

九州工業大学・全学セキュアネットワーク導入における無線 LAN 更新

福田 豊^{1,a)} 中村 豊^{1,b)} 佐藤 彰洋^{1,c)}

概要：九州工業大学では、2014 年 9 月に戸畑、飯塚、若松の 3 キャンパスに渡る全学セキュア・ネットワークシステムを導入した。この導入の中で、無線 LAN システムを IEEE 802.11ac に対応する機材に更新し、3 キャンパスそれぞれに無線コントローラを設置していた構成の見直しや、冗長構成化等を実施した。本稿では、更新における機材選定や構成の見直し、導入時の移行方法等について述べる。

キーワード：無線 LAN, 導入, 運用

Campus WiFi upgrades at Kyushu Institute of Technology

1. はじめに

九州工業大学は 2014 年 9 月にネットワーク設備の更新を行った。今回の更新では本学の戸畑、飯塚、若松の 3 キャンパスに渡って別々に導入されてきたネットワークを統合し、より効率的で安全な運用管理が可能なネットワーク基盤を目指して構成を検討した。更新後のネットワーク構成は有線ネットワーク機材とファイヤーウォール、および無線 LAN に大別できるが、本稿ではこの内、無線 LAN について述べる。

本学では 2001 年から無線 LAN による情報コンセントサービスをスタートさせ、2010 年度には戸畑、飯塚両キャンパスで自律分散型のアクセスポイントから集中制御型無線 LAN 装置に切替えた。導入当初は講義室を中心に飯塚キャンパスに 34 台、戸畑キャンパスに 47 台、合計 81 台のアクセスポイントを設置した。また、若松キャンパスは 2007 年度に集中制御型無線 LAN を導入し、37 台のアクセスポイントを設置した。以後、戸畑、飯塚両キャンパスで建屋改修時にアクセスポイント設置を提案したり、無線 LAN 整備プロジェクトを企画・実行した結果、更新直前

には 3 キャンパス合計でアクセスポイントを 198 台まで増やすことができた。さらにこのエリアの拡大に伴って、無線 LAN の 1 日当たりの平均利用者数も図 1 に示すように順調に増加して来た。

こうした利用状況の拡大傾向を踏まえ、今回の無線 LAN の更新では、(1) 無線 LAN の処理性能向上と、(2) 更なる提供エリアの拡充、及び (3) 管理体制の強化を目指すことにした。この目標の下、更新後の構成について以下に示す検討を行った。

- (1) IEEE 802.11ac [1] の導入
- (2) 無線 LAN エリアの拡充
- (3) コントローラの集約と冗長構成化
- (4) PoE (Power Over Ethernet) 全面導入
- (5) 無線 LAN 統合管理システムの導入
- (6) 認証システムの導入

上記項目に従って調達機材の要件を定義し、調達機材決定後は要件を満たすことができるようにネットワークを構築した。こうした検討に加えて、出来るだけ無線 LAN のダウンタイムを短くできるように移行作業を工夫した。具体的には、新しいコントローラで提供する無線 LAN 用に予めネットワークアドレスを確保し、新旧コントローラを並行稼働させることで、接続停止時間の短縮化を図った。

以降、2 節では更新前の無線 LAN システムについて、3 節で新システムの要件、4 節では導入について述べ、最後に 5 節でまとめと今後の課題を示す。

¹ 九州工業大学 情報科学センター
Information Science Center, Kyushu Institute of Technology,
Sensui 1-1, Tobata, Kitakyushu, Fukuoka 804-8550, Japan

a) fukuda@isc.kyutech.ac.jp

b) yutaka-n@isc.kyutech.ac.jp

c) satoh@isc.kyutech.ac.jp

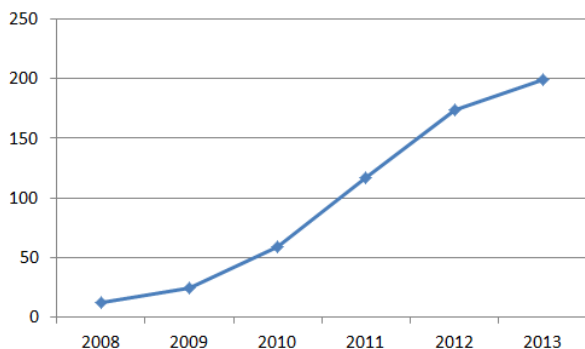


図 1 1 日平均利用者数 (2008 年 ~ 2013 年)

2. 更新前の無線 LAN システム

更新前の無線 LAN システムを表 1 と図 2 に、また SSID (Service Set Identifier) と認証方式、及び割り当てていたネットワークアドレスを表 2 に示す。

