2014 年度 WIDE 春合宿 Net 報告書

Camp-1403 Net PC 一同 (camp-1403-net@wide.ad.jp)

1 はじめに

本稿では，2014 年 3 月 10 日 – 13 日にかけて静岡県浜松市にある浜名湖ロイヤルホテルで行われた 2014 年度 WIDE 春合宿における合宿地ネットワークの運用および実験に関する報告を行う．

2 合宿テーマ

今回の合宿では，2013 年 12 月研究会の流れを汲み,「セキュリティと SDN」を合宿ネットワークテーマに掲げた．近年，多数ホストからの数百 Gbps の DDoS 攻撃にみられるように，セキュリティの重要性が高まっている．そこで今回は，オープンソースの IDS である Snort や脆弱性スキャナの Nessus, 複数の Firewall を利用して堅牢なネットワーク構築を目指した．さらに近年注目され始めた「Software-Defined Networking（SDN）」と組み合わせることで，より効率的なネットワーク監視を試みた．さらに，Camp-1309 からのビッグ・データ解析の流れを引き継ぎ，今回も traffic fulldump を行った．これらを Snorby と組み合わせ，不審なパケットを送信しているホストの通信のみを pcap として取り出す仕組みを整えた．

もう一つ，Net-PC 運用のテーマとして「教育」と「引き継ぎ」を掲げた．これは，近年の Net-PC のネットワーク構築の際に不足しているのが上記の 2 つであると感じられたためである．その取り組みとして，StarBED を利用して比較的長期間にわたってサーバ構築を行うことで，学習の時間や作業記録を残す時間を確保した．詳細は 7 節にて述べる．

3 合宿ネットワーク概要

本節では，今回の合宿にて構成した合宿地ネットワークの概要について示す．

3.1 対外接続

合宿地からの対外接続には，フレッツ網と衛星回線 2 種類（JSAT，IPStar）の，3 種類の回線を用意した．フレッツ網および衛星回線の対向地から先は，商用 ISP 経由でインターネットへの到達性を確保した．

フレッツ網では L2TPv3 による Layer 2 トンネリングを行い，合宿地と StarBED を接続した．衛星回線では，衛星の対向地である神戸情報大学院大学から OpenVPN を用いて StarBED とトンネリングを行った．どちらも StarBED から JAIST 経由で WIDE BackBone（WIDE-BB）へと抜けるようにした．

フレッツ網からのインターネット接続に用いた商用 ISP サービスでは, IPv4 Internet には PPPoE にて接続し，IPv6 Internet には IPoE 上で DHCP-PD を受けて接続した．アドレスは，global IPv4 address 1 つ (動的アドレス) と global IPv6 adddress /56 (2409:251:9140:10::/56) 空間が割り当てられた．

