≪「**報告書詳細版**」は巻末の付録USBメモリに収録しています ≫
≪ 追加資料を巻末の付録USBメモリに収録しています ≫

第22部

WIDEネットワークの現状（概要版）

近藤 賢郎、大谷 亘、豊田 安信、遠峰 隆史、LB DNS運用サブグループ、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は国内はもとより海外にも拠点（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。図1は2021年12月31日現在のWIDEバックボーンの概略図である。

第２章　WIDEバックボーンの運用

2.1　本年度の活動方針

例年と同様に本年度も主に100Gbps、10Gbps回線に基づいてWIDEバックボーンを運用した。2019年度よりNTTコミュニケーションズ社が開発するソフトウェアルータKamuee[184]を藤沢拠点に導入し運用試験を行っているが、その後の安定的な稼働を踏まえて、本年度はKDDI大手町拠点にもKamueeを導入した。KDDI大手町拠点はバックボーンの東日本におけるコア拠点の一つであるWIDEるが、インターネットフルルートの経路数の増大の影響で2019年9月頃よりインターネットフルルートによる運用を中断していた。本報告書の執筆時点ではKDDI大手町拠点のコアルータを今回導入したKamueeに移設出

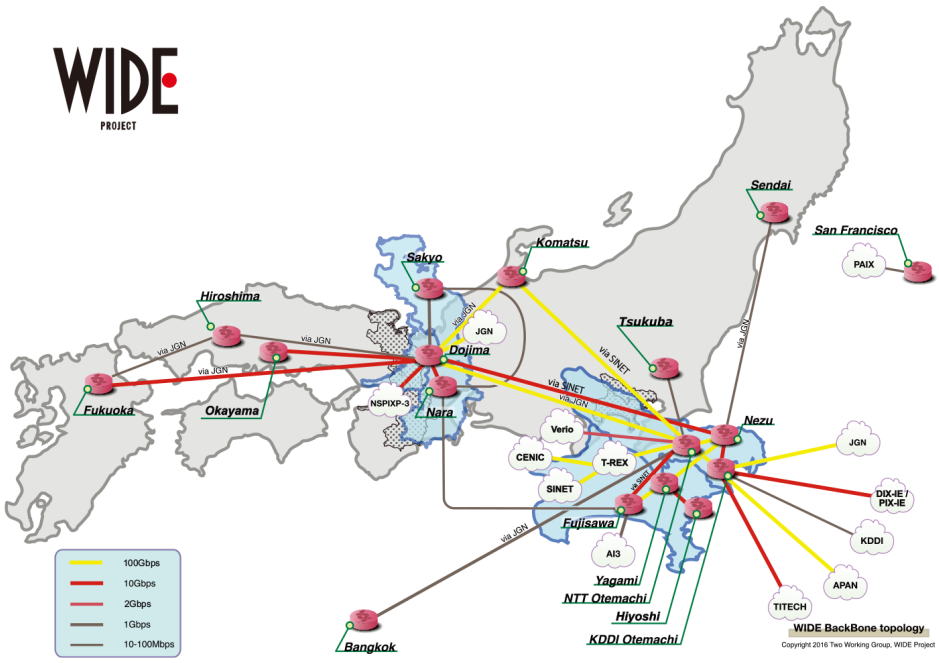

図1　WIDEバックボーントポロジ

来ていないが、KDDI大手町拠点も近日中にインターネットフルルートによる運用に復帰することが見込まれる。このほか2.2節で述べるように根津拠点のコアルータ機器の更新もあったことから、WIDEバックボーンを構成する全ての主要拠点においてコアルータ機器はインターネットフルルートに基づいた同一の経路計算結果を保持できる見込みがたち、WIDEバックボーン全体の可用性の向上が図られる。

2021年2月にはWIDEバックボーンとARENA-PAC間がNTT大手町拠点にて接続された。これに伴いData Movable Challenge（DMC）における大容量データ伝送に利用するAARnet = NICT間の伝送パスを、ARENA-PAC、JGNと協調しながら提供した。ARENA-PACによりアジア太平洋地域を中心に国際REN（Research and Education Network）コミュニティとWIDEとの関係がなお一層深まりつつある。従来TWO WGから国際RENコミュニティの会合に参加するメンバはごく一部に限られていたが、ネットワーク運用技術やセキュリティ運用技術などの議論を中心に、今後より積極的な関与が望まれるものと考える。

