第25部

WIDEネットワークの現状

遠峰 隆史、近藤 賢郎、豊田 安信、澤田 開杜、石原 匠、斉藤 楽、宇多 仁、
小林 和真、松本 智、菊田 一真、関谷 勇司、中村 遼、山本 成一

第１章　はじめに

WIDEバックボーンネットワークは我が国の各地に拠点（NOC，Network Operation Center）を持つ広大なレイヤ2およびレイヤ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．2024年の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う．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．

第２章　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2024年1月1日から2024年12月31日までの運用報告と2024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2024年12月31日現在のWIDEバックボーンの概略図である．

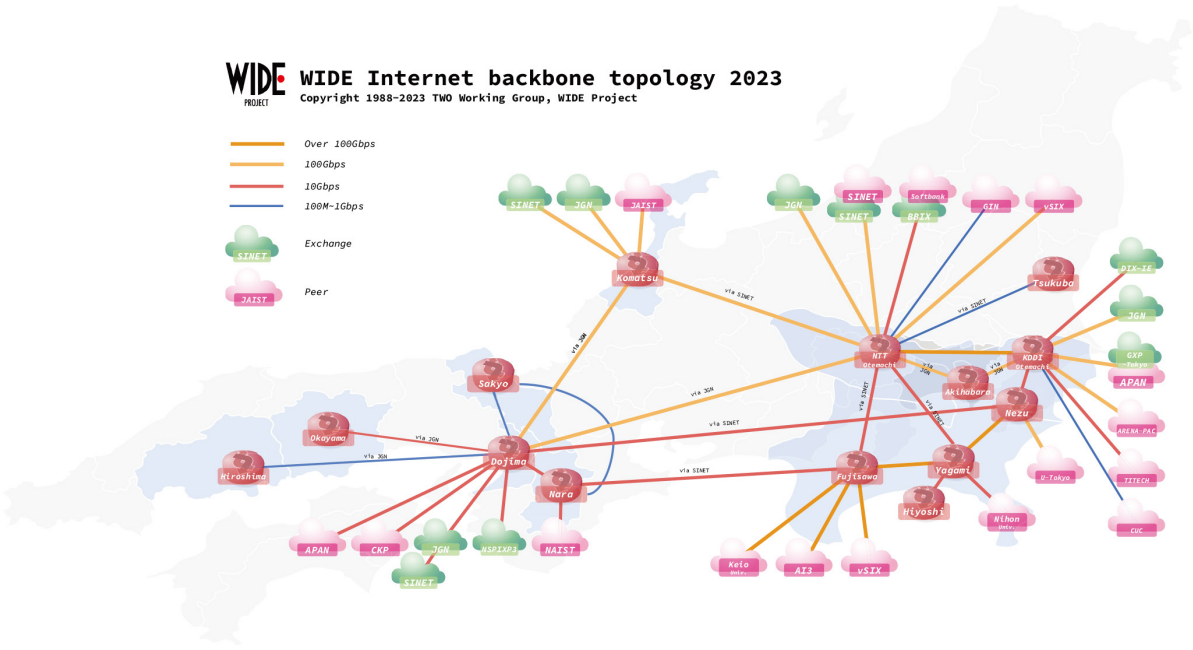

図1　WIDEバックボーントポロジ

2.1　本年度の活動方針

例年と同様に本年も主に100Gbps，10Gbps回線に基づいてWIDE-BBを運用した．昨年度より順次実施していたWIDE NOC拠点のリファクタリングはKDDI大手町拠点で引き続き実施され，引き続き堂島拠点においても実施した．KDDI大手町拠点と堂島拠点ともに使用していない機材を棚卸しして今後の研究活動にて利用可能な機材設置のスペースを確保した．岡山拠点は堂島拠点との接続に利用していたJGNによる回線サービスの利用終了にともない，WIDE NOC拠点としての運用が終了した．

2024年を通して矢上拠点と根津拠点間の回線において伝送装置の不調が継続している．当該区間の回線は藤沢拠点から大手町拠点にまで到達するために必要なWIDEバックボーンの基幹回線のひとつで，復旧に向けて新しい伝送装置の手配が進んでいる．当該回線が復旧するまでの間は，慶應義塾が利用するSINET回線上に設置されたL2VPNサービスにより藤沢拠点とNTT大手町拠点とを直通させるバックアップ回線が利用されている．

2.2　筑波

筑波NOCは筑波大学内に設置されており、パブリックミラーサービスの提供や筑波大学内の実験ネットワークとの接続を行っている。

筑波NOCはSINET L2接続サービスを利用してNTT大手町NOC（notemachi）と接続しており、現在接続の10Gbps化を進めている。2023年12月31日時点で筑波NOCからSINET L2接続サービスまでの経路の10Gbps化が完了している。今後は筑波NOC内の設備の10Gbps対応やNTT大手町NOC側の設定の確認などを行う予定である。

パブリックミラーサービスには、1日当たり概ね150～200万件のリクエストが発生している。2021年にサーバー機器を更新し、同時にミラー同期管理方式や機器監視方式の変更を行った。現在はミラー同期管理方式としてsystemdを用いた同期スケジュール管理を、機器監視方式としてZabbixを採用している。

