分散システム／インターネット運用技術 21－2
（2001．5．25）

大学キャンパス無線アクセスシステムの構築

篠宮 俊輔　萩原 洋一

東京農工大学 総合情報処理センター

概要

IEEE802.11b 無線 LAN 製品の普及に伴い、大学キャンパス内においても無線 LAN による学内ネットワークやインターネットへのアクセスの要望が高まっている。しかし、現在主流の安価に提供されている無線 LAN 製品は一般家庭や小規模オフィスなどを対象としているため、キャンパスにおいては、それらの利用形態をそのまま当てはめたサービス提供は難しい。大学のキャンパスという比較的部外者の出入りが自由で、多人数が生活する場所での接続サービスの提供には利用者のプライバシー確保、セキュリティ、不正利用対策などの問題が伴う。また、サービスエリアが広範囲に及ぶため、多数の無線 LAN のアクセスポイントの管理についても考慮しなければならない。

本稿では、上記問題に対応する一つの方式として、市販無線 LAN と VPN を組み合わせたキャンパス無線アクセスシステムの構築と運用について述べる。

A construction of wireless access system in campus

SHINOMIYA Shunsuke, HAGIWARA Yoichi

General Information Processing Center, Tokyo University of Agriculture and Technology

Abstract

The requests of access to the intramural network and the Internet using wireless LAN are raising in the university campus with popularization of IEEE 802.11b wireless LAN products. However, because the mainstream wireless LAN products low priced offered are targeting use at a home, small scale office, etc., service provide which applied these use form as it was is difficult in the campus. The provide of access service involves privacy reservation of a user, security, problem of wrong utilization in the campus where outsider can visit comparatively free and a lot of people live. And, because a service area reaches widely, we should consider about management of the many access point of wireless LAN.

In this paper, we describes the construction and management of a wireless access system in campus which combined a general wireless LAN product and VPN as one system solution for the above mentioned problem.

1. はじめに

ノート PC の普及に続いて安価な一般向け無線 LAN 製品の出現と普及により大学においても無線 LAN を用いた学内ネットワークやインターネットへのアクセスサービスの要望が高まっている。IEEE802.11b 無線 LAN 製品は、従来の無線 LAN 製品と比べ、標準化されたことなどを理由に安価に提供され、家庭、小規模オフィス向け無線 LAN 製品が大学生協、PC ショップなどに行けば容易に目にすることができるようになり、一万円を切る価格の無線 LAN カードも出現しつつある。

しかし、物理メディアとして無線を用いているため、ケーブルの敷設などコストや手間、利用可能場所の制約などが有線 LAN と比べて低くなった一方で、無線 LAN アクセス設備の利用者、提供者ともにセキュリティ、プライバシー確保について考慮しなければならない部分が多くなっている。

また、家庭や小規模オフィスを対象とした無線 LAN 製品は、一台～数台の無線 LAN のアクセスポイント(以下、AP)により構成され、利用者数が数名～数十名程度の規模を想定しているため、キャンパス内ネットワークのようにサービスエリアが広く、多数の利用対象者を抱える大学キャンパスなどにおいては無線 LAN 製品ベンダが利用形態として提案するようなネットワーク構成や、標準添付の管理ツールを用いての運営を行うことは難しい。

東京農工大学総合情報処理センターでは、上記の点に対応した、大学教職員、学生、研究生が市販の無線 LAN 製品を用いて手軽に学内ネットワークにアクセスできることを目的としたシステムを構築し、運用を開始した。本稿では、キャンパス内をサービスエリアとし、WEP、MAC アドレスフィルタリングおよびVPN接続時の個人認証を組み合わせた「キャンパス無線アクセスシステム」の構築、運営について述べる。

2. システムの概要

本システムは、東京農工大学小金井キャンパス内各所をサービスエリア(図 1)とし、教職員、学生、研究生合計 6,500 人の利用対象者に、学内ネットワークへの無線によるアクセス手段を提供している。本学もう一つのキャンパスである府中キャンパスについても、同様のシステムによりサービスを開始する予定である。

