部外者からの組織内限定サービスへのアクセスを保護するLANアクセス制御システム

山井成良[†] 岡山聖彦[†] 木澤政雄[††,☆]
土居正行[††,☆☆] 河野圭太[†] 大隅淑弘[†]

大学などの組織においてLANアクセス環境を提供する場合，特に学会などのイベント開催時には組織内利用者とそれ以外の利用者（部外者）が混在して利用することが多い．このような場合，部外者でも組織内限定サービスを利用できるなどの問題が生じる．そこで本論文では，LANアクセス環境の利用者には，プライベートアドレスなど，組織内グローバルアドレスとは別のアドレスを割り当て，アクセス先に応じてNAT（Network Address Translation）機能を適用するかどうかを決定する方法を提案する．この方法では部外者が組織内限定サービスへアクセスした場合でも，サーバ側での既存の設定に基づいたアクセス制御が可能となる．また，この方法は既存の組織内ネットワークをそのまま利用するため，LANアクセス環境を場所によらず容易に提供できるという特徴を持つ．提案方法に基づくLANアクセス制御システムを試作して運用した結果，提案方法は十分実用的であることが確認された．

A LAN Access Control System with Protection of Restricted Services from Guest Users

Nariyoshi Yamai,[†] Kiyohiko Okayama,[†] Masao Kizawa,[††,☆]
Masayuki Doi,[††,☆☆] Keita Kawano[†] and Yoshihiro Oosumi[†]

LAN access control systems are often used at many organizations such as universities, to provide network accessibility to both insiders and guest users. However, most of existing LAN access control systems have some problems such that guest users can access some services restricted to insiders. In this paper, we propose a LAN access control method by assigning to user terminals a kind of external addresses such as private addresses. By applying NAT function conditionally depending on whether access to an internal server or not, this method makes it possible to protect restricted services from guest users, without modifying any configuration of existing servers. According to a field testing, the proposed system has been confirmed to be effective and practical.

1. はじめに

近年，軽量・高性能で携帯可能な小型計算機（いわゆるノートPC）が比較的安価に入手できるようになり，このような計算機を個人で所有して持ち歩く利用形態が恒常化している．これにともない，多くの組織では，たとえば大学における図書館や情報処理センターのようなパブリックスペース，あるいは学会などのイベント開催時の会場において，情報コンセントや無線LAN（以下では，これらをまとめて情報コンセントなどと表記する）を設置して，利用者の計算機をネットワークに接続できるような環境（以下，LANアクセス環境）を提供している．

このような環境では，ネットワーク不正利用を防止したり不正利用を行った利用者を追跡できるようにしたりするため，利用者の認証を行って有資格者だけにネットワークアクセスを許可し，また誰がいつネットワークを利用したかを記録できるようなアクセス制御機構が必須である．実際にも，このようなアクセス制御機構を実現するため，LANA[1)]，LANA2[2)]，OpenGate[3)]，PortGuard[4)]など多くのLANアクセス制御システムがこれまで開発されてきた．これらのうち

† 岡山大学総合情報基盤センター
Information Technology Center, Okayama University
†† 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
☆ 現在，株式会社日立製作所
Presently with Hitachi Ltd.
☆☆ 現在，株式会社ACCESS
Presently with ACCESS Co., Ltd.

特に LANA2 は，利用資格の有無によるアクセスの可否だけではなく，利用者ごとにアクセスを許可する IP アドレスやポート番号を制御するような機能を有しており，同機能を用いることによりたとえば大学において管理者，教員，学生，学外者などの区分（以下，利用者属性）に応じてアクセス可能な IP アドレスの範囲を個別に設定することが可能である．

ところが，組織外の利用者（以下，部外者）に対して上記のような LAN アクセス環境を提供する場合，上記のような LAN アクセス制御システムを導入しても様々な問題が生じることが多い．すなわち，たとえば WWW における組織内限定コンテンツの提供においてサーバ側で IP アドレスに基づくアクセス制御が用いられている場合，部外者が情報コンセントを利用してこのような情報にアクセスすると，サーバ側では組織内からのアクセスと区別できないためこれを許可してしまうという問題が生じる．一方，LAN アクセス制御システムを用いて部外者からサーバへのアクセスを遮断すると，組織内限定コンテンツだけでなく組織外にも公開しているコンテンツについても部外者がアクセスできないという別の問題が生じる．このほかにも，たとえば独自に LAN アクセス環境専用のネットワークを構築して ISP（Internet Service Provider）経由でアクセスさせる方法など，いくつかの方法が考えられるが，いずれも管理コストが大きく，実用的ではない．このような理由により，たとえば部外者からの組織内限定コンテンツへのアクセスを黙認したり，逆に部外者から組織内へのアクセスは公開コンテンツも含めていっさい認めなかったり，あるいは部外者に対しては LAN アクセス環境の提供自体を行わなかったりするなど，不適切なアクセス制御を行っている組織は，我々が確認できたものだけでも多数存在する．

そこで，本論文では部外者からの組織内限定サービスへのアクセス保護を，管理コストを増加させずに可能にする LAN アクセス制御システムを提案する．本システムは NAT（Network Address Translation）[5] 機能の適用条件を工夫することにより，部外者が組織内限定サービスへアクセスした場合でも，サーバ側での設定に基づいたアクセス制御を行うことが可能である．また，本システムは既存の組織内ネットワークを利用するため，LAN アクセス環境の提供が場所によらず容易に行えるという特徴を持つ．

