NAIST-IS-DT9561014

博士論文

インターネットにおけるネットワーク構成技術の高機能化に関する研究

小林 和真

2000 年 2 月 1 日

奈良先端科学技術大学院大学
情報科学研究科 情報システム学専攻

本論文は奈良先端科学技術大学院大学情報科学研究科に
博士 (工学) 授与の要件として提出した博士論文である.

論文番号： NAIST-IS-DT9561014

提出者： 小林 和真

審査委員： 山本 平一 教授
千原 國宏 教授
福田 晃 教授
山口 英 助教授

提出日： 2000 年 2 月 1 日

インターネットにおけるネットワーク構成技術の高機能化に関する研究*

小林 和真

内容梗概

インターネットの発展を振り返ると，WWW による情報発信や電子メールなどの利便性が広く世間に認められるにしたがって，ユーザの急激な増加が見られるようになった．日本では，1993 年に初めてインターネット接続サービス事業者が誕生し, 現在では 2000 社を超える事業者が接続サービスを提供している．ユーザによるインターネットの利用形態は多岐にわたり，携帯電話による電子メールの受発信や，ノート型のパーソナルコンピュータを持ち歩き，移動先でも WWW にアクセスするといった光景が，しばしば見られるようになってきた．これらは，これまでに行われてきた数多くのネットワーク構築技術の高度化がもたらした効果に他ならない．インターネットは，こうしたネットワーク構成技術の高度化に支えられ，その発展を維持している．

本論文では，このインターネットの利便性の向上と，より一層の普及を目指し，従来のネットワーク構築技術に加え，新たに付加した 4 つのネットワーク構成技術を提案した．これは，筆者のインターネットにおけるネットワーク構成技術の高機能化に関する研究成果をまとめたもので，モバイルコンピューティングの実現に不可欠なセキュリティと認証機構，モバイル認証に対応したゲートウェイの実現，インターネットにおける経路制御についての新たなアプローチとしてのソースアドレスルーティング，岡山情報ハイウェイの構築により確立した地域ネットワーク構築モデルについての提案である．

*奈良先端科学技術大学院大学 情報科学研究科 情報システム学専攻 博士論文, NAIST-IS-DT9561014, 2000 年 2 月 1 日.

まず，モバイルセキュリティの実現を目指したアプローチとして，モバイルコンピュータなどの移動体に認証情報 (パスポート) を付加することでセキュリティ機能を高めた資源割当て手法である DHCPA(DHCP with Authentication) を提案した．次に，モバイル認証を前提とした DHCP 環境での，ネットワークへのアクセス制御を実現するモバイル認証ゲートウェイとして DAG(DHCP Access control Gateway) を提案し，その設計と実装を行った．実装したシステムにより，大学の講義室や企業の会議室など，第 3 者がアクセスし得るネットワーク環境においても，ユーザ認証によりネットワークへのアクセス許可を動的に制御することができ，安全なネットワークとして機能させることが可能となった．

また，地域 IX(Internet eXchange) を実現する時に問題となる経路制御についての新たな解決アプローチとしても利用可能な，送信者の持つソースアドレスを利用した新たな経路制御手法である STAR(Source address oriented Traffic Arrangement Router) を提案し，実装とその評価を行った．そして，岡山情報ハイウェイプロジェクトの基幹研究として筆者が実施した，地域インターネット構築モデルの確立に関する研究は，国内有数の地域インターネットエクスチェンジである OKIX(OKayama Internet eXchange) の実現に貢献した．本研究で確立した地域ネットワーク構築モデルである” パブリックファイバーモデル” は，地方自治体におけるネットワーク構築のモデルとして認知されており，域内の通信基盤を都市部なみに向上させることが可能となる．また，このモデルは岡山県以外の地域ネットワーク構築にも適用可能で，地域ネットワークの普及に役立っている．

これらのインターネットにおけるネットワーク構成技術の高機能化に関する研究は，インターネットの利便性の向上に大きく貢献し，これまで以上に，より広範囲のユーザが利用できる環境の実現を可能とした．

キーワード

モバイルセキュリティ，DHCP，認証，ソースアドレスルーティング，地域インターネット，地域 IX

Research on improvement of network construction technology in the Internet*

Kazumasa Kobayashi

Abstract

The number of Internet users is increasing rapidly as the benefits and convenience of the network are widely recognized. We have come to see active user's who accesses the Internet in different locations, such as e-mail and the World Wide Web accesses by carrying the notebook computers and the cellular phones, etc. The enhancement of these benefits and convenience in the Internet is just an effect of the research conduced for the improvement of the network technologies. The purpose of this thesis is to clarify network technologies that the author newly proposed. In this thesis, fore areas of technologies are focused as author's contributions to improvement of the Internet technologies.

First of all, DHCPA which added an authentication mechanism to DHCP, which was the resource allocation mechanism of the Internet standard, was proposed. The security where the resource is allocated by DHCP has been improved by adopting the passport for a mobile computer as authentication information.

Another contribution to the Internet technologies was DAG(DHCP access control gateway) that was designed and implemented as a gateway system which transmitted only packets of authenticated mobile computers. This DAG system can dynamically control the access permission to the DHCP service network by mobile authentication. It is possible to secure resources even in the DHCP service network environment that everyone is accessible.

*Doctor's Thesis, Department of Information Systems, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-DT9561014, February 1, 2000.

Thirdly, the STAR(Source address oriented Traffic Arrangement Router) system which was a new routing control mechanism was proposed for giving a solution for the regional Internet routing. A flexible route can be controlled with this system which uses not only the destination address but also the source address for routing path selections.

Finally, the author proposed the regional network architecture model. The proposed model uses attracting regional IX together with the construction of a public optical fiber by the local government. This model has been adopted actually in the Okayama information highway project.

The regional network architecture model in this research is acknowledged to the Ministry of Posts and Telecommunications. By applying this model, the communication infrastructure in the region can be constructed with the same scheme utilized in metropolitan areas. Obviously, this model is generic and not depends on situations around Okayama Prefecture therefore; it is a powerful scheme for expanding services of regional networks.

Keywords:

mobile security, DHCP, authentication, source address routing, Regional Internet, Regional IX

目 次

図 目 次

表 目 次

第 1 章

序論

インターネットは，地球上のすべての人々が自由に情報の交換を行うことを可能とし，知識の共有や世界中の人と双方向のコミュニケーションを楽しめるこれまでに無い新しい通信メディアである．この章では，このインターネットを取り巻くマルチメディア通信の現状を把握するとともに，本論文の位置付けと目的を明確にする．

1.1. インターネットの発展と普及

郵政省の平成 11 年度通信白書 [1] によると，平成 11 年 3 月現在の日本国内におけるインターネット利用者は，総人口の 13.4 % (約 1700 万人)，世帯普及率 11 %に達するという統計結果が掲載されている．インターネットを利用する企業数もすでに 80 %を超えており，ネットワークを活用した電子商取引は，情報流通，さらには物流に関するこれまでの社会構造を根底から変革させ，情報通信革命に対応することができない企業は生き残ることができないとまでいわれている．米国ではインターネットでの住所にあたるドメイン名 (企業名.com など) が高額で売買され，あらゆる産業分野でインターネットを利用した電子商取引が拡大を続けている．そして日本においても，社会生活におけるインターネットのかかわりは日増しに増加する傾向にある．

これまでのインターネットの発展を振り返ると，WWW による情報発信や電子メール，チャットなど，ユーザの利便性が広く世間に認められるにしたがって利用者の急激な増加が見られるようになった．日本では，1993 年に初めてインターネット接続サービス事業者が誕生し，現在では 2000 社を超える事業者が接続

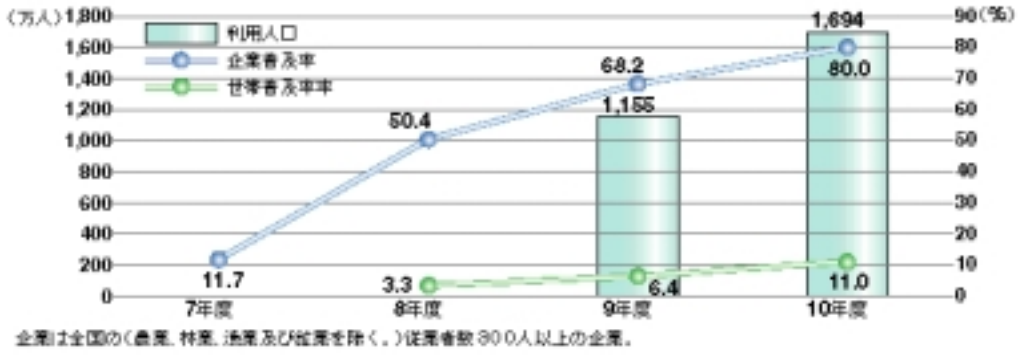


図 1.1 日本におけるインターネット普及率（郵政白書より抜粋）

サービスを提供している．また，インターネットに情報や映像などのコンテンツを発信するサーバ専門のレンタル事業や，インターネット上に設置されたサーバのアプリケーションをネットワーク経由で利用させるアプリケーション貸しサービスなど，インターネット事業の形態も多岐にわたり，今後も確実に拡大する傾向にある．

これら企業サイドの事業形態の多様化は，ユーザによるインターネットの利用形態の多様化と，ほぼ同時に進行している．携帯電話による電子メールの送受信や WEB サーバへのアクセス，ノート型のパーソナルコンピュータを用いた移動先でのインターネットへのアクセス，といった光景が街中でもしばしば見られるようになってきた．飛行機内でノート型のパーソナルコンピュータ用の電源が利用できるようになったことも，こうしたユーザの増加が大きく影響していると考えられる．日本におけるインターネットを利用した電子商取引も，オンライン投資信託，自動車販売，書籍販売，オンラインオークション，部品・資材の調達と幅広く普及しはじめており，情報化による産業形態の変革をさらに加速させている．

これらインターネットの発展と普及にともない，新たなネットワーク構成技術が必要となってきている．拡大するユーザニーズを支える新たなアプリケーションにとって，電子商取引で必要とされるセキュリティ技術の向上や通信サービスにおける品質の保証など，ネットワーク構成技術の高機能化は不可欠である．

一方，急速なインターネットの普及は，これまであまり考えられなかった新たな社会問題を引き起こしはじめている．インターネット先進国である米国では，“デジタルデバイド (digital divid)” という言葉を耳にするようになってきた．これは，所得や学歴，地域格差などによりインターネットの利用環境に格差が生じ，その格差が再び所得や学歴により大きな格差を生じさせることを意味する造語である．このデジタルデバイドは，個人ユーザだけでなく，国や企業，大学などの教育機関などの間でも広がりつつあり，情報化社会におけるあらたな差別として問題視されはじめており，早急な対策の必要性が指摘されている．

1.2. ネットワーク構築技術の高機能化

インターネットの普及に関連して，いくつかの転換期がこれまでに存在した．学術研究ネットワークとして誕生したインターネットは，多くの大学や企業の研究者らの活用を経て，商用サービスへの転換が行われた．学術研究用のネットワークとしての活用を通じてその利便性が広く認められ，社会的な情報インフラストラクチャとしての地位を築くに至ったわけである．商用化によりこれまで以上に多くのユーザがインターネットを利用するようになり，今日の爆発的なユーザ増加をもたらした．

インターネットには，ほとんどすべてのユーザが利用するキラーアプリケーション (killer application) と呼ばれるタイプのアプリケーションが存在する．キラーアプリケーションの具体例として，WWW(World Wide Web) が挙げられるが，この WWW の出現でインターネットでのデータ通信が，文字中心から画像や音声などを含んだマルチメディアデータ通信へと変遷することになった．この WWW の爆発的な普及による通信量の急激な増大は，インターネットを構成するネットワーク技術にとって文字通り “キラー” となった．将来のマルチメディア通信を睨んで研究開発がすすめられていた ATM(Asyncronus Toransfer Mode) や POS(PPP over SONET) に対応した超高速ネットワーク製品が相次いで製品化され，この爆発的な通信需要に適応できる新しいネットワーク技術がインターネットを支えることとなった．また，発生する通信量そのものを減少させるため，WWW データに着目したキャッシング技術を応用した製品も多数開発され脚光を

浴びることとなった．特定のユーザからのアクセスを優先して伝送するような帯域制御を技術も注目を集めており，いくつかのアイデアが製品化に結びついている．ネットワーク業界の製品化のサイクルは，ドッグイヤー (ネットワーク業界の 1 年は従来の 3 年〜5 年は進む) とよばれるほどで，急激なユーザ増加やユーザニーズの変化に対応するための激しい技術開発競争が今もなお続いている．

インターネットの最近の特徴として，他のメディアとの融合がある．既存の CATV 網を活用した高速インターネット接続サービスや，携帯電話からのインターネット接続サービスなど，既存メディアの特性を生かした新たな利用形態が注目を集めている．また，これらを利用するユーザの爆発的な増加は，それぞれのメディアの特徴を生かした新たなネットワーク構築技術がこれまで以上に必要であることを示唆している．

このように，これまでのインターネットの発展の歴史は，ユーザニーズに適応したネットワーク構成技術の高機能化に支えられている．インターネットは，理論よりも実践的で，実用的な動作するプログラムや装置を重要視してきた．誕生した新たなアプリケーションに適用できるように，新たなネットワーク構成技術が提案され，新たな技術を用いたネットワーク構築を繰り返しインターネットは発展を遂げてきた．

1.3. 本論文であつかう題目

本論文では，インターネットの利便性を高め，より一層の普及を加速すべくインターネットにおけるネットワーク構成技術の高機能化を目標として，これまでに筆者が行ったふたつの異なる側面からの研究成果について述べる．

ひとつめは，ノート型のパーソナルコンピュータなどの移動体通信における安全なネットワーク接続環境を提供するためのモバイルセキュリティに関する要素技術の研究，ふたつめは，より広範囲のユーザに等価なサービスを提供するための，地域ネットワーク構築技術の確立に関する研究である．

1.3.1 モバイルセキュリティに関する研究

マイクロソフト社が，Windows95/98 のネットワーク接続機能の標準として採用した DHCP(Dynamic Host Configuration Protocol)[2][3] は，Windows の普及とともにユーザに浸透し，すでに各所で効果的に利用されている．DHCP を利用すれば，ユーザは，自分のコンピュータをネットワークに接続する際のわずらわしい設定作業から開放され，ケーブルをコネクタに差し込むだけで接続することができるようになる．しかしながら DHCP は，ネットワーク接続時のユーザ認証 (コンピュータの識別) を何も行っておらず，悪意を持った不正利用者によるネットワーク接続を防ぐ手立てはこれまで存在しなかった．筆者は，この問題を解決するために，ノート型のパーソナルコンピュータのような可搬型のコンピュータを認証するためのモデルとしてパスポートモデルを提案し，DHCP にこのモデルによる認証機構を組み込んだ DHCPA(DHCP with Authentication) を実装し有効性を検証した．

さらに認証後の堅牢なネットワークアクセス制御を実現するために，DHCP とアクセス制御ゲートウェイを連携させるアーキテクチャを提案し，その実装として DAG(DHCP Access Gateway) を開発し，有効性の検証を実施している．これらの一連の研究で，DHCP 利用者に対するネットワーク利用における安全性を高めることができ，利便性の向上に貢献している．また，研究の成果は，実際の製品化にも貢献しており，この技術を取り入れた製品がすでに出荷されている [4]．

1.3.2 地域ネットワーク構築に関する研究

インターネットによる膨大な情報を活用するための通信基盤 (情報インフラ) は、確実な需要が見込まれる都市部から順に整備されてきた．そのため，インターネットの特徴のひとつである地理的な制約を受けないというメリットが，かなりの部分で失われてしまっている．地方都市や過疎地の住民は，都市部の住民に比べて多大な通信費用を負担しなければインターネットを利用できなかったり，低速なネットワークしか利用できないのが現状である．このような情報インフラの整備についての不平等は，情報インフラ格差による新たな差別として “デジタルデバイド (digital divide)” と呼ばれる情報差別を引き起こしはじめている．そこで筆

者は，より多くのユーザに十分に平等なインターネット利用環境を提供できる枠組みとして，地域ネットワークの構築に着目し，地域ネットワーク構築時の技術的な課題の解決に取り組んだ．

まず，前述のアクセス制御ゲートウェイの研究で得たゲートウェイ構築に関する技術を活かし，地域ネットワーク構築で技術的な懸案となっていたルーティング問題の解消を試みた．インターネットにおけるこれまでの通信では，受信者の宛先情報 (ディスティネーション IP アドレス) のみを利用してデータ送信の経路を決定していた．この経路決定に発信者アドレス (ソース IP アドレス) を活用することで，ユーザ毎に異なる経路を選択することを可能とする新たなルーティング手法として，STAR(Source address oriented Traffic Arrangement Router) の提案を行った．この手法は，筆者が中心となって構築した岡山情報ハイウェイにおける地域インターネットエクスチェンジ (地域 IX：Regional Internet eXchange) でも利用されており，地域ネットワーク構築における新手法として利用されている．

一方で，地方都市の情報化は，東京や大阪などの都市部と比較すると思ったほど進展していない．インターネット接続サービスを提供する事業者は，事業採算性を考慮するため，中小規模の都市や過疎地域では大規模な事業展開はなかなか行われない．もちろん，時間が経過すればそれなりのサービスが提供されることは間違い無いが，このままでは都市部との情報格差は拡大する一方である．情報化による経済の変革が叫ばれる中で，地域の情報化を着実に推進するには，地方自治体など行政による情報化への取り組みが不可欠である．地域住民が各種の情報に接する機会を，都市部住民と同等に提供することは，21 世紀を目前に進展しつつある情報革命に追随する上でとても重要なことである．

その中で，筆者が取り組んだ岡山情報ハイウェイ構想は，地方自治体が主導する新たな地域情報化の実現手法として注目を集めている．この研究において筆者が提案した地域ネットワークにおける構築手法モデルには，(1) 自治体が光ファイバーを自設することで，域内の高速通信インフラを構築し活用する，(2) 域内の高速性を最大限に生かすため，地域 IX を通信インフラと同時に実現する，(3) インターネットへの接続環境を行政が独自に用意せず，地域 IX に接続しているインターネット事業者を活用する，(4) 住民の地域ネットワークへのアクセス手段は，地域 IX に接続している CATV 事業者やインターネット接続事業者が提供

する接続サービスを利用する，という特徴がある．

平成 7 年に始まった岡山情報ハイウェイ構想は，3 年の実験期間を経て平成 11 年 4 月から一般事業者に開放され，地域ネットワークを活用した新たな情報産業の育成に貢献し始めており，岡山県以外の自治体でも同様な取り組みが活発に行われはじめている．

1.4. 本論文の構成

本論文は，以下の章で構成される．

第 2 章では，インターネットを構成する主要な構成技術について説明する．インターネット構築におけるルールを定めたインターネットプロトコル，インターネットにおける通信の仕組みの中で，本論文で取り扱うモバイルコンピューティングに関連するプロトコル，資源割当てのための DHCP(Dynamic Host Configuration Protocol)，認証技術，経路制御プロトコルについて論ずる．

第 3 章では，従来のインターネット構築技術に加え，本研究により付加したモバイルネットワークの高機能化に関する技術についてふたつの視点から述べる．まず，モバイルセキュリティの実現を目指したアプローチとして，モバイルコンピュータなどの移動体に認証情報 (パスポート) を付加することで，セキュリティ機能を高めた資源割当て手法である DHCPA(DHCP with Authentication) を提案する．モバイル認証を前提とした DHCP 環境でのネットワークへのアクセス制御を実現する手法として，DAG(DHCP Access control Gateway) を提案し，その設計と実装について述べる．

第 4 章では，地域ネットワークにおける構築手法を考察し，本研究により確立した地域ネットワークの高機能化に関する技術について提案する．まず，地域 IX(Internet eXchange) を実現する時に問題となる経路制御問題についての解決アプローチとして，送信者の持つソースアドレスを利用した新たな経路制御手法である STAR(Source address oriented Traffic Arrangement Router) を提案し，その設計と実装を行い，地域ネットワークにおける有用性を示す．

そして，実用的な地域インターネットの構築を目指し，岡山情報ハイウェイプロジェクトの基幹研究として実施した，地域インターネット構築モデルであるパ

ブリックファイバーモデルの確立に関する研究の成果について論じ，実際に稼動している地域インターネット網である岡山情報ハイウェイについて，その構成技術と特徴を述べる．

第 5 章は，結論であり，本論文で得られた成果を総括するとともに，今後の課題について述べる．

第 2 章

インターネットを構成する技術

この章では，インターネットにおける通信の仕組みを述べ，本論文で取り扱うモバイルコンピューティングに関連するプロトコル，動的な資源割当てプロトコルである DHCP(Dynamic Host Configuration Protocol)，認証技術，経路制御のためのルーティングプロトコルについて示す.

2.1. インターネットプロトコル

インターネットでのさまざまな取り決めは，RFC(Request for comments) と呼ばれているドキュメントとして公開されている．インターネットに接続する装置，プログラム，ネットワークプロトコルなどの標準規約は，この RFC で規定されている.

インターネットは，動作するプログラムと現実的なプロトコルによってささえられている．RFC は実際に動作するネットワークで検証され，現実的な運用に耐えられるように何度も改定されている．この論文で言及している RFC は，論文執筆時点で有効なものである．最新の RFC については，インターネットで公開されているので [5] を参照して欲しい.

