[論文]

# 大学の情報教育における情報セキュリティ教育の研究

星野　隆

〈目　次〉

## 1．概要

今日の日本の大学における情報教育には、大きく分けてテーマが12ある。

1）ハードウェア教育　2）ソフトウェア教育
3）プログラミング教育　4）ネットワーク教育
5）データベース教育　6）マルチメディア教育
7）Web 教育
8）情報システム・経営情報システム教育
9）アプリケーション教育
10）情報数学・統計学・経営科学・数値計算等数理教育
11）情報倫理と情報セキュリティ教育
12）その他情報関連教育

今回の論文のテーマは、11番目の大学における情報セキュリティ教育の問題である。

今日では、インターネット（個人）、イントラネット（企業）、エクストラネット（企業間）やソーシャルネット（公共）とあり、総称してインターネットと呼び世界的規模で普及している。日本人の情報セキュリティ感は、性善説に基づいた考え方から脱却し、充分に情報セキュリティを考慮した考え方に変貌しつつある。

安全な情報システムの条件は、

1）機密性（confidentiality）を備える
2）可用性（availability）を備える
3）完全性（integrity）を備える

以上の3大原則を達成することにある（JIS X 5080:2002）。

情報セキュリティ対策の実施は、社会的責任であり、他人の権利との衝突を避けるべく、ネットワークを利用する各経営体・各組織体や各個人が最低限守るべき規定であり、ルールである。

情報セキュリティ対策にたいしての意識の改革は、ネットワーク社会を安全に生きていく基本である。

情報セキュリティは、情報の共有と活用をする中で、特定のグループの人達だけで特定の情報を共用し、活用しあう事によって、他の競争グループと差別化をはかり競争を優位な方向に導くのが目標である。

情報セキュリティの目的は、その情報を共有する特定のメンバー以外に価値の高い情報が漏洩しないように管理することである。すなわち、情報セキュリティの機能と役目は、情報の共有・活用と情報の管理を両立させることである。

情報セキュリティは、技術的問題としてだけ考えるのでなく、個々の情報がどの程度重要であり、それが漏洩したときにどの程度のリスクがあるか、各リスクがどの程度の脅威がありどの程度保護する必要があるかを前もって明らかにしておく必要がある。

その上で、利用されるセキュリティ技術は、どの種類の何技法をどの程度のレベルで活用するかが決定される。

これらの対策は、情報セキュリティポリシーを確立し、その運用で決定される。

情報セキュリティの問題と言われてもそれほど重要問題とは、考えない経営者が多いのが現状ですが、一旦ことが起こると社会的な影響は計り知れないものがある。責任問題に発展し、場合によっては、経営者や管理担当者の経営・管理責任が問われる場合が多々ある。

大変有用であるが障害に脆い情報システムを安全に守るための情報セキュリティ問題は、最善に解決してこそ、初めて安心して利用でき、優れたインターネット社会を築くことが出来ると言っても過言ではない。

このような情報セキュリティのしっかりしたネットワークシステムの構築、情報処理の開発と情報処理システムの運用環境を作るための大学における情報セキュリティ教育は、如何にあるべきかについての考察をする。

すなわち、この論文の主旨は、情報セキュリティ問題を大学の情報教育の立場から考察することにある。

## 2．安全な情報セキュリティの構築に関する教育

### 2.1　情報倫理教育による倫理面からの対応

情報倫理は、情報を取り扱う人々がいつも備えておくべき規範であり、情報倫理を理解しない人には、啓蒙して理解してもらい、その上で、情報処理をする事が肝要である。

情報倫理は、次のように定義される。

「情報倫理とは、情報ネットワーク社会における個人および組織体が、情報技術を使って仕事をするときの守るべき規範となるもの」と定義できる。

ＩＴ社会（情報化社会）は、大変もろい社会である、この社会を安全に守っていくのは、構成員である人々全員である。ＩＴ社会は、構成員である各個人が悪いこと

はしないという規範の基に成り立った社会である。

このような基盤に立ったＩＴ社会ではあるが、いろんな危険が取り巻いているのも事実である。その危険に対応する備えがなければ、ＩＴ社会は、持ちこたえられないのである。

情報セキュリティは、危険に対する備えであるといって過言ではない。

次に、情報処理システムを教育し、運用する大学は、大なり小なり情報倫理教育をしていると考えられるが、本学の例を紹介する。

### 2.2　中央学院大学の情報倫理規範

中央学院大学のホームページの巻頭には、本学の「情報倫理」規定が掲示されている。それを披露すると次のようになる。

> 現代の情報社会は、高い倫理観によって成り立つ社会である。倫理に反することをすれば、社会に与える影響は甚大であり、多大な損害を与える場合もある。コンピュータ、インターネット、データベースが有機的に統合された情報社会では、各個人が最低限守るべき情報倫理が存在する。情報倫理とは、「情報社会において、われわれが社会生活を営む上で、他人の権利との衝突を避けるべく、各個人が最低限守るべきルール」である。(*参照)

本委員会は、本学の情報システムを利用する本学の学生及び教職員及びその他の利用者に対して、公序良俗に従い、情報社会の道徳的な規範である情報倫理を遵守することを強く要望する。

*参照「インターネットと倫理教育」1999年版　私立大学情報教育協会発行　平成13年３月31日　情報システム運営委員会

### 2.3　中央学院大学インターネット利用ガイドライン

前述した情報倫理規定の後を受け「中央学院大学情報システム利用規定」、「中央学院大学情報システム利用細則」、そして、ここで紹介する「中央学院大学インターネット利用ガイドライン」である。このガイドラインは情報ポリシーであり本学の学生、教職員、大学関係者が守らなければならない行動指針である。

その構成は、

１）基本原則
２）セキュリティ
３）電子メール
４）ＷＷＷとその他
５）関連法規の遵守

の５項目から構成されている。

セキュリティでは

１）大学の保有する機密情報及び個人情報公開の禁止
２）ユーザＩＤとパスワードの管理についての遵守事項
３）コンピュータウイルス対策について

を詳細に規定している。

### 2.4　人的セキュリティ

情報倫理に裏打ちされたＩＴ社会を守り、育て、発展させるのも人であり、大学における情報セキュリティの教育は、まず、人的セキュリティに関する理解と実践である。

情報セキュリティに関する対策を推進するポイントは、人的セキュリティであるといって過言ではない。いかに最新技術の技法や機器を導入しても、あるいは運用規則等を制定しても、情報を利用することを許された人が不正をする、組織上の権限で情報利用を許された人が規則等を遵守しなければ、情報セキュリティは堅持できないのである。

