電子ジャーナルの地理的なサイトライセンス契約条件に適応するロケーションフリーネットワークシステム

大隅淑弘† 岡山聖彦† 山井成良† 藤原崇起† 稗田 隆†

多くの大学や企業などの研究機関では，文献検索や資料収集のため電子ジャーナルを契約している．組織で電子ジャーナルを契約する場合には，通常はサイトライセンスを契約するが，サイトライセンスは利用者の場所や所属などによって契約されるため，利用者の条件によって利用できる電子ジャーナルは異なっている．一方，近年のネットワークシステムの高機能化により，端末をネットワークに接続するときに利用者や端末を認証し，不正な利用を排除すると共に，ダイナミック VLAN によって，利用者あるいは端末の属性に基づく VLAN に接続させることができるようになった．利用者は，認証できる範囲であればどこでも決まった VLAN に接続することができる．しかし，電子ジャーナの利用では，利用者がどの場所からアクセスしているのかの区別が付かず，サイトライセンスを保証できなくなる．そこで，本論文ではロケーションフリー機能を実現しながらも，電子ジャーナルのサイトライセンスに適応するネットワークシステムを提案する．

A Location Free Network System applicable to geographical terms of the Electronic Journal Site License

YOSHIHIRO OHSUMI† KIYOHIKO OKAYAMA† NARIYOSHI YAMAI†
TAKAOKI FUJIWARA† TAKASHI HIEDA†

In the research institutes such as universities or companies, they contract electronic journals for document retrieval and document collection. When an organization contracts electronic journals, the site license is usually contracted. Because of conditions of a site license include location or affiliation of users, available electronic journals differ from users. On the other hand, the user and the terminal are authenticated when the terminal was connected with the network, so an illegal user is excluded, and the terminal is able to connect to VLAN that had been allocated by dynamic VLAN. The user can connect to the network of the same VLAN anywhere. However, in such network environment, it cannot be determined where a user accessed by the IP address of the user's terminal, and it is not able to warrant the site license. In this paper, we propose a network system that adjusts to the site license of electronic journals on the location free network.

1. はじめに

大学や企業などの研究機関では，文献検索や資料取集のため，インターネット上の多くの電子ジャーナルやデータベースサービス（以下，これらを総称して電子ジャーナルとする）を契約している．組織で電子ジャーナルを契約する場合には，サイトライセンスを契約するのが一般的である．サイトライセンスでは，利用者が組織に所属していることの他にも，利用者の所属を条件としているものがあり，特定の事業所や部署（大学では特定のキャンパスや特定の学部，学科に相当する）などに関係付けて契約を行っている．このため，電子ジャーナルを契約している場合には，利用者がどこからアクセスしているのかを判別し，正当な利用者であることを保証する必要がある．

一方でネットワーク装置の高機能化により，端末をネットワークに接続する場合に，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）．認証ネットワークでは，利用者や端末の属性値として VLAN-ID を持たせることができるため，認証ネットワークの範囲内であれば，どこでも同じ VLAN に接続をすることができる（以下，ロケーションフリーネットワークとする）．しかし，利用者が場所を移動するときにどこでも決まった VLAN に接続すると，電子ジャーナルによってはライセンス違反になる場合がある．例えば，電子ジャーナルのサイトライセンスが，特定の事業所や部署からのアクセスに限って契約されている場合に，利用者の現在位置が判別できないと，必要なアクセス制限ができなくなる恐れがあるためである．

そこで，本論文では，ロケーションフリーネットワークを実現しながらも，利用者がどこからネットワークに接続しているのかを判別することで，電子ジャーナルのサイトライセンスに適応できるネットワークシステムを提案する．本システムでは，ネットワーク認証による VLAN-ID と実際に割り当てられるサブネットアドレスを工夫することにより，利用者がどこから接続しているのかを判別し，サイトライセンスに適応したアクセス制御をすることができる．また，組織に所属する者が VPN(Virtual Private Network)[1]接続サービスによって自宅や出張先から組織内に接続し，さらに組織外のサイトに接続をした場合（以下，VPN 利用者とする）や，組織に所属しないが正当な利用者として認められている利用者が，組織内のネットワークに接続する場合（以下，ゲストとする）についても同様の制御が可能である．

以下，まず第２章では，電子ジャーナルのサイトライセンスとロケーションフリーネットワークについて説明し，ロケーションフリーネットワークを構成する上での問題点について述べる．次に第３章では，提案

† 岡山大学情報統括センター
Center For Information Technology And Management

するロケーションフリーネットワークの構成方法について述べ，第４章で提案方法に基づいて実装したシステムについて説明する．

2. ロケーションフリーネットワークによる電子ジャーナル利用の問題点

2.1 想定する環境

本論文では，組織に所属する利用者が，その組織内の様々な場所から電子ジャーナルにアクセスする場合を想定する．また，VPN 利用者とゲストについても考える．各電子ジャーナルの契約はサイトライセンスであり，利用条件は電子ジャーナルによって異なっているものとする．すなわち，利用者はその組織に所属する者であると共に，電子ジャーナルによっては特定の事業所や部署からのみ利用が可能である．また，組織内ではロケーションフリーネットワークを運用しており，利用者は組織内のどこでネットワークに接続しても，いつもと同じ手順で認証をすれば，決まった VLAN に接続されるものとする．利用者の端末は，ネットワーク接続時に認証が成功すれば DHCP(Dynamic Host Configuration Protocol)[2]サーバから IP アドレスを取得し，ネットワークの利用が可能になる．なお，認証方式は，一般に WEB 認証，MAC アドレス認証，IEEE802.1X 認証などが良く利用されているが，本論文では，主に WEB 認証を想定して説明をする．電子ジャーナルへアクセスする様子を図 1 に示す．

