第XXI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 21 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　2002 年秋合宿実験ネットワーク

本章では、2002 年 9 月 9 日 (月) から 12 日 (木) まで山梨県八ヶ岳ロイヤルホテルにおいて開催された WIDE プロジェクト秋合宿 (以降、本合宿) におけるネットワーク構成および、そのネットワーク上で行われた実験結果を報告する。

1.1 ネットワーク構成

図 1.1 に本合宿のネットワーク構成を示す。

図中、左右の点線より上部が慶應義塾大学湘南藤沢キャンパス (SFC)、下部が合宿地である。四角はルータまたはホスト (サーバ) を表し、線はイーサネット、専用線あるいは無線 LAN を表す。二点鎖点は衛星回線を表現する。

合宿会場とインターネット (SFC) との接続には地上線として HSD 128 kbps 4 本多重回線 (512 kbps) および衛星回線 (上り 512 kbps、下り 1.5 Mbps) を用いた。図左上の INS 回線 (128 kbps) は設営時や障害時のバックアップ回線である。

衛星回線には HTTP および FTP をプロキシサーバ (proxy) 経由で流し、地上線にはそれ以外のトラフィックを nat 経由で流す予定であった。しかし、地上線の帯域がこれまでの合宿より比較的小さかったため、帯域を使いきってしまい、途中から衛星回線にも HTTP, FTP 以外のトラフィックを流すように経路を変更した。

合宿会場では無線 LAN と有線の LAN をそれぞれ 6 サブネット設営した (Cable-BOF1, ..., Cable-Lobby2, Wireless-BOF1, ..., Wireless-Lobby)。各サブネットは 1 台のルータ (router0) および会場での各種サービス (http, ftp, 等) を提供するサーバ (hatchan) に接続した。

無線 LAN は、この後で述べる 1.3、1.4 の実験のため、別々のサブネットとした。

1.2 合宿ネットワークを利用した実験項目

本合宿では以下に挙げる 6 つの実験が行われた。

1. ユーザ/計算機の地理的位置情報提供実験
2. Mobile IPv6 Return Routability 実証実験
3. network music
4. moCA WG による PKI エクセサイズ
5. PAFFI による IP Traceback(パケット経路判別) 実験
6. SNMP による Hash-based trace back 技術実装実験

以下では各実験について報告する。

1.3 ユーザ/計算機の地理的位置情報提供実験

実験責任者: 羽田 久一

所属: 奈良先端科学技術大学院大学

1.3.1 目的

本実験の目的は、位置情報の焦点をあて、人やもの (ノート PC) の位置情報を取得すること、および、位置情報などを扱うためのプラットフォームを提供し、モデルを含めたその評価を行うことである。加えて、本実験を通して、合宿における参加者の activity などを可視化できるように測定し、今後の合宿に役立てることも目的とする。

1.3.2 概要

合宿では、個人ごとに情報を集中管理するモデルである、Personal Server Model に基づき、そのプラットフォームを構築した。

実空間から取得する情報として RF-ID[18] による人の位置情報、位置からの情報検索、移動透過性を提供するプロトコルである LIN6[94] を利用したノート PC の位置情報、Personal Server IP アドレスの取得、ポットの温度情報を取得した。これらの情報を web インタフェースを用いて提供した。

位置情報を利用するために、プラットフォームへのプロトコル定義および、C 言語用ライブラリ策定・公開した。このライブラリを利用することにより、実空間における情報を利用するアプリケーションの開

