第19部

先端技術研究会の開催および研究会用仮設ネットワークによる高度な実験運用

山内 正人、砂原 秀樹、岡田 光代
山内 正人、横山 輝明、鈴木 恒平、CampPC1809一同

第１章　2017年12月WIDE研究会

1.1　概要

本稿では2017年12月16日に慶應義塾大学三田キャンパスの東館4階セミナー室及び三田東宝ビル4階で開催された2017年12月WIDE研究会について報告する。

1.2　実施体制及びテーマ

2017年12月WIDE研究会は例年と違い1日のみの開催とし、またProgram Comittieも3名での実施とした。
時間も限られることからテーマもWIDEにおけるセキュリティーに絞り実施した。

1.3　プログラム概要

プログラムは大きく分けると午前中にBoF及びワークショップを配置し、午後はプレナリのセッションとした。

午前中は9:00-9:50, 10:00-10:50, 11:00-11:50の3スロット用意し、東館4階セミナー室では3スロット使用して「SINDAN Hackathon」が実施された。三田東宝ビル4階では 9:00-9:50 で「Migration NSPIXP-3 OSAKA to FAUCET Umbrella」が実施され、10:00-10:50及び11:00-11:50の2スロットを使用して「Traffic information ttestbed@WIDE」が実施された。午後は三田東宝ビル4階でプレナリセッションを実施し、13:00-15:00のスロットで「moCAの今後」についての議論を行い、15:00-17:00のスロットで「WIDEインターネットとセキュリティ対応」について議論した。のべ40名程度参加し、特に午後に実施した「moCAの今後」及び「WIDEインターネットとセキュリティ対応」についてはその後の合宿や研究会においても継続的な議論に繋がっている。

第２章　2018年3月WIDE合宿

2.1　概要

2018年3月の合宿では、合宿の構成に関して大きく変える試みを行った。一つは、合宿において集中的に討議する話題を決め、シングルトラックで運営するプログラムを組み込むこと。もう一つは2泊3日の日程とし、集中的に議論をすることである。

そのため、前半の1泊2日をSecurity Dayとしてセキュリティに関わる議論を行うこととした。これは2017年8月に実施されたボード主催夏合宿からスタートした一連のテーマとして進めてきたものである。こうしたことを考慮して12月に実施された研究会においてもセキュリティの議論の中核に置いた。

合宿のSecurity Dayでは、より品質の高いインターネットを構築し提供することを目指し議論を行った。ここでの議題は、2.2、2.3に示した通りである。特に、「WIDEインターネットとセキュリティオペレーション」に関しては、WIDEとしてCSIRTを設置したことから、その役割と運用について議論を行っておりWIDE Incident Response Teamの活動を加速している。

後半の1泊2日は、WIDE Activity Dayとして3並列でBOFなどのセッションを行っている。

合宿の運用を少人数で行い、合宿の構成も大きく変えたため改善の余地はあるが、WIDE Projectとして集中的に研究開発を行うべきテーマを据え議論を行うことは必要であると考えられる。

2.2 3月6日 Security Day1

利用者認証とIdentity（moCA 2） Chair: 木村 泰司	IDとPasswordによる利用者認証が限界をむかえ、新しい利用者認証の検討が必要となってきている。ここではmoCA2としてWIDE Projectの中で運用するべき新しい利用者認証について議論した。
IoTセキュリティ Chair: 井上 博之	自動車におけるIoTの現状を紹介しながら、IoTセキュリティについて議論を行った。
セキュリティに関する標準化と国際連携 Chair: 門林 雄基	セキュリティに関連した標準について紹介をしながら、標準に基づく国際連携について現状を把握すると共に、WIDE Projectとしての体制を議論した。

2.3 3月7日(水) Security Day 2 / WIDE Activity Day 1

WIDEインターネットとセキュリティオペレーション Chair: 中村 修	WIDE ProjectのCSIRTであるWIRTの役割と体制を議論しながら、特に情報共有を核に据えてWIRTの活動体制に関する検討を進めた。
Block Chain技術とBASE Alliance Chair: 鈴木 茂哉	Block Chain技術に関する研究コンソーシアムであるBASE Allianceについて紹介しながら、WIDEにおけるBlock Chain技術に関する研究活動に関する議論を行った。

第３章　2018年5月WIDE研究会及び2018年9月合宿

3.1 概要

本稿では2018年5月25日-26日に慶應義塾大学大阪シティキャンパスで開催された2018年5月WIDE研究会及び2018年9月4日-7日にロイヤルホテル長野で開催された2018年9月合宿について報告する。5月の研究会及び9月の合宿における統一テーマとして「WIDEプロジェクトの活性化」を設定した。5月の研究会ではWIDEプロジェクトの活性化として、WIDE外の方も研究会へ参加可能とし、これまでWIDEへ触れる機会の無かった方へWIDEプロジェクトの活動をアピールしプレゼンスを高めた。9月の合宿ではknowhowを共有する企画等によりWIDEメンバーがWIDE内で活発に活動出来ることを目指した。

