

2018年12月研究会および2019年3月合宿プログラム報告

近藤賢郎 (latte@itc.keio.ac.jp) 豊田安信 (yas-nyan@sfc.wide.ad.jp)
小林 諭 (sat@nii.ca.jp) Camp-1903 プログラム委員会 (camp-1903-pc@wide.ad.jp)

1 はじめに

本文書では、2019年12月22日(土)から2019年12月23日(日)にかけて東京大学で開催されたWIDE研究会、及び2019年3月5日(火)から2019年3月7日(木)にかけて静岡県THE HAMANAKOにて開催されたWIDE2019年春合宿について報告する。

2 12月研究会

2018年12月に開催されたWIDE研究会は、「Designing next generation WIDE network」を標題に掲げ開催した。WIDEプロジェクトは30周年を迎え、開始時とは社会の状況が大きく代わりその果たすべき役割を再考すべき時期が来ている。本会では特にWIDEプロジェクトが運用するバックボーンネットワークについて、その再構築にあたってのデザインと運用を再考することを趣旨とした。特にテストベッドやネットワーク運用技術についての最新動向について理解を深めることで、次世代技術の研究開発を支えることのできるWIDEバックボーンの立ち位置と役割についての議論に繋げることを目指した。

本研究会では、1件の基調講演、2件の招待講演、1件の議論セッションが行われた。また6件のBoFと6件のポスター発表が行われた。本研究会は2019年12月22日(土)から2019年12月23日(日)にかけて東京大学本郷キャンパスで行われた。

2.1 基調講演

本研究会では以下の基調講演が行われた。

1. AI・機械学習を活用した異常検知技術と事例のご紹介

発表者 榎並利晃、藤原和成(ブレインズテクノロジー)、松山信仁(アラクサラネットワークス)

概要 本講演では、AI・機械学習を活用した異常検知技術のご紹介と、機械学習がIoTやネットワーク分野で価値を提供するシーンを、事例を交えて説明します。

- 大量なセンサー、音、動画データに対するプラント設備の故障予兆検知
- 製品完了検査における不良検出、要因分析
- 測定データを利用したネットワークの運用

2.2 招待講演

本研究会では、2件の招待講演が行われた。

1. 第五世代移動通信(5G)がもたらす社会の変革と研究開発の現状

発表者 中尾彰宏(東京大学)

概要 第五世代モバイル通信(5G)は、東京オリンピック・パラリンピックの開催に合わせ、2020年にサービスインが予定されている我が国が総力を挙げて取り組む事業であり、大きな経済効果が期待されている。5Gでは、大容量通信(eMBB)、超多数通信(mMTC)、超高信頼・超低遅延通信(URLLC)というこれまでにない通信品質が実現される予定であり、早期のサービスインに向けた研究開発が推進されている。本講演では、5Gがもたらすことが予想される社会の変革、および、それを支える最新の学術研究開発の成果を紹介する。

2. Network infrastructure & management of Huawei Clouds.

発表者 Xie Baoshu, Zheng Wei(Huawei)

概要 Huawei Clouds is operating a massive infrastructure which is connected by thousands of networks devices. To support Huawei's whole station IT solutions, its network infrastructure must be reliable and stable, so in this session we will introduce briefly the network infrastructure itself and how SRE(Site Reliability Engineering) team achieves its SLAs goals by leveraging software tools, e.g. Monitoring, Automation.

言語 本講演は英語で実施された。

2.3 議論セッション

本研究会では、1件の議論セッションが行われた。

1. WIDE-BB 再設計セッション

座長 近藤賢郎 (慶應義塾大学)

概要 WIDE インターネットは、学術研究機関からの commodity Internet への接続を支える backbone network であると共に、研究活動の中で実装した成果物を実際に動かして実証する基盤として、またバックボーン級のトラフィックの動態を解析する為の計測基盤としての役割を併せ持っています。このセッションでは、次回合宿で実施予定の「WIDE インターネット再設計・再実装」に関わる議論に先立って、現在の WIDE インターネットの構成を振り返るとともに、今後も自由で尖った研究を進める基盤としてどのような機能が必要となるかを広く議論したいと考えます。

2.4 BoF

本研究会では、6件の BoF セッションが行われた。

1. SINDAN プロジェクト

代表者 石原知洋 (東京大学)

概要 The goal of SINDAN project is to establish a method to evaluate the state based on observations from the user and to establish a method that enables network operators to grasp problems quickly.

