経路情報を用いたパケットフィルタリングによるIPアドレス詐称対策

中野 学[†] 松本 勉[†]

発信元IPアドレス詐称対策に関して，送信側がパケットの発信元IPアドレスを監視し，発信元IPアドレス詐称をともなったパケットを破棄するという方式は有効である．しかし，その実現のためには対策を行うネットワークに則したフィルタリングルールが必要であり，その設定を適切に行うためには管理者の手間がかかる．本論文では，ルータが経路情報を利用して自動的にフィルタリングルールを作成することにより，フィルタリングルール作成における管理者の手間を削減するというアイディアを示している．また，正確な経路情報に基づいたルールを作成するために，経路情報の正当性を確認する手順を入れることによって，さらに信頼性のある発信元IPアドレス詐称対策のアイディアを提案している．

Routing Information Based Packet Filtering for IP Spoofing Prevention

Manabu Nakano[†] and Tsutomu Matsumoto[†]

As one of the effective measures against IP address spoofing, there is a way for a network administrator not to pass outside the packet of which source IP address is misrepresented, by means of the packet filtering. For that purpose, it is important to set up the newest filtering rule that reflects pertinently the change in the network that is the target of management. This paper proposes how to make the suitable filtering rule by using routing information, and it proves measures against IP source address spoofing which an administrator can perform efficiently.

1. はじめに

近年のネットワーク構築技術の進歩により，ネットワークを介して行われるサービスは年々増加傾向にある．しかし，一方でネットワーク管理者が行わなければならない作業も，サービスの増加に比例して煩雑になりつつある．最近はネットワークセキュリティも重視されるようになり，ネットワーク攻撃への耐性を考えたうえで，各種サービスを維持する必要がある．

ネットワークセキュリティにおける防護技術には一般に限界があり，各サーバの管理者がセキュリティ対策を行うだけでは防げない攻撃も存在する．また，ユーザのモラルの低下により，内部ネットワークから攻撃者が現れる可能性も高まる傾向にある．このような状況の中で，各ネットワーク管理者はそれぞれの管理するネットワークから，他者を攻撃するパケットを外部に出さない努力が必要である．しかし，ネットワーク管理者の多くはサービスの維持などの仕事をかかえている場合も多く，セキュリティ対策に多くの労力を割くことが困難であることも多い．

本論文では，パケットフィルタリングを利用した発信元IPアドレス詐称対策について論じる．パケットを受信する側だけでは防げない問題であるIPアドレス詐称という問題に対し，その防御策をなるべく少ない労力で行うためのアイディアを提案する．さらに，IPアドレス詐称攻撃を行う際に経路情報詐称攻撃が併用された場合も考え，セキュリティレベルの向上を目指した．

以後，2章でルータの役割とパケットフィルタリングについて述べる．3章では発信元IPアドレス詐称と経路情報詐称の問題と防御策について触れ，著者らが提案する発信元IPアドレス詐称の提案アイディアについて述べる．4章では提案アイディアのアルゴリズムを紹介し，そのアルゴリズムに従って実装を行った際の動作確認結果を記載する．さらに，5章で実装環境下での実験結果を提示し，問題点について考察を行い，6章でまとめと今後の課題について述べる．

† 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University

2. ルータの役割

本章では，ルータによるパケットの経路制御（ルーティング），経路情報，および，パケットフィルタリングについて説明する．

2.1 ルーティング

送信者の送信したパケットは，ルータ間を転送されながら受信者に届く．ルータがパケットを転送するときに，そのパケットに記載された宛先 IP アドレスに応じて，次にどのルータに転送すればよいのかを決める処理がルーティングである．ルータは周囲のネットワークのネットワークアドレスをルーティングテーブルに記録し，送られてきたパケットの転送先をルーティングテーブルに従って決定する．

経路情報の管理方式には，ルータが他のルータと情報を交換してルーティングテーブルを自動的に生成・更新する動的経路制御（ダイナミックルーティング）と，管理者が手作業で設定する静的経路制御（スタティックルーティング）の 2 通りの方式がある．どちらの方式であっても，ルータは送られてきたパケットの宛先 IP アドレスを参照して，経路情報の書かれたルーティングテーブルからパケットの最適な経路を選び，転送する．