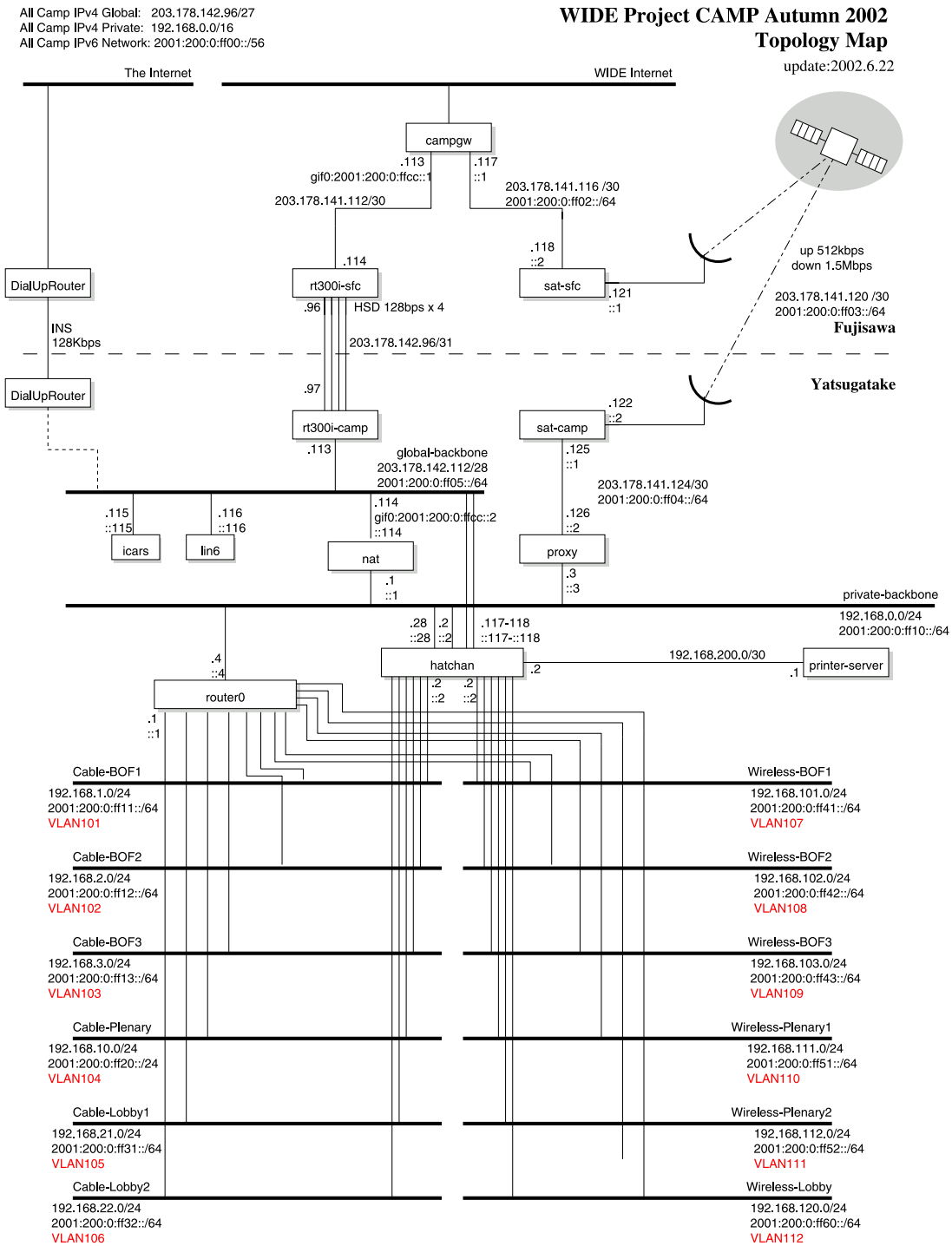


図 1.1.　ネットワーク構成

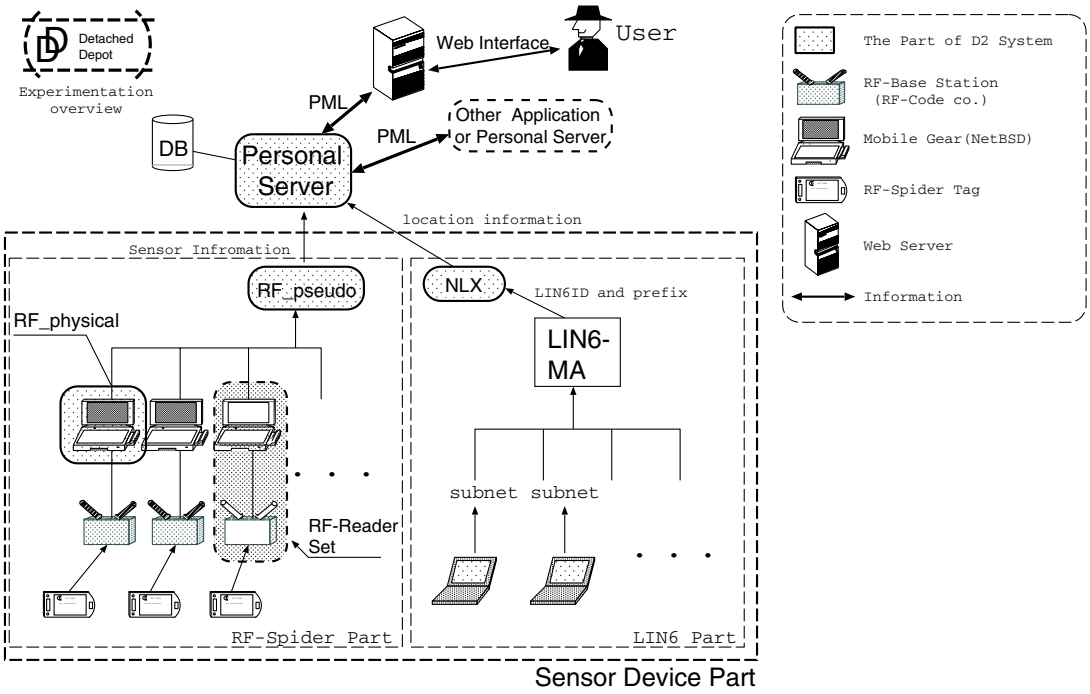


図 1.2. 全体構成概要

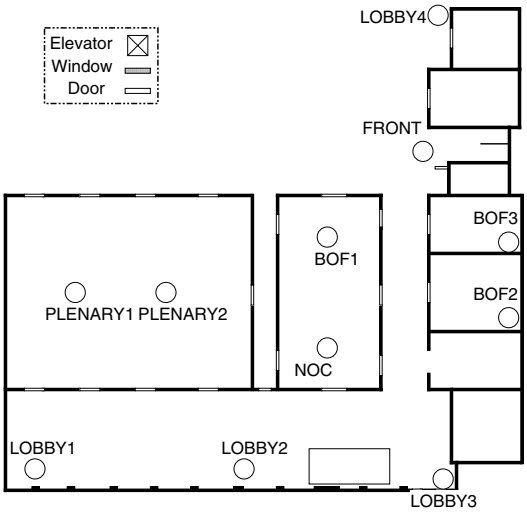


図 1.3. ホテル全体図

発を容易に行うことができる。

図 1.2 に実験での全体概要を示す。下部に位置する多数のセンサデバイスから、Personal Server にセンサ情報を送信している。ユーザは、web インタフェースを通じて Personal Server にアクセスする。

図 1.3 に、実証実験が行われたホテルの地図を示す。“BOF1” のように、部屋ごとに位置情報のラベルをつけた。実験参加者の位置情報は、このラベルを利用して表現される。このラベル設定は手動で行った。図中の白丸は、後述する RF-Spider の基地局を設置した場所を示している。

また、後述する LIN6 での場所検知のために、各部屋ごとにセグメントを分け、ノート PC の IP アドレスが部屋を示すようになっている。

続いて、使用したセンサについて述べる。

RF-Spider

本実験では人の位置を検出するためのシステムとして RF-Code[132] 社の Spider(RF-Spider) を利用した。

各参加者に RF-Spider 付属の RF-ID タグを携帯してもらった。この RF-ID タグは電池を内蔵した無線タグであり、それぞれが固有の ID をもち、その ID を電波として発信している。この電波を RF-Spider の基地局が補足することにより、参加者がその基地局の検出範囲内にいることを検知する。

LIN6

本実験ではノート PC の位置を検出するためのシステムとして、LIN6 を拡張したシステムを用いた。LIN6 では、各ホストに対して、LIN6ID という一意の ID が割り振られる。LIN6 では、ホストに prefix が割り当てられると、LIN6ID と prefix が合成され、IP アドレスが自動的に生成される。この IP アドレスを、Mapping Agent(MA) に登

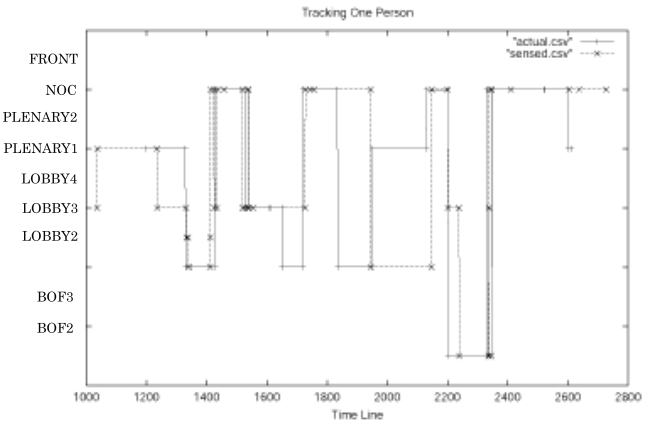


図 1.4.　実際の移動履歴と検知された移動履歴

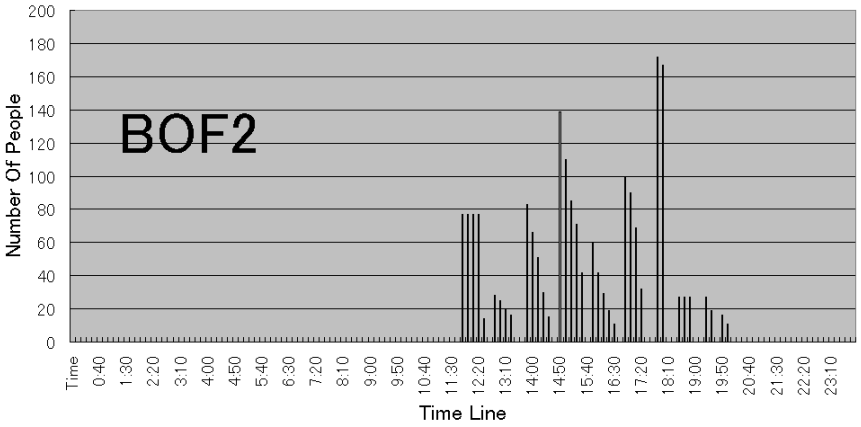


図 1.5.　BOF2 における時間軸と人数とのグラフ

録することにより、位置透過性を実現する。

参加者がノート PC を各部屋のネットワークに接続すると、IP アドレスが自動生成される。この IP アドレスが LIN6ID とともに MA に送られる。IP アドレスを受け取った MA は NLX(Network Location eXchanger) と呼ばれるデーモンに IP アドレスおよび LIN6ID を送信する。本実験では各部屋ごとに異なる prefix を持つネットワークが構築されているため、この prefix およびネットワークを把握することでノート PC の地理的位置を知ることが可能である。

ポット

電気ポットの温度を取得するセンサノードを利用した。このセンサノードは、H8/306F(20 MHz) 上に microITRON4.0 の API に基づき実装された。また、IPv6 スタックおよび、TCP/UDP が実装され、ポットの温度などをサーバに対して送信した。

1.3.3 結果

特定個人の移動追跡

実際の移動とセンサを通じて取得した移動との比較を行った。図 1.4 は 24 時間 (夜間はセンサ検知範囲から退去したため、実質 18 時間) での実際の位置とセンサによって検出された位置を示す。この図では、横軸が時間軸、縦軸が当該時間に存在した場所を示している。実線は実際の場所を、点線は RF-Code によって検知された場所である。

部屋ごとの人数

人の動きが特徴的だった部屋を選択し、以下に示す。図 1.5 は BOF2 の、図 1.6 は LOBBY3 を示している。これらの図は、その部屋の人数を時間軸で表した図である。BOF2 は BOF が開始された 11:30 ごろから人が検出され始めている。また、20:00 以降の夜間はまったく検出されていない。しかし、通路である LOBBY3 では、早朝を除き、常に検出され

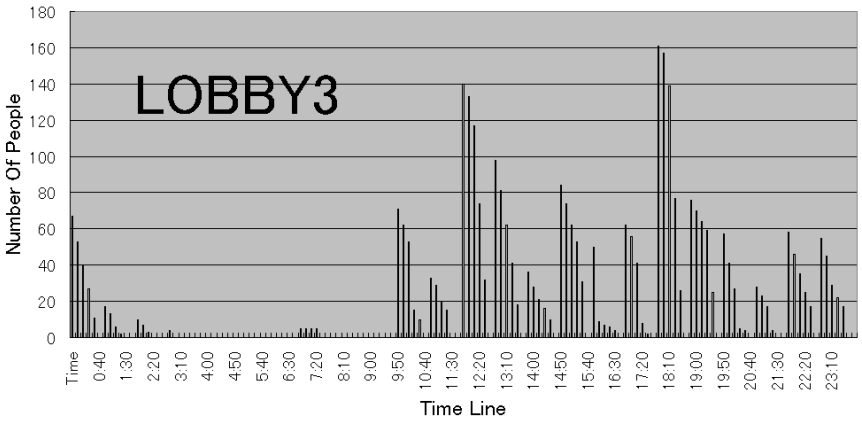


図 1.6. LOBBY3 における時間軸と人数とのグラフ

ている。

また、両者ともに右肩下がりが繰り返されている傾向が見受けられる。このことより、BoF の開始・終了時刻とともにみなが移動し、また別の部屋へと移動するという移動パターンが読み取れる。

1.3.4 まとめ

この実験では、人およびノート PC、ポットなどに関する、位置情報をはじめとするさまざまな情報を提供するためのプラットフォームを提案・作成・提供した。しかし、これらの実空間における情報を利用するアプリケーションに関しては、残念ながら実験中に作成できなかった。従って、実験終了後、新たなアプリケーションを検討し、作成することとした。LIN6 実験では、iCARs 実験のためのセンサノードとして移動ノードの位置情報を提供すると同時に、移動ノードが送受信するメッセージの統計情報の測定を行った。統計情報の測定は、各移動ノードのユーザ空間プログラムに改良を加え、テキストデータとして取得し、後に収集した。その結果、位置登録パケットが連続して送られ、確認応答が返信されないことや、移動ノードの位置情報の要求が何度も返信されることなく送信されていることが確認できた。このことは、ネットワークの移動処理に時間がかかり、通信をスムースに継続できていないということを示しており、ネットワークの移動処理をスムースに行う必要があると考えられる。

