大学における情報モラル教育支援環境の課題

江澤　義典　　小林　孝史　　中芝義之*

要　旨

高度情報化の「影」の部分が顕在化している．とくに最近は，迷惑メールやウィルス被害の蔓延など様々な社会問題が報道される機会が増えてきている．このような問題について正しい理解と対処法を身に付けることが要請されているのである．関西大学は教職免許として教科「情報」の認可を受けた教育課程を提供しており，全学的にも，情報モラル教育を支援する体制の整備が必須要件となっている．とくに，将来を見込んだ若者に新しいモラルの確立や，新しい常識の確立，情報価値の認識向上など，情報のあり方について基本的な認識を与える場を提供しなければならない．ユーザにネットワークの適切な利用を促すための事前教育や事前措置とともに，運用規則に反する事例が発生した場合の対策も重要である．

本論文では，関西大学のネットワーク運用管理や利用に関する規程，ユーザ支援体制，ユーザ教育，バイオメトリックスを応用した個人認証システムの導入効果，などについて検討する．そして，情報モラル教育においては「知的財産の保護」や「不正アクセス防止」，「個人情報保護とプライバシ」といった，個別の知識を教えるだけでなく，技術の発展とともに構築されてきた情報倫理の歴史的視点が重要であることを指摘した．

Infrastructure for Computer Moral Education in a University

Yoshinori EZAWA, Takashi KOBAYASHI, Yoshiyuki NAKASHIBA*

Abstract

Computer moral education is one of the biggest problems in IT educational courses for university students. This paper includes the report of annual construction plans of computer network infrastructure by the Information Processing Center of Kansai University. Moreover, we discuss about the implementation of a digital identification method that was introduced in the Faculty of Informatics in 2001. The biometrics used in this new tool might be unusual for university students, but it is now a common tool in business applications. The abuse of

* 関西大学情報処理センター

computers by novice students with cracking software was dramatically decreased since this finger print identification tool had been implemented.

1．はじめに

高度情報化の「影」の部分が顕在化している[1][2]．とくに最近は，迷惑メールやウィルス被害の蔓延など様々な社会問題が報道される機会が増えてきている．このような問題について正しい理解と対処法を身に付けることが要請されているのである[3][4][5]．

高等学校の普通科で教科「情報」が必修科目として平成15年度から設置された[6]．その準備として昨年度までに，現職教員の研修や新規の教員養成が進められた．また，各々の高等学校には，科目「情報」の学習指導要領で示された実習重視の視点から，コンピュータの導入が計画的に実施され，ハードウェアの整備と同時にソフトウェアも準備された．さらに，IT推進のインフラストラクチャとしてネットワーク接続も整い，いわゆるインターネット環境も格段に充実してきた．今後は，高等学校普通科における情報教育のあり方や大学における情報教育の内容を，社会的な視点からも検討する必要がある[7]．

また，高等学校の専門教育に関する教科「情報」も新設されたのであるが，その教育目標として，「高度情報通信社会の諸課題を主体的，合理的に解決し，社会の発展を図る創造的な能力と実践的な態度を育てる」ことが求められている[6]．その学習指導要領解説では，つぎのように記述されている．「高度情報通信社会では，豊かな社会生活を実現させることができるが，同時に著作権等の保護や情報モラルに関する問題など社会生活に与える影響の大きさへの十分な理解も必要とされ，それらの課題を合理的に解決するためには，常に自ら課題を見付け，自ら考え，課題の解決に当たる主体的な態度を身に付けることが重要となる．」

中学校学習指導要領「技術・家庭」の技術分野にコンピュータ活用が含まれており，「情報とコンピュータ」では，「情報化が社会や生活に及ぼす影響を知り，情報モラルの必要性について考えること」が目標となっている[6]．

とくに，高等学校学習指導要領では情報分野の「各科目の指導においては，内容の全体を通して情報モラルの育成を図ること」となっている[6]．そこでは，情報モラルを，「情報社会で適正な活動を行うための基になる考え方と態度」と捉えることとしている．そして，情報モラルの育成とは，「何々をしてはいけないというような対処的なルールを身に付けるだけではなく，それらのルールの意味を正しく理解し，新たな場面でも正しい行動がとれるような考え方と態度を育てること」とされている．

