Mar. 4, 2025
IAM session @ APAN59, Yokohama

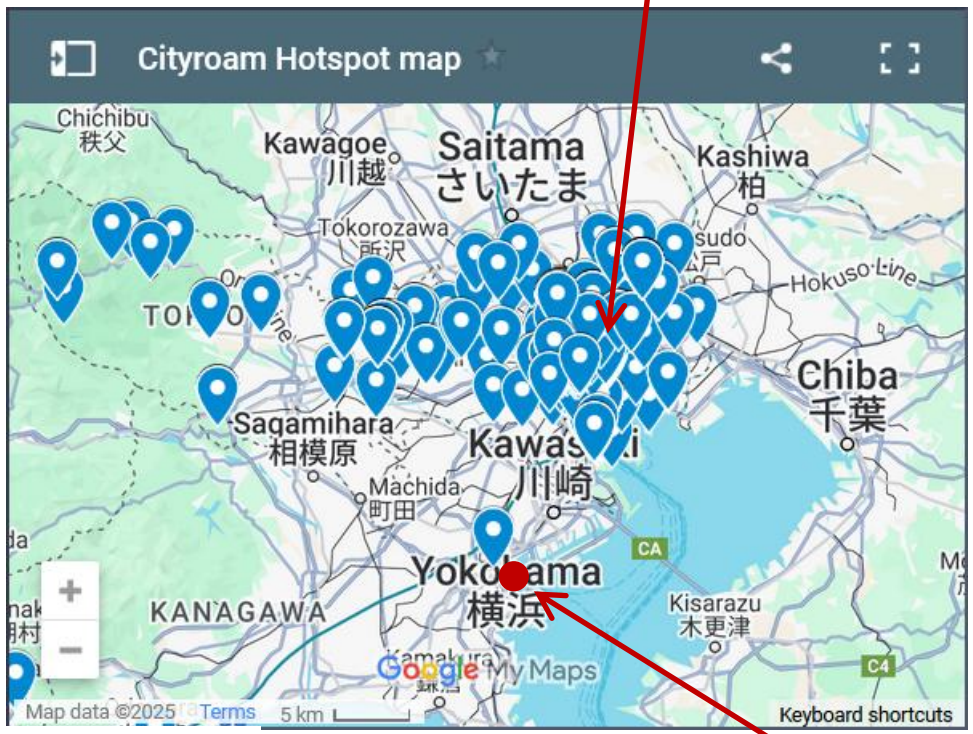
Building a national Secure Wi-Fi infrastructure with international roaming

– Supporting the society and education in the digital era –

Hideaki Goto　Tohoku University / NII, Japan

OpenRoaming is available here!

Tokyo



APAN59 venue

OPENROAMING™
ここから登録
Sign up now
TOKYO
FREE Wi-Fi
TOKYO METROPOLITAN GOVERNMENT

https://wi-fi.metro.tokyo.lg.jp/en/

Google, Apple, or LINE account
is required for Sign-Up.

cityroam

for more locations, etc.

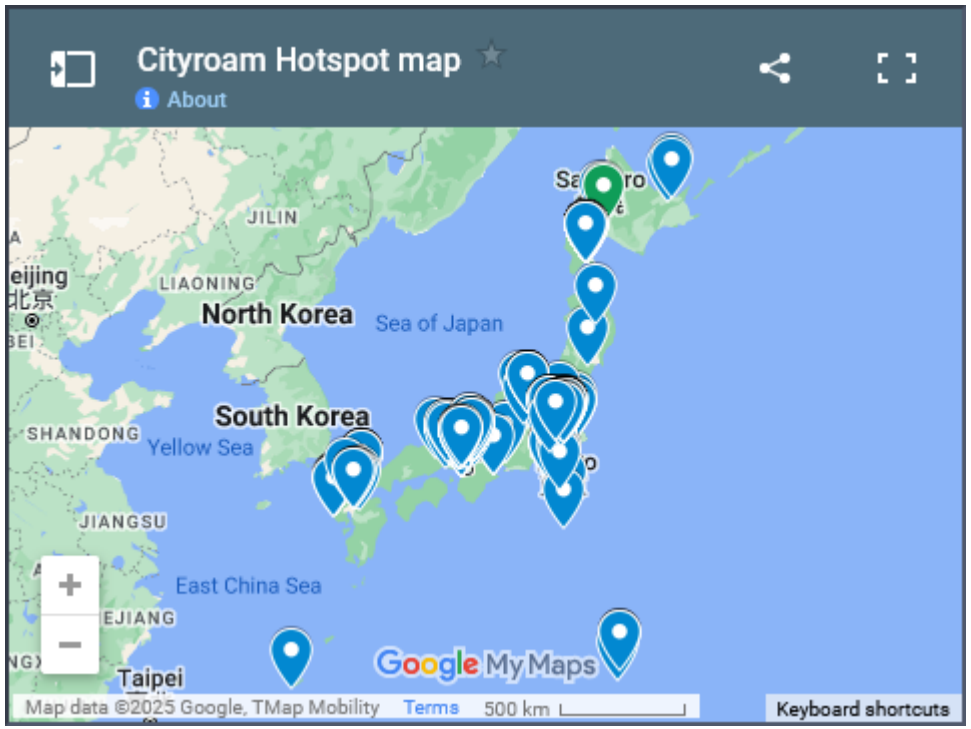
Nationwide Cityroam deployment in Japan

Your countries can have a similar one !

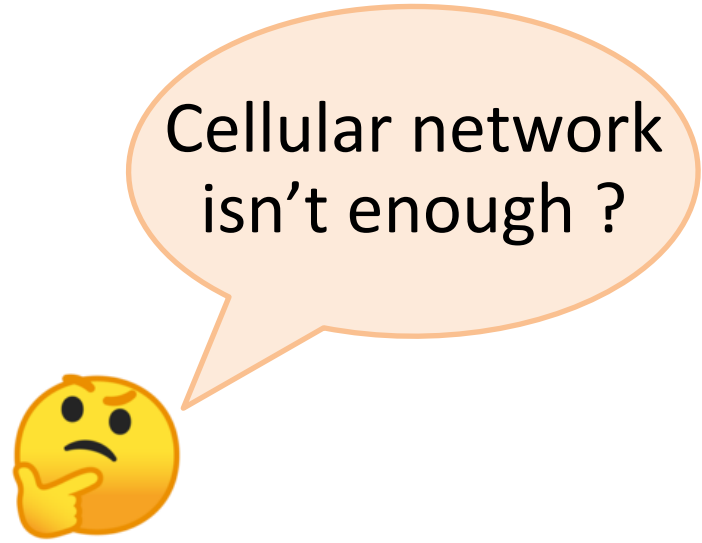
- Cityroam, a federation providing secure roaming system for Public Wi-Fi since 2018.
- All sites provide both eduroam and OpenRoaming (2020-).
- Unique sites across the nation.

cityroam

1000+ spots (Jan. 2025)



Why Public Wi-Fi?



Pros

- Higher bandwidth than cellular networks
- Autonomy
- Easier deployment with freedom
- Less expensive deployment and operation
- Less technical knowledge

Cons -> can be overcome

- Low (or no) security in the legacy Free Wi-Fi systems
  - Many people say “security is a concern”.
    They are still using it or won’t use it at all !
- Cumbersome registrations here and there
- Unclear privacy protection measures

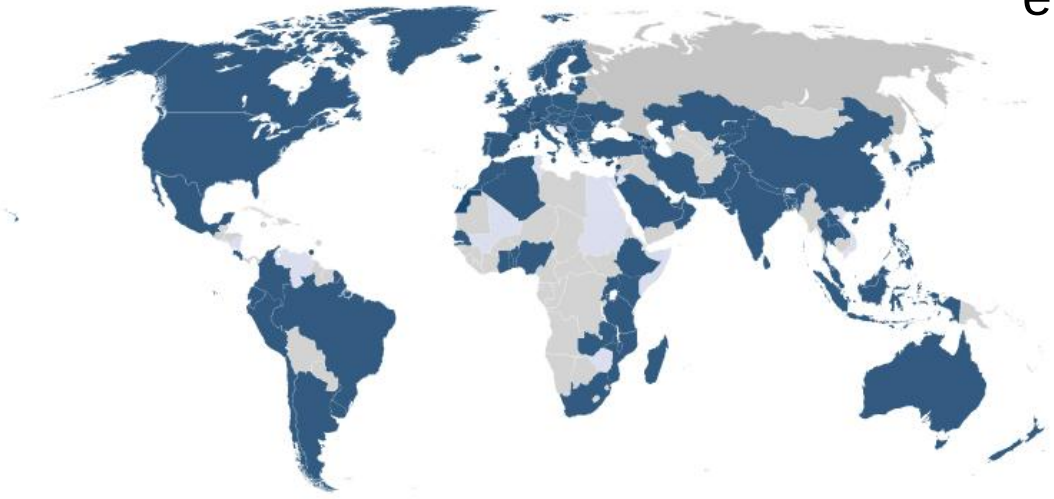
Public Wi-Fi as an infrastructure

- WiFi4EU's case
  - Project for EU-wide Free Wi-Fi deployment
  - Public Wi-Fi is a society infrastructure like water and electricity.
  - Provide network access means to everyone including those who cannot have a DSL at home.
  - Access to digital government services is crucial.

