第 XXIX 部

大規模な仮設ネットワークテストベッドの設計・構築とその運用

第 29 部
大規模な仮設ネットワークテストベッドの設計・構築とその運用

第 1 章　2009 年春合宿ネットワークに関する報告

1.1 2009 年春合宿ネットワークに関する報告

1.1.1 概要

WIDE 合宿ではプログラム委員にて会場ネットワークが構築される。これは合宿参加者向けのネットワークインフラのみならず、このネットワークを利用した実験へのテストベッドとなっている。実験参加者は 200 名規模の合宿参加者を対象とした実験を行うことで、多数の被験者を用いた実験の実施が可能となり、各々の研究室では得られない知見を得ることが可能である。本合宿で実施された実験は、以下の通りである。

- P2P ネットワークを用いた写真の共有
- ALM 対応 HD 会議試作機による中継実験
- WiFi オペレーション
- IPsec with QKD
- WIDE 合宿におけるネットワークカメラを利用した研究参加支援システム

1.1.2 合宿ネットワーク

1.1.2.1 合宿地の対外線

今回の合宿会場である信州松代ロイヤルホテルでは、例年対外線として NTT 東日本のフレッツ ADSL を 2 回線と衛星回線 1 回線を引き込んで利用している。今回も同様に手配を行った。

合宿地では WIDE インターネット配下のネットワークを提供するために、WIDE インターネット拠点へ接続する必要がある。衛星回線は WIDE 藤沢 NOC の地球局へ繋がるため WIDE 内部への直接接続である。地上線の専用回線は高価なので、近年はトンネル技術を用いて接続する。ここ最近は藤沢 NOC の Cisco7206VXR へ IP-in-IP トンネルや GRE トンネルを行う手法がメジャーであったが、スループットが出ない問題や IP フラグメントを発生させる問題が合宿途中で発覚し、トンネル終端先を変更する事態となるケースが起こっている。

そのため今回の合宿ネットワークでは、ルータで L3 トンネルを行うのではなく、ルータ間に専用の L2 トンネル装置を配置する構成とした。スループットや IP フラグメントの問題は L2 トンネル装置側で処理させたため、ルータでは専用回線で結んでいるように接続できた。L2 トンネル装置は、PC に PacketiX VPN をインストールしたものと NEC IX2015 を 2 台ずつ 2 ペア用意し、ADSL 回線それぞれに接続した。PacketiX VPN と IX2015 は方式は異なるが、Ether over IP を実現する装置である。WIDE 藤沢 NOC へフレッツ回線を直接引き込むことはできないため、フレッツ ADSL 回線上で固定 IP アドレスのインターネット接続を用意しインターネット VPN 接続とした（図 1.1）。

また L2 トンネル装置は tagged VLAN（IEEE802.1Q）対応のものを用意し、実験実施者からの要望があれば WIDE バックボーンから VLAN 回線の引き込みに対応できるようにした。しかしながら、VLAN 利用の申し込みがなかったため利用されなかった。PacketiX VPN は、tagged VLAN 対応に改変したソフトウェアを用意してもらったが、インストールした PC 搭載の NIC（Broadcom BCM5721）が Jumbo Frame に対応していなかったため、VLAN tag ヘッダ分を引いた 1496 byte のパケットしか透過できない問題が合宿直前に発覚した。VLAN 利用の実験申し込みがなかったため、NIC を交換するなどの措置はとらず、今後の参考に留めることとした。

1.1.2.2 合宿地での基幹インフラ

会場ネットワークには、2 台の PC ルータを用意した。外部接続用の gw.camp とユーザ収容用の nat.camp である。nat.camp のユーザ収容に関しては、1.1.2.3 で詳しく述べる。各セグメントの構成は、図 1.2 の通りである。

ADSL 回線 2 本と衛星回線 1 本を gw.camp へレイヤ 3 接続した。OSPF のコスト調整で、ADSL 回線を優先回線とし、衛星回線はバックアップとした。

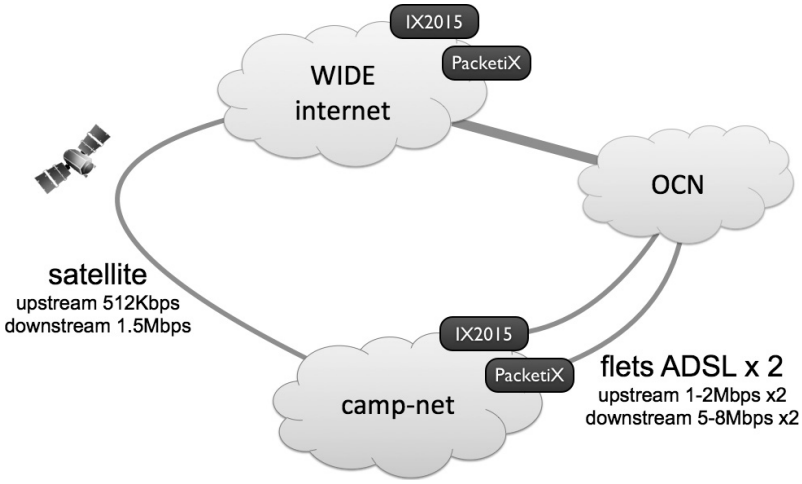


図 1.1.　対外線の構成

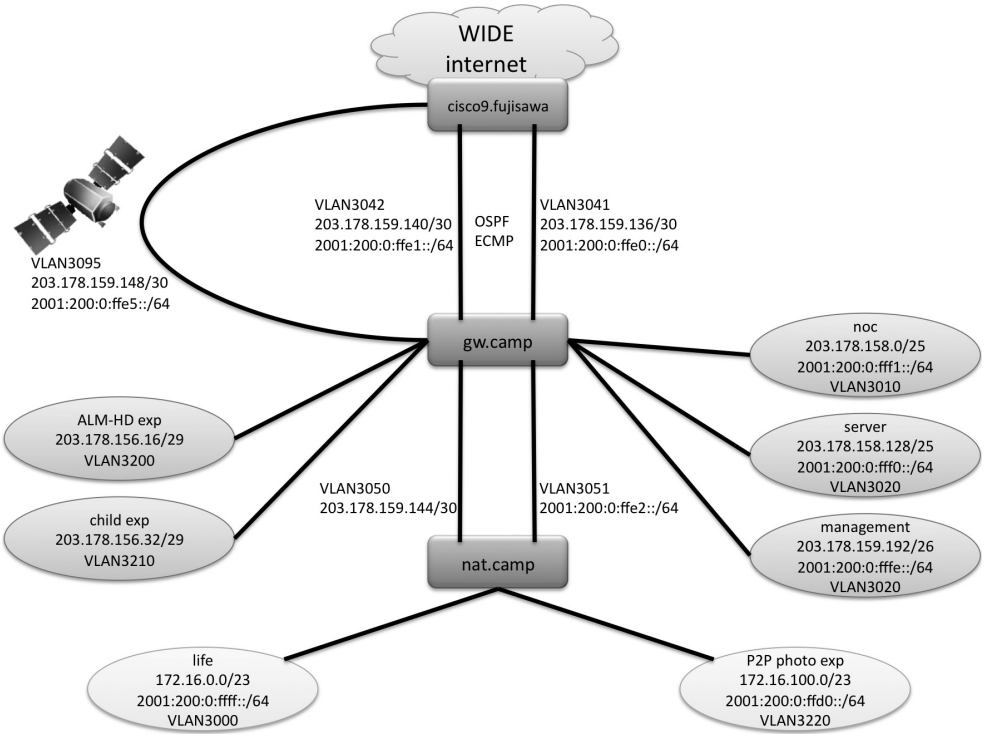


図 1.2.　レイヤ 3 構成

ADSL の 2 回線は OSPF を等コストで設定し、WIDE 藤沢 NOC から合宿地方向は Cisco ルータの機能で OSPF ECMP（Equal Cost Multi Path）で動作した。gw.camp は PC にインストールした Linux 上で quagga を動作させることで構築した。Linux が IPv4 ECMP をサポートしていたため、会場からインターネット方向の IPv4 トラフィックは 2 回線に分散したが、ECMP が働かない IPv6 トラフィックは片回線を流れた。合宿期間を通じての外部接続とのトラフィック量は、図 1.3 の通りである。ADSL は下り方向で 6 Mbps のスループットを出すことが可能であったので、2 回線でロードバランスすることで快適な接続環境を提供することができた。衛星回線はバックアップであったが、何もトラフィックが流れない事態を避けるため 3 日目に Policy Routing を実施し、一部セグメントの Web トラフィックのみ衛星回線を流れるように設定した。

サービス用のサーバセグメントと各実験セグメン

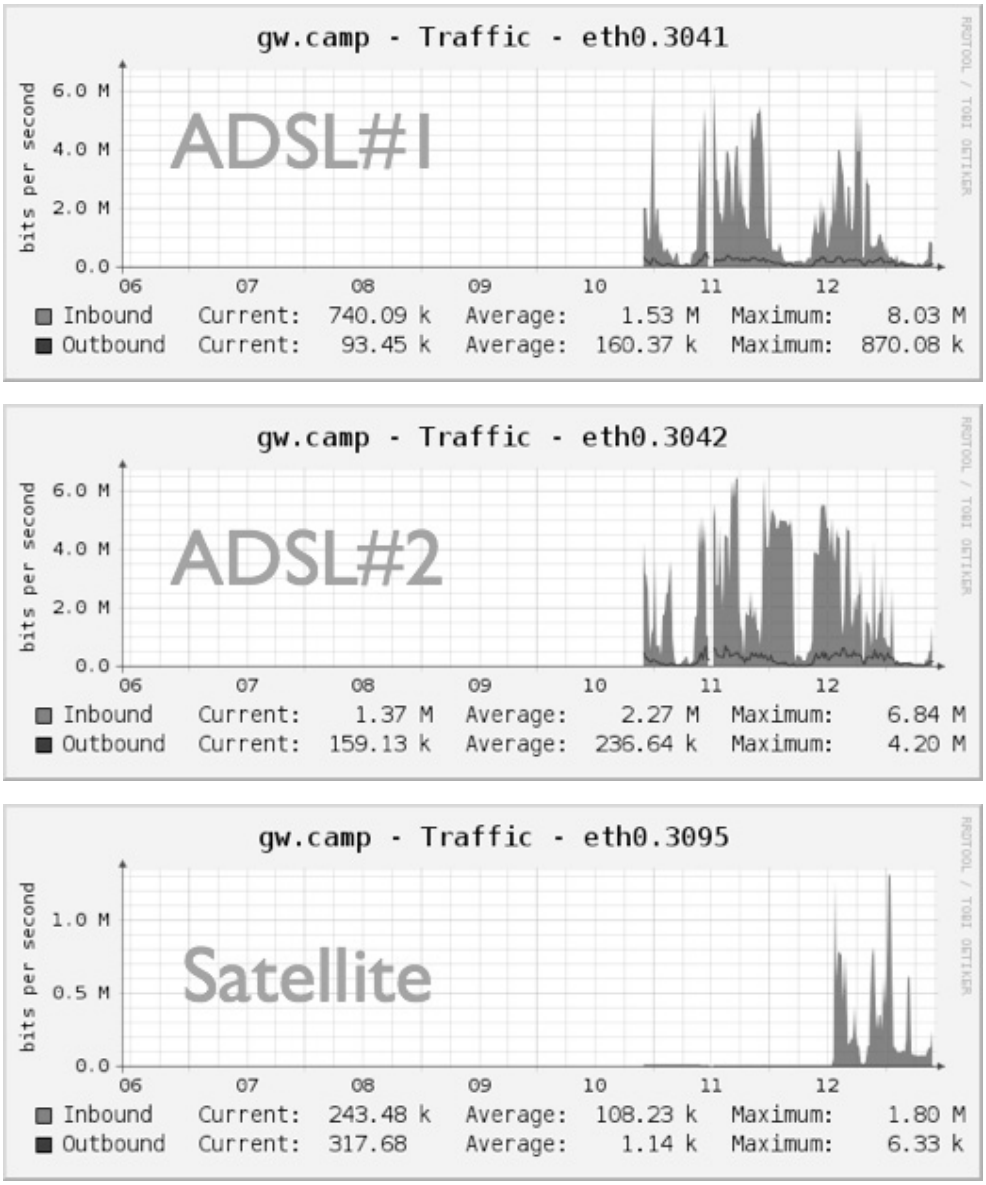


図 1.3. 対外回線のトラフィック量

トは、gw.camp に収容した。gw.camp は PC ルータで十分な数の NIC を搭載していないため、レイヤ 2 スイッチから tagged VLAN で接続し、VLAN サブインターフェースとしてルーティング制御を行った。

さらに、gw.camp と nat.camp 間は IPv4 と IPv6 で接続 VLAN を分けた。これによりユーザセグメントの IPv4 と IPv6 トラフィック量を分けて取得できた（図 1.4）。

1.1.2.3 ユーザ収容

ユーザには無線 LAN によるネットワークアクセスを提供した。今回は無線 LAN 運用自体が実験という位置づけだったので、詳しくは 1.1.3.3 にて報告する。

今回はインフラに関わる実験申請が無かったため、プログラム委員側でチャレンジ要素があるネットワークを用意することにした。昨今の IPv4 アドレス枯渇を背景に、枯渇後のインターネット接続形態が議論されている。例年の WIDE 合宿ネットワークでは、ユーザセグメントにおいて IPv4/IPv6 グローバルアドレスによるサービスを行っているが、IPv4 はプライベートアドレスによる提供とした。

さらに Large Scale NAT などに搭載が予定されている 1 ユーザあたりのセッション数制限機能を具備

図 1.4.　ユーザセグメントの IPv4/IPv6 トラフィック

pf による NAT とセッション数制限の設定例

```
# NAT の設定
nat on $external_if from $internal_network to any -> $external_addr

# 500 ノードまで、1 ノードあたり 100 セッション制限設定
pass in quick on $internal_if from $internal_network to any keep state
    (max 80000, source-track rule, max-src-nodes 500, max-src-states 100 )
block in quick on $internal_if from $internal_network to any
```

した。これは FreeBSD の pf を利用して実施した。その設定例の一部は 300 ページの囲みにある通りで、FreeBSD BOX にてセッションテーブルを保持し、source IP address ごとのセッション数を数え、新規セッションに属するパケットの通過を制限するものである。

ユーザごとのセッション制限数は、合宿日程中に徐々に減少させ、初日 200 セッションからスタートし 1 日ごとに約半減させ、ユーザごとに使用セッション数を記録した。しかし、DNS の名前解決はセッション数制限の対象から除外した。最終日に 1 ユーザあたり 5 セッションとかなり強めの制限にしたところ、図 1.5 のように Google MAP の一部が欠けた。IPv4 枯渇関連で、セッション数制限時の状況に関して調査結果などを知識として知っている合宿参加者は多かったが、実際に体験をしたことがある参加者は少なかったので多くの参加者から有意義な経験だったという感想を得た。合宿の日程を通して実セッション数の推移を見たところ、1 ユーザ当たり 150 セッション程度あれば、利用者本人が認識しない傾向であった。

