eduroam環境構築のためのTips

中村 素典 / 国立情報学研究所

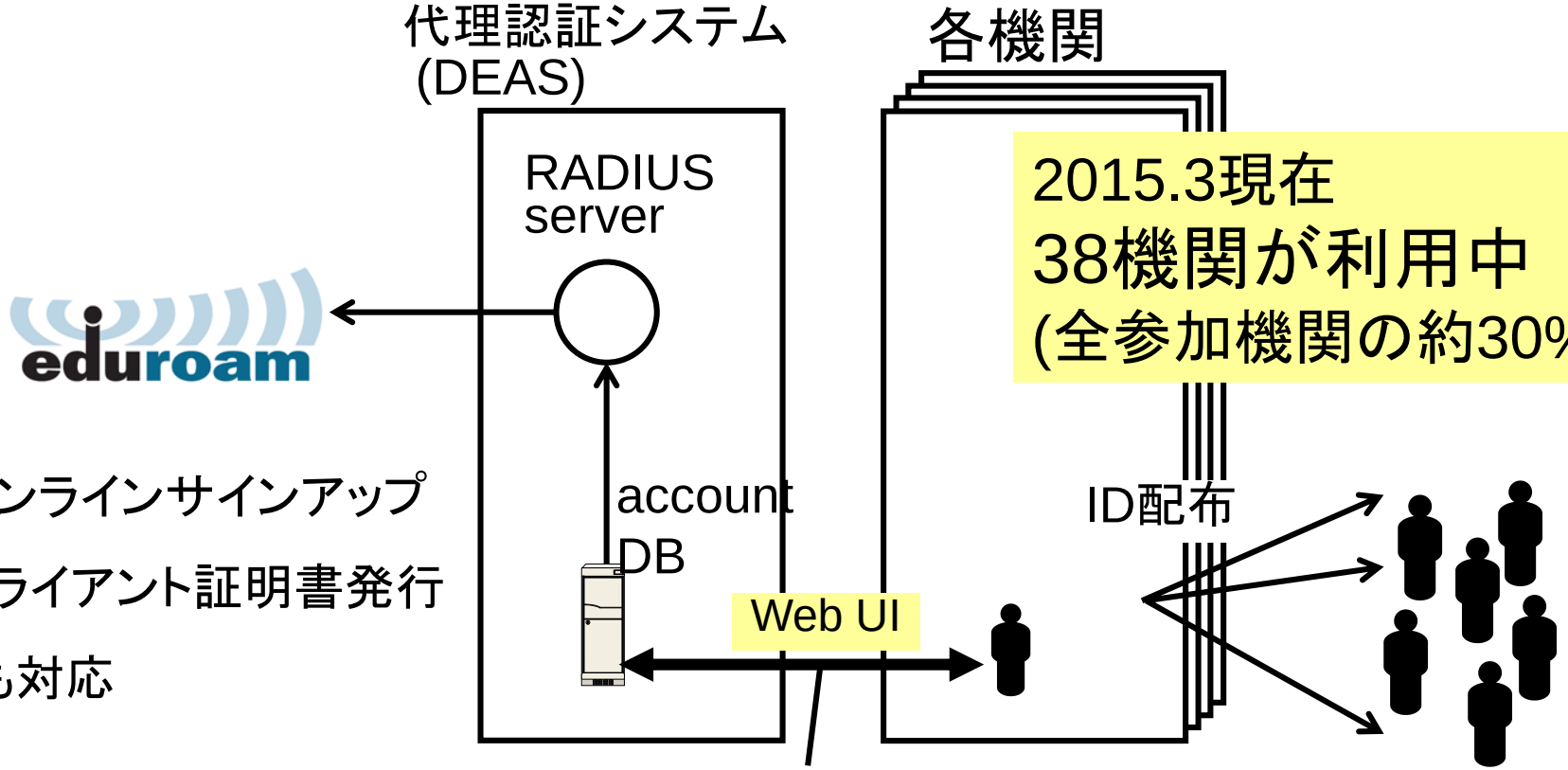
NII学術情報基盤オープンフォーラム2017

eduroamへの参加方法（訪問先での利用）

- 自機関構成員向けアカウントの準備（3つの選択肢）
  1. Radiusサーバを構築・運用（クラウド利用可）
     - 学内アカウントをそのまま利用することが可能

