経済学研究院におけるネットワークセキュリティ対策について

馬場, 直子
九州大学大学院経済学研究

https://doi.org/10.15017/1470675

出版情報：九州大学情報基盤センター広報 : 学内共同利用版. 4 (2), pp.79-87, 2004-08. 九州大学情報基盤センター
バージョン：
権利関係：

経済学研究院における ネットワークセキュリティ対策について

馬場 直子*

1 はじめに

経済学研究院におけるネットワークセキュリティ対策について説明します．ここ数年のコンピュータウィルスをはじめとしたネットワークの被害，特に，2003年8月に学内で感染が広まったウィルスの一種であるBlasterワームによる被害により，ネットワークセキュリティの向上を図っている支線は多いと思います．本研究院においても，数々のネットワークの被害を経験し，ネットワーク構成やネットワークセキュリティ対策の強化を図ってきました．支線によってネットワーク構成や利用環境も様々で，セキュリティ対策の方法も異なると思いますが，本研究院の事例が参考になれば幸いです．

本稿では，まず，本研究院のネットワーク構成および利用環境，そして，今までに発生したウィルス感染をはじめとしたネットワークの被害について説明します．次に，現在のセキュリティポリシとセキュリティ対策について説明します．最後に今後の課題について述べます．

2 ネットワークの現状

2.1 ネットワーク構成

本研究院の現在のネットワーク構成の概要は図1のとおりです．

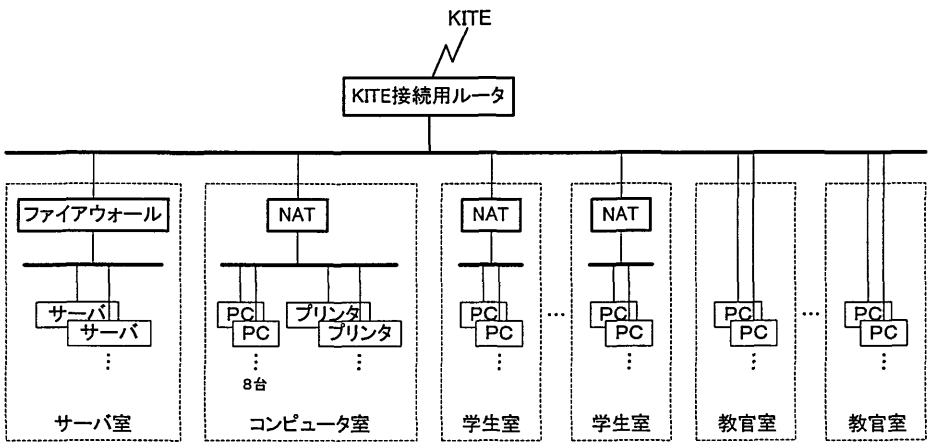

図 1: ネットワーク構成概略図

*経済学研究院 E-mail: maxima@en.kyushu-u.ac.jp

サーバ室のサーバマシンは，ファイアウォールの内側に配置し管理しています．サーバ用のOSには，FreeBSDなどのUNIX系OSを使用しています．教官室のPersonal Computer（以下，PC）は，DHCP[*1]サーバでIPアドレスを自動的に割り当てています．また，ネットワークに接続しているPCを特定するためにMACアドレス[*2]で管理しています．各学生室とコンピュータ室のPCは，NAT[*3]機器の内側に配置し，NAT機器ごとに1つの固定IPアドレスを使用し，プライベートネットワークを構築し管理しています．経済学研究院コンピュータ室(以下，コンピュータ室)は，教官や学生が共用できるPCを設置している部屋です．

ネットワーク管理業務や，ネットワークに関する利用者支援などの業務は，著者を含む助手2名（以下，コンピュータ室助手）が行っています．

2.2　ネットワーク利用環境

本研究院のネットワークの利用環境について，利用者の人数，所有しているPCの台数，管理体制，使用用途などを説明します．概要は表1のとおりです．

表1: ネットワーク利用環境

(2004年5月現在)

	人数	部屋数	PC数	管理	OS
教官	58名	52	168台	各自	Windows (一部 Macintosh や Linux)
学生（学府生）	約230名	17	約70台	各自	〃
コンピュータ室		1	8台	コンピュータ室助手	Windows

教官は58名で，合計168台のPCを個々に所有しています．学生は約230名で，そのうち1/3程度がPCを個々に所有しています．教官，学生とも，主にWindows OSのPCを使用しています．管理は各自で行うことになっています．但し，ウィルス感染など緊急の問題発生時には，コンピュータ室助手がサポートを行っています．コンピュータ室にはWindows OSのPCを8台設置しています．この部屋の管理はコンピュータ室助手が行っています．

