SDNを利用したIXの設計に関する一検討

岡田　和也†　関谷　勇司††　門林　雄基†

† 奈良先端科学技術大学院大学 情報科学研究科　〒630-0192 奈良県生駒市高山町 8916-5
†† 東京大学 情報基盤センター　〒113-8658 東京都文京区弥生 2-11-16
E-mail: †{kazuya-o,youki-k}@is.naist.jp, ††sekiya@wide.ad.jp

あらまし　SDN (Software Defined Networking) は，コントロールプレーンとデータプレーンの分離により動的なネットワーク構築を可能にする．現在，SDN 技術は，主にデータセンタ，ISP 網内，エンタープライズを対象とした研究開発が行われている．OpenFlow を始めとする SDN 技術を利用することで，柔軟なトラフィック制御，オンデマンドなネットワーク構成の提供ができる．一方で，IX (Internet eXchange) といったドメイン間での SDN 技術の活用は，十分な議論・研究がされていない．本論文では，現在の IX の仕組みとそのトレードオフについて述べ，SDN 技術を利用した IX (Internet eXchange) について検討した．この IX は，SDN の機能を用いて AS 間の動的な転送制御，負荷分散，サイバー脅威に対する防御機能を提供する．また，IX の sFlow データから SDN を用いた IX を実現する上での問題について議論した．

キーワード　SDN, OpenFlow, IX

A Design Consideration for SDN-based Internet eXchange

Kazuya OKADA†, Yuji SEKIYA††, and Youki KADOBAYASHI†

† Graduate School of Information Science, Nara Institute of Science and Technology
Takayama 8916-5, Ikoma, Nara, 630–0192 Japan
†† Information Technology Center, The University of Tokyo
Yayoi 2-11-16, Bunkyo District, Tokyo, 113–8658 Japan
E-mail: †{kazuya-o,youki-k}@is.naist.jp, ††sekiya@wide.ad.jp

Abstract　SDN (Software Defined Networking) is an new network architecture. The technology enables dynamic and flexible network control by programmable control plane. Current SDN solutions and researches are focusing on Data Center Network, Intra-network and Enterprise network. There are a few discussion and consideration of inter-domain network area. In this paper, we consider an IX (Internet eXchange) with SDN technologies. We discuss the features and a concept architecture of the IX. The IX enables dynamic forwarding, traffic load balancing and cyber defense by dynamic configuration. Also, we discuss deployment consideration of the IX with statistic data of a running IX.

Key words　SDN, OpenFlow, IX

1. はじめに

SDN は，コントロールプレーンとデータプレーンを分離し，運用者がプログラムにより経路，フィルタリングの動的な制御を可能にする．昨今，SDN 技術の研究が進み SDN 製品が市場に投入され，商用でも SDN 技術が利用されるようになってきた．しかし，現在の研究や製品は，データセンタ，ISP 網内，エンタープライズといったドメイン内ネットワークを対象としたものが主流である．SDN では，コントロールプレーンの役割を外部のコントローラが担い，プログラムに基づいてスイッチ・ルータを制御する．この際，制御対象の機器は，一つの管理ドメイン内である必要があり，複数の異なる管理ドメインをまたがるような制御が難しい．そのため，IX やドメイン間ネットワークでの SDN 利用は，他の用途と比べて議論・研究が少ない．

IX (Internet eXchange) は，複数の AS (Automonous System) が相互に接続する場を提供し，AS 間のトラフィックを転送する役割を果たしている．IX には，AS 同士をレイヤ 2 で接続するレイヤ 2 方式，IX のルータを介して経路交換を行うレイヤ 3 方式，経路サーバを介して AS 同士で経路を交換するルートサーバ方式がある．各 AS は，境界ルータ間でパスベクトル型の経路制御プロトコルである BGP (Border Gateway

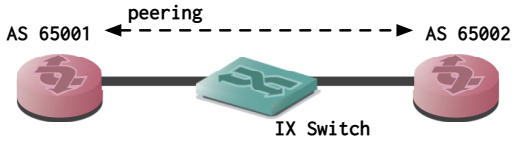


図 1　レイヤ 2-IX 方式

Protocol) により経路を広告，同時に他 AS からの経路を受信し AS 内からインターネットへの接続性を提供している．

経路制御に用いる BGP では，経路制御の最小単位がプレフィックス単位である．しかしながら，AS 間で発生するトラフィック量は，時間単位で大きく変動する．そのため，既存の経路制御では，常に変化する負荷に応じてプレフィックス単位で経路を変更しトラフィックの負荷分散を図ることが難しい．