3.2 5月研究会

3.2.1 研究会の実施概要

本年の5月研究会は関西にて開催した。久しぶりの関西での開催ということもあり、関西のWIDE外のメンバー、特に関西の大学／高専／専門学校の教員や学生、企業の方なども参加できるようにWIDE外メンバーの参加を許した研究会とした。

研究会Webページ:
http://member.wide.ad.jp/meeting18spring/

開催日時と場所は、以下の通り。

2018年5月25日(金)・26日(土)
慶応大阪シティキャンパスグランフロント大阪
ナレッジキャピタル 北館タワー C 10階

3.2.2 プログラム内容

今回はWIDE外部の方を招いての講演（神戸デジタル・ラボ 村島 正浩さま、Panasonic 森田 智彦さま）、7つのセッション、2つのワークショップ、1つのBoFを開催した。その他、ポスター 3件、ブース出展3件があった。

3.2.3 実施結果

93名（WIDE 55名, WIDE外 38名）の参加者の参加があった。研究会両日のそれぞれの参加者数は下記となった。

25日：46名（WIDE: 37名, WIDE外: 9名）

26日：72名（WIDE: 44名, WIDE外: 28名）

3.2.4　アンケート結果

35名のアンケート回答があり、WIDE外の参加者からも高評価であり、今後もWIDE内外の交流を求める意見があった。また、大阪などの東京以外での開催を歓迎する声があった。ただし、従来型のWIDEメンバー向けの研究会としての機能（議論、発表など）を求める声もあった。2日間を目的に応じて分けるなどのバランスも重要だと考えられる。これらの結果から、東京以外やWIDE外メンバーも意識した研究会や他イベントの開催の価値を確認できた。

3.3　9月合宿のプログラム

「聞きたいセッションが被っていて聞けなかった」と言われるぐらい活発でワクワクするWIDE合宿を目標とした。セッションは一般的なプレナリセッションとBoFから構成した。プレナリでは新しい話題による知的好奇心を刺激するためBoard Plenary「5G世界に向けたWIDEの役割」、2017年12月研究会から継続的に議論している「WIDE CSIRTについて」、能動的に活動出来るようハンズオンを主体とした「BoF Development」及びその報告と表彰、密な議論を個別に行え毎回好評であるポスターセッションを配置した。

「BoF Development」はWIDEメンバーの広がりとともに各組織内でknowhowを共有する機会が少なくなってきていることを背景とし、面白いネタを(潜在的に)持っている人がBoF開催のknowhowも得ることでWIDE内で活発に活動出来るようにすることを目指しグループワークとしてネタ出しからBoFの開催まで実践する企画である。また、最終日に各BoFでの議論を報告すると共に魅力的なBoFを作り上げたチームへは表彰も行った。

BoFは3スロットパラレルで実施し、BoF Developmentで開発されたBoF8セッション及びProgram Comittieが予め企画した非WGのBoF5セッション、直近の合宿における公募型BoFスロットの稼働率をもとに全部で30スロット用意し97%のスロットが埋まった。

「IT野球盤と欺瞞防御」、「検証NW構築の方法を探るBoF」、「守りっこ BoF」、「ゲーミングセキュリティについて考えるBoF」、「ヘルスケアデータの解析と可視化(特に睡眠リズム)」、「自動化の自動化 BOF」、「Introduction to Quantum Computing & Quantum Networking」、「好きなことで生きていくBoF」がBoF Developmentで開発されたBoFとして開催され「Introduction to Quantum Computing & Quantum Networking」が魅力的なBoFに選ばれ表彰された。また「WIDE-WG」、「NetPC」、「英語論文の書き方」、「BSD」、「IP over デジタル放送」をPC BoFとして開催した。

台風による交通機関の影響や会場の停電等もあったが100名弱の参加があり、参加者からのアンケート結果で「興味のあるBoFが同じセッションで同時にやってる場合、その中の一つしか参加できないのはかなり悔しいと思いました」「いつもよりBoFの重複に苦しんだ印象。それだけ面白いBoFが多かったということでもあります」といった声が聞かれ、合宿プログラムの目標を達成できたと考える。

第４章　2018年9月WIDE合宿ネットワーク

4.1　はじめに

本稿では2018年9月4日（火）から9月7日（金）にかけて開催されたWIDE秋合宿におけるインターネット環境の設計・構築・運用結果および実験の結果について報告する。WIDE合宿期間中に会場内で提供されるネットワークはWIDE Project参加組織の有志によって設計・構築・運用されている。また、会場で提供されるネットワークは合宿参加者へのインターネット接続性の提供だけでなく、同時に実施されるネットワークを用いた実験のためのネットワークとしても機能している。