2.1.1 ホストと IP アドレス

インターネットでは，ネットワークに接続されるコンピュータの事をホストと呼んでいる．それぞれのホストには，ネットワーク上でホストを識別するための番号として，IP アドレスが割り振られている．インターネットでは，この IP ア

ドレスでネットワーク上のホストを識別し，両者間の通信路を確立している．

現在広く利用されている IP アドレスは，IPv4 アドレスと呼ばれるもので 4 オクテットから構成され，“163.221.10.10” のように各オクテットの 10 進数表現を “.”(ピリオド) で区切って表現されている．一般的に用いられている “www.aist-nara.ac.jp” などのホスト名（ドメイン名）は，ユーザがわかりやすいように，この IP アドレスに対応付けられた名前である．

また IP アドレスは，そのホストが接続しているネットワークを意味するネットワークアドレスと，ホスト自身を識別するためのホストアドレスのふたつの部分に分けられている．通信しようとする両者間では，相手ホストの IP アドレスから，まず通信相手のホストが接続しているネットワークを特定し，次にホストアドレスで相手ホスト自身を特定している．

2.1.2 ネットワーク間の接続

ネットワークとネットワークを相互に接続する装置のことを，“ルータ” または “ゲートウェイ” と呼んでいる．ルータは，接続しているネットワーク双方の情報を持ち，通信相手のホストにデータを到達させるための中継処理を行っている．

ルータの重要な機能のひとつに経路情報の交換がある．経路情報とは，ルータがデータの中継処理を行う場合に必要な情報で，送信相手のネットワークにデータを到達させるために，次にどのルータに対してデータを中継すればよいかを決めるために利用される．このルータ間での経路情報の交換に用いられる専用のプロトコルをルーティングプロトコルと呼んでいる．

インターネットは，このルータによって相互に接続されたネットワーク群から構成された大規模なネットワークである．

現在のインターネットでは，ルーティングプロトコルは，大学や企業など組織内部で用いる IGP(Interior Gateway Protocol) と外部との接続に用いる EGP(Exterior Gateway Protocol) に大別されている．

2.1.3 IP アドレスに関する諸問題

IPv4 アドレスは，32bit でアドレス情報を表現している．インターネットの普及とともに，32bit で表すことができるアドレス空間 (2^{32}) では，利用者のニーズに対応できないという “アドレス枯渇” の問題が発生している．

この問題に対応するために，次世代の IP アドレスとして IPv6[6] の開発が推進されている．IPv6 は，128bit でアドレス情報を表現しているため，IPv4 と比べて広大なアドレス空間を利用することが可能である．

また，現行の IPv4 アドレスをより有効に活用するための仕組みも提案され，効果を発揮している．インターネットへの接続が不要なホストに割り当てるためのプライベートアドレス [7] の導入や，プライベートアドレスをインターネットへのアクセスが可能なグローバルアドレスに変換する NAT(Network Address Translater)[8]，すべてのホストに個別にアドレスを割り当てるのではなく，必要になった時に動的にアドレスを割り当てる DHCP(Dynamic Host Configuration Protocol)[2][3] などがアドレス空間の有効利用に貢献している．

2.2. モバイルコンピューティング

インターネットでは，IP アドレスを用いてホスト自身の識別と接続位置に関する情報を表現している．そのため移動ホストの場合，移動先での接続に新たな IP アドレスを必要とし，移動前と異なる IP アドレスになるため結果的に別のホストとして識別されてしまう．そのため，現在の IP アドレスを移動するホストにそのまま対応させることはかなり難しい．一般に移動するホストは，移動によって異なる IP アドレスが割り当てられてしまうため別のホストとして識別されてしまう．

ネットワークに接続されていたホストが，ホスト自身の物理的な移動により，別のネットワークに接続地点を変更した時に，ホストの移動をユーザに意識させない性質をネットワーク透過性と呼ぶ．このネットワーク透過性を持ちながら人の移動に伴ってネットワーク的にも移動するホストを “移動ホスト (Mobile Host)” と呼んでいる．もし，ホスト自身の識別情報と位置情報を分離することができるならば，ホストがネットワーク上を移動しても位置情報のみを変更すればよいこ

とになる．あるいは，ホストが移動しても，IP アドレスが変更されないような仕組みを提供すれば，ホストの移動を意識しなくてすむ．この場合，ホスト自身の識別情報は移動にかかわらず一定となり，ネットワーク透過性を実現できる．この移動ホストとネットワーク透過性を実現するために，インターネットではさまざまな提案がなされている．

その代表的なものは，移動ホストの IP アドレスを変更せず移動先のネットワークでトンネリングの技術を用いて仮想的に本来のネットワークに接続する方法である．この方法は IETF(Internet Enginiaring Task Force) で議論され，インターネット標準の MobileIP プロトコルとして採用されている [9][10]．また，筆者らが参加しているインターネットに関する研究プロジェクトである WIDE プロジェクトで開発された VIP(Virtual Internet Protocol) [11][12][13] も，移動ホストに関する問題を解決するアプローチのひとつである．

2.2.1 MobileIP

MobileIP プロトコル [14] は，RFC2002[9] で規定されているインターネット標準のモバイル対応プロトコルである．移動ホストの本拠 (ホームエージェント) とホストに移動先ネットワークで MobileIP を実現するために動作する外部エージェントとの間を IP トンネリングの技術を用いることで仮想的に接続し，移動後も常に本拠のネットワークと接続しているように見せかけている．これにより，ユーザは移動ホスト自身の移動を意識すること無く，ネットワークを利用することが可能となる．MobileIP プロトコルは，標準化の過程で最も多くの提案が行われたプロトコルである．その結果さまざまな提案を寄せ集めた仕様となってしまい，標準化が完了した現在でも，このプロトコルを全面的に採用している製品はあまり多く見られない．

現実的なインターネットにおいては，セキュリティの確保や各ネットワーク毎の運用ポリシなどに違いがあるため，必ずしも MobileIP を実現するための前提を満たしたネットワークとなっていない．また，すべてのネットワークが外部エージェントを有する事態を想定すると，MobileIP で用いられている IP トンネリングの影響で経路制御がかなり複雑化してしまい，肝心のスケーラビリティが失われてしまう恐れがある．こうした事実も普及を阻む大きな要因となっている．

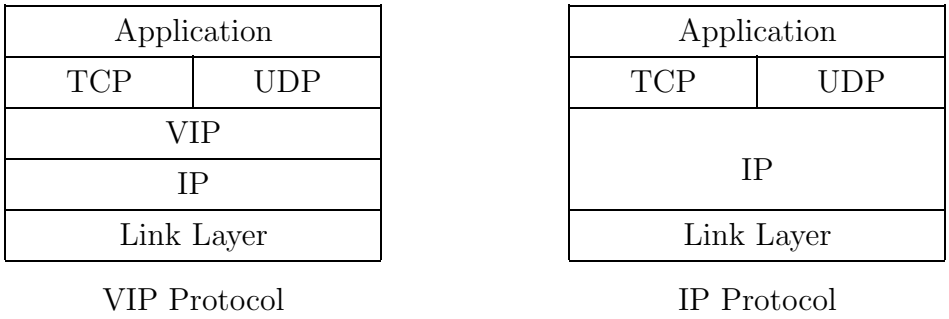


図 2.1 VIP と IP の比較

VIP Address		
IP Address		
Timestamp		
Flags	Timer	unused

図 2.2 VIP プロトコル : AMT Table Entry

2.2.2 VIP

VIP は，ネットワーク層をホスト識別のための仮想ネットワーク層と物理的な接続位置に関する情報を表すためのネットワーク層のふたつに分け，識別情報と位置情報を分離している．この概念をインターネットプロトコルに適用すると，ホスト自身の識別情報は VIP アドレスで，ネットワーク上の接続位置に関する情報は IP アドレスで表現される．

図 2.1に VIP プロトコルと IP プロトコルの違いを示す．

VIP では，実際の通信時にホストの識別子である VIP アドレスに位置情報を対応させるデータベースが必要になる．そこで，AMT(Address Mapping Table) を用いて VIP アドレスと IP アドレスのマッピングを行い，ホストの識別情報と位置情報の整合をはかっている．図 2.2に，AMT に登録されるマッピング情報 (AMT Table Entry) を示す．

このような用途に用いられるデータベースは，インターネットにおける広範囲

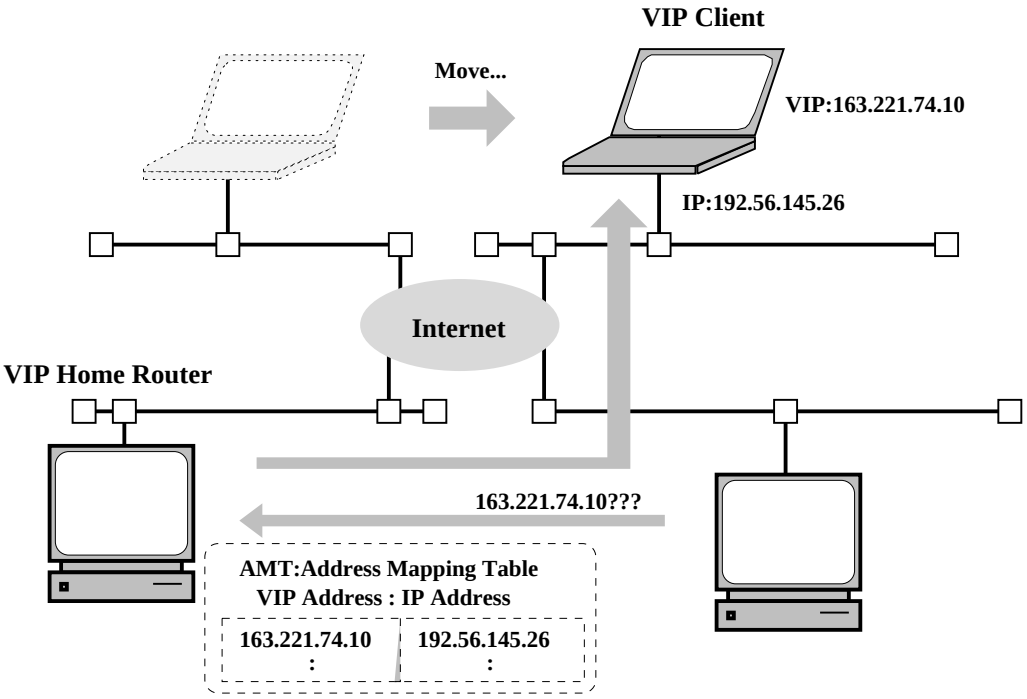


図 2.3 VIP プロトコル：VIP 環境における移動ホストとの通信

の情報を一貫して更新できる必要がある．さらに，データの検索速度も高速性が要求され，通常のデータベースでは対応することが難しい．

そのため，AMT の更新には拡散キャッシュ法 [15] を用いている．拡散キャッシュ法とは，ネットワークを流れる通信データを用いてデータベースエントリを更新していく手法で，通信データが流れる経路に関係するデータベースのエントリのみを効率よく更新させる方法である．

図 2.3は VIP 環境における移動ホストとの通信のメカニズムついて示したものである．この図を用いて VIP の通信メカニズムを簡単に説明する．

移動ホストが以前と異なるネットワークに接続されると，ホームルータに対して AMT に登録されているエントリを更新するパケットを送信する．ホームルータとは，移動ホストが所属する仮想ネットワークから実際のネットワークへのルーティングを行うホストである．

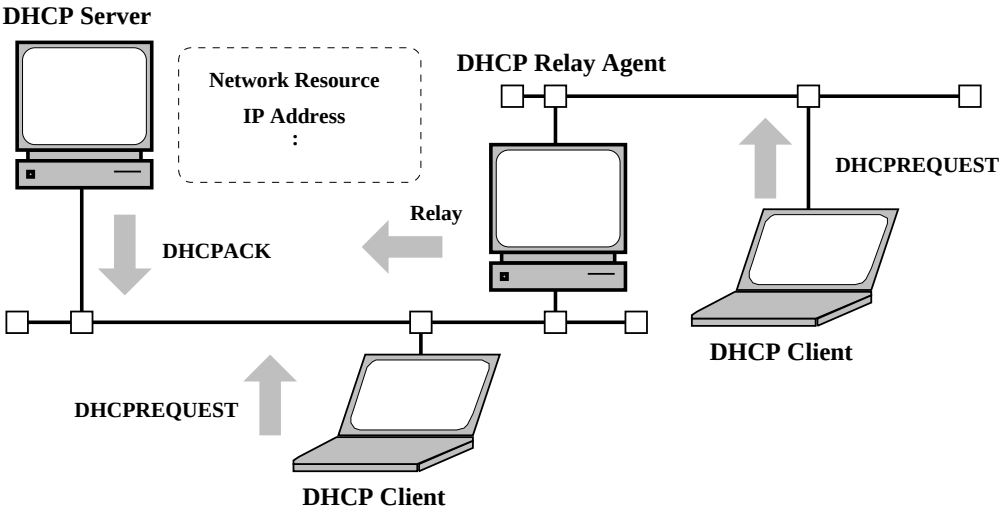


図 2.4 DHCP

移動ホストに対して通信を要求するホストは，移動ホストの識別子である VIP アドレスに対してパケットを送信する．このパケットは移動ホストの所属するホームルータに送られる．移動ホスト宛のパケットをホームルータが受け取ると，AMT に照らし合わせ，移動ホストの現在の IP アドレスにパケットを中継する．このとき経路上の VIP に対応したルータ装置の AMT エントリも更新されるため，それ以降のパケットは，移動ホストと通信相手のホストと間で直接送信される．

これにより，ネットワーク的な移動にかかわらずホストの識別情報は VIP アドレスとして常に一定となり，ネットワーク透過性を確保できる．

2.3. DHCP

DHCP(Dynamic Host Configuration Protocol) [16][17][18] は，ユーザの介在無しに自動的に資源の割り当てができ，かつ割り当てた資源の回収が可能な資源割り当てプロトコルである．

DHCP はネットワーク資源の割り当てを行う DHCP サーバと，資源を要求す

るクライアント，割り当て要求を中継するリレーエージェントから構成される (図2.4参照).

DHCP は，マイクロソフト社の Windows95/98 などにも標準機能として採用され，UNIX ワークステーションなどでも数多く利用されている．ユーザがホストをネットワークに接続するだけで，煩わしい設定作業は DHCP が自動的に実行してくれるため，ノートパソコンを利用しているユーザなどに人気が高い.

2.4. 認証とデジタル署名

本論文で議論する認証モデルでは，公開鍵暗号系 [19] のひとつである RSA 暗号系 [20][21] [22][23] を用いたディジタル署名を応用して移動ホスト認証系を実現する.

2.4.1 暗号化/復号化の記述

本論文中での暗号化，および復号化の記述は次のように定める.

$$E\{Message\}^{K_{key}} \cdots (1)$$
$$D\{Cypher\}^{K_{key^{-1}}} \cdots (2)$$

式 (1) は，秘密鍵 K_{key} によりメッセージ $Message$ を暗号化することを意味し，式 (2) は，公開鍵 $K_{key^{-1}}$ によりメッセージ $Cypher$ を復号化することを意味する.

2.4.2 MD5

本論文で取り扱うメッセージの認証確認には，MD5 Message Digest Algorithm[24] を利用したメッセージ復元法を用いる．メッセージ復元法とは，受信した認証データを復号化し，復元したメッセージが正当なメッセージかどうかを判断し認証する方法である．これにより，送信メッセージの偽造や改竄を防ぐことが可能となる.

MD5 では，任意の大きさの入力メッセージ ($Message$) に対して，一方向関数による 128 ビットの $MessageDigest$ を生成する．

$$\text{MD5 } MessageDigest = \text{MD5}[Message]$$

MD5 アルゴリズムは，入力メッセージ ($Message$) が完全に同じ場合のみ，同じ MD5 $MessageDigest$ を生成する．この性質を利用して，受信者側でのメッセージの認証確認に利用する．

送信者側でメッセージ $Message$ を暗号化する際に，この $Message$ の MD5 $MessageDigest$ を計算し，送信メッセージに含めて送信する．

$$\text{送信メッセージ} = \text{E}\{\text{MD5 } MessageDigest + \text{MD5}[Message]\}^K$$

受信側では，受信したメッセージを，$Message$ と MD5 $MessageDigest$ に切り分け，$Message$ の MD5 $MessageDigest$ を計算する．この MD5 $MessageDigest$ が受信したメッセージに含まれていたものと一致すれば，送られてきたメッセージは，正しいメッセージ $Message$ であると認証できる．

2.4.3 デジタル署名

文書の最後に，本人が書いたことを証明するために，古来から本人の名前などを署名してきた．これと同様に，電子的な文書やデータにも，その文書やデータの信頼性を保証するために，暗号化技術を駆使した電子的な署名を “デジタル署名” として添付することができる．

一般的なディジタル署名では，受信者 R と送信者 S の間で，次の 3 つの条件を満足する必要がある．

1. R が受信したメッセージが，S が送信したものであると確認できること．
2. R を含む第三者 T が，S のメッセージを偽造できないこと．
3. S が，メッセージを R 宛に送信した事実を送信後に否定できないこと．

ディジタル署名に利用できる主な暗号系には，DES などの慣用暗号系と RSA などの公開鍵暗号系がある．慣用暗号系を用いる場合には，送信者と受信者の間

で鍵を共有しなければならない．このため，送受信者の組合せの数だけ鍵を用意する必要があり，不特定多数との通信を前提とするインターネットでは，あまり現実的なシステムとは言えない．また，署名法には，受信者が受信したメッセージの正当性を直接確認する直接署名法と，信頼できる第三者を調停者としてメッセージの正当性を確認する調停署名法がある．

2.5. インターネットとルーティング

インターネットは，数多くのネットワークが相互に接続されることで，巨大なネットワークを構成している．これらのネットワークは，個々が自律系 (AS:Autonomous System，以下 AS と略す) として機能し，自らのネットワークに接続されているネットワークについての経路情報を集約し，各 AS 間で相互に交換することで到達性を確保している．インターネット接続事業者は，それぞれひとつ以上の AS を構成し，他の接続事業者との間での接続性を確保するために，他事業者 AS との間で経路情報の交換を行っている．

また，AS 間の接続情報を相互に交換するための交換場所として，インターネットエクスチェンジ (IX:Internet eXchange，以下 IX と略す) とよばれる相互接続ポイントが形成されている．

インターネット接続事業者は，各 AS 内部，すなわち自らのネットワーク内部のホストやネットワーク間での経路交換と，他事業者との間の経路交換のふたつの経路交換を行うことになる．こうした，AS 内での経路交換プロトコルは IGP(Interior Gateway Protocol) と呼ばれ，代表的なものに RIP(Routing Information Protocol)[25][26]，OSPF(Open Shortest Path First)[27] などがある．また，異なる AS 間での経路交換プロトコルは EGP(Exterior Gateway Protocol) と呼ばれ，BGP(Border Gateway Protocol)[28] などが用いられている．

2.5.1 OSPF

OSPF(Open Shortest Path First) は，AS 内のすべてのルータが，ネットワーク全体の構成を把握し，最適な経路を決定することができるルーティングプロトコルである．比較的規模の大きな組織内ネットワークなどで利用され，目的ホス

トまでの経路が複数存在するようなバックボーンネットワークで，主に用いられるプロトコルである．

OSPF では，リンクステート型のアルゴリズムを用いてルータ間でネットワーク情報を交換している．リンクステートとは，各ルータのネットワークへの接続情報を意味し，IP アドレスやサブネットマスク，宛先への経路選択の優先順位を表すメトリックなどが交換される．そして各ルータから得られた情報を元に全体のネットワーク構成をまとめたネットワークトポロジを作成する．そして得られたトポロジ情報をもとに，各ルータはトポロジ内の自分の位置を起点とした他のルータへの最短経路を SPF(Shortest Path First) アルゴリズムにより計算し，ルーティングテーブルを作成する．これにより，目的のホストまでの最適な経路による通信を可能としている．

OSPF のもうひとつの長所は，VLSM(Variable Length Subnet Mask) に対応している点である．VLSM は，IP アドレスでのネットワーク部分とホスト部分の割り当て比率を，サブネットマスクによって変更するもので，本来はホストアドレスとして利用するアドレスブロックを細分化し，新たなサブネットワークとして利用できるようにするメカニズムである．VLSM を用いれば，ネットワーク規模に応じたアドレス空間を割り当てることができ，枯渇している IP アドレスを有効に利用できる．

2.5.2 BGP

BGP(Border Gateway Protocol) は，AS 間での経路交換に用いられるルーティングプロトコルである．ISP(Internet Service Provider) 間のほとんどの経路交換で，BGP プロトコルの最新バージョンである BGP-4 が利用されている．

このプロトコルの特徴は，AS を経路決定のひとつの単位として扱う点で，AS 内に存在するすべてのネットワークを同一視することで，AS 単位の経路選択を可能としている．

各ルータは，得られた AS に関する情報を集約し，最短の AS に至る経路 (AS Path) を計算し，データを中継すべき経路を決定する．

2.6. インターネットエクスチェンジ

日本国内における著名な IX は，筆者も運営，構築に参加している WIDE プロジェクト [29] の NSPIXP-2(東京)/NSPIXP-3(大阪)[30] や，商用 IX として運営されている JPIX や MEX がある．

これらの IX は，インターネットにおける通信の到達制を確保するために構築されており，IX に接続するインターネット接続事業者は，自身の AS に所属するすべてのネットワークについての経路情報を，他の接続事業者との間で相互に交換している．IX での経路交換などにより得られる，インターネットに接続しているすべてのネットワークに関する経路情報のこと “Full Route” と呼んでいる．こうした Full Route の交換が可能な IX を，特に GIX(Global Internet eXchange) と呼んでいる．前述の，NSPIXP-2/NSPIXP-3 や JPIX，MEX は，いずれも GIX である．これらの GIX では，数多くのインターネット接続事業者が相互に経路情報の交換を行っている．

一方，すべてのネットワークについての経路交換を目的とせず，地域内のネットワークに関する経路情報のみの交換を目的に設置された IX も存在する．このような IX は，一般には地域 IX や RIX(Regional Internet eXchange) と呼ばれ，GIX とは異なる位置付けの IX として定着しつつある．

