平成 13 年度

学士学位論文

組織における情報セキュリティポリシーの策定手法

The decision technique of an information security policy in an organization

1010417　　戸梶 桃

指導教員　　菊池 豊

2001 年 2 月 5 日

高知工科大学 情報システム工学科

要 旨

組織における情報セキュリティポリシーの策定手法

戸梶 桃

近年，不正アクセスなどネットワークを利用した犯罪が急増している．その中，情報セキュリティ対策を行うにあたって「セキュリティポリシー」を組織内で定める手法が注目されている．セキュリティポリシーとは，組織の体制や情報セキュリティに対する考え方，そして取り組み方を表した方針である．

本研究の目的は，セキュリティポリシーの策定手法を検証することである．この目的を達成するために，セキュリティポリシーを採用した英国の規格 BS7799 を検証した．そしてその手段として，菊池研究室で BS7799 を導入することを試みた．

その結果，BS7799 は小規模の組織には向いていないと結論する．BS7799 の導入には人的・時間的なコストがかかり，小規模な組織では，コストに比較して得られるセキュリティ強度が小さすぎる．BS7799 の導入には，セキュリティ対策に人員・時間を割くことのできる，ある程度大規模の組織が向いている．

キーワード　セキュリティポリシー，BS7799，検証

Abstract

The decision technique of an information security policy in an organization

Momo Tokaji

In recent years, the crime using networks is increasing rapidly such as unjust access. The technique of defining a security policy in an organization attracts attention in performing an information security. At this time, the technique of defining a "security policy" in an organization attracts attention in performing an information security. A security policy is a policy express system of an organization, the view over an information security of one, and the way of tackling which receives.

The purpose of this research is verifying the decision technique of a security policy. In order to attain this purpose, I verified the standard BS7799 of Britain which adopted the security policy. And as the means, I tried to introduce BS7799 at the Kikuchi laboratory. Consequently, I conclude that BS7799 has not turned to a small-scale company. Human and time cost start introduction of BS7799, and the security strength obtained as compared with cost is too small in a small-scale organization. The to some extent large organization can spare a staff and time for the security measure is fit for introduction of BS7799.

key words security policy, BS7799, verifying

目次

図目次

表目次

第 1 章

はじめに

昨今，ネットワーク技術は急速に進歩を遂げ，電子商取引などが普及し，IT 革命の時代となっている．そしてこれからは，会社とつながっている自宅のパソコンで仕事が行える在宅勤務なども増え，ネットワークに頼った生活が益々増加していくであろうことが予測される．

しかしそれと同時に，不正アクセスなどネットワークを利用した犯罪も急速に発展してきていることは無視できない．日本では，昨年一年間で不正アクセスが続発する事実などもあり，情報セキュリティに対する考えの甘さが浮き彫りにされた．欧米では次々に情報セキュリティに関する整備が行われてきている．このような欧米で今，「セキュリティポリシー」が注目されてきている．

セキュリティポリシーは，日本では銀行・金融業界など，機密情報や個人情報を多く扱う組織で取り入れられている考え方である．昨年セキュリティの弱さが取り上げられた中央省庁はセキュリティ強化のために「情報セキュリティポリシーに関するガイドライン」を 2000 年 7 月に定めている．このガイドラインでも，セキュリティポリシーを採用している．そこで本研究では，セキュリティポリシーの策定手法の検証を目的とした．セキュリティポリシーの策定手法を実際に自分の研究室に採用し，検証することによって，セキュリティポリシーの有効性の有無を確認したいと考えた．私は，いくつかあるセキュリティポリシーを採用している規格の中でも，今特に注目され，中央省庁のセキュリティ対策の基盤ともなっている英国の規格 BS7799 を検証した．

以下 2 章でネットワーク犯罪やセキュリティ技術など，ネットワーク社会の現状について

述べる．次に 3 章で BS7799 の概要を述べ，セキュリティ対策のシステムを確立する手順について説明する．この手順は，BS7799 の内容を要約したものである．そして 4 章で実際に手順に沿って検証した過程を示す．4 章の最後では，実行過程の結果より BS7799 の利点・欠点を挙げ，考察してまとめた．最後に第 5 章で，結論と今後の課題を記す．

第 2 章

ネットワーク犯罪と情報セキュリティ技術

この章では，ネットワーク犯罪や情報セキュリティ技術の現状を述べ，「セキュリティポリシー」についての説明を行う．

2.1　ネットワーク社会の現状

この節では，日本のネットワーク社会でのパソコンの普及率やインターネット利用の推移を述べる．

2.1.1　パソコン普及状況

経済企画庁の発表によると，近年のパソコンの普及率の推移は図 2.1 によると，確実に延びてきている．この結果は，米国の 50 %と比較するとまだまだ普及率は低い．しかし，今後益々家庭においてのパソコン普及が見込まれると予測する．

2.1.2　インターネットの利用状況

近年の日本でのインターネット利用状況を，利用者，利用世帯，利用企業別に表す．

- インターネット利用者

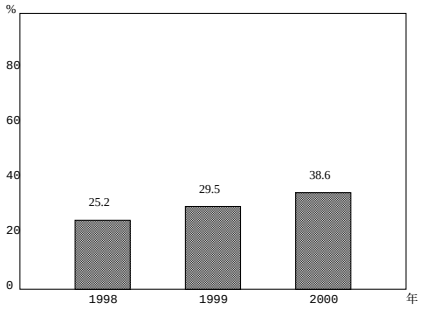

図 2.1　パソコンの普及率の推移

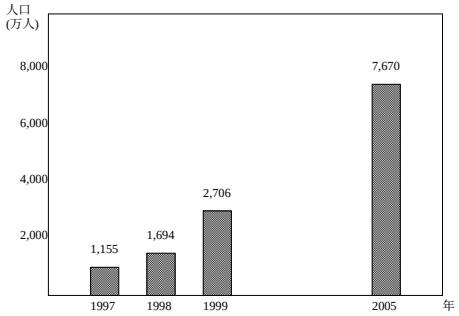

図 2.2　インターネット利用者の推移

パソコンの普及に伴いインターネット利用者も年々増加しており，図 2.2[*1] によると，1999 年にはその 2 年前 1997 年の約 2 倍の 2706 万人になっており，2005 年にはその約 3 倍の 7670 万人に達すると推計されている．そして，現在のインターネット利用人口は世界第 2 位，普及率は世界第 13 位となっている．[*2]

- インターネット利用世帯

[*1] 郵政省 通信白書 我が国におけるインターネットの普及状況図表
http://www.mpt.go.jp/policyreports/japanese/papers/h12/1index.html より抜粋

[*2] 郵政省 通信白書 インターネットの普及
http://www.mpt.go.jp/policyreports/japanese/papers/h12/1index.html より抜粋

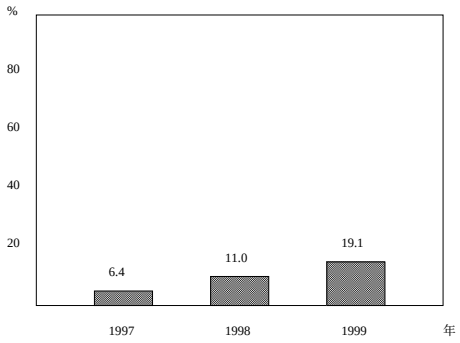

図 2.3　インターネット利用世帯の推移

利用者と同様に，インターネット利用世帯も年々増加しており，図 2.3[*3]によると，普及率は 1997 年から 1999 年の 2 年間で約 3 倍となっている．在宅勤務などの理由でインターネットを自宅で利用する機会が増え，今後更に普及していくと考える．

- インターネット利用企業

  図 2.4[*4]によると，インターネットを利用している企業は 1997 年の時点で 68.2 %と高く，1999 年には 88.6 %とほとんどの企業がインターネットを利用している．この背景には，インターネットによる情報収集，電子商取引やイントラネット、エクストラネットの利用などが考えられる．

2.1.3　企業によるセキュリティ対策状況

この節では，企業のファイアウォール構築状況とファイアウォール以外のセキュリティ対策の状況を記述する．

- ファイアウォール構築状況

[*3] 郵政省 通信白書 我が国におけるインターネットの普及状況図表
http://www.mpt.go.jp/policyreports/japanese/papers/h12/1index.html より抜粋

[*4] 郵政省 通信白書 我が国におけるインターネットの普及状況図表
http://www.mpt.go.jp/policyreports/japanese/papers/h12/1index.html より抜粋

