社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38 (17)
2007／7／19

認証ネットワークにおける未承認接続の排除方法に関する提案

三宅 猛† 鈴木 春洋†† 北野 文章†† 岩田 彰†

† 名古屋工業大学大学院 〒466-8555 名古屋市昭和区御器所町
†† 株式会社 中電シーティーアイ 〒450-0003 名古屋市中村区名駅南 1-27-2
E-mail: †takes@mars.elcom.nitech.ac.jp, iwata@nitech.ac.jp, ††{Suzuki.Shunyou,Kitano.Fumiaki}@cti.co.jp

あらまし LANにおいてネットワーク認証システムを構築するためのIEEE802.1Xという技術がある．LANスイッチと認証サーバにより実現されるIEEE802.1X認証システムは，未許可端末からの不正接続防止に有効である．しかし実際には，リピータハブを介しての接続や基幹ネットワークへの接続などにより，未許可端末によるLANへの接続が可能となっている．そこで本稿では，ARP偽装を用いた接続無効化システムの設定部分に，IEEE802.1X認証による認可情報を利用することにより，ネットワーク管理者による端末の登録を不要とした，不正接続排除システムを提案する．

キーワード IEEE802.1X, RADIUS, ARP

A Method of Excluding Disapproval Connection on Authentication Network

Takeshi MIYAKE†, Shunyo SUZUKI††, Fumiaki KITANO††, and Akira IWATA†

† Nagoya Institute of Technology Gokisocho, Syouwa-ku, Nagoya-shi, 466-8555 Japan
†† Chuden CTI CO.,LTD Meiekiminami 1-27-2, Nakamura-ku, Nagoya-shi 450-0003 Japan
E-mail: †takes@mars.elcom.nitech.ac.jp, iwata@nitech.ac.jp, ††{Suzuki.Shunyou,Kitano.Fumiaki}@cti.co.jp

Abstract IEEE802.1X is a technology to construct the network authentication system on LAN. The IEEE802.1X authentication system which achieved by LAN switch and the authentication server is effective to an illegal connected prevention from the teminal of the unpermission. However, it is possible to practually connect to LAN with the unpermission terminal by the connection through the repeater hub and the connection to key network. In this paper, we propose the system that excludes an illegal connection from the network, without registering the terminal, by using IEEE802.1X authorization information, in the system that exclude illegal connection by the ARP camouflage.

Key words IEEE802.1X, RADIUS, ARP

1. はじめに

近年，インターネットやイントラネットの普及に伴い，不正接続による情報漏洩やウイルス感染などの被害が拡大している．特に企業・大学などの組織ネットワークにおいては組織外部からの侵入だけでなく、組織内部での接続に対しても配慮する必要がある．

組織内ネットワークにおける不正接続防止に有効な技術として，ネットワーク接続時にユーザ認証を行うことで不正接続を排除するIEEE802.1Xがある．現在では無線LANでの利用が主となっているが，IEEE802.1Xは有線LANにも対応した規格となっており，それぞれIEEE802.1Xの規格に対応したアクセスポイントやLANスイッチを使用することで実現が可能である．

しかし，有線LANにおいて，このIEEE802.1X認証システムを構築した場合，LANスイッチはポート単位でアクセスの制御を行っているため，端末との間にリピータHUBを挟むと，1台の端末が認証に成功すれば同じHUBに接続された他の端末は認証無しで接続が可能となる．もしくは，LANスイッチを介することなく，直接基幹ネットワークに接続してしまえば，容易にLANに接続できる．このようにIEEE802.1X認証システムを実際に有線LAN上で運用するには，安全性において本質的な問題があり，これら想定外の接続を排除する仕組みが必要となる．

IEEE802.1X 認証システムとは別に，許可しない接続をネットワーク上から排除する方法として ARP 偽装技術の利用が挙げられる．しかし，この方法によりシステムを実現する場合，許可する端末のアドレスを予め設定しておく必要があるため，大規模なネットワーク環境では変更や追加の管理が煩雑となる．

