IPv4無線LANホットスポットへのIPv6リーチャビリティ提供技術の開発

青島 史郎　　藤崎 智宏　　三上 博英
NTT情報流通プラットフォーム研究所

IEEE802.11bに準拠した無線LAN製品の普及に伴い、公衆エリアでの無線LANアクセスポイントからのインターネット接続への期待が高まっている。実際に国内外において、公開実験や商用サービスなどによる無線LANホットスポットサービスが行われている。
本稿では、このように今後さらなる注目が予想される無線LANホットスポットに対し、既存のIPv4ネットワーク／システムへの影響を与えずに、IPv6 インターネットへの接続性を提供する技術について報告する。

Providing IPv6 Reachability for IPv4 Wireless Hotspots

Shirou AOSHIMA　　Tomohiro FUJISAKI　　Hirohide MIKAMI
NTT Information Sharing Platform Laboratories

The expectation for the Internet connectivity from the wireless LAN access point in public area is growing with the spread of the wireless LAN products based on IEEE802.11b. Inside and outside the country, wireless LAN hotspot service by an open experiment, commercial service, etc. is actually offered. This paper reports the technology providing IPv6 reachability for the wireless LAN hotspot, where the further attention will be expected from now on, without having influence of the IPv4 network / system on existing.

1　背景

ADSLやCATVなどの常時接続サービスの低価格化が進み、インターネットは一般家庭に広く普及してきた。そんな中で、近年では無線を用いたインターネット接続やLAN構築に注目が集まっている。特に、IEEE802.11bの標準化に伴い、市販の無線LAN製品が普及し、無線LANの利用は爆発的に増加し始めている。

インターネットへの接続性を提供するサービスプロバイダにおいても、アクセス回線として無線技術を利用することが注目されている。実際に、国外では既に無線LANアクセスを提供するホットスポットが商用サービスとして始まっており、国内においても各種の実験が始められている[1]。

日本では、NTT DoCoMoのiモードサービスが爆発的に普及し、無線を用いたインターネットアクセスの需要の可能性を示している。最近では、携帯電話よりも画面サイズが広く、マシンパワーも優れているPDA端末が売行きを伸ばしており、新たな市場として期待されている[2]。PDAに対応したPHSや無線LANカードなども多数販売されるようになり、携帯端末からのインターネット接続は、今後も増加が予想される。

このように、無線でのインターネット接続サービスを考えた場合、携帯端末からのインターネット接続を無視する事はできない。無線LANを用いたホットスポットサービスが普及すると、ノートPCやPDAなどの多くの携帯端末が、ホットスポットを介してインターネットへ接続することになる。しかしながら、現在のインターネットの標準であるIPv4では、今後数の増加が予想されるPDAなどの携帯端末全てに対して、

グローバルなIPアドレスを割り振る事は不可能である。そのため、外部ネットワークからその端末を特定することは不可能となり、本来のインターネットの使い方である端末同士での情報のやり取りを実現できない。

このような状況を打開する仕組みとしてIPv6が存在する[3]。アドレスが24ビット長であるIPv4に対し、128ビット長のアドレスを持つIPv6を用いれば、全ての携帯端末に一意のアドレスを割り振る事が可能となる。

また、IPv6には、ネットワーク設定の自動化、セキュリティ機能の標準実装、経路テーブルの効率化など、今後発展が予想される無線アクセスサービスを行う上で必要な機能を備えており、IPv6技術の普及は必要と言える。

しかしながら、現状では、公衆エリアでのアクセスポイントとして使用できるようなIPv6対応機器が不足している。そのため、現在行われている無線LANホットスポットサービスは、どれもIPv4のみの対応となっており、IPv6の利用は想定されていない。

また、無線LANにおけるセキュリティ技術の不足も指摘されている。無線LANを用いた場合、電波の届く範囲であれば誰でも使用できる可能性がある。特に、公衆エリアにおいて不特定多数のユーザを対象とするホットスポットサービスにおいては、重要な要素である。

現状では、無線LANアクセスポイントを使用可能な端末として特定する手段として、ESS IDによるアクセス制限や、事前に登録されたMACアドレス以外からのアクセスを拒否する方法などがある。

