マルチメディア通信と分散処理　111－1
コンピュータセキュリティ　20－1
（2003．2．27）

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用

藤川 賢治† 古村 隆明‡ 岡部 寿男†
†京都大学大学院情報学研究科 ††(財) 京都高度技術研究所

我々は京都を中心とし，無線 LAN を利用した無線インターネット接続実験，みあこ (MIAKO) ネットを展開している。みあこネットでは，固定 IP アドレス付与を含む無線インターネットアクセス，高いレベルのセキュリティ，Community Area Network (CAN) へのアクセス，位置依存のコンテンツなどを提供している。本稿ではみあこネットの基本方針及び，ネットワーク設計と運用に関して述べる。

Design and Management of Kyoto Wireless Internet Project MIAKO-Net

FUJIKAWA Kenji† KOMURA Takaaki‡ OKABE Yasuo†
†Kyoto University ‡ASTEM

We are developing wireless Internet access experiment MIAKO-Net based on wireless LANs in Kyoto. MIAKO-Net provides wireless Internet access with fixed IP address assignment, high-level security, access to a Community Area Networks (CAN), and location-dependent contents. This paper describes the basic policy of MIAKO-Net, and design and management of its network.

1. はじめに

我々は京都を中心とし，無線 LAN(IEEE802.11b[1),2)]) を利用した，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[3)] と称し，非営利法人，日本サスティナブル・コミュニティ・センター (SCCJ)[4)] のプロジェクトの一つとして進められている。

みあこネットの最終的な目標は，安価な無線技術を用いて，京都の街中すみずみまで，無線インターネットアクセス環境を提供することである。

実際，複数の無線基地局が電波の切れ目なく配置されているところでは，その範囲内を移動しても，高速なハンドオーバー機能により，接続が切れることなくインターネットに接続することができる。将来的にはこのようなネットワーク基盤上で，格安もしくは無料のインターネット電話など，様々なアプリケーションが提供されることを期待している。

しかし現実に京都市街のすみずみまで設置しようとなると，IEEE802.11b の無線基地局が数千の単位で必要となり，現時点では運営上の問題から対応できない。そこで現在は 200 程度の無線基地局で運営している。この結果残念ながら無線基地局がとびとびに配置され，一般のホットスポット的サービスとそう変わらないものとなってしまっている場所が多いのも事実である。

以下本稿では，2 章でみあこネットの基本方針，3 章でネットワーク構成の設計・運用，4 章でみあこネット環境下で現在行われている実験や今後の展望について述べる。

2. みあこネットの基本方針

みあこネットは次のような機能を提供するという基本方針のもと，インターネット接続実験を行っている。

- 無線 LAN 技術を用いた無線インターネットアクセス機能
- 高いレベルのセキュリティ機能
- Community Area Network (CAN) 機能

以下，それぞれについて説明する。

2.1 無線インターネットアクセスの提供

我々は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，無線端末にグローバル 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ている。

また固定のグローバル IP アドレスの提供も重要であると考えている。固定でアドレスを持てることで，無線端末がサーバとして機能する。またインターネット電話も簡単に実現できる。

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[5)] を利用している。ただし 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 6), 7) 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が必要となる。みあこネットは以下の三つのセキュリティ機能により，高いレベルのセキュリティを提供する。

(1) 無線端末の認証
これにより正規利用者の同定ができ，不正な利用者による使用を排除することができる。

(2) 無線区間の暗号化
これにより無線区間の盗聴を防ぐことができる。

(3) 無線基地局の認証
偽無線基地局への接続を抑止することで，偽のインターネットや偽のサイトに接続させられてしまうことを防ぐことができる。

このため，我々は既に MIS (Mobile Internet Service) 認証方式と呼ぶ，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。MIS 認証方式は 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。MIS 認証方式の詳細については 7), 8) を参照されたい。

