調査報告

802.1X 認証技術を導入した 学内情報セキュリティ強化

Improvement of Information Security with IEEE 802.1X Authentication

油田健太郎[†‡]　　藤本竜之介[†§]
Kentaro ABURADA　　Ryunosuke FUJIMOTO

† 熊本県立大学　総合管理学部
‡ 宮崎大学大学院　工学研究科
§ 北陸先端科学技術大学院大学　知識科学研究科

1. はじめに

近年、インターネットの普及によりウェブ閲覧や電子メールだけではなく、P2Pでのファイル共有を利用するユーザが増加している。P2Pとは、どこかの会社や誰かが運用している特定のサーバを使わずに、ユーザがインターネットを介して相互に接続して情報をやりとりするシステムである。いわば、持ち合いで運用するシステムであり、その技術を利用してユーザ同士でファイルを共有するP2Pファイル共有ソフトが生まれた[1]。

P2Pファイル共有ソフトは、様々なファイルを手軽にダウンロードできる反面、ウイルスに感染したファイルも出回っており、ウイルスに感染する危険性が高い。ウイルスに感染していることに気づかずにP2Pファイル共有ソフトを使い続けると、PC上に保存されたファイル（個人情報などを含む）を他のPCにばらまいてしまう。このファイル共有ソフトを媒介とするウイルス感染により、現在多くの情報漏洩事件が起こっている[2]。

1.1. 情報漏洩事件発生

2006年5月26日に、本学ネットワークシステム管理を委託している会社の社員がP2Pファイル共有ソフトによるウイルス感染が原因で本学の個人情報・システム情報を漏洩させてしまう事件が起きた。漏洩した主な情報は、以下のとおりである。

[個人情報]

・氏名、電話番号、メールアドレス

[システム情報]

・管理者パスワード、ユーザの初期パスワード

・情報処理実習室PC・貸出しノートPCのMACアドレス

・ダイアルアップ番号

・ファイアウォールの設定

・IPアドレスやホスト名などのネットワーク情報

これらの情報漏洩対策のために、情報セキュリティ対策プロジェクトチームが発足された。情報セキュリティ対策プロジェクトチームを中心に「流出した情報を無効化すること」および「可能な限り原状に戻すこと」を基本方針として、検討・実施したセキュリティ強化策について述べる。

以下、二次被害防止のために実施した対策、学内 LAN のセキュリティ強化のために実施した対策及び今後の課題について述べる。

1.2. 管理者パスワード、ユーザの初期パスワードの変更

5月26日の情報漏洩事件発覚後、直ちに中央コンピュータ室で管理している情報処理実習室 PC の管理者パスワードやサーバの管理者パスワードを変更した。また、初期パスワードから変更していないユーザのパスワードを一括して強制的に変更した。該当ユーザには、新たなパスワードの設定を指導した。

1.3. MACアドレス変更

情報処理実習室 PC については、6月17日に新たな LAN ボードを追加し、機械構成を変更することで漏洩した情報を無効化させた。しかしながら、ノート PC については機器の追加や変更ができないため、5章で述べる学内 LAN 侵入対策にて対応することとした。

2. ダイアルアップ番号の変更

本学では、学外からのメールの送受信、学内 LAN を介したインターネットへの接続を希望するユーザに対して、電話回線を使って学内 LAN へ接続するダイアルアップサービスを提供していた。利用するユーザは、外部に公開していない本学専用の番号に接続後、ユーザ認証を行うことにより学内 LAN への接続が許可される。ダイアルアップを行うためには、