本稿では，ARP 偽装を用いた不正接続を排除するシステムの設定に関して，IEEE802.1X 認証により認証サーバで送受信される認証情報を取得して，認可済み端末の物理アドレスを登録することにより，設定作業にかかる負担を軽減するシステムを提案する．また，本提案では従来の IEEE802.1X 認証システムに大きな変更を加える事なく，想定外の接続の排除を可能にすることを目的とする．

2. IEEE802.1X 認証システム

IEEE802.1X は端末と LAN スイッチ間の接続や無線端末とアクセスポイント間の接続において，ポートに接続されている端末を認証し，認証プロセスに失敗した端末から LAN への接続を防止する規格である．本章では IEEE 802.1X の概要について述べ，問題点を説明する．

2.1 概　　要

IEEE802.1X 認証システムを構成する要素は 3 つある．認証を受ける端末に必要なソフトウェア（Supplicant），認証結果によりポートの開閉を行う LAN スイッチやアクセスポイント（Authenticator），ユーザ情報を管理する認証サーバ（Authentication Server）である．認証サーバとして一般に RADIUS サーバが利用される．

Supplicant と Authenticator 間のプロトコルには PPP の認証手順を拡張した EAP over LAN を，Authenticator と RADIUS サーバ間には RADIUS 認証プロトコルを拡張した EAP over RADIUS を用いる．

図 1　IEEE802.1X

EAP（PPP Extensible Authentication Protocol）は PPP（Point to Point Protocol）を拡張し、認証機能を備えたプロトコルであり，パスワードにより認証を行う EAP-MD5 や公開鍵証明書を利用して相互認証を行う EAP-TLS など，様々な認証方法を使用することができる．

有線 LAN における IEEE802.1X 認証システムの動作を図 2 に示す．

始めにサプリカントが LAN スイッチに対して認証の開始を要求し，EAP によるネゴシエーションが行われる．その後，サプリカントと RADIUS サーバの間で暗号仕様及び証明書の交換などが行われ，RADIUS サーバが正当なユーザであると判断した場合，認証の成功を意味する RADIUS Access-Accept パケットを LAN スイッチに送信する．最後に LAN スイッチは EAP-Success パケットをサプリカントに送信し，ポートを開けて端末を LAN に接続させる．

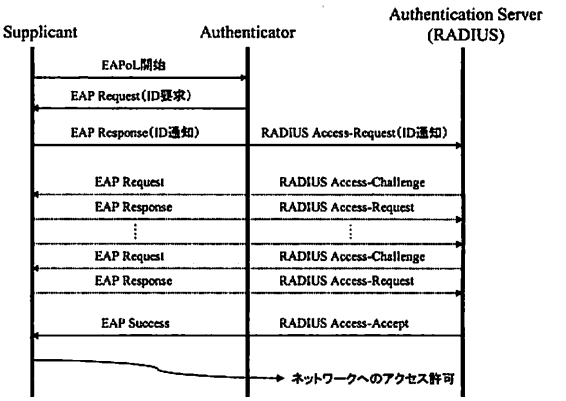

図 2　IEEE802.1X の動作

2.2 問　題　点

IEEE802.1X 認証システムではユーザ認証を行うことにより，LAN スイッチのポートで端末の接続を制御することができるため，VLAN などの技術と組み合わせた効果的な利用が可能である．システムを構築する場合には，LAN スイッチは IEEE802.1X の規格に対応している必要があり，また，利用するユーザの分だけポートが必要となる．しかし，実際にはこれらの条件を満たしても全ての接続を管理できるわけではなく，有線 LAN 上の IEEE802.1X 認証システムではネットワーク管理者の意図しない接続により以下のような問題が発生する．

