2008－IOT－2 (6)
2008／7／24

全教員に個別ファイアウォール機能を提供するキャンパスネットワークの構築

相原玲二 西村浩二 近堂徹 岸場清悟 田島浩一
広島大学 情報メディア教育研究センター

概要 平成 20 年度より広島大学で運用を開始した新キャンパスネットワークについて紹介する。新ネットワークは、教員数程度（約 2,000）の独立したファイアウォール機能を提供し、各教員が希望する場所で利用することができる。これまで各自で購入し、各自の部屋に設置していたルータやファイアウォールの機能を全学的に整備した。異なる建物や地区でも同一のファイアウォール配下に収容できるため、遠隔地にある同一研究室などでの利便性が向上した。本稿では、その実現方法について述べ、通信性能測定結果などを示す。

Construction of a Campus Network System Providing Dedicated Firewall Function for All Academic Staff

Reiji Aibara, Kouji Nishimura, Tohru Kondo, Seigo Kishiba, and Koichi Tashima

Information Media Center, Hiroshima University

Abstract: We describe a new campus network system opening at FIY 2008 in Hiroshima University. The network system is designed to provide dedicated firewall function for all academic staff of about 2,000 members, at any room or building. This function will cover routers or firewall systems prepared in the past by each staff. It is available to setup an inside network under a firewall for different rooms, buildings or campuses. In this paper, we demonstrate the implementation method and transmission measurement results of the system.

1. まえがき

大学などの高等学術機関では、教育研究のための高度で柔軟なキャンパスネットワークが求められるため、大規模な組織においては学部や学科などの単位でサブネットを構成し、サブネット内の運用には当該組織が責任を持つ代わりに比較的自由な運用を行ってきた。しかし、ネットワークがライフラインとしての重要性を増す一方で、インターネット上で発生するセキュリティ上の問題が多様化したことから、管理方針の大幅見直しを迫られている。本稿では、セキュアでスケーラブルなキャンパスネットワークを目指し構築した広島大学の新キャンパスネットワーク HINET2007[1][2]のファイアウォール機能について述べる。HINET2007 は教員数程度（約 2,000）の独立したファイアウォール機能を提供し、各教員が希望する場所で利用することができる。異なる建物や地区でも同一のファイアウォール配下に収容できるため、遠隔地にある同一研究室などでの利便性が向上した。本稿では、その実現方法について述べ、通信性能測定結果などを示す。

2. キャンパスネットワークの要件

広島大学での本格的なキャンパスネットワークは FDDI を基幹に採用した HINET93 であり、1994 年度より稼動した。約 40 台の FDDI ルータを中心に構成され、各ルータからは主に 10Base5 の支線が建物内へ配線され、一部は他の建物へも延長された。このネットワークを補完するように ATM を基幹とする HINET95 が、1996 年度より稼動した。主に動画像、音声（キャンパス間電話を含む）の伝送に利用された。HINET93 と HINET95 は、2001 年度より Gigabit Ethernet を基幹とする HINET2001 に更新され、現在に至っている。HINET2001 は、本学の主要 3 キャンパスにそれぞれ 1 台の L3 スイッチ（ルータ）を設置するシンプルな構成で、主要な建物に約 50 台の L2 スイッチを配置し、同一キャンパス内の L3 スイッチと Gigabit Ethernet で接続された。L2 スイッチの配下には、各部屋への配線のための LAN スイッチが接続されているが、それらは原則として部局が整備し管理しているため、全学的には把握できていない。それまで運用されていた 100 を越える学部等のサブネットは、IP ア

ドレスの変更を行わず、そのまま HINET2001 に収容した。現在、広島大学は教員約 1,800 人、職員約 3,300 人、学生約 15,000 人（附属学校の児童、生徒約 4,000 人は含まない）の規模である。

これまでの運用経験を基に、近年のネットワークに対する要求を勘案すると、HINET2001 に替わる新キャンパスネットワークの要件は以下のようになる。

(1) 全学的な一元管理体制

多くの部局では、これまでのサブネット管理体制では対応要員の確保が不可能であり、維持が困難となっている。全学的な一元管理体制をとるため、ネットワーク接続状況を各部屋の情報コンセント単位で把握できることが望まれる。そのため、主要フロアに設置する接続機器まで全学管理とする必要がある。