そこで必要になるのは、大学における情報セキュリティ教育である。会社においては、社内研修や情報セキュリティのための啓蒙キャンペーン等である。

大学当局では、情報セキュリティポリシーを確立し、守るべき対策基準、情報セキュリティ技術に関して各種教育資料を作成する。大学の教職員、学生、その他の関係者に対しては、それぞれの立場での情報セキュリティ教育をする必要がある。新たに構成員に対しては、適宜にスケジュールを作って教育する必要がある。

特に情報関連の学科・情報関連のコースの学生には、「情報セキュリティ論」を１セメスターで教育することをこの論文で提案する。「情報セキュリティ論」のカリキュラムの内容については、この論文の中で素案を提案したい。

利用者側で最も重要なのは、情報セキュリティポリシーを遵守することである。たとえば、ポリシーに従って各種パソコンの設定・運用を厳密に行う、ダウンロードしたファイルの安全性を検査するなど、ポリシーに記述

された事項を実際に守ることである。個人認証のID、パスワードの運用は、利用者におけるセキュリティ対策事項として最重要点であり、大切に取り扱い、情報の漏洩から守るべく努力しなければならない。

「騙し」対策など、ソーシャルエンジニアリングに関する教育も忘れてはならない。さらに、災害・障害が発生した場合はパニックにならず、あらかじめ決められたルールに従って行動がとれるように、平時に対応手順を訓練しておくことも必要である。

なお、個別の情報システムに関しては、各種情報システムの教育と予防対策が不可欠である。

啓発とキャンペーンによる啓発には、ハンドブックの配布、ポスター掲示によるキャンペーン、担当者よる見回り、ワークショップの開催、懸賞論文の募集と優良論文の表彰などが有効である。

情報セキュリティの定着には、中央学院大学がしっかりした情報ポリシーの基に対応策を考えるとともに、一大学だけの問題でなく、日本の全大学、地域社会全体、日本全体、そして世界全体のグローバルな問題である。

情報セキュリティは、ダムの壁面にたとえるとよく理解できる。各壁面の高さが均一でない場合、壁面の一番低いところまでしか水を蓄えることができない。この壁面を各部分部分に分けると各部分の一つ一つを、種々の情報セキュリティ対策、運用ルール、各個人と考えれば、情報セキュリティレベルも同じである。つまり、特定の対策だけに過度な投資を行っても意味をなさず、要は、対策のバランスが重要だということである。

また、往々にして人間が足を引っ張り、情報セキュリティレベルを下げる事態を招くことを肝に銘ずる必要がある。情報セキュリティと言うと技術的側面にばかりに目を向けがちだが、しよせんは「人の問題」である。情報システムを攻撃する側も人ならば、守る側も人である。一番低い壁面は、人であることが多いので情報セキュリティ教育の必要性が改めて認識される。

たとえば情報セキュリティ対策に対して攻撃側は、技術的な攻撃が難しい場合、いろいろな情報を入手するために詐欺的な手法を用いたりする。システム管理者やプロバイダなどになりすましてパスワードを聞き出すなどの手口を使う。こうした行為を「ソーシャルエンジニアリング」と呼ばれている。解読できないようにパスワード設定のルールが決められていても、推測しやすいパスワードを使っている人がいれば、なりすましによるシステムの不正使用の危険性は高くなる。情報セキュリティのルールは、厳しくすると使い勝手を悪くすることもあるが、その面倒なルールを守るか否かも人次第であり、最終的に、情報セキュリティ問題は人の問題なのである。

本論では、情報セキュリティの問題を大学教育に限定して論じているが、ネットワークを使う小学生から社会人まですべての問題であると言うことを認識して頂きたい。

## 3。情報セキュリティの特性

### 3.1 インターネット上の脅威の現状

今年の夏は、MS Blaster と Sobig. F という2つのウイルスが猛威を振るった。

両者とも、マイクロソフトの Windows のセキュリティ・ホールを悪用して感染を広げる「MS Blaster (MSBLAST Lovsan)」ウイルス（ワーム）が8月12日に出現し、お盆休みの国内を襲った。

大きな被害が予想されたために、8月13日以降、ウイルス対策ソフト・メーカーに限らず、経済産業省なども強く警告していた。マイクロソフト社は電話相談の窓口を24時間体制に切り替え対応に備えた。

「Windows Update を頻繁に利用する」、「ウイルス対策ソフトを利用する」や「ファイアウォール」を使うなどで防御する対応策をこうじないと、高い確率で感染する可能性があった。対応策を施していなくても感染していないという場合は、現在使用しているブロードバンド・ルーターなどが防いでくれている場合がある。

ネットワークに障害を発生させる“新種”のウイルスは、同じセキュリティホールを悪用する、次の Blaster が出現する。実際、8月18日には、別のセキュリティホールも悪用する新種ウイルス「Welchi (Nachi, MSBLST. D)」が出現した。このウイルスは、感染を広げる際に Blaster よりも多量のデータを送信するために、ネットワークに障害を引き起こす可能性があり、8月19日には、複数の企業や組織で障害が発生した。

今後、セキュリティホールを放置したままでいると必ず感染する。マイクロソフト社が公開する「Blaster 対策ページ」などを参考に対策を実施する必要がある。とにかく、Windows Update の利用は不可欠である。

「発信者の不明なメールに添付されているファイルは絶対に開かない」と言われ続けている原則を守ることが重要である。このような脅威と対策について教育する必要がある。

情報処理振興事業協会のIPA PH（ホームページ）のなかの警視庁のHP『ハイテク犯罪等に関する相談』の統計表を図1として提示する[1]。

### 3.2 インターネットの脅威

サイバーアタックを目的としたクラッキングは、Webページの改竄やDoS攻撃など直接的なものばかりでなく、密かに準備作業が行われ、何らかの方法でセキュリティの網を破ってシステムを利用するためのユーザ権限を奪取することである。

3.2.1 クラッキングの前段階の手法を列挙するとつぎのようになる。

1）ポートスキャン
2）パスワードクラック
3）ソーシャルハツキング
4）バッファオーバーフロー

特にターゲットとなったプログラムがroot権限で実行されている場合、一気にroot権限を乗っ取られる可能性があり、非常に危険である。サーバプログラム関するセキュリティ上の脆弱性の主な原因になっている。2003年3月に相次いで発見されたsendmailのセキュリティホールもこれであった。

