


学術情報基盤オープンフォーラム2015
2015年6月11日

eduroam update

中村素典 / 国立情報学研究所
後藤英昭 / 東北大学



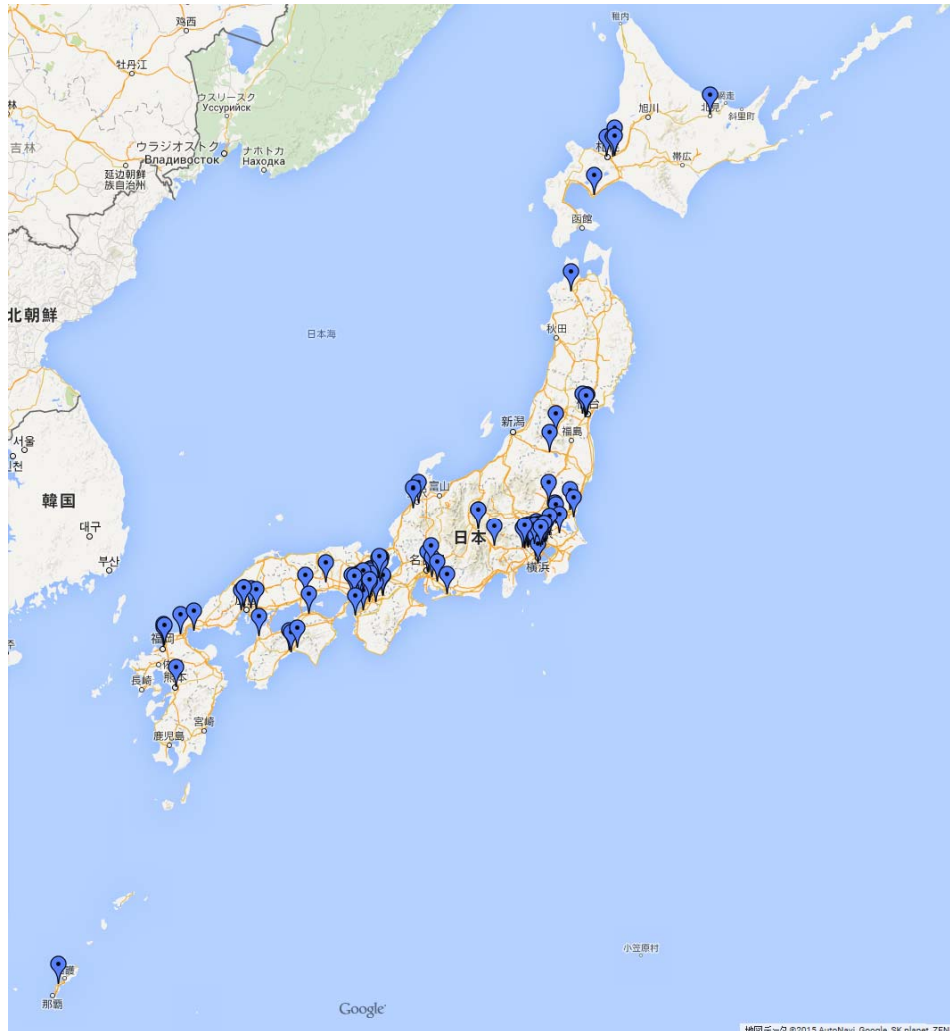


国際学術無線LANローミング基盤「eduroam」

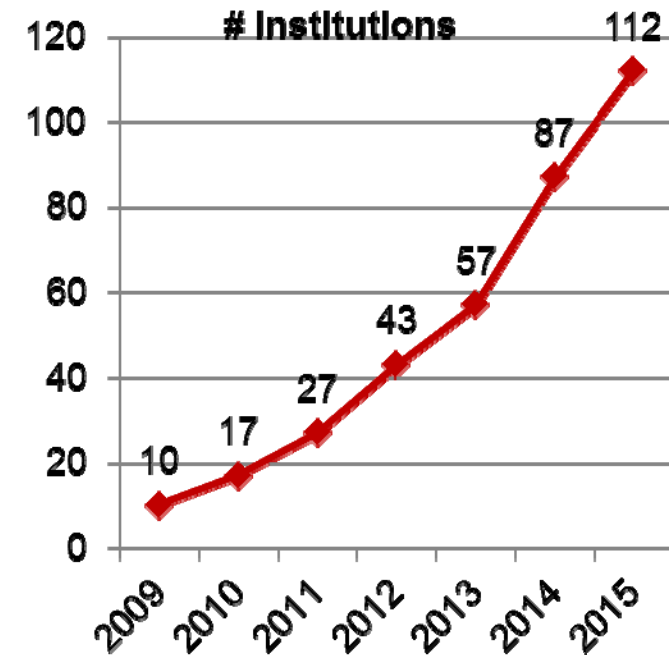
- 欧州TERENAで開発された教育・研究用の学術無線LAN (Wi-Fi)ローミング基盤
 - 国際的デファクト・スタンダード
- 日本は「eduroam JP」の名称で参加
 - 訪問先の無線LANが無料で利用可能
 - ESSIDは“eduroam”
 - IDは“ user@大学名.jp”
 - どこでも使える共通アカウント
 - 互恵の精神に基づくサービス
- メリット
 - 802.1X方式による安全なユーザ認証
 - Windows/Mac/スマートフォン等に対応
 - 来訪者のためのネットワークを毎回構築する必要なし

eduroam JP と国内動向

- 国内のeduroam参加機関 (2015.6現在)

