情報処理学会論文誌　Vol. 51　No. 3　1040–1046 (Mar. 2010)

サブネットワーク内の使用できないIPアドレスを用いたインターネット観測手法とその評価

桝田秀夫[†1]　竹内徹哉[†2,*1]

近年，インターネットに接続する機器の増加にともない，システムの脆弱性を突いた攻撃を受ける例が増加している．これらの攻撃に対し，インシデントやその予兆の観測や分析に関する研究を行うプロジェクトが多数運営されている．これらのプロジェクトでは，より正確な分析結果を得るため，観測ボックスをインターネット上の様々なIPアドレスへ設置することが望まれている．一方，インターネットに接続する機器の増加から，現行のIPv4ではIPアドレスの枯渇が問題となっている．そのため，観測ボックス専用にIPアドレスを使用してしまうことが難しくなってきている．そこで本研究では，IPアドレスを無駄に使わずに観測できる仕組みとして，サブネット内で使用されないネットワークアドレスやブロードキャストアドレスを用いて観測を行う手法を提案した．本手法を，インターネット観測プロジェクトの1つであるWCLSCANの観測ボックスとしても動作するルータとして実装し，そのオーバヘッドの評価を行った．その結果，観測ボックスが稼動したことによる転送処理性能の低下は見られず，攻撃を観測している場合においても転送処理性能の低下は見られなかった．

Implementation and Evaluation of Internet Observation Sensor System Using Unusable IP Address inside a Subnet

Hideo Masuda[†1] and Tetsuya Takeuchi[†2,*1]

Recently, many projects that concern the Internet observation and analyze the incident of the Internet have been managed to Internet attacks. In such observation projects, to obtain more accurate analysis is required many observation sensor box as possible. Therefore, the observation sensor boxes require many IPv4 addresses, but the IPv4 addresses are costly due to shortage. In this paper, we propose that observation sensor box integrates into Linux router. Our sensor box for WCLSCAN acts as a router and watches packets to network address and/or broadcast address of inner LAN. As a result, performance is almost same as normal router.

1. はじめに

近年，情報の流通速度が速まったことによって脆弱性の発見からexploitコードや攻撃コードの出現までの期間は非常に短くなっている．これに対抗し広域を攻撃するインシデントを早期発見するために，攻撃のシグニチャの基になるデータを明らかにする必要性が求められている[1)]．そのためにインターネット上の大量のパケットを収集し，分析を行うプロジェクトが運営されている．たとえば，警視庁のインターネット定点観測システム[2)]では，全国の警察施設に設置されたIDSおよびファイアウォールにおける検知状況の結果から，「インターネット治安情勢」を毎月公表している．また，SANSのInternet Storm Center（ISC）[3)]では，世界50カ国以上で合計500,000個以上のIPアドレスを用いて観測を行っている．ほかにも，Telecom-ISAC Japan[4)]の広域モニタリングシステム，IPAのTALOT2[5)]，JPCERT/CCのISDAS[6)]，Dshield.orgのDistributed Intrusion Detection System[7)]，CAIDAのTelescope Analysis[8)]などが知られている．

これらのプロジェクトのほとんどは，インターネット上に多数の観測点として専用のIPアドレスを確保し，モニタリングを行う装置（観測ボックス）を設置する必要がある．観測ボックスは，通常それぞれがインターネット上において特定のIPアドレスを持ち，このIPアドレスに対して送られてくるパケットを観測し，ログデータなどの収集を行う．このため，各観測ボックスは特定のIPアドレスを占有して利用する必要がある．そして，各観測ボックスが収集したデータをサーバで集約し，統計，解析といった処理を行うことにより，インターネット上の攻撃行動の推定などを行っている．より正確な推定を行うためには，観測ボックスをインターネット上のIPアドレス空間の中に，できるだけ偏りなく，かつ，多数設置することが望ましい．

一方，現在インターネット上で用いられているプロトコルのIPv4（Internet Protocol version 4）ではIPアドレスは32 bitで表し，その総数は約43億個である．近年インターネットに接続する機器が増加した結果，近い将来にはIPv4におけるIPアドレスが枯渇する

†1 京都工芸繊維大学情報科学センター
Center for Information Science, Kyoto Institute of Technology
†2 京都工芸繊維大学工芸学部電子情報工学科
Department of Electronics and Information Science, Kyoto Institute of Technology
*1 現在，株式会社エヌ・ティ・ティ ネオメイト
Presently with NTT Neo-Mate Co., Ltd.