・非公開のダイアルアップ専用の番号

・本学のアカウント（ユーザ名、パスワード）

が必要であり、ある程度のセキュリティは保たれていた。しかしながら、情報

漏洩事件により、非公開のダイアルアップ番号が漏洩したことにより、本学のアカウント情報さえ分かってしまえば、なりすまし行為が可能となってしまった。現状、教員のユーザ名は大学 HP に公開されており、容易に推測できるパスワードを設定している場合に悪意のある第三者によってなりすまし行為が行われる危険性がある。また、ダイアルアップ番号には同時接続数に限りがあり、本学にアカウントを持たないユーザが多数の接続を試みることにより、ダイアルアップ回線を占有されてしまい、本学ユーザが利用できない状況が発生する可能性もある。そこで、6月20日にサービスを一旦停止して7月24日までにダイアルアップ番号を変更した。番号を変更後、学内にアナウンスを出し希望者に対してダイアルアップ専用番号と接続方法を通知することとした。

3. メールサーバのセキュリティ強化

本学のメールサーバにおけるセキュリティ強化について、3.1節で学外から電子メールを受信する際の通信傍受防止対策を述べる。3.2節でメールアドレスが漏洩したことにより増加すると予想されるスパムメールの対策について検討結果を述べる。

3.1. POPサービスの暗号化

本学では、学外から学内のメールを読むことができるサービスを POP3プロトコルで実装していた。POP3プロトコルは、ユーザ名、パスワード、メールの本文などが平文（暗号化されていないプレーンテキスト）にて通信されるため、通信を傍受される危険性があるが、一般的にも広く利用されており、サービス提供を希望する声が多かったため継続してきた。しかしながら、情報漏洩事件により学外からもメールが受信できることが公になり、ダイアルアップ時のユーザ認証と同様に悪意のある第三者によりメールを盗み見られる危険性が生じたため、6月20日にこのサービスを停止した。

学外からの POP3サービスの停止により、学外から学内のメールを読む手段として外部のメールアドレスに転送する方法もあるが、学内で既に読んだメール

も全て転送してしまうため、必要な情報を選別する手間がかかるという問題がある。そこで、従来通りの使い勝手とセキュリティを両立する方法を検討した結果、８月１日に POP3プロトコルの代わりに POPS プロトコルを実装した。POPS プロトコルでは、ユーザの PC と学内メールサーバまでの通信が暗号化されるため、通信を傍受される危険性が低く、使い勝手も今までとほぼ変わらない（図１）。なお、学内からメールを受信する場合においては、従来の POP3プロトコルも存続させる。