4.2　合宿ネットワークの設計

2018年秋合宿におけるネットワーク構成図を図1に示す。

会場ネットワークの設計はWIDEバックボーンとの接続を担う対外接続と内部で使用するネットワークの2つに大別することができる。内部ネットワークにはサーバを収容するセグメントと、来場者へのネットワークを払い出すためのセグメントと、各ネットワーク機器が単一セグメントに接続される管理用セグメントよって構築されている。来場者へのネットワークの払い出しはNAT64/DNS64を利用し

たIPv6アドレスのみで接続を行うセグメントと、従来のようにIPv4/IPv6デュアルスタックでアドレスを払い出すセグメントを準備した。

ネットワークの構築にあたっては、対外接続、内部設計、サーバ、セキュリティといった担当に分かれて議論を進めた。8月23日から26日にかけて慶應義塾大学湘南藤沢キャンパスで実施された事前検証期間中に、各グループで実装したソフトウェアやネットワーク設計をつなぎ合わせて、会場ネットワークを構築した。

4.3　ネットワークにおける挑戦

合宿ネットワークの構築に関しては昨年度までの踏襲があるが、今回はゼロからネットワークを設計したため、いくつかの点で昨年度までとは異なる構成をとった。本節ではその取組と昨年度までとの差異について述べる。

4.3.1　対外接続

2017年度までは合宿用のIPアドレスをWIDEProject藤沢NOCにて広報していたが、2018年秋合宿では、合宿用のIPアドレス帯をWIDE Project小松NOCにて広報した。また、対外接続のために、合宿地にて商用のISPを契約し、ISPから付与されたIPv6アドレスをアンダーレイとして、小松と合宿地の間でオーバレイネットワークを構築し、拠点間の接続を行った。

対外接続に用いるルータはLinux（Ubuntu16.04）をベースとしたPCルータをネットワーク構築チームにて自作した。PCルータは、WIDE Project小松NOCへのトンネル装置としての役割と会場内のルーティングを担う。トンネル装置としての役割を果たすうえでは、GREによってEthenetフレームをカプセリングし、小松NOCに設置したトンネル装置と接続させた。また、会場内のルーティングについては、IPv6アドレスの設定にRAおよびSLAACを用いるために、radvdを設定した。

4.3.2　無線接続

今回の合宿ではcamp wlan 2.4GHz、camp wlan 5GHz、camp wlan v6onlyの3種類のSSIDを提供した。camp wlan 5GHzおよびcamp wlan 2.4GHzではSSIDごとに周波

