社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＱＡＩ－21（９）
2006／10／24

VPNサーバを分散させた公衆無線インターネットみあこネット３の設計

古村 隆明† 藤川 賢治†† 岡部 寿男†

† 京都大学 〒606-8501 京都市左京区吉田本町
†† ルート株式会社 〒141-0031 東京都品川区西五反田 7-21-11 第 2TOC ビル 8F
E-mail: †{komura,okabe}@media.kyoto-u.ac.jp, ††fujikawa@root-hq.com

あらまし みあこネットは，無線基地局の設置者が費用を負担し，そこを訪れる利用者に無料の無線インターネットを利用してもらうという，「おもてなし」の心をもとにした独特のモデルで成り立っている公衆無線インターネットプロジェクトである．我々は 2002 年 5 月からみあこネットの設計・開発・実験運用を行ない，安全に無線インターネットを利用するために VPN 接続を必須とするネットワーク環境を構築した．本稿では，従来の集中型 VPN サーバを利用する「みあこネット２」方式の問題点を明らかにし，VPN サーバの分散について検討を行なった．そして，基地局に VPN サーバ機能を内蔵するという，「おもてなし」の心でみあこネットを支えている基地局設置者にとっても有益な「みあこネット３」のモデルを提案し，設計を行った．
キーワード 公衆無線インターネット，自立分散 VPN サービス，PPTP サーバ

Design of MIAKO.NET 3: Public Wireless Internet using Distributed VPN Servers

KOMURA TAKAAKI†, FUJIKAWA KENJI††, and OKABE YASUO†

† Kyoto University Yoshida-Honmachi, Sakyo-ku, Kyoto, 600-8501 Japan
†† ROOT INC. 2nd TOC Bldg., 7–21–11, Nishi-GoTanda, Shinagawa-ku, Tokyo, Japan
E-mail: †{komura,okabe}@media.kyoto-u.ac.jp, ††fujikawa@root-hq.com

Abstract MIAKO.NET is a public wireless internet project which is based on this unique method born out of "OMOTENASHI" hospitality: Users can use wireless internet service without charge due to a owner of wireless base router pays the cost instead of them. Since May 2002, we have started to design, development and trial operation of MIAKO.NET, and setup the network environment which VPN connection is required for. That environment made you can use wireless internet securely. In this paper we has cleared up the problems of "MIAKO.NET 2" which use centralized VPN servers, and then considered the better suited way of VPN servers' distribution. And also we proposed and designed the new model "MIAKO.NET 3," in which a VPN server is installed in every base router. This model should be valuable for all owners of wireless base router who are supporting MIAKO.NET with their "OMOTENASHI" hospitality.
Key words Public Wireless Internet, Autonomous Distributed VPN services, PPTP server

1. はじめに

「みあこネット」は，地域の情報化を進めるため，市民有志の負担で無線基地局 (以下，基地局) を設置し，無線インターネットの利用できるエリアを広げてきたプロジェクトである．基地局設置者 (以下，設置者) が費用を負担して基地局を設置し，そこを訪れる利用者に無償で無線インターネット環境を提供するという，「おもてなし」の心を基にした独特のモデルで成り立っている．

設置者にとっても利用者にとっても安全な無線インターネット環境を提供するため，みあこネットではこれまで新旧二つの方式を実現し，それぞれを「みあこネット１」「みあこネット２」と命名して実験 [1–4] を行なってきた．

本稿では，みあこネット２の特定のサーバがトラフィックのボトルネックや単一障害点となり得る問題点について述べ，それらを解決して大規模展開を可能にする「みあこネット３」方式を提案し設計を行う．

2. 章で，みあこネット１からみあこネット２への移行に際し

て検討した点について触れ，3. 章では，みあこネット 2 の持つ問題点をまとめる．4. 章で，みあこネット 3 方式を提案し設計する．

2. みあこネットの変遷

本章では，実験開始当初の接続方式「みあこネット 1」と，約 1 年後にそれまでの実験結果を考慮して接続方式等を一新した「みあこネット 2」について述べる．

2.1 みあこネット 1

みあこネットは，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」において，「IPv6 無線インターネット接続実証実験」[5] のために整備されたインフラを用い，2002 年 5 月に実験を開始した．

