

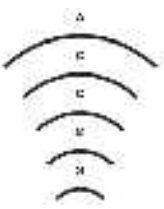
IdP,SPの構築状況

シングルサインオン実証実験中間報告会@NII (2008/11/10)

京都大学学術情報メディアセンター

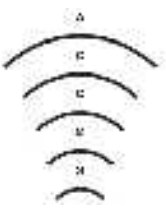
古村隆明

<komura@media.kyoto-u.ac.jp>



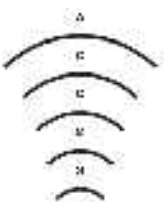
IdP, SP 構築状況

- NIIへの metadataの登録完了
 - IdP: idp1.kuins.kyoto-u.ac.jp
 - SP: eduroam.kuins.kyoto-u.ac.jp
- 利用ハードウェア・OS
 - CPU: Intel Xeon 2.00GHz x 4
 - RAM: 4GB
 - CentOS 5.1
 - Xenによる仮想環境上にIdPとSPを構築（それぞれ CentOS 5.1）
- IdPに登録されたアカウント情報は動作試験用
- SPのWebアプリケーションは作成中
 - eduroam 用匿名アカウント発行システム
- 別系統のIdPとSPを準備中
 - 2008年12月にメディアセンタに導入される仮想マシンサービスを利用
 - 将来的に学内統合LDAP内のデータと連携を想定



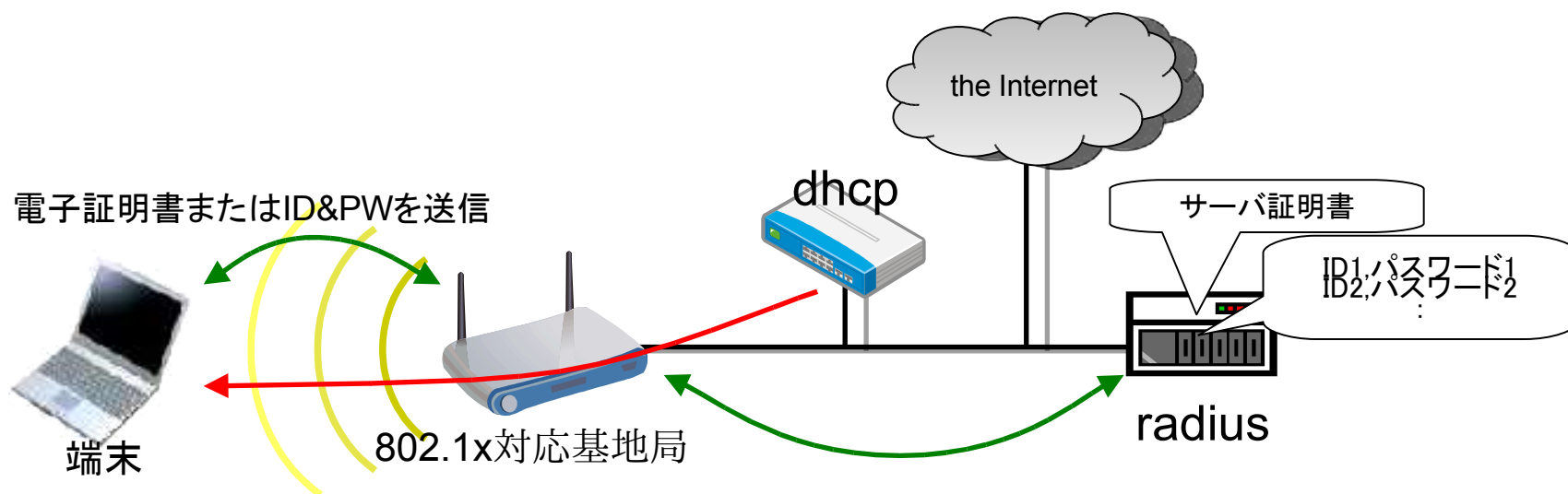
SP用アプリケーション(開発中)

