ロケーションプライバシーを保護する eduroam匿名アカウントの提案

第9回東海地区CSI事業報告会
（2008/12/24）

京都大学学術情報メディアセンター
古村隆明
komura@media.kyoto-u.ac.jp

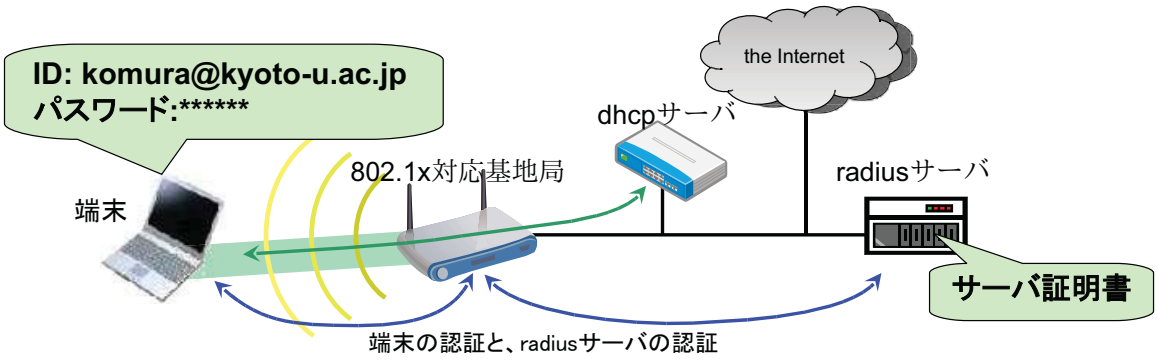
内容

- eduroamの仕組み
- ロケーションプライバシー
- 匿名アカウントの提案

- 京都大学での無線LAN環境の紹介

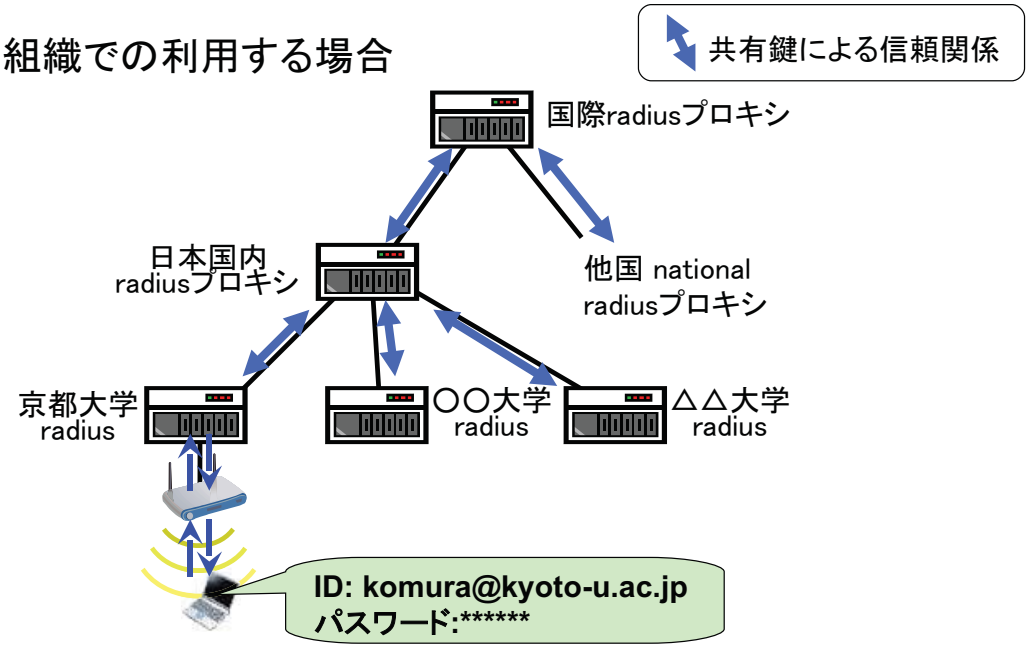
eduroamの認証方式

- 802.1X認証 - radiusサーバを利用した認証
- 利用者をIDとパスワードで認証
  クライアント証明書を利用する方式もある
- サーバ証明書でradiusサーバを認証