第 3 章

モバイルネットワークに関する高機能化

この章では，従来のインターネット構築技術に加え，本研究により付加したふたつのモバイルセキュリティ技術について述べる．まず，移動ホスト認証のための汎用モデルとしてパスポートモデルを提案し，DHCP(Dynamic Host ConfigurationProtocol) を拡張することによる資源割り当て時におけるホスト認証問題の解決手法を提案する．また，DHCP 環境における認証機構の欠点を指摘し，これを補うことができる DAG(DHCP Access control Gateway) を提案する．このふたつを組み合わせることで，移動ホスト環境における安全なネットワーク環境の構築が可能となる．

3.1. モバイルセキュリティ

これまでにもインターネットでは，移動するホストに対応するために数多くのプロトコルや実装が提案され，実用化を目指した研究が行われてきている．しかし移動ホストに対応した環境を実際に構築してみると，さまざまな問題点が明らかになってくる．そのひとつが移動ホストの認証に関する問題である．ホストが移動した先でも，移動前と同様にインターネットのサービスを利用するには，移動の前後で同一のホストであることを示す必要がある．そのためは，移動するホストの認証技術が必要不可欠である．

3.1.1 移動ホストと資源割り当て機構

コンピュータ関連技術の急速な進歩にともなって，コンピュータも小型軽量化が進んでいる．これにより，従来のワークステーションに匹敵する能力を持つシステムを簡単に持ち運ぶことができるようになってきた．利用者にとって必要な計算機利用環境をそのまま持ち運べ，かつインターネットへと接続できるホストを実現できれば，移動した先や移動中などさまざまな場所で自由にコンピュータを用いた作業を行うことができる．このような環境を実現する技術は従来のコンピュータの利用形態に大きな変革をもたらす技術となり得る．このような利用者とともに移動しネットワークに接続されるホストを，“移動ホスト” (Mobile Host) と呼んでいる．

インターネットでは，ネットワークに接続されたホストを識別するために IP アドレスを用いてホスト自身の識別と接続位置に関する情報を表現している．そのため移動ホストの場合，移動先での接続に新たな IP アドレスを必要とし，移動前と異なる IP アドレスになるため結果的に別のホストとして識別されてしまう．

この問題を解決するために，MobileIP[9] や VIP(Virtual Internet Protocol)[11][13] が提案されている．

移動ホストに対応するためのこれらの提案では，ほとんどの場合に移動した先で IP アドレスなどの何らかのネットワーク資源を必要とする．

他にも従来から用いられてきた X ターミナルや，ディスクレスクライアントなど，起動時にサーバの情報や Boot プログラムなどのネットワーク資源の割当を要求する装置も存在する．このような要求に対応するために，インターネットではいくつかの資源割当機構が提案されている．

BOOTP(Bootstrap Protocol) [31] は，ホストに設定する IP アドレスや Boot プログラムなど要求されたネットワーク資源をユーザの介在無しに割当てることができるプロトコルである．

DHCP(Dynamic Host Configuration Protocol) [16][17][18] は，BOOTP 上位互換の資源割り当てプロトコルであり，ユーザの介在無しに動的な資源の割り当てができ，かつ割り当てた資源の回収が可能なプロトコルである．本論文では，動的資源割り当て機構として，この DHCP に着目する．

3.1.2 移動ホスト認証の必要性

BOOTP や DHCP などの資源割り当てプロトコルは，割り当て要求を行うクライアントとして，X ターミナルやディスクレスワークステーションなど処理能力が著しく低いホストを想定している．これらのホストの場合は，資源割り当て時に複雑な認証処理を行わせることが能力的にも非常に困難であり，装置の設置場所も一定で認証を考慮する必要性が少ないと従来は考えられてきた．

しかし，マイクロソフト社の Windows95/98 などの，DHCP クライアントを標準で装備しているオペレーティングシステムの出現や，携帯型のノートパソコンの普及など，新たな資源割り当てに対するニーズが大幅に広がってきている．

また，無線 Ethernet や赤外線 (IR) 通信装置のような無線ネットワークの場合は，無線が届く範囲内であれば比較的簡単にネットワークに接続できてしまう．

ところが BOOTP プロトコルや DHCP プロトコルでは，資源の割り当てに際して割り当てるホストの認証をまったく考慮していない．これらのプロトコルを扱う BOOTP サーバや DHCP サーバは，どのようなクライアントからの割り当て要求に対しても，その要求に応じて IP アドレスなどの資源を割り当ててしまう．サーバから自動的に割り当てられたアドレスで，誰でもネットワークを利用できるため，セキュリティの上からも明らかに好ましくない．

そこで本論文では，移動ホストの認証を考慮した資源割り当て機構を提案し，この問題の解決を試みる．

3.1.3 パスポートモデルの提案

我々が海外に出かける場合，自分自身の身元を証明するためにパスポートを所持する．パスポートによって他国への入国が許可され，現地での活動を許される．本論文で提案する移動ホストのための認証機構モデルでは，このパスポートの概念を用いる (以下パスポートモデルと呼ぶ).

パスポートモデルでは，移動ホストの身元を証明するために識別情報である PASSPORT をホスト毎に用意する．PASSPORT は，移動ホストの所属する組織 (サイト) の責任において発行され，移動ホストの身分を保証する．また，この PASSPORT を発行するサーバをホームサーバと呼ぶ (図 3.1参照)。

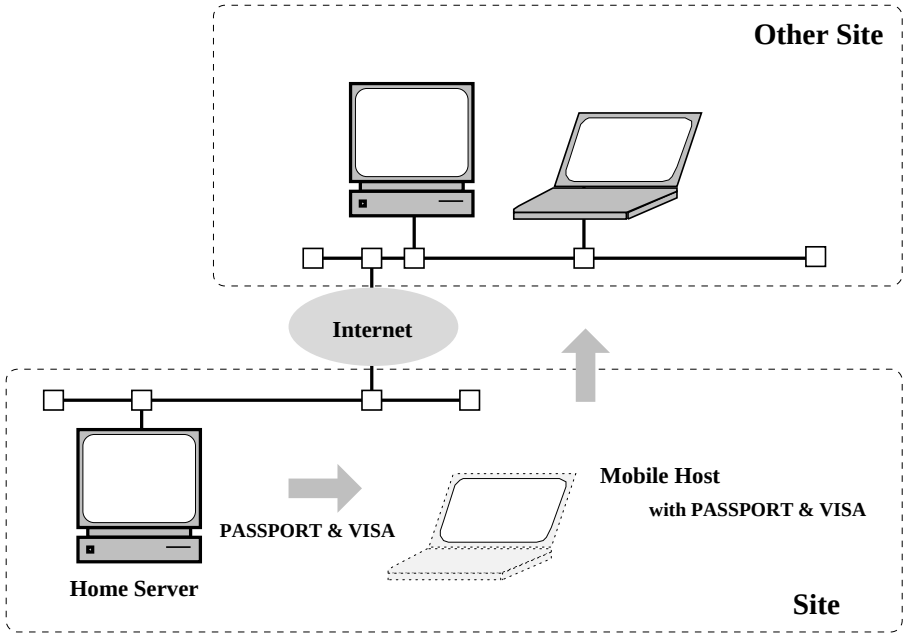


図 3.1 パスポートモデル

PASSPORT には，移動ホストを認証するために必要な情報を記述する．また，実社会のパスポートでは身分照合にサインを用いているが，提案するモデルではディジタル署名をホストの身分照合に用いる．表 3.1に，実社会のパスポートとこのモデルとの対応を示す．

移動ホストの接続予定先のサイトによっては，事前に接続認可を取るなどサイト固有の認証条件を付加する必要があるかもしれない．そのためにパスポートモデルでは，このような条件を規定するために $VISA$ の概念を導入する．

PASSPORT や VISA に実際に記載される暗号鍵や認証情報については，ここでは特に規定しない．移動ホストの認証に必要な情報が与えられ，何らかのメカニズムで認証処理を行うことができれば十分である．

表 3.1 パスポートと PASSPORT の比較

	パスポート	PASSPORT
通用範囲	国交のある国	交流のあるサイト
発行者	国 (外務省)	サイト (ホームサーバ)
照会方法	サイン	ディジタル署名

ディジタル署名

パスポートモデルでは，ディジタル署名による認証を想定している．ディジタル署名に利用可能な暗号系には，DES などの慣用暗号系と RSA などの公開鍵暗号系がある．慣用暗号系を用いる場合には送信者と受信者の間で鍵を共有しなければならない．このため送受信者の組合せの数だけ鍵を用意しなければならずインターネット環境ではあまり現実的ではない．また署名法には，受信者が受信したメッセージの正当性を直接確認する直接署名法と，信頼できる第三者を調停者としてメッセージの正当性を確認する調停署名法がある．

確実なディジタル署名を実現するには，第三者による調停署名法を用いるべきである．しかし，現在のインターネット環境では調停者である第三者の正しさを認証することは，まだ技術的に困難であることが予想される．そこで本論文での実装では，公開鍵暗号による直接署名方式 (表 3.2参照) を用いることにする．

この方法では，ディジタル署名の安全性を保障するすべての条件を満足することはできないが，移動ホストからのメッセージの認証確認と送信メッセージの偽造を防ぐことは可能である．

3.1.4 DHCPA の提案

パスポートモデルを資源割り当てプロトコルである DHCP に適用した実装例として，DHCPA(DHCP with Authentication) を提案する．ただしディジタル署名で利用する暗号系で必要な暗号鍵の配送については本論文では厳密には議論しない．最も単純な鍵の配送方法は鍵交換を直接人が行う “手動法” と呼ばれる手法であるが，スケーラビリティの問題が存在する．公開鍵暗号法を用いた場合に

表 3.2 公開鍵暗号による直接署名法

Step 1 :	$Cypher$	$\leftarrow$	$E\{D\{Message\}^{K_S}\}^{K_{R^{-1}}}$
Step 2 :	*send Cypher to R*		
Step 3 :	$Message$	$\leftarrow$	$E\{D\{Cypher\}^{K_R}\}^{K_{S^{-1}}}$

K_S : Sender Secret Key
$K_{S^{-1}}$: Sender Public Key
K_R : Receiver Secret Key
$K_{R^{-1}}$: Receiver Public Key

は，信用できる第三者から公開鍵証明書を入手し公開鍵を獲得する手法が実用化 [32][33] されている．これらの手法を用いて安全な鍵交換が実現されていることを前提として DHCPA を提案する．

DHCPA の構成要素

DHCPA は認証処理を行い資源を割り当てるサーバ (DHCPA Server) と，資源割り当て要求を出すクライアント (DHCPA Client)，PASSPORT を発行するホームサーバ (DHCPA Home Server) から構成される (図 3.2参照).

DHCPA サーバは，移動ホストである DHCPA クライアントからの割り当て要求に含まれている PASSPORT を用いてホスト認証を行い，資源の割り当てを実行する．また，付加されている認証機構以外は，通常の DHCP と同様に動作する．

DHCPA の PASSPORT

DHCPA の PASSPORT に含まれる情報を次に示す。

- ホームサーバの IP アドレス
- クライアントの MID(Mobile ID)
- ディジタル署名されたクライアントの認証情報

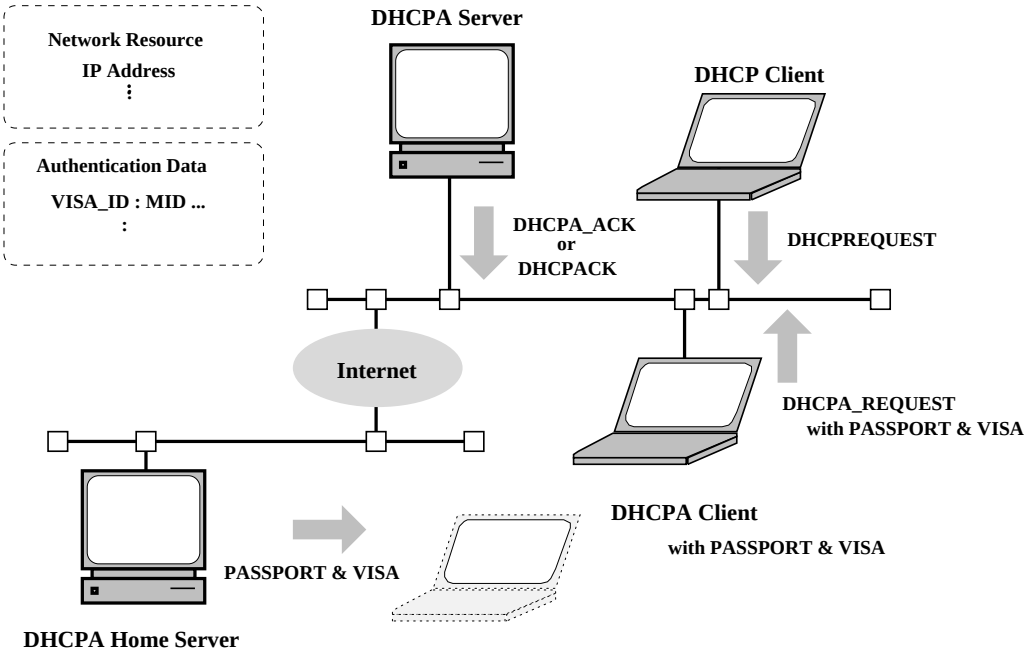

Network Resource
IP Address
Authentication Data
VISA_ID : MID ...
DHCPA Server
DHCP Client
DHCPA_ACK
or
DHCPACK
DHCPREQUEST
Internet
DHCPA_REQUEST
with PASSPORT & VISA
DHCPA Client
with PASSPORT & VISA
PASSPORT & VISA
DHCPA Home Server

図 3.2 DHCPA

- ホームサーバの秘密鍵で暗号化されたクライアントの公開鍵
- クライアントの秘密鍵で暗号化された VISA とタイムスタンプ

ホームサーバは，クライアント (移動ホスト) 毎に固有の PASSPORT を発行する．また，ディジタル署名には公開鍵暗号法である RSA[20] と MD5[24] を用いているが，これ以外の署名法にも対応できるように考慮している．

3.1.5 DHCPA の設計と実装

DHCPA プロトコル

DHCPA サーバと DHCPA クライアント間での認証処理に必要な情報を，DHCPA では DHCP プロトコルのオプションである Class-identifier オプションに記述している．DHCP の Class-identifier オプションを用いれば，サーバ側で異なる処理を行わせることが可能となる．このオプションを利用することで，既存の DHCP との互換性を確保しつつ，新たな機能を追加することが可能となる．

DHCP Class-identifier オプションに記述する，DHCPA の Header Format を図 3.3に示す.

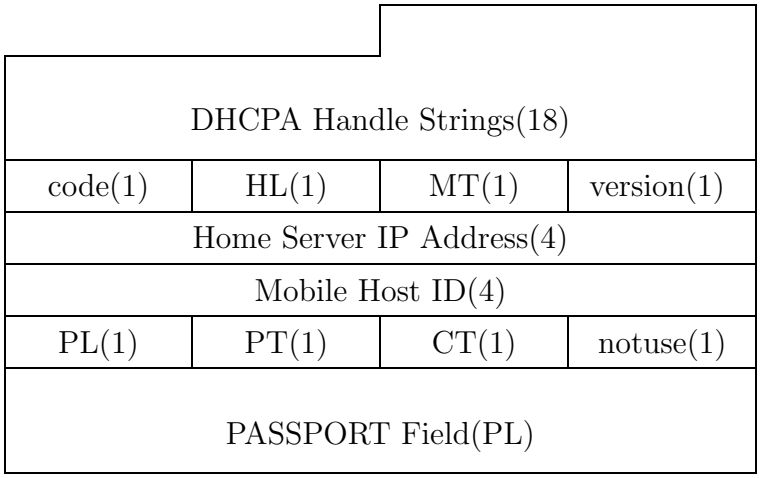
DHCPA PASSPORT Field

DHCPA の PSAAPORT Field は，DHCPA で用いる認証情報などを格納する領域である．この領域の長さは，DHCP プロトコルで規定されている DHCP オプションの長さの制約から，220 バイトに制限されている．

図 3.4は，DHCPA Header に含まれる PASSPORT Field を示している．ここには，DHCPA ホームサーバの秘密鍵 K_H で暗号化された DHCPA クライアントの公開鍵 $K_{M^{-1}}$ と，VISA の要求時のタイムスタンプを DHCPA クライアントの秘密鍵 K_M で暗号化した認証情報が含まれている．

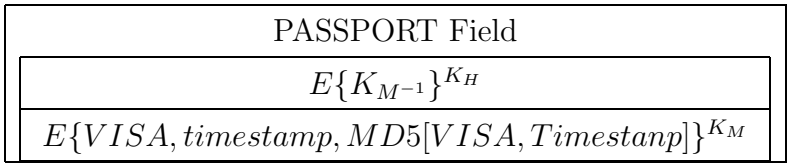
DHCPA パケットの送信

DHCPA では，認証情報を含んだパケットを DHCP Class-identifier オプションとして送信することで，既存の DHCP との完全な互換性を維持しながら認証機



code : DHCPoption Code field(future)
HL : DHCPA Header Length
MT : DHCPA Message Type
version : DHCPA Version
PL : Passport Field Length
PT : Passport Field Type
CT : Crypt Type

図 3.3 DHCPA Header Format



K_H : Home Server Secret Key
K_M : Mobile Host Secret Key
$K_{M^{-1}}$: Mobile Host Public Key

図 3.4 DHCPA PASSPORT Field

表 3.3 DHCPA Message Type

0x00	: DHCPA_QUERY message
0x01	: DHCPA_OFFER message
0x02	: DHCPA_REQUEST message
0x03	: DHCPA_ACK message
0x04	: DHCPA_NAK message
0x05	: DHCPA_RELEASE message
0x06-ff	: future use

構を実現している．DHCP の各処理のフェーズで，Class-identifier オプションを利用した DHCPA パケットの送受信を行い，認証情報の交換を実現している．

DHCPA Message Type フィールドは，DHCP サーバ/クライアント間で送受信される DHCPA パケットを識別するために利用する．DHCPA プロトコルで用いる DHCPA Message を表 3.3に示す．

次に，DHCPA クライアントの認証処理の流れを図 3.5に示す．

1. DHCPA クライアントは，接続要求を受け付けてくれるサーバを特定するため，DHCPDISCOVER とともに DHCPA_QUERY を送信 (Broadcast) する．

2. DHCPA サーバは，要求のあったクライアントに対して DHCPOFFER とともに DHCPA_OFFER を送信する．

3. クライアントは，受け取った DHCPOFFER と DHCPA_OFFER からサーバを選択し，DHCPREQUEST と DHCPA_REQUEST を送信 (Broadcast) する．

4. DHCPA サーバは，資源の割り当てが可能なら DHCPACK を DHCPA_ACK とともに送信する．もし要求された資源の割り当てが不可能なら，DHCP-NAK を DHCPA_NAK とともにクライアントに送信する．

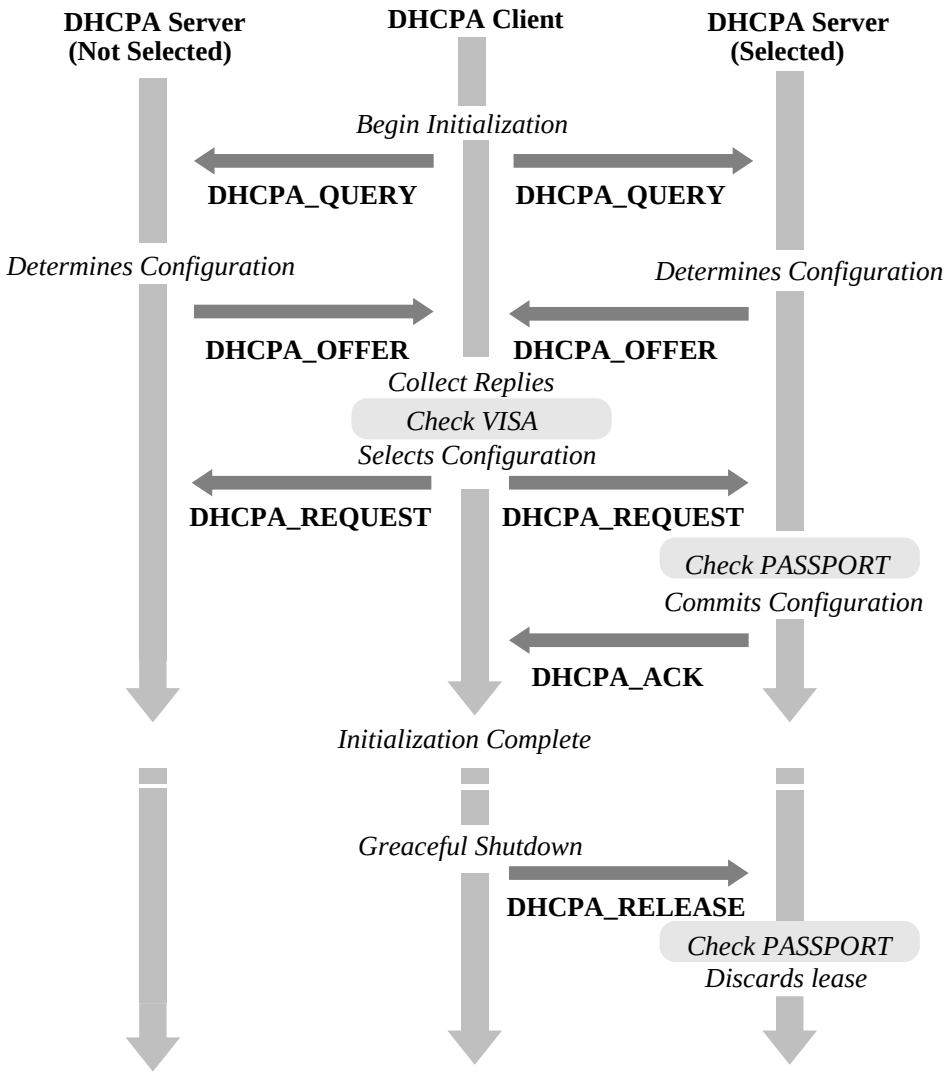


図 3.5 DHCPA プロトコルの処理の流れ

3.1.6 DHCPA の評価

DHCP との互換性

本論文で提案した DHCPA は，移動ホストからの割り当て要求に応じて，まず移動ホスト認証を行った後に，要求されたネットワーク資源を割り当てる安全なメカニズムを実現している．この DHCPA は，サーバ/クライアントとも，既存の DHCP のサーバ/クライアントと完全な互換性があり，従来の DHCP 環境でもそのまま利用することができる．そのため，従来の DHCP 環境から，安全な DHCPA への移行も比較的スムーズに行うことが可能である．

