情報処理学会論文誌 Vol.56 No.3 788–797 (Mar. 2015)

同一サブネットにおいて利用者の位置情報を判別可能なロケーションフリーネットワークシステム

大隅 淑弘[1,a)] 山井 成良[2,b)] 岡山 聖彦[1,c)]

受付日 2014年6月24日, 採録日 2014年12月3日

概要：ネットワーク装置の認証機能によって，組織内でロケーションフリーネットワークシステムを構成することができるようになった．利用者は，ロケーションフリーネットワークのどこからでも自分のネットワークに接続することができる．しかし，その反面，利用者の現在位置が判別できなくなることが問題になる場合があった．これに対して VLAN-ID とサブネット IP アドレスの組合せを，位置情報を区別する場所によって変更する構成方法が提案されている．しかし，この場合には，利用者が位置情報が異なる場所に移動すると，端末が同一サブネットに接続されないという問題があった．そこで，本研究では，利用者がどこに移動しても同一ブロードキャストドメインにおけるサブネットに接続することが可能であり，端末の送信元 IP アドレスから利用者の位置情報を判別できるロケーションフリーネットワークシステムを提案する．本提案手法は，NAT ルータや DHCP サーバを動的に設定することによって構成する．本提案に基づいて試作したシステムを評価し，有効に機能することを確認した．

キーワード：ロケーションフリーネットワーク，認証，VLAN，NAT，DHCP

A Location Free Network System Which Can Be Identified the Location of the User in the Same Subnet

Yoshihiro Ohsumi[1,a)] Nariyoshi Yamai[2,b)] Kiyohiko Okayama[1,c)]

Received: June 24, 2014, Accepted: December 3, 2014

Abstract: Recently, by the authentication function of a network device, it became possible to configure a location free network system in an organization, the user of the organization can connect his/her terminal to their own network anywhere. However, in some cases, it become a problem when the user's current location cannot be distinguished. So, a configuration method that changes relation of the subnet IP address and VLAN-IDs at each site has been proposed. But, when a user moves the site, his/her terminal is not connected to the same subnet. In this paper, we propose a location free network system that the user is possible to connect to the same subnet and is identified the location from a source IP address of the terminal by configuring a NAT router and a DHCP server dynamically, even if the user moves the site. We confirmed the effectiveness by evaluating the prototype system.

Keywords: location free network, authentication, VLAN, NAT, DHCP

1. はじめに

近年，ネットワーク機器の高機能化により，端末をネットワークに接続するときに利用者あるいは端末を認証することができるようになった（以下，認証ネットワークとする）．このようなネットワークでは，利用者や端末を認証し，その属性に応じて VLAN の割当てが可能なため，利

[1] 岡山大学
Okayama University, Okayama 700–8530, Japan
[2] 東京農工大学
Tokyo University of Agriculture and Technology, Koganei, Tokyo 184–8588, Japan
[a)] oosumi@cc.okayama-u.ac.jp
[b)] nyamai@cc.tuat.ac.jp
[c)] okayama@cc.okayama-u.ac.jp

用者は認証ネットワークの範囲内であればどこでも同じサブネットに接続できるサービスを利用することができる（以下，ロケーションフリーネットワークとする）．しかし，利用者が組織内のどこからでも同じサブネットに接続できると問題が生じる場合がある．たとえば，大学が契約している電子ジャーナルのサイトライセンスでは，電子ジャーナルによって閲覧が許可されているキャンパスや部局が異なるため，利用者の現在位置が判別できないと，利用者の正当性を保証することができないことがある．岡山大学では，約 6,800 の電子ジャーナルを契約しているが，“American Journal of Physiology” [1] や “Journal of biological chemistry” [2] などの約 500 については，学内の一部のキャンパスからのみ閲覧が許可されている．

この問題に対して文献 [3] が提案されている．これは，ロケーションフリーネットワークにおいて，位置情報を区別する場所が異なるとサブネット IP アドレスが変更されるようにネットワークを構成する．この構成方法では，利用者の現在位置が端末の IP アドレスから判別できるため，利用者の正当性を保証することができる．しかし，この場合，端末が接続されるサブネット IP アドレスが，位置情報を区別する場所によって異なるため，利用者が位置情報の異なる場所に移動すると，同一ブロードキャストドメインにおけるサブネットへの接続が保証されないという新たな問題が生じる．

そこで，ロケーションフリーネットワークシステムの新たな構成方法として，利用者に対して同一ブロードキャストドメインにおけるサブネットへの接続を保証しながらも，サブネットを越えて情報資源にアクセスする場合には，そのサーバでは，端末の送信元 IP アドレスにより利用者の場所を識別できるネットワークの構成方法を提案する．利用者は，前述のような組織の一部の場所について契約している電子ジャーナルのサイトライセンスを利用し，さらに自分のサブネット内だけで情報資源の共有を許可するような場合にも，ロケーションフリーネットワークの利用が可能になる．また，判別する情報は，位置情報だけでなく，個人の身分や様々な属性に対しても適用することができる．

以下，2 章ではロケーションフリーネットワークとその問題点について説明する．3 章では提案するロケーションフリーネットワークシステムの構成方法について述べ，4 章では提案に基づいて実装した試作システムについて説明する．最後に，5 章でまとめと今後の課題について述べる．

2. ロケーションフリーネットワークにおける問題点

2.1 認証ネットワーク

端末をネットワークに接続するときに，利用者や端末を認証することができるネットワークシステムが普及している．認証は，一般には L2 スイッチであるエッジスイッチで行うが，上位のディストリビューションスイッチや L3 スイッチで行う場合もある．認証によって不正な利用者を排除することのほかにも，利用者や端末を識別し，その属性に基づいて動的に VLAN を割り当てることができる（以下，ダイナミック VLAN とする）．認証方法は，EAP（Extended authentication protocol）[4] を用いて認証を行う IEEE802.1X 認証 [5]，端末の MAC（Media Access Control address）アドレスで認証する MAC アドレス認証，利用者のユーザアカウントで認証する WEB 認証などが普及している．また，複数の認証方法を用いるマルチステップ認証なども利用できる．認証サーバには一般に RADIUS [6] サーバが用いられるが，LDAP [7] サーバで認証情報を運用し，RADIUS サーバがそれを参照する方法も用いられる．

