

eduroamの動向と事業化にともなう 今後の運営について

平成28年度 SINET説明会
国立情報学研究所

eduroamの動向

国際学術無線LANローミング基盤「eduroam」

- 教育・研究用の学術無線LANローミング基盤
 - 欧州TERENA(現GÉANT)で開発
 - キャンパス無線LAN相互利用のデファクトスタンダード
- 日本でのサービス名称は「eduroam JP」
 - 加入すると訪問先加入機関の無線LANが無料で利用可能
 - ESSIDは「eduroam」で世界共通
 - IDは「[ユーザ名@組織名.jp](#)」 ex)hoge@example-u.ac.jp
 - 互惠精神に基づく相互利用サービス
- メリット
 - IEEE802.1Xによるセキュアなユーザ認証
 - 偽基地局による各種攻撃への対策が可能
 - Windows/Mac/スマートフォン等に対応
 - 来訪者用ネットワークの随時構築が不要

erudoam JPサービス

- 2006年9月より運用開始

- 実証実験プロジェクト
- ネットワーク運営連携本部 認証作業部会による運営
- RADIUS Proxy以外にも様々なシステムを開発・運用
 - 仮名アカウント発行システム
 - 代理認証システム
 - 会議向けアカウント発行システム

- 加入機関数

- 国内: 161機関(2016/11現在)
- 関東圏の会議場、カフェ等に約130のアクセスポイント

- 2016年4月よりNIIが正式事業化

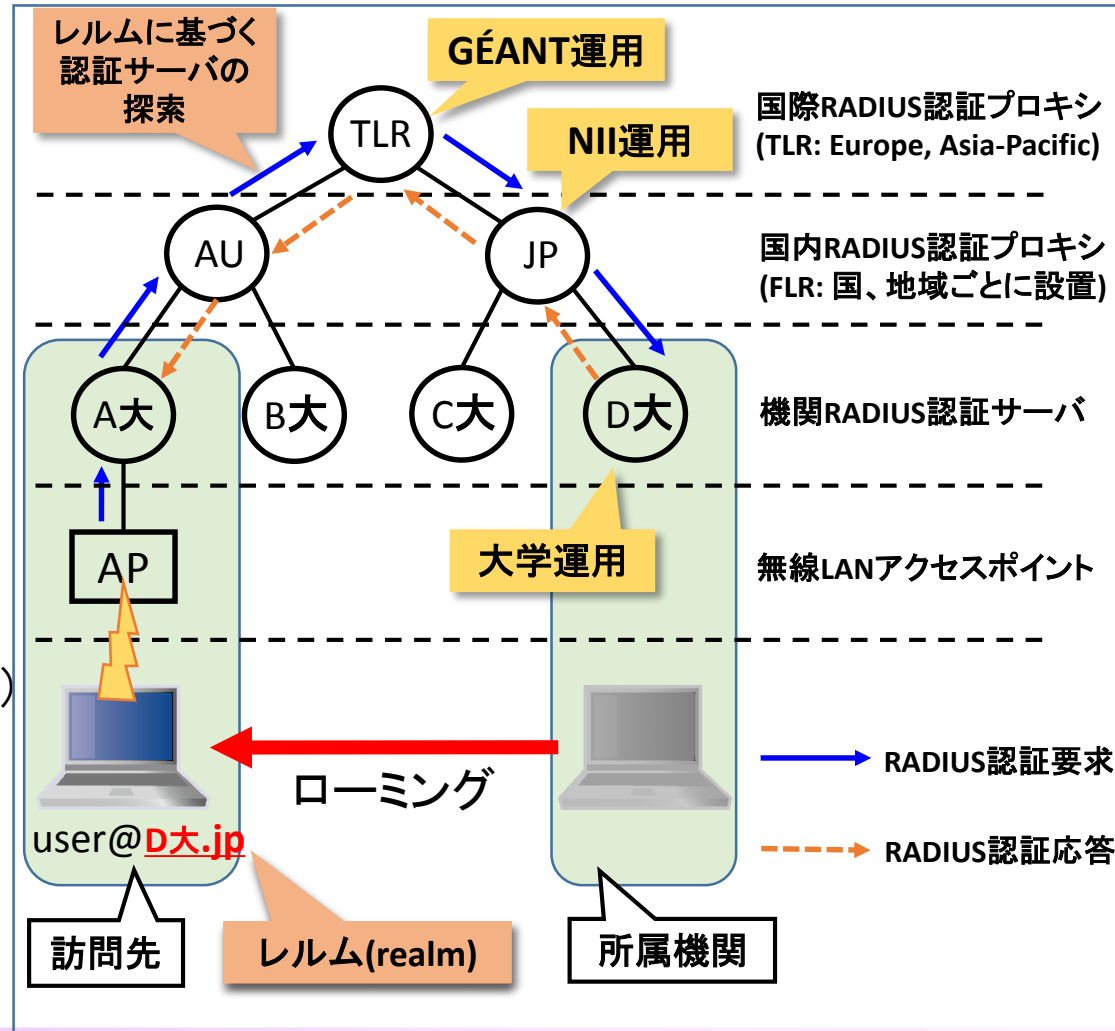
eduroamの仕組み

• 互惠精神に基づく相互利用サービス

- 加入機関の構成員は他の加入機関の無線LAN環境を利用できる
- 加入機関は他の加入機関の構成員に自組織の無線LAN環境を提供する

• IEEE802.1Xによる認証

- 所属機関のアカウントをそのまま利用
 - [ユーザID@レルム\(組織名.jp\)](#)
- Web認証より安全
 - 偽基地局による攻撃対策
- クライアント証明書認証も可能



国際動向

