

東京薬科大学における無線 LAN システムの導入と LISM との連携

森河 良太¹⁾, 松崎 日出海¹⁾²⁾, 宮川 毅¹⁾²⁾, 小杉 義幸¹⁾, 関口 薫³⁾, 加藤 哲太¹⁾

東京薬科大学 ネットワーク¹⁾, 情報処理教育センター²⁾, 株式会社センオス³⁾

morikawa@toyaku.ac.jp

概要：東京薬科大学では、学生会館と研究棟へのコントローラ型無線 LAN システムの導入を新たにおこなった。一般にセキュリティと利便性はトレードオフの関係にあり、無線 LAN システムの導入においてもしばしば問題となるが、本学では既存の LISM や Open Directory の統合認証システムと連携することにより、問題を解消した。具体的にはユーザーが携帯する通信端末の MAC アドレスを含むユーザー情報を一元管理することによって、Web 認証と MAC アドレス認証の選択をユーザーレベルで行えるように、無線 LAN 認証システムを構築した。

キーワード：無線 LAN、認証システム、LISM、OD2、Web 認証、MAC アドレス認証

1 はじめに

近年、各大学では教育研究の情報基盤、特に学生ユーザーとのインターフェイスとして、大規模なパソコン端末教室を整備する場合と、学生一人一人にノート型パソコンを必携してもらい、大学側はそれをネットワークに接続する環境を整備する場合に二極分化しているようである。大学の様々な事情により、それぞれ特色ある情報基盤のインターフェイスが構築されているが、東京薬科大学では後者、すなわち学生に一人一台、ノート型パソコンをキャンパスライフのための道具として入学時に購入してもらう教育方針を、1995年4月より継続している[1]。

この方針の示す大きな目標は、「パソコンを身近な道具として感じ、苦手意識を減らす」、「パソコンのメンテナンスを学生自身が管理者となっていく」、「専門科目の授業や研究の場面で、必要なアプリケーションを学生自身で導入する」という3点であり、最終的には“Do it yourself”という標語に集約されると考えている。この目標に到達するためには、授業計画や不定期の講習会に盛り込まれたカリキュラムを実施するだけでなく、授業以外の場面でノート型パソコンを十分に活用できるような情報基盤を、学内に整備、展開する必要がある。

そのため本学では学生が所持するノート型パソコンを学内ネットワーク (TYCOON) に IP 接続できるように、学内各所の教室に有線 LAN 接続施設を順次構築してきた[2]。そして2011年10月現在では、29教室、約3,600口の情報コンセントが学内に整備されている。これらの施設を学生

に頻繁に使ってもらうためにも、アクセシビリティの高いシステムによる、ノート型パソコンの IP 接続法が望まれる。しかし同時に、システムの利便さ故に、学生の ICT 活用能力を低下させることのないような教育的配慮を、システムに埋め込む必要があると考えられる。さらに大学と無関係の第三者による利用や悪用を防ぐためにも、多少の利便性を低下させても、セキュリティの確保をしっかりと行わねばならない。

これらの教育的要件を考慮しつつ、東京薬科大学では2010年度に増築した学生会館 (旧厚生棟) および翌年度に竣工した新研究棟 (研究4号館; 130周年記念館) において、IEEE802.11a/b/g/n (11Mbps、54Mbps)の規格に基づく無線 LAN 接続システムを構築した。

2 無線 LAN システムの概要

2.1 無線 LAN 導入に至る経緯

無線 LAN システムは、学生会館の増改築および研究棟の新築に伴い、情報基盤整備事業のインフラ整備の一環として新たに設計・構築した。本学では3、4年前より、無線 LAN の導入に対する要望は、学生や教員のみならず、学生の父兄からも強い声で望まれていた。しかし当時は、学内ネットワークにおけるセキュリティの確保、無線 LAN 自身のセキュリティの技術レベル、大量同時アクセス時における通信速度の顕著な低下の問題、そして機器が高価であることなどが、導入の障害として議論されていた。そしてそれ以上に、学生が無線 LAN をネットワークゲームに利用するという、教育上の懸念も無線 LAN の導入を躊躇さ

