〔論説〕

文系学生に対する情報管理教育のあり方に関する考察と提言 —1—

太田　聡

あらまし

近年，イントラネットやWebベースシステムなどの技術開発によって，エンドユーザ・コンピューティングの社会に果たす役割が拡大している。この流れは，商学などの既存文系学部で行われている従来の情報管理教育のあり方の変化を促している。具体的には，MIS等の専用システム（クローズなシステム）に必要とされた情報管理から，オープンなシステムで必要とされる情報管理へのニーズの変化である。これはセキュリティやリスク管理を中心とし情報工学的知識が多く要求される為，一般の文系学生のみならず教育者側においても取り扱いにくい対象となっている。しかしながら，インターネットビジネスに対する文系学生の関心が高まる中で，時代に即した情報管理教育の必要性が増している現状を考慮し，ここでは，文系学生に対する情報管理教育に関するフレームワーク（目的，範囲，方法）について考察し提案した。

Abstract

(A proposal on Frameworks of Subject “Information Management” for Students of Faculty of Commerce —1—)

Internet and End-user computing has recently come to play an important role in Social system, accompanying with development of information technologies, such as Intranet, Web-base system and so on. This phenomia causes a change in content of "Information Management" education, that is, from an information management education in closed network system to an information management education in open network system. In this paper, a new framework of Information Management education, for students who have limited chance to study information-subjects in Faculty of Commerce well organized in traditional subjects, are proposed.

キーワード

情報教育，情報管理，文系学生，インターネット，ホームページ

Keywords

Information education, Information Management, faculty of commerce, Internet, Web, WWW

目次

1　まえがき

文系学部における情報管理教育のあり方は，ブラウジング・ソフト出現の以前と以降で大別される。インターネットが一般的でない時代は，MIS (Management Information System)，DSS (Decision Support System)，SIS (Strategic Information System) などの中央センター処理型の各種情報システム(注-MIS) および専用端末操作に必要とされる情報管理教育が中心的に行われていた。また，プログラム言語教育もそれに連動して，事務システム用言語のCobolの教育がなされていた(注—Cob)。

その後，1994年頃以降は，ブラウザソフトの登場によって，急速にインターネット利用が活性化し，1980年代後半から始まっていた分散型処理システムに於いて利用者層を専門技術者から一般ユーザへと拡大させてきた。それに伴い，文系学部における情報処理教育もこの流れに対応することが要求されている。

現在ではさらに，XML，統合アプリケーションソフト(APソフト)，セキュリティなどのインターネット関連技術の進展によって，インターネットを包含した情報システム（イントラネットやWebベース情報システム）へと展開が進んでいる。これらの一連の動きは，エンドユーザに対する情報リテラシー教育の必要性を高め，その結果，教育現場においても今日までに数多くの方法論や事例研究が報告される様になってきた。しかし，こ

れ迄は，インターネット利用や情報化技術の利用促進と浸透を目的としていた為，どちらかと言うと，利便性を中心とした教育がなされてきたと言ってよいだろう。

しかし，本当に情報化技術を一般社会に浸透させていく為には，「情報化社会に対する信頼感」が社会の中で醸成されることが必要であり，その為，それを支える「情報管理教育（セキュリティー教育，情報倫理教育）」を一般ユーザに対して行なっていくことが必要である。

そこで，ここでは，情報化社会（インターネット社会）を定着させていく事を目的として，文系学生に対する情報管理教育はどう有るべきかを検討した。

2　情報化社会の定着に向けた課題としての情報管理

2-1　インターネット（情報化社会）の定着とその課題

現在，日本のインターネット人口が約1500万人(H11.2)を超えたと報告され，また，インターネット通販市場規模に関しては，通販店舗数として約1万2500店(H11.3)，消費者向けEC市場規模として約650億円(H10時点）が推定されている［INT.H-1］。さらに，EC市場規模については，教育課程が改定される2003年には約3兆円に達するとの予測もなされている［JHO.K-1］。この様な状況において，日本におけるネットワークビジネスの立ち後れ［NIK.B-1］や，Webビジネスへの投資の増額を指摘する意見も出されている［NIK.B-2］。

その中で，日本では，近年，電子マネーシステムの実験が相次いで行われている［NIS.S-20］。ただし，今のところインターネットの様なオープン性はなく，限られた地域と参加者（企業，お客）を対象としたリアルモー

ルでの実験となっている。なお，九州でも，①銀行 POS システム(デビットカードシステム）や②電子マネーシステムに関する実験が進められている。①は福岡，佐賀，長崎の三県の金融機関による「Qネット」，および，肥後銀行（熊本県）と鶴屋百貨店との「肥銀バンクポス」などである。②は富士通九州センターが同社のグループ社員を対象として，1997年秋から福岡で開始されている。以下，日本における電子マネーシステムの実証実験の状況を述べる。表2-1-1に神戸と渋谷での実験状況を示した［NIS.S-1］。実験に参加している企業の取り扱う商品に依存するが，今回の実験では，電子マネーの１回当たりの使用料金が千数百円程度となっており，小口利用となっている。正確な分析は後日なされる思うが，システムの構築や維持に関するコスト，および，リスクに関わるコストを考えると，この電子マネーシステムを採算ベースに乗せる為には，一層の，電子マネーシステムの一般ユーザへの教育宣伝が不可欠であると思われる。

また，一方，1998年の後半から米国で，電子マネーの実験の中止が報告されている［YOM.S-1］。オンラインでの少額決済（ｅキャシュ；ネットワーク決済型）を狙った「米デジキャシュ社」が会社更生法の申請を行ない，また，IC カード型に関しても，ニューヨークなどで行なわれていた電子マネー実験（ビザ・インターナショナル，大手銀行４社合同）も次々に中止や苦戦に追い込まれている事が報じられている。この様な米国での電子マネー実験の苦戦の原因として，オンライン少額決済が既存の決済方式に対して明確な優位性を持つ事が出来なかったとの分析がなされている。しかしながら，この様にインターネット先進国の米国で「電子商取引が遅々として進まないこと」の理由として，一般消費者や小規模会社が大手企業や政府を信頼していないことも論じられている［Rog.C-1］。これは，情報化社会への不信感や，情報管理に関する不透明性から生じたものと考えら

表2-1-1　電子マネー実験の状況（西日本新聞より引用［NIS.S-1］）

①スマート・コマース・ジャパン（SCJ）による神戸でのリアルモール実験結果
（1997年10月開始→1998年4月末現在の利用状況）

項目	利用ICカード枚数	使用金額
IC型クレジットカードの発行数 （ビザ系列のクレジットカード）	24468枚	—
電子マネーのリロード（再補充）	7419件	7913万7448円
電子マネーでの買い物	30098件	5617万7961円
	（1回の平均）	1867円
参加店舗	（結果的に，神戸ダイエーの店舗に利用が集中した。特に飲食店売り場）	

②渋谷スマートカードソサエティによる渋谷のリアルモール実験の成果
（1998年7月開始→1998年9月現在の利用状況；実験参加店舗約800店）

項目	利用ICカード枚数	使用金額
ビザキャシュカードの発行数	86000枚	—
（使い切り型）	（51000）	—
（リローダブル型）	（35000）	—
電子マネーのリロード（再補充）	5800件	4416万9000円
電子マネーでの買い物	20098件	2876万7000円
	（1回の平均）	1431円
参加店舗	飲食店5割（主としてスナック，パブ），生活雑貨3割，ファッション2割	

・取材（西日本新聞）協力；郵政省，大蔵省
・データ出典；「郵便貯金ICカード実証実験」（郵政省），「インターネットキャシュサービス開始について」（サイバービジネス協議会），「デビットカードサービス基礎資料」（日本デビットカード推進協議会），「電子マネー及び電子決済の環境整備に向けた懇談会報告書」（大蔵省），「海外のEC関連企業・組織等の動向調査」（電子商取引実証推進協議会）。以上［NIS.S-1］より引用。

