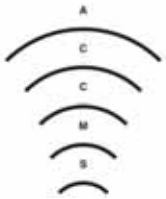


認証技術の応用

ネットワークセキュリティ技術研修
2008/12/28

京都大学学術情報メディアセンター
古村隆明

内容

- **背景**
- eduroam
- **みあこネット**
- **京都大学でのネットワーク・機器構成**
- **接続用アカウント**
  - **ゲストアカウント**
  - **ロケーションプライバシーを守る**

背景

- 無線LANをどこからでも安く安全に利用したい

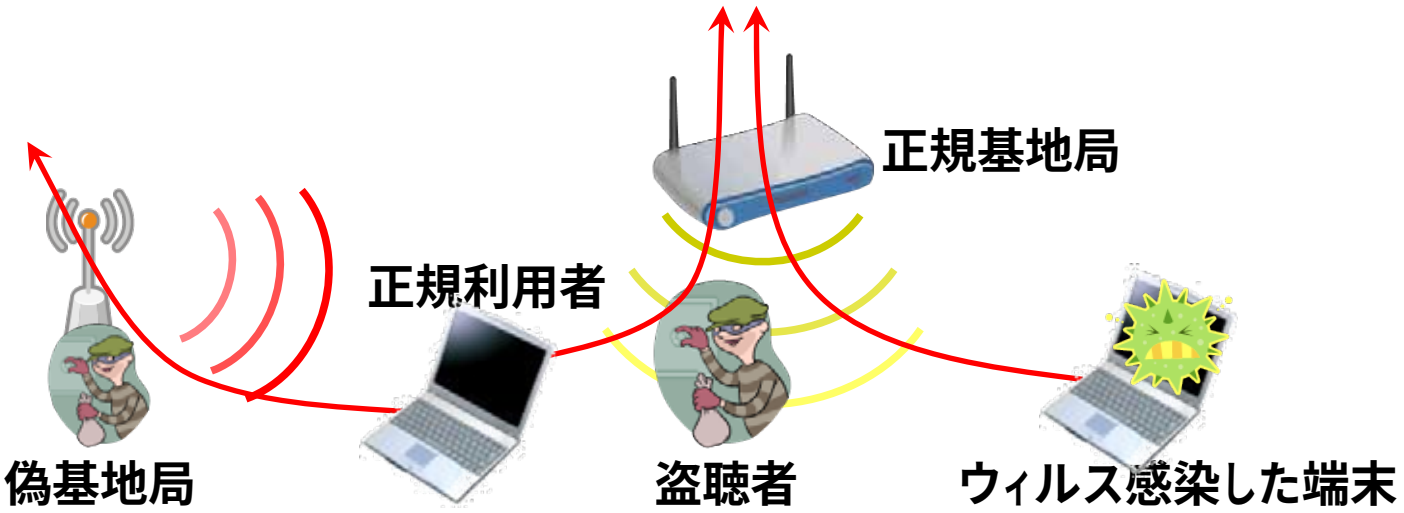
- 普段生活している場所の多くでは利用可能
  - 必要な場所には自分たちで設置できる
- 外出すると利用できる場所が意外に少ない
  - 複数サービスが乱立
    - 複数サービスに加入する？　→ 方式の違い、お金がかかる
    - 事業者の基地局増設を待つ？　→ なかなか増えない

- 広範囲で利用できる環境を作るには
  - お互いに、設置した基地局を訪問者にも提供する

→二つの立場：利用者として、基地局設置者として

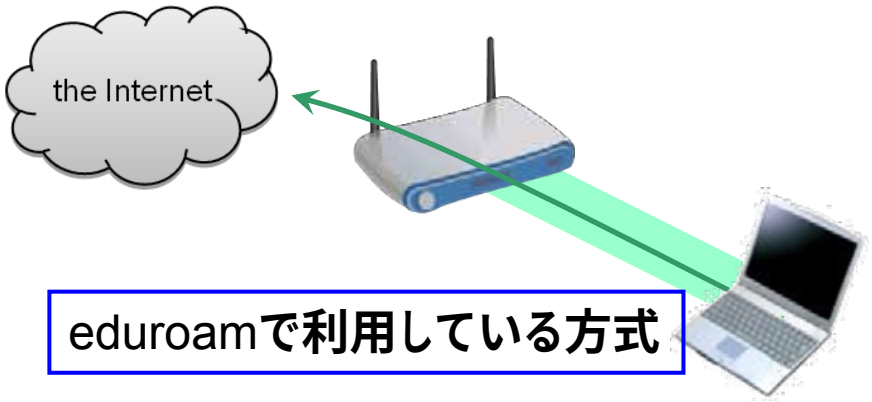
無線LANにつきまとう危険性

- 利用者側
  - 他利用者による
    盗聴，改ざん，なりすまし等
  - 偽基地局による
    情報の搾取，フィッシングサイトへの誘導等
- 基地局設置者側
  - 非正規利用者の利用
  - 不正利用発覚時の追跡
    ウィルスメール送信，攻撃

