公衆無線インターネットプロジェクト「みあこネット」の運用技術

古村 隆明†, 大平 健司‡, 藤川 賢治‡, 岡部 寿男‡
†(財) 京都高度技術研究所 ‡京都大学

我々は，平成14年5月から，京都を中心とした公衆無線インターネット接続実験「みあこネット」を展開している．みあこネットでは，無線インターネットアクセスにおける固定IPアドレス付与と高いレベルのセキュリティの提供を特徴としている．みあこネットは，NPOを中心とするボランティアベースの実験プロジェクトであるが，比較的大規模かつ長期のものであるため，運用コストを削減することがプロジェクトを継続し発展させていくための鍵となる．そのため，プロジェクト開始約1年後に，「みあこネット2」と呼ぶ新しいクライアント接続方式や基地局の接続方式を導入する大きな改革を行った．本稿では，初期のみあこネットを運用していく上で発生した問題，その解決としての第二段階である「みあこネット2」，さらに現在開発中の「みあこネット3」の設計について述べる．

Management Technologies of the MIAKO.NET Public Wireless Internet Service

KOMURA TAKAAKI† KENJI OHIRA‡ FUJIKAWA KENJI‡ AND OKABE YASUO‡
†ASTEM RI, ‡KYOTO UNIVERSITY

We have been serving a public wireless Internet access MIAKO.NET in Kyoto based on IEEE802.11b wireless LAN technology. MIAKO.NET provides mobile Internet access with a fixed IP address and high-level security. MIAKO.NET is a volunteer-based experimental project managed by a non-profit organization, but the scale is larger and the period is longer than many other experiments. Thus minimization of the management cost is the key issue so as to develop the project sustainably. After one-year experience, we newly introduce technologies called "MIAKO2" for authentication and authorization of clients and for up-link connection of access routers. In this paper, we describes the problems occured in the first year, the MIAKO2 second-phase technologies as the solution of the problems, and the conceptual design of the next phase "MIAKO3."

1. はじめに

我々は，京都を中心とし，IEEE802.11b無線LANを利用した，公衆無線インターネット接続実験を行っている．本実験名は，みあこ (Mobile Internet Access in KyotO: MIAKO) ネット[1]と称し，特定非営利活動法人 日本サスティナブル・コミュニティ・センター (SCCJ)[2]のプロジェクトの一つとして運営され，それに京都大学と (財) 京都高度技術研究所が協力する形で進められている．

みあこネットの第一期は，通信・放送機構 (TAO) の平成13年度成果展開等研究開発事業 (委託型) としてとして採択された「モバイルネットワーク基盤システムの研究開発」[3]において，「IPv6無線インターネット接続実証実験」[4]のために整備されたインフラを用い，平成14年5月にスタートした．

初年度は，モバイルインターネットサービス (MIS) 社が平成14年4月に商用サービスを開始したGenuineサービス[5]と全く同じMISP[6]およびMIS MobileIP[7]を用いる方式 (以下，Genuine方式) を，クライアントの接続方式に採用した．Genuine方式は，我々も開発に加わったもので，強固なセキュリティを特徴とするが，残念ながら，現時点での普及型サービスとしては課題も多かった．そこで，Genuine方式は存続させつつ，Virtual Private Network (VPN) の一つであるMicrosoft PPTP (Point-to-Point Tunneling Protocol)[8]を用いる方式 (以下，PPTP方式) を新たに導入し，平成15年3月にサービスメニューに追加した．

また，平成14年度には平成14年度経済産業省e!プロジェクト (ITショーケース事業) 京都地区「地域情報基盤におけるコンテンツ配信とピアツーピア環境の構築」[9]とも連携し，基地局数を従来の100局余りから大幅に増やす機会を得たが，1基地局あたりの設置コストを最小化するために，無線基地局にIP over TCPトンネリング機能などを内蔵し，予め必要な設定を行って出荷することで，インターネットに接続できる環境ならどこでも基地局を接続するだけで設置が完了する接続方式とした．