なお，「ビザ・キャシュ」は世界標準に沿った仕様であるが，これ以外にも，国際的カード発行会社による電子マネーもあり，標準化競争はこれからと思われる。これらの動向に関しては別報で論説する予定である。

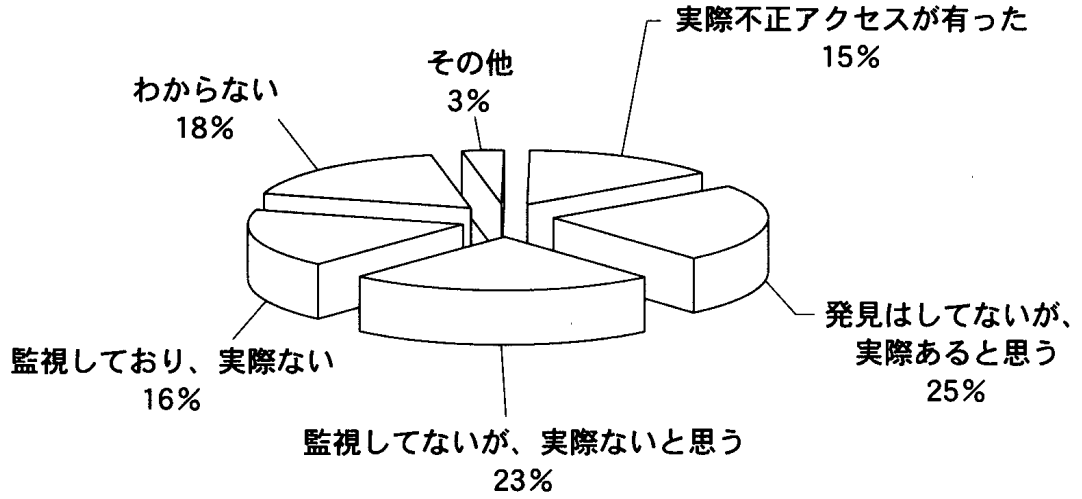
れ，今後，情報化社会が定着していく際の大きなボトルネックになっていくと思われる。その対策として，セキュリティー問題や情報管理など，ネットワーク・ビジネスに関する不信感を払拭する為の教育が大切になると考えられる。むろん，これらの利用者への教育とともに，実質的なセキュリティ対策技術（SET や SSL など）の開発・改善が重要である事は論をまたない（注—SET)。

2-2　インターネット上の情報管理（セキュリティ・リスク管理）の考え方

インターネット犯罪に関する報道が近年増加している。しかし，罰則に対する法的整備が不十分である為，ユーザ側としてはどの様な対応をとって良いか分からない状況となっている。日本では以前よりソフトウエアやデジタル資産に関する権利意識やリスク管理意識が乏しく，1999年初頭の時点で，先進７ヶ国の中で不正アクセスを取り締まる法律がないのは日本だけとなっている。しかし，1998年度版の「警察白書」ではハイテクに関する犯罪について特集がなされ，法的な対応も検討されている(注—法律)ことが報告されている。それらの検討によって，不正アクセス禁止に関する法案が今年の国会で成立し2002年に施行される予定となっている。

次に，企業や社会におけるインターネット犯罪に関する意識レベルについて述べる。図2-2-1に不正アクセスを受けているかというアンケート調査の結果（[NIK.CM-0]）を示した。この上場企業のシステム担当者を対象とした不正アクセスの実態調査（1998年）では，回答社数335社（専用線 IP 接続利用企業＝常時インターネット接続）のなかで15％の企業が実際に不正アクセスを受けている。この種の不正アクセスは，サーバや企業システムへのハッキングの事前段階となっており，放置しておくと企業情報の破壊・盗難・改竄などが行われ，経営資源の損失とともに社会的信用の喪失

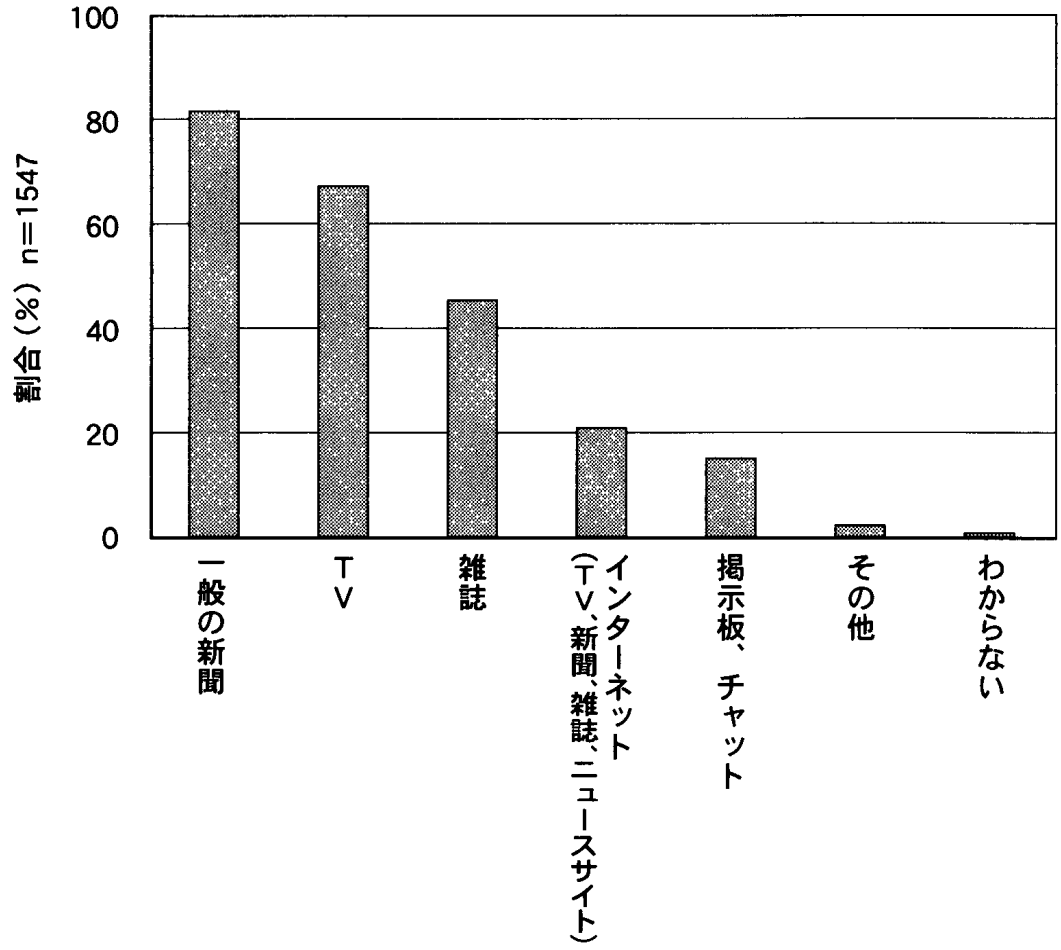
図2-2-1　上場企業のシステム担当者を対象とした不正アクセスの実態調査
（日経コミュニケーションより引用［NIK.CM-01］）



という危険が発生する。この様な状況の中で，企業内のセキュリティ意識は高まっており，ファイアフォールやアンチウィルスソフトが広く利用されるようになっている。また，企業が行なうべき具体的なセキュリティ対策として，①アクセスログの管理，②サーバ（ファイアウォールサーバ，電子メールサーバ，Webサーバなど）ソフト，OSソフト，および，アンチウィルスソフトなどのメンテナンス（バージョンアップ，バグ修正＝ソフト•パッチ），③パスワード管理，④セキュリティ教育，⑤セキュリティ監査などが指摘されている。これらの対策は技術的に難しく 企業の中のネットワーク管理者の責任となっている。しかし，近年の急速な技術革新の進展によって，多くの企業はこれらのセキュリティ技術に対応出来ずにいる。その為，未だにセキュリティに関する社内体制や管理システムが構築出来ていない企業は多い。

なお，この様な不正アクセスなどのハイテク被害を受けているのは企業だけではなく，広く一般ユーザやSOHOユーザも被害者となっている。ただし，この場合，自分が被害にあっている事を認識できるユーザは極めて

