博　士　論　文

地理的に分散した組織の
ネットワーク構築・運用に関する研究

平 成 ２７ 年 ３ 月

大隅　淑弘

要約

ICT(Information and Communication Technology) は，世界全体に急速に浸透し，産業や社会基盤，企業のビジネスモデル，個人のライフスタイルなど，様々な領域で大きな変化をもたらしている．企業や団体などの組織にとって ICT は極めて重要なインフラであり，ICT の基盤となるネットワークの利活用は組織の活動に大きな影響を与える．情報基盤としてのネットワークは，信頼性，可用性，利便性，セキュリティ，コストへの要求が一段と高まっている．

一方で，計算機システムの性能向上，計算リソースの大規模化，クラウドコンピューティングの拡大などにより，情報システムは従来の集中設置型から，分散配置型への移行が進んでいる．さらに，2011 年 3 月の東北地方太平洋沖地震の教訓や，今後発生が予想されている東海・東南海・南海地震の被害の想定から，BCP(Business Continuity Plan) への取り組みが強化され，情報資源の冗長化やディザスタリカバリの整備が進められている．このような情勢から，地理的に分散配置したサーバを冗長化し，サービスの信頼性と可用性を確保する情報基盤の整備が重要になっている．

本研究では，このような要件に対応するネットワークシステムを構成し，また，実際の運用環境への適用に取り組んだ．

ネットワークシステムの認証機能によって，利用者はロケーションによらず適用範囲内であればどこでも決まったネットワークに接続できる，ロケーションフリーネットワークを構成することができる．しかしながら，電子ジャーナルのサイトライセンスのような，利用者のロケーションに基づいたサービスを利用する場合には，利用者の現在位置が判別できなくなり，契約者である組織は利用者の正当性を保証できない．そこで，このような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を提案する．提案の方法では，認証によって割り当てられる VLAN-ID と，VLAN-ID によるサブネットの対応を，利用者のロケーションによって変更する．利用者のロケーションの違いがクライアントの IP アドレスから判別可能になり，サービス利用者の正当性を保障することができる．本提案に基づいて岡山大学でシステムを構成し，電子ジャーナルのサイトライセンスに適用して実用性を確認した．

前述のロケーションフリーネットワークシステムでは，利用者のロケーションによって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に接続されない特性を有する．そこで，そのような条件が必要な場合に対して，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を提案する．すなわち，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，また，サブネットを越えて通信する場合には，端末の送信元 IP アドレスから利用者の位置情報を識別できる．利用者の位置情報を認証ネットワークから取得し，アクセス先のシステムが識別する端末の送信元 IP アドレスを，位置情報に基づいて変更する．提案方法に基づいた試作システムを構成し，提案どおりに動作することを確認した．また，同時多数の接続を想定した負荷試験を行い，数十台の端末の同時接続も可能であることを確認した．以上より，本提案方法の有効性が確認された．

また，ICT システムの止まらないサービスは重要な課題となっている．サービスの信頼性や可用性の向上のためには，地理的に分散して設置されたサーバを冗長化する構成方法が有効である．従来このような構成方法には，DNS によって冗長化を行うもの，サービスの仕様にサーバの冗長化機能があるもの，クライアントの実装によって冗長化が可能なものがある．しかし，サーバとの通信に大きな遅延が発生したり，ダウンしているサーバに接続しようとしたりする問題がある．ま

た，主系サーバがダウンし待機系にフェイルオーバした後，主系サーバが復旧しても主系サーバにフェイルバックしない問題がある．そこで，本論文では，組織のネットワークにおいて IP Anycast を用いることで，地理的に分散した複製サーバの冗長化構成を提案する．提案の構成では，従前の問題を解決し，さらに主系サーバが復旧すればフェイルバックする．また，IP Anycast は，従来，世界規模や国家規模のような大規模なネットワークに用いられているが，一般的な組織のネットワークにも適用できることを示した．本提案に基づいて試作システムを実装し，有効に機能することを確認した．さらに，組織内の LDAP(Lightweight Directory Access Protocol) サーバに適用し，実用性を確認した．

関連発表論文リスト

1. 論文誌

   1-1 大隅淑弘，山井成良，岡山聖彦，”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”，情報処理学会論文誌 55 巻 3 号 2015 年 3 月発行に掲載予定

   1-2 Y. Ohsumi, K. Okayama and N. Yamai, ”A Configuration of Location Free Network Applicable to Location Dependent Services”, Journal of information processing, Vol.21, No.3, pp.433-440, 2013

2. 国際会議

   2-1 Yoshihiro Ohsumi, Kiyohiko Okayama, Nariyoshi Yamai, Takaoki Fujiwara, Takashi Hieda,”A Location Free Network System Applicable to Geographical Terms of the Electonic Journal Site License”, in Proceedings of the 12th Annual International Symposium on Applications and the Internet (SAINT 2012), pp.357-362, Izmir, Turkey, July 2012.

3. 国内研究会

   3-1 大隅淑弘，山井成良，岡山聖彦，河野圭太，藤原崇起，”地理的に分散したサーバ間のフェイルオーバ・フェイルバックを可能にする複製サーバ冗長化構成”，情報科学技術フォーラム講演論文集，第 12 巻，第 4 号，23 頁〜27 頁，2013 年 9 月

   3-2 大隅淑弘，山井成良，藤原崇起，岡山聖彦，河野圭太，稗田隆，”IP alias と経路制御を用いた複製サーバ冗長化構成”，情報処理学会研究報告 IOT [インターネットと運用技術]，2012-IOT-18 巻，第 4 号，1 頁〜6 頁，2012 年 6 月

   3-3 大隅淑弘，岡山聖彦，山井成良，藤原崇起，稗田隆，”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”，情報処理学会インターネットと運用技術研究会 インターネットと運用技術シンポジウム 2011 論文集，2011 巻，51 頁〜58 頁，2011 年 12 月

   3-4 岡山聖彦，山井成良，大隅淑弘，河野圭太，藤原崇起，稗田隆，”岡山大学における認証・ロケーションフリーネットワークの構築”，学術情報処理研究，第 15 号，161 頁〜165 頁，2011 年 9 月

目 次

第1章　序論

1.1　組織におけるネットワーク

情報基盤としてのネットワークは，1837 年にアメリカのモースがモールス信号を発明したことに始まり，1960 年代に米国防総省による分散型ネットワークである ARPANET によりインターネットの本格的な普及が始まった．日本においては，e-Japan 構想（2000 年〜2005 年）により，通信インフラの整備と普及を進め，u-Japan 構想（2006 年〜2010 年）により ICT(Information and Communication Technology) のさらなる利活用を目指した取り組みが行われた．インターネットの普及当初には，ネットワークは高性能コンピュータや周辺機器などのリソースを遠隔利用するためのものであったが，現在では情報を共有する，情報にアクセスすることが主な目的となっている．また，近年では，モバイルネットワークの発展により，メール，WEB，SNS，IP 電話などのようなモバイルデバイスからのクラウドサービスやオフィスネットワークの利用が進んでいる．情報基盤としてのネットワークは世界全体に急速に浸透し，ICT 産業だけでなく，社会基盤，企業のビジネスモデル，個人のライフスタイルなど様々な領域で大きな変化をもたらしている．ネットワークは，あらゆる分野であらゆる目的で利用されるようになった．ネットワークの通信速度においては，端末の通信速度は 1 ギガビット/秒が一般的となった．組織のバックボーンにおいては，10 ギガビット/秒，40 ギガビット/秒のネットワークシステムが普及しており，単一波長で 100 ギガビット/秒のシステムの普及も始まっている．インターネットのトラフィック量は爆発的に増えており，10 年後には現在の数百倍になるとも推測されている．一方で不正アクセスやコンピュータウイルスによる情報の漏洩，改竄，破壊，DoS 攻撃 (Denial of Service Attack) などのサービス妨害なども深刻な問題であり，ネットワークにおけるセキュリティ対策も重要な課題となっている．

企業では，近年のクラウド化へのシフトによってビジネスの効率やスピードが大きく改善されている．ビジネスの要求内容に応じて必要とされるシステムの拡張，縮小が簡単に実行できるようになった一方で，ネットワークへの依存性は極めて高くなっている．ネットワークが停止するとあらゆる情報資源にアクセスできなくなり，ビジネスに支障を来す．企業にとってネットワークの信頼性や可用性は，ビジネスの重要な構成要素である．また，コスト削減も重要な要件であり，ICT システムの構築や運用のためのコストダウンも要求されている．

大学や研究機関のネットワークは，研究者や学生による研究，教育のためにオープンで自由であると同時に，クローズドであることが必要である．組織の構成員だけでなく，学会や外部の研究者などの一時的な来訪者にも柔軟に対応する．組織内部に持ち込まれる端末も様々である．大学や研究機関においては，守るべき情報を適切に保護できるセキュリティとともに，便利で自由に利用できることが必要である．

国や自治体などの公共機関では，ICT によるサービス提供の取り組みが進んでいる．ネットワークの停止は公共サービスの停止につながり，住民の生活に支障をきたすことになる．このため，止まらないサービス，止まらないネットワークが重要になっている．また，公共団体では，特に個人情報などの秘匿性の高い情報を扱うため，高いセキュリティが要求されている．

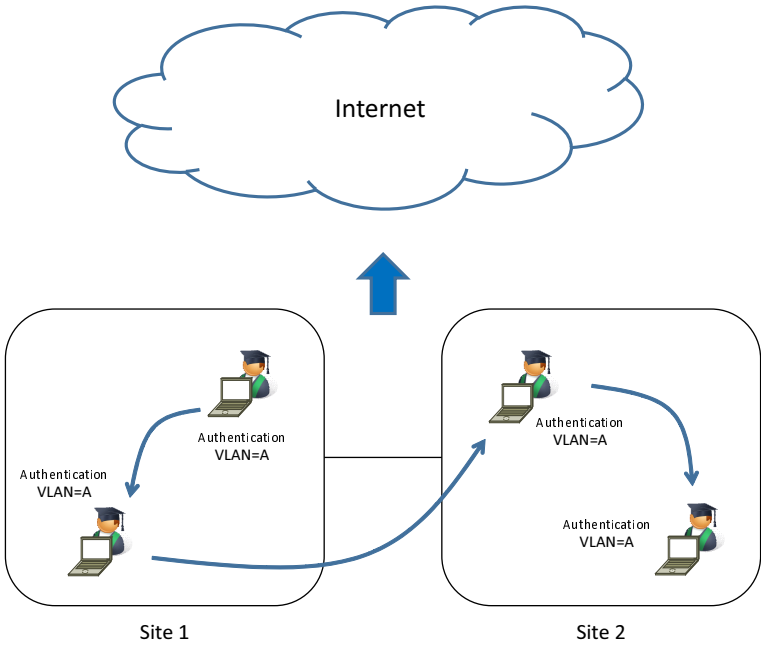


図 1.1: ロケーションフリーネットワーク

一方で，組織における情報システムは，情報機器の高性能化と低価格化，ネットワークの高速化，クラウドコンピューティングの拡大などにより，従来の集中設置型から，分散配置型への移行が進んでいる．さらに，2011 年 3 月の東北地方太平洋沖地震の教訓や，今後発生が予想されている東海・東南海・南海地震の被害の想定から，BCP(Business Continuity Plan：事業継続計画)への取り組みが強化され，情報資源の冗長化やディザスタリカバリの整備が進められている．このような情勢から，地理的に分散配置したサーバを冗長化し，サービスの信頼性と可用性を確保する情報基盤の整備が重要になっている．

企業，団体，その他，様々な組織にとって，ネットワークは極めて重要なインフラであり利活用の成否は組織の活動に大きな影響を与える．ネットワークは，信頼性，可用性，利便性，セキュリティ，コストへの要求が一段と高まっている．

1.2　ネットワークシステムの現状

近年のネットワークシステムでは，端末をネットワーク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者を排除するだけでなく，ダイナミックな VLAN の割り当て（以下，ダイナミック VLAN と記す）によって，どこでも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．以下，このようなネットワークをロケーションフリーネットワークと呼ぶ．ロケーションフリーネットワークでは，利用者は組織内のどでも同じネットワークに接続できる利便性を有しているため，多くの組織で導入が進んでいる．図 1.1 にロケーションフリーネットワークを示す．

ICT システムの信頼性や可用性を保障するために冗長化が用いられる．ネットワーク機器の冗長化では従来の構成方法として，物理的な多重化，冗長化プロトコルを用いる方法，仮想化技術を用いる方法がある．一般的な例としては，スタック，FT(Fault Tolerant)，VRRP(Virtual Router

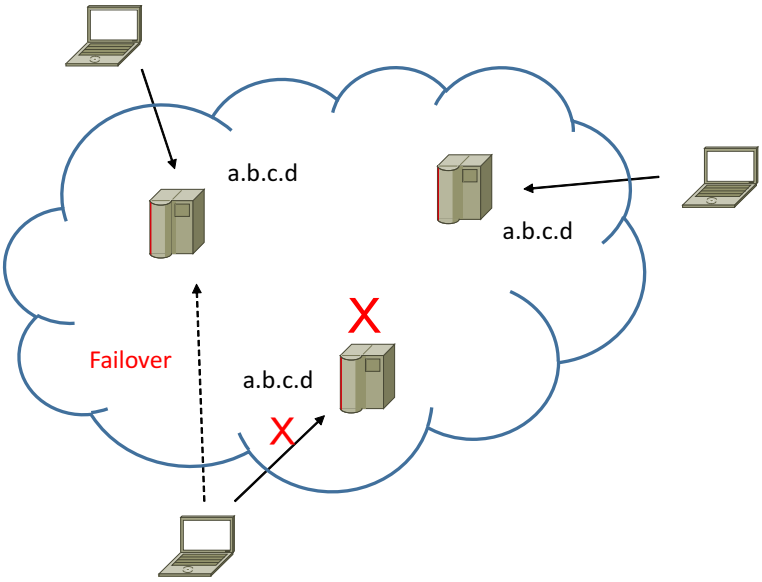


図 1.2: IP Anycast

Redundancy Protocol)[1]，シスコ社の VSS(Virtual Switching Supervisor) などがある．通信回線の冗長化では，組織内においては，STP(Spanning Tree Protocol)，LAG(Link Aggregation) などが用いられている．遠隔の拠点間や組織間などの接続においては，リングプロトコル [2] や回線のフルメッシュ型トポロジーなどが一般に利用されている．

また，情報提供サービスの可用性を保証するために，サーバの冗長化が行われる．冗長化には，ロードバランサを用いる方法，仮想化システムにおいて HA(High Availability) 構成や FT 構成を用いる方法が一般的であるが，サーバルームにサーバを集中設置することが前提となる．一方，地理的に分散して設置（以下，分散配置と記す）されたサーバを冗長化したい場合がある．例えば，大きな組織で複数の拠点があり，サーバを分散配置することでサービスの信頼性を保障したり，BCP を整備したりする場合である．地理的に分散とは，各サーバが異なるサブネットに属し，両者の間には少なくとも 2 台のルータが存在するような場合である．このような場合，ロードバランサや HA，FT は適していない．

分散配置されたサーバの冗長構成方法に IP Anycast[3] がある．IP Anycast は，ネットワーク的に分散配置された複数のホストに，1 つの IP アドレスを同時に割り当てることで，ルーティングトポロジーにおいて，クライアントから最も近いホストと通信を行う．ホストの障害時には経路が更新されることにより，他の場所にある別のホストに自動的に接続変更されてサービスを継続する．また，平均応答時間の短縮や DDoS(Distributed Denial of Service) 攻撃の効果を抑制する効果もある．IP Anycast は，従来 DNS(Domain Name System)[4] のルートサーバの冗長化のようなステートレスなプロトコルを対象に用いられてきた [5] が，近年では CDN(Contents Delivery Network) による WEB 配信サービスや，サーバのロードバランサへの適用例 [6] もある．文献 [7] では，DNS の TXT レコードを用いて既存の IP Anycsat の実装を評価している．IP Anycast の動作を図 1.2 に示す．