と考えられている[9]．そこで CIDR（Classless Inter-Domain Routing）を用いてサブネットマスクを分割して指定することで IP アドレスを効率的に使用する，NAPT（Network Address Port Translation）を用いることで複数のホストに 1 つの IP アドレスを割り当てるといった方法がとられている．

しかし，上記のようなサブネット分割や NAPT を用いた方法で効率的に IP アドレスを使用していても，今後の IP アドレスの枯渇は避けられないものとなっている．将来的には IP アドレスを 128 bit に長くすることによって，IP アドレスの総数を増やした次世代のプロトコルである IPv6（Internet Protocol version 6）への移行が考えられているが，現在のところはまだ実験や商用化が始まった段階である．そのため，現状では IP アドレスは非常に高価な資源になり，観測ボックスを多数設置することは難しいものとなっている．

そこで本研究では，観測ボックスをできるだけ多数配置する際に障害となりうる，（通常使用可能な）IPv4 アドレスの枯渇問題を少しでも緩和するために，無駄となっている IP アドレスを活用した観測システムの開発とその実現可能性の評価を行うことを目標とする．この目標のために，いくつか存在するインターネット観測システムの中で，共同研究を行っている WCLSCAN（Wide area Common Log Scanner）プロジェクト[10] を実例にとり，サブネット分割された内部ネットワークのルータに観測ボックスの機能を実装し，外部ネットワークからは使用できない IP アドレス，つまりネットワークアドレス，およびブロードキャストアドレスを用いて観測を行う手法を示し，観測ボックス機能を実装した場合のルータの性能評価を行う．

2. アイディア

まず，本研究で対象とする WCLSCAN プロジェクトの全体のシステム構成を**図 1** に示す．WCLSCAN プロジェクトは，鈴木裕信氏を中心に企業や大学からのボランティアにより支えられている研究プロジェクトである．WCLSCAN はインターネット上に設置した特定の IP アドレスを持つ複数の観測ボックスで観測されるポートスキャンのログをログサーバに収集し，ベイズ推定に基づいてインターネット上の広域的なネットワーク攻撃の活発化による危険性を解析し，それを自動的に通知，公表するシステムとなっている．

本研究では，観測ボックスをできるだけ多数配置する際に，障害となりうる（通常使用可能な）IPv4 アドレスの占有状態を可能な限り緩和するための手法の開発を目標とする．そのために，サブネット分割を用いた内部ネットワークの構成について検討する．

内部ネットワークにおけるネットワークアドレスとブロードキャストアドレスには特別な

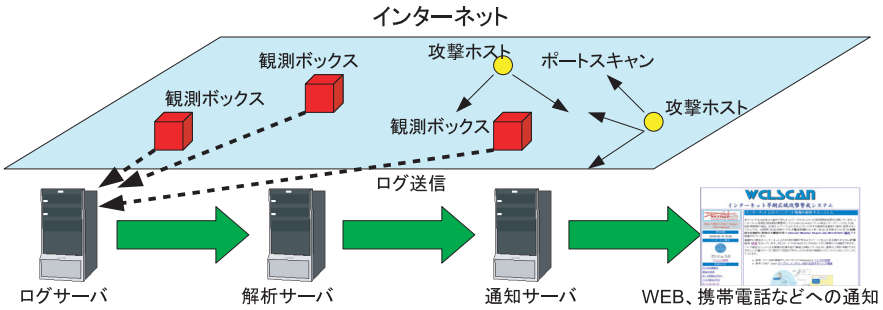

図 1　WCLSCAN の構成図
Fig. 1　Framework of WCLSCAN.

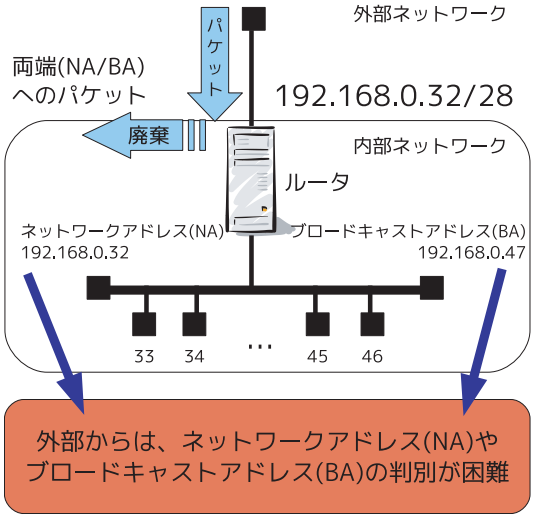

図 2　サブネット分割されたネットワーク
Fig. 2　Example of subnetted network.