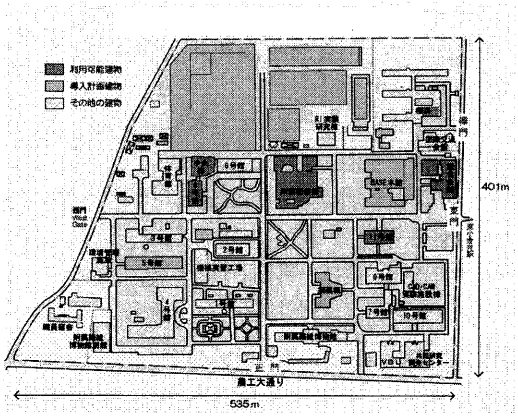

図 1 無線アクセスシステム
サービスエリア(小金井キャンパス)

2.1 システム構成

図 2 に本システムの構成図を示す。システムの構成は無線ネットワーク管理サーバ、VPN サーバ、認証情報サーバと 38 台(2001 年 4 月現在)の AP である。各種サーバと AP 間の接続は、建物間が 100baseFX、建物内は 100baseTX で接続し、一部の AP については LAN 間接続用無線 LAN 機器を用いて接続している。無線ネットワークは、学内ネットワークとの間でパケットフォワーディングは行わない独立したネットワークとしている。また、無線ネットワークは VPN サーバへ接続するためのインフラストラクチャとして用い、無線ネットワーク内で利用できるアプリケーションサービスは提供していない。学内ネットワークの各種リソースを守るためにサンドイッチ構造としている。

2.2 無線ネットワーク管理サーバ

本システムを構成する AP の管理および無線ネットワーククライアントのための DHCP サービス、名前解決サービスおよび、AP 管理ツールの実行を行う。DHCP は、クライアントが VPN サーバへ接続するための IP 設定情報を提供し、割り当てられる IP アドレスはプライベートアドレスである。名前解決サービスは、BIND のラウンドロビンによる VPN サーバへの接続の分散などのために設置している。

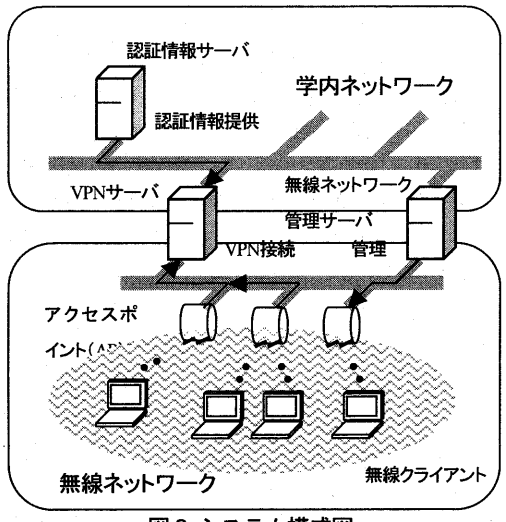

図2 システム構成図

2.3 VPN サーバ

無線ネットワーククライアントを学内ネットワークへ接続するための VPN サーバである。本システムを利用するクライアントは、各人のパスワードによる認証を受け、VPN サーバと接続することによりグローバル IP アドレスが割り当てられ、学内ネットワークへアクセスできる。

VPN プロトコルとして PPTP[1](Point-to-Point Tunneling Protocol)を用い、認証プロトコルに CHAP、MSCHAP、MSCHAPv2、暗号化プロトコルとして MPPE(40bit、128bit)を利用可能である。VPN サーバは、負荷分散、障害対策のために複数台設置している。

2.4 認証情報サーバ

VPN 接続時のアカウント認証情報を提供するサーバである。本システムの認証情報は、メールアカウントを用いており、認証情報サーバはメールサーバである。

2.5 アクセスポイント(AP)

AP は、メルコ社製 WLA-L11[1]を使用している。本 AP 一台あたり 20～30 クライアントが同時に利用することが可能であり、金属遮蔽物のない見通しの良い屋内で 25～50m、屋外で 160m 程度の範囲が通信可能エリアとなっている。

