学認春CAMP
2014年5月30日

eduroam（エデュ ローム）の最新動向と耐災害性・耐障害性向上

後藤英昭
東北大学サイバーサイエンスセンター　／　国立情報学研究所

内容

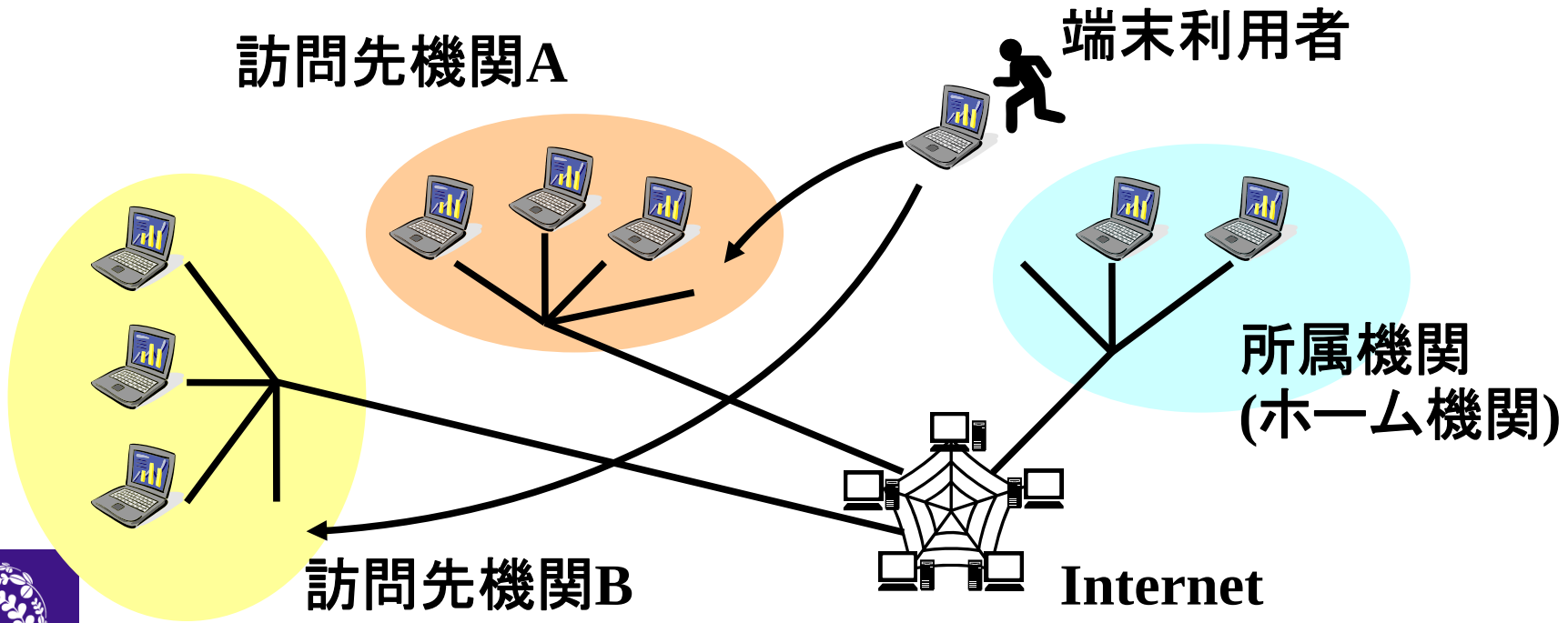
- eduroamによる学術系国際無線LANローミング
- 国内外のeduroamの動向
  - 国内状況
  - 国際状況
  - 利便性の改善
- 耐災害性・耐障害性向上のための研究開発
  - ローミング時の安定性の向上
  - クライアント証明書を用いたEAP-TLS認証
  - ローカル認証による耐災害・耐障害eduroam
- 無線LANインフラの展望

TOHOKU UNIVERSITY

国内外のeduroam最新動向

eduroamによる学術系国際無線LANローミング

- 「認証連携」技術により、
  利用者が所属機関のアカウントを使って
  他機関の無線LANインフラを利用できる仕組み



eduroam JP と 国内動向

■ 国内のeduroam参加機関 (2014.5現在)

- 国立情報学研究所
- 北海道大学
- 北海道医療大学
- 札幌学院大学
- 北見工業大学
- 室蘭工業大学
- 東北大学
- 宮城教育大学
- 東北学院大学
- 尚絅学院大学
- 山形大学
- 茨城大学
- 高エネ研
- 千葉大学
- 東京大学
- 日本医科大学
- お茶の水女子大学
- 学習院女子大学
- 早稲田大学
- 東京有明医療大学
- 芝浦工業大学
- 成城大学
- 東京電機大学
- 武蔵大学
- 立教大学
- 東京海洋大学
- 東京農工大学
- 電気通信大学
- 国立国語研究所
- 東京工科大学
- 実践女子大学
- 実践女子短期大学
- 一橋大学
- 東京学芸大学
- 理化学研究所
- 横浜商科大学
- 山梨大学
- 金沢大学
- 名古屋大学
- 名古屋工業大学
- 豊橋技術科学大学
- 京都大学
- 京都教育大学
- 同志社大学
- 大谷大学
- 京都工芸繊維大学
- 奈良教育大学
- 奈良女子大学
- 大阪大学
- 国立民族学博物館
- 関西大学
- 大阪教育大学
- 大阪府立大学
- 大阪工業大学
- 大阪体育大学
- 神戸大学
- 甲南大学
- 岡山大学
- 広島大学
- 広島工業大学
- 広島国際学院大学
- 広島修道大学
- 愛媛大学
- 香川高等専門学校
- 九州大学
- 福岡工業大学
- 九州工業大学
- 熊本大学
- 沖縄科学技術大学院大学学園

