社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－MBL－28　(2)
2004／3／4

セキュリティレベルを考慮した無線LAN環境を実現するアクセスポイント及びネットワーク構成方法

谷澤佳道† 後藤真孝† 高木雅裕†

無線 LAN の認証システムにセキュリティレベルを導入し、アクセスポイントにセキュリティレベルの異なる複数のネットワークを接続する。最もセキュリティレベルの高いネットワークは、無線クライアントからアクセス不可能な無線 LAN 管理用ネットワークであり、その他のネットワークは、複数の認証レベルに対応したサービスを提供するネットワークである。認証サーバは無線クライアントの認証結果に認証レベルを付加し、アクセスポイントはその認証レベルに応じて接続先ネットワークを選択する。これによりクライアントの認証レベル毎に異なるネットワークサービスを提供する無線 LAN 環境が実現できる。本稿では、提案する無線 LAN システムのネットワーク構成、アクセスポイント構成、及び実装例について述べる。

A Structure of Access Points and Network Systems Building Security Level Aware Wireless LAN Environments

Yoshimichi Tanizawa,† Masataka Goto† and Masahiro Takagi †

We introduce “security level” into the authentication mechanism on the Wireless LAN environments. In these environments, the Access Points are attached to multiple networks that have own security levels. The network of the highest security level is the authentication network which authenticate clients and no wireless client can access. The other networks provide services corresponding the security levels of the networks. When the Authentication Server authenticates the client with the authentication network, it specifies the authentication level of the client. Then the Access Point selects the network the client will access by its authentication level. The Access Points and the network structure realizes the security-aware wireless LAN environments that support variable network services depending on the authentication level of the client. We describe the structure of the network system and the Access Point in the proposed Wireless LAN environments, and an implementation of the proposed Access Point.

1. はじめに

無線 LAN は、ネットワークケーブルの接続を行うことなく、無線での LAN アクセスを可能とするものであり、IEEE802 委員会 802.11 ワーキンググループにより標準化されている[1)]。有線 LAN と異なりネットワーク配線を必要としないため、ネットワークシステムの可用性、柔軟性を大幅に向上させるが、その一方で無線であるが故の暗号化/認証等のセキュリティ対策が必要となる。

また、近年では、従来の様なオフィスネットワークへの適用だけでなく、屋外へと適用範囲の拡大がはかられており、工場設備の監視システムの無線化や、携帯電話へ内蔵させて街角で利用する等の形態が考えられている。特に、公共環境に無線LANシステムを設置し、利用者に無線ネットワークアクセスを提供するホットスポットと呼ばれるサービスは、既に複数の ISP によって開始されている。現在は駅のホームやコーヒーショップ等が主なホットスポットエリアとなっているが、我々は屋外へのホットスポットサービスの展開を目標としている。屋外の公共環境では、不特定多数の多種多様な目的を持った利用者の端末がクライアントとなり得る。よって、悪意のある利用者に無線 LAN の認証サーバを含む管理用ネットワークへアクセスされないようにする認証方式が必要となる。

IEEE は既に、無線 LAN の認証標準として、IEEE802.1X[2)] を標準化している。これは、クライアン

† 株式会社東芝 研究開発センター
TOSHIBA Corporation R&D Center

トがアクセスポイントに接続要求をする際に、アクセスポイントが認証サーバに問い合わせ、そのクライアントを認証する三者間認証手順である。IEEE802.1X 実装の多くは、クライアントにアクセスを許可するネットワークと、認証サーバを設置するネットワークが同一であることから、クライアントによる、認証サーバへの不適切なアクセスが可能となる恐れがある。