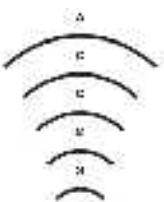
- eduroamアカウント発行システム
 - ロケーションプライバシーを守る匿名アカウント
 - アカウント発行時に有効期限を設定可能
 - 1日～数ヶ月の範囲で選択可能
 - 出張時などに使い捨て利用を想定
 - 他大学のIdPとも連携し、
他大学の利用者に対してもアカウント発行



eduroamの認証方式

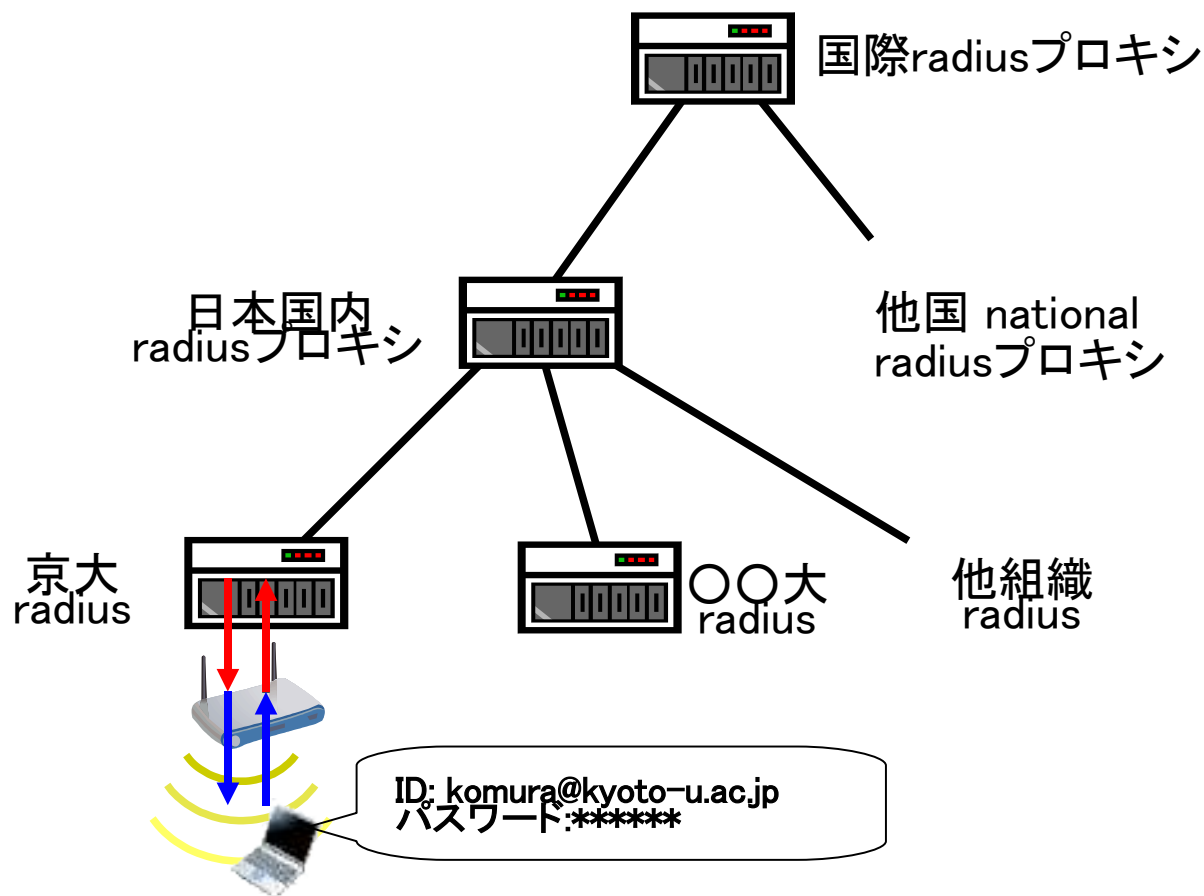
- 802.1x認証
 - radiusサーバを利用した認証
 - サーバ証明書で、認証サーバ(radius)の正真性を確認
 - クライアント証明書またはID&PWで、利用者を認証