1.4 Mobile IPv6 往復経路確認 (Return Routability) 実証実験

実験責任者: 島 慶一

所属: 株式会社インターネットイニシアティブ技術研究所

1.4.1 目的

Mobile IPv6 は IPv6 に移動通信機能を持たせるための仕様である。Mobile IPv6 の仕様は現在インターネットドラフトとして発行されており、IETF の IP Routing for Wireless/Mobile Hosts 分科会で議論されている。Mobile IPv6 の仕様には、移動ノードと固定ノードの間で最適な経路を使って通信するための経路最適化 (Route Optimization) の仕組みが定義されている。移動ノードと固定ノード間で経路を最適化するためには、移動ノードが固定ノードに自分の現在位置を通知しなければならない。この動作は対応付け更新 (Binding Update) と呼ばれる。しかし、パケットの経路決定に関わる情報を認証なしに信用することはできない。そのため、Mobile IPv6 では往復経路確認 (Return Routability) と呼ばれる簡易認証方式が導入された。往復経路確認は、Mobile IPv6 の仕様で新たに定義されたプロトコル制御用の拡張ヘッダであるモビリティヘッダ (Mobility Header) を用いて実現される。本実験では経路最適化の手順が動作することを実証するとともに、Mobile IPv6 の制御パケット (モビリティヘッダ) がネットワークに与える影響を調査する。

1.4.2 概要

モビリティヘッダは主に以下の 4 つの場合に利用される。

- 移動ノードとホームエージェント間の対応付け

更新 (Binding Update)

- 往復経路確認
- 対応付け更新の再要求
- エラーの通知

ひとつめは、移動ノードがホームエージェントに新しい移動先を通知するための通信であり、移動ノードが新しい出先ネットワークに接続するたびに発生する。2 番目は移動ノードと固定ノードとの間で認証情報をやりとりするための通信であり、移動ノードが移動先で固定ノードと最初に通信する時と、移動ノードが新しい出先ネットワークに移動した際に発生する。3 番目の通信は、すでに確立している対応付けの情報の有効時間を更新するための通信であり、対応付けの有効時間が切れる直前に実施される。4 番目はプロトコルエラーを通知するための通信である。

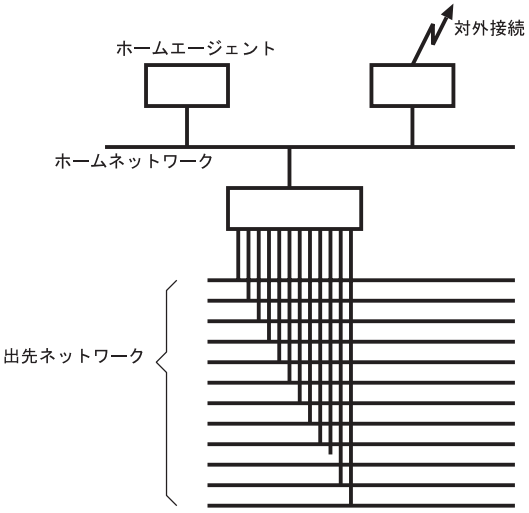


図 1.7.　実験ネットワーク概要

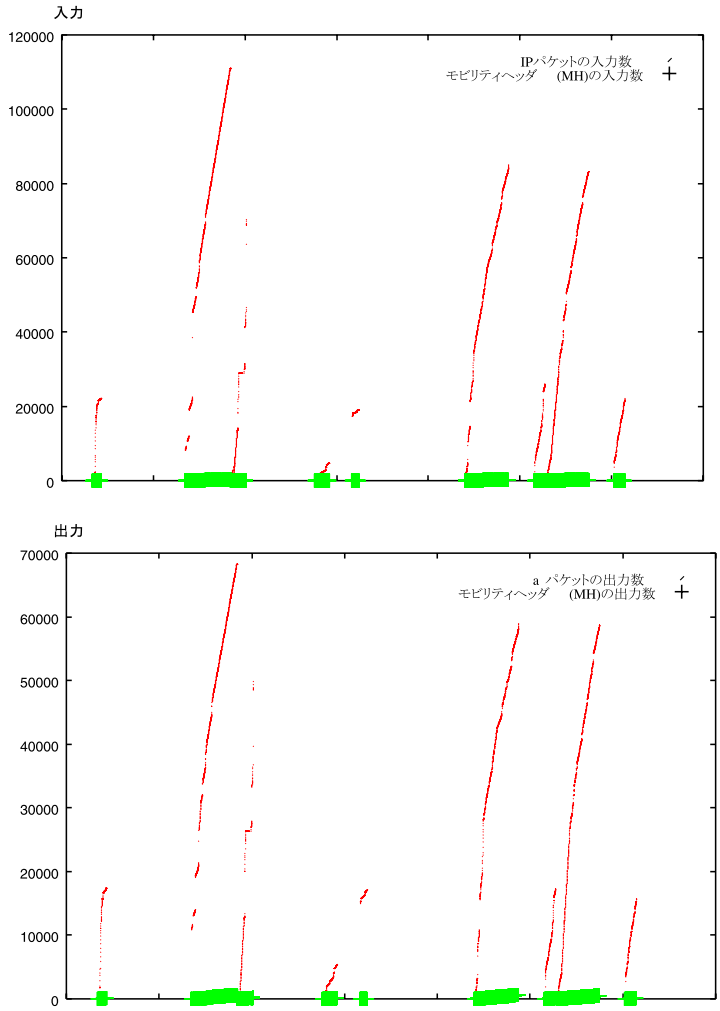


図 1.8.　移動ノードでのパケット入出力数の推移

図 1.7 に実験ネットワークの概要図を示す。合宿地に施設されたサブネットワークのひとつをホームネットワークとし、ホームエージェントを運用した。合宿地には、合宿参加者が利用するサブネットワークが 12 個施設してあり、移動ノードは 12 個のサブネットワーク上を自由に移動する。

モビリティヘッダが通常の通信中に占める割合を計測するため、ホームエージェントと移動ノード上でパケット数を測定した。モビリティヘッダが固定ノード同士でやりとりされることはないため、ホームエージェントと移動ノード上でパケットを測定することでモビリティヘッダ占有率の近似値を計算することができる。

