Eduroam によるゲスト用無線 LAN サービスの更改

伊藤 和哉, 中村 直毅, 長瀬 祥子, 葭葉 純子,

高畑 知香, 鈴木 麻里恵, 冨永 悌二

東北大学大学院 医学系研究科・医学部 情報基盤室

k.ito@med.tohoku.ac.jp

Renewal of the Wi-Fi for Visitors Using Eduroam

Kazuya Ito, Naoki Nakamura, Sachiko Nagase, Junko Yoshiba,

Chika Takahata, Marie Suzuki, Teiji Tominaga

Information Infrastructure Office, School of Medicine, Tohoku University.

概要

昨今、大学キャンパスで行われる各種学会やセミナーでは、会場内でのゲスト（来訪者）用無線 LAN サービス（以下、ゲスト無線）の提供が必要不可欠となっている。一方、ゲスト無線は、その特性上、接続するユーザが不特定多数であるとともに、接続する機器のセキュリティ対策の状況が不透明であり、管理上のセキュリティリスクが非常に高く、注意して運用する必要がある。また、大学の教職員が日常業務で利用する無線機器や無線空間を併用する場合、ゲスト無線の提供による日常業務への影響を最小限にする考慮が必要である。今回、東北大学星陵キャンパスでは、無線サービス向上を目的として現状のゲスト無線を廃止し、教育研究機関間の国際無線 LAN ローミング基盤 eduroam（以下、eduroam）を導入し、キャンパス全域にサービスを展開した。本稿は、その整備の詳細について報告する。

1 はじめに

医療系の部局が集約された東北大学星陵キャンパスでは、4 部局が共同で 1 つの統合されたネットワーク基盤を運用している。約 7 年前からゲスト無線を提供しているが、ゲスト無線の利用の度に複雑な設定をする必要があり、運用の改善が必要な状況であった。そこで、従来のゲスト無線を廃止して新たに eduroam［1］を導入することとした。eduroam は国内教育研究機関のみならず、全世界共通でアカウントを利用することが可能であり、利便性がとても高い。東北大学では大学本部で eduroam を提供する基盤［2］を用意しており、学内の多くの部局で導入している。

星陵キャンパスでは既に無線環境が整備されているため、運用中の無線環境に相乗りして組み込む必要があり、現状の構成や設定ポリシーを踏襲して実現する必要があった。

本稿では、先ず 2 章でゲスト無線の概要と構成について述べる。3 章では eduroam の特徴と導入における課題及び実装の詳細を述べる。4 章では本番環境への切り替えとその後の運用状況を述べる。5 章は本稿のまとめである。

2 ゲスト無線の概要

2.1 システム構成

始めに星陵キャンパスの無線環境におけるシステム規模を**表 1** に示す。

表 1 無線環境のシステム規模

無線の主な利用ユーザ	大学教員、事務職員、技術職員、研究支援者、研究室スタッフ、学部生、大学院生、外部講演者、外部ゲスト、関連業者、大学病院医師、看護師、医療スタッフ、医事職員、入院患者
無線利用ユーザ数	常時約 1500ユーザ
無線アクセスポイント数	約900台
無線アクセスポイント機器種類	8種類（機器ベンダー4社）
無線コントローラ数	6台（機器ベンダー2社）
SSID数	25SSID

※上記対象は大学管理の無線機器のみ（各研究室管理の無線機器は除く）

利用ユーザは大学の教職員と学生、外部ゲストの他、大学病院の医療系スタッフなど様々で、常時約 1500 ユーザが利用している。また、通常のキャンパスネットワークとは違い、病院の診療業務

による無線の利用がある。診療業務では無線エリア全域で機器の冗長化が必要となり、設置している無線アクセスポイントは約 900 台に上る。

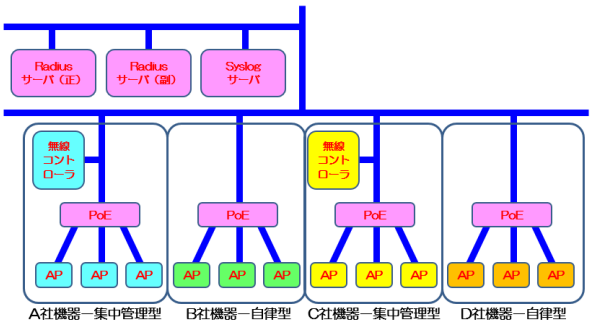

図１　無線環境の物理構成

次に、無線環境の物理構成を**図１**に示す。

既存の無線アクセスポイントは、無線コントローラによる一括管理を行う集中管理型と、無線アクセスポイント自身が単体で動作する自律型のそれぞれが運用しており、更にその両方にて複数ベンダーの機器が稼働している。また、無線アクセスポイントへは PoE（Power over Ethernet）給電にて電力を供給し、接続時のユーザ認証は Radius サーバ（正・副）が行い、認証ログとアクセスログは Syslog サーバが一括管理している。