DHCPA の安全性

DHCPA の認証の強度は，ディジタル署名で用いた RSA 暗号の強度に依存している．また，DHCP プロトコルにおける DHCP オプションの長さの制限から，認証で用いている暗号鍵の長さが制限されているため，より安全な認証強度を求める事はかなり困難である．現在の実装は，DHCP との互換性を一番に考慮し，その範囲で実現可能な安全性を確保している．

認証の単位

本論文の DHCPA の実装では，移動ホストを認証の単位として用いた．この場合，ホスト自身の盗難や PASSPORT の不正なコピーなど，いくつかの問題に対応することができない．しかしながら，利用者を認証の単位として考えた場合，パスワードの入力などで，どうしても自動化できない部分が生じてしまう．無線ネットワーク環境などでの利用を考えると，無線のエリア切替え時の資源割り当て要求のニーズなどもあり，完全に自動化できる認証機構としての実現を重要視している．そのため，本論文で紹介した DHCPA では，ホストを認証の単位として実装を行っている．

利用開始時にパスワードを入力し，ユーザ認証と組み合わせてホスト認証を行うなど，この点は再度検討できる部分であると考えている．

3.1.7 モバイルセキュリティについてのまとめ

これまでに述べたように，移動ホストは移動した先のネットワークに接続するためにIPアドレスなどのネットワーク資源を必要としている．しかしながら，有力な選択肢のひとつであるDHCPでは，移動ホストの認証をまったく考慮しておらず，移動ホストからの割り当て要求に従って，そのままIPアドレスなどの資源の割り当てを行っている．

こうした現状を踏まえ，本論文では移動ホスト環境におけるホスト識別のための汎用的な認証モデルとして，パスポートモデルを提案した．パスポートモデルは，移動ホスト毎に身元を保証するために，個々のホストに個別のPASSPORTを所有させ，これによりホストの認証を行う認証モデルである．さらに，パスポートモデルをDHCPに適用し，DHCPを拡張したDHCPAプロトコルの設計と実装を行うことにより，移動ホストの認証を考慮した資源割り当て機構の有効性を示した．

3.2. モバイル認証ゲートウェイ

マイクロソフトWindows95にも標準で採用されたDHCPは，数多くのネットワークサイトで利用されている．しかし，現在普及しているDHCPは，セキュリティについてまったく考慮されておらず，ネットワークに接続しようとするすべてのユーザからの要求を同じ様に処理し，接続に必要なIPアドレスなどのネットワーク情報の割り当てを行ってしまう．つまり，誰にでもネットワークへのアクセスを許してしまうセキュリティ上の重大な欠点がある．

インターネットの普及とともに，ネットワーク環境におけるセキュリティの必要性も同時に認識され，Firewallを構築し内部ネットワークに対するアクセス制御を行なうサイトが急速に増加している．こうした背景からIETF(Internet Enginiaring Task Force)でもDHCPにおけるセキュリティの重要性が議論され，IETF Draft[34]をはじめとする幾つかの方向性が示されつつある．

しかし，IETF Draftや関連する提案で述べられている方法では，DHCPサービスを提供しているネットワークを物理的に盗み見て接続に必要な情報を入手し，不正にアクセスしようとするユーザや，過去に入手した情報をもとにアクセスし

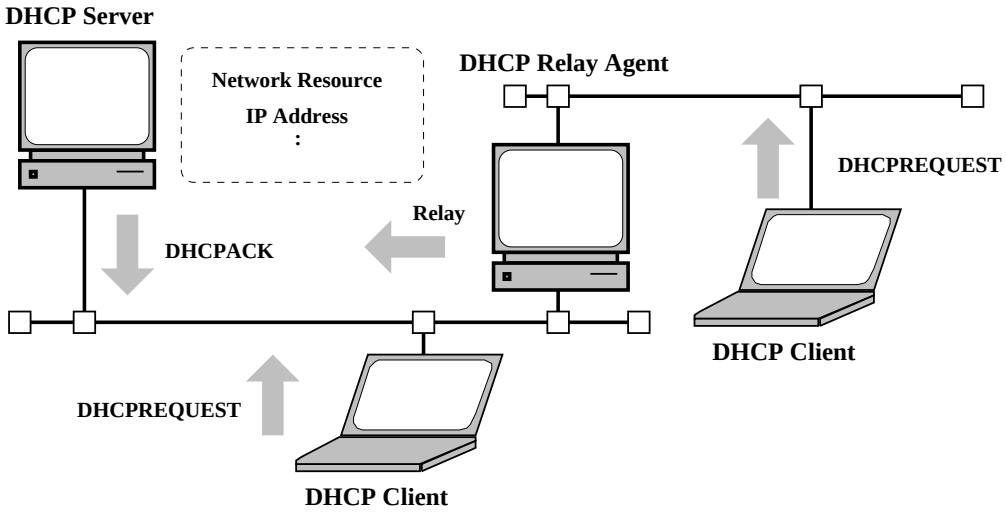


図 3.6 DHCP

ようとする不当なクライアントに対して有効な，具体的な対処法がまったく述べられていなかった．実際に DHCP を利用するネットワークを構築する場合には，こうした不正アクセスの排除は，セキュリティ上明らかに必要な機能である．

そこで，不正なアクセスを行おうとするクライアントからの通信を排除し，接続のための資源を DHCP サーバによって正当に割り当てられたクライアントのみが通信できるメカニズムを，ゲートウェイに組み込んで実現する手法について述べる．

3.2.1 DHCP におけるセキュリティ

資源の割り当てメカニズム

本論文で着目している DHCP は，ユーザの介在無しで自動的に資源の割り当てができ，かつ割り当てた資源の回収が可能なプロトコルである．DHCP はネットワーク資源の割り当てを行う DHCP サーバと，資源に割り当てを要求するクライアント，要求を中継するリレーエージェントから構成される (図 3.6参照)．

IP アドレスなどのネットワーク資源を割り当てられたクライアントは，DHCP サービスを提供しているネットワークから，構内ネットワークやインターネットに対して通信を実施することになる．

DHCP メッセージの認証

先に述べたように，BOOTP プロトコルや DHCP プロトコルでは，資源の割り当てに際して，割り当てるホストの認証をまったく考慮していない．これらのサーバは，どのようなクライアントからの割り当て要求に対しても，要求に応じて資源を割り当ててしまうため，セキュリティの観点から特に問題視されている．逆に，割り当てられたアドレスが正当な DHCP サーバから割り当てられたものなのか，という問題もあるため，状況によってはクライアントによるサーバの認証も考慮する必要がある．

DHCP のメカニズムにおいてセキュリティ上重要なポイントは，DHCP サーバと DHCP クライアントの間の DHCP メッセージの交換の安全性にある．この安全性を確保する手法として，サーバ・クライアント間の一連の処理において交換する DHCP メッセージにディジタル署名を付加することが考えられる．これを用いれば DHCP サーバと DHCP クライアントとの間で認証処理を行ない，正当なクライアントにのみネットワーク資源の割り当てを行なうことが可能である．これらの認証情報は，DHCP 認証に関連する分野では Message Authentication Code(MAC) [35] と呼ばれている．

IETF Draft における認証

IETF で議論されている DHCP メッセージの認証方式は，サーバとクライアントで暗号鍵を共有し，この鍵を利用して生成される MAC により認証処理を行うものである．

実際に伝送される DHCP メッセージには，次の情報が含まれる．

DHCP Message, counter,
$f(K$, MD5(message + counter))

DHCP Message は，DHCP サーバとクライアントの間で交わされるネットワーク

資源を割り当てる通常の DHCP 処理のために送られるメッセージである．counter はリプレイアタック (繰り返し攻撃) を防止するための情報で，通常は時間などを含んだ値を設定する．これらの情報に加えて，共有している鍵 K、DHCP Message と counter から生成されるメッセージダイジェスト (MD5)[24] を，一方向関数 f で変換した値がディジタル署名として付加される．

あらかじめ，DHCP サーバとこれを利用するクライアントの間で，秘密鍵 K を共有しておくことにより，サーバとクライアントの双方で，送られてきた DHCP メッセージをもとに，正当なサーバ／クライアントであることを認証することができる．また，共有する秘密鍵 K の生成において，DHCP におけるクライアント ID などの固有の情報を用いれば，送られてきたメッセージからクライアントを完全に特定することも可能である．

DHCP における認証については，IETF で議論されている最中であり，Internet Draft として “Authentication for DHCP Message” が公開されている．

3.2.2 アクセス制御機構の設計

本論文で提案するアクセス制御機構は，DHCP サーバがネットワーク接続のための情報をクライアントに割り当てる DHCP サービスセグメントと，正規に IP アドレスなどを割り当てられたクライアントからのアクセスのみを許可する内部ネットワークとの間に，不正アクセスを監視するゲートウェイを用意する．そして，このゲートウェイによって不正なクライアントに対するアクセス制御を実現する．DHCP ネットワーク用のアクセス制御ゲートウェイであるので，DAG(DHCP Access control Gateway) と呼んでいる．

基本的なアイデア

DHCP メカニズムの認証処理の流れを，図 3.7に示す．DHCP クライアントは，まず DHCP サーバを探すため DHCPDISCOVER メッセージを送信する．これを受けた DHCP サーバは，アドレスの割当が可能なら DHCPOFFER メッセージをクライアントに対して送信する．クライアントはアドレスを要求するサーバを決め，DHCPREQUEST メッセージをサーバに対して送信する．これを受けとった DHCP サーバは，割り当てる情報を DHCPACK メッセージとともにクライア

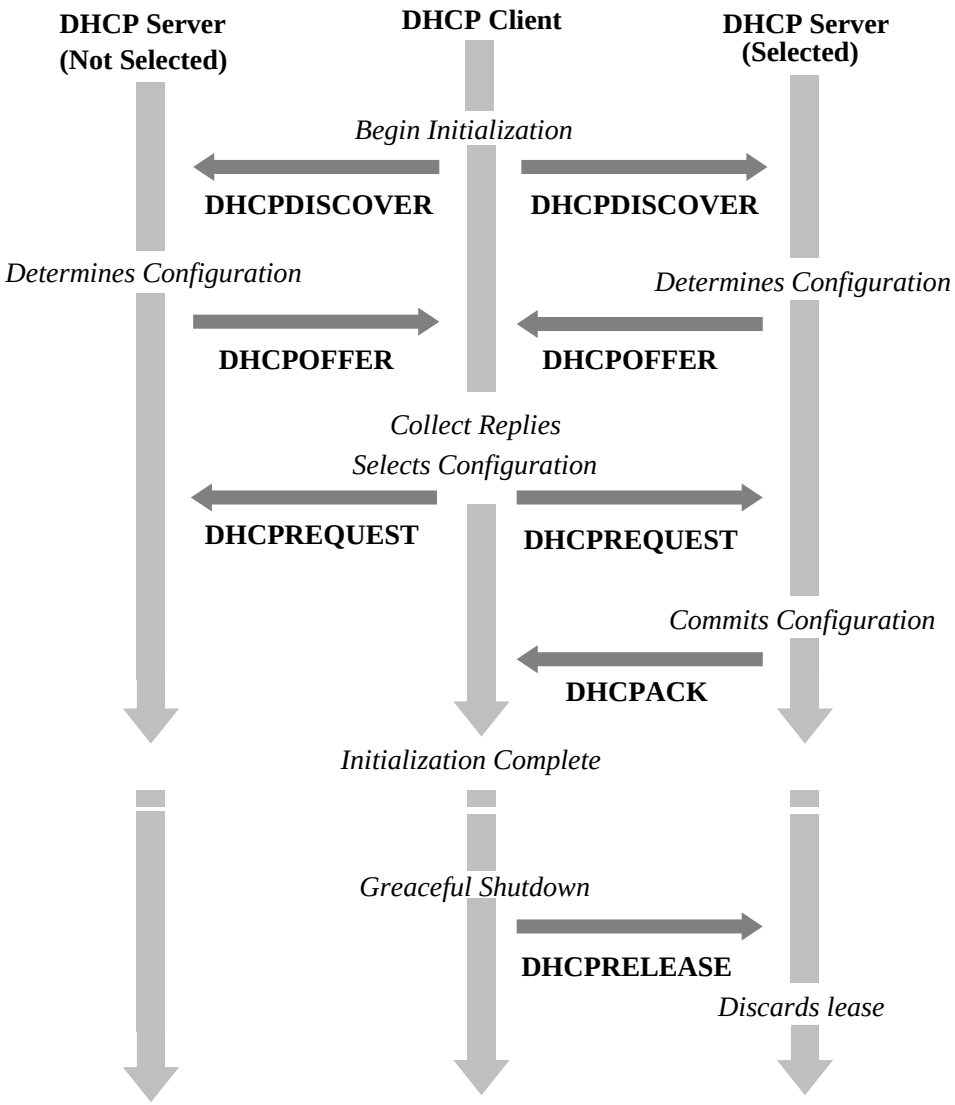


図 3.7 DHCP プロトコルの処理の流れ

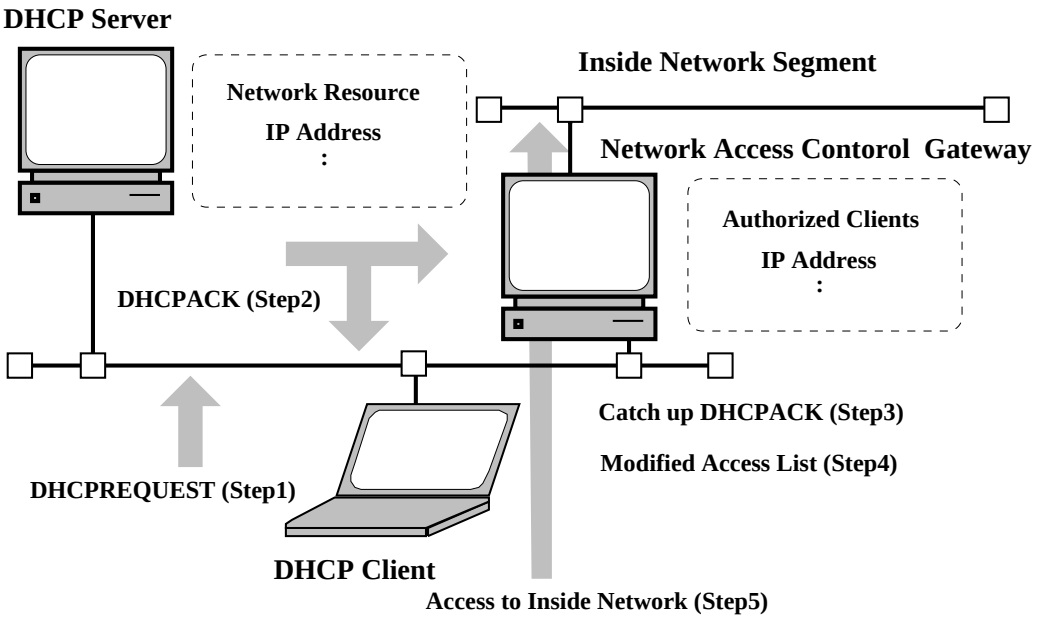


図 3.8 アクセス制御ゲートウェイのしくみ

ントに送信し，クライアントは受けとった情報に従ってネットワークなどの設定を行なうことになる．

一連の DHCP サーバとクライアントの間で交換される DHCP メッセージの中で，具体的に割り当てられた情報が交換されるのは，DHCPACK メッセージである．しかもこの情報はブロードキャストされるため，同一ネットワーク上に存在するゲートウェイでも当然ながら受信することができる．そこで，DHCP サーバがサービスを提供するセグメントと，アクセスの許可を必要とする内部のネットワークとの間にアクセス制御ゲートウェイを用意して，DHCP サーバから DHCP クライアントへの DHCPACK メッセージをゲートウェイでも受信する．そして受信したメッセージに含まれるアドレスに対して必要ならば認証処理を行い，アクセスを許可してパケットの中継処理を実行する．つまり，アクセス制御ゲートウェイでは，正当に DHCP サーバによって割り当てられたクライアントの情報を，実際の DHCP サーバの資源割り当てパケットから得てアクセス制御を実行することになる (図 3.8参照).

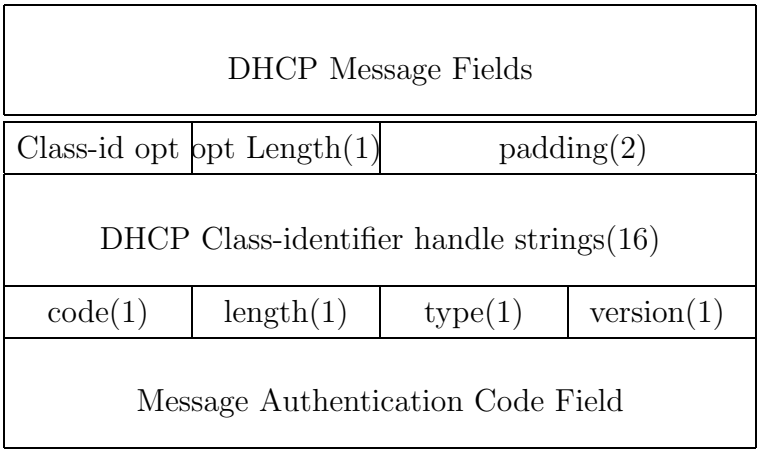


図 3.9 DHCP MAC Header Format

このシステムでは，アドレス割り当て時に，DHCP サーバからアクセス制御ゲートウェイに対して割り当てた旨の情報を伝送しなくても，通常の割り当て処理を監視することで正確な割り当て情報を得ることが可能である．

DHCP メッセージの認証

IETF Draft の”Authentication for DHCP Message” では，資源の割り当て処理に必要な情報に加えて，MAC(Message Authentication Code) と呼ばれるディジタル署名を一連の割り当て処理で伝送する DHCP メッセージに付加している．実際の実装方法については，Internet Draft では述べられていないが，DHCP プロトコルのオプションに記述することで伝送することが可能である．ここで述べる実装では，DHCP オプションのひとつである Class-identifier オプションに MAC を記述することにより，サーバとクライアントの間で認証処理を行なっている．DHCP プロトコルでは，このオプションを用いてサーバ固有の処理を行わせることが許されている．本来ならば MAC を記述するためのオプションが規定されるべきであるが，実装時の DHCP オプションではまだ規定されていない．そのため本研究における実装では，正規の DHCP オプションとして定義されても最小限の変更で対応できるよう，これまでに規定されている DHCP オプションの記述と互換性のあるフォーマットを採用した．DHCP Class-identifier オプションに記述した MAC の Format を図 3.9に示す．

3.2.3 アクセス制御ゲートウェイ (DAG) の実装

アクセス制御ゲートウェイにおいて DHCP サーバの認証を厳密に行うならば，DHCP メッセージの認証機構を必要とする．しかし，厳密に認証する必要が無い場合でも，そのまま適用できるアーキテクチャを選択しアクセス制御ゲートウェイの実装を行った．すなわちアクセス制御機構を実現するうえで変更が必要な部分は，大部分がアクセス制御ゲートウェイに関するものであり，既存の DHCP サーバの変更を行なわなくてもすむよう配慮して設計されている．

提案するアクセス制御ゲートウェイは４つの部分から構成される．

1. DHCP パケットの監視
2. アクセスコントロールデータベースの管理
3. アクセス制御
4. パケットの中継処理

DHCP パケットの監視には，bpf(Berkelay Packet Filter) などの低レベルインターフェースから直接データを入手するメカニズムが必要である．これを提供できるオペレーティングシステムとして，BSD 系の PC-UNIX を開発環境として選択した．また，アクセス制御と中継処理の主要な部分については，フィルタリング機能を持つ既存のソフトウェアである ip_fil3.1.0 を利用した．

実装を行った dhc_fild プログラムは，DHCP メッセージを監視し DHCP サーバからクライアントへ送られる DHCPACK メッセージから，割り当てられたアドレスを抽出し，これを ip_fil に登録する処理を行うプログラムである．同様に DHCP クライアントからサーバに DHCPRELEASE メッセージが送られた時に，返却されるアドレスを ip_fil から削除する処理も行っている．

DHCP サーバでの DHCP メッセージの認証が行われている場合には，DHCP サーバと dhc_fild プログラムで秘密鍵を共有することにより認証処理を行うことができる．また，認証処理の有無を dhc_fild.conf ファイルに定義しておくことにより，認証を行わない通常の DHCP サーバに対する処理方法も選択できるよう実装上の配慮を行った．認証処理において，DHCP サーバのメッセージ認証で必要な一方向関数 f には MD5 を使用した．

3.2.4 アクセス制御ゲートウェイ (DAG) の評価

実装したシステムは，BSDI 社の PC-UNIX である BSD/OS(v2.1/v3.0) で動作する．移動ホストからの割り当て要求に応じて，DHCP サーバにより正当な割り当てを行ったクライアントのみアクセスを許可するアクセス制御ゲートウェイを実現できた．また，本稿で提案したメカニズムでは，これまでに利用されてきた DHCP サーバ，クライアントとの互換性を重視しており，従来の DHCP 環境でもそのまま利用することが可能である．

安全性

提案したシステムでは，DHCP メッセージにディジタル署名を含むため，DHCP オプションフィールドの大きさの制限から利用できる暗号化方式や鍵の長さに制限がある．IETF で提案されている方式は，秘密鍵をサーバとクライアントで共有する方式で，その認証メカニズムはオプションフィールドの利用を考慮したものである．

秘密鍵を共有する場合の問題点として，クライアント側での鍵の漏洩がすでに指摘されている．そのため，ユーザ自身にも解読できない鍵生成関数を用意して，これにより鍵の自動生成を行う方式の是非についても，IETF では議論されている [34].

