第５部

特集5 ネットワーク相互接続の実証実験

NSPIXP WG

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。特に、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や、スマートフォンのファームウェア更新などによる突発的なトラフィック増大、スマートフォンアプリの流行にともなう時期的なトラフィック増大に対して、トラフィックの輻輳を防ぎ、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手法の検討と検証を行う。また、大規模災害等の障害にも対応できるための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行う。

さらに、特に注力している研究テーマとして、Software Defined Network(SDN)技術のIXへの導入があげられる。SDN技術をIXに導入することにより、トラフィックの柔軟な制御や攻撃を防御するためのセキュリティ機能を提供することができる。本報告書では、特にこのSDN技術を用いた次世代IXである、PIX-IE(Programmable Internet Exchange)の実現を目指した研究活動について述べる。

本研究は、WIDE Projectのサブプロジェクトである Network Service Provider Internet exchange Point(NSPIXP)プロジェクトとして行われている。NSPIXPプロジェクトは、日本初のIXを構築・運用したプロジェクトであり、現在はDIX-IE、NSPIXP-3、NSPIXP-23と呼ばれるIXを運用し、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ている。PIX-IEはこれらのIXに続く、実験的なIXとして構築・運用されている。

本報告書では、第2章にてプロジェクトの背景と現在の構成を述べ、第3章にて本年度の研究計画を述べる。さらに第4章にて、その研究計画に基づいた研究の遂行状況と研究成果を報告し、最後に第5章にてまとめとこれからの展望について述べる。

第２章　プロジェクトの背景と現状

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、現在は、東京エリアに分散配置されたDIX-IEと、大阪に配置されたNSPIXP-3、ならびにこの2つのIXを結合した、NSPIXP-23という3つのIXを運用している。DIX-IE、NSPIXP-3、NSPIXP-23ともにIPv4/IPv6デュアルスタックにて運用されている。さらに、SDN機能を取り入れたIXである、PIX-IE(Programmable Internet eXchange in EDO)の試験運用も平成27年12月に正式に開始された。

表2.1 実証実験拠点一覧

DIX-IE	KDDI 大手町拠点 NTT Communications 大手町拠点 ComSpace-1 拠点 @Tokyo 豊洲拠点 NTT Data 大手町拠点
NSPIXP-3	NTT テレパーク堂島拠点
NSPIXP-23	KDDI 大手町拠点 NTT Communications 大手町拠点 ComSpace-1 拠点 @Tokyo 豊洲拠点 NTT Data 大手町拠点 NTT テレパーク堂島拠点
PIX-IE	KDDI 大手町拠点 NTT Communications 大手町拠点 NTT Data 大手町拠点

表2.1に、平成29年1月時点での、DIX-IE、NSPIXP-3、NSPIXP-23、PIX-IEそれぞれの実証実験拠点を示す。

平成29年1月時点での、DIX-IEならびにNSPIXP-23の接続トポロジを図2.1に示す。

DIX-IEとNSPIXP-3は半商用、半アカデミックな性質を持つIXであり、24時間365日体制での安定した運用を目指している。平成28年は、DIX-IEならびにNSPIXP-3においては、通信に影響を与えるような重大な障害は発生しなかった。

一方、NSPIXP-23は実験的な要素を含む広域IXであり、運用はDIX-IE、NSPIXP-3より実験を重視した体制となっている。平成28年度は、NSPIXP-23においても、数回の計画メンテナンスを除いては通信に影響をあたえるような重大な障害は発生しなかった。長距離区間を利用した広域IXにおいて、冗長回線への切替手法やその切り替えの閾値などは引き続き課題となっている。従来のSTP等の冗長性確保手法ではなく、区間に数か所のスイッチを経由した場合でも区間ごとの冗長性を明示的に担保するための手法が必要とされている。NSPIXP-23は実験的に提供されているIXであり、今後もこれらの課題を改善するために実証実験に取り組んでいく。

第３章　平成28年度の研究計画

NSPIXPプロジェクトでは、新たなIXモデルの形成に関する研究に注力している。従来のIXが担っていたトラフィックの効率的な交換という役割に加え、よりインターネットを安全かつ高信頼なものにするための付加機能をインターネットコアにおいて提供するための研究開発に取り組んでいる。これをふまえて平成28年度当初に

