学術無線 LAN ローミング基盤 eduroam における IoT デバイス・周辺機器の接続手法の調査検討

原田 寛之 [1)], 後藤 英昭 [2)], 漆谷 重雄 [3)]

1) 札幌学院大学 情報処理課
2) 東北大学 サイバーサイエンスセンター
3) 国立情報学研究所

se-harada@e.sgu.ac.jp

Survey and investigation of connection methods for IoT devices and peripherals in eduroam, an academic wireless LAN roaming infrastructure

Hiroyuki Harada [1)], Hideaki Goto[2)], Shigeo Urushidani[3)]

1) Information Processing Division, Sapporo Gakuin University
2) Cyberscience Center, Tohoku University
3) National Institute of Informatics

概要

キャンパス無線 LAN 環境においては，WPA2 Enterprise を使用する方式が多く使われており，認証基盤を相互接続して利用者がキャンパス無線 LAN をローミング利用できる eduroam への加入機関も年々増加の傾向にある．一方，WPA2 Enterprise を利用できないクライアントへの対応のため，WPA2 Personal とキャプティブポータルによる Web 認証を用いた独自 SSID によるキャンパス無線 LAN 環境を並行運用している機関も少なくない．WPA2 Personal によるサービス提供については安全性の懸念点があることに加え，2022 年現在においては利用者の PC やスマートフォンについてはほぼ全てが WPA2 Enterprise に対応していることから，札幌学院大学ではキャンパス無線 LAN を eduroam および市民向けの Cityroam のみの運用とし，WPA2 Personal による独自 SSID の廃止に踏み切った．しかしながら，キャンパス内には IoT デバイスや周辺機器などをキャンパス無線 LAN に接続したいというニーズが一定数存在する．本研究では，このような機器を eduroam にローミング接続されたキャンパス無線 LAN に接続するにあたり，ネットワークポリシーやアカウント管理における課題を明らかにすると共に，クライアント側に必要となる WPA2 Enterprise 実装状況を調査した．また加えて個人所有の機器以外で eduroam に接続されているキャンパス無線 LAN への接続を実現した事例を挙げる．

1 はじめに

学術無線 LAN ローミング基盤 eduroam[1]は，国内 348 機関（2022 年 8 月現在），世界 106 か国（地域）が参加する基盤へと成長し，参加機関の構成員は相互にキャンパス無線 LAN を利用可能な仕組みが広く運用されている．クライアントが eduroam に接続する際に用いられるのは WPA2 Enterprise（IEEE 802.1X）である．キャプティブポータル認証（Web 認証）については，国立情報学研究所 eduroam JP サービス技術基準・運用基準[2]において安全性の問題から明示的に禁止されている．eduroam JP が 2006 年にサービス開始してから 2017 年頃までの間は，利用者が持ち込む一部のメーカーのスマートフォンの独自実装によって，WPA2 Enterprise による無線 LAN 接続設定に特別な手順が必要であるなどの問題があり，キャンパス無線 LAN においても独自 SSID にて WPA2 Personal（事前共有キー）によるキャプティブポータル認証方式を併設している例が見られた．しかしながら 2022 年現在では利用者が持ち込む PC やスマートフォンのうち OS ベンダーによるサポートが継続しているものはほぼ全てが WPA2 Enterprise に標準的な手法で接続できるようになっており，持ち込み端末のためのサービス提供の観点からは独自 SSID による WPA2

Personal の接続サービスは廃止できる状況にある．

一方，キャンパス内には WPA2 Enterprise に対応していない IoT デバイスや周辺機器などで，キャンパス無線 LAN に接続したいというニーズが存在する．これらは，大学が全体のサービス提供のために設置するものと，利用者が自己の利用のために持ち込むものに分けられるが，キャンパス無線 LAN の安全性の確保の面からは，WPA2 Personal やキャプティブポータルといった安全性に問題があるサービス提供を永続的に続けていくことは避けるべきである．

