平成 13 年度

学士学位論文

セキュリティポリシー策定方法の実地例に基づいた検証

A study of the planning method of BS7799 security policy framework

1020289　　澤田明美

指導教員　　菊池 豊

2002 年 2 月 8 日

高知工科大学 情報システム工学科

要 旨

セキュリティポリシー策定方法の実地例に基づいた検証

澤田明美

近年、多様化しているネットワーク犯罪には、技術的なセキュリティ対策だけでは不十分である。それを受けて、企業などの組織は、組織的なセキュリティ対策の手段としてセキュリティポリシーに注目している。

しかし、現状では実際にセキュリティポリシー策定を行なっている組織は少なく、特に大学などの学術組織では皆無に近い。

そこで、セキュリティポリシーの策定を基盤としたセキュリティ規格 BS7799 を情報システム工学科に試行し、検証を行った。本研究では、組織的なセキュリティ対策の骨組みとなる文書を作成した。その過程で、情報システム工学科は組織的なセキュリティ対策が不十分であるということが明らかになった。このことにより、BS7799 の導入を視野に入れて、情報セキュリティ管理システムを構築していけば、最終的に組織的なセキュリティ対策を行なえるということを示した。また、本研究では運用までにはいたらなかったが、本研究で策定した管理枠組を見直しすることによって、より情報システム工学科に適応した情報セキュリティ管理システムとなる。

キーワード　BS7799, セキュリティポリシー, 検証

Abstract

A study of the planning method of BS7799 security policy framework

SAWATA Akemi

In recent years, in order to prevent a diversified network crime, just the technical security measure is inadequate. The organization is observing security policy as a means of the systematic security measure.

However, there are few organizations which are actually performing security policy decision, and they are especially near in scientific organizations, such as a university.

Then, it verified by trying the security standard BS7799 security policy framework to the department of information system engineering. In this research, the document used as the framework of the systematic security measure was drawn up. In the process, it became clear that the department of information system engineering has a systematic inadequate security measure. BS7799 into the view and constructing the information security management system by this, it was shown that the systematic security measure can finally be performed. It did not result by employment in this research, it becomes the information security management system which was more adapted for the department of information system engineering by looking over again the management framework upon which it decided by this research.

key words BS7799,security policy,verified

目次

図目次

表目次

第 1 章

はじめに

はじめに、近年のインターネット普及の背景や多様化するネットワーク犯罪について述べる。

1.1 背景

近年、パソコンのめまぐるしい発達により、電子メールや WWW の閲覧はもちろんのこと、インターネットショッピングや電子商取引も普及し始めている。今やコミュニケーションや情報収集の手段としてインターネットが、ビジネスや私達の生活に欠かせないものになってきている。

その一方で、インターネットは、世界中の人と繋がっており、解放的なネットワークである。そのため、国境を越えた不正アクセスや、コンピュータウィルスなどのネットワーク犯罪が問題になってきている。最近、日本でも官庁 HP 書き換え事件が起こり、日本のセキュリティ意識の低さと、ネットワーク犯罪が身近なものであるという認識が高まった。以前から日本には、不正アクセスを取り締まる法律がないことが問題になっていた。しかし、この事件をきっかけに、2000 年 2 月 13 日に「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） が施行され、少しずつではあるが国内でも情報セキュリティに対する関心が高まってきている。

1.2 ネットワーク犯罪の種類

ここでは、増加し多様化するネットワーク犯罪について述べる。

盗聴

インターネット環境に設置されたサーバ上のデータを不正にアクセスして盗み見る。

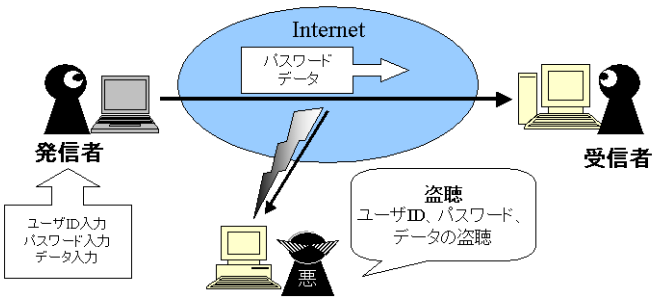

図 1.1　盗聴

改ざん

インターネット環境に設置しているサーバ上のデータを不正にアクセスして、データの内容を書き換える。

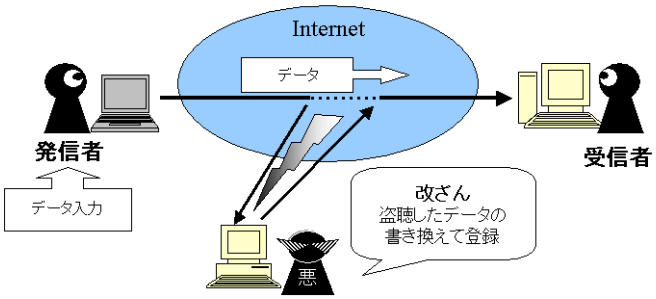

図 1.2　改ざん

なりすまし

インターネット環境で提供されているサービスを他人の ID や権限を使って利用する。

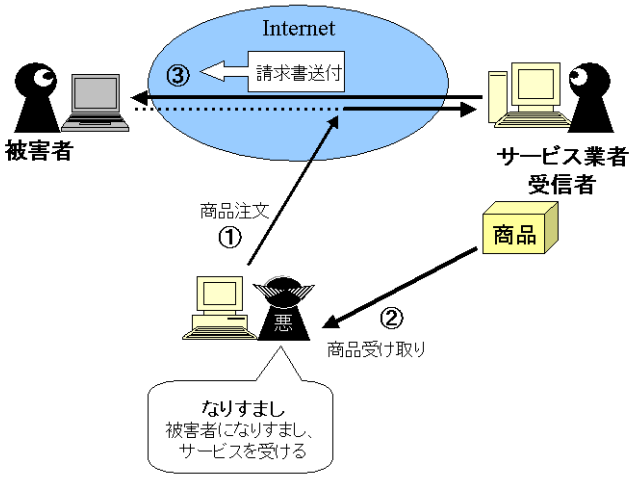

図 1.3　なりすまし

コンピュータウィルス

インターネット環境に設置されたサーバ上にウィルス感染したデータを送り込み、何らかの方法を使って感染させる。

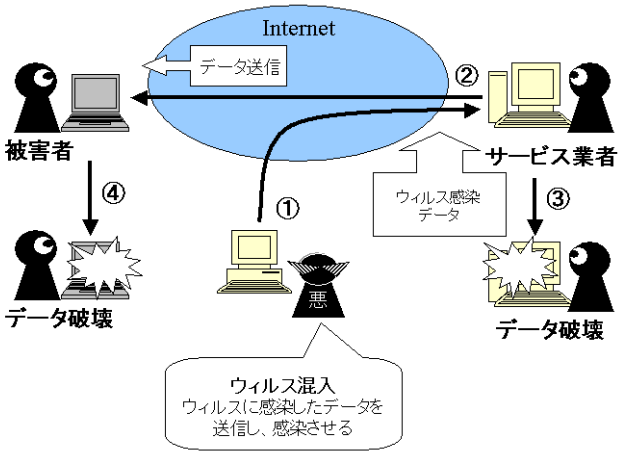

図 1.4　コンピュータウィルス

DoS 攻撃

インターネット環境に設置されたサービスを提供するサーバに一方的にパケットを送り込み、サーバ負荷を増大させサービスをダウンさせる。最近注目されているものに、踏み台にした複数のサーバから一斉に DoS 攻撃を仕掛ける DDoS 攻撃という手法もある。図 1.5 と図 1.6 に示す [1]。

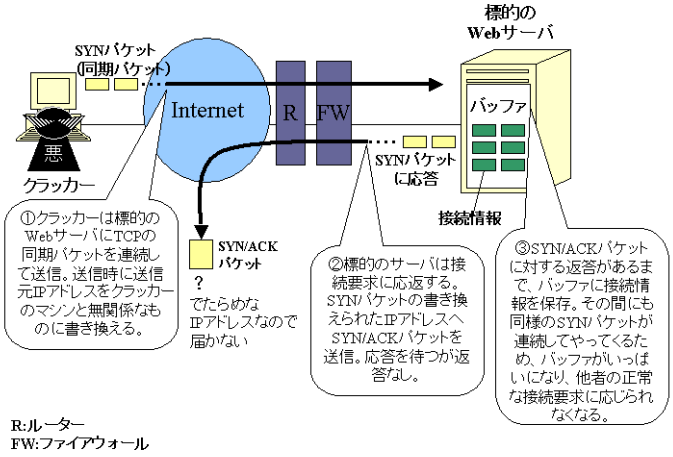

図 1.5　dos 攻撃 (TCP SYN flood の場合)

