平成 14 年度

学士学位論文

大学における情報セキュリティポリシー策定の試行と検証

A Study of Applying Information Security Policy to University

1030261　　川西志穂

指導教員　　菊池 豊

2003 年 2 月 24 日

高知工科大学 情報システム工学科

要 旨

大学における情報セキュリティポリシー策定の試行と検証

川西志穂

近年，不正侵入や情報の漏洩などネットワークに関わるさまざまなセキュリティ上の問題が急増してきている．その中，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策定を行う大学が年々多くなってきている．昨年，澤田が情報システム工学科においてセキュリティ規格 BS7799 を用いてセキュリティポリシーを作成した．しかし，この情報セキュリティポリシー文書だけでは，学生に興味を持たせ，セキュリティレベルを上げられるとは考えにくい．

本研究の目的は，学生が容易にセキュリティレベルを向上させることができるセキュリティポリシーの策定である．その目的を達成するために，菊池研究室のセキュリティポリシー文書を作成し，それに基づいてアンケートシステムを構築した．さらにこのシステムを情報システム工学科で運用し，評価を行った．

その結果，アンケートシステムを導入することにより，従来のセキュリティポリシー策定手順に比較して，学生が効果的にセキュリティ対策を行えることがわかった．また，各研究室によってセキュリティレベルに違いがあることが分かった．今後の課題は，各研究室に特化したアンケートシステムを作成することである．

キーワード　BS7799，セキュリティポリシー，アンケートシステム

Abstract

A Study of Applying Information Security Policy to University

KAWANISHI shiho

Various problems of security that relate network have been increasing in recent years. For example unauthorized invasion and leak of information. Therefore many colleges have been applying rule of security policy to do the countermeasure for a security. Sawada made security standard BS7799 at the Department of information system engineering last years. I don't think that students would not be interested in that, and they could not have a high level of security.

An aim of this study is to apply rule of security policy which students can easily raise level of security. To achieve that, I made reports of security policy at Kikuchi laboratory, and construct a questionnaire system. I worked this system and valued at Department of information system engineering.

As a result, students could do the countermeasure for a security more efficiently than old days of that. But there was a difference of level of security by each laboratory. A future subject is that I make a questionnaire system that suits each laboratory.

key words BS7799, security policy, questionnaire system

目次

図目次

表目次

第 1 章

はじめに

近年，インターネットの普及により，インターネットは企業にとって業務の効率化や情報収集のために欠かせない道具となってきた．また，インターネットは，電子商取り引きやオンライントレードなど新しいビジネスを創出した．しかし，その一方ではインターネットからの不正侵入や情報の漏洩などネットワークに関わるさまざまなセキュリティ上の問題が表面化してきている．このため，企業などの組織では，今まで以上に情報セキュリティの強化が必要となってきている．

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ものである．これをを定めることによって組織全体で一貫したセキュリティ対策が行える．

澤田は，情報システム工学科においてセキュリティ規格 BS7799 [2] を策定し，検証を行い，情報セキュリティポリシー文書を作成した [4]．それにより，組織的なセキュリティ対策を行えることが分かった．しかし，この情報セキュリティポリシー文書だけでは学生がセキュリティに対して関心を持ち，大学全体のセキュリティレベルが上がるとは考えにくい．そこで，本研究では，大学生がセキュリティについて関心を持ち，容易にセキュリティレベルを向上させることができるセキュリティポリシーを策定することを目的とした．セキュリティ規格 BS7799 を用いて，大学におけるセキュリティポリシーを策定し，情報システム工学科 (研究室) のセキュリティレベルや作成したセキュリティポリシーを検証した．

以下第 2 章で，ネットワーク社会の現状やセキュリティ対策について説明する．次に第 3 章で BS7799 とセキュリティポリシーの説明と大学におけるセキュリティポリシーの問題点

とその解決策を述べ，アンケートシステムの説明をする．そして，第 4 章では菊池研究室における調査を，第 5 章ではアンケートシステムを用いての情報システム工学科での実験と，その結果を述べた．第 6 章は，アンケートシステムに対しての考察と改良点を述べた．最後に，第 7 章で結論と今後の課題を記す．

第 2 章

ネットワーク社会の現状とセキュリティ対策

本章では，ネットワーク社会の現状や脅威への対処法と，大学や企業の侵害事案やセキュリティ対策の現状を述べる．

2.1　ネットワーク社会の現状

インターネットの利用による， ネットワーク環境は急速に変化している．そこで本節では，ネットワーク社会の現状とそれに伴うインターネット利用者の推移について述べる．

2.1.1　パソコンの普及率の推移

内閣府経済社会総合研究所の発表によると，日本の世帯当たりパソコンの普及率は 57.2 %にまで上昇した (図 2.1 参照)．米国商務省の調べでは，米国は 2001 年 9 月時点で 56.5 %で，日本が初めて逆転した．2 年前の 2000 年では，米国が 50 %と約 12 %の差があったにもかかわらず，着々と延び続け米国を抜く結果となった．この表を見る限りでは，これからも延び続けると考える．

2.1.2　インターネットの利用者数

日本のインターネット利用者数は，ここ数年で急速に増加を続けている．総務省が行った通信利用動向調査によれば，平成 13 年末における日本のインターネット利用者数は 5,598

2.1　ネットワーク社会の現状

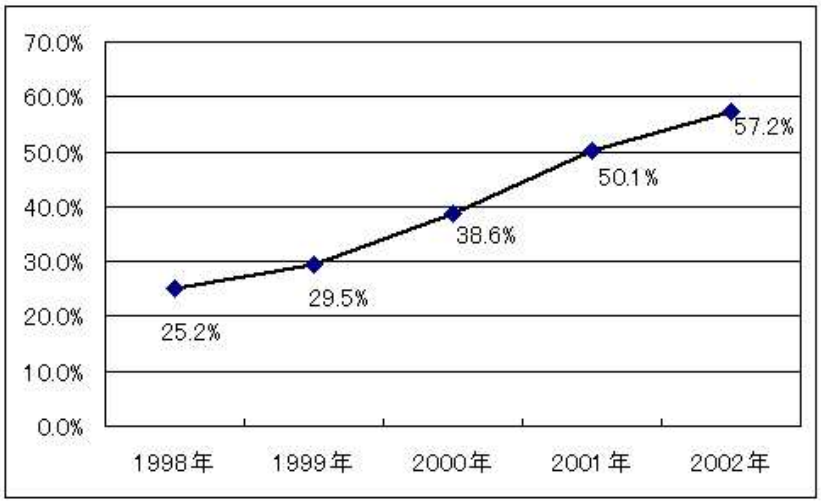

図 2.1　パソコンの普及率

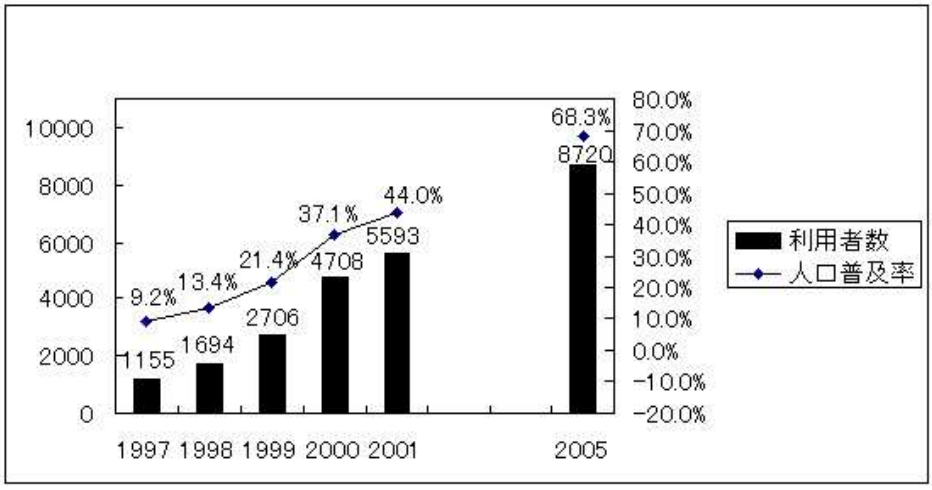

図 2.2　インターネット利用者数および人口普及状況

万人と推計され，人口普及率は 44 %となっている (図 2.2)[*1]．平成 17 年には，インターネット利用者は 8,720 万人に達するものとみこまれている． また，世界におけるインターネット人口普及率は，世界第 16 位である．しかし，インターネット利用者数は，アメリカ

[*1] 総務省 情報通信白書 インターネットの人口普及状況図表
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h14/index.html より抜粋

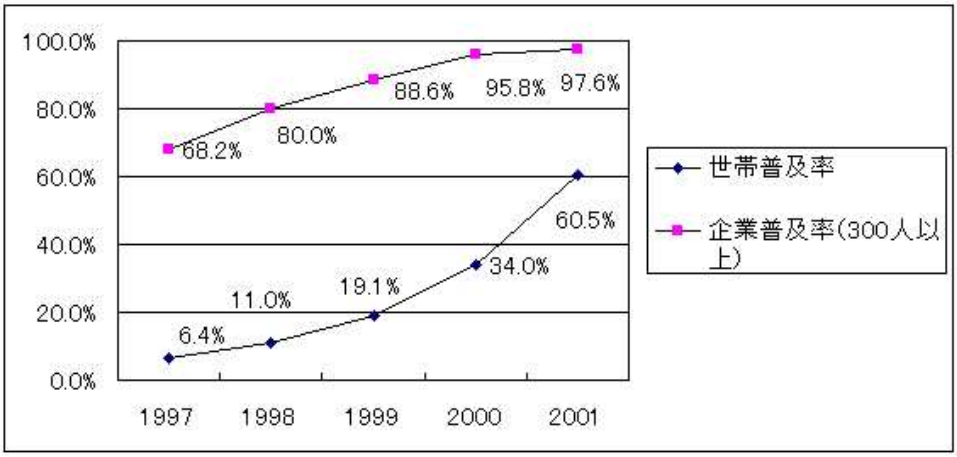

図 2.3　世帯・企業でのインターネット普及率

に次ぐ世界第 2 位となっている[*2].

2.1.3　世帯・企業でのインターネット普及率

インターネットの世帯普及率は，平成 12 年末の 34.0 %から平成 13 年末には 60.5 %と全世帯の 6 割を超え，世帯でのインターネット利用が急速に進んでいることが分かる．今後は，ネットショッピングやオークション等の利用により，ますます普及していくと考えられる．また，企業普及率は，97.6 %と，既にほとんどの企業で利用されているなど，インターネットの普及は着実に進んでいる (図 2.3)[*3].

2.2　ネットワーク犯罪の種類

前節で述べたように，インターネットの普及は着実に進んでいる．それにより，人々の暮らしはより豊かなものになってきている．しかし，それを利用したネットワーク犯罪が増えている．この節では，インターネットを利用したネットワーク犯罪の種類について述べる．

[*2] 総務省 情報通信白書 世界におけるインターネットの普及状況
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h14/index.html より抜粋

[*3] 総務省 情報通信白書 世帯・企業でのインターネット普及率図表
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h14/index.html より抜粋

- コンピュータウィルス

  コンピュータウィルスとは自己感染，滞在，発病などの機能を持ち，ユーザの意図しない動作をするプログラムである．ウィルスには，単にいたずらのような画面や音を出すものから，システムを壊すものまで多数ある．新しいウィルスが数々出現しており，ウィルス退治のワクチン製造が追いつかぬ程である．感染経路としては，フロッピーやCD-ROM などの物理媒体，インターネットでは FTP や HTTP によるソフトウェアのダウンロードやメールに添付されて感染することが多い．

- 盗聴

  盗聴とは通信内容が第三者に無断で傍受される脅威である．ネットワーク上を流れる情報は，それが不特定多数のコンピュータを通過する過程において当事者以外の第三者に漏洩する可能性が高く，同時に第三者が積極的に情報を盗聴することも容易である．そして，その被害は，プライバシーの侵害もさることながら，第三者によって入手された情報が更に悪用されることにより，改ざん，なりすまし，内部ネットワークへの不正侵入につながる．

- 改ざん

  改ざんとはネットワーク上を流れる情報が盗聴され，情報が書き換えられて受信者に届けられたりすることである．電子的な情報は書き換えや消去することが容易であり，その痕跡も残らないのである．そのため，情報が通信途中に改ざんされたとしても，誰も気づかない場合が多い．

- なりすまし

  なりすましとはネットワークを介して受信するデータの正当な送受信者のふりをして，企業内ネットワークに侵入したり，不正に情報を取り引きする行為のことである．被害者は，身に覚えのない請求所が送付されて初めて被害を認識することが多いため，なりすましが行われてから捜査当局が認知するまでにタイムラグが生じやすく，捜査が困難化しがちである．

