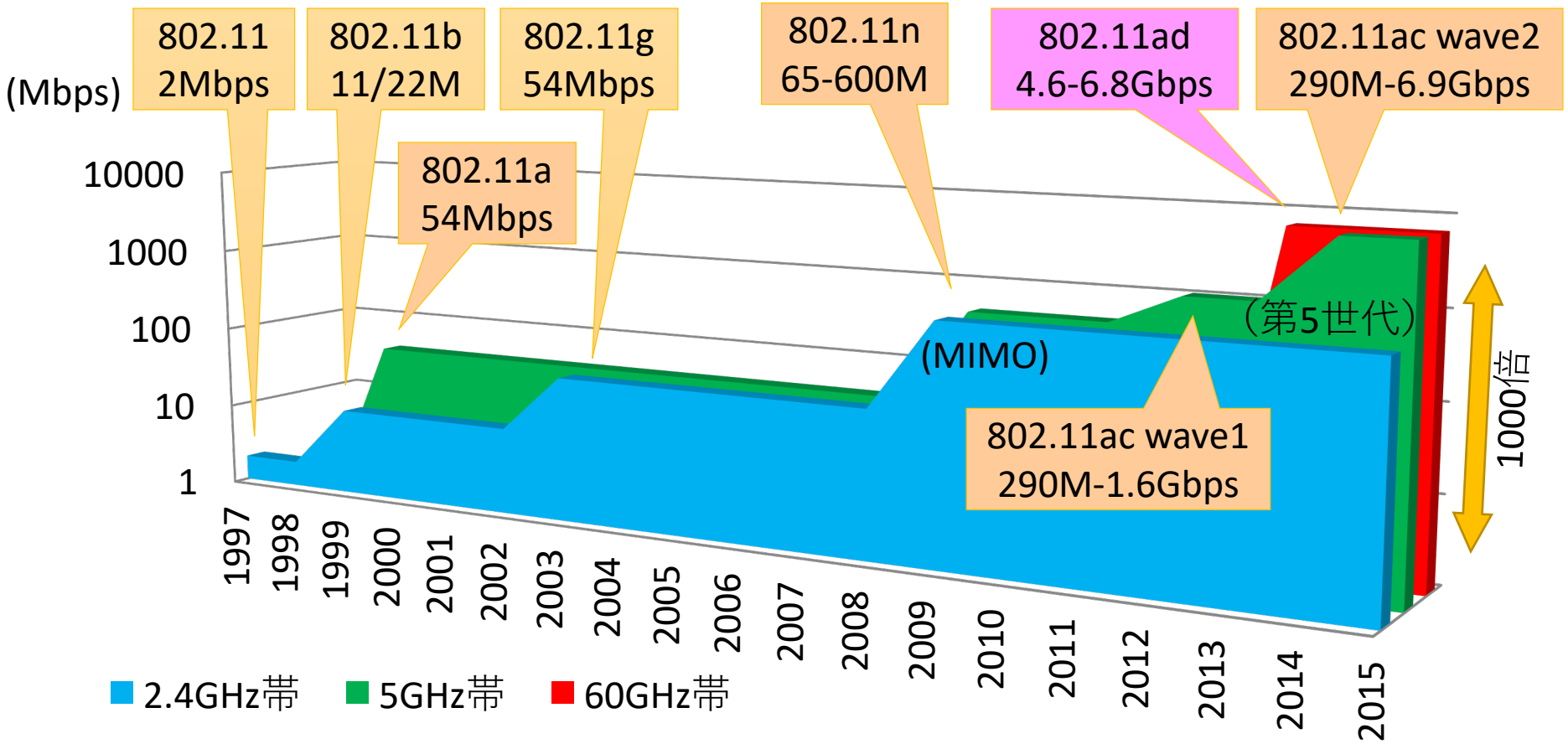
eduroam
基本チュートリアル

国立情報学研究所

オープンフォーラム2019

802.11無線LAN規格ー高速化の歴史



高速化の技術： 変調データの多ビット化、待ち時間削減、フレームサイズ拡張、
フレームアグリゲーション、帯域幅の拡張（～x8）、
MIMO（複数ストリーム ～x8）、ビームフォーミング

ネットワーク環境整備

- 環境整備のトレンドは有線から無線にシフト
  - 無線LAN対応端末の普及
  - ネットワーク構築・運用コストの低減化
  - 認証によるセキュリティの確保

- 大学・学会等の大人数が集まる会場での安定した運用への要求
  - 大講義室、大会議室、ホールなど（100～1000人規模）
    - BYOD：構成員による端末持ち込み増加
      - 一人が複数の端末を接続することも
  - 検討項目
    - 端末収容能力、安定性の高い機器の採用
    - アクセスポイントの数（チャネル割り当てに応じて）
    - チャネル割り当て、出力調整
    - 壁、床、天井の透過性
    - 干渉源の検出、排除
    - 古い規格（802.11b等）の利用制限（切り捨て）によるパフォーマンス向上
    - セキュリティ（認証方式、なりすまし・盗聴対策）

アクセスポイント管理の効率化

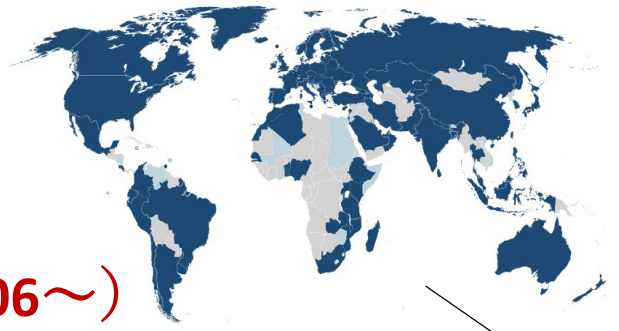
- スタンドアロン
  - 管理が面倒
  - 機種の統一が不要
- 無線LANコントローラ （2004年頃～）
  - チャネル割り当ての最適化
  - カバレッジ調整
  - ロードバランシング（スムーズなローミング）
  - 大規模ネットワーク向き（基地局が安くなる？）
- コントローラのクラウド化 （2013年頃～）
  - コントローラ導入が容易に
  - 管理のアウトソーシング
    - マネージドサービス