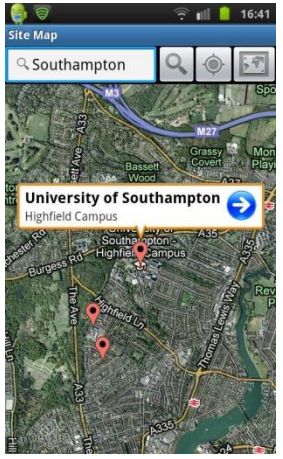
> *"Everyone benefiting from connectivity means that it should not matter where you live or how much you earn. So we propose today to equip every European village and every city with free wireless internet access around the main centres of public life by 2020.*
> ***Jean-Claude Juncker - State of the Union speech, September 2016"***

eduroam (RFC 7593)

- Secure Wi-Fi Roaming system for Research & Education
  - Started as a pilot at TERENA (now GÉANT).
  - 104 countries/territories worldwide (as of 2025)
  - De facto standard of campus Wi-Fi in the world.
  - Mutual benefit system.
  - High security and usability based on 802.1X.

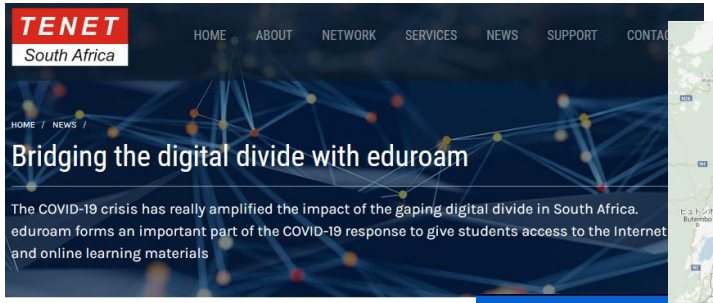


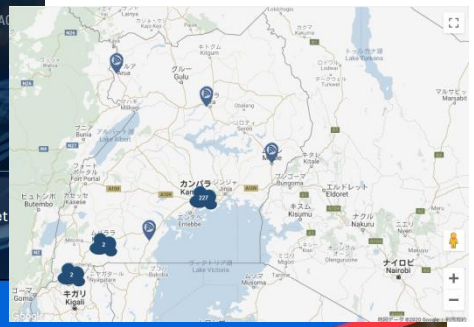
eduroam Companion (Android, iOS)



Off-campus eduroam as a digital infrastructure

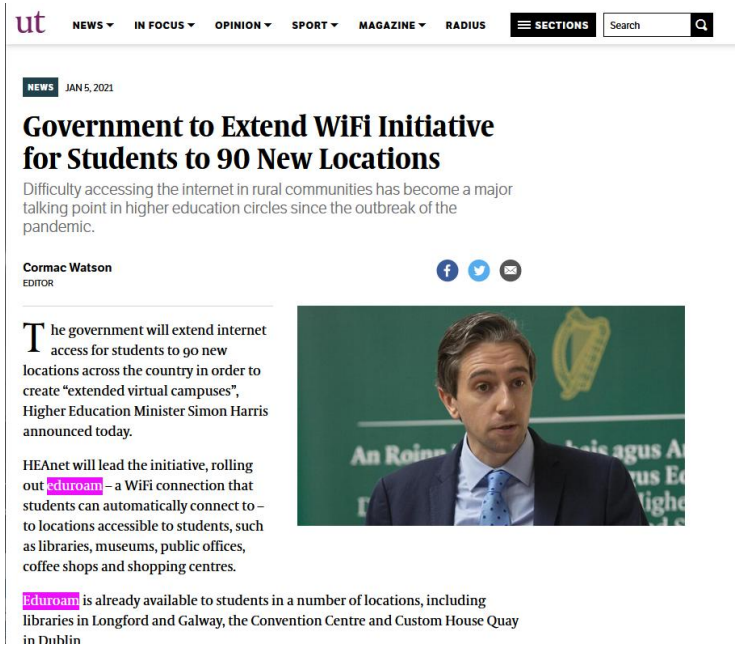
South Africa:
eduroam at most universities, addressing digital divides and COVID-19 (July 2020)





Today a University of Cape Town student living in Khayelitsha can access eduroam, the high-speed Internet offered by nearly all South African universities and an additional 105 countries around the world, at their local library. A University of Witwatersrand (Wits) student living in Sebokeng needs only to travel 30 minutes to North-West University's Vaal Triangle Campus to download their course content and videos quickly and for free on the eduroam network, while a University of South Africa (UNISA) student anywhere can check the eduroam interactive map to see where their closest internet access point is.

RENU in Uganda:
Town-wide eduroam to help students learning under COVID-19 (Oct. 2020)

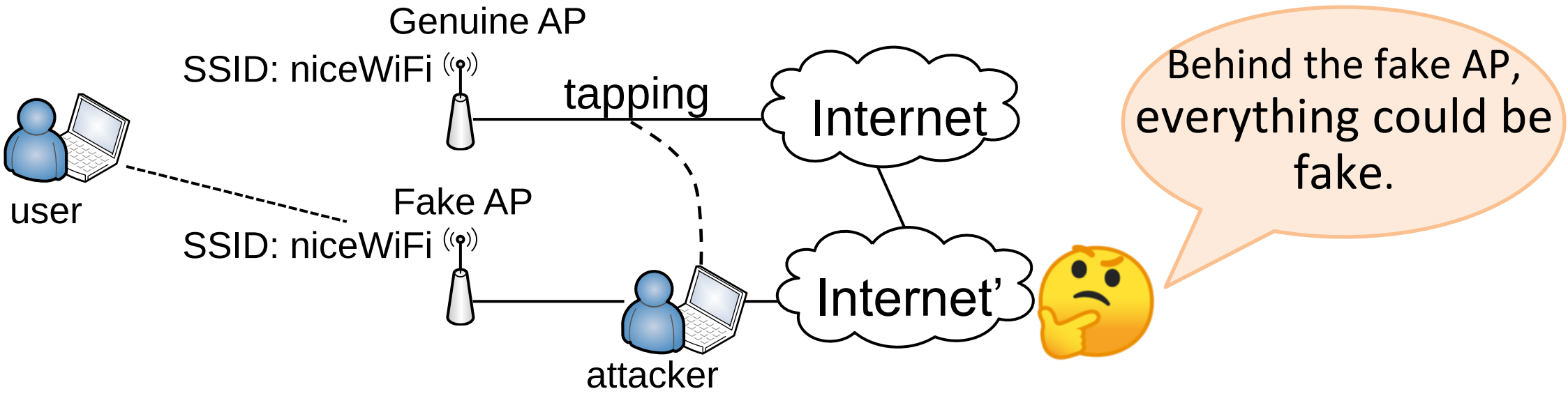


"Extended virtual campuses" in Ireland (Jan. 2021)
http://www.universitytimes.ie/2021/01/heanet-to-extend-wifi-initiative-for-students-to-90-new-locations/

Jisc, UK (May, 2021)