3.2 Layer 3 構成

合宿地ネットワークの Layer 3 構成を図 1 に示す．

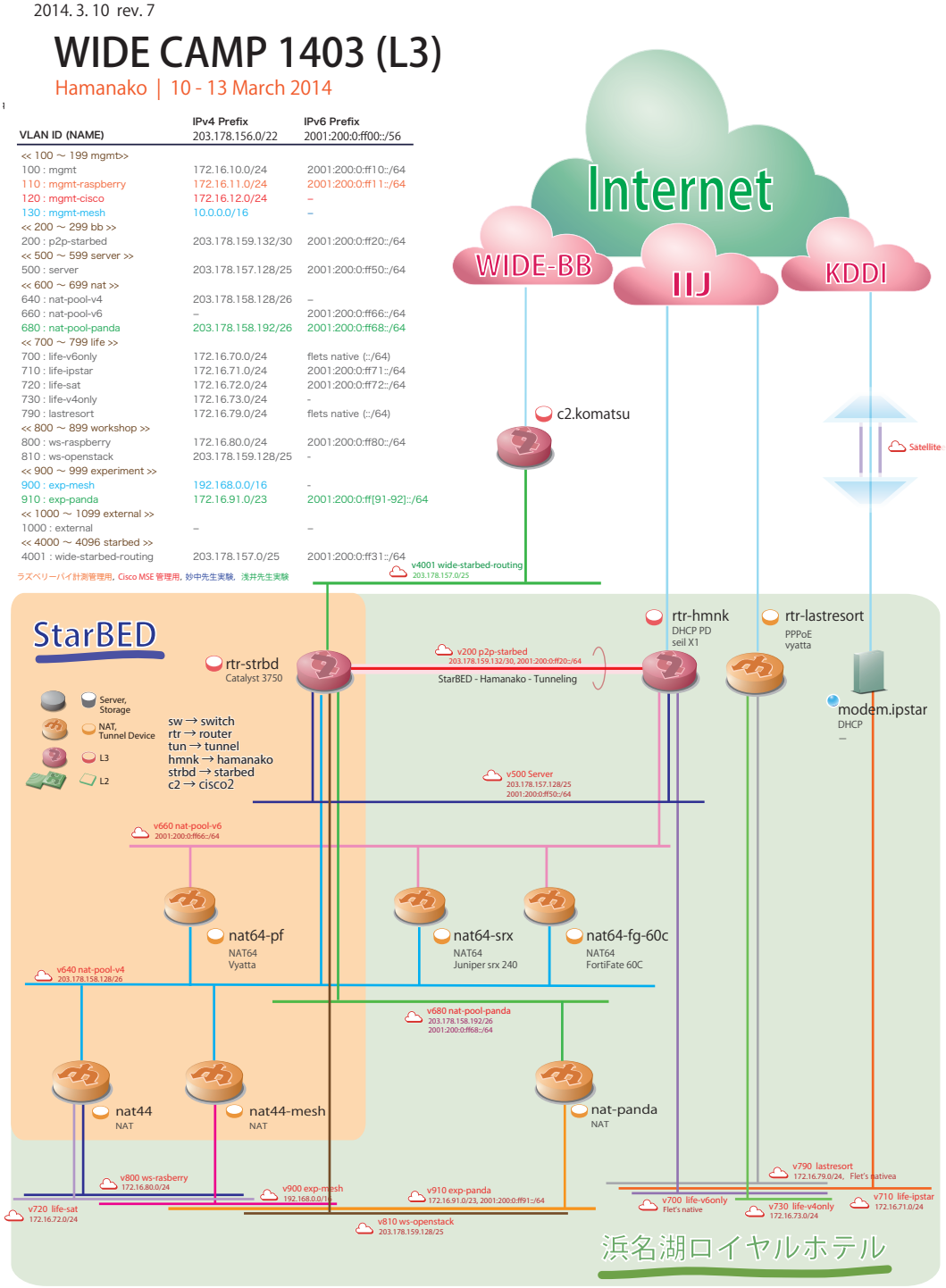


図 1　2014 年度 WIDE 春合宿ネットワーク Layer3 概要

3.2.1 設計概要

今回の合宿では，WIDE の 合宿用 address 空間 (203.178.156.0/22, 2001:200:0:ff00::/56; camp-prefix) に加えて，フレッツ網でのインターネット疎通性確保のために契約した ISP から割り当てられた adddress 空間 (動的 IPv4 アドレス 1 つ，2409:251:9140:10::/56; IIJmio-prefix) も利用した．camp-prefix は，主に合宿地ネットワークの基幹サーバ群および各種実験用途に使用した．IIJmio-prefix の IPv6 アドレスは合宿参加者がインターネットに到達するためのセグメント (生活線セグメント) にて使用し，IPv4 アドレスは，合宿地での基幹サーバ群の故障や WIDE-BB 内で障害が発生した場合を想定して作成した last resort セグメントにて使用した．

合宿ネットワークにおけるルーティングを行うため，3 つのルータを設置した．1 つ目は StarBED 内に設置した rtr-strbd である．今回は StarBED と L2 フラットな設計を行ったため，L3 は StarBED で提供し，合宿地には L2 のみを持ち込むという原則で設計した．しかし，IPv6 のルーティングに関しては現地で行うことにしたため，IPv6 ルーティングを行う rtr-hmnk を合宿地に持ち込んだ．3 つ目は IPv4 ルーティングを行う rtr-lastresort である．合宿地ネットワーク内のすべてのサブネットは，これら 3 つのルータのいずれかを gateway として持つように構成した．

camp-prefix に関する WIDE-BB 内での経路広告は，cisco2.komatsu (c2.komatsu) にて行った．すなわち，c2.komatsu にて camp-prefix を rtr-strbd に向ける static route を設定し，それらを WIDE-BB 内の OSPF にて redistribute した．

3.2.2 生活線セグメント

今回の合宿では，生活線として IPv6 only セグメントである life-v6only，衛星の JSAT を利用した life-sat，衛星の IPStar を利用した life-ipstar．そして障害が発生した際に利用するセグメントとして lastresort を提供した．

IPv6 only のセグメントでは，IIJmio-prefix の IPv6 address を用いて IPv6 only network を構成する一方で，IPv4 Internet への疎通性を持たせるために NAT64 を設置した．NAT64 は OpenBSD に実装された pf (Packet Filter) によるものと Juniper SRX240 , FortiGate 60C によるものの 3 つを用意した．いずれの NAT64 も camp-prefix 中の IPv4 address を 64 変換に用いるよう設定し，生活線利用者が WIDE-BB 経由で IPv4 Internet に到達出来るようにした．

生活線セグメント内から IPv4 Internet へのアクセスは，ラウンドロビン式に 3 つの NAT64 に分散させてロードバランスを計った．すなわち，DNS64 が補完する IPv6 prefix を 3 種類用意し，それらをラウンドロビン式に問合わせ元のユーザに返すようにする．加えて，それらの IPv6 prefix と NAT64 とを紐付けする static route を rtr-hmnk に設定することで上記ロードバランスを実現した．しかし，ラウンドロビン式だと特定のパケットだけ通らない際に，どの NAT64 に問題があるのかの切り分けが難しいため，時間によって DNS64 で返す prefix を制限し，SRX240 のみや FortiGate 60C のみの時間も作った．

JSAT を利用するセグメントでは, IPv4 のみの提供とし，DHCP や NAT なども全て StarBED 上のサーバーで提供した．life-sat のパケットは JSAT を通り神戸情報大学院大学に届き，そこから OpenVPN で StarBED まで運ばれ, そこで NAT されて WIDE-BB に抜けるようになっている．

IPStar を利用するセグメントでは，IPv4 のみの提供とし，DHCP や NAT などは全て IPStar のモデムで行った．life-ipstar のパケットは IPStar を通り商用 ISP に抜けるようになっている．つまり StarBED と合宿地のトンネルや WIDE-BB に障害が発生しても利用可能になっている．

3.2.3 実験用セグメント

今回の合宿では, 実験に関連する三つのサブネット群を用意した．一つ目は無線 mesh ネットワーク実験用に用意した exp-mesh である．StarBED にて

提供する nat44-mesh を G/W とする private IPv4 address 空間を用いて構成した．二つ目は自作ソフトウェアルータの評価実験の exp-panda である．ユーザのアクセス線となる IPv4 ・IPv6 ネットワーク，NAT 変換後の IPv4・IPv6 のバックボーンの合計四つのサブネットを用意した．三つ目は Net-PC の実験であり，OpenFlow による経路制御を間に挟んだネットワークである life-v4only である．これらは rtr-lastoresort を G/W としたシンプルな構成にて提供した．また，このセグメントは JSAT を通して神戸に提供されており，神戸の学生らが衛星を通してインターネットに抜ける実験にも利用された．

3.3 Layer 2 構成

合宿地ネットワークの Layer 2 構成を図 2 に示す．

3.3.1 設計概要

合宿地ネットワークは大きく分けて (i) 合宿参加者が利用する生活線セグメントと (ii) 合宿地基幹サーバが接続するバックボーンの二つの部分から構成される．(i) については合宿地会場の各部屋ごとに設置した Layer2 スイッチから利用できるように，(ii) については StarBED に置いたサーバと合宿地のサーバを共に同じセグメントに所属させ，migration しても意識せずに利用できるような構成をとった．