(2) すべての場所で機器接続に利用者認証

これまでサブネット管理者が行ってきたサブネット内の機器管理を全学一元管理とするには、研究室内を含めすべての場所で機器の接続には何らかの利用者認証を要求する必要がある。ただし、古い OS 等にも対応する必要があるため、全員に IEEE802.1x 認証などを強制することは不可能である。また、研究室内での利用を考慮すると、認証後はワイヤレートでのデータ転送が望まれる。

(3) 個別ファイアウォール機能の提供

接続機器を個別に管理するため、これまでサブネット内あるいは研究室内に設置していたファイアウォール機能（ブロードバンドルータ等を含む）は、キャンパスネットワークの機能として提供する必要がある。対外接続の境界に設置する全学的なファイアウォールのみでは不十分であり、利用者が希望する単位（研究室単位、教員単位など）で個別ファイアウォール機能を提供する必要がある。

(4) VLAN による柔軟な仮想配線を提供

研究室内に学外向けサーバを設置したい、IPv6 を利用したい、研究開発用テストベッドネットワーク JGN2 などを利用したいという要望に対して、キャンパス内に専用の配線が追加できない場合は多い。また、個別ファイアウォール機能を提供した場合、同一ファイアウォール配下としたい部屋が同一フロア内とは限らない。そのため、従来以上に IEEE802.1q (TagVLAN)機能による柔軟な設定が求められる。

3．運用方針と移行方針

前節で述べた要件を満たすよう設計し、2008 年 5 月より稼動している広島大学のキャンパスネットワーク HINET2007[1][2]の概要を図 1 に示す。本稿では特に、個別ファイアウォール機能の提供に焦点をあてて述べる。

3.1　ゾーン構成とアクセス制御

HINET2007 では、学内外からのアクセス可否パターンおよび利用形態により区別される「ゾーン」という概念を導入した。主要なゾーンは表 1 に示す 4 種類である。これらゾーン間および外部ネットワーク（インターネット）間のアクセス制御の概要を図 2 に示す。全学ファイアウォールと個別ファイアウォール（部局ファイアウォール）を導入し、ゾーンごとに使用の有無を決定している。なお、これらファイアウォールは IPv4 通信に対してのみ適用している。