一方、ホットスポットサービスでは、異なる目的や権限を持った各利用者に対して異なるネットワークサービスを提供したい。例えば、ISP のホットスポットサービスに未登録の利用者に対してはサービス登録を呼びかけるためのコマーシャルコンテンツのみを提供し、登録済みの利用者に対しては、インターネットアクセスサービスを提供する。また、課金済みの利用者に対しては有料コンテンツの閲覧サービスを許可し、ホットスポット及びネットワーク管理者に対しては、サービスメンテナンス用のネットワークへのアクセスを許可する事などが考えられる。現状のアクセスポイントは、クライアント認証の可否のみから、ネットワークアクセスを決定するため、クライアントの種類や目的に応じて適切な権限を付与し、それぞれを異なったネットワークへ接続するサービスは実現が難しい。

そこで、本稿では、無線 LAN の認証システムにセキュリティレベルを導入し、アクセスポイントにセキュリティレベルの異なる複数のネットワークを接続する方式を提案する。本方式により、以下の用件を満たす無線 LAN 環境が容易に実現可能となる。

- 認証サーバ及び管理用ネットワークを、無線 LAN クライアントからアクセス不可な場所へ配置し、ネットワークの堅牢性を高めること
- 無線 LAN クライアントの認証結果に、認証の可否だけでなく、認証レベルを含めることで、クライアントをその認証レベルに応じて異なるネットワークサービスへとアクセスさせること

以後、2 章では、従来の無線 LAN システムにおける認証方式について述べる。3 章では、提案する無線 LAN システムの構成について述べる。4 章では、提案システムの実装例であるアクセスポイント WA-7000 について述べる。5 章でまとめと今後の課題を述べる。

2. 無線 LAN システムにおける認証方式

本章では、IEEE802.1X 標準に基づく無線 LAN システムの認証方式について、802.1X と WEP 暗号化を組み合わせた認証方式 (IEEE802.1X + WEP) を想定して述べる。802.1X は、認証プロトコルとして、EAP(PPP Extensible Authentication Protocol)[4] を用いることが決められている。EAP は、無線クライアントアクセスポイント間では EAPoL(Extensible Authentication Protocol over LAN) を、アクセスポイント認証サーバ間では、RADIUS(Remote Authentication Dial In User Service)[3] を用いて配送される。図 1 にシーケンス図を示す。

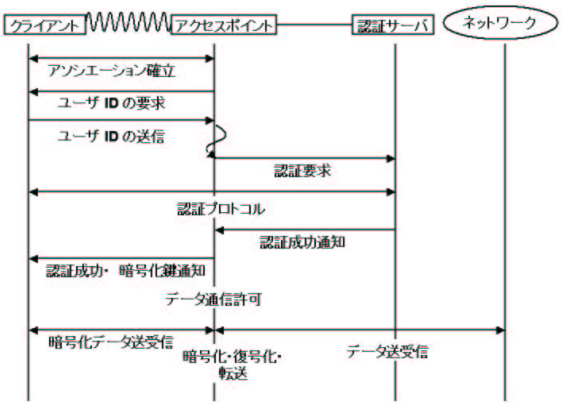

図 1 無線 LAN システムにおける認証シーケンス

(1) クライアントはアクセスポイントとの間でアソシエーションを確立し、アクセスポイントに対してクライアント認証要求を送信する。

(2) アクセスポイントはクライアント認証要求を受け取ると、クライアントに対してユーザ ID を要求する。

(3) クライアントは、MAC アドレスをユーザ ID として送信する。

(4) アクセスポイントは、認証サーバにクライアントの認証を要求するデータグラムを作成し、認証サーバへ送信する。これにはクライアントのユーザ ID が含まれる。

(5) 認証サーバは、受信データグラムに含まれるユーザ ID を認証対象として識別する。

(6) 以後、クライアント、認証サーバ、アクセスポイントの三者によるクライアント認証プロトコルが動作する。
認証サーバが送信する認証データグラムはアクセスポイントで受け取られ、クライアントが受信可能な認証フレームとして作り直された後、無線ネットワークへと送信される。クライアントが送信する認証フレームはアクセスポイントにて受け取られ、認証サーバが受信可能な認証データグラムとして作り直された後、有線ネットワークへと送信される。

