ルータ上のパケットフィルタで端末間通信を処理するためのDHCPサーバ構成法

齊藤明紀[†] 桝田秀夫[††]

組織内のネットワークシステムでは，ウィルスやワーム等からの攻撃パケットを阻止するために，ファイヤウォールやルータ上でのパケットフィルタが用いられている．しかし，同一レイヤ2ネットワーク内の通信はルータを経由しないため，感染済みのパソコンが情報コンセント等組織内に持ち込まれた場合には対処できない．また，ワクチンソフトやパーソナルファイヤウォールの正しい運用を各個人に100%徹底させることは非常に困難である．本論文では，同じL2ネットワークに接続するルータと端末に異なるネットマスク設定を持たせることにより，同一L2ネットワーク内のIPv4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．また，この設定をDHCPサーバを用いて配布することで，クライアントとなるパソコンに事前の設定作業をすることなく，本方式が適用可能であることを確認した．本方式を用いることで，外部からのパケットと同一L2ネットワーク内のパケットのやりとりの双方を1つのルータ上でフィルタリングすることが可能となる．

A DHCP Server Configuration to Process PC to PC Communication Packet on Router's Packet Filter in a Single Layer2 Network

Akinori Saitoh[†] and Hideo Masuda[††]

Firewalls and packet filter on routers are useful to protect client PCs from network attacks such as computer virus or worm. But PCs are still vulnerable if someone had brought an already-infected PC into a LAN. Illegal packets from infected PCs from other subnet could be discarded by routers' packet filter. But PC to PC infection in a single Layer2 network is left with no control. We propose a DHCP server that supplies a tweaked configuration to each client. With the configuration, each client PC will pass every IPv4 packets to the router even if its final destination is the neighbor PC. With proposed method, the packet filter on a single router could process incoming, outgoing and PC to PC local communication packets.

1. はじめに

ここ数年来，DoS攻撃やワーム等の被害が社会的な問題となってきている．また，パソコン間でのファイル共有設定を誤り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，あるいは他のPCに感染したウィルスから書き換えられるという問題も生じている．これは特に，十分な保守が行われているとは限らない個人所有のパソコンを持ち込む情報コンセント（**図1**）で大きな問題となっている．

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，組織外からのものはファイヤウォールで，組織内の他のサブネットからのものはルータのパケットフィルタで検知して破棄することが可能である．また，CIFS[1)]のパケットを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もできる．しかしながら，同一のレイヤ2（L2）ネットワーク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（**図2**）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．このことはブラスターワームの蔓延以来問題となっている．

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，接続PCのワクチンソフトの導入や最新パターンの利用，あるいはパーソナルファイヤウォールの適切な設定は期待できない．一部ではあるが，うかつな利用者がどうしても出てきてしまう．そのため，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

† 鳥取環境大学
Tottori University of Environmental Studies
†† 大阪大学サイバーメディアセンター
Cybermedia Center, Osaka University

本報告で提案する接続方式は特許出願済みである．

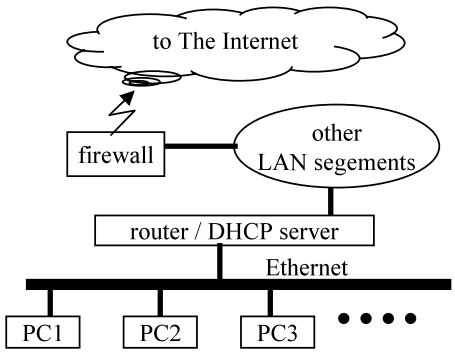

図 1 DHCP ベースの情報コンセント
Fig. 1 DHCP client and network.

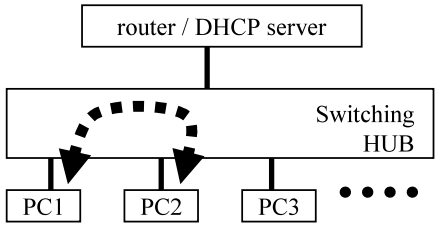

図 2 同一 L2 ネットワーク内での直接通信
Fig. 2 Direct communication in single L2 network.

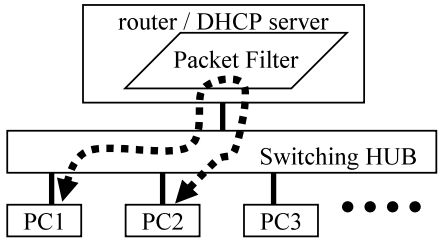

図 3 同一 L2 ネットワーク内でのルータ経由通信
Fig. 3 Via router communication in a single L2 network.

