慶應義塾

慶應義塾におけるeduroam提供

慶應義塾ITC本部
細川 達己

NII 大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
学術情報基盤オープンフォーラム2017

内容

1. 慶應義塾におけるeduroam提供の概要
2. eduroam対応システムの構成・構築・注意点
3. 提供開始以来の利用状況
4. まとめ・今後の課題

慶應義塾におけるeduroam提供状況

- **時系列**
  - 2015年6月　参加申請・開発開始
  - 2015年9月　試験運用開始
  - 2015年12月 運用開始
- **学内の対象ユーザ**
  - 学生・教職員：合計約45,000名
- **アクセスポイント**
  - 全主要6キャンパス＋一部サテライトキャンパス（新川崎、鶴岡）のITC設置全Wi-Fiアクセスポイント
- **開発**
  - OSS利用で内製

https://monitor.eduroam.org/eduroam_map.php?type=jp
（三田キャンパス近辺）

学内ユーザの認証方法

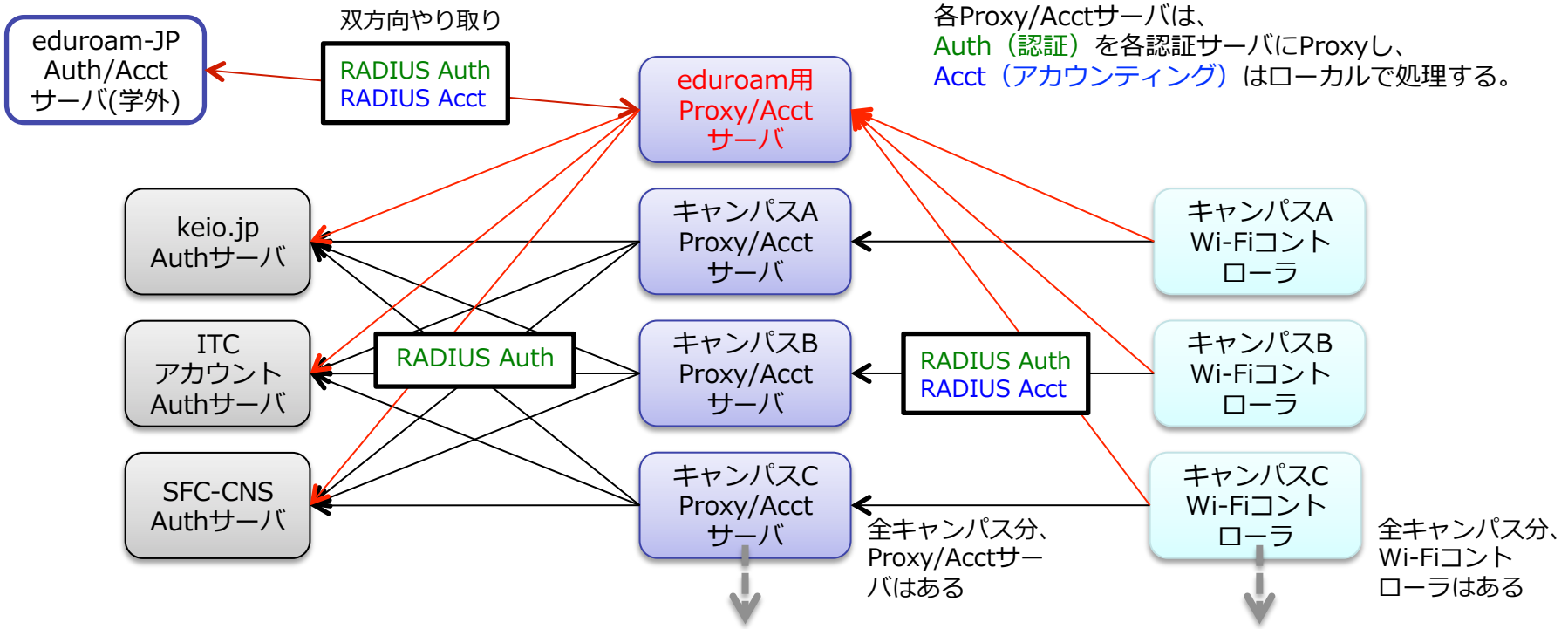
- **既存のWi-Fi用RADIUSインフラを利用**
  - keiomobile2という802.1X認証のWi-Fiが提供済みだった
  - レルムが@keio.jpと@*.keio.ac.jpの両方あるがeduroam-JP的には特に問題ない
- **PEAPのパスワードは通常のログイン用のものとは別**
  - Webインターフェースで独自のパスワードを取得する
  - 複雑で長いランダムパスワードを発行・更新