本稿では，第 2 章で実際に WPA2 Personal による独自 SSID の廃止に踏み切った札幌学院大学のキャンパス無線 LAN の構成と運用について述べる．第 3 章では，キャンパス内の IoT デバイスや周辺機器のキャンパス無線 LAN 接続にあたり検討すべき課題を明らかにし，実際の各機器の WPA2 Enterprise 対応状況や，個人所有の機器以外で eduroam に接続されているキャンパス無線 LAN への接続を実現した事例について述べる．第 4 章は本稿のまとめである．

2　札幌学院大学のキャンパス無線 LAN の構成と運用

2.1 札幌学院大学におけるキャンパス無線 LAN の構成

札幌学院大学では 2011 年にキャンパス内に導入学部の違いなどから複数存在していた無線 LAN を統合すると共に，利用可能エリアをキャンパス内全域に拡張し，学生及び教職員がキャンパス内でどこでも無線 LAN 接続にできる環境を整備した．更に 2012 年に eduroam に参加し，本学構成員のみならず eduroam アカウントを持つ学外者がキャンパス無線 LAN の全てのアクセスポイントを利用できる環境を整備した．また本学では図書館やホール，産学連携拠点といった設備を市民が利用することが想定されており，キャンパス無線 LAN の市民への開放に対応するため，セキュア公衆無線 LAN ローミング研究会 [3] が 2017 年に次世代ホットスポット（NGH）基盤として整備した Cityroam [4] に 2018 年より接続し，市民へのキャンパス無線 LAN 開放を行っている．

2021 年度までは WPA2 Enterprise に対応していないデバイスの接続のため，接続方式を WPA2 Personal としキャプティブポータル認証や MAC アドレスの事前登録を経て利用できる独自の SSID と，WPA2 Enterprise による独自の SSID も併用してサービス提供してきた．しかし，利用者の持込クライアントについてはほぼ WPA2 Enterprise に対応した状況にあることに加え，インターネット上の Web サイトの常時 SSL 化が進み利用者が接続時にトラブルを抱えやすくなったこと，WPA2 Personal では偽基地局の判別が行なえず安全性に問題があるといった懸念点を排除するため，従来の独自 SSID の廃止に踏み切った．現在，運用中のキャンパス無線 LAN 環境は eduroam/Cityroam のみとなっている．

2.2 独自 SSID の廃止に至る経緯

無線 LAN 環境においては，アクセスポイントが SSID ごとに一定時間毎にビーコンを送信している．クライアントはプローブリクエストを周辺に向け一斉に送信し，これを受けたアクセスポイントは SSID ごとにプローブレスポンスをクライアントに応答している．このような仕組みにより，キャンパス内で多数の SSID を運用している環境下においては，ビーコンやプローブのような管理制御用の通信でチャンネルが占有されてしまう．これは，利用できるチャンネル数が少ない 2.4GHz 帯の無線 LAN 環境において顕著である．このような観点から，大学キャンパスのように限られた空間に多数のアクセスポイントを高密度で設置する場合，発信する SSID はなるべく少なくすることが望ましい．本学キャンパスにおいては，各アクセスポイントが eduroam/Cityroam の SSID に加え，独自の SSID2 つの計 4 つの SSID を送出し

ている状況であった． 2021 年 4 月に新たに開設した本学新札幌キャンパスにおいては，6 階建ての建屋 1 つに無線 LAN コントローラで管理されるアクセスポイントを 205 基設置しており，ビーコンやプローブによるチャンネルの占有を抑えることが利用者のキャンパス無線 LAN へのつながりやすさに寄与すると考えられた．

また本学の構成員は，本学キャンパスでは独自の SSID に接続し，他機関訪問時にのみ eduroam に接続する利用形態を取るものが多かったが，他機関訪問時に初めて eduroam への接続トラブル（ID やパスワードの誤りなど）に気づくケースがあり，他機関での無線 LAN のスムーズな利用の面で課題があった．これは，自機関においても eduroam を常用することで未然に抑制することが可能であるため，本学キャンパス内で本学構成員が利用するキャンパス無線 LAN を eduroam とする方針とした．

