

京都大学における無線LANサービスの展開

小椋 正道^{*1} 四方敏明^{*1} 古村隆明^{*2} 岡部寿男^{*2}

^{*1} 京都大学情報環境部情報基盤課

^{*2} 京都大学学術情報メディアセンター

内容

- × みあこネットおよびeduroamについて
- × 無線LAN基地局の紹介
- × 無線基地局の設置
- × 上流ネットワークの設計
- × 仮名アカウント発行システム

みあこネットについて（歴史）

MIAKO（Mobile Internet Access in KyotO）

- × 2002年5月誕生
- × ～2005年3月31日 実証実験
- × 2005年4月～2008年3月31日
 - + 支援企業や団体や個人による運営
 - + 実証実験時代の基地局は 京都アイネット株式会社が継承
- × 2008年4月～ 各団体による自律分散型運用の開始
 - + 京都大学
 - + 国立病院機構 京都医療センター

<http://www.miako.net/>

みあこネット方式

外部からの訪問者に無料でネットワークを貸すことを前提とした
無線インターネットサービス方式

× 基地局提供者側からみると

- + VPNプロトコル(暗号化＋認証)だけを通させる無線基地局を一般に公開
 - × MS PPTP
 - × OpenVPN
 - × SSH (secure Shell)
 - × POP/SSL (TCP 995), IMAP/SSL (TCP 993), SMTP/SSL (465)
- + VPNプロトコル以外は通さないで、SPAM発信や掲示板荒らしなどはない
⇒ 認証に伴うリスクや管理コストなし

× 利用者側からみると

- + 基地局側での認証手続きなく直接自分の持っているVPNサーバに接続
⇒ VPNで暗号化されるので盗聴やなりすましのリスクなし

× 単に部外者が基地局に接続しただけでは何も出来ない。

- + VPN接続していなければ、「みあこCAN(利用方法案内ページ)」にしか接続出来ない。

VPNの普及が課題

eduroamについて

- ✕ ヨーロッパ生まれのローミング方式。大学や研究機関で用いられている。
- ✕ 自組織で発行されたアカウントをeduroam参加他機関でもシームレスに利用出来る仕組み。各組織がRADIUSサーバ及びRADIUSプロキシサーバを用いることで、他機関からの利用でも、所属組織のRADIUSサーバに中継される。認証はIEEE802.1xで行われ、EAP-TLSやEAP-TTLS やEAP-PEAP等を用いることで、認証と暗号化における安全性を確保している。
- ✕ 参加機関: 500程度。日本では特に東北大学が積極的に進めている。
- ✕ 参考URL: <http://www.eduroam.jp/>
<http://www.eduroam.org/>



Legend for Asia Map:
Green: Countries that have joined
Blue: Countries in the process of joining
Yellow: European Root

>>> ASIA MAP



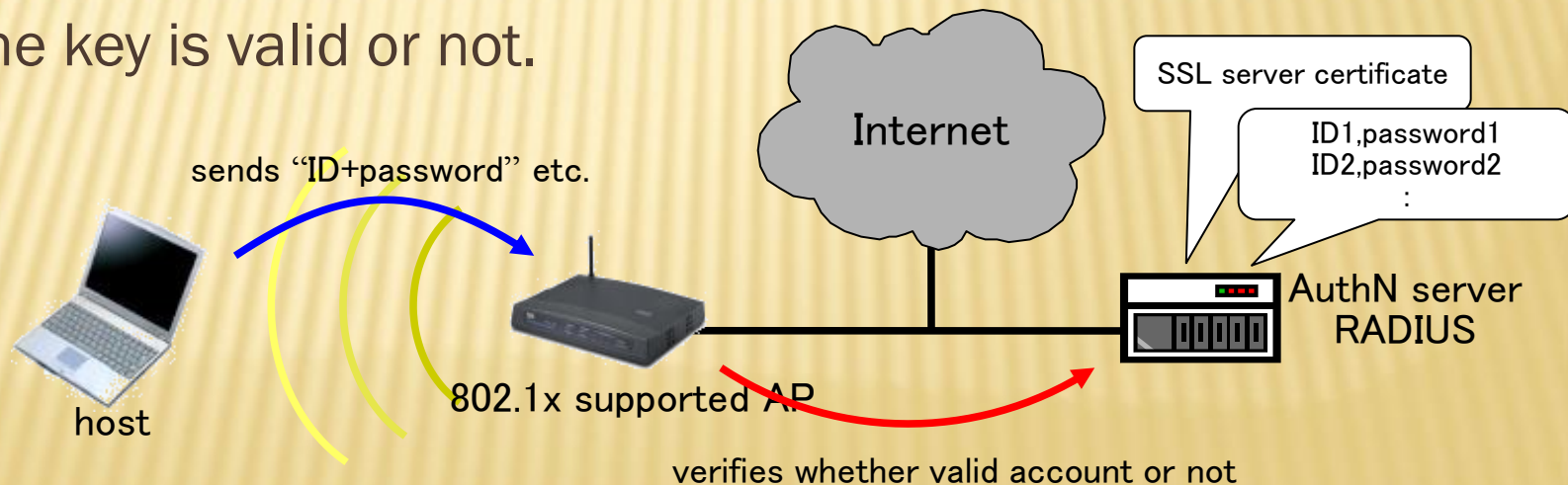
Legend for Europe Map:
Green: Countries that have joined
Blue: Countries in the process of joining
Yellow: Asian Root