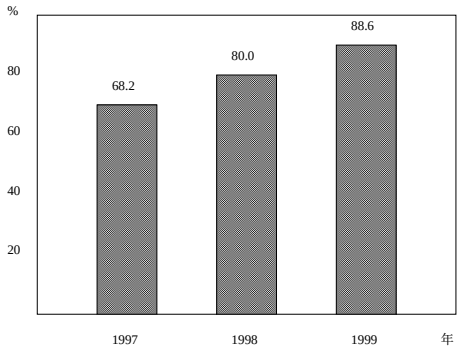

図 2.4　インターネット利用企業の推移

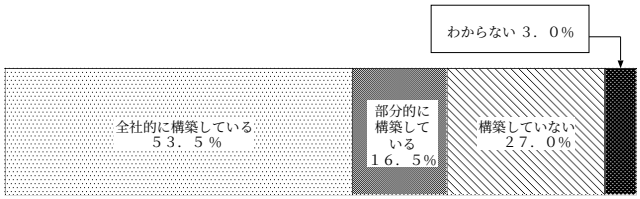

図 2.5　ファイアウォール構築状況

ファイアウォールは，セキュリティにおいて最も重要な対策の一つである．特に企業では，イントラネットの構築などでネットワークを利用する機会が多く，不正アクセスなどの被害にあう可能性が高くなる．そのセキュリティ対策としてファイアウォールを構築している企業が多い．図 2.5 によると，全体の半数以上である 70 %の企業がファイアウォールを構築している．これは昨年と比較すると増加傾向にある．これは，最近続出した不正アクセスが原因だと考える．図 2.4[4] によると，1999 年に 88．6 %の企業がインターネットを利用しているのに対して，ファイアウォール構築企業は 70 %となっている．よって，約 18.6 %の企業が未だファイアウォールの構築なしでインターネットを利用していると予測する．

- ファイアウォール以外のセキュリティ対策の有無状況

  図 2.6[4] によると，企業ではファイアウォール以外のセキュリティ対策はあまり行われ

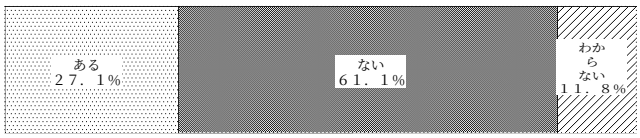

図 2.6　ファイアウォール以外のセキュリティ対策の有無状況

ていないのが現状である．企業の規模別で考えると，ファイアウォール以外のセキュリティ対策を導入している企業は 100 人未満の小規模企業が多い [4].

2.2　ネットワーク犯罪の実例

近年，日本で実際に起きたネットワーク犯罪をいくつか挙げる．

- 科学技術庁に不正アクセス (平成 12 年 1 月)

  科学技術庁ホームページが 24 日，クラッカーによって「いまや日本人は負け犬だ」などと日本人を批判する文章が英語で書き換えられた．そして 2 日後の 26 日，同ホームページの「調整中」の画面が中国語で南京大虐殺の抗議文に書き換えられた. *5
- 統計局の HP データ、消去 (平成 12 年 1 月)

  総務庁統計局のホームページ用ウェブサーバのデータやプログラムがすべて消去された．外部から何者かがウェブサーバーに侵入し，データを消去したと見られている. *6
- 他人のパスワードを使用してホームページ開設 (平成 12 年 3 月)

  他人のＩＤ・パスワードをクラッキング・ツール等で入手し，不正にインターネットに接続してホームページを開設し，違法に薬物を販売しようとしていた．　*7
- 新種ウイルス「HYBRIS(ハイブリス)」が急増 (平成 13 年 1 月)

  新種のコンピューターウイルス「ハイブリス」の国内感染が急増していることが明らか

*5 Mainichi INTERACTIVE, http://www12.mainichi.co.jp/より抜粋
*6 Mainichi INTERACTIVE, http://www12.mainichi.co.jp/より抜粋
*7 警視庁 HP, http://www.npa.go.jp/より抜粋

になった.「ハイブリス」とは，電子メールの添付ファイルとして感染するウイルスで，日本語環境の場合，差出人，件名，本文が空白の，8 文字のアルファベット名の exe ファイルを添付した電子メールを一定の時間をおいて，返信メールとして送信する症状がある．また，インターネットからダウンロードしたプラグインを組み込む機能もあり，渦巻きのアニメーションを表示してパソコン操作を妨害するタイプも発見されているという.[*8]

2.2.1 ネットワーク犯罪の現状

この節で挙げた例はほんの一部であり，現状としては様々なネットワーク犯罪が急増している．科学技術庁や統計局への不正アクセスの例に関しては，2000 年 1 月から 2 月にかけて急増した中央省庁への不正アクセスの一部として挙げた．これは，1 月だけでも科学技術庁，総務庁，郵政省など中央省庁や，その関連機関サイトが 20 件以上書き換えの被害に遭っている[*9] ．

情報処理振興事業協会の報告によると，コンピュータウイルスが発見された件数は昨年と比較して，3 倍に増加しているのに対し，パソコンが実際にウイルス感染する被害に遭った割合は，99 年の 53.6 % (1953 件) から 2000 年は 19.6 % (2182 件) と大幅に減少しており[*10]，コンピュータウィルス技術が急増している反面，コンピュータウィルス対策の上では良い方向に進んでいると考える.

2.3 情報セキュリティ技術とその動向

この節では，現在の情報セキュリティ技術の説明を行い，その動向を述べる．取り上げた技術は，暗号技術，認証技術，ファイアウォールである．そして最後に不正アクセス禁止法についての説明とその動向について述べる.

[*8] Mainichi INTERACTIVE, http://www12.mainichi.co.jp/より抜粋
[*9] Mainichi INTERACTIVE, http://www12.mainichi.co.jp/より抜粋
[*10] Mainichi INTERACTIVE, http://www12.mainichi.co.jp/より抜粋

2.3.1 暗号技術

暗号技術とは，メッセージを一定のルールに従って変換することにより，ルールを知らない第三者がメッセージの内容を探知することを防ぐための技術である．

暗号技術について簡単に説明すると，基本的にはメッセージを暗号化すること及び復号することである．暗号化とは，メッセージの文字列又はデータ列を暗号化鍵によって別の文字列又はデータ列に変換することをいう．そして復号とは暗号文を復号鍵により変換前の文に戻すことをいう．[*11]

現在の主要な暗号技術の標準は，ほとんど米国で開発されたものである．機密性を確保するための共通鍵暗号技術は，DES が米国政府標準暗号として 1977 年に制定されて以来標準的な地位を確保してきたが，1997 年から 1999 年にかけての DES 解読コンテストにより，DES の安全性の限界が見え始めた．これに対応するため米国では 1997 年から次世代共通鍵暗号の米国政府標準化作業 (AES) を行っている．

一方，1997 年 3 月，各国政府が暗号政策に関する協力を定めた暗号に関する「暗号策定ガイドライン」が OECD 加盟国により制定された．これは，暗号政策について 8 つの原則を定めており，暗号に関してプライバシーの保護や電子商取引の発展に伴い基本的な項目の世界的な整合性を図るためもので，加盟各国の暗号政策に反映させるべきであるとしている[*12]．

2.3.2 認証技術

認証技術とは，ユーザーの信頼性そして情報の正当性を確認する技術である．その中でも電子認証とは，ユーザが本人であるということを電子的に確認する技術で，ECOM(電子商取引実証推進協議会) が認証技術に関するガイドラインとしてまとめている認証手段は，大きく分けて 3 つある．その 3 つとは，バイオメトリクス (生体計測)，その人しか持ち得ない

[*11] 警察庁 HP, 不正行為への対策, http://www.npa.go.jp/hightech/sec_repo/1-2.htm より抜粋
[*12] 株式会社エスパ, 暗号入門, http://www.e-space.ne.jp/espa/ango/ango.htm より抜粋

であろう所持品，そしてその人特有の秘密情報である．

まず，バイオメトリクスとは，指紋や掌形，筆圧やサインなど，人間の生体や行動などの特徴，本人特有の情報のことである．バイオメトリックスを使った認証は，指紋スキャナの前で本人が自分の指をスキャナに押し当て，その場で確認するような入退室管理などの利用に制限されているのが現状である．

次に，その人しか持ち得ないであろう所持品というのは，クレジットカードや運転免許証，IC カードなどである．これらによる認証は，身分を証明するための手段として提示する場合がほとんどである．IC カードによる認証は，入退室管理などにも使用されている．

その人特有の秘密情報とは，例えばパスワードや暗証番号などである．この方法は，ネットワークを介した認証を考えると，最も主流である．バイオメトリクスや IC カードなどと併用して認証される方法が FISC 監査安全部によって推奨されている．そして，現在はこのように盗聴ができるようなネットワークを介してでも安全に認証できるような手段として様々な方式も考えられてきている．それらの方式には，チャレンジ&レスポンス方式，ワンタイムパスワード方式，kerberos 方式，公開鍵暗号方式などがある[*13]．

2.3.3 ファイアウォール

ファイアウォール [1] は日本語では「防火壁」という意味であり，組織の外部ネットワークと内部ネットワークの間のアクセス制御を行うものであり，通常，内部ネットワークを不正アクセスなどから保護することを目的として導入される．アクセス制御方式には，パケットフィルタリング，トランスポートゲートウェイ，アプリケーションゲートウェイなどの種類があり，現在ではアプリケーションゲートウェイが主流である．ファイアウォールの基本的な機能は，組織外部からのアクセスに対して許可されたパケットのみ許可するアクセス制御と，ウィルスチェックや危険な Java アプレットなどの侵入を阻止するセキュリティの機能がある．

[*13] FISC 監査安全部, 平成 11 年度情報セキュリティ講演会報告 (その 2)2000 年 6 月 29 日更新版, http://www.fisc.or.jp/info/t52_000629.htm#2 より抜粋

