2004－MBL－28　(11)
2004／3／4

アンテナ指向性制御を組合せた無線 LAN 統合認証方式

西村 俊和† 　前田 忠彦† 　小川 均†

†立命館大学理工学部 〒525-8577 草津市野路東 1-1-1

E-mail: †{nisimura, tmaeda, ogawa}@cs.ritsumei.ac.jp

あらまし 無線 LAN によってインターネット接続を他者と安全に共有できる方式を提案する．無線 LAN ルータで認証に失敗した通信パケットを破棄せずに VPN(Virtual Private Network)技術で外部に設けた認証機構に送信することにより，異なった保安レベルの利用者が同時に利用可能となる．また，特定の無線 LAN クライアント方向への指向性をアンテナで動的に制御することにより，認証時のように重要な内容の無線通信を維持することができ，通信を妨害する他電波源の影響を軽減することができる．

キーワード 無線 LAN, 認証, VPN, 指向性制御,

Unified Authentication System for Wireless LANs Using Directivity Controlled Antenna Systems

Toshikazu NISHIMURA† 　Tadahiko MAEDA† 　and 　Hitoshi OGAWA†

† College of Science & Engineering, Ritsumeikan University 1-1-1 Nojihigashi, Kusatsu C., 525-8577 Japan

E-mail: †{nisimura, tmaeda, ogawa}@ cs.ritsumei.ac.jp

Abstract This report proposes the method that allows users to share the internet access with guest users in secure way. In order to send unauthorized packets from wireless LAN routers to the external authorities on the net, VPN (Virtual Private Network) Technology is applied in our method. Wireless resources can be used efficiently in the space domain, even in the shared-frequency systems, by optimizing the radiation patterns of base station antennas for WLAN systems adaptively and dynamically based on the required security level at the application layer.

Keyword Wireless LAN, Authentication, Virtual Private Network,, Directivity Control

1. はじめに

近年，光ファイバ網が発達し，商業ビルを始め，居住マンションや一般住宅へ引かれている．従来は，光ファイバからルータまたはファイアウォールを介して，イントラネットまたは家庭内 LAN に繋がっており，保安が維持されている．最近は，配線が不要な無線ルータが普及してきている．特に，一般の住宅における利用が多く見られる．

無線ＬＡＮの利点は，単にケーブルを引き回す手間が省けることだけでなく，無線が届く場所であれば原則的に何処でも利用できることにある．そのため，駅構内や喫茶店等の不特定多数の人が集まるところでは，無線ＬＡＮとノートパソコンの組合せはインターネット利用の方法として適切な環境を提供しているといえる．しかしながら，このような無線ＬＡＮを利用するには，その無線ＬＡＮの管理者が発行する，または，予め認めているＩＤ取得者のみが利用可能である．したがって，異なる管理の無線ＬＡＮを利用するためには異なるＩＤが必要となり，位置透過性が特徴であるＬＡＮの有効性を生かすことが出来ない状態となっている．さらに，無線ＬＡＮを一般的に提供している業者の設備がない一般住宅地では，各戸では無線ＬＡＮが利用されている場合でも，一般的には他の人が使えない状況となっている．たとえば，各無線ルータを誰でも利用できるように設定することは可能であるが，そうした場合，各無線ルータの所有者の機器構成等の情報が公開となり，接続機器の無断使用・ファイル等の覗きなどプライベートが守られない状況となる．このことが無線 LAN アクセスポイント(無線 AP)の乱立をまねき，相互に干渉を発生させ不要な電波の発射をおこすため，周波数の有効利用を大きく妨げてきている．また，無線 LAN 使用者がインターネット内で迷惑行為を行った場合，外部からは無線ルータ所有者が行

った行為と区別が付かず，迷惑行為の責任を追及するのは困難となる．

従来の無線 AP では単一保安レベルのみ実現されているため，単一認証機構で拒否されると利用不能であった．日本サスティナブル・コミュニティ・センターによる接続実験は認証機構を AP 外で実現したが，認証機構は単一であり問題は同様である．従って，異なった保安レベルの利用者が同時に安全に無線 LAN を利用可能とする技術が必要であると考える．