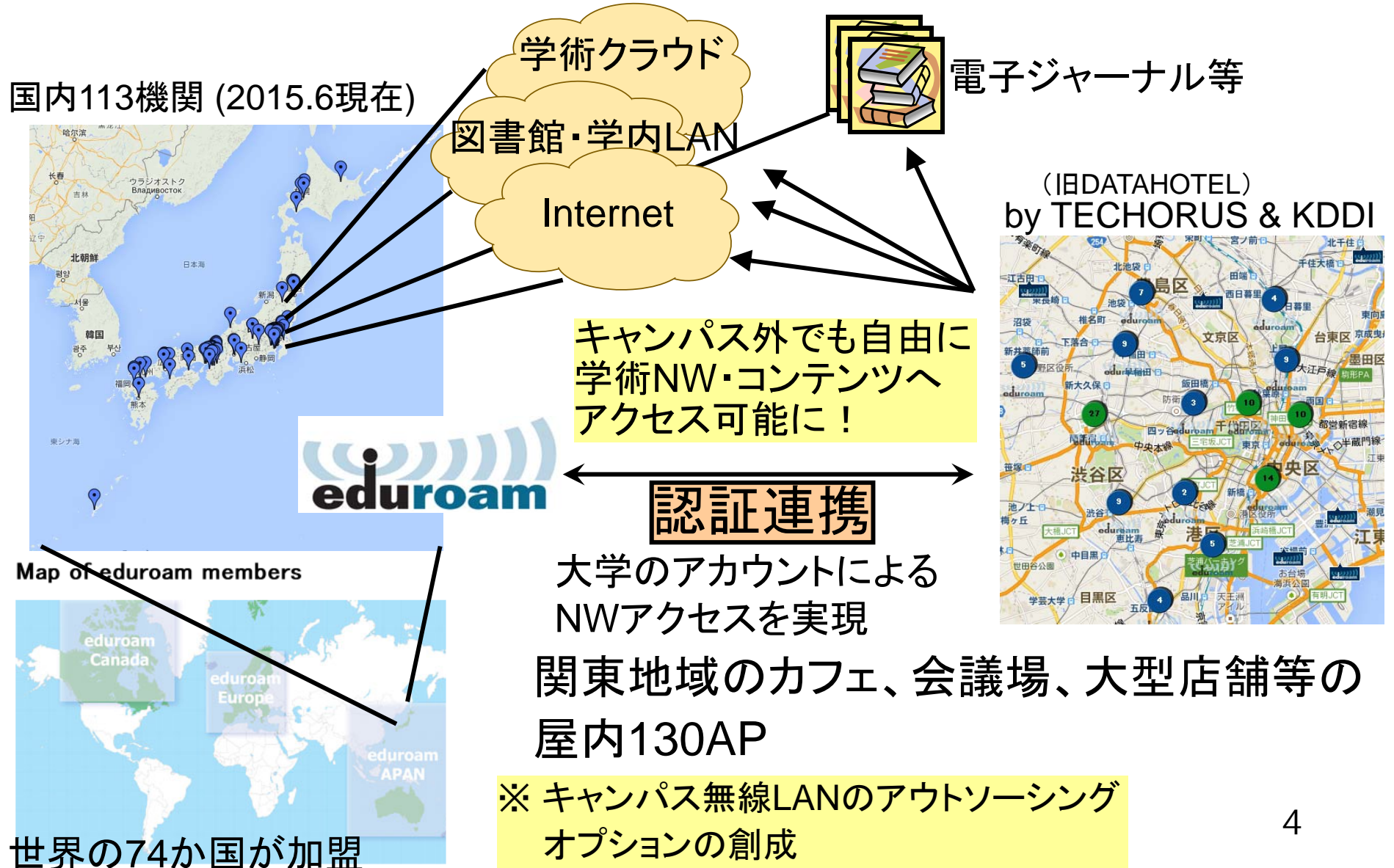


参加機関募集中!



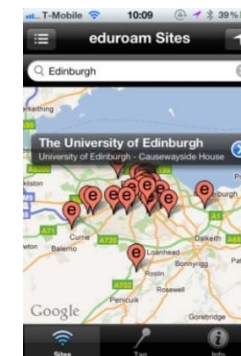
ISP-eduroam連携 継続中！

- 仮想的なキャンパスネットワークの拡大 !!



国内動向

- 大学、短大、高専に加えて、**専門学校も参加OK!**
 - 専門学校からの問い合わせがあり、ネットワーク運営・連携本部・認証作業部会で審議、参加を認めることとした。
- 基地局マップのデータ収集
 - 利用者が基地局の場所を探しやすいように
 - **参加機関は協力をよろしくお願いします!**
 - 提出データはXML形式



国際動向

■ 世界74か国(地域)に普及 (2015.6現在)

- 欧州の全域
- アジア14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等
- スバルバル諸島やニューカレドニアにも!



■ 新興国では電源・ネットワークの不安定さ、狭い帯域に対応が必要


- 我々の耐災害・耐障害eduroamのアーキテクチャが利用できそう. (検討中)

国際動向：アジア・オセアニア各国

(survey by H. Goto in Nov. 2014)


country (territory)	joined inst.	#total univ.+col.	deployment rate	
Australia	39+10	39+61?	100%	(AP regional server 1)
Hong Kong	9	9	100%	(AP regional server 2)
China	?	1,700+ ?		(no activity for years, re-starting)
Taiwan	217?	170+ ?		
Japan	75	1,200+	6.3%	
New Zealand	8+2	8+?	100%	
PNG	1	6 ?		hosted by AARNet
Macau	1?	?		
India	64	?		
South Korea	3	?		
Singapore	4	8	50.0%	
Thailand	18	160	11.3%	
Malaysia	5	73	6.8%	
Philippines	?	?		(no activity since 2007, re-starting)

- 機関数の少ない国では、近隣の国によるホスティングが有効.



eduroam構築・運用支援

- SINETにおけるeduroamアクセスネットワーク収容
- 代理認証システム
- 会議向け期間限定eduroamアカウント
- オンラインサインアップシステム(代理認証システム)
- クライアント証明書発行システム(代理認証システム)