この実現のためには， eduroam を利用する学外者用のネットワークと，本学構成員が利用するネットワークを分離する必要がある．具体的には，学内限定公開しているサーバ等へのアクセス制限の必要性の他に，図書館で契約している電子ジャーナルは契約の関係上ゲスト利用が許可されていないためである．このため，キャンパス無線 LAN において認証 VLAN の仕組みを構築し，自機関のレルムによる認証は学内者向け VLAN に，自機関以外のレルムによる認証はゲスト用 VLAN にクライアントを収容する構成とした．ゲスト用 VLAN の上流には，国立情報学研究所が提供している eduroam アクセスネットワーク収容サービスを利用することで，ゲストがインターネットにアクセスする際の接続元 IP アドレスについても学内者のものとは別になっている（図 1）．

また，自キャンパス内の eduroam においては，本学で発行したアカウントについてはレルムを付与して設定するよう案内していたものの，実際にはレルム無しでの認証も可能としていた．利用者にとっての接続トラブルを減らすことを目的としていたが，レルム無しの設定では他機関訪問時には接続できない問題があった．これについては学内に周知広報したうえで，RADIUS Proxy 側でレルム無しの認証要求については拒絶するよう設定を変更した．

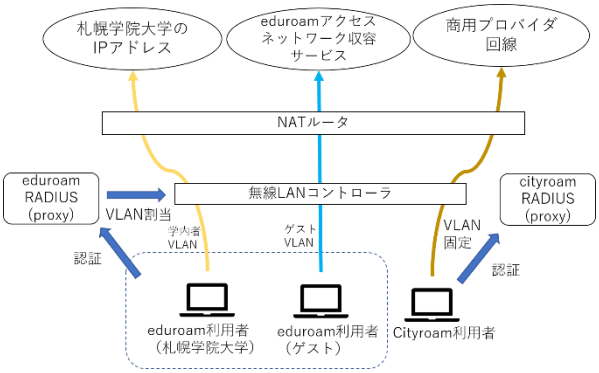

図 1 札幌学院大学におけるキャンパス無線 LAN の VLAN とアクセスネットワーク．

このような経緯を経て 2022 年度に独自 SSID を廃止し，本学の構成員が本学キャンパスで利用するキャンパス無線 LAN は eduroam に統一した．

これにより，本学構成員は学内・他機関訪問時を問わず常時 eduroam を使用することとなり，学会等で他機関を訪れた際に eduroam が利用できなかったとの相談（多くは当日に解決できず事後に相談に来られる状況であった）は減少した．また学生の留学先など本学のスタッフのサポートが受けられない環境においても，本学が発行した eduroam アカウントの利用が増加している（外部から本学への認証要求件数による）．

2.3 独自 SSID の廃止で生じた課題

独自 SSID においては，利用者の持込クライアントだけではなく，プロジェクター等の周辺機器など，WPA2 Enterprise に対応していない機器が一部収容されていた．独自 SSID の廃止に伴い，現状これらの機器については学内 LAN から切断し，それぞれの機器に対してアドホックでクライアントが接続して利用する方式としている．しかしながら例えばプロジェクターにおいては，クライアントから投影しながら学内 LAN に接続したいといったニーズには対応することができない．この解決

のためには，プロジェクター等の周辺機器をeduroamによるキャンパス無線LANに収容することが必要となる．このような機器の接続にあたってどのような点に留意すべきか，現状を調査して整理し実現可能性を検討することとした．

3 eduroam へのキャンパス内 IoT デバイスや周辺機器の接続

3.1 前提条件と検討すべき課題

IoTデバイスや周辺機器がeduroamに接続するためには，まず機器側がWPA2 Enterpriseによる接続をサポートしている必要がある．機器自身がこれをサポートしていない場合は，何らかの中継装置を用いて eduroam と機器を相互接続することも考えられるが，この場合は当該機器の利用にあたりどのようなネットワークにおける接続性（リーチャビリティ）が必要なのかも合わせて検討する必要がある．例えば，測定値をクラウドに送信するセンサーのようなIoTデバイスは単にインターネットへのアクセスがあればよいが，プロジェクターやプリンターのように利用者の持込クライアントと双方向に通信して動作するものは，当該機器が学内 LAN 側から検出できることや，学内 LAN 上の他のクライアントとの相互通信が必要となる．札幌学院大学においては，キャンパス無線 LAN クライアント間の通信については無線 LAN コントローラ側で遮断するクライアントアイソレーションの構成にて運用しているため，このような機器の運用についてはネットワークのポリシーに手を加える必要がある．

