Vol.2015-IOT-28 No.1
2015/3/5

疎なネットワークにおける未使用IPアドレス宛の攻撃を効率的に収集するハニーポットの試作

長坂 真志[1,a)]　桝田 秀夫[2,b)]

概要：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 Class 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，そのブロック内の使用中 IP アドレスは疎らとなりがちである．本報告書では，疎なネットワークにおける使用中 IP アドレスを動的に調査し，外部からの未使用 IP アドレス宛の攻撃を効率的にハニーポットへ取り入れる手法を提案する．また，提案した手法で試作したシステムの現段階での実装状況とその性能も報告する．

キーワード：ハニーポット，大学ネットワーク運用

Proposal of a honeypot to effectively capture attacks with unused IP addresses as the destination in sparse network

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

Abstract: Many universities, which have connected to the Internet for a long time, has Class B IPv4 address block by historical background. However, there are only a few universities that have used up all of the IP addresses in the given block. And, using condition of the IP addresses in the block tends to be sparse because renumbering the IP addresses is a hard task. In this paper, we propose a system to search dynamically unused IP address in sparse network, and to collect effectively packets, addressed to the unused IP address, to honeypot. In addition, we report a present state and a performance of the proposed system.

Keywords: honeypot, campus network operation

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．

特に，広範囲の IP アドレス空間を利用した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や，spam 送信サーバのアドレスブロックの発見等，狭い範囲の IP アドレスの観測だけでは発見することが難しいような攻撃の検知に成功している．

本研究ではそのような広範囲に渡る不正通信の観測を実

[1] 京都工芸繊維大学 工芸科学部 情報工学課程
Undergraduate 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

現するため，本学の未使用 IP アドレスを用いる．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 Class 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，そのブロック内の使用中 IP アドレスは疎らとなりがちである．残りの未使用 IP アドレス宛の通信は原則として不適切な通信であることから，それらを不正通信の観測対象にできると同時に，大学の未使用 IP アドレスの有効活用にもつながる．

また，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，その攻撃が成功したときの被害を調べることは難しい．広範囲の IP アドレス空間を利用して実際の攻撃パターンを見るには IP アドレスベースでハニーポットとしてホストを仮想的に用意し，ある程度の段階まで攻撃者に攻撃が成功しているように見せかける必要がある．また，学内で一時的に使われていない IP アドレスを用いる場合，ハニーポットによる応答が正規の応答と重複しないように，未使用 IP アドレスの正確な調査が必要がある．

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，本学のようにサブネットが疎らに存在し，サブネット内の IP アドレスも利用状況が疎らな IP アドレス空間では，上記の手法では学内の大量の未使用 IP アドレスを調査することは煩雑である．そこで，本研究では疎なネットワークであっても，ARP 観測により使用中 IP アドレスを正確かつ動的に割り出し，外部からの未使用 IP アドレス宛の攻撃を仮想デバイスを用いて効率的にハニーポットへ取り入れることが可能な手法を提示する．

2. 関連研究

2.1 ハイブリッド型ハニーポットフレームワーク

広範囲の IP アドレス空間をハニーポットとして利用し，ネットワークへの攻撃を検知するシステムとして Hassan らが提案したハイブリッド型ハニーポットフレームワーク [7] が挙げられる．このシステムでは，広範囲の IP アドレス空間を低対話型ハニーポットである Honeyd[8] を用いて監視し，Honeyd サーバへの通信を Honeyd サーバに接続した高対話型ハニーポットへ中継することによって攻撃者との対話を行う．Honeyd はサーバ上でひとつのプロセスとして起動し，IP アドレスベースで何千もの仮想ホストをエミュレートすることができる．さらに，その仮想ホスト宛の通信を Honeyd を起動しているサーバとは別のホストへ中継し，そのホストからの応答を Honeyd でエミュレートしている仮想ホストの応答に見せかけて攻撃者に送信するプロキシ機能をもつ．中継先を高対話型ハニーポットとすることで，攻撃者からは何千台もの本物のサーバが稼働しているように見え，Honeyd はホストのエミュレートと中継に徹し，高対話型ハニーポットは攻撃者との対話に徹するように処理を分割することができる．本研究でも広範囲の IP アドレス空間を利用したハニーポットにこの手法を採用する．

2.2 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 アクセスの収集のため，上述のシステムで中継先のハニーポットに SSH サービスのエミュレートに特化した Kippo を用いている．また，Honeyd により応答させる未使用 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 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，サブネット毎で密に IP アドレスが使用されている場合は効率のよい手法といえるが，サブネット毎で IP アドレスの使用状況が疎らなネットワークでは効率が悪い．