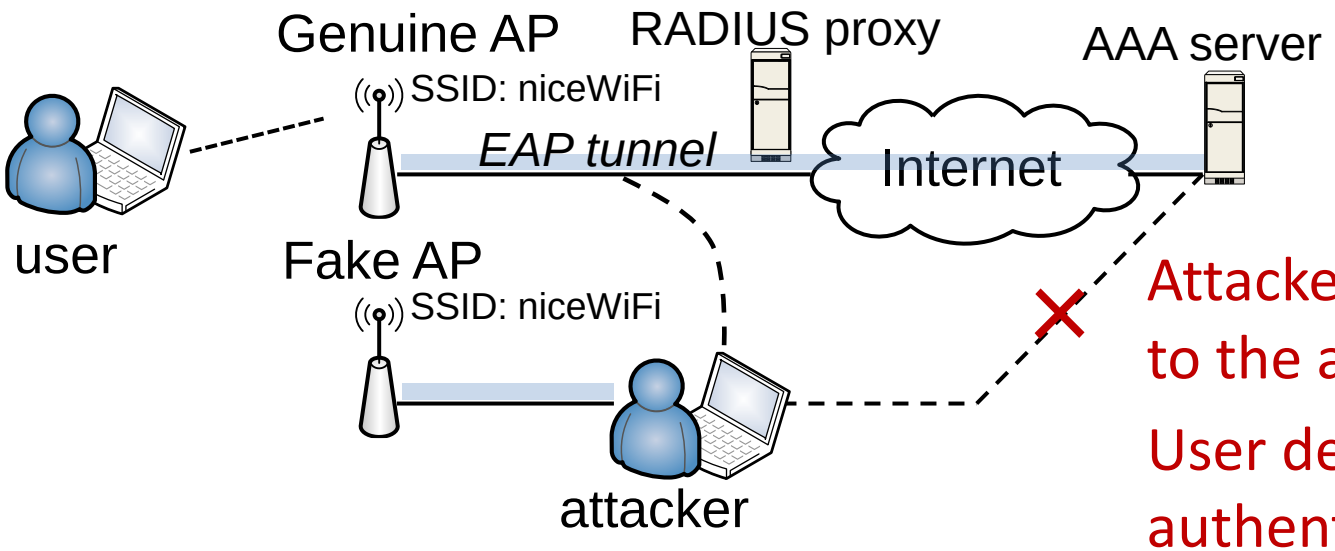
Evil Twin Access Points

- If *open Wi-Fi* is used, there's no security or privacy.
  Anyone can plant an Evil Twin AP.
- If many people are using *WPA Personal*, sharing a *Pre-Shared Key* (PSK), the network is also unsecure.
- If you have joined a fake network, many attacks become possible.
  E.g., MITM, eavesdropping, malware injection, and active attacks.



Secure Public Wi-Fi Using WPA2/WPA3 Enterprise

- Users should check whether the AP is a genuine one provided by an authorized operator.
  Server authentication in 802.1X makes it possible.
- Password protection as well as privacy protection is needed.
  EAP (Extensible Authentication Protocol) can provide protection.



Attacker cannot gain access to the authentication server.

User device fails in the server authentication before sending out password.

Wi-Fi Security is not only for end-users…

- Security for Wi-Fi operators:
  - Make clear the responsible bodies.
  - Keep user traceability in case of network abuse or crime.
    User Verification is important.

- Security for the society:
  - Suppress crimes such as fraud.
  - Suppress organized crimes and terrorisms.
  - Disaster prevention and mitigation utilizing user activity analysis.
  - Smart City design through data analysis.
  - Securing people's communication means under disasters.

WBA OpenRoaming

- **Seamless connection experience for everyone.**
  eduroam-like, but not limited to Research&Education community.
  - eduroam since 2003, now 100+ countries/territories.
- **Advanced and multipurpose** than eduroam (RFC 7593).
- Based on Passpoint and WRIX framework.
- PKI and RadSec + Dynamic Peer Discovery
  - Similar to eduroam, but in larger scale.
- Two policies using different RCOIs
  - Settled: Accounting and intermediary are required.
  - Settlement-free: No roaming fee. Much easier adoption.

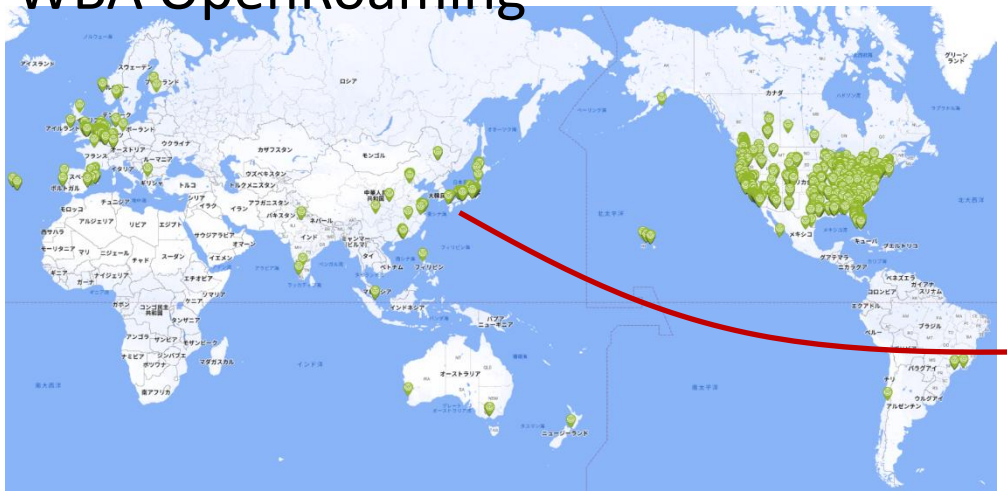
Fit with our purposes.

RCOI: Roaming Consortium Organization Identifier

Cityroam's rapid growth – why?

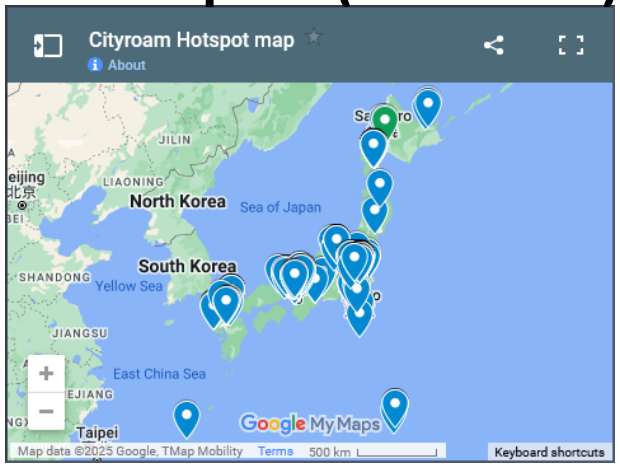
- Organized a Roaming Federation
  - **Community supports** (seminars, tech tests & discussions, etc.)
  - -> **Wireless Identity Federation Association** (est. Apr. 2024)
- Affordable roaming platform with Simplified inter-connections (central hub).
  - IdP: eduroam, Cityroam Cloud IdP, operators in Japan, telcos/ISPs and cities overseas via OpenRoaming™ Wireless Broadband Alliance
- eduroam/OpenRoaming combined architecture
- Involvement of Municipal Wi-Fi (multi-vendor, multi-operator scheme)

WBA OpenRoaming

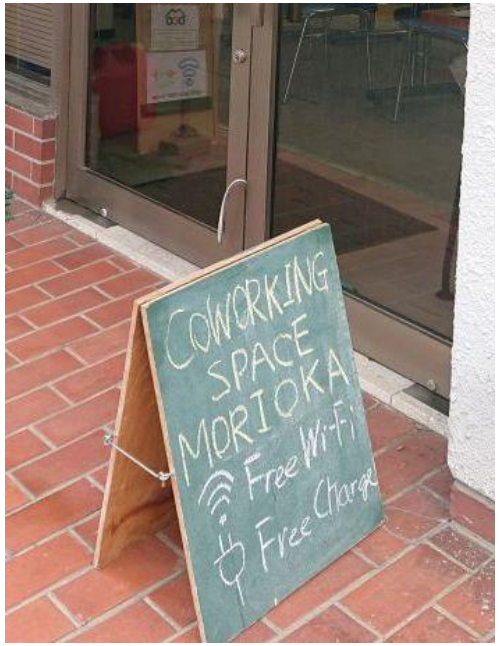


90+ spots (Jan. 2023)

1000+ spots (Jan. 2025)



Cityroam sites – early adopters of OpenRoaming



Co-working space in Morioka
(OpenRoaming was added
in 2020)

Conference Center in Nagano
(May 2021)