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等の被害を受けてしまう．

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．

我々は，同一 L2 ネットワークに接続している端末相互が，IP 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ネットワーク構成方式について検討してきた[2]．本方式は IPv4 に対して，**図 3** のように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し，パケットの廃棄や改変等を行うことができる．提案方式では，DHCP[3] を用いて端末に設定情報を配布することでこれを実現する．そのため端末 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という利点がある．また，特殊な設定を行う DHCP サーバソフトウェアのほかに追加の機材を必要とせず，安価に実施できることも特徴である．

1.1 提案方式の位置づけと既存手法

本研究では，大学等での学生の持ち込み PC に対する情報コンセントサービスや，学会会場等の一時的に構築される情報コンセントやホットスポットサービスのための端末間パケットフィルタ手法について考える．

これらの用途では，以下のような要請がある．

- ハードウェアが低コストであること．
  既設のネットワークや安価な L2 スイッチの利用が可能であることが望ましい．
- 運用コストが低いこと．
  これらは無償サービスであることが多く，運用・ユーザサポート要員を潤沢に割り当てることはできない．
- 利用手順が簡便であること．
  事前の登録なしに，すぐに使えることが望ましい．また，利用者の技術レベルがまちまちで初心者が非常に多く，さらにユーザサポートに割ける人員も少ないため，利用の手順が複雑な方式は避けなければならない．また個人所有のパソコンを前提とするため，特定のエージェントソフトウェアの導入を強制したり，NT ドメイン等管理システム下に入ることを強制もできない．
- Windows だけでなく，MAC OS X や Linux 等多くの端末 OS で利用できること．
- セキュリティレベルがやや低くても容認する．
  うかつな初心者の保護を主眼とし，悪意を持った技術レベルの高い利用者の行動を阻止することまではカバーできなくてもやむをえない．

本論文で提案する方式は端末相互の通信を L2 で直接通信せずにルータ経由にさせる手法である．情報コンセントを集約する上位ルータで，端末相互の通信もフィルタ処理を行う（図 3）．本方式は以下のような特徴を持つ．

- 単純な（フィルタ機能や taggedVLAN 機能を持たない）ハブを用いた既設ネットワークがそのまま使える．
- DHCP サーバの設定を変えるだけで実現できる．ただし既設ルータのフィルタ能力に不足がある場合には，ルータの増設または交換も必要である．
- DHCP をもちいるため，ほとんどすべての OS で設定なしに接続するだけで利用できる．
- フィルタの対象は IPv4 ユニキャストパケットに限定される．
- 端末 OS やルータの実装依存の部分がある．

端末相互の通信パケットの監査を行う既存手法には，L2 レベルの方式と L3 での方式に大別できる．

L2 スイッチにパケット監査機能を持たせることは最も単純な解法であり，またプロトコルを選ばない．

L3 すなわちルータでパケットを監査する方式とは，個々の端末を異なるネットワークに置く方式である．たとえば IEEE802.1Q Tagged VLAN 機能を持ったハブの各ポートを異なる VLAN に所属させ，1 ポートに 1 つずつの端末を接続する方式が考えられる．また各端末を物理的には同じ L2 ネットワークに置きながら仮想的な point-to-point リンクで端末とルータとを結ぶ方式も考えられる．

これらのうち，ハードウェア的な解法は端末の分離度の高さやプロトコルを選ばない点等多くの利点を持つが，ネットワーク装置の交換が必要でまた各機器のコストも高くなるという問題がある．

仮想的に point-to-point の（L2）ネットワークを構成する方式には，PPPoE[4] や PPTP[5] 等がある．この場合端末のローカルインタフェースは point-to-point 型となり，自分自身以外のすべての宛先へのパケットはルータ（仮想回線の接続先）に投げられる．

PPPoE は接続と同時に利用者認証も完了するという利点はあるが，数十〜数百程度の中規模の端末数をサポートする安価なサーバが入手しにくいという問題がある．PPPoE クライアント機能を標準搭載する OS は WindowsXP 等いまだ一部であり，他の OS ではドライバの導入作業が必要である．また，WindowsXP でも数ステップにわたる設定作業を行わなければ利用できない．

筆者らは以前，PPPoE 情報コンセントを試験的に提供実験を行ったことがある[6),7)]．その試験運用では自力では接続できない利用者や，情報コンセントが使えるように設定すると自宅でプロバイダに接続できなくなったという苦情を寄せる利用者がある程度存在し，規模を拡大するとユーザサポートに人員を必要とすることが予想された．また，ある Linux では PPPoE の利用のためにはカーネルの再コンパイルが必要であるが，ハードディスク容量の余裕の少ないノート PC であったためその場で導入することができないというトラブルも起きた．PPPoE や PPTP は本研究で想定するような，ほとんどすべての利用者が自力で短時間で確実に接続できることが必要な情報コンセントには不適と考えられる．