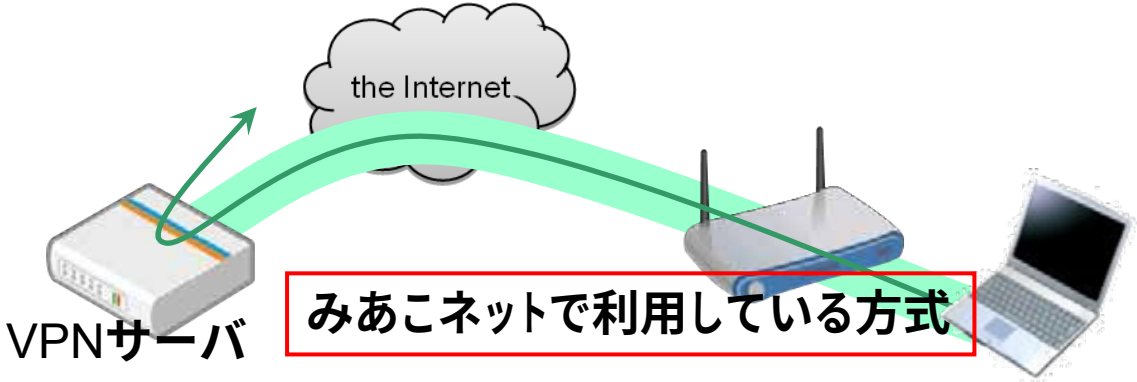


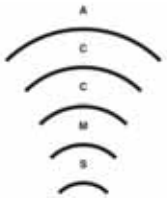
無線LANを安全に使う

- **無線区間を安全に**
  - WPA / WPA2
  - 802.1X **認証**



- **途中経路(無線も有線も含む)を安全に**
  - VPN**接続**

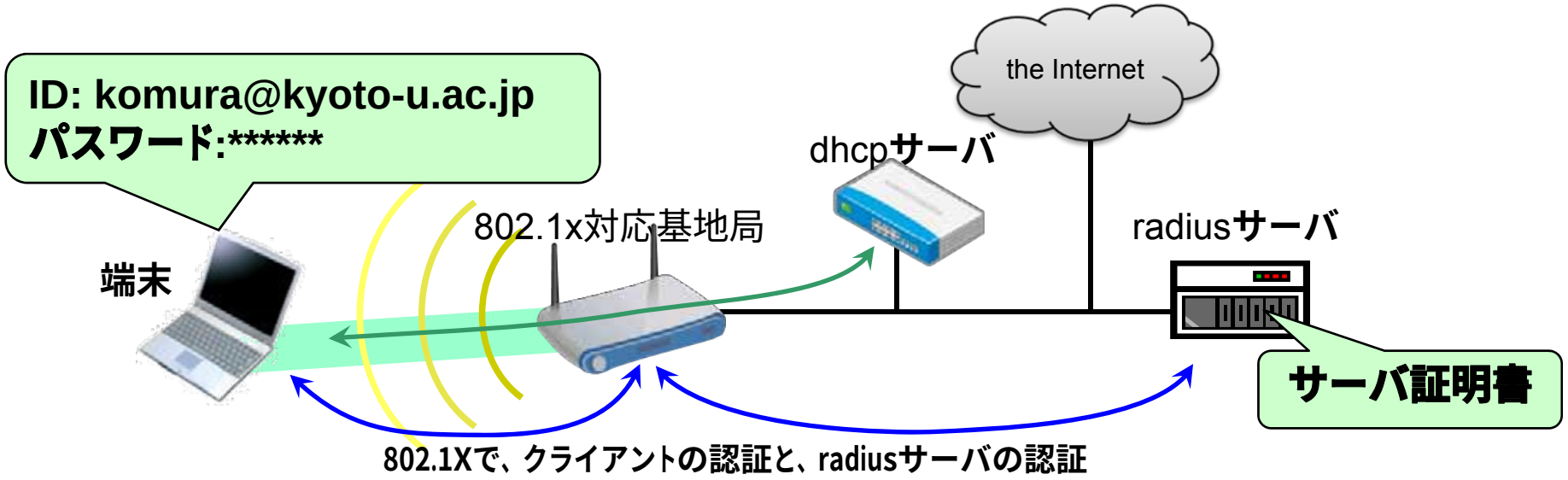




eduroam

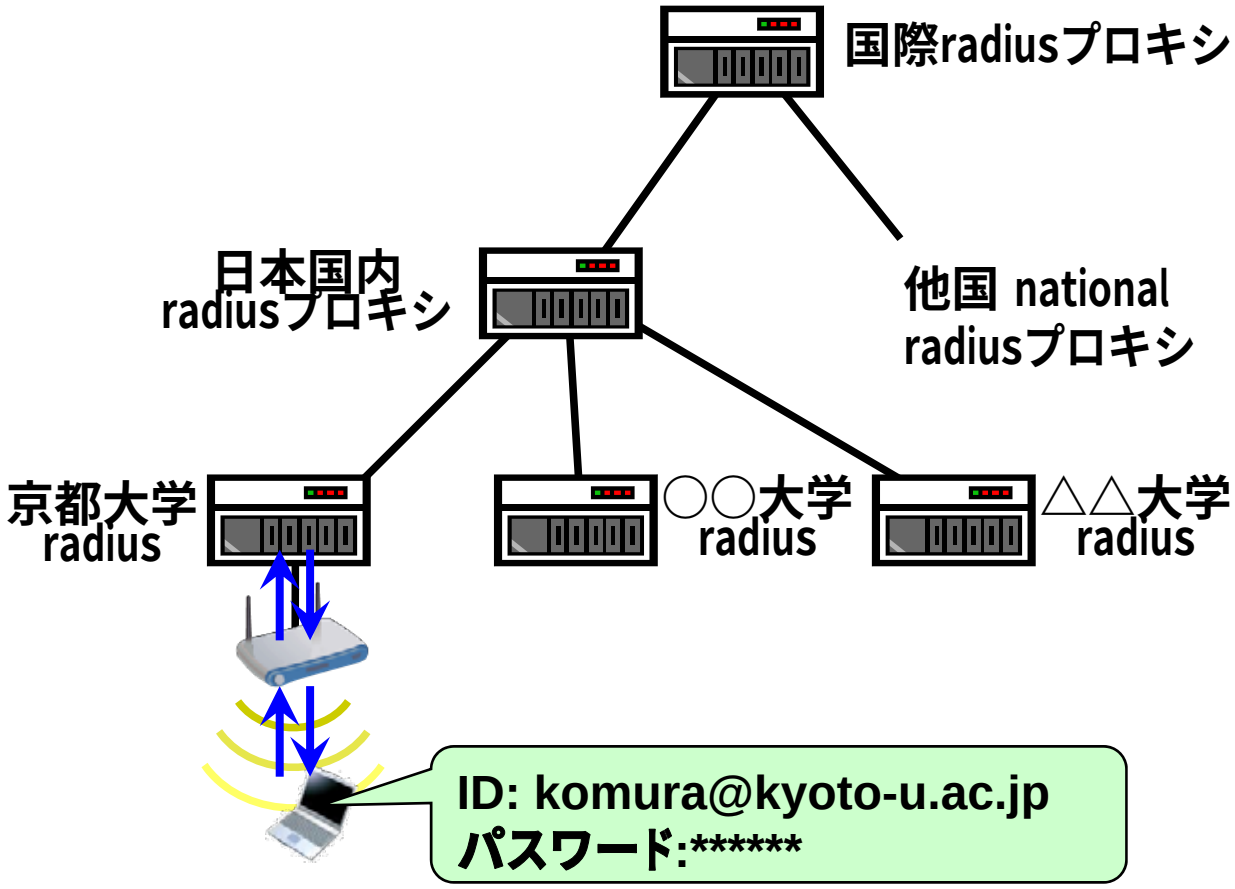
eduroamの認証方式

- 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**



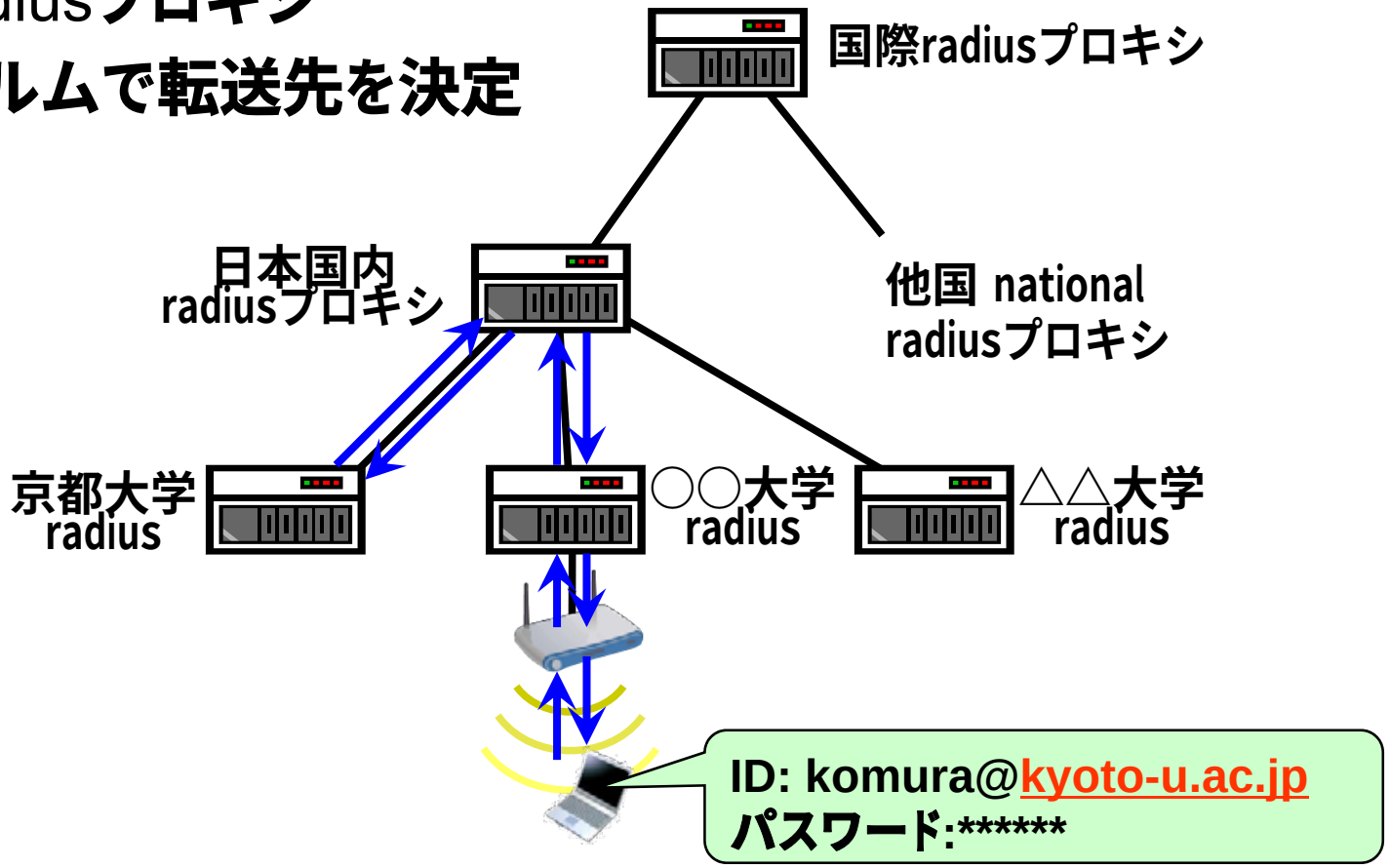
eduroamのローミング

- **自組織での利用する場合**



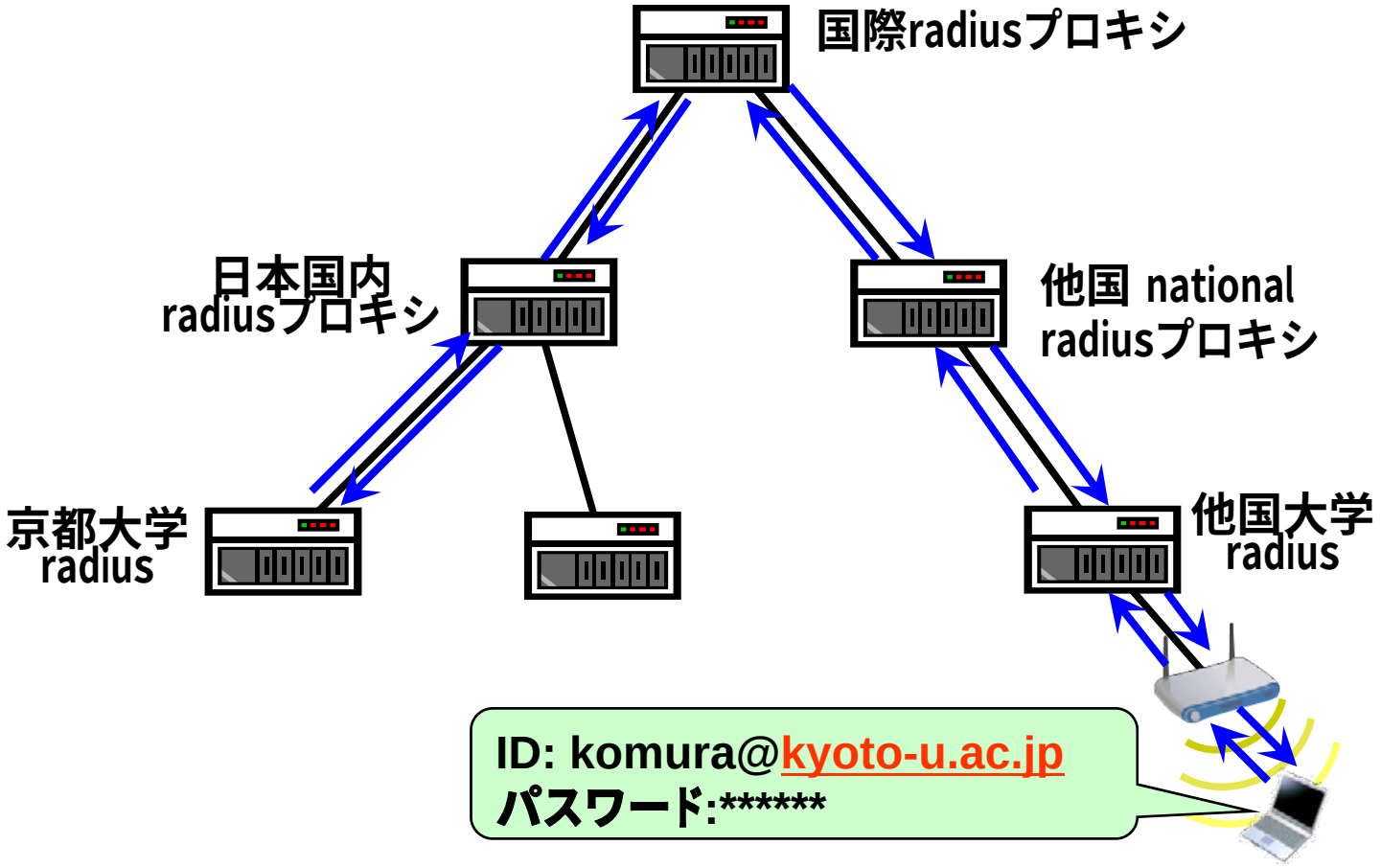
eduroamのローミング

- **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**



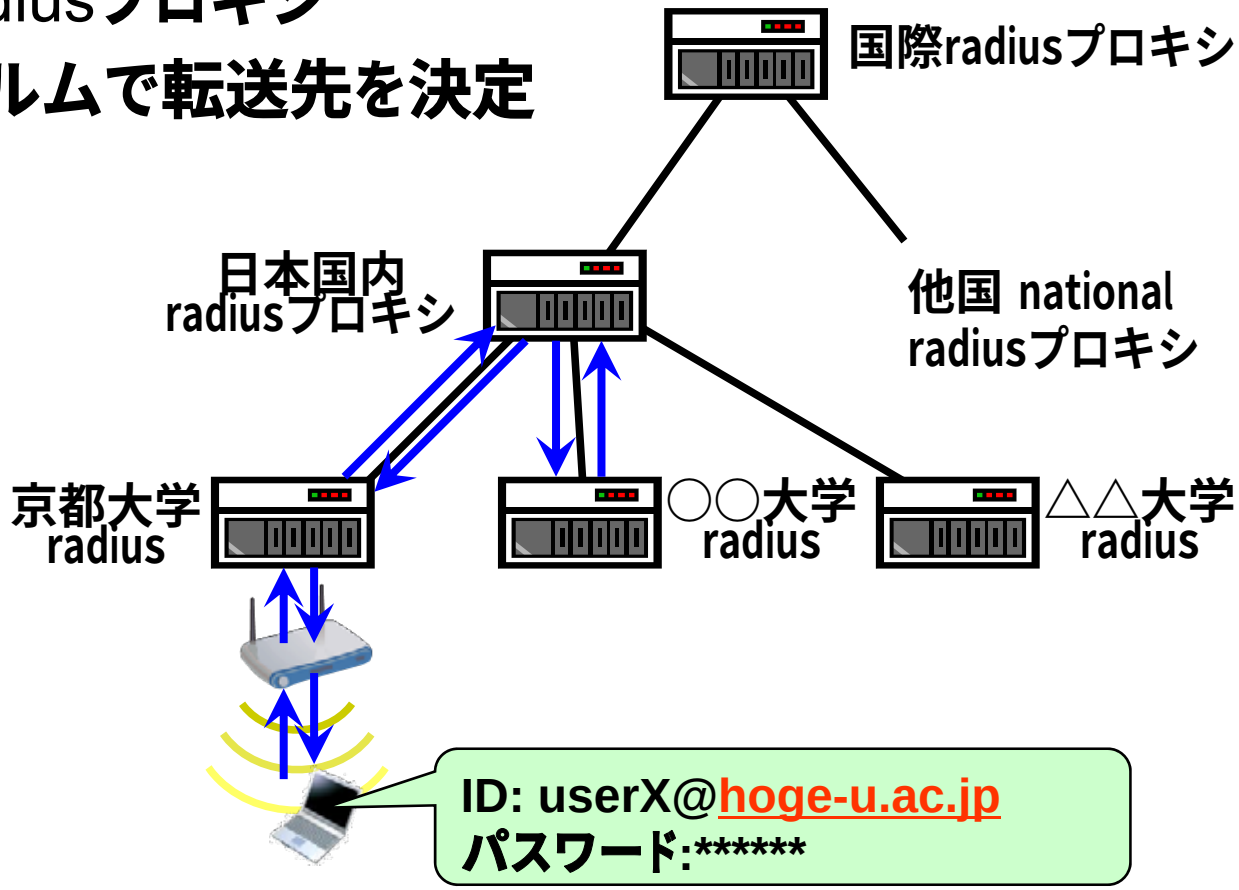
eduroamのローミング

- 国外から利用する例