また，別の問題としてサイバー脅威の増加がある．昨今のサイバー脅威は，DoS/DDoS，マルウェア，フィッシングと多種多様である．サイバー脅威は，複数のドメインにまたがるボットネット，改ざんしたウェブサイト，メールといった様々な手段が用いられる．現在は，個別の組織内のネットワークでファイアウォール，IDS/IPS を用いて悪意のあるトラフィックを検知，フィルタリングしている．しかしながら，マルウェアの感染拡大や DoS/DDoS 攻撃は，他の複数組織から行われるため防ぐことが単一組織だけで防ぐことが困難である．外部からの攻撃に対する AS 境界での防御は，AS 内への攻撃を防ぐことができたとしても，攻撃トラフィックに帯域が消費されてしまうからである．

そこで，本論文では，SDN 技術を用いた IX (SDN-IX) について検討する．SDN-IX は，SDN 技術を用いた IX での柔軟な経路制御と，サイバー脅威に対する防御機能を提供する．また，実際の IX で転送されるパケット数，フロー数を計測し SDN-IX を実現する上での問題点について議論する．

本論文の構成は下記の通りである．まず，2 節に於いて従来の IX の仕組みとその役割について述べる．3 節では，SDN 技術について述べる．4 節では，SDN 技術を用いた IX で提供する機能について述べる．5 節では，SDN-IX の実装について述べる．6 節では，実際の IX におけるフロー数の計測結果を述べる．7 節では，SDN-IX を実現する上での問題点について議論する．8 節で本論文のまとめとする．

2.　IX の仕組み

本章では，従来の IX の仕組みと方式とドメイン間経路制御技術を紹介する．

2.1　IX の機能

レイヤ 2-IX：レイヤ 2-IX は，図 1 に示すように顧客 AS と IX に設置されたレイヤ 2 スイッチにより構成される．IX に接続している AS は，同じ IX に参加している AS と，各 AS の方針に基づいて相互にピアリングを行う．そのため，必ずしも IX に参加している全 AS とピアリングするわけではない．既存の IXP の多くが，レイヤ 2-IX に該当する．

レイヤ 3-IX：レイヤ 3-IX は，図 2 に示すように顧客 AS と

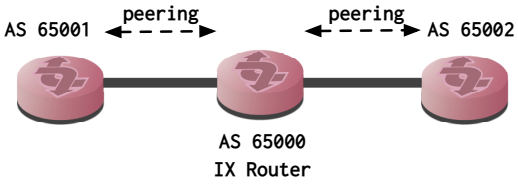


図 2　レイヤ 3-IX 方式

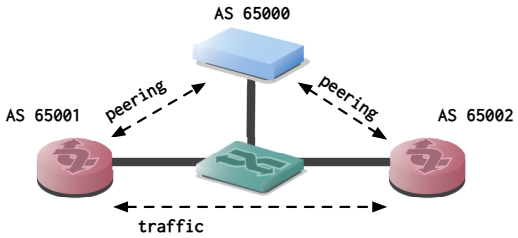


図 3　経路サーバ方式

IX のルータが経路交換を行う．この方式は，レイヤ 2-IX と異なり複数 AS とのピアリング不要となる．各 AS からは，IX がトランジットのように振る舞い，経路交換とトラフィックの中継を行う．

経路サーバ：現在，一部の IX では，図 3 に示すように IX に設置された経路サーバを用いた方式が採用されている．この仕組では，顧客 AS は，直接 AS 間で経路交換せずに IX 側が設置した経路サーバ (Route Server) と経路交換を行う．そのため，この方式では，複数の AS とピアリングが必要なく IX の経路サーバとのみピアリングをするだけでよい．実際のトラフィクは，経路サーバを介して取得した経路を元にボーダルータ間で転送される．経路サーバ方式は，その仕様について IETF の IDR (Inter Domain Routing) 分科会や GROW (Global Routing Operations) 分科会で議論されている [1] [2].

2.2　ドメイン間経路制御

AS 同士のドメイン間経路制御には，BGP が用いられている．BGP では，境界ルータが各 AS の経路をピアリング先 AS と経路交換し，パケットの宛先 IP アドレスに応じて適切な AS へと転送する．転送先 AS は，受信した経路単位で設定した属性情報を元に決定される．また，ピア先への経路広告時には，広告するプレフィックス毎に属性を設定することで，トラフィックの負荷分散，ポリシに合わせたトラフィックの受信を行う．しかし，現在の BGP では，あくまで広告するアドレスブロック単位でしか経路制御ができずフロー単位でコンテンツに合わせた宛先選択ができない．

3.　SDN

3.1　SDN の定義

ONF (Open Networking Foundation) [3] における SDN の定義では，プログラム可能，アジャイル，集中制御，動的な設定，オープンな標準で且つベンダに非依存であることが定義として挙げられている．SDN では，ネットワーク機器から経路制御を行うコントロールプレーンと転送処理を行うデータプレー