利用可能なID	対象	レルム名	認証方法
共通認証システム	全学	@keio.jp	EAP-PEAP
ITCアカウント	全学	@user.keio.ac.jp	EAP-PEAP
SFC-CNS	湘南藤沢	@sfc.keio.ac.jp	EAP-PEAP/EAP-TLS

表：keiomobile2で利用可能なRADIUS認証サーバ
(eduroamでも同様に利用可能とした)

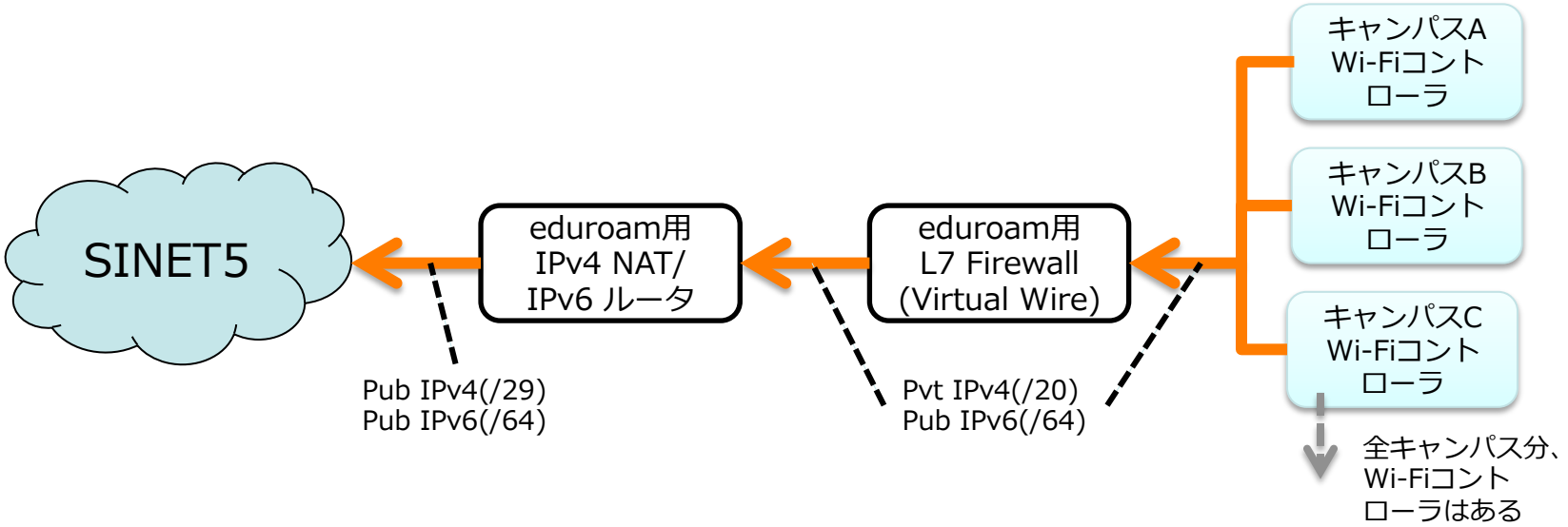
RADIUSインフラにeduroam対応追加

- **eduroam用RADIUS Proxy/Acctサーバを追加**
  - 各キャンパスのSSID:eduroamによるRADIUS Auth（認証）とRADIUS Acct（アカウンティング）をこのサーバに送信
  - eduroam-JPサーバとは、AuthとAcctを双方向に送受信



