IPアドレス/MACアドレス偽造に対応した情報コンセント不正アクセス防止方式

石橋勇人[†] 山井成良[††] 安倍広多[†]
大西克実[†] 松浦敏雄[†]

計算機の小型軽量化にともなって，モバイルコンピューティングが急速に普及してきている．大学などの教育機関においては，これらの計算機に対してネットワークサービスを提供するために，図書館などのパブリックスペースに情報コンセントを設置するところが増えている．しかしながら，このような環境下では，利用者の計算機の設定を限定することは事実上不可能であるため，ネットワークの不正利用を防止することが困難であった．本論文では，事前に登録された正規利用者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する方法を提案する．本方式では，利用者が登録されていればIPアドレスやMACアドレスの事前登録は不要である．本論文で提案した方式を実装し実験を行った結果，利用者認証なしにネットワークにアクセスすることやMACアドレスやIPアドレスを偽って不正にネットワークにアクセスすることは不可能であり，安全な情報コンセントの構築に役立つことが確認された．

A Protection Method against Unauthorized Access and/or Address Spoofing for Open Network Access Systems

Hayato Ishibashi,[†] Nariyoshi Yamai,[††] Kota Abe,[†]
Katsumi Ohnishi[†] and Toshio Matsuura[†]

Personal computers are getting much smaller and easier to carry about in these days. LAN sockets providing network accessibility for those mobile computers are often set in public places like libraries, computer centers, and so on. However, it is difficult to prevent illegal access to networks in such cases. In this paper, we propose a protection method to cope with illegal access. Our method provides the following functions: (1) only valid users can access to the network, (2) preventing malicious users from invalid use of the network by IP and/or MAC address spoofing, and (3) no need for pre-registration of IP and/or MAC addresses. We have implemeted this method as a system named LANA. The design and implementation of LANA are also discussed.

1. はじめに

最近，軽量・高性能で携帯可能な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，このような小型計算機を個人で所有し，持ち歩く利用者が増えてきた．これにともなって，たとえば大学における図書館や情報センターのようなパブリックスペースに情報コンセントを設置し，利用者が自分の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環境を提供する組織が増えてきている．

† 大阪市立大学学術情報総合センター
Media Center, Osaka City University
†† 岡山大学総合情報処理センター
Computer Center, Okayama University

このような環境では，一般にネットワークに計算機を接続してアクセスできるのは認められた利用者のみであり，それ以外の第三者によるアクセスは不正なものである．また，認められた利用者であるか否かにかかわらず，他人（他の計算機）を偽って，すなわち，各計算機に与えられた識別子（たとえば，IPアドレスやMACアドレス）を偽ってネットワークにアクセス（パケットを送出）することも正当な行為ではない．本論文では，これらの不正な行為を不正アクセスと呼んでいる．

情報コンセントに接続される計算機は利用者が自由に設定可能であるため，不正アクセス対策は容易ではない．利用資格を持たない第三者によるアクセスへの対策として従来から試みられている手法のほとんどは，

IP アドレスや MAC（Media Access Control）アドレスを利用者識別のために用いているため，これらを偽造されると不正アクセス対策として用をなさない．

本論文では，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アクセス防止方式を提案する．本方式では，正規の利用者であれば，IP アドレスや MAC アドレスの事前登録なしに情報コンセントに計算機を接続して利用することができ，また，既存の OS やアプリケーションプログラムを修正する必要がないなど，管理・運用が容易であるという特徴を持っている．

2. 不正アクセス防止方式の機能

2.1 不正アクセス防止方式が満たすべき条件

本論文において想定している利用環境では，情報コンセントはたと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，DHCP サーバなどの IP アドレス割当て機構に対してネットワークを介して IP アドレスを要求することによって動的に IP アドレスの割当てを受けた後に，キャンパス LAN やインターネットにアクセスする．

このようなオープンな利用環境では，物理的にはだれでも任意の計算機を情報コンセントに接続できるため，そこへ導入する不正アクセス防止方式は次のような条件を満たす必要がある．