一方，無線通信は本質的には傍受される特質をもっていることは否めない．このために指向性を制御して不要な方向への電波の放射を抑圧する方法が考えられるが，本稿で考えている公衆無線 LAN システムに適応するには，以下のような問題点を有する．無線において特定の方向に電波を放射するためには，アンテナや高周波ブロックのリソースを多く必要として，全てのトラフィックに対して，指向性制御を適応することは無線ルータが大型化し経済的にも問題である．したがって，必要なセキュリティーレベルを判断し，アンテナや高周波ブロックのリソースを適応的にスケジューリングする必要がある．ところが，このセキュリティーレベルの判断はアプリケーションと密接に関連するため，物理レベルに近いレイヤだけの情報では適切な判断を下すことが出来ない問題点があった．このため，セキュリティーレベルを判断した上で合理的にアンテナや高周波ブロックのリソース配分がなされていないのが現状である．

一方で，従来の無線周波数の管理はシステムごとに周波数を割り付けるという，方針のもとになされてきた．このため，アクセスポイントを設置したものが独占的にその周波数を使用することが起きている．そのため，独占的な電波の使用を排除し，空間的にしかも適応的に周波数資源を利用し有効活用しようとする考えに基づく「アンテナ制御を含めた認証によるアクセスポイントの共用」という発想が必要であると考える．この問題を解決するための一つの切り口としてアンテナシステムと認証システムを連携させる方法を提案する．

本報告では，無線ルータ所有者の機器等のセキュリティを完全に確保しつつ，不特定多数に対する無線ＬＡＮの利便性を追求する無線ＬＡＮルータについて提案し，その検証システムについて議論する．

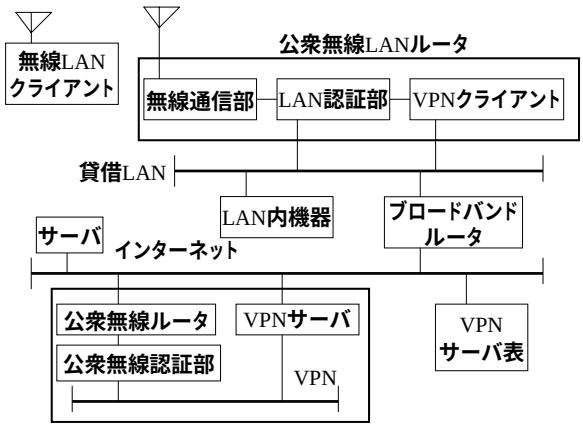

図 1: 公衆無線 LAN ルータの構成

2. 認証機構と公衆無線 LAN ルータ

家庭などで広く用いられているインターネット接続においては，接続ノードの識別子となる IP(インターネットプロトコル) version 4 アドレスを接続機器台数分提供されることはまれであるので，ブロードバンドルータ等アドレス変換機能を持つルータを介して LAN を接続することが多い．ローカルルータ機能をもつ無線 AP をここでは無線ＬＡＮルータと呼ぶ．本研究で用いる無線 AP も同様の機能を持っているため，特にこれを公衆無線ＬＡＮルータと称することにする．

本報告では無線 AP を本来の利用者とそうでない者とで兼用するため, それぞれの無線 LAN クライアントを区別する必要がある．ここでは公衆無線 LAN ルータに直結した LAN を, 貸借有線 LAN と呼ぶ. 貸借有線 LAN は家庭内 LAN や組織のイントラネットであるので, LAN 内機器が接続されていて，本来の利用者のみが利用できなければならない．ルータ所有者に許可を得て, 貸借有線 LAN や LAN 内機器を利用できる無線 LAN クライアントを内部機器と呼ぶ．それ以外の無線 LAN クライアントは外部機器と呼ぶ．

図１に本報告が提案する認証機構の構成とインターネットとの関係を示す．セキュリティを確保すべき内部機器については，MAC アドレス登録等の手法により認証あるいは区別可能であるとする．無線 LAN クライアントが IP 通信を行うことを考える．無線 LAN クライアントの IP データグラムは，通常通りイーサネ

ットのフレーム(イーサフレーム)に乗せられて，公衆無線ＬＡＮルータの無線通信部へ届く．この無線通信部で受信されたイーサフレームは，当ルータ内部の LAN 認証部に送られる．LAN 認証部では，上記の方法で内部機器と外部機器を判別できるので，従来の無線 AP の動作そのまま，内部機器のイーサフレームを有線 LAN に送ることができる．これによって，ルータ所有者の登録機器は通常通り貸借有線 LAN と通信でき，従って，プリンタ等の LAN 内機器を利用することができる．