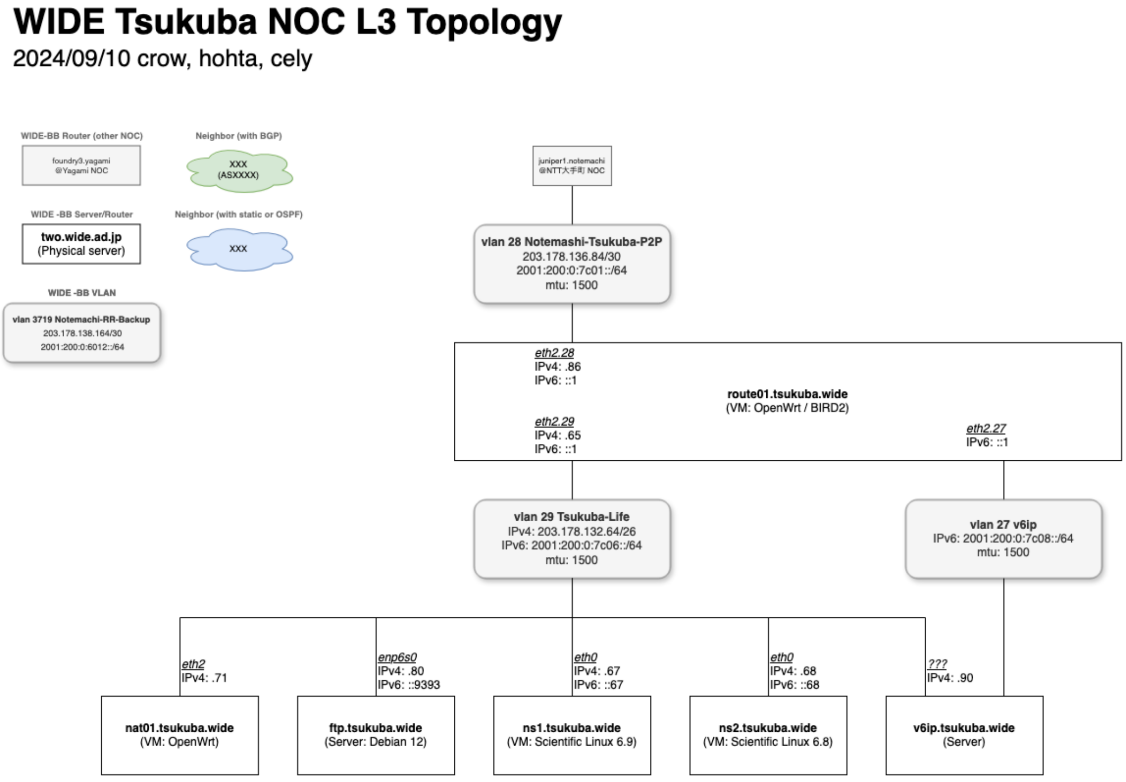

図2　筑波NOC L3トポロジ

- (2024/04)WIDEバックボーンとの接続機器をソフトウェアルーターに変更
- (2024/08)notamachi SINET接続でのSINET側障害に伴い予期せず全断(冗長接続の検討を開始)

2.3 根津

根津NOCは，WIDE関東地区の重要な接続拠点として，東京大学や東芝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．2021年は根津NOCの設置されている東京大学情報基盤センターの耐震改修工事に伴い今までの本館から別館にNOCを移設した。またこの作業に伴い、コアルータをMLXe4からJuniper NetworksのMX204にリプレースした。

2.4 NTT大手町

NTT大手町NOC (notemachi)は，1999年終りから稼働した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を設置しISPおよび学術研究NWを収容している．

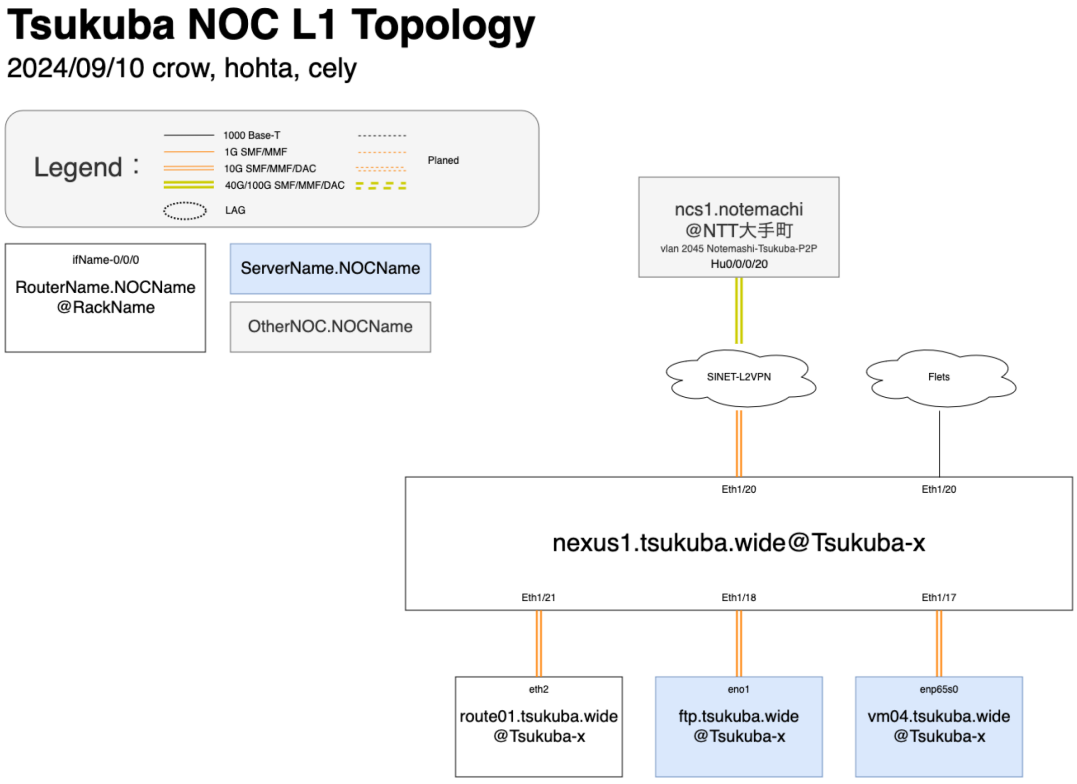

図3 筑波NOC L1トポロジ

2.5 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．

2.6 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，同大学理工学部とデジタルメディアコンテンツ統合研究センターおよび周辺の研究組織を収容している．慶應義塾との間のBGP接続の点では，藤沢NOCにおける接続のバックアップピアとしての機能を担う．またWIRT（WIDE CSIRT）によるネットワークトラフィック計測とその異常検知に関わる基盤の運用も担っている．

• （2024/8/25）矢上キャンパス法定停電対応

2.7 藤沢

藤沢NOCは慶應義塾大学湘南藤沢キャンパスデルタ館内に所在し，慶應義塾大学や同・村井研究室の他、周辺のWIDE内の研究プロジェクトとの相互接続を行っている．またW3CやAI3のような外部研究組織へののインターネット疎通性提供や，ccTLD及びccSLD権威サーバの運用も担う．