AP により無線 LAN カードのフィルタリングを行っており、無線ネットワークへはシステムの利用登録が行われている無線 LAN カードだけが接続できる。

3. 利用者認証とプライバシーの確保

大学キャンパスは、事実上、学外の人間も出入りが自由となっている。また、無線を媒体としているため通信状況が良ければキャンパス外でもキャンパス内設置の無線 LAN 設備を利用できる可能性がある。そのため不特定多数の人間からのアクセスが可能であり、それらへの対策なしではサービスを提供することは難しい。

無線 LAN 製品はセキュリティ対策として、IEEE802.11b オプションの WEP(Wired Equivalent Privacy)の他にもセキュリティ向上のための機構が用意されているものがある。本システムを構成している AP にも WEP(40bit)の他に MAC アドレスベースのフィルタリング機能が備わっている。そこで本システムでは、WEP、MAC アドレスフィルタリング、VPN 接続時の認証と暗号化を組み合わせることにより利用者の把握、不正利用防止、利用者のプライバシー確保に備えている。

3.1 WEP による暗号化

WEP により、通信内容を暗号化することにより WEP キーを知る者以外に対してセキュリティを確保することができる。しかし、WEP は暗号化、復号化に同一の WEP キーを用いるため、利用対象者が数千人いる環境ではキーの配布、更新や利用対象者以外へのキーの漏洩を防ぐことは難しいと考えられる。また、WEP キーを共有している者の間では、シェアード HUB を用いて構成した有線 LAN に接続している場合と同様に、同一セグメントの利用者同士で容易に通信内容を確認することが可能である。更に、WEP はアルゴリズム上の脆弱性も指摘されている[3]。

3.2 MAC アドレスベースフィルタリング

AP に利用者の無線 LAN カードの MAC アドレスを登録することにより、それ以外のカードからの AP への接続を拒否することができる。利用者の MAC アドレスについては、利用者登録時に MAC アドレスを受付け、リストを作成している。

本システムを構成している AP では、登録できる MAC アドレスの数の上限が 255 アドレスとキャン

パスでのサービスを考えると小さいものとなっている。この件については、AP のメーカ側に対策を依頼するとともに、後述の管理ツールにより対処することを考えている。

上記二つの AP によるセキュリティ対策は、環境によっては有効に機能するが、無線ネットワークをキャンパス展開するには不十分である。AP による MAC アドレスベースのフィルタリングは利用対象者、非対象者の選別に対して有効な手段ではあるが、登録済み無線 LAN カードの紛失、盗難や MAC アドレスの詐称に対しては無力である。そのため、これら機能だけで利用対象者と非対象者を区別することは難しい。

3.3 VPN による利用者認証、記録、暗号化

本システムでは、前述の AP によるセキュリティ対策の他に、VPN を用いて利用者の認証および利用者記録の取得、プライバシーの確保を行っている。VPN のプロトコルとして PPTP 採用している。PPTP は、TCP/IP ベースのネットワークをインフラストラクチャとしてクライアント、サーバ間でトンネリングを行い、エンドツーエンドの通信内容の暗号化が可能である。本システムではサーバ、クライアント間の通信内容を暗号化することにより、WEP キーを共有する者の間であってもプライバシーを確保できるようにしている。

VPN プロトコルとして PPTP を選択した一つの理由として、PPTP が無線アクセスシステム利用対象者の多くが Microsoft Windows を利用しており、PPTP が Windows の標準機能(「仮想プライベートネットワーク」)として用意されていることである。仮想プライベートネットワークは Windows98、Me においては標準でインストールされないが、簡単な操作でインストール可能である。Windows95 についてはアップデートモジュールで対応できる。また、Microsoft Windows 以外の OS についても、Linux、FreeBSD、NetBSD、MacOS において別途ソフトウェアをインストールすることにより利用可能である。ただし、MacOS 環境については、現在のところ無償で使用できるクライアントプログラムが見つかっておらず、有償のプログラムについても暗号化を行った場合の動作が確認できていない。