無線 LAN コントローラは戸畑、飯塚、若松の 3 キャンパスそれぞれで独立して稼働しており、各アクセスポイントは同じ IP アドレス体系ながらもキャンパスごとに異なる VLAN ID を割り当てられたネットワークに所属していた。また、アクセスポイントへの給電は PoE [2] と PoE インジェクタ、及び AC 電源を用いていた。

戸畑、飯塚キャンパスで提供していた無線 LAN 規格は IEEE 802.11a/b/g/n [3] で、2.4 GHz 帯には学内用に加えて eduroam [4] と学外者の一時的な無線 LAN 利用向けの 3 つの SSID を、5 GHz 帯には学内用に 1 つの SSID を提供してきた。eduroam には若松を含む 3 キャンパス共用で /24 のネットワークアドレスを 1 つ割り当てていた。学内向け SSID には戸畑、飯塚キャンパスそれぞれに /24 のネットワークアドレス 1 つを確保し、2.4 GHz と 5 GHz 用 SSID で共用していた。

また学内用/学外者用の SSID では、2013 年度までは NetSpring 社 Ferec 720 による web 認証を利用し、無線 LAN 専用の ID/Password を発行していた。さらに、無線 LAN に同時接続出来る端末は 1 台のみという制限も設けていた。しかし、本学で統合 ID 環境が整備されたことから、2014 年度からは学内統合 ID を利用した IEEE 802.1X [5] 認証に変更し、同時接続数の制限も無くすことにした。これに伴い、Ferec による web 認証は学外者の一時的な利用向けにのみ残すことになった。

一方、若松キャンパスは IEEE 802.11 b/g に対応した無線 LAN コントローラを利用しており、2.4 GHz 帯で学内向けと eduroam 向けの 2 つの SSID を提供していた。また、学内向けの SSID では mac アドレスによる認証を行い、mac アドレスはコントローラ内部で管理していた。AP への給電には主に Cisco 社の PoE インジェクタ AIR-PWRINJ3 を利用していた。

3. 新しい無線 LAN システムの要件

1 節で述べたように、今回の導入では (1) 無線 LAN の処理性能向上と、(2) 更なる提供エリアの拡充、及び (3) 管理体制の強化を目指して、以下に示す 6 つの要件を検討した。本節では各項目について述べる。

3.1 IEEE 802.11ac の導入

今回の更新では、貸借期間が従来の 4 年から 5 年へと 1 年間延長されることになった。よって、それだけ長い期間に渡って本学のネットワーク基盤として活用できる機材が必要となる。導入機材の検討期間中、通信速度がより高速化された IEEE 802.11ac の標準化作業が進んでいたが、更新時期に対応機材が発売されるかどうかは不明であった。しかし、従来と同規格の IEEE 802.11n での移行では今後の通信需要増大に十分応えることが出来なくなる恐れがあるため、IEEE 802.11ac の導入を前提として標準化動向を注視し、更新時期に間に合うよう製品が発売されることを確認後、IEEE 802.11ac に対応することを導入機材の必要要件とした。また、従来の中央制御型に加え、コントローラを必要としない自律分散型の無線 LAN 製品も検討したが、大規模無線 LAN での運用実績や運営管理が未知数であったため、自律型分散型は時期尚早と考え、従来通りコントローラを備え集中制御可能であることを要件とした。

3.2 無線 LAN エリアの拡充

2010 年度に集中制御型の無線 LAN コントローラを戸畑、飯塚キャンパスに導入後、講義室やリフレッシュスペース等公共性が高い場所を中心にアクセスポイントの整備を進めてきた。こうした場所に加えて、今回は有線機材が全キャンパスに渡って展開されることから、設定投入やトラブル対応時にインターネットへのアクセス回線を確保するために、ノードスイッチが設置される場所にはアクセスポイントを設置することにした。さらに、改修された建屋や PBL (Project Based Learning) 学習等のために新設された講義室には、アクセスポイントを新設することにした。

3.3 コントローラの集約と冗長構成化

更新前は戸畑、飯塚、若松の 3 キャンパスそれぞれに無線 LAN コントローラを設置し、異なる VLAN ID を利用して各キャンパス内に閉じた管理を行ってきた。しかし、費用対効果の面からコントローラは戸畑、飯塚各キャンパスの 2 台体制に集約し、若松キャンパスのアクセスポイントは戸畑キャンパスのコントローラに収容することにした。これに伴い、既存のアクセスポイント管理用 VLAN は廃止し、キャンパス間にまたがって運営管理を行う機材向けの VLAN ID から無線 LAN 用を確保し、全てのアクセス



