ソリューション・レポート

セキュリティポリシーに関するコンサルティング・サービスの紹介

EST コンサルティング本部　EST コンサルティング部　**西川征一**

１．はじめに　～セキュリティポリシーの必要性～

近年、インターネットを活用したビジネスが急速に進展しており、セキュリティ関連の市場も拡大しつつある。しかし、日本ではセキュリティ対策というと、ウィルス対策、ファイアウォール構築、暗号化などの技術面への関心は高いが、セキュリティに関する組織や人に係わる運用管理面への関心はうすく、後回しにされている感がある。個人情報の漏洩や内部からの企業情報の流出などは、それを扱う人間の意識やモラルが未成熟であるために、起こるべくして起きた事件といえる。また、2000年の１月下旬から２月上旬に起きた日本の政府関連機関のホームページ改ざん事件や、同じ頃に米国で発生した、ヤフーを始めとする大手サイトをサービス不能にいたらしめた攻撃事件などは、セキュリティ対策をどこまでやれば安全かを見極めることの難しさを示している。別な見方をすれば、システムのどこに脆弱性が潜んでいるかが十分に認識されておらず、その脆弱性に対して効果的な対策が講じられていないことを示している。技術面だけでなく、運用管理面での対策が必要であり、そのためには以下のような点を徹底的に分析／検討すること（リスク分析）が第一歩となる。

・何が重要で、何を守りたいのか
・社内外を含めて、どのような脅威が存在するか
・誰が行う、どのような行為から守りたいのか
・現在の弱点（脆弱性）は何か、どこが最も危ないか
・セキュリティ対策費用はどの程度必要か
・どのような優先順位で対策を施すのか

この分析の結果を受けて、セキュリティを高め、維持管理するための基本的な考え方や技術面、設備面、運用管理面について具体的な対策を明文化したものが「セキュリティポリシー」である。しかし、現実的には経営理念に基づいてセキュリティポリシーを策定している事業体は非常に少なく、２割に満たない状況である（第９章「参考情報」を参照）。

２．セキュリティ評価基準の国際標準化の動向

これまで、日本における情報システムのセキュリティ対策は、企業やシステム・インテグレータの独自の判断で行われてきた。一方、欧米企業では政府機関をはじめとして、情報システムやコンピュータ関連製品を導入する際にセキュリティ機能を評価／認証する制度を持ち、運用されてきた歴史がある。日本情報処理開発協会（JIPDEC）が平成11年度に実施した「情報セキュリティに関する調査」によると、日本の場合は「セキュリティ対策を講じている企業が何に準拠して策定したか」という質問に対して76.2%が「独自の対策」による、と回答している（第９章「参考情報」を参照）。

アメリカでは1985年に、軍事システム向けに調達する製品のセキュリティ基準としてトラステッド・コンピュータ・システム評価基準（TCSEC）を策定し、国防省のナショナル・コンピュータ・センター（NCSC）による検定が行われている。この TCSEC が欧州各国に影響を与え、1991年にイギリス、フランス、ドイツ、オランダの４カ国によって情報技術セキュリティ評価基準（ITSEC）が制定された。さらに、1993年にはカナダでカナディアン・トラステッド・コンピュータ製品評価基準（CTCPEC）が制定された。

しかし、これらの評価基準は評価対象や運用方法が各国

で異なっていたため、これらを統一し、評価結果を互いに利用するためにコモン・クライテリア・エディトリアル・ボード（CCEB）を発足し、1996年にセキュリティ評価基準としてCommon Criteria第1版が発表された。その後1998年に第2版が出され、暗号やプライバシーに関する要件が追加された。

一方、国際標準化機構（ISO）でも1991年からセキュリティ評価基準の検討を始めていたが、CCEBと協力し合うことに決め、1998年にCommon Criteria第2版に基づくセキュリティ評価基準をドラフト標準として制定し、1999年12月にISO／IEC15408として発行した。

このように欧米では、国際標準のセキュリティ評価基準による認証が、政府機関や民間企業の取引において入札条件になる傾向にあるのに対して、日本ではやっと2000年にISO／IEC15408のJIS化がなされた状況であり、このままでは国際的な競争力に影響を及ぼす可能性が大きい。