2.3 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 アドレスを利用して，ハイブリッド型ハニーポットフレームワークを実現している．Honeyd は DHCP クライアントとしての機能を備えており，DHCP サーバが管理している未使用 IP アドレスを自身の仮想ホストに自動で割り当てることができる．学内の DHCP サーバが管理しているセグメント内に Honeyd サーバを設置すれば，動的にそのセグメント内の未使用 IP アドレスが仮想ホストに割り当てられ，IP アドレスの衝突問題を回避できる．しかし，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 サーバの管轄下でない 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．

3. 未使用 IP アドレス宛の攻撃の収集方法

以降，本報告書での未使用 IP アドレスは，常に使用されていない IP アドレスだけでなく，一時的にオフラインであるものも含めるものとする．

3.1 収集システムの概要

本研究で提案する収集システムの概要を図 1 に示す．ハニーポット自体の構成は 2.1 節で述べたハイブリッド型ハ

ニーポットフレームワークを採用する（図 1，③〜⑤に相当）．また，本研究では本来ファイアウォール方向に流れる学外から学内宛のパケットを Honeyd サーバで受信するためにスイッチのミラーポートを利用する．

Honeyd がエミュレートする仮想ホストの IP アドレスは学内に割り当てられた IP アドレス全てとし，Honeyd が入力に用いるデバイスを TAP デバイス [9] とする．学内のファイアウォールの外に設置されたスイッチのミラーポートに接続されたデバイス（図 1，devA）で学外から学内への全パケットを受信し（図 1，①），Honeyd サーバ上で稼働させる 3.2.6 節のシステムがメモリ上に保持する学内の IP アドレスの使用状況をもとに，学内の未使用 IP アドレス宛のパケットのみを TAP デバイスに書き込む（図 1，②）．TAP デバイスに書き込まれたパケットを OS が物理デバイスから受信したパケットと同様に処理するので，Honeyd には未使用 IP アドレス宛のパケットのみを物理デバイスから受信したものとして処理させることができる．すなわち，未使用 IP アドレス宛の攻撃の収集のために，Honeyd がエミュレートする仮想ホストの IP アドレスを動的に変更するのではなく，Honeyd の入力デバイスとなる TAP デバイスに書きこむパケットを送信先が学内の未使用 IP アドレスのパケットのみになるように動的に変更する．

また，この収集システムでは，学外との通信について，入力が TAP デバイスに限定され，出力するパケットも Honeyd がジェネレートしたものに限られる．そのため，学内のネットワークとの通信を行うデバイス（図 1，devC）を別に用意して，学外への出力用のデバイス（図 1，devB）は受信するパケットをすべて破棄することで，Honeyd サーバ自体が外部からの攻撃の標的になることを防ぐ．

3.2 使用中 IP アドレスの動的な調査手法

3.2.1 調査システムに要求される機能

本研究で提示する収集システムでは，3.1 節で述べたように未使用 IP アドレス宛のパケットのみを TAP デバイスに書き込むため，学内の未使用 IP アドレスを調査する必要がある．Honeyd サーバが管理する IP アドレスと学内で使用中の IP アドレスとの衝突が起きれば，それらの応答が重複し，学内の正規のホストと外部との通信を邪魔するだけでなく，攻撃の誤検知にもつながるため，調査システムにおいて IP アドレスの使用状況をリアルタイムに把握できる機能は不可欠といえる．ただし，実際の運用を考えると，完全にリアルタイムに把握する必要性は低い．なぜなら学外から学内への通信が先に起こるような場合は，その宛先の機器は学外に対して何らかのサービスを提供しているサーバであり，そのようなサーバが頻繁に落ちたり，ネットワークの切断を行うとは考えにくいからである．それよりも対応すべきなのは学内でクライアントとして起動し，学外に対して通信を開始する機器である．この場合は