WaaS
Wireless (WiFi) as a Service

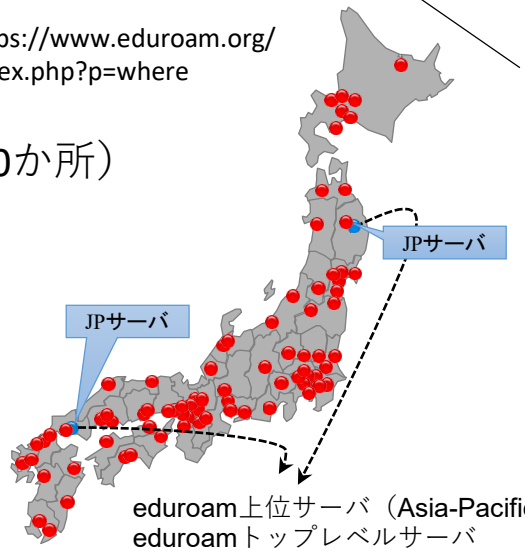
国際学術無線LANローミング基盤「eduroam」

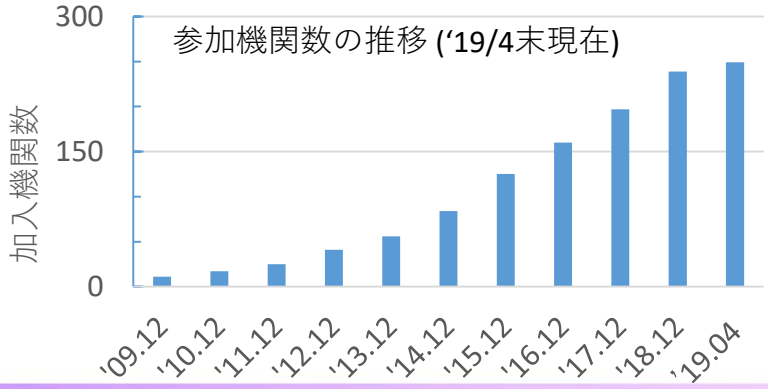
- **GÉANTで開発された教育・研究用の学術無線LAN (Wi-Fi) ローミング基盤**
  - 国際的デファクト・スタンダード
- **互恵の精神に基づくサービス**
  - 基地局を運用・提供している機関だけが、その構成員に利用させる ことができる
- **日本では「eduroam JP」の名称で運用（2006～）**
  - 原則として学術研究機関が対象（参加費不要）
  - 訪問先の無線LANが無料で利用可能
    - ESSIDは“**eduroam**”で統一、IDはuser@大学名.ac.jp等
    - 関東の貸会議室やカフェ等の一部でも利用可能（約130か所）
    - 海外では、駅や空港でつかえる国も