三つのセキュリティ機能のうち 2. と 3. の機能は，ネットワーク提供者が提供しなくとも，無線端末自身で自己防衛できる。そこで我々は，2. と 3. よりも 1. の無線端末の認証機能を重視している。この提供を怠ると，不正な利用者からの DOS 攻撃，SPAM やウィルスメールの配布など，インターネット全体に対して甚大な被害を与えうるためである。

なお MIS 認証及び MIS 版 MobileIP を利用するためには，各 OS に専用なドライバのインストールを必要とし，Windows 98/Me/2000/XP，FreeBSD 4.x，NetBSD 1.5.x 用が用意されている。

2.3 CAN の提供

Community Area Network (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。[9] 我々は CAN のための WWW サーバも用意しており，このサーバには，MIS 認証方式により認証されていない利用者もアクセス可能である。

利用者に対してセキュリティを提供しない方式も並存するという問題はあるが，アクセスは CAN 用の WWW サーバへのものに限定されるため，2.2 節で述べたインターネット全体に対してい甚大な被害を与える，ということはく，重大な問題ではないと考えている。

3. ネットワーク設計と運用

本章では詳細なネットワーク設計と運用について述べる。図 1 はネットワーク構成を示している。

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。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，43.245/16 の空間を用いている。

以下，図 1 の各構成要素について説明する。

3.1 無線基地局 (RGW)

無線基地局として，ルート社製の RGW2400 シリーズ (以下 RGW) を利用している。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 が搭載されており，高機能ルータとして機能する。NetBSD OS が搭載されていることで，2.2 節で述べた高レベルのセキュリティ，及び以下に説明する PPPoE や VTun，gif トンネルによる上流回線との接続，など様々な機能が容易に実現できる。

3.1.1 PPPoE による上流回線との接続

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が提供できる。そこで RGW に PPPoE クライアントを組み込むことで，RGW を地域 IP 網及び ASTEM を介してインターネット接続させると共に，RGW からの ASTEM 内への各種サーバへのアクセスを可能にしている。具体的には，RGW は，NTT 西日本 (株) 社が提供するフレッツ ADSL もしくは B フレッツを介してインターネットに接続されることになる。

MIS 認証方式は，各無線端末にグローバル IP アドレスを割り当てられることを期待しているので，各 RGW には PPPoE により /26 の空間 (IP アドレス 32 個) を割り当てることとした。このアドレス空間から無線端末へグローバル IP アドレスが割り当てられ，MobileIP の気付けアドレスとして使用される。

3.1.2 VTun による上流回線との接続

フレッツ ADSL や B フレッツは導入されていないが，既にインターネット接続されている地点からでもみあこネットに参加できるように，VTun[10] クライアントを RGW に組み込んだ。VTun とは，IP over TCP/IP によるトンネル技術の一つである。単純な IP over IP 技術では，NAT 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 アドレスが利用できるようになる。

各 RGW は PPPoE の場合と同じく，VTun により /26 の空間を割り当てられ，MIS 認証方式によって無線端末にその空間の IP アドレスを配布する。

3.1.3 gif トンネルによる IPv6 インターネットとの接続

IPv6 インターネットとの接続は，NetBSD OS に標準で備わっている gif トンネル機能を用いて行われる。gif トンネルは，KAME プロジェクト [11] により開発された機能であり，主に IPv6 over IPv4 トンネルにより，既存の IPv4 網を利用して，ノードを IPv6 インターネットに接続するためのものである。

