第４部

特集4 高度情報インフラストラクチャの構築に関する研究

関谷 勇司、岡田 和也、山本 成一

第１章　はじめに

本研究では、商用インターネットを相互に接続する場合の問題点を明確にし、それを解決するための技術や手法の研究開発ならびに実証実験を行うことを目的とした実証実験を行う。また、近年成長し続ける動画系のインターネットトラフィックに対して、トラフィック輻輳を防ぎ、ユーザへの応答性を保つためのトラフィックエンジニアリングや、大規模災害等の障害にも対応可能な強固なインターネットバックボーンの形成に関する実証実験を目的とする。さらに、Software Defined Networking (SDN) のIXへの適用を検討し、より柔軟な構成やトラフィック制御が可能な次世代IXのモデルに関する研究を行う。

具体的には、WIDE Project のサブプロジェクトである、Network Service Provider Internet eXchange Point (NSPIXP) プロジェクトにて行われている、DIX-IEならびにNSPIXP-3 の運用を通じて、新技術の研究開発や実証実験を行った。これにより、インターネットがより信頼性を有した高度情報インフラストラクチャとして機能するために必要となる機能の検証や開発、ならびにその実証実験を行った。

NSPIXP プロジェクトは、1994年のNSPIXP-1運用開始、1996年のNSPIXP-2運用開始、1997年のNSPIXP-3運用開始を経て、東京に分散配置したDIX-IE、大阪に分散配置したNSPIXP-3、IPv6に特化したNSPIXP-6の運用を基盤とした実証実験を行ってきた。2008年6月にNSPIXP-6の運用を終了し、現在はDIX-IE、NSPIXP-3におけるプロダクション品質のIPv6/IPv4デュアルスタック運用に取り組んでいる。さらに2012年は、DIX-IEとNSPIXP-3を連結した、広域IXであるNSPIXP-23の運用も開始した。本年度は、さらに柔軟なトラフィック制御を可能とすべく、SDN を取り入れた SDN-IX の構築に関する検討と準備をすすめた。

本報告書では、第2章にて該当期間の研究計画を再掲し、その研究計画に基づいた該当期間の成果を第3章にて報告する。最後に、第4章にてまとめを行い、今後の活動方針について述べる。

第２章　本年度の研究計画

NSPIXP プロジェクトでは特に近年、高信頼性および高効率性を考慮した上での分散ネットワークアーキテクチャに着目し、トラフィック制御技術の実証および展開の検討と議論を行ってきた。現在、今後のトラフィック動向をふまえたIXの利用方法に関する議論と、次世代 IX に向けた取り組みであるSDN-IX の実現手法に関する活動を中心とした研究を行っている。さらに、東阪を接続した広域IXであるNSPIXP-23では、トラフィックエンジニアリングに重心をおいた実証実験を行なっている。関東と関西にまたがった広域IXを利用し、より強固な、拠点単位の災害に対応することのできるインターネットバックボーンとIXのアーキテクチャに関する実証実験に取り組んでいる。

研究計画書にて示した通り、該当期間の研究課題は以下の3項目である。

2.1　拠点障害にも対応できるIXならびにサービスアーキテクチャの研究

DIX-IEならびにNSPIXP-3では、トラブルを極力低減し、万が一の障害発生時においても自動的に回復することの

できるようなIXアーキテクチャに関する設計と検証を進めてきた。この成果として、2012年には、DIX-IEとNSPIXP-3を相互接続する形で、図2.1に示すNSPIXP-23を構築し、サービス開始を行った。NSPIXP-23上にて、サービス全体を高速にマイグレーションするためのクラウドクラスターマイグレーションの実証実験を開始した。近年の仮想化技術では、一台の物理サーバの中に仮想サーバを複数起動し、多重化して利用する傾向にある。この際、サーバの仮想化を行うソフトウェア技術をハイパーバイザと呼ぶが、本研究では仮想サーバ単体ではなく、ハイパーバイザごとすべてマイグレーションすることを目的とした実証実験を行った。このためには、ハイパーバイザ技術自体の抽象化や仮想化、ストレージの移動技術といった要素技術が必要となる。2013年はこれらの研究課題に取り組んだ。さらに、より障害に強いIXアーキテクチャとして、東京と大阪にまたがる広域IXの構成のみならず、それを利用したサービスの展開手法についての検討と検証を行った。具体的には、現在東京と大阪両方に存在する、Root DNS サーバや JP DNS サーバに関して、それぞれが障害時にお互いの役割を補うことができるような構成の検討、構築を行った。さらに、実験参加者の中にも、東京と大阪両方の拠点にインタフェースを有し、負荷を分散してコンテンツ配信実験を行った事業者も存在した。

これらの成果をうけ、2014年はより柔軟な分散サービス構築やトラフィック交換を可能とすべく、別課題であるSDN-IXと連携した分散IXアーキテクチャの研究を行った。ユーザの接続要求に対してどちらの拠点にあるサービスにそのトラフィックを導くか、また拠点の間でQoSを保証して専有したトラフィック交換を行うためにはどうすれば良いか、そのアーキテクチャの検証と実証を行う予定である。

さらに、品質の保証に関して2013年から試験的に実施している、EtherOAMを活用したCC(Continuity Check)とLT(Link Trace)による広域IXの監視手法の確立課題に関しても、2014年も引き続き取り組んだ。NSPIXP-23は、その構成上多段スイッチ構成にて構築されているため、何か障害が発生した場合には、どの地点の回線、もしくは機器にて障害が発生したのかを突き止める必要がある。従来の手法であれば、スイッチのリンク状態の監視や、スイッチ間にping用の端末を設置することでping監視を行い、障害箇所の特定を行なっていた。一方、EtherOAMを利用した場合には、追加の機材や監視のためのネットワーク設定を必要とすることなく、多段スイッチ構成においても障害点を特定することが可能となる。そのため、広域IXを構成する場合の多段構成での監視モデルの確立に関する研究を行う。

2.2 IPv4/IPv6トラフィック成分分析に関する研究

IPv4からIPv6への移行が進むにつれて、IX におけるIPv6でのBGP peering も増加している。これはIPv4アドレス枯渇にともなうIPv6への移行が本格化してきたことを反映していると考えられる。IPv4のトラフィック成分とIPv6のトラフィック成分を比較分析することで、IPv4とIPv6の利用形態の違いが判明し、IPv6の健全な普及に貢献することができると考えられる。現在、各ISPや事業者においてはNetFlowやsFlowといったフロー技術を用いて、交換されるトラフィックの成分分析が行われている。しかし、これらは一社のデータであり、IXのようなインターネットのコアバックボーンに近い箇所において採取