     原則はこちらです
  2. 代理認証サービスを利用
     - eduroam専用アカウント発行サービス
  3. 仮名アカウント発行サービス（学認連携）を利用
     - 学認用のIDを用いてeduroam用一時アカウントを発行

2. 代理認証システム (2008年～)



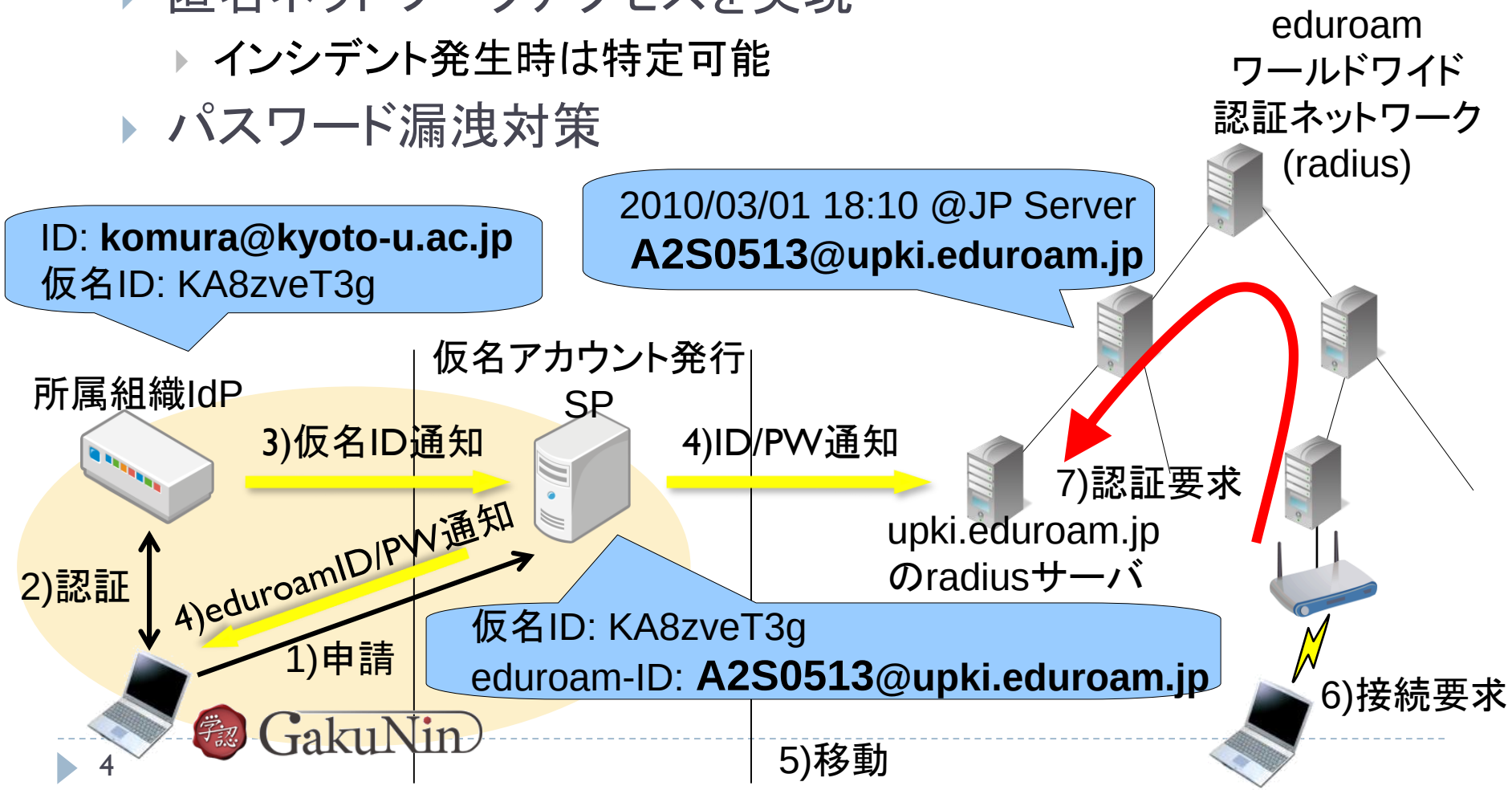