3．セキュリティポリシーの役割と定義

では、セキュリティ対策を効果的に施すためのセキュリティポリシーは、どのような役割を持ち、どのように定義されているだろうか。いくつかの事例から、セキュリティポリシーの役割と定義を整理してみる。

⑴ セキュリティポリシーの役割

実効性のあるセキュリティポリシーには、以下の2つの役割がある。

・経営者からの宣言
・遵守すべき具体的な規定の提示

セキュリティポリシーは、企業や組織の情報資産を守ることを主たる目的とするため、ある程度の強制力を持って発効される必要があり、罰則などが盛り込まれることになる。罰則を含む規定を社員に受け入れてもらうためには、その規定の目的や重要性を十分に説明し、理解を得ることが必要である。そのためには、企業の情報資産を守るための「経営者からの宣言」として、トップ自らがセキュリティポリシーを社員へ伝えるべきであり、また遵守すべき規定を具体的に示すことである。

⑵ セキュリティポリシーの定義

日本の法人の中でも、㈶金融情報システムセンター（FISC）では、特に積極的にセキュリティ対策に取り組んでいる。FISCは、「セキュリティポリシーとは、会社（もしくは組織）の情報資産（情報および情報システム）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であり、そこでは、保護する必要がある情報資産は何か、それらをなぜ保護するのか、それらについての責任はどのようになっているか等を明確にすること」と定義している。

また、情報資産の保護をするための要素を、一般的にCIAという略語で表す。“C”は機密性（Confidentiality）、“I”は完全性（Integrity）、“A”は可用性（Availability）を意味する。「情報資産が適切に保護されている状態」とは、「CIAを維持すること」である。CIAを以下に簡単に解説する。

・機密性(C)：正しい権限を持った者に対して、定められた条件下でのみ情報資産へのアクセスを許す。
・完全性(I)：情報資産の正当性、正確性、網羅性、安全性を維持する。
・可用性(A)：正しい権限を持った者に対し、必要時に情報資産へのアクセスを可能な状態を維持する。

4．セキュリティポリシーの構造

セキュリティポリシーの構成には、いくつかのパターンがあるが、ここでは当社のビジネスパートナーである株式会社アズジェント(以降、アズジェント社と称す)のセキュリティポリシーの構成概念を紹介する。

アズジェント社のセキュリティポリシーは3階層構成になっており、階層の上位から「エグゼクティブレベルポリシー」、「コーポレートレベルポリシー」、「プロダクトレベルポリシー」が位置付けられている。各階層（レベル）の呼称はFISCやJISAのガイドラインとは異なるが、構造は同様である。アズジェント社では、セキュリティポリシーのさらに上位に、IR（Investor Relationship）的な意味合いを含めた宣言書（ステートメント）を置いている。

アズジェント社のセキュリティポリシーの階層イメージを図1に示し、参考としてFISCとJISAの呼称を併記する。

各階層（レベル）について、以下に解説する。

・ステートメント（宣言書）
　エグゼクティブレベルポリシーを概略化したもので、企業のセキュリティに対する姿勢を示し、社外に開示することを目的とする。
・エグゼクティブレベルポリシー
　企業理念等を踏まえて、セキュリティに関する企業方針を、経営者の観点から記述する。特定の製品、システム、技術に依存しない汎用的／抽象的な表現になる。
・コーポレートレベルポリシー
　エグゼクティブレベルポリシーを達成するために、何を行い、何を守るべきかを記述する。手順、方法ではなく、運用規定レベルの表現になる。
・プロダクトレベルポリシー
　上位レベルのポリシーを受けて、どのようにセキュリティ対策を講じるかを記述する。どのような製品を導入して運用／管理するかを、具体的な手順／方法として示す。