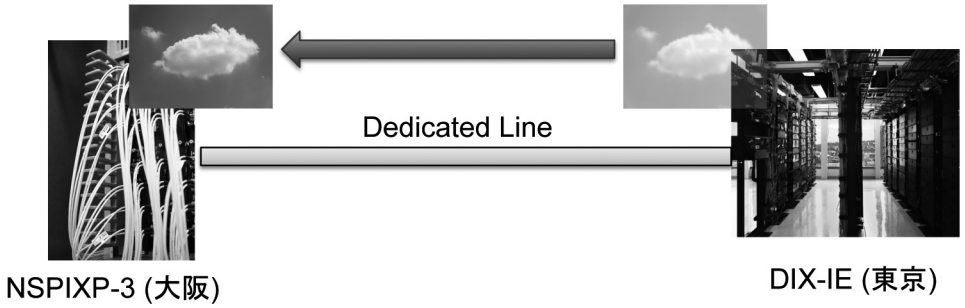

図2.1 広域サービスマイグレーション

したデータを、このような成分分析といった研究に用いている例はほとんど存在しない。商用IXの場合、自身のトラフィックに関するデータを見ることはできるが、プライバシー等の問題から、他社のトラフィックに関するデータを取得することはできず、かつIX事業者自身も研究目的ではないため、複数社のトラフィックを使ったトラフィック成分分析を行う場合は少ない。しかし、DIX-IEならびにNSPIXP-3は研究IXであるため、インターネット全体の発展に貢献するための分析として、複数社のトラフィックデータを用いた成分分析を行なっている。もちろん、トラフィックのプライバシーには十分留意し、どの事業者のどんなユーザのトラフィックなのかは特定できないような分析結果を公表している。

この流れをうけ、DIX-IE, NSPIXP-3では、sFlowを利用したトラフィック成分分析を2011年から開始している。NSPIXP-23も同様、sFlowによるトラフィック収集を行なっている。DIX-IEは2013年5月時点において、すべての拠点にてsFlow データを取得することが可能となったため、2014年は、DIX-IEの全拠点におけるトラフィックデータを用いた、より詳細なIPv4/IPv6トラフィック成分分析を行なった。

図2.2は、KDDI拠点の一部のスイッチにおいて、IPv4とIPv6の単純なトラフィック流量の割合を、sFlowを用いて分析した一例である。

図2.2は、ある拠点の一部の収容ポートにおける、2013年9月20日から2013年9月30日の間のIPv4/IPv6 トラフィック流量である。グラフにおいて緑色にて示される部分が IPv6 トラフィックの帯域である。総トラフィック量の約1割をIPv6トラフィックが占めており、IPv6への以降が確実に進行していることを示す証拠となっている。実際には、それぞれの発信元、宛先ポート番号を見ることでアプリケーション分析を行なっており、IPv4でのアプリケーション利用分布とIPv6でのアプリケーション

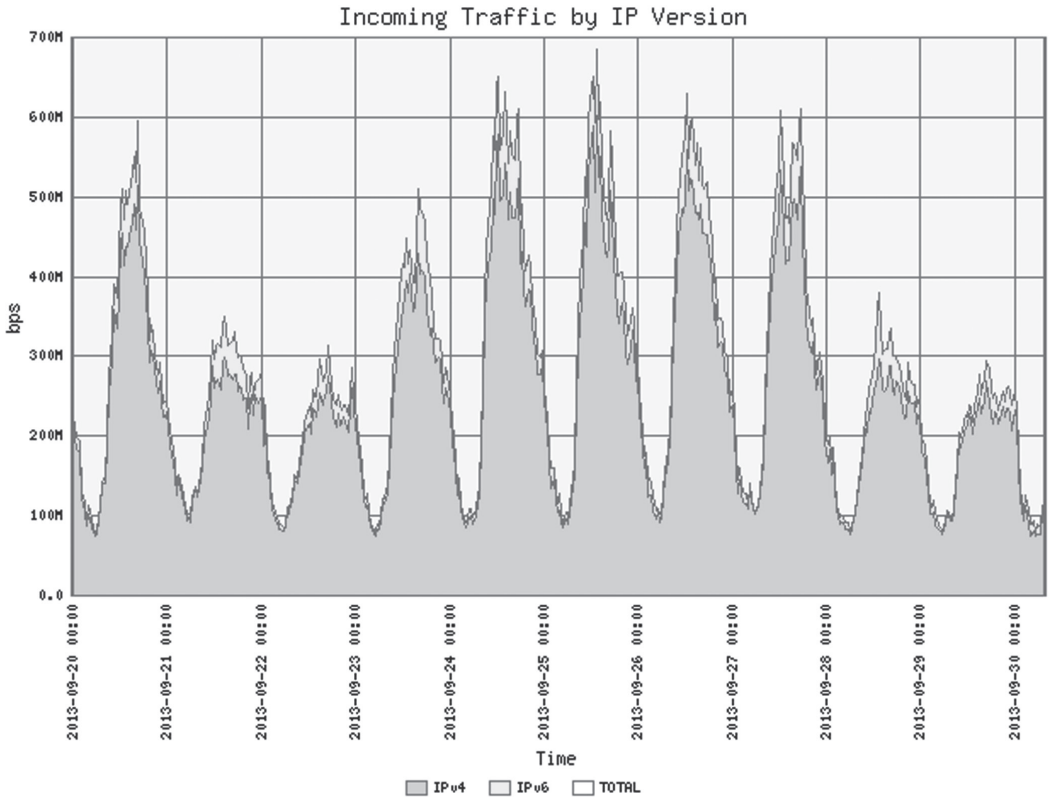

図2.2 IPv4/IPv6 トラフィック成分分析例

利用分布の分析を進めている。2014年も引き続き分析を行い、結果を公表した。

2.3 Software Defined IX の設計検討

現在のIXは、Layer-2もしくはLayer-3においてBGP peeringを行い、経路を交換することでトラフィック交換を行うことが一般的となっている。この際のトラフィック交換の粒度は、あくまでBGPで交換できるプレフィクスが単位となり、IPv4の場合は通常 /24と呼ばれる256個のIPv4アドレスを単位とした制御となる。また、IPv6の場合は通常/48と呼ばれる、2^76個のIPv6アドレスを単位とした制御となる。

さらに、トラフィック制御に用いる指標は、あくまでもIPアドレスであり、それ以外の情報、例えばURIであるとか、ポート番号であるとかいった情報を指標とした広域な経路制御を行うことはできない。これは、インターネットを情報インフラストラクチャとして見た場合には、単純かつ冗長性を確保するために十分な仕組みであるが、より高度なトラフィック制御を行おうと思った場合には、機能が不足する。そのため、BGPを用いたトラフィック制御は限界があり、増加し続けるトラフィックを高度に制御するためには、より柔軟なトラフィック制御手法が求められる。そこでSDNを用いたIX、すなわち Software Defined IXを構築し、様々な指標を使い、かつより詳細な粒度でのトラフィック交換制御ができるIXを構築することを目指す。2013年は、この要求事項と要素技術の検討と検証を行った。これを受け、2014年はより具体的なSDN-IXの実現に向けた実証実験を展開した。

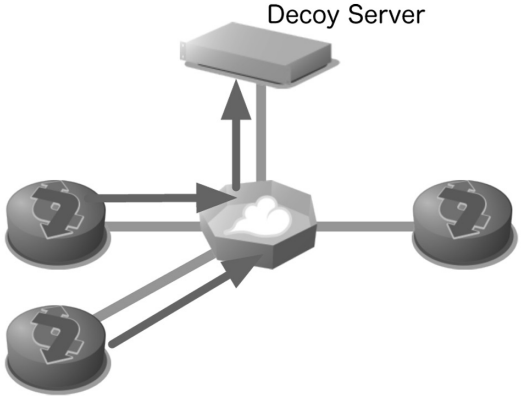

図2.3 DDoS トラフィックの緩和

具体的には、次の4機能を提供するSDN-IXを構築することを2014年の目標とした。

・悪意のあるトラフィックフィルタリング
・悪意のあるトラフィックの緩和
・ASをまたいだQoS保証可能な専有トラフィック交換

これらの機能を有することで、従来のIXでは困難であった、コンテンツに応じたトラフィック制御や、サービス妨害攻撃への効果的な対応が可能となる。

例えば、図2.3に示す通り、トラフィックの内容に応じて囮となるサーバにトラフィックを誘導し、フィルタリングを行なうことで、正しいトラフィックのみをピアリング相手に渡すことや、より詳しいDPI (Deep Packet Inspection)などの技術を適用することも可能となる。これらの機能を、IXが提供することによって、それぞれのISPや事業者が個別に対応するよりも、より連携した、かつ効率的な機能を提供することが可能になる。