無線LANにおける通信の暗号化方式として、WEP(Wired Equivalent Privacy)と呼ばれる方式が用いられているが、全てのユーザに共通の鍵を用いるため、鍵の配布や更新、対象者以外への鍵の漏洩など、多くの問題点が指摘されている[4]。

そこで、本稿では、IPv4で提供されている無線LANホットスポットに対し、既存のIPv4ネットワーク／システムに影響を与えずに、IPv6リーチャビリティ及びセキュリティ機構を提供するシステムについて述べる。本システムは、既存IPv4無線LANホットスポットにIPv6用ゲートウェイ（以下IPv6 GW）を新たに設置することにより、IPv6インターネットへの接続性を提供する。

以下、第2章で本システムの概要を述べ、第3章では本システムの核となるIPv6 GWの機能について説明する。第4章では、IPv6 GWの実装について述べる。第5章において実装を行ったIPv6 GWに対する検証を行った後、第6章でまとめる。

2 IPv6 GWの概要

2.1 IPv4無線LANホットスポット

図1に本システムで想定する既存IPv4無線LANホットスポットの構成図を示す。環境は以下を想定する。

- ホットスポットにおいて、ユーザへ無線LANによるIPv4インターネット接続を提供する。ユーザへのIPv4アドレス付与はDHCP[5]により実現する。
- 予めユーザに付与したユーザID及びパスワードを用いた認証を行う。
- 認証結果と連携したアクセス制御を行う。

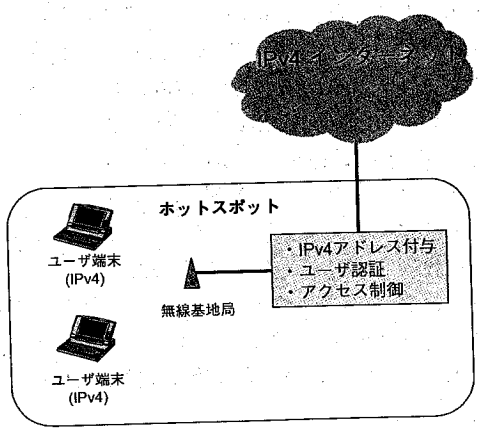

図1 既存IPv4無線LANホットスポットの構成図

想定するホットスポットでは、ユーザ認証及びその結果と連携したアクセス制御を行う事により、許可されていないユーザの不正利用を規制している。

2.2 IPv6 GW の特徴

本システムは、2.1 で示したような IPv4 無線 LAN ホットスポットに対し、IPv6 GW を新たに設置することにより、ホットスポットを使用するユーザに IPv6 インターネットへのアクセスを提供する。提案システムの構成図を図 2 に示す。

IPv6 GW は、以下に示す 4 つの機能を持つ。

(1) ホットスポットに接続されるノードに対する IPv6 アドレスの付与
(2) 上位 IPv6 ネットワークへの接続性の提供 (Native／トンネル両方に対応)
(3) ユーザの認証機能 (必要に応じ、既存 IPv4 ホットスポットのユーザ認証との同期をとる)
(4) 認証と連携したアクセス制御機能

IPv6 GW はユーザ認証、アクセス制御など、既存のシステムで要求されている機能を有しているため、既存 IPv4 無線 LAN ホットスポットは、IPv6 GW を設置するだけで、IPv6 インターネットへのアクセスを提供することが可能となる。同時に、既存のネットワーク／システムへの影響を最小限に抑えることも可能である。

また、ホットスポットへの IPv6 ネットワークの Native な接続がない場合でも、IPv6 over IPv4 トンネリング接続を利用することで、IPv6 接続性の提供が可能である。

3 IPv6 GW

本章では、提案する IPv6 GW の各機能について説明する。

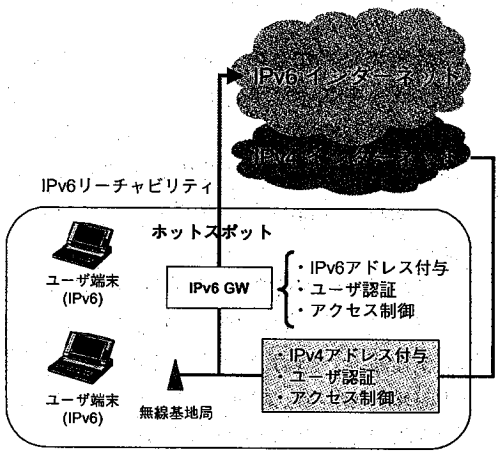

図 2 提案システムの構成図

3.1 IPv6 アドレスの付与

IPv6 の自動設定機能を用いて接続端末に IPv6 アドレスを付与する。

IPv6 アドレスは 128 ビットの長さを持っているため、ノート PC に限らず、PDA など、今後数の増加が予想される全ての携帯端末に対しても、グローバルアドレスを附与することが可能である。

