# VPNを用いた学内無線LANサービスの運用方式

久保美和子・牧野　晋・大塚秀治・林　英輔
麗澤大学　国際経済学部
麗澤大学　情報システムセンター

概要

近年、大学の構内ネットワークにおいてモバイル環境を実現するために、無線LANは必須のものとなりつつある。しかし、大学のような比較的オープンな空間で無線LANをサービスするためには、セキュリティ面での配慮が必須である。麗澤大学では、ユーザ認証VLANスイッチを利用した無線LAN認証システムを運用している。このシステムでは、認証サーバに登録されている属性に従って所属VLANにマップされるため、ユーザごとのポリシーの適用がしやすいという利点がある。しかし、ユーザ認証VLANとの認証パケットを解析できれば、ユーザアカウントの入手が可能となる欠点がある。本稿では、麗澤大学の無線LANシステムの概要とその問題点を述べる。さらに、改良案としてVPNアクセスルータを用いた無線LANを運用する方策を提案するものである。

# The System of the Wireless LAN Service in the Campus LAN using VPN.

Miwako KUBO, Susumu Makino, Hideharu OHTSUKA, Eisuke HAYASHI
The International School of Economics and Business Administration
Reitaku University
Reitaku University Information System Center

Abstract

In recent years, in the network environment of a university, wireless LAN is becoming important. Then, it is necessary to consider security in order to serve wireless LAN. We implement the user authentication system using authenticated VLAN switch in Reitaku University. In this system, it is mapped by VLAN for every user according to the attribute registered into the authentication server. By this system, it becomes possible to reflect a network policy for every user. However, in this system, when the packet used for attestation is analyzed by methods, such as a packet capture, there is a problem of becoming possible to get user account information. In this paper, the outline the wireless LAN system of Reitaku University and the problem in the present environment are described. In addition, the safer wireless LAN system which strengthened security using the VPN access router is discussed.

## 1. はじめに

大学の構内ネットワークにおいてモバイル環境を実現するために、無線LANは必須のものとなりつつある。従来、大学では教室内や共有スペースに情報コンセントを設置し、持込みPCの利用環境が提供されてきた。しかし、情報コンセントではPCにケーブルを接続する必要があり、移動や着席の自由度が低い。このため、ケーブルレスで利用できる無線LANの要望が高くなりつつある。

麗澤大学では、2003 年 4 月より、従来の自営構内 PHS 網[1]によるモバイルサービスを IEEE802.11b ベースの無線 LAN に切り替えて運用を開始した。本稿では、学内無線 LAN サービスの概要と運用状況、その問題点を述べる。さらに、改良案として VPN アクセスルータを用いた無線 LAN を運用する方策を提案するものである。

## 2. 無線 LAN 利用の諸問題

無線 LAN は利用場所の自由度が高い反面、有線の情報コンセントと比較すると、いくつかの問題をもつ。主要なものを以下にまとめる。

### 2.1 AP の配置設計

全ての教室やパブリックスペースで利用可能にするためには、一定数のアクセスポイント(AP)の配置が必要となる。このため隣接する AP 間での干渉が問題となる。装置間の干渉を抑止するためには、利用チャンネルの割り当てプランを十分に検討する必要がある。特に大規模教室などでは 1 つの AP に収容できるユーザ数を勘案すると、複数個の AP を配置する必要がある。IEEE802.11b では利用できるチャンネル数が少ない[2]ため、設計上の制限が多い。AP は出力を調節できるものを採用することが望ましい。

### 2.2 セキュリティの問題

無線 LAN の利用に際しては、外部からの利用や盗聴を排除するために、AP の名前(SSID)と暗号化(WEP)キーを設定する。SSID はダイアルアップ接続であればアクセスポイントの電話番号に相当する。暗号化を行うことで、無線 LAN のスループットは低下するが、キャプチャされても解読される危険は減少する。暗号化のためには WEP キーと呼ばれる暗号化鍵の交換を行う。このキーは一般に 40 ビット長と 104 ビット長のものが用いられる。40 ビット長はテキスト文字なら 5 文字のパスワード強度に相当するので、安全とは言い難い。104 ビット長の WEP キーは、古い無線 LAN カードやドライバでは対応しないものも多く、利便性とのトレードオフとなる。