ンを分離する．従来は，ネットワーク機器ベンダにより実装された経路制御プログラムを改変することはできなかった．しかし，コントロールプレーンを機器から分離することで利用者が自由に経路制御やフィルタリングを API を介してプログラム可能になる．

3.2 OpenFlow

OpenFlow [4] は，SDN の一つの実現方法でありパケットを制御する機能と転送する機能を分離する．OpenFlow では，コントロールプレーンの機能を OpenFlow コントローラからの制御により OpenFlow スイッチで転送処理を行う．コントローラは，API を用いてパケットが持つ複数の識別子（Src/Dst IP, Src/Dst TCP/UDP port など）の組み合わせ毎にどのような動作（転送，ドロップ，書き換えなど）をするかを決める．OpenFLow スイッチは，受信パケットをコントローラにより設定されたルール（フローエントリ）に基づいた処理を行う．もし，受信パケットに対して適切なフローがスイッチ内のフローテーブルに存在しない場合は，コントローラに該当するルールが存在するかを問い合わせて処理する．OpenFlow の利点は，ネットワークの運用・開発者が API を介して新しい経路制御プロトコル，フィルタリングシステム等を Ruby, C といったプログラミング言語により実装できる点である．現在，OpenFlow の技術仕様は，ONF で策定されており最新の仕様は ver.1.3.2 である．

4. SDN-IX

IX は，AS 間を相互に繋ぐ中間に位置しており，IX でフィルタリングができればサイバー攻撃を AS に流入する手前で止めることができる，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．

しかし，既存の IX に設置された L2 スイッチは，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ができない．前述の SDN 技術は，外部のプログラムから動的に転送制御を行うことができ，且つ既存の経路制御プロトコルと異なる独自の転送制御ができる．そこで，我々は，上記の機能を IX において SDN 技術を用いて実現する方法 (SDN-IX) を検討している．SDN-IX では，IX でフィルタリング，転送制御機能を実現するため，各 AS で既存のネットワーク機器及び構成の変更が不要である．

以下本節では，SDN-IX で提供する機能を述べる．そして，次節で本節で述べた機能を実現する SDN-IX コントローラの概要を説明する．

4.1 SDN-IX の構成

SDN-IX は，図 4 に示すように顧客 AS を収容するスイッチに OpenFlow スイッチを採用する．SDN-IX コントローラは，設定内容を元に OpenFlow スイッチの制御を行う．IX に接続している顧客 AS は，BGP により AS 間での経路交換を行う．各 AS の運用者が，SDN-IX コントローラを介して経路制御，フィルタリング等の設定を投入し制御する．

4.2 SDN-IX の提供機能

SDN 技術を用いて IX で新たに提供する機能として次の 5 機能を検討した．以下では，それぞれの機能について説明する．

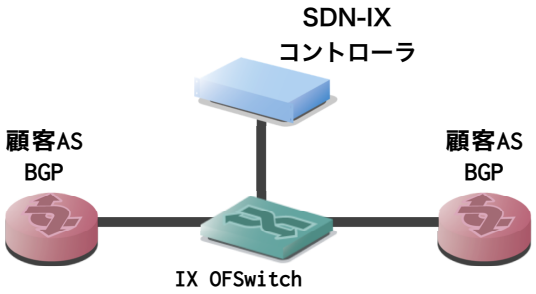


図 4　SDN-IX の構成

- 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フィルタリング
- 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

コンテンツ種別による転送先制御

AS 間のトラフィックは，各 AS が広告している経路情報に基づいて宛先の AS へ転送される．単純には，AS path の長さによって各パケットをどの AS へ転送するかが決定される．そのため，アドレスブロック単位でしか転送先 AS を制御できず，細かなアドレス，コンテンツ種別毎に転送先 AS を変えるなど柔軟な負荷分散が難しい．そこで，SDN-IX では，OpenFlow の制御機能によりパケットのヘッダに含まれる IP アドレス，TCP/UDP ポート番号に基づいて転送先を決定する転送制御を実現する．これにより，帯域を圧迫するような動画，ストリーミングといったトラフィックをその他のトラフィックとは異なる AS へ転送し，トラフィックをの負荷を分散する．

悪意のあるトラフィックフィルタリング

サイバー脅威対策では，主に DoS 攻撃，既知の脆弱性に対する外部からの攻撃を防ぐ目的でネットワーク機器（ルータ，ファイアウォール等）において攻撃元からのパケットをフィルタリングする手法が導入されている．しかしながら，これらの対策は，自 AS 内のネットワークでしか適応できない．そのため，対策を施していない他のネットワークでは，マルウェアの感染といった悪性活動が拡大してしまう．