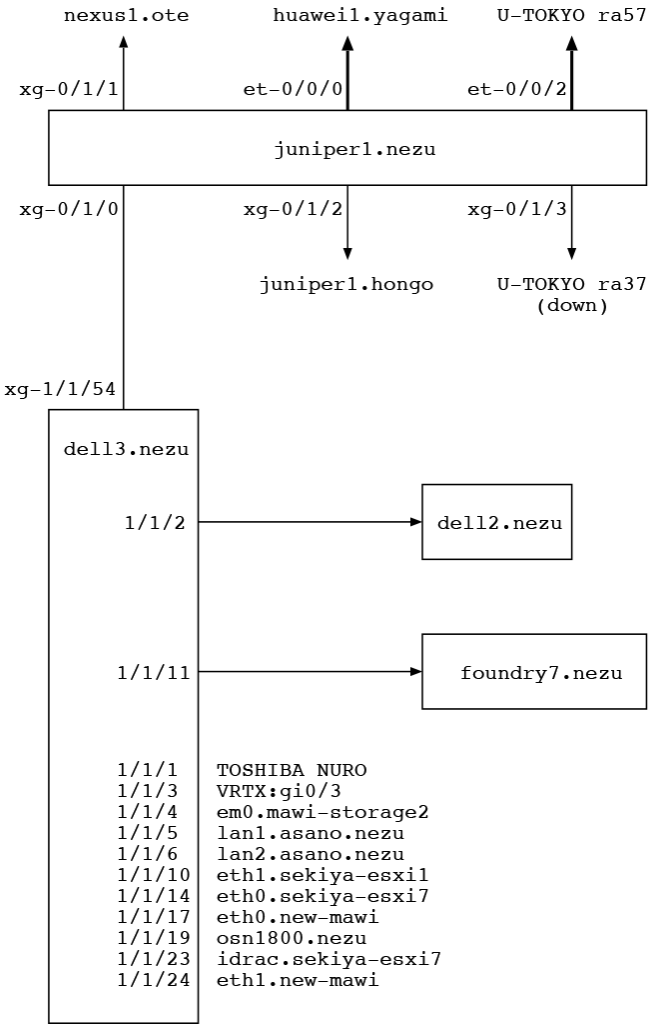

図4 根津NOC

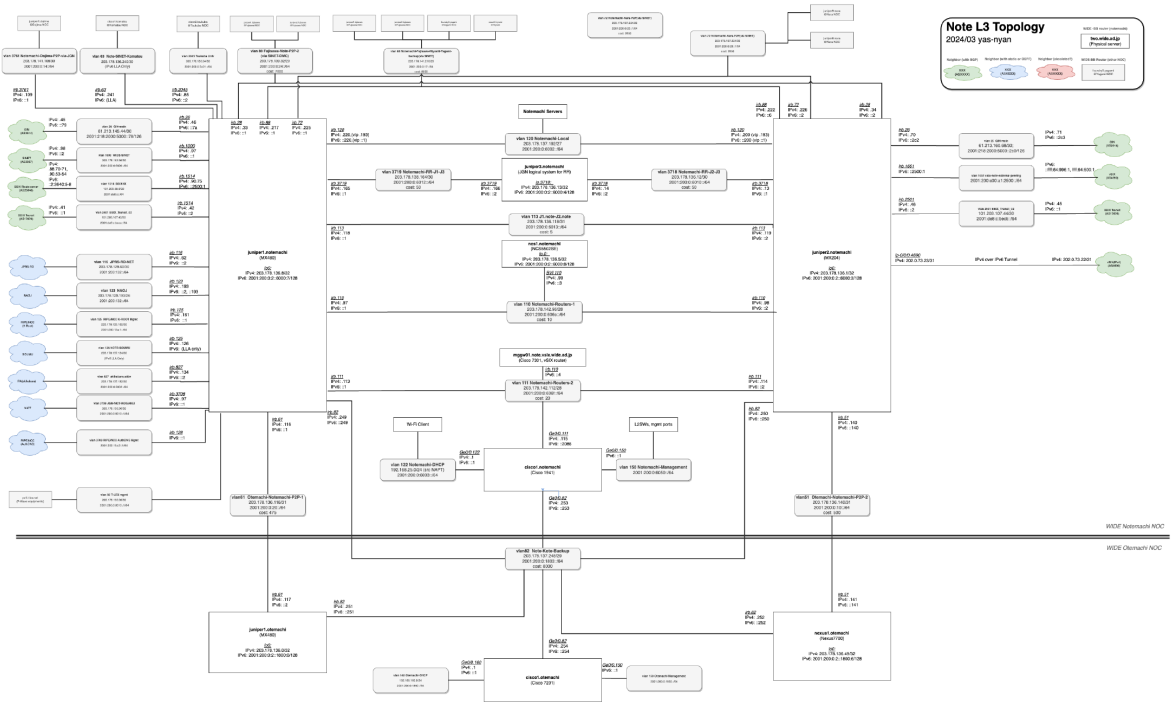

図5 NTT大手町NOC

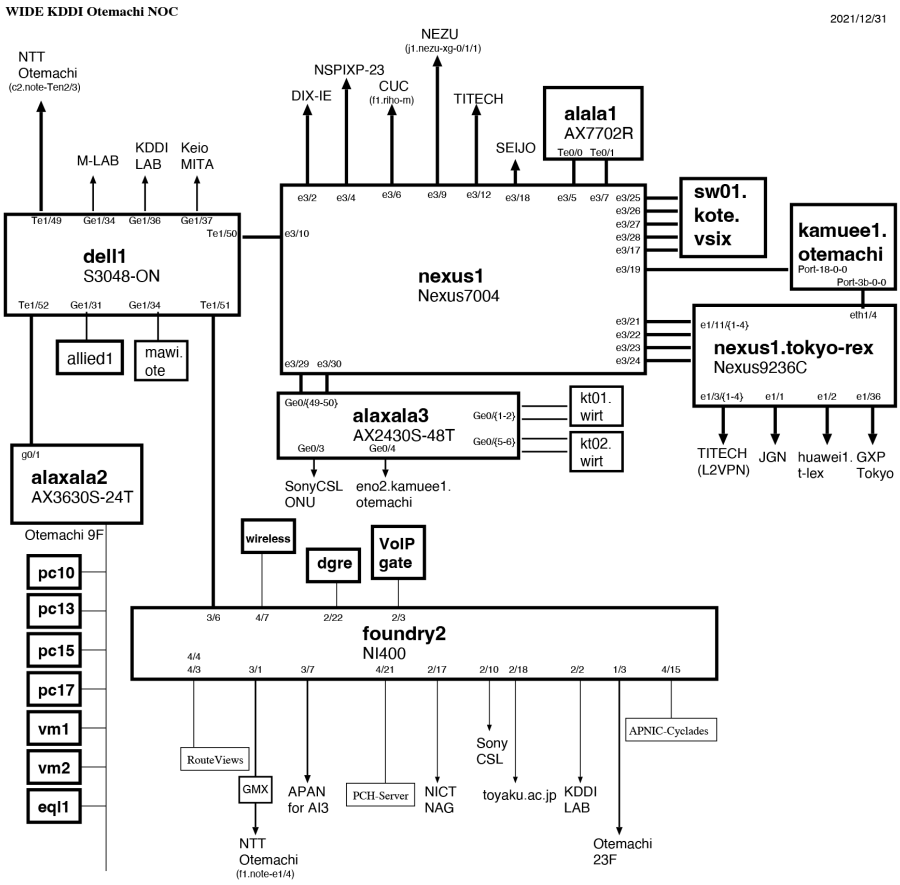

