

# eduroam JPのサービスについて

末永光弘(国立情報学研究所)

2017年6月7日 NII学術情報基盤オープンフォーラム

# erudoam JPサービス

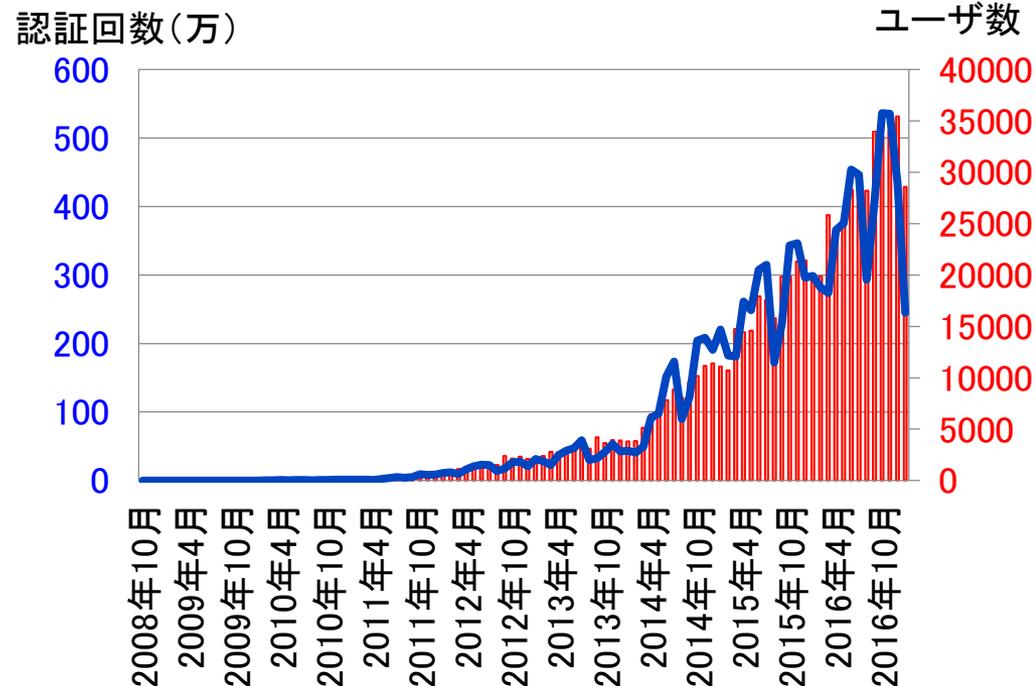
- 2006年9月より運用開始

- 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
    - 機関向け利用サービス
    - 会議向け試行サービス

- 加入機関数

- 国内: 179機関 (2017/4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 JP運営体制の変更

## • 2006～2016

- 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

## • 2016～2017(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～

- 新しい運営体制の下でNII学術基盤課が提供

# 新たに明文化・整備されるもの

## • 規程等の制定

- 学術無線LANローミング基盤サービス加入規程(2017/2/7公開)
- 学術無線LANローミング基盤サービス eduroam JP実施要領(2017/4/19公開)
- 学術無線LANローミング基盤サービス eduroam JPサービス技術基準・運用基準(2017/5/XX公開)

## • eduroam JP申請システムの運用

- 加入申請、変更申請、脱退申請の受付
- 7月稼働開始予定

## • eduroamグループの設置

- 規程、実施要領、技術・運用基準等の改訂の議論など
- 海外での活動や海外のコミュニティとの連携

# 加入機関様へのお願い

- 継続参加の意思確認をいたします
  - 申請システムより改めて加入申請をお願いします
    - システムからの加入申請をもって継続参加希望とさせていただきます
  - 加入規程、実施要領、技術基準・運用基準をご一読の上、継続の可否をご判断ください
  - 継続の意思を確認するまでは、引き続きご利用いただけます
- 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

## 加入機関様へのお願い

- 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
- 技術的要件および制約
  - 基地局マップなどの運用状況データの提出の義務化
    - 未提出の機関様にはご提出をお願いいたします
  - 各種ログの記録項目と保存期間の明文化