主な用途は，電子メール，インターネット，論文や授業用の資料作成などで，利用しているソフトウェアは，Microsoft OfficeやOutlook Expressなどです．メールについては，各研究室単位ではなく，本研究院で一つのメールサーバを共用しています．

2.3　ネットワークの被害例

ここでは，本研究院で発生したウィルス感染をはじめとしたネットワークの被害の実例をあげ，被害の傾向や発生時に行った対策について説明します．主な被害例は表2のとおりです．

最近の被害の傾向として，メール経由よりもWindowsの脆弱性によるウィルス感染の割合が多くなっています．その理由として，度重なるメール経由でのウィルス感染により，利用者のセキュリティへの意識が高まったことが考えられます．例えば，日常的に使用しているメールについては，添付ファイルの開封に注意を払うなどの対策をとる利用者が増えました．また，

[*1]Dynamic Host Configuration Protocolの略．クライアントPCに対して，IPアドレスなどのネットワーク情報を自動的に割り振るためのプロトコルのこと．

[*2]Media Access Control Addressの略．ネットワーク機器に設定されている固有の番号のこと．

[*3]Network Address Translationの略．ネットワークアドレス変換技術のこと．

2004年4月以降は，サーバ側にウィルス対策システムを導入したため，メール経由のウィルス感染は発生していません．2003年8月に猛威をふるったウィルス「Blaster」は，Windowsの脆弱性を利用して感染するワームですが，本研究院においては，情報基盤センターのBlaster感染リストに載ることはありませんでした[1, 2]．その理由として，地道な対処が功を奏したと考えられます．具体的には，メールでのアナウンスをはじめ，各研究室ドアにも注意喚起の掲示を行うなど，アナウンスを徹底しました．さらに，コンピュータ室助手が各研究室をまわり，PCの調査とWindows Updateなどの対処を行いました．

それぞれの被害発生後の対処方法として，サーバ側では，被害の傾向を考慮し，ファイアウォールの構築やウィルス対策システムの導入を行うなど，状況に応じたセキュリティ対策を行っています．利用者に対しては，メールやホームページへの掲載などによるアナウンスを行い，注意を喚起しています．詳細は，次節の「セキュリティ対策」で説明します．

表2: ネットワークの被害例

（2002年度以降抜粋）

日付		被害内容（ウィルス名等）	対処方法
2002年7月	○	ウィルス「Frethem」，メール経由の感染	アナウンス
2002年12月	●	spamメール，不正中継	コンピュータ室助手が個別に対処
2003年3月	●	ウィルス「CodeRed」	〃
2003年5月	○	ウィルス「Sobig.B」，メール経由の感染	アナウンス
2003年6月	○	ウィルス「Bugbear」，メールやネットワーク共有経由の感染	〃
2003年7月	●	ウィルス「Deloder」，Windowsファイル共有（ポート445経由）による感染	NAT機器をネットワークから切断
2003年8月	○	ウィルス「Blaster」，Windows脆弱性（ポート135経由）による感染	アナウンス，個別に対処（全PC）
2003年8月	○	ウィルス「Sobig.F」，メール経由の感染	アナウンス
2004年1月	○	ウィルス「Beagle」，メール経由の感染	〃
2004年1月	○	ウィルス「Mydoom」，メールやファイル交換ソフト経由の感染	〃
2004年4月	●	ウィルス「Gaobot」，Windows脆弱性やパスワード未設定による感染	アナウンス，個別に対処
2004年5月	○	ウィルス「Sasser」，Windows脆弱性による感染	アナウンス
2004年5月	●	ウィルス「Gaobot」，Windows脆弱性やパスワード未設定による感染	アナウンス，個別に対処

○‥学部内の感染に留まったもの，●…学部外へ影響を及ぼしたもの（情報基盤センターから感染の連絡があったもの）

3 セキュリティ対策

本研究院で現在行っているセキュリティ対策について，サーバ側とクライアント側に分けて説明します．セキュリティ対策は，次のサーバとクライアントに分けたセキュリティポリシに従い行っています．

サーバのセキュリティポリシ

サーバマシンについては，ネットワーク管理者が管理し，外部からの攻撃や侵入を防ぐというポリシで運用しています．具体的には，メールやDNSなど必要なサーバアプリケーション以外の不要なサービスを止め，かつ，サーバが提供するサービスに必要な通信以外は遮断するというポリシにしています．