初日にクライアント PC で IPv6 アドレスが中々取得できない問題が発生した。原因は NAT でリンクローカル通信がパケットフィルタで止められているため RS メッセージを nat.camp で受信できていなかった。フィルタの修正で解決したが、IPv6 はグローバルアドレス通信のほかに、リンクローカルアドレスに関してファイヤーウォールへの配慮が必要だとという知見が得られた。

今回の合宿では、ADSL 2 回線の良好なリンク速度（6 Mbps 以上）とロードバランスで帯域不足の不満は少なかったが、例年の合宿では参加者の苦情が出ることが多い。そのため、会場ネットワーク内に Web Proxy サーバを用意し、NAT に transparent

図 1.5. セッション制限時の Google MAP

proxy の設定を入れ、クライアント PC 側の設定変更無しに IPv4 HTTP トラフィックは Proxy を利用してもらった。キャッシュサイズは合宿 3 日間で 20 GB に及び、合宿 2 日目の Windows Update 時にネットワークの安定に寄与した。

1.1.3 実験

1.1.3.1 P2P ネットワークを用いた写真の共有

本実験は合宿参加者の写真を P2P ネットワーク上で共有し、実際の P2P アプリケーション構築に関わる様々な問題点を発見した。実験参加者には利用している計算機にアプリケーションをインストールしてもらうだけで、各個人が撮影した写真を実験参加者と共有できる。以下に詳細を述べる。

1.1.3.1.1 実験背景

デジタルカメラの普及によって高画素・高精細な写真データを身近に利用出来るようになった。デジタルカメラでは現像するコストや保存するコストがほとんどかからないため、個人が撮影する枚数は飛躍的に増加している。また、CMOS センサーの技術向上によって、写真の画素数も 1000 万画素を越えるものが主流となりつつあり、写真のデータ量は大きく増加している。一般利用者の写真データであっても、各個人が保有しているデータ量は膨大になることが想定でき、今後もますます増えていくと予想できる。

これらの写真をインターネット上で共有するサービスが増えている。多くのものはクライアント・サーバ型によるサービス提供を行っているが、サーバへ写真データを集中させることは負荷の増加に繋がる。特に写真データは 1 枚ではたいした量にならないものの、数が増えることで非常に大きな容量を占める。こうした問題に対応するため、P2P ネットワークを用いて写真の共有を行う「PSP2P」を開発し、前回の合宿で実験を行った。前回の実験では以下の反省点があった。

■ **Churn 問題**　オーバーレイネットワークはノードの自由な参加と離脱（Churn）を想定しているが、合宿ネットワークでは予想以上の Churn が発生したため、オーバーレイネットワークの構造維持が困難であった。一般的に Churn への対処としては共有している情報の複製を行う方法があるが、参加者全員で共通の無線 LAN を利用したような細い帯域の環境では、トラフィックを増やすことは望ましくないため、別の対策が必要となる。

■ **P2P 接続に関する問題**　PSP2P は写真を保有しているノードに直接 TCP のコネクションを生成し、高画素の写真データを取得する。しかし、合宿のネットワークという小規模なものでも P2P 接続が行えない計算機が発生したため、PSP2P による写真の取得を行えないことがあった。

■ **NAT 問題**　合宿ではユーザがラップトップの計算機を利用しているため、NAT を用いて接続するノードは存在しないと考えていたが、参加した計算機上で動作する仮想計算機（VM）などは NAT を利用してオーバーレイネットワークに参加することがあった。これも P2P 接続が行えないため、アプリケーションを利用することができなかった。

1.1.3.1.2 PSP2P の改良

実験を行うに当たり、特に Churn の影響を考慮して階層型のオーバーレイネットワークを構築した。例を図 1.6 に示す。図のようにオーバーレイネットワークを階層化し、下位層に Churn の激しいノードを集めることで上位層に配置された写真に関しては Churn の影響を受けることなく写真を取得することが可能になる。上位層には負荷が集中するが、現実的なリクエスト数を考えれば特に問題はない。以下に詳細を記す。

■階層型オーバーレイネットワーク　提案するオーバーレイネットワークに参加するノードは以下の情報を識別子とする。

- リング上の識別子（ID）
- 参加した時刻（t）

ノードはそれぞれルーティングテーブルを持ち、識別子とそのノードと通信するために必要な IP アドレスなどの情報を保持する。ID は Chord と同様に IP アドレス等をハッシュ関数を用いて変換する。参加時刻は現在時刻 Now を用いて、以下のように階層 L へ変換される。

$$L = \lfloor \log_2(Now - t) \rfloor \tag{1}$$

各ノードは他のノード情報として ID と T を受け取り、式 (1) を用いて現在の階層を各自で判断するため、時間経過に伴ってノードの階層が変わったとしても他のノードへ知らせる必要はない。

ノードは L 以下の階層すべてに所属する。各階層は Chord と同様のリングトポロジとなるため、successor、predicessor はそれぞれ L 個のノードとなる。successor は ID の管理範囲に密接に関係があるため、定期的にメッセージを送受信することで生存の確認を行い、ID の管理範囲が変化していないかを常に監視する。式 (1) のように L は参加時間の対数と定義しているため、時間経過に対して L が正比例して増えることはない。例えば経過時間が 1 か月の L は 21 であるが、1 年が経過しても L は 24 である。実際には $Now - t$ に対して下限の閾値を用いるため、生存の確認を行う相手ノードはもっと少なくなる。また、階層 l の successor が $l+1$ の successor と同じ場合、l より下の階層については生存確認を行わない。ノードはリングの多重化を防ぐために最も参加時間の長いノードをルーティングテーブルに必ず保持する。このノードはサービス提供者の用意する計算機になることを想定しているため、参加する際にサービス提供者などが用意する初期ノード（ブートストラップサーバ）から受け取ることにより対処する。

1.1.3.1.3 実験結果

合宿での実験を行った結果、最大で 10 ノードによるオーバーレイネットワークの構築を確認した。以下に考察を記す。

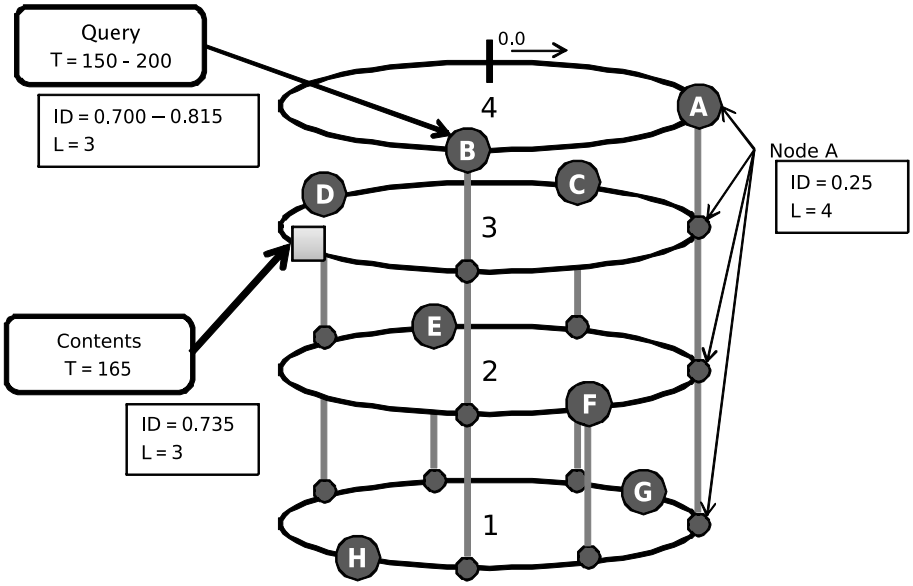


図 1.6.　階層化オーバーレイネットワーク概要図

■階層化による効果　ノードの参加時刻を基にしたオーバーレイネットワークの階層化を行った。しかし、合宿参加者は基本的に夜以降には計算機の電源を落とすため、その時点でオーバーレイネットワークから離脱してしまう。そのため、上位層の計算機はブートストラップサーバとして用意した計算機だけになり、そこに負荷が集中したため、クライアント・サーバ型と同様の形になってしまった。ノードが増えることで階層化は効果が出ると予測できるが、ノードが少ない環境でのP2Pアプリケーションの開発を考え、今後の知見とする。

■アプリケーションに対する魅力　写真を共有するという行為が多くの利用者に対して魅力的でなかったことがノード数を集められなかったことの原因であると考えられる。写真を使ったアプリケーションや、遊びの要素は多々残されているため、それらのアプリケーションを開発することでノード数を集め、クライアント・サーバ型では実現できない写真の共有を行いたい。

1.1.3.1.4 今後の課題

合宿参加者によるP2Pネットワークはクライアント・サーバ型と同程度の安定性を確保することが非常に困難であった。無線LANに接続されたラップトップの計算機という特性を考慮しなければ安定性や利用者を集めることが非常に難しい。今後は利用者が楽しめるアプリケーションを開発しつつ、少数のノードであっても安定できるP2Pネットワークの研究を進める。

1.1.3.2 ALM対応HD会議試作機による中継実験

パナソニック株式会社の米田、小西、村本がHD映像コミュニケーションシステムの拡張機能として導入予定のALM配信機能を搭載した試作機をデモ展示し、意見収集を行なった。具体的には、プレナリに設置したカメラのHD映像を会場の廊下、およびBOF1部屋へ配信するデモ展示と屋台村において以下の点に関する意見収集を実施した（図1.7、1.8）。

- DCCP、SCTP、XCASTを実装していない理由に関連して意見、感想
- RTCP拡張ヘッダを用いたQoS機能（FEC、ARQ、TFRC）実装について意見
- ALMによる配信の利用の障害要因
- 所属先などでALMによるHD映像配信システムを導入される可能性

この結果、以下のようなフィードバックが得られた（代表的な意見を抜粋）。

- プレゼンテーションの文字まで鮮明に見えてよい
- DCCP以外のTFRC実装：いろんな実装の試みがあるのは良い
- QoS機能標準化：必要＝53%、独自でよい＝22%
- 障害要因：強いてあげるなら、のぼりの帯域が増えることがALMの難点

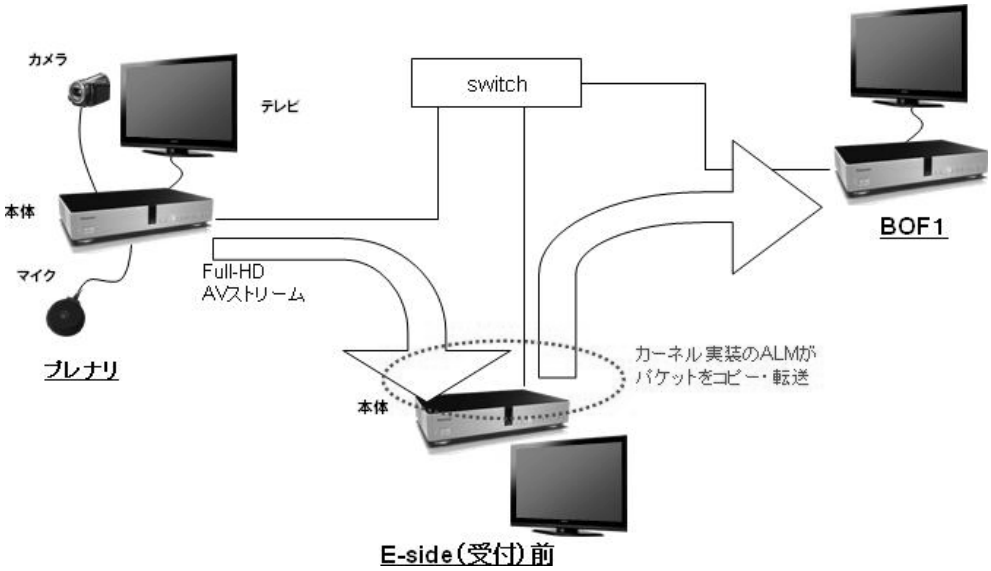


図1.7.　ALM対応HD試作機のデモ展示の構成

図 1.8.　ALM 対応 HD 試作機のデモ展示の様子

- テレビ会議のように特定時間だけ繋ぐのではなく、遠隔事業所のオフィスなどを繋ぎっぱなしにしておく。この使用帯域と解像度なら、そういう利用用途も可能だと思う。

1.1.3.3 WiFi オペレーション

本実験は、IETF76 広島における無線 LAN 設計に問題がないかどうかを検証するために実施された。

実験では、WIDE 合宿参加者が持ち込む様々な WiFi デバイスに対して、IETF76 にて使用予定の無線 LAN 機器による無線 LAN サービスを提供し、以下の項目についての評価をおこなった。

- IEEE 802.11n への対応状況と有効性の把握
- 持ち込まれた WiFi デバイスの接続性
- 100 から 150 ノード程度の利用環境におけるシステムの安定性

1.1.3.3.1 構成と設定の要点

実験は、プレナリ部屋において行われ、合計 5 台の Cisco 社製 Aironet 1250 無線 LAN アクセスポイントが展開された。本アクセスポイントは、IEEE802.11a/b/g に加え、11n (5 GHz) および、11n (2.4 GHz) に対応した製品となっている。

無線 LAN 通信規格としては、IEEE802.11a/b/g および、11n (5 GHz) を中心に検証し、暗号化なし、WPA/WPA2-パーソナル、WPA/WPA2-エンタープライズ（個人証明書）の規格にて運用をおこなった。なお、WPA/WPA2 エンタープライズにおける証明書の検証には、FreeRADIUS を利用しており、アクセスポイントにおいて、次のような EAP 認証用設定が導入されている。

設定例

```
aaa group server radius rad_eap
 server 192.168.0.1 auth-port 1812
 acct-port 1813
!
aaa authentication login eap_methods
group rad_eap

dot11 ssid wide
   vlan 111
   authentication open eap eap_methods
   authentication key-management wpa
   guest-mode
! freeradius server IP: 192.168.0.1
radius-server host 192.168.0.1
auth-port 1812 acct-port 1813
key 7 SHAREDKEY
```

1.1.3.3.2 運用結果

サービスした無線 LAN を分類すると表 1.1 の通りである。分類したサービスごとの利用クライアント数の推移は図 1.9 のようになった。

結果、802.11n への対応および、5 GHz 帯の利用 (802.11a および、n (5 GHz)) が進んでおり、2.4 GHz 帯利用者が 1 に対して、5 GHz 帯は、0.88 と、約 47%の利用者が 5 GHz に対応している。5 GHz 帯は、2.4 GHz に比べ、利用可能なチャンネル数が多く、かつ、同帯を他の無線機器が使う可能性がすくないため、高密度に利用者を収容する際には、非常に

