vSIX プロジェクト: IPv6 前提インターネットの運用実験基盤

豊田安信 *　　深川祐太 †

2021 年 12 月

1　はじめに

1.1　IPv6 に関わる現在の社会情勢

1998 年に IP version 6（IPv6）標準仕様が策定されて以降 [1]，2021 年現在まで IPv6 インターネットと IPv4 インターネットの独立した 2 つのインターネットが並行して存在する状態が続いている. 現在では主要なホスト OS の IPv6 実装はおおよそ完了しており [2]，インターネットに接続するホストのうち 30% 以上が IPv6 インターネットに疎通性を持っている [3]．一方で，IPv6 対応が遅れている領域も依然として存在している．Cisco 社が提供している調査 [4] によれば，本稿執筆現在，日本国内において，インターネットユーザの 40% 程度が IPv6 を利用している一方で，主要な 500 の WEB コンテンツのうち IPv6 に対応しているサイトは 24% 程度に留まっている．また，すべての JP ドメインのうち IPv6 対応している FQDN は 3.59% のみとも言われている [5]．コンテンツサービスプロバイダー (CSP) の IPv6 対応が今後の IPv6 移行の大きな課題になると言える．

IPv6 移行の手法として最も一般的なものが IPv4/IPv6 デュアルスタックである．これは各ホストに IPv4 と IPv6 双方のアドレスを紐付け，2 つのネットワークに接続するプリミティブなモデルであるが，以下のようなサービス運用上の問題が指摘されており，各事業者の IPv6 対応の障壁となっている．

- IPv4 アドレスの継続的調達が困難
  各 Regional Internet Registry（RIR）の IPv4 アドレスプールでは実質的に割り当てを終了しており [6]，CSP やネットワーク事業者にとって IPv4 アドレスをサービスの成長にあわせて継続的に調達していくことは困難である．民間市場の市況に調達コストが左右されるため長期的な見通しが立てにくい.
- オペレーションコストの肥大化
  デュアルスタック環境では 2 つの異なる IP プロトコルを同時に運用する必要があるため、シングルスタック環境と比べて運用コストの増加が見込まれる.
- ネットワーク機器に求められる性能の増加
  デュアルスタック環境では，シングルスタック環境よりも多くの経路やポリシーをネットワーク機器が保持しなければならないため，より高性能な機器を導入する必要が生じる.

一方で，インターネット技術は IPv6 を前提とした設計が行われる段階を迎えている．2016 年には IAB[*1]により，“IAB Statement on IPv6” が発表され，インターネット標準では IPv6 に最適化した標準策定を行う方針が確認されている [7]．例えば既に Segment Routing over IPv6（SRv6）のような新しい標準は IPv6 の拡張ヘッダを利用した技術として策定が進められており [8]，IPv4 を前提とした長期的なネットワーク運用は限界を迎えているといえる.

1.2　vSIX プロジェクトについて

vSIX プロジェクトは完全な IPv6 シングルスタックを前提とした “vSIX ネットワーク” の設計・構築・運用を通して，IPv6 シングルスタックでのネットワーク運用に関連する問題の解決策を模索し，得られた知見や成果を社会還元することを目的として，学術プロジェクトである WIDE プロジェクト内のワーキンググループ (WG) として組織された.

また IPv6 関連技術に限らず，これからのインターネッ

* 慶應義塾大学政策・メディア研究科 後期博士課程
† 慶應義塾大学政策・メディア研究科 修士課程

*1 Internet Architecture Board. https://www.iab.org/

トを支える技術開発や若手人材の育成の場としての役割も担う．

2　vSIX の活動

2.1　活動体制

vSIX WG のメンバは WIDE プロジェクトに所属する各組織の研究者から構成されており，Slack[*2]やオンラインミーティングツールを活用して議論を行っているほか，第 5 章で述べる VPN サービスを利用して日常的に vSIX ネットワークに接続し研究課題の発見に努めている．

vSIX ネットワークやサービスの開発・運用は，ネットワークサービスの運用経験が浅い若手研究者を中心として，テーマや内容に応じた分科会に分かれて行われている．各分科会の活動内容に関しては次章以降で詳しく述べる．

また vSIX プロジェクトに直接関係しない研究活動にも精力的に取り組んでいる．過去には FRRouting[*3]の SRv6 機能開発や，トラフィックエンジニアリングのプロトコルの相互接続検証などに関する有志での勉強会を実施した．

2.2　vSIX BoF

WIDE プロジェクト内との成果の共有や議論と場として定期的に “vSIX BoF” を開催している．過去に開催された BoF の一覧を下記に示す．特に WIDE 合宿では合宿参加者にインターネット疎通性を提供する “Camp-Net” の役割を担うことも多い．

- **WIDE 2020 年 12 月研究会（2020/12/11 - 12）**
  “本気で IPv6 シングルスタック AS について考える BoF”
- **WIDE 合宿 Spring 2021（2021/03/16 - 18）**
  “vSIX BoF”, “Camp-Net BoF”
- **WIDE 2021 年 5 月研究会（2021/5/28 - 29）**
  “vSIX BoF”
- **WIDE 合宿 Autumn 2021（2021/9/7 - 9）**
  “vSIX BoF”, “Camp-Net BoF”
- **WIDE 2021 年 12 月研究会（2021/12/3 - 4）**
  “vSIX BoF”