キャンパス	種別	メーカー名	型番	台数	備考
戸畑	コントローラ	Aruba	3600	1	
	アクセスポイント	Aruba	AP-105	107	IEEE 802.11a/b/g/n, 2x2 MIMO
飯塚	コントローラ	Aruba	3400	1	
	アクセスポイント	Aruba	AP-105	54	IEEE 802.11a/b/g/n, 2x2 MIMO
若松	コントローラ	Aruba	a2400-48	1	
	アクセスポイント	Aruba	AP61-W5X	37	IEEE 802.11b/g

- (1) 認証機能として、Web 認証、MAC 認証、IEEE802.1X 認証向けの RADIUS 機能を有すること
- (2) 証明書を発行する機能を有すること
- (3) アカウントの作成、編集、削除機能を有すること
- (4) アカウントの一括編集機能を有すること
- (5) 外部 LDAP/AD にユーザ情報を参照して、認証を行う連携機能を有すること
- (6) 本調達に含まれる仮想基盤システム上で動作すること

表 2 各周波数帯の SSID, 認証, ネットワークアドレス

キャンパス	SSID	周波数帯	認証	ネットワークアドレス
戸畑	学内用	2.4 GHz, 5 GHz	IEEE 802.1X	/24 を 2.4 GHz 用と 5 GHz 用の SSID で共用
	eduroam	2.4 GHz	IEEE 802.1X	/24 を 3 キャンパスで共用
	学外者用	2.4 GHz	web 認証	/24 を使用
飯塚	学内用	2.4 GHz, 5 GHz	IEEE 802.1X	/24 を 2.4 GHz 用と 5 GHz 用の SSID で共用
	eduroam	2.4 GHz	IEEE 802.1X	/24 を 3 キャンパスで共用
	学外者用	2.4 GHz	web 認証	/24 を使用
若松	学内用	2.4 GHz	mac アドレス認証	/24 を使用
	eduroam	2.4 GHz	IEEE 802.1X	/24 を 3 キャンパスで共用

4. 導入

本節では, 新たに導入した機材と導入作業, および導入後の稼働状況について述べる.

4.1 新しい機材

調達の結果, 新たに導入する機材はこれまでと同様 Aruba 社製品となった. 無線 LAN コントローラは 7210, アクセスポイントは AP-225 (1 箇所のみ屋外用として AP-175P を導入) である. PoE スイッチは Juniper 社の EX2200-24P と EX3300-48P となった. 共に IEEE 802.3at/af に対応しており, EX2200-24P は最大 405 W, EX3300-48P は 740 W まで給電可能である. また, PoE インジェクタは IEEE 802.3at 対応の Microsemi 社 PD-9001GR/AC-JP となった. また, 認証システムは日立電線ネットワークの Account@Adapter となった. 導入機材の一覧を表 3 に示す.

4.2 構成検討

まず最初にアクセスポイントとコントローラの接続構成について, 全てのトラフィックがコントローラを経由する *Tunnel* 方式と, アクセスポイントから幹線側に直収される *Bridge* 方式を検討した. *Bridge* 方式の場合, コントローラとの接続が切断されても接続済の端末はそのまま通信を継続することができる. また, 若松キャンパスのアクセスポイントは戸畑キャンパスのコントローラを経由せずに通信することができる. その一方で, 全てのアクセスポイントまで SSID に紐づく VLAN を延伸する必要があることや, コントローラでの web 認証が利用不可であること, アクセスポイント側での処理負担増により通信性能が低下することが分かったため, 今回は従来と同様全てのトラフィックがコントローラを経由する *Tunnel* 方式とした.

コントローラは検討通り戸畑, 飯塚キャンパスに集約し, 若松キャンパスのアクセスポイントは戸畑キャンパスに設置するコントローラに収容することにした. またコントローラは戸畑, 飯塚間で冗長構成を組むことにした. この構成では若松キャンパスのトラフィックは必ずキャンパス間を経由することになるため, コントローラは幹線スウィ

チではなく, より上位のキャンパス間スイッチの配下に接続することにした. また, トラフィックがコントローラに集中する対策としては, コントローラとキャンパス間スイッチの接続を 10 GBASE-SR に増強した. なお, ライセンスはコントローラ間で集約して利用可能であり, 個別の同数ライセンス導入は不要であった.

PoE スイッチとインジェクタは, 運用管理効率を考慮して各建屋の受け口となるノードスイッチに収容することにした. なお, 各スイッチの詳細については [7] を参照.

