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

2008－DPS－134 (30)
2008－CSEC－ 40 (30)
2008／3／7

ARPテーブルの集中管理による認証ネットワーク上の不正接続検出と排除方法の提案

三宅 猛[†] 鈴木春洋[†††] 北野文章[†††]
村瀬晋二[†††] 若山公威[††] 岩田彰[†]

LANにおけるネットワークアクセス認証方式の１つであるIEEE802.1Xは認証スイッチと認証サーバにより実現され，未許可端末からの不正接続防止が期待できる．しかし現実には，物理的なネットワーク機器構成の変更等により，未許可端末がLANへ不正侵入する危険性が存在する．本稿ではIEEE802.1X認証によるユーザ認可状況を把握することでネットワーク上の有効なMACアドレスを管理し，また，クライアントのARPテーブルを一括管理することにより不正端末の検出，排除を可能とするシステムを提案する．

A Method of Detection and Excluding Disapproval Connection on Authentication Network by Centraized Control of ARP Table

Takeshi MIYAKE[†] ,Shunyo SUZUKI[†††] ,Humiaki KITANO[†††]
,Shinji MURASE[†††] ,Kimitake WAKAYAMA[††]
and Akira IWATA[†]

IEEE802.1X that is one of the network authentication methods in LAN is achieved by the authentication switch and the authentication server, and an illegal connected prevention from the unpermission teminal is expected. However, There is actually danger that the unpermission terminal invades LAN by the changing a physical network equipment. In this paper, we propose the system that detects and excludes an illegal terminal by understanding the user authorization state on the IEEE802.1X and managing an effective MAC address on the network, and managing the ARP table of the client.

1. はじめに

近年のコンピュータネットワークの普及に伴い，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・大学などの組織内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、組織内部からの接続に対してもセキュリティを考慮する必要がある．

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の１つに，ネットワーク接続時に電子証明書等を認証子として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．主に無線LANでの利用が知られているが，IEEE802.1Xは有線LANにも対応した規格であり，それぞれIEEE802.1Xに対応したアクセスポイントや認証LANスイッチを設置することで利用が可能となる．

しかし，有線LAN環境下において，このIEEE802.1X認証ネットワークを構築した場合，認証LANスイッチを認証機能を持たないHUBにすり替えるなど，物理的にネットワーク構成を変更させることで，未許可端末でも認証無しで容易にLANを利用することが可能な場合もある．これはIEEE802.1X認証ネットワークを実際に運用するにあたって，セキュリティを確保する上で本質的な問題となる。

IEEE802.1Xとは別に，内部からの不正端末の接続を防御する方法としてARPの脆弱性を利用した方法が挙げられる．しかし，本方式を利用する場合，予め接続許可を与える端末のアドレスを確認，設定する必要があり，大規模なネットワーク環境や端末の追加変更の頻繁な環境では管理が煩雑となるために向いてい

† 名古屋工業大学大学院
Nagoya Institute of Technology
†† 名古屋外国語大学
Nagoya University of Foreign Studies
††† 株式会社中電シーティーアイ
chuden CTI

ない．また，MAC アドレスや IP アドレス等偽装の容易な情報を認証子とするためセキュリティ上の問題も存在する．

本稿では，IEEE802.1X を利用した認証ネットワーク上において，不正端末による接続を排除することを目的として，IEEE802.1X 認証の認可状況からネットワーク上で接続が有効な端末の MAC アドレスを把握し，各端末から収集する ARP テーブルと照合することにより未認可端末の存在を検知し，他端末との通信を無効化するシステムを提案する．また，提案方式について，従来方式と比較した場合の安全性，実用性について考察を述べる．

2. IEEE802.1X 認証ネットワーク

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ための規格である．本章では IEEE 802.1X の概要について述べ，利用する上で想定される問題点を提示する．

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は 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，様々な認証方法を利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．

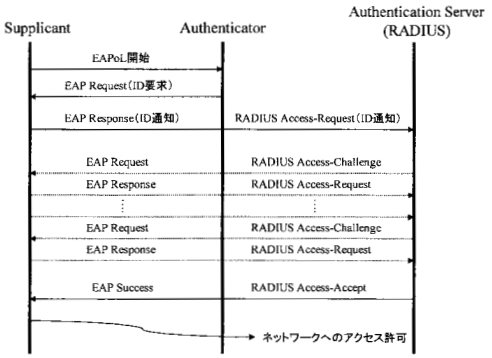

図 2　IEEE802.1X の動作

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等が行われ，RADIUS サーバが正当なユーザであると判断した場合には，認証の成功を意味する RADIUS Access-Accept を LAN スイッチに通知し，LAN スイッチはポートを開いて端末を LAN に接続させる．

2.2 現状の課題

IEEE802.1X 認証ネットワーク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，ネットワークを利用する端末の数だけ物理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以下のような接続により問題が生じることがある．