表 1.1. SSID の分類

SSID	周波数帯	認証方式
wide	2.4 GHz	無し
wide-5G	5 GHz	WPA/WPA2 パーソナル
wide-wpa2-enterprise	2.4 GHz	WPA/WPA2 エンタープライズ
wide-5G-wpa2-enterprise	5 GHz	WPA/WPA2 エンタープライズ
wide-quantum	2.4 GHz	WPA/WPA2 エンタープライズ

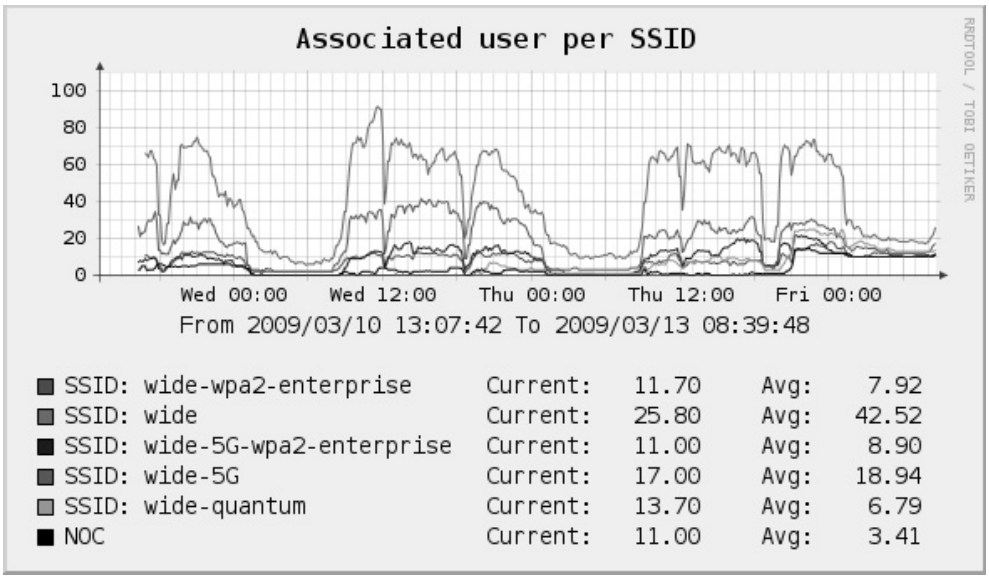


図 1.9. SSID ごとのアソシエーション数

有用な周波数帯である。したがって、この結果より、積極的に、5 GHz 帯を提供することにより、2.4 GHz の帯域不足を補うことが可能であるといえる。

また、IEEE802.11n についても全体の 25%の利用者が利用している。このため、IEEE802.11n により、クライアントがチャンネルを占有する時間を短縮化することができ、無線リソースの利用効率を高めることできるといえる。また、各通信規格ごとの安定性について、調査したところ、802.11n がもっとも安定しており、802.11a/b/g については、ほぼ同じ傾向となった。したがって、5 GHz 帯での 802.11n の利用は、有用であるといえる。

次に、WiFi デバイスの安定性についての調査の結果から、約 26%の利用者が安定した接続ができなかったことが判明した。これについては、有線側ネットワークの障害や、WPA/WPA2 エンタープライズにおけるサプリカントの相性問題も加味されているため、一概に無線 LAN のみに原因があるとはいえないといえるが、これ以上の原因特定は困難であったため、今後の原因調査が必要である。

以上の 2 点から、IETF での運用は、利用機器としては問題なく、利用する通信規格は、2.4 GHz 帯における 802.11b/g および、5 GHz 帯における 802.11a および 802.11n (5 GHz) が望ましいと結論づけられた。

1.1.3.4 IPsec with QKD

本実験では、CAMP-NET の一部区間に量子鍵配送を用いた IPsec 網を構築した。Internet Key Exchange (IKE) の実装である racoon2 を元に IKE の量子鍵配送拡張をおこない、raQoon2 と命名して実装した。raQoon2 の実用性検証のために、200 人弱のユーザの生活トラフィックがある CAMP-NET で実証実験をおこなった。

1.1.3.4.1 実験の背景と目的

量子鍵配送は、乱数を秘密に共有できる最も安全な方法である。量子効果の、観測すると状態が確定する性質とクローン不可能定理により、光子一つ一つに情報を乗せて送信することで乱数共有における盗聴者の有無を検知できる。量子鍵配送は安全性が

量子力学によって保証されているため、離散対数問題によって安全性が保証されている Diffie-Hellman 鍵共有や公開鍵暗号よりも安全である。

現在のコンピュータによる効率的な素因数分解の不可能性が証明されていない点や、量子コンピュータが開発されれば素因数分解が効率的に解かれることが既に示されている点から、離散対数問題による鍵共有に変わる安全な鍵共有として量子鍵配送の実用化が期待されている。

量子鍵配送装置は既に開発されており、量子鍵配送は実現されている。しかしながら、インターネットと組み合わせて利用する研究は行われておらず、今後の課題となっている。本実験では、インターネットでの量子鍵配送の実用性検証のために、量子鍵配送で作成した鍵で暗号化する IPsec の運用実験をおこなった。

実験にあたり、NEC 社より量子鍵配送装置 QUICS をお借りした。QUICS は量子鍵配送を行い、装置内部の UNIX FILE SYSTEM 上に鍵をファイルとして保存する機能を持つ。

1.1.3.4.2 実験内容

本実験は、IKE の WIDE プロジェクトによる実装である racoon2 を元に、IKE の量子鍵配送拡張をおこなって新プロトコルを構築し、raQoon2 を実装して実施した。

本実験は、図 1.10 のようなネットワークでの利用を想定し、図 1.11 のネットワークでおこなった。

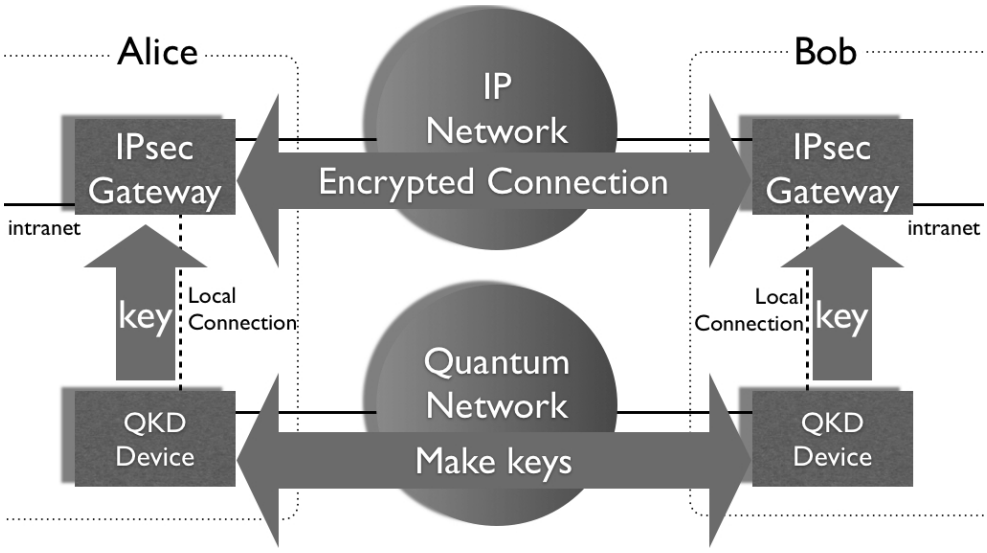


図 1.10.　ネットワーク想定図

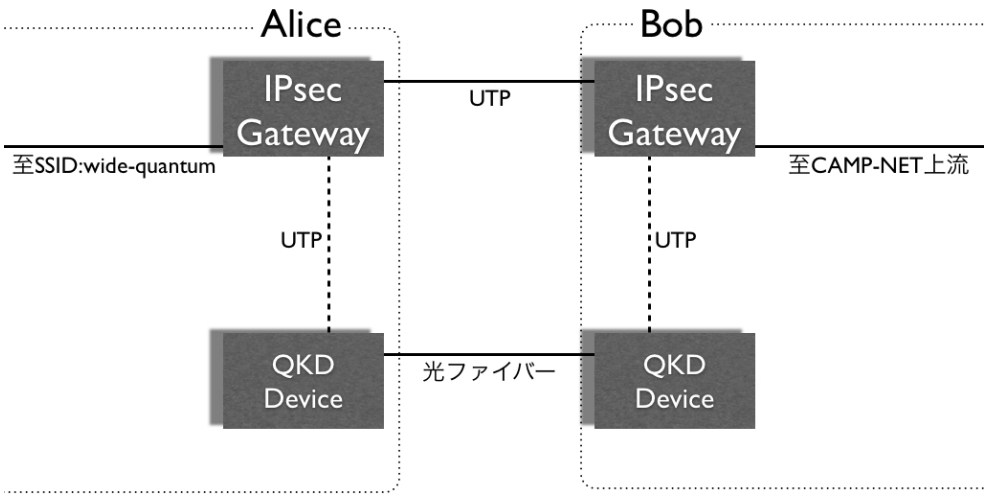


図 1.11.　実験ネットワーク図

本実験では、Alice 側を閉域網とし、Bob 側をインターネットとしている。Alice 側の先は無線 LAN を用いて生活ネットワークを提供し、Bob 側は CAMP-NET 上流を通りインターネットと接続している。Alice 側 Bob 側共に、IPsec Gateway と量子鍵配送装置が一台ずつ設置されている。IPsec Gateway と量子鍵配送装置を繋ぐ接続は安全に運用する必要がある。IPsec Gateway 同士は、インターネットを想定した UTP ケーブルで繋がれている。この接続は安全ではないことを想定している。量子鍵配送装置同士は光ファイバーで接続されている。この光ファイバーを利用して光子を送受信し量子鍵配送を行う。将来的に、この接続は量子ネットワークを介することを想定している。

本実験では IPsec は以下の手順で実現された。

1. 量子鍵配送装置が、量子鍵配送により乱数を秘密に共有する
2. raQoon2 が、量子鍵配送装置から乱数を取得する
3. raQoon2 が、取得した乱数を鍵に利用して、Security Association の折衝を行う
4. raQoon2 が、通常の IKE と同様に IPsec を実行する

1.1.3.4.3 評価とその後

本実験により、量子鍵配送と IKE の量子鍵配送拡張プロトコル、raQoon2 はインターネット通信の暗号化に実用できることが明らかとなった。

IKE 量子鍵配送拡張プロトコルは、標準化のため 2009 年 10 月に広島で行われた IETF2009 において Internet Draft -00[72] として発表した。今後も、標準化のため IETF で活動していく予定である。

1.1.3.4.4 acknowledgement

NEC 社の本実験と研究へのご協力に感謝致します。

1.1.3.5 WIDE 合宿におけるネットワークカメラを利用した研究参加支援システム

- 実験実施者：新 麗、二宮 恵、宮川 祥子

1.1.3.5.1 実験の概要

さまざまなライフステージにおいて、仕事や研究への関わりかたは様々である。社会的には、仕事や研究には一定期間継続して従事することが期待されるが、個人をとりまく環境によっては継続が難しいこともある。例えば、育児や介護、あるいは病気や怪我などで仕事や研究に従事する時間が限られたり、通勤・通学が難しくなったりすることもある。これまでは、仕事や研究の継続には会社や大学にいなければならなかったため、環境が変化すると継続を断念せざるを得ないことが多かった。

しかし近年の画像や音声の電子化技術や伝送技術の発展によって、場所に縛られずに様々な情報を得たり、コミュニケーションを取ったりすることができるようになってきた。これらの技術を活用すれば、実際にその場所にいなくても仕事や研究を継続していける可能性がある。しかし、これらの技術はシーズとしては揃いつつあるものの、システムとしては完成しておらず、実際に活用するには、ネットワーク、アプリケーションの環境を整えるほかに、それぞれの技術に対する専門知識が必要となる。

本実験では、育児中の研究者が子供同伴で WIDE 研究会合宿に参加する場合に、特に夜の会議への参加を支援するシステムを設計し、実際の研究会において構築し実証実験を行った。システムとしては、夜の早い時間帯に会議場の外から会議に参加する「仮想会議参加システム」と遅い時間帯に会議場にいながら寝室の子供の監視を行う「仮想子供見守りシステム」の 2 種類を設計し、WIDE 研究会合宿において実際に構築、運用を行った

1.1.3.5.2 実験の背景

WIDE 研究会合宿は、3 泊 4 日で朝 9 時から夜 22 時頃まで議論を行うという形態である。朝 9 時から 19 時頃まではベビーシッターを依頼することで、保育園に預けての通常の勤務体系と同じ状況を確保するため、会議参加には特に問題はない。しかし 19 時以降は寝る準備と寝かしつけ、また寝た後は様子を見ていなければならず、これまでは 19 時以降に会議に参加することは困難であった。

まず、子供と保護者の夜 19 時から 22 時までのだいたいのスケジュールを表 1.2 に整理する。子供の状況に応じ、21 時前後の就寝前と就寝後とでは必要となる対応が違うため、それぞれに対して異なる要求事項が生じることになる。

子供が就寝前に遊んでいる時間は、現状では保護者が部屋などで相手をしており会議には参加できない。しかし入眠直前でなければ部屋で過ごす必要はなく、子供も多少は動きたがる時間である。一方で会議は行われており、できれば参加したいができな

表 1.2.　19 時から 22 時までのスケジュール

時間	保護者	子供
19 時	夕食	夕食/入浴
20 時	会議	遊ぶ/就寝準備
21 時	会議	就寝
22 時	懇親会	就寝

い時間になる。しかし子供が会議場に入っておとなしく聞くことは不可能なため、会議場の外で会議の様子を知ることができるシステムが必要である。

子供が就寝した後は、保護者は部屋で様子を見なければならず、やはり会議やその後の懇親会に参加することはできない。ときどき目覚めて泣くこともあるため目を離せないが、よく眠っていれば特に手がかからないため、会議にも参加したい時間帯となる。懇親会の場合は、会議の様子を知ることだけではなく直接その場に参加しなければ意味がないため、会議場から子供の様子を知ることができるシステムが必要となる。

1.1.3.5.3 システム構成

2009 年 WIDE 春合宿では 1. 仮想会議参加システムと 2. 仮想子供見守りシステムを構築した。仮想会議参加システムは、会議場の様子を音声で中継して、会議場の外から仮想的に会議に参加するシステムである。具体的には、会議場の音声をパソコンに取り込み、Skype ソフトウェアのグループ通話機能を利用して実現する。保護者は Windows Mobile 等の携帯端末を持ち、Skype の Mobile 対応版を利用して音声を聴講する。