2.2 ロケーションフリーネットワークシステム

認証ネットワークによるダイナミック VLAN を利用することによって，利用者は認証ネットワークの範囲であれば，どこでネットワークに接続しても，認証に成功すれば自分が所属するネットワークに接続することができる．所属するネットワークの情報は，VLAN-ID を端末の MAC アドレスやユーザアカウントに対する属性値として割り当てる．

2.3 ロケーションフリーネットワークの問題点

前述のとおり，ロケーションフリーネットワークによって，利用者は組織内のどこでも同じサブネットに接続できるが，組織の特定の場所だけで利用できるサイトライセンスを契約している場合などには，それがライセンス違反になる場合がある．従来のネットワークでは，端末に割り当てられる IP アドレスは，場所や建物などの地理的な位置条件によって決められていたため，その端末の IP アドレスを確認すれば利用者の位置を判別することが可能であった．しかし，ロケーションフリーネットワークでは，端末の IP アドレスが地理的な位置条件に基づかないため，利用者の位置を判別できなくなる．

文献 [3] では，ロケーションフリーネットワークによって，利用者は組織内のどこからネットワークに接続しても同じ VLAN に接続できるが，位置情報を区別する場所ごとに VLAN-ID とサブネット IP アドレスの関係を変更する．これにより，利用者の現在位置が異なると，端末が接続されるサブネットが変更される．この構成方法では，利用者が現在ネットワークに接続している場所が端末の IP アドレスから判別可能なため，利用可能な場所を制限したサイトライセンスを利用する場合にも，利用者の正当性を保証することができる．サイトライセンスによって契約している電子ジャーナルへのアクセスの例を**図 1** に示す．

しかしながら，この構成方法では利用者が，位置情報を

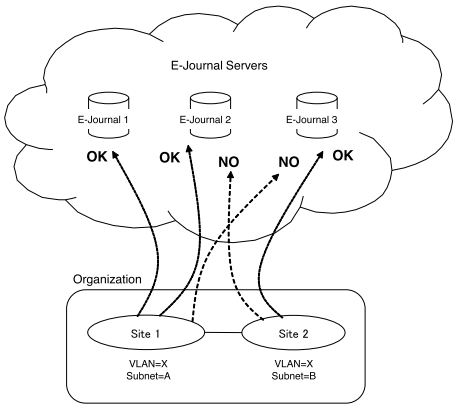


図 1 電子ジャーナルへのアクセス
Fig. 1 Access to electronic journals.

区別している他の場所に移動すると，端末が同じサブネットに接続されないという問題がある．すなわち，利用者はどこでも同じ VLAN-ID に接続されるが，利用者が他の場所に移動すると端末が接続されるサブネットが異なるため，同一ブロードキャストドメインにおけるサブネット内での接続性が保証されない．このような場合，たとえば，利用者が日頃接続しているサブネットに NAS やプリンタなどがあり，そのサブネット内の端末についてのみアクセス許可をしている場合，利用者が位置情報を区別している他の場所に移動すると，これらの資源へのアクセスができなくなる．

3. 同一サブネット内の接続を保証するロケーションフリーネットワークシステム

前章で述べたように，従来のロケーションフリーネットワークシステムの構成方法は，同一ブロードキャストドメインにおけるサブネット内での接続性が保証されないという問題があった．そこで，本論文では，ロケーションフリーネットワークシステムの新たな構成方法として，同一ブロードキャストドメインにおけるサブネットへの接続を保証しながらも，サブネットを越えて通信する場合には，端末の送信元 IP アドレスにより利用者の位置情報を識別できるネットワーク構成方法を提案する．また，利用者の位置情報を認証ネットワークから取得する．

3.1 提案する構成方法の概要

従来の問題の原因は，利用者の現在位置を判別するために，位置情報を区別している場所ごとにサブネット IP アドレスを変更していることにある．そこで，利用者の端末が接続するサブネット IP アドレスをどの場所でも変更することなく，また，同一サブネット内の端末について，そのサブネットの外側で識別される端末の送信元 IP アドレスを変更する構成方法を提案する．NAT（Network Address Translation）[8] ルータや DHCP（Dynamic Host Configuration Protocol）[9] サーバの動作を，利用者の現在位置によってダイナミックに変更することにより構成する．すなわち，利用者の位置情報によって，NAT によるアドレス変換後の IP アドレスが変更されるため，サービスを提供するサーバなどでは，送信元の IP アドレスから利用者の現在位置を判別することができる．利用者はどこでも自分のサブネットに接続することができ，また，組織の一部の場所について契約しているサイトライセンスを利用する場合にも，正当性を保証することができる．判別する情報は，位置情報だけでなく，個人の身分や様々な属性に対しても適用することができる．本論文では，主に IPv4 のネットワークを想定しているが，IPv6 のネットワークにおいても，認証ネットワークで NAT を運用する場合には利用が可能である．なお，NAT については，NAPT（Network Address Port Translation）[10] でも同様に動作可能であるため，以下，NAT と NAPT を含めて NAT と記述する