- 世界80カ国・地域に普及(2016/09現在)
 - 欧州全域
 - アジア16地域
 - カナダ、USA、ロシア、南アメリカ各国、南アフリカ共和国、カタール、UAEなど
- 2010年GeGC(Global eduroam Governance Committee)発足
 - 各地域からの代表11名
 - 日本からも1名(東北大学・後藤先生)
- APAN(Asia-Pacific Advanced Network)においてIAM-TF(Identity and Access Management-TF)立ち上げ
 - アジアにおける認証連携(SAMLフェデレーション)とeduroamのコミュニティ

国際動向：キャンパス外での普及例

- スウェーデン (SUNET)
 - 空港や主要鉄道駅でeduroam提供
- ノルウェー (UNINETT)
 - 国内14の空港でeduroam提供
- ルクセンブルク市
 - 自治体が運営するHotCityの市街地基地局で利用可能
- ミュンヘン、ヨーク、ポルト、etc.....
 - 市街地で利用可能
- ロンドン自然史博物館、その他

地元のNRENや大学の貢献度大
(経費負担等)

eduroamのアカウント管理方法

A) 機関にRADIUS対応認証サーバを設置

- 機関の認証基盤と連携/非連携
- 認証システム導入時からeduroam対応の検討を推奨
 - 既存の認証基盤に接続できない可能性があるため
 - RADIUS認証対応アプライアンス製品を使う方法もあり

B) 代理認証システム

- eduroam JPが提供するアカウント発行Webサービス
- 機関のRADIUS対応認証サーバ設置不要
- 機関の管理責任者のオンラインサインアップのみで利用可能

C) 仮名アカウント発行システム

- 機関のRADIUS対応認証サーバ設置不要
 - 「学認」のアカウントと連携  GakuNin
 - 利用者は随時eduroam用のアカウントを取得可能
- 新機能: 少数のゲストアカウント発行
 - 少人数の打合せ向け, 打合せ担当教員等による責任で発行, 短期間利用