- DoS 攻撃

DoS(Denial of Service) 攻撃とは，何らかの方法により，攻撃のターゲットとなるサーバやネットワークが提供するサービスを妨害する行為である．DoS 攻撃をされると回線がパンクし，インターネットが利用できなくなる可能性がある．DoS 攻撃により，発生する被害 (脅威) には以下のようなものがある．

- OS，サービスのダウン (停止)

  DoS 攻撃のターゲットとなった OS またはサービスが，攻撃によりダウンしてしまう．そのため，意図的に OS やサービスを再起動しなければ，正常サービスの提供が開始されない．この被害は，セキュリティホールを悪用した DoS 攻撃により発生する場合が多い．

- 一般的なサービスの停止

  主にこの被害は，ネットワークに対して過負荷を与える DoS 攻撃により生じるもので，多量のパケットを利用した DoS 攻撃の場合，パケット数が一定値以下に削減されることで，正常なサービスが提供できる状態に戻る．DoS 攻撃を受けている間，正常サービスの提供が妨害されてしまうが，攻撃終了後，正常なサービス提供が復旧する．

- DDoS 攻撃

  前に説明した DoS 攻撃の攻撃元が複数で，標的とされたコンピュータがひとつであった場合，その標的とされるコンピュータにかけられる負荷は，より大きなものとなる．このような攻撃が DDoS(Distributed Denial of Service) 攻撃と呼ばれている．

- ソーシャルエンジニアリング

  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．

2.3　脅威への対応策

脅威への対応策として，次のようなものがあげられる．

- 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，許可しなかったりするものである [3].
- ウィルス対策ソフト

  ウィルス対策ソフトは，パソコンにインストールするソフトウェアだけではなく，インターネットから送られてきたメールやダウンロードしたファイルなどの中身のチェックも行えるものがある．
- 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 [3].
- 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．
- 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ある．

2.3.1　侵害事案の発生事態

本節では，昨年度一年間のネットワーク犯罪による侵害状況について述べる．

総務省が 2002 年 3 月に行った調査によると，民間企業では，過去一年間に侵害事案が発生した企業が全体の 60 %を占め，また，そのうちの約 96 %が「ウィルス・ワーム感染」に

よる被害を受けている (図 2.4，2.5)[*4]．また，大学が企業を上回る被害を受けており，全体の 73 %が過去 1 年間に侵害事案が発生している．民間企業と同様,「ウィルス・ワーム感染」による被害の発生率が約 96 %と圧倒的に高いが,「スパムメールの中継利用・踏み台」,「ホームページ改ざん」など他の侵害事案についても発生率が高くなっている．この結果から，大学はネットワーク犯罪の標的になっていることが分かる．

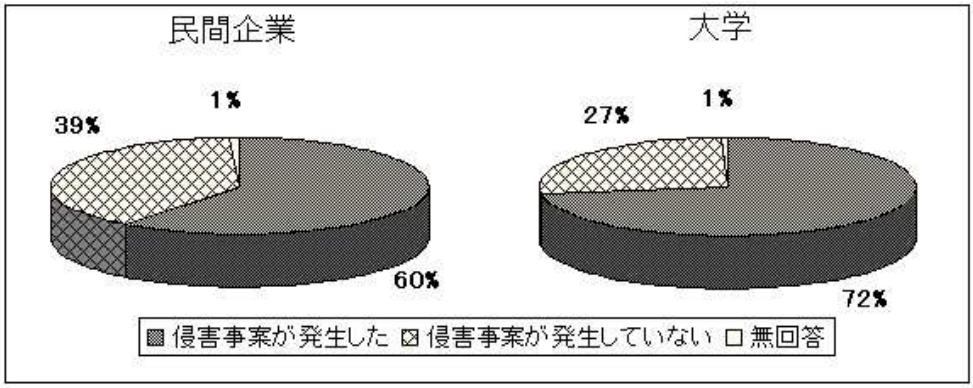

図 2.4　企業，大学における侵害事案の発生状況

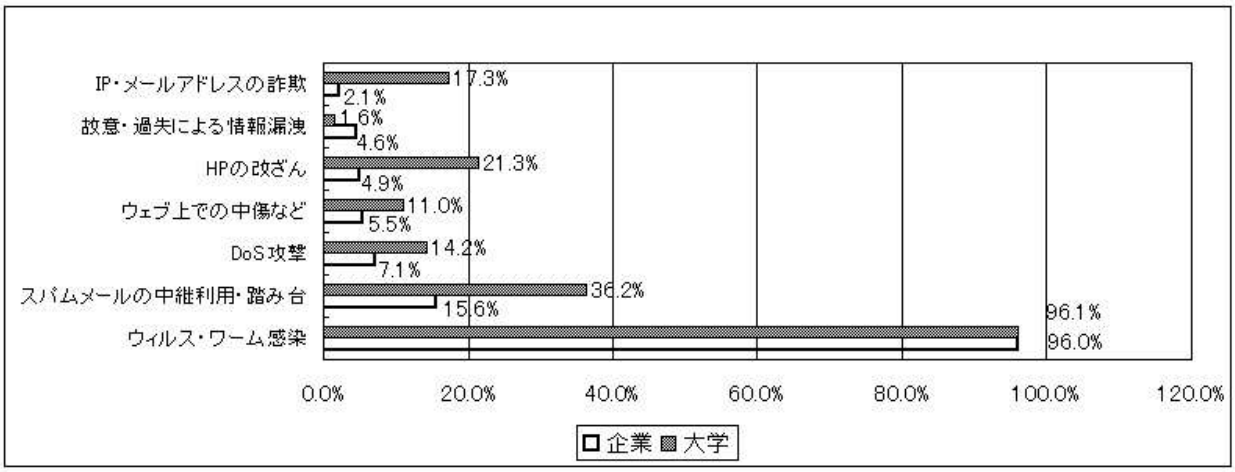

図 2.5　企業，大学における侵害事案の内容

[*4] 総務省 情報セキュリティ対策の状況調査 http://www.soumu.go.jp/s-news/2002/pdf/020509_2_1.pdf より抜粋

2.3.2　セキュリティ対策の現状と大学におけるセキュリティ対策

第 2.3.1 節で述べたような事態の中，多くの企業は第 2.3 節で述べたような対応策を行うことが多い．しかし，新しい脅威への対応策のために，膨大なコストがかかってしまう．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がある．組織的なセキュリティ対策が行えていないと，自組織だけでは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．そこで，最近，「セキュリティポリシーの必要性」がクローズアップされるようになってきた．セキュリティポリシーとは，組織のセキュリティ対策を効率よく，効果的に行うための指針であり，その場限りの対策ではなく，恒久的にセキュリティを維持するための方針である．

図 2.6[*5]によるとセキュリティポリシーを策定している企業は，全体の約 29 %にとどまっている．また，大学でのセキュリティポリシー策定状況としては，企業よりも少なく全体の 18.3 %にとどまっている．このことから，大学でのセキュリティポリシー策定は遅れていることが分かる．しかし，策定を検討しているが 45 %となっていることから，今後，大学におけるセキュリティポリシーの策定が着実に進むものと考えられる．

このように一部ではあるが「大学」という組織で，セキュリティポリシー策定を行っていることが分かった．しかし大学という組織で，セキュリティポリシー策定を行ったとしても，大学全体にセキュリティポリシーがうまく機能するかどうかは限らない．大学全体にセキュリティポリシーを機能させようとすると，膨大なコストと人件費がかかるし，大学には色々な学部がありそれに伴って環境が変わってくるからである．このことから，個々の団体には個々の団体のセキュリティポリシーの策定が必要であると考える．

[*5] 総務省 情報セキュリティ対策の状況調査 http://www.soumu.go.jp/s-news/2002/pdf/020509_2_1.pdf より抜粋

2.3　脅威への対応策

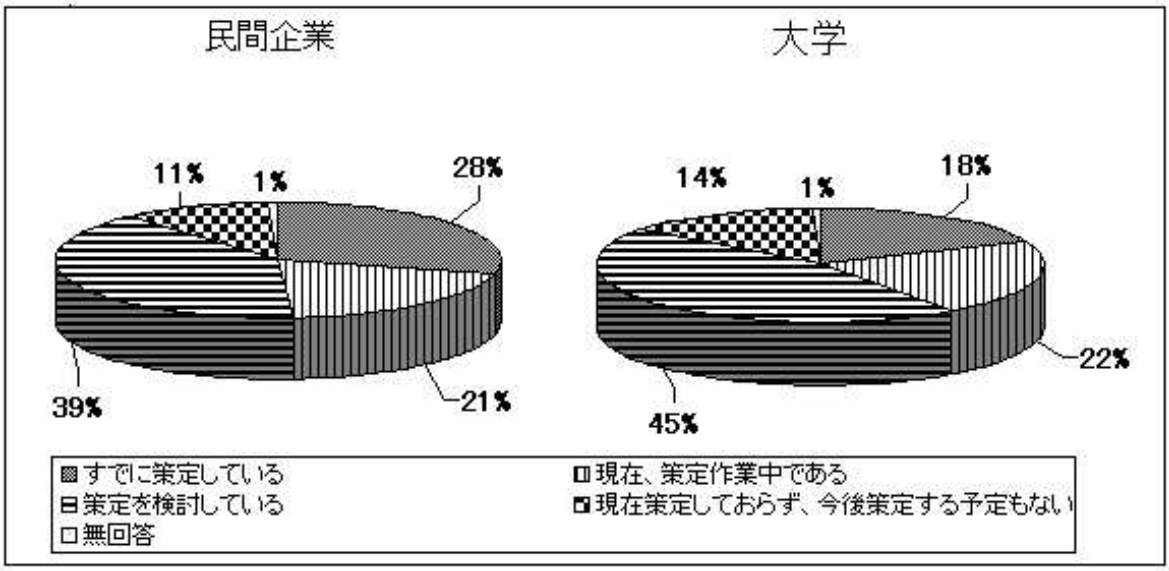

図 2.6　セキュリティポリシー策定有無

第 3 章

BS7799 とセキュリティポリシーの問題点

本章では，BS7799 と大学におけるセキュリティポリシー策定の問題点について述べる．

3.1 BS7799

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 [2].

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 部構成となっている．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，BS7799 を実装するための必須事項が書かれている．

3.2 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．

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 [2]．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．

3.2.1　セキュリティポリシー策定の手順

この節では，セキュリティポリシーを策定するときの BS7799 で定められている手順について，簡単に述べる [3]．

1. 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．
2. 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．
3. 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．
4. 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．

3.3　大学におけるセキュリティポリシー策定の問題点

BS7799 を大学に導入するに当たっての問題点として以下があると考える．

- リスク分析やセキュリティポリシー文書の作成，運用・管理を行うことは，人的・時間的なコストがかかる．
- 頻繁に研究室の構成メンバーが変わってしまうため，一年に一回はリスク分析を行う必要がある．そのため，人的・時間的なコストがかかってしまう．
- 学生がセキュリティポリシーを守る可能性が低いので，コストに対して比較して得られるセキュリティ強度が小さい [1]．
- 学生はセキュリティ意識が低いため，セキュリティ文書を読む可能性が低い．

図 3.1 は，セキュリティポリシーを策定する場合の一般的な手順とそれに対しての問題点を描いたものである．

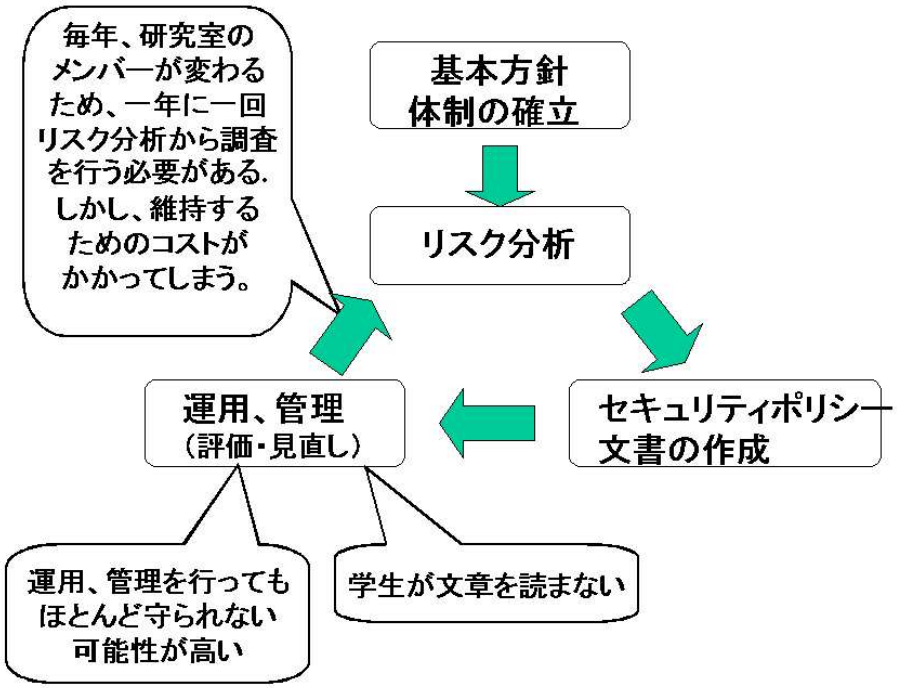

図 3.1　BS7799 を大学で導入した際の問題点

3.4　問題点に対する解決方法の考察

本節では前節で述べた問題点の解決策を示す.

