Network Diagrams of WIDE Backbone

櫨山寛章 (hiroa-ha@is.naist.jp)
堀場勝広 (qoo@sfc.wide.ad.jp)
上野幸杜 (eden@sfc.wide.ad.jp)
垣内正年 (masato@itc.naist.jp)
井上博之 (hinoue@hiroshima-cu.ac.jp)
津崎善晴 (tsuzakiyo@net.ist.i.kyoto-u.ac.jp)
中野博樹 (cas@net.ist.i.kyoto-u.ac.jp)
岡部寿男 (okabe@i.kyoto-u.ac.jp)
Glenn Mansfield Keeni (glenn@cysols.com)
齋藤武夫 (saito@cysols.com)
土井一夫 (kazuo@cysols.com)
松本智 (matsumoto@tsukuba.wide.ad.jp)
高橋航平 (flast@tsukuba.wide.ad.jp)
畠山元也 (genyakun@tsukuba.wide.ad.jp)
近藤賢郎 (latte@inl.ics.keio.ac.jp)
川口慎司 (alfy@inl.ics.keio.ac.jp)
関谷勇司 (sekiya@nc.u-tokyo.ac.jp)　　中村遼 (upa@wide.ad.jp)
山本成一 (yama@wide.ad.jp)

平成 27 年 1 月 5 日

本ドキュメントでは、WIDE backbone と各 NOC の現状について述べる。

1　はじめに

WIDE バックボーンネットワークは国内はもとより San Fransico, Losangels, Bangkok など海外にも拠点（NOC, Network Operation Center）を持つ広大なレイヤー 2 およびレイヤー 3 ネットワークである．WIDE バックボーンネットワークは各接続組織の対外接続ネットワークとして活用されるだけではなく，インターネットの新技術を開発している研究者，開発者らの新技術の運用実験の場としても頻繁に活用されている．

WIDE バックボーンネットワークの運用は Two ワーキンググループに参加する各 NOC の運用者による定常的な運用に支えられている．本年度の Two ワーキンググループの活動報告として，WIDE バックボーンネットワークの運用報告を行い，合わせて，レイヤー 2 接続のオーバーレイ化を目指した VXLAN の運用実験についても報告する．最後に今後の WIDE バックボーン運用についての展望を述べる．

2　WIDEバックボーンの運用

本節では，WIDE バックボーンの各拠点での 2012 年 12 月 31 日から 2014 年 12 月 31 日までの運用報告と 2014 年 12 月 31 日現在の WIDE バックボーンのネットワーク構成を報告する．図 1 は 2014 年 12 月 31 日現在の WIDE バックボーンの概略図である．

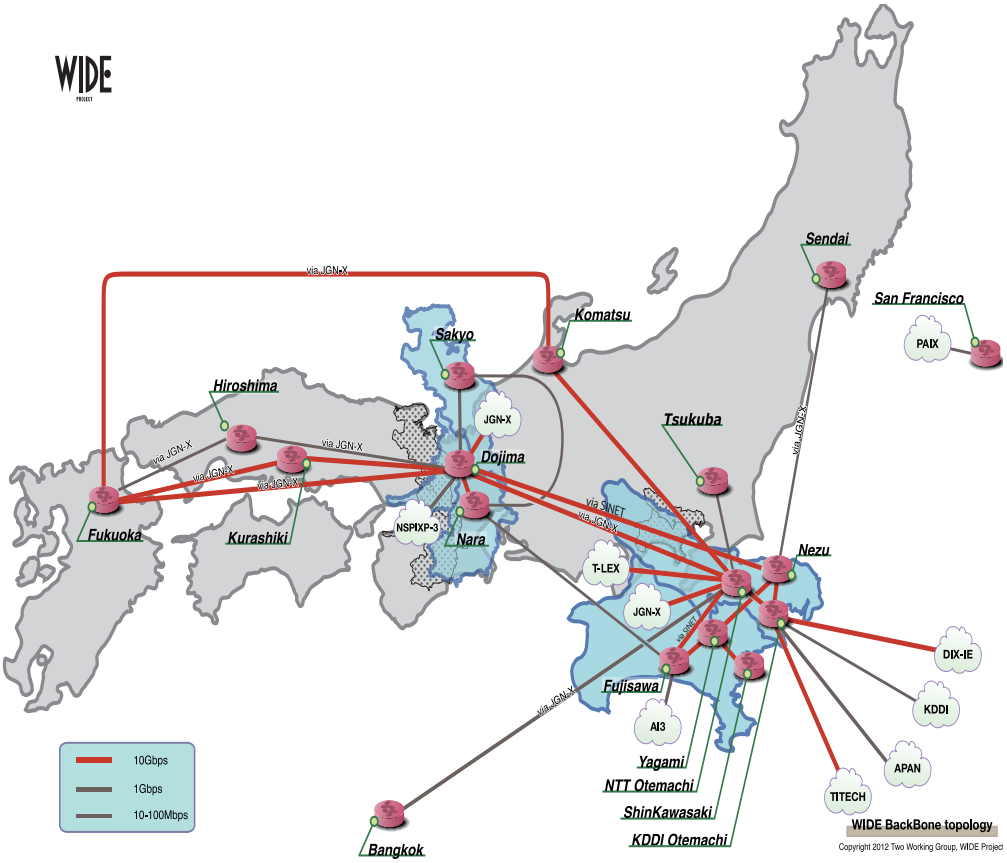

図 1: WIDE バックボーントポロジ

2.1 San Francisco

サンフランシスコ NOC(sanfrancisco) は，2004 年 4 月からそれまでの sanjose に代わり稼働した新しい NOC で，Los Angeles から OC-3 により接続されていた．その後 OC-3 から 100M Ethernet に変更された．主な接続先は，PAIX や ISC である．

2010 年 9 月の Los Angeles NOC 撤収にともない，2010 年 10 月に Los Angeles と San Francisco 間の回線も廃止され，専用線による接続の無い独立 NOC として存在する．

2013 年は M-ROOT 関連の機材更新があったが、WIDE SFO NOC としての構成変更は無かった。2014 年も、JP DNS 関連の機材更新があったが、WIDE SFO NOC としての構成変更は無かった。

As of 2014/12/28

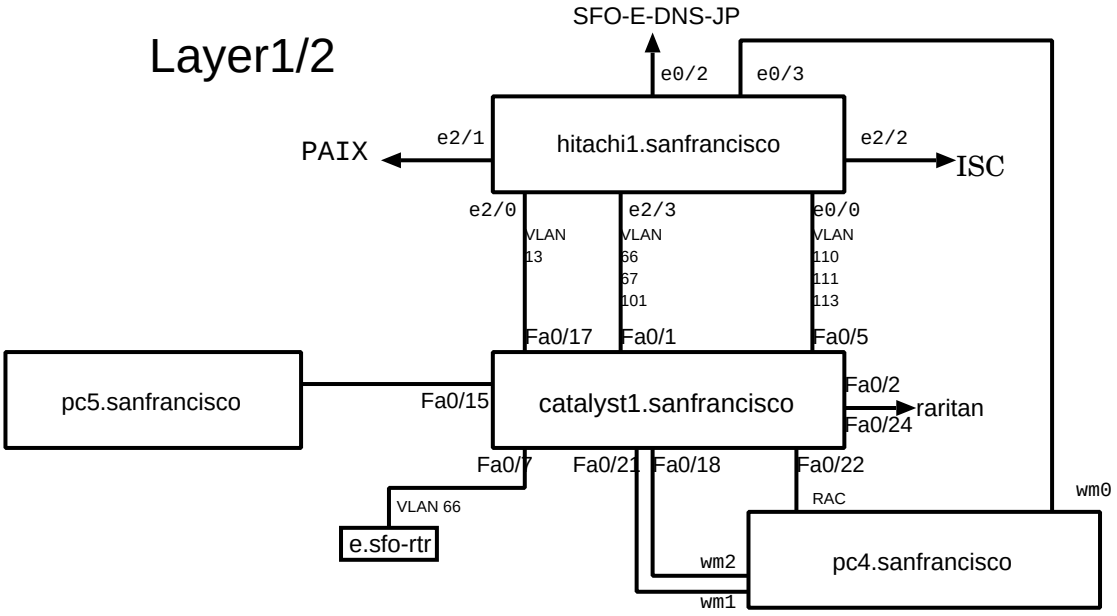

図 2: San Francisco NOC

2.2 仙台

仙台 NOC は仙台周辺の拠点を収容する NOC として運用されている．接続回線の計画断以外の障害や停電もなく，安定して運用された．NOC 内のトポロジーに変更はなく，根津側の収容ルータが foundry3 から brocade1 に変更された．

- (2014/05/09) 根津側の IPv4/IPv6 接続ルータが foundry3 から brocade1 に移行
- (2014/09/25-26) JGN のメンテナンスに伴う回線断
- (2014/11/14) 東北大学サイバーサイエンスセンター構内工事に伴う回線断