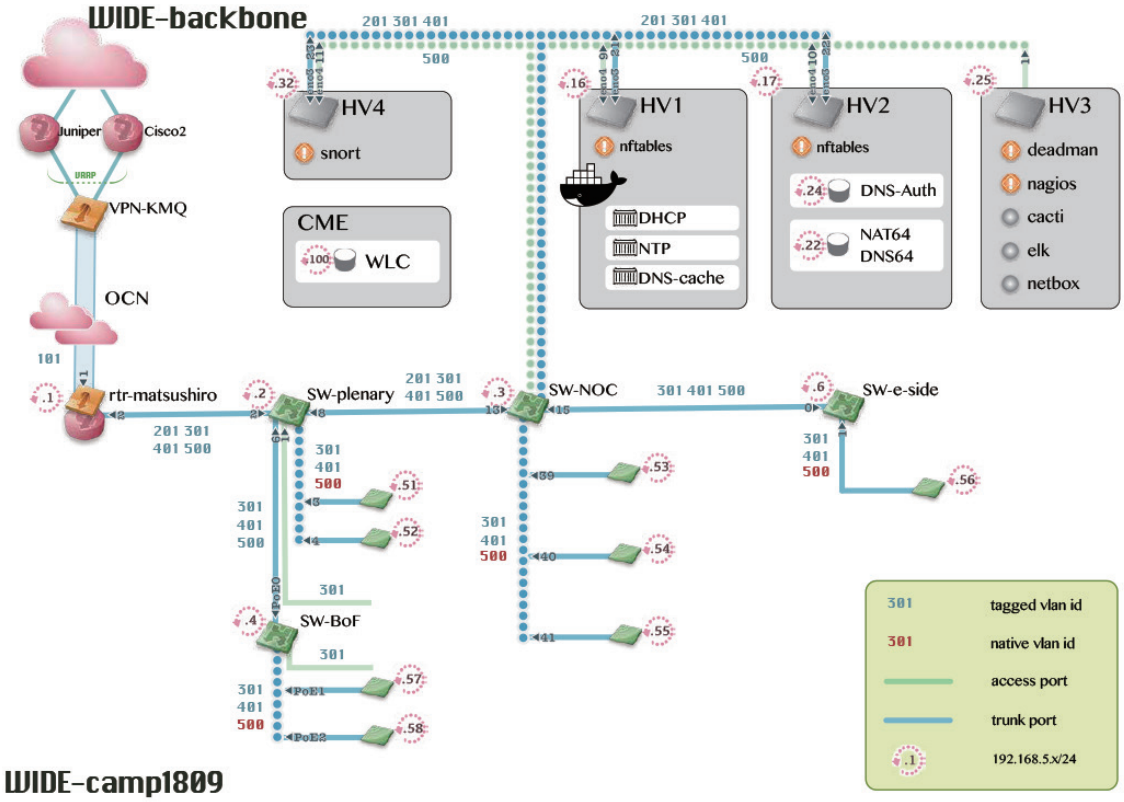

図1　2018年秋合宿のネットワーク構成図

数帯を分け、IPv4/IPv6デュアルスタックによるインターネット接続環境を提供した。また、camp wlan v6onlyでは先述したIPv6アドレスのみによるインターネット環境を提供した。

技術的な挑戦として、今回はQRコードを用いて該当するSSIDに接続できるように工夫を行った。また、今回はコントローラーを用いずに、シスコシステムズの提供する、Cisco Mobility Express（CME）[57] という技術を用いて無線接続環境を提供した。一般的な会場ネットワークはWireless LAN Controllerを用いて会場にあるアクセスポイントを管理するが、CMEを用いた場合、コントローラを用いずにAP間で自律的に設定を同期することができる。これを用いることで、会場に搬出する機材の量を減らし、準備、撤収における手間を削減し、無線ネットワーク運用の簡素化を行った。

4.4 コンテナ技術の応用

ネットワークを構築する上で必要となるDNSやDHCPなどのソフトウェアを、今回はコンテナ技術を応用して提供した。コンテナランタイムにはDockerを用い、基幹サービスのすべてをコンテナを用いて提供した。

4.4.1 ソフトウェアと連携した監視システム

会場内ネットワークの監視には、トラフィック、リソース使用率、会場内のサーバの死活監視を行った。従来まではこれらの監視パラメータはメールによって通知していたが、アラームの通知にはsys-logやSMNP等で入手した情報をElasticsearch、Logstash、Kibanaといったオープンソースソフトウェアを組み合わせて、特定のしきい値を超えたら通知を行うといったアクションを実施した。また、各ノードの監視にNetDataを用い、管理者が各ノードの情報を確認できるようにした。

4.4.2 セキュリティに関する取り組み

セキュリティの取り組みとして、Snortによる異常検知と、そのログから自動的に不審なIPアドレスを遮断するソフトウェアを実装した。IPアドレスの遮断のためにはsyslogに出力されたSnortのログを解析し、期間中における一定のしきい値を超えたIPアドレスを対象として、nftablesによってフィルタを設定し、遮断をした。

4.5 実験

今回の合宿では、合宿ネットワークを用いて2件の実験が行われた。6節および7節にて各実験の概要と結果を報告する。

4.6 ブロードキャストパケットを用いた端末OS推定データセット作成実験

岡田和也、関谷勇司（東京大学情報基盤センター）

4.6.1 概要

本実験は、端末が送信するブロードキャストパケットから、その特徴を利用して各端末のOS・バージョンを高精度で推定するために必要なデータセット作成を目的として実施した。昨今では、企業において個人の端末を持ち込むBYODが広く行われており、多種多様な端末・OSが混在する環境が一般的になっている。そのため、各人が所有する端末種別やOSの把握が困難になってきている。ネットワーク内に存在する端末やサーバのOSバージョンを把握できれば、OSのバージョン情報から潜在的なセキュリティ脆弱性を把握でき、事前のセキュリティ対策や端末所有者・サーバ管理者への注意喚起を迅速に実施できる。こうした状況下で個別の端末について利用者にヒアリングなどにより端末・OSの情報を把握することは煩雑であり、且つ端末・サーバのOSはバージョンアップや入れ替えにより変化し常に把握し続けなければならない。これに対して端末やサーバから明示的に情報を得ることなく、ネットワーク側で取得できるパケット情報からのみでOSやそのバージョンを推定できれば効効率よく管理できる。このようなOS推定手法を開発するには、OS毎に生成される特徴のあるパケットを同定しなければならない。しかしながら、実際のネットワークにおいて端末やサーバが生成するパケットとOS種別（バージョンを含む）を対応づけたデータセットは存在しない。

そこで、本実験では、前述のデータセットを作成することを目的として、WIDE合宿期間中の生活セグメントにおいて、ブロードキャストパケットを収集するセンサーを設置し各種パケットデータを収集した。また、収集したパケットデータと端末のOS・バージョンを突合させる為に合宿参加者にアンケートを実施し、利用してるOSの種別、インターフェイスのmacアドレス情報を収集した。