外部機器からのイーサフレームは上記認証を成功させることはできない．ここでは認証に失敗したイーサフレームを破棄せずに，LAN 認証部から VPN クライアントへ送り，ここで当イーサフレームを GRE(Generic Routing Encapsulation)[1]等の手法で IP カプセル化するものとする．特定の VPN サーバ宛の IP ヘッダをつけてしまえば，当イーサフレームは IP データグラムのデータ部に過ぎないため，カプセル化した IP データグラムを貸借有線 LAN へ送信しても LAN 内機器には到達できず，そのままブロードバンドルータ等アクセス線を通じてインターネット上へ送信されることになる．よって，外部機器が LAN 内機器に作用したり，インターネット上の任意のサーバに直接アクセスしたりすることはありえない．

カプセル化された前述イーサフレームは到着先の VPN サーバにより，インターネットと隔離された VPN(Virtual Private Network)へ送信され，イーサフレームへ変換される．このイーサフレームをさらに公衆無線で利用可能かどうか認証するものとする．認証機構は前述 LAN 認証部と同様である．認証できないイーサフレームは破棄し，認証済みイーサフレームのみを対象とし，その IP データグラムをルータを通じて通常のインターネットへ送信する．これにより，インターネットの他のサーバ(例えば Web サーバ)へ到達可能な IP データグラムは，LAN 認証部あるいは公衆無線認証のいずれかで必ず認証されていることが保証される．よってインターネット上の迷惑行為等，無線 LAN 利用者自身の責任を，認証結果に応じて追及することが容易となる．

また，複数の公衆無線認証を準備して適切な VPN へ送信できるよう工夫すれば，異なった保安レベルを実現することが可能である．例えば複数組織において本システムを共用し，各組織の運用原則にのっとった認証方式・管理ポリシー等を定めることも自由に行える．この工夫のためには，外部機器ごとに対応する VPN と VPN サーバを保持しておくデータベースをひとつ準備して，各公衆無線 LAN ルータから参照できれば十分である．このようなデータベースはここでは VPN サーバ表と呼ぶ．図 1 では公衆無線 LAN ルータからアクセス可能なインターネット上の特定の資源として準備されていることを想定している．また，VPN サーバ表は公衆無線 LAN ルータに内蔵されていてもよいため，例えば図 2 のような構成も可能である．

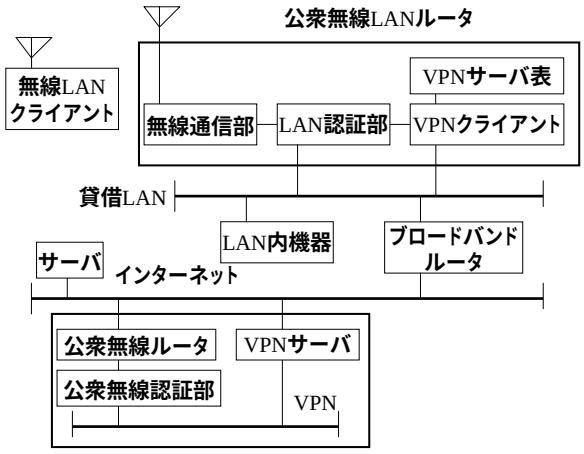

図 2　VPN サーバ表を内蔵した
公衆無線 LAN ルータの構成

本研究で提案する異なった保安レベルの実現方法は認証方法や VPN の構成方法によらないので，LAN 無線認証部での認証方式と公衆無線認証での認証方法は必ずしも MAC アドレスの区別による方法でなくてもよく，また公衆無線認証での認証方法に適した VPN の構成方法を用いればよい．上記の説明ではイーサセグメントを VPN へ送信しているため，例えば PPPoE(Point-to-Point Protocol over Ethernet)[2] でユーザ認証をすることもできる．また，イーサセグメントの代わりに，イーサセグメントのデータ部に存在する IP データグラムを取り出し，これを VPN へ送信しても同様の効果が得ることができる．この場合，PPTP(Point-to-Point Tunneling Protocol)[3], IPsec AH(Authentication Header)[4]等認証機構つき VPN 構成方式を利用してもよい．例えば PDA のように無線 LAN クライアントに特定