ダイナミックルーティングのプロトコルには，RIP（Routing Information Protocol）[1),2)] や OSPF（Open Shortest Path First）[3)] などがある．

2.2 経路情報

経路情報とは，ルータがパケットを転送する際に参照する，周囲のネットワークのデータである．この経路情報はルーティングテーブルに記録されている．大規模なネットワークを構築しているシステムの多くは，動的経路制御方式を採用している．しかし，ルーティングプロトコルを利用した経路情報の構築は管理者の手間を削減するというメリットがある一方で，経路情報を改竄されるという危険性も存在する．静的経路制御方式では，経路情報を設定する際にネットワーク管理者が手作業で経路を入力する必要がある．そのため，ルータに何者かが侵入しない限り，外的な要因によって経路情報を改竄される危険性はない．

2.3 パケットフィルタリング

パケットフィルタリングとは，パケットのヘッダ情報などによってそのパケットを通すか破棄するかを判断・処理するシステムである．IP パケットの発信元 IP アドレスや宛先 IP アドレス，プロトコル番号，ポート番号などを監視し，管理者の決めるフィルタリングルールに従ってパケットの扱いを決定する．

3. 詐称攻撃

本章ではネットワーク中で行われる詐称攻撃の中でも，同時に行われることのある 2 つの詐称攻撃，IP アドレス詐称攻撃と経路情報詐称攻撃について述べる．

3.1 IP アドレス詐称

IP アドレス詐称とは，発信元 IP アドレスを偽ったパケットを生成し，送信することである．IP アドレス詐称により身元を隠された場合，詐称されたパケットの受信者が攻撃者を特定するのは困難である．なぜなら，一般的なパケットが持っている発信元の情報は発信元 IP アドレスだけであるため，IP アドレス詐称をともなう攻撃を受けた際に，被害を受けたホストがその発信元を探査するには，攻撃を受けたサーバにつながるすべての経路について，ログを頼りに 1 つ 1 つ遡っていく作業が必要とされるためである．

発信元 IP アドレスを自由に詐称できる攻撃者は，まったく無害の組織体からの攻撃をしているかのように見せかけることができる．攻撃を受けているシステムの管理者が，詐称された IP アドレスの示す攻撃元から来るすべてのトラフィックをフィルタリングした場合，詐称された IP アドレスを使っていた悪意のない正規ユーザのアクセスさえも遮断する可能性がある．

3.2 IP アドレス詐称対策

前節のように，IP アドレス詐称攻撃は受信側で防御することが難しい．これは発信元 IP アドレスの詐称を見分け，防御策を行うことが困難であることが原因である．そこで，詐称されたパケットを受け付けない方式ではなく，それぞれのネットワークから詐称されたパケットを出さない方式[4)] が提案されている．これは内部ネットワークから外部ネットワークにパケットを転送する際に，パケットの発信元 IP アドレスを確認し，内部ネットワークに存在しない IP アドレスを発信元 IP アドレスとしたパケットを破棄するという方式である．

3.3 経路情報による IP アドレス詐称対策

ここで，ルータが持つ経路情報を利用して IP アドレス詐称対策を容易に行うという提案アイディアについて述べる．

通常のルーティングでは，ルータはパケットを転送する際に宛先 IP アドレスだけを参照し，それに見合った経路に向けてパケットを転送している．しかし，ルータは経路情報を参照することによって，内部ネットワークのネットワークアドレスを知ることができる．それをもとに，不正な発信元 IP アドレスを持つパケットを内部から外部ネットワークに転送しないようにフィ

ルタリングルールを作成することにより，IP アドレス詐称対策が行える．動的経路制御方式を利用している場合，ネットワークの変化はルーティングプロトコルによって伝えられるので，提案方式を定期的に実行することにより，自動的にネットワークの変化に則したフィルタリングルールが構築される．