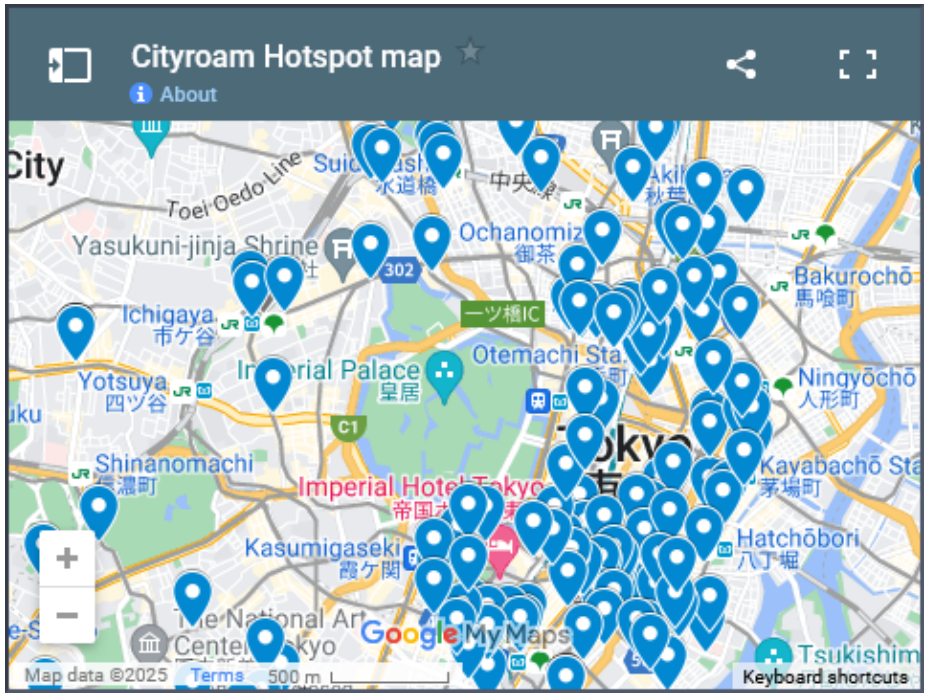
Hot Spring facility in Nagano
(May 2021)

Resort Hotel & Complex in Ise
(Feb. 2022)

Vending machines in
Kyoto City Parks
(May 2020)

TOKYO FREE Wi-Fi supports OpenRoaming

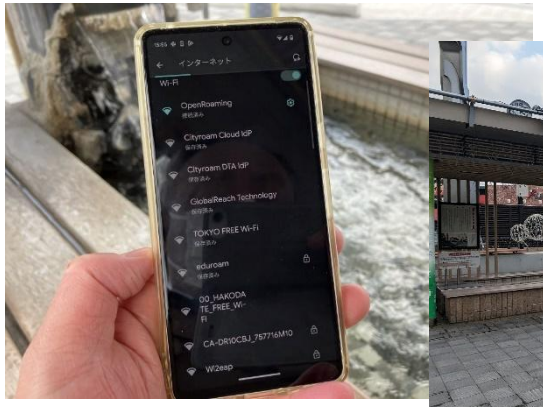
- Released on Mar. 31, 2023
- Tokyo Metropolitan Government + KDDI / Wire & Wireless (Wi2)
- Enhanced security, safety, and usability. ☺

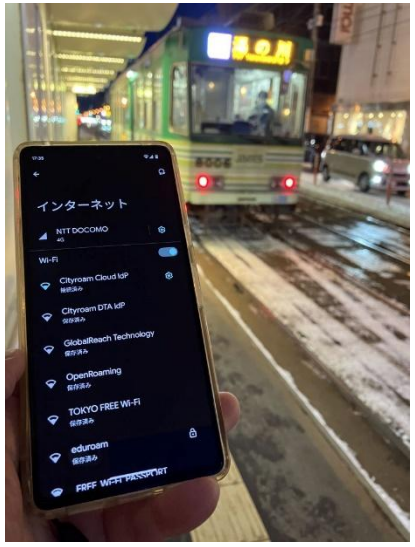


https://wi-fi.metro.tokyo.lg.jp/en/

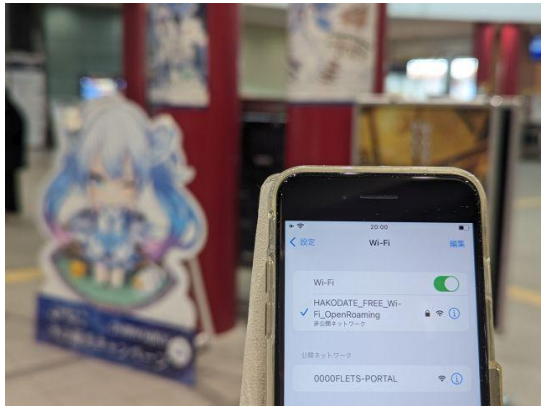
HAKODATE FREE Wi-Fi

- Nov. 30, 2023 –
- eduroam and OpenRoaming become available.





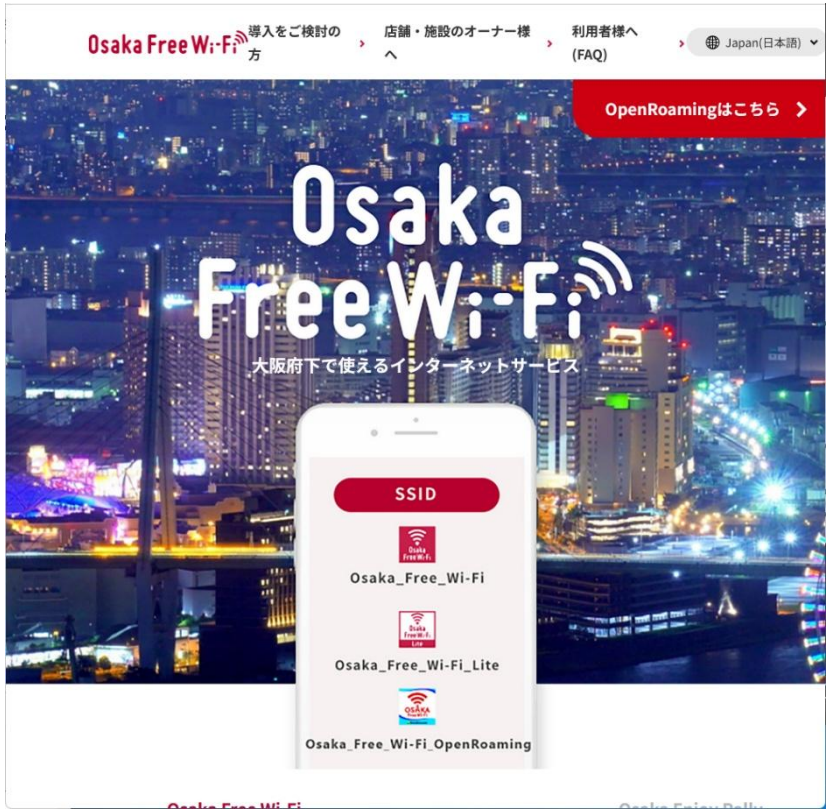
Enjoy eduroam / OpenRoaming
at the footbath (hot spa), airport, trams !



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

Osaka Free Wi-Fi

- Oct. 10, 2024 –
- Initial deployment focuses on Public Transport. (for EXPO 2025)



OSAKA Free Wi-Fi
Open Roaming

https://ofw-oer.com/

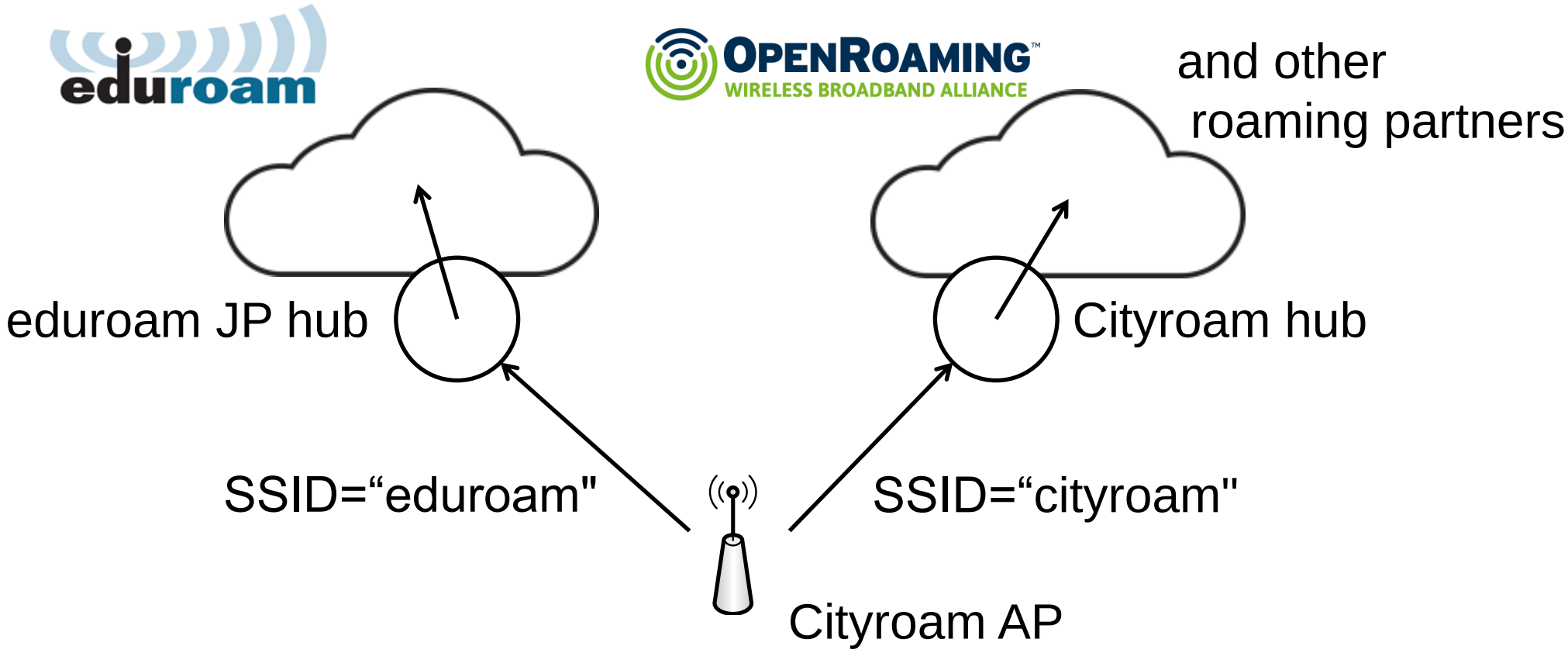
Why eduroam/OpenRoaming combination?