実験開始当初は，MIS 社の開発した認証方式 [6-8] を用いてモビリティとセキュリティをサポートしていた．この方式を「みあこネット 1」と呼ぶ．

我々は，セキュリティに関して下記のような要件を満たす必要があると考えており，みあこネット 1 方式もこれらを満たしている．

（1） 無線区間の盗聴から守る

（2） 匿名利用を排除する

（3） 偽基地局による通信の搾取を防ぐ

利用者は，専用のドライバをインストールする必要があり，導入の敷居が高い方式となってしまっていた．また，ドライバが提供されていたのは，Windows，PocketPC，FreeBSD 等の一部の OS に限られており，他の OS 利用者はみあこネットを利用できないといった問題があった．

2.2 みあこネット 2

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」とも連携し，基地局数を大幅に増やす機会を得た際に，利用者がより簡単にみあこネットを利用できるように，認証方式と基地局の設置方法等の変更を検討し，「みあこネット 2」と呼ぶ新しい方式で実験を行なった．

みあこネット 2 の認証方式は，Windows をはじめ，MacOS や unix 系 OS などの多くの OS で利用でき，安全性についても十分に配慮されている Microsoft Point-to-Point Tunneling Protocol (MS-PPTP) [9] と呼ばれる VPN プロトコルを用いる事にした．

利用者はまず基地局から DHCP で IP アドレスを取得し，続いて VPN サーバに対して接続する．利用者が，みあこネットの基地局を発見し易くするために，全基地局で SSID を "MIAKO" に統一した．VPN を利用することで，下記のようにセキュリティに関する問題が解決できる．

（1） 無線端末から VPN サーバまでの通信が暗号化されるので，無線区間の通信も暗号化されている．

（2） VPN 接続の際に認証が行われるため，匿名利用を排除できる．

（3） PPTP では相互認証が行われるため，たとえ偽基地局を利用してしまったとしても偽物の PPTP サーバに接続してしまうことは無く，実質的に偽基地局問題を回避できる．

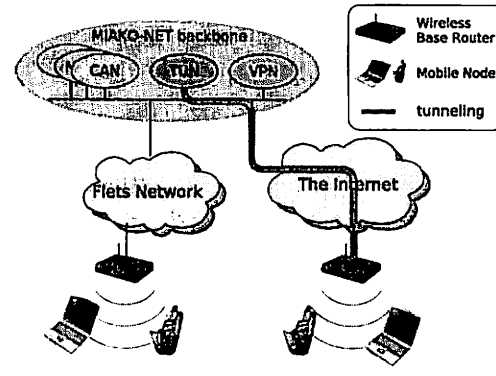

図 1 みあこネットのネットワーク構成

VPN 接続を必ず利用してもらうため，基地局配下の機器は VPN 接続を行なわないとインターネットと通信できなくした．

また，PPTP の設定が正しくできていない利用者向けに，みあこネットに閉じた Web ページ「みあこ CAN」を見せる仕組を作った．PPTP 接続をせずにどこかの Web ページにアクセスしようとすると強制的にこのページが表示される．みあこ CAN 内には，PPTP の設定方法や，アカウントの取得方法，みあこネットの紹介，ユーザサポート用の掲示板などを用意した．

みあこネット 1 では基地局を設置できる回線は，kyoto-Inet に接続できる NTT 西日本のフレッツ ADSL に限定されていた．これは，基地局から無線端末に対してグローバル IP アドレスを割当てる必要があり，各基地局毎に /27 のアドレス空間が利用できる PPPoE アカウントを用いて接続を行っていたためである．