3.2 上位 IPv6 ネットワーク接続

既存のネットワーク／システムの関係上、IPv6 の Native なネットワークをホットスポットに直接接続することが困難な場合は、既存 IPv4 ネットワークと IPv6 上位ネットワークとの接続点にトンネルサーバを設置する。このトンネルサーバと IPv6 GW との間に、IPv6 over IPv4 トンネルを張ることにより、新たに IPv6 用のネットワークを構築することなく、上位 IPv6 ネットワークへの接続を提供する。

このような接続を実現するため、IPv6 GW は IPv6 over IPv4 トンネルサーバの機能を持つ。

3.3 ユーザ認証機能

公衆エリアからのインターネット接続を行うホットスポットにおいては、ユーザ認証は重要な機能である。IPv6 GW では、認証サーバを用いた認証機構を実現しているが、任意の認証技術を実装することが容易である。

また、IPv6接続性を、既存IPv4無線LANホットスポットに対する付加機能として実現する場合、既存ユーザ認証との連携が必要な場合がある。IPv6 GW ではこのような場合の対応も考慮している。

3.4 アクセス制御

認証されたユーザのみに外部ネットワークへの接続を許可するアクセス制御機能を持つ。

IPv6 の場合、一台の端末に対して割当てられる複数 IP アドレスへのアクセス制御が必要となる。

4 システムの実装

対象とする既存 IPv4 無線 LAN ホットスポットを想定し、第 3 章で示した IPv6 GW の実装を行った。

4.1 IPv6 GW の実装

3 章で述べた機能を、UNIX PC 上に実装した。OS は FreeBSD 4.4R を用い、IPv6 スタックは OS に組み込まれているものを使用した。

IPv6 GW は RA を発行し、IPv6 に対応したノードに対し、IPv6 グローバルアドレスを附与する。

認証システムは、IPv6 及び SSL に対応した Web サーバ上で動作する CGI を用いて、ユーザがユーザ ID 及びパスワードの入力を行うことにより実現する。この認証システムは、既存システムで用いられている認証サーバに対応するよう実装を行う。

ノードから認証システムへの接続は、リンクローカルアドレスによる通信を用いる。リンクローカルアドレスを用いることにより、将来 IPv6 GW がプレフィックスの異なる複数のホットスポットに導入されたとしても、ホットスポットごとに IPv6 GW のアドレスを変更する必要がなくなるため、運用が容易に行える。

また、認証を受けたノードに対してのみ、外部ネットワークへのアクセスを許可するようなアクセス制御機能も実装し、認証を受けていないユーザからの不正アクセスを制限する。

IPv6 ネットワークとの Native な接続がないホットスポットに対応するため、IPv6 GW にトンネルサーバとしての機能も実装している。

4.2 動作の詳細

実装を行った IPv6 GW を導入した無線 LAN ホットスポットのシステム構成図を図 3 に示す。実際の処理の流れを以下に示す。

(1) RA による IPv6 グローバルアドレスの割り当て

IPv6 に対応したノードは、無線基地局を経由して RA を受信し、IPv6 グローバルアドレスを生成する。

(2) Web サーバを用いたユーザ認証

ユーザは、予め周知されている Web サーバのリンクローカルアドレスに対し、IPv6 リンクローカルアドレスに対応した Web ブラウザを用いてアクセスする。CGI を用いてユーザ ID 及びパスワードを入力し、認証サーバに問合せを行い、認証を受ける。ユーザと Web サーバとのセッションは SSL により暗号化されている。