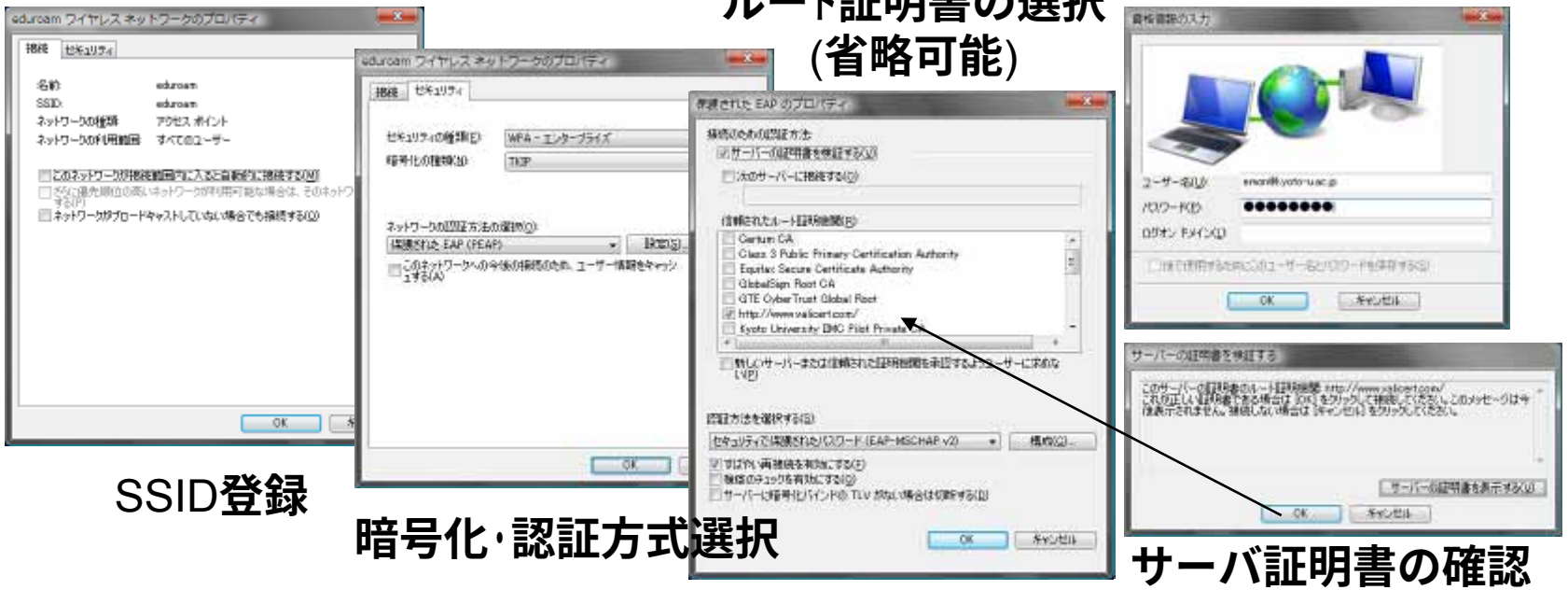
eduroamのローミング

- **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**



eduroam**設定例**(1)

- 802.1x**認証用クライアントソフト(サプリカント)が必要**
  - Windows**標準**(2000sp4**以降**/XP/Vista), MacOS X**標準**
  - Intel**社製**, Juniper**社製(有償)**, Xsupplicant (**オープンソース)等々**
- Windows**標準サプリカントの設定例**



eduroam設定例(2)

- FreeBSDでの例 (FreeBSD 6.0以降)
  意外に簡単
- **設定ファイルを書く** (wpa_supplicant.conf)

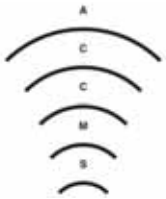
```
network={
    ssid="eduroam"
    scan_ssid=1
    proto=TKIP
    key_mgmt=WPA-EAP
    eap=PEAP
    identity="test-user@eduroam.kyoto-u.ac.jp"
    password="password"
    ca_cert="valicert.pem"
}
```