また，合宿地における生活線セグメント及び実験セグメントは，全て無線ネットワークとして合宿参加者に提供された．

3.3.2 Layer 2 トンネリング

3.1 節で示したとおり，合宿地ネットワークは，フレッツ網経由では L2TPv3 を利用して StarBED と Layer 2 トンネリングを行った．その際，vlan タグも通せるように設定し，StarBED と合宿地のどちらに置くかを意識せずに利用できるようにした．また，L2TPv3 は IIJmio-prefix の IPv6 でトンネリングを行い，PPPoE で取得する IPv4 は用いなかった．JSAT 経由の回線上では OpenVPN を用いて StarBED と Layer 2 トンネリングを行った．フレッツ網・衛星共に, StarBED から JAIST の c2.komatsu を通って WIDE-BB と接続した．

3.3.3 vlan ID 設計

合宿地ネットワークを構成するサブネットは 9 つのカテゴリに分類して vlan ID を割り振った．すなわち，(i) 合宿地ネットワークの管理に用いるサブネット，(ii) 合宿地のバックボーンを構成するサブネット，(iii) 合宿地の基幹サーバに用いるサブネット，(iv) nat64 変換のアドレスプールに用いるサブネット，(v) 合宿参加者のアクセス線に用いるサブネット，(vi) 合宿ワークショップで利用するサブネット，(vii) 実験に用いられるサブネット，(viii) 対外接続に用いるサブネット，(ix) StarBED で利用されるセグメントである．これら 9 つの分類は図 2 に示す通り vlan ID の百の位と千の位を区別することで行った．

3.3.4 無線チャネル設計

本合宿では，Cisco Wireless LAN Controller5508 と Aironet2602i 20 台にて campnet 無線 LAN を構築した．AP20 台のうち 6 台が通信を提供し，残り 14 台は位置情報等のモニタリング専用で利用した．SSID は実験者からの要望により，以下を 7 つを提供した．

- life-v6only (生活線)
- life-ipstar (上流を IP Star とする生活線)
- life-sat (上流を WIDE の衛星回線とする生活線)
- lastresort (camp-pc 用の臨時線)
- ws-raspberry(WS 利用．WS 部屋の AP のみ)
- ws-openstack(WS 利用．WS 部屋の AP のみ)
- exp-panda (実験利用)

camp-net では，2.4GHz 帯の ch1 と 5Ghz 帯の W52 および W53 を利用した．周波数帯は全て 20Mhz 幅運用とした．2.4GHz 帯は実験との関係で 1 チャネルしか確保できなかったため，5GHz 帯に端

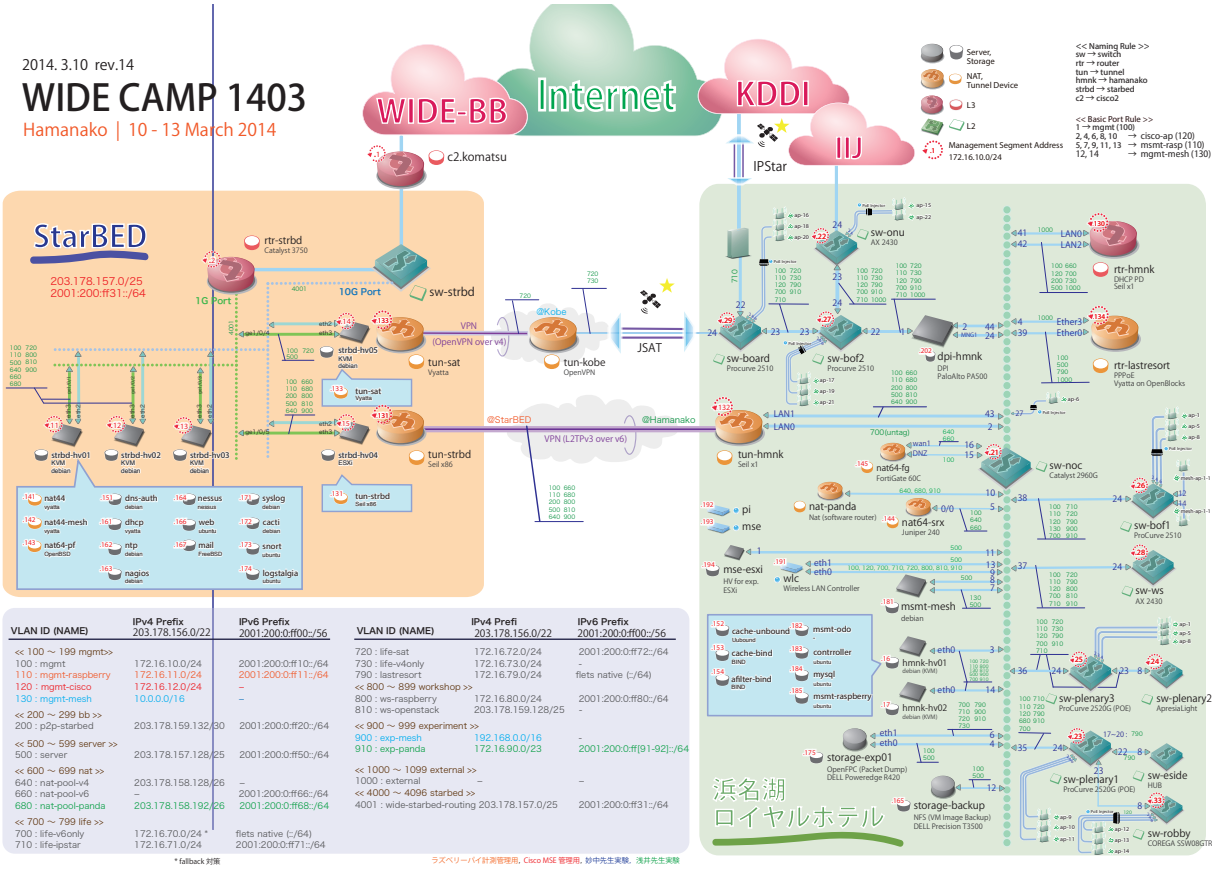


図 2　2014 年度 WIDE 春合宿ネットワーク Layer2 概要

末を誘導する調整を行った．5GHz 帯への誘導のため，BandSelect 機能を有効にし，5G の電波が 2.4G よりも強く端末に到達するように送信出力を調整した (5G をレベル 2，2.4G をレベル 4 に設定)．最低通信レートは 2.4G が 11Mbps，5G を 12Mbps とした．