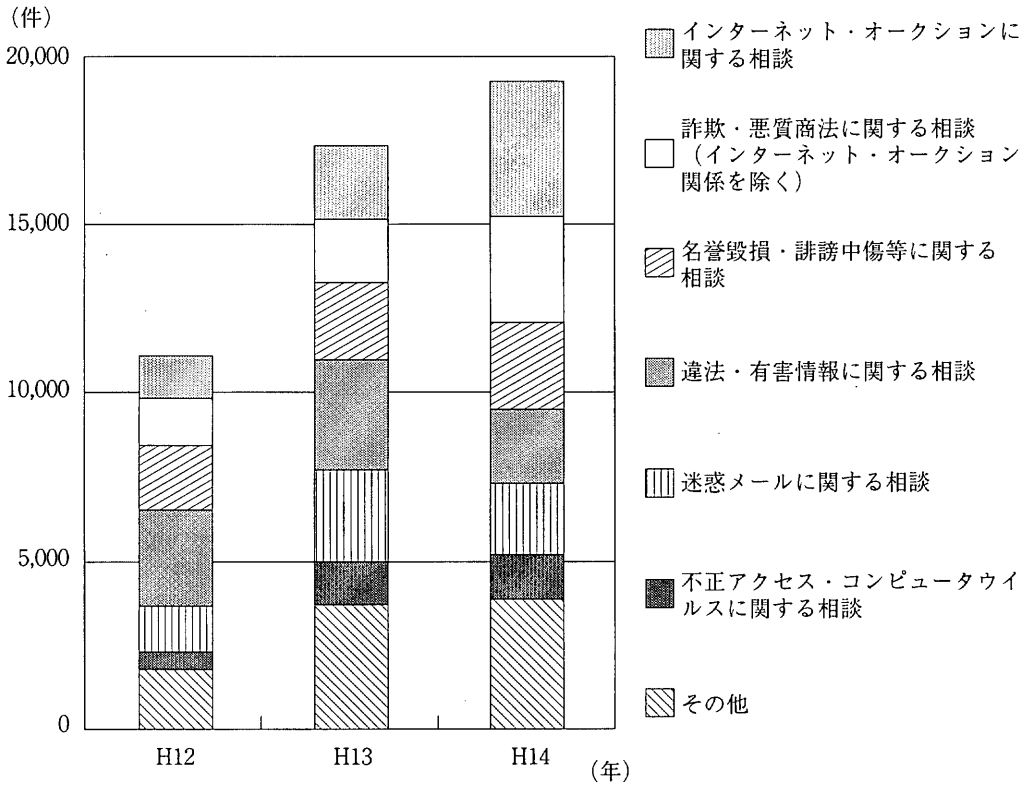
5）ワーム

ネットワークを介して他のマシンに自動的に感染し増殖するワームには、バッファオーバーフローによる脆弱

図1　ハイテク犯罪等に関する相談

ハイテク犯罪等に関する相談受理件数は、19,329件で前年の17,277件と比べて約12%増加

【ハイテク犯罪等に関する相談受理状況】




出典　警察庁ＨＰ　http://www.npa.go.jp/hightech/arrest_repo/kenkyo_2003_.pdf

1）情報処理振興事業協会のHP内の警視庁のHP「ハイテク犯罪等に関する相談」のホームページを掲示する。

性を突いてシステムに感染するものがある。近年、このタイプのワームが増えており、2003年8月のMS Blasterもその一つである。

3.2.2　クラッキング後の行動

一度侵入に成功してしまえば、クラッカーの行動の選択肢は大きく広がる。クラッキングは、すべての始まりである。そして、クラッカーは不正アクセス、なりすまし、盗聴、データ破壊、改竄、事後否認、スパムメール、サイバーテロなどの不正を行う。

このようなことをしないように教育し、このようなことにならないように自衛手段をこうじたり、不正をした人を特定し、二度としないように法律で罰したり、制度化して情報社会を精神面、法律面、技術面で支え維持していくのが情報基盤（インフラ）であると言って過言ではない。

そこで、大学の情報セキュリティ教育は、情報教育のあらゆる機会を捕らえて実施し達成しなければならない課題である。

## 4．大学における情報を専門としない学部、学科、コースのコンピュータ利用者の教育

### 4.1　はじめに

大学における情報システムの利用者である学生、教職員、大学関係者（大学構成員）に対するセキュリティ教育は以下の形で行われることが多い。

1）学内の情報システムセンター、情報処理センターなどと連携した情報システム運営委員会等で検討され、決議された内容を学長に答申し承認を受けたものを全構成員に告示し、徹底する。
2）大学の公開しているHP（ホームページ）などで告示する。
3）情報リテラシー教育や情報処理論などの情報基本教育に教育の一貫として情報倫理とパスワードの必要性と重要性を徹底させる。
4）大学の公開しているホームページなどにコンピュータウイルスに対する注意事項として大学構成員に提示し注意と警告をする。情報の性質上、ホームページへのアクセスを学内限定にする大学も多いのである。
5）情報システム部のメディア課で、情報リテラシー等の情報倫理の時間に欠席した学生に「利用者の情報倫理教育」の実施をする。
6）「情報リテラシー」、「情報処理論」等の情報基礎教育で情報倫理と情報セキュリティの講義を行う必要がある。

### 4.2　セキュリティ対策について

大学の構成員に対するセキュリティ対策は、情報倫理教育、電子メールの取扱い、パスワードとウイルス防止などの対処方法が中心になる。

「情報リテラシー」の時間に情報倫理教育を入れる。

ＩＴ社会は、情報と言う大変もろいものが、中心になって活動している社会であり、個々の構成員が不正なことはしないと言う確固たる信念の基で、生きていく社会であることを情報教育の情報倫理教育で徹底させる。

### 4.3　パスワード

パスワードは、ユーザ認証の手段であり、コンピュータを利用する構成員が覚えやすく他人にとって類推されにくい文字列がよい。パスワードがサーバーには暗号化されて保存されており解読が困難なようだが辞書検索や、端末からサーバーまでの伝送路で盗聴者に解読されたりして、パスワードが読み取られる可能性がある。

その他あらゆる手段で、パスワードを探し出し、それによって成りすまして浸入し、悪いことをする。

良いパスワードとしては、

1）自分の好きな詩集、小説等の文章の頭文字で作る
2）適当の期間で更新する。
3）英文字と数字の組み合わせてつくる
4）他人に推定されないものを作る
5）自分だけが知っていることで作る

などが良いとされている。

どんなに優れたパスワードでも、長く使っている間に解読されたりするので、時々変更するとか、定期的に変更するのが良いとされている。

パスワードをキーボードに向かって入力するときは他人に見られないように配慮すべきであるが、逆に他人がパスワードを入力するときは、見ないように目線を他に

向けるという配慮も必要である。

パスワードの入力はクライアント端末であり、実際にシステムが動作するのは別室のサーバーであったり、インターネットを通して外部にあるサーバーであったりするので、パスワードそのものがネットワークを流れることが多い。この生パスワードがネットワークを流れることによる解読を防ぐために暗号化技術があり安全のため頻繁に使われる。

