大学ICT推進協議会 2022年度 年次大会
2022年12月13日 発表

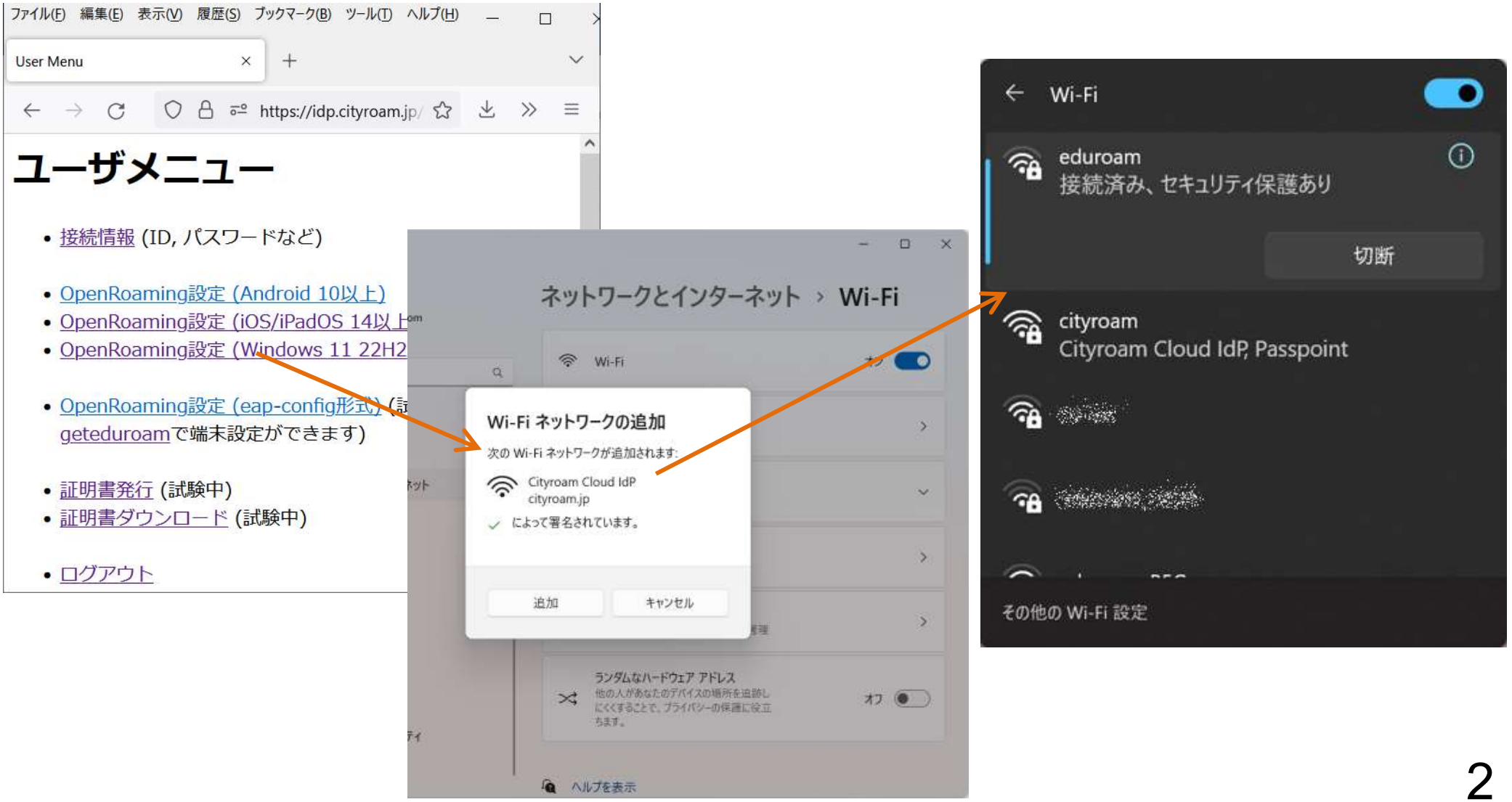
Wi-Fiプロファイルを用いた eduroam / OpenRoamingのパスワードレス設定

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4年度NII公募型共同研究の助成を受けました.