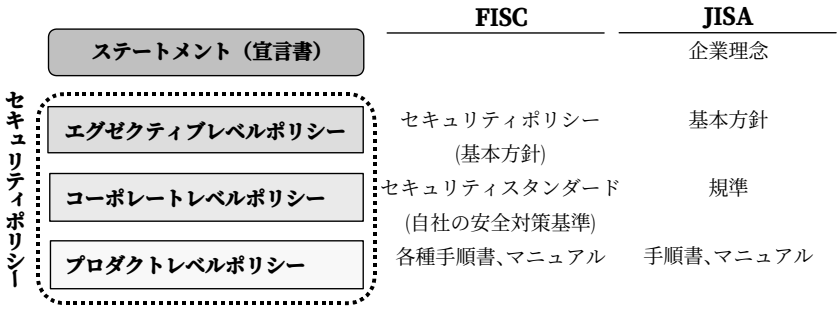

図１　セキュリティポリシーの階層構造（アズジェント社）

また、ホームページ改ざん事件後、政府も情報セキュリティ対策推進会議を設置して、2000年７月に「情報セキュリティポリシーに関するガイドライン」を策定しており、そこでは全体の構成は図２のような構成になっている。

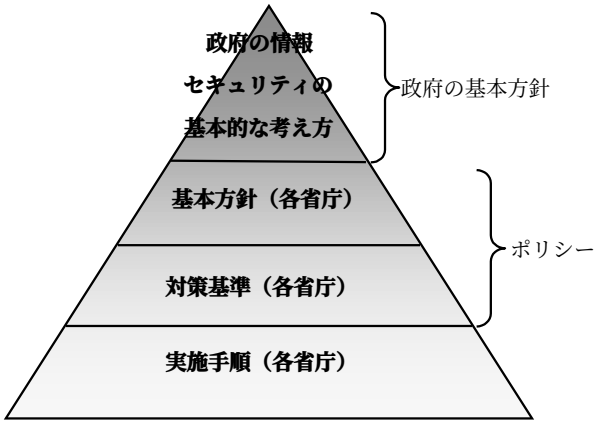

図２　「情報セキュリティポリシーに関するガイドライン」の構成

５．セキュリティポリシーの策定手順

アズジェント社に限らず、民間企業におけるセキュリティポリシー策定手順は企業機密に近いノウハウであり、この場で公開するのは問題がある。そこで、ここでは政府、およびJISAのガイドラインが示す策定手順を紹介する。

いずれの手順においても、ポリシーそのものの策定も重要だが、それに先立ってリスク分析を行うことが最も重要であるとしている。「何が重要で、何を守りたいのか」、「どのような脅威が存在するのか」、「現在の弱点は何か」などを十分に分析してから、ポリシーを策定することが肝要である。政府の「情報セキュリティポリシーに関するガイドライン」における策定手順、および「JISAの策定手順の標準」を図３、図４にそれぞれ示す。