世界101か国・地域に展開



https://www.eduroam.org/index.php?p=where

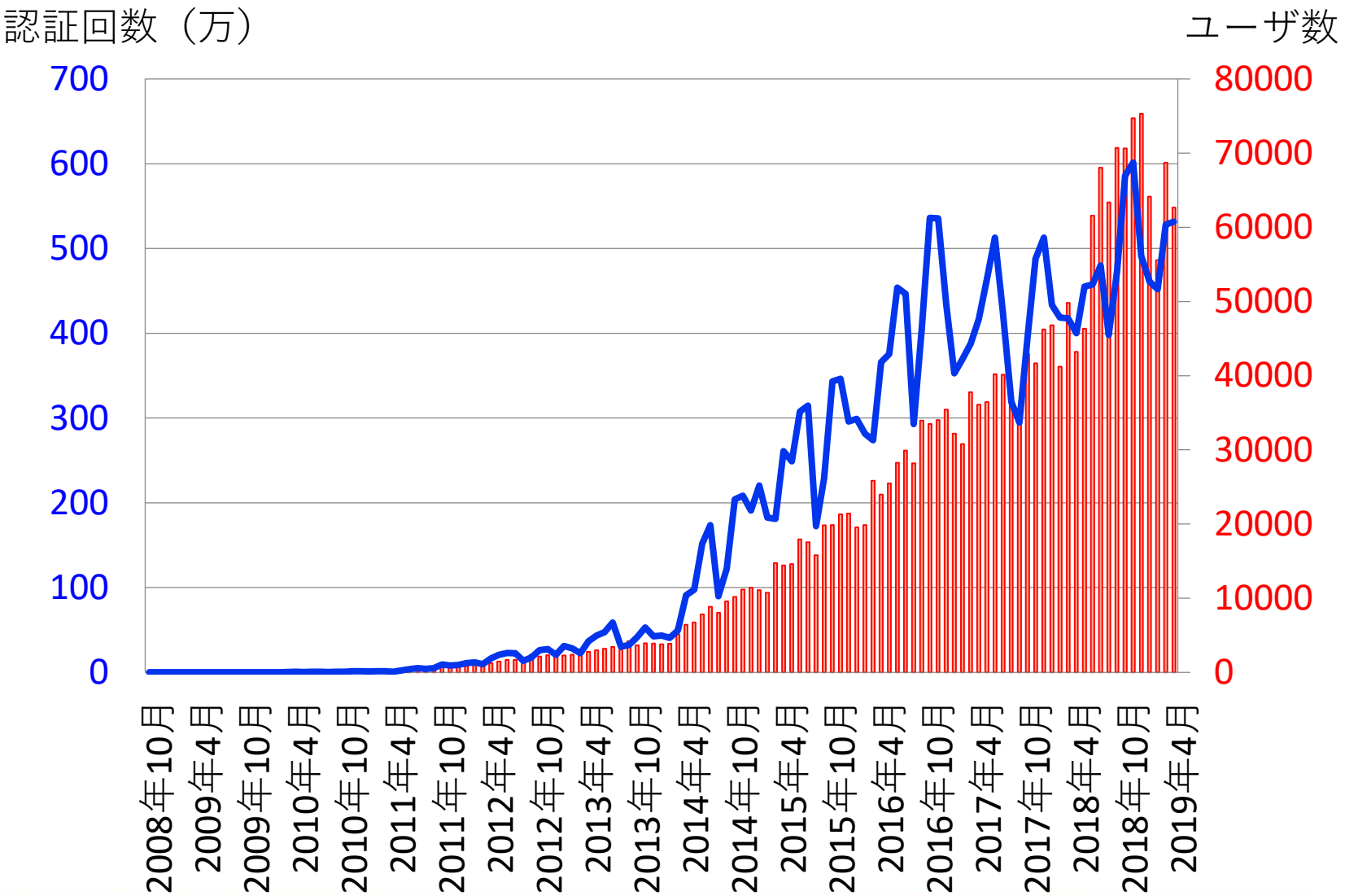




by TECHORUS & KDDI
（旧DATAHOTEL）

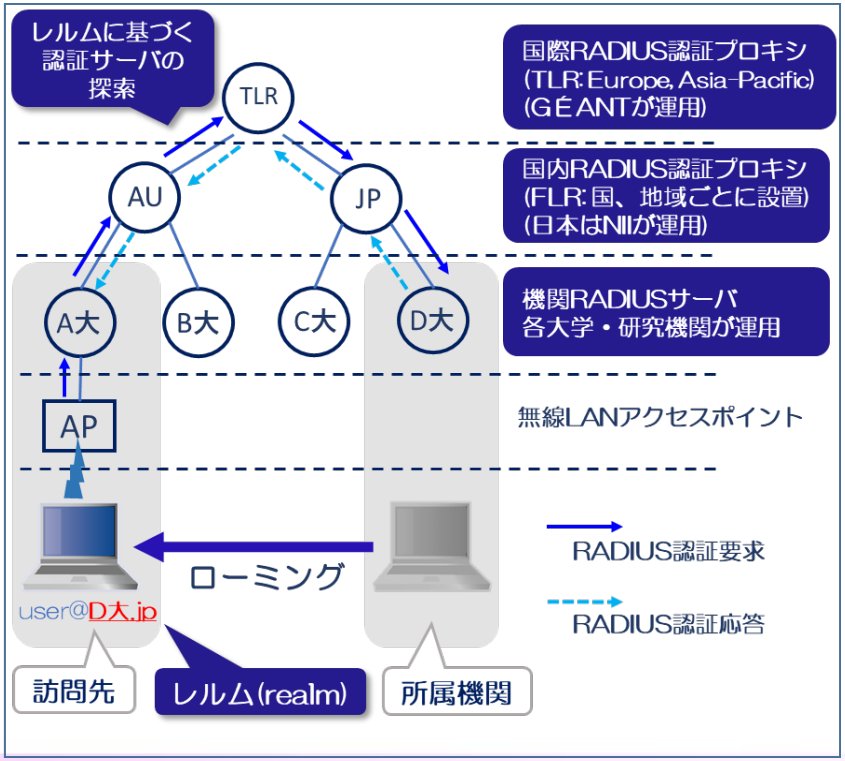
www.eduroam.jp

eduroam月間アクセス数(国内全アクセス)



eduroamの仕組みとメリット

- **訪問先の無線LANが無料で利用可能**
  - 互恵の精神に基づくサービス（訪問先での利用＋ゲストへの提供）
  - 来訪者向けネットワークを毎回構築する必要なし
    - 会議用一時アカウント発行も提供中（試行サービス）
- **所属する大学のアカウントがそのまま利用できる**
  - ”user@大学名.ac.jp”
  - 「学認」とも連携可能
- **国際標準IEEE 802.1x方式による セキュアなユーザ認証**
  - Windows/Mac/スマートフォン等に対応
  - Web認証より安全
    - なりすまし基地局による パスワード漏洩対策
  - クライアント証明書による認証も利用可能



