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 札幌学院大学
後藤英昭 東北大学
漆谷重雄 国立情報学研究所

大学ICT推進協議会
2022年度年次大会
(2022年12月3日)

One life, Many answers

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

札幌学院大学のキャンパス無線 LANの構成と運用

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

- 文系総合大学
- 学生数　およそ 3200名

2011年　キャンパス全域にWi-Fi
2012年　eduroam参加
2018年　Cityroam参加
2022年　独自SSID廃止

現在：WPA2 Enterprise のみ提供
（eduroamとCityroam）

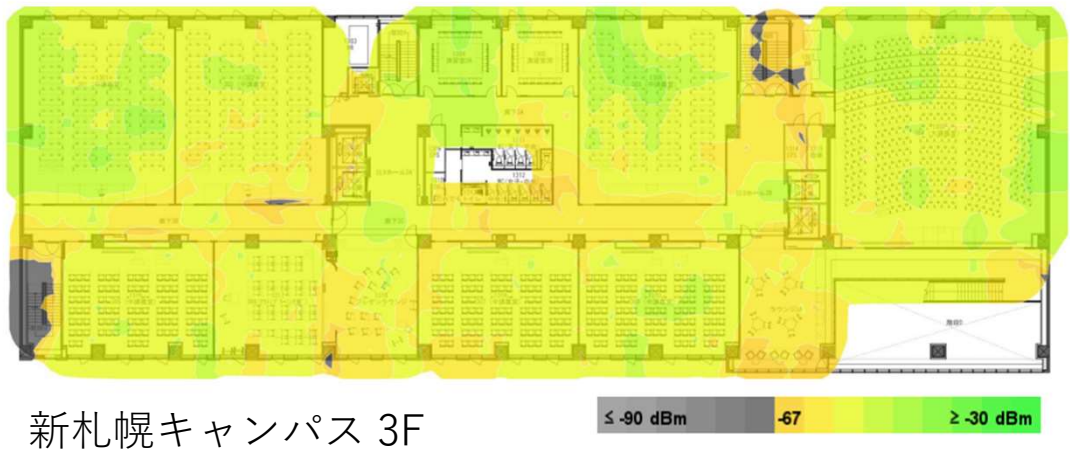
独自SSIDの廃止に至る経緯(1) SSIDを減らしたい

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

札幌学院大学新札幌キャンパス
- 6階建ての建屋
- APを高密度に配置（204基）

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

→　SSIDは少ない方がよい



新札幌キャンパス 3F

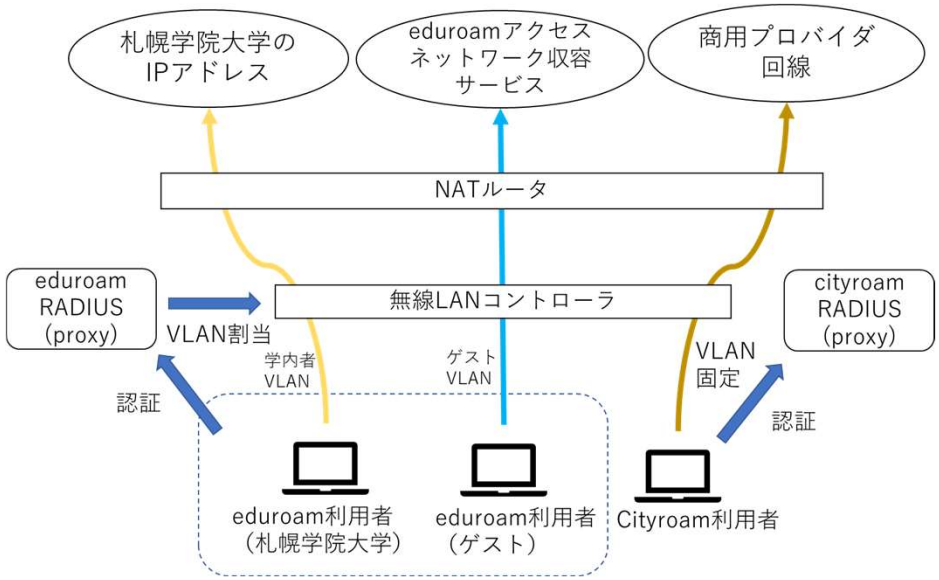
独自SSIDの廃止に向けて - 認証VLANの導入

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

- 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
- 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不許可

<u>認証 VLAN</u>

- 自機関のレルムによる認証
  →学内者向け VLAN
- 自機関以外のレルムによる認証
  →ゲスト用VLAN



独自SSIDの廃止に至る経緯(2) eduroamの常用

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

2021年度まで

- 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

  → 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る

  → 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

2022年度から

- 独自SSIDを廃止し，eduroamとCityroamのみに統合

eduroam へのキャンパス内 IoT デバイスや周辺機器の接続

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

キャンパス無線LANがeduroam（WPA2 Enterprise）のみとなった

- これまでWPA2 Personalで接続していた機器の扱い

→　各部局と調整のうえ，WPA2 Enterpriseに対応しないものは遮断

→　キャンパス内にあるIoTデバイスや周辺機器をリストアップして調査し，WPA2 Enterpriseに対応する後継機種があれば更新

- 無人で設置される人が介在しない機器の実装状況を調査

プロジェクター（セットトップボックス）

持込クライアントからの入力映像などをプロジェクターに投影

- Apple ： Apple TV　（プロファイル適用で可能）
- Google：ChromeCast（接続不可）
- Amazon ： Amazon Fire TV（接続不可）
- 内田洋行：Wivia R+（**PEAP/MSCHAPV2** または **EAP-TTLS/MSCHAPv2**に対応）