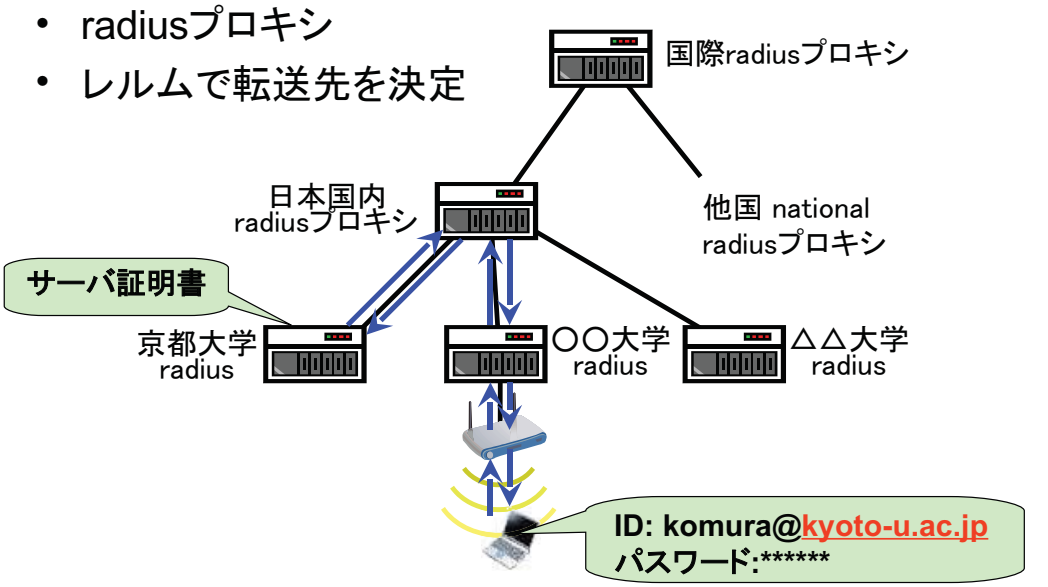
eduroamのローミング

- 自組織での利用する場合

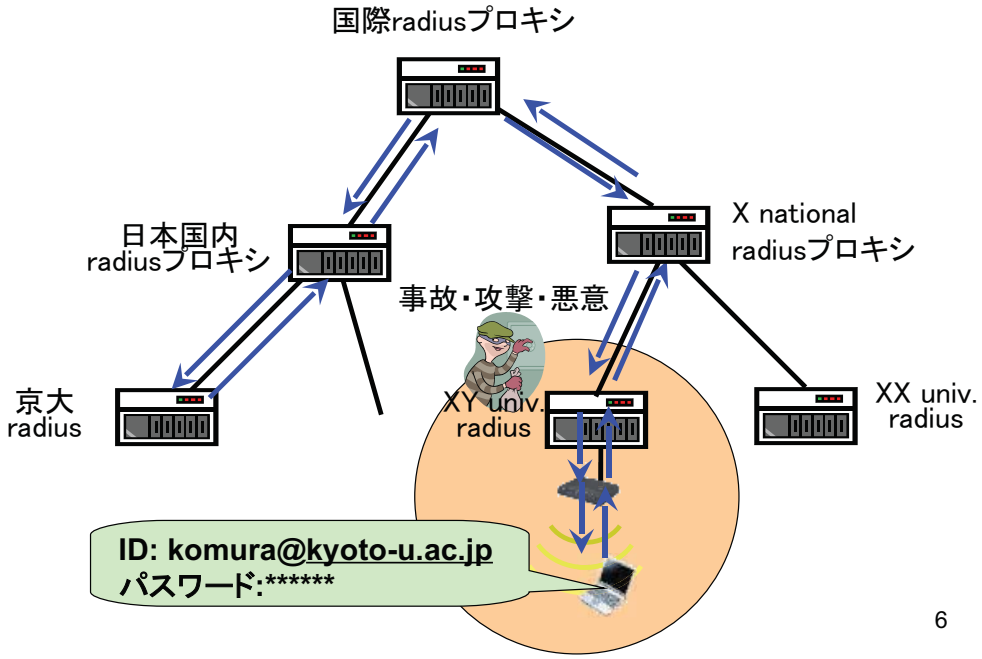


eduroamのローミング

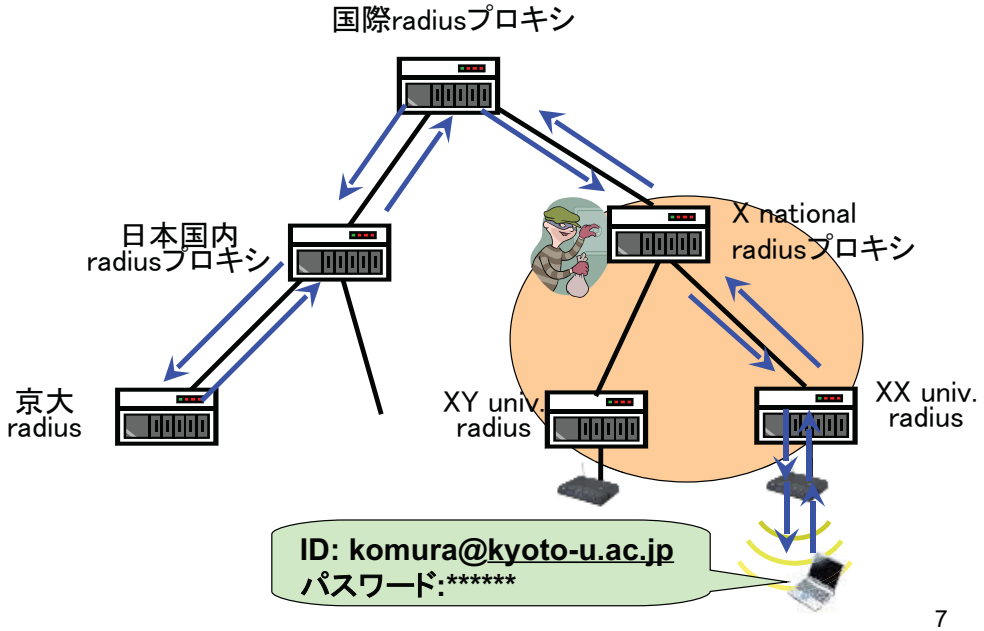
- 他組織から利用する例
- radiusプロキシ
- レルムで転送先を決定



ロケーションプライバシー問題(1)



ロケーションプライバシー問題(2)



ロケーションプライバシーを守る

- 誰がどこへ移動したか追跡できる
  →人物とひも付けできる情報を含まないIDを利用
- ある人物の移動経路が分かる
  →使い捨てIDを利用し、IDを切り替える

使い捨て
匿名アカウント

- どの組織の人がどこへ移動したか分かる
- 複数組織の利用者が
  行動を共にしていることが分かる
  →組織の識別子を含まないIDを利用する

組織間連携
匿名アカウント

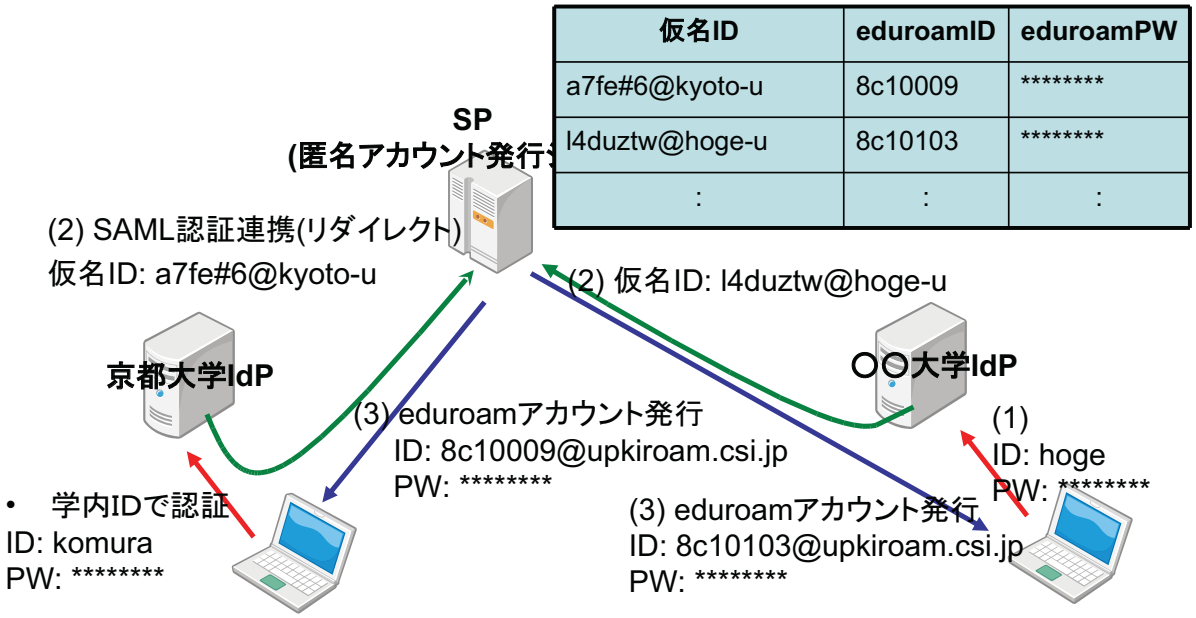
使い捨て匿名アカウント

- 他のIDで認証したあと匿名アカウントを発行
- ID体系（案）: YMDNNSL@upkiroam.csi.jp

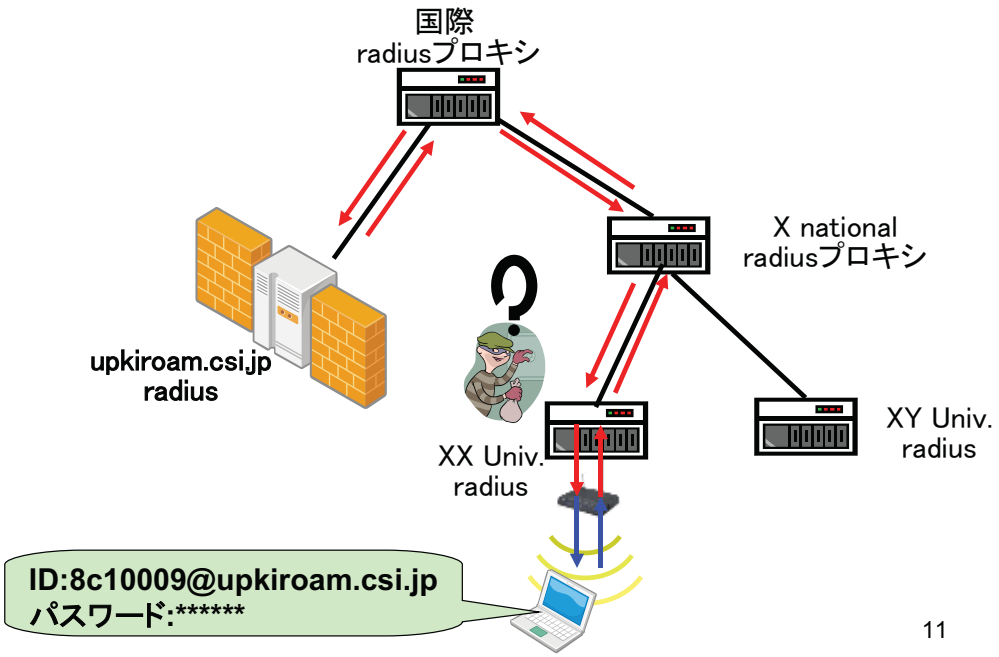
[Y]	発行年西暦下一桁 [0-9]
[M]	発行月 [1-9a-c]
[D]	発効日 [1-9a-v]
[NN]	同一発効日内での通し番号 [00～zz]
[S]	利用開始日 (発効日からのオフセット) [0-9a-z]
[L]	有効期間 [0-9a-z]

匿名アカウントの例: **8c10009@upkiroam.csi.jp**
(2008年12月1日発行、当日から9日間有効)

組織間連携匿名アカウント

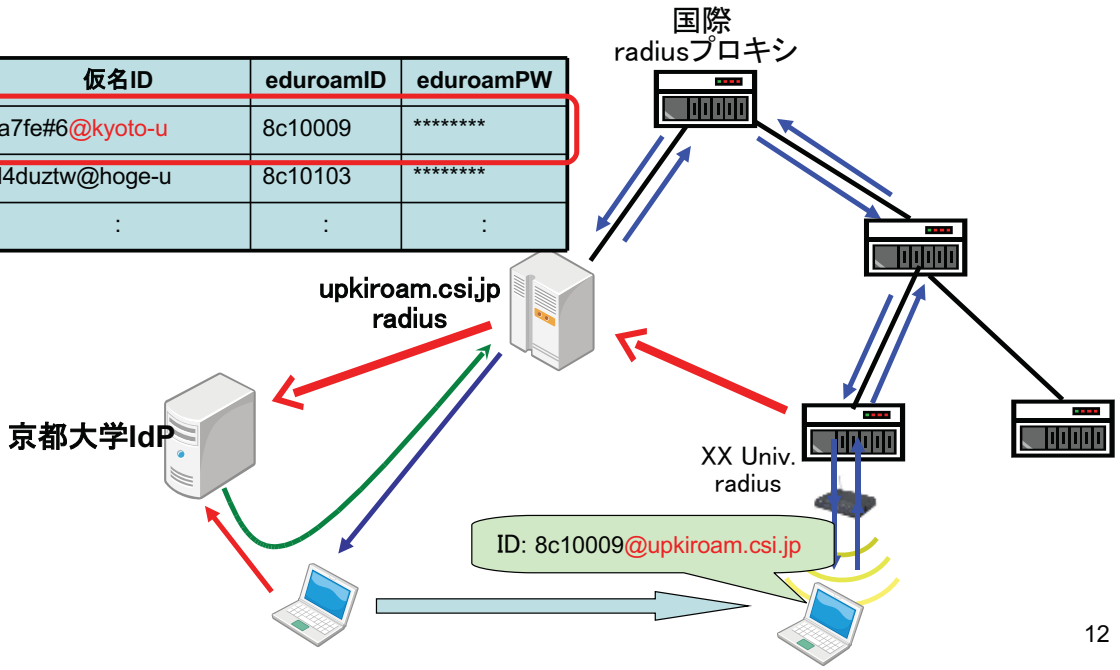


組織間連携匿名アカウントによる認証



組織間連携匿名アカウント利用時の インシデントレスポンス

仮名ID	eduroamID	eduroamPW
a7fe#6@kyoto-u	8c10009	********
l4duztw@hoge-u	8c10103	********
:	:	:



匿名アカウントとパスワード

- IDとパスワード発行の仕組みを単純化
  - IDとパスワードをまじめに管理すると
    radius サーバへIDの追加・削除が必用
  - 秘密のアルゴリズムを利用して
    IDからパスワードを一意に生成
    例: *secret*(“8c10009”) → “E4JA78AZG1”
    secret(“8c10103”) → “KJY9UELQ70”
  - (秘密の)アルゴリズムをアカウント発行サーバと
    radiusで共有すれば、IDの追加・削除が不要
  - 有効期限情報はID内にエンコード済み

京都大学の
無線LAN環境の紹介

環境

- 京大内のネットワーク
  - 多数のVLAN (Virtual VAN) で構成
  - 研究室やプロジェクトなどごとにサブネットを割当
  - サブネット毎にVLANを設定
  - バックボーンは tagged VLAN の嵐
  - 通常の利用者に VLAN は見せない (port VLANで提供)

導入機器の紹介

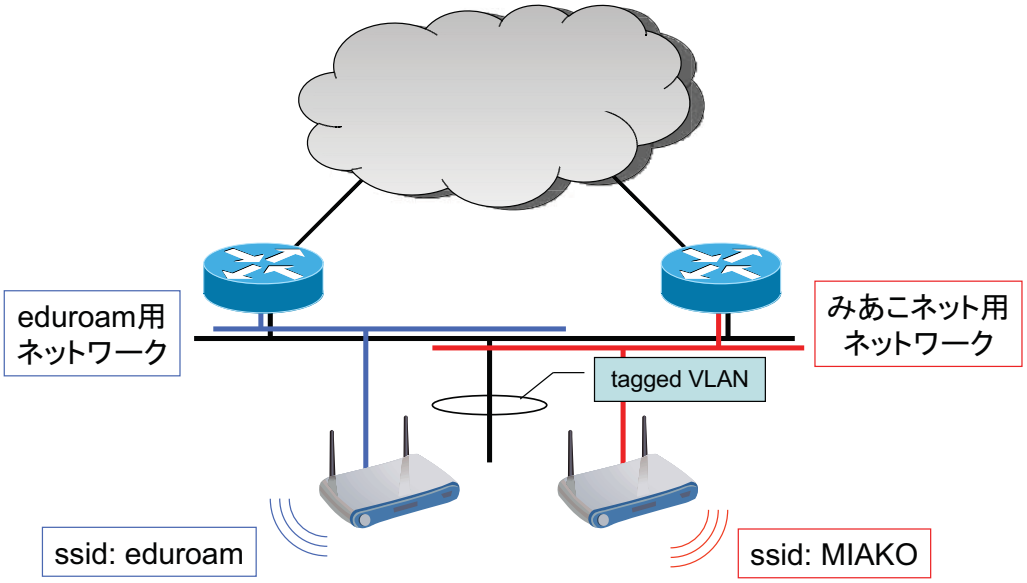
- Allied Telesis AT-TQ2403

特徴

- 802.1X 認証対応
- マルチSSID、tagged VLAN対応
  - 一台の基地局で複数のSSIDを扱える
  - SSID毎に有線側tagged VLANと対応付け可能
  - SSID毎に異なる認証方式を設定可能

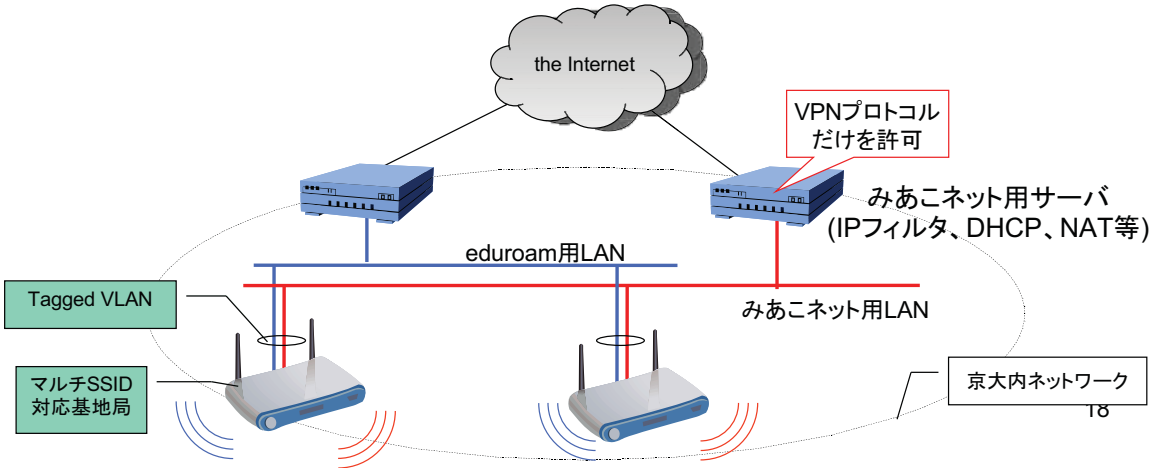
→ポリシーの異なる複数の無線ネットワークを一台の基地局で提供可能

tagged VLAN＋マルチSSID

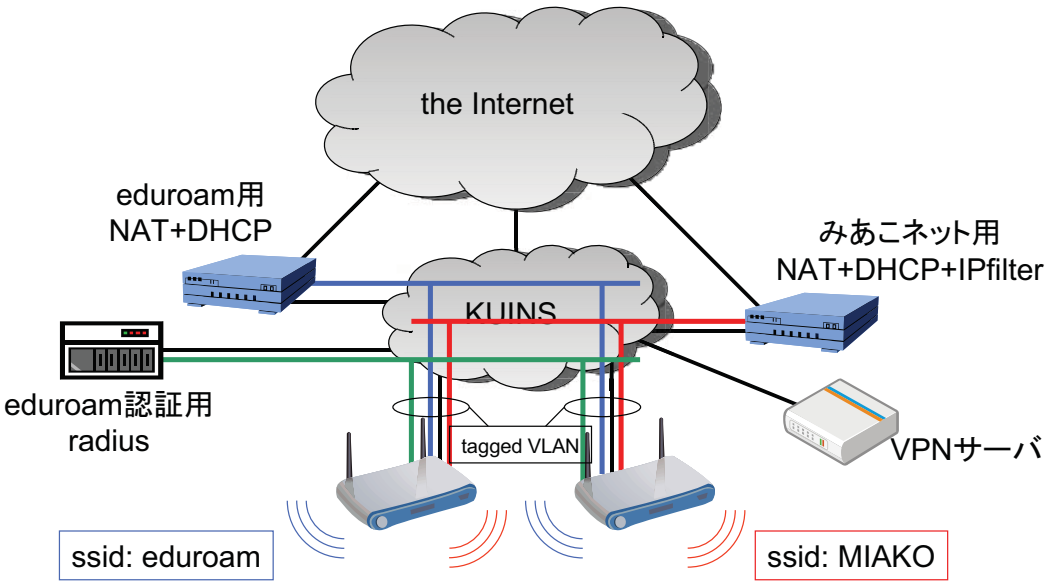


eduroam+みあこネット

- 複数のSSIDを利用し、複数の無線LAN環境を提供
  - eduroamとみあこネットを同時に提供
- tagged VLAN 接続
- ケーブルを抜かれると危険→設置場所の工夫やケーブルに鍵



ネットワーク構成



まとめ

- eduroamローミングの仕組み
- ロケーションプライバシー
- 匿名アカウントの提案
  - SAML連携
  - IDとパスワードの生成

- 京都大学での無線LAN環境の紹介