2. Camp-net BoF

代表者 豊田安信 (慶應義塾大学)

概要 2019年3月合宿での Camp-Net の構成や実験の内容についてご紹介します。

3. ネブカワーキンググループ BoF

代表者 砂川真範 (北陸先端科学技術大学院大学)

概要 Introduction of NEBUCHA Working Group, Demonstration using JAIST's CyberRange.

4. moCA とトラストの今後

代表者 木村泰司 (JPNIC)

概要 一年間行ったトラストの議論を振り返り、今後の活動を相談します。

5. Log analysis BoF

代表者 Satoru Kobayashi(NII)

概要 This is a closed meeting. We will have a first meeting of log analysis project with Huawei.

言語 本 BoF は英語で実施された。

6. BoF (Medicri WG)

代表者 奥村貴史 (北見工業大学)

概要 麻疹等感染症への対応における携帯位置情報活用について、情報交換します。

2.5 BoF

本研究会では、6件のポスター発表が行われた。なおポスター発表については表彰が行われ、西尾真氏の「High Fidelity Qubit Mapping for IBMQ」が最優秀ポスター賞に、また新津雄大氏の「Generating a large

number of IPv6 addresses」が優秀ポスター賞にそれぞれ選ばれた。

1. LAN セキュリティ監視プロジェクト

発表者 落合秀也 (東京大学)

概要 LAN の内側は、セキュリティ脆弱性を抱えやすい一方で、近年では LAN の内部に簡単にマルウェアが侵入できる状況となっている。LAN 内部の怪しい挙動を捉えるための LAN 監視プロジェクトを始動する。

2. Towards Automatic Syslog Template Generation

発表者 山城裕陽 (東京大学)

概要 Although the format of log output is largely different depending on systems, syslog is widely used for managing them in service. For efficiently extracting information from syslog, it is necessary to create log templates that regulate the type of logs to be output. In this work, we design and implement log template generation algorithm from the source code and propose application of log templates.

3. Generating a large number of active IPv6 addresses

発表者 Yudai Aratsu(東京大学)

概要 Active IPv6 address lists are needed for efficient IPv6 network scan. Recent researchers propose methods to generate active IPv6 addresses from small seed addresses. In this work, we implemented them, and by comparing their result we discuss how to generate more active IPv6 addresses and the limit of address generating methods.

4. ルールベースアルゴリズムで IOT デバイスの安全通信相手を抽出提案

発表者 オンカンチャナ ポラパット (東京大学)

概要 As the number of IoT devices continues to grow every day, we can say without a doubt that one day IoT devices will be used in every aspect of our life. However, devices without an appropriate security management can be easily exploited by adversaries and used for malicious reasons. This research focuses on a way to secure end-device and we have proposed a system which prevents malicious traffic from intruding into the system. Our target IoT devices are device which main functions are gathering data and transferring those data to its server. Our approach is to determine a set of rules based on network traffic, any hosts which not comply with the rules are considered invalid and all of the traffic related to it would be cut down by the switch. Hosts which followed the rule are acknowledged as secure and added to list called "White List". In our experiment, all of the hosts found in the white list are valid hosts, such as device's NTP, DNS, HTTP, DHCP servers. Experiment was only conducted on 2 devices; more experiment result is necessary before implementing into real environment.

5. パルスリンク法 : PPLC-PV 通信のためのパケット抽出アルゴリズム

発表者 幸田大智 (東京大学)

概要 Power generation with photovoltaic is promising for realizing energy-sustainable society, and subject to be further installed toward the future. This paper considers the monitoring communication of elemental PV modules one-by-one, especially focusing on PPLC-PV, and proposes "pulse-link algorithm" for improving its receiving performance. The power conditioner of PV-system depresses the communications deployed on the powerline because of its generated noises. The pulse-link algorithm, with the

four steps described in this paper, can retrieve packets of PPLC-PV even under such an environment. The evaluation with real equipment of 48 PV panels has shown that the algorithm has improved to 95% success on cloudy days and 97% success on sunny days whereas the legacy algorithm has only achieved around upper 70% success.

6. High Fidelity Qubit Mapping for IBMQ

発表者 西尾真 (慶應義塾大学)

概要 Existing quantum computer processors have topological limitations on the execution of CNOT gates. Moreover, the degree of operational imperfection differs according to qubits. Mapping qubit variables to processor has a strong influence on the feasibility and fidelity on the current processors. In this research, we defined simple error model Sest using Randomized Benchmarking and compared it with the result of executing the circuit with IBM Q20. The result shows Sest is enough high accuracy for CNOT path selection.