クライアントのセキュリティポリシ

クライアントPCについては，クライアント（利用者）が個々に管理し，保守を行うというポリシで運用しています．具体的には，詳細な対応は規程していませんが，昨今のネットワークの被害を考慮し，ウィルス対策ソフトを導入する，Windows Updateを行う，サーバプログラムを起動させないなどの対策を，利用者に行ってもらうことにしました．基本的には，個々のPCは個人の責任でセキュリティ対策を行うというポリシにしています．

3.1　サーバ側のセキュリティ対策

サーバ側ではサーバのセキュリティポリシに従い，次のセキュリティ対策を行っています．

(1) ファイアウォール

外部からの不正アクセスを防ぐために，ファイアウォールを構築し，ポートを制御しています．ファイアウォールは，表3のルールで運用しています．学部外からの利用で最も多いメールについては，POP[*4]ポートを閉鎖し，SSL[*5]ポートを使用するメールツール「WebMail」を用意し対応しています．「WebMail」は，Webブラウザから実行可能なメールツールです．

表3: ファイアウォールのルール

学部外から学部内	開放	学部外からのネットワーク利用に必要な最低限のポート 例）SSL, SSH
	閉鎖	上記以外のセキュリティ上問題のある全てのポート 例）POP, FTP, TELNET
学部内から学部外	開放	下記以外の全てのポート
	閉鎖	セキュリティ上問題のあるポート 例）RPC

(2) ファイアウォールでのウィルスチェック

本研究院のメールサーバが受信する全メールのウィルスチェックを行うために，ファイアウォールにウィルス対策システムを導入しています．ファイアウォールでウィルスチェックを行うことにより，ウィルスに感染している添付ファイルの削除を行います．ファイアウォールでメールをチェックした後，メールサーバに転送しています．また，検知したウィルス名等の情報をメール受信者に送信しています．

[*4]Post Office Protocolの略．サーバ/クライアント間で電子メールデータのやり取りを行う．

[*5]Secure Socket Layerの略．Webデータのやり取りの際に，サーバ/クライアント間で通信データの暗号化を行う．

(3) MACアドレスによるPCの管理

本研究院のネットワークに接続しているPCを特定するために，DHCPサーバでは登録されたMACアドレスに対してのみIPアドレスを割り当てています．これにより，IPアドレスの枯渇を防ぎ，かつ，問題発生時にPCを特定することで，早い対応を可能にしています．また，学生室のPCについては，NATを用いてプライベートネットワークを構築しています．これにより，外部からの直接攻撃を防ぐとともに，NAT内部での問題発生時にNAT機器をネットワークから切り離すことで，早い対応を可能にしています．

表4は今までに行ってきたサーバ側の主なセキュリティ対策例です．2.3節のネットワークの被害の傾向を考慮して導入した対策や，予防的に導入した対策などです．

表4: サーバ側のセキュリティ対策例

対策	導入理由等
～2002年度(2002年3月まで)	
1. 教官用PCの固定IPアドレスをDHCPへ移行	IPアドレス枯渇化対処のため
2. 学部外からのPOPポート使用によるメール受信の廃止．SSLポート使用のメールツールを用意	パスワード保護のため
3. 全サーバの学部外からのFTP，TELNETポートの使用を禁止．SSHポートは設定を随時更新	サーバへの不正アクセスを試みた形跡が認められたため
4. 緊急時の各研究室への立入許可を承認	緊急時に研究室所有者が不在で，迅速なセキュリティ対策を行えなかったため
2002年度～2003年度(2002年4月～2003年3月)	
5. 学生室のネットワーク接続をNAT機器で管理	IPアドレスの枯渇化対処のため．外部からの直接攻撃を防ぐため． (2003年3月から実施)
6. 教官用PCをMACアドレスで管理 (教官数 約60名，PC数 約170台)	ネットワーク接続のPCを特定するため (2003年10月から実施)
7. ファイアウォールを構築	不要なポートを塞ぎ不正アクセスを防ぐため (2004年3月設定完了，設定を随時更新)
2004年度～(2004年4月から)	
8. ファイアウォールにウィルス対策システムを導入	メール経由のウィルス感染を防ぐため (2004年4月から実施)
9. コンピュータ室のPCを利用者認証(IDとパスワード)により管理	部外者のPCの利用を防ぐため．利用者を把握するため (2004年度中に設定完了予定)
10. 学生用PCをMACアドレスで管理 (学生数 約230名，PC数 約70台)．NAT機器の更新	ネットワーク接続のPCを特定するため (2004年度中に設定完了予定)