情報コンセントにおけるウィルスの持ち込みの防止という観点では，検疫ネットワークも用いられ始めている．ただし検疫サーバからの問合せに答えるエージェントが導入されていない PC や，Linux 等対応外の OS からは利用できない．また高価なサーバや認証機能つきスイッチの導入が必要な点で，本研究で想定する用途には適切ではない．

2. 基本的なアイディア

本章では，提案手法の基本的な発想について説明する．

2.1 非対称な多重サブネット

提案手法は 1 つの L2 ネットワーク上で仮想的な IPv4 サブネットを多重かつ非対称に運用することで，「1 端末 1（論理）IPv4 サブネット」を実現するものである．

IPv4 では本来，1 つの L2 ネットワークには 1 つの IP サブネットワークを割り当て，L2 ネットワーク内のすべてのホストは同一のネットマスク値を有し，IP アドレスのネットワーク部も同一とするような運用を想定している．

端末相互の通信パケットのフィルタリングをルータで行うには，端末をそれぞれ異なる IP サブネットワークに置けばよい．L2 ネットワークに複数の IP サブネットワークを収容する手法は，トリッキーな手法ではあるがネットワーク配線やハブのコスト節約のため利用される事例は存在する[8)]．

情報コンセントにおいても，各端末に異なる IP サブネットに属するアドレスを割り付ければ，IP 通信に関しては同じ L2 ネットワークに接続していてもルータ経由となるであろう．この場合，1 つの L2 ネットワーク内に端末の数と同数の IP サブネットが多重に存在することになる．ただしそのためには，端末の数と同数のルータのポート（物理ポートまたは論理ポート）が必要になる（**図 4**）．

提案手法は，ルータのネットワークインタフェースを物理的にも論理的にも 1 個だけ使用しながら，端末には相互に異なる IPv4 サブネットに属すると認識させる手法である．

提案手法の基本的アイディアは，単一の L2 ネットワークにおいてルータやサーバ等端末との直接相互通信を行って差し支えない機器と，端末とで異なるネットマスクの値を設定することにある．

たとえば図 1 で，ルータが 192.168.1.1/24，端末 PC1 が 192.168.1.10/30，端末 PC2 が 192.168.1.14/30 を持つとする．

ルータにとっては PC1 も PC2 も自ホストと同じ 192.168.1.0/24 のサブネットワークに接続するホストに見えるので，直接パケットを送信する．PC1 にとっ

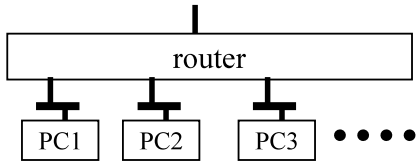

図 4 1 端末 1 サブネット構成
Fig. 4 Single PC in each logical IPv4 subnet.

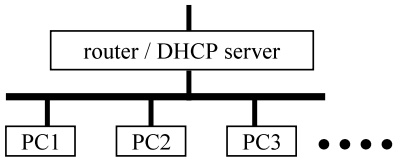

図 5 ルータにとってのネットワーク認識
Fig. 5 Router's view of the network.

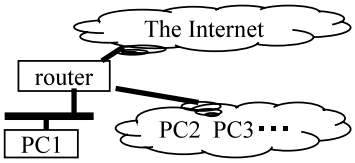

図 6 端末にとってのネットワーク認識
Fig. 6 PC1's view of the network.

ては PC2 は他のサブネットに属するホストに見えるので，PC2 宛のパケットはデフォルト経路（ルータ）経由となる．PC2 から PC1 の通信も同様である．

このように，同一 L2 ネットワーク上のルータやサーバと端末でサブネットマスクの設定値を変えることにより，ルータやサーバにとってはこの L2 ネットワーク全体が 1 つの IPv4 サブネットに見える（**図 5**）が，端末にとっては端末ごとに細分されているように見える（**図 6**）という非対称性を持たせることが特徴である．なお，端末にとっては他の端末が自身とは異なる IP サブネットに属することだけが検知可能であり，他の端末も小さなサブネット（1 端末 1 サブネット）に属していることは認識できない．

単純に上記のような設定を行った場合，端末にとってデフォルト経路のルータも端末とは異なる IP サブネットに属するように見えてしまう．この問題の解決手法が 1 つの課題となる．ただし，あくまでも同一の L2 ネットワークに接続しているので，端末が ARP を送出すればルータは応答し，その応答を端末は受信可能であるし，宛先 MAC アドレスとしてルータの MAC アドレスを持つイーサネットフレームを送出すればそれはルータに届く．

端末相互の通信はルータから見ると冗長経路である，本来ルータは ICMP リダイレクトを送信して端末に対して直接通信を促す（RFC1812[9]）が，この動作は抑止するようにルータを設定する必要がある．