- **サプリカントを起動**

```
# wpa_supplicant -i iwi0 -c wpa_supplicant.conf
```

eduroamのまとめ

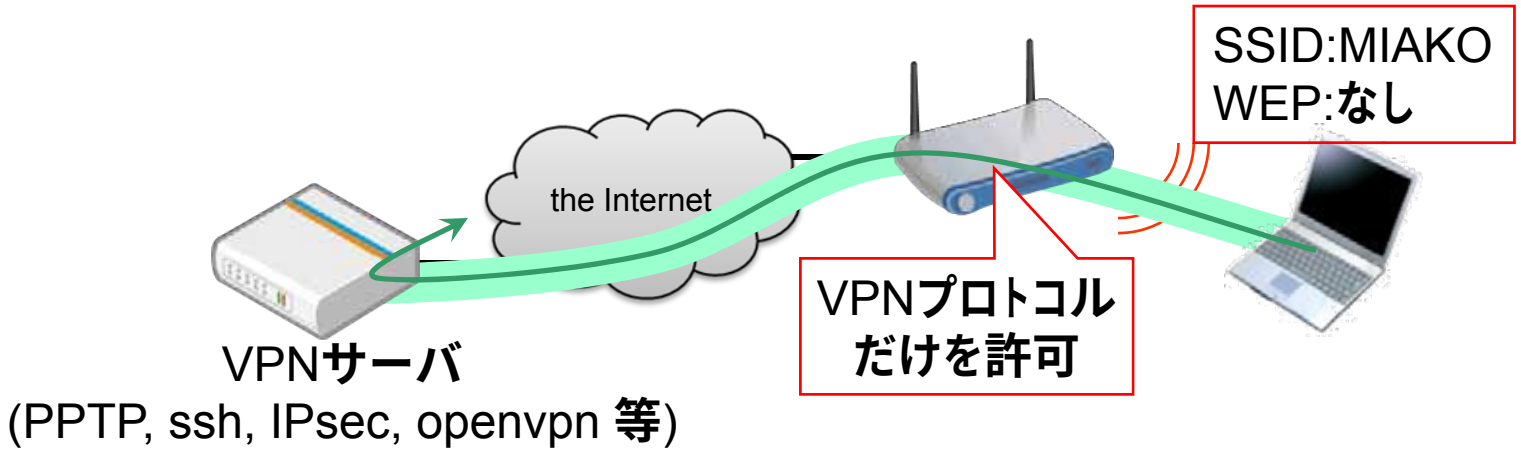
- **学術･研究機関を対象とする無線LANローミング方式**
- **参加組織間で、radius連携による無線LANの認証連携**
  - **どの組織で発行されたIDでも認証可能**
  - **参加組織数 350以上**
  - **日本は2006年8月に参加**
    - **国立情報学研究所、北海道大学、東北大学、高エネルギー加速器研究機構、名古屋大学、京都大学、九州大学**
- **参加組織募集中!!**
  - **詳細は** http://www.eduroam.jp/



みあこネット

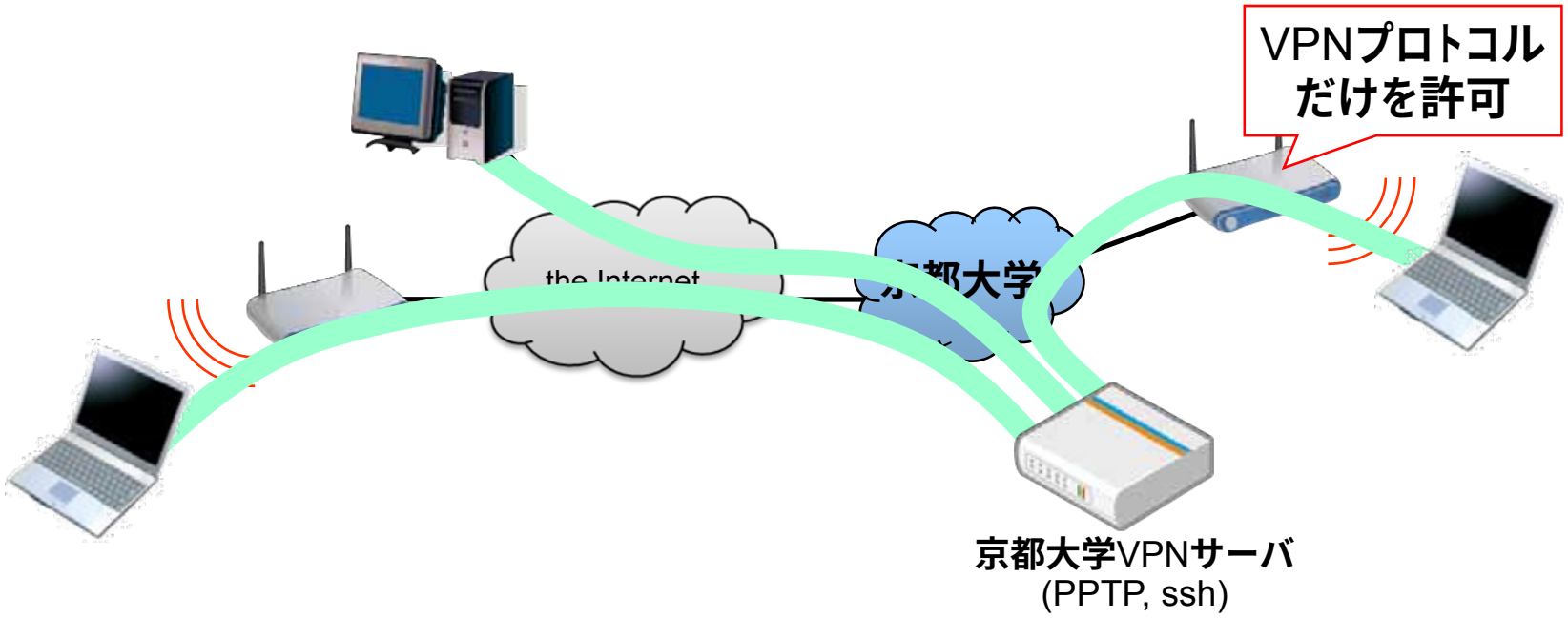
みあこネットの紹介

- VPN通信しか許さない無線LAN基地局
  - 「SSID: MIAKO, WEP: なし」で誰でも接続可能
  - VPN通信以外は基地局でフィルタ
    - PPTP, ssh, IPsec, openvpn など(認証と暗号化)
    - VPNプロトコルであれば世界中どこへでも接続可能



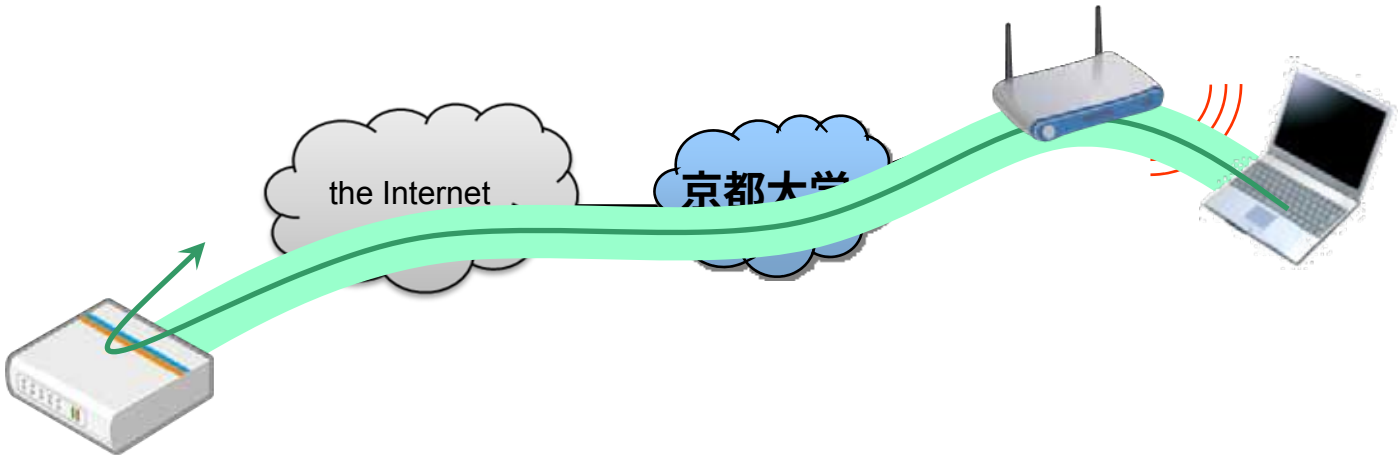
みあこネットの利用形態

- 本学構成員の利用形態
  - 学内のみあこネット基地局から
  - 学外のみあこネット方式基地局から
  - 自宅から (学内限定サービスへのアクセス)



みあこネットの利用形態

- 来訪者の利用形態
  - 学内のみあこネット基地局から、
    自組織で立ち上げているVPNサーバへ接続



eduroamとみあこネットの比較

	eduroam	みあこネット
方式	802.1X認証＋radiusサーバ間連携	VPN接続のみを許可するフィルタ
方式の利点	認証後は現地のIPアドレスが割当てられインターネットと直接通信可能	基地局とVPNサーバ間に 連携のための設定が必要ない
方式の欠点	基地局とradius間、複数のradius間 であらかじめ連携の設定が必要	全ての通信がVPNサーバ経由になり 経路に無駄がある
利用対象者	eduroam参加組織の構成員	VPNサーバに接続できる利用者
利用者にとっての利点	常に一つのIDとパスワードで認証 認証完了後は普通に通信可能	常に一つのVPN接続設定で利用可能
利用者にとっての欠点	802.1x認証の相性問題、 基地局によって非対応方式も有り	数多くあるVPNプロトコルの 全てに対応はできない

