情報コンセントにおける認証とMACアドレス/IPアドレス偽造防止を実現するシステムLANAの設計と実現

石橋勇人[1]，山井成良[2]，安倍広多[1]，大西克実[1]，松浦敏雄[1]
[1] 大阪市立大学 学術情報総合センター　[2] 岡山大学 総合情報処理センター

概　要

計算機の小型軽量化にともなって，自分の計算機を持ち運んで利用するモバイルコンピューティングの形態が急速に一般化してきている．大学においては，これらの計算機をネットワーク接続するために，情報コンセントを図書館等に設置することへの要望が極めて高い．しかしながら，このようなオープンな環境化では，ネットワークの不正利用を防止することが難しく，このことがこれまでの大きな課題であった．
我々は，正規ユーザのみが情報コンセントを利用することができ，かつ，IPアドレスやMACアドレスを偽造することによる不正なネットワークアクセスを防止できるシステムLANAを開発した．LANAでは，IPアドレスやMACアドレスの事前登録は不要である．
本稿では，LANAの設計と実装について述べる．

LANA: A System for Open Network Access with Authentication and Protection against MAC/IP Address Spoofing

Hayato Ishibashi[1], Nariyoshi Yamai[2], Kota Abe[1], Katsumi Ohnishi[1] and Toshio Matsuura[1]
[1] Media Center, Osaka City University　[2] Computer Center, Okayama University

Abstract

Personal computers are getting much smaller and easier to carry about in these days. LAN sockets providing network accessibility for these mobile computers are often settled in public places like libraries. It is difficult to prevent illegal access to the network in such cases.
We have developed a network access control system named LANA. LANA provides the following functions: (1) Only valid users can access to the network, (2) Preventing invalid use of the network by MAC address and/or IP address spoofing, (3) No need for pre-registration of MAC/IP addresses.
In this paper, we describe the design and implementation of LANA system.

1　はじめに

最近，軽量・高性能な携帯可能小型計算機が比較的安価に入手できるようになってきたため，個人で所有し持ち歩く学生も増えてきた．これに伴い，これらの小型計算機を通して，ネットワーク上の種々のサービスを受けられるように，図書館，情報センター等のパブリックスペースに情報コンセントを設置する大学が増えてきている．

このような環境では，ネットワークの不正利用を防ぐため，ネットワークに対するアクセス制御機構が必要となる．すなわち，正規の利用者だけが情報コンセントを通して，ネットワークにアクセスでき，また不正利用が発覚した場合には，あとで追跡できるような仕組みが必要となる．しかし，情報コンセントに接続される計算機はシステム管理者の管理下にはなく，利用者が自由に設定可能であるため，不正利用対策は容易ではない．特に，IPアドレスやMAC(media access control)アドレスを利用者が偽造すると，従来の不正利用防止手法のほとんどは用をなさない．

我々は，ほとんどの計算機で利用可能なTCP/IPによる通信を対象とし，IPアドレスおよびMACアドレスの偽造にも対応した，情報コンセントに接続された計算機に対する不正防止手法を提案し[4]，システムとして実現することによって動作を確認した(以下では，実現したシステムをLANAと呼ぶ)．本システムでは，正規の利用者であればMACアドレスやIPアドレスの事前登録を必要とせず，任意の計算機を接続できる．また，ユーザ側で既存のOSやアプリケーションを修正する必要がない．

2　情報コンセントにおけるセキュリティ

本手法において想定している利用環境では，情報コンセントは例えば図書館や情報センターなど不特定多数の人が出入りする場所に設置されている．利用者は所有する計算機を情報コンセントに接続し，DHCPサーバから動的にIPアドレスの割り当てを受け，ネットワークにアクセスする．

このような環境では, 誰でも任意の計算機を接続できるため, 以下のような点について考慮してアクセス制御を行う必要がある.

- 正規の利用者以外の者が接続する可能性がある.
- 利用者が計算機の設定を自由に変更したり, MAC アドレスや IP アドレスを偽造したりなどして不正なネットワークアクセスを試みる可能性がある.
- 利用者の所有する計算機の種類は一般には限定できない.
- 正規の利用者の数が非常に多い (学生数が 1 万人以上の大学も多い) 場合がある. 但し, この場合でも, 例えば情報処理センターなどで学生や教職員を一括登録しており, その登録情報を利用して正規の利用者かどうかを認証することは可能であることが多い.

