DHCPを用いた情報コンセントにおけるウィルス感染を防止する一手法

齊藤明紀† 桝田秀夫††

組織内のネットワークシステムでは，ウィルスやワームの侵入を防ぐ機構としてファイアウォールが有効であるが，情報コンセント等の組織内から，感染済のパソコンを持ち込まれる場合には対処は困難である．またルータでパケットフィルタを実施した場合でも，同一セグメントに接続した他のパソコンへの感染は阻止できないという問題がある．本研究では，特殊な応答を返すDHCPサーバを用いることで，クライアントとなるパソコンに特殊な設定をすることなく，同一セグメント内の通信であっても，パケットをルータに経由させることができる方式を提案する．本方式を用いることで，同一セグメント内のパケットのやりとりに対してもフィルタリングをかけることが可能となり，他のパソコンへのウィルスやワームの感染を防止することが可能となる．

A method to protect client PCs form worm or virus in DHCP environment

Akinori SAITOH† Hideo MSAUDA††

Firewalls are useful to protect client PCs from network attacks such as computer virus or worm. But firewalls has no effect if someone had bring a already-infected PC into a LAN . Illegal packets from infected PCs could be discarded by routers' packet filter. But PC to PC infection in a single network segment is left with no control. We propose an DHCP server that supplies a tweaked respose to each clients. With our DHCP server, each client PC will submits any packet to router even if the destination is neighbour PC. Packet filter on the local router can inspect and/or discard packet between client PCs.

1　はじめに

ここ数年来, DoS攻撃やワームなどの被害が社会的な問題となってきている．また, 情報コンセントや一部のISPなどでは, 自宅でのパソコン間でのファイル共有設定を解除しないままに接続して, ハードディスクの内容を他の利用者から覗かれてしまうという問題も生じている．端末を攻撃するパケットや感染を試みるワームからのパケットは, 通常はファイヤウォールで検知して破棄される．また, CIFSのパケットもルータやファイヤウォールで破棄することで, ファイル共有を阻止することができる．しかしながら, 同一のレイヤー2(L2)に接続している端末相互はハブを経由して直接通信するため, ルータ等のパケットフィルタで保護することができない．また, 最近ではスイッチングハブが広く用いられるようになり, 感染状況を調べるために端末相互の通信を傍受することも難しくなっている．

図1のような, 個人所有のパソコンを接続する情報コンセントでは, 自宅等でワーム等に感染したパソコンが持ち込まれ, 接続されることを阻止できない．ひとたび感染したパソコンが持ち込まれると, 同一ハブに接続した他のパソコンも感染などの被害を受けてしまう．

本論文では, 同一L2ネットワークに接続している端末相互が, IPでの通信に際して, 直接の通信を行わず必ずルータを経由するように仕向ける方式について報告する．これにより, たとえば図1のルータのパケットフィルタでPC1とPC2の間で行われる通信を監査することができる．またこの際, 端末PCに対して事前に特殊な設定作業を行ったりソフトウェアをインストールしたりする必要がないことが特徴である．

2　基本的なアイディア

通常, 一般利用者の端末計算機の経路表には外部ネットに接続するルータへのデフォルトルートが登録されている．

IPv4ノードでは, パケットの宛先アドレスを調べて, 同一のネットワークに接続する宛先なら直接送信し, そ

†鳥取環境大学, Tottori University of Environmental Studies
††大阪大学, Osaka University
*本報告で提案する接続方式は特許出願済みである．

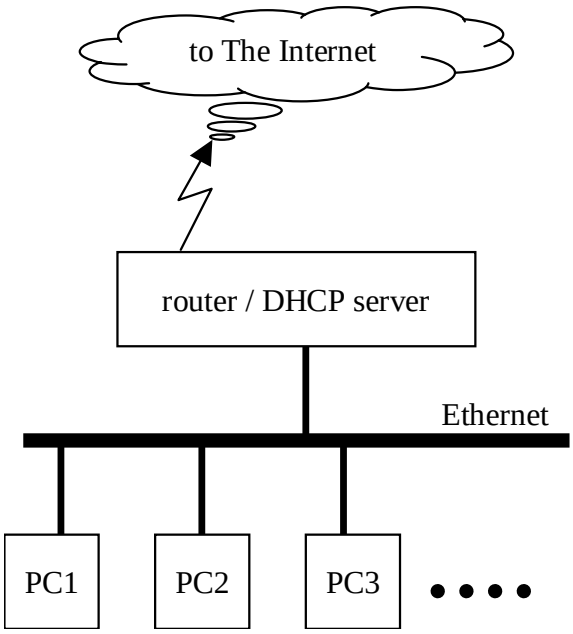

図 1: DHCP ベースの情報コンセント

うでなければ, 経路表に従ってルータにパケットを転送する.