無線 LAN では暗号化していても、AP がビーコンと呼ばれる制御パケットを用いて SSID をテキスト状態で配信する。このため、部外者でも SSID は入手可能となる。また、ユーザへ利用方法を周知する資料にも SSID は印刷配布される必要がある。WEP キーも同様に文書で利用者に配布されるため安全ではない。

従って、SSID と WEP キーの入手は困難ではなく、無線 LAN の到達性を考えれば道端にシェアードハブが置かれている状態と考えればよい。このため WEP キーは適当な間隔で変更しなければならない。図 1 は無線 LAN のパケットをキャプチャ中の画面である。WEP キーを設定すれば、通常のパケットキャプチャと同様にアドレス、プロトコル、データなど全てを知ることできる。

この問題を解決する技術として IEEE802.1x がある。しかし、現状では対応している OS が少なく、大学のようなマルチベンダー環境で運用に持ち込むには課題も多い。

### 2.3 ユーザ認証の問題

無線 LAN でも、一般の情報コンセントと同様に、ユーザ認証を行わなければ、利用者を特定することは出来ない。前項の通り、SSID と WEP キーの対はユーザに配布されるため、誰がどの PC で利用したかというログが必要となる。また、同時に利用できないようにしなければ、アカウン

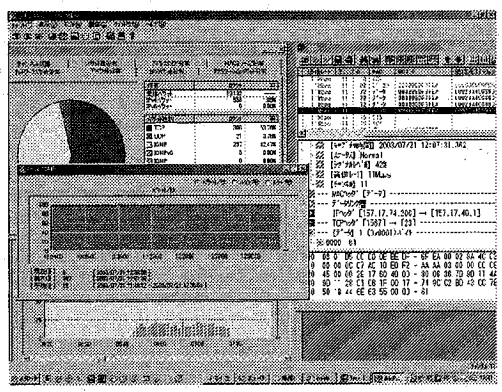

**図.1 無線 LAN のパケットキャプチャ**
WEP キーを入力すると解読パケットとして表示され、通常のパケットアナライザと同様にデータの内容を知ることが可能となる。

[1] 構内に複数の PHS アンテナを配置し、最大 32Kbps の通信を実現するサービス。通常のダイアルアップサービスと同様の技術を使うが、アクセスポイントに登録された PHS 子機を使うため、構内での利用時には通信料は不要となる。しかし、自営網に対応する子機の入手が困難になりつつあることや、PHS 自体の利用者の減少から無線 LAN への移行が計画された。

[2] Cisco 社製の AP などチャンネル自動割当機能を持つものがある。しかし、干渉を抑止するためには綿密な設置計画が必要となる。

トの共有や貸与や売買といった問題が生じる。

この問題は情報コンセントの利用と同様なので、従来の方法で解決できる。一般にこの問題の解決には、

1）認証付きゲートウェイを配置して、認証を受けなければ、外部への接続（インターネットサービスの利用）が出来ないようにする方法
2）ユーザ認証 VLAN 装置を配置して、認証を受けたものが、利用者属性に応じて、外部到達性のある VLAN にマップする方法
3）MAC アドレス認証を行い、登録された MAC アドレスを持つもののみが DHCP よりアドレス配布を受けて、ネットワークの利用を可能にする方法

などが採用されるが、導入コスト・運用コストを考えると一長一短である。特にキャンパス内の無線 LAN は駅周辺や飲食店などでサービスされるホットスポットと違い、インターネット接続だけできればよいというものではなく、LAN 内の

