大学ICT推進協議会 2024年度 年次大会
奈良県コンベンションセンター
2024年12月10日 発表

無線LANローミングにおける個人データ活用と認証負荷削減のためのオフライン属性共有手法

後藤英昭　東北大学
原田寛之　札幌学院大学
漆谷重雄　国立情報学研究所

本研究の一部は、令和6年度NII公募型共同研究の助成を受けました.

cityroam https://cityroam.jp/

- 市民向けのセキュア無線LANローミング基盤
- キャンパス外eduroamとWBA OpenRoamingを展開
- 海外キャリアのSIM認証にも対応

京都市
長野市
北九州市
神戸市
姫路市
小清水町
西海市
沖縄市
成田市
和泉市
　他、各種施設

2023/11～

2023/3～

2024/10～

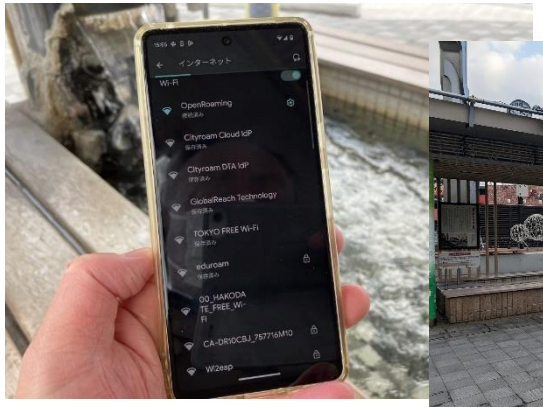
Osaka Free Wi-Fi

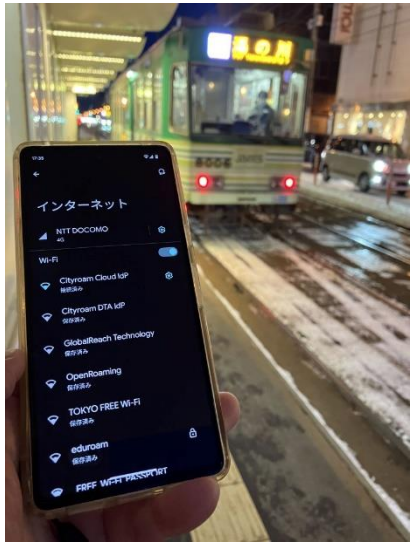
- Oct. 10, 2024 –
- EXPO 2025を視野に、交通機関から重点的に整備.

https://ofw-oer.com/

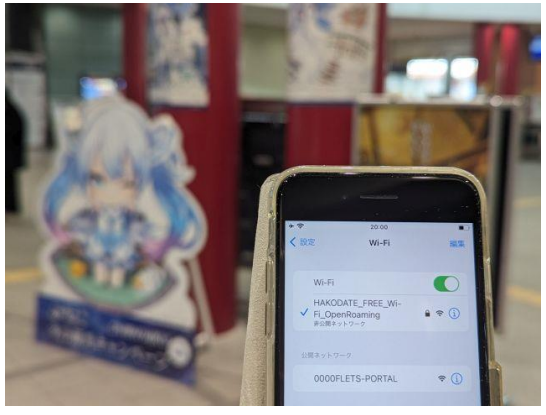
HAKODATE FREE Wi-Fi

- Nov. 30, 2023 –





空港、市電、足湯でも、
eduroam / OpenRoamingが利用可能



https://wi2.co.jp/release/press/2023/20231130-hakodate_openroaming.html

従来のフリーWi-Fiの問題点

- 利用者の同意を得ない、または、不十分な同意確認の下での、
  - 個人情報 (属性) 利用
  - 行動解析
  - アクセス制限、フィルタリング

ローミング環境ではどうか？

- 初等・中等教育機関向けのeduroamでは、フィルタリングの要望が出ることがある. (本来、端末側で処理すべきだが……)
  - 「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」
- サイトブロックなどを実装するには、利用者の同意が必要.
  - 訪問者から同意を得るための仕組みがない.
  - サイトごとにAUPが大きく違うなら、ローミングのメリットが薄くなる.