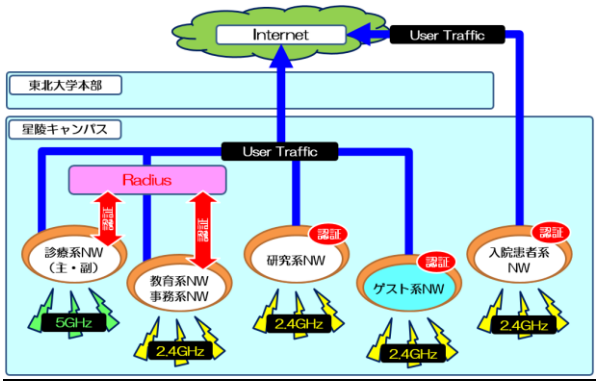

図２　無線環境の論理イメージ

表２　ネットワーク詳細

NW分類	周波数帯	認証	暗号化	利用規模	その他
診療系（主）	5G	802.1X／TLS	WPA+WPA2	大	SSIDステルス
診療系（副）	2.4G+5G	802.1X／PEAP	WPA+WPA2	小	SSIDステルス
入院患者系	2.4G	PSK、WEB認証	WPA+WPA2	小	入院患者のみ利用
教育系、事務系	2.4G	802.1X／PEAP	WPA2	大	学生の利用あり
研究系	2.4G	PSK	WPA+WPA2	小	SSIDステルス
ゲスト系	***2.4G***	***PSK***	***WPA2***	***小***	***電波は都度出力***

続いて、無線環境の論理イメージと各ネットワークの詳細を**図２**及び**表２**に示す。

全 25 種類の SSID を用途別に集約すると 5 つのネットワークに分類できる。その中には診療系ネットワーク、教育・事務系ネットワーク、研究系ネットワークなどがあり、周波数帯は診療系ネットワークが 5GHz 帯、その他のネットワークが共同で 2.4GHz 帯を利用する。認証方式は用途に合わせて IEEE802.1X 認証と PSK（事前共有キー）認証の両方を採用している。また、水色の網掛け部分は今回の更改対象となったゲスト系ネットワークである。

2.2　ゲスト無線の現状

現状のゲスト無線は、利用希望者からの申請があった際に、管理者が場所と期間を限定して既存の無線アクセスポイントにゲスト用 SSID を追加し、終了後は SSID を削除する運用である。また、ゲスト用 SSID は PSK による認証を採用し、パスフレーズは都度異なる内容で申請者のみに個別通知している。しかし PSK の場合は、ゲストユーザ全員が同じ接続設定（アカウントの使い回し）となるため、ユーザ個人の特定が困難である。このため何らかのセキュリティインシデントが発生した場合、誰がいつどこにアクセスしたかといったトレーサビリティを追跡できないため、何れは IEEE802.1X 認証や WEB 認証（キャプティブポータル）などによる認証機能の強化が必要であった。

また、星陵キャンパスの既存無線環境は、これまで段階的に導入や拡張を繰り返してきたため、運用中の無線アクセスポイントの機種やスペック、機器ベンダーが様々で、複数種類の無線コントローラが稼働している。その結果、同じ目的の設定を行う場合であっても、アクセスポイントに直接設定変更するもの、無線コントローラ経由で設定変更するもの、設定反映に再起動が必要なもの、不要なもの、というように無線アクセスポイントの機種ごとに手順が大きく異なっており、管理者は作業の度に機種ごとの手順と利用者への影響を正確に把握しながら作業する必要があった。このように、複数の管理者が何度も設定変更する運用は作業ミスを誘発する原因であり、ゲスト無線利用の度に設定変更を必要としない仕組みへ改善する必要があった。

前述した管理者側の課題を解決するとともに、利用者の利便性を向上するため、従来のゲスト無線の継続利用を廃止し、eduroam を利用した新たな無線環境を導入することにした。

3　eduroam を利用したゲスト無線の実装

3.1　eduroam の特徴

eduroam とは教育研究機関間の国際無線 LAN ローミング基盤であり、日本を含む世界 76 か国・地域で運用されている。eduroam では、自身の所属機関が発行したアカウントを使って、国内外の参加機関はどこに行っても同じ接続設定で無線の利用が可能である。

