2005－DSM－39（11）
2005／10／14

徳島大学における無線ネットワーク認証基盤とその運用

三好康夫† 大家隆弘† 松浦健二‡ 金西計英‡ 佐野雅彦‡ 大恵俊一郎‡ 矢野米雄†

† 徳島大学 工学部
‡ 徳島大学 高度情報化基盤センター

徳島大学では，現在無線ネットワークの基盤整備を進めており，無線基地局の設定内容の統一，利用者認証情報の提供，利用者認証サーバの提供を行っている．これにより，学内公共エリアに設置された無線基地局を通じ，学内の全ての教職員，学生が無線 LAN 接続による学内ネットワークを同等に利用できるようになった．また，以後の無線基地局の増設時に，利用者の登録，認証サーバの設定，維持等の費用がかからない．

Implementation and Operation of Authentication Infrastructure for Wireless Network in Tokushima University

Yasuo Miyoshi † Takahiro Oie † Kenji Matsuura ‡
Kazuhide Kanenishi ‡ Masahiko Sano ‡ Shunichiro Oe ‡ Yoneo Yano †

† Faculty of Engineering, Tokushima University
‡ Center for Advanced Information Technology, Tokushima University

We have created and maintained the wireless network infrastructure for students and staff in Tokushima University. Both of the students and staff can equally use campus network with wireless LAN connection through base stations placed at campus public area. We have standardized setting of the base stations in our campus and provided authentication information and certificate servers. Registration of users, setting of additional certification servers and expense of maintenance are not necessary for extended base stations in future.

1．はじめに

近年のインターネットの進歩にともない，無線によるネットワーク利用の可能性が拡大している．一般ユーザが無線 LAN を導入し，モバイル PC を無線 LAN 接続で利用するためには，無線基地局（以下，単に基地局）とそれに接続するための無線 LAN カードを PC にインストールするだけで利用可能であり，実際に徳島大学においても多くの研究室で既に導入し利用されている．また，現在販売されているモバイル PC のほとんどに無線 LAN カードが内蔵されていることも，無線 LAN 利用の普及に拍車をかけている．しかし，徳島大学のキャンパス情報ネットワーク基盤は，主に有線系のネットワークが整備されているのみであり，学内の公共エリアで利用できるような無線ネットワークの基盤整備が望まれている．

学内の公共スペース等に基地局を設置するには，無計画に基地局を設置することは望ましくない．何故なら，無秩序な基地局の設置は基地局間の電波干渉の問題を引き起こし，無線 LAN の性能の低下を誘発することになるとともに，利用者が接続すべき基地局が不明となり結果として接続不能などのトラブルの原因となるからである．

我々は，学内の公共エリアにおける基地局の設置に関して，それらで行うべき利用者の認証を画一的に行うための認証サーバを設置し，基地局設置の方法と基地局利用のための統一的な方法について整備した．

2．無線 LAN 基盤整備の指針

2.1．学内公共エリア設置の無線 LAN 基地局

学内公共エリアとは，学内の講義棟や講義室，自習室，リフレッシュエリア等，利用面において特定の部局や学科に限定されないエリアのことである．学内公共エリアに設置された基地局は，学内の全ての教職員と学生が同等に無線 LAN 接続できることを条件とする．また，学会等のイベント開催時に学内を訪れる来客者に対する無線 LAN の利用サービスを提供可能とする．

このような場所に設置された基地局においては場所毎に異なる接続方法を要求することは得策ではなく，同じ手順で接続できることが望まれる．そのためには複数の基地局について

- 無線 LAN 接続プロトコル
- 無線 LAN のネットワーク名
- 利用者の認証方式

などの設定を共通にしておくとともに，利用者の認証を外部の統一された認証サーバに委ねる必要がある．

2.2．無線 LAN 基盤整備でサポートする範囲

通常，無線 LAN 基地局を設置するためには 1 台あたり基地局の購入費用として 2〜3 万円程度，基地局を取り付ける場所によっては敷設費用として 2 万円程度の費用とコストが必要である．また，無線 LAN の到達範囲が 20〜30m 程度，1 台の無線 LAN 基地局に収容できるユーザ数が 20〜30 ユーザ程度を考慮すると，学内の公共エリア全てに無線 LAN の基地局を設置するためには，少なくとも数千万円規模の予算が必要となる．

また，仮に基地局の設置を全て行ったとしても，ユーザである学生や教職員のモバイル PC の所有率は 100%には程遠く，またモバイル PC といえども長時間の利用に際しては商用電源の準備なども範疇にいれて計画をしなくてはならないことから，全学に同時に無線 LAN を普及させるには更に多くの設備投資が必要となることが予想される．