本手法の目的は, このような環境において正規の利用者だけが情報コンセントに接続された計算機から外部ネットワークにパケットを送信できるようにアクセス制御し, また正規の利用者が利用する場合でも誰がいつどこからどの IP アドレスを使ってアクセスしたかを記録できるようにすることである. そのためには, 次の機能が必要である.

1. MAC アドレス偽造防止機能
2. IP アドレス偽造防止機能
3. 利用者認証機能
4. アクセス記録機能

3 不正アクセス防止機能の概要

本章では, 前章で述べた各機能を実現する方法について, その概略を説明する.

3.1 MAC アドレス偽造防止機能

市販のハブには, 各ポートに対して事前登録された MAC アドレスを持つフレームだけを通過させる機能 (MAC アドレスセキュリティ機能) [1] やフレーム内の任意のパターンでフィルタリングしたり中継先のポートを制限したりできる機能 (フレームフィルタリング機能) [5] を持つものがあり, この機能を利用すれば MAC アドレスの偽造を防止することができる. しかし, 本研究で想定している利用環境では計算機の MAC アドレスを接続前に知ることはできないため, これらの機能を単純に用いることはできない.

そこで, 本手法では (1) 接続時には他の計算機で既に利用されている MAC アドレスと同じアドレスの利用を許さない, (2) 接続後は MAC アドレスの変更を許さない, の 2 点を MAC アドレス偽造防止の目標とし, フレームフィルタリング機能を持つハブを用いて次のような方法で MAC アドレスの偽造を防止する.

まず, 初期状態ではフレームフィルタリング機能を用いて, 通信できる範囲を DHCP サーバに限定する. 次に情報コンセントに接続された計算機から IP アドレスの割り当てを要求されると, DHCP サーバは同じ MAC アドレスが使われていない場合に限り IP アドレスを割り当て, その際に当該 MAC アドレスを持つフレームだけを中継するようにフレームフィルタリング機能を設定し, その代わりに通信範囲の制限を解除する.

3.2 IP アドレス偽造防止機能

IP アドレスの偽造防止は, 基本的には DHCP サーバで割り当てた IP アドレスを持つパケットだけを外部ネットワークに中継するようにハブでフィルタリングすることにより行う. しかし, IP アドレスだけでフィルタリングを行うと, 他の計算機に割り当てられた IP アドレスを故意に用いて外部ネットワークに不正にパケットを送出できる可能性が生ずる.

そこで本手法では MAC アドレスの偽造を前節の手法で防止した上で, MAC アドレスと IP アドレスの対でフィルタリングを行う.

3.3 利用者認証機能・アクセス記録機能

利用者認証は, 前節の IP アドレス偽造防止においてフィルタを設定するする直前に行う. このとき, 管理者の負担を軽減するために (ダイアルアップによるネットワークアクセスや Unix ログインのために) 予め登録されているログイン名とパスワードを用いることができる. 認証に成功した時にはフィルタを設定するとともに, 利用者名, MAC アドレス, IP アドレス, ハブとそのポート番号の組合せを記録し, 不正利用時に追跡できるようにする.

4 関連研究

情報コンセントにおけるアクセス制御を行う手法として, MAC アドレスセキュリティ機能を持つハブを用いる手法 (手法 1)[1], DHCP により割り当てた IP アドレスを持つパケットのみをルータで通過させる手法 (手法 2)[2][3], DHCP に認証情報を追加する手法 (手法 3)[8] などがある.

手法 1 は, 予め登録された MAC アドレスを持つ計算機だけがハブを利用できるようにする方法である. しかし, この手法は IP アドレスの偽造を考慮しておらず, また発信 MAC アドレスを正規の MAC アドレスへ偽造されると不正利用を防ぐことができない. また, 接続される可能性のある計算機の MAC アドレスを全て予め登録しておく必要があるため, 管理者の負担が大きくなる.

手法 2 では, DHCP サーバにより割り当てられた IP アドレスを持つパケットだけ外部ネットワークに中継するようにフィルタリングを行う手法である. しかし, この手法は MAC アドレスの偽造を考慮しておらず, また発信 IP アドレスを既に他の計算機に

割り当てられたIPアドレスへ偽造された場合に外部ネットワークへの不正パケットの流出を防げない.

手法3では利用者の計算機がDHCPサーバと共通の暗号鍵を持つかどうかでアクセス制御を行う. しかし, この方法もMACアドレス, IPアドレスの偽造を考慮しておらず, また利用者の計算機に特殊なDHCPクライアントソフトウェアが必要になる.