このアイディアを用いれば，IP アドレス詐称やパケットフィルタリングに詳しくない管理者でも，効率的に IP アドレス詐称対策が行える．しかし，フィルタリングルールの作成は，信頼できる経路情報に基づいて行わなければならない．

3.4 経路情報詐称

ダイナミックルーティングを利用しているネットワークでは，攻撃者がルータに偽の経路制御情報を送ることで，経路情報を改竄することが可能である．また，このような改竄が成功し攻撃者が目的を果たした後，攻撃者が新たに正しい経路制御情報を送信することにより，攻撃の痕跡を消すことが可能である．

ダイナミックルーティングプロトコルのほとんどは，経路情報の変化のログをとる機能を備えていない．そのため，経路情報詐称攻撃の行われていた時間が短時間であった場合は，管理者が攻撃途中に経路情報を確認しない限り，一時的に経路の改竄が行われていたことに気づくことは困難である．また，経路の変化の多いネットワークにおいては，経路情報の変化はつねに発生する可能性があり，その中から攻撃を判断することは難しい．

3.5 提案アイディアの経路情報詐称に対する脆弱性

経路情報詐称が行われている場合，提案アイディアを用いたとしても，改竄された経路情報をもとに誤ったフィルタリングルールが設定されるため，IP アドレス詐称のなされたパケットが外部ネットワークに流出する危険性がある．

すなわち，提案アイディアによる IP アドレス詐称対策が行われているルータを通して，発信元 IP アドレス詐称攻撃を行いたい攻撃者が，経路情報詐称を併用した攻撃を考えたとする．そのとき攻撃者は，経路情報詐称によって攻撃者が IP アドレス詐称に利用したい IP アドレスを含むネットワークが内部ネットワークに存在するとルータに誤認識させ，ルータが IP アドレス詐称のなされたパケットを破棄しないようにできる．また，攻撃後に経路情報を正しいものに戻しておけば，それに従ってフィルタリングルールも再構築されるので，IP アドレス詐称対策の行われたネットワークが，一時的に IP アドレス詐称攻撃可能になっていたことに管理者が気づくことも困難となる．したがって，提案アイディアによる対策をより安全なものにするためには経路情報詐称に対する耐性を強化する必要がある．

3.6 経路情報詐称対策

経路情報詐称には 2 通りあり，1 つは存在するネットワークを存在しないと詐称するものであり，もう 1 つは存在しないネットワークを存在すると詐称するものである．IP アドレス詐称に併用して行われるのは，後者の攻撃方法である．経路情報詐称が行われた場合，ルータの持つ経路情報には存在しないネットワークが書かれることになる．そこで，経路情報をフィルタリングルールに変換する前に，内部ネットワークの記述に関して，経路情報が正しいかどうかの確認をすれば，経路詐称に対する耐性を高めることができる．

提案実装手法では内部ネットワークの正当性の確認に，対策を行うマシンと指定ホスト間でパケットの送受信が行えることを調べる ping コマンドを利用した．この ping をルーティングテーブルに書いてあるネットワークに対してブロードキャストし，反応が返ってこない場合は警告を出し，該当するネットワークを発信元アドレスとするパケットを遮断する．反応が返ってくるネットワークに属する IP アドレスのみを通すようにフィルタリングルールを構築する．ping の反応が期待できないネットワークや，ネットワーク内に稼動しているホストが存在しない場合に関しての考察は，後ほど 5.5 節で詳しく述べる．

4. 提案方式のアルゴリズムと実装

本章では，まず提案実装手法の概略図（**図 1**）を示し，そのそれぞれについて説明する．提案アイディアによる IP アドレス詐称対策を行うためのアルゴリズム，利用したソフトウェア，このアルゴリズムの実装手順について述べる．最後に提案実装手法を実行することによって得られた動作結果を示す．