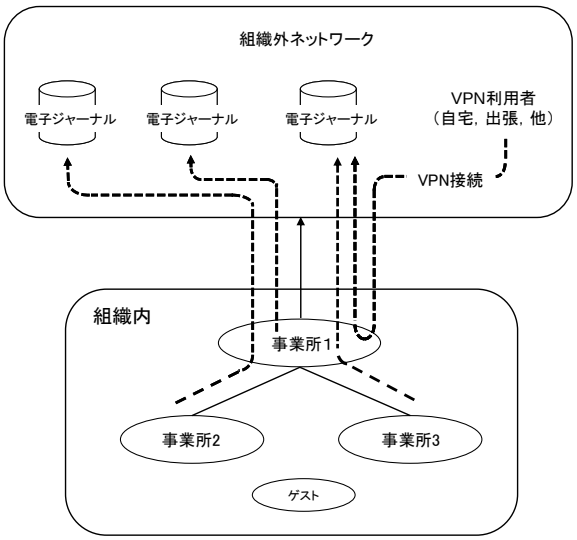


図 1　電子ジャーナルへのアクセス
Figure 1　Access to electronic journals

2.1.1 電子ジャーナルのサイトライセンス

電子ジャーナルは，主として学術雑誌が電子化されオンラインで閲覧できるものをいう．組織が電子ジャーナルを契約する場合には，サイトライセンスによる契約が一般的である．サイトライセンスの場合には，電子ジャーナルベンダ（以下，ベンダとする）とユーザの間で利用してよい条件を決め，その範囲内であれば契約した電子ジャーナルを無制限に利用することができる．この条件には，利用者の所属に関して契約されているものが多いが，契約者である組織は，電子ジャーナルの利用者がその条件に適合していることを保証する必要がある．利用許可の判定方法として，利用者の端末の IP アドレスや利用者認証が使用されることが多い．実際の契約では，IP アドレスに関しては，ベンダに対して利用者の端末の IP アドレスの範囲を通知し，電子ジャーナル側で契約範囲内からの接続のみを許可する．また，利用者認証に関しては，組織内に認証機能を有するプロキシサーバなどを運用し，その IP アドレスを電子ジャーナルで利用許可することにより，正しく認証された利用者だけが電子ジャーナルを利用するなどがある．近年は Shibboleth 認証を利用するものもある．

2.1.2 ロケーションフリーネットワーク

近年のネットワークシステムの高機能化により，端末をネットワークに接続するときに利用者や端末を認証することができるようになった．認証によって不正な利用を排除すると共に，利用者や端末を識別し，ダイナミックな VLAN の割り当て（以下，ダイナミック VLAN とする）によって，利用者の端末を利用者あるいは端末の属性に基づく VLAN に接続させることができるため，利用者は認証できる範囲であればどこでも決まったネットワークに自動的に接続されるという利便性を有する．ダイナミック VLAN の方式では，MAC ベース VLAN，サブネットベース VLAN，ユーザベース VLAN などが利用できる．本稿では，認証スイッチにアラクサラ社の AX2400S を使用した例として，MAC ベース VLAN によるダイナミック VLAN で説明を進める．

2.2 ロケーションフリーネットワークによる問題点

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決まった VLAN に接続できるようになるが，実際にはネットワークの構成上の理由や電子ジャーナルの利用において問題が生ずる．

ロケーションフリーネットワークを実現する基本的な方法は，全ての事業所に全ての VLAN を通し，完全なロケーションフリーを実現することである．しかし，この場合には，VLAN が通過している通信回線に全ての VLAN によるブロードキャストトラフィックが発生するため，接続端末数においてネットワークの規模が大きくなってくると，幹線の通信回線に十分な帯域がなかったり，複数の事業所のある組織で各事業所間の通信回線に十分な帯域がなかったりする場合には利用できない．

これに対し，全事業所に全ての VLAN を同じように運用し，ロケーションフリーネットワークを実現するが，各事業所間の VLAN を分離し，プロキシサーバあるいは NAT(Network Address Translation)[3]によって接続する方法が考えられる．この方法であれば，事業所間の通信回線に大きなブロードキャストパケットが流れることがないため，事業所間の通信回線が高速でなくても実現できる．しかし，各事業所でプロキシサーバや NAT を運用する負担が発生したり，事業所間の端末同士が通信するための設定をプロキシサーバや NAT に施す負担が発生したりするなどの問題がある．

また，ロケーションフリーネットワークを各事業所内だけに限定し，各事業所で別々の VLAN を割り当てれば，事業所間の通信回線に大きなブロードキャストパケットが流れることはないが，この場合には，認証後に接続されるVLANの認証情報を各事業所で個別に運用する必要があるため，事業所毎に個別に認証サーバを運用するなどの負担が生じる．