仮想子供見守りシステムは、寝室で眠っている子供の様子を中継して会議場から仮想的に子供を見守るシステムである。基本的には静かに寝ている子供を中継するため、ずっと画面を監視するのではなく、泣くなどのイベントを検知して通知する仕組みを同時に構築する。保護者はイベント通知を受け取ったら画像を確認して、様子を確認する。具体的には、中継についてはパナソニックコミュニケーションズ株式会社製のネットワークカメラを利用して実現する。搭載されたカメラとマイクにより、会議場の画像と音声を取得できる。また、配信システムも装備されており、中継も実現できる。見守る保護者は無線 LAN 機能を有し、Windows mobile 等が搭載されていて Web ブラウザを利用できる携帯端末から画像を見る。また、音声検知と通知システムについては別システムが必要であるため、マイクとリレーを使って作成するほか、カメラの機能である動作検知機能を利用する。通知については、ネットワークカメラに装備されている、アクションによってメールや画像の保存を行う機能を利用する。

仮想子供見守りシステムを構築するためには、研究会会場と同じネットワークを寝室にも用意する必要がある。必要となるのは、実験参加者である 3 名 3 室に対してローカルなネットワークサービスを提供すること、および外部接続を利用して研究会会場のネットワークシステムに VPN を構築することである。カメラを外部ネットワークサービスに接続することも可能であるが、画像が外部に公開されることになり望ましくない。そこで、VPN の構築が必要となる。

まず、部屋間のローカルなネットワークはパナソニックコミュニケーションズ株式会社製の PLC（Power Line Communication）を利用する。次に、外部ネットワークサービスについては、株式会社インターネットイニシアティブの iijmobile サービス/タイプ DS（固定グローバル IP アドレス割当）およびデータ通信カードを利用する。データ通信カードは、同じく株式会社インターネットイニシアティブ製の SEIL というルータに接続し、ローカルに接続した 3 室のネットワークから研究会のネットワークに VPN を構築する。ネットワーク構成を図 1.12 に示す。

1.1.3.5.4 実証実験

2009 年 WIDE 春研究会合宿において、本システムを稼働させ実証実験を行った。2 日目にはネットワークも含めてシステムの構築が完了し、一部の部屋で仮想子供見守りシステムを利用することができた。3 日目は 3 室とも仮想見守りシステムが稼働し、懇親会の時間に議論に参加することができ、また、子供が寝返ったり泣いたりした場合にはメールで通知され、カメラを見て寝返りなのか泣いているのかを確認してから寝室に様子を見に行くことができた。仮想会議参加システムについては、会議場の近くで子供を見ながら発表や議論を聞くことができた。

1.1.3.5.5 まとめと今後の課題

実証実験を通じて、本システムの稼働が研究活動の継続に有益であり、これまでできなかった議論に

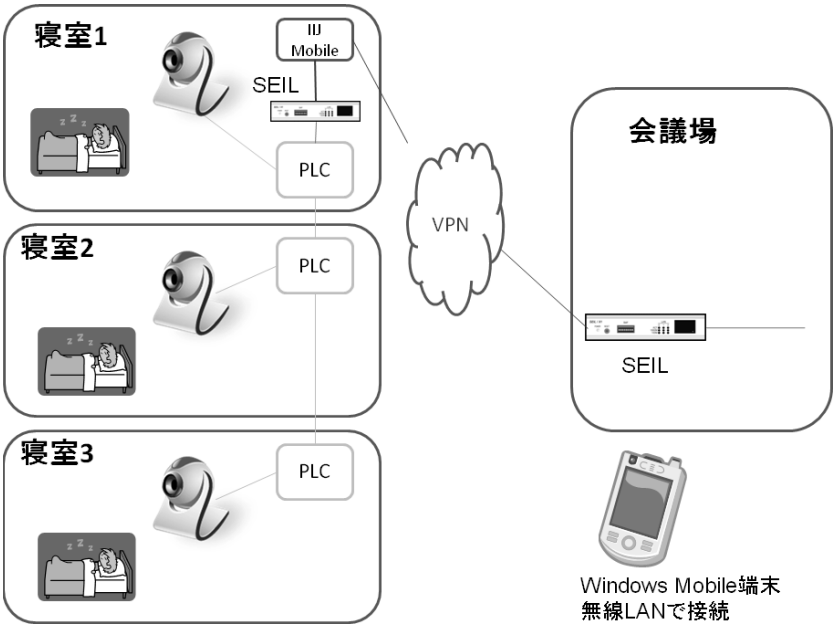


図 1.12. ネットワーク構成図

参加できたという結果を得た。今後は、寝室との双方向通信の実現や、構築・設定の簡易化をさらに進めるなどの課題を解決し、実証実験を重ねるとともに、本システムの他分野への応用も検討する。

本システムは利用者である実験実施者にとって有用であることは間違いない。しかし、今後の発展や応用を考える場合には、システム自体の評価をどう行うかを検討する必要がある。評価指標は 1 つではなく、ネットワーク帯域の評価、システムが実現する機能の評価、構築の方法や時間に関する評価、使用感に関する評価など多数の視点が考えられる。今後は評価指標についても考慮しつつ、再度実証実験を行う予定である。

1.1.4 まとめ

本合宿では、初日に IPv6 が繋がりにくいという問題が発生した以外は障害が発生することなく、無線 LAN を含めて安定したネットワークを提供できた。

また、アプリケーションを中心とした実験を実施し、実験者が想定する動作結果を得られた。しかしながら、実験の目的などの実験内容の紹介が合宿参加者へ十分ではなく、実験実施のみならず、研究発表的な側面からのサポートをプログラム委員で強化すべきではないかと感じた。実験者は、実験準備にかなりの稼働を用するので、このような機会を最大限活用できるよう、今後の合宿に期待したい。

1.2 プログラム報告

1.2.1 はじめに

本節は、2009 年 3 月 10 日（火）から 13 日（金）にかけて、長野県長野市松代町にて開催された WIDE 合宿ミーティングの活動をまとめたものである。

1.2.2 プログラム報告

1.2.2.1 プログラムのねらい

2009 年春合宿では、過去数回の合宿にて試験的に導入されたプログラムや活動の成熟化を図るとともに、WIDE における研究のアクティビティを活発化する、という目標のもと、プログラムを構成した。今回の合宿では、ワーキンググループ BoF、研究発表などの従来のプログラムに加え、2008 年の春・秋合宿にて試験的に導入され、好評であった以下のプログラムを施行した。

- チュートリアル
- mini ワークショップ
- 屋台村（ポスターセッション）

また、人材および共同研究者を求めるワーキンググループや個人、グループのために、人材募集を行う枠をプレナリセッションに設けた。以下、個別のプログラムについて述べる。

1.2.2.2 チュートリアル

本合宿でのチュートリアルには 2 件の応募があった。両者とも WIDE の研究アクティビティの向上に大きく寄与するとの判断に基づき、従来の並列セッションではなく、プレナリセッションとしてチュートリアルを開催した。今回開催されたチュートリアルは以下の 2 つである。

- 演目：Internet Infrastructure Governance
  講演者：Ole Jacobsen (Cisco Systems)
- 演目：Reading and Writing Research Papers in English
  講演者：Rod Van Meter (Keio University)

各チュートリアルには、プレナリセッションでの枠の他に、より詳細な議論を行うために BoF 枠を別途設けた。

1.2.3 mini ワークショップ

本合宿においても、2008 年秋合宿にて好評であった mini ワークショップを実施した。前回の開催に寄せられた意見に、長時間の mini ワークショップは他の参加した BoF との衝突が起こりやすい、というものがあった。これを踏まえ、今回は mini ワークショップを 3 日目の午後に集約する対策をとった。開催された mini ワークショップは以下の 3 つである。

- Live E! Development Workshop
  コーディネータ：落合 秀也（東京大学）、松浦 知史（奈良先端科学技術大学院大学）、山内 正人（慶應義塾大学）
  概要：Live E! のソースコードや開発機材を持ち込み、開発に明け暮れる。PIAX との Integration を始め、Armadillo 組込み機器への DTN 実験プログラム移植など自由に何でも持ち込み可&面白いネタ大歓迎している。
- BabyStarBED WS at WIDE camp
  コーディネータ：宮地 利幸（NiCT）
  概要：Nerdbox Freask の活動の一環として行っている、実験を支援するためのソフトウェア群の利用方法を仮想機械を利用した手元の環境で体験するためのワークショップを行う。PC クラスタを制御し環境の構築とシナリオの実行を支援する SpringOS、設定ファイルから自動的に zebra bgpd の設定を生成する Anybed、そして、xen を利用し大規模な Inter-AS 環境を構築する XENebula の使い方を説明する。
- workshop for cool website design
  コーディネータ：奥野 隆大、廣海 緑里、酒井 慎一（慶應義塾大学）
  概要：かっこいい WEB デザインを実現するための重要点について学び、WEB サイト構築のアイディアとテクニックを習得する。

1.2.4 研究アクティビティの向上

WIDE における研究アクティビティの向上を図るために、初日のプレナリセッションにおいて人材募集を行うセッションを設けた。新人などの人材を募集している各ワーキンググループから、研究トピックの紹介とどのような人材を求めているのか、といった募集がなされた。しかし、事前に十分な告知や準備がなされなかったこともあり、ワーキンググループやメンバー間での研究活動の共有や促進に大きく寄与できるような成果が得られなかった。

また、二日目午前の BoF セッションでは、ボード主催による「WIDE でのこれからのリサーチディレクションについて考える会」が開催された。このセッションでは WIDE における研究・運営の体制を包括的に見直し、今後の 10 年の活動を見据えた議論が行われた。ここでの議論の成果は次回以降の合宿、研究会に引き継がれ、WIDE における研究体制改革の基盤となっている。

1.2.5 プログラムまとめ

2009 年春合宿では、過去数回に渡って試験的に取り入れられたプログラムの成熟化を図るとともに、WIDE における研究アクティビティの向上を目標にプログラムを構成した。チュートリアル、mini ワークショップなどのプログラムは今回も好評を博し、プログラムの成熟化には一定の成果が得られた。一方、人材募集など一部のプログラムには、準備や構成の不備が見られた。以後のプログラム委員は、今回の反省や、アンケート結果を通じて得られたフィードバックを反映して、より魅力的な合宿プログラムの構成に取り組んでもらいたい。

第2章　2009年秋合宿ネットワークに関する報告

2.1 はじめに

本章は、2009年9月7日（月）から10日（木）にかけて、長野県長野市松代町にて開催されたWIDE合宿におけるネットワークと各実験の報告を述べる。合宿プログラム委員会では、ネットワーク構築・運用チームを編成し、合宿参加者のインフラストラクチャおよび参加者を被験者とした大規模実験テストベットとなるネットワークを構築した。

本合宿中に実施された実験は、以下の5件である。

- WIDE合宿におけるネットワークカメラを利用した研究参加支援システム
- 「模倣インターネット環境と実インターネットワークの統合実験」～最後は模倣harm～
- パケットヘッダ情報を用いた仮想識別システムの検討
- フリーの監視ツールを用いたネットワーク監視
- Eブルーシートとプレゼンテーター表示システムを使った合宿（会議）支援システム

2.2 合宿ネットワーク

2.2.1 合宿ネットワークの設計

本合宿では、各実験グループの要求事項を満たすよう、以下の方針に従ってネットワークを設計した。

- 対外線の冗長化を行う。
- 参加者のIPv6への移行を目的とした、IPv6/IPv4トランスレータ（TRT）の運用。
- 合宿地で運用するサーバに対して、VMWare ESXiの仮想化技術を用い、状況に応じてサービスの追加・複製・削除・コールドマイグレーションを臨機応変に行えるようにする。
- “「模倣インターネット環境と実インターネットワークの統合実験」～最後は模倣harm～” 実験（模倣実験）の要求事項：各部屋ごとに異なるセグメント（VLAN）を提供し、各ネットワークを模倣実験ネットワークへ収容する。
- “Eブルーシートとプレゼンテーター表示システムを使った合宿（会議）支援システム” 実験の要求事項：他の実験機器を挟まない、合宿地内での安定して使用できる無線セグメントを提供する。

合宿参加者用のネットワークとして、表2.1に示す9種類のネットワークを無線LAN（IEEE802.11a/b/g/n）により提供した。“widecamp” および “widecamp-eap” ネットワークでは、IPv4 NAPTおよびIPv6のデュアルスタックネットワークを提供した。また、このネットワークでは、IPv6/IPv4トランスレータ（`FAITH`、RFC 3142）を導入し、IPv6ネットワークからIPv4ネットワークへのアクセスを行えるようにした。“satelife” ネットワークでは、IPv4（NAT無し、グローバルアドレスでの運用）およびIPv6のデュアルスタックネットワークを提供した。このネットワークでは、“Eブルーシートとプレゼンテーター表示システムを使った合宿（会議）支援システム” 実験の要求である、安定した合宿地ネットワークを提供するために、実験機器を挟まずに合宿基幹ネットワークに直接収容した。対外線については、ポリシーベースルーティングにより衛星回線を利用し、IPv4グローバルアドレスを使用したい利用者や衛星回線を体験したい合宿参加者にこのネットワークを提供した。実験ネットワークである “moho*[P1234B]*” ネットワークは、IPv4を模倣

表2.1.　合宿参加者に提供したネットワーク

ネットワーク名/SSID	無線認証方式	ネットワーク	提供範囲
widecamp	WEP	IPv4 NAPT/TRT + IPv6	全部屋
widecamp-eap	WPA2-EAP	IPv4 NAPT/TRT + IPv6	全部屋
satelife	WEP	IPv4 (global) + IPv6	全部屋
mohoP	WEP	IPv4 NAPT（模倣実験）+ IPv6	プレナリ
moho1	WEP	IPv4 NAPT（模倣実験）+ IPv6	BoF 1
moho2	WEP	IPv4 NAPT（模倣実験）+ IPv6	BoF 2
moho3	WEP	IPv4 NAPT（模倣実験）+ IPv6	BoF 3
moho4	WEP	IPv4 NAPT（模倣実験）+ IPv6	BoF 4
mohoB	WEP	IPv4 NAPT（模倣実験）+ IPv6	Board部屋

実験から NAPT で提供し、IPv6 を合宿基幹ネットワークから提供した。これらの実験ネットワークは、表 2.1 に示す範囲で提供した。

今回の合宿ネットワークでは、対外線としてフレッツ光ネクスト回線（上り・下り 100 Mbps（ベストエフォート））1 本および衛星回線（上り 0.5 Mbps、下り 1.5 Mbps）1 本を利用した。衛星回線では、慶應義塾大学湘南藤沢キャンパス（SFC）から合宿地まで双方向衛星通信回線により WIDE 藤沢 NOC–合宿ネットワーク間の L2 接続性を確保した。また、フレッツ光ネクスト回線上に国立天文台三鷹キャンパスと合宿地間で L2-VPN（NetBSD 5.0.1、OpenVPN）を確立し、WIDE 国立天文台ブランチ–合宿ネットワーク間の L2 接続性を確保した。