また次年度後半に予定されるNTT大手町拠点の本館ビルから別館ビルへの移設に先立ち、NTT大手町拠点に係る機器や回線の棚卸しが順次行われた。2021年12月には本件担当のプロジェクトチームがNTTコミュニケーションズ社と合同で立ち上がり、移設に係る詳細な議論が開始された。

2.2　WIDEバックボーンの主要な更新事項

本節では2021年に実施されたWIDEバックボーン内拠点の主要な更新事項について時系列に沿って纏める。

07/30：NTT大手町拠点では従来よりJGN所有のCRSから物理ルータ1台を借用し、crs1-1.notemachiとして主にWIDEバックボーンの東日本地区におけるBGP RRとしての機能を担っていたが、JGN内の機器更新によりcrs1-1.notemachiが退役して、新規にJGNから借用したJuniper logical system上の仮想ルータであるjuniper3.notemachiが同様の役割を担い運用が開始された。

11/26：小松拠点では従来より北陸地区におけるBGP RRや小松拠点 = 堂島拠点間接続における小松拠点側のルーティングポイントなどの機能を担ってjuniper1.komatsu（Juniper MX240）が稼働していたが、機器リースアップに伴い、juniper1.komatsuがJuniper MX240からJuniper MX204に更新された。

12/04：根津拠点では拠点コアルータとしての機能を担って従来よりBrocade MLX4e（brocade1.nezu）が稼働していたが、機器老朽化に伴う機器更新の一環としてJuniper MX204が導入され、juniper1.nezuとして稼働を始めた。

12/14-16：藤沢拠点では従来より慶應義塾との接続や拠点コアルータとしての機能を担ってnexus1.fujisawa（Cisco Nexus7706）が稼働していたが、機器リースアップ対応に伴い新規にjuniper1.fujisawa、juniper2.fujisawa（何れもJuniper MX204）が導入された。併せて藤沢拠点のコアルータとしての機能は従来より導入済みであったkamuee1.fujisawa、kamuee2.fujisawaに移設された。

12/22：堂島拠点では従来よりJGN所有のCRSから物理ルータ1台を借用し、crs1-1.dojimaとして主にWIDEバックボーンの西日本地区におけるBGP RRや小松拠点 = 堂島拠点間接続における堂島拠点側のルーティングポイントなどの機能を担っていたが、JGN内の機器更新によりcrs1-1.dojimaが退役して、今回新規にJGNから借用したJuniper logical system上の仮想ルータであるjuniper2.dojimaが同様の役割を担い運用が開始された。

第３章　WIRTの活動

WIRTはTWO WG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バックボーン及びその接続組織に関わるインシデントの発生を把握しその収束までのレスポンスを管理する。例年同様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・連携を組織間に跨がって進めた。2020年4月よりWIRTはの幹事会員となり、学術系ネットワークの運用者のNCA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

2019年度よりWIRTではWIDEバックボーン内のフロー情報の収集基盤の構築を進めており、昨年度までにNTT大手町拠点、KDDI大手町拠点、藤沢拠点にフロー情報の計測用サーバを設置して、それぞれGIN（AS2904）への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、藤沢拠点のアップリンクのおけるフロー計測を開始していた。本年度はKDDI大手町拠点にさらにもう1台フロー情報の計測用サーバを追加して、APAN-JP（AS7660）とのピアリンクにおけるフロー計測を開始した。これらのサーバ機器ではntop社のnProbe[185]が稼働しており、各拠点で観測されるトラフィックのフロー情報を1:1サンプリングでNetFlow v9フォーマットにて計測する。

図2にはWIRTのSIEM基盤（*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。WIDE TWSには観測されたフロー情報の他に、経路情報、ダークネット観測情報、OSINT情報、商用の脅威インテリジェンス情報などアトリビューションに有用な情報が順次取り込まれる。これらの情報に対してWIDE TWS上で定期的に解析スクリプトを実行することによって、WIDEバックボーンにおける異常事象の準リアルタイムな（現在時刻から約15分の遅延を含む）検知に利用される。