2.の学部外からのPOPによるメール受信を禁止する際は，利便性を考慮し，代替ツールとして，SSL対応のメールツール「WebMail」を用意しました．

6.の教官用PCのMACアドレスの調査と設定を完了するまでに約3ヶ月を要しました．調査済のPCには全て許可シールを貼付し，PCの管理を徹底しています．10.の学生用PCのMACアドレスによる管理は2004年度中に完了予定です．また，学生用PCについては，MACアドレスを記入した申請書を年度ごとに提出してもらうことにし，PCの利用者と台数等の把握を正確に行えるようにしました．現在は，各学生室ごとにNATを用いてプライベートネッ

トワークを構築し管理しています.

8. のファイアウォールへのウィルス対策システム導入の費用は，初年度が約80万円，翌年からは約15万円です．また，次節の「クライアント側のセキュリティ対策」でも説明していますが，2004年4月から，ウィルス対策ソフトのサイトライセンス契約(150ライセンス)もしています．その費用は，初年度が約40万円，翌年からは約15万円です．8. のウィルス対策システム導入の費用と合計すると，初年度が約2万円／教官1名，翌年から約5千円／教官1名になります．個々にウィルス対策ソフトを更新する場合，毎年約5千円の予算がかかることを考慮すると予算面においても有効だと思います．

セキュリティ向上を図ることは利便性と相反する面がありますので，利用者全員の理解と協力を得るのは難しいことがあります．しかし，本研究院においては，ここ数年の度重なるウィルス感染をはじめとしたネットワークの被害が影響し，様々な対策を導入することにつながりました．導入の決定は次のようなプロセスで承認されました．コンピュータ委員会は，コンピュータ室助手2名と助教授以上のコンピュータ委員長1名とコンピュータ委員3名で構成されている委員会です．コンピュータ委員長と各委員の任期は2年です．

1. コンピュータ室助手がコンピュータ委員会(不定期に開催)で議題にあげる
↓
2. コンピュータ委員会で審議され，決定される
↓
3. 教授会(月1回)で審議され，承認するかどうか決定される

3.2　クライアント側のセキュリティ対策

クライアント（利用者）側では，クライアントのセキュリティポリシに従い，日常的に次のセキュリティ対策を各利用者に行ってもらうことにしています．日常的に行う対策や，問題発生時の対策の方法については，メールやホームページなどによるアナウンスを行っています．

(1) ウィルス対策ソフト導入によるウィルス対策

ウィルス対策ソフトの導入と，ウィルス定義ファイルの更新を行ってもらっています（設定を自動更新にする．緊急時には手動で行う）．また，本研究院ではウィルス対策ソフトのサイトライセンス契約（150ライセンス）をし，教官に貸出を行っています．このことで，個々にソフトの更新を行う手間が省け，更新切れのまま放置する利用者が減っています．

(2) Windows Updateによるセキュリティホール対策

Windows関連のソフトウェアに対するセキュリティホール（脆弱性）を修正するために，Windows Updateを行ってもらっています（設定を自動更新にする．緊急時には手動で行う）．

(3) その他の対策

Administrator権限のアカウントに必ずパスワードをつけてもらっています（パスワードは安易な文字列にしない）．

(1)〜(3)の対策は既使用のPCについて，日常的に利用者側で行うようにアナウンスしている内容です．(3)のその他の対策には，「メールの添付ファイルを安易に開封しない」，「保証できないホームページは覗かない」，「持ち込みデータはウィルスチェックを行う」など注意すべき事項が多々あります．また，新規購入のPCについては特に，「購入後すぐに，ウィルス対策ソフトを導入し，Windows Updateを行う」ようにアナウンスしています．

以上の日常的に行う対策や，問題発生時の対策の方法については，コンピュータ室助手が随時，利用者に対してアナウンスを行っています．アナウンスは主に，次のメール，ホームページ，掲示の3つの方法で行っています．

メールによるアナウンス

教官と学生用のメーリングリスト（以下，ML）宛に通知しています．教官用MLは全教官宛ですが，学生用MLは全員を網羅できていませんので，ホームページや掲示物による通知を行っています．

ホームページによるアナウンス

経済学研究院コンピュータ室のホームページ http://www.en.kyushu-u.ac.jp/cpr/ に，メールで通知した同内容を掲載しています．また，セキュリティとウィルスについての情報や，各種マニュアルなども掲載しています．このホームページの学外からの閲覧は，IDとパスワード認証により本研究院関係者にのみ許可しています．