- 「リスク分析やセキュリティポリシー文書の作成，運用・管理を行うことは，人的・時間的なコストがかかる.」「頻繁に研究室の構成メンバーが変わってしまうため，一年に一回はリスク分析を行う必要がある．そのため，人的・時間的なコストがかかってしまう.」ことに対しての対応策
  - セキュリティポリシー文書を作成するようなプログラムを構築することで，人的・時間的なコストを下げる.
  - インターネット上でアンケートを行うことで，リスク分析のコストを軽減させる.
- 「学生がセキュリティポリシーを守る可能性が低いので，コストに対して比較して得られるセキュリティ強度が小さい.」ことに対しての対応策
  - セキュリティ意識が低いという事を自覚させるような表示方法にする.
  - コスト削減のために，セキュリティポリシー文書の作成をプログラム化する.
- 「学生はセキュリティ意識が低いため，セキュリティ文書を読む可能性が低い.」ことに対しての対応策
  - 学生でもすぐ守れるような簡単な文章にする.
  - 守るべきプロシージャを強調するようなセキュリティポリシー文書を作成する.

3.5　アンケートシステムを用いたセキュリティポリシー策定手順の提案

前節で述べた解決策を全て考慮して，アンケートシステムを用いたセキュリティポリシー策定手順を提案する (図 3.2)．この策定手順は，図 3.1 の「運用・管理」をアンケートシステムに置き換えた．そうすることで，効率的なセキュリティレベルの向上につながり，運用・管理が機能し，大学におけるセキュリティポリシーを策定することができると考える.

本提案は，まず対象者がセキュリティ診断を行い，その集計結果に基づいて管理者がリスク分析をする．そして，セキュリティポリシー文書の作成を行い，アンケートシステムの評価や見直しをするというものである．このサイクルが回ることで，そのときどきのセキュリティレベルにあったセキュリティ対策を行うことができる．

アンケートシステムとは，インターネット上でセキュリティアンケートを行うことにより，対象者のセキュリティに対する弱点を調べ，その弱点に対するセキュリティ診断がアンケートを行った直後にでてくる仕組みである．

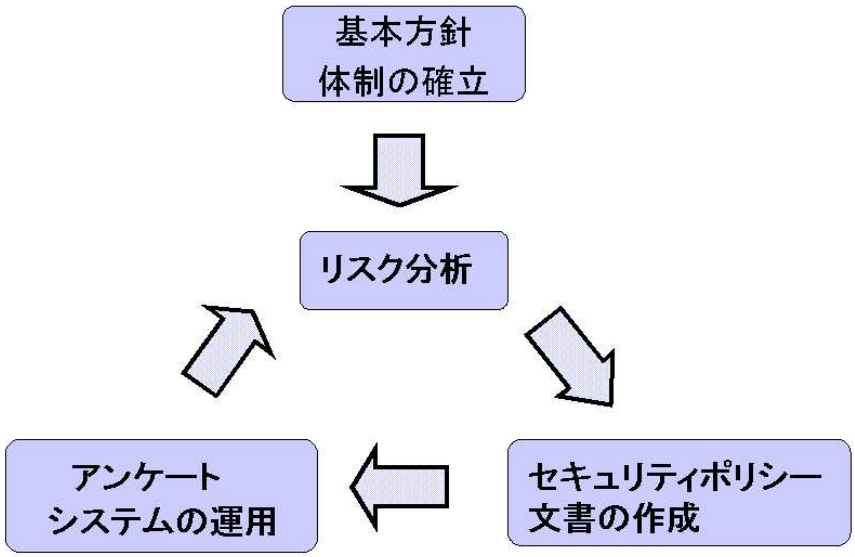

図 3.2　アンケートシステムを用いたセキュリティポリシー策定手順

3.6　提案方法に基づく実験手順

情報システム工学科 (研究室) のアンケートシステムを構築するにあたって，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 の策定手順に基づいて，菊池研究室においてリスク分析をし，セキュリティポリシー文書を作成することにした．

本来ならば，情報システム工学科 (研究室) のセキュリティポリシーを作成しなければならない．しかし，情報システム工学科 (研究室) でアンケートを行いセキュリティポリシーを策定すると，人的・時間的コストがかかってしまい，コストに比較して得られるセキュリティ強度が小さくなる．そこで情報システム工学科各研究室の代表として菊池研究室のセキュリティポリシー文書を作成することにした．人数が少ないことにより，アンケート集計にかかる人的・時間的コストが削減される．

次に，セキュリティ文書からアンケートシステムを構築し，情報システム工学科においてアンケートシステムを用いた実験を行う．そのアンケートの集計結果を考察し，作成するセキュリティ診断の評価・見直しを行う．考察とセキュリティ診断の評価・見直しを第 5.2.1 節と第 6 章で述べる．

第 4 章

菊池研究室セキュリティポリシー文書の作成

本章では，アンケートシステムの構築における菊池研究室のセキュリティポリシー文書の作成について述べる．

4.1 セキュリティポリシー文書作成における実験内容

アンケートシステムを作成するために，菊池研究室において，セキュリティポリシー策定を基板としたセキュリティ規格 BS7799 を試行した．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．

4.2 リスクアセスメント

まず，リスクアセスメントとして菊池研究室に対してのリスク分析を行った．リスク分析を行うにあたって，情報資産，脅威，脆弱性の洗い出しを行った．脆弱性の洗い出しでは，アンケートをし調査した．第 4.3 節でアンケート内容と結果を示す．

- 情報資産の洗い出し
  - 菊池研における情報資産は，研究内容である．
  - 情報資産のある場所は，菊池研究室 (高知工科大学 A 棟 A311,A312) である．
  - 情報資産の状態は，紙媒体 (研究データ)，電子媒体 (メール，研究データ，研究室

のネットワーク情報) である．

- 脅威の洗い出し
  - 菊池研究室における脅威には，外部からの脅威，内部からの脅威，その他の 3 つに分ける．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てはまる．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表 4.1 に列挙した．

表 4.1　菊池研究室における脅威

	脅威
悪意による脅威	データの持ち出し，破壊，改ざん
	不正アクセス
	盗難，盗聴
	情報口外
	コンピュータウィルス
過失による脅威	データの破壊，機器破損
	ウィルス 2 次感染
	見ず知らずの人を部屋にいれたトラブル
	情報漏洩
自然災害による脅威	データの破壊，機器破損

- 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．菊池研究室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．この調査では，主にアンケートが用いられる．アンケートはセキュリティの現状がどのようなものかを知る効果的な方

法である．アンケート調査の結果，菊池研究室のセキュリティ意識は低いと判断した．次節で，アンケート内容と結果を示す．

4.3　アンケート内容と結果

菊池研究室の学生 13 名を対象に，ある脅威に対する意識レベルを調べる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．また，そのアンケートの選択肢と，起こり得る脅威についても示す．また，アンケート調査の結果を表 4.2 にまとめた．

1. 設問：研究室に業者と名乗る見ず知らずの人が作業にきた場合，次のうちあなたはどの行動をとりますか？
   選択肢：すぐ入れる，担当者に確認をとってから入れる，入れない，どちらでもない
   脅 威：見ず知らずの人を入れたトラブル
2. 設問：研究室から個人に割り当てられたパソコンを他人に貸したり，他人が使用したことはありますか？
   選択肢：ある，ない，どちらでもない
   脅 威：データの持ち出し，破壊，改ざん，情報漏洩
3. 設問：差出人不明のメールを研究室のマシンから受け取った場合，あなたならどうしますか？読みますか，読みませんか？
   選択肢：読む，読まない，どちらでもない
   脅 威：コンピュータウィルス
   (a) 設問：読むと答えた人に質問です．そのメールにファイルが添付されていた場合，そのファイルを開きますか？
   選択肢：はい，いいえ
   脅威：コンピュータウィルス
4. 設問：あなたは研究室のマシン上で違法だと思われる行為をしたことがありますか？
   選択肢：ある，ない，どちらでもない

脅 威：データの破壊，コンピュータウィルス

5. 設問：研究室で使っているマシンにインターネットからソフトウェアをダウンロードしたことがありますか？

   選択肢：ある，ない，どちらでもない

   脅 威：データの破壊，機器破損

6. 設問：他人に研究室のマシンに入るための login パスワードを教えたことはありますか？

   選択肢：ある，ない，どちらでもない

   脅 威：不正アクセス，情報の漏洩，盗聴・盗難

7. 設問：研究室のマシンに入るための login パスワードをメモしたことがありますか？

   選択肢：ある，ない，どちらでもない

   脅 威：情報の漏洩，盗聴・盗難，不正アクセス，データの持ち出し

8. 設問：研究室のマシンに入るための login パスワードは何文字ですか？□の中に数字を書いてください.

   □文字

   脅 威：盗聴・盗難，不正アクセス，情報の漏洩，破壊

9. 設問：Ａ－ＷＳのマシンの login パスワードと研究室のマシンの login パスワードは同じですか？

   選択肢：同じパスワード，違うパスワード，どちらでもない

   脅 威：情報の漏洩，盗聴・盗難，不正アクセス，データの持ち出し

10. 設問：自分のホームページに自分の住所，学校のメールアドレス，携帯番号（PHS，自宅の電話番号)，自分の顔の内どちらか一つでものせているものはありますか？

    選択肢：はい，いいえ，どちらでもない

    脅 威：情報漏洩，改ざん，不正アクセス，データの持ち出し

4.3　アンケート内容と結果

表 4.2　菊池研究室のアンケート結果

問 *1.* 見ず知らずの人を部屋に入れるか	すぐいれる	確認してから	入れない	どちらでもない
	2	11	1	2
問 *2.* 研究室から個人に割り当てられたパソコンを他人に貸したことがあるか	はい	いいえ	どちらでもない	
	9	6	1	
問 *3.* 差出人不明のメールを受け取った場合どうするか	読む		読まない	
	9		6	
問 *3-1.* 読むと答えた人に質問. そのメールにファイルが添付されていた場合，どうするか	開く		開かない	
	2		9	
問 *4.* あなたは研究室のマシンで違法行為をしたことがあるか	はい	いいえ	どちらでもない	
	3	11	2	
問 *5.* インターネットからソフトウェアをダウンロードしたことがあるか	はい	いいえ	どちらでもない	
	13	0	2	
問 *6.* ログインパスワードを教えたことがあるか	ある		ない	

	1		15
問 *7.* ログインパスワードをメモしたことがあるか	ある		ない
	4		12
問 *8.* ログインパスワードは何文字か	6 文字	8 文字	9 文字以上
	2	10	4
問 *9. A-WS* と研究室のログインパスワードは同じか	同じパスワード	違うパスワード	どちらでもない
	6	9	1
問 *10.* 自分のホームページに本名，学校名，学校のメールアドレス，自分の顔のうちどれか一つでものせているものはあるか	はい		いいえ
	13		3

4.4　リスク評価

リスク分析の結果をもとに，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．表 4.3，4.4，4.5 のように，悪意を持った者により起こりえる脅威，過失によって起こりえる脅威，その他によって起こりえる脅威の 3 つに分けリスク評価をした．リスク評価の基準として，リスクの高い順に A，B，C の 3 つの段階に分け，頻度，被害の大きさの観点から評価した．

表 4.3　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	B	B	B
盗難，盗聴	C	A	B
情報口外	B	C	C
コンピュータウィルス	B	A	A

表 4.4　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	C	A	B
ウィルス *2* 次感染	C	B	B
見ず知らずの人を部屋に入れたトラブル	C	B	B
情報漏洩	B	C	C

表 4.5　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

4.5　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をもとに，セキュリティ管理の方針・規定としてセキュリティポリシー文書を作成した．原文は，付録 A.1 に記載する．

本来 BS7799 においてセキュリティポリシー文書は，基本ポリシー，スタンダード，プロ

シージャの 3 層に分けて策定することが定められている．スタンダードには，組織全体での共通の規定を記述し，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．しかし今回は，対象が研究室であり，BS7799 で想定する組織規模に比較して小さい．研究室で 3 層に分けて策定してしまうと，個人個人に対する具体的な手順までをセキュリティ文書に書くことになってしまうので，策定・運用に対するコストがかかってしまう．そこで，スタンダードとプロシージャを合わせて 2 層に分けて策定することにした．

