Vol.2016-IOT-34 No.4
2016/6/25

インアクティブIPアドレスとOpenFlowベースのセッション分別を用いたハニーポットの提案

長坂 真志[1,a)]　桝田 秀夫[2,b)]　森 真幸[2,c)]

概要：未使用 IP アドレス宛への通信は攻撃者の不正な活動によるものであることから，未使用 IP アドレスの全てをハニーポットに利用することで，多数の IP アドレスを保持する大学等のネットワーク全体を疎らにハニーポット化した大規模な攻撃解析システムを実現できる．本稿では，IP アドレスの利用状態を自動的に調査し，その状態遷移に従って，未使用 IP アドレス宛のパケットを OpenFlow を用いてハニーポットへ動的に転送する手法を提案する．

キーワード：ハニーポット，大学ネットワーク運用, OpenFlow

Proposal of honeypot using inactive IP addresses and session control based on OpenFlow

Masashi Nagasaka[1,a)]　Hideo Masuda[2,b)]　Masayuki Mori[2,c)]

Abstract: The cause of communication to unused IP addresses is malicious activities by attackers. Therefore, a large-scale system for analyzing attack can be implemented by honeypot using all unused IP addresses of campus network which has large IP address block. We propose a method that transfers packets sent to unused IP address to honeypot. The method automatically checks state transitions of IP addresses in campus network and dynamically controls the transfer by OpenFlow without disturbing communication between attackers and honeypot.

Keywords: honeypot, campus network operation, OpenFlow

1. はじめに

ネットワーク技術の進歩と普及に伴い，現在ではインターネットを利用した様々なサービスが存在し，現代社会の重要なインフラとなっている．一方，ネットワークを利用したシステムの脆弱性を突く攻撃や攻撃対象を探索するポートスキャンなど様々な不正通信も多く存在する．ネットワークの安全な利用のためには，このような攻撃への対策として，不正通信を観測，分析し，攻撃を検出，予測していくことが重要である．

トラフィック観測の研究例として，広範囲に渡るポートスキャンを観測し，攻撃の早期予測を行う WCLSCAN[1] や大分大学のポートスキャン可視化技術 [2] やメール送信サーバの分布の調査 [3] などが挙げられる．それぞれの研究では，脆弱性をついた攻撃の早期検知や水平ポートスキャンの検出，spam 送信サーバのアドレスブロックの発見等，様々な攻撃の検知に成功している．

ただし，ただ観測しているだけではポートスキャンのように攻撃対象を探索する通信の解析はできても，実際の攻撃パターンや攻撃が成功したときの被害を調べることは難しい．そのため，ハニーポットを利用して攻撃性の通信に

[1] 京都工芸繊維大学 工芸科学研究科 情報工学専攻
Graduate School of Information Science, Kyoto Institute of Technology
[2] 京都工芸繊維大学 情報科学センター
Center for Information Science, Kyoto Institute of Technology
[a)] m-ngsk15@dsm.cis.kit.ac.jp
[b)] h-masuda@kit.ac.jp
[c)] morim@kit.ac.jp

応答することで攻撃解析を行う研究も行われている．先行研究として，筑波大の学内の未使用サブネット宛の通信をルーティング機能を用いてハニーポットへ流す手法 [4][5] や九州大の DHCP サーバが管理する未使用 IP アドレスを利用する手法 [6] が提案されている．

しかし，単一の IP アドレスや一部のサブネットをハニーポットに利用しても，ハニーポットの IP アドレスやサブネットだけを攻撃者に回避されてしまう可能性が考えられる．そこで本研究では本学のネットワーク全体をハニーポットに利用するシステムを提案する．本学に限らず，古くからインターネットに接続している大学等では歴史的経緯からクラス B の IPv4 アドレスブロックが割り当てられていることが多い．しかし，そのブロックの IP アドレスを使い切っていることは稀であり，また，IP アドレスのリナンバリングが大変なため，そのブロック内には未使用の IP アドレスが疎らに存在することが多い．未使用 IP アドレス宛への通信は攻撃者の不正な活動によるものであることから，全ての未使用 IP アドレスをハニーポットに利用することで，大学等のネットワーク全体を疎らにハニーポット化した攻撃解析システムを実現できると同時に大学の未使用 IP アドレスの有効活用にもつながる．