また、セキュリティポリシーは一度策定すればよいというものでない。定期的に見直して、新たな脅威が発生していないか、環境の変化はないかを確認しながら、継続的な

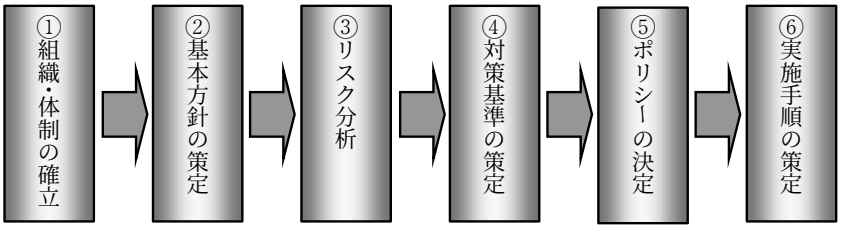

図３　「情報セキュリティポリシーに関するガイドライン」における策定手順

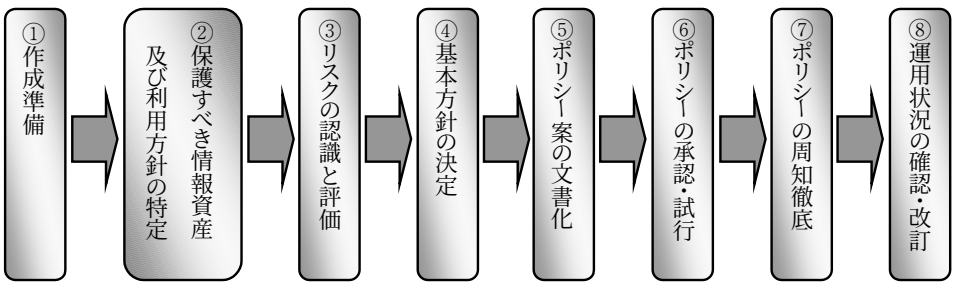

図４　JISAの策定手順（標準）

セキュリティ対策を講じていくことが必要である。政府の「情報セキュリティポリシーに関するガイドライン」におけるセキュリティポリシーの実施サイクルを図５に示す。

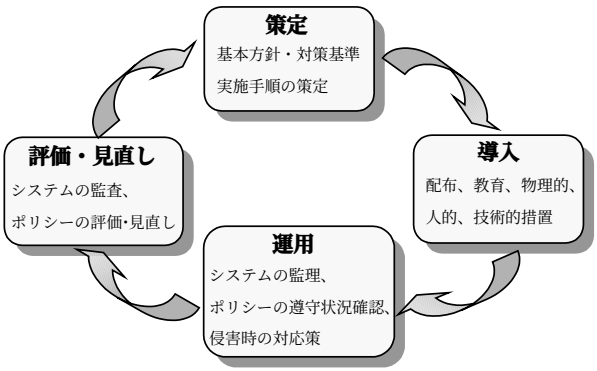

図５　セキュリティポリシーの実施サイクル

６．セキュリティポリシーの事例

2000年にアズジェント社と協働で策定／実施した、セキュリティポリシーの事例を紹介する。機密保持上、実際の全容は公開できないが、「情報セキュリティ基本方針(例)」として、ポリシーとして盛り込むべき主要な項目を資料１に紹介する。

７．情報セキュリティに関する国際標準／ガイドライン

企業にとって、情報セキュリティを確保して適切に維持することは非常に重要であり、義務でもある。グローバルにビジネス展開している企業であれば、国際的に通用する

資料１　情報セキュリティ基本方針（例）

情報セキュリティ基本方針（例）

はじめに

情報セキュリティ対策の目的は、XX 株式会社が所有、または管理する電子媒体上の情報資産を盗難、改ざん、破壊、漏洩等の不正行為から防ぎ、企業の損失を最小化することである。

この基本方針では電子情報のみでなく、電子情報を管理するためのシステム、それらが適切に機能し、正しく利用され、復旧または保護するために必要な仕組みや取り決めまでを「情報資産」と定義する。

目的

この基本方針は、XX 株式会社の意思決定、業務継続、コスト削減、管理効率の向上のため、情報資産に対して管理や保護を安全に行うことを目的としている。このためには、情報資産のオーナー、利用者やその開発者および管理者が、情報資産の開発、管理、利用、共有を安全に行うことが必要である。

この基本方針は XX 株式会社の情報セキュリティ対策へ取り組む体制や責任を明確にすることにより、意志統一されたセキュリティ対策を適切に実装できることを目的とする。セキュリティ対策を適切かつ円滑に実施するための対策基準や手順書は、この基本方針に基づいて策定する。

適用範囲

この基本方針は、XX 株式会社が所有、または管理するすべての情報資産および情報資産のすべての利用者（役員、従業員および派遣社員）に適用する。外部委託業者への方針の適用については別途記載する。利用者とは･･･････

体制

情報セキュリティの統括責任者として、最高情報セキュリティ責任者と情報セキュリティ委員会を設置する。･･･････

役割

最高情報セキュリティ責任者、情報セキュリティ委員会などの役割を定義。

情報資産の分類と管理に関する責任

情報システムと外部ネットワークの保護に関する責任

利用に関する責任

基本要件

情報資産の分類、リスク管理、識別・認証、アクセス制御、監視・記録（説明責任)、緊急時対応計画、個人情報の保護などの基本要件を記述。

セキュリティ基本方針の遵守と継続的な運営

この基本方針の外部委託業者への適用

セキュリティポリシーの保持は必須であり、取引条件の１つになることが多い。国際的な情報セキュリティに関する標準として、以下に紹介するISO／IEC15408とISO／IEC17799（BS7799）がある。

⑴ ITセキュリティ評価基準：ISO／IEC15408

ISO／IEC15408は、情報処理関連の製品やシステムのセキュリティレベルを評価するための国際標準であり、1999年12月に発行された。この標準は、セキュリティ機能をもったハードウェア、ソフトウェア製品、それを包含するシステムの全てを対象とし、必要なセキュリティ対策が装備されているかどうかを確認する基準である（本論のテーマであるセキュリティポリシーが対象とする範囲とは異なる）。