計69機関 ← 43機関 (2012.12) ← 27 (2011) ← 17 (2010)

TOHOKU UNIVERSITY

従来のキャンパス無線LANの問題点
(eduroamがない場合)

公衆Wi-Fiで一般的だが、
偽AP対策ができない問題

- 低いセキュリティ
  - ウェブ認証方式、MACアドレス登録方式、共有WPAキーなど
  - 教務システム等との、ID/PWの不適切な共用化
- 学生・教職員が訪問先で利用できない
  - 他大学での受講や、非常勤業務における不便
  - 会議場などの民間施設や市街地での不便
- 企業などの訪問者や、市民が利用できない
  - 公衆無線LANの空白地帯
  - 共同研究や会合、図書館、大学病院などで不便

TOHOKU UNIVERSITY

従来のキャンパス無線LANの問題点 (続き)

- 基地局やサービスの乱立による効率低下、混乱
  - 場所ごとに異なる利用方法
  - 携帯電話会社ごとのオフロード対策 (AP乱立)
  - 学会会場など、モバイルルータの持ち込みによる輻輳
- 同時接続数の不足
  - 授業で数百人同時ログインなど
  - 学会でも百人程度が同時利用，　3G回線は慢性的飽和
- 導入・運用の難しさ
  - 独自方式ではサポート負担大
  - 仕様検討に専門知識が必要
  - 日常的な運用・管理の負担大

TOHOKU UNIVERSITY

これからのキャンパス無線LAN

大学目線で欲しいもの

- 安全で使いやすいシステム
  - 無線区間の暗号化　— ウェブ認証では不可！
  - 個人の認証　— 共通鍵では不可！
  - 標準的なユーザ認証方式
  - 大学の認証システムと連携
- 導入・運用が楽なシステム
  - 標準的なシステム構成
  - 運用まで含めたアウトソーシング (オプション)
- 他大学でもシームレスな相互利用環境
  - 大学間認証連携

TOHOKU UNIVERSITY

これからのキャンパス無線LAN (続き)

- 会議場などの民間施設や市街地で利用可能
  - キャリア/ISPとの連携
  - 仮想的なキャンパスネットワーク拡大
- 大人数で同時利用可能
  - 高速・大容量のAP
  - 授業・演習、学会のサポート
- 高速性と高度なアクセス制御を両立
  - 学内・学外利用者のトラフィック分離
  - 学内サーバへの容易で効率的なアクセス
- 市民等の訪問者も利用可能
  - 公衆無線LANサービスのキャンパス展開

TOHOKU UNIVERSITY

ISP-eduroam連携

- 仮想的なキャンパスネットワークの拡大 !!

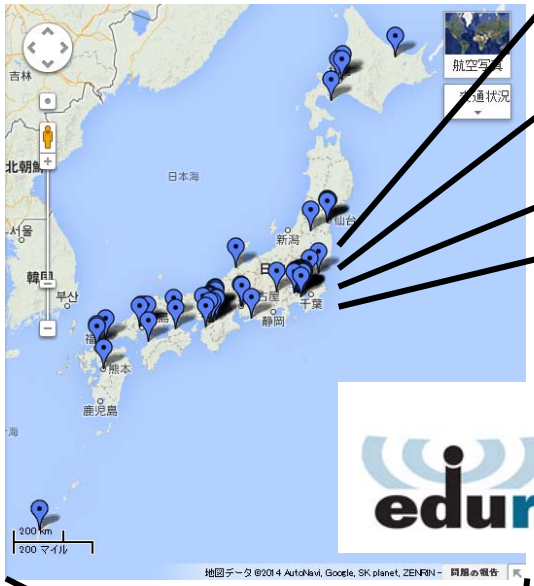
学術クラウド

図書館・学内LAN

Internet

電子ジャーナル等

国内69機関 (2014.5現在)