問題となる状況の 1 つが，LAN スイッチと端末の間にリピータ HUB を挟んだ場合である．基本的に 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，認証に成功した端末と LAN スイッチの間にリピータ HUB が存在した場合，そのリピータ HUB の空きポートに接続すれば，IEEE802.1X による認証を受けずに LAN に接続できてしまうことになる．しかし，既存の多くの LAN スイッチでは，認証に成功した端末の MAC アドレス以外からの接続を遮断する機能を備えており，この問題は解決している場合が多い．

しかし，もっと単純に，例えば認証用の LAN スイッチを認証未対応のものに取り換えてしまったり，直接基幹 LAN にリピータ HUB を設置して接続した場合でも，当然 IEEE802.1X による認証は行なわれない．ネットワーク機器の構成をユーザが勝手に変更できな

いように物理的な対策がとられていなければ，LANに侵入することは容易に可能である．

このように，有線LANでIEEE802.1X認証を利用する際には，認証を回避して接続される可能性を考慮に入れる必要がある．

3. ARPの脆弱性を用いた不正接続防止手法

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，通信相手を変更することがプロトコルの仕様上可能[2]となっており，この脆弱性を利用してネットワーク上の通信を制御する方法がARP spoofingとして知られている．

ARPの基本動作については以下の通りである．

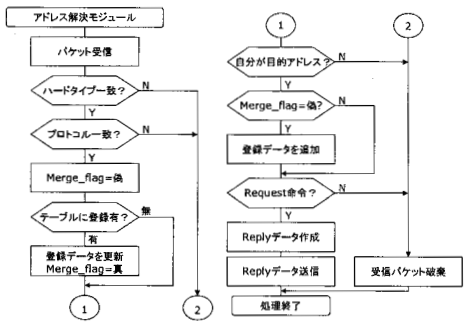

図3 ARPアドレス解決モジュールの動作

(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．

ARPの脆弱性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，通信開始前に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目的とする端末との通信が不可能となる．通信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，これらの操作を行うことで，不正接続を排除するネットワークを実現できる．

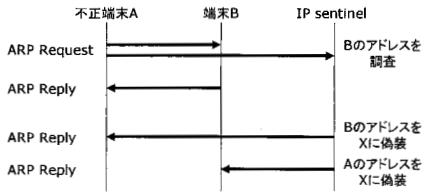

図4 IP Sentinelの動作

このようなARPの脆弱性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，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．そのため端末の追加，変更が頻繁に起こり得る大規模ネットワークなどでは管理が煩雑になるため実用的では無い．また，アドレスが登録されているにもかかわらず，実際には使用されていない期間が存在すると，未使用のアドレスを不正に利用して侵入される可能性があり，セキュリティ面においても問題が残る．

4. 提案方式

本章では，第2章と第3章で述べた不正接続排除方式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の脆弱性を利用して不正接続の排除を行うには，通信を許可する端末のMACアドレス（もしくはIPアドレス）をリスト登録する必要があるが，本提案ではIEEE802.1X認証の結果を利用して，認証成功時にサーバに認可された端末のMACアドレスを把握し，許可アドレスとしてリストに登録を行う．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，管理者はネットワーク上の端末の追加，変更を意識する必要がなく，認証サーバ上のユーザ情報を管理するだけで済む．

提案方式により，認証を通過していない端末は全てネットワークから排除されるため，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

証ネットワークよりも高い安全性を実現できる．

4.1 提案システム概要

提案するシステムの構成を図 5 に示す．

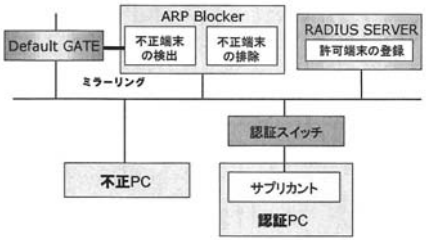

図 5 提案システム

提案システムでは従来の IEEE802.1X のシステムに，認証に成功した端末の MAC アドレスを把握し，接続を許可するアドレスの通知を行う機能を認証サーバに追加する．また，許可アドレスを管理して，ネットワーク上の不正端末を検知し，接続無効化までを行うサーバ（ARP Blocker）を追加する．

次節以降でこれらの機能を実現する具体的な方法について解説を行う．

4.2 MAC アドレスの管理

4.2.1 RADIUS プロトコル [5)]

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 パケットは Code，Identifier，Authenticator からなるヘッダ部分と Attribute で構成される．まず 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，この部分には認証端末や 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，IEEE802.1X 認証で認可された端末の MAC アドレスを検出し，管理する．