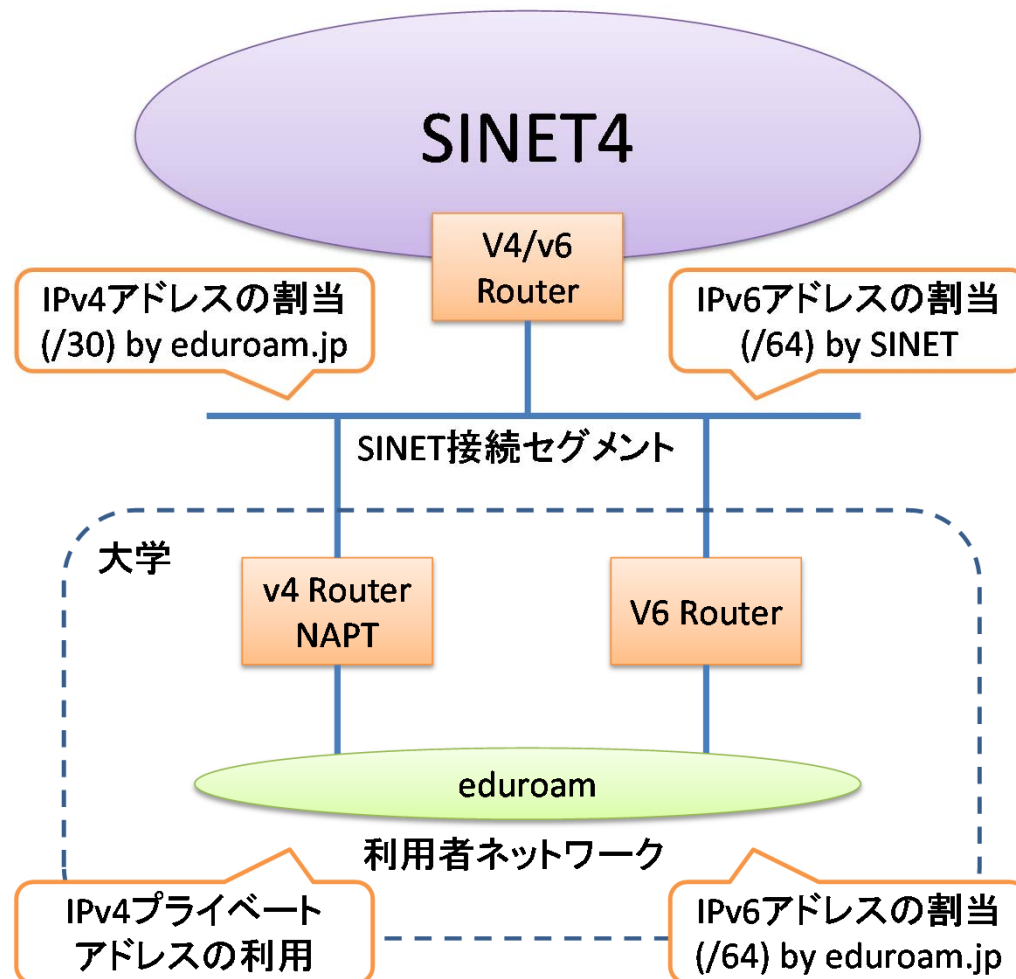


SINETにおけるeduroamアクセスネットワーク 収容

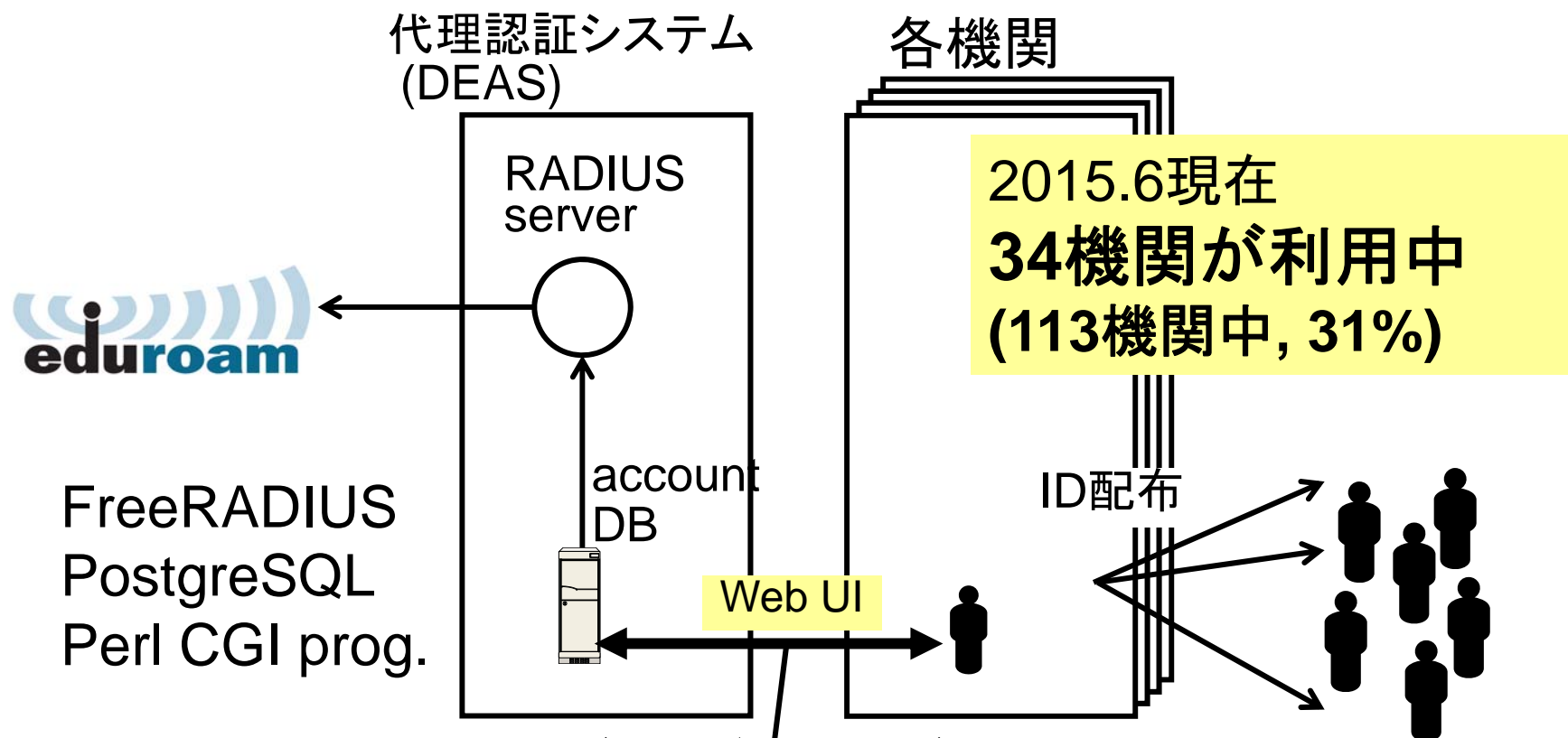
- 大学の保有するIPアドレスとは異なるアドレスをゲストに割り当てたい
 - IPアドレスによるアクセス制限による学内限定サービス等との兼ね合い

- SINET4では、/30のIPv4アドレスと、/64のIPv6アドレスを割り当て、SINET経由でアクセス可能とするサービスを提供中
 - /30のIPv4アドレスは、NATルータによる接続を想定
 - SINET5でも継続して提供予定

eduroamアクセスネットワーク収容のイメージ



代理認証システム (2008年～)



- アカウント発行ウェブサービス (ウェブ画面) または
- Shibbolethによるシングルサインオン (開発中)

※ 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

新サービス1:

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
 - 偽の会議をどのように排除できるか？
 - 利用資格の基準をどのように設定するか？
 - eduroam JP事務局の負担をどのように下げるか？



利用資格(仮)

- 会議主催者はSINET加入機関または学術団体(学振認定)であること
 - 実行委員会は機関ではないので、これをどのように扱うのか？
 - 共催者やスポンサー、現地担当委員会に利用させてもよいか？
- 実務担当者はSINET加入機関(eduroam参加機関が望ましい)の職員であること

アカウント配布シート(例)

[eduroam guest ID for this symposium](type I)
* This ID (a pair of username and password) is valid for Wi-Fi connection by eduroam (International Educational Roaming Infrastructure).
* The device must support the IEEE802.1x protocol.
* Members of eduroam participating universities can use eduroam as usual with your eduroam ID assigned by your university.
* To learn more on eduroam, visit <http://www.eduroam.org/>.

Username: <>
Password: <>

** The following terms inform you of the conditions of use of the ID. Please read these carefully. Using the ID indicates that you have read and accepted these terms.

- + The symposium provides the guest eduroam ID to each registered participant.
A specifically assigned participant is authorized to use eduroam connection with the ID free of charge. The ID is not transferable.
- + The symposium may provide user's privacy information when asked by operators of the Wi-Fi network or eduroam for security reason.
- + The ID is valid for the term of the symposium (from <<>> to <<>>). Please erase the ID setup when you leave the symposium.
- + The ID is provided to be used at eduroam areas in the venue.
It might be usable at some eduroam areas in Japan, but not guaranteed. Don't use the ID at eduroam areas outside Japan.
- + The use of the ID must comply with telecommunication laws.
Profit-oriented use, copyright infringement, and other illegal use are prohibited.
- + The service of eduroam is no-warranty and as-is.
If you have any difficulty or inquiry on using eduroam, contact the reception desk, or try other way for Wi-Fi connection.