みあこネット 2 でも同様に端末にはグローバル IP アドレスを割当てることにしたが，フレッツ ADSL 以外の回線にも設置できるようにするため，IP トンネル技術を用いて /27 のアドレス空間を確保することにした．NAT 配下からでもトンネルを掘れるように IP over TCP トンネル方式の VTun [10] を採用した．基地局は，DHCP で IP アドレスを自動的に取得し，みあこネットのトンネルサーバに接続して，動作に必要なアドレス空間をトンネルを通して確保する．この仕組のおかげで，インターネットとの接続性があるネットワークであれば，ほとんどの環境で基地局を設置できるようになった．

これらの改良により，利用者にとってはより利用し易くなり，基地局を設置も容易になり，みあこネットの実験規模を拡大することが可能になった．京都府を中心に日本全国に約 300 局の基地局が設置され，利用者数はのべ 10,000 人に達する．

なお，みあこネットのネットワーク構成は図 1 のようになっている．

3. みあこネット２の問題点

本章では，基地局数を更に増やし，より多くの利用者にサービスを提供する際に問題となる点について述べる．

3.1 VPN サーバ

無線インターネットを安全に利用するため，みあこネットの全利用者は PPTP による VPN 接続をしたうえでインターネットと通信を行う必要がある．このため，みあこネットでは利用者向けに複数台の VPN サーバを立ち上げて PPTP アカウントを発行している．

この方式は，全利用者からの通信が全てみあこネットが管理する VPN サーバを経由するため，下記のような問題がある．

- VPN サーバに全利用者からの通信が集中するので，ボトルネックや単一障害点となる
- VPN サーバで，全利用者のアカウントを管理する必要がある

前者については，VPN サーバを増設するなどの対処方法も考えられるが，みあこネットは利用者から利用料を徴収しないビジネスモデルのため，利用者数の増加に合わせてサーバを増設するのは費用等の問題で難しく，他の方法による解決が必要である．

また，後者は，利用者数が爆発的に増加した場合に，全アカウントの管理を我々みあこネットのプロジェクトだけで行うのは現実的ではないので，アカウントの管理を分散させる仕組が必要になると考えられる．

3.2 トンネルサーバ

無線基地局では，端末に DHCP でグローバル IP アドレスを配るために，IP トンネリングを利用している．

みあこネット 1 では，IP トンネリングを利用していなかったが，代わりに，kyoto-Inet に接続できるフレッツ ADSL 回線にしか基地局を設置できないという制限があった．また，NTT フレッツ網を利用せずに /27 などのグローバル IP アドレス空間を確保するのは，現状の IPv4 ネットワーク環境では難しいため，IP トンネリングを採用してアドレス空間を確保することになった．

トンネルを用いる方式では，基地局配下の端末が通信する際，全てのパケットがトンネルサーバを経由するため，トンネルサーバがボトルネックや単一障害点となり得る問題点がある．

4. みあこネット３の設計

本章では，前章でまとめた問題点を解決する手法について検討する．

現みあこネット２の利用者が多数存在することから，新しい方式に対応した基地局でもこれまでと同じ方法で利用できる，みあこネット２の延長上のサービスとなる事が望ましい．そのため，SSID が “MIAKO” の基地局に接続して DHCP でアドレスを取得した後，VPN 接続をしてインターネットと通信をするという基本的な流れは変更しないことにする．

4.1 分散 VPN サーバの利用

VPN サーバへの負荷の集中と，管理するアカウント数が増大する問題への対処法として，VPN サーバの分散を行う．VPN サーバの分散とは，みあこネット自らが多数の VPN サーバを設置するだけでなく，既に分散して動作している既存の有料 VPN サービスや，企業や大学などで関係者向けに提供されている VPN サービスをも利用するという意味である．みあこネット自身が多数の VPN サーバを設置する方法は次節で扱い，本節では既にインターネット上で分散して稼働している VPN サーバを利用する方法について議論する．