# 継続参加の意思確認

- 確認期間: 2017年7月～12月まで
  - 制定された規程および実施要領、技術基準・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
- eduroam JP申請システムからの申請を再度お願いします。

# その他のeduroam JPのシステム

- **RADIUS JP Proxy更新に伴う接続先切り替え**
  - RADIUS JP ProxyサーバのIPアドレスの変更を予定しています
  - 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
- **代理認証システム**
  - これまで通りご利用いただけます
- **仮名アカウント発行システム**
  - **認証連携IDサービス**として更新します
  - 詳細は次の講演で！

# 利用者様へ

- 利用方法等の変更はありません

- 所属機関が継続して加入する場合はこれまでどおりご利用いただけます
- 仮名アカウント発行システムは認証連携IDサービスに移行します
  - 認証連携IDサービスより発行される学生用アカウントは有効期間が3か月となります。
  - その他の変更については次の講演で！

加入規程  
實施要領  
技術基準・運用基準

# 加入規程

## • 加入対象の明文化

- 高等教育研究機関と関連組織
  - 高等教育研究機関が設置する組織
  - 高等教育研究機関を支援する組織
- 学会、学術研究法人、大学相当の教育施設
- 研究を目的とするネットワークの参加機関
- eduroam SPを提供する事業者
- その他、特に認めた機関・組織

# 加入規程

- 機関責任者
  - 課長職以上、または教授相当以上の方  
または、サービスの運用を担う部門の長
- 技術担当者
  - eduroamで使用する機器の運用等を担当
  - 二名置くこと
  - 一名は機関責任者と兼任可能
- 不正利用等の調査協力義務

# 実施要領

- 加入申請手続き

- SINET加入機関

- 機関の長の公印と郵送を省略可能

- SINET非加入機関

- 機関の長の記名・公印の押印と郵送が必要
    - 加入後は一定条件を満たせば公印と郵送を省略可能

- 利用者への対応

- 加入機関の担当部署は自組織の利用者向けに問い合わせ受付窓口を設置し、問い合わせ先を開示してください

# 実施要領

- eduroam JP運用連絡会
  - 加入機関の機関責任者、技術担当者の連絡先を登録いたします
  - インシデント対応のため、インシデントに関係する機関の担当者連絡先をお互いの機関に開示することがあります

ご理解とご協力をお願いいたします。

# 技術基準・運用基準

- eduroam IdPの技術基準・運用基準

- アカウント管理について
- 自機関の利用者への対応
  - 問い合わせ窓口の設置
  - 不正利用に対する指導と啓蒙
- ログに記録する項目と保存期間
  - 期間は最低6か月
  - 機関ごとに定めがある場合は応相談(より長いのはOK)
- 複数レルムとサブレルムについて
  - JP RADIUS Proxyは同一機関が使用するすべてのレルムの転送先を一つにまとめています
  - サブレルムの処理がeduroam JPのサーバに戻らないよう処理してください

# 技術基準・運用基準

- eduroam SPの技術基準・運用基準
  - 基地局マップの提出の義務化
  - ログに記録する項目と保存期間
    - 期間は最低6か月(期間についてはIdPと同様、応相談)
    - 項目がIdPと少し違います
      - ARP sniffingログ、DHCPログ等
      - NAPTを利用する場合はアドレス/ポート変換のログ
  - 障害情報の公知
    - 実施要領にも書いてますが、自機関・他機関の利用者に障害情報をわかりやすく開示してください。
      - ウェブサイトへの掲載など

# 技術基準・運用基準

- 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
  - やむを得ず制限をかける場合は制限対象のプロトコルを利用者に公知
    - 制限する場合はeduroam JPに届け出ること
  - 詳細はeduroam JPの規程類およびWebサイトをご覧ください
    - URL: [https://www.eduroam.jp/service\\_for\\_eduroam/](https://www.eduroam.jp/service_for_eduroam/)  
※記載内容を近日更新予定です