4.6.2 データ収集方法

実験は、2018年9月に松代ロイヤルホテルで開催されたWIDE合宿の合宿用ネットワークの無線LANセグメントにブロードキャストパケットをtcpdumpでキャプチャし保存するサーバを設置し実施した。IPv4のブロードキャストパケット、IPv6のマルチキャストパケットをそれぞれ収集した。アンケートはGoogle Formを用いて作成しURLを合宿参加者に共有することで実施した。このアンケートにてmacアドレスについてはプライバシーに配慮し下4桁のみ収集した。収集したmacアドレスデータは、収集したpcapデータの同定が完了した後、pcapデータのmacアドレスをランダマイズし破棄した。

表1 OS 種別と台数

OS	台数
Android 7.0	1
Android 8.0	2
iOS 11	2
MacOS El Capitan	2
MacOS High Sierra	13
Windows 10	3
Windows 8.1	1

4.6.3 データ収集の結果と今後

3日間の合宿期間中に収集されたpcapデータの容量はIPv4とIPv6合計で約1.2GBであった。pcapデータから観測された端末数の総計は175台であり、そのうちアンケートに回答された端末と一致する台数は、25台であった。表1にOS種別と台数の内訳を示す。端末にはノートPCの他にスマートフォンやタブレットも利用されていた。WindowsやMacOSといったPC向けOSの他にも複数のバージョンのAndroid、iOSのデータも収集できた。

今回収集・作成したデータセットを元にランダムフォレストなどの機械学習を利用したOS推定アルゴリズムを開発していく。

4.7 センサデバイスを用いたネットワーク状態計測の手法

淺葉祥吾(北陸先端科学技術大学院大学)

4.7.1 背景と目的

ネットワークの安定運用には、ネットワーク機器が故障してもネットワークシステムが止まらない冗長構成や、ネットワーク障害への迅速な対応が必要である。

そこで、ネットワーク障害を発見する方法として、アクティブ測定とパッシブ測定がある。アクティブ測定は、プローブと呼ばれる計測用のパケットを送りネットワーク状態を測定し、ネットワークのスループットや往復遅延時間やパケットロス率、ジッタを計測する。パッシブ測定は、計測用のパケットを送らずに、ネットワークに流れるパケットを測定し。実際のトラフィック量やパケットの種類、サービスの状態を計測する。ネットワーク管理者は、アクティブ測定とパッシブ測定を用いてネットワークの監視を行なっている。

WIDE合宿で提供されるネットワークは、合宿のために構築、運用されるネットワークである。このようなイベントネットワークは、イベント開催の数日で構築し、安定運用しなければならない。しかし、ネットワーク管理者の不足やネットワークを構築する機器に制限があり、また、ネットワークに関する実験も同時に行われるので。安定運用するまでに様々な障害が発生しやすい環境である。

今回のWIDE合宿で提供されたネットワークは、Nagios3とNetdata、NetBox、Elastic Stackのオープンソースソフトウェアを使用して監視を行なった。Nagios3は、ホストやサービス、リソースなどの状態を監視し、異常時に通知するフレームワークである。Netdataは、リアルタイムでホストのパフォーマンスを可視化し監視できるツールである。NetBoxは、IPアドレス管理(IPAM)およびデータセンターインフラストラクチャ管理(DCIM)ツールである。Elastic Stackは、SyslogとSnortのアラートを可視化と検索ができるように構築した。

しかし、ネットワーク状態を計測するのは、実際に様々

なウェブページにアクセスを行わなければ発見できない障害もある。そこで、本実験は、今回のWIDE合宿で提供される各ネットワークセグメントに、センサデバイスを用いてネットワーク状態計測を行い、障害発生を、確認できるか調査した。

4.7.2 調査の概要

今回の調査では、ネットワーク状態計測を行うセンサデバイスは、WIDEワーキンググループであるSINDAN Projectが開発しているSINDAN Clientスクリプトを実行できるRaspberry Piを利用した。

表2に、SINDAN Clientの計測項目の各階層レイヤで確認している概要を示す。階層レイヤは、データリンク層（datalink）、インターフェース設定層（interface）、ローカルネットワーク層（localnet）、グローバルネットワーク層（globalnet）、名前解決層（dns）、ウェブアプリケーション層（web）であり、各階層の計測結果によりどこに障害があるのか判断できる。

データリンク層は、TCP/IPの階層におけるネットワークインターフェイス層にあたり、隣接機器との接続性を確認するための階層である。ネットワークインターフェイスのDown/Upからリンクアップできるまでを計測する。無線ネットワーク環境は、どの無線基地局に繋がっているのかとAssosiationが確立するまで計測する。