の通信パケット認証機構を準備するのが困難な場合，Web 認証のような簡便な方法で Web 利用のための認証をすることも可能である．本システムを利用する際の保安強度は，実現に用いる認証と VPN に主に依存している．

3. アンテナ指向性制御と認証の連携

無線通信はケーブルで接続されたネットワークと異なり，通信線路のケーブルに物理的に接続するなどの方法によらなくても，通信を傍受される特質を持っている．このためアンテナシステムと認証システムを連携させ,認証時には不要な方向への電波の放射を抑圧する技術が重要である．

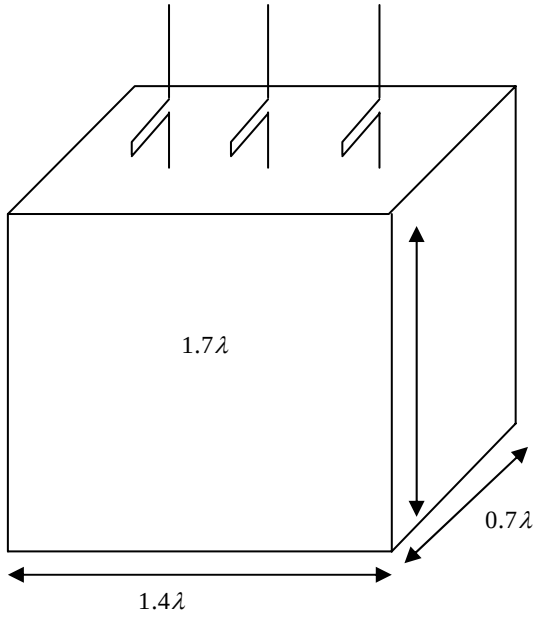

図 3 アクセスポイント

アクセスポイントに取り付けられたアンテナの指向性はアクセスポイントの筐体電流の影響を受ける．筐体上の電流を低減するために給電点をオフセットしたり，筐体表面の給電位置において，電圧給電に近い給電条件を用いる手法が良く用いられる．一方で，筐体電流を積極的に制御して，指向性を変化させる方法が考えられる．筐体電流の影響が指向性に与える影響の例を示すために，図 3 に示す構造のアクセスポイントを想定する．使用する周波数帯が２．４GHｚ帯である場合，高さは２００mm 程度となり，上面には３組の垂直偏波用のスタブ付きのアンテナが設置されていることを想定している．このアンテナシステムからの放射指向性を計算するために，筐体の部分をワイヤグリッドで近似してモーメント法を用いて放射特性を計算した．なお、具体的な計算には、PC クラスタを用いた並列化とアンテナ形状を考慮したインピーダンス行列の計算量の低減化を組み合わせることにより行った[5].

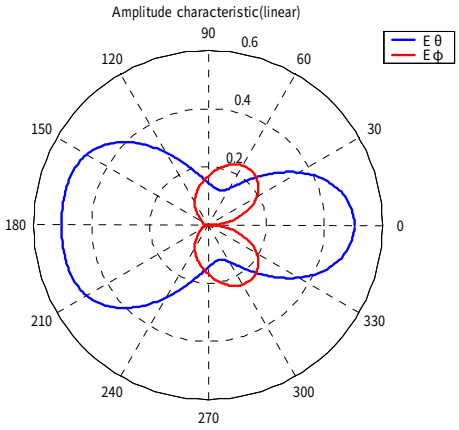

図 4　放射素子（中心）の放射指向性

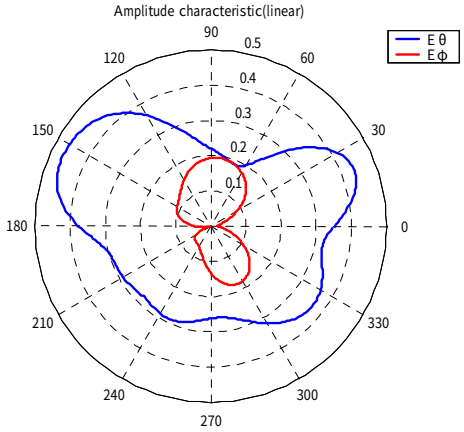

図 5　放射素子（右側）の放射指向性

図４から図６に H 面での放射指向性を示す．図中には主偏波である垂直偏波成分(E_θ)および交差偏波成分である水平偏波成分(E_ϕ)の計算結果を合わせて表示してある．ダイバーシチ受信を想定して複数のアンテナを用いているが，素子間相互結合と筐体のために各素子とも均一な全方向性の指向性を示してはいない．中心素子の放射特性も構造の非対称性による筐体電流の不均一のため対称性を示していない．なお，これらの指向性は各アンテナの給電点におい