新時代の eduroam / OpenRoaming 設定

- ウェブサイトから数クリックのみで接続完了.
- ID・パスワード入力の必要なし！

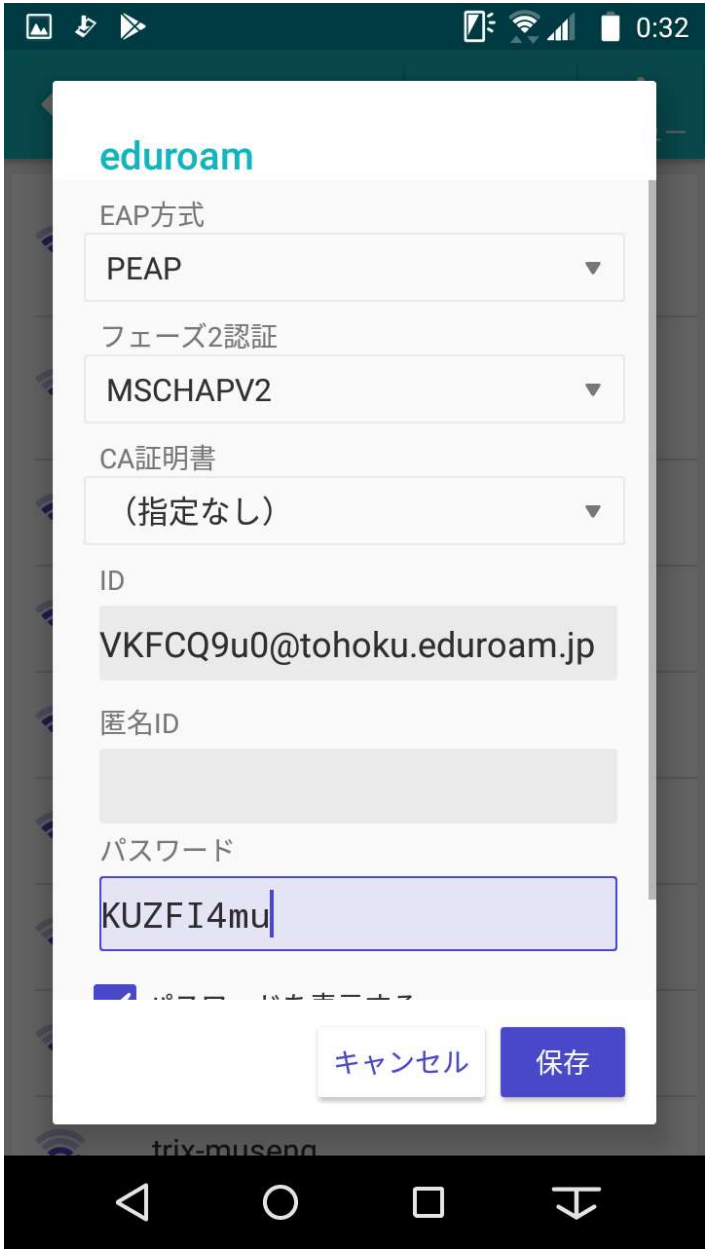


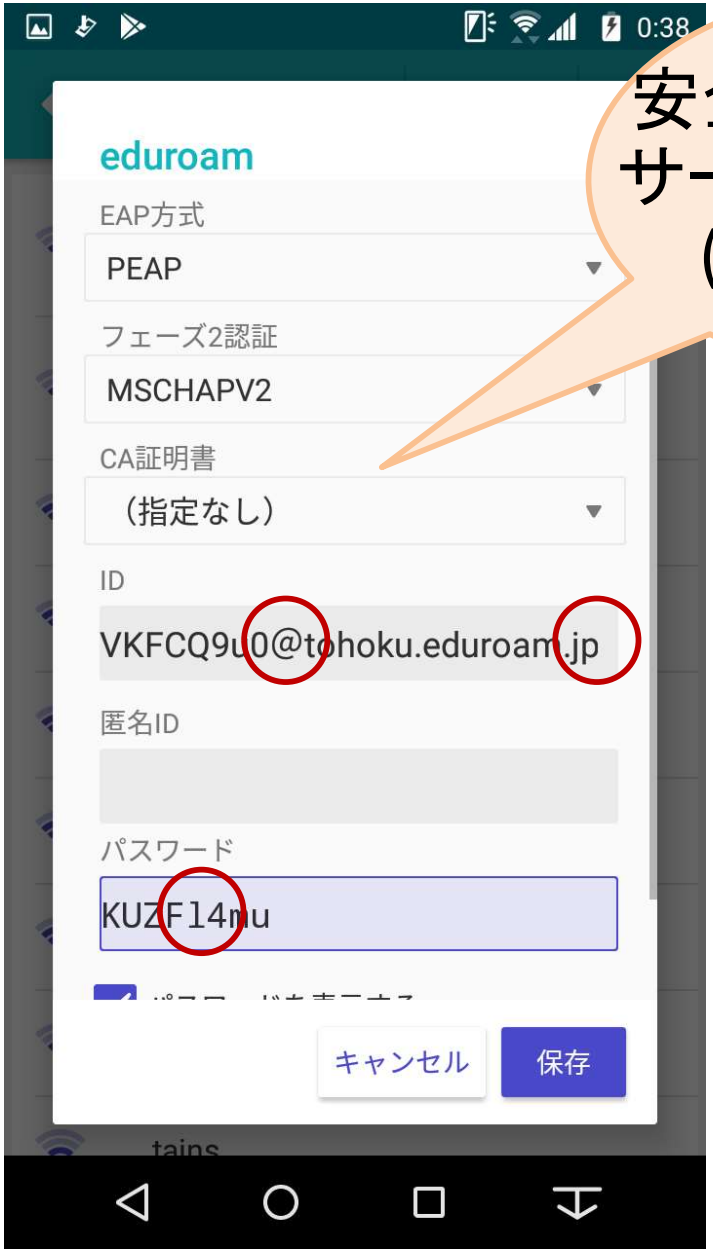
従来のeduroam設定

（NII オープンフォーラム2018より）

ID・PWの入力が手間

誤入力のトラブルが多い





安全のため、本来サーバ認証が必要(設定が面倒)