2.3.4　不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）

ここに記している不正アクセス禁止法は，情報セキュリティ技術ではない．しかし，ネットワーク犯罪を防ぐために効果的だと考えるので，不正アクセス禁止法をセキュリティ対策の一つとして記述する．これは企業や政府機関などのコンピュータやネットワークに不正アクセスすることを禁止するという法律である，この法律は 2000 年 2 月に成立した．不正アクセスを行うと 1 年以下の懲役または 50 万円以下の罰金が科せられる．この法律は，不正アクセスをした情報が重要であるかどうかは関係なく，アクセスすることが禁止されているコンピュータやネットワークへのアクセス行為そのものを罰することが特徴である[*14]．

2.4　最良の情報セキュリティ対策

この節では，情報セキュリティの定義より，最も良い情報セキュリティ対策を考える．

2.4.1　情報セキュリティの定義

最良のセキュリティを，情報セキュリティの定義から考える．定義には，英国の規格 BS7799 の「情報の定義」を抜粋した [2]．情報セキュリティの定義を最も満たす方法が最良の情報セキュリティにより近づくことができると考えたからである．

情報セキュリティの定義：「情報の機密性、完全性及び利用の可能性の維持」

- 機密性：情報にアクセスすることが認可された者だけがアクセスすることを可能にすること．
- 完全性：情報及び処理方法の正確さ，及び完全である状態を完全防護すること．完全である状態というのは，情報及び処理方法の少しも欠けていない状態をいう．
- 利用の可能性：認可されたユーザが，必要時に，情報及び関連財産にアクセスできることを確実にすること．

[*14] Mainichi INTERACTIVE, http://www12.mainichi.co.jp/より抜粋

機密性を考えると，外部からのアクセス制限を強化しなければならない．完全性に対しても，正確な情報を維持するためにできるだけアクセスを制限しなければならない．しかし利用の可能性を考えると，機密性，完全性とは反対にアクセスの制限を緩めなければならなくなる．よって，情報セキュリティを完璧にすることは非常に困難で，いかにリスクを最小限にしながら，自分達にとっては制限の少ない環境をつくるかが大事である．つまり，機密性，完全性，利用の可能性，この 3 つのバランスをうまくとることによって，良いセキュリティが生まれる．

2.5　セキュリティポリシー

現在、セキュリティポリシー [3] を組織内で決定し，情報セキュリティ対策に取り組む方法が注目されている．セキュリティポリシーとは，組織の体制や，組織の情報セキュリティに対する考え，取り組み方を具体的に表した方針である。セキュリティポリシーに沿ってリスク分析などを行い，組織にとってどの情報が重要で，どのような脅威が起こるのか，そしてその脅威が起こりそうな確率，起きたときの被害の大きさなどを明確に定めるので，何をどのように，そしてどの程度守るべきなのかが明らかになる．よってこのセキュリティポリシーを採用する情報セキュリティ対策が，前の節で述べた機密性，完全性，利用の可能性のバランスが最もとれやすい方法だと考える．

セキュリティポリシーを策定することによって，組織全体のセキュリティ意識を統一し，より高めることができる．セキュリティポリシーを採用していない組織のセキュリティ対策は，組織の一部の専門家のみで行われているのが一般的である．セキュリティ対策が組織全体に伝わっていないと，どんなにセキュリティを強化しても，組織の人間には「これをしてはいけない.」ということしか伝わらず「なぜしてはいけないのか.」ということが伝わらないので，セキュリティ違反者が増えるといった結果になってしまう．セキュリティポリシー策定により，組織全体の意識を統一し，高めることによって最良の情報セキュリティ対策により近づくことが可能なはずである．

2.6 様々な情報セキュリティ規格

セキュリティポリシーを用いた情報セキュリティの規格の中でも，注目されているISO15408，TR13335，そしてBS7799の3つの規格を挙げる．この3つの規格は，セキュリティ規格という点と，セキュリティポリシーを採用しているという2点で同じである．しかし対策を行う対象が全て異なっているので，内容は全く違っている．この3つの規格はよく比較され，セキュリティポリシーを採用した規格の代表として示されることが多い．

- ISO15408

  「IT セキュリティ評価基準」と呼び，情報処理製品や情報処理システムなどのセキュリティ品質を評価するための規格である．つまり，「製品やシステムの開発・製造・運用にかかわった資材を検査することによって，大丈夫であることを確認する」という規格である．検査の対象は，通常の開発や運用で作成する文書などであり，プログラム設計書，プログラムソースコード，マニュアル，開発者・業務者への教育・業務規約などがある．これらに加えて，セキュリティ基本設計書と脆弱性分析書も含まれる．機能の面と，システムの品質の面から評価される．

  ISO15408 にはセキュリティ設計ガイドと呼ばれる，具体的な仕様や管理方法以外の共通部分だけを取り出した文書がある．例えば，具体的な機能仕様と品質管理方法を除いた，保護対象資源利用方針，評価対象のセキュリティ脅威，対策方針などである．これらは製品種別や業務種別ごとに共通に利用できる[*15]．

- ISO/IEC TR13335(GMITS)

  TR 13335 は，IT 製品を導入した機関においてシステムを管理するための手順等に関する指針を記述した規格である．IT 製品が高度のセキュリティ要件を満たしていたとしても，それを利用する組織内で入室，記憶媒体，パスワード等の種々の管理を厳密に行わなければ，セキュリティ機能は維持できない．そこで GMITS では，ユーザ機関の

[*15] SO15408 の意義とビジネス・システム開発への影響，(社) 日本情報システム・ユーザー協会，http://www.juas.or.jp/pub/mnl/iso15408.html より抜粋

システム運用に関わる管理手続き等に関する指針を定めている．GMITS は，概念とモデル，管理と計画，技術手段，安全保護手段の選択，ネットワークセキュリティ管理指針の 5 部で構成されている．[*16]

- BS7799

  システムを安全に運用するための主に組織、教育等の運用面でのセキュリティ管理方法を定めた規格[*17]．技術的な詳細手順を定めているのではなく，組織全体で情報セキュリティ対策を行っていく上での管理方法を定めている．

  2001 年に通産省は，認証制度として国際標準である BS7799-1 を取り入れた ISO/IEC 17799-1 を定めることを決定している．これは，BS7799 の第 2 部に記されている情報セキュリティ管理システム要求事項の仕様書によって認証が行われている．[*18]

  日本では，BS7799 は今は参考文献として使用されている程度である．しかし ISO 規格に定められることによって，日本でも益々普及してくるであろうことを予測する．

以上の 3 つの規格を比較して，BS7799 を菊池研究室で検証することにした．その理由として BS7799 は，組織全体で情報セキュリティ対策を行っていく上での管理方法に重点を置いているからである．この方法が最も「情報セキュリティの定義 (2.4.1 参照)」を満たすことができると考えた．

もう一つの理由として，BS7799 の情報セキュリティの管理システムの手順は，詳細のまで定められていないことである．よって組織の特徴，種類に関係なく，どの組織でも導入することができるので，菊池研究室でも導入が容易だと考えた．

本研究の目的であるセキュリティポリシーの策定手法を検証するという目的を達成するために，この BS7799 の規格を検証した．その手段として，菊池研究室で BS7799 を導入することを試みた．

[*16] DIS 17799-1(情報セキュリティ管理指針) に関する主な論点，苗村 憲司，http://www.itscj.ipsj.or.jp/jp/ns01015.html より抜粋

[*17] 情報セキュリティの標準化, 富士通株式会社, http://www.fujitsu.co.jp/hypertext/svision/secure/service/infosecure/iss1.h より抜粋

[*18] 月刊アイソス 2000 年 11 月号，http://www.wnn.or.jp/wnn-eco/iso/topics/0011_m.html より抜粋

第 3 章

BS7799 の概要

この章では，BS7799 に記述されている情報セキュリティ管理システムの確立方法について，一連の作業の説明する．情報セキュリティ管理システムとは，BS7799 で記されている情報セキュリティ対策を行うためのシステムである．

3.1 BS7799 の構成

1999 年に英国で発行された BS7799[2] は, 次の 2 部から構成される．

3.1.1 第 1 部：情報セキュリティ管理実施基準

BS7799 第 1 部の基盤は BS7799-1:1995 であり，これは情報セキュリティにおける最善の方法をまとめた包括的管理策を規定するために，1995 年に発行された．この規格は情報システムが工業及び商業分野で使用される際に，ほとんどどの状況でも必要とされる管理策の範囲を明確にするための基準として使用されることを目的としている．

1999 版では，ネットワークや通信などの情報処理技術の利用における最近の発展を考慮に入れており，BS7799-1:1995 と比較すると，情報セキュリティにおける事業の関わり及び責任に大きな重点を置いている．

3.1.2 第 2 部：情報セキュリティ管理システム仕様

第 2 部では，いくつかあるセキュリティ対策の要求事項に対する最良の方法についての仕様書を記述している．つまり情報セキュリティ管理システムを確立するための一連の作業の

仕様書になっている.

BS7799 第 2 部の基盤は BS7799-2:1998 である．これについての変更点はほとんどない．しかし第 1 部から第 2 部へ引用する箇所があるので，第 1 部が 1995 年版から 1999 年版になったときの変更点が，その部分に反映されたのみである．その他の変更点はない.