さらに、SDN-IXを提供する機器は、従来の機器に比べてかなり安価な機器を使って実現する予定である。これにより、ポート単価を抑えることができ、10Gbpsや40Gbpsのポートを、現在の1Gbpsポートの単価程度にて提供することが可能となる予定である。これにより、他のIXのバックアップ用途としてのIXに用いることができるようになり、非常時のトラフィック交換に用いることができるIXを実現することも目指す。

以上の通り、2014年はSDN-IXの実構築を行い、試験運用を開始した。なお、当初はKDDI大手町拠点、NTT大手町拠点、NTT データ大手町拠点でのSDN-IXを構成した。

第３章　研究成果

本章では、(1) 〜 (3)の各研究項目に関する、研究成果を報告する。

3.1 拠点障害にも対応できるIXならびにサービスアーキテクチャの研究

本年度は、いままでの研究方針に引き続き、広帯域化によるトラフィック増加に対応するための、IX アーキテクチャの研究と運用を通じたその実証を行った。表3.1に、2014年8月時点での、DIX-IE ならびに NSPIXP-3 の実証実験拠点を示す。

耐障害性の観点から言えば、本年度は特に大きな構成変更を伴う作業は行わなかった。しかし、NSPIXP-23の接続性に関して一件大きな障害が発生したため、その障害の回避手法について今後の検討が必要であると思われた。そのため、NSPIXP-23の障害とその原因分析、ならびに障害回避手法の検討を中心に、成果報告を行う。2014年8月時点での、DIX-IE ならびに NSPIXP-23の接続トポロジを図3.1に示す。

表3.1 DIX-IE / NSPIXP-3 実証実験拠点一覧

DIX-IE	KDDI 大手町拠点(WIDE)
	NTT 大手町拠点(NTT Communications)
	NF 西大井拠点(MIND)
	ComSpace-1 拠点(Vectant)
	@Tokyo 拠点(@Tokyo)
NSPIXP-3	NTT 堂島拠点(WIDE)

この図に示す通り、DIX-IEとNSPIXP-23はKDDI大手町拠点の一台のスイッチを用いて接続されている。耐障害性の観点から言えば2回線を2台のスイッチそれぞれに接続し、STP (Spanning Tree Protocol)相当の Layer-2冗長化プロトコルを用いるか、もしくは最近であれば、マルチシャーシリンクアグリゲーションプロトコルを用いた冗長化構成にする手法が考えられる。しかし、東京 = 大阪間の回線はやはり高価であり、常時2回線をアクティブなままとして活かしておくのは実験プロジェクトとしては無理であった。もちろん、東京 = 大阪間の利用帯域が

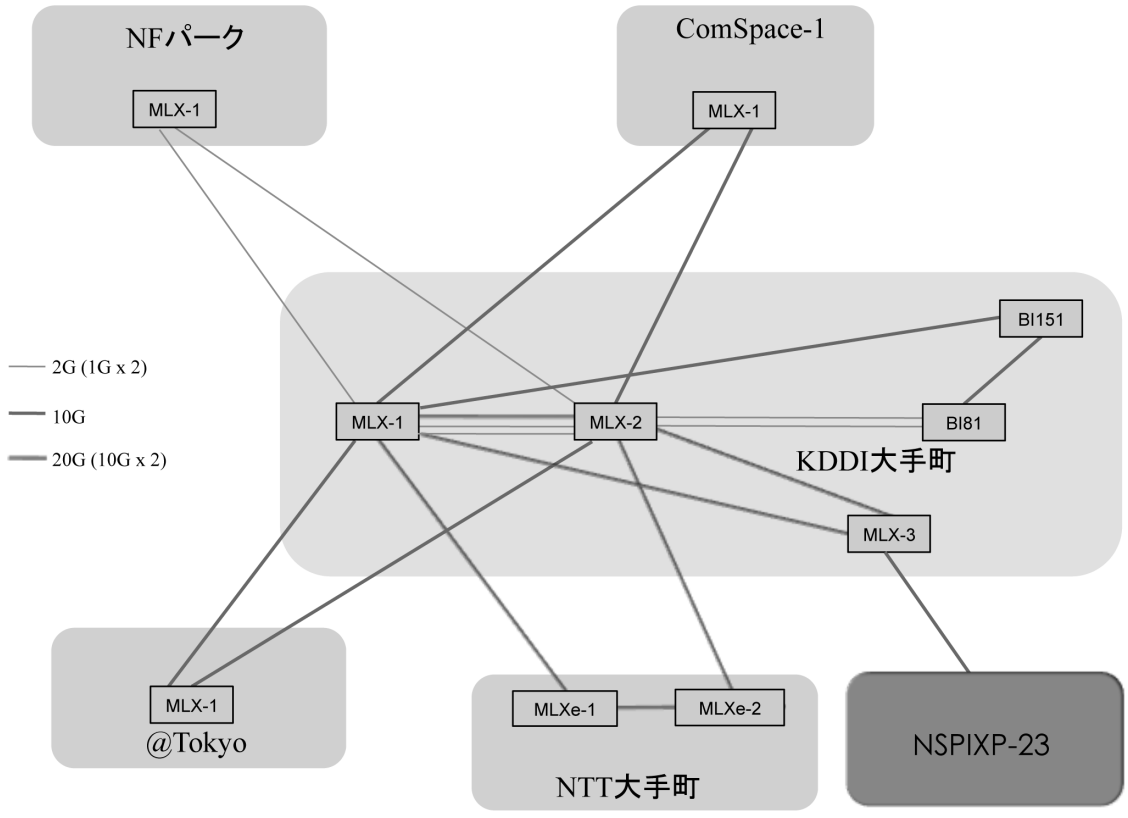

図3.1 DIX-IEならびにNSPIXP-23構成図

増加し、現在の 10GbE 1回線では足りなくなった場合には、2回線に増強してマルチシャーシリンクアグリゲーションを行うのが効率的である。しかし、この場合にも本来ならば冗長性の観点から、実帯域 + 1回線を確保しておく必要があり、3回線確保する必要がある。また、近距離であればDF(ダークファイバ)として回線を調達し、WDM等の光伝送装置を用いることも現実的であるが、東京 = 大阪のような長距離の場合には、回線事業者で無い限り、設備投資的に現実的ではないと判断した。

そこでNSPIXPプロジェクトでは、2回線確保するものの、1回線は通常は別の用途に使用し、NSPIXP-23に利用している回線に障害が発生した場合にのみ、別利用回線をNSPIXP-23利用に瞬時に振り分ける手法に関して、検討を行った。