役割があるため，ホストにこれらのアドレスを付与することはできない．ネットワークアドレスはネットワークの識別に用いられ，ブロードキャストアドレスはネットワークに所属するホストにブロードキャストを用いて通信を行う際に利用される．ここで，例として**図 2** のように 192.168.0.32/28 でのネットワークについて考える．この場合，ネットワーク内の

使用可能な IP アドレスは 192.168.0.32 から 192.168.0.47 までとなる．そのうち，ネットワークアドレスは 192.168.0.32，ブロードキャストアドレスは 192.168.0.47 である．この場合においても，ネットワークアドレスとブロードキャストアドレスをホストに付与することはできない．しかし，外部から見ると 192.168.0.32 や 192.168.0.47 といったアドレスが，ネットワークアドレスやブロードキャストアドレスであるかを判別することは難しく，ホストに付与した IP アドレスであるかのように見える．そのため，これらのネットワークアドレスやブロードキャストアドレスを用いて観測を行うことが可能であると考えられる．

また，図 2 での内部ネットワークに対して，外側からネットワークアドレス 192.168.0.32 やブロードキャストアドレス 192.168.0.47 を宛先とするパケットが送られると，この内部ネットワークのルータまで到達する．そして，ルータによってパケットが破棄される．ブロードキャストアドレスは内部ネットワークでは使用されるが，このアドレスに対して外部からパケットがやってくることは通常考えられない．そのため，観測を行うためにルータの外側のインタフェースを用いることに問題はないと考えられる．

以上により，ネットワークアドレスやブロードキャストアドレスを用いてルータに実装された観測ボックスによる観測を行うことができるならば，観測ボックスを設置する環境の拡大が期待される．また，この観測に使用する IP アドレスは，この内部ネットワークと外部ネットワークを接続するルータにとっては別途設定することなく自動的に導出できるので，ルータに組み込むことができれば，観測ボックスの設定管理が非常に容易となることも期待できる．

3. 要　　求

本章では，観測ボックスをルータに組み込む際の要求についてまとめる．

まず，観測ボックスはネットワーク内のネットワークアドレスおよびブロードキャストアドレスを用いてパケットの観測を行うことができる必要がある．それ以外のパケットに関してはルータ機能によって正しくルーティングを行わなければいけない．この際，ブロードキャストアドレスは内部ネットワークのホストが利用するため，内側インタフェースでのブロードキャストアドレスへの通信は観測を行ってはならない．

また，実際に運用する際には観測ボックスを実装したことによってルータの性能が低下することはできるだけ避けなければならない．ルータの主な目的はルーティングを行い，目的のホストへ正しくデータを受け渡すことであるので，その転送性能が極力低下しないようにする必要がある．

以上の要求を満たすことができれば，運用上の問題が発生しない観測ボックスのルータへの実装が行うことができると考えられる．

4. 実　　装

本稿では，WCLSCAN [11] が公開している観測ボックスを Debian GNU/Linux [13] 上で構築し，それにルータ機能の追加と，観測データの収集設定を変更することで実装した．

オリジナルの観測ボックスは，iptables [14] を用いて，ログサーバとの通信以外のすべてのパケットをフィルタし，それらを記録する，という形で実装されている．