RGW は，PPPoE もしくは VTun を用いて IPv4 インターネットに接続されたのち，gif トンネルにより IPv6 インターネットにも接続される。

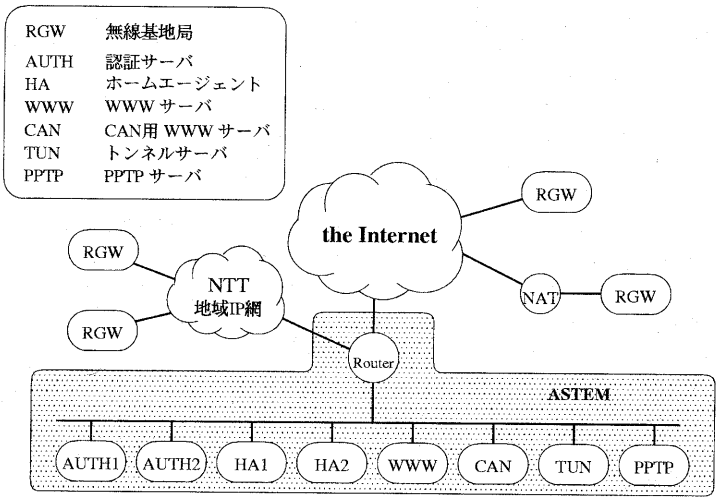

図 1 みあこネットのネットワーク

3.1.4 gif トンネルによる CAN 用 IP アドレスの付与

認証されていない無線端末が CAN 用 WWW サーバに接続することを許し，かつそれからのインターネットへの攻撃を禁止するため，認証されていない無線端末に割り当てられる IP アドレスは PPPoE や VTun で割り当てられるものとは別空間から取ることとした。そのために gif トンネルを利用する。

gif トンネルの一般的な用途は既に述べた通りだが，みあこネットプロジェクトでは IPv4 over IPv4 トンネルを実現するためにも流用している。

既に PPPoE や VTun によりインターネット接続されている RGW で，gif トンネルにより更に別の /26 のアドレス空間を取得し，それを CAN 用の IP アドレスとして DHCP により配布する。無線端末から CAN 用 IP アドレスを取得するには，無線 LAN(IEEE802.11b) の設定で，SSID 指定なし，WEP なし，とし，DHCP クライアントを起動すればよい。

3.2 トンネルサーバ

トンネルサーバは FreeBSD OS が搭載された PC であり，上述の RGW の VTun に対するサーバ，及び gif のトンネルの相手先として機能する。☆

VTun で配布している IP アドレスを送信元とするパケットに対するフィルタは設定されていない。

一方 gif で配布している IP アドレスを送信元とするパケットは，CAN 接続専用の IP アドレスであるので，図 1 のサーバ群への接続に限定するフィルタが設定されている。またポート 80 番に対するアクセスは 図 1 内の CAN 用 WWW サーバに強制的にリダイレクトされるように設定されている。

☆ PPPoE サーバは，みあこネットプロジェクトとは関係なく既設されていたものを使用している。

3.3 認証サーバ

これらは MIS 認証方式の認証サーバであり，冗長性を確保するため 2 台設置されている。機能としては

- RGW からの認証要求の受け付け
- 必要があれば，他の認証サーバへの認証要求の転送

があげられる。

みあこネットは，MIS 社の実験 [12] 及び，福岡での無線インターネット接続実験 Fukuoka Mobile BroadBand (FMBB)[13] と協力しており，認証サーバのプロキシー機能によりそれぞれののユーザがこれらのサービス地域のどこであっても，MIS 認証方式により接続できるようにしている。

3.4 ホームエージェント

これらは MIS 版 MobileIP のホームエージェント，すなわち MobileIP を実現するためのサーバである。現在，2 台設置してあり，それぞれ別のアカウントの管理をしている。

3.5 WWW サーバ

みあこネットの各種情報が提供される WWW サーバである。(トップページは `http://www.miakol.net/`)

また，エニキャスト技術による，位置依存サービスの提供のための WWW サーバとしても利用される。位置依存サービスとは，どの無線基地局配下からでも特定の URL を指定すると，その無線基地局に依存したコンテンツを提供するサービスである。エニキャスト技術に関しては 14) を参照されたい。