4.2.2 許可 MAC アドレスの決定

IEEE802.1X 認証により認可された端末の MAC アドレスがサーバに登録されるまでの流れを説明する．IEEE802.1X による認証後，RADIUS サーバから Access-Accept を種別コードに持つ RADIUS パケット（RADIUS Access-Accept）が送信された場合，対応する RADIUS Access-Request の属性情報の中から認可端末の MAC アドレスを取得し，許可アドレスとして管理サーバ（ARP Blocker）へと通知する．その後，ARP Blocker が保持する許可アドレスのリストに，認可を受けた端末の MAC アドレスが追加される．

ただし，LAN 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 アドレスについては例外アドレスとして始めからリストに登録しておく必要がある．

4.3 接続状態の把握

許可リストに登録されたアドレスは，使用されていない間もリストに残ったままになっている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除外する必要がある．本提案では RADUS アカウンティング機能を利用することにより端末の接続状態を確認する．

LAN スイッチが RADUS アカウンティング機能を利用している場合には，端末の接続切断時に RADIUS サーバに対して接続の終了を示す RADIUS Accounting が通知されるため，これを解析することにより接続を終了した端末の MAC アドレスを取得し，削除アドレスとして ARP Blocker へ通知する．その後，ARP Blocker が保持する許可アドレスのリストから該当端末の MAC アドレスが除外される．

4.4 不正端末の検出

ネットワーク上の不正端末検出方法については，アドレス解決時に送信される ARP Request を解析することにより検出する方法が従来方式として存在するが，本節ではさらにクライアントの ARP テーブルを集中管理することにより不正端末を検出する方法を提案し，それぞれの検出方式を導入した提案システムについて述べる．

4.4.1 従 来 方 式

従来方式では図 4 のように ARP Request がブロードキャストであることを利用して，同一ネットワークセグメントで通信を実行しようとする端末を特定する．

提案システムの全体の動作を図 6 に示す.

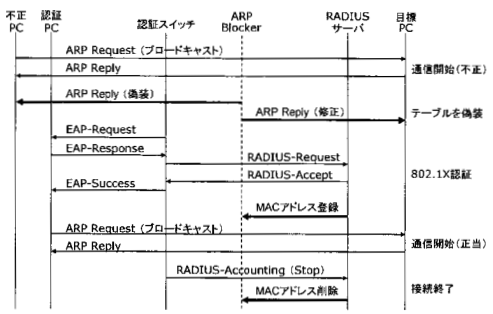

図 6 従来検知手法を用いた提案システムの動作

提案システムの一連の動作は以下の通りである.

(1) IEEE802.1X による認証成功後に RADIUS サーバから認可パケット (RADIUS Accept) が送信された場合, 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) 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偽装 ARP による ARP テーブルの書き換えを行う.

(3) 接続終了後にスイッチから RADIUS サーバに送信されるアカウンティングパケット (RADIUS Accounting) を受信した場合, 接続を終了した端末の MAC アドレスを取得し, 削除アドレスとして ARP Blocker のリストから除外する.

従来方式を用いたネットワークでは, 不正端末がアドレス解決方法として ARP Request のブロードキャストを正しく行っていれば, 問題なく不正端末として検出されるが, それ以外の方法で ARP 解決を行った場合には効力がない. 例えば, ブロードキャストではなく, ユニキャストで直接目的とする端末に ARP パケットを送信する場合などである. このような場合には本方式では不正端末の存在を検出できない. 3 章で述べたように, ARP の脆弱性を利用してパケットの盗聴, 改竄等を容易に実行するツールも存在しており, 危惧すべき問題であると考えられる.

4.4.2 提 案 方 式

提案方式では, 認可済みクライアントの ARP テーブルを確認することにより, 同一ネットワークセグメントで通信しようとする不正端末を特定する. 提案システムの全体の動作を図 7 に示す.

提案システムの一連の動作は以下の通りである.

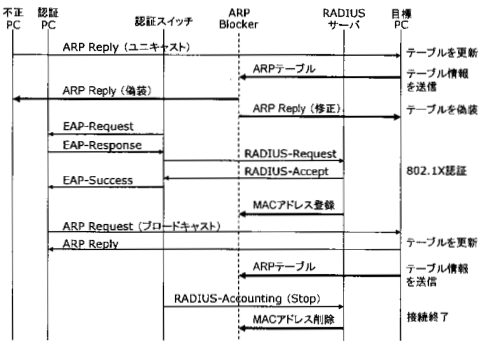

図 7 提案検知手法を用いた提案システムの動作

(1) IEEE802.1X による認証成功後に RADIUS サーバから認可パケット (RADIUS Accept) が送信された場合, 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) 認可済み端末にはエージェントを導入し, ARP テーブルの状態を逐一チェックする. ARP テーブルのエントリに更新があった場合, ARP Blocker に ARP テーブルの内容を通知する. ARP Blocker では端末から取得した ARP テーブルについて, 許可アドレスリストと照合を行い, リストに存在しない MAC アドレスがエントリとして存在する場合にはその MAC アドレスを不正端末と見なして ARP テーブルの偽装を行う.