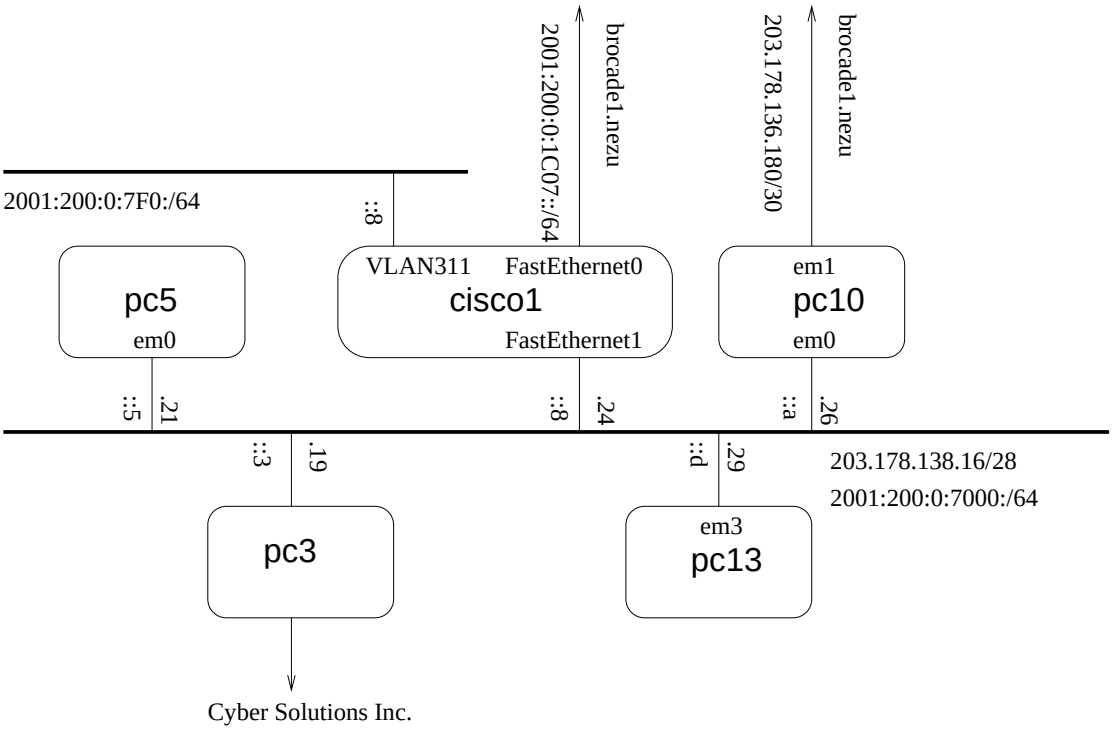

図 3: 仙台 NOC

2.3 筑波

筑波 NOC は筑波大学学術情報メディアセンター内に設置されている，システム情報工学研究科産学間連携推進室をはじめとする周辺の研究組織を収容している．

株式会社ソフトイーサと共同で、グローバル・固定 IPv6 アドレス割当型トンネル接続実験サービス (`v6ip.tsukuba.wide.ad.jp`) を運用しており、2012 年には DNS64/NAT64 による IPv4 ネットワークとの相互接続の試験運用も開始した．

- (2014/02/08) 雪に依る瞬電のため一部コアスイッチに障害発生・疎通全断
- (2014/02/09) 復旧
- (2014/10/25) 電気事業法に基づく電気設備の定期点検のため停止
- (2014/10/26) 同上・復電時に再度コアスイッチに障害発生・同日復旧
- (2014/12/11) ftp.tsukuba.wide.ad.jp のストレージに障害発生、一切のサービスを停止
- (2014/12/14) ftp.tsukuba.wide.ad.jp 復旧

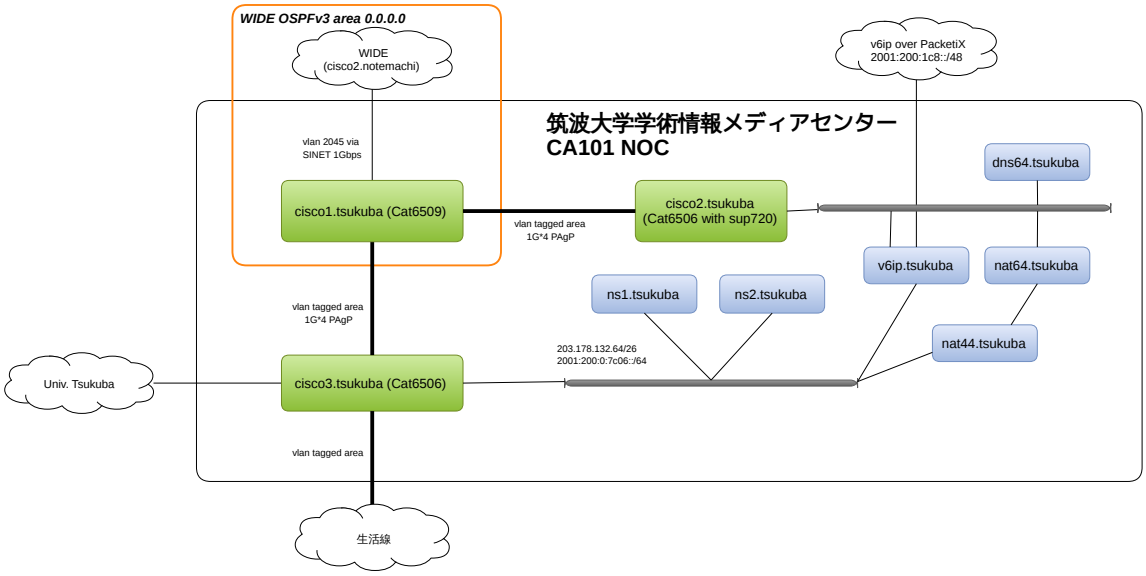

図 4: 筑波 NOC

2.4 根津

根津 NOC は，WIDE 関東地区の重要な接続拠点として，東京大学，JGN-X，SINET 等との接続を行っている．また WIDE クラウドの拠点としても重要な機器が設置されている．

- (2014/01/20) brocade1.nezu 導入
- (2014/05/27) foundry8.nezu (Q-in-Q 用スイッチ) 設置
- (2014/06/13) brocade1.nezu cam partition 変更のため reload
- (2014/08/29) 堂島 == 根津の L2 パス開通 (SINET)
- (2014/09/28) 東京大学法定点検のため停電 (ダウン無し)
- (2014/10/06) brocade1.nezu パケットロスにより reload
- (2014/10/26) 東京大学法定点検のため停電 (ダウン無し)

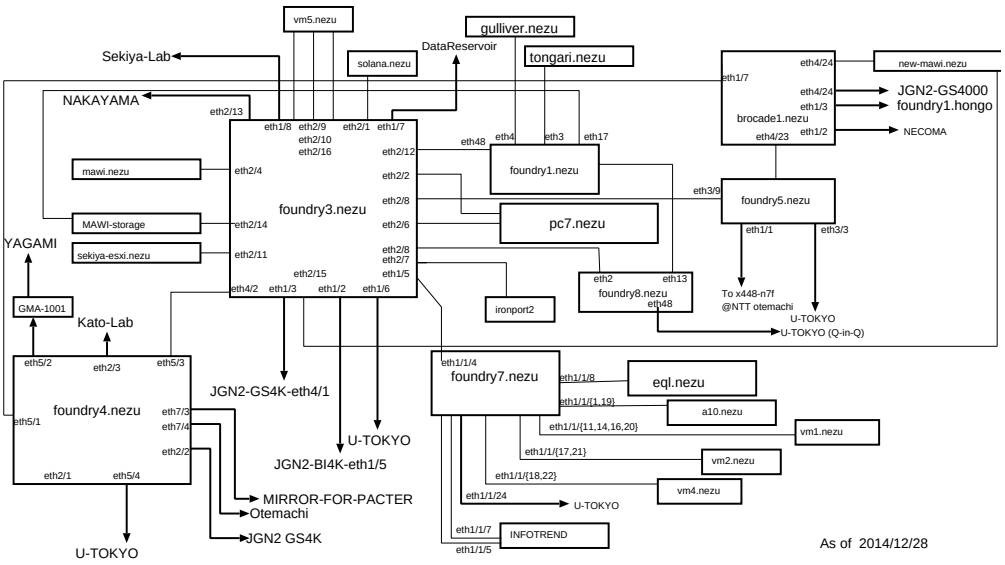

図 5: 根津 NOC

2.5 NTT 大手町

NTT 大手町 NOC(notemachi) は，1999 年終りから稼働した比較的新しい NOC で，現在，関西方面，北陸方面への L2 網，JGN-X ，APAN-JP の接続拠点として重要な立場にある．また，日本のインターネットトラフィック交換の 1 拠点として，DIX-IE ， T-LEX を設置し ISP および学術研究 NW を収容している．

- (2014/03) 明星大学接続解除
- (2014/07) 明星大学回線撤去
- (2014/07) 森ビル接続用 catalyst 故障
- (2014/08) 経路表用メモリ配分変更のため cisco2.notemachi 再起動

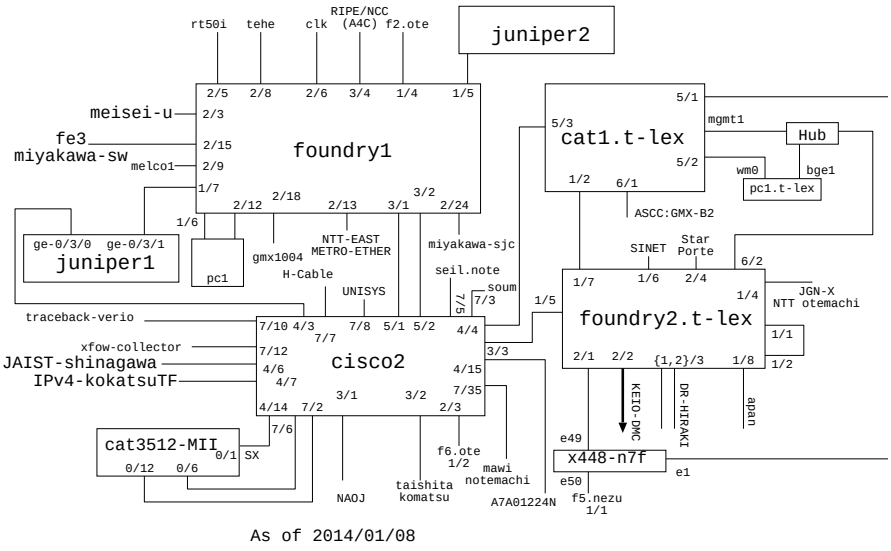

図 6: NTT 大手町 NOC

2.6 KDDI 大手町

KDDI 大手町 NOC は WIDE バックボーンの中でも中核を担う重要な NOC となっており，外部組織接続が最も多い NOC となっている．10GbE によるバックボーンが導入され，NTT 大手町 NOC との連携がより強まり，WIDE から DIX-IE への接続拠点となっている．