京都大学での
ネットワーク・機器構成

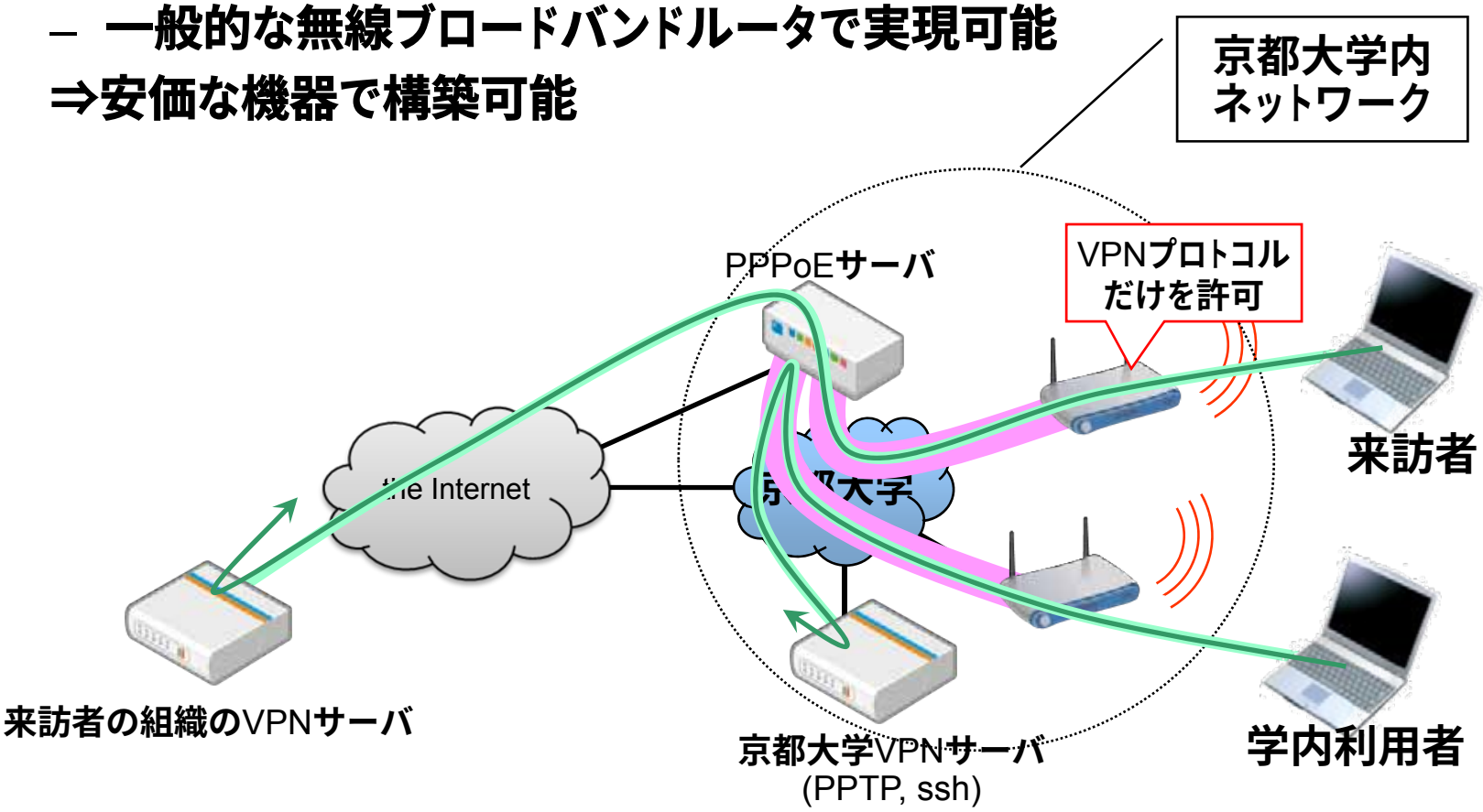
環境

- 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)

学内での導入事例(1)
みあこネット

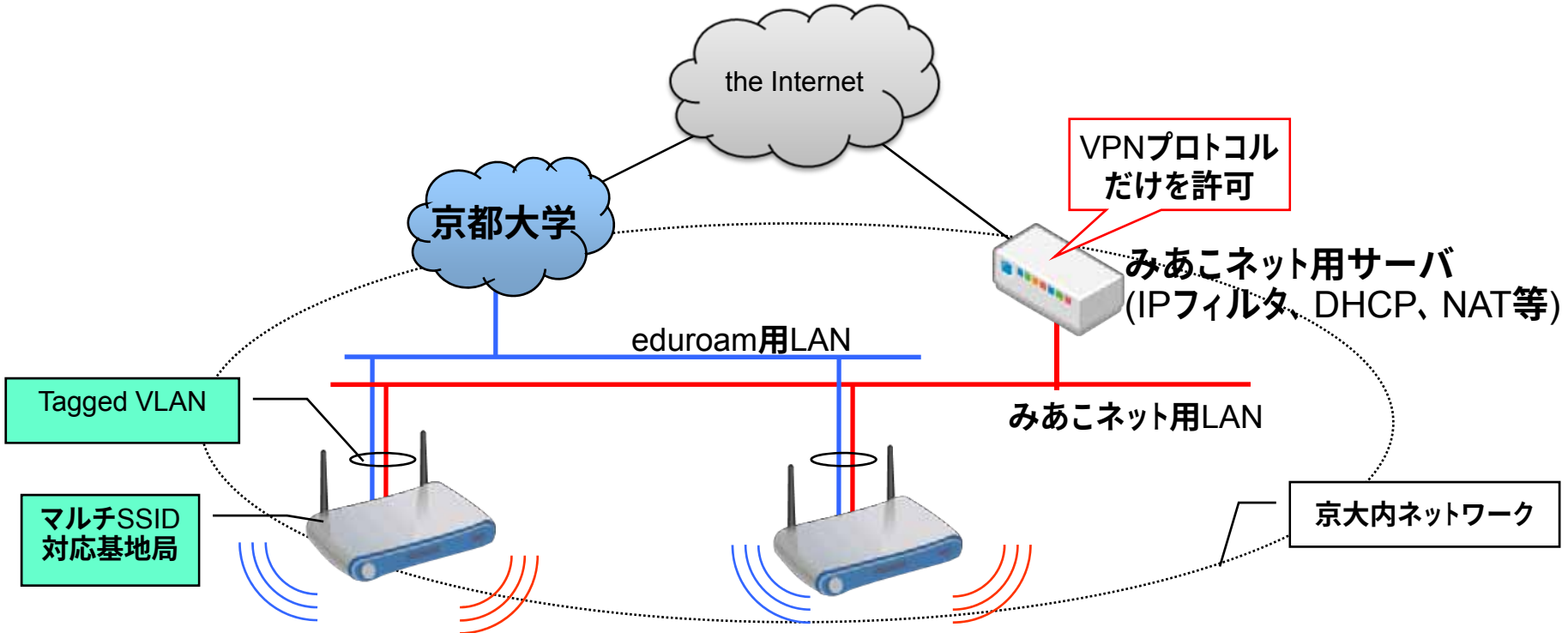
- **学内ネットワーク内でPPPoE接続**
  - **ネットワークケーブルを抜かれた場合への対策**
  - **一般的な無線ブロードバンドルータで実現可能**

  ⇒安価な機器で構築可能



学内での導入事例(2)
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**
- **みあこネットとeduroamを同時に提供**
- tagged VLAN **接続**