以上のクライアント接続方式および基地局の接続方式を，みあこネット第二期として「みあこネット２」と呼んでいる．さらにその発展形として，VPN サーバを，だれもが自由に設置し自律分散的に運用できる次世代の方式「みあこネット３」を提唱し，設計開発を行っている．

以下本稿では，２章でみあこネットの設計目標について述べる．３章で初期の「みあこネット」における問題点を挙げ，４章でそれらの問題を解決した「みあこネット２」について述べる．５章では，自律分散型の公衆無線インターネットインフラの考え方「みあこネット３」について述べる．

2. みあこネットの設計目標

みあこネットは，IEEE802.11b 無線 LAN 技術を用いた無線インターネットアクセスを，高いレベルのセキュリティで提供する，という基本方針のもと，実証実験を行っている．

なお，ネットワーク運用は，京都市の研究機関である (財) 京都高度技術研究所 (ASTEM) で行っており，各種サーバは ASTEM に置かれている．

2.1 グローバル固定 IP アドレスの提供

我々は，真のインターネットアクセスの提供とは，単にインターネット上のホストへの通信ができる環境ではなく，端末にグローバル IP アドレスを与えて，NAT などの介在物なく，インターネット上のホストとの通信が自由に行える環境を提供することと定義し，実践している．これは来たるべき IPv6 の時代を見越してのことである．このため，IPv6 普及・高度化推進協議会による「大規模 IPv4 アドレス空間実験」[10] により/16 のアドレス空間の割り当てを受け，すべての基地局および無線クライアントにグローバルの IPv4 および IPv6 アドレスを割り当てている．

さらに，移動していても常に同一固定のグローバル IP アドレスを提供することを目標とする．これにより，無線端末をサーバとして機能させたり，インターネット電話で IP アドレスを電話番号として用いることが簡単にできる．今日の多くのブロードバンド接続サービスが，ダイヤルアップ IP 接続時代の名残で，常時接続においてもグローバル IP アドレスが固定でないのに対し，我々は，移動環境でもグローバル固定 IP アドレスが使えるようにすることで，新しい時代のアプリケーションの設計の土台を提供しようとしている．

みあこネットの初期段階 (以下，「みあこネット１」と呼ぶ) では，無線端末が移動して接続する無線基地局が切り替わった場合でも固定の IP アドレスが使えるようにする技術として，MobileIP[11] を利用していた．MobileIP 本来の仕様は範囲が広いため，無線インターネット環境に最適化した MIS 版 MobileIP を採用している．MIS 版 MobileIP の詳細は 7)，12) を参照されたい．

2.2 高いレベルのセキュリティ機能の提供

無線は，有線と違い，盗聴やなりすましが容易であるため，有線よりも高いレベルのセキュリティ機構が必要となる．具体的には以下の４つの観点からセキュリティ対策を行う必要がある．

(1) 利用者の観点
- (1-a) 無線区間での盗聴や乗取を避けられる
- (1-b) 偽基地局に接続させられない

(2) 基地局運用者の観点
- (2-a) 課金のための利用記録が採取できる
- (2-b) すべての通信で発信者を特定できる

(1-a) は，通常の無線 LAN のセキュリティでも考慮されている点である．だが残念ながらいわゆる無線ホットスポットサービスのほとんどで，最低限の暗号化すら行われておらず，MAC アドレスや ESS-ID による識別のみに依っている[13]．また WEP (wired equivalent privacy) による暗号化を行っている場合でも，多くはそのキーがすべての利用者に共通であるため，他の利用者による攻撃を避け得ない．

(1-b) は，(1-a) 以上に深刻な問題を引き起こし得るが，現在の無線ホットスポットサービスのほとんどで考慮されていない．各アプリケーションは SSL を用いることで偽サーバに接続させるいわゆる man-in-the-middle attack を避けることができるが，実運用では，たとえば一般ユーザの多くが Web ブラウザが SSL モードで動作しているかどうかを意識していないという問題があり，効果は限定的である．

