6S-9

無線 LAN 統合認証方式の実装

山下　真純[†]　　西村　俊和[‡]　　小川　均[‡]
立命館大学大学院理工学研究科[†]
立命館大学情報理工学部情報コミュニケーション学科[‡]

1. はじめに

従来の無線 LAN ではセキュリティを高めるために，AP(アクセスポイント)におけるアクセス制限を行ってきた．一般的な手法として，MAC アドレスでのフィルタリングや，WPA(Wi-Fi Protected Access)のネットワークキーを利用してきた．無線 LAN は有線 LAN に比べ接続が容易であるため利便性は高いが，不特定多数のユーザーに AP を開放した場合，ネットワーク管理者はその AP に接続したユーザーがネットワーク上で行う行為に対し責任を取らなくてはならない．ユーザーが行う行為には迷惑行為も含まれるため，管理者は身元のわかるユーザーに対してのみ，AP を開放することでセキュリティを確保する．そのため，ネットワーク管理組織毎の AP が必要となり，AP の乱立による電波干渉や周波数資源の独占等の新たな問題が発生することが考えられる．

無線 LAN のメリットとして，接続の容易さが上げられるが現状では前述のアクセス制限によってメリットを十分に享受していないと考える．ここで問題となるのは不特定なユーザーに対して AP を開放することであるため，ユーザーが特定できればアクセス制限は必要ない．そうなれば多くの AP も利用が出来るため利便性は向上し，AP の乱立に伴う問題点も解決される．

その解決方法として著者らが提案した無線 LAN 統合認証方式[1]がある．本方式は無線 LAN の利便性を生かすため，外部に認証機構を置き，AP におけるフィルタリングを行わない．また安全に認証を行うために、AP からのパケットを VPN(Virtual Private Network)を利用して外部の認証機構に伝送する．

本稿では，無線 LAN 統合認証方式における AP，認証機構，VPN の実装方法について報告する．

「The implementing system unified Authentication for Wireless LANs」
†「Masumi Yamashita・Ritsumeikan University」
‡「Toshikazu Nishimura・Ritsumeikan University」
‡「Hitoshi Ogawa・Ritsumeikan University」

2. 無線 LAN 統合認証方式

2.1 全体構成

本方式は，VPN クライアント，LAN 認証部，AP からなる「公衆無線 LAN ルータ」及び認証機構によって実現する．以下の図 1 に全体構成図を示す．

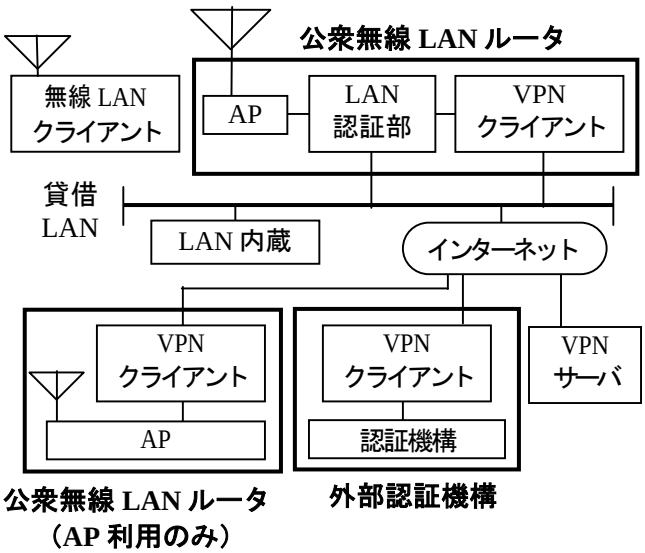

図 1．全体構成図

2.2 公衆無線 LAN ルータ及び認証機構

公衆無線 LAN ルータは VPN，LAN 認証部，AP の機能を持つ事を原則とするが，設置目的に応じてその機能は必ずしも全て必要ではない．例として，AP の有効範囲を広げる事を目的とし，貸借 LAN の LAN 内蔵器を利用しない場合では LAN 認証部は必要でない．（図 1.［AP 利用のみ］と書かれた公衆無線 LAN ルータ）

また外部の認証機構は VPN クライアントを利用して VPN へ接続する．（図 1. 外部認証機構）

以下にそれぞれの機能の特徴を述べる．

2.2.1 AP（アクセスポイント）

一般に AP を設置する場合はフィルタリング等を行ってアクセス制限を行うが，本方式では認証機構が外部に存在するため，フィルタリングは行わず不特定多数のユーザーに対し開放されるものとする．