以下に実際に策定したポリシーの一部を掲載する．

- 基本ポリシー
  - 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．
  - 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．
- スタンダード＆プロシージャ
  - 誰もいない場合は，ドアや窓は施錠すること．
  - 個人が管理しているマシンについては，管理者が責任をもつこと．
  - 研究室内から個人に割り当てられたコンピュータを自分がいないときに他人にさわらせないこと．

第 5 章

アンケートシステムを用いての情報システム工学科 (研究室) の検証

本章ではアンケートシステムの構築とそれを用いた情報システム工学科における実験について述べる．まず，第 4 章で作成したセキュリティポリシー文書を基にアンケートシステムの構築を行った．次にアンケートシステムを用いて情報システム工学科において実験をし，セキュリティ診断の評価・見直しを行うために，アンケートの集計結果を考察した．

5.1　PHP によるアンケートシステムの構築

本節では，PHP によって構築したアンケートシステムについて述べる．システムの概要を図 5.1 で示す．まず，被験者にアンケートをしてもらいその解答から分析した結果，セキュリティアドバイスがでてくる仕組みとなっている．また，アンケート結果や研究室・学年についてはファイルに蓄積することとした．この分析方法は，菊池研究室のセキュリティポリシー文書のプロシージャ＆スタンダード (付録 A.1 参照) を基に行った．

5.1.1　アンケート設問内容

菊池研究室で行ったアンケートは，菊池研究室セキュリティポリシー文書から情報システム工学科 (研究室) で必要であると思われる部分を選び，アンケートを作成した．アンケート内容は以下の通りである．

5.1　PHP によるアンケートシステムの構築

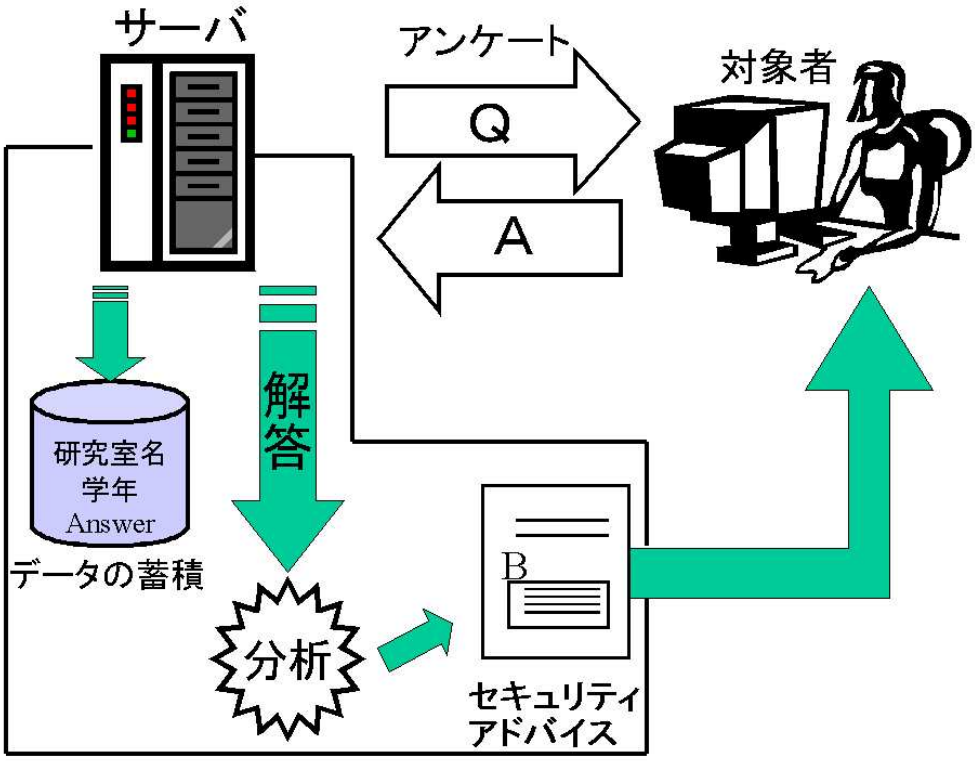

図 5.1　アンケートシステムの構成図

1. 設問：研究室に業者と名乗る見ず知らずの人が作業にきた場合，次のうちあなたはどの行動をとりますか？

   選択肢：すぐ入れる，担当者に確認をとってから入れる，入れない，どちらでもない
2. 設問：研究室から個人に割り当てられたパソコンを他人に貸したり，他人が使用したことはありますか？

   選択肢：ある，ない，どちらでもない
3. 設問：差出人不明のメールを研究室のマシンから受け取った場合，あなたならどうしますか？

   選択肢：読む，読まない，どちらでもない

   (a) 設問：読むと答えた人に質問です．そのメールにファイルが添付されていた場合，そのファイルを開きますか？

   選択肢：はい，いいえ

4. 設問：研究室で使っているマシンにウィルス対策ソフトをいれていますか？
   選択肢：はい，いいえ，どちらでもない
5. 設問：あなたは研究室のマシン上で違法だと思われる行為をしたことがありますか？
   選択肢：ある，ない，どちらでもない
6. 設問：他人に研究室のマシンに入るための login パスワードを教えたことはありますか？
   選択肢：ある，ない，どちらでもない
7. 設問：研究室のマシンに入るための login パスワードは何文字ですか？
   選択肢：パスワード数
8. 設問：Ａ－ＷＳのマシンの login パスワードと研究室のマシンの login パスワードは同じですか？
   選択肢：同じパスワード，違うパスワード，どちらでもない
9. 設問：自分のホームページに自分の住所，学校のメールアドレス，携帯番号（PHS，自宅の電話番号），自分の顔の内どちらか一つでものせているものはありますか？
   選択肢：はい，いいえ，どちらでもない
10. 設問：あなたの研究室で共有しているものは，物品管理をしていますか？
    選択肢：はい，いいえ，どちらでもない
11. 設問：あなたの研究室は何らかのセキュリティ教育を実施していますか？
    選択肢：はい，いいえ，どちらでもない

5.1.2　アンケートの Web 上の表示方法

アンケートの Web ブラウザ上での表示例を図 5.2 に示す．研究室と学年はプルダウンメニューで選択するようにし，打ち間違いを防いだ．また，質問に対する答えの選択については，ラジオボタンにより回答できるようにした．パスワード数を答える問題では，選択数が多いため，ラジオボタンではなく，プルダウンメニューでの選択にした．

また，今後のアンケート改良の参考とするため，メールで意見を募集することにした．

5.1　PHP によるアンケートシステムの構築

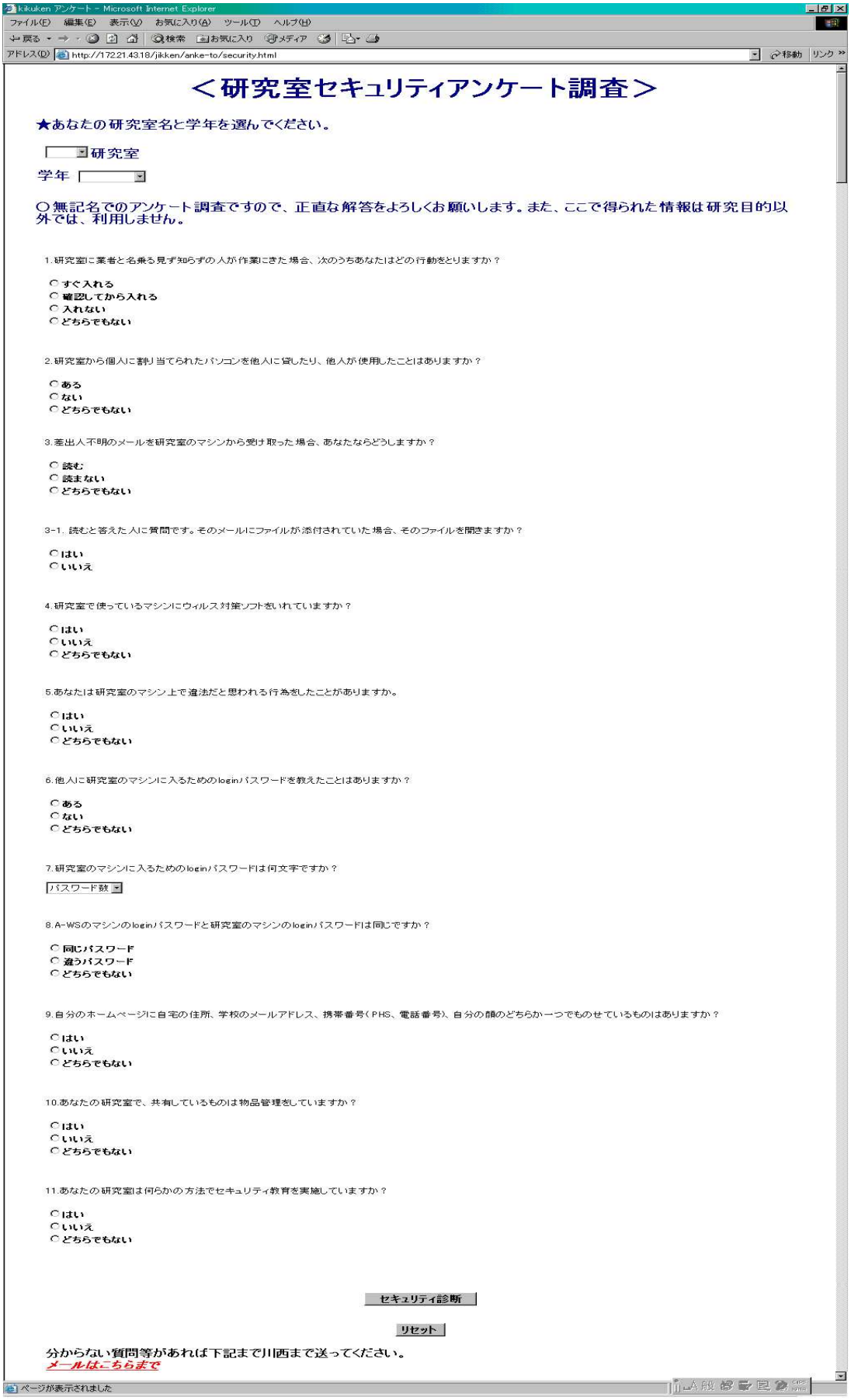

図 5.2　Web 上でのアンケート表示例

5.1.3　セキュリティ診断の Web 上の表示方法

セキュリティ診断結果はセキュリティレベルとセキュリティアドバイスを表示する．まず，被験者のセキュリティレベルを評価の高い順に ABCDE の段階で表示する (表 5.1)．セキュリティレベルは，対象者が選んだアンケートの解答によって，数字を換算しその合計により決定するようにした．本研究で作成したセキュリティアンケートの表示例を図 5.3 で示す．

表 5.1　セキュリティレベルの評価

レベル	評価点
A	3 点以下
B	4 点〜7 点
C	8 点〜13 点
D	14 点〜18 点
E	19 点以上

次に，設問の解答に対するアドバイスについてはスタンダード＆プロシージャを基に作成した．以下にその具体例を示す．また，セキュリティレベルの段階分けをするためにアンケートの設問の解答においてリスクの高い順に「＋ 3」,「＋ 2」,「＋ 1」の段階でセキュリティレベルに換算する．

- アンケート 1.「研究室に業者と名乗る見ず知らずの人が作業にきた場合，次のうちあなたはどの行動をとりますか？」

  「すぐ入れる」にチェックした場合,「知らない人を入れる場合は，必ず確認してから入れるようにしましょう．業者と偽った犯罪を犯すケースが増えています．注意してください」というアドバイス文章を表示する．