3.1.3　第 1 部と第 2 部の関係

第 1 部と第 2 部の関係について述べる．第 2 部で記述されている情報セキュリティ管理システムを確立する際のの中に，第 1 部の管理目的及び管理策から選択仕様書になっているのに対して, 第 1 部は一般的な場合についての管理策が示されており, その中から組織に応じて適切な管理策を選択し, 第 2 部の仕様書から作成されるドキュメントに組み込む仕組みになっている.

3.2　情報セキュリティ管理システムの要求事項

BS7799 の第 2 部には情報セキュリティ管理システムにおける一連の行動が記述されている．よってここではシステム確立のための要求事項を要約する．情報セキュリティ管理システム (Infomation Security Management System) とは，BS7799 が提案する，情報セキュリティ対策のシステムを確立する仕様書を表す．情報セキュリティ管理システムを以下 ISMS と呼び，ISMS 確立の過程で作成されるドキュメントを ISMS ドキュメンテーションと呼ぶ.

ISMS 要求事項の流れを図 3.1 に表した.

3.2.1　一般の管理

組織は ISMS を確立して文書化し，これを維持しなければならない．作成された ISMS は，保護すべき財産，リスクマネジメントに対する組織の取り組み方法，管理目的及び管理策，それらに対すて保証できる度合いに対応したものでなければならない.

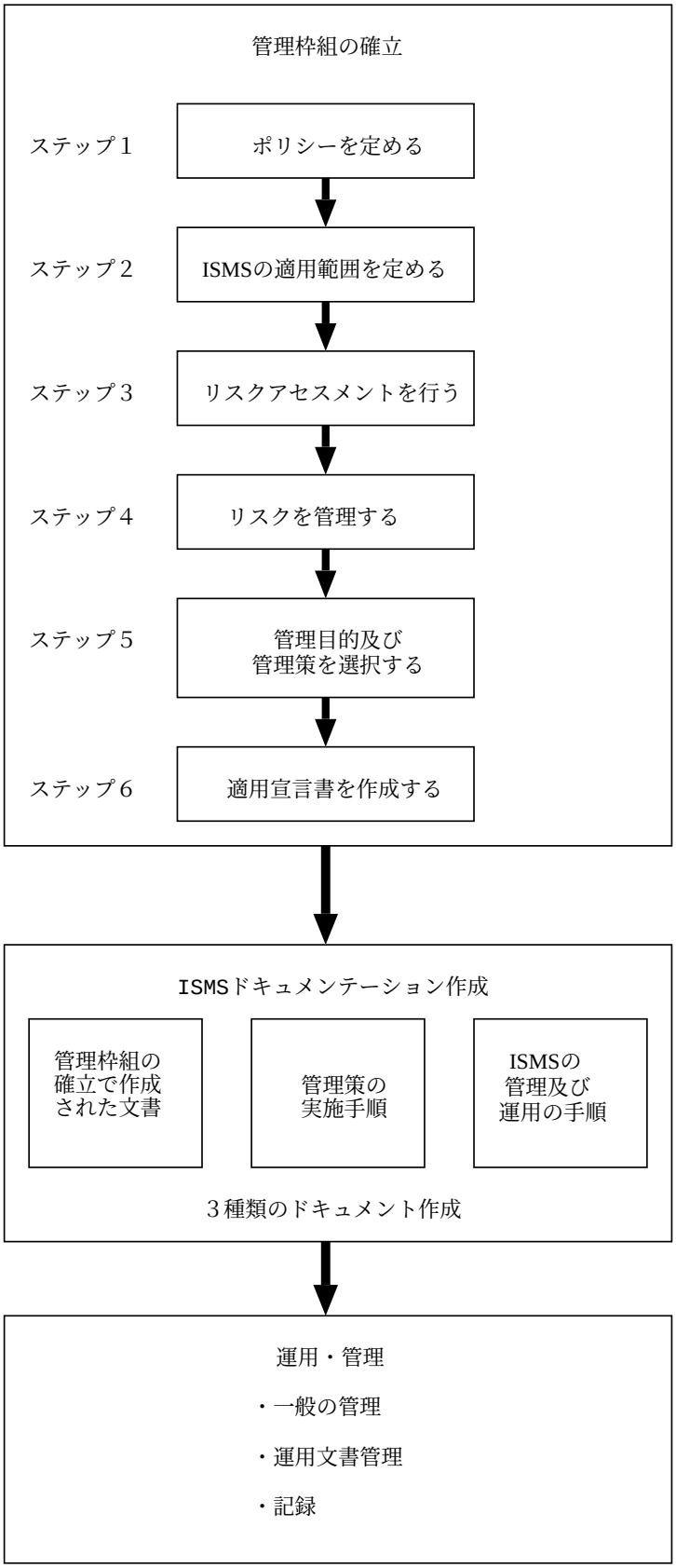

図 3.1　ISMS 要求事項の流れ

3.2.2　管理枠組の確立

管理枠組の確立とは，情報セキュリティ対策の骨組みを確立することである．

- 情報セキュリティポリシーを明確に定めなければならない．
- 情報セキュリティ管理システムの範囲を明確に定めなければならない．境界は，組織の特性，組織の位置，財政及び技術の点から定めなければならない．
- 適切なリスクアセスメントを実施しなければならない．リスクアセスメントでは，財産に対する脅威，バルネラビリティ (脆弱性)，並びに組織に及ぼす影響を明らかにしなければならず，さらに，リスクの度合いを決めなければならない．
- 管理すべきリスクのエリアは，組織の情報セキュリティポリシー並びに要求される保証の度合に基づいて明らかにしなければならない．
- 組織による運用のために，適切な管理目的及び管理策選択を第 1 部，または第 2 部の 4 節から選択しなければならない．第 2 部 4 節の管理目的及び管理策は完全なものでなく，第 1 部から引用したものなので，追加の管理策を選択することもできる．
- 適用宣言書を作成しなければならない．選択された管理目的や管理策，並びにそれらを選択した理由を適用宣言書に文書として示さなければならない．この宣言書には，第 2 部の 4 節に列挙されている運用管理策のうち，除外されたものも記録しなければならない．

これらの作業項目は，必要に応じ，適切に定められた間隔でレビューをしなければならない．

3.2.3　運用

選択された管理目的及び管理策は，組織によって有効に実施されなければならない．管理策を実行するために定められた手順の有効性はレビューによって確認されなければならない．

3.2.4　ISMS ドキュメンテーション作成

ISMS ドキュメンテーションは、次の情報で構成されなければならない：

- 3.2.2 で示される，実施された行動の証拠.
- 情報セキュリティポリシー並びに適用宣言書に記述された管理目的及び実行された管理策を含め，管理枠組の要約．この文書はセキュリティポリシー文書と一緒に組み込んでも良い.
- 3.2.3 で示された管理策を実施するために採用された手順．この手順では，責任及び関連行動を記述しなければならない．この文書はセキュリティポリシー文書と一緒に組み込んでも良い.
- ISMS の管理及び運用について定めた手順．この手順では，責任及び関連行動を記述しなければならない.

3.2.5　文書管理

組織は，3.2.4 より要求される全てのドキュメンテーションが次の条件を満たすことを確実にするために，そのドキュメンテーションを管理する手順を確立し，維持しなければならない.

- 容易に利用できる.
- 定期的にレビューし，組織のセキュリティポリシーと照らして必要に応じて改訂する.
- バージョンの管理により維持され，さらに，ISMS が有効に機能するために不可欠な作業が実施されるすべてのロケーションにおいて，入手可能である.
- 実情からかけ離れたものになった場合には，速やかに廃止される.
- 実情からかけ離れたものになったが，法律に関わる目的又は知識の保存のため，もしくは両方の目的のために要求される場合には，区別され，保管される.

ドキュメンテーションは読みやすく，日付が記述されており，容易に識別でき，整理整頓された状態で維持されており，指定された期間に渡って保管されなければならない．種々の形式の文書を作成及び修正するための手順及び責任を確立し，維持しなければならない．文書は，ハードコピー又は電子媒体など，どんな媒体によるものでもよい．

3.2.6　記録

運用は，ISMS の運用の結果として記録が必要であり，それらは，当該システム及び組織に適用される．BS7799 の第 2 部の要求事項に準拠していることを実証するために維持されなければならず，それらの記録としては，例えば，ビジターの記録，監査記録及びアクセスの認可などがある．

組織は，準拠を実証する記録を識別し，維持し，保持し，処置する手順を確立し，維持しなければならない．

記録は，読みやすく，識別可能で，関係している活動を突き止めることができるものでなければならない．記録は，容易に取り出すことができるように保管し，維持されなければならず，また，損傷，劣化，紛失／消失しないように保護されなければならない．記録は，ハードコピー又は電子媒体など，いかなる媒体にされてもよい．

第 4 章

BS7799 の検証

この章では，菊池研究室で実行した BS7799 検証の過程を記述する．本研究では，まず BS7799 の管理枠組の確立を行った．次に，対策手順などを定めるマニュアル作成やその運用・管理が可能であるかを考察した．最後に作成した文書を研究室の管理担当学生に提示し，その意見及び提案をまとめた．

4.1 準備

まず，研究室内の学生に BS7799 検証の旨を伝え，研究室という組織の情報セキュリティ対策を行う強い意識を持ってもらうために BS7799 の内容について説明を行った．組織全体が組織の情報を保護するということについて強い意志がないと，セキュリティポリシーの意味がなくなってしまうからである．そして，セキュリティについての技術的な知識をつけるためにネットワーク犯罪の実例やその対策などを中心に勉強した．