3 合宿プログラム

2019年3月に開催された WIDE 合宿は、「Redesign and Reimplementation of WIDE Internet」と銘打ち、実験網としての WIDE インターネットの今後を議論することを目的に開催した。

WIDE インターネットは、学術研究機関からの commodity Internet への接続を支えるバックボーン・ネットワークであると共に、研究活動の中で実装した成果物を実際に動かして PoC する基盤として、またバックボーン級のトラフィックの動態を解析する為の計測基盤としての役割を併せ持っている。このような ”operational” で ”experimental” な学術系バックボーンの独自性を堅持し、且つその性質を活かした自由で尖った研究を進める基盤として今一度 WIDE インターネットを再設計・再実装することをテーマに据えた議論が展開された。

本合宿では、プレナリセッション 3 件と研究発表セッション 1 件を行った。また 13 件の BoF セッション、8 件のポスター発表、1 件の研究発表を行った。

3.1 プレナリセッション

本合宿では、3 件の以下のプレナリセッションが行われた。

1. Plenary session (backbone security)

概要: 前回合宿での議論に引き続き、今回の合宿でも WIDE における CSIRT 活動のあり方について議論します。特に今回のセッションでは WIDE における組織間 CSIRT 連携のあり方に着目します。まず、千葉大学シーサート / 伊藤忠シーサートの佐藤先生をお招きし、学術 CSIRT と企業 CSIRT の違いにつき議論します。学術・企業といった差を乗り越えて当たり障りのないインジケータ情報等の共有から一歩踏みこんだ CSIRT 連携を実現すべく、一定のトラストを前提とした皆で活用できる脅威分析情報のアーカイブや広域サンドボックス環境の構築を検討します。

2. Plenary session (WIDE インターネット再設計)

概要: WIDE インターネットは、学術研究機関からの commodity インターネットへの接続を支える backbone network であると共に、研究活動の中で実装した成果物を実際に動かして実証する基盤として、またバックボーン級のトラフィックの動態を解析する為の計測基盤としての役割を併せ持っています。このセッションでは、昨年 12 月研究会で実施した「WIDE インターネット再設計・再実装」に関わる議論に引き続き、今後も自由で尖った研究を進める基盤として WIDE インターネットにどのような機能が必要となるかを広く議論したいと考えます。

3. Plenary session (board plenary)

概要: 3/4 のボード合宿での議論を元にしたセッションを開催します。

3.2 BoF セッション

本合宿では、13 件の以下の BoF セッションが行われた。

1. WIDE-WG BoF

代表者 加藤 大弥 (慶應義塾大学)

概要 WIDE 合宿では毎年多くの学部・修士の学生が新しく WIDE メンバーとして参加しています。そのようなまだ右も左もわからない学生を対象に BoF を開催します。WIDE で様々な Working Group での具体的な活動の紹介や WG に参加する意義や参加して良かったことなどを共有することで、若いメンバーたちが WG に参加するきっかけを作ることを目的とし、「WIDE プロジェクトの活性化」を図ります。WIDE 合宿初参加や Working Group に参加したことのない若手メンバーの方を歓迎しております。

2. Persistent Privacy Preserving Real Time Monitoring of the WIDE Internet

代表者 Paul Vixie (Farsight Security)

概要 No single network carries enough traffic to provide insight into community behaviour. By cooperating in the operation of open source sensors under a narrow contractual umbrella, all network operators and all authorized network researchers can witness and either analyze or store meta-traffic which could include Darknet / Network Telescope, Passive DNS, NetFlow, and system logs including firewall logs. The WIDE Internet will be stronger if it is well studied and if its traffic patterns are well understood.

3. Software Defined Media WG BoF

代表者 塚田 学 (東京大学)

概要 Software Defined Media の進捗報告、今後の活動についての議論 <http://sdm.wide.ad.jp/>

4. IoTsec

代表者 井上 博之 (広島市立大学)

概要 家電や自動車のような組み込み機器のエッジデバイスのセキュリティについて。特に、最近話題になっている NICT による IoT 機器調査及び利用者への注意喚起の取組「NOTICE」について取りあげたい。

5. DNS

代表者 石原 知洋 (東京大学)

概要 DNS のプロトコルならびに運用に関する問題について議論を行う。

6. 篠田研 BoF

代表者 篠田研 M1 (JAIST)

概要 篠田研の公開ゼミ

7. SHINDAN

代表者 石原 知洋 (東京大学)

概要 ユーザ側からネットワーク障害点を検出する SHINDAN システムについて議論をおこなう。

8. NEBUCHA Working Group BoF

代表者 砂川 真範 (JAIST)

概要 サイバーレンジの研究に関する議論を行う。また、サイバーセキュリティトレーニングフレームワーク CyTrONE を用いた体験型デモを行う。

9. MAWI

代表者 長 健二郎 (IIJ Research Lab.)