3.2　本年度の主要な活動実績

本年度にWIDEバックボーン内で観測された確定セキュリティ事案へのWIRTの対応状況を以下に纏める。これらの事案はWIDEバックボーン自身に係るものとWIDEネットワークへの接続組織に係るものの双方を含む。

- OpenVPN reflection検知（3件）
- SNMP reflection検知（2件）
- SMTPセッション大量接続検知
- DNS reflection検知（2件）
- NTP reflection検知（2件）
- SSH brute force / massive scan検知（1件）
- SSH brute forceのC2基盤へのシグナリング検知（1件）

加えて、WIDEネットワークへの接続組織からの問い合わせに基づいて、接続組織で確認された事象がばら撒き型/標的型の何れに該当するかのアトリビューションに

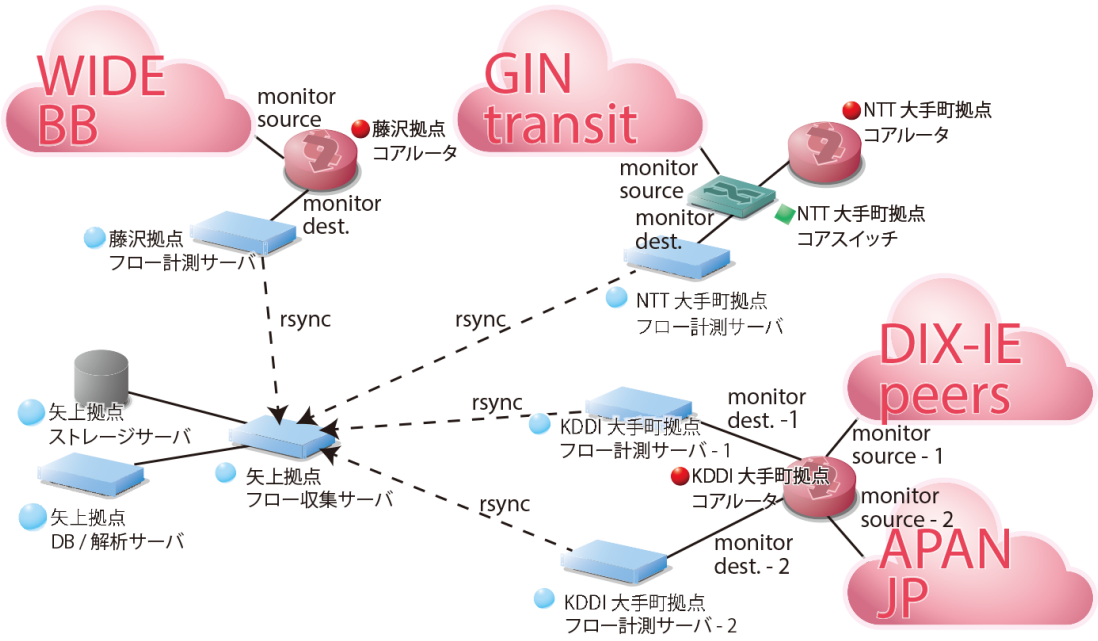

図2　WIDE TWSの構成概要

協力するといった活動も実施した。

またWIRTではインターネットバックボーン環境における効率的な異常検知およびアトリビューション技術の研究開発に取り組む。昨年度に引き続いて、BGP経路情報に基づいたフロー情報の集約に基づいたトラフィックの異常検知機構であるGAMPAL[186]の研究開発を実施し、今年度は汎化性能の向上と異常検知機構のリアルタイム化[187]に注力した。またフロー情報で観測されたトラフィックの振る舞いに対して主にOSINT活動で収集される情報を付与してアトリビューションする仕組みの研究開発への取り組みを開始した。

第４章　ccTLD及びccSLD権威サーバの運用に関する報告

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。本節では、これらのDNS権威サーバの運用にかかる経緯、設計、運用について記述する。

4.1　背景

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によって運用されている[188]。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。

ccTLD権威サーバを割り当て国以外で運用することにより、地政学的観点から可用性の高いccTLD運用を実現した。また、アジア太平洋地域のフルサービスリゾルバ・エンドユーザに対し、より低遅延な名前解決サービスを提供している。