4.1.1 管理枠組の確立

管理枠組の確立とは，情報セキュリティの骨組みを確立する過程である．

最初に，3 章で示した情報セキュリティ管理システムの要求事項の中の管理枠組の確立の手順に沿って文書を作成した．この節では，定めたセキュリティポリシー文書を記述する．BS7799 の第 2 部に記述されている管理策の一つに「情報セキュリティポリシー文書」の項目があるので，それに基づいて情報セキュリティポリシー文書を作成した．「情報セキュリティポリシー文書」を引用したものを次に示す．

情報セキュリティポリシー文書を書く

ポリシー文書は，経営陣によって承認され，発行され，妥当であるならば組織内の全ての人に知らされることが望ましい．ポリシー文書には，経営陣の参加を明記し，情報セキュリティの管理に対する組織の取組方法を定めることが望ましい．最低条件として，次の手引きを含めることが望ましい：

1. 情報セキュリティの定義，その全般的な目的及び適用範囲，並びに組織で情報を共有するためのセキュリティの重要性[*1]
2. 情報セキュリティの目標及び原則を支持する経営陣の意向声明書
3. 組織にとって特に重要なセキュリティポリシー，原則，規格及び準拠要求事項等の説明

   それらの例としては，次のようなものがある：

   - 法的及び契約上の要求事項への準拠
   - セキュリティ教育要求事項
   - ウィルス及び他の不正ソフトウェアの予防及び検出
   - 事業継続管理
   - セキュリティポリシー違反の結果
4. セキュリティ事故の報告などを含め，情報セキュリティ管理の一般的及び特定責任の定義
5. ポリシーを支持する可能性がある書類，例えば，特定の情報システムについてのさらに詳細なセキュリティポリシーや，ユーザが従うことが望ましいセキュリティ規則などの参照指示

この引用文に沿って情報セキュリティポリシー文書を作成したものを次に示す．

[*1] BS7799 では「情報共有を可能にするための機構としてのセキュリティの重要性」とあるが，分かりやすいように「組織で情報を共有するためのセキュリティの重要性」とする．

1. 情報セキュリティの定義

   「情報の機密性，完全性及び利用の可能性の維持」

   詳しくは 2.4.1 を参照

2. 情報セキュリティの目的

   研究室の損害を最小限に抑え、研究の継続性を確実にするために，研究室の学生全員が協力して広範囲にわたる脅威から情報を保護する．

3. 適用範囲

   情報セキュリティ対策を取り入れる範囲は，基本的には菊池研究室とする．財産的な範囲として，研究室内で共有している情報，研究室の研究に関係する全ての情報を，情報セキュリティ管理システムの適用範囲とする．

   そして，研究室内の者全員にこのシステムを適用することとする．

4. 組織で情報を共有するためのセキュリティの重要性

   研究室の情報や，その情報を扱うシステムやネットワーク，そして情報を扱う際のプロセスなどは，研究室にとって重要な財産である．その財産を保護するため，研究室全体で情報セキュリティに真剣に取り組むことによって，研究室の財産は保護され，研究室という組織が成立する．誰か一人でもそれに違反する者が現れた場合は，研究室が重大な危機に陥る可能性が出てくる．

5. 意向声明書

   研究室生全員がセキュリティポリシーに従い，責任を持って研究室の情報資産を保護していくものとする．

6. 研究室にとって重要なセキュリティポリシー，原則，規格及び準拠要求事項

   - 本ドキュメントに準拠すること．
   - 本ドキュメントは，定められた手順に従い，定期的にレビューされること．
   - ポリシーに変更・追加があった場合は，研究室内の学生全員に知らされること．
   - 新しいソフトウェア導入の際は，定められた手順に従い，厳密に協議されること．
   - 入退室管理を厳密に行うこと．

- 法律的な違反のチェックが定期的に行われること.
- ネットワーク事故又はセキュリティホールが発見された場合の対処が，定められた手順に沿って速やかに行われること.
- セキュリティの技術的な面は，専門的知識を有する研究生，又は教員によって講義が行われ，教育されること.
- セキュリティポリシーに違反する行為が見られた場合，直ちに協議され，それに沿った処罰が与えられること.

7. セキュリティ管理の一般的及び特定責任の定義

   一般的には研究生個人が各研究の情報，個人の情報を責任を持って保護すること．セキュリティ事故の報告も責任の範囲とする.

8. その他の参照書類

   特になし.

4.1.2 セキュリティポリシーの考察

定めたポリシーに対して，マニュアル作成やその運用・管理が可能であるか考察した．その結果を記述する.

1. 情報セキュリティの定義

   結果：情報の機密性，完全性，利用の可能性の全てを維持することは困難である.

2. 情報セキュリティの目的

   結果：この目的達成のためには，情報セキュリティの定義の中の「利用の可能性の維持」を犠牲にしなければならない．すなわち，セキュリティ対策のためにアクセスを制限しすぎて，逆にアクセスを許可された者がアクセスしたいときにできない場合が起きてしまう．よって，このように機密性について全く考えていない目的を持つことは，良いセキュリティ対策とは言えない.

3. 適用範囲

結果：他組織との共同研究によって情報を共有する場合，その情報は範囲に含められるのか．そしてその場合，共同研究をする組織も情報セキュリティ管理システムの範囲に含められるか．メールなど個人の情報は範囲に含めるかが問題となる．

4. 情報共有を可能にするための機構としてのセキュリティの重要性

結果：この説明文を読むことによって，全員に研究室の情報の重要性，情報セキュリティの必要性が伝わるかどうかが問題である．この項目に対して誰からの理解も得ることができなかったら，この項目は全く意味がない．そうなると，この項目をセキュリティポリシーに組み込むことが必要かどうかが問題となる．

5. 意向声明書

結果：セキュリティーポリシーに従う意志のない者も，形式上意向声明書に同意することができる．もし，そのような者が存在する場合は，この意向声明書は意味がない文章になってしまう．

6. 研究室にとって重要なセキュリティポリシー，原則，規格及び準拠要求事項

- 本ドキュメントに準拠すること．

  結果：意向声明書に同意した時点でこの方針は満たされている．意向声明書と同じである．

- 本ドキュメントは，定められた手順に従い，定期的にレビューされること．

  結果：研究室は，人間の入れ替わりが頻繁である．レビューによりポリシーを常に研究室に沿った内容にできる．そして，ポリシーを定期的にチェックすることで，ポリシーの内容常に念頭に入れておくことができる．しかし定期的にレビューを行い，ポリシーを常に維持することにコストがかかる．

- ポリシーに変更・追加があった場合は，研究室内の学生全員に知らされること．

  結果：可能である

- 新しいソフトウェア導入の際は，定められた手順に従い，厳密に協議されること．

  結果：新しいソフトウェア導入の度に手順に従って協議することは，時間的コスト及び人的コストの面で困難となる．

- 入退室管理を厳密に行うこと.

  結果：IC カードで主な侵入を防ぐことができるものの，現実には部外者全ての入室を拒否することは不可能である.

- 法律的な違反のチェックが定期的に行われること.

  結果：研究室内で，法律に関しての専門的な知識を有する者を設けることは困難である.

- ネットワーク事故又はセキュリティホールが発見された場合の対処が，定められた手順に沿って速やかに行われること.

  結果：実際にネットワーク事故やセキュリティホールが発見された場合，定めた手順とは異なる方法をとってしまう可能性がある.

- セキュリティの技術的な面は，専門的知識を有する研究生，又は教員によって講義が行われ，教育されること.

  結論：普段から互いに教え合うことや，時間を設けて講義をすることは可能である.

- セキュリティポリシーに違反する行為が見られた場合，直ちに協議され，それに沿った処罰が与えられること.

  結果：研究室内で処罰の実行は困難である．ほとんどが互いに注意し合うことで解決できる範囲である.

7. セキュリティ管理の一般的及び特定責任の定義

   結果：セキュリティ事故に対する個人の認識が異なるため，責任を定めることができない.

8. その他の参照書類特になし.

4.1.3 セキュリティポリシー考察のまとめ

研究室用に定めたセキュリティポリシーで，マニュアル作成や管理・運用が可能であるか考察した結果，セキュリティポリシーにはほとんど問題点があった．よってこのセキュリティポリシーで管理・運用を行っても，ほとんど守られないという結果になる可能性があ

る．全体的に問題点を見ると，人的・時間的コストの問題が多い．そして手順を定めても従われない可能性が高い．

4.1.4　管理枠組の確立の結果

管理枠組の確立を行い (3.2.2 参照)，作成した文書を研究室の管理担当学生に提示し，それに対する個人々々の意見及び提案をまとめた．ここでは，まとめた文書の一部を記述し，文書全体は付録 A に示す．

1. 情報セキュリティポリシー

   2.4.1 参照.

2. ISMS の範囲

   情報セキュリティ対策を取り入れる範囲は，基本的には菊池研究室とする．財産的な範囲として，研究室内で共有している情報，研究室の研究に関係する全ての情報を，情報セキュリティ管理システムの適用範囲とする．

3. リスクアセスメント

   ここでは，起こり得る外部からの脅威の表を表 4.1 に示す．

表 4.1　外部からの脅威

脅威	影響	度合い
データの持ち出し，破壊，改ざん，盗聴	データ喪失，情報漏洩など	中
不正アクセス	データ喪失，情報漏洩など	中
コンピュータウィルス	データ喪失，信用喪失など	大
物質破損	データ喪失，金銭的損害など	中
盗難 (HD，極秘資料など)	データ喪失，金銭的損害など	大

4. リスク管理

起こり得る外部からの脅威に対する対策の表を表 4.2 に示す.

