第５部

特集5 vSIXプロジェクトの取り組み

豊田 安信、深川 祐太、澤田 開杜、金谷 光一郎、宮 太地、橘 直雪

第１章　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[106]、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[107]、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[108]。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[109]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[110]。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[111]、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[112]。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[113]、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組織された。

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

またIPv6関連技術に限らず、これからのインターネッ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。

2020年12月に実施されたWIDE研究会での議論をもとに、半年弱の準備期間を経て、2021年5月よりWIDEプロジェクト内のワーキンググループ(WG)としての活動を開始している。

第２章　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”
- WIDE2021年12月研究会(2021/12/3 - 4)
  “vSIX BoF”

第３章　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

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

＊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

タ(External Edge)間はBGP Confederation[114]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。

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”[115]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[116]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[117]、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。

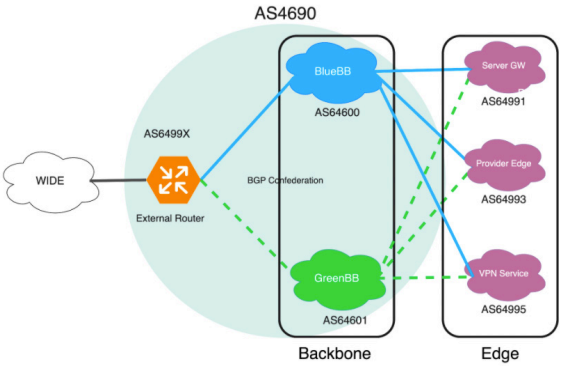

図1　Outline image of vSIX Backbone

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”[118]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

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

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機構を備える。

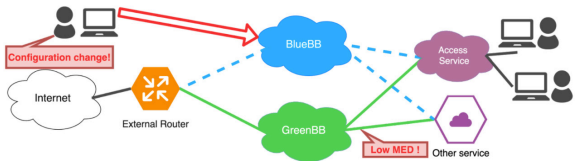

図2 Blue/Greenの切り替え手法

図3 アプリケーションからの通知画面

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。

第4章 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

＊5 執筆時点では構成管理ツールである nsible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。https://github.com/traviscross/mtr
＊7 https://www.docker.com/

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。

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。

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

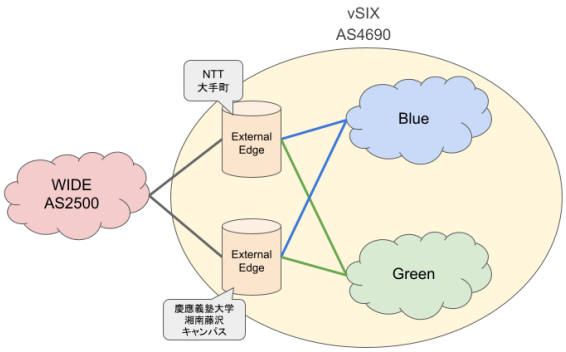

図4　vSIXネットワークの対外接続状況

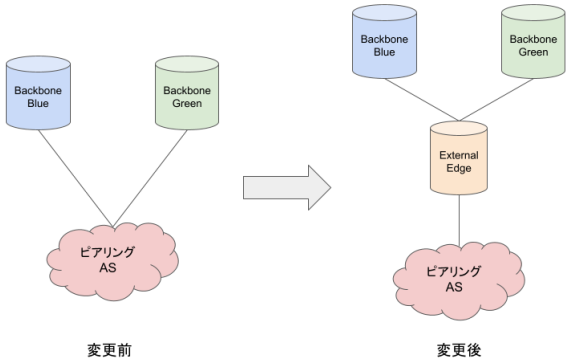

図5　External Edge

＊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

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）[119]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。