たとえば図 1 において, 同一データリンクネットワークに接続した宛先ホスト PC2 を他の IP ネットワークに接続しているものとパケット発信元端末 PC1 に認識させることができれば, パケットはルータを経由して送られることになり, ルータでのパケット監査が可能となる. ただし, 通常のルータはパケットの着信したインターフェースと転送先インターフェイスが同一である場合には ICMP リダイレクトを発して端末に対して直接送信するように促すので, この機能は休止させなければならない.

IP では, 宛先 IP アドレスがローカルな IP ネットワークに属するかどうかの判断には, 端末のローカルな IP アドレスとネットマスクを用いる. すなわち, ローカル IP アドレス IP_s, ネットマスク M_s, 宛先 IP アドレスを IP_d として,

$$(IP_s \& M_s) = (IP_d \& M_s)$$

であれば* , 同一ネットワークに接続しているものと解釈し, 直接送信する. ただしこの際, IP_d がマッチする経路情報が経路表にあればそちらが優先される.

そこで, IP_d あてのパケットをルータに送るように仕向けるには, 以下の 2 つのいずれかであればよい.

- IP_d への経路 (ホストルートあるいは, M_s よりもマッチング長の長い宛先ネットワークを持った経路表エントリ) がある.
- $(IP_s \& M_s) \neq (IP_d \& M_s)$ となるような M_s が端末に設定されている.

前者に当てはまるためには, 同一セグメント内の全端末に対するホスト経路を端末に設定することになる. 最も広く用いられている Windows 端末では, デフォルトルータを 1 つだけ経路表に登録する方式が用いられる. そこで, 複雑な経路表を設定することが必要となる前者の方式は本研究では避け, 後者を検討する.

後者に当てはまる方式には, PPTP や PPPOE など, 仮想的な poin-to-point 回線をイーサネット上で運用する方法がある. この場合端末のローカルインターフェースはネットマスク 255.255.255.255 となり, 自分自身以外のすべての宛先へのパケットはルータに投げられる. しかしながら, これらは所定のドライバソフトウェアを端末に事前にインストールし, またログイン名とアクセスパスワードの登録等を事前に行わねばならない. ドライバのインストールやパスワード登録を行うことは一般のパソコンユーザにとっては困難であり, またパスワード発行・管理の手間が情報コンセント運用側に追加されるので望ましくない. そこで, 通常の DHCP クライアントのパソコンを追加設定作業なしに用いて, 目標を満たすことを考える.

以降具体例で検討する. 簡単のために, ルータと DHCP サーバとパケット監査装置を同一のホストが兼ねているものとする (図 1 の「router / DHCP server」). ルータの (情報コンセント側の)IP アドレスを 192.168.1.1, ネットマスク 255.255.255.0 だとする.

ここで図 1 のネットワークでルータが 192.168.1.1(ネットマスク 255.255.255.0) に設定されており, 端末 1 がアドレス 192.168.1.10 を持つ状態を考える. 通常のネットワーク運用方式では同じデータリンクネットワークに接続した IP ノードはすべて同じネットマスク値を共有する. しかし, 本研究ではルータと端末が異なるネットマスク値を持ちながら, 同じイーサネットに接続するという方式を考える.

2.1 方式 1

DHCP 端末 のネットマスク長が 32 ビット (ネットマスクが 255.255.255.255) である場合について考察する.

端末 1(192.168.1.10) にとって, 他のすべての端末 (2,3,$\cdots$) は他の IP サブネットに接続しているものとして認識され, それら宛の IP パケットはルータに送られる.

ただしこの場合, ルータが端末 1 のローカルな IP ネットワークの外にあることになるので, UNIX(BSD, Linux を含む) ではルータへのデフォルトルートを設定することができない. しかし Windows の現状の実装† では問

*ここでの&は C 言語の&と同様のビットごとの論理積演算子である.

†Windows 9x/NT 系双方で確認した.

題なく運用することができる.

ブロードキャストアドレスとしては, 端末 IP アドレスとネットマスクの組み合わせに対して整合性のある 255.255.255.255 を用いる.