ただし，各端末がブロードキャストを行った場合にはそれは他の端末にも届いてしまう．各端末が到着したパケットを破棄するか受け入れるかは，用いる IPv4 ブロードキャストアドレス等に依存する．

2.2 有効性の検討

サブネットマスクが異なるホストが同一の L2 ネットワークに接続していることは IPv4 の本来の想定外の運用である．

しかし，以下のように IP 通信に支障はないと考えられる．

- 行きと帰りで経路が異なることがある（一方はルータ経由）：
  IP の規定上問題ない．
- L2 ネットワークで直接送信可能な宛先なのにルータにパケットを転送する：
  ルータがパケットの転送を行いさえすれば問題は起きない．
- 直接通信を想定して着信パケットのソース MAC アドレスの内容を用いるプロトコルへの障害：
  IP のアプリケーション層プロトコルではソース MAC アドレスを用いることはないので問題は生じない．ARP 等非 IP プロトコルに関しては本方式の適用外なので，直接端末間でパケットが送受される．

2.3 DHCP の利用

上記のような端末設定を，各利用者の手で確実に行わせることは難しい．そこで，DHCP でこれらの設定を端末に与えることで，利用者側での端末設定の手間を省くことができる．

ここでは 4 つの論点がある．

- dhcp サーバソフトウェアがそのような設定を配布する能力を持っているか．
  dhcp サーバソフトウェアの改造が必要になる場合がある．
- 端末側の DHCP クライアントソフトウェアが，受信した設定値を受け入れるか，不正な値として拒否するか．
- 端末側の OS（IPv4 プロトコルスタック）が上記の設定を受け入れ，期待したように働くか．
- 設定を受け入れた端末がリース期間が終了した際の再割当てや接続終了時に行う DHCP サーバとの通信が，正常に行えるか．

それぞれについて，考察，確認が必要である．

3. 提案方式の分類

端末のネットマスク値をルータと異なる値に設定する方式は，いくつかに分類することができる．ここでは，通常の運用方式，すなわちルータの持つネットマスクと同じものを端末にも設定する方式を便宜上「通常方式」と称する．

本方式ではルータのほかに，情報コンセントの L2 ネットワークに直接接続するサーバ類（DHCP サーバ，プリントサーバ等）等，ルータと同じネットマスク設定を持つ機器が存在することも許容する．

3.1 /30 方 式

端末のネットマスク長を 30 ビット（ネットマスク値が 255.255.255.252）とする方式である．これは通常利用可能な最小サイズのサブネットであり，すべての IPv4 実装に対して適用可能と期待される．

ネットワークサイズは 4 であり，ホストアドレスとして使用可能な IP アドレスは 2 個あるので，それらのうち 2 個をルータと端末に割り当てればよい．30 ビット未満のマスク長でも同様に運用可能であるが，IP アドレスの使用効率の観点からは利点がないので本論文では議論しない．

端末からの外部ネットワークへのパケットは，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，ルータの設定に従って処理される．すなわち，宛先アドレスをルータのインタフェースのネットマスク値で処理すると同一 IP サブネット内にあると分かるので，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．

この方式においてルータ・端末双方が自然なブロードキャストアドレス（自ホスト IP アドレスのホスト部をすべて 1 にしたもの）を用いるように設定すると，ルータと端末が異なるブロードキャストアドレス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．

NetBIOS 名前解決等の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．ただし，rfc1122 [10] では 255.255.255.255 は接続された物理ネットワーク上のすべてのホストによって受信されると規定されているが，インタフェースの初期設定データのブロードキャストアドレスの値として受け付けて働くべきかどうかについては明記されていない．よって，ブロードキャストアドレスとして 255.255.255.255 を設定することは実装依存と考えるべきであろう．

ここで問題になるのは端末からルータへのパケット到達である．単純な手法としては，ルータのインタフェースエイリアスを端末の個数だけ設定して，端末に設定された経路の nexthopIP アドレスを実際にルータに持たせるという方法がある．しかしながら，現在の UNIX や専用ルータは数十あるいは百数十のアドレスを 1 つのインタフェースに与えた場合，効率や管理の手間の点で問題が生じる可能性がある．

ここで，ルータのアドレスが 192.168.1.1 であり，端末が 192.168.1.10/30，端末のデフォルト経路が 192.168.1.9 に設定された場合を例に考える．

端末の IP パケット送信動作について考察してみると，192.168.1.9 を IP レベルの宛先とした通信を端末が行う必要性はほとんどないことが分かる．DHCP サーバへのアドレス割当て継続要求はユニキャストで行われるので，DHCP サーバが 192.168.1.9 で応答する必要はない．動的経路制御や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．