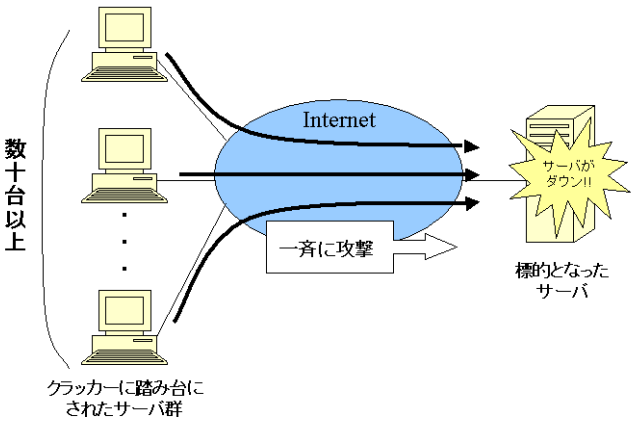

図 1.6　ddos 攻撃

1.2.1　ソーシャルエンジニアリング

1.2 では、技術的な手口のネットワーク犯罪について述べてきた。1.2.1 では、技術的なセキュリティ対策の隙をつくネットワーク犯罪であるソーシャルエンジニアリングについて述べる。

ソーシャルエンジニアリングとは、クラッキングに必要な情報へのアクセス権を持つ者をだまし、パスワードなどの機密情報を取得する詐欺の手口のことである。ソーシャルエンジニアリングは、組織へクラッキングを行う際のパスワード解析を効果的に行うための情報収集の手段に用いられることが多い。

ソーシャルエンジニアリングの手口は非常に多岐にわたっている。また、それらの手口を様々な形で組み合わせて臨機応変に適用する。様々な手口の中で、主なものを次に述べる。

- トラッシング

  ゴミとして廃棄された物の中から、目的の情報を取得する方法のこと。
- 構内侵入

  実際に、クラッキング対象の建物内に侵入する行為のこと。
- 覗き見

  構内侵入の後、パスワードなどの必要な情報が露見しているところをみつけて見ること。
- なりすまし

  他人になりすまして、構内侵入したり、情報を引き出したり、変更させたりすること。

  なりすましの手段には、電話、手紙、メール、Web、変装がある。

ソーシャルエンジニアリングは、人の心理、行動の弱点をつく詐欺であるため、ファイアウォール、暗号化など、どんな技術的なセキュリティ対策をしていたとしても効果がない。技術的なセキュリティ対策だけでなく、組織員のセキュリティ意識を高め、ソーシャルエンジニアリングのような詐欺の被害にあわないようにすることが必要となる。

本節ではネットワーク犯罪の参考資料として [2] を用いた。

1.3　組織的なセキュリティ対策の必要性

本節では、様々な情報セキュリティ技術についての説明と、組織的なセキュリティ対策の必要性について述べる。

情報セキュリティの定義

定義としては、情報に関する脅威に対し、不安と危険のない安全な状態を維持することである。また、機密性、保全性、可用性の 3 大要件を確保することともいえる [5]。

情報セキュリティ技術

一般的に、企業や組織などに導入されているセキュリティ技術には様々なものがある。主なものを次にあげる。

- ファイアウォール

  FireWall（防火壁）のことで、ネットワークとネットワークの間に存在し、あらかじめ設定されたルールに基づいてそれぞれのネットワーク間での中継を許可したり、許可しなかったりパケットを判断するものである [5]。
- コンピュータウィルス対策ツール

  コンピュータウィルスの存在を検知し通知するものや、一度ウィルスに感染したマシンにワクチンプログラムを使用することによって修復するものがある。
- 侵入検知システム

  不正アクセスや DoS 攻撃を検出するためのデータベースを持っていて、ネットワークやホストの状態をリアルタイムに監視することにより、不正アクセスやあらかじめ設定されたルールに基づく事象を発見し、様々な形で通知するもの [5]。
- 通信データの暗号化

  送信者は、通信データを暗号化し、第 3 者から見ても意味のわからない内容にして相

手に送る。受信者は、決められたルールに従い復号して解読する。暗号化の方法には、共通鍵暗号方式や公開鍵暗号方式がある。

1.3.1　組織的なセキュリティ対策

上記で述べた幾つかのセキュリティ技術を次々に導入するというのも、セキュリティ対策の 1 つの手段である。しかし、その方法は、コストがかかる上、多様化するネットワーク犯罪全てに対処できるとは限らない。セキュリティ技術を導入していても、1.2.1 で述べたソーシャルエンジニアリングのような人間の心理や行動の隙をついてくるような犯罪には意味がない。また、ネットワーク犯罪は、セキュリティ対策の甘い組織を踏み台にする傾向にある。組織的なセキュリティ対策が行なえてないと、自組織だけでなくコミュニティ全体の脆弱性につながる。よってセキュリティ教育を行ない個人のセキュリティ意識を高めたり、組織でセキュリティの規定を決めたりといった組織ぐるみの対策が必要となる。

我々は、組織的なセキュリティ対策の手段としてセキュリティポリシーに注目してきた [3]。セキュリティポリシー対する世間の認識が薄いため策定のノウハウは不足している。そこで、本研究ではセキュリティポリシー策定方法の検証を行なうことを目的とした。また、警視庁が 2000 年に実施した不正アクセス対策に関するアンケート調査[*1]によると、大学の過去 1 年間の不正アクセスの被害率は 5 割を越えている。しかし、セキュリティポリシー策定を行なっている大学は、10.2 %と少ない。このことをふまえ検証方法として、情報システム工学科を対象にセキュリティポリシーを基盤とした管理枠組を、セキュリティ規格 BS7799 をもとに作成した。管理枠組とは、セキュリティ対策の骨組みである。評価基準としては、学術組織でうまく機能するかどうかに定めた。

次章では、本研究で用いるセキュリティ規格 BS7799 について詳しく述べる。

[*1] http://www.npa.go.jp/hightech/fusei_ac4/

第 2 章

BS7799

本章では、英国規格 BS7799 の概要を情報システム工学科での検証を前提に述べる。

BS7799 とは、情報セキュリティに関する英国規格のことで、情報システム全般を対象とした管理規格である。

BS7799 は、情報セキュリティ対策の指針となるだけでなく、認定機関より準拠性の認定を受けることにより、ISO9000 シリーズや ISO14000 シリーズと同様に組織の社会的な信用を向上させることができる。

BS7799 は、2 部構成となっており、第 1 部が「情報セキュリティ管理実施基準」として、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管理方法がまとめられている。第 2 部では、「情報セキュリティ管理システム仕様」として、第 1 部の補足的な内容であり、情報セキュリティ管理システムとして、BS7799 を実装するための必須事項が書かれている。

2.1 BS7799 管理枠組確立のプロセス

BS7799 では、セキュリティ対策の骨組みとなる管理枠組を確立し、維持しなければならないとしている [4]。管理枠組確立のプロセスについては、図 2.1 参照。

まず、組織で BS7799 導入の決定が行われたら、リスクアセスメントとして、組織のセキュリティ管理の現状を調べリスクを洗い出す。リスク管理として、洗い出されたリスクに対し、評価を行い対策を立てる。次に、リスクアセスメント・リスク管理の結果を考慮し、BS7799 文書に記述されてある管理目的・管理策を自組織に適用できるか判断して選択した

り、組織のニーズに合わせて新しい管理策を設計したりしてセキュリティポリシー文書にする。その時の選択理由もしくは選択しなかった理由を適用宣言書に記述する。セキュリティポリシー文書は、組織のセキュリティ管理の方針・規定として活用し、適用宣言書は、管理策の批評を行った文書として、今後の管理策の見直しに役立てる。