SSID は, 若松キャンパスに 5 GHz 帯の学内用 SSID を追加した他は従来環境をそのまま引き継ぐことにし, チャネルボンディングによる増強も導入時点では見合わせた. 一方で, IEEE 802.1X 認証の導入後, 無線 LAN を利用する端末数が急速に増加しており, 導入直前には /24 のネットワークでは不足であることが判明した. 一人当たり無線 LAN に接続する端末はノートパソコンだけでなくタブレットやスマートフォンなど多様化しているため, 今後の増加も見越して, 戸畑, 飯塚キャンパスの学内向け SSID には /20 のネットワークを提供することにした.

学外者の無線 LAN のアカウントは Account@Adapter で管理することにし, 認証は Aruba 7210 の captive portal による web 認証を利用することにした. これにより, 同時接続の制限を受けずに, アカウントを提供することが可能となった. 以上の検討による無線 LAN の新しい構成を図 3 に示す.

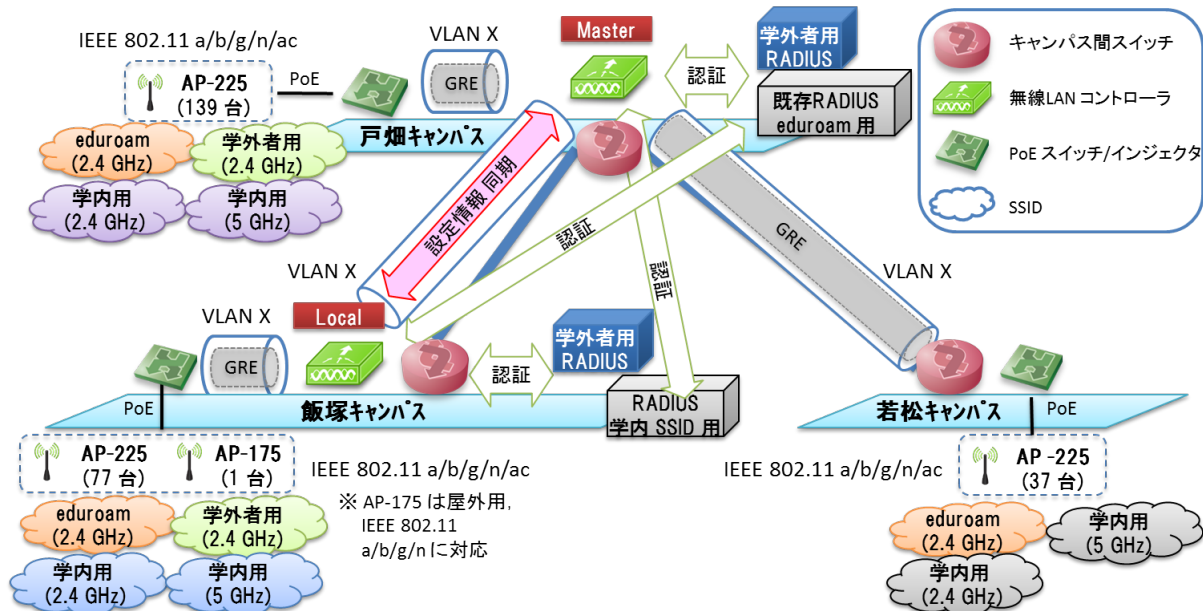
4.3 移行作業

試験期間などを避けて調整した結果, 実際の機材更新作業は以下のように進めることになった.

- 7/19, 20 若松キャンパス内機材更新. 戸畑キャンパスに無線 LAN の新コントローラ投入
- 8/12 キャンパス間スイッチ更新
- 8/13,14 戸畑キャンパス・コアスイッチ更新
- 8/15 飯塚キャンパス・コアスイッチ更新. 飯塚キャンパスに無線 LAN の新コントローラ投入
- 8/18 以降, 順次ノード, フロアスイッチ, アクセスポイント等更新

無線 LAN の更新はネットワーク停止を出来るだけ最小限に抑えるため, 新しいコントローラで提供する SSID 用

種別	メーカー名	型番	台数	備考
コントローラ	Aruba	7210	2	戸畑, 若松キャンパスに設置, 冗長構成化
アクセスポイント	Aruba	AP-225	253	IEEE 802.11ac 対応, 3x3 MIMO
屋外用アクセスポイント	Aruba	AP-175	1	IEEE 802.11a/b/g/n, 2x2 MIMO
統合管理ソフトウェア	Aruba	AirWave	1	仮想基盤上にインストール
PoE スイッチ	Juniper	EX2200-24p, EX3300-48P	55	IEEE 802.3af/at 対応
PoE インジェクタ	Microsemi	PD-9001GR/AC-JP	10	IEEE 802.3af/at 対応
認証システム	日立金属	Account@Adapter	1	仮想基盤上にインストール