Map of eduroam members

世界の約69か国が加盟

キャンパス外でも自由に
学術NW・コンテンツへ
アクセス可能に！

認証連携

**大学のアカウントによる
NWアクセスを実現**

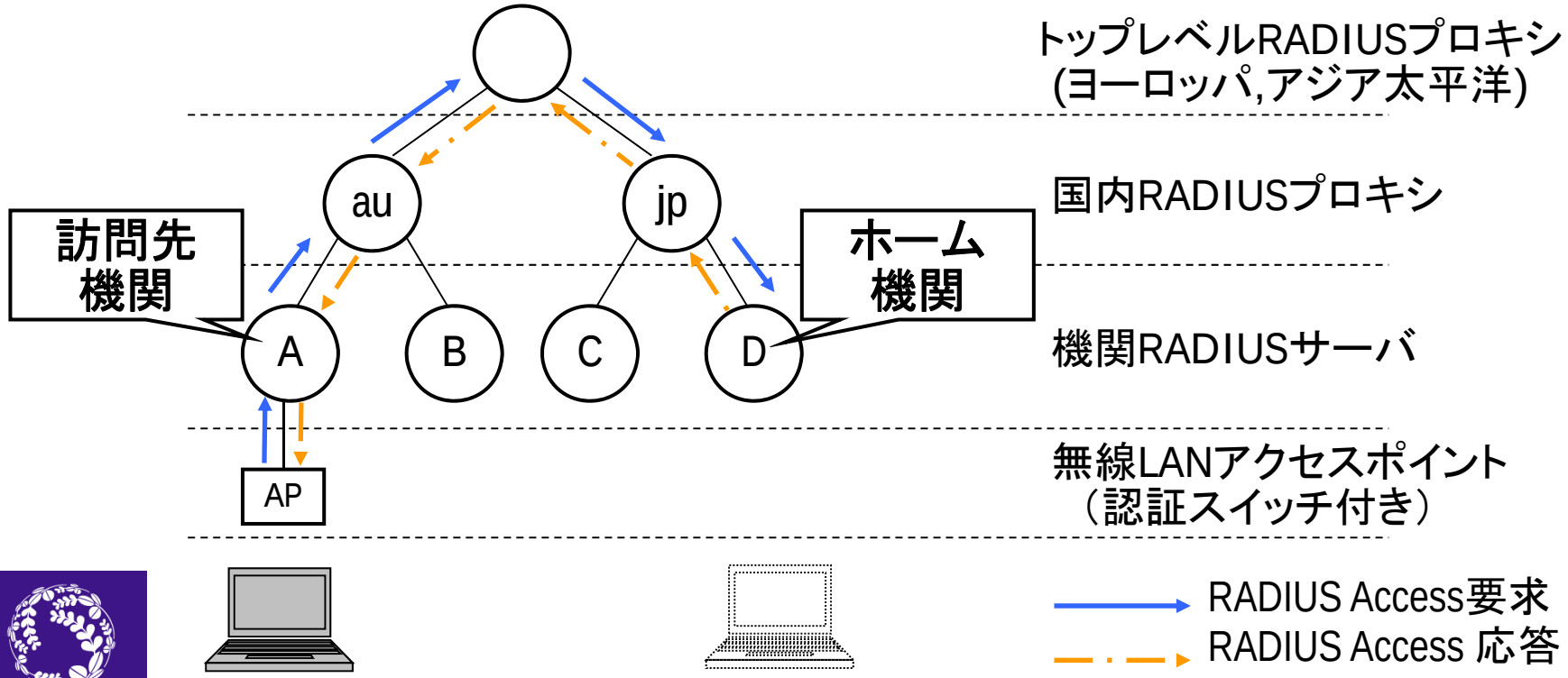
by DataHotel & KDDI

関東地域のカフェ、会議場、大型店舗等の
屋内130AP

※ キャンパス無線LANのアウトソーシング
オプションの創成

eduroamのしくみ

- IEEE802.1x認証に基づいた，**安全なユーザ認証・認可**
- RADIUSツリーを介して認証情報を相互利用（認証連携）
- 標準の構成では、機関ごとにRADIUSサーバが必要
  → **日本では様々な構成が可能**



国内動向：アカウント発行まわり

- 各機関にRADIUS対応の認証サーバを設置
  - 機関の認証システム(LDAP, AD等)と連携／非連携
  - 既存システムに接続できないことがあるので、
    認証システムの導入時からeduroam対応がお奨め
- 「代理認証システム」の利用
  - eduroam JPが提供するアカウント発行ウェブサービス
  - 機関のサーバ設置が不要で、機関管理者のオンライン
    サインアップのみで利用可能
- 「仮名アカウント発行システム」の利用
  - 機関にRADIUSサーバ設置不要
  - 学術認証フェデレーションのアカウントと連携し、
    エンドユーザが随時eduroamアカウントを取得可能
- 業者提供のアカウントサービス(IdP)を利用