端末の設定パラメータ	
端末アドレス	192.168.1.10
ネットマスク	255.255.255.255
ブロードキャスト	255.255.255.255
デフォルトルータ	192.168.1.1

ルータのインターフェースの設定においてもブロードキャストは 255.255.255.255 として設定すればよかろう.

この場合 DHCP 端末相互で, IP ブロードキャストを用いた通信は直接やり取りできてしまう. しかし, ワームの感染を試みるパケットはユニキャストで送られるのが通例である. またブロードキャストパケットによる攻撃がが直接届いたとしても, それへの応答はユニキャストで行われる. 応答のユニキャストパケットを破棄することで感染を阻止することは可能と考えられる.

ルータに対する ARP リクエストとそれへの応答はネットマスク値と無関係に行われるので, とくに阻害されることはない.

端末の外部ネットワークへのパケットは, やはりデフォルトルータ宛てに送られ, 最終的に宛先に到着する. 端末への外部ネットワークからのパケットは, ルータに届いた後, ルータのインターフェース設定にしたがって処理される. すなわち, 宛先アドレスをルータのネットマスク値で処理すると同一 IP ネットワーク内にあるとわかるので, ARP で MAC アドレスを調べた後に直接送信され, 正常に到着する.

DHCP サーバへのアドレス更新要求は, ユニキャストで行われる. 図 1 の例ではルータが DHCP サーバをかねているので特に問題はない. そこで, ルータと DHCP が異なる計算機の場合について考察する. クライアントからの DHCP RENEW 要求はユニキャストであるのでルータに送られて, 通常の IP ルーティングによって DHCP サーバに届けられる. この際イーサネットヘッダのソース MAC アドレスは, クライアントではなくルータとなる. しかし, ペイロード中の DHCP リクエストパケットの ciaddr フィールドにクライアントのハードウェアアドレスが含まれる [1] ので, DHCP サーバは問題なくリクエストを処理できる. DHCP サーバはネットマスクがルータと同じく /24 に設定すればよく, リクエストに対する応答パケットは DHCP サーバから直接クライアントに届けられる.

2.2 方式 2

DHCP 端末 のネットマスク長が 30 ビット (ネットマスクが 255.255.255.252) 以下である場合について考察する.

ここでは, 端末にとっての接続ネットワークとして 192.168.1.8/29 を用いる場合を考える. この場合 IP アドレスのホスト部が 1〜6, すなわち 192.168.1.9〜14 までの 6 つの IP アドレスが端末の IP アドレスとして利用可能であるが, たとえば 192.168.1.10 を端末に割り当てるとする.

多くの UNIX/BSD/Linux の IP プロトコルスタックの実装では, , デフォルトルータとしてルータの IP アドレスである 192.168.1.1 を与えると, エラーを発して受け付けない. 192.168.1.8/29 の内部のアドレスを与える必要がある. そこで, たとえばデフォルトルータとして 192.168.1.9 を端末 1 に与えるとする. この場合, 他の 5 つの IP アドレスは他の端末には割り当てず未使用とする. こうすると, 存在するすべての他の端末の IP アドレスはサブネット 192.168.1.8/29 の外に存在することになり, パケットはルータに送られることになる. 8 つの IP アドレスの割り当ては次のとおりである.

ネットワーク部	ホスト部	割り当て
192.168.1.8/29	0	不使用
192.168.1.8/29	1	デフォルトルータ
192.168.1.8/29	2	端末
192.168.1.8/29	3	不使用
192.168.1.8/29	4	不使用
192.168.1.8/29	5	不使用
192.168.1.8/29	6	不使用
192.168.1.8/29	7	ブロードキャスト

しかし, ルータの実際のアドレスは 192.168.1.1 であるので, このままでは端末がルータにパケットを転送することができない.

単純な手法としては, ルータのインターフェース alias を端末の個数だけ設定して, 実際に端末から見たデフォルトルータの IP アドレスをルータに持たせるという方法がありえる. しかしながら, 現在の UNIX は数 10 あるいは 100 数十のアドレスを一つにインターフェースに与えた場合効率の点で問題が生じる可能性がある.