関西大学は教職免許として教科「情報」の認可を受けた教育課程を提供しており，全学的にも，情報モラル教育を支援する体制の整備が必須要件となっている．とくに，将来を見込んだ若者に新しいモラルの確立や，新しい常識の確立，情報価値の認識向上など，情報のあり方について基本的な認識を与える場を提供しなければならない．ユーザにネットワークの適切な利用を促すための事前教育や事前措置とともに，運用規則に反する事例が発生した場合の対策も重要である[8][9]．

本論文では，関西大学のネットワーク運用管理や利用に関する規程，ユーザ支援体制，ユーザ教育，バイオメトリックスを応用した個人認証システムの導入効果，などについて検討する．

2．全学的な情報モラル教育支援体制

関西大学の情報処理センターは，工業技術研究所の電子計算機室に導入されたコンピュータを教員や学生が研究用に共同利用していたものが母体となり，総合図書館の地階に移設されたときより，全学の共同利用施設として運用されてきた．とくに，そのファイル管理規定は全国の大学におけるコンピュータ処理を目的とした電磁ファイルの管理規定として嚆矢となるものであり，多くの大学におけるコンピュータセンター規定制定の魁であった[10][11]．その後，コンピュータはネットワーク利用が中心となり，ネットワーク利用に関する規定が整備された[12][13]．

2.1 ネットワークの利用規則[12]

ネットワーク利用の上での禁止事項として以下の８項目を列挙して情報モラル教育の指針としている．

(1) システムの改変，破壊や運用上の不正利用
(2) 個人のプライバシに係わる利用
(3) 営利を目的とした利用
(4) 公序良俗に反する利用
(5) 犯罪行為に結び付く利用
(6) 関西大学の名誉を傷つける利用
(7) 本学関係者又は第３者に不利益を与えると判断される利用
(8) その他法令に反する利用

学外との接続に関してはrouterとFire Wallでポートおよびプロトコルのフィルタリングを行っている．

情報処理センターのサーバ利用は年度単位での申請制であり，学内利用者数は教育用システムで約14700名，研究用システムでは約1100名が登録申請している．いずれも登録対象者の約50%である．

一方，高槻キャンパスの総合情報学部在籍者は全員を，入学時点で高槻キャンパス内サーバに，利用者登録している．

2.2 危機管理マニュアルの作成[8]

インターネット利用の普及とともに，CodeRedやNimda等のウィルスさらにはスパムメールなどが学内においても発生し，ネットワークサービスに多くの被害をもたらしている．

従来は，情報処理センターが関連部署と連携し障害対応を行っていたが，多くの利用者にとっては，障害発生時に情報処理センターがどのような体制でどのような対処を行っているか見えないとの不満があった．そこで，障害対策の手順を文書（マニュアル）化することによって，各種サーバやネットワークの障害などのいわゆる「危機」を管理する方策や責任体制を明確にすることになった．

2.2.1 障害の分類

障害が発生した場合，利用者にとっては「あるサービスが正しく動作していない」という現象が現れ，個別に障害の解消を求めて情報処理センターなどの管理部門に連絡を行うことになる．情報処理センターでは，現象の確認および簡易調査を行い，障害（トラブル）を５種類に分類している．

(1) サーバ障害:

各種のサーバで，ハード障害などが生じたとき（ウィルス等は除く）．

(2) 学外ネットワーク障害：

学外とのネットワークがハード障害やネットワークへの高負荷により，接続が不安定な状態や切断されたとき．

(3) 学内ネットワーク障害：

学内ネットワークにおいて，ネットワークの不通や利用できない等の障害（ウイルス等は除く）．

(4) ウィルス感染：

各種ウィルスソフトの蔓延が学内で発生した場合．

(5) ネチケットトラブル：

電子メールやブラウザを利用して，ネチケットに違反した行為が発生した場合．

2.2.2 処理 Step および判断 Level

危機管理において，対処の内容を Step，危機の度合いを判断 Level として，整理した．危機の度合いとしてはサービス停止時間（復旧見込み時間）が基準となるものと障害の広がり具合，すなわち障害を受けたコンピュータの台数や影響範囲などを基準とした．ここでは，サーバ障害とウィルス感染の場合について示す．