また，IoT デバイスや周辺機器は不特定多数がキャンパス施設内に無人で設置されることがあるため，機器の盗難や設定情報へのアクセスにより認証情報が漏洩することは避けなくてはならない．設定情報へのアクセスは管理者パスワード等で防止できる機器もあるが，平文で EAP-TTLS の認証情報を格納するような 機器については注意しなければならない．

さらに，eduroam JP サービス運用基準においては，eduroam IdPにおけるアカウント管理として“全てのアカウントは，当該の機関が管理する有効な利用者情報に基づかなければならない”と規定されている．このため， IoTデバイスや周辺機器などを大学側がキャンパス無線 LAN に接続するにあたっては，接続に用いるアカウントはeduroamアカウントではなく，あくまで自機関のキャンパス無線LANにWPA2 Enterpriseで接続するためのアカウントとして発行する必要がある．本学においては，仮に当該機器が他機関に持ち出されたとしても他機関のキャンパス無線 LAN を eduroam クライアントとして利用することがないよう，認証情報のレルム等を自機関でのみ有効なものとしている．

3.2 2022 年現在の周辺機器等のサポート状況

そこでまず，キャンパス内で主に利用されているネットワーク接続が必要な周辺機器を洗い出し，そのWPA2 Enterpriseによる無線LAN接続のサポート状況を確認することとした．

3.2.1 プロジェクター（セットトップボックス）

キャンパス内に設置されているプロジェクターの一部には，セットトップボックス（STB）と呼ばれる持込クライアントからの入力映像や，各種ストリーミングサービス等の受信映像をプロジェクターに投影できるものがある．代表的なSTBとしては，Appleの Apple TV，Googleの ChromeCast, Amazonの Amazon Fire TV，また汎用的な機器として内田洋行の Wivia [5]がよく利用されている．Apple TVは管理者がプロファイルを適用することで WPA2 Enterpriseによる無線LANに接続可能である．一方，ChromeCast や Amazon Fire TV は WPA2 Enterpriseに対応していない．Wiviaについても従来対応していなかったが，最新のWivia R+（2021年12月～）については標準でWPA2 Enterprise (PEAP/MSCHAPV2 または EAP-TTLS/MSCHAPv2)に対応している．但し，キャンパス無線 LAN 上で PC 等と Wivia が相

互通信することとなるため，無線 LAN クライアント間の通信を遮断するポリシーで運用している場合は注意が必要となる．Wivia については有線 LAN も搭載されているため，本学では有線 LAN で学内 LAN に接続することを原則としている．

3.2.2 プリンター

キャンパス内には，利用者が共同で利用できるプリンターが設置されており，現状は全て有線 LAN による．しかしながら教員からはまれに研究室内での無線 LAN によるプリンター接続について相談があることから，合わせて調査した．2022 年 8 月の大学生協カタログに掲載されているプリンターメーカーは，ブラザー，エプソン，NEC，OKI，キャノン，リコーであった．各社共に WPA2 Enterprise による無線 LAN 接続に対応している機種が販売されている．ただし安価な機種においては WPA2 Enterprise 非対応のものが多いため注意が必要である．また，プロジェクターと同様に無線 LAN クライアント間の通信となるため，現在の本学のネットワークポリシーでは利用に問題が生じる．

3.2.3 サイネージ

キャンパス内には，複数個所に従来の掲示板を置き換える目的でサイネージが設置されている．学内 LAN とは接続されておらずローカルで運用されているものあるが，一部はコンテンツ配信サーバがクラウド上にあり，コンテンツ更新のためにインターネットへのアクセスが必要である．本学で運用中のサイネージについては，全て制御部に Windows が使用されており，WPA2 Enterprise によるキャンパス無線 LAN への接続は容易である． 但し，EAP-TLS による接続については，設置個所によっては証明書の定期的な更新作業の負荷に注意する必要がある．また，コンテンツの更新のために学内 LAN 上の他のクライアントと相互通信が必要な場合は，ネットワークポリシーにより利用できないため，サイネージ導入担当部署と事前にコンテンツ更新方法について調整しておくことが重要となる．