- オンラインサインアップ
- クライアント証明書発行

にも対応

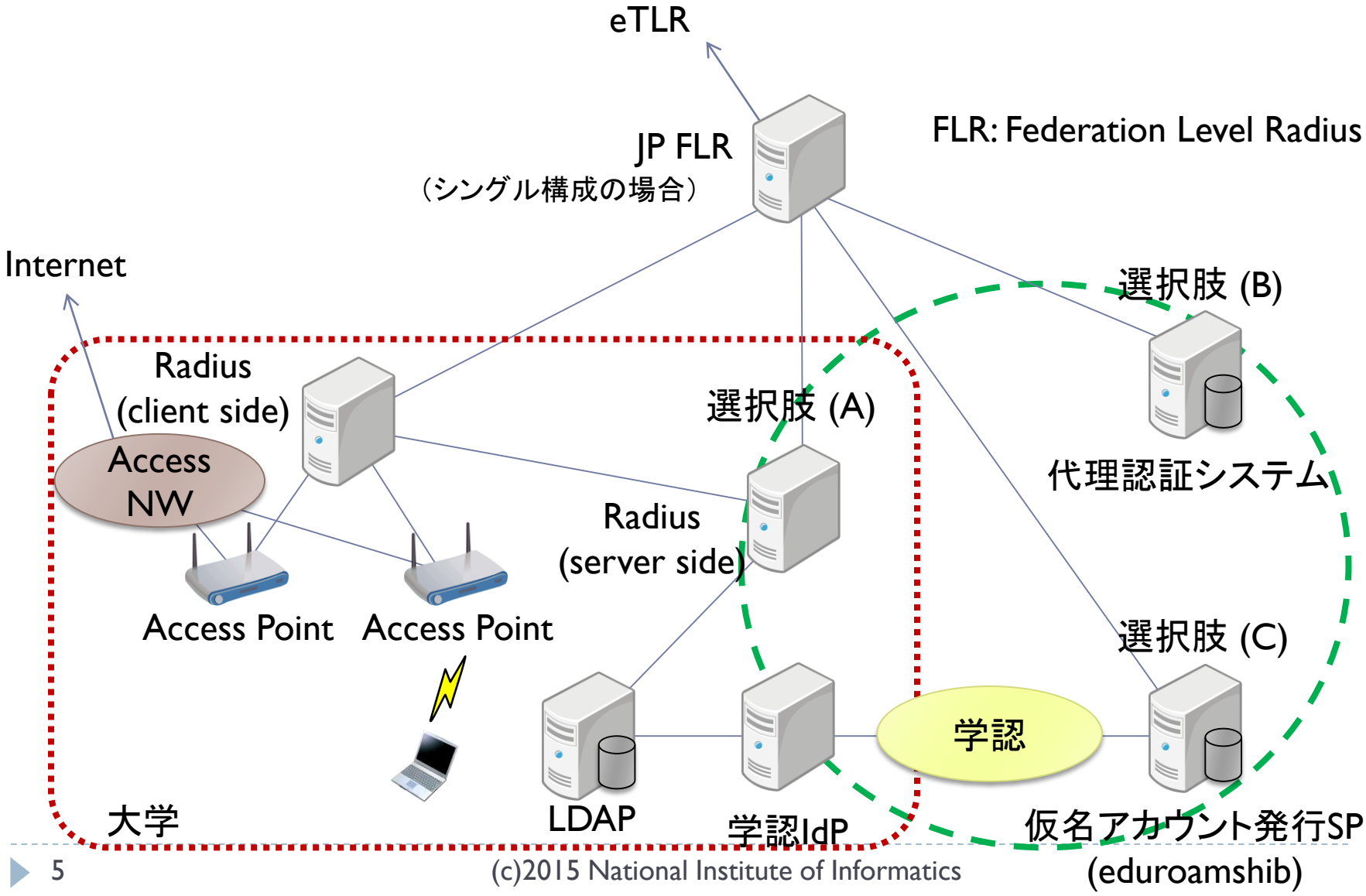
- ID取得だけで、管理者がアカウントをバルク請求・発行可能
- ゲスト用アカウントの発行も可能
- 会議向け期間限定eduroamアカウント発行用にも利用(2014.7～)