1.4.3 結果

図 1.8 に移動ノードで計測したパケット数の推移を、図 1.9 にホームエージェントで計測したパケット数の推移を示す。

なお、図 1.8 でグラフに結果が表示されていない期間は、移動ノードがシャットダウンしていた時間である。

また、それぞれのノード種別毎にパケット数の総計を計算した結果を表 1.1 に示す。

1.4.4 考察

図 1.8、図 1.9 から、IP パケットとモビリティパケットの比率は時間によらずほぼ一定であることがわか

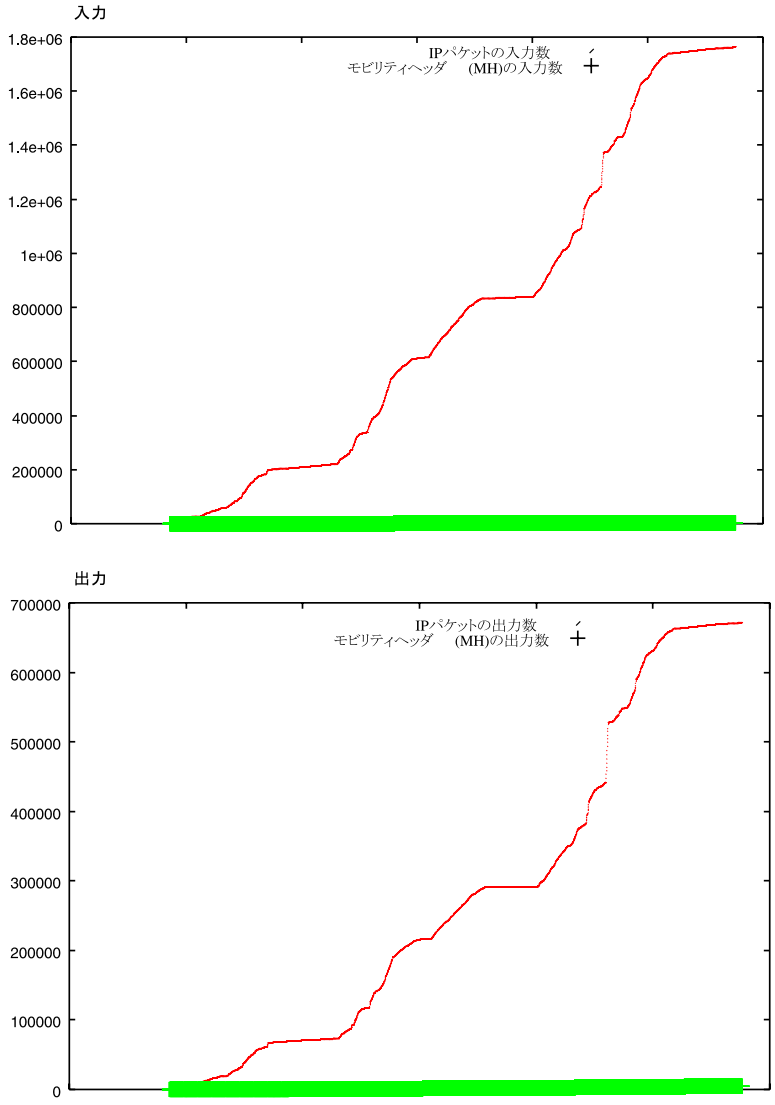


図 1.9. ホームエージェントでのパケット入出力数の推移

表 1.1. 移動ノードとホームエージェントにおける入出力パケット数

移動ノード			
	IP パケット	MH パケット	比率
入力	443807	1102	0.24%
出力	304899	2380	0.78%

ホームエージェント			
	IP パケット	MH パケット	比率
入力	1765015	4497	0.25%
出力	671921	4487	0.66%

る。よって、実環境に近い運用状況下において、モビリティヘッダによる爆発的なトラフィックが発生することはないと考えられる。

また、表 1.1 からわかる通り、移動ノード、ホームエージェント共、全体の入出力パケット数に占めるモビリティヘッダ数は 0.25%から 0.8%までと低い値に収まっている。さらに、モビリティヘッダは移動を通知するためのほぼ固定長の情報しか含まれないため、通常の IP パケットと比較してパケット長も小さい。加えて、実際のネットワークでは、移動とは関係ない固定ノード同士の通信も存在するため、ネットワーク全体におけるモビリティヘッダの比率はさらに低い値になると考えられる。

以上の結果から、Mobile IPv6 で導入された制御パケットがネットワークに与える影響は軽微であることが確認できた。

1.4.5 (参考) 往復経路確認

図 1.10 に往復経路確認の概要を示す。

移動ノードは固定ノードに認証の開始を知らせるための「ホームテスト開始」と「気付テスト開始」を送信する。固定ノードは、それぞれのパケットに対して「ホームテスト」と「気付テスト」を返送する。ホームテストには移動ノードのホームアドレスと固定ノードだけが知っている秘密鍵 K_{cn} を使って計算されたハッシュ値 (ホームクッキー) が、気付テストには移動ノードの気付アドレスと固定ノードだけが知っている秘密鍵 K_{cn} を使って計算されたハッシュ値 (気付クッキー) を含める。移動ノードは、ホームクッキーと気付クッキーのハッシュ値を計算し、それを移動ノードの秘密鍵 K_{bm} とする。対応付け更新には秘密鍵 K_{bm} を使って計算されたハッシュ値が含まれる。固定ノードは移動ノードに送信したホームクッキーと気付クッキーから K_{bm} を再計算できるので、受信した対応付け更新と固定ノードで再計算した K_{bm} を使って対応付け更新のハッシュ値を検算する。

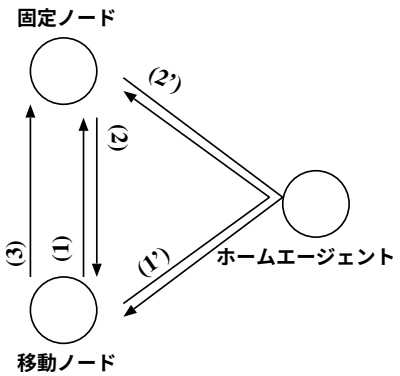
1.5 network music

実験責任者: 原 貴洋

所属: ヤマハ株式会社

1.5.1 目的

ネットワークを介した音楽セッションについては従来から多くの手法が提案されている [97, 64]。しかし、これらの手法は最大遅延が保証された高速なネッ



(1) 気付テスト開始

(2) 気付テスト
気付クッキー(MAC_Kcn(気付アドレス))を含む

(1') ホームテスト開始

(2') ホームテスト
ホームクッキー(MAC_Kcn(ホームアドレス))を含む

(3) 対応付け更新
Kbu = Hash(ホームクッキー | 気付クッキー)
MAC_Kbu(気付アドレス
| 固定ノードアドレス
| 更新パケット内容)を含む

図 1.10. 往復経路確認の概要

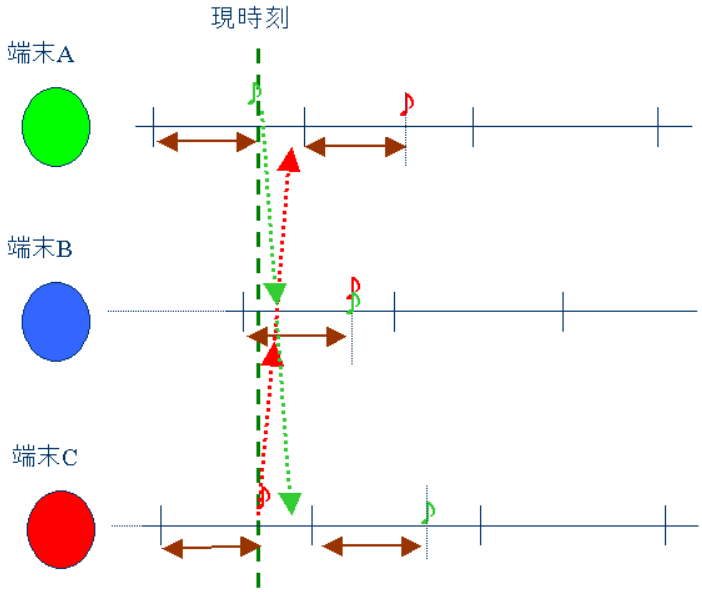


図 1.11. 3 つの接続端末における演奏情報の流れ

トワークを前提としているため、現実的には利用できる環境が大きく制限される。これに対し、多様なネットワーク環境で音楽セッションを行うことを目的とした GDSM[183] という提案がある。本実験では、GDSM に基づく試作システムの実装と実運用に則した評価を行い、その有効性を検証する。また利用したユーザからの意見を収集することで、実利用における問題点、改善点を検証する。

1.5.2 概要

本実験では、GDSM の概念を基に、変更・拡張を加えたシステムの実装を行った。このシステムは以下のような特徴を持つ。

- 音楽セッションに参加する演奏者はそれぞれ 4 小節などの音楽的な区切り (以下、これを演奏区画とする) にしたがって演奏する。それぞれの演奏者は演奏区画を単位として演奏情報を送信する。演奏者が送信した演奏情報は、それを受信した演奏者の演奏区画に合わせて再生される (図 1.11)。演奏者が直接に接続していない場合でも、その間に接続されている演奏者を通じて、演奏情報を伝達する。演奏情報には最大ホップ数が付与されているので、ある限られた範囲にのみ伝達される。
- 参加している端末のひとつがサーバとなり、演奏者は音楽セッション参加時にそのサーバに接続する。このサーバは演奏に参加している端末やその接続状態についてのデータベースを持っており、利用者に対して図 1.12 のような仮想空間を提供する。演奏者はサーバに接続すると、この仮想空間上の適当な場所にマッピングされる。演奏者はこの仮想空間を移動することで、音楽セッションをする相手や接続状態を自由に変化させることができる。

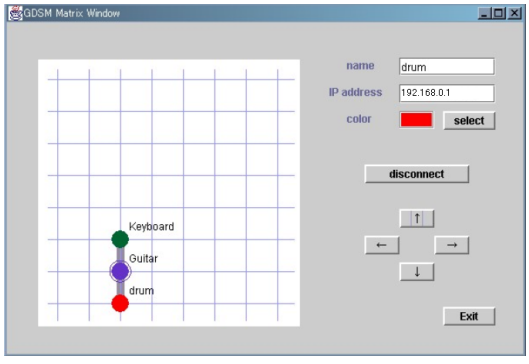


図 1.12. 仮想空間画面

- 演奏者の端末は、セッションを行っている相手からの演奏情報を視覚化する画面を持つ (図 1.13)。画面上の縦軸は時間を表し、横軸は受信した演奏情報の音高を表している。他の演奏者から受信した演奏情報は、画面上の点で表される。受信した演奏情報は、画面上部から下部に向かっ