1.3 本研究の目的

1.2 節のとおり，ロケーションフリーネットワークを構成することで，ネットワークにおける利便性やセキュリティを向上することができる．しかし，ロケーションフリーネットワークを通常の方法で構成すると，利用者のロケーションに基づいたサービスを利用する場合に問題が生ずる．すなわち，利用者は認証できる範囲であればどこでも決まった VLAN に接続されるため，利用者がどの場所からサービスにアクセスしているのか識別できず，サービスの契約者である組織は，利用者の正当性を保証できない．このようなサービスの例として，クライアントの IP アドレスに基づいてアクセス制限をする電子ジャーナルのサイトライセンスがある．この問題の解決のため，利用者のロケーションに基づいたサービ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の構成に取り組む．また，本提案に基づいてシステムを試作して評価することで有効性を確認する．さらに，実際のネットワークに適用して実用性を検証する．

次に，2 つ目の問題の解決に取り組む．前述のロケーションフリーネットワークシステムでは，利用者がロケーションの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特性がある．そこで，このような要件が必要な場合に対して，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を提案する．すなわち，利用者のロケーションに基づいたサービスに適応し，端末のネットワーク接続においては，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する．本提案に基づいたシステムを試作して評価することで有効性を確認する．

最後に，サービスの信頼性と可用性を向上させるため，地理的に分散配置したサーバを冗長化する目的に取り組む．このような場合の構成方法には，従来サービスの仕様にサーバの冗長化機能を有しているもの，DNS によって冗長化を行う方法，クライアントの実装によって冗長化を行う方法があるが，それぞれ問題点を有している．すなわち，停止しているサーバへの接続がタイムアウトしなければ次のサーバに接続されなかったり，停止しているサーバに接続しようとしたりする問題である．また，サーバの障害でフェイルオーバした後でそのサーバが復旧してもフェイルバックしない問題がある．そこで，一般的な組織において，分散配置されたサーバのこのような問題を解決するための冗長化を行う．提案方法に基づいてシステムを試作して評価することで有効性を確認する．さらに，実際のネットワークに適用して実用性を検証する．

1.4 本論文の構成

本論文の構成について述べる．まず，2 章では従来のネットワーク構成方法と問題点について述べる．次に，3 章で利用者のロケーションに基づいたサービ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について述べる．また，本論文に基づいて構成したシステムを評価するとともに，電子ジャーナルのサイトライセンスに適用した結果を述べる．4 章では，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について述べる．また，本論文に基づいて試作したシステムによって有効性を評価する．5 章では，地理的に分散したサーバ間のフェイルオーバ・フェイルバックを可能にする複製サーバ冗長化構成について述べる．本論文に基づいて構成した試作システムを評価し，さらに，LDAP サーバに適用した結果について述べる．最後に，6 章では本論文の成果を要約し，今後の課題について述べる．

第2章　従来のネットワーク構成方法と問題点

2.1　利用者のロケーションに基づいたサービスの利用と問題点

2.1.1　想定するネットワークの環境

利用者のロケーションに基づいたサービスの例として，電子ジャーナルのサイトライセンスがある．本論文では，各電子ジャーナルの契約はサイトライセンスであり，その組織に所属する者だけが利用できるものとする．利用者のロケーションによって，各電子ジャーナルの利用条件が異なっている．また，組織には地理的に離れた 2 つ以上の拠点があるものとする．拠点とは，例えば大学ではキャンパス，企業では支店，営業所，工場などのような場所である．

次の利用者がロケーションフリーネットワークによって，組織内外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．電子ジャーナルへのアクセスのモデルを図 2.1 に示す．

- 組織に所属する利用者が，組織内で端末をネットワークに接続している．
  以下，この利用者を一般利用者と記す．
- 組織に所属する利用者が，組織外から VPN(Virtual Private Network)[8] 接続によって端末を組織内のネットワークに接続している．
  以下，この利用者を VPN 利用者と記す．
- 組織に所属しない来訪者が，組織内で端末をネットワークに接続している．
  以下，この利用者をゲスト利用者と記す．

2.1.2　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，サイトライセンスが一般的である．サイトライセンスでは，電子ジャーナルベンダ（以下，ベンダと記す）と契約者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．この条件は，利用者の所属に関して契約されることが多いが，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しなければならない．利用者が契約範囲内であるかどうかの判定方法として，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．IP アドレスを用いる場合，組織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を許可する．プロキシサーバを用いる方法では，プロキシサーバに接続する利用者を認証し，電子ジャーナルではそのプロキシサーバについて接続を許可する．近年，利用者の認証方法として，Shibboleth 認証 [9] も広く利用されている．電子ジャーナルによっては，日本における学術認証フェデレーションの GakuNin[10] に対応しており，Shibboleth 認証

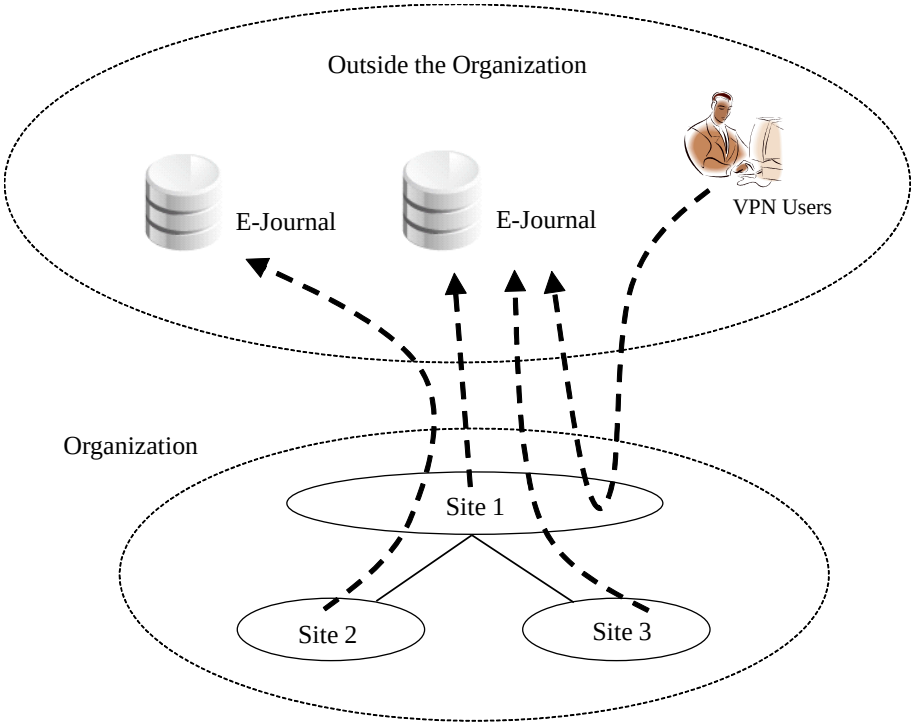


図 2.1: 電子ジャーナルへのアクセス

に基づいたアクセス制限を行っている．Shibboleth 認証では，利用者のロケーションにかかわらず電子ジャーナルに接続が可能である．

2.1.3 ロケーションフリーネットワーク

近年，認証機能を有したレイヤ 2 スイッチやレイヤ 3 スイッチでは，端末がネットワーク接続されると認証を行い，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．認証方式としては，MAC アドレス認証，WEB 認証（ユーザ認証），EAP(Extended Authentication Protocol)[11] を用いる IEEE802.1X 認証 [12] などが一般的に利用されている．また，これらの認証を組み合わせて利用するマルチステップ認証が可能なスイッチもある．このようなネットワークスイッチを用いることで，利用者がどこでネットワークに接続しても，同じ VLAN に接続できるロケーションフリーネットワークを構成することができる．従来のネットワークでは，場所や建物などによって固定的な IP アドレス割り当てを行っていため，利用者が場所を移動すると移動先の IP アドレスを使用する必要があった．

本論文では，ロケーションフリーネットワークについて次の定義を用いる．

定義 1 利用者はどこでも同じ VLAN-ID のサブネットに接続できる

定義 2 利用者はどこで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できる

定義 1 は，利用者の属性値である VLAN-ID によってロケーションフリーネットワークを構成するために必要な要件である．ただし，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性は保障されない．このような場合，例えば，NAS(Network Attached Storage) やサーバな

どの情報資源へのアクセスを，IP アドレスで制限していると利用できないことがある．そのような要件が必要な場合に対して定義 2 を用いる．定義 1 は 3 章で，定義 2 は 4 章で用いる．

ネットワーク接続において認証が成功すれば，端末は属性による VLAN-ID のサブネットに接続され，DHCP(Dynamic Host Configuration Protocol)[13] サーバから IP アドレスを取得してネットワーク利用が可能になる．本論文では，認証方式は WEB 認証，MAC 認証であり，ダイナミック VLAN の方法は MAC アドレスベース VLAN を想定する．このような条件は，例えばアラクサラ社の AX2400S[14] のような，一般的な L2 スイッチを用いて構成が可能である．

また，認証情報について，近年，多くの大学では統合的な認証基盤の整備が進んでおり [15][16][17][18]，このような統合認証基盤を用いることで，人事情報や学務情報に基づいたシームレスなユーザ ID 管理が可能になっている．この認証情報をロケーションフリーネットワークに利用することができる．

2.1.4 ロケーションフリーネットワークの問題点

ロケーションフリーネットワークでは，適用範囲内では利用者はどこでも同じサブネットに端末を接続することができるが，ネットワークの構成や電子ジャーナルの利用において問題が生ずる．

(1) ネットワーク構成の問題点

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，全ての拠点に全ての VLAN を通してネットワークを構成することである．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通過するため，接続端末数においてネットワークの規模が大きくなると，バックボーンに十分な帯域がなかったり，複数の拠点のある組織で各拠点間の通信回線に十分な帯域がなかったりする場合には構成できない．

これに対し，全ての拠点に全ての VLAN を運用してロケーションフリーネットワークを構成するが，各拠点間の VLAN を分離し，プロキシサーバあるいは NAT(Network Address Translation)[19] によって接続する方法が考えられる．この方法であれば，バックボーンや拠点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，高速な通信回線がなくても構成できる．しかし，各拠点でプロキシサーバや NAT を運用する負担が生じたり，拠点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 に施す負担が生じたりする問題がある．

また，ロケーションフリーネットワークを各拠点で独立に構成し，各拠点で別々の VLAN を割り当てれば，拠点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．しかし，この場合には認証情報を各拠点で個別に運用する必要があるため，拠点毎に個別に認証サーバを運用するなどの負担が生じる．

(2) サイトライセンスの利用における問題点

また，ロケーションフリーネットワークを運用している組織が，電子ジャーナルのサイトライセンスを契約する場合に問題が生ずる．サイトライセンスを組織の一部，例えば，特定の拠点や拠点内の特定の場所に限って契約している場合である．すなわち，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できなくなり，サイトライセンスによる利用者の

範囲を保証できない．また，VPN 利用者やゲスト利用者についても判別する必要がある．なお，利用者はどこからでも電子ジャーナルにアクセスするので，2.1.2 節で述べたように，Shibboleth 認証ではこの問題に対応できない．

2.2 分散配置したサーバの冗長化と問題点

これまでにもサーバの分散配置が可能な冗長化構成方法はいくつか知られているが，それぞれ問題点を有している．以下では，代表的な冗長化構成方法とその問題点を述べる．

2.2.1 サービスの仕様による冗長化

サービスによっては，冗長化機能がその仕様に含まれているものがある．たとえば，DNS ではコンテンツサーバの冗長化が仕様 [4] に含まれており，一部のサーバが停止した場合でもサービスを継続することが可能である．クライアントはリゾルバに複数の DNS サーバを登録しておくことで，参照する DNS キャッシュサーバを冗長化することができるが，多くの実装では DNS サーバの参照は設定された順番に行われる．このため，1 番目のサーバで障害が発生している場合にも，まず 1 番目のサーバが参照され，タイムアウトするまでは次のサーバが参照されず，クラアントは毎回タイムアウトの発生を待たなければならない．

別のサービスとして，SMTP[20] がある．SMTP も 1 つのドメインに対して複数の MX レコードを DNS サーバに登録することにより，MTA (Mail Transfer Agent) の冗長化を行うことができる．しかし，MTA の選択は MX レコードに付随した優先度（同じ優先度の場合にはランダム）によって決定される．このため，DNS と同様に優先度の高い MTA に障害が発生している場合には，送信 MTA ではタイムアウトを待たなければ次の優先度の MTA に接続されない．

2.2.2 DNS による冗長化

DNS Round Robin[21] は，1 つの FQDN(Fully Qualified Domain Name) に対して複数のサーバそれぞれの IP アドレスを A レコードとして登録し， その FQDN の問合せに対してその A レコードを順番を変えて返す技法である．クライアントは複数の A レコードのうち任意のものを使用することが許されるが，多くの実装では最初の A レコードを使用するため，応答中の A レコードの順番を変更することによりサーバへのアクセスを分散させることができる．この技法の本来の用途はサーバ間の負荷分散であるが，アクセスしようとしたサーバに障害が発生していた場合でも，クライアントが次の A レコードを参照したり，もう一度 DNS サーバに問い合わせたりするなどの方法で別のサーバへのアクセスを試みる機能を有していれば，冗長化にも DNS Round Robin を用いることができる．

しかし，どれかのサーバに障害が発生していても，DNS サーバはその事実を認識しないため，障害が発生したサーバの IP アドレスが最初の A レコードとしてクライアントに返された場合には，クライアントはタイムアウトが発生するまで目的のサーバにアクセスできない．また，最初の A レコードに対応するサーバがネットワーク的に遠方にある場合には，無駄なトラフィックが発生したり，遅延時間が大きくなったりする問題が生じる．

経路情報をもとに DNS の応答を最適なサーバへ誘導する手法が提案されている [22]．これは，クライアントからの DNS クエリに対して，最適なサーバを回答することで負荷分散を行う．しかし，この方法では DNS の A レコードを変更しても，DNS レコードの TTL(Time To Live) を無視して，変更前の A レコードを使ってアクセスする端末のあることが報告されている [23]．また，GeoDNS サービスにより，クライアントから見たサーバの位置に応じて，DNS の応答を変えることも可能であるが，この場合も一部の端末が DNS レコードの TTL を無視する問題がある．さらに，その位置精度は，国，都市，ISP(Internet Services Provider) などの広範囲なものであり，組織におけるサーバの冗長化には適していない．

2.2.3　クライアントの実装による冗長化

クライアントの実装によっては，サーバの指定において同一の機能を持つ複数のシステムを指定できるものがある．例えば，Dovecot[24] で LDAP(Lightweight Directory Access Protocol)[25] 認証を利用する場合，複数の LDAP サーバを設定することにより，それまでアクセスしていたサーバに障害が発生した時点で自動的に次のサーバにアクセスし，以降はこのサーバを使い続ける（以下，この動作をフェイルオーバと記す）機能を有している．この機能により，クライアントはフェイルオーバ後にタイムアウトの発生を待つことなく直ちにサーバにアクセスすることができる．このようなフェイルオーバ機能を持つクライアントは Dovecot 以外にも多数存在する．

ところが，最初にアクセスしていたサーバに障害が発生してフェイルオーバが起こり，その後サーバが障害から復旧した場合，本来であれば復旧した時点でアクセス先は元のサーバに戻る（以下，この動作をフェイルバックと記す）べきであるが，多くの実装ではフェイルバックしない．このような状況では，複数のサーバ間で負荷分散が適切に行われなくなったり，ネットワーク的に遠いサーバにアクセスするため，無駄なトラフィックが発生したりする問題がある．岡山大学情報統括センターでは，POP3(Post Office Protocol)[26] や IMAP(Internet Message Access Protocol)[27] のサーバとして Dovecot を使用しており，地理的に離れて設置された 2 台の LDAP サーバを設定して参照しているが，実際にこのような問題が発生した．