- (2014/01/21) PCH 機材更新
- (2014/02) cisco7.otemachi のソフトウェア不具合により ASSOCIO 向け接続障害，reboot で復旧
- (2014/07/02) PCH RAID コントローラ交換
- (2014/07) foundry6.otemachi のラインカードモジュールの一部が down し otemachi と notemachi 間が一時疎通断
- (2014/12/18) cisco3.otemachi 引退

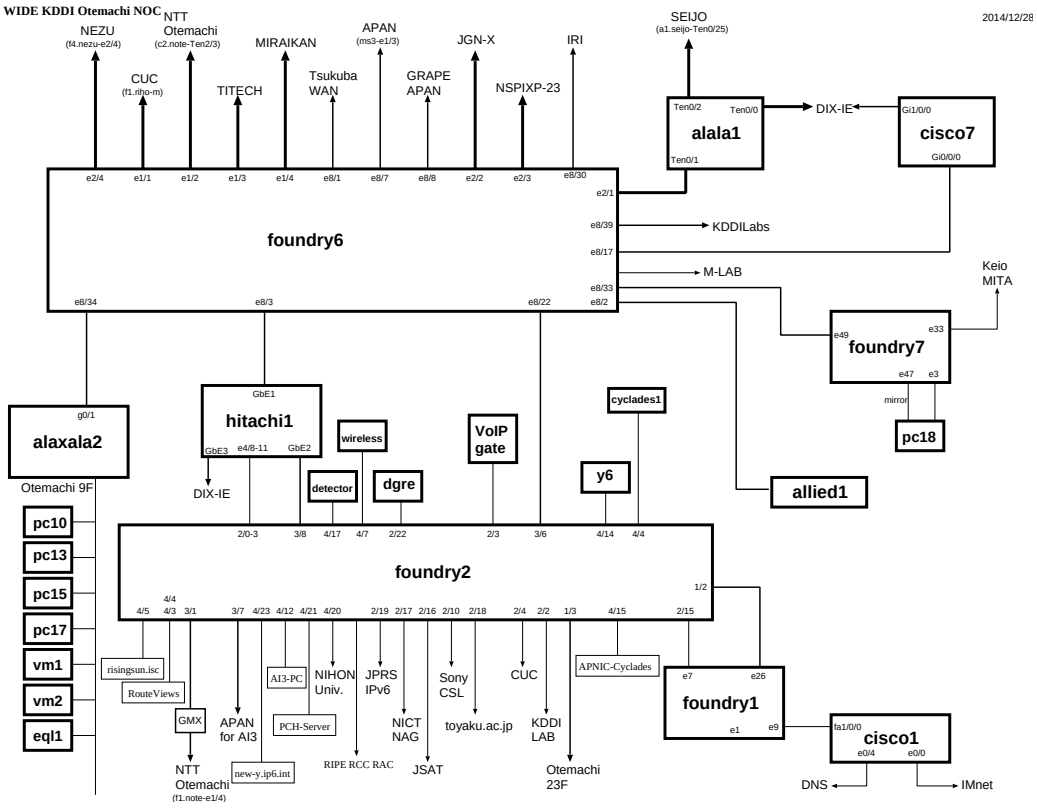

図 7: KDDI 大手町 NOC

2.7 矢上

矢上 NOC は慶應義塾大学理工学部矢上キャンパス構内にあり，同大学理工学部情報工学科および周辺の研究組織を収容すると共に慶應 DMC を介して JGN-X, CineGrid との接続を行っている．

- (2014/01/29) 矢上 – 富士ゼロックス間 ダークファイバ開通
- (2014/04/18) 矢上 – 富士ゼロックス間 ルーティング切り替え
- (2014/05/15) 矢上 – 富士ゼロックス間 広域 Ethernet 回線廃止
- (2014/06/24) 矢上 – アラクサラ間 DF 回線借用
- (2014/07) 矢上 NOC 内 UPS 電池交換
- (2014/08/16) 慶応大学矢上キャンパス法定停電
- (2014/08) cisco2.yagami の更新 (cat3750 → cat3560)
- (2014/12/22) 矢上 – 根津間 DF 回線借用

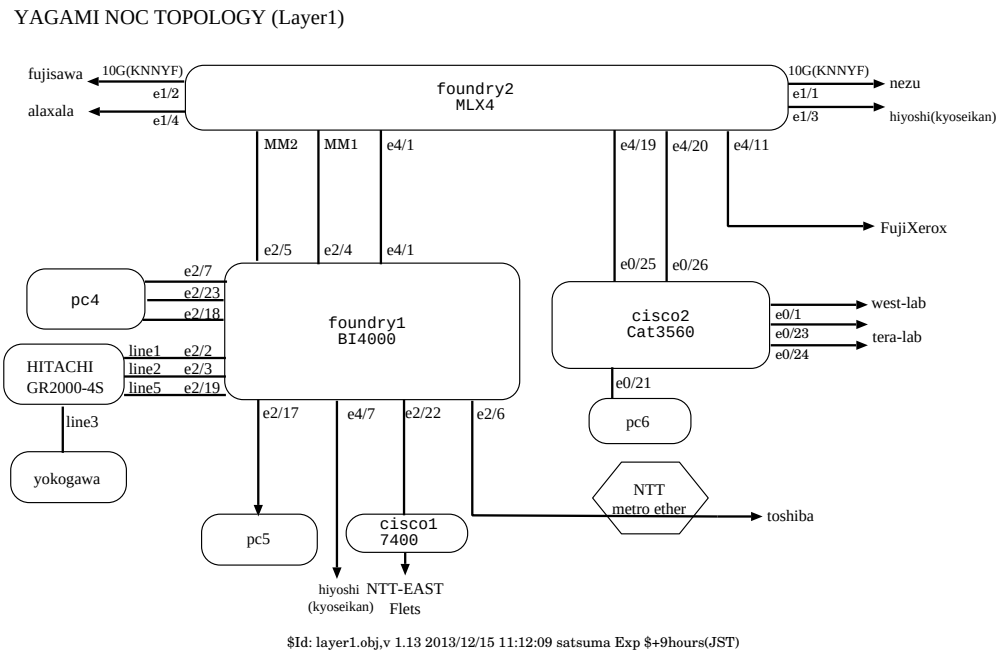

図 8: 矢上 NOC Layer-1 トポロジ

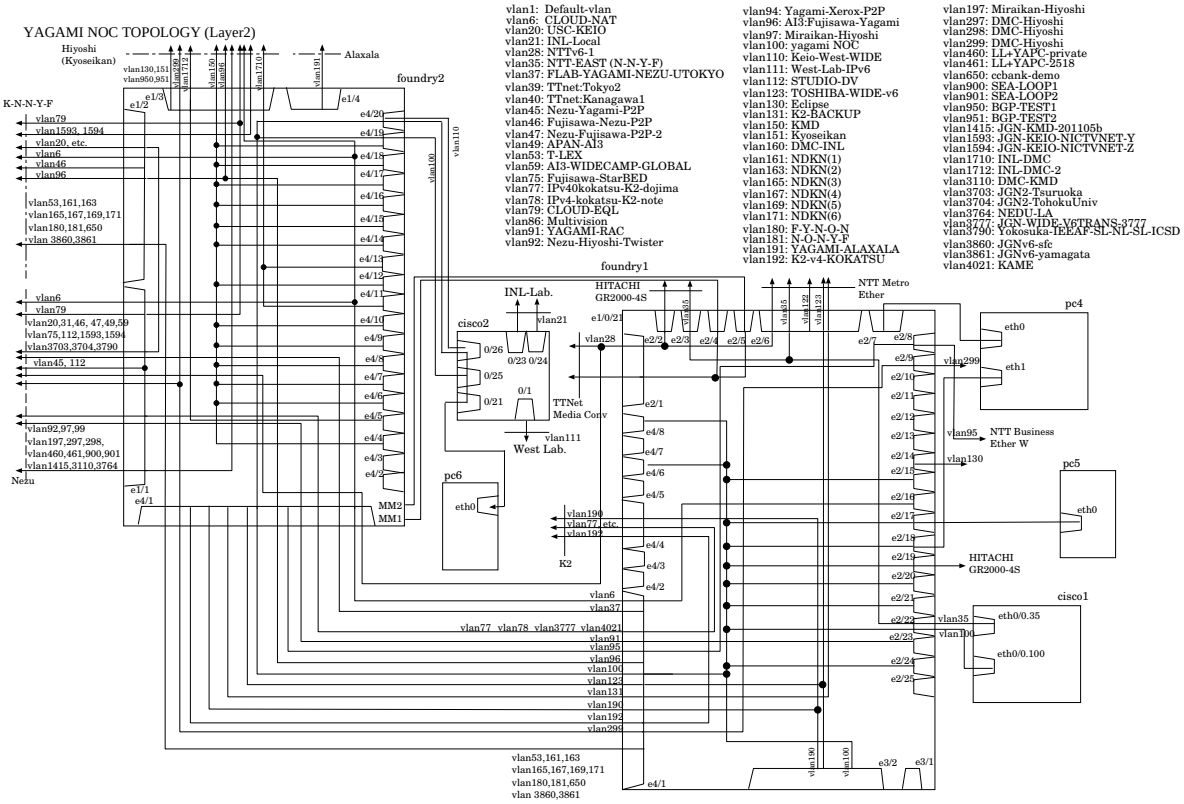

図 9: 矢上 NOC Layer-2 トポロジ

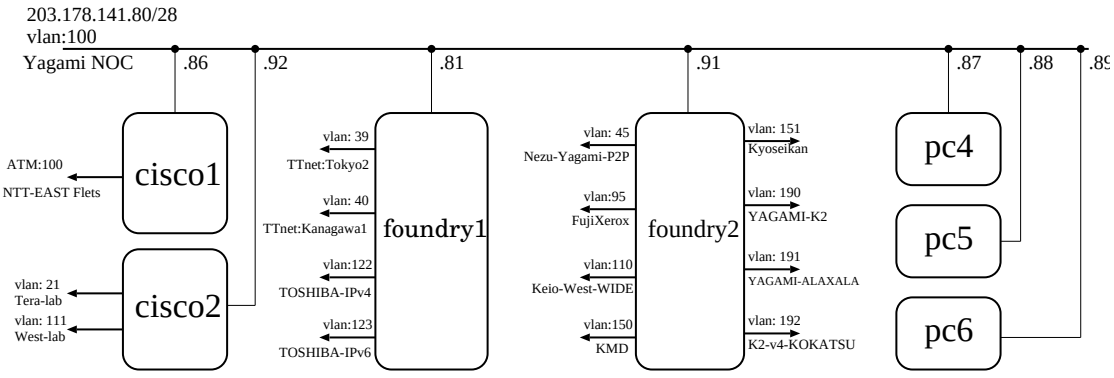

図 10: 矢上 NOC Layer-3 トポロジ

2.8 藤沢

藤沢 NOC は慶應義塾大学湘南藤沢キャンパス内にあり、慶應義塾大学や村井研究室の他、周辺の研究組織を収容している。同時に W3C や AI3 との接続、VoIP 関連サービス、外部研究組織のトラフィック計測サーバの設置及び接続性の提供などを行っている。