アットマークが全角

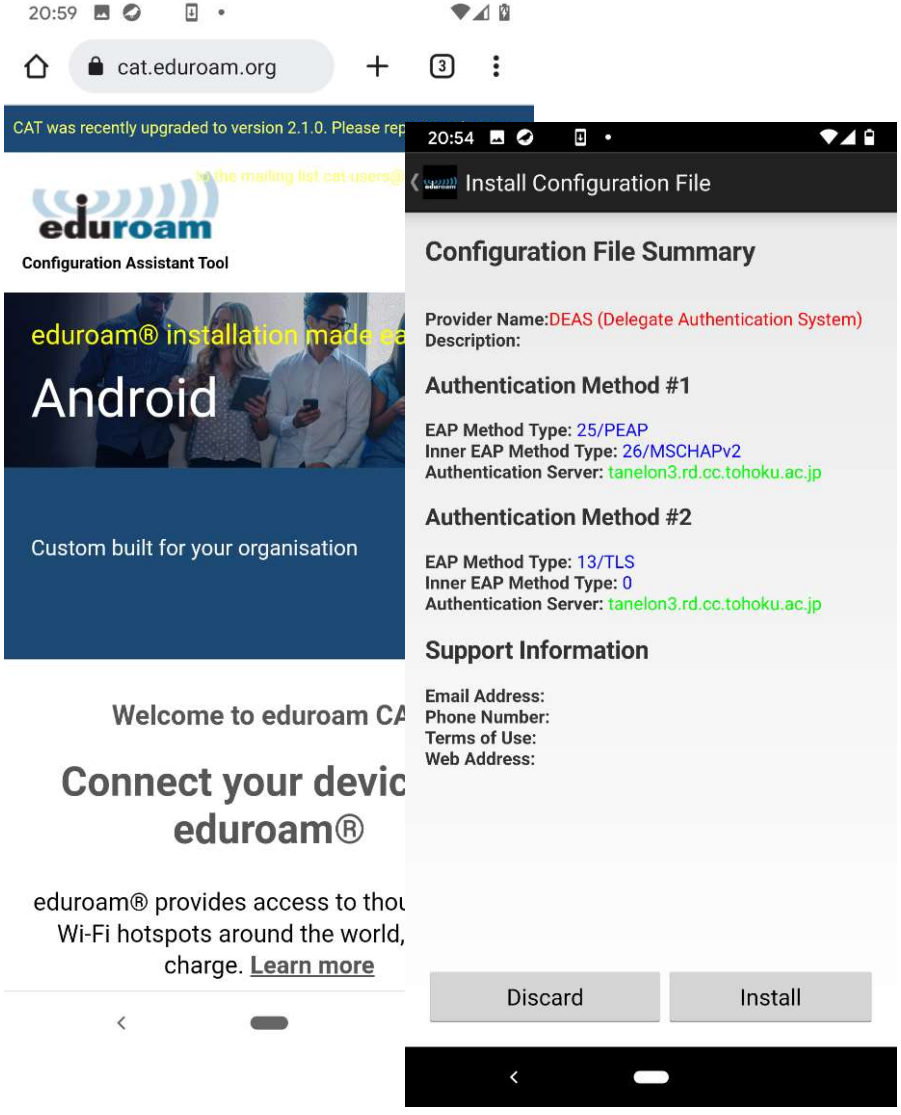
末尾に空白

アイ が エル

eduroam CAT / geteduroam

- 認証方式やサーバ認証の設定を、容易かつ確実に実施.

eduroam Configuration Assistant Tool



geteduroam app

現在のeduroam設定における問題点

- ID・パスワード入力の手間とトラブルが少なくない.
- eduroam CAT / geteduroamが十分に利用されていない.
- サーバ認証の設定が不十分だと、偽基地局による攻撃に弱い (パスワード漏洩など).

- うまく接続できないからといって、利用を諦めてしまう学生がちらほら.
- サービスデスクの負担
- …

容易かつ安全なオンボーディング手法が望ましい

次世代ホットスポット Passpoint のオンボーディング手法

- レガシーな802.1X認証と比べて設定項目の多いPasspointでは、「Passpointプロファイル」を使う.
- 認証情報や認証方式、サーバ認証、電子証明書などの、安全・確実な設定を実現.
- セキュア無線LANローミング基盤OpenRoamingの普及により、重要性が高まってきた.
- 主要なOSが「web-based Wi-Fi provisioning」の機能をサポートするようになった.
  MDM (Mobile Device Management)と共通点が多い.

- 実は eduroam にも応用できる.

でもまだOSSのプロファイル生成ツールがない

Web-based Wi-Fi provisioning 調査結果

スキーム	OS	概要
PPS MO (Per-Provider Subscription Mobile Object	Android	Wi-Fi Alliance標準. 署名なし. Passpoint専用. レガシー802.1XやPSKは非対応.
ONC (Open Network Configuration)	ChromeOS	Google製. なぜか後継がないまま非推奨になっている. Passpointに非対応. 教育研究コミュニティで、普及率が高く、重要.
.mobileconfig	iOS, iPadOS, macOS	Apple製. MDMをフルサポート. 署名はオプション.
ms-settings: URI scheme	Windows 10, Windows 11	Microsoft製. Windows 10, 11 (21H2)ではEV証明書による署名が必要. (Win 11 22H2でEV縛りがなくなった.) EAP-TLSに非対応. 有効期限のフィールドがない. OSの内部構造に強く依存. トラブルシューティングが面倒.
.eap-config	(OS非依存)	eduroamで10年以上使われている、OS非依存の形式. EAP-SIM/AKAに非対応. 予めアプリを導入しておく必要あり. (geteduroam, etc.) https://github.com/GEANT/CAT/blob/master/devices/xml/eap-metadata.xsd