# eduroam JP申請システム

# システムの概要

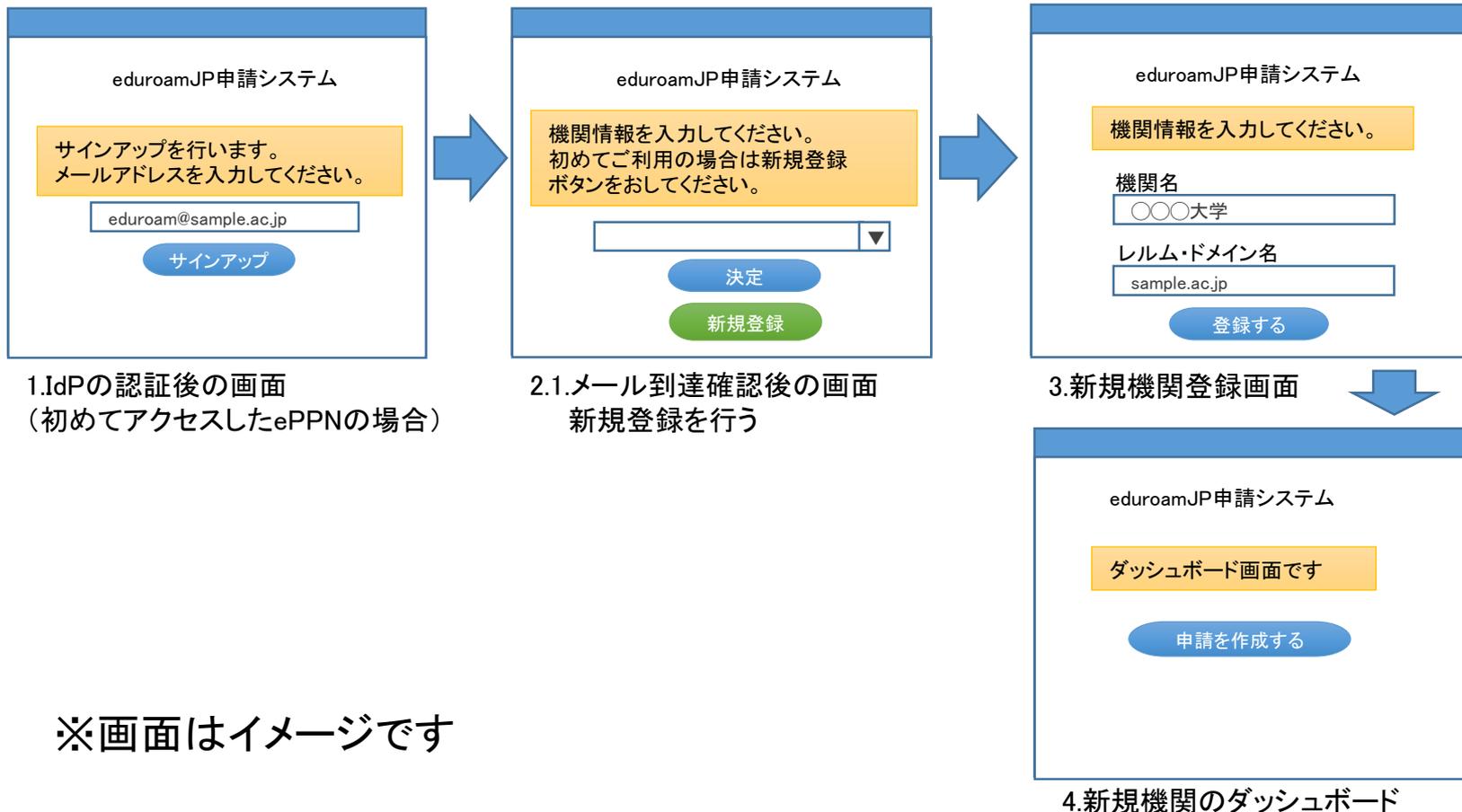
- 各種申請の受付
  - 加入申請、変更申請、脱退申請
  - 代理認証システム利用/利用停止申請
  - 認証連携IDサービス利用/利用停止申請
- 7月稼働開始予定
- 学認のSPとして登録
  - 学認参加機関は所属機関のIdPで認証
  - それ以外はOpenIdPのアカウントを取得して認証
  - eduPersonPrincipalName(ePPN)の送信が必要