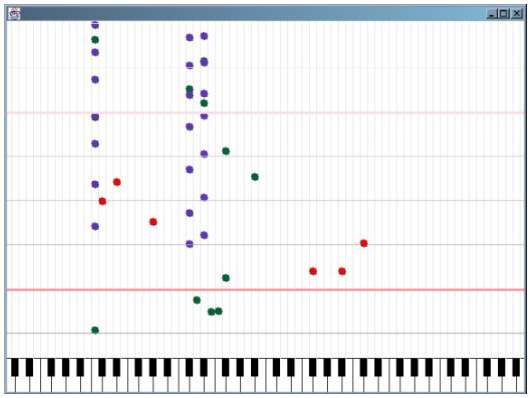


図 1.13.　演奏情報の視覚化画面

て移動し、実際に端末上で発音されると同時に画面下部の鍵盤の描かれた部分に到達するよう画面上に表示される。

このシステムによって、以下のような効果が期待できる。

- ネットワーク環境のスケーラビリティを持つ。ネットワーク品質、回線速度の違い、変化を吸収できる。
- それぞれの端末は演奏の開始および再生タイミングの同期を取る必要がなく、同期を取るためのサーバなどのシステムを必要としない。
- 演奏者が接続する位置を主体的に変更することによって、演奏情報の伝達経路を動的に変化させ、全体の演奏に大きな影響を与えることができる。
- 音楽セッションにおいて、相手の音の情報だけでは相手に合わせて演奏することは難しい。受信した演奏情報を視覚化することで次に流れてくる音が先に見え、相手の演奏に対応する演奏ができる。

これらの機能を持つ試作システムを搭載した計算機 3 台を、Plenary、NOC、Lobby のそれぞれの場所に配置した (図 1.14)。それぞれの計算機には MIDI によってコントロール可能な電子楽器を接続し、参加者に自由に利用してもらうことで評価を行った。NOC に配置した計算機上はサーバとして動作させ、他の計算機は NOC のサーバに接続することで音楽セッションを行った。また演奏時に NOC のサーバ上でトラフィックを観測した。

実験では演奏区画を、テンポ 120-4/4 拍子の 4 小節 (8 秒) と設定した。

1.5.3 結果

特に大きな問題は発生せず、合宿期間中は正常に音楽セッションができる状態を維持できた。以下の現象が 1 度ずつ発生したがソフトウェアの再起動、再接続により復旧した。

- 他の端末と接続しても、データの送出はされるがまったく受信されない
- 連続しているはずのデータが 1 小節ごとに途切

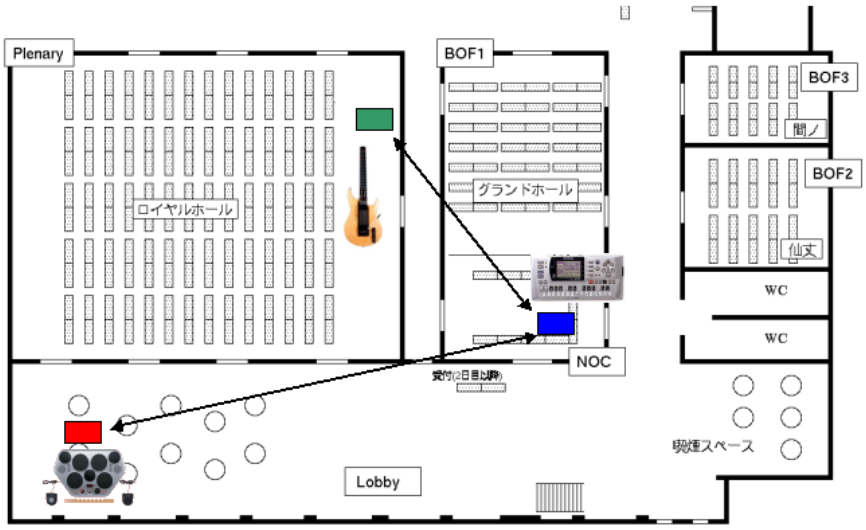


図 1.14.　実験における配置図

表 1.2. 音楽セッション中における各端末の使用帯域

NOC 端末 Uplink	61.18 kbps	14.91 Packets/sec
NOC 端末 Downlink	35.75 kbps	12.03 Packets/sec
Plenary 端末 Uplink	9.08 kbps	5.71 Packets/sec
Plenary 端末 Downlink	39.42 kbps	8.25 Packets/sec
Lobby 端末 Uplink	26.67 kbps	6.32 Packets/sec
Lobby 端末 Downlink	21.76 kbps	6.65 Packets/sec

れたり、細分されたりする

トラフィック観測から計算した音楽セッション中における演奏中の帯域を、表 1.2 に示す。

利用者からは、以下のような意見があった。

- 相手の演奏情報の視覚化は相手とのコミュニケーションの手段として面白い。
- 楽器演奏の経験があるが、4 小節遅れるようなこのシステムでの合奏はかなり難しい。
- 仮想的なネットワークのつながりの視覚化や接続状態によって演奏が変化する要素など、Peer-toPeer アプリケーションとしての面白さがある。

1.5.4 考察

Plenary に設置した端末では、上りと下りで使用した帯域は合わせて 50 kbps 以下であった。NOC に設置した端末においては、それぞれの演奏情報を中継しているため、2 コネクション分のトラフィックが発生しているが、それでも上り、下り合わせて 100 kbps 以下である。

またこの試作システムは、フルメッシュ型の接続モデルではなく、直接接続している端末を介して他の端末と通信するモデルであり、演奏情報には最大ホップ数も決められている。そのため、参加する端末が増えても、1 端末あたりのトラフィックの増大を抑制することができる。

これらの結果から、このシステムがネットワーク規模と参加人数に対してスケーラビリティを持つことが示された。

音の情報を先に視覚化することができるシステムに対する利用者の評価は高かった。また、演奏情報だけではなく、コード (和音) 情報なども表示してもらえると演奏がしやすいという意見もあった。こられは、ネットワーク音楽セッションにおいて、音の情報を流すだけでは不十分であり、視覚化など演奏を補助するための仕組みの重要性を示唆するものである。

また、4 小節前の相手の演奏に合わせるという演奏形態は、楽器の演奏経験を持つ演奏者にとっても難しいものであった。既存の音楽とは違うこの形態において演奏者が演奏しやすくするためのアプリケーションでの工夫はまだ必要である。

運用中に、セッションができない状況に陥ることがあった。ソフトウェアの実装上の問題であると思われる。ソフトウェアのデバッグ、テストはまだ不十分であった。

これらの問題点に関しては、今後のソフトウェアのアップデートで対応していく予定である。

1.6 moCA WG による PKI エクセサイズ

実験責任者: 櫻井 三子
所属: 日本電気株式会社

1.6.1 目的

PKI 技術のプロモーション、特に組織内で構築する PKI の応用について追求すること。組織内での利用場面から組織外での利用場面にいたるまで、WIDE メンバ向けに実験運用している moCA(members oriented CA) が発行した、WIDE メンバ証明書を実際に合宿会場で使いながら、さらなる利用場面を考えること。

1.6.2 概要

WIDE メンバ証明書はあらかじめ 7 月に配付してあり、9 月の実験では WIDE メンバ証明書をブラウザ、メールツールにインストールずみであることを前提に、合宿会場から利用できる 4 つの利用場面を構築し提供した (表 1.3)。プロモーション効果を図るために、各エクセサイズの利用回数を、アンケートやアクセスログによって調べた。

エクセサイズ 1〜3 は、WWW サーバとブラウザの組み合わせで実現し、エクセサイズ 4 は、WWW

表 1.3.　各 PKI エクセサイズの特徴

	利用場所	実験期間	アピールポイント	応用プロトコル
エクセサイズ 1 合宿会場 WWW サーバの閲覧	合宿会場内	合宿期間のみ	パスワードの代わり	HTTPS (HTTP over TLS)
エクセサイズ 2 会議の出席簿登録	合宿会場内	合宿期間のみ	入力の手間削減、データアップロード作業者名の自動表示	HTTPS
エクセサイズ 3 パーティ申込み	組織外	合宿期間を含め 1 ヶ月程度	入力の手間削減、認証後の属性利用処理への応用 (割引き)	HTTPS
エクセサイズ 4 S/MIME 署名検証のテスト	組織内外	合宿期間を含め 1 ヶ月程度	WWW 以外の応用	HTTPS および S/MIME

サーバとブラウザ、およびメールツールの組み合わせで実現した。
実験のために特別なネットワーク設計が必要となることはなかったが、エクセサイズ 2 では他のグループの実験で必要となったネットワーク構成を利用する形となった。
以下では各エクセサイズの概要について述べる。

エクセサイズ 1　合宿会場 WWW サーバの閲覧

合宿会場でのみ運用される WWW サーバでは、従来 WIDE 共有パスワードを使ってアクセス制限を実現してきたが、今回は証明書に対応した WWW サーバを構築し、WIDE 共有パスワードの代わりに WIDE メンバ証明書を利用して合宿関連情報を閲覧できるようにした。WIDE メンバ証明書が使えない場合を考慮し、WIDE 共有パスワードを利用した WWW サーバも別途用意した。

エクセサイズ 2　会議の出席簿登録

合宿期間中は、WG や BoF ごとの会議が 30〜40 ほど開催される。従来の会議では、会議の主催者が後日の活動のために会議参加者の出席をとろうと紙をまわして出席簿を作成していた。しかし、紙の出席簿をもとに ML を作成しようとする時に、メールアドレス入力のミスや手間の問題があった。そこで、主催者の便宜を図るべく、出席簿のオンライン作成について実現する場面で、WIDE メンバ証明書を利用することにした。
会議参加者が出席簿登録ページへアクセスしたいと思う意欲を高めるため、各会議ごとに資料置き場を設け、「会議参加者が会議中に資料置き場へ必要な資料を取りに行くと、出席登録が自動的に行える」というシナリオとした。そして、出席簿登録に必要な「誰が」「いつ」「どの会議室にいた」かという情報を登録者に入力させることなく出席者表示を行った。また、資料をアップロードする時に、WIDE メンバ証明書を提示し、誰が資料を置いたか自動表示できるようにした。