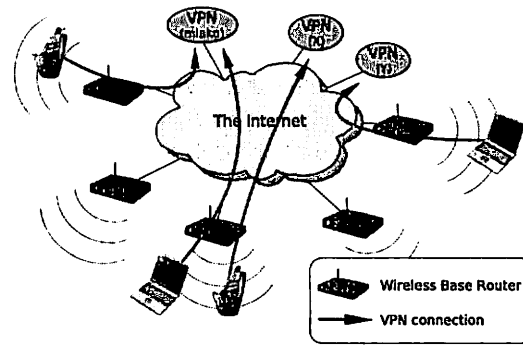

図 2 VPN サーバの分散: 任意の VPN サーバへの接続を許可

みあこネットが提供する VPN サーバの負荷を減らし，同時に，みあこネットで管理する VPN アカウントを減らすため，他の VPN サービスを利用できる利用者に対しては，みあこネットが提供する VPN サーバを利用せず各自の VPN サーバに直接接続することを推奨する．

VPN の接続を許す先としては次の二つが考えられる．

- みあこネットと連携した組織の VPN サーバ
- インターネット上の任意の VPN サーバ

前者は，VPN サービスを提供する組織とみあこネットとでお互いに信頼関係を持った上で接続を許可する方式であり，組織間の信頼関係が成立しているため安心感は有るが，接続先を増やすためには連携相手を増やす必要がある．

一方，後者はみあこネットと VPN 接続先組織とは何の信頼関係もない場合も多いが，任意の VPN サーバに接続できるため本方式を利用できる利用者数は飛躍的に増大する．

VPN は，接続時に認証が行われて，正規の利用者であることが確認された利用者だけが通信を許可される．そのため，みあこネットから VPN 接続を許可する相手は，組織間の信頼関係に頼らず，VPN サーバと VPN クライアント間で認証が完了したかどうかに任せておけば十分であると考えることができる．そこで，みあこネット３では図 2 のように，インターネット上の任意のホスト (図中の VPN(X) や VPN(Y)) に対して VPN 接続を許可することとする．

ここで少し視点を変えて，他の組織が提供する無線アクセス環境で本提案と同様の接続形態が許可されている場合を考える．他組織の基地局から，インターネット上の任意の VPN サーバへの接続が許可されていれば，みあこネットの利用者はみあこネット VPN サーバに接続してインターネットに接続できる．このような方式が広く採用されれば，特定のプロバイダの会員

だけが基地局を利用できるのではなく，本方式を採用している基地局であればどこからでも，各自が普段利用する VPN サーバに接続してインターネットと通信することができるようになる．

この結果，利用者にとってはより多くの基地局を利用でき，利用可能エリアが広がることになる．また，基地局を提供する組織にとっても，自ら設置した基地局だけでなく，他組織が設置した基地局によって利用可能エリアを広がり，利用者へのアピールに繋がるという利点がある．

みあこネット 2 でも，既にこの方式を取り入れており，インターネット上の任意 IP アドレスを持つ VPN サーバへ接続ができるように IP フィルタの設定変更を行なった．なお，VPN プロトコルとして，MS-PPTP 以外に Cisco CheckPoint, SST (Shiva Smart Tunneling), ssh (Secure SHell) なども加えた．なお，フィルタでは，IP のプロトコル番号や，TCP・UDP のポート番号などで VPN と考えられるパケットを許可している．

4.2 VPN サーバの分散配置

本節では，みあこネットとして多数の VPN サーバを分散配置する方法を検討する．

みあこネット 2 では，高性能な PC で VPN サーバ (集中型 VPN サーバ) を構築し，全利用者が数台の VPN サーバを共有している．VPN サーバを分散配置する方法として，これまでと同じように高性能な PC を増設する方法は 3.1 節で述べたように，利用者からの収入が無いビジネスモデルのため難しい．

そこで，みあこネットの利用エリアを広げると同時に，小規模な VPN サーバを増設する効果的な方法として，無線基地局に VPN サーバ機能を導入する方法を提案する．

みあこネットでは，基地局設置者自身やその関係者もみあこネットを利用できるように，設置者に対して「オーナーアカウント」と呼ぶ 10 個の VPN アカウントを配布してきた．オーナーアカウントは，設置者が個人の場合は家族，設置者が企業の場合は従業員などに利用してもらうことを想定しており，設置者の責任で実際の利用者に配ってもらっている．