本研究で実現したアクセス制御機構の安全性は，DHCP のメッセージ認証の強度に依存する．DHCP サーバからのメッセージを偽造することが出来なければ，それと等価に安全であると言える．アクセス制御ゲートウェイで DHCP サーバからのメッセージ認証を行うため，DHCP サーバとクライアントに加えてアクセス制御ゲートウェイでも秘密鍵を共有する必要がある．この部分での安全性の低下が考えられるが，ゲートウェイ自身の安全性に依存するので考慮の対象外とした．

性能

DHCP メッセージの認証処理によるフィルタの設定に必要な時間は，DHCP サーバからクライアントへの送信データをそのまま利用しているため無視できる範囲であると考えられる．

実際にアクセス制御ゲートウェイを経由して内部ネットワークと通信する場合のゲートウェイ処理のオーバヘッドについては，本稿で示している実装では IP フィルタ機能をフリーソフトウェアである ip_fil3.1.0 を利用して実現しているため，ip_fil とその実装ハードウェアの処理能力に依存する．

問題点

本稿で提案しているメカニズムでは，アクセス制御ゲートウェイが起動した時点で，すでに DHCP サーバによってネットワーク接続のための資源が割り当てられているクライアントを認識することが出来ない．しかしながら，内部ネットワークとの接続がアクセス制御ゲートウェイを経由してしか出来ないネットワーク環境での利用を想定しているため，それ以前の割り当てを考慮せず起動後の割り当て処理のみで十分であると考えている．また，この問題はクライアントから割り当て情報の更新要求を，再度 DHCP サーバに出すことにより，正常な認証処理を行わせることができるので，運用で対応することが出来る問題でもある．

3.2.5 モバイル認証ゲートウェイのまとめ

DHCP を用いたモバイルネットワークにおいて，移動ホストの認証を前提としたアクセス制御機構を提案し，実際に稼動するシステムである DAG を設計し実装した．DAG を利用することで，不特定多数が利用する可能性がある会議室などのネットワークにおいても，DHCP サービスを提供し，管理者が意図したセキュリティを設定することが可能となる．

現在の DAG の実装では，割り当てられたまま返却されないアドレスについての対応が不十分である．DHCPACK メッセージにはアドレスの有効期限も含まれている．こうした情報を有効に利用して有効期限の切れたアドレスについては中継処理を行わないようにする必要がある．また，サーバ側で指定した最大有効期限を越えているアドレスについても，同様な処理を行う必要がある．

さらに，IETF で議論されている DHCP メッセージの認証機構以外の認証機構への対応とアドレス以外のリソースに対するアクセス制御について考える必要がある．具体的には，筆者が移動ホストの認証モデルとして提案しているパスポートモデルへの拡張などが考えられる．

また最近は，筆者がモバイルセキュリティに関心を持って研究を始めた時期とは異なり，インターネットに接続されるすべてのホストについてのセキュリティを議論する必要が生じている．インターネットプロトコルのためのセキュリティアーキテクチャ(The Security Architecture for the Internet Protocol)[36] や IP ヘッダとそのペイロードに対して認証機構を提供する IP 認証ヘッダ (IP Authentication Header)[37][38] などが提供され，セキュリティに対する関心がこれまで以上に高まってきている．ユーザのセキュリティに対するニーズも多岐にわたり，単一のアーキテクチャですべてを提供できる環境では無くなりつつある．ファイヤーウォールとの連携や複数の認証機構を併用するメカニズムの提供など，今後のモバイルセキュリティを取り巻く環境に必要とされるネットワーク構築技術に対する課題は，より複雑化してきている．今後も新たな利用形態を考案し，より利便性を持つモバイル環境の実現に貢献したい．

第 4 章

地域ネットワークに関する高機能化

この章では，従来のインターネット構築技術に加え，本研究により付加した地域ネットワークの高機能化に関する技術について述べる．まず，地域 IX(Internet eXchange) を実現する場合の経路制御問題を解決するアプローチとして，送信者の持つソースアドレスを利用した新たな経路制御手法を提案する．次に，実用的な地域インターネットの構築を目指して実施した地域ネットワーク構築モデルの確立に関する研究について論じ，その成果を適用した，岡山情報ハイウェイ構想と OKIX(Okayama Internet exchange) について述べる．

4.1. ソースアドレスルーティング

インターネットにおける通信は，データの宛て先として指定されたディスティネーション IP アドレスによって，データを中継するべきネットワークが選択される．この経路選択のメカニズムに，送信者アドレスであるソース IP アドレスを活用することで，これまで以上に柔軟な経路制御を行うことが可能となる．この手法を経路制御問題を抱えている地域ネットワーク構築に適用することで，地域 IX の構築の課題のひとつを解決することができる．

4.1.1 地方自治体による地域 IX の構築

各地の地方自治体では，地域の活性化を目指した情報化を推進する動きが活発化している．特にインターネットの利用環境の整備を事業の中心とした，地域ネットワークの構築が数多く計画され，その実現に向けた活動が急速に広まってきて

いる．自治体主導の地域ネットワークの構築の多くは，インターネット接続事業者 (ISP: Internet Service Provider) と連携をはかり，その地域の通信を円滑に行うための地域 IX を併設する場合が多い．これは，その地域のユーザトラヒックを国際的なインターネットへと中継する手段を確保すると同時に，ISP が持つ高度なインターネット技術をその地域のために利用しようとするからである．しかし，地域 IX において複数の ISP の接続を誘致し，さらに ISP 間の相互接続を実現するには，解決すべき数多くの課題が存在する．そのため，構築された地域ネットワークが思ったほど効果を発揮していない事例が数多く見受けられる．そこで，地域ネットワークに地域 IX を併設する場合の諸条件についてまとめ，解決すべき問題をまず明らかにする．そしてその課題のひとつである地域 IX における経路制御問題を解決を目指し，筆者らが提案したソース IP アドレスを用いた経路制御システムについて述べる．

4.1.2 地域 IX とルーティング問題

インターネットは，数多くのネットワークが相互に接続されることで，巨大なネットワークを構成している．これらのネットワークは，個々が自律系 (AS:Autonomous System) として機能し，自らのネットワークに接続されているネットワークについての経路情報を集約し，各 AS 間で相互に交換することで到達性を確保している．インターネット接続事業者は，それぞれひとつ以上の AS を構成し，他の接続事業者との間での接続性を確保するために，他事業者 AS との間で経路情報の交換 (peer) を行っている．

また，AS 間の接続情報を相互に交換するための交換場所として，インターネットエクスチェンジ (IX:Internet eXchange，以下 IX と略す) とよばれる相互接続ポイントが形成されている．日本で運用中の IX は，WIDE プロジェクト [29] が運営している実験 IX である NSPIXP-2(東京大手町)/NSPIXP-3(大阪)[30]，商用の IX として有料接続を行っている JPIX や MEX などがある．

これらの IX は，インターネットにおける通信の到達性を確保するために構築されており，IX に接続するインターネット接続事業者は，自身の AS に所属するすべてのネットワークについての経路情報を，他の接続事業者との間で相互に交換している．IX での経路交換などにより得られるインターネットに接続している

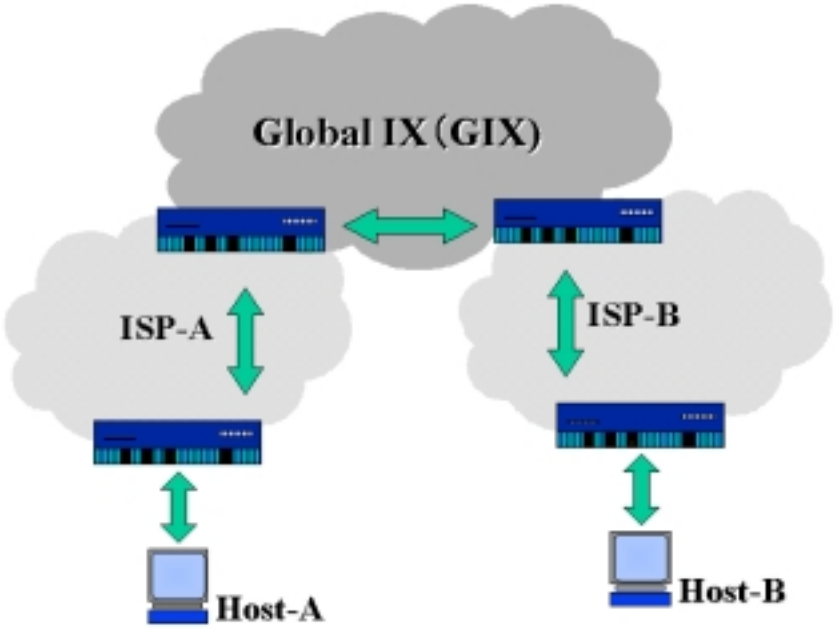


図 4.1 Global な IX を経由する経路

すべてのネットワークに関する経路情報のことを “Full Route” と呼んでいる．こうした Full Route の交換が可能な IX を特にグローバル IX(GIX: Global Internet eXchange) と呼んでいる．前述の，NSPIXP-2/NSPIXP-3 や JPIX，MEX は，いずれも GIX である．

GIX は経済的な側面による影響で，東京や大阪などの大都市に集中して構築されている．すなわち，現在のインターネットの設計は大都市を中心とした設計となっており，情報コンテンツの集中や地方都市間の通信における不必要な遅延の発生など，いくつかの問題を引き起こしている [39]．また，同じ地方都市にあるホスト間の通信でも，契約しているインターネット接続事業者 (ISP: Internet Service Provider) がそれぞれ異なると，両者間の通信は GIX を経由することになる (図 4.1 参照).

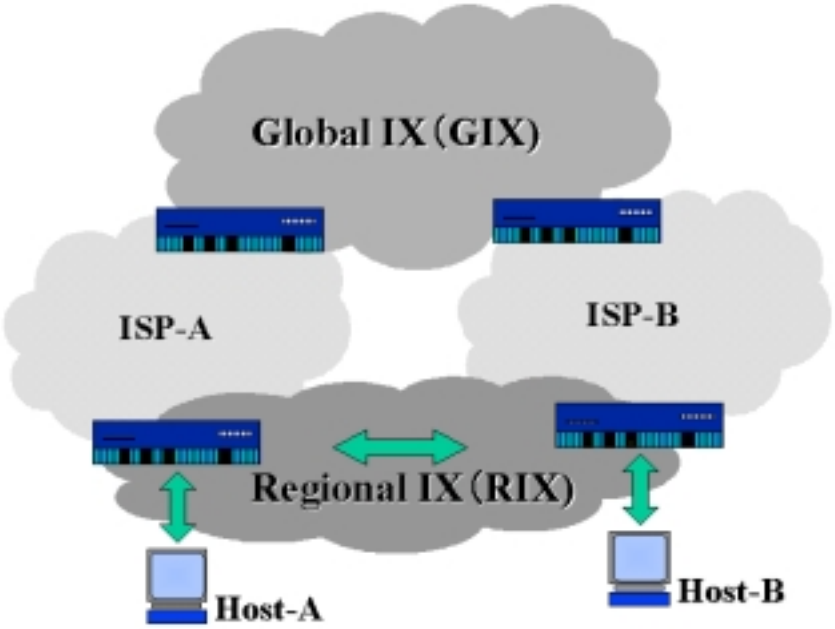


図 4.2 地域 IX で折り返す経路

これにより，不必要な通信遅延が発生したり，GIX までの経路上の他地域の災害の影響を受けたり，地域内の通信経路を地域側で制御できない，などの問題を抱える原因となっている [39]. また，地方自治体がいかに高速な地域ネットワークを構築したとしても，GIX を経由してしまう冗長経路問題が解決できなければ，その高速性を発揮することは難しい.

そこで，すべてのネットワークについての経路情報の交換を目的とせず，地域内のネットワークに関する経路情報のみの交換を目的とした IX が誕生した. このような IX は，一般に地域 IX(RIX: Regional Internet eXchange) と呼ばれ，GIX とは位置付けのことなる IX として定着しつつある．地方都市において地域 IX を作り，そこで ISP を相互に接続すれば，その地域の域内通信を地域内で折り返すことが可能となる (図 4.2 参照). これにより先に述べた GIX を経由する

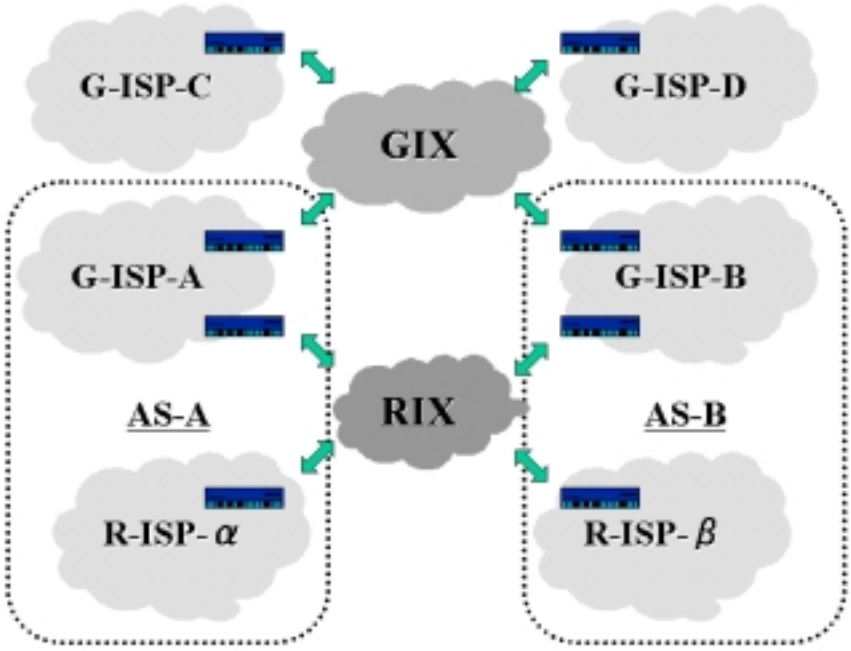


図 4.3 地域 IX の形態

冗長な経路問題を解決することができるため，高速な地域ネットワークの構築と合わせて地域 IX を構築する動きが活発化している．

これらの問題はどの地方都市においてもほぼ共通しており，地域内通信の効率化と安定化，地域に関する情報の地域からの発信，他の地域の障害に強いネットワーク構築，地域情報コミュニティの形成，通信路の決定権の取得などの目的を達成するために地域 IX の構築についての検討が行われてきた．これまでに，岡山県 [40][41]，山梨県，富山県，東海地域，東北地域などで，地域 IX 構築に関する実験が実施されている．

相互接続実験を行なっている地域 IX には，様々な形態が存在する [39]．そのひとつとして，地域 IX 自体が外部との接続性を持ち，ISP の様な役割を果たす形態がある (図 4.3参照)．この形態では，その地域のみにサービスを提供してい

る地域 ISP(R-ISP:Regional ISP) は，それぞれ大手 ISP(G-ISP:Global ISP) と接続契約を行い，インターネットとの接続性を確保する．地域 ISP は大手 ISP との接続を，RIX を経由して実現する．この場合，地域 ISP の経路は，大手 ISP の AS に含まれることになる．この形態の利点は，地域 ISP 間 (R-ISP-α,R-ISP-β) の通信を，RIX を経由する最短な経路で行うことができることである．地域内の経路情報を RIX 内部で完結させることができるので，大手プロバイダ間の経路交換を RIX で行う必要はなくなる．

4.1.3 GIX における経路制御の問題点

GIX に接続している ISP 間では，主に BGP-4 プロトコルによる経路交換を行っている．同じ ISP の間で，複数の IX で経路交換を実施するとすると，複数ルータで経路情報が交換されることになる．こうした場合，AS 内部で経路情報を集約し，最適化してから最適な経路を使用することになる．そのため，経路の最適化を行うための計算コストは，経路交換の場所が増えるに従って大幅に増加する．IX において，他の ISP との間で経路交換を行うルータを，AS ボーダルータと呼んでいるが，これらの数は高々数台〜十台程度が限界とされている．

すなわち，RIX が GIX と同じように BGP-4 プロトコルを用いて相互接続することは，地域 IX の今後の増加を考えると，まったく現実的で無いことがわかる．また，図 4.3の様な地域 IX の形態において，G-ISP-A と R-ISP-α，G-ISP-B と R-ISP-βがそれぞれ契約している場合，上流となる ISP (G-ISP-A や G-ISP-B) は，契約した地域 ISP(G-ISP-A の場合は R-ISP-α のみ，G-ISP-B の場合は R-ISP-β のみ) のデータだけを伝送したいのであって，契約していない地域 ISP のデータは伝送したくはない．しかし，地域 IX において GIX と同様にすべての経路情報を交換すると，契約していない地域 ISP のパケットも伝送する可能性が生じてしまう．

これらの問題を解決するためには，地域 IX における新しい経路制御技術が必要である．

4.1.4 地域 IX の実現

地域内通信を地域内に閉じることを目的とした地域 IX を構築する上で，考慮すべき技術的制約は以下の通りである．

- 制約 1: 同じ AS の組み合わせの間で Peer の数が増加しない
- 制約 2: AS 番号は有限であるため新たに AS を取得しない
- 制約 3: 経路情報の伝送が可能である
- 制約 4: ネットワーク管理のオーバヘッドが少ない
- 制約 5: 高度なネットワーク管理技術を必要としない
- 制約 6: 地域インターネット事業者ごとに上流とするインターネット事業者の選択が可能である

図 4.3のような形態の地域 IX における経路制御の実現法として，現在の技術で考えられる実現法についてまず議論する．

現状技術による地域 IX 構築の問題点

[**実現法 1**] として地域 IX を 1 つの AS として運用する手法が考えられる．この手法では上記の制約 2 を満足できない．これは AS 番号は 2^{16} しかないため，地域 IX が今後も増加することを考慮すると，AS 番号の枯渇という問題が生じるため拡張性に問題がある．

[**実現法 2**] として地域 IX がプライベート AS を使用する手法が考えられる．この場合，新たに AS を取得しないため，AS 番号の枯渇という問題は解決される．しかし，制約 3 を満足することができない．すなわち，地域 IX の下流にさらに独立した AS をつくった場合，プライベート AS を用いた IX では経路を中継するトランジット AS にはなれないという問題がある．

[**実現法 3**] としてインターネット接続事業者の間で，お互いに経路を静的 (static) に設定する手法が考えられる．この手法では制約 4 を満足できない．経路を静的

に設定する場合には，他の ISP 事業者のネットワークトポロジーが変更されるたびに，管理者は自分の管理するルータの経路の設定を行なわなければならない．ネットワーク管理者は他の ISP 事業者のために自社ルータの設定を行う必要が生じるため，実際の運用環境においては非現実的である．

[**実現法 4**] として IP トンネリング技術を使用する手法が考えられる．しかし，この手法では制約 5 を満足できない．IP トンネリングを行なう ISP の数が増加すると，ネットワークの構成がかなり複雑になり，運用管理がより困難となる．さらに, トンネリングを行なう ISP 内部での経路制御も，通常より複雑になる可能性が指摘されており，技術レベルの低い地域では現実的では無い [42].