この問題に対処するには，たとえば一定時間ごとにフェイルバックが可能であるかどうかを調べる機能の追加が考えられる．しかし，既存のクライアントの多くはこのような機能は有しておらず，また同機能の追加実装もソースプログラムが公開されているものを除き一般的には容易ではない．

第3章　利用者のロケーションに基づいたサービ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

3.1　システムの概要と設計

2.1.4 節のとおり，ロケーションフリーネットワークを従来の方法で構成すると，利用者のロケーションに基づいたサービスを利用する場合に問題が生ずる．そこで，このようなサービスに適用できるロケーションフリーネットワークの新たな構成方法が必要になる．また，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．

本章では，VLAN-ID とサブネットの割り当て方法を工夫することで，このような問題を解決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を提案する．本章においては，電子ジャーナルのサイトライセンスのような，利用者のロケーションに基づいたサービスに適応することを目的とするため，ロケーションフリーネットワークの定義は，2.1.3 節の定義 1 を用いる．

3.1.1　認証結果による VLAN-ID に対するサブネットの割当

2.1.4 節 (2) で述べた問題は，VLAN-ID 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，認証によって VLAN-ID が決定すると，利用者の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ため，利用者がどのロケーションにいるのかがクライアントの IP アドレスから判別できない．

この問題に対して，認証によって割り当てられる VLAN-ID はどこでも同じであるが，VLAN-ID に対して割り当てられるサブネットを利用者のロケーションによって変更する構成方法を提案する．この方法では，利用者のロケーションによってサブネット IP アドレスが異なるため，どこからネットワークに接続しているのかを IP アドレスから判別可能となる．電子ジャーナルのサイトライセンスのような利用者のロケーションに基づいたサービスの利用に適応することができる．さらに，2.1.4 節 (1) で述べたような認証情報やサーバを必要としない利点を有する．

3.1.2　レイヤ 3 スイッチの VRF 機能による拠点間の接続

近年，多くの組織では，セキュリティや運用ポリシーの理由で VRF(Virtual Routing and Forwarding)[28] 機能を有するレイヤ 3 スイッチを導入している．VRF によって 1 台のルータに仮想的に複数のルータを作成することができる．各仮想ルータによって VRF ドメインと呼ばれるサブネットのグループを形成し，各 VRF ドメインをネットワーク的に分離することができる．各 VRF ドメイン間は，IP ルーティングやファイアウォールで接続することで，運用ポリシーに基づいた通信制御が可能になる．以下では，ルータとレイヤ 3 スイッチを総称して L3 スイッチと記す．

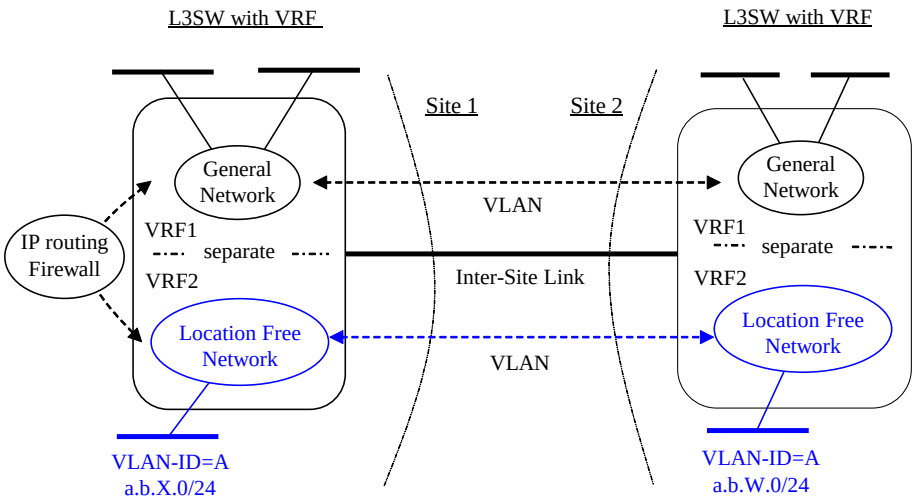


図 3.1: VRF 機能を有した L3 スイッチによる拠点間の接続

図 3.1 では，一般的なネットワークとロケーションフリーネットワークが VRF によって分離されており，拠点 1 の VRF は拠点 2 の対応する VRF と接続している．各 L3 スイッチでは同じ VLAN-ID で異なったサブネットを運用する．利用者の端末の IP アドレスが拠点 1 と拠点 2 で異なるため，ロケーションに依存したサービスを提供するサーバでは，クライアントの IP アドレスから利用者の現在のロケーションを判別することができる．図 3.1 において，ロケーションフリーネットワークに接続しているクライアントの IP アドレスが，a.b.X.0/24 であれば拠点 1 からの接続であり，a.b.W.0/24 であれば拠点 2 からの接続であることが判別できる．

3.1.3 VLAN-ID 変換による接続

(1) VLAN-ID 変換による拠点間の接続

図 3.1 において，拠点 2 の L3 スイッチが VRF 機能を有しない場合，拠点 1 の VRF を拠点 2 の L3 スイッチに通常の方法で接続すると問題が生ずる．すなわち，拠点 1 の全ての VRF が拠点 2 の L3 スイッチで IP ルーティングによって接続されるためである．拠点 2 の L3 スイッチでアクセスリストによる接続制御をすることも考えられるが，サブネットが多い場合は，接続制限する VLAN とルーティングが必要な VLAN の設定が複雑になり，事実上運用が困難である．この場合，拠点 1 の VLAN を拠点 2 に接続し，拠点 2 ではルーティングしない VLAN として運用することで，拠点 1 の VLAN が拠点 2 で接続されることなく運用可能となる．しかし，この場合には拠点 1 と拠点 2 のサブネットが同じになるため，クライアントの IP アドレスからロケーションの判別ができない．

そこで，VRF 機能を有しない拠点との接続においては，VLAN-ID 変換をする構成方法を提案する．VLAN-ID 変換による接続を図 3.2 に示す．図 3.2 において，拠点 1 の VLAN-ID=B のサブネットは拠点 2 との接続において VLAN-ID 変換を行い，拠点 2 では VLAN-ID=A として運用する．利用者が拠点 1 で端末をネットワークに接続すると，VLAN-ID=A が割り当てられて a.b.X.0/24 のサブネットに接続される．同じ利用者が拠点 2 で端末を接続をすると VLAN-ID=A が割り当て

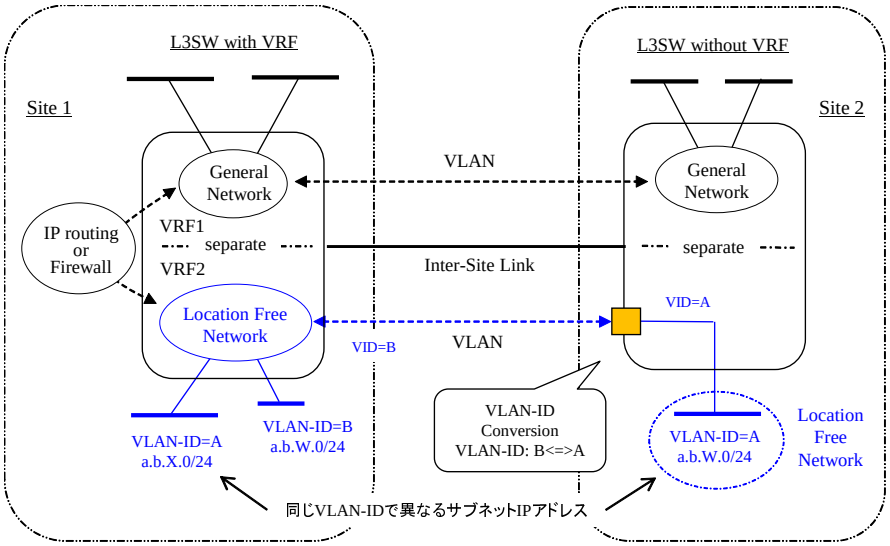


図 3.2: L3 スイッチの VLAN-ID 変換による拠点間の接続

られるが，サブネットは a.b.W.0/24 になる．電子ジャーナルへのアクセスでは，拠点 1 と拠点 2 でクライアントの IP アドレスが異なるため，ロケーションの判別が可能になる．VLAN-ID 変換は，拠点 1 と拠点 2 のどちらで実行してもよいが，その VLAN-ID は各拠点の L2 スイッチあるいは L3 スイッチにおいて，他のセグメントに使用されていないことを条件とする．L3 スイッチが VLAN-ID 変換の機能を有していない場合は，VLAN-ID 変換のための L2 スイッチを用いるなどの構成が可能である．シスコ社やアラクサラネットワークス社などの一般的な L2 スイッチは VLAN-ID 変換機能を有している．

(2) VLAN-ID 変換による拠点内の接続

ロケーションに基づいたサービスが拠点内の特定の場所だけに制限されている場合は，その場所を他の場所と区別する必要がある．例えば，大学が契約している電子ジャーナルが特定の学部や学科についてのみ利用を許可している場合は，電子ジャーナルのサーバでは該当の利用者についてのみアクセスを受け付ける必要がある．特定の学部や学科には L2 スイッチが設置され，拠点の L3 スイッチと接続されている．このような場合にも VLAN-ID 変換が利用できる．VLAN-ID 変換による L2 スイッチとの接続を図 3.3 に示す．図 3.3 において利用者は組織内では VLAN-ID=A が割り当てられる．利用者がこの拠点内にいる時には，接続されるサブネットは a.b.X.0/24 になるが，場所 α にいるときには L3 スイッチにおける VLAN-ID=B である a.b.W.0/24 になる．

3.1.4 ロケーションに基づくサービスへの適用

提案の構成方法により，端末の IP アドレスからその利用者の現在のロケーションが識別できるため，ロケーションに基づくサービスを提供しているプロバイダでは，サーバやファイアウォールなどによって，クライアントの IP アドレスによるアクセス制限をすることができる．電子ジャーナルでは，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，ライセンスの条件に適

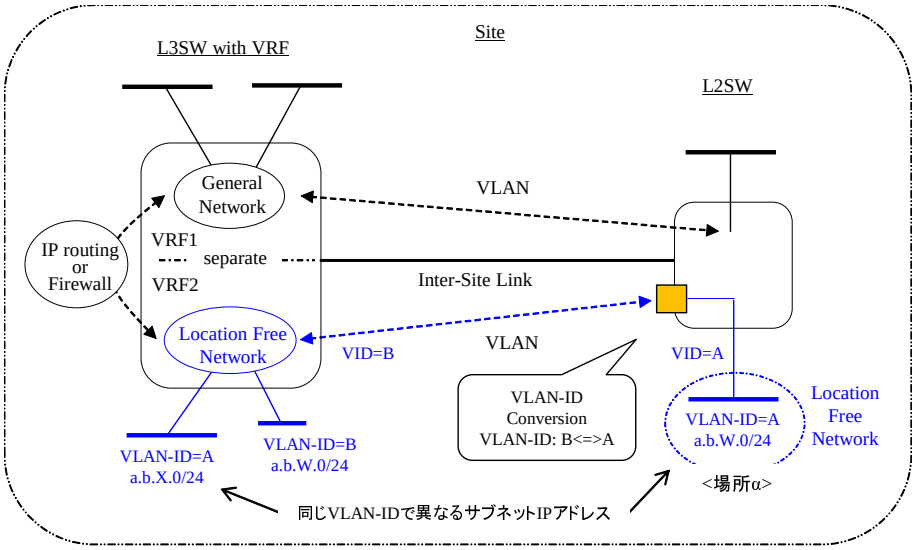


図 3.3: VLAN-ID 変換による L2 スイッチとの接続

合する．また，利用者はロケーションフリーネットワークにより，便利にネットワークを利用することができる．

この構成方法では，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 利用者やゲスト利用者などにも適用することができる．さらに認証情報として利用者や端末の様々な属性情報を使用すれば，多様なアクセス制御を行うことができる．

3.1.5 システムの構成

本提案基づいたシステムの構成例を図 3.4，図 3.5 に示す．図 3.4 は組織のネットワークがグローバル IP アドレスで運用されている場合，図 3.5 はプライベート IP アドレスで運用されている場合である．システムは，RADIUS(Remote Authentication Dial In User Service)[29] サーバ，DHCP サーバ，レイヤ 3 スイッチ，レイヤ 2 スイッチ，認証機能を有したレイヤ 2 スイッチ（以下，認証スイッチと記す）で構成している．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 ルータを用いる．

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．認証が成功すると，端末が VLAN-ID による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て通信が可能になる．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 サーバに問い合わせる構成も可能である．

図 3.4，図 3.5 において，拠点 1 と拠点 2 の L3 スイッチは VRF 機能を有しているが，拠点 3 では VRF 機能を有していないため，VLAN-ID 変換を利用している．各 L3 スイッチで運用するサブネットを図 3.4，図 3.5 に示している．拠点 3 における VLAN-ID=A のセグメントは，拠点 1 におけるロケーションフリーネットワークである VLAN-ID=C のサブネットを VLAN-ID 変換によって接続しているため，サブネット IP アドレスは a.b.Z.0/24 になる．拠点 1 の場所 α では，VLAN-ID

変換機能を有したL2スイッチが設置されている．場所αにおけるVLAN-ID=Aのセグメントは，拠点1のロケーションフリーネットワークであるVLAN-ID=Bのサブネットを VLAN-ID変換により接続していることにより，サブネットIPアドレスは，a.b.W.0/24になる．

VPN利用者は個人に割り当てられているVLAN-IDによらず，すべてVLAN-ID=Vを割り当てる．一般利用者，ゲスト利用者，VPN利用者に割り当てられるVLANは，それぞれVLAN-ID=A，VLAN-ID=G，VLAN-ID=Vである．なお，簡略化のためにVPNサーバは図3.4，図3.5には記載していない．

3.1.6 端末接続におけるシステムの動作

(1) アクセス制限の適用

組織は，K，L，M，Nの4つの電子ジャーナルのサイトライセンスを契約しており，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，組織内の全ての場所からとVPN利用者の利用が可能である．また，電子ジャーナルLは拠点1から，Mは拠点2から，Nは拠点1の場所αからのみ利用が可能である．各電子ジャーナルの利用を表3.1，表3.2に示す．表3.1は組織内のネットワークがグローバルIPアドレスで運用されている場合，表3.2はプライベートIPアドレスで運用されている場合である．電子ジャーナルのプロバイダは，表3.1や表3.2に基づくアクセス制限を行う．

(2) グローバル IP アドレスにおける動作

図3.4において，利用者が端末を組織のネットワークに接続するためには，組織内のいずれかの認証スイッチに接続するか，あるいは学外からVPNサーバに接続をする．利用者の端末は次の手順でネットワークに接続される．

1. 端末が組織内のネットワークに接続されると，認証スイッチあるいはVPNサーバが認証サーバに対して認証要求をする．認証が成功するとRADIUSサーバが認証結果とVLAN-IDを回答する．組織内で端末を接続する場合は，割り当てられるVLAN-IDは，AまたはGとなる．VPN利用者の場合，RADIUSサーバが回答するVLAN-IDはV以外のものとなるが，3.1.5節で述べたようにVPNサーバでは，VPN利用者のVLAN-IDは全てVを割り当てる．

2. 認証スイッチが，端末をVLAN-IDがAまたはGのVLANに接続する．VPNサーバでは，端末をVLAN-ID=VのVLANに接続する．それぞれの端末は次のようにサブネットに接続される．