iptables は，Linux で広く使用できるパケットフィルタリングシステムであり，主にパケットがシステムに入ってくる部分（Chain INPUT），転送処理をする部分（Chain FORWARD），システムから出てくる部分（Chain OUTPUT）のそれぞれに対して，フィルタリングルールを記載することができ，ルールに対してアクションが指定できる．オリジナルの観測ボックスでは，Chain INPUT に対して，ログサーバとの通信だけを受け入れ（ACCEPT）と指定し，それ以外のすべてのパケットについて LOG と指定したうえで DROP とするこ

```
01 #!/bin/sh
02 #
03 # iptables の初期化
04 iptables -F INPUT
05
06 # ログサーバとの通信を許可（133.16.XXX.XXX はログサーバのアドレス）
07 iptables -A INPUT -s 133.16.XXX.XXX --protocol tcp --sport YY \
       --dport 1025:65535 -i eth1 -j ACCEPT
08
09 # ログをとる IP アドレスの設定（内部側：eth0，192.168.0.160/28）
10 ## ブロードキャストアドレスは外部からのパケットのみログをとる
11 iptables -A INPUT -d 192.16.0.160 -j LOG --log-level debug
12 iptables -A INPUT -d 192.16.0.175 -i eth1 -j LOG --log-level debug
13
14 ## ログをとったパケットは破棄する
15 iptables -A INPUT -d 192.16.0.160 -j DROP
16 iptables -A INPUT -d 192.16.0.175 -i eth1 -J DROP
17
18 # それ以外のパケットは通信を許可する
19 iptables -A INPUT -j ACCEPT
```

図 3　/etc/rc.boot/iptables-reject の内容
Fig. 3　Code of /etc/rc.boot/iptables-reject.

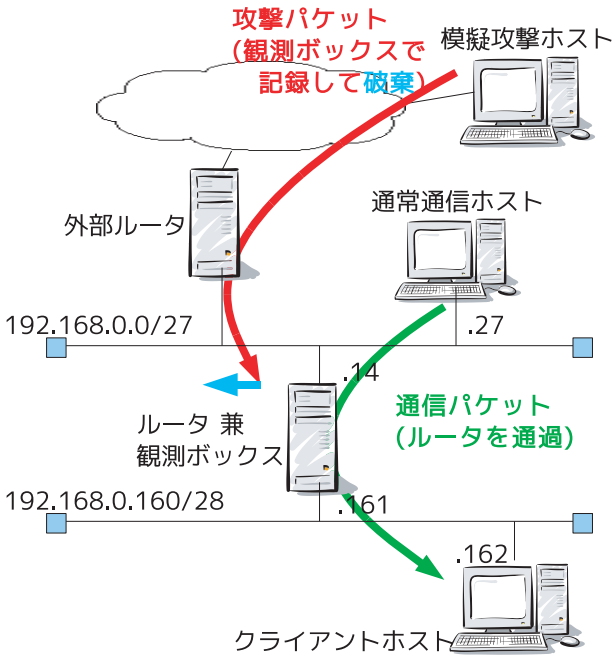

図 4　測定ネットワークの構成
Fig. 4　Configuration of evaluation network.

表 1　実験に用いたルータのスペック
Table 1　Specifications of Router hardware.

OS	Debian GNU/Linux 4.0 r0
CPU	Intel PentiumIII 933 MHz
メモリ	512 MB SD-RAM PC13
HDD	40 GB IDE 100 ATA
NIC	Intel Pro/100 NIC × 2

表 2　測定に使用したマシンのスペック
Table 2　Specifications of Evaluation service.

通常通信ホスト	Intel PentiumIII 866 MHz × 2 512 MB RAM 250 GBHDD × 4 RAID10 Intel Pro/100 NIC
模擬攻撃ホスト	AMD K6-III 450 MHz SD-RAM PC133 E-IDE HDD (UltraATA-33) Vine Linux 3.2 Intel Pro/100 NIC
クライアントホスト	Intel PentiumIII 1333 MHz 384 MB SD-RAM PC133 IDE 37 GB (ST340810A)) Debian GNU/Linux 4.0 r0 Intel Pro/100 NIC

とで，記録を残しつつパケット自体は破棄するようになっていた．

そこで，この設定を変更し，外部向けインタフェースに限定して，内部向けインタフェースのネットワークアドレス，およびブロードキャストアドレス宛のパケットを記録し，またルータとして機能するため，それ以外のパケットは破棄（DROP）せずに処理する（ACCEPT）するという形に変更した．編集後のこのファイルを**図 3** に示す．

この設定を施したうえで，**図 4** の構成で観測すると設定した IPv4 アドレス宛のパケットが，当該インタフェースまで到達しログに記録されることを確認できた．

5. 性 能 評 価

本章では，実装したルータ機能付き観測ボックスを使用する場合に，観測ボックス機能がルータ機能に与える影響を，ルータを通過するデータの転送に要する時間を測定することで，その評価を行う．性能評価に用いた機器のスペックを**表 1**，**表 2** に示す．