その結果、リンクの状態監視には従来から用いているEtherOAMを用いたリンク状態監視が有効であるとの結論を得て、NSPIXP-23に用いている回線は、常にEtherOAMによるリンク状態監視を行った。この状態監視によって障害を検知した場合には、回線の切り替えを行うよう構成した。この切替は当然STP等のプロトコルを用いても可能であり、あえてEtherOAMと連携せずとも障害検知と回避が可能である。しかし、東京 = 大阪のような長距離イーサネットにおいてSTPを行うよりかは、EtherOAMによる監視によって切り替えプログラムが発動し、VLAN 設定をばっさりと切り替える、という手法の方が確実であると判断した。実際には、スイッチの VLAN mapping (VLAN 番号変換)機能を用いて、瞬時の切り替えを可能とした。この際、別用途に使っていた回線のトラフィックは、さらに別の経路に迂回されるよう構成した。この迂回に関しては、Layer-3での迂回とLayer-2での迂回が存在した。Layer-3での迂回は、OSPFやBGPの経路切替に従って、バックアップ回線もしくは別経路への自動的なトラフィック迂回となるが、Layer-2での迂回は、VLANの再設定を必要とする。別回線にはNSPIXP-23とは別の利用用途のVLANが複数設定されており、これらVLANを瞬時に移し替え迂回することは、設定上の齟齬やタイミングによる事故が発生しやすいため、迂回にはVXLANを用いることにした。VXLANによるLayer-2の迂回はまだ設計段階で実現できていないため、本年度は設計を述べる。東京と大阪の両端にVLANをVXLANに変換するゲートウェイを設置し、NSPIXP-23のVLAN切り替えが発生した場合に、別用途に利用していた回線に設定されているVLANを全てVXLANゲートウェイに投げることで、設定されているVLAN全ての迂回を可能とした。これは、VXLANに変換してしまえば、UDPのパケットとなるため、Layer-3の迂回さえ正確に行われれば、そのLayer-3の迂回に従ってVXLANパケットが転送されるため、結果としてVLANの迂回が可能となる。

この手法は、本来であればNSPIXP-23自体のVLANにも用いることができる技術であるが、VXLANへの変換を行うにあたっては、いくつかの課題が存在する。

・VXLAN変換へのオーバヘッド
・VXLAN仕様の不一致
・VXLANパケットのフラグメント (断片化)

といった問題である。まず変換オーバヘッドであるが、最近はチップセットレベルでVXLANへの変換をサポートしている製品が登場しているため、ほぼワイヤーレートにてVLANとVXLANの変換が可能となっている。しかし、カプセリング技術であるため、通常のVLANにて通信する場合に比べて、いくぶんかの遅延が増える。また、VXLANの仕様の不一致も問題点となる。これは、VXLANの仕様がまだ固まっていないことにも起因するが、実装上の工夫に任されている部分があるためである。例えば、VXLAN本来の仕様であれば、マルチキャストを用いてFDB(Forwarding Data Base)の情報を交換する仕様となっているが、これを行わずにVXLANをユニキャスト通信を用いたVPNのように用いる実装も存在する。単に2拠点間のVXLANであれば、この実装でも問題なく利用できるが、VLANはイーサネット技術であるため、あるVLANが複数拠点に設定される場合も存在する。その場合は、FDB情報の交換を行わないと、パケット転送が効率的に行えない。さらに、VXLANパケットのフラグメント問題が存在する。例えば、通常の 1500バイトのイーサネットパケットをVLANからVXLANに変換する場合、UDPヘッダ+IPヘッダが余分に付加されるため、その分だけパケットサイズが増大する。イーサネットのMTUを通常値の1500バイトに設定している場合は、1500バイトのVLANパケットをVXLANに変換した場合、VXLANパケットは結果として1500バイトを超える大きさとなってしまう。そのた

め、VXLANゲートウェイにてUDPパケットフラグメントが発生する。すると、受信側のVXLANゲートウェイは、フラグメントされたパケットをリアセンブル(組み立)する必要があり、大きな通信性能劣化につながる。性能が劣化するだけならまだしも、VXLANゲートウェイの中にはフラグメントを行わず、単にMTUを越えたパケットを破棄してしまうものもあり、結果としてうまくVXLANでの通信を行うことができない。これらの注意点が存在するものの、Layer-3の迂回経路に従ってLayer-2通信を迂回できる技術であるVXLANは非常に有用であり、今後もその可能性を検証していく所存である。

3.2 IPv4/IPv6トラフィック成分分析に関する研究

NSPIXPプロジェクトでは、DIX-IE ならびに NSPIXP-3ともに、sflowを用いたトラフィック成分分析を開始している。特に、DIX-IEにおいては全拠点のコアスイッチと参加者収容スイッチの全インタフェースにおいてsflowを有効にし、トラフィック成分情報を収集している。NSPIXP-3においても、NTT堂島拠点のスイッチにおいて、sflowを有効にしている。

sflowを用いたトラフィック成分分析の解析例として、KDDI拠点の一部の収容ポートにおける、2013年9月1日から2014年8月20日までのIPv4/IPv6 トラフィック動向を図3.2に示す。グラフにおいて緑色にて示される部分がIPv6 トラフィックの帯域である。2014年5月以降を境に、IPv6トラフィック増加していることが見てとれる。

さらに、2014年8月1日における、IPv6トラフィックのトランスポートプロトコルと宛先ポート番号による分類を図3.3に示す。この分析結果を見る限り、よく知られているポート番号としては、SMTP(25)、DNS(53)、HTTPS(443)が存在していることがわかる。一方で、それ以外のトラフィックのほとんどは著名なポート番号ではないため、P2Pアプリケーション等のトラフィックが含まれるものと思われる。