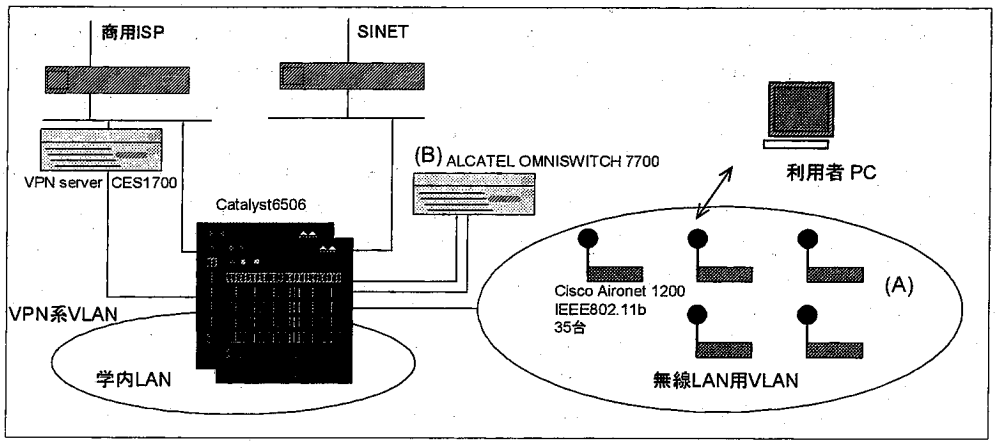


**図.2 無線 LAN の構成**

本学の無線 LAN ドメイン(A)は複数の Catalyst6506 で実現する VLAN 上に構成される。AP は Cisco 社製の Aironet1200 でカード交換で IEEE802.11a,802.11g に対応する。PC と AP 間は複数の WEP キーで認証接続され、WEP キーによって異なる VLAN にマップされる。通常は、デフォルトの VLAN にマップされ、更に図中(B)の ALCATEL 社製認証 VLAN スイッチ OS7700 を利用して認証を受ける。Catalyst と OS7700 間も 802.1qTagVLAN により接続されており、認証時にユーザ属性に従って所属 VLAN にマップする。この方法でユーザを特定できるが、WEP キーが漏れると無線 LAN 通信はキャプチャ可能となる。

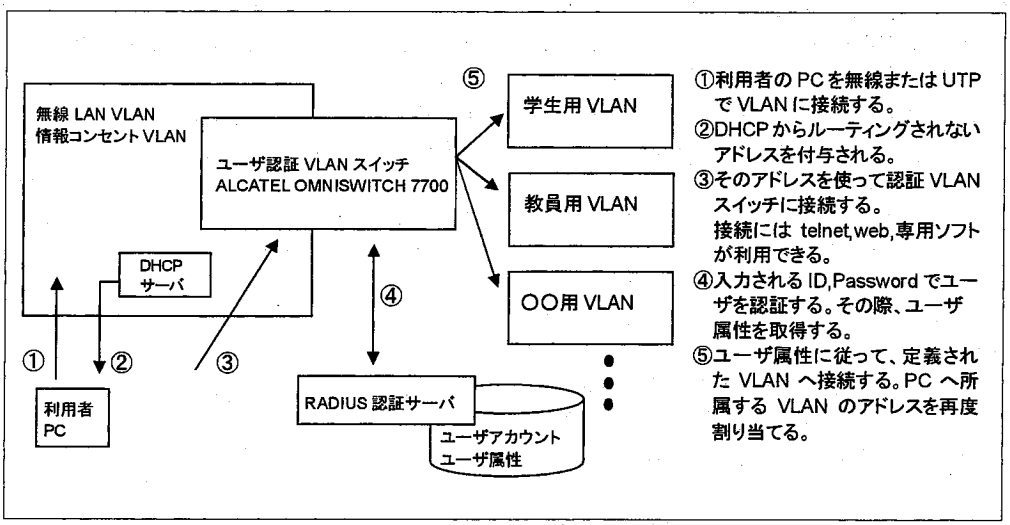


**図.3 無線 LAN へ接続する際の遷移図**

無線 LAN を学内 LAN に接続するまでの状態遷移を示す。図中の全ての VLAN は複数の Cisco6506 で構成されている。

資源にもアクセスできるようにする配慮が必要となる。

## 3. 本学の無線 LAN の構成

すでに述べたように、本学では 2003 年 4 月より、IEEE802.11b ベースの無線 LAN の運用を開始した。その構成を図 2 に示す。図のように、無線 LAN を収容する VLAN を複数台の Catalyst 6506 上に構成する。この VLAN 上に 35 台の Cisco 製 AP (Aironet1200)が接続されている。なお、本学情報システムの利用登録者数は約 4,000 名で、無線 LAN や情報コンセントサービスを利用する登録ユーザ数は約 100 名である。無線 LAN を必須とする授業は行われておらず、同時利用は最大でも 10 名以下である。この場合でも同一 AP に集中することはない。