(7) 認証プロトコルの結果、認証サーバにて対象ク

ライアントのネットワークアクセスが承認されると、認証サーバはアクセスポイントに対して、認証成功を通知する。

(8) アクセスポイントは、これを受信すると、認証されたクライアントとの無線通信区間を暗号化するための鍵 (WEP Key) を作成もしくは選択し、無線クライアントに対して、認証成功及び無線通信区間の暗号化に用いる暗号化鍵を通知する。

(9) 以後、クライアントはアクセスポイントを介したネットワークアクセスが可能となり、以降の無線通信は暗号化される。クライアントが有線ネットワーク上のシステム宛に送信するフレームはアクセスポイントにて、対応する暗号化鍵で復号化された後、有線ネットワーク上へと転送される。有線ネットワーク上のシステムからクライアントへ宛てたフレームは、アクセスポイントにて、対応する暗号化鍵で暗号化された後、無線ネットワークへと転送される。

3. 提案システムの構成

本章では、提案システムのネットワーク構成とアクセスポイント構成について述べる。

3.1 ネットワーク構成

図 2 に提案システムのネットワーク構成を示す。提案システムは、セキュリティレベルの異なる複数のネットワーク、無線クライアント、認証サーバ、アクセスポイントからなる。従来のネットワーク構成は、アクセスポイントに対して有線ネットワークが一つだけ接続されていたが、提案システムのネットワーク構成は、一つの管理用ネットワークと、提供するセキュリティレベルに対応した複数のネットワークを一つのアクセスポイントに接続している。以下に構成要素のそれぞれについて説明する。

- ユーザネットワーク:
  無線クライアントが認証された結果、アクセス可能となるネットワークである。各ユーザネットワークには、セキュリティレベルが割り当てられている。セキュリティレベルとは、そのネットワークで扱う情報の機密性の程度を表現するもので、その値が大きい程、情報の機密性が高いものとする。各ユーザネットワークではセキュリティレベルに応じて種々のネットワークサービスが提供されている。図 2 では、セキュリティレベル 0 からセキュリティレベル 4 までの 5 つのユーザネットワークを示している。

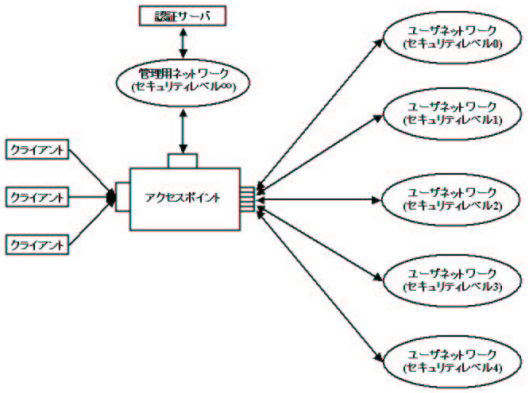

図 2 提案システムのネットワーク構成

- 管理用ネットワーク:
  アクセスポイントと認証サーバが接続されており、アクセスポイントに対して認証要求を行う無線クライアントの認証プロトコルを動作させるネットワークである。セキュリティレベルの最も高いネットワーク (セキュリティレベル∞) として位置付けられ、無線クライアントからはアクセスすることができない。認証サーバの他にも、無線 LAN 環境の管理用サーバ等が設置される。
- 認証サーバ:
  従来の認証サーバは、アクセスポイントからの問い合わせに対して、クライアントの認証の可否を答えるのみであったが、提案システムの認証サーバは、これに認証レベルを付加する。認証レベルとは、クライアントのネットワークアクセス権限の程度を示すもので、認証サーバに予め登録された情報や、認証の際に利用したプロトコルの種類に応じて、クライアントに割り当てられる。
- アクセスポイント:
  複数の有線ネットワークインタフェースを持ち、管理用ネットワークと複数のユーザネットワークに接続されている。管理用ネットワーク上で無線クライアントを認証し、その結果得られる認証レベルに応じて無線クライアントからのフレームを適切なセキュリティレベルを持つユーザネットワークへと転送する。
- 無線クライアント
  認証完了時に認証レベルを付与され、そのアクセスは、認証レベルに対応するセキュリティレベルを持つユーザネットワークに制限される。