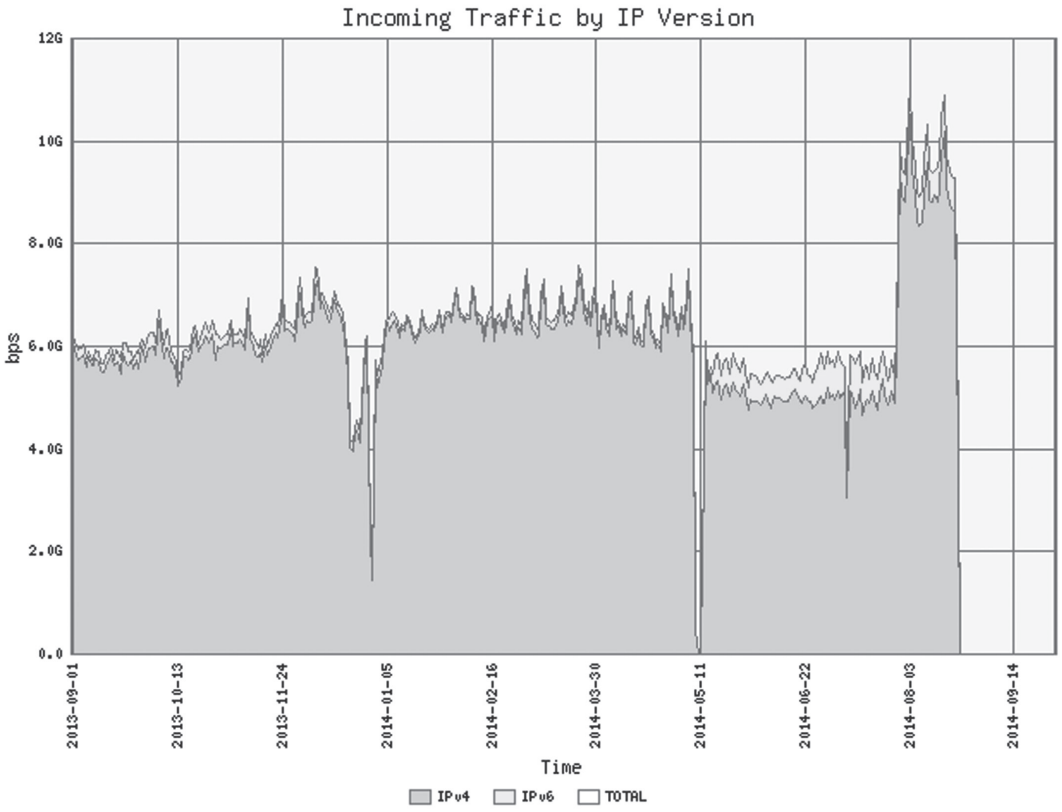

図3.2 KDDI拠点における IPv4/IPv6 トラフィック割合

3.3　Software Defined IX の設計検討

NSPIXPプロジェクトが現在最も力を入れている研究活動のひとつが、SDN-IXの構築である。SDN-IXとは、SDN技術を取り入れたIXのことであり、従来のLayer-3もしくはLayer-2のIXに、SDN技術を用いて付加的な機能を加えたIXを意味する。NSPIXPプロジェクトが目指す、SDN-IXの概念を図3.4に示す。

この図が示す通り、従来のIXに対して

・Granularity
・Security
・Flexibility

の要素を加えたものをSDN-IXと定義する。さらに、SDN-IXは一般的な名称であるため、NSPIXPプロジェクトでは、新たに構築するこのSDN-IXを、PIX-IE (Programmable Internet eXchange In Edo) と名づけた。これは、SDNというとどうしてもOpenFlowのみを思い浮かべる人も多いため、もっと広義な意味におけるSDNであることを意味するため、あえてProgrammable という語句を用いた。この語句が示す通り、回線を収容するネットワーク機器のみならず、周辺に設置する汎用サーバを用いたプログラミングも含め、Programmable IXと定義した。

このPIX-IEは、新たな実験IXとして構築され、運用される。従来のDIX-IEやNSPIXP-3とは性格が異なるIXとして構築、運用されるため、その性格の差異を図3.5に示す。

もちろん、アグレッシブな実験だからといってPIX-IEが

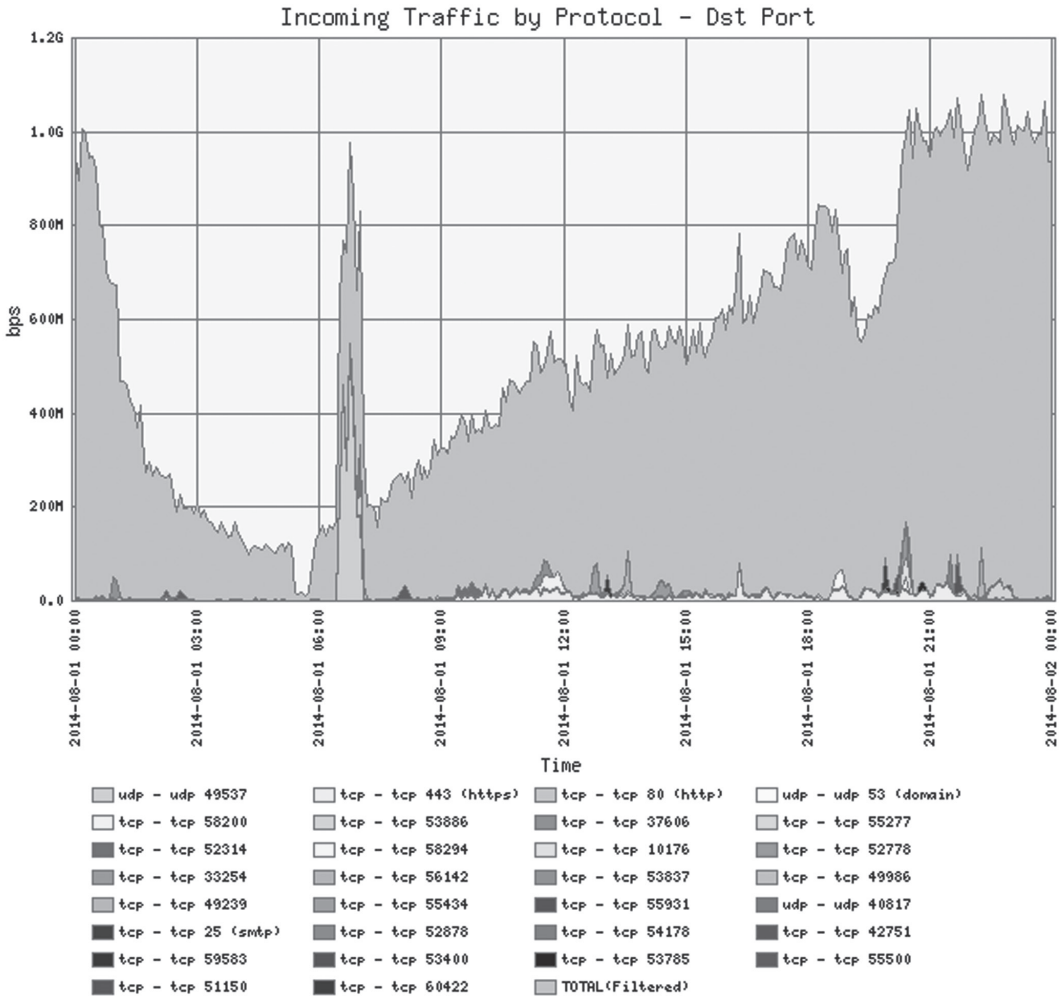

図3.3　8月1日におけるIPv6トラフィックの成分分析

不安定なIXというわけではなく、新たな機能を導入することを恐れず、便利な機能を段階的に搭載し、積極的に実験するIXとなる。そのため、計画メンテナンスの頻度は、従来のIXに比べ多くなる予定である。しかし、なるべく既存の通信に影響を与えず、新たな機能の実験を行えるよう構築・運用する所存である。

PIX-IEが有する、Granularity, Security, Flexibility それぞれの特徴に関し、どのような機能を提供する計画なのか、以下に述べる。

・Granularity

現在のインターネットにおける経路制御はBGPによって行われており、その際のトラフィック制御の最小粒度は、IPv4の場合 /24、IPv6の場合 /48というプレフィクス単位になる。これは粒度としては非常に粗い粒度であり、これがインターネットにおけるトラフィックエンジニアリングを不自由なものとし、経路数の増大の一要因となっている。

そこでPIX-IEでは、より細かな粒度で経路制御をできる機構を提供することを目指す。BGPでの経路制御とともに、SDN技術を用いた経路制御を行うことで、より柔軟な経路制御とトラフィックエンジニアリングを可能とする。もちろん、PIX-IE以外の従来の世界はBGPで経路制御を行っているため、その互換性を確保しつつ細かな粒度の経路制御を目指す。

