マルチメディア通信と分散処理　94－25
分散システム／インターネット運用技術　14－25
（１９９９．７．１６）

情報コンセントにおける認証とアドレス偽造防止を VLAN 機能により実現するシステム LANA2

石橋勇人[1]　阪本晃[2]　山井成良[3]　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] 大阪市立大学大学院 工学研究科
[3] 岡山大学 総合情報処理センター

概　要

本稿では，これまでの提案をふまえて情報コンセントにおける不正アクセスを防止するための方式を原理的なレベルから考察するとともに，具体的な不正アクセス防止システムを提案している．本システムでは，(1) 利用者の認証とアクセスの記録，(2) 認証なしにネットワークへアクセスすることの防止，(3) MAC アドレスの偽造防止，(4) IP アドレスの偽造防止，が可能である．しかも，認証のために通常の計算機の利用者情報のみを利用しており，IP アドレスや MAC アドレスの事前登録は不要であるため，管理者の負担が少ない．我々の提案する方式は，スイッチングハブの持つ機能に応じていくつかの適用が可能であり，本稿では，スイッチングハブの VLAN(Virtual LAN) 機能を用いて情報コンセントから外部ネットワークへの不正アクセスを防止する機能の実装方法について述べる．

LANA2: An Access Control System for LAN Sockets using VLAN Functions

Hayato Ishibashi[1] , Akira Sakamoto[2] , Nariyoshi Yamai[3] , Kota Abe[1] ,
Katsumi Ohnishi[1] and Toshio Matsuura[1]
[1] Media Center, Osaka City University
[2] Graduate School of Engineering, Osaka City University
[3] Computer Center, Okayama University

Abstract

In this paper, we describe a new principle to achieve secure access on open LAN sockets environment. This principle can provide the following functions: (1) user authentication and logging, (2) protection against unauthorized access, (3) protection against MAC address spoofing, and (4) protection against IP address spoofing. It needs user registration, but doesn't need MAC address registration nor IP address registration. Our principle can be applied to a variety of LAN switches. We also discuss two kinds of implementation for LAN switches with VLAN functions.

1　はじめに

最近，軽量･高性能で携帯可能な小型計算機の普及に伴い，例えば大学における図書館、情報センター等の公共スペースに情報コンセントを設置し，利用者が小型計算機を接続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な環境を提供する組織が増えてきている．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になる．これに対して我々は IP アドレスおよび MAC アドレスの偽造にも対応した，情報コンセントの不正アクセス防止方式を提案し [1]，フレームレベルでのフィルタリング機能を持つスイッチングハブを用いて実現した [2]．しかし，スイッチングハブが一般にこのような高度なフレームフィルタリング機能を持っているわけではない．

そこで，本稿では我々が文献 [1] において提案した不正アクセス防止方式の原理を整理し，同原理の応用として，より多くの種類のスイッチングハブに実装されている VLAN(Virtual LAN) 機能を用いた不正アクセス防止機能の実現について 2 通りの方法を述べる．また，この方式に基づく情報コンセント不正アクセス防止システム LANA2 の実装についても述べる．

2 不正アクセス防止方式

2.1 必要な機能

本稿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大学における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，IP アドレス割り当てサーバから動的に 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．

本稿で述べる不正アクセス防止方式の目的は，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正規の IP アドレスを持つパケットを送出できるようにアクセス制御を行ない，またネットワーク利用時に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，次の各機能が必要となる．

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

2.2 不正アクセス防止方式の原理

ここでは，[1] で述べた不正アクセス防止方式の動作原理を整理した形で提示する．

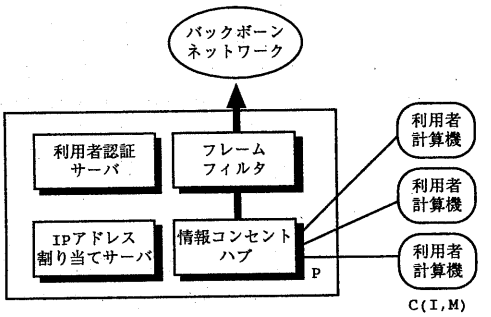

図 1: 不正アクセス防止システム

本方式に基づくシステムは，利用者認証サーバ，IP アドレス割り当てサーバ，フレームフィルタ，情報コンセントハブから構成される（図 1）．情報コンセントハブは利用者の計算機を接続する複数のポートを持ち，利用者の計算機からパケットを受け取って必要に応じて他のポートへ中継する．各ポートにはそれぞれポート識別子（たとえば，逐次的に振られた番号）を用意しておき，受け取ったパケットは各々ポート識別子に対応づけることができるものとする（このためには，例えばポート毎に接続可能な MAC アドレスを限定できれば良い．詳しくは後述）．フレームフィルタは 2 つのネットワークインタフェースを持ち，情報コンセントハブから送られてきたフレームを（IP アドレス，MAC アドレス，ポート識別子）の 3 つ組に基づいて IP アドレス割り当てサーバ，利用者認証サーバ，およびバックボーンネットワークに中継するか破棄するかを制御できる．