条件 1 IP アドレスや MAC アドレスを含めて，利用者の計算機の設定に依存することなく不正アクセスを防止できる．

条件 2 情報コンセントへの接続にあたって，既存の利用環境で使用している OS やアプリケーションプログラムに変更を加えない．

また，一般に正規の利用者の数は非常に多い☆ため，管理・運用を容易に行うには，導入する不正アクセス防止方式は以下のような条件を満たす必要がある．

条件 3 多数の利用者が存在する場合にも適用できるように，情報コンセントにおいて利用者認証を行うために必要となる管理コストが小さい．

条件 4 多数の利用者が同時に利用するような環境に適用できる．

2.2 必要とされる機能

本論文において提案する不正アクセス防止方式の目的は，前節で述べた環境において，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のみを送出できるようにアクセス制御を行い，また，追跡調査のために，ネットワーク利用時にだれが・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．

このためには，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
ネットワークにアクセスしようとしている利用者が利用資格を有するかどうかを確認するために，利用者認証の機能が必要である．また，認証の際に，時刻，利用者名，情報コンセントの位置，割り当てた IP アドレスを記録する機能が必要である．

(2) アクセス制御機能
認証を受けた利用者だけが外部ネットワークにパケットを送出できるようにアクセス制御を行う機能が必要となる．

(3) 送信元 IP アドレス偽造防止機能
送信元 IP アドレスは，IP ネットワークにおいて送信元計算機を特定するための識別子である．IP アドレスの値は利用者が自由に設定できるが，IP アドレスから利用者を特定できるようにするためには，システムから割り当てたアドレス以外は使用できないようにしておく必要がある．すなわち，利用者が勝手な IP アドレスを使用すること，特に，送信元 IP アドレスを他の利用者の IP アドレスへと偽造することを防止できる必要がある．

(4) 送信元 MAC アドレス偽造防止機能
送信元 MAC アドレスは，Ethernet などのデータリンク層において送信元計算機を特定するための識別子である．ある送信元 IP アドレスが，偽造されたものではなく，本来その計算機に割り当てられたものであることを確認するためには，送信元 IP アドレスと計算機との対応をつける必要がある．このとき，計算機を識別するために必要となるのが送信元 MAC アドレスなので，これが偽造されないようにしておく必要がある．

3. 関連研究

情報コンセントにおいてアクセス制御を行う方式として，MAC アドレスによるフィルタリング機能を持つハブを用いる方式（方式 1），DHCP によって割り

☆ 1 万人以上の利用者を有する大学も少なくない．

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方式（方式2）[1),2)]，DHCPに認証情報を追加する方式（方式3）[3)]などがある．

方式1は，あらかじめいくつかのMACアドレスをハブに登録しておき，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，この方式はIPアドレスの偽造を考慮しておらず，また，送信元MACアドレスがハブに登録された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．さらに，接続される可能性のある計算機のMACアドレスをあらかじめすべて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．MACアドレスの事前登録を必要とせず，最初に接続された計算機のMACアドレスのみを有効とする設定が可能なハブも市販されている☆が，接続される計算機が頻繁に入れ替わることを前提とした情報コンセントの設置目的には合致しない．

方式2は，情報コンセントが設置されたネットワークセグメントと外部ネットワークの間にルータを設置し，DHCPサーバによって割り当てられたIPアドレスを持つパケットのみを外部ネットワークに中継するようにルータでフィルタリングする方式である．しかし，この方式は送信元のIPアドレスをすでに他の計算機に割り当てられたIPアドレスへと偽造された場合に，外部ネットワークへの不正パケットの流出を防げない．

方式3では，利用者の計算機がDHCPサーバと共通の暗号鍵を持っている場合に限りIPアドレスを利用者の計算機に割り当てる方式である．しかし，この方法もIPアドレスを偽造されると外部ネットワークへの不正アクセスが可能であり，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となる．

このように，既存のアクセス制御方式はいずれも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．

4. 不正アクセス防止方式

本論文で提案する方式では，システムは利用者認証サーバ，IPアドレス割当てサーバ，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，たとえばポートごとに接続可能な

☆ たとえば，Cisco社製Catalyst2900や3Com社製SuperStackIIなど．

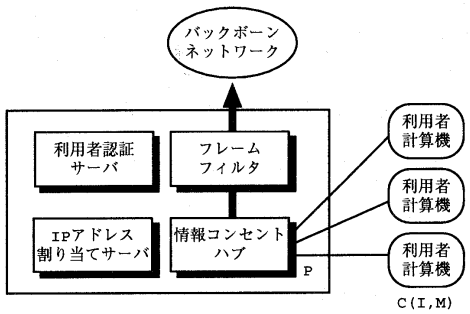

図1 不正アクセス防止のための構成
Fig. 1 Block diagram of our protection mechanism.