- (2014/01/25) sam-WG の終了に伴い藤沢 NOC 設置サーバを撤去
- (2014/02/18) 文教大学への接続性提供を終了
- (2014/03/27) VxLAN 検証のためコアルータをファームウェアアップグレード
- (2014/04/02) 奈良・左京・藤沢間専用線サービス切り替え工事
- (2014/05/17) Huawei S6700-48-EI の導入に伴うトポロジ変更
- (2014/09/16) NTT 東日本フレッツ回線開通工事
- (2014/09/29) AI3 関連 VLAN を VxLAN へ移行
- (2014/10/22) リース終了に伴いコアルータをリプレース
- (2014/10/22) WIDE クラウド関連 VLAN を VxLAN へ移行
- (2014/12/07) SFC 構内全域の変電設備の定期保安点検による構内停電
- (2014/12/15) 防衛大学校回線接続機器のリプレースに伴う現地確認の立ち会い

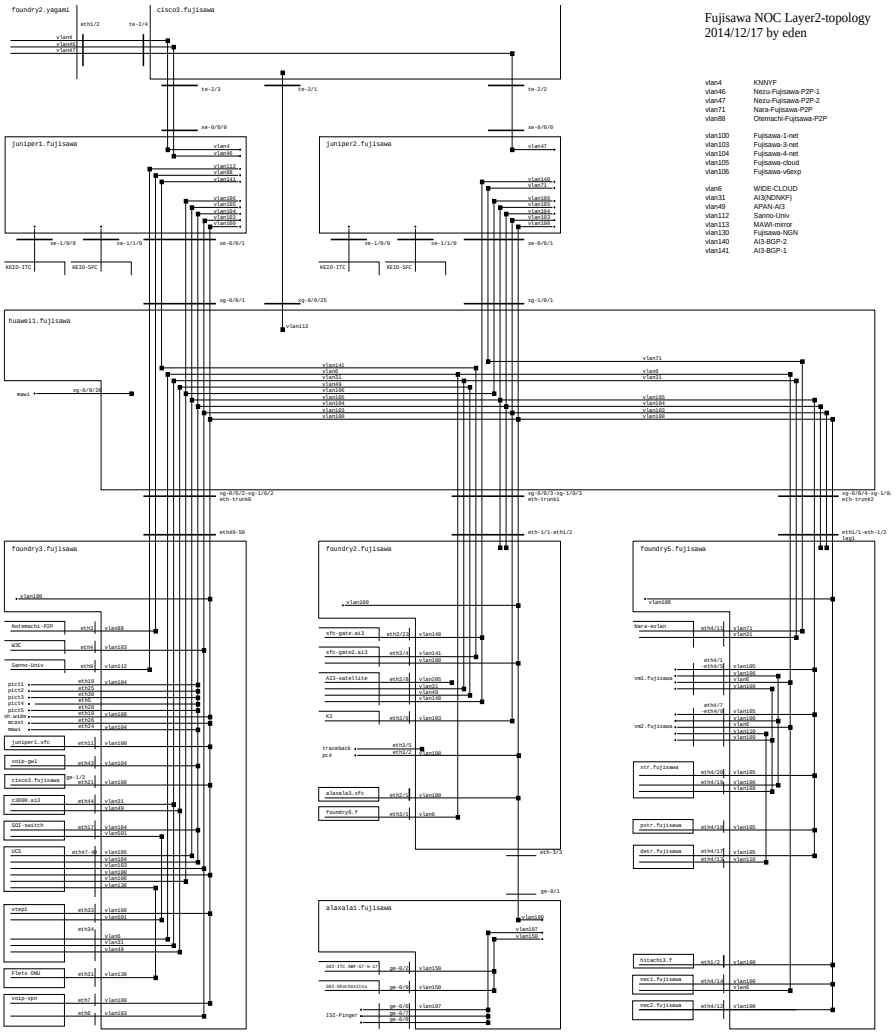

図 11: 藤沢 NOC Layer-2 トポロジ図

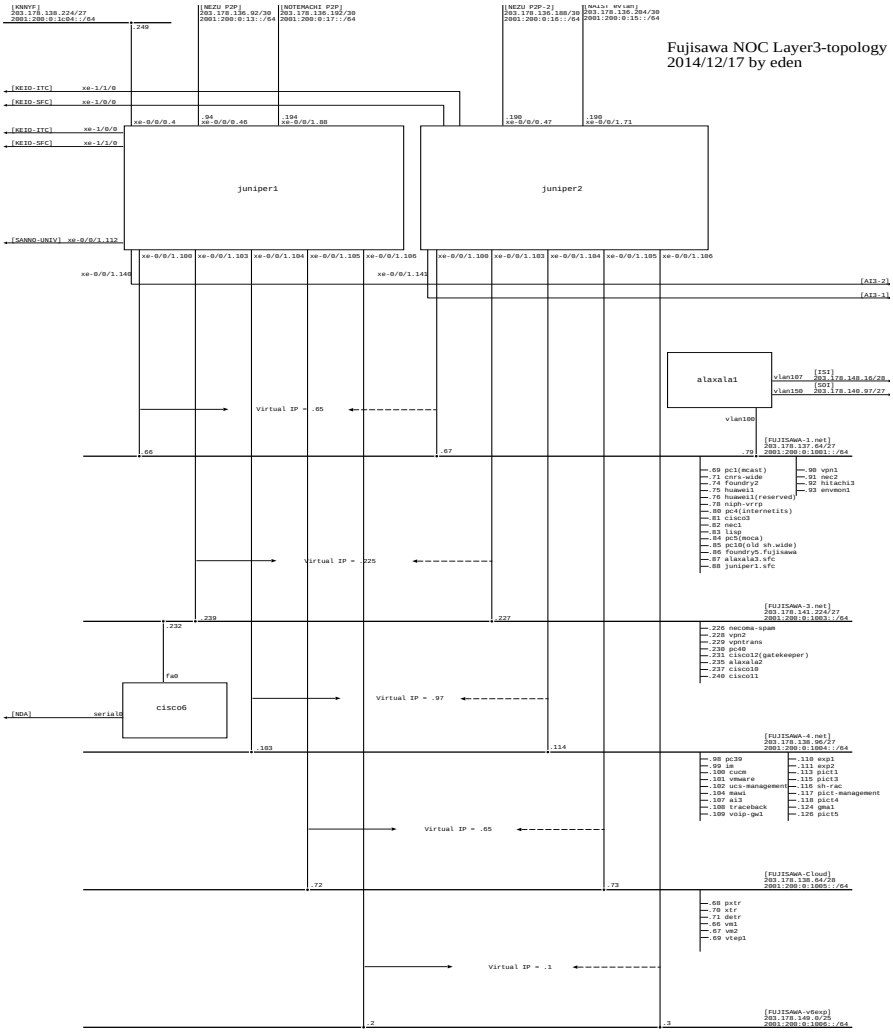

図 12: 藤沢 NOC Layer-3 トポロジ図

2.9 小松

小松 NOC は北陸先端科学技術大学院大学 (JAIST / 石川県能美市) 内に設置された NOC であり，同大学，NICT 北陸 StarBED 技術センター (通称: StarBED) 等への接続を収容している．NOC 間接続として関東および関西方面に対し複数のリンクを持ち，東阪間リンク障害時の迂回経路としての役割も担っている．