3.2 利用者の現在の位置情報の取得

利用者の現在の位置情報をネットワークから取得する方法としては，国や地域などの広い範囲で適用できるものとして，Whois データベース [11] の情報や GeoIP ロケーションサービス [12] を利用する方法，Ping や Traceroute の応答から位置情報を推測する方法などが知られている．一方，組織内などの限られた範囲でも利用可能な方法が文献 [13] に示されている．DNS（Domain Name System）[14] サービスを拡張し，DNS レコードを郵便番号のような階層的な位置情報として利用する．利用するためには，位置情報を表す DNS レコードを構成して DNS サーバを運用する必要がある．そのほかにも携帯電話やスマートフォンなどの GPS（Global Positioning System）から情報を取得することも可能であるが，いつでもどこでもすべての利用者がそれを持っているとは限らない．利用者自身が何らかの方法で位置情報を認識することも考えられるが，必ずしも正しい情報とは限らない．さらに，情報を入力するシステムも必要となる．このように従来の位置情報の取得方法では，広域での利用を想定したものや，特別なシステムが必要となる．

3.2.1 認証ネットワークからの位置情報の取得

認証ネットワークでは，利用者の端末の位置情報を認証スイッチから取得することができる．ロケーションフリーネットワークシステムなどの認証ネットワークでは，端末がネットワークに接続されると認証スイッチが認証サーバに対し，利用者のアカウント情報や端末の MAC アドレスを認証情報として問い合わせる．通常では端末が接続される認証スイッチは，その端末と比較的近い場所にある．たとえば同じ建物内とか，同じ建物の同じ階などである．すなわち，利用者の現在の場所は，後述する無線 LAN のような状況を除いて，認証スイッチが設置されている場所の

付近と見なすことができる．認証サーバでは，認証要求をした認証スイッチの IP アドレスと端末の MAC アドレスが確認できるため，この情報を参照すれば認証要求をした認証スイッチの IP アドレスから利用者の位置情報を取得することができる．

位置情報の精度については，区別する位置情報が隣接していない場合，たとえば大学ではキャンパス，企業では事業所などのような場合には誤差は生じない．しかし，無線 LAN を利用しており，位置情報を区別する場所が非常に近い場合には，端末が他の認証スイッチに接続された無線 AP（Acccess Point）に接続されていると，正しく位置情報が取得できないことがある．このような状況では，隣接した建物，上下フロアでの識別には誤差を生じる．この場合には，無線 AP の設置状況を考慮して利用する必要があるが，次のような対策方法が考えられる．1 つには，位置情報が異なる場所の無線 AP では SSID（Service Set Identifier）を変更することで，端末を他の場所の無線 AP に接続しないようにする．他には，無線 LAN の BSSID（Basic Service Set Identifier）情報や受信電波強度分布から位置推定をする研究 [15] があり，このような技法を適用することも考えられる．無線 LAN を利用していない場合には，認証スイッチの FDB（Forwarding DataBase）も利用すれば，情報コンセント単位での位置情報を識別可能である．

3.3 利用者の位置情報に基づいた IP アドレスの変更

端末の送信元 IP アドレスを，NAT ルータや DHCP サーバによって変更するためには，次の方法を用いることができる．

(1) NAT ルールを変更する方法
　以下，この方法を DNC（Dynamic NAT Configuration）とする．
(2) NAT ルールに基づいて，DHCP サーバによる IP アドレスリースを変更する方法
　以下，この方法を DAL（Dynamic IP Address Lease）とする．
(3) ゲートウェイ IP アドレスを変更する方法
　以下，この方法を DGL（Dynamic Gateway IP Address Lease）とする．
(4) ネクストホップを変更する方法
　以下，この方法を DRC（Dynamic Routing Configuration）とする．

認証が成功したときに利用者の位置情報を基に，ネットワーク装置や端末に対して動的な設定を行う．認証方法は MAC アドレス認証，WEB 認証，IEEE802.1X 認証のどの方式にも適用できる．

3.3.1 利用者の位置情報と端末情報の取得

まず初めに，利用者の位置情報と端末情報の取得について説明する．3.2.1 項のとおり，利用者が接続している認証スイッチの IP アドレスからは利用者の位置情報が得られるため，認証スイッチの IP アドレスと端末の関係を位置情報として利用する．一方でロケーションフリーネットワークでは，通常，認証スイッチにおいて認証が成功すると，端末は割り当てられた VLAN のサブネットに接続され，DHCP サーバから IP アドレスがリースされる．この IP アドレスのリース情報を参照し，端末情報として利用する．

次に提案する構成方法の動作や特徴について述べる．

3.3.2 NAT ルールの動的な変更

3.3 節の DNC による構成である．利用者の位置情報に基づいて NAT ルールを動的に変更して設定する．すなわち，端末にリースされた IP アドレスが，区別する位置情報に基づいた NAT 変換後の IP アドレスに変換されるように，NAT ルールを動的に設定する．処理の流れを以下に示す．

(1) 端末がネットワークに接続され認証が成功する．
　認証情報から利用者の位置情報を取得する．
(2) DHCP サーバが IP アドレスをリースする．
　IP アドレスリース情報から端末情報を取得する．
(3) 端末情報と位置情報を参照し，リースされた IP アドレスによる NAT ルールを NAT ルータに設定する．
(4) 位置情報に基づく NAT 変換後の IP アドレスによって外部との通信が開始される．

この構成方法の特徴としては，RADIUS サーバ，DHCP サーバは通常の機能のものが利用できるが，NAT ルータは NAT ルールを動的に変更して設定する必要がある．また，接続端末数に応じた数の NAT ルールを設定する必要がある．端末が接続されるサブネットの IP アドレス数は，区別する位置情報の数で分割されるが，NAT 変換前 IP アドレスの範囲内であればどの IP アドレスでも利用可能であり，柔軟な IP アドレスの運用が可能である．端末が接続されるサブネットは，複数のサブネットによって構成することも可能である．NAT ルータのルール設定によって，端末の位置情報を変更するため，組織のネットワーク構成に柔軟に対応できる．NAT ルータで設定可能な NAT ルールの最大数や処理能力を考慮して，システムを設計する必要がある．NAT ルータの性能により，小規模から大規模なネットワークでの運用が可能である．動作の手順を**図 2** に示す．