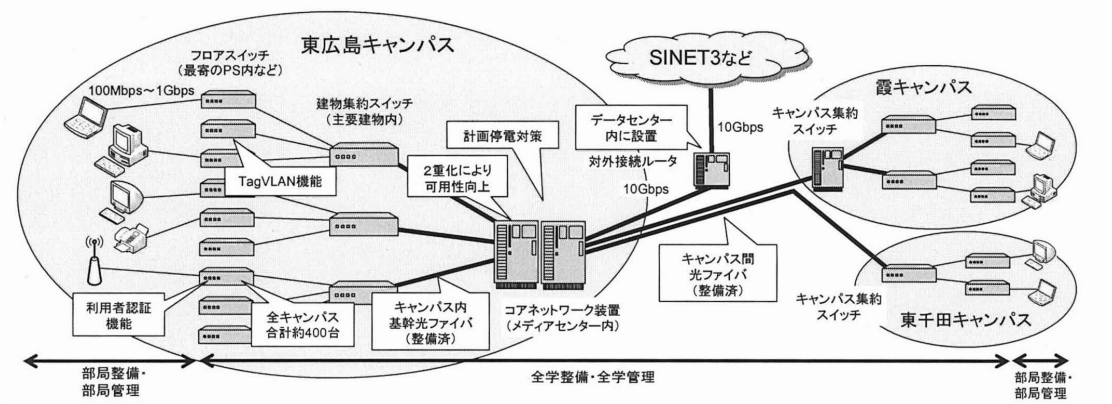


図 1　HINET2007 の概要

ゾーン名 略称	グローバルゾーン ゾーンA	ファイアウォールゾーン ゾーンB	ローカルゾーン ゾーンC	公衆ゾーン ゾーンD
主な用途	学外向けサーバ接続	学内共有サーバ接続	一般クライアント接続	オープンスペース
外部IPアドレス	グローバル 固定割当	グローバル 固定割当	グローバル 固定割当	グローバル DHCP割当
内部IPアドレス	外部IPアドレスと同じ	外部IPアドレスと同じ	プライベート(NAPT) DHCPまたは固定割当	外部IPアドレスと同じ
ゾーン外からの アクセス	学内外とも制限なし	学外から不可 ゾーンAを除く学内から可	同一ローカルゾーン以外 から不可	学外から不可 ゾーンAを除く学内から可
学外へのアクセス	制限なし	制限なし	原則制限なし (NAPTによる制限あり)	制限なし
端末認証	MACアドレス認証	MACアドレス認証	Web認証または MACアドレス認証	Web認証

表１　HINET2007で提供する主要ゾーン種別

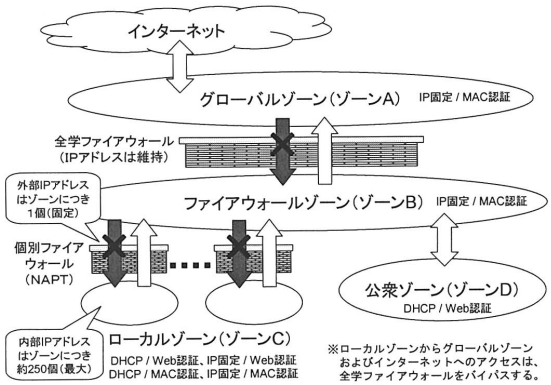


図２　ゾーン間のアクセス制御概念

X → Y 方向のアクセス可否

X ＼ Y	ゾーンA	ゾーンB	ゾーンC	ゾーンD	全学 サーバ	2001 Global	2001 FW	学外
ゾーンA	○	×	×	×	○	○	×	○
ゾーンB	○	○	×	○	○	○	○	○
ゾーンC	○	○	△	○	○	○	○	○
ゾーンD	○	○	×	○	○	○	○	○
全学サーバ	○	○	×	○	○	○	○	○
HINET2001 Global	○	○	×	○	○	○	○	○
HINET2001 FW	○	○	×	○	○	○	○	○
学外	○	×	×	×	○	○	×	−

全学サーバ：全学電子認証システムなど全学的サーバ接続用
HINET2001 Global：HINET2001の全学ファイアウォールに入っていないサブネット
HINET2001 FW：HINET2001の全学ファイアウォールに入っているサブネット

△：同一ゾーンC内ではアクセス可、異なるゾーンC間ではアクセス不可

表２　ゾーン間のアクセス可否

３.２　新ネットワークの運用方針

表１および図２に示しているが、HINET2007 では原則としてすべての接続端末に認証が求められる。認証方式は Web 認証と MAC アドレス認証のいずれかで、利用できる認証方式はゾーンにより決まる。ゾーン C では両認証方式を利用できるが、これはフロアスイッチの同一ポート配下で２認証方式が共存していることを意味する。

移行段階では HINET2001（旧ネットワーク）も並行運用するため、ファイアウォールによるアクセス可否の関係は複雑となる。主要４ゾーン以外を含めたアクセス可否の関係を表２に示す。

運用方針は以下のようにしている。

- 個別ファイアウォールの例外設定（特定ポートへのアクセス許可など）は受け付けない。
- 個別ファイアウォールのローカル側アドレスの希望は受け付けない。（センターが指定）
- 希望すればフロアスイッチの下流ポートへ Tagged での接続ができるが、VLAN ID の希望は受け付けない。（センターが指定）

３.３　新ネットワークへの移行方針

HINET2007 はこれまでのキャンパスネットワークと大幅に異なる構成となるため、移行時期を全学的に決定することは困難と判断した。そのため、HINET2001 を並行運用し、利用者が研究科、専攻、研究室等の単位で移行時期を決定できるよう配慮した。ただし、並行運用の期限は 2008 年度末までとし、その時点で HINET2001 を停止する予定としている。

具体的な移行作業はスイッチ配線の差し替えと機器の設定変更である。フロア内の最寄パイプスペース等に新旧のスイッチを設置している場合が多く、その場合はパイプスペースで各部屋へ伸びる LAN 配線を差し替える。また、原則 IP アドレスの変更（リナンバ）作業が発生するため、利用