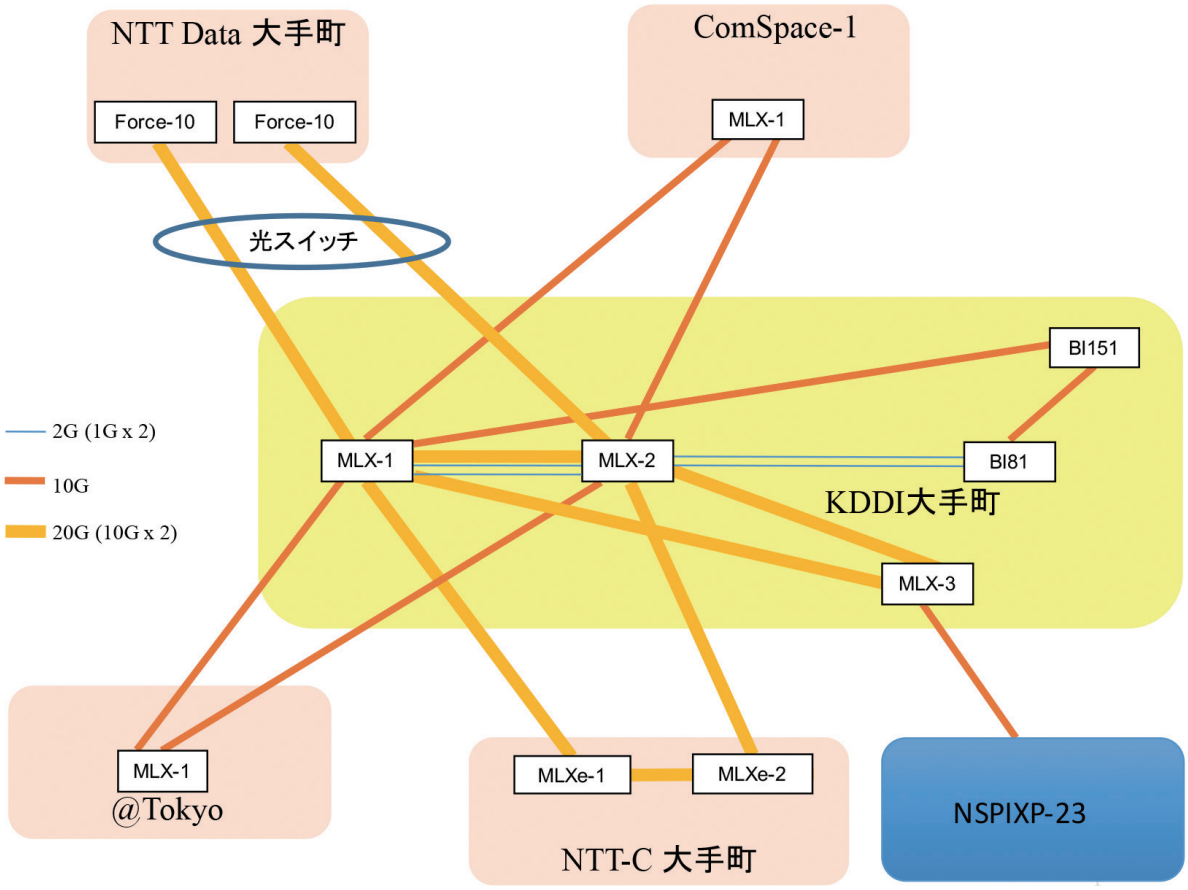

図2.1　DIX-IEならびにNSPIXP-23構成図

示した研究課題について再度まとめる。

3.1 広域におけるSDNを利用したパス制御とトラフィック制御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、平成24年度には、DIX-IEとNSPIXP-3を相互接続する形で、東京と大阪にまたがるLayer-2 IXであるNSPIXP-23を構築し、サービス提供を開始した。平成25年度からは、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の構成をもとに、回線の冗長化と分散拠点のアーキテクチャの組み立て方に関して、検討と検証を行った。IXの冗長のために専用に割り当てられている回線のみならず、通常時は別の用途に利用されている回線を、緊急時には優先してIXトラフィックを交換するための回線として使うための、切り替え技術等を検討し、検証した。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と実験を行った。さらに、実験参加者を募り、東京と大阪両方の拠点にインタフェースを有し、負荷を分散する手法に関して検討を行った。

これらの成果をうけ、平成28年度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、SDN-IXと連携した分散IXアーキテクチャの研究を行う。SDNを用いたIXを実現するためには、SDNにて構成されたパスのサービス品質を関しするための技術(OAM技術)が必須であり、品質監視からのフィードバックを受けて、パスの切り替えを行う必要がある。また、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といった、広域における負荷分散もSDNを用いることで、より柔軟に行える可能性が生まれる。すなわち、従来のBGPによるトラフィック制御のみでは不可能であった、サービスを賄うための基盤としてIXが有効に機能することが可能になると考える。