以上, 現在の技術を用いた [**実現法 1**] 〜[**実現法 4**] では，制約 1 〜6 のすべてを満たすことはできない．

ソース IP アドレスを利用した経路制御システムの提案

上記すべての制約を満たすために，“ソース IP アドレスを考慮した経路制御システム” を提案する．

提案する手法は経路制御システムにおいてソースアドレス集合を定義し，そのアドレス集合ごとに独立した経路表を持たせる．そしてソースアドレスごとに独立した経路表を検索し，目的ホストまでの経路を選択する．

この手法では，地域 IX より下流のネットワークでは IGP(InternalGateway Protocol) による経路交換を実施する．これにより，地域内の通信は地域内で完結させることが可能となる．また，R-ISP-α は AS-A に，R-ISP-β は AS-B に含まれるため，AS の数を増やす必要もない (図 4.3 参照). 次に，R-ISP の下流ネットワークに新たに別の AS を作ったとしても，経路情報を伝送できるため制約 3 も満足できる．また，経路情報は動的に交換され，現在ある他のシステムやプロトコルなどを全く変更する必要も無い．経路制御システムの一部を置き換えるだけなので従来のネットワーク運用に比べても，特に困難を伴うとは思えない．

よって提案するソース IP アドレスを用いた経路制御手法は，制約 1〜制約 6 のすべてを満たすことが可能である．

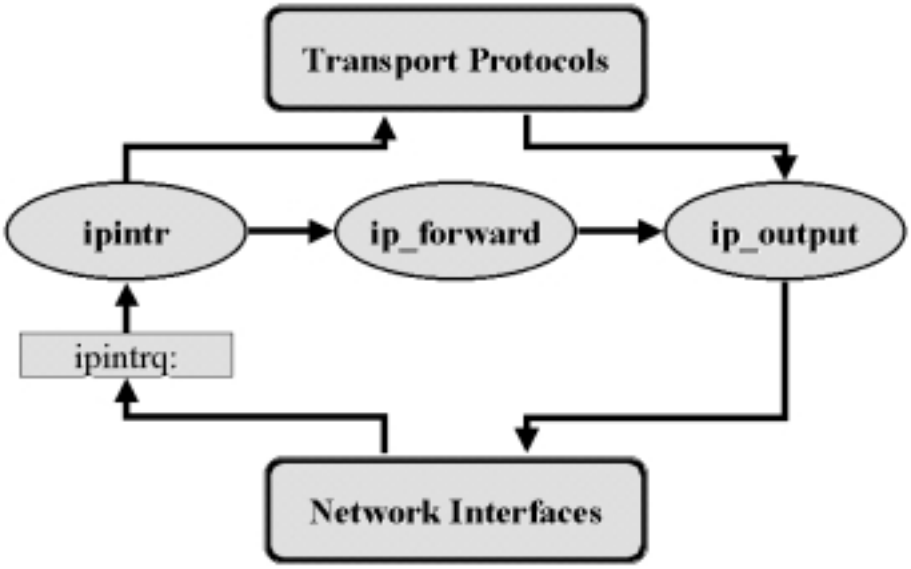


図 4.4 パケット転送メカニズム

4.1.5 ソース IP アドレスを考慮した経路制御システム

インターネットにおける通信は，データトラヒックの送信者が指定した相手先のアドレスであるディスティネーション IP アドレスによって決定される．ここでは，経路決定におけるパケット転送メカニズムについて述べ，提案する発信者のアドレスであるソース IP アドレスを経路制御に利用する新しい経路制御システムの実現方法とその効果について検証する．

パケット転送メカニズム

経路制御システムにおいてパケット転送時のメカニズムを図 4.4 に示す．経路制御システムは受け取ったパケットの宛先を判別し，自ホスト向けのパケットはそのままトランスポート層に渡す．他ホスト向けのパケットは関数 ip_forward に

おいて経路表を探索することにり，次の宛先を決定する．

経路制御システム (STAR) の実現

提案する経路制御システムでは，各 ISP に属するホスト群を，アドレス集合として定義する．経路制御システムは，ひとつのアドレス集合に対して，ひとつの経路表を持つ．具体的には，カーネル内部に確保されるアドレスファミリ AF_INET に対して，複数の経路表を持つようにする (図 4.5 参照)．そして，経路を選択する関数 ip_forward が呼び出された場合に，パケットのソース IP アドレスを調べ，どのアドレス集合に属するホストから来たパケットかを判断する．その後，そのアドレス集合に対応した経路表を，複数ある経路表の中から選択し，次のパケット転送先を決定する．経路決定をソース IP アドレスに基づいて決定するため，提案システムを “Source address oriented Trafficc Arrangement Router(STAR)” と呼ぶことにする．

提案する経路制御システム (STAR) を用いると，次のような効果が得られる．

- E1. 冗長な経路を短縮することで，GIX を経由することなく地域内で通信を折り返すことができる．

- E2. 伝送される回線の選択では，伝送速度や伝送コストの違う回線があるが，目的ホストまでの伝送回線を様々なポリシにもとづいて選択できる．

- E3. ソース IP アドレス詐称を禁止する経路制御システムを利用できるため，予め登録していないアドレス集合から来たパケットは転送しない様に設定できる．これにより，ソース IP アドレスを偽った通信を禁止することができる．

- E4. 構築された地域 IX 内に，さらに狭い地域を対象とした地域 IX を作ることができる．すなわち，地域 IX を階層的に作り，構築した地域 IX でも E1 〜 E3 までの効果を得ることができる．

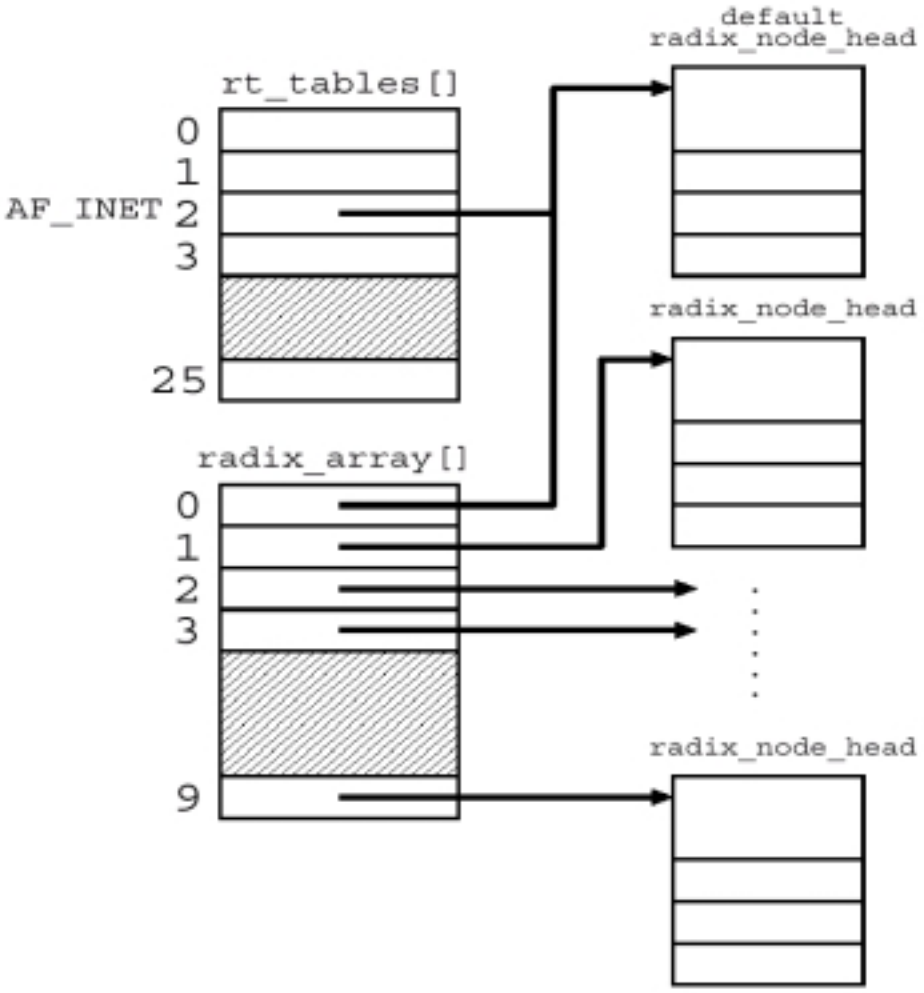

default
radix_node_head
rt_tables[]
0
1
AF_INET 2
3
25
radix_node_head
radix_array[]
0
1
2
3
9
radix_node_head

図 4.5 複数の経路表

4.1.6 経路制御システム (STAR) の実装

UNIX オペレーティング (FreeBSD V2.2.1) を対象に経路制御システム (STAR) の実装を行った．UNIX での既存の経路表はカーネル内にあるため，経路表を複数もつように変更するには，カーネル内に直接組み込む方式が適切である．そこで，複数の経路表へのポインタを保持するために，1 次配列 (radix_array[ ]) を新たに設けた (図 4.5参照)．現在の実装では，経路表は最大 10 個まで持つことができるようになっているが，この値はカーネル内に定義されているマクロ (RADIX_MAX_NUM) を変化させることにより変更できる．また，rt_tables[2] に保持している経路表へのポインタと，radix_array[0] に保持している経路表へのポインタは同じであり，この経路表をデフォルトの経路表と呼ぶことにする．パケット転送時おいて，ソース IP アドレスが含まれるアドレス集合が定義されていない場合には，デフォルトの経路表を検索し転送先を決定する．

STAR では，既存の経路アルゴリズムで用いている radix_array[ ] を拡張することで，ルーティングの基本的なメカニズムに手を加えることなく，自然な拡張が実現できている．

追加したコマンド

STAR システムでは，複数の経路表に対し必要な操作を行うためのコマンドを新規に追加している．これらのコマンドは，特徴を理解しやすいように既存コマンドの先頭に “s” を追加したコマンド名で統一し，複数経路表に対する操作を指定する部分以外は，既存コマンドとの互換性を維持している．

sroute(8)

通常，管理者が経路表に経路情報を追加あるいは削除する場合には，route(8) が利用される．複数ある経路表のどの経路表に対して，経路情報を追加あるいは削除を指定するため，新しいコマンドとして sroute(8) を用意した．

snetstat(8)

複数の経路表を表示するためのコマンドとして，snetstat(8) を追加した．

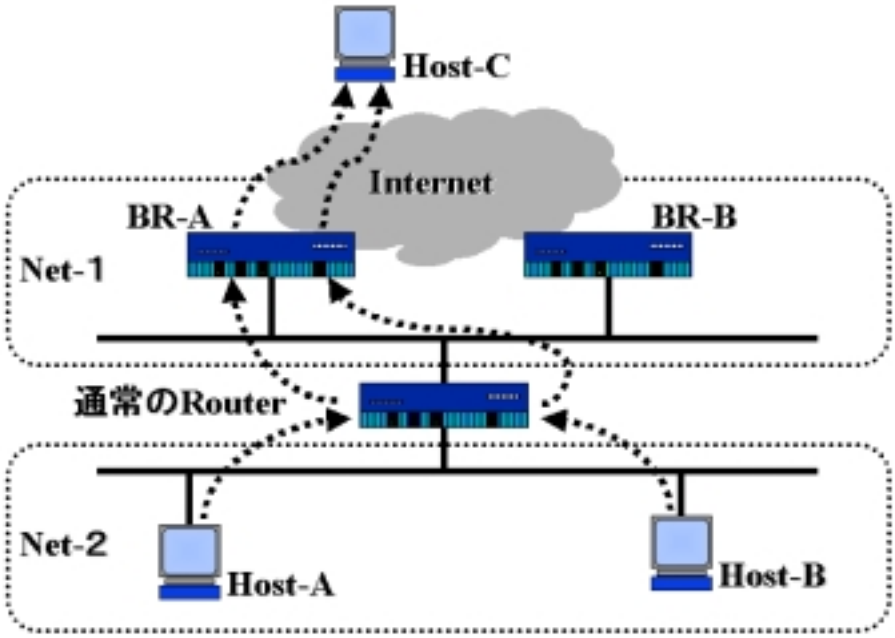


図 4.6 通常のルータを利用した場合

sifconfig(8)

経路表毎にインターフェイスの設定ができるように sifconfig(8) を用意した.

4.1.7 STAR システムの評価

提案した STAR システムの有効性を検証するため，実験環境を構築しシステムの評価を実施した.

実験環境による通信評価

実験ネットワークとして Net-1 と Net-2 を使用し，ネットワーク間には “Router” を設置する (図 4.6 参照). Router のデフォルトルートは BR-A を示しているた

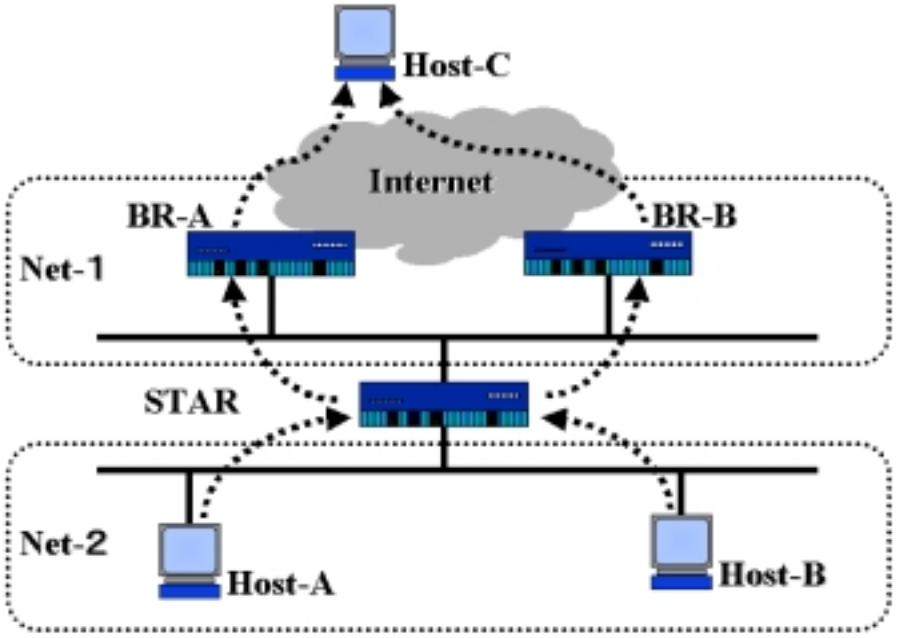


図 4.7 STAR システムを利用した場合

め，Host-A や Host-B が Host-C と通信する場合には BR-A を経由する．

次に STAR システムを用いた場合の動作について説明する．Host-A と Host-B にそれぞれ専用の経路表を STAR システムに作成する (図 4.8 参照)．

Host-A の経路表のデフォルトルートを BR-A，Host-B の経路表のデフォルトルートを BR-B に設定する．すると，Host-A をソース IP アドレスとする通信は BR-A を経由し，Host-B をソース IP アドレスとする通信は BR-B を経由することが分かる (図 4.7参照)．

パケット転送能力

FreeBSD ver2.2.1 に実装した STAR システムと，標準のままの FreeBSD でのパケット転送能力を比較してみた (表 4.1参照)．インターネットでのトラヒック

```
Radix tree: No.1
Address group: 202.244.160/24
Destination                Gateway              Flags
default                    202.244.160.1        UGSc
163.221/16                 202.244.160.7        UG
202.244.160/19             202.244.160.7        UG

Radix tree: No.2
Address group: 203.178.153/24
Destination                Gateway              Flags
default                    203.178.153.1        UGSc
163.221/16                 203.178.153.10       UG
202.244.160/19             203.178.153.2        UG
```

図 4.8 snetstat コマンドの実行結果

表 4.1 パケット転送能力の比較 (単位：pps)

Data Size	512 Byte	1024 Byte	1472 Byte
FreeBSD	998	658	498
STAR	984	652	494

測定ツールとして公開されている Netperf[43] を使用し，出来限り多くの UDP パケットを 2 台のホスト間で送信し，STAR システムにおいて転送されるパケット数を実測した．ただし，STAR システムの経路表は 10 個とし，送信するデータサイズは 512 Byte，1024 Byte，1472 Byte の 3 つの場合について測定した．表 4.1から STAR システムを導入してもたかだか 10 個程度の経路テーブルであれば，パケット転送能力はほとんど変化しないことが分かる．

安定性

STAR システムの安定性を実証するため，まず研究室の有志数人に依頼し，このシステムを使用したネットワークを実際に稼動させた．その結果，特に問題が発生しなかったので，岡山情報ハイウェイにおける CATV インターネット接続などで実験的に利用され，安定的に動作することが確認された．

4.1.8 ソースアドレスルーティングのまとめ

提案した STAR システムは，これまでの経路制御の考え方を見なおした画期的な経路制御手法である．後述する岡山情報ハイウェイでも，ソース IP アドレスを用いた経路制御手法が地域 IX の構築において採用され稼動している．実装手段は異なるが，インターネットルータ市場でのトップシェアを誇る CISCO 社のルータにも，ソース IP アドレスを用いたポリシールーティングの機構が実装され，ソース IP アドレスを用いた地域 IX の構築手法は，市販される製品を組み合わせても実現できるようになった．

STAR システムの実装において，いくつかの検討項目が未解決のまま残っている．経路表へのポインタの探索が 1 次配列の線形探索のため，経路表の数が増加すると経路表へのポインタを探索する時間は O(n) のオーダで増加する．よって，将来的に経路表の数が増加するならば，経路表へのポインタも radix_tree に格納するべきである．この場合，必要となる経路探索時間は，経路表へのポインタを探す時間 O(log n) と実際に経路表で経路を探索する時間 O(log n) の和となり，O(logn) のオーダで抑えることができる．また，現在の実装ではデフォルトの経路表への経路情報の追加・削除のみを，ルーティングデーモン (gated,routed) が動的に行っている．これ以外の経路表への経路情報の追加・削除は，管理者が静

的に行っている．運用管理上の問題もあるため，早急に複数経路に対応したルーティングデーモンを導入する必要があるだろう．

4.2. 地域ネットワーク構築モデルの確立

地域ネットワークの構築は，社会的な公共インフラストラクチャとしての役割を担っており，情報化による地域の活性化は地方自治体にとってもはや欠かすことができなくなりつつある．そこで地域ネットワーク構築時の汎用的な手法としてパブリックファイバーモデルを提案する．

4.2.1 地域情報化の必要性

民間企業による地方都市での情報化は，東京や大阪などの都市部と比較すると思ったほど進展していない．インターネット接続サービスを提供する事業者は，事業採算性を考慮するため，中小規模の都市や過疎地域では大規模な事業展開はなかなか行われない．もちろん，時間が経過すればそれなりのサービスが提供されることは間違い無いが，このままでは都市部との情報格差は拡大する一方である．情報化による経済の変革が叫ばれる中で，地域の情報化を着実に推進するには，地方自治体など行政による情報化への取り組みが不可欠である．地域住民が各種の情報に接する機会を，都市部住民と同等に提供することは，21 世紀を目前に進展しつつある情報革命に追随する上でとても重要なことである．

情報化の進展を計る尺度の一つに，通信基盤 (情報インフラ) の整備状況が挙げられる．地方都市と都市部とを比較すると，あきらかに需要が見込まれる都市部から順に整備されている．そのため，インターネットの特徴のひとつである地理的な制約を受けないというメリットが，かなりの部分で失われてしまっている．地方都市や過疎地の住民は，都市部の住民に比べて多大な通信費用を負担しなければインターネットを利用できなかったり，低速なネットワークしか利用できないのが現状である．この様な情報インフラの整備についての不平等は，情報格差による新たな差別として “デジタルデバイド” と呼ばれる差別問題を引き起こしはじめている．しかも，情報化社会への急速な進展でその格差は拡大する一方である．また，こうした情報格差は，日本国内にとどまらず世界レベルで発生する

ことを忘れてはならない．なぜなら，電子商取引に代表されるインターネット経済は，国境を超えたサイバースペースで提供されるため，従来型の国内での競争はあまり意味を持たない．デジタルデバイドは，すでに国家間の情報格差へと拡大しつつあるのである．

そこで，世界的に見ても公平なインターネット利用環境を，地域のユーザにも十分提供できる枠組みとして，地域ネットワークの構築に着目し，岡山県が推進する岡山情報ハイウェイ構想において，実際に稼動し機能する地域ネットワークの構築を試みた．

4.2.2 地域ネットワークの構築

全国各地の地方自治体が地域インターネットや地域情報ネットワークに関連する情報化構想を打ち出し，そのいくつかはすでに実際に運用を始めている [44]．このように地方自治体が主体となって構築された地域ネットワークをコミュニティエリアネットワーク (CAN: Community Area Network) と呼んでいる．行政情報をインターネットに向けて発信するだけであれば，その地域でサービスを実施しているインターネット接続事業者のネットワークを利用すれば，比較的容易に実現できる．しかし自治体やその関係機関が，自らの手でネットワークを構築しようとすると，数多くの課題に直面する．本論文では，都道府県や政令指定都市規模の比較的大規模な地域ネットワークを構築する場合の課題について議論し，これらのネットワークに適用できる構築手法モデルを提案する．

筆者が参画した岡山県が目指した情報化構想には，自治体自らの手による全県にわたる広域ネットワークの構築と，地域 IX の実現の双方が織り込まれており，実現にむけてかなりの課題が存在した．解決しなければならない技術的な課題として，インターネットにおけるデータの到達性の鍵を握る経路制御の問題があった．利用者に割り当てるドメイン名やネットワークアドレスなどのネットワーク資源に関する問題も存在する．構築したネットワークを維持し，管理・運用する技術者の育成も緊急の課題として議論された．ネットワーク管理者は世界的に見てもあきらかに不足している．日本でもこの傾向は見られ，各地のネットワーク構築に同じ人材がかかわっていることも珍しくない．最も大きな課題は域内通信コストの問題である．受益者の負担を考えず，ただ単に無料 (あるいは格安) のイ

ンターネットサービスを提供すれば良いとうことでは無い．行政が通信事業者に費用を支払って通常の通信回線を借り上げ，これを開放していたのではお話にならない．長期にわたってその費用を税金でまかなうことは事実上不可能である．

また，地方自治体側の人事制度も情報化への取り組みを阻害している一因に思える．都道府県庁や市町村の情報担当部署の人事には，ほぼ 2,3 年で担当者が別の部署に移動する慣例がある．専門的な知識が必要とされる情報部門に，その分野にこれまで無関係であった者が配置されるため，適切な判断を行えるよう再教育しなければならない．そのため，進歩が激しい情報分野においては致命的な停滞を余儀なくされることになる．

これらの課題を克服し，実際に稼動する地域インターネット網を構築した点で岡山県の取り組みは高く評価することができるだろう．

4.2.3 パブリックファイバーモデルの提案

本論文で提案する地域ネットワーク構築手法モデルは，通信基盤として地方自治体が自ら敷設した “パブリックファイバー (公共ファイバー)” と呼ばれる光ファイバーを用いる．自治体が公共目的に通信基盤整備を行うことから，経済的な収益が十分に見こめない地域であっても，情報格差の是正を目的として都市部に匹敵する情報基盤を構築することも可能となる．合わせて域内の高速通信を実現するために，地域 IX を併設して構築する．

パブリックファイバーによる高速通信基盤の構築と域内高速通信を実現するための実用的な地域 IX を併設させる地域ネットワークの構築モデルを，本論文ではパブリックファイバーモデルと呼ぶ．