4.1 提案方式のアルゴリズム

ルーティングテーブルからパケットフィルタリングに必要な情報を取り出しそれをもとに IP アドレス詐称対策を行うためのアルゴリズムを以下に示す．

(1) 対策を行うルータのルーティングテーブルから，内部ネットワークのネットワークアドレスを抽出する．
(2) 抽出したネットワークアドレスが存在するか確認するために，それぞれのネットワークアドレスに対して ping を実行する．この際，反応がない場合には，ネットワークが存在しないと判断し警告を出す．

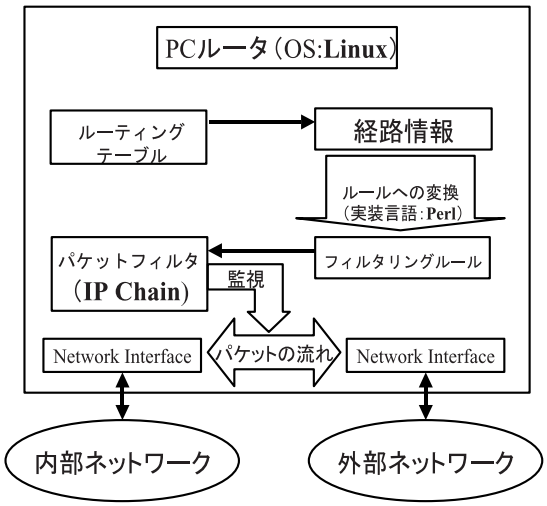

図 1 提案実装手法の概要
Fig. 1 Outline of the proposed method.

(3) 抽出したネットワークアドレスの中で，存在が確認されたネットワークから送られてきた IP アドレス詐称がなされていないパケットを通すフィルタリングルールを作成し，そのルールをパケットフィルタに設定する．

(4) 設定したフィルタリングルールに従って，パケットフィルタは転送するパケットの発信元 IP アドレスを監視し，IP アドレス詐称のなされたパケットを発見して破棄する．

(5) (1)〜(4) の動作を繰り返し行う．

このアルゴリズムによって，経路情報をもとにした適切なフィルタリングルールを動的に設定することができ，フィルタリングルールの設定の手間を削減することができる．

4.2 利用したソフトウェア

提案方式の実装環境として，PC ルータの OS として Red Hat Linux 7J を，またパケットフィルタリングツールとして IP Chain を用いた．提案方式を具現化する際のプログラムにはプログラミング言語 Perl を利用した．

IP Chain [5)]

IP Chain とは，Linux Kernel 2.2.X 以降で利用できるパケットフィルタであり，チェインという仕組みを使って，フィルタリングルールを鎖のように数珠つなぎにしてルールリストを作る．カーネルはパケットを受け取ると，この鎖のようにつながったルールに対して先頭から順番にパケットとルールのマッチングを行い，ルールに書かれた条件にあてはまる場合にそのパケットにルールに書かれた操作を適用する．

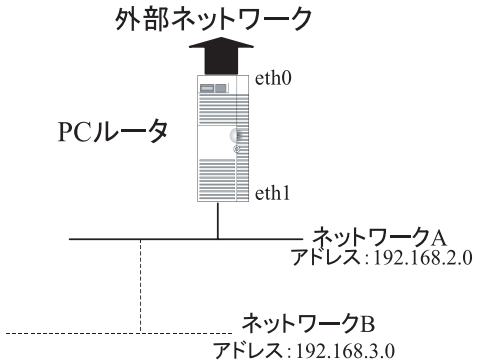

図 2 仮定したネットワーク
Fig. 2 The assumed network.

4.3 ルールの自動設定・更新プログラム

ここでは，提案方式の実装に利用したプログラムと，プログラムで行う手順について説明する．なお，例として**図 2** のようなネットワークを仮定し，PC ルータが内部ネットワーク（図 2 中：eth1 以下）に対して本提案実装手法を施した際の手順を図とあわせて示す．なお，この図の中でネットワーク B は，ネットワーク A の中にいる攻撃者によって経路情報詐称され PC ルータがその存在を誤認識させられている，実際には存在しないネットワークであるとする．

