国際学術無線LANローミングサービス eduroamについて

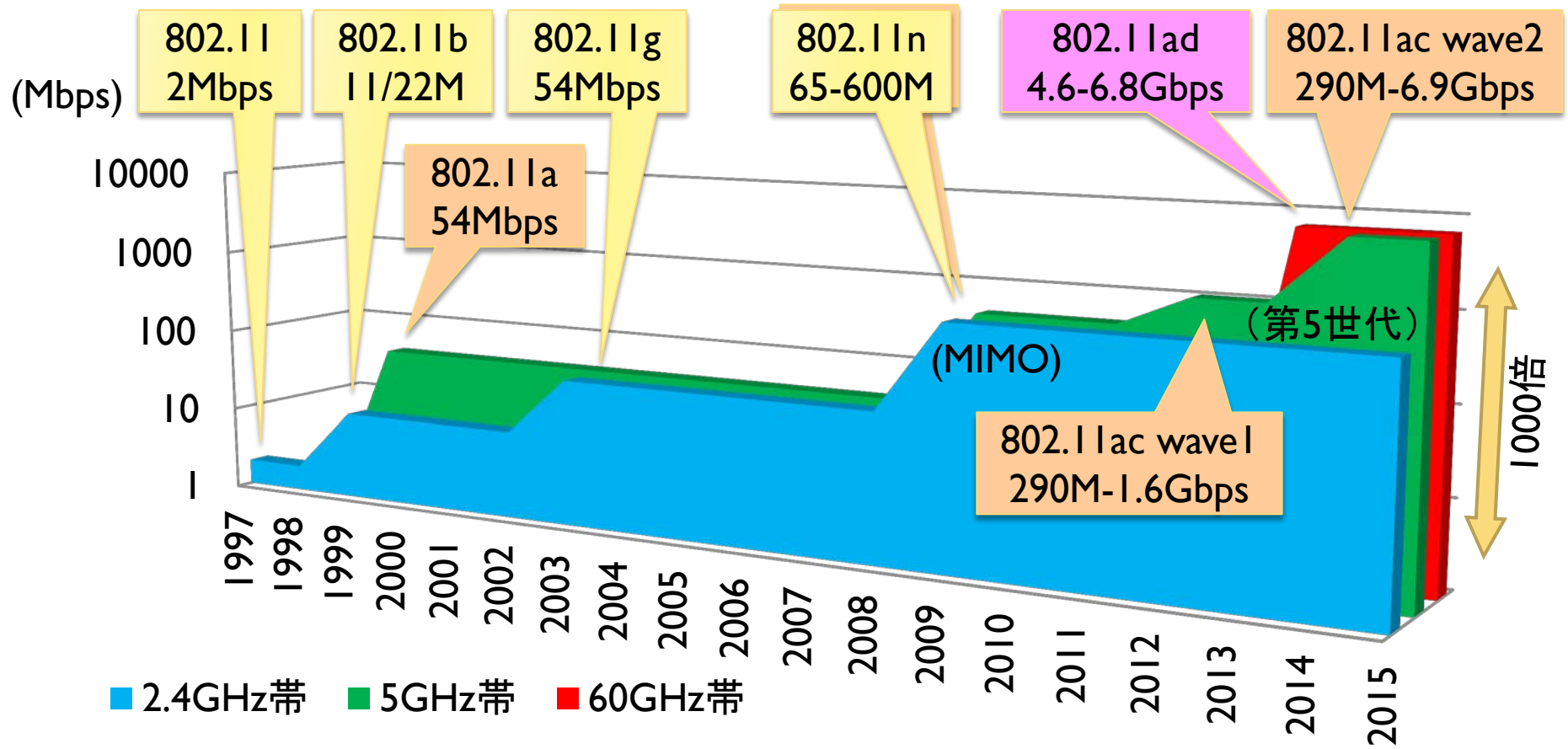
中村素典（NII）・後藤英昭（東北大）

2016年5月26日 NII学術情報基盤オープンフォーラム

2016.5.30改訂版

http://www.eduroam.jp/

802.11無線LAN規格—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）
    - 企業等の大規模オフィスなども
      - モバイル端末の増加により、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

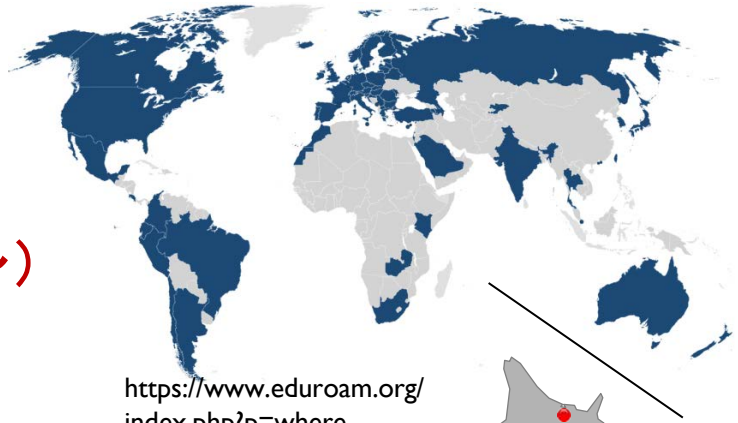
- スタンドアロン
  - 管理が面倒
  - 機種の統一が不要
- 無線LANコントローラ（2004年頃～）
  - チャネル割り当ての最適化
  - カバレッジ調整
  - ロードバランシング（スムーズなローミング）
  - 大規模ネットワーク向き（基地局が安くなる？）
- コントローラのクラウド化（2013年頃～）
  - コントローラ導入が容易に
  - 管理のアウトソーシング
    - マネージドサービス

WaaS
Wireless (WiFi) as a Service

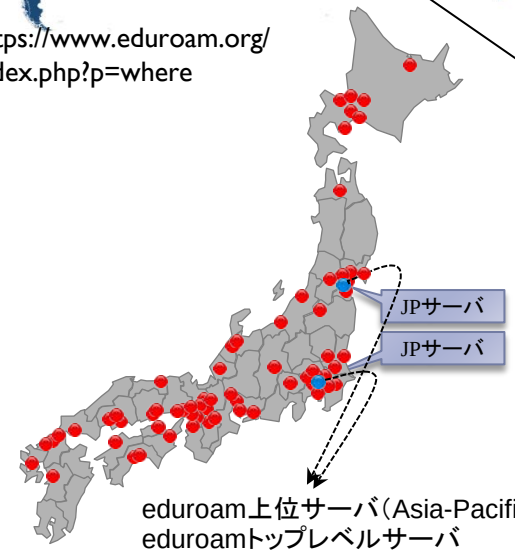
国際学術無線LANローミング基盤「eduroam」

- **欧州TERENA（現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
- **日本から「eduroam JP」の名称で参加（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.jp”
    - 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75か国・地域に展開