3.2 アクセスポイント構成

図 3 にアクセスポイント構成図を示す。アクセス

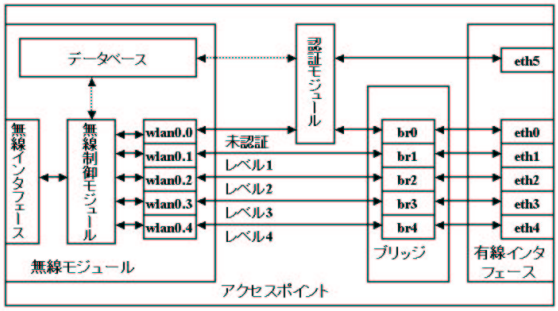

図 3　提案システムのアクセスポイント構成

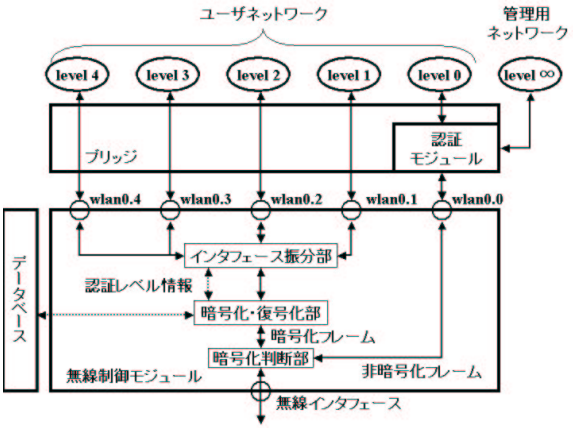

図 4　アクセスポイントにおける無線制御モジュールの構成

ポイントは、認証モジュール、ブリッジ、有線インタフェース、無線モジュールからなる。認証モジュールは 802.1X 認証をおこなう。有線インタフェース eth5 を介して管理用ネットワーク上の認証サーバとの間で認証用データグラム (RADIUS) のやりとりを行い、また、無線モジュールの内部インタフェース wlan0.0 から、認証用フレーム (EAPoL) のみを抜きだし、無線クライアントとのあいだでやりとりを行うことで、認証プロトコルを動作させる。有線インタフェースは有線ネットワークとフレームの送受信をおこなう。eth5 は管理用ネットワークと、eth0 から eth4 はそれぞれユーザネットワークのセキュリティレベル 0 からセキュリティレベル 4 へと、それぞれ接続されている。ブリッジは無線モジュールの内部インタフェースと有線インタフェースとの間でフレームを転送する。ブリッジインタフェース br$i$($i = 1, 2, 3, 4$) は、それぞれ無線モジュールの内部インタフェース wlan0.i と有線インタフェース eth$i$ をブリッジする。

無線モジュールは、無線インタフェース、無線制御制御モジュール、データベース、内部インタフェースから構成される。無線インタフェースは、無線クライアントとのアソシエーションを管理し、フレームの送受信を行う。無線制御モジュールは、クライアントから受信した暗号化フレームの復号化及びクライアントへ送信するフレームの暗号化を行う。また、受信時には出力先内部インタフェースの選択、送信時には暗号化鍵の選択を行う。データベースは、認証した無線クライアントのユーザ ID、暗号化鍵、暗号化鍵のインデックス、認証レベルを保持する。内部インタフェースはその出力をブリッジへと転送する。

3.3　無線制御モジュールの構成とフレーム送受信

図 4 に無線制御モジュールの内部構成を示す。無線制御モジュールは、暗号化判断部、暗号化・復号化部、インタフェース振分部からなる。暗号化判断部は、無線インタフェースから受信したフレームが暗号化されているか否かを判断するものである。暗号化・復号化部はフレームの暗号化・復号化と、フレーム受信時の認証レベル特定を行うものである。認証レベルや暗号化鍵の特定はデータベース部へアクセスして行う。インタフェース振分部は、複数の内部インタフェースとの間でのフレームの送受信を行うものであり、内部インタフェースが接続されるネットワークのセキュリティレベルの値と、暗号化・復号化部の間でやりとりする認証レベルの値を対応づけて保持する。