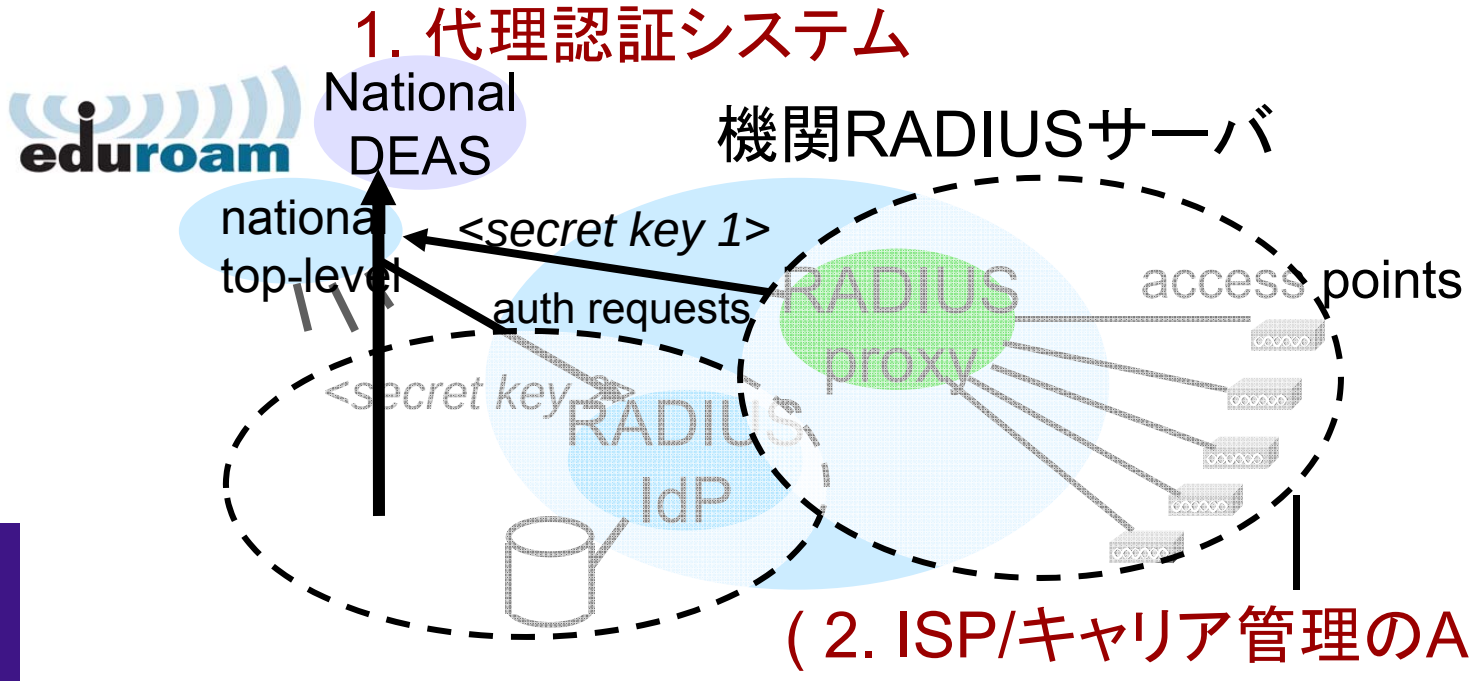
TOHOKU UNIVERSITY

国内動向：認証アプライアンス

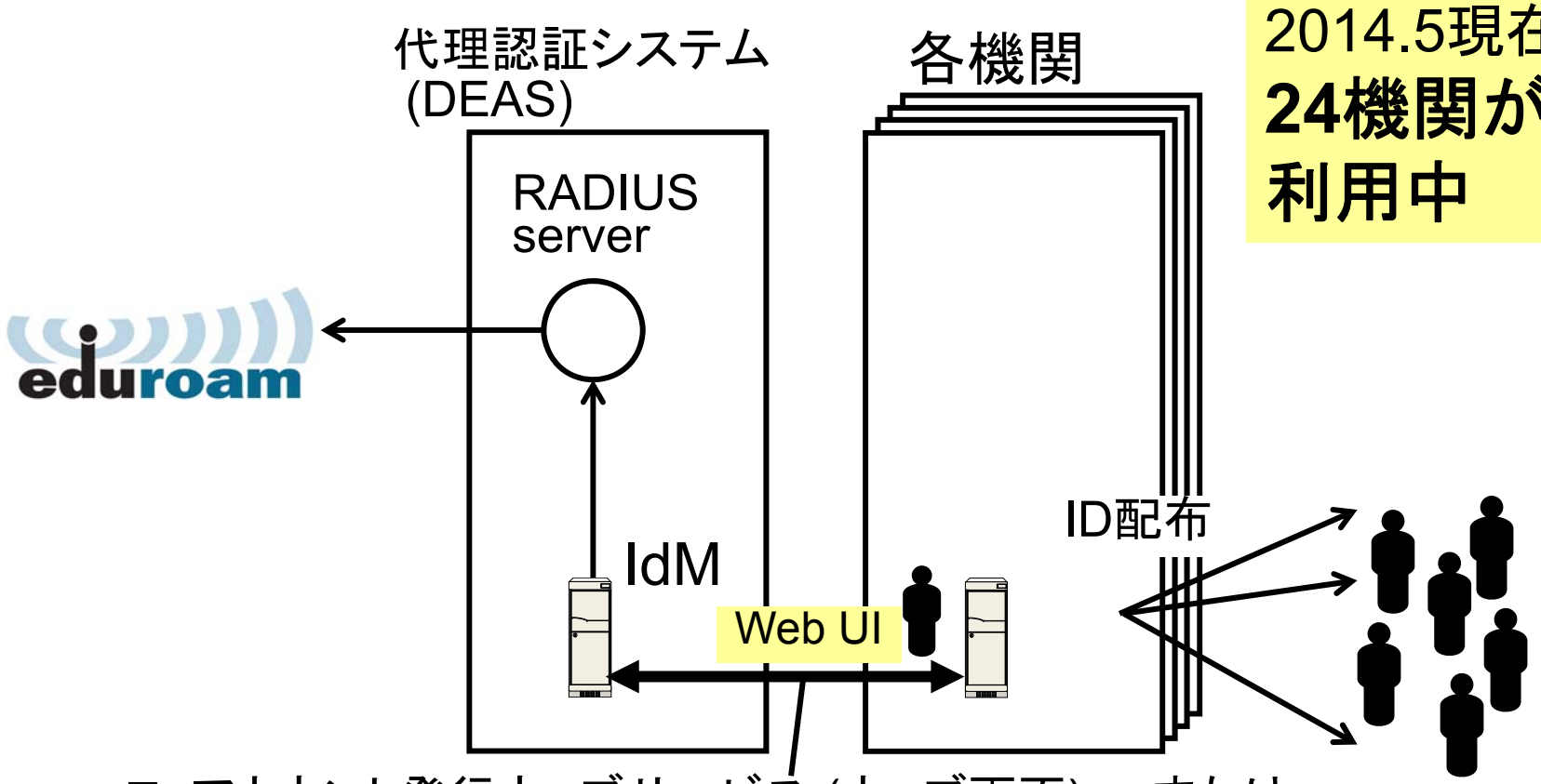
- eduroam(RADIUS)対応の認証アプライアンス製品が国内数社から提供されている
  - 煩雑なインストール作業や設定から解放され、eduroamの導入が容易に
  - 学術認証フェデレーション(Shibboleth)に対応した製品もある

代理認証システム (DEAS, Delegate Authentication System)

- 東北大学で開発、2008年より実証実験サービス提供中
- 機関ごとのIdP構築を不要に
  - eduroam導入の容易化
- RADIUSツリーの単純化
  - 1X認証の安定化



代理認証システム (つづき)



2014.5現在
24機関が利用中

- 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)