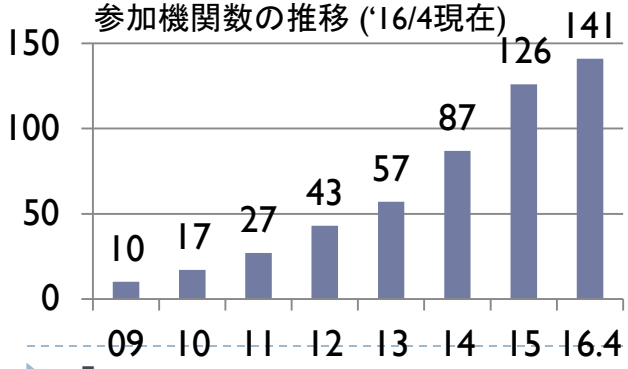


https://www.eduroam.org/index.php?p=where



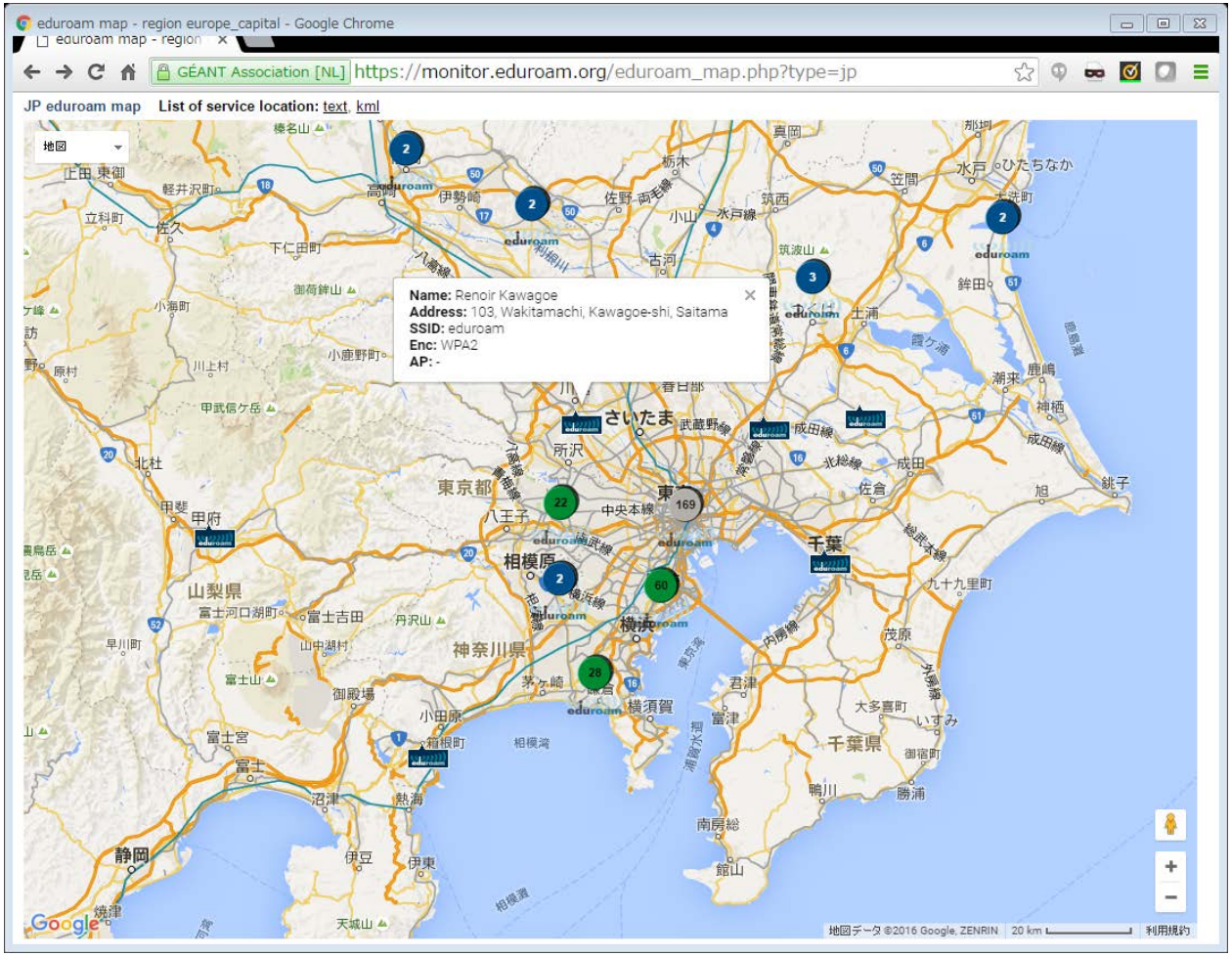
eduroam上位サーバ（Asia-Pacific）
eduroamトップレベルサーバ

www.eduroam.jp



by TECHORUS & KDDI（旧DATAHOTEL）

利用可能な場所を地図上で確認できます



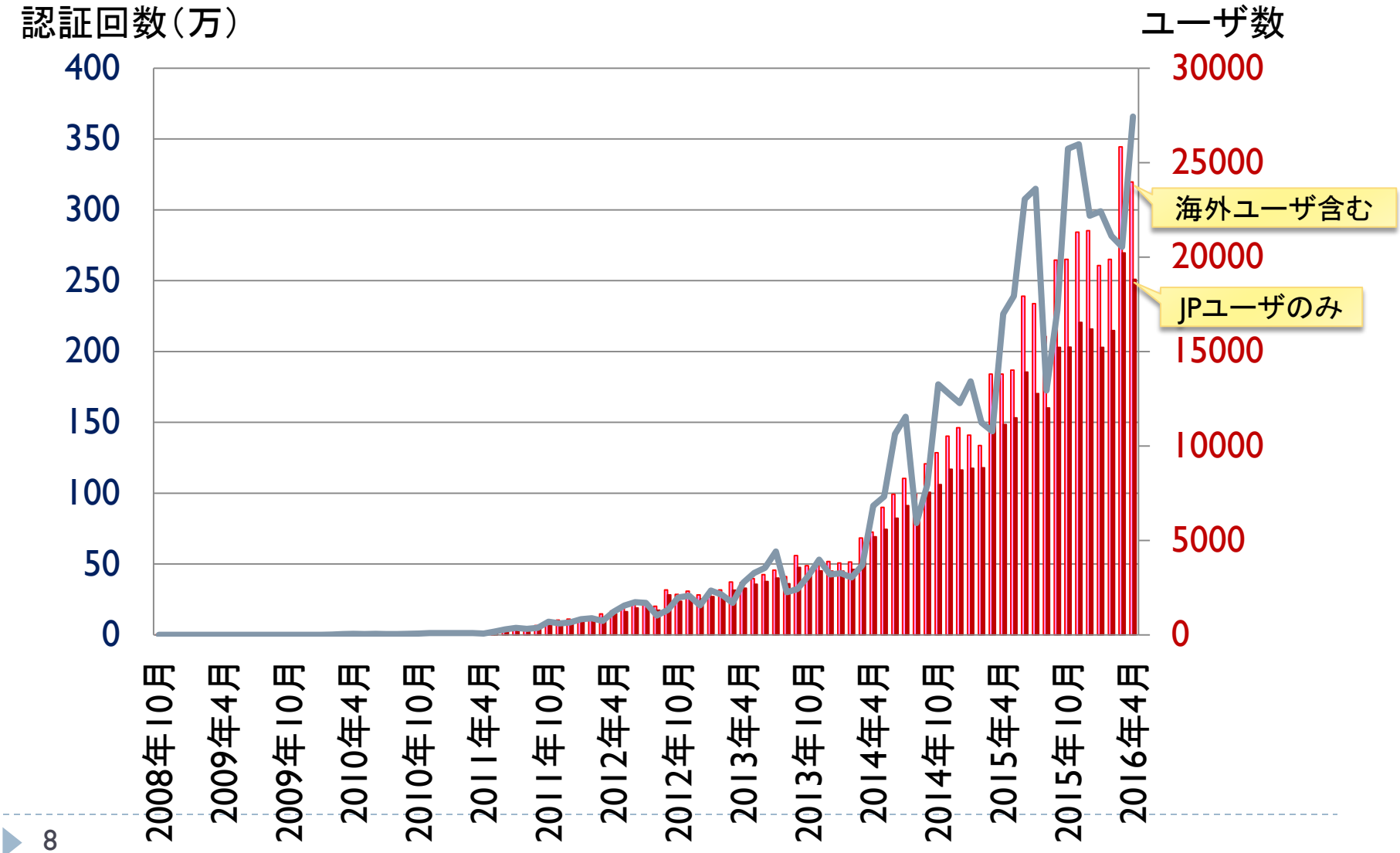
基地局所在地情報の提供にご協力をお願いします

eduroam JPの事業化について

- NIIによる事業化（2016/04～）
  - これまで認証作業部会が提供してきたeduroam JPは、NIIによる正式事業となります
    - 運営体制が新しくなります
    - 実施要領等を整備します
    - 新しい各種申請フォームを準備しています