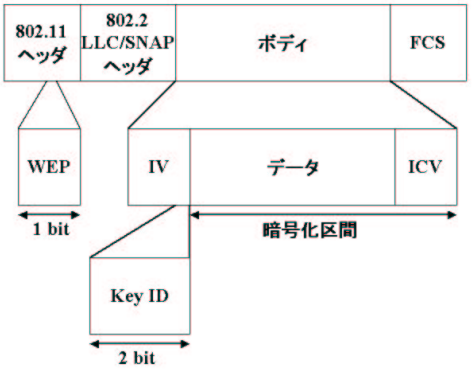

図 5　無線 LAN フレームフォーマット

フレーム受信時の動作について説明する。無線インタフェースから受信したフレームは暗号化判断部にて受け取る。暗号化判断部は、受信フレームが暗号化されているか否かを判断する。暗号化フレームであるか否かの判断は、802.11 ヘッダの WEP ビットを参照する (図 5)。暗号化されていないフレームは、セキュリ

ティレベル 0 ネットワーク宛てのフレーム、もしくは認証プロトコルに関するフレームであるので、wlan0.0 内部インタフェースを介して認証モジュールへと転送する。暗号化されたフレームであれば、それを暗号化・復号化部へ転送する。暗号化・復号化部は、送信元クライアントのユーザ ID と暗号化鍵のインデックスをもとにしてデータベースにアクセスし、復号化に用いる暗号化鍵と、クライアントの認証レベルを特定する。暗号化鍵のインデックスは、IV (Initialization Vector) に含まれる Key ID に示される (図 5)。復号化されたフレームは、認証レベルと共に、インタフェース振分部に転送される。インタフェース振分部では、認証レベルからセキュリティレベルを決定し、復号化フレームを対応するセキュリティレベルに接続される内部インタフェースから出力する。

ここでは、インデックスの値が $i(i = 0, 1, 2, 3)$ の場合、認証レベル $(i + 1)$ であると判断し、内部インタフェース wlan0.$(i + 1)$ からブリッジへと転送し、セキュリティレベル $(i + 1)$ のネットワークへと送信する。

フレーム送信時の動作について述べる。認証モジュールが作成する認証用フレーム (EAPoL) 及びセキュリティレベル 0 ネットワークから送信されたフレームは wlan0.0 内部インタフェースから暗号化判断部へ到達する。暗号化判断部は、このフレームを暗号化せず無線インタフェースより送信する。一方、ユーザネットワークより送信されたフレームは、ブリッジ部を介して内部インタフェースよりインタフェース振分部へ到達する。インタフェース振分部は、フレームを受信した内部インタフェースから、そのフレームのセキュリティレベルを判断し、そのセキュリティレベルから、宛先クライアントの認証レベルを決定して、認証レベルと共にフレームを暗号化・復号化部へ転送する。暗号化・復号化部は、フレームの送信先クライアントのユーザ ID と認証レベルをもとにデータベースへアクセスし、暗号化に用いる暗号化鍵とそのインデックスを特定する。求めた暗号化鍵で暗号化したフレームは暗号化判断部を介して無線インタフェースへと転送し、無線ネットワークへと送信される。

ここではセキュリティレベル $l(l = 1, 2, 3, 4)$ ユーザネットワークから送信されたフレームは、内部インタフェース wlan0.l を介してアクセスポイントに到達し、認証レベル l と特定され、インデックス $(l - 1)$ の暗号化鍵により暗号化され、無線クライアント宛てに送信される。