(1) サーバ障害の場合

対処 Step としては「Step0」から「Step7」まで８段階とした．

Step0:予防的な措置で,RAID 装置の導入などにより利用者データの対障害性の向上を図る．

Step1：管理者の日常監視や，当事者からのメールや電話による連絡で障害が発覚．

Step2：連絡内容から，障害状況の確認を行う．その障害の Level を決定し，障害発生を関連部署に連絡する．

Step3：ホームページ等により学内外への情報提供（発生および経過）を行う．

Step4：関連部署や業者と連携し，障害の原因調査を行う．

Step5：関連部署や業者と連携し，障害の対処（復旧作業等）を行う．

Step6：復旧後，障害復旧を関連部署に連絡する．

Step7：ホームページ等により学内外への情報提供（復旧）を行う．また当事者へも連絡する．

サーバ障害の判断 Level は，復旧見込時間，すなわちサービス停止時間を基準と考え，危機の

度合いとして6段階を設けた．ただし，サーバの重要度によってはLevelを1段階下げる場合もある．

Level1：復旧見込時間が10分以内

Level2：復旧見込時間が30分以内

Level3：復旧見込時間が90分以内

Level4：復旧見込時間が3時間以内

Level5：復旧見込時間が12時間以内

Level6：復旧見込時間が12時間以上

(2) ウィルス感染の場合

対処Stepとしては「Step0」から「Step7」まで8段階としている．

Step0：予防的な措置で，ウイルスチェックソフトの導入やセキュリティパッチの対応など．

なお，Step1からStep7まではサーバ障害の場合と同様になっている．

次に，ウィルスの被害タイプを3段階に分類した．

Type1：軽微な障害

Type2：パソコンでの障害またはサーバでのサービス停止などの障害

Type3：パソコンでの重大な障害またはサーバでの重要なデータの漏洩など

そして，ウィルス感染の判断Levelは，ウィルスの被害タイプおよび感染の広がり（台数）を基準として，6段階を設けた．

Level1：障害内容がType1，影響台数が数台

Level2：障害内容がType1，影響台数が数十台

Level3：障害内容がType2，影響台数が数台

Level4：障害内容がType2，影響台数が数十台

Level5：障害内容がType3，多数の機器に影響

Level6：障害内容がType3，学内および学外の多数の機器に影響

2.3 対策システムの導入

関西大学において2001年度には，不正なメール中継，学内資源への不正アクセス，学内外からのDoS (Denial of Service) 攻撃，ホームページ改竄などの事件が次々と発覚した．特にCodeRedやNimdaにより，学内外の機器やネットワークに多大な被害が発生した．そこで，2002年8月上旬に，ウィルス・チェック・システム，DoS対策システム，不正侵入検知システム，ネットワーク脆弱性検知システムをそれぞれ導入した．各システムの概要を以下に紹介する．

(1) ウィルス・チェック・システムは，学外との電子メールの受発信を検査し，ウィルスの侵入防止および学外への送信を防止するようにした．その結果，学外からの電子メールに添付されたウィルスによる感染を防止できるようになった．

(2) DoS対策システムとは，DoS攻撃（情報システムの処理能力を超えた要求を当該システム

に送りつけ，当該システムでのサービス継続が困難になるもの）を防止するものである．そのためにレイヤー７スイッチ（レイヤー３における不具合の検知のみならず，レイヤー７までも含めた対策を可能にしている）を設置して，ネットワークの切断やFire Wallの停止を，ほとんど防止できるようになった．

(3) 不正侵入検知システムは，Fire Wall で承認している正規のポートを利用した不正アクセスをも自動的に検知するシステムである．このシステムの導入により，不正アクセスの早期発見が可能となった．

(4) ネットワーク脆弱性検知システムを導入した結果，ネットワーク機器およびサーバのセキュリティの問題点を予防的に検査し，セキュリティ的に強固なネットワーク環境を整備・維持することが可能となった．関西大学のキャンパスネットワークには，多種多様なネットワーク機器およびサーバが接続されており，従来は，セキュリティに関して設定上の問題や不備が散見されたが，本システムの導入後は，設定上の欠陥などを集中的に検査できるような運用が可能になっている．

３．総合情報学部における情報モラル教育支援体制

総合情報学部は高槻キャンパスに在り，千里山キャンパスの既存６学部とは物理的に離れているので，コンピュータ・ネットワーク環境の維持管理には特別の工夫が必要になる[14]．
まず，インターネット利用については，関西大学ドメインを使うので千里山キャンパスにある情報処理センターのゲートウェイを経由しての接続となっている．また，教育課程の特質として全学部生および全大学院生に入学と同時に学部内のコンピュータへの自由なアクセス権限を与えている．そこで，情報モラル教育の支援体制に工夫が要ることになる．