利用者は SSID と WEP キーを自身の PC に設定し、最寄りの AP と接続する。この段階で、デフォルト VLAN に接続され、デフォルト VLAN 上の DHCP サーバから IP アドレスが割り当てられる。次に、そのアドレスを使って、ユーザ認証 VLAN スイッチである ALCATEL 社製の OS7700 を使って認証を受ける。認証には専用クライアントソフトまたは telnet または Web インターフェースが利用できる。

認証を受けると、認証サーバに登録されている属性に従って所属 VLAN にマップされる。例えば、学生は学生用 VLAN、教員は教員用 VLAN にマップされることになる。この方法では、利用者と利用者の無線カードの MAC アドレスが紐付けられるため、異なる AP に移動しても継続して利用が可能となる。接続までの状態遷移を図 3 に示す。接続の解除は、認証手順と同様のインターフェースでログアウトを明示的に行う必要がある。一定時間利用されない場合にはタイムアウトしてデフォルト VLAN へ再マップされる。このため、タイムアウト時には現在所属している VLAN が不明となるユーザが多く、リセット動作が煩雑となっている。

なお、AP の Aironet1200 自体が VLAN に対応するため、異なる SSID と WEP キーの対で別の VLAN に直接接続[3]させることも可能である。

本学のこの構成の場合、WEP キーが外部に漏れても、ユーザ認証 VLAN の認証が必要となるため、部外者が利用することは出来ない。しかし、WEP キーが外部に漏れると、図 1,図 5 に示すように簡単にキャプチャが可能となる。従って、ユーザ認証 VLAN スイッチとの認証パケットを解析すれば、ユーザアカウントの入手は容易である。

## 4. より安全な利用

前述のように、無線 LAN では WEP キーが漏れると簡単にパケットキャプチャが可能となる。大学などでは、利用ガイド等に SSID と WEP キーが印刷されて配布されることもある。このため、パケットキャプチャに対応する設計と運用が求められる。

大学における無線 LAN サービスは、商用のホットスポットサービスと同様に、セキュリティ的に保護されていないネットワークの利用と同じであると考える必要がある。ユーザはホットスポットやプロバイダと接続するように学内でも利用することになる。

無線 LAN サービス上で VPN 接続による利用を強制利用させることで、パケットキャプチャに対しても安全な利用環境を実現できる。本稿ではその方法として図 4 のようなシステムを提案する。

### 4.1 VPN 接続について

本来、VPN (Virtual Private Network) の技術は学外から学内へインターネットを使って安全にアクセスしたり、遠隔キャンパス間をインターネット越しに安全に接続したりするための技術である。

本学では従来 Notel 社のアクセスルータ CES1600/1700 を用いて VPN サービスを提供してきた[1]。この製品では、GUI によるクライアントソフト[4]を無償配布できるため、大学などユーザ数の多い環境では導入コスト、運用支援の面で都合がよい。

---

[3] この機能を使うことで、業務用 VLAN や学会や研究会に対応する外部公開用 VLAN を共通の無線 AP を使って同時に利用することができる。運用システムを使いながら、実験用 VLAN の構築もできるので利点は多い。

[4] ssh などオープンソフトを使っても簡単に実現可能であるが、VPN を強制的に利用させるためには導入やユーザサポートが手軽なものが望ましい。製品版であるため、セキュリティホールへの対応も早い。

### 4.2 構成と動作

図4に示すように、VLANを用いて無線LAN専用網を学内LAN上に構成する。網内にはAPの他DHCPサーバとVPNルータのみが置かれ、他のネットワークへの経路情報は定義しない。このため、仮にSSIDとWEPキーを入手しても、専用網内に接続できるだけである。

クライアントのPCはAPと通信を開始し、リンクが確立した時点でDHCPサーバからアドレスを取得する。利用者は学内情報資源やインターネット上のサービスにアクセスするために VPNルータへ専用クライアントソフトで接続を行う。VPNルータはIPアドレスやDNS、デフォルトゲートウェイを付与し、以降の通信を暗号化して保護する。