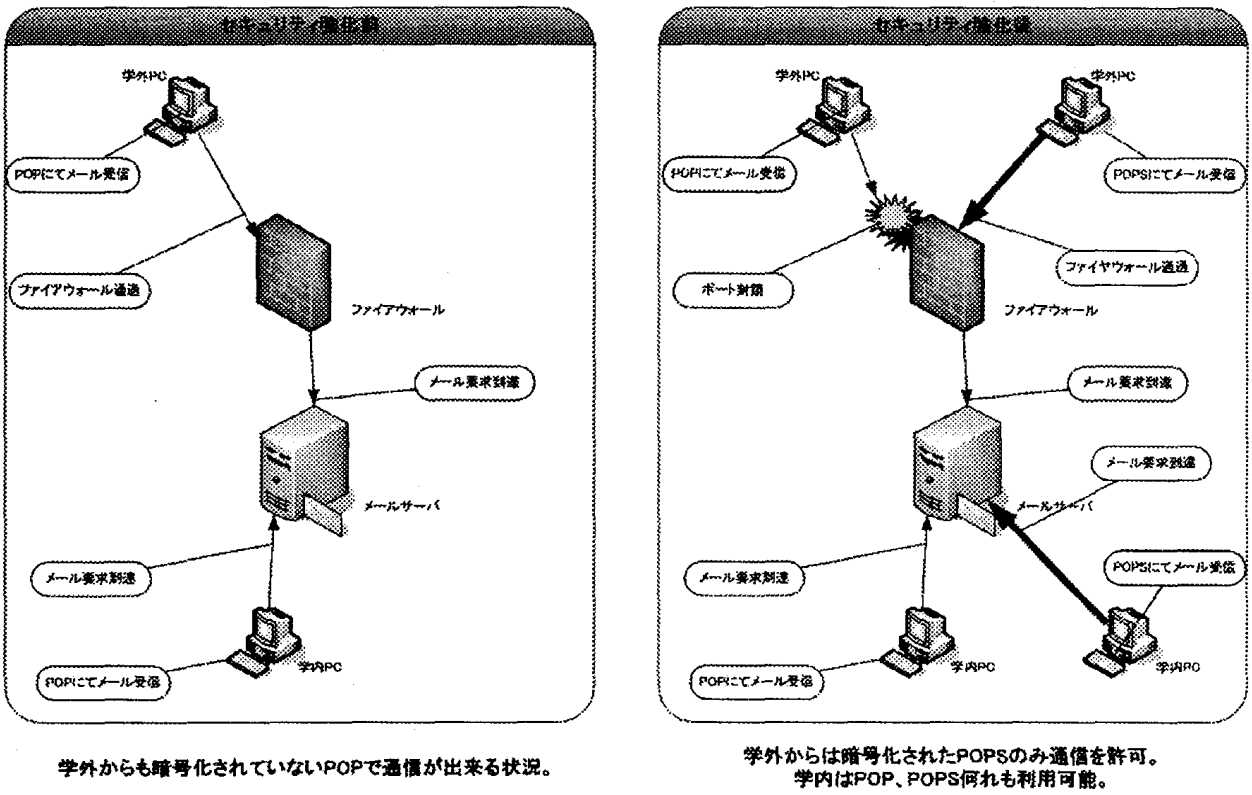

図１　メールサーバのセキュリティ強化

以下に代表的なメールソフトでの POPS の設定方法のリンクを載せる。

・Outlook Express

http://intwww.pu-kumamoto.ac.jp/ccr/site/teacher_staff/pops_outlook.html

・Mozilla Thunderbird

http://intwww.pu-kumamoto.ac.jp/ccr/site/teacher_staff/pops_thunderbird.html

POP3プロトコルを POPS プロトコルに置き換えることにより、使い勝手とセ

キュリティの両立を実現したが、POPS は Al-Mail などの一部のメールソフトに対応していない。昨今、ブラウザを利用してメールの送受信を行う Web メールが注目されている。Web メールは、通信の暗号化が可能であり、セキュリティも高く、学外からもメールの送受信を行うことができる。また、メールサーバにウイルス対策ソフトを導入することにより、メールからのウイルス感染を防ぐことができる。現在、本学でも試験的に Web メール[3]を実装しているが、操作性が大きく変わってしまうことやメールの移行に手間がかかるという課題がある。今後、本学での運用に適した Web メールの検討を進めていく。さらに、操作に関して不十分な点の補足やスムーズなメールの移行のためにマニュアルなどの環境整備が必要である。

3.2. スパムメール対策

本学では、スパムメールへの対策として、本学に存在しないアカウントへの送信が複数回あった場合やユーザからの申告により、送信者をブラックリストとして登録してメールがユーザに届く前に破棄している。しかしながら、スパムメールは増え続けており、同じ送信元からのメールは少なく、様々な送信元から送信される特徴を持っているため、現状の対策では効果を挙げることが困難になっている。

このような状況の中、今回の情報漏洩事件により、本学のメールアドレスが漏洩してしまったため、今後スパムメールが著しく増加することが予想される。そこで、スパムメールの削減対策として、スパムメールをフィルタリングする専用ソフトウェアの導入を検討した。スパム対策ソフトの選定には、まず1点目にスパム対策ソフトが何らかの原因で障害が起こった場合においても学内 LAN に与える影響が少ないこと、2点目にスパム対策ソフトでは、スパムメールではない必要なメールを誤って判断して破棄してしまう可能性があるため、サーバ側ではスパムメールと思われるメールの件名にマークを付ける処理のみを行い、それらのメールの破棄はユーザ側に任せるスパムスタンプ形式の処理を行うことを条件とした。様々な製品が販売されているなか、F-Secure 社のアンチウイルス Linux ゲートウェイ[4]というソフトウェアが上記の条件に合致し