図6 KDDI大手町NOC

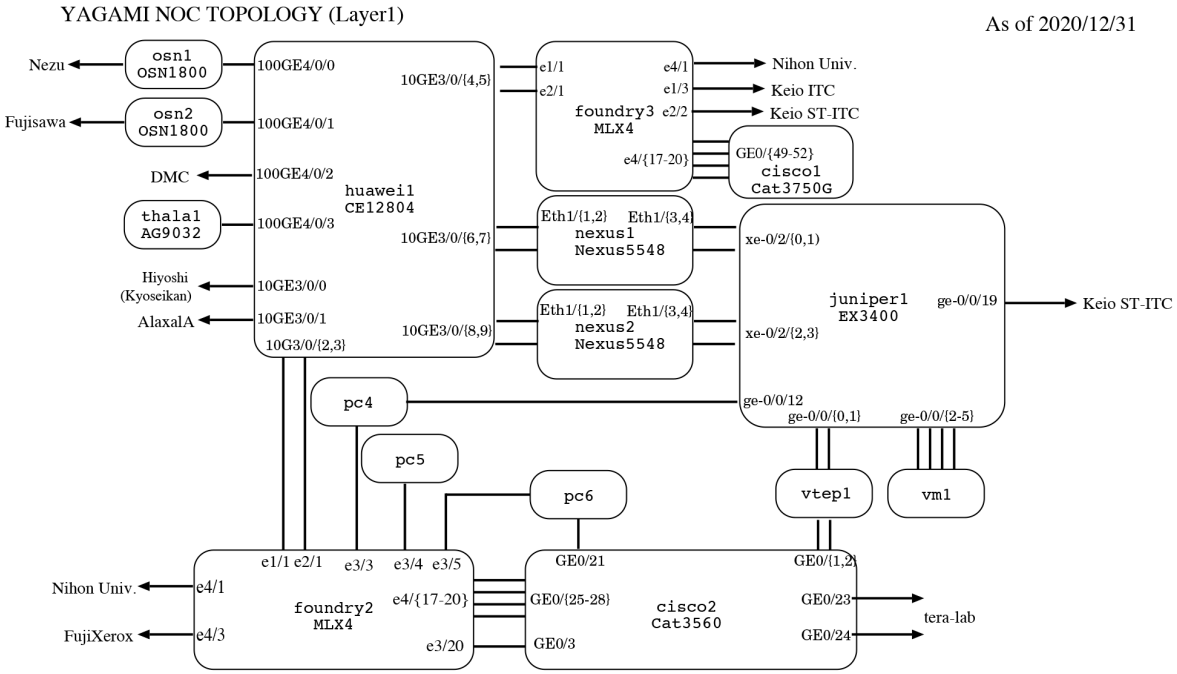

図7 矢上NOC Layer-1トポロジ.

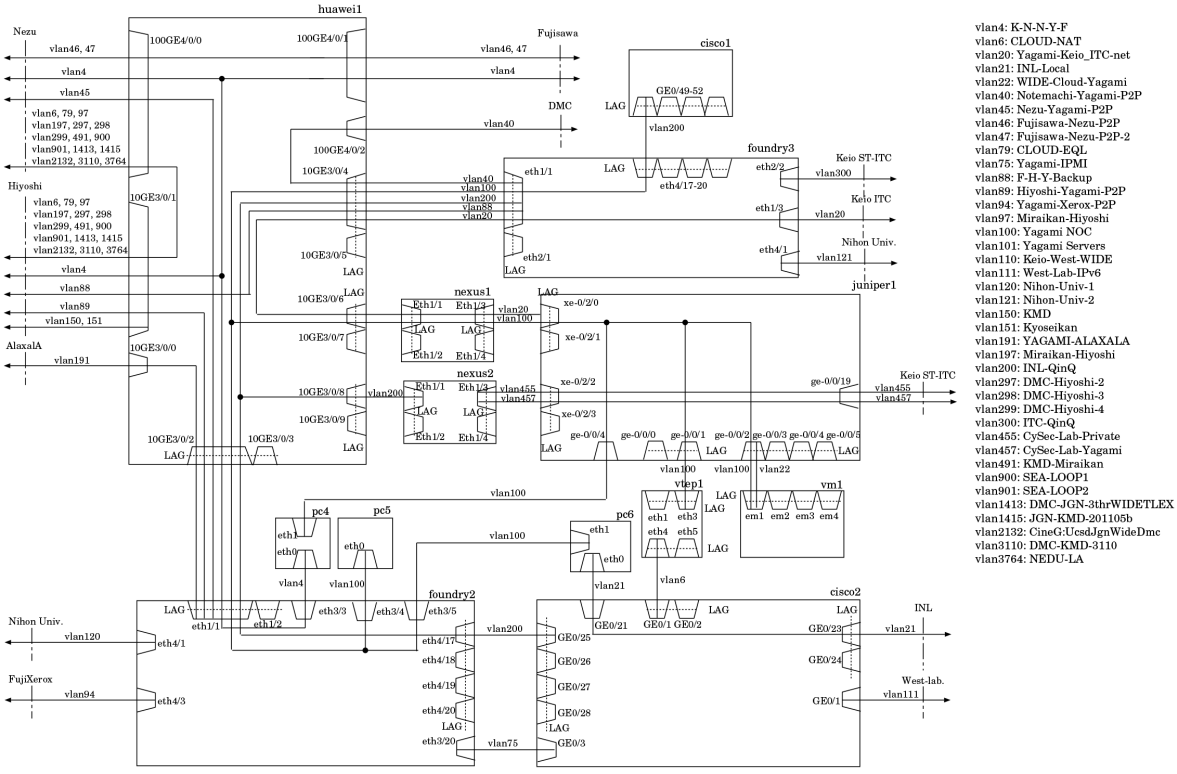

図8 矢上NOC Layer-2トポロジ.