概要 計測およびデータ解析研究のための WG

10. PPAP

代表者 川上 秀彦 (KDDI)

概要 ルータをはじめとするパケット処理装置の開発者が集い、技術情報の交換や高度開発に取り組む

11. TWO

代表者 近藤 賢郎 (慶應義塾大学)

概要 WIDE-BB の運用報告と実験報告 / WIDE-BB の再設計に関する議論

12. moCA/Trust BoF

代表者 木村 泰司 (JPNIC)

概要 moCA と IP アドレス認証局の話題を取り上げてトラストについて議論します。

13. LENS

代表者 壇 俊光 (大阪弁護士会)

概要 最近の法律に関わる問題を議論します。

3.3 ポスター発表

本合宿では、8 件の以下のポスター発表が行われた。

1. マルチベンダーの IoT セキュリティに向けた IP アドレス認証局

発表者 木村 泰司 (JPNIC)

概要 私たちの身の回りのモノがマルチベンダーであるように、IoT 環境はマルチベンダーで構成されると考えられる。インターネットにおけるホストの識別子である IP を使った電子証明書を自動的に提供する「IP アドレス認証局」を軸にして、そのサンプルを作成し新しい認証の構造について議論する。

2. DNS Observatory: Monitoring Global DNS Performance

発表者 Paul Vixie (Farsight Security)

概要 DNS Observatory is a new research project by Farsight Security that aims at monitoring the performance, content, and security of the global DNS. We present a preliminary analysis of the world's top 10,000 authoritative DNS servers, responsible for 87% of all DNS traffic we saw in January 2019. We found that just 500 top servers and 9 networks receive majority of all queries, that although most servers respond in ≤ 25 ms, 20% need over 100ms, and that response delay is generally smaller for more popular DNS servers.

3. ネットワークオントロジ Bonsai に基づくネットワーク構成のインスタンス自動生成機構

発表者 橋本 大樹 (慶應義塾大学)

概要 インターネットの内部構造はエンドユーザやアプリケーションに対してブラックボックスとなり、広域ネットワーク管理が困難となっている。そこで、筆者らはネットワーク情報の収集と活用のためのフレームワークである KANVAS を開発している。KANVAS は様々なネットワーク情報を Bonsai と呼ばれるネットワークオントロジのインスタンスとして知識ベースに格納し、この知識をユーザに提供することによりネットワーク管理やアプリケーションに役立てる。本発表では、ネットワーク構成情報を収集し、収集した情報を Bonsai のインスタンスとして知識ベースに格納する機能の自動化機構を提案する。

4. ユーザ空間とカーネル空間の連携を考慮した Network Function Chaining 基盤

発表者 攝待 大輔 (慶應義塾大学)

概要 ユーザ空間 NF とカーネル空間 NF が連携し動作する NFC を構築するシステムを提案する。NFV では複数の NF をそれぞれ仮想環境で動作させるため、データ転送におけるメモリコピーやインスタンス生成に伴う計算資源の点でオーバーヘッドが大きい。処理が簡単な NF をカーネル内でチェイニングさせ、複雑な NF のみユーザ空間に配置させることでオーバーヘッドの最小化を図る。

5. モバイル環境を想定したマルチパス動画ストリーミングの実装と検証

発表者 栗原 祐二 (慶應義塾大学)

概要 近年インターネットを活用した動画配信が増加しており、高品質かつ耐障害性が求められている。本研究では UDP に対してシーケンス番号の付与、マルチパスの実装を行った。これらにより最良ネットワーク経路を選択することが可能であり、高品質かつ耐障害性への有用性を確認することができた。

6. 立体音響を用いる小型サラウンドスピーカー環境の研究

発表者 庄子 琢郎 (慶應義塾大学)

概要 ホームシアター環境のような複数のスピーカーを用いた立体音響システムは、音の聞こえてくる方向が正確である。しかし、大規模なシステムの導入は難しい。ヘッドホン・イヤホンを用いれば簡単に立体音響を体験できるが、音の聞こえてくる方向の精度は低いものになる。そこで、ホームシアター環境のような、複数のスピーカーを用いたシステムを小型化させることで、誰でも簡単に使用できる高精度の立体音響システムを提案する。