3.3.3 IP アドレスリースの動的な変更

3.3 節の DAL による構成である．DHCP サーバが，利用者の位置情報に基づく NAT ルールに適合するように，端末の IP アドレスを動的に変更してリースする．すなわち，NAT 変換後の IP アドレスが，区別する位置情報によって異なるような NAT ルールを NAT ルータに静的に設定しておく．DHCP サーバが利用者の位置情報に基づく NAT 変換前の IP アドレスを動的にリースする．処理の流れを以下に示す．

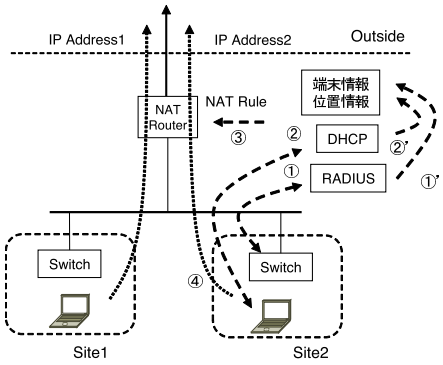


図 2 DNC による NAT ルールの動的な変更
Fig. 2 Dynamic NAT configuration.

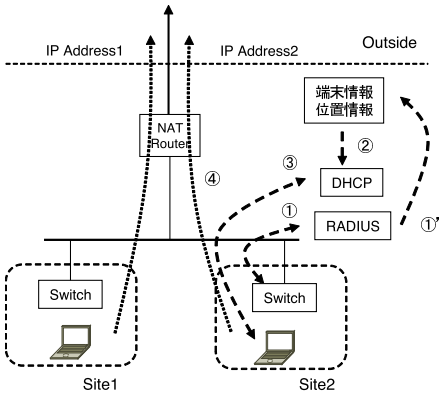


図 3 DAL による IP アドレスリースの動的な変更
Fig. 3 Dynamic IP address lease.

(1) 端末がネットワークに接続され認証が成功する．位置情報を取得する．
(2) DHCP サーバが位置情報を参照する．
(3) DHCP サーバが NAT ルールに対応した IP アドレスをリースする．
(4) 位置情報に基づく NAT 変換後の IP アドレスによって外部との通信が開始される．

この構成方法の特徴は，NAT ルータは通常の機能で利用できるが，DHCP サーバは NAT ルールに基づいた IP アドレスを動的にリースする必要がある．端末にリースする IP アドレスは，区別する位置情報の数に基づいて割り当てる範囲を固定的に分割しておく必要があるが，端末台数が多い場合にもサブネットのネットマスクを調整することで対応が可能である．NAPT を利用する場合においては，接続する端末の最大数が NAT ルータの NAT ルール設定可能最大行数の影響を受けにくいという利点がある．DNC と同様に NAT ルータのルール設定によって，端末の位置情報を変更するため，組織のネットワーク構成に柔軟に対応できる．小規模から大規模なネットワークでの運用が可能である．動作の手順を図 **3** に示す．

3.3.4 ゲートウェイ IP アドレスリースの動的な変更

3.3 節の DGL による構成である．利用者の端末が，位置情報に基づいて決定された NAT ルータを経由して通信

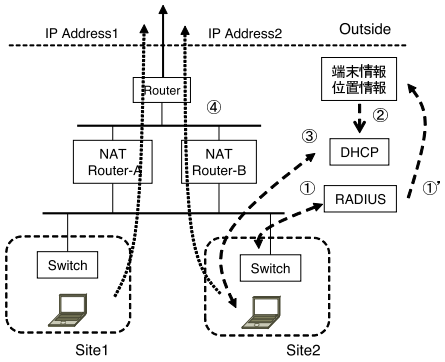


図 4 DGL1 によるゲートウェイ IP アドレスの変更
Fig. 4 Dynamic gateway IP address lease by DGL1.

するように，端末のゲートウェイ IP アドレスを動的に変更する．すなわち，DHCP サーバが端末に通知するゲートウェイ IP アドレスを，区別する位置情報によって動的に変更する．そのゲートウェイ IP アドレスに対応した NAT ルータにより NAT 変換後の IP アドレスを変更する．処理の流れは，DAL と同様であるが，(3) の処理において端末の IP アドレスをリースするとともに，位置情報に基づいたゲートウェイ IP アドレスを通知する．DHCP サーバがリースする端末の IP アドレスは，位置情報によって変更する必要はない．この構成を実装するには 2 つの方法がある．

- ゲートウェイ IP アドレスの変更
  1 つの方法は位置情報を区別するサブネットに，区別する数の NAT ルータを運用し，各 NAT ルータでは NAT 変換後の IP アドレスをそれぞれで変更しておく方法である．以下，この方法を DGL1 とする．DHCP サーバでは，端末からの IP アドレス取得要求に対し，位置情報に対応した NAT ルータの IP アドレスをゲートウェイ IP アドレスとして割り当てる．NAT ルータを多段運用することも可能である．この構成方法の特徴は，DHCP サーバはルールに基づいたゲートウェイ IP アドレスを動的に割り当てること，区別する位置情報の数に応じた NAT ルータを運用することがあげられる．1 つのサブネットに対して複数の NAT ルータを動作させる必要があるため，組織が比較的小さな規模でネットワークを構成している場合に適している．動作の手順を図 **4** に示す．
- マルチホームでのゲートウェイ IP アドレスの変更
  もう 1 つの方法は，組織がマルチホームの環境であり，利用者の位置情報を，インターネット接続の ISP (Internet Service Provider) から割り当てられた IP アドレスによって判別することが可能な場合である．以下，この方法を DGL2 とする．DHCP サーバが割り当てるゲートウェイ IP アドレスとして位置情報に対応した ISP の NAT ルータを割り当てる．この方法では区別できる位置情報の数がマルチホームの数に制限さ

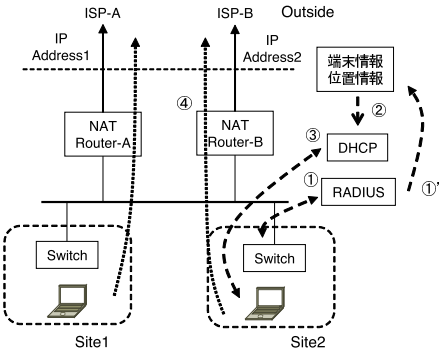


図 5 DGL2 によるマルチホームでのゲートウェイ IP アドレスの変更
Fig. 5 Dynamic gateway IP address lease by DGL2.