オーナーアカウントはこれまで集中型 VPN サーバに登録してきたが，本提案のように基地局に VPN サーバ機能を導入すれば，オーナーアカウントを設置者自身の基地局に登録することができるようになり，集中型 VPN サーバの負荷を減らすことができる．また，設置者が自己の責任で，基地局内の VPN サーバに VPN アカウントを追加登録して利用者を増やすといった運用も可能になり，おもてなしの心でみあこネットを支えている設置者にとっても有益な方法になると考えられる．

図 3 のように設置者自身の基地局の無線を利用するとき (図 3 左) も，それ以外の基地局の無線を利用するとき (図 3 右) も，常に設置者が持つ基地局に VPN 接続してインターネットと通信をすることになる．

このような VPN サーバ機能を持つ基地局がインターネット上に多数設置されれば，集中型の VPN サーバへの負荷を増やすことなく利用エリアを広げることができる．

また，前節で述べたように，他組織の VPN サーバへの接続も許可することで，図 4 のように，本方式と同等の通信方式に

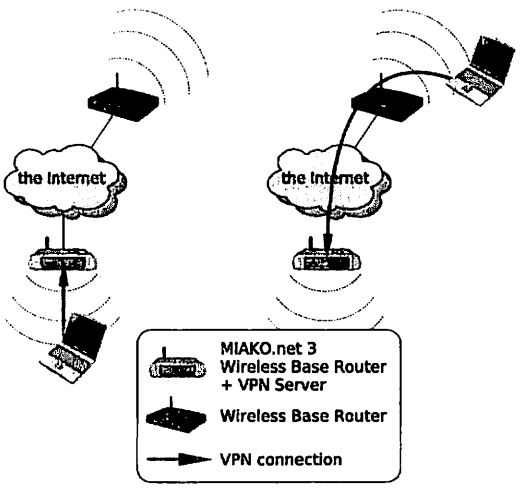

図 3 みあこネット 3 基地局の利用法

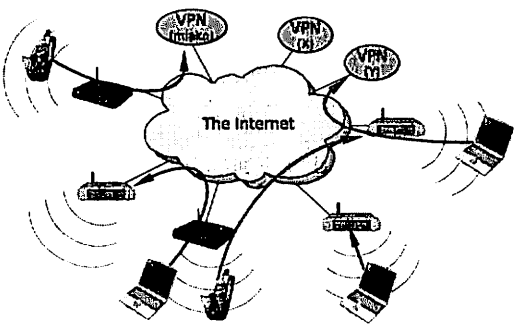

図 4 みあこネット 3 構想

対応した基地局であればどの組織が設置したものであっても，利用者は違いを意識することなく自分の VPN サーバに接続してインターネットと通信することができる．

なお，どの組織が設置したか分からない基地局を利用したり，偽基地局に繋がってしまった場合に，情報を盗聴・改竄される危険性があるが，適切な VPN 接続を利用することでこれらの問題を回避できる．PPTP では認証を行う際，サーバ・クライアント間で相互認証を行うため，正しい PPTP サーバとしか接続しない．PPTP 接続できた場合は正しい PPTP サーバに接続されており，その後の通信は全て暗号化されているので，たとえ偽基地局に繋いでしまった場合でも，途中経路で情報を盗聴・改竄される危険性はない．

4.3 プライベート IP アドレスの利用

みあこネット 2 では，DHCP でグローバル IP アドレスを配るために，IP トンネリングで/27 のアドレス空間を基地局までトンネルして利用していた．全基地局がトンネルサーバにトンネルを張るため，ボトルネックや単一障害点となる危険性があった．

そこで，みあこネット 3 方式では，グローバル IP アドレスの利用を諦めて NAT を利用することを検討した．NAT はインターネットのエンド・ツー・エンド原理を崩し，様々な弊害を

引き起すことが知られているため，これまでみあこネットではグローバル IP アドレスを利用することにこだわってきた．しかし，現在の IPv4 ネットワーク上で，みあこネット 3 の分散環境を実現するためには，NAT を利用せざるを得ないという結論に達した．