ユーザに教育する場合は利用するシステムにそのような安全な対応機能がある場合は積極的に利用するようにさせる。

パスワードを解読されることは、本人ばかりに留まる問題だけではなく、そこを踏み台にしてその組織内から外部の組織に入り込み盗み見たり、改竄したりすることに使われることが危険であり、防御が必要である。

パスワードのセキュリティ対策としてワンタイムパスワード（One Time Password）は、1回だけのパスワードである。これを用いることで安全性を保つことはできるが、1回1回パスワードが変わるので運用が大変である。

### 4.4 コンピュータウイルスに対する対策

情報セキュリティを侵害するもの、それを防御しようとする技術は、情報セキュリティ教育で十分に指導する必要がある。

世界で8割以上のシェアを持つマイクロソフトのＯＳ Windows を対象にしたコンピュータウイルスやワームは、感染したパソコンにとどまらず広範囲に伝染する。そこでワクチンを使ったり、外部からのネットワークの入り口にファイヤーオールなどを設けて危険なものは入れないような防御が必要になる。

ファイアウォール（Firewall）については、入れてはいけない通信と入れても良い通信とを分別するサイトの門番の働きをする。ファイアウォールや不正アクセス監視ツール（IDS（Intrusion Detection System））でもセキュリティ対策は万全ではない[2]。そこで、入り口ばかりでなくサイト内に何重にかける場合がある。

コンピュータウイルスなどの防止は定評のあるコンピュータウイルス防止ソフトウェア（ワクチンともいう）をインストールし、さらには新しいコンピュータウイルスを防止するためにインターネットなどを通してウイルス定義ファイルのデータの更新を一定の間隔でやるべきである。特に新種のコンピュータウイルスが出たと報道された場合は、データ更新を行うべきである。

大学や企業等で発生した場合に発見者は、ネットワークを管理している情報システム部等にすぐ連絡し、被害が拡大しないようにする体制を早くから作っておく必要がある。これが情報セキュリティポリシーの確立である。

最近のように、毎月新手のコンピュータウイルスが出現している状況では、組織としてコンピュータウイルスの侵入や逆に進出を止める対策を施さないと大学・企業等の組織としての責任が問われる。

大学等の組織としてコンピュータウイルスをチェックする場合には今まで個人が行ってきたウイルス添付ファイルの処理に加えて、管理組織が個人宛ての電子メールを開けるわけには行かないので、電子メール用のパスワードを強化したり、怪しげな電子メールは、開封しないで廃棄したり、ネットワークを管理する情報システム部に連絡を取ったりして、組織内でのセキュリティポリシーの方策を周知徹底する必要がある。

コンピュータウイルスに感染した場合の処置は、信頼できるコンピュータウイルス防止のためのホームページから情報を得てなるべく早く処置する必要がある。

大学のネットワークを管理する組織（情報システム部）等で新手のウイルス情報を察知し、大学の構成員にウイルスの状況、対処法等を丁寧に説明した文章または、大学のホームページ等を告示することで被害の発生や被害の拡大を防ぐ必要がある。

不幸に感染した場合は、被害にあったパソコンをネットワークから外して、ウイルスを駆除してから復帰させる。

これら一連のウイルス対策の流れを構成員に周知徹底するのも、大学における情報セキュリティ教育の一貫である。

### 4.5 天災・人災によるセキュリティ

コンピュータ関連の天災・人災によるセキュリティは、大きく分けると

2）「Webサイト攻撃の手口」「NETWORK」2003年12月号　IDGジャパン　110－114頁

1）自然現象
2）人間の行動で不注意から生ずるもの
3）人為的なもの

などの3種類のセキュリティ問題として列挙してみる。

1）自然現象の地震、雷、台風、水害、電気ノイズ等によるものは、偶発的で避けがたいものである。このような現象に対しては、あらかじめセキュリティポリシー等で対策を考えておき、普段から対応策を実施し、危険に対しても正常な状態に復帰できるようにしておくことが肝要である。

2）人間の行動で不注意から生ずるものは、コンピュータ利用者の中には、お茶、コーヒー、水飲んでこぼしたり、コンピュータ室で飲食してこぼしたり、ほこりを出したり、コンピュータをつけたまま席を離れて他人に盗聴されたり、パスワードを他人に貸したり、端末の近くにパスワード書いたものを置いたり、パスワードの入力時に他人見られるミスをしたりして大事に至る場合が多々ある。

3）犯罪者は、メールの盗聴をし、無線LANでの盗聴し、機器を持ち出し、部屋に無断侵入し、機器の破壊をし、火災等の人による故意的な行動でネットワークを破壊する。

この問題は、セキュリティ防御対策もさることながら、大学における情報倫理教育や情報セキュリティ教育を充実して不正を未然に防ぐための対策をしないといけないと思われる。

これら、ケースバイケースに応じたセキュリティ対策を施すことが大切であり、ＩＴ時代に生きていく最低限のルールでありマナーであると考えられる。

情報システムを管理する管理者サイドの対策としては、管理者対策を利用する大学の構成員に、構成員サイドで実施可能な対策を説明し、対策を実施してもらわなければならない。

セキュリティの問題は、新しいウイルスの出現でわかるように、日々新しい攻撃があり、情報セキュリティホールが見つかっている。組織の管理者からも、日々新しいセキュリティ情報を流すことも必要である。一般の大学の構成員は、日常的にワクチンデータの更新を行う必要がある。また、一般の大学の構成員は、遠隔からの操作において暗号などを使った安全な通信を理解して実施する必要がある。

上記の対応と共に、組織としてのセキュリティポリシーを確立しそれを理解してもらい、できれば組織としてのセキュリティポリシーの策定に大学の構成員からも積極的に参加してもらうとよい。セキュリティポリシーは、その組織の仕事（業務）に密接に関係しており、大学の構成員が理解でき積極的に実施してもらえるものが好ましい。

経済産業省より「ISMS 適合性評価制度導入」が公表されたのは2000年の夏である。さらに2002年４月から「ISMS 適合性評価制度」が始まりました。

インターネットなどのネットワークの拡大は、企業や組織体における情報セキュリティの重要性が増し、社会における他のインフラと同様な役割を果たすようになった。

## 5．大学にあけるセキュリティ教育

### 5.1　はじめに

大学におけるセキュリティ教育は、情報リテラシー、情報処理論等の学生全員に行う一般の情報教育の中で下記のＡ、Ｂで教育されている。

Ａ）コンピュータを利用する前に実施する教育（１時間）。

Ｂ）インターネット活用法の講義冒頭に情報倫理教育とセキュリティ教育がなされるのが一般的である。（１時間）

Ｃ）文系・理系の情報セキュリティに関する１セメスターの教育（15コマ）。

Ｃについては、今回の論文の主題である。

Ｄ）情報セキュリティの２セメスターで実施する理工系のカリキュラム（30コマ）。

Ｄのカリキュラムと授業の内容に関しては、紙数の都合上次回に発表するものとする。

Ａ）では、大学のキャンパス LAN のコンピュータを利用する時のマナーとしてパソコンの構造と取り扱い方からコンピュータを使った不正な行為をしないように情報倫理を理解するように指導する、また、いかなる時にもコンピュータの異常なことに気が付いたらすぐに対応しなければならない、たとえば授業中なら担当教員に、自学自習の場合には、そのまま放置するのでなく情報教育