本システムは次のように動作する．

1. 初期状態では，情報コンセントの各ポートに接続された利用者計算機からは IP アドレス割り当てサーバに対してのみアクセス可能な状態としておく．
2. 利用者は自己の計算機 C を情報コンセントのポート P に接続する．
3. C は，IP アドレス割り当てサーバから IP アドレス I の割り当てを受ける．この IP アドレスは，接続時に動的に決定される．
4. システムは，C から送られてきた IP アドレス要求パケットより C の MAC アドレス M を取得し，ポート P からバックボーンに流入可能なパケットの送信元 MAC アドレスを M に，送信元 IP アドレスを I に限定する．また，ポート P から利用者認証サーバへのアクセスを許可する．
5. C と利用者認証サーバとの間で利用者認証を行う．認証に成功すれば，利用者名，IP アドレス等を記録し，ポート P からバックボーンネットワークへのパケットの送出を許可する．

以上の動作により，2.1 で述べた機能を実現することが可能となる．

本方式の動作原理は，利用者の計算機を（IP アドレス，MAC アドレス，ポート識別子）の 3 つ組に基づいて識別する点にある．すなわち，本方式では，IP アドレスと MAC アドレスの両者に加えて，ポート識別子という，利用者からは制御不可能な要素を利用してアクセス可能な計算機を限定しているため，送信者の IP アドレス・MAC アドレスの偽造にも耐え得る不正アクセス防止を実現することができる．

しかも，本方式は（1）IP アドレスを動的に割り当てる，(2) MAC アドレスを自動的に学習する，(3) 利用者認証情報は既存のものを流用できる，などの特徴を有するため，本方式を導入することによって新たに管理上の負担が増加することはない．

2.3 VLAN機能を持つハブによる不正アクセス防止機能の実現

2.2の原理に基づく不正アクセス防止方式には，いくつかの実現方法が考えられる．[2] では，フレームフィルタリング機能を有するスイッチングハブを利用した実現を示した．

本稿では，VLAN 機能を持つスイッチングハブを使用し，同原理に基づいて不正アクセスを防止するシステムの実現方法について述べる．

2.3.1 方法 1: MAC アドレスフィルタリング機能の利用

情報コンセントで使用するハブが，特定の送信元 MAC アドレスを持つフレームのみを通過させる MAC アドレスフィルタリング機能を持つ場合には，次のような方法によって不正アクセス防止が実現できる．

1. VLAN 機能を使用することによって，初期状態では利用者の端末がアクセスできる範囲を IP アドレス割り当てサーバに限定しておく．
2. IP アドレスの割り当てに成功した後，認証が終了するまでの間は，認証サーバのみに接続が可能であるよう VLAN を切り替える．
3. 認証に成功した後は VLAN を切り替えて外部へのアクセスを許すようにする．
4. ハブの MAC アドレスフィルタリング機能を利用してポートごとに接続を許す MAC アドレスを限定し，これによって（MAC アドレス，ポート識別子）の対応関係を固定する．
5. フレームフィルタにおいて，(MAC アドレス，IP アドレス）の対によって通過できるフレームを限定する．

この場合，4 において，あるポートから流入可能なフレームを特定の MAC アドレスをもつものに制限しており，さらに 5 においてフレームフィルタを通過できるフレームを MAC アドレスと IP アドレスの組によって制限している．したがって，結果的にフレームフィルタを通過できるフレームは，特定の（MAC アドレス，IP アドレス，ポート識別子）の組を持つものだけとなる．

2.3.2 方法 2: VLAN タギング機能の利用

IEEE では，ハブにまたがって VLAN を構成するための標準として 802.1Q[3] を定めており，この仕様に則ったハブであれば，メーカや機種を問わずに組み合わせてハブにまたがる VLAN を構成して使用することができる（図 2）．このとき，ハブとハブとの間を接続するケーブルの上には，異なる VLAN に属するフレームが混在して流れることになるため，MAC フレームのフォーマットを拡張することによって各々のフレームが属する VLAN を識別できるようになっている．これが VLAN タギング (VLAN tagging) である．

