eduroamをもっと使いやすくする技術と運用
(eduroam Techincal & Operation Guide)

後藤英昭（東北大学/国立情報学研究所）

2018年6月21日　NII学術情報基盤オープンフォーラム

内容

- eduroam構築・運用・利用上の悩み
  - 利用者視点
  - 管理者視点
- 無線LANシステムの一本化のススメ
  - 利用者の混乱が減少！
  - とにかく運用・管理が楽！
  - 利用者ごとに異なるポリシー適用も容易！
- トラブルの傾向と対策
  - ありがちな設定ミス
  - 不適切なシステム設計・構築

eduroam利用上の悩み（利用者視点）

- 複数ある無線LANシステムの使い分けが面倒
  - なぜ複数あるのか？
- （なぜか）学内ではeduroamを使わないように言われる
  - ポリシーが違う？　混雑するから？
- 学外で便利なのに、（なぜか）eduroamが学内であまり知られていない
  - 広報不足

eduroam利用上の悩み（続）

- 他のSSIDと接続が勝手に切り替わってしまう
  - 手動で切り替えても、接続を維持できない
  - 端末で優先度が設定できない
- eduroamに接続されると、学内サービスや電子ジャーナルにアクセスできない
  - 利用者には理由が分かりにくい
- 利用者が増えるとすぐ遅くなる　　……等々

eduroamの問題ではなく、運用上の都合では？

eduroam構築・運用上の悩み（管理者視点）

- 複数の無線LANシステムの構築・運用が面倒
  - なぜ複数あるのか？
- 訪問者向けなので、構成員にeduroamは使わせたくない
  - eduroamが互恵システムなので仕方なく基地局を提供している？
  - 「eduroamは訪問者向け」という誤解
- 構成員には学内専用システムのポリシーを適用したいのに、eduroam側を使われてしまう

eduroam構築・運用上の悩み（続）

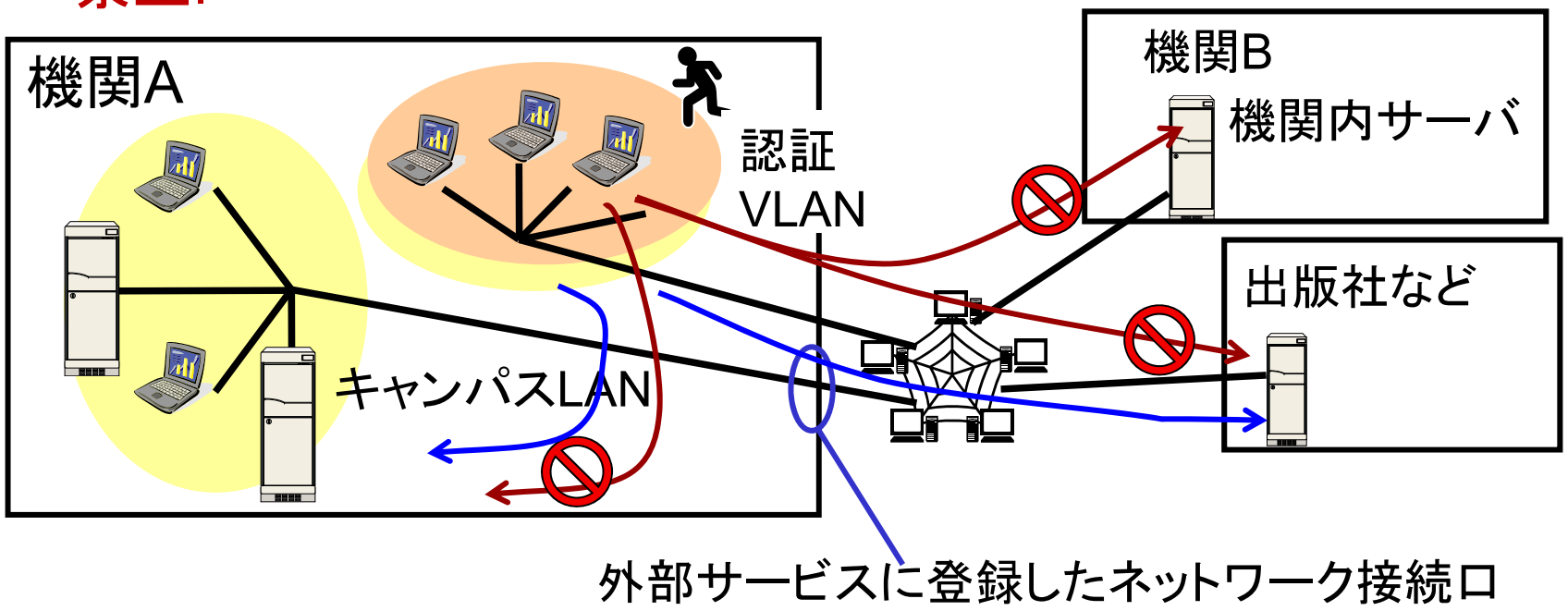
- 学内サービスが利用できないと不満が出る
  - 利用者に理由が伝わりにくい
  - 窓口の負担
- 構成員に使われて、帯域不足になる
  - 訪問者用のネットワーク(NAPT, FW含む)の帯域不足？