そこで，SDN-IX では，AS が接続している IX スイッチにおいて，悪性の活動に対して一括でフィルタリング設定を行うことで，SDN-IX の組織への攻撃及び感染の拡大を防ぐ．個別の AS では，対応に差が生じたり，時間差が生じ迅速な対応が取れなくなる．IX での対応では，一括でポリシを強制することができ，迅速に対応できると考える．ただし，効果範囲は，SDN-IX に接続している AS に限られる．

悪意のあるトラフィックの緩和

現在は，DoS/DDoS の緩和 (Mitigation) は，ルータでのフィルタリングや DDoS ミティゲーション専用機器により行われている．これらの機器では，s/netFlow 情報等を元に攻撃を検知し，該当するパケットをトラフィックから除去することで攻撃を緩和している．また，ISP のオペレータが該当するパケットを送信元 IP アドレス，アドレスブロック単位でルータの ACL

により棄却する対策もされている．

SDN-IX では，DoS/DDoS を緩和するために IX 内で攻撃トラフィックを攻撃先に模倣した囮サーバへ誘導し，トラフィック負荷を軽減する機能を実現する．この緩和策の利点は，個々の AS で緩和用の機器を保持する必要がなくなる，もしくは軽減できる点と，攻撃先 AS 内のネットワーク負荷を軽減できる点である．また，攻撃者が IX の接続 AS 内に存在する場合には，上位のネットワークへと転送される前に SDN-IX 内で囮サーバへ転送することで，攻撃先ネットワークまでのトラフィック負荷を軽減できる．既に筆者らは，LISP (Locator/ID Separtion Protocol) を用いた DoS/DDoS の緩和策を提案している [5]．この手法は，LISP のマップサーバに攻撃元からのパケットに対して囮サーバへと誘導するマップエントリにより，攻撃トラフィックのみを囮サーバへと誘導する．

図 5 は，OpenFlow を用いて同等の緩和機能を実現する仕組みを示している．図中では，被害サーバが AS65001 に攻撃元サーバが AS65002 に位置しており，AS 間を IX の OpenFlow スイッチ (OF Switch) により接続している．通常の IX では，正常トラフィックも攻撃トラフィックも全て宛先 AS へと転送される．OpenFlow を用いた緩和手法では， 正常トラッフィクと攻撃トラフィックを別々のフローエントリとして登録することで，異なった転送制御を行う．まず，攻撃元サーバ以外からの正常トラフィックは，宛先のアドレスを広告している AS へと転送される．一方で攻撃元サーバからの攻撃トラフィックに対しては，攻撃元サーバの IP アドレス (AttackerIP) から来たトラフィックを囮サーバへと転送する．これにより，攻撃元サーバからのトラフィックは，全て囮サーバへと誘導され，正常なサーバとそのネットワークに攻撃トラフィックが流入することを防ぐ．また，攻撃者に攻撃対象が囮サーバであることを感知されないように，囮サーバ（IP アドレス:DecoyIP）から攻撃元サーバへのトラフィックは，OF Switch で送信元アドレスを被害サーバの IP アドレス (VictimIP) に書き換えて転送する．攻撃元では，受信したパケットが囮サーバからなのか被害サーバからのパケットなのか判断が難しくなり，この対策に気づかれにくくなる．

図 5 では，IP アドレスの送信元 (src)・宛先 (dst) の組み合わせによる悪意のあるトラフィックの緩和手法を説明した．しかし，ドメイン間では，AS 内で LSN (Large Scale NAT) により複数のホストが一つのグローバルアドレスを変換されている可能性もある．また，特定のポート番号宛のトラフィックを誘導したいといった状況も考えられる．こうした場合，単一の宛先 IP アドレスだけでなく，TCP/UDP ポート番号を利用した誘導も必要である．

外部の脅威情報共有機構との連携

この機能は，SDN の柔軟性を活かし他のサイバー脅威情報共有機構と連携したセキュリティ対策を実施する．サイバー脅威の影響は，単一，少数のネットワークでは対処できないこともある．そこで，SDN-IX は，インターネット上の様々な箇所 (研究組織，セキュリティソフトベンダ等) で観測，検知された脅威情報を AS，IX 間で共有することで攻撃を無力化，局所化する．この機能では，当該 IX にかかわらず複数の拠点で観測，検知されたサイバー脅威情報を標準化された形式で組織間で共有する．そして，共有情報を元に IX では，各 AS の運用者，IX 運用者が前述のフィルタリングや囮サーバへの転送といったセキュリティ対策を施す．また，予め AS 運用者がポリシを設定することで影響範囲の大きい攻撃を自動でフィルタリングするといった防御の自動化も実施できると考える．