MACアドレスを限定するなどの手段により，パケットがどのポートから発信されたかを識別できる状態で他のポートに中継する機能を有する．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アドレス割当てサーバからIPアドレス I の割当てを受ける．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アドレスなどを記録し，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，2.2節で述べたすべての機能を実現することができる．

本方式の特徴は，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．従来方式では，利用者の計算機を送信元のIPアドレスあるいはMACアドレスのみで識別していたが，これらは利用者の側で任意に変更することが可能であるため，悪意を持ってアドレスを偽造された場合に不正アクセスを防止することが不可能であった．これは，IPアドレスとMACアドレスの組で識別しようとしても同様である．しかし，本方式では，IPアドレスとMACアドレスの両者に加えて，さらに情報コンセントのポート識別子という，利用者による偽造が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うる不正アクセス防止（2.1節の条件1）を実現できる．

また，本方式では利用者認証のための機能が必要となるが，これは通常のアプリケーションプログラムとして実現可能であり，OSや既存アプリケーションを変更する必要はない（2.1節の条件2）．

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取得する，（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登録負担が増加することはなく，2.1節で述べた条件3を満たすことができる．

なお，条件4に関しては，方式的に特に問題となる点はないと考えられる．実際に試作したシステムの評価に関しては，6章で述べる．

5. システムの実現

前章で述べた方式に基づき，不正アクセス防止のためのシステムを作成した．以下では，このシステムをLANA（LAN Authentication system）と呼ぶ．

5.1 LANAのシステム構成

実現したLANAシステムは，フィルタリング機能付きハブと，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2**）．

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よい．

フィルタリング機能付きハブ　今回実装したシステムでは，次のような機能を有するスイッチングハブ☆を使用している．

（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

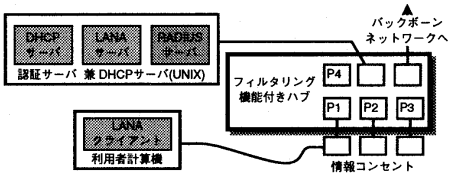

図2　システム構成
Fig. 2　LANA system.

（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[5]によって制御する機能（トラップを含む）

これらの機能により，このハブは単独で図1における情報コンセントハブとフレームフィルタの機能をあわせ持っている．

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[6]をマルチスレッド対応となるよう修正して利用している．

LANAクライアント　利用者計算機上で動作し，利用者認証を行うためにLANAサーバと通信を行うプログラムである．セキュリティを高めるため，利用中はLANAサーバとLANAクライアントとの間でつねにコネクションを確立した状態になっており，このコネクション上の通信はすべて暗号化される．今回はC++（Windows95/98用）ならびにJavaによって実装した．なお，単に利用者認証を行うだけであれば，たとえばWWWブラウザなどの既存のアプリケーションをそのまま利用することも考えられるが，認証を受けた計算機が現在も接続されているかどうかをより確実に確認するために導入している．

DHCPサーバ　DHCPサービスを行うプログラムで，通常のDHCPサーバに対してLANAサーバと通信する機能を付加したものである．ISC

☆ Bay Networks社のBayStack 301[4]（BS301）

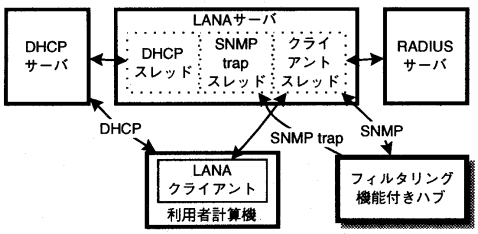

図3 各サーバ，クライアント間の関係
Fig. 3 Functions of each unit.

DHCPD[7]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，利用者認証およびアクセス記録のために，RADIUS[8),9)]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，利用者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[10]を用いた．

LANAにおける各構成要素の関係を**図3**に示す．

5.2 フィルタの詳細

LANAで用いたハブBS301のフィルタリング機能は，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．1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．

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_CL*nnnn*だけは利用者計算機のMACアドレス，IPアドレスによって内容が異なるため，利用者計算機の接続時に動的に定義し，その他のフィルタはLANAシステムの初期化時に定義する．

5.3 動作の詳細

5.3.1 初 期 化

LANAサーバは，利用者計算機が接続されるポートのすべてに，フィルタ（F_COMMON，F_DROP）☆を割り当てる．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．

☆ この表記によって，複数のフィルタグループをこの順序で適用することを表す．

表1 LANAで使用するフィルタ
Table 1 Filters setup.