本稿では ARP 観測により学内の IP アドレスの利用状態を自動的に調査し，その状態遷移に従って，学外からの未使用 IP アドレス宛のパケットを OpenFlow を用いて正規の通信に干渉せずにハニーポットへ動的に転送する手法を提示する．

2. 関連研究

2.1 筑波大学の SSH アクセス収集システム

筑波大学の佐藤らの研究 [5] では SSH サービスのエミュレートに特化したハニーポットである Kippo を用いて，未使用 IP アドレス宛の SSH アクセスの収集を行っている．この研究では，応答させる未使用 IP アドレスの選定を学内のコアルータで行っている．学内のコアルータのルーティングテーブルに対し，筑波大に割り当てられている 2 つのクラス B ネットワークへの next hop を，Honeyd[7] を稼働させているサーバとすることで，コアルータの最長一致の方式により，利用されているサブネット宛の通信は正しいルーティングが行われ，利用されていないサブネット宛の通信は Honeyd サーバに送られる．この手法では，コアルータのルーティング機能を用いて容易に IP アドレスの衝突問題を回避できるが，普段から使用されていない一部のサブネットしかハニーポット化できないため，組織全体のネットワークをハニーポットに利用するのは困難であり，ハニーポット化したサブネットのみが攻撃者に回避される可能性がある．

2.2 九州大学の DHCP セグメントの監視システム

九州大学の溝口らの研究 [6] では，DHCP が管理する未使用 IP アドレスを動的にハニーポットに割り当てて利用することで，未使用 IP アドレス宛のアクセスを収集している．DHCP 管理下の IP アドレスしか用いないため，IP アドレスの衝突問題を回避できるが，この手法はあくまでも DHCP サーバが管理しているセグメント内でしか使えないため，DHCP サーバが管理していない IP アドレスが大量に存在するような環境では未使用の IP アドレスを網羅することは難しい．

2.3 OpenFlow とハニーポットを用いた SSH ログイン防止手法

大阪市立大学の薛らの研究 [8] では，SSH サーバのアクセスログや IP アドレスのブラックリストから送信元 IP アドレスが攻撃者かどうか判別し，攻撃者からの SSH アクセスを OpenFlow を用いてハニーポットへ転送する手法を提案している．この手法では OpenFlow でパケットごとに実際の SSH サーバとハニーポットのどちらに送信するかを決定できるため，学外から送信されたパケットの宛先 IP アドレスが学内で使用されていたとしても，攻撃性のあるパケットのみハニーポットへ転送し，正規の通信は実際の SSH サーバへ送信できるような機構を実現できる．

この利点に着目し，本研究では，IP アドレスの状態遷移に従うフロー制御のシステムに OpenFlow を用いることで，宛先 IP アドレスの利用状態が使用中から未使用に切り替わる際に攻撃者とハニーポットとの通信を中断させないような機構を実現する．

3. 提案手法

3.1 本稿での IP アドレスの分類

本研究では未使用 IP アドレスを利用するが，その厳密な定義のため，本稿では以下の用語を定義して用いる．

3.1.1 アクティブ IP アドレス

あるネットワーク内で実際に稼働中かつ，サーバあるいはクライアントとして外部ネットワークと通信可能な機器の NIC に設定された IP アドレスをアクティブである IP アドレスと定義する．また，これをアクティブ IP アドレスと表現する．

3.1.2 インアクティブ IP アドレス

あるネットワークで利用可能な IP アドレスのうち，アクティブ IP アドレス以外の全ての IP アドレスをインアクティブである IP アドレスと定義する．また，これをインアクティブ IP アドレスと表現する．