エクセサイズ 3　パーティ申込み

PKI で利用する公開鍵証明書には公開してもよい公開鍵情報が記載されているため、公開鍵の所有者情報についても公開できる程度の情報を証明書に記載しておけば、組織外で提示して使える。そこで、WIDE メンバ証明書を WIDE 以外 (組織外) で提示して使える場面を示すため、「WIDE メンバ以外も参加するパーティの申込み用 WWW サーバにて、WIDE メンバ証明書を提示して申し込む」という利用場面を提供した。
オンラインでのパーティ申込みフォームでは、少なくともパーティ参加者の氏名や連絡用のメールアドレスを入力する項目がある。申し込む時に WIDE メンバ証明書を提示したパーティ参加者は、氏名やメールアドレスを入力しなくても、証明書の記載情報を

表 1.4. アンケートおよびアクセスログからの結果

合宿参加者 272, アンケート回答数 141, 回答率 51.8% アンケート「どの場面で証明書を使ってみたか?」に対する結果			ログから得たアクセス数
エクセサイズ 1	合宿会場 WWW サーバの閲覧	47 (17.28%)	707
エクセサイズ 2	会議の出席簿登録	38 (13.97%)	1803
エクセサイズ 3	パーティ申込み	3 (1.10%)	119
エクセサイズ 4	S/MIME 署名検証テスト	3 (1.10%)	12
その他	two WG の WWW サーバ閲覧	7 (2.57%)	-

表 1.5. エクセサイズ 2 の出席簿記録より

会議出席簿登録ページにアクセスした人	58	(合宿参加者の 21.32%)
会議出席簿登録ページに記録されたのべ人数	472	

表 1.6. エクセサイズ 3 の参加記録より

証明書を利用してパーティへの参加登録をした人	15	(パーティ出席者の 15%)
証明書を所持しているが利用しなかった人	1	(パーティに出席した証明書保持者全体の 6%)

利用して自動的に入力できるようにした。
また、証明書による認証と同時に WIDE メンバであるという属性を、データベースに問い合わせることなく得られる特徴を利用し、「WIDE メンバだったらパーティ参加費を割り引く」というルールを実現した。

エクセサイズ 4　S/MIME 署名検証のテスト

PKI の応用プロトコルとして、電子メールのセキュリティを強化する S/MIME がある。S/MIME を試そうとするときは、まず S/MIME でやりとりできる相手を探す必要があるが、相手と本格的にやり取りする前に、相手が利用する S/MIME 対応メールツールと相互運用性があるツールか調べたい場合がある。また、複数のメールツール間の S/MIME 相互運用性を試したい場合、あるツールから他の複数のメールツールに毎回署名を作成して送信していたのではテストに手間がかかる。
そこで、各種ツールで作成した S/MIME 署名つきメールを WWW サーバ上にデータとして集めておき、相互運用性を調べたい人が、調べたいツールの署名つきメールを選択し、指定した宛先に送って検証する、という方法を提供した。

エクセサイズ 4 は、S/MIME をどのような場面で利用したらよいか、という観点ではなく、本格的に利用する前のテストを効率よく行うという観点であり、他のエクセサイズの趣旨とは異なっている。

1.6.3 結果

アンケートおよびアクセスログ (実験期間終了まで) からの結果を表 1.4 に示す。
エクセサイズ 2 については、さらに出席簿の記録より表 1.5 に示す結果が得られた。
また、エクセサイズ 3 については、さらに参加登録の記録より表 1.5 に示す結果が得られた。
アンケートでは、実験に参加できなかった方からのコメントも得られた。

- テンポラリにでも WIDE メンバー証明書を配って欲しかった
- 証明書をブラウザにインストールできなかった

1.6.4 考察

- プロモーションの場面設定に対する効果
  合宿会場でのみ利用できるエクセサイズ 1、2 の方がエクセサイズ 3、4 よりも利用回数が多かったことから、プロモーションを行う場所での活

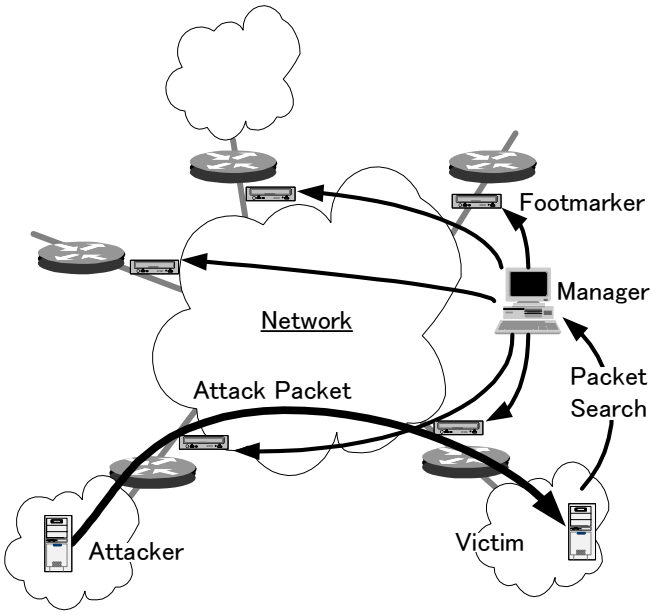


図 1.15.　PAFFI 動作概念図

動を意識した方が実験参加の動機付けが高まるといえる。

- 証明書の継続利用傾向
  表 1.5 よりエクセサイズ 2 では、会議の出席簿登録ページにアクセスしたことのある人は、一人平均約 8 回会議出席簿登録ページにアクセスしたことになる。毎日使える場面設定を増やしていけば、証明書が身近なツールとして受け入れられると思われる。
- 証明書の組織外での名刺的な利用可能性
  エクセサイズ 3 の結果 (表 1.4, 表 1.6) を見ると、予想したよりもアクセス数は少なかった。しかし証明書を持っている人は、パーティへの参加登録に証明書を利用する割合が高く、持っていれば使うという傾向が伺える。一般のイベント申込みで名刺を持っていれば使うことを考えると、証明書を名刺代わりにした利用場面をさらに作り出せそうである。

エクセサイズ 4 は、当初 SOI WG と moCA WG とが中心となって行う予定であったが、双方とも作業の都合がつけられず、また、関心を寄せる人自体が少なかった。

1.6.5 まとめ

実験途中からエクセサイズとして用意した利用場面の他に、two WG の WWW サーバ閲覧が増えた。これは、エクセサイズ 1 と同様の応用であり、エクセサイズを通じてさらなる利用場面を考えるという、実験の目的に対する一つの成果が得られたといってよい。

合宿ネットワークを利用した実験に参加することによって、単独に実験するよりも実験の説明をする機会を容易に得られ、フィードバックも多く得られた。

1.7 PAFFI による IP traceback 実験

実験責任者: 星野 浩志
所属: 横河電機株式会社

1.7.1 目的

IP パケットの発信元を追跡する IP traceback の一手法である Hash Based IP Traceback システムを実現した PAFFI (PAcket Footmark FInder) を、実ネットワークで運用することで、実環境での IP traceback システムの有効性と問題点を確認する。

1.7.2 概要

PAFFI は、ネットワークの境界等各所に設置した Footmarker によって記録蓄積された、通過パケットの特徴情報である『パケット Footmark』の中から、追跡したいパケットのパケット Footmark に一致するものを検索することで、ユーザが入力したパケットの通過経路を特定する。

本実験では、合宿ネットワーク内部の複数のパケッ

ト監視ポイントで PAFFI を使って パケットを常時監視記録し、ユーザが送受信したパケットがどこを通過したかを検索して見せた。 次の二つの方法を用意した。

(1) tcpdump で取得したパケットの検索

合宿参加者は、自分のマシンで tcpdump でパケットを取得して、tcpdump の出力を、PAFFI に入力 (web-browser 操作画面経由) すると、PAFFI が、そのパケットがどの監視ポイントを通過したかを表示する。 約 5 分前の記録まで検索することができる。

(2) 送信した ping パケットの検索

合宿参加者が特定ノードに、通常の ping やソースアドレス偽装 ping をかけることで、ping パケットの検索が自動的に行われ結果が記録される。(1) に比べて簡単にパケット検索をすることができる。

1.7.3 実験環境

実験では、パケットがどの BOF 部屋または Plenary 部屋の、有線 (Cable) もしくは無線 (Wireless) ネットワークを通過したかを特定できる環境を構築した。各部屋の有線または無線のセグメントは 12 本あり、すべて BI4000 ルータに集線されている。そのうち 6 セグメントを監視対象とした。

BI4000 から出ている監視対象セグメントの CAT-5 ケーブルに、ケーブルタップ装置 (Century TAP) をしかけた。ケーブルタップ装置からは inbound, outbound 両方向の監視用の線が出るので、各セグメントの出入り口における、流入 (inbound) および流出 (outbound) パケットを区別して監視することができる。また各 Footmarker は 3 つの監視用インターフェースを持つ。