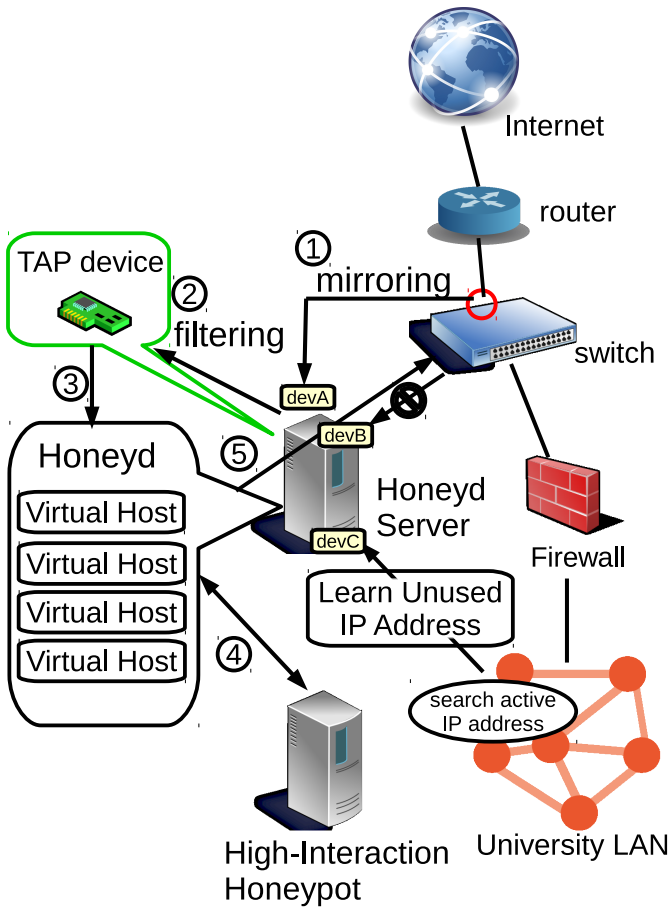

図 1　収集システムの概要図

学内からの通信が先に起こるので，学内から学外への要求に対する応答が返ってくるまでの間に Honeyd サーバがメモリ上で保持する当該の IP アドレスの使用状況を瞬時に使用中に切り替えれば IP アドレスの衝突を防ぐことができる．

また，収集システムでは Honeyd サーバ上で使用中と判定している IP アドレス宛のパケットを Honeyd が読み込むことはないので，IP アドレスの使用を止めたタイミングの把握が遅れることに関してはシステムの運用上問題はない．ただし，本当は使用中であるにも関わらず，Honeyd サーバで未使用とみなすと衝突が起きる可能性があるので，把握している IP アドレスの稼働確認（使用中であることの確認）ができる機能も必要である．

3.2.2 調査システムの概要

3.2.1 節のような機能要求を満たすためには ICMP や TCP/UDP を用いた通常のネットワークスキャンでは，多くのネットワーク帯域を消費する他，ホストの探索に時間がかかるため，IP アドレスの使用状況の正確な把握が難しい．そのため，本研究では学内に流れる ARP リクエスト，ARP リプライの観測により動的な IP アドレスの調査を行う．特に初回の通信では IP アドレスと MAC アドレスの

紐付けが行われないと通信を行えないので，ARP リクエストが必ず送信されるはずである．さらに ARP はレイヤ 2 プロトコルであり，通信においてほぼ必須の機能であることから，個々のホストに拒絶されるとは考えにくいため，ARP リプライを観測できた時点でその IP アドレスを使用中と判定できる．また，本来の通信よりも先に ARP のやりとりが行われるので，IP アドレスの使用開始のタイミングにいち早く対応することができる．しかし，ARP は個別のサブネット内でしか観測できないため，学内全域の未使用 IP アドレスを把握するためには，学内全域のスイッチやサブネット毎に ARP 観測による調査システムを稼働させて学内全域の使用中 IP アドレスを調べ，その補集合を未使用 IP アドレスとする必要がある．本報告書では後述の 3.2.3 から 3.2.5 節の 3 種類の IP アドレス使用状況調査システムを提示し，3.2.6 節で IP アドレス使用状況調査システムが管理する IP アドレスの使用状況を集約するシステムを提示する．

3.2.3 ARP 観測による受動的調査システム

このシステムはスイッチのミラーポートを利用する．基本的にはスイッチに接続されている全ポートをミラーリングし，それらの通信から ARP リクエストと ARP リプライを抽出して処理する．IP アドレスの使用状況を動的に調査するには 3.2.2 節で述べたように，ARP リプライを発見したときに，その送信元 IP アドレスと宛先 IP アドレスの使用状況 [*1] を使用中に切り替えればよい．また，IP アドレスの使用開始を瞬時に把握するため，ARP リプライ発見前の段階で未使用だった IP アドレスは，その ARP リプライの発見をトリガーとして，集約システムに使用状況 [*1] が切り替わったことを伝える必要がある．

