

SAML連携による eduroam仮名アカウント発行システムの実装

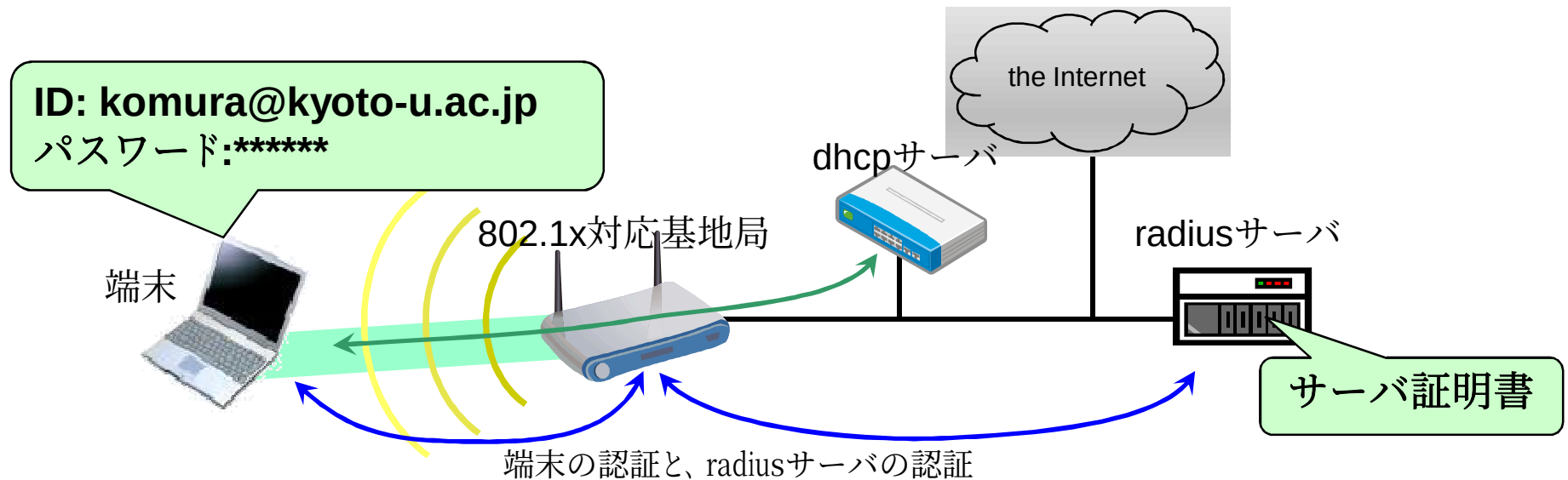
京都大学学術情報メディアセンター

古村隆明

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

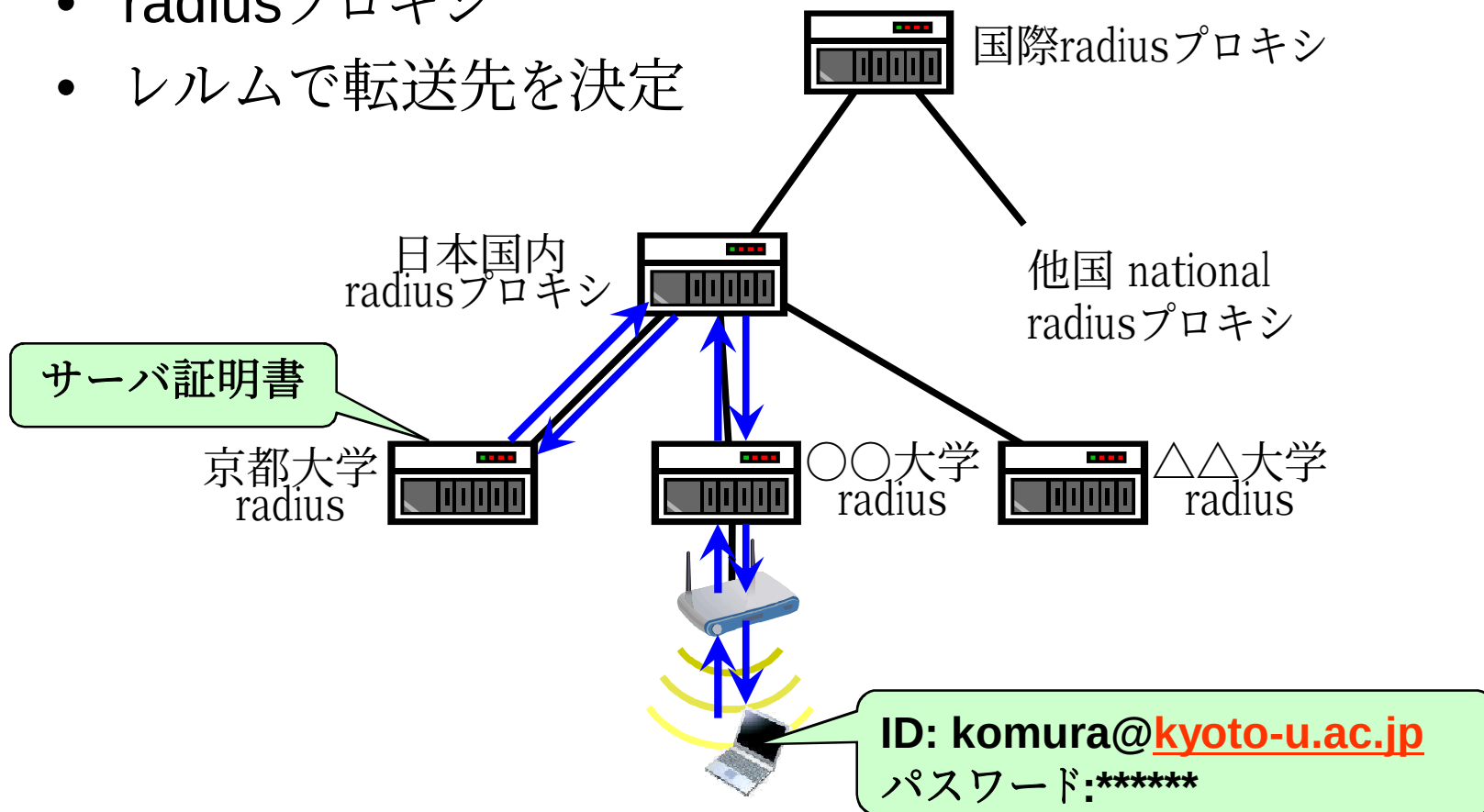