- eduroam has a matured **autonomy**.
  - Virtually monolithic.
    If you see “eduroam” SSID, **the service is always there**.
  - Single basic policy + minor variants.
    (won’t bother users so much)
  - eduroam can be “**a group of reliable IdPs**”
    that provides good credentials with strict user verification,
    probably accompanied with enlightenment.

- Many students and staff are carrying devices already configured with eduroam.

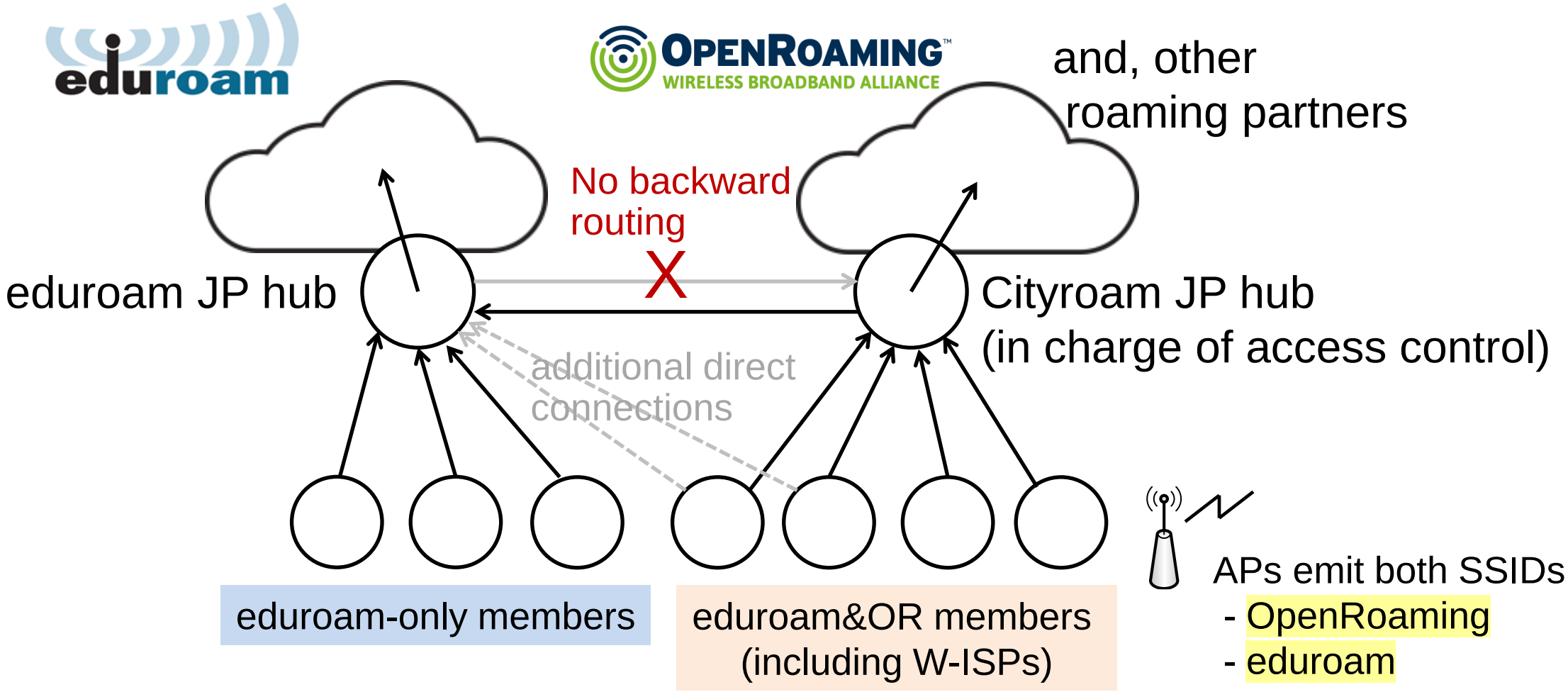
Great advantage

eduroam traffic separation – basic (but complex) implementation



- Require multiple RADIUS connections
- Complex AP configuration

eduroam/OpenRoaming combined architecture



Forward to eduroam if ("%{Called-Station-Id}" =~ /:eduroam/)

(e.g. Called-Station-Id = de-ad-be-ef-01-23:eduroam)

Access analysis in the eduroam/OpenRoaming combined deployment

It is quite important to lower onboarding hurdles.

- **Municipal Wi-Fi profiles have become popular.** (>50%)
- SIM-based authentication is second popular.
  - User authentication is quite stable, with few errors.
- **eduroam accesses account for 10%.** (as of 2024)

Embedded profiles work well!

Summary

- eduroam / OpenRoaming combined deployment is quite useful for the societies in the digital era,
  supporting education, lifelong learning, tourism, and economy.
- Many municipalities in Japan (Kyoto, Tokyo, Hakodate, Kobe, Himeji, Osaka, etc.) have already deployed Cityroam.
- Cityroam architecture is open. You can do the same. 👍

On-going work

- **User activity analysis, data acquisition and sharing, under users' consent**.
- eduroam for K-12, IoT, and some other applications.

Supplementary slides

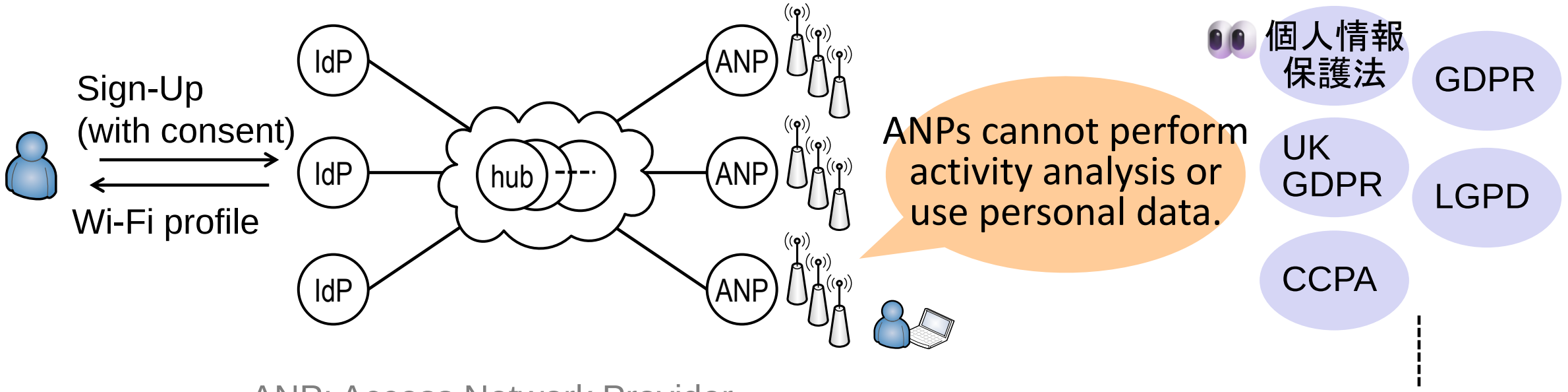
Development of a user data sharing system

- Owners want to know / do …
  - Age group
  - Gender
  - Nationality
  - Language (browser setting)
  - Device/OS (for app development)
  - Wi-Fi usage location and staying time
  - Travel routes (e.g. shop-hopping in a mall, tourist sites), etc.