せていた。

先に述べたように、本学では全学生が入学と同時にノート型パソコンを必携し、情報教育をはじめとする様々な教育カリキュラムの中で、学生ネットワークに接続しながら利用されている。近年では、iPhone や Android などのスマートフォンなどの携帯電話の普及に伴い、学内でも多くの学生がスマートフォンを利用するようになり、従来通りキャンパスライフの情報端末としてノート型パソコンも使いつつも、情報収集・活用のツールとしてスマートフォンをメインの情報端末として利用する学生も増えている。具体的には、学生ポータル、図書システム、履修申請などでスマートフォンを利用する例が多々見受けられるようになった。これらの背景や事情を考慮すると、学内に無線 LAN を整備し、ユビキタスなネットワーク環境を整備することは、避けて通ることは難しい状況となった。

2.2 無線 LAN システムの導入

前述の理由により、本学では新規に無線 LAN システムを TYCOON の一部として導入することになった。そして複数ある無線 LAN システムの会社から Meru Networks 社の無線 LAN システムを採用した。特に採用に際して、チャンネル設計とセキュリティの 2 点に関しては、選定の重要項目として取り上げた（以下の「無線 LAN システムの特徴」2、4 に該当）。

無線 LAN システムの特徴[6]

- 1.集中制御型無線 LAN システム（一元管理）
 - ・自律分散型→集中制御型
- 2.チャンネル設計が容易（チャンネルの干渉）
 - ・マイクロセル方式→シングルチャンネル方式
- 3.ハイデンシティ（エアタイムフェアネス）
 - ・クライアント毎に均等に時間を割り当て
- 4.セキュリティ（ネットワーク通信の安全性）
 - ・標準セキュリティの採用（WPA、WPA2 等）
 - ・802.1x 認証
 - ・MAC フィルタリング
 - ・その他
- 5.IEEE802.11a/b/g/n（11Mbps, 54Mbps）
 - ・高速通信
- 6.バーチャルセル/バーチャルポート
 - ・移動通信
- 7.電波の身体への影響
 - ・医療機関の事例（福井大学医学部付属病院）

8.統合認証システムと無線 LAN システムの連携

- ・LISM 及び LDAP とのシステム連携
- ・Web 認証、MAC アドレス認証

9.その他

2.3 無線 LAN システム導入における課題

一般に、無線 LAN システムを大規模に導入する際に一番問題となる点は、Wi-Fi チャンネルの設計に関する前準備である。無線 LAN アクセスポイント（以下“AP”と略）を設置する対象となる大学の建築物の構造は、一つのフロアに複数の研究室があり、かつ、上下階のフロアが存在する。このことから無線 LAN を設計・構築する際に、AP 同士の電波干渉を起こさないように電波を計測し、AP の設置を決め、かつ、チャンネルの振り分けを検討する必要がある[3]。この場合、専用機器による調整が必要となるため難しく費用がかかる。

これに加え多くの大学では、研究室単位で勝手に無線 LAN ルータを導入しているケースが多々みられる。すなわち設置されている既存の無線 LAN システムとの共存、すなわちチャンネルの再設計を各部署に要請する必要もある。

そこで本学では、導入する無線 LAN システムの要件として、従来のチャンネルマイクロセル方式ではなく、シングルチャンネルデプロイメントを挙げた。これにより 1 台の無線 LAN コントローラで同一チャンネルを制御することができ、PoE(Power over Ethernet)に対応した LAN スイッチを設置している場所であれば、ほとんど自由に、事前の詳細な設計なしに複数の AP を建屋内に配置することが可能となった（表 1）。