5.1　転送時間の測定

本稿での性能評価は，図 4 中にある通常通信ホストと内部ネットワークとなる 192.168.0.160/28 のネットワーク内のクライアントホストとの間で，通信トラフィックを発生させた場合の通信に要する時間を指標とした．通信トラフィックとしては ftp を用い，各サブネットは 100BASE-TX のスイッチを使用している．

また，観測ボックスの構成上，外部ネットワークから到着するパケットは iptables によるパケットの峻別とログ記録が行われるが，内部ネットワークから到着するパケットは基本的にそのまま転送されることから，トラフィックの流れる方向によって性能に差違がある可能性がある．そのため，転送時間の測定は，主に通常通信ホストからクライアントホストにトラフィックが流れる（ftp における GET）ダウンロード時間と，主にクライアントホスト

から通常通信ホストに流れる（ftp における PUT）アップロード時間のそれぞれで実施した．通常通信トラフィックの発生方法は，以下のコマンドを用いて作成したランダムな内容を持つ 20 MB のファイル（testfile）を，PUT を用いて通常通信ホストにアップロードする操作と GET を用いてクライアントホストにダウンロードする操作を交互に 150 回ずつ，総計 300 回連続して実施することで行った．

```
# dd if=/dev/urandom of=testfile bs=20M count=1
```

そのうえで，ダウンロードとアップロードの個別の転送時間を ftp コマンドのステータス情報から入手した．この転送時間データから，ダウンロード時間の平均値を平均受信時間，アップロード時間の平均値を平均送信時間として求める．ftp コマンドのステータス情報は，100 分の 1 秒単位で表示されている．

さらに，観測ボックスがログサーバと通信を行う間隔は 5 分ごと（オリジナルの観測ボックスでは 10 分間隔）に設定した．理論上，100 Mbps の通信回線を用いて 20 MB の転送にかかる時間は 1.6 秒となるので，300 回の実施中に少なくとも 1 回はログサーバとの通信が行われると考えられる．

これらの通信トラフィックのルーティング処理だけであれば，観測ボックスとしての記録は発生しないため，記録を取るオーバヘッドはほとんどない．そこで，観測ボックスとしての処理を行いながらルータ処理をする場合の影響を評価するために，模擬攻撃サーバから観測用 IP アドレスに向けて，以下のようなコマンドを用い，攻撃トラフィックを発生させた．

```
# dd if=/dev/urandom | socat - udp:192.168.0.160:10000
# dd if=/dev/urandom | socat - udp:192.168.0.175:10000
```

このコマンドによって，ランダムな内容を持つデータを，観測ボックスの udp のポート 10000 に対して継続的に送付することができる．

5.2　測定実験群の設定

観測ボックス機能の影響を評価するために，観測ボックス機能のない通常のルータとして動いている場合（未稼動）と，観測ボックス機能を付加した場合（観測稼動）の 2 通り，またそれぞれに対して，通常通信トラフィックだけが流れている場合（攻撃なし）と，それに加えて攻撃トラフィックも同時に発生している場合（攻撃あり）の 2 通り，合計 4 通りの場合について測定を行った．

観測ボックス機能の有無は，iptables の設定を有効にするか無効にするかで制御をすることができるものとした．

表 3　各測定実験群における平均送信時間および平均受信時間
Table 3　Mean time of send/receive transfer against attack or not.

条件	平均送信時間	平均受信時間
(a) 未稼働 - 攻撃なし	1.80 秒	1.91 秒
(b) 観測稼動 - 攻撃なし	1.80 秒	1.91 秒
(c) 未稼働 - 攻撃あり	1.81 秒	2.07 秒
(d) 観測稼動 - 攻撃あり	1.81 秒	2.07 秒