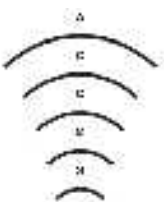




eduroamのローミング

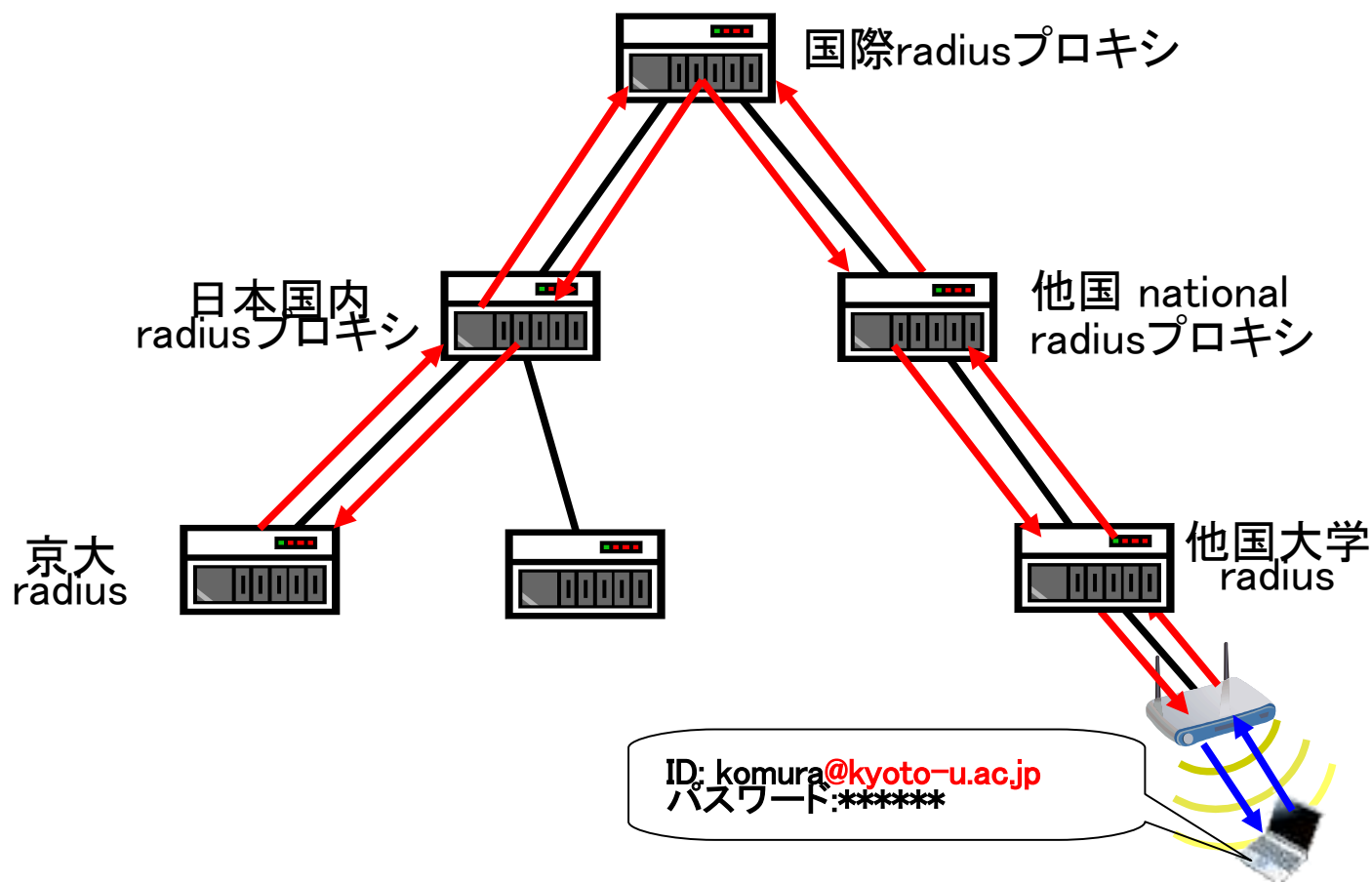
- 自組織での利用の場合

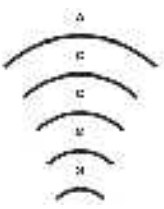




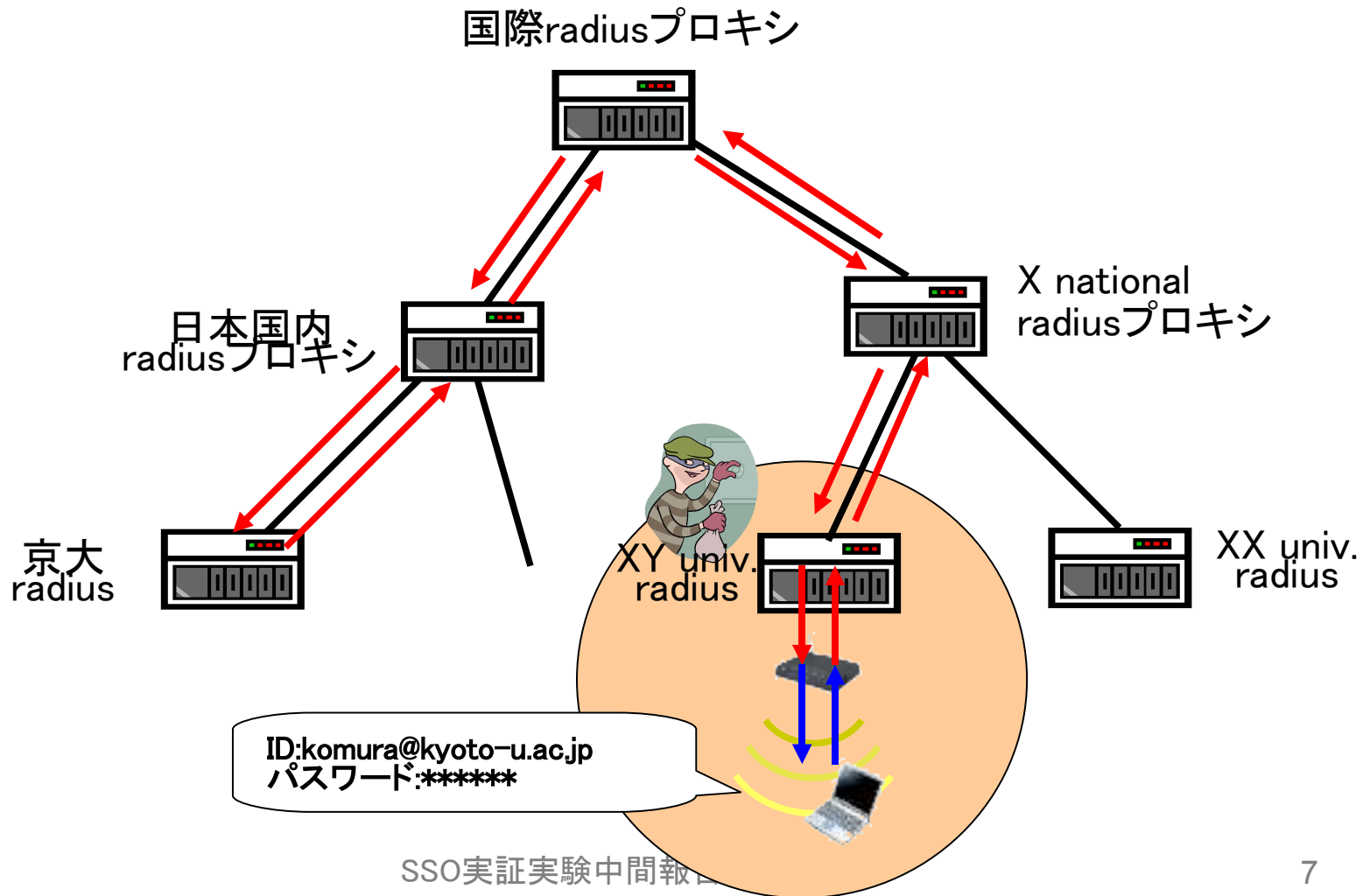
eduroamのローミング

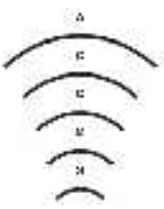