表 4.2 外部からの脅威への対策

脅威	対策	保証の度合
データの持ち出し，破壊，改ざん，盗聴	ファイアウォール，暗号化，認証技術強化 ログ取り，バックアップなど	中
不正アクセス	ファイアウォール，暗号化 認証技術強化，ログ取りなど	中
コンピュータウィルス	コンピュータウィルス対策ソフトなど	中
物質破損	施錠，警備強化など	大
盗難 (HD，極秘資料など)	施錠，警備強化など	大

5. 管理目的及び管理策

BS7799 の第 1 部より選択した管理目的及び管理策の中，一つの項目を挙げる.

- 情報の分類

  目的：情報財産が適切なレベルの保護を確実に受けられるようにすること.

  情報は，保護の必要生，優先順位及び保護の程度を決定するために分類すること.

  ここで注意することは，情報は必ずしも常に一定の重要レベルではないということである．例えばポリシーなどの変化に沿って情報財産のレベルが変化することなども考えられる.

6. 適宜宣言書

管理目的及び管理策を選択した理由を記述する適宜宣言書を一つの項目について挙げる.

- 情報の分類

  情報を重要度のレベルに分類することにより，どの場所にどの程度情報セキュリティ対策を取り入れるかを明らかにするため.

4.1.5 管理枠組の確立のまとめ

管理枠組の確立を行うにあたっての反省点を 2 点述べる．そしてその反省点より，管理枠組の確立においての注意点を考察する．リスクアセスメントの方法と意見・提案の収集方法について述べる．

最初にリスクアセスメントの方法について述べる．リスクアセスメントを行う際に，研究室で保護すべき情報の分析を行うべきであった．本研究で作成したリスクアセスメントの表 (例：表 4.1) には，何が危険であるか，どこが脅威にさらされるのかが示されていない．よってリスク管理の際に，何を守るべきなのか，どこに対策を立てるのか明らかにされないまま対策を立てることになってしまった．

リスクアセスメントの最初の作業として「保護すべき情報」,「情報の場所」,「情報の重要な程度」を明らかにしておくべきである．リスクアセスメント，そしてリスク管理は情報セキュリティ対策において最も重要な過程の一つである．この過程で，何をどのように，どの程度守るべきなのかをはっきりさせていないと，全体の情報セキュリティの質が低いものになってしまう．

次に意見・提案の収集方法について述べる．この実行方法は，提示した文書に対して研究室の管理担当学生それぞれの意見を集める方法をとった．これにより，管理担当学生全員が集まる時間を削減できる．しかしこの方法では，文書に対してのみの意見・提案しか出ない．よって，全体的に文書に対しての意見が少ない結果になった．

管理担当学生で会合を開き，互いに文書に対しての意見を交換する方法がより多くの意見が出るはずであるし，全員が納得できるセキュリティポリシーを効率良く定めることができる．管理枠組の確立の過程では，話し合いによる決定の方が効果的である．

4.1.6 ISMS ドキュメンテーション作成・運用

- ISMS ドキュメンテーション (マニュアル)

  ISMS を確立する作業において完成した文書，リスクアセスメントとリスク管理によっ

て得られた対策の具体的な手順書，そして管理目的及び管理策選択で選択した管理策の具体的な手順書を作成する．マニュアルの作成である．これについてはまだ完成しておらず，作成にあたっては，専門的な知識を有する人の意見が必要となってくる．

- 運用

  ISMS ドキュメンテーションが完成していないので，一般作業，実行，文書管理，記録といった運用の面での作業もまだ実行していない．運用の過程は重要である．運用していく上で次のような問題が発生することも予測される．

  - セキュリティ対策の手順が追い付かない
  - 文書に矛盾点がある
  - 違反者が続出する
  - セキュリティホールが発見される
  - 新しい脅威が発見される

  よって，運用時には定期的に期間を定めてレビューを行い，ISMS ドキュメントに修正を加え，矛盾点，問題点を解決していくことが必要である．この点を考慮して運用を行わなければならない．

4.2 考察

BS7799 を菊池研究室で検証した結果について考察する．

4.2.1 BS7799 の利点，欠点

菊池研究室で BS7799 の導入を試みた結果の利点及び欠点を記述する．

まず利点を述べる．セキュリティポリシーの策定により，研究室のセキュリティ対策に対する欠点やセキュリティ対策に対する取り組み方を明確にすることができる．これは，定めたセキュリティポリシーに対してマニュアル作成や運用・管理が可能かどうか考察することで，より明確になる．

次に欠点を述べる．まず，BS7799 導入によって人的コストがかかることが予測される．策定したセキュリティポリシーより，マニュアル作成や管理・運用が可能であるか考察した結果，セキュリティポリシーにはほとんど問題点があった．全体的に問題点をまとめると，コストがかかるという問題が多い．

次の欠点として，セキュリティのレベルを上げるために無理なセキュリティポリシーを策定しても，必ずレベルの高いセキュリティ対策ができるとは限らないことである．組織よりレベルの高いセキュリティポリシーを策定すると，それだけ運用・管理が困難になる．

最後の欠点として，BS7799 では情報セキュリティ管理システムの具体的な手順が詳細まで定められていないことである．これは，組織に特定せず BS7799 を導入することができるという，BS7799 の利点として挙げられている部分である．しかしこの利点によって，セキュリティポリシーの策定方法や，リスクアセスメントの方法の詳細が分からず，人的にも時間的にもコストがかかってしまう結果となってしまった．

4.2.2 検証のまとめ

菊池研究室で BS7799 を導入することは，利点より欠点の方が多くなるという結果となった．よって，BS7799 の導入は菊池研究室には向いていない．

欠点の解決策として，ポリシーの策定やリスクへの対策そして管理目的及び管理策を定める際，実際にこれらの決定事項に沿って，運用・管理を行うことが可能であるかを考察することが必要である．そしてその考察に沿ってポリシーなどを組織に合ったレベルに定める．そうすることによって，無理にコストがかかることを防ぎ，管理・運用でポリシーと大きな相違が現れる可能性を削減できる．この解決策を実行するにはコストがかかるが，実行する価値は充分ある．

そして BS7799 の検証にあたって一番の反省点は，実際に管理・運用にまで追い付かなかったことである．実際に管理・運用していないので，作成したドキュメント通りに管理・運用できるか，本当に考察と同じ結果になるのか，そして他の規格を導入するよりも良いセキュリティ対策ができるのかを検証することができなかった．

第 5 章

まとめ

本研究では，セキュリティポリシーの策定手法を検証した．菊池研究室で BS7799 の導入を試みることにより，組織でセキュリティポリシーを策定することによる利点・欠点を考えた．そしてこの章で結果を記述する．

5.1 まとめ

BS7799 の導入は，研究室のような小規模の組織には向いていないと結論する．

BS7799 の導入には人的・時間的なコストがかかり，小規模な組織では，コストに比較して得られるセキュリティ強度が小さすぎる．コストよりも大きいセキュリティ強度を得るためには，セキュリティ対策に人員・時間を割くことのできる，ある程度大規模の組織である必要がある．

そして，BS7799 を導入する際に注意すべき点は，正確な，そして組織のレベルに沿ったセキュリティポリシーの策定を行うことである．レベルの高いセキュリティ対策を意識するあまり無理なセキュリティポリシーを策定してしまうと，管理・運用が追い付かなくなる．その結果，逆にセキュリティホールが増えてしまったり，情報セキュリティ対策にばかりコストがかかってしまうという結果になる．セキュリティポリシーを定める際は，実際にそのセキュリティポリシー通りに管理・運用できるかを考察して確認して定めるべきである．

5.2　今後の課題

本研究の今後の課題は，まず本研究を最後まで実行することである．管理枠組の確立で作成した文書から ISMS ドキュメントを完成させ，運用を実現し，その上でもう一度 BS7799 そしてセキュリティポリシーの策定手法の検証を行いたい．

その後、セキュリティポリシーを採用した他の規格を導入して BS7799 と比較したい．そうすれば BS7799 の利点・欠点がより明らかになると考える．よって，ISO15408 や GMITS，またはこれから策定されるかもしれない新しい規格を実際に菊池研究室に導入して，比較することが必要であると思う．

次の課題は，コストに見合ったセキュリティ対策が実現可能になる組織の大きさを調査することである．コストに見合ったセキュリティ対策は，大企業で実行可能であることは予測できる．しかし，どの規模の企業から可能になるかは不明である．よって，数十人規模の IT 関連企業で BS7799 の導入を試みたい．

そして，研究室程度の小さい規模の組織でも，コストよりセキュリティ効果の方が大きくなるようなセキュリティポリシーの策定手法を考えたい．

謝辞

菊池 豊助教授，本研究及び資料作成の指導や参考文献の紹介をしていただき，ありがとうございました．

正岡くん，情報セキュリティについていろいろ教えてもらい，そして参考文献を貸してくれてありがとう．

菊池研究室の角谷くん，最高の文献を紹介してくれてありがとう．

菊池研究室の杉山さん，いつもはげましてくれて本当にありがとう．

菊池研究室の田渕さん，アンケートへの回答ありがとう．そしていつもお勧め食糧をくれて感謝です．

菊池研究室の長尾さん，つらいとき，いつも元気をもらってました．本当にありがとう．

菊池研究室の西内くん，アンケートへの回答ありがとう．BGM もたくさん紹介してくれて感謝しています．

菊池研究室の広瀬くん，アンケートへの回答や，トラブルが発生したときに助けてくれてありがとう．

菊池研究室の舟橋くん，アンケートへの回答ありがとう．そしておみやげおいしかったです．

菊池研究室の３年生のみなさん，いつも応援してくれてありがとう．

ラック研究室の浜田さん，休憩や朝御飯にいつも誘ってくれてありがとう．

参考文献

[1] 山口英, 鈴木裕信. 情報セキュリティ. 共立出版, 1 2000.

