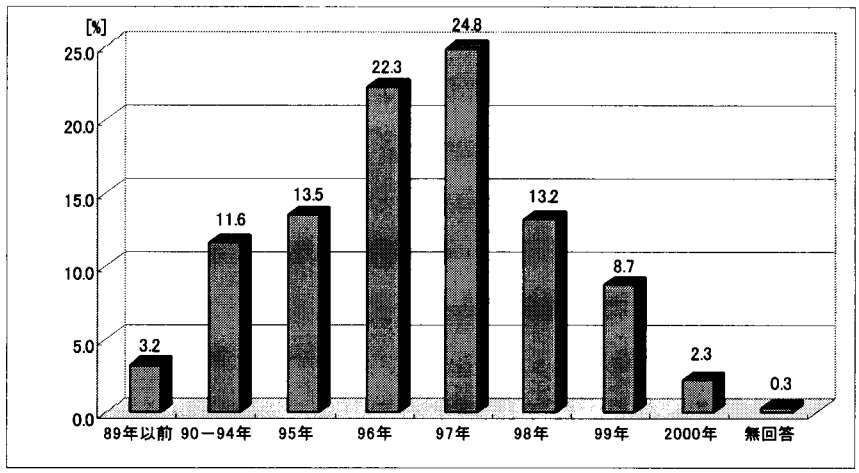
ユーザ企業のインターネットの利用は 1996 年、1997 年に急速に進んでいる。1995 年までにインターネットを利用し始めた企業は 28.3%であったのに対し、1997 年時点では 75.4%の企業が利用を行っており、1997 年頃から企業におけるインターネット利用は特別なことではなくなっている状況が伺える。

図表3-1　インターネットの利用状況（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）

図表3-2　インターネット利用開始時期（N=310）

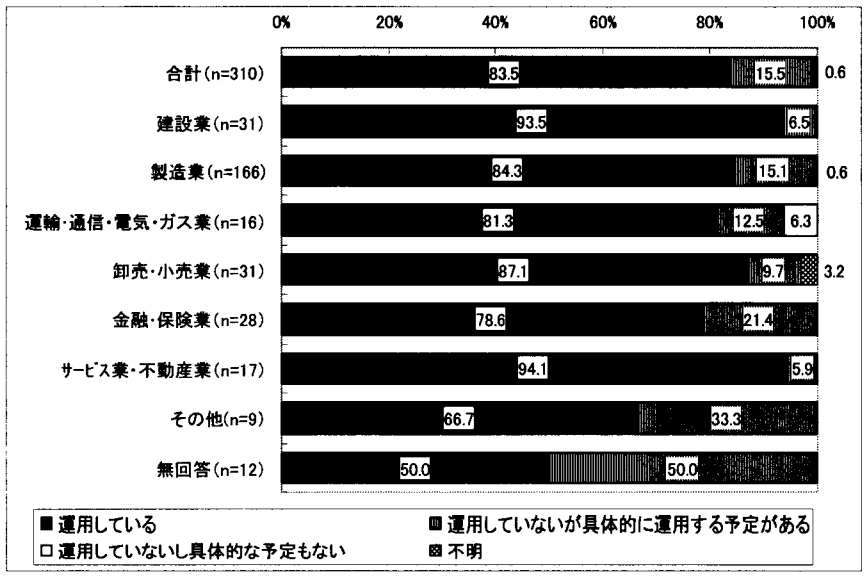


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

ユーザ企業の 83.5%は公開用 Web サーバを運用している。検討中の企業を含めると、今後、ほぼ全ての企業が公開用 Web サーバを運用する状況になる。業種別には、運輸・通信・電気・ガス業の一部に公開用 Web サーバを運用する計画をしていない企業があることが特徴となっている。

近年企業における Web の活用方法は、企業 PR に加えて、IR 情報の開示や電子商取引や電子調達などへと高度になってきている。これに伴い、万一不正アクセスなどの被害を受けた場合に生じる損害が多大なものになる恐れがある。企業におけるネットワーク利用の拡大に伴い、サイバーセキュリティへの取り組みの必要性が高まってきている。