以下，まず 2 章では，LAN アクセス環境が満たすべき条件を述べ，従来の LAN アクセス制御システムを同環境に適用した場合の問題点について述べる．次に 3 章では，提案する LAN アクセス制御手法について述べ，4 章で提案手法に基づいて試作したシステムの実装について説明する．また，2005 年 8 月に岡山大学で開催された国際会議において本システムの運用を行ったので，5 章ではその結果を報告する．

2. LAN アクセス環境とアクセス制御

2.1 想定するネットワーク環境

本論文では，**図 1** に示すように，組織内限定サービスが提供されているネットワークにおいて，部外者が利用可能な LAN アクセス環境を構築する場合を想定する．その場合，LAN アクセス環境の提供場所や端末数は定まっておらず，たとえばイベントなどによって異なり，また特に規模の大きいイベント開催時には複数箇所で同時に提供することもありうるものとする．

この図において，組織内限定サービスを提供するサーバの一部は，LAN アクセス環境とは独立して管理されているものとする．すなわち，LAN アクセス環境の管理者は，上記のサーバについて存在や組織内限定サービスの内容を必ずしも知っているとは限らず，同様に上記のサーバの管理者は LAN アクセス環境について特に関知していないものとする．また，上記のサーバの一部はアクセス元のクライアントが組織内，組織外のどちらに属するかを IP アドレスに基づいて判断し，その結果に応じてアクセス制御を行っているものとする．さらに，ネットワーク構成の動的な変更に容易に対応できるようにするため，組織内ネットワークでは少なくとも基幹部において RIP [6] などの動的経路制御プロトコルを用いて経路制御を行っているものとする．

このようなネットワークは，大学など多数の下部組織を有するような比較的規模の大きい組織では一般的なものである．また，IP アドレスに基づくサーバのアクセス制御も特に WWW においてよく見られる一

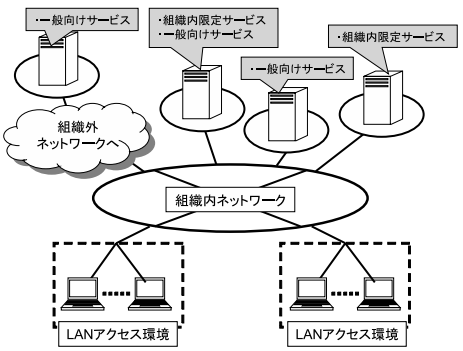

図 1 想定するネットワーク環境
Fig. 1 Target network environment.

般的な方法である．なお，サーバにおけるアクセス制御には，IP アドレスに基づく方法以外に利用者認証に基づく方法が考えられるが，これについては 2.3 節で議論する．

2.2 部外者による組織内限定情報へのアクセス

前節で述べたネットワーク環境において部外者が利用可能な LAN アクセス環境を構築する場合，従来のアクセス制御技術では部外者による組織内限定サービスへのアクセスにおいて問題が生じる．以下では，この問題について詳細に述べる．

図 1 で示したようなネットワーク環境の場合，利用者端末にはしばしば組織内ネットワークで利用されるグローバル IP アドレスが割り当てられ，これがそのまま通信に用いられる．この場合，利用者端末からサーバにアクセスすると，サーバ側では受け取ったパケットの送信元アドレスに基づいて組織内からのアクセスと判断するため，結果として部外者による組織内限定サービスへのアクセスを許すことになる．一方，利用者端末にプライベート IP アドレスが割り当てられる場合では，そのままでは組織外との通信が行えないため通常は組織内ネットワークとの接続点に NAT 機能が導入され，利用者端末からサーバに送出されたパケットは同機能により送信元 IP アドレスがプライベート IP アドレスからグローバル IP アドレスに変換された後にサーバに中継される．したがって，利用者端末にグローバル IP アドレスを割り当てる場合と同様に，サーバではこれを組織内からのアクセスと判断し，本来行われるべき組織内限定サービスへのアクセス制御が実際には機能しないことになる．この様子を**図 2** に示す．

このように，組織内ネットワークをそのまま利用して LAN アクセス環境を提供する場合，単純な方法では組織内に存在するすべての組織内限定サービスへのアクセスを部外者にも許可するという問題が生じることになる．

2.3 従来のアクセス制御方法とその問題点

上記の問題に対処する既存の方法として，以下に示すような方法があげられる．

- LAN アクセス制御システム側でのフィルタリング
- サーバ側での特定 IP アドレスからのアクセス拒否
- サーバ側での利用者認証
- LAN アクセス環境専用ネットワークの利用

ところが，これらの方法はいずれも機能上あるいは管理上の問題点を有する．以下では，これらの問題点について述べる．

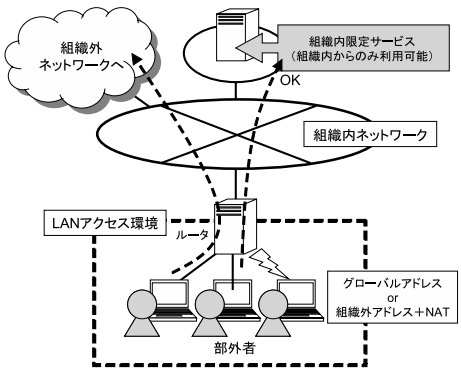

図 2 部外者からの組織内限定サービスへのアクセス制御における問題点

Fig. 2 A problem on access control of restricted services from guest users.