(2-a) は，課金を行う商用サービスの事業者においては必須の機能である．しかし，課金のみが目的であれば，認証をそれほど厳格に行う必要は実はあまりない．

しかし，(2-b) の発信者特定責任の問題を考えると，無料の事業であっても利用者を特定することが必要である．これは，無線基地局を介した不正アクセス，ウイルス発信，あるいは掲示板への書き込みによる名誉棄損，著作権上問題のあるコンテンツの配信，さらには脅迫や身の代金要求など犯罪への悪用などがあった際に，プロバイダ責任制限法などより，サービスの提供者として発信者特定の責任が伴うと考えられるからである．

MIS 社の Genuine サービスおよび我々のみあこネット１では，MISP 方式と呼ぶ，無線端末と無線基地局間の高速認証プロトコルを設計し実装したもの[14] を採用した．MISP 方式は DHCP のように IP アドレスを付与する機能も兼ね備えている．このアドレスは，MobileIP の気付けアドレスとして利用される．MISP 方式の詳細については 6)，15) を参照されたい．

3. 「みあこネット１」の課題

本章では，平成 14 年 5 月から実験を開始した「みあこネット１」での運用上の課題について述べる．なお，みあこネット１のネットワーク構成に関しては 18) に詳しい．

3.1 Genuine方式

「みあこネット1」では，MISP方式によるクライアントの認証とMIS MobileIPによる固定IPアドレスの付与がクライアントからの接続方式の基本であった☆．これは，モバイルインターネットサービス(MIS)社による商用サービスであるGenuineサービスと互換性を持ち，ローミングにより，Genuineサービスの利用者が特別な設定なくみあこネットの基地局を利用できるようになっていた．

しかし，1年弱の運用において，Genuine方式には以下の制限や問題点が顕在化した．

- 無線LANカードや対応プラットフォームの制約
  Genuine方式は，IEEE802.11bに基づく無線LAN技術を用いるが，通常用いられるインフラストラクチャモードではなく，ネイティブアドホックモードと呼ばれるモードを用いる．このため専用のデバイスドライバが必要であり，対応するオペレーティングシステムや無線LANカードが限定されていた．
- 専用ドライバの組み込みの困難
  専用ドライバの組み込みは，初心者には必ずしも容易ではなかった．設定を間違えても，どこがおかしいのかすぐにわかるようにはなっていなかった．また，通常の無線LANとしての利用との切替えが簡単にできるるようにはなっていなかったことも問題であった．さらに，ドライバのアンインストール時に不具合が起き，OSのクリーンインストールを余儀なくされる事態も発生した．

MISPおよびMIS Mobile方式は，基地局間の高速ハンドオーバを特徴としているが，残念ながら平成14年時点では移動しながら使えるサービスエリアはごく限られていた．また，PDA用のドライバの開発が遅れた結果，ドライバの対応がノートPC用のみであったものの，ノートPCのを歩きながら使うというのは現実的でなく，せっかくの高速ハンドオーバ性能もそれを生かす機会がほとんどないというのが実状であった．

さらに，MIS社が平成14年12月にGenuine方式の商用サービスの休止を発表するに至り，ドライバなどの基本ソフトウェアをMIS社に依存しているみあこネットの体制の脆弱性が見えてきた．そこで，MIS社の独自方式であるGenuine方式は残しつつ，オープンかつ普及しているVPN技術であるPPTPを採用することになった．詳細は4.1節で述べる．

3.2 無線基地局(RGW)の設置

ASTEMはNTT西日本(株)社が提供する地域IP網と接続しており，インターネットの上流回線を提供できる．初年度は，地域IP網とのPPPoEによる接続のためにRGWとは別にブロードバンドルータを配置し現地に要員を派遣して設定を行っていたため，設置コストが高くなっていた．

また，基地局はクライアントに付与するグローバルIPアドレスが必要であったために，PPPoEでネットワーク型接続をして必要なグローバルアドレスを割り当てていた．しかしこのために，基地局を設置する場所に，必ずNTTのアクセス回線を引かなければならないという制約があった．既に別のインターネットアクセス回線を持っている場所に基地局を設置するような場合には，余分な投資を強いられる結果となった．