3. eduroam仮名アカウント発行サービス

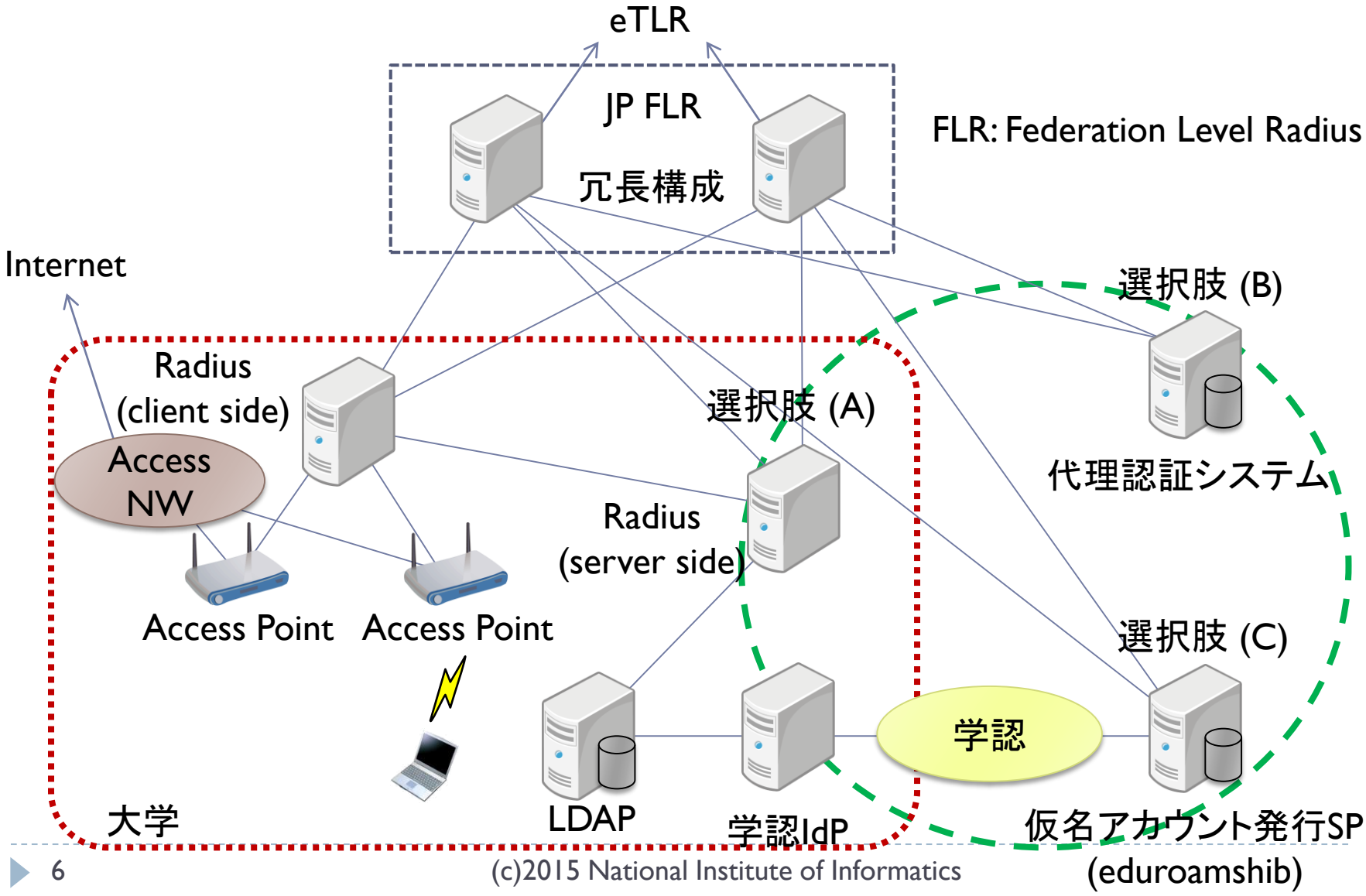
- シボレス認証し、eduroam一時アカウントを発行
  - 匿名ネットワークアクセスを実現
    - インシデント発生時は特定可能
  - パスワード漏洩対策