   (a) VPN利用者の端末は利用者のVLAN-IDによらず，常にa.b.V.0/24のサブネットに接続される．

   (b) ゲスト利用者の端末はVLAN-ID=Gであるa.b.G.0/24のサブネットに接続される．このサブネットは全てのサイトで共通に運用している．

   (c) 拠点1の場所αを除いて，VLAN-ID=Aは拠点1のロケーションフリーネットワークのVRFであるa.b.X.0/24のサブネットである．一般利用者が場所αを除く拠点1にいるときには，端末はa.b.X.0/24のサブネットに接続される．

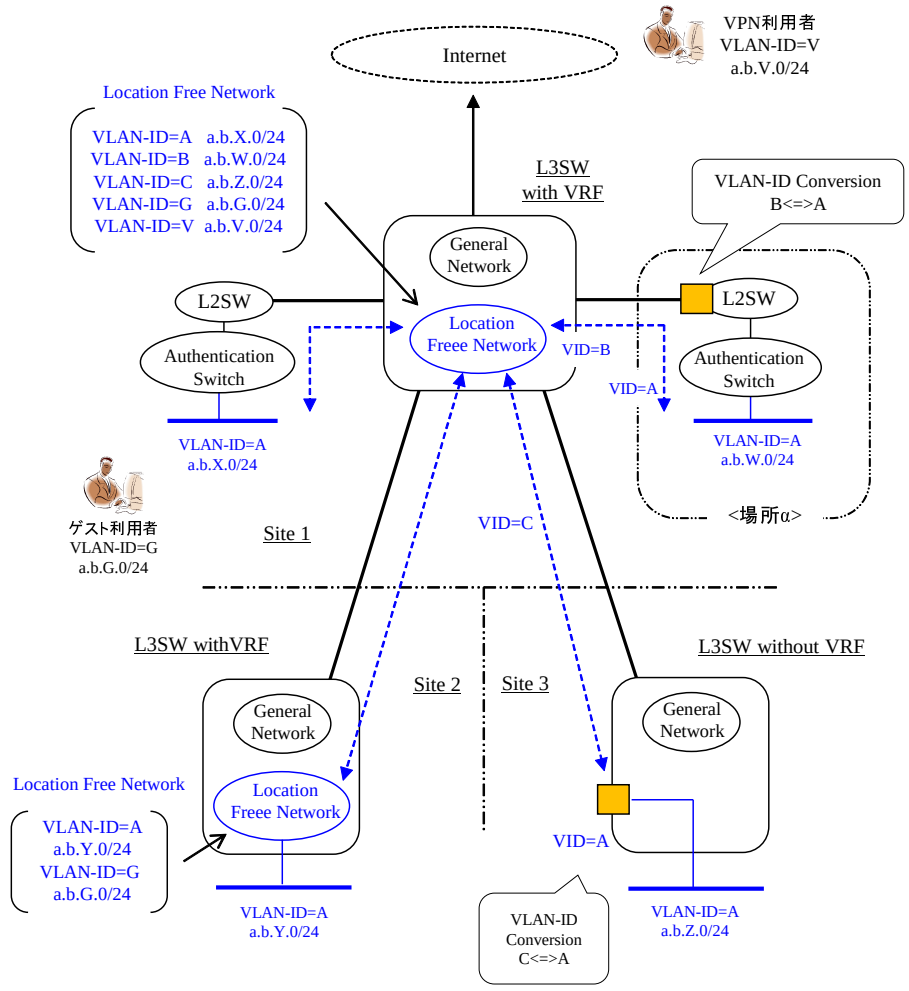


図 3.4: グローバル IP アドレスにおける構成

(d) 拠点 2 において，VLAN-ID=A は拠点 2 のロケーションフリーネットワークの VRF である a.b.Y.0/24 のサブネットである．一般利用者が拠点 2 にいるときには，端末は a.b.Y.0/24 のサブネットに接続される．

(e) 拠点 3 において VLAN-ID=A は，拠点 1 のロケーションフリーネットワークの VRF である VLAN-ID=C の a.b.Z.0/24 を VLAN-ID 変換によって接続している．一般利用者が拠点 3 にいるときには，端末は a.b.Z.0/24 のサブネットに接続される．

(f) 拠点 1 の場所 α では，VLAN-ID=A は，VLAN-ID 変換により拠点 1 の VRF である VLAN-ID=B の a.b.W.0/24 に接続している．一般利用者が場所 α にいると，端末は a.b.W.0/24 のサブネットに接続される．

端末が VLAN によるサブネットに接続されると，DHCP サーバから IP アドレスがリースされる．電子ジャーナルサーバではクライアントの IP アドレスに基づくアクセス制限が可能になる．

表 3.1: グローバル IP アドレスにおける電子ジャーナルの利用

利用者とロケーション (IP アドレスレンジ)	電子ジャーナル			
	K	L	M	N
場所 α を除く拠点 1 の一般利用者 (a.b.X.0/24)	○	○		
拠点 1 の場所 α の一般利用者 (a.b.W.0/24)	○	○		○
拠点 2 の一般利用者 (a.b.Y.0/24)	○		○	
拠点 3 の一般利用者 (a.b.Z.0/24)	○			
VPN 利用者 (a.b.V.0/24)	○			
ゲスト利用者 (a.b.G.0/24)				

表 3.2: プライベート IP アドレスにおける電子ジャーナルの利用

利用者とロケーション (IP アドレスレンジ)	グローバル IP アドレス	電子ジャーナル			
		K	L	M	N
場所 α を除く拠点 1 の一般利用者 (p.q.X.0/24)	e.f.g.h1	○	○		
拠点 1 の場所 α の一般利用者 (p.q.W.0/24)	e.f.g.h4	○	○		○
拠点 2 の一般利用者 (p.q.Y.0/24)	e.f.g.h2	○		○	
拠点 3 の一般利用者 (p.q.Z.0/24)	e.f.g.h3	○			
VPN 利用者 (p.q.V.0/24)	e.f.g.h5	○			
ゲスト利用者 (p.q.G.0/24)	e.f.g.h6				

(3) プライベート IP アドレスにおける動作

図 3.5 は組織のネットワークがプライベート IP アドレスの場合である．組織内のプライベート IP アドレスである，p.q.0.0/16 が NAT によってアドレス変換されること以外は図 3.4 と同様である．表 3.2 の左列に利用者の条件と割り当てられるサブネットを示している．端末が組織外にアクセスすると，p.q.0.0/16 の IP アドレスは，対応するグローバル IP アドレスである，e.f.g.0/24 に変換される．電子ジャーナルサーバでは，同様にクライアントのグローバル IP アドレスに基づくアクセス制限が可能になる．

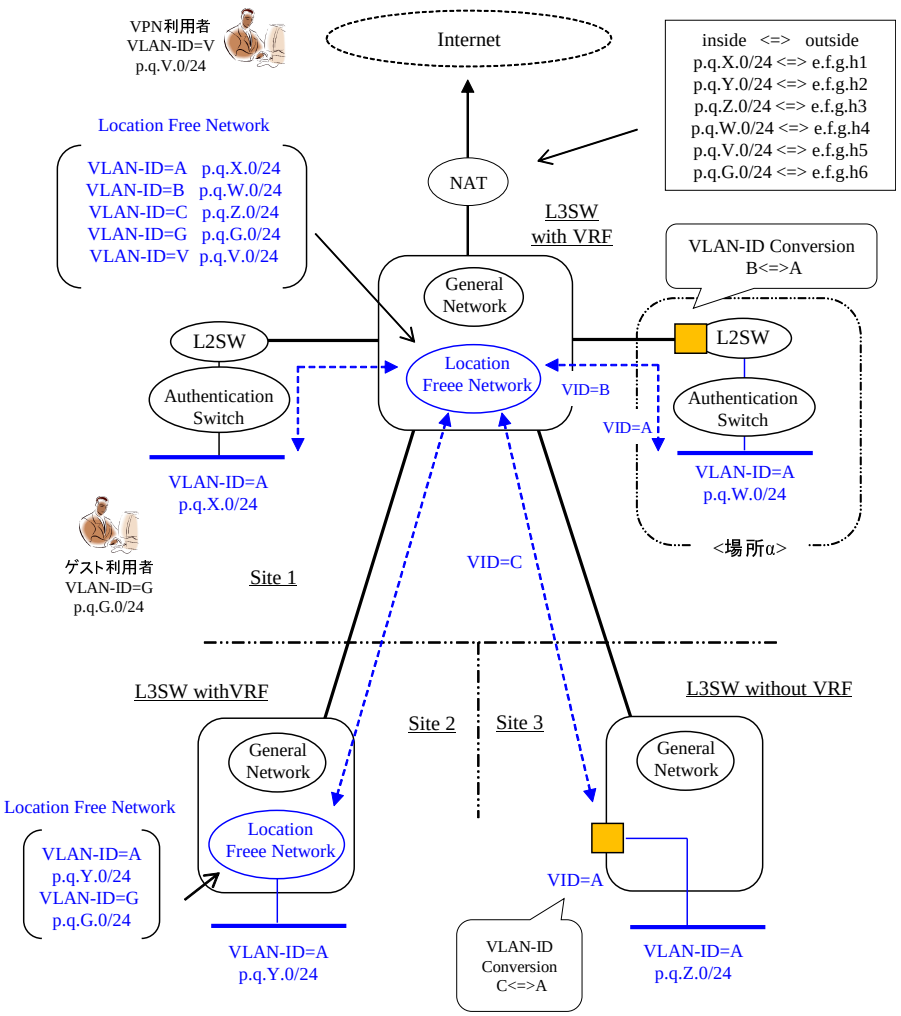


図 3.5: プライベート IP アドレスにおける構成

3.2 システムの実装

3.2.1 システムの概要

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 IP 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，提案方法に基づいて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．ロケーションフリーネットワークは，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，芳賀キャンパスでサービスをしている．実装したシステムの構成を図 3.6 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 [30]（以下，OKIX と記す）を介して接続されており，三朝キャンパスは OKIX および鳥取情報ハイウェイ [31]（以下，TIH と記す）を介して接続されている．

津島キャンパスと鹿田キャンパスの L3 スイッチは VRF 機能を有しており，それぞれの VRF でロケーションフリーネットワークを運用している．津島キャンパスと鹿田キャンパスの対応する

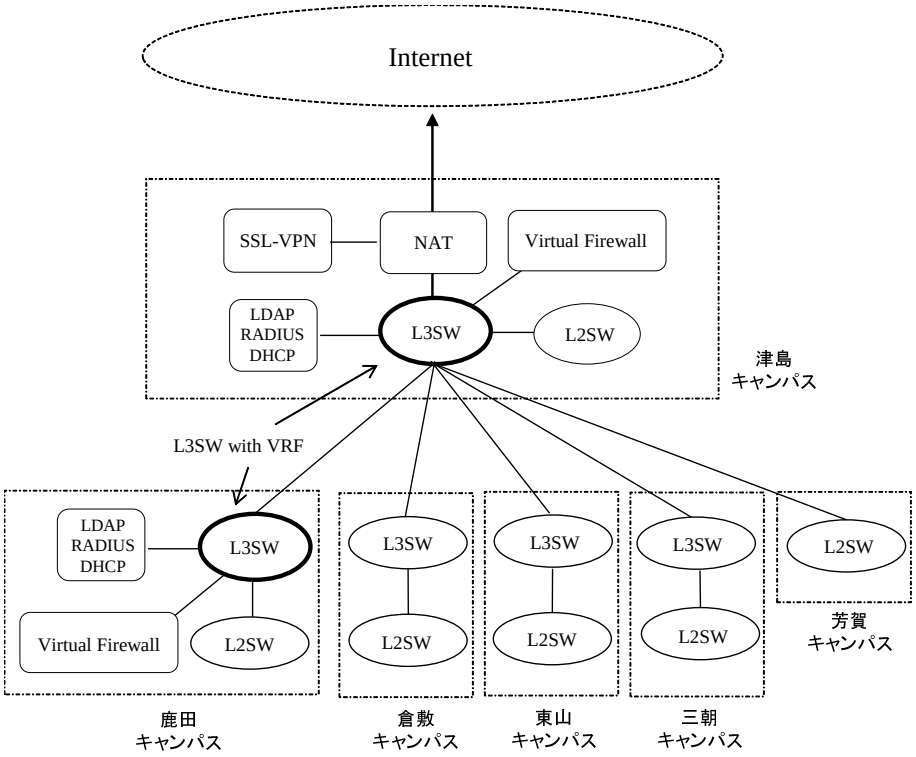


図 3.6: 実装したシステムの構成

VRF は，OKIX の光ケーブルを介して接続されている．また，各 VRF 間は，セキュリティポリシーにより，津島キャンパスの L3 スイッチにおいて，バーチャルファイアウォールを介して接続されている．津島キャンパス，鹿田キャンパスの各 VRF におけるセグメントは，そのキャンパスの L3 スイッチの VRF 内で直接接続されている．倉敷キャンパス，東山キャンパス，三朝キャンパスのロケーションフリーネットワークは，3.1.3 節 (1) で述べた構成方法により，津島キャンパスのロケーションフリーネットワークの VRF を VLAN-ID 変換により接続している．芳賀キャンパスでは L3 スイッチを運用していないため，3.1.3 節 (2) で述べた構成方法を用いている．倉敷，東山，三朝，芳賀の各キャンパスの L3/L2 スイッチでは，VLAN-ID 変換をアラクサラネットワークス社のスイッチのコマンドである ”switchport vlan mapping ”によって設定した．

なお，岡山大学では同じキャンパス内の特定の場所に限って契約されているサイトライセンスがないため，同一拠点内での L3 スイッチと L2 スイッチ間の VLAN-ID 変換による接続は行っていない．

3.2.2 システムの構成

(1) 認証スイッチ

エッジスイッチにアラクサラ社の AX2400S を使用し，認証スイッチとしても利用している．認証スイッチのポートに端末が接続されると MAC 認証を試み，認証が失敗すると 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 サーバから回答された VLAN-ID のサブネットに端末を接続する．

(2) RADIUS サーバ

RADIUS サーバは，FreeRADIUS[32] を使用した．LDAP サーバと連携し，認証スイッチからの認証要求に対して回答する．

(3) 認証サーバ

認証サーバには，岡山大学統合認証システムの LDAP サーバを使用した．この 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おり，登録者の属性値として VLAN-ID を登録して WEB 認証で使用している．また，MAC アドレス認証では端末の MAC アドレスと VLAN-ID を登録している．

(4) NAT ルータ

岡山大学のロケーションフリーネットワークでは，VPN 利用者以外はプライベート IP アドレスで運用しているため，NAT ルータが必要である．NAT ルータは一般的なファイアウォールアプライアンスによって運用している．

3.1.6 節 (3) で述べた構成に基づいて，ロケーションフリーネットワークの次の種別ごとに，それぞれに対応するグローバル IP アドレスへの IP アドレス変換を行っている．

- 各キャンパスの教員および職員
- 各キャンパスの学生
- ゲスト利用者

(5) SSL-VPN システム

SSL-VPN システムとして，SSL-VPN アプライアンスを運用している．VPN 利用者には，グローバル IP アドレスの 2 つのサブネットを割り当てている．1 つは教員と職員用のもの，もう一つは学生用のものである．SSL-VPN システムは，RADIUS サーバの認証結果による VLAN-ID によらず，ユーザの種別によってどちらかのサブネットに端末を接続する．

(6) バーチャルファイアウォールシステム

仮想ファイアウォール機能を有した，ファイアウォールアプライアンスを運用している．この装置は UTM(Unified Threat Management) 機能によって，グローバル IP アドレス空間とロケーションフリーネットワークのアドレス空間とのトラフィックを監視する．