# 申請にあたって

- 機関責任者
  - 課長以上もしくは教授以上
- 技術担当者
  - 二名を置くこと
  - 一名は機関責任者と兼任可能
  - 業務委託先の人も可能
- レルム
  - DNSドメイン名をもとに決定
  - 代理認証システム、認証連携IDサービスは入力されたDNSドメイン名からeduroam JP側がレルムを決定

# 加入申請

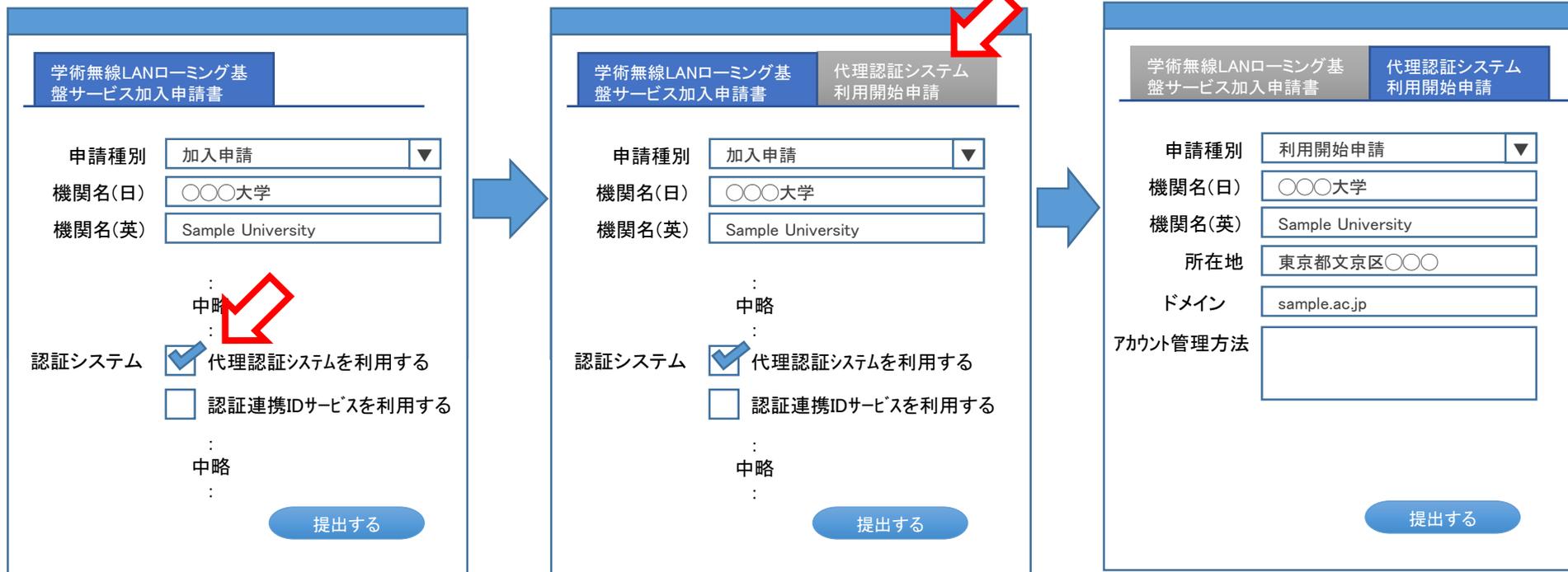
## ・サインアップ (IdPでの認証後の初回アクセス)



※画面はイメージです

# 加入申請

## ・新規申請(サインアップ終了後)



The image shows a three-step process of filling out an eduroam application form. Each step is represented by a screenshot of the web interface, connected by blue arrows pointing from left to right.