さらに，電子ジャーナルのサイトライセンスを契約している場合に問題になることがある．すなわち，サイトライセンスを組織の一部，例えば，特定の事業所や事業所内の特定の部署に限って契約している場合である．利用者がロケーションフリーネットワークによって，どこでも決まった VLAN に自動的に接続されると，利用者が現在どこから電子ジャーナルに接続しているのかの区別がつかなくなり，サイトライセンスによる利用者の範囲を保証できなくなる．また，VPN 利用者やゲストについても区別する必要がある．

3. サイトライセンスに適応するロケーションフリーネットワークシステム

前章で述べたとおり，単純にロケーションフリーネットワークを実現すると，電子ジャーナルのサイトライセンスを利用する場合に問題が生じる．また，ロケーションフリーネットワークを構成するためには，組織の様々なネットワークトポロジに柔軟に対応できなければならない．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構成方法について提案し，以下に説明をする．

3.1 認証後の VLAN-ID とサブネットの割り当て方法

2.2 節で述べた問題は，VLAN とサブネットの対応が固定されていることにある．すなわち，認証の結果として VLAN が決定すると，ロケーションにかかわらず同じサブネットが割り当てられるので，利用者がどの事業所にいるのかが外部から判別できない．この問題に対しては，利用者の認証情報はどの事業所でも共通でありながらも，実際に割り当てられるサブネットが異なるような仕組みが必要となる．

本論文では，上述した仕組みを実現する方法として，認証後の VLAN-ID はどこでも同じであるが，実際に割り当てられるサブネットアドレスを各事業所で変更する方法を提案する．この方法では，利用者の場所ごとにサブネットが異なるため，どこからネットワークに接続しているのかを判別することが可能である．また，利用者の認証後の VLAN-ID はどこでも同じとなるため，認証情報や認証サーバの運用を一元化することが可能である．

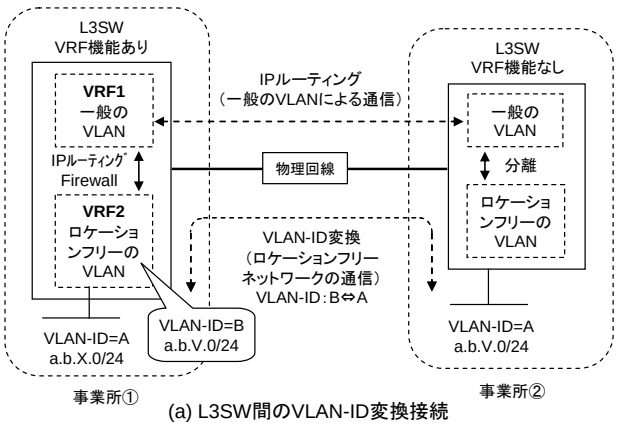
さらに，事業所間の通信は IP ルーティングによる接続が可能なため，事業所間の通信回線にロケーションフリーネットワークのVLANによるブロードキャストトラフィックが流れることがなく，事業所間の通信回線の帯域によらず利用が可能である．また，事業所間の相互通信にも，NAT やプロキシサーバを必要としない．

3.2 VLAN-ID 変換による拠点間の接続

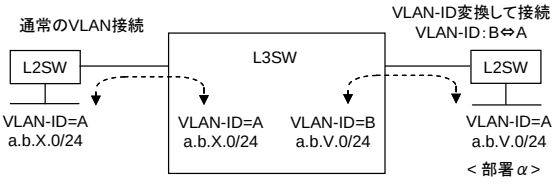
3.2.1 事業所間での VLAN-ID 変換

セキュリティや運用ポリシーなどの理由により，事業所内のロケーションフリーネットワークを他のサブネットと分離させたい場合がある．通常は，VRF(Virtual Routing and Forwarding) [4]機能によりルーティングドメインを分離すればよいが，VRF 機能が利用できない場合などには，VRF 機能を有している他の拠点のレイヤ 3 スイッチで生成したサブネットを，その事業所のスイッチにVLANで接続することなどが考えられる．しかし，VRF 機能のある相手側事業所でもロケーションフリーネットワークを構成している場合には，VLAN-ID とサブネットが同じであると，どちらの事業所の利用者なのかの区別ができなくなる．そこで，このような場合には，他の事業所のレイヤ 3 スイッチと VLAN-ID 変換によってサブネットを接続する方法を提案する．これにより，事業所間で VLAN-ID が同じでも異なったサブネットを運用することが可能になるため，双方でロケーションフリーネットワークを運用する場合でも，IP アドレスにより，利用者がどこから接続しているのかを区別することができる．この様子を図 2 の（a）に示す．事業所②でロケーションフリーネットワークを運用し，事業所内の他のネットワークと分離したいが，事業所②のレイヤ 3 スイッチで VRF 機能が利用できないため，事業所①で生成した VLAN-ID=B のサブネットを VLAN-ID 変換し，VLAN-ID=A として事業所②で利用する．

この方法では，ロケーションフリーネットワークに関して，事業所間の通信回線には，VLAN-ID 変換しているサブネットによるトラフィック以外は流れないという利点もある．