本来、eduroamは学内外でシームレスに使うもの.
多くは技術で解決できる.

無線LANシステムの一本化のススメ

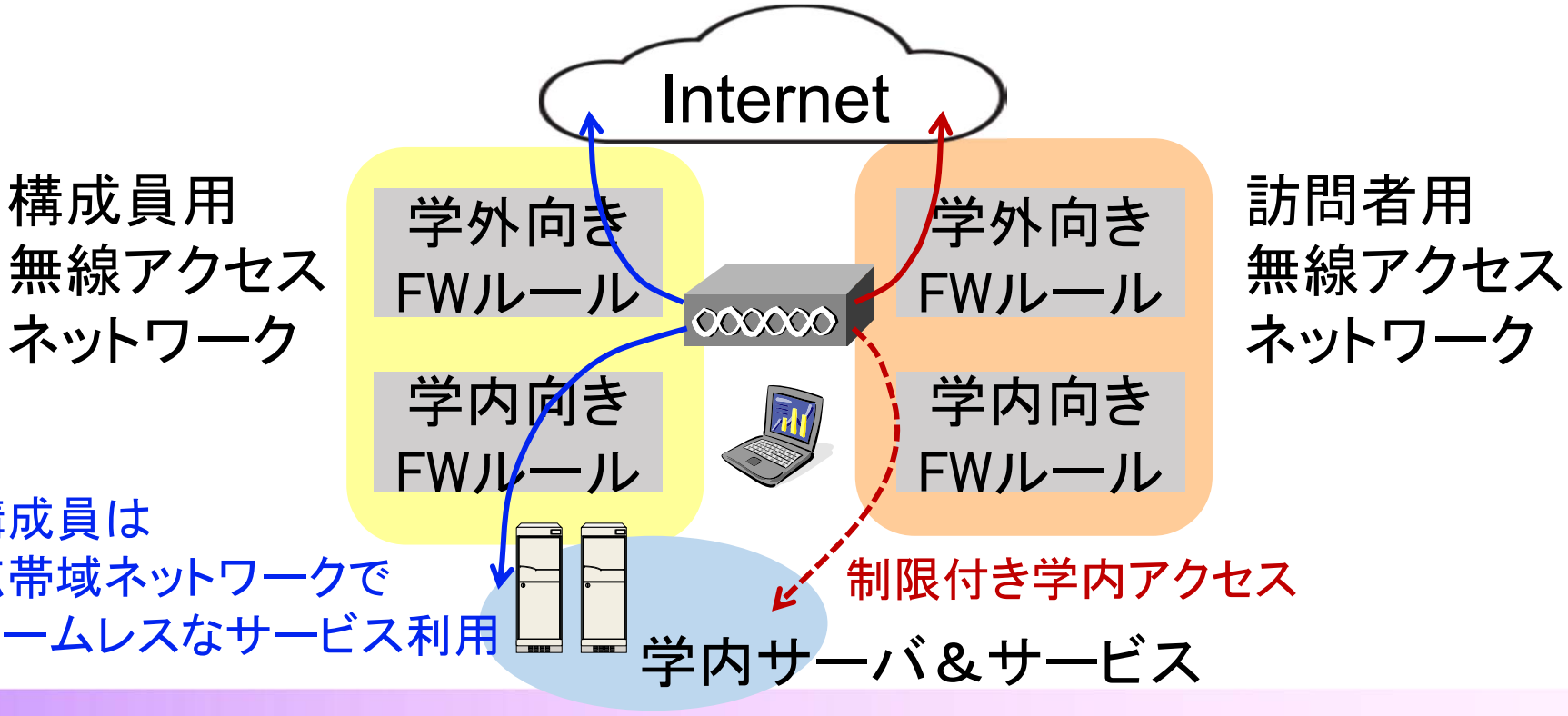
- 「認証VLAN」を導入すれば、自機関の利用者として認証された者の端末をLANに直接収容することが可能. → 利便性が大幅に向上.

訪問者はゲストネットワークに収容し、学内LANにアクセス禁止.



認証VLANによる個人別ポリシー適用

- 構成員用と訪問者用のネットワークを、基地局上でVLAN分離
- 学外向き・学内向きで異なるアクセス制限



認証VLAN導入のメリット

- 構成員は、自由に学内サービスや電子ジャーナルを利用可能（キャンパス内での利用の場合）
- SSIDは“eduroam”のみ
  - 接続が安定する（異なるSSIDの間でパタつかない）
  - 利用もサポートも容易
- 訪問者に学内サービスの一部を公開可能
- 教職員・学生のポリシー分離も可能

デメリット

- 明示的にネットワークを切り替えられない（要る？）

認証VLANの実現方法

1. 機関のRADIUS IdPで属性値を挿入（APがそれを利用）
   - Tunnel-Type = 13
   - Tunnel-Medium-Type = 6
   - Tunnel-Private-Group-Id = <VLAN番号>
2. レルムの機関名一致を調べてproxyで属性値挿入
   - @<機関名>.eduroam.jp
   - proxyで見えるのはouter-identityなので、偽装に注意.
     訪問者に高い権限を付与するケースでは利用不可.
     (共用IdPの場合、機関名を書き換えることで、
     機関内の構成員が訪問者になりすますことが可能)