(3) 接続終了後にスイッチから RADIUS サーバに送信されるアカウンティングパケット (RADIUS Accounting) を受信した場合, 接続を終了した端末の MAC アドレスを取得し, 削除アドレスとして ARP Blocker のリストから除外する.

本提案方式では管理サーバが ARP テーブル情報を収集するためにクライアントにエージェントを導入する必要があるが, ゲートウェイ等のエージェントを導入できない機器からは ARP テーブルを収集できない. このような機器に対しては, ポートミラーリング等を利用して受信 ARP パケットを監視し, 未許可端末からの不正な ARP パケットを検出する必要がある.

5. 評　　価

5.1 比較・考察

提案システムについて, 従来のネットワークシステムと比較して考察を述べる。従来の IEEE802.1X 認証ネットワーク, ARP 脆弱性を利用した不正接続無

効化手法（IP sentinel 等），2 種類の不正接続検出手法を導入した提案システムについて，機能面と管理面に関して比較したものをそれぞれ表 1，表 2 に示す。

表中において，提案（1）は検出手法に従来方式を導入したシステム，提案（2）は検出手法に提案方式を導入したシステムとする．

表 1 機能面の比較

	ARP の脆弱性利用	IEEE 802.1X	提案 (1)	提案 (2)
ユーザ認証機能	×	○	○	○
不正検知・排除	○	×	○	○
spoofing 対策	×	×	×	○

表 2 管理面の比較

	ARP の脆弱性利用	IEEE 802.1X	提案 (1)	提案 (2)
ユーザ管理	不要	必要	必要	必要
アドレス管理	必要	不要	不要	不要
エージェント導入	不要	不要	不要	必要
管理の煩雑さ	×	○	○	△

提案システム（1）と（2）では IEEE802.1X 認証ネットワークにおいて，ARP 脆弱性を利用することにより不正端末の検知・排除機能を追加し，安全性を高めている．さらに管理の煩雑さの観点で見ると，認証結果に基づいた動的な MAC アドレスの管理を行うため，ユーザ情報の管理は必要となるが，煩雑なアドレス管理を必要とせず，従来の ARP 脆弱性を用いただけの手法に比べて手間が少ないという利点がある．

また，2 つの提案システムに関して比較してみると，提案システム（1）は ARP spoofing のような攻撃に対しては効果が無く，セキュリティ面を考えれば，不正接続の検出手法を変えた提案システム（2）を利用するべきである．しかし，提案システム（2）では全てのクライアントに対してエージェントを導入する必要があり，管理面では多少難がある．

5.2 提案システムに対する脅威

本提案システムに関する課題について考察する．

不正端末検出に提案手法を用いた提案システムではクライアントに導入したエージェントによりサーバへ ARP テーブル情報の送信を行なうが，不正端末からの ARP spoofing 攻撃によりサーバとの通信を妨害，盗聴される恐れがある．解決策としては，クライアントの ARP テーブルについてサーバのエントリを静的なものに変更する，通信経路を暗号化するなどの方法が挙げられる．

また，本提案システムにより，未認可の端末による ARP spoofing を防ぐことはできるが，IEEE802.1X 認証により信頼された MAC アドレスを持つ端末に通信許可を与えるという特性上，既に認可された端末による ARP spoofing には対応することができない．認可済み端末による ARP spoofing を検出するためには，MAC アドレスと対になる IP アドレスを正しく管理し，ARP テーブルの内容と照合する必要があるが，本稿では考慮されていないため，今後の課題としたい．

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，ネットワーク管理者の意図しない接続が行われる危険性がある．また，ARP の脆弱性を利用した接続無効化手法にもスケーラビリティとセキュリティの面で課題がある．

そこで IEEE802.1X による認証結果に基づいて動的に MAC アドレスを管理し，認証により許可を得ていない端末に対しては ARP 偽装により接続無効化を行うことにより，認証ネットワークにおいて管理者の意図しない接続を排除するシステムを提案した．

また，不正端末を検出する方法としてクライアントの ARP テーブルを集中管理する手法を導入することで，提案システムをより安全性の高いものとし，その実用性についても評価した．

今後の課題として，提案検出手法を改良し，認可済み端末による攻撃についても対策を行いたい．

参 考 文 献

1) 三宅猛, 鈴木春洋, 北野文章, 岩田彰, " 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", 情報処理学会研究報告, 2007-CSEC-38, pp.113-118, 2007.
2) David,C.: An Ethernet Address Resolution Protocol, RFC826, 1982.
3) IP sentinel
http://www.nongnu.org/ipsentinel/
4) dsniff
http://www.monkey.org/dugsong/dsniff/
5) 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.