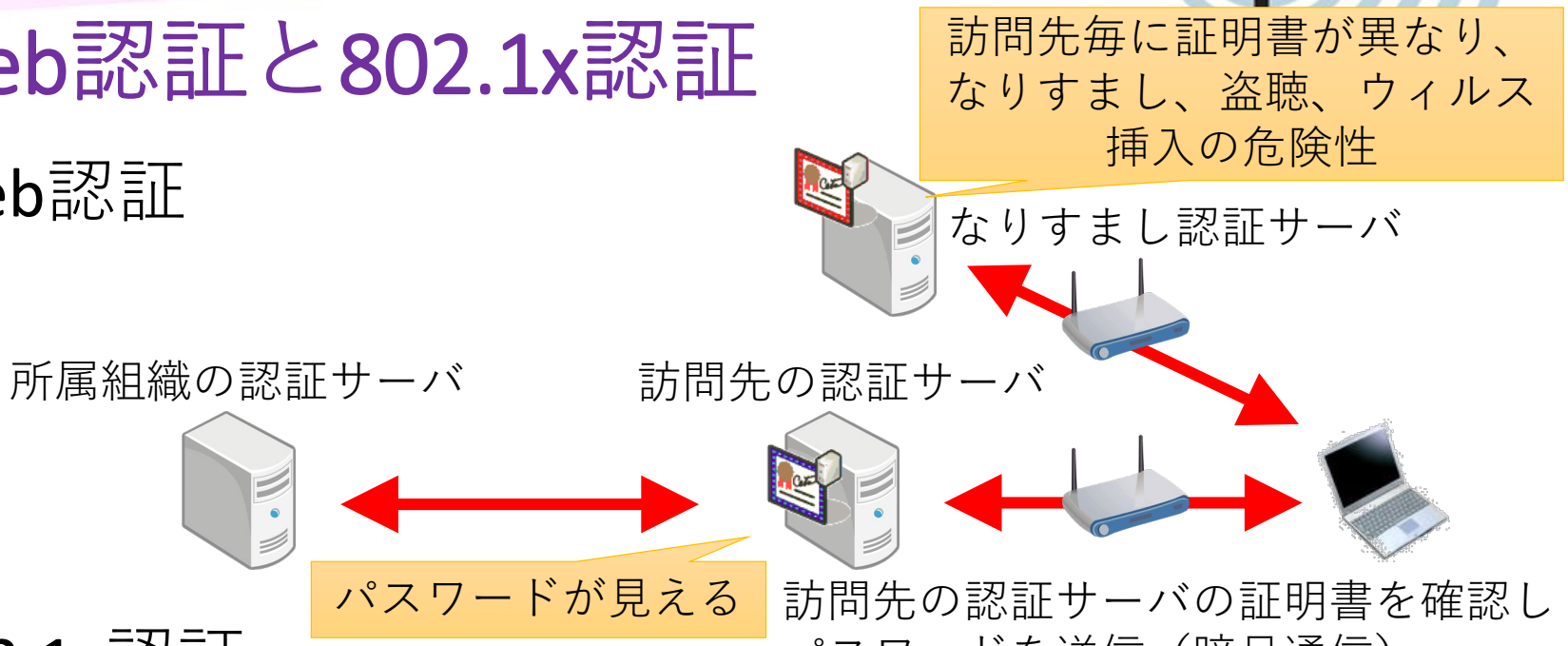
無線LANセキュリティ規格の変遷

- WEP （802.11規格の一部, 1999）
  - 暗号化
    - 2001年以降、容易に解読できることが明らかに
      - 解読ツールで数分以内に解読できてしまう
- WPA （802.11iのサブセット、2002）
  - 鍵の更新による対策
    - 2008年以降、WPA-TKIPに脆弱性が指摘される
      - 10分程度で攻撃が成功する
- WPA2 （802.11i- 2004）
  - 暗号強度の向上（AESの実装を義務化）
  - 認証方式
    - PSK (Personal)
    - EAP/802.1x (Enterprise)