2.3.1 LAN アクセス制御システムにおけるフィルタリング

1 章で述べたように，LAN アクセス制御システムには，たとえば文献 2) のシステムなど，利用者単位でのアクセス制御機能を備えているものが知られている．このようなシステムでは，組織内限定サービスを提供するサーバへのアクセスを部外者に対しては禁止するように設定する方法が適用可能である．

ところが，このような設定を行うためには，組織内限定サービスを提供するすべてのサーバを LAN アクセス制御システムの管理者があらかじめ把握しておく必要がある．これは管理者への負担増大を招き，特に総合大学でよく見られるように，独立性の高い下部組織を多数有するような組織では事実上困難である．また，WWW のようにサーバ単位ではなくコンテンツ単位でアクセス制御できるようなサービスの場合には，IP アドレスに基づいてアクセス制御を行うと一般利用者に公開しているコンテンツにも部外者はアクセスできなくなる危険性があるという新たな問題も生じる．

したがって，この方法を実際に適用できるのは，組織内限定サービスを特定のサーバに集約しているような組織に限られ，一般の組織への適用は困難である．

2.3.2 サーバ側での特定 IP アドレスからのアクセス拒否

LAN アクセス制御システムにおいて利用者端末にグローバル IP アドレスを割り当てる場合，端末に割り当てられる可能性のある IP アドレスを一定の範囲に収めることにすれば，部外者による組織内限定サービスへのアクセスをサーバ側で拒否することが可能になる．すなわち，端末に割り当てられる可能性のある IP アドレスについてはサーバ側でアクセスを拒否す

るように設定すればよい．また，上記の方法とは異なり，この方法ではコンテンツ単位でのアクセス制御にも対応することが可能である．

ところが，この方法では組織内限定サービスを提供するすべてのサーバにおいて，管理者は部外者の端末に割り当てられるアドレスを把握したうえでアクセス制御の設定変更を行う必要があり，該当サーバが多い組織では特に，各サーバの管理者の負担が増加する点が問題となる．また，利用者属性に応じたアクセス制御を行うためには，たとえば割り当てられるIPアドレスの範囲を利用者属性に応じて切り替え，かつ各サーバにおいてもこれに応じてアクセス制御の設定を調整するなど，煩雑な作業が必要になる．さらに，特に下部組織を多数有するような組織などにおいて各サーバが独立して管理されている場合には，組織内限定サービスのアクセス制御設定が不適切であるため部外者からのアクセスを許す危険性は依然として存在する．

なお，利用者端末にプライベートIPアドレスが割り当てられる場合では，NAT機能により変換された後の送信元IPアドレスがアクセス制御の対象となるため，これを一定の範囲に収める必要があることに注意する．

2.3.3 サーバ側での利用者認証

組織内限定サービスを部外者のアクセスから保護する別の方法として，サーバ側で何らかの利用者認証を行う方法が考えられる．この方法を用いれば，LANアクセス環境だけでなく利用者がどこからアクセスしても適切にアクセス制御を行うことが可能となる．また，この方法は多くのサービスで利用可能であり，実際にもよく用いられている．

しかし，利用者認証は特定多数の利用者に対するアクセス制御方法であり，組織内限定サービスのように組織内の不特定多数の利用者に対するアクセス制御方法としては適していないと思われる．すなわち，この方法では各サーバはアクセス許可の対象となるすべての利用者について認証可能となるように事前登録が必要となるため，利用者が不特定多数であると事前登録が事実上困難である．この状況は，組織内の全利用者を登録した認証サーバがあれば，これを活用することにより登録の手間を軽減することが可能である．しかし，その場合でもこれまで利用者認証によるアクセス制御を行っていなかったすべての組織内限定サービスにおいて利用者認証を行うように設定変更する必要があり，管理者の負担が大きくなったり不適切なアクセス制御設定のため部外者からのアクセスを許したりする点は改善されない．

2.3.4 LANアクセス環境専用ネットワークの利用

さらに別の方法として，LANアクセス環境専用のネットワークを構築してISP経由で部外者にアクセスさせるようにする方法があげられる．この方法はLANアクセス環境の利用者は組織外のネットワークに直接接続されるため，IPアドレスに基づく組織内限定サービスのアクセス制御は期待どおりに機能する．しかし，特にイベント開催時などLANアクセス環境を提供する場所が定まっていない場合には，提供場所に応じて専用ネットワークを構築しなおす必要があり，管理者の負担が大きくなる点は改善されない．また，LANアクセス環境用に十分な帯域を確保するには，ISPとの契約にともなう相応の費用が必要となり，その負担も無視できない．

3. 部外者の利用を考慮したLANアクセス制御

3.1 提案方法の概要

前章で述べたように，組織内ネットワークを用いてLANアクセス環境を提供する場合，IPアドレスに基づく既存のアクセス制御方法をそのまま用いると適用範囲が限定されたり管理者の負担が増大したりする問題が生ずる．この問題の根本的な原因は，部外者かどうかにかかわらず，LANアクセス環境の利用者による組織内限定サービスへのアクセスが組織内のIPアドレスを用いて行われる点にある．

そこで，本論文では部外者が組織内ネットワークにアクセスする場合には，各サーバが組織外として認識するIPアドレス（以下，LANアクセス環境用組織外アドレス）を用いる方法を提案する．この方法では，IPアドレスに基づく既存のアクセス制御をそのまま用いて部外者からの組織内限定サービスへのアクセスを制御することが可能であるため，管理者の負担を大幅に削減できる．また，LANアクセス環境用組織外アドレスの経路情報を組織内ネットワークに広告することにより，原理的には組織内ネットワークの任意の場所に容易にLANアクセス環境を構築することが可能となる．