3.2 SDN技術を用いたIXへの付加機能の提供に関する研究

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PIX-IEでは、経路情報に限らず様々な指標を使い、SDN技術を用いて、BGPより詳細な粒度でのトラフィック制御ができるIXを構築することを目指す。図3.1に、IXに対する付加機能を含んだ、PIX-IEが目指すIXに関する指標を示す。

平成28年度は、より具体的な細かな粒度でのトラフィック制御を実現するためのIXの実現に向けた実証実験と、セキュリティ機能の提供を目指す。細かな粒度によるトラフィック制御の具体例として、本年度は次の二つの機能をPIX-IEに実装することを目指す。

・悪意のあるトラフィックの検知と緩和
・組織間にまたがった柔軟なプライベートパスの構築

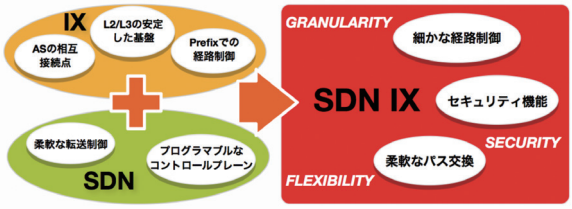

図3.1 PIX-IEの目指す付加機能

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、次に示す通り、悪意を持ったトラフィックの緩和や監視が可能となる。従来のIXでは、図3.2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。

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3.3に示す通り、ソースIPア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。

一方でPIX-IEの場合には、図3.4に示す通り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。

また、図3.5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。

また、IXにおける異常トラフィックの検知技術も、IXにおける攻撃緩和を実現する大きな要素技術となる。そこで平成26年度からは、DIX-IEやNSPIXP-3を流れるトラフィックを元に、ポート番号をベースとした異常検知に関する分析を開始した。その一例を、図3.6に示す。

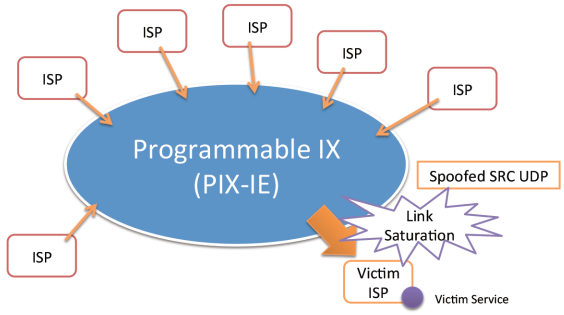

図3.2 DDoS攻撃の例

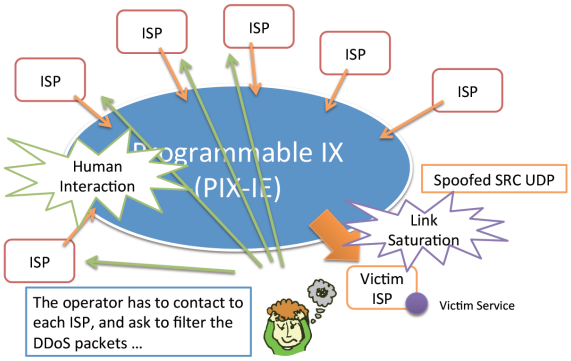

図3.3 DDoS緩和の対処的手法

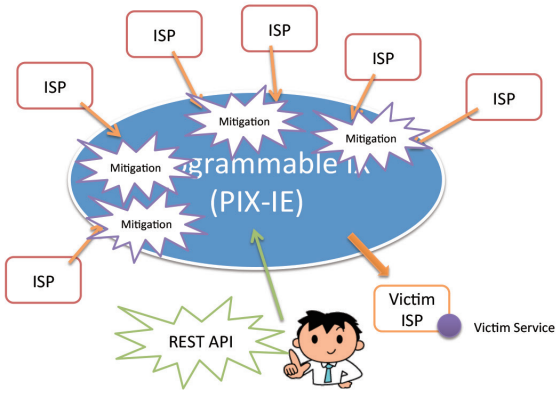

図3.4 PIX-IEにおける攻撃緩和対策

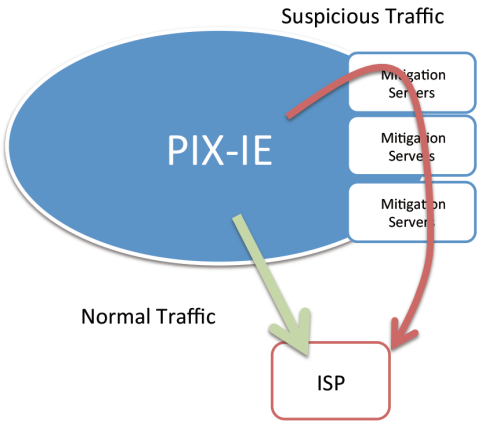

図3.5 囮サーバによる攻撃分析

図3.6は、通信フローのsrc/dstポート番号と、そのトラフィック流量によって円をプロットしたマトリクスである。これは実際に2015年1月5日におけるDIX-IEを流れるデータを用いて作成した。この図にて、左下の赤い円はNTP増幅攻撃を示しているものであり、明らかにIXにおけるトラフィック状況に大きな特異点をもたらしていることがわかる。平成28年度はさらにこの分析を進め、異常トラフィックの動的な検知を可能とするためのシステム設計と構築を行う。

3.3　SDN-IXアーキテクチャの設計と構築

現在のIXは、Layer-2もしくはLayer-3においてBGP peeringを行い、経路情報を交換し、その経路情報に基いてトラフィック交換を行うことが前提となっている。この際、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。

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交換制御は限界があり、より増加し続ける動画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SDN-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。

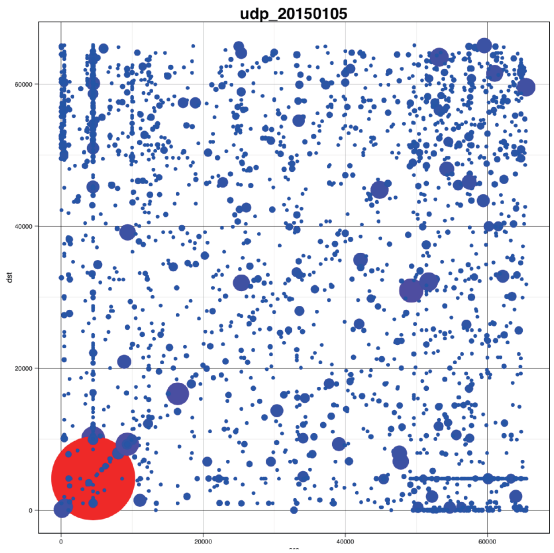

図3.6　ポート番号ベースの異常検知

また、IXはAS間を相互に繋ぐ場として存在しており、IXのポート全体にて特定通信のフィルタリングやQoSを行うことができれば、DDoS等のサービス妨害攻撃を、ASに流入する手前で止めることが可能となる。これにより、各ASの対外接続の帯域が不要なトラフィックに浪費されることを防ぐことができる。しかし、既存のIXに設置されたL2スイッチでは、AS運用者からの要望に合わせてIX内でフィルタリングを行ったり、トラフィック毎の転送制御を行ったりすることができない。そこでSDN技術を用いると、外部のプログラムから動的にトラフィック制御を行うことができ、かつ既存の経路制御プロトコルを上書きする形で、特定のトラフィックだけを制御することが可能となる。これらの利点を生かし、NSPIXPプロジェクトでは、次の3機能を提供するSDN-IXである、PIX-IEを設計、構築することを目指す。

・コンテンツ種別による転送先制御
・悪意のあるトラフィックの緩和
・外部の脅威情報共有機構との連携

これにより、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、より無駄のないトラフィック交換が可能になると考える。

さらに、PIX-IE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としてもPIX-IEを用いることができるようになり、非常時のトラフィックを柔軟に交換するためのIXも実現可能となる。

第４章　研究成果

本章では、4.1 ～ 4.3の各研究項目に関する、研究成果を報告する。

4.1　広域におけるSDNを利用したパス制御とトラフィック制御アーキテクチャの研究

平成28年は、PIX-IEを複数拠点に展開し、複数拠点での運用を開始することを目指した。図4.1に、平成29年1月時点でのPIX-IEの構成を示す。

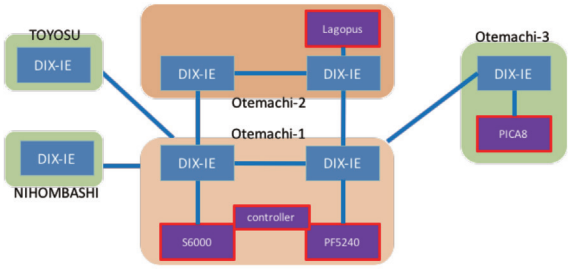

図4.1　PIX-IE構成図

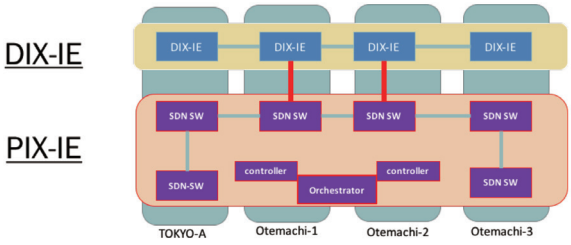

図4.2　PIX-IEが目指す最終形態

現時点でのPIX-IEは、既存のIXであるDIX-IEを利用して構築されている。DIX-IEの拠点間接続を利用し、DIX-IEのVLANを複数PIX-IE用に予約して利用することで、PIX-IEの拠点間接続を実現している。つまり、拠点間におけるパス制御は現在はVLANの番号変換によって実現しており、PIX-IEが本来目指すパス制御とは異なる形式となっている。本来は、PIX-IEスイッチ同士を直接拠点間ファイバにて接続し、トラフィックを制御することによって実現される。しかし、現時点ではDIX-IEの方が主流であり、PIX-IE専用の拠点間ファイバを確保できるまでに至っていない。PIX-IEの参加者が増え、DIX-IEを縮小する段階になれば、PIX-IEの機器同士を専用の拠点間ファイバにて接続する形態に移行する。PIX-IEの最終形態を図4.2に示す。

この構成では、PIX-IEとDIX-IEがそれぞれ別のIXとして構成され、いくつかの拠点にて相互乗り入れを行っている形となる。この場合、やはり耐障害性の観点から、各拠点毎にSDNコントローラが設置され、それを統括するSDNオーケストレータが中心となる拠点に設置される。

平成29年1月現在において、PIX-IEを構成する機器を図4.3に示す。

図に示す通り、旧来のIXに比べ、安価なスイッチ機器にて構成されている。ToR(Top of Rack)と呼ばれる小型スイッチや、PCを利用したソフトウェアスイッチによって

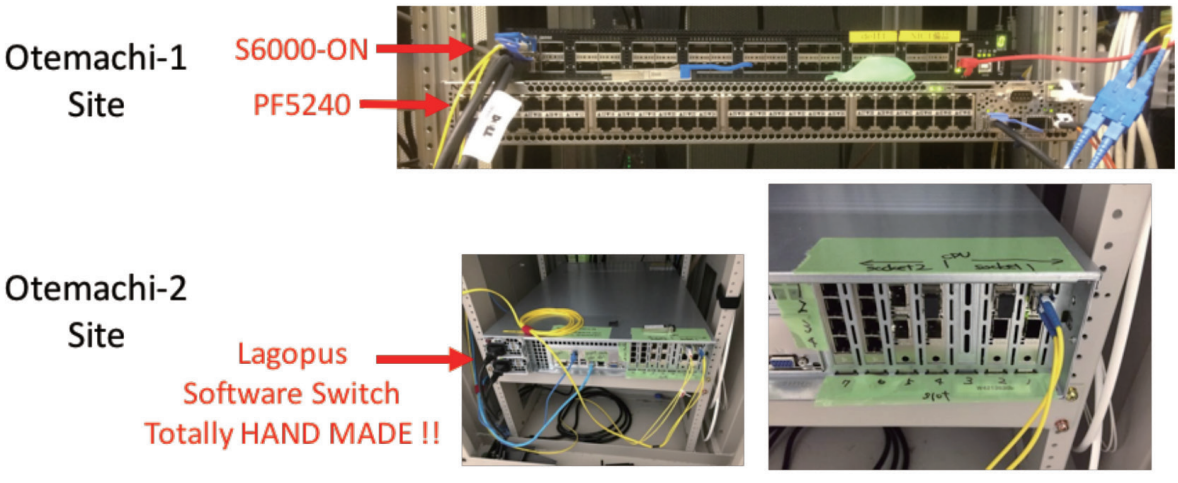

図4.3　PIX-IEを構成する機器

構成されている。これはOpenFlowをサポートしている機器が、このようなToR機器に多いことが理由の一つにあげられる。従来のIXに用いられているBrocadeのようなスイッチにおいてもOpenFlowやSDN機能はサポートされているが、限定的であったりサポートされている仕様が古かったりしており、ToR機器の方がより最新の仕様に従ったOpenFlowを利用可能となっているためである。PIX-IEではOpenFlow 1.3を利用しており、OpenFlowを利用したトラフィック制御を実現している。PIX-IEではOpenFlow以外のSDN機能も利用する予定であり、その観点から最適なOSを選択できるよう、WhiteBoxスイッチと呼ばれるIntelアーキテクチャのCPUを採用したスイッチを利用している。具体的にはDELL社のS6000-ONを利用しており、現在はFTOSと呼ばれるOSを搭載してOpenFlow機能を利用している。しかし、今後PIX-IEが求める機能を実現するにあたってより最適となるOSや手法が提供された場合には、OSを切り替えて利用することも検討している。