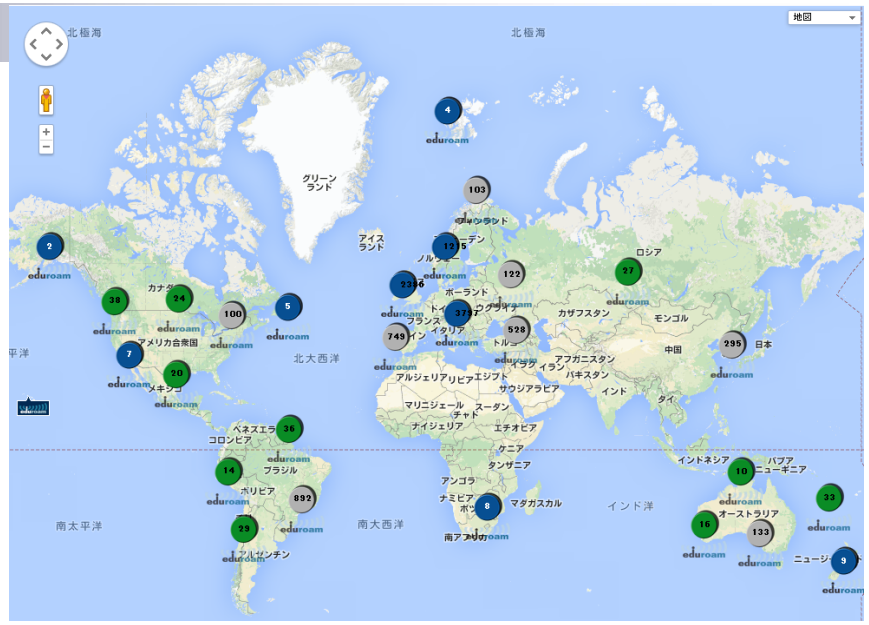
- ID取得だけで、管理者がアカウントをバルク請求・発行可能
- ゲスト用アカウントの発行も可能

代理認証システムの新機能 (開発中)

- オンラインサインアップシステム
  - 既存の認証システムと連携できない機関など
  - エンドユーザがウェブ上でeduroamアカウントを申請、機関管理者が承認
  - 機関の発行したメールアドレスを利用して間接的に認証
- クライアント証明書発行システム
  - EAP-TLS認証のサポート (自動接続の安定化, 安全性向上)
  - エンドユーザ自身が証明書を取得、インストール
  - 耐災害・耐障害eduroamのサポート
- ゲストアカウント発行 (新運用)
  - 会議主催者の申請により、会期のみ有効なゲストアカウントを発行

TOHOKU UNIVERSITY

国際動向



- 世界69か国(地域)に普及
  (2014.5現在)
  - 欧州のほぼ全域
  - アジア12地域
  - カナダ, USA, ロシア,
    南アメリカ各国, 南アフリカ共和国等
  - スバールバル諸島やニューカレドニアにも！
- 2010年GeGC (Global eduroam Governance Committee) 発足
  - 各地域からの代表者11名: EU, US, CA, AP, Latin America, South Africa
  - 日本からも1名、第1期&第2期(再選)

TOHOKU UNIVERSITY

国際動向：アジア・オセアニア各国

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+ ?		
Taiwan	217	170+ ?		
Japan	69	1,200+	5.8%	
New Zealand	8+2	8+?	100%	
PNG	1	6 ?		hosted by AARNet
Macau	1	?		
India	41	?		
South Korea	3	?		
Singapore	3	8	37.5%	
Thailand	12	160	7.5%	

(as of May 2014)

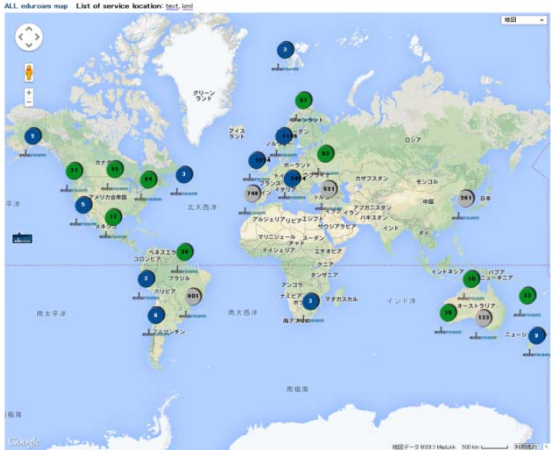
TOHOKU UNIVERSITY

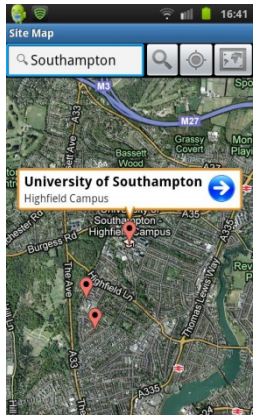
国際動向：キャンパス外におけるeduroam (例)

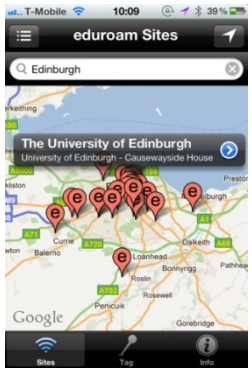
- スウェーデン (SUNET)
  - 空港や主要鉄道駅でeduroam提供
- ノルウェー (UNINETT)
  - 国内14の空港でeduroam提供
- ルクセンブルク市
  - 自治体が運営するHotCityの市街地基地局で利用可
- ミュンヘン
  - 中心部の広場などで利用可
- ロンドン自然史博物館
- ……

利便性向上のための開発・活動

- eduroam CAT (Configuration Assistant Tool)
  - 端末の無線LANと1X認証の設定を容易にするツール
  - Windows 8, 7, Vista, OS X, iOS, Linux
  - 日本では設定プロファイルを未提供 (今後の課題)
- eduroam基地局マップ
  - 出先で最寄りのeduroamサイトを地図上で検索可能
  - eduroam Companion (iOS, Android) でも利用可能
  - 各機関のマップデータ提供にご協力ください!