図2-2-2　インターネットユーザのインターネット犯罪に関する情報源
（インターネット白書より引用［INT.H-1］）



希であり，現状ではインターネット初心の学生や社会人に於いては全くセキュリティ意識がないと言っても過言ではない。図2-2-2に一般のインターネットユーザを対象とした調査（インターネット白書）結果を示す。これによるとインターネットユーザといえども，現状では新聞やTVなどを通してインターネット犯罪の情報を得ている状況が覗われる。今後は学校でセキュリティ教育が充実していくことが望まれる。

一方，セキュリティ対策に関して次に述べる動きに注目したい。即ち，インターネット技術の普及に伴ってASP (Application Service Provider) という概念が，米国で盛んになっている［NIK.B-3］。これは，ネットワー

クを介して行なう「業務のアウトソーシング」に関するもので，ASPとは具体的には，インターネット販売システムや顧客管理などのサービスを，サーバシステムの構築と管理を含めて委託される外部業者のことを指している。インターネットにおける電子メールサービスやWWWサイト管理を行なっている商用ISP（Internet Service Provider）がASPの原形と考えられる。このASPは，さらに，顧客に関しては個人から企業へ，業務に関しては電子メールから基幹業務へと拡大したものといえる。この動きと共に，インターネット上のセキュリティに関しても，企業内で対応するよりも外部委託で行なう方が，コストや人材育成の手間に関し有利と考える動きも盛んになっている[NIK.CM-1]。この動きは，今後進展していくと思われる。しかし，インターネット等に関する犯罪は，内部不正によるものが多く[NIK.CM-0] [NIK.CO-1]，情報セキュリティのアウトソーシング，即ち，情報管理の「人任せ」は危険に関する本質的な対策にはならないと思われる。むしろ，この様な情報セキュリティ対策の外部発注は「時間がない」とか「技術がない」という問題に対する補足的対策に過ぎないと筆者は考える。今後は，学校教育の中で，セキュリティ教育，広義には情報管理教育を充実させ，将来の社会システムが健全に運営される様になる事を期待する。

3　文系学部におけるインターネット・情報教育の現状と方向性

3-1　既存学部におけるインターネット教育と情報管理教育

さて，ここで，学校における情報教育に目を向けてみる。近年，インターネット（Web，電子メール，ftpなど）を取り入れた情報教育が盛んに行われており，特に，Webサイトに関係した教育手法が教育研究会において数

多く報告されている[Kam.S-1]，[Ari.T-1]，[Kun.Y-1]，[Niw.T-1]。しかし，一般的に既存の文系学部の場合，学部として必要な科目が多数ある中で，情報教育は限られた時間の中で行なわれている。例えば，商学部における情報教育に関しては，商学に必須な商学系科目(流通，貿易，交通，金融，マーケティングなど)，経営学系科目(企業，経営，財務，労務など)，および，会計学系科目（簿記，会計，税務，など）と共に，情報学系科目(情報処理など)が少数ながら開講されている。そして，そこでは，基本的なアプリケーションソフト（ワープロ，表計算，プレゼンテーション）の利用方法を中心とした教育が行なわれ，一連の講義の後半でやっとインターネット利用(e-mail，Web)の指導が可能となる。1例として本学商学部の場合を考えると，H10年度の時点でインターネット利用学生の割合は，受講者数と講義内容から判断して，約1～2割と推定される。また，情報処理科目（情報処理概論）の授業の中で行われる情報管理教育に関しては，一般的にはFDの個人管理やパスワード変更などを初期の時点で指導するに留まっている。この様な状況は，日本の既存文系学部の共通の現象と考えられる。

一方，H10年頃から，就職活動の際にインターネットを利用する企業が顕在化し[NIK.B-0]，大学や学生も積極的にこの動きに対応していこうとしている。具体的には，企業側では，従来のインターネット上での会社案内や就職ガイダンス情報の掲示から，H10年度では就職試験エントリーシートの配布（ダウンロード）に至るまでインターネットの利用を広げており，また，学生側では，ニュースグループやWeb掲示板を利用して面接試験情報の交換などを行なう者が出てきている。インターネット上のエントリーシート（就職活動における企業アクセスの第一歩で，履歴書の一歩手前の書類である）の活用例としては，1998年度卒業生の場合，例えば，

ソニーの文系学生の採用試験で，エントリーシートを提出した5000名から一次選考で1000名に絞ったことが報告されている[NIK.B-0]。また，直接，学生と電子メールのやり取りをする企業も現れている。

この様な直接的な就職活動とは別に，文系の学生側に於いても，個人的にインターネットに深い感心を抱くものが増加しつつあり，商用IP業者との接続，外部から学内LANへのアクセス，および，インターネットビジネスへの展開を希望する動きが出始めている。大学サイドでも，近年，インターネット，Windows，Officeなどを中心とした教育を全国的に行なうようになってきているが，以上述べた最近の動向（需要）に対応しきれない状態にある。情報教育に関する限られた時間の中で，この新しい動きに対応していく為には，情報教育のフレームワークを見直す必要があると考えられる。

3-2　文系学部の情報教育における，新しい動きとしてのセキュリティ教育

2-2項で述べた企業における不正アクセスなどのインターネット犯罪が，今日では，大学にとって「対岸の火事」ではなくなってきている。これまで，情報化教育に関しては，欧米に比べて立ち後れている日本の現状を踏まえ，情報化技術の浸透を目的として主として利便性を中心とした教育がなされてきた。しかし，前述した様にインターネットに関しては，初心の学生には把握しきれない数多くの危険や問題が存在している為，教育者側はこの課題に対応していく必要がある。

不正アクセスの具体的な中味と歴史を表3-2-1に示す。日本では，まず，1980年代の後半から，コンピュータへのハッキングに関する報道や解説記事が出てきた(注—ハック)。その後1995年に日本で初めてのハッカー被害届（パソコン通信でIDが盗用）が出されて以来ネットワーク犯罪の報告が

増加し，さらにインターネットの普及に併せ，特に1997年から被害や対策に関する記事が急増している[NIK.CO-01]，[ASA.S-1]，[NIK.CO-02]，[NIK.S-01]，[NIK.CO-03]，[NIK.CO-04]，[NIK.S-02]，[NIK.S-03]。当初は，企業のネットワーク犯罪の被害額が１企業100万ドルと報道される[NIK.B-01]中で，大学関係へのハッカー行為はあまり表に出ていなかった。しかし，1997年10月に報道された東大の大型計算機センターへの不正アクセス事件[MAI.S-01]などから推測される様に大学のネットワークはもはや安全とは言えなくなっている。

この様な現象を反映して，情報倫理教育の必要性が一般新聞でも言われるようになってきている[ASA.S-2]。大学教育においても，近年，エンドユーザ（学生）に対する情報セキュリティや，情報倫理（モラル）教育に関して，多くの検討がなされる様になってきた[Sho.M-1][Nag.k-1][Yam.N-1][Mur.T-1][Kud.H-1][Shi.Y-1][Wat.N-1]。この動きは現在のインターネット利用に関する安全性のレベルから考えると不可欠のものといえる。

しかし，情報に関わるセキュリティ技術は工学的な内容を多く含み，文系学生には難しい内容となっている。そのため，文系学生に対するセキュリティ教育に関しては，現在，主としてパスワード管理に主力が置かれている。また，倫理（モラル）教育に関しては，対象が広範囲に及ぶものの「倫理」という言葉からくる制約によって，必ずしも，学生にとって分かり易い体系化になっているとは言えない。其のため，今後は，早急に文系学生に適したカリキュラムを考えていく必要がある。なお，後者の「倫理教育」に関しては，辰巳らによって，「情報倫理教育」から「情報危機管理教育へ」という提言も出されている[Tat.T-1]。