- (2014/03/15) 08:00–17:00 JAIST 全学停電に伴うサービス停止．

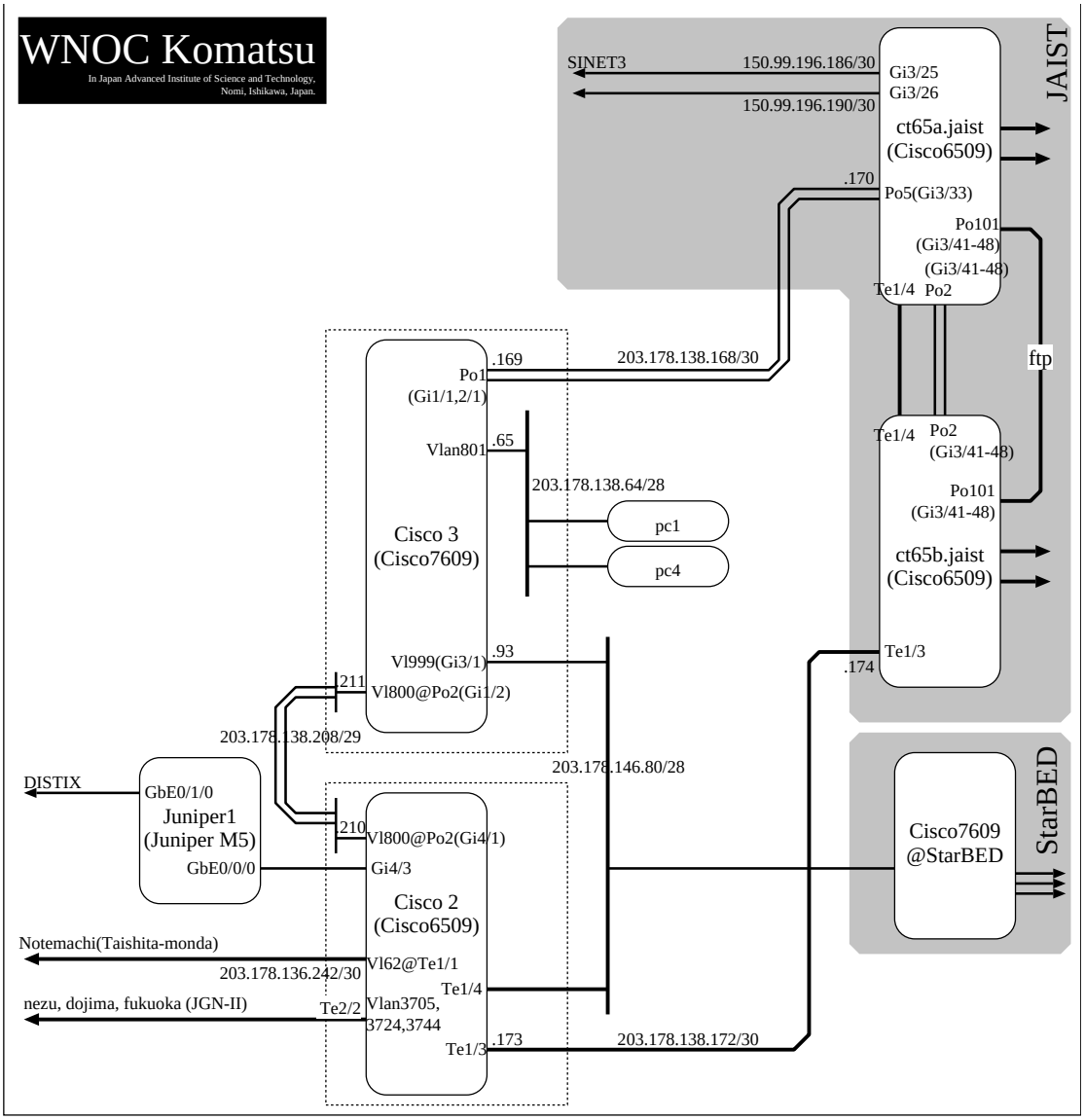

図 13: 小松 NOC

2.10 堂島

堂島 NOC は，WIDE プロジェクトのネットワークにおける西日本のコア拠点となっている．NTT テレパーク堂島第 1 ビルと第 3 ビルに拠点を構え，NTT 大手町 NOC とともに 10GigabitEthernet バックボーンの 1 点を担ったり，大阪における学術 IX(NSPIXP3) 拠点を担ったりしている NOC である．また，第 3 ビル内において JGN や SINET とも接続し，西日本方面の多数の NOC とリーフサイトを収容している．主に NSPIXP3 と WIDE バックボーンの接続を担っている `cisco2.dojima` の老朽化が顕著となっており，近い将来に向けたリプレースの検討が進んでいる．

- (2014/07/12) `juniper1.dojima` (Juniper MX240), `cisco5.dojima` (Catalyst 3560E-12D), `foundry6.dojima` (Foundry FLS624) 設置
- (2014/08/20) JGN-X 接続、`foundry4.dojima` 接続を `cisco2.dojima` から `cisco5.dojima` に収容変更
- (2014/08/28) NAIST 接続を `cisco2.dojima` から `juniper1.dojima` に収容変更
  KUSA 接続を `cisco2.dojima` から `cisco5.dojima` に収容変更
- (2014/08/29) SINET 経由 堂島–根津 開通
- (2014/11/20) 左京、小松、広島、福岡、NTT 大手町接続 IPv4/IPv6 収容を `cisco2.dojima` から `juniper1.dojima` に収容変更

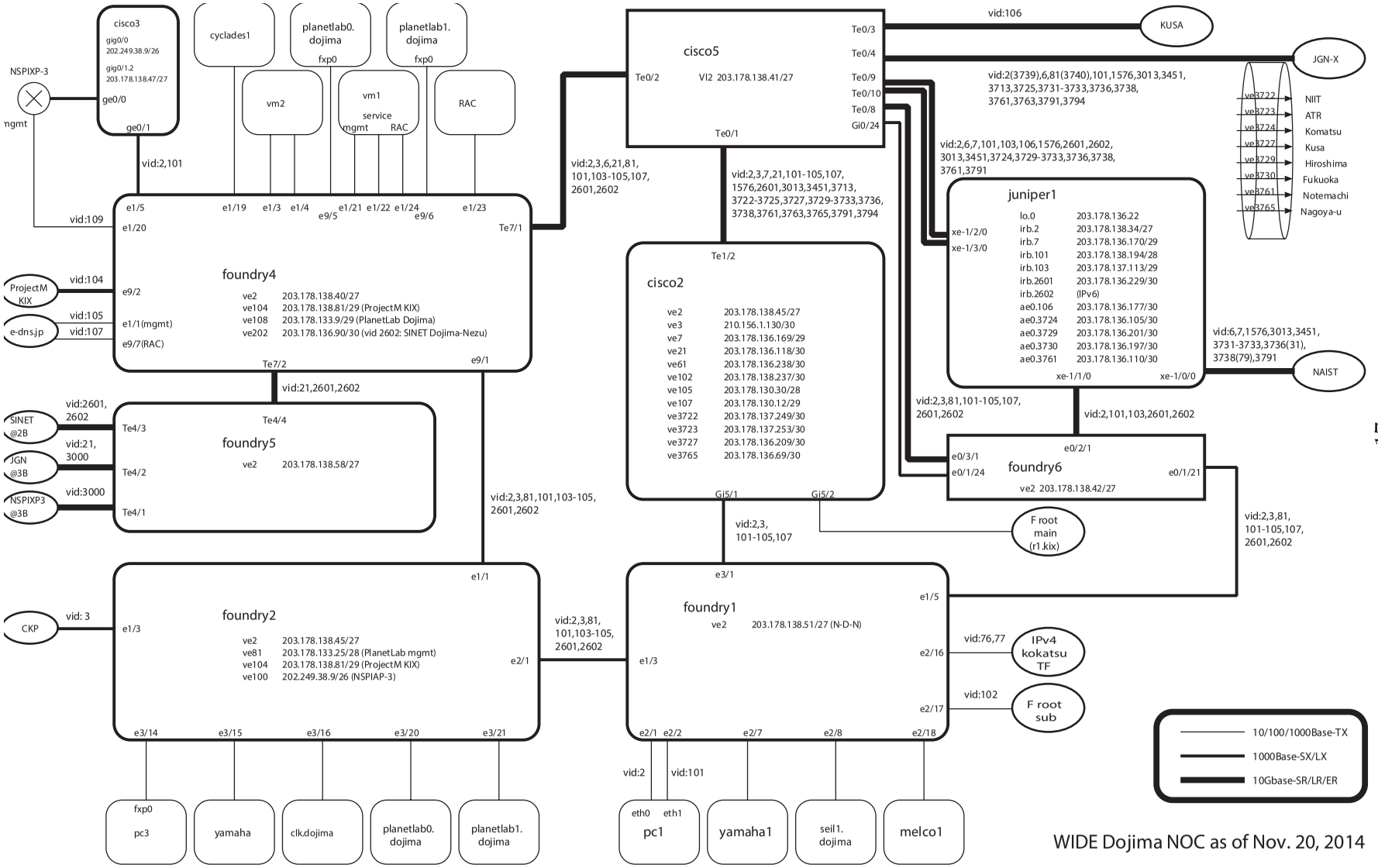

図 14: 堂島 NOC トポロジ

2.11 奈良

奈良 NOC は奈良先端科学技術大学院大学内にあり，大学および NOC 周辺の研究組織を収容するとともに AI3 と接続している．また，Debian JP 等の公式ミラーを始めとする 10 以上のミラーを提供する FTP ミラー (`ftp.nara.wide.ad.jp`) をサービスしている．

- (2014/8/28) 堂島収容ルータを cisco2.dojima から juniper1.dojima に切り替え
- (2014/11/20) 奈良 - 堂島線 L3 ルーティングポイントを cisco2.dojima から juniper1.dojima に切り替え