eduroam Provisioning Tools
Passpoint Provisioning Tools

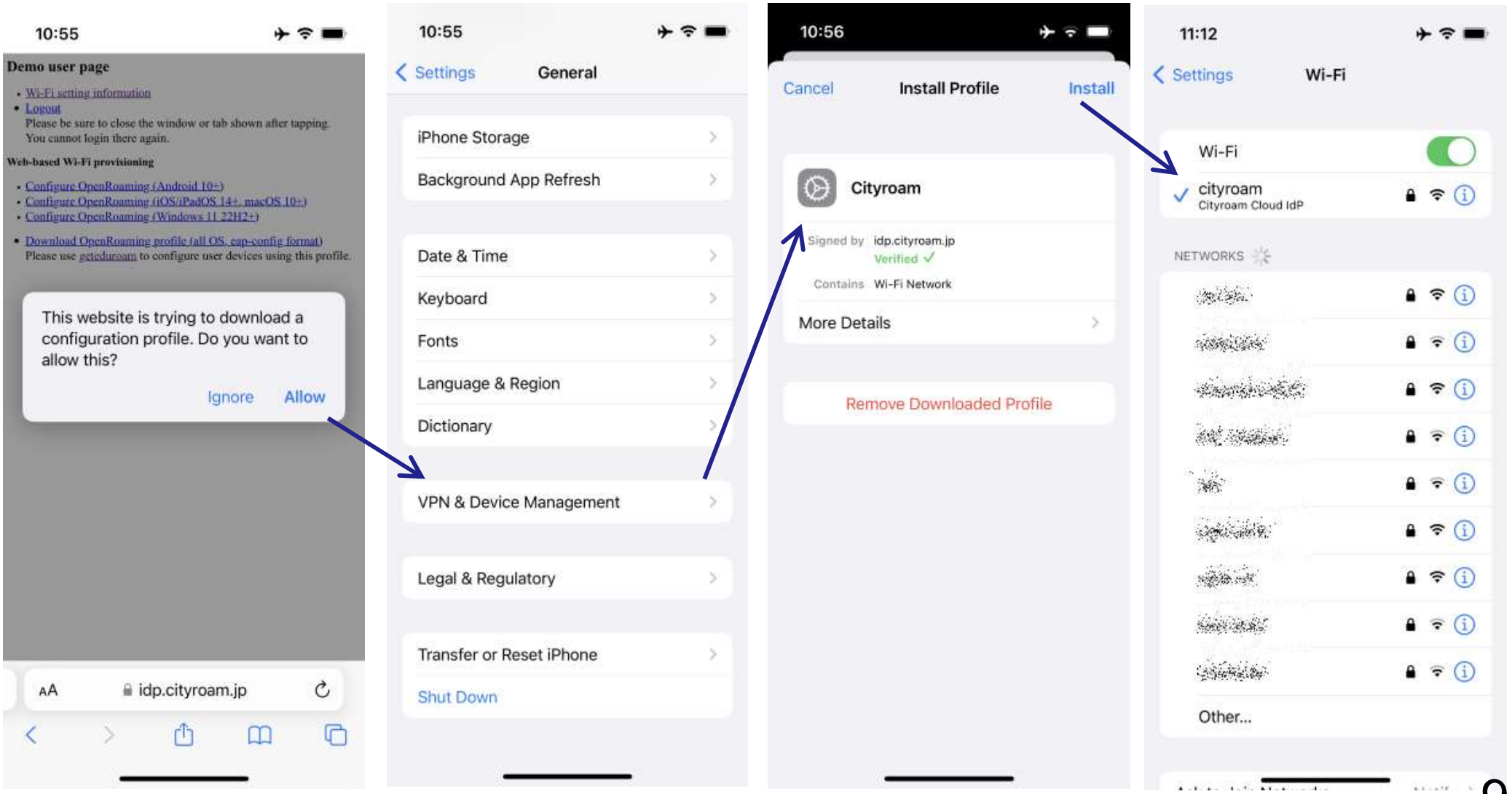
作りました！

- 機関の情報システムのウェブサイトに組み込める、
  CGI Perlスクリプト集. (GitHubにて公開)
- ウェブ界隈の先進的な認証システムを利用して、Wi-Fiプロファイルを発行できる. (パスワードレス認証, FIDO2, Passkey, …)
- eduroam / OpenRoamingのパスワードレス設定を実現.
- geteduroamでも、ID・パスワードの入力が不要になる.
- 期限付きプロファイルが発行可能 (対応OSのみ)

今時の学生は自宅にネット環境がある.
学校の情報システムにログインできる環境がある.