階層レイヤ	階層レイヤの計測概要
データリンク層 datalink	隣接機器との接続性 ネットワークインタフェースの Down/Up リンクアップを確認 無線ネットワークでは Assosiation が確立するまで
インターフェース設定層 interface	IP アドレス設定 IPv4 は DHCP による自動アドレス設定 IPv6 は RA による SLAAC と DHCPv6 による自動アドレス設定
ローカルネットワーク層 localnet	同一セグメントにおける IP の到達性 デフォルトルートへの到達性 ローカルネットワークにあるネームサーバへの到達性
グローバルネットワーク層 globalnet	組織外の外部サーバへの IP 的な到達性 指定したサーバへの到達性 指定したサーバへの Traceroute
名前解決層 dns	DNS による名前解決の確認 ドメイン名から IP アドレスを 取得する名前解決の確認 名前解決にかかった時間
ウェブアプリケーション層 web	ウェブアプリケーションに特化 ウェブアプリケーションに特化して評価 HTTP での通信が可能か確認

表2 SINDAN Clientの計測項目の各階層レイヤで確認している概要

インターフェース層は、TCP/IP階層モデルにおけるインターネット層にあたり、IPアドレス設定を計測する階層である。IPv4では、DHCP（Dynamic Host Configuration Protocol）[58] による自動アドレス設定を計測する。IPv6では、RA（Router Advertisement）[59] によるSLAAC（Stateles Address Auto Configuration）[60] の確認やDHCPv6 [61] による自動アドレス設定を計測する。

ローカルネットワーク層は、TCP/IP階層モデルにおけるインターネット層のローカルネットワークへのIP的な到達性を計測する階層である。ローカルネットワーク内にあるデフォルトルートやネームサーバへの到達性とPingコマンドによりRTT（Round Trip Time）とパケットロスト率、パスMTUを計測する。

グローバルネットワーク層は、TCP/IP階層モデルにおけるインターネット層のグローバルネットワークへのIP的な到達性を計測する階層である。Pingコマンドにより RTT（Round Trip Time）とパケットロスト率、tracerouteコマンドによるパス計測の到着性の確認、パスMTUを計測する。

名前解決層は、TCP/IP階層モデルにおけるアプリケーション層のDNS（Domain Name System）よる名前解決の確認を行う階層である。アプリケーションを利用する際に必須となる機能として、ドメイン名からIPアドレスを取得する名前解決があり、名前解決できるかと名前解決するまでの時間を計測している。OSのresolver API毎に挙動が異なることが想定されるので、DHCP/DHCPv6等で得られた自動アドレス設定で配布されたネームサーバとパブリックDNSサーバとの挙動に変化があるのか確認する。パブリックDNSサーバは、どんなDNSサーバも設定可能である。今回の計測では、WIDE ProjectのDNSサーバとGoogleのパブリックDNSサーバを利用している。また、Aレコードのみや AAAAレコードのみ、双方をもつサーバドメイン名の名前解決できるか計測する。

ウェブアプリケーション層は、TCP/IP階層モデルにおけるアプリケーション層にあたり、ウェブアプリケーションに特化して計測する階層である。この層では、組織外の外部サーバに対してHTTPでの通信が可能か計測する。

今回のWIDE合宿は、参加者に対して以下のネットワークセグメントが提供された。

・camp wlan 2.4GHz
・camp wlan 5GHz
・camp wlan v6only

この各ネットワークセグメントに、SINDANClientスクリプトを実行できるRaspberry Piを置き、センサデバイスとしてネットワーク状態計測を行なった。Raspberry PiにUSBの無線LANアダプタのドングルGW-450D2を取り付け、2.4GHz帯と5GHz帯で通信できるようにした。ネットワーク状態計測は、5分に1回にした。この値は、ネットワーク状態計測のトラフィックが、ネットワーク機器に高負荷を与えずに、計測できるように調整した。

図2に、センサデバイスを用いてネットワーク状態計測を行い、計測結果をネットワーク管理者に報告するイメージを示す。今回は、計測結果を保存するためのデータベースは、SINDAN Projectが所有しているサーバを利用した。

4.7.3　調査結果

9月5日18時33分(JST)に、camp wlan v6onlyでおきたDNSサーバの設定ミスの障害が、センサデバイスからのネットワーク状態計測の結果により確認できた。図3に、9月5日18時33分(JST)のcamp wlan v6onlyのセンサデバイスからのネットワーク状態計測の結果を示す。この図より、ウェブアプリケーション層と名前解決層の一部の計測結果が赤くなっていることから、計測が失敗していることが読み取れる。

9月5日19時18分(JST)頃に、9月5日18時33分(JST)に確認されたcamp wlan v6onlyでおきたDNSサーバの設定ミスの障害の復旧が、センサデバイスからのネットワーク状態計測の結果により確認できた。図4に、9月5日19時18分(JST)のcamp wlam v6onlyのセンサデバイスからのネットワーク状態計測の結果を示す。この図より、9月5日18時33分にウェブアプリケーション層と名前解決層の一部の計測結果が失敗してた箇所が、緑になっていることから、計測が成功していることが読み取れる。