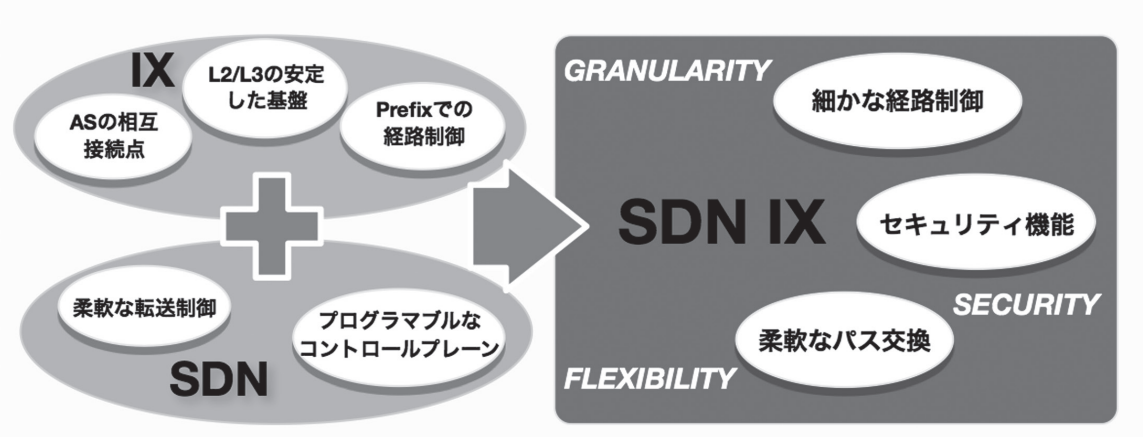

図3.4 SDN-IXの概念

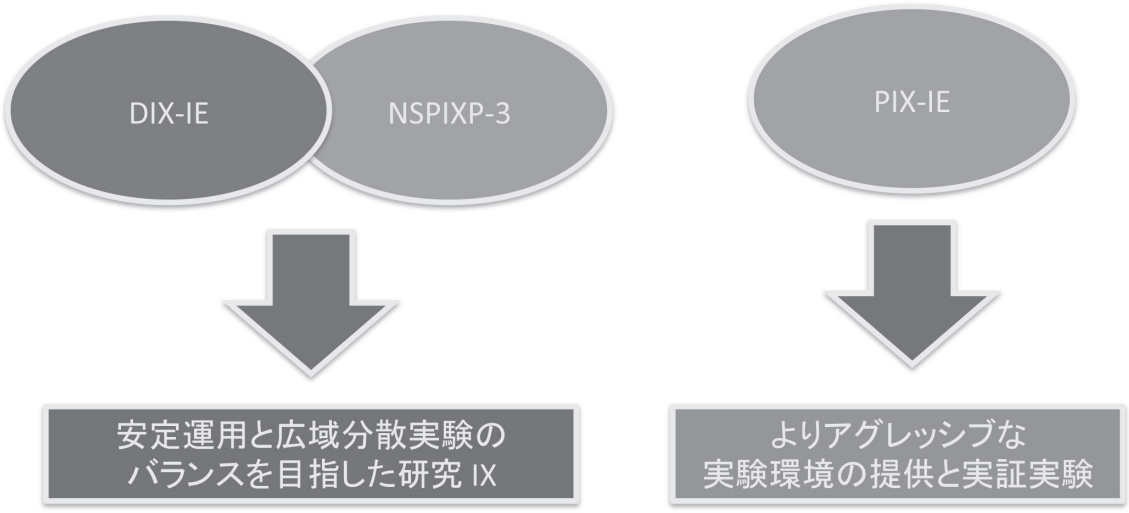

図3.5 従来のIXとPIX-IEの運用方針の差異

・Security

IXにおいてDDoS等のサイバー攻撃を防御するための機構を提供することを目指す。例えばDDoSの場合には、従来のIXの場合では、図3.6に示す通り、IXへの接続回線をDDoSにて埋められてしまった場合には、たとえ組織側に高性能なファイアウォール機器があったとしても役には立たない。回線帯域を埋めることで、正常なサービスを妨害することができるためである。