唯一，192.168.1.9 の MAC アドレスを知るための ARP リクエストに，いずれかのホストが応答する必要があるだけである．そこで，192.168.1.n(5,9,13,17,···) 宛への ARP リクエストに対して何らかの機器が応答してルータの MAC アドレスを返せば，端末がルータにパケットを転送する動作は成功する．一般的にはルータ自身が上記の ARP リクエストに応答すればよい．

3.2 /32 方 式

端末のネットマスク長が 32 ビット（ネットマスク値が 255.255.255.255）である場合である．1 端末あたりの仮想的なサブネットのサイズが 1 であるので，IP アドレスの利用効率は高い（100%）．

RFC1122 [10] には，ICMP マスク問合せで得られたネットマスクの妥当性チェックで全ビットが 1 である場合は妥当でないとするべきだと記述されている．またこの方式ではルータの IP アドレスを端末のサブネット内におくことができないため本来動作しないはずの方式である．

後述のように現在の Windows（98/Me/2000/XP）の実装では動作するため，利用価値がある．

3.3 /31 方式

端末のネットマスク長が 31 ビット（ネットマスク値が 255.255.255.254）の場合である．

この方式は RFC3021 [11] をサポートしている OS かあるいは偶然実装が本方式を拒絶しないようになっている場合にのみ動作すると考えられる．

この場合はネットワークのサイズが 2 となる．必要な IP アドレスとして，端末自身，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，端末ともに用いればよい．

3.4 通常-/32 併用方式

端末によって通常方式と/32 方式を使い分け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（端末間通信は L2 直送）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 を設定すればよい．

この場合はどのような 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 サーバ等の台数を除いた残りが割当て可能である．

3.5 /30-/32 併用方式

Windows 以外の OS に対してもパケット監査を行うには，/30 方式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%以下）する．

そこで，Windows 端末には/32 を，それ以外の OS の端末には/30 を設定すれば，IP アドレス空間の無駄が少なくなる．

4. 方式の詳細と確認実験

前節の各方式が適用可能かどうかまた，動作させるために必要な設定の詳細を発見するため，実験を行った．DHCP 経由で設定を配布する場合のほか，可能であれば IP アドレスを静的に設定する形態での動作も確認した．

実験では，NetBSD/i386（1.5.4）をルータ兼 DHCP サーバとして用いた．本方式はルータでパケットフィルタを行うために施行することを前提としているが，実験ではルータでのフィルタ設定は行わず，端末間の通信パケットがルータを通過するか否かを確認した．DHCP サーバソフトウェアは ISC の dhcpd-3.0.1rc9 [12] を用いた．クライアントとして用いたのは，Windows98SE，WindowsMe，Windows2000workstation， WindowsXP professional，NetBSD1.6-release，Linux（カーネル 2.4.26）である．Windows は 2004 年 2 月時点でのサービスパッチ等を適用した状態で実験を行った．実験ではルータは 192.168.1.1/24 を用いた．DHCP クライアントとしての動作実験では各端末は通常の DHCP クライアント設定（出荷時のデフォルトの設定）とした．

2.1 節で指摘したように，ルータでの ICMP リダイレクトの生成を抑止する必要がある．今回ルータとして NetBSD を用いたので，次のような sysctl を行った．

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

4.1 /30 方式

端末には 192.168.1.10/30（ホスト部=2）を割り当て，192.168.1.8，192.168.1.9，192.168.1.11 は他のどの端末にも割り当てずに不使用とする．デフォルト経路としては 192.168.1.9 を端末に与えた．また，ルータで ARP テーブルへの手動登録を**図 7** のように行った．図中の `$MAC` はルータの MAC アドレスとする．

```
arp -s 192.168.12.9 $MAC pub
```

図 7 ARP 設定
Fig. 7 Proxy arp registration.

これにより，端末がパケットをルータに転送する動作はどの端末 OS でも問題なく行われた．

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 サーバを兼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，DHCP サーバはリクエストパケットのソース MAC アドレスではなく DHCP リクエストパケットの ciaddr フィールドのクライアントのハードウェアアドレスフィールド[3] を用いるので，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値がルータと同じ（この例では/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．

```
shared-network DHCP30-NET {
 subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.8 192.168.1.254
                  netmask 255.255.255.252;
  }
}
```

図 8 /30 方式の設定例
Fig. 8 /30 style DHCPD configuration.