導入機器の紹介

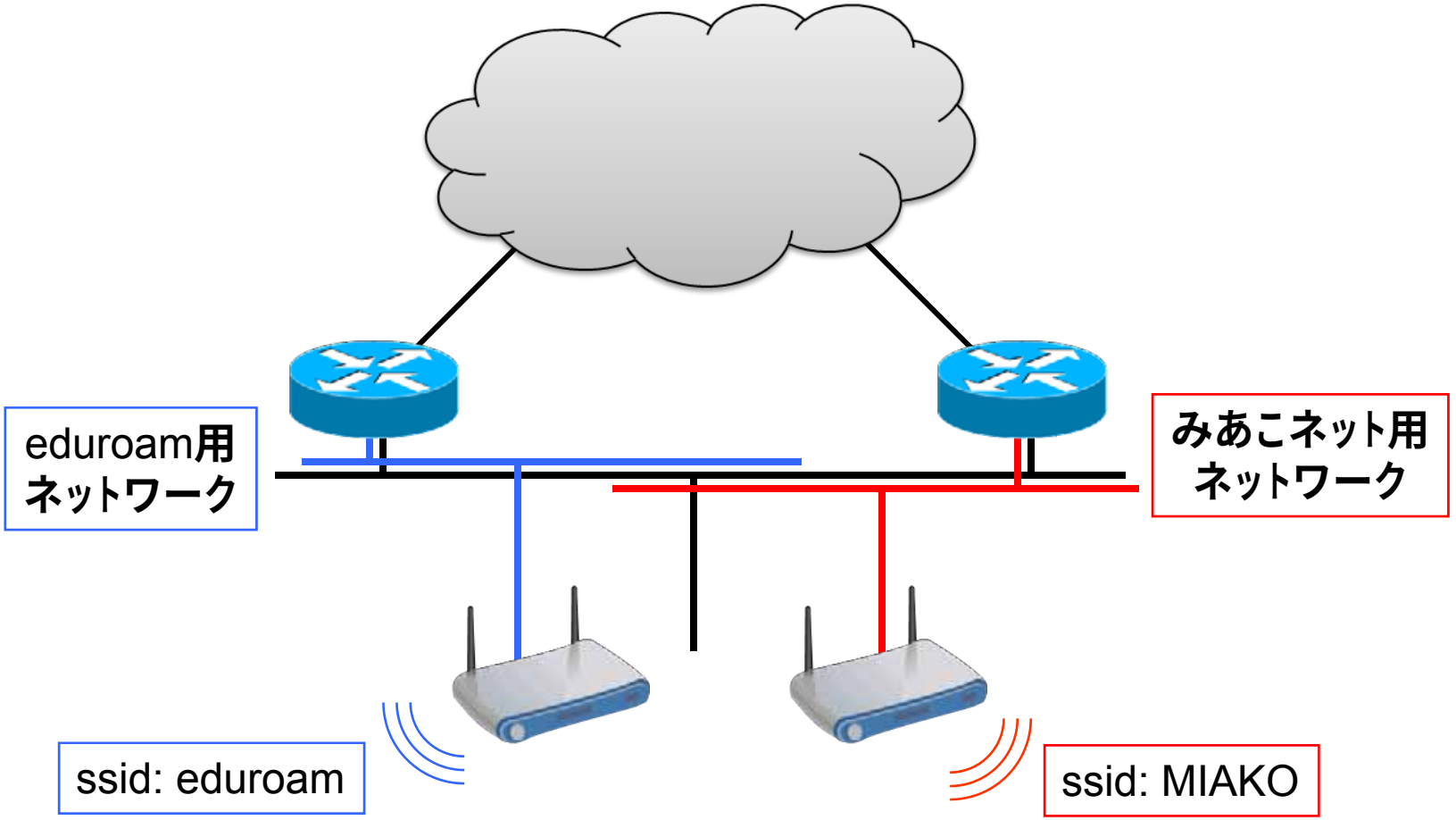
- Allied Telesis AT-TQ2403

特徴

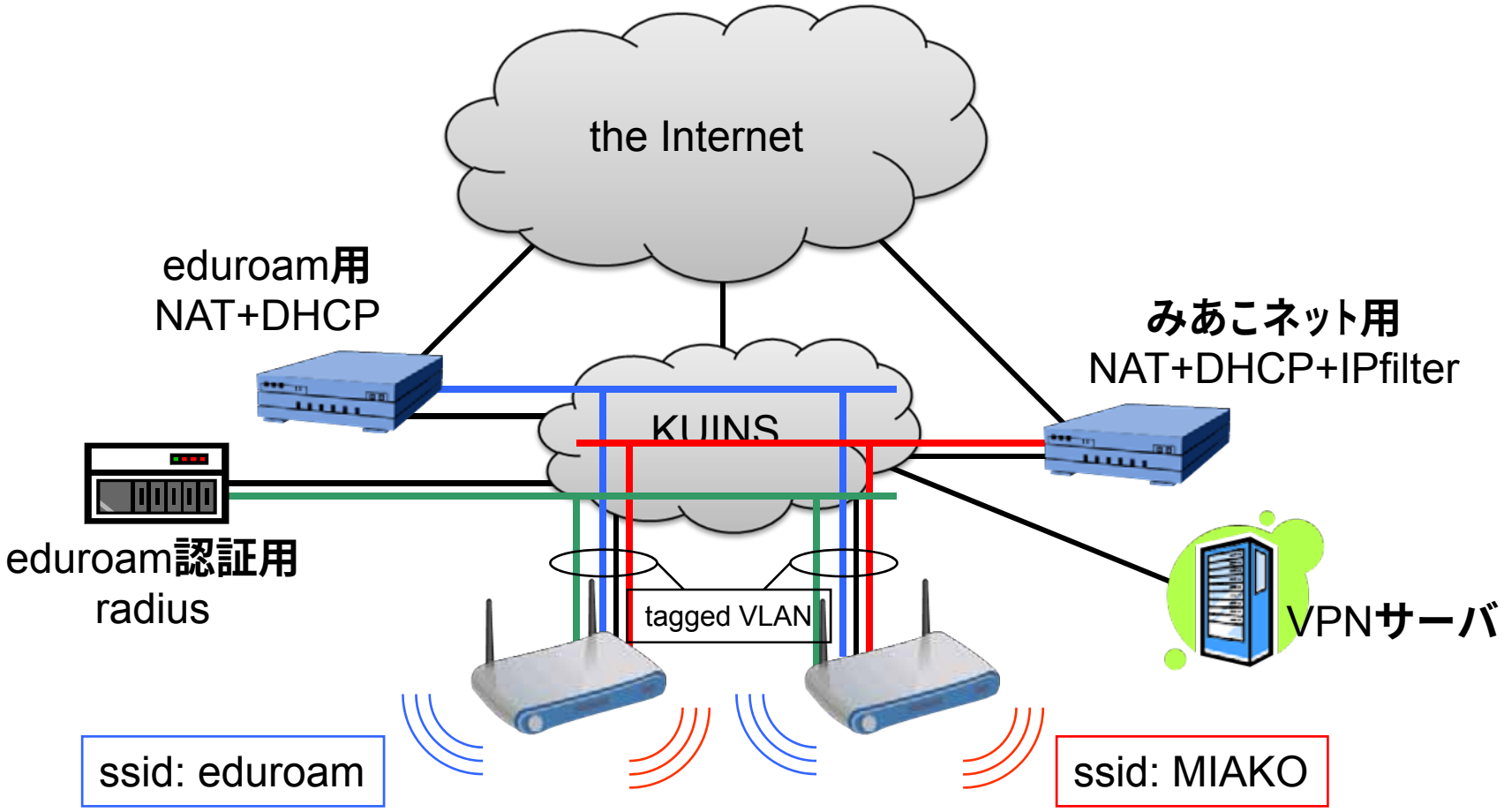
  - 802.1X **認証対応**
  - **マルチ**SSID、tagged VLAN**対応**
    - **一台の基地局で複数の**SSID**を扱える**
    - SSID**毎に有線側**tagged VLAN**と対応付け可能**
    - SSID**毎に異なる認証方式を設定可能**

→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

マルチSSID，tagged VLAN



ネットワーク構成


the Internet
eduroam用
NAT+DHCP
みあこネット用
NAT+DHCP+IPfilter
KUINS
eduroam認証用
radius
tagged VLAN
VPNサーバ
ssid: eduroam
ssid: MIAKO

接続用アカウント

京都大学で提供中のVPNサービス

- PPTP
  MS-CHAPv2**で相互認証が行われ，偽基地局にも対処可能**
  - ECS-ID **による認証**
  - **ゲストアカウント**
    - **学会等イベント開催時の参加者向け**
    - **教職員の権限で期限付きアカウントを発行可能**
- SSH (ssh port forward)
  - ECS-ID **による認証**

ECS-ID:
京大の学生･教職員が取得可能な教育システムを対象としたアカウント

利用形態

- **学内･学外のみあこネット方式基地局から接続**
- **学外から学内専用サービスへアクセスするため接続**

京都大学で提供中のVPNサービス

来訪者向けの臨時アカウント

- 教職員の権限でゲストアカウント発行可能
  - PPTP接続用 (みあこネットの利用を想定)
  - 学内で開催される学会、セミナー等の参加者向け
  - Webで一度に複数のアカウントを申請可能
  - 1アカウントずつ印刷できるようレイアウト
  - アカウント名の一部に、
    発行者を特定できるIDを埋め込み