3.2.3　ロケーションフリーネットワークシステムの運用

まず，岡山大学のロケーションフリーネットワークの環境について述べる．各ユーザには，教員，職員，学生の種別と，学部，学科，附属施設などの所属に基づいた VLAN-ID が割り当てられており，岡山大学統合認証システムに各ユーザの属性値として登録されている．ロケーションフリーネットワークのサブネットは，10.0.0.0/8 のプライベートアドレス空間を使用しており，利用者数によってネットマスクが/22〜/24 の IP アドレスレンジを割り当てている．ゲスト利用者には，10.0.0.0/8 のプライベートアドレス空間からマスクが/24 のサブネットが割り当てられている．VPN 利用者には，150.46.0.0/16 のグローバルアドレス空間から，マスクが/24 のサブネットが 2 つ割り当てられている．ロケーションフリーネットワークで使用している VLAN-ID の数は，教員と職員のものが 212，学生のものが 164，ゲスト利用者が 73，VPN 利用者が 2 である．

ロケーションフリーネットワークにおいて，同じ利用者がキャンパス間を移動すると，端末に割り当てられるサブネット IP アドレスがキャンパスによって異る．その利用者が学外と通信をする場合には，端末の IP アドレスは，NAT システムによってキャンパスに基づいたグローバル IP アドレスに変換される．このように，利用者のロケーションが IP アドレスから判別できるため，利用者のロケーションに基づいたサービスにも，ロケーションフリーネットワークを適用させることができる．

倉敷，三朝，東山，芳賀の各キャンパスでは，津島，鹿田に所属する利用者について，所属によるロケーションフリーネットワークのサブネットを作成していない．その代りに，教員・職員用と学生用に 2 つのサブネットを作成した．倉敷，三朝，東山，芳賀において，津島，鹿田の利用者がロケーションフリーネットワークを利用する場合は，利用者の所属によらず，教員・職員，学生でそれぞれ共通のサブネットに接続される．

次にこのような構成にした理由について述べる．もし，教員・職員，学生の種別と所属に基づくサブネットをすべて準備すると，各キャンパスについて 449(=212+164+73) 個の VLAN が必要になるため，津島キャンパスで必要になるロケーションフリーネットワークの VLAN-ID の総数が，2245(=449 × 5) になる．さらに，今後ロケーションフリーネットワークのキャンパスが増えた場合には，そのキャンパスにつきさらに 449 の VLAN-ID が必要になる．このような理由から，現在のロケーションフリーネットワークの構成方法を選択している．

3.2.4　電子ジャーナルのアクセス制限

岡山大学附属図書館では，約 6800 の電子ジャーナルを契約しているが，”American Journal of Physiology ”[33] や ”Journal of biological chemistry ”[34] 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を許可されている．従来これらの電子ジャーナルは，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，ロケーションフリーネットワークのサービス開始前に，3.2.2 節 (4) のネットワーク種別について，NAT 変換後のグローバル 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契約に基づいてその IP アドレスレンジを設定し，電子ジャーナルサーバへのアクセス許可を行った．

我々はロケーションフリー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 利用者やゲスト利用者も適切に利用が制限されていることを確認した．

以上より，利用者のロケーションに基づいたサービ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の有効性と実用性が確認された．

第4章　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

4.1　システムの概要と設計

3 章によるロケーションフリーネットワークシステムによって，利用者のロケーションに基づいたサービスを利用できるようになった．しかし，端末が接続されるサブネット IP アドレスが，利用者のロケーションによって異なるため，利用者がロケーション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．この理由は，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，このような条件が必要な場合に，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を提案する．すなわち，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．利用者の位置情報を認証ネットワークから取得し，NAT ルータや DHCP 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．本章では，同一サブネットへの接続性を保証することを目的とするため，ロケーションフリーネットワークの定義は，2.1.3 節の定義 2 を用いる．なお，3 章では，利用者の現在位置の情報を拠点や領域などの比較的大きな範囲を想定してロケーションと呼んだ．本章では，認証スイッチ単位，最小では認証スイッチのポート単位の精度で利用者の場所を識別可能なため，利用者の現在位置の情報を位置情報と呼ぶ．

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．NAT については，NAPT(Network Address Port Translation)[35] でも同様に動作可能であるため，以下，NAT と NAPT を含めて NAT と記す．

4.1.1　利用者の現在位置の取得

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 [36] の情報や GeoIP ロケーションサービス [37] 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は，文献 [38] に示されている．DNS 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．その他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．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．

(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．例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みなすことができる．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，識別する位置情報が隣接していない場合，例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を推定する手法 [39] があり，このような方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，認証スイッチのポート単位での位置情報を識別可能である．

4.1.2 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，次の動作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) と記す
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) と記す
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) と記す
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) と記す

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．

(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述べる．4.1.1 節 (1) 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．

以下に提案する構成方法の動作や特徴について述べる．

(2) NAT ルールの動的な変更

4.1.2 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，識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
   認証結果の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，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，識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 ルールによって，端末の位置情報を決定するため，識別する位置情報の変更や組織のネットワーク構成に柔軟に対応できる．一方で，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．また，ネットワークから離れた端末の NAT ルールを削除する機能が必要である．動作の手順を図 4.1 に示す．

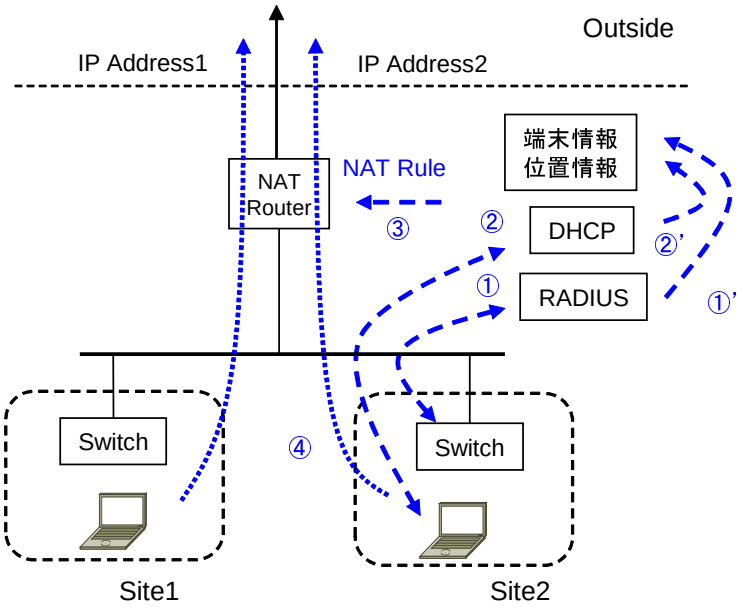


図 4.1: DNC による NAT ルールの動的な変更

(3) IP アドレスリースの動的な変更

4.1.2 節の DAL による構成である．利用者の位置情報に基づく NAT ルールに適合するように，DHCP サーバが端末の 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，識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き，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．

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，識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マスク長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利点がある．DNC と同様に NAT ルールによって端末の位置情報を決定するため，識別する位置情報の変更や組織のネットワーク構成に柔軟に対応できる．ただし，識別する位置情報の数が変わると，端末にリースする IP アドレスの範囲を再構成する必要がある．ネットワークか

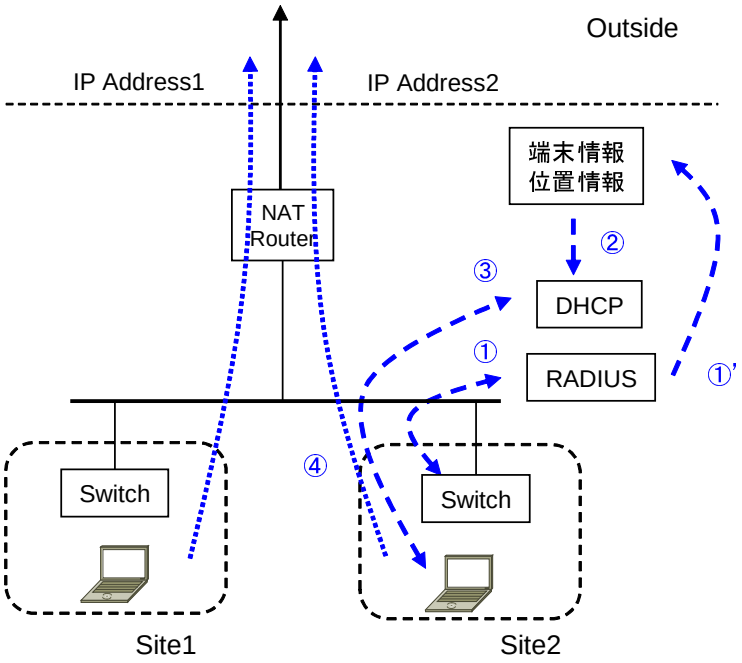


図 4.2: DAL による IP アドレスリースの動的な変更

ら離れた端末の無効化は，DHCP の IP アドレスリースの動作で実行される．動作の手順を図 4.2 に示す．

(4) ゲートウェイ IP アドレスリースの動的な変更

4.1.2 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するように，端末のゲートウェイ IP アドレスを動的に割り当てる．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，識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共に，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．また，DAL と同様にネットワークから離れた端末の無効化は，DHCP の IP アドレスリースの動作で実行される．このように接続する端末の管理が比較的容易である．動作の手順を図 4.3 に示す．実装には 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，位置情報を識別するサブネットに，位置情報を区別する数の NAT ルータをゲートウェイとして運用する．以下，この方法を DGL1 と記す．NAT ルータを多段運用することも可能である． 1 つのサブネットに対して，識別する位置情報の数に応じた NAT ルータを運用する必要がある．

- マルチホームでのゲートウェイ IP アドレスの変更

表 4.1: ネットワーク規模に対する適応性

構成方法	大規模	中規模	小規模
DNC	○	◎	◎
DAL	◎	◎	◎
DGL	-	-	◎
DRC	-	○	◎

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 アドレスによって識別することが可能な場合である．以下，この方法を DGL2 と記す．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．この方法では識別できる位置情報の数がマルチホームの数に制限される．

(5) ネクストホップの動的な変更

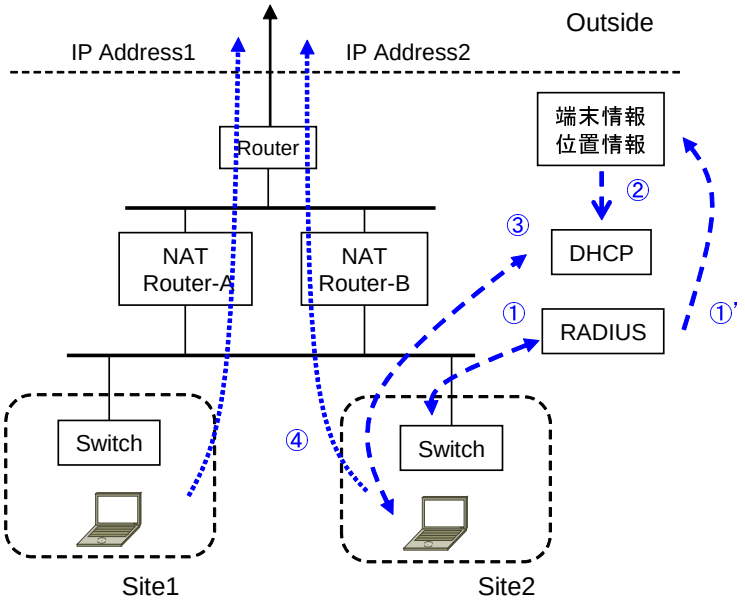
4.1.2 節の DRC による構成である．ルータで PBR(Policy-Based Routing) を用いることで，パケットを位置情報に基づいた NAT ルータにルーティングする．動作には 2 つの方法がある．1 つは端末に割り当てられた IP アドレスによってルートマップを動的に設定する方法（以下，DRC-M と記す），もう 1 つは固定的に設定されたルートマップに基づいて DHCP がリースする IP アドレスを動的に変更する方法（以下，DRC-A と記す）である．また，ネットワークの物理的な構成は，識別する数の NAT ルータを運用する方法（以下，DRC1 と記す）と，マルチホームによる方法（以下，DRC2 と記す）がある．識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機能が必要である．1 台のルータの下流に複数のサブネットを運用し，それぞれにルートマップを適用できるため，柔軟なネットワーク構成が可能である．DRC-M では，DNC と同様にネットワークから離れた端末のルートマップを削除する機能が必要である．動作の手順を図 4.4 に示す．

(6) 動作方法によるネットワークへの適応性

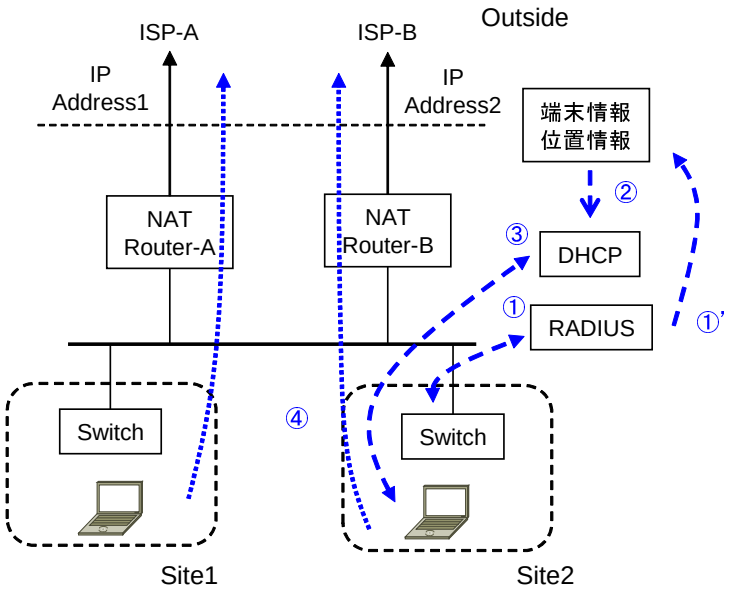
前述のとおり，各動作方法によってそれぞれの特性を有している．ネットワーク規模に対する各動作方法の適応性を表 4.1 に示す．DGL や DRC は組織の一部でロケーションフリーネットワークを運用する場合に適用するなども考えられる．

4.1.3 組織のネットワークへの適用に関する考察

組織のネットワークへの適用について，3 章による構成と本章による構成の特徴を述べる．3 章による構成方法では，位置情報が異なる場所では同一サブネットに接続できないが，VLAN-ID とサブネットの構成によって実現可能でありスケーラビリティが高い．これに対して本章での構成方法では，同一サブネットに接続可能であるが，位置情報を管理する機能を運用し，NAT ルータや DHCP サーバ，ルータの動的な設定が必要になる．組織のネットワークへの適用においては，