  「すぐ入れる」にチェックした場合は「＋ 3」を,「入れない」にチェックした場合は「＋ 1」をセキュリティレベルに換算する．

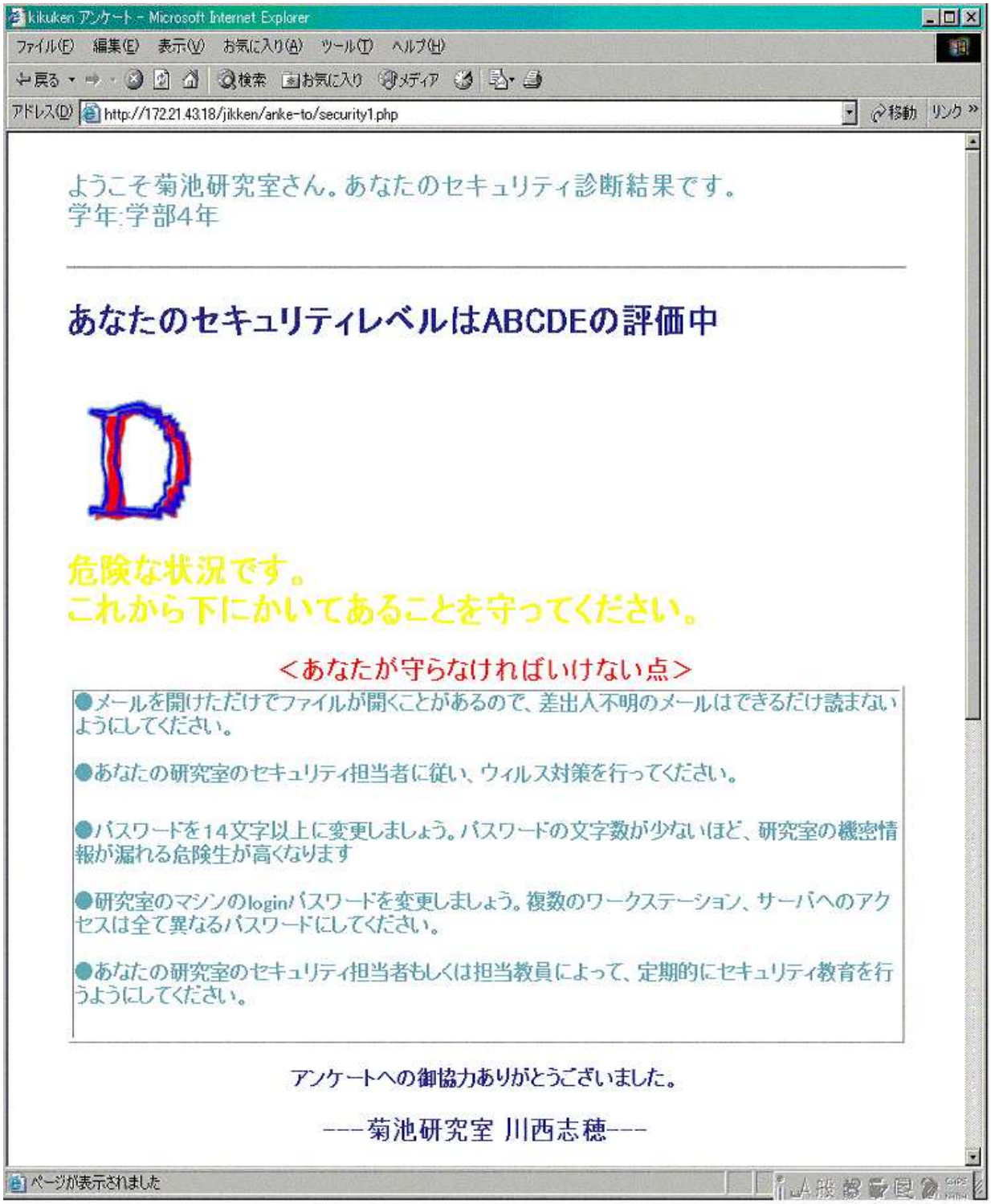

図 5.3　セキュリティ診断結果の表示例

- アンケート 2.「研究室から個人に割り当てられたパソコンを他人に貸したり，他人が使用したことはありますか？」

  「ある」にチェックをした場合,「研究室のパソコンを他人に貸すときや他人が使用する場合は，自分が見ている所で操作してもらうようにしましょう．研究室のコンピュータを第 3 者によって，悪用される危険性があります.」が表示され，セキュリティレベルには「＋ 2」を換算させる．
- アンケート 3「差出人不明のメールを研究室のマシンから受け取った場合，あなたならどうしますか？」

  アンケート 3-1.「読むと答えた人に質問です．そのメールにファイルが添付されていた場合，そのファイルを開きますか？」

  第 3 問で「読む」にチェックをし，3-1 問で「はい」にチェックをした場合には「差出人不明のメールを受け取った場合，できるだけ開けないようにしましょう．また，ファイルが添付されていた場合，ファイルにウィルスが入っていることがあるので，開けないようにしましょう」を,「いいえ」にチェックをした場合には「メールを開けただけでファイルが開くことがあるので，差出人不明のメールはできるだけ読まないようにしてください.」と表示する．

  また，第 3-1 問で「はい」にチェックした場合「＋ 3」を,「いいえ」にチェックした場合は,「＋ 2」をセキュリティレベルに換算する．
- アンケート 4.「研究室で使っているマシンにウィルス対策ソフトをいれていますか？」

  「いいえ」にチェックをした場合,「あなたの研究室のセキュリティ担当者に従い，ウィルス対策を行ってください」と表示し，セキュリティレベルには「＋ 2」を換算する．
- アンケート 5.「あなたは研究室のマシン上で違法だと思われる行為をしたことがありますか.」

  「はい」にチェックした場合，セキュリティレベルに「＋ 2」を換算する．
- アンケート 6.「他人に研究室のマシンに入るための login パスワードを教えたことはありますか？」

「ある」にチェックした場合,「パスワードを他人に教えてはいけません．教えた場合や，知られた可能性がある場合はすぐに変更しましょう」が表示され，セキュリティレベルには「＋ 1」を換算する．

- アンケート 7.「研究室のマシンに入るための login パスワードは何文字ですか？」

  「5 文字以下」から「12 文字」の間でチェックした場合は,「パスワードを 14 文字以上に変更しましょう．パスワードの文字数が少ないほど，研究室の機密情報が漏れる危険生が高くなります」と表示する．

  – 5 文字以下〜6 文字

    セキュリティレベルに「＋ 3」換算

  – 7 文字〜8 文字

    セキュリティレベルに「＋ 2」換算

  – 9 文字〜12 文字

    セキュリティレベルに「＋ 1」換算

- アンケート 8.「A-WS のマシンの login パスワードと研究室のマシンの login パスワードは同じですか？」

  「同じパスワード」にチェックした場合,「研究室のマシンの login パスワードを変更しましょう．複数のワークステーション，サーバへのアクセスは全て異なるパスワードにしてください.」と表示し，セキュリティレベルには,「＋ 2」換算する．

- アンケート 9.「自分のホームページに自宅の住所，学校のメールアドレス，携帯番号 (PHS，電話番号)，自分の顔のどちらか一つでものせているものはありますか？」

  「はい」にチェックをした場合,「自分のホームページに自分の住所，学校のメールアドレス，電話番号などの個人情報や研究室の機密情報を載せてはいけません．ただちに省いたほうがよいでしょう」と表示し，セキュリティレベルには,「＋ 1」換算する．

- アンケート 10.「あなたの研究室で，共有しているものは物品管理をしていますか？」

  「いいえ」にチェックした場合,「いますぐにでも研究室内で相談し，物品管理を行うようにしてください．また，研究内容の書かれた書類の管理も行うようにしましょう」と

表示し，セキュリティレベルには「＋ 2」換算する．

- アンケート 11.「あなたの研究室は何らかの方法でセキュリティ教育を実施していますか？」

  「いいえ」にチェックした場合,「あなたの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，定期的にセキュリティ教育を行うようにしてください.」と表示し，セキュリティレベルは「＋ 3」換算する．

5.2　アンケートシステムを用いての実験

第 5.1 節で作成したアンケートシステムを用いて情報システム工学科 (研究室) において実験を行い，考察した．この実験では，研究室所属学生の 74 %の人から協力を得ることができた．次節からアンケート調査の結果と考察を述べる．

5.2.1　アンケート調査の結果と考察

セキュリティ診断の評価・見直しを行うために，アンケートの集計結果 (表 5.2，図 5.4 ～図 5.15) から考察した．このグラフや表を基に行った考察をアンケート 1 から順に列挙する．

- アンケート 1.「研究室に業者と名乗る見ず知らずの人が作業にきた場合，次のうちあなたはどの行動をとりますか？」の結果 (図 5.4).

  図 5.4 によると，各研究室とも同じような結果であることが分かる．また,「確認してから入れる」という回答が大半を占めており，セキュリティレベル面では良い結果であったと考える．しかし,「すぐ入れる」と答えた人も全体の１０%以上を占めており，あまり，良い結果であるとは言えない.
- アンケート 2.「研究室から個人に割り当てられたパソコンを他人に貸したり，他人が使用したことはありますか？」の結果 (図 5.5).

  図 5.5 によると，研究室によって，結果は様々で，大体の研究室は,「ある」より「な

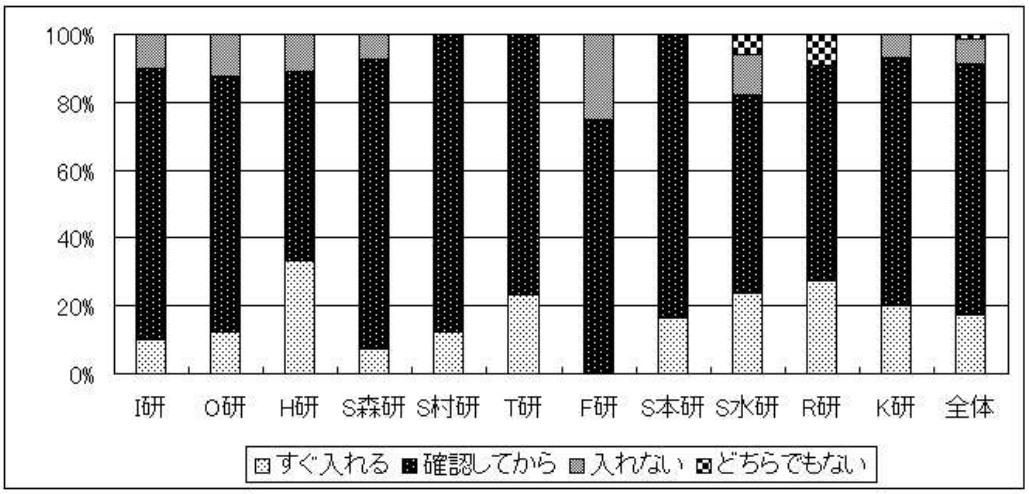

図 5.4　業者と名乗る見ず知らずの人がきた場合の対応

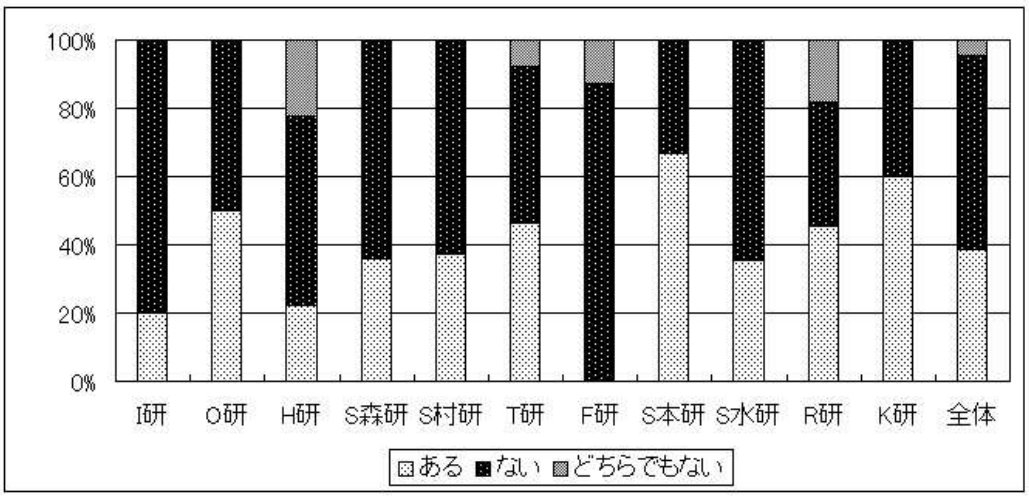

図 5.5　研究室のパソコンの他人による使用の有無

い」という割合の方が多くなっている．また，全体のグラフをみると，約 40 %の人が「ある」と答えていることがわかる．この結果は，セキュリティ意識の低さを物語っていると考える．

- アンケート 3.「差出人不明のメールを研究室のマシンから受け取った場合，あなたならどうしますか？」 アンケート 3-1.「読むと答えた人に質問です．そのメールにファイルが添付されていた場合，そのファイルを開きますか？」の結果 (図 5.6 と図 5.7).