問題点の 1 つが，LAN スイッチのポートにリピータ HUB を接続した場合である．LAN スイッチは一端ポートが開くと，認証が有効な間は全てのパケットを通すようになるため，リピータ HUB に別の端末が接続されている場合，その端末は IEEE802.1X による認証を行うことなく LAN に接続できてしまう．しかし，多くの LAN スイッチでは，認証に成功した端末の MAC アドレス以外を遮断する機能を持っており，この問題は解決している場合が多い．

同様の問題として，認証用の LAN スイッチを介さずに接続する場合が挙げられる．基幹 LAN にリピータ HUB 等を設置して接続した場合，当然 IEEE802.1X による認証は行なわれないため，容易に LAN に侵入することが可能となる．

このように，有線 LAN で IEEE802.1X 認証を実現する際には，認証をすり抜けて接続される可能性を考慮に入れる必要がある．

3. ARP 偽装技術

通常端末がネットワークに接続する場合，ARP の要求（ARP Request）と応答（ARP Reply）により，通信相手の MAC アドレスを取得し，IP アドレスと MAC アドレスの組み合わせ（ARP エントリ）の一覧である ARP テーブルを作成する．

この ARP パケットを偽装することにより，対象の端末の ARP テーブルを強制的に書き換え，通信を制御することがプロトコルの仕様上可能 [1] となっており，ARP spoofing 技術と

して知られている．

ARP の基本動作は以下の通りである．

（1） 送信先情報が自分のアドレスである ARP パケットを受信した場合，送信元情報を無条件に ARP エントリとして ARP テーブルに反映する．ブロードキャストの自分宛ではないパケットは無視する．(送信先情報がブロードキャストである場合は，ARP テーブルに該当するエントリが存在すれば書き換える)

（2） その後に，ARP Request ならば自分の情報を送信元情報に設定し ARP Reply として送信元に送る．

（3） ARP パケットによる更新後，使用されなかった ARP エントリは一定時間が経過すると ARP テーブルから削除される．

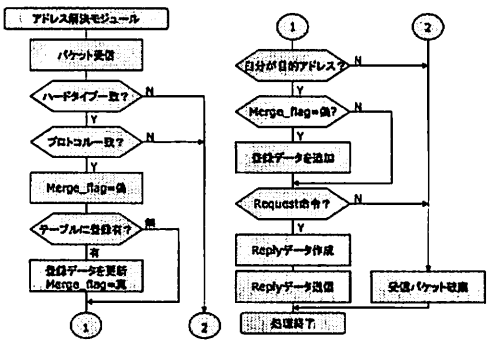

図 3 ARP アドレス解決モジュールの動作

この ARP を用いてネットワークの管理を行うツールとして，IP sentinel [3] や dsniff [4] 等が存在する．

IP sentinel では図 4 に示すように，通信を行おうとして ARP Request をブロードキャストした端末に対して，送信元情報に偽の MAC アドレスが記載された ARP Reply を返すことにより ARP テーブルの上書きを行う．上書きされるアドレスはネットワーク上に存在しないものであるため，ARP テーブルを書き換えられた端末は通信を行うことが不可能となる．接続を許可させたい端末のアドレスを予め登録しておき，未登録のアドレスに対して，これらの偽装を行うことで，簡単に不正接続を排除するネットワークを実現できる．

IP sentinel の動作と設定方法の例を以下に示す．

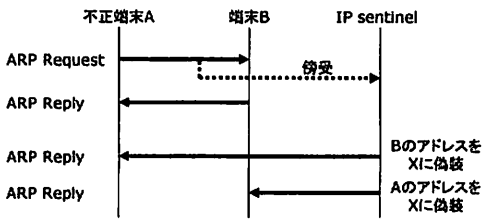

図 4 IP Sentinel の動作

このようなツールを用いて不正接続を排除するネットワークを実現する場合，図 5 に示す様に，予め接続を許可する全ての端末について，アドレスを登録しておく必要がある．ネットワークに端末を追加，又は削除する度に設定の変更が必要となるため，大規模ネットワークにおいては管理が煩雑である．また，すでに接続されていない端末のアドレスが登録されたまま残っていると，アドレスを不正利用して侵入される可能性がある．

```
0.0.0.0/0
*@!aa:aa:aa:aa:aa:aa
*@!bb:bb:bb:bb:bb:bb
*@!cc:cc:cc:cc:cc:cc
```