た。しかしながら、初期導入費及び毎年の保守費が高価であるため、現行の予算では導入を先送りすることとした。中央コンピュータ室に設置されているサーバ機器の契約更新と併せて将来的に検討をすすめる。

4. 学内LANアクセス対策

4.1. ウイルス等に利用されうるポートの閉鎖

本学では、学外から学内への通信は不正アクセスを防止するためにかなり強度な制限を設けているが、学内から学外への通信は、教育研究活動に支障の無いよう広く公開していた。そのため、学内 LAN に接続している PC がウイルス等に感染した場合に、学内の情報が学外に漏洩する危険性がある。そこで、JPCERT/CC の注意喚起・緊急報告[5]にて報告された脆弱性があるポート及びネットワーク運営上、遮断を推奨されているポートを閉鎖することとした。ただし、学内 LAN の利用状況やユーザの利便性を考慮し、いくつかのポートは閉鎖しないこととした。表１に、今回の対策によって閉鎖したポートの一覧を示す。なお、ポートの閉鎖は８月18日に実施した。

表１　閉鎖ポートおよびサービス名一覧

ポート	サービス名	FW 作成 service 名
69/UDP	TFTP	TFTP
79/TCP	Finger	Finger
111/TCP,UDP	SunRPC	SunRPC
135/TCP,UDP	RPC Windows RPC	RPC Windows RPC
137/TCP,UDP	netbios-ns NETBIOS Name Service	netbios-ns NETBIOS Name Service
138/TCP,UDP	netbios-dgm NETBIOS Datagram Service	netbios-dgm NETBIOS Datagram Service
139/TCP,UDP	netbios-ssn NETBIOS Session Service	netbios-ssn NETBIOS Session Service

161/TCP,UDP	snmp	snmp
162/TCP,UDP	snmptrap	snmptrap
411/TCP,UDP	RMT(RemoteMTProtcol)	RMT(RemoteMTProtcol)
445/TCP,UDP	SMB SMB	SMB(port445)
512/TCP,UDP	exec,biff	exec,biff
513/TCP,UDP	login,who	login,who
540/TCP	uucpd	uucp
600/TCP	sadmind	sadmind
692/TCP	ToolTalk RPC	ToolTalk RPC
1025/TCP	MSDTC & COM+	MSDTC & COM+
1433/TCP	ms-sql-s	ms-sql-s
1434/UDP	ms-sql-m	ms-sql-m
2049/TCP,UDP	NFS	NFS
5900/TCP	RealVNC Server	RealVNC Server
6000-6063/TCP,UDP	X11	X11

また、ウイルス感染による情報漏洩や著作権侵害の温床となるP2Pファイル共有ソフトの使用に関しても制限する必要がある。しかしながら、多くのP2Pファイル共有ソフトは自由にポート番号を設定できるため、アクセス制限での対策が困難である。P2Pファイル共有ソフトの使用禁止に関しては、6月23日のメールにて学内に告知した。今後、学内におけるP2Pファイル共有ソフトの利用を禁止する規約をまとめる必要がある。

4.2. ウイルス対策ソフトの配布

3.2節で述べたように、スパムメールが増えることによりウイルス感染の可能性が高まることが予想される。そこでウイルス感染による被害を防ぐため、学内LANに接続する以下のOSを管理もしくは使用する教職員を対象にウイルス対策ソフト McAfee VirusScan Enterprise ver.8.0i [6]を配布することとした。

OS： Windows NT 4.0 SP6/6a

Windows XP Home Edition SP1, 2または Professional Edition SP1, 2

Windows 2000 Professional SP2, 3, 4

Windows XP Tablet PC

希望者には、ウイルス対策ソフトのライセンスシールを付与し、インストールメディアを貸出す。ライセンスがあることを証明するために、ライセンスシールは必ずインストールするPCに貼り付けることとした。