表3-2-1に不正アクセスの具体的な被害例。（日経コミュニケーションから引用）

報道時期	被害に遭った企業・機関	業種	被害の内容
97／5	朝日放送	マスコミ	WWWサーバに不正アクセスされ，天気予報のページが書き換えられた
6	NTTPCコミュニケーションズ	プロバイダ	ダイヤルアップ会員のID／パスワードが外部に漏洩
9	NTT四国支社	通信	社内ネットワークに不正侵入
10	NTT情報通信研究所	通信	社内ネットワークに1年にわたって不正侵入され，開発中のソフトウエアのソース・コードが漏洩
98／1	通産省	官公庁	メール・サーバをスパム・メールの中継に悪用された
	ポンポンネット	プロバイダ	社内ネットワークに不正侵入され，会員情報が外部に漏洩
3	JPNIC	社団法人	ドメイン名を管理するサーバに不正侵入
	トヨタ自動車	製造業	カタログ請求者の個人情報の一部が外部に漏洩
5	ソニーコミュニケーションネットワーク	プロバイダ	ダイヤルアップ会員のパスワードを類推する不正アクセスを受け，一部ID／パスワードが漏洩
	リムネット	プロバイダ	ダイアルアップ会員のパスワードを類推する不正アクセスを受けた
	ジェントリー	パソコン販売／プロバイダ	クレジットカード番号を含む会員情報が外部に漏洩
10	オリコン	市場調査	アンケート回答者の個人情報が外部に漏洩
	ガジェット	市場調査ほか	社内ネットワークに不正侵入され，会員情報の一部が漏洩
12	近畿大学	大学	学内ネットワークに不正侵入され，ID／パスワードが漏洩
99／1	北海道教育大学旭川校	大学	学内ネットワークに不正侵入
5	リムネット	プロバイダ	会員ID／パスワードが第三者に盗まれ，これを基にスパム・メールが大量に送信された
6	毎日新聞	マスコミ	WWWサーバに不正アクセスされ，トップページが書き換えられた
	朝日新聞	マスコミ	WWWサーバに不正アクセスされ，トップページが書き換えられた

([NIK.CM-1]「(特集) プロに任せるセキュリティ対策」，日経コミュニケーション，1999.9.20号，(1999) p.94-111)

4　これからの情報システムに関する１つの方向性

「情報システム」そのものに関してはこれまで多くの研究と開発がなされている。この情報システムの対象業務については，花岡によってシステム化が①「強制される業務（C型業務）」と②「自発的な業務（S型業務）」に分類されている[HAN.S-1]。①のC型業務は大量情報処理やバッチ処理的なプロセスが多く，その為「業務的MIS」として以前よりコンピュータ利用が進んでいる業務である。②のS型業務は非定型，非構造的な情報処理である為コンピュータ処理は困難と考えられ，「管理的MIS」，「戦略的MIS」として進化が要求されてきた。「業務的MIS」は，業務の効率化という観点から，企業経営に与える効果は主として経費の節約に繋がる為「消極的利益確保の為のシステム」と表現することが出来る。一方，「戦略的MIS」は，新しい商品開発，業務開発が期待されているので，「積極的利益確保の為のシステム」であり，企業経営において高い期待が寄せられている。しかし，人の判断領域（不確実性）に立ち入る為，期待する成果が得られにくい傾向がある。其の為，これ迄に，数々の理論と試行錯誤を経て，MISから意志決定支援システム(DSS)，そして戦略的情報システム(SIS)へと発展的移行が行われている［Aki.T-1］［Kat.T-1］。

これまでのこの様な情報システムの発展における特徴を著者なりに表現すると，①従来の企業内業務をどの様にコンピュータ化するかという試行錯誤的システムの開発，②システム内の情報を如何に利用するかを中心とした性善説的システムの開発（情報が改竄されているとか，間違っているデータがあるとかについて，利用者はほとんど考えていない），③システムの大規模化に伴い，従来の手工業的システム開発から工業的なソフトウエ

ア開発（定型的は方法論や技法を用いる）への移行［TAC.S-1］。④大型汎用計算機を中心とする中央センター処理型システムの開発，⑤専用端末，専用回線（もしくはLAN），専用ユーザからなるシステムの開発（分散型システムの場合でも同じ），などを挙げる事ができる。

今後の動向としては，これからも，この様な大規模の情報システムは資産として残っていくであろうし，また，大規模組織における業務的MISは有効なシステムとして継続されていくと思われる。しかし，一方で，インターネットを中心とする情報化・ネットワーク化技術の進展によって，これからの情報システム構築に際し大きな影響を与えていく因子がある。それは，(1)オープンネットワークの利用，(2)システムユーザに対するWebベースの共通プラットフォーム化の普及，(3)電子商取引の進展，などである。これらによって，これまで組織の中で分離・整理されていた業務［Kat.T-1］［Uot.K-1］がシームレス化していく，また，同時に，企業間の業務もシームレス化が進んでいく。このことは，論理的な情報システムと物理的な情報システムとの乖離が進んでいくを示唆している。情報管理教育という観点で考えると，(a)論理的情報システムの拡大はユーザにとって使いやすいシステムの構築に繋がり，従来の「利用促進を中心とした情報管理教育」は「マネージメント・サイエンス」にシフトし［TAC.S-2］，また，(b)物理的情報システムの複合化はユーザにとってセキュリティ管理やリスク管理などの新しい情報管理教育が要求されることを意味している。

それでは，この様な情報システムに関する動きについて少し具体的に述べておく。まず，(1)の「オープンネットワークの利用」についてであるが，これはLANや専用回線などのクローズなネットワークを用いた情報システムから，インターネットや一般回線を利用した情報システムに変っていくことである。それでは，我々一般ユーザ，もしくは，インターネットビ

ジネスを考える文系学生にとって，この様な「オープンなネットワークを利用する」とは一体どのような意味を持つものであるのか？ 電気通信事業者が進めているネットワークのオープン化（注—オープン）は，上記のオープンなネットワークとは若干意味合いが異なる。しかし，セキュリティ確保を必要とするユーザの観点から眺めてみると，１つの利用可能な技術に突き当たる。それは，インターネットを利用したVPN(Virtual Private Network)である[NIK.CO-30]。現在試行されつつある具体的な例としては，例えばネットワークとしてNTTのOCNを使用し，さらにVPN用装置とソフトを導入して，全国の拠点間における全通信を暗号化するネットワークシステムがある。VPNは従来からあるWAN(wide area network)の形態の１つであり，従来のものとしては例えば①フレーム・リレー網やATM網をベースにして構築した「閉域のビジネス向けIPサービス」，②専用線，および③フレーム・リレーなどがある。その中でこのインターネットVPNは通信料金が安いという観点から，将来に対する可能性は高いと考えられる。むろん，セキュリティやスループットは専用線を利用する場合に比べて問題は残っているが，専用線のコスト負担に耐えられない企業などに於いては有効なネットワークシステムとして利用されて行くと思われる。

次に，(2)の「システムユーザに対するWebベースの共通プラットフォーム化の普及」に関しては，(1)のオープンネットワークの利用と連動したものであり，その関連から次の様に表現出来る。即ち，1995年以前（Webブラウザの出現によって爆発的にインターネットがブームになる以前）から検討が進められていた各種情報システムは基本的にはクローズなネットワークを用いたシステムになっている。そして，1995年以降は，家庭や一般企業からのインターネット接続の普及に伴い，インターネットユーザが

ネットワーク大衆となりつつある為，ネットワーク・ビジネスに対するマーケティングが変化してきた。その結果，それまでに検討中もしくは実験中の各種情報システムは，インターネット対応への変化を余儀なくされている。たとえば，電子商取引に関する電子マネーのプロトコルについてはTCP／IPをベースとしたSSLがSETより普及していること，また，DBに関してはWWWブラウザから各種のツールや言語を介してRDBMS (relational database management system) へアクセスするなどの技術を例として挙げることができる(注－DB)。学校での教育システムも同様な経緯を経ている。そして，今後，ネットワーク情報システムを考える場合，インターネット関連技術とインターネットユーザの動向は重要な判断要因となっていくと思われる。