現在のPIX-IEを実現する主要なソフトウェアコンポーネントを次に示す。

- Ryu(SDNコントローラ)
- Lagopus(SDNソフトウェアスイッチ)
- IXP Manager(IXPポータルサイト)
- PIX-IEトラフィック制御エンジン
- d4c(DNS DoS Mitigationソフトウェア)
- DORANECO(スレショルドベースDoS検知ソフトウェア)
- Agurim(Multi-Dimensional Flow Aggregation Tool)

これらソフトウェアのうち、上記3つはオープンソースとして開発されているものである。PIX-IEトラフィック制御エンジンは本研究開発にて開発されたものであり、d4c, DORANECO, Agurimはサイバーセキュリティに関連するNECOMAプロジェクトにて開発された成果を利用している。

PIX-IEトラフィック制御エンジンは、PIX-IE参加組織同士の通信をOpenFlowルールを投入することで許可したり、PIX-IEとDIX-IEの相互接続を実現する機能を提供している。PIX-IEの大きな特徴として、既存のIXであるDIX-IEとの相互接続を実現している点があげられる。これは、現在研究プロジェクトとしていくつかのSDN-IXが世界に存在するが、どのSDN-IXも実現していない特徴となっている。既存のL2 IXであるDIX-IEと、OpenFlowで制御されているPIX-IEを相互接続するためには、ARPやNDPなどの近隣探索プロトコルを相互変換する必要がある。これによって既存のL3ルータがOpenFlowに対応せずともPIX-IEに接続したり、DIX-IEに接続されているL3ルータがPIX-IEに接続されているL3ルータと相互通信することが可能となっている。この相互変換の概念図を図4.4に示す。

PIX-IEトラフィック制御エンジンが、ARPやNDPのパケットを代理で中継するプロキシとなり、必要最低限の近隣探索パケットだけを中継することで、ブロードキャストストームなどの事故を防ぎつつ、既存のIXとPIX-IEとの相互接続を可能としている。

また、IXP managerはオープンソースにて開発が進められているソフトウェアであり、IXの管理ポータルサイトを簡易に提供するためのソフトウェアである。PIX-

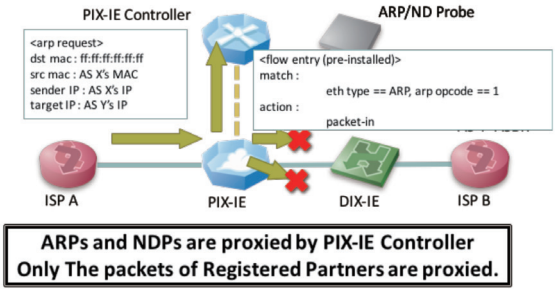

図4.4 PIX-IEトラフィック制御エンジンによる変換

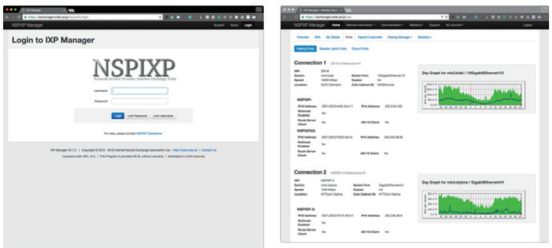

図4.5 IXP managerスクリーンショット

IEではこのIXP managerを改造し、PIX-IE特有の機能を提供するWebインタフェースやコマンドライン・インタフェースを提供することを目指している。DIX-IE、NSPIXP-3、NSPIXP-23、ならびにPIX-IEでは、平成28年7月にIXP managerを参加者に対して提供開始した。IXP managerのスクリーンショットを図4.5に示す。

4.2 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行っている。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。一方でPIX-IEの場合には、OpenFlowを始めとしたSDN機能と、sFlow等のFlowによるトラフィック監視技術の両方を実現できるスイッチ実装は限られており、sFlowに頼らないトラフィック監視技術が必要となる。

特にPIX-IEではセキュリティ機能の一環として、トラフィックを監視して攻撃を発見する機能の提供を目指しているため、sFlowに代わるトラフィック監視技術の実現は急務の課題となる。OpenFlowの機能である、Port StatsやFlow Statsといった機能を利用し定期的に情報を収集することで、従来のSNMPやsFlowが実現していたようなトラフィック監視を実現することは可能である。SNMPが実現しているトラフィック流量の監視だけであれば、Port Statsの機能を利用することでほぼ同様の監視が可能となる。同様にSDNを利用してIXを構築している研究プロジェクトであるTouSIXプロジェクトでは、独自開発したUmbrellaというIXトラフィック制御エンジンの中で、OpenFlowプロトコルによるトラフィック監視