れる．こちらも組織が比較的小さな規模でネットワークを構成している場合に適している．この動作の手順を図 5 に示す．

3.3.5 ネクストホップの動的な変更

3.3 節の DRC による構成である．ルータで PBR（Policy-Based Routing）を用いることで，パケットを位置情報に基づいた NAT ルータにルーティングする．動作には 2 つの方法がある．1 つは端末に割り当てられた IP アドレスによってルートマップを動的に設定する方法と，もう 1 つは固定的に設定されたルートマップに基づいて DHCP がリースする IP アドレスを動的に変更する方法である．また，ネットワークの物理的な構成は，区別する数の NAT ルータを運用する方法と，マルチホームによる方法がある．区別できる位置情報の数は，NAT ルータの数やマルチホームの数に制限される．また，ルータには接続する端末数のルートマップを動的に設定することが必要である．ポリシベースルーティングにより，比較的柔軟にネットワークを構成できるため，小規模から中規模のネットワークに適している．この動作の手順を図 6 に示す．

3.4 システムの応用に関する考察

本論文では，サイトライセンスを例にして，利用者の位置情報を判別可能なロケーションフリーネットワークシステムの構成方法を提案した．しかし，判別する情報は位置情報だけでなく，利用者や端末の様々な属性を用いることができる．たとえば，その人の性別，身分，職権，所属，嗜好，端末の特性，等々を対応する IP アドレスと関連付けておくことが考えられる．アクセス制御をする場合には，クライアントの送信元 IP アドレスによってネットワーク機器のポリシを設定すればよく，シンプルなシステムの運用が可能である．

4. 試作システムの実装と評価

4.1 試作システムの実装

提案するシステムを評価するため，試作システムを構成

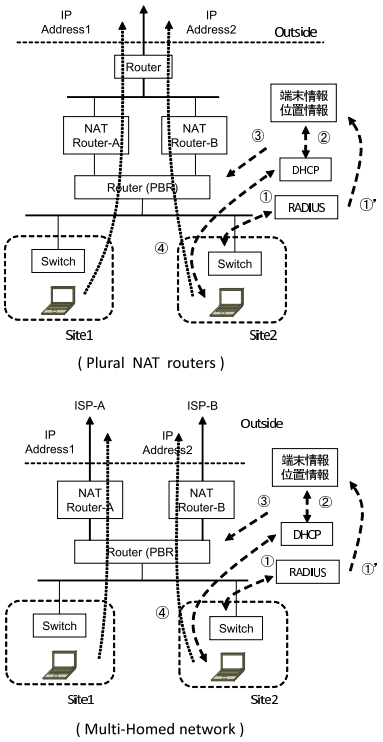


図 6 DRC によるネクストホップの動的な変更
Fig. 6 Dynamic Routing Configuration.

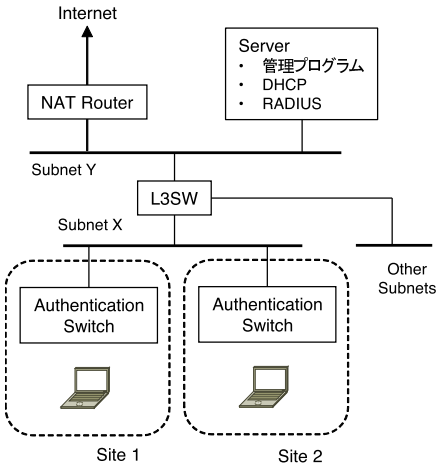


図 7 試作システム
Fig. 7 Prototype system.

した．システムの接続構成を図 7 に，機器構成を表 1 に示す．

サーバでは 1 台の Linux サーバに DHCP サーバ，RADIUS サーバ，後述する管理プログラムを運用した．RADIUS サーバは Free RADIUS2 [20] である．DHCP サーバは，通常機能で運用する場合には ISC DHCP [21] を使用したが，DAL や DGL による場合には，試作 DHCP サーバを使用した．

4.2 管理プログラムの実装

提案するシステムでは，利用者の位置情報と端末情報を取得し，ネットワーク機器に対して位置情報に基づく設定

表 1 システムの機器構成
Table 1 Specifications of the prototype system.

	機器構成
NAT Router	NEC Corporation UNIVERGE IX2025 [16] （IPv4 転送性能 200 Mbps NAPT 最大エントリ 65,535 静的 NAT 最大設定数 256 行）
Server	CPU Celeron D 325（2.53 GHz） Memory 1 GB CentOS-5.10 32 bit [17]
Layer3 Switch	Cisco Systems, Inc. WS-C3750G-24TS-E [18]
Authentication Switch	Allied Telesis K.K. CentreCOM GS908M V2 [19]
Personal Computer	Microsoft Windows 7 Core i3 2.3 GHz Memory 4 GB

を動的に行う必要がある．そこで，試作システムでは，管理プログラム，NAT ルータ設定プログラム，試作 DHCP サーバを使用した．これらのプログラムは Perl [22] で作成した．