表 1 無線 LAN の配備

	場所	面積 (㎡)	AP
研究 4号館	1階フロア	1,435	6
	2階フロア	1,337	9
	3階フロア	1,379	8
	4階フロア	1,337	9
	5階フロア	1,337	9
	合計	6,825	41
学生 会館	1階学生スペース(ラウンジ)	490	5
	1階食堂(柏木)	974	8
	1階サービスエリア	127	0
	2階学習スペース(談話室)	254	3
	2階学習スペース(PIT)	235	0
	2階カフェテリア	691	5
	合計	2,771	21

注 1) 学習スペース (PIT) : 有線 LAN を設置

3 無線 LAN 接続における認証

東京薬科大学では、電子メールシステムや e ラーニングシステムのユーザー認証システムとして、統合認証管理システム LISM (LDAP Identity Synchronization Manager) [4]をメタディレクトリとする、Open Directory (Open LDAP) [5]および Active Directory を運用している (TYCOON 認証システム)。この認証システムには本学の全構成員が登録されており、個々人に割り振られたユーザー識別子は「東薬 ID」と呼ばれている。前述の無線 LAN 接続においても、東薬 ID によるユーザー認証を用いることは、アクセシビリティを高めることに繋がる。しかし Meru Networks 社の無線 LAN[6]における Web 認証システムは、外部認証システムとして LDAP や Active Directory に対応しておらず、TYCOON 認証システムをそのまま使うことができなかった。そこで Open Directory (Open LDAP) サーバとして用いている Mac OS-X Server 10.6 にて、標準で装備されている RADIUS サーバを追加稼働し、Open LDAP と RADIUS 認証を連携させ、無線 LAN におけるユーザー認証を行った (図 1)。嬉しいことに Mac OS-X 10.6 Server では、特別なカスタマイズなしに RADIUS の設定のみで、RADIUS と Open LDAP を自動的に連携させることができた。

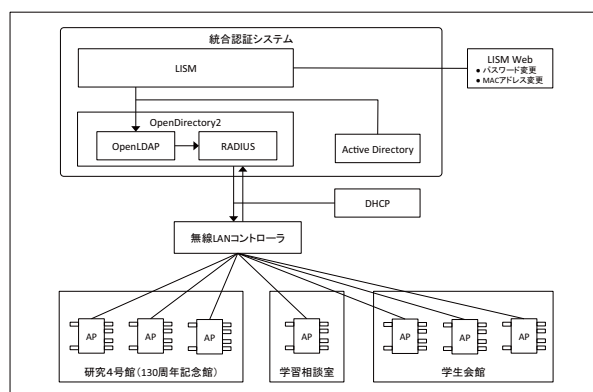


図 1 無線 LAN システムの構成

Web 認証は学内の統一した ID を用いるという点で、ユーザーはパスワードを忘れることなく、平易に認証を成功させることができる。しかし研究棟のような、研究者や教員が日常的に無線 LAN を利用する施設では、無線 LAN 接続を行う度に Web ブラウザを立ち上げてユーザ名とパスワードを入力する作業は、大変面倒で退屈な作業となる。そこで無線 LAN 端末となるパソコンの MAC アド

レスを用いた機器認証が、その解決策として挙げられた。ただし、パソコンを新規に購入する度に事務的に MAC アドレスをネットワーク管理者に申請、登録することは、大学という自由で自主的な世界、少なくとも本学においては、まだまだ敷居の高い行為である。よって LISM と連携して稼働している東薬 ID のパスワード変更 Web システムに手を加え、無線 LAN に接続したい端末の MAC アドレスを最大 2 つまで、教員と事務員に限り、パスワード変更サイトから登録できるようにした (図 2)。