(a) L3SW間のVLAN-ID変換接続



(b) L3SWとL2SW間のVLAN-ID変換接続

図 2　VLAN-ID 変換
Figure 2　VLAN-ID swapping

3.2.2 同一事業所内での VLAN-ID 変換

同じ事業所内の一部の部署だけがサイトライセンスを契約している場合などのように，同じレイヤ 3 スイッチ配下で通信を行っている一部の領域だけを他と区別したい場合がある．この場合には，レイヤ 2 スイッチとの間で VLAN-ID 変換を行うことにより，VLAN-ID が同じでありながら, 異なったサブネットをその領域に割り当てることが可能になる．この様子を図 2 の（b）に示す．この事業所内ではどこでも VLAN-ID=A で利用するが，部署αについては，実際に割り当てられるサブネットは VLAN-ID=B のものである．

3.3 電子ジャーナルへの適用

提案する方法により，利用者が現在どこからネットワークに接続しているのかを, 接続元の IP アドレスから判別することができるため，電子ジャーナルのサーバやファイアウォールなどで，IP アドレスによるアクセス制限をすることが可能となる. 電子ジャーナルは，サイトライセンスの範囲に適合した者だけが利用可能となり，ライセンスの範囲を保証することができる．一方で利用者は，ロケーションフリーネットワークの利便性により，どこでもいつもと同じようにネットワークに接続することができる．

なお，この方法では，ネットワーク認証の方式は，WEB 認証, MAC アドレス認証, IEEE802.1X 認証など，どの方式でも利用可能であり，VPN 利用者やゲストなどにも適用することができる．さらに多様な認証情報を活用すれば，利用者の個人属性に基づいたアクセス制御を柔軟に適用することができる．

3.4 システム構成

提案するシステム構成は，RADIUS[5]サーバ，DHCP サーバ，レイヤ 3 スイッチ，レイヤ 2 スイッチ，認証スイッチから構成する. 組織内がプライベート IP アドレスで構成されている場合など，組織内から組織外への通信に対して IP アドレス変換をする場合には, NAT 装置を用いる. NAT 装置は送信元アドレスにより, NAT 変換後のグローバル IP アドレスを変更できるものであり, 各事業所, 事業所内の特定の部署, VPN 利用者，ゲストなどのサブネットアドレスによって異なったグローバル IP アドレスに変換する．

RADIUS サーバは，認証スイッチからの認証要求に対して認証を行う．また，各利用者や端末の属性値として，認証成功後に接続する VLAN-ID を保持しており, 認証スイッチに対して認証の判定と共に VLAN-ID を回答する．認証情報については別に LDAP サーバなどを運用し，RADIUS サーバが LDAP サーバから情報を取得する構成でもよい．

DHCP サーバは，利用者が認証に成功し，所定の VLAN に接続されたときに IP アドレスを割り当てる．

レイヤ 3 スイッチは，事業所内及び事業所間のネットワークについて IP ルーティングや VLAN によりサブネットを接続する．また，必要により対向するスイッチとの間で VLAN-ID 変換をする．

認証スイッチは，利用者が最初にネットワーク接続したときに RADIUS サーバに対して認証要求し，成功の場合には RADIUS サーバから取得した VLAN-ID を端末の MAC アドレス，あるいは利用者が接続されている認証スイッチのポートに割り当てる．これにより端末はその VLAN による通信が可能となる．

3.5 システムの動作手順

ある組織の利用者が本システムにより，電子ジャーナルを利用する場合を考える．

3.5.1 想定する条件

組織に所属する利用者が，このロケーションフリーネットワークに端末を接続し，認証に成功すると VLAN-ID=A の VLAN を割り当てられるものとする．VPN 利用者には認証により VLAN-ID=C の VLAN が，ゲストには認証により VLAN-ID=D の VLAN が割り当てられるものとする．

また, この組織では 4 つの電子ジャーナル K, L, M, N を契約しており，いずれもこの組織に所属する者だけが利用できるものとする．電子ジャーナル K は組織内の全ての事業所からと VPN 利用者が利用できるが，電子ジャーナル L は事業所Ⅰからのみ利用が許可されており, 電子ジャーナル M は事業所Ⅱからのみ利用が許可されている．さらに電子ジャーナル N は，事業所Ⅰ内の部署αからのみ利用が許可されている．

3.5.2 組織内にグローバル IP アドレスが割り当てられている場合の動作手順

組織のグローバル IP アドレスを a.b.0.0/16 とし，図 3 により動作手順を説明する．この例では，事業所Ⅰと事業所Ⅲの接続は，3.2 1 節による接続例であり，事業所Ⅰの部署αとの接続は 3.2.2 節による接続例である．

ロケーションフリーネットワークによって，利用者が端末をネットワークに接続すると，事業所Ⅰの部署α以外では VLAN-ID=A において a.b.X.0/24 が，部署αでは a.b.V.0/24 が割り当てられるようにする．事業所Ⅱでは VLAN-ID=A において a.b.Y.0/24 が，事業所Ⅲでは VLAN-ID=A において a.b.Z.0/24 が割り当てられるようにする．VPN 利用者は VLAN-ID=C において a.b.VPN.0/24 が, ゲストはどの事業所でも VLAN-ID=D において a.b.GST.0/24 が割り当てられるようにする．

また, 電子ジャーナル K では a.b.X.0/24, a.b.Y.0/24, a.b.Z.0/24，a.b.V.0/24，a.b.VPN.0/24 の端末について接続を許可し，電子ジャーナル L では a.b.X.0/24 と a.b.V.0/24 からの接続を，電子ジャーナル M は a.b.Y.0/24 からの接続だけを，電子ジャーナル N は a.b.V.0/24 からの接続だけを許可する．