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。

4.2　設計

4.2.1　サーバ/ネットワーク

サーバ設計においては、可用性を重視し、一つのサービスアドレスに対して複数台のサーバを用意することとした。また、物理障害に対する耐障害性を確保するため、複数台の物理サーバ上に複数台の仮想マシン（ノード）を構築することとした。

ネットワーク設計においては、冗長性のあるサーバ設計を前提とし、可用性を確保する設計を行った。具体的には、NSレコードに紐付くA/AAAAレコードとして公開されるサービスアドレス1つを複数のノードに対して割り当て、AS内の経路広告による動的経路制御を行うこととした。

また、各ノード内で権威サーバ実装とソフトウェアルータが稼働し、ノード自らが経路広告を行うことにより、図3に示すL7及びL3の双方の観点で単一障害点を排除した（cf.[189]）。これにより、状況によって柔軟にトラフィックを分配したり、特定ノードへのトラフィックを止めることで容易にメンテナンスしたりと、運用コストの低減を見込むことができる。

4.2.2　DNS委任関係

DNS的な委任関係の設計においては、4.2.1節で述べたネットワーク設計を考慮し、図4に示すようにns-jp.lbdr.org.lb.という単一のホスト名に対して委任することとし

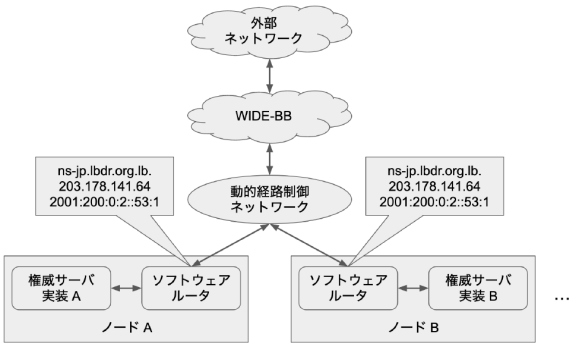

図3　L3ロードバランサレスアーキテクチャ

た。このホスト名には単一のA/AAAAレコードを紐付けた。これにより、運用事故発生時にlame delegationが発生する蓋然性を低減した。

4.2.3　権威サーバ実装の選択

権威サーバ実装はメンテナンス性や開発・運用コストを考慮し、オープンソースな既存の実装を用いることとした。また、実装ダイバーシティを確保するため、ノードにより異なる複数の実装を採用することとした。実装の選定は、大規模な権威サーバを運用する事業者での採用事例やそれぞれのコミュニティが公開しているパフォーマンス測定結果を基に実施し、比較的信頼できccTLD及びccSLDの運用に耐えうるパフォーマンスを持つものを採用した。

4.2.4　サービス安定性

ccTLD及びccSLDのゾーンホストという条件につき、セキュリティ的に安定したサービス稼働が求められる。そのため、基本的にノードへの手動での設定変更等は行わない方針とし、人為的ミスによる運用事故を減らすことを目的に運用自動化ツールであるAnsible[190]を導入することとした。これにより、平時のオペレーションで必要な設定変更や、障害児やメンテナンス時のトラフィック制御に必要な設定変更を安全に行うことを見込む。

また、物理セキュリティについては、各物理マシンの設置場所を物理アクセス制限システムの整った国内データセンタから選定した。また、具体的な設置場所・データセンタについては非公開とした。

ns-jp.lbdr.org.lb.はプライマリ権威サーバからゾーン転送を受けてゾーンホストを行うセカンダリ権威サーバとして機能する。そのため、ゾーン転送においてはTSIG[191]による認証を用いることとし、サービスアドレスとは異なるIPアドレスでの転送に限定し、転送元サーバ運用者にそのIPアドレスのみへの転送に限定するように依頼した。