7. Load Distribution in NTP Pool

発表者 新津 雄大 (東京大学)

概要 NTP Pool はボランティアによるタイムサーバの大きな仮想クラスターであり、主要な Linux 向けパッケージや Android OS のデフォルト問い合わせ先となっている。本発表ではいくつかの国に展開した NTP サーバをプールに登録し、そこで見られる NTP クエリをもとに、膨大な量の問い合わせが流入している NTP Pool の現状を提示する。

8. FPGA クラウドサービスを利用したネットワークパケットスケジューラの実装

発表者 小林 克志 (東京大学)

概要 AWS をはじめとするクラウド事業者からユーザが自身のハードウェアアクセラレータをプログラム可能な FPGA を搭載した IaaS が低コストで提供されている。我々はアプリケーション毎に異なる遅延要求をサポートするインターネットの実現を目指し、これに必要な Earliest Deadline First (EDF) パケットスケジューラのハードウェア実現性を on-premise の FPGA 開発環境で検証してきた。我々はこのパケットスケジューラをクラウド FPGA, AWS EC2 F1 上に実装し、ネットワークシステム研究におけるクラウド FPGA の有用性を確認した。

3.4 研究発表

本合宿では、1 件の以下の研究発表が行われた。

1. 公衆無線 Captive Portal における Covert Channel を経由した不正利用リスクの実態調査

代表者 増田 英孝 (東京大学)

概要 公衆無線 LAN サービスでは、利用者からの不正なインターネットアクセスを抑制するために、ユーザ認証機構を備えている場合が多い。ユーザ認証のための代表的な手法として Captive Portal が存在する。Captive Portal は認証が完了するまで、認証に関わらない通信を遮断しなければならないが、設定の不備により ICMP・DNS 等の通信を透過する場合がある。Covert Channel を利用すると、ICMP・DNS といったプロトコルで、認証が完了する前の Captive Portal でエンドツーエンドの通信を実現できる。本研究では東京都と神奈川県に設置されている公衆無線 LAN を対象に Covert Channel 通信による不正利用が可能なアクセスポイントを調査し、その数を集計した。その結果、955 個のアクセスポイントのうち 693 個は Covert Channel 通信が可能であることがわかった。

4 合宿ネットワーク

本節では 2019 年 3 月度に行った WIDE 合宿 1903 における、生活・実験用ネットワークについて述べる。

4.1 概略

2019 年春の WIDE 合宿では、Simple(誰でもわかる), Portable(どこでも出来る), Resilience(何度でも蘇る)をテーマに有線・無線によるインターネットアクセス提供及び、各種 IaC(Infrastructure as Code) ツールを利用したサービス提供を行った。本ネットワークでは主に参加者のインターネット接続を趣旨としたコミュニティネットワークと、後述する実験用テストベッドネットワークの二つの役割を担う。本ネットワークの詳細な L2/L3 構成図を図 1 に示す。