- Especially, municipalities want to know / do …
  - Travel routes
  - Analysis of tourist sites
  - Analysis for disaster response / mitigation, and urban design

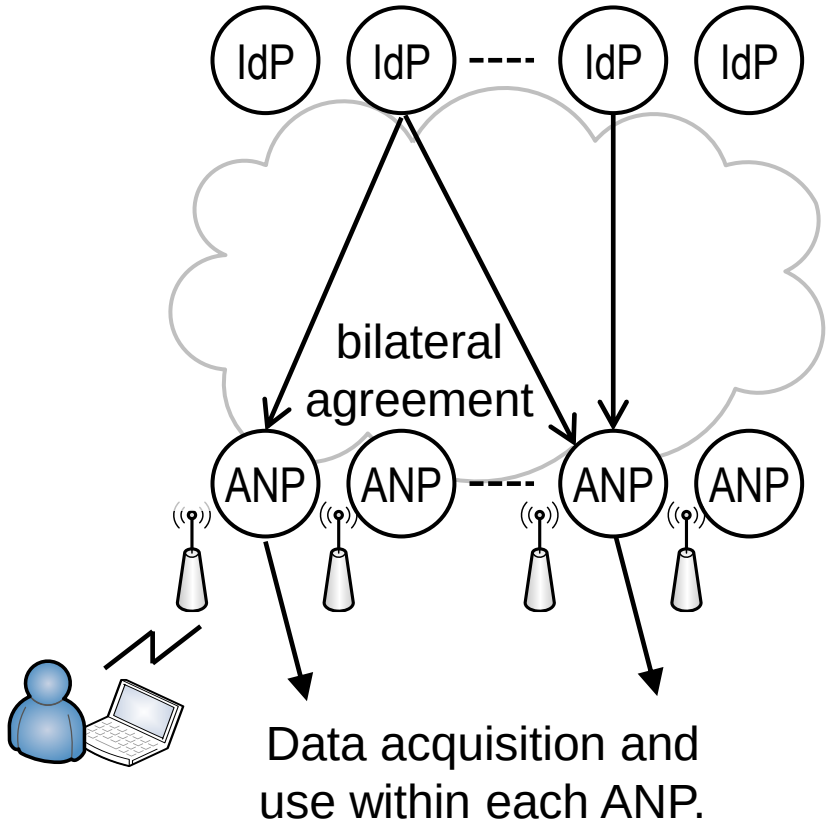
Challenges in user activity analysis and data usage

- IdP and ANP are separated.
- **ANPs cannot see “real user ID” or obtain user’s consent.**
  - Outer-Identity is anonymized, e.g. anonymous@example.com
    Inner-Identity is protected by EAP tunnel from ANPs.
  - EAP-TLS (with TLS 1.3) hides the contents of Client Certificate.
  - Ephemeral MAC addresses, etc.