4.2.1 位置情報管理プログラム

利用者の位置情報を取得して管理する．RADIUS サーバの radius.log を “tail -f -n0’ で監視し，端末の MAC アドレスと認証スイッチの IP アドレスの関係を位置情報データベースとして運用する．データベースシステムは GDBM [23] を使用した．

4.2.2 NAT ルータ設定プログラム

DNC で使用するプログラムであり，利用者の位置情報に基づいた NAT ルールを動的に設定する．DHCP サーバの dhcpd.leases を “tail -f -n0” で監視し，IP アドレスがリースされた直後に，端末の MAC アドレスをキーに位置情報データベースを参照して，位置情報に基づく NAT ルールを NAT ルータに設定する．プログラムを起動すると NAT ルータに Telnet 接続を行い，セッションを維持して各端末の NAT ルール設定を行う．NAT ルータへの接続は Perl の Net::Telnet モジュールを使用した．

4.2.3 試作 DHCP サーバ

DAL および DGL で使用するプログラムであり，利用者の位置情報に基づいたアドレス情報を端末に動的にリースする．IP アドレスをリースする直前に，端末の MAC アドレスをキーに位置情報データベースを参照し，位置情報に基づく NAT ルールに対応した IP アドレスやゲートウェイ IP アドレスを端末にリースする．なお，端末から意図しない DHCP REQUEST を受けた場合には DHCP NAK を送り，DHCP DISCOVER から処理を行う．

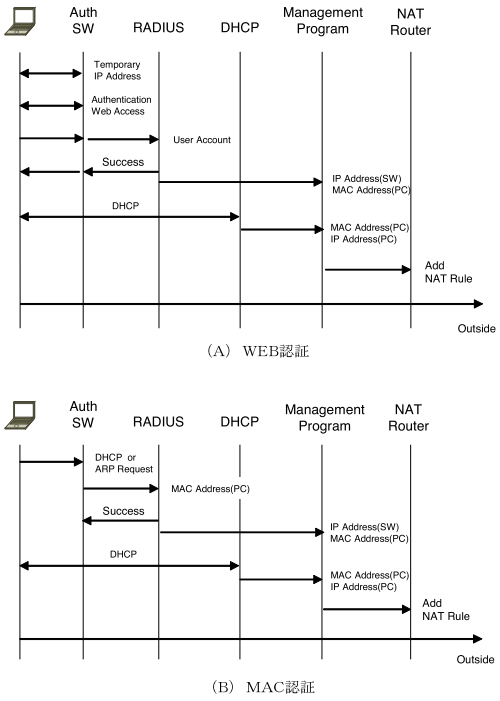


図 8 DNC による動作手順
Fig. 8 Procedure of operation by DNC.

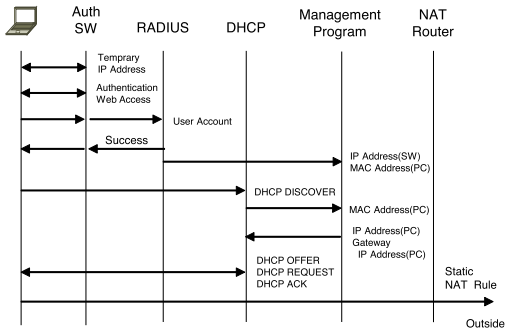
4.3 試作システムの動作試験

4.3.1 動作確認試験

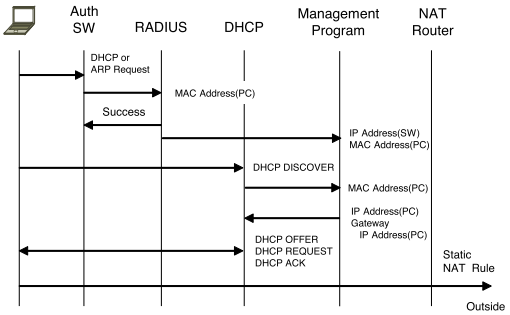
試作システムにおいて，認証スイッチをマルチプルダイナミック VLAN モードで動作させ，WEB 認証，MAC 認証で動作試験を行った．RADIUS サーバには，認証情報としてユーザ名とパスワードおよび VLAN-ID が 10,000 件，MAC アドレスと VLAN-ID が 10,000 件の合計 20,000 件が登録されている．また，位置情報データベースには，10,000 件の端末が登録されている．一般の利用環境においては NAPT が利用されることが多いため，NAT ルータでは NAPT によるアドレス変換を行った．

この環境において，DNC，DAL により通信試験を行った．それぞれの場所の端末について，NAT ルータの外側では位置情報に対応した IP アドレスに変換されて通信が行われることを確認した．また，DGL においては，それぞれの場所の端末について，位置情報に対応したゲートウェイ IP アドレスが割り当てられて通信が行われることを確認した．DRC については位置情報に対応したルートマップにより，ネクストホップが変更されることを確認した．以上より，提案するシステムが設計どおりに動作することが確認された．

動作手順について，DNC のものを**図 8** に，DAL，DGL のものを**図 9** に示す．DRC については，図 8 において，NAT ルールを設定する動作をルータのルートマップを設定する動作に置き換えたものと同様である．なお，認証方法として，IEEE802.1X 認証を使用する場合も同様に動作する．



（A）WEB認証



（B）MAC認証

図 9 DAL，DGL による動作手順
Fig. 9 Procedure of operation by DAL and DGL.