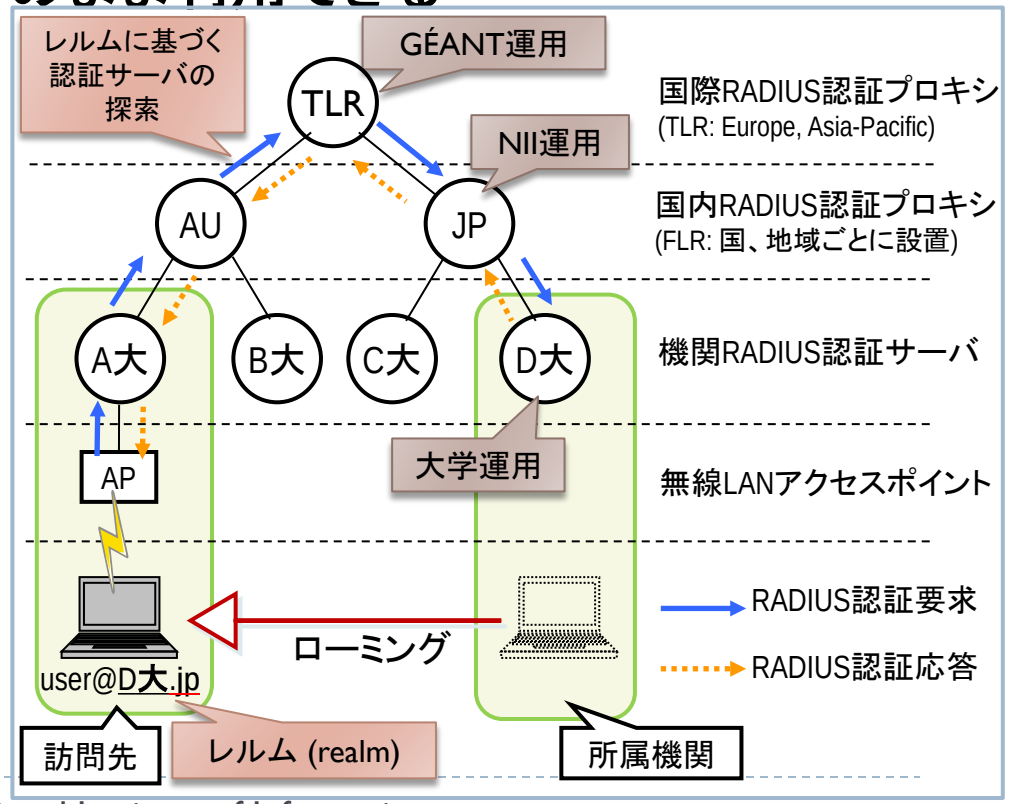
- 参加機関の皆様へ
  - 新しい実施要領に基づくサービスに移行します
    - 参加費は引き続き無料です
    - 実施要領の内容に同意いただけるか、7月をめどに継続参加の意思を確認させて頂きます
    - 参加機関側のシステムはそのまま利用できます
      - 設定変更や継続申請など、お手数をおかけすることになるかもしれませんが、ご協力をお願いいたします。

eduroam JP月間アクセス数



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.jp”
  - 「学認」とも連携可能
- **国際標準IEEE 802.1x方式による安全なユーザ認証**
  - 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

2通りのユーザ認証方式

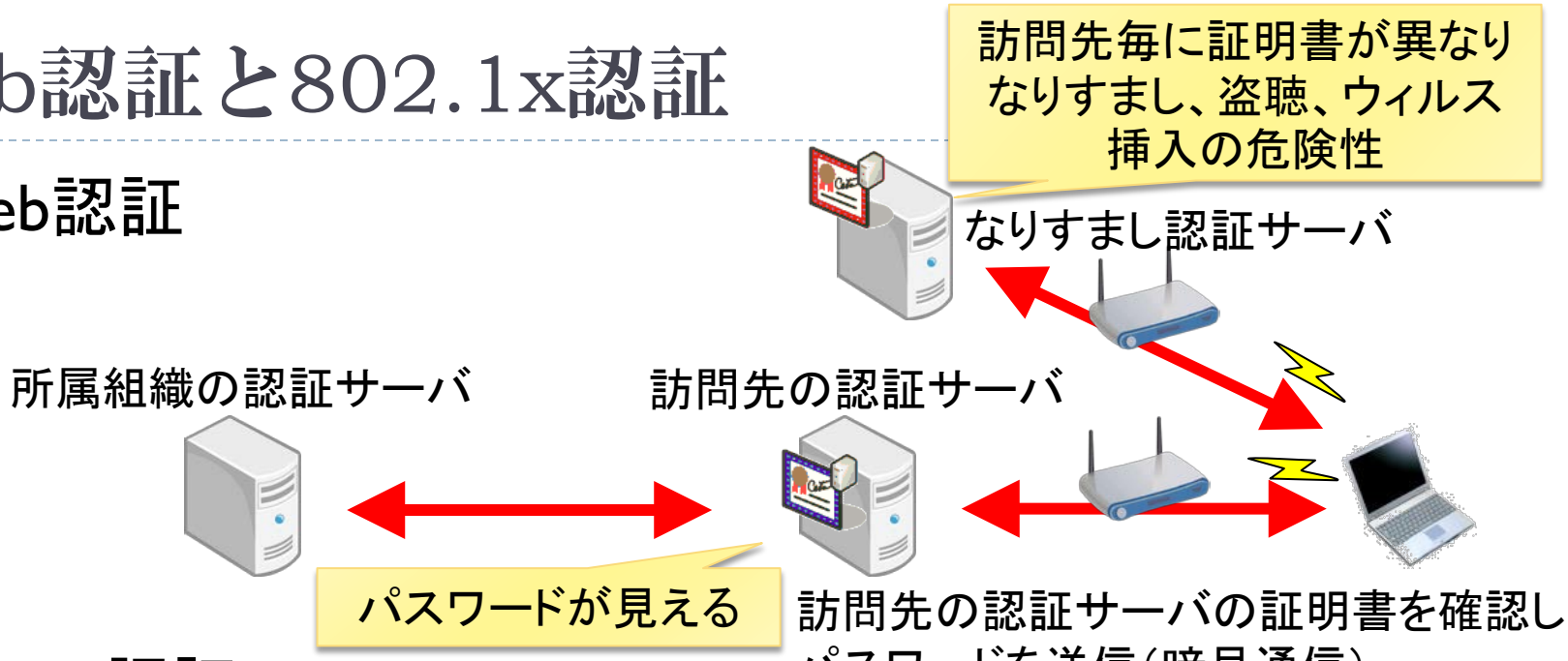
- Web認証 (Captive Portal)
  - 認証前のユーザへの情報提供が容易
  - **APのなりすましへの注意が必要（パスワード等の漏洩、中間者攻撃、ウィルスの挿入など）**
    - SSLサーバ証明書の確認が重要だが徹底が困難
    - クライアント証明書認証はパスワード漏洩対策

- 802.1x認証
  - 外部の認証サーバ（RADIUS等）に問い合わせ
  - パスワード認証
    - PEAP / MS-CHAPv2 （RFC 2759）による相互認証
      - 暗号通信(TLS)の内側で用いることで脆弱性（2012年に指摘）を回避
    - EAP-TTLS
  - クライアント証明書認証（パスワードの漏洩がない）
    - EAP-TLS