初年度の約100の基地局に加え，第二年度でさらに200以上の基地局を増やすことになったが，初年度と異なり基地局の設置と設定に伴う作業はみあこネットプロジェクト側の負担となった．そのため，機器設置にかけるコストを最小限にする必要があった．

これらの問題の解決について，詳しくは4.2節で述べる．

4. みあこネット2

本章では，「みあこネット2」について，前章で説明した問題点をどのよう解決しているか，また，「みあこネット2」で新たに採用した技術について述べる．図1は「みあこネット2」のネットワーク構成とトンネルを用いた接続形態を示している．

無線基地局はNTT地域IP網経由，もしくはインターネットを介したトンネル技術を用いて接続される．IPアドレスとしては，IPv6普及・高度化推進協議会から時限で割り当てを受けた43.245/16の空間を用いている．

4.1 PPTP方式によるクライアント接続

3.1節で述べた問題を解決するため，独自仕様であったGenuine方式は残しつつ，オープンで普及しているVPN技術であるPPTPを用いた新たな方式を採用した．PPTPを選択した理由は，Windowsをはじめとする多くのOSでサポートされており，特殊なドライバをインストールすることなく利用でき，設定の難易度も高くないためである．

PPTP方式では，クライアント端末は，通常のIEEE802.11bにおいて所定のESSID(通常は「MIAKO」)を用いWEPによる暗号化がされない状態でまずDHCPでIPアドレスを取得する．ここで取得するIPアドレスは，みあこCAN (Community Area Network)と呼ぶ，外部への接続が制限されたネットワークのグローバルIPアドレスであり，基地局毎に異なるものである．クライアントは，ここでさらにみあこCAN内にあるPPTPサーバに接続することで，インターネットへ自由に接続できるようになる．

Genuine方式ではMIS Mobile IPによりクライアントに固定IPアドレスを付与していた．PPTP方式でも同様のことを実現するために，PPTPサーバに設定を追加し，同一アカウントに対しては常に同じIPアドレスを割り当てるようにした．但し，Genuine方式ではMobile IPにより基地局間のハンドオーバが行えたのと異なり，基地局を移動するとPPTPのセッションが切れるため再接続が必要となる．

利用者の観点からのセキュリティレベルは，PPTPが採用す

☆ この他に，IPv6によるさまざまな接続方式の検証を実験的に行っていた．

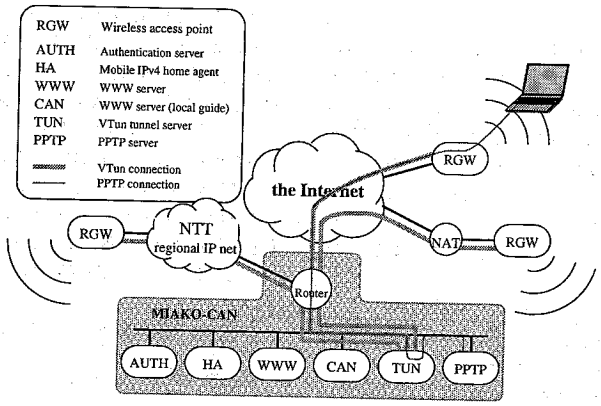

図1 みあこネット2のネットワークと接続形態

る MS-CHAP に依存する．最新版の MS-CHAP ver.2 では，暗号化は，PPTP サーバとクライアント間で行われ，暗号化のキーはセッション毎にかつ送信と受信で異なるものが用いられる．サーバとクライアントとの間では相互認証が行われるため，万一 IP アドレスの擬装や DNS の乗っ取りにより偽 PPTP サーバに接続させられたとしても，認証の段階でクライアントが自動的に接続を拒否する．

4.2 RGW の設置と設定

3.2 節で述べた，RGW の設置等のコストを削減するために採用した方法について述べる．

「みあこネット2」の PPTP 方式を提供する無線基地局は，通常の DHCP サービス機能を有しグローバル IP を付与できること，外部へのアクセスを IP アドレス，IP プロトコル番号および TCP・UDP のポート番号で制限できることができるものであれば，どのようなものでもよい．我々は，Genuine 方式と並行運用させるため，みあこネット1と同様にルート社製の RGW2400 シリーズ (以下，RGW) を採用している☆．