3.1 パスワード教育の困難さ

一般に，コンピュータシステム利用に際しての個人認証にはユーザ ID とパスワードの組み合わせが用いられるのであるが，パソコンユーザの場合には自宅や研究室ではパスワードを設定しなくてもセキュリティの危険が少ないという現実があり，実習用パソコンの個人認証を蔑ろにする傾向があった．

実際，総合情報学部においては，その開設当初から第１年次生の実習科目でワークステーションの電子メール利用課題を与えていたが，パスワードの管理が十分に指導できなかった．授業では，具体的なパスワードの考案方法だけでなく，その更新手順も含めて実習したのであるが，定期的なパスワード更新は多くの利用者にとって面倒な作業そのものであった．それは，学生だけの傾向ではなく，教員の中にも安易なパスワードを設定し，数年間もパスワード更新を怠っているものがあった．その結果，極めて遺憾な事態ではあったが，興味本位に他人のパスワードに対するクラッキングを試みる学生が出現し，その対策に悩まされることになった．とくに，1998 年度には学部教授会に報告された事例（表１参照）に示すように，成りすましメールの被害者まで

が顕在化し，学部教授会としての抜本的な対策が検討された．

表１．総合情報学部教授会で報告された事件の関連記録

（1998年度秋学期から2002年度まで）

1998. 10. 14	実習用メールの不正使用：被害学生からの訴えで発覚したが，犯人は特定できず．
1998. 11. 11	教育用サーバのCPU交換（11／15)予告があった．
1998. 12. 09	TC205教室ダウン，PCのWindows95からWindows98への移行計画が報告され，研究用メールサーバのリプレース計画も報告された．
1999. 05. 26	インターネット掲示板への中傷投稿をした学生を補導した．
1999. 06. 09	不正アクセス対策としてPC教室にログ管理ソフトを導入する．
1999. 07. 14	プロバイダー経由のクラッキング，被害学生のアカウントを停止した． パスワード不正入手事件の被疑者を特定できず． FRDにファイアーウォールを導入する．
1999. 09. 29	パスワード盗用事件があり，被害学生のアカウントを臨時停止した．
1999. 10. 13	被疑者（学生）のネットワーク使用停止した．
2000. 01. 17	全利用者に対するパスワード変更を督促して欲しいとの依頼があった．
2000. 01. 26	ウィルス感染ソフトおよびハッキングソフトを利用した学生がいた．
2000. 01. 26	指紋認証（FP）システム導入を提案した．
2000. 03. 07	情報倫理教材（INFOSS）無償導入の報告があった．
2001. 04. 12	FPシステム導入の決定報告があった．
2001. 06. 13	ウィルスソフトのダウンロード事件が２件発覚したとの報告があった．
2001. 06. 14	FP実施計画（9／12から）の説明があった．
2001. 06. 28	FPの機能説明があり，通常パスワードとの併用運用とする方針説明があった．
2001. 07. 12	FP導入の作業日程報告があった．
2001. 09. 26	ウィルスソフト（ニムダ）の被害が報告された．
2001. 09. 27	FP登録を10／12までに完了するとの報告があった．
2001. 10. 10	FPトラブル，SE体制改善の報告があった．
2001. 10. 11	FP登録10／13以降の処理方法が報告された．
2001. 10. 25	FPトラブルの報告（11／２にレベルアップ対策）があった．
2001. 11. 28	Webサーバのクラッキング被害の報告があった．
2001. 12. 12	Webサーバの２回目のクラッキング被害報告があった．
2002. 01. 17	Webサーバのリプレース計画，FPトラブル（DNS設定ミス）の報告があった．
2002. 04. 10	第１回目の授業でFPトラブルの報告があった．
2002. 05. 08	ウィルスダウンロード事件の発覚（当該学生は３度目の補導）報告があった．
2003. 01. 16	ウィルスに関与した学生２名を補導したとの報告があった．

3.2 FP認証システムの導入

そこで，急遽さまざまな対策が調査され，バイオメトリックスを応用した技術が望ましいとの方向が示された．なかでも指紋データを用いる方式が対費用効果的にも有用であることが分かった．しかし，指紋データを使うという点に心理的な面から抵抗感を抱く教員からの指摘もあり，その導入には，さらに慎重な検討が加えられた．（表１参照）

実際には，2000年の９月から実習用パソコン（約270台）にサーバ方式のFP（Finger Print）認証システムを導入して，約2500名の学生に提供している．また，アンチウィルスソフトウェア