ここで端末 1 の通信について考察してみると, 動的経路制御を行っていないので, ルータ 192.168.1.9 を IP レベルの宛先とした通信を端末 1 が行うことはほとんどないことがわかる. DHCP サーバがアドレス 192.168.1.1 で応答すれば, アドレス割り当て継続要求は 192.168.1.1 宛てに行われる. ルータの稼動状態を確認するために手動で ping を行うというような場合は別として, 192.168.1.9 が IP ホストとして応答しなくても支障はない.

唯一つ, ルータの MAC アドレスを知るための ARP リクエストに, 192.168.1.9 が応答する必要があるだけである. そこで, 192.168.1.n(9,17,25,$\cdots$,249) 宛への ARP リクエストに対してルータが応答すれば, 端末がデフォルトルータにパケットを転送する動作は成功する.

次にブロードキャストアドレスについて考察する. ルータ・端末双方が自然なブロードキャストアドレス (自局 IP アドレスのホスト部を all 1 にしたもの) を用いるように設定すると, ルータは 192.168.1.255, 端末 1 は 192.168.1.15 を用いることになり, 通信が成立しない. お互いのブロードキャストパケットは到着するが, IP プロトコルスタックによって破棄される.

CIFS などブロードキャストを用いるサービスを端末に対して提供しない場合はこの設定でよい. 端末相互のブロードキャストも破棄されるため安全である.

ブロードキャストによる通信が行える必要がある場合には, 255.255.255.255 をルータ・端末双方に設定すればよい.

2.3 方式 3

端末のネットマスク長が 31 ビット (ネットマスクが 255.255.255.254) の場合について考察する.

この場合はネットワークのサイズが 2 である. 必要な IP アドレスとして, 端末自身, デフォルトルータ, ブロードキャストと 3 つあるので, ブロードキャストアドレスは, IP サブネットの外のアドレス, すなわち 255.255.255.255 をルータ, 端末ともに用いる.

そこで, 二つのアドレスのうちホスト部が 0 のものをデフォルトルータに, 他方を端末のアドレスとして設定する.

ルータの ARP 応答等に関しては方式 2 と同じである.

2.4 選択的に方式 1 を用いる

端末 のネットマスク長が 30 ビット (以下) のものと 32 ビットのものを混在させる場合について考察する.

現在ウィルス/ワームの被害が深刻なのは Windows のみであり, Linux 等はウィルスの事例が皆無ではないものの深刻な状況ではない. そこで, Windows 端末のみパケット監査の対象とし, それ以外の OS は通常の DHCP 情報コンセントと同じ設定 (ルータでのパケット監査なし) を配ることを考える. そのためには, Windows 端末には/32 を, それ以外の OS の端末には/24 で応答すればよい.

Windows 端末が発信する DHCP のアドレス割り当て要求パケットにはオペレーティングシステムの種別を示すオプションフィールドが含まれており, Windows 端末からの要求であることを DHCP サーバが識別することが可能である.

この場合はどの OS の端末でも IP アドレスを密に割り当ててよいので, IP アドレス空間をすべて利用できる. /24 のネットワークでは, 254 からルータや DHCP サーバの台数を除いた残りが割り当て可能である.

```
ddns-update-style interim;
ddns-updates off;
### Server Identifier
server-identifier 192.168.1.1 ;
### Global Parameters
option domain-name "example.jp" ;
option domain-name-servers 192.168.1.1 ;

### /32 clients
shared-network NET32 {
   ### Shared Network Specific Parameters
   default-lease-time 500 ;
   max-lease-time 850 ;
   get-lease-hostnames true ;
   subnet 192.168.1.0 netmask 255.255.255.255 {
      ### Subnet Specific Parameters
     option subnet-mask       255.255.255.255 ;
     option broadcast-address 255.255.255.255 ;
     option domain-name-servers 192.168.1.1 ;
     option time-offset         32400 ;
     option routers             192.168.1.1 ;
   }
}
```

図 2: 方式 1 の設定例

2.5 方式 1+2

Windows 以外の OS に対してもパケット監査を行うには, ネットマスク長が 30 ビット以下 (24 ビット以上) の設定を配布する必要がある. ただし, それでは IP アドレスの利用効率が低下 (25%) する.

そこで,DHCP サーバが Windows 端末には/32 で, それ以外の OS の端末には/30 で応答することができれば, アドレス空間の無駄が少なくなる.

3 動作確認実験

前節のアイディアの有効性を確認するため実証実験を行った.