[2] (財) 日本規格協会海外規格課（編）. 情報セキュリティ管理 英和対訳版. 英国規格協会, 1999.

[3] 三輪信雄. セキュリティポリシーでネットビジネスに勝つ. NTT 出版, 6 2000.

[4] 日本インターネット協会. インターネット白書 2000. 株式会社 インプレス, 6 2000.

付録 A

管理枠組の確立の結果

管理枠組の確立を行い，作成した文書を研究室の管理担当学生に提示し，それに対する個人々々の意見及び提案をまとめたものを記述する．

A.1　情報セキュリティポリシー

1. 情報セキュリティの定義

   「情報の機密性，完全性及び利用の可能性の維持」

   詳細は 2.4.1 参照.

2. 情報セキュリティの目的

   研究室の損害を最小限に抑え、研究の継続性を確実にするために，研究室生全員が協力して広範囲にわたる脅威から情報を保護する．

3. 適用範囲

   情報セキュリティ対策を取り入れる範囲は，基本的には菊池研究室とする．財産的な範囲として，研究室内で共有している情報，研究室の研究に関係する全ての情報を，情報セキュリティ管理システムの適用範囲とする．

   そして，研究室内の者全員にこのシステムを適用することとする．

4. 情報共有を可能にするための機構としてのセキュリティの重要性

   研究室の情報や，その情報を扱うシステムやネットワーク，そして情報を扱う際のプロセスなどは，研究室にとって重要な財産である．その財産を保護するため，研究室全体で情報セキュリティに真剣に取り組むことによって，研究室の財産は保護され，研究室

という組織が成立する．誰か一人でもそれに違反する者が現れた場合は，研究室が重大な危機に陥る可能性が出てくる．

5. 意向声明書

研究室生全員がセキュリティポリシーに従い，責任を持って研究室の情報資産を保護していくものとする．

6. 研究室にとって重要なセキュリティポリシー，原則，規格及び準拠要求事項

- 本ドキュメントに準拠すること．
- 本ドキュメントは，定められた手順に従い，定期的にレビューされること．
- ポリシーに変更・追加があった場合は，研究室内の学生全員に知らされること．
- 新しいソフトウェア導入の際は，定められた手順に従い，厳密に協議されること．
- 入退室管理を厳密に行うこと．
- 法律的な違反のチェックが定期的に行われること．
- ネットワーク事故及びセキュリティホールが発見された場合の対処が，定められた手順に沿って速やかに行われること．
- セキュリティの技術的な面は，専門的知識を有する研究生，又は教員によって講義が行われ，教育されること．
- セキュリティポリシーに違反する行為が見られた場合，直ちに協議され，それに沿った処罰が与えられること．

7. セキュリティ管理の一般的及び特定責任の定義

一般的には研究生個人が各研究の情報，個人の情報を責任を持って保護すること．セキュリティ事故の報告も責任の範囲とする．

8. その他の参照書類

特になし．

A.2 ISMS の範囲

情報セキュリティ対策を取り入れる範囲は，基本的には菊池研究室とする．財産的な範囲として，研究室内で共有している情報，研究室の研究に関係する全ての情報を，情報セキュリティ管理システムの適用範囲とする．

A.3 リスクアセスメント

BS7799 の定義から引用すると，リスクアセスメントとは,「情報及び情報処理施設／設備に対する脅威，それらへの影響及びそれらのバルネラビティ並びにそれらが起こる可能性の評価」である．

まず，リスクアセスメントを行うにあたって，研究室の管理担当者に対して，研究室で保護すべき情報のアンケートをとった．その結果としては，個人情報，メール，研究のデータ，研究室のネットワークの情報 (ネットワークの構成，経路など) などが挙げられていた．

リスクアセスメントで明らかにする項目は，財産に対する脅威，組織に及ぼす影響，リスクの度合の 3 項目である．見やすいように，外部からの脅威，内部の脅威、その他の 3 つに分類して考えた．リスクの度合は，大が最も被害が大きいことを表し、中、小と順に被害が小さくなっていくことを表す．

- 外部からの脅威

  考え得る外部からの脅威を表 A.1 に示す．ここでは主に，情報の喪失，漏洩に関する脅威なので，その情報の重要さの度合によってリスクの度合が異なる．

- 内部の脅威

  考え得る内部の脅威を，表 A.2 に示す．情報の喪失，漏洩については，ここでも情報の重要度によってリスクの度合が変わってくる。

- その他の脅威

  考え得るその他の脅威を，表 A.3 に示す．ここでは，災害の大きさ，喪失する情報の大切さによってリスクの度合は変わってくる．

表 A.1　外部からの脅威

脅威	影響	度合い
データの持ち出し，破壊，改ざん，盗聴	データ喪失，情報漏洩など	中
不正アクセス	データ喪失，情報漏洩など	中
コンピュータウィルス	データ喪失，信用喪失など	大
物質破損	データ喪失，金銭的損害など	中
盗難 (HD，極秘資料など)	データ喪失，金銭的損害など	大

表 A.2　内部の脅威

脅威	影響	度合い
データの持ち出し，破壊，改ざん，盗聴	データ喪失，情報漏洩など	中
研究室外に対して不正アクセス	信用喪失，違法責任負担など	大
資源の個人的使用	ネットワーク負荷，資源の浪費など	中
情報を口外する	情報漏洩など	大
物質破損	データ喪失，金銭的損害など	中
盗難 (HD，極秘資料など)	データ喪失，金銭的損害など	大

表 A.3　その他の脅威

脅威	影響	度合い
災害 (火災，水害，地震等)	データ喪失，金銭的損害など	大

A.4　リスク管理

リスクアセスメントで考えられた脅威に対しての対策を考え，その対策について保証できる度合を求める．詳細の手順は，後の段階である ISMS ドキュメンテーションの過程の際に定める．保証の度合は，大が最も対策が効果的であることを表す．

- 外部からの脅威

  考え得る外部からの脅威についての対策を，表 A.4 に示す．外部からの脅威に対する対策は，ファイアウォール，暗号化，認証技術の強化，ログやバックアップを取ることによってある程度脅威から情報を保護することができる．

表 A.4　外部からの脅威への対策

脅威	対策	保証の度合
データの持ち出し，破壊，改ざん，盗聴	ファイアウォール，暗号化，認証技術強化 ログ取り，バックアップなど	中
不正アクセス	ファイアウォール，暗号化 認証技術強化，ログ取りなど	中
コンピュータウィルス	コンピュータウィルス対策ソフトなど	中
物質破損	施錠，警備強化など	大
盗難 (HD，極秘資料など)	施錠，警備強化など	大

- 内部の脅威への対策

  考え得る内部の脅威についての対策を，表 A.5 に示す．ファイアウォールや暗号化など技術的な対策は，外部への対策と同じである．しかし内部の脅威について，情報漏洩や盗難などに関しては，組織の者に「してはいけない理由」を理解させることが必要である．

- その他の脅威

  考え得るその他の脅威についての対策を，表 A.6 に示す．災害の大きさによっては，全

表 A.5　内部の脅威

脅威	対策	保証の度合
データの持ち出し，破壊，改ざん，盗聴	ファイアウォール，暗号化，認証技術強化 ログ取り，バックアップなど	小
研究室外に対して不正アクセス	ファイアウォール ログ取り，説得など	小
資源の個人的使用	チェック，説得など	小
情報を口外する	説得など	小
物質破損	厳重警戒など	中
盗難 (HD，極秘資料など)	説得など	小

ての財産を失うことも考えられる．

表 A.6　その他の脅威の対策

脅威	対策	保証の度合
災害 (火災，水害，地震等)	警備強化，バックアップなど	大〜小

A.5　管理目的及び管理策

管理目的及び管理策は，BS7799 の第 1 部から選択する．BS7799 に記述されている内容は理解しにくいので，選択した内容を菊池研究室用に要約した．BS7799 に示されている文章は，もっと詳細の点まで記述されている．全部で 36 項目あるが，ここでは一部である 11 項目を掲載する．

- 情報セキュリティの基盤

  目的：研究室内において情報セキュリティを管理すること．

情報セキュリティポリシーを承認し，セキュリティの役割を割り当て，研究室全体のセキュリティの実施を調整するために，管理担当者を指導者とする会合が開かれることとする．