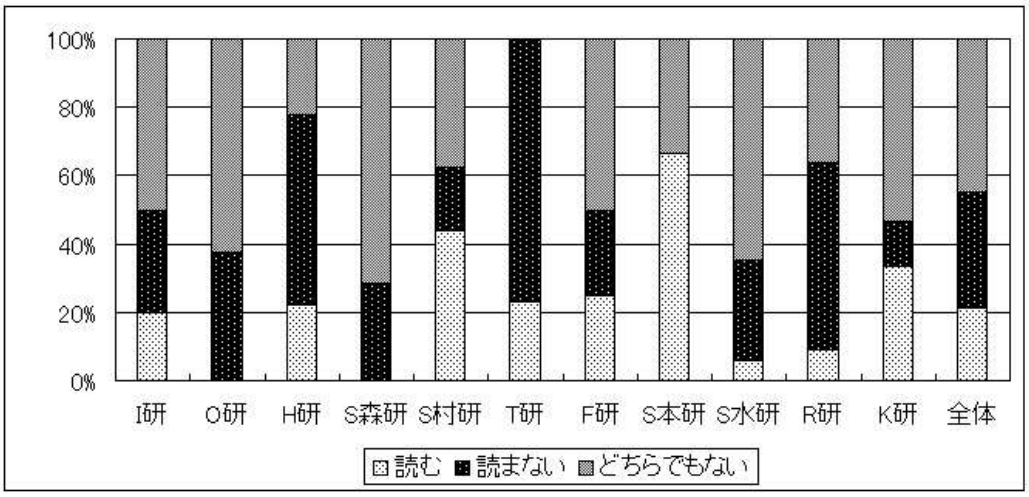

図 5.6　差出人不明のメールを受け取った場合の対応

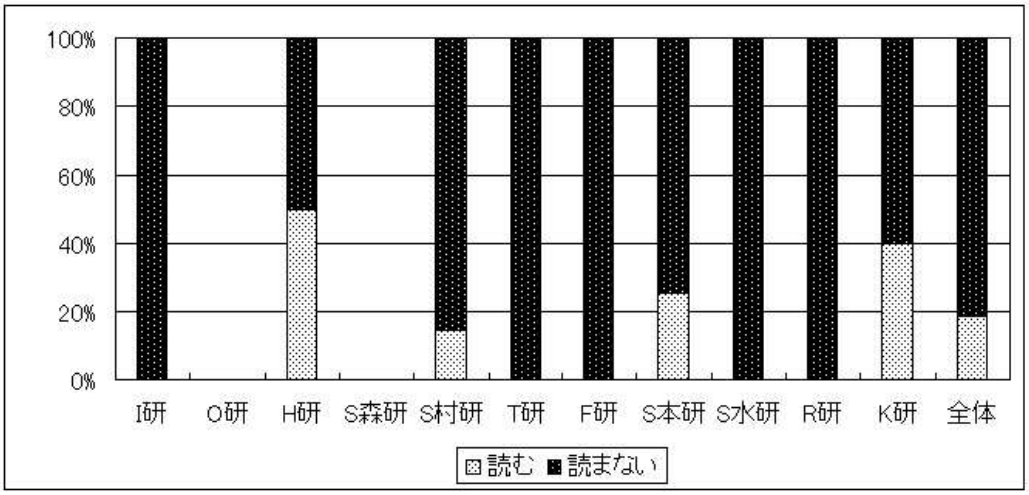

図 5.7　メールにファイルが添付されていた場合の対応

図 5.6 によると，研究室によって違う結果がでている．「読む」と答えた人が多い研究室もあれば，「読まない」と答えた人が多い研究室もあった．また，全体のグラフによると「いいえ」と答えた人が約 20 %以上いた．メールを開けただけで，ウィルスに感染してしまうというケースが多くあるため，注意をする必要がある．

また，図 5.7 によると，すべての人が「読む」と答える研究室と「読まない」と答える研究室が少し含まれている場合とで分かれた結果になっている．

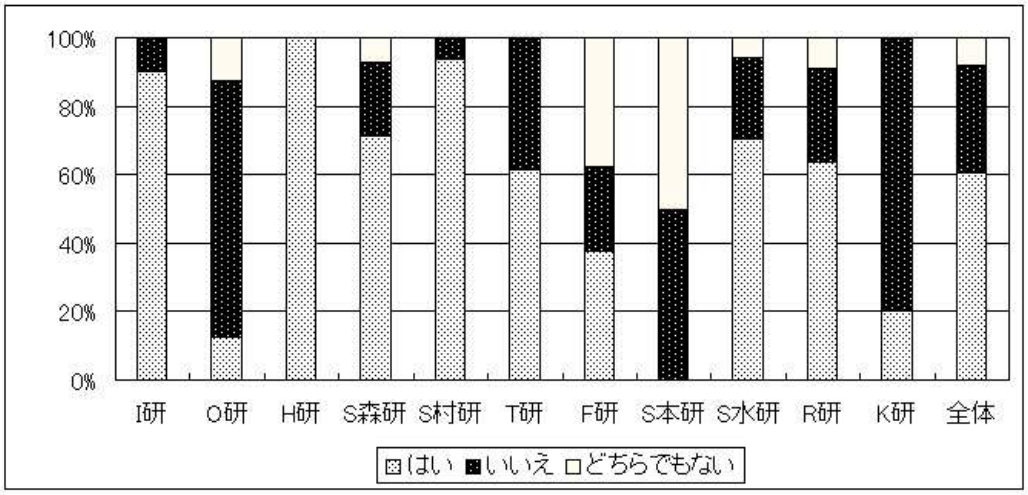

図 5.8　ウィルス対策ソフトをいれているかどうか

- アンケート 4.「研究室で使っているマシンにウィルス対策ソフトをいれていますか？」の結果 (図 5.8).

  図 5.8 によると，ウィルス対策ソフトを入れている研究室と入れていない研究室の差があることが分かる．また，全体のグラフからみて分かるように，「はい」と答えた人は，全体の 6 割以上である．

- アンケート 5.「あなたは研究室のマシン上で違法だと思われる行為をしたことがありますか.」の結果 (図 5.9).

  図 5.9 によると，ほとんどの人が研究室での違法行為をしていないという結果になった．全体のグラフを見ると，10 %の人が，違法行為を行ったことがあるということが分かった.

- アンケート 6.「他人に研究室のマシンに入るための login パスワードを教えたことはありますか？」の結果 (図 5.10).

  図 5.10 によると，90 %以上の人がログインパスワードを教えたことがないという結果になった.

- アンケート 7.「研究室のマシンに入るための login パスワードは何文字ですか？」の結果 (図 5.11).

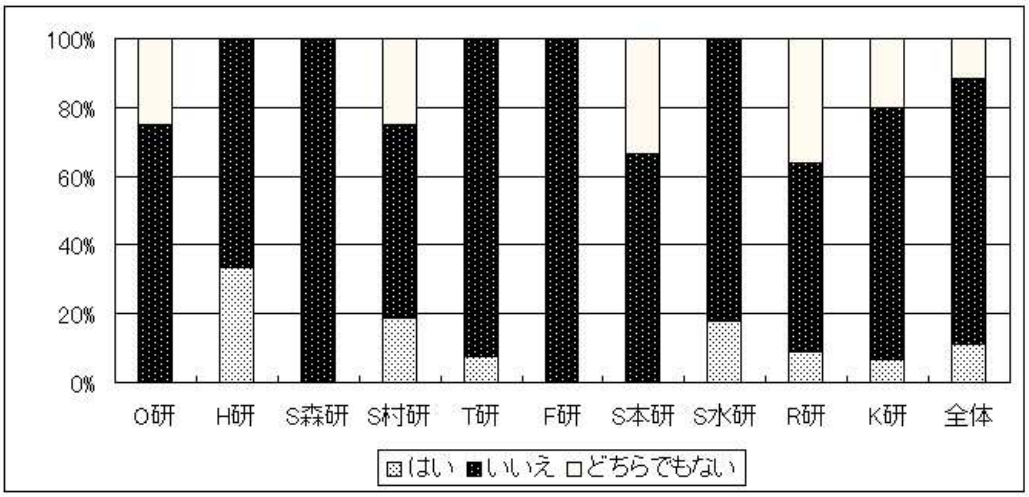

図 5.9　研究室での違法行為をしたことがあるか

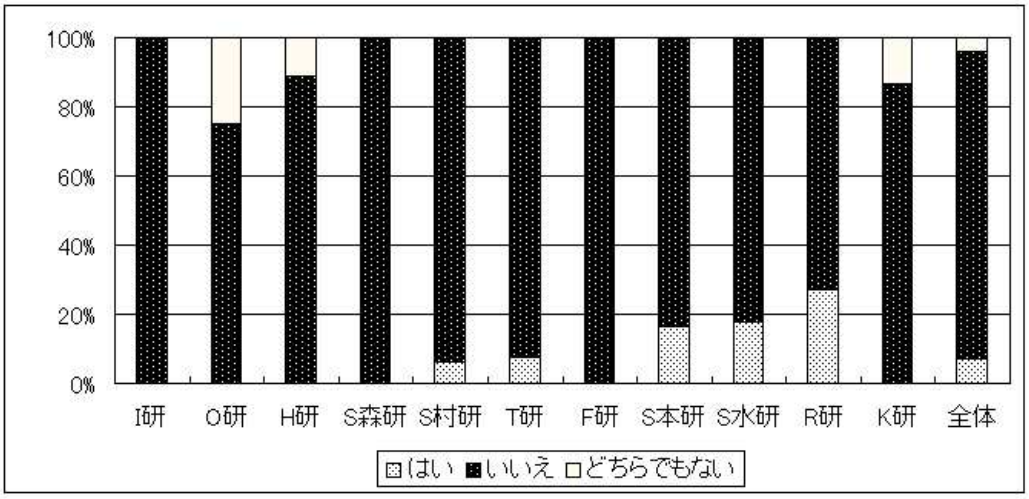

図 5.10　ログインパスワードを教えたことがあるか

図 5.11 によると，パスワード数が 8 文字の人が 50 %以上であることが分かる．これは，入学当初のコンピュータリテラシーの時間でパスワードは 8 文字以上と言われたことからでた結果であると推測する．

- アンケート 8.「A-WS のマシンの login パスワードと研究室のマシンの login パスワードは同じですか？」の結果 (図 5.12).

  図 5.12 研究室によって異なった結果がでており，研究室ごとのセキュリティに対する

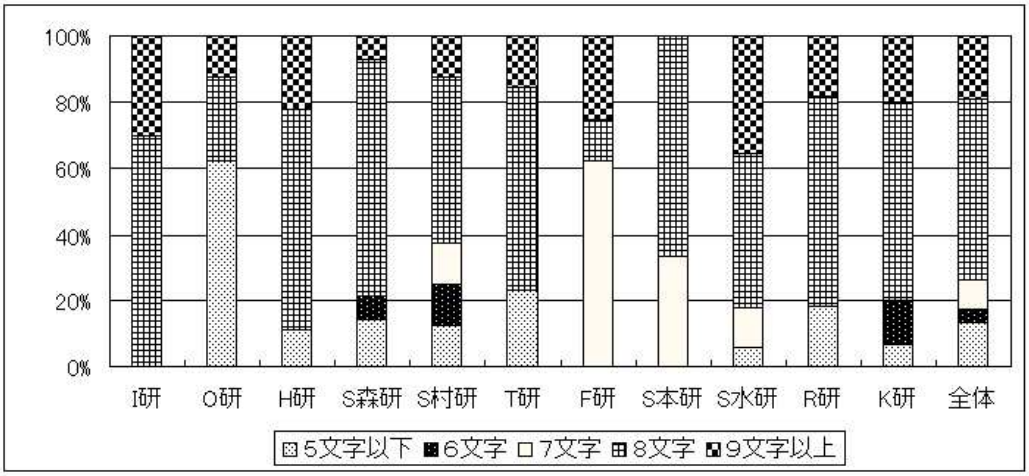

図 5.11　ログインパスワードは何文字か

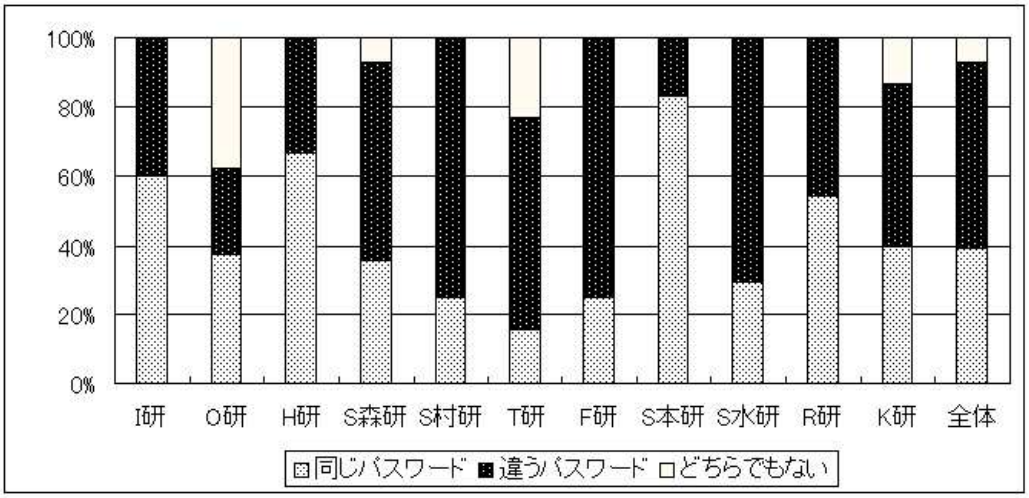

図 5.12　A-WS と研究室のマシンのパスワードは同一であるか

意識の差があることが感じられる．また，全体のグラフによると，「同じパスワード」と答えた人が 4 割おり，セキュリティ意識の甘さがうかがえる．

- アンケート 9.「自分のホームページに自宅の住所，学校のメールアドレス，携帯番号 (PHS，電話番号)，自分の顔のどちらか一つでものせているものはありますか？」の結果 (図 5.13).