無線アクセスネットワークの整備

• ゲスト用ネットワークのIPアドレス

i. 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)

ii. 新たにIPアドレスブロックを取得して利用

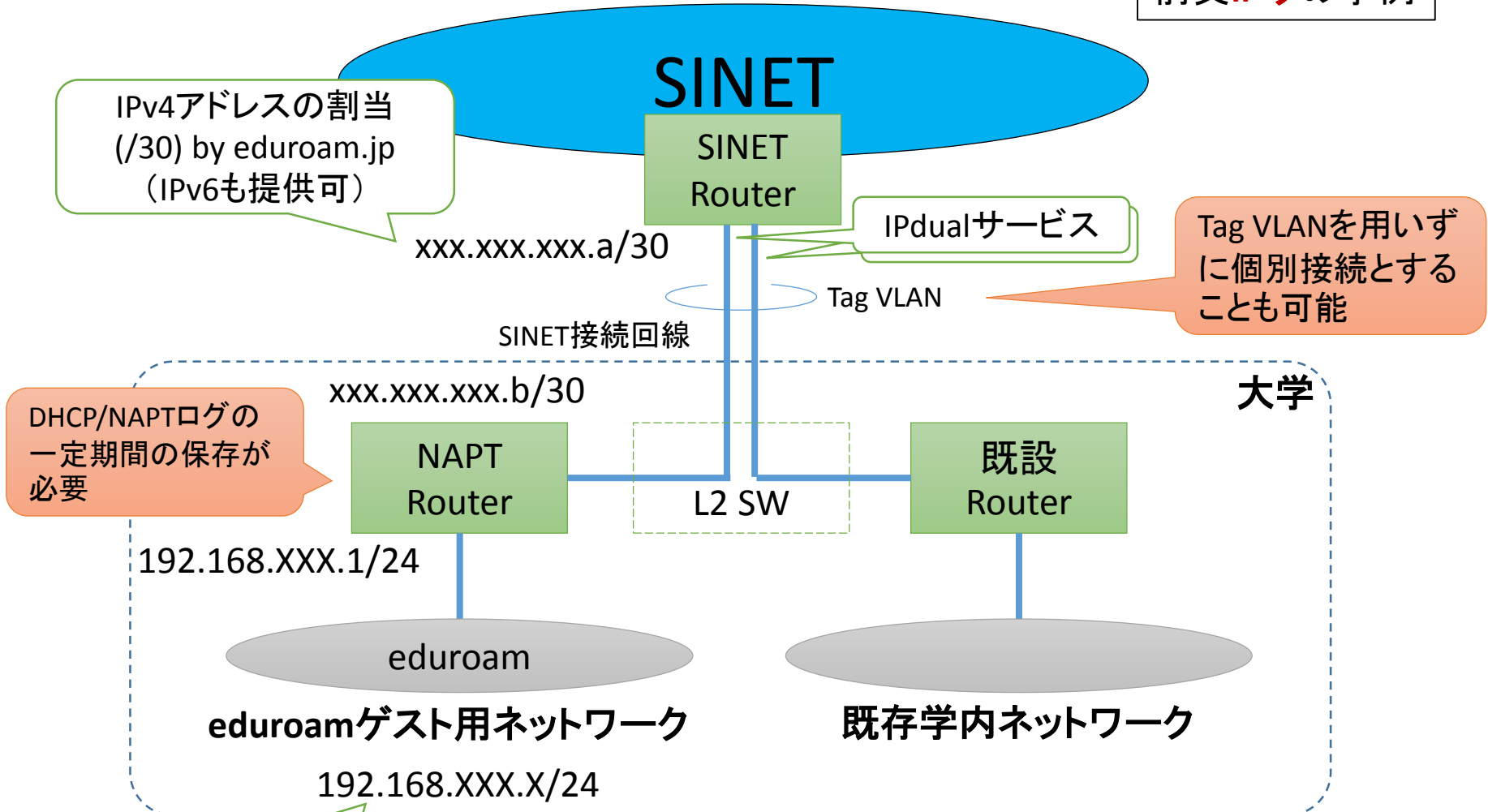
ア) 新たに商用回線等を導入し、その回線に付随するIPアドレスを利用

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、最近では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り当てを受けたアドレス(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)