3.2 提案手法の概要

本節では外部ネットワークを送信元とするパケットのうち，インアクティブ IP アドレス宛のパケットのみをハニー

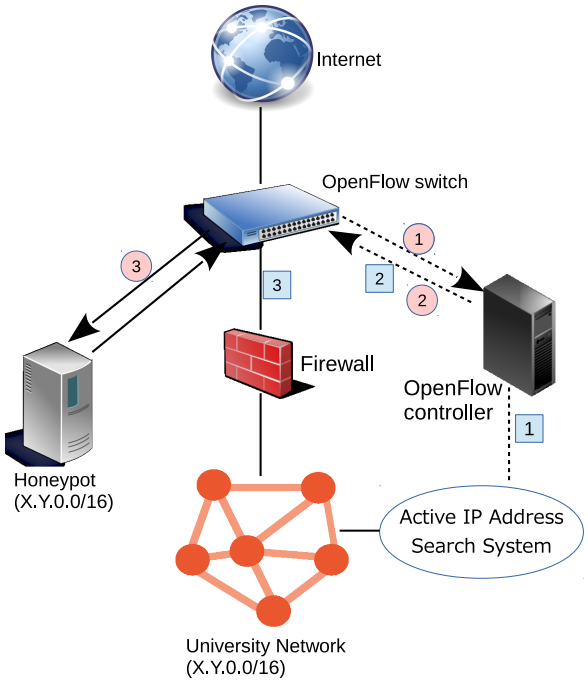

図 1　提案システムの概要図

ポットへ転送することで，アクティブ IP アドレス宛の正規の通信を妨害せずに，インアクティブ IP アドレス宛の不正な通信に対してハニーポットで応答する手法の概要を述べる．

まず，本稿で提案する手法を実現するためのシステム（以降，本稿では，このシステムを提案システムと表現する）の概要を図 1 に示す．提案システムはハニーポット，OpenFlow スイッチ，OpenFlow コントローラ，アクティブ IP アドレス探索システム（以降，本稿では探索システムと省略して表現する）から構成される．OpenFlow スイッチは学外から学内への全てのパケットを OpenFlow スイッチに受信させるため，学内のネットワークとインターネットとの接続境界に設置する．また，OpenFlow スイッチを制御するための OpenFlow コントローラとインアクティブ IP アドレス宛の通信に対して応答するためのハニーポットを OpenFlow スイッチに接続する．探索システムは学内のネットワークの各ブロードキャストドメインに設置し，OpenFlow コントローラと通信可能な状態にしておく．3.3 節でアクティブ IP アドレス探索システム，3.4 節で OpenFlow コントローラ，3.5 節で本研究で用いるハニーポットの詳細な説明を行う．

本節では 3.2.1 項，3.2.2 項で提案システム全体の動作を大まかに説明し，3.2.3 項で提案システムの特徴を述べる．

3.2.1　アクティブ IP アドレス宛の通信の制御

アクティブ IP アドレス宛の通信の制御を行うため，提案システムでは以下のように動作する．

1 各探索システムが自身の属するブロードキャストドメインでアクティブに切り替わった IP アドレスを OpenFlow コントローラに通知する．

2 通知された IP アドレスを宛先とするパケットを学内ネットワークへ転送するフローエントリを低い優先度で追加する．

3 OpenFlow スイッチは追加されたフローエントリに従ってアクティブ IP アドレス宛の通信を学内へ送信する．

1 では IP アドレスの状態遷移に即座に対応し，正規の通信を妨害しないようにする必要がある．その具体的な手法は 3.3 節で述べる．また，探索システムから通知したアクティブ IP アドレスのうち，インアクティブに切り替わった IP アドレスがあった場合，その IP アドレスをコントローラへ通知し，2 で一度追加したフローエントリを削除する処理も行う．

3.2.2　インアクティブ IP アドレス宛の通信の制御

インアクティブ IP アドレス宛の通信の制御を行うため，提案システムでは以下のように動作する．

① 学外から受信したパケットの宛先 IP アドレスが 3.2.1 項の 2 で追加したどのフローエントリにもマッチしなかった場合，コントローラに受信したパケットを送る．

② ①で受信したパケットと同じ L4 の情報をもつパケットをハニーポットへ転送するフローエントリを高い優先度で追加する．

③ 追加されたフローエントリに従ってインアクティブ IP アドレス宛の通信をハニーポットへ送信する．

②では，追加したフローエントリは攻撃者との通信時のみ存在していれば十分なので，追加したフローエントリが一定時間参照されなかった場合，そのエントリを削除することでインアクティブ IP アドレス宛の通信をセッション単位で制御する．