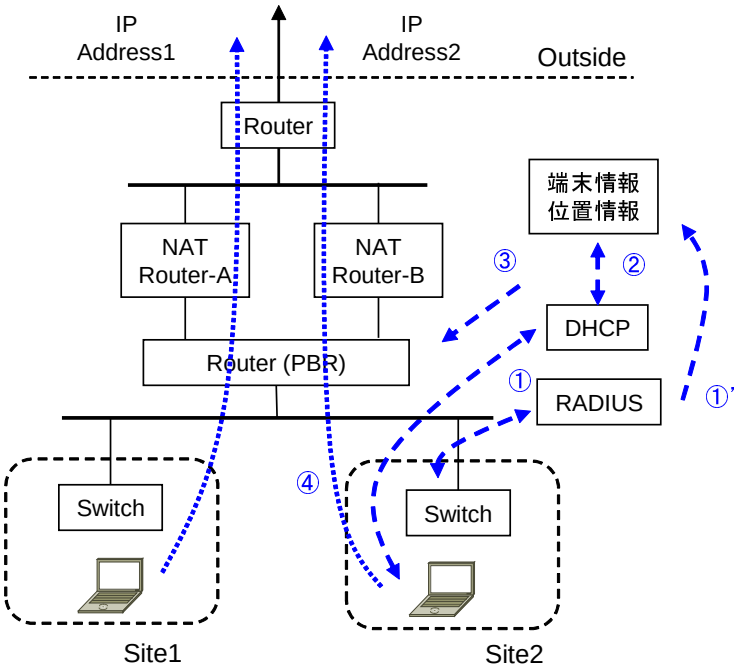


（DGL1による構成）

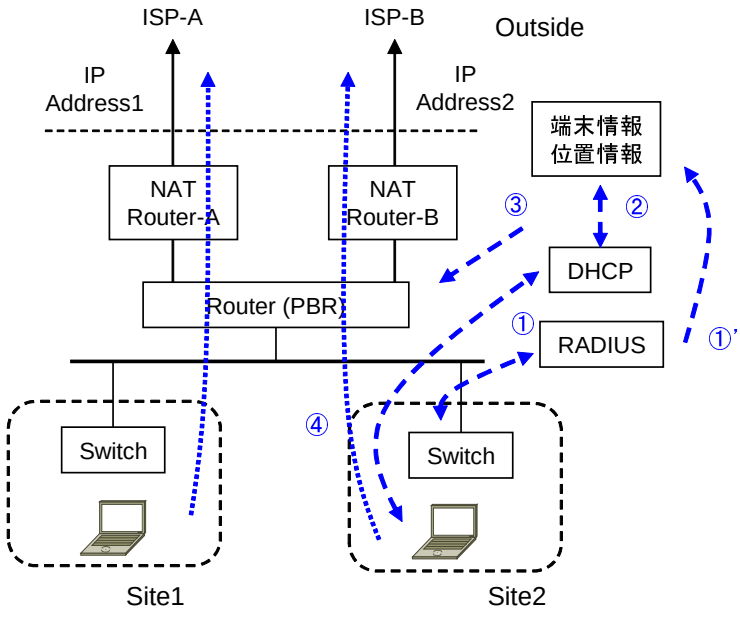


（DGL2による構成）

図 4.3: DGL によるゲートウェイ IP アドレスリースの動的な変更



（DRC1による構成）



（DRC2による構成）

図 4.4: DRC によるネクストホップの動的な変更

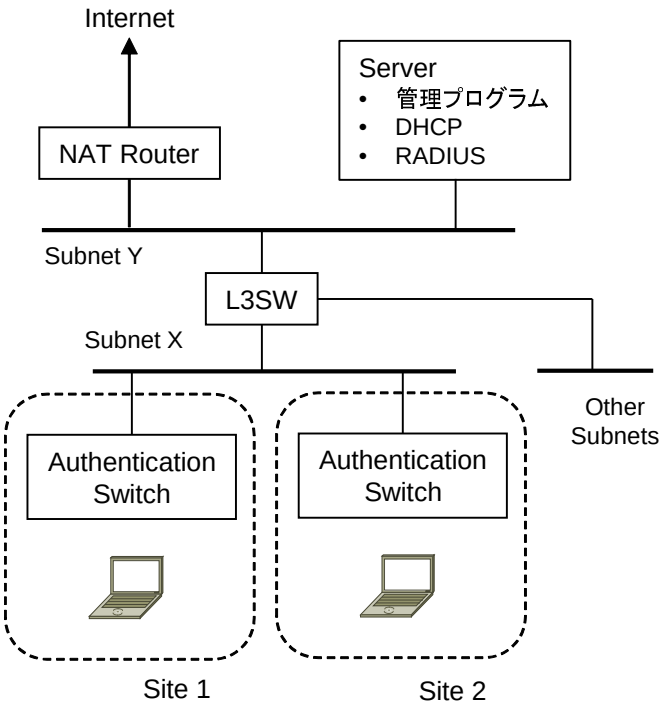


図 4.5: 試作システム

このような特徴を考慮して構成方法を選択する．あるいは，全体的なネットワークは 3 章の方法で構成し，同一ブロードキャストドメインにおけるサブネットの接続性が必要なセグメントでは，本章の方法を適用することが考えられる．

4.2 試作システムの実装と評価

4.2.1 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した．システムの接続構成を図 4.5 に，機器構成を表 4.2 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 である．DHCP サーバは，通常機能で運用する場合には ISC DHCP[40] 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．

4.2.2 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を動的に行う．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[45] で作成した．

表 4.2: システムの機器構成

	機器構成
NAT Router	NEC Corporation UNIVERGE IX2025[41] （IPv4 転送性能 200Mbps NAPT 最大エントリ 65,535 静的 NAT 最大設定数 256 行）
Server	CPU Celeron D 325(2.53GHz) Memory 1GB CentOS-5.10 32bit[42]
Layer3 Switch	Cisco Systems, Inc. WS-C3750G-24TS-E[43]
Authentication Switch	Allied Telesis K.K. CentreCOM GS908M V2[44]
Personal Computer	Microsoft Windows 7 Core i3 2.3GHz Memory 4GB

(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[46] を使用した．

(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．

(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 IP アドレス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．

4.2.3 試作システムの動作試験

(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，DAL，DGL について，NAT ルータでは NAPT によるアドレス変換を行った．

まず，DNC，DAL において通信試験を行った．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．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 にお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 4.6 に，DAL，DGL のものを図 4.7 に示す．DRC については，図 4.6 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．

(2) 性能評価試験

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 100Mbps，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 4.5 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．

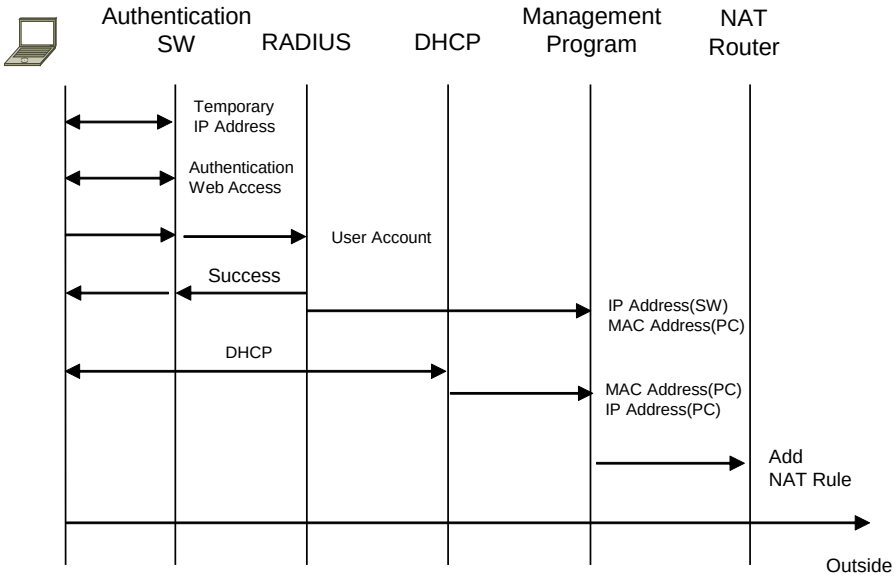
まず，DNC について，WEB 認証では認証スイッチのログイン画面にユーザ名，パスワードを入力してから，NAT ルータに NAT ルールが設定されるまでの時間を，MAC アドレス認証では，端末を認証スイッチに接続し，リンクアップしてから NAT ルールが設定されるまでの時間を測定した．結果を表 4.3 に示す．

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 4.4 に示す．

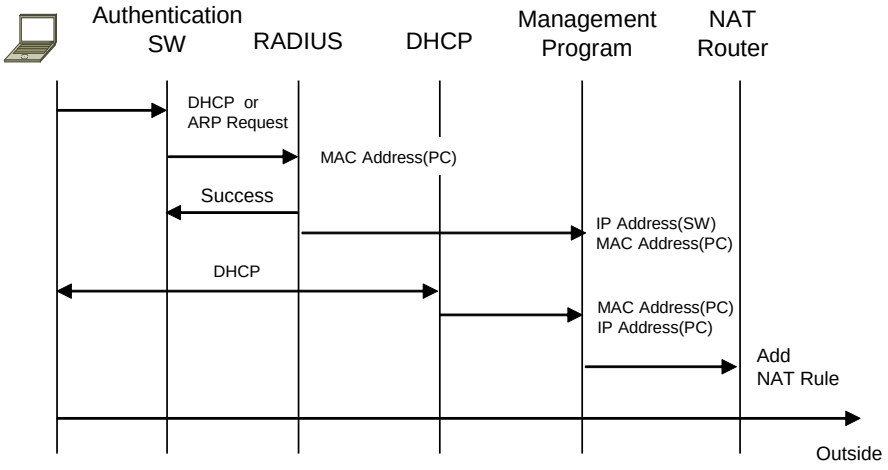
比較のため，通常動作の場合，すなわち試作システムにおいて NAT ルータや DHCP サーバで動的な変更をしないで，通常の認証と通常の DHCP アドレスリースを行った場合の処理時間を表 4.5 に示す．

(3) 高負荷時の性能評価試験

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，複数の端末では全てが同時に DHCP による IP アドレス取得ができなかったため，複数端末の同時のアクセスを

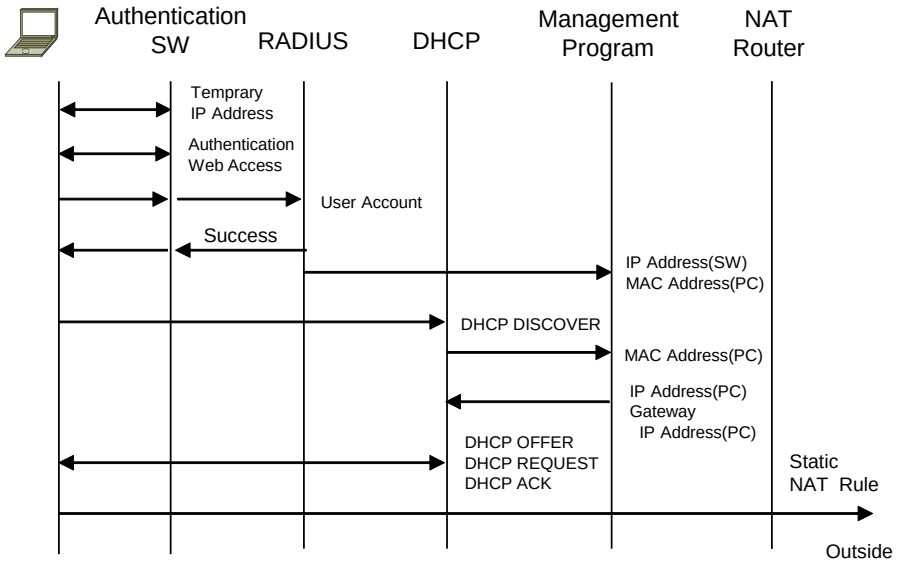


（A） WEB認証

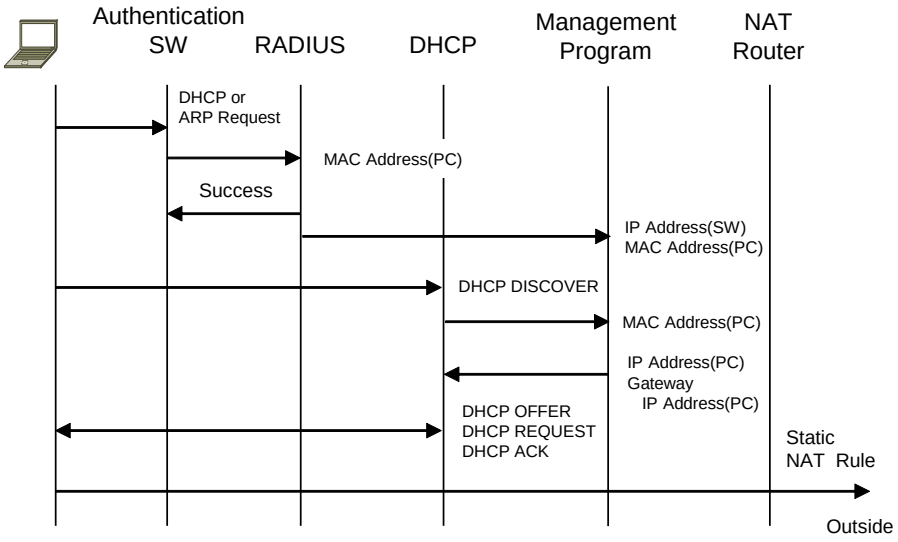


（B） MAC認証

図 4.6: DNC による動作手順



（A） WEB認証



（B） MAC認証

図 4.7: DAL，DGL による動作手順

表 4.3: DNC によるスループット

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 4.4: DAL,DGL によるスループット

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 4.5: 通常動作のスループット

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

実行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 ルール設定のスループットを測定した．結果を表 4.6 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[47] 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 4.7 に示す．また，DHCP クライアントとして使用した端末の諸元を表 4.8 に示す．

表 4.6: NAT ルール設定の処理時間

実行時間の範囲 (ミリ秒)	15〜17
平均値 (ミリ秒)	16.5

表 4.7: 試作 DHCP サーバの IP アドレスリース時間

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 4.8: DHCP クライアント端末の諸元

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

(4) 動作試験の評価

まず，表 4.3，表 4.4，表 4.5 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 4.5 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 4.6，表 4.7 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．位置情報を判別する場合は，しない場合に対して平均で 0.2 ミリ秒程度が加算されるが，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，同時多数の DHCP 要求を十分に再現しているとは言えないが，同時多数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．

識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，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の有効性が確認された．

第5章　地理的に分散したサーバ間のフェイルオーバ・フェイルバックを可能にする複製サーバ冗長化構成

5.1　システムの概要と設計

2.2 節で述べたように分散配置されたサーバの冗長化において，従来の冗長化方法では停止しているサーバに接続しようとたり，フェイルオーバするとその後はフェイルバックをしなかったりする問題がある．そこで，本章では組織内のネットワークにおいて IP Anycast を用いることで，地理的に分散したサーバの冗長化構成を提案する．提案の構成では従前の問題を解決し，さらに複製サーバ間のフェイルオーバ，フェイルバックが可能である．従来 IP Anycast は，主にステートレスなプロトコルを対象に用いられているが，TCP 通信に適用した場合でもクライアントがサーバ接続のリトライ機能を有していれば pop switch に対応できることに着目する．また，IP Anycast は，世界規模や国家規模のような大規模なネットワークに用いられているが，本章では一般的な組織のネットワークにも適用できることを示す．

5.1.1　IP Anycast による冗長化

IP Anycast は 1 つの IP アドレスを複数のサーバに対して共通に割り当てるアドレッシング方法であり，分散配置された複数のサーバによる冗長化が可能である．IP Anycast では，クライアントからのパケットは，ルーティングによりそのクライアントから見てネットワークトポロジの観点で最も近いサーバに転送される．このため，2.2.1 節および 2.2.2 節で述べたようなタイムアウトや無駄なトラフィックが発生せず，また最も近いサーバに障害が発生した場合でもルーティングにより次に近いサーバに接続するように動作する．さらに，障害のサーバが復旧し，経路が元に戻ると接続先が自動的に以前のサーバに戻る特性を有する．IP Anycast を用いた冗長化の問題点として，経路に変更があるとクライアントが送出したパケットが異なるサーバで受信されることがあげられる．この場合，特に TCP ではコネクションが確立されていないサーバがパケットを受信すると RST フラグ付きパケットを返すため，pop switch が発生する．このため，従来 IP Anycast はステートレスな UDP のサービスについて適用されることが多い．しかし，TCP のサービスにおいても，クライアントが pop switch 発生時にサーバへの接続をリトライする機能があれば適用が可能である．また，pop switch は障害が発生していたサーバが復旧した際にも発生するため，このリトライ機能を利用すれば迅速なフェイルバックも行うことができる．また，ルーティングプロトコルのメトリックを調整することで，冗長化したサーバを Active-Active や Active-Standby で動作させることができる．Active-Active とは，複数の複製サーバを同時に稼働して処理を分散すること，Active-Standby とは，複数の複製サーバを動作させておき，Standby のサーバではサー