提案モデルの特徴

提案するパブリックファイバーモデルには，前述の問題を解決するために，次の様な特徴がある．

1. 自治体が光ファイバーを自設することで，域内の高速広帯域通信インフラの実現を図る．

2. 域内の高速性を最大限に生かせる地域 IX を情報インフラと同時に実現する．

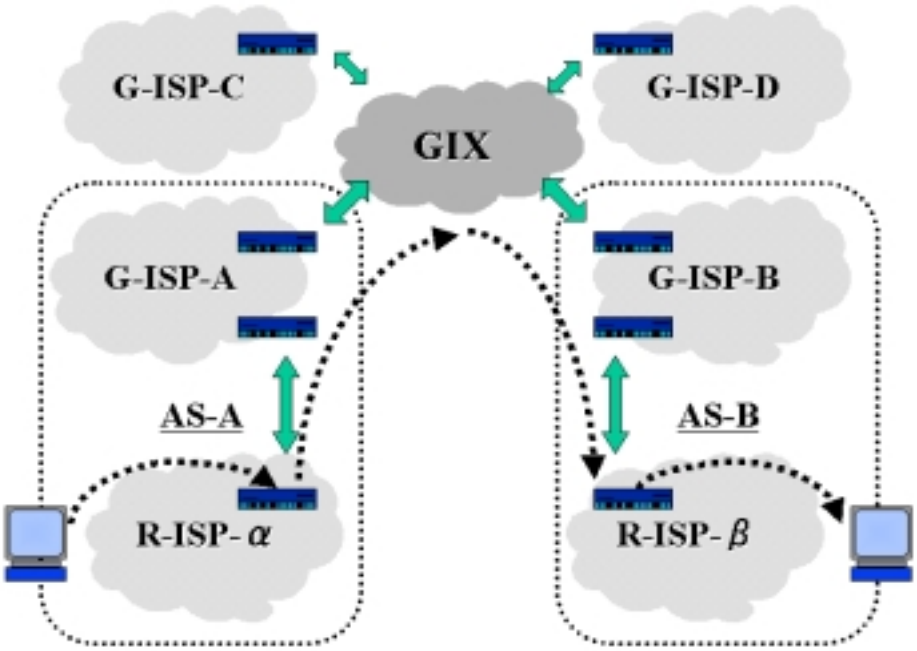


図 4.9 Global IX を経由する経路

3. インターネットへの接続環境を地域ネットワークが独自に用意せず，地域 IX に接続しているインターネット事業者を活用する．

4. 住民の地域ネットワークへのアクセス手段は，地域ネットワークに接続している CATV 事業者やインターネット接続事業者の接続サービスを活用する．

4.2.4 地域 IX の必要性

インターネットでは，非常に多くのインターネットサービス事業者 (ISP: Internet Service Provider/プロバイダ) が事業を展開しており、経路情報の交換に付随する新たな問題が指摘されている．現在の日本のインターネットでは，異なるプロバイダ間での経路情報の交換は，国内に数箇所しかない IX(Internet eXchange)

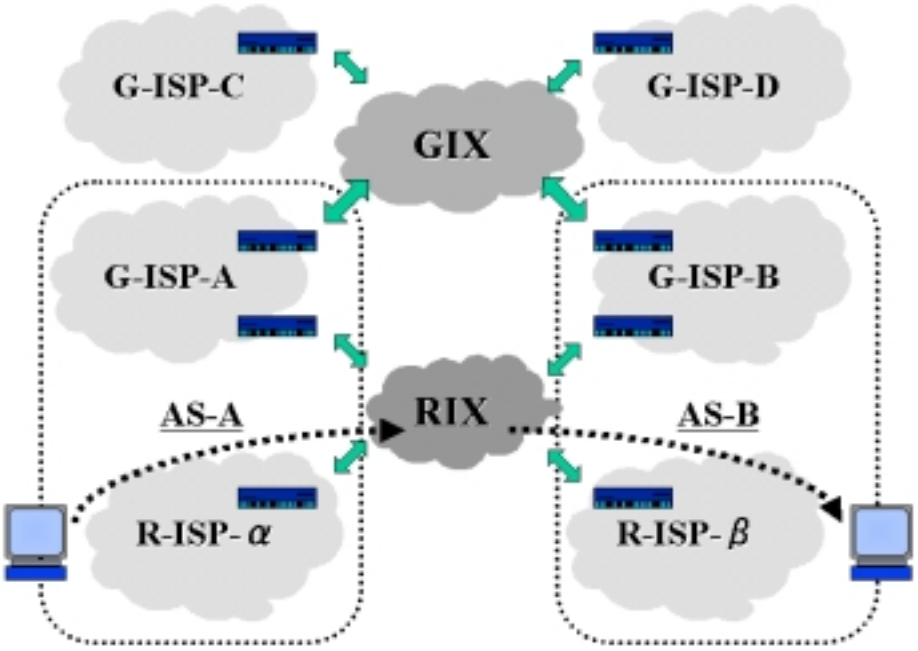


図 4.10 地域 IX がある場合の経路

を経由して行われている．国内最大規模の NSPIXP-2 は東京大手町に設置されており，大手プロバイダ間の経路情報の交換は主にここで行われている．そのため，たとえ隣人との間での通信であっても，加入しているプロバイダが異なれば，NSPIXP-2 を経由した通信になってしまう．つまり，地方で発生した通信データは，NSPIXP-2 のような大都市に設置されている IX(Internet eXchenge) に一旦集められ，また地方へと回送されることになり，冗長な通信路のために快適な通信を享受することが出来ないのが現実である．このことは，たとえ高速な地域ネットワーク網を整備しても，それだけではその高速性を発揮できないことを意味する (図 4.9，図 4.10参照)．

提案モデルで必要としている地域 IX は，通常の IX とは異なる性格を持つ．通常の IX の場合，インターネット接続事業者が持つすべての経路に関する情報を，

BGP-4 プロトコルを利用して相互に交換するのが一般的である．しかし，この手法だと他のインターネット事業者との接続点を増やせば増やすほど，経路の計算が複雑になり，安定的な運用ができなくなったり，正常に機能しなくなってしまう欠点がある．これでは，インターネット事業者が安易に地域 IX に接続することは不可能である．地域 IX では，域内経路の短縮だけを実現できれば良く，すべての経路に対する到達性を確保する目的で設置される通常の IX とは明らかに目的が異なる．そこで，域内経路の提供だけをインターネット接続事業者に求め，それ以外の経路交換については各事業者間の自由裁量という方式を採用することで，地域 IX へのインターネット接続事業者の参入を可能としている．

これまでに述べた地域ネットワーク構築に関する研究成果は，岡山情報ハイウェイの構築に適用され，実用化を遂げた岡山情報ハイウェイは，日本を代表する地域ネットワークとして現在稼動中である．

4.2.5 岡山情報ハイウェイの構築

岡山県では，地理的な制約から生じる情報格差を是正し，誰もがネットワークを使うことができる環境を県民の基本的な権利と位置付け，公共ネットワーク基盤としての岡山情報ハイウェイの構築を推進している [40][45][46]．本論文で提案した地域ネットワーク構築モデルであるパブリックファイバーモデルは，岡山情報ハイウェイ構想において，実際に稼動する地域ネットワークを早期に実現するために考案した構築手法モデルである．

岡山情報ハイウェイ構想は，1996 年 2 月に策定された「岡山県高度情報化基本計画」に基づいた岡山県における地域情報化構想である．特に通信基盤としての岡山情報ハイウェイの整備において，次の目標を掲げてネットワークの整備にあたっている．

- ユニバーサルサービスの実現

  国際的に適正な価格・品質のサービスを提供できるインフラの整備を目指し，産業分野における新たなビジネスチャンスの創出と国際競争力を持つ県内産業の発展と雇用の確保を図る．

- バリアフリーコミュニケーションの確立

ネットワーク社会における地域間の情報格差 (情報過疎) の是正と，高齢者，障害者など，誰もが情報を利用できるネットワーク環境を実現する．

- 県民と県庁とのグループウェアの実現

  ネットワークを利用した行政情報の公開や，福祉・医療・教育分野などでの活用により，居住地域での高度サービスの提供を実現する．

- 地域ネットワーク（CAN: Community Area Network）モデルの確立

  各地で取り組まれている地域ネットワーク構築のモデル事例として，地域ネットワーク構築における各種のノウハウを，失敗例を含めて可能な限り公開する．

こうした目標を実現するために，1996 年から 3ヵ年，“岡山県高度情報化実験推進協議会” が組織され，ネットワークを活用する数多くの実験が実施された．また，実際に動作する地域ネットワークを構築するために，技術的な課題を克服する目的で，インターネットワーキング技術コンソーシアム (代表 村井純 慶応大学教授，筆者は副代表) が組織され，岡山情報ハイウェイが採用するネットワークアーキテクチャの決定や，運用ルールの策定などを行ってきた．

岡山情報ハイウェイの特徴

岡山情報ハイウェイは，筆者が提案したパブリックファイバーモデルに基づく地域ネットワークを構築している．そのため，提案モデルの特徴として示した 4 つの特徴をすべて兼ね備えている．

1. 岡山県が独自に光ファイバー網 (パブリックファイバー) を自設することで，域内の高速広帯域通信インフラを実現している．

2. 域内の高速性を最大限に生かせる地域 IX として，OKIX(OKayama Internet eXchange) を情報インフラと同時に実現している．

3. インターネットへの接続は，OKIX に接続しているインターネット事業者のいずれかと契約することで実現する．

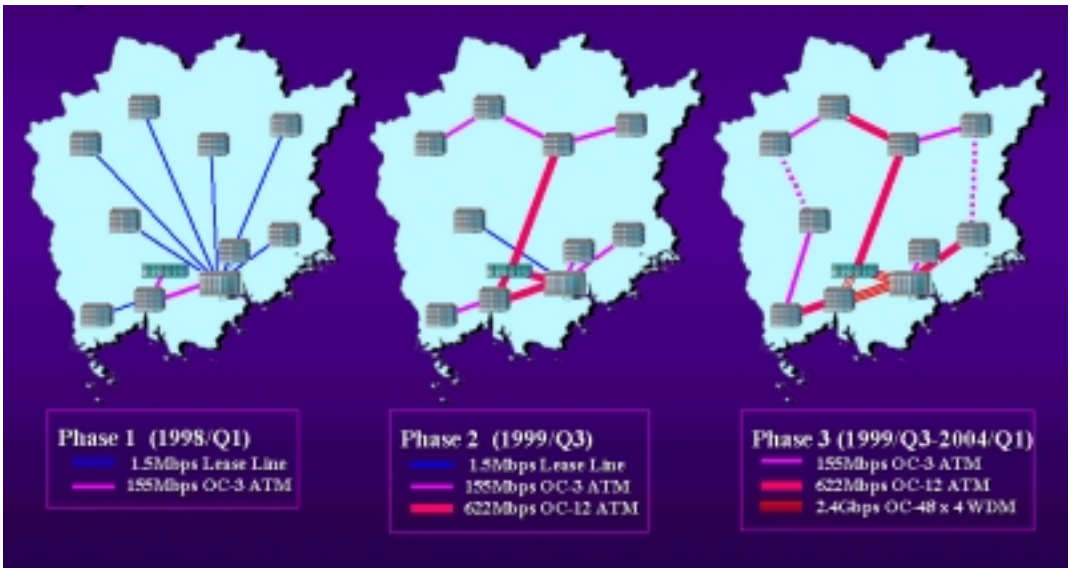


図 4.11 ネットワーク構築計画

4. 住民の岡山情報ハイウェイへのアクセス手段は，OKIX に接続している CATV 事業者やインターネット接続事業者の接続サービスを活用する．

岡山県 (人口約 195 万人，世帯数 65 万世帯) には，県内全域をカバーするため 9 箇所に地方振興局が設置されている．岡山情報ハイウェイは，この地方振興局と県庁に設置された合計 9 箇所の接続ポイント (POP: Point of Presence) と，ネットワークの運営を統括するネットワークオペレーションセンタ (NOC: Network Operation Center) を相互に接続する自設光ファイバー網を中心に構成されている 4.11．利用者は，県内いずれかの POP や NOC に，自らのネットワークを直接接続するか，ここに接続している CATV 事業者やインターネット接続事業者と契約することで，岡山情報ハイウェイを活用できる．

パブリックファイバー

岡山情報ハイウェイ構想は，他の地方自治体が推進するさまざまな地域情報ネットワーク化の計画の中で特筆するべき特徴を持っている．県内の地方振興局間のネットワーク接続において，基幹となる光ファイバー網を建設省や岡山県の負担

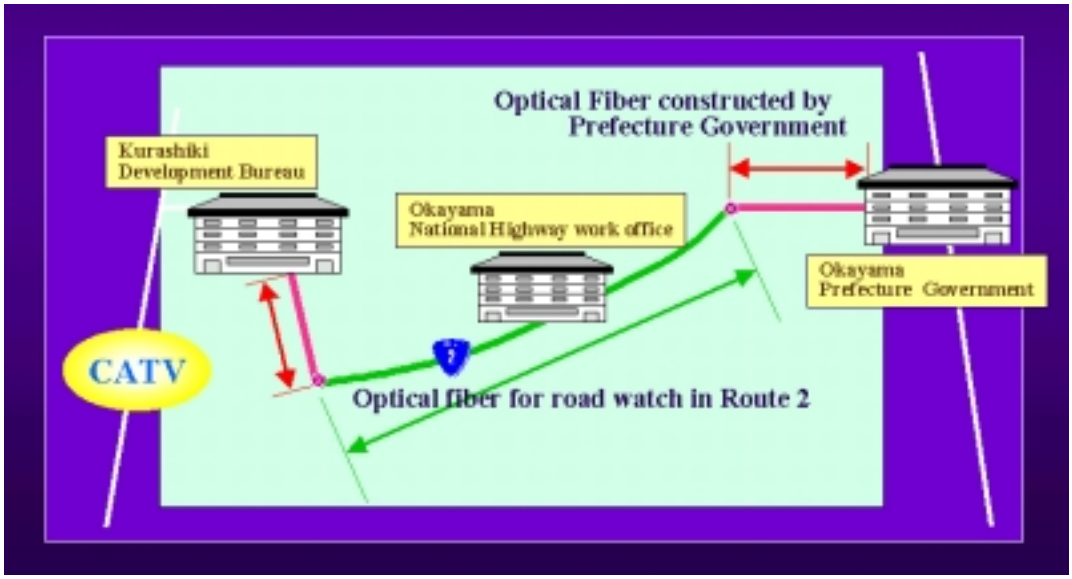


図 4.12 パブリックファイバー

により独自に敷設している．これは建設省が推進している国道沿いの情報ボックスを活用した光ファイバー敷設の先行事例であるとともに，日本で初めての自治体主導による自設光ファイバー網を活用した地域ネットワークとなっている (図4.12参照)．

岡山県では，県が独自に敷設した光ファイバーのことを “パブリックファイバー(公共ファイバー)” と呼んでいる．特定の 2 地点間を光ファイバーで接続しようとした場合，通信事業者が所有する用いられていない遊休光ファイバーを活用する事例が多い．このような事例で用いられる遊休ファイバーは，通信のための光が通過していないため，ダーク (暗いままの) ファイバーと呼ばれている．しかし一般県民に，そのままダークファイバーと説明すると，“ダーク” という言葉からあまり良い印象を与えられない．そのため，あえてパブリックファイバーと呼び，公共目的で活用されていることを印象付けられるよう配慮している．

自治体が自設の光ファイバー網を所有することで，県内域の通信コストを低く押さえることができるとともに，需要に応じて各地点間の通信速度の変更が容易に実現可能となる．

地域 IX の構築

岡山情報ハイウェイの整備と同時に，地域 IX である岡山インターネットエクスチェンジ (OKIX:OKayama Internet eXchange) を構築し，域内の円滑な通信の実現を図っている．

OKIX では，域内経路の短縮だけを実現できれば良く，すべての経路に対する到達性を確保する目的で設置される通常の IX とは明らかに設置目的が異なる．そこで域内経路の提供だけを OKIX に接続するインターネット接続事業者に求め，それ以外の経路交換については各事業者間の自由裁量というルールで運用している．岡山情報ハイウェイ内の域内経路 (regional route) は，OSPF プロトコルを用いての交換を義務付け，域外経路 (external route) の BGP-4 プロトコルによる交換は，希望する事業者のみが行うという独特の地域 IX として機能している．

地域 IX におけるもうひとつの問題として帯域制御の問題がある．経路制御とあわせてこれらの問題を解決するために，地域 IX で利用できると言われている 5 つの手法について岡山情報ハイウェイへの適用の可否を検証している．

1. 通常の AS を用いた BGP による手法
2. Private AS を用いた BGP による手法
3. 接続事業者間で互いに静的な経路 (Static routes) を設定する手法
4. VPN などの IP トンネリング技術を用いた手法
5. ソースアドレスルーティングを用いた手法

これらすべての手法を実践し，技術的・経済的な側面から評価し IP トンネリングとソースアドレス・ルーティングを組み合わせた手法を地域 IX に採用している．インターネット接続事業者は，これにユーザとの契約に応じた帯域制御技術を組み合わせることにより，岡山情報ハイウェイに接続しているユーザを顧客とするビジネスの機会を得ている．

現在 OKIX には，4 社の CATV 事業者と 10 社のインターネット接続事業者が接続し，岡山情報ハイウェイを経由したインターネット接続を提供している．

図 4.13 アクセスポイント一覧 (http://www.pref.okayama.jp/より抜粋)

図 4.14 ネットワークオペレーションセンタ

ネットワークオペレーションセンタ

岡山情報ハイウェイにおけるネットワーク運用の拠点として，県営のネットワークオペレーションセンタを設置している．ここには常駐の運用スタッフがおり，3 交代制による 24 時間/365 日の運用・監視体制を維持している．また，インターネットサービス事業者や通信事業者による利用を想定したハウジングとしての機能を有している．たとえば，二酸化炭素消化設備や無停電電源設備，24 時間の入退室管理，耐震構造などの各種の通信事業法上の通信設備を設置するための法的基準を満足している．また，ここでのネットワーク接続は，1999 年の 4 月から一般に開放されており，筆者が所属している倉敷芸術科学大学も，ここを活用して岡山情報ハイウェイとの相互接続を実現している．

住民の利用

岡山情報ハイウェイは，平成 11 年の 3 月末で第 1 段階としての実験フェーズを終了し，今年の 4 月から一般開放を認めた公開運用体制に移行している．ネットワーク自体は，県庁や地方振興局などの県の機関を相互に接続した行政ネットワークの一部を民間に開放する形式を取っているため，行政財産の利用申請を行うことで，一般企業や市町村，大学などによる活用が可能となっている．また，申請は随時受け付けられており，各振興局を核にその地域に根ざした情報化推進のための地域情報化推進委員会が組織されている．

一般の県民が岡山情報ハイウェイを利用しようとする場合には，次の方法が考えられる．

1. インターネット接続事業者と契約

   OKIX に接続しているインターネット接続事業者と契約することで，契約事業者のアクセス回線を経由して，岡山情報ハイウェイを利用できる．OKIX に接続している事業者には，岡山県内のユーザに関する経路情報を，岡山情報ハイウェイに対してアナウンスするよう義務付けているため，契約する事業者が異なっているユーザ間の通信でも，岡山県内で完結する．

2. CATV インターネット

   岡山県には，自主放送を行っている CATV 事業者が 15 社存在する．このうちの 4 社が CATV インターネットの事業化を目指しており，1999 年 11 月の倉敷ケーブルテレビを皮切りに，順次 CATV インターネット接続事業を開始する予定である．

3. 自らが機器を持ち込み直接接続

   倉敷芸術科学大学や岡山市民生協，倉敷中央病院など 9 件のユーザが NOC や POP に独自に機材を持ちこんで利用している．NOC や POP にネットワーク機器やサーバを設置することで，岡山情報ハイウェイの高速性を享受できる．

4. 公共端末を利用

岡山県がバスターミナルや県立の美術館，博物館などに設置している情報キオスク端末などの公共端末を使って活用する．

5. 高等学校や大学などを利用

岡山県内の県立高校は，すべて岡山情報ハイウェイに接続されている．これらの学校や，岡山情報ハイウェイと接続している大学のマルチメディア講義室や実習室などを利用することで，間接的に岡山情報ハイウェイを活用できる．

もちろん，OKIX に接続していないインターネット事業者と契約したとしても，岡山情報ハイウェイにアクセスすることは可能である．しかしながら，OKIX に接続していない事業者との通信は，一般的には東京や大阪の GlobalIX を経由することになり，折角構築した高速な地域ネットワークの性能を十分に生かしきることができない．

また，岡山県では県民の理解を深めるため，さまざまな啓蒙活動を実施している．岡山情報ハイウェイをわかりやすく解説した小冊子 [45] の作成やシンポジウムの開催，岡山情報ハイウェイを活用した実験に対する助成金などにより，少しずつであるが住民主導の情報化が進展し始めている．

高等学校のネットワークへの接続

岡山情報ハイウェイを活用した具体的な地域情報化の事例として，岡山県内の高等学校の接続がある．岡山県には県立の高等学校や各種学校が合計で 79 校あり，これらのすべての学校が最寄りの地方振興局 POP を経由して，専用線で岡山情報ハイウェイに接続されている．岡山県では，高等学校における情報化教育の拡充のために，他地域よりもいち早く県内全校に対するインターネット接続を実施した．

提供しているネットワークは，すべて 128kbps 以上の専用線で，学校現場の教師や生徒が利用時間の増加による通信費用の心配をしなくても良いように配慮されている．高校ネットワークは，仮想ネットワーク技術 (VPN: Virtual Private Network) を用いることで，教職員用のネットワークと生徒用のネットワークに完全に分離されている．また，文部省の指導に従い，生徒用のネットワークからのイ