以上のように設定されたロケーションフリーネットワークにおいて，組織に所属する利用者が端末を持って事業所間を移動する．まず，事業所Ⅰにおいて部署α以外の場所で端末をネットワークに接続し，認証に成功すると VLAN-ID=A が割り当てられ，実際のサブネットは a.b.X.0/24 が割り当てられる．この状態で電子ジャーナルにアクセスすると，電子ジャーナル K と L は利用できるが, 電子ジャーナル M と N は利用できない. 部署αに移動し, 認証に成功すると VLAN-ID=A によって a.b.V.0/24 が割り当てられるため，電子ジャーナル K，L，N は利用できるが，電子ジャーナル M は利用できない．その後，この利用者が事業所Ⅱに移動し，認証に成功すると VLAN-ID=A によって

a.b.Y.0/24 が割り当てられるため，電子ジャーナル K と M は利用できるが，電子ジャーナル L と N は利用できない．さらに，事業所Ⅲに移動し，認証に成功すると VLAN-ID=A によって a.b.Z.0/24 が割り当てられるため，電子ジャーナルは K だけが利用できる．VPN 利用者は a.b.VPN.0/24 のサブネットが割り当てられるため，電子ジャーナル K だけが利用できる．ゲストは VLAN-ID=D によって a.b.GST.0/24 のサブネットが割り当てられるため，どの電子ジャーナルも利用できない．なお，ゲストについても利用規模が大きい場合には，事業所ごとにサブネットを変更し，事業所間を IP ルーティングするなどの方法でもよい．表 1 に利用者の移動によってアクセスできる電子ジャーナルを示す．

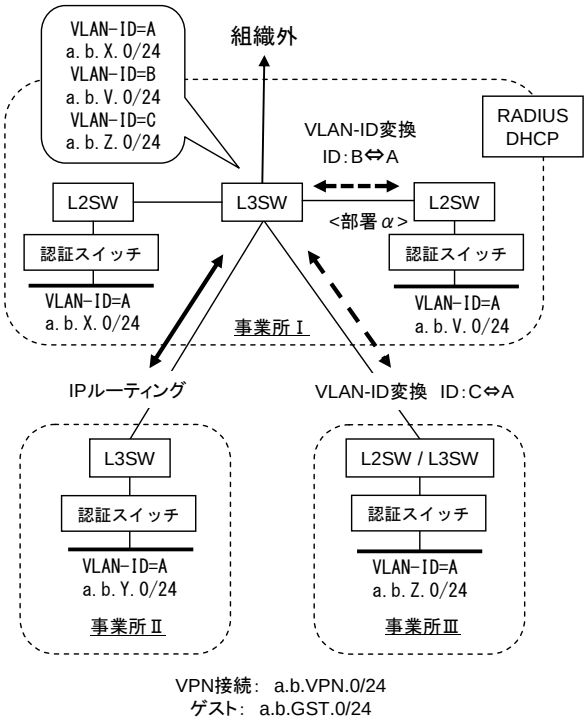


図 3　提案方法の構成と動作
Figure 3　The structure and operation of proposed location free network system

表 1　電子ジャーナルへの接続例
（グローバル IP アドレス）
Table 1　Example of access for electronic journals (global IP address)

事業所による サブネットの割当	電子ジャーナルの利用			
	K	L	M	N
事業所Ⅰ (a.b.X.0/24)	○	○	×	×
部署α (a.b.V.0/24)	○	○	×	○
事業所Ⅱ (a.b.Y.0/24)	○	×	○	×
事業所Ⅲ (a.b.Z.0/24)	○	×	×	×
VPN 利用者 (a.b.VPN.0/24)	○	×	×	×
ゲスト (a.b.GST.0/24)	×	×	×	×

3.5.3 組織外への接続で NAT による IP アドレス変換を行う場合の動作手順

図 4 により動作手順を説明する．この例でも，事業所Ⅰと事業所Ⅲの接続は，3.2 1 節による接続例であり，事業所Ⅰの部署α との接続は 3.2.2 節による接続例である．組織が使用しているグローバル IP アドレスは e.f.g.0/24 であり，組織内は p.q.0.0/16 のプライベート IP アドレスが割り当てられているものとする．

ロケーションフリーネットワークによって，利用者が端末をネットワークに接続すると，事業所Ⅰの部署α以外では VLAN-ID=A において p.q.X.0/24 が，部署α では p.q.V.0/24 が割り当てられるようにする．事業所Ⅱでは VLAN-ID=A において p.q.Y.0/24 が，事業所Ⅲでは VLAN-ID=A において p.q.Z.0/24 が割り当てられるようにする．VPN 利用者は VLAN-ID=C において p.q.VPN.0/24 が，ゲストは VLAN-ID=D において p.q.GST.0/24 が割り当てられるようにする．また，組織外に接続する場合には，NAT によって表 2 のように変換される．電子ジャーナル K では，組織のグローバル IP アドレスのうち e.f.g.h1, e.f.g.h2, e.f.g.h3, e.f.g.h4, e.f.g.h5 について接続を許可し，電子ジャーナル L では e.f.g.h1，e.f.g.h4 からの接続を，電子ジャーナル M は e.f.g.h2 からの接続だけを，電子ジャーナル N は e.f.g.h4 からの接続だけを許可しているものとする．