フィルタグループ名	内 容
F_COMMON	1. ARP request/replyは中継 2. IP以外のフレームは破棄 3. IP option付きフレームは破棄 4. SNMPポートへのフレームは破棄 5. DHCPクライアントからDHCPサーバへのフレームはDHCPサーバの接続されているポートへ転送
F_DROP	1. すべてのフレームを破棄
F_LANA	1. 宛先IPアドレスがLANAサーバでないフレームは破棄
F_CL*nnnn*（*nnnn*はポート識別子）	1. 送信元MACアドレスが利用者計算機のものでないフレームは破棄 2. 送信元IPアドレスが利用者計算機のものでないフレームは破棄

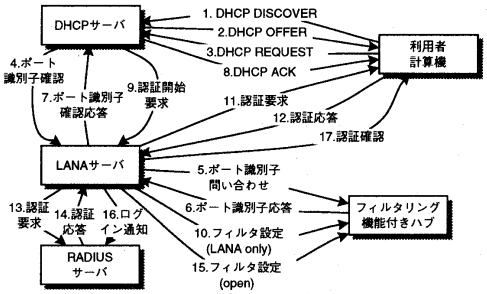

図4 接続シーケンス
Fig. 4 Protocol sequences.

5.3.2 利用者計算機の接続

利用者計算機の接続は，**図4**のシーケンスで行われる．

(1) 利用者は，あらかじめ接続しようとする計算機上でLANAクライアントソフトウェアを動作させておく．

(2) 利用者は，所有する計算機を情報コンセントに接続する．利用者計算機は，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4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から利用者計算機のMACアドレスを取り出し，LANAサーバに対してポート確認要求を送信して，利用者計算機が接続されているポート識別子を問い合わせる（図4の4）．

(4) LANAサーバはポート確認要求を受信すると，各ハブのMACアドレステーブルを検索し，当

該計算機が接続されているハブとポート識別子を特定する．ポート識別子が特定できた場合には，そのハブとポート識別子の情報をDHCPサーバに返す．ポート識別子が得られなかった場合には，エラーを返す（図4の5〜7）．

また，当該MACアドレスが他のポートですでに使用されている場合には，先に接続されていた利用者計算機に対して存在確認を要求する．存在が確認された場合には，あとから接続された利用者計算機のMACアドレスは偽造されたものであると判断してIPアドレスを与えない．先に接続されていた利用者計算機がすでに存在しない場合には，利用者計算機が移動したと考えられるので，先に接続されていたポートに対して切断処理を行い，通常のシーケンスを続行する．

(5) DHCPサーバは，LANAサーバがポート識別子を特定できれば利用者計算機に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指示する（図4の8，9）．ポート識別子を特定できなかった場合はDHCP NAKを返し，利用者計算機に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取ると，当該利用者計算機のMACアドレス，IPアドレスを持つパケットのみを通過させるようなフィルタF_CL*nnnn*を設定し（*nnnn*は利用者計算機が接続されたポート識別子），利用者計算機が接続されたポートのフィルタを（F_COMMON, F_CL*nnnn*, F_LANA）と設定する．これによって，当該ポートは，MACアドレスあるいはIPアドレスの少なくとも一方がフィルタの設定と異なるパケットは通さないようになる．また，この段階では，フィルタF_LANAによって利用者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4の10）．

次に，LANAサーバは利用者計算機上で動作しているLANAクライアントとTCPコネクションを確立し，指数鍵交換方式[11]により秘密鍵を共有した後，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，利用者から利用者名，パスワードを受け取って，LANAサーバに送信する（図4の11，12）．

(7) LANAサーバは利用者名，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4の13，14）．正しい場合，以下の処理を行う（図4の15〜17）．

- フィルタを（F_COMMON, F_CL*nnnn*）と設定し，すべ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利用者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．

5.4 実装上の留意点

本方式を実装するうえで特に留意すべき点とLANAでの解決策について述べる．

5.4.1 DHCPサーバとの接続性の維持

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アドレス，IPアドレスにかかわらずすべ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5番目の式）．これにより，何らかの原因によってある利用者の利用終了をLANAサーバが検出できていない状態で別の計算機が接続されたとしても，その計算機は通常どおりDHCPによってIPアドレスを取得し，利用を開始することができる．