3.4 サーバ構成

今回の合宿では，原則として StarBED 上にサーバーを構築し，一部のサーバーのみを合宿地の物理マシン上に構築した．StarBED 上のサーバーは，合宿地のルーターとの間で L2TP/IPsec による VPN を構築し，フラットな L2 ネットワークを利用できるようにした．これにより HotStage 期間中に構築した環境を，対外線の IP アドレスに関する部分を除きそのまま移行することを可能にしている．

StarBED の物理マシンは 4 台存在し，2 台をそれぞれ衛星経由，有線経由の VPN トンネルとして使用し，残りの 2 台をマスターとバックアップの Hypervisor として使用した．マスターの Hypervisor 上では，DHCP，ntp，syslog などの基幹サービスを担う基幹サーバー群を仮想マシンとして構成し，StarBED 上のバックアップと，合宿地の物理マシン上にバックアップを随時行うことで，トラブルが生じたときに早期復旧が可能となる．

原則として StarBED を用いたが，遠隔地に置くことで不都合の生じるサーバー群については，合宿地の物理マシン上に Hypervisor を構築し，その Hypervisor 上に仮想マシンとして構築した．実験の計測データを格納するサーバー群については，大容量のストレージを必要とすることと対外線の帯域への負荷の大きさを考慮し，合宿地の Hypervisor 上に仮想マシンとして構築した．また DNS キャッシュサーバーについても，一度 VPN を経由して StarBED との往復を行うとキャッシュサーバーの利点である応答速度がスポイルされるため，同じく合宿地の Hypervisor 上に構築した．

3.5 Layer 0/1 構成

合宿地の物理構成を図 3 に示す．浜名湖のホテルでは，各部屋の電源電圧の容量が小さく，合宿参加者に電源を提供するために拡張電源を追加した．また，床電源は合宿参加者が蹴つまずくことが多く，机の下に位置させることが好ましい．前回同様，無線 AP は位置情報取得用，通信用，実験の Raspberry Pi を設置するため，各所に UTP を延ばした．扉の下に UTP を這わす際，人の出入りが多いことを考慮せず配線してしまったことは反省すべき点である．

4 計測・可視化活動

今回の合宿では，大きく分けて運用用途と合宿 PC 実験用途とでの二種類の計測活動を Net-PC で行った．

4.1 運用用途での計測活動

運用用途では (i) 対外接続・基幹スイッチ群の死活監視と基幹サーバ群の死活/ サービス監視，(ii) SNMP ベースでの合宿地ネットワークの監視・可視化，(iii) DPI によるネットワークの計測，(iv) Snort によるネットワーク不正侵入検知を行った．

まず (i) について，合宿地ネットワークで生じた障害をいち早く検知するために，WIDE-BB へのトンネリング及び基幹スイッチ群の死活監視，基幹サーバ群の死活 / サービス監視を nagios により行った．監視した基幹サービスとしては，ntp，DNS，HTTP 等がある．

また，(ii) については合宿地ネットワークの状態推移を監視するために，SNMP ベースでネットワーク機器の監視を行い，それらを cacti で可視化した．監視項目としては，セグメントごとの帯域消費の推移，CPU 負荷，メモリ消費量等である．具体例として，図 4 には 3/10 午前から 3/11 午前にかけての合宿地ネットワークの StarBED における G/W router のトラフィック量を示してある．

(iii) については，NTT-AT 様が提供してくださった DPI をネットワークの上流にインラインで設置し，流れる全てのトラフィックの計測を行った．cacti では各セグメントごとのトラフィック量も計測することができないが，DPI ではセグメントごとのトラフィックに加え，利用されているアプリケーションの種類も判別することができる．図 5 には 3/13 の 9 時から 3/13 の 10 時にかけての合宿地ネットワーク