図表3-3　公開用Webサーバの運用状況（N=310）



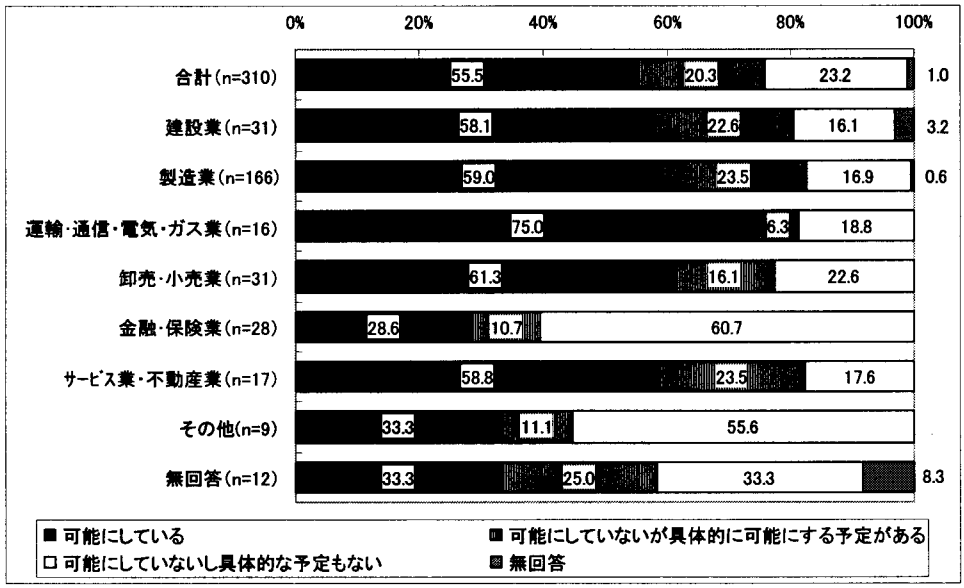
資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

(2)リモートアクセス

イントラネットなどの普及に伴い、外出先などからも社内システムを利用できることへのニーズが高まっている。これに伴い、リモートアクセスの環境を整える企業は増えており、現在、55.5%の企業がリモートアクセスを実現している。現在、具体的な予定を持っている企業が20.3%あることから、今後もリモートアクセス環境を整える企業は増え、75.8%の企業で利用される状況になる。業種別には金融・保険業での取り組みが比較的少ないことが特徴である。

リモートアクセスは、出先からでも社内ネットワークと同一の環境が利用可能となり、製品情報や在庫情報をその場で確認することや、営業情報等を入手することが可能になるなど企業の生産性向上に寄与する。その反面、認証システム等が介在するとはいえ、公衆回線から社内システムへのアクセスルートができることから、セキュリティ上の脆弱点となり得る危険性を持つ。そのため十分なサイバーセキュリティ対策が必要になる。