4.3.2 性能評価試験

次に，システムの有効性を確認するため，試作システムのスループットを測定した．端末が接続されているスイッチのポートは 100 Mbps，Full Duplex，MDIX 固定であり，認証前に一時的に割り当てられる IP アドレスのリース時間は 10 秒である．判別する位置情報は図 7 に示すとおり 2 カ所である．測定は 5 回行い，その範囲と平均値を示す．

まず，DNC について，WEB 認証では認証スイッチのログイン画面にユーザ名，パスワードを入力してから，NAT ルータに NAT ルールが設定されるまでの時間を，MAC アドレス認証では，端末を認証スイッチに接続し，リンクアップしてから NAT ルールが設定されるまでの時間を測定した．結果を**表 2** に示す．

同様に，DAL および DGL について，WEB 認証ではログイン画面にユーザ名，パスワードを入力してから，IP アドレスがリースされるまでの時間を，MAC アドレス認証では，端末を認証スイッチ接続し，リンクアップしてから IP アドレスがリースされるまでの時間を測定した．結果を**表 3** に示す．

比較のため，通常動作の場合，すなわち試作システムにおいて NAT ルータや DHCP サーバで動的な変更をしないで，通常の認証と通常の DHCP アドレスリースを行った場合の処理時間を**表 4** に示す．

4.3.3 高負荷時の性能評価試験

また，多数の端末の同時アクセスを想定した性能評価を行った．試験方法について，複数の端末では，すべてが同時に DHCP による IP アドレス取得ができなかったため，

表 2 DNC によるスループット
Table 2 Throughput of DNC.

WEB 認証	
測定結果の範囲（秒）	7.6～9.9
平均値（秒）	8.4
MAC 認証	
測定結果の範囲（秒）	7.9～11.5
平均値（秒）	9.6

表 3 DAL によるスループット
Table 3 Throughput of DAL.

WEB 認証	
測定結果の範囲（秒）	6.6～11.1
平均値（秒）	8.2
MAC 認証	
測定結果の範囲（秒）	7.8～11.5
平均値（秒）	9.7

表 4 通常動作のスループット
Table 4 Throughput in normal operation.

WEB 認証	
測定結果の範囲（秒）	6.8～10.1
平均値（秒）	8.4
MAC 認証	
測定結果の範囲（秒）	7.4～11.5
平均値（秒）	9.5

表 5 NAT ルール設定の処理時間
Table 5 Execution time of NAT rules set.

実行時間の範囲（ミリ秒）	15～17
平均値（ミリ秒）	16.5

複数端末の同時のアクセスを再現することが困難であった．このため，提案する構成方法に特有な機能について，高負荷を想定した連続的な処理を発生させて処理時間を測定した．判別する位置情報は前述の性能評価試験と同様に 2 カ所である．

まず，DNC では，DHCP サーバの IP アドレスリースを疑似的に 200 件発生させて，NAT ルータ設定のスループットを測定した．結果を**表 5** に示す．

次に，DAL，および DGL について，位置情報を判別する場合と，判別しない通常の場合の IP アドレスリースの処理時間を測定した．DHCP サーバが DHCP DISCOVER を受信してから DHCP ACK を送信するまでの処理時間である．それぞれの場合について，DHCP クライアントによる IP アドレス取得を 200 件発生させて測定した．DHCP クライアントは，OS に実装されている dhclient を expect [24] で動作させることで，連続した IP アドレス要求を発生させた．ルータを介した DHCP RELAY による IP アドレス取得である．結果を**表 6** に示す．また，DHCP クライア

表 6 試作 DHCP サーバの IP アドレスリース時間
Table 6 IP address lease time of the prototype DHCP server.

位置情報を判別する場合	
実行時間の範囲（ミリ秒）	5.6〜8.4
平均値（ミリ秒）	6.1
位置情報を判別しない場合	
実行時間の範囲（ミリ秒）	5.4〜8.2
平均値（ミリ秒）	5.9

表 7 DHCP クライアント端末の諸元
Table 7 Specifications of the DHCP client terminal.

CPU	Celeron 1007U（2 コア，1.5 GHz）
メモリ	2 GB
OS	CentOS-5.10 32 bit

ントとして使用した端末の諸元を**表 7** に示す．

4.3.4 動作試験の評価

まず，表 2，表 3，表 4 について述べる．DNC，DAL とも，端末で認証が成功してからネットワーク利用が可能になるまでの時間の平均値は 8〜10 秒程度である．表 4 の通常動作の処理時間とほとんど変わらない．若干の時間のずれがあることについては，測定値のばらつきによるものである．なお，試作システムの環境においては，認証スイッチで MAC アドレス認証をする場合には，RADIUS サーバで認証が完了するまでに 3〜5 秒程度を要している．これは，認証スイッチの固有の動作によるものと考えられる．認証スイッチに他の機器を使用すれば，MAC 認証による処理時間はもっと短縮される可能性がある．

次に，高負荷時の性能評価として，表 5，表 6 について述べる．DNC においては，1 つの NAT ルールを設定する時間は平均 16.5 ミリ秒である．これが位置情報を判別しない通常の処理に追加されるが，事実上無視できる時間である．30 台の接続でも処理時間は 0.5 秒程度となる．処理能力の高い NAT ルータではこれよりも高速な処理が可能であり，数十台以上の同時接続も可能と考えられる．

試作 DHCP サーバによる IP アドレスリースでは，位置情報を判別する場合の平均時間は 6.1 ミリ秒，判別しない場合は 5.9 ミリ秒であった．通常の処理に対して，平均で 0.2 ミリ秒程度が追加されるが，事実上無視できる時間である．位置情報を判別する場合，50 台の接続でも処理時間は 0.3 秒程度となる．なお，DHCP クライアントでの 1 回あたりの IP アドレス要求の実行時間は約 300 ミリ秒程度であり，多数同時の DHCP 要求を十分に再現しているとはいえないが，多数同時でも位置情報を判別する処理で大きな遅延はないと考えられる．DHCP サーバを複数動作させたり，処理能力の高い DHCP サーバを利用したりすることにより，数十台以上の同時接続も可能と考えられる．

区別する位置情報について，試作システムでは 2 カ所であるが，一般の運用環境においては，場合によっては数十カ所以上の判別を要することも考えられる．しかし，ハッシュなどを用いることで位置情報の数に関係なく同等の時間で処理をすることが可能である．