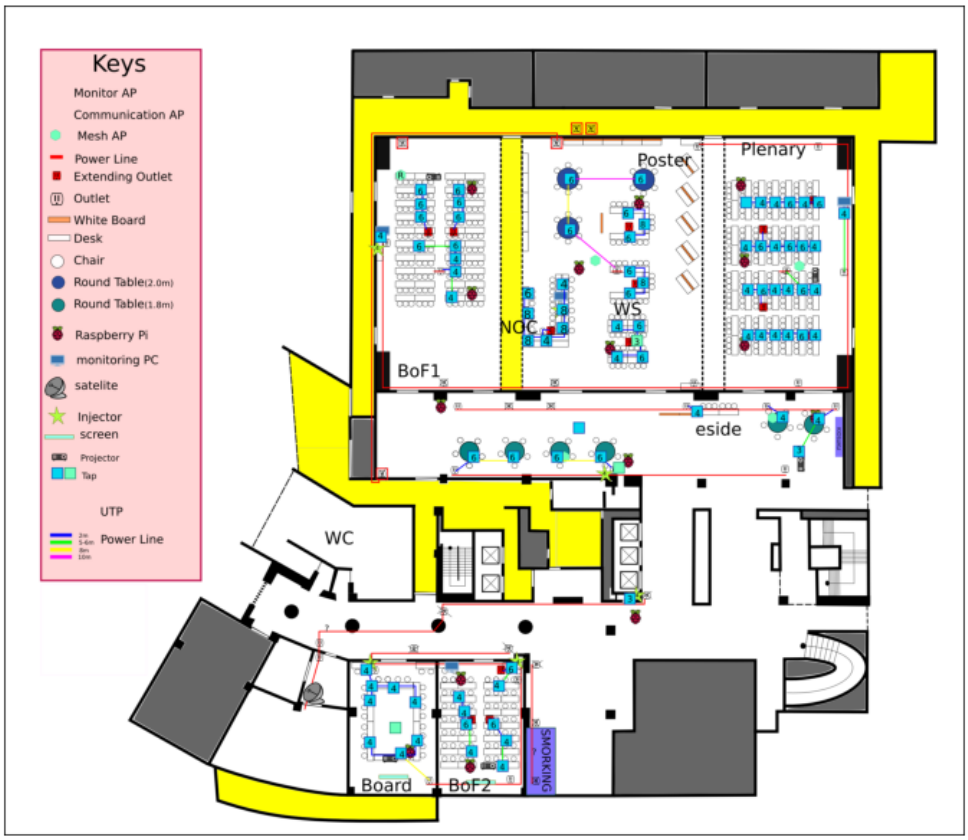


図 3　合宿地物理構成

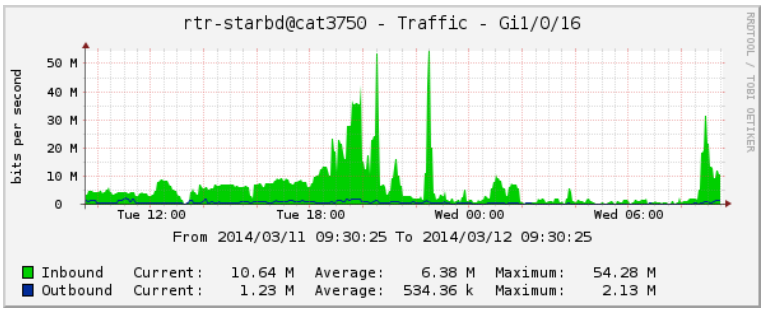


図 4　cacti による合宿地トラフィックの可視化

の vlan ごとのトラフィック量を，図 6 には 3/13 の 9 時から 3/13 の 10 時までの間で利用されたプロトコルを多い順に示した．

最後に，不正侵入検知システムである Snort の可視化ツールである Snorby を用いて，合宿ネットワークにおける不審なトラフィックを監視した．Snorby では不正なアクセスの件数をグラフ化し，詳細な内容をランキング形式で表示する．図 7 には 3/13 の合宿地ネットワーク内の不正な通信を示してある．これらのグラフは Web から見られるようにし，更に daily report として毎日 24 時にメールを送信するようにした．