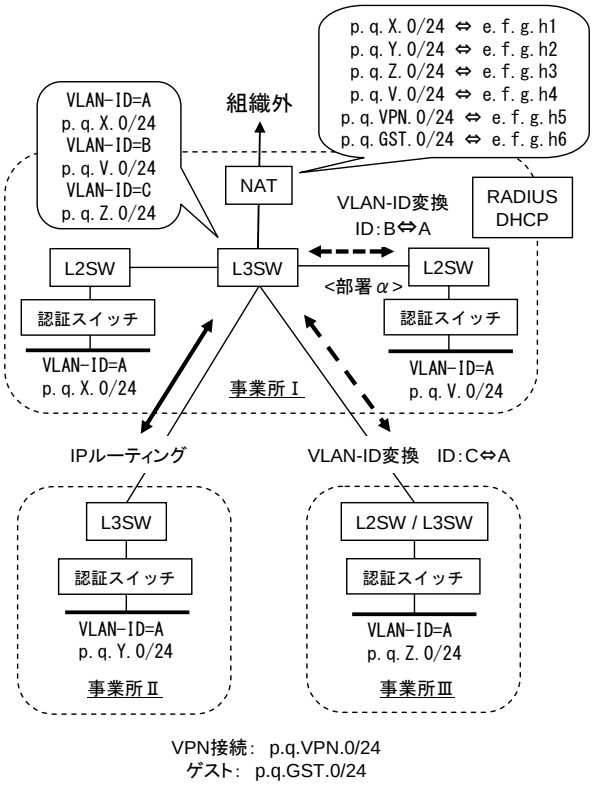


図 4　提案方法の構成と動作（NAT あり）
Figure 4　The structure and operation of proposed location free network system (NAT)

以上のように設定されたロケーションフリーネットワークにおいて，組織に所属する利用者が事業所間を

移動する場合，ゲストが事業所を移動する場合，VPN 利用者についても 3.5.2 節と同様の結果となる．表 2 に NAT による IP アドレス変換を行う場合に，利用者の移動によってアクセスできる電子ジャーナルを示す．

このように，利用者はロケーションフリーネットワークによって組織内のどこでもいつもと同じ手順で認証をしてネットワークに接続できるが，電子ジャーナルは契約の範囲に適合しているものだけが利用できるという制御が可能になる．なお，動作手順の説明では，利用者の位置による条件について説明をしたが，利用者の身分や所属などについても VLAN を構成すれば同様の制御が可能である．

表 2　電子ジャーナルへの接続例（NAT）
Table 2　Example of access for electronic journals (NAT)

事業所による サブネットの割当	変換後 IP アドレス	電子ジャーナルの利用			
		K	L	M	N
事業所Ⅰ (p.q.X.0/24)	e.f.g.h1	○	○	×	×
部署α (p.q.V.0/24)	e.f.g.h4	○	○	×	○
事業所Ⅱ (p.q.Y.0/24)	e.f.g.h2	○	×	○	×
事業所Ⅲ (p.q.Z.0/24)	e.f.g.h3	○	×	×	×
VPN 利用者 (p.q.VPN.0/24)	e.f.g.h5	○	×	×	×
ゲスト (p.q.GST.0/24)	e.f.g.h6	×	×	×	×

4. システムの実装

岡山大学では，キャンパス情報ネットワークシステムの更新に伴い，“生活系ネットワーク”の名称でプライベートアドレスによる，ロケーションフリーネットワークのサービスをすることになった．そこで，3 章で述べた提案方法に基づき，我々は岡山大学のキャンパス情報ネットワークにシステムの実装を行った．実装したシステムの構成を図 5 に示す．RADIUS サーバ，認証サーバ，DHCP サーバは津島キャンパス，鹿田キャンパスに各 1 台を設置して冗長構成とした．各サーバの OS は Red Hat Enterprise Linux5 である．なお，倉敷キャンパスは岡山情報ハイウエイ [6]（以下，OKIX とする）を介して接続されており，三朝キャンパスは OKIX 及び鳥取情報ハイウェイ [7]（以下，TIH とする）を介して接続されている．

従来のキャンパス情報ネットワークは，グローバル IP アドレスを固定的に割り当てたネットワークであるが，本システムによるロケーションフリーネットワークでは，セキュリティポリシーの理由により，従来のキャンパス情報ネットワークとはバーチャルファイアウォールを介した接続をすることになった．このため，バーチャルファイアウォール以外では，従来のキャンパス情報ネットワークと接続しないことになっている．