この研究の取り組み

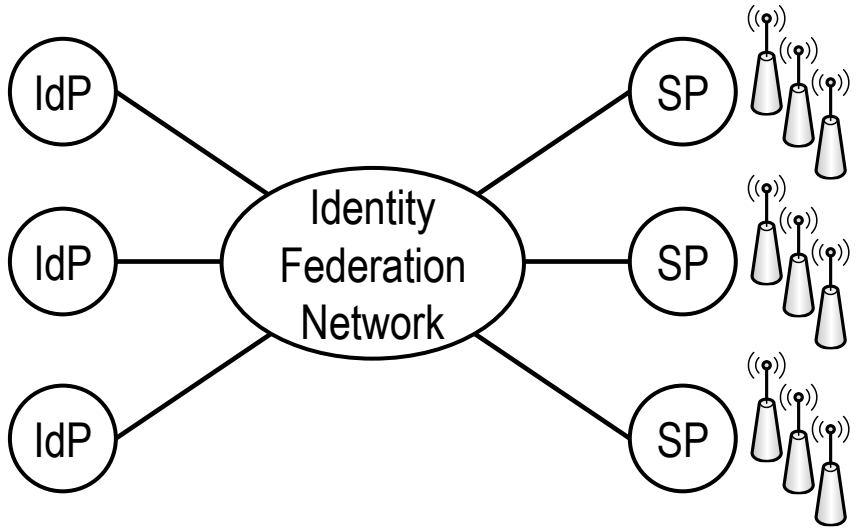
1. ローミング基盤の認証負荷削減
   - 期限切れアカウントによる高負荷を抑制

2. 属性情報を安全に通知する技術の開発
   - 利用者からの明示的な「同意取得」と、SPへの通知
   - 同意に基づいた属性情報の通知・交換
   - 同意に基づいたアクセス制御や行動解析

✔ プライバシー保護が不可欠
✔ オフライン認証でも使えるような仕組みにしたい
(機内Wi-Fiや被災地対応のため)

ローミング環境におけるプライバシー保護

- IdPとSP (ANP) が分離されている.
- プライバシー保護のため、実際の利用者が誰か、SPには知らせない.
  - Outer-Identity は anonymous@example.com のように匿名化.
    認証情報はEAPで保護された Inner-Identity として端末から送出.
  - EAP-TLSでは、SPに対してクライアント証明書を秘匿 (要TLS 1.3).
  - MACアドレスランダム化や, ユニークになりにくい属性値を利用.



SPが好き勝手に
データ取得・行動解析
できないようにしたい

ANP: Access Network Provider (eduroamで言うSPに同じ)
EAP: Extensible Authentication Protocol

1. ローミング基盤の認証負荷削減

問題

- 期限切れアカウントを利用者が削除してくれない (卒業生など)
- 認証失敗した端末は頻繁にリトライする → ローミング基盤の負担増
- 有効期限をプロファイルに仕込めるのは一部のOSだけ
- Deauthentication Imminent が提案されたが、まだ普及していない
- (例)「代理認証システム」(利用機関数 134, 2023年度実績)
  期限切れによるAccess-Reject: 全体の9.6%
  Login incorrectの行数: 20.4%

対策案

- 期限切れアカウントの認証要求を、基地局に近い所で止める.
- 中間プロキシやIdPの負荷やログの増大を抑制する.