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

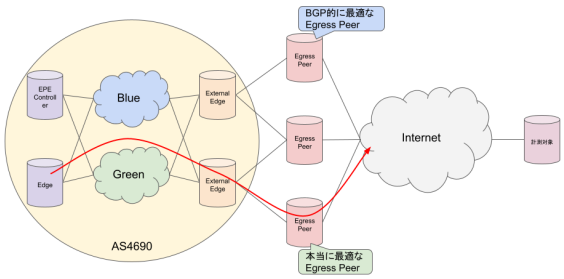

図6　Egress Peer Engineering

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。

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。

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）。

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。

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

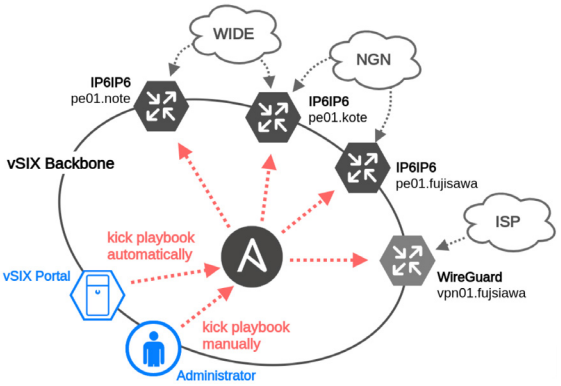

図7　Access Serviceの全体像: 3拠点4台のVMをNetBoxとAnsibleで構成管理

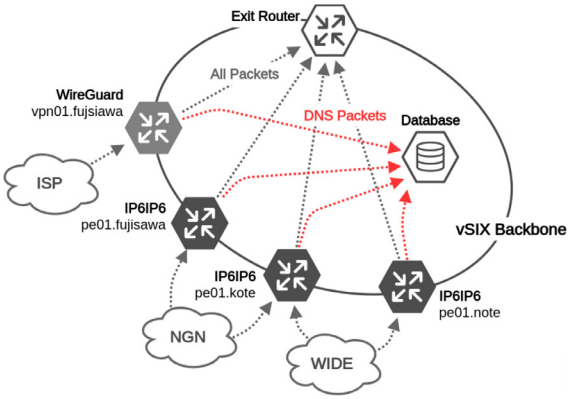

図8　Telescreen: すべてのDNSクエリ・レスポンスペアをデータベースに保存

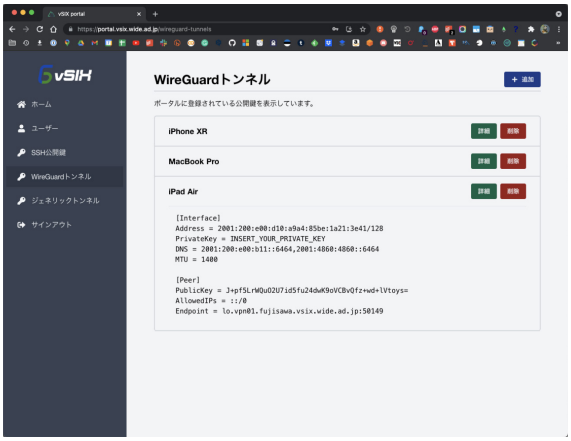

図9　vSIX Portal: 各種接続方式の申し込みとセットアップ支援情報を提供

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

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。

第6章 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[120]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。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[121]。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[122]。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

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

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。

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。

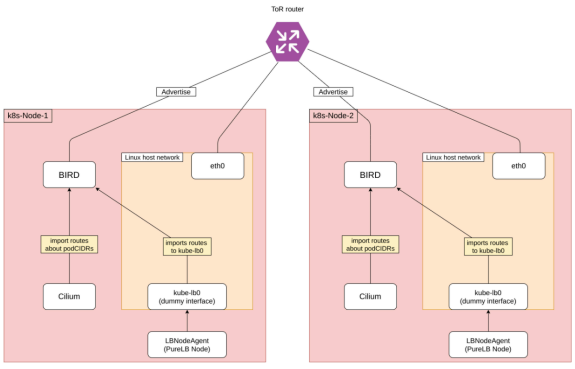

図10　Kubernetes topology

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[123]。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。

第7章　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。

＊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/

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
- 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

第８章　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WGとして運営体制、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。