図 5 アドレスの設定例

4. 提案方式

本章では，第 2 章と第 3 章で挙げられたような不正接続排除システムにおける課題を解決する方法を提案する．

第 3 章で述べたように，ARP 偽装により不正接続の排除を行うためには，利用を許可する端末の MAC アドレス（もしくは IP アドレス）を登録する必要があるが，本提案では IEEE802.1X 認証システムを利用して，認証成功時にサーバに認可された端末のアドレスを取得し，許可アドレスとして登録を行うこととした．これにより，認証に成功した端末にのみ，接続の許可が与えられるため，管理者は LAN にどんな端末が接続されているかを意識する事なく，認証サーバのユーザ情報を管理するだけで良くなる．

提案方式により，認証を通過していない接続も全て排除されるため，第 2 章で述べたような問題も同時に解決され，従来の IEEE802.1X 認証システムよりも高い安全性を実現できる．また，IEEE802.1X 認証システムと ARP 偽装により排除を行うシステムは機能が完全に分離されているため，現状の IEEE802.1X のシステムに対して大きな変更を行う必要はなく，新たに装置を追加するだけで実現が可能である．

4.1 提案システム概要

提案するシステムの構成を図 6 に示す．

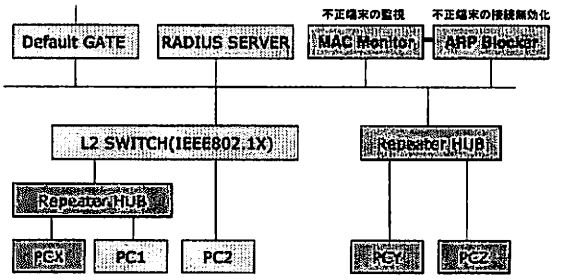

図 6 提案システム

図中の PCX，PCY，PCZ は 2.2 で説明した方法により，不正に接続を行おうとする端末である．

提案システムでは従来の IEEE802.1X のシステムに，認証の成功を検知し，接続を許可するアドレスの登録管理を行う機能

(MAC Monitor) と不正端末の接続を検知し接続無効化を行う機能 (ARP Blocker) を追加する．具体的な動作については次節で説明する．

それぞれの機能は独立した装置として実装されていることが望ましい．これは，ARP Blocker が何らかの理由により動作不能となった場合でも，MAC Monitor により常時ネットワークの監視だけは行えるようにするためである．

4.2 提案システムの動作

提案システムの全体の動作を図 7 に示す．

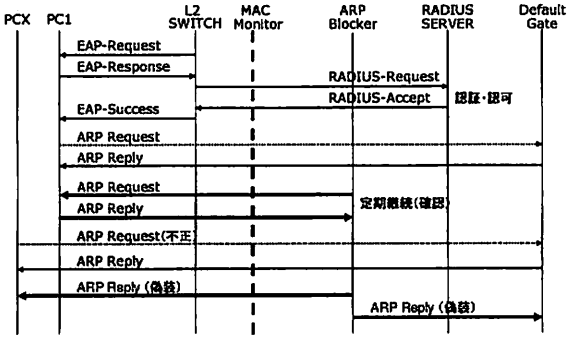

図 7 提案システムの動作

MAC Monitor と ARP Blocker のそれぞれの動作は以下の通りである．

4.2.1 MAC Monitor の動作

MAC Monitor はプロミスキャスモードで動作し，受信のみを行う．

(1) IEEE802.1X による認証成功後に RADIUS サーバから送信される認可パケット (RADIUS Accept) を受信した場合，認証に成功した端末の MAC アドレスを取得し，接続認可アドレスとして ARP Blocker に登録する．