>>> EUROPE MAP



AUTHENTICATION MECHANISM OF EDUROAM (1/2)

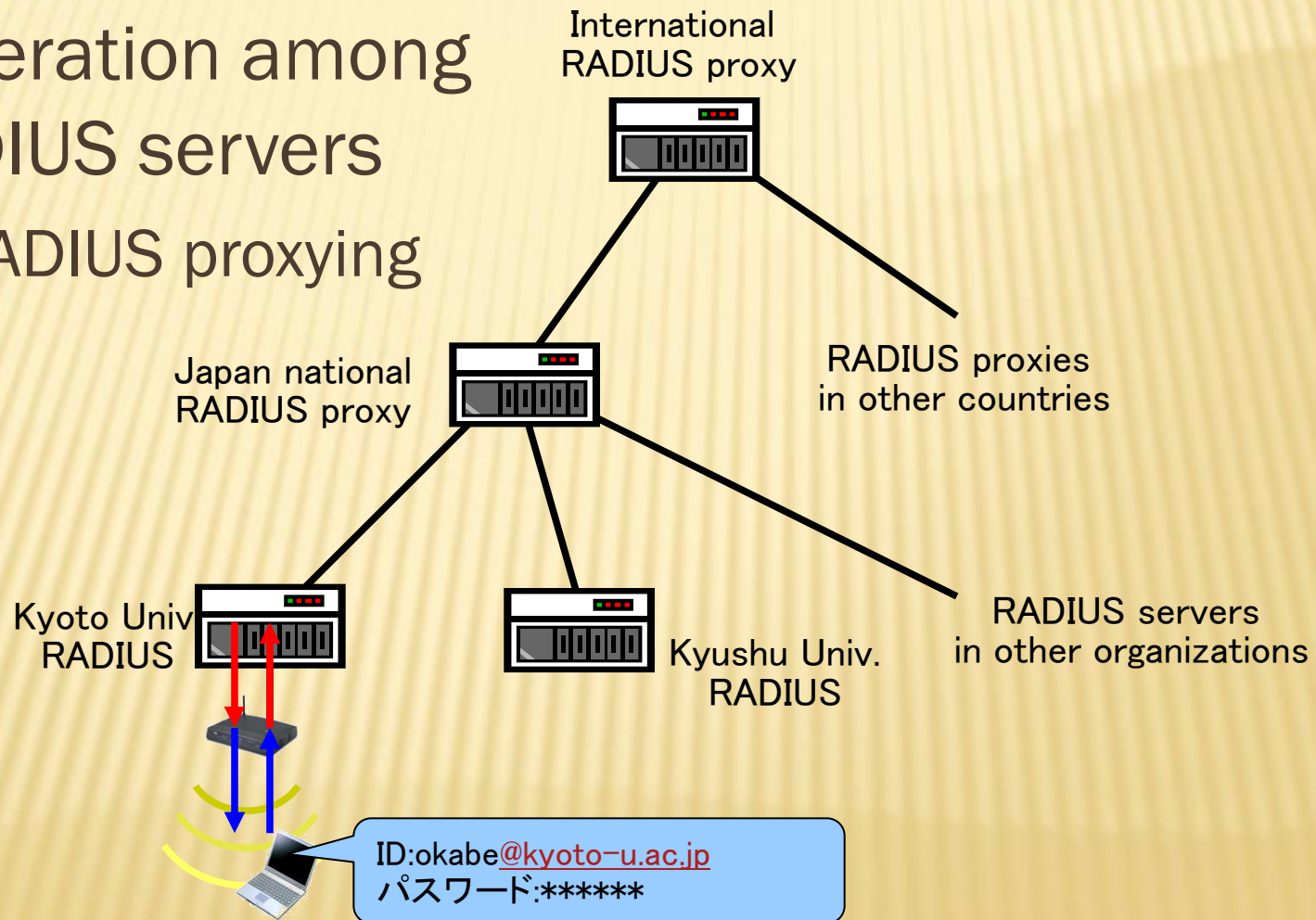
- ✗ Utilization of IEEE 802.1x
 - + Authentication is performed at wireless access points (AP)
 - + A Client host sends either “ID+password” or “SSL client certificate” as the authentication key
 - + AP asks the authentication server via RADIUS whether the key is valid or not.