東北大学でも大学本部にて eduroam を利用するための基盤が整備されており、IEEE802.1X 認証と WPA2/AES による暗号化が実装され、セキュリティの高い安全な通信が可能である。また、認証時のレルムをもとに教職員用、学生用、他機関用でそれぞれ異なったネットワークを提供できるようになっており、具体的にはダイナミック VLAN を使って Radius アトリビュートにて受け取った VLAN ID を動的に割り当てる制御をしている。

3.2　既存環境への eduroam 導入の課題

現状の無線環境に eduroam を相乗りさせるための課題を整理した。

大学本部の eduroam に加わるためには、eduroam 用の Radius サーバ（キャンパス外に設置）による認証が必要である。そのため、既存の Radius サーバに加えて eduroam 用の Radius サーバを設定する必要があるため、Authenticator（無線アクセスポイント）では SSID ごとに複数の Radius サーバの設定が必要である。

また運用サポートの面では、ユーザ問合せや接続トラブルの調査に Radius サーバの認証ログが不可欠であるため、eduroam を利用する場合にも既存の Radius サーバと同様、集約されたログを保持する必要がある。

3.3　機能検証

eduroam の導入にあたり必要な技術的要件である**【ダイナミック VLAN】**と**【複数 Radius 指定】**について検証を行った。

今回は eduroam をキャンパス全域で展開することを目的としており、既存の全ての機種で要件を満たすかどうか確認し、仮に満たさない機種がある場合には代替案も含めた検討が必要である。

初めに、既存の無線アクセスポイントについて機器ベンダーでグループ分けを行い、計 4 種類（A 社-AP、B 社-AP、C 社-AP、D 社-AP）に分類した。そして 4 種類それぞれに対して、**【ダイナミック VLAN】**と**【複数 Radius 指定】**の検証を行った。その検証結果を**表 3** に示す。

表 3　技術的要件の機能検証

AP種類	設置台数	ダイナミックVLAN	複数Radius指定	適合
A社-AP	227	可能	可能	OK
B社-AP	32	不可	機器全体で1台まで	NG
C社-AP	596	可能	可能	OK
D社-AP	47	不可	周波数帯ごと1台まで	NG

この検証により、比較的導入時期が古い「B 社-AP」と「D 社-AP」の 2 種類は eduroam の要件を満たさないことが判明した。これらは設置エリアが限定的で、2 種類の合計台数も約 80 台しかなく、これは全無線アクセスポイント総数の 10%未満であった。残りの 90%には eduroam が展開できる見込みが立ったため、当初計画通りに進めることとし、「B 社-AP」と「D 社-AP」が集中して設置された建屋に対しては利用優先度が比較的高い場所（ユーザが集中する会議室や講義室等）のみ、予備として保有していた「A 社-AP」に置き換えることで展開不可能な状況を救済することにした。

3.4　実現した構成

前述した検討の結果、認証ログは大学本部管轄の Radius サーバを参照する運用ではなく、キャンパス内で管理するため、**図 3** に示す通り、Authenticator と大学本部管轄の Radius サーバの間に Radius プロキシを設置した。

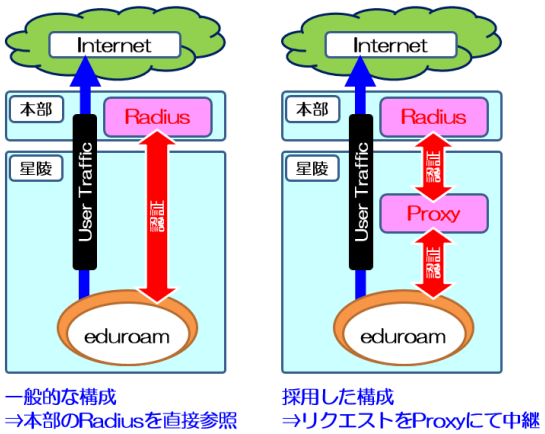

図 3　Radius プロキシによる認証

Authenticator が参照する Radius サーバは Radius プロキシにして、Radius プロキシへの認証リクエストは大学本部管轄の Radius サーバへ転送する構成とした。

Radius プロキシは既存の仮想基盤上に CentOS と FreeRADIUS で構築し、冗長化と負荷分散を考慮して 2 サーバ構成で実装した。構成は以下の**図４**であり、破線に囲まれた箇所が今回の更改対象である。