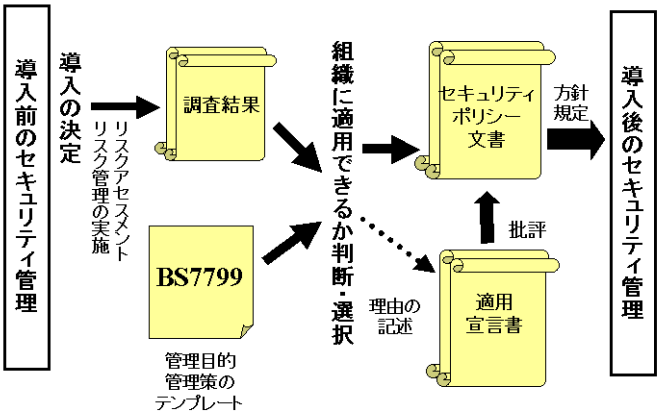

図 2.1　BS7799 管理枠組確立のプロセス

2.2　セキュリティポリシー

本節では、セキュリティ規格 BS7799 の基盤となっているセキュリティポリシーの概要を述べる。

セキュリティポリシーとは、組織全体で取り組むセキュリティ対策を具体的に記述したドキュメントのことである。

BS7799 によるとセキュリティポリシー策定の目的は、情報セキュリティのための経営陣の指導及び支援を規定することとなっている [4]。セキュリティポリシー策定による効果は、個人のセキュリティ意識が高まることによるセキュリティレベルの向上である。

2.2.1　セキュリティポリシー策定の流れ

この節では、セキュリティポリシーを策定するときの一般的な手順について、簡単に述べる [5]。

- 基本方針、体制の確立
  - 目的、範囲、役割分担を明確にする。
  - 成果物を明確にする。
  - 組織全員に承認を得る。

- リスク分析
  - 情報資産、脅威、脆弱性の洗い出しを行う。
  - リスクを評価する。
  - 対策を決定する。

- セキュリティポリシー文書作成
  - リスク分析の結果を参考にしながら、基本ポリシー、スタンダード、プロシージャの 3 層に分けてポリシーを策定していく。
  - 基本ポリシーには、ポリシー全般の運用や作成に対する基本方針を記述する。
  - スタンダードには、組織全体での共通の規定を記述する。
  - プロシージャには、特定の対象者や用途ごとにスタンダードを実行するための具体的な手順を記述する。

- 運用
  - セキュリティポリシー文書を対象者に配布し、承諾を得る。定期的に評価や見直しを行い、必要に応じて改訂する。

第 3 章

情報システム工学科における検証

本章では、前章で述べた BS7799 をもとに管理枠組作成のために実行したプロセスについて述べる。

3.1 実験概要

第 1 章の 1.3 では、組織的なセキュリティ対策の必要性について述べた。本実験は、2001 年 9 月に開始した。実際に学術組織である情報システム工学科で組織的なセキュリティ対策を行うために、セキュリティポリシー策定を基盤としたセキュリティ規格 BS7799 を試行した。この実験の評価基準は、作った管理枠組が情報システム工学科で機能するかということにする。次節からは、実際に管理枠組確立の手順に沿って行ったセキュリティポリシー策定手順を述べる。

3.2 リスクアセスメント

まず、リスクアセスメントとしてリスクの洗い出しを行った。

- 情報資産の洗い出し
  - 情報システム工学科における情報資産は、個人情報と研究内容である。
  - 情報資産のある場所は、各研究室である。
  - 情報資産の状態は、紙媒体、電子媒体である。
- 脅威の洗い出し

– 情報システム工学科における脅威には、外部からの脅威、内部からの脅威、その他の 3 つにわける。外部からの脅威には、悪意をもった者による脅威があてはまる。内部からの脅威には、組織内部の人による過失があげる。その他については、自然災害などが当てはまる。その 3 つの観点から、考えられる全ての脅威を列挙した。
– 33 ページの付録 A.1、A.1、A.1 参照

- 脆弱性の洗い出し
  – 組織的なセキュリティ対策の場合、脆弱性を洗い出す上で欠かすことのできないのが、ユーザの存在である。本研究でユーザにあたるのは、情報システム工学科の学生である。学生のセキュリティ意識がどの程度のレベルであるのかということを把握する必要がある。そこで、情報システム工学科の学生全員を対象に、セキュリティ意識調査のためのアンケートを実施した。
  – アンケート調査の内容を以下に示す。
    1. あなたは、この大学に入学してから今までで、あなたが大学で用いるマシンのパスワードを他人に知らせたことがありますか？
       選択肢 ある、ない
    2. あなたが大学で用いるマシンのパスワードは、以下のどの期間、変更していませんか？
       選択肢 1 ヶ月未満、3 ヶ月未満、6 ヶ月未満、6 ヶ月以上
    3. 個人所有のパソコンを学内に持ち込んだことはありますか？
       選択肢 はい、いいえ
    4. 3 ではいと答えた人は、そのパソコンを学内ネットワークに繋いだことがありますか？選択肢 ある、ない
    5. あなたが学内で用いるマシンに、インターネットからダウンロードしたソフトウェアをインストールしたことがありますか？
       選択肢 ある、ない、わからない

6. 実験室もしくは研究室に、業者と名乗る見ず知らずの人が作業に来ました。その部屋には、あなたしかいません。その人は、担当者の許可をとっていると言っています。あなたは、どうしますか？

   選択肢 すぐに入れる、担当者に確認をとってから入れる、入れない

7. セキュリティに関して意見があれば、教えてください。

– 情報システム工学科の学生全員を対象に実施したセキュリティ意識調査のためのアンケートの結果を表 3.2 から表 3.2 にまとめた。また、わかりやすくするために質問ごとのグラフを図 3.1 から図 3.6 に示した。

– 学生は入学当初に、コンピュータリテラシーの時間を使って、パスワードの機密性についての説明を受けている。しかし、図 3.1 のアンケート結果をみると、パスワードを他人に教えたことのある人が小数派であるが存在していることがわかる。また、学年別にみると研究室に配属になっている 4 年生に一番多く、研究活動におけるパスワードの機密性の重要度からみれば問題である。

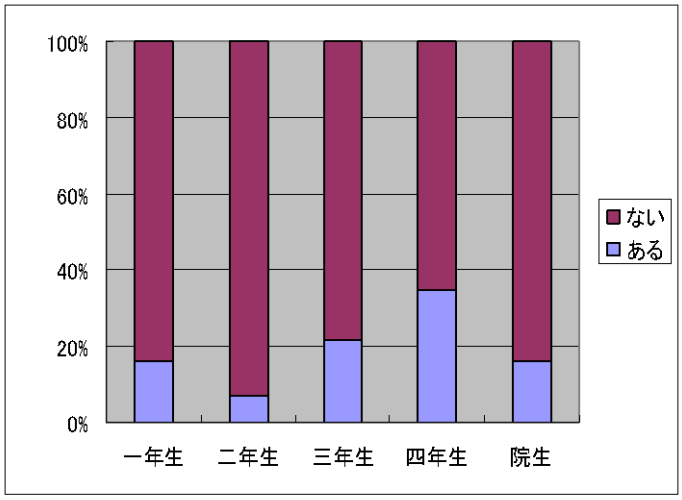

図 3.1　パスワードを他人に教えたことがあるか

– 一般的にパスワードは、定期的に変更したほうがセキュリティ的に安全である。しかし、図 3.2 のアンケート結果をみると情報システム工学科におけるパスワード変更は定期的に変更されているとはいえない。

3.2　リスクアセスメント

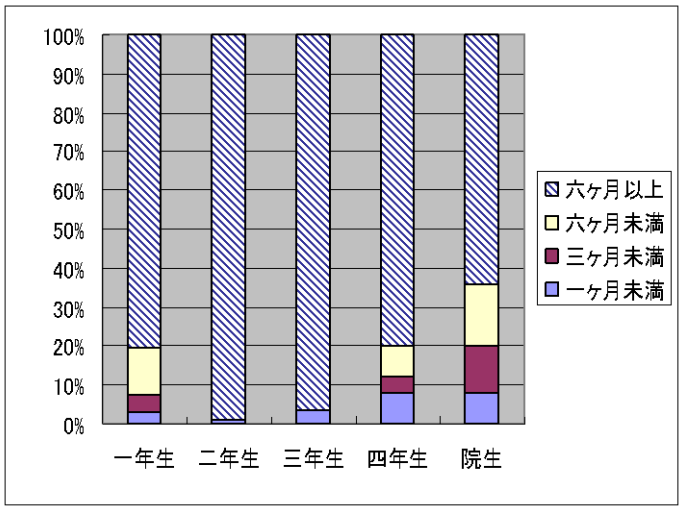

図 3.2　パスワードの変更期間

表 3.1　一年生へのアンケート結果

一年生 92 人				
問 *1.* パスワードを他人に知らせたことがあるか	**ある**		ない	
	15		77	
問 *2.* パスワードを変更していない期間	1 ヶ月未満	3 ヶ月未満	6 ヶ月未満	6 ヶ月以上
	3	4	11	74
問 *3.* 個人所有のパソコンを学内に持ち込んだことがあるか	**ある**		ない	
	38		54	
問 *4.* 個人所有のパソコンを学内ネットワークに繋いだか	**繋いだ**		繋がなかった	
	30		9	
問 *5.* インターネットから, ダウンロードしたソフトウェアをインストールしたことがあるか	ある	ない	**わからない**	
	35	42	14	
問 *6.* 見ず知らずの人を部屋に入れるか	すぐ入れる	**確認してから入れる**		入れない
	33	45		12