本合宿で構築した基幹ネットワークの L2、L3 トポロジーをそれぞれ図 2.1、図 2.2 に示す。

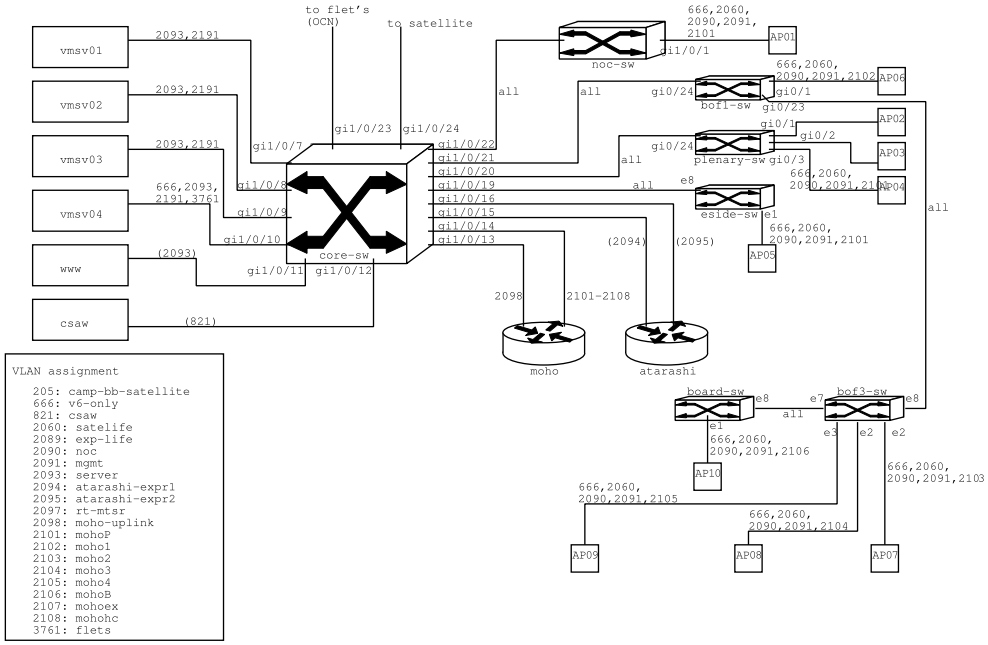


図 2.1.　L2 トポロジー

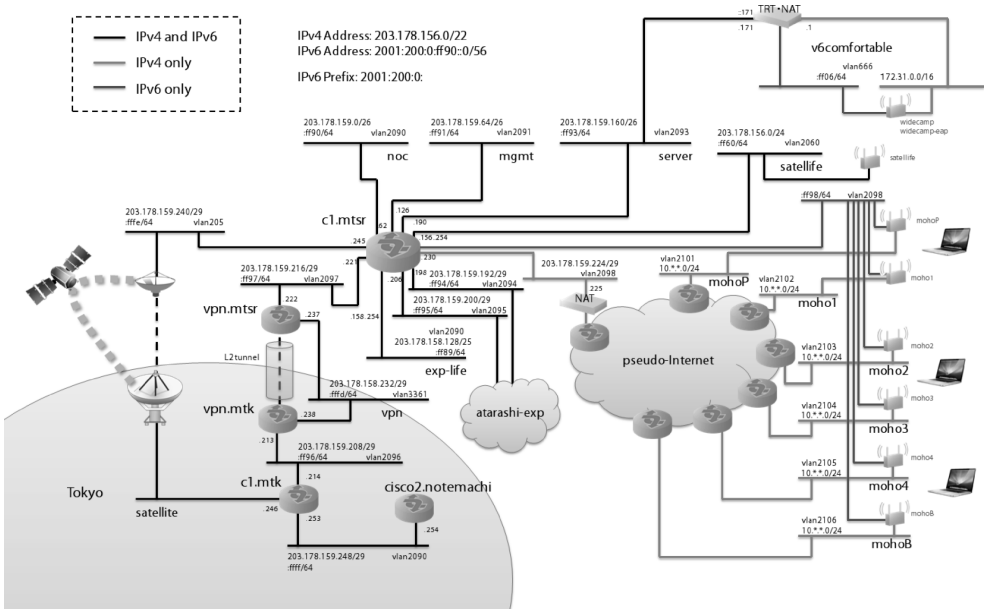


図 2.2.　L3 トポロジー

2.2.2 合宿ネットワークの運用

L2-VPN の運用　本合宿では、過去の合宿ネットワークの構築において指摘されていた MTU 問題（RFC 2923）への対処として、IP トンネルではなく L2-VPN により対外接続を確立した。しかし、基幹ネットワークでの利用を想定されていないソフトウェア VPN（OpenVPN）では、特定のフレーム長に対してフラグメント処理によりパケットロスが発生することがあった。運用中にこの問題の調査を行ったが、発生条件・再現性を特定することさえも困難であった。基幹ネットワークで安定した運用を行うには、利用条件がサポートされたハードウェアでの L2-VPN を用いるべきであるという知見が得られた。

対外線の冗長構成　フレッツ光ネクスト回線上に張った L2-VPN 経路での実測値で 20 Mbps 以上のスループットが確認できた。そのため、ポリシーベースルーティングを行わず、衛星回線をバックアップ回線として用いることにした。

ポリシーベースルーティングを行わないことにより、ダイナミックルーティングプロトコルを用いて対外線の冗長化および障害時の経路の自動切り替えを行うことができた。本合宿では、ダイナミックルーティングプロトコルとして OSPF を用いた。OSPF において衛星回線のコストをフレッツ回線上に張った VPN のコストよりも高く設定することにより、衛星回線をバックアップ経路として対外線の冗長化を図った。

合宿期間中の運用において、8 日（火）の午前 9 時頃から午前 10 時 30 分頃まで、イーサネットケーブルの断線のため、フレッツ回線が使用できなかった。この際に、経路の自動切り替えが発生し、衛星回線が使用されたことがわかる（図 2.3、2.4）。この代替経路への自動切り替えにより、利用者へ接続性を提供し続けることができた。

IPv6 移行に向けたトランスレータの導入　IPv6/IPv4 トランスレータ（FAITH、RFC 3142）を導入した。さらに、利用者の IPv6 を促すことを目的として、トランスレータを介さない IPv4 通信のセッ

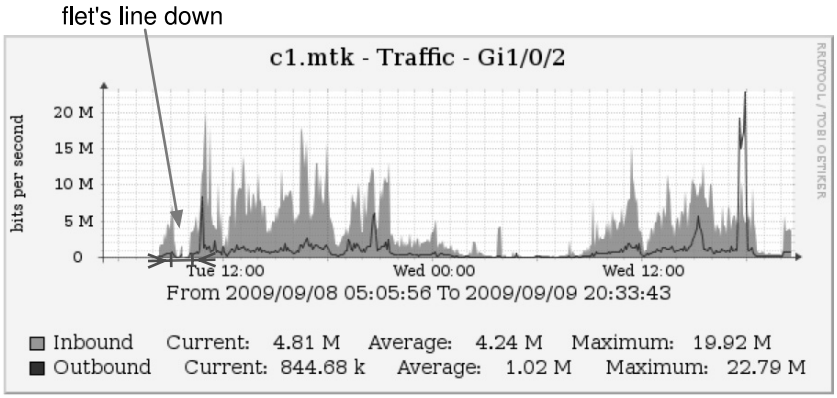


図 2.3.　フレッツ光ネクスト上に張った VPN 回線のトラフィック

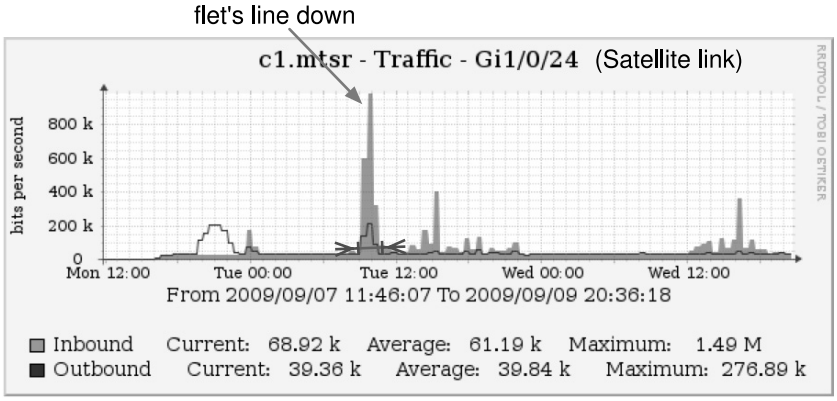


図 2.4.　衛星回線のトラフィック

表 2.2.　IPv6 トラフィックの割合（9 日（木）午前 9 時 45 分–午前 10 時 15 分）

計測対象ネットワーク	IPv6 トラフィックの割合
moho*[P1234B]*（トランスレータ無し）	5.72%
widecamp/widecamp-eap（トランスレータ有り）	44.8%

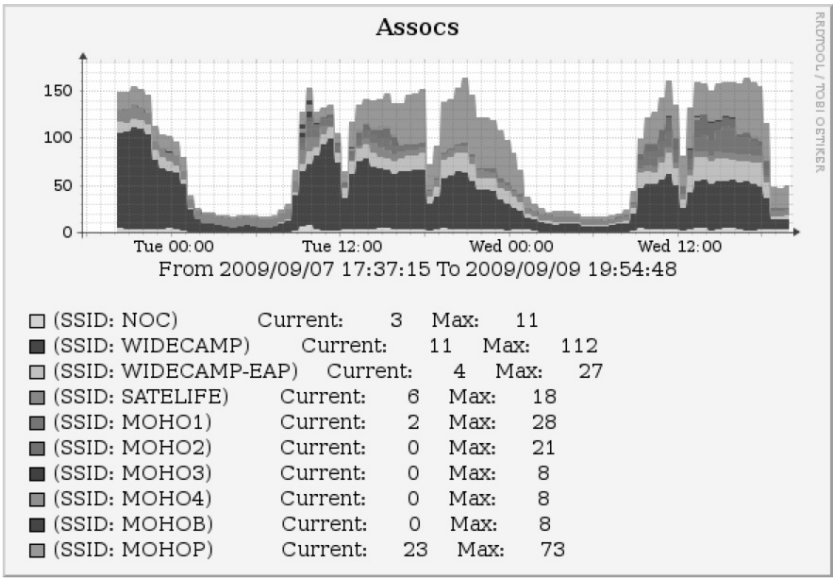


図 2.5.　SSID ごとの無線クライアント接続数の時間遷移

ション数を制限した。

トランスレータを導入することにより、利用者の IPv6 トラフィックの割合を大幅に増やす結果となった（表 2.2）。このことより、クライアントの IPv6 対応が進んでいる一方、サーバの IPv6 対応が進んでいないということが分かる。

トランスレータによりクライアントの IPv6 利用を促すことができたが、トランスレータを導入したことによって通信の透過性を犠牲にしたため、問題の切り分けが困難となってしまい、トラブルシューティングに時間を要する結果となってしまった。さらに、セッション数制限により意図した制限なのか、トラブルなのかを切り分けることが困難になり、結果的に利用者にとって不満を抱かせるネットワークを提供することになってしまった。

無線ネットワークの運用　ほぼ全ての合宿参加者の持参する端末が無線 LAN 対応となり、数年前の合宿より、合宿参加者へのネットワークは無線 LAN のみで提供されている。本合宿でも、合宿参加者に提供するインフラストラクチャとして無線 LAN を利用した。本合宿では、IEEE802.11a/b/g/n 対応のアクセスポイント 5 台および IEEE802.11a/b/g 対応のアクセスポイント 5 台を設置・運用した。本合宿期間中、最大 164 台の無線クライアントによる同時アクセスを記録した。SSID ごとの無線クライアント接続数の時間遷移を図 2.5 に示す。

2.2.3 反省

MTU 問題への対応として、ソフトウェアによる L2-VPN を利用したが、これによりさらに複雑な問題を生じることになってしまった。利用条件をサポートしたハードウェアでの L2-VPN をすることが望ましいという知見を得た。

また、今回の合宿では、IPv6/IPv4 トランスレータを実験ネットワークではなく、一般利用者の使用するネットワークに導入してしまったことにより、制限されたネットワークを提供することになってしまい、合宿参加者に不満を抱かせる結果となってしまったことは、大きな反省点である。さらに、IPv6/IPv4 トランスレータの説明不足により、利用者を混乱させてしまった。この経験を今後の IPv6 移行プロセスでの運用に活かしたい。

2.3 実験

2.3.1 WIDE 合宿におけるネットワークカメラを利用した研究参加支援システム

- 実験実施者：新 麗、二宮 恵、宮川 祥子

2.3.1.1 実験の概要

2009 年 WIDE 春合宿において、子供同伴で WIDE 合宿に参加し、夜の時間帯の会議に参加するための、仮想会議参加システムと仮想子供見守りシステムを設計・構築し、実証実験を行った。2009 年 WIDE 秋合宿でも同様のシステムを構築して運用を行うと共に、実際に流れたトラフィックを計測し、利用状況を観測した。

2.3.1.2 システム構成

2009 年 WIDE 秋合宿でも、仮想会議参加システムと仮想子供見守りシステムを構築した。仮想会議参加システムは、会議音声を聴講する携帯端末を Windows Mobile 端末から iPhone などに変更した他は同じシステムを構築した。仮想子供見守りシステムは、前回は 3 室だったのに対し 2 部屋になったこと、また部屋間ネットワークを PLC から無線 LAN に変更したことが春合宿とは異なる。ネットワーク構成図を図 2.6 に示す。

2.3.1.3 実証実験と計測結果

2009 年 WIDE 秋合宿において、本システムを稼働させ実証実験を行った。図 2.7 に 4 日間の各ネットワークカメラ上の Web サーバからのトラフィックの様子を示す。このグラフからどの時間帯にどのカメラの画像が閲覧されていたかが分かる。1 日目と 3 日目の深夜にカメラ A、B の画像が閲覧されており、それ以外は主に昼間にカメラ C の画像が閲覧されていた。カメラ C が置かれていた部屋は、昼間 3 人の子どものベビーシッター部屋となっていたため、カメラ C では昼間の子どもの様子を見ることができ、会議場にいる親が子どもの様子を確認するために閲覧していたことによりトラフィックが発生していたと思われる。

図 2.8 に各カメラからのメールの送信回数を示す。カメラからメールを送信する際は、通常 1 度の検知で複数のアカウント宛てにメールを送信しているが、本実験では、その送信先の一つに共通のメールアドレスを設定しておき、後で実験全体でのカメラからのメールの受信回数を確認出来るようにした。図 2.8 のグラフでは、この共通メールアカウント宛のメールの送信回数を時間軸に対して表示した。