(2) 接続認可アドレスには，ARP Blocker から定期的に ARP Request を発行して，MAC Monitor で接続状態を把握する．

(3) ARP Request に対する Reply が 2 回続けてない場合は，接続が切断されたものとして管理対象から外す．

4.2.2 ARP Blocker の動作

ARP Blocker は MAC Monitor によって更新される登録情報に従い，接続された端末の状態確認と拒否端末の ARP 偽装を行う．

(1) 基幹スイッチ，ゲートウェイ，認証サーバなどネットワークを構成する基本装置の MAC アドレスは例外アドレスとして登録しておく．

(2) ARP Blocker に登録されていない MAC アドレスからの ARP Request が LAN 上に送信された場合，不正接続と見なして ARP Reply による偽装を行う．また，ARP Reply のブロードキャストを行うことにより，LAN 上の端末の ARP テーブルに不正端末のエントリが存在していた場合に，該当エントリを書き換える．

(3) 接続認可アドレスには，ARP Blocker から定期的に ARP Request を発行して，MAC Monitor で接続状態を把握する．

4.3 認可アドレスの検出

4.3.1 RADIUS プロトコル

IEEE802.1X 認証システムでは LAN スイッチと RADIUS サーバの間は RADIUS プロトコルにより通信が行われる．RADIUS プロトコルはサーバクライアント間において認証 (Authentication)，認可 (Authorization) 及びアカウンティング (Accounting) の処理に必要な情報を伝送するための UDP ベースのプロトコルである．RADIUS パケットの構造を図 8 に示す。

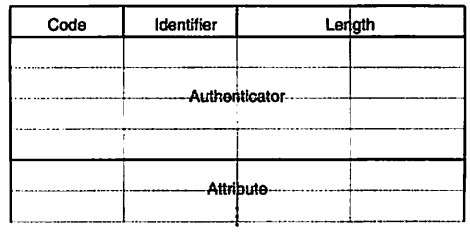

図 8 RADIUS パケットの構造

RADIUS パケットは Code (種別コード) によって用途が分けられる．一般的に使用される種別コードとしては端末からサーバへの要求を意味する Access-Request や，接続の許可を意味する Access-Accept がある．

Identifier (識別子) は要求パケットと応答パケットの対応付けのために使われ、要求ごとに異なる値を入れる必要がある．

Authenticator (認証符号) はパスワードを隠蔽して正しい RADIUS サーバにしか解読できないようにするために利用される．また，データの改竄防止に利用される．

Attribute (属性情報) にはユーザの ID やパスワードなど，認証を行うのに必要な情報が入る．IEEE802.1X 認証では Access-Request の場合，この部分には端末や LAN スイッチの MAC アドレスも記述される．

提案システムではこれらの値を確認することにより，認証の成功を検知し認可された端末の MAC アドレスを検出する．

4.3.2 検出方法

前提条件として，MAC Monitor は RADIUS パケットを取得するために，プロミスキャスモードで動作し，LAN スイッチと RADIUS サーバの間を流れるフレームは全て MAC Monitor に届く状態にする．

MAC Monitor は IEEE802.1X 認証により送信されるパケットを監視し続け，Access-Request を種別コードに持つ RADIUS パケット (RADIUS Request) を検知すると，そのパケットを一時的に保持しておく．その後，Access-Accept を種別コードに持つ RADIUS パケット (RADIUS Accept) を検出すると，その識別子を確認し，保持されている RADIUS Request の識別子と一致すれば，属性情報の中から端末の MAC アドレスを取り出し，ARP Blocker の登録リストに追加する．