みあこネット配下の基地局から `http://koko.miako.net/` を指定すると，接続している無線基地局が置かれている場所に密着したコンテンツが提供される。具体的なコンテンツとして，祇園囃子の情報，地図情報などを用意している。例えば，祇園囃子の情報を取得したければ，その近辺へ実際に出向き，対応する無線基地局の電波を拾い接続し，上記 URL を指定することになる。

3.6 CAN 用 WWW サーバ

CAN 用 WWW サーバは，みあこネットの無線基地局に接続した利用者に対して，CAN 用コンテンツを提供する。CAN 用コンテンツとしては，みあこネットへの接続方法等を説明した WWW ページ，CAN 専用掲示板システム，CAN 専用チャットシステムなどを用意している。利用者は MIS 方式により認証されていても，認証されていなくても構わない。

認証されていない無線端末からの通信でも，CAN 用サーバへのアクセスは制限をかけていないため，CAN 用コンテンツへのアクセスは自由に行える。逆に，一部の CAN 用コンテンツは，みあこネット以外のネットワークからは見えないように設定してある。

認証されていない無線端末からインターネットへ接続が試みられた場合は，トンネルサーバに設定している L4 スイッチ機能によって強制的に CAN 用 WWW サーバにパケットを転送する。CAN 用 WWW サーバでは delegate[15] 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するようにしている。

3.7 PPTP サーバ

2.2 節で述べたように，MIS 認証や MIS 版 MobileIP を利用するには，無線端末に専用のドライバをインストールする必要がある。高レベルのセキュリティを提供する代わりに，一般利用者にとって導入の敷居が高いということが運用を通して明かになった。

そこで Windows マシンにおいて，全くドライバのインストールをせずに，安全にインターネットに接続でき，かつ固定グローバル IP アドレスを提供するため，Point-to-Point Tunneling Protocol (PPTP) サーバを設置することとした。PPTP は Virtual Private Network (VPN) 技術の一つであり，Windows マシンに最初から組み込まれている。

Windows OS の無線端末では，まず DHCP で CAN 用 IP アドレスを取得し，その後 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。PPTP クライアントの設定は必要だが，特別な無線 LAN の設定は必要はない。

この方式の問題点として，MIS 認証方式ほどセキュリティが強固でない部分がある，ハンドオーバーができない，ということがあげられる。

4. おわりに

本稿では，京都の街中を中心に展開している，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，ネットワーク設計，運用に関して述べた。みあこネットでは，各種サーバにより，固定 IP アドレスの付与も含む無線インターネットアクセス，高いレベルのセキュリティ，CAN，位置依存のコンテンツなどを提供している。

現在は PC だけでなく，Windows CE 機等の PDA を用いて，音声による WWW アクセスやインターネット電話の実験を行っている。

今後は PDA 向けのコンテンツの提供や音声サービスの提供に特に注力する予定である。

謝　辞

みあこネットを実際に運営して頂いている隅岡 敦史氏，高木 治夫氏をはじめとする SCCJ の皆様に深く感謝致します。無線基地局の各種機能を実現して頂いた大森 幹之氏をはじめとする九州大学，ISIT の皆様に深く感謝致します。その他，みあこネット実現のために関わって頂いたすべての皆様に深く感謝致します。

参 考 文 献

1) IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE802.11, August 1999.
2) IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer Extention in the 2.4 GHz Band,", IEEE802.11b, September 1999.
3) http://www.miako.net/
4) http://www.sccj.com/
5) Perkins, C., "IP Mobility Support," RFC2002, October 1996.
6) 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.
7) http://www.mbassoc.org/
8) 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.
9) http://www.can.or.jp/
10) http://vtun.sourceforge.net/
11) http://www.kame.net/
12) http://www.miserv.net/
13) http://www.fmbb.org/
14) 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.
15) http://www.delegate.org/
16) Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and Zorn, G., "Point-to-Point Tunneling Protocol (PPTP)," RFC2637, July 1999.