てアンテナ各素子の共振時でのインピーダンスに整合が取れているものとして計算を行っている．実際には複数の受信機が内蔵され，各アンテナが受信機に整合回路を通じて接続されている状態を模擬しているといえる．この状態において，方位角方向に不均一な指向性を有しているが，この不均一の程度やビームの方位角方向での偏りは，各アンテナの終端条件によって可変することができる．ここでは，実際のビームの可変範囲などの詳細は省略する．

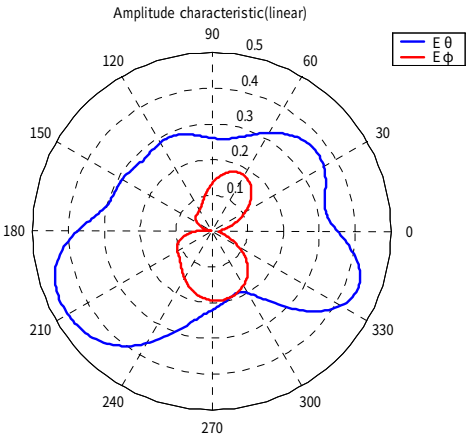

図 6　放射素子（左側）の放射指向性

この例の様に，アンテナは電波の空間的分布を物理的に変更できる素子である．本質的に電波を傍受されにくくするためには「必要以外の方向に電波を放射しない」ということが基本原則である．しかしながら，本稿で取り上げている無線 LAN の統合認証方式を実現しようとする場合，アンテナの指向性を固定していたのでは，「広く開かれたサービス」という，本来の目的を達することができない．このため，通常は周囲の電波を受信し，周囲に存在している端末局を調査し，その局の識別符号，電波の到来方向や電界強度などの情報をテーブルとして作成しておくことにより，認証などの重要信号の送出にあたっては所望方向に適した指向性を選択する．また，悪意の妨害やアクセスが判明している場合，その方向に対して抑圧特性をもつ指向性設定条件を採用する．ここで，方位推定には受信機や送信機との接続状態や切り離し時における終端条件を変化させて，指向性を制御する簡易的なビーム切り替えや，MUSIC 法[6]などが考えられる．MUSIC 法を適応する場合に反射波の強度が強くコヒーレント波と考えられる場合，そのレベルに応じて MUSIC スペクトルのピークは入射する 2 波の間の角度となる．この場合，空間的な平均化による分離が必要となる．一般に，到来方向推定は素子数が多いほど精度が向上するが，現実には基地局の大きさが素子数を制限する．

実際には，大まかな指向性の制御を行うことを想定する場合と，大掛かりな指向性制御を想定する場合では条件がかなり異なると考えられる．図 4 や図 5 の指向性変化のレベルであれば，送受信するアンテナを切り替えるだけでも，指向性を左，右，中央と振り分けることが可能である．このビーム制御をアクセスポイントの上位層との協調によって実現する．

アンテナのような物理層の末端の装置はアプリケーションから見て最下流に位置するため，アンテナシステムの制御は認証制御という上位のアプリケーションからの要求により適応的な制御がなされてはいなかった．従来のアンテナとアプリケーションの協調を想定しない方法では，アプリケーションの要求からくるセキュリティーレベルを維持しつつ，統合的な周波数資源の空間的高効率利用の実現が困難であったと考えられる．

4. 検証システム

以上で論じたシステムが現技術で実現可能なことを示すために，プロトタイプとなる検証システムを実現した．以下に各部で用いた既存技術について説明する．

4.1. LAN 認証部

通常の無線 LAN には SSID(Service Set ID)や WEP(Wired Equivalent Privacy)等の保安機能が準備され，内部機器の通信のみを許可し，外部機器の通信を拒絶することができる．しかしながら本研究の提案においては外部機器についても無線通信を行う必要があるため，上記二点の方法をそのまま適用することは必ずしも容易でない．ここでは LAN 認証部の実現の一例として，通常の無線 LAN で用いられている MAC アドレス認証を模して，登録されている MAC アドレスのイーサフレームのみを貸借 LAN へ送信することとする．MAC アドレス認証は万能でないという指摘[7]があるものの，イーサフレームのヘッダにある MAC アド