一般的に利用されている NAT では，TCP や UDP に対して，IP アドレスとポート番号の組合せを変換しているが，PPTP では，TCP と GRE プロトコル [11] が利用されており，PPTP に対応した NAT を利用しないと複数人での同時利用できない場合がある．

また，オーナーアカウントを用いて基地局の VPN サーバに接続する場合も，アカウント毎に個別のグローバルアドレスを利用することはできなくなるため，NAT を利用する必要がある．

4.4 みあこ CAN

みあこネット 2 では，VPN を利用しないまま Web アクセスをすると，強制的にみあこ CAN を表示する仕組があった．この仕組はトンネルサーバやその他のサーバの連携によって実現している．

みあこネット 3 の分散環境で同等の機能を実現するには，基地局内にみあこ CAN を強制的に見せるための仕組を導入する必要がある．具体的には，無線ネットワークからの宛先ポート番号 80 番 (HTTP) の通信を検出して，パケットを本来の宛先に転送せずに横取りする機能や，CAN のページの内容を Web ブラウザ送信する機能が必要になる．

これまでと同等のみあこネットに関する情報を提供するだけでなく，設置者が独自の宣伝用ページを作成して利用者に見せるといった応用も考えらる．

なお，みあこ CAN のコンテンツは，基地局内に記録する方法と，インターネット上の特定の Web ページから取得してブラウザに転送する方法とが考えられる．

5. まとめと今後の課題

みあこネット方式を大規模に展開する場合に，現在のみあこネット 2 方式では VPN サーバとトンネルサーバへの負荷の集中が問題となるため，インターネット上の任意の VPN サーバへの接続を許し，基地局に VPN サーバ機能を内蔵して分散 VPN サーバの環境を構築するみあこネット 3 の設計を行なった．このとき，複数のグローバル IP アドレスを利用することが難しいため，やむを得ず NAT を利用することとした．このように設計したみあこネット 3 を実現するための実装を行っており，今後実験を行なっていく予定である．

今後の課題としては，グローバル IP アドレスの利用を諦め NAT を利用するという結論に達したが，IPv6 のネットワーク環境を前提に設計を行えばグローバル IPv6 アドレスを利用することは実現可能であるため，IPv6 を活用した方式を検討する．

また，VPN を用いた通信は，認証と暗号化により安全性が確保できるが，通信が常に VPN サーバを経由するため効率が悪いという欠点も有る．その為，認証が完了したあとは，通信相手と直接通信を行える方式についても検討を行っていきたい．

文　献

[1] 藤川, 岡部, 古村："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", 情報処理学会研究報告 2003-DPS-111 (2003).

[2] 古村, 大平, 藤川, 岡部："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", 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 2004 (DSM2004) (2004).

[3] T. KOMURA, M. KOSUGA, K. FUJIKAWA and Y. 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) (2003).

[4] 古村, 北原, 藤川, 上原, 岡部："みあこネットでの実時間動画像マルチキャスト実験", 信学技法, **NS2004-217,IN2004-217**, pp. 101–106 (2005).

[5] http://www.root-hq.com/pressrelease/02.2.18.html.

[6] "ＭＢＡ標準 0201 号「ＭＩＳプロトコル仕様書 ver.1.02」". http://www.mbassoc.org/j-services/mbas0201r060606.pdf.

[7] "ＭＢＡ標準 0202 号「ＭＩＳモバイルＩＰ仕様書」". http://www.mbassoc.org/j-services/mbas0202r060606.txt.

[8] "ＭＢＡ標準 0301 号「ＭＩＳＡＵＴＨプロトコル仕様書」". http://www.mbassoc.org/j-services/mbas0301.pdf.

[9] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn: "Point-to-point tunneling protocol (pptp) [rfc2637]" (1999).

[10] http://vtun.sourceforge.net/.

[11] T. Li, S. Hanks, D. Meyer and P. Traina: "Generic routing encapsulation (gre) [rfc2784]" (2000).