加えて，上記のように設置された基地局を統一的に利用できるようにするためには，接続にかかる認証を受け持つ認証サーバを設置し，このサーバにユーザの認証情報を登録する作業や各基地局にこのサーバを利用するための設定，調整等の作業が発生する[1]．

よって本基盤整備では，基地局の設置は各部局が必要に応じて行うものとし，その基地局が任意に利用できる認証サーバの提供，設置時の設定および運用面の簡便さを追求することで，費用面，作業面の負担を軽減することを目標とする．すなわち，基地局設置にかかる

- 基地局の設定内容の統一
- 利用者認証情報の提供
- 利用者認証サーバの提供

である．そのために本基盤整備においては，学内で共通に利用できる利用者認証サーバの運用を開始し，基地局が必要なときに利用できる状態とする．言い換えると，基地局の設置，運用を簡潔に行うことができる基盤を整備する．したがって，基地局の設置にかかるコストは基地局の価格と取付け工事のみとなり，利用者の登録や認証サーバの設定，維持等にかかる費用は発生しなくなる．

3．ユーザ認証基盤

3.1．各研究室での無線 LAN 認証

従来，研究室内などで運用されている無線 LAN 基地局やその設定においては，WEP（Wireless Equivalent Privacy）認証が多く利用されている．しかし，この認証方式はかなり

[1] 自前で行えば費用はかからないが，業者に委託すると恐らくこれだけでも数 100 万円程度の費用が必要であると予想される．

以前から，長時間通信を継続すると無線通信の内容を容易に盗聴できるというセキュリティ的な問題が指摘されている．また，1 台の基地局に設定できる認証のためのパスワードは 1 つのみで，無線 LAN を利用するユーザがそのパスワードを共有して利用するため，

- パスワードが漏洩しやすい
- パスワードを変更しにくい
- 利用者の特定が困難である

という問題がある．

最近では WEP と比較して盗聴されにくいと言われる WPA-PSK（Wi-Fi Protected Access with Pre-Shared Key）認証が普及してきているが，これも 1 台の基地局に 1 つのパスワードしか設定できず，先に挙げた問題を解決しない．

これらの問題は研究室内の限定された利用であれば克服できるかも知れないが，全学の利用者を対象としてパスワードの秘密性を保ちつつそのパスワードを共有して無線 LAN の運用を行うことは困難である．

3.2. 他大学での無線 LAN 認証

学内公共エリアでの無線 LAN サービスの提供は他大学においても始められているが，その多くの大学で用いられている無線 LAN 利用のためのユーザ認証はプロキシサーバを用いたものである．この方式では，無線 LAN 接続の認証には WEP や WPA-PSK 等の簡易な方法を用い，認証付きのプロキシサーバを経由してインターネットへ接続する．

利点としては，利用可能なシステム条件が低く，WPA-PSK を用いなければ比較的古い PC（OS）で利用できることが挙げられる．

しかし，利用可能なプロトコルに制限があることや，無線接続のためのパスワードの秘密性は保たれにくいため無線通信を傍受されやすいという欠点がある．

3.3. 本学における無線 LAN 認証

3.3.1. WPA-EAP

さて，無線 LAN の認証を 1 台のサーバに集約して行う技術に EAP（Extensible Authentication Protocol）[1][2] がある．この技術の詳細については文献に譲るが，EAP を用いると基地局での認証処理を外部の認証サーバへと委託することができる．また，TKIP（Temporal Key Integrity Protocol）と呼ばれる WEP の脆弱性を補強した暗号化方式を用いると，基地局-PC 間での通信の暗号化（WEP）で用いる秘密鍵を定期的に更新することが可能となり，通信内容の漏洩などのセキュリティの問題が解決する．

そこで本学の無線 LAN 基盤整備では，EAP と TKIP を採用した認証方式である WPA-EAP [3] を利用している．これは単に WPA と呼ばれたり，WPA エンタープライズと呼ばれる方式である．なお，AES（Advanced Encryption Standard）と呼ばれるさらに強固な暗号化方式が採用された WPA2 方式も存在するが，普及率を考慮して現在は WPA（TKIP）を用いている．

また，EAP で提供されている認証方式のうち公開鍵暗号を用い，かつ現在の多くの PC で利用可能な

- EAP/TLS（Transport Layer Security）：認証サーバ，ユーザともに公開鍵暗号を用いる
- EAP/PEAP（Protected EAP）：認証サーバのみ公開鍵暗号を用いる