表 3.2　二年生へのアンケート結果

二年生 83 人				
問 *1.* パスワードを他人に知らせたことがあるか	**ある**		ない	
	6		77	
問 *2.* パスワードを変更していない期間	1 ヶ月未満	3 ヶ月未満	6 ヶ月未満	6 ヶ月以上
	1	0	0	81
問 *3.* 個人所有のパソコンを学内に持ち込んだことがあるか	**ある**		ない	
	38		42	
問 *4.* 個人所有のパソコンを学内ネットワークに繋いだか	**繋いだ**		繋がなかった	
	32		12	
問 *5.* インターネットから, ダウンロードしたソフトウェアをインストールしたことがあるか	ある	ない	**わからない**	
	21	56	5	
問 *6.* 見ず知らずの人を部屋に入れるか	すぐ入れる	**確認してから入れる**		入れない
	44	29		10

表 3.3　三年生へのアンケート結果

三年生 57 人				
問 *1.* パスワードを他人に知らせたことがあるか	**ある**		ない	
	12		44	
問 *2.* パスワードを変更していない期間	1 ヶ月未満	3 ヶ月未満	6 ヶ月未満	6 ヶ月以上
	2	0	0	55
問 *3.* 個人所有のパソコンを学内に持ち込んだことがあるか	**ある**		ない	
	20		37	
問 *4.* 個人所有のパソコンを学内ネットワークに繋いだか	**繋いだ**		繋がなかった	
	17		7	
問 *5.* インターネットから, ダウンロードしたソフトウェアをインストールしたことがあるか	ある	ない	**わからない**	
	34	20	3	
問 *6.* 見ず知らずの人を部屋に入れるか	すぐ入れる	**確認してから入れる**		入れない
	26	17		14

表 3.4　四年生へのアンケート結果

四年生 49 人				
問 *1.* パスワードを他人に知らせたことがあるか	**ある**		ない	
	17		32	
問 *2.* パスワードを変更していない期間	1 ヶ月未満	3 ヶ月未満	6 ヶ月未満	6 ヶ月以上
	4	2	4	39
問 *3.* 個人所有のパソコンを学内に持ち込んだことがあるか	**ある**		ない	
	23		26	
問 *4.* 個人所有のパソコンを学内ネットワークに繋いだか	**繋いだ**		繋がなかった	
	19		4	
問 *5.* インターネットから, ダウンロードしたソフトウェアをインストールしたことがあるか	ある	ない	**わからない**	
	38	9	2	
問 *6.* 見ず知らずの人を部屋に入れるか	すぐ入れる	**確認してから入れる**		入れない
	26	20		3

表 3.5　院生へのアンケート結果

院生 25 人				
問 *1.* パスワードを他人に知らせたことがあるか	**ある**		ない	
	4		21	
問 *2.* パスワードを変更していない期間	1 ヶ月未満	3 ヶ月未満	6 ヶ月未満	6 ヶ月以上
	2	3	4	16
問 *3.* 個人所有のパソコンを学内に持ち込んだことがあるか	**ある**		ない	
	12		13	
問 *4.* 個人所有のパソコンを学内ネットワークに繋いだか	**繋いだ**		繋がなかった	
	10		1	
問 *5.* インターネットから, ダウンロードしたソフトウェアをインストールしたことがあるか	ある	ない	**わからない**	
	26	20	3	
問 *6.* 見ず知らずの人を部屋に入れるか	すぐ入れる	**確認してから入れる**		入れない
	11	12		1

– 図 3.3 は、学内や、研究室へのパソコンの持ち込みについての質問である。全体的に約 4 割から 5 割の人が個人所有のパソコンを学内もしくは研究室に持ち込んでいるという結果になった。外部から持ち込んだパソコンで研究活動をおこなうことにより、パソコンに機密情報が蓄積する。機密情報を記憶したパソコンを外部で紛失することにより情報漏洩が起こる。

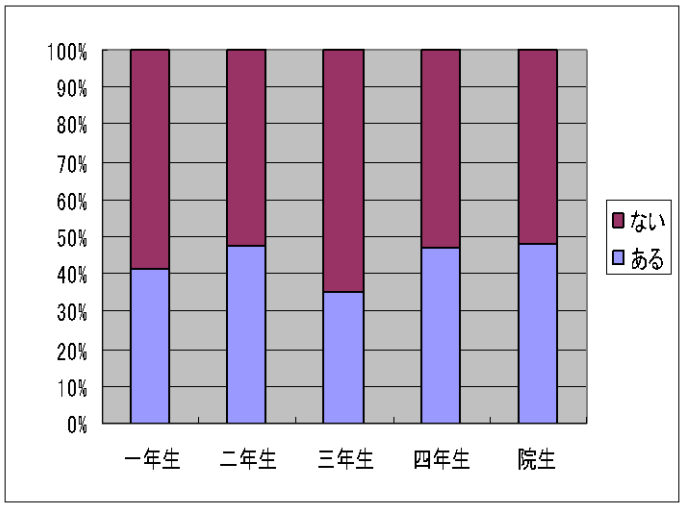

図 3.3　個人所有のパソコンの持ち込み

– 図 3.4 は、個人所有のパソコンを学内もしくは研究室に持ち込んだ人の中で、学内ネットワークに繋いだ人の割合を表したものである。図 3.4 によると、個人所有のパソコンを学内に持ち込んだ場合、ほとんどの人が学内ネットワークへの接続を行なっているという結果になった。利用者、パソコン端末が識別・認証できなければ、アクセスの正当性が確認できない。

– 図 3.5 は、インターネットからダウンロードしたソフトウェアを研究室や実験室で使うマシンにインストールしたことがあるかという質問に対する結果である。図 3.5 によると、4 年生と院生は多くの人がインターネットからダウンロードしたソフトウェアのインストール経験があるということがわかった。インターネットからダウンロードしたソフトウェアは、信頼性が低いためダウンロードする際には信頼性を確認する必要がある。