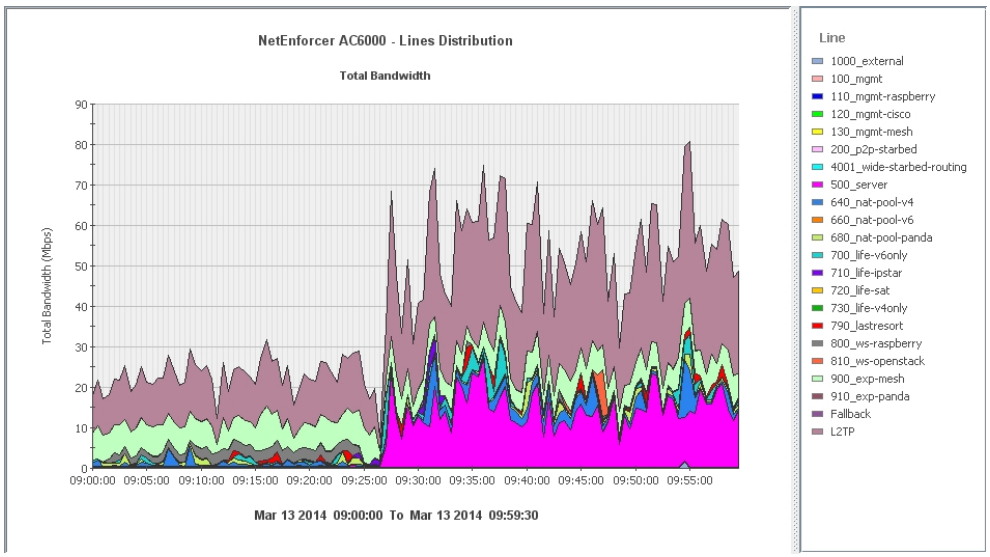


図 5　DPI による合宿地トラフィックの vlan ごとの可視化

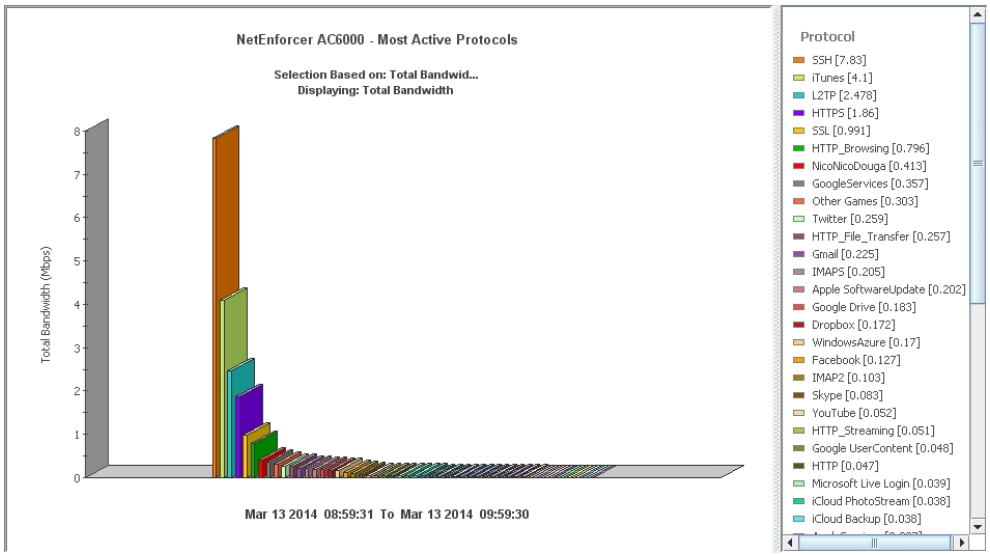


図 6　DPI による合宿地トラフィックのプロトコルの可視化

4.2　合宿 PC 実験の計測活動

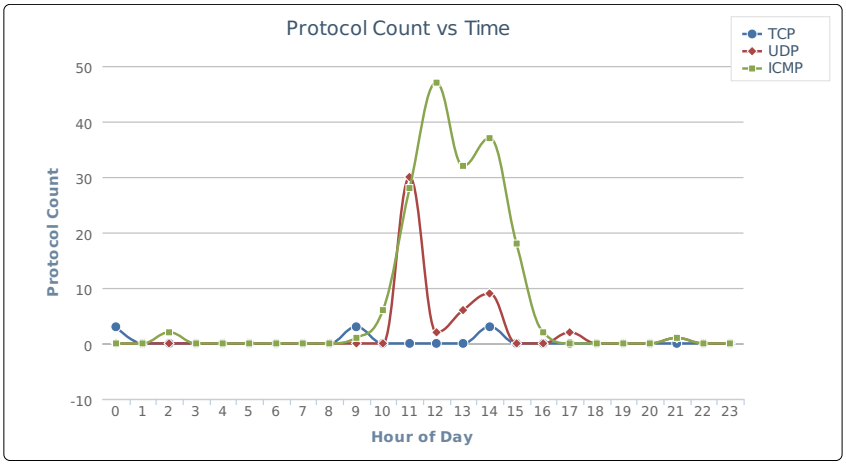
Camp-1309 から行っている「行動履歴の解析」の流れを汲んで，今回も合宿地ネットワークの traffic fulldump の計測を行った．

合宿地ネットワークの traffic fulldump は，合宿参加者が利用する生活線セグメントに対して行った．具体的には，NOC 内のスイッチにて生活線セグメントの vlan に対してミラーリングを行い，プロミスキャス・モードに設定した NIC をもつサーバにて OpenFPC を用いて dump file を生成した．

なお，合宿参加者の屋内位置情報の計測を実験にて行った．それらの詳細は，6 節を参照されたい．

Protocols

TCP Count	UDP Count	ICMP Count	Total
9	50	174	233



Top 15 Signatures

Signature Name	Percentage	Event Count
ICMP PING	66.95%	156
SNMP request udp	16.31%	38
WEB-PHP Setup.php access	3.86%	9
SNMP public access udp	3.43%	8
ICMP Destination Unreachable Network Unreachable	3.0%	7
ICMP PING NMAP	3.0%	7
SCAN UPnP service discover attempt	1.29%	3
ICMP Destination Unreachable Port Unreachable	0.86%	2
ICMP Echo Reply	0.43%	1
ICMP Destination Unreachable Communication with Destination Ho...	0.43%	1
MS-SQL ping attempt	0.43%	1

Top 10 Source Addresses

Source IP Address	Percentage	Event Count
203.178.157.172	16.3%	30
184.105.139.67	8.7%	16
204.11.51.59	8.15%	15
218.159.146.126	7.61%	14
12.129.199.100	6.52%	12
64.38.240.2	4.89%	9
12.130.81.230	4.89%	9
74.217.78.143	4.89%	9
74.217.78.144	4.89%	9
64.38.212.35	4.89%	9

図 7　Snorby による不正侵入検知

5　収集データの共有方法

Camp-1309 では，合宿 PC 企画として「行動履歴の解析」セッションを執り行うために，4.2 節で述べた収集データを合宿参加者で共有が必要となったが，前回はデータ収集の枠組みを整えたが，共有方法は十分ではなかった．本節では Camp-1403 で提供した共有方法について述べる．

収集データは，大きく分けて (i) ファイル形式のものと (ii) RDB 中のテキスト情報に分けられる．具体例を挙げると，前者は traffic dump ファイルであり，後者は Cisco MSE で収集した位置情報である．

まず，トラフィック情報を合宿参加者で共有するために，OpenFPC を用いた．OpenFPC はオープンソースのパケットキャプチャツール群である．今回は OpenFPC の機能の 1 つである Web UI を用いて，収集した dump file を合宿参加者へリアルタイムに共有する仕組みを提供した．OpenFPC により dump file の一部をフィルタリング，pcap file としてダウンロードすることが可能となり，利用目的に応じた収集データの柔軟な提供を実現した．OpenFPC 利用に際するユーザ名とパスワードは dump file 利用希望者のみに発行し，適切なアクセス管理を行った．

次に位置情報データの共有のため，CiscoMSE の WebAPI からデータを取得して DB に格納し, HTTP サーバにて提供した．公開したデータは以下の通り．

- real-time location
  最新の位置が取得できる．24 時 間以内に active だったものは最後に track された場所が記録される．
- history
  過去に遡って検出された位置．10m 以 上動いたと検知されるたびに情報が更新される．

ただし，収集した情報のなかには，traffic dump や参加者の MAC アドレスのようなセンシティブな個人情報を含むものが少なくなかったため，利用希望者のみ配布する形式にした．上記ページにアクセスするためには専用ユーザとパスワードの入力を必須とし，収集データを利用したい合宿参加者から合宿 PC に問い合わせした際に個別にパスワードを配布した．

6　合宿地における実験

今回の合宿では，6 件の実験が行われた．

6.1　実験概要

今回の合宿では，以下に挙げる実験が合宿地ネットワークにて行われた．

1. 新しい無線メッシュネットワークのベンチマーク
2. 無線ネットワーク状態の可視化実験
3. 無線 LAN インフラによるクライアント位置情報取得実験
4. 自作ソフトウェアルーター
5. IPv6 実験
6. 赤外線マルチホップ通信

6.2　新しい無線メッシュネットワークのベンチマーク

複数チャネルを並列に利用する事で通信容量の拡張を可能とする無線メッシュネットワークを試験した．利用した要素技術は Wireless Internet ワーキンググループの報告書で説明した．また，実験結果については，国際会議で発表された原稿 [1] を参照されたい．

6.3　無線ネットワーク状態の可視化実験

本実験については北口らによる論文 [2] を参照されたい．

6.4 無線 LAN インフラによるクライアント位置情報取得実験

前回（2013 年 9 月）の WIDE 合宿に続き，Cisco MSE（Mobility Service Engine）による無線 LAN 端末の位置取得実験を行った．前回の実験では取得した位置と実際の位置との差に関する情報が不足していたため，今回は事前に観測用の固定 raspberry pi 端末の実際の位置を記録し，検出位置との差を把握することにした．実験トポロジと検出データを図 8 に示す．不明な原因により，図面上部のホール周辺のデータが左に寄るトラブルに遭遇した．合宿期間中に原因が判明せず，このエリアの検出データは不正確である．図面下部の会議室周辺では，この傾向は現れず正常に検出できた．