5.3　測 定 結 果

観測ボックス機能の有無と攻撃トラフィックの有無による，4 通りの条件における平均受信時間，平均送信時間の測定結果を**表 3** に示す．

この結果から，攻撃トラフィックがない場合に，観測ボックス機能が稼動していない場合 (a) と稼動している場合 (b) の平均受信時間，平均送信時間ともにほとんど変化がなかったことが分かる．これにより，観測ボックス機能がログサーバと通信を行うことによるルータ機能への影響は非常に小さいと考えられる．一方，攻撃トラフィックがある場合に，観測ボックス機能が稼動していない場合 (c) と稼動している場合 (d) を比較すると，こちらも平均受信時間，平均送信時間ともにほとんど変化が見られなかった．そのため，観測ボックスがログを収集したことによるルータ機能への影響も非常に小さいと考えられる．平均送信時間よりも平均受信時間の方が攻撃トラフィックの有無による影響が大きく出ている理由は，観測用 IP アドレスに到着する攻撃トラフィックが外部ネットワークへの 100BASE-TX のリンクに重畳されるため，ダウンロード側のトラフィックに大きな影響が出たと考えられる．

次に，測定結果から実際に観測ボックスを運用した際の影響について検討する．今回の測定では，観測ボックスへ直接攻撃を行っているような状況を作り上げており，その場合においてもルータ性能には大きな影響は見られなかった．実際の観測ボックスの運用環境では観測ボックスが直接攻撃を受ける状況は考えにくく，観測できる攻撃パケット数は今回の測定での状況よりも少ないと予想される．

また，本研究で用いたルータ PC は，ネットワークのルーティングを行うために特別なチューニングを行ってはいない．しかし，実際に用いられているルータは，転送性能，ルーティング性能を向上させるためにチューニングを行っている．チューニングが行われていない PC で今回の測定結果が得られたため，実際のルータにおいては観測ボックスの実装による影響は小さくなると考えられる．

以上のことを考慮すると，実際に観測ボックスを実装して運用を行った場合，観測ボック

ス機能によるルータ機能への影響は，今回の測定よりもさらに小さいものになると考えられる．

6. 考　　察

本研究により，観測ボックスをルータに組み込むことによって，サブネット分割されたネットワーク内のネットワークアドレスおよび，ブロードキャストアドレスを用いた観測を行うことが可能であることが分かった．この結果から，ネットワーク内で使用されていない IP アドレスを用いて観測を行うことにより，インターネット上に観測ボックスを設置する環境を増やし，より多くのデータ収集を行うことを可能にするという部分においては本研究の目的を達成したと考えられる．

また，観測ボックスを組み込んだ場合に，ルータの転送性能への影響もほとんど見られないということが分かった．そして，実際の運用上においては，観測ボックスの影響はさらに小さくなると考えられる．

しかし，観測ボックスを実装することによる影響がほとんど見られないという結果が得られたが，実ネットワークのどのレイヤのルータに対しても問題がないかは現時点では不明である．たとえば，会社や学校などの大規模なネットワークの基幹ルータなどに観測ボックスを設置すると，ルータを経由するデータ量が多く，また多数のコンピュータとの間でデータのやりとりが行われるため，ネットワーク内の広範囲のコンピュータに影響を及ぼす可能性があるため，このようなルータに観測ボックスを設置することは難しくなることが予想される．

このようなルータに観測ボックスを実装するには，ルータ機能への影響が生じるのを回避するために，さらに観測ボックスによるルータへの影響を小さくする必要があり，より高性能・高速な NIC への対応や，メモリやディスクの消費量などを極力小さくするといった改良を行うことが求められると考えられる．

一方，ネットワークの末端に位置するルータでは経由するデータ量，接続されている PC の台数がどちらも少ないため，今回の評価環境に近く，観測ボックスを設置しても内部のネットワークへの影響は少ないと予想される．そのため，観測ボックスの実装とその運用は，末端に位置するルータに組み込むことが望ましいと考えられる．現時点では，WCLSCAN のような研究者・ボランティアベースのプロジェクトの場合，影響範囲が狭い方が理解が得やすい面もあると予想される．

以上より，ルータの設置されている環境とその使用状況，また観測ボックスを実装することによる影響について考慮を行ったうえで，実際の観測ボックスの実装，およびその運用を行うことを検討していく必要がある．

7. 関 連 研 究

インターネット観測システムでは，インターネット上でいっさいのネットワークサービスを提供しない IP アドレス（dark IP）に到達するアクセスパケットの観測を行う．文献 15) では，インターネット観測システムにおいて，定点観測用センサをおかず，ルータやスイッチで収集されるネットワーク・フローを利用して dark IP を割り出して利用する方法を提案している．また，使用されていない IP アドレスを用いてネットワークに対する攻撃行動を検出する研究として，文献 16)，17) などがある．これらの方式は，ネットワークサービスを提供しない IP アドレスを利用するという観点で本研究と類似している．