事前登録者用

インシデント対応のため
利用者の紐付けが必要

[eduroam guest ID for an on-site participant](type II)
* This ID (a pair of username and password) is valid for Wi-Fi connection by eduroam (International Educational Roaming Infrastructure).
* The device must support the IEEE802.1x protocol.
* Members of eduroam participating universities can use eduroam as usual with your eduroam ID assigned by your university.
* To learn more on eduroam, visit <http://www.eduroam.org/>.

Username: <id>
Password: <password>

** The following terms inform you of the conditions of use of the ID. Please read these carefully, and sign in the slip at the bottom to indicate that you have read and accepted these terms.

- + The symposium provides the guest eduroam ID to each registered participant.
A specifically assigned participant is authorized to use eduroam connection with the ID free of charge. The ID is not transferable.
- + The symposium may provide user's privacy information when asked by operators of the Wi-Fi network or eduroam for security reason.
- + The ID is valid for the term of the symposium (from <<>> to <<>>). Please erase the ID setup when you leave the symposium.
- + The ID is provided to be used at eduroam areas in the venue.
It might be usable at some eduroam areas in Japan, but not guaranteed. Don't use the ID at eduroam areas outside Japan.
- + The use of the ID must comply with telecommunication laws.
Profit-oriented use, copyright infringement, and other illegal use are prohibited.
- + The service of eduroam is no-warranty and as-is.
If you have any difficulty or inquiry on using eduroam, contact the reception desk, or try other way for Wi-Fi connection.

Name and
signature


----- >8 ----- >8 ----- >8 -----

[eduroam guest ID for an on-site participant]
I have read and accepted the conditions of use.
[Name: _____, Signature: _____]

(Official use: ID: <<>> Reg. No.: _____ Identification document: _____)