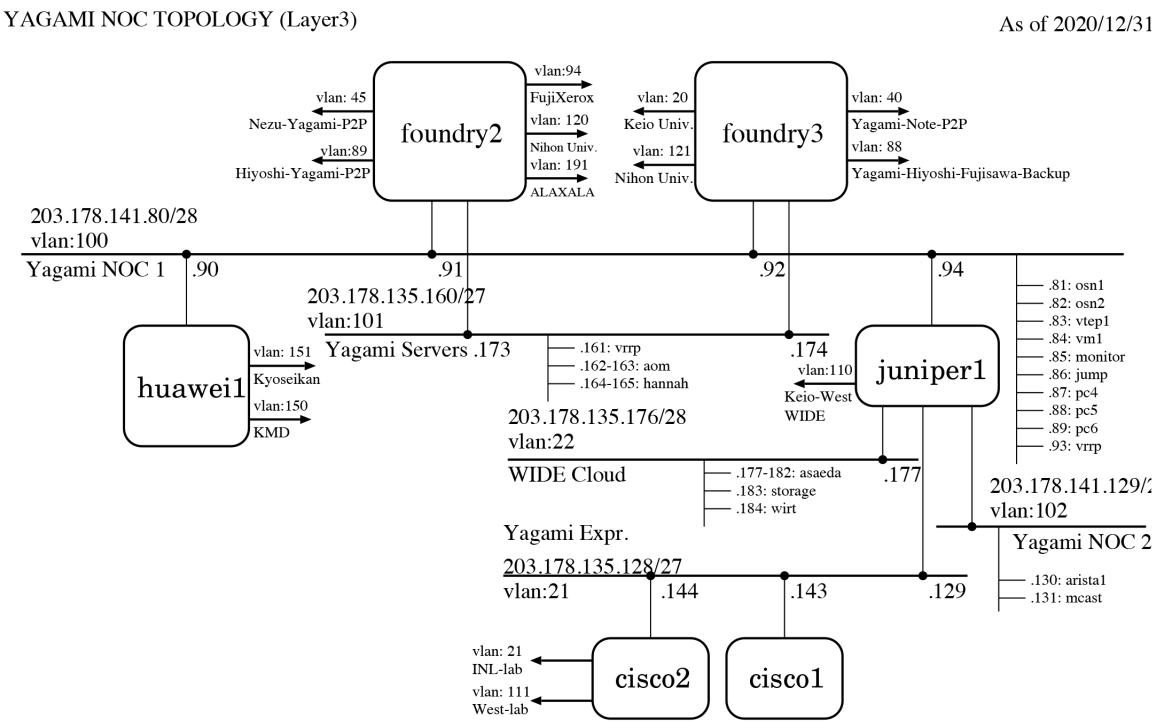

図9 矢上NOC Layer-3トポロジ.

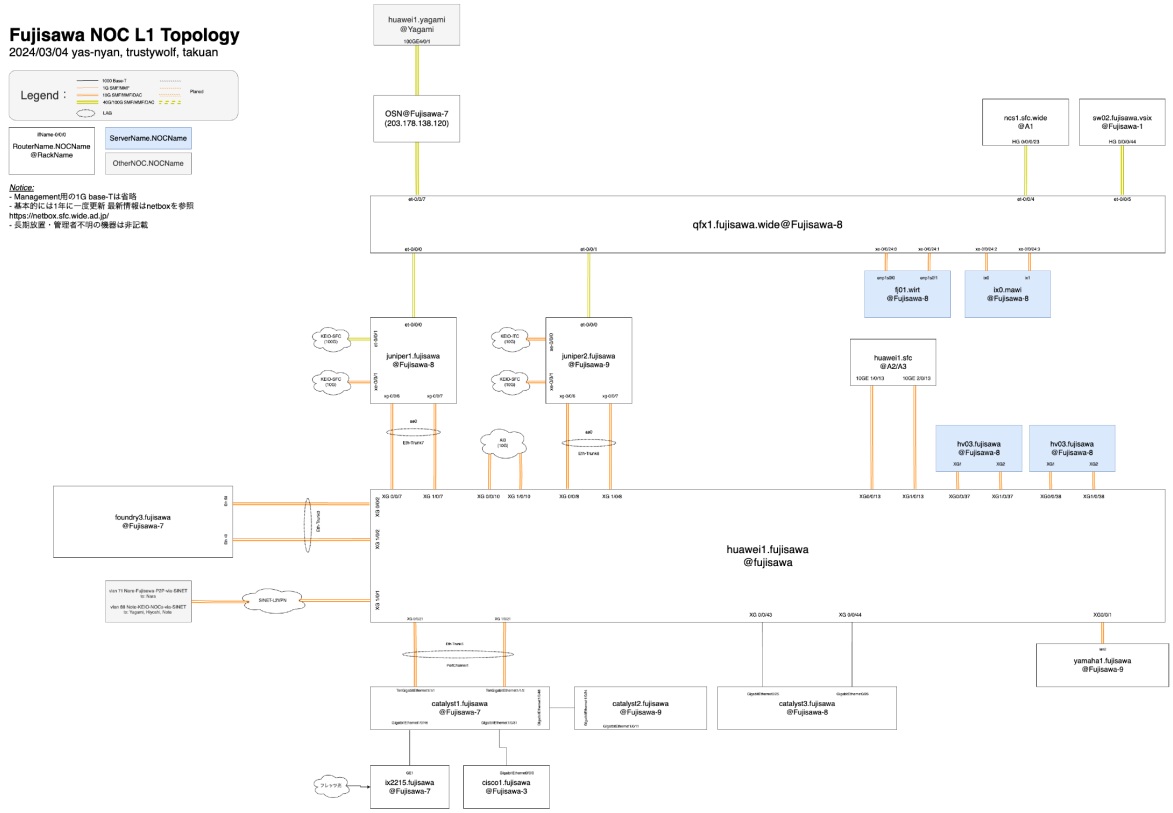

図10 藤沢NOC Layer-1トポロジ図

本年度は下記のように，新規にWIDE内の他プロジェクトとの接続を開始したほか，トポロジーを一新し，よりフレキシブルで強力な実験・開発環境の整備に努めた．時系列でイベントを書く．