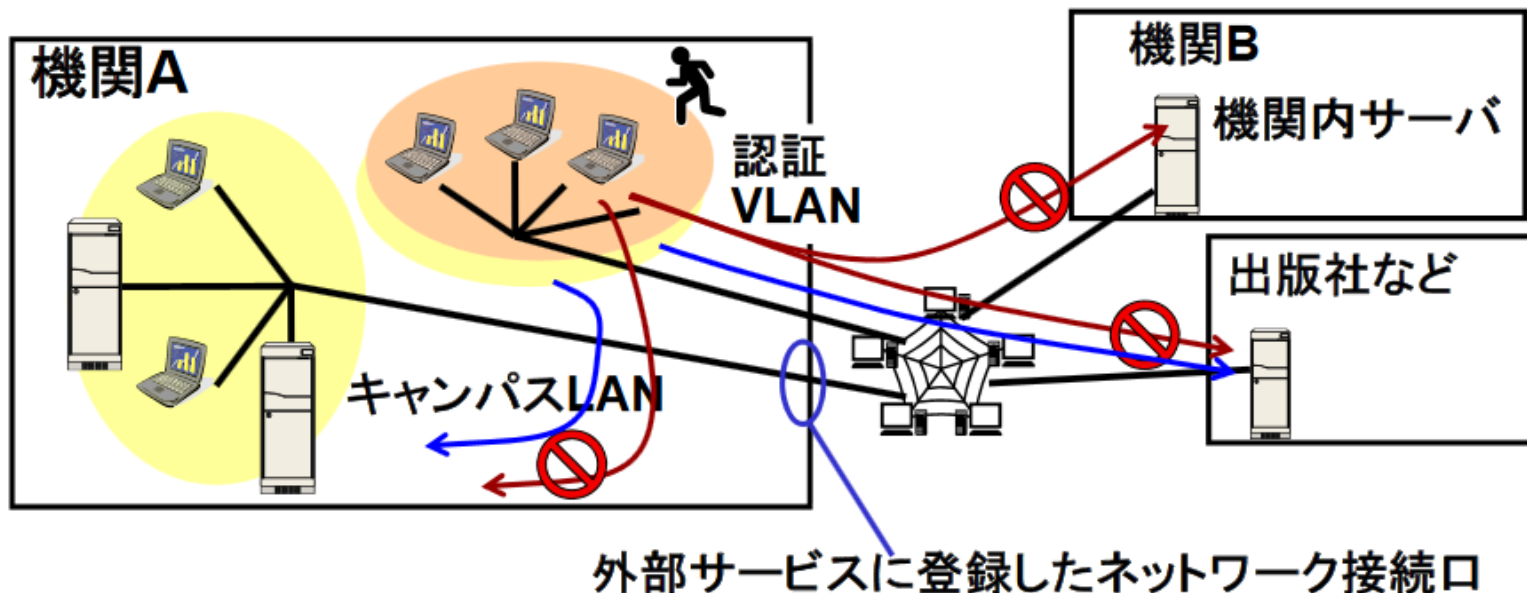
前頁ii-ウの事例



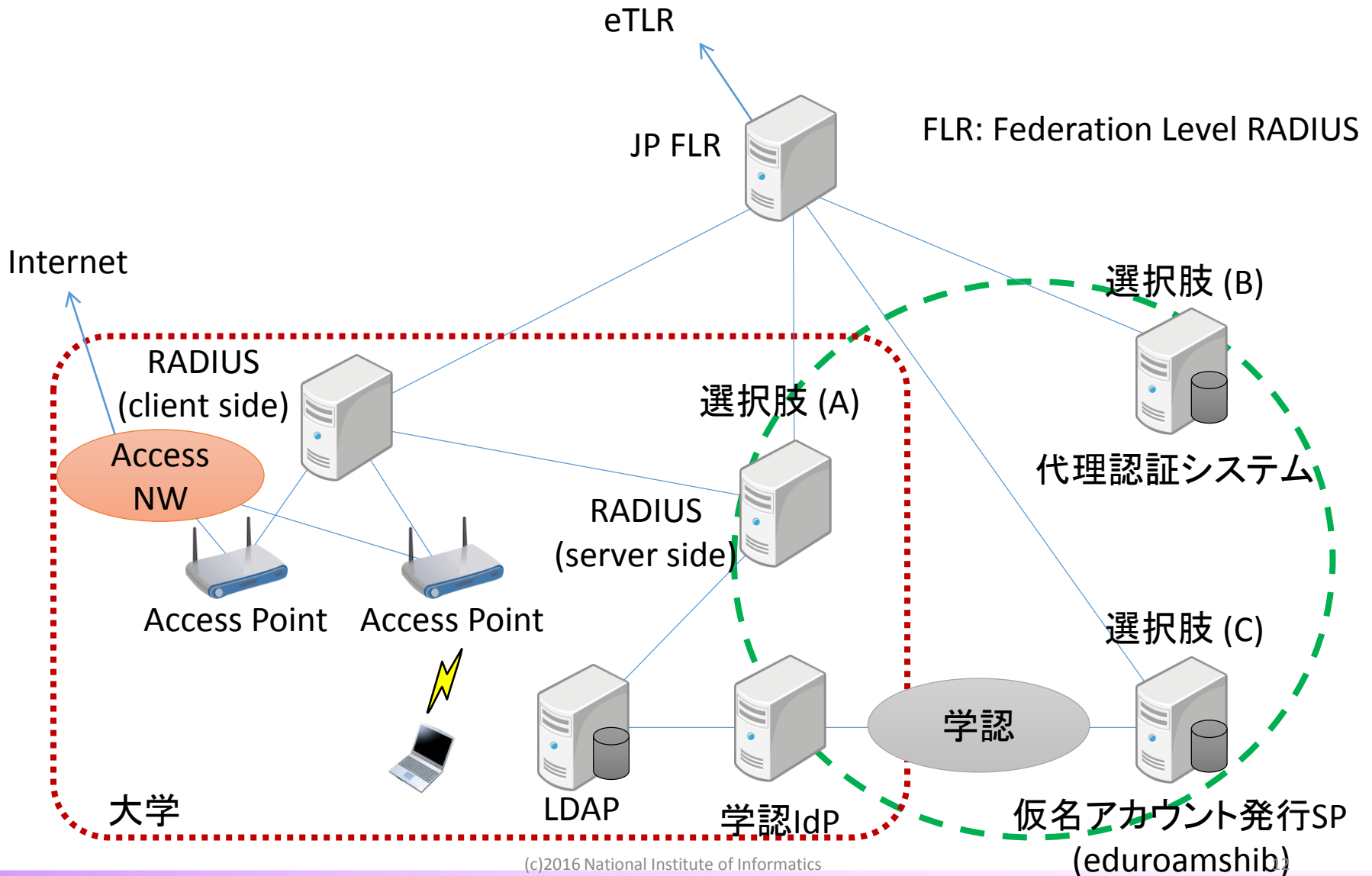
詳細は次のURLをご参照ください
<http://www.eduroam.jp/docs/SINET5-eduroam-connect.pdf>