なお，このように不整合が生じた状態で，悪意を持った利用者が直前に接続されていた計算機のMACアドレスとIPアドレスの両方を偽造して計算機を接続す

ると，不正利用を許してしまう可能性がある．この問題に対しては，6.3.4 項で述べる対策を行っている．

5.4.2 再送された DHCP REQUEST の処理

利用者計算機が DHCP で IP アドレスを取得する際，DHCP REQUEST を出してから DHCP ACK/NAK を受信するまでに DHCP REQUEST を再送し，DHCP サーバが重複した 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．

LANA では，DHCP サーバの変更点を最小限にするため，DHCP サーバが DHCP REQUEST を受信すると，必ず LANA サーバにポート確認要求を送信するようにしている．LANA サーバは，認証中あるいは認証済の利用者計算機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，認証開始要求を送信しない．

5.4.3 ポートの終了処理

DHCP では，使用していた IP アドレスの解放を明示的に示すためのメッセージ（DHCP RELEASE）が存在するので，このメッセージを受信した場合に情報コンセントの利用が終了したものとして終了処理（ハブのポートを初期状態に戻す）を行うことが考えられる．しかし，DHCP RELEASE の送信は必須ではないので，必ずしも送信されるとは期待できず，終了処理を行うタイミングが問題となる．

LANA では，5.3.3 項で述べたようにして利用者計算機の切断を検出しているので，DHCP RELEASE に頼らずに利用の終了を検出することが可能であり，結果的に DHCP RELEASE に対する特別な処理は不要となっている．

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ができる．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）．利用者管理は 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．

そこで，考慮すべきは LANA サーバのスケーラビリティであるが，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することは問題ないので，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．

表 2 ハブの操作に要する時間
Table 2 Time consumption for hub operations.

操 作	時 間 (ms)
初期設定	23.5
認証時のフィルタ設定	35.0
認証成功後のフィルタ設定	23.5
ポート識別子の確認	7.5

6.2 試作システムに関する評価

6.2.1 ハブの処理時間

現在使用しているハブである BS301 では，フィルタリングなど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）計算機数が決まってくる．そこで，LANA で必要とされる 3 種類のフィルタのそれぞれについて設定に要する時間を計測した．また，排他的な操作ではないが，利用者計算機が接続されているポート識別子の確認についても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 より，フィルタの設定に要する時間は 23.5〜35.0 ms であり，1 秒あたり 12 台（$= 1000/(23.5 + 35.0)$）程度を処理できることになる．これは，1 台のハブに対して同時に新たな接続が発生したときの制限であることを考慮すると，運用上問題になることはないと考えられる．

また，DHCP によって最初にアドレスを取得する場合に，既存の DHCP サーバでは存在しなかったハブのポート識別子確認という操作が加わっているが，これに要する時間は 7.5 ms 程度である．一方，DHCP において DHCP 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[12]．したがって，LANA システムのために追加された処理に要する時間は十分短く，DHCP シーケンスに及ぼす影響は無視できると考えられる．

6.2.2 登録可能なフィルタ数の制約

LANA サーバにおいて設定するフィルタのうち，利用者計算機に依存するのは前述の F_CL*nnnn* のみである．これは，利用者計算機数（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 5＋1＋1（それぞれ F_COMMON，F_DROP，F_LANA で使用する数）＋2（F_CL*nnnn* で使用する数）× 利用者計算機用ポート数（22）＝51 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．

6.3 セキュリティレベル

4 章で述べたように，本システムでは利用者計算機における 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．

6.3.1 偽 DHCP サーバ

悪意のある利用者が偽の DHCP サーバを稼動させた場合を考える．

この場合，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．

6.3.2 偽造 ARP

悪意を持つ利用者が ARP reply メッセージを偽造し，他の利用者宛ての ARP reqeust に対して自分の MAC 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，悪意のある利用者が他人の MAC アドレスをかたって不正を働くことはできない．

6.3.3 DoS 攻撃

LANA システムは，サービス不能攻撃（Denial of Service Attack）について特別な考慮の対象とはしていないが，特定の利用者計算機から LANA システムの各サーバに対するパケットのレートがある閾値を超えた場合に，そのポートを使用不可とするなどの対策が可能であろう．

6.3.4 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，さら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，通常どお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，ダムハブ上には悪意を持つ利用者の計算機が存在するために情報コンセントハブはリンクダウンを検出できず，SNMP トラップ（Link Down トラップ）を送信しない．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．