支援担当部署の職員（本学の場合は、７階メディア準備室）に連絡し対処するように徹底して指導する。また、パスワードの重要性とその取り扱い方、コンピュータ室内でのマナー等についても徹底して指導する。

B）インターネット活用法の講義冒頭に情報倫理教育とセキュリティ教育がなされるのが一般的である。（１時間）

この時間では、あらかじめ規範を提示して、ホームページなどで見て良いもの、見るのが不適切なものを判断させ大学生としての情報倫理としてのマナーを身につけさせる。

電子メールをよく利用しているが、迷惑メール等の不正行為をしないように指導することが大切であり、送られてきた異体の知れない出所不明の怪しげなメールがあった場合は、ウイルスが添付されている恐れがあるので開封しないで廃棄するように厳重に指導することが要求される。

便利さ、有用性と即時性を備えたインターネットであるが、その中のデータの信憑性は、出所をよく調べ適正な判断をしてから使用しないとデマ情報であったりすることがある。

特にインターネットオークションや E-Commerce などで、クレジットカードを安易に使わないように喚起しないと、暗号化されていなくて、盗聴されたり、クレジット番号と暗証番号を読み取られ不正行為に使われたりする恐れがあるので十分に注意する必要のあることを喚起しなれればならない。詳しくは E-Commerce 教育で述べたい。

C）文系・理系の情報セキュリティに関する１セメスターの教育（15時間）。

前述の一般情報処理論の中で、情報セキュリティ教育をすることも大切であるが、専門教育として情報関連学部、情報関連学科や情報関連コース等では、独立した科目として、「情報セキュリティ」を１セメスターの15コマ（１コマ：90分として）で情報関連のリスクに対応できる人材養成する必要がある。

D）情報セキュリティの２セメスターで実施する理工系のカリキュラム（30コマ）。

情報工学関連の専門家を養成する学科・コースでは、暗号技術とファイアウォール等の防御技術の理論と実践を重要視して教育する必要がある。これらについて紙数の都合からも、今回の論文より外し次回の課題としたい。

また、大学院における情報工学の専門家を養成する情報技術関連専攻科の技術者を養成するカリキュラムについては、情報セキュリティの演習・実習を伴う複雑な問題が山積しており、紙数の都合からも、今回の論文より外し次回以降の課題としたい。

### 5.2 情報セキュリティ論のカリキュラム試案

C）文系・理系の情報セキュリティに関する１セメスターの教育（15コマ）のシラバスとそこに盛り込まれる教育内容について考察する。

講義内容として、セキュリティ教育で盛り込むべき項目について、順序は大学によって異なるが内容として次のことが考えられる。

①ＩＴ社会とセキュリティ
②情報倫理
③情報セキュリティ
④ネットワークのセキュリティ
⑤インターネットのセキュリティ
⑥E-ビジネスのセキュリティ
⑦情報セキュリティの関連法
⑧情報セキュリティ関連の規格・制度
⑨暗号技術論
⑩認証技術と認証監査機関
⑪情報セキュリティポリシーの確立
⑫リスク管理

と多岐にわたる。

これをカリキュラムにして、セキュリティ教育で具体的に教える項目にすると次のようになる。

１時限　ＩＴ社会とセキュリティ
２時限　情報倫理
３時限　情報セキュリティ
４時限　脅威に対する対処法１（ウイルス対処法）
５時限　脅威に対する対処法２（ファイヤーオール）
６時限　ネットワークのセキュリティ
７時限　インターネットのセキュリティ
８時限　E-ビジネスのセキュリティ
９時限　情報セキュリティの関連法
10時限　暗号化技術(1)
11時限　暗号化技術(2)
12時限　情報ポリシーの策定、構築

13時限　実施ポリシーの策定・運用
14時限　演習とまとめ
15時限　テストと評価
このカリキュラムは系統立てて教育する必要がある。

C）文系・理系の情報セキュリティに関する１セメスターの教育（15コマ）。
講義の時間ごとの授業項目と内容の試案を時間ごとに披露する。

１時限　ＩＴ社会とセキュリティ
ＩＴ（情報技術）社会における情報技術の発展の歴史とその技術を側面から支えてきた情報セキュリティの歴史を対比しながら、情報セキュリティのその時々に求められた、その必然性と重要性について講義する。
また、現在抱えている情報セキュリティの問題点を指摘し、次回以降の講義で課題別最先端の情報セキュリティ技術が、なぜ要求されるかのアウトラインを講義する。

２時限　情報倫理
情報を扱うのは人であり、情報倫理は、ＩＴ社会を維持・発展させるために情報技術を利用するすべての人が、理解し、実践しなければならない規範であり、行動指針である。
特に、情報倫理は、ネットワーク（インターネット）を利用するすべてのユーザが持たなければならない資質であり、規範である。
「職業と倫理」、インターネット扱う時の諸問題、電子メールを扱う場合の諸問題、著作権問題等の事例を挙げて情報倫理観を育成する講義をする。

３時限　情報セキュリティ
主にネットワークと関連した種々のセキュリティ上の脅威や危険から情報資産を保護し、正常に情報システムを保持し、利用者が安心して使えるようにする。
情報資産の機密性、完全性、可用性の観点に加えて、E-Commerce による電子認証などの認証性を満たさなければ成らなくなってきている。
セキュリティ技術、情報セキュリティポリシーの構築・運用、情報セキュリティの管理・運用、情報セキュリティ法の遵守などを講義する。

４時限　脅威に対する対処法１（ウイルス対処法）
ウイルスの歴史について講義する。ウイルス対策は、ルータの直後に、ウイルスチェック用のサーバーマシンを用意してウイルス検知してワクチンで駆除するようになってきている。これによりサーバーマシンやクライアントマシンに到着する前でウイルスチェックをする構成が増加している。サーバーマシンでウイルス検知を行っていてもクライアントマシンでウイルスチェックをしておかないとウイルスがメールの添付されていて増殖する場合がある。
最近の有名なウイルスは、今年の８月12日に猛威を振るった「MS ブラスト」である。
キュリティホールの情報と修正プログラムが公開されたのは７月17日であった。
マイクロソフト社をはじめとして、いろいろ手を打ったにもかかわらず、それでも感染を防げなかった。それは、警告してもなんら対策を実施しないでそのまま放置する人か多くいるからである。
「MS ブラスト」は、インターネットに接続するだけで感染するのであり、メールや Web の利用に注意していれば大丈夫な時代ではなくなり、対応が必要になった。
これは、本論の投稿時の事例でありますが、ウイルスは毎日のように新手が発生しているので、このカリキュラムが実施されるときには、それに即した実例で講義をすればよいと考える。