各カメラのメール送信の状況を見てみると、カメラ A は主に夜間に利用されており、午前 0 時前後にカメラからメールが送信されている。カメラ B は、ほぼ全日カメラのメール送信機能を有効にしていたため、ハウスキーピング等も検知しており、頻繁に

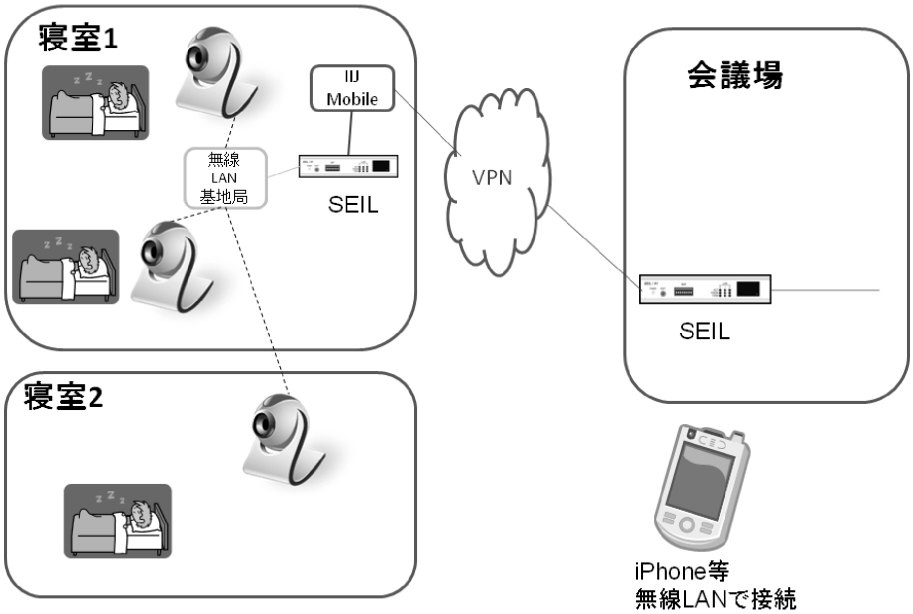


図 2.6. ネットワーク構成図

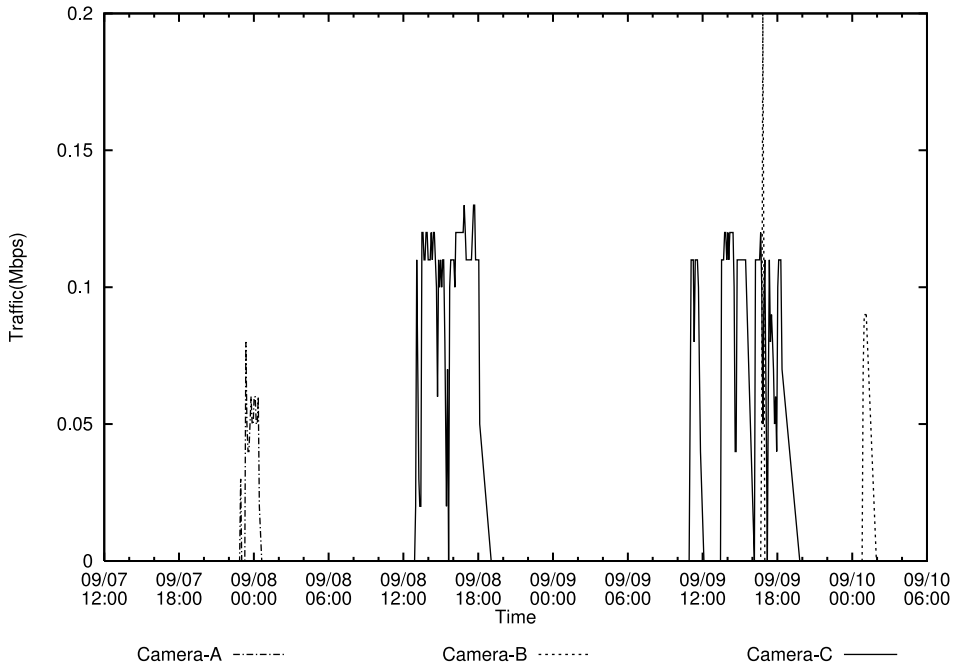


図 2.7.　各カメラの画像閲覧トラフィック

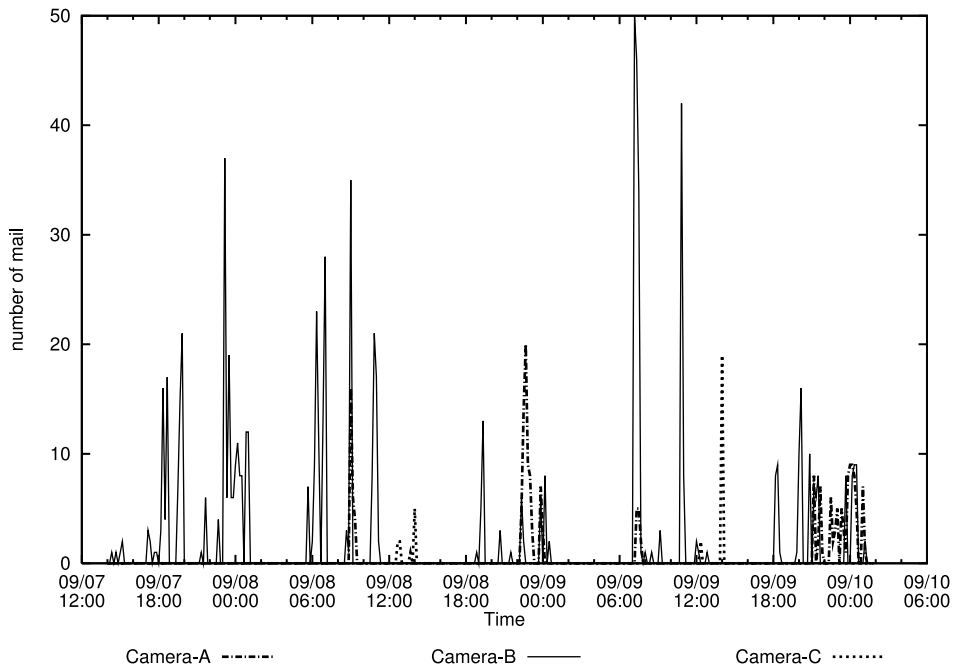


図 2.8.　各カメラのメール送信回数

カメラからメールが送信されていた。カメラ C の設置されていた部屋は前述の通り昼間はシッター部屋であったため、子どもが在室している間（シッティング中）は送信回数が頻繁になってしまうため、カメラからのメール送信の設定は行われていなかった。午後にカメラ C からメールが送信されているのは、子どもが外出先から帰ってきたことを検知してメールが送られたと考えられる。

2.3.1.4 まとめと今後の課題

ネットワーク構成に関しては、PLC から無線 LAN に切り替えたことで設置時間が短縮された。ただし、

事前準備としてはPLCは親機子機の認識を1度行えばよいのに対し、無線LANはアドレスや暗号設定などの設定が必要になる。

稼働中のトラフィックについては最大で0.25 Mbpsであり、モバイルサービスでも十分対応できる流量である。ただし、トラフィックはカメラの台数に比例するため、見守る対象が増える場合にはシステムを再設計する必要がある。

本システムは、子供同伴でWIDE研究会合宿に参加し、研究活動を行うには必須になりつつあり、構築および実験を継続する必要がある。ただし、子供は年齢に応じて活動の様子が変わるため、システムの要求条件も変化してきており、設計を見直す必要があると考えられる。

また、今回はトラフィック計測により、システムのひとつの側面での客観的な観測を行った。使用するネットワーク帯域と利用時間帯などの使い方についてはデータを取得でき、今後システムの再設計や応用の際には有効と思われる。他の視点でのシステム評価についてはまだ課題があり、構築、機能についての評価は十分とは言い難い。またこのシステムを構築したことで、他の参加者にメリットがあるかどうかについては、別途アンケートなどで意見収集をする必要がある。

2.3.2 模倣インターネット環境の実インターネット環境への統合実験

ネットワークエミュレーションテストベッドでの実験手法の確立や、各種の仮想化技術の革新によって、実インターネットに規模的にも機能的にも近い環境がテストベッド上で簡単に構築できるようになりつつある。このような模倣インターネット環境構築技術の発展を前提に、模倣インターネット環境と実インターネット環境の結合を想定すると、さまざまな運用上、セキュリティ上の問題が存在すると考えられる。そこで、本実験では合宿ネットワーク内に模倣eBGPトポロジを構築し、ネットワークの安定運用に必要な知見の洗い出しを行った。

2.3.2.1 実験の背景と目的

我々は、これまで、実機（物理ノード）によるネットワーク実験環境での実験手法[68, 92]や仮想化技術を用いたネットワーク実験環境の研究開発を行ってきた。また、インターネット実証実験の代わりに利用できる実験環境を目指して、インターネットを模倣した環境をネットワーク実験環境上に構築する技術[39, 40, 133]についても、研究開発を行っている。これらの模倣インターネット環境構築技術の進展により、模倣インターネット環境はすでにいくつかの実験で利用されており、模倣インターネット環境を実験に利用する場合や、模倣インターネット環境を実インターネットと結合する場合の運用上、セキュリティ上の問題を明らかにすることが求められている。模倣インターネット環境を実際に運用されているネットワークに結合する実験は、昨年2008年秋の合宿から始まっている。模倣インターネットの性能の評価と、運用上やセキュリティ上の問題を明らかにすることを目的として行われた前回の実験では、模倣網に1つの入り口と出口を設け、1つの模倣BGP経路についてその安定性を確認した。しかし、模倣網の上流がボトルネックとなっていたので、十分な確認がとれない結果となった。また、安定性の確認とは別に、実BGP網との類似性を確認しておくことにより、模倣網の挙動から実ネットワークでの影響について類推することが可能となる。

2.3.2.2 実験環境

本実験では、合宿ネットワーク内のIPv4網のほぼ全てを模倣インターネット網を構築し、実験を行った。

合宿ネットワークの参加者向けのIPv4の無線LAN（プレナリ部屋、BoF部屋×4、ボード部屋）とNOCネットワークとの間に、構築した模倣インターネット網を挟み込む形で構成した。これにより、合宿参加者がこの無線LANを用いて合宿ネットワークより外のインターネットなどと通信する場合には、模倣インターネット網を経由することになる。前回の実験では模倣網の入り口と出口を1つずつ用意したが、今回は、複数の入り口を設け、1つの出口に向けて複数の経路を用いる構成となっている。今回の実験には、デモ用の機器セットである「StarPOD（StarBED of Portable operation Domain：可搬型StarBED）」を用いた。StarPODとは、StarBEDのデモに欠かせない複数のノードとスイッチを小型ラックに構成したまま持ち運び可能としたもので、今回の実験のように、実験装置を持ち込む場合に有用である。

今回の実験の構成は、以下の通り。

- 実際に模倣インターネット網を構築するMohou Slave Server（6台）
- 模倣インターネット網を管理するためのMohou Master Server

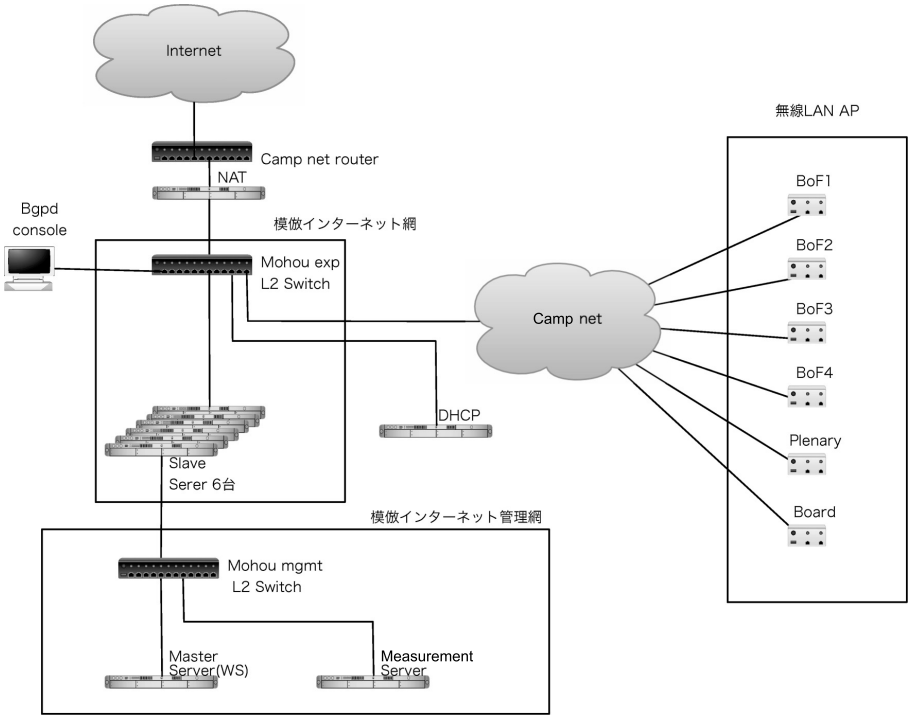


図 2.9.　模倣インターネット網と合宿ネットワークとの物理接続図

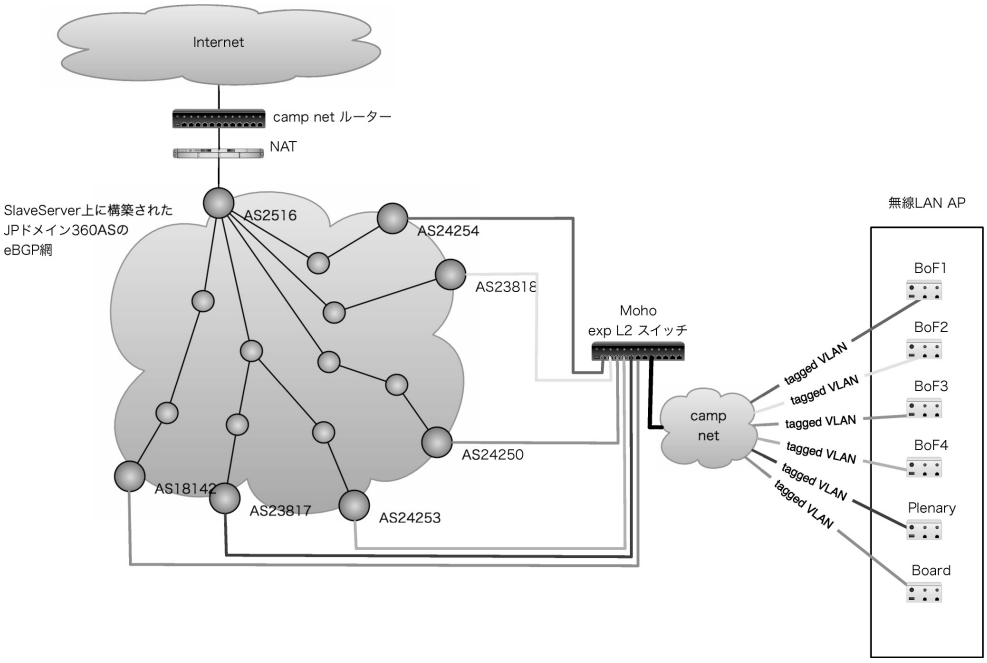


図 2.10.　模倣インターネット網と合宿ネットワークとの Layer 2 接続図

- 模倣インターネット網を観測するための Mohou Measurement Server
- 模倣インターネット網を監視および状態の閲覧をするための Mohou bgpd Console
- NOC ネットワークと接続するための Mohou NAT
- 無線 LAN、MohouNAT と接続するための exp L2 Switch
- これらをつなぐ mgmt L2 Switch