津島キャンパスと鹿田キャンパスでは，レイヤ 3 スイッチが VRF 機能を有しているため，ロケーションフリーネットワークについて，キャンパス間の接続は同じ VRF 階層での IP ルーティングを行っている．倉敷キャンパス，三朝キャンパス，東山キャンパスのレイヤ 3 スイッチでは，VRF 機能が利用できないため，これらのレイヤ 3 スイッチにロケーションフリーネットワークで利用者が接続するサブネットを生成すると，既存のグローバル IP アドレスによるネットワークとバーチャルファイアウォール以外で接続されてしまう．このため，これらのキャンパスでは，ロケーションフリーネットワークのサブネットは，津島キャンパスレイヤ 3 スイッチのロケーションフリーネットワーク用 VRF で生成したサブネットを当該キャンパスのスイッチとの VLAN-ID 変換によって接続した．芳賀キャンパスでは，キャンパス規模の理由でレイヤ 3 スイッチが設置されていないため，レイヤ 2 スイッチにより，津島キャンパスのレイヤ 3 スイッチと接続されている．このため，芳賀キャンパスでは，ロケーションフリーネットワークで利用者が接続するサブネットは，津島キャンパスで生成したサブネットをレイヤ 2 スイッチとの VLAN-ID 変換によって接続している．

なお，現在は同一キャンパスにおいて，レイヤ 3 スイッチで生成した VLAN をレイヤ 2 スイッチとの VLAN-ID 変換によって一部の領域で運用する方法は用いていない．これは，岡山大学が契約している電子ジャーナルでは，今のところキャンパス内の特定の学部や学科に限ってサービスされているものがないためである．

生活系ネットワークでは，セキュリティ強化とロケーションフリーによる利便性向上が期待されるため，一般の端末について従来のキャンパス情報ネットワークからの移行が進められている．

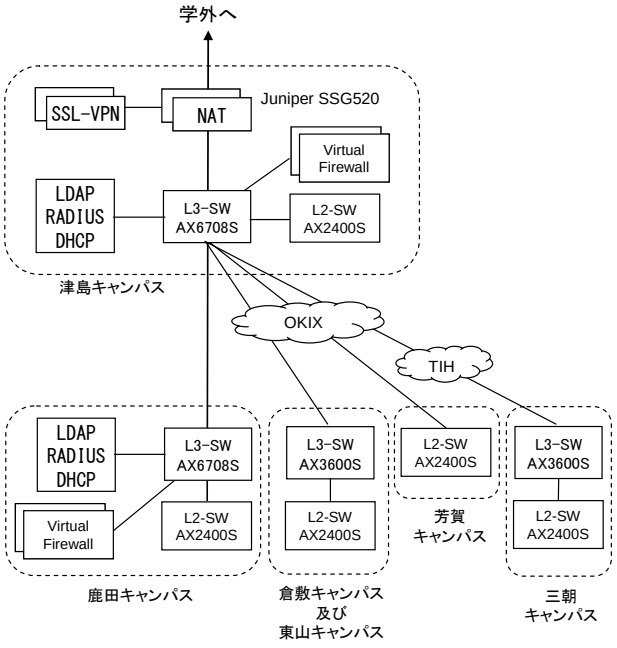


図 5　実装したシステムの構成
Figure 5　The structure of implemented system

4.1 基本機能の実装

4.1.1 認証スイッチ

フロアスイッチにアラクサラ社の AX2400S[8]を使用

し，認証スイッチとしても利用している．端末がネットワークに接続されると MAC 認証を試み，認証が失敗すると（MAC アドレスの登録がない場合），ユーザ名，パスワードによる WEB 認証を行う．認証要求は RADIUS サーバに対して行い，認証に成功すると RADIUS サーバから取得した VLAN-ID のサブネットに端末を接続する．

4.1.2 RADIUS サーバ

FreeRADIUS[9]を使用した．認証スイッチからの認証要求に対して認証サーバの情報を確認し，認証成功の場合には認証 OK と VLAN-ID を回答する．

4.1.3 認証サーバ

岡山大学統合認証システムの LDAP サーバを使用した．LDAP サーバには学生を含む岡山大学の全構成員が登録されているため，全登録者の属性に VLAN-ID を登録し，WEB 認証で使用している．また，MAC アドレス認証では，各 VLAN-ID のエントリに対して端末の MAC アドレスを属性値として登録している．

4.1.4 NAT 装置

Juniper networks 社の SSG520M[10]をファイアウォール兼 NAT として使用している．2 台を Active/Standby 構成とし，学外との接続ポイントで運用している．4.2 節で説明する生活系ネットワークにおいては，ネットワークの種別を以下のように分類し，それぞれ異なったプライベート IP アドレスレンジを割り当てている．NAT 装置では，送信元の IP アドレスレンジにより，それぞれに対応したグローバル IP アドレスに変換して学外と接続する．

- ●津島キャンパスの教員・職員用，学生用ネットワーク
- ●鹿田キャンパスの教員・職員用，学生用ネットワーク
- ●三朝キャンパスの教員・職員用，学生用ネットワーク
- ●倉敷キャンパスの教員・職員用，学生用ネットワーク
- ●東山キャンパスの教員・職員用，学生用ネットワーク
- ●芳賀キャンパスの教員・職員用，学生用ネットワーク
- ●津島，鹿田，三朝，倉敷，東山，芳賀の各キャンパスのゲスト用ネットワーク

4.1.5 SSL-VPN 接続システム

F5 ネットワークス社の FirePass4120[11]を 2 台で冗長化構成している．最大で同時 200 の接続が可能であり，SSL-VPN 用に用意されたグローバル IP アドレスレンジから利用者の端末に IP アドレスが割り当てられる．