このように, 既存のアクセス制御手法はいずれもMACアドレスやIPアドレスの偽造を考慮しておらず, ネットワークの不正利用を防ぐことができない.

5 LANAの実現

5.1 システム構成

LANAシステムは, フィルタ機能付きハブと, LANAサーバ, DHCPサーバ, RADIUSサーバ, およびLANAクライアントによって構成される (図1). 図ではLANAサーバ, DHCPサーバ, RADIUSサーバが同一の計算機で動作しているが, 異なった計算機に割り当てても良い.

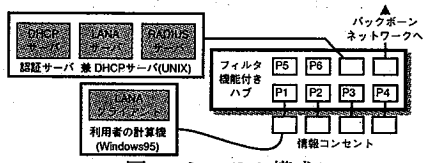

図1: システム構成

フィルタ機能付きハブ 今回実装したシステムでは, MACフレームレベルのフィルタリング機能を有し, SNMP[6]によって制御可能なBay Networks社のスイッチングハブ Bay Stack 301 (BS301)[5]を使用した.

LANAサーバ LANAの中核となるプログラムで, ハブ, DHCPサーバ, RADIUSサーバ, LANAクライアントと通信を行い, ハブのフィルタリング機能を制御する. このサーバは, 今回新規開発したもので, マルチスレッドで構成している. 現在, Solaris2.6上で稼働しているが, POSIX threadが動作する環境ならば容易に移植可能である. SNMPを扱うために, CMUのSNMPライブラリ[11]をマルチスレッド対応に変更して利用した.

LANAクライアント 利用者の計算機上で動作し, ユーザの認証を行うために, LANAサーバと通信を行うプログラム. 今回はWindows95/98用のものをC++で実装した.

DHCPサーバ DHCPサービスを行うプログラムで, 通常のDHCPサーバにLANAサーバと通信する機能を追加したものである. ISC DHCPD[13]を修正することによって実装した.

RADIUSサーバ LANAシステムでは, 利用者のアカウント管理に, RADIUS[9, 10]プロトコルを用いている. RADIUSは, ダイアルアップによるアクセス環境における事実上の標準として広く使用されており, ユーザの認証やアクセス状況の管理が可能となっている.

RADIUSサーバとして, 今回はRADIUSのフリーの実装の1つである, DTC Radius[12]を用いた.

それぞれの関係を図2に示す.

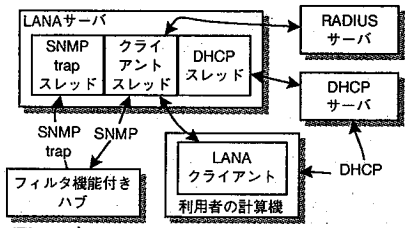

図2: 各サーバ, クライアント間の関係

5.2 フィルタの詳細

BS301のフィルタは, フィルタ式を定義し, ハブの各ポートに対していくつかのフィルタ式から構成されるフィルタグループを割り当てることによって利用する. フィルタグループはフィルタグループ名によって区別する. 一つのポートに複数のフィルタグループを割り当てることができ, この場合, フィルタは割り当てた順に適用される. フィルタ式は64個まで定義することができ, 各ポートにはフィルタグループを最大16個割り当てることができる.

表1: LANAで使用するフィルタ

フィルタグループ名	内容
F_COMMON	1. ARP request/replyは通す 2. IPでなかったら破棄 3. IP optionが付いていたら破棄 4. DHCPクライアントからDHCPサーバへのパケットはDHCPサーバのポートへ転送
F_DROP	1. 全てのパケットを破棄
F_LANA	1. 宛先IPアドレスがLANAサーバでなければ破棄
F_CLnnnn (nnnnはポート番号)	1. 送信元MACアドレスがクライアントのものでなかったら破棄 2. 送信元IPアドレスがクライアントのものでなかったら破棄

LANAで使用するフィルタを表1に示す. このうち, フィルタ *F_CLnnnn* だけはクライアント計算機のMAC/IPアドレスによって内容が異なるため, クライアント計算機の接続時に動的に設定し, その他のフィルタはLANAシステムの初期化時に設定する.

5.3 動作の概要

5.3.1 初期化

LANA サーバは, 利用者の計算機(クライアント計算機と呼ぶ) が接続されるポート (情報コンセントに接続されている) の全てに, フィルタ (F_COMMON, F_DROP) をこの順序で割り当てる. これによって, DHCP 以外の通信を遮断する. 認証サーバおよびバックボーンに接続されたポートに対してはフィルタを設定しない.