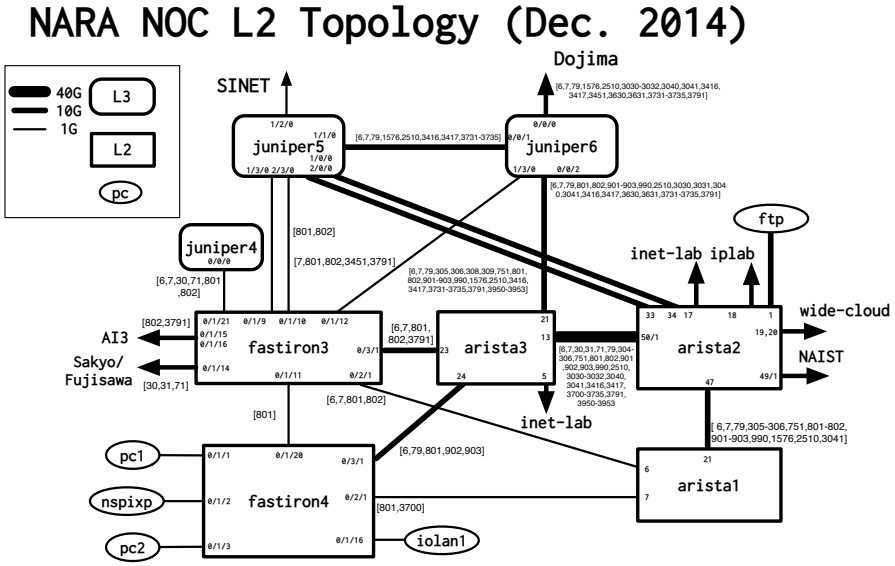

図 15: 奈良 NOC Layer-2 トポロジ

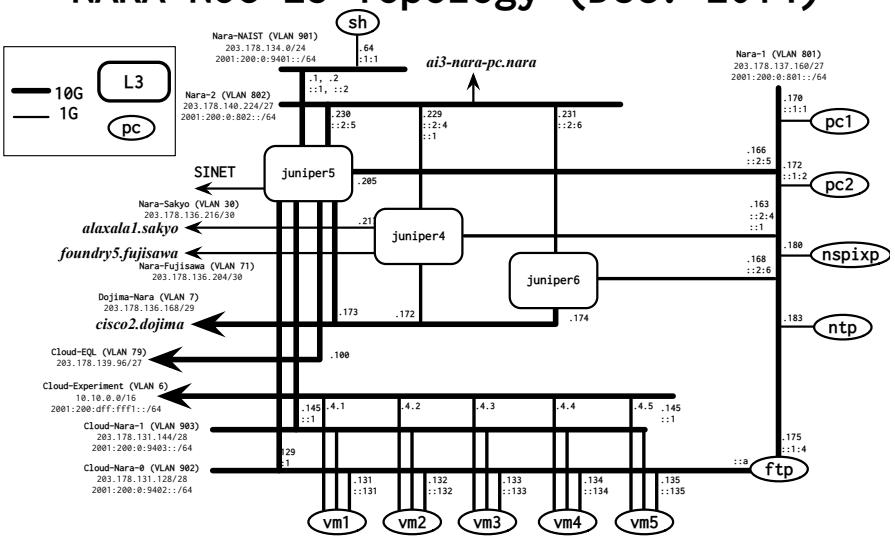

図 16: 奈良 NOC Layer-3 トポロジ

2.12 左京

左京 NOC は京都およびその周辺に存在する組織に対する接続拠点であり京都大学に設置されている.

- (2014/04/02) 対奈良 NOC 回線の切り替え

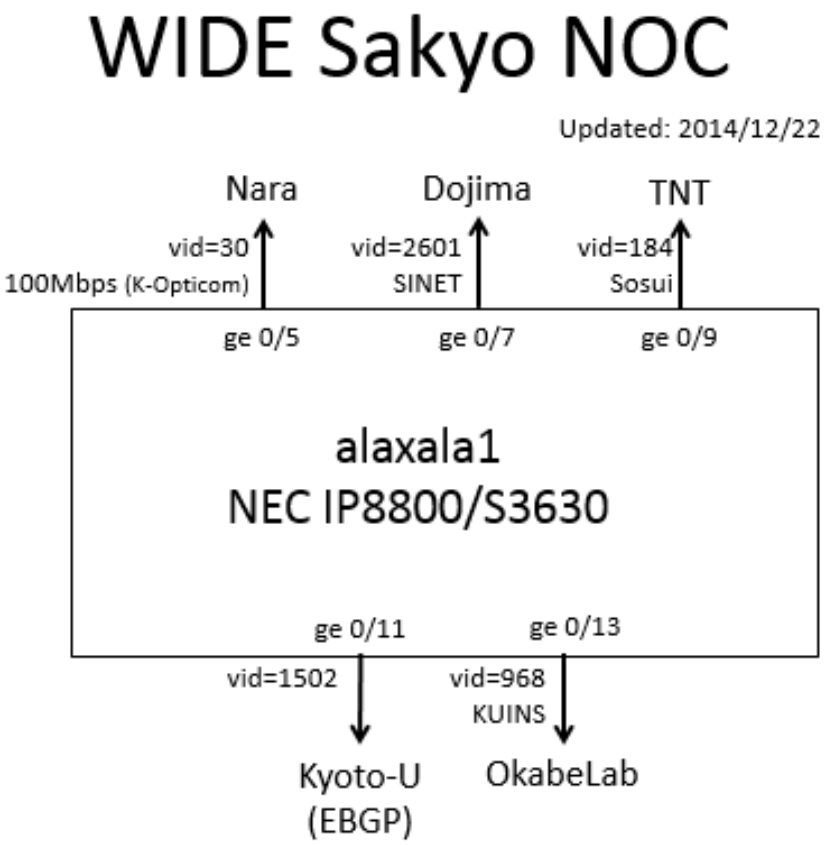

図 17: 左京 NOC

2.13 倉敷

倉敷 NOC は，平成 24 年度に学内ネットワーク機器の更新にともない NOC 機器の更新など全体構成の変更を実施した．外部接続回線を収容していた GS4K は ASR9K に更新し，対外的な L3 ルータのうち GR4K を Juniper MX80 に更新した．基本的な接続設定は，従前の装置の設定を踏襲している．また，倉敷 NOC 機器については，死活監視ツールで監視を行っているが特に大きな問題もなく運用されている．

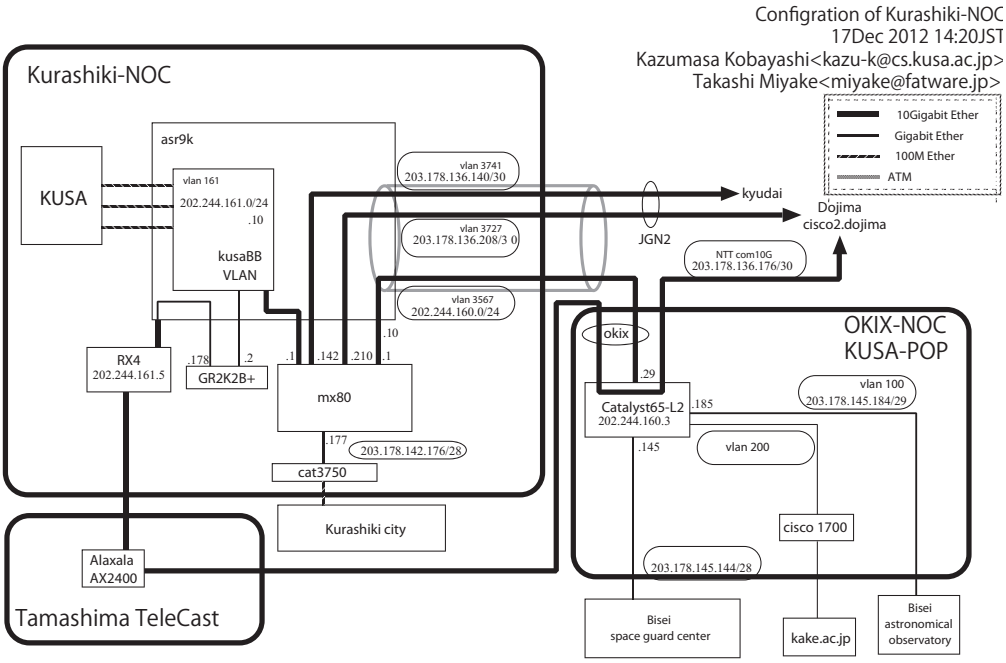

図 18: 倉敷 NOC

2.14 広島

広島 NOC は，トポロジー図の通り，大阪 NOC と福岡 NOC の中間に位置し，WIDE バックボーンに対して大阪〜福岡間の冗長性も同時に提供している．ソフトウェアルータによる運用を 2012 年より続けており，Xen Hypervisor 上で動く VM（Virtual Machine）である Vyatta Router を使用している．また，ローカルサービス用の Linux サーバも，同じ VM として動作させている．VM としての運用による問題はこれまで生じておらず，パフォーマンス，安定性ともに高い性能を維持できている．

大阪 NOC と福岡 NOC の接続には JGN-X の VLAN を経由しており，さらに地域プロバイダである SuperCSI を経由し，また設置場所である大学内もまた VLAN を経由して接続している．よって，各接続点での L2 SW は経路的に冗長化されておらず，運用上の注意が必要である．

- (2014/09/13) 大学内での VLAN トポロジの変更
- (2014/09/14) 法令点検による計画停電

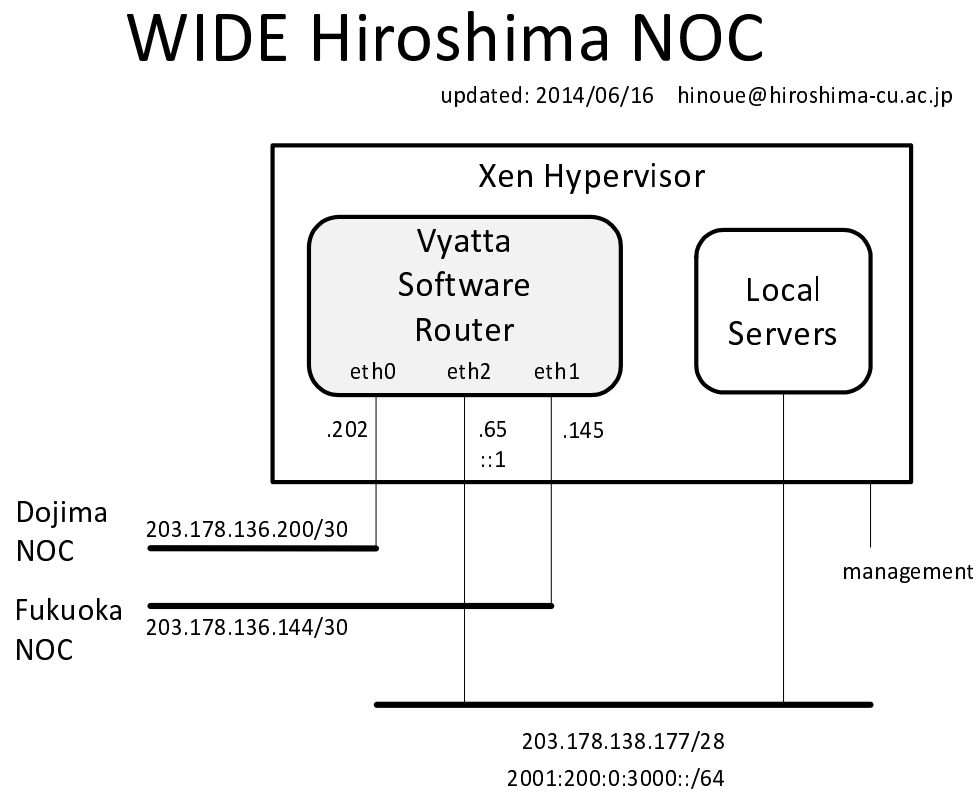

図 19: 広島 NOC

2.15 福岡

福岡 NOC では、日立 GR2000 をコアルータとして運用を行なっている。支線は 2 つあり、それぞれ帯域を必要としないローカル実験用の 100Mbps のセグメントと、グローバル実験用の 1Gbps のセグメントである。ローカル実験用の経路情報は現在、インターネットには広告していない。