- (2024/07)NOC内の配線整理

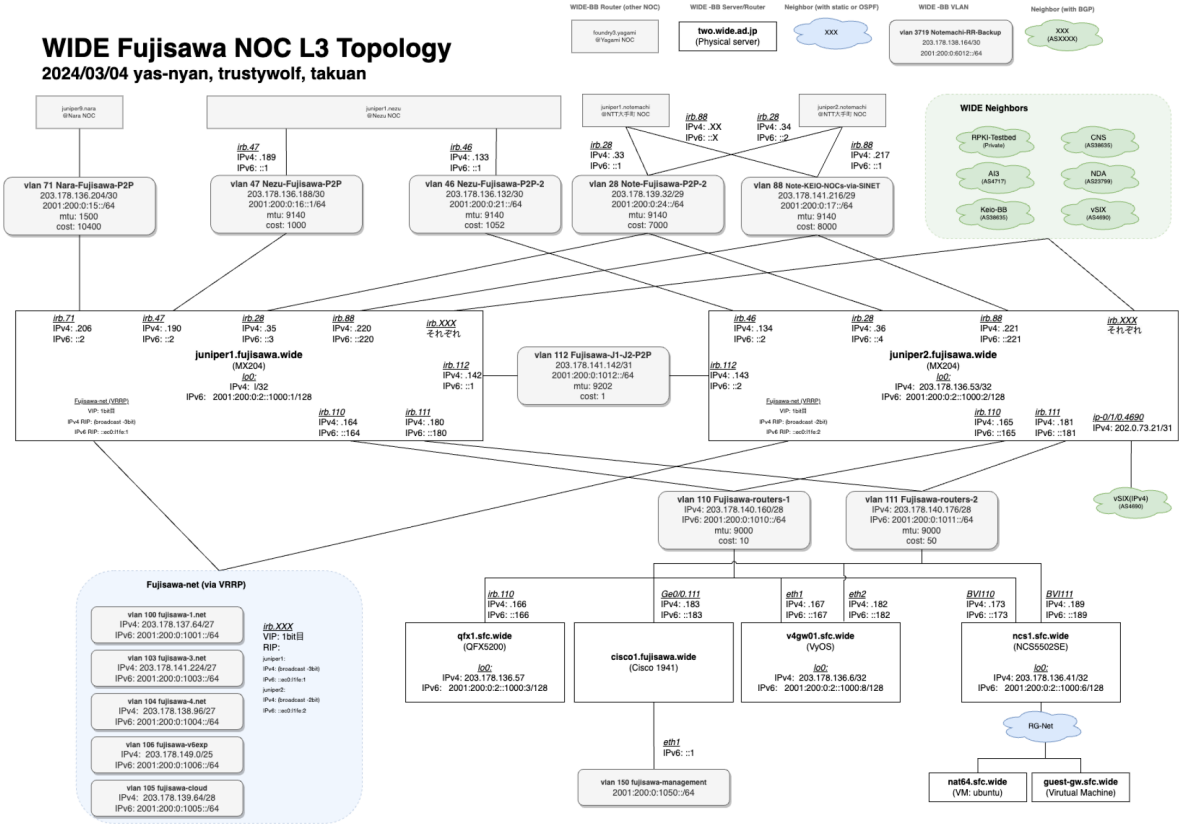

図11 藤沢NOC Layer-3トポロジ図

2.8 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。

2.9 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10Gigabit Ethernet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．ルーティングポイントのcisco2.dojimaからjuniper1.dojima，crs1-1.dojimaへの移行を進めている．

- (2024/02)大掃除(機材退役、ラック内整理、不要ケーブル撤去、ラベリング、廃棄機材集約)
- (2024/02)cisco2.dojima停止、alaxala1.dojima停止
- (2024/12)不要物品の廃棄