大学におけるeduroamシステム構成例



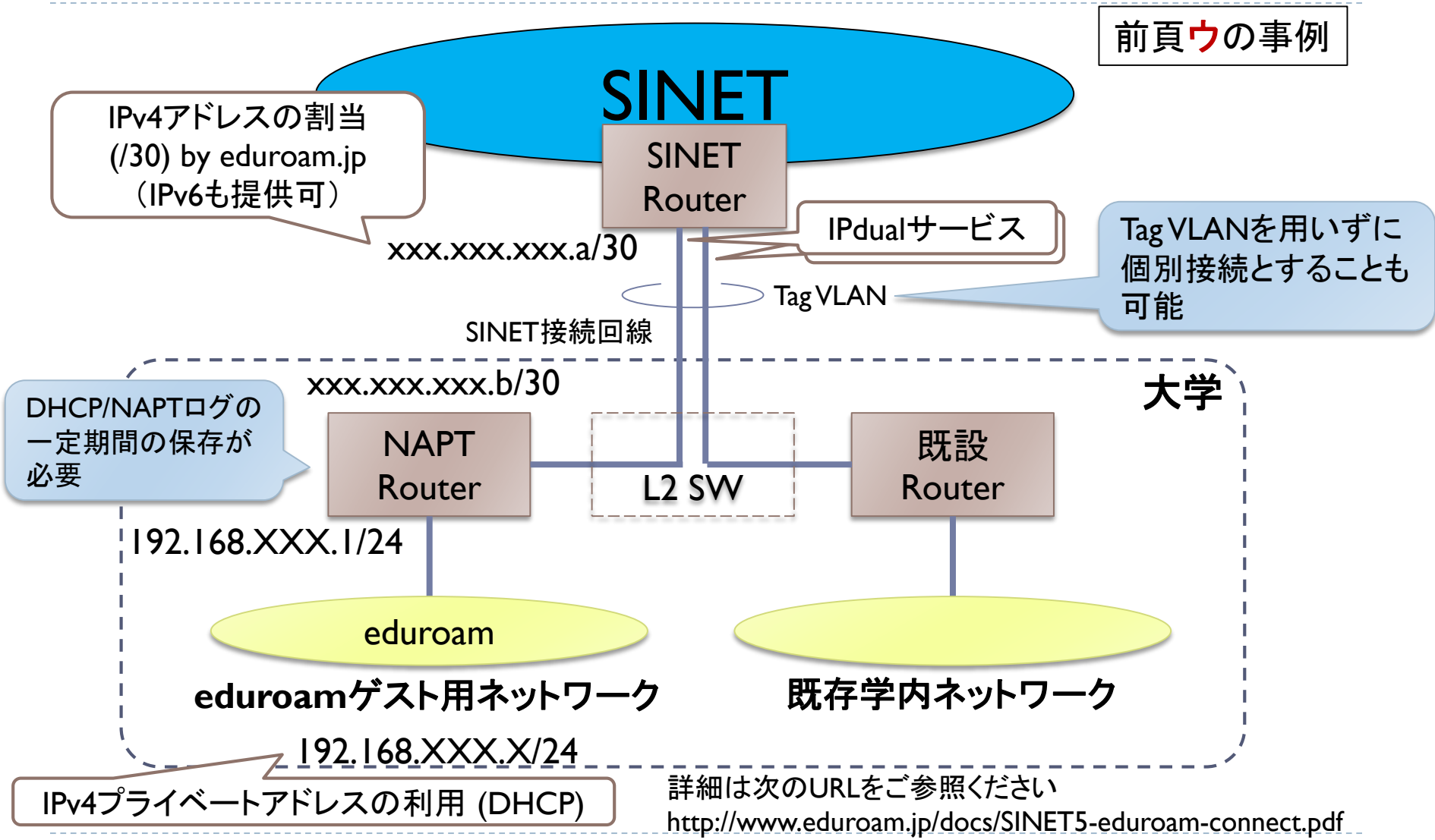
大学におけるeduroamシステム構成例



eduroamへの参加方法（ネットワークの提供）

- 無線アクセスネットワーク（アクセスポイント）の準備
  - ゲスト用に用いるIPアドレスの主な選択肢
    （多くの機関では、機関内からのアクセスのみを許可し、ゲストには同じIPアドレスを利用させたくないという要求がある。）
    - 自機関が保有するIPアドレスブロックを利用（eduroam用のIPアドレスブロックの切り出し）
    - 新たにIPアドレスブロックを取得して利用
      - ア) 新たに商用回線等を導入し、その回線に付随するIPアドレスを利用
      - イ) 既接続回線提供者(SINET含む)からIPアドレスブロックの割り当てを受け、当該回線で利用