今回の調査で、センサデバイスからのネットワーク状態計測の結果により、障害に関する情報が把握できること

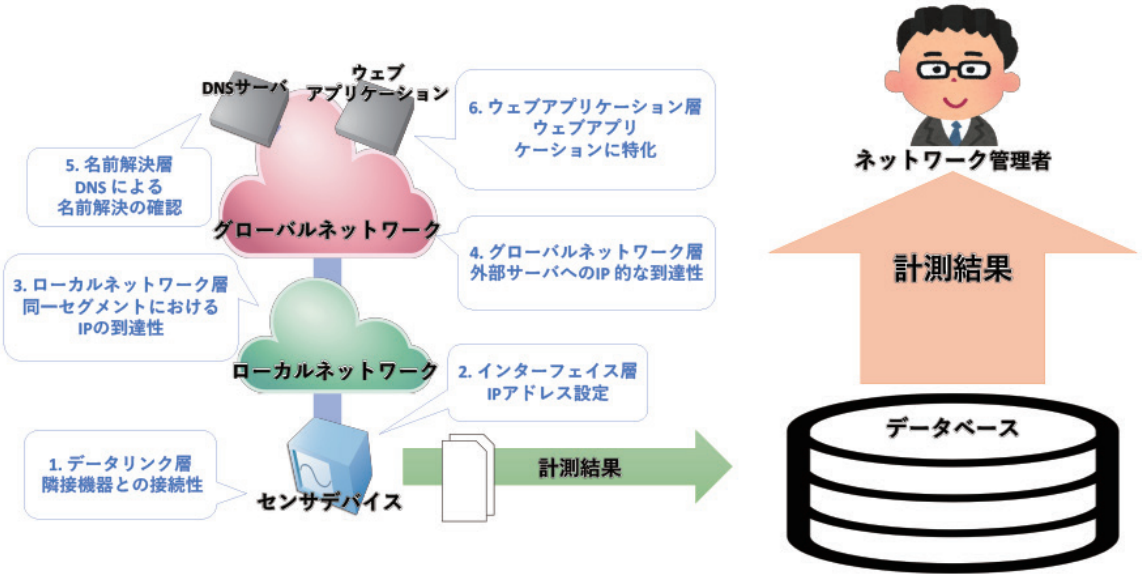

図2　センサデバイスを用いてネットワーク状態計測を行い計測結果をネットワーク管理者に報告するイメージ

ログキャンペーン詳細

編集

キャンペーンUUID	6664a672-bdc3-4bf3-87f9-e16c8caf5a93
SSID	camp_wlan_v6only
MACアドレス	00:22:cf:e0:6c:8c
OS	Raspbian GNU/Linux 9.4 (stretch)
発生日時	2018/09/05 09:33:21

診断ログ一覧

All | Log | Error

レイヤ	計測グループ	計測タイプ	計測ターゲット	計測結果詳細
ウェブアプリケーション層	IPv6	v6http_srv	www.wide.ad.jp	000
ウェブアプリケーション層	IPv6	v6http_srv	www.yahoo.co.jp	000
名前解決層	IPv6	v6dnsqry_A_ipv6.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv6.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_AAAA_ipv6.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv6.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_AAAA_ipv6.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv6.sindan-net.com AAAA +time=1 ; (1 server
名前解決層	IPv6	v6dnsqry_A_ipv6.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv6.sindan-net.com A +time=1 ; (1 server fou
名前解決層	IPv6	v6dnsqry_AAAA_ipv6.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv6.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_A_ipv6.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv6.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_AAAA_ipv4.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv4.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_A_ipv4.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv4.sindan-net.com A +time=1 ; (1 server fou
名前解決層	IPv6	v6dnsqry_AAAA_ipv4.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv4.sindan-net.com AAAA +time=1 ; (1 server
名前解決層	IPv6	v6dnsqry_A_ipv4.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv4.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_A_ipv4.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv4.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_AAAA_ipv4.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv4.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_AAAA_dual.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 dual.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_A_dual.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 dual.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_AAAA_dual.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 dual.sindan-net.com AAAA +time=1 ; (1 serve

図3 9月5日18時33分(JST)のcamp wlan v6onlyのセンサデバイスからのネットワーク状態計測の結果

ログキャンペーン詳細

編集

キャンペーンUUID	6a505bc9-7fc3-427f-9d3b-a7b573c00597
SSID	camp_wlan_v6only
MACアドレス	00:22:cf:e0:6c:8c
OS	Raspbian GNU/Linux 9.4 (stretch)
発生日時	2018/09/05 10:18:03