3.2.3　提案システムの特徴

3.2.1 項と 3.2.2 項で述べた制御方法により，ハニーポットへ誘導している通信の宛先が学内でアクティブに切り替わったとしても，追加したフローエントリの優先度に従って，攻撃者とハニーポット間の通信をセッション単位で維持しつつ，新規の正規な通信を学内へ送信できる．また，この仕組みを利用すれば，学内のアクティブ IP アドレス宛のパケットのうち，ルータなどの外部からのアクセスを直接受ける必要のない機器の IP アドレスを宛先とするパケットのみをセッション単位でハニーポットへ転送するような機構も実現できる．

また，提案システムではアクティブ IP アドレス宛の通信は IP アドレスの状態遷移時に追加されたフローエントリに従ってハードウェアの処理のみで制御できるため，正規の通信を高速に処理できると考えられる．ただし，インアクティブ IP アドレス宛の通信時にはセッション単位のフローエントリを追加し続けることになるため，これによ

りフローエントリ数が増加しすぎるとOpenFlowスイッチの性能が低下する可能性がある．これに関しては提案システムで実際のフローエントリの増加傾向を調査する実験を行った．この実験については4章で述べる．

3.3 アクティブIPアドレス探索システム

探索システムは学内ネットワークの各ブロードキャストドメインに一つ以上設置され，自身が属するブロードキャストドメインの全てのアクティブIPアドレスを探索し，ブロードキャストドメインの範囲（ネットワークアドレスとサブネットマスク）とその範囲内の全てのアクティブIPアドレスをOpenFlowコントローラにUDPを用いて通知する．

アクティブIPアドレスの探索にはARPを用いる．各サーバ機器は通信の初回時にARPリクエストをブロードキャストで送信するため，これを観測することでサーバ機器のIPアドレスがアクティブに切り替わるタイミングをTCPやUDPによる通信が発生する前に検知できる．検知したアクティブIPアドレスを即座にOpenFlowコントローラに通知することで，サーバの通信開始と同時に外部ネットワークとの通信を制御できる．また，一度アクティブになったIPアドレスの状態を検査するため，定期的にARPリクエストをブロードキャストドメインの全IPアドレスに対して送信してARPリプライを観測し，応答しなくなったIPアドレスをOpenFlowコントローラに通知する．一般的にこのようなARPスキャンによるサーバ機器の稼働状況の調査はICMP等のIPベースのスキャンよりも高速で信頼性も高い[9]．

3.4 OpenFlowコントローラ

本節では3.2.1項，3.2.2項で述べた提案システムの動作を実現するために行うOpenFlowコントローラの処理のアルゴリズムを述べる．また，追加および削除するフローエントリの説明のため，フローエントリに設定する優先度を0〜3の4つに分けて表現する．優先度は昇順で，優先度0を最低優先度，優先度3を最高優先度とする．

まず，OpenFlowスイッチの起動時に以下のフローエントリを追加する．

- 入力ポートが学内の場合，出力ポートを学外とする（優先度0）．
- 入力ポートがハニーポットの場合，出力ポートを学外とする（優先度0）．
- 入力ポートが学外の場合，出力ポートを学内とする（優先度0）．

以降，提案システムのOpenFlowコントローラがFlow ModメッセージをOpenFlowスイッチに送信するトリガーは以下の4つである．

（1）アクティブIPアドレスが通知された場合

通知を行った探索システムが未知のブロードキャストドメインを監視していた場合，そのブロードキャストドメインを既知と見なし，次のフローエントリを追加する．『入力ポートが学外かつ，通知を行った探索システムが属するブロードキャストドメインに宛先IPアドレスが含まれている場合，Packet InメッセージをOpenFlowコントローラに送る（優先度1）』．さらに，次のフローエントリを追加する．『入力ポートが学外かつ，宛先IPアドレスが通知されたものである場合，出力ポートを学内とする（優先度2）』．また，追加後は探索システムと確実に同期させるため，Barrier RequestメッセージをOpenFlowスイッチに送信する．

（2）インアクティブIPアドレスが通知された場合

マッチ条件で宛先のIPアドレスが通知されたIPアドレスであり，アクションで出力ポートを学内としているフローエントリを削除する．

（3）通知が途絶えた探索システムが存在する場合

当該探索システムが監視していたブロードキャストドメインを未知と見なし，マッチ条件で宛先のネットワークがそのブロードキャストドメインであり，アクションでPacket Inメッセージを出力するようなフローエントリを削除する．