1. ローミング基盤の認証負荷削減 (続)

提案手法

realmに有効期限を埋め込む．(SPでも見ることができる)

(例) anonymous@vu250331.example.com

安全性

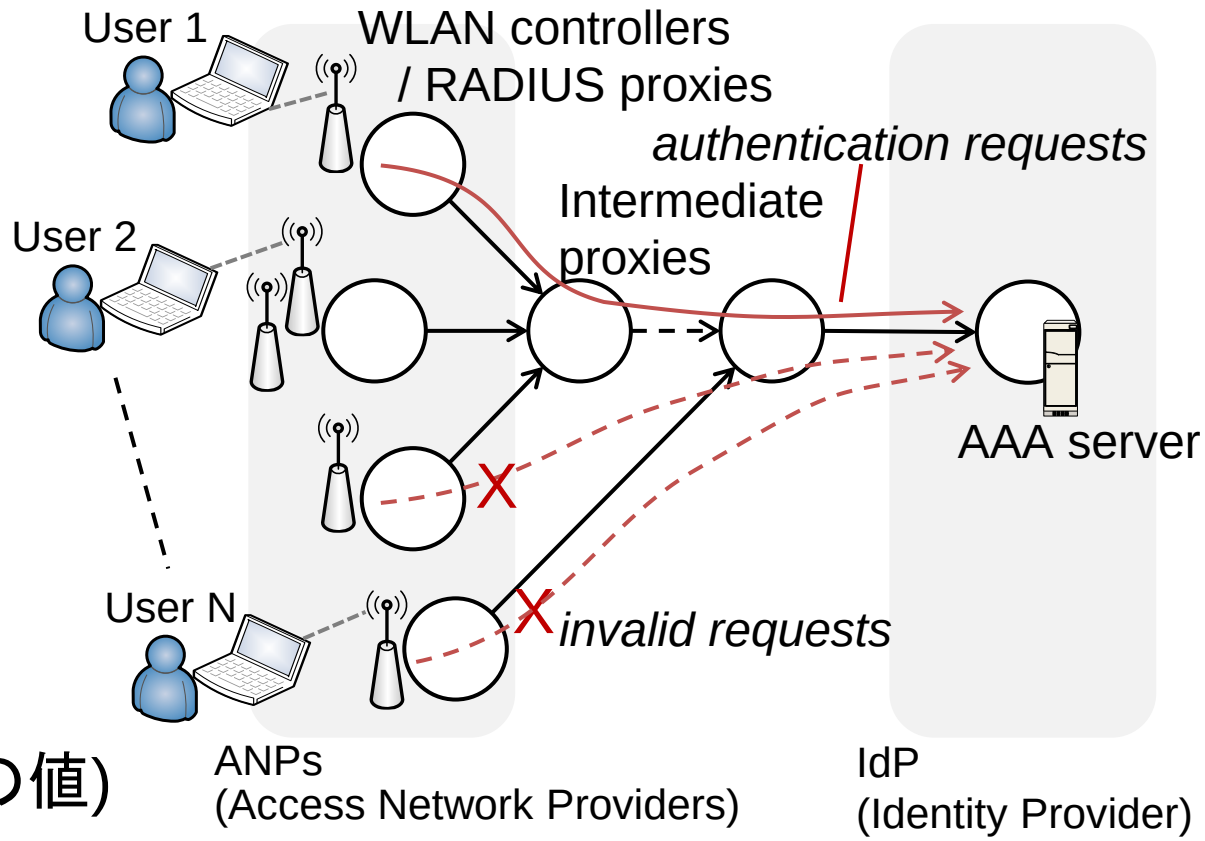
利用者が偽造できるが、IdPは真の有効期限を知っているので、問題にならない．

注意点

利用者ごとにユニークな値にならないようにする．(プライバシー保護)

効果

上限20%程度の抑制 (前述の値)