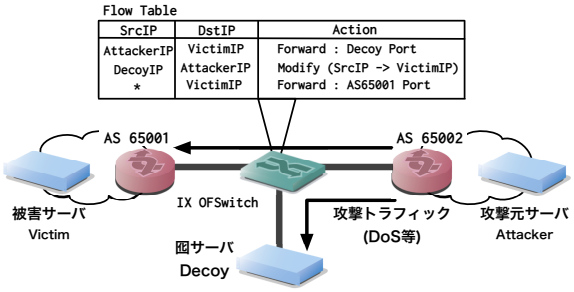


図 5　悪意のあるトラフィックの緩和

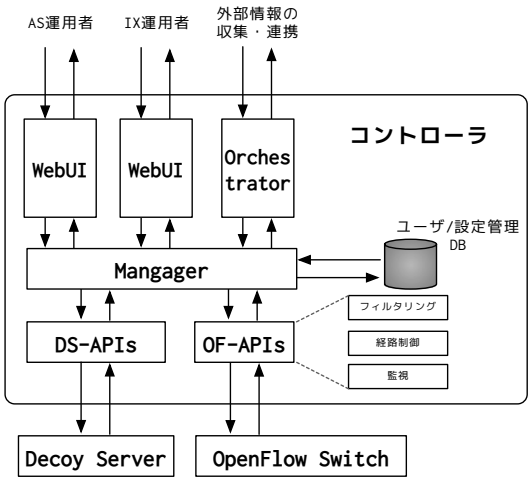


図 6　SDN-IX コントローラの構成

5.　SDN-IX コントローラの概要

本節では，前述の機能群を IX で提供するための SDN-IX コントローラの概要を述べる．図 6 は，SDN-IX コントローラの構成図である．各 AS を収容する IX のスイッチには，OpenFlow に対応したスイッチを導入することを想定し，SDN-IX コントローラを介してフローテーブルを制御する．以下では，各構成要素について説明する．

AS 運用者用 WebUI

AS 運用者用 WebUI は，SDN-IX に参加している各 AS 運用担当者が，自 AS の方針にもとづいてフィルタリング，経路制御を設定できるようにする．設定では，OpenFlow で制御可能なフロー識別子を組み合わせてフロー毎に転送先 AS の設定，フィルタリングを設定する．

IX 運用者用 WebUI

IX 運用者用 WebUI は，SDN-IX 全体の運用管理・監視を行うための UI であり，各事業者が設定している設定内容の把握，OpenFlow スイッチの状態監視を行う．

オーケストレータ（外部システム連携用）

現在，様々なサイバー脅威情報が各国の CERT，学術組織，有志によりオンラインで共有されている．例えば，PhishTank [6] は，フィッシングサイトの URL，運用されているネットワーク情報が提供されている．また，ポーランドの CERT Polska の n6 [7] では，広域で収集したサイバー脅威情報を一元管理し，利用者に json 形式で配信する試みがされている．この配信情報は，インシデント毎に分けれらており，ボットネット，DoS 送信元の IP アドレス情報などが含まれている．オーケストレータは，こうした外部のサイバー脅威解析・情報共有基盤からサイバー脅威情報を受信し，AS 運用者，IX 運用者に脅威情報を提示する．AS 運用者は，提示された脅威情報を元に SDN-IX に必要な対策を設定する．

マネージャ

マネージャは，各事業者の設定をデータベースで管理し，投入された設定を OpenFlow スイッチ用 API を介して OF スイッチに反映する．また，AS の経路情報，設定情報を元に投入された設定が，他の AS に影響を与えないように設定の排他制御を行う．

ユーザ・設定管理用 DB

このデータベースでは，運用者のログイン情報，各 AS が広告している経路情報，各 AS の設定情報を管理する．経路情報は，BGP (Border Gateway Protocol) により各 AS から広告されている経路情報を把握し登録する．このため，IX では，経路情報を収集するための経路サーバを用意し，IX の参加組織と経路を交換し経路情報を集める．この情報を元にマネージャは，各 AS が自 AS の経路に該当するフローのみを正しく設定しているか管理し，投入された設定が他の AS の通信に影響を与えないかを把握し，排他制御を行う．

OpenFlow スイッチ用 API (OF-APIs)

OpenFlow スイッチ用 API では，OpenFlow スイッチに対してフィルタリング，経路制御及び監視・計測を行う機能を提供する．フィルタリング API では，パケットの送信元，宛先のアドレス及びポート番号を組み合わせたフィルタリング設定を行う．経路制御 API では，パケット種別（ポート番号）による転送先 AS への経路を設定できるようにする．また，監視・計測 API では，OpenFlow スイッチから SDN-IX の運用に必要な各フィルタリングルール毎のルール適用回数，トラフィック流量，障害情報（リンクダウン等），フローテーブルサイズといった情報を取得する．