トラブルの傾向と対策（利用者編）

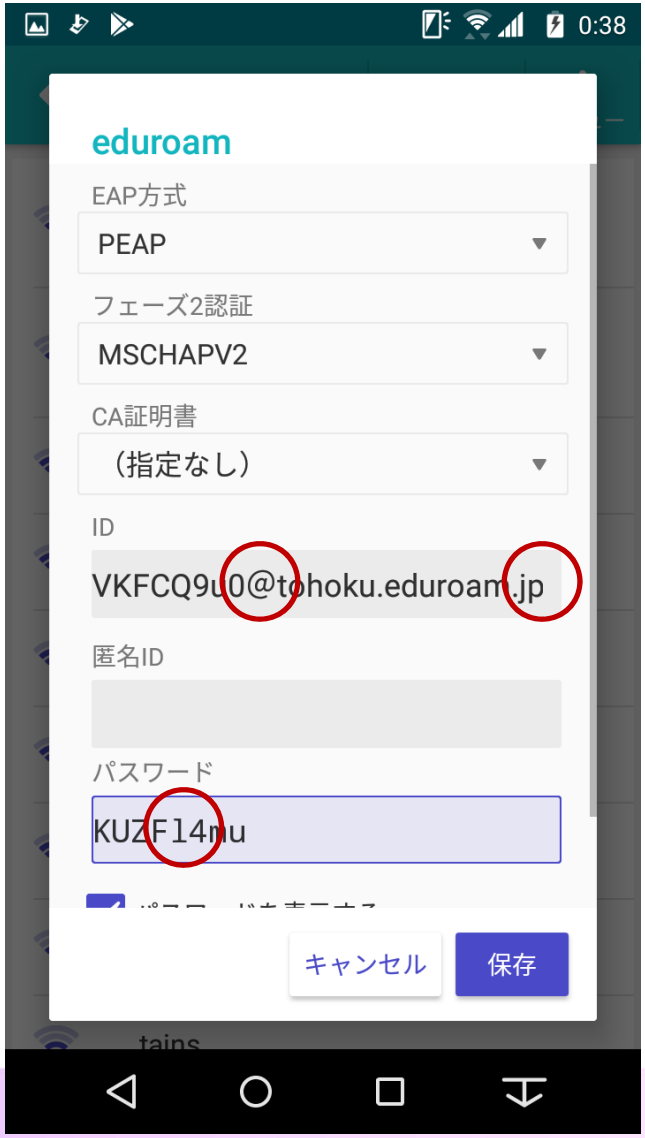
ありがちな設定ミス

- レルムを入力していないので、訪問先でつながらない
  - 注意喚起も必要だが、
    機関内でもレルム無しではつながらない設定
    にしておくと設定時に気付きやすい.
    （出先で不幸になりにくい）
- メールアドレスなど、異なるシステムのIDを入力する
  - 注意喚起に加えて、何よりも、
    eduroamの情報に容易にたどり着けるように配慮.
- IDやパスワードの打ち間違い
  - ありがちな入力ミスを例示して、注意喚起.
  - 入力ミスしやすい文字を使わない.（またはフォントに注意）

トラブルの傾向と対策（続）

正しい入力

誤入力

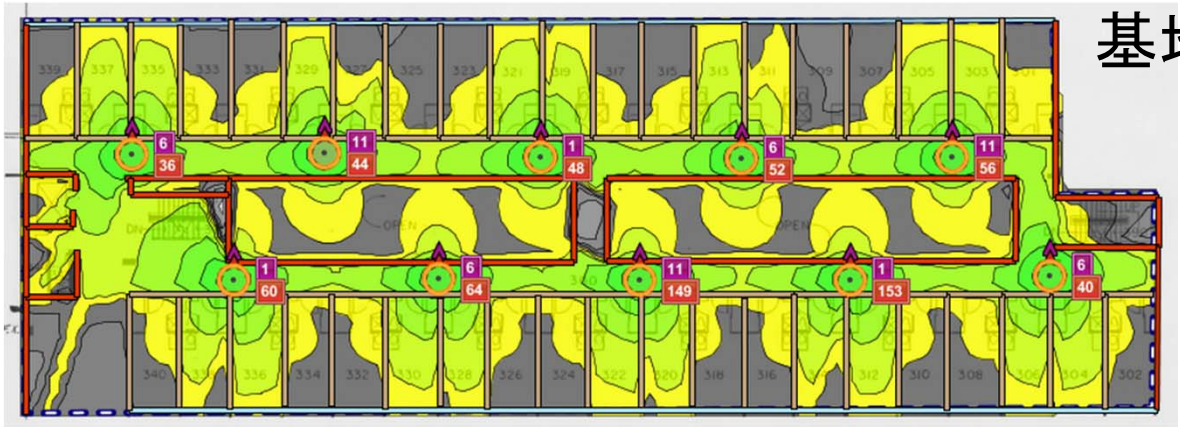


アットマークが全角

末尾に空白

アイ が エル

トラブルの傾向と対策（管理者編1）



基地局を廊下に設置

基地局どうしがよく受信しあえるので、自動調整で電力が絞られてしまう.

電力を上げると干渉が酷くなる.

基地局を室内に設置

Wi-Fi Design: APs in Hallways
http://community.arubanetworks.com/t5/Technology-Blog/Wi-Fi-Design-APs-in-Hallways/ba-p/314718

トラブルの傾向と対策（管理者編2）

DHCPやNATの設計不良　→　eduroamのせいにされてしまう ☹

- 100人教室だからアドレス120もあれば十分だろう
  →端末複数持ちが多くてアドレス不足
- DHCPのリース時間は適当に2時間でいいかな
  →人々の入れ替わりに追いつけなくて枯渇
- 利用者数×アプリ数の数倍ぐらいのNAPTでいいか
  →多数ポート使うアプリのせいでパケ詰まり

十分なサブネットの広さとアドレスレンジを確保.
NAPTの容量に注意.
大規模な会議を想定した設計.
（認証VLANで構成員のNATを分離、帯域確保を推奨）

まとめ

- 技術をうまく駆使して、eduroamの利便性向上や運用コスト低減を図りましょう.
  - 認証VLAN導入のメリットは大きい
  - 利用者ごとに異なるポリシー適用も可能
- トラブルの傾向を分析した対策を.
  - 利用者の設定ミスを減らす工夫、特に広報は重要.
  - 基地局の設置は、装置と電波の特性をよく考えて.
  - アドレス不足、NAT容量不足を起こさないような余裕ある設計を.