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

2006－ＤＳＭ－41（17）
2006／5／12

部外者の利用を考慮した情報コンセントアクセス制御システム

木澤 政雄† 山井 成良†† 岡山 聖彦††
土居 正行† 河野 圭太†† 大隅 淑弘††

†† 岡山大学 総合情報基盤センター
〒700-8530 岡山市津島中3丁目1番1号
† 岡山大学 大学院自然科学研究科
〒700-8530 岡山市津島中3丁目1番1号
E-mail: †{kizawa,mdoi}@dist.cne.okayama-u.ac.jp, ††{yamai,okayama,keita,oosumi}@cc.okayama-u.ac.jp

あらまし 大学などの組織において情報コンセントシステムを運用する場合，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．そこで本稿では，アドレス変換の適用条件を工夫することにより既存の組織内限定サービスをそのままで部外者から保護できるような情報コンセントシステムを提案する．提案システムを試作して運用した結果，本システムは十分実用的であることが確認された．

キーワード 情報コンセント，セキュリティ，アクセス制御，利用者認証，アドレス変換

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

Masao KIZAWA†, Nariyoshi YAMAI††, Kiyohiko OKAYAMA††,
Masayuki DOI†, Keita KAWANO††, and Yoshihiro OOSUMI††

†† Information Technology Center, Okayama University
3-1-1, Tsushima-naka, Okayama, 700-8530, Japan
† Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Okayama, 700-8530, Japan
E-mail: †{kizawa,mdoi}@dist.cne.okayama-u.ac.jp, ††{yamai,okayama,keita,oosumi}@cc.okayama-u.ac.jp

Abstract 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 services restricted to insiders. In this paper, we propose a LAN access control system to protect restricted services from guest users, without modifying any existing servers by applying NAT function conditionally. According to a field testing, the proposed system has been confirmed to be effective and practical.

Key words LAN access contol system, security, access control, user authentication, network address translation

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．これに伴い，多くの組織では，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，あるいは学会等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，特に断らない限り，これらを代表して単に情報コンセントと表す）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事後に不正利用者を追跡したりするため，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す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，これまで多くの方法が提案されてきた [1]〜[4]．特に文献 [2] のシステムでは利用資格の有無によるアクセスの可否だけではなく，利用者毎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，たとえば大学において管理者，教員，学生，学外者などの身分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，サーバ側で組織内に限定したサービスを提供するために IP アドレスに基づいてアクセス制御を行っている場合，上記のような環境ではたとえアクセス可能な IP アドレスの範囲を設定したとしても様々な問題が生じる．すなわち，通常では情報コンセントの利用者からのアクセスでは送信元 IP アドレスとして組織内のグローバル IP アドレスが用いられるため，情報コンセントの利用者が実際には部外者であってもサーバ側ではこれを部外者によるアクセスと認識できずにアクセスを許可してしまうという問題が生じる．これを解決する方法の一つとして，たとえば岡山大学の一部の部局では独自に情報コンセント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ようにしているが，この方法では情報コンセント環境を提供する部屋に応じて専用ネットワークを構築しなおす必要があり，また ISP との契約に伴う金銭面での負担も無視できないなどの問題がある．

そこで本稿では，上記の問題の解決を図る情報コンセント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，情報コンセント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，従来の情報コンセント環境における部外者に対するアクセス制御の問題点について述べる．次に 3 章では，提案する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情報コンセント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. 従来の情報コンセント環境における問題点

前章で述べたように，組織内で部外者を含む利用者に情報コンセント環境を提供する場合，

（1） 組織内ネットワークをそのまま利用する方法

（2） 組織内ネットワークとは異なる専用ネットワークを準備し，組織内ネットワークとは別の ISP を利用してインターネット接続を提供する方法

の 2 つの方法が考えられる．このうち，(2) については情報コンセント環境は組織外ネットワークと同等であるため，アクセス制御機能上の問題は原理上生じない．しかし，この方法では情報コンセント環境を提供する部屋に専用ネットワークを敷設する必要があるため，開催イベントによって情報コンセント環境の提供場所が変わる場合にはネットワークの再構築が必要になり，管理者の負担が大きくなるという問題が生じる．また，専用ネットワークの構築には一般には多額の費用がかかるだけでなく，特に組織内ネットワークへのアクセスが ISP 経由で行われるため，通信速度や対故障性の面での問題も生じる．そこで以下では (1) について議論する．