ISO／IEC15408は、次の３つのパートから構成される。

①パート１：セキュリティ評価の概要と一般モデル
- セキュリティ評価のためのアプローチ
- セキュリティ基本設計書（Security Target：ST）の仕様
- セキュリティ要求仕様書（Protection Profile：PP）の仕様

②パート２：セキュリティ機能要件
- セキュリティ機能に関する要件を11のクラスに分類

③パート３：セキュリティ保証要件
- セキュリティ保証に関する要件を10のクラスに分類
- ７段階の評価保証レベル（EAL１～７）を規定

EAL（Evaluation Assurance Level：評価保証レベル）は、一般の商用製品ではレベル３～４、特殊な用途に用いられる製品やシステムでは、それ以上のレベルが求められる。

⑵ 情報セキュリティ管理基準：ISO／IEC17799（BS7799）

ISO／IEC17799は、英国規格協会の情報セキュリティ・マネジメント基準BS7799のパート１を2000年９月にISO標準としたものである。

この基準は、ISO／IEC15408のように特定の製品やシステムを対象にするのではなく、企業や組織における情報システム全般を対象とする。セキュリティポリシーから始まり、組織、インフラ、物理的なセキュリティ、人の管理、アクセス制御、システム開発、事業継続管理など広範囲にわたる項目が規定されている。ISO／IEC15408が設計／開発段階でのセキュリティ確保を主な目的にしているのに対し、ISO／IEC17799は情報システムの運用管理においてのセキュリティ確保を主な目的とする。

ISO／IEC17799とISO／IEC15408の位置付を図６に示す。

ISO／IEC17799は、以下のような２部構成になっている。「第１部：情報セキュリティ管理実施基準」はBS7799そのものであり、あらゆる業種や規模の組織において、共通して適用可能な情報セキュリティの管理方法がまとめられている。「第２部：情報セキュリティ管理システム仕様」は

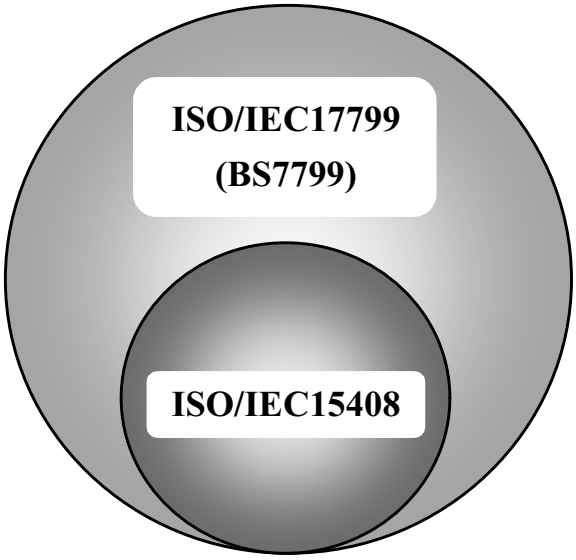

図６　ISO／IEC17799とISO／IEC15408の位置付

第１部の補完的な内容であり、情報セキュリティ管理システム（ISMS：Information Security Management System）として、実施基準（BS7799）を実装するための必要事項が仕様形式でまとめられている。

ISO／IEC17799の実装ステップを図７に示す。

⑶ 国際標準への日本の対応

ITセキュリティ評価基準「ISO／IEC15408」は、2000年７月にJIS規格化され、JIS X5070となっている。政府は、この基準に基づいて政府が利用するIT関連製品のセキュリティ機能／品質をチェックする「情報セキュリティ評価／認証体制」を整備しており、2001年４月から経済産業省を皮切りに運用を開始した。順次、各省庁へ拡大され