者は配線差し替えの前後に PC 等の設定を変更する必要がある。

HINET2007 では、約 2,000 の個別ファイアウォール機能を提供するが、基幹スイッチ等の設定はあらかじめ行っておき、利用者の要望に応じてフロアスイッチ等の VLAN 設定を変更することで、希望する場所で個別ファイアウォール機能を利用できるようにしている。したがって、HINET2007 利用開始後、利用者の移行にともなう基幹スイッチ等の設定変更は原則発生しない。

4．ファイアウォール機能の実現

HINET2007 の基幹ネットワークの構成を図３に示す。装置やリンクの故障に備え、基幹部分は概ね２重化されている。L3 コアスイッチ内部の構成を図４に示す。この構成により各ゾーンの接続性（アクセス可否等）を実現している。今回導入した L3 コアスイッチ(Cisco Catalyst 6509)は内部にファイアウォールモジュール(FWSM)を 3 モジュール内蔵している。また、2 種類(VRF および MSFC)の独立した L3 ルーティング機能を提供することができる。L3(MSFC)および HINET2001 の L3 スイッチには、送信元および宛先 IP アドレス等の組合せによる経路制御（いわゆる Policy Routing）を設定し、必要なルーティングを実現した。

L3 コアスイッチに内蔵する FWSM は、全学ファイアウォールに 1 モジュール、個別ファイアウォールに 2 モジュールを割当てた。個別ファイアウォールの設定状況の一部を表３に示す。1 つの物理 FW (FWSM)あたり最大 20 の仮想 FW (VFW)を構成できる。また、1 つの VFW あたり最大 50 の内部インタフェース（内部ネットワーク）を定義できる。2 つの FWSM を使用することで

$2 \times 20 \times 50 = 2{,}000$

の内部ネットワークを構成できる。ただし、同一 VFW 配下の内部ネットワーク間はルーティングにより通信が可能となる。そこで、フィルタを設定することで内部ネットワーク間の通信ができないようにしている。