RGW は，単純なブリッジではなく，NetBSD 1.5.2 をベースとした OS が搭載された高機能ルータとして動作する．みあこネットはパートナー契約により OS を含む全てのソフトウェアのソースコードの提供を受けていることで，MISP 方式による高レベルのセキュリティや，MISP 方式と PPTP 方式の併用，以下に説明する PPPoE や VTun による上流回線との接続など様々な機能が実現できている．

「みあこネット2」では基地局の設置や設定に共なう作業はみあこネットプロジェクトの負担となったため，コストのかかる屋外型アンテナの設置は原則見送り，無線基地局である RGW に PPPoE クライアントや IP over TCP トンネリング機能などを内蔵させることでハードウェアコストを最小限にするとともに，予め必要な設定を行った上で「基地局オーナ」と呼ぶ協力者のところへ郵送等で出荷し，初心者でも既設のネットワークに基地局を接続するだけで設置が完了し，以後の設定変更やバージョンアップは ASTEM からリモートで行えるようにして，メンテナンスコストを圧縮した．

基地局の設定を自動的に行うプログラムも開発し，設定コストを最小化した．

4.2.1 PPPoE による上流回線との接続

ブロードバンドルータを介することなく NTT 西日本の地域 IP 網と接続できるようにするため，PPPoE (PPP over Ethernet) クライアントを組み込んだ RGW を開発した．予め必要な設定を組み込んで出荷することで，RGW を NTT 西日本の地域 IP 網に接続するだけで ASTEM を介してインターネット接続させることを可能にしている．現在，NTT 西日本のフレッツシリーズによるブロードバンドサービスの多くのメニューで月額追加料金なしに2セッションの利用が可能となっており，既設のインターネット接続のための契約に相乗りする形での接続が追加のランニングコストなしで可能であるというメリットがある．

4.2.2 VTun による上流回線との接続

既に，NTT 西日本のフレッツ以外のブロードバンドサービスでインターネット接続されている地点で，上流回線として既設の接続を流用する形で RGW を設置し，簡単にみあこネットに参加できるように，VTun[19] クライアントを組み込んだ RGW を開発した．VTun とは，IP over TCP/IP によるトンネル実装の一つである．単純な IP in IP 技術では，NAT ルータ (正確には NAPT ルータ) の内側からトンネルをはることは通常できないため，IP over TCP/IP を利用することとした．これにより NAT ルータを導入している場合でも，RGW をその配下の設置し，RGW 配下ではグローバルの IP アドレスが

☆ アドホックモードとインフラストラクチャモードを同時並行運用するため，プロミスキャスモードを用いた特別なファームウェアで動作させている．この実装は九州大学の大森幹之氏による

利用できるようになる．

4.3 PPTP サーバ

PPTP サーバは，Linux や FreeBSD 上で，オープンソースの PPTP サーバ実装である PoPToP[20] を用い，アカウント毎に固定 IP アドレスの付与する設定をしている．さらに，同一アカウントによる重複ログインに対して，重複ログインを排除する通常の設定に代えて，古いセッションを強制的に終了させた後，新しいセッションを受け付けるようなスクリプト処理を追加している．これは，クライアントの移動などにより，クライアント側は PPTP セッションが切断したと認識しているがサーバ側にはセッションが残っている場合，クライアントが再接続を試みると，サーバ側では重複ログインが起きたと判断されるためである．

4.4 みあこ CAN

みあこネット２のネットワークでは Community Area Network (CAN) と呼ばれる仕組を提供した．CAN とは，ある地域の内にのみ情報発信を行うことを目的としたネットワークである[16]．我々は，CAN の考え方にならって，PPTP に接続しない状態で端末がアクセスできる範囲のネットワークを，みあこネットの無線基地局のエリア内にのみ情報発信を行うネットワークとしても位置付け，みあこ CAN と名付けている．