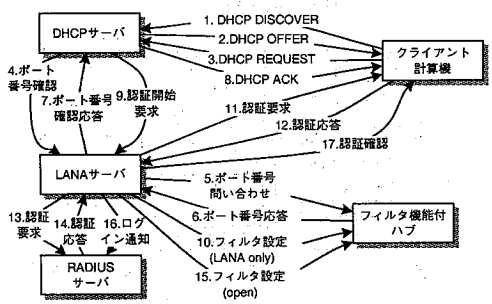

図 3: 接続シーケンス

5.3.2 利用者計算機の接続方法

利用者計算機の接続は, 図 3 のシーケンスで行われる.

1. 利用者は, 接続に先だってクライアント計算機上で LANA クライアントを動作させておく.
2. 利用者がクライアント計算機を情報コンセントに接続する. クライアント計算機は, 使用する IP アドレスを取得するために通常の DHCP のシーケンスを発行する (図 3 の 1–3).
3. DHCP のメッセージは DHCP サーバが受信する. LANA の DHCP サーバは, DHCP REQUEST に対して IP アドレスを付与する直前に, LANA サーバに対してポート確認要求を送信し, 利用者計算機が使用しているポート番号を問い合わせる (図 3 の 4).
4. LANA サーバはポート確認要求を受信すると, ハブの MAC アドレステーブルを検索し, 当該クライアントが接続されているハブとポート番号を特定する. ポート番号が特定できた場合には, その番号を DHCP サーバに返す. ポート番号が得られなかった場合には, エラーを返す (図 3 の 5–7).
5. DHCP サーバは, LANA サーバがポート番号を特定できればクライアント計算機に IP アドレスを付与し (DHCP ACK), LANA サーバに対して認証開始要求を送信して認証シーケンスの開始を要求する (図 3 の 8–9). ポート番号を特定できなかった場合は DHCP NAK を返し, クライアントに IP アドレスを与えない.
6. LANA サーバは, 認証開始要求を受けとると, 当該クライアント計算機の MAC アドレス, IP アドレスからではないパケットを破棄するようなフィルタ F_CLnnnn を設定し (nnnn はクライアント計算機が接続されたポート番号), クライアントが接続されたポートのフィルタを (F_COMMON, F_CLnnnn, F_LANA) と設定する. これによって, 当該ポートからは, クライアント計算機以外のパケットは通さないようになる. また, この段階では F_LANA によって, クライアント計算機は認証サーバとは通信できるが, 認証サーバ以外との通信はできない.(図 3 の 10).
   次に, LANA サーバはクライアントで動作している LANA クライアントと TCP コネクションを張り, 認証情報を要求する. LANA クライアントは, 画面にウインドウをポップアップし, 利用者からユーザ名, パスワードを受け取り, LANA サーバに送信する (図 3 の 11–12).
7. LANA サーバはユーザ名, パスワードが正しいかどうかを RADIUS サーバに問い合わせる (図 3 の 13–14). 正しい場合, 以下の処理を行う (図 3 の 15–17).
   - フィルタを (F_COMMON, F_CLnnnn) と設定し, 全てのホストと通信できるようにする.
   - RADIUS サーバに対して当該ユーザがログインしたことを伝える.
   - LANA クライアントに対して, 認証に成功したことを伝える.

   なお, LANA サーバと LANA クライアントとの間の TCP コネクションはクライアントが接続されている間は維持されており, 接続の確認や切断の要求に使用する.

5.3.3 利用者計算機の切断方法

クライアントがネットワーク接続を切断する際, LANA サーバはフィルタの設定を初期状態 (F_COMMON, F_DROP) に戻し, RADIUS にログアウトを通知する. これは, 以下の契機に行われる.

- LANA クライアント上で切断操作を行い, 切断通知が LANA サーバに送信された場合.
- ハブから SNMP トラップ (Link Down トラップ) が送信された場合. これは利用者が情報コンセントからコネクタを引き抜く, あるいはクライアント計算機の電源を切断することによって発生する.
- LANA サーバと認証クライアント間のコネクションが切断された場合.

5.4 実装上の留意点

LANA システムを実装する上での留意点を述べる.

5.4.1 DHCP サーバとの通信維持

何らかの原因で LANA サーバと LANA クライアントの間で状態の不整合が発生すると, ポートに MAC/IP アドレスフィルタが設定されたまま放置される可能性がある. この状態では, 他の計算機を接続しても通信ができない. このため, DHCP のメッセージは MAC/IP アドレスに関わらず全て通すようにフィルタ F_COMMON を設定するようにした (F_COMMON の 4 番目の式). これにより, どの計算機を接続しても DHCP による IP アドレスの取得から再試行できる.