将来は、仮想化ルータを導入し、NOC 仮想化および再構成を計画しているが、着手できていない。

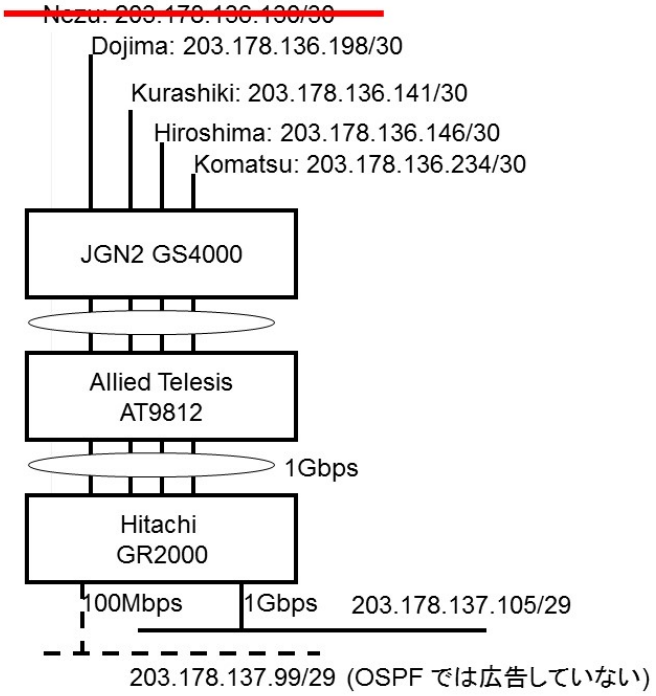

図 20: 福岡 NOC

2.16 バンコク

2007 年 5 月 15 日に設置されたバンコク NOC は，NECTEC や UniNET といったタイの学術研究組織との研究活動強化を目的に設立された．今年度も引き続き，WIDE プロジェクトとしての独自の回線は存在しないが，JGN-X の回線を利用し，VLAN を用いて WIDE インターネットをバンコクまで延長し，IPv4，および IPv6 の接続性を提供している．バンコク NOC は，JGN-X バンコク回線を収容している NECTEC と同じ建物に存在し，そこから UTP ケーブルを延伸し，バンコク NOC が存在する部屋にネットワークを引いている．バンコク NOC の主な利用者は，バンコクを中心に活動している SOI Asia プロジェクトのメンバーである Patcharee Basu，および関係者になる．

2013 年 1 月に故障したルータ (pc1.bangkok) の代替として、2013 年 10 月に yamaha rtx810 が設置され、接続性が回復した。

- 2014 年は構成変更や障害等はなかった。

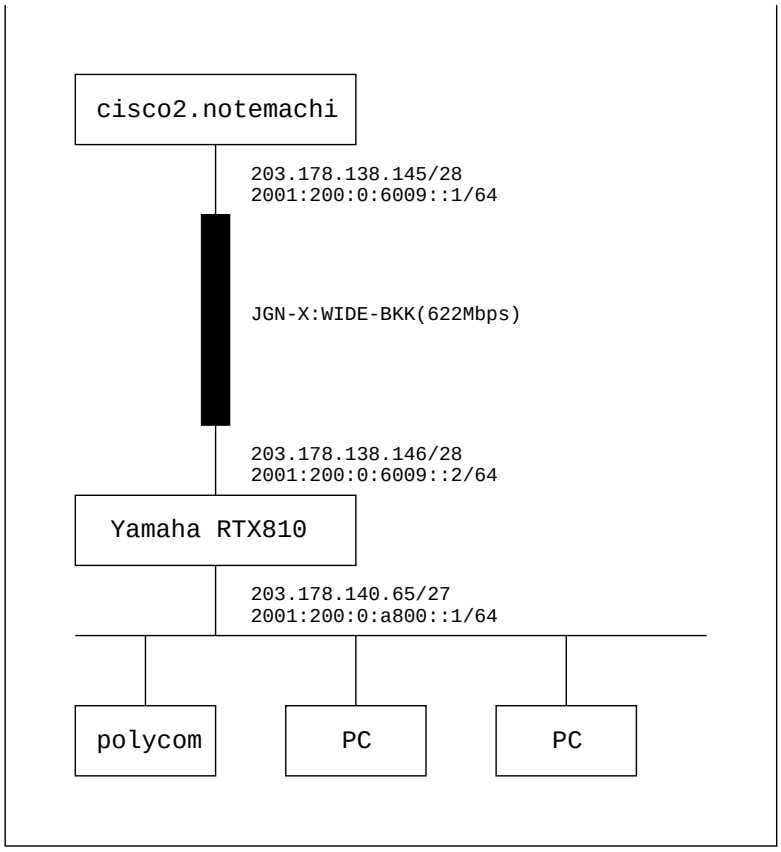

図 21: Bangkok NOC

3　WIDE-BB における Vxlan トライアル

近年、Virtual eXtensible Local Area Network (VXLAN)[1] をはじめとした複数のオーバーレイネットワーク構築を目的としたプロトコルが標準化され、データセンタ内など一部の閉域網において実際に運用されている。これらのプロトコルを用いることで、レイヤ 3 で接続されたノード間でレイヤ 2 のオーバレイネットワークを構築することが可能になる。two-WG では広域レイヤ 2 ネットワークを構築・運用するための技術として VxLAN を新たに導入し、運用負荷の軽減を図る。

WIDE-BB では、レイヤ 2 ネットワークにおいて特に冗長性の確保を行う必要がある場合、スパニングツリープロトコルが使用されている。スパニングツリープロトコルはレイヤ 2 での冗長性確保を可能にするが、WIDE-BB 上に OSPF を用いて構築されているレイヤ 3 ネットワークとは独立して動作し、管理すべきトポロジがツリー毎に増大していくため、オペレータにとって運用負荷が高いという問題があった。また、WIDE-BB を構成する各拠点の対外接続用装置がレイヤ 2 ネットワークをバイパスする機能を持たない場合があり、別途レイヤ 2 ネットワークを通すためのリンクを用意するなど、トポロジが複雑化するという問題があった。このような複数拠点にまたがるレイヤ 2 ネットワークに起因する問題は、オーバレイネットワーク技術によって解決可能である。two-WG では、拠点間 VLAN をオーバーレイネットワークによる運用に移行することを目標として、本年度より拠点間広域 VxLAN ネットワークの構築実験及び導入を進めている。本年度行った主な活動内容は以下の通りである。

1. 広域 VxLAN ネットワーク構築実験
2. 構築実験に基づいた構築方針の決定
3. 一部拠点における実運用開始

3.1　広域 VxLAN ネットワーク構築実験

two-WG では、VxLAN を実際の運用に用いる事前準備として、広域 VxLAN ネットワーク構築実験を行った。実験の概要を図 22 に示す。また、実験に用いたパラメータを表 1 に示す。

実験の事前準備として WIDE-BB 内マルチキャスト網の設定見直しを行い、WIDE-BB 内のレイヤ 3 ルータの大部分に実装されている PIM-SM を大手町 NOC-藤沢 NOC 間で有効にした。さらに、VxLAN によりカプセル化されるフレーム長を考慮し、NTT 大手町 NOC-藤沢 NOC 間の IPMTU を 9000 バイトに変更した。以上の設定後、Linux kernel 内で VxLAN を有効にすることにより、大手町 NOC-藤沢 NOC 間の VxLAN ネットワーク上で、vlan を用いたレイヤ 2 通信が可能であることを確認した。

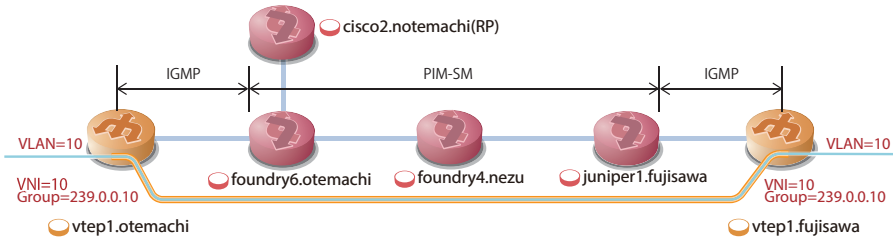

図 22: 広域 VxLAN ネットワーク構築実験の概要

表 1: 実験に用いたパラメータ

VNI	10
VLAN ID	10
マルチキャストアドレス	239.0.0.10
マルチキャストルーティングプロトコル	PIM-SM
マルチキャスト RP	203.178.136.29
マルチキャスト TTL	16
実装	Linux kernel 3.11.3 の VxLAN モジュール