レスを検査するだけで容易に認証可能であるため，本研究の検証システムに採用した．

4.2. VPN

多くのインターネット接続においては，接続ノードの識別子となる IP version 4 (IPv4) アドレスは必ずしも固定でなく，接続のたびに異なったアドレスが割り当てられることが多い．一方，異なったアドレスに対して一定水準の暗号化やセキュリティポリシーを IP 層で適用することは必ずしも容易でない．

また，無線 AP の成りすましの可能性が指摘されているので[7], 例えば近隣の成りすまし無線 AP が無線 LAN クライアントから認証情報を騙し取り，本来の認証を不正に成功させる中間者攻撃を行うことは避けなければならない．例えば無線 LAN クライアントに専用の認証ソフトウェアを導入し，公衆無線認証部と相互に認証を行うことによってこの問題を回避可能することが可能である．しかし，このような認証ソフトウェアを任意の端末に導入することは必ずしも容易ではない．よって本研究では，IPv4 が固定的に割り当てられない環境においては IP アドレス以外の方法で各 VPN クライアントを認証し, 利用が許可された公衆無線 LAN ルータのみが VPN に接続することが必要であると考える．

本研究では IP version 6(IPv6)に準備された保安機構を利用するため, 認証によって各 VPN クライアントに固定的な IPv6 アドレスを付与する方法を採用している[8][9]．この場合，無線 LAN クライアントの IPv4 データグラムは IPv6 データグラムでカプセル化され，さらに IPv4 データグラムに乗せられて VPN サーバに送信されることになる．イーサセグメントをカプセル化するには，例えば EtherIP[10]等の手法も利用可能であると思われる．

4.3. 公衆無線認証部

前節の手法によって公衆無線 LAN ルータと VPN サーバ間に認証された VPN が実現されていると仮定すれば，公衆無線認証部では，無線 LAN クライアントが利用可能な認証方式を実現すれば十分である．現在は利用可能なサービスを Web アクセスに限定し，未認証クライアントからの利用要求を認証用 Web ページへリダイレクトすることによって実現している．

検証システムで用いた VPN は IP 層での接続を行っているので PPPoE は利用できないが，無線 LAN クライアントに仮に IP アドレスを付与し，PPTP によって認証を行うことは可能である．

5. 考察

いわゆる Hot Spot は，無線を利用したインターネットアクセス方法のサービスエリアを指す言葉である．IEEE802.11ｂ等の無線 LAN を介してインターネットアクセスが可能なものが多い. NTT コミュニケーションズの登録商標「ホットスポット」のような商用サービス[11]では，サービスエリア内であっても他利用者が自由に利用することはできず，例えば事前に登録したアカウントで Web 認証を行うことが必要となる．

無線 LAN は例えば携帯電話の基地局等別の無線設備よりもサービスエリアが狭いため，このような方式で地域内を遍くサービスエリアにするためには，単一事業者が広く通信設備を設置しなければならず，先行投資等の問題から実現は容易でない．また，同一地域で複数の事業者が無線 AP を設置した場合無線チャネルの衝突や一部事業者による無線チャネルの占有等のおそれもある．

FREESPOT 協議会のサービス「FREESPOT」は Host Spot と同様に，無線 LAN でインターネットにアクセスできる環境を開放するものである[12]．公共施設や飲食店等，利用者へ FREESPOT サービスを提供したい設置者がインターネット接続と無線 AP を準備する運用方針のため，技術的には単一事業者が通信設備を準備する必要はなく，地域内を遍くカバーするには例えばホットスポットよりも適していると考えられる．また FREESPOT の多くの設置者は無料でサービスを提供しているため，複数事業者が同一地域で競って無線チャネルを占有するような事は考えにくく，電波資源の有効利用が図れる．

利用形態は無線 AP 設置者によって異なるものの，他無線 LAN クライアントへの通信を禁止する専用無線 AP を用いることによって，開放された無線 LAN 内の保安を維持するものが多い．インターネットでの迷惑行為の追及や利用個人特定は，事前登録や利用者チェック等，無線 AP 設置者の運用方針に強く依存している．