５時限　脅威に対する対処法２（ファイヤーオール）
ファイアウォールは、外部から進入しようとする不正なアクセスを防ぐためのアクセス制御を実行するシステムである。
ファイアウォールは、その歴史、ファイアウォールの原理、ファイアウォールの構成要素、設定方法、セキュリティ対策やファイアウォールの必要性について講義することが必要である。
ファイアウォールの１次フィルタリングを介して外部インターネットに接続される。
経由する通信記録をアクセスログとして保管したり、不正なアクセスを受けたらネットワーク管理者に知らせたり、外部ネットワークへのゲートウェイとして365日休むことなく正常に稼動する必要がある。このように、このファイアウォールは、大切な防護手段であり、１つ

設置するだけでは不安の場合は、種類の異なる複数個のファイアウォールをかけて防護する場合がある。このようにファイアウォールをかけたから安全という時代ではなくなりつつあり、新たなファイアウォールの研究が進んでいるのも現状である。その運用法も講義する必要がある。

6時限　ネットワーク（インターネット）セキュリティ1

インターネット利用環境において情報セキュリティを確保するには、インターネットセキュリティが必要である。インターネットセキュリティは、境界セキュリティとトランザクションセキュリティの2つからなっている。

6時限目は、境界セキュリティ（Boundary Security）について講義する。

境界セキュリティは、大学・研究所のコンピュータシステムとシステム内に保管されている情報を守り保護することである。インターネットを経由した外部からの不正アクセスから大学内のキャンパスLANを守ることは、境界セキュリティの例である。

このように情報システムを不正アクセスやサイバー攻撃から守る働きを境界セキュリティは行っており、システムセキュリティとも呼ばれている。

プロキシサーバは、内部のネットワークとインターネットとの境界に設置、内部のネットワークからインターネットとの通信を監視する働きをする。

プロシキサーバを置かないときは、二次フィルタリングから一次フィルタリングを介して外部のインターネットに接続する。

パケットフィルタリングは、パケットの種類によって通行を禁止するか許可するかのルールである。

リバースプロキシサーバは、インターネットから内部のネットワークへの働きをする。

アプリケーションゲートウェイは、あらかじめ決められた通信を許可するアプリケーションだけを通過させる働きをする。

進入探知システム（IDS）は、ファイアウォールだけでは、防げないインターネットから内部のネットワークへの不正アクセスを監視するシステムである[3]。

7時限　ネットワーク（インターネット）セキュリティ2

7時限目は、トランザクションセキュリティ（Transaction Security）ついて講義する。

1）トランザクションセキュリティとは、電子メール、電子商取引などの通信において、インターネット上のメッセージや重要情報を盗聴されたり、改竄されたり、破壊されたりすることから守る技術の総称である。

トランザクションセキュリティ技術は、インターネット上で不特定多数の相手との安全な通信を保障するため、通信データの改竄、盗聴、通信相手のなりすましを防ぎ、信頼のおける情報の授受を実現する技術であり、秘密のまま保持するための技術であり、暗号化技術が使われている。暗号化の各手法について講義する。

この暗号鍵には、暗号化方式の違いから「秘密鍵」と「公開鍵」の2種類があり、ほとんどの暗号化技術には、共通鍵暗号方式か公開鍵暗号方式のいずれか、または両方が使われている。

2）共通鍵暗号方式

共通鍵暗号方式は、暗号化と復号化に同一の鍵を使用する暗号化技術（Encryption technology）である。この方式では、暗号化処理が高速に行われるため、大きなデータに対しても効率のよい暗号化と復号が可能である。これらについて簡単に概要を講義する。

3）公開鍵暗号方式

公開鍵暗号方式では、二つの独立した鍵を一対として使用する暗号化技術である。一つの鍵は広く配布しても構わない公開鍵で、もう一方は秘密鍵で秘密に管理する必要のある。

これら二つの鍵のうち、一方の鍵でデータを暗号化し、他方の鍵で復号化する方式である。

これらについて原理を講義する。

4）デジタル署名

デジタル署名の目的は、受信したメッセージの送信元を認証し身元を特定し、「なりすまし」を防いだりする。

デジタル署名について仕組みを簡単に講義する。くわしくは、11時限目に講義する。

5）SSL 認証と認証局（Certificate Authority）

電子商取引におけるクレジットカード番号の伝送のような、安全なトランザクションを提供するために使われ

3）赤尾隆著「企業ネットワーク設計の極意」リックテレコム　2003年　192－212頁

る Web 用の暗号化技術である SSL（Secure Socket Layer）は、Web サーバと Web ブラウザ間のHTTP通信を暗号化して送受信する業界標準の通信プロトコルである。SSL クライアント機能は一般の Web ブラウザに標準で搭載されており、Web ブラウザを利用した電子商取引のプロトコルとして広く使われている。

SSL の技術は、40ビット、128ビットの暗号化により通信文の内容を保護し、第三者の認証局（Certificate Authority）によりその通信に不正がないことの認証を受けたものである。

これらについて講義する。

6）VPN

VPN（Virtual Private Network）とは、インターネットのような公衆網を利用して仮想的に構築する独自ネットワークのことである。もともとは、公衆電話網を専用網のように利用できる電話サービスの総称であった。最近では、企業ネットワーク内に点在する各支社・支店の LAN を、インターネット経由で接続し、専用線のようにインターネットを利用する通信形態を VPN と呼ぶことが多くなった。また、これまでの VPN と区別するためインターネット VPN と呼ぶことがある。

インターネット VPN の利用形態として、モバイルアクセス構成及び LAN 間接続構成の 2 種類がある。

これらについて簡潔に講義する。

8時限　E - コマースのセキュリティ

E - コマースに対して疑問を持つ方は、セキュリティに対する不安（リスク）が伴うので利用しない人が多いのである。

「自分の個人情報が漏洩しないか」、「クレジットカードの番号を使って暗証番号を類推し不正使用しないか」「取引の相手が見えない」「契約書面に署名や捺印がない」という不安は、E - コマースの早急に解決しなければならない最大の欠点である。