物理接続を図 2.9 に示す。Layer 2 の接続を図 2.10

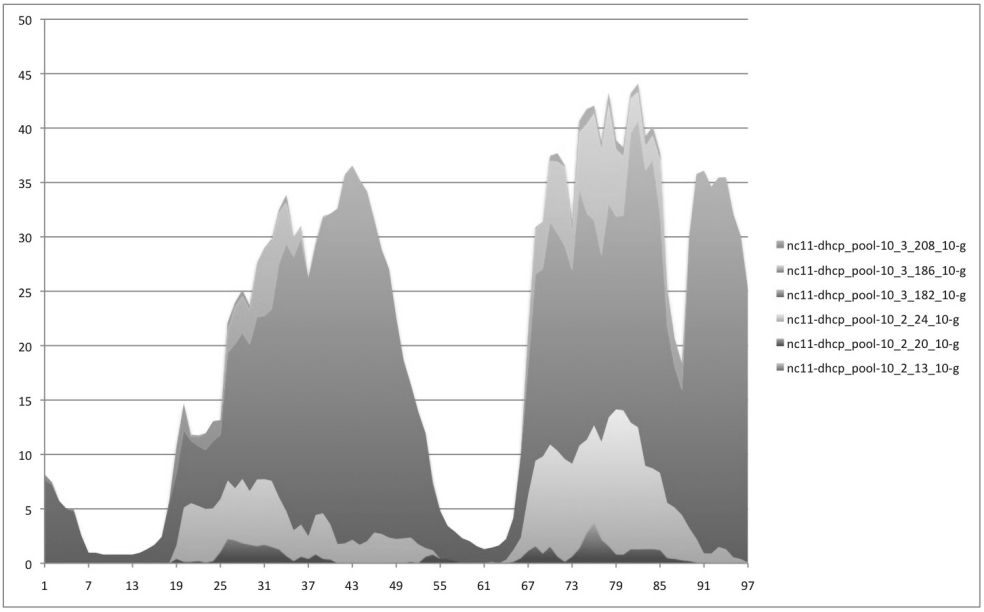


図 2.11. 模倣インターネット網の DHCP アドレスリース状況（3 日間）

に示す。

今回用いた模倣インターネット網は、実際のインターネットの観測データに基づく AS 間ネットワーク（eBGP トポロジ）を模倣した模倣 eBGP トポロジである。CAIDA AS Ranking プロジェクト [24] で公開している AS の接続関係を推定したデータセット（以降、AS 接続関係データセット [18]）の 2009 年 7 月 1 日時点のデータのうち、JPNIC の 2009 年 8 月 14 日時点の AS 一覧に記載されていて、接続関係がある 360 AS を、AS 接続関係データセットの接続関係に基づいて模倣した。図 2.10 にあるように、複数の無線 AP と、NOC ネットワークへの出口をそれぞれ別の AS に接続した。前節に示した実験環境を用いて実験を行った。

下記の実験を行う予定であった。

1. 模倣インターネット網上の複数の経路を利用した場合の性能
2. 模倣インターネット網の構成を変更した場合の収束までの状態
3. 模倣インターネット網を利用した別実験の実行

前回の実験では、NOC ネットワークから WIDE バックボーンへの接続点が不安定であったため、1 について再び確認した。3 については、別実験の主催者の都合により実験しなかった。

模倣インターネット網上の経路を利用した場合の性能については、模倣インターネットを構成する各機器の状態の確認と、模倣網そのものの状態の確認を行った。各機器の状態については、Mohou Measurement Server 上に監視ツール munin を用いた模倣網の状態監視については、フルメッシュ ping で常に到達性の確認を行った。

構成を変更した場合の収束までの状態は、traceroute や ping を用いて状態確認を行った。

ネットワークの利用状況としては DHCP による IP アドレスのリース状況から判断した。図 2.11 は合宿中の DHCP による IP アドレスのリース状況である。初日は宣伝不足などの影響で少なかったものの、2 日〜3 日は 30〜40 名の利用であった。

実験構成ノードの状況については、NOC 側のエッジ AS を保有しているノード nc1 について確認する。CPU 稼働状況（図 2.12）、メモリ稼働状況（図 2.13）、インターフェースのパケット転送レート（図 2.14）を図示する。CPU の処理状況には余裕があり、メモリの利用状況も良好である。転送レートのグラフでは、負荷試験時のピークを除けば、問題はないといって良い。模倣網の確認では、全 AS ルーターへの到達性をラウンドロビンで確認した。期間中 11633 回のフルメッシュ ping 確認を行ったうち、全 AS が接続していた期間は 10%の 1263 回であった。安定稼働までの作業時間帯を考慮する事により、結果の向上が見込まれる。模倣網内の全 AS を横軸に配置し、各 AS の故障回数の様子を図 2.15 に示す。

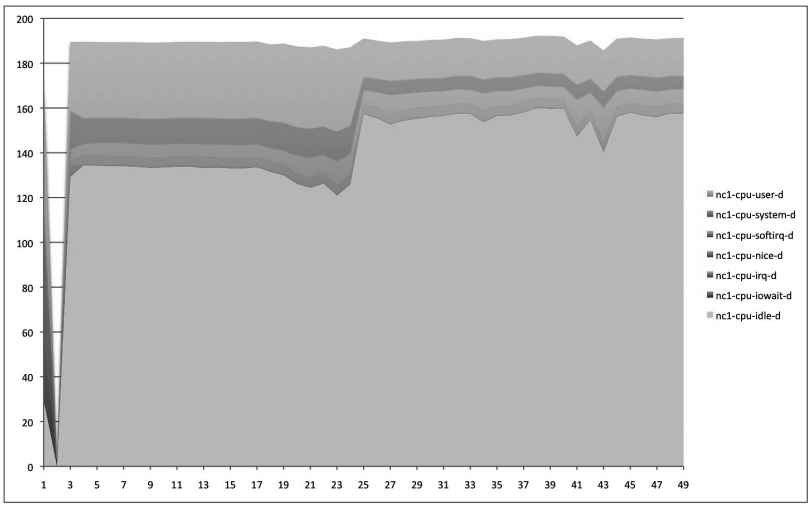


図 2.12.　nc1 の CPU 稼働状況（2 日間）

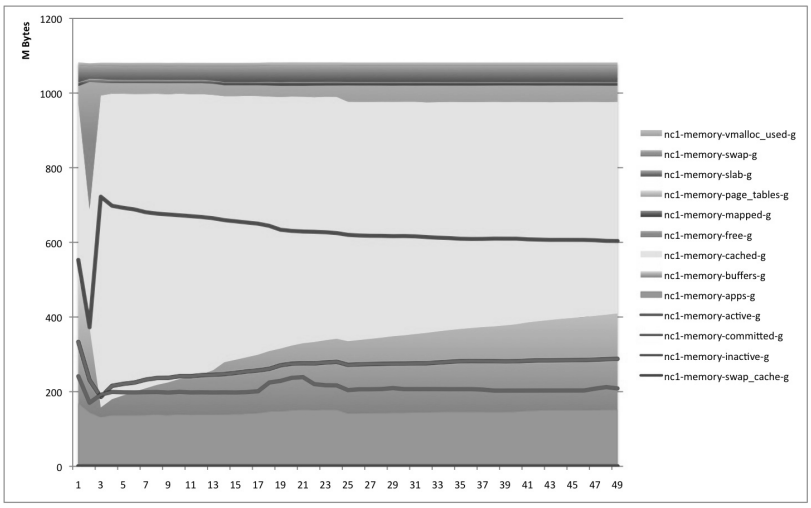


図 2.13.　nc1 のメモリ使用状況（2 日間）

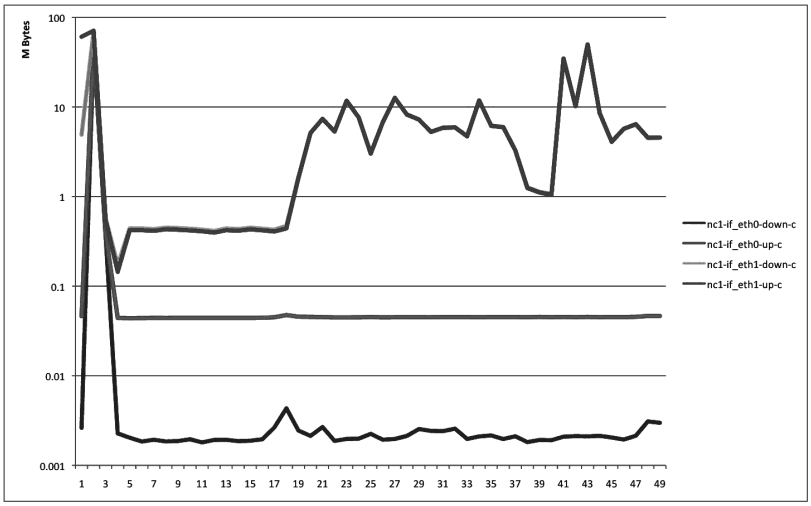


図 2.14.　nc1 のインターフェースのパケット状況（2 日間）

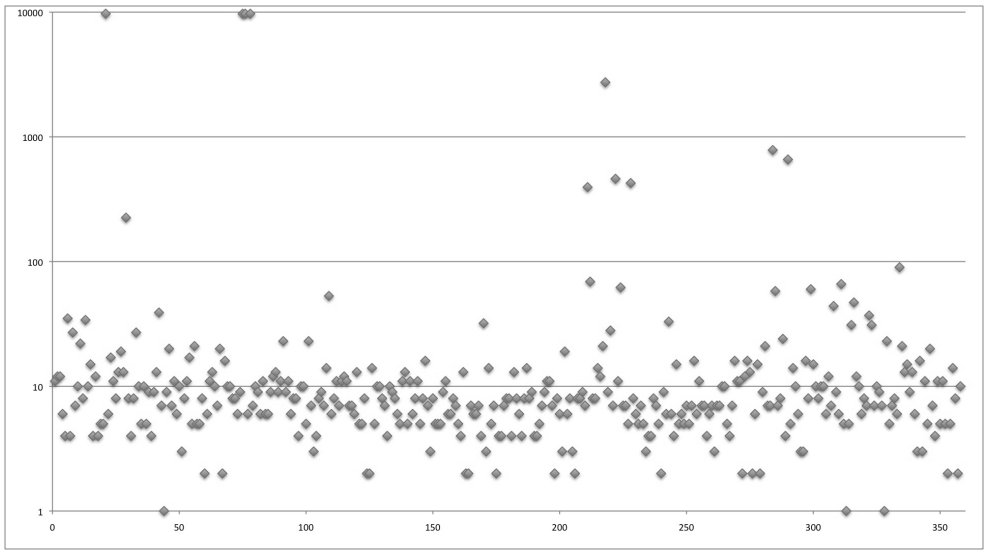


図 2.15. 全 AS の到達性チェック（3 日間）

無線 AP から Internet までの 1 部 BGP 経路を切断/復旧させ、接続状況の確認を行った。代替経路への切替えと、障害経路復旧による経路の復元は予定どおりの動作となった。

2.3.2.3 評価と課題

実験の 3 日間を通して、模倣インターネット網は安定していた。6 箇所の無線 LAN のうち、設定ミスにより 1 箇所が不安定だったものの、他の接続性は良好であった。実験構成機器の監視では、メモリ、CPU、インターフェースは良好であった。ただし、メモリについては XenDom0 の分であり、また、インターフェースも全体的な話であったため、DomU 単位での詳細な情報を得られる工夫が必要である。今後は、今回実施できなかった他実験の模倣網上での実施や、AS 内のネットワークの模倣についても検討したい。

2.3.3 パケットヘッダ情報を用いた仮想ユーザ識別システムの検討

- 実験実施者：上原 雄貴

2.3.3.1 概要

情報技術の発展に伴い、一人のユーザが複数台のホストを所有する場合や、単一のホストを複数人で使用するなど、ユーザの利用形態は多岐に渡る。しかし、ユーザの行動や興味動向の調査を行う際、前述したユーザが識別できず、ネットワークによってユーザ識別に利用できる情報が違うため、ユーザを基準としたネットワークの実態調査が困難である。そこで、様々なネットワークでもユーザ識別が可能とするために、パケットのヘッダ情報のみを用いてユーザを識別するシステムを提案した。

2009 年度秋合宿においては、本提案手法の前段階として、パケットヘッダ情報のみでホスト識別が可能かの検証を目的とし、筆者の所属する研究室 7 人のホストを一意に識別できるかどうかの実験を行った。また、パケット情報取得にあたりユーザの同意を得て、WIDE 合宿で無線 LAN を利用したホスト全てのトラフィックを取得した。

2.3.3.2 本システム設計

本システムは、大きく 3 つの動作に分けられる。IP アドレスからホストを判定する **IP 判定モジュール**、ホスト上のアプリケーションの動作からホストを分類する**パターン解析モジュール**、ホストの振る舞いを統計解析する**統計解析モジュール**の 3 つである。

本システムの設計を図 2.16 で示す。

1. **IP アドレス判定モジュール**

   IP アドレス判定モジュールは、パケットの IP アドレスを基に、ホストを推定する。ネットワークの DHCP リースタイム時間内に、該当する IP アドレスはすべて同じホストであると判断する。しかし、DHCP のリースタイム時間内に該当する IP アドレスから通信がなかった場合は、そのホストはネットワークから離れたものとする。