eduroamの認証方式

- 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

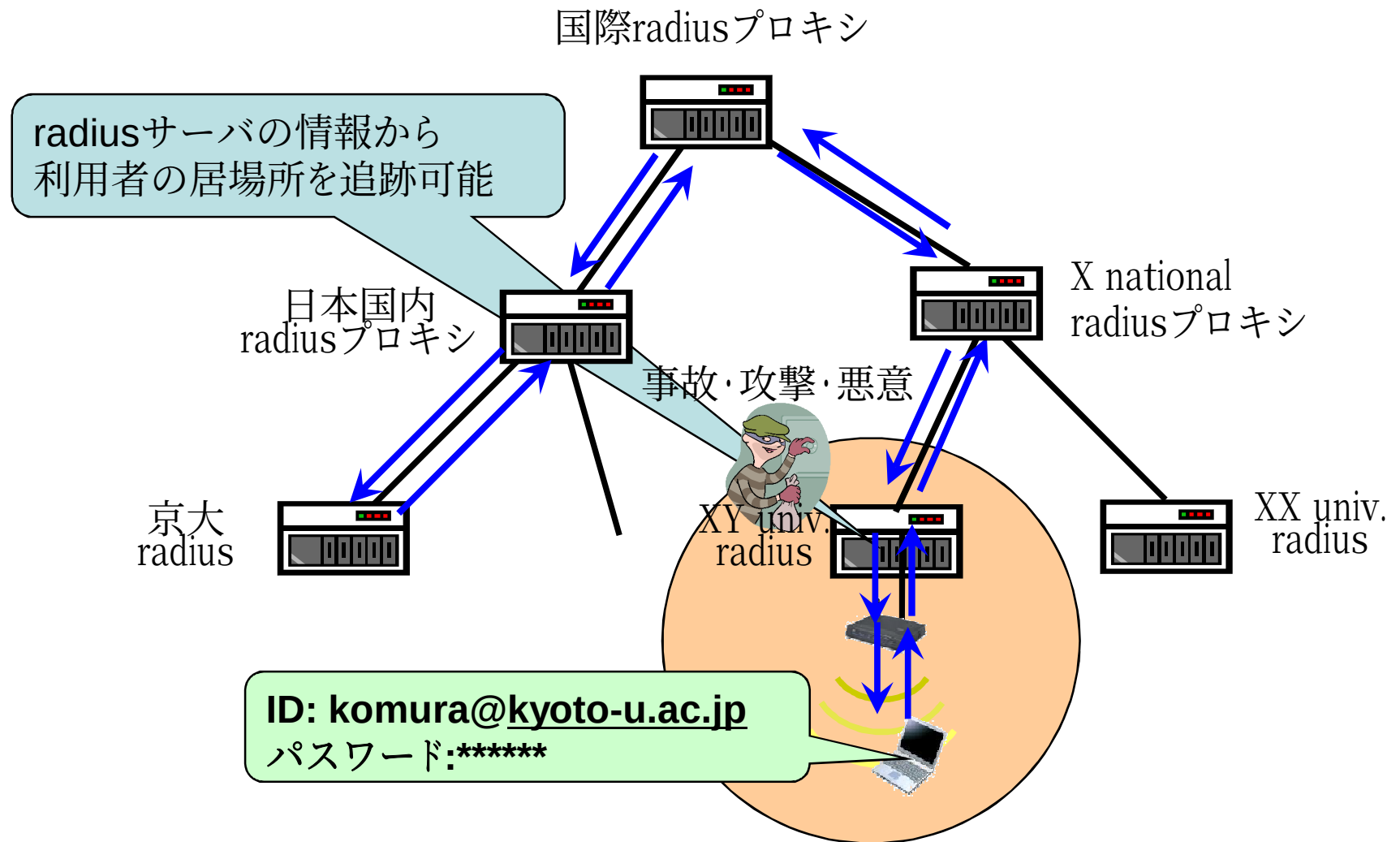


eduroamのローミング

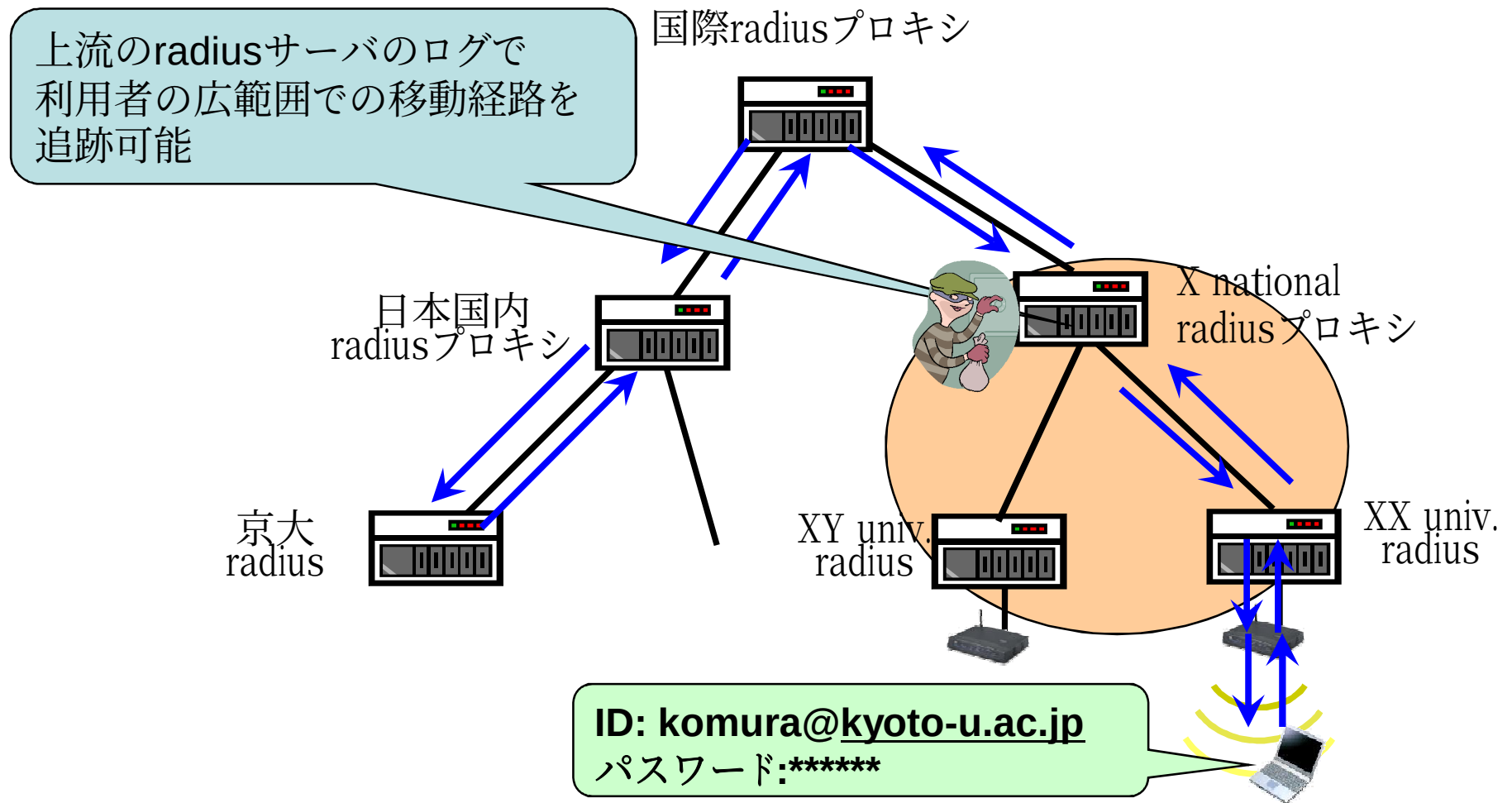
- 他組織から利用する例
- radiusプロキシ
- レルムで転送先を決定



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
仮名アカウント

- 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
仮名アカウント

使い捨て仮名アカウント

- 本IDで認証したあと仮名アカウントを発行
- 仮名ID体系

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]

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

組織間連携仮名アカウント

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

SP
(仮名アカウント発行システム)

(2) SAML認証連携(リダイレクト)