図 8 の矢印に示すとおり，全体的に検出位置は実際の位置より数 M 離れて（ずれて）おり，その周辺で分散していることが分かった．この実際位置から離れる”ずれ”が，本実験での測定精度である．MSE は端末の周辺に AP（受信機）を配置し電波強度によって位置推定を行っているが，今回の実験環境（建物内の電波環境と AP の設置密度）では，このような精度になった．実際位置と検出位置の関係を図 9 に示す．測定精度の限界により実際位置と検出位置には ” ずれ ” が存在し，検出位置はリアルタイムの環境変化の影響も受けて誤差の範囲で広がる．このように，今回の実験により，検出データの精度と傾向を把握することができた．今後は，この情報をもとに応用を検討する予定である．

6.5 自作ソフトウェアルーター

In this experiment, we had tested a developing networking operating system called PIX (Packet-based Information Chaining Service) designed and implemented from scratch. This operating system implements basic IPv4 and IPv6 routing and two experimental network functionalities for this experiment: 1) Unicast IPv6 router advertisement, and 2) NAT66-like functionality that force disables IPv6 privacy address extension. The former has been discussed in IETF v6ops WG to avoid frequent multicast RA delivered to mobile devices for battery saving. The latter is a quite odd functionality that translates the source address suffix for outgoing packets and inserts an entry to a translation table for the reverse translation of the destination address of incoming packets. This functionality enables incident tracking without client address logging schemes, and might be useful for operators. Through this experiment, we confirmed all the functionalities had been stably working for three days without any troubles and performance degradation. Currently, the APIs of PIX are not much sophisticated and requires almost same implementation cost as POSIX applications for these functionalities. We will discuss and design notable new APIs for network functionalities.

6.6 IPv6 実験

3.2.2 節で述べたように，前回に引き続き DNS64/NAT64 を Camp Net にて提供した．また，DPI による NAT64 トラフィックの計測は 4.1 節を参照されたい．

6.7 赤外線マルチホップ通信

本実験では，新規に開発した赤外線マルチホップノードの動作実験を行った．自由空間光通信は近年，そのメディアの特性，セキュリティ・帯域・デプロイコストの観点から注目が集まる通信方式である．現在のところ既設の電灯を活用した可視光通信の分野において活発に研究開発が行われている．

われわれは，光通信のもう一つの特徴であると言われる，遮蔽に関する特性を研究するために赤外線を用いた光通信ノードを開発した．自由空間光通信

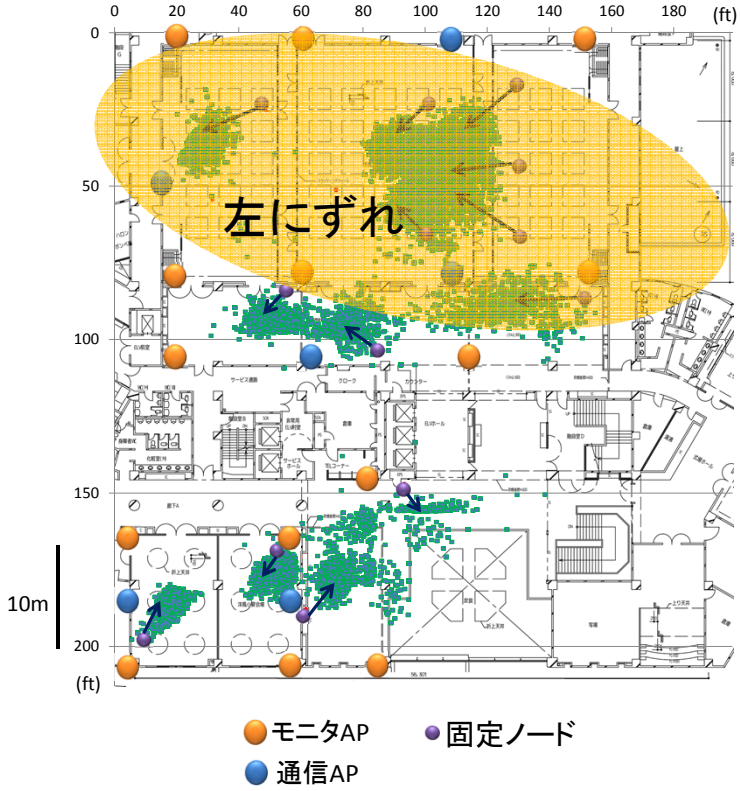


図 8　実験トポロジと検出データ

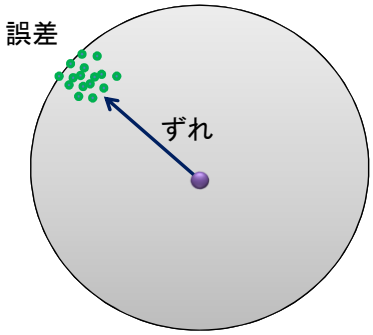


図 9　実際位置と検出位置の関係

においては，壁面や床面での反射により伝搬距離が変化するが，実空間，特に建物においての実験例は少ない．本ノードを用いてこれらの特性を明らかにする．

WIDE 実験では，第一回目の実験としてノウハウの蓄積を目的とした．ノードに対してフラッディングベースのマルチホップ通信を行うファームウェアを搭載し，7 台のノードを一本の線路として，伝搬特性が環境によってどのように変化するかを調査した．実験結果については現在，解析を進めている．

7 Net-PC の運用

2 節で示したとおり，今回の Net-PC のテーマとして「教育」と「引き継ぎ」をテーマに掲げた．hotstage の期間は 1 週間と短く，必然的に既に知識のある PC メンバーがコア構築に携わることになり，知識のない PC メンバーが構築に携わりにくいという現状がある．そのため，一部の PC メンバー以外は得られる知識が少ない．複数回 Net-PC に参加したにも関わらず，ネットワークの知識が身についていないという声もある．また，過去の構築の際の情報の蓄積が次回以降の Net-PC に引き継がれていない点も問題である．過去の PC メンバーが次回にも参加して口頭で伝えているため，PC メンバーの卒業により蓄積が失われてしまう．