5.4.2 カスケードハブ問題

LANA システムのハブに, 利用者が別のダムハブ (スイッチング機能のないリピータハブ) をカスケード接続し, 複数の計算機を接続することを許した場合, トラフィックの盗聴の可能性がある. このため, LANA ではハブの 1 ポート当り 1 計算機のみの接続しか認めないこととした.

このため, LANA サーバがポート確認要求を受信してポートを特定する時に, 当該ポートが他のクライアント計算機によって使用されていないかをチェックする (存在確認用のメッセージを送信). 使用されていた場合, 後から接続したクライアントには接続を認めない (DHCP サーバにエラーを返す).

5.4.3 DHCP REQUEST の再送

クライアント計算機が DHCP で IP アドレスを取得するとき, DHCP REQUEST を出してから DHCP ACK/NAK を受信するまでに, DHCP クライアントが DHCP REQUEST を再送して, DHCP サーバが再度 DHCP REQUEST を受信する場合がある. また, DHCP クライアントは, 貸与されたアドレスの使用期限を延長するためにも DHCP REQUEST を送信する [9].

DHCP サーバの変更点を最小限にするため, 再送された DHCP REQUEST に対しても DHCP サーバは LANA サーバにポート確認要求を送信する. LANA サーバは, 認証中あるいは認証済のクライアントに対するポート確認要求に対しては DHCP サーバに特別な応答を返すようにした. DHCP サーバはこの応答を受け取ると, 認証開始要求は送信しない.

5.4.4 DHCP のアドレス開放

LANA サーバでは, DHCP クライアントからのアドレス開放 (DHCP RELEASE) に対しては, 特に対処を行っていない. これは, DHCP RELEASE は必ずしも送信されるとは限らないのと, クライアント計算機の切断は別の契機で判断できるためである.

6 評価

6.1 スケーラビリティ

ここで実現したシステムでは, 1 つの LANA サーバが複数台のハブをコントロールすることを仮定している. DHCP サーバに関しては, それぞれが管理するアドレスを独立な空間から割り当てることによって複数台設置可能である (これは, 通常の DHCP の運用と同じ条件である). ユーザの管理は RADIUS サーバによって行っているが, これは大規模ダイアルアップ環境において広く使われているサーバであり, 十分にスケーラブルであると考えられる. したがって, LANA サーバのスケーラビリティについて考察する. なお, 互いに管理するハブが異なっていれば 1 つのネットワークに複数の LANA サーバが同時に存在しても問題はないので, LANA サーバを増やすことによって処理能力を上げることが可能である.

6.1.1 処理時間による制約

現在使用しているハブである BS301 では, フィルタリング等の設定を書き込む一連の処理において排他制御が必要であり, 同時に複数実行することができない. このため, この処理の実行時間によって単位時間に処理できる (1 ハブあたりの) ユーザ数が決まってくる. そこで, LANA で必要とされる 3 種類のフィルタリングのそれぞれについて, 設定に要する時間を計測した. この結果 (15 回計測した平均値) を表 2 に示す.

表 2: フィルタリングの設定に要する時間

フィルタ設定	時間 (ms)
初期設定	23.5
認証時の設定	35.0
認証成功後の設定	23.5

ところで, DHCP においてクライアントが DHCP REQUEST メッセージを送出してから DHCP ACK/NAK メッセージを受け取るまでの典型的なタイムアウト値は, 最初に DHCP REQUEST の再送を試みるまでが 4±1 秒, 最終的にあきらめて DHCP シーケンスを最初からやり直すまでは 64 秒である [7].

これらのタイムアウト値は, 1 クライアントのフィルタの設定に要する時間 (23.5ms〜35.0ms) に対して十分長く, LANA システムのために追加された処理が DHCP シーケンスに及ぼす影響は無視できると考えられる.

6.1.2 フィルタ数による制約

LANA サーバにおいて設定するフィルタのうち, クライアントに依存するのは前述の F_CLnnnn のみである. これは, クライアント数 (すなわちハブのポート数) に比例する数が必要となる. ハブには,

これに残りの定数個のフィルタを加えた合計の数だけフィルタが定義できる必要がある.