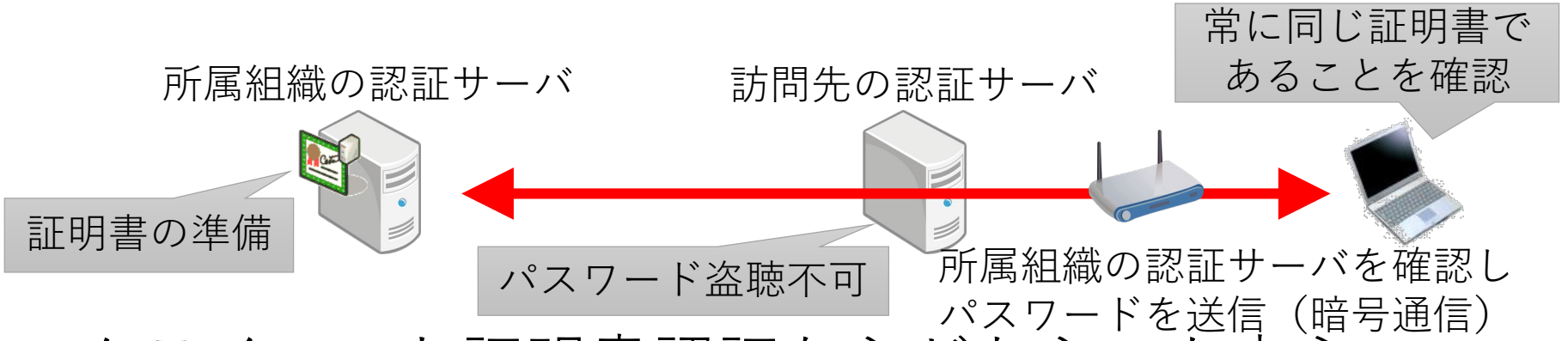
ユーザごとに異なるパスワードまたは証明書を用いる

Web認証と802.1x認証

- Web認証



- 802.1x認証



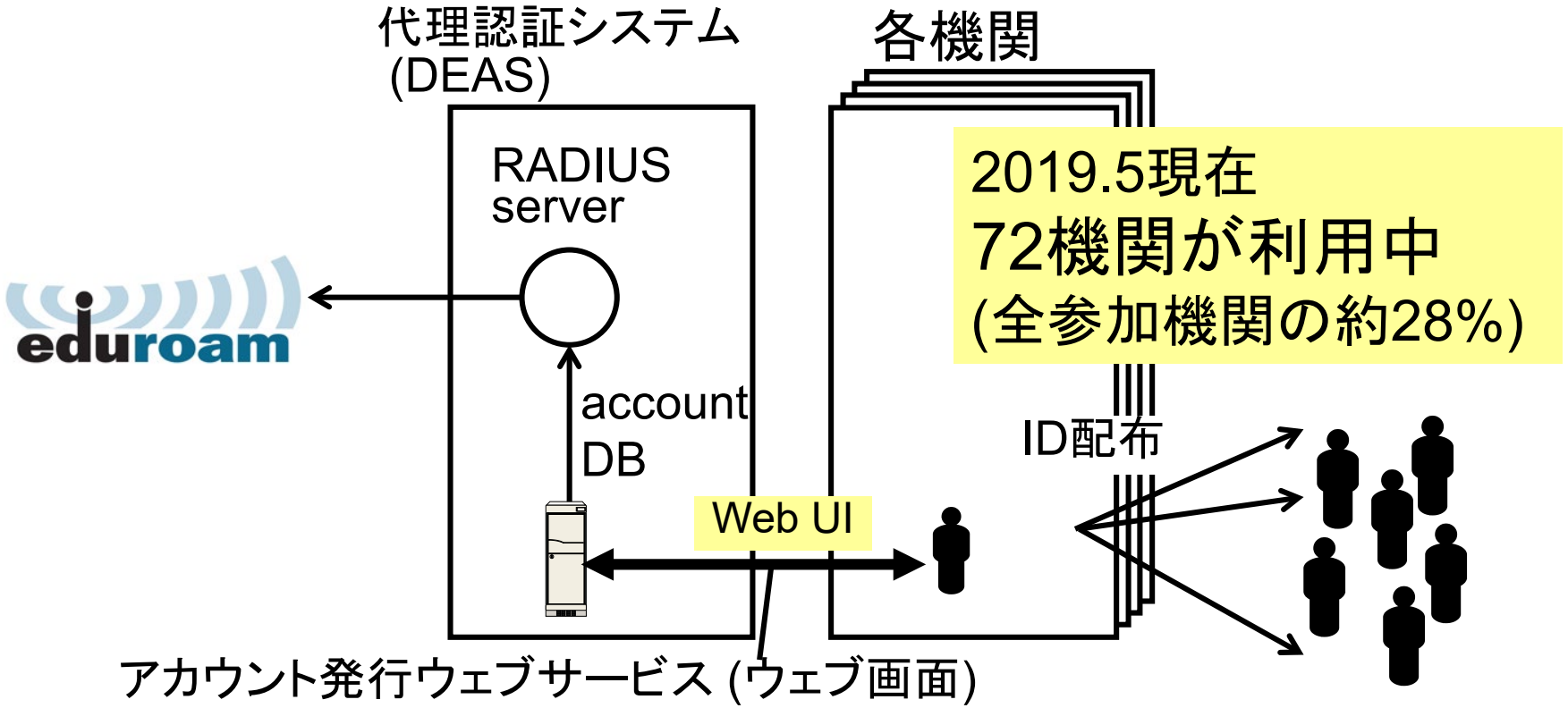
- クライアント証明書認証ならどちらでも安心

相互認証によるサーバ確認の可能

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サーバを自機関で構築・運用（クラウドも利用可）
     - 学内アカウントをそのまま利用することが可能
  2. 代理認証システムを利用
     - eduroam専用アカウント発行サービス
  3. 認証連携IDサービス（学認連携）を利用
     - 学認用のIDを用いてeduroam用仮名アカウントを発行
       - 認証用クライアント証明書発行機能あり
       - クライアント証明書によるeduroam接続認証に対応
     - 教職員はゲストアカウントの発行も可能
       - 通常のゲストアカウントは学内からの接続のみ
     - イベント向け(学外会場も対応)の大量発行機能あり
       - 構成員へのアカウント発行を制限してゲストアカウント発行のみ行うことも可能

代理認証システム (2008年～)