また、「仮想プライベートネットワーク」は、「ダイアルアップ接続」のインタフェースで提供されているため、利用者の多くが設定、利用の経験があると思われる電話での ISP へのダイアルアップ接続と同様の感覚で扱うことができる。また、Linux、FreeBSD、NetBSD などで利用可能な PPTP クライアントプログラムについても、PPP 接続とほぼ同様の設定、利用方法が可能となっている。そのため、オンデマンドダイアリング機能により、接続操作の手間を省くこともできる。

VPN 接続時の認証情報には、メールのアカウントと同一のパスワードを用いている。インターネットへの接続サービスを提供した場合、利用者アカウントの部外者への安易な貸し借りが行われる可能性があるが、認証情報をメールアカウントと同一とすることによりそれらの行為を抑制することを意図している。

4. 広範囲なエリアでの提供

キャンパス内各所での無線接続サービスの提供を検討し始めた当初、サービスの上で問題の一つとなったのが広範囲なエリアでの提供に伴う問題であった。大学のキャンパスという多数の建物が広範囲に建ち並ぶ場所でのサービス提供は、クライアントへ割り当てる IP セグメントとそのアドレスの数の割当てや、それらのアクセス制御および、キャンパス内に点在する多数の AP の管理が問題となった。

4.1 広範囲なエリアでの提供に伴う問題

本学では、既設の有線学内ネットワークでは、建物、フロア毎にネットワークセグメントを割り当てているが、そのセグメントの延長として無線ネットワークを接続しようとした場合、次の二点が問題となった。

(1) AP とクライアントへの IP アドレスの割当て

無線 LAN クライアントから学内ネットワークへ接続するためには、接続先の AP が近くの学内ネットワークへ有線 LAN で接続する必要がある。しかし、AP はキャンパス内の各所に点在することになるため、既存の学内ネットワークを利用した場合には、それらを同一の IP ネットワークセグメントに接続することが難しい。AP 毎に異なった IP セグメ

ントに接続すると、無線 LAN のクライアントがローミングを行った場合、IP の設定については利用者は接続する AP を意識しなければならない。また、無線 LAN クライアントへグローバル IP アドレスを与える場合、サービスエリア毎に利用者数を見越した IP アドレスの割当てを行わなければならず、相当な数のアドレスを無線アクセスシステムのために割り当てなければならない。これらは現実的な構築ではない。クライアントへはプライベートアドレスだけを割り当て、NAT やプロキシサーバによる構成を取ることもできるが、クライアントで利用できるアプリケーションの制限や、アドレス変換後のグローバルアドレスから実際の利用者を特定することが難しいためそのような手法は選択しなかった。

(2) アクセス制限

既存学内ネットワークに AP を設置し、無線サービスを行った場合、前述のように学外者など、AP 設置前には想定していなかった利用者からのアクセスが行われる可能性がでてくる。そのため、クライアントが、既設の有線 LAN での接続なのか無線 LAN での接続かを判別し、有線 LAN のクライアントよりも厳しいアクセス制限をかける必要がでてくる。しかし、アクセス制限をかけるためには AP 毎に追加設備が必要となり、それら機器の設置のコストや管理の手間が大きくなってしまう。

4.2 本システムによる対応

サービス提供検討時に問題となった上記二つの事項についても、本システムは、既設学内ネットワークとは別の無線ネットワーク IP セグメントの設置と VPN によるクライアントへの一時的なグローバル IP アドレスの割当てにより解決している。

無線ネットワークは、既設のキャンパス内ネットワークの空き光ファイバーを用いキャンパス各所に設置された AP を接続し構成している。無線ネットワークには単一のクラス B のプライベートアドレスを割り当て、全ての AP と無線 LAN クライアントを同一 IP セグメントにおさめている。そのため、クライアントが AP 間を移動した場合でも他の IP セグメントへ紛れ込むことや、DHCP サーバからの設定情報の再取得などの手間が必要なくなり、ローミング時にも IP の設定について意識をする必要がない。また、クライアントへ割り当てるグローバル IP アドレスについても、同時にサービスを受けるクライアントの数だけ用意するだけでよく、効率の良い IP アドレスの利用ができる。