（4）Packet Inメッセージを受信した場合

受信したPacket Inメッセージから，そのパケットの送信元と宛先のIPアドレスとポート番号をマッチ条件とし，パケットの出力先をハニーポットとするフローエントリを優先度3で一定時間のidle timeoutを設けて追加する．また，追加後にPacket Inメッセージで受信したパケットをハニーポットへPacket Outメッセージで送信する．

以上で述べたアルゴリズムでは3.3節で述べた探索システムの仕様により，IPアドレスがインアクティブからアクティブに切り替わったタイミングには即座にフローエントリの追加で対応できるが，アクティブからインアクティブに切り替わったタイミングには遅れてフローエントリを削除する処理を行う可能性がある．しかし，アクティブからインアクティブの切り替えが遅れてもハニーポットへ転送し始めるタイミングが遅れるだけで，実際に稼働しているサーバの通信を妨害することはないため，上記のアルゴリズムで問題ないと考えられる．

3.5 ハニーポット

提案システムで利用するハニーポットは学内の全てのインアクティブIPアドレスに対して応答できる必要がある．提案システムではOpenFlowスイッチでハニーポットに入力するパケットを分別していることから，ハニーポットは予め学内のクラスBのIPアドレスの全てに対して応答できるようにすれば十分である．

2.1 節で述べた先行研究では Honeyd のプロキシ機能を用いて大量のホストをエミュレートすることで，大量の IP アドレス全てに対して単一の SSH ハニーポットが応答できるようにする仕組みが提案されている．この手法では実際に応答するハニーポット自体には単一の IP アドレスを設定するだけで実現できるが，送信元と宛先の IP アドレスの情報をデータベースに登録する際に，ハニーポットと Honeyd の受信ログを照合する必要がある．

本研究ではこれを簡易にするため，Honeyd を使わずに IP エイリアスでハニーポットにクラス B の IP アドレスの全てを設定する．本研究では実際に単一の NIC に IP エイリアスとしてクラス B の全 IP アドレス（65534 個）を設定し，IP エイリアスを設定していない状態と比較しても通信遅延が発生しないことを確認した．

4. 試作システムでの実験

4.1 実験内容

3 章で述べた提案システムでは，インアクティブ IP アドレス宛の通信が発生する度に，セッション単位でフローエントリを追加するため，フローエントリ数の増大によって OpenFlow スイッチの性能が低下する可能性がある．そのため，本研究では，実際に提案システムを稼働させた場合のフローエントリの増加傾向を調査した．

4.2 実験手法

本実験では 3.4 節で述べたアルゴリズムで OpenFlow コントローラを実装し，3.3 節で述べた探索システムを学内のクラス C の IP アドレスブロック内のアクティブ IP アドレスを探索できるように設置した．提案システムの OpenFlow スイッチは Open vSwitch によりソフトウェアで実装し，今回は試験的に学外からの全パケットを学内の基幹スイッチからミラーリングして OpenFlow スイッチで受信して，OpenFlow スイッチ上のフローエントリの増加傾向を調査する．今回はミラーポートからの受信のみになるため，ハニーポットは稼働させておらず，3.4 節で述べたアルゴリズムに従ってフローエントリを追加，削除するのみとし，3.4 節の（4）で述べた idle timeout を 60 秒とした．また，OpenFlow スイッチの構成を表 1 に示す．

さらに，本実験では実際のインアクティブ IP アドレス宛の通信との関連性も調べた．一般的にダークネットへの通信はポートスキャンやバックスキャッタなど様々な通信が観測されることが知られている．今回の実験ではその中でも TCP の SYN スキャン，Connect スキャンとの関連性を調査した．具体的には，1 分ごとに OpenFlow スイッチ上のフローエントリ数を取得すると同時に，それまでの 1 分間で Packet In メッセージで送信されてきたパケットのうち，TCP の SYN フラグが 1 のものをカウントしておき，その全パケット数とフローエントリ数を比較した．本実験ではポートスキャンへの応答を行わないため，SYN スキャンと Connect スキャンとの判別はできない．そのため，以降は SYN スキャンと Connect スキャンをまとめて SYN スキャンとして扱うこととする．