最後に，(3)の「電子商取引ECの進展」に関して述べる。EC，EDIとも，インターネットブームが始まる以前より提案されている概念であるが，現在では，インターネットの普及がEC (electoric commerce) やEDI (electoric data interchange) を引っ張っり始めている。セキュリティに関して大きな課題が残っているが，1999年から日本ではECに関する大きな実証実験が開始されており，新たな段階に入りつつある。今度構築される各種情報システムはこのEC，EDIと連携がとれたシステムとなることが要求されて行くだろう。なお，これらに関する論説は別途報告したい。

以上述べたように，今後の情報システムはインターネットを包含しながら進んで行くと思われる。その際のキーワードは，XML，SSL，モバイル，インターネットVPN，共通プラットフォームなどである。これらのキーワードはこれからの文系学生にとっても必要な事柄であるので，別途，整理をしていく予定である。

5　既存文系学部におけるこれからの情報管理教育のフレームワーク

以上，述べてきた様に，今日のインターネット時代に於いては，文系学生といえどもセキュリティ管理・リスク管理を中心とする情報管理教育が必要である。そこで，本章ではその情報管理教育のフレームワークについて考える。まず，情報管理教育の対象範囲として，①情報保管技術としてのファイル保存･管理から，②プライバシ管理（個人情報管理），③セキュリティ管理，④情報の有効利用方法(従来の情報管理)，⑤著作権侵害，までを捉えることとする。

なお，情報保管技術，プライバシ管理，および，セキュリティ管理は危機管理（リスク管理）に直接対応している。学生にとっては，「情報管理」という語感よりも「危機管理」の方が，具体的なイメージを描きやすいとも考えられるので，ここでは，情報管理と危機（リスク）管理とを，同じ位置づけにおいて考えていくことにする。また，セキュリティ管理という言葉に関しても，同様な観点で広義に解釈し，情報管理や危機管理(リスク管理)と同様に扱う(言い換えると，本論文の段階では明確な区分や定義はしない）こととする。なお，情報セキュリティそのものを対象とすると，内容が理工学的となりかなり難しいものなる。

5-1　危機管理から見たエンドユーザの守備範囲

ファイアウォールを中心とする業務上のリスク管理（危機管理）に関しては，主としてネットワーク管理者の責務である。しかし，セキュリティホールのチェックという観点では，関連する全ての項目や人間を対象として相互関係の中でセキュリティを考える必要がある。その為，ネットワー

表5-1-1　危機管理(リスク管理)の構造

危機管理レイヤ	NW 管理者	EU
③法律的に対応（権利意識）	○	○
②技術的に対抗（力比べ）	◎	△
①危険事項からの回避（逃げ）	—	◎

ク管理者とエンドユーザ (EU) との連携が重要である。そこで，この観点からネットワーク管理者とエンドユーザとの守備範囲の枠組み（危機管理の構造）を整理して表5-1-1に示した。

エンドユーザへの教育としては，まず，①危険事項からの回避が重要である。これは危険なサイトへのアクセスや危険なサイトからデータをダウンロードしないこと，および，危険なメールなどに関する対処方法に関する教育となる。②に関しては，エンドユーザでは対応が困難であり，主として，ネトワーク管理者が行なう領域となる。しかし，エンドユーザに対しても，パスワード管理やウィルス対策などの基本的知識に関する教育は不可欠である。さらに，今後は，エンドユーザにとっても，③の法律的対処に関する知識が必要なものになっていくと予想される。ただし，現在の段階では,インターネット犯罪に関する法的整備は遅れているので(注—法律)，教育の場で早急に対応することは難しい。

5-2　危険（リスク）の分類

ISO (国際標準化機構) で制定されつつある「セキュリティ評価基準」に，「想定される脅威」と「その対処方法」が詳細に整理されている [NIK.CO-3]（注—ISO)。しかし，そこで述べられている表現は，管理者 (専門家) 向けのものであり，一般ユーザにとっては若干解りにくい内容となっている。「情報」自体が一般ユーザにとって抽象的なものであり，その情報に関

表5-2-1　リスクの分類

リスクの分類	リスクの中味		主たる対策
取引系リスク	詐欺商法	・商品が届かない ・不良商品	相手先確認 別連絡方法
	ID/Passwordの無断使用	・偽発注 ・口座無断使用	Password管理
コンテンツ系リスク	情報流出	・金銭的損失 ・プライバシーの侵害	個人情報管理
	情報流入	・スパムメール ・ウィルス	メーラ，アクセス先の管理 著作権侵害
	改竄	・財産・信用の低下	
通信系リスク	傍受	・情報財産の消失	ハブの管理 サブネット管理
	不通・中断	・仕事の中断	
ソフト系リスク	破壊	・再購入支出	ウィルス等の管理
	一時故障	・仕事の中断	
ハード系リスク	情報破壊	・財産の消失	記憶媒体の管理
	一時故障	・仕事の中断	

わる危機(リスク)・セキュリティや損害などと言っても，具体的なイメージを持たせる事は困難である。その為，一般ユーザにとって身近な環境の中で，情報に絡むリスクとその管理を分かり易く表現していく事が必要である。

表5-2-1に，エンドユーザコンピューティングの要素を基に，リスクの分類を行なった結果を示す。

なお，コンピュータネットワークのリスクとして，①管理系，②侵入系，③障害系に分類している例もある［Hir.T-1］。ユーザとしてリスクを全体的に理解する場合は有効な分類だと思われる。参考として，それを表5-2-2に示す。

表5-2-2　コンピュータ・ネットワークリスクの分類
([Hir.T-1] から引用)

分類	項目
管理系リスク	パスワード管理関係
	コンピュータウィルス関係
	著作権侵害
	オフィスの機密データの持ち出し
	電子メール
	インターネット関係
	ファイル（文章，画像など）等のバックアップの不備
	パソコンや周辺機器の乱暴な取り扱い
侵入系リスク	ハッカー（正式にはクラッカー）による被害
	インターネット関連
障害系リスク	地震，火災，ソフトウェアのバグ，事故

5-3　Webサイトの危険性に関する教育

Webサイトは既にクラッカー達の標的にされており，これまで，FBI，米国エネルギー省，および，米国上院などのWeb掲示板への不正書き込み等のニュースが数多く報告されている [Mae.T-1]。このWebサイトへのクラッカーの侵入手口は技術的に高度かつ最新である為，文系の学生，一般ユーザ，および，教育者側では対応が取りにくい状況にある。その為Webサイトの管理に関しては，一般的にネットワーク管理者が行い，文系の学生や一般社員は基本的に関与していない。その為か，学校でWebサイトの危険性を教育している事例はあまり報告されていない。

しかし，現在，学校における情報教育がWebを中心に展開されつつあること，および，第4章で述べた様に社会における各種情報システムもWebベースとなる傾向を示していることから，文系学生に対するエンドユーザ

表5-3-1　Webに関係した具体的危険性（可能性があるもの）

個人情報の漏洩	Webサイトへのアクセスで，自分の使用しているブラウザ，IPアドレス，ドメイン，メールアドレスなどが相手先に知られる。
	接続先が記録するログ情報（IPアドレス）から，自分の所属や場所がある程度特定される。
	契約しているプロバイダがハックされると，自分の個人名も特定される。
	ディスクキャシュ（Webの閲覧履歴）の中を見られる
	自分のメールアドレスを不特定多数に知られる。
作成した情報の漏洩	送信した情報を，転送中に第三者に監視される。
	自分達のローカルファイルが読まれる。
パソコンへの侵入と操作	ハードディスクの中味を書き換え・消去させられる。
	自分のパソコンを勝手に操作される（サーバソフトの埋め込みとクライアントソフトによる操作）
	意図的なプログラムを実行させられる（バグを利用して）。
	悪意のあるCGIを読み込む。
	ブラウザを異常終了させられる。
パスワード	パスワードを破られる（知られる）。