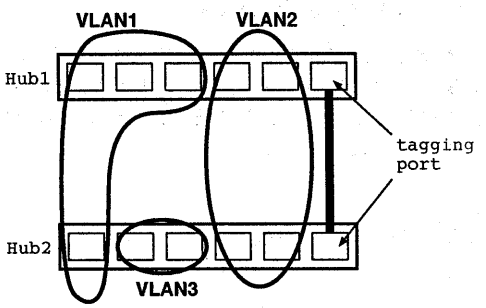

図 2: VLAN タギング

ハブが IEEE 802.1Q をサポートしている場合には，次のような方法が可能である．

1. VLAN 機能を使用することによって，初期状態では利用者の端末がアクセスできる範囲を IP アドレス割り当てサーバに限定しておく．
2. IP アドレスの割り当てに成功した後，認証が終了するまでの間は，認証サーバのみに接続が可能であるよう VLAN を切り替える．
3. 認証に成功した後は VLAN を切り替えて外部へのアクセスを許すようにする（このとき，ハブのポートごとに異なる VLAN を用意する）．
4. フレームフィルタが接続されているポートはあらかじめタギングポート（タグ付のフレームが流れるポート）に指定しておく．
5. フレームフィルタにおいて，(MAC アドレス，IP アドレス，VLAN タグ）の 3 つ組に基づいて通過させるフレームを決定する．
6. 認証に成功した時点でその計算機からのフレームが通過できるようフレームフィルタを設定する．

この方法では，フレームフィルタが接続されているポートがタギングポートに指定されているため，フレームフィルタに届くフレームには VLAN タグが付加されている．したがって，VLAN をポートごとに異なるように設定しておけば，VLAN タグを利用してどのポートからやってきたフレームであるかをフレーム単位で識別することが可能となる．したがって，(MAC アドレス，IP アドレス，ポート識別子）の 3 つ組によって通過すべきフレームを選択することができる．

3 LANA2の実装

本章では，前章で述べた方法を実現するシステムの実装について述べる．なお，以下では，VLAN方式を利用した不正アクセス防止システムをLANA2と呼ぶことにする．

3.1 システム構成

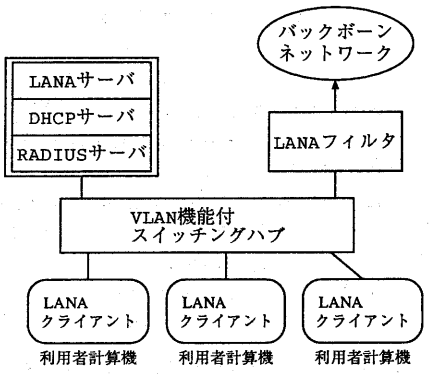

図 3: LANA2 システムの構成

LANA2システムの構成を図3に示す．LANA2システムは，LANAサーバ，LANAフィルタ，DHCPサーバ，RADIUSサーバ，VLAN機能付きスイッチングハブから構成される．今回は，LANAサーバ，DHCPサーバ，RADIUSサーバを同一の計算機上で動作させているが，異なった計算機上で動作させても差し支えない．

3.1.1 LANAサーバ

LANAシステムの中心となるサーバで，DHCPサーバやRADIUSサーバなどと通信して情報を交換し，LANAフィルタやスイッチングハブを制御する．このサーバはマルチスレッドで実現されており，現在はSolaris 2.6上で稼働させているが，POSIX threadのあるOSならば移植は容易である．

LANA2では，基本部分がハブの持つ機能に依存しないよう，ハブを抽象化して扱っている．これによって，上位モジュールにとってハブの機種による設定コマンドの違いが隠蔽されているだけでなく，本稿で述べたVLANを利用した方法に加えて文献[2]で提案したフレームフィルタリング機能付ハブを使用する方法についても同一のサーバで扱うことが可能となっている．

3.1.2 LANAフィルタ

2つのネットワークインターフェースを持ち，一方をVLAN機能付きスイッチングハブに，他方をバックボーンネットワークに接続する．LANAフィルタは，2つのインターフェースの間でフレームを中継するものであり，フィルタリング機能とアクセス記録機能を持っている．

今回は，FreeBSD 3.1上にBPF（Berkeley Packet Filter）を用いてユーザレベルプロセスの形で実装している．BPF機能を持つUNIX系OSへの移植は容易である．