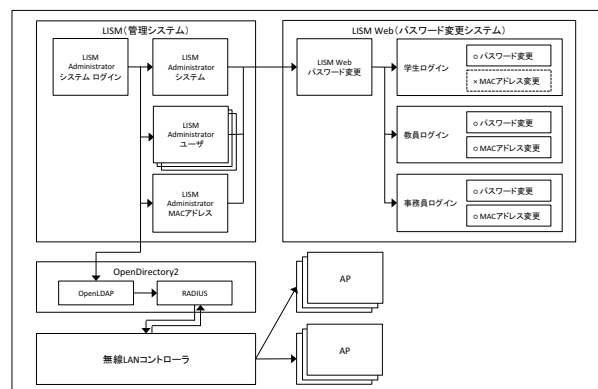


図 2 Web 認証システム

SSID による無線 LAN のグループ認証は、WPA2/PSK の暗号化方式に従って予めセキュリティキーを無線 LAN 端末となるパソコンに登録することによって行われる。大学によってはこのセキュリティキーの文字列を、施設の掲示板に貼り出しているところも見受けられるが、本学ではそのような掲示は行っていない。それはセキュリティ上の問題というよりはむしろ、情報教育上の問題として対応しているからである。

現状における無線 LAN 認証の方法については以上であるが (表 2)、将来、学生に対する認証セキュリティを更に向上させる必要性が生じた場合、Web 認証と MAC アドレス認証の双方を満たすことを、利用のための必要条件として設定することも検討している。

表 2 無線 LAN 接続における認証方法

	SSID 認証	Web 認証	MAC アドレス認証
学生	必要	可能	不可能
教員 事務員	必要	可能	可能

4 今後の展望

本学では無線 LAN 接続システムとして、バーチャルセル技術を独自開発した Meru Networks 社のシステム[6]を採用し、学内の2つの Wi-Fi チャンネル(2.4GHz 帯 1ch と 5GHz 帯 48ch)のみをネットワーク運営委員会として管理しさえすれば良いようになった。そして残りのチャンネルについては、従来通り教室や研究室の独自管理に任せることができ、管理コストの削減を行うことができた。

また食堂や談話室など「学生の憩いの場」となる学生会館と、その対極にあるアカデミックな「研究棟」に対し、同時期に無線 LAN 認証接続サービスを開設した。そのためユーザー認証に基づく Web 認証と、機器認証である MAC アドレス認証の二つの方法を選択できるよう、認証システムを構築した。他大学においては、この2種類の認証を同時に課すような厳しいシステムを運営している事例もあるが、本学ではそこまで厳重なセキュリティを課さねばならないようなトラブルは、今のところ幸いにして生じていない。

今後は学内における無線 LAN 接続施設を増やしていくことを予定しているが、バーチャルセル技術の御陰で、複雑なチャンネル分配計画とそれに伴う AP の物理的配置を検討する必要性は今のところ全くない。すなわちこれは、巨額の予算を投じて一気に全学を無線 LAN 化する計画を立てる必要がないことを意味する。我々ネットワーク管理者は、学内のユーザーからの要望と運用コストを考慮しながら、必要に応じて必要な場所に AP を柔軟に配置することができるのである。

参考文献

- [1] 森河 良太、林 昌樹、「東京薬科大学における情報ネットワークと教育への活用」、平成 8 年度 情報教育研修集会講演論文集、1996.
- [2] 森河 良太、林 昌樹、宮川 毅、土橋 朗、「TYCOON の概要と現状」、東京薬科大学研究紀要、第 1 号、pp.77-84、1998.
- [3] 木村 真一、木本 雅也、大野 賢一、「無線 AP 配置の最適化による電波利用率の向上」、学術情報処理研究、No.15、2011.
- [4] 森河良太、松崎 日出海、宮川 毅、小杉 義幸、東浦 康友、関口 薫、加藤 哲太、「LISM による認証基盤の統合と拡張」、平成 22 年度 情報教育研修集会講演論文集、pp.153-155、

2010.

- [5] 松崎 日出海、濱田 真向、森河 良太、宮川 毅、小杉 義幸、土橋 朗、「東京薬科大学 OpenDirectory2 を用いた認証システムの構築事例」、平成 18 年度 情報教育研修集会講演論文集、pp.526-527、2006.
- [6] Meru Networks 無線 LAN システム、<http://www.merunetworks.co.jp/>