この状態で無線 LAN のパケットを既知のWEPキーを使ってキャプチャしたものが図5下の図である。利用者のパソコンに割り当てられたIPアドレスとVPNサーバのアドレス、UDPのパケットであることが分かるだけで利用しているプロトコルさえ解読できない。このため、暗号化データは入手することができるが復号は困難である。この方法では、無線LAN専用網と外部との接続点が1点であるため、確実にVPNを利用することを求めることができる。

### 4.3 問題点

この方法を用いることで、比較的安全に無線LANの利用が可能になるが、以下のような問題も指摘される。

1）SSIDとWEPキーが入手できれば専用網までは接続できるためDoS攻撃、ウィルスの伝播などの妨害活動が可能である。また、無線LAN専用網に接続中の、他のPCの情報が検索される可能性がある。

2）上記の問題を排除するためにMACアドレスなどの認証付きDHCPを用いたとしても、SSIDとWEPキーが分かれば、IPアドレスを手作業で設定することにより、同様の攻撃が可能となる。

このような問題は情報コンセントサービスでも同様に議論されてきたところであり、どこまでのリスクを許容するかは運用ポリシーに依存するものと思われる。ひとつの解決策としては、フロントエンド側に認証VLAN装置を置いて認証接続を行い、更に通信をIPレベルで暗号化する方法も一つの解決策である。

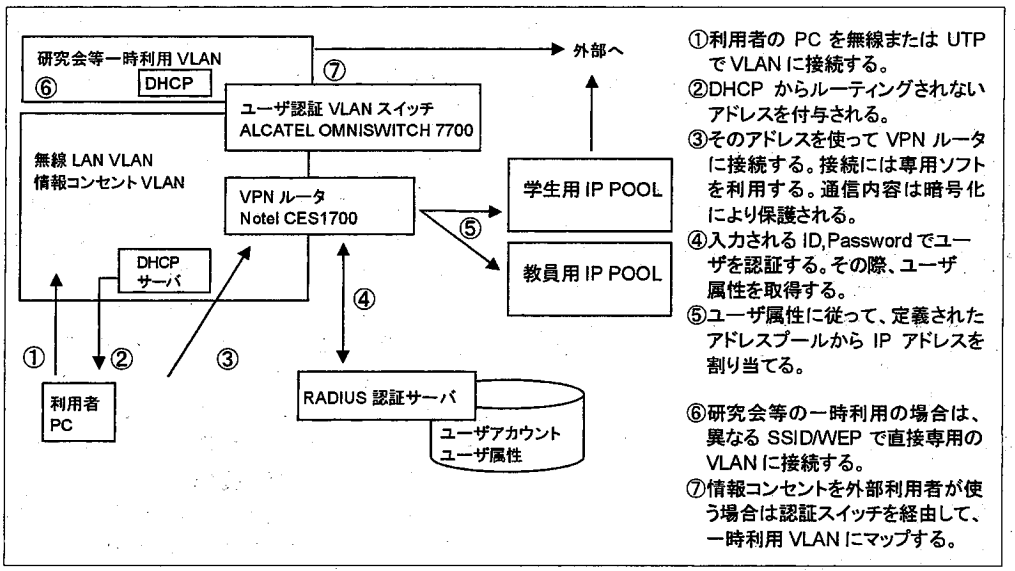


**図.4 提案するシステム**

VPNを用いて学内LANに接続するまでの状態遷移を示す。学内LANおよび学外との通信に際してはVPNの利用が必須となる。ただし、研究会等の一時利用の場合、当日限りのWEPキーを配布し同一APから直接研究会用VLANにマップする。このVLANを学内LANと遮断しておくことで一定のセキュリティを維持できる。研究会等で情報コンセントを利用する場合には、ユーザ認証VLANにより研究会VLANにマップすることができる。研究会VLANを利用するユーザ数にもよるが、装置内部のテーブルを利用することで認証サーバは不要となる。もちろん、認証サーバを共有することも可能である。