図表3-4　社内システムへのリモートアクセスの利用状況



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）

2．サイバーセキュリティへの対応状況

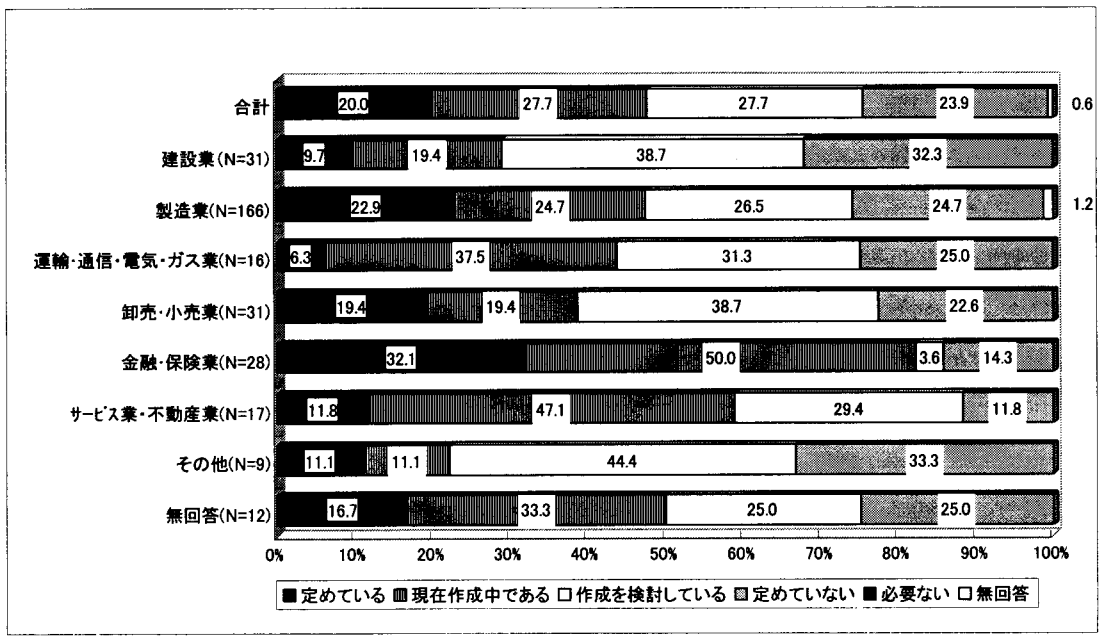
(1)セキュリティポリシー

情報セキュリティ対策の指針や基準を明文化したセキュリティポリシーを策定することの重要性が指摘されるようになっている。セキュリティポリシーとは、金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準」によると「会社（もしくは組織）の情報資産を適切に保護するための会社としての安全対策に関する統一方針」とされている。組織として守るべき情報資産や、守るべき理由、責任の所在等を明文化し、組織全体の情報セキュリティ対策の考え方を体系化するものである。セキュリティポリシーの策定により、組織全体としての総合的な情報セキュリティ対策の実現や、組織内での情報セキュリティの重要性に関する認識向上に繋がるといった効果があることが指摘されている。

企業におけるセキュリティポリシーへの取り組み状況をみると 20.0%の企業が既に策定している。現在策定中の企業を加えると、今後、約半数の企業がセキュリティポリシーを策定する状況となる。

業種別には、特に金融・保険業の取り組みが進んでいる。金融監督庁の金融検査マニュアルのチェックポイントにセキュリティポリシーの策定が挙げられているといった要因もあり、32.1%の企業がセキュリティポリシーの策定を行っている。さらに 50.0%の企業が現在作成中である。

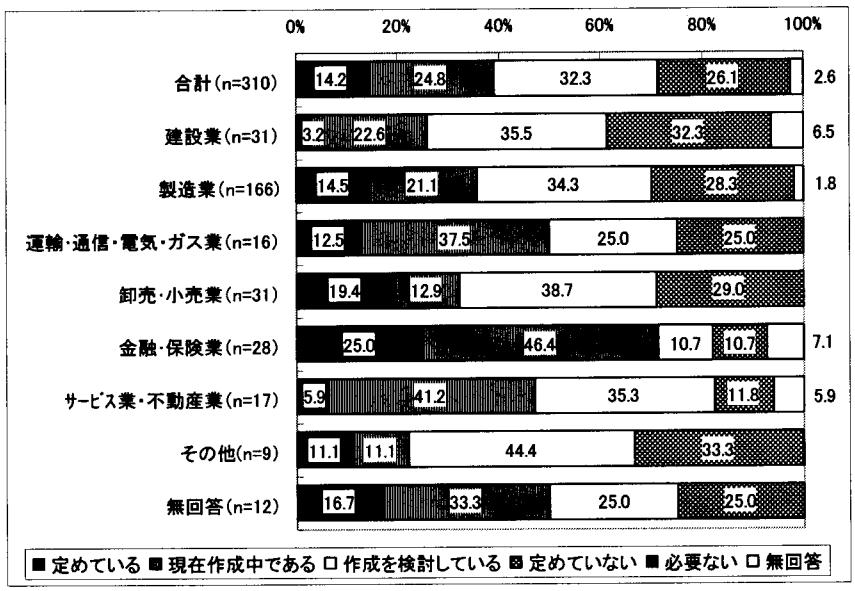
図表3-5　経営理念に基づいたセキュリティポリシーの策定状況（N=310）



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）

セキュリティポリシーに基づき、具体的な操作や業務処理手順を規定するセキュリティガイドラインの策定は14.2%の企業が取り組んでいる。セキュリティポリシーの策定状況と比較すると、まだ少ない状況にある。業種別には金融・保険業の取り組みが進んでいる。

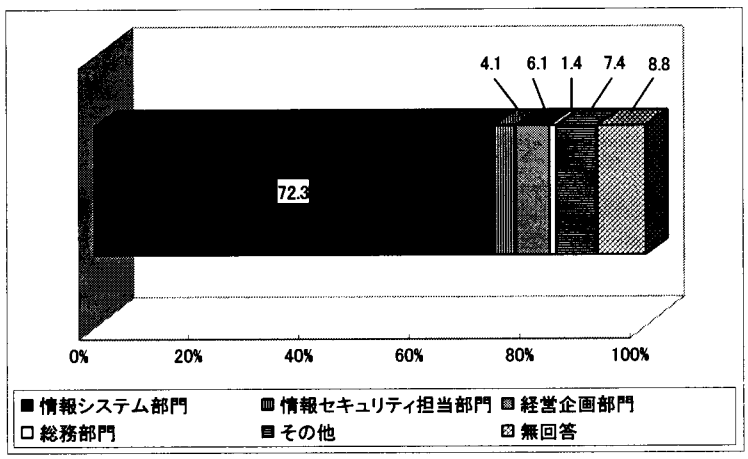
図表3-6　セキュリティガイドラインの策定状況



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）
（注）セキュリティガイドライン：セキュリティポリシーに基づき、具体的な操作や業務処理手順などを定めたものとした