/30 方式を DHCP 環境で行うには，1 つの割当てアドレスに対し前後の 3 個を不使用とする必要があるので，ISC 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った．

/30 方式に基づく IP アドレス割当てを行わせるため，dhcpd の改造を行った．具体的には，設定ファイルの range 節の構文規則を変更した．たとえば**図 8** のように

```
range 192.168.1.4 192.168.1.253
    netmask 255.255.255.252;
```

と記述すると，/30 方式を意味する．この場合，指定の IP アドレス範囲のうち，ホスト部が 2 であるものだけが割当て用プールに入れられる．またその端末アドレスに適用されるデフォルト経路はホスト部が 1 であるアドレスが登録される．

また，DHCP 応答パケットを生成する際に，/30 方式の適用対象であれば，端末に通知するサブネットマスク値とデフォルトル経路アドレスを方式に適合するものに書き換えるようにした．

必要な改造は 200 行弱であった．

さらに，ルータが端末にとっての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 設定を動的に行う機能を dhcpd に追加する方式と，使用されうるすべてのアドレスに対して図 7 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うる．今回の実験では後者を用いた．

この dhcpd により動作確認用の DHCP サーバを構成し，今回用いたすべての端末 OS において意図したとおり動作することを確認した．

4.2 /32 方式

端末 PC1（192.168.1.10）にとって，他のすべての端末（PC2, PC3, ···）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 PC1 のローカルな IPv4 サブネットワークの外にあることになる．Windows 経路表[13] エントリは，宛先アドレスと宛先マスク，nexthop IP アドレス，使用インタフェース等から構成されている．経路表を引く時点では nexthop のアドレスに送信可能な interface を検索するという動作はせず，経路表に登録されたインタフェースに対して必要なら ARP による MAC アドレス検索を行って IP パケットを送出すると考えられる．すなわち，この PC1 の例でいえばデフォルト経路（Network Address が 0.0.0.0, Netmask0.0.0.0）として，Gateway Address を 192.168.1.1，使用インタフェース 192.168.1.10 を登録できれば，通信できないはずの nexthop192.168.1.1 に，192.168.1.10/31 のインタフェースから IP パケットを転送する動作をすると考えられる．

調査した結果 UNIX（BSD を含む）ではこのような経路情報は不正な値と見なされて設定することができなかったり，ネットマスクの値をナチュラルネットマスクに自動的に置き換えられたり（Linux）することが分かった．

しかし Windows の現状の実装☆では DHCP サーバから以下のような設定を配布した場合には，これを拒否することなく受け入れ，問題なく運用することができることが分かった☆☆．

Windows で動作に成功した/32 方式の設定は以下のとおりである．

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
ルータ： 192.168.1.1

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，特に阻害されることはなかった．

既存の DHCP サーバ[12] の設定ファイルの記述だけで，/32 方式に基づくアドレス割当てを行うことができる．**図 9** が設定例である．

4.3 /31 方式

実験の結果，Windows はどれもマスク長 31 の設定を受け付けず動作しないことが分かった．

また NetBSD では，ホスト部 0 の側をルータとして設定すると ARP 送信に失敗することが分かった．ホスト部 0 の側を端末，1 の側をルータ，255.255.255.255 をブロードキャストアドレスとして用いなければならない．

動作する OS が限られるうえ，最もシェアの多い Windows に対応できないため，現状では/31 方式を積極的に利用する用途はないと考えられる．

☆ Windows 9x/NT 系双方で確認した．
☆☆ Windows でも手動設定では値が不適正であるとされて設定できない．

```
ddns-update-style interim;
ddns-updates off;
server-identifier 192.168.1.1 ;
option domain-name "example.jp" ;
option domain-name-servers 192.168.1.1 ;
### /32 clients
shared-network NET32 {
   get-lease-hostnames true ;
   subnet 192.168.1.0 netmask 255.255.255.0 {
     option subnet-mask       255.255.255.255 ;
     option broadcast-address 255.255.255.255 ;
     option domain-name-servers 192.168.1.1 ;
     option routers             192.168.1.1 ;
     range 192.168.193.2 192.168.193.249 ;
   }
}
```

図 9 /32 方式の設定例
Fig. 9 /32 style DHCPD configuration file.

```
shared-network DHCP32-and-NATURAL-NET {
 subnet 192.168.1.0 netmask 255.255.255.0 {
  option routers 192.168.1.1 ;
  range 192.168.1.2 192.168.1.254 ;
 }
}
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 10 通常-/32 併用方式の設定例
Fig. 10 Normal/32 co-regidense configuration.

将来，Windows が/32 設定を拒絶しかつ RFC3021 をサポートするするように改変された場合には利用を検討することになろう．

4.4 通常-/32 併用方式

図 10 が端末が Windows であったら/32 方式を，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 9 と同じであるので省略してある．Windows からの DHCP リクエストのオプションフィールド vendor-class-identifier は “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．

4.5 /30-/32 併用方式

/30 方式に対応するように改造した dhcpd を用いると，/30-/32 併用方式も実現できる．**図 11** が，その設定例である．IP アドレス範囲 192.168.1.2〜192.168.1.127 を Windows 端末用に，192.168.1.128〜192.168.1.250 の範囲のうちの 4 つおきのアドレスをそれ以外の OS の端末用に割り当てている．