2. 属性情報を安全に通知する技術の開発

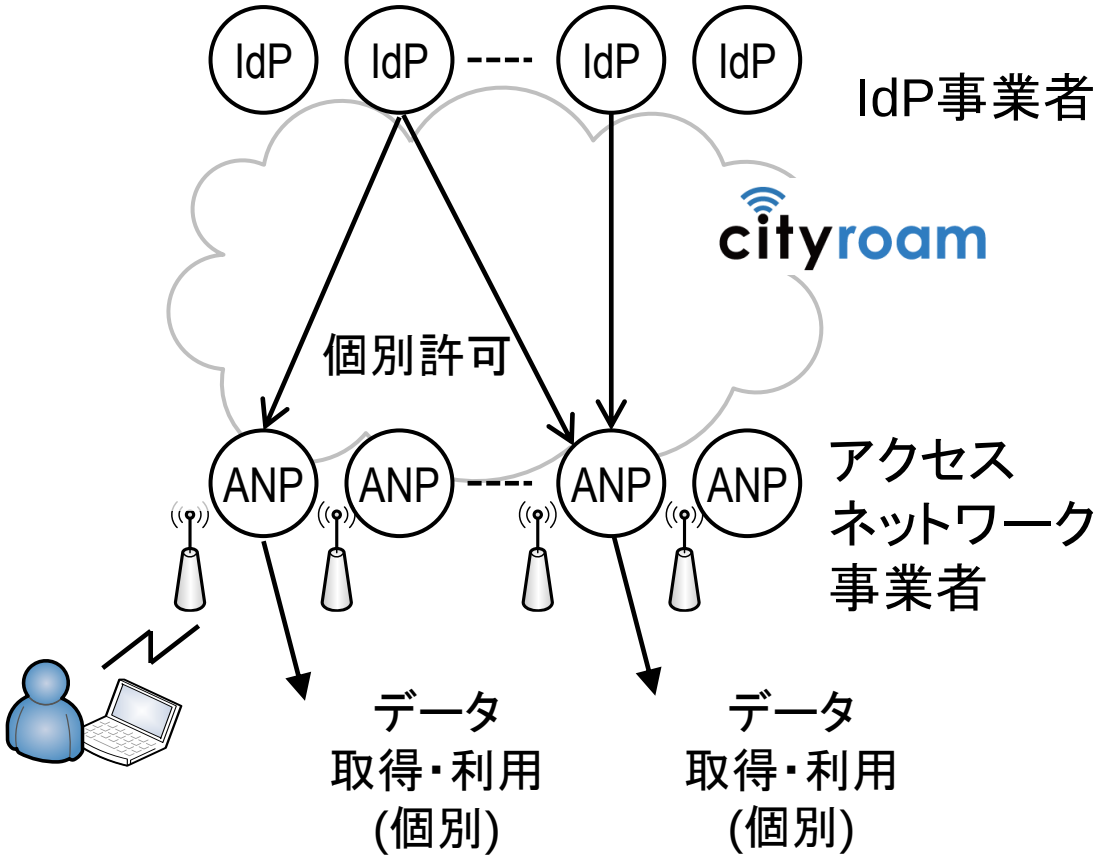
- オーナーから要望の多い属性値・行動情報
  - 年齢層
  - 性別
  - 国籍
  - 言語 (ブラウザの設定値などから取得)
  - 利用環境 (アプリ等の開発に反映)
  - 無線LANの利用場所，滞在時間
  - 移動経路 (ショッピングモール内で立ち寄った店舗や，観光スポットの分析)