この方法におけるLANアクセス環境用組織外アドレスには，従来の組織内グローバルIPアドレスとは別のものを新規に取得する方法が考えられる．しかし，最近はIPアドレス枯渇問題が顕在化してきたため，IPアドレスの新規取得には厳しい条件が課せられ☆，常時使われるとは限らないLANアクセス環境のため

☆ 文献7)の10.2節参照

に専用アドレスを取得することは必ずしも容易ではない．また，たとえこれを取得できたとしても，たとえばイベントの規模に応じて LAN アクセス環境の同時提供数や全体の端末数が変わるため，IP アドレス数に大幅に過不足が生じる恐れもある．

そこで，提案方法では，たとえばプライベート IP アドレス[8] など他組織との通信には用いられないアドレスを LAN アクセス環境用組織外アドレスとして用いる．その際，たとえばすべてのプライベート IP アドレスを組織内アドレスとして運用しているような環境では，代わりに IANA が予約しているアドレス[9] を利用してもかまわない．ただし，正式に取得していないこれらのアドレスをそのまま用いると，組織外との通信を行うことはできないという弊害が生じる．そこで，提案方法では，NAT 機能の適用条件を工夫することにより，部外者が組織内ネットワークにアクセスする場合には LAN アクセス環境用組織外アドレスを，それ以外の場合には組織内グローバルアドレスをそれぞれ送信元アドレスとして用いるような技法を用いる．

以下では，提案方法の詳細について述べる．

3.2 システム構成

提案する LAN アクセス制御システムは，**図 3** に示すように，アクセス制御装置に NAT ルータを付加した構成となっている．

このうち，アクセス制御装置は通常の LAN アクセス制御システムで用いられるものと同様に利用者認証機能を持ち，部外者を含むネットワーク利用有資格者に対してのみネットワークへのアクセスを許可する．また，利用者単位でのアクセス制御機能を備えており，部外者に対してはネットワーク層およびトランスポート層において対外接続用ファイアウォールなどと同等のアクセス制御を行うようにする．一方，NAT ルータは次節で述べるように送信先 IP アドレスと宛先 IP アドレスが特定の条件を満たしているときに限りアドレス変換動作を行う．また，利用者端末で用いられる LAN アクセス環境用組織外アドレスの経路情報を組織内ネットワークに広告する役割も果たす．なお，1 つの装置が NAT ルータとアクセス制御装置の両方の機能を持つような構成や利用者単位でのアクセス制御機能を NAT ルータが持つような構成であってもかまわない．

このほかにも，利用者端末から不正利用が行われた場合に備えてアクセス記録を採る機能など，従来の LAN アクセス制御システムで実現されている機能がいくつか存在するが，これらの機能については以下では説明を省略する．

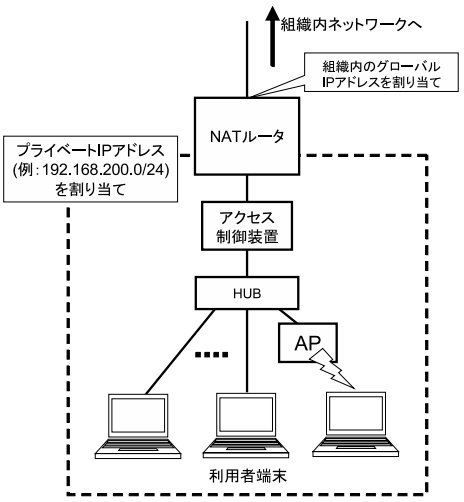

図 3 提案システムの構成
Fig. 3 A structure of the proposed system.

3.3 システムの動作手順

次に本システムの動作手順について，順に説明する．

(1) 組織内ネットワークへの経路情報の広告
LAN アクセス制御システムが組織内ネットワークに接続されると，NAT ルータは RIP などの動的経路制御プロトコルを用いて利用者端末に割り当てられる LAN アクセス環境用組織外アドレスを組織内ネットワークに広告する．これにより，LAN アクセス環境用組織外アドレスを割り当てられた利用者端末と組織内ネットワークとの間でアドレス変換を行わずに直接通信することが可能になる．

(2) 利用者端末への IP アドレス割当て
LAN アクセス制御システムに接続されると，利用者端末は DHCP などの動的 IP アドレス割当て機能を用いて IP アドレスの割当てを要求する．アクセス制御装置あるいは NAT ルータはこの要求に応じて利用者端末に LAN アクセス環境用組織外アドレスのうちの 1 つを割り当てる．

(3) 利用者の認証
アクセス制御装置は利用者端末の認証を行い，利用者がネットワーク利用有資格者かどうかを判定する．もしそうであれば，当該端末によるネットワークアクセスを許可する．さらに，認証に成功した場合には，NAT ルータは当該利用者の属性および利用者端末の IP アドレスを取得する．

(4) アドレスの変換
NAT ルータでは，利用者属性が組織内利用者（部内者）である利用者端末に関するパケットは，通信相手の IP アドレスによらずに LAN アクセス環境用組織外アドレスと組織内グローバルアドレスとの間で通常のアドレス変換を行う．一方，利用者属性が部外者である利用者端末に関するパケットは，通信相手の IP アドレスに応じてアドレス変換を行うかどうかを決定する．すなわち，通信相手が組織外である場合に限って NAT ルータはアドレス変換を行ってから中継し，そうでない場合にはそのまま中継する．