このような環境で各 Footmarker の監視ポイントを通過したパケットの、以下の統計情報を記録した。

- 通過 IP パケット数
- パケット Footmark の衝突回数
  (パケットの Footmark 値がすでに Footmark Table に記録されている Footmark 値と同一であった回数)

Footmarker がパケット Footmark を記録蓄積する Footmark Table は 5 秒毎に切替えるため、これらは 5 秒間の統計情報として記録される。

また実験期間中にパケットの検索を行い、検索結果の False Positive の割合を調べた。

1.7.4 結果

上の環境で、2002/9/10 14:52 から 2002/9/11 8:49 までの間実験を行った結果を以下で説明する。

実験開始から終了までの、各パケット監視ポイントを通過した IP パケットの Footmark の衝突率を、表 1.7 に示す。衝突率は、監視ポイントを通過したすべての IP パケットのうち Footmark の値が同一になったパケットの割合である。

比較的パケット Footmark 衝突率が高かった BOF 無線セグメントからの流出トラフィックについて、パケット Footmark 衝突回数の度数分布を表 1.8 に示す。

全体の 99.7%の Footmark Table で、Footmark 値の衝突回数が 2 以下だった。また最大衝突回数は、88 回だった。

一方、PAFFI に対して検索が行われたパケットの数は 1273 だった。これらの検索結果で False Positive が出たかを確認したかったが、記録のしくみの用意ができなかったため、確認できなかった。しかし、自らで検索した 56 回中 False Positive は 0 件だった。

1.7.5 考察

検索結果で False Positive が出なかったことから、本実験環境のもとでは PAFFI によってパケット通過ポイントを十分特定できることを確認できたと、言うことができる。

False Positive は、Footmark 値の衝突率が高いほど出やすい傾向があるが、表 1.7 によればパケットの Footmark 値の衝突率は、すべての監視ポイントで 0.034%以下と十分に低い衝突率であることがわかる。表 1.8 ではトラフィック量が少ないこともあって、各 Footmark Table で衝突はほとんどおきていないことがわかるが、一方で 5 秒間に 88 回もの衝突が起きているケースもある。図 1.16 に示す、トラフィック量に対するパケット Footmark の衝突回数の分布図によれば、トラフィック量が増えると衝突回数が増えるという傾向ではないことがわかる。例えば 88 回衝突したときは、トラフィック量は約 480 packets/5 sec だった。異なる 88 パケットがすべて同じ Footmark 値になることは稀であるため、これは同じパケットを短時間に大量に送信したものと考えられる。仮にこの

表 1.7.　各監視ポイントのパケット Footmark 衝突率

Footmarker 一覧 No. 説明	監視ポイント一覧 No. 説明	通過 IP パケット数合計	衝突回数合計	衝突率 (%)
1 CB-BOF-in BOF 部屋への流入監視用	1 BOF1 無線セグメントへの流入	4064810	631	0.016
	2 BOF2 無線セグメントへの流入	732629	64	0.009
	3 BOF3 無線セグメントへの流入	360023	27	0.007
2 CB-BOF-out BOF 部屋からの流出監視用	1 BOF1 無線セグメントからの流出	3755266	1293	0.034
	2 BOF2 無線セグメントからの流出	669151	134	0.020
	3 BOF3 無線セグメントからの流出	344468	43	0.012
3 CB-Plenary-in Plenary 部屋への流入監視用	1 Plenary 有線セグメントへの流入	1202763	53	0.004
	2 Plenary 無線セグメント 1 への流入	4178338	543	0.013
	3 Plenary 無線セグメント 2 への流入	4368916	803	0.018
4 CB-Plenary-out Plenary 部屋からの流出監視用	1 Plenary 有線セグメントからの流出	1108597	27	0.002
	2 Plenary 無線セグメント 1 からの流出	3417819	683	0.020
	3 Plenary 無線セグメント 2 からの流出	3881341	1318	0.034
5 CB-NAT NAT 監視用	1 NAT への流入	2928712	416	0.014
	2 NAT からの流出	2896812	360	0.012
	3 (未使用)	—	—	—

表 1.8.　パケット Footmark 衝突回数分布

Footmark 衝突回数	BOF1 無線からの流出	BOF2 無線からの流出	BOF3 無線からの流出
0	28656	29151	29185
〜1	410	31	13
〜2	76	7	4
〜4	33	8	3
〜8	14	9	2
〜16	2	1	0
〜32	12	0	0
〜64	2	0	0
〜128	2	0	0
129〜	0	0	0

ようなパケットを検索した場合でも、False Positive にはならない。

1.7.6 まとめ

本実験環境では PAFFI によってパケット通過ポイントを十分発見できることを確認することができた。PAFFI 側が個別の Tagged-VLAN を監視する機能に対応できなかったため、Tag なしの線と、多くのケーブルタップ装置と Footmarker が必要になったが、今後 VLAN 対応することで改善する予定である。

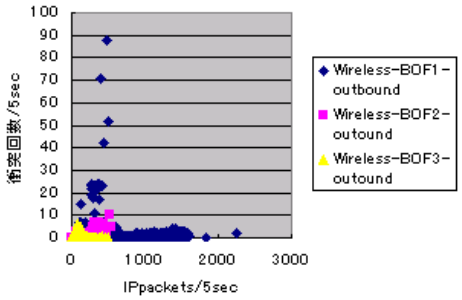


図 1.16.　トラフィック量対 Footmark 衝突回数の分布

1.8 SNMP による Hash-based 技術実装実験

実験責任者: 太田 耕平

所属: 株式会社サイバー・ソリューションズ

1.8.1 目的

IP アドレスを詐称したパケットによる攻撃が問題となっている現在のネットワークでは、詐称したパケットの実際の発信元を追跡する技術が必要である。本実験では、IETF54 で提案された、An Architecture IP Packet Tracing [84] に基づいた SNMP による実装を実ネットワーク上で運用し、その性能評価を行った。本実装は、企業内 LAN などのようなネットワークトポロジ、物理層トポロジが変化しないネットワークを追跡対象ネットワークと想定する。

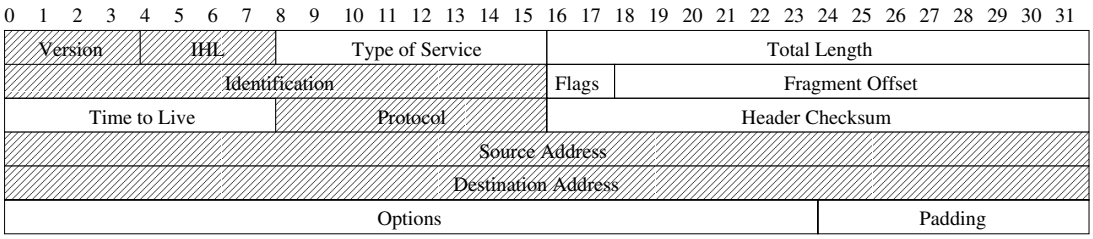


図 1.17. IPv4 ヘッダ中のパケットレコード値算出に用いられたフィールド

表 1.10. 実験使用機材

	OS	スペック
ippt-pra1	FreeBSD 4.5-RELEASE	PentiumIII 850 MHz
ippt-pra2	FreeBSD 4.5-RELEASE	C3 800 MHz
PT	Solaris 8(IA)	NotePC PentiumIII 650 MHz
IDS†	Linux	OpenBlockSS PowerPC 405GP 200 MHz

表 1.9. 追跡対象パケット送信スケジュール

送信時刻	発信元	宛先
毎時 0 分	BOF–2 (*)	Plenary
毎時 5 分	Plenary (*)	ロビー
毎時 10 分	ロビー (*)	BOF–2
毎時 15 分	BOF–2 (*)	ロビー
毎時 20 分	Plenary	NAT
毎時 25 分	ロビー	NAT
毎時 30 分	BOF–2	NAT
毎時 35 分	Plenary (*)	BOF–2
毎時 40 分	ロビー (*)	Plenary

1.8.2 概要

本実験システムはパケットレコードエージェント (PRA)、侵入検知システム (IDS)、パケット追跡マネージャ (PT) からなる。

パケットレコードエージェント

モニタリング対象ネットワークを通過する全てのパケットのパケットレコード値を算出し、一定期間保存する。パケットレコード値の算出には、ルータにより変更されない IP ヘッダのフィールド箇所 (図 1.17 の網かけ箇所) を抽出し、それを元にハッシュ関数 (MD5) を適応し、その結果を循環バッファに格納した。ここでは最新 1000 パケットのパケットレコードを格納するように循環バッファのサイズを定めた。

侵入検知システム

侵入検知システムのこのシステムでの役割は、検知したパケットのパケットレコードを算出し、その値をパケット追跡マネージャに通知することである。本実験では、IDS に snort-1.9.0 を用い、SNMP Trap でパケットレコード値をパケット追跡マネージャに通知した。検知後対象となる全パケット情報がネットワーク上に流れることはない。