教育においてもWebのセキュリティに関する問題は今後避けては通れないと考える。

Webに関するリスクとその対策に関しては別報告にて整理しようと考えているが，大まかには表5-3-1に示すような項目が考えられる。

これらに関する技術的内容はかなり難しいが，エンドユーザ側としては，ある程度の知識を持ち注意をしていれば防げることが多い。其の為，今後は，文系学部でも，技術的内容に踏み込みながらWebサイトに関するセキュリティ教育を行なう事が望ましいと考える。

6　むすび

情報化社会の定着に向けて，文系学生（商学部）対する情報管理教育について検討を行なった。

学問領域（科目）が確立されている既存の文系学部では，情報関連の授業数は限られている。また，今日のインターネットブームの中では，文系学生に対してもオープンシステムにおける分散処理型エンドユーザコンピュティングの利用が期待されていること，および，学生自身もインターネットビジネスに多くの関心を示しているので，インターネットを中心とした教育を効率良く行なうことが不可欠であると考えられる。

一方，インターネットには多くの危険性が潜んでいることから，本報告では，文系学部の情報教育の中に，インターネットの危険性に関する管理教育が必要であることを指摘し，その教育を効率的に行なうことを目的に，情報管理教育のフレームワークを提案した。

注釈

●(注－MIS)

MIS, DSS および SIS に関しては多くの解説書が出されており，改めてここで注釈を付ける必要はないが，簡単に内容を確認をしておく。

MIS（Management Information System，経営情報システム）は，コンピュータ(第3世代以降)を利用した経営機械化であり，1960年代後半から脚光を浴びた概念である。これはコンピュータシステムと経営活動全体の総合的システム化によって，情報処理システムを介した経営活動の統一性を求めるという目的を持ったシステムである。日本では，1958年に日本 IBM が自社内で汎用中型コンピュータ IBM650を設置し業務用に導入し，MIS の先鞭となっている。しかし，この MIS は専門の技術者集団好みの開発となり易く，業務現場との連携が必ずしもうまく行かない状況が多く発生し

た。その為，今日ではMIS失敗論が語られている。

DSS（Decision Support System，意志決定支援システム）は，1971年にMichael S. Scott Mortonによって提唱された経営上の意志決定支援システムで，データベースとモデルベースを基盤とし，インターフェースを介して経営者や上位管理者の持つ非構造的または半構造的な問題についての意思決定を支援するシステムである。1977年のSan JoseでのDSS会議，1981年の国際会議を経て，世界的に広まっていった。この時代から，第4世代言語への期待が高まっている。

SIS（Strategic Information System，戦略的情報システム）は，1980年代後半から登場した概念で，差別化戦略を情報システムで支援する目的を持ったシステムである。業務間結合や企業間業務統合が対象とされ，ネットワークが重要な意味を持つようになって来ている。

（[Wat.S-1] 渡部栄，「情報管理概論」，白桃書房，(1997)，2版，[Miy.K-1] 宮下幸一，「情報管理の基礎」，同文館，(1998)，7版，[Sas.H-1] 佐々木宏，「図解 経営情報システム 理論と実践」，同文館，(1997)，初版）

●(注－Cob)

第3世代言語に属するCOBOLは，CODASYL委員会によって制定された事務処理計算用言語で，英文に近い記述が可能であり，汎用性が高い。其のため，現在でも，事務処理アプリケーションの分野（オンライン・アプリケーション，バッチ処理とも）では圧倒的なシェアを有している。そして，多くの企業はCOBOLファイルの資産を多数抱えている。

10年以上前から，「COBOLは徐々に第4世代言語に置き換わる」と言われているが，この4GLが最終的にどの様なものに落ち着くか未だに定かではなく，其のため，今後も，COBOLの地位は変わらないと思われる。しかし，同じく10年以上前からワークステーションの導入が進んでおり，今後新しく分散型システムを構築する場合は，増加しつつあるC言語技術者がワークステーションの良さを生かせるCを用いて分散処理システムを構築していく可能性も高い。ただ，マルチウインドウやマウスなどを使うアプリケーションに関しては，ユーザ・インターフェースの部分（C）とアプリケーション本体(COBOL)とを別々に作成する様になっているので，用途に応じてそれらの言語は使い分けられている。因みに，10年前は，主なUNIXマシンが20台(20種類)あるとすると，その内，C言語は18台，COBOLは1台に標準提供されていた。オプションを含めてもCOBOLは8種類のUNIXマシンでしかサポートされていなかった(日経コンピュータ，1990／5／7号，(1990) p.109-117)。今日では，(インターネットでCOBOLの検索をすると)，Windows OS上で28件，Mac OS上で0件，Unix OS上で11件，M／F上で2件(WindowsとUnixでは重複有り)となり，COBOLが徐々にワークステーションに移植されていることがわかる。このことは，今後とも企業はCOBOL資産を継承していく意向を持っていることを示すものと考えられる。因みに，日立製作所では，「COBOLのスキルで手軽にWebアプリケーションの開発ができる

表ー付録1　ミドルシステムの開発例（インターネットWebページより引用）
(http://www.jsc.co.jp/textpage/welcomt.htm 株式会社ジャパンシステムクリエーション)

ミドルシステム部開発事例		
概要	プラットフォーム	開発言語
モバイル連携ミドルウア設計開発	UNIX, Windows 95, Windows NT, Windows NT サーバ	Visual C++, Visual BASIC
Java 運用支援設計開発	オフコン	C, Java
グループウェア設計開発	Windows 95, Windows NT, UNIX	Visual C++, Visual BASIC
コード変換ツール設計開発	オフコン	C
物流業務支援システム設計開発	Windows 95, Windows 3.1	Notes, Excel VBA, Form WAVE
DB 管理システム設計開発	Windows 95	Visual C++, ORACLE
証明書クライアント設計開発	Windows 95	Visual C++
イントラネット情報システム設計開発	Solaris	C, SQL
通信プロトコル制御機能設計開発	Windows 95	Visual C++
インストール支援ツール設計開発	オフコン	アセンブラ
性能解析支援機能設計開発	オフコン	アセンブラ
保守支援機能設計開発	オフコン	アセンブラ
書類ファイリングシステム設計開発	Windows 95	Visual BASIC, イメージギア, Acrobat SDK
情報検索システム設計開発	Windows 95	Access
受発注管理システム設計開発保守	オフコン	COBOL
物流管理システム設計開発	Windows NT	Visual BASIC, SQL Server
登記簿管理システム設計開発	Windows 3.1	Excel, Visual BASIC
クラサバ連携ビジネス向けミドルウエア	オフコン, UNIX, Windows NT サーバ	Visual C++, C

スクリプト言語」として，「COBOL スクリプト，500000円」を販売している。具体的には，「Web ブラウザ」+「HTML」+「Active X」で画面を作成して，HTML に COBOL スクリプトを埋め込み記述することで，Web ブラウザ上で数値チェックや計算処理，オブジェクト操作を可能にしている。これによって Web ベースの業務システムの構築が可能となっている。

なお，この様に，メインフレーム対応のシステム開発（COBOL を使用）の需要は，今後とも落ちる事はないが，中規模以下の新しいシステムの開発に関しては，やはり，C 言語の利用が進んでいくと思われる。参考として，表にインターネットに掲載されたソフトウエアハウスの宣伝記事を示す。

ただし，「第 4 世代言語（4GL：4th Generation Language」とは，定型的な事務処理を行うためのオンラインのアプリケーションを，実際にアプリケーションを使う人（エンドユーザ）が対話形式で設計・開発できるようしたプログラミング言語と言われている。この 4GL は，COBOL などの専業プログラマを必要とする従来のプログラミング言語よりも生産性が高いとされている。機械語を第 1 世代，アセンブリ言語を第 2 世代，COBOL などの高級言語を第 3 世代と呼ぶことから，第 4 世代と呼ばれている。

●（注－SET）

SET（secure electron transaction）とは，1996年，Master Card 社（SEPP 方式）と VISA 社（STT 方式）が合意して決めたもので，電子商取引（EC）のトランザクションにおけるセキュリティを守るための方式である。