5

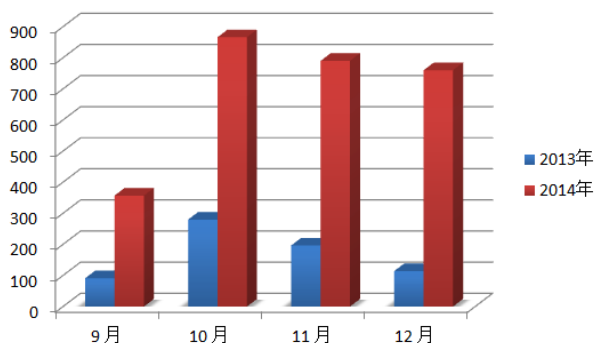


図 4 平均利用者数 (9 月 ~ 12 月)

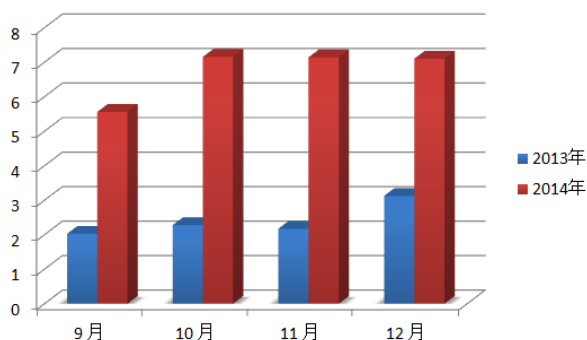


図 5 平均利用回数 (9 月 ~ 12 月)

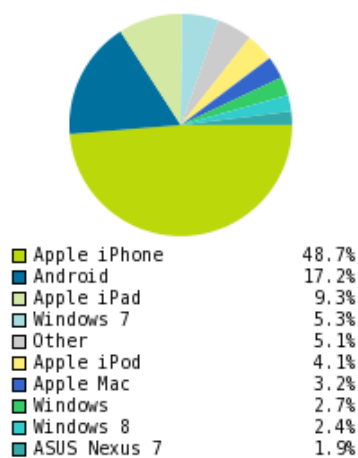


図 6 端末種別

くなったこと、スマートフォンやタブレットなどの普及により一人が持つ無線 LAN 接続端末が増えたこと、などが挙げられる。最後に、接続端末数が 900 台を超えたある時間における端末種別を図 6 に示す。図 6 より、本学では iPhone/iPad ユーザが非常に多く半数を超えることが分かる。今回の更新で導入した無線 LAN 管理ソフトウェアによりこうした情報に素早くアクセスすることができるようになった。よって今後は取得出来る情報を活用した無線 LAN の効果的な運用を行う必要がある。具体的には混雑状況からアクセスポイントの増強を検討したり、電波干渉対策等を実施する予定である。

5. まとめと今後の課題

本稿では本学での無線 LAN 更新作業について述べた。導入機材は今後 5 年間に渡る使用期間を考慮して IEEE 802.11ac 対応とし、コストの低減と耐障害性の向上のためにコントローラは 2 キャンパスに集約し冗長構成を組むことにした。また、移行作業の際には移行後の新ネットワークアドレスを予め確保することで新旧コントローラを並行稼働させ、無線 LAN の停止を極力短くするようにした。さらに、規模の拡大に対して効率的な運営管理を行うため、無線 LAN 管理ソフトウェアを新たに導入した。

今後の課題として、各学科の研究室など大学の無線 LAN サービスを提供していないエリアへの拡張がある。またこうした規模の拡大に併せて、大学全体としての電波管理や各研究室や個別の部署に無線 LAN をどのように提供していくかも検討を行っていく予定である。

参考文献

- [1] IEEE : IEEE Standard for 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-Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz, IEEE 802.11ac-2013 (2013).
- [2] IEEE : IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Data Terminal Equipment (DTE) Power Via Media Dependent Interface (MDI), 802.3af-2003 (2003).
- [3] IEEE : IEEE Standard for 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, IEEE 802.11-2012 (2012).
- [4] eduroam : <http://www.eduroam.org>
- [5] IEEE : IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control, IEEE 802.1X-2010 (2010).
- [6] IEEE : IEEE Standard for Information technology- Local and metropolitan area networks- Specific requirements-Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements, 802.3at-2009 (2009)
- [7] 中村豊, 福田豊, 佐藤彰洋 : 九州工業大学における全学セキュア・ネットワークの導入について, 情報処理学会技術研究報告 (インターネットと運用技術研究会), 2015