パケット追跡マネージャ

侵入検知システムから通知されたパケットプリント値を元に、パケットレコードエージェントに問いあわせる。本実験では、問いあわせのプロトコルに SNMP を採用し、新たな MIB を定義した。

本実験では、BOF-2(Cable)、ロビー (Wireless)、Plenary(Cable) の各セグメントに配置した追跡対象パケット生成・受信装置から、追跡パケットを送信した。表 1.9 に追跡パケット送信スケジュールを記載した。なお、本実験では追跡対象パケット生成・受信装置は侵入検知システムを兼ねた。

今回の実験に用いた機材を表 1.10 に挙げる。

2002 年秋合宿におけるネットワークにおける、パケットレコートエージェント、侵入検知システム、パケット追跡マネージャの配置図を図 1.18 に示した。

† 追跡対象パケット送信・受信装置を兼ねる

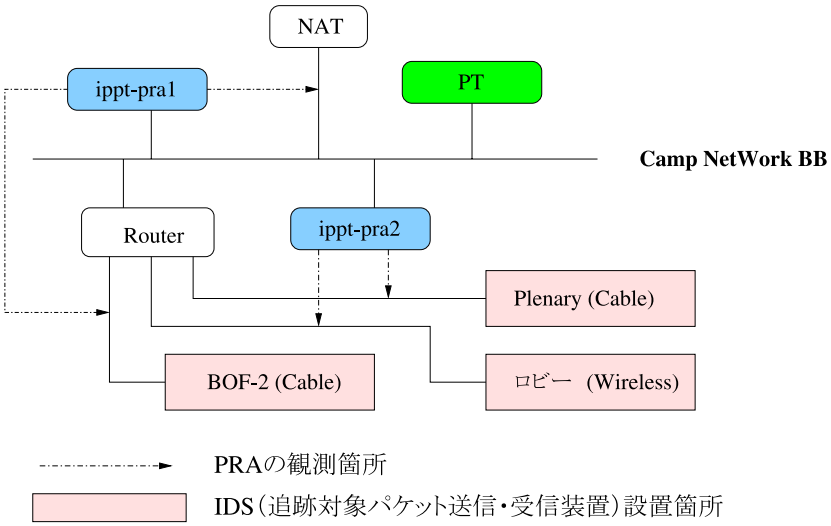


図 1.18.　実験ネットワーク概略図

この配置の目的は、複数のセグメントにわたったパケット追跡の可能性を検証するものである。
実験は 9 月 10 日の 15 時 00 分から 9 月 11 日の 18 時 40 分まで行った。

1.8.3 結果

本実験では、以下の項目について評価を行った。

1. 追跡成功率、誤検知率
2. パケット追跡に要した時間

最初に、各 PRA からの反応が正しく返答できているか、つまり追跡が正しく達成できたかについて検証した。この実験においての追跡成功率は

$$\text{追跡成功率} := \frac{\text{正しい PRA からの返答回数}}{\text{攻撃パケット発信回数}}$$

で定義した。ここでいう正しい PRA からの返答とは、物理的トポロジおよびネットワークトポロジから通過したと確定できる PRA からのみ返答が得られた場合をさす。それ以外の PRA から返答があった場合は誤検知とし、誤検知があった場合は正しい PRA からの返答はなかったものとする。例えば、ロビーから Plenary に追跡対象パケットを送信した場合、図 1.18 によればそのパケットはロビー、Router、Plenary を経由するので、ロビーと Router 間、Plenary と Router 間を観測している PRA から反応があり、かつその他の PRA からは反応がなかった場合のみ、正しい PRA からの返答があったものとする。
表 1.11 に、追跡成功率を記した。

表 1.11.　追跡成功率 (試行回数 28)

	追跡成功率	失敗時刻
毎時 0 分	100.0%	
毎時 5 分	100.0%	
毎時 10 分	100.0%	
毎時 15 分	100.0%	
毎時 20 分	92.9%	9 月 11 日 17、18 時
毎時 25 分	92.9%	9 月 11 日 17、18 時
毎時 30 分	92.9%	9 月 11 日 17、18 時
毎時 35 分	100.0%	
毎時 40 分	100.0%	

また、本来検知されるべきではない PRA から検知されてしまった誤検知率についても調査したが、今回の実験では誤検知は発生しなかった。
次に、パケット追跡に要した時間の評価を行った。パケット追跡に要した時間の評価には、追跡対象パケットを検知してからパケット追跡マネージャが SNMP Trap を受信するまでの時間 T_1、パケット追跡マネージャが SNMP Trap を受信してから、パケットレコードエージェントに最初の問いあわせパケットを送信するまでの時間 T_2、パケット追跡マネージャがパケットレコードエージェントに最初の問いあわせをしてから、最後の返答が得られるまでの時間 T_3 を用いた (図 1.19 参照)。$T_1 + T_2 + T_3$ は、追跡対象パ

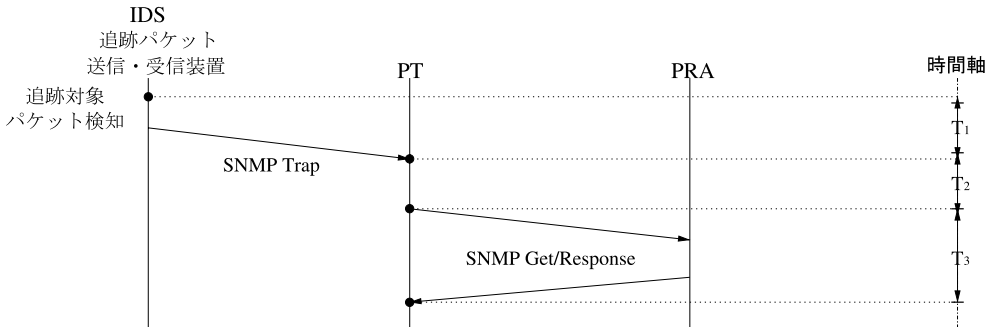


図 1.19. パケット追跡の評価に用いた時間

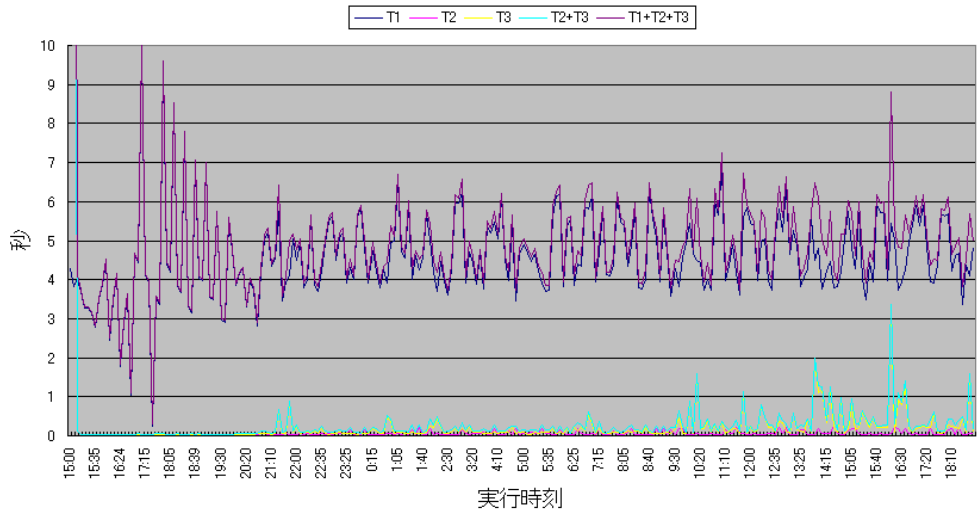


図 1.20. 追跡に要した時間

ケットが検知されてから、パケット追跡が完了するまでの一連の作業に要する時間を、$T_2 + T_3$ は、PT がパケット追跡に要した時間を表わしている。図 1.20 に測定した結果を表示した。

1.8.4 考察

追跡成功率、誤検知率に関しては 3 日目 17 時、18 時の毎時 20 分、毎時 25 分、毎時 30 分に発生したパケットの追跡が成功していなかったが、これは、本来反応があるべき PRA、CampNetworkBB と NAT との間の通信を観測している PRA からの反応がなかったためである。この時間帯の追跡失敗の原因は、ネットワークトポロジの変更があったことであると思われる。従って、ほぼ全ての追跡対象パケットを誤検知することなく追跡することができた。これは、PRA の設定パラメータ (循環バッファサイズ、パケットレコード算出ハッシュ関数) が、本実験ネットワークの規模では適切だったといえる。

パケットの追跡に要した時間に関しては、図 1.20 より、IDS(追跡パケット生成・受信装置) が SNMP Trap を PT に送信するのに、パケット追跡時間の時間が費やされていた。また、2 日目 17 時台から 22 時台は SNMP Trap の送信にかかる時間に、また 3 日目の 13 時台から 17 時台は検索 SNMP パケットの受信にかかる時間に大きな変動が見られた。

また IPv6 ネットワークへの応用も比較的容易であるので、その上での検証も今後の課題である。最後に、本実験ネットワークの場を準備していただいた camp-pc、net-pc に感謝の意を表する。