相反するポリシ実現のためのセキュリティ強化の試み

河野 英太郎　　前田 香織　　† 三好哲也　　‡ 浅田 尚紀
kouno@ipc.hiroshima-cu.ac.jp

広島市立大学 情報処理センター
† 豊橋創造大学 経営情報学部
‡ 広島市立大学 情報科学部
〒 731-3194 広島市安佐南区大塚東 3-4-1

あらまし
組織のセキュリティ強化にはファイアウォール等を外部ネットワークとの境界点に設置することが多いが，統一的なセキュリティポリシの策定が難しい場合，ネットワークの構成によっては，必ずしもこのように設置できるとは限らない．広島市立大学では現行のネットワーク構成を変更することなく，ファイアウォールをキャンパス LAN を 2 分割するような位置に FW を設置し，相反するポリシ実現を試みた．その経緯について報告し，セキュリティ強化後の影響について IDS の記録や通信性能に関する計測データなどを元に考察した．また課題等についても報告する．

キーワード　ファイアウォール，セキュリティポリシ, キャンパスネットワーク，相反するポリシ

A Trial to Obtain a Secured Campus Network with Two Conflicting Security Policies

Eitaro KOHNO　　Kaori MAEDA　　† Tetsuya MIYOSHI　　‡ Naoki ASADA

Information Processing Center, Hiroshima City University
† Faculty of Management and Information Science, Toyohashi Sozo College
‡ Faculty of Information Science, Hiroshima City University

Abstract
A firewall is often installed at a gateway to an outside network to secure an internal network. However this kind of installation is not always available depending on a network topology in the case of realizing two or more security policies. We tried to realize two security policies by installing a firewall at the point deviding a campus LAN into two groups logically. We report the process of the installation and consider its effects using IDS logs and measuring network performance. Also, we mention the future problems.

key words　Firewall, Security Policy, Campus Network, Conflicting Policy

1 はじめに

最近のセキュリティインシデントの急激に伴い，インターネットに接続する組織のセキュリティ対策が必要とされている．2000年から最近にかけて，いわゆる「不正アクセス防止法」をはじめとして複数の法整備が行なわれていることからも，セキュリティ強化に対する社会的な要求も急速に高まっている．

組織全体のセキュリティレベル向上の一手法として，組織内部への不正アクセス防止のため，組織と外部ネットワークとのゲートウェイにファイアウォール (以下 FW と記す) などを設置し，組織全体を一つのセキュリティ・ポリシで統一し，外部から遮蔽する方法が取られる [1].

大学の構成員もセキュリティに対する意識が高まりつつあるが，不正アクセスの方法の多様化により，一般ユーザによる自前できめ細かい対応には限界が来つつある．このようなユーザに対しては，「不要なサービスやポートなどを極力閉じる」,「認証されたユーザ以外のアクセスを禁止する」など高いセキュリティをもったネットワーク環境が必要とされる．しかし，理系や情報系学部など，研究・教育においてはFW などのセキュリティ機器の設置を望まない部局もある [4].

このように相反するセキュリティポリシをまとめることは一般に難しく大学などの研究機関へのセキュリティ機器の導入を難しくしている．更に，それまで FW などを設置していなかった組織に新たにセキュリティ機器を導入することになると，組織構成員からの心理的反発も大きくなる．

我々は，解決策として，FW をキャンパス LAN を 2 分割するような位置に設置し，相反するポリシ実現を試みた．また，導入・運用にあたり，通過トラフィックなどのデータを計測した．本稿ではその経緯と効果，課題等について報告する．

2 学内ネットワークの現状

広島市立大学 (以下 本学と記す) は 国際学部，情報科学部，芸術学部の 3 学部構成で 1994 年に開学した．現在で 9 年目を迎え，現在 3000 名弱のユーザ (教職員 約 300 名) が所属している．開学当初は FDDI を基幹とするリング状のネットワークで構成されていた [2] が，1999 年に機種更新を迎え，Cisco 社のスイッチングハブ Catalyst を用いたスター型のネットワークに移行した [3]．また，後述する各々の学内部局単位，情報科学部各講座単位の管理サブネットには，トランク機能を用いて VLAN を設定している．学内には現在 59 の管理サブネットが存在する．