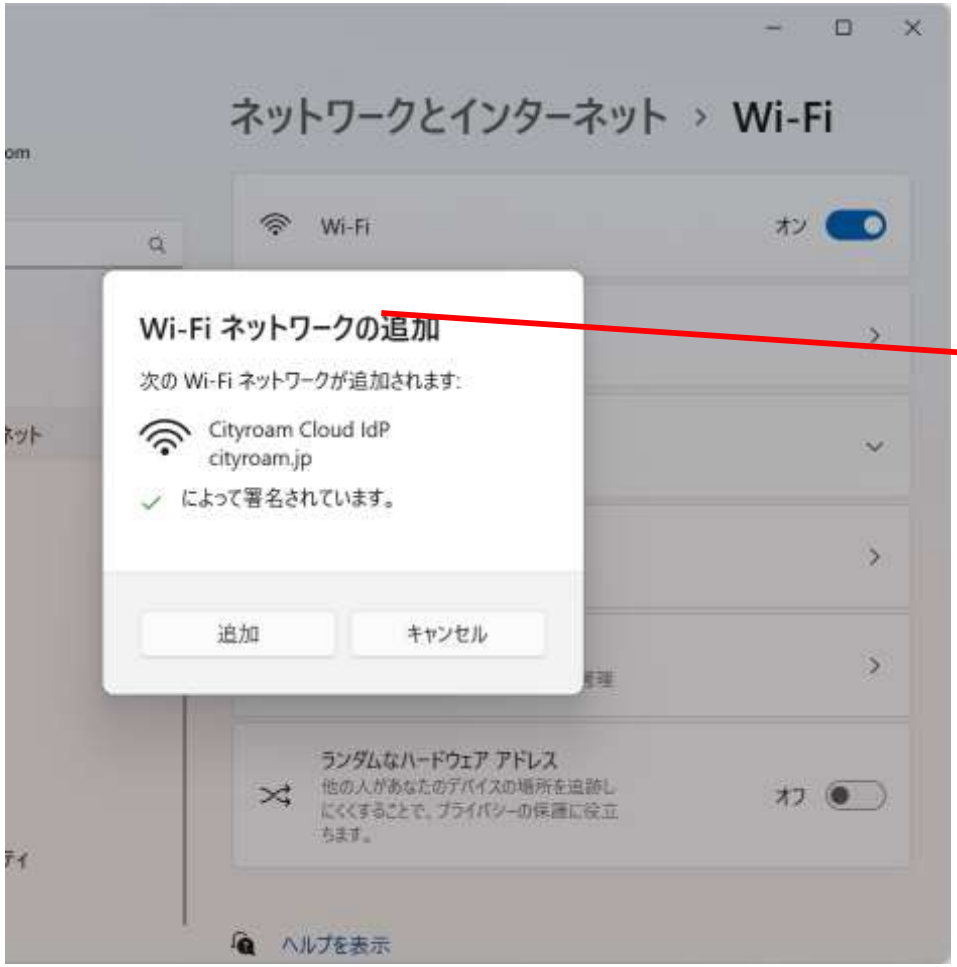
iOS/iPadOS/macOS

- .mobileconfig形式を利用したMDM



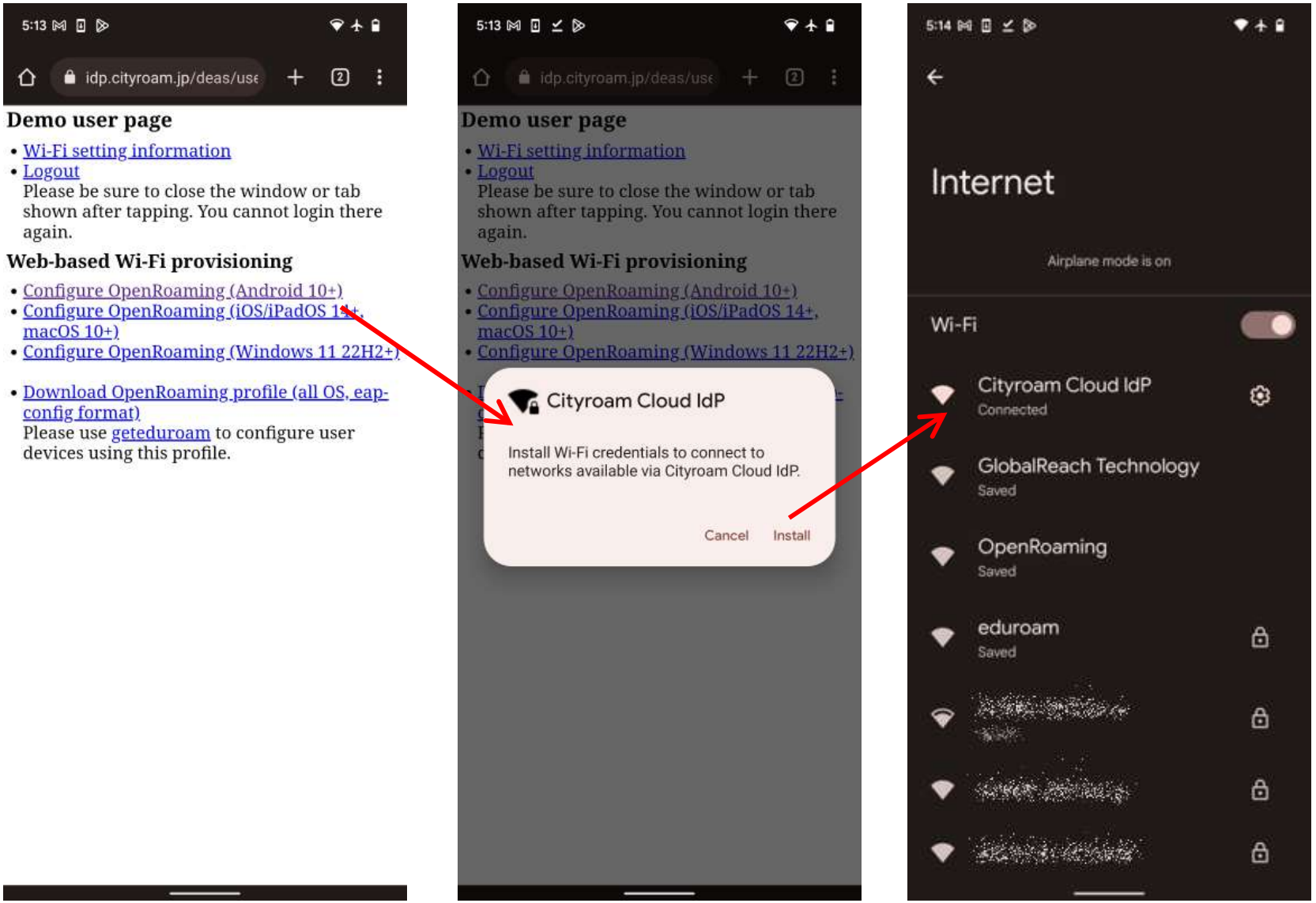
Windows 10, Windows 11

- ms-settings: URI schemeによるWi-Fi設定
- EAP-TTLS のみ対応
- Windows 10, Windows 11 (21H2)では、EV証明書による署名が必要