フィルタリング機能 LANAフィルタは，指定された条件に基づいてフレームを通過させるべきか否かを決定し，許されたフレームのみを中継するフィルタリング機能を持つ．フィルタリングの条件として指定する要素には，(1) MACアドレス，(2) IPアドレス，(3) VLANタグ[1]，がある．また，(4) TCP/UDPポート番号，を条件に加えることにより，情報コンセントの利用者が使用できるサービスを限定することも可能である．我々の方式では，フレームはポート識別子，すなわち利用者の計算機と対応づけられているので，利用者ごとにサービスやアクセス先の限定が可能である．

フィルタリングのための条件は，LANAサーバから設定される．

アクセス記録機能 LANAフィルタでは，通過するすべてのフレームをチェックすることが可能であるため，使用されたUDPのポート番号やTCPのポート番号を利用者ごとに記録したり，同時にTCPパケットのSYNビットやFINビットなどの情報をチェックすることによってTCPセッションの開始/終了時刻を記録するなど，利用者の各種の活動記録を取ることが可能である．

3.1.3 DHCPサーバ

図1におけるIPアドレス割り当てサーバに相当し，DHCPプロトコル[4]によって利用者の計算機に対してIPアドレスを割り当てるサーバである．ISCのDHCPサーバ[5]をベースとしてLANAサーバとの通信機能を付加したものを使用している．

3.1.4 RADIUSサーバ

図1における認証サーバとして，ここでは，RADIUS[6, 7]サーバを用いている．RADIUS

[1] VLANタギングを利用する場合

サーバには，フリーの実装の 1 つである DTC RADIUS[8] を使用しており，修正は加えていない．

RADIUS サーバでは，利用者の認証と，情報コンセント使用開始・終了の記録を行う．

3.1.5 VLAN 機能付きスイッチングハブ

VLAN 機能に加えて，MAC アドレスフィルタリング機能ないし IEEE 802.1Q VLAN タギング機能を持つスイッチングハブであり，利用者の計算機が接続される．

ここでは，Cisco 社製 Catalyst 2912XL を使用した．ハブをコントロールするためには，LANA サーバからハブに対して制御用の telnet セッションを開設し，これを利用してコマンドを実行させている．もちろん，SNMP(Simple Network Management Protocol) やシリアルラインによる制御としてもかまわない．

また，1 セットの LANA サーバ，LANA フィルタで複数台のスイッチングハブを管理することが可能である．

3.2 利用者認証

不正アクセス防止のためには，利用者の認証が必要である．LANA2 では，認証のために利用者の計算機上で動作し，LANA サーバと通信して認証情報の交換を行うクライアントソフトウェア（LANA クライアント）を作成した．現在，Windows9x 用に C++で記述したクライアントと Java で記述したクライアントの 2 種類を用意している．

我々の提案する不正アクセス防止方式は，認証のために必ずしも専用クライアントを必要とするものではない．その代わりに，たとえば WWW や telnet などを用いてユーザ名とパスワードを入力させ，認証することも可能である．

しかし，専用クライアントを用いることによって，次に掲げるような問題（カスケードハブ問題 [2]）に対してほぼ対処することができ，より高いセキュリティレベルを維持できるという利点がある．

カスケードハブ問題: 悪意を持つ利用者が LANA システムの情報コンセントハブに別のダムハブ（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，更にその先に計算機を接続した場合を考える．善意の利用者が誤ってダムハブに計算機を接続して認証を行い，通常通り使用した後にダムハブからコネクタを引き抜いたとすると，通常であればシステムが切断を検出して初期化処理を行う．ところが，ダムハブ上に悪意を持つ利用者の計算機が存在すると，情報コンセントハブは切断を検出できない．したがって，フィルタが初期化されないままの状態となるので，その後に悪意の利用者が善意の利用者の計算機と同一の MAC アドレス・IP アドレスを偽造して使用すると，外部ネットワークに対する不正アクセスが可能となってしまう．

これに対して，我々は LANA クライアントと LANA サーバの間で定期的に認証を行って利用者計算機の存在を確認することにより，認証された計算機の入れ替わりを防止している（サーバ・クライアント間で使用している TCP コネクションを乗っ取られるという最悪の場合でも，認証間隔より長い時間の不正利用は防止できる）．

また，LANA クライアントの導入によって利用者が能動的に認証過程を起動する必要がないため，初心者にとってより使いやすいシステムとすることができる．

3.3 動作の詳細

以下では，LANA2 システムの具体的な動作シーケンスについて述べる．ただし，紙数の関係上，本筋からはずれると思われる部分（タイムアウト処理など）には省略があることをお断りしておく．