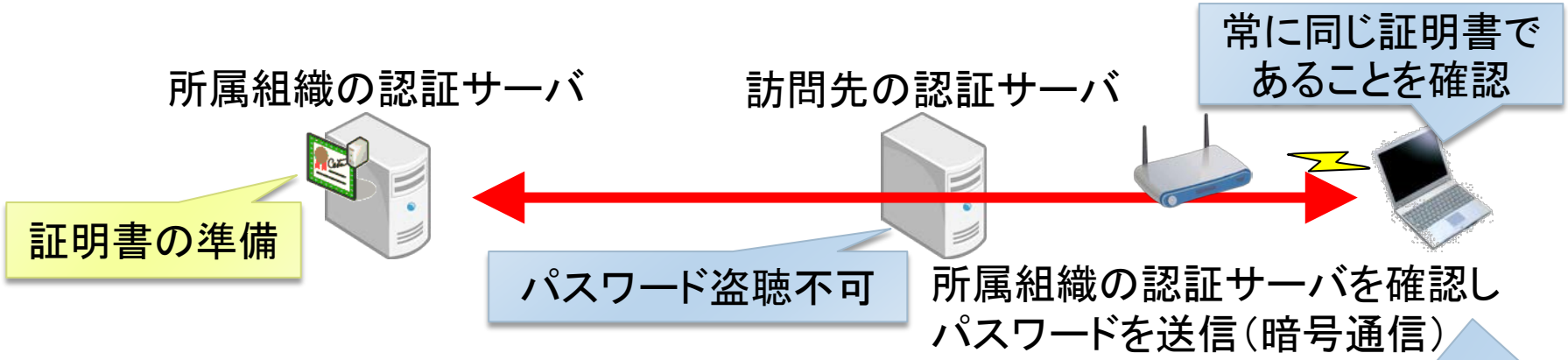
サーバ証明書による
認証サーバの確認が可能

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の場合も安心

相互認証による
サーバ確認が可能

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）

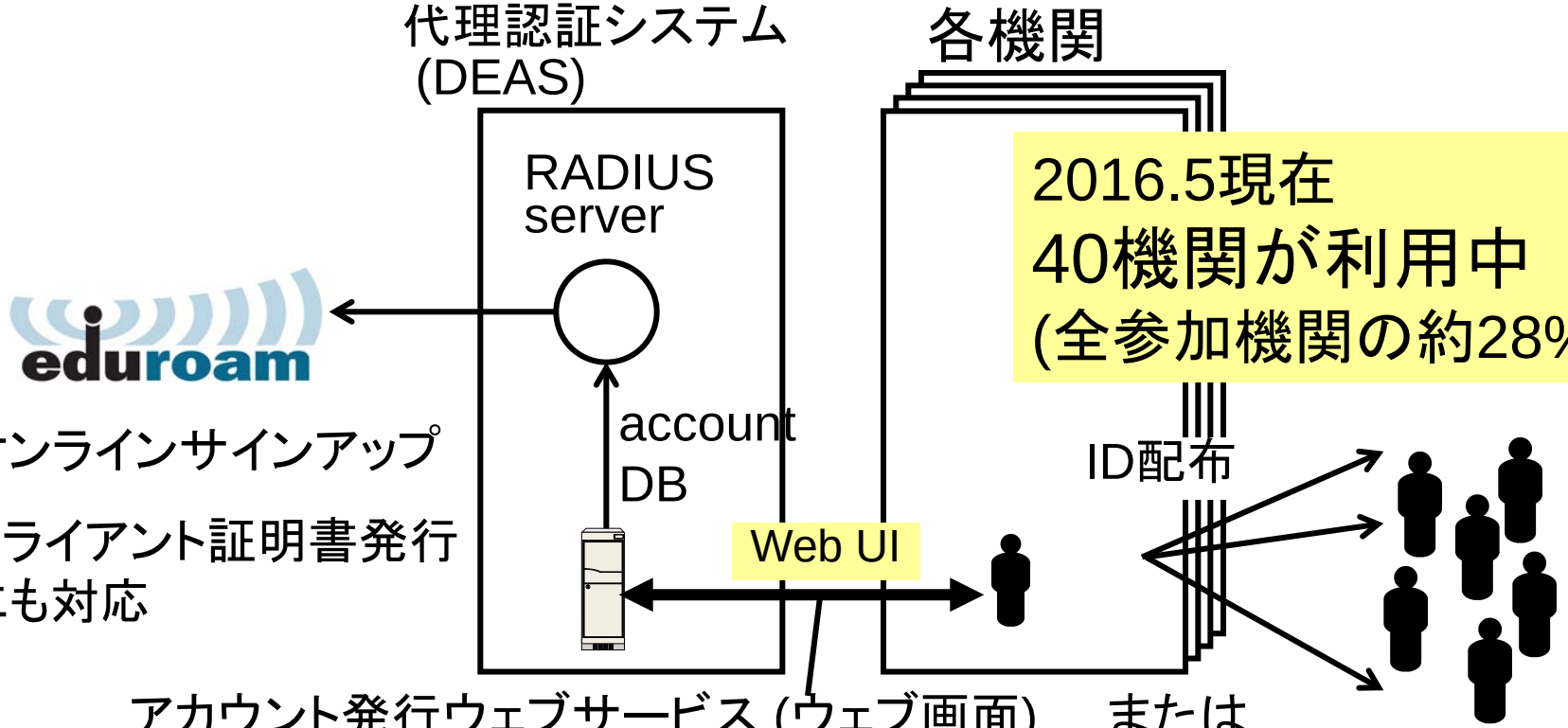
1. RADIUSサーバを構築・運用（クラウドも利用可）
   - 学内アカウントをそのまま利用することが可能

原則はこちらです

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. 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

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

※ 認証連携なしのシステムは既に サービス提供中!

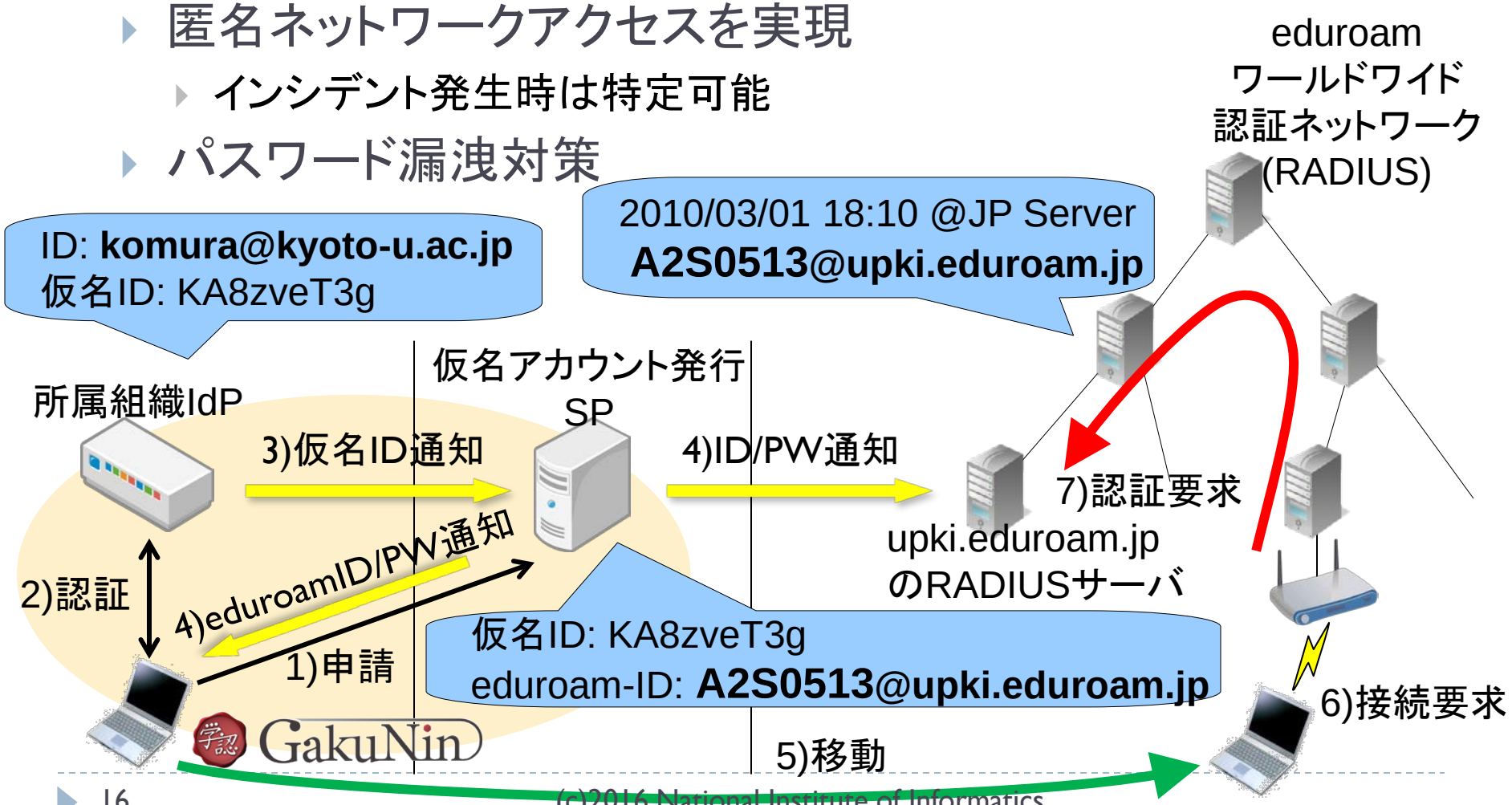
- ID取得だけで、管理者がアカウントをバルク請求・発行可能
- ゲスト用アカウントの発行も可能