ネットワーク技術、個人認証技術、情報管理技術やサイバーアタックから守れるセキュリティ技術を駆使して安全な信頼性のある情報システムを作るとともに、セキュリティポリシーを明確にして、ＥＣサイトとしてしっかりとした防御技術を用いて、信用を得る努力が大切である。

E - コマースは、インターネット上の商取引としてこれからの商取引の中心をなすであろう。また、E - コマースは、電子認証の正確性の保証があってこそ成り立つのである。

このE - コマースの便利さと有効性は大変優れた考え方のシステムであり、本学では、1セメスターで「E - コマース」の講義がなされる。

9時限　情報セキュリティの関連法

新しい情報関連の技術を生かして社会に活用していくには、法的な整備が欠かせないのである。一つの例を取り上げると、E - コマースの電子署名に関しては、2001年4月から施行された「電子書名および認証業務に関する法律」によって公開鍵番号によるデジタル署名を安心して電子商取引に利用できるような基盤が整備されたことになる。

情報セキュリティの関連法は、何年にどのような法律が制定されたかを表1で紹介するにとどめる。講義する教員が法律の専門家ならば話が違うが、情報の専門家の先生ならば深い解釈を講義するのでなく、紹介に留める。

10時限　暗号化技術(1)

情報の暗号化は、情報の機密を確保するセキュリティ対策の技術である。暗号化の種々の理論を講義する。

1）暗号の役割、暗号理論の歴史

暗号の概要や歴史の講義は、興味深く暗号解読の歴史を講義するとよい。暗号理論には特有の用語があり、用語を理解できるように講義する。

2）共通鍵暗号方式

共通鍵暗号方式は、暗号化と復号化に同一の鍵を使用する暗号化技術であり鍵が同一か簡単に類推できる方式である。共通鍵暗号方式では、暗号化処理が高速に行われるため、大きなデータに対しても効率のよい暗号化と復号が可能である。しかし、暗号化と復号化に同じ鍵が用いられるため、事前に鍵を受け渡すことが必要となり、インターネットのように不特定多数に開かれたネットワークでは、鍵の管理と配布の安全性が問題である。

3）公開鍵暗号方式

公開鍵暗号は、暗号化の鍵と複合化の鍵は異なりお互いに簡単に類推できない暗号方式である。

公開鍵暗号方式では、二つの独立した鍵を一対として使用する暗号化技術である。一つの鍵は広く配布しても

表1　最近の情報セキュリティに関する法律[4]

| 公布日 | 施行日 | 法律名 |
|---|---|---|
| 1999／8／13 | 2000／2／13 | 不正アクセス行為の禁止等に関する法律 |
| 1999／8／18 | 2001／4／1 | 犯罪捜査のための通信傍受に関する法律 |
| 2000／5／31 | 2001／4／1 | 電子署名及び認証業務に関する法律 |
| 2000／11／6 | 2001／1／6 | 高度情報通信ネットワーク社会形成基本法 |
| | 2001／6／1 | 特定商取引に関する法律 |
| 2001／6／29 | 2002／12／25 | 電子消費者契約及び電子承諾通知に関する民法の特例に関する法律 |
| 2001／11／28 | 2002／4／1 | 商法等の一部を改正する法律 |
| 2001／12／12 | 2001／12／12 | 犯罪捜査のための通信傍受に関する法律（改正） |
| 2002／4／17 | 2002／7／1 | 特定電子メールの送信の適正化等に関する法律 |
| 2002／6／19 | 2002／6／19 | 著作権法（改正） |
| 2002／7／31 | 2002／7／31 | 公証人法（改正） |
| 2002／7／31 | 2002／7／31 | 民法施工法（改正） |
| 2002／12／5 | 2002／12／25 | 刑法の一部を改正する法律 |
| 2002／12／13 | 2002／12／13 | 商業登記法（改正） |
| 2002／12／13 | 2002／12／13 | 住民基本台帳法（改正） |
| 2003／5／30 | 2003／5／30 | 個人情報の保護に関する法律 |
| 2003／5／30 | 2003／5／30 | 行政機関の保有する個人情報の保護に関する法律 |

構わない公開鍵で、もう一方は秘密鍵で秘密に管理する必要がある。

これら二つの鍵のうち、一方の鍵でデータを暗号化し、他方の鍵で復号化する。二つの鍵の間には複雑な数学的関係があり、公開鍵だけでは、他方の鍵の値を計算で求めたりすることが不可能に近い暗号アルゴリズムが使用される。これらアルゴリズムについて講義する。

公開鍵暗号方式は、前者の公開鍵暗号方式と比較して、暗号化と復号化の処理に時間がかかるため大量データの暗号化には不向きである。

4）公開鍵方式のRASのアルゴリズムを教育する。

公開鍵暗号方式の暗号アルゴリズムとしては、発明した3人の開発者の頭文字からとったRSA方式が有名で広く使われている。

暗号理論は、秘密を守り、プライバシーを守るセキュリティ技術の理論である。

暗号技術は、情報セキュリティを支える重要な技術であることを講義する。

11時限　暗号化技術(2)

1）認証技術

認証技術はアクセス制御と共にセキュリティを支える基本技術であり、これからも展開する技術と思われる。

研究者を目指す学生や認証技術の実用化を目指し新しい認証技術の創造をする学生には、認証の基礎概念から教える。

2）デジタル署名

認証技術をもう少し具体的な技術としたのがデジタル署名ないしは、電子透かしである。電子データに対してそのデータの作成者を明らかにするための印を付ける。

デジタル署名の目的は、受信したメッセージの送信元を認証し身元を特定し、「なりすまし」を防いだりする。また、送信メッセージが改竄されないで、到着しているか確認する。

また、送信メッセージは、メッセージ内に記されたデジタル署名が本人からのものであると特定され、否認できない。このことを「否認防止」といわれている。

デジタル署名は、認証、完全性、否認防止というセキュリティの基本的な3要素を提供する。デジタル署名においては、先に述べた秘密鍵暗号方式、公開鍵暗号方式、

4）辻井重雄、笠原正雄著「情報セキュリティ」昭晃堂　2003年　9頁

及びハッシュ関数の技術の組合せにより利用される。

次に、その公開鍵入りの電子証明書を、秘密鍵で暗号化したデジタル署名付きメッセージと一緒に受信先に送付する。

一方、受信側では、電子証明書から取り出した公開鍵でメッセージとデジタル署名を復号して、それぞれのハッシュ値を照合することでデータの完全性を確認する。

さらに、受信側は、電子証明書が正しいものであるかを、第三者機関に問い合わせることができるため、なりすましを排除することができることについて講義する。

3）デジタル透かし

デジタル透かしとは、ある電子データに別のデータを入れ込む手法である。マルチメディアデータに知的所有権のデータを埋め込む等に使われる。

4）IC カード

IC カードは高度なセキュリティ記憶媒体であり要素技術と解決手段である。IC カードの構造、その働き、機能とその実現する効果に加えて応用分野等について講義する。

5）電子投票システム（Electronic voting）

電子投票や電子入札は、いろいろな暗号理論の応用を駆使して実現された暗号プロコトルである。情報セキュリティが使われている最新の先端技術の応用として講義する。

12時限　情報ポリシーの策定、構築

情報セキュリティ対策は、大学の経営者、情報システム部、学生、教職員等の組織全体の構成員で取り組まなければならない問題である。

ＩSMS（Information Security Management System）は、セキュリティポリシーを基本に据えた情報セキュリティを維持・管理・運営するための仕組みである。