TOHOKU UNIVERSITY

耐災害性・耐障害性向上のための研究開発

無線LANインフラの耐災害性・耐障害性向上

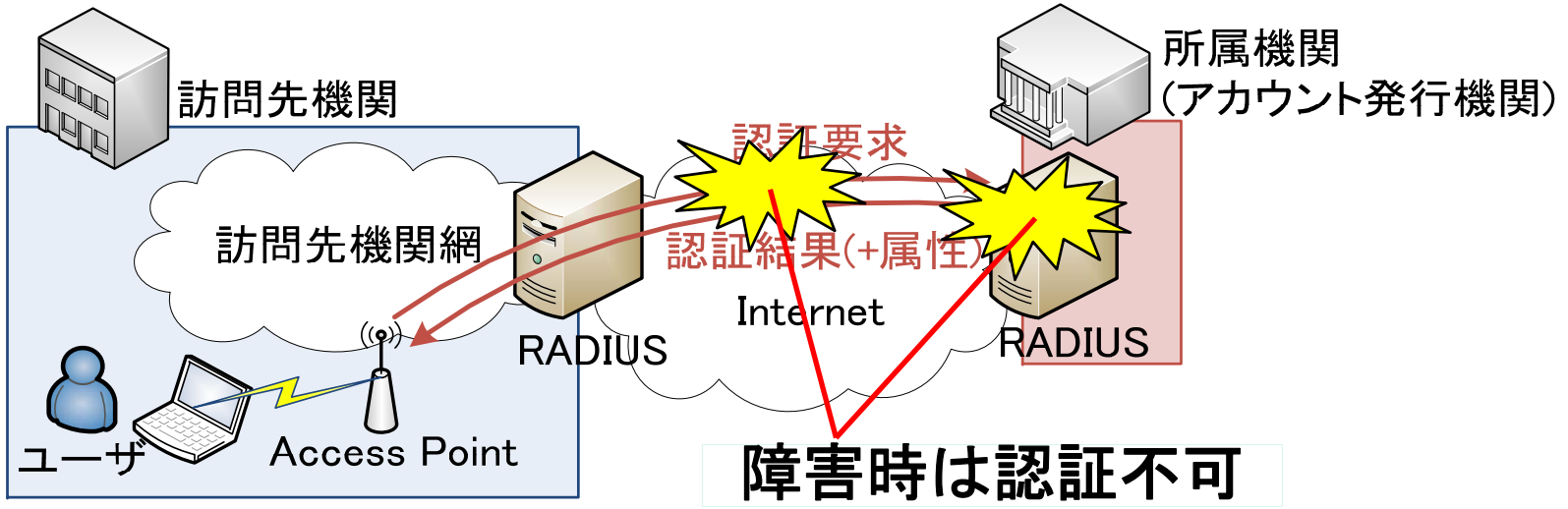
背景

- 東日本大震災において、被災地・避難所の通信手段確保の必要性がクローズアップ
- 東日本大震災において、eduroamの有用性が明らかに (AXIES 2012で既報)
- 長距離(海外)ローミングの認証がやや不安定
  - ユーザ認証に時間がかかることがある
  - 利用中にネットワークが突然切断される
- 認証要求を中継するRADIUSプロキシやネットワークの障害に弱い

TOHOKU UNIVERSITY

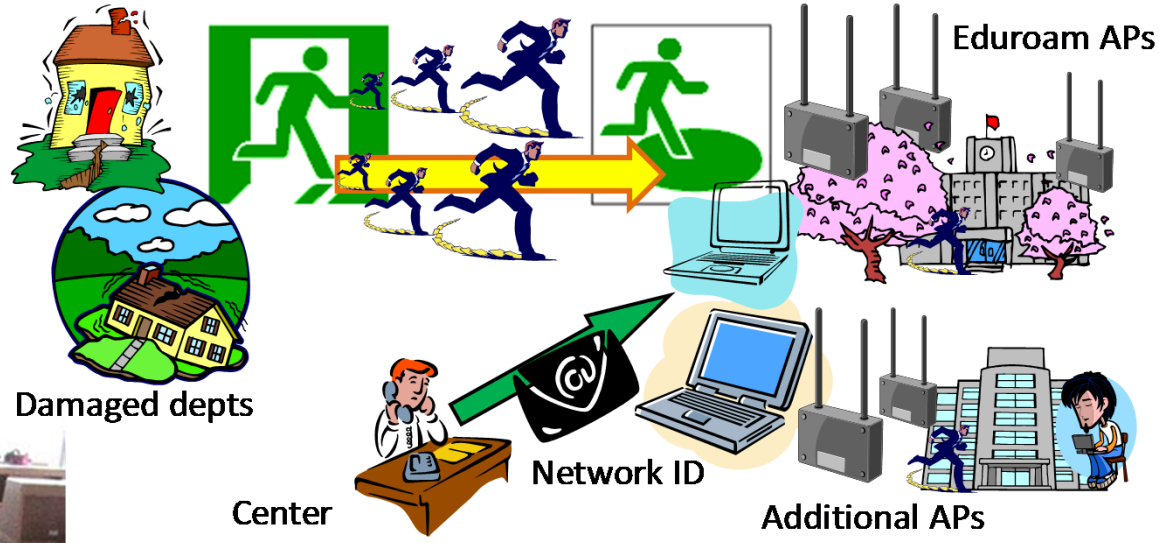
従来のローミング手法の問題点

- RADIUSの認証ネットワークの分断に弱い.
  - ホーム機関が被災
  - IdPの電源喪失や故障
  - 経路上のRADIUSプロキシの不調



被災時に有効な無線LANインフラ

- 被災直後には有線より無線接続の方が物理的に安全
- 学内どこでも、他大学でもシームレスに使える無線LANが必要　(平時でも有用)
- 管理の手間がかからない頑強なシステムが必要