（処理手順終わり）

なお，上記の手順において，アクセス制御装置が利用者認証を IP アドレスの割当て前に行える場合には，手順 (2) と (3) の処理を入れ替えることが可能である．また，認証成功後に IP アドレスを新たに割り当てたり以前の割当てを変更したりできるようなアクセス制御装置を用いている場合には，部内者用と部外者用の 2 種類の LAN アクセス環境用組織外アドレスを用意し，利用者の属性に応じたアドレスを認証成功後に割り当てることにより，手順 (3) において NAT ルータが行う利用者属性および利用者端末の IP アドレスの取得を省略できる．この場合，NAT ルータではあらかじめ LAN アクセス環境用組織外アドレスを含むパケットについてはアドレス変換を行わないように静的に設定しておくだけでよい．

例として，部外者が LAN アクセス制御システムを利用した場合の提案方法の動作を**図 4** に示す．

この例において，NAT ルータの組織内ネットワーク側 IP アドレスは組織内グローバルアドレスである A.B.C.D，LAN アクセス環境側 IP アドレスはプライベートアドレス 192.168.X.1 が割り当てられている．組織内には LAN アクセス環境用組織外アドレスとして 192.168.X.0/24 への経路が広告されており，このアドレスは組織内のすべてのサーバにおいて組織外アドレスとして認識されているものとする．

ここで，ともに部外者である利用者 A，B がそれぞれ端末を LAN アクセス制御システムに接続し，利用者認証に成功した後に利用者 A は組織外へ，利用者 B は組織内にアクセスする場合を考える．この場合，NAT ルータは利用者 A，B はともに部外者であることをアクセス制御装置より通知されているため，パケットの宛先が組織外であるかどうかの判定が必要であると判断する．利用者 A から送られたパケットについては，宛先が組織外であるため，NAT ルータは送信元 IP アドレスを端末に割り当てられた 192.168.X.2 から A.B.C.D に変換する．このアドレスはグローバルアドレスであるため，利用者 A は組織外との通信が可能になる．一方，利用者 B から送られたパケットについては，宛先が組織内であるため，NAT ルータはアドレス変換を行わず，端末に割り当てられた 192.168.X.3 をそのまま送信元アドレスとして用いながら組織内ネットワークに中継する．組織内限定サービスを提供するサーバでは，このアドレスを組織外のものと見なすため，利用者 B からのアクセスを正しく拒否することができる．

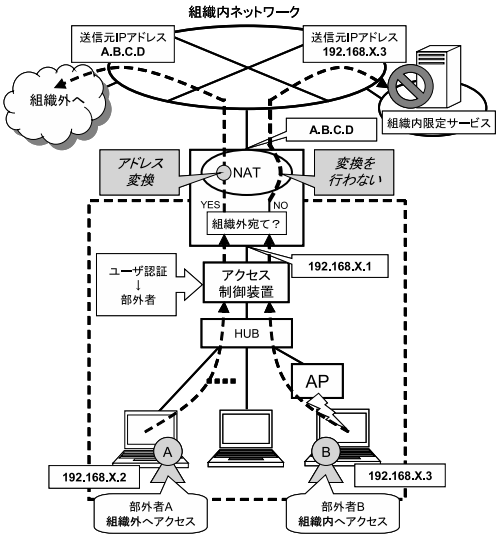

図 4 部外者利用時の提案方法の動作
Fig. 4 Behavior of the proposed method in case of access by guest users.

この例のように，提案方法は利用者に対して，組織外ネットワークへのアクセスを許しながら，組織内限定サービスへのアクセスについては IP アドレスに基づく従来のアクセス制御設定をそのまま用いて拒否することが可能となる．

4. 試作システムの実装

前章で述べた提案方法に基づき，我々は試作システムの実装を行った．本システムの構成を**図 5** に示す．なお，本システムは，5 章で述べる試験運用の時点では，利用者属性に基づいたアクセス制御機能は未実装であり，すべての利用者を部外者として扱った．そこで，以下ではまず試験運用の時点でのアクセス制御機能（以下，基本機能）の実装について述べ，次に利用者属性に基づいたアクセス制御機能の実装において変

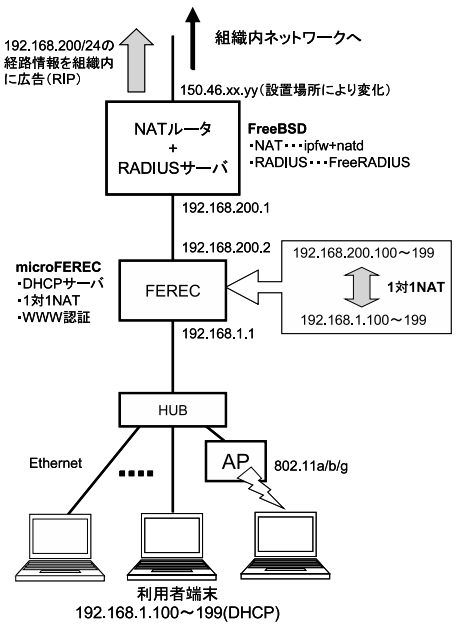

図 5 試作システムの構成
Fig. 5 The structure of the prototype system.