- Step 1:** The form is titled "学術無線LANローミング基盤サービス加入申請書". The "申請種別" (Application Type) is set to "加入申請". The "機関名(日)" (Institution Name in Japanese) is "〇〇〇大学" and the "機関名(英)" (Institution Name in English) is "Sample University". Under "認証システム" (Authentication System), the checkbox for "代理認証システムを利用する" (Use proxy authentication system) is checked, and "認証連携IDサービスを利用する" (Use authentication linkage ID service) is unchecked. A red arrow points to the checked checkbox. A "提出する" (Submit) button is at the bottom.
- Step 2:** The form now has two tabs in the header: "学術無線LANローミング基盤サービス加入申請書" and "代理認証システム 利用開始申請". The "申請種別" remains "加入申請". The institution name fields are the same. Under "認証システム", the same checkboxes are present. A red arrow points to the newly added "代理認証システム 利用開始申請" tab. A "提出する" button is at the bottom.
- Step 3:** The form now has two tabs: "学術無線LANローミング基盤サービス加入申請書" and "代理認証システム 利用開始申請". The "申請種別" has changed to "利用開始申請". The institution name fields are the same. The "所在地" (Location) is "東京都文京区〇〇〇" and the "ドメイン" (Domain) is "sample.ac.jp". The "アカウント管理方法" (Account management method) field is empty. A "提出する" button is at the bottom.

1.学術無線LANローミング基盤サービス加入申請において、代理認証システムを利用するにチェック

※画面はイメージです

2.代理認証システム利用開始申請が自動的に追加される  
 認証連携IDサービスにチェックをつけた場合も同様に認証連携IDサービス利用開始申請が追加される

3.代理認証システムおよび認証連携IDサービス利用開始申請の内容は自動的に設定可能なものはすべて反映

# 加入申請

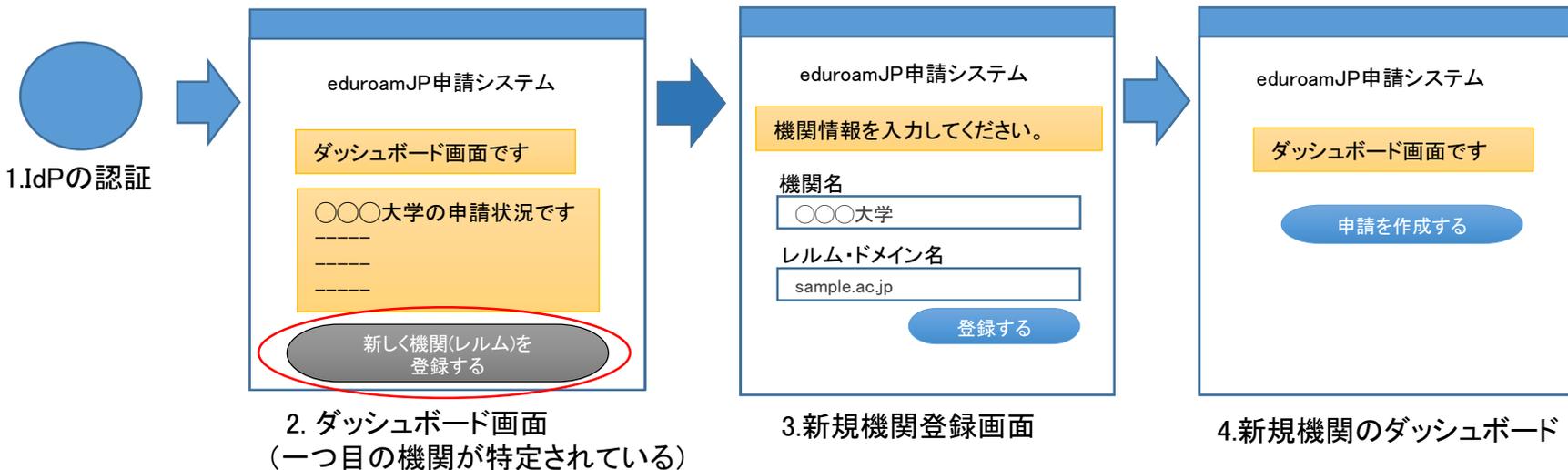
- 申請システムからの申請提出後
  - eduroam JP担当にて申請内容確認
  - NII eduroam担当者による申請内容確認後
    - SINET加入機関 → 機関の長の押印・郵送省略可  
(記名についてはシステムで入力)  
システム上での提出のみ
    - SINET非加入機関 → PDFを出力して印刷  
機関の長の記名・押印後、郵送
  - 電子提出あるいはNII eduroam担当に書類到着後、承認