SSL（secure socket layer）とは，ネットスケープコミュニケーションズ社が提供するセキュリティ機能である。SSL は上位プロトコル（HTTP, SMTP, FTP, NNTP）と TCP/IP の間に位置し，上位プロトコルから受取ったデータを暗号化して TCP/IP に渡す機能を持っている。SSL が組み込まれた OS，クライアントソフト，サーバソフトを使用すると，ネットワーク上では，自動的に暗号文にされたデータが送られることになる。暗号化の他に，認証や電子署名の機能も備えている。

現在，SET より仕組みが簡単な SSL の方が普及している。しかし，現在のところ SSL はクレジットカードのみに対応しているのに対して，SET はデビットカードやチップカードにも対応する。そのため，複数の通貨や多様な金融機関が利用出来るというメリットが SET にはある。

●（注－法律）

1998年版警察白書（1998.9.11発表）では，「ハイテク犯罪の現状と警察の取り組み」が特集として取り上げられている。そこでは，インターネットの普及などによって，5 年間で 8 倍と急増し深刻化するコンピュータ犯罪に対処する為に，法律を整備し，専門捜査体制を強化していく方針が打ち出されている。また，ハイテク犯罪の特徴として，①匿名性が高い（ID 番号などを利用するため），②犯罪の痕跡が残りにくい，③被害が広範囲に及ぶ，④証拠の隠滅が容易（デジタル情報であるため），⑤国境がボー

ダレス，などを指摘している。さらに，今後の動向として，(1) EC や EDI の普及に伴い，経済犯罪事件のハイテク化が進む，(2)社会機能を不全に陥れる「サイバー（電脳）テロ」の発生，(3)誘拐などの凶悪事件にインターネットなどを使用する，などを予測している。そして，それらの対策としては，(a)コンピュータネットワークへの不正アクセスの禁止／処罰する法律の制定，(b)「サイーバーポリス（電脳警察）」体制の確立などの方針を示している（以上，1998.9.11および，1998.9.12の各種新聞記事より要約した)。

なお，1999年になってから，「不正アクセス禁止法案(警察庁，郵政省，通産省の三省庁)」が4月16日に閣議決定され，8月6日「不正アクセス行為の禁止等に関する法律」として国会において可決・成立，8月13日に公布された。施行は，一部を除き，平成12年2月13日からとなっている。

一方，中央官庁の行政文章を対象とした「情報公開法」が1999.5.7に成立し，政府は制度開始に向け作業を本格化させることが新聞で報じられている［ASA.S-1]。

なお，現（1999.10.）時点でも，ハイテク犯罪に関する法律は未だ整備されていないが,既に存在している刑法でインターネット犯罪に関係しそうなものを下記に示す。

表一付録2　法律

名称(罪)	罰
電磁的公正証書原本不事実記載罪	5年以下の懲役もしくは50万円以下の罰金
不実電磁的公正証書供用罪	5年以下の懲役もしくは50万円以下の罰金
電磁的記録不正作出罪	5年以下の懲役もしくは50万円以下の罰金
不正電磁的記録供用罪	5年以下の懲役もしくは50万円以下の罰金
電子計算機使用詐欺罪	10年以下の懲役（未遂も含む）
電磁的記録毀棄罪	3ヶ月以上7ヶ月以下，5年以下の懲役
文書偽造罪	それぞれの法令により罰せられる（未遂も含む）
著作権違反罪	著作権法による
わいせつ文章等頒布（はんぷ）罪	2年以下の懲役もしくは250万円以下の罰金 もしくは科料

この他，内容によっては，横領罪，軽犯罪，詐欺罪，恐喝罪，侮辱罪，名誉毀損罪，業務妨害罪，信用毀損罪，脅迫罪などに該当することもある。

因みに最近の例として，インターネットのホームページに「知人を殺してほしい」などの文面を掲示したとして，大阪の女性が脅迫容疑で，京都府亀岡区検に書類送検

されたことが新聞で報じられている。実害がないものの記載内容が具体的であり，主婦が恐怖を感じていたことから「脅迫罪」が適用可能と判断されている［YOM.S-1］。

（［ASA.S-1］「情報公開法成立　関連政令は来月以降」，朝日新聞，平成11年5月7日［YOM.S-1］“ネットで「あの人殺して」”，読売新聞，1999/9/22））

●(注－ハック)

ハッカーとクラッカーとの違いに関する記述は多く見かけられるが，一般誌では「ハッカー」という表現を用いている場合が多い。その理由として，クラッカーという言葉がまだ一般的ではない為と考えられるが，一方，法的対応（他のコンピュータシステムへの侵入が意図的か，偶然か，或いは，何らかの損害を与えたか，与えないかなど）がまだ十分になされていないことも理由の1つとして考えられる。

1980年代の後半に一般読者を対象に出されたハッカーに関する記事としては次の様なものがある。①「米国ではハッカーが年々増倍，日本でも同じようになる」，日経コンピュータ，1986/11/10号，(1986) P.38，②「ハッカーの侵入を防ぐデータ通信用セキュリティ・システム」，日経バイト，1986/12/1号，(1986) P.80，③「混沌の館にて：ハッカー会議」，日経バイト，1987/5/1号，(1987) p.223，④「脳のダウンロードを題材にAI研究者・ハッカーたちが夢を語る：トゥモローメーカー」，日経エレクトロニクス，1988/5/16号，(1988) p.269

なお，IETFがRFC1983において行なった定義は以下の様になっている。

「ハッカー」；システム，特にコンピュータやコンピュータネットワークの内的な働きを深く理解することに喜びを覚える人。

「クラッカー」：コンピュータシステムにアクセス権限を持たないのにアクセスしようとする人物である。クラッカーはしばしばハッカーとは対照的に悪意を持っており，システムに侵入する多数の手段を思いのままに使う。

●(注－オープン)

「ネットワークのオープン化」に関しては，NTTが1985年の民営化以降，電気通信市場の活性化や新規参入事業者との相互接続の促進などを目的として推進している。また，1994年のSPC化（stored program control：クロスバ交換機を電子交換機，デジタル交換機に更改すること）の完了を経て，1995年から，さらにネットワークのオープン化を加速させている。ここでも，民営化以降の「公正競争の実現」がキーポイントとなっており，具体的には，相互接続点（POI：point of interface）に関して，1995年以前の1個所／1県（NTTの市外交換機のみ）から，「アクセス系のオープン化」として市内交換機接続，加入者回線接続などの新たな相互接続点をオープンにしている。以上述べたことは，どちらかと言うと，通信業者間（NTTと新規参入業者）の為のネットワークのオープン化であるが，結果的には，新たな接続形態が出現し，例えば，①国内・国際一貫通信サービス（国際事業者と長距離事業者との合併），②他事業者間の相互接続（異種事業者間の業務提携）などを生み出している。言葉を換えると，(1) NTTと他事業者との相互接続；2者間接続，から，(2)多数事業者間接続への移行

が始っている。技術的には，新しい「相互接続インターフェースの開発」，「事業者間料金精算方式の高度化」，「市内交換機機能のオープン化」が必要となっている［NTT.G-1］。これらは従来の電気通信事業の中で始ったネットワークのオープン化であるが，現在は，インターネットへの対応を含めて多様な形態へと展開が進んでいる。

（［NTT.G-1］ 伊東則昭，吉村勝仙，他「(特集) ネットワークオープン化の技術的動向」，NTT 技術ジャーナル，Vol.10，No.3，(1998) p.12-25）

●(注－DB)

ここで述べる「DB との連携」はイントラネットの概念の中にあり，クライアントの Web ブラウザから WWW サーバ(HTTP サーバ)を介して，CGI コマンドで DBMS にアクセスするものである。リモート SQL を用いる場合もある。

●(注－ISO)

情報セキュリティを検討している国際標準化委員会（ISO）として，ISO／IEC JTC 1／SC 27 があり，3つのワーキンググループから構成されている。そこでは，応用を考えないフレームワークの規格をつくることが中心であったが，1996年からはアルゴリズム（暗号などの方式の計算手順）も検討されている。SC 27 委員会が作成した主な情報セキュリティ規格としては，次の表に掲げるものがある。