1）本ポリシー（大学としての基本的方針と宣言）

2）標準的ポリシー（各学部、事務局の各部課としてどう対応するか）

3）実施ポリシー（対策基準・実施要領の策定）ここは、13コマ目で講義する。

基本ポリシーの内容について各項目を綿密に規定する。標準的ポリシーでは、セキュリティ管理組織、セキュリテイ問題への対処法、リスクとセキュリティ対策の方針、情報管理手法、ハード・ソフトのセキュリティ管理、通信セキュリティの管理などについて詳細に規定する。

2002年4月より「ＩＳＭＳ適合性評価制度」が始まり国際基準で情報セキュリティの適合度を評価し、基準を満足した組織に認証を与える制度である。「ＩＳＭＳ適合性評価制度」は、ISO／ＩＥＣ17799および2002年9月に、BS7799-2:2002と改定され、「ＩＳＭＳ適合性評価制度」も「ＩＳＭＳ認証基準（Ver. 2）」[5]となった。

セキュリティポリシーの策定、構築などの実践的知識と必要性を講義することが大切である。

この他に、802.11セキュリティは、IEEE 802委員会で検討された。IEEE 802委員会は、LAN（Local Area Network）、MAN（Metropolitan Area Network）に関する規格を扱う委員会である。その中のワーキンググループの一つである802.11グループで無線 LAN の規格が検討されたのが 802.11セキュリティである[6]。無線 LAN は、今後の主流になるので重要視する必要がある。

13時限目　実施ポリシーの策定・運用

13番目の実施ポリシーでは、対策基準・実施要領の策定の策定をする。

実施セキュリティポリシーの運用規定の作成は、標準的規則を教職員組織の各部署の実施段階までブレークダウンする。

セキュリティポリシーの対策基準・要領の策定は、自然災害等の物理対策、情報関係者の管理、各種申請書等の文書管理、各種情報の記憶媒体の管理、業務の継続のためのバックアップ体制、アウトソーシング等の基準策定、セキュリティ実施要領の作成、変更の更新管理、罰則規定の作成や変更の更新管理等を策定する。

これらの策定の手法について講義する。その後で、情報ポリシーの運用とその他評価基準、ガイドライン等の実践的知識と活用法を講義する必要がある[7]。

5）中野明著「ISMS の基本と仕組み」秀和システム　2003年　19頁
6）Bruce Potter 著「802.11セキュリティ」O'REILLY Japan　2003年　10-13頁
7）田渕治樹著「ISMS 構築のための情報セキュリティポリシーとリスク管理」オーム社　2003年　40－64頁

14時限目　演習とまとめ

15時限目　テスト・評価

これが情報セキュリティのカリキュラム案であるが、実施の段階で、セキュリティ技術の進歩は、目を見張るものがあり、その都度新しい詳細項目が出現し変更をする必要があると考えられる。その際は、柔軟な対応をしていく所存である。

## 6．まとめ

セキュリティ問題は、1985年頃から情報処理システムの重要課題になってきた。

筆者は、その脅威と対策について常に考えてきた。情報システムは、汎用コンピュータを主体にした情報システムであり、その脅威は、主に物理的災害、自然的災害、人的災害であった。1995年以降のパソコンLANの普及とＯＳのWindows 95の登場は、インターネットの隆盛をもたらした。この頃より「コンピュータの2000年問題」が起こり関係者の努力により事なきを得た。

近年、インターネットは、コンピュータ犯罪の温床となり、それを防ぐ情報セキュリティの重要性が増してきたとも言える。

そこで、暗号技術による情報の隠蔽が必要となってきた。また、不正なものを進入させない技術は、ファイアウォールの技術の発展をもたらして来たのも事実である。

厳しい防御システムは、それを破ろうとするハッカー、クラッカー、その他犯罪者や愉快犯などによる犯罪を防ぐために活躍しているが、問題点もあり完全を目指して日夜努力しているのが現状である。

技術だけでは、守りきれない側面を倫理やセキュリティの面から、安全な社会を作る必要がある。

そのために、情報倫理教育、情報セキュリティ教育は、しっかりしたカリキュラムの下で教育する必要に迫られている。本論は、情報セキュリティ教育の１セメスター制カリキュラムを考案し、提案したものである。

情報セキュリティの分野は、研究がいまだ緒に就いたばかりでこの論文も先駆けとなるものである。筆者は、今後も継続して研究していく所存である。

**【参考文献】**


（1） Charlie Kaufman, Radia Perlman “Network Security” PTR Prentice Hall, 1995.

（2） Rana Tassabehji “Applying E-Commerce in Business” SAGE Publications, 2003.

（3） Elaine Lawrence “Technology of Internet Business” WILEY, 2002.

（4） Paul Jackson, Lisa Harris,Peter M. Eckersley “e-Business Fundamentals”, Routledge, 2003.

（5） 板倉正俊著「インターネット・セキュリティとは何か」日経BP社　2002年

（6） 打川和夫著「情報セキュリティポリシーの実践的構築手法」オーム社　2003年

（7） 坂野直人著「情報セキュリティの仕組みと対策」中央経済社　2002年

（8） ラックSNSチーム著「ネットワークセキュリティとシステム開発」ソフト・リサーチ・センター　2002年

（9） 三宅功、斉藤洋著「ユビキタスサービスネットワーク技術」電気通信協会　2003年

(10) 梅田博之、山田理恵著「Ｅ－コマースサイトの構築・運用法」リックテレコム　2001年

(11) 一瀬小夜、黒沢裕二著「ウイルスの原理と対策」ソフトバンク　2002年

(12) 白井豊著「情報セキュリティ実践対策」日本理工出版会　2002年

(13) 岸田明著「経営課題としての情報セキュリティ入門」ソフトバンク　2003年

(14) 島田裕次・他共著「情報セキュリティ監査制度」日科技連　2003年

(15) 橋本晋之介著「RSA暗号技術の基礎からC＋＋による実装まで」ソフトバンク　2001年