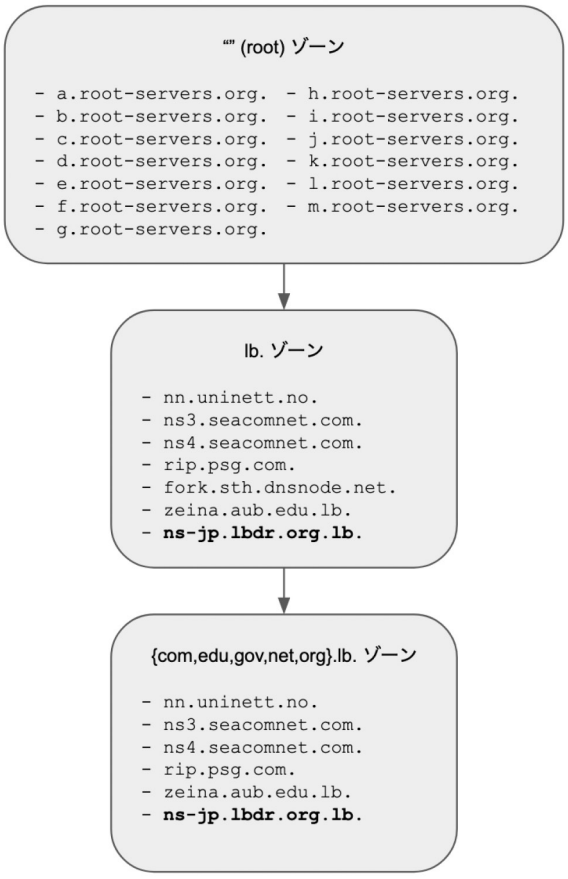

図4　委任関係の構図

4.3　運用

前項までの設計を元にサーバ・ネットワークのデプロイをすすめ、2021年8月7日よりlb.ゾーンを除くccSLDのゾーンについて、同月10日よりlb.ゾーンについて、親ゾーンからの委任及び権威応答を開始した。

4.3.1　監視

迅速な障害検知のため、監視システムによる継続的な監視を行っている。また、障害発生時における障害点・障害原因の迅速な把握のため、AS内とAS外に複数の監視点を設置している。監視点の設置場所により監視項目を分担しており、AS外では外形監視としてサービスの死活監視や応答時間の監視などを行っており、AS内ではゾーン転送異常検知のためのSOAレコードSERIAL値の監視やノード自体のOSレベルでの死活監視などを行っている。

4.3.2　障害・セキュリティ対応

本稿執筆時点において特筆すべき障害は発生していないが、前述の監視体制による障害検知や後述する組織外からの情報提供に基づき、常に障害に対応できる体制を敷いている。また、WIDE-BB上の障害に関してはTWOワー

キンググループ内で連携して対応を行っており、重大な障害発生時には他の権威サーバ運用者を介してIANAへの報告など必要な措置を行う。

セキュリティ運用に関しては、WIDE Projectの組織内CSIRTであるWIRTと連携し、ネットワーク上に設置したトラフィック監視システムによる異常な通信の監視を行っている。

4.3.3　サービス安定性

複数組織での権威サーバ群運用にあたり、他の権威サーバ運用者とメーリングリストやオンラインミーティングを介した情報交換を行っている。

4.4　トラフィックの分析

WIRTが計測するフロー情報をもとに、2021年12月6日から12日までの1週間における5 tuples（送信元IPアドレス、送信元ポート番号、送信先IPアドレス、送信先ポート番号、プロトコル）に基づくトラフィックフローの分析を行った。

4.4.1　クエリ概況

図5、図6、図7はそれぞれ権威サーバのサービスアドレスに対するDNSクエリと応答について、セッション数、クエリ元IPアドレス数、送受信バイト数を日ごとに集計したものである。

いずれも曜日による大きな変化はない。クエリ数（図5）をみると、1日あたりの平均でIPv4では約576万クエリ、IPv6では約182万クエリ、あわせて約758万クエリを受けている。クエリ元IPアドレス数（図6）をみると、1日あたりの平均でIPv4では約14.5万ホストから、IPv6では約4.28万ホストから、あわせて約18.9万ホストからクエリを受けている。また、同様の仮定において、IPv4でクエリしているホストはIPv6でクエリしているホストよりも約3.39倍多く、IPv6の普及が十分進んでいないことがわかる。送受信バイト数（図7）をみると、IPv4とIPv6をあわせて1日あたりの平均で約578MBを受信、約1.54GBを送信している。

4.4.2　国・地域別トラフィック量

WIRTのSIEM基盤に含まれるGeoIPデータベースを使い、送信元IPアドレスを国・地域ごとに分類した。図8、図9にそれぞれIPv4とIPv6の国・地域別送信元IPアドレス数の割合を示す。