情報科学部においては講座や実験室のサブネット内のネットワークサーバ類やユーザの PC などはサブネット単位で，責任をもって管理するという分散管理体制のもとで運用されている．これ以外のサブネットに関しては情報処理センター (以降 センターと記す) で管理している．ただし，ユーザの利用 PC は原則として自己管理である．

セキュリティ対策については，開学当時には対外的な FW は設置されていなかった．学内への不正アクセスに対しては，機器のトラブルと同様，サブネット管理者とセンターとの間で，個別に相談を受けていた．しかし，1999 年の機種更新以降ぐらいから分散管理に対応出来ないところが目立ってくるようになり，予防的な措置に関する相談も含め，センターとの間で個別対応してきたセキュリティ問題の数が激増してきた．さらにセキュリティ対策をセンターで集中的に実施することに実施することに対する要望が高まった．

セキュリティ対策として，FW のみ設置するのではなく，通信性能やセキュリティポリシをスムーズに反映させるためには，ネットワーク構成も含めて検討することが望ましい．しかし現行のネットワーク構成の変更はできないため今回は VLAN を利用することとした．

複数のセキュリティポリシの実現例 [4] も本学と同様 VLAN を活用している．[4] では研究室単位でのアクセス制限を実現するため，スイッチ (ルータ) のアクセスリストを記述して対応する方法で，本学でもこれを適用することも可能であった．しかし，室数の変動やポリシ変更に逐一対応するための作業負荷やポリシ管理の繁雑さなど長期的な管理としては困難な点も多い．

本学では細かなポリシ設定を避け，大学を「多少利便性は下がるが安全度の高い利用」と「従来通り自由にネットワーク利用するが」安全性管理は自己責任」の 2 グループに分けて管理する方針を決定した．

3 セキュリティ対策

3.1 ファイアウォールの設置

図 1 に本学で 2001 年度から実施しているセキュリティ対策を施した後の学内 LAN の概略を示す．図 1 に示すように，FW をキャンパス LAN を 2 分割する位置に設置し，セキュリティポリシが異なる二つの領域 (本学ではゾーンと呼ぶ) に分割した．本学では各サブネット内にそれぞれのサーバを設置・運用するという分散管理体制との整合性から DMZ(DeMilitarized Zone; 非武装地帯) は設置しなかった．また，学内の各サブネットの IP アドレスはゾーンの如何に関わらず，グローバル IP アドレスを持っている．学内のそれぞれのゾーンは下記

のようになる．なお，括弧内の数字は 2002 年 7 月 22 日現在でのゾーンに所属するサブネットの数である．また，図 1 の構成に変更した後，FW をまたがった異なるゾーン間には NFS などはされていないが，分散管理の都合上 FW をまたがる DNS サーバ同士のトラフィックなどは発生している．また，

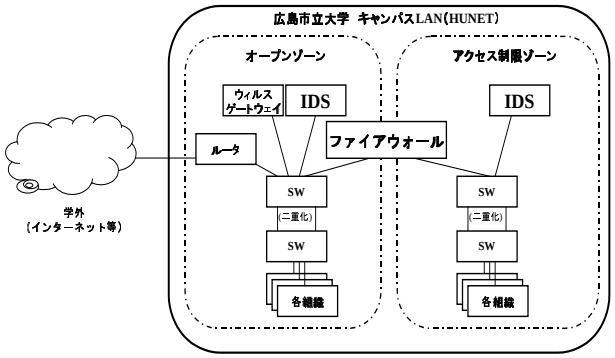

図 1: 広島市立大学におけるセキュリティ対策

ゾーンの分割については既存のネットワーク構成を変更せず VLAN を多用した，VLAN の設定により各々のゾーンへの所属を変更できる．

オープンゾーン (18) 今までのキャンパス LAN と同じセキュリティレベルである．下記の「アクセス制限ゾーン」での通過可能プロトコル制限などを必要としないサブネットを収容する．このゾーン内に残るサブネットでは，クライアントマシン，サーバマシン等での個別のセキュリティ対策を行なう必要がある．このゾーンに属するサブネットでは，セキュリティについては自己責任で管理する必要がある．