2.1 部外者に対するアクセス制御における問題

多くの組織では，特に WWW における組織内限定情報の提供のように組織内の利用者に限定したサービスを提供しており，その提供方法としてクライアント側の IP アドレスに基づくアクセス制御がその簡便さからよく用いられている．ところが，上記 (1) のような情報コンセント環境では，部外者が組織内限定サービスにアクセスする際にサーバ側でのアクセス制御機能がうまく働かないという問題が生じる．以下では，この問題について詳細に述べる．

上記 (1) のような情報コンセント環境では，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，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，通常は組織内ネットワークとの接続点で NAT 機能が導入されており，利用者端末からサーバに送出されたパケットは NAT 機能により送信元 IP アドレスの部分がプライベートアドレスからグローバル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，サーバ側では同様に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 1 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情報コンセント環境を提供する場合，単純な方法では組織内に存在する全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ことになる．

2.2 従来のアクセス制御方法とその問題点

本稿で想定しているような環境においてサービス提供対象を限定する方法として，これまでに多くのアクセス制御方法が提案されている．これらは以下の 3 種類に分類することができる．

- 情報コンセント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

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．

2.2.1 情報コンセントシステムにおけるフィルタリング

1 章で述べたように，情報コンセントシステムには，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．

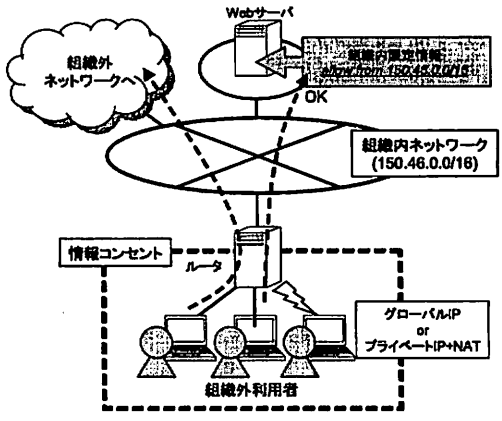

図 1 IP アドレスによるアクセス制御での問題点

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全てのサーバを情報コンセントシステムの管理者が予め把握しておく必要があり，管理者の負担が増大するという問題がある．また，特に 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部外者にも公開しているコンテンツにも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．

2.2.2 サーバ側での特定 IP アドレスからのアクセス拒否

情報コンセント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．

ところが，この方法では組織内限定サービスを提供する全てのサーバにおいてアクセス制御の設定変更が必要になり，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，利用者に権限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の権限に応じて切り替え，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．

2.2.3 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，情報コンセント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全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全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る点は改善されない．

3. 部外者の利用を考慮したアクセス制御

2 章で述べたように，組織内ネットワークを用いて情報コンセント環境を提供する場合，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，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．

もし，このアクセスにおいてたとえばプライベートアドレスなど各サーバが組織外として認識する IP アドレス（以下，組織外アドレス）が送信元アドレスとして用いられるのであれば，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も十分に機能すると思われる．但し，組織外との通信には組織外アドレスをそのまま用いることはできない．そこで本章では，部外者が組織内ネットワークにアクセスする場合には組織外アドレスを，それ以外の場合には組織内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アクセス制御方法を提案する．

以下では，提案方法の詳細について述べる．

3.1 対象となるネットワーク環境

まず，提案方法の適用対象となるネットワーク環境で満たすべき条件を挙げる．

- 接続用組織内（グローバル）IP アドレス

従来の情報コンセントシステムと同様に，提案方法でも情報コンセントシステムを組織内ネットワークに接続するためにグローバル IP アドレスが 1 つ必要である．このアドレスは静的に割り当てられる必要はなく，DHCP 環境等で動的に取得したものをそのまま用いても構わない．

- 利用者端末用組織外 IP アドレス

提案方法では，情報コンセントに接続する利用者端末には組織外 IP アドレスを割り当てる．このアドレスには通常はプライベート IP アドレスの利用が適していると思われるが，たとえば全てのプライベート 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 [6] を利用しても構わない．必要なアドレス数は端末数によるが，通常では/24 のネットワークが 1 つ利用できれば十分であると思われる．なお，複数の情報コンセントシステムを同時に運用する場合には，各システムについて異なるアドレスを割り当てる必要がある．

- 組織内ネットワークでの経路制御

提案方法では，管理の省力化を図るため RIP [7] 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ことが望ましい．この場合，上記の利用者端末用組織外 IP アドレスに対する経路情報を情報コンセントシステムから組織内ネットワーク全体に広告できるように予め設定しておく必要がある．

これらの条件は多くのネットワーク環境で容易に満足することが可能であり，提案方法は幅広いネットワーク環境に適用可能であるといえる．

3.2 システム構成

提案する情報コンセントシステムは，図 2 に示すように，通常の情報コンセントシステムで用いられる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 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，情報コンセント側で用いられる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．また，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も必要である．