3.2.4 サーマルカメラ・防犯カメラ

コロナ禍の対策の１つとして，キャンパス建屋の入館時に検温を行うサーマルカメラが設置されている．本学ではスリーアールソリューションの 3R-TMC03 を採用しているが，利用者への検温と音声による注意喚起のみの運用で設置している．当該機器は有線/無線のネットワークインターフェースを搭載していない．また，導入時に他に提案があった機器として HIKVISION の製品があるが，こちらは有線 LAN インターフェースを有している．サーマルカメラにおいて無線 LAN 接続が必要なものは確認できなかった．

キャンパス各所に設置している防犯カメラについては，学内 LAN に接続せずローカルで運用しているものと，学内 LAN に接続しレコーダー等に映像送信しているものがある．いずれも設置にあたっては施設に工事を伴って設置することがほとんどであり，今後もあまり無線 LAN への接続のニーズは本学ではないと考えられる．

一方で，研究室等では小型の Wi-Fi 接続できるカメラを研究等の目的で設置することがある．アトムテックの ATOM Cam 2 は非常に安価でありよく利用されているが，実装されている無線 LAN への接続方式は WPA2 Personal に留まっている．

3.2.5 施設設備管理系

キャンパス内の空調機器等，施設設備管理装置等の一部には，ネットワーク接続により集中管理を行っているものがある．本学においては学内 LAN に専用の VLAN を設定し，全て有線 LAN での接続を行っているため，無線 LAN 接続の要望はいまのところない．また機械室等はキャンパス無線 LAN のエリア外であることが多く，そのような点からも有線 LAN での接続が多いものと考えられる．

また一部の部屋の入退室・施錠解錠に IC カードリーダーを使用している．これは現状，キ

ャンパス内に物理的に独立した LAN を構築しており，キャンパス LAN とは接続されていない．

3.2.6 その他の IoT デバイス

本学では設置事例がないが，IoT 機器においては内部に Wi-Fi を内蔵するマイクロコントローラがよく利用されている．特に，ESP32 チップ[6]は低コスト，低消費電力であり，これを搭載する ESP32 モジュールは多く利用されている．これを利用して小山高専学内無線 LAN の WPA2 Enterprise への接続が可能な IoT デバイスの試作が行われている[7]．認証情報は Arduino IDE のスケッチファイルに平文で記述する実装[8]を元にしているため，EEPROM の吸い出しによる認証情報の漏洩等に注意する必要がある．

また ESP32 においては，WPA2 Personal であればスマートフォンからアプリ経由で設定が行える ESP-TOUCH プロトコル[9]と SDK が提供されている．この仕組みを利用するなどして，将来的には ESP32 を利用する組み込み機器のようなヘッドレスデバイスにおいても，WPA2 Enterprise による接続時のアカウントの登録や確実な失効を行う手法の開発に繋げられる可能性がある．

3.3 個人所有の機器以外で，eduroam への接続を実現した例

2021 年度に開設した新札幌キャンパスでは，学生が学生証を用いて無人の貸出ロッカー（図 2）より自動で貸出を受けられるノート PC を 80 台配置した．貸出 PC は貸出ロッカーへの格納中に充電とディスクイメージ配信サーバからのイメージ受信・復元を兼ねて USB Type-C ケーブルで有線 LAN により学内 LAN に接続されている．学生により貸出手続きが行われると貸出ロッカーの 1 つが自動で開錠され利用可能な状態となり，貸出 PC は USB Type-C ケーブルの抜去以降は全てキャンパス無線 LAN に接続された状態で動作する．