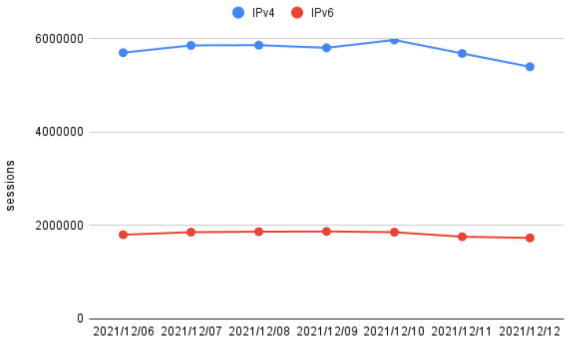

図5　クエリ数の変化

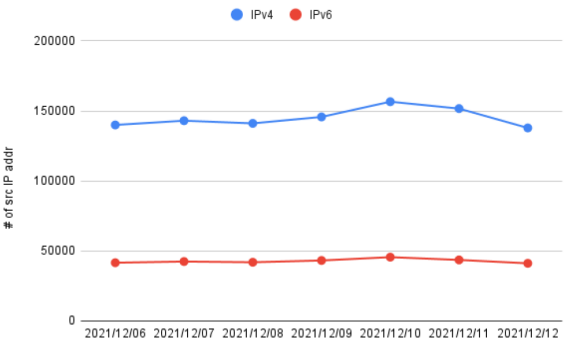

図6　クエリ元IPアドレス数の変化

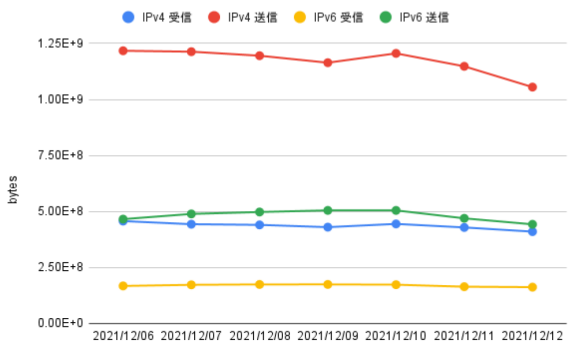

図7　送受信バイト数の変化

IPv4・IPv6共にアメリカからのクエリが多いことがわかる。アジア太平洋地域では、インド、日本、ロシア、台湾、中国からのクエリが多いことがわかる。

第５章　まとめと展望

本年度はWIDEバックボーンを構成する主要な拠点のコアルータ機器の更新が複数実施され、KDDI大手町拠点を中心にKamueeなどの先進的なソフトウェアルータの導入が進んだ。またWIRTによるSIEM基盤であるWIDE TWSの整備が進み、WIDEバックボーン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。

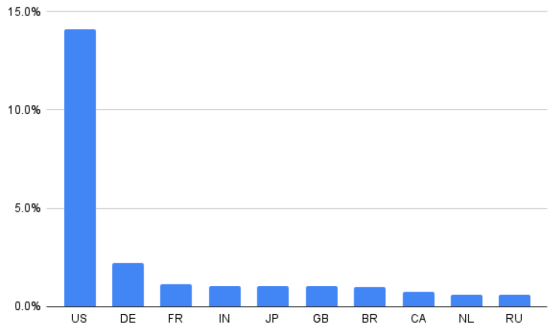

図8　国・地域別送信元IPアドレス数の割合（IPv4）
（上位10 ヵ国）

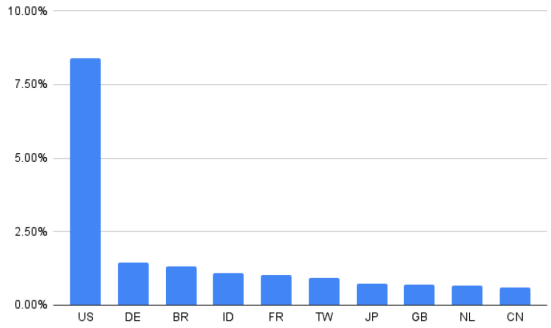

図9　国・地域別送信元IPアドレス数の割合（IPv6）
（上位10 ヵ国）

今後はWIDEバックボーンの主要拠点全体でインターネットフルルートの基づく一貫した経路制御が可能となるようWIDEバックボーン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西日本地区においても検討するとともに、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、それらの基盤にを基づいた研究活動も順次計画していく。