1）初期設定と仮定

提案方式では動的経路制御を利用したルータを想定しているが，PC ルータ内部のルーティングテーブルを利用するため，ルーティングプロトコルに依存しない．また，IP Chain の基本的ルールとして，先に forward（ルータでのパケット転送）というルールの中で許可が出されているパケット以外は通さないように設定しておくとする（policy REJECT）．したがって，フィルタリングルールにより許可されたパケットのみ転送される．

2）経路情報の取得

ルーティングテーブルの中の経路情報を走査し，インタフェースが内部ネットワークにつながるイーサカードと同じである経路情報を取り出し，そのネットワークアドレスとサブネットマスクの値をリストに入れる．

3）ネットワークの確認

リストにあるネットワークに対して，ネットワークコマンド ping を実行し，記述されているネットワークが本当に存在するかどうかを確かめる．このとき，反応が返ってこなかったネットワークに関しては，存在しないものと判断し，警告を出すとともにリストから削除する．

```
[root@Darjeeling /root]# /sbin/ipchains -nL
Chain input (policy ACCEPT):
Chain forward (policy REJECT):
Chain output (policy ACCEPT):
[root@Darjeeling /root]#
[root@Darjeeling /root]# perl chain10.pl
WARNING: pinging broadcast address
192.168.3.0   is bad route

[root@Darjeeling /root]# /sbin/ipchains -nL
Chain input (policy ACCEPT):
Chain forward (policy REJECT):
target     prot opt     source               destination          ports
ACCEPT     all  ------  192.168.2.0/24       0.0.0.0/0            n/a
ACCEPT     all  ------  0.0.0.0/0            192.168.2.0/24       n/a
Chain output (policy ACCEPT):
[root@Darjeeling /root]#
```

図 3 動作確認結果
Fig. 3 The result of experiment.

4）ルールへの変換

リストに残った経路情報からネットワークアドレスとサブネットマスクを取り出し，IP Chain のフィルタリングルールに変換する．経路情報と IP Chain では，サブネットマスクの表記方法が違うため，サブネットマスクを IP Chain 用の値にすることも，この変換に含まれる．

なお，提案実装手法のプログラムではフィルタリングルールを「内部ネットワークに含まれる発信元 IP アドレスを持ったパケットであればすべて転送する」としている．内部ネットワークから送られるパケットのサービスも限定したい場合には，このルールに使用を許可するプロトコルを書き加えることにより行える．

5）フィルタリングルールの更新

最後にフィルタリングルールリストを作成し，IP Chain へのフィルタリングルールの書き込みを行う．提案実装手法ではパケットの転送時にフィルタリングルールを適用する「forward」というチェインの中にルールを書き込んでいる．ルールが書き込まれた瞬間から IP Chain はそのルールをもとに，ルータを通して転送されるパケットに対してパケットフィルタリングを実行する．

4.4 動作確認結果

作成したプログラムを実験用に構築した図 2 のようなネットワークにおいて実行した．プログラムの動作確認結果の例を**図 3** に示す．実験時のプログラム名は chain10.pl としている．ルーティングテーブルから必要な内部ネットワークの経路情報を得て，それをフィルタリングルールとして実際に書き込み，パケットフィルタリングが意図したように容易に実行できることが確認できた．

また，図 2 でも示したとおり，このルータには「192.168.3.0」という実際にはネットワークに存在しない経路情報を書き加えておいた．この動作確認結果では，ping コマンドが実行された後に，「192.168.3.0」のネットワークが存在しないという警告が発生している．そのため，作成されたフィルタリングルールに，「192.168.3.0」を発信元 IP アドレスとするパケットを転送許可とするルールが含まれていない．このことから，作成したプログラムが，経路情報の正当性を確認する処理の結果として詐称された経路情報を発見し，それによって経路情報詐称に対する耐性を有していることも確認できた．

5. 考　　察

提案実装手法の処理速度を計測するために，まず経路詐称が行われていない状況で内部ネットワークの数を増やし，どの程度の規模のネットワークで有効に利用できるかを考察する．動作確認用のルーティングテーブルを作成し，それをもとにフィルタリングルール自動作成プログラムを実行した．内部ネットワークの数を 10 から 50 まで，10 ずつ増やしながら実験した結果が**表 1** である．なお，この処理時間は 20 回計測した値の平均値である．この結果からフィルタリン

表 1 処理時間 1
Table 1 The processing time 1.