アクセス制限ゾーン (41) 不必要なアクセスを FW で制限する領域である．このゾーンへの通過プロトコルは限定されている．更に，許可されたプロトコルであっても申請により登録されたマシン以外への接続は拒否される．また，このゾーンから外向き (オープンゾーン，学外) へのプロトコル制限は設けていない．

各々の管理サブネットはどちらかのゾーンに属することになるが，各サブネットの意向により，それぞれのゾーンを選択した．また，アクセス制限ゾーンへの通過プロトコルは初期値を決めて仮運用をはじめ，新しい要求が出てきた時に学内委員会で協議することとした．アクセス制限ゾーン内の登録変更等マシン，ゾーン外からのアクセスを通すためには，センターに対し，書式に従って申請を提出する必要がある．また，所属ゾーンの変更など，大きな変更に対しても申請書の提出を求め，学内委員会で議論し決定する．

3.2 IDS の設置

FW の内外にネットワーク型侵入検知システム (Intruder Detection System; IDS) を置き，FW と併せて，統計情報を定期的に収集している．これにより，セキュリティポリシの調整など学内ネットワークの調査などに役立てている．

3.3 ウィルス検知

調査機関の途中で増えてきたメールに添付されたワーム，ウィルスなどによる被害を防ぐため，ウィルスゲートウェイを設けた．これにより，学外から学内，学内から学外に通過するメールについてフィルタをしている．また，これと並行して，センターが管理する教育用 PC にはワクチンソフトを導入している．また，教育用 PC の乗っ取り防止のため，一般ユーザからのフロッピディスク，CD-ROM からの起動を禁止し，BIOS に対してパスワードを設定している．教職員個人用の PC のウィルス対策のためには，ワクチンソフトのサイトライセンスを取得し，教職員に配布している．

3.4 FW 導入時・運用時のトラブル

FW を導入する際，キャンパスネットワーク管理者，および学内ユーザに対する周知期間として 3 カ月程度を設定し，内容への理解と協力を求めた．今回の導入ではオープンゾーンを設けたため，あまり大きな混乱は発生しなかった．

しかし，FW を導入して約 2 カ月の間は，さまざまなトラブルが発生した．主なものとしては，設定ミス，FW の通過可能セッション数制限による通信不可など，初歩的なものが多かった．ちょうど，初期トラブル発生時には CodeRed が流行し，FW の機能により感染の広がりをある程度食い止めることができたが，IDS のディスク容量の溢れなどでログを消失するなどの事象が発生した．また，UPS 設置未対応のため停電により FW のディスク障害を発生した．FW は動的経路制御可能という仕様だったが，正常に動作しないため実際には FW の隣接ルータ 4 台にも 59 サブネットの経路の静的な設定を余儀なくされた．FW 障害時には，これらのルータの設定変更にも短時間で対応する手順を整えることとなった．

また，初期トラブルが収束してからは，比較的安定して運用できているが，ログファイル容量の溢れ，セッションライセンスに伴う通信不良などの事象は発生している．

4 セキュリティ強化の影響

セキュリティ強化のために，FW をはじめ，いくつかの機器を導入した．これによって学内のシステ

ムが受けた影響を，いくつかの観点から検討した．

4.1 セキュリティレベルの向上

FW はじめ，セキュリティ機器の導入によってセキュリティに関して，どの程度の向上が見られたかを FW と IDS のログにより比較する．なお，下記のデータ採取時には FW はプロキシ型で動作している．

4.1.1 平常時の効果

調査期間中，FW の設置によって不正アクセスを引き起こす可能性があるトラフィックがどれだけ減少したかの観測結果を表 1 に示す．観測期間は 2001 年 12 月 19 日 10:00〜2002 年 1 月 18 日 13:00 である．表中の分類は，Web，E-mail，DoS(Denial of Service) 関係で，IDS に登録されているシグニチャのうち，特に多かったものをいくつか選んである．Web 関係には，CodeRed およびその亜種 [5][6]，Nimda [7] が含まれている．「FW 内/学内」の列に示した割合は，FW 内で計測された IDS の警告数が学内全体で計測された警告数に対してどのくらいの割合になっているかを示している．