- 国外から利用する例



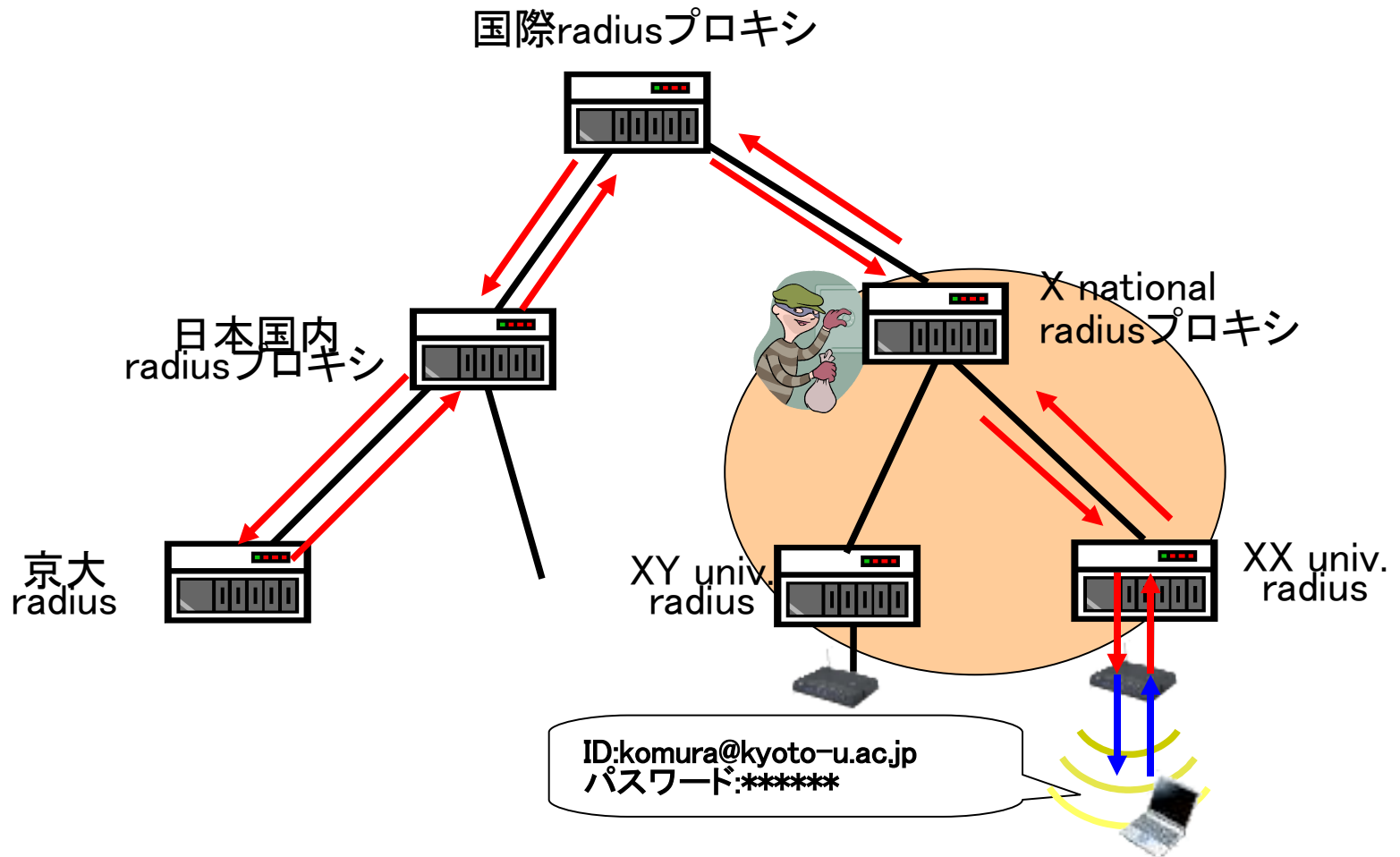


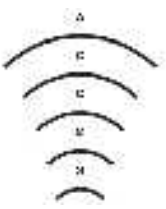
ロケーションプライバシー問題(1)





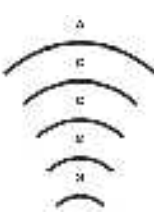
ロケーションプライバシー問題(2)





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
- 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



匿名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

組織間連携匿名アカウント

認証チケット	eduroamID	eduroamPW
a7fe#6@kyoto-u	8b50300	*****
l4duztw@hoge-u	8b50301	*****
:	:	:

SP
(匿名アカウント発行)

(2) SAML認証連携(リダイレクト)