囮サーバ用 API (DS-APIs)

囮サーバ用 API は，攻撃トラフィックを囮サーバに誘導するために囮サーバの立ち上げ，破棄，サーバ設定に必要な API を提供する．囮サーバは，各 AS が IX 内に設置したサーバ内で仮想サーバ環境を構築し，囮サーバ用の仮想マシンを立ち上げる，具体的には，OpenStack や CloudStack といった CMS (Cloud Management System) 環境を利用し，API 経由でマシンの作成・削除，ネットワーク設定を投入する．攻撃を受けている AS の運用者は，攻撃対象のコンテンツをホストしているサーバイメージを各サーバにアップロードし起動する．そして，コントローラから攻撃トラフィックを誘導するフローエントリを登録し，該当のサーバへと誘導し攻撃を緩和する．攻撃が終了した後は，フローエントリとサーバからイメージを削除し，誘導を止める．ただし，ホスティングサービスのように AS の運用者とコンテンツの運用者が一致しない場合も想定される．この場合は，攻撃を受けているコンテンツ運用者からの攻撃緩和要求に基づいて AS 運用者が設定を代行する仕組みが必要である．

6. IX におけるフロー数解析

SDN-IX では，OpenFlow スイッチを介して AS 間のトラフィックを制御する．OpenFlow では，OpenFlow スイッチが持つフローテーブルにコントローラがフロー単位の振る舞いをフローエントリとして記述する．したがって，転送制御やフィルタリングの最大設定数は，フローテーブルの容量に依存する．IX では，複数の AS 間で多量のパケットが転送されており，フィルタリングや転送制御の粒度（IP アドレスの範囲，TCP/UDP ポート番号の範囲等）が細かければ，多量のフローエントリを OpenFlow スイッチに設定しなければならない．そこで，IX における制御対象のフローの大きさを，実際の IX での単位時間当たりのフロー数を sFlow の計測結果から見積る．

6.1 データ収集方法

トラフィックデータは，分散型レイヤ 2IX である DIXIE のトラフィクを IX スイッチの全ポートから sFlow により，通信の秘匿性を確保した状態で，本提案手法の評価のために 24 時間分のデータを用いた．sFlow のサンプリングレートは，8192 である．

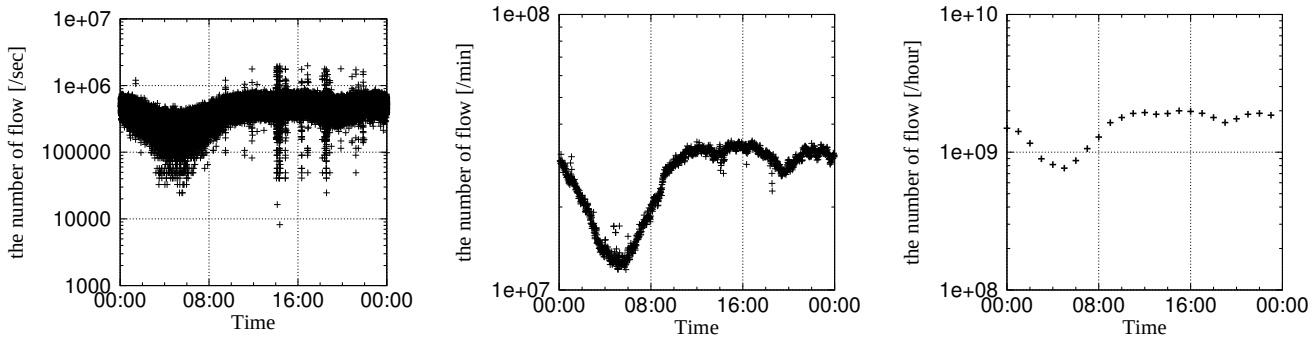
6.2 解 析 結 果

図 7 は，毎秒，毎分，毎時単位の総パケット数（近似）の時間変化をグラフ化したものである．パケット数は，各単位時間毎のサンプリングパケット数を求め，それにサンプリングレートの 8192 を乗ずることで得た近似した総パケット数である．図 8 は，sflow でサンプリングされた単位時間当たりのパケット数の中に含まれる TCP パケットの割合から，毎秒，毎分，毎時単位の TCP フロー数の時間変化をグラフ化したものである．フローは，単位時間内で Src IP, Dst IP, Src TCP Port, Dst TCP Port が共通するものを単一フローと識別し計算した．この結果，DIXIE における TCP フロー数は，毎秒で約 1000〜100 万，毎分で約 1,000 万〜3,000 万，毎時で約 6,000 万〜1 億 1,000 万フローで推移している．