内部ネットワークの数	処理時間（ms）
10	48.0
20	56.9
30	64.7
40	74.1
50	83.0

表 2 処理時間 2
Table 2 The processing time 2.

処理時間(s)	経路詐称:有	経路詐称:無
詐称耐性:有	10.062	0.044
詐称耐性:無	0.031	0.028

グルールを手動で設定する場合に比べてきわめて迅速に内部ネットワークに対して IP アドレス詐称対策を行えることを確認した．

さらに，経路詐称が行われる可能性も考えて，経路情報の確認を行ってプログラムを動かした．提案実装手法では，ネットワークの確認のために ping というネットワークコマンドを利用した．このコマンドは，パケットを一度に多くの場所に送ることができるため，ネットワーク有無の探査には適している．応答待機時間を含めたプログラム処理時間を**表 2** にまとめた．

この表は処理時間を 20 回計測した結果の平均所要時間である．経路詐称が行われている場合は，処理時間が大きくなっているが，この処理時間のうち 10 秒は ping の反応待ち時間である．この反応待ち時間についての考察は 5.5 節で行う．

また，経路詐称耐性を付加しない状況で同様のネットワークに対して実験を行った結果も併載した．経路詐称耐性のための ping 待ち時間以外の実質処理時間は 0.1 s 以下であるという，迅速な処理が行えることが明らかとなった．

5.1 関 連 研 究

IP アドレス詐称対策としては，DHCP（Dynamic Host Configuration Protocol）を用いた方式[6] がある．この方式では内部ネットワークからゲートウェイを通り外部ネットワークに流れるパケットで，DHCP により貸出し中のアドレスが送信元 IP アドレスと同じであるものだけを通す方式である．この方式では，攻撃者が IP アドレスを詐称できる範囲を狭めることができる．しかし，この方式を実行するには，対策を行うネットワークが DHCP を利用していなければならず，ゲートウェイが DHCP サーバを兼ねている場合でなければ有効ではない．

また，DHCP に認証を組み込み，IP アドレス詐称を完全に行えなくする方式[7] も提案されているが，この提案ではクライアントやサーバに特別なソフトウェアが必要となるうえ，ユーザに認証という作業が必要となる．

経路情報を利用するフィルタリング手法としてリバースパスによるフィルタリングという方式[8] も提案されている．この方式ではルーティングテーブルを利用したフィルタリングルールを設定することで IP アドレス詐称を行うアプローチは酷似しているが，本提案方式では自動更新によって動的にフィルタリングルールを設定することで，RIP などに代表される動的経路制御を行うプロトコルにも対応することができる．

このように既存の提案と比較して，本提案方式ではルータならば必ず所持している経路情報によってフィルタリングルールを決定するため，特別なソフトウェアやプロトコルに依存することなくルータの管理者が独自に IP アドレス詐称対策を行えるという意味で有用である．

5.2 セキュリティレベル

本節では不正アクセスや本提案方式への攻撃に対して考察する．

ルーティングテーブルの経路情報をもとにフィルタリングルールを設定している以上，内部ネットワークの IP アドレスを詐称したパケットが外部ネットワークに送信されること止めることはできない．この問題に対して完全な防御策を望むのであれば，ネットワーク利用者に認証を行わせるなどのユーザ側のアクションが必要となるであろう．本提案は内部ネットワークとして複数のネットワークを持つルータに対して，ルータが単独で行える最低限のセキュリティを施すものといえ，ネットワーク管理者が多大なコストを払うことなく独自にセキュリティレベルを引き上げるために役立つと考えられる．