表 1　OpenFlow スイッチの構成

CPU	Inter Xeon E5620 2.5GHz Quad Core x2
Memory	24GB（DIMM 1333 MHz 4096MB x6）
NIC	Intel 82575GB
OS	Linux 3.10.0 229.el7.x86_64 （CentOS 7.1）
Open vSwitch	Open vSwitch 2.3.1

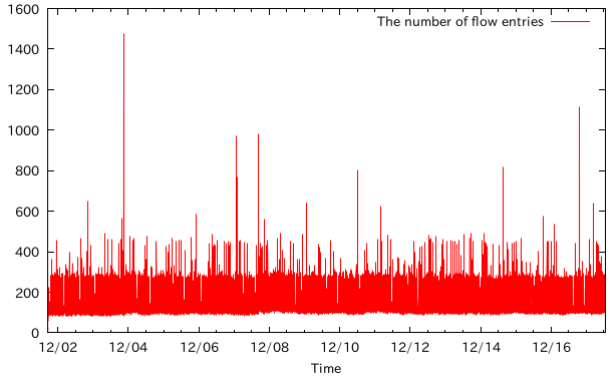

図 2　フローエントリ数の推移

4.3 実験結果

4.2 節で述べた手法で実験を行った結果を図 2 と図 3 に示す．

実験を実施した期間は 2015/12/1 17:00〜2015/12/17 13:00 であり，図 2 は全期間のフローエントリ数の推移を示したものである．探索システムが探索対象とした学内のクラス C の IP アドレスブロックにおけるアクティブ IP アドレス数は全期間を通して 70〜80 程度であった．このことから図 2 の結果より，フローエントリ数の推移について，アクティブ IP アドレスに関するフローエントリが全エントリのほとんどを占めている状態と，インアクティブ IP アドレス宛の大量の通信を受けてフローエントリ数が瞬間的に増加している状態を短期間で断続的に繰り返していることが分かる．

また，図 3 はフローエントリ数と受けた SYN スキャンの回数を同時に調査したものであり，実験期間のうち，12/2 の 0:00〜12:00 の期間の実験結果である．図 3 より，フローエントリ数が瞬間的に増加するタイミングのほとんどで SYN スキャンの回数も同程度増加していることが分かる．

5. 考察

本章では，提案手法についての考察を行う．5.1 節では OpenFlow スイッチの性能面から見た提案システムの実現可能性を述べ，5.2 節では提案システムで利用するハニーポットについて述べる．

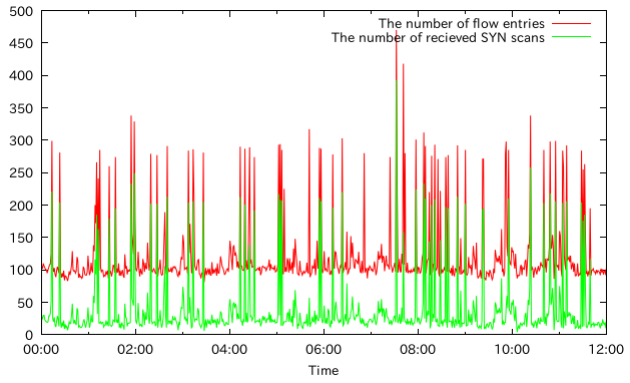

図 3 フローエントリ数と受けた SYN スキャンの回数の推移

5.1 OpenFlow スイッチ

図 2 より，フローエントリはクラス C のネットワークで平時に 300〜400 程度（100 程度がアクティブ IP アドレス），ピーク時に 1000 以上まで増加しており，クラス B まで拡張した場合，エントリ数は平時に 100k 程度でピーク時に 200k を超える可能性があると考えられる．また，ハニーポットを実際に稼働させた場合は今回の実験結果よりも増加すると見込まれる．現状のフローエントリの登録方法では一般に公開されている OpenFlow スイッチ [10] の性能限界を超えてしまう可能性があるため，フローエントリ数を抑える必要がある．

図 3 では，アクティブ IP アドレスが 70〜80 程度であったことを考えれば，フローエントリが増加しているタイミングのほとんどで SYN スキャンの数だけエントリ数が増加していると考えられる．このことから，ポートスキャンによるフローエントリの増加を抑えられれば，現実的なエントリ数で提案システムを運用できると考えられる．例えば，学外から受信したインアクティブ IP アドレス宛のパケットのうち，SYN フラグが 1 のパケットをハニーポットへ直接転送するような処理をするだけでも，図 3 より，大幅なエントリ数の削減が可能であると考えられる．また，実際にハニーポットを稼働させ，ポートスキャンに応答した場合にセッションを継続させる攻撃者の割合がどの程度になるか調査することも重要であると考えられる．