3.2 構築実験に基づいた構築方針の決定

two-WG では、実験結果を受けて実網を構築するための方針を検討し決定した。WIDE-BB 上に VxLAN ネットワークを構築するにあたり、VxLAN 上のネットワーク識別子である VNI、VLAN ID、マルチキャストアドレスの対応関係を考慮する必要がある。two-WG 内での検討の結果、これらの識別子は全て 1 対 1 に対応させることとした。これは、VxLAN ネットワーク上の Broadcast/Unknown-Unicast/Multicast(BUM) フレームの配送先を最小化することを重視したためである。表 2 に、実際のパラメータ生成ルールを示す。

表 2: 構築パラメータ

VNI	任意
VLAN ID	VLAN ID
マルチキャストアドレス	239.0.VNI の上二桁.VNI の下二桁
マルチキャストルーティングプロトコル	PIM-SM
マルチキャスト RP	203.178.136.29
マルチキャスト TTL	16
実装	限定しない

さらに、VxLAN を運用する際には、網内の IP MTU を考慮する必要がある。VxLAN は Ethernet フレームをカプセル化して転送するため、カプセル化後のパケット長が 1500 バイトを上回る場合がある。一方で、動作中のネットワークの IP MTU を変更する際ネットワークの断を伴う場合があり、WIDE-BB 内には 1500 バ

イト以上の IP MTU が使用不可能な機器があることも想定されるため、全ての拠点間で 1500 バイトより大きい IP MTU を確保することは困難である。本問題については two-WG での検討及び実験の結果から、カプセル化後の IP フラグメントを許容し、アンダーレイネットワークの IP MTU は 1500 バイトを想定することとした。

3.3 一部拠点における実運用開始

本年度の活動として、two-WG 内で行った事前実験及び構築方針を踏まえ、WIDE-BB 内藤沢 NOC において拠点間 VLAN を VxLAN ネットワークへ移設する作業を行った。図 23 に現在の WIDE-BB における VxLAN ネットワークの概要を示す。藤沢 NOC では計 3 つの拠点間 VLAN を使用しており、全て VxLAN への移設を完了している。また、大手町 NOC、奈良 NOC については VTEP の設置が完了している。これらの NOC については順次拠点間 VLAN を VxLAN ネットワークに移設する予定である。NTT 大手町 NOC、北陸 NOC、堂島 NOC、小金井 NOC については今後 VTEP を設置予定である。

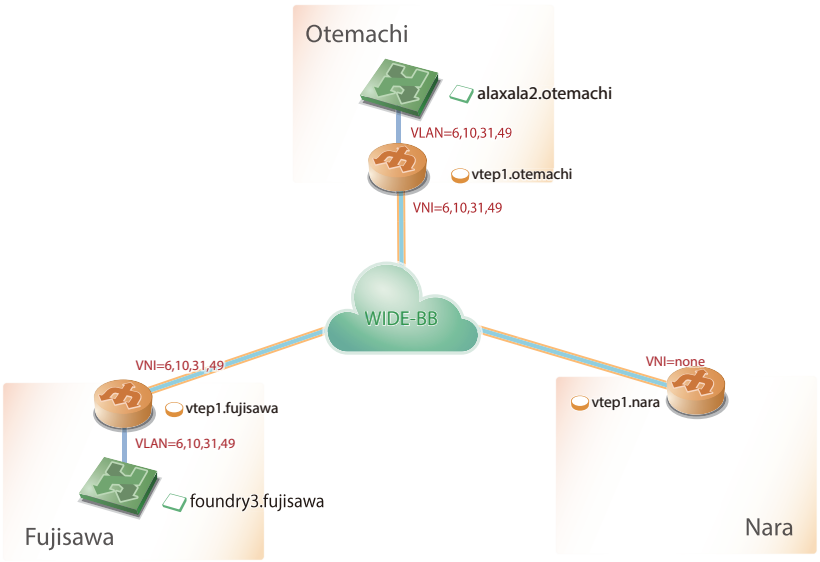

図 23: 現在の WIDE-BB における VxLAN ネットワーク

なお、two-WG では、現在 VTEP の実装として Linux kernel のみを使用している。Linux kernel ではバージョン 3.7 以降デフォルトで VxLAN をサポートしており、vxlan stanza[2] を導入することで標準インターフェースと同様に VxLAN の設定を行うことができる。以下に vxlan stanza を使用した設定例を示す。

```
auto vxlan{VNI}
iface vxlan{VNI} inet manual
    vxlan-vni {VNI}
    vxlan-group {Multicast addr}
    vxlan-dev {Physical interface}
    post-up ifconfig vxlan{VNI} up
    post-up ifconfig vxlan{VNI} mtu {MTU}
```

参考文献

[1] M. Mahalingam, D. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright. Vxlan: A framework for overlaying virtualized layer 2 networks over layer 3 networks, RFC 7348. IETF, August 2014.

[2] vxlan stanza. `https://github.com/upa/vxlan-stanza`. Retrived: December 2014.

4 Open Redirect ノード対策

DNS，NTP，Chargen，SNMP などUDP ベースのプロトコルでグローバルにアクセス可能になっているノードが反射型分散サービス攻撃 (Distributed Redirection Denial of Service) の反射ノードとして使われることが問題となっている．WIDE バックボーン外部からの忠告や停止依頼などのセキュリティインシデントとして発生し，反射ノードとして悪用されているノードの存在の確認と対応を数多く行った．本節では WIDE バックボーンでの Open Rediret ノード対策に関してまとめる．

4.1 2014 年度における Open Redirect ノードに関するセキュリティインシデント

2014/01/15 : mawi のトラフィック観測にて src port 123, dst port 123 の UDP トラフィックがトランジット回線に流れていることが確認される．WIDE バックボーン内のサーバや配下のネットワークのノードに関しては連絡し，対応を依頼した．

2014/02/05 : DDOS Attack from 133.4.0.37:123 から DDoS 攻撃を受けているとのセキュリティインシデントの報告が外部から寄せられ，対応を行う．

2014/02/06 : two コアオペレータにて ntpdate -b に応える且つ増幅するバックボーンルータを数多く特定する．対応できるものから各ルータにて ACL 設定を投入する．

2014/02/10 : トランジット回線にてトラフィック観測を行ったところ，NTP に応答する，外部からの NTP リクエストに応答すべきではないノード（ルータや踏み台サーバなど）が数多く存在し，NTP refection 攻撃に利用されていることが明らかとなり，トランジットにて ACL を設定する．また，各ノードの管理者にノード側での適切な ACL 設定を依頼する．

2014/02/25 : 202.249.2.194 が不正利用されている NTP だとのセキュリティインシデント報告が外部から通知される．IPv4 アドレスの利用者に連絡し，ACL の設定を投入してもらう．

2014/02/28 : APNIC や JANOG のメーリングリストなどで一般的な NTP reflection に対する ACL の設定方法が広く共有される．

2014/03/14 : Open NTP ノードが WIDE バックボーンに存在して，そこから攻撃されているとのセキュリティインシデントの対応依頼が送られてくる．l 調査の結果 kix-mon.edns.jp が Open NTP ノードになっていることがわかり，適切な NTP 設定を施すことで対応した．

2014/08/31 : 203.178.141.90 が chargen の Open Redirection ノードになっており DDoS に利用されているとのセキュリティインシデントが報告される．調査の日立ケーブル製の光アンプ装置のマネジメントアクセスポートに割り当てらてた IPv4 アドレスであることがわかり，かつ，ファームウェアアップデートも行えない古い機種であること，マネージメントポートと光アンプ部は独立して動作しており死活監視にならないこと，などが確認されたため，yagami NOC にて リンクダウン設定を行った．

2014/09/08 : 203.178.134.128, 203.178.134.127, 203.178.134.53 が Open SNMP ノードとして DDoS 攻撃に利用されているというセキュリティインシデントの連絡を受ける．該当ノードはポリコムと cisco telepresence ノードで，連絡後奈良 NOC にて適切な SNMP の設定を行った．

2014/09/28 : 203.178.142.235 が Open SNMP ノードとして DDoS 攻撃に利用されているというセキュリティインシデントの連絡を受ける．根津 NOC にて対応を行った．

2014/11/01 : JPCERT/CC から 203.178.142.210 が NS の再帰的な問合せ (recursive queries) を使った DDoS 攻撃の踏み台として使用されているとの報告が入ったとの連絡が来る．該当ノードの管理者によって DNS 設定が見直され対応された．

2014/11/28 : 203.178.142.235 が Open SNMP ノードとして DDoS 攻撃に利用されているというセキュリティインシデントの連絡を受ける．根津 NOC にて該当ノードの SNMP を一旦停止し，その後ルータで ACL を設定して対応する．

2014/12/19 : 203.178.143.11 が Open Recursive Resolver になっており DDoS 攻撃に不正利用されているとのセキュリティインシデントの報告を受ける．ひとまず，cisco2.notemachi にて OSPF の設定で/32 のブラックホール経路を書き，トラフィックを制限する．その後，藤沢 NOC にて該当ホストの DNS 設定の見直しと設定変更をおこない，ブラックホール経路を元に戻すというインシデント対応を行った．また，OSPF によるブラックホール経路フィルタは簡単で便利なため今後も利用する方針となった．

4.2 OSPF によるブラックホール経路フィルタリング

前節の報告で説明したように 201412 月 19 日のセキュリティインシデントから OSPF を用いたブラックホール経路フィルタによる DDoS 攻撃緩和（抑制）を実施し始めた．下記が cisco 製のルータによるブラックホール経路の設定例である．

```
ip route 203.178.143.11 255.255.255.255 Null0 tag 666
!
route-map static-opsf permit 999
 match tag 666
 set metric 1
 set metric-type type-2
!
```

5　おわりに

本年度も WIDE バックボーンネットワークの安定運用を行ってきた．来年度は，VXLAN の本格運用や OSPF 計測の再開など広域運用環境を用いた実験を精力的に行っていく予定である．

6　CopyRight