5. AP の管理

本システムで採用している AP は、Web ブラウザで容易に管理できることを特徴としている。しかし、管理する AP が数十台となる本システムでは、一台ずつマウスとキーボードを併用しての設定は手間がかかる。また、フィルタリング用の MAC アドレスのリストについても多数の MAC アドレスを誤りなく数十台の AP に登録することは現実的ではない。

そこで、Perl 言語により AP 管理ツールを作成、運用に用いている。この管理ツールは、HTTP により AP にアクセスし、AP の設定の取得および変更を行う。システムを構成する AP の ESS-ID、WEP キーやネットワークインタフェースの設定などの共通設定と、AP 名、使用する無線チャネルの設定など AP 個別の設定を分けて記述することができ、管理作業の省力化に役立っている。図 3 は、管理ツール用設定ファイルの一部である。

```
default{
        DUPLEX = HALF
        DHCPC = ON
        GROUP = xxxxxx
        ESSID_TYPE = INPUT
        ESSID = xxxxxx
        ROAMING = ON
        WEP_TYPE = HEX
        WEP = xxxxxxxxxx
}
172.24.0.17{
        NAME = COOP_1F_Cafe
        CHANNEL = 1
}
172.24.0.18{
        NAME = COOP_1F_Diner2
        CHANNEL = 9
}
```

図 3 管理ツールの設定ファイルの一部

また前述のように、本システムを構成している AP の MAC アドレスフィルタリングリストは一台あたり 255 エントリまでしか登録できない。この制限による問題を解決するために、現段階では実運用は行っていないが、本来静的なフィルタリングリストを動的に書き換えるツールを作成した。このツー

ルは、APから得られる、

・フィルタリングリスト

・現在接続中のクライアントのリスト

・フィルタにより接続拒否されたMACアドレスのリスト

および、本システムで利用が許可された無線LANカードのMACアドレスのリストを入力として、接続許可リストを動的に書き換える。しかし、APの持つ上記三つのリストの取得とフィルタリングリストの更新にHTTPを用い、また、最新のリスト取得のために全てのAPに対して絶えず十秒程度の間隔でポーリングを行わなければならいため、あまり現実的ではない。また、接続許可リストを更新している間の一秒程度の間、APとして機能しなくなるため、クライアントの通信がその時間だけ停止してしまうという問題も残されている。

6. 大学生協との連携運用

登録業務などのアウトソーシングとして、本システム利用者登録を生協に依頼している。具体的には、利用者登録作業として学生証、職員証の提示をもとめ、学籍番号、氏名などの個人識別と無線LANカードのMACアドレスとの関連付け登録作業を行っている。APでのフィルタリング用MACアドレスリストは、このデータを元に作成している。

このことにより、総合情報処理センターは、本システムの運用管理に専念することができる。また、生協は新入生を対象として、無線LANカードを標準添付したノートパソコンの販売を独自に行っている。

7. おわりに

本稿では、市販無線LAN製品を用い、大学キャンパスという広いエリアにおいて、学内ネットワークへの無線アクセスサービスを提供するシステムの構築と運用について述べた。

本システムにより、無線LANを用いながらも、VPNにより通信内容を暗号化し、個人認証を伴ったセキュアなアクセス手段を提供することができる。また、広いエリアにおける無線LANの展開方法と、その多数のAPを効率的に管理運用する事例を示した。

現時点では、無線ネットワークを介して接続できるVPNサーバは総合情報処理センター設置のサーバだけである。しかし、無線ネットワークとVPNを組み合わせた本システムは、学外からの来客用や研究室外からのセキュアな研究室サーバへのアクセスなどの利用目的別にVPNサーバを設置することにより、様々な用途に対応できる柔軟性も持っている。今後、学科単位、研究室単位などでVPNサーバの設置を許可、支援を行うことについても現在検討中である。

参考文献

[1]Bruce Perlmutter、Jonathan Zarkower著 、株式会社ドキュメントシステム訳、VPN入門、株式会社ピアソン・エデュケーション発行、2001年

[2] 株式会社メルコ WLA-L11製品仕様、http://buffalo.melcoinc.co.jp/products/catalog/item/w/wla-l11/siyou.html

[3] ISAAC、Security of WEP algorithm、http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html