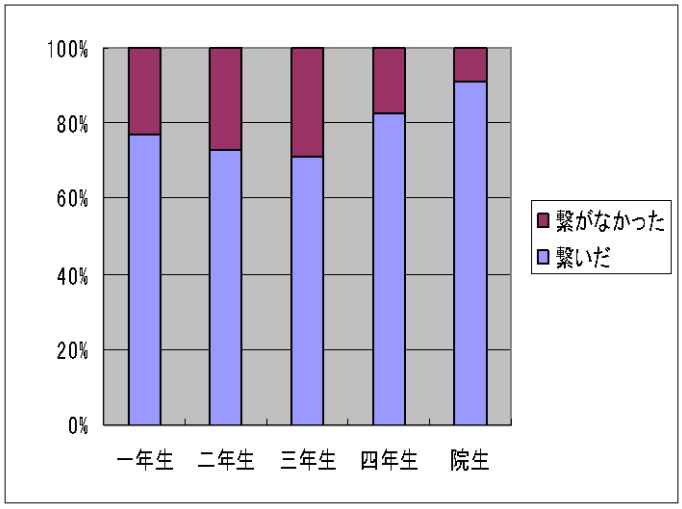

図 3.4　個人所有のパソコンのネットワーク接続

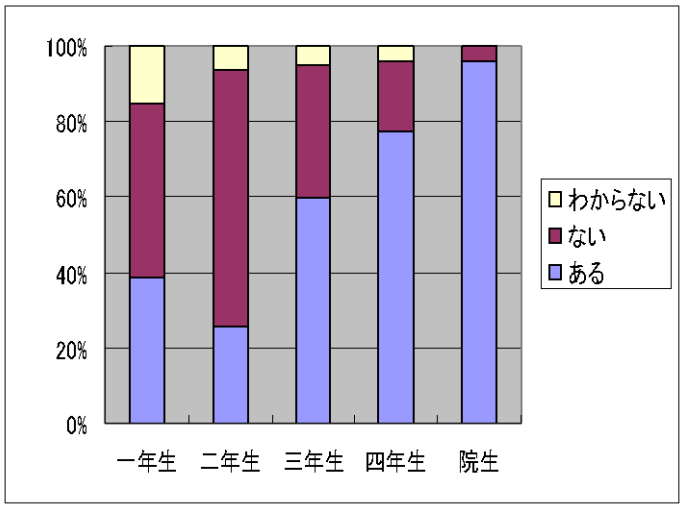

図 3.5　インターネットからダウンロードしたソフトウェアのインストール

– 図 3.6 は、自分しかいない時に見ず知らずの人の入室を許可するかどうかという質問に対しての結果である。基本的に研究室や実験室は、IC カードがなければ入室できないが、業者の人などが作業のために入室することがある。しかし、業者を装っての犯罪も増えてきており、注意が必要である。面識のない人への対応は、判断基準の規定がないためアンケートの回答は個人によって様々であった。
– セキュリティに関して意見があるかという質問に対し、いくつかの回答があった。主なものを以下に列挙する。

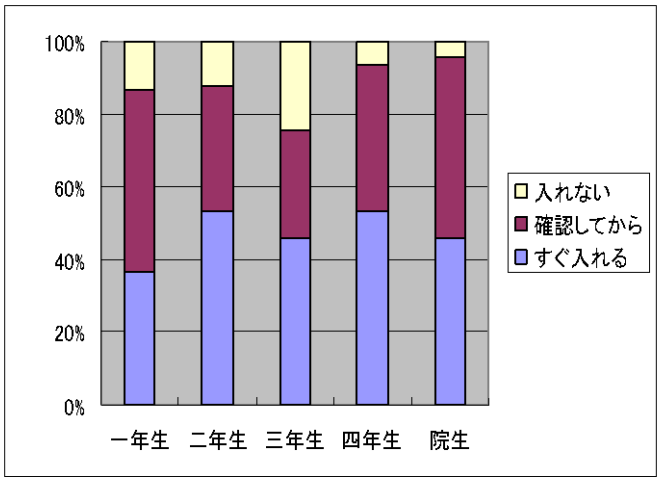

図 3.6　見ず知らずの人への対応

＊ 研究室に所属している人のカードさえあれば、誰でも研究室に入れる。

＊ セキュリティへの意識が、人それぞれで統一されてない。

＊ 各人専用 PC となっているため、一括してパッチをあてるのが難しい。

＊ パスワードが簡単すぎる。

＊ 個人レベルの対策と、ネットワーク管理者側での対策が必要だが、管理者に負荷集中するのはよくない。

＊ 研究室に誰もいないのに、ドアが開いていることがある。

＊ ウィルス対策ソフトが使用されていない。

– アンケート調査の結果、全体としてセキュリティ管理は管理者まかせであり個人のセキュリティ意識は低いと判断した。また、個人のセキュリティ意識レベルやセキュリティに関する知識には個人差があり、学科として統一されたセキュリティ規定を設けることが必要であるという結果になった。

3.3　リスク管理

- リスクアセスメントの結果をまとめリスク評価を行った。
  - 上記の結果をもとに頻度と被害の大きさの 2 つのポイントから、リスク評価を行った。リスク評価の基準として、リスクの高い順に A,B,C の 3 つの段階にわけた。
  - 付録 A.1 参照
- リスク評価の結果を基に対策を決めた。物理的対策、技術的対策、管理的対策の 3 つの観点から対策を決定した。
  - 物理的対策
    - 入室管理を徹底する。
  - 技術的対策
    - 組織の環境に最適なセキュリティ技術を導入する。
    - 常に、バックアップやログなどをとっておく。
  - 管理的対策
    - セキュリティ規定の策定と運用を行う。
    - ユーザ教育を定期的に行う。
    - 緊急時対策の訓練を行っておく。
  - 上記の結果をわかりやすく表にまとめた。付録、表 A.1 参照。

3.4　セキュリティポリシー文書の作成

前節で行ったリスク分析の結果をもとに、セキュリティ管理の方針・規定としてのセキュリティポリシー文書を作成する。

セキュリティポリシー文書は、管理・参照が容易に行えるようにするため Web 形式にする。原文は、付録、A.2 に記載。

- ポリシーを、基本ポリシー、スタンダード、プロシージャの 3 層に分けて考え策定した。
- 基本ポリシーは、情報セキュリティに関する基本方針、ポリシー全般の運用や作成に関

する組織の管理者および、策定担当者からの宣言書となる。具体的には、情報セキュリティポリシーを運用していくための体制や構成についての説明や用語の定義、遵守の義務などである。以下に実際に策定したポリシーの一部を掲載する。

  - 全てのセキュリティ管理は、本ポリシーに準拠すること
  - 本ポリシーは、定期的に評価・見直しされ、常に最新かつ最適なものに更新されること
  - 各研究室ごとに定期的にセキュリティ教育が行われること

- スタンダードは、情報システム工学科全体のセキュリティに関する規定を記述した基準書となる。リスクアセスメントの結果を考慮し、BS7799 文書から管理目的・管理策を選択する。この時、自組織に適用しやすいように変更・追加して記述する。以下に実際に策定したポリシーの一部を掲載する。
  - 情報セキュリティ教育を実施する
  - パスワードの簡単に類推できるものを使用しない
  - 個人が管理する財産は、個人が責任をもって管理しなければならない
- プロシージャは、研究室ごとにスタンダードの管理策を実行するための具体的な手順を記述した文書となる。以下に実際に策定したポリシーの一部を掲載する。
  - 新メンバーの加入時または、重要なセキュリティ情報入手時にセキュリティ教育を行う
  - パスワードは、最低 15 文字以上、単語は使用不可
  - 各マシンには、用途と研究がわかるようにラベルを張る

3.5　適用宣言書の作成

適用宣言書は、セキュリティポリシー策定時に BS7799 文書から選択した管理策について、その選択理由を記述する。また本来は、選択しなかった管理策についてもその理由を記述すべきである。しかし、本研究では選択しなかった項目数が選択した項目数をはるかに上

回ったため記述しなかった。適用宣言書は管理策運用後、管理策の見直しを行う際の参考資料として活用する。

3.6　運用

前節で、策定したポリシーを Web 形式にする。リンクなどを使い、関連ドキュメントも参照しやすくする。本来ならば、実際に学科全員に公布し、承諾を得て運用を行うべきである。しかし、今回は時間がないため、運用することができなかった。

第 4 章

結果

本章では、本研究で行った管理枠組確立の結果と、策定したセキュリティポリシーについての考察を述べる。

4.1 情報システム工学科における管理枠組確立の結果

本節では、本研究で行った管理枠組確立の結果判明したことと、セキュリティポリシー策定によるメリットを述べる。

- リスクアセスメントにより、以下のことが判明
  - 情報システム工学科の学生は、セキュリティ管理を管理者任せにしており、全体的にセキュリティ意識が低い。
  - 個人のセキュリティ意識や知識に格差がある。
  - セキュリティ事故が起こった場合の研究室間における連絡網がない。
  - セキュリティ管理が各研究室任せになっているため、セキュリティ対策の甘い研究室がセキュリティホールになっている。
- セキュリティポリシー策定によるメリット
  - 研究室内の情報資産の管理手順が明確になった。
  - セキュリティに対する研究生の責任が明確になった。
  - 研究室間のセキュリティ情報の共有が可能になった。

4.2 考察

本節では、策定したセキュリティポリシーのうち、遵守が難しいと考える部分を理由とともに列挙する。セキュリティポリシー全体は、付録 A.2 参照。

4.2.1 基本ポリシー

- 各研究室ごとに、定期的にセキュリティ教育が行われること。
  - 学科に、セキュリティ教育を行える専門家が存在しない。

    必要人数は、学科に数名程度で良いが一人に一任してしまうのは、セキュリティ上の問題があるので最低２名は必要である。
  - また、定期的にセキュリティ教育行える時間的余裕がない。