を導入して実習環境の保全を図ることにした．その結果，パーソナルコンピュータを用いたクラッキングソフトの使用は激減した．市販されているCDROMのなかには悪質なクラッキングソフトが含まれている場合があるが，そのようなソフトを実習教室のコンピュータで試みる学生に対しては，該当するソフトを実習用コンピュータにインストールしようと試みると，即時に警告画面が表示されモニター記録が電磁ファイルに保存されるので，学生の補導が厳格に実施できることになった．その効果は顕著であり，FP 認証システムを導入して以降のパソコン不正使用は皆無といってよい．

この FP 認証システムに関しては，年度末には卒業生のデータ削除が必要となる．また，４月の第１週には新入生（約 600 名）のデータ登録が必要になる．これまでの運用実績としては，数度のバージョンアップを経て，運用トラブルは減少し安定期に入ったと考えられる．この FP 認証システムのハードウェアは静電容量式で解像度は 500dpi である．また，ソフトウェアは第４版であり，指紋データの登録レベルは９，照合レベルは７で運用している．

ただし，指紋データの登録不適合となる利用者が約 1.5%あるので，従来とおりのパスワード登録方式も併用している．その場合にはパスワードの有効期限は 90 日に制限されている．また，このシステムのソフトウェアは Windows パソコンだけしかサポートしていない．ワークステーション（Solaris）の場合にはネットワーク経由での認証が必須になるという技術的な課題の克服が望まれている．

４．おわりに

情報モラル教育においては「知的財産の保護」や「不正アクセス防止」，「個人情報保護とプライバシ」といった，個別の知識を教えるだけでなく[15]，技術の発展とともに構築されてきた情報倫理の歴史的視点が重要であることを指摘しておきたい[16][17]．
また，世界的な学会組織においては，コンピュータ技術の専門家としての倫理綱領が作成され，その運用についての議論が非常に有用である点も情報モラル教育に含めたいものである[18][19]．

謝辞

日常的に ML などで情報モラルの実習教育に関して様々な示唆を頂いている，総合情報学部の基本ソフトウェア実習担当者の皆様に深謝しています．また，ネットワークセンター職員の方々には，総合情報学部の実習環境を整えるにあたって色々なアイデアを具体的に検討する段階でお世話になりました．

参考文献

［１］S. Baase（日本情報倫理協会訳）：IT 社会の法と倫理，p.341，ピアソンエデュケーション （2002）．
［２］D.G. Johnson（水谷・江口監訳）：コンピュータ倫理学，p.342，オーム社（2002）．

［3］梅本吉彦：情報社会と情報倫理，p.204，丸善（2002）.
［4］情報教育学研究会：インターネットの光と影，p.183，北大路書房（2000）.
［5］廣瀬英彦：情報の倫理－インターネット時代を生きる－，p.254，富士書店（2000）.
［6］文部省：高等学校学習指導要領解説　情報編，p.223，開隆堂出版（2000）.
［7］岡本敏雄：高校新教科「情報」と大学における人材育成の課題，教育の情報化フォーラム，私立大学情報教育協会（2001）.
［8］土田昭司・中芝義之：危機管理マニュアルについて，関西大学情報処理センターフォーラム，No.16，（2001）.
［9］江澤義典・中芝義之：セキュリティ対策と個人認証システム，教育の情報化フォーラム，私立大学情報教育協会，pp.74-77（2002）.
[10] 関西大学情報処理センター：ファイル管理規程，利用の手引き（1983）.
[11] 関西大学情報処理センター：利用データセットの利用に関する内規，　利用の手引き（1985）.
[12] 関西大学情報処理センター：ネットワーク利用の規則，利用の手引き（1995）.
[13] 関西大学情報処理センター：Internetの利用に関する暫定措置について，利用の手引き（1995）.
[14] 関西大学総合情報学部：ネットワーク利用上の内規，大学要覧（1995）.
[15] 情報教育学研究会：インターネット社会を生きるための情報倫理，p.105，実教出版（2002）.
[16] 江澤義典：IT革命と情報倫理，システム／制御／情報，Vol.45，No.9，pp.523-527（2001）.
[17] 江澤義典：情報モラル育成のポイント，ICTE情報教育セミナーin Keio，（2002）.
[18] T. Costlow: The Ethical Organization, IEEE Spectrum, December, pp.56-58（2002）.
[19] E. Vonderheid：　Writing the Code of Ethics, The Institute, IEEE, Vol.27, No.1, pp.12-13（2003）.