  →インシデント発生時の追跡を容易に

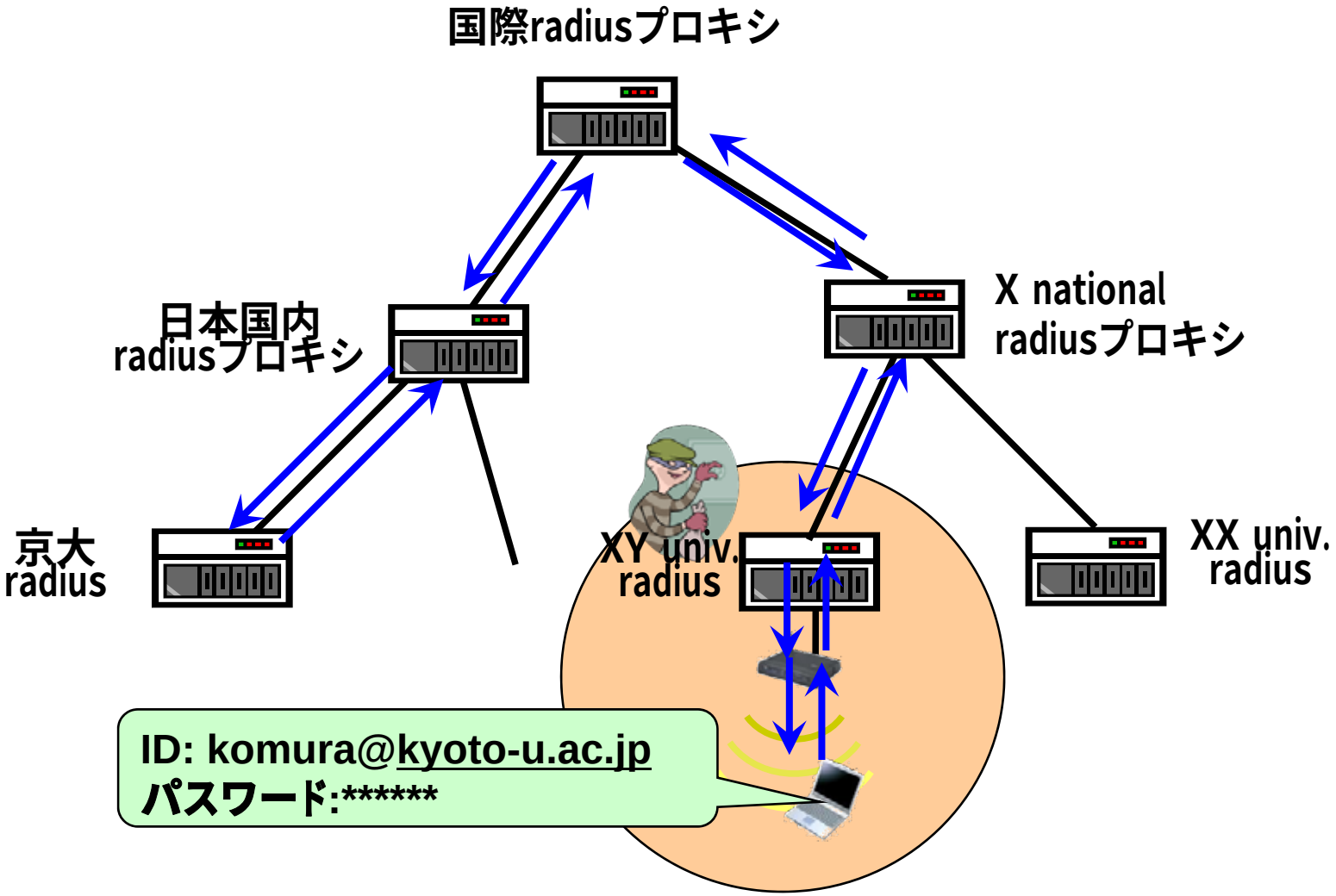
eduroam用アカウント

どのようなIDをeduroamアカウントとして利用するか？

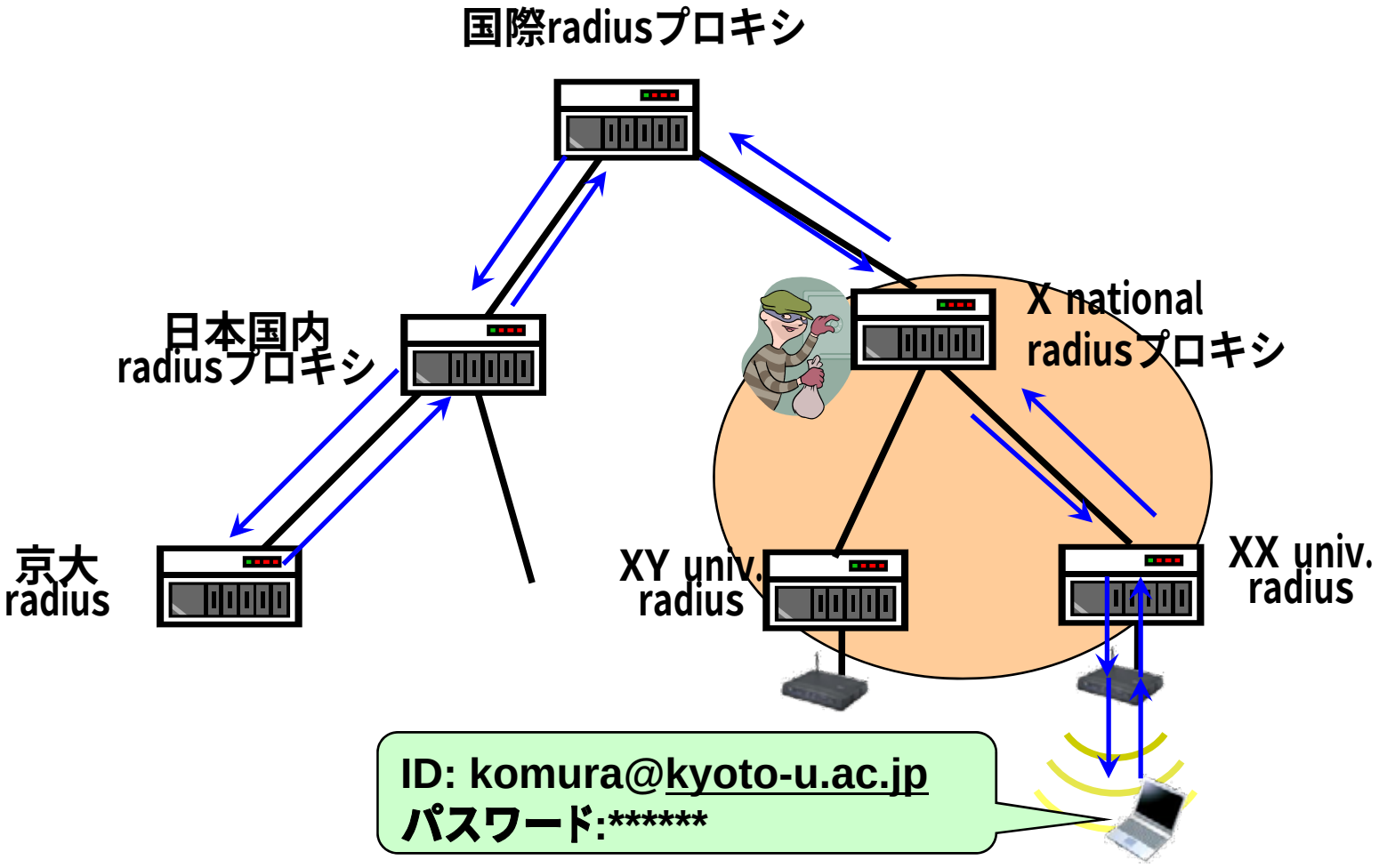
- 学内システム共通のECS-IDは？
  - 利用者の利便性は高い

  しかし
  - セキュリティレベルの違う複数システムで同一IDを共有すべきではない
    - eduroam はセキュリティ的に問題のあるWeb認証も許していた (2007/9以降は禁止のはず)
  - ロケーションプライバシー侵害の恐れ

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

- ある組織の人物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

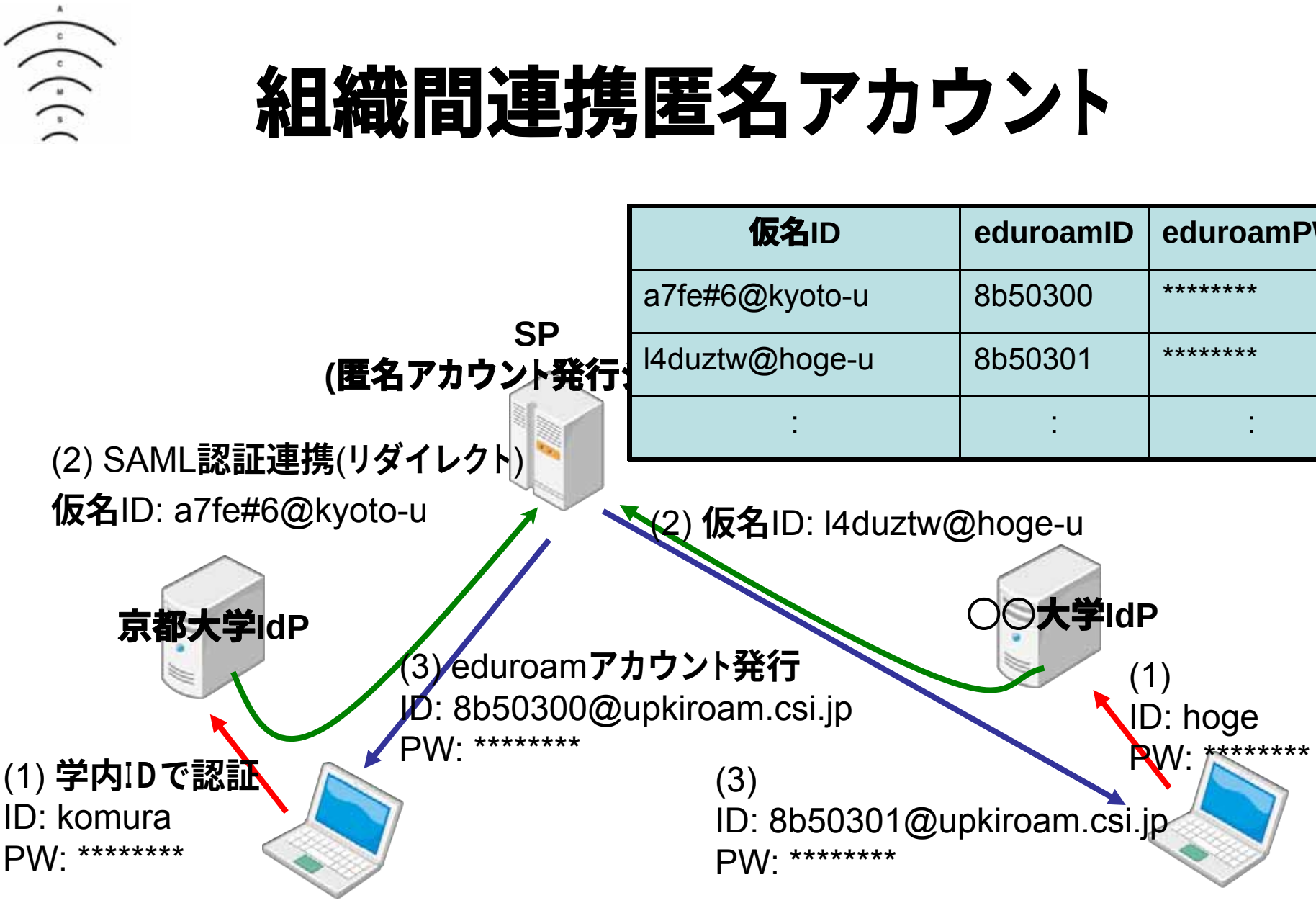
- **他のIDで認証したあと匿名アカウントを発行**
- **ID体系 (案)** : YMDSLNN@upkiroam.csi.jp