ビス要求があればいつでもサービスを提供できるように，システムを動作状態にしておくことである．

なお，システムの構成について，従来の冗長化の構成方法では，前述のとおりサーバやクライアントに実装が必要であったり，DNS レコードの登録が必要であったりする．これに対して提案の冗長化構成方法では，そのような要件はないが，IP Anycast に用いる IP アドレスの経路情報をネットワークに広告したり，後述するサービスの死活監視を運用したりする必要がある．

5.1.2 冗長化構成の条件

提案手法が正しく動作するためにクライアントおよびサーバに必要な条件を以下に示す．

- クライアントは任意のトランスポート層プロトコルでサーバと通信してよいが，TCP コネクションの切断など pop switch による動作異常を検出する機能を有し，検出後は同一の IP アドレスを持つサーバへの再アクセスを十分長い時間試みることができる．
- クライアントがサーバへ再アクセスを行う場合，pop switch 発生前に行われた通信内容を引き継がず，最初から通信し直すように動作する．
- 全てのサーバはクライアントからの通信に対して同じ動作を行う．
- 全てのサーバはそれぞれ独立して動作し，セッション管理や処理の継続，データ同期などは必要としない．

5.1.3 システムの構成

まず，各複製サーバにおいて IP Anycast アドレスとしてネットマスクが 32 ビットの仮想 IP アドレスを設定し，その経路情報をネットワーク上に広告するためのルーティングデーモンを動作させる．経路情報の広告方法によって，Active-Active や Active-Standby の構成が可能である．Active-Active の場合は，クライアントから見て最寄りのサーバのメトリックが，もう一方のサーバのものよりも小さくなるように設定する．Active-Standby の場合は，クライアントから見て Active のサーバのメトリックが，Standby のサーバのそれよりも小さくなるように設定する．32 ビットのネットマスクは，経路情報の最長一致のためである．

この構成だけでも動作するが，目的のサービスだけが停止した場合，すなわち，サーバは動作しており経路情報は広告しているが，サービスが停止している場合には，ブラックホールサーバとなり，サービス障害が発生する．この対策としてサービスの死活監視が必要である．この機能については，5.1.5 節で述べる．2 台のサーバで冗長構成する例を図 5.1 に示す．

なお，本論文では，主に組織の内部における冗長化を想定するため，IGP(Interior Gateway Protocol) を用いるものとする．IGP では，一般に RIP(Routing Information Protocol)[48] や OSPF(Open Shortest Path First)[49] が利用されるため，本論文では，RIP や OSPF の利用を想定して説明をする．

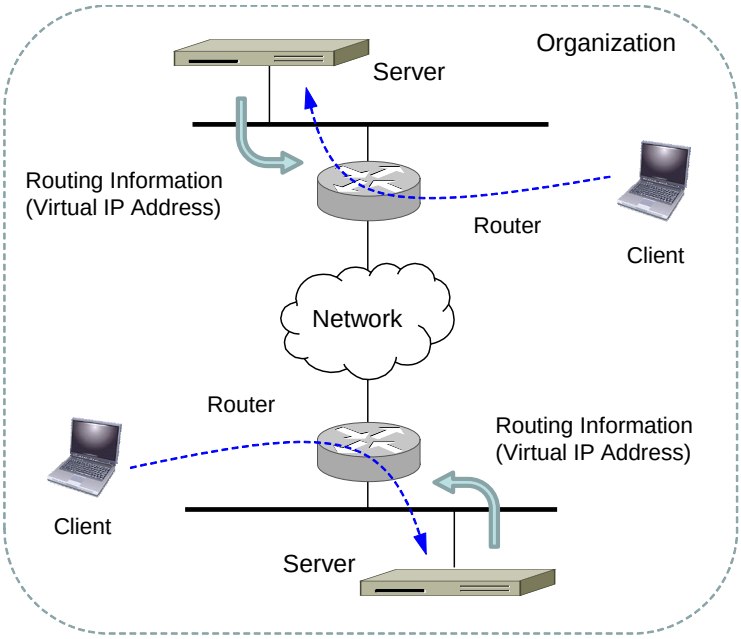


図 5.1: IP Anycast による冗長構成の例

5.1.4 提案方法の動作手順

本提案方法により，フェイルオーバ，フェイルバックする動作手順を説明する．Active-Active，Active-Standby とも同様である．

1. 障害の発生によりサーバへの経路が変更される．
   クライアントの接続先は他のサーバに変更される．

2. クライアントでは pop switch が発生するが，サーバへの接続をリトライすることでサーバの切替を完了する．（フェイルオーバ）

3. 障害のサーバが復旧し経路が以前の状態に戻る．
   クライアントの接続先は以前のサーバに戻る．

4. クライアントでは pop switch が発生するが，サーバへの接続をリトライすることでサーバの切替を完了する．（フェイルバック）

(1) 複数のサービスへの IP Anycast の適用

1 台のサーバが IP Anycast によって複数のサービスを提供する場合には，各サービスは独立して冗長化を行う必要がある．IP Anycast では一般的には，ループバックインターフェースに IP alias で仮想 IP アドレスを設定して動作させるが，サービスが複数ある場合には複数の仮想 IP アドレスの経路情報を独立して制御できない場合がある．例えば，サーバのルーティングデーモンとして，Quagga Routing Suite[50] などが一般によく用いられるが，Quagga では，IP alias の場合にはそれぞれの経路情報を個別に制御することができない．

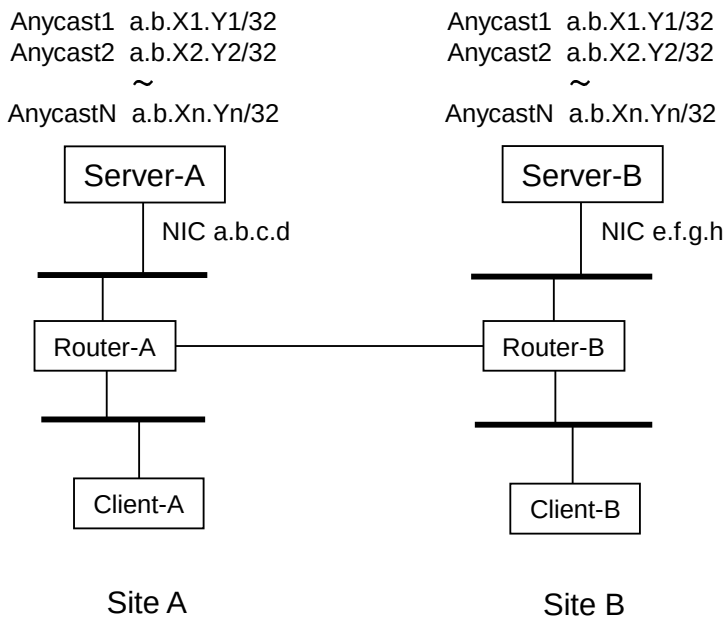


図 5.2: 複数の IP Anycast アドレスの運用

このような場合には，ルーティングプロトコルに OSPF を使用し，IP トンネルの生成や VLAN インターフェースの生成によって，仮想 IP アドレスを複数作成する方法を用いることができる．OSPF ではインターフェースごとにコストの変更が可能なため，各仮想 IP アドレスに対応したサービスが独立して IP Anycast による経路制御を行うことができる．

なお，RIP などのようにインターフェースごとにメトリックを変更できない場合には，サーバのルーティングデーモンとルータの間に経路情報を制御する機構を組み込むなどの方法が考えられる．複数のサービスへ IP Anycast を適用するモデルを図 5.2 に示す．

5.1.5 サービスの死活監視

本提案による冗長化構成では，サーバあるいはルーティングデーモンが停止したときには，経路情報が更新されてバックアップとなるサーバに自動的にフェイルオーバするが，サービスのプロセスだけが停止した場合には，経路情報が更新されないため自動的にフェイルオーバしない．このため，障害を検知して直ちに経路情報を更新し，フェイルオーバさせるための機能が必要である．なお，サーバのルーティングデーモンとネットワークが正常に動作している状態であれば，経路情報の変更によるフェイルオーバの時間は，ルーティングプロトコルのコンバージェンス時間に基づく．サーバが突然ダウンしたような場合には，RIP では Flash タイマー，OSPF では Dead 間隔に基づいた時間でフェイルオーバする．サービスの死活監視にはいくつかの方法がある．

(1) 死活監視用に別システムを運用する方法

別に運用する監視用のシステムでヘルスチェックを行い，障害が発生したときには，ルータやサーバに指示を出してフェイルオーバさせる（以下，別システム監視と記す）．この方法では，ネッ

トワークやサーバの状態を総合的に管理できるため，柔軟な運用が可能になる利点があるが，単一障害点になる可能性があり，監視用システムの冗長化なども検討する必要がある．

(2) 冗長化するサーバ自身が死活監視を行う方法

別の監視用システムを利用することなく，サーバ自身がヘルスチェックを行うことができる．別システム監視と同様にヘルスチェックで障害を検出した場合には，ルータやサーバに指示を出してフェイルオーバさせる．この場合には，ヘルスチェックとフェイルオーバでそれぞれ 2 つの方法がある．ヘルスチェックでは，自分自身の動作チェックをする方法と，他のサーバの動作チェックをする方法がある．他のサーバの動作をチェックする方法では，他のサーバやネットワークの状況に応じて動作することができる．

フェイルオーバでは，自分への経路の優先度を上げる方法と下げる方法がある．自分の優先度を上げる方法では，特に冗長の多重度が大きい場合には負荷が集中する場合のあること，優先度を上げたサーバの動作に異常がある場合には，ブラックホールとなってサービス障害を起こす場合がある．自分自身のヘルスチェックを行い，障害時には自分への経路の優先度を下げる方法をセルフ監視と記す．また，他のサーバのヘルスチェックを行い，障害時には自分への経路情報の優先度を上げる方法を相互監視と記す．セルフ監視では，監視機能がそのサーバ内だけで動作するためシンプルな構成が可能であるが，他のサーバやネットワークと協調した動作はしない．相互監視では，他のサーバやネットワークの状況に応じて動作することができるが，前述のとおり負荷集中やブラックホールとなる場合があるため注意が必要である．

これらの方法は，別システム監視のような総合的な管理機能が必要でない場合に有効であり，単一障害点や通信経路のボトルネックの問題を回避することができる．ライトウェイトな冗長化システムとして運用することが可能である．

冗長化の要件に応じて，これらの構成方法を選択することができる．本論文ではシンプルな冗長化システムとして，主にセルフ監視を想定する．

5.2 評価システムの実装と評価

TCP に IP Anycast を適用した冗長化においてサーバの切替りを検証するため，岡山大学のキャンパス情報ネットワークに評価システムを構成した．

5.2.1 評価システムの実装

RADIUS サーバが LDAP サーバを参照する構成により評価システムを実装した．この構成は，5.1.2 節の条件に適応している．評価システムの接続構成を図 5.3 に，機器構成を表 5.1 に示す．L3SW-A と L3SW-B の間はバックボーンであり，ルーティングプロトコルは OSPF を運用している．また，L3SW-A と L3SW-B の支線では RIP を運用し，RIP のエージングタイマーは 180 秒に設定されている．

各 LDAP サーバでは RIP を運用し，IP Anycast の仮想 IP アドレスの経路情報をネットワークに広告する．RADIUS サーバは，認証情報として LDAP サーバを参照するため，参照先として LDAP サーバの IP Anycast アドレスを指定する．RADIUS サーバは FreeRADIUS を，LDAP サーバは OpenLDAP を使用した．

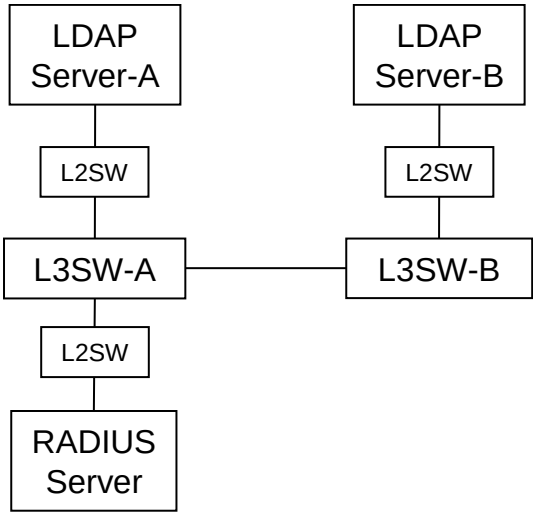


図 5.3: 評価システムの接続構成

5.2.2 評価システムによる動作検証および評価

評価システムにおいて，RADIUS サーバが現在参照している LDAP Server-A の LAN ケーブルを抜き差しすることで，疑似的に障害と復旧を発生させ，RADIUS サーバの参照先の切替りを確認した．なお，RADIUS サーバの参照先が切替る契機は，サーバの停止，ルーティングデーモンの停止，サービスのプロセスの停止である．LAN ケーブルが抜かれることは，LDAP サーバからの経路情報が届かなくなることであり，サーバでのルーティングデーモンが停止することと同様である．また，サービスのプロセスが停止した場合は，5.1.5 節のサービスの死活監視によってサーバへの経路を変更するため，サーバでのルーティングデーモンが停止することやサーバが停止したことと同様である．LDAP Server-A，LDAP Server-B では tcpdump を実行し，サーバの通信状態を確認した．また，RADIUS サーバでは，localhost に対して radtest を 1 秒間隔で実行し，認証の成功と失敗を確認した．検証実験の手順を以下に示す．

- 障害の発生によるフェイルオーバ

  1. Server-A の LAN ケーブルを抜く
  2. RADIUS サーバの参照先が LDAP Server-B に移る

- 障害の復旧によるフェイルバック

  3. Server-A の LAN ケーブルを差す
  4. LDAP Server-A の物理インターフェースの通信が復活する
  5. RADIUS サーバの参照先が LDAP Server-A に戻る

この検証を 5 回行い，切替りの時間を測定した結果を表 5.2 に示す．フェイルオーバの時間が平均 171 秒であり，RIP のエージングタイマーが 180 秒であることから妥当な時間と言える．また，

表 5.1: 評価システムの機器構成

	機器構成
L3SW-A,B	ALAXALA Networks Corp. AX6708S
LDAP Server-A	CPU Xeon 3065(2.33GHz) メモリ 2GB OS CentOS 5.10 64bit
LDAP Server-B	CPU Pentium D(3GHz) メモリ 1.5GB OS CentOS 5.10 64bit
RADIUS Server	CPU Pentium D(3GHz) メモリ 1.5GB OS CentOS 6.5 64bit

表 5.2: 切替り時間

動作	平均時間	検証手順の対応
フェイルオーバ	171 秒	1 から 2 の時間
LAN ポートのネゴシエーション	30 秒	3 から 4 の時間
フェイルバック	11 秒	4 から 5 の時間

フェイルバックの 11 秒についても，RIP の Update が 30 秒であることから妥当な時間と言える．pop switch は手順 2 と 5 で発生するが，サーバの切替りとほぼ同時にサービスが再開されることを確認した．なお，LAN ポートのネゴシエーションは本論文とは無関係であるが，検証手順の明確化のため記載した．

学内ネットワークの設定を変更することは運用に支障が生じる可能性がありできなかったが，もし全てのルーティングを OSPF で運用したとすると，経路の切り替わり時間が短縮される．フェイルオーバは，OSPF の Dead 間隔である 40 秒程度に，フェイルバックは OSPF のコンバージェンス時間に短縮されると考えられる．

5.3 LDAP サーバへの適用

岡山大学では統合認証システムのサービスを行っており，津島キャンパスと鹿田キャンパスに各 1 台の LDAP サーバを運用している．2 台の LDAP サーバはレプリケーションによって同じ情報を有する複製サーバとなっている．これらの LDAP サーバは本学の教・職員，学生，来訪者の一時アカウントなど全てのユーザのアカウント情報を有しており，ロケーションフリーネットワークシステムの 2 台の RADIUS サーバ，教務システムの 2 台のサーバおよび 16 台の PC 端末から認証サーバとして利用されている．LDAP クライアントであるこれらのサーバや PC 端末では，運用しているシステム構成により，LDAP サーバとして設定できるホストが 1 台に限られる問題があった．通常では各 LDAP クライアントはどちらかの LDAP サーバを参照しているが，LDAP