以下に、ウイルス対策ソフトの設定方法のリンクを載せる。

http://intwww.pu-kumamoto.ac.jp/ccr/site/teacher_staff/mcafee/mcafee.htm

なお、2006年9月28日の配布開始より2007年1月10日までに、64のライセンスを付与している。

5. 学内LAN侵入対策

情報漏洩事件により、学内LANの重要なデータ（IPアドレス、ホスト名、利用者情報、設置場所など）が漏洩した。通常、学内LANに接続するためには、情報コンセントにLANケーブルを接続して、場所に応じた適切なネットワーク設定を行う必要があり、その設定情報を知らなければ学内 LAN に接続できない。しかしながら、IP アドレスや設置場所のネットワークの設定情報が漏洩したため、外部の第三者が学内にPCを持ち込み学内LANに接続する危険性が生じた。また、利用者情報まで漏洩したことから悪意のある第三者が安易になりすまし行為が行える状態にあった。そこで、学内LANへの侵入対策として学内LANに接続する前にIEEE802.1Xユーザ認証（以下、802.1Xと呼ぶ）を実施して、正規ユーザ以外は学内LANを利用できない仕組みを実装することとした。

5.1. 802.1X 導入における問題点と対応策

まず、802.1X が本学の PC 環境に適用できるか、また導入する場合にどのような障害が起こるかを検討するために、学内 LAN に接続されている全ての PC 及びネットワーク機器の調査を行った。表2にその調査結果を示す。

表2　PC及びネットワーク機器の調査結果

【機器構成】

種別	台数
FW	2
HUB	127
SW	8
サーバ	14
パソコン	1,096
プリンタ	307
ルータ	69
その他	25

【内訳】

802.1X認証	台数	割合
可能	477	43.5%
条件付可能	555	50.6%
不可能	1	0.1%
故障中、詳細情報なし	63	5.7%

【OS構成】パソコン(一部抜粋)

種別	台数
OS8	5
OS9	36
MacOSX10.3未満	12
MacOSX103以上	94
Windows98	37
Windows98 SE	4
WindowsMe	10
WindowNT4.0	6
Window2000 Pro	36
WindowXP	783

調査結果により、PC1096台のうち913台とほぼ全てのPCが802.1Xに対応している（MacOS X 10.3以上、Windows2000 Pro、WindowsXP）ことが分かった。以下の(ア)から(ウ)の3ケースに該当する場合は技術的に802.1Xを適用できない。認証を未適用と設定するとそこから学内LANに侵入されてしまう危険性があることから、それぞれの場合ごとに申請書の提出を必須とした。

各申請書及び802.1Xの設定方法

http://intwww.pu-kumamoto.ac.jp/ccr/site/teacher_staff/8021x/index.html

申請書には、機器固有の値であるMACアドレスを記入し、そのMACアドレスを接続する情報コンセントを管理するネットワーク機器に登録することにより、該当機器のみ認証なしで学内LANへの接続が許可される。

(ア) ネットワークプリンタ

→ネットワークプリンタが接続されている情報コンセントとは異なる情報コンセント配下に接続している PC から印刷を行う場合、ネットワークプリンタにも認証が必要となる。しかしながら、ネットワークプリンタは認証機能を有していないため、認証対象としないこととした。

(イ) ブロードバンドルータ

→802.1X に対応したブロードバンドルータ（以下、ルータと呼ぶ）もあり、ルータ配下の PC で個々に802.1X を行える機種もあるが、現在販売されている大部分の家庭用ルータでは有線・無線を問わず802.1X に対応していないため、ルータは認証対象としないこととした。ルータは、学内 LAN への接続確立後は配下に接続された PC を含めたネットワーク機器を認証なしで学内 LAN に接続させることが可能である。また、ルータの技術的な性質上、ルータの配下のネットワーク構成は設置者しか分からず、中央コンピュータ室での一元管理は実装していない。そこで、ルータを設置する場合はルータ及びその配下に接続するクライアント PC の管理、運営、障害対応等については、管理責任者が責任を持って管理することを条件とした。

