4. 無線LANによる移動体通信の事例

3 無線LANによる公衆無線インターネットサービス みあこネット

MIAKO.NET：Public Wireless Internet Service based on Wireless LAN

古村 隆明[*1]　大平 健司[*2]　藤川 賢治[*3]　岡部 寿男[*4]

[*1]（財）京都高度技術研究所
[*2, 3, 4] 京都大学

[*1] komura@astem.or.jp　[*2] ohira@net.ist.i.kyoto-u.ac.jp
[*3] fujikawa@i.kyoto-u.ac.jp　[*4] okabe@i.kyoto-u.ac.jp

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LAN技術を用いた公衆無線インターネットサービスにおける固定IPアドレスの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2段階である「みあこネット2」の設計について述べる．

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1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かたちで進められている．

みあこネットの第1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]とまったく同じ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1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，あらかじ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2期として「みあこネット2」と呼んでいる．

以下本稿では，まずみあこネットの設計目標を述べる．次に初期の「みあこネット」における問題点を挙げ，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．

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．

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の詳細は文献7），12）を参照されたい．

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っ取りを避けられる
　(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による識別のみによっている[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の気付アドレスとして利用される．MISP方式の詳細については文献6），15）を参照されたい．

「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文献18）に

詳しい．

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[☆1]．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，疑似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分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り替えが簡単にでき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ー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ー性能もそれを活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．詳細は後述する．

無線基地局の設置

ASTEMはNTT西日本が提供する地域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（PPP over Eternet）による接続のために無線基地局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．すで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2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，詳しくは次章で述べる．

みあこネット2

「みあこネット2」について，前述の問題点をどのように解決しているか，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西日本の地域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．

PPTP方式によるクライアント接続

みあこネット1での課題を解決するため，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を始めとする多くの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

☆1 このほかに，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．

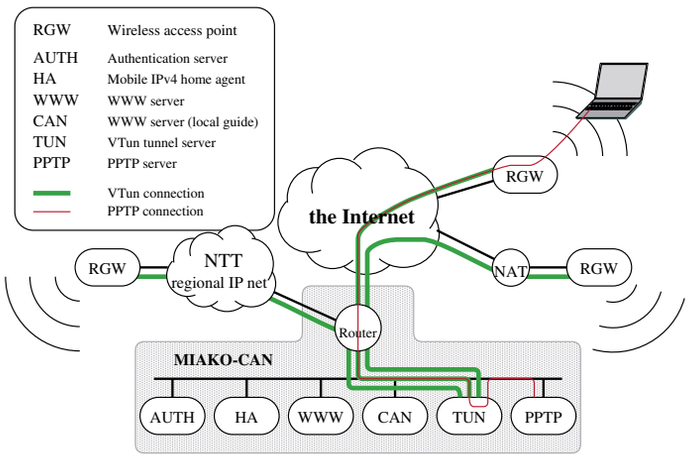

図-1　みあこネット2のネットワークと接続形態

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，基地局ごと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．ただし，Genuine方式ではMobile IPにより基地局間のハンドオーバー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ごと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．

RGWの設置と設定

無線基地局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アドレスを付与できること，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☆2．

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を含むすべ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さまざま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伴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，あらかじ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から遠隔から行えるようにして，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．

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

☆2　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（現，筑紫女学院大学）による．

の地域IP網と接続できるようにするため，PPPoEクライアントを組み込んだRGWを開発した．あらかじ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かたち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．

VTunによる上流回線との接続

すでに，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によるトンネル実装の1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をその配下に設置し，RGW配下ではグローバルのIPアドレスが利用できるようになる．

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，アカウントごとに固定IPアドレスを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．

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2段階のネットワーク設計に関して述べた．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．たとえば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いきたい．

謝辞　みあこネットを運営している高木治夫氏，隅岡敦史氏を始めとする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九州大学の大森幹之氏（現，筑紫女学院大学）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) MISプロトコル仕様書Ver. 1.02, MBA標準0201号，モバイルブロードバンド協会，http://www.mbassoc.org/j-services/mbas0201v102.pdf（Apr. 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0202号，http://www.mbassoc.org/j-services/mbas0202t.pdf（Apr. 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（Oct. 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（Oct. 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（Mar. 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（Mar. 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（Mar. 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（Mar. 2001）．
22) Komura, T., Kosuga, M., Fujikawa, K. and Okabe, Y.：Design 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）．

（平成16年7月1日受付）