表 1: 平常時に観測された IDS の警告数

	学内 (件/日)	FW 内 (件/日)	FW 内/学内 (%)
Web 関係	2488.9	2096.6	83
E-mail 関係	1888.3	534.9	28
DoS 関係	3225.1	58.0	2.0

表 1 では，特にに DoS の防御率が大きいが，これはたくさんのパケットを流して，正常な通信を妨害する，または学内 IP アドレスに対する無差別なスキャンに伴うトラフィックであるため，表 1 のように大きな効果が現れると考えられる．

4.1.2 特定事例 (Nimda 等) に対する効果

調査期間内には CodeRed, CodeRed II およびその亜種 [5][6]，Nimda[7] といったワームが流行した．その時の不正アクセスの減少度を表 2 に示す．データ採取期間は 2001 年 12 月 5 日 15:30 〜 12 月 10 日 13:00 までである．表 2 における「FW 内/学内」は，表 1 と同じ計算方法で算出している．表 2 によると，大学全体へのアクセス数 (200053 件/日) と比較して，3807 件/日となった．これは全体の 1.9 % にあたり，FW によって不正侵入を誘発するトラフィックの減少に役立っているといえる．また，他のアクセスも減少している．

特定アクセス増加時・通常時とも，FW によるアクセス制限の効果は現れているが，本学における現在の運用状況 (サブネット内に DNS,WWW,E-mail サーバを含み，独自管理が行なわれる) では，アクセス制限ゾーン内に，不正アクセスにつながるトラフィックを誘導する．アクセス制限ゾーン内の安全性を更に向上するためには，この運用体制についても考える必要がある．

表 2: CodeRed,Nimda 発生時の IDS 警告数

	学内 (件/日)	FW 内 (件/日)	FW 内/学内 (%)
Web 関係	200053	3607	1.9
E-mail 関係	2266	576	26
DoS 関係	2197	33	1.5

4.2 学内トラフィックの推移

FW の設置によって，学内全体のトラフィックに大きな影響が現れるかどうかを調査した．

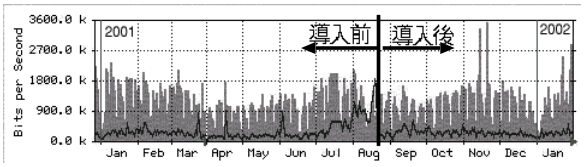

図 2: 学外とのトラフィックの推移

図 2 は FW の導入前後の学内と学外とのトラフィックの MRTG による IP パケットの通信量を示す．折れ線グラフの方が，学外から学内へ，もう一方が学内から学外へのトラフィックを示す．図 2 の 8/20 (図 2 で太い線で示した部分) 付近のトラフィックに着目すると，導入前のトラフィックと比較して大きな変化は見られない

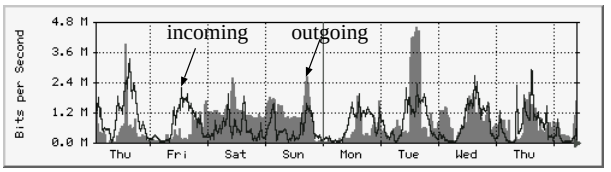

図 3: FW を通過するトラフィック

図 3,4 は，FW を通過するトラフィックと FW の CPU 負荷率を示す．データの計測時期は 2002 年 7 月 11 日から 18 日である．図 3, 4 に示した FW の CPU 使用率から FW 機器の性能による通信パフォーマンス低下は発生していないと考えられる．