必要セキュリティポリシーの策定は情報システム部門が主導して進められているケースが多い。経営企画部門が主導して策定したケースは6.1%である。

図表3-7　セキュリティポリシー策定の中心部署（N=148）

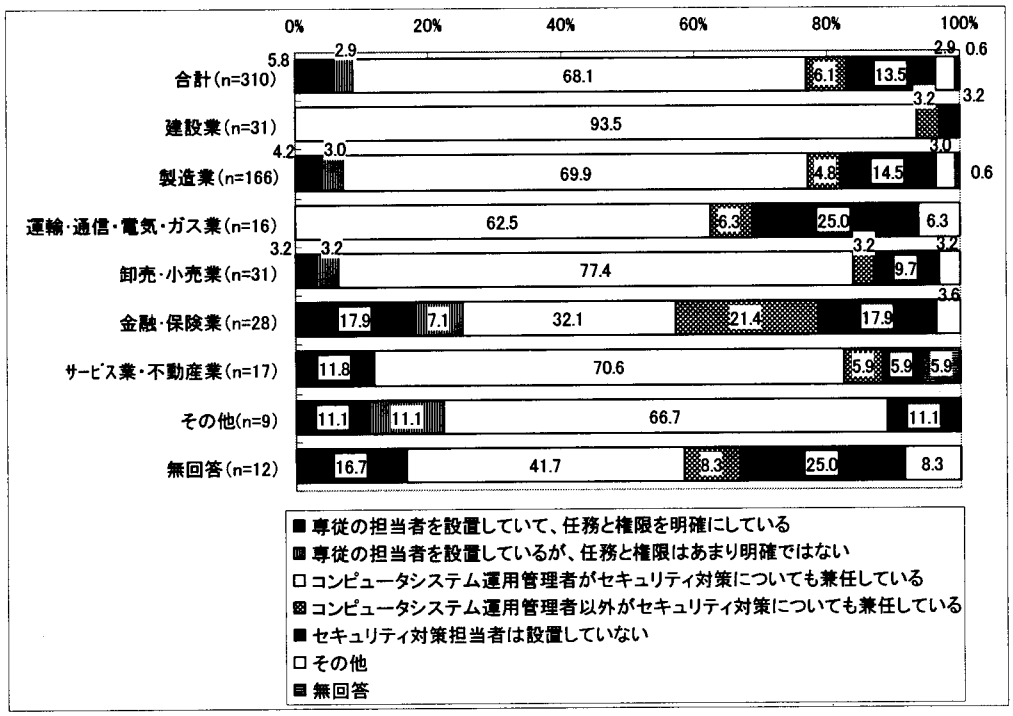


資料：社会安全研究財団「サイバーセキュリティの取り組みに関する調査」（2000.12）

(2)セキュリティ管理体制

企業におけるセキュリティ担当者は、大半の企業ではコンピュータシステム運用管理者が兼任して担当している。専従のセキュリティ担当者を設置している企業は8.7%にとどまる。一方でセキュリティ担当者を設置していない企業も 13.5%あるなど、体制面でのばらつきがみられる。業種別にみると金融・保険業では 25.0%の企業が専従担当者を設置している。

図表3-8　セキュリティ対策担当者の設置状況



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）

不正アクセスに使われる技術やツールが進歩していく中で、サイバーセキュリティ対策には専門的な技術や知識が要求されるようになってきている。今後は、コンピュータシステムの運用管理と兼任してセキュリティ対策を行う体制では、十分な情報収集や対策を施していくことが難しくなっていくことが考えられる。

3．サイバーセキュリティ対策への取り組み状況

(1)コンピュータウィルス対策

近年、マクロウィルスやメール悪用ウィルスといった、広範な感染力をもつコンピュータウィルスが増えたことなどから、情報処理振興事業協会（IPA）に届けられたコンピュータウィルスの発見件数は大幅に増加している。特に、2000 年 5 月に広