認証VLAN導入の奨め

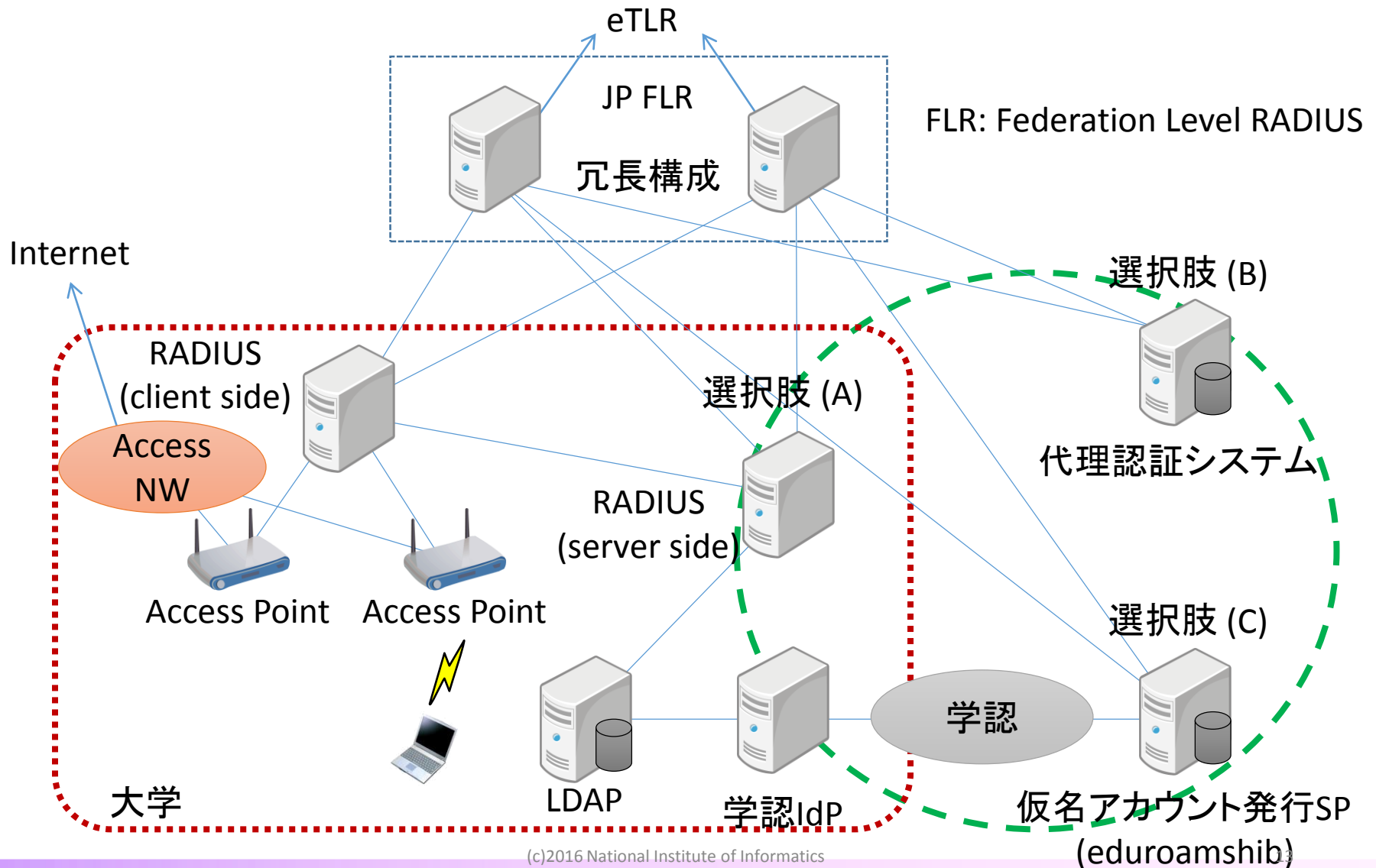
- 一般的なゲスト用eduroamネットワーク
 - 利用者が自機関でeduroam接続を利用する場合も外部アクセスと判定
 - 自機関内での利用時に利便性があまりよくない
- 認証VLAN
 - 利用者による自機関内でのeduroam接続を学内LANに直接収容可能
 - 利便性が大幅に向上