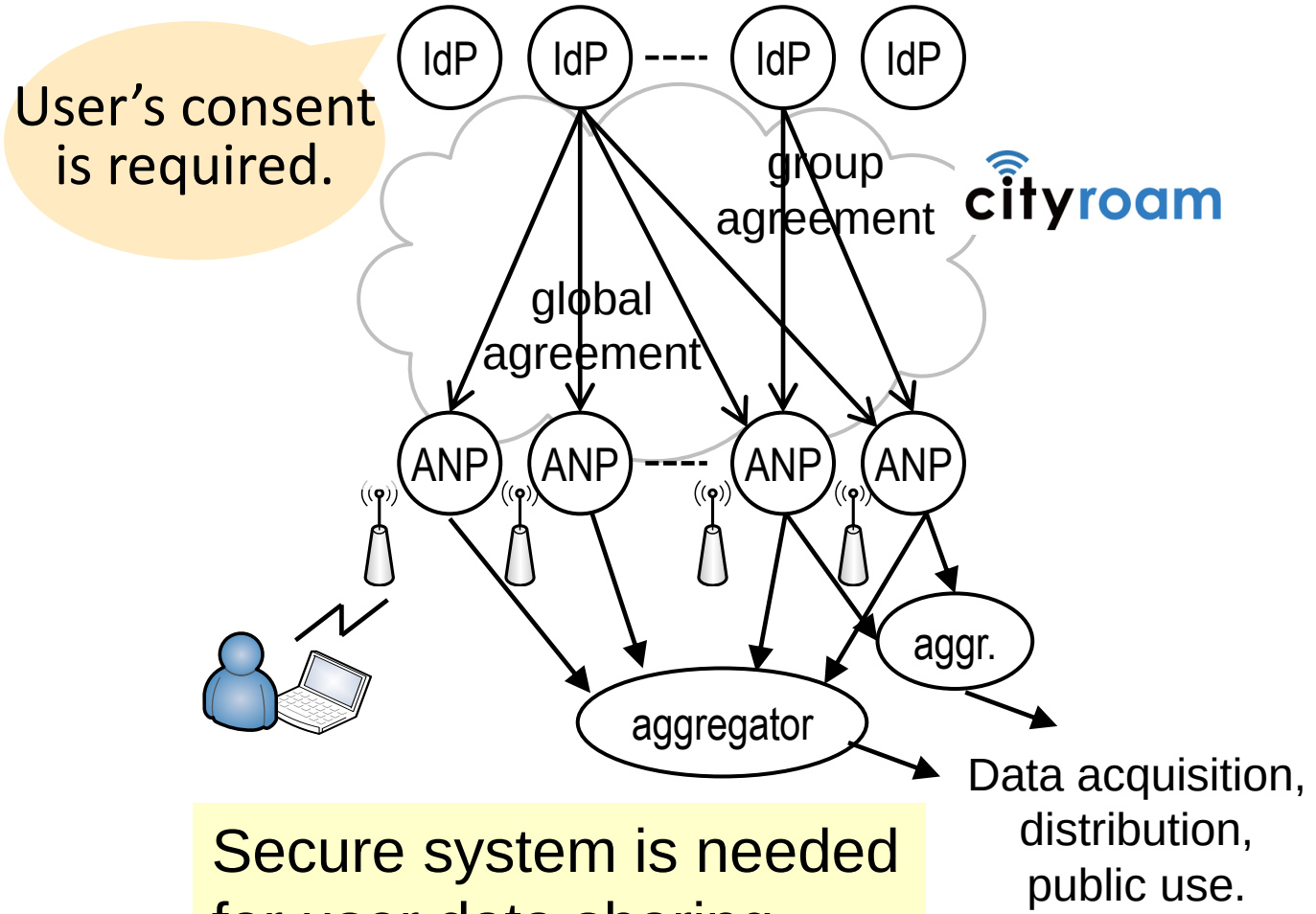


ANP: Access Network Provider
EAP: Extensible Authentication Protocol

Development of a user data sharing system



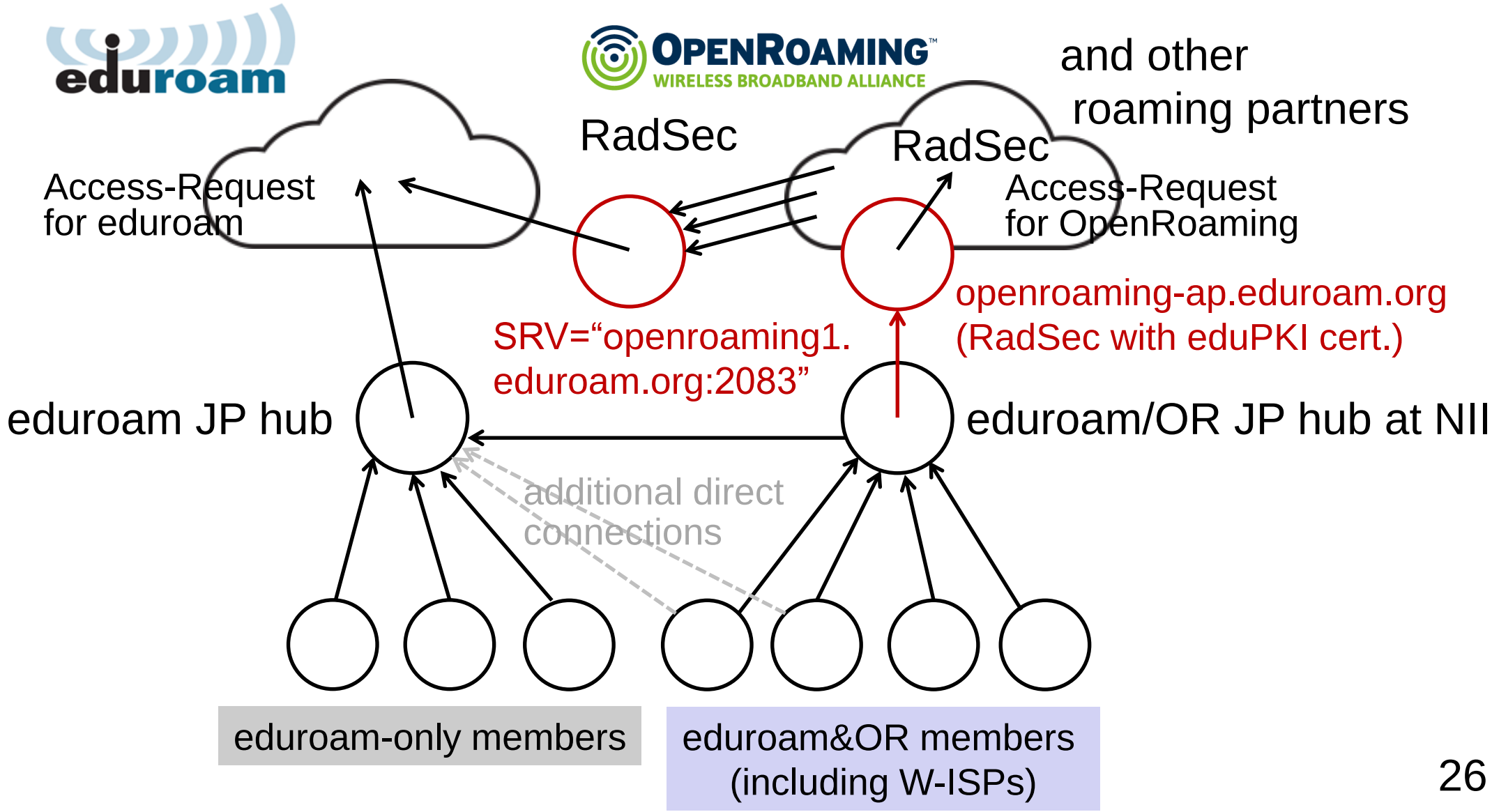
Bilateral agreements lead to low scalability.



Secure system is needed for user data sharing.

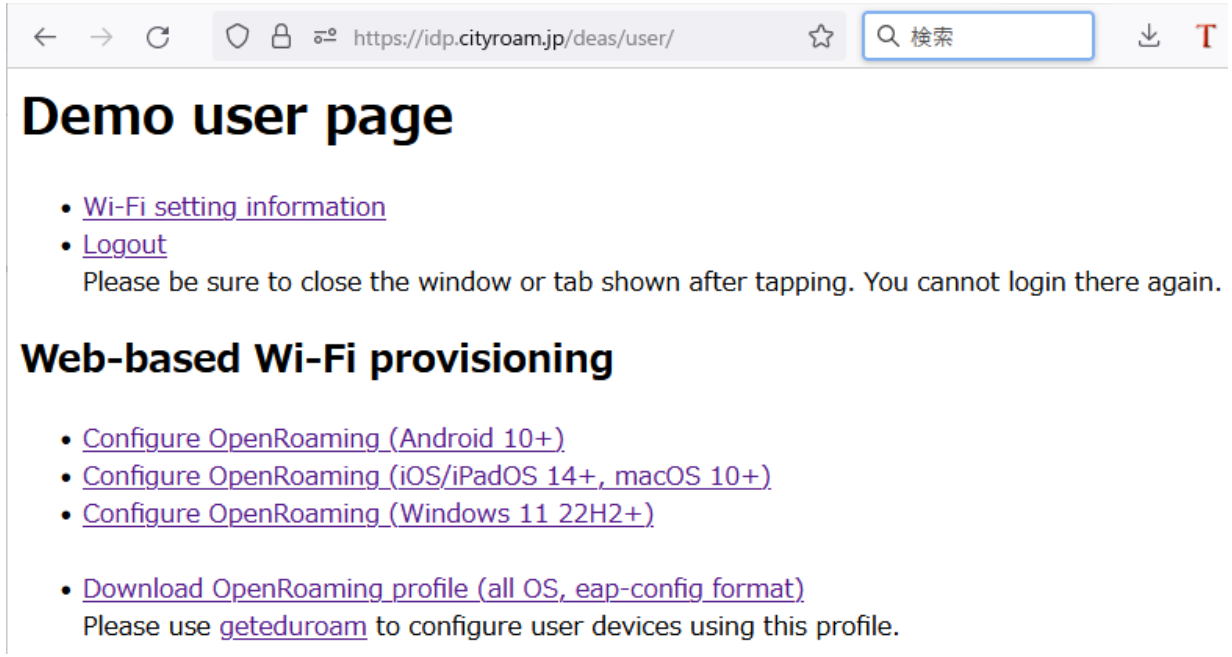
A part of this work is supported by a commissioned research program at National Institute of Information and Communications Technology (NICT) in Japan.

Using the eduroam.org OpenRoaming proxy (under dev.)



Passpoint Provisioning Tools

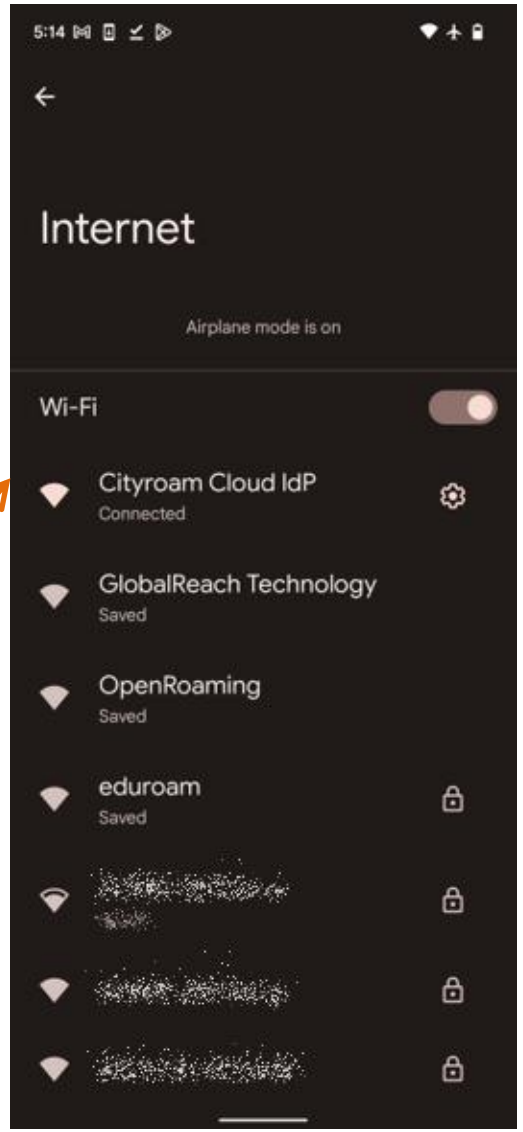
- Tools and codes that help operators develop their own Passpoint profile provisioning systems.
- The CGI perl scripts allow end users to download Passpoint profiles and configure Wi-Fi without typing in Wi-Fi ID/password or certificate.