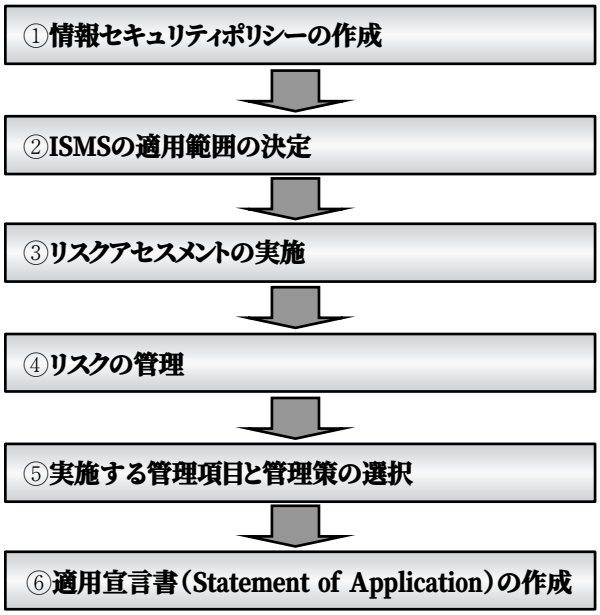

図７　ISO／IEC17799の実装ステップ

ると予想する。

情報セキュリティ管理基準「ISO／IEC17799」は、まだJIS規格化されていないが、2001年内の規格化を目指して準備を進めている。さらに、この標準を踏まえて、第三者適合性評価制度「ISMS（Information Security Management System）制度[*1]」がJIPDECを中心に策定されている。ISMS制度の導入により、昭和56年に開始された「情報サービス業情報システム安全対策実施事業所認定制度（安対制度）」は廃止されることになる。

8．おわりに～当社のセキュリティ・ビジネスへの取り組み～

コンサルティングからシステム・インテグレーション、システム運用まで一貫した情報サービスを提供する「One Stop Service Provider」として、当社も情報セキュリティに対して積極的に取り組んでいる。セキュアな情報システム、およびサービスを顧客へ提供することは、当社の使命であり、万全の体制で継続的に取り組むことが必要である。現在（2001年４月）の対応体制は以下としている。

- 品質保証部：国際標準やガイドラインなどの調査と社内普及
- EST コンサルティング部：セキュリティポリシー策定のためのコンサルティング
- 応用技術研究室：セキュリティ実装技術／ツールの調査／研究
- SI／SO 事業部門：セキュリティ対策の実装と運用管理

しかし、今後のネットビジネス（システム）の拡大に伴って、セキュリティ対応の強化がますます要求されると予想する。ビジネスの進展に対応した強化と拡充が必要となるだろう。

9．参考情報～日本のセキュリティ対策の現状

JIPDECの平成11年度「情報セキュリティに関する調査」は、1999年10月～12月に実施された。記名式のアンケートによって、日本の企業、および事業体における情報セキュリティの現状と意識、さらに今後の計画を調査した。アンケートの発送総数は4,714件で、回収したのは867件（回収率18.4%）であった。セキュリティに関する調査結果の一部を、以下に参考情報として紹介する。

(1) 経済産業省の安全対策施策について

経済産業省（旧通商産業省）の提唱する安全対策に関する諸施策についての認知度は、「利用している」と答えた企業は15%にも達せず、「知っている」がやっと50%前後であった。

本設問の回答結果を表１に示す。

また、コンピュータウィルス、およびコンピュータ不正アクセス被害の届出機関として指定されている情報処理振興事業協会（IPA）を、約30%の企業が「知らない」と回答している。さらに、コンピュータ緊急対応センター（JPCERT／CC）については60%が、個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q15001規格）にいたっては、83%の企業が「知らない」と回答している。

この調査結果から判断すると、実態として“国の安全対策施策（基準）が各企業、および事業体で十分には利用されていない”のが現状といえる。

(2) セキュリティ管理一般について

企業のセキュリティ対策について、全般的には積極的な取り組みがされているとは言い難い。ただし、これは業種によって差があるようだ。例えば、セキュリティポリシー制定の実施率は、情報処理サービスが37.1%と高く、金融／保険業では24.2%、公共サービス業では21%となっている。また、セキュリティ・ガイドラインとして操作、および業務処理手順書を定めている業種は、金融／保険業が47.3%、情報サービスが41.6%である。しかし、それでも

表１　経済産業省の安全対策の諸施策についての認知度

施　策	利用している	知っている	合計
情報システム安全対策基準	14.1%	49.5%	63.6%
コンピュータウイルス対策基準	12.0%	54.3%	66.3%
コンピュータ不正アクセス対策基準	10.0%	51.6%	61.6%
システム監査基準	10.6%	56.3%	66.9%
システム監査企業台帳制度	1.6%	35.8%	37.4%