掲示，電話，その他によるアナウンス

緊急時には，各研究室ドアに掲示を行うなどし通知しています．必要に応じて，各教官のメールボックスへの文書の投入も行っています．問題発生源が特定できている場合は，個別に電話で通知しています．

アナウンス内容をもとに，各自で対処できる場合は，利用者が個々に，Windows Updateや，ウィルス定義ファイルの更新とウィルスチェックなどを行います．各自で対処できない場合は，コンピュータ室助手がウィルス対策ソフトの操作やWindows Updateの方法などについての教示や，ウィルス駆除処理などのサポートを行っています．また，緊急時で，かつ，PCの所有者が不在で連絡が取れない場合は，本研究院の会計掛立会いのもと，該当研究室に入りLANケーブルを抜くなど，物理的にネットワークから切り離す処置を行います．該当研究室の利用者が不在時に，コンピュータ室助手が緊急入室することについては，コンピュータ委員会および教授会で承認されています．

4 今後の課題

本研究院のネットワーク管理やネットワークセキュリティ対策における今後の課題について述べます．

管理体制の問題

ネットワークの規模やサービス内容にもよりますが，ネットワークを管理する場合，サーバ管理や利用者支援を行う人員が，数人必要です．本研究院では現在，ネットワークの管理業務を2名体制で行っています．日常的な管理や保守作業には現在のところ問題はありません．しかし，ウィルス感染等の問題発生時には人員が足りず，作業が滞ることが多々あります．今後，ネットワークの利用環境の変化などに伴う業務内容の変化に対応できるように，人員を考慮していかなければなりません．また，複数人で管理業務を行っている場合，どの人員でも緊急時に対応できるように，管理知識を有し，それぞれが業務内容を把握しておく必要があります．そのためには，業務内容を明記したドキュメント作りも重要です．ドキュメント作りは時間と労力のかかる業務の一つですが，人員の交代などにも備えて，作成しておく必要があります．

九大内で，アウトソーシング（サーバの外部委託）を行っている部局があります[3, 4, 5]．本研究院では，アウトソーシングのサービス内容やサポート体制，そして，利用者からのサポート要請などを考慮したうえで，メールサーバなどのアウトソーシングは現在のところ行っていません．ネットワークを部局内で管理するか，または，アウトソーシングを行うかを決定する際には，どの業務を内部に残し，どの業務を外部に託すかの見極めが重要であると思います．

利用者への啓蒙活動

サーバ側でファイアウォールの構築や，ウィルス対策システムの導入を行うことにより，セキュリティの向上は図れます．しかし，ウイルスの増加と複雑化や，モバイルPCの普及に伴う外部からのウィルスの持ち込みなどに対処するためには，利用者側でも個々にセキュリティ対策を行うことが不可欠です．2.3節の「ネットワークの被害例」で説明しているBlasterワーム発生時に行った対処方法には，多大な時間と労力を要しました．被害が発生するたびに同様の手段をとるのは得策ではありません．利用者が個々に，日頃からセキュリティ対策を行い予防することが最も望ましい状態です．そのため，利用者にセキュリティ対策の重要性について理解を深めてもらい，全員に対策を徹底してもらうことは，本研究院のネットワークセキュリティ対策における今後の課題の一つです．

5　おわりに

本稿では，本研究院で現在行っているネットワークセキュリティ対策について紹介しました．本研究院では，コンピュータ委員会を通して，部局全体として，ネットワークセキュリティ対策に取り組んでいます．セキュリティ対策を行ううえでは，軸となる指針であるセキュリティポリシを，部局全体の合意のもとに作成する必要があります．また，対策の導入と運用にあたっては，利用者全員の理解と協力を得ることと，利用者一人一人が常にセキュリティについて意識しておくことが重要です．

参考文献

[1] 笠原義晃, Blaster ワームの概要とその対策, 九州大学情報基盤センター広報, Vol.3, No.3, 2003

[2] 情報基盤センターネットワーク運用掛, ワーム「Blaster/Welchia」の統計情報, 九州大学情報基盤センター広報, Vol.3, No.3, 2003

[3] 鈴木敦典, メールサーバのアウトソーシング事例ー大学院言語文化研究院の場合ー, 九州大学情報基盤センター広報, Vol.3, No.1, 2003

[4] 北祐一郎, サーバのアウトソーシング事例紹介, 九州大学情報基盤センター広報, Vol.3, No.1, 2003

[5] 小川稔, 附属図書館におけるコンピュータ関連のアウトソーシングの実際, 九州大学情報基盤センター広報, Vol.3, No.1, 2003