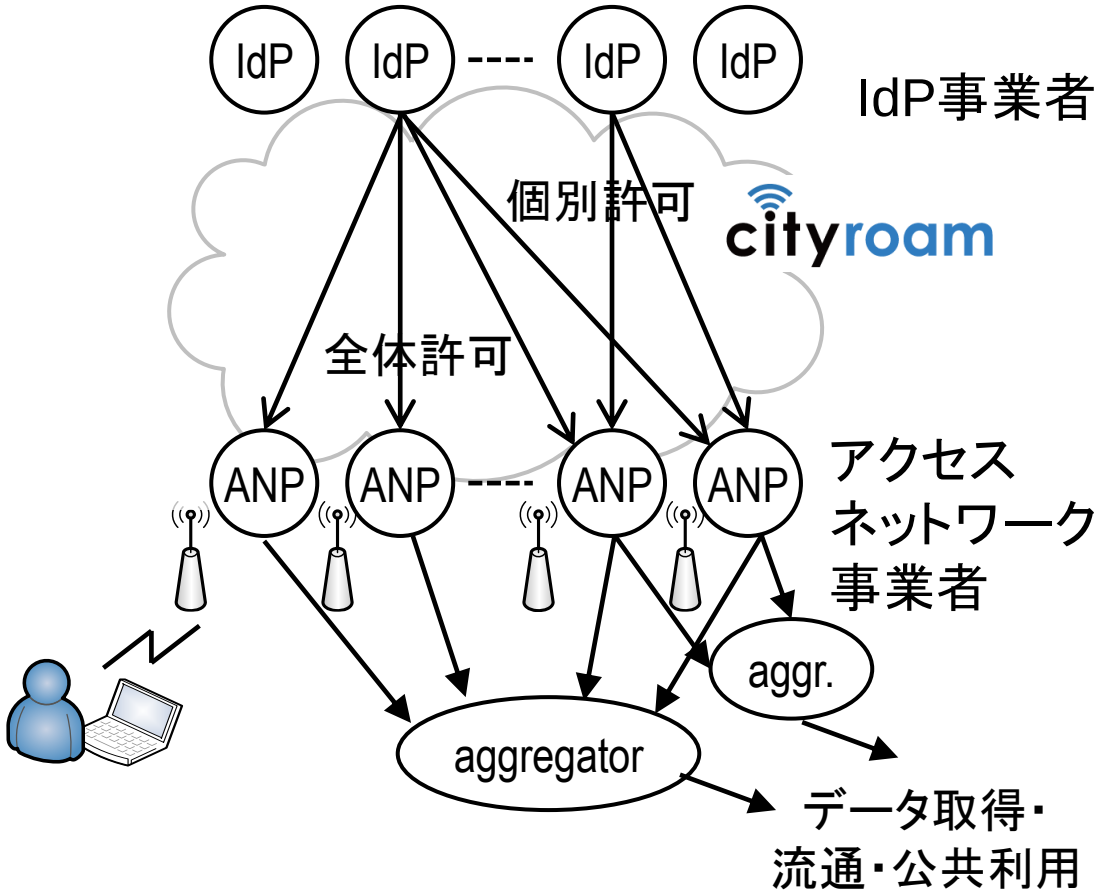
ビジネスに有用なものがある

- 特に自治体Wi-Fiで要望のある用途
  - 移動経路
  - 観光スポットの分析
  - 防災・減災・都市設計のための分析

観光・都市設計などの重要な用途がある

2. 属性情報を安全に通知する技術の開発 (続)





2. 属性情報を安全に通知する技術の開発 (続)

問題

- RADIUSサーバがベンダ固有属性 (VSA)を送出する方式は、オフライン認証では使えない.
- realmに埋め込んだ文字列は利用者やANPに偽造される恐れがある.
- ANPは、行った行為について同意が得られていると、偽の主張ができる.