そこで今回の合宿では，StarBED を用い合宿の一ヶ月以上前から構築を始めることで，経験のないメンバーが時間をかけて構築できるようにした．また，通常は時間がなく構築の知識を文書化することが出来ないが，今回は時間をとって全サーバーの作業記録を残すようにした．これらを次回以降に引き継ぎ更新していくことで，より迅速な構築が可能になると考える．

また，技術の共有も可能な範囲で行うように心がけた．今回は Hypervisor を KVM で構築したが，それらの知識がないメンバーのために Skype による勉強会を開き，bridge の設定方法や VM の作成方法を共有した．hotstage 期間にはスイッチの設定方法が分からない PC メンバーに vlan の仕組みを伝え，実際に設定を行ってもらった．

8 考察 / 今後の課題

合宿ネットワークの構築や運用の過程で得られた知見や課題を以下に述べる．

8.1 対外線契約

対外線契約をするのが前泊からであるため，対外線の設定が合宿地に行ってからしかできないのは改善の余地があるように感じた．今回は前泊で PPPoE にて IPv4 が取得できず，ルータの設定などの見直しに時間をかけたが，結局 PPPoE のサービスが開始されていなかったことに起因していた．同様に Camp-1303 でも IPoE の契約が間違っていたために IPv6 が一つしか取得できないなどのトラブルがあった．hotstage の設定のまま機材を持ち込んでも動作しないため，前泊での作業が多くなってしまう．それらを防ぐため，hotstage 会場でも同様の対外線を契約する，もしくは合宿地で先に契約をしておいてトンネリングにより hotstage 会場で合宿地と同様の環境で作業が行えるようにするなどの解決策が考えられる．

8.2 運用

今回は可能な範囲で多人数への仕事の分担を試みたが，多人数に仕事を分散することの問題点として，全員の進捗を確認することが困難であることが挙げられる．この問題を解決するため，今回は trac のチケットの進捗度合いをガントチャートで可視化した．図 10 のように進捗具合がグラフになり，期限までに進捗が遅れているチケットは赤く，順調に進んでいるチケットは青く表示される．この可視化により，効率的に各メンバーの進捗を管理できた．このような進捗管理を準備期間だけでなく hotstage 期間も行うことで，より仕事を分担して作業が進めることが可能であると考えられる．

また，今回は経験の少ない PC メンバーもコア構築に携わってもらったが，その結果必要な vlan を消してしまったりといった重大なオペレーションミスが発生してしまった．人単位で仕事を割り振るのではなく，経験のある PC メンバーと経験のない PC メンバーをチームにして，チーム単位で仕事を割り振るといった解決策が考えられる．

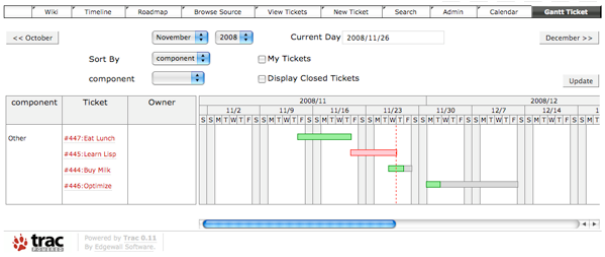


図 10　trac のガントチャートによるチケット進捗の可視化

8.3　障害

今回の合宿前半では，Web の閲覧などに非常に長い時間がかかるという現象が多くの参加者より報告された．原因は大きく分けて二つあった．まず１つ目は，合宿地を抜ける際の速度には問題がなく，バックボーンで遅延が発生しているというものであった．これは WIDE バックボーンでオペレーションミスが発生し，海外を経由してしまっていることが原因であった．合宿地での問題と考え調査を進めていたため，原因究明に時間がかかってしまった．

１つ目の問題が解決されたあと再度遅延が発生した．報告を受けて調査したところ，スループットは十分に高いが, 外部サーバへの往復遅延時間が非常に大きいことが判明した．このような現象は hotstage では見られなかったため，原因究明は困難を極めた．最終的には，NTT 東日本から提供されたホームゲートウェイの故障が原因であり，これを経路上から取り除くことで問題は解消された．

今後の対策として，問題の原因を幅広く考えること，またあらかじめ提供された機器や設置された機器を使う場合にも，十分な検証作業を行うべきであると言える．特に，対外線に関する作業は合宿地でしか行えないことを踏まえると，十分に検証作業を計画するべきであるし，障害に備えて衛星回線などを準備することは非常に有意義であると結論付けられる．

9　まとめ

今回の合宿での Net-PC の活動は，合宿参加者に安定したネットワークを提供する取り組みに加えて，Snorby や OpenFPC などの過去に合宿で利用経験のないサービスの利用を試みた．セキュリティ面では Firrewall を複数台使用し，Nessus などの脆弱性スキャナも用いることで堅牢なネットワーク構築に注力した．また，それらを OpenFlow と組み合わせることで SDN との融合をはかった．

行動履歴の収集にあたっては，位置情報，トラフィック，様々なデータの収集をするだけでなく，収集したデータを合宿参加者に共有する仕組みを整えた．

Net-PC の運用の観点では，今一度運用方法を見直し，参加した Net-PC 全員にとって有意義になるような方法を模索した．

今回は，様々な新しい試みを行ったため，今後はそれらの迅速な構築と安定した運用を目指す次第である．

参考文献

[1] Y. Taenaka, M. Tagawa, and K. Tsukamoto. Experimental deployment of a multi-channel wireless backbone network based on an efficient traffic management framework. In *Proceedings of the 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 3PG-

CIC '14, pp. 579–584, Washington, DC, USA, 2014. IEEE Computer Society.

[2] 北口善明, 石原知洋, 高嶋健人, 田川真樹, 田中晋太朗. Raspberry pi を用いた無線ネットワーク状態評価手法の提案. 情報処理学会研究報告. CSEC,[コンピュータセキュリティ], 2014(8):1–6, 2014.