2.10 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．

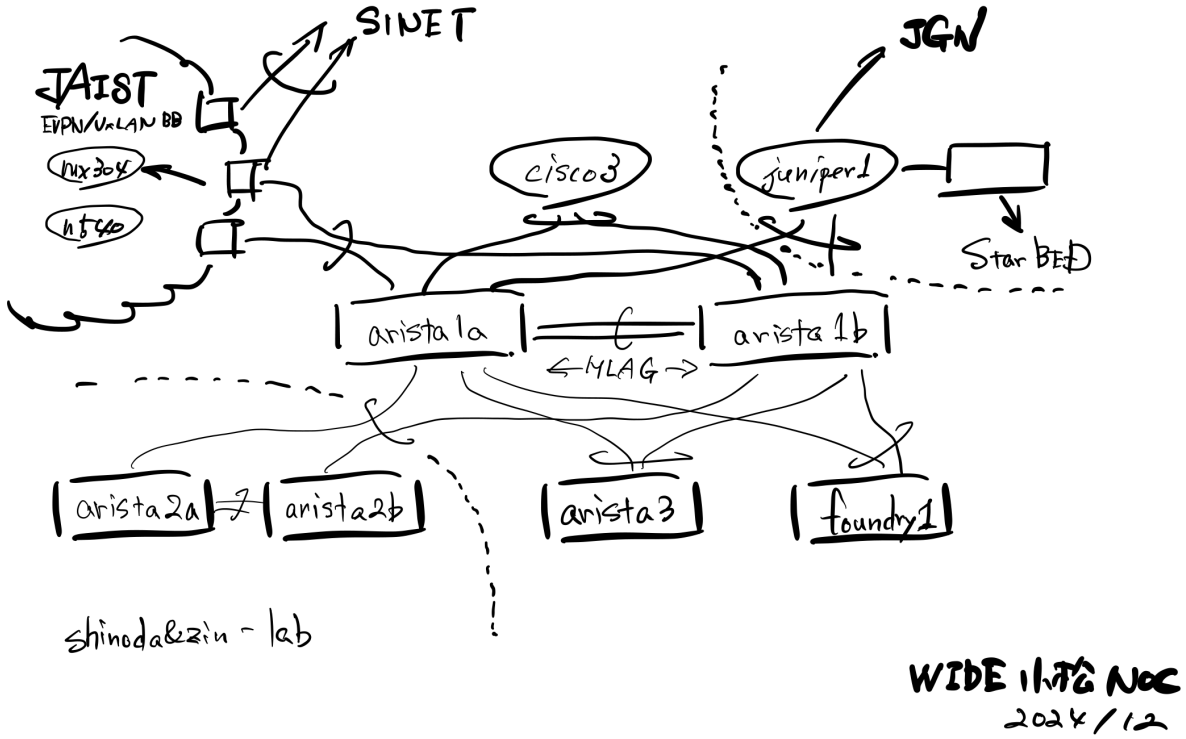

図12 小松NOC

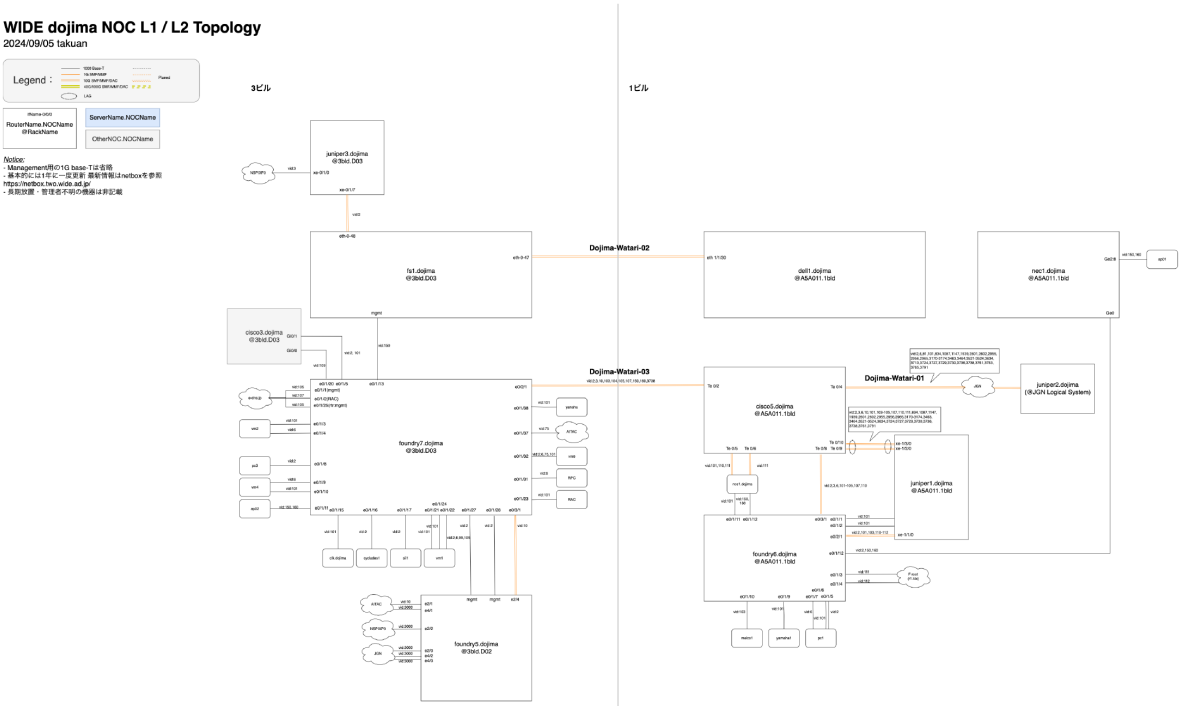

図13 堂島NOCトポロジ

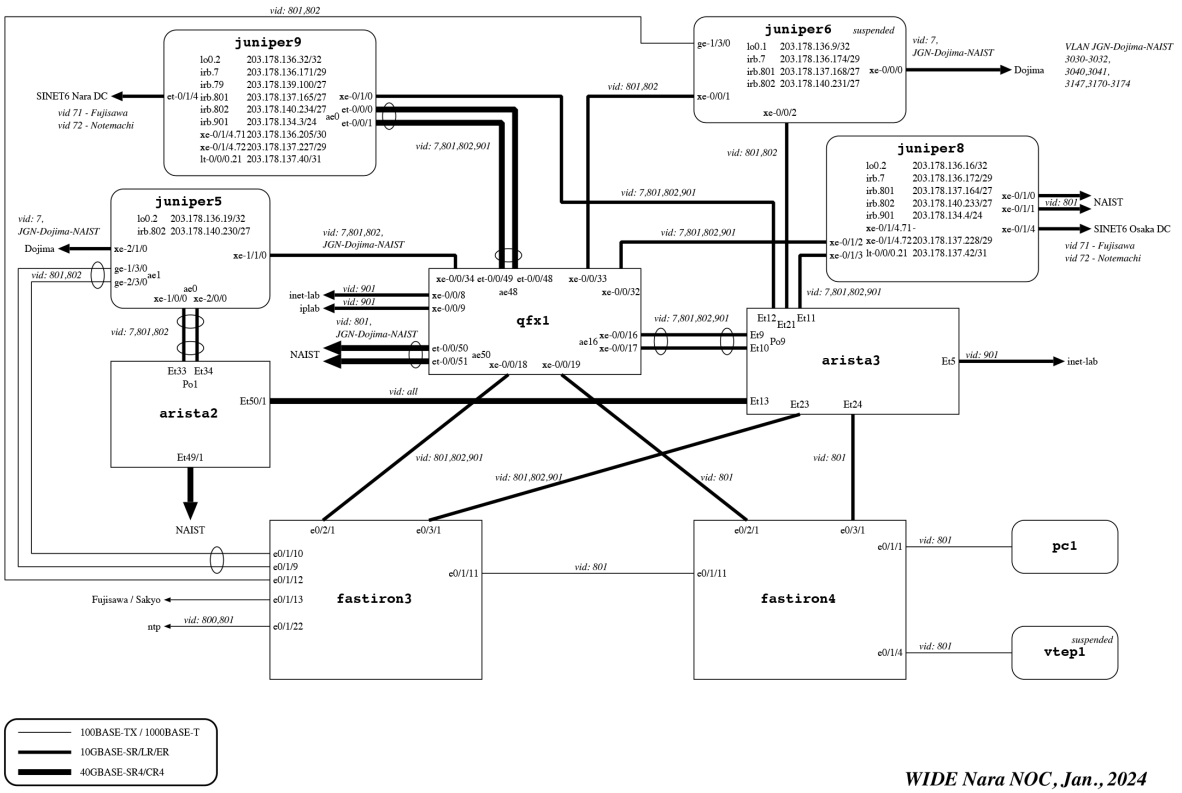

図14 奈良NOCトポロジ

2.11　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．

第３章　WIRTの活動

WIRT（WIDE Incident Response Team）はTWOワーキンググループに所属する一部メンバにより構成された組織内CSIRTであり，WIDE-BBにおける情報セキュリティインシデントの発生から収束までの対応を管理すると同時に，関連する技術の研究開発を実施する．組織外のCSIRT間の連携の点では，日本シーサート協議会（NCA）や学術系シーサート交流ネットワーク等を中心に，インシデント事例分析や脆弱性情報の共有を進めている．NCAにおいては2020年4月よりWIRTは幹事会員となり，学術系ネットワークの運用者の立場から積極的に情報発信を実施している．