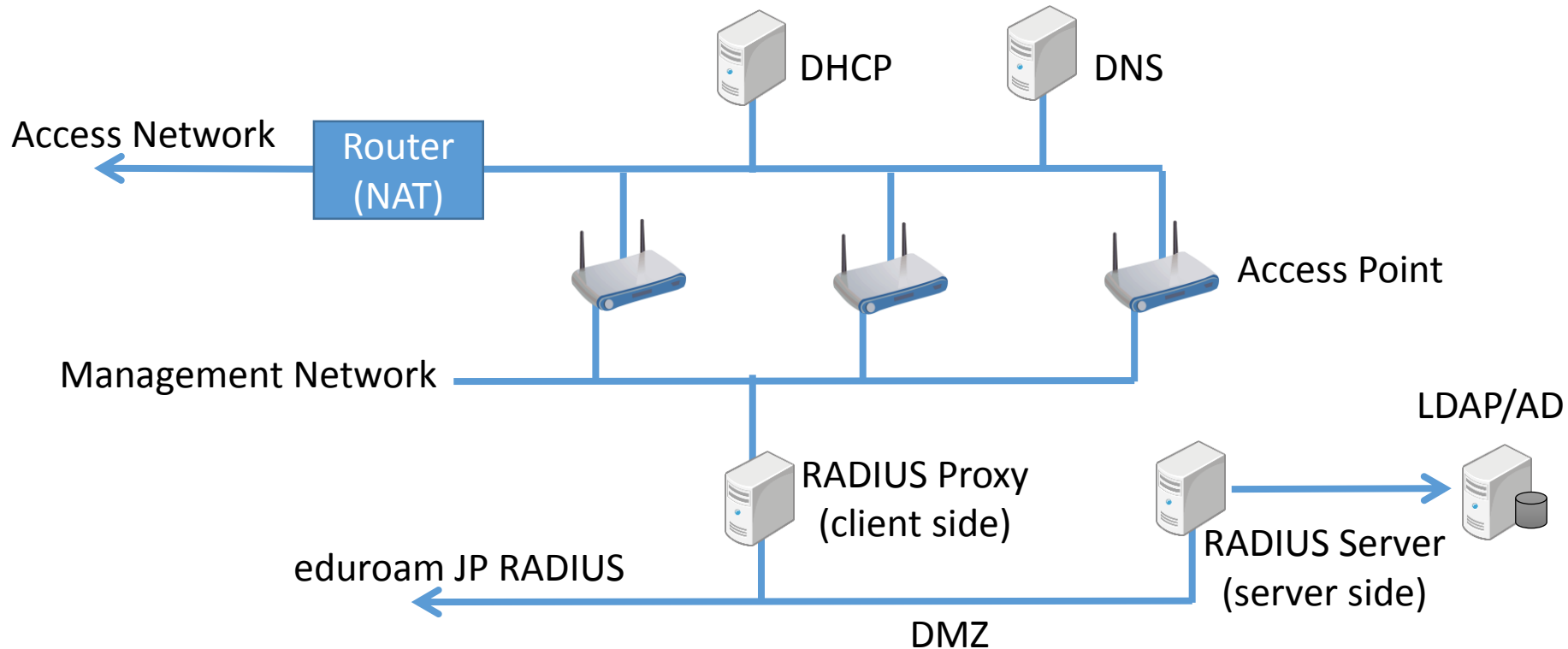
大学でのeduroamシステム構成例



大学でのeduroamシステム冗長構成例



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

参考資料

- 学術基盤オープンフォーラム2016資料
 - 国際学術無線LANローミングサービスeduroamについて

http://www.nii.ac.jp/csi/openforum2016/track/pdf/20160526AM_G_03_nakamura.pdf

事業化にともなう 今後の運営について

eduroam JP運営体制の変更

- 2006/09～2016/03
 - 学術ネットワーク運営・連携本部 認証作業部会による提供
 - 実証実験プロジェクトとして提供
 - 実証研究の一環として試験的な運営
 - 加入機関の増加による対応コストの問題
- 2016/04～2017/03(移行期間)
 - NIIの事業として継続的に提供
 - 東北大学および旧認証作業部会の支援を受けつつNII学術基盤課が提供
 - 運営体制を整備
- 2017/04～
 - 新しい運営体制の下でNII学術基盤課が提供