        （ただし、最近はIPv4で十分なサイズのIPアドレスブロックの割り当てを受けることは非常に困難）
      - ウ) eduroam.jp から、SINET 接続による eduroam サービス提供用として割当を受けたアドレス(IPv4/IPv6)を利用
        （前項のIPアドレスブロック割り当て手続きの簡略化。ただし、接続形態を規定。詳細は次ページ参照）

SINETによるeduroamアクセスネットワーク収容のイメージ（SINET5でも継続提供）



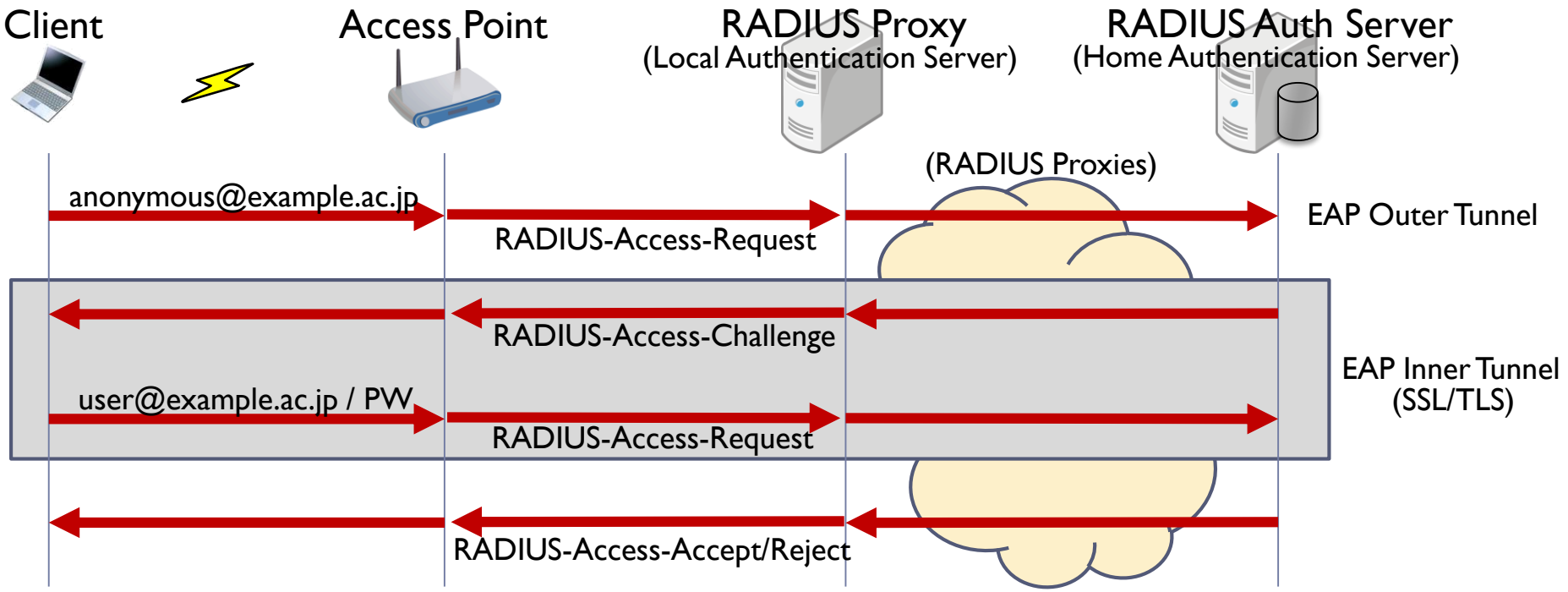
詳細は次のURLをご参照ください
http://www.eduroam.jp/docs/SINET5-eduroam-connect.pdf