AUTHENTICATION MECHANISM OF EDUROAM (2/2)

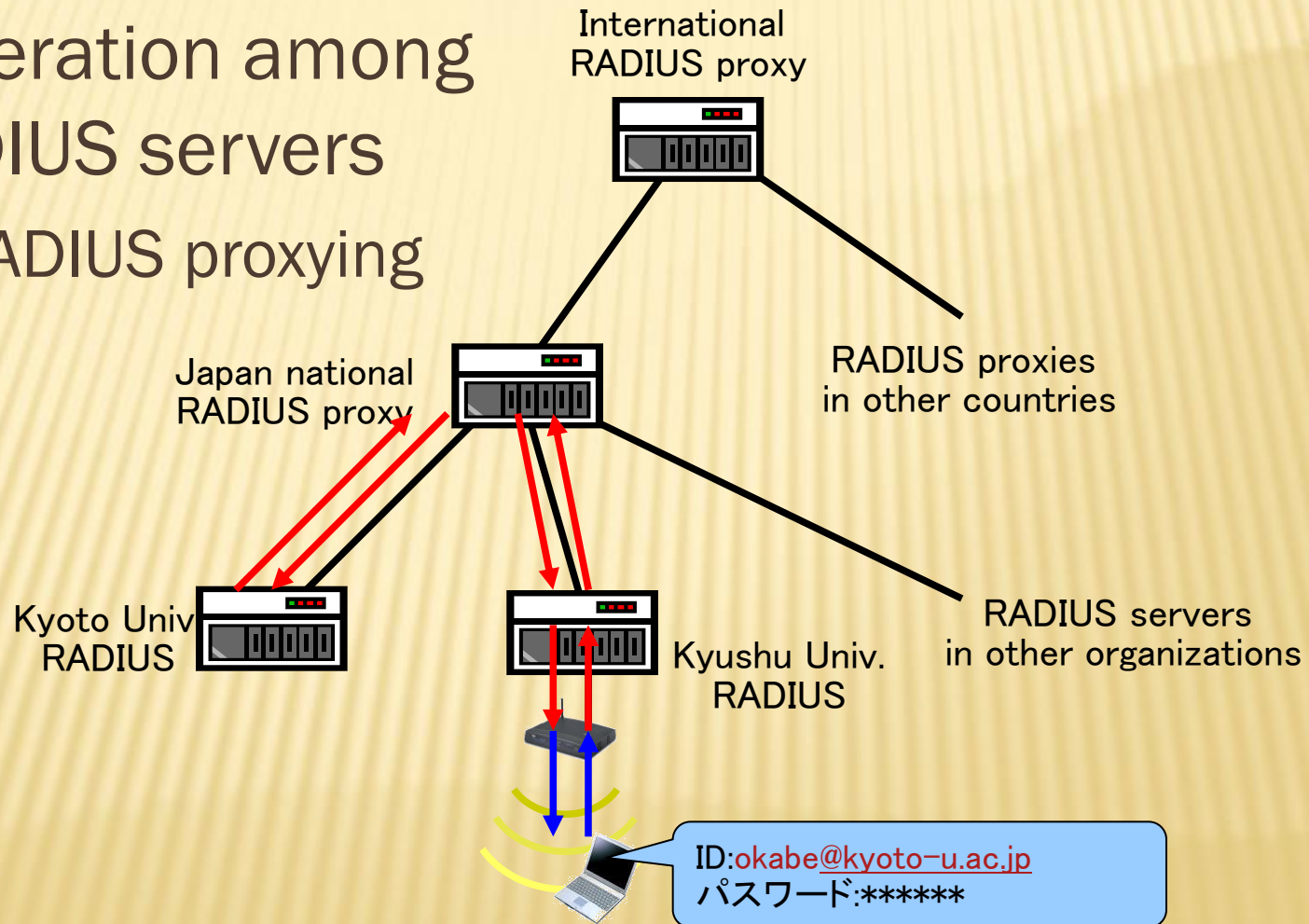
✕ Federation among
RADIUS servers

+ RADIUS proxying



AUTHENTICATION MECHANISM OF EDUROAM (2/2)

- ✕ Federation among RADIUS servers
- + RADIUS proxying



EDUROAM対応無線LAN アクセスポイントの展開

- ✕ 全学のアクセスネットワーク整備と連携して無線LANアクセスポイントを展開
 - + アライドテレシス TenQ AT-TQ2403
 - + 現在200台以上稼働
(H21年度内に400台超の予定)
 - + Eduroam方式とMIAKOネット方式の併用
 - ✕ 学内学外者も利用可
(学内LANとは別のアドレスブロックを割り当て)



今回設置している基地局

(アライドテレシス社製 AT-TQ2403)