– 会合

情報セキュリティとは，研究室の全メンバーによって共有される事業上の責任である．従って，セキュリティの提案のための明瞭な指示及び管理担当者による支持のための会合を開くこと．

– 情報セキュリティ責任の割り当て

個々の財産に対する責任，並びに具体的なセキュリティ対策の実施過程に対する責任は，明確に定めなければならない．

セキュリティポリシーには、研究室内のセキュリティの役割及び責任の割り当てを記述すること。

– 情報処理施設/設備の認可プロセス

新しい情報処理施設/設備に対する，管理担当者に認可される過程を決定する．

– 専門家によるセキュリティ助言

専門家によるセキュリティ助言は，情報セキュリティアドバイザによって行われること．情報セキュリティアドバイザは，研究室内で情報セキュリティの経験を積んだ者が任命されることとする．

– 組織間の協力

セキュリティ事故が起きた場合，適切な処置が素早く取られ，適切な助言を得るために，法律施行者，規制機関，情報サービス供給者及び通信オペレータ等との適切な連絡が維持されるべきである．

– 情報セキュリティの独立レビュー

情報セキュリティポリシー文書には，情報セキュリティのポリシー及び責任が記述される．組織による実行がポリシーに反映し，実行可能であるということを保証するために，情報セキュリティポリシーを独立してレビューする必要がある．情報セ

キュリティポリシーを独立してレビューすることによって，定めたセキュリティポリシーがISMSドキュメンテーションや管理・運用に反映しているかどうかを調べることができる．

- 財産に対する責任

  目的：組織の財産の適切な保護を維持すること．

  全ての主要な情報財産は，その価値が明らかにされ，所有者が決定していなければならない．全ての主要な財産に対して所有者を明確にすることが望ましく，適切な管理策を維持する責任を割り当てなければならない．

  – 財産目録

    各情報システムに関わる重要な財産について目録を作成し，維持しなければならない．各財産は明確に識別され，その所有権及びセキュリティの分類は協議により決定され，その現在の場所とともに文書に記述されること．

- 情報の分類

  目的：情報財産が適切なレベルの保護を確実に受けられるようにすること．

  情報は，保護の必要生，優先順位及び保護の程度を決定するために分類すること．ここで注意することは，情報は必ずしも常に一定の重要レベルではないということである．例えばポリシーなどの変化に沿って情報財産のレベルが変化することなども考えられる．

- 研究室学生の訓練

  目的：研究室生が，情報セキュリティの脅威及び懸念を理解し，その通常の作業において，研究室のセキュリティポリシーを支持する体勢が確実に取れるようにすること．

  起こり得るセキュリティリスクを最小限に抑えるため，研究室学生は，セキュリティ手順及び情報処理施設／設備の正しい使用について訓練を受けなければならない．

- 安全領域

  目的：研究用敷地及び情報への認可されていないアクセス，損傷および妨害を防止する．

  重要な，又は取り扱いに慎重を要する情報処理施設／設備は，安全な領域に設置され，

保護されること.

– 物理的セキュリティ外壁

事業敷地及びに情報処理施設／設備の周りにいくつかの物理的バリアを設けることによって，物理的保護が行われる．例えば，壁，カード制御，係による受け付けなどを設けるなどである.

- 運用手順及び責任

目的：情報処理施設／設備の正しく安全な運用を確実にすること.

全ての情報処理施設／設備の管理及び運用の責任及び手順を確立しなければならない.

– 操作手順書

セキュリティポリシーによって明確にされた操作手順書は文書化し，維持されること．操作手順は，正式な文書として取り扱い，変更は管理担当者によって認可される.

– 運用変更管理

情報処理施設／設備及びシステムの変更は管理されなければならない.

– 事故管理手順

セキュリティ事故に対して，迅速，効果的かつ整然とした対処を確実に行うことができるように事故管理の責任及び手順を確立しなければならない.

– 外部施設の管理

情報処理施設／設備の管理を研究室外の者に依頼する場合は，データの損傷又は消失等を引き起こす可能性がある．これらのリスクはあらかじめ明らかにし，管理担当者の同意を得て，適切な管理策を契約に組み入れられなければならない.

- ネットワークの管理

目的：ネットワークにおける情報の安全防護.

コンピュータ・ネットワークでは，セキュリティを達成，維持するために，一連の管理策が要求される．ネットワーク・マネージャは，ネットワークにおけるデータを保護し，接続されているサービスを認可されていないアクセスから確実に保護するために，

管理策を実行しなければならない.

- ユーザアクセス管理

  目的：情報システムへの認可されていないアクセスを防止すること.

  情報システム及びサービスへのアクセス権の割り当てのための正式な手順があること.

  – ユーザ登録

    全てのマルチユーザ情報システム及びサービスについて，それらへのアクセスを許可するための，正式なユーザ登録及び登録抹消手順があること.

  – ユーザパスワードの管理

    パスワードは，情報システム又はサービスにアクセスするユーザ ID を確認する一般的な手段である．パスワードの割り当ては，正式な管理プロセスによって管理されなければならない.

  – ユーザアクセス権のレビュー

    データ及び情報サービスへのアクセスを有効に制御するため，管理担当者は，定期的に手順を実施して，ユーザのアクセス権をレビューしなければならない.

- 暗号による管理策

  目的：情報の機密性，真証性又は完全性を保護すること.

  – 暗号による管理策の使用についてのポリシー

    暗号ソリューションを用いることが適切であるかどうかの判定は，リスクアセスメント及び管理策の選択のための過程の一部と見ることが望ましい.

  – 暗号化

    暗号化は，情報の機密性を保護するために用いることができる暗号手法である．保護するレベルは，リスクアセスメントに基づき，使用される暗号化アルゴリズムのタイプ及び質，並びに使用すべき暗号キーの長さを考慮に入れなければならない.

  – デジタル署名

    デジタル署名は，電子文書の真正性及び完全性を保護する手段である．これは，電子的に処理される文書なら何にでも適用できる．使用にあたっては，私用キーの機

密性を保護し，公用キーの完全性を保護しなければならない．

- 研究継続管理

  目的：研究活動に対する障害に対処し，重大な故障や災害から重要な研究過程を保護すること．

  – 研究継続管理プロセス

    研究室全体の研究継続のための管理されたプロセスが整っていること．まず，研究過程によって起こることが考え得る障害を明らかにし，それに対する対策手順を考え，研究継続計画を作成する．そしてそれは，定期的に試験され，維持されるために再評価されるべきである．

- 法的要求事項への準拠

  目的：掲示及び民事法，制定法，規制又は契約上の義務，並びにセキュリティ上の要求事項の違反を避ける．

  – 知的所有権

    著作権，意匠権又は商標など，知的所有権がある物件について，法的制限事項に確実に準拠するように，適切な手順を実行すること．

    所有権があるソフトウェア製品は，通常，使用許諾契約を条件として支給されるが，この使用許諾契約では，製品の使用は指定の機械のみに限定され，コピーは，バックアップコピーの作成のみに限定されることがあるので，それに沿った管理策を考慮しなければならない．

A.6　適宜宣言書

管理目的及び管理策選択の 11 項目に対しての適宜宣言書を作成した．

- 情報セキュリティの基盤

  情報セキュリティの基盤を作ることによって，情報セキュリティ対策について研究室全体で取り組む体制を確立するため．これによって，研究室の情報セキュリティが維持さ

れる．この項目は最も重要であり，必ず守られなければならない．

- 財産に対する責任

  財産に対する価値，そしてそれに対する所有者及び責任を決定することにより，それぞれの財産を保護する有効性を高めるため．担当責任を明確に定め，それぞれが責任を持って担当財産を管理するので，それによって研究室内で保護されていない財産が現れるというセキュリティホールを消滅させる．

- 情報の分類

  情報を重要度のレベルに分類することにより，どの場所にどの程度情報セキュリティ対策を取り入れるかを明らかにするため．

- 研究室生の訓練

  研究室生にセキュリティ対策について理解させ、訓練することにより，一部の者だけで対策が行われるというような労力の偏りを防ぎ，研究室全体で情報セキュリティ対策に取り組むため。この訓練がないと，研究室内で違反者が現れる可能性が高くなる上，違反者が現れたときに対処できる者も一部の者に制限されてしまう．このような脅威を防ぐため．

- 安全領域

  安全領域を設置することにより，特に重要な物や情報をあらゆる脅威から厳重に保護するため．

- 運用手順及び責任

  運用手順，そしてそれに対する責任を決定することにより，考え得る全ての対策に対する運用手順が定められ，その全ての手順が確実に実行されるようにするため．

- ネットワークの管理

  ネットワークを管理することにより、不正アクセス、過剰負荷などを防ぎ，安全な研究を可能にするため。

- ユーザアクセス管理

  ユーザアクセスを管理することにより，不正アクセスなどを防ぐため．

- 暗号による管理策

  暗号を使用することにより、情報の盗聴、漏洩，改ざんなどを防ぐため．そして，デジタル署名によって，研究室の情報の正当性を証明するため．

- 研究継続管理

  研究継続管理計画書を作成することにより，研究継続の管理が確実に行われ，研究室の継続の可能性を高めるため．

- 準拠

  違反，規制などを明瞭にし，違反しているという自覚のない違反者が現れることを防ぎ，同時に自覚のある違反者を減少させるため．