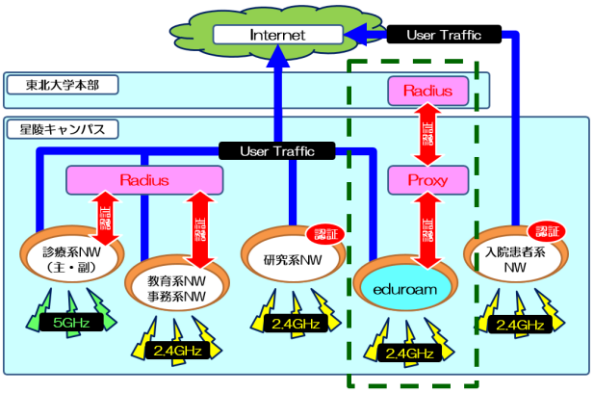

図４　無線環境の最終構成イメージ

認証元の Authenticator の IP アドレスや Supplicant（無線端末）の Mac アドレスといった認証に関連する情報が、Radius プロキシから適切に中継されることを確認した。これにより、セキュリティインシデントが起きた際に、大学本部管轄の Radius サーバと Radius プロキシの両方で証跡を確認することが可能になった。

4　切り替えと運用

4.1　切り替え

先述の通り、星陵キャンパスの無線環境は大学病院の診療業務でも利用しているため、原則 24 時間 365 日の可用性が必要である。またネットワークの停止や遅延、通信の不安定といった何らかの作業に伴う運用影響が生じる場合は、予め影響範囲と影響時間を正確に把握し、事前に関係者に通知してスケジュールの合意、許可を受ける、といったルールである。

今回の eduroam への切り替えも運用影響が予想されたが、”影響範囲と時間を正確に把握”という点で問題があった。従来は、実装時点で全ての機器で切り替えの事前シミュレーションを行って詳細な運用影響を把握してきたが、今回は一部の機器で本番環境以外に検証機が無く、事前シミュレーションの実施が困難であった。

そこで対策を検討し、今後の運用も見据えた検証機の必要性を鑑みて、本番環境の構成を見直すことにした。具体的には本番環境で稼働中の機器の１つを本番環境から切り離し、検証機として利用することにした。検証機が確保できたことで全ての機器で切り替えの事前シミュレーションが可能になった。そして詳細な切り替えスケジュールを策定後、関係者の許可を受領、無事に eduroam への切り替えが完了した。

4.2　運用

今回整備したゲスト無線により学会やセミナーの開催時に管理者の負担が無くなり、来訪者にも快適なゲスト無線を提供することができるようになった。また、eduroam アカウントで接続者の身元（所属機関）が把握できるため、安心してゲスト無線を提供できるようになった。さらに一時的なゲストアカウントを本部で発行することができるため、eduroam アカウントを持たない来訪者やシステムの保守ベンダーもゲスト無線を利用することができるようになり、利便性が向上した。

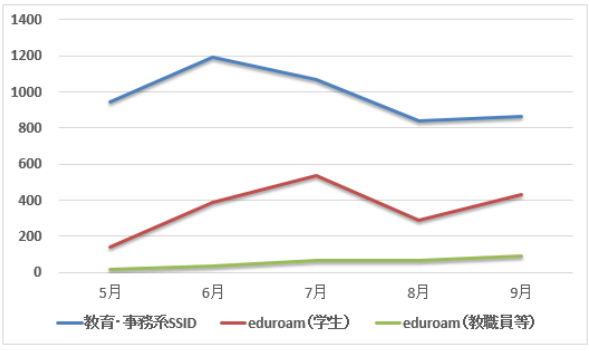

図５　無線利用アカウント数（1 日平均）

直近 5 ヶ月の 1 日平均の無線利用アカウント数の推移を**図５**に示す。グラフの青は既存の教育・事務系の SSID、赤は eduroam の学生アカウント、緑は eduroam の教職員アカウントを表している。

これによると 5 月と 8 月、9 月は連休が多いため利用数自体が比較的少ないが、全体の傾向としては従来から提供していた教育・事務系 SSID の利用が徐々に減少し、eduroam の学生アカウントによる利用が大きく増加している。これは多くの学生が他のキャンパスでも利用可能な eduroam にシフトしたもの、と考えられる。

このように eduroam は多くのユーザに支持され、キャンパスの運用に不可欠なネットワークとして定着した。

5 まとめ

本稿では eduroam の導入について、計画から運用までの一連の取り組みについて述べた。今後は eduroam の大学内における利用シーンを探して、利用者の拡大に努めていきたい。

星陵キャンパスでは多数の無線アクセスポイントが設置されているため、持ち込みルータやスマートデバイスのテザリング機能によって 2.4GHz 帯のチャネルの干渉によるスループットの低下が時々発生している。そこで、2.4GHz 帯から 5GHz 帯の W56(計 11 チャネル)に移行または分散させることで電波状況の改善を検討中である。

参考文献

[1] 「eduroam JP」、http://www.eduroam.jp/
[2] 「東北大学総合情報ネットワークシステム TAINS － eduroam アカウントサービス」、http://www.tains.tohoku.ac.jp/kyousyokuin/eduroam.html