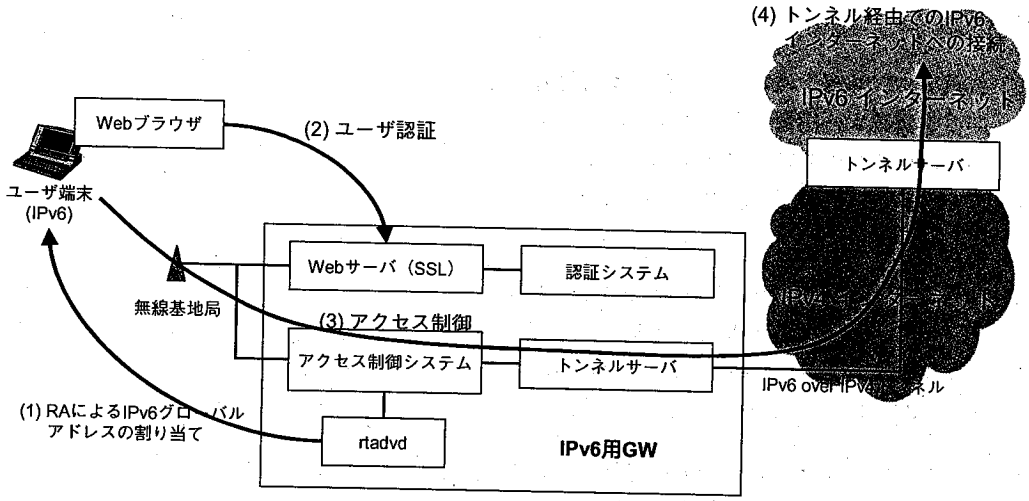

図3　IPv6 GWを導入した無線LANホットスポットのシステム構成図

(3) 認証と連携したアクセス制御

ユーザ認証されたノードに対するアクセス制御を変更し、外部アクセスを可能にする。

(4) トンネル経由でのIPv6インターネットへの接続

ユーザはIPv6 over IPv4トンネルを経由し、IPv6インターネットへ接続する。

5　本システムの評価

IPv6ネットワークにおける無線LANアクセスを制御するために本システムを導入し、検証を行った。ユーザは、外部ネットワークへアクセスする際には、本システムのユーザ認証システムにより認証処理を受ける必要がある。本システムでは、認証を受けたユーザに対してのみ、外部ネットワークへのアクセスを許可することにより、無線LANアクセスにおけるアクセス制御を実現する。

IPv6 GWは、IPv4無線LANホットスポットに対するIPv6ネットワークへのアクセス提供のみならず、IPv6ネットワークにおける、無線LANアクセス制御を行うゲートウェイとして機能させることも可能である。

また、このIPv6 GWを介して、IPv6音声アプリケーションによる通話実験を行った。音声アプリケーションが使用する帯域は256kbpsとなっており、多少の遅延は認められたものの、通常の会話を行える程度の品質であった。

6　まとめ

本稿では、既存のIPv4無線LANホットスポットに対し、既存ネットワーク／システムへの影響を与えずに、IPv6リーチャビリティを提供する技術について提案し、その実装であるIPv6 GWについて述べた。

本システムを、IPv6ネットワークにおける無線LANアクセス制御のために導入し、その有用性を確認した。

今後は、実装システムの改良を進めると共に、MobileIPv6技術による固定グローバルアドレスを用いた通信の実現、IPv6の標準となっているIPSec[6]を利用した認証、セキュリティの確保等を実現していく予定である。

参考文献

[1] 高槻芳, “‘本家’モバイルを脅かす新勢力 エリア重視か, 圧倒的な安さかモバイル通信 2000 年への展望”, 日経コミュニケーション, 11 月 5 日号, no.353, pp.114-122, 2001 年 11 月

[2] 枝洋樹, 進藤智則, “無線 LAN と PDA に望みを託す IT 不況の突破口を模索”, 日経エレクトロニクス, 12 月 3 日号, no.810, pp.57-64, 2001 年 12 月

[3] S. Deering and R. Hinden: "Internet Protocol, Version 6(IPv6) Specification", RFC2460, p.39 (1998)

[4] “ISAAC, Security of the WEP algorithm”, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[5] R. Droms: “Dynamic Host Configuration Protocol”, RFC 1541, p.39 (1993)

[6] S. Kent and R. Atkinson: "Security Architecture for the Internet Protocol", RFC2401, p.66 (1998)