みあこ CAN では，コンテンツとして，みあこネットへの接続方法等を説明した Web ページを提供している．Web サーバの提供は，みあこネット１で，設定に不備があった場合にシステム側から提供される情報が少なく，結果としてユーザサポートのコストが大きくなったことの反省として導入された．PPTP による認証を経ていない無線端末からみあこ CAN 外へ HTTP 接続が試みられた場合は，みあこ CAN 内部の L4 スイッチ機能によって強制的に CAN 用 WWW サーバにリクエストを転送する．CAN 用 WWW サーバでは delegate[17] によるサーバが動作しており，利用者が要求してきた URL を書換えて CAN 用のコンテンツを表示し，PPTP の接続がされていないことの警告や PPTP 方式による接続手順を示すようにしている．この他，基地局ごとの位置依存コンテンツも提供できるようにしており，セキュリティ上問題のない範囲で，認証なしにすべての来訪者に情報提供を可能としている．

5. 「みあこネット３」構想

みあこネット２では，ユーザや基地局設置者の負担を少なくした分，みあこネットの管理する中央のサーバ部分にトラフィックや運用コストが集中する．また，セキュリティを重視しユーザ一人一人に無料でアカウントの発行を行っているため，アカウント発行事務のコストも無視できない．したがってこのままのアーキテクチャで基地局数やユーザ数をスケーラブルに増やすことは不可能である．その一方で，すでにみあこネットの活動は京都から松山，沖縄など全国へ広がりはじめており，リモート運用の難しさの問題も表面化してきている．そこで，次世代の技術として，無線基地局と VPN サーバをそれぞれだれもが自由に設置し自律分散的に運用できる方式「みあこネット３」を提唱し，設計開発を行っている (図 2)．

みあこネット３では，まず，現在みあこネットがサービスしている VPN サーバの機能を分散することを目指す．そのために，みあこネット２ではみあこ CAN 内に制限していた PPTP サーバへの接続を，インターネット全体に拡大するとともに，対象とするプロトコルとして PPTP に加え L2TP + IPsec や CheckPoint 方式，Cisco 方式，および SSH (Secure Shell) などを追加している．これにより，アカウント発行事務やプロバイダ責任制限法上の発信者特定責任のコストを，VPN サーバの運用者に移すことができる．すでにいくつかの企業において，社員用に VPN サーバを運用し，みあこネットを利用して社内 LAN に直接 VPN 接続することを行っている．しかし我々は，各家庭のブロードバンドルータに VPN サーバの機能を持たせることで，ホームネットワークに外出先から安全にアクセスする応用こそ今後重要になると考えており，そのための個人レベルで運用可能な VPN サーバについていくつかの製品を評価中である．

無線基地局については，前述のように，通常の DHCP サービス機能を有しグローバル IP を付与できることと外部へのアクセスを IP アドレス，IP プロトコル番号および TCP・UDP のポート番号で制限できることができるという条件の下では，上述のような指定の VPN プロトコルのみ対外接続を許す設定をすることで，だれでもみあこネットと同等の無線基地局を運用できる．すでに，みあこネット側でもこのような形での基地局の広がりを想定し，みあこネット基地局以外からのみあこネット PPTP サーバへの接続を一定の条件の下に限定的に許可している．しかし，現段階では，公衆無線インターネット接続サービス用にグローバル IP アドレスを必要数確保することが極めて高コストである．代替案として，VPN マルチパススルー機能をもつ NAT ルータの利用や，PPP over SSH のような NAT を通過できる VPN プロトコルの採用，あるいは 6to4 による IPv6 over IPv4 tunneling にさらに IPv4 over IPv6 tunneling を組み合わせた方式などを種々評価しているところである．

6. おわりに

本稿では，京都を中心に展開している，公衆無線インターネットプロジェクト「みあこネット」の基本方針と，初年度の反省，第二段階のネットワーク設計，さらに第三段階の構想に関して述べた．みあこネットでは高いレベルのセキュリティと固定 IP アドレスの付与が特徴の公衆無線インターネットアクセスを，ボランティアベースで無償で提供している．そのための運用コストの低減のための技術や，公衆無線インターネット