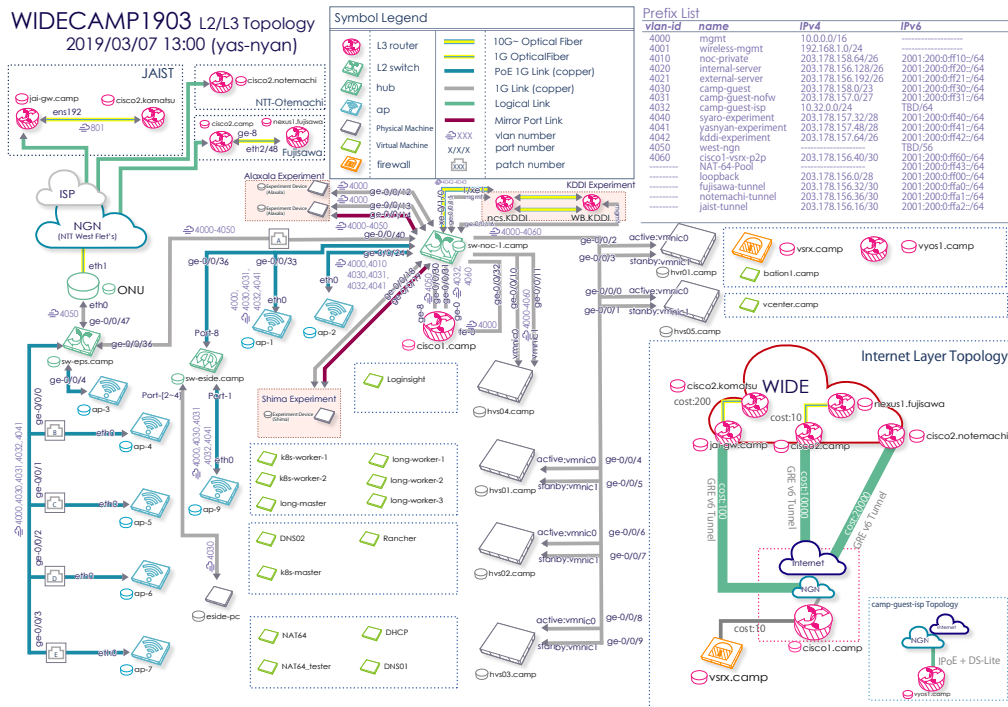


図 1: WIDE 合宿 1903 ネットワーク図

4.2 対外接続

生活系ネットワークでは対外接続に NTT 西日本フレッツ閉域網を利用し、GRE over IPv6 トンネリング[?]によって WIDE-BB 各拠点(小松 NOC・藤沢 NOC・NTT 大手町 NOC)にマルチホームに接続する主系と、DS-Lite(Dual Stack Lite)[?]を利用して商用 ISP に接続する副系の 2 系統のインターネットアクセスを提供した。

4.3 コモディティネットワーク

本ネットワーク全体で提供を行った各コモディティネットワークを表 1 に示す。

無線 LAN アクセス環境として、これらの主・副系統のネットワークのほか、各所属組織の認証情報を接続に利用できる国際組織間ローミングサービス (Eduroam¹) によるインターネットアクセス提供を行った。

¹<https://www.eduroam.org/>

加えて、合宿参加者が利用可能な IPv6 シングルス tack ネットワークの構築・運用を実施した。このネットワークでは通常の IPv6 ネットワークに加えてステートフルプロトコル変換[?]を利用し、IPv6 シングルス tack ネットワークにおける透過的な IPv4 インターネット到達性の提供を行った。

これらのネットワークではそれぞれステートフルパケットインスペクションによるパケットフィルタリングを行い、ネットワーク外部から接続が確立されない機構を敷設した。一方で特殊なユースケースを想定して、一部の参加者に本フィルタリングが提供されないネットワークも同時に提供した。

4.4 合宿ネットワークを利用した実験

本合宿ネットワークを利用した実験を募集し、以下の 4 件の実験を実施した。

1. PhishFinder(担当: IIJ イノベーションインスティテュート 島慶一)

表 1: WIDE 合宿 1903 で合宿参加者に提供された各コモディティネットワーク

対外接続系統	Wi-Fi SSID	周波数帯	概要
WIDE(主系)	CampGuest	2.4Ghz / 5Ghz	全ての参加者に提供した基本的なネットワーク
WIDE(主系)	CampGuest-noFirewall	2.4Ghz / 5Ghz	一部の参加者向けに提供されたフィルタリングの無いネットワーク
WIDE(主系)	CampGuest-v6only	2.4Ghz / 5Ghz	NAT64 による IPv4 アクセスを前提とした IPv6 シングルスタックネットワーク
mfeed(冗長系)	CampGuest-DSLite	2.4Ghz / 5Ghz	WIDE-BB 障害時を想定した商用 ISP 網を利用したネットワーク
WIDE(主系)	eduroam	2.4Ghz / 5Ghz	国際組織間ローミングによる認証を提供するネットワーク

NML プロジェクト²で作成したフィッシング URL 判定プログラムを用いて、合宿ネットワークで観測される URL をリアルタイム分類する

- SNMP MIB を用いたネットワークトポロジ情報の取得 (担当: 慶應義塾大学 橋本大樹)
ネットワーク上のルータやスイッチから SNMP を用いて IP アドレスや MAC アドレス等の MIB 情報を取得し、それらの情報を基にネットワークトポロジをネットワークオントロジのインスタンスとして表現する。
- Whitebox in WIDE Camp Network (担当: KDDI 川上 秀彦)
KDDI が開発したホワイトボックスルータを利用した IP 伝送試験
- ネットワーク可視化 (担当: アラクサラネットワークス 河野 智彦)
アラクサラネットワークスが開発したセンサー・コレクタを用いた通信トラフィックの収集と可視化。

²<https://nml.ai/>