RADIUS Accept を受信する度に識別子（Identifier）を確認するのは，同時期に複数の認証が行われて RADIUS パケットが混在していた場合に，RADIUS Accept がどの RADIUS Request に対するものであるかを区別するためである．本提案では識別子により認証を区別しているが，この識別子は長さ 1 バイトであり，つまり 1 から 256 までの値しか存在しないため，認証頻度の高い環境では他の認証と衝突が起こる可能性がある．そのような場合には，別の認証を識別する値，例えば，属性情報の中のユーザ名や LAN スイッチのアドレスなどを一緒に確認することにより，MAC アドレス取得時の誤動作を防ぐ必要がある．

4.4 接続状態の把握

ARP Blocker に登録されたアドレスは，放置しておくと不正接続を許す要因となるため，端末が切断された後は速やかに削除する必要がある．そのため，MAC Monitor は登録された端末の接続状態を常に把握しておく必要がある．しかし，端末が接続を切断されたことを通知するような動作は，IEEE802.1X 認証のプロセスには含まれていないため，認証サーバで送受信されるパケットからは判断することができない，そこで，ARP Blocker から定期的に登録端末宛ての ARP Request を送ることにより各端末の接続状態を確認する．

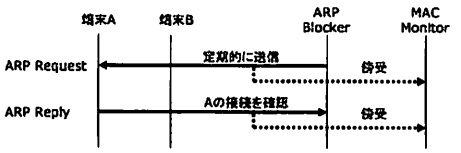

図 9 接続状態の把握

ARP Request を数回繰り返しても ARP Reply が返ってこなければ，MAC Monitor は端末が接続されていないものと判断し，登録リストから削除する．

4.5 ネットワークへの影響

動的な ARP エントリは参照されることなく一定時間が経過すると，ARP テーブルから削除される．ARP テーブルからエントリが削除された端末と通信を行う場合は，ARP Request により再度 MAC アドレスを取得して ARP テーブルを更新することになる．そのため，ARP エントリが削除されるまでの間隔が短いと，ARP Blocker による偽装が頻繁に行われることになり，ネットワークへの負荷が増大する可能性がある．

表 1 は主な OS における ARP テーブルのエントリ保持時間であるが，これらの値を参考にすると，ARP Blocker による偽装は大体数分の間隔で行われると予想できるため，ネットワークに対する負荷は無視できる範囲であると考えられる．

5. 評　　価

提案システムに懸念される問題として，ARP Blocker における登録アドレスの反映時間がある．提案システムでは IEEE802.1X 認証システムの認証結果に基づいて接続認可アドレスの設定を行うため，LAN スイッチが認証結果を受けてから，端末の通信を許可するまでの時間が短いと，ARP Blocker に設定が反映されるより前に，端末により ARP が送信されて，認証に成功したはずの端末の接続が無効化されてしまう危険性がある．そこで，提案システムの性能に関して以下の評価を行った．

表 1 ARP テーブルのエントリ保持時間

OS	ARP エントリ保持時間（分）
Windows XP Professional SP2	2
RedHat Linux 9	7〜10
Vine Linux 4.1	3〜9
Solaris 8	約 26
FreeBSD 6.2	約 23

5.1 評 価 環 境

提案システムの実装には，ARP Blocker としてフリーのソフトウェアである IP sentinel を利用した．また，MAC Monitor と ARP Blocker の機能を同一サーバ上に配置した．評価環境の詳細は以下の通りである．

表 2 機 器 構 成

RADIUS サーバ	FreeRADIUS 1.0.5
認証端末	Microsoft Windows 2000 SP4
LAN スイッチ	Cisco Catalyst 2950