＊１）ISO／IEC17799、およびISMS制度の詳細については、品質保証部発行の「ISO／IEC17799調査レポート（2000年１～３月）」を参照されたい。

50%未満であり、まだまだ低い値といえる。

本設問への回答結果を表２に示す。

なお、⑦の質問の派生として、「セキュリティ対策を講じている（YES）場合、何に準拠して定めているか」という問いに対しては、「独自の対策をしている」という回答が76.2%と圧倒的に多く、「システム展開先の国の法規制を基準にして」は7.1%であった。

情報セキュリティ管理についての問題点への問い（複数回答）には、以下の回答が上位に挙がっている。

・組織の従業員に対する教育・訓練がいきとどかない（48.6%）
・コストがかかりすぎる（47.9%）
・どこまでやればよいのか基準が示されていない（47.2%）
・対策を構築するノウハウが不足している（44.8%）

なお、「トップの理解が得られない」との回答は9.3%であったが、前回(1997年)の調査では5.8%であり、トップの認識がまだこのあたりに止まっていることがうかがえる。

⑶ 不正アクセス対策について

2000年２月に施行された「不正アクセス行為の禁止等に関する法律を知っている」と答えたのは約半数の50%に止まっている。また、「不正アクセスの被害にあった（1998年１～12月期間中)」との回答は6.1%であり、不正アクセスが実際の脅威としての実感がないのが現状のようだ。不正アクセス対策としては「管理責任者の設置」、「入室管理」、「カード／パスワードの利用」が、各企業で実施されている。しかし、リモートアクセスを行っている企業の比率は50%であり、情報処理サービス業では70%を超えている。以下のような実態を考察すると、かなり脆弱な現状であり、不正アクセス対策についての問題点は、情報セキュリティの場合とほぼ同様であるといえる。

・情報についての機密度のランクを設定しているか（YES：26.5%）
・パスワードは定期的に変更しているか(YES：17.8%)
・暗号を採用しているか（YES：4.7%）
・不正アクセス対策について従業員に教育や訓練の場を設けているか（YES：18.5%）

⑷ 情報リスクマネージメント関連について

情報セキュリティ確保のための重要な視点は何か、という質問(複数回答)については、「社内全体の理解(74.9%)」、「経営者の理解（53.7%)」という回答結果であり、大多数が全社員の協力と経営サイドの関与が必須と感じていることを示している。

また、セキュリティ対策を行う上でリスク分析を「実施している」のはわずか12%であり、実施していない理由は、「手法がわからない（44.7%)」、「効果がわからない(33.2%)」、「予算がない（21.9%)」等が挙げられている。その反面で、情報システムのリスクが発現すると「企業の倒産や多大な損失がある」との回答は60%にも達している。

最後に、「従業員に対し、情報セキュリティの教育を実施しているか」という質問の結果は、「実施している」が12.9%、情報処理サービスでも36%と低い状況にとどまっており、今後の安全対策を実施していく上での大きな課題といえる。

表２　セキュリティポリシーの設定の仕方

質　　問	YES
① 経営理念に基づきセキュリティポリシーを定めているか	18.9%
② 操作および業務処理手順書を定めているか	27.9%
③ 出張中・移動中の環境についてのガイドラインがあるか	26.0%
④ ガイドラインは定期的に見直しているか	54.1%
⑤ 専任のセキュリティ責任者または担当者がいるか	23.8%
⑥ 国際的に情報システムを展開・利用しているか	6.7%
⑦ ⑥でYESの場合、セキュリティ対策を講じているか	72.4%

注）③、④は②で「操作および業務処理手順書を定めている」と答えた中での比率

〈参考文献〉

１．『情報化白書2000』，日本情報処理開発協会（2000年６月発行）
２．『わが国における情報セキュリティの実態』，日本情報処理開発協会（2000年３月発行）
３．『金融機関等におけるセキュリティポリシー策定のための手引書』，金融情報システムセンター（1999年11月発行）
４．『情報サービス産業白書2000』，情報サービス産業協会（2000年５月発行）
５．『平成11年度セキュリティ・ビジネスの動向に関する調査』，情報サービス産業協会（2000年３月発行）
６．上原孝之著：『ネットワーク危機管理入門』，翔泳社（2000年７月発行）