4.3 ゾーン間のアクセス速度

本学のセキュリティ対策の前後では，アクセス制限ゾーンに属したサブネットに対しては FW へのアクセスが増加することから，アクセス制限ゾー

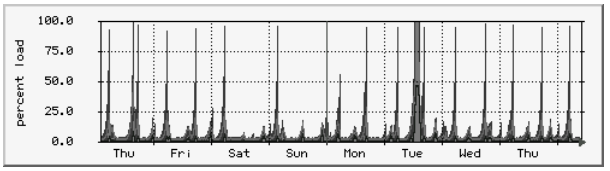

図 4: FW の CPU 使用率

ン内のサブネットからは「以前に比べてアクセス速度が低下したのではないか」という意見があった．これに関するデータも定期的に採取している．

実験方法を図 5 に示す．

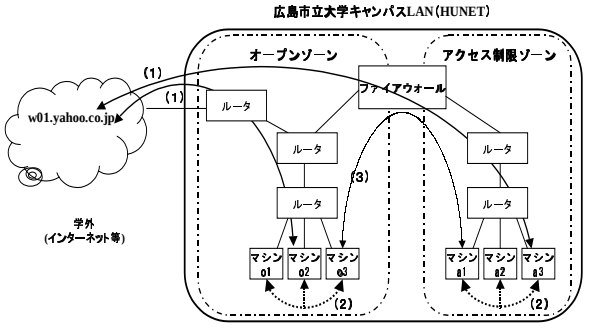

図 5: ゾーン毎のパフォーマンス計測

図 5 に示すとおりアクセス制限ゾーン，オープンゾーンから特定のサーバに対して ping を行ない，その RTT(Round Trip Time) より各々のゾーンでの通信速度を計測した．

表 3: 学外との通信

(単位 ms)

	9:00	14:30	15:00 (講義中)
(1)FW 内 (A) →学外	23	62	38
(1)FW 外 (O) →学外	25	63	39

表 3，表 4 のデータは 2002 年 1 月 24 日と 25 日の各時間帯で 30 分間計測したデータの平均値をとったものである．表 3 は学外と各々のゾーンへの通信速度の計測結果である．学外のサーバとしては w01.yahoo.co.jp を指定している．どちらの場合も，それぞれの差が 1 から 2 (ms) となっており大きな差は見られない．

また，表 4 は学内のマシン同士の通信速度の計測結果であり，それぞれ表 4 は同一ゾーン間の，表 4 は異なるゾーン間の通信速度の計測結果である．どちらの計測結果を見ても，各々のゾーン間の通信速度の差は 2 (ms) 以下になっており，大きな通信速度の差は見られない．

表 4: 同一ゾーン内，異なるゾーン間の通信

(単位 ms)

	9:00	14:30	15:00 (講義中)
(2)(同一ゾーン内)A → A	2.3	3.0	2.7
(2)(同一ゾーン内)O → O	1.7	18	1.5
(3)(異なるゾーン間)A → O	1.5	1.7	1.3
(3)(異なるゾーン間)O → A	1.5	1.7	1.0

4.4 プロキシ型と IP フィルタ型

FW には動作方法によって大きくプロキシ型と IP フィルタ型に分かれる．一般には安全性としてはプロキシ型の方が，通信性能としては IP フィルタ型の方が優れているといわれている．これについて，同じ FW の動作モードを変更し，学外サーバから 17.0[MB] のデータを転送した．その計測結果を表 5 に示す．表 5 は FW がそれぞれプロキシ型，IP フィルタ型として動作していた平日時 (プロキシ型は 11 日間，IP フィルタ型は 19 日間) の計測結果を平均したものである．なお，調査期間は 2002 年 4 月 24 日から 2002 年 6 月 5 日である．

表 5: 動作モードの違いによる転送速度

動作モード	プロキシ型 (kbps)	IP フィルタ型 (kbps)
FW 外→学外	120	85
FW 内→学外	106	63

表 5 の計測結果からは，明らかに IP フィルタ型の動作モードの場合の転送時間が長くかかっており，FW の実装やネットワークトラフィックによっては，必ずしも IP フィルタ 型の方が動作が早いとは限らない．

4.5 ウィルスゲートウェイによるフィルタ

調査を進めている間に CodeRed, Nimda など，学内 PC の感染により，キャンパス LAN 内，学外各組織に対して大量のトラフィックを発生するウィルスが流行した．これらへの対処も早急に迫られたことから，学内にウィルスゲートウェイを設置した．ウィルス検知はゾーンに関係なく全ユーザのメールについて，学外への送信，学外からの受信だけでなく異なるサブドメイン間のメールの送受も検知対象としている．表 6 にウィルスゲートウェイによってフィルタされた主なウィルスメールの総数の集計結果である．調査期間は 2002 年 4 月 15 日から 2002 年 7 月 21 日である．表 6 の「比率」は，フィルタされた全ウィルスつきメール数に対するウイルス種別の割合を示す．