さらに進んだ設計に向けての検討

- 認証VLAN
- クライアント証明書の活用

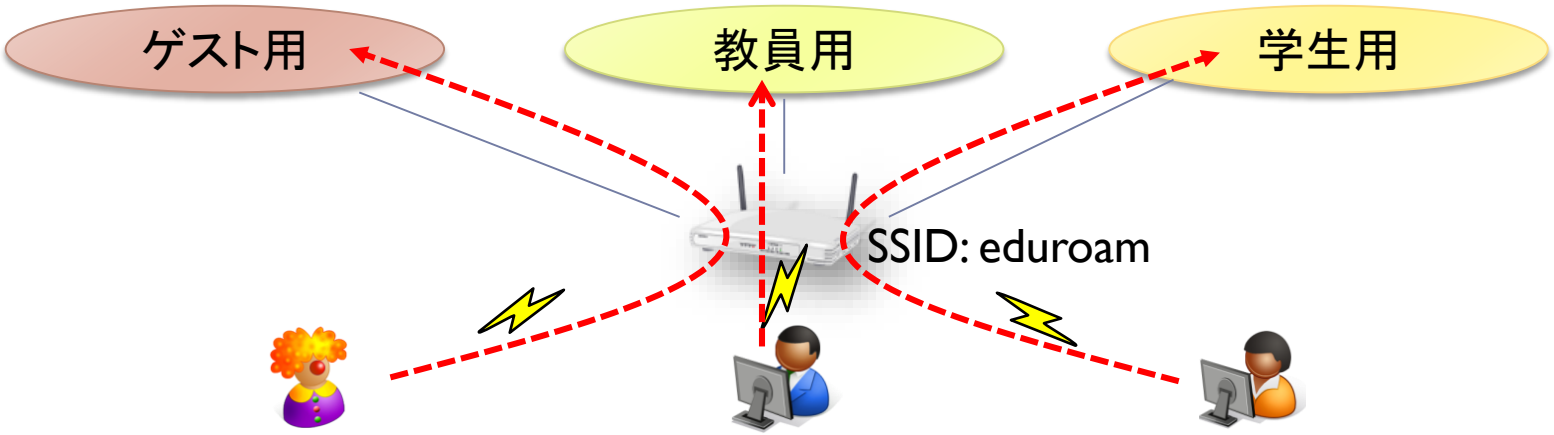
EAP/RADIUSにおける認証の手順（概略）

- 認証はトンネルの中で行われる
  - 本当のユーザIDはトンネルの中を流れるため、プロキシではわからない
  - パスワード認証もトンネルで守られる（サーバ証明書の確認が重要）
    - サーバ証明書は認証を行うRADIUSサーバのものであることを確認
      - 訪問先が変わっても、サーバ証明書がかわることはない
  - プロキシでは、トンネルの中を流れる情報を改変・追加できない



認証VLAN （ダイナミックVLAN）

- 同一SSID (eduroam) を用いて、
  - 大学関係者とゲストで接続先のVLANを変える
    - IPアドレス等によりアクセス可能なリソースの範囲を制御したい
  - さらに、教員と学生とで接続先のVLANを変える



- 「レルム」で接続先のVLANを選択可能
  - 教職員用レルムと、学生用レルムの分離など

RADIUSのVLANに関する属性情報

- Tunnel-Type = 13, VLAN
- Tunnel-Medium-Type = 6, IEEE 802 (802.1x)
- Tunnel-Private-Group-Id = 100 VLAN番号

ユーザ毎に異なるVLAN番号を指定する運用も可能

- 認証に成功したユーザが、指定されたVLANに接続される
  - 他機関のユーザに付随する属性情報は無視
- アクセスポイント製品に応じて、指定すべきパラメータが異なることがあるので注意が必要
  - Tunnel-TypeやTunnel-Media-Typeが省略可だったり

レルムによる識別

- 教職員のレルム
- 学生のレルム
- その他のレルム

```
sites-enabled/default:
post-proxy {
        if ("%{Realm}" == "f.example.jp") {
                update reply {
                        Tunnel-Private-Group-Id = 100
                }
        }
        if ("%{Realm}" == “s.eduroam.jp") {
                update reply {
                        Tunnel-Private-Group-Id = 200
                }
        }
        update reply {
                Tunnel-Private-Group-Id = 300
        }
```