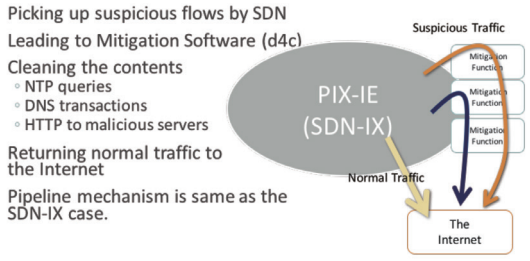

図4.6 トラフィックのサンプリング監視による攻撃防御手法

を実現している。なお、このTouSIXプロジェクトの中心人物であるMarc Bruyere博士は、平成28年11月より来日し、東京大学においてPIX-IEプロジェクトの一員として活動している。

PIX-IEにおけるトラフィック成分の監視に関しては、sFlowに代わる技術として、OpenFlowのFlow Stats技術が利用可能と考えられる。しかし、ポート番号別にFlow情報を統計するためには、ポート番号別のルールをスイッチに投入する必要があり、あまり多くのルールを投入すると監視によるスイッチ負荷が増大してしまう。そこで、OpenFlowルールを用いたサンプリングによるポートミラー機能を実装し、ポートミラー先に解析用ソフトウェアを搭載したPCを接続することで、トラフィック成分分析を行うという手法が考えられる。現在PIX-IEではこの手法を実現すべく、研究開発を行っている。この手法では、図4.6に示す手順にて攻撃トラフィックを発見し、防御することを想定している。

1. パケットサンプリングによるポートミラー
2. ポートミラー先に接続されたPCでフロー情報を収集
3. フロー情報をAgurimならびにDORANECOにて解析
4. 攻撃が疑われるトラフィックのみを抽出し別の物理ポートに出力させるルールを挿入
5. 別の物理ポートに接続されたPCにてd4cを動作させ攻撃トラフィックを浄化
6. 正常なトラフィックのみ通常のパスに戻す

これにより、PIX-IEにてアプリケーション等のトラフィック成分に応じた監視と防御が可能となる。

4.3 SDN-IXアーキテクチャの設計と構築

PIX-IEでは、前述の通りSDN技術を適用し、より安全性と利便性を高めたIXを提供することを目的とした研究開発と実証実験を行っている。しかし一方でOpenFlowに代表される現在のSDN技術はまだその技術自体が熟成されておらず、既存のL2技術に比べると信頼性の点で劣る、もしくは未知数であることは否めない。そこでPIX-IEでは、OpenFlowの技術特性を利用し、対障害性を向上させる工夫を行っている。その一例として、OpenFlowスイッチに投入するOpenFlowルールの階層化があげられる。

図4.7にその実現概要を示す。

図に示す通り、L2 IXとして最低限機能するためのフロールールを優先度を高くして投入し、付加機能であるセキュリティ実現のための監視やフロー誘導のルールは、プライオリティを低くして投入する。OpenFlowスイッチには、その実装による差異も存在するが、コントローラとの通信が切れた場合の挙動を設定できる実装が多い。何らかの障害によってOpenFlowスイッチとコントローラとのコントロールプレーン通信が切断されてしまった場合には、L2 IXとして最低限パケット転送を行うためのルールを残し、他の付加的なルールは破棄する方が安全と考える。そのため、コントローラとの通信が切断されている間は、セキュリティ監視や防御機能は機能しなくなり、新たな機器が接続された場合のARPやNDPのプロキシ等も機能しなくはなるが、L2 IXとしてのパケット転送は実現されているため、トラフィック事故は発生しない。コントローラとの通信が復活した場合には、付加機能を実現するルールを再度OpenFlowスイッチに対して投入することで、セキュリティ監視を実現する。