試作と動作確認では, NetBSD-i386(1.6release) をルータ兼 DHCP サーバとして用いた. DHCP サーバーソフトウェアは ISC の dhcpd-3.0pl2 を用いた. クライアントとして用いたのは, Windows98, Windows2000, WindowsXP, NetBSD1.6, Linux(カーネル 2.4.26) である.

図 1 のようなネットワークで端末相互の通信の IP パケットがルータに届くと, 冗長な経路を指摘する ICMP メッセージ (`ICMP_REDIRECT`) がルータから端末に送られる. 本方式ではこのような迂回経路は意図したものなので, ICMP の生成を抑止する必要がある. NetBSD では次のような sysctl を行う.

```
sysctl -w net.inet.ip.redirect=0
```

```
shared-network DHCP30-NET {
 ### Shared Network Specific Parameters
 default-lease-time 500 ;
 max-lease-time 850 ;
 subnet 192.168.1.4 netmask 255.255.255.252 {
  ### Subnet Specific Parameters
  option subnet-mask 255.255.255.252 ;
  option broadcast-address 192.168.1.7 ;
  option routers 192.168.1.5 ;
  option time-offset 32400 ;
  range 192.168.1.6 ;
  }
  subnet 192.168.1.8 netmask 255.255.255.252 {
  ### Subnet Specific Parameters
  option subnet-mask 255.255.255.252 ;
  option broadcast-address 192.168.1.11 ;
  option routers 192.168.1.9 ;
  option time-offset 32400 ;
  range 192.168.1.10 ;
 }
 subnet 192.168.1.12 netmask 255.255.255.252 {
  ### Subnet Specific Parameters
  option subnet-mask 255.255.255.252 ;
  option broadcast-address 192.168.1.15 ;
  option routers 192.168.1.13 ;
  option time-offset 32400 ;
  range 192.168.1.14 ;
 }
 (以下略)
}
```

図 4: 方式 2 の動作確認用設定例

```
arp -s 192.168.12.5 $MAC pub
arp -s 192.168.12.9 $MAC pub
arp -s 192.168.12.13 $MAC pub
      :
     以下略
```

図 5: arp 設定

3.1 方式 1

既存の DHCP サーバ [2] の設定ファイルの記述だけで, 方式 1 に基づくアドレス割り当てを行うことができる. 図 2 が設定例である.

3.2 方式 2

IP アドレスをサブネット単位で扱う必要があるので, DHCP サーバの設定ファイルの記述だけで対応することはできず, プログラムコードを変更する必要がある.

また, 端末にとってのデフォルトルータのアドレスに対する ARP に応答する設定も必要である. これには, ARP 設定を行うように dhcpd を改造する方式と, 使用されうるすべてのアドレスに対して図 5 のような ARP 設定をルータ起動時に行っておく方式がありえる. ここでは, `$MAC` はルータの MAC アドレスとする.

ただし, 潜在的な端末の個数だけインターフェイス

```
shared-network DHCP32-NET {
    ### Shared Network Specific Parameters
    default-lease-time  500 ;
    max-lease-time   850 ;
    subnet 192.168.1.0 netmask 255.255.255.0 {
      ### Subnet Specific Parameters
      option   domain-name-servers  192.168.12.8 ;
      option   routers     192.168.1.1 ;
      option   time-offset 32400 ;
      range 192.168.1.2 192.168.1.249 ;
    }
}
class "windows-clients" {
#    "MSFT 5.0"  Windows2000
#    "MSFT 98"   Windows98
   match if substring
        (option vendor-class-identifier, 0, 5)
          = "MSFT ";
   option subnet-mask    255.255.255.255 ;
   option broadcast-address 255.255.255.255 ;
}
```

図 6: 方式 1 を選択的に適用する場合の設定例

alias を作成する方式でなら, 既存 DHCP サーバの設定ファイルの記述で対応できるので, 図 4 の設定で動作確認を行った. この設定ファイルでは端末用アドレス 1 個につき一つの subnet セクションを記述するため設定ファイルが非常に冗長になっている. また, dhcp サーバデーモン起動に先立って図 3 のようなコマンド列で (図中の $intf は, ルータのインターフェースの論理名である) インターフェイス alias を設定しておく必要がある.

3.3 方式 3

/31 であるので端末にとってのネットワークサイズが 2 であるが, 実験の結果, デフォルトルータとしては, ホスト部が 0 のものを割り当てると経路設定に失敗し正常に動作しないことがわかった (Linux および NetBSD). 端末にホスト部 0, デフォルトルータにホスト部 1 のアドレスを割り当てると動作する.