- 本ポリシーまたは法律的な違反行為が発見された場合は、協議され、処罰があたえられること。
  - セキュリティ違反行為について監視する者がいないため。
  - 学生への処罰は現実的に難しい。

4.2.2 スタンダード

- ログインしたまま席を離れない。
  - 研究室において、他人が自分のコンピュータを悪用する可能性が少なく、席を離れるたびにログアウトする手間を省く者が多い。

4.2.3 考察のまとめ

- 本ポリシーでは、各研究室の管理者への負担が多いため、頻繁に構成メンバーの入れ替わりがある各研究室では難しい。
- 3 層に分けてポリシーを作成したため、所属によって参照するドキュメントが絞られ参

照しやすい。

- ポリシーを Web 形式にしたため、管理しやすく参照しやすい。
- Web 形式のため、外部の第 3 者に開示しないような配慮が必要である。
- 緊急時対策マニュアルは、紙媒体のものも作成しておく。

情報システム工学科の構成メンバーが頻繁に入れ替わる上、情報セキュリティ管理システム発案から、構築、運用まで時間がかかるので発案当初のポリシーを守っていけるかどうかわからない。

また、セキュリティ専門家の不在については、情報システム工学科は研究組織であるので、組織の一員がセキュリティについて勉強し、専門知識を身に付けることで解決できる。ただし、セキュリティ担当者が情報システム工学科を去る場合には、後任者を立てて引き継ぎすることにする。

大学のような学術組織では、研究のためにある程度のネットワークシステムが基盤としてある。しかし、セキュリティに対し一般企業ほど危機感がない。しかも、一年ごとに学生の一部入れ替わりが起こる。人の入れ替わりが頻繁にあるということは、常に一定のセキュリティレベルを保つことが困難であるということである。このような組織において、組織的なセキュリティ対策が万全に行なわれているとは考えにくい。従って、大学がネットワーク犯罪の標的にされるということが十分にあり得る。また、大学自身をクラッキングの最終目標にすることよりも、大学のセキュリティの甘さを狙って踏み台にし他の組織を最終標的にすることもあると考える。

であるので、設備の整った組織である高知工科大学情報システム工学科に、組織的なセキュリティ対策を導入することは、将来的に考えて非常に重要なことである。

第 5 章

まとめ

本研究では、組織的なセキュリティ対策の骨組みとなるセキュリティ管理の文書を作成し、情報システム工学科で BS7799 の導入を試みた。その過程において、情報システム工学科では組織的なセキュリティ対策が不十分であるということが判明した。またそれにより、BS7799 の導入を視野に入れ、情報セキュリティ管理システムを構築していけば、組織的なセキュリティ対策を行えるということを示した。

情報セキュリティ管理システムを導入する上で考慮しなければならないのは、セキュリティレベルを高くすればするほど細かい規定や制約ができるので、ユーザにとっては不便になるということである。ユーザが遵守できないポリシーは意味がないので、策定担当者とポリシー対象者であるユーザと協議が十分に行われ、管理策の評価・見直しが常に必要である。そのため本格的な運用までには時間がかかり、本研究では運用段階までにはいたらなかったが、今後本研究で作成した管理枠組を見直すことにより、情報システム工学科に適した情報セキュリティ管理システムになると考える。

本研究の今後の課題は、情報システム工学科におけるセキュリティ管理活動の活発化である。

2001 年 11 月、情報システム工学科で、ROOTS (Resolve Ourselves On Technology and Science) という学生主体の管理者組織が発足した。ROOTS メンバーは、情報システム工学科の各研究室の代表者で構成されている。ROOTS としての活動は、ネットワークチームと WorldWideWeb チームの 2 つに分かれて行うことになっている。組織図は、図 5.1 参照。チームの中でさらに担当を決めているのだが、2 つのチームのうちネットワークチームにセキュリティ班がある。ROOTS としての活動はまだ始動したばかりである。今後、セキュリ

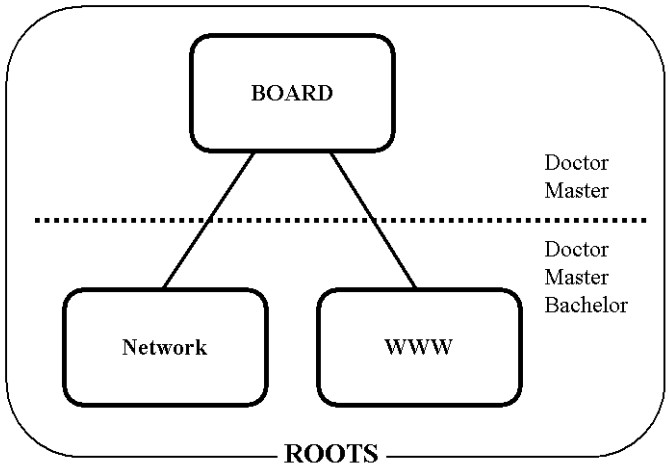

図 5.1　ROOTS の組織図

ティ班が本研究を参考に組織的なセキュリティ対策を行っていくことになる。セキュリティ班に期待する役割は、本研究で行なった管理枠組の見直し、運用・保守と学科全体におけるセキュリティ教育・啓蒙活動である。

ROOTS の活動を通じ、情報システム工学科に適した組織的な情報セキュリティ管理システムを実現させることが今後の課題である。

謝辞

本研究を行うにあたって、多くの方にご協力いただきました。

リスクアセスメントでは、情報システム工学科に所属する学生のみなさんにアンケート調査にご協力いただきありがとうございました。

菊池研究室の広瀬さん、正岡さん、西内さん、舟橋さん、田渕さん、研究について貴重なアドバイスをありがとうございました。

菊池研究室の小川さん、いつも楽しい話を聞かせてもらってすごく楽しかったです。ありがとう。

菊池研究室の澤野くん、マシンの設定の仕方を教えてくれたり、食糧の買いだしに行ってくれてありがとう。

菊池研究室の豊島くん、いつも b4 のまとめ役を引き受けてくれた優しさに感謝します。

菊池研究室の藤岡さん、いろんなことを教えてくれたり、困った時に助けてくれてありがとう。

菊池研究室の前田さん、豆知識を教えてくれたり、親身になって相談にのってくれてありがとう。

岩田研究室の原田さん、いつも励ましをありがとう。

最後に、菊池 豊助教授、本研究及びプレゼンテーション資料作成・発表の指導をしていただきありがとうございました。

参考文献

[1] 日経コミュニケーション No.314. 日経 BP 社, 2000.

[2] 株式会社オーエスケイ IT コンサルティング課. これで作れる情報セキュリティポリシー. 株式会社ローカス, May 2001.

[3] 戸梶桃. 組織における情報セキュリティポリシーの策定手法. PhD thesis, 高知工科大学, 2001.

[4] (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.

[5] 上原孝之. ネットワーク危機管理入門. 翔泳社, July 2000.

付録 A

管理枠組

A.1　リスク管理の結果

- ここでは、悪意を持った者による起こり得る脅威と、過失によって起こり得る脅威と、その他によって起こり得る脅威の 3 つに分け、そのリスク評価を A.1、A.1、A.1、に示す。またリスクの度合として、リスクの高い順に、A、B、C、の 3 段階に分け、頻度、被害の大きさの観点から評価した。

表 A.1　悪意による脅威

脅威	頻度	被害	総合
データの持ち出し、破壊、改ざん	C	A	B
不正アクセス	C	C	C
盗聴、盗難	B	B	B
情報口外	B	C	C
コンピュータウィルス	A	A	A

- ここでは、リスク評価の結果を基に、物理的対策、技術的対策、管理的対策の 3 つにわけてまとめたものを A.1 に、示す。

表 A.2　過失による脅威

脅威	頻度	被害	総合
データの破壊、機器破損	A	A	A
ウィルス *2* 次感染	B	A	A
見ず知らずの人を部屋に入れたトラブル	C	B	C
情報漏洩	B	B	B

表 A.3　自然災害による脅威

脅威	頻度	被害	総合
データの破壊、機器破損	C	A	A

A.2　情報セキュリティポリシー

本研究で作成した情報セキュリティポリシーを Web に載せた原文のまま以下に掲載する。

情報システム工学科セキュリティポリシー

基本ポリシー

１．定義

１．１情報セキュリティ

情報の機密性，完全性及び利用の可能性の維持

１．２情報セキュリティポリシー

組織がセキュリティ対策を行う上での方針，規定等を明文化したもの

１．３基本ポリシー

セキュリティポリシーの一部

情報セキュリティに対する基本方針

１．４スタンダード

表 A.4　対策

対策	具体例
物理的対策	入室管理システム
技術的対策	コンピュータウィルス対策
	暗号化
管理的対策	セキュリティ規定の策定と運用
	ユーザ教育
	緊急時対策

セキュリティポリシーの一部

組織全体で共通の規定のみを記述

１．５プロシージャ

セキュリティポリシーの一部

研究室ごとに独自のポリシーを記述

２．目的及び適応範囲

２．１．目的

情報システム工学科の情報資産を，学科全員で様々な脅威から守り，損害を最小限に抑える．

２．２．適応範囲

・情報システム工学科における情報資産

・情報資産とは，個人情報や各研究室における研究に関する全ての情報

・このセキュリティ管理システムは，情報システム工学科の全員に適応される

３．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

時代の推移と共に，組織並びにその情報システム及び，ネットワークは，コンピュータ支援による詐欺，スパイ行為，破壊行為，火災または洪水など，

広範囲の様々なセキュリティの脅威に直面している.