7. 議　　論

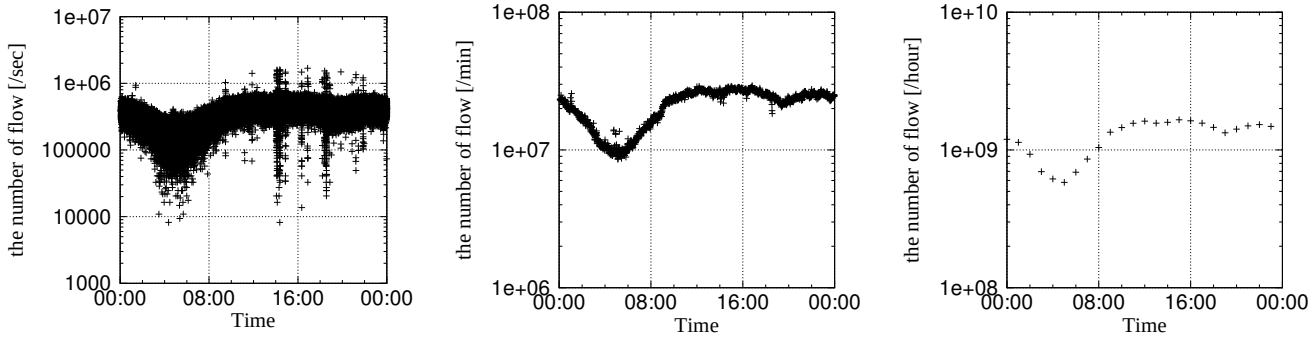
7.1 AS 間の分離

IX では，複数の AS が一つもしくは複数のスイッチに接続されて相互に通信を行う．SDN-IX では，さらにスイッチの設定を各 AS の運用者が設定する．そのため，AS 運用者の設定内容や間違いが他の AS の通信へ影響する可能性がある．具体的には，AS の運用者が自 AS から広告していない他 AS のアドレスに対してフローを設定すると他 AS の通信が影響を受けてしまう．SDN-IX 側では，それぞれの AS がどの経路を広告し



[1] 毎秒　　[2] 毎分　　[3] 毎時

図 7　IX における総パケット数（近似値）



[1] 毎秒　　[2] 毎分　　[3] 毎時

図 8　TCP フロー数（近似値）

ているかを把握し，各 AS 運用者の設定内容が適切であるかどうかを判断しなければならない．

7.2　フローテーブルの容量

OpenFlow は，設定したルール毎にスイッチ内のフローテーブルにエントリを設定する．データセンタ内など特定の組織内で行われる通信では，制御内容にもよるが単一ドメイン内で且つ通信が予測しやすくにフロー数が限定される．しかし，SDN-IX では，AS に接続している利用者の通信を扱うため，IP アドレスだけに限っても多量でありフロー数を事前に見積もることが困難である．既存の OpenFlow スイッチでは，フローテーブルの容量がハードウェアの制限から数万から数十万エントリ程度である．したがって，IX で転送されるトラフィックに対するフィルリング，転送制御は，フローテーブルの容量により制限される．

SDN-IX スイッチのフローテーブルは，大きく分けて AS 間の通常トラフィックの転送，攻撃フィルタリング，コンテンツ単位の転送用のエントリから構成される．通常の AS 間の転送処理に必要なテーブル数は，IX のスイッチがレイヤ 2 スイッチとして機能すれば良いため，MAC テーブルと同程度の数を確保できればよい．残りの 2 種類のエントリは，各処理で制御するフロー数に依存する．図 8 より毎分でのフロー数は，約 1,000 万〜3,000 万フローである．そのため，個別のフロー単位でフィルタリング・転送制御は，フローテーブル容量を大きく越えてしまう．ArborNetworks のレポートでは，DDoS 攻撃の 65%が 30 分以内である [8]．そのため，一つの攻撃を緩和するために必要なフローエントリの占有時間は，比較的短い時間ですむ．攻撃開始と収束を検知できれば，攻撃の発生期間のみ緩和でき且つフローテーブルを浪費しなくてすむ．攻撃パケットの破棄・転送，コンテンツ単位の転送制御は，送信元・宛先アドレスの組み合わせに限らず，TCP/UDP ポート番号も考慮したフローエントリが必要となる．そのため，単純にエントリを追加していくだけでは，フローテーブルを消費していくため，送信元・宛先で共通する部分を定期的にエントリをまとめあげるといった工夫が必要である．制御対象をアドレスブロック単位（例，192.168.0.0/24）で設定などの工夫によりテーブルの消費を抑制することができる．