また，IP アドレスの使用状況の把握のため，長時間 ARP リクエストや ARP リプライによって確認されなかった IP アドレスを未使用とみなす処理も必要となる．そのため，一般的な OS の ARP テーブルのクリア間隔 [*2] から，未使用と判断するための ARP リクエストや ARP リプライを観測できない期間を 30 分 [*3] とする．

ただし，長時間通信を行わなかった IP アドレスに関しては次の通信の瞬間まで ARP リクエストは送信されないので，通信間隔が極めて疎らな IP アドレスの稼働確認ができないことが考えられる．ただし，この問題は集約システム側で，ほぼ対処可能である．

3.2.4 ARP 観測による能動的調査システム

このシステムは自身がサブネットに参加し [*4]，そのサブネット内の全ホストの稼働確認のため，サブネット内の IP アドレスに対して順に ARP リクエストをブロードキャストで送信し，一定時間内に ARP リプライを受信すれば，その IP アドレスが設定された機器が存在しているものと見なす．逆に一定時間内に ARP リプライが返ってこなければ，その IP アドレスが設定された機器は存在していないと見なす．また，ARP リクエストは初回の通信では宛先 MAC アドレスがブロードキャストとして送信されるため，調査システムでプロミスキャスモードで観測していれば，IP アドレスの使用の開始時に送信された ARP リクエストを見ることができるので，IP アドレスの使用の開始に瞬時に対応することができる．

このシステムの利点は，あるホスト上でこのシステムを稼働させるだけで，そのホストが所属するサブネット内の全 IP アドレスの使用状況を把握できることである．さらに特定の IP アドレスが未使用になるタイミングが最長でもサブネット内の IP アドレスを巡回する間隔で判明するため，本報告書で紹介する 3 種の調査システムのうち，最も調査精度の高いシステムといえる．

3.2.5 ARP テーブル参照による調査システム

このシステムでは SNMP でルータの ARP テーブルを取得し，その ARP テーブルに含まれる全 IP アドレスを 3.2.6 節の集約システムに送信する．SNMP で通信できるだけよいので，3.2.3 や 3.2.4 節のシステムのようにスイッチやサブネット毎にこのシステムを稼働させる必要はない．しかし，このシステムでは定期的に SNMP で問い合わせるだけなので，3.2.1 節で述べた不可欠な機能要求である IP アドレスの使用の開始のタイミングを瞬時に把握することが難しい．本システムで使用開始のタイミングを瞬時に把握するには，SNMP で問い合わせる間隔を限りなく短くして稼働させる必要があり，多くのネットワーク帯域を消費するとともに，問い合わせ先の機器に大きな負担をかけしまう．そのため，IP アドレスの使用状況の変化の頻度が不明であるようなネットワークにこのシステムは向いていない．しかし，問い合わせ先のホストが所属するサブネット内の全ホストの IP アドレスの使用状況がほぼ変わらず安定していると予めわかっているような場合は，このシステムは有効な手段であるといえる．

3.2.6 IP アドレス使用状況集約システム

このシステムでは Honeyd サーバ上で稼動させ，調査システムである 3.2.3 や 3.2.4，3.2.5 節から送信される使用中の IP アドレスを受信し，一括で管理する．送信される IP アドレスは使用中のものだけなので，本システムで調査システムから送信されなくなった IP アドレスを未使用に切り替える必要がある．そのため，各調査システムからの送信間隔以上で本システムが管理する全 IP アドレスの使用状況をクリアする必要がある．

また，3.2.3 節での問題を解決するために，調査システム

[*1] システムがメモリ上で保持している IP アドレスの使用状況のことを指す．
[*2] デフォルト値は Windows で 2 分，Linux で 15 分，BSD 系 OS で 20 分と様々である．
[*3] あくまで各 OS のデフォルトの設定を前提とした値であり，運用環境に合わせて適切に決めるべきである．
[*4] このシステムを稼働させる機器にはそのサブネットに属する IP アドレスが設定されている必要がある．

から送信されなくなった IP アドレスに対し，ICMP echo request を送り，そのリプライが返ってくれば使用中とみなす．ただし，ICMP を拒絶される可能性もあるので，リプライが返ってこなかった場合にその IP アドレスと TCP の 3 way hand shake を試みる．この際，拒絶されても RST フラグの TCP パケットを送出するホストであれば，ルータに向けて ARP リクエストを出させることができ，3.2.3 節のシステム側で対応できる．