ただし, /31 の場合は逆に Windows がこの設定を受け付けず動作しないことがわかった.

3.4 方式 1 を選択的に適用する

図 6 が端末が Windows であったら方式 1 を, そうでなければ通常の DHCP 端末設定 (/24) を行う場合の例である. 設定ファイルの冒頭部分は図 2 と同じであるの省略してある. Windows からの DHCP リクエストのオプションフィールド vendor-class-identifier が “`MSFT␣`” という文字列で始まるので, これを検出して /32 の設定を配布する.

```
ifconfig $intf alias 192.168.1.5 netmask 255.255.255.252
ifconfig $intf alias 192.168.1.9 netmask 255.255.255.252
ifconfig $intf alias 192.168.1.13 netmask 255.255.255.252
   :
   (略)
```

図 3: インターフェイス alias の設定

3.5 効率と負荷に関する考察

本方式では端末の発信するすべてのパケットはルータに集まる. このため, スイッチングハブを用いていてもトラヒックがルータのポートに集中してしまう. しかしながら, 情報コンセントの典型的な利用形態では端末がアクセスするのは WWW サーバや POP サーバなどであり, ルータを経由した外部に存在する計算機である. 端末相互の通信はほとんど行われない. 端末が相互に直接通信するのは以下のような場合である.

1. NeTBIOS の名前解決のためのパケット
2. ウィルス/ワームの侵入行為に伴うパケット
3. P2P ツールの稼動に伴うもの

1 は, トラヒックが少なく問題ない. 2 は, トラヒックが非常に多いがこれをルータで把握することが本研究の目的であり避けられない. 3. は, 通常情報コンセントに接続する端末で行うことは少ないと考えられる.

図 1 のような構成の情報コンセントに本方式を適用した場合でルータのパケットフィルタ能力に問題が生じた場合には, 容易にルータを複数台並列に設置して負荷分散を行うことができる.

3.6 制限事項

本方式は原理的に IPv4 通信しか対応しないので, IPX など他のプロトコルでの攻撃に対しては無力である. また, ping of death のようにパケットの到着が即ち被害発生となるような攻撃がブロードキャストで行われると防ぐことができない.

Windows での NETBEUI が非 IP プロトコルとしては広く使用されてきたが, 近年の Windows では NeTBIOS over TCP/IP(NBT) に移行して NETBEUI を使わない傾向にあるので, 本方式は十分に有効であると考えられる.

3.7 パケットフィルタルール

動作確認では, ルータにはパケットフィルタは設定せず, 端末 PC 相互の通信パケットがルータを経由することを確認するにとどめた.

ウィルス等に感染した PC からの同一 L2 ネットワーク内での攻撃は, 多くはルータ越しの攻撃と同じ手法が用いられる. そこで, 本方式を用いた際のルータのパケットフィルタの設定は, 基本的にはファイヤウォールとしての設定に, 各端末でのパーソナルファイヤーウォールでのフィルタルールを併合したものでよいと考えられる.

そこに, たとえば CIFS ファイル共有のパケットは通信相手がファイルサーバである場合のみ通す, 端末が DHCP サーバとしてのパケットを生成していたら破棄する, など L2 内通信特有のルールを追加することになろう.

4 まとめ

DHCP サーバを用いて, 同一 L2 ネットワーク上のクライアント端末装置相互の IP 通信をルータ経由に仕向ける方式を提案した. 本方式は, 同一 L2 ネットワークに接続したサーバとクライアントに異なるネットマスク値を持たせることを特徴とする. また提案した形態のうちのいくつかは, 既存の DHCP サーバの設定ファイルの記述だけで実現できることを確認した.

本方式により, 端末相互でのワーム感染等の事故をルータのパケットフィルタでパケットを破棄することで防止できる.

本報告では動作確認が主目的であったので, 既存の DHCP サーバソフトウェアをそのまま使用することを優先したため, 設定ファイルの記述が冗長になった面がある. 本方式を取り込んだ DHCP サーバの開発と, ルータでのパケットフィルタルールの生成手法の確立が今後の課題である.

参考文献

[1] R. Droms:“Dynamic Host Configuration Protocol”, RFC2131(Mar. 1997).

[2] Internet Systems Consortium,Inc: “ISC Dynamic Host Configuration Protocol”, http://www.isc.org/index.pl?/sw/dhcp/ (2004).