を本無線 LAN 基盤整備で用いる．両者はどちらも認証サーバに対して公開鍵暗号に必要なサーバ証明書を発行する必要があるが，これは認証サーバの運営開始時に 1 回だけ行えば良い．

3.3.2. 教職員の認証（EAP/TLS）

“EAP/TLS”利用時には，ユーザの公開鍵暗号に必要な個人証明書が必要となる．セキュリティ的には勿論“EAP/TLS”を利用することが好ましいが，多くのユーザにとって個人証明書の発行を受けることは作業手順が増えるものでしかない．そこで，

- 通信内容の秘密性の重要度（学生が行う通信内容は教職員の行うものに対して秘密性の重要度は低い．）
- 個人証明書の無線 LAN 以外の利用の可能性（学生に対する無線 LAN 利用アカウントは無線 LAN 利用に限定して発行される[2]が，教職員に関しては個人証明書を無線 LAN

[2] 現在，学生に対して提供されている無線 LAN アカウント発行システムは，無線 LAN 利用に限定されたものである．

以外にも利用できる可能性がある[3].）の観点から，教職員に関しては“EAP/TLS”を用い，学生に関しては“EAP/PEAP”を用いて認証を行うこととした．

教職員の認証に必要な個人証明書（X.509 個人証明書）の発行は，“教育・研究者情報データベース（EDB）”[4]が運用する“EDB 公開鍵基盤（EDB/PKI）”の Web ページ[5]で発行手続きを行うことができる．また，EDB/PKI については 4 章で詳しく述べる．

3.3.3. 学生，来客者の認証（EAP/PEAP）

学生の認証で用いる“EAP/PEAP”では，個人証明書を必要とせず，アカウント名とパスワードで認証を行う．来客者に対して無線 LAN の利用サービスを提供する際の認証方式も，個人証明書と比較してユーザが簡易に扱えるパスワードを用いた“EAP/PEAP”方式を採用する．

学生が無線 LAN を利用するために必要なアカウントは，Web ページ[5]で発行を受けることができる．現在の運用では，学生の無線接続用アカウントの有効期限は半年間とし，期限が切れると再申請しなければならない．

来客者に対するアカウント発行については，5.2.節にて述べる．

3.3.4. 認証サーバの設置

図 1 は PC を基地局に接続する課程での認証手続きの様子を示したものである．個々の基地局は

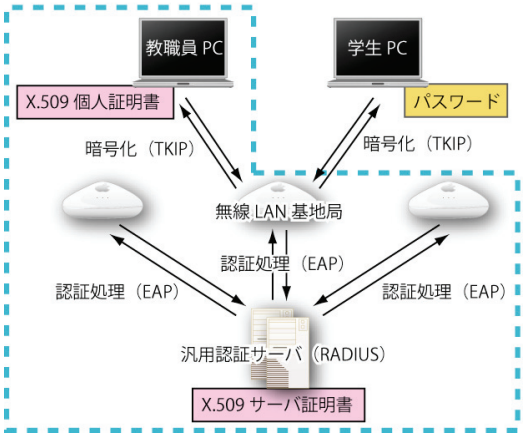

図 1 無線 LAN 認証基盤

[3] 例えば，学内 Web サーバの SSL 認証や電子メールのディジタル署名，暗号化など．

ユーザ PC からの認証要求に対して独自に認証を行うのではなく，外部に用意された認証サーバ（RADIUS）に認証のための情報を中継し，認証サーバでの検査の結果を受け取ることによってユーザの認証を行う．

現在，我々はこの認証サーバを 2 台設置し既に運用を行っている．サーバの諸元やそれぞれ基地局と PC の設定等，無線 LAN の設定に関連する情報は文献[6]に示している．

4. EDB/PKI

4.1. 教育・研究者情報データベース（EDB）

教職員を対象に提供する認証サービスに利用する公開鍵基盤（PKI: Public Key Infrastructure）は，教育・研究者情報データベース（EDB: Educator and Researcher Information Database）に登録された教職員のアカウント情報を基に構築された．

EDB は，主に教員の業績に関する情報が登録されたデータベースであり，徳島大学の EDB の Web サイト[4]にアクセスすれば，公開情報として登録された情報であれば，誰でも閲覧可能である．また，EDB 自身に関するドキュメントも充実しているので，EDB の詳細な解説についてはそちらを参照していただきたい．