表－付録 3　国際標準化委員会（SC 27）の主な情報セキュリティ規格

識別番号	名称
ISO/IEC 9796-1～3 (JIS X 5054)	メッセージ回復型デジタル署名
ISO/IEC 9797-1～2 (JIS X 5055)	データ完全性メカニズム (ブロック暗号アルゴリズムを使用した暗号チェック関数)
ISO/IEC 9797-1～5 (JIS X 5056-1～4)	相手認証
ISO/IEC 9997 (JIS X 5060)	データ暗号技術―暗号アルゴリズムの登録手順
ISO/IEC 10116 (JIS X 5053)	n ビット長　暗号利用モード
ISO/IEC 10118-1～4 (JIS X 5057-1, 2)	ハッシュ関数
ISO/IEC 11770-1～3	鍵管理
ISO/IEC 13888-1～3	否認防止
ISO/IEC 14888-1	付録型デジタル署名：ジェネラル
ISO/IEC 14888-2	付録型デジタル署名：ID ベースメカニズム
ISO/IEC 14888-3	付録型デジタル署名：証明書ベースメカニズム

[NTT.G-1] 森田光，小林邦生，「SC 27 会合を中心とするセキュリティの標準化活動」，NTT 技術ジャーナル，Vol.11，No.9，(1999) p.59-61

参考文献

[INT.H-1] 日本インターネット協会編，「インターネット白書'99」，㈱インプレス，(1999.7)。

[JOH.K-1] ㈶日本情報処理開発協会，「日米電子商取引の市場規模の調査」。

[NIK.B-1] 「特集（シリーズ　日本復活の条件）e 革命の波に乗れ」，日経ビジネス，1999.3.1号，(1999) p.20-37。

[NIK.B-2] 梅田望夫「(トレンド　情報化戦略) ウェブ投資，日本企業は即10倍増やせ」，日経ビジネス，1999.9.20号，(1999) p.14。

[NIS.S-20] 「電子マネー実験花盛り」，西日本新聞，1998.9.2。

[NIS.S-1] 「21世紀を読む　実験進む電子マネー」，西日本新聞 NIE 版，西日本新聞，1999.2.8。

[YOM.S-1] 「(マルチメディア) 電子マネー実験　米で中止相次ぐ」，読売新聞，1998.11.11。

[Rog.C-1] Roger Clarke，安藤進翻訳，「インターネットのプライバシー問題の解決には政府の介入も必要だ」，情報処理，Vol.40，No.7，(1999) p.730-736。

[NIK.CM-0] 「(特集) 日本企業800社のセキュリティ白書」，日経コミュニケーション，1998.11.2号，(1998) p.84-109。

[NIK.B-3] 稲葉則夫「(新サービス) 米国で話題沸騰の ASP とは？」，日経ビジネス，1999.6.21号，(1999) p.15。

[NIK.CM-1] 「(特集) プロに任せるセキュリティ対策」，日経コミュニケーション，1999.9.20号，(1999) p.94-111。

[NIK.CO-1] 川又英紀「(特集) セキュリティ七つの不安」，日経コンピュータ，1998.11.23号，(1998) p.118-138。

[Kam.S-1] 神村伸一，安江正治「文系大学での CS 基礎概念を意識した情報リテラシー教育」，情報処理学会研究会報告，98-CE-49，p.15-21。

[Ari.T-1] 有賀妙子，吉田智子「ネットワークリテラシー教育のシラバスと教材研究」，同上，98-CE-50，p.25-32。

[Kun.Y-1] 久野靖「高校情報化におけるネットワーク教育の内容と構成」，同上，98-CE-50，p.65-72。

[Niw.T-1] 丹羽時彦，雄山真弓「WWW を用いた新しい数学教育の試み」，同上，98-CE-50，p.1-8。

[NIK.B-0] 廣松隆志，「(第 2 特集) 激変，就職戦線，したたかな攻防」，日経ビジネス，1999年 3 月 8 日号，(1999) p.34-39。

[NIK.CO-01]「日本で初めてのハッカー被害届，パソコン通信でIDが盗用される」，日経コンピュータ，1995/12/11号，p.116。
[ASA.S-1]「新種ウィルス電子メールで被害急増」，朝日新聞，1996/12/27。
[NIK.CO-02]「インターネット・ウィルス防止ソフト新タイプが続々」日経コンピュータ，1997/01/06号，(1997) p.68。
[NIK.S-01]「不正アクセス多発数千人規模コンピューター被害相次ぐ　http://www.jpcert.or.jp」，日経新聞 1997/01/11。
[NIK.CO-03]「年末年始に不正アクセス多発システム管理者の不在を狙う」，日経コンピュータ，1997/02/17号，(1997) p.215。
[NIK.CO-04]　通産省が不正アクセス対策　セキュリティ・センタ設置」，日経コンピュータ　1997/03/03号，p.93。
[NIK.S-02]「コンピュータウィルス被害急増　通産省調べ4月200件」，日経新聞，1997/05/10。
[NIK.S-03]　日本経済新聞　1997/06/07　コンピュータウィルス増殖　5月230件被害最高。
[NIK.B-01]「会社の情報が危ない　1企業100万ドル被害」，日経ビジネス，1998/1/12号，(1998) p.96。
[MAI.S-01]「東大の大型計算機センター　無登録者　他人のIDを盗み“不正アクセス10年」，毎日新聞，1997/10/16。
[ASA.S-2]「コンピュータ犯罪防止に倫理教育必要」，朝日新聞，1997/05/15。
[Sho.M-1]　小路真木子,「パスワード変更の指導法とその効果」,第12回私情協大会資料，(1998) P104-105。
[Nag.k-1]　永田清，青木智子,「学生のコンピュータに関するセキュリティ意識構造の分析」，同上，(1998) P106-107。
[Yam.N-1]　山下倫範，他,「コンピュータネットワーク不安意識調査」，平成10年度情報処理教育研究集会，(1998) P373-376。
[Mur.T-1]　村田孝子,「ネットワーク上のモラルについての意識調査(2)」，同上，(1998) P385-388。
[Kud.H-1]　工藤英男，他,「インターネットにおける情報倫理に関する意識調査(2)」，同上，(1998) P389-392。
[Shi.Y-1]　白井靖敏，小島浩司「学生のインターネット利用におけるセキュリティとモラル」，同上，(1998) P517-520。
[Wat.N-1]　渡部昇，他「ネットワークのセキュリティ問題と利用者教育」，同上，(1998) P521-522。
[Tat.T-1]　辰巳丈夫,「情報倫理教育から情報危機管理教育へ」，同上，(1998) P619-622。
[HAN.S-1]　花岡菖，「経営革新と情報技術」，日科技連，(1995)，p.15。

[Aki.T-1] 秋山哲男,「実践 経営情報システム」, 中央経済社, (1998), p.62-69。
[Kat.T-1] 加藤忠宏,「産業社会と情報化徹底マスター」, ソフトバンク株式会社, (1995)。
[TAC.S-1] TAC 情報処理講座編,「システム開発」, TAC 株式会社, (1997)。
[Uot.K-1] 魚田勝臣, 田村幸子,「情報とコンピュータ」, 嵯峨野書院, (1997) p.146。
[TAC.S-2] TAC 情報処理講座編,「情報システム v.2.0」, TAC 株式会社, (1997) p.140。
[NIK.CM-30] 「(特集)再点検：インターネット VPN」, 日経コミュニケーション, 1999.6.7号, (1999), P.72-89。
[NIK.CO-3] 田淵治樹「セキュリティ評価基準の詳細と対策（前編)」, 日経コンピュータ, 1998.12.21号, (1998), および, 田淵治樹「セキュリティ評価基準の詳細と対策（後編)」, 日経コンピュータ, 1999.1.4号, (1999) p.124-133。
[Hir.T-1] 平能哲也,「実践！ネットワーク社会の危機管理」, 竹内書店新社, (1999)。
[Mae.T-1] 前川徹,「標的となるウェブサイト」, 情報処理, Vol.40, No.8, (1999) p.822-823, など多数有。