```
class "windows-clients" {
 match if substring
  (option vendor-class-identifier, 0, 5)
    = "MSFT ";
 option subnet-mask 255.255.255.255 ;
 option broadcast-address 255.255.255.255 ;
}
shared-network DHCP32-and-30-NET {
 subnet 192.168.1.0 netmask 255.255.255.0 {
  option routers 192.168.1.1 ;
 }
 pool {
  allow members of "windows-clients" ;
  range 192.168.1.2 192.168.1.127 ;
 }
 pool {
  deny members of "windows-clients" ;
  range 192.168.1.128 192.168.1.250
   netmask 255.255.255.252 ;
# 192.168.1.252/30 is not used for safety.
 }
}
```

図 11 /30-/32 併用方式の設定例
Fig. 11 /30-/32 co-regidense configuration.

5. 評　　価

前章の実験結果に加えて考察を行い，提案方式を評価する．

5.1 コ ス ト

導入に関しては，DHCP サーバの設定だけで実現できるため低コストである．L2 スイッチに認証機能や VLAN 機能を必要としないため既設のハブやスイッチをそのまま利用できる．既設ルータのフィルタ能力が不足する場合にはルータの交換/増設が必要になるが，安価な PC-UNIX をルータ兼パケットフィルタ装置兼 DHCP サーバとして用いることができる．

運用コストも，DHCP を用いた情報コンセントと同じで，ほとんどの利用者が自力で接続可能であるため，ユーザサポートに人手をとられることが少なく安価である．

5.2 適用範囲と完全性

端末相互の分離の完全性という観点では対象が IPv4 ユニキャストに限定されるという点で，VLAN や PPPoE 等他の方式に劣る．代表的非 IP プロトコルとしては Windows での NETBEUI が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．また既知のウィルスやワームは TCP/IP にて感染動作行うものばかりであるので，本方式は十分に有効であると考えられる．

ブロードキャストには対応していないため，ping of

death のようにパケットの到着がすなわ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．

適用範囲としてはあくまでも悪意のない利用者のうかつな計算機利用への対処に限られると期待すべきであろう，悪意のある利用者が DHCP 設定を無視して固定的なインタフェース設定を行うことで他の端末に L2 で直接通信することは阻止できない．ただし，被攻撃端末からの応答パケットはルータ経由となるので，事態の検出やある程度の対処（応答パケットを破棄することで，攻撃のための通信セッションを成立させない等）は可能である．

5.3 効率と負荷

本来 L2 ネットワークでは端末相互通信は直接行われルータには負荷をかけない．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 サーバ等であり，ルータを経由した外部に存在する計算機である．端末相互の通信はあまり行われないので本方式を利用してもルータを通過するパケット数はあまり変わらないと考えられる．

端末が相互に直接通信する（本方式の利用によりルータの負荷が高まる）のは，たとえば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ともなうパケット
(3) P2P ソフトウェアの稼動にともなうパケット

(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方式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．ただ，教室の端末で P2P の電子会議や高画質 TV 電話を全席でいっせいに行わせるような形態の授業や演習を行う場合には，本方式ではルータの性能限界（フィルタ性能，インタフェース飽和）に問題を起こしやすいと考えられる．

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．

5.4 実装依存性

IPv4 では 1 つの L2 ネットワークに接続したホストは同一のネットマスク値を持つことを想定している．そのため，機器の実装によっては本方式の運用ができない可能性は否定できない．

参考事例としては 1980 年代に多く見られた，サブネット機能のある機器とない機器を同じ L2 ネットワークに接続する事例がある．この場合 proxyarp 等を適切に運用しないとブロードキャストストーム等のトラブルが発生した．

本方式では，ルータがパケットフィルタ動作を行うことを想定している．パケットの着信インタフェースが次段の送信先インタフェースでもあるという状況で異常を起こさないことと，そのようなパケットでもフィルタ操作が可能であることが必要である．

現存する機器の実装状況からすると，以下のような注意を払えば支障はないと考えられる．

- 当該 L2 ネットワークで動的経路交換は行わない．
- パケットが着信したのと同一のインタフェースから出てゆくことを許容する設定ができるルータを用いる．
- ルータでの ICMP REDIRECT の生成を抑止する．

端末の実装依存としては，端末がルータ検索やネットマスク検知動作を行うと動作に支障が生じる可能性があると考えられる．DHCP 以外にネットワーク構成問合せを行わないことが必要である．また，すでに述べたように/32 方式は現在の Windows の実装に依存して利用可能な方式である．また提案方式の中にはブロードキャスト IPv4 アドレスとして 255.255.255.255 をインタフェースに設定する場合が含まれるが，このような設定を拒絶する OS がもしあれば，本方式の情報コンセントの利用ができない．