4.2. EDB/PKI の特徴

認証に利用する公開鍵基盤（EDB/PKI）では，異種の認証システムとの連係を考慮しており，LDAP，RADIUS，Kerberos などの認証システムの登録情報を，EDB の登録情報を元に作成できる．また，EDB では，LDAP 等へのディレクトリ情報，DNS/BIND 等の登録情報も提供しているため，個人（クライアント）と DNS の情報（サーバ）の認証情報を管理し，矛盾のない公開鍵基盤を形成することができる．

公開鍵基盤には認証局（CA: Certification Authority）が必要であるが，一般に第三者により証明された認証局（Public CA）を運用するには膨大な資金を必要とする．しかし，利用範囲を学内（構成員）に限定するならば，自己認証局（Private CA）であっても Public CA と同等のサービスを提供できるため，現在 EDB/PKI では Private CA を用いて運営している．

4.3. EDB/PKI での証明書の発行

EDB/PKI が証明書を発行する対象は，EDB の登録情報（個人，擬人，ホスト）とし，1 登録情報に対して 1 通までの証明書を発行できる．

個人(擬人)の証明書の CN(Common Name) が教職員のアカウント名となり，学生アカウント名の c で始まる学籍番号や V で始まる来客者アカウント名と容易に区別できるように，教職員アカウントの CN は S で始まり，EDB 登録情報の識別子（EID）が続く．（ホストの証明書の CN は，いわゆる FQDN (Fully Qualified Domain Name）とする．FQDN は IP アドレスが直接関係づけられていない ALIAS（別称）でも構わない．）

証明書は EDB の Web インタフェース上で発行できる．証明書発行には，必要な一連の作業（RSA 鍵のペアの作成，証明書要求の作成，証明書の発行）を自動的に行う「おまかせモード」と，OpenSSL のコマンド等で作成済みの証明書要求ファイルから証明書を発行する「エキスパートモード」の 2 つのモードを用意している．おまかせモードでは，OS やアプリケーションにインポートするための PKCS#12（Personal Information Exchange Syntax Standard）形式のファイルがダウンロードされる．教職員は，いずれかのモードで個人証明書を発行し，PKCS#12 ファイルとルート証明書をコンピュータにインストールすることで，無線 LAN 認証や Web ページのパスフレーズレス認証等の EDB/PKI と連係した認証システムを利用できるようになる．認証サーバ（RADIUS サーバ）のサーバ証明書も同様に，上で述べた EDB インタフェース上で発行したものを利用する．

図 1 の点線で囲んだ箇所が無線 LAN 認証基盤における EDB/PKI に該当する部分である．

5. 本認証基盤を利用した運用例

5.1. 会議資料のペーパレス化

5.1.1. 工学部における教授会のペーパレス化への取組み

本学の工学部教授会と工学研究科会はほぼ月に一度の頻度で開催されており，参加資格を有する教員はそれぞれ約 80 名である．平成 17 年 1 月からの会議資料のペーパレス化に伴い，会議出席者に対して Web ページによる資料の開示を行っている．これにより，会議資料として大量に消費していた紙が節約され，大幅なコスト削減が期待できる．ただし，プライバシーに関わる情報を含む資料の扱いなど，まだ完全にペーパレスではない部分もあるが，将来的にさらなるペーパレス化を目指している．

また，会議室には本認証基盤を利用した無線 LAN 環境を用意しており，会議出席者は自由に利用することができる．これにより，会議出席者は次に示すいずれかの方法で会議中に資料を閲覧できる．

- 無線 LAN を利用できるモバイル PC を持ち込み会議資料 Web サーバに直接アクセスする
- 会議前に必要な資料をダウンロードし，個人的に印刷して持参する
- 会議室のスクリーンに投影された資料を見る

5.1.2. ペーパレス会議システムの概要

ペーパレス会議システムの構成を図 2 に示す．本システムの特徴は次の通りである．

- 会議資料を Web サーバで公開しているため，どこからでも資料をダウンロードできる
- 回収資料へのアクセスは，外部流出を防ぐため，議長の PC からのみ許可される（会議出席者はスクリーン上の資料を見る）
- 会議参加者数分の接続に十分耐えられる台数（4 台）の基地局を会議室に設置した
- スクリーンを 3 カ所設置したことにより，どの席からでも会議資料を見やすい