3　Backbone Network

Backbone 分科会では，主に vSIX ネットワーク[*4] 内部の経路制御や，新たなネットワークバックボーン開発手法について，検討・運用を実践している．

3.1　現在のネットワークバックボーンの構成

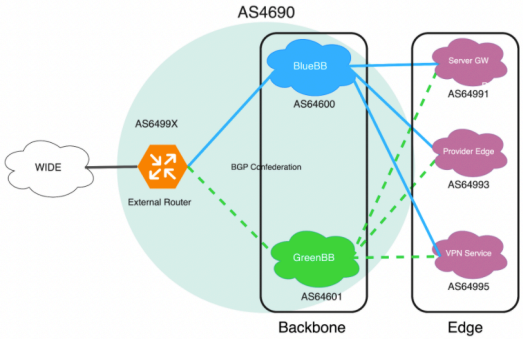

図 1　Outline image of vSIX Backbone

本稿執筆時点で，vSIX ネットワークは慶應義塾大学湘南藤沢キャンパス, KDDI 大手町, NTT 大手町の 3 拠点を結ぶ，“Blue” と “Green” の 2 系統のバックボーンネットワークにより構成されている．これらのネットワークは 3.2 節で述べる独自のデプロイメント手法により独立して管理されており，ネットワークを稼働させながら継続的に設計変更を行うことが可能である．

現在，各拠点のコアを担うルータは物理筐体と仮想ルータ（NFV）が混在して稼働している，2022 年度 に計画されている構成変更により，既存のネットワークバックボーンは独自にカスタマイズされたルーティングデーモンを利用した NFV で再構築し，新たにいくつかの拠点を追加で整備する予定である．

図 1 に vSIX バックボーンネットワークと vSIX 利用者や各分科会が設置するルータ（Edge）との接続関係を示す．各 Edge には vSIX ネットワーク内で一意のプライベート AS 番号を割り当てており，各拠点のバックボーンルータと BGP による経路交換を行っている．各系統のバックボーンルータと vSIX 外の AS とのピアリングを行うルータ（External Edge）間は BGP Confederation[9] による接続関係にある．そのため各 Edge は両系統のバックボーンルータに対して共通の AS 番号（AS4690）として接続することが出来る．

[*2] 組織やプロジェクト単位で利用可能なチャットサービス．https://slack.com/
[*3] オープンソースのルーティングプロトコル実装．https://frrouting.org/
[*4] vSIX ワーキンググループで運用しているネットワーク．AS 番号 4690

3.2 Internet Backbone における新しいデプロイメント手法の開発

Backbone 分科会では，vSIX ネットワークの基本的な運用だけでなく，新たなネットワーク運用モデルの検討及び運用実践も行っている．

3.2.1 従来のネットワーク運用モデル

サービスプロバイダーにおけるネットワークのポピュラーな運用モデルの一つとして，Cisco が提唱する “PPDIOO”[10] がある．このモデルでは，ネットワークのライフサイクルを Prepare, Plan, Design, Implement, Operate, Optimize のフェーズに分けて説明しており，各フェーズは基本的に一方向に遷移する．これはプロジェクトマネジメントで用いられるウォータフォールモデル [11] に近しい運用モデルであるといえる．

このような手法で構築されたネットワークは，一般に 5 年後のサービスを想定した設計が要求されると言われており [12]，運用フェーズで見つかった要求事項の変更は次のライフサイクルでの設計時に考慮することになるため，一度ネットワークの運用を開始するとしばらくの間は大きな構成変更を行うことができない．このような長期的サイクルでのネットワーク開発手法には以下の４つの点で課題がある．

1. **サービス要件の変化**
   インターネットアプリケーションの変化に伴って，顧客が必要とするトラフィックのパターンも日々変化する．設計段階での機能要件が，ネットワークのライフサイクル中の顧客のニーズに合致し続けるとは必ずしもいえない．
2. **技術革新に伴う陳腐化**
   ネットワーク構成技術や手法は常に新たなものが開発され続けており，当初の要件を充足するために最適な技術設計もそれに応じて変化していくことが考えられる．
3. **実利用の環境に即したテストが困難**
   設計・検証段階において，実際のサービストラフィックを利用した試験を実施できない．
4. **エンジニア・オペレータの育成**
   ネットワークのライフサイクルに関わり続けることは人材の能力開発の面で大きなメリットとなるが，ライフサイクルが長期に渡るため，その機会を十分に活用できない場合がある．

3.2.2 Blue-Green Deployments

本研究ではソフトウェアサービスのデプロイメント手法を取り入れることにより，先述した従来型のネットワーク運用モデルにおける諸問題の解決を目指す．

“Blue-Green Deployments”[13] は，WEB サービスを中心としてソフトウェアサービスの運用に近年頻繁に活用されている運用モデルである．Blue-Green Deployments では複数の独立した環境を用意し，時と場合によってどちらかを顧客へのサービス提供に利用する．サービス提供に利用されていない方の環境を利用して新しいバージョンの環境を構築することで，より短いスパンでのデプロイメントを可能にする．つまり新しいバージョンの展開及び古いバージョンへの切り戻しが安全かつ容易に行えるため，継続的インテグレーション（CI），継続的デプロイメント（CD）と親和性が高いことが大きな特徴である．