4. 実 装 例

本章では、提案方式を実装したアクセスポイント WA-7000 について概説する。

WA-7000 は、屋外設置を想定し、提案方式を実現するアクセスポイントである。その他、802.11a/b/g 同時使用可能、柔軟設定可能なパケット及びフレームフィルタリング機能、管理プロトコルの暗号化、WPA, QoS 等先進規格のサポート、起動時の設定情報自動取得機構、無線 LAN クライアント同士の通信制御、屋外設置や機器への組み込みを想定した多様な筐体などの特徴を持つ。

図 6 に WA-7000 の構成概要を示す。管理用ネットワーク、セキュリティレベル 0 のゲストユーザネットワーク、セキュリティレベル 1 の正規ユーザネットワークの 3 種のネットワークを VLAN として扱う有線インタフェースを備える。また、無線制御モジュールは無線インタフェースのデバイスドライバとして実現しており、2 つの内部インタフェースは、ネットワークインタフェースとして見える。暗号化されていないフレームは wlan0.0 から、暗号化されているフレームは wlan0.1 から出力される。仮想ブリッジを利用し、セキュリティレベル 0 ユーザネットワークと内部インタフェース wlan0.0 を、セキュリティレベル 1 ユーザネットワークと内部インタフェース wlan0.1 をそれぞれブリッジする。この構成であれば、認証サーバが認証レベルを返さなくても、認証済みと未認証/認証失敗のクライアントを異なるユーザネットワークへと接続する事が可能である。認証モジュールはユーザレベルのソフトウェアとして実装している。wlan0.0 から EAPoL フレームを抜きだし、デバイスドライバから送られるメッセージを利用してデータベースの内容を参照する。

5. まとめと今後の課題

無線 LAN の、屋外設置を含めた適用範囲の拡大や、ホットスポットサービス実現の要求に答えるべく、セキュリティレベルを考慮した無線 LAN 環境の実現方式を提案した。本方式は、無線 LAN の認証システムにセキュリティレベルを導入し、アクセスポイントにセキュリティレベルの異なる複数のネットワークを接続するものである。これにより、無線クライアントに対して、それに付与する認証レベルに応じた異なるネットワークサービスを提供可能になるとともに、認証及び無線 LAN 管理用サーバを、無線クライアントからアクセスできないネットワーク上に配置することがで

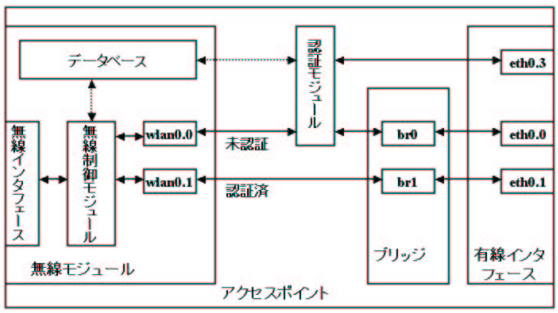

図 6 WA-7000 の構成概要

きる。本稿では、本方式を実現するためのネットワーク構成、アクセスポイント構成、及びアクセスポイント実装例について述べた。

今後の課題について以下に述べる。4 種類以上のセキュリティレベルを持つ提案システムを実装するためには、デバイスドライバが 3 つ以上の内部インタフェースを備えることと、認証サーバが認証結果に認証レベルを付加して返すことが必要になる。また、システムに対する要求として、クライアント自身に接続先のユーザネットワークを選択させることも考えられる。これらの実現には、認証サーバや無線クライアント自身の変更が必要であるため、アクセスポイント、認証サーバ、クライアント、認証プロトコルのそれぞれにとって、最もインパクトの少ない方法を探ってゆく。

参 考 文 献

1) ISO/IEC8022-11 ANSI/IEEE Std 802.11 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 1999
2) IEEE Std 802.1X-2001
IEEE Standard for Local and Metropolitan Area Networks : Port-Based Network Access Control, 2001
3) RFC 2865: RADIUS
http://www.ietf.org/rfc/rfc2865.txt
4) RFC 2284: PPP Extensible Authentication Protocol (EAP)
http://www.ietf.org/rfc/rfc2284.txt