仮想化技術を用いた安全な無線通信方式の研究

傍士　裕生

フロンティア工学コース

E-mail：115139m@gs.kochi-tech.ac.jp

1　はじめに

近年，ネットワークを構築する際，無線 LAN を用いる企業が増加している [1]．企業は無線 LAN を用いることで運用コストの削減が可能である．しかし，無線 LAN を用いたネットワーク構築には安全な認証方式が必要である．また，安全な認証方式であっても使用可能な動作環境が限定されている場合がある．そこで，本研究では安全な認証方式を不特定の動作環境で使用可能にする方式の提案，検証を行う．

2　研究背景

企業において，無線 LAN を用いたネットワークの構築が行われている．従来の有線 LAN と比較し，無線 LAN を用いることでネットワーク構築や維持費用の削減が可能である．しかし，無線 LAN を用いる場合，盗聴やなりすましの危険がある [2]．そのため，無線 LAN を安全に使用するために通信の暗号化やユーザ認証を行う必要がある．無線 LAN のユーザ認証規格として IEEE802.1X がある．また，IEEE802.1X において様々な認証を可能にするプロトコルとして，EAP(PPP Extensible Authentication Protocol) がある．IEEE802.1X/EAP の認証方式として EAP-IPN がある．EAP-IPN は従来の方式と比べ，認証サーバを必要とせず，盗聴やなりすましが防止可能で安全な認証方式である．そのため，EAP-IPN を導入することで無線 LAN を用いた安全なネットワークが安価に実現可能である．しかし，EAP-IPN には動作環境が限定されるという問題点がある．

3　研究内容

本研究では，従来利用できない動作環境において，無線 LAN 認証方式を使用する方式の提案，検証を行った．以下で，提案方式，検証についてそれぞれ示す．

3.1　提案方式

提案方式は，従来無線 LAN 認証方式が使用不可能な動作環境に，動作可能な環境を用意し通信を行うというものである．提案方式を図 1 に示す．ユーザが操作する OS 上に仮想化技術の一種である仮想化ソフトウェアを用い，無線 LAN 認証方式の動作環境を仮想マシン上に構築する．使用する仮想化ソフトウェアの条件として，USB2.0 の制御が可能なこと，ユーザが操作する OS と仮想マシン間において，2 点間の限定通信が可能な必要がある．構築した仮想マシン環境上に USB 無線 LAN 子機を制御するための OS を導入する．この USB 無線 LAN 子機アダプタによって無線 LAN 親機との通信が行われる．そして，導入した OS に Proxy サーバを構築する．ユーザが操作する OS 上で Proxy サーバの使用設定を行うことで，ユーザが操作する OS の通信は USB 無線 LAN 子機を制御するための OS を経由した安全な通信となる．

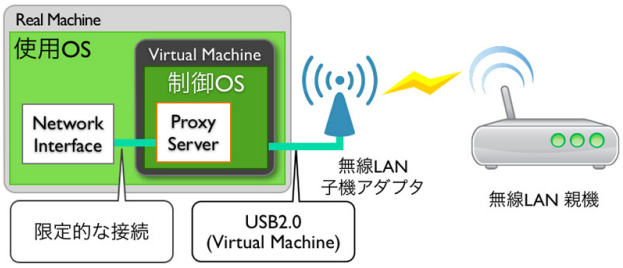

図 1　提案方式

3.2　提案方式の検証

提案方式の検証として，提案方式を実装した環境を構築し，通信の疎通を確認した．ユーザが操作する OS として Mac OS X 10.6.5 を用い，仮想化ソフトウェアである virtualbox4.02 によって仮想マシンを構築した．仮想マシン上に Windows XP を導入し，仮想マシンが制御する USB2.0 のポートに無線 LAN 子機アダプタである GW-US54GXS を接続した．そして，Windows XP に Proxy サーバとして ANHTTPD 1.42p を導入した．Mac OS 上のネットワークデバイスを全て停止し，Mac OS のネットワーク設定において，Proxy サーバの接続設定を行った．そして，Mac OS 上から，通信が可能であることを確認した．

4　おわりに

本研究では，仮想化技術を用い，従来使用不可能であった動作環境で，安全な無線 LAN 認証方式が使用可能になることを示した．今後は，実用的なシステムを構築する．

参考文献

[1] 財団法人インターネット協会, “インターネット白書 2009,” 株式会社インプレス R&D,2009.

[2] 加藤聰彦, “無線 LAN セキュリティー次世代技術 IEEE 802.11i と WPA の実際,” 構造計画研究所, 2006.