当日登録者用

詳細: <http://www.eduroam.jp/conf.html>

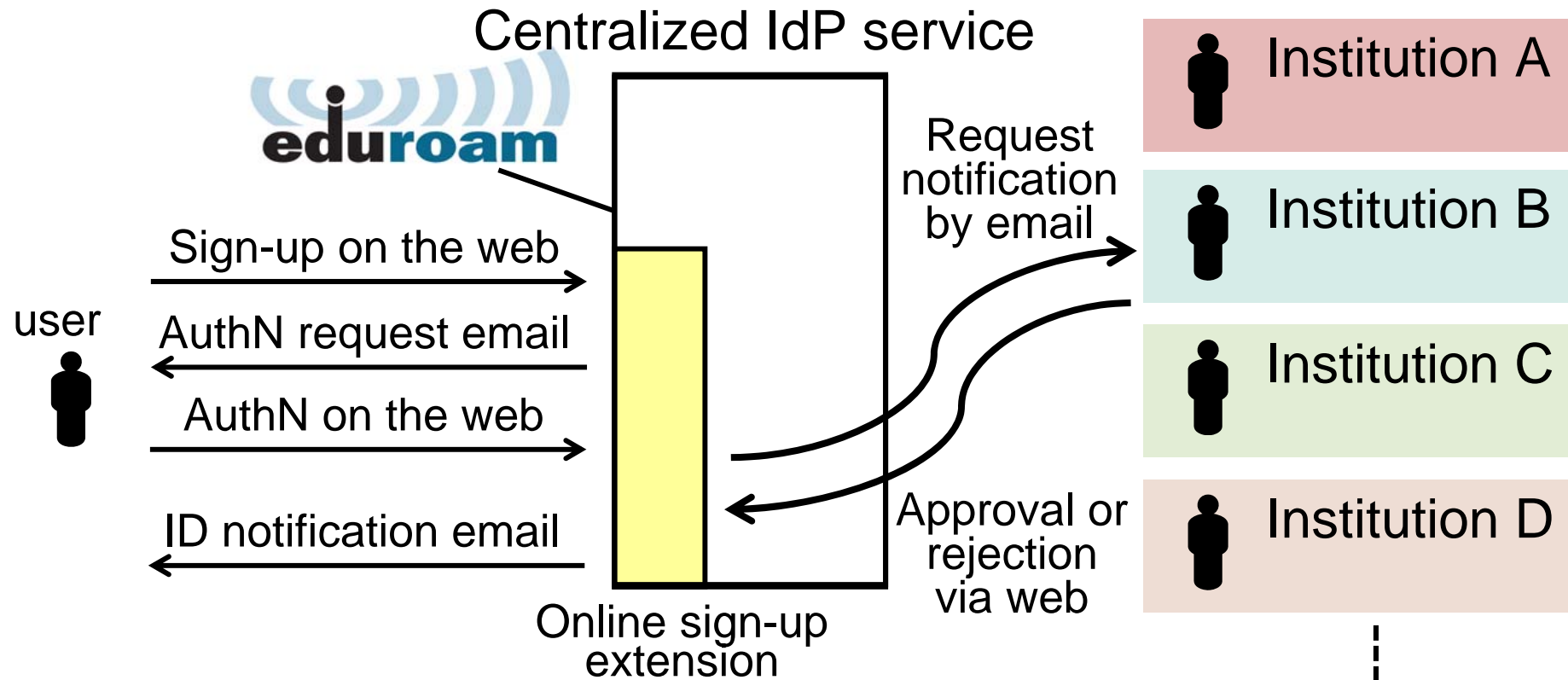


新サービス2:

オンラインサインアップシステム (代理認証システムの拡張)

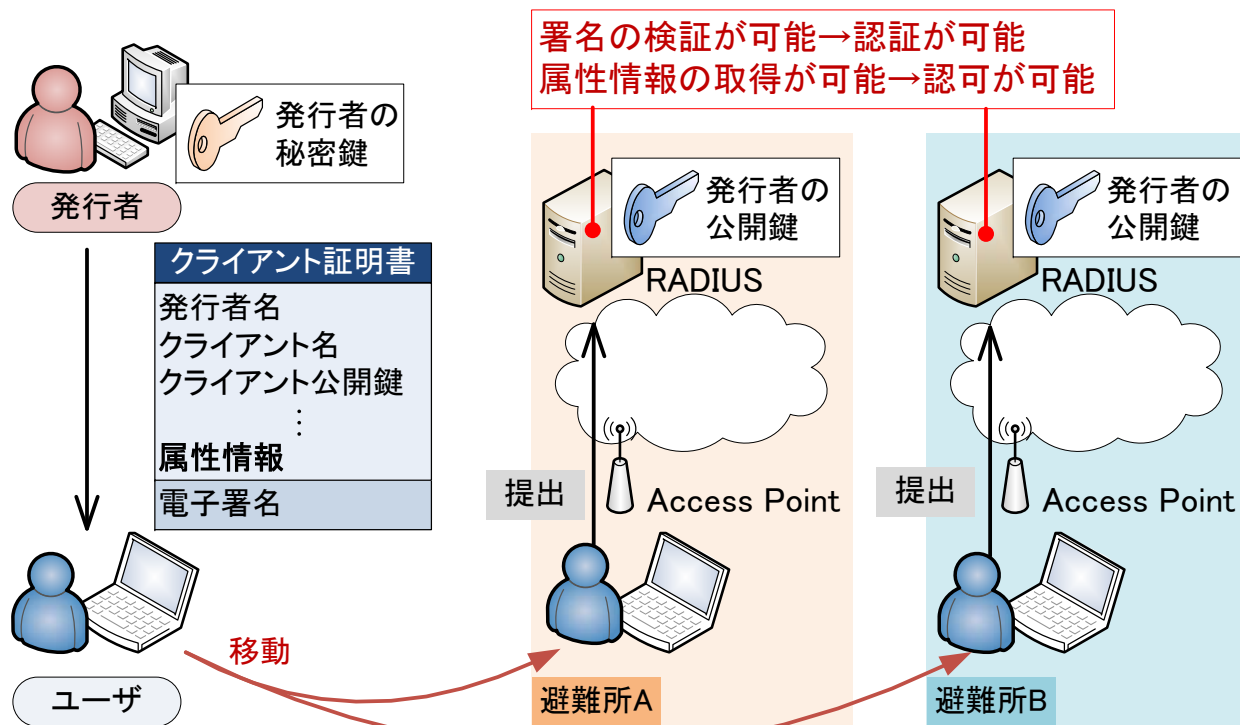
- 機関内でのアカウント配布(従来は手動)を容易化
 - 大規模な機関でも利用しやすい
- 利用者自身がオンラインサインアップによりeduroamアカウントを取得可能
- 機関管理者がサインアップごとに承認操作する
- 機関が発行した電子メールアドレスを初期の認証に利用
 - 機関管理者が受付可能なアドレスを登録しておく
 - アドレスの末尾が一致する利用者のみ、eduroamアカウントの申請が可能