表 6: ウィルスゲートウェイによるフィルタ結果

ウィルス種別	件数	比率 (%)
WORM_KLEZ.H,G,E	4360	92
WORM_YAMA.E,D	185	3.9
WORM_BADTRANS.B	59	1.2
WORM_FRETHEM.K	43	0.9
その他	75	1.6
合計	4722	100

5 今後の検討事項

5.1 セキュリティポリシの見直し

FW の導入後，サブネットの都合により運用途中でゾーンの移行申請が 2 件あった．それはいずれも アクセス制限ゾーンからオープンゾーンへの移行であった．ゾーン移行の際の主な理由は次のようになった．

- サブネット内に独自のプロトコルを通す必要があるためアクセス制限ゾーンのポリシと合わない．
- アクセス制限ゾーンでのセキュリティポリシが緩いため独自 FW の管理下のもとで管理したい．

このような意見を参考にしながら，学内のセキュリティポリシを見直す必要があると思われる．

5.2 システムの運用の柔軟性

前述の実験のとおり，FW のネットワークトラフィックや運用状況によっては，通過パケットの処理速度は IP フィルタ 型の方が優れているとはいえないことが分かった．本学のように，FW 内から外部へのアクセス制限を設けない設定の場合，明らかに IP フィルタ型の方が運用は容易である．またキャンパス LAN を流れるトラフィックの増加にしたがって，FW のパケット処理速度が問題になってくる．キャンパス LAN 内のトラフィックが非常に多い組織の場合，FW への出入口で負荷分散を行なっている場合もある．このような問題も考慮に入れて，FW の動作モードについて考える必要がある．

6 むすび

本稿では，一般に統一的なセキュリティポリシの策定が難しい場合が多い大学において，FW をキャンパス LAN を 2 分割するような位置に設置した際の経緯や効果，課題等について報告した．

大学内に二つの異なるセキュリティポリシをもつゾーンを設け，FW を導入することにより，初期トラブル以外では比較的混乱が少なく移行できている．

本稿で報告した各種のデータは，現在も継続して採取中である．今後は調査結果やセキュリティ強化に対する各種の試みを，次回の機器更新の際のキャンパス LAN の構成へも反映する予定である．さらに，急速に広がっている無線 LAN へのセキュリティ対策や多様化する自宅や出張先等からの利用形態に対する VPN の導入などについても考えていかなければならない．

謝辞

本稿にあげたファイアウォールを含め，学内 LAN の運用・管理についてセンタースタッフの中島賢治氏，大迫誠氏，北地智恵氏，勝部章子氏，松元朋子氏，辻直子氏，また本学センター専門委員各位に御協力をいただいた．ここに記して謝意を表す．

参考文献

[1] J. H. Allen,:"The CERT Guide to System and Network Security Practice", Addison-Wesley, 2001

[2] 前田香織，河野英太郎，天野橘太郎：" 広島市立大学キャンパスネットワーク HUNET とマルチメディア情報通信実験", 電子情報通信学会技術報告, IN96-26, pp. 49-56, 1996

[3] 前田香織，河野英太郎，石田賢治，岩根典之：" キャンパス情報ネットワークシステムの分散管理の粒度", 情報処理学会研究報告, 2000-DSM-18-5, pp. 25-30, 2000

[4] 大塚秀治，久保美和子，牧野晋，山戸田芳雄，林英輔："VLAN 機能による研究室単位の多様なセキュリティポリシーの実現" 情報処理学会研究報告, 2001-DSM-23-8, pp. 43-48, 2001

[5] "CA-2001-19: "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL", CERT Advisory, http://www.cert.org/advisories/CA-2001-19.html, 2001

[6] "CA-2001-23: Continued Threat of the "Code Red" Worm", CERT Advisory, http://www.cert.org/advisories/CA-2001-23.html, 2001

[7] "CA-2001-26: Nimda Worm",http://www.cert.org/advisories/CA-2001-26.html, CERT Advisory, 2001