なお，図 2 では NAT ルータとアクセス制御装置が異なる構成要素として示されているが，1 つの装置が両方の機能を持つような構成であっても構わない．

3.3 システムの動作手順

次に提案する情報コンセント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

情報コンセント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情報コンセント側の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，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．

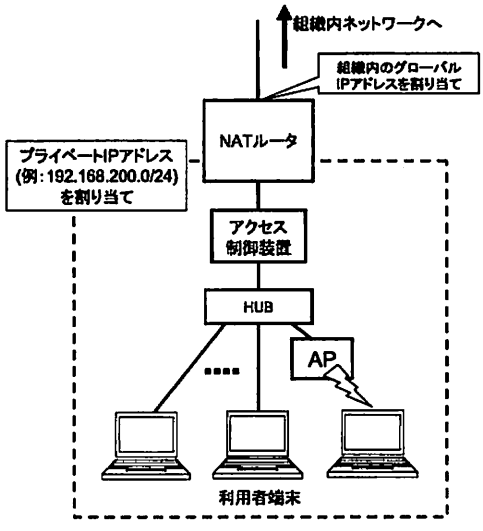

図 2 情報コンセントシステムの構成

（2） 利用者端末への IP アドレス割当て

情報コンセントに接続されると，利用者端末は DHCP 等の動的 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 IP アドレスを割り当てる．

（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認証した利用者が部外者かどうかを判別し，その結果を利用者端末の識別子（IP アドレスや MAC アドレスなど）とともに NAT ルータに通知する．

（4） アドレス変換

NAT ルータでは，手順 (3) において組織内利用者と判別された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通常のアドレス変換を行う．一方，手順 (3) において組織内利用者と判別された利用者端末に関するパケットは，通信相手に応じて以下のように処理する．

- 通信相手が組織内である場合

この場合には，NAT ルータは当該端末に関するパケットに対してはアドレス変換を行わない．

- 通信相手が組織外である場合

この場合には，NAT ルータは当該端末に関するパケットに対してアドレス変換を行う．

（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，組織内利用者用と部外者用の 2 種類の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) における認証結果の NAT ルータへの通知を省略できる．この場合，NAT ルータでは予め部外者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，部外者が情報コンセントシステムを利用した場合の提案方法の動作手順を図 3 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 アドレスはグローバルアドレスである 150.46.xx.yy，情報コンセント側 IP アドレスは 192.168.200.1 が割り当てられている．組織内には情報コンセント用アドレスとして 192.168.200.0/24 への経路が広告されており，このアドレスは組織内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，部外者である利用者 A，B がそれぞれ端末を情報コンセントシステムに接続し，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

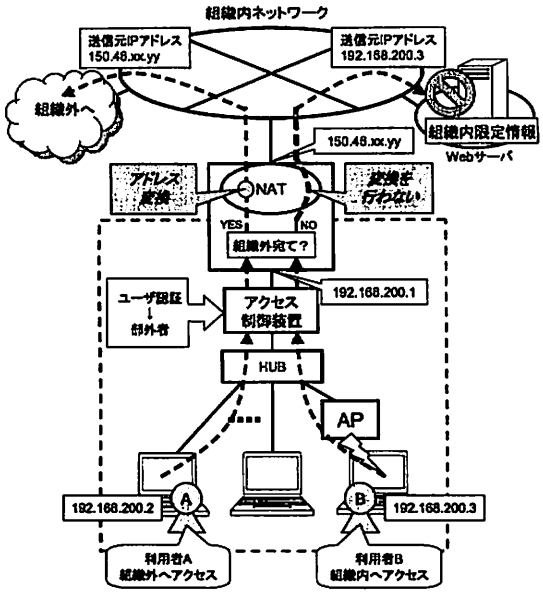

図 3　部外者が利用した場合の動作例

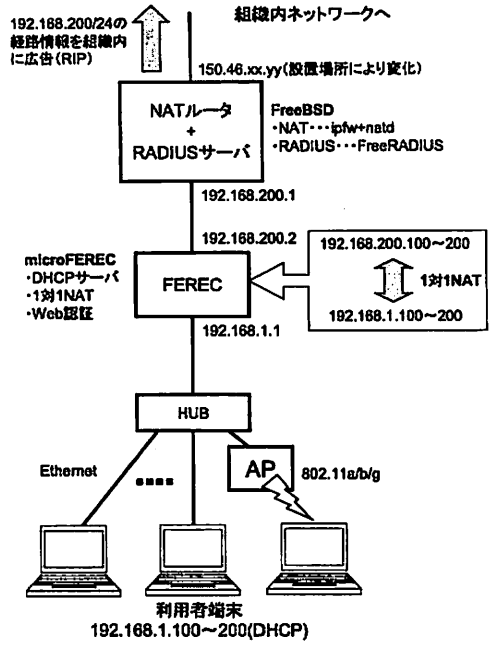

図 4　試作システムの構成

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 192.168.200.2 から 150.46.xx.yy 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 192.168.200.3 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．