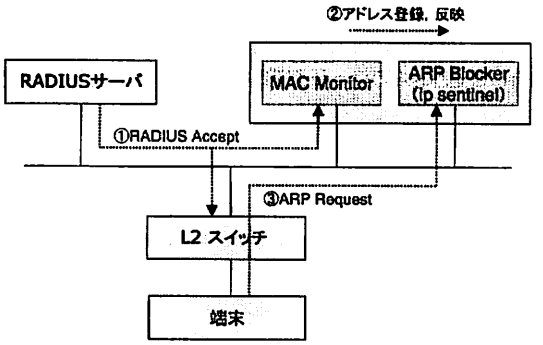

図 10 提案システムの実験環境

また，提案システムの実装に利用したソフトウェアを以下に示す．

- 使用ソフトウェア
  - libpcap 0.9.6
  - IP sentinel 0.12

5.2 性 能 評 価

実装システムの評価として，認証に成功してから設定が ARP Blocker に反映されるまでの時間と，認証に成功した端末が通信可能となるまでの時間を比較した．

実験では MAC Monitor が RADIUS Accept を取得してから，ARP Blocker に拒否アドレスとして登録を行い，端末を偽装可能になるまでの時間を測定した（図 10 の 1 と 2）．

また，RADIUS サーバが RADIUS Accept が送出してから，LAN スイッチがポートを開き，端末が実際に通信可能になる

までの時間を測定した（図 10 の 1 と 3）．端末のサプリカントには Microsoft Windows2000 SP4 の標準のものを利用した．実験結果を表 3 に示す．

表 3 測定結果

通信開始までの時間 (秒)	設定反映までの時間 (秒)
0.153	0.0163

5.3 考　　察

結果を見る限りでは，認証に成功してから ARP Blocker に反映されるまでの時間と通信が可能となるまでの時間を比較すると 10 倍程の違いがある．

実装に用いた IP sentinel ではパケットを取得する度に設定を読み込んでいるため，登録したアドレスが実際に反映されるまでの処理は比較的高速であると考えられる．

それに対して，LAN スイッチのポートが開放された直後は，DHCP による IP アドレス取得などの処理が行われるために，それらが完了するまでは通信不可能な状態であり，これにより，接続までの時間が多少延びているものと考えられる．しかし，これは実験環境に依存するものであり，LAN スイッチやサプリカント等を変更すれば異なる結果が得られると思われる．

別の環境では通信が許可される時間の方が早くなる可能性があるため，単純に比較することは難しいが，ポート開放直後に通信が開始されることは多くないため，この性能ならば，実用上は問題ないものと考えられる．ただし ARP Blocker に設定されるアドレス数が肥大化した場合や，認証頻度が極端に高い場合には処理速度の低下が予想されるため，そのような環境への対応が今後の課題となる．

6. ま と め

IEEE802.1X 認証は不正アクセス防止に有効な技術であり，無線 LAN だけではなく有線 LAN での利用も今後期待されるが，その場合ネットワーク管理者の意図しない接続が行われる可能性がある．また，ARP 偽装により接続の無効化を行うシステムにもスケーラビリティの点で問題がある．

そこで IEEE802.1X 認証システムによる認証結果に基づいて動的に設定を行い，認証により許可を得ていない端末に対して ARP 偽装により接続無効化を行うことにより，管理者が端末の登録管理を必要としないシステムを提案した．また，同時に IEEE802.1X 認証システムにおいて管理者の意図しない接続をネットワークから排除することを可能とした．

また，実装システムの評価として実際に認可されてから設定に反映されるまでの時間を測定し，端末の通信が許可されるまでの時間と比較して，実用上問題ない速度であることを確認した．今後の課題としては，接続確認を行う間隔の適切な設定や，EAP-TLS 以外の認証への対応を考慮に入れたい．

文　　献

[1] David,C.: An Ethernet Address Resolution Protocol, RFC826, 1982

[2] Jonathan Hassel, RADIUS ユーザ認証セキュリティプロトコル, オライリー・ジャパン, 2003

[3] IP sentinel
http://www.nongnu.org/ipsentinel/

[4] dsniff
http://www.monkey.org/dugsong/dsniff/

[5] FreeRADIUS
http://www.freeradius.org/

[6] tcpdump
http://www.tcpdump.org/