更した点について述べる．

4.1 基本機能の実装

4.1.1 アクセス制御装置

試作システムでは，アクセス制御装置として市販製品の microFEREC [10] を用いた．microFEREC の利用者は，有線（イーサネット）もしくは無線（IEEE 802.11a/b/g）でネットワークに接続し，microFEREC が提供する WWW 認証に成功した端末のみが通信を許可される．また，microFEREC は DHCP サーバ機能を有しており，試作システムでは利用者端末への IP アドレス割当てにこの機能を用いた．microFEREC では同時に 125 人までの利用が可能であるが，試作システムでは 5 章で述べる試験運用の規模などから最大同時利用者数を 100 人とし，LAN アクセス環境用 IP アドレスとして 192.168.1.100〜199 を用いた．

microFEREC には NAT 機能が搭載されており，試作システムではこの機能の利用について事前に検討を行った．その結果，この NAT 機能では前章で述べたような条件付きのアドレス変換を行うことができなかったため，図 5 のように別途 NAT ルータを導入することにした．この場合，アクセス制御装置ではアドレス変換機能が不要になるが，当時の microFEREC ではアドレス変換を多対 1 もしくは 1 対 1 のうちのいずれかのモードで必ず作動させる必要があったため，やむをえず 1 対 1 のアドレス変換を採用し，端末に割り当てた 192.168.1.100〜199 を 192.168.200.100〜199 に変換するように設定した．なお，変換後のアドレスもプライベートアドレスであるが，学内のサブネット管理者にはサブネット内では使用しないようにあらかじめ通知しているため，組織外のアドレスとして認識されるものと想定している．

4.1.2 NAT ルータ

試作システムでは，FreeBSD 5.3 が稼動する計算機を用いて NAT ルータを実装した．その際，FreeBSD 5.3 において NAT 機能を提供する標準的なプログラムである `natd` [11] を利用し，3.3 節で述べたようなアドレス変換を行った．具体的には FreeBSD における標準的なファイアウォールプログラム `ipfw` において **図 6** のようにルールを記述することにより，組織外へのアクセスの場合にのみアドレス変換を行うようにした．

この図において，192.168.200.0/24 は LAN アクセス環境用組織外アドレス，150.46.0.0/16 は岡山大学に割り当てられたグローバルアドレス，150.46.xx.yy は NAT ルータにおける学内ネットワーク側インタフェースの IP アドレスをそれぞれ表す．したがって，図 6 の 110 番のルールは，利用者端末から学外宛の IP パケットを `natd` に渡すことを意味する．その結果，利用者端末から学外宛のパケットは `natd` により送信元アドレスが 150.46.200.0/24 から 150.46.xx.yy に多対 1 変換されて中継される．一方，120 番のルールは学外から NAT ルータ宛へのパケットを `natd` に渡すことを意味する．これにより学外から NAT ルータ宛のパケットが `natd` により利用者端末宛になるようにアドレス変換されて中継されるようになる．なお，利用者端末と学内との通信で用いられるパケットは，65535 番のルール（デフォルトルール）☆によりそのまま中継される．

また，NAT ルータは LAN アクセス環境用組織外アドレス（192.168.200.0/24）に関する経路情報を学内ネットワークへ広告する必要がある．岡山大学では，基幹ネットワークにおいて RIP による動的経路制御を行っているため，NAT ルータにおいて，学内ネットワーク側に 192.168.200.0/24 のネットワークに関する RIP 経路情報を広告するように設定した．

4.1.3 RADIUS サーバ

microFEREC では，内部に登録できるアカウント情報が最大 200 人分に限られているが，それ以上のア

☆ FreeBSD では OS 構築時のオプション指定によりデフォルトルールの内容をこのように変更できる．

```
00110 divert natd ip from 192.168.200.0/24 to not 150.46.0.0/16
00120 divert natd ip from not 150.46.0.0/16 to 150.46.xx.yy
65535 allow ip from any to any
```

図 6 NAT ルータにおける ipfw ルールの初期設定
Fig. 6 Initial ipfw rules on the NAT router.

```
00010 allow ip from 192.168.200.2 to me
00020 allow ip from me to 192.168.200.2
00110 divert natd ip from 192.168.200.0/24 to not 150.46.0.0/16
00120 divert natd ip from not 150.46.0.0/16 to 150.46.xx.yy
65535 allow ip from any to any
```

図 7 NAT ルータにおける変更後の ipfw ルール設定
Fig. 7 Modified ipfw rules on the NAT router.

カウント情報を扱えるように RADIUS サーバ[12] を外部アカウントサーバとして指定することが可能である．そこで試作システムでは，同サーバの 1 つである FreeRADIUS[13] を NAT ルータ上で動作させ，microFEREC から参照できるようにした．その際，図 6 の設定だけでは，microFEREC（192.168.200.2）–NAT ルータ（192.168.200.1）間で発生する RADIUS 関連の通信も natd に渡され，正しく認証できないことが判明した．そこで，ipfw のルールを**図 7** に示すように変更することにより，microFEREC − NAT ルータ間の通信については natd に送らないようにした．

4.2 利用者属性に基づいたアクセス制御機能の実装

利用者属性に基づいたアクセス制御を行うためには，3.3 節で述べたように NAT ルータは利用者認証成功時に利用者端末の IP アドレスと利用者属性の両方（以下，利用者情報）を取得し，これに基づいて当該利用者端末のアドレス変換条件を設定する必要がある．以下では，これらの処理方法について述べる．