3.3.1 MAC アドレスフィルタ方式の場合

1. 接続開始にあたって，利用者の計算機が接続されるポートをそれぞれ認証用の VLAN に属するよう設定しておく．
2. 利用者が計算機を情報コンセント（ハブ）のポート P に接続すると，DHCP シーケンスが開始される．この計算機（インターフェース）の MAC アドレスを M とする．
3. DHCP サーバは，IP アドレス要求パケットから MAC アドレス M を抽出し，これから利用者の計算機に与えようとする IP アドレス I とともに LANA サーバに通知する．
4. LANA サーバは，P から流入可能なフレームの送信元 MAC アドレスを M に限定するフィルタをハブにセットする[2]．
5. DHCP サーバは IP アドレス I を利用者の計算機に与える．
6. LANA サーバと（利用者の計算機で動作している）LANA クライアントの間で認証情報の交換を行う．LANA クライアントが存在しない

[2] ハブのなかには，最初に接続された計算機の MAC アドレスに対して自動的にフィルタをセットできるものがある．その場合には，明示的に MAC アドレスフィルタをセットする必要はない．

(LANA クライアントからの応答がない) 場合には, LANA サーバは利用者計算機が (WWW, telnet などの手段によって) 自発的に認証を行うまで待つ.

7. 認証に成功すると, LANA サーバは LANA フィルタに対して (M, I) の組を持つフレームを通過できるよう設定する.
8. ポート P の属する VLAN を, LANA フィルタが接続されている VLAN に切り替える.

3.3.2 VLAN タギング方式の場合

1. 接続開始にあたって, 利用者の計算機が接続されるポートをそれぞれ認証用の VLAN に属するよう設定しておく.
2. 利用者が計算機を情報コンセント (ハブ) のポート P に接続すると, DHCP シーケンスが開始される. この計算機 (インターフェース) の MAC アドレスを M とする.
3. DHCP サーバは, IP アドレス要求パケットから MAC アドレス M を抽出し, これから利用者の計算機に与えようとする IP アドレス I とともに LANA サーバに通知する.
4. DHCP サーバは IP アドレス I を利用者の計算機に与える.
5. LANA サーバと (利用者の計算機で動作している) LANA クライアントの間で認証情報の交換を行う. LANA クライアントが存在しない (LANA クライアントからの応答がない) 場合には, LANA サーバは利用者計算機が (WWW, telnet などの手段によって) 自発的に認証を行うまで待つ.
6. 認証に成功すると, LANA サーバは, 利用者の計算機の MAC アドレス, IP アドレスに加えて, ポートごとに定義された VLAN (V_P) の情報を加えた (M, I, V_P) の組を LANA フィルタに伝え, これを充たすフレームが LANA フィルタを通過できるようにする.
7. ポート P の属する VLAN を, V_P に切り替える.

3.3.3 利用者計算機の切断検出

利用者が情報コンセントの利用を終了し, ネットワーク接続を切断する際には, LANA サーバはポートの設定を初期状態に戻し, 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 (リンクダウントラップ) 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, あるいは利用者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 LANA クライアント間のコネクションが切断された場合.
- LANA サーバから LANA クライアントへの存在確認要求に対して正しい応答がなかったとき.

4 まとめ

本稿では, 情報コンセントにおいて利用者の認証を行い, IP アドレスや MAC アドレスの偽造防止を可能とする方式について提案した. また, VLAN 機能を用いることによって本方式を実現したシステムである LANA2 について述べた.

参考文献

[1] 山井成良, 石橋勇人, 安倍広多, 大西克実, 松浦敏雄: 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, コンピュータセキュリティシンポジウム'98 論文集, 情報処理学会, pp. 141–146 (1998).

[2] 石橋勇人, 山井成良, 安倍広多, 大西克実, 松浦敏雄: 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, 分散システム/インターネット運用技術シンポジウム'99 論文集, 情報処理学会, pp. 69–74 (1999).

[3] IEEE: *802.1Q-1998 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridge Local Area Networks*, IEEE (1998).

[4] Droms, R.: Dynamic Host Configuration Protocol, RFC 2131 (1997).

[5] Internet Software Consortium: ISC DHCP, `http://www.isc.org/dhcp.html`.

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

[7] Rigney, C.: RADIUS Accounting, RFC 2139 (1997).

[8] デジタルテクノロジー (株) : DTC Radius 2.03, `http://www.dtc.co.jp/Radius2.0/`.