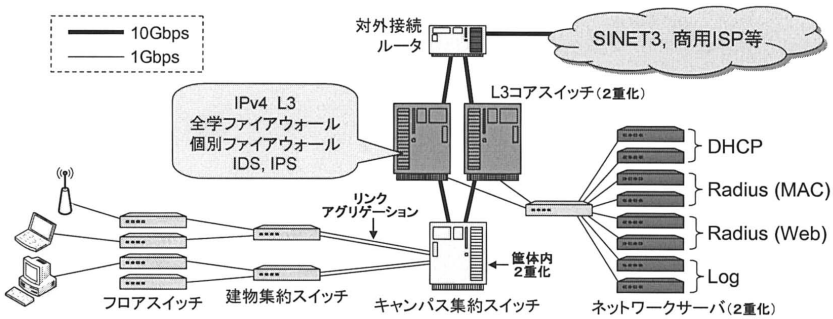


図３　基幹ネットワーク構成

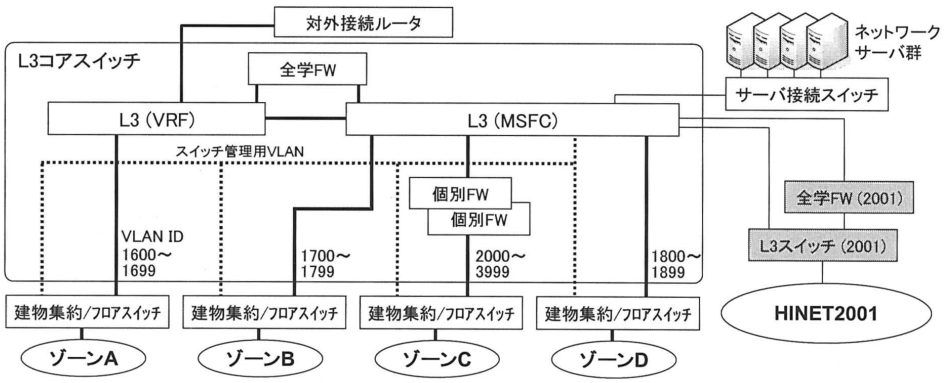


図４　L3 コアスイッチ設定概要

内部インタフェース		外部インタフェース			仮想FW	物理FW
ネットワーク	VLAN	ホストアドレス	ネットワーク	VLAN		
10.20.0.0/23	2000	133.41.74.8	133.41.74.0/26	1501	VFW#1	FWSM#2
10.20.2.0/23	2002	133.41.74.10				
10.20.4.0/23	2004	133.41.74.12				
10.20.6.0/23	2006	133.41.74.14				
10.20.8.0/24	2008	133.41.74.16				
10.20.9.0/24	2009	133.41.74.17				
:	:	:				
10.20.49.0/24	2049	133.41.74.57				
10.20.50.0/24	2050	133.41.74.72	133.41.74.64/26	1502	VFW#2	
:	:	:				
10.20.99.0/24	2099	133.41.74.121				
10.21.0.0/24	2100	133.41.74.136	133.41.74.128/26	1503	VFW#3	
:	:	:				
10.21.49.0/24	2149	133.41.74.185				
10.21.50.0/24	2150	133.41.74.200	133.41.74.192/26	1504	VFW#4	
:	:	:				
10.21.99.0/24	2199	133.41.74.249				
10.22.0.0/24	2200	133.41.75.8	133.41.75.0/26	1505	VFW#5	FWSM#3
:	:	:				
10.22.49.0/24	2249	133.41.75.57				
10.22.50.0/24	2250	133.41.75.72	133.41.75.64/26	1506	VFW#6	
:	:	:				
10.22.99.0/24	2299	133.41.75.121				
10.23.0.0/24	2300	133.41.75.136	133.41.75.128/26	1507	VFW#7	
:	:	:				
10.23.49.0/24	2349	133.41.75.185				
10.23.50.0/24	2350	133.41.75.200	133.41.75.192/26	1508	VFW#8	
:	:	:				
10.23.99.0/24	2399	133.41.75.249				

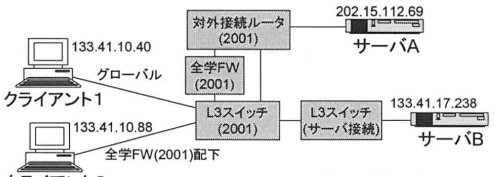
表３　個別ファイアウォールの設定（抜粋）

ファイアウォールの設定は、表３に示すとおり、各内部ネットワークが NAPT 機能により１つの外部 IP アドレスとなって外部へのアクセスを行う。内部ネットワークは、原則 /24 ブロックであるが、一部（表３の最初の４ブロック）は例外的に /23 としている。また、原則すべての内部ネットワークに対して DHCP を提供している。

なお、ゾーン A ではデュアルスタックにて IPv6 を提供しているが、現在の技術水準等を考慮して IPv6 のファイアウォール機能は使用していない。

５．性能測定

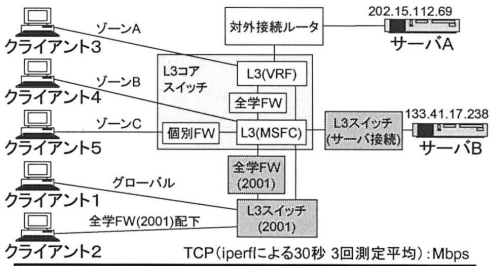
HINET2007 のファイアウォールが通信に与える影響を調べるため、HINET2007 の本格的な稼動に先立ち、通信速度の測定を行った。比較のため HINET2001 での測定を行った結果を図５に示す。HINET2007 の測定結果を図６に示す。HINET2007 の測定は、基幹ネットワークの設定はすべて完了し、約 2,000 のゾーン C を提供できる状態にした上で行った。また、図では記載を省略しているが、対外接続ルータとサーバ A の間には ISP のルータ、図６の L3 コアスイッチとクライアント３～５の間にはキャンパス集約スイッチと建物集約スイッチが存在している。いずれも、iperf[3]を用い TCP にて 30 秒間の測定３回の平均を示している。図５および図６の測定に使用した主な機器の名称または仕様を表４に示す。