事業範囲の変更

これまで

認証作業部会による運営範囲

- RADIUS Proxyサーバ運用
- eduroam JP窓口業務
 - 加入・変更・脱退申請の受付
 - 問い合わせ対応
- eduroam JP Webサイト運営
- 仮名アカウント発行システム
- 代理認証システム
- 会議向けアカウント発行システム
- 広報

これから

NIIによる事業化後の運営範囲

- RADIUS Proxyサーバ運用
 - eduroam JP窓口業務
 - 加入・変更・脱退申請の受付
 - 問い合わせ対応
 - eduroam JP Webサイト運営
 - **加入機関向けメーリングリスト運用**
 - 仮名アカウント発行システム
 - 広報
-
- 代理認証システム
 - 会議向けアカウント発行システム
(当面の間, 東北大学の支援により運用)

運営体制移行により整備されるもの

• 規程等の制定

- eduroam JPサービス加入規程、eduroam JPサービス実施要領・運用基準などを準備中

• 申請フォームの整備

- 各種申請書/変更届を準備中
- 加入申請、変更申請/変更届、脱退申請
- フォームが準備でき次第Webサイト等でお知らせいたします

• eduroam運用委員会(仮)の設置

- 規程、実施要領・運用基準等の改訂の議論など
- 海外での活動

• eduroamコミュニティ

- 運用担当者の情報交換メーリングリストを用意いたします

体制変更に伴う加入機関様へのお願い

• eduroam JPサービス加入規程

- 既に参加済みの機関様は引き続き利用可能
- 機関責任者および技術担当者の設置
 - 機関責任者は一人, 技術担当者はレムムごとに二人必要
 - 詳細は後日公開される規程および実施要領・運用基準を参照すること

• 継続参加の意思確認

- 各加入機関様に今後も継続参加いただけるか確認いたします

• 年次運用状況調査の実施(予定)

- 届出どおりの設定で運用されているか
- 運用基準に沿って運用されているか
- 責任者や技術担当者に交代はないか

➤可能な限り煩雑にならないようにいたします

体制変更に伴う加入機関様へのお願い

• 実施要領

- インシデント発生時の処置と責任
 - インシデント発生時は調査へのご協力をお願いします
 - 特に該当アカウントの発行機関様は責任を持って対処・調査・報告・協力をお願いします

• 運用基準

- 技術的要件および制約
 - 認証方式はIEEE802.1Xのみ
 - 基地局マップなどの運用状況データの提出
 - 各種ログの記録と保存
- プロトコル制限についての制約
 - 原則として制限をかけないこと
 - やむを得ず制限を掛ける場合は制限対象のプロトコルを利用者に公知

継続参加の意思確認

- 2017年1月～3月まで
 - 制定された規程および実施要領・運用基準への同意
 - 新体制による運営への同意
 - 各加入機関の責任者・技術担当者の方に連絡いたします
- 責任者および技術担当者について
 - 現在の届出から交代がある場合、変更のご連絡をお願いします
 - 継続参加の意思確認の連絡をはじめ、大切なお知らせが届かない可能性があります

その他のeduroam JPのシステム

- 代理認証システム
- 会議向けアカウント発行システム
 - 上記二つについては開発・改良を継続中であるため、当面の間、東北大学様の支援を受けて運用

その他

- RADIUS JP Proxy更新に伴う接続先切り替え
 - RADIUS JP ProxyサーバのIPアドレスの変更が必要です
 - 各機関様のRADIUSサーバ設定変更をお願いいたします
 - 切り替えの時期についてはWebサイトで告知、
および機関責任者・技術担当者の方に連絡いたします

お問い合わせ先

参加の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