このような事態が発生した場合、今現在は対処療法的な処置を行うしか防御方法は存在しない。例えばUDPによるDDoSの場合には、図3.7に示す通り、ソースIPア

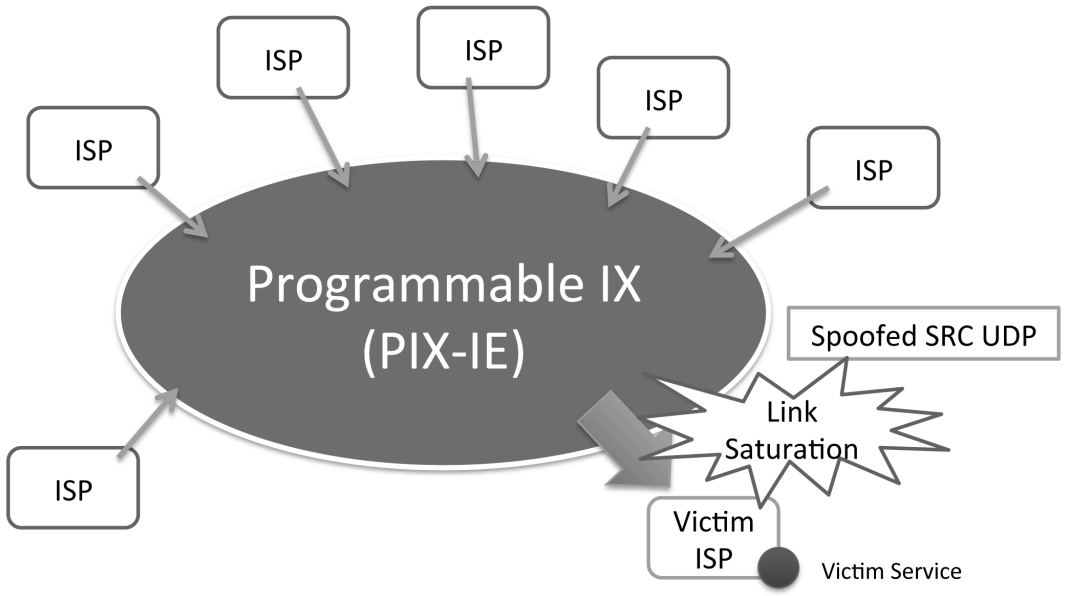

図3.6 IXにおけるDDoS攻撃

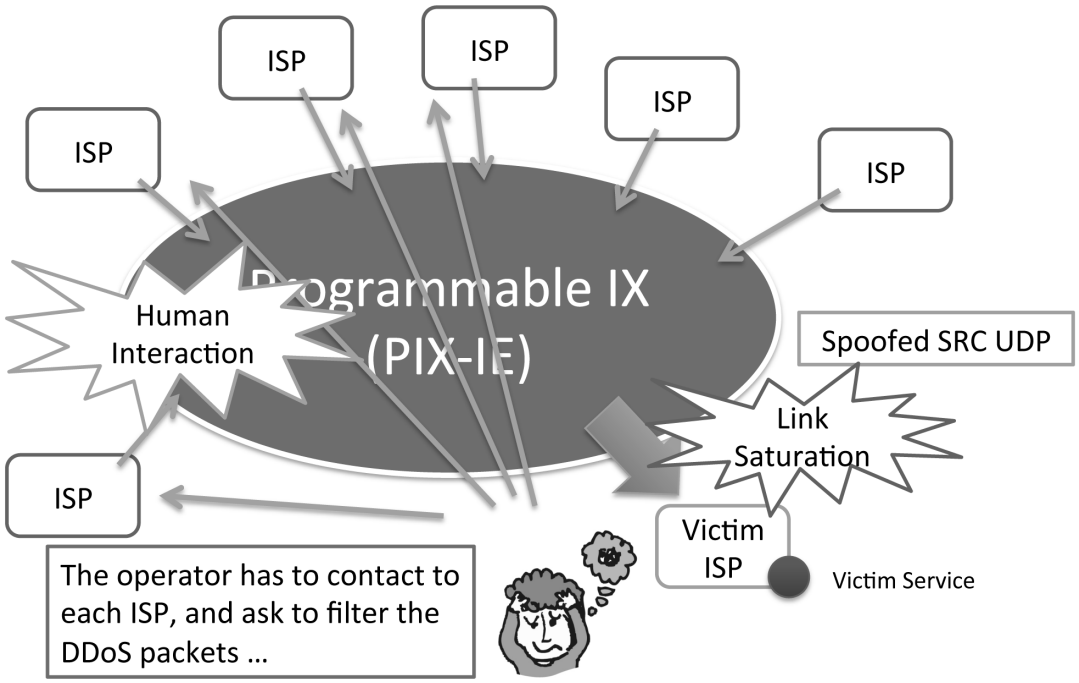

図3.7 DDoSに対する現在の対処療法

ドレスを偽装されたパケットが、どのISP からどれだけ来ているのかを確認し、それぞれのISPにフィルタリングをお願いするのが一般的である。

ところがPIX-IEを用いた場合には、自身が受信するパケットは自身の責任において操作ができるため、攻撃パケットと思われるパケットのみをIXにてドロップすることが可能となる。概念図を図3.8に示す。

さらに高度なパケット操作として、図3.9に示す通り、PIX-IEはパケット処理用のサーバも提供する計画である。このサーバはIntel DPDKやnetmapなどの高速パケット処理技術を適用できるサーバとして構築し、パケットのペイロード部分を見た処理、いわゆるDPI (Deep Packet Inspection) 処理を行うことができる資源を提供する。Intel DPDKやnetmap技術を用いた場合には、ほぼワイヤーレートに近いパケット処理が可能となるため、10G NICを複数搭載したサーバを複数台用意することで、広帯域のDPIを可能とする。

この資源提供により、DNS問い合せにおける特定の名前問い合わせパケットのみをドロップするといった、柔軟な処理が可能となる。また、その処理はプログラミングにて実現するため、参加組織が独自のプログラムを作成し、PIX-IEサーバにアップロードすることでも適用可能となるよう構築する。

・Flexibility

柔軟性に関しては、組織間での柔軟なパス形成機能を提供することを目指す。これは、前述のVLAN VXLAN変換のように、VLAN同士のVLAN番号変換や、VXLANとVLANの相互変換を行うことによって、PIX-IEに接続している組織同士で、Layer-2パスを柔軟に形成させることを目指す。用途としては、例えば組織の顧客同士があるネットワークを相互接続したい、もしくは別クラウド事業者に置いてあるプライベートクラウド同士を連結したい、といった場合に用いることができる。

パス形成例としてのフローを、図3.10に示す。

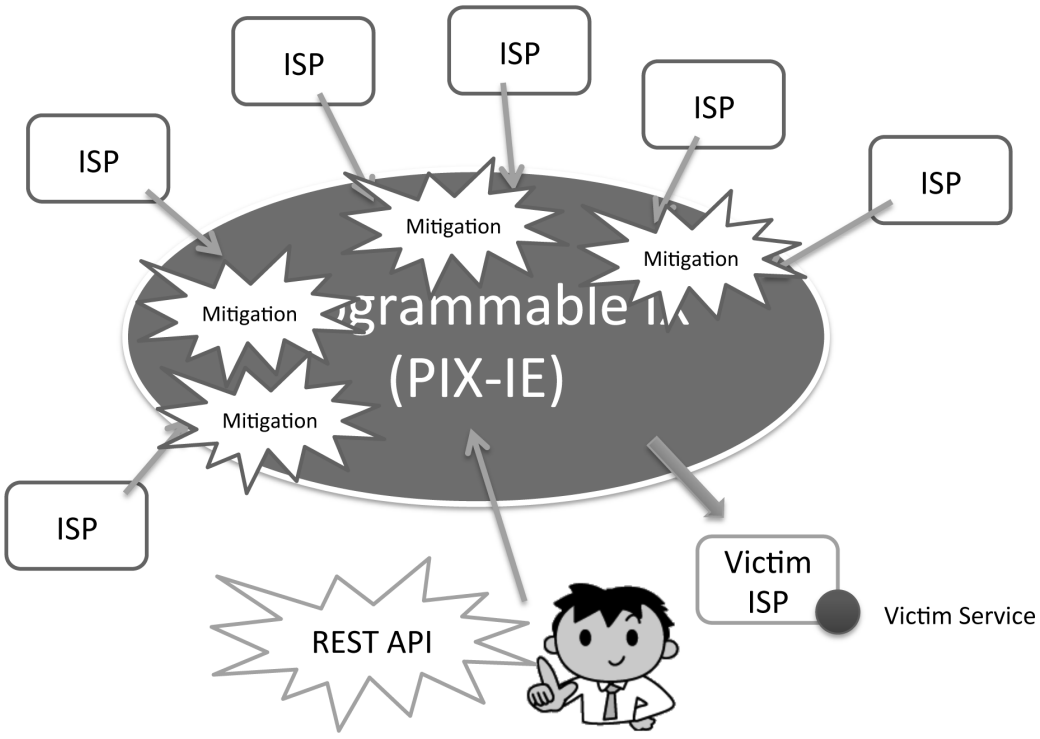

図3.8 SDNを用いたDDoS防御

このように、管理者がそれぞれのポータル画面を用いてパス操作を行うことで、組織間でのLayer-2パスを構成することを可能とする。

以上の通り、本年度は、PIX-IEでまず提供する機能を議論し、具体化することができた。これら機能の一部は既に実装済みであり、パス形成機能に関しては2014年6月に幕張メッセで開催された、Interop Tokyo 2014において、実運用デモンストレーションを行った。図3.11に示す通り、会場内に存在する2 つのASを、大手町に設置したPIX-IEを経由して柔軟なパス制御を行い、会場内に接続性を提供した。この実験では、約70パスが形成され、帯域は最大で7Gbpsほどのトラフィックが交換された。

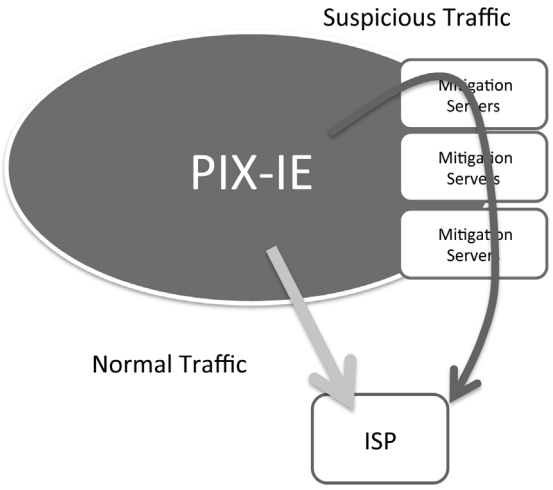

図3.9 Intel DPDK / netmap 技術を用いたDPI

引き続き検証を重ね、KDDI大手町、NTT Communications 大手町、NTT Data 大手町拠点にて、実運用を開始する予定である。

第４章　おわりに

本報告書では2014年に行った、実証実験に関する成果について述べた。これからのISPやエンドユーザに求められる、高度情報インフラストラクチャとしてのIXサービスのありかた、というものを念頭に、より強固なインターネットバックボーンとサービスを実現するための、高度