この不正アクセスを防ぐために，本システムでは LANA サーバが共通の秘密鍵を持つ LANA クライアントが存在するかどうかを定期的に（1 分に 1 回の割合で）確認するようにしている．この方法でも確認が実行されるまでは不正アクセスの可能性が残されているが，最大でも 1 分間という比較的短い時間に限定される．

また，あわせて，正規に設置された情報コンセント以外に対して不用意に接続しないよう利用者に対して教育しておくことにより，実際の運用上は十分対処可能であると考えられる．

なお，LANA サーバと LANA クライアントの間の通信は 5.1 節で述べたように暗号化されているので，ダムハブを利用して LANA のパスワードを盗聴することはできない．ただし，認証が終了して外部のネットワークに接続された後の通信が盗聴されることについては，利用者の責任である．

7. おわりに

本論文では，不特定多数が計算機を接続しうる情報コンセントにおいて，登録された利用者のみに使用を許し，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方式を提案した．また，本方式を LANA システムとして実装し，その安全性について確認した．

今後の利用者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．今後の課題としては，より多様なハブに対応すること，利用者計算機の接続・切断に加えて，より詳細な挙動の把握を可能とすること，などがあげられる．

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〔現シャープ（株）〕，阪本晃氏，ならびに同大学学術情報総合センター来山至氏（現テキサス大学）に感謝いたします．

参考文献

1) Kobayashi, K. and Yamaguchi, S.: Network Access Control for DHCP Environment, *IEICE Trans. Communications*, Vol.E81-B, No.9,

pp.1718–1723 (1998).
2) 久長 穣, 岡田 隆, 刈谷丈治：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.
3) Droms, R. and Arbaugh, W. (Eds.): Authentication for DHCP Messages, Internet Draft (1998). draft-ietf-dhc-authentication-09.txt.
4) Bay Networks: *Using the BayStack 301 Ethernet Switch* (1996).
5) Case, J.D., Fedor, M., Schoffstall, M.L. and Davin, J.R.: Simple Network Management Protocol (SNMP), RFC 1157 (1990).
6) Carnegie Mellon University: CMU SNMP Library. http://www.net.cmu.edu/projects/snmp/.
7) Internet Software Consortium: ISC DHCP. http://www.isc.org/dhcp.html.
8) Rigney, C., Rubens, A.C., Simpson, W.A. and Willens, S.: Remote Authentication Dial In User Service (RADIUS), RFC 2138 (1997).
9) Rigney, C.: RADIUS Accounting, RFC 2139 (1997).
10) デジタルテクノロジー（株）：DTC Radius 2.03. http://www.dtc.co.jp/Radius2.0/.
11) Schneier, B.: *Applied Cryptography*, John Wiley & Sons (1996).
12) Droms, R.: Dynamic Host Configuration Protocol, RFC 2131 (1997).

(平成11年6月16日受付)
(平成11年9月 2 日採録)

石橋 勇人（正会員）

昭和62年京都大学大学院工学研究科修士課程情報工学専攻修了．平成元年同博士後期課程情報工学専攻退学．同年京都大学大型計算機センター助手．平成10年より大阪市立大学学術情報総合センター講師．高速ネットワーク，ネットワーク管理システム等に関する研究に従事．人工知能学会，IEEE，ACM各会員．

山井 成良（正会員）

昭和61年大阪大学大学院工学研究科（電子工学専攻）博士前期課程修了．昭和63年同大学大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程中退．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師を経て，現在岡山大学総合情報処理センター助教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

安倍 広多（正会員）

平成4年大阪大学基礎工学部情報工学科卒業．平成6年同大学大学院博士前期課程修了．同年NTT入社．平成8年大阪市立大学助手．マルチスレッド機構の実装，マルチメディアアプリケーションの設計等に興味を持つ．電子情報通信学会会員．

大西 克実（正会員）

平成4年大阪大学工学部通信工学科卒業．平成6年同大学大学院修士（通信）課程修了．平成8年大阪市立大学助手となり現在に至る．組合せ最適化問題の解法，分散処理環境の利用に関する研究に従事．電子情報通信学会，日本OR学会各会員．

松浦 敏雄（正会員）

昭和50年大阪大学基礎工学部情報工学科卒業．昭和54年同大学大学院基礎工学研究科（情報工学専攻）後期博士課程退学後，同大学基礎工学部助手．平成4年同大学情報処理教育センター助教授，平成7年大阪市立大学教授．工博．ユーザインタフェース，マルチメディア，情報教育等に興味を持つ．ACM，IEEE，電子情報通信学会各会員．