4.1.6 バーチャルファイアウォール

フォーティネット社の FotiGate-310 を冗長化構成とし，津島キャンパスと鹿田キャンパスで運用している．学生用ネットワーク及びゲスト用ネットワークについて，キャンパス情報ネットワークと接続する部分で UTM として動作している．

4.2 プライベート IP アドレスによるロケーションフリーネットワークへの適用

生活系ネットワークは，教員・職員，学生について，各学科，施設，部署ごとに VLAN を構成し，/22～/24 のサブネットを割り当てている．学外者によるゲストは，各キャンパスで/24 のサブネット 1 つを割り当てている．割り当て済みの VLAN 数は，教員・職員及びゲストのものが 798，学生及び学生ゲストのものが 633 である．アドレス空間は 10.0.0.0/8 を使用した．この生活系ネットワークをロケーションフリーネットワークとして，津島キャンパス，鹿田キャンパス，倉敷キャンパス，三朝キャンパス，東山キャンパス，芳賀キャンパスに実装した．これらのキャンパスでは，各利用者の VLAN-ID が決まっており，同一キャンパス内であればどこでも同じサブネットに接続されるが，キャンパスを移動すると，実際に接続されるサブネットアドレスが変更される．例えば，倉敷キャンパスに所属する利用者は，認証に成功すると 1359 の VLAN-ID を割り当てられる．この VLAN-ID によって倉敷キャンパス内で利用する場合には 10.17.0.0/23 のサブネットが割り当てられるが，津島キャンパスでは 10.1.102.0/23 が，鹿田キャンパスでは 10.9.102.0/23 が割り当てられる．学外に接続する場合には，NAT によってそれぞれのサブネットに対して割り当てられた固有のグローバル IP アドレスに変換される．このように，ロケーションフリーネットワークシステムを利用しても，学外からはその端末がどこからネットワークに接続しているのかを，送信元 IP アドレスから判別することができる．

4.3 電子ジャーナルのアクセス制限

従来，岡山大学図書館で契約している電子ジャーナルでは，学内に固定的に割り当てられたグローバル IP アドレスをベンダに通知し，電子ジャーナルサーバでサイトライセンスに基づくアクセス制限を行っていた．そこで，生活系ネットワークの運用開始により，4.1.4 節のネットワーク種別について，各キャンパスの生活系ネットワークの NAT 変換後グローバル IP アドレスをベンダに通知した．ベンダでは，各サイトライセンスの範囲に基づいてそのグローバル IP アドレスを追加し，電子ジャーナルサーバへのアクセス制限を更新した．

以上の状況に基づき，我々は生活系ネットワークの利用において，電子ジャーナルへのアクセス制限が正常に機能しているかを検査した．その結果，全キャンパスから利用できるものは適切に利用できることを，特定のキャンパスについてのみ契約されているものは，そのキャンパスからのみ利用できることを確認した．また，VPN 利用者やゲストも適切に利用制限がされていることを確認した．これにより，提案する方法を用いることで，電子ジャーナルのサイトライセンスに適応する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可能であると言える．

5. おわりに

本論文では，認証ネットワークによってどこでも決まった VLAN に接続できる利便性を有しながらも，電子ジャーナルを利用する場合には，利用者が現在どこからアクセスしているのかを判別し，サイトライセンスによるアクセス制限に適応することができる，ロケ

ーションフリーネットワークシステムの構成方法を提案した．また，この方法では，事業所間あるいは特定の領域との通信を IP ルーティングだけでなく，VLAN-ID 変換によっても接続することが可能なため，多様なネットワークトポロジやサイトライセンスに柔軟に対応ができることを示した．さらに，岡山大学のキャンパス情報ネットワークシステムに実装することによって，その有効性を確認した．

今後の課題として，本論文の適用範囲を電子ジャーナルに限らず，場所，所属，身分など利用者個人の属性によって利用条件を変更するサービスへの応用を検討したい．

参考文献

1) Loa Anderson, Tove Madsen: Provider Provisioned Virtual Private Network (VPN) Terminology, RFC4026, IETF (2005)
2) Ralph Droms: Dynamic Host Configuration Protocol, RFC 2131, IETF (1997)
3) Kjeld Borch Egevang, Paul Francis: The IP Network Address Translator (NAT), RFC1631, IETF (1994)
4) アラクサラネットワークス株式会社: ネットワークパーティション,
http://www.alaxala.com/jp/solution/network/npar1.html
5) Carl Rigney, Allan C. Rubens, William Allen Simpson, Steve Willens: Remote Authentication Dial In User Service (RADIUS), RFC 2865, IETF (2000)
6) 岡山県情報政策課:岡山情報ハイウエイとは,
http://www.pref.okayama.jp/page/detail-67451.html
7) 鳥取県情報政策課:鳥取情報ハイウェイ,
http://www.pref.tottori.lg.jp/dd.aspx?menuid=10012
8) アラクサラネットワークス株式会社: AX2400S,
http://www.alaxala.com/jp/products/AX2400S/index.html
9) The FreeRADIUS Project: freeRADIUS The world's most popular RADIUS Server., http://freeradius.org/
10) Juniper Networks, Inc.: SSG520M セキュア・サービス・ゲートウエイ，http://www.juniper.net/jp/jp/products-services/security/ssg-series/ssg520m/
11) F5 Networks Japan K.K.: FirePass,
http://www.f5networks.co.jp/product/firepass/index.html