この例のように，提案方法は部外者に対して，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である．

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 4 に示す．なお，試作システムでは組織内利用者と部外者の識別は未実装であり，全ての利用者を部外者として扱った．

以下では，試作システムの実装の詳細について述べる．

4.1 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 [8] を用いた．microFEREC の利用者は，有線（イーサネット）もしくは無線 (802.11a/b/g) でネットワークに接続し，microFEREC が提供する Web 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 名とし，情報コンセント用 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．しかし，この NAT 機能では前章で述べたような条件付のアドレス変換を行うことができなかったため，図 4 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，microFEREC では多対 1 もしくは 1 対 1 のアドレス変換のうちのどちらかが必ず作動するものであったため，止むを得ず 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．この設定により，192.168.1.xx は 192.168.200.xx に変換されるが，変換後のアドレスも組織外のアドレスとして認識されるものである．

4.2 NAT ルータ

試作システムでは，FreeBSD が稼動する計算機を用いて NAT ルータを実装した．FreeBSD 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 [9] を利用し，3.3 節で述べたようなアドレス変換を行う．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 5 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 は利用者端末の IP アド

```
divert natd ip from 192.168.200.0/24 to not 150.46.0.0/16
divert natd ip from not 150.46.0.0/16 to 150.46.xx.yy
```

図 5　NAT ルータにおける ipfw ルール

```
allow ip from 192.168.200.2 to me
allow ip from me to 192.168.200.2
```

図 6　利用者認証のための ipfw ルールの追加

レス，150.46.0.0/16 は岡山大学で使われるグローバルアドレス，150.46.xx.yy は NAT ルータの学外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 5 の 1 行目は，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，2 行目は学外から 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．

また，NAT ルータは情報コンセント用アドレス (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，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 メッセージを広告するように設置した．

4.3　RADIUS サーバの設置

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，RADIUS サーバ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 [10] を NAT ルータ上に動作させ，microFEREC から参照できるようにした．その際，図 5 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，図 5 のルールの前に図 6 に示す 2 行を追加することにより，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．

以上の構成および設定により，情報コンセントシステムを試作し，岡山大学ネットワークに接続したところ，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，WWW で提供される学内限定情報にアクセスできないことを確認した．これにより試作システムは意図したとおり機能することが確認できた．

5.　運 用 事 例

試作システムは，2005 年 8 月に岡山大学にて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．

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，情報コンセントサービスを提供したところ，3 日間の開催期間中に約 200 名の参加者が情報コンセントを利用した．試作システムでは最大同時利用者数は 4.1 節で述べたように 100 名としたが，実際の同時利用者数は最大でも 20 人程度であった．

サービス初日において，参加者全員がアクセスが出来ないという不具合が発生した．原因を調査したところ，ある利用者の端末がウイルスに感染しており，パケットを大量に送信していたことが判明したため，これが障害の原因と思われる．これ以外には目立った接続障害も無くサービスが運用でき，また性能上や機能上の問題も発生しなかったため，試作システムは十分実用に耐えうるといえる．

6.　ま と め

本稿では，組織内利用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情報コンセントシステムを提案した．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，情報コンセント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，試作システムでは未実装となっている，組織内利用者と部外者を識別してアドレス変換の適否を決定する機能の実装が挙げられる．

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．

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と用いた有線/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] K. Egevang, P. Francis: The IP Network Address Translator (NAT), RFC1631, IETF, 1994.

[6] IANA: Internet protocol v4 address space, http://www.iana.org/assignments/ipv4-address-space, 2006.

[7] G. Malkin: RIP Version 2, RFC2453, IETF, 1998.

[8] 株式会社ネットスプリング: FEREC, http://www.ferec.jp/, 2006.

[9] Archie Cobbs, Charles Mott, Ari Suutari, Dru Nelson, Brian Somers, Ruslan Ermilov: “natd - Network Address Translation daemon”, FreeBSD System Manager's Manual, 2003.

[10] The FreeRADIUS Project: FreeRADIUS - building the perfect RADIUS server, http://www.freeradius.org/, 2004.