2.2.2 LAN 認証部

AP からのパケットは，LAN 認証部において認証を行う．既存のシステムでは認証出来なかったパケットは破棄されるが，本方式では VPN を利用して外部の認証機構にパケットを転送する．

2.2.3 VPN (Virtual Private Network)

認証できなかった認証要求パケット，もしくは既に外部の認証を終えネットワークを利用中のパケットを暗号化，トンネリングすることで安全に外部の認証機構に転送する．VPN クライアントは VPN ハブに接続することで，複数の外部認証機構へのアクセスが可能となる．

2.2.4 認証機構

LAN 認証部において認証できなかったパケットは，VPN を経由して認証機構に送られる．認証機構では ID，パスワード等を用いてユーザー認証を行い，ユーザーに対し IP アドレスの付与等を行う．

2.3 既存の無線 LAN との違い

本方式は従来の無線 LAN の問題点を解決する有力な方法であることを述べたが，以下にその理由と本方式の特徴を述べる．

1. 従来は AP においてアクセス制限を行ってきたため，誰もが自由に無線 LAN のメリットを享受できなかった．本方式は，AP の先にある認証機構によってアクセス制限を行うため自由に AP を利用することが可能である．
2. 従来，AP は 1 組織に 1 台必要であった．本方式では複数の認証機構を利用でき，1 つの AP を共有するため，組織毎の AP は必要ない．
3. 従来は単一の認証方法しか選べなかったが，本方式では組織毎に独自の認証方式で認証が可能であり，セキュリティレベルを組織毎に設定可能となる．
4. 認証機構までを VPN で繋ぎ，安全に認証パケットを伝送できる．

3. 実装

以下に実装例を挙げる．先に提案された方式では VPN クライアントが VPN 表を持ち，それぞれの認証機構までの VPN を構築していたが，本稿のシステムでは，PPPoE を利用することで同等の機能を持たせている．

3.1 全体像

図 1 に示した公衆無線 LAN ルータ内にある VPN クライアントを VPN ハブに接続することでシステムの一部となる．全体の拡張にはこの公衆無線 LAN ルータの増設を行うことで，広範囲で利用可能となる．

3.2 実装方法

VPN の実装には SoftEther を使用する．SoftEther は容易に VPN を構築でき，既存の VPN プロトコル (PPTP[Point to Point Tunneling Protocol],L2TP[Layer2 Tunneling Protocol]) と異なりデータリンク層で接続，ブリッジすることで物理的に離れた Ethernet を接続できるという利点を持つ．データリンク層での通信を行うため Layer2 での異なる認証方法を利用できる．また LAN over TCP により Firewall や NAT といった Layer3 での制限を受けない．SoftEther では仮想 HUB，仮想 LAN カードが用意されており，仮想 HUB に仮想 LAN カードを接続することで VPN を構築するが，仮想 HUB には複数の仮想 LAN カードを接続できるため増設が容易である．

LAN 認証部，認証機構には PPPoE サーバを構築する．PPPoE はサービス名の指定により複数の認証機構の中から認証を受けたいサーバを指定できる．また Ethernet 上で PPP を利用するため，ユーザー認証，IP アドレスの付与が出来る．また NAT を利用することで無線クライアントは擬似的にグローバル IP を取得している．

公衆無線 LAN ルータは上記の仮想 LAN カードを持つ VPN クライアント，PPPoE サーバの LAN 認証部，AP を LAN で接続することで実現される．

システム全体の実現方法は，外部に仮想 HUB を用意し公衆無線 LAN ルータの VPN クライアントが仮想 HUB に接続することで完了する．

4．性能評価

上記の実装方法で構築されたシステムの性能評価を行う．VPN を経由した場合と経由しない場合にテストケースを分け，それぞれのスループット計測を行った．計測結果を以下の表 1 にまとめる．有線 LAN に 100Base-TX，無線 LAN に IEEE802.11g を使用した．

表 1. 実効値(単位：Mbps)

VPN 経由せず	VPN 経由
21.75	16.14

VPN を経由することにより 25%程度スループットが低下するが，十分なスループットが得られている．また 3 つの認証機構を用意し 1 つの AP からそれぞれの認証を受けることが出来た．

文　献

[1] 西村 俊和，前田 忠彦，小川 均，アンテナ指向性制御を組み合わせた無線 LAN 統合認証方式，情処研究報告 2004-MBL, Mar. 2004.