しかし，本研究で観測に使用する IP アドレスは確実にインターネット側との通信を行わないことが保証できるが，文献 15) の手法は，観測時にたまたま通信がなかっただけであり，本当に dark IP であるのかは保証できない．また，文献 16)，17) では，本来なら通常使用可能ではあるがその時点で使われていない IP アドレスに着目している点で異なる．

8. ま　と　め

本研究ではインターネット上のインシデントやその予兆の観測や分析を行う WCLSCAN プロジェクトの観測ボックスについて，サブネット分割されたネットワーク内の不使用 IP アドレスを用いて観測する手法を適用し，その性能評価を行った．その結果，ルータに観測ボックスを組み込むことによる影響は非常に少ないという結果が得られた．

今後の課題としては，ブロードバンドルータなど省リソースデバイスへの適用が考えられる．

参　考　文　献

1) 鈴木裕信：ポートスキャンログからみたインターネットセキュリティの一考察，ソフトウェア技術者協会ソフトウェアシンポジウム 2001 (2001).
2) 警察庁，インターネット定点観測システム@police. http://www.cyberpolice.go.jp/detect/observation.html
3) SANS，Internet Storm Center. http://isc.sans.org/
4) 財団法人データ通信協会，Telecom-ISAC Japan. https://www.telecom-isac.jp/
5) 独立行政法人情報処理推進機構セキュリティセンター，インターネット定点観測

（TALOT2）.
http://www.ipa.go.jp/security/txt/2005/documents/TALOT-0502.pdf
6) JPCERT コーディネーションセンター，インターネット定点観測システム（ISDAS）.
http://www.jpcert.or.jp/isdas/
7) Dshield.org, Distributed Intrusion Detection System.
http://www.dshield.org/indexd.html
8) The Cooperative Association for Inter Data Analysis, Network Telescope Research.
http://www.caida.org/research/security/telescope/
9) JPNIC：IPv4 アドレス在庫枯渇問題に関する検討報告書（第一次）(2007.12).
http://www.nic.ad.jp/ja/ip/ipv4pool/ipv4exh-report-071207.pdf
10) 鈴木裕信，石黒正樹，村瀬一郎，大野浩之：インターネット早期広域攻撃警戒システム WCLSCAN，ソフトウェア技術者協会ソフトウェアシンポジウム 2004 (2004).
11) WCLSCAN プロジェクト．http://www.wclscan.org/
12) 石黒正揮，鈴木裕信，村瀬一郎，大野浩之：ベイズ推定に基づくインターネット攻撃検知システムの開発，電子情報通信学会暗号と情報セキュリティシンポジウム（SCSI2004）(2004).
13) Debian GNU/Linux. http://www.debian.org/
14) Linux IPv4 packet filtering. http://www.netfilter.org/projects/iptables/
15) 下田晃弘，後藤滋樹：広域ネットワークにおけるフロー解析に基づく脅威検出法，第 6 回情報科学技術フォーラム，LL-001, pp.365–366 (2007).
16) 鈴木和也，馬場俊輔，高倉弘喜：未利用アドレスブロックに到達するトラフィックの解析，信学技報，IA2005-23, pp.25–30 (2006).
17) 武蔵泰雄，松葉龍一，杉谷賢一：DNS 解決 PTR レコード分散型サービス妨害攻撃の自動検知と自動阻止システムの開発，情処学会研究報告，2004-DSM-34，pp.43–48 (2004).

(平成 21 年 6 月 19 日受付)
(平成 21 年 12 月 17 日採録)

桝田　秀夫（正会員）

1970 年生．1998 年大阪大学大学院基礎工学研究科物理系専攻情報工学分野博士後期課程修了．1998 年より大阪大学情報処理教育センター助手．2000 年より大阪大学サイバーメディアセンター情報メディア教育研究部門助手を経て，2005 年より京都工芸繊維大学情報科学センター助教授（現，准教授）．分散システムの運用管理技術に関する研究に従事．博士（工学）．平成 18 年度情報処理学会山下記念研究賞受賞．電子情報通信学会，ACM 各会員．

竹内　徹哉

1985 年生．2008 年京都工芸繊維大学工芸学部電子情報工学科卒業後，株式会社 NTT ネオメイトに入社．現在は，NTT における NGN 網の装置開発に従事．