### 4.4 性能比較

図 4 で提案する方法では、利用者 PC と無線 AP 間および利用者 PC と VPN ルータ間で暗号化が行われることになる。VPN よる性能低下が許容できる範囲であるかを調べる目的で転送性能を、FTP を用いて測定した。転送は VPN ルータと異なる VLAN 上のファイルサーバとノート PC 間で行い、転送の内容はテキストファイル（約 15MB）と圧縮されたバイナリファイル（約 40MB）を用いた。WEP キーはそれぞれ 104bit 長を用いた。測定はファイルサーバから PC へのダウンロード（get）で、条件毎に 10 回繰り返した。また、インターネットからのダウンロードの速度をインターネット上の速度評価サイトを使って行った。いずれも同一の Proxy サーバを利用し、アップリンク回線は商用の 100Mbps のものを利用した。上位プロバイダも同一である。

図 6 は測定結果を bps に換算して示したものである。VPN ルータは圧縮機能を持つのでテキストファイルの転送速度が速くなる。他の条件では

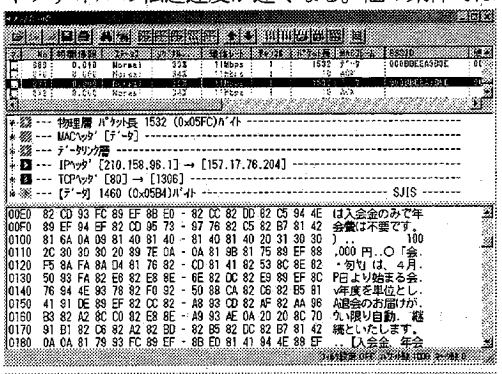

**図.5 パケットキャプチャの比較**

画面は、既知の WEP キーを使ってパケットキャプチャを行った結果である。上の図では転送データの内容が完全に読み取れる。下の図は VPN を利用した場合である。IP アドレスと UDP パケットであることは分かるが、内容は簡単に解読することはできない。

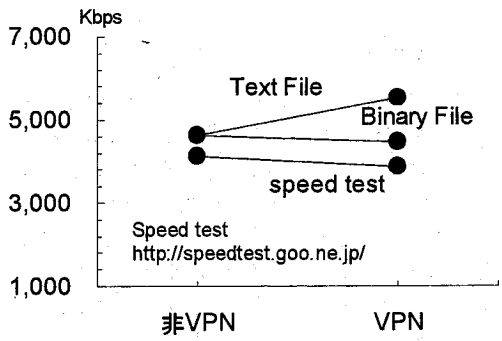


**図.6 転送速度の比較**

非 VPN ではファイルの種別に関係なく約 4.8Mbps の速度を得られることが示された。一方、VPN の場合テキストファイルの転送速度は 5Mbps を超える。これは VPN ルータが圧縮機能を持つためである。圧縮されているバイナリデータの場合速度が低下することが分かる。学外のスピードテストサイトを利用した場合も VPN 条件で速度低下が若干認められるが、運用上の問題はないと思われる。

若干の速度低下が認められるが、実運用上大きな障害になるとは考えられない。

VPN を用いる場合、無線リンクが確立した後、手入力による認証の手間が生じる。しかし、パスワード入力から仮想回線の確立に要する時間は数秒程度であるからユーザに強制することの障害とはならない。これは、認証 VLAN を用いる場合の接続時間と同程度である。接続の解除は VPN クライアントにより明示的に行うことになるため、ユーザは状態遷移を理解しやすい。また、利用中に接続が切れた場合でも状態が把握しやすい。

## 5. まとめ

本稿では、無線 LAN をサービスする際の問題点をまとめた。さらに、本学で運用中の無線 LAN ネットワークを紹介し、その問題点を示した。このうち、無線 LAN のパケットキャプチャに対処するための方策として VPN ルータを用いて IP レベルの暗号化を行うことで、安全に利用できる方法を示し検討を行った。この方法によっても、DoS 攻撃などの可能性は排除できないが、運用ポリシーよっては許容できるものである、ということが議論された。また、転送速度の比較から VPN を用いても大きな性能低下は認められないため、実運用上の問題とはならないことが示された。

### 参考文献

[1] 大塚秀治・牧野晋・久保美和子・柴田昌彦・林英輔,VPN 接続サービスの運用と課題,平成 14 年度情報処理教育研究集会講演論文集,pp294-297(2002).