https://github.com/hgot07/PasspointProvisioningTools

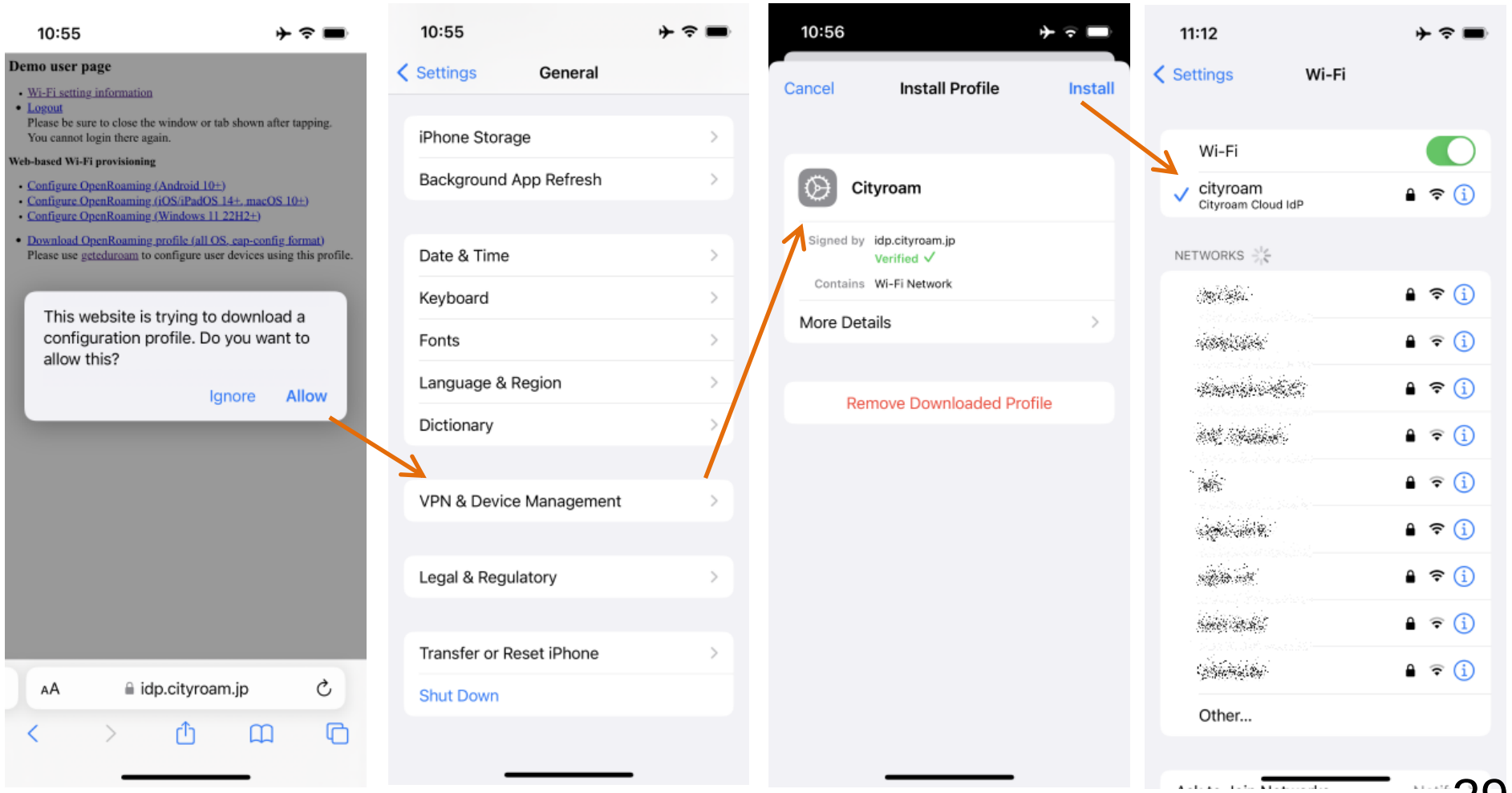
Profile Provisioning for Android

- Profile in PPS MO format (w/o signing)



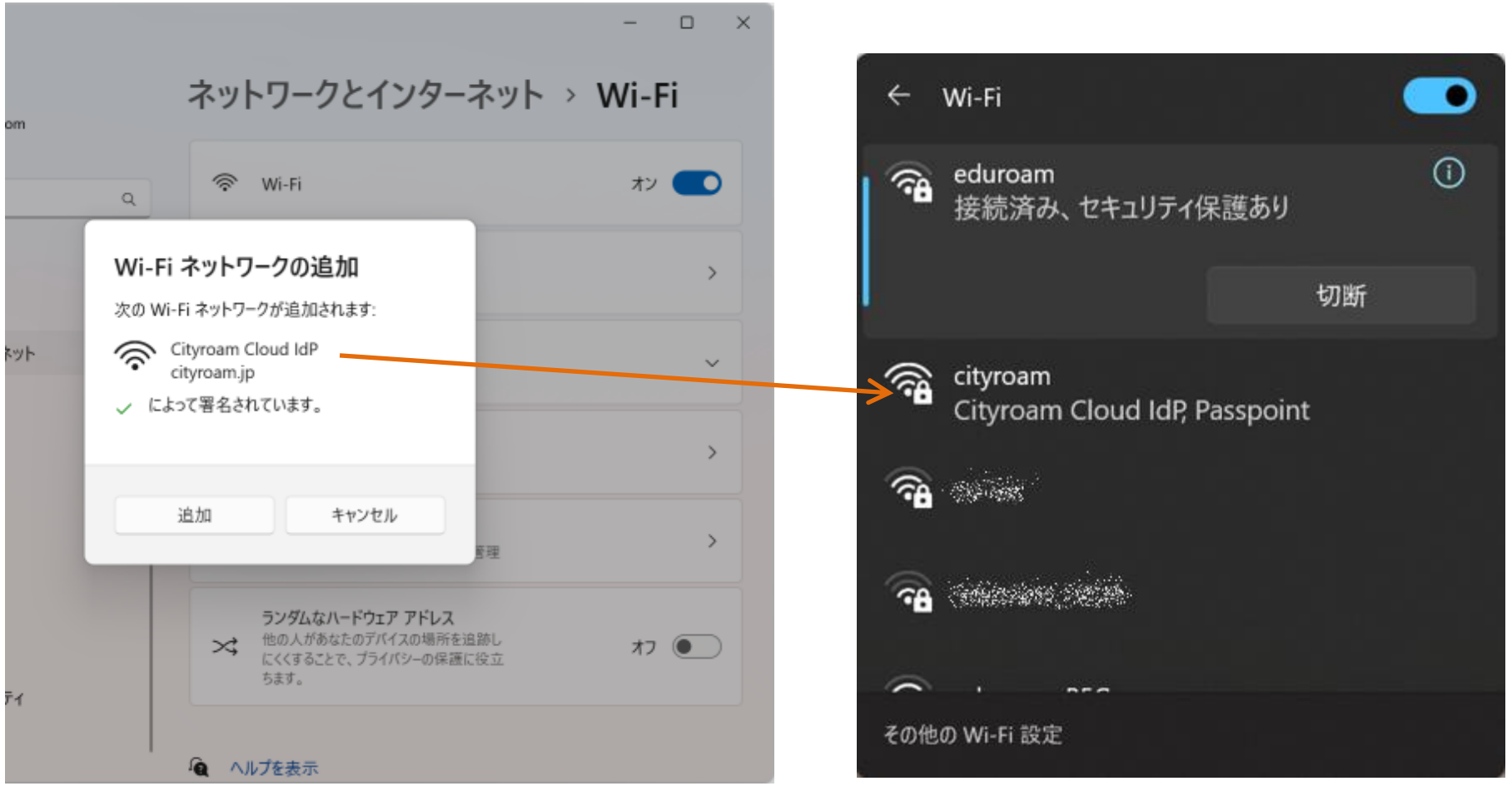
Profile Provisioning for iOS/iPadOS/macOS

- MDM using .mobileconfig
- Signing is optional.



Profile Provisioning for Windows 10/11

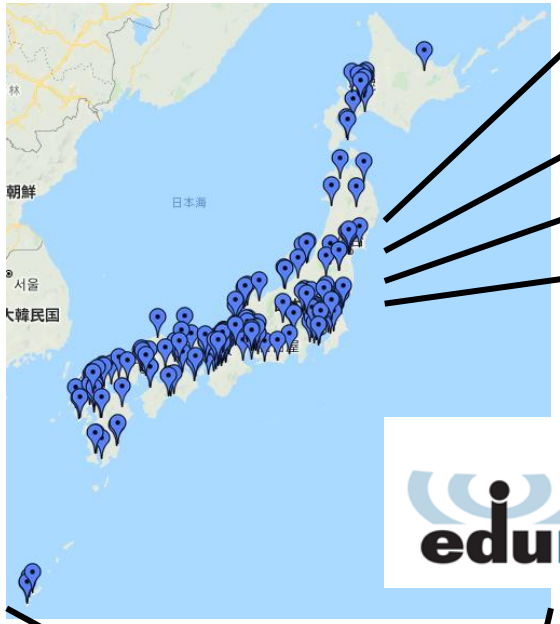
- ms-settings: URI scheme (EAP-TTLS only)
- Signing is required.
  (Windows 11 21H2 and older require EV cert.)



Collaboration with Public Wi-Fi services

- Virtual expansion of campus networks.

451 institutions in Japan
(Feb. 2025)



Academic cloud

Library
/ campus LAN

Internet

e-Journals

Cityroam since 2018

eduroam

Enable accesses to academic NW and contents from downtown areas

Federation

NW accesses using universities accounts

104 countries worldwide

130+ in-door APs at cafes, conference sites, large shops in and around Tokyo (2011-2020)