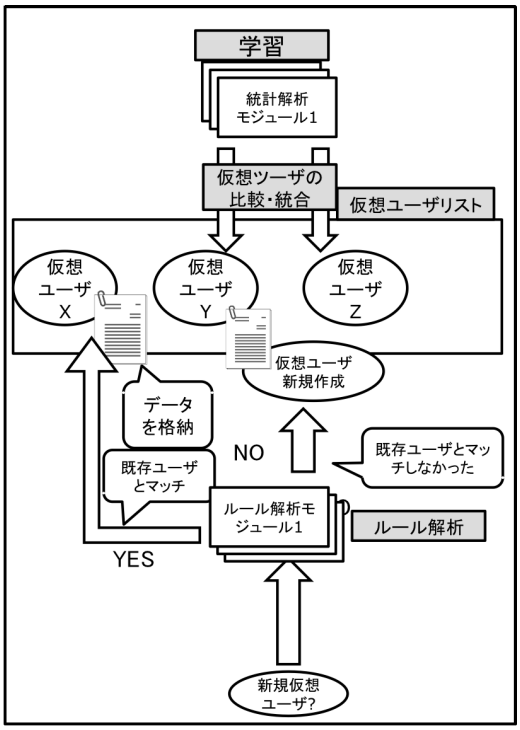


図 2.16.　ホストの識別モデル

2. **パターン解析モジュール**

ホスト上のアプリケーションの動作からホストを分類する。このモジュールは状況に応じて複数個作成する。また各モジュールごとにパターンを解析するアルゴリズムは変化する。例えば、メールサーバにアクセスする頻度や回数をホストを分類するための識別子とする。

3. **統計解析モジュール**

このモジュールは、ホストの振る舞いをベースに統計解析を行い、類似するホストを探す役割を持つ。例えば、ネットワークの接続時間、生活時間と接続先サーバなどの傾向から、関連性を見つけ出し、類似するホストを発見する。このモジュールもパターン解析モジュールと同様に、用途に応じて複数作成する。

各モジュールで類似するホストを発見した場合、ホストが保有する情報は該当するホストの情報に統合される。そして、これらのモジュールによって新規ホストが既存のホストとマッチしなかった場合にはじめて、新たなホストが作成される。これら一覧の作業を繰り返すことによって、ホストを識別する。

識別子として利用した情報はパケットヘッダ情報、起動時間・接続頻度、接続位置、ユーザが利用するサービス、OS の種類 PC 起動時の挙動（スタートアップ、NetBIOS、ソフトウェアアップデート）である。

2.3.3.3 実験結果と考察

2009 年 WIDE 秋合宿において、本システムの実証実験を行った。WIDE 合宿期間中に無線 LAN を利用した 264 台のホストを観測し、ターゲットとなった 7 台のホストのうち 4 台を一意に識別することができた。

まず、264 台のホストから ssh プロトコルを利用しているホストの宛先 IP アドレスと利用頻度を識別子としてグループを分類した。次に smtp、imap、pop プロトコルを利用するホストが接続する mail サーバと利用頻度を元に更に詳細なグループの分類をした。

これによって 246 台のホスト集合群から 12 台までグループを分類することが可能となった。そのグループ内において、p0f による特有ポートの利用状況観測から OS を特定することで、ターゲットとするホスト 4 台の識別ができた。しかし、ほか 3 名の一意の識別ができない、もしくは誤判定をしてしまう結果となった。

識別ができなかったケースを解析した結果、大きく二つの問題が挙げられた。まず、ホストが、twitter や Gmail のように複数のサーバが分散設置されているサービスを利用するケースがある。これによって、同じサービスを利用しているにも関わらず、別のサービスを利用していると誤判定されてしまう。次に、ホストが数分間のみネットワークに接続し、十分なデータを取ることができずにネットワークから離れたケースである。本システムの識別手法はホストの振る舞いによって結果が変化する可能性があるため、短時間しかデータが取得できなかった場合に別のホストとして誤判定してしまう。他にも、ユーザが普段と異なる挙動をした場合、他のホストと誤認識されてしまうという問題点が判明した。

今後の課題としては、より高精度な識別子や統計指標の確立をする必要がある。そのため、同一ホストと判断する識別子の重み付けをすることによって、似たような挙動のホストをより細かく識別できるようすることや、DNS との連動やサーバを分散しているサービスのアドレスブロックの把握することで、同一なサービスをホストが受けていても判断可能であるように設計する必要がある。

2.3.3.4 まとめ

本稿ではパケットのヘッダ情報のみを用いて、ホストを識別するシステムを実装し、実験を行った。合宿参加者の同意を得て、本システムをネットワークの中継地点に設置し、定常的にヘッダ情報を収集した。実験は WIDE 合宿のネットワーク上でターゲット 7 台のホストを識別出来るかを検証し、7 人中 4 人のホストを識別できるという結果となった。今後の課題として、ホスト識別に利用する情報や情報の組み合わせ手法の議論、サーバを分散しているサービスの判断や、短時間しかネットワークに参加しなかったホストの判別基準の設定などの問題を踏まえて、システムの再設計をする必要がある。

2.3.4 フリーの監視ツールを用いたネットワーク監視

- 実験実施者：紅林輝（名古屋大学）

2.3.4.1 概要

ネットワークを通じて安定したサービスを提供するには、サーバやネットワーク機器の安定運用が必須である。ネットワーク管理において、障害をいち早く検知し、管理者に通知する監視ツールの役割は重要である。

今回、GroundWorkMonitor というフリーの監視ツールを使い、合宿のネットワークの監視を実験枠で行ったので、報告する。

2.3.4.2 GroundWorkMonitor

GroundWorkMonitor は、米国の GroundWork Monitor Opens Source 社が提供する NAGIOS ベースの統合監視ソフトウェアである。MySQL、RRDtool、Cactai 等の OSS を統合し、このソフトウェアで一元的に管理ができるよう、設計されている。全ての設定を Web ベースで行うことが可能である。

2.3.4.3 監視

合宿ネットワークを構成する計 32 のネットワーク機器及びサーバ類の監視を行った。監視は基本的に ping による死活監視を行った。監視対象がダウンしていた場合、アラートメールによる通知を行った。

2.3.4.4 結果と反省

合宿の 1 日目から最終日まで、上述の監視を行った。基本的には合宿期間中、システムを稼働させ続けて、監視を行うことができた。また、監視対象機器がダウンした際には、アラートメールが発信され、合宿ネットワーク管理係から「助かった」という言葉を頂いたこともあった。

しかし、ping 応答しない機器や、GroundWorkMonitor に対する設定ミス等により、余計なアラートメールを大量に送ってしまうこともあり、結果として、あまり信用されない通知機能となってしまった。

今回、不注意と現場での検証不足のために、このようなことが起こってしまった。したがって、必要最低限のテストと調整を行った上で、監視ツールを稼働させる必要があった。

2.3.5 E ブルーシートとプレゼンテーター表示システムを使った合宿（会議）支援システム

- 実験実施者：井上博之、重近範行

2.3.5.1 概要

合宿（会議）の参加者を支援するためのシステムで、今回の WIDE 合宿にてプロトタイプの実証実験を行い、完成したシステムを 11 月に開催される第 76 回 IETF 広島会議にて展開した。

1. 参加証（名札）に装着した RFID や非接触 IC カードを使用して参加者識別を行う。
2. IETF Meeting で使用されているブルーシート（参加者の名前とメールアドレスを記入する紙）の代わりに、E ブルーシートという RFID リーダ付きの端末を回覧することにより、リアルタイムに参加者を集計し、また BOF 部屋の外からも参加者情報を知ることができる。
3. BOF などで発言している人のプロフィール（自分で登録したもの）を表示する。BOF 部屋の外からも誰が発言中かをリアルタイムで知ることができる。参加者の識別は、マイクの傍に装着した RFID リーダ端末に、参加証の RFID タグを読ませることによって行う。

2.3.5.2 実験機材と構成

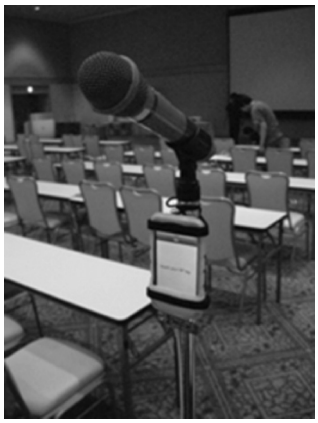
RFID タグとしては、13.56 MHz 帯を使用するものを使用し、タグリーダを読み取り用端末に接続し、読み取り端末がサーバとネットワーク経由で通信を行う。読み取り端末としては、無線 LAN が使用でき、バッテリー駆動ができるものとして、今回は Apple 社の iPod Touch に USB 経由の RFID リーダユニッ

(1) E ブルーシート端末と RFID タグ

(2) 参加者による出席記録の様子

図 2.17.　E ブルーシート

(1) RFID 端末



(2) 発言者表示用にマイクへ取り付けたもの

(3) 発言者表示用 PC とプロジェクタ

図 2.18.　発言者表示システム

トを接続したもの（以下、RFID 端末）を使用した。RFID 端末とその外観を図 2.17 および図 2.18 に示す。

合宿では、発言者表示システムを実際に Plenary の部屋に配置し、E ブルーシートをいくつかのセッションで回覧し出席者情報を収集した。発言者表示システムの機器レイアウトを図 2.19 に示す。ネットワークとしては、RFID 端末およびそのサーバのために専用のセグメントを用意し、無線 LAN の ID なども一般とは別に用意し、合宿全体のトラフィックが RFID 関係の機器の動作に影響を及ぼさないようにした。

2.3.5.3 実験結果

発言者表示システムの基本動作は問題なく、RFID の読み取りの不具合やシステムのトラブルもなかった。表 2.3 に示すとおり、合宿全体として 192 名が発言者表示システムを利用し、9 つの Plenary セッションで利用された。E ブルーシートは 6 つのセッションで使用し、各セッションに出席している参加者の ID をスムーズに読み取ることができた。今回、合宿で動作させて合宿アンケートで改善点などを収集したところ、ユーザインタフェースに対して色々な改善意見が出され、それらに対応し IETF 会議に臨むようにした。

合宿に適用したことで問題が明確になり、ユーザインタフェースで大きく変更した点がいくつかある。発言者表示で最後に発言した人のプロフィールが出たままになるため、表示を消すための専用 RFID タグ（ワイプアウトカードと呼ぶ）を用意してマイクの横に置くことで、明示的に発言者表示を消すこと

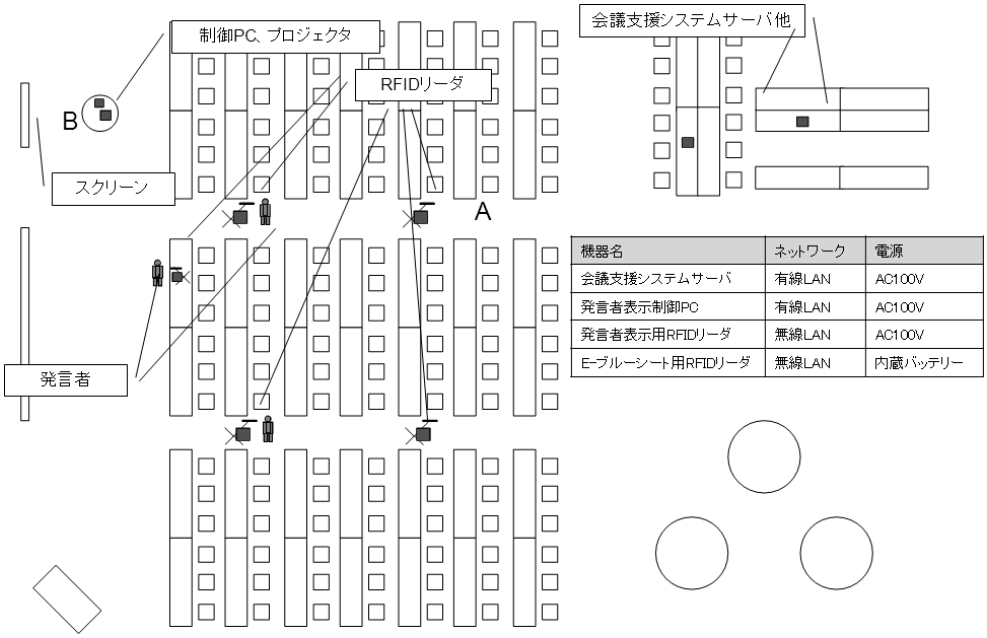


図 2.19. 機器レイアウト

表 2.3. 発言者表示の統計情報

会議参加者統計情報（全体）

会議名称	WIDE CAMP
Registants	192
実験実施セッション数	9
延べ参加者数	448

会議参加者統計情報（セッション毎）

種別	セッション名称	開催日時	E-ブルーシート	発言者表示
Plenary	IETF Hiroshima conference supprtsystem	2009/09/07 19:20–2009/09/07 19:50	—	23
Plenary	Medical plenary II: Crisis in Japanese	2009/09/08 16:00–2009/09/08 18:00	93	10
Plenary	Board plenary II	2009/09/08 19:00–2009/09/08 21:00	110	42
Plenary	Yataimura I	2009/09/08 21:00–2009/09/08 22:00	5	—
Plenary	Research presentation II	2009/09/09 20:00–2009/09/09 21:00	107	9
Plenary	Yataimura II	2009/09/09 21:00–2009/09/09 22:00	—	9
Plenary	Medical plenary wrapup	2009/09/10 09:00–2009/09/10 09:15	67	—
Plenary	Ice break wrapup	2009/09/10 09:15–2009/09/10 10:15	—	7
Plenary	net-PC and experiment groups activity report	2009/09/10 10:30–2009/09/10 11:10	66	18
合計			448	118

ができるようにした。プライバシー保護の観点から、表示内容を参加者自身が編集できる機能が必要という意見が多く出され、初期状態では登録された参加者の情報は最小限とし、編集用の Web インタフェースから参加者自身でプロフィールを登録してもらうことにした。また、E ブルーシート端末は、バッテリーによる駆動時間をもっと長くとる必要があり、余り小型にしないほうが扱いやすいことがわかったので、IETF では予備バッテリーと一体化した透明ケースに入れるようにした。

2.4 まとめ

2009 年 9 月 7 日（月）から 10 日（木）にかけて、開催された WIDE 合宿におけるネットワークと各実験の報告を行った。合宿プログラム委員会から編成したネットワーク構築・運用チームは大規模実験テストベットとなるネットワークを構築した。ネットワーク構築・運用チームはこのネットワーク構築から様々な知見を得た。IPv6 トランスレータ運用では、利用者に対する説明不足も原因となり、利用者に不満を頂かせてしまったことは残念である。しかし、同時に、IPv6 トランスレータの運用において、アドレスファミリの変換によって発生する問題の切り分けの難しさを経験した。この経験を今後の IPv6 への移行に向けたネットワーク運用に活かしたい。

また、本合宿中に以下の 5 件の実験が行われた。

- WIDE 合宿におけるネットワークカメラを利用した研究参加支援システム
- 「模倣インターネット環境と実インターネットワークの統合実験」～最後は模倣 harm～
- パケットヘッダ情報を用いた仮想識別システムの検討
- フリーの監視ツールを用いたネットワーク監視
- E ブルーシートとプレゼンテーター表示システムを使った合宿（会議）支援システム

各実験の詳細については、第 2.3 節にまとめた。