情報システム工学科も例外ではなく，自組織で情報資産を守らなければならない.

その情報資産を守るためには，組織全員がセキュリティ管理に参加することが必要不可欠である.

4．意向声明書

情報システム工学科全員が，セキュリティポリシーに従い，情報資産を各自の責任で管理，保護していくものとする.

5．情報システム工学科にとって，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等

- 全てのセキュリティ管理は，本ポリシーに準拠すること
- 本ポリシーは，定期的に評価，見直しされ，常に最新かつ最適なものに更新されること
- ポリシーに何らかの変更，追加があった場合，対象者全員に通知され，承諾を得ること
- ポリシー適応範囲におけるネットワークの変更や新しいシステム導入時には，ネットワーク管理関係者間で，厳密に協議されること
- 緊急時には、本ポリシーの緊急時対策マニュアルで定められた基準に沿って、対処されること
- 各研究室ごとに、定期的にセキュリティ教育が行われること
- 本ポリシーまたは、法律的な違反行為が発見された場合は、協議され、処罰が与えられること

6．セキュリティ管理の一般的及び特定責任の定義

基本的には，情報システム工学科に属する各個人が所有する全ての情報資産は、各個人が責任をもって管理する．セキュリティ事故が起こった場合の対処も各個人の責任とする.

７．その他の参考ドキュメント

・スタンダード

・各研究室プロシージャ

８．変更履歴

スタンダード

１．定義

スタンダードは、基本ポリシーを実践するための、具体的な規定である。

２．対象者

情報システム工学科に属する全ての者。

３．改訂

内容は，常に基本ポリシーに従い，基本ポリシーが変更，追加される場合は，

その部分に関連するところも，変更されること．

４．スタンダードの構成

(1)．**セキュリティ組織**

(2)．**財産に対する責任**

(3)．**情報セキュリティ教育、訓練**

(4)．**装置のセキュリティ**

(5)．**パスワード管理**

(6)．**媒体の取り扱い及びセキュリティ**

(7)．**研究室内で使用するコンピュータの取り扱い**

(8)．**機密情報の取り扱い**

(9)．**電子メールの利用**

(10)．**WWW の利用**

(11)．**ソフトウェアのインストール**

(12)．**コンピュータウィルス対策**

(1). セキュリティ組織

《目的》

組織内において、情報セキュリティを管理すること

《セキュリティ対策における注意点》

・セキュリティ管理者の会議

管理者の会議を開き、セキュリティに関する取り決めを明確にしなければならない。

・情報セキュリティ責任の割り当て

個人が管理する財産は、個人が責任を持って管理しなければならない。

・研究室間の協力

研究室の管理者間での適切な連絡が維持されなければならない。

研究室間でのセキュリティ情報が共有されなければならない。

(2). 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

《セキュリティ対策における注意点》

・財産目録を作成し、維持しなければならない

(3)．情報セキュリティ教育、訓練

《目的》

情報セキュリティの脅威を認識し、その通常の作業において、組織のセキュリティポリシーを支持する態勢が取れるようにすること。

(4)．装置のセキュリティ

《目的》

財産の損失、損傷又はそのセキュリティが損なわれることを防止すること。

《セキュリティ対策における注意点》

・財産目録を作成し、維持しなければならない

(5)．媒体の取り扱い及びセキュリティ

《目的》

財産に対する損傷、及び研究活動に対する妨害を防止すること

《セキュリティ対策における注意点》

・取り外し可能なコンピュータ媒体の管理

取り外し可能なコンピュータ媒体、例えば、テープ、ディスク、カセット及び重要書類等について、その管理がなされなければならない。

・媒体の処分

媒体は、不要となった場合、安全、確実に処分しなければならない。

(6)．パスワード管理

《目的》

許可されていないユーザアクセスを防止すること

パスワードの機密性を保持する

《適用対象者》

情報システム工学科において，一つ以上のパスワードを所有している

全ての者

《セキュリティ対策上の注意点》

・パスワードは簡単に類推できるようなものを使用しない.

・複数のワークステーション, サーバへのアクセス, 管理者パスワードは全て異なるものにする事.