3.3 TAP デバイスによる入力用デバイスの実装方法

ミラーポートから受信する物理デバイスの TCP/IP オフロード機能を無効にし，動作モードをプロミスキャスモードにして，そのデバイスからパケットをイーサネットヘッダから読み込み，そのパケットの IP ヘッダを見て，宛先 IP アドレスが学内で未使用であればイーサネットヘッダから全データを TAP デバイスに書き込めばよい．また，パケットのフィルタリングを高速化するため，TAP デバイスへ書き込む処理を 3.2.6 節のシステムに組み込み，集約システムがメモリ上に保持する IP アドレスの使用状況を参照できるようにする．また 3.2.6 節のシステムをマルチスレッド化し，ミラーポートからのパケット受信から TAP デバイスへの書き込みまでの処理をひとつのスレッドとして生成し，集約システム内でそのスレッドの優先度を最大にすることで TAP デバイスのスループットを最大限に高める．

4. 現時点での実装状況とその性能

4.1 研究室内で試作した収集システムとその動作実験

3 章で提案した手法で研究室内で試作したシステムの概要を図 2 に示す．研究室内のネットワークの構成は，研究室のゲートウェイとなるルータの下に各研究室員のルータがあり，そのルータの下に VLAN で区切られた各研究室員のネットワークが存在する．本研究では図 2 のように自身のネットワーク上で収集システムの動作実験を行った．

4.1.1 ネットワーク外からのアクセスを Honeyd サーバに取り込む実験

実験環境では，外部からの通信が Honeyd サーバに流れない環境を構築するため，自身のルータ（図 2，ルータ A）で未使用 IP アドレスを含むネットワーク（図 2，ネットワーク A）のネクストホップを Honeyd サーバとは異なる機器（図 2，ホスト A）に指定する．ホスト A の下には実際にはネットワーク A は存在しないので，ホスト A はルータ A から送信されたネットワーク A に属する IP アドレス（図 2，IP_{netA}）宛のパケットは無視する．しかし，各研究室員のネットワークに利用されているスイッチの全ポートをミラーリングしたトラフィックを Honeyd サーバで受信し，そのうち研究室内の未使用 IP アドレスが宛先のパケットを Honeyd の入力である TAP デバイスに書き込んでいるので，未使用 IP アドレスである IP_{netA} 宛のパケットは IP_{netA} が設定された仮想ホストをもつ Honeyd が処理し，実際の TCP/UDP のサービスを行っているホスト B に中継し，その応答を自身のルータに送信している．

表 1 TAP デバイスのスループット

ルータ A – Honeyd サーバの TAP デバイス	638.7 Mbps
ルータ A – Honeyd サーバの物理デバイス	932.0 Mbps

表 2 Honeyd サーバの環境

CPU	Inter Core i5-650 3.2GHz x4
Memory	2GByte(DIMM Synchronous 1333 MHz 1GB x2)
NIC	Intel PRO/1000 (e1000e ドライバ)
OS	Linux 2.6.32 504.1.3.el6.x86_64 (CentOS 6.3)
Honeyd	Honeyd-1.5c

4.1.2 IP アドレスの使用状況調査実験

この実験では研究室の未使用 IP アドレスを把握した．各研究室員が利用している機器の IP アドレスの使用状況を調査するため，スイッチの全ポートのミラーポートに接続された Honeyd サーバ上で 3.2.3 節のシステムを稼働させた．さらに，研究室ゲートウェイの下には他に研究室の HTTP サーバや DNS サーバが属するネットワークとのゲートウェイであるルータもあるため，3.2.5 節のシステムを稼働させて，そのルータの ARP テーブルを参照し，それらの使用状況も把握した．実際の使用状況の確認は各研究室員が明らかにしている機器の使用状況との比較や ICMP による疎通確認によって行った．

4.1.3 TAP デバイスのスループット測定実験

本研究では，Honeyd の入力に仮想デバイスを用いており，入力部をソフトウェア化することによるスループットの低下が実際の運用に問題にならないかどうか検証するため，試作した収集システムの TAP デバイスのスループットを測定した．Honeyd サーバ上で iperf をサーバとして動作させ，ルータ A から iperf をクライアントとして IP_{netA} 宛のパケットを送信するように動作させた．また，TAP デバイスに書き込んだ iperf のパケットを OS が処理できるようにするため，TAP デバイスの RPF[*5] を無効にし，TAP デバイスの IP アドレスに IP_{netA} を設定した．さらに比較のため，通常の通信であるルータ A と Honeyd サーバの物理デバイス間のスループットも測定した．