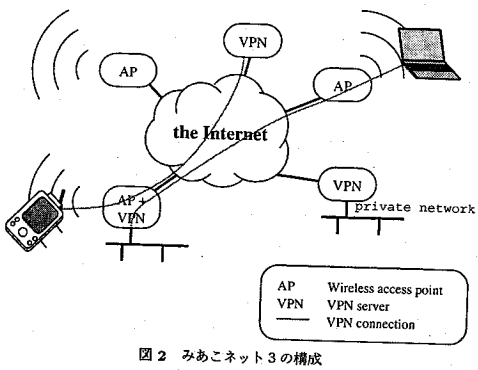

図 2 みあこネット 3 の構成

をスケーラブルに発展させるための構想について，特に詳しく述べた．

本稿では公衆無線インターネットアクセスとしてのインフラ部分を中心に説明を行ったが，みあこネットを活用したアプリケーションの実験も，特徴的なものが開始されてきているところである．例えば ANYCAST に基づく位置依存コンテンツの提供[21]や，Windows CE 機等の PDA を用いたインターネット電話の実験がある[22]．今後はアプリケーションとの連携やアプリケーション側の要請に基づく機能の向上についても検討して行きたい．

謝　辞

みあこネットを実際に運営している高木治夫氏，隅岡 敦史氏をはじめとする SCCJ の各位，ならびにみあこネットをボランティアの立場で支えるすべての方々に感謝する．無線基地局の各種機能を実現した大森幹之氏をはじめとする九州大学，ISIT の各位に深謝する．

参 考 文 献

1) http://www.miako.net/
2) http://www.sccj.com/
3) http://www.shiba.tao.go.jp/kenkyu/seikatenkai/itaku/h130/ichiran.htm
4) http://www.root-hq.com/pressrelease/02.2.18.html
5) http://www.miserv.net/
6) モバイルブロードバンド協会, MIS プロトコル仕様書 Ver. 1.02, MBA 標準草案 0201 号 http://www.mbassoc.org/j-services/mbas0201v102.pdf (April 2002).
7) モバイルブロードバンド協会, MIS モバイル IP 仕様書, MBA 標準草案 0202 号 http://www.mbassoc.org/j-services/mbas0202t.pdf (April 2002).
8) Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and Zorn, G., "Point-to-Point Tunneling Protocol (PPTP)," RFC2637 (July 1999).
9) http://www.astem.or.jp/proj/e-proj/
10) http://web2.v6nic.jp
11) Perkins, C., "IP Mobility Support," RFC2002 (October 1996).
12) 大森 幹之, 太田 昌孝, 平原 正樹, 真野 浩, 荒木 啓二郎, モバイル IPv4 による異なるメディア間でのハンドオーバの実現, DPS ワークショップ (October 2002).
13) 清水渉, 小林稔幸, 無線ホットスポットサービスのセキュリティ, 情報処理学会研究報告 2002-DPS-107 (March 2002).
14) 藤川 賢治, 中野 博樹, 太田 昌孝, 平原 正樹, 真野 浩, 池田 克夫, 無線インターネットサービスに必要なセキュリティを提供する高速認証システム, 情報処理学会研究報告 2001-DPS-107, March 2002.
15) モバイルブロードバンド協会, MISAUTH プロトコル仕様書, MBA 標準草案 0301 号 http://www.mbassoc.org/j-services/mbas0301.pdf (Sep. 2003).
16) http://www.can.or.jp/
17) http://www.delegate.org/
18) 藤川賢治, 古村隆明, 岡部寿男, 京都無線インターネットプロジェクト みあこネットの設計と運営, 情報処理学会研究報告 03-DPS (March 2003).
19) http://vtun.sourceforge.net/
20) http://www.poptop.org/
21) 朝長 康介, エニキャストを用いた位置依存サービス, 情報処理学会研究報告 2001-MBL-20 (March 2001).
22) Takaaki KOMURA, Masakatsu KOSUGA, Kenji FUJIKAWA, Yasuo OKABE, "Desgin and Implementation of the MIAKO.phone Peer-to-peer Mobile IP Phone System," 5th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT2003) (Nov. 2003).