オンラインサインアップによる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

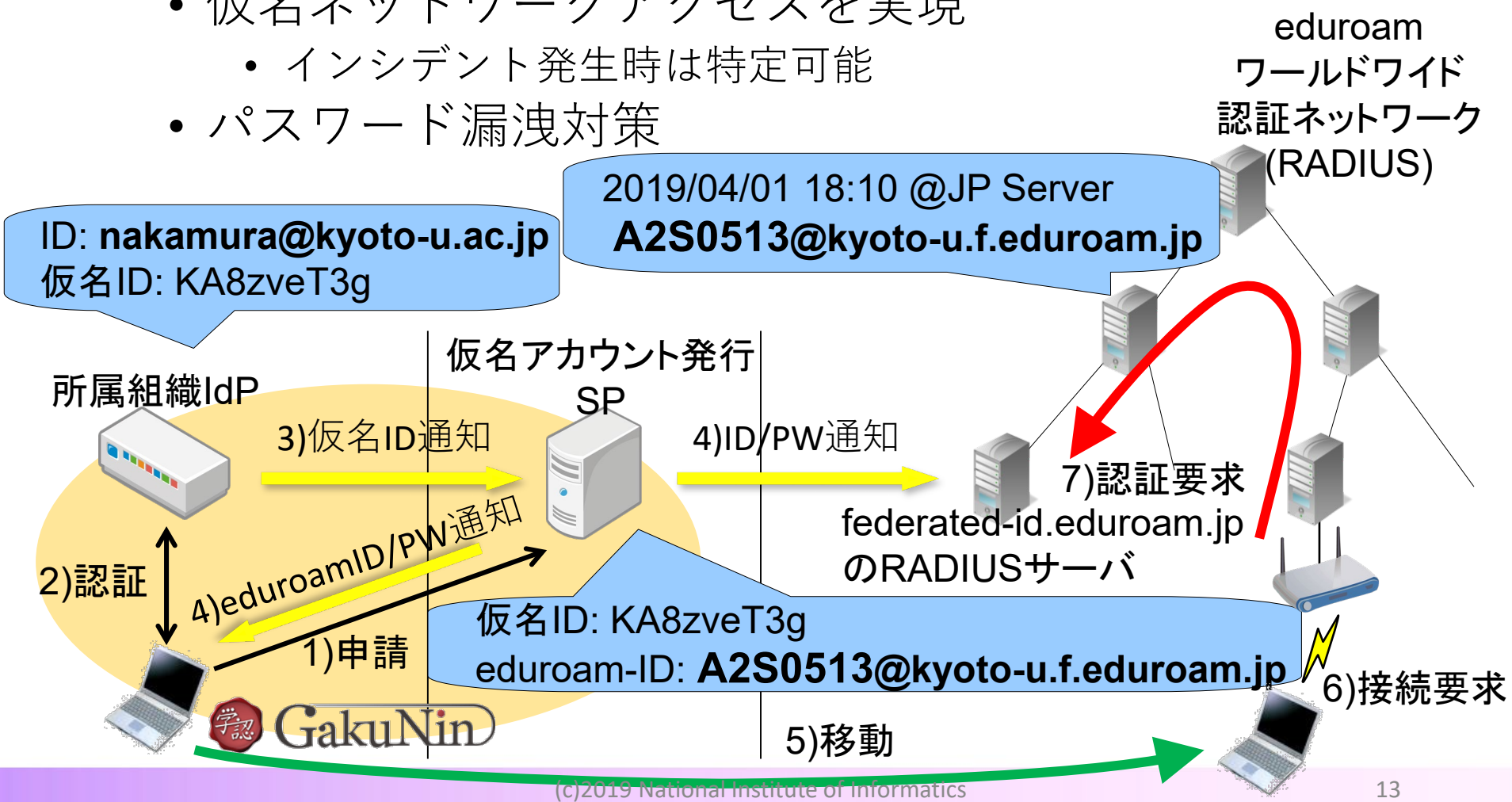
- ゲスト用アカウントの発行も可能

会議向け期間限定 eduroamアカウントの試行 (2014.7〜)

- 国内のeduroam対応大学・会議施設などで開催される学術系の会議、シンポジウム、ミーティングが対象
  - eduroam対応だが、大学・会議場がゲストアカウントを発行できない例がある
- 「代理認証システム」を利用
  - 会議/シンポジウム/ミーティングを仮想機関(VO)とみなし、機関管理者用アカウントを発行
  - 会議開催ごとに申請が必要
- 現在、提供条件を検討しながら、試行中
  - 偽の会議の申請を排除したい
  - eduroam JP事務担当の負担が増えないようにしたい
  - 利用資格の基準をどのように設定するか？
- これ以外に認証連携IDサービスのゲストアカウント大量発行機能もあり
  - 学認加入機関はこちらでのゲストアカウント(学内のみ/学外OKの両方可)発行も検討を

認証連携IDサービスSP

- Shibboleth認証し、eduroam仮名アカウントを発行
  - 仮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



eduroamへの参加方法：ゲストへの提供

- 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
    （機関内システムへのアクセスを制限するためセグメントを分離）