また，フローテーブルに全ての転送処理を記述するのではなく，OpenFlow で処理（パケットの棄却，通常と異なる宛先への転送，パケットの書き換え）が必要なパケット以外は，通常の MAC テーブルを用いて転送しフローテーブルを削減するといった対策が必要である．こうした議論は，IETF の l2rs 分科会 [9] でも行われており，今後ハイブリッドな SDN 製品が出てくることが期待される．しかしながら，上記のようなテーブルを分離したハードウェアであったとしてもフローテーブルの容

量に限界があるため，負荷分散の経路制御やフィルタリングを追加していくとフローテーブルが溢れてしまう可能性がある．現在の OpenFlow の仕様 (ver.1.3.2) では，プレフィックス単位 (192.168.0.0/24 など) でのフローエントリを記述することができるが，実際にスイッチ側のフローテーブルに登録される際には，アドレス単位で登録されてしまいフローテーブルを浪費してしまう．そのため，SDN-IX では，実際に運用上どの程度のフローが必要となり，AS の接続数の限度がどの程度であるかを実装と共に評価しなければならない．

7.3 コントローラの処理能力

sFlow の解析結果からも分かる通り，TCP フローに限定しても数秒単位で膨大なフローが発生する．実際には，フロー毎に継続する時間に長短があるため単位時間あたりで発生する新規のフローは少なくなるがそれでも膨大である．そのため，SDN-IX のスイッチでは，受信したパケットに応じて SDN-IX コントローラへ packt_in により多量に問い合わせが発生する可能性がある．したがって，SDN-IX コントローラには，時事刻々と発生するフローに対する処理可能な能力が求められる．この問題の対策としては，複数のコントローラ用サーバを設け新規フローに対する処理の負荷分散を図る方法が考えられる．また，コントローラ側に設定されたルールをスイッチからの問い合わせ前に，フローテーブルに登録する方法も考えられる．しかしながら，この方法では，ルールに該当しないトラフィック転送されていたとしてもフローテーブルにエントリが登録される．事前にフローテーブルに登録する方法では，必要のないエントリによりフローテーブルが消費されてしまう可能性が大きい．分散コントローラで処理する場合は，一貫性を保つためにコントローラ間で設定内容の同期が必要となる．また，コントローラへの問い合わせを処理するには，コントローラ台数がどの程度必要になるか検討する必要がある．

8. おわりに

SDN 技術は，データセンタ，ISP 網内，企業内ネットワークでの応用が検討されている．一方で，AS 間の相互接続を行う IX において SDN の応用については，あまり議論がなされていない．本論文は，SDN 技術を利用した IX について検討・議論を行った．SDN 技術の一つである OpenFlow を IX で用いたフロー単位の粒度での動的な経路制御・負荷分散，悪意のある攻撃のフィルタリング・緩和を検討した．また，実際の IX で収集した sFlow データから SDN-IX の OpenFlow スイッチに求められる要件について検討した．今後は，SDN-IX コントローラを実装し各機能毎に規模拡張性，性能の面から評価を行う．

謝辞　本研究は，総務省の戦略的国際連携型研究開発推進事業及び欧州連合 (EU) の第 7 次研究枠組み計画 (FP7) からの助成 (助成番号 608533:NECOMA) により得られた成果である．

文　献

[1] E. Jasinska, N. Hilliard, R. Raszuk, and N. Bakker, “Internet Exchange Route Server,” Internet-Draft draft-jasinska-ix-bgp-route-server-03.txt, IETF Secretariat, Oct. 2011.

[2] E. Jasinska, N. Hilliard, R. Raszuk, and N. Bakker, “Internet Exchange Route Server Operations,” Internet-Draft draft-hilliard-ix-bgp-route-server-operations-03.txt, IETF Secretariat, June 2013.

[3] “Open Networking Foundation”. https://www.opennetworking.org

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “Openflow: enabling innovation in campus networks,” SIGCOMM Comput. Commun. Rev., vol.38, no.2, pp.69–74, March 2008.

[5] 齋藤利文，榎本真俊，櫨山寛章，門林雄基，“LISP における二段階マップテーブルを用いた DDoS 攻撃緩和方式の実装と評価，” 電子情報通信学会 技術研究報告, vol. 112, no. 489, IA2012-89, pp.37–42，3 月 2013 年．

[6] “PhishTank”. https://www.phishtank.com/

[7] “CERT Polska n6”. http://n6.cert.pl/

[8] ArborNetworks, “Infrastructure Security Report,” 2012. http://www.arbornetworks.com/research/

[9] “IETF Interface to the Routing System (I2rs)”. http://datatracker.ietf.org/wg/i2rs/charter/