5.3 経路情報詐称対策

経路情報詐称対策の必要性とその限界について考察する．

本提案方式はルータが単独で行える防御策に主眼を置いている．そのため，経路情報詐称対策に関しては耐性の強化は行ったが，完全な経路情報詐称対策は提供できなかった．ただし，実際は，ルーティングプロトコルの設定によってパスワードや MD5 などのハッシュ関数によって認証を行えるため，経路情報詐称を行うのは難しいともいえる．しかし，ネットワーク中の複数のルータをそれぞれ違う管理者が担当している場合など，お互いの犯罪行為防止のための抑止策とし

て，各ルータが簡単な経路情報詐称対策を行うことは有効である．

また，本提案方式の実装例は，BGP（Border Gateway Protocol）のような AS（Autonomous System）間経路制御には対応していない．それは，IP アドレス詐称対策のために利用しているパケットフィルタリングは，すべてのパケットを監視するため転送されるパケット量に比例してマシンやネットワークに負荷をかけると考えたからである．本提案方式はパケットの流れの比較的少ないエッジルータ近くで実行することが効果的である．5.2 節でも述べたように，本提案方式では内部ネットワークの発信元 IP アドレス詐称を防ぐことはできない．攻撃者が詐称に利用できる IP アドレスを狭めるためや，同じネットワーク内で IP アドレス詐称攻撃が行われた際に攻撃者を特定しやすくするためにも，エッジルータの近く，つまり AS 内経路制御の範囲内での利用が有効と考えられる．

5.4 フィルタリングルールの更新頻度

つねにネットワークが変化する可能性があるため，フィルタリングルールの再構築は頻繁に行わなくてはならない．この更新の間隔は，実装するマシンのスペックやネットワークの利用状況にもよって異なるが，ルーティングプロトコルに RIP を利用している場合，最大でも 30 秒以内にすることが望ましい．この 30 秒という値は，RIP における経路制御情報の更新間隔である．

動的経路制御の場合，経路制御情報の交換は非同期になりうる．そのため，本提案実装手法に利用したプログラムを実行するトリガを経路情報の受信としない限り，経路情報の更新とフィルタリングルールの更新にタイムラグが生じる．新しい正規のネットワークが加わった場合，更新頻度に設定した時間だけ，ネットワーク不通時間が発生する可能性がある．しかし，経路情報詐称によって経路情報だけが更新されたとしても，パケットフィルタのポリシを「許可のあるパケットだけ通す」としているため，経路情報とフィルタリングルールの更新におけるタイムラグによって，経路情報詐称攻撃をともなった IP アドレス詐称攻撃が成功することはない．

5.5 ping によるネットワーク存在確認

本提案実装手法では経路情報の真偽を確かめる際，ping によってネットワークの存在を確認しているが，ホストが存在しない場合や，設定によってホストが ping に反応しない場合も存在する．ネットワークが存在していても ping への反応がない場合，現在の仕組みではそのネットワークから送信されるすべてのパケットを破棄することになる．このため，ping に反応しないようなネットワークでは本提案実装手法を実行することができない．これは本提案実装手法の限界であり，ルータが単独で行える経路情報詐称対策を研究することが今後の課題である．

経路情報詐称に関しては，ルーティングプロトコルレベルでの経路情報詐称対策を信頼することが最善策と考えられる．しかし，ルータが単独で行える経路情報詐称対策として，ping でネットワークの存在確認をすることで，経路情報の真偽を確かめる方法によって，経路情報詐称耐性の強化を図ることも有効である．

また，本提案実装手法を熟知した攻撃者が，詐称した経路制御情報をルータに送った後にパケットの流れを監視し，ping の応答要求に対してにせの ping の反応を返す攻撃も考えられる．このような攻撃の防御策は，今後の研究課題として考えていく必要がある．

最後に ping の反応時間の長さに関して．今回はオプションコマンドを入れずに ping を使用したため，10 秒ほどの反応待機時間がかかった．これは ping にオプションコマンドを入れることによって，反応待機時間や送出パケット数を調整できるが，このような設定はネットワーク環境に左右されると考えたため，実験ではデフォルトの設定に従った．本提案実装手法を実施するネットワーク管理者は，対策を行うルータがどれくらいの負荷を負っている状態では，末端のホストに ping を実行したときに，返信までにどれくらいの時間がかかるのかということを，あらかじめ調査しておく必要がある．