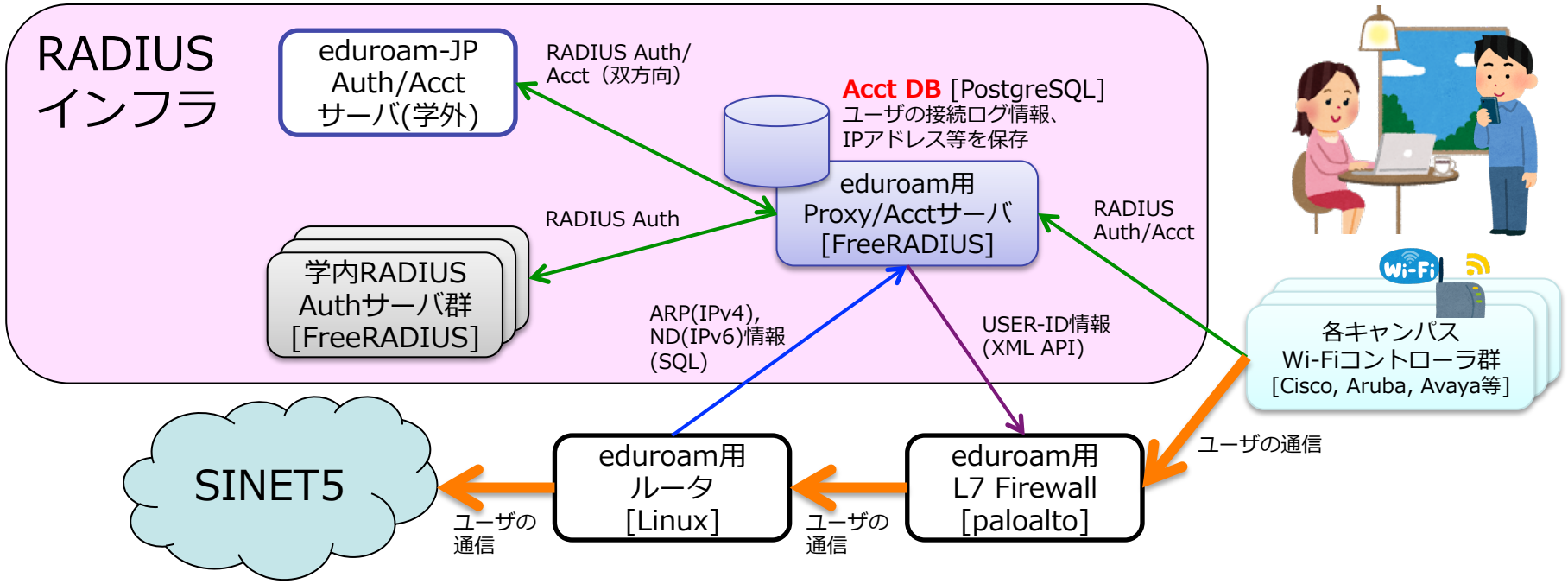
提供ネットワークとユーザトラフィック

- **SINET5のeduroam用ネットワークを提供**
  - 通常の学内ネットワークとは別ネットワーク
  - IPv4はNATによるプライベートネットワーク(/20)
  - IPv6はグローバルネットワーク(/64)
  - ルータはLinuxで構築（スクリプトを動かすため）



慶應義塾eduroamシステム構成概要

- **FreeRADIUS+PostgreSQLでAcct DBを記録**
  - 負荷軽減と検索・更新の簡便さのため
- **ルータがIP・MACアドレス対応をAcct DBに記録**
  - この結果を元に、ユーザとIPアドレスの対応をFirewallに設定



