≪ 詳細版を電子データとして提供します ≫

第25部

WIDEネットワークの現状（概要版）

近藤 賢郎、豊田 安信、加藤 良輔、西野 大、遠峰 隆史、TWOワーキンググループ

第１章　はじめに

WIDEバックボーンネットワーク（WIDE-BB）は国内の各地に拠点（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-BB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-BB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．図1は2023年12月31日現在のWIDE-BBの概略図である．

第２章　WIDE-BBの運用

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．2021年12月から漸次的に計画実施してきたNTT大手町拠点の本館ビルから別館ビルへの移転作業では，2022年末までに大部分の機材の移設を終えていたが，本館ビルに一部の回線とその収容機材が残置されていた．このため，本年はそれらの回線の別館への収容替えを実施した後に不要な機材を破棄して，本館からの完全撤退を実施した．本館から別館への一連の移設に当たっては，ただ単に機材を移設するのではなくWIDE-BBの高速化と将来を見据えた対応を行ったため，結果的にNTT大手町拠点のリファクタリングと

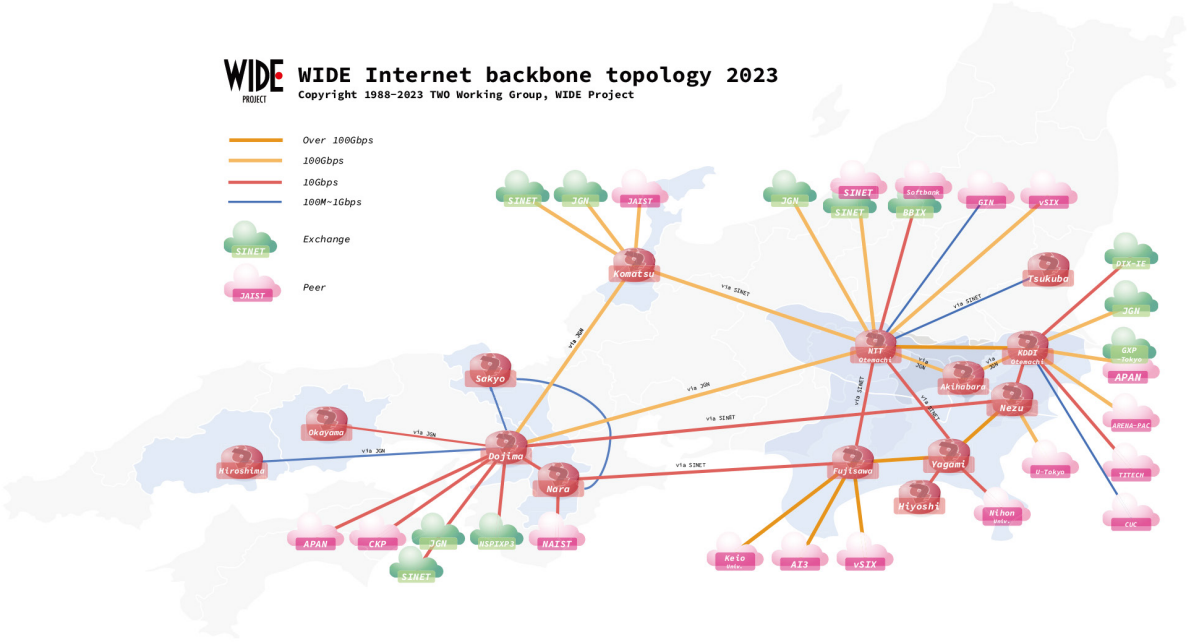

図1　WIDE-BB トポロジ

なった．その成果を元に本年はKDDI大手町拠点のリファクタリングも併せて実施した．NTT大手町拠点/KDDI大手町拠点のリファクタリングについては，第3節にて詳説する．

対外接続の点では，RPKI技術に関する研究開発を実施するために，2023年7月にNTT大手町拠点においてBBIXとの10Gbps回線による接続が追加された．この接続では，BBIX東京拠点に接続する各社と対等ピアの関係で経路交換するとともに，BBIXよりトランジット経路の提供を受けている．従来よりWIDE-BBにおけるトランジット回線の冗長化が課題となっていたが，今回の接続追加によって結果的にその課題解消に資することとなった．またBBIXへの接続に際してAS-SETなどBGPによる経路広告ポリシの整理を実施した．

NTT大手町拠点の移設の結果，WIDE-BBと国内/国際REN（Research and Education Network）との接続拠点が従来から変更されたものもある．加えて，上記の通りBBIXとの接続の追加もあったことから，現在WIDE-BBがNTT大手町拠点とKDDI大手町拠点を介して接続する主要ネットワーク/IXを今一度整理すると以下となる．

- NTT大手町拠点: GIN，BBIX，SINET
- KDDI大手町拠点: DIX-IE，JGN，APAN-JP，GXP-Tokyo，ARENA-PAC

第３章　NTT大手町拠点/KDDI大手町拠点のリファクタリング

3.1　リファクタリングに至った経緯と方針

第2節に記載した通り，NTT大手町拠点の本館から別館への移設は1年以上の期間をかけて実施された．移設前の本館におけるNTT大手町拠点では，管理者や詳細不明なIAサーバやルータ機器が多数残置されていたり，縦横無尽で無理のあるラック間・対外接続回線の引き回しが行われていた．このため，移設にあたって破棄可能な資産の区別や現用の接続回線の確認のために数多くの現地調査や打合せを要する結果となった．加えて，NTT大手町拠点に限らずWIDE-BBを構成する他拠点を含め同様の状況がみられることもあり，本件を契機として，WIDE-BBの運用コストも押し上げている現況を再認識するに至った．