避難先(プレハブ、他部局、他大学)でNW利用可能

3.11夜の日本の明かり

(NOAA Environmental Visualization Laboratory)

http://www.nnvl.noaa.gov/MediaDetail.php?MediaID=697&MediaTypeID=1

TOHOKU UNIVERSITY

東日本大震災の経験

- 建物の倒壊や水没、重度損傷による即日立ち入り禁止など
- 数日にわたる広域停電、サーバ停止
- 携帯電話の通信制限、構内電話や学内LANの機能停止
- ネットワークやサーバ、部屋、設備の損壊、長期の利用不可
- 技術担当者が通勤不可能、業者が対応できない
- 海底ケーブルが首の皮一枚……

通信手段の確保は？

ネット上のアイデンティティはどこ？

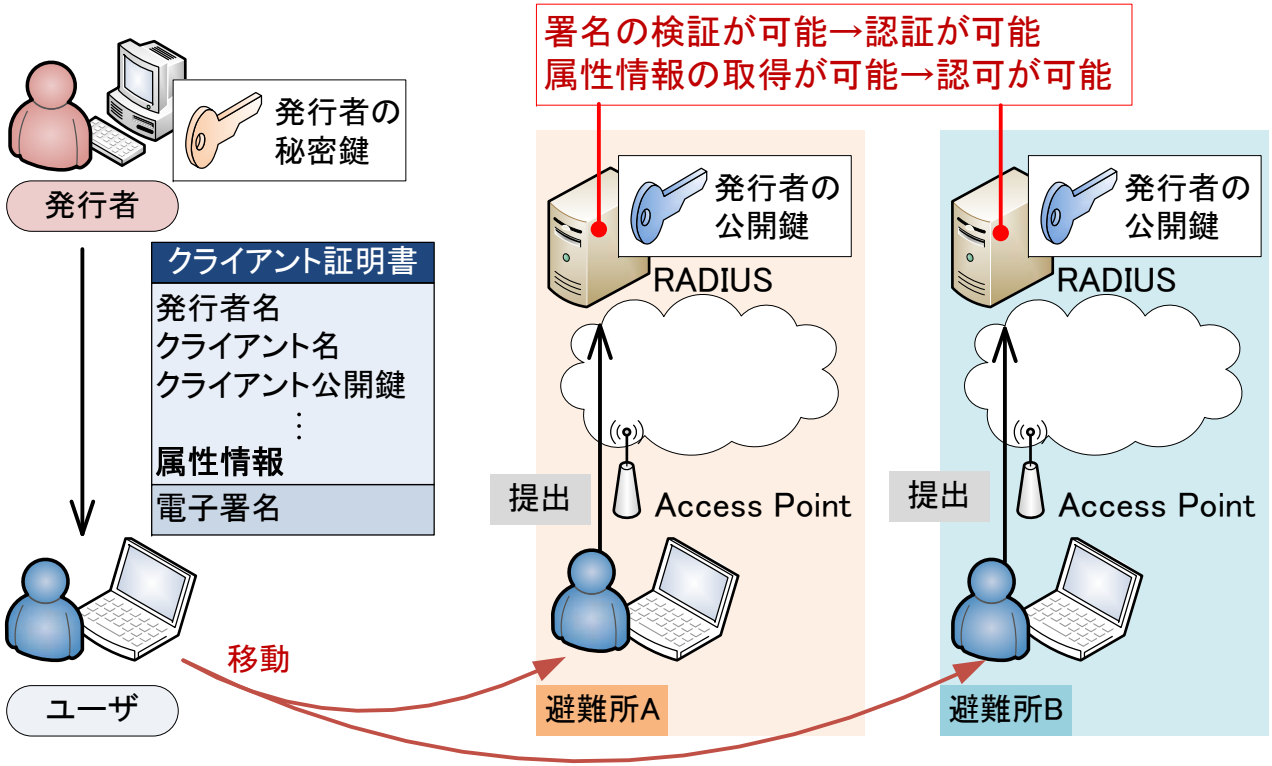
そんなIdPで大丈夫か？

各種サービスのために、まずは通信手段を

TOHOKU UNIVERSITY

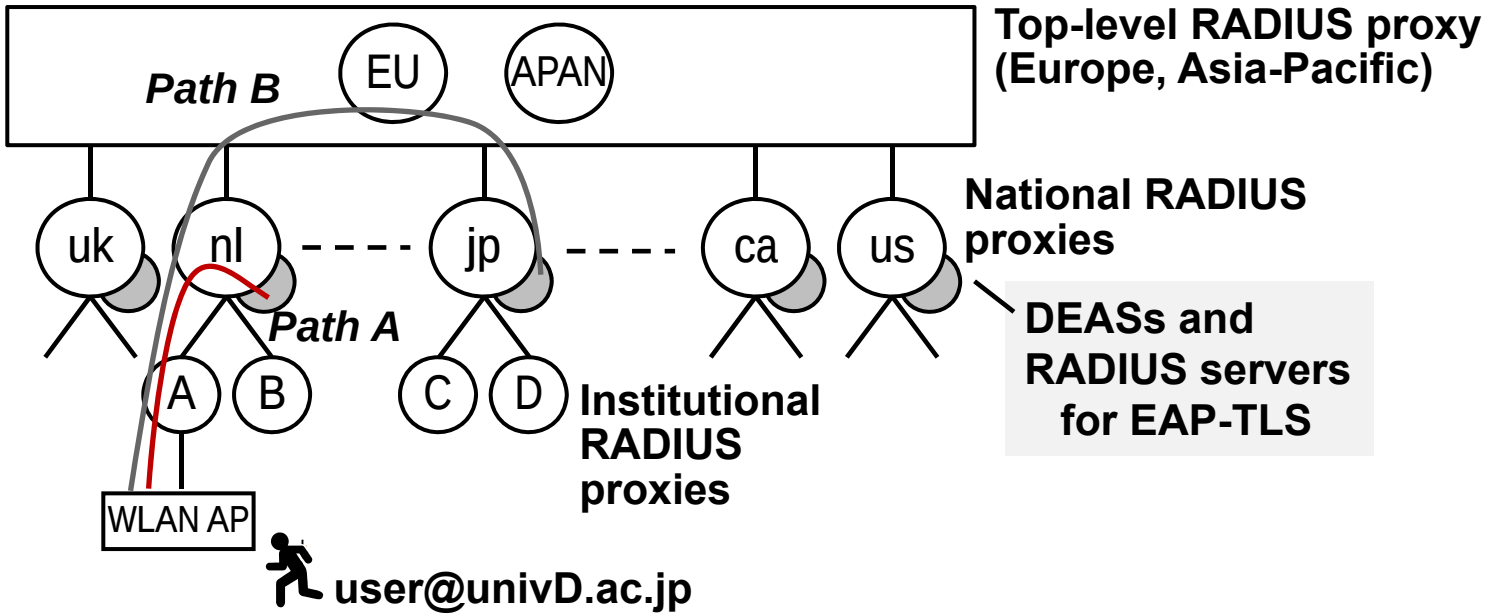
クライアント証明書を用いたEAP-TLS認証

- eduroamでは主流のPEAPの他、EAP-TTLS、EAP-TLSなど様々な認証方式が利用可能
- 証明書を用いるEAP-TLSでは、ローカル認証方式が実現できる (耐災害アクセスポイントの開発より)



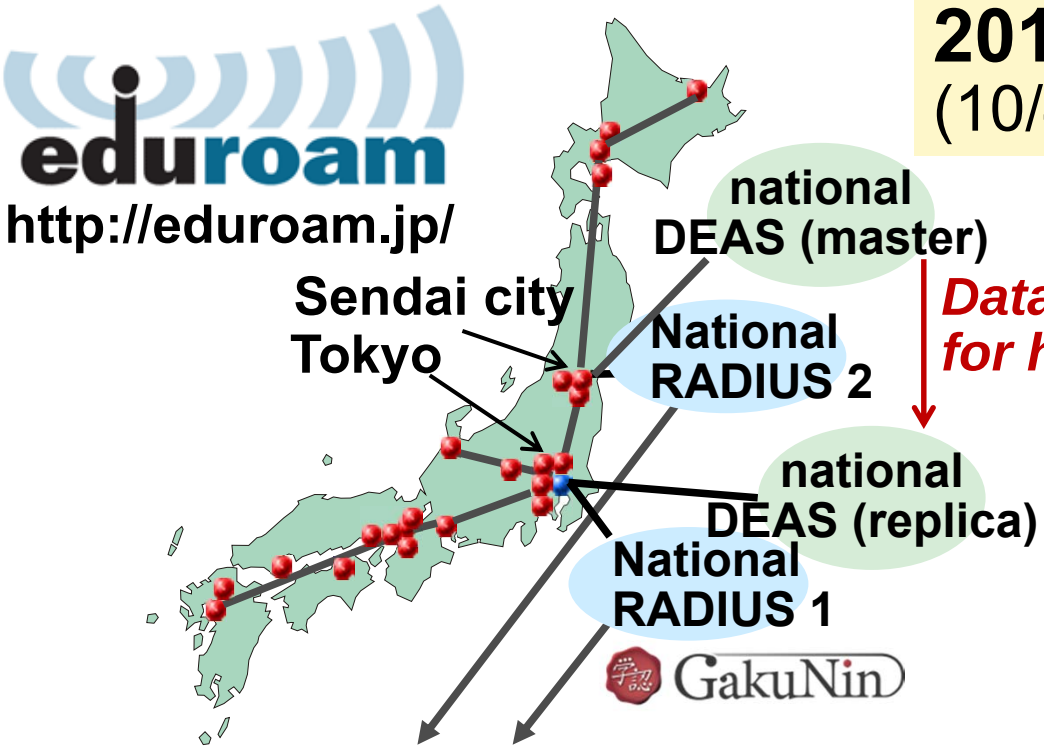
ローカル認証による耐災害・耐障害eduroam

- 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、他機関でネットワーク&サービス利用可能