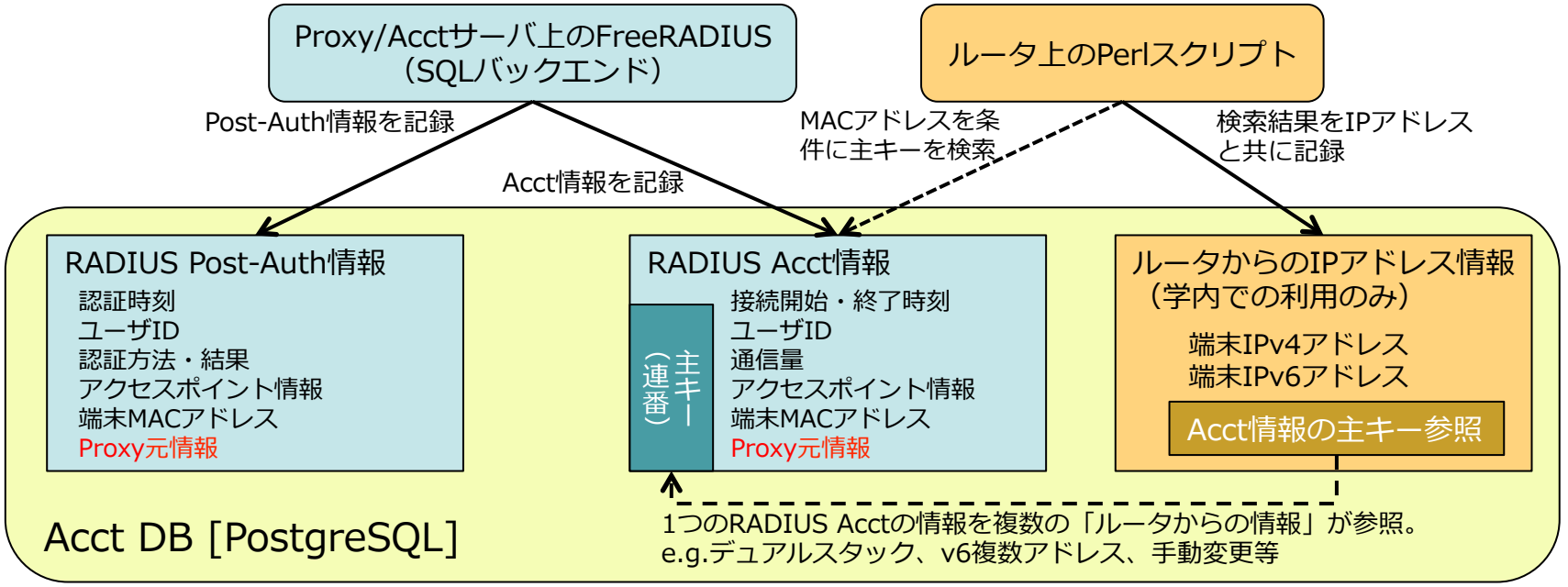
eduroamにおけるRADIUS関連注意点

- **RADIUS Acctを送らない参加組織**
  - 学内ユーザの学外でのeduroam利用時、信用できる記録はPost-Authログ
  - Acct情報は来ないことがある
- **匿名IDを利用する学外ユーザ**
  - TLSチャネルを匿名IDで要求
    - 「anonymous@レルム名」等
  - TLSチャネル内でリアルなIDで認証を行うが、AP側のログに残るのは匿名IDのみ
  - 特に実害はないが知っておこう