Wivia R+

キャンパス無線 LAN 上で PC 等と STBが相互通信する
→　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

プリンター

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

- 札幌学院大学においては，現状すべて有線LANでの接続
- 教員からはまれに研究室内の無線LANによるプリンター接続について相談がある

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

- ブラザー，エプソン，NEC，OKI，キャノン，リコー

→　各社ともにWPA2 Enterpriseによる無線LAN接続に対応しているモデルが販売されている（ただし，安価な機種は非対応が多い）

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，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

サイネージ

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

- 札幌学院大学で運用中のものは，すべて制御部はWindows
- WPA2 Enterpriseによるキャンパス無線LANへの接続は容易
- EAP-TLSによる接続を行う場合は，定期的に証明書の更新作業が発生する
  （埋込設置などの場合はメンテ方法を確保しておく）
- コンテンツ更新に他のクライアントの相互通信が必要かどうか，設置部局と事前調整

サーマルカメラ・防犯カメラ

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

キャンパス建屋の入館時に検温を行うサーマルカメラ

- 札幌学院大学で運用中のモデルは，ネットワーク接続を行っていない（ネットワークインターフェース非搭載）
- 他メーカー機器で有線LANインターフェースを有するモデルはあるが，無線LAN接続が必要な機種は確認できなかった

防犯カメラ

- 施設工事を伴って設置することがほとんど
  → あまり無線LAN接続のニーズはない

研究目的のカメラ

- 実装されているのはほぼWPA2 Personalにとどまる
- どちらにせよ電源は必要なので，有線LAN(PoE)接続の機種の調達がおすすめ

施設設備管理系

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

空調管理系

- 札幌学院大学においては，学内LANに専用のVLANを設定し，すべて有線LANで接続
- 機械室などはキャンパス無線LANのエリア外であることも多く，無線LAN接続のニーズはない

入退室・施錠開錠

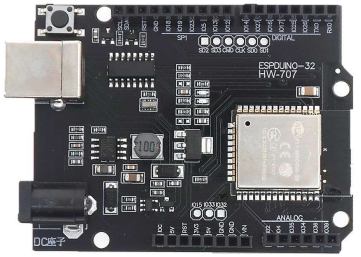
- キャンパス内に物理的に独立した有線LANが構築されている

その他のIoTデバイス

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

Wi-Fiチップを内蔵するマイクロコントローラ（ESP32など）

- 認証情報をArduino IDE のスケッチファイルに平文で記述する実装例はある
  （EEPROM の吸い出しによる認証情報の漏洩等に注意）
- 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 プロトコルと SDK が提供されている



ESP32デバイスの例

→　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

個人所有の機器以外で キャンパス無線LAN への接続を実現した例

PC自動貸出ロッカー（CO-OnSen）の基本動作

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

札幌学院大学における動作

- PC は貸出ロッカーへの格納中は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（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・復元を兼ねる）.
- 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.
- 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.

Active Directory の貸出PCのグループポリシー

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

PC起動後はコンピュータの認証としてキャンパス無線 LANに接続
ユーザーがログインする際に AD アカウントにより再認証

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IEEE802.1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）

貸出PCによるキャンパス無線LANへの接続

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

そのままではルーティングできないので，FreeRADIUS上でRealmによる経路を上書きする（sites-available/default）

```
if (&Stripped-User-Name =~ /^host¥/.*¥.xxx¥.sgu¥.ac¥.jp/){
        update {    &control:Proxy-To-Realm := ‘sgu_ad_flr’    }
        return
}
if (&Stripped-User-Name =~ /^AD-Domain¥¥.*/){
        update {    &control:Proxy-To-Realm := 'sgu_ad_flr‘    }
        return
}
```

貸出PCの起動時のログ（ログイン待ちの状態）

2022-12-10 18:06:23 Login OK: [host/XXXX.xxx.sgu.ac.jp] (from client X port 0 cli xx-xx-xx-xx-52-80)

学生による貸出PCへのログイン時のログ

2022-12-10 18:08:53 Login OK: [AD-Domain¥StudentID] (from client X port 0 cli xx-xx-xx-xx-52-80)

学外では他のeduroam加入機関を含めて利用不可

まとめ

札幌学院大学
SAPPORO GAKUIN UNIVERSITY

- キャンパス無線LANをWPA2 Enterpriseのみにしても，大きな混乱なく運用することができている.
- 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WPA2 Enterpriseのキャンパス無線LAN 配下で運用できることを示した.
- 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.