また，動作試験の評価について，DGL では，DAL による結果と同様である．DRC については，DNC において，Telnet で NAT ルータを設定する動作が，ルータのルートマップを設定する動作に変更される以外は同様のため，DNC による結果と同様である．

以上より，提案するシステムの有効性が確認された．

5. まとめ

本論文では，ロケーションフリーネットワークシステムの新たな構成方法として，同一ブロードキャストドメインにおけるサブネットへの接続を保証しながらも，サブネットを越えてアクセスする場合には送信元 IP アドレスによって利用者の位置情報を識別できるネットワーク構成方法を提案した．また，システムを実装し，設計どおりに動作していることを確認した．さらに，提案するシステムの有効性を確認するため性能評価試験を行い，このシステムが有効であることを確認した．

今後の課題としては，提案するシステムを実際の環境で運用するための実用化プログラムの開発があげられる．1 つは DHCP サーバであり，これは ISC DHCP サーバプログラムにモジュールを追加することを検討している．この DHCP サーバによる負荷試験も行いたい．もう 1 つは，DNC や DRC においては，端末がネットワークから離れたことを検出して設定情報を削除する機能である．ネットワークスイッチの MAC アドレステーブルを利用する方法を検討している．また，3.4 節のシステムの応用について実際に適用し，動作を確認することがあげられる．

謝辞 本研究は平成 24 年度科学研究費補助金（奨励研究，課題番号 24919006）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] American Physiological Society: WWW.PHYSIOLGY.ORG (online), available from ⟨http://www.physiology.org/⟩ (accessed 2014-09-11).
[2] American Society for Biochemistry and Molecular Biology: THE JOURNAL OF BIOLOGICAL CHEMISTRY (online), available from ⟨http://www.jbc.org/⟩ (accessed 2014-09-11).
[3] Ohsumi, Y., Okayama, K. and Yamai, N.: A Configuration of Location Free Network Applicable to Location Dependent Services, *Journal of Information Processing*, Vol.21, No.3, pp.433–440 (2013).
[4] Aboba, B., Blunk, L., Vollbrecht, J., et al.: Extensible Authentication Protocol (EAP), RFC 3748, IETF (2004).
[5] IEEE: 802.1X - Port-Based Network Access Control (online), available from ⟨http://www.ieee802.org/1/pages/

802.1x.html⟩ (accessed 2014-09-11).
[6] Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC 2865, IETF (2000).
[7] Wahl, M., Howes, T. and Kille, S.: Lightweight Directory Access Protocol (v3), RFC 2251, IETF (1997).
[8] Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC 1631, IETF (1994).
[9] Droms, R.: Dynamic Host Configuration Protocol, RFC 2131, IETF (1997).
[10] Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, IETF (1999).
[11] Daigle, L.: WHOIS Protocol Specification, RFC 3912, IETF (2004).
[12] Maxmind Developer Site: GeoIP Products (online), available from ⟨http://dev.maxmind.com/geoip/⟩ (accessed 2014-09-11).
[13] Imielinski, T. and Navas, J.: GPS-Based Addressing and Routing, RFC 2009, IETF (1996).
[14] Mockapetris, P.: Domain Names – Concepts and Facilities, RFC 1034, IETF (1987).
[15] 伊藤誠悟，吉田廣志，河口信夫：locky.jp：無線 LAN を用いた位置情報・測位ポータル，情報処理学会研究報告 MBL［モバイルコンピューティングとユビキタス通信研究会研究報告］，Vol.2005, No.90, pp.25–31 (2005.09.15).
[16] NEC Corporation: UNIVERGE IX2025 (online), 入手先 ⟨http://jpn.nec.com/univerge/ix/Info/ix2025.html⟩ (参照 2014-09-11).
[17] The CentOS Project: CentOS (online), available from ⟨http://www.centos.org/⟩ (accessed 2014-09-11).
[18] Cisco Systems, Inc.: Cisco Catalyst 3750 シリーズスイッチ (online), 入手先 ⟨http://www.cisco.com/web/JP/product/hs/switches/cat3750/prodlit/cat50_ds.html⟩ (参照 2014-09-11).
[19] Allied Telesis K.K.: CentreCOM GS908M V2 (online), available from ⟨https://www.allied-telesis.co.jp/products/list/switch/gs900mv2/catalog.html⟩ (accessed 2014-09-11).
[20] The FreeRADIUS Server Project and Contributors: The FreeRADIUS Project (online), available from ⟨http://freeradius.org/⟩ (accessed 2014-09-11).
[21] Internet Systems Consortium, Inc.: ISC DHCP (online), available from ⟨https://www.isc.org/downloads/dhcp/⟩ (accessed 2014-09-11).
[22] Perl.org: The Perl Programming Language (online), available from ⟨http://www.perl.org/⟩ (accessed 2014-09-11).
[23] Poznyakoff, S.: GDBM (online), available from ⟨http://www.gnu.org.ua/software/gdbm/⟩ (accessed 2014-09-11).
[24] Libes, D.: The Expect Home Page (online), available from ⟨http://expect.sourceforge.net/⟩ (accessed 2014-09-11).

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処理センター（現，情報統括センター）技官を経て，現在，同技術専門職員．平成 23 年岡山大学大学院自然科学研究科（産業創成工学専攻）博士後期課程入学，平成 26 年単位取得後退学．キャンパス情報ネットワークの運用管理に従事．

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，情報統括センター）助教授を経て，平成 18 年同教授．平成 26 年より東京農工大学大学院工学研究院教授．分散システム，ネットワーク運用管理，ネットワークセキュリティの研究に従事．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，奈良先端科学技術大学院大学情報科学研究科助手．岡山大学工学部助手，同大学情報基盤センター助教を経て，平成 22 年同大学情報統括センター助教，平成 23 年同准教授．博士（工学）．インター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．