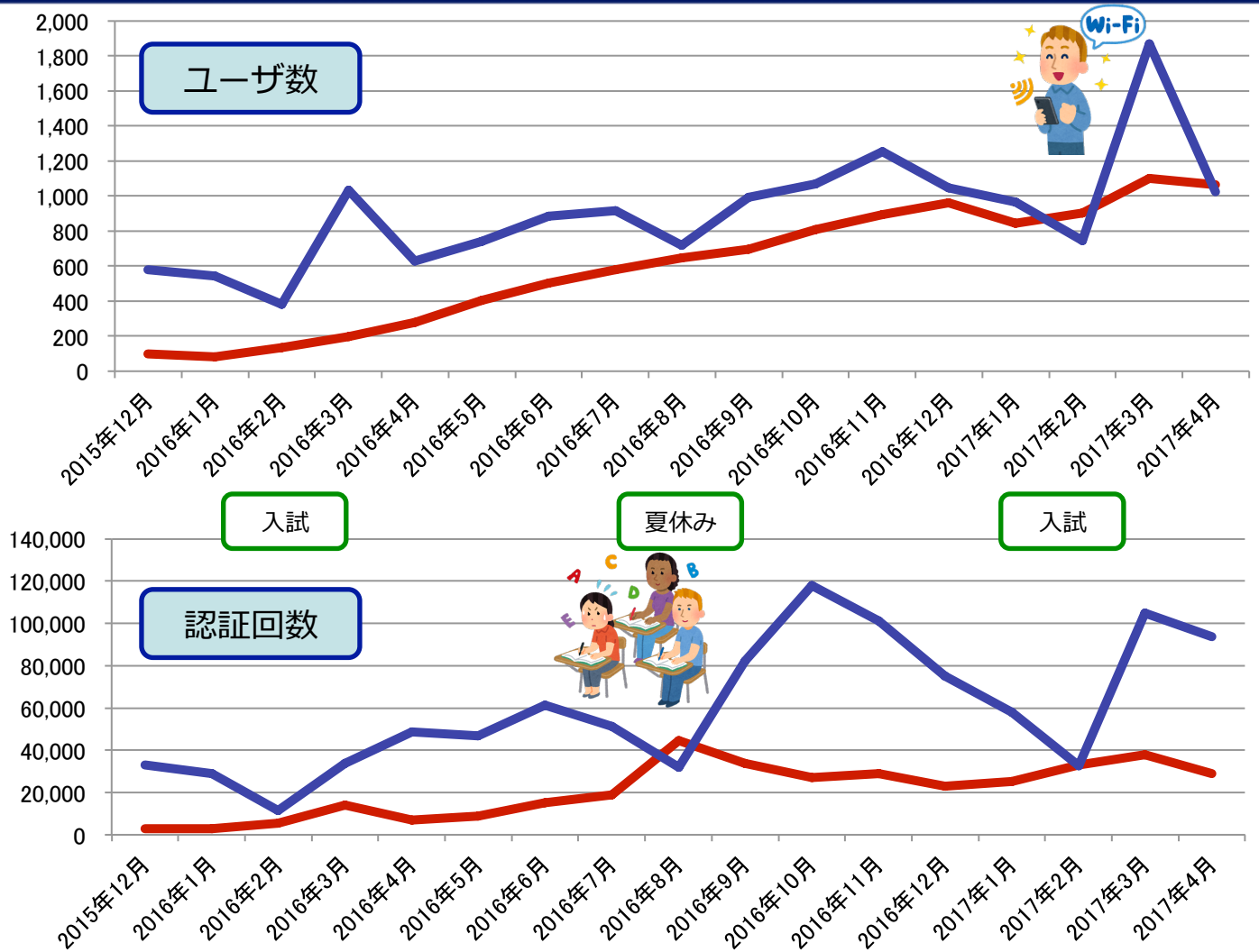
anonymous@realm
guest@realm

Acct DBに記録する情報

- **主なテーブル**
  - RADIUS Post-Auth情報（学内外問わず認証結果を記録）
  - RADIUS Acct情報（主に学内APでの利用状況を記録）
  - ルータからのIPアドレス情報（もっぱら学内APでの利用状況を記録）
- **「Proxy元情報」とは？**
  - クライアント短縮名（clients.confのshortname、標準では記録されない）
    - 認証要求がeduroam-JPからのものか各キャンパスからのものか等を判別