将来的には、ネットワーク運営組織より市場の動向を見ながら802.1X に対応したルータを推奨スペックとして提示し、順次移行を進めて全ての学内ユーザに802.1X の実施を義務付ける予定である。

(ウ) 802.1X に対応していない PC（旧端末）

→802.1X は、クライアント側の OS のバージョンに依存する。802.1X が適用できる PC は以下のようになっている。

Windows ： Windows2000 SP4、WindowsXP SP2以上

MacOS ： MacOS 10.3 以上

上記の OS 以外を旧端末と定義した。2006年10月より2007年 9 月30日までを、802.1X 環境への移行期間と位置づけ、移行が可能なユーザから適宜、移行を進める。2007年10月 1 日以降は、一部の例外を除き、旧端末を学内 LAN に接続することを認めない。一部の例外とは、教育研究活動に必要なソフトウェアが特定の OS のバージョンでしか動作しない場合など、やむを得ず現行の OS が必要

な場合などを指す。一部の例外に相当する旧端末の接続については、現在のところ、いつまでという期限は決めていないが、将来的に旧端末を利用されなくなった場合や、OS 提供元のサポートが終了した場合などに再度どのような形で運用するか検討することとした。ルータ配下で旧端末を使用する場合にも、申請書を提出する必要があり、2007年10月１日以降は学内 LAN への接続を認めない。

上記、(ア)(イ)(ウ)の３つ以外にも、サーバルーム内やファイアウォールを設置している環境(管理棟)、ドメインを構築している環境(情報処理実習室)は、802.1X を導入する必要性が低い、あるいは技術的に不可能であるため認証を未適用とした。

5.2. 802.1X 対応機器への更新

Windows98、WindowsME、MacOS 8などの OS は、メーカーからのサポートが終了しており、今後重大なバグがあった場合でも修正プログラムが提供されない。そのため、旧端末の利用は、学内 LAN に影響を及ぼす危険性がある。よって、特別な事情がない限り早急なバージョンアップが望ましい。原則、OS の更新に伴う費用は、申請者負担としたが MacOS 9から MacOS 10.2に関してはメーカーのサポート対象であるため、学術情報メディアセンターより希望者に Mac OS 10.4のライセンスを付与した。付与するライセンス数は、当初60程度と予想していたが、結果は13とかなり少ない数となった。この理由として、MacOS 9 から MacOS X へのアップデートは大幅な仕様変更が伴っているため現在インストールしているソフトウェアが動作しなくなってしまうことが挙げられた。

5.3. 802.1X 導入後の問題

802.1X の導入実施は、10月１日より順次行われた。以下に実施後に発生した問題点とその解決方法を述べる。

- Windows にて、PC がスタンバイ状態になった場合に、認証が無効となってしまう
  →PC の再起動もしくは再度認証処理を行うことで接続可能となる

- Windows にて、ユーザ名とパスワードを入力するバルーンが表示されない
  →認証の設定を再度確認する、もしくはネットワーク接続を一度無効に設定し、再度有効に設定し直す
- MacOS X にて、AppleTalk を利用する場合に認証処理よりも先に AppleTalk がネットワーク接続を確立しようとするため、AppleTalk が動作しない
  →認証確立後に一度、AppleTalk を無効に設定し、再度有効に設定し直すことで動作するが PC 起動毎に行う必要がある
- パスワードを長期間変更していない場合に認証ができない
  →パスワードを変更することで、認証可能となる
- アライドテレシス社などの一部の HUB を使用している場合に認証を行うことができない
  →学術情報メディアセンターより代替の HUB を用意した

6. 今後の課題

情報漏洩事件が発覚し、色々な角度から学内 LAN のセキュリティを見直すこととなり、様々な課題が浮かび上がった。以下に、その課題と今後の学内 LAN の運営について述べる。