まず，利用者属性の設定については，RADIUS において利用者に適用すべきフィルタ名を表す Filter-ID 属性[12] が用意されており，microFEREC においても同属性に基づくフィルタリング機能を有するため，これをそのまま用いることにした．また，NAT ルータにおける利用者情報の取得については，本実装では NAT ルータが RADIUS サーバを兼ねているため，FreeRADIUS のログ機能を利用した．すなわち，NAT ルータ上で FreeRADIUS の出力するログ情報☆を監視しておき，認証成功時に新たなログ情報が記録されると，その中から利用者情報を取得するようにした．

NAT ルータにおけるアドレス変換については，以下のように設定を行うように改良した．ipfw の基本的なルール設定は図 7 と同様であるが，部内者が認証に成功すると，当該部内者が使用する IP アドレスに関しては通信相手が組織内の場合でもアドレス変換を行うためのルールを追加するようにした．このルールには管理のために IP アドレスに対応した番号が付けられており，FreeRADIUS のログ情報監視により部内者の利用終了が確認されたとき，あるいは同じ IP アドレスを割り当てられた部外者が認証に成功したときにはこのルールを削除して，誤って部外者に適用されないようにした．

例として，図 5 において部内者および部外者がそれぞれ 192.168.1.123 および 192.168.1.124 を割り当てられた端末から認証に成功した場合の ipfw ルールを**図 8** に示す．この例では，部内者に割り当てられた 192.168.1.123 に関して 10123 番☆☆のルールが追加されている．これにより，192.168.1.123 から送出されるパケットに対しては，宛先が学外および学内の場合にそれぞれ 00110 番および 10123 番のルールが適用されるため，いずれの場合にもアドレス変換が行われる．一方，部外者に割り当てられた 192.168.1.124 に関しては何のルールも追加されていない．したがって，192.168.1.124 から送出されるパケットに対しては，宛先が学外の場合には 00110 番のルールが適用されアドレス変換が行われるが，宛先が学内の場合に

☆ アカウンティング情報と認証応答情報には，それぞれ利用者端末の IP アドレスと利用者属性が含まれる．

☆☆ ルールの番号は 10000 +（IP アドレスの 4 オクテット目）としている．

```
00010 allow ip from 192.168.200.2 to me
00020 allow ip from me to 192.168.200.2
00110 divert natd ip from 192.168.200.0/24 to not 150.46.0.0/16
00120 divert natd ip from any to me via interface
10123 divert natd ip from 192.168.200.123 to 150.46.0.0/16
65535 allow ip from any to any
```

図 8 部内者・部外者混在時における ipfw ルール設定
Fig. 8 ipfw rules for mixed users of an insider and a guest.

は 65535 番のルールが適用されアドレス変換が行われない．このような動作により，部内者と部外者が混在する場合でも適切にアクセス制御が行われることになる．なお，図 8 では図 7 と比べると 00120 番のルールが異なるが，これは以下の理由による．

- 送信元アドレス範囲の any への変更は，部内者が利用する場合には学外からだけでなく学内から NAT ルータに送られるパケットについてもアドレス変換の対象となったために必要である．
- 宛先アドレス範囲の me への変更および適用対象インタフェース via *interface* の指定は，従来の 150.46.xx.yy と等価であり，このルールが 150.46.xx.yy の変更に依存しないようにするための改良である．なお，*interface* は NAT ルータにおける学内ネットワーク側インタフェース名を表す．

4.3 動作試験

以上の構成および設定に基づき，我々は LAN アクセス制御システムを試作し，同システムを岡山大学の学内ネットワークに接続してアクセス制御機能が正常に動作するかどうかを調査した．その結果，学外者としてアクセスした場合には，利用者端末から学内，学外へのアクセスは原則として可能であるが，いくつかの WWW サーバにおいて提供される学内限定情報にはアクセスできないことを確認した．また，一部の計算サーバにおける telnet や ftp など，WWW 以外の学内限定サービスへのアクセスも試みたが，いずれも利用者端末からはアクセスできないことを確認した．一方，学内者としてアクセスした場合には，WWW サーバの学内限定情報や WWW 以外の学内限定サービスを含めたすべてのサービスについて，本システムを用いない場合と同様にアクセスできることを確認した．これにより，調査した範囲では，試作システムは部内者と部外者を識別し，サーバ側の設定を何ら変更することなく，部外者に対する組織内限定サービスへのアクセス保護機能を提供できることが確認された．

5. 運用事例

試作システムは，2005 年 8 月に岡山大学で開催された国際会議において試験運用された．本章ではその結果を紹介する．なお，4 章で述べたように，試験運用の時点では試作システムは利用者属性に基づいたアクセス制御機能は未実装であり，すべての利用者を部外者として扱った．

会場となった岡山大学一般教養棟の 1 教室において試作システムを学内ネットワークに接続し，LAN アクセス環境を提供したところ，3 日間の開催期間中に約 200 人の参加者が同環境を利用した．試作システムでは最大同時利用者数は 4.1.1 項で述べたように 100 人としたが，実際の同時利用者数は最大でも 20 人程度であった．

開催期間中の運用状況を以下に示す．

まず，試作システムの設置および設定に関しては，システム搬入後に教室内の情報コンセントに接続し，NAT ルータの学内ネットワーク側インタフェースの IP アドレスを設定し，さらにこの IP アドレスに基づいて図 7 の 00120 番のルールを書き換えるだけで完了し，システム搬入時間を除くと 10 分以内に完了した．学内ネットワークでは，本システムで使用する 192.168.200.0/24 についてもすでに経路情報を RIP により広告できるように設定されていたため，特に設定を変更する必要はなかった．