3.1　WIRTによるトラフィック情報収集

WIRTではWIDE-BB内のフロー情報の収集基盤の構築を進めており，NTT大手町拠点，KDDI大手町拠点を中心に計測用サーバを設置して，トランジットリンク，DIX-IE経由の国内商用ISPとのピアリンク，国内/国際RENとのピアリンクなど，WIDE-BBにおける主要な対外接続のフロー情報を計測している．これらのサーバ機器ではフロー情報を1:1サンプリングでNetFlow v9フォーマットにて出力し，WIRT内で運用されるSIEM基盤である（WIDE TWS）に集約される．WIDE TWSはフロー情報の他に，経路情報，ダークネット観測情報，境界管理情報などのOSINT情報，商用の脅威インテリジェンス情報など脅威検知に有用な情報が順次取り込まれる．WIDE TWSにはルールベースと振る舞いベースの異常検知エンジン[100, 101]が実装されており，上記で取り込まれた情報を用いることでWIDE-BBにおける準リアルタイムな（現在時刻から約15分の遅延を含む）異常検知を実施している．

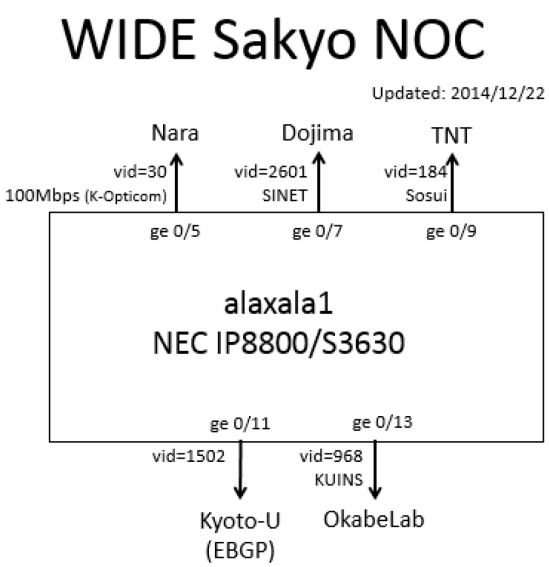

図15 左京NOC

図16にはWIDE TWSの構成の概要を示す．NTT大手町拠点，KDDI大手町拠点，藤沢拠点に設置されたフロー情報収集サーバからはフロー情報が5分毎の間隔で矢上拠点に設置されたWIDE TWSにまで配送される．WIDE TWSはRDBMS（PostgreSQL）に基づいて構成される．

3.2　本年の主要な活動実績

本年に実施した主な対応を以下に示す．WIDE TWSにおける異常検知に基づいて多国籍宛のスキャニング相当の通信や既知のマルウエアのシンクホール宛の通信を検知して対応した．またCVE-2024-6387（regreSSHion）の脆弱性への対応を実施した．WIDE-BB内に本件脆弱性に該当する可能性がある機器が複数あり，SSH経由で認証を経ない遠隔の第三者がWIDE-BB内の機器に接続する可能性を考慮して，網羅的に当該脆弱性に対する対応を実施した．

- 2024年2月:WIDE-BB内から多国籍宛の大量のスキャニング相当の通信検知・対応
- 2024年6月:WIDE-BBスタブ組織からシンクホール宛の通信の検知・対応
- 2024年7月:CVE-2024-6387（regreSSHion）への対応

この他にも，境界管理情報を用いたWIDE-BB内の脆弱性管理やダークネット観測情報を用いた異常検知を随時実施した．

第４章　おわりに

本年は，例年通りWIDE-BBの安定した運用を実施するとともに，KDDI大手町拠点と堂島拠点のリファクタリングを推進した．またWIRTによるSIEM基盤であるWIDE TWSの整備が進み，WIDE-BB内のセキュリティ環境の改善が進んだ．

今後はWIDE-BBの藤沢拠点から大手町拠点にかけてAPN（All-Photonics Network）の実験が計画されており，そのための実験設備の設置が予定されている．またWIRTでは，フロー情報の収集基盤の構築を堂島拠点においても進めるとともに，インターネットバックボーンにおける異常検知技術やサービス単位でのトラフィックのアトリビューション技術の研究開発を実施する予定である．

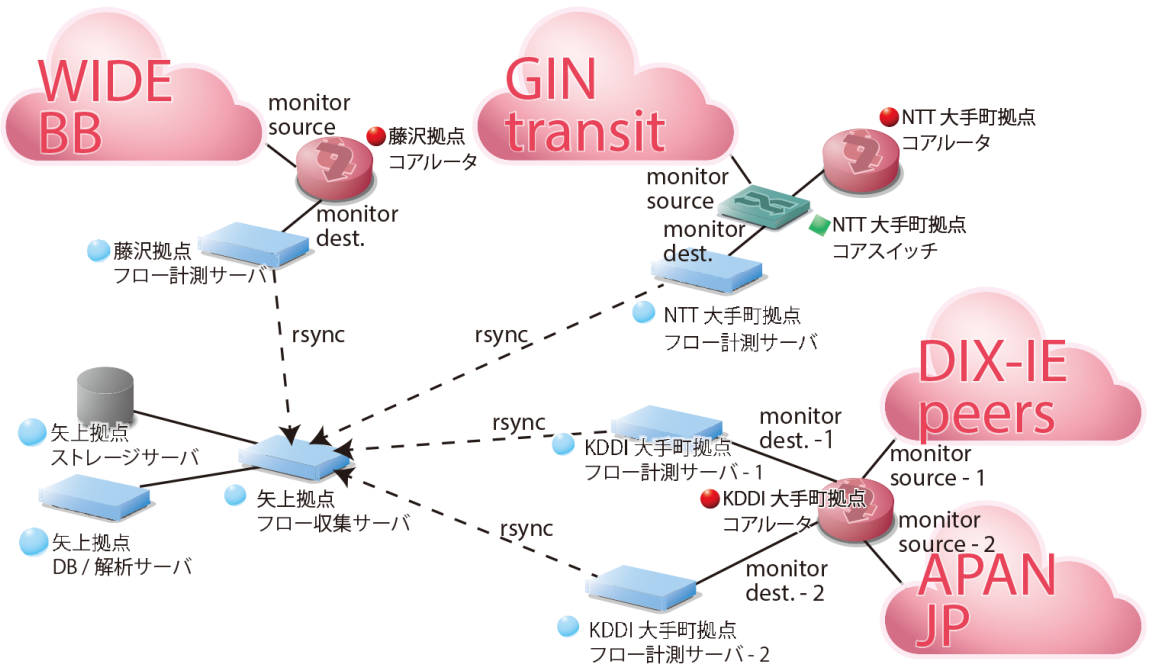

図16　WIDE TWSの構成概要．