現在使用している BS301(24 ポート) では, 最大 4 + 1 + 1 (それぞれ F_COMMON, F_DROP, F_LANA で使用する数) +2 (F_CLnnnn で使用する数) × クライアント用ポート数 (22) = 50 個 のフィルタを定義する可能性があるが, この値は上の要件を満たしており, 現実的にそれほど無理のない制約であると思われる.

6.2 セキュリティレベル

3 章で述べたように, 本システムではクライアントにおける MAC アドレスおよび IP アドレスの偽造による不正アクセスを防ぐことができる. ここでは, それ以外に不正アクセスあるいは運用妨害につながりそうな手段について検討する.

6.2.1 偽 DHCP サーバ

悪意のあるユーザが偽の DHCP サーバを稼動させた場合を考える.

他のポートからの DHCP REQUEST メッセージはフィルタによって正しい DHCP サーバにのみ届くため, 偽の DHCP サーバによる影響はない.

6.2.2 偽造 ARP

悪意を持つユーザが ARP reply メッセージを偽造し, 他のユーザ宛ての ARP reqeust に対して自分の IP アドレスで答えた場合について考える.

この場合には, やはりハブに設定されたフィルタによってパケットはハブのポートを通過できないため, 悪意のあるユーザが他人の IP アドレスをかたって不正を働くことはできない.

6.3 機種依存性

6.3.1 ハブ

今回実装したシステムでは, BS301 のフレームフィルタリング機能等を使用している. ここで, ハブに必要とされる機能は, (1) 指定した送信元 MAC アドレスによるフィルタリング機能, (2) 指定した送信元 IP アドレスによるフィルタリング機能, (3) 指定した TCP/UDP ポート番号によるフィルタリング機能, (4) 指定した MAC アドレスのホストがどのポートに接続されているかを調べる機能, (5) これらを SNMP によって制御する機能 (トラップを含む), である. これらの機能を有するハブであれば, BS301 以外の機種でも使用可能である.

6.3.2 クライアント

今回実装した LANA クライアントは Windows95/98 用に Visual C++環境で開発されており, OS に依存している. 現在 Java による同様なクライアントの実装を進めており, これによって, JavaVM が動作する計算機であれば同様に利用可能となることが期待される.

7 おわりに

本稿では, オープン利用される情報コンセントにおいて, ユーザの認証により正規ユーザのみの利用を許し, かつ, アドレスの偽造による不正なアクセスをも防止するシステム LANA について述べた. 今後のユーザ数の増大とネットワークの広がりを考えると, このようにセキュリティに十分配慮したネットワーク運用がますます重要となると考えられる.

謝辞 LANA システムの開発にあたり, システムの実装に協力していただいた大阪市立大学大学院工学研究科 伊佐岡慶浩氏, 阪本晃氏, ならびに来山至氏に感謝いたします.

参考文献

[1] アライドテレシス (株) 編: Perfect Networker Ver.1.0, アライドテレシス (株), 1997.

[2] 小林, 山口: "DHCP 環境におけるアクセス制御についての考察", 情報処理学会マルチメディア通信と分散処理研究報告, 78-9, pp.49–54, 1996.

[3] 久長, 岡田, 刈谷: "情報コンセントのユーザ認証について", 学術情報処理研究, No.2, pp.77–81. 1998. (http://www.sv.cc.yamaguchi-u.ac.jp/jacn/journal/pp077)

[4] 山井, 石橋, 安倍, 大西, 松浦: "情報コンセントに接続された計算機に対する MAC アドレス/IP アドレスの偽造防止手法", 情報処理学会コンピュータセキュリティ研究会コンピュータセキュリティシンポジウム'98 論文集, pp. 141–146, 1998.

[5] Bay Networks: "Using the BayStack 301 Ehternet Switch", Bay Networks, 1996.

[6] J.D. Case, M. Fedor, M.L. Schoffstall, and C. Davin: "Simple Network Management Protocol (SNMP)", RFC 1157, 1990.

[7] R. Droms: "Dynamic Host Configuration Protocol", RFC 2131, 1997.

[8] R. Droms, W. Arbaugh (eds): "Authentication for DHCP Messages", draft-ietf-dhc-authentication-09.txt, Internet Draft, 1998.

[9] C. Rigney, A. Rubens, W. Simpson, S. Willens: "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, 1997.

[10] C. Rigney: "RADIUS Accounting", RFC 2139, 1997.

[11] http://www.net.cmu.edu/projects/snmp/

[12] http://www.dtc.co.jp/Radius/

[13] http://www.isc.org/dhcp.html