6. ま と め

ネットワーク管理者は，管理するネットワークで発生する様々な問題に対処しなければならない．人為的なミスをなくすためにも，ゆとりをもったセキュリティ対策が望まれるが，現実にはネットワークセキュリティの実務に投入できる人材が不足がちであることも事実である．そこで人間に代わってセキュリティ上の問題を自動的に発見，処理するようなシステムが必要である．攻撃が多様化している現代では，すべての攻撃を把握することは難しいが，このようなシステムが有用であるためには，様々な攻撃に耐えられるように改良を重ねる必要がある．また，古くからのプロトコルなどを利用している環境も少なくなく，そのような環境においても利用できるようなシステムが必要とされている．

IP アドレス詐称という問題は，詐称されたパケットを受け取った側で防御策をとることが難しい．その

ため，それぞれのネットワークがソース IP アドレスの詐称されたパケットを外部に流出させない必要がある．本論文では IP アドレス詐称対策に関して，管理者の手間を省くアイディアを提案し，実証した．また，その研究過程において，経路情報詐称に対する脆弱性の存在を確認し，実装したプログラムの動作確認結果を検討することにより改良への足がかりを得た．

また，残された課題として，経路情報詐称対策のセキュリティレベルや本提案実装手法実行のタイミングの考察があげられる．経路情報詐称対策の検討においては，ネットワークに所属するすべてのホストが ping に反応しない場合の検討や，攻撃者が偽の ping 情報を返す場合の検討などがあり，今後これらについて研究を行う必要がある．

謝辞 本論文の原稿につき，内容と表現の改善に関して匿名の査読者をはじめ多くの方から貴重なコメントを頂戴した．ここに記して謝意を表したい．

参 考 文 献

1) Hedric, C.: Routing Information Protocol, Request for Comments 1058 (1988).
2) Malkin, G.: RIP Version2, Request for Comments 2453 (1998).
3) Moy, J.: OSPF Version2, Request for Comments 1583 (1994).
4) Ferguson, P. and Senie, D.: Network Ingress Filtering, Request for Comments 2827 (2000).
5) 久米原栄：ファイアウォール管理者ガイド，ソフトバンクパブリッシング (2000).
6) 石橋勇人，山井成良，安部広多，大西克実，松浦敏雄：IP アドレス/MAC アドレス偽造に対応した情報コンセント不正アクセス防止方式，情報処理学会論文誌，Vol.40, No.12, pp.4353–4361 (1999).
7) 古森 貞，齋藤孝道，森井章夫，安藤広基，武田正之：ユーザ認証付き DHCP の提案と実装，コンピュータセキュリティシンポジウム 2001（CSS2001）予稿集，pp.155–160 (2001).
8) 菊地高広，浅見 徹，力武健次，永田 宏，濱井龍明：IP アドレス詐称対策のためのリバースパスによるフィルタリング手法，コンピュータセキュリティシンポジウム 2001（CSS2001）予稿集，pp.191–196 (2001).

(平成 15 年 12 月 4 日受付)
(平成 16 年 6 月 8 日採録)

中野 学（正会員）

2001 年和歌山大学システム工学部情報通信システム学科卒業．2003 年横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期修了．現在，同博士課程後期に在学．ネットワークセキュリティの研究に従事．

松本 勉（正会員）

1986 年 3 月東京大学大学院博士課程（電子工学）修了，工学博士．同年横浜国立大学工学部専任講師．現在，同大学大学院環境情報研究院教授．1981 年より，暗号・電子署名のアルゴリズムとプロトコル，ディジタル証拠性，耐タンパーソフトウェア，情報ハイディング，ネットワークセキュリティ，認証方式，バイオメトリクス，人工物メトリクス等の各種情報セキュリティ技術の研究教育とその実応用に力を注ぐ．1982 年に「明るい暗号研究会」を数人の仲間とともに創り研究をはじめた．国際暗号学会 IACR 理事．CRYPTREC 暗号モジュール委員会委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．