提案手法

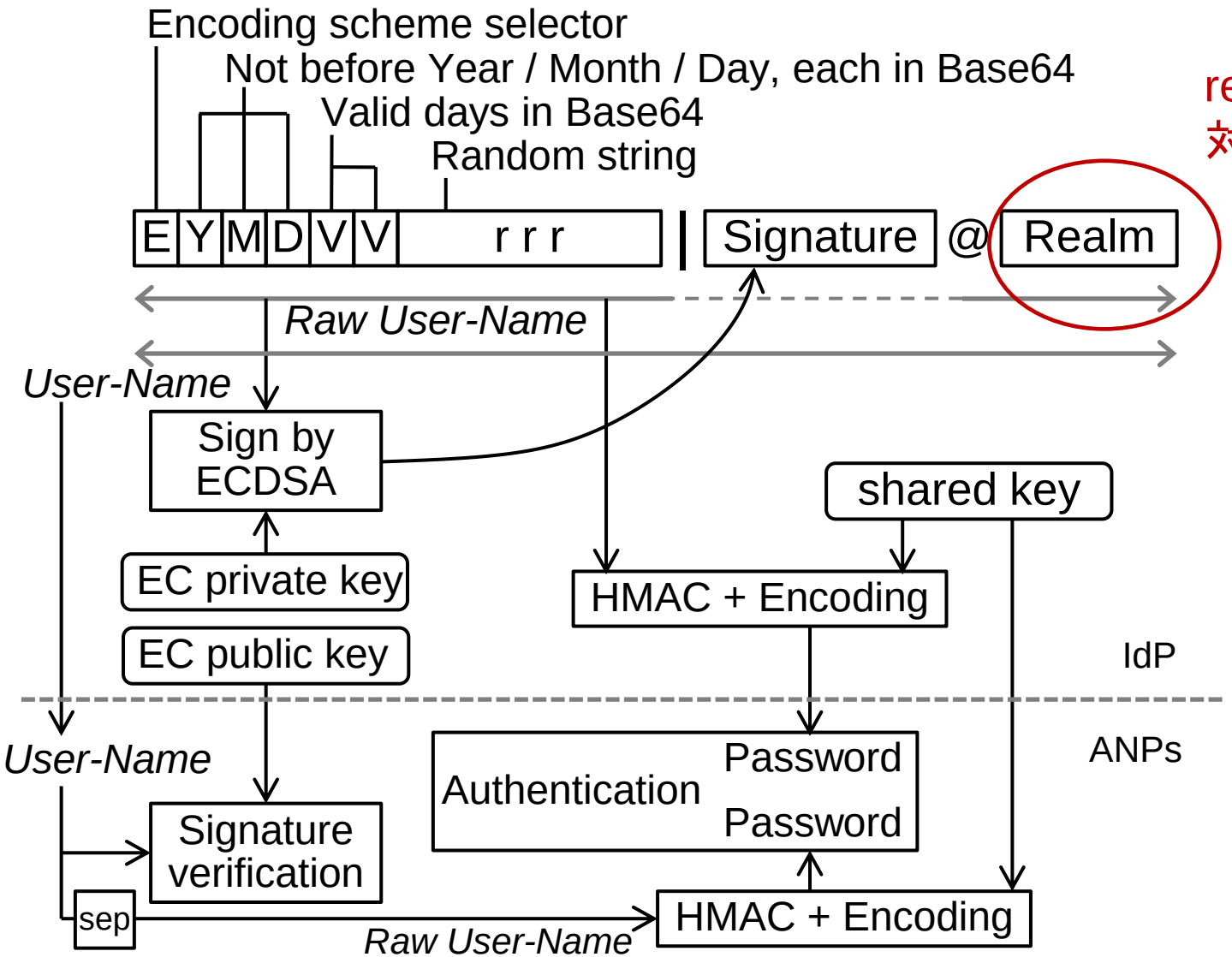
HMACベースのオフライン認証方式と署名の組み合わせ (既開発) を改良.

暗号化した属性値 (同意フラグも含む)をrealmに埋め込み、電子署名する.

制約事項

- Outer-Identityのユニーク化を避けるため、シンプルな属性値に限定.
- 暗号にランダム性を入れにくい. (プライバシー保護とのバランス)

HMACと電子署名によるローカル認証 (改)



realmも署名の
対象に入れる (改良点)

ID:
CYEPBcv7T|MCUCEQC3SwoCbmNfPno3KRvZP7qLAhBg+cHjunGEo6CwKPzHeNz7@xattrjeztqpof52n2xxm7vphkeocp5aqbil43.example.com”

PW:
OAKkwZe/

Ref. Hideaki Goto, “Disruption-tolerant Local Authentication Method for Network Roaming Systems,” JIP, Vol.32, pp.407-416, 2024.

まとめ

- eduroamやOpenRoamingなどのローミング環境では、利用者の同意や属性をIdPからSPに伝えるための標準的な手段がなかった. → フリーWi-Fiの普及の妨げ
- 利用者の同意に基づいたアクセス制御や属性利用、行動解析が必要な旨を説いた.
- 期限切れアカウントの認証要求が多く、ローミング基盤の負担になっていた.
  (有効期限を属性値としてSPに通知したい)
- プライバシー保護に配慮した、属性交換の仕組みを開発した.

- (課題) 具体的に交換する属性値の取捨選択
- (課題) プライバシー保護と暗号強度の考察