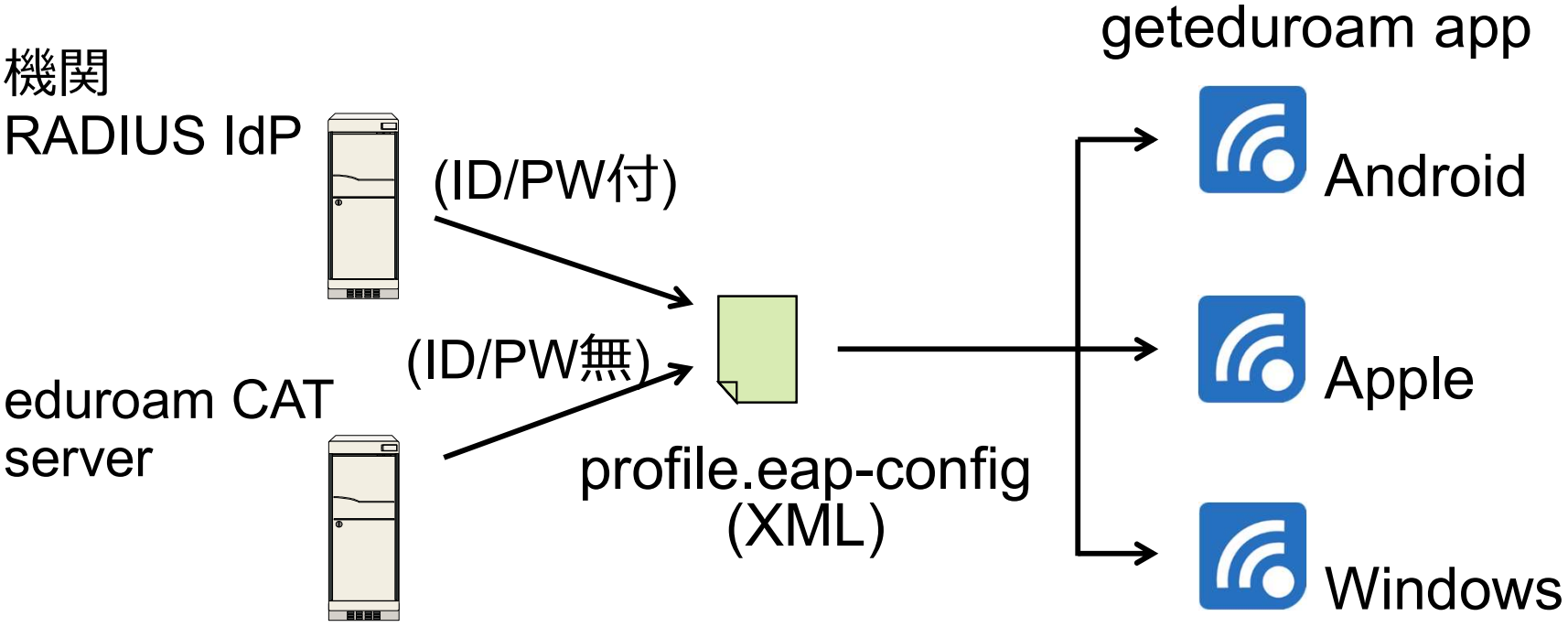
Android

- PPS MO形式を利用したWi-Fi設定
- eduroamでは利用できない．(レガシーな802.1Xに非対応)



.eap-config形式によるWi-Fi設定

- eduroam CAT (Configuration Assistant Tool) や geteduroam appで利用できる、OS非依存なプロファイル形式.
(現在、eduroam CAT アプリから geteduroam へ移行が促されている)



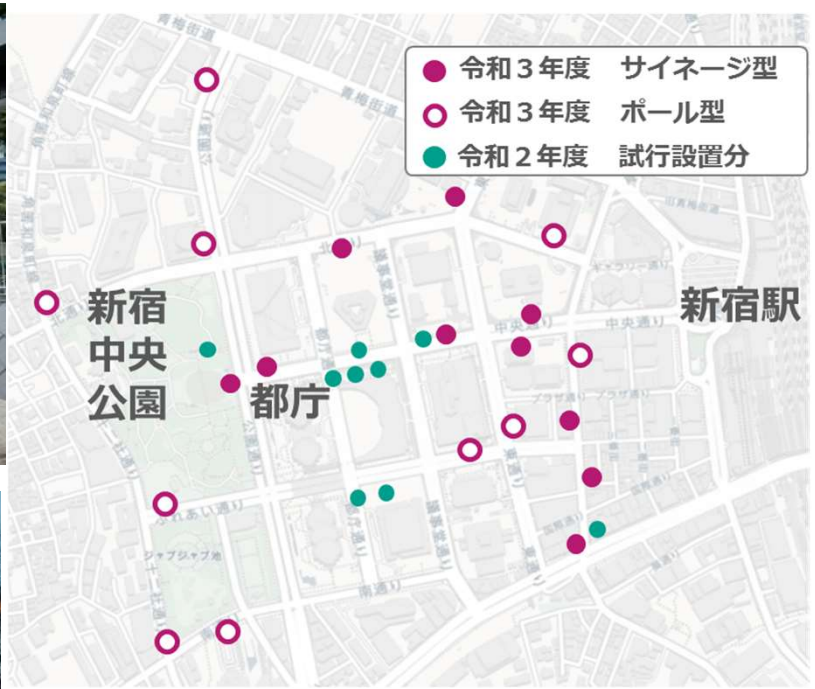
まとめ

- 現在のeduroamでは、ID・パスワードなどの手入力の煩わしさがあり、トラブルが少なくない.
- 次世代ホットスポット Passpoint / OpenRoaming の普及に伴い、主要OSで web-based Wi-Fi provisioning の機能が使えるようになった.
- これ↑を使うと、eduroamでもID・パスワードレス設定が実現.
- 機関の情報システムに組み込める、プロファイル発行スクリプトを開発した.

- OS側の対応に未熟なところがあり、Wireless Broadband Alliance (WBA)を通じてベンダにフィードバックしている. Passpoint / OpenRoamingの技術開発にも貢献.

東京都・西新宿5G搭載スマートポール

- 西新宿エリアにおけるスマートポールの面的設置，運用及び検証事業
  https://www.digitalservice.metro.tokyo.lg.jp/tokyodatahighway/smart_pole.html
- Smart City実現に向けて，スマートポールにeduroam, Cityroam (WBA OpenRoaming含む) を追加.
  - 令和2年度分2基、令和3年度分20基 稼働、令和4年度 増強中



eduroam accesses: 75.4%