まず、ダイアルアップの運用について現状利用者がかなり少なくあまり活用されていないことが分かった。ブロードバンドの普及により、電話回線を使ってインターネットに接続するユーザが減少したことが理由である。今後、ダイアルアップに代わるサービスとして VPN（Virtual Private Network）の導入も視野に入れ、どのような形でサービスを提供するかどうか検討を進めていく。

次に、802.1X についてユーザは学内 LAN 接続時にユーザ名とパスワードを認証サーバまで送信し、それらが正しい値であった場合に接続が許可される。認証サーバは、障害に強い設計になっているが、１台しかないため何らかの障害や保守対応のため、一時的にサーバがダウンしてしまうと、学内 LAN に接続できなくなる可能性がある。今後は、認証サーバを増設して、障害に強いネット

ワークの構築を目指す。

7. まとめ

本稿では、P2P ファイル共有ソフトを媒介したウイルス感染が原因により発生した情報漏洩事件に対して、情報セキュリティ対策プロジェクトチームを中心にシステム的な側面より検討・実施した結果をまとめた。

まず1.2節、1.3節で、漏洩した管理者パスワードや MAC アドレスにより二次被害を防止するために行ったパスワード変更、機器の変更について述べた。2章では、漏洩したダイアルアップ番号を変更することで漏洩した情報を無効化させたことについて述べた。3章で、学外から学内のメールを受信する場合に暗号化して通信の傍受を防ぐプロトコルを実装したこと、またメールアドレスの漏洩により増加が予想されるスパムメール対策について検討したことについて述べた。4章では、学内の情報が学外へ漏洩することを防ぐために過去に脆弱性が報告されたポートやネットワーク運営上、遮断を推奨されているポートを閉鎖したことについて述べた。5章では、ネットワーク情報の漏洩により、外部の第三者が学内 LAN に容易に侵入できる状況になったため、学内 LAN の接続に IEEE 802.1X ユーザ認証を取り入れたことについて述べた。6章は、セキュリティ強化を検討した上で様々な課題が浮かびあがったため、現状を整理して、今後の運用における考察を加えた。

4章で情報漏洩防止対策を行ったが、P2P ファイル共有ソフトの通信を遮断することは技術的に困難であることから、システム上で完全に情報漏洩を防ぐことは不可能である。また、このような情報漏洩を引き起こすタイプのウイルスはウェブ閲覧やメールの添付ファイルからも感染する可能性がある。そこで、ウイルス感染や情報漏洩を未然に防ぐためにウイルス対策ソフトを導入して、Micorosoft Update[7]によりパソコンを最新の状態に保つことが必要である。さらに、P2P ファイル共有ソフトを使用しない、知らない相手からのメールの添付ファイルを開かない等のユーザの IT スキル、情報モラルの向上も求められる。

謝辞

学内情報セキュリティの検討において、議論に参加して御指導、御教授頂きました松岡泰教授および市村憲治教授ならびに飯村伊智郎助教授に深く感謝を致し、心からお礼申し上げます。また、事件発生からセキュリティ対策を実施する過程で学内ユーザに対して真摯に対応してくれた中央コンピュータ室嘱託職員（今村沙織氏、西口美樹氏、天池綾子氏、関谷春花氏）の皆様に感謝致します。

参考文献

[1] 金子 勇，“Winny の技術”，アスキー書籍出版部，2005.
[2] 個人情報漏洩事件一覧，http://www.security-next.com/cat_cat25.html.
[3] Active! mail 2003, https://webmail.pu-kumamoto.ac.jp/am_bin/am_main.cgi/.
[4] F-Secure アンチウイルス Linux ゲートウェイ，
http://www.f-secure.co.jp/products/linux_gw/.
[5] JPCERT/CC の注意喚起・緊急報告，http://www.jpcert.or.jp/at/.
[6] McAfee VirusScan Enterprise 8.0i，http://www.mcafee.com/japan/products/mcafee/vse80.asp.
[7] Micorosoft Update, http://update.microsoft.com/microsoftupdate/.