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事務局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？

eduroam仮名アカウント発行サービスSP

- Shibboleth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



GakuNin 学術認証フェデレーション「学認」

- シングルサインオン(SSO)技術に基づく学術研究支援IT基盤の構築 — クラウド活用を支援
- IdP・SP相互の信頼を持続する信頼フレームワークの提供 — LoA 認定による、PubMed、e-Radアクセス
- 国際連携・産学連携による利便性向上、付加価値の実現、新サービスの創出 — 学割サービス
- 多様なニーズに応え、利便性・セキュリティを向上させる技術開発 — 多要素認証、個人情報保護、Virtual Organization

SP

図書館システム / Webメール / グループウェア / Eラーニング / 電子ジャーナル

サービス提供

大学間連携

GakuNin運営組織
- フェデレーション　ポリシーの策定
- IdP運用評価
- 広報・普及

ディスカバリーサービス / 学認申請システム / メタデータリポジトリ / 情報提供サイト

ID管理 IdP

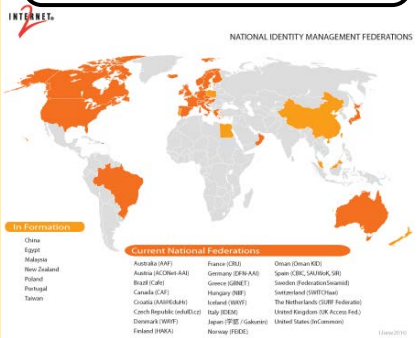
匿名性・仮名性実現 / 学内統合認証との連携 / 属性情報提供

大学 A（教員）— 個人認証で学外からも快適アクセス

大学 B（職員）— ID管理工数の低減 セキュリティレベルの底上げ 個人情報保護

大学 C（学生）— シングルサインオンでスムーズなアクセス

フェデレーションの構築は世界各国で進行中!



コンテンツ系サービス

ScienceDirect, ISI Web of Knowledge, SpringerLink, SCOPUS, CAMBRIDGE UNIVERSITY PRESS, PATHOLOGY IMAGES, ebrary, EBSCO HOST, 17, KOD, IEEE Xplore, 360, IOPscience, KARGER, BioOne, Emerald, CENGAGE Learning, HighWire, nature.com, palgrave macmillan, ANNUAL REVIEWS, eduroam, Informatics SQUARE 情報学広場, JAIRO Cloud, CiNii, NII-REO, Researchmap, RefWorks, Microsoft DreamSpark, GakuNin Ready!, ICTSFC

Most of Major Publishers

各種基盤系サービス

UQ WiMAX, edubase, 学内事務サービス, eLearning ePortfolio, FaMCUs, WebELS Ver. 6.0, Fshare β, Foodle

金沢大学総合メディア基盤センターデータリポジトリ IMC Data Repository Information Media Center of Kanazawa University

金沢大学 KANAZAWA UNIVERSITY, 山形大学 YAMAGATA UNIVERSITY, 広島大学, 佐賀大学

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
    （多くの機関では、機関内からのアクセスのみを許可しているサービスが運用されており、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

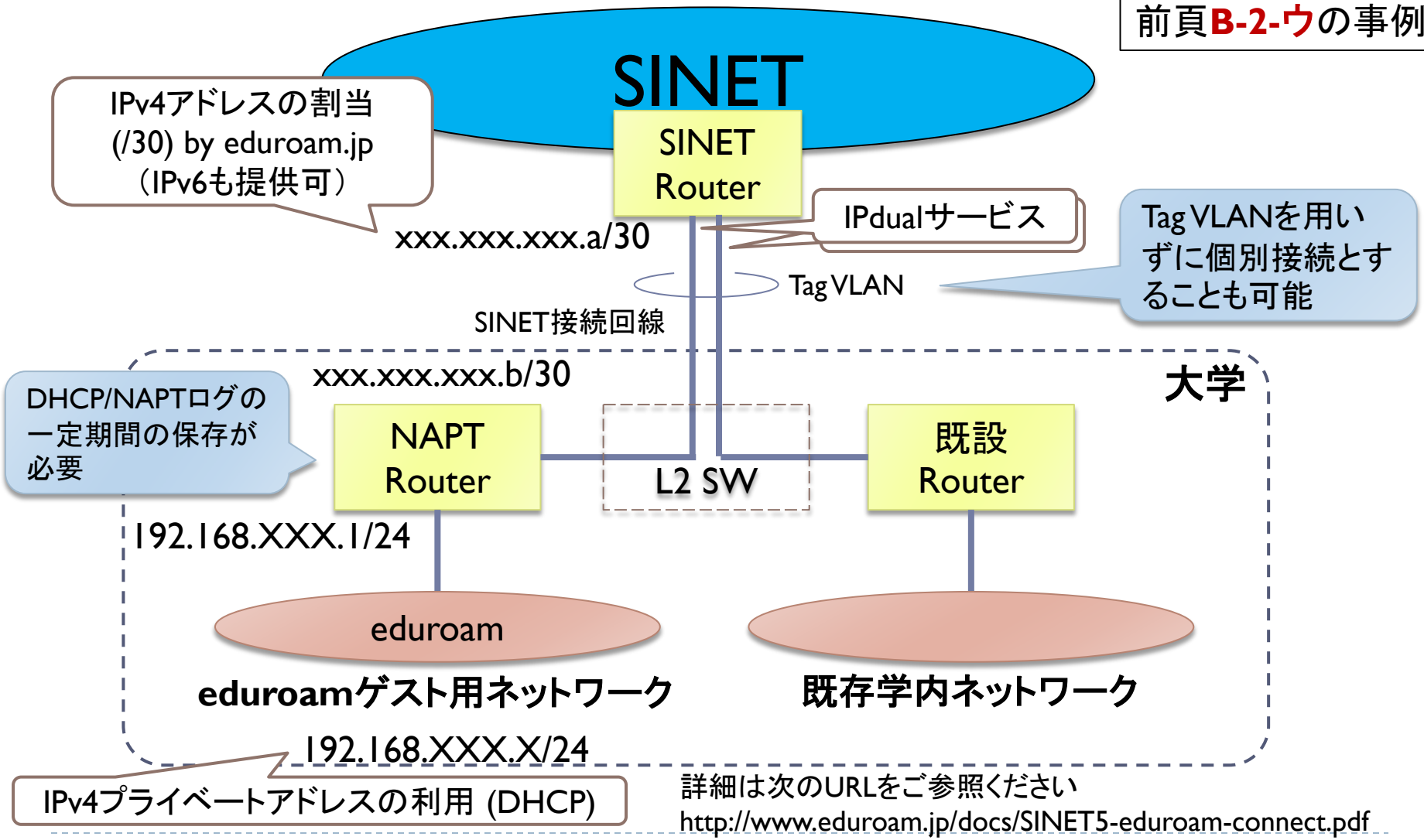
      ア) 新たに商用回線等を導入し、その回線に付随するIPアドレスを利用