連携ID: a7fe#6@kyoto-u

(2) 連携ID: l4duztw@hoge-u

京都大学IdP

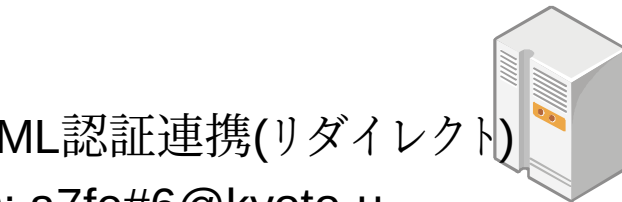
〇〇大学IdP

(1) 学内IDで認証
ID: komura
PW: *****

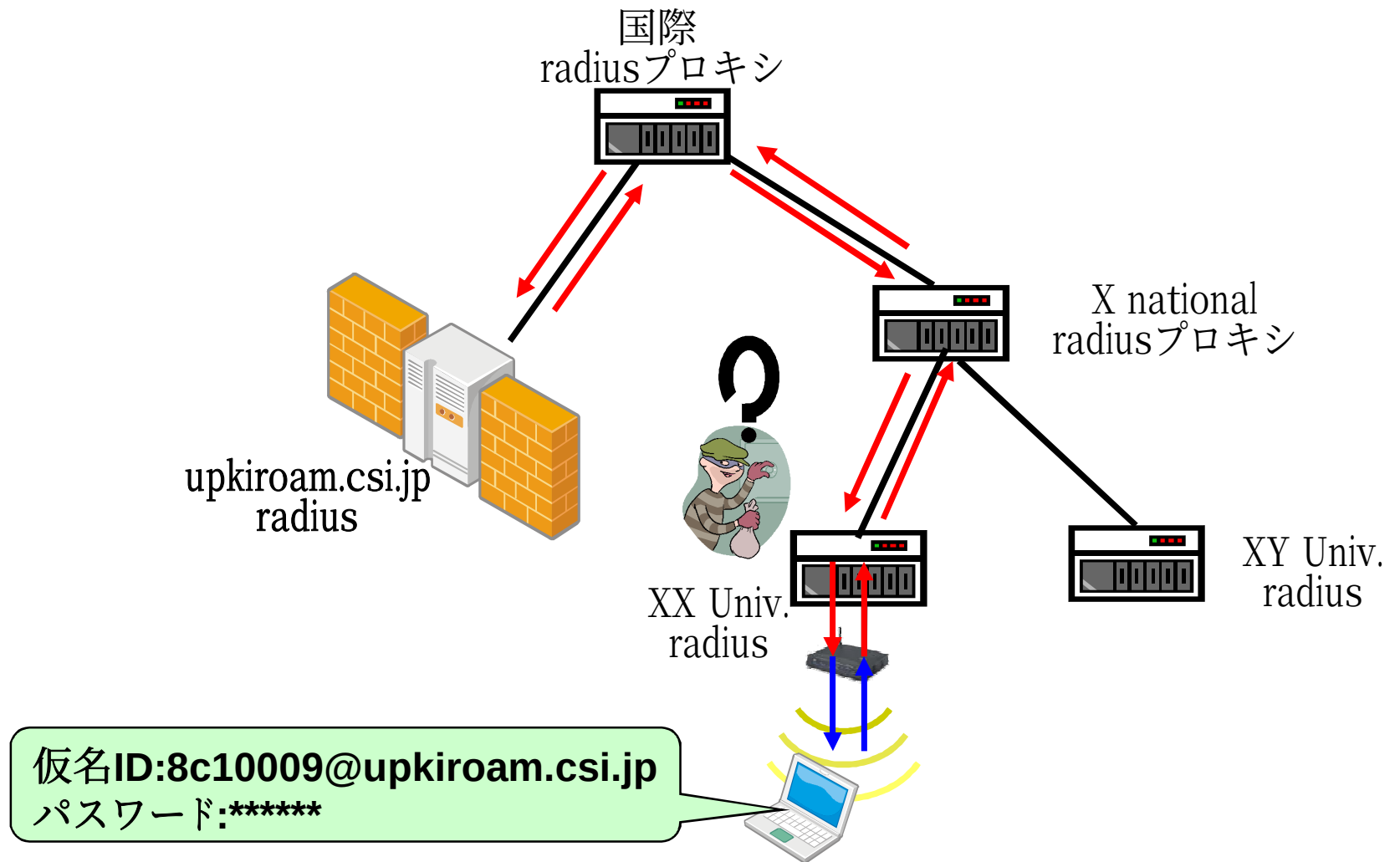
(1)
ID: hoge
PW: *****

(3) eduroamアカウント発行
仮名ID: 8c10009@upkiroam.csi.jp
PW: *****

(3) eduroamアカウント発行
仮名ID: 8c10103@upkiroam.csi.jp
PW: *****



組織間連携仮名アカウントによる認証



組織間連携仮名アカウント利用時の インシデントレスポンス