4.2 試作した収集システムの性能

4.2.1 TAP デバイスのスループット

4.1.3 節の構成で測定したスループットを**表 1** に示す．また，このときの Honeyd サーバの環境を**表 2** に示す．

4.2.2 Honeyd のプロキシ機能使用時の性能

試作したシステムで未使用 IP アドレス（図 2，IP_{netA}）宛に通信を試みた場合，収集システムの中継先のホストと

[*5] Reverse Pass Forwarding

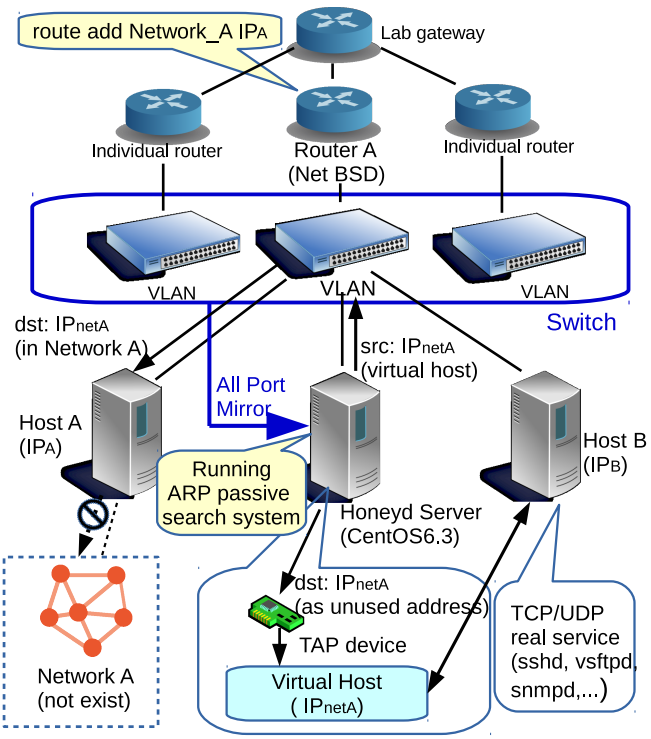

図 2　試作したシステムの概要図

の通信において，SSH や SNMP 等での TCP/UDP での送受信の成功を確認した．しかし，FTP 等で巨大サイズのデータを送信する際に，極端にスループットが低下し，ストールする現象が確認された．この現象は Honeyd サーバの IP アドレス宛にパケットを送信し，物理デバイスで受信したパケットを Honeyd の入力としたときにも確認されたので，Honeyd 自体の巨大サイズのデータのパケットに対する処理に問題がある可能性が高い．

4.2.3　IP アドレスの調査性能

4.1.2 の構成で，研究室内の使用中 IP アドレスの動的な把握に成功していることを確認した．ただし，本当にこのシステムで IP アドレスの衝突が避けられているかはまだ確認できていない．

5.　おわりに

本報告書で提示したシステムを研究室内で試作し，稼働させたところ，研究室ネットワークの IP アドレス空間において，使用中の IP アドレスの動的な調査が可能であることが分かった．ただし，本研究では実際に本システムによって IP アドレスの衝突を避けられるかという検証はまだできておらず，試作したシステムを学内全域に拡張した上で，どの程度の衝突が起きるか調べる必要がある．また，本システムにおける Honeyd サーバの入力である TAP デバイスのスループットは 1Gbps の物理デバイスの約 70%の性能を記録した．しかし，実際の運用を考えてより高性能の NIC を利用した場合の性能の調査が必要である．また，Honeyd の巨大サイズのパケットに対する処理に不具合がある可能性が高く，現状では巨大サイズのパケットの収集が難しい状況にある．今後の課題として IP アドレスの使用状況を調査するシステムの精度を高めるため，学内の IP アドレスの実際の使用状況の傾向などを調査する必要もあると考えられる．また，収集システムで攻撃を誘い込んでいる IP アドレスが学内で使われ始めたときに，そのホストが攻撃にさらされることが懸念されるため，その攻撃に対する対応策も必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す．

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] Artail, H., Safa, H., Sraj, M., Kuwantly, I. and Al-Masri, Z.: A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks, *Computers & Scurity*, Vol. 25, No. 4, pp. 274–288 (2006)．
[8] Provos, N.: Developments of the Honeyd Virtual Honeypot, Niels Provos (online), available from ⟨http://www.honeyd.org/⟩ (accessed 2014-11-28)．
[9] Brini, D.: Tun/Tap interface tutorial, backreference (online), available from ⟨http://backreference.org/2010/03/26/tuntap-interface-tutorial/⟩ (accessed 2014-11-10)．