[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]
[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]
[NN]	**同一発効日内での通し番号** [00〜zz]

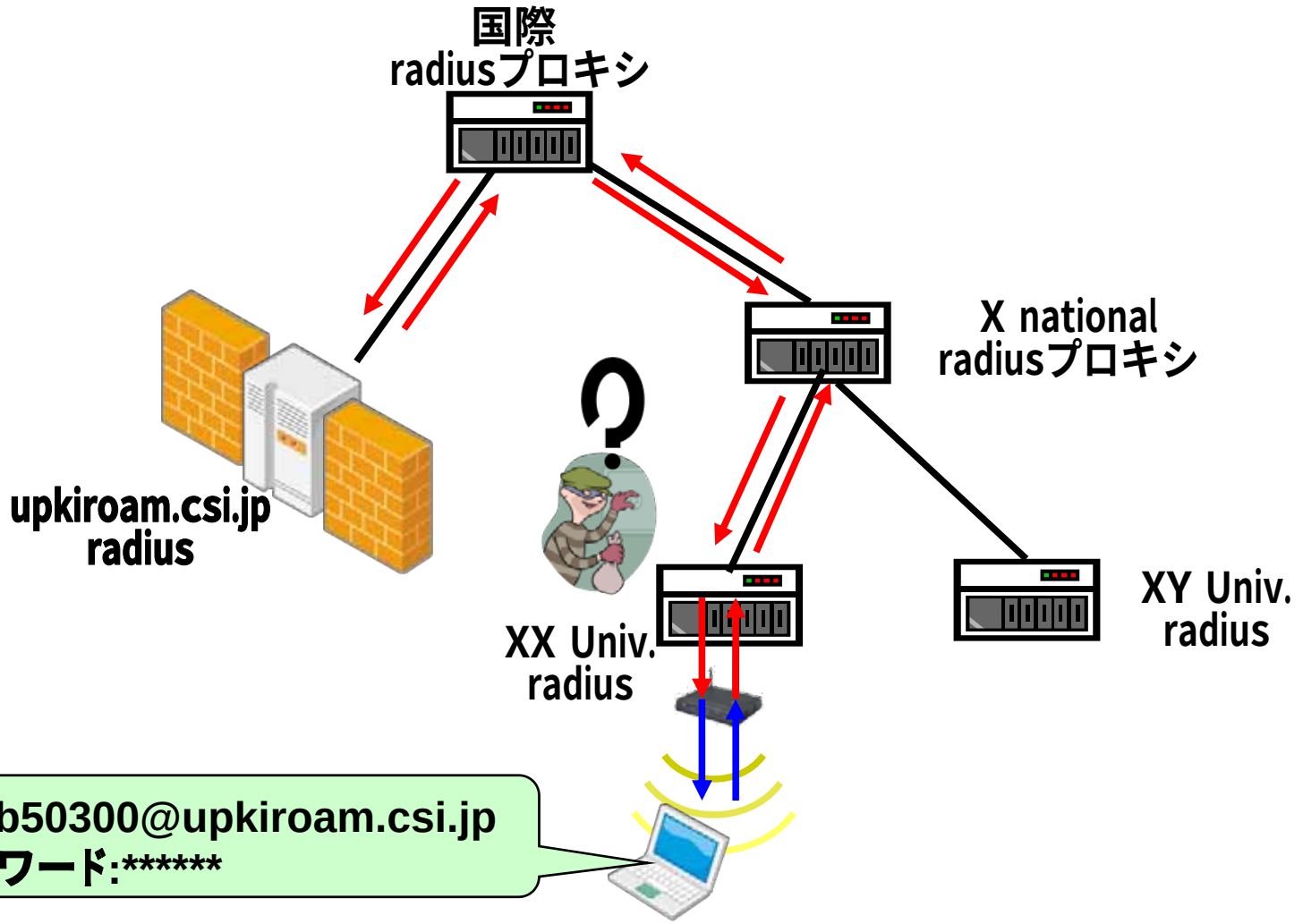
匿名アカウントの例: **8b50300@upkiroam.csi.jp**
(2008年11月5日発行、当日から3日間有効)

組織間連携匿名アカウント

仮名ID	eduroamID	eduroamPW
a7fe#6@kyoto-u	8b50300	********
l4duztw@hoge-u	8b50301	********
:	:	:

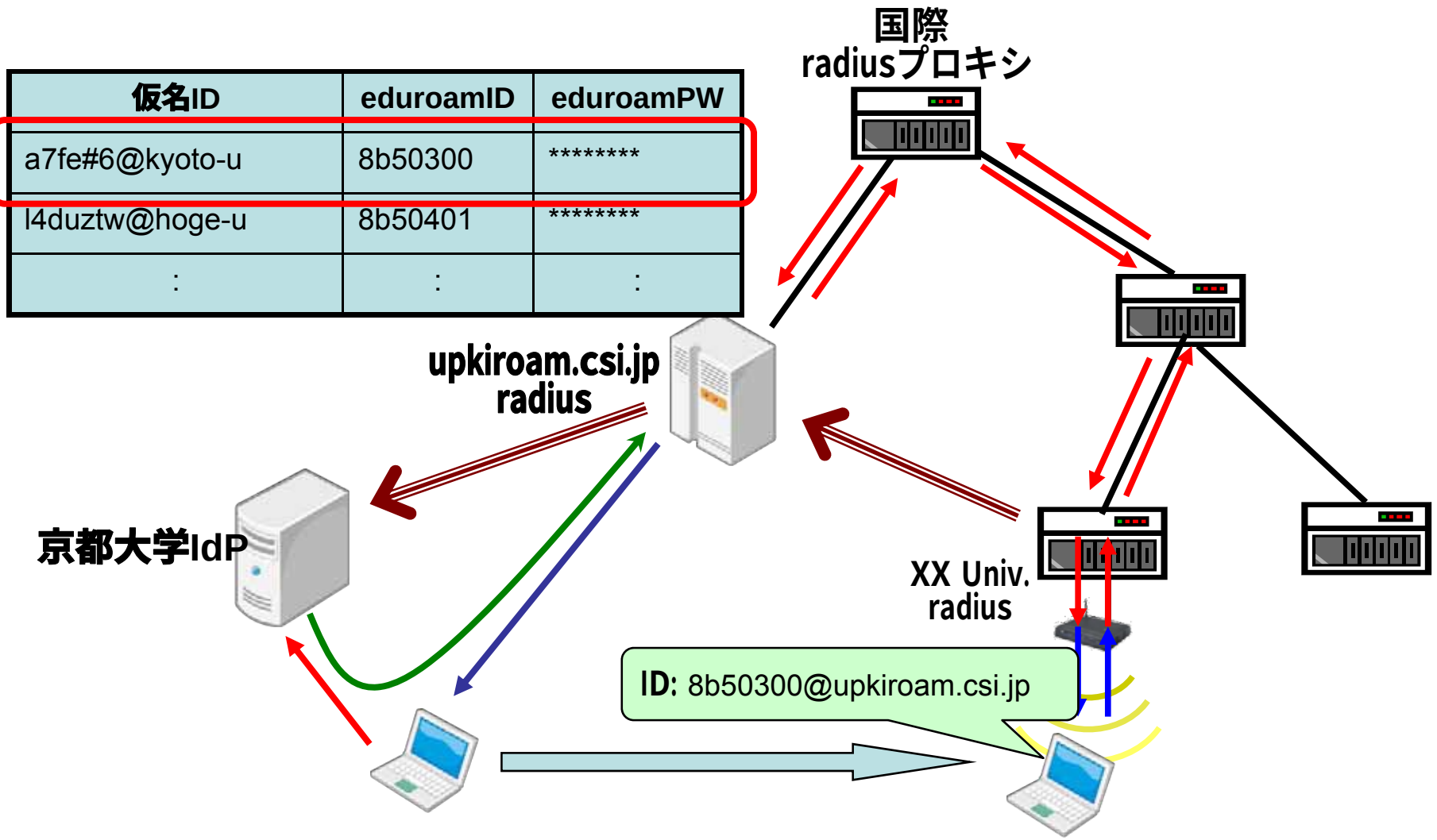


組織間連携匿名アカウントによる認証



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	8b50300	********
l4duztw@hoge-u	8b50401	********
:	:	:



まとめ

- 無線ＬＡＮを安全に利用するための二種類の通信方式
  - eduroam　　802.1X認証 + radius連携
  - みあこネット　　VPN (PPTP, ssh, OpenVPN...)
- 京都大学での導入事例の紹介
  - ポリシーの異なる複数の無線LANサービス
  - マルチSSID、tagged-VLAN 対応基地局
- 無線認証用アカウント
  - ゲストアカウント
  - ロケーションプライバシーを意識した使い捨てアカウント