ンターネットアクセスについては，有害コンテンツを排除する目的で文部省指定のフィルタ機能が提供されているプロキシサーバによるフィルタリングを実施している．岡山県ではすべての県立高校生に対してメールアドレスを作成しており，すでに 6 万名を超える高校生ユーザが岡山情報ハイウェイを活用している．各高校からのインターネットアクセスは，それぞれの高校が希望するインターネット接続事業者を岡山情報ハイウェイに接続している事業者から選択でき，現在 7 つの事業者が利用されている．高校側に事業者の選択権がある自由競争のためか，ほぼ満足のいくサービスが各校には提供されているようである．

県内の高等学校によるインターネットの活用は，高校生の手によるインターネット文化祭企画 (スクールフェスティバル 99) などのような複数高校間でのコラボレーション，授業の一環としてのデータ収集など，実際の教育効果が期待できる事例が増えつつある．これからも生徒達の自由な発想を妨げないよう，効果的な教育インターネットの形成を模索する必要があるだろう．

4.2.6 地域ネットワーク構築モデルに関するまとめ

地域ネットワークの構築では，地域ネットワークで活用する情報インフラの整備に関して，通信事業者やインターネットサービス事業者などの民間サービスと行政主導のサービスの役割分担の必要性がしばしば指摘されている．厳しい意見の中には，行政による地域ネットワーク情報インフラの整備を完全に否定する声もある．行政による地域情報化の推進を，単にインターネット接続サービスと捉えるとこうした誤解が生じてしまう．岡山情報ハイウェイの構築により実現された県内ユーザ間の高速接続や，他地域の障害に影響されない域内ネットワークは，明確な行政のインセンティブがなければ到底実現し得ないものである．

また，インターネットは身体障害者や高齢者など社会的な弱者のハンディキャップを解消する手段に十分になり得る．しかしあまりにも急速な情報化のために，地域間の情報化格差が発生していることも事実として受け止めなければならない．また，パソコンなどの情報機器を使いこなせるかどうかによる “デジタルデバイド” などの新たな差別を生じさせないようにしなければならない．そのためには，行政だけでなく産業界や大学・高等学校などの教育機関，地域の住民が一体となった情報化とその活用をこれからも模索し続ける必要がある．

岡山情報ハイウェイ構想は，ネットワークを活用する各種のアプリケーション開発と，実際に稼動するネットワーク構築事業を両輪として推進されてきた．このうちネットワーク構築事業については，自設光ファイバーであるパブリックファイバーを用いた最初の事例でもあり，各方面からかなりの注目を集めている．このような域内高速接続可能なネットワークが，一般に普及した時に考えられる行政サービスアプリケーションは，従来の物とは全く次元の違うはずである．ネットワークは，環境，福祉，医療などさまざまな分野でも活用できる共通の基盤である．それぞれの分野での活用が活発化するように，自治体として異業種へのIT(Internet Technology) コンサルテーションの拡充とネットワーク型コンテンツの確保を重視した施策を推進して行く必要があるだろう．

また，インターネットの分野は技術革新のサイクルが最も急速であると言われている．行政主導のネットワーク構築は，しばしば技術革新について行けずに硬直状態に陥ることがある．その様な状況に陥らないように，積極的に新技術を取り入れて使いやすい地域ネットワーク環境の整備を継続して欲しい．そして，岡山だけが特殊な事例にならないよう全国に地域インターネットのアクティビティが波及することを期待している．

第 5 章

結論

この章では，本論文で得られた成果を総括するとともに，今後の課題について述べる．

5.1. 本研究の成果

本論文では，インターネットにおけるネットワーク構成技術の高機能化に関して，筆者が奈良先端科学技術大学院大学情報科学研究科博士前期課程および博士後期課程 (情報システム学専攻) 在学中に行った研究の成果をまとめたものである．以下，本研究で得られた成果を総括して述べる．

高機能化にかかわる具体的な研究成果として

1. モバイル認証技術
    - パスポートモデルの提案と DHCPA の実現
    - セキュリティ認証ゲートウェイ DAG の設計と実装
2. 地域ネットワーク構築技術
    - ソースアドレスルーティング技術 STAR の設計と実装
    - 地域ネットワーク構築モデル (パブリックファイバーモデル) の確立

がある．筆者は，ふたつの異なる側面からネットワーク技術の高機能化に取り組んできた．ひとつは，ノート型のパーソナルコンピュータなどの移動体通信に

おける安全なネットワーク接続環境を提供するための要素技術の研究，ふたつめは，より広範囲のユーザに等価なサービスを提供するための地域ネットワーク構築技術の確立に関する研究である．

筆者は，ノート型のパーソナルコンピュータなどの移動ホストにおける一般的なセキュリティの枠組みとして，パスポートモデルを提案した．人間の世界でのパスポートの概念を移動ホストにあてはめ，ユーザに直感的にわかりやすくセキュリティを実現しようとしたアプローチである．このパスポートモデルを DHCP に適用し，セキュリティ上の欠点であったネットワーク接続時のユーザ認証 (コンピュータの識別) の問題を解決するための認証機構を新たに組み込んだ DHCPA(DHCP with Authentication) を提案した．

さらに移動ホスト認証後の堅牢なネットワークアクセス制御を実現するために，DHCP とアクセス制御ゲートウェイを連携させるアーキテクチャである DAG(DHCP Access Control Gateway) の設計と実装を行い，その有効性を検証した．これらの一連の研究で，DHCP 利用者に対するネットワーク利用における安全性を高めることができ，ノート型のパーソナルコンピュータなどを用いた移動体通信における安全なネットワーク接続環境を提供でき，ユーザがより安心できるネットワーク構築技術を提供することができた．また，これらの研究成果は，実際の製品化にも貢献しており，提案した技術の一部を取り入れた超小型の DHCP サーバや NAT 機能を有した小型ファイヤーウォールなどの製品が出荷されている [4]．

また，より多くのユーザに平等なインターネット利用環境を提供できる枠組みとして，地域ネットワークの構築に着目し，地域ネットワーク構築時の技術的な課題の解決に取り組んだ．地域ネットワーク構築で技術的な懸案となっていたルーティング問題の解消を試み，送信者の情報であるソースアドレスをルーティングに利用する STAR(Source address oriented Traffic Arrangement Router) を提案し，ユーザ毎に異なる経路を選択する新たな経路制御技術を実現した．

次に，地方都市における情報化への取り組みのありかたについて持論を述べ，地域ネットワーク構築における構築構築手法モデルとして地方自治体による自設光ファイバー (パブリックファイバー) を用いて地域ネットワークを実現するパブリックファイバーモデルを提案した．この提案モデルには 4 つの大きな特徴がある．

1. 自治体が光ファイバーを自設することで，域内の高速広帯域通信インフラの実現を図る．

2. 域内の高速性を最大限に生かせる地域 IX を情報インフラと同時に実現する．

3. インターネットへの接続環境は自治体が独自に用意せず，地域 IX に接続しているインターネット事業者を活用する．

4. 住民の地域ネットワークへのアクセス手段は，地域ネットワークに接続している CATV 事業者やインターネット接続事業者の接続サービスを活用する．

これらの研究成果は，岡山情報ハイウェイの構築に適用され，日本を代表する先進的な地域ネットワークとして現在も稼動している．

岡山情報ハイウェイの構築は，郵政省研究所の研究報告書などでも “地域ネットワーク構築における岡山モデル” として紹介され，地域ネットワーク構築の先進事例として他地域からも注目を集めている．

以上のことから，本論文において提案した方式は，従来のネットワーク構成技法と比べ，より広範囲のユーザにインターネットの利便性を拡大できるとともに，これまで以上に多くのユーザによる利用を期待できる有効な方式である．

5.2. 今後の課題

モバイルコンピューティングの普及は，予想を上回る速度で進展している．携帯電話を利用したインターネット接続や高性能な PDA(Personal Data Assistant) の日本国内での利用者は，すでに数百万人に達している．これらのユーザの利便性は，通信速度や可搬できる大きさ・重量などによる制約のため，まだまだ十分であるとは言えないが，各種の条件の中で十分なユーザニーズを捉えていると考えられる．今後も新たな利用形態を考案し，より利便性を持つモバイル環境の実現に貢献したい．

地域ネットワークの構築は，社会的な公共インフラとしての役割を担っており，情報化による産業構造の変革が叫ばれる中で，岡山県だけにとどまらない地域情報化の推進を働きかけていく必要がある．幸いなことに，岡山情報ハイウェイに

触発された形で，西日本だけ見ても，広島県，山口県，三重県，和歌山県，香川県などで，地域ネットワーク化構想が提唱され，実際の構築作業も始められつつある．

ネットワーク技術の高機能化に対する取り組みは，インターネットを構成するあらゆる部分で必要とされている．モバイルコンピューティングや地域ネットワークに限らず，これからも，国際的な広い視野でインターネットをとらえ，より一層の普及と高機能化をめざした研究活動に取り組んで行きたい．

謝 辞

本研究を行なう機会を私に与えて下さり，懇篤なる御指導，御鞭撻を賜った奈良先端科学技術大学院大学 情報科学研究科 教授 山本 平一 博士，同大学情報科学研究科 教授 千原 國宏 博士，同大学 情報科学研究科 教授 福田 晃 博士に深甚なる謝意を表する．

本研究を遂行するにあたり，折りにふれ懇切丁寧なるご指導と御厚意溢れるご支援を賜った奈良先端科学技術大学院大学 情報科学研究科 助教授 山口 英 博士に心より御礼申し上げる．

本研究の途上，熱心な御討論と有益な御助言を頂いた奈良先端科学技術大学院大学 情報科学研究科 情報ネットワーク講座の皆様，ならびに，岡山県高度情報化実験推進協議会 インターネットワーキングコンソーシアムの皆様，サイバー関西プロジェクトの皆様，WIDE プロジェクトの皆様に心より感謝申し上げる．

本研究において，STAR については，日本電信電話株式会社 マルチメディアネットワーク研究所の鍛冶武志氏が，奈良先端科学技術大学院大学 博士前期過程在学中に実装したもので，筆者の研究指導のもとに行った研究の成果である．地域ネットワークの実現の中で，鍛冶氏の貢献は多大なもので，ここに感謝の意を表する．

また，奈良先端科学技術大学院大学への社会人留学を許可頂き，経済的な支援と研究環境を与えて頂いた，学校法人 加計学園 倉敷芸術科学大学 加計 勉 理事長と産業科学技術学部 一村 稔 学部長に厚く御礼申し上げる．

最後に，私が大学院において研究するにあたり，並々ならぬ理解と支援を頂き，また，温かく見守ってくれた私の家族，妻 良子，娘 由衣 に深く感謝の意を表する．

参考文献

[1] 郵政省: 平成 11 年版 通信白書, 1999.

[2] R. Droms: Dynamic Host Configuration Protocol, RFC 2131, Mar 1997.

[3] R. Drams S. Alexander: DHCP Options and BOOTP Vendor Extensions, RFC 2132, Mar 1997.

[4] WorldAxle ホームページ, http://www.worldaxle.com/, 1999.

[5] JPNIC ホームページ/RFC, ftp://ftp.nic.ad.jp/rfc/rfc-index.txt/, 1999.

[6] R.Hinden. S. Deering: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, Dec 1998.

[7] Y. Rekhter, B. Moskowitz, D. Karrenberg, and G. de Groot: Address Allocation for Private Internets, RFC 1597, March 1994.

[8] P. Francis and K. Egevang: The IP Network Address Translator (Nat), RFC 1631, May 1994.

[9] C. Perkins: IP Mobility Support, RFC 2002, Oct 1996.

[10] S. Glass C. Perkins: Mobile-IPv4 Configuration Option for PPP IPCP, RFC 2290, Feb 1998.

[11] Fumio Teraoka and Mario Tokoro: Host Migration in Virtual Internet Protocol, In *Proceedings of Inet'92*, June 1992.

[12] K. Uehara, F. Teraoka, H. Sunahara, and J. Murai: Enhacement of VIP and Its Evaluation, In *Proceedings of Inet'93*, August 1993.

[13] WIDE Project: 移動ノード, 1992 年度 WIDE プロジェクト研究報告書, 1993.

[14] ジェイムズソロモン: 詳細 MobileIP, プレンティスホール出版, 1998.

[15] Fumio Teraoka, Yasuhiko Yokote, and Mario Tokoro: A Network Architecture Providing Host Migration Transparency, In *Proceedings of ACM SIGCOMM 91*, September 1991.

[16] R. Droms: Dynamic Host Configuration Protocol, RFC 1541(Obsoleted by RFC1541), October 1993.

[17] 富永明宏, 寺岡文男, 村井純: 動的ホスト設定プロトコル (DHCP) の実装と評価, 情報処理学会マルチメディア通信と分散処理ワークショップ論文集, November 1993.

[18] WIDE Project: 移動計算機の支援, 1993 年度 WIDE プロジェクト研究報告書, 1994.

[19] アルトサロマー: 公開鍵暗号系, 東京電気大学出版, 1992.

[20] R. L. Rivest, A. Shamir, and L. Adleman: A method of obtaining digital signatures and public-key cryptosystems, In *Communication of ACM,Vol21, No.2*, Feburary 1978.

[21] 笠原 正雄辻井 重男: 暗号と情報セキュリティ, 昭晃堂, 1990.

[22] 松井甲子雄: コンピュータのための暗号組立法入門, 森北出版株式会社, 1986.

[23] 小山 謙二池野 信一: 現代暗号理論, 電子通信学会, 1986.

[24] R. Rivest: The MD5 Message-Digest Algorithm, RFC 1321, April 1992.

[25] C Hedrick: Routing Information Protocol, RFC 1058, June 1988.

[26] G Malkin: RIP Version 2 Carrying Additional Information, RFC 1723, November 1994.

[27] J Moy: OSPF Version 2, RFC 1583, March 1994.

[28] Y Rekhter and T Li: A Border Gateway Protocol 4 (BGP-4), RFC 1771, March 1995.

[29] WIDE プロジェクトホームページ: http://www.wide.ad.jp/, 1999.

[30] NSPIXP ホームページ: http://xroads.sfc.wide.ad.jp/nspixp, 1998.

[31] B. Croft and J. Gilmore: Bootstrap Protocol(BOOTP), RFC 951, September 1985.

[32] WIDE プロジェクト ROOT CA ホームページ : http://www.wide.ad.jp/wg/moca/wide_root_ca.html, 1999.

[33] 日本ベリサインホームページ: http://www.verisign.co.jp/, 1999.

[34] R. Droms: Internet Draft — Authentication for DHCP Message, February 1996.

[35] R. Canetti. H. Krawczyk, M.Bellare: HMAC: Keyed-Hashing for Message Authentication, RFC 2104, Feb 1997.

[36] R Atkinson: Security Architecture for the Internet Protocol, RFC 1825, August 1995.

[37] R Atkinson: IP Authentication Header, RFC 1826, August 1995.

[38] R Atkinson: IP Encapsulation Security Payload (ESP), RFC 1827, August 1995.

[39] 中川郁夫, 米田政明, 安宅彰隆: 国内における地域 ix の動向, 情報処理学会 分散システム運用技術研究報告, 1997.

[40] 岡山県ホームページ: /http://www.pref.okayama.jp/kikaku/joho/, 1999.

[41] 岡山情報ハイウェイホームページ: /http://www.okix.ad.jp, 1999.

[42] 今野幸典, 桶地正浩: プライベートなインターネットエクスチェンジを実現する経路制御手法の提案, 情報処理学会 分散システム運用技術研究報告, 1997.

[43] Netperf ホームページ : http://www.cup.hp.com/netperf/netperfpage.html, 1998.

[44] 郵政省郵政研究所: 調-98-vi-03 地域におけるインターネットの活用に関する研究調査報告書, 1998.

[45] 岡山県企画振興部: ～そこが知りたい～ 岡山情報ハイウェイ Q＆A, 1999.

[46] K. Kobayashi, K. Shinmen, S. Yamaguchi, and J. Murai: Construction of Okayama Information Highway, In *Proceedings of Inet'99 SanJose*, June 1999.

研究業績

論文

1. Kazumasa Kobayashi，Suguru Yamaguchi：“Access Control for DHCP Environment”，IEICE Transaction on Communications，E81–B，No. 9，pp. 1718–1723，September 1998.
2. 小林 和真：“岡山情報ハイウェイの構築 — 自治体主導による光ファイバー網の敷設と地域の活性化 —”，情報処理学会 学会誌，41 巻 1 号，January 2000.

国際会議

1. Kazumasa Kobayashi，Suguru Yamaguchi：“Access Control for DHCP Environment”，In proceedings of INET’97 Kuala Lumpur，June 1997.
2. Kazumasa Kobayashi，Kunio Shinmen，Suguru Yamaguchi，Jun Murai：“Construction of Okayama information highway”，In proceedings of INET’99 San Jose，June 1999.

研究会発表

1. 小林 和真，山口 英，山本 平一：“移動ホスト認証を考慮した資源割り当て機構の提案”，情報処理学会 マルチメディア通信と分散処理研究会研究報告，95–DPS–7 71–12， pp. 67–72 ， July 1995.

2. 小林 和真，山口 英，山本 平一：“移動ホスト認証可能な動的資源割り当て機構の提案”，情報処理学会 プログラムシンポジウム「モーバイル&ユービキタスコンピューティング」報告書，S-MBL95，July 1995.

3. 小林 和真，山口 英：“DHCP 環境におけるアクセス制御についての考察”，情報処理学会 マルチメディア通信と分散処理研究会研究報告，96–DPS–9 78–9， pp. 49–54，September 1996.

4. 小林 和真：“モーバイルコンピューティングとネットワークプロトコル”，電子情報通信学会 第 9 回情報伝送と信号処理ワークショップ，November 1996.

5. 小林 和真：“岡山県における情報ネットワーク化の取り組み”，電子情報通信学会 第 3 回コミュニティネットワークシンポジウム，CNJ97，November 1997.

6. 小林 和真：“地域ネットワークの新しい展開”，情報処理学会「分散システム/インターネット運用技術シンポジウム’99」，S–DSM99， February 1999.

7. 小林 和真：“岡山情報ハイウェイにおけるテストベッド構築”，情報処理学会 第 4 回高品質インターネット研究グループ研究会 「わが国の次世代インターネットと高速ルータ開発に関するシンポジウム」，S–HQI99， October 1999.

国内会議 (査読あり，共著)

1. 阿部 哲士，村山 公保，小林 和真：“汎用ルータ設定ソフトウェア CiShell の開発”，情報処理学会「マルチメディア，分散，協調とモーバイル (DICOMO’99) シンポジウム」，S–DICOMO99，pp. 453–458，June 1999.

研究会発表 (共著)

1. 田中 顕彦，小林 和真，山口 英：“広域ネットワークにおける動画像の配送に関する考察”，情報処理学会 マルチメディア通信と分散処理研究会研究報告，96–DPS–9 78–2， pp. 7–12，September 1996.

2. 南方 伸哉，小林 和真，梅比良 正弘，山本 平一：“ワイヤレス ATM による移動通信環境に関する考察”，情報処理学会 マルチメディア通信と分散処理研究会研究報告，96–DPS-9 78–12， pp. 67–72，September 1996.
3. 新本 真史，小林 和真，梅比良 正弘，山本 平一：“ATM インターネットにおけるプラグアンドプレイ環境の構築”，情報処理学会 マルチメディア通信と分散処理研究会研究報告，97–DPS–7 2–6， pp. 31–36，July 1997.
4. 藤田 謙，小林 和真，山口 英：“VIP による IP ローミングの実現手法”，情報処理学会 モーバイルコンピューティング研究会研究報告，97–MBL–7 2–8，pp. 43–48，July 1997.
5. 竹永 吉伸，小林 和真，山口 英，尾家 祐二：“ATM ネットワーク網における動的な帯域割り当てシステムの提案”，情報処理学会 分散システム運用技術研究会研究報告，97–DSM–10 7–4， pp. 19–24，October 1997.
6. 森島 直人，小林 和真，山口 英，尾家 祐二：“自律系における経路情報の監視方法の提案”，情報処理学会 マルチメディア通信と分散処理研究会研究報告，97–DPS–11 85–28， pp. 159–164，November 1997.
7. 鍛冶 武志，小林 和真，山口 英，尾家 祐二：“ソース IP アドレスを考慮した経路制御システムの提案〜地域 IX における経路制御問題の解決〜”，情報処理学会 分散システム運用技術研究会研究報告，97–DSM–11 8–2， pp. 7–12，November 1997.
8. 中村 克之，小林 和真，山口 英，尾家 祐二：“動画像伝送環境 (VINE) の提案および評価”，電子情報通信学会 信学技報，IE97–94，pp. 25–30，November 1997.
9. 上山 晴久，小林 和真，山口 英：“DHCP におけるメッセージ認証機能の実装と評価”，情報処理学会 モーバイルコンピューティング研究会研究報告，97–MBL–11 3–2， pp. 7–12，December 1997.

その他の研究活動

1. “地域におけるインターネットの活用に関する研究調査報告書”，郵政省 郵政研究所，調–98–VI–03，pp. 44–61，June 1998.

2. “インターネットワーキング技術 実験事業報告”，岡山県高度情報化実験推進協議会 岡山県光度情報化モデル実験事業報告書，pp. 17–26，March 1999.

公共ネットワーク構築等

1. “APEC’95 OSAKA Internet”，November 1995.
2. “Internet 1996 World Exposition”，January 1996 – December 1996.
3. “サイバー関西ネットワーク”，July 1996 – 継続中.
4. “UNFCCC COP3”，December 1997.
5. “UNFCCC COP4”，December 1998.
6. “岡山情報ハイウェイ”，November 1997. – 継続中.