      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）

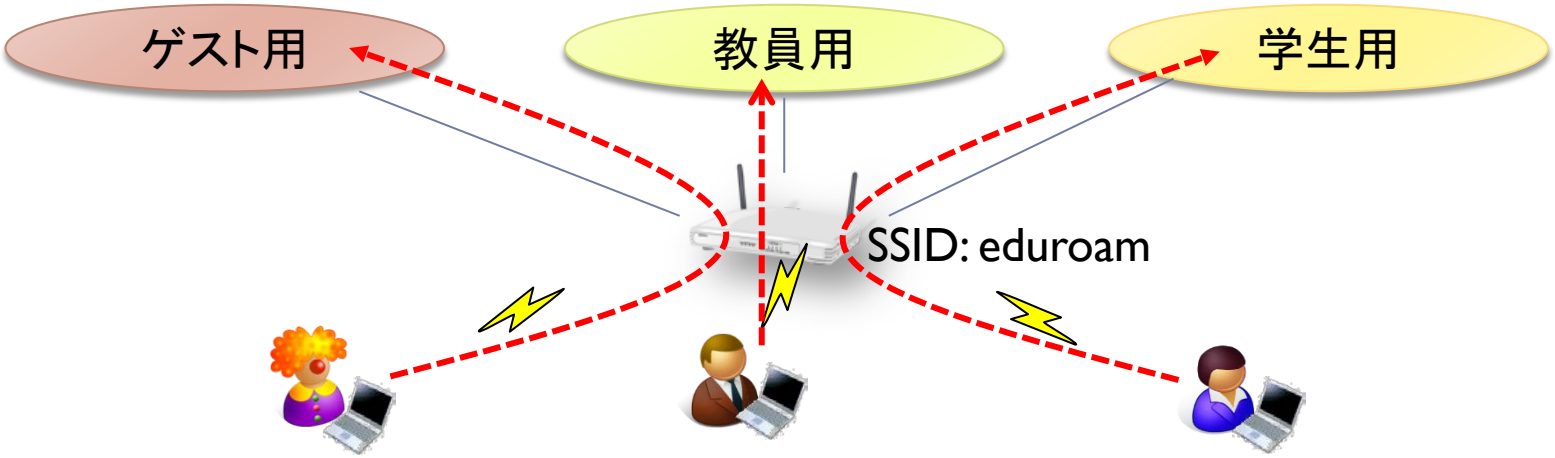
前頁B-2-ウの事例



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

ダイナミックVLANでeduroamに一元化

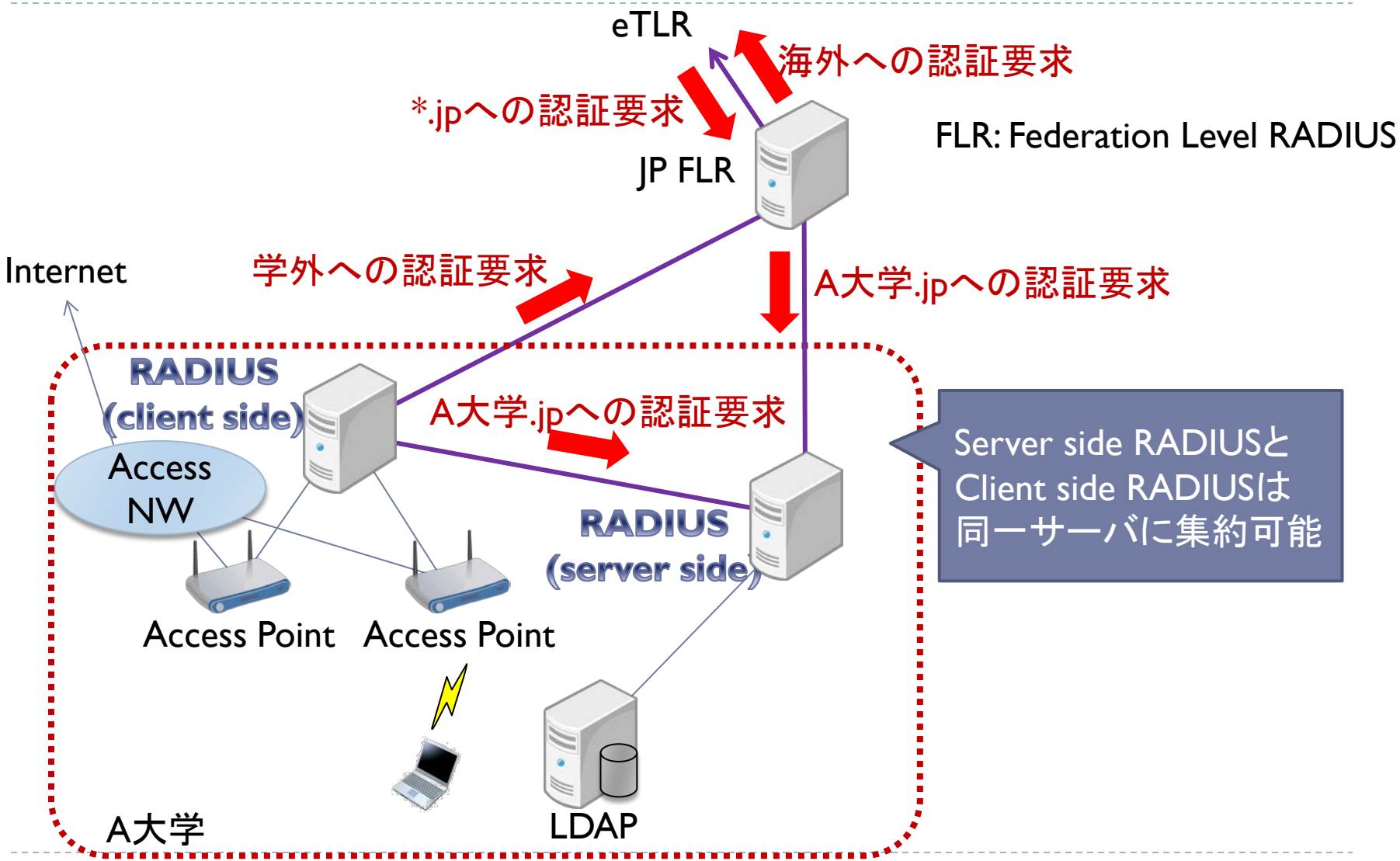
- 同一SSID「eduroam」を用いて
  - 大学関係者とゲストで接続先のVLANを変える
    - 「レルム」に基づく接続先の指定
      - IPアドレス等によりアクセス可能なリソースの範囲を制御したい
      - 常にeduroamの設定のままでネットワークを利用したい
  - さらに、教員と学生とで接続先のVLANを変える、など
    - 認証DBの属性情報に基づく接続先の指定