診断ログ一覧

All | Log | Error

レイヤ	計測グループ	計測タイプ	計測ターゲット	計測結果詳細
ウェブアプリケーション層	IPv6	v6http_srv	www.wide.ad.jp	200
ウェブアプリケーション層	IPv6	v6http_srv	www.yahoo.co.jp	301
ウェブアプリケーション層	IPv6	v6http_srv	www.wide.ad.jp	200
名前解決層	IPv6	v6dnsqry_AAAA_ipv6.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv6.sindan-net.com AAAA +time=1 ; (1 server
名前解決層	IPv6	v6dnsqry_A_ipv6.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv6.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_AAAA_ipv6.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv6.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_A_ipv6.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv6.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_A_ipv6.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv6.sindan-net.com A +time=1 ; (1 server fou
名前解決層	IPv6	v6dnsqry_AAAA_ipv6.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv6.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_AAAA_ipv4.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv4.sindan-net.com AAAA +time=1 ; (1 server
名前解決層	IPv6	v6dnsqry_A_ipv4.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 ipv4.sindan-net.com A +time=1 ; (1 server fou
名前解決層	IPv6	v6dnsqry_AAAA_ipv4.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv4.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_AAAA_ipv4.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv4.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_A_ipv4.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:4860:4860::8888 ipv4.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_A_ipv4.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 ipv4.sindan-net.com A +time=1 ; (1 server f
名前解決層	IPv6	v6dnsqry_A_dual.sindan-net.com	2001:200:0:ff41::2	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2001:200:0:ff41::2 dual.sindan-net.com A +time=1 ; (1 server fou
名前解決層	IPv6	v6dnsqry_AAAA_dual.sindan-net.com	2606:4700:4700::1111	; <<>> DiG 9.10.3-P4-Raspbian <<>> @2606:4700:4700::1111 dual.sindan-net.com AAAA +time=1 ; (1 serve
名前解決層	IPv6	v6dnsqry_AAAA_dual.sindan-net.com	2001:4860:4860::8888	; <<>> DiG 9.10.3-P4-Raspbian <<>>

図4 9月5日19時18分(JST)のcamp wlan v6onlyのセンサデバイスからのネットワーク状態計測の結果

を示した。また、SINDAN Clientは、ネットワーク状態計測として、障害を検出できる。

4.7.4　まとめ

センサデバイスを用いたネットワーク状態計測は、ネットワーク障害を検出できる。しかし、ネットワーク障害を検出した際に、ネットワーク管理者に報告するアラートを出さないと、ネットワーク管理者は、ネットワーク状態計測の結果を毎回確認しないといけない。また、ネットワーク計測結果から頻繁にアラートを出してしまうと、重要なアラートを見逃してしまうことにつながる。ネットワーク計測結果からどのような計測結果時にアラートを送るのか議論の余地がある。そして、アラートから緊急な障害を優先して対応できように、アラートのトリアージについても議論の余地がある。また、計測ログと障害ログ、復旧作業ログを付き合わせて管理することで、ネットワーク管理者が運用しやすい環境になるのか議論の余地がある。

4.8　アンケートの結果

合宿終了時のアンケートの結果を図5に示す。

「良かった」という回答については、QRコードによる接続に感動したというコメントを頂いた。

一方、悪かったという回答については、無線につながらない、IPv6 onlyでの接続時におけるセッション断や、MTUサイズによるVPNのセッション断の発生がその理由として挙げられていた。無線につながらないという問題に関しては、調査の結果、CMEのファームウェアの不具合によって、クライアントがARPの解決に失敗し、IPによる通信ができなくなる場合があるということに由来していたことがわかった [62] 。このため、参加者の端末によって、セッション断が発生する場合もあれば、発生しない場合もあった。その他のコメントとしては、停止状況や障害状況の公開を求める声や、対外接続を小松経由にしたことによるRTTの増大といった指摘を頂いた。

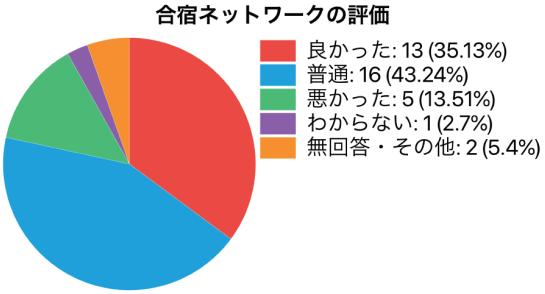

図5 合宿終了時「ネットワークについて」の回答

4.9　おわりに

本稿では2018年9月4日(火)から9月7日(金)にかけて開催された2018年9月合宿におけるネットワーク環境の設計について紹介し、運用および実験の結果について報告をした。WIDE合宿におけるネットワーク構築は、実際にネットワークを設計・運用する機会が減ってきた今日において、技術者養成としての面や実トラフィックを用いた実験の場としての役割を果たせる貴重な機会であることから、今後も継続して提供されることを強く望む。