    A：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）

    B：新たにIPアドレスブロックを取得して利用

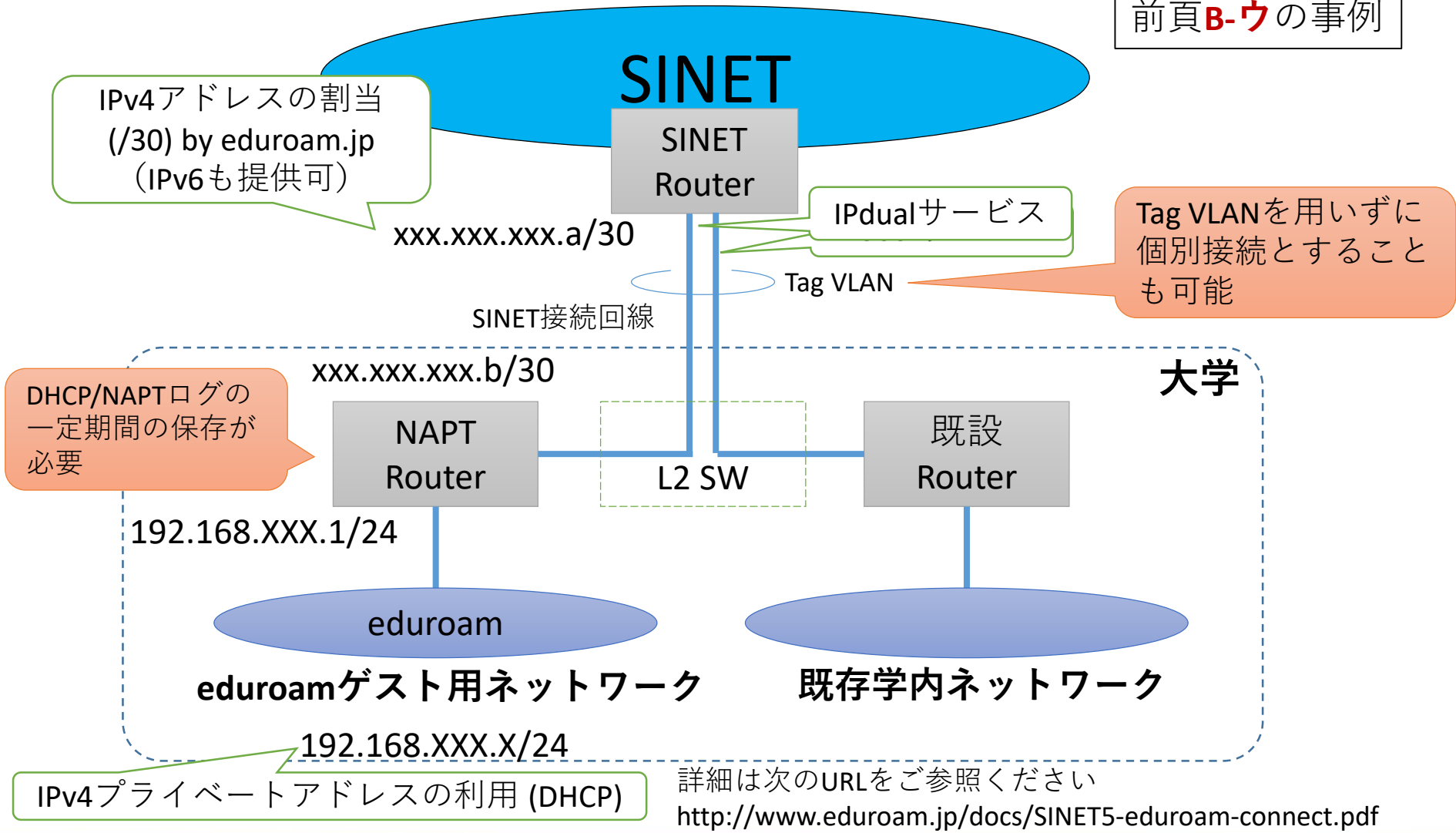
    ア) 新たに商用回線等を導入し、その回線に付随するIPアドレスを利用

    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）

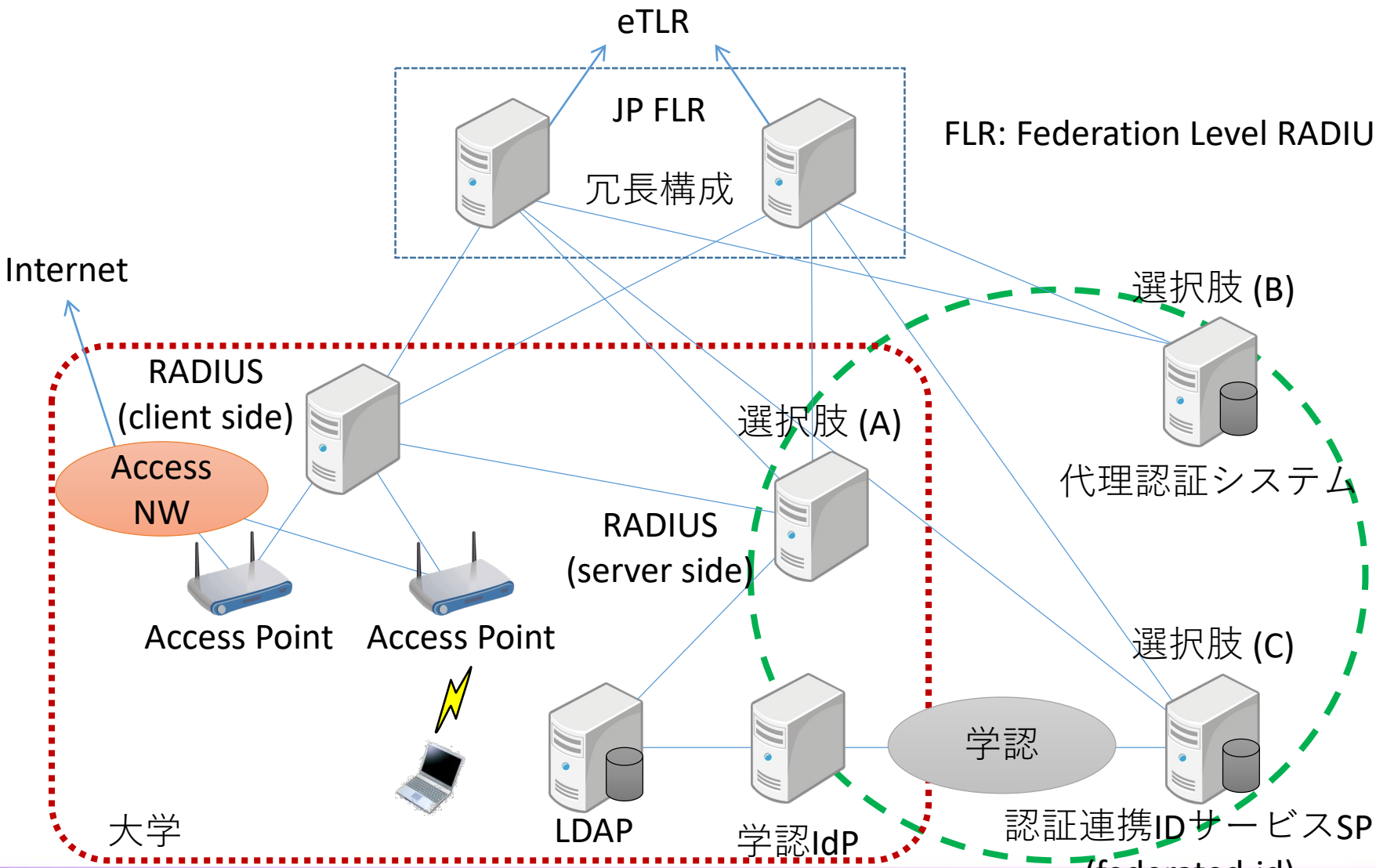
SINETによるeduroamアクセスネットワーク収容のイメージ

前頁**B-ウ**の事例

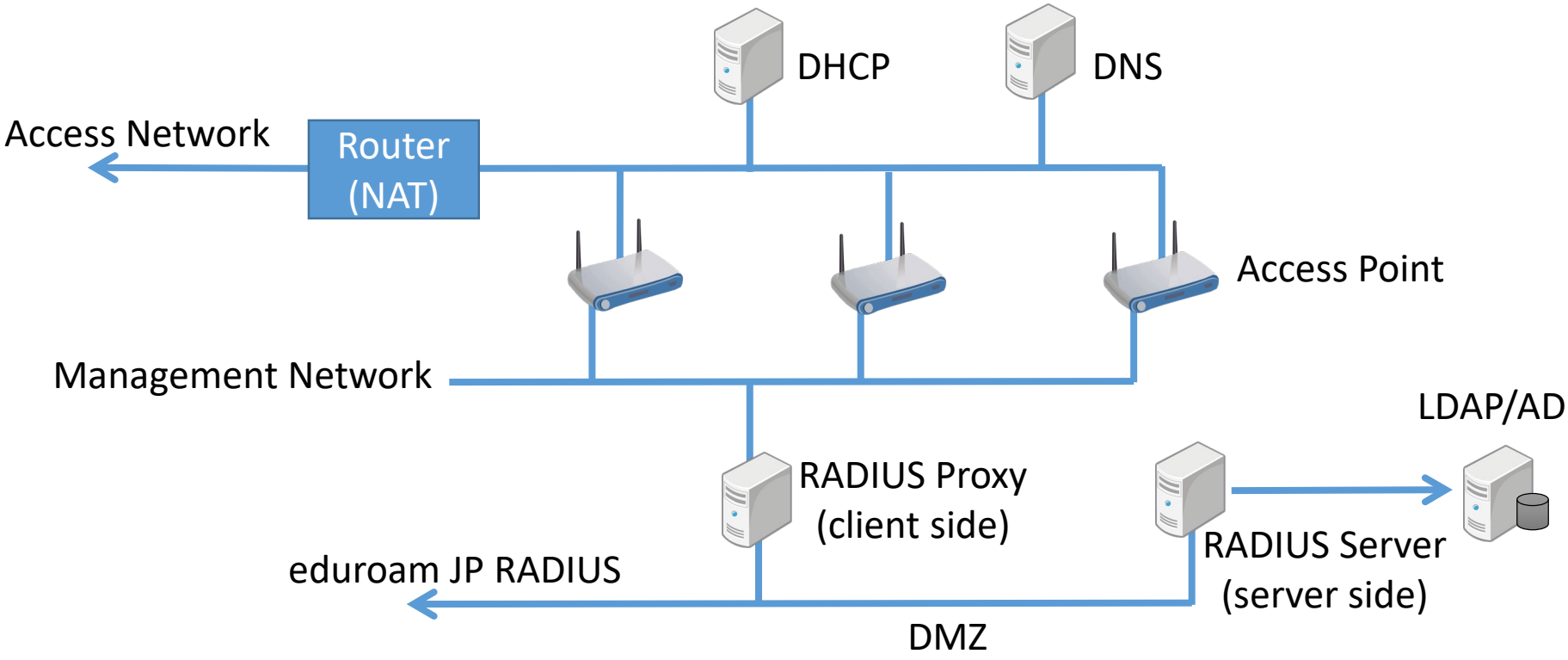


詳細は次のURLをご参照ください
http://www.eduroam.jp/docs/SINET5-eduroam-connect.pdf

大学でのeduroamシステム構成例



アクセスネットワークの基本設計



- インシデント対応のために、RADIUS (ID/MAC)、DHCP (MAC/IP)、NAT (IP/port)などのログの取得が必要

eduroamの加入申請方法

- eduroam JP申請システムより加入申請提出
  - 学認参加IdPまたはOpenIdPのアカウントでログイン
  - 機関情報、担当者情報、ネットワーク情報、RADIUSサーバ情報等を記入
    - 詳細：https://meatwiki.nii.ac.jp/confluence/x/u2NHAQ
  - 規程類をご一読ください。
    - 規程類：https://www.eduroam.jp/rules/
  - 導入前に先に加入申請だけしたい→OK
  - APの整備が追い付かない
    →原則加入後1年以内に整備
    ※大講堂、図書館など訪問者がよく利用する場所だけでもOK

お寄せいただいた質問への回答

- ID/パスワードから紛らわしい文字や記号を抜いてほしい
  - できるだけ紛らわしい文字を排除するルールを適用していますが、不十分なようでしたら善処します。(具体的な文字をご連絡ください)
  - 記号の排除は安全性の面からできません
- マニュアルが古いものがあるので更新してほしい
  - 少しずつですが更新していますのでお待ちください
- インシデントが起きたらどうしたらいいの？
  - ログから該当端末のMACアドレス、IPアドレス、レルム、日時情報、わかればユーザIDをお知らせください
  - アカウント発行機関に連絡します

お寄せいただいた質問への回答

- 学内無線LANとeduroamの違いを分かりやすく説明したい