・パスワードを見える位置に書き留めておかない

・他人にパスワードを教えない

・パスワードは定期的に変更する

(7). 研究室内で使用するコンピュータの取り扱い

《目的》

研究室内のコンピュータを第三者によって、悪用されないようにすること

《適用対象者》

情報システム工学科において、研究室に属する全ての者

《セキュリティ対策上の注意点》

・ログインしたまま席を離れない

・個人に割与えられたコンピュータを他人に使用させない

(8). 機密情報の取り扱い

《目的》

情報資産の機密性を保持する

《適用対象者》

情報システム工学科において、情報資産を所有する全ての者

《セキュリティ対策上の注意点》

・研究内容の書かれた書類の管理や、処分に注意する

・外部の人に、機密情報を口外しない

(9). 電子メールの利用

《目的》

電子メールによってもたらされるおそれのあるセキュリティ上のリスクを軽減するため

電子メールによる、機密情報の漏洩を防ぐ。

電子メールによる、コンピュータウィルス感染を最小限に抑える。

《適用対象者》

情報システム工学科において、電子メールを利用する全ての者

《セキュリティ対策上の注意点》

・機密情報をメールでやりとりする場合は、暗号化する。

・差出人不明のメールを受け取った場合は、メールを開かない。

・容量の大きいメールは、開かない。

(10).WWW の利用

《目的》

自作ホームページによる情報漏洩を防ぐ。

Web soopfing というソーシャルエンジニアリングの手口を防ぐ。

《適用対象者》

情報システム工学科において、WWW を利用する全ての者

《セキュリティ対策上の注意点》

・自作ホームページで公開すべきでない情報

本名、家族構成、家族の名前や親しい人の名前

パスワード

自宅の住所

勤務先や学校名、出身校

最寄りの駅やバス停、通勤通学の経路

電話番号（FAX、携帯電話、PHS、自動車電話などを含む）

銀行などの口座番号、暗証番号

自分の顔写真

メールアドレス

研究室の機密情報

・信頼性のないホームページを見ない。

(11). ソフトウェアのインストール

《目的》

機密情報の保全性、可用性を保護する。

《適用対象者》

情報システム工学科に属する者で、研究室の自分のマシンに何らかのソフトウェアをインターネットからインストールする者。

《セキュリティ対策上の注意》

・信頼性のあるソフトウェアのみインストールする。

・信頼性の確認ができない場合、研究室内で協議してから、インストールすること

(12). コンピュータウィルス対策

《目的》

コンピュータウィルスから、保全性、可用性を守る。

《適用対象者》

情報システム工学科において、本学科のコンピュータを使用するもの

《セキュリティ対策上の注意》

・研究室ごとに、管理者の指示にしたがってウィルス対策を行う。

・最新のウィルス情報を入手したものは、速やかに研究生に通知する。

(13). データの暗号化

《目的》

情報の機密性、又は完全性を保護すること。

《適用対象者》

情報システム工学科において、機密情報を取り扱う全ての者。

《セキュリティ対策上の注意》

・機密情報が盗聴される恐れがある場合には、暗号化する。

・暗号化の方法については、各研究室の管理者の指示を受ける。

(14). ネットワーク環境の変更

《目的》

ネットワーク環境の設定変更などによる、セキュリティホールの発生を防ぐ。

《適用対象者》

情報システム工学科において、ネットワーク環境の構築や管理に携わる全ての者。

《セキュリティ対策上の注意》

・既存のネットワーク環境を、変更する場合は、管理関係者間で協議し、承諾を得る。

・新しいネットワーク環境を構築する場合は、管理関係者間で協議し、承諾を得る。

(15). セキュリティ最新情報の収集と配布

《目的》

本ポリシーを常に最新の状態を保ち、信頼性を高めるため。

《適用対象者》

情報システム工学科の研究室に属する全ての者。

《セキュリティ対策上の注意》

・各自が、最新のネットワーク犯罪の情報を収集する。

・各自が、最新のセキュリティ技術に関する情報を収集する。

・最新情報が、各研究室の管理者に集まるようにする。

・管理者は、必要に応じて研究生に情報を配布する。

(16). ログの収集と分析

《目的》

セキュリティ事故が起こったときのために、備える。

《適用対象者》

各ネットワーク管理者

《セキュリティ対策上の注意》

・常に、ログを収集しておくこと。

・分析については、セキュリティ事故が起こった時もしくは、

定期的に行う。

(17). バックアップ

《目的》

セキュリティ事故が起こったときのために、備える。

《適用対象者》

各ネットワーク管理者

《セキュリティ対策上の注意》

・定期的に必要なバックアップをとっておく。

(18). セキュリティ事故への対処

《目的》

セキュリティ事故による損害を最小限に抑え、そこから学習すること

《セキュリティ対策上の注意》

セキュリティ事故は、事故発見後速やかに、適切な管理者連絡網を

通して報告されなければならない。

《適用対象者》

情報システム工学科に属する全ての者

《しなければならない事》

・管理責任者に報告。

・被害状況の確認。

・原因の究明

・関係各所に連絡し、2 次的被害を食い止める。

・もし、対策可能であれば対策を行う。

・必要に応じ、情報処理振興事業協会セキュリティセンター（IPA）へ被害届けを出す。

(19)．研究継続管理

《目的》

研究活動に対する障害に対処すること、重大な故障または災害の影響から重要な研究過程を保護すること。

《セキュリティ対策上の注意》

・研究継続管理過程

組織全体に渡る研究継続するための管理されたプロセスが、整っていなければならない。

(20)．法的要求事項への準拠

《目的》

刑事及び民事法、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さけること。

《セキュリティ対策上の注意》

・知的所有権

知的所有権に関わるソフトウェア製品の使用について、法的制限事項に確実に準拠するように、適切な手順を実行しなければならない。

プロシージャ

１. 定義

プロシージャは，対象者や目的によって必要な規定のみを記述したもの.

その内容は各研究室ごとに異なり，具体的な内容であるため，日常的に

参照するもの.

２. 対象者

情報システム工学科の研究室に所属する全ての者である.

ただし，その内容は所属する研究室により異なる.

研究室の構成メンバーは，頻繁に入れ替わりがあるが，メンバーに加わった

時点でポリシーの承諾を得ること.

３. 評価と改訂

基本理念は，基本ポリシーやスタンダードに従い，それらが変更されれば，

その部分に関連するプロシージャも変更される.

内容が研究室独自であるため，著しく他研究室と異なる場合は，代表者会議

で協議されること.

４. 各研究室のプロシージャ

・菊池研究室

菊池研究室プロシージャ

１. 定義

本ドキュメントは，情報システム工学科の基本ポリシーとスタンダードを

基本理念におき，具体的に実践するためのものである.

２. 対象者

菊池研究室に属する全ての者。

３. 改訂

・内容は，基本ポリシーとスタンダードを基本理念としているため，これらが

変更されれば，その部分に関連するところも，変更されること.

・菊池研究室を取り巻く環境が変化した場合，本ポリシーも必要に応じて改訂する．

・改訂については，菊池研究室に属する全員の承認を得ること．

・改訂後も，全員に変更内容の説明をし，全員の承諾得ること．

４．プロシージャの構成

（1）．セキュリティ教育

（2）．セキュリティポリシーの承諾

（3）．パスワード管理

（4）．マシン管理

（5）．変更履歴

（1）．セキュリティ教育

《目的》

個人のセキュリティ意識を高め、研究室の情報資産を保守するため

《適用対象者》

菊池研究室に所属するすべての者

《セキュリティ対策上の注意点》

・研究室に新メンバー加入時もしくは重要なセキュリティ情報入手時に研究室メンバーに対し実施する

・セキュリティ教育は、研究室のセキュリティ担当者もしくは担当教員によって行なう。

（2）．セキュリティポリシーの承諾

《目的》

ポリシーの存在を明らかに示し，承諾を得ることで，

準拠対象を明確にし，個人のセキュリティ意識を高める．

《適用対象者》

菊池研究室に属する全ての者.

《セキュリティ対策上の注意点》

・研究室に属した時点で，承諾すること.

・承諾したからには，ポリシーに従って行動する.

・ポリシー変更時には，変更箇所確認とその内容に対しての承諾を行なう.

・研究室メンバーでなくなる際には，ポリシー内容を口外しないこと

(3). パスワード管理

《目的》

パスワードの機密性を保持する.

《適用対象者》

菊池研究室におけるマシンのパスワードを保持している全ての者

《セキュリティ対策上の注意点》

・パスワードは簡単に類推できるようなものを使用しない.
最低 15 文字以上、単語の使用不可

・パスワード情報が第３者にわたった危険性がある場合，速やかにパスワードの変更を行なうこと.

(4). マシン管理

《目的》

個々のマシンの管理責任の所在を，明確にする.

《適用対象者》

菊池研究室において，研究室のマシンを管理している全ての者

《セキュリティ対策上の注意点》

・個人で管理しているマシンについては，個人が管理する.

・研究ごとに，使用しているマシンについては，各研究の代表者が

マシンの管理責任者となる.

・各マシンには，用途と研究がわかるように，ラベルを張っておく.

(5). 変更履歴

A.3　情報セキュリティ管理システムの適用範囲

情報セキュリティ管理システムの適用範囲は、情報システム工学科である。

A.4　適用宣言書

BS7799 によると、選択された管理目的及び管理策、なら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とある。
そこで、ここに付録 A.4 に列挙した項目について、情報システム工学科に適用した理由を以下に述べる。

A.4.1　セキュリティポリシー

- セキュリティポリシーは、組織的な情報セキュリティ管理システムを導入する上で欠かせないものであるため。

A.4.2　セキュリティ組織

- セキュリティ組織は、情報セキュリティ管理システムを運営していく上で、情報セキュリティの基盤となるものであるため。
- セキュリティ管理は、研究室間の協力が必要であり、情報システム工学科全体として、取り組む必要があるため。

A.4.3　財産に関する責任

- 情報資産に対する責任の所在をあきらかにし、各自が責任をもって財産を保護するようにする必要があるため。
- 財産目録を作成し、守るべき財産を明確にする必要があるため。

A.4.4　情報セキュリティ教育、訓練

- 情報システム工学科の学生の、セキュリティに関する知識や認識が、個人によって格差があるため。
- 万が一セキュリティ事故が起こったときに、迅速に適切な対応を行える

A.4.5　装置のセキュリティ

- 情報システム工学科には、多数の装置が存在しており、それぞれの装置には、様々な情報資産が記憶されている。その情報資産の漏洩を守るために、装置の管理または処分には注意が必要であるため。

A.4.6　媒体の取り扱い及びセキュリティ

- 情報システム工学科には、多数の媒体が存在しており、特に移動可能なコンピュータ媒体や重要書類については、取り扱いに気をつける必要があるため。

A.4.7　情報及びソフトウェアの交換

- 情報システム工学科では、日常的に情報の交換がされており、機密情報を保護する必要があるため。

A.4.8　ユーザの責任

- 情報システム工学科では、多数のユーザが存在しており、セキュリティ意識がユーザによって様々であるため。

A.4.9　暗号による管理策

- 機密情報の機密性、完全性を保護するため。

A.4.10　研究継続管理

- 万が一研究活動に支障のある障害が起こっても、その影響が最小限に抑えられるようにするため。

A.4.11　法的要求事項への準拠

- 法的要求事項への準拠は、情報システムに携わる者の最低限守るべき基準であり、組織に属する者の違反を防ぐため。