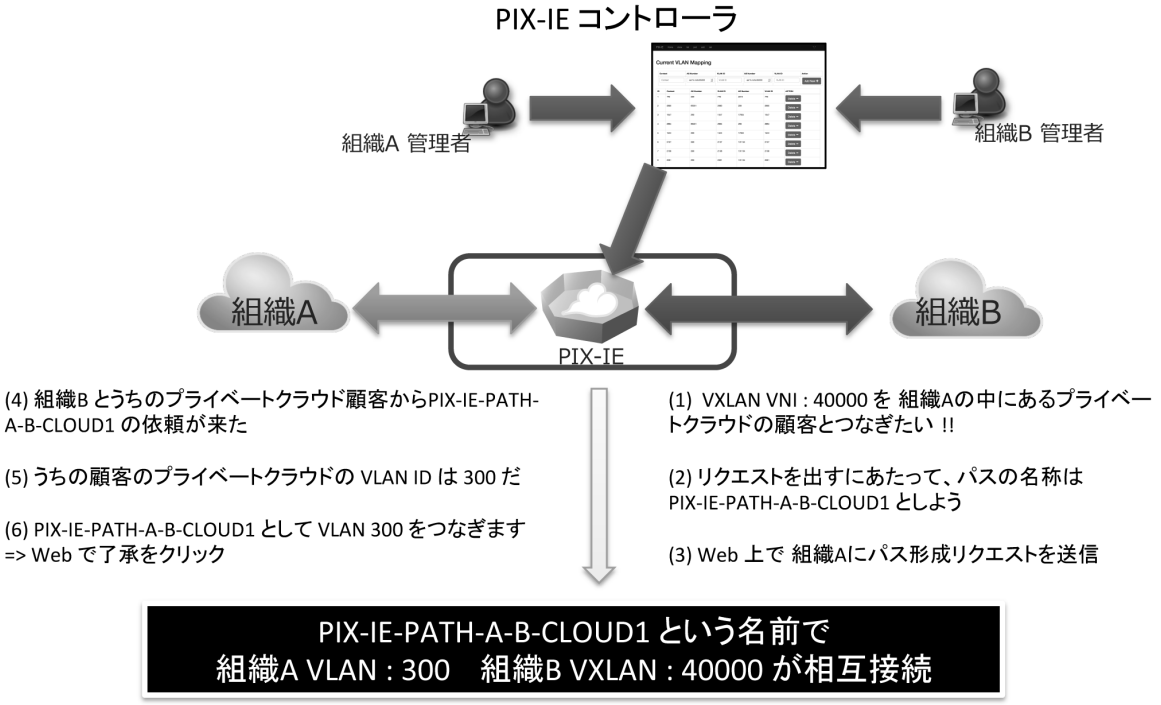

図3.10 PIX-IEを利用した組織間パス形成フロー

な運用技術の研究開発ならびに実証実験を行った。次期以降も引き続きこの方針にて活動していく所存である。

特にPIX-IEに関しては、次期中の試験運用開始を目指し、研究を進める。PIX-IEとして用いる機材は、ファームウェアレベルで柔軟なソフトウェア改造が行える機材、もしくはOpenFlowに適している機材を用いる予定であり、現在機種選定と検証を進めている。今後のスケジュール概要を以下に述べる。

NSPIXP プロジェクトでは、従来のIXとは違う、付加価値を持ったより柔軟なIXの構築を目指すことで、商用IXとは異なった性格の実証実験を推進していく所存である。

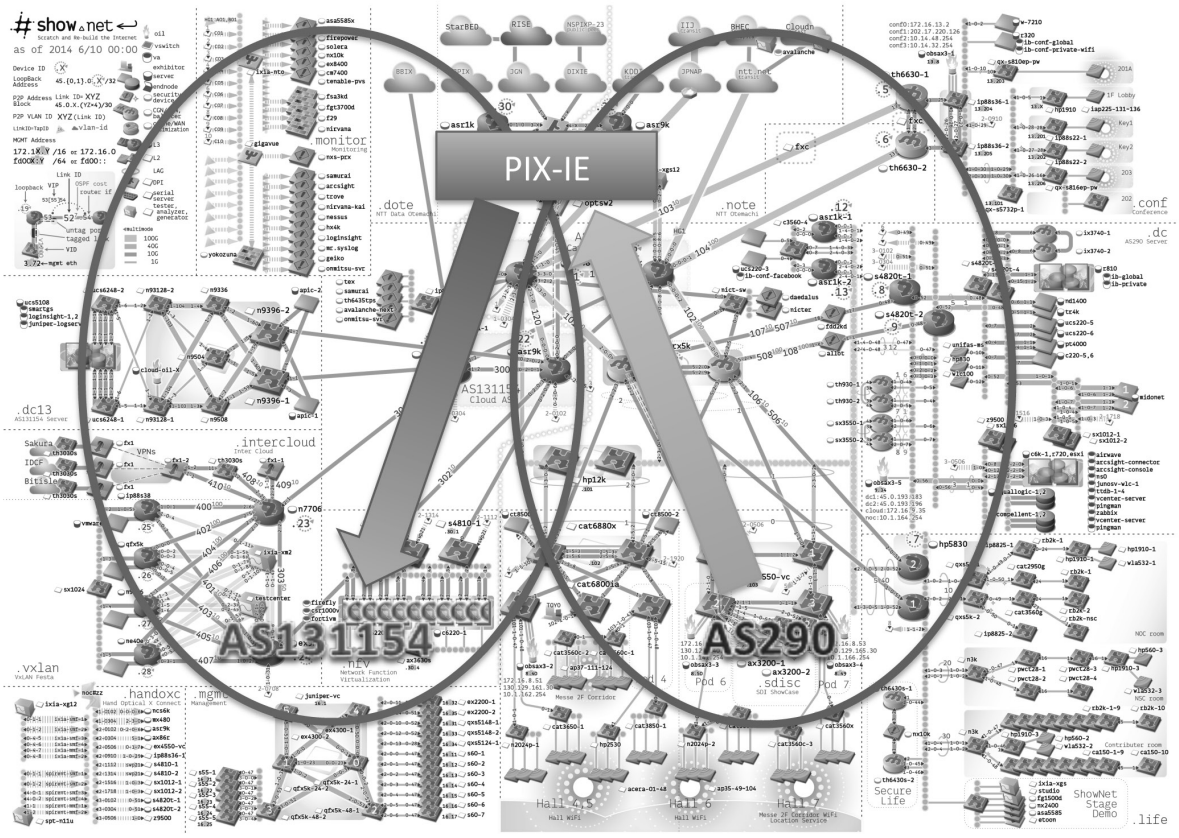

図3.11 Interop Tokyo 2014 における PIX-IE実験