図 2　PC 自動貸出ロッカー

貸出 PC は全て学内の Active Directory にコンピュータとして登録されており，学生は貸出 PC 起動後に自分の Active Directory アカウントにてログインして利用を開始する．この際，AD アカウントでの認証にはネットワーク接続が必要であることから，貸出 PC はログイン前の時点でキャンパス無線 LAN に接続されている必要がある．これは，Active Directory のグループポリシーにおいて、ユーザーログオン前にコンピュータの認証としてワイヤレスネットワーク接続を行うよう設定することで実現している（図 3）．当該ポリシーにより，ユーザーがログインする際に AD アカウントによるキャンパス無線 LAN への認証が再度行われる．

コンピュータの構成/ポリシー/Windowsの設定 セキュリティの設定/ワイヤレスネットワーク IEEE 802.1 ポリシー	
ネットワーク名（SSID）	eduroam
このネットワークが接続範囲内に入ると自動的に接続する	有効
セキュリティメソッド	WPA2-エンタープライズ・AES-CCMP
ネットワークの認証方法	Microsoft: 保護されたEAP（PEAP）
認証モード	ユーザまたはコンピュータの認証
シングルサインオン	このネットワークに対するシングルサインオンを有効にする（ユーザーログオンの直前に実行する）

図 3　貸出 PC に適用したグループポリシー

この一連の動作において WPA2 Enterprise の PEAP 認証に用いられるユーザー名は下記の通りとなる．

１）起動直後（コンピュータの認証）

host/コンピュータの FQDN 名

２）ユーザーのログイン時（ユーザの認証）

AD ドメイン名¥ユーザー名

キャンパス内の無線 LAN アクセスポイントからの認証要求を処理する RADIUS Proxy においては、通常想定されている eduroam アカウント以外の上記の認証要求についても，自機関の上位サーバに転送するようルールを記述している．具体的には、FreeRADIUS で構築した RADIUS Proxy の sites-available/default において，Stripped-User-Name が上記１）または２）に合致する場合は自機関の上位サーバに転送するようにしている．

いずれも，eduroam JP ではルーティングされないレルムであり，また Active Directory は学外からは直接参照できないため，本学キャンパス内での利用に限定される，という仕組みを実現している．

4 まとめ

本稿では，札幌学院大学における WPA2 Enterprise による eduroam/Cityroam でのキャンパス無線 LAN 統合と WPA2 Personal による独自 SSID の廃止により生じた IoT デバイス・周辺機器のキャンパス無線 LAN への接続における課題について調査した．また，通常の個人の持込端末と異なり，不特定多数の学生が貸出利用する貸出 PC においても, 利用者を紐づけてキャンパス無線 LAN 配下で運用できることを示した．今後，さらに無人で運用される人が介在しない機器の接続についても検討を進めていきたい. 本研究の一部は，令和 4 年度国立情報学研究所公募型共同研究の助成を受けた.

参考文献

[1] eduroam JP: https://www.eduroam.jp/
(2022 年 9 月 28 日参照)

[2] 国立情報学研究所，“国立情報学研究所 eduroam JP サービス技術基準・運用基準.”: https://www.eduroam.jp/document/81/
（2022 年 10 月 11 日参照）

[3] セキュア公衆無線 LAN ローミング研究会（NGHSIG）: https://nghsig.jp/
（2022 年 9 月 28 日参照）

[4] Cityroam: https://cityroam.jp/
（2022 年 9 月 28 日参照）

[5] 株式会社内田洋行，ワイヤレス画面転送装置 Wivia[ワイビア] : https://www.uchida.co.jp/wivia/
（2022 年 9 月 28 日参照）

[6] Espressif Systems, ESP32.: https://www.espressif.com/en/products/socs/esp32/
（2022 年 10 月 11 日参照）

[7] 加藤康弘, “ESP32 モジュールの開発環境構築と IoT 機器の試作.”，第 24 回高専シンポジウム 講演要旨集 PI-33: https://www.oyama-ct.ac.jp/24sympo_bk/contents/24sympo-youshi.html
（2022 年 10 月 11 日参照）

[8] JeroenBeemster/ESP32-WPA2-Enterprise: https://github.com/JeroenBeemster/ESP32-WPA2-enterprise/
（2022 年 10 月 11 日参照）

[9] Espressif Systems, ESP-Touch Overview: https://www.espressif.com/en/products/software/esp-touch/overview/
（2022 年 10 月 16 日参照）