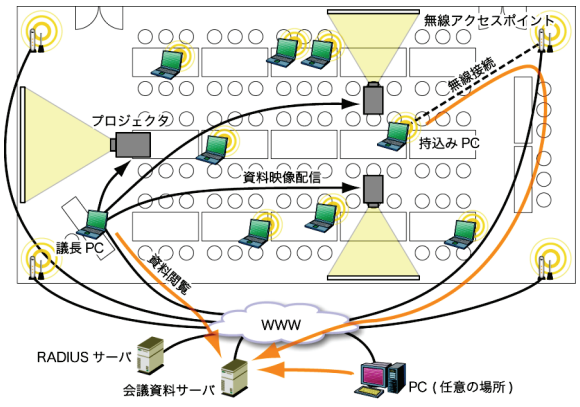

図 2 ペーパレス会議システムの構成

会議資料を公開している Web サーバは，EDB/PKI により発行されたサーバ証明書を利用して SSL/TLS プロトコルによる通信の安全化を図っており，会議参加有資格者のみが閲覧可能である．現在は，個人証明書による認証と EDB ワンタイムパスフレーズによる認証[4]を併用しているため，個人証明書を持つユーザはパスフレーズレスで認証でき，持たないユーザは EDB ログイン用のパスフレーズで認証できる．

5.2. イベント時の無線ネットワークの開放

本無線 LAN 認証基盤を利用して，学会開催等のイベント時に来客者に対して無線 LAN 接続サービスを提供可能である．

5.2.1. アカウント発行

イベント期間のみ有効としたアカウントをあらかじめ多めに発行しておき，イベント主催者にアカウントの一覧（アカウント名，パスワードのみのリスト）を提供する．イベント参加者は接続申請書を記入すると，アカウント名とパスワードを与えられ無線 LAN 接続が可能になる．

イベント主催者は，アカウント名と実際の利用者の対応がとれるように利用者から提出された申請書にアカウント名を記入し，ネットワーク管理者にすみやかに提出する．

5.2.2. 応用物理学会学術講演会での運用実績

秋期第 66 回応用物理学会学術講演会[7]において，参加者に対して本認証基盤を用いて無線 LAN 接続サービスを提供した．約 4500 名の参加者に対し，1000 アカウントをあらかじめ用意していたが，申請に対し約 660 名分のアカウントを配布した．

本認証基盤は WPA-EAP を採用したため，接続するクライアントの必要条件は，OS が Windows であれば Windows XP SP1 以上，Mac OS であれば Mac OS X 10.3 以上でなければならず，また無線 LAN カードのドライバが WPA（TKIP）に対応していなければならない．しかし，希望者の 2〜3 割は必要条件基準に達しておらず接続できなかった．

本稿執筆時にはまだ開催されていないが，2005 年度にはこの他に，日本教育工学会第 21 回全国大会[8]においても無線 LAN 接続サービスを提供する予定である．

6. おわりに

本稿では，学内公共エリアにおける無線 LAN サービスを提供するための EDB/PKI を用いた無線 LAN 認証基盤について述べた．

本稿で述べた無線 LAN 基盤整備では，学内の公共エリアに設置する基地局とその基地局に PC を無線接続して利用する場合を想定したが，今後の課題としては，各部局や学科に依存した基地局の設置についても対応させたい．これは利用者のアクセス範囲などを限定した基盤構築を行う必要があり，各部局の希望にあわせた基盤整備が必要となる．

本認証基盤は，学内における無線 LAN の利用方法を強制するものではない．しかし，学内の公共エリアの無線 LAN 基地局が共通の設定を行うことにより，利用者の利便性が飛躍的に向上することは容易に想像できる．

参考文献

[1] J. Hassell, “RADIUS — ユーザ認証セキュリティプロトコル”, O'Reilly Japan.

[2] M. S. Gast, “802.11 無線ネットワーク管理”, O'Reilly Japan.

[3] 総務省, “安心して無線 LAN を利用するために”, http://www.soumu.go.jp/joho_tsusin/lan/pdf/lan_1.pdf

[4] “教育・研究者情報データベース（EDB）”, http://web.db.tokushima-u.ac.jp/

[5] “EDB 公開鍵基盤（EDB/PKI）”, https://web.db.tokushima-u.ac.jp/assist/authentication.html#edb-pki

[6] “徳島大学無線ネットワーク”,http://ldap.db.tokushima-u.ac.jp/wireless/

[7] “2005 年秋季 第 66 回応用物理学会学術講演会”, http://www.jsap.or.jp/activities/annualmeetings/2005autumn.html

[8] “日本教育工学会第 21 回全国大会”, http://jset2005.is.tokushima-u.ac.jp/