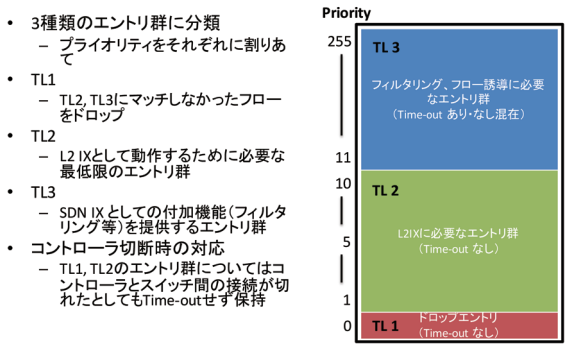

図4.7 フロールールの分類

また、コントローラ単体の障害に備えるべく、コントローラの二重化も検討している。図4.8にその概念図を示す。

図に示す通り、コントローラ自体では何も状態を保持せず、状態はすべてデータベースに保持する設計を目指す。これにより、コントローラはデータベースから情報を取り、その情報に基づいてスイッチにOpenFlowルールを投入するためのインタプリタとしてのみ存在する。この設計であれば、コントローラは最低限の状態保持のみを行い、WebUIでのユーザの操作やセキュリティ監視プログラムからの指示はSDNコントローラではなくデータベースに書き込まれ、コントローラが定期的にデータベースの状態をチェックすることでOpenFlowスイッチに反映する形態となる。もしコントローラに障害が発生し、スタンバイコントローラに制御が移った場合には、OpenFlowスイッチが保持しているフロールールの状態をデータベースから状態を読み込むことで再現し、プライマリコントローラからの制御を引き継いで動作するこ

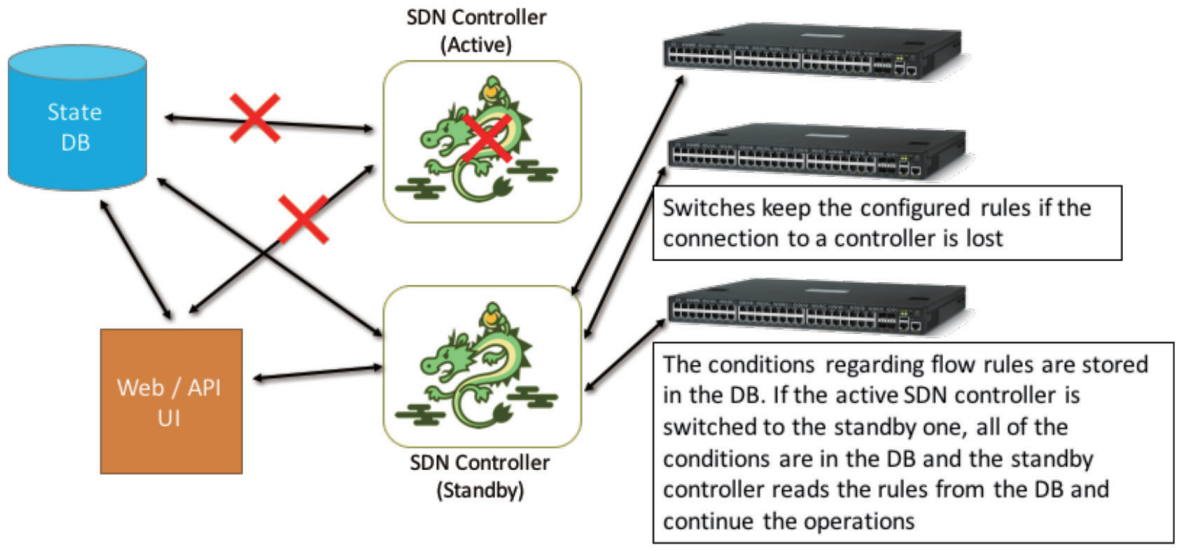

図4.8 PIX-IEにおけるコントローラ冗長化の概念

とを目指す。この冗長性は現在研究開発中であり、完成次第実運用に投入する。

第５章　おわりに

本報告書では、平成28年におけるNSPIXPプロジェクトでの研究開発と実証実験に関して、その成果をまとめた。特にPIX-IEに関して、次世代IXを目指す注力技術として研究開発と実証実験を行った。NSPIXPプロジェクトでは、これからのISPやコンテンツ事業者に求められる、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を常に念頭におき、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、高度な運用技術の研究開発ならびに実証実験を行っていく所存である。

PIX-IEは、引き続き本研究における最重要テーマであり、その実現に関して最優先に取り組んでいく所存である。安定性と機能性、そして安価なコストを実現した次世代IXを、世界規模での運用に発展させることが、NSPIXPプロジェクトの社会貢献であり、存在意義であると考える。

以下に、今後の予定を示す。

平成29年1月～平成29年4月
- PIX-IEにおけるトラフィック成分監視技術の完成
- PIX-IEにおけるフロー情報ベース情報解析の開始
- PIX-IE大阪拠点の試験運用開始

平成29年5月～平成29年7月
- Interop Tokyo 2017における実証実験
- PIX-IEワークショップの開催

平成29年8月～平成29年12月
- PIX-IEにおけるコントローラ冗長化技術の完成
- PIX-IEにおけるDNSパケット攻撃浄化機能の試験提供開始