以上の事情から，NTT大手町拠点の別館への移設にあたっては，機器の設置や回線の引き回しにあたってラック毎の役割を明確化するソフト面のポリシ制定に加え，それらのポリシの履行を容易とするためパッチシステムなどのハード面の拡充が行われた．別館のNTT大手町拠点には5つのラックが配備されているが，それらの主な役割はそれぞれランディング（接続収容）用，DIX-IE/PIX-IE用，WIDE-BB用，国際接続用，研究プロジェクト用に分割した．さらに，ラック間の配線や対外回線の収容に用いるためのパッチシステムを各ラックにも配備した．このことにより，別館への移設を契機にNTT大手町拠点リファクタリングされ，対外回線や各ラックの利用状況が明確化して定常的な運用コストの低減に資するだけでなく，新規にTWOワーキンググループに加入した者がWIDE-BBの運用や実験に参加する際の障壁の低下も見込まれる状況となった．

NTT大手町拠点のリファクタリングに続いて，本年にはKDDI拠点のリファクタリングも随時実施された．NTT大手町拠点と同様に，リファクタリングにあたってはラック毎の役割を明確化するソフト面のポリシ制定とハード面の拡充が実施された．ハード面の拡充にあたっては，上記で述べたラック間のパッチシステム導入といったユーティリティ向上だけでなく，NTT大手町拠点=KDDI大手町拠点間接続の高速化を目的にDWDM導入までが実施された．この結果両拠点間の帯域の総容量は現在1.1Tbpsに到達するまでに至っている．

3.2　具体的なリファクタリング内容

2021年末のNTT大手町拠点の移設開始以降本年までに両拠点で実施されたリファクタリング項目としては以下が挙げられる．

- インフラの高速化への対応（SMF化，LC化）
- MPOパッチシステムによる構造化配線の導入
- ロジスティックスの効率化（UTP，Fibre，電源コードの先行準備）

- ラックの集約と役割の明確化
- MX480導入による100GbE機器の増強
- KDDI大手町拠点=NTT大手町拠点間接続におけるDWDM導入
- ネットワーク管理用サーバ・インフラの強化

第４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．

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[182]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．

本年にWIRTが検知の上で対応を実施した主な事案は以下の通りである．

- 2023年4月: WIDE-BB内からのNTPリフレクション相当の通信検知・対応
- 2023年5月: WIDE-BBスタブ組織から多国籍宛の大規模スキャニング活動検知・対応
- 2023年10月: WIDE-BB内から多国籍宛の大量のSMTP相当の通信検知・対応
- 2023年11月: WIDE-BBスタブ組織からのSNMPリフレクション相当の通信検知・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．また，2023年5月に開催されたNCAのインシデント事例分析ワーキンググループではWIRTが実施するWIDE-BBにおけるセキュリティ運用について発表した．

WIDE TWSで収集するフロー情報に関しては，2023年5月にSINETとのピアリンク，2023年8月にBBIXとのピアリンクに対する計測をそれぞれ追加した．従来よりWIDE TWSにおける振る舞いベースの異常検知エンジンとしてGAMPALの研究開発を実施していたが，異常検知精度の向上や学習時間の削減を主な目的としてGAMPALv2[183]の研究開発を継続実施している．それと同時に，暗号化トラフィックを含んだトラフィックを対象としたトラフィック分類手法であるOLIViS[184]の研究開発も行っており，WIDE TWSへの機能追加を今後実施する．

第５章　ccTLD及びccSLD権威サーバの運用

WIDE Projectでは2021年度よりlb.，com.lb.，edu.lb.，gov.lb.，net.lb.，org.lb.のDNSゾーンの権威サーバを運用している．各ゾーンはレバノン共和国に割り当てられたccTLDとそのサブドメイン（ccSLD）のゾーンであり，ドメインレジストリはLBDR[185]によって運用されている．権威サーバ群はベイルート・アメリカン大学をはじめとする学術組織及びコミュニティによって運用されており，WIDE Projectでは2021年8月より権威サーバとしてns-jp.lbdr.org.lb.の運用を開始した．設計から運用にあたり，TWOワーキンググループ内でM-ROOTの運用者や20代の若手研究者を含むサブグループを組織した．これ

までの経験やroot DNSゾーンの運用知見に基づく効率的な運用を行うだけでなく，情報交換や本運用における実務経験を通して高度なDNSオペレーションを行うことのできる若手人材の育成にも貢献している．

例年通り引き続き本年も安定的に運用を行ってた．2023年7月に権威サーバをホストするハイパーバイザホストの一部でメモリのハードウェア障害が発生した．その他のメモリは正常に稼働しているため該当ホストにおいて致命的なエラーとはなっていないものの，故障したメモリの早期交換が求められる．また2023年12月には権威サーバをホストするハイパーバイザホストのバージョン更新を実施した．権威サーバは2台のハイパーバイザホストでホストされているが，本件バージョン更新作業は1台ずつ順に実施した．このため，権威サーバのサービス停止は最小限に抑えられた．来年度はさらなる運用の効率化やTLD権威サーバの特性を生かした研究にも努めたい．

第６章　まとめと展望

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，NTT大手町拠点とKDDI大手町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．さらにccTLD及びccSLD権威サーバの運用が開始され，地政学的及びグローバルな名前空間であるDNSの可用性・多様性の観点から価値ある活動を推進した．

今後はWIDE-BBの西日本の期間拠点である堂島拠点のリファクタリングを進める予定である．また，BBIXとの接続が追加されたことで複数のトランジットからインターネットフルルートを受信する環境となったことから，主要拠点全体で一貫した経路制御が可能となるようWIDE-BBの再構成を推進する．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．さらにccTLD及びccSLD権威サーバの運用を維持するとともに，それらの基盤に基づいた研究活動も順次計画していく．