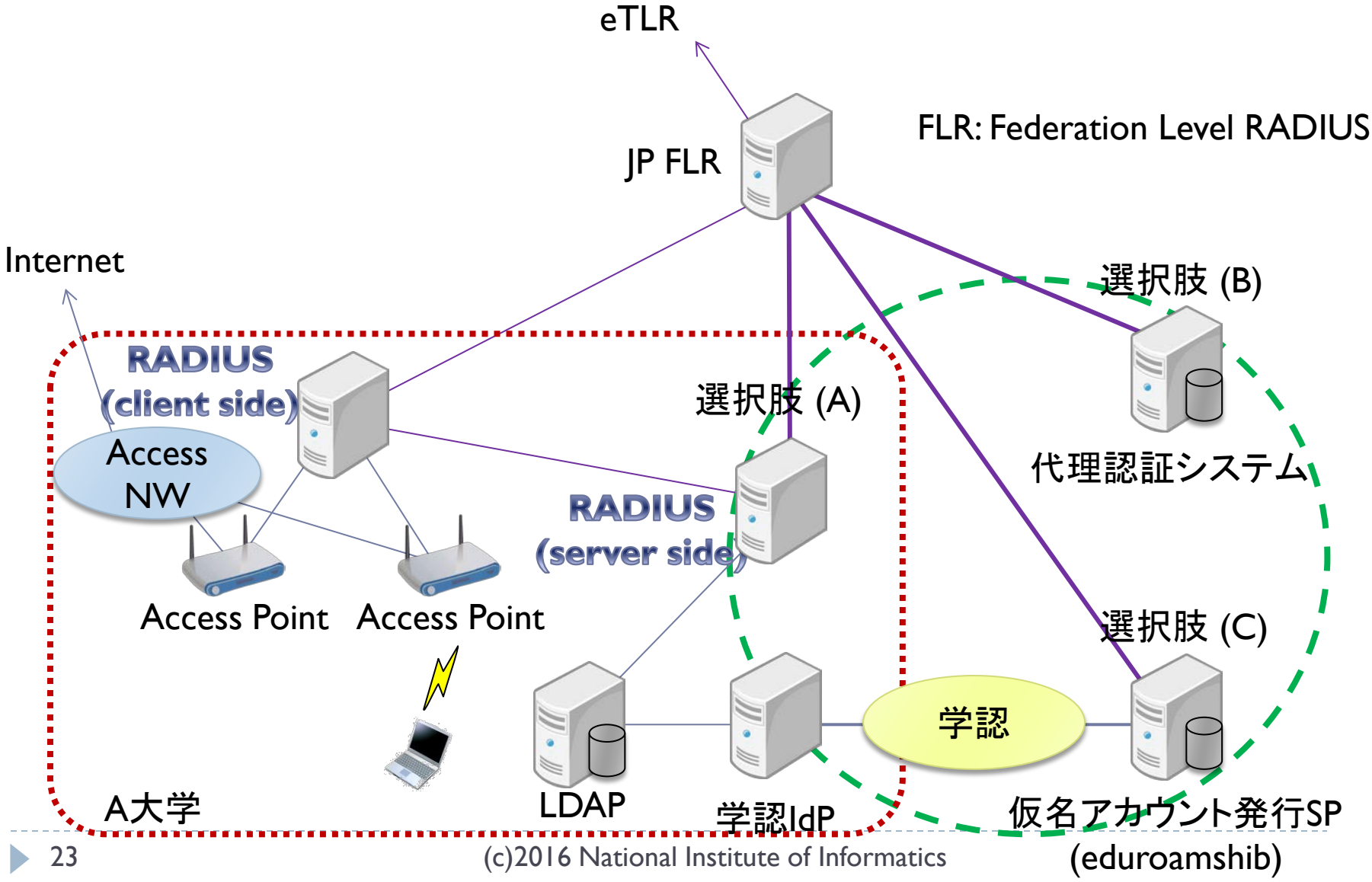
eduroamで提供すべきプロトコル/ポート

- 原則としてプロトコル/ポート制限をかけないこと
  - ステートフルインスペクションやOP25B等の防御的セキュリティ対策は可
- ファイアウォールで制限する場合でも以下は通すこと
  - VPN（NAPT等で技術的な制約がない限り）
    - Standard IPsec VPN – IP/50(ESP),51(AH), UDP/500(IKE)
    - OpenVPN 2.0 – UDP/1194
    - IPv6 Tunnel broker service – IP/41
    - IPsec NAT-Traversal – UDP/4500
    - Cisco Ipsec VPN over TCP – TCP/10000
    - PPTP VPN – IP/47(GRE), TCP/1723（必ず許可）
  - HTTP – TCP/80,443
  - Mail – TCP/143,993,110,995,465,587
- やむを得ず制限する場合は、内容をeduroam JP事務局に連絡すること