認証チケット: a7fe#6@kyoto-u

(2) 認証チケット:l4duztw@hoge-u

京都大学IdP

〇〇大学IdP

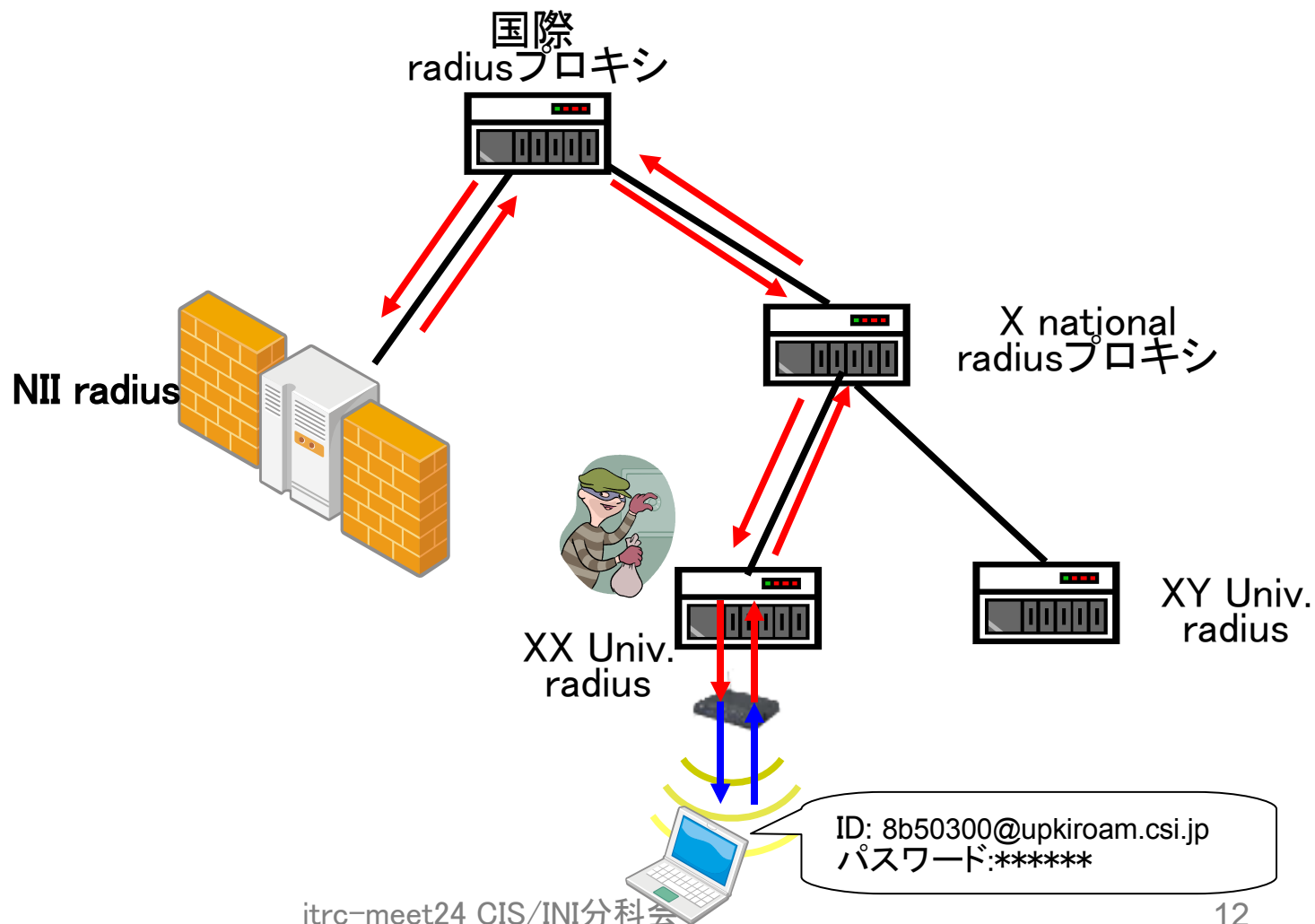
(3) eduroamアカウント発行
ID: 8b50300@upkiroam.csi.jp
PW: *****

(3)
ID: 8b50301@upkiroam.csi.jp
PW: *****

(1)
ID: hoge
PW: *****

• 学内IDで認証
ID: komura
PW: *****

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

認証チケット	eduroamID	eduroamPW
a7fe#6@kyoto-u	8b50300	*****
l4duztw@hoge-u	8b50401	*****
:	:	:

