セキュアなVPN適用無線LANの構成と特性

塩田　宏明*

Characteristics of Wireless LAN using a VPN

Hiroaki SHIOTA*

Abstract

This paper presents the wireless LAN using a VPN(Virtual Private Network). The wireless LAN is based on IEEE 802.11b standard.

The wireless access point(AP) is connected to a VPN server, which is connected to the Internet. The wireless station (STA) is a VPN remote access point. The wireless LAN using a VPN between an AP and a STA is based on the Point to Point Tunneling Protocol(PPTP).

Key Word:Wireless LAN, IEEE802.11b, Remote access VPN, PPTP

1. はじめに

近年、インターネットはブロードバンド化が進み、広帯域 Ethernet 機器が安価になるとともにネットワークの無線化の流れがインターネット機器にも適用されている。 無線化により機器間を接続するケーブルを不要とするとともに、ラップトップコンピュータの場合、いつでも、どこでも使用できる環境が実現した。

この無線 LAN においても広帯域化の検討が進みIEEE 802.11bと互換性のあるIEEE 802.11gにより54Mb/s の伝送が可能となるなど、高速、広帯域化が検討されIEEE 802.11a、IEEE 802.11g でドラフト化されている。

一方IEEE 802.11b 無線 LAN が汎用的に使用されるに伴い、無線 LAN システム規格が有するセキュリティ問題が指摘され、問題提起とともにインターネット上に各種ツールソフトが公開されている。

著者は、既に無線 LAN と小型ブロードバンドルータで良好なスループット特性の環境を提供する実験室LANの構成法とその特性を調査し、卒業研究環境に提供していることを報告している[1]。

本報告では、無線 LAN のセキュリティ問題を考慮し、リモートアクセス VPN 技術を適用したセキュアな実験室LANの構築とその特性を述べる。

2. セキュアな実験室 LAN の構成

2.1 無線 LAN の脆弱性問題

無線 LAN と小型ブロードバンドルータで良好なネットワーク環境を提供する実験室 LAN は実現できたが、無線 LAN のシステム規格が有するセキュリティ問題が明らかな現在において、セキュリティの確保が必要となった。

無線 LAN 区間のセキュリティ確保には以下の項目をまずアクセスポイント(AP)に設定することが必要とされている。

① ESSID の設定
② WEP の適用
③ MAC アドレス制限

ESSID は無線LANカードを具備したPCステーション(STR)のグループ化と認証、つまりESSID を

＊情報工学科

2003 年 9 月 12 日受付

知らないSTRはAPにアクセスできない。次に、WEPにより通信文を暗号化する。また、MACアドレス制限は、APにアクセスするSTRを制限すること（認証）ができるとされている。しかし、インターネット上にはこれら機能の解読ツールが流布している。また、機器によっては対応できない機能があるのが現状である。

この結果、電波の到達範囲に存在する悪意のあるSTRは ① ANY ESSID AP へのアクセスや Windows XP における簡易設定の利用、② MACのなりすましにより不正にネットワークにアクセスするとか、通信を傍受できる。また、正規のSTRがなりすましのAPにアクセスしてしまい、情報を取得されるなどの被害を受けることになる。

2.2　実験室ＬＡＮへの対応

ネットワーク中における無線 LAN の配置位置について、インフラストラクチャモードAPは、リピータハブと同一動作をすることから、APに接続したイサーネットワーク上に伝送される情報が全て無線区間に伝送される。これを、防ぐ対策として、前論文で、ルータを介してAPを配置することは、効果があることを述べた。

無線区間中での無線 LAN の脆弱性を整理すると、① アクセス制御機能、② 暗号化、③APなりすましである。①に対しては ESSID の隠蔽など、また、②に対する対策として、IEEE802．11iで検討中あるいは802．1xなどの高コストシステムがある[2]。これらの事項が、機器により未対応であるとかAPなりすましに対しては、STR使用者が注意するしかないのが現状である。

ところで、インターネットにおいてトンネリング技術として検討されている VPN[3]は、Windows OSにおいて標準添付され、PPTP あるいは IPSec などのプロトコルにもとづいたネットワークが容易に、安定的に構築できるようになっている。特に、PPTP は機器、サポートソフトの互換性がこなれている上、無線区間をトンネリングすることにより ① APとSTRの接続性の認証、② 通信文の暗号化を行うことができる。使用機器に対する多少の投資が必要であるが、汎用機器レベルでの構築が可能である。これらのことから、小型ブロードバンドルータと無線 LAN で構成した実験室 LAN に対し PPTP によるVPNを適用し、その効果を確認した。

2.3　実験室ＬＡＮ区間への追加機能

適用するネットワークでは、STRとAP間（無線区間）のレイヤ2に、PPTPによるトンネルを設定し、無線通信により通信していたTCP/IP信号をGRE伝送することである。図1に示すように、実験室LANが学内LANに接続するルータ側にPPTPサーバを、STRにPPTPのクライアント機能をそれぞれ設定した。

無線LAN区間に適用したPPTPにより ① APとSTRの接続性と認証、② 通信文の暗号化を行うことができる。

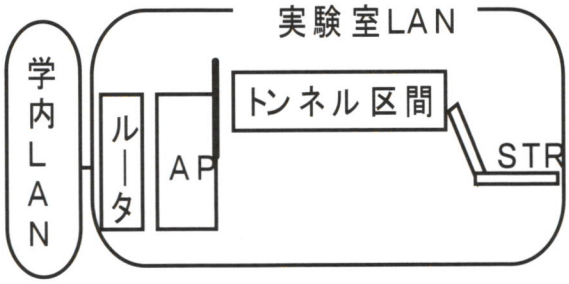

図１　実験室LANの構成

STRにおけるPPTPのクライアント機能は、OS（Windows XP および Windows 2000）に標準で添付されている機能を使用する。たとえば、Windows XPの場合ネットワーク接続ダイアログボックス中に仮想プライベートネットワークの表示が現れる。クライアント設定時に、仮想プライベートネットワーク名を「Wirless VPN」としておくとその名前がついて表示される。

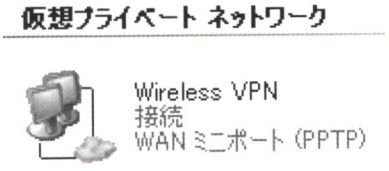

図2　Windows XPにおけるVPNの表示

PPTPサーバとしては、今回はブロードバンドル

ータの機能を使用した。PPTPはPPPを機能拡張したものである。APとSTR間の伝送フレーム構成は、データグラムを暗号化するとともに相手認証をするPPPヘッダを、更にGREヘッダでカプセル後、トンネル用ヘッダを加えたフレームを伝送する。

クライアントからのアクセスには、ESSID の設定による無線接続のほか、ユーザ名、パスワードによる相手認証処理を行う必要が生じる。このため、無線LANにおけるAPのなりすまし防止あるいはAPに対する正規アクセスSTRのみの接続が可能となる。

この結果、正規クライアント以外のSTRがAP経由で、学内LANに侵入し、学内LAN資源の破壊あるいは学内LANを踏み台にして学外のインターネットワークに対するハッキングを及ぼす危険性を防止できる。

3. 無線LAN室内ネットワーク

無線LAN区間に、PPTPプロトコルによるリモートアクセスVPNを適用して、トンネル区間を構築した。このためルータ、STRのソフトとしてルータのPPTPサーバおよびSTR（パソコンのOS Windows XPまたは2000など）のPPTPクライアントを使用可能なように設定した。

図3に示す網掛け部分が、ハードおよびネットワークに追加した追加機能である。

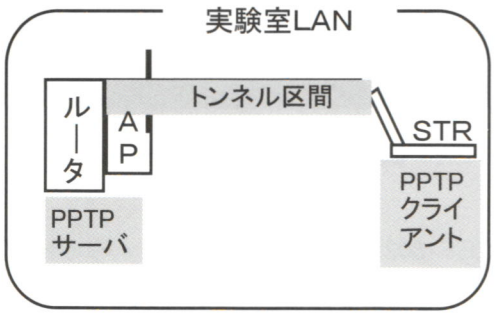

図3　無線LAN区間のVPN

OSとして Windows XPを使用したパソコン（STR）の場合、接続可能なワイヤレスネットワークAPがOSにより検出され、表示されるので任意のAPを選択することにより、無線区間の接続が容易に完了するが、VPNを無線区間に適用しているので、更にクライアントパソコン（PPTPクライアント）からAPにアクセスする処理として Wireless VPN 画面でのユーザ名、パスワード入力が要求される。これにより、APおよびSTRの認証が行われ、PPPコネクションが確立する。構築した無線区間の電波状態、無線LANの設定状態のほかWireless接続にVPNを適用したネットワーク接続状態を示す Windows 画面を合わせて図4に示す。

図4　無線LANの設定状態および電波状態

Wireless VPNは、図5に示すように認証にはMS Charp Ver2が、また、暗号化には RSA Data Security 社の RC4 を利用するMPPE 128（暗号化キーの bit 数、128bit）が適用されている。

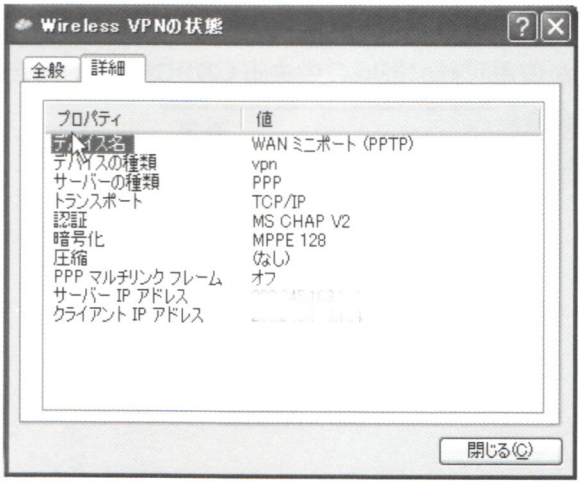

図　5　PPTPクライアントの状態

無線によるLAN回線設定後は、無線区間（VPNサーバとクライアント間）に形成されたPPTPによるトンネルを使用して、レイヤ3のIPデータグラムなどのパケットがGREでカプセル化された状態で伝送され

る。図6にPPP確立初期時にVPNサーバとクライアント間で送受信されるパケットを示す。3Wayハンドセイクでお互いに確認し、コネクションを確立する。その後PPTPプロトコルによる接続認証、暗号化等の処理を行っている。やがてGREパケットの伝送が行われていることがわかる。

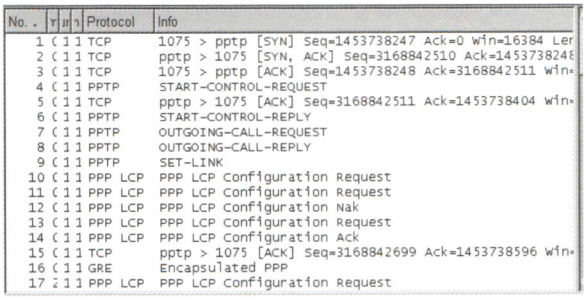

図6　PPPコネクション初期のシーケンス

4. VPNを適用した無線LAN区間の特性

4-1.　無線特性と通信エリア

無線LANは、セキュリティ面から考えると不要な範囲に信号を伝送しない、つまり可能な限り信号の伝播を制限することが望ましい。このためには、送信電力制限機能付のAPを使用することが望ましいが、機能がない機器もある。図7に実験に使用したAPの配置と表1に実験室内の観測点におけるSN値を示し、伝播特性を示す。また、図8にSN観測例を示す。使用無線CHとしては、無線LANが使用可能な帯域の中央近くの9CHを使用した。

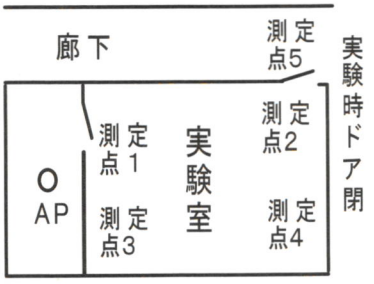

図7　観測点

表1　各観測点のSN値

観測点	1	2	3	4	5
SN（dB）	52	36	34	32	33

図7に示すように実験準備室の実験机上に設置したAPの信号は、実験室との間のドアを開くと実験室では表1のような値が得られた。実験室内で人の移動等が無い状態であれば、全観測点でリンク速度11Mb/s程度が得られた。

また、廊下側ドア（ドア面に隙間がある）を閉めても、測定点5のSN値が示すように、廊下側に信号が漏れていた。測定点2と5のSN値を比較するとほぼ同一値である。この結果から、AP送信電力を制御できない機器の場合、無線伝送特性としては伝播に伴う信号減衰あるいは障害物による電波減衰しか期待できず、通信エリアは広い範囲に及ぶ。

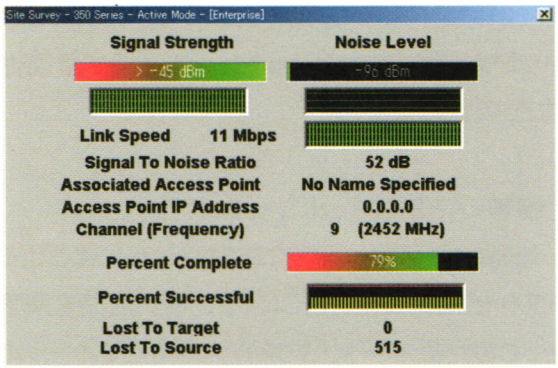

図8　SN観測例

4-2.　無線LAN信号特性

AP－STR間の信号例を図9に示す。

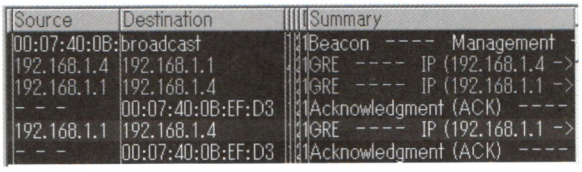

図9　AP－STR間の信号例

IEEE 802.11b 無線LANでは、パケットの衝突を回避するためCDMA/ADを採用しており[4]、図10に示すACK信号が図9に示すような頻度で通信されていた。

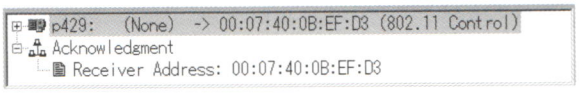

図10　ACK信号

図9 に示す信号の内、無線APから送信されているビーコン信号の一部を図11に示す。この図から、ビーコン信号中にはSSID（またはESSIDともいう。）、使用チャネルなど無線区間での接続情報が周囲のSTRに対して送出されている。

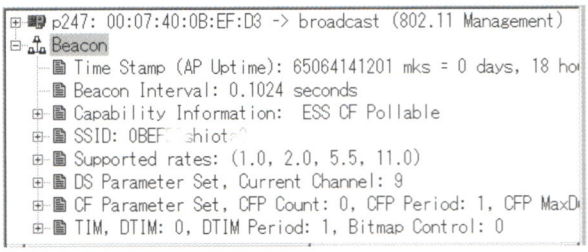

図11 ビーコン信号

このため Windows XPではこの信号を受信し、受信されたAPをList表示する機能を有している、そのためANY対応のAPの場合当該APを選択するだけで無線区間の設定が容易に完了する。また、APの所在を知るツールソフトが、インターネット上で配布されていることから、これらに対しても、ESSIDをビーコン信号に載せて放出しないAPステルスと呼ばれている機能を持ったAPを使用することが望ましい。

IEEE802．11bにもとづいた無線LANにおけるAP（IPアドレス：192.168.1.1）からSTR（IPアドレス：192.168.1.4）に向け送信された信号を図12に示す。AP－STR間は、PPPプロトコルにもとづいて通信されており、GRE Ver1により暗号化されているために、Raw PPPの欄で示されるように暗号化され、他人に容易にはその内容が知れないことがわかる。

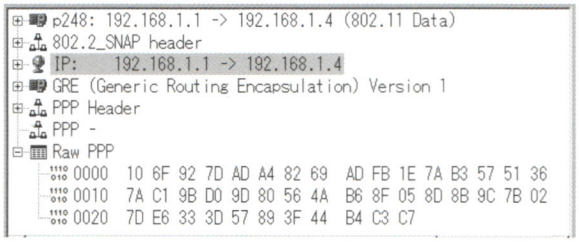

図12 APからSTR向け信号

図13は、反対にSTRからAP向けの信号である。これも暗号化されていることがわかる。

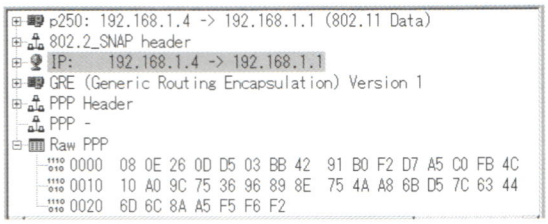

図13 STRからAP向け信号

5. むすび

小型ルータと無線LANで構成した実験室LANに存在するネットワークの脆弱性の排除と便利で設定が容易な無線LAN通信から一歩進み、利用者の通信の秘密を確保し、ネットワーク管理に対する管理者の負担が少なく、かつ、設備費の負担が少ないネットワークを、VPN技術の利用で実現でき、構築したネットワーク特性から秘話、認証などに関して一定の効果を確認した。

学内LANにおいてもWAN側（有線側）のファイアオール等によるガードのみならず、前論文の発表後、数多くの無線LAN APが校内 LAN に組み込まれたことから今後無線LANを考慮したLAN構成の検討が必要と思われる。

参考文献

[1] 塩田宏明，松井美香，“無線LANによる室内ネットワーク構成と特性”，p69，2001年11月

[2] 日経ネットワークセキュリティ，“無線LANパニック”，pp64－69，2003年，4月日経BPムック

[3] 金城俊哉，“よくわかる最新IP-VPNの基本と仕組み”，p74，002年12月

[4] 松江英明,森倉正博，“802．11高速無線LAN教科書”，p66，2003年，3月，IDGジャパン