* 約400台を全学的に配置予定

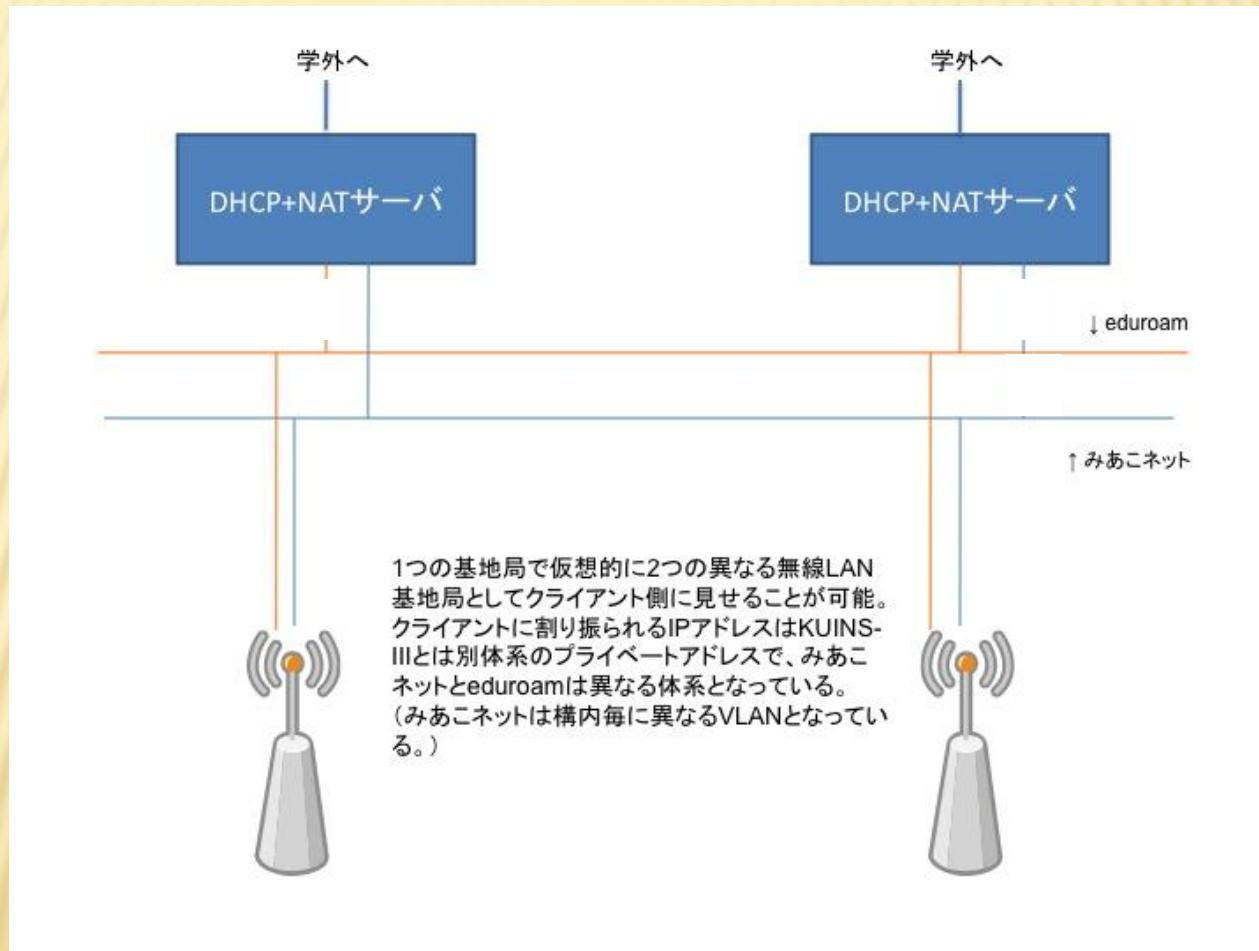
アライドテレシス社製AT-TQ2403の特徴

×「アクセスポイント選定のポイント」

(eduroam.jp 技術資料より)

- + IEEE802.1x認証に対応 (eduroam標準)
- + WPAまたはWPA2以上の無線暗号化対応 (eduroam推奨)
- + マルチSSIDおよびマルチVLANに対応
 - みあこネット方式とeduroam方式の同時サポート
 - × 複数SSIDのビーコンをアナウンスできる
 - × マルチSSID機能においてSSIDやサブネットの主副を問わず必要な暗号化の設定ができる

VWN(*)機能を利用した基地局運用イメージ



((*) Virtual Wireless Networkの略)

インターネットに接続するための仕組み

- ✕ NAT経由で学外に接続(eduroam、みあこネット共通)
 - + クライアントはDHCPサーバ(NATサーバと兼用)により、プライベートIPアドレスが割り当てられる。
 - ✕ みあこネットはVPN接続必須
 - + 京大構成員は、学外からのアクセス用のPPTPサーバやポートフォワード専用SSHサーバに接続
 - ✕ Eduroamは学内LANとは別のグローバルIPアドレスを確保
 - + 学内LANのIPアドレスで学内onlyのアクセス制限をかけているWebページ等を外来者に見せたくない
 - + とりあえず、昔使っていたクラスCアドレス /23を転用、しかし...
- ⇒ eduroam用にNIIで確保したIPアドレス領域を、SINET3 L2VPNサービスを用いて全国で利用可に！

基地局の設置条件

(工事費が確保できなかったので...)

- ✕ 原則として、教職員が常駐している
- ✕ 不在時には施錠されている

→ 条件を満たす候補: 事務室や図書室

これらの部屋に設置し、隣接エリアにも漏れ電波が届くように調整を行う。

(図書室の場合は、図書室内で完結するような配置にしているケースもある。)

基地局の設置条件(II)