クラウド型代理認証システム

2012.10サービス開始
(10/4 プレスリリース)



eduroam Top-level servers (Asia-Pacific)
eduroam Global

- EX-CLOUDサービス(データホテル社)の上にレプリカサーバを構築 (PostgreSQL + FreeRADIUS)
- Slony-1を用いたレプリケーションを実施、RADIUS認証のアカウント情報を一方向同期

TOHOKU UNIVERSITY

無線LANインフラの展望

展望

- 「キャンパス無線LAN」と「公衆無線LAN」をシームレス化
  - 学生・教職員が市街地で無線LAN利用
  - 企業の研究者や市民も、大学施設等で無線LAN利用

- 災害地の緊急連絡手段としてのeduroam, 公衆無線LAN
  - 普段使いのシステムとして構築するのが良い
    (東日本大震災の経験より)
  - 大規模イベントの対応にも有効

- 利用者の属性に基づいた高度なアクセス制御(認可)を実現

- 海外からの旅行者にも使いやすい公衆無線LANインフラ

TOHOKU UNIVERSITY

まとめ

- eduroamは全大陸(南極除く)、計69か国に普及した、キャンパス無線LANのスタンダード
  - 国内69機関が参加、成長中
  - 欧州は既に相互利用が一般的な時代
  - 1X方式による安全な認証・認可
- 利便性を高める活動
  - 基地局マップ　など
  - 各機関のマップデータの提出にご協力を
- 耐災害性・耐障害性を有するeduroamシステムを構築中
  - 平常時のサービス安定化、大容量化
  - 公衆無線LANにも適用可能な技術

TOHOKU UNIVERSITY