最初に設定した値が有効

eduroamJP認証連携ID発行サービス（新仮名アカウント発行システム）

- レルム（realm）を変更します
  - 旧システムのレルム
    - XXXXXXX@upki.eduroam.jp
  - 新システムのレルム
    - AAAAAAA@DDD.f.eduroam.jp（本人用アカウント）
    - BBBBBBB@DDD.v.eduroam.jp（ビジター用アカウント）
      - DDDは機関名を識別するサブドメイン
        - 機関についての匿名性はなくなります。
- レルム情報を活用することで、ゲストかどうかで、接続先のネットワークを変えることが可能

UPKIクライアント証明書の活用

- eduroamJP認証連携ID発行サービスでのクライアント証明書認証では、プライベートなクライアント証明書を提供。
  - CN=AAAAAAA@DDD.f.eduroam.jp

- パブリックなUPKIクライアント証明書を利用するには？
  - CN=Motonori Nakamura（emailはSubjectAltNameに格納）

証明書の検証

- CA証明書の取得
  - https://repo1.secomtrust.net/sppca/nii/odca3/index.html
  - 国立情報学研究所 オープンドメインS/MIME用SHA-2認証局CA証明書
    - https://repo1.secomtrust.net/sppca/nii/odca3/nii-odcasmime.cer
  - 国立情報学研究所 オープンドメインSHA-2認証局CA証明書
    - https://repo1.secomtrust.net/sppca/nii/odca3/nii-odca3sha2.cer
  - Security Communication RootCA2 Certificate
    - https://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer

- 証明書を検証する際の注意点
  - 2016年12月26日のメンテナンス以降、全てのS/MIME証明書は、「NII Open Domain S/MIME CA」から発行されます。
  - 2016年12月26日以降も、用途にS/MIMEを含まないクライアント証明書は、これまで通り「NII OpenDomain CA - G4」から発行されます。
  - クライアント証明書では、OCSPによる失効検証は提供されていません。

FreeRADIUSによるクライアント証明書認証

- CA_file = CA証明書(PEM)を並べたファイルを指定
- check_crl = yes
  - CRLファイルは定期的にダウンロードし、毎回更新後にradiusdを再起動
    - http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg4.crl
    - https://repo1.secomtrust.net/sppca/nii/odca3/fullcrlsmime.crl
- check_cert_issuer = "/C=JP/L=Academe/O=National Institute of Informatics/CN=NII Open Domain CA - G4"
  - 複数のCAから発行されたクライアント証明書を同時に利用する場合は、このチェックは使えない（自作スクリプトへの組み込み）
- check_cert_cn は使えない（自作スクリプトでチェック）

自作スクリプトですべきこと

- CRLの定期ダウンロードとCRLに基づく確認
  - 失効されていない証明書であること
- CA証明書に基づく発行者の確認
  - 有効なUPKIクライアント証明書であること
- クライアント証明書のDNの確認
  - 自機関に属する利用者であること
    - /C=JP/L=Academe/O=××University

- 検討課題
  - UPKIクライアント証明書によるeduroam認証

- その他の注意点
  - クライアント証明書認証がFWを通らない？？
    - パケットサイズの問題？

eduroamの参加申請方法（まとめ）

- **認証サーバに関する項目**
  1. Radiusサーバを構築・運用する場合
     - レルム、Radiusサーバのアドレス、パスワード
  2. 代理認証サービス利用の場合
     - レルム（代理認証サービスの申請）
  3. 仮名アカウント発行サービス利用の場合
     - （別途、学認への参加、IdPリストへの登録依頼）

- **認証プロキシ（アクセスポイント）に関する項目**
  1. アクセスポイントを独自に運用
     - Radiusプロキシのアドレス、パスワード
     - 必要に応じてSINETによるeduroam用アドレスを申請
  2. マネージドWiFiサービス
     - プロバイダーを含め調整
  3. 準備中の場合
     - 予定について記載（時期、台数など）

詳細については以下を参照ください
http://www.eduroam.jp/join.html