本手法を用いてリリースのスパンが短くすることで，サービス要件の再検討が行いやすくなり，より柔軟に顧客のニーズに対応可能になる．また積極的に新技術を採用したアグレッシブなサービス設計を検証・展開しやすくなるほか，より短いスパンでの人材の能力開発を行うことが期待される．

3.2.3 Canary release

Blue-Green Deployments において，影響範囲を限定した安全なリリースを行う技術の一つに “Canary release” がある．

Canary release とは一部のユーザのみを他のユーザとは異なるサービス提供環境に誘導し，ユーザの実際のトラフィックを利用して十分に検証を行った後に，徐々に全ユーザを新しいバージョンの環境に切り替えていくリリース手法である．

これにより，影響範囲を最低限に抑えた新構成の展開が可能になり，より安全に実トラフィックを利用した計測・評価を行うことができる．Blue-Green Deployments と Canary release の両方を適用したデプロイメント手法のことを，以降 Canary release with Blue/Green Deployments として呼称する．

3.2.4 Canary release with Blue/Green Deployments の要件

Canary release with Blue/Green Deployments を適用するためには下記の 5 つの要件を満たす必要がある．提供するサービスの種別によっては本モデルを適用できない場合があることに留意されたい．

1. **モデルを適用するスコープの明確化**
   サービスや環境に応じた明確な対象領域の定義が求められる．
2. **“Blue/Green” の独立性**
   ２つの環境は相互に依存しない独立した環境にする必要がある．
3. **リアルタイムなモニタリング**
   ２つの環境のそれぞれにおいて，“サービス提供が想定通りにどうか” をリアルタイムに把握する必要性がある．
4. **インターフェースの共通化**
   ユーザーのトラフィックを Blue/Green の両環境に誘導する方法や，そのインターフェースは共通化されている必要がある．
5. **ステート情報の取り扱い**
   顧客に対してステートフルなサービスを提供する場合，セッション情報を２つの環境内でどのように共有するかを検討する必要がある．

3.3 Blue/Green Deployments による vSIX バックボーンネットワークの運用実験

Backbone 分科会では，ネットワーク運用における Canary release with Blue/Green Deployments のフィジビリティを評価するために，vSIX バックボーンネットワークでの運用実験を行っている．

3.2.4 節で述べた 5 つの要件を満たすために，本運用実験では以下のような前提条件を設定している．

1. **モデルを適用するスコープの明確化**
   本運用実験では，各拠点を接続するバックボーンネットワークを Blue/Green Deployments の対象領域とする．vSIX 外部との接続を担う External Edge は本モデルの対象領域としない．
2. **“Blue/Green” の独立性**
   vSIX における Blue/Green バックボーンは相互に接続しない，論理的に独立した設計を採用している．
3. **リアルタイムなモニタリング**
   本運用実験では “正常な動作” をネットワークレイヤーで正しく疎通可能であることと定義している．具体的なモニタリング手法に関しては 3.4 節で述べる．
4. **インターフェースの共通化**
   3.1 節で述べたように，各 Edge とバックボーンルータの間は BGP により接続される．トラフィックの誘導方法に関しては 3.3.1 節で示す．
5. **ステート情報の取り扱い**
   本運用実験ではステートレスに処理出来る IP パケットのフォワーディングのみを対象とする．

3.3.1 Blue/Green の切り替え手法

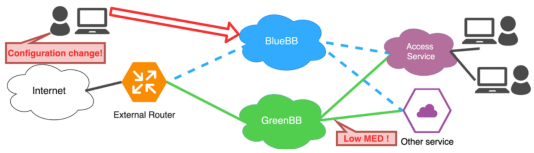

図 2　Blue/Green の切り替え手法

vSIX バックボーンにおける Canary release with Blue/Green Deployments において，各ユーザ (Edge) のトラフィックの振り分けは BGP Path Atrribute を用いて行う．図 2にトラフィックのフローを示す．本環境では MULTI_EXIT_DISC(MED) の値をソフトウェア[*5]から操作することにより実現している．

.

3.4 経路監視アプリケーション

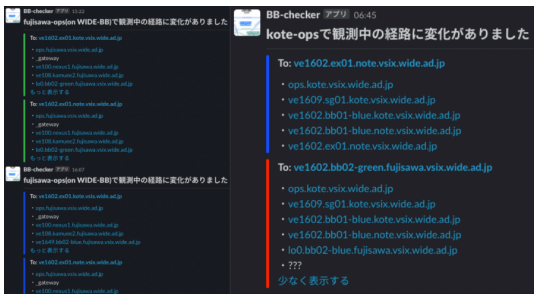

図 3　アプリケーションからの通知画面

Blue/Green の両環境が適切に動作するか，ユーザのトラフィックが現在どちらの環境に誘導されているかを監視するために，経路監視アプリケーションを実装した．このアプリケーションの実際の動作画面を図 3に示す．

このアプリケーションでは，内部で定期的に `mtr` コマンド[*6]を実行しており，事前期待される経路を記述したファイルを参照して経路のトレース結果を評価している．経路に変更があった際にリアルタイムにオペレータに通知する

[*5] 執筆時点では構成管理ツールである Ansible を利用したプッシュ型の操作を行っている．`https://www.ansible.com/`
[*6] パケットの Hop-limit の値を操作することで経由するルータを可視化するアプリケーション．を `https://github.com/traviscross/mtr`

機構を備える．．

なお本アプリケーションは様々な環境で動作させることを期待し， Docker[*7]を利用したコンテナ化を行うことで，高可搬性を実現している．

3.5　今後の展望

Backbone 分科会では，vSIX ネットワーク拠点の拡大や，Blue/Green Deplyoments の運用環境の改善を継続して行う予定である．現在 vSIX バックボーンは 3 つの拠点を相互に接続する単純な三角形のネットワーク・トポロジを採用しているが， Canary release with Blue/Green Deployments の有効性をより深く検証するためにも，いくつかの WIDE 組織の施設への新拠点の設置を予定している．複雑なネットワークでの運用試験を行うことが可能になり，より社会に対する貢献度を高めることが期待されている．

また 3.3.1 節や 3.4 節のような，Blue/Green Deployments に不可欠な機能を総合した独自の SDN ソフトウェアの開発も予定している．今後はこのソフトウェアをビルトインした独自の NFV バックボーンルータを各拠点に展開し，より高度なオペレーションの実現に向けた取り組みを積極的に継続していく．

4　External Network

External 分科会では，主に対外接続や AS としての経路ポリシーの策定を行っている．

4.1　External 分科会の現在の課題

External 分科会は，他の AS と対外接続を行い vSIX ネットワークのインターネット接続性を確保すること，外部 AS からのトラフィックをバックボーンネットワークに適切に流すこと，また他の AS から vSIX ネットワークのコンテンツへのアクセスをより効率良く提供することがある．

1 つ目として，vSIX ネットワークからインターネットへの接続性を提供するためには，トランジットに接続する必要があり，またより安定したインターネット接続性を提供するために複数のトランジットに接続する必要がある．さらに，接続する拠点も複数用意し，より冗長化して接続できる環境を用意する必要がある（4.2.1 節）．

2 つ目として，3.1 節でも紹介した通り，vSIX ネットワークのバックボーンネットワークは Blue/Green Deployments を行っており，トラフィックに応じて Blue や Green のどちらの面を利用するかを決定する．仮にこのバックボーンルータが直接外部 AS とピアリングをした場合，外部 AS がバックボーンネットワークが広報する BGP アトリビュートを守らず，想定とは異なる面を利用してしまう可能性がある（4.2.2 節）．

3 つ目として，一般に AS がコンテンツを配信する場合，純粋な BGP で学習した経路情報は何らかの理由で理想的な経路とは異なる可能性がある．例えば本ワーキンググループが直面した事例として，本来 3-hop で到達可能な場所にある AS が 5-hop 経由するよう学習されていた場合があり，これにより著しくコンテンツへのアクセスが遅くなった．この問題を解決するために，コンテンツ配信側が適切に経路を学習し，不適切な経路を学習している場合，それを検出する仕組みや経路を変更する仕組みが必要である（4.2.3 節）．

4.2　External 分科会の活動状況

4.2.1　vSIX ネットワークの対外接続状況

図 4 に示す通り，現在 vSIX ネットワークは WIDE ネットワーク[*8]をトランジットとして利用しており，現在多少の問題点は存在するが，慶應義塾大学湘南藤沢キャンパス拠点，NTT 大手町拠点の 2 拠点で WIDE ネットワークと接続している状況である．しかし，まだ単一の AS しかトランジットとして利用できていない状況であるので，冗長化の観点で課題が存在している．

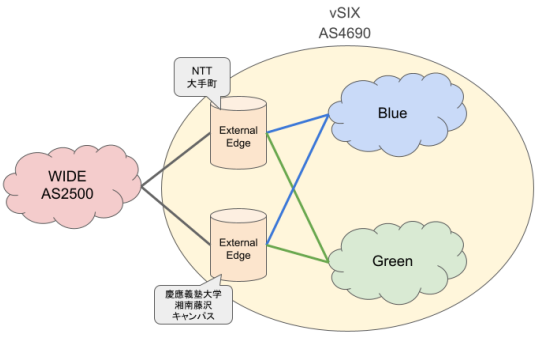

図 4　vSIX ネットワークの対外接続状況

[*7] https://www.docker.com/

[*8] WIDE プロジェクトで運用しているネットワーク．AS 番号 2500

4.2.2　バックボーンネットワークとのトラフィック連携

図 5 に示す対外接続用のルータとして External Edge を作成し，ピアリング AS とバックボーンネットワークとの間に配置した．

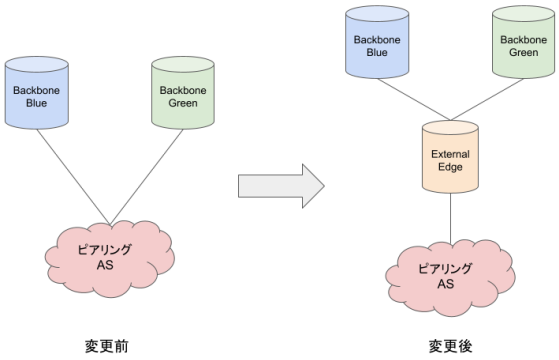

図 5　External Edge

このルータの作成意図は，トラフィックに応じて Blue や Green のどちらの面を利用するかを決定する主体を外部 AS ではなく，vSIX ネットワーク内のオペレータ（本分科会）に行わせるためである．バックボーンネットワークでは Blue/Green Deployments を行っており，MED 値を広報することでトラフィックが Blue 面と Green 面のどちらを流れるかを決定している．しかし，ピアリング AS が Local Preference 値などを設定し vSIX ネットワークが広報する MED 値に依らずにパケットを転送してくる可能性が存在するため，External Edge を作成した．External Edge は対外接続を担うと同時にバックボーンネットワークともピアリングを行うことにより，ピアリング AS からのトラフィックを External Edge が受信し，そのトラフィックを Blue/Green 面を適切に選択してバックボーンネットワークに転送することにより，バックボーンネットワークが想定する面へのトラフィックの転送を実現した．

4.2.3　柔軟な経路選択機構

今後 AS 内でコンテンツを配信した際にそのコンテンツをユーザに効率よく配信するために Egress Peer Engineering（EPE）[14] の検証を行っている．図 6 で示したように，EPE とは AS がインターネットに出ていく通信に対して，既存の BGP に依らず意図的に狙ったピア（Egress Peer）に向けてトラフィックを転送できる技術のことである．

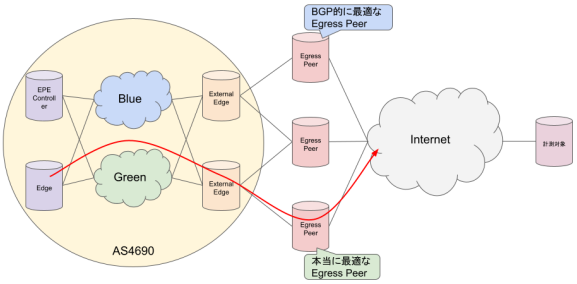

図 6　Egress Peer Engineering

本分科会では EPE を実現するための技術として Segment Routing IPv6（SRv6）を利用することとした．SRv6 は BGP アトリビュートを変更するよりオペレーションコスト低く柔軟な経路制御が行えることや，各 Edge での処理を自分で追加できるため拡張性に富んでいることなどが SRv6 を導入した理由である．また，External Edge の BGP 接続状況を監視したり，ping や traceroute を用いて通信品質を監視し，その状況に応じて SRv6 で経路制御を行うための encap や decap の処理をルータに投入する役割を担う EPE コントローラを作成した．

現状の EPE は以下のような手順を実装し，実現している．

1. External Edge は EPE コントローラに対し Egress Peer の BGP ステート情報や経路情報を送信する
2. EPE コントローラが External Edge に対し，SRv6 のヘッダを decap して狙った Egress Peer に送信するためのコンフィグを送信する
3. 計測対象の宛先を 1 つ決定し，その宛先への経路を受信している Egress Peer の中から 1 つを選び，その Egress Peer を経由するよう SRv6 ヘッダを encap する処理を EPE コントローラ自身に記述する
4. EPE コントローラは ping を送信することで，特定の Egress Peer を経由する場合の RTT の情報を入手する
5. 項目 3, 4 の処理を，経由する Egress Peer を変更して行う
6. 項目 3, 4, 5 により，ある宛先に対し最適な Egress Peer が決定すると，他のルータのルーティングテーブルに対しその最適な Egress Peer を経由するように SRv6 ヘッダを encap する処理を記述したコンフィグを投入する
7. 項目 3, 4, 5, 6 で示した処理を宛先を変更して計測を行う

今は上記の単純な仕組みで動いているが，今後はより柔軟な経路制御を行うための仕組みを構築する必要がある．

4.3 今後の展望

4.2.1 節で述べたように，現状では単一の AS しかトランジットとして利用できておらず，冗長性に課題がある．また EPE の機構を作成したが，現状 Egress Peer は全て WIDE ネットワークのルータのため，EPE の機構がどれほど有意なものであるかの検証がしづらいという問題点が存在する．これらの問題点を解決するために，接続するトランジットの数を増やしていく必要がある．

また，3.1 節で述べたように，今後 vSIX のネットワークは新拠点が追加されるため，各拠点へ External Edge を追加していく必要がある．

さらに，4.2.3 節で述べたように，EPE の実験は現状不完全であるため，今後は宛先アドレス以外の情報を考慮して encap 情報を記述したり，RTT 以外のポリシーも考慮して最適な経路の決定を行っていく必要がある．

5 Access Service

Access Service 分科会は，エンドユーザ収容の設計・開発・運用を担当し，生活ネットワークとしての vSIX ASs を提供する．

5.1 全体像

現状のシステム構成を図 7 に示す．NTT 大手町拠点，KDDI 大手町拠点，慶應義塾大学湘南藤沢キャンパス拠点の 3 拠点に接続ルータを展開し，NTT 大手町拠点および KDDI 大手町拠点にて WIDE バックボーンからの，KDDI 大手町拠点および慶應義塾大学湘南藤沢キャンパス拠点にて NGN からのユーザ直収に対応する．なお，KDDI 大手町の NGN 端点は，東京大学江崎研究室のフレッツ線を L2 延伸したものである．いずれのルータも，NetBox と Ansible により構成管理され，デプロイ工程は完全に自動化されている．

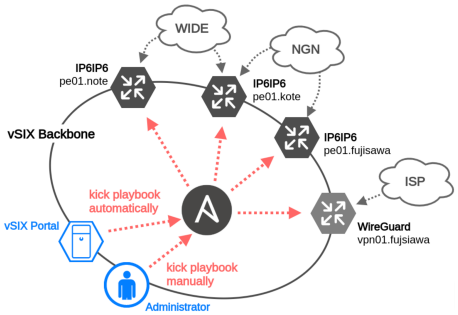

図 7 Access Service の全体像: 3 拠点 4 台の VM を NetBox と Ansible で構成管理

また，研究目的から，vSIX バックボーンに流れるすべての DNS トラフィックは，分科会内製ツール[*9]を用いてキャプチャし保存している（図 8）．

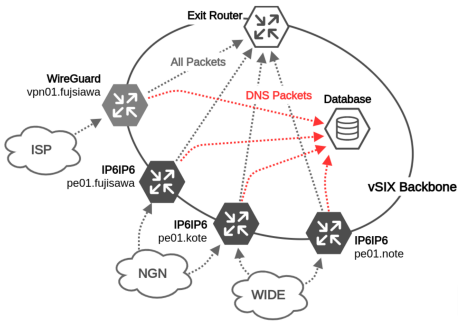

図 8 Telescreen: すべての DNS クエリ・レスポンスペアをデータベースに保存

接続方式として **Generic Tunneling Service（5.3 節）** と **Remote Access VPN Service（5.4 節）** の 2 種類を提供，また，それらのフロントエンドとして **vSIX Portal（5.2 節）** と，Raspberry Pi ベースのブロードバンドルータ **vSIX Pi（5.5 節）** を開発した．

5.2 vSIX Portal

ユーザ情報の確認，接続方式の申し込みと変更，端末のセットアップ支援情報を提供する Web フロントエンドである（図 9）．バックエンドは NetBox，Ansible と連携しており，ユーザの操作を安全かつ即座に本番環境へ反映する．

[*9] Telescreen - a tiny program intercepting DNS query-response pairs（`https://github.com/wide-vsix/telescreen`）

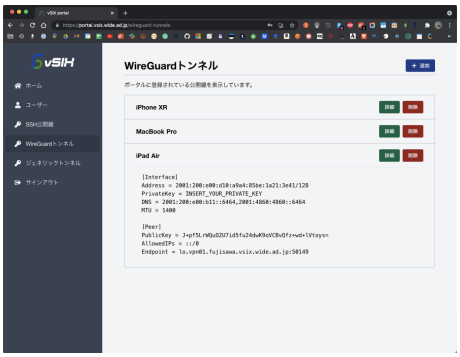

図 9　vSIX Portal: 各種接続方式の申し込みとセットアップ支援情報を提供

5.3　Generic Tunneling Service

ユーザ所有ルータとの間に IP6IP6 トンネルを構築し，トンネル越しの DHCPv6-PD により，/60 のグローバルプレフィックスを配布する．NGN もしくは WIDE バックボーン経由での接続を受け付けており，これにより vSIX ユーザに対して，商用 ISP によらないインターネット接続性を提供する．

5.4　Remote Access VPN Service

WireGuard[*10]を用いたインターネット経由での VPN サービスで，/128 のグローバルアドレスを配布する．別章にて説明する SIIT-DC により，IPv4 クライアントからの接続も受け付けているため，IPv4 接続性のみを有するユーザに対して，vSIX AS 経由での IPv6 接続性を提供可能である．

5.5　vSIX Pi

vSIX 公式ブロードバンドルータであり，その実体は，cloud-init[*11]を用いて，Raspberry Pi を vSIX 接続ルータ兼 Wi-Fi アクセスポイントとしてセットアップするユーティリティである．vSIX Portal にて提示される情報を YAML 形式の設定ファイルに記載するだけで，必要な cloud-config が自動生成されるため，誰もが手軽に Generic Tunneling Service を扱えるようになる．

ネットワーク技術に明るくないアプリケーション開発者を主なターゲットに，即席の IPv6 シングルスタック・マルチホーム環境の構築手段を公式に提供することで，vSIX ネットワークのテストベッド利用促進に繋がると期待し開発した．

5.6　今後の展望

Backbone，External 分科会の動きに合わせて，Access Service 分科会でも SRv6 の導入を進めている．IP6IP6 と DHCPv6-PD による現在のアドレス配布方式を，SRv6 の VPN 機能で同等に実装し，SR ドメインのエンドユーザまでの拡大を目標とする．

また，vSIX Pi にバックボーン正常性確認機能を実装し，エンドユーザ視点でのサービス品質計測を実現する．ネットワーク品質計測に知見を有する SINDAN WG からの技術支援を受けながら，vSIX プロジェクト に特化したシステムとして完成させる予定である．

6　Service

Service 分科会では，主にサービスプラットフォームの開発・運用実験を行っている．

6.1　DNS64

vSIX ネットワーク内のサーバ機器及び利用者に対して DNS フルサービスリゾルバを提供している．vSIX は IPv6 シングルスタックネットワークであるため，vSIX 内からインターネット上の IPv4 サービスにアクセスするためには NAT64 と DNS64 機構が必要である．そのため，Service 分科会の提供するフルサービスリゾルバでは通常の名前解決サービスに加え， DNS64 サービスを提供している．実装には既存の OSS 実装である Unbound[15] を利用している．サービス提供開始直後にはプロキシリゾルバとして外部の DNS64 パブリックリゾルバに対してクエリを転送していたが，2021 年夏頃よりフルサービスリゾルブを開始した．現在は単独のノードで運用しているが，可用性確保と遅延低減のため今後は複数 NOC に複数ノードを配置し運用する予定である．

6.2　Kubernetes と IPv6

vSIX ではプラットフォーム上でのサービス提供基盤として， Kubernetes[*12] を選定した．vSIX は IPv6 シングルスタックネットワークであるため， Kubernetes 上の任意のコンポーネントは IPv6 に対応している必要がある．

[*10] WireGuard: fast, modern, secure VPN tunnel （https://www.wireguard.com/）
[*11] https://cloud-init.io/
[*12] https://kubernetes.io/

Kubernetes とその周囲のコンポーネントの IPv6 対応状況としては， Kubernetes そのものが IPv6 シングルスタックおよび IPv4/IPv6 デュアルスタックに対応している [16] ．また，今年度に vSIX 活動の一環としてコンテナ間及びコンテナ内外の通信を管理するコンポーネントである Container Network Interface（CNI） の IPv6 対応状況について調査を行った [17]． しかし，他の Kubernetes 周辺のコンポーネントについては， IPv6 シングルスタックにおける対応状況が周知されていないのが現状である．

このことから Service 分科会では , Kubernetes を IPv6 シングルスタック で構築・運用するための知見を整理することを目標に， Kubernetes の各種コンポーネントの選定及び構築を行った．

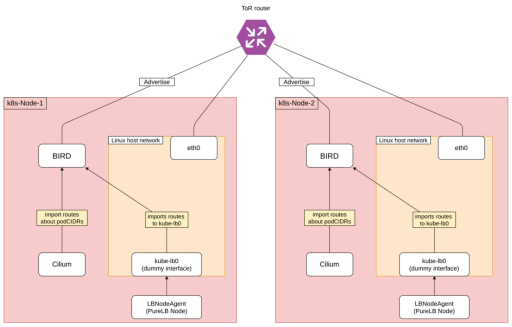

図 10　Kubernetes topology

Kubernetes プラットフォームのトポロジを，図 10に示す．

採用した Kubernetes プラットフォームの構成は以下のとおりである．ロードバランサの候補としては，MetalLB[*13]，PureLB[*14] の 2 つが候補として挙げられた．MetalLB は L3 モードで IPv6 に対応していなかったため， PureLB を採用した．CNI の候補として，Calico[*15], Cilium[*16] の 2 つが候補として挙げられた．Calico は PureLB と組み合わせるとうまく動作させることが出来なかったため， Cilium を採用した．また，PureLB の経路と Cilium の経路の両方を広告するために，BIRD[*17] を用いている．

6.3　今後の展望

Service 分科会では，6.2 節で述べたように IPv6 シングルスタック環境における Kubernetes の各種コンポーネントの対応状況を整理し，現状におけるベストプラクティスの構成を示した．しかし，Kubernetes はあくまでサービスをデプロイするための基盤であり，今年度における活動はその地盤を固めたにすぎない．来年度以降は，実際に Kubernetes 上でサービスを稼働させ，IPv6 環境下での Kubernetes コンポーネントの対応状況の検証を行いつつ，各サービスのデプロイの自動化/簡略化を進める予定である．

また，近年 Kubernetes の機能である Custom Resource Definitions（CRD）を用いてネットワーク運用を行うアプローチが出てきている [18]．今後は Kubernetes を用いて，ネットワーク運用に関しても自動化が行われるような開発的アプローチも行う．

7　Camp-Net

WIDE 研究会及び WIDE 合宿は，新型コロナウイルス感染症の感染拡大防止のため，2020 年春以降オンラインで行われてきた．

7.1　2021 年 9 月合宿での vSIX WG の貢献

オンサイト WIDE 合宿にて提供してきた Camp-Net（現地参加者のための実験用会場ネットワーク）に代わる新たな試みとして，vSIX（AS4690）を経由した IPv6 シングルスタックでのインターネットアクセスを提供した．合宿に先立って vSIX Access Service（5 章） を正式にリリースし，WIDE メンバから接続希望者を公募，Slack に招待したのち，開発者らが直接ユーザの環境セットアップを支援した．

合宿期間中のユーザからのフィードバックにより，vSIX ネットワークの技術的な不具合がいくつか発見，修正されている．また，IPv6 シングルスタック環境で動作しないサービスやアプリケーション，その他の知見を積極的に共有し合うことで，参加者同士のコラボレーションを促進した．

7.2　実績報告

以下に実績をまとめる．

- **新規登録ユーザ数:** 14 名が新規に WG に参加した

[*13] https://metallb.universe.tf/
[*14] https://purelb.gitlab.io/docs/
[*15] https://www.tigera.io/
[*16] https://cilium.io/
[*17] https://bird.network.cz/

- **Generic Tunneling:** 11 件の接続申請を受け付け，合計 176 の/64 プレフィックスを払い出した
- **Remote Access VPN:** 30 件の接続申請を受け付け，合計 30 の/128 アドレスを払い出した
- **A/AAAA クエリ数:** 372555 件の A クエリ，594140 件の AAAA クエリを観測し，記録した
- **AAAA レスポンス数:** 196246 件がネイティブアドレスで，177429 件が変換アドレスで返却された

8 終わりに

本報告では本年度に新しく組織された vSIX プロジェクトの狙いや WIDE プロジェクト WG としての運営体制，vSIX ネットワークで行われている実験活動について詳細に述べた．

本 WG では今後も将来のインターネットを支える運用技術の開発や人材の輩出を目指し，日々精力的に活動を行っていく．

9 謝辞

本プロジェクトは森泰吉郎記念研究振興基金研究者育成費交付により組織・実験・対外発表が遂行されたものです．国際発表参加費や実験用品の整備に充てさせていただきました．この度のご支援に対して厚く御礼を申し上げます．

参考文献

[1] B. Hinden and D. S. E. Deering, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998. [Online]. Available: https://rfc-editor.org/rfc/rfc2460.txt

[2] 北口善明, 近堂徹, 鈴田伊知郎, 小林貴之, and 前野譲二, "クライアント os の ipv6 実装検証から見たネットワーク運用における課題の考察," **デジタルプラクティス**, vol. 9, no. 4, pp. 902–922, oct 2018.

[3] Google, "Ipv6 statistics," accessed: 2021-12-31. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html

[4] Cisco, "6lab - the place to monitor ipv6 adoption (japan)," accessed: 2021-12-31. [Online]. Available: https://6lab.cisco.com/stats/cible.php?country=JP

[5] M. NABESHIMA, "Jp ドメイン ipv6 survey 2021," accessed: 2021-12-31. [Online]. Available: https://www.kosho.org/blog/net/ipv6survey2021/

[6] potaroo, "Ipv4 address report," accessed: 2021-12-31. [Online]. Available: https://ipv4.potaroo.net/

[7] C. Morgan, "Iab statement on ipv6," 2016, accessed: 2021-12-31. [Online]. Available: https://www.iab.org/2016/11/07/iab-statement-on-ipv6/

[8] C. Filsfils, P. Camarillo, J. Leddy, D. Voyer, S. Matsushima, and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming," RFC 8986, Feb. 2021. [Online]. Available: https://rfc-editor.org/rfc/rfc8986.txt

[9] P. S. Traina, J. Scudder, and D. R. McPherson, "Autonomous System Confederations for BGP," RFC 5065, Aug. 2007, accessed: 2021-12-31. [Online]. Available: https://rfc-editor.org/rfc/rfc5065.txt

[10] K. Wallace and M. Watkins, *CCDP ARCH Quick Reference*, ser. Quick Reference. Pearson Education, 2007. [Online]. Available: https://books.google.co.jp/books?id=14TrM1Go8ekC

[11] D. B. Kai Petersen, Claes Wohlin, "The waterfall model in large-scale development," 2009. [Online]. Available: https://doi.org/10.1007/978-3-642-02152-7_29

[12] A. Sholomon and T. Kunath, *Enterprise network testing: Testing throughout the network lifecycle to maximize availability and performance*. Pearson Education, 2011.

[13] J. Humble and D. Farley, "Continuous delivery: Reliable software releases through build, test, and deployment automation," ser. Addison-Wesley Signature Series (Fowler). Pearson Education, 2010, pp. 261–262. [Online]. Available: https://books.google.co.jp/books?id=6ADDuzere-YC

[14] "draft-filsfils-spring-segment-routing-central-epe-01," https://datatracker.ietf.org/doc/html/draft-filsfils-spring-segment-routing-central-epe-01.

[15] NLnet Labs, "Unbound - About," accessed: 2021-12-31. [Online]. Available: https://nlnetlabs.nl/projects/unbound/about/

[16] "Kubernetes 1.23: Dual-stack ipv4/ipv6 networking reaches ga," accessed: 2021-12-31. [Online]. Available: https://kubernetes.io/blog/2021/12/08/dual-stack-networking-ga/

[17] "Kubernetes/cni の ipv6 対応の現状と実態," ac-

cessed: 2021-12-31. [Online]. Available: https://ipv6-wg.connpass.com/event/214373/

[18] "High Functional Cloud NFV System Design and Implementation at LINE Cloud," accessed: 2021-12-31. [Online]. Available: https://speakerdeck.com/line_developers/high-functional-cloud-nfv-system-design-and-implementation-at-line-cloud