TCP（iperfによる30秒 3回測定平均）：Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	505	444	672	620
クライアント2	--	360	680	645

図５　測定結果：HINET2007 移行前



TCP（iperfによる30秒 3回測定平均）：Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	471	517	704	709
クライアント2	--	365	691	615
クライアント3	637	685	712	878
クライアント4	--	348	696	801
クライアント5	--	292	--	433

図６　測定結果：HINET2007 移行後

装置	機器の名称または仕様
L3コアスイッチ (2007)	Cisco Catalyst 6509 FWSM x3, IDSM x2
対外接続ルータ (2007)	Alaxala AX6304S
L3スイッチ (サーバ接続)	Cisco Catalyst 6506
L3スイッチ (2001)	Cisco Catalyst 6509
全学FW (2001)	Alteon Switched Firewall Director/Accelerator Checkpoint Firewall-1
対外接続ルータ (2001)	Hitachi GR2000-BH
サーバA, B	CPU: Pentium4 (3.06GHz)、メモリ: 512MB OS: CentOS 4.6 (kernel 2.6.9-67.0.4)
クライアント1～5	CPU: Pentium4 (2.8GHz)、メモリ: 512MB OS: Debian GNU/Linux 4.0 (kernel 2.6.16.29)

表４　主な機器の名称または仕様

図５および図６における通信速度の差は、ファイアウォールを経由することによる遅延時間の影響が大きいものと思われる。HINET2001 と HINET2007 の全学ファイアウォールの影響については、図５のクライアント２と図６のクライアント４の結果を比較することで分かるが、ほぼ同様の結果となっている。これらに対して、図６のクライアント５の通信速度はやや低い。これは、１つのファイアウォールモジュールに 20 の仮想ファイアウォールを設定し、合計約 1,000 の内部ネットワークを定義したことによるものと思われる。

６．むすび

本稿では、広島大学で構築中の新キャンパスネットワーク HINET2007 について、個別ファイアウォール機能を中心に述べた。運用状態における性能測定結果を示し、今回導入した方式の性能に与える影響を定量的に示した。個別ファイアウォールが TCP 性能に与える影響は、少なからずあることが分かったが、実用上問題のない程度であると判断している。

新ネットワークへの移行は、原則として IP アドレスのリナンバリングを伴うため約 1 年間の移行期間を設けた。基幹ネットワーク装置等の設定はすべて行った状態で、移行の要求を随時受け付け、フロアスイッチ等の VLAN 設定により対応している。今回導入したフロアスイッチの総ポート数は約 13,000 であり、約 2,000 の VLAN を順次それらスイッチのポートへ割り当てる作業を行っている。１ポートへの割当であっても複数のスイッチを経由する場合があり、設定作業を円滑に進めるためネットワーク設計ツール VLAN.Config[4]を利用している。

HINET2007 では、原則としてすべての場所で機器接続に利用者認証を必要とする。認証スイッチの Web 認証には https プロトコルを使用するため、約 450 台分のサーバ証明書が必要となる。今回は国立情報学研究所 UPKI イニシアティブの UPKI サーバ証明書プロジェクト[5]に参加し、入手した証明書を利用している。

謝辞

HINET2007 の構築および運用に尽力して頂いている広島大学総務室情報化推進グループおよび情報メディア教育研究センターの関係者に感謝します。

参考文献

[1] 相原他: “利用者認証機能を持つ大規模キャンパスネットワークの構築”, 2008 年電子情報通信学会総合大会 BS-8-7, pp.S-116 – S-117, 2008 年 3 月.

[2] 広島大学情報メディア教育研究センター: “HINET2007 情報”, http://home.hiroshima-u.ac.jp/infra/hinet2007info/.

[3] NLANR/DAST: “The iperf project”, http://dast.nlanr.net/Projects/Iperf/.

[4] 株式会社イイガ: “ネットワーク設計ツール VLAN.Config”, http://www.iiga.jp/solution/config/vlan.html.

[5] 国立情報学研究所 UPKI イニシアティブ: UPKI サーバ証明書発行・導入における啓発・評価研究プロジェクト, http://upki-portal.nii.ac.jp/.