次に，試作システムの利用に関しては，サービス初日において，利用者全員がアクセスができないという障害が発生したため，その原因を調査した．その結果，ある利用者の端末からパケットが大量に送信されていたことが判明したため，その後ただちにその利用者の端末をネットワークから切り離し，障害から復旧した．この障害の発生中には NAT ルータではほとんどトラフィックが観測されなかったことから，この障害の原因は LAN アクセス環境内での輻輳であり，NAT ルータの過負荷によるものではないと推測される．

これ以外には特に障害は発生せずに LAN アクセス

環境を提供でき，また性能上や機能上の問題も特に発生しなかったため，試作システムは従来の LAN アクセス制御システムと同等の水準で十分実用に耐えうるといえる．

6. ま と め

本論文では，部内者と部外者が混在する環境において，部外者が組織内限定サービスへアクセスした場合でも，サーバ側での設定を変更することなく IP アドレスに基づくアクセス制御を行えるような LAN アクセス制御方法を提案した．また，この方式は，既存の組織内ネットワークを利用するため，LAN アクセス環境の提供が場所によらず容易に行えるという特徴を持つことも明らかにし，試作システムの実装および試験運用によりその有効性を示した．

今後の課題としては，利用者の区分を細分化し，たとえば下部組織内限定サービスと組織内限定サービスを区別してアクセス制御を行えるように提案方式を拡張することがあげられる．

謝辞 本研究の一部は，総務省・戦略的情報通信研究開発推進制度（特定領域重点型研究開発プログラム）の補助を受けている．ここに記して感謝の意を表する．

参 考 文 献

1) 石橋勇人，山井成良，安倍広多，大西克実，松浦敏雄：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，情報処理学会論文誌，Vol.40, No.12, pp.4353–4361 (1999).
2) 石橋勇人，山井成良，安倍広多，阪本 晃，松浦敏雄：利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式，情報処理学会論文誌，Vol.42, No.1, pp.79–88 (2001).
3) 渡辺義明，渡辺健次，江藤博文，只木進一：利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発，情報処理学会論文誌，Vol.42, No.12, pp.2802–2809 (2001).
4) 西村浩二，秋成秀紀，野村嘉洋，相原玲二：遠隔機器制御プロトコルを用いた有線／無線 LAN 用情報コンセントシステム，情報処理学会論文誌，Vol.43, No.2, pp.662–670 (2002).
5) Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC1631, IETF (1994).
6) Malkin, G.: RIP Version 2, RFC2453, IETF (1998).
7) 社団法人日本ネットワークインフォメーションセンター：JPNIC におけるアドレス空間管理ポリシー (2005). http://www.nic.ad.jp/doc/jpnic-01041.html
8) Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G.J. and Lear, E.: Address Allocation for Private Internets, RFC1918, IETF (1996).
9) IANA: Internet protocol v4 address space (2006). http://www.iana.org/assignments/ipv4-address-space
10) 株式会社ネットスプリング：FEREC (2006). http://www.ferec.jp/
11) Cobbs, A., Mott, C., Suutari, A., Nelson, D., Somers, B. and Ermilov, R.: natd—Network Address Translation daemon, *FreeBSD System Manager's Manual* (2003).
12) Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC2865, IETF (2000).
13) The FreeRADIUS Project: FreeRADIUS—building the perfect RADIUS server (2004). http://www.freeradius.org/

(平成 18 年 7 月 7 日受付)
(平成 19 年 1 月 9 日採録)

山井 成良（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．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，岡山大学総合情報処理センター（現，総合情報基盤センター）助教授を経て，現在同教授．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）．

岡山 聖彦（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．平成 6 年奈良先端科学技術大学院大学情報科学研究科助手．平成 10 年岡山大学工学部助手．平成 17 年同大学総合情報基盤センター助手．博士（工学）．インタネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

木澤 政雄（学生会員）

平成 17 年岡山大学工学部通信ネットワーク工学科卒業．平成 19 年同大学大学院自然科学研究科博士前期課程修了．同年株式会社日立製作所入社．インターネット運用技術等に興味を持つ．

土居 正行（学生会員）

平成 15 年津山工業高等専門学校情報工学科卒業．平成 17 年岡山大学工学部通信ネットワーク工学科卒業．平成 19 年同大学大学院自然科学研究科博士前期課程修了．同年株式会社 ACCESS 入社．オペレーティングシステム，分散システム等に興味を持つ．

河野 圭太（正会員）

平成 12 年大阪大学工学部電子情報エネルギー工学科卒業．平成 14 年同大学大学院工学研究科（情報システム工学専攻）修士課程修了．平成 16 年同大学院情報科学研究科（情報ネットワーク学専攻）博士課程修了．同年岡山大学総合情報基盤センター助手．モバイルネットワーク，分散システムの研究に従事．IEEE，電子情報通信学会各会員．博士（情報科学）．

大隅 淑弘（正会員）

昭和 58 年近畿大学理工学部電気工学科卒業．昭和 63 年静岡大学電子工学研究所技官．平成 4 年岡山大学総合情報基盤センター（現，総合情報基盤センター）技官．平成 10 年同技術専門職員．ネットワーク管理，ネットワークセキュリティの研究に従事．