5.5 IPv6 への適用の可能性

IPv6 でも原理的には同じ方式が適用可能である．しかし，いくつか問題がある．

まず，IPv6 では同一 L2 ネットワーク内のホストはリンクローカルアドレスを使って通信できる．そのため IPv6 対応のウィルスが将来開発されて，リンクローカルアドレスを用いて感染や攻撃をした場合は防げない．

現状では，IPv6 グローバルアドレスの下位 64 ビットは各ホストが自律的に決定する．この場合外部から与えることができる可能性があるのは上位 64 ビットのみである．よって，1 端末あたり/64 サイズの IPv6 アドレス空間を消費することになってしまう．IPv6 サイトが持つネットワークサイズは 70 ビット（16 ビット SLA+64 ビット）であるため，本方式の適用は小規模組織でない限り難しい．

IPv6 でも DHCP（DHCPv6）が規定されている[14]．しかし，現在はプロバイダが家庭のルータにアドレスブロックを配る（Prefix Delegation）場合での使用が予定されている．将来 DHCPv6 が IPv6 ホストの必須実装機能になり現状の DHCP（v4）と同様に多くの OS でデフォルトで有効化されている状況になれば，提案方式をそのまま 128 ビットに拡大することで IPv6 でも利用可能と考えられる．

6. 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 IPv4 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，DHCP サーバ環境で多くの OS に対して実施可能であることを確認した．

本方式により，端末相互でのワーム感染等の事故を防ぐための端末間パケットフィルタをルータのパケットフィルタを用いて行うことが可能になる．一方で本方式は，IPv4 に限定した方式である，ブロードキャストパケットの伝達は止められない，等の制限はあるが，安価にかつ容易に端末保護を実現することができる．

今回は提案方式の実現可能性の確認が主目的であったので，DHCP サーバソフトウェアの内部構造はほとんど変えず，最小限の改造のみを行った．提案方式により端末間の通信をルータのパケットフィルタで処理することが可能になるが，実用に供するにはルータでのフィルタルールの設定も必須である．提案方式を基本構造に取り入れた 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) Leach, P., et al.: CIFS: A Common Internet File System (1996). http://www.microsoft.com/mind/1196/cifs.asp
2) 齊藤明紀，桝田秀夫：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，*IPSJ SIG Notes*, dsm34-4 (2004).
3) Droms, R.: Dynamic Host Configuration Protocol, RFC2131 (1997).
4) Mamakos, L. et al.: A Method for Transmitting PPP Over Ethernet (PPPoE), RFC516 (1999).
5) Hamzeh, K. et al.: Point-to-Point Tunneling Protocol, RFC2637 (1999).
6) 桝田秀夫ほか：生協食堂における無線 LAN サービス実証実験（続編），2003 年 PC カンファレンス，pp.383–384 (2003).
7) Masuda, H. and Nakanishi, M.: Secure wireless LAN service at a COOP cafeteria, *PACRIM'03*, pp.704–707 (2003).
8) 桝田秀夫ほか：教育用計算機システムにおける印刷システムに求められる要求とその実装について，情報処理学会九州支部：火の国情報シンポジウム 2002，pp.107–114 (2002).
9) Baker, F.: Requirements for IP Version 4 Routers, RFC1812 (1995).
10) Braden, R.: Requirements for Internet Hosts — Communication Layers, RFC1122 (1989).
11) Retana, A., et al.: Using 31-Bit Prefixes on IPv4 Point-to-Point Links, RFC3021 (2000).
12) Internet Systems Consortium, Inc: ISC Dynamic Host Configuration Protocol (2004). http://www.isc.org/index.pl?/sw/dhcp/
13) Microsoft Corporation: Windows NT の TCP/IP ルーティングの基本 (ja;140859) (2003). http://support.microsoft.com/
14) Droms, R., et al.: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC3315 (2003).

(平成 16 年 7 月 13 日受付)
(平成 17 年 2 月 1 日採録)

齊藤 明紀（正会員）

平成 3 年 3 月大阪大学大学院博士課程修了．同年同大学基礎工学部助手，情報処理教育センター講師，大学院情報科学研究科助教授を経て，平成 16 年鳥取環境大学情報システム学科教授．工学博士．電子情報通信学会会員．

桝田 秀夫（正会員）

平成 10 年 3 月大阪大学大学院博士課程修了．同年同大学情報処理教育センター助手を経て，平成 12 年サイバーメディアセンター助手．博士（工学）．電子情報通信学会会員．