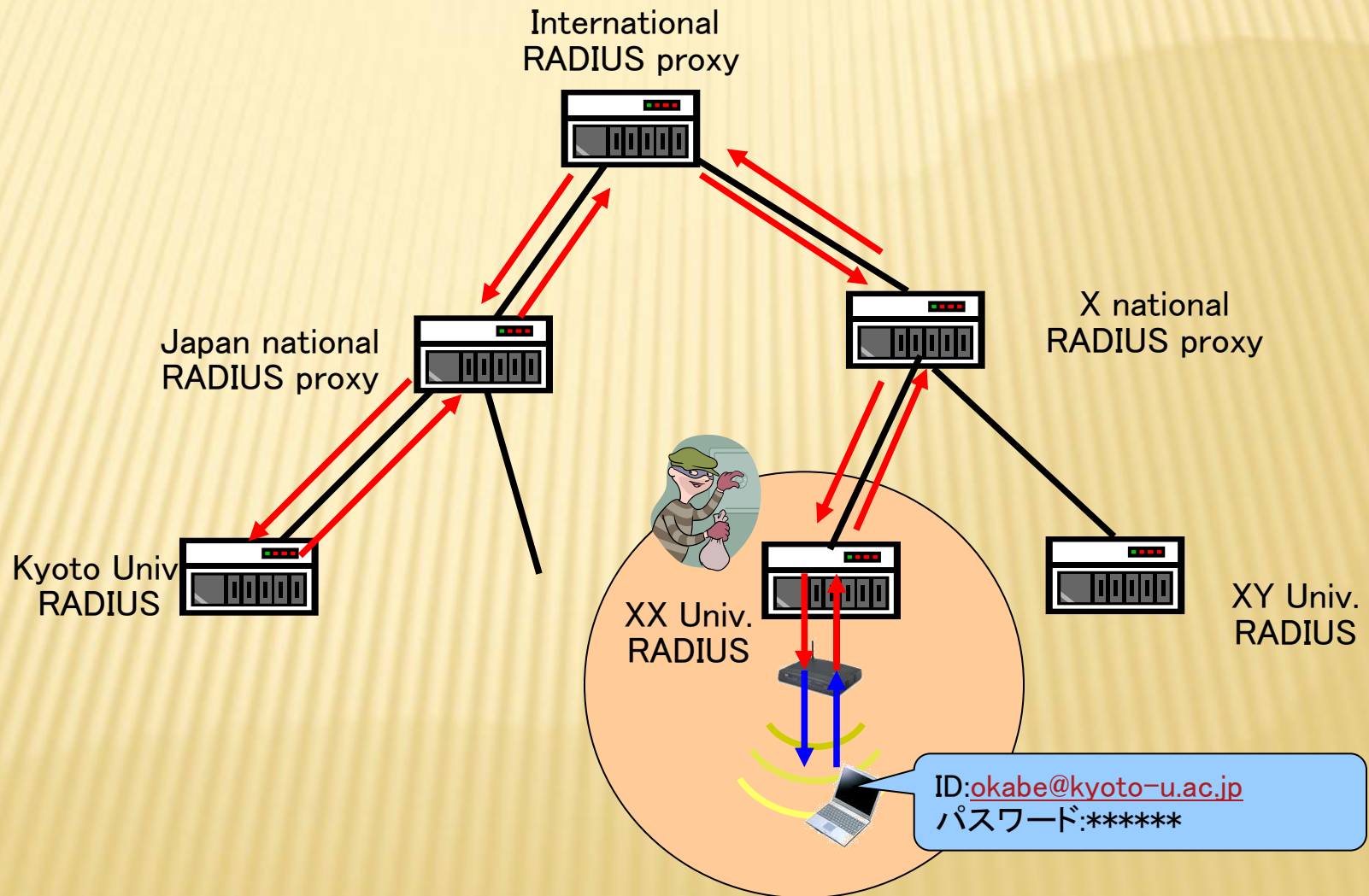
- ✕ 事務室や図書室以外でも、同等程度の物理的セキュリティを確保出来れば、会議室等にも設置している。
- ✕ 補助的対策として、無線LAN基地局とLANケーブルを接続するコネクタに金具＋南京錠で固定し、盗難対策とした。