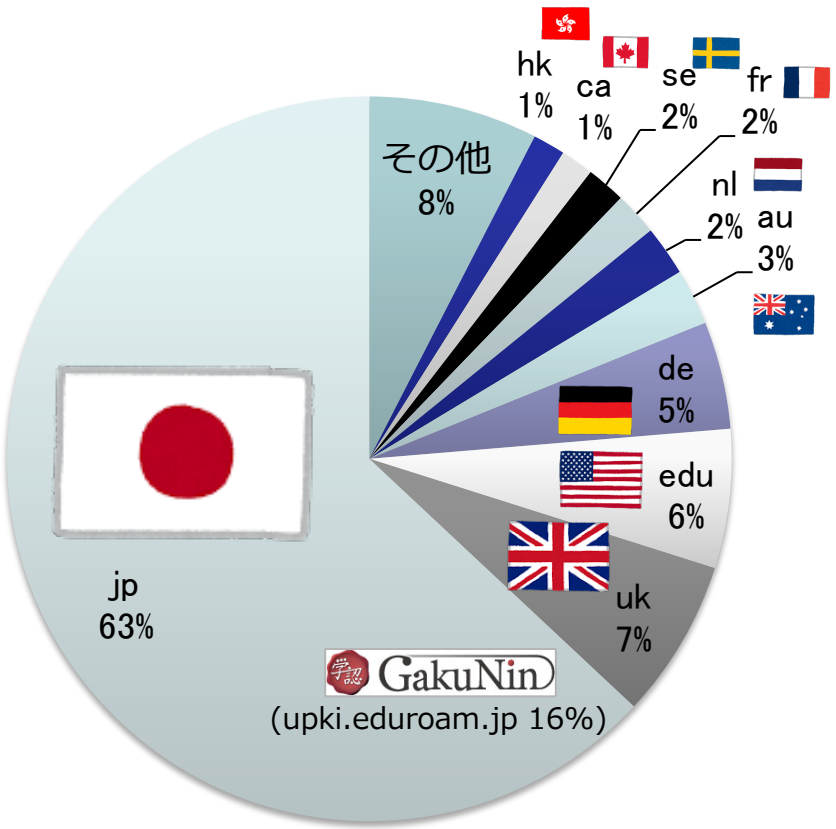
慶應義塾におけるeduroam利用状況



学内ユーザ：
学外組織での利用
学外ユーザ：
学内での利用
(匿名IDは1ユーザ/レルム扱い)

学外ユーザのTLD内訳（2016年度）

- **学外ユーザ数での集計**
  - 学内ユーザは対象外
  - 匿名IDは1ユーザ/レルム扱い
- **全体の63%がjpドメイン**
  - 学認仮名アカウント16%
- **欧州のドメインが多い**
  - その他（ユーザ数降順）：
    ch, it, be, at, es, dk, sg, cn, no, cz, th, kr, fi, pt, pl, tr, tw, ie, is, nz, cat, eu, za, si, rs, mo, lt, hu, gr, com, sk, sa, mt, il, hr, gov, br



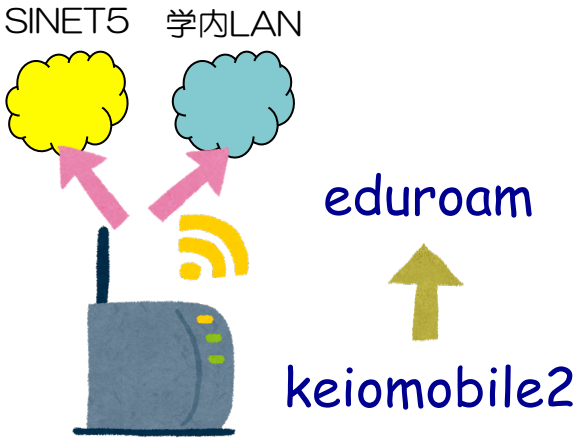
総計6,870ユーザ

その他苦労した点

- **導入に向けての調整**
  - 主に教員から「eduroamを入れて欲しい」と要望があったのが追い風となった
  - インシデント対応等に対する懸念なども、L7 Firewallの運用経験を積んできたことなどもあり、軽減することができた
- **拠点間でRADIUS用プライベートアドレスが衝突**
  - 調整して片方にリナンバーしてもらった

今後の課題

- **利用者が増えてきたので拡張したい**
  - 本システムでルータの並列配置が可能か？
    - 1つのLANに複数ルータを置くと、DHCPとNDが両方のルータとネゴしてしまう模様
    - キャンパス等でルータを分けた方がいい？
  - SINETからのアドレスはおかわり（拡張）済
    - 今はプライベート側アドレス拡張で一息…
- **認証VLAN化で学内WiFiとの統合**
  - keiomobile2との統合
    - トラブル確認は学認仮名アカウントで？
    - あまりトラブル報告が来なくなるのでは？
  - 全拠点で提供可能かどうかなど、検討中
    - 様々なメーカーのAPがある上に、コントローラ配下にないものも



ありがとうございました。

（おまけ）基地局マップ情報を登録しよう
http://www.eduroam.jp/docs/mapdata.html