eduroamオンラインサインアップシステム



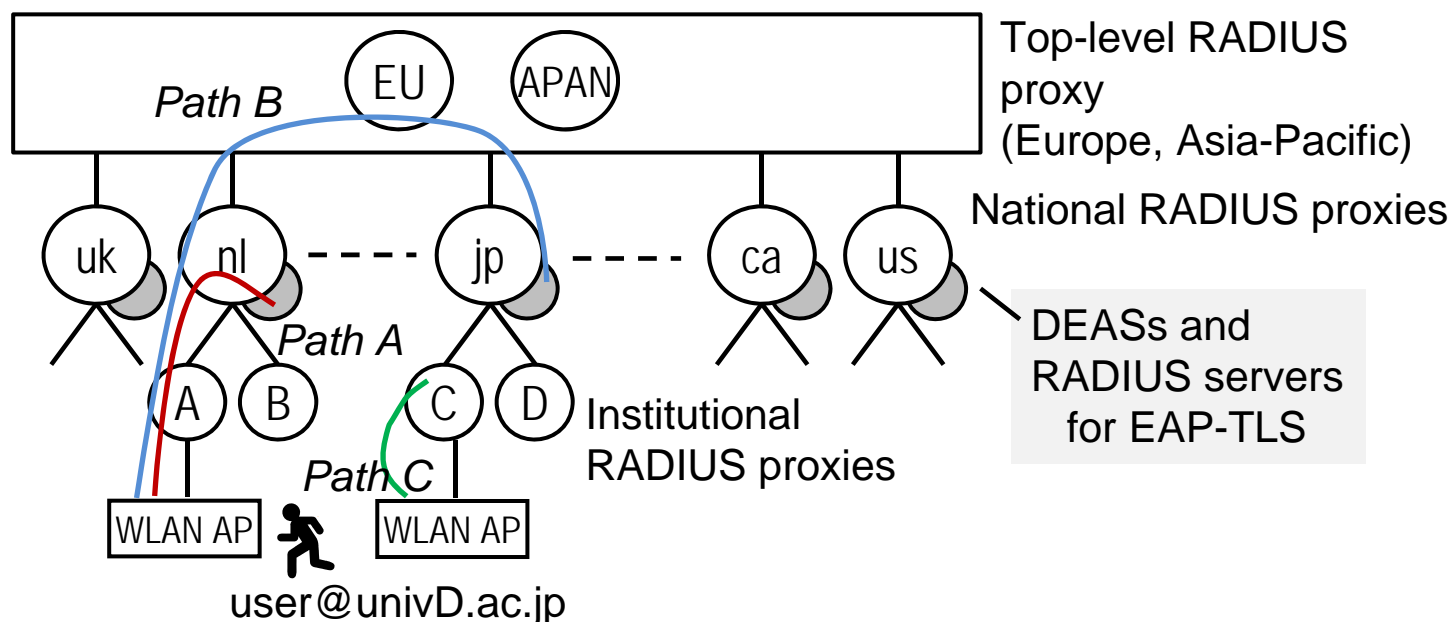
新サービス3: クライアント証明書発行システム

- 代理認証システムで、EAP-TLS認証をサポート
- 証明書を用いるEAP-TLSでは、ローカル認証方式が実現可能



応用例: ローカル認証による耐災害・耐障害eduroam

- 代理認証システムに証明書発行機能を追加
- 代理認証システムとローカル認証方式の組み合わせにより、認証処理の信頼性を向上
 - 中継するプロキシの数を削減し、信頼性を向上
 - 自機関のサーバ群が被災した場合でも、他機関でeduroamが継続利用可能





まとめ

- eduroamは全大陸(南極除く)、計74か国(地域)に普及した、キャンパス無線LANのスタンダード
 - 国内113機関が参加
 - 大学・高専に加えて、専門学校も参加可能に
 - 基地局マップのデータ提出にご協力をお願いします

- 国内機関向け新サービス
 - 会議向け期間限定eduroamアカウントの試行
 - オンラインサインアップシステム
 - クライアント証明書発行システム