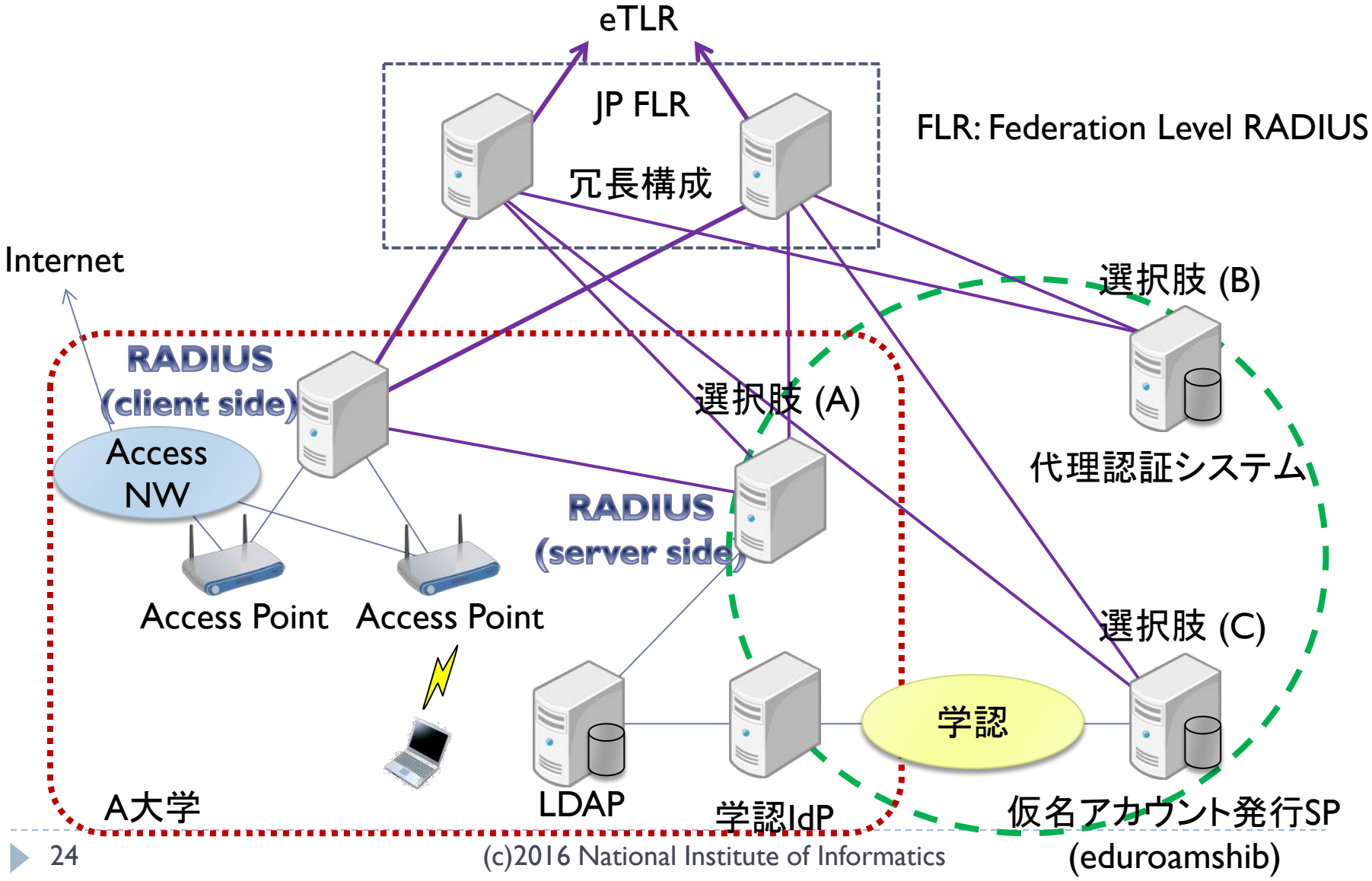
大学でのeduroamシステム構成例（基本）



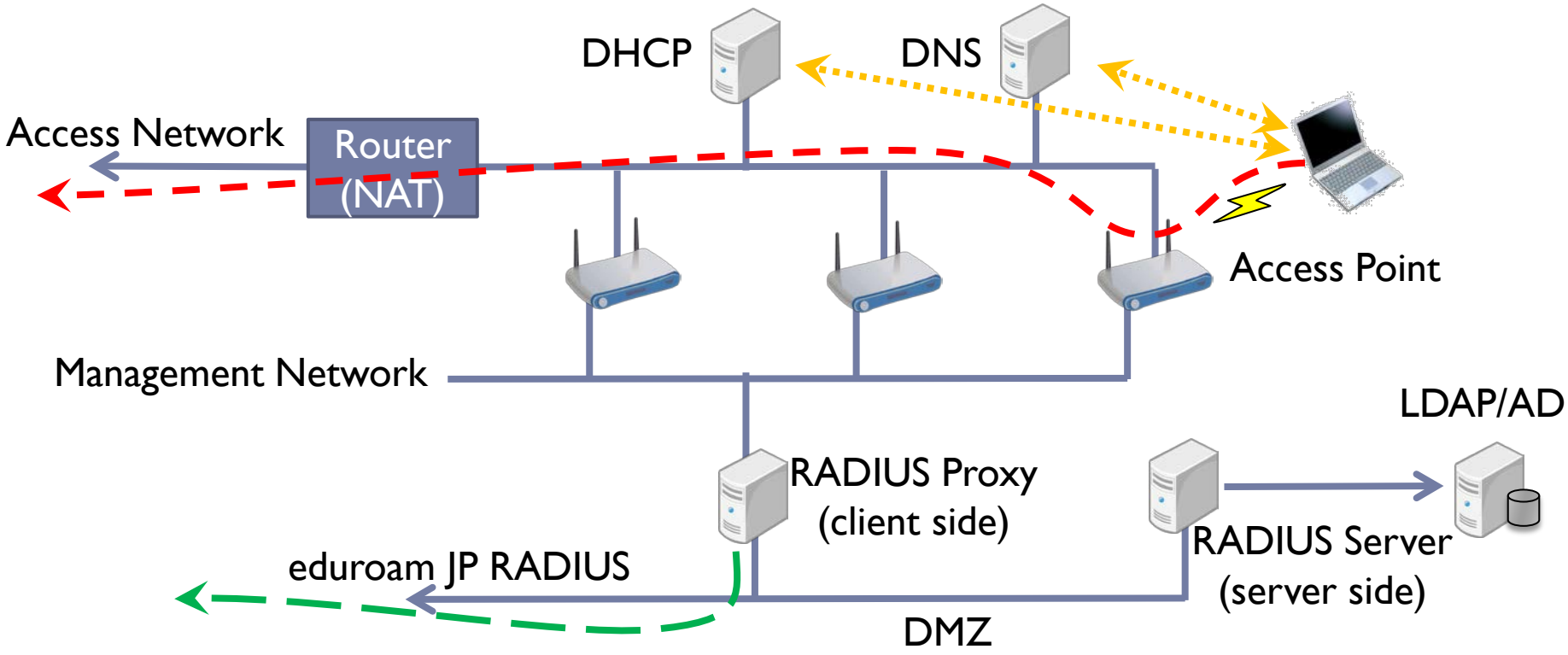
大学でのeduroamシステム構成例（他の選択肢）



大学でのeduroamシステム構成例（冗長構成）



アクセスポイント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)などのログを取得することも検討が必要

eduroamの参加申請方法

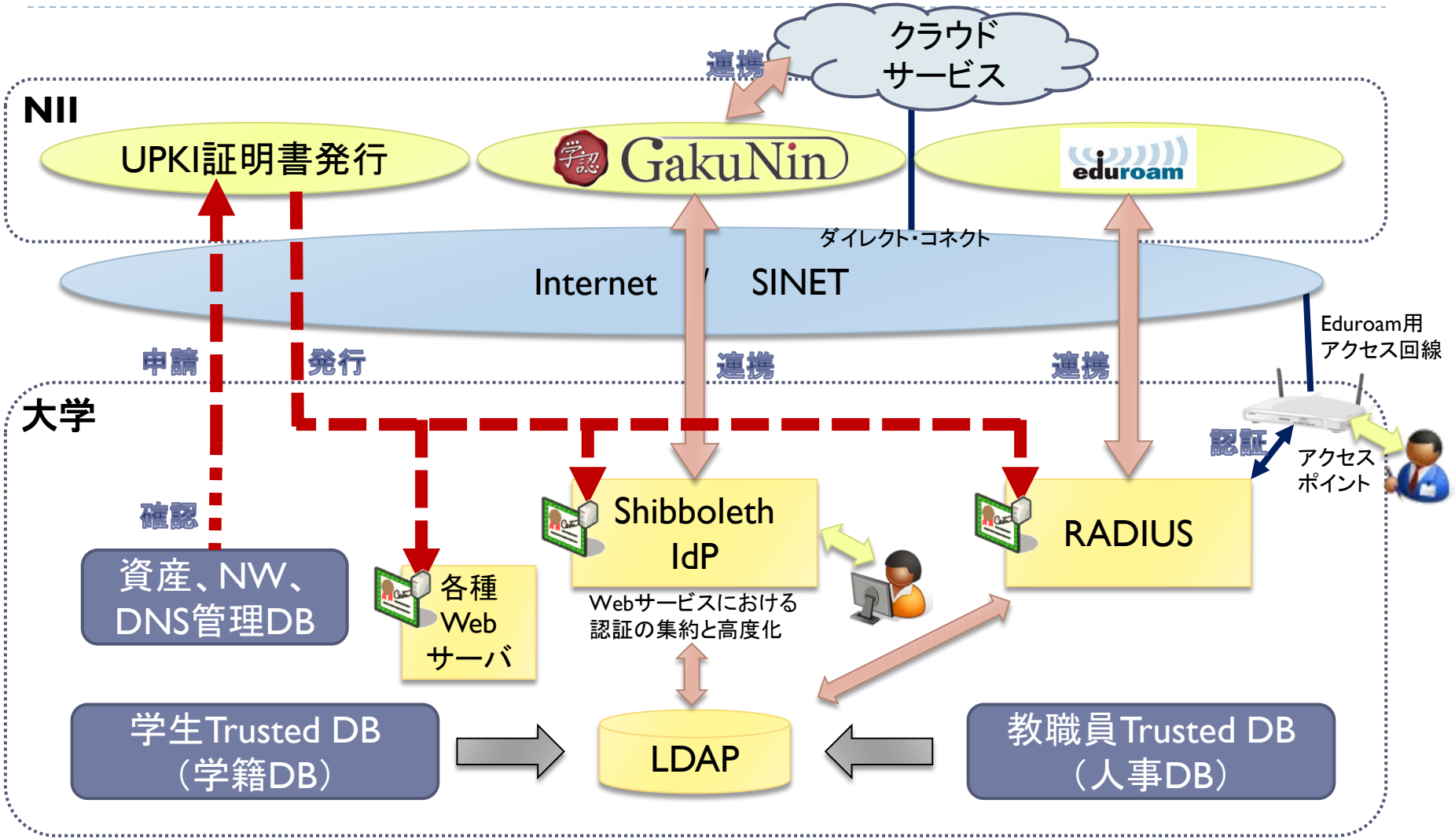
- 認証サーバに関する項目
  1. RADIUSサーバを構築・運用する場合
     - レルム、RADIUSサーバのアドレス、パスワード
  2. 代理認証サービス利用の場合
     - レルム（代理認証サービスの申請）
  3. 仮名アカウント発行サービス利用の場合
     - （別途、学認への参加、IdPリストへの登録依頼）

- 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Wi-Fi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

eduroam全般のお問い合わせ先：
tech@eduroam.jp

NIIが提供するセキュアアクセスを支援するサービスの大学における活用イメージ



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のか（上記のいずれにも当てはまらないとき）