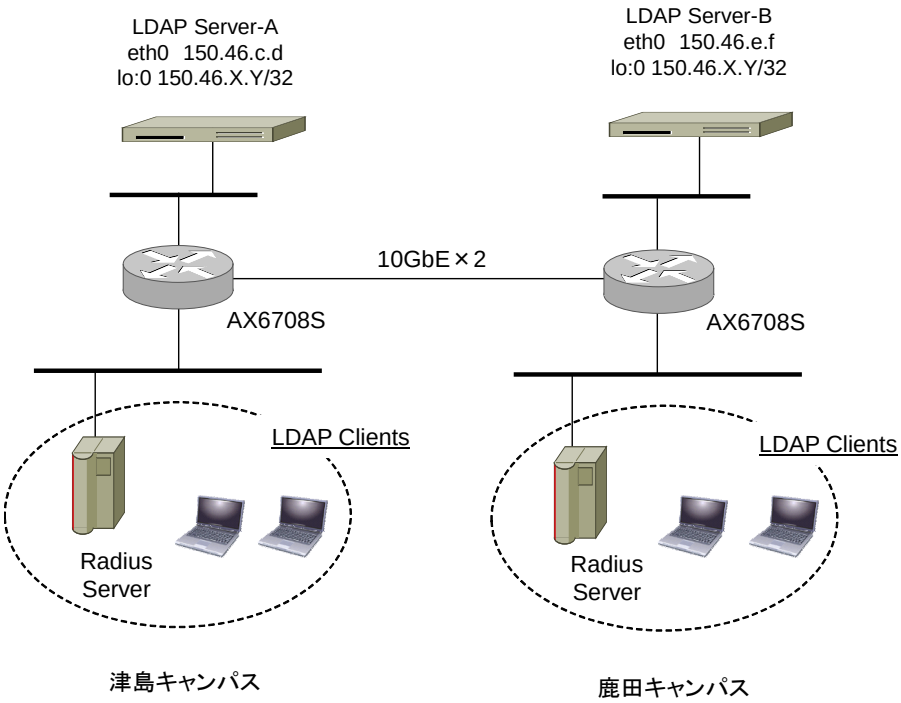


図 5.4: LDAP サーバの冗長構成

サーバで障害が発生すると，各 LDAP クライアントの設定を手作業で変更し，もう一方の LDAP サーバを参照させなければならなかった．このため，長時間のサービス停止と多大な作業工数が発生する問題があり，障害が発生した場合でも，数分以内に自動的にサービスを復旧させる必要があった．

そこで，2 台の LDAP サーバについて IP Anycast を構成し，Active-Active としてシステムを実装した．どちらかの LDAP サーバで障害が発生すると，もう一方にフェールオーバしてサービスを継続する．また，サーバが復旧し経路情報が戻るとフェイルバックする．サービスの死活監視は，セルフ監視である．2 台の LDAP サーバは運用状態のため，本論文のために切替り時間などをテストすることはできなかったが，システムの構築作業において，障害を想定した動作試験でフェイルオーバとフェイルバックが有効に動作し，数分以内に自動的にサービスが復旧することを確認している．なお，LDAP サーバは，NEC 社の Enterprise Directory Server（以下，EDS と記す）であり，OS は RedHat Enterprise Linux 5 である．津島キャンパスと鹿田キャンパスには，それぞれコアスイッチとなるレイヤ 3 スイッチが設置され，両キャンパス間は光ファイバによって 10GbE × 2 回線で接続されている．IP Anycast による LDAP サーバの冗長構成を図 5.4 に示す．

以上より，地理的に分散したサーバ間のフェイルオーバ・フェイルバックを可能にする複製サーバ冗長化構成の有効性と実用性が確認された．

第6章　結論

6.1　本研究のまとめ

本論文では，組織におけるネットワークの信頼性，可用性，利便性，セキュリティの向上，およびコストの低減を実現するためのシステムの構成に取り組んだ．

まず，利用者のロケーションに基づいたサービ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の構成方法を提案した．ロケーションフリーネットワークでは，利用者がどのロケーションからアクセスしているのかを識別できない問題があった．この問題を解決するため，VLAN-IDとサブネットIPアドレスの関係を，利用者のロケーションによって変更する構成方法を提案した．また，本提案に基づいて試作したシステムを実装して評価し，有効性を確認した．さらに，このようなサービスの例として，岡山大学附属図書館が契約している電子ジャーナルのサイトライセンスに適用して実用性を確認した．

次に，前述のロケーションフリーネットワークシステムでは，利用者がロケーションの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特性がある．そこで，このような条件が必要な場合に対して，新たなロケーションフリーネットワークの構成方法を提案した．利用者はロケーションフリーネットワークを利用するが，どこで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る．構成方法および多様なネットワークに適した実装方法を示した．本提案に基づいて試作したシステムを評価し，有効性を確認した．

最後に，サービスの冗長化の問題の解決に取り組んだ．地理的に分散配置されたサーバの冗長化には，従来DNSを用いるもの，サービスの仕様によるもの，クライアントの実装によるものがある．しかし，サーバとの通信に大きな遅延が発生したり，ダウンしているサーバに接続しようとしたりする問題がある．また，フェイルオーバするとフェイルバックしない問題がある．そこで，組織のネットワークにおいてIP Anycastを用いることで，地理的に分散した複製サーバの冗長化構成を提案した．従来の問題を解決し，さらにフェイルオーバ後にシステムが復旧すればフェイルバックする．また，IP Anycastが一般的な組織のネットワークにも適用できることを示した．本提案に基づいて試作したシステムを評価して有効性を確認した．さらに，LDAPサーバに適用して実用性を確認した．

6.2　今後の課題

第3章のロケーションフリーネットワークシステムにおいては，本論文の適用範囲を電子ジャーナルに限らず，場所，所属，身分などの利用者個人の属性や端末の属性など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．

第4章のロケーションフリーネットワークシステムにおいては，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，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を構成することである．認証スイッチの FDB の情報を利用することを検討している．また，認証スイッチの FDB の情報を利用して位置情報の精度向上を行いたい．

第 5 章の複製サーバ冗長化構成においては，死活監視機能の精度を上げ，サービスがダウンした場合のフェイルオーバ時間を短縮したい．また，サーバ間でのセッション管理や処理の継続，データ同期などを実装すること，本論文による冗長化構成の応用範囲を広げることがあげられる．

謝辞

本研究に際し，懇切なる御指導ならびに御助言を賜りました，自然科学研究科 横平徳美教授に衷心より感謝の意を表します．

本研究の全過程を通じ，懇切なる御指導と御鞭撻を賜り，本研究をまとめるに際しても親身なる御指導ならびに御助言を賜りました情報統括センター 山井成良教授（現在，東京農工大学大学院工学研究院教授）に衷心より感謝の意を表します．自然科学研究科在籍時より，多くの御指導ならびに御助言を賜り，本研究に際しても懇切なる御指導ならびに御助言を賜りました，大学院自然科学研究科 舩曳信生教授に衷心より感謝の意を表します．

本研究に際し，懇切なる御指導ならびに御助言を賜りました，情報統括センター 岡山聖彦准教授に衷心より感謝の意を表します．

本研究に際し，多くの御助言ならびに御支援を賜りました，情報統括センター 谷口秀夫センター長，河野圭太准教授に深謝いたします．

本研究を進めるにあたり，多くの御支援を賜りました，岡山大学病院医療情報部 合地明教授，黄勇助教，病歴室職員の皆様，診療情報管理士の皆様，情報統括センター 吉田満統括主査，宮崎万紀子氏に感謝の意を表します．

最後に，様々な場面で親身なる御助言ならびに御支援を賜りました，環境管理センター 竹内文章准教授に深謝いたします．

4 章の研究は，平成 24 年度科学研究費補助金（奨励研究，課題番号 24919006）の補助を受けています．ここに記して感謝の意を表します．

参考文献

[1] R. Hinden，"Virtual Router Redundancy Protocol (VRRP)"，RFC 3768 (IETF), 2004.

[2] S. Shah and M. Yip，"Extreme Networks' Ethernet Automatic Protection Switching (EAPS) Version 1"，RFC 3619 (IETF)，2003.

[3] C. Partridge, T. Mendez, and W. Milliken, "Host Anycasting Service"，RFC 1546 (IETF), 1993.

[4] P. Mockapetris，"DOMAIN NAMES - CONCEPTS AND FACILITIES"，RFC 1034 (IETF)，1987.

[5] C. Metz, "IP Anycast Point-to-(Any) Point Communication", IEEE INTERNET COMPUTING, Volume 6, Issue 2, pp.94-98, Mar. 2002.

[6] F. Weiden and P. Frost, "Anycast as a Load Balancing feature", LISA'10 Proceedings of the 24th international conference on Large installation system administration, pp.1-6, 2010.

[7] H. Ballani, P. Francis, and S. Ratnasamy, "A Measurement-based Deployment Proposal for IP Anycast", IMC '06 Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, pp.231-244, 2006.

[8] L. Andersona and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026 (IETF), 2005.

[9] Shibboleth Consortium, "Shibboleth", available from <http://shibboleth.net/> (accessed 2015-01-09).

[10] 国立情報学研究所 学術基盤推進部学術基盤課，"GakuNin：学術認証フェデレーションとは"，available from <https://www.gakunin.jp/> (accessed 2015-01-09).

[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748 (IETF), 2004.

[12] Institute of Electrical and Electronics Engineers, Inc., "802.1x: 802.1X - Port-Based Network Access Control", available from <http://www.ieee802.org/1/pages/802.1x.html> (accessed 2015-01-09).

[13] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131 (IETF), 1997.

[14] ALAXALA Networks Corporation, ”Alaxala: AX2400S シリーズ”, available from <http://www.alaxala.com/jp/products/AX2400S/index.html> (accessed 2015-01-09).

[15] 沖野 浩二，布村紀男，”富山大学における認証基盤の整備による業務軽減評価”，学術情報処理研究，No.14，pp.31-39，Sep. 2010.

[16] 桝田 秀夫，”Shibboleth を含んだ統合認証システムの導入～京都工芸繊維大学の 2010 年導入事例～”，第 4 回統合認証シンポジウム，pp.15-18，Dec. 2010.

[17] 松平 拓也，”Shibboleth による金沢大学統合認証基盤の構築と今後の展開”，第 4 回統合認証シンポジウム，pp.33-48，Dec. 2010.

[18] 河野圭太，藤原崇起，大隅淑弘，岡山聖彦，山井成良，稗田隆，”岡山大学における生涯 ID を実現する統合認証システムの構築”，学術情報処理研究，No.15，pp.171-175，Sep. 2011.

[19] K. Egevang and P. Francis, ”The IP Network Address Translator (NAT)”, RFC 1631 (IETF), 1994.

[20] J. Klensin, ”Simple Mail Transfer Protocol”, RFC 5321 (IETF), 2008.

[21] T. Brisco, ”DNS Support for Load Balancing”, RFC 1794 (IETF), 1995.

[22] 下川俊彦, 木場雄一, 中川郁夫, 山本文治, 吉田紀彦, ”広域分散環境における DNS と経路情報を利用したサーバ選択機構”, 電子情報通信学会論文誌 B, 通信 J86-B 巻，8 号, pp.1454-1462, 2003.

[23] 神屋郁子, 下川俊彦, 岡村耕二, 河合栄治, 寺田直美, 岡本裕子, 谷崎文義, 赤藤倫久, ”経路情報を利用した広域分散配信の実証実験”, インタ-ネットコンファレンス論文集 2009, pp.83-90, 2009.

[24] ”Dovecot: Secure IMAP Server”, available from <http://dovecot.org/index.html> (accessed 2015-01-09).

[25] M. Wahl, T. Howes, and S. Kille, ”Lightweight Directory Access Protocol (v3)”, RFC 2251 (IETF), 1997.

[26] J. Myers and M. Rose, ”Post Office Protocol - Version 3”, RFC 1939 (IETF), 1996.

[27] M. Crispin, ”INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1”, RFC 3501 (IETF), 2003.

[28] ALAXALA Networks Corporation, ”Virtualization: Network Partition”, available from <https://www.alaxala.com/en/solution/network/np/> (accessed 2015-01-09).

[29] C. Rigney, S. Willens, A. Rubens, and W. Simpson, ”Remote Authentication Dial In User Service (RADIUS)”, RFC 2865 (IETF), 2000.

[30] 岡山県県民生活部情報政策課，”岡山県：OKIX”, available from <http://www.pref.okayama.jp/page/detail-8208.html> (accessed 2015-01-09).

[31] 鳥取県総務部情報政策課，”鳥取県：鳥取情報ハイウェイ”, available from <http://www.pref.tottori.lg.jp/10012.htm> (accessed 2015-01-09).

[32] The FreeRADIUS Server Project and Contributors, ”FreeRADIUS: The FreeRADIUS Project”, available from <http://freeradius.org/> (accessed 2015-01-09).

[33] The American Physiological Society, ”WWW.PHYSIOLGY.ORG”, available from <http://www.physiology.org/> (accessed 2015-01-09).

[34] American Society for Biochemistry and Molecular Biology, ”THE JOURNAL OF BIOLOGICAL CHEMISTRY”, available from <http://www.jbc.org/> (accessed 2015-01-09).

[35] P. Srisuresh and M. Holdrege, ”IP Network Address Translator (NAT) Terminology and Considerations”, RFC 2663 (IETF), 1999.

[36] L. Daigle, ”WHOIS Protocol Specification”, RFC 3912 (IETF), 2004.

[37] MaxMind, Inc.，”MAXMIND: GeoIP Products”, available from <http://dev.maxmind.com/geoip/> (accessed 2015-01-09).

[38] T. Imielinski and J. Navas, ”GPS-Based Addressing and Routing”, RFC 2009 (IETF), 1996.

[39] 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]，2005 巻，90 号，p.25-31，Sep. 2005.

[40] Internet Systems Consortium. Inc, ”Internet Systems Consortium: ISC DHCP”, available from <https://www.isc.org/downloads/DHCP/> (accessed 2015-01-09).

[41] NEC Corporation, ”NEC：UNIVERGE IX2025”, available from <http://jpn.nec.com/univerge/ix/Info/ix2025.html> (accessed 2015-01-09).

[42] The CentOS Project, ”CentOS”, available from <http://www.centos.org/> (accessed 2015-01-09).

[43] Cisco Systems, Inc., ”Cisco Catalyst 3750 シリーズ スイッチ”, available from <http://www.cisco.com/web/JP/product/hs/switches/cat3750/prodlit/cat50_ds.html> (accessed 2015-01-09).

[44] Allied Telesis K.K., ”CentreCOM GS908M V2”, available from <https://www.allied-telesis.co.jp/products/list/switch/gs900mv2/catalog.html> (accessed 2015-01-09).

[45] Perl.org, ”The Perl Programming Language”, available from <http://www.perl.org/> (accessed 2015-01-09).

[46] Sergey Poznyakoff, ”GDBM”, available from <http://www.gnu.org.ua/software/gdbm/gdbm.html/> (accessed 2015-01-09).

[47] "The Expect Home Page", available from <http://expect.sourceforge.net/> (accessed 2015-01-09).

[48] G. Malkin, "RIP Version 2", RFC 2453 (IETF), 1998.

[49] J. Moy, "OSPF Version 2", RFC 2328 (IETF), 1998.

[50] "Quagga Routing Suite", available from <http://www.nongnu.org/quagga/> (accessed 2015-01-09).