5.2 ハニーポット

3.5 節ではハニーポットに IP エイリアスを設定することで，クラス B の全 IP アドレスに応答可能にすることを述べた．しかし，図 2 より，ポートスキャンを受けたときにクラス B でピーク時に 200k 程度のコネクションが要求されることが予想されるため，一時的に膨大なプロセスを起動できるような環境が必要になる．対策としては Docker 等の軽量な仮想化基盤を利用して複数のハニーポットを起動し，攻撃者へ応答する処理を分散させることなどが考えられる．また，複数のハニーポットを用意する際に，設定の異なるハニーポットを複数用意して，攻撃者からのアクセス回数などに応じて挙動の異なるハニーポットに転送することも可能であると考えられる．

6. おわりに

本稿では OpenFlow によるセッション単位でのフロー制御を行い，正規の通信を妨害せずに学内のインアクティブ IP アドレス宛の通信をハニーポットへ動的に転送する手法を提示した．

また，提案システムで OpenFlow スイッチのフローエントリ数の推移を実環境で計測し，現実的なエントリ数で運用できる可能性を示した．

今後の課題としては，提案手法で外部からアクセスを受ける必要のないアクティブ IP アドレスをハニーポットに利用することなどによって提案システムを拡張させることが考えられる．また，実環境でハニーポットを稼働させることで，実際に不正通信を調査するとともに，どの程度の攻撃者がセッションを継続させるかどうか調査することも重要であると考えられる．

謝辞 本研究の一部は JSPS 科研費 26330104 の助成を受けたものである．

参考文献

[1] 鈴木裕信：WCLSCAN - インターネット早期広域攻撃警戒システム，WCLSCAN project（オンライン），入手先 ⟨http://www.wclscan.org/⟩（参照 2014-9-10）．
[2] 小刀稱知哉，松井一乃，池部実，吉田和幸，金高一：トラフィック情報表示システムによる scan 攻撃の可視化法，情報処理学会研究報告，Vol. 2013-IOT-21, No. 18, pp. 1–8 (2013).
[3] 小刀稱知哉，松井一乃，池部実，吉田和幸：大分大学宛のメール送信サーバの分布，情報処理学会研究報告，Vol. 2013-IOT-21, No. 19, pp. 1–7 (2013).
[4] 佐藤聡，三田尚貴，新城靖，板野肯三：ハニーポットを利用した筑波大学の未使用 IP アドレス宛の HTTP リクエストの解析，情報処理学会研究報告，Vol. 2013-IOT-23, No. 8, pp. 1–3 (2013).
[5] 佐藤聡，小川智也，新城靖，吉田健一：筑波大学におけるハニーポットを用いた不適切な SSH アクセスの収集とその解析，情報処理学会研究報告，Vol. 2014-IOT-25, No. 17, pp. 1–3 (2014).
[6] 溝口誠一郎, Erwan, L. M.，堀良彰, 櫻井幸一：DHCP によって管理されたセグメントに存在する未使用 IP アドレスの監視手法, 情報処理学会研究報告, Vol. 2008-CSFC-41, No. 41, pp. 55–60 (2008).
[7] Provos, N.: Developments of the Honeyd Virtual Honeypot, Niels Provos (online), available from ⟨http://www.honeyd.org/⟩ (accessed 2014-11-28).
[8] 薛微微，石橋勇人：OpenFlow とハニーポットを用いた SSH ログイン攻撃防止手法の提案と実装，情報処理学会研究報告，Vol. 2015-IOT-28, No. 3, pp. 1–6 (2015).
[9] Lyon, G. F.: Nmap Host Discovery, Nmap (online), available from ⟨https://nmap.org/book/man-host-discovery.html⟩ (accessed 2015-2-2).
[10] NEC: SDN 対応製品 UNIVERGE PF シリーズ，NEC Corporation（オンライン），入手先 ⟨http://jpn.nec.com/univerge/pflow/spec_pfs.html⟩（参照 2016-5-10）．