# 加入申請

- 同一担当者による複数機関の申請
  - 大学法人が運営する複数の大学等について同じ担当者が申請する場合
    - 申請は大学ごとに行ってください
    - 最初の一つ目の機関は今までの紹介のとおりの手順
    - 二つ目以降の申請については次以降のスライドで説明
  - 担当者が異なる場合は通常の手順で申請してください

# 加入申請

- 同一担当者による複数機関の申請(二つ目以降)



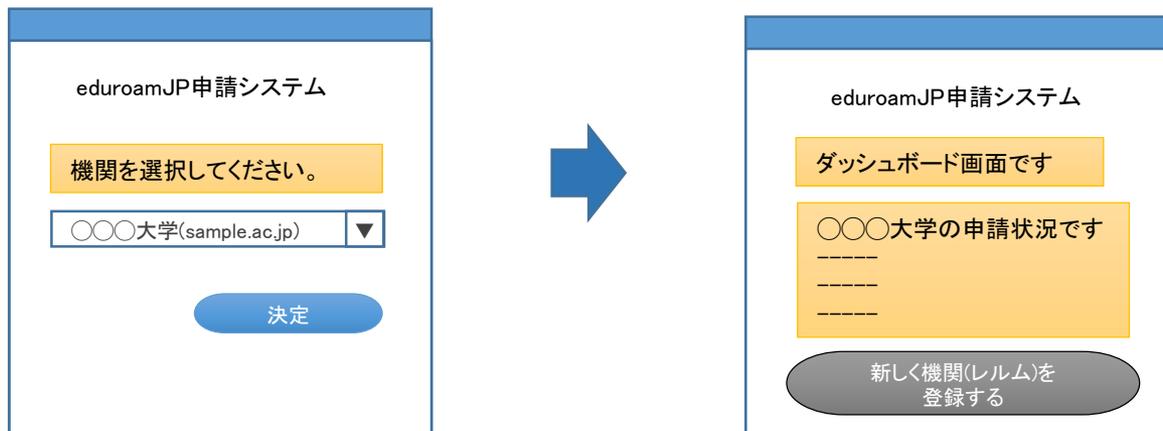
- 三つ目以降は繰り返し

※画面はイメージです

# 加入承認以後のシステム利用

## • ログイン

- 複数の機関を担当している場合はログイン後に申請を行う機関をリストから選択



複数の機関に紐づくePPNの場合の選択画面

※画面はイメージです

# 加入承認以後のシステム利用

## • 変更申請

### • 機関情報の変更

- 機関名称変更
- RADIUSサーバの情報変更
- 責任者変更
- 技術担当者変更

### • SINET加入機関

- システムからの申請のみ、郵送等は不要

### • SINET非加入機関

- 印刷後、責任者の自署・押印・郵送
- 機関責任者のePPNが登録されている場合、オンライン確認可能
  - この場合は自署・押印・郵送は不要

# 加入承認以後のシステム利用

- 代理認証システムの利用/利用停止
- 認証連携IDサービスの利用/利用停止



オンライン申請のみで随時利用/利用停止可能

- 代理認証システムの利用について
  - 卒業者・離籍者等のアカウントロック(利用停止)など、適切なアカウント管理をお願いします。
    - 申請時にアカウント管理の状況についてご記入ください。
    - 例) ○○大学アカウント管理規則に従って毎年○月に離籍者のアカウントをロックする、など
    - 代理認証システムでは作成したアカウントを消去できませんので、離籍者等のアカウントについてはロック機能で利用停止してください

# 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