日本サスティナブル・コミュニティ・センターの運営する公衆無線インターネットプロ

ジェクト「みあこネット」は，ホットスポットと同様に設置者がインターネット接続を準備して無線 AP を設置可能なインターネットアクセス環境である[13]が，事前登録によるアカウントの認証の結果，無線 LAN クライアントには常に同一のグローバル IP アドレスが割り当てられる点が他のシステムと異なっている．これによって，利用 IP アドレスから一意に利用個人が特定でき，インターネットでの迷惑行為の追及等が容易となっている．

IP アドレスの割り当てには MobileIP[14]類似技術と PPTP との二種類の方式が準備されている．また，VPN や PPPoE 等の手法を用いることによって，異なった接続事業者に接続された無線 AP を一つのアドレス空間に集約している．そのため MobileIP 類似技術を用いた接続時には，無線 AP 間のハンドオーバーも可能である．

認証サーバはシステム内に一種類用意され，同じシステムを利用した他プロジェクトの認証情報を併用することもできるが，任意の認証方式や VPN を利用することはできない．よって本研究で意図しているように，異なった保安レベルの利用者を共存させることは困難である．また，無線 LAN から設置者の有線 LAN に影響しないよう工夫されているため，自身の有線 LAN への直接のアクセス手段として設置者が無線 AP を利用することはできない．

本研究で提案する統合認証方式では，みあこネットと同様に，設置者がインターネット接続を準備することを想定しているが，公衆無線 LAN ルータを設置者自身が無線 AP として利用可能である点が特長の一つである．すなわち，利用者が自身の有線 LAN への直接のアクセス手段として別途無線 AP を準備する必要がないため，

- 既存のインターネット接続利用者の協力を得やすい
- 通常の無線 LAN ルータとの置換が容易
- 近接無線 AP の使用チャネルを避けやすい

等の利点が考えられる．

6. おわりに

本研究では無線 LAN を用いたインターネット接続手法を提案した．無線 LAN ルータで認証に失敗した通信パケットを破棄せずに，インターネット上の公衆無線認証部へ VPN 技術で送信することにより，貸借有線 LAN 内の機器を外部機器のアクセスから保護しながら，インターネット接続を外部機器ユーザと共有することができる．また，上位のアプリケーション層での要求にあわせてアンテナの指向性を制御することにより，認証時のように重要な情報を確実に無線通信することが可能となる．

無線 LAN においては傍受や乗っ取り等，保安上の問題がある．特に本提案では無線部分を他者と共有しているので，実運用での保安対策が必要であると思われる．また，無線 AP 間のハンドオーバーは無線 AP の実現に依存しているため，無線 LAN クライアントを高速移動体に搭載する場合は，その利用形態にあわせたシステム設計が必要となる．

文　献

[1] Farinacci, D., et al, Generic Routing Encapsulation (GRE), RFC2784, Mar. 2000.

[2] Mamakos, L. *et al*, A Method for Transmitting PPP Over Ethernet (PPPoE), RFC2516, Feb. 1999.

[3] Hamzeh, K. *et al*, Point-to-Point Tunneling Protocol (PPTP), RFC2637, Jul. 1999.

[4] Kent, D., et al, IP Authentication Header, RFC2402, Nov. 1998.

[5] 浅川　公男，裕川　昌子，馬場　聡史，前田　忠彦、PC クラスタによるアンテナ解析の高効率化の検討，信学技報　AP-2003-*，Mar. 2004 (to appear).

[6] R. O. Schmidt, Multiple Emitter Location and Signal Parameter Estimation, IEEE Trans., vol. AP-34, No.3, pp. 276-280, Mar., 1986.

[7] 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，情処研究報告 2002-DPS-107, Mar. 2002.

[8] DHIS, ATNCPC, Automatic Tunnel Configuration Protocol, tunnel broker, http://www.dhis.org/atncpc/

[9] Gilligan, R., *et al*, Transition Mechanisms for IPv6 Hosts and Routers, RFC2893, Aug. 2000.

[10] Housley, R. *et al*, EtherIP: Tunneling Ethernet Frames in IP Datagrams, RFC3378, Sep. 2002.

[11] http://www.hotspot.ne.jp/

[12] http://www.freespot.net/

[13] 藤川 賢治，岡部 寿男，古村 隆明，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，情処研究報告 2003-DPS, Mar. 2002.

[14] Perkins, C., IP Mobility Support, RFC2002, Oct. 1996.