  全体のグラフによると，「はい」と答えた人と「いいえ」と答えた人が半々という結果になった．ホームページに乗せた内容から，情報が流出す，研究内容の漏洩につながる

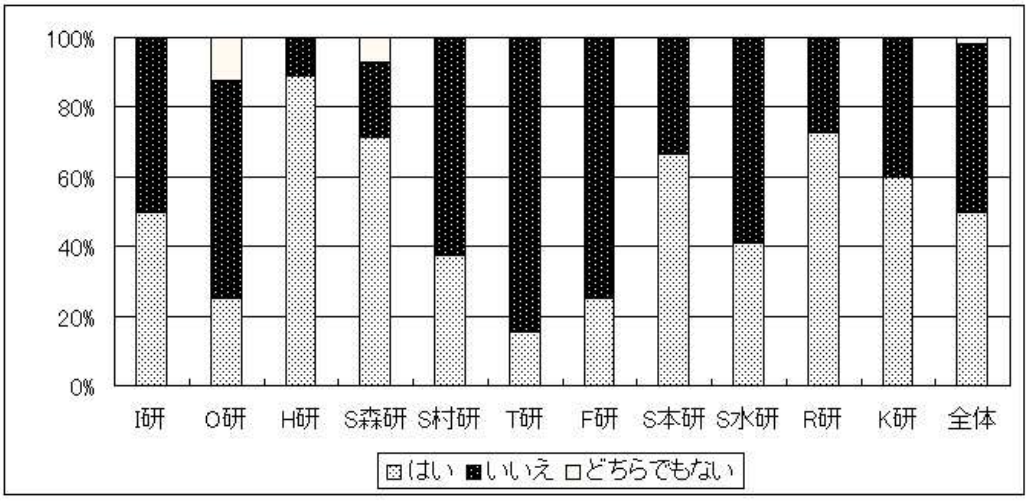

図 5.13　ホームページに自宅の住所などの個人情報を載せているか

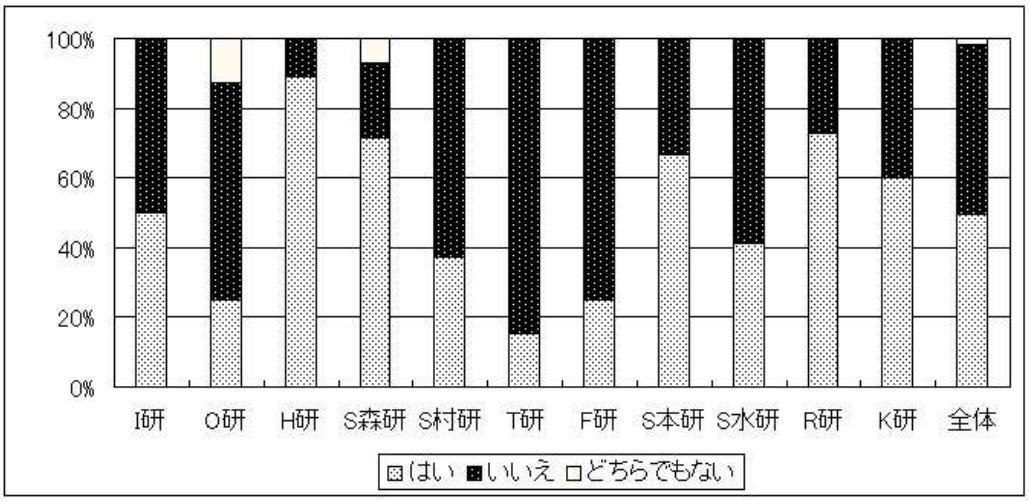

図 5.14　研究室で物品管理を行っているか

ということが考えられるので，注意が必要である．

- アンケート 10.「あなたの研究室で，共有しているものは物品管理をしていますか？」の結果 (図 5.14).

  全体のグラフをみてわかるように，物品管理については，半分が物品管理ができていることが分かる．しかし，研究室によって，意識の違いが生じているので，あまり正確なデータではないことが分かる．

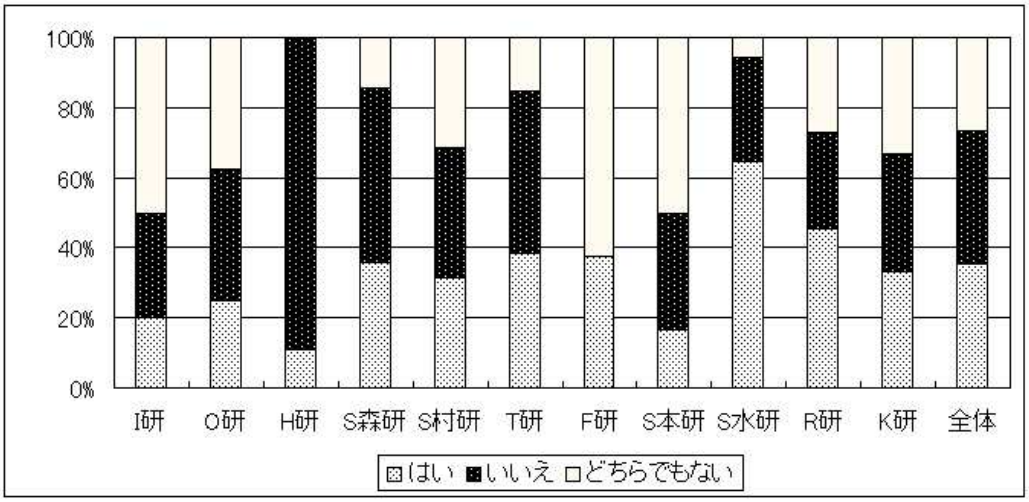

図 5.15　セキュリティ教育を実施しているか

- アンケート 11.「あなたの研究室は何らかの方法でセキュリティ教育を実施していますか？」の結果 (図 5.15).

  セキュリティ教育の実施は，できていないところが多いという結果になった．また，研究室ごとのグラフから見て分かるように，同じ研究室であるにもかかわらず，意識の差がでてきていることが分かる．これは，研究室の教育不足であると考える．

5.2.2　セキュリティレベルの集計結果

アンケートのセキュリティレベル最大値における各研究室，学年別のセキュリティレベルの割合を図 5.16 と図 5.17 で示す．

この数値は [セキュリティレベルを集計した結果] ÷ (アンケートにおけるセキュリティレベル最大値×人数) において出したパーセンテージである．また，図 5.17 をもとに作成した研究室の順位を下記に示す．この図 5.17 から，研究室によってセキュリティリスクに差があることが分かる．また，F 研究室と S 本研究室は同じ部屋であるのにセキュリティレベルに差がでている．また，学年別にみるとセキュリティリスクに差がないことが分かった (図 5.16).

5.2　アンケートシステムを用いての実験

1. F 研究室
2. I 研究室
3. S 水研究室
4. R 研究室
5. S 森研究室
6. T 研究室
7. S 村研究室
8. O 研究室
9. K 研究室
10. H 研究室
11. S 本研究室

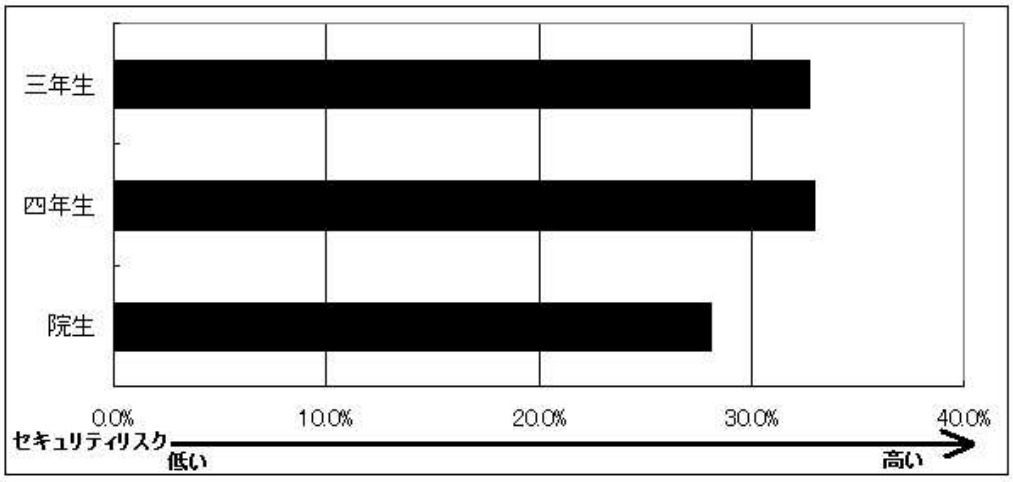

図 5.16　学年別のセキュリティリスク

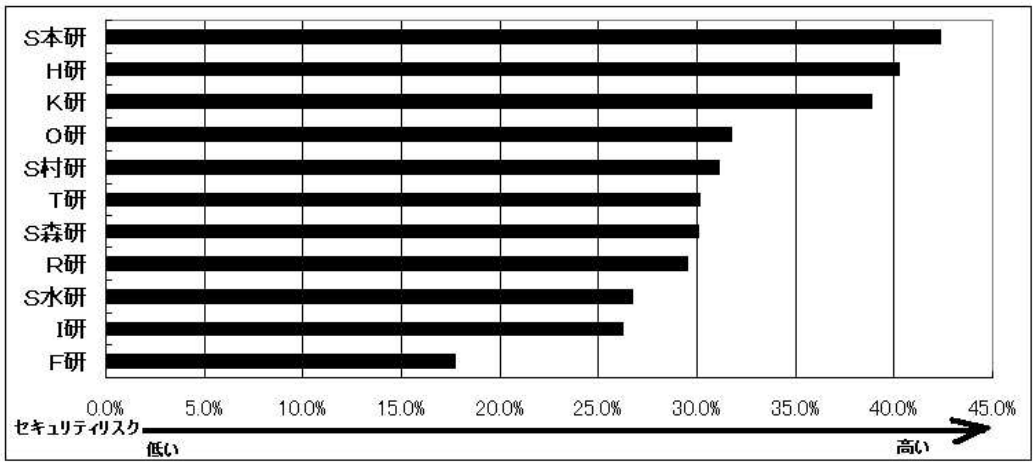

図 5.17　各研究室のセキュリティリスク

表 5.2　情報システム工学科のアンケート結果

問 *1.* 見ず知らずの人を部屋に入れるか	すぐいれる	確認してから	入れない	どちらでもない
	22	93	9	2
問 *2.* 研究室から個人に割り当てられたパソコンを他人に貸したことがあるか	はい	いいえ	どちらでもない	
	49	71	6	
問 *3.* 差出人不明のメールを受け取った場合どうするか	読む	読まない	どちらでもない	
	27	43	57	
問 *3-1.* 読むと答えた人に質問. そのメールにファイルが添付されていた場合，どうするか	開く		開かない	
	5		22	
問 *4.* 研究室で使っているマシンにウィルス対策ソフトを入れていますか	はい	いいえ	どちらでもない	
	70	40	10	
問 *5.* 研究室のマシンで違法行為をしたことがあるか	はい	いいえ	どちらでもない	
	14	98	15	
問 *6.* ログインパスワードを教えたことがあるか	はい	いいえ	どちらでもない	

	9		113		5
問 *7.* ログインパスワードは何文字か	5 文字以下	6 文字	7 文字	8 文字	9 文字以上
	13	5	8	78	23
問 *8. A-WS* と研究室のログインパスワードは同じか	同じパスワード		違うパスワード		どちらでもない
	48		70		9
問 *9.* 自分のホームページに自宅の住所, 学校のメールアドレス, 携帯番号，自分の顔のうちどれか一つでものせているものはあるか	はい		いいえ		どちらでもない
	63		62		2
問 *10.* 研究室で共有しているものは物品管理をしているか	はい		いいえ		どちらでもない
	89		21		17
問 *11.* セキュリティ教育を実施しているか	はい		いいえ		どちらでもない
	45		48		34