  - eduroamでは**認証VLAN**の導入を推奨しています
    (午後のセッションにて詳述)
    - 無線LANをeduroamに一元化し、認証VLANで学内ユーザと訪問者の収容ネットワークを区別する運用が標準
    - 一元化しておくと、わざわざ違いを説明する必要がない
  - 認証VLANを導入しない場合、こんな問題が
    - 構成員が自機関でeduroamに接続すると
      - 学内専用システムにアクセスできない
      - IPアドレス制限のある電子ジャーナルなどを閲覧できない
        (学認経由で使えるものはOK)

ネットワーク運用に関することは以下の資料を参照してください。
オープンフォーラム2018 eduroam講演資料：
https://www.nii.ac.jp/service/openforum2018/track/pdf/20180621AM_GN_eduroam02_Goto.pdf

お寄せいただいた質問への回答

- うまくつながらない時はどうしたらいいの？
  - 後のスライドで！

- 他大学で接続できない時の問い合わせ窓口を
  わかりやすく提示してほしい
  - エンドユーザからの問い合わせ対応は加入機関のeduroam担当部署にお願いしています。
  - 各加入機関におかれましては、利用者への問い合わせ窓口の周知をお願いいたします。
  - eduroam JPは加入機関担当者からの問い合わせのみを受け付けています。

トラブルシューティング
端末がeduroamに繋がらないときは?

- 所属組織を離れる前に、利用予定の端末での接続テストをしておくことをお勧めします
  - 訪問先でうまく繋がらない場合の問題の切り分けが容易になります（以下の1〜3の問題でないことの確認）
- 問題の切り分けのポイント
  1. アカウント自体が有効かどうか（他の端末で使えるか？）
  2. 端末での設定方法に問題がないか（パスワードの打ち間違い、認証方式の 選択、サーバ証明書の確認方法、など）
  3. 端末の機能に問題がないか（バージョンが古い、アクセスポイン トとの相性が良くない、など）
  4. 認証サーバに障害が発生していないか（発行元が同じである他のアカウントは他の場所でも使えているか？）
  5. 訪問先大学のアクセスポイントに障害が発生していないか（周辺にいる人は使えているか？）
  6. 認証連携ネットワークに障害が発生しているか（上記のいずれにも当てはまらないとき）

お問い合わせ先

eduroam JPの詳細については以下をご覧ください
https://www.eduroam.jp/

eduroam全般のお問い合わせ先：
eduroam-office@nii.ac.jp