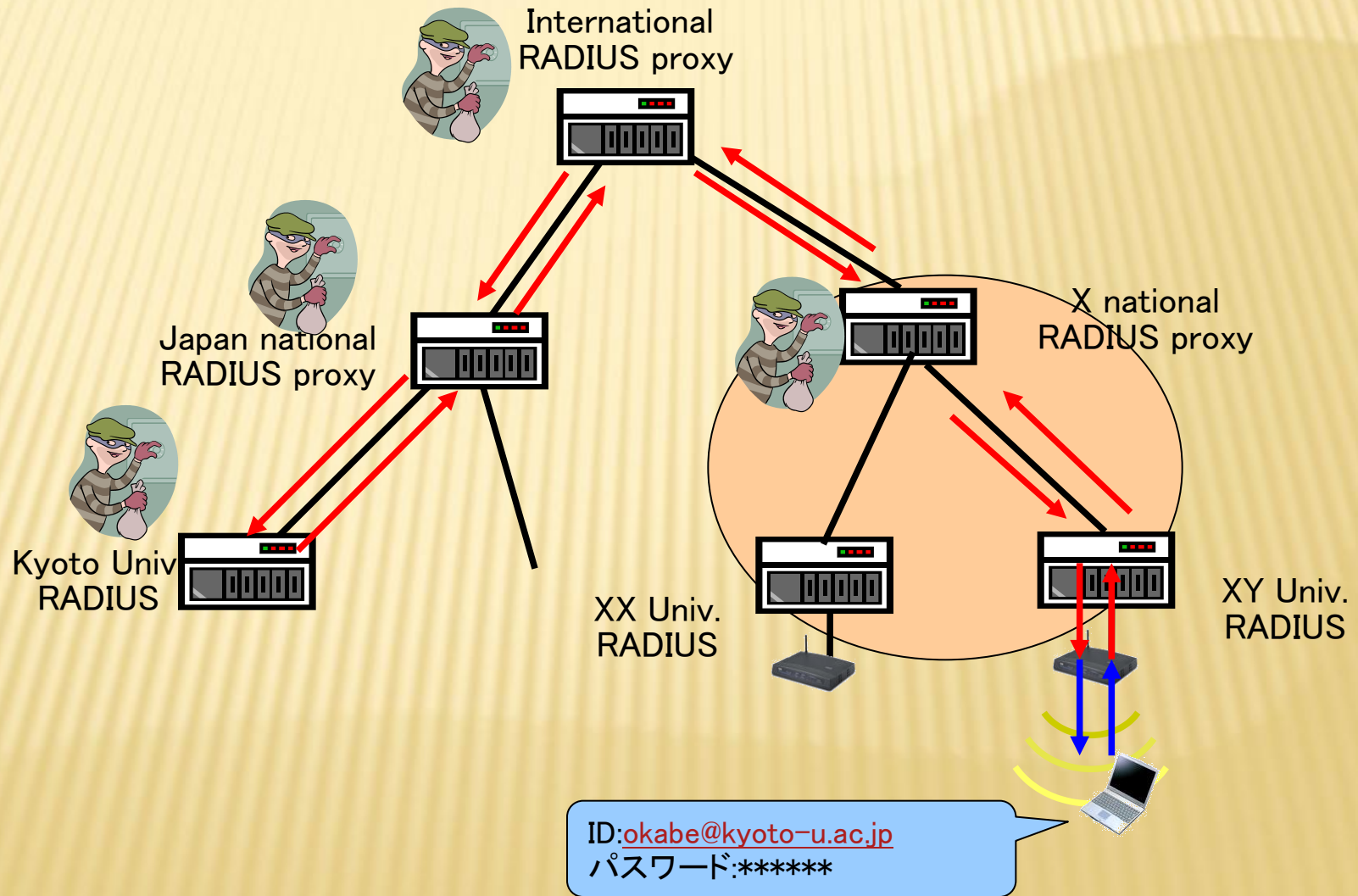
IEEE802.3af
Power over Ethernet (PoE)対応

マグネット付

LOCATION PRIVACY ISSUES IN ROAMING ACCESS



LOCATION PRIVACY ISSUES IN ROAMING ACCESS



EDUROAM仮名アカウント発行システム

- × ロケーションプライバシーを守る
eduroam用仮名アカウント発行システム
 - + eduroamの認証に利用できるアカウントを発行
 - + 他大学のIdPとも連携
 - × 他大学の利用者にもアカウント発行可能
 - + アカウントに利用者を識別できる情報を含まない
 - + アカウント発行時に有効期限を設定可能
 - × 1日～数ヶ月の範囲で選択可能
 - × 出張時などに使い捨て利用を想定

仮名EDUROAMアカウント

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]

- ✖ 各大学IdPで認証し、個人の識別情報を受け渡さずSSO連携
 - + 本システムへ必要以上の情報を送らない
 - + 本システムで発行したアカウントで不正なアクセスが行われた場合、ログから認証したIdPを抽出してIdPへ問い合わせ

[ログアウト](#)

ログインID: a0030703

登録日: 2009-05-11

申請内容

利用開始日時: 2009-05-11 00:00:00+09:00

利用終了日時: 2009-05-12 23:59:59+09:00

利用可能期間: 2日

eduroamアカウント

eduroamアカウント: 95B0202@eduroam.kyoto-u.ac.jp

eduroamパスワード: d1v8gC

まとめ

- ✕ 学内構成員に対しては、利用しやすく安全な無線LAN環境を提供
 - ✕ 学外者に対しては、みあこネット方式およびeduroamにより、自組織のアカウントで接続可能な環境を提供
 - + 学術認証フェデレーションによる仮名アカウント発行サービスを準備中
- 今後も未設置部局に対して展開を行う予定である。

謝辞

最後に、本整備は一部、国立情報学研究所委託事業
「最先端学術情報基盤の構築に関する研究開発と調査」
による。