5.2.3　アンケート集計結果の考察のまとめ

アンケートの問題によって，答え方が各研究室とも同じような結果である場合と違う場合とがあった．このことから，研究室別にセキュリティ診断を変える必要があると考えた．また，セキュリティレベル別にみると，各研究室によって差があることが確認できた．

研究室の物品管理やセキュリティ教育の実施などについては，同じ研究室であるにもかかわらず，意識の差がでているという結果が得られた．

第 6 章

考察

本章では，アンケートシステムを用いた策定手順の提案と今回行った実験においての考察を述べる．

6.1　アンケートシステムの考察

提案手法に基づいてアンケートシステムを用いた実験を行い，情報システム工学科でアンケートシステムを用いて運用することができた．また，研究室所属学生の 74 %がセキュリティアンケートを行った．これは，情報システム工学科において第 3.5 節の図 3.2 のサイクルが機能したということにつながる．これにより，本研究の目的である大学生が容易にセキュリティレベルを向上させることができるセキュリティポリシーを策定することができたと考える．また，大学におけるセキュリティポリシーの問題点においても，このシステムによりカバーできることを再確認した．まず，「人的・時間的コストがかかる」という面では，システムを作ることで，セキュリティ文書を作成するコストや運用・管理に伴うコストが軽減される．次に「学生がセキュリティ文書を読まない」という面では，学生にホームページでアンケートをしてもらうことが，セキュリティ文書を読むという動作と同じなのでこの問題を解決できたと考える．

6.1.1　アンケートシステムの利点と欠点

情報システム工学科でアンケートを実施したことにより分かった，アンケートシステムの利点と欠点を述べる．

- 利点
  - 学生がセキュリティに対して関心をもち，セキュリティレベルをあげることができる．
  - その場ですぐ結果がでるので，学生がセキュリティに対して関心をもつ．
  - Web 上でのセキュリティポリシーであるため，アンケート用紙の収集等の管理コストがかからない．もし，Web 上でなければ，アンケートのコピー用紙のコストや，それを配ったり収集したりする時間的・人的コストがかかる．
  - 情報システム工学科という構成メンバーが頻繁に入れ替わる場合でも，新しいメンバーが入ってきた場合にアンケートシステムを行えば，セキュリティ対策を行うことができる．
- 欠点
  - 研究室によって環境が違うので，質問があてはまらない場合がある．例えば，問 2 の場合「研究室から個人に割り当てられたパソコンを他人に貸したり，他人が使用したことがありますか」という質問である．研究室から個人に割り当てられたパソコンが他の人との共有物だった場合，この問題に当てはまらなくなってしまう．
  - アンケートに答える場合「どちらでもない」にチェックされた時に，どういう答えであったか集計できない．

6.1.2　アンケートシステムの改良策

前節での欠点等を踏まえ，アンケートシステムの改良案を示す．

- 研究室ごとのセキュリティアンケートシステムを作成する．
  - 今回のアンケート調査を基に，研究室のセキュリティレベルに見合ったアンケートやセキュリティアドバイスをする．
- アンケートに答える場合に「どちらでもない」というチェックボタンの下に書き込みができるテキストエリアを作成し，自分の答えについて書いてもらう．それをしてもらう

ことで，アンケートの改善に役立つ．

- セキュリティアドバイスの際，アドバイスに対しての詳しい説明に飛ぶようなリンクを用意しておく．
- アンケートの質問の聞き方に関しての，不適切な点の改良
  - 問 2 の「研究室から個人に割り当てられたパソコンを他人に貸したり，他人が使用したことはありますか」という問いに対して，自分の管理下で他人が使ったことがある場合はどうしたらよいかという質問がきた．そこで，「研究室から個人に割り当てられたパソコンを他人に貸したり，他人が自分の管理下ではない所で使用したことがありますか」という質問に変更するべきだと考える．
  - 問 3 の質問に対して，「どちらでもない」という解答をする人が多かった．そこで，「ウィルス検出ソフトを使用する」という選択肢を追加したほうがよいと考えた．
  - 問 9 の「自分のホームページに自分の住所，学校のメールアドレス，携帯番号 (PHS，電話番号)，自分の顔のどちらか一つでものせているものはありますか」という問いに対して，学校のメールアドレスと，自分の顔は，授業で作成するホームページに載せる必要があったという意見があった．そこで，「自分のホームページに自分の住所，携帯番号 (PHS，電話番号)，銀行などの口座番号，暗証番号のどちらか一つでものせているものはありますか．という質問に変更すべきだと考える．しかし，自分の顔をホームページ上に載せるということはセキュリティ上，問題である．これは，授業を改善するべきであると考える．

第 7 章

まとめ

本研究では，大学生がセキュリティについて関心を持ち，簡単にセキュリティレベルを向上させることができるセキュリティポリシーを策定することを試みた．そこで，アンケートシステムを構築し，情報システム工学科 (研究室) で実験を行った結果，本研究の目的である大学におけるセキュリティポリシーを策定することができたと考える．

しかし，アンケート結果により，各研究室によってセキュリティレベルに違いがあることが分かった．そこで，本研究の今後の課題は，今回のアンケート結果により，各研究室のリスク分析を行い，第 6.1.2 節のアンケートシステムの改良策を視野に入れながら，各研究室のアンケートシステムを作成することである．そして，情報システム工学科 (研究室) において本格的にアンケートシステムを導入したい．

謝辞

本研究を行うにあたって，多くの方に御協力いただきました．

アンケートシステムを用いた実験では，情報システム工学科の研究室に所属する学生のみなさんに御協力いただきありがとうございました．

菊池研究室の田渕さん，西内さん，舟橋さん，広瀬さん，正岡さん，豊島さん，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．

菊池研究室の金井さん，研究についてのアドバイスをくれたり，励ましてくれてありがとう．

菊池研究室の富永くん，マシンの設定の仕方を教えてくれたり，お菓子をくれてありがとう．

最後に，菊池 豊助教授，本研究の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．

参考文献

[1] 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. 高知工科大学卒業論文, 2001.

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

[4] 澤田明美. 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. 高知工科大学卒業論文, 2002.

付録 A

情報セキュリティポリシー

A.1　菊池研究室セキュリティポリシー

本研究で作成した菊池研究室セキュリティポリシーを以下に掲載する.

菊池研究室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，規定などを明文化したもの

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＆プロシージャ

セキュリティポリシーの一部

A.1　菊池研究室セキュリティポリシー

菊池研究室情報セキュリティ規定と実施手順

２．　目的及び適応範囲

２．１目的

**　菊池研究室の情報資産を，研究員全員でさまざまな脅威から守り，損害を最小限に抑える．**

２．２適応範囲

・　菊池研究室における情報資産

・　情報資産とは，個人情報や菊池研究室における研究に関するすべての情報

・　このセキュリティ管理システムは，菊池研究室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，広範囲の様々な脅威に直面している．菊池研究室も例外ではなく，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，研究生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

菊池研究生全員が，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．菊池研究室にとって，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など

・ すべ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

・ 定期的にセキュリティ教育を行うこと

・ 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，菊池研究室に属する各個人が所有するすべての情報資産は，各個人が責任を持って管理する．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＆プロシージャ

８． 変更履歴

スタンダード＆プロシージャ

１． 定義

スタンダード＆プロシージャは，基本ポリシーを実践するための，規定である．

２． 対象者

菊池研究室に属するすべての者

３．　改定

・　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．

・　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，是認の承認を得ること．

４．　スタンダード＆プロシージャの構成

（１）　セキュリティ組織

（２）　財産に対する責任

（３）　研究室員規制

（４）研究室学生の教育，訓練

（５）安全領域

（６）物理的な出入り管理対策

（７）研究室内で使用するコンピュータの扱い

（８）パスワード

（９）研究室の機密情報の取り扱い

（１０）研究室の電子メールの利用

（１１）www の利用

（１２）コンピュータウィルス対策

（１３）データの暗号化

（１４）ネットワーク環境の変更

（１５）セキュリティ最新情報の収集と配布

（１６）ログの収集と分析

（１７）バックアップ

（１８）セキュリティ事故への対処

（１９）法的要求事項への準拠

（２０）セキュリティポリシーの承諾

（1）　セキュリティ組織

＜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．

＜セキュリティ対策における注意点＞

・研究室での会議

菊池研究室で会議を開き，セキュリティに関する取り決めを明確にすること．

・　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すること．

・　専門家によるセキュリティ助言

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ものが任命されること．

（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

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，維持すること．

○　情報資産の目録はこのような形で記録すること．

・資産識別

・　資産の内容

・　管理者

・ 所有者

・保管場所

（3） 研究室員規則

＜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．

＜規則＞

・ 研究室生は，基本ポリシー，スタンダード，プロシージャを遵守する．

・ 研究内容を外部に漏らさない．

・ 個人が管理しているマシンについては，管理者が責任をもつ．

・ 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になること．

（4）研究室学生の教育，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指示する体制が確実にとれるようにすること．

＜セキュリティ対策における注意点＞

・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，セキュリティ手順および情報処理施設・設備の正しい仕様について訓練を受けること．

（5）物理的な出入り管理対策

＜目的＞

菊池研究室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．

＜セキュリティ対策における注意点＞

・ 研究生がいない場合は，ドアや窓は施錠すること．

・ 研究室への無許可の訪問者は退出させること．

（6） 研究室内で使用するコンピュータの扱い

＜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

＜セキュリティ対策上の注意点＞

・ 研究室から個人に割り当てられたコンピュータを自分がいないときに他人にさわらせない．

・ ログインしたまま席を離れないこと．

（7） パスワード

＜目的＞

許可されていないユーザアクセスを防止するため．

＜規定＞

・ パスワードをメモすることは禁止する．

・ A-WS，K-WS，**菊池研究室，菊池研究室のサーバへのアクセス，管理者パスワードはすべて異なるものにする．**

・ パスワードは１Q **と３**Q **が始まった時に変更する．**

・ パスワード情報が第三者に渡った危険がある場合，速やかにパスワードの変更を行うこと．

・パスワードは他人に教えない．

（8） 研究室の機密情報の取り扱い

＜目的＞

情報資産の機密性を保持する

＜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こと．

（9） 研究室の電子メールの利用

＜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

＜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，なるべく開かない．

（やむをえずメールを開き，ファイルが添付されていた場合は，絶対にそのファイルを読まない）

（１０）WWW の利用

＜目的＞

自作，菊池研究室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．

＜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はない情報

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

電話番号

銀行の口座番号，暗証番号

自分の顔写真

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）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．

＜セキュリティ対策上の注意点＞

・ 菊池研究室の管理者の指示に従って，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 lab のメーリングリストに流す．

・ソフトウェア使用承諾契約書の契約事項の遵守と非認可ソフトウェアの使用を禁止

する．

・ 外部ネットワーク経由で，あるいは，他の媒体より，ファイル及びソフトウェアを入手する場合には，作成元を確認する．作成元が信頼できない場合には入手してはならない．入手する場合には，コンピュータウィルスの検査を行う．

・ 不正ソフトウェアに関する情報を積極的に収集する．

（１２）データの暗号化

＜目的＞

情報の機密性，または完全性を保護すること

＜セキュリティ対策上の注意＞

・ 機密情報が盗聴される恐れのある場合には，暗号化する．

・ 暗号化の方法については，菊池研究室の管理者の指示を受ける．

（１３）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．

＜セキュリティ対策上の注意＞

・ 研究室の既存のネットワーク環境を，変更する場合は，研究室全体で話し合いをし，承諾を得る．

・ 新しいネットワーク環境を構築する場合は，研究室全体で話し合いをし，承諾を得る．

（１４）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．

＜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．

・ 最新情報を入手したら，速やかに `lab` のメーリングリストに流す．

（１５）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．

＜セキュリティ対策上の注意＞

- **常に，ログを収集し，lab のメーリングリストに流す．**
- **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．**

（１６）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．

＜セキュリティ対策上の注意＞

- **研究生各自が定期的に必要なバックアップをとっておく．**

（１７）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

＜規定＞

セキュリティ事故は，事故発見後，速やかに菊池研究生全員に報告されなければならない．

＜事故が起こった場合しなければいけないこと＞

- **菊池豊助教授，研究室管理責任者に連絡**
- **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．**

（１８）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，重大な故障または被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

研究室全体の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．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こと．

（１９）法的要求事項への準拠

＜目的＞

刑事及び民事法，制定法，規制または契約上の義務，並びにセキュリティ上の要求事項の違反を避けること．

＜セキュリティ対策上の注意＞

・ 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．

（２０）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．

＜規定＞

・ 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．