大学ICT推進協議会 2023年度 年次大会
名古屋国際会議場
2023年12月14日 発表

eduroam / OpenRoamingにおける現地情報通知

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5年度NII公募型共同研究の助成を受けました.

キャプティブポータルの問題

- Captive Portal (Splash Page, Landing Page)
  フリーWi-FiやホテルWi-Fiで、無線LANがつながったと思ったら「ぴょこん」と出てきて通信を邪魔してくるアイツ.
  - 利用規約を表示
  - ログインを要求する (アクセス制御)
  - 利用者の同意が得られるまで通信をブロック
  - ポータルサイトに誘導 (広告, 現地情報の提供, …)

重要!

- まともに動かないところが結構ある
  - ログイン画面 / 許諾画面が出なくて、無線LANが使えない.
  - httpアクセスで回避できることがあるが、セキュリティ的にダメ
  - 無限ポータル地獄 (動作不良)
  - そもそも暗号化されていない「オープンWi-Fi」の時点で、ダメ

eduroam と OpenRoaming

- eduroam (2003～) : 教育・研究向けの国際無線LANローミング基盤
  eduroam JP (2006～) : 国内のeduroam基盤 (現在409機関が参加)
- OpenRoaming (2020～) : 市民一般向けのセキュア無線LANローミング

よいところ

- WPA2/WPA3 Enterpriseによる強固なセキュリティ
- 自動的につながる

わるいところ

- 勝手につながってしまう (?)
- 利用規約や注意事項を提示できない (学校などから不満)
- ポータルサイトに誘導できない (フリーWi-Fiのオーナーに不評)

現地情報を提示する
仕組みが欲しい → 開発！

現地情報の提供方法

- キャプティブポータルを併用
  - 現行の仕組みは、大抵、アクセス制御が込み.
  - 通信がブロックされるので、利便性を大きく損なう.

- Passpoint Rel.3 の Venue URL 属性を使う
  - 対応している端末と基地局が少ない.
  - 利用者への通知機能が、まだ多くのOSに入っていない.
  - Passpointでしか利用できない.

- Captive Portal API (RFC 8908) ← 後発だけあって、筋がよい.
  - 一部のOSしか対応していない.
  - 利用者への通知機能が不十分.

キャプティブポータル (CP) の変遷

- 初期の実装
  - http (80/tcp)のアクセスをひったくり、ローカルのウェブページに飛ばす.
  - https の普及により、基本的には利用できなくなった.

- OSやブラウザの独自実装
  - 端末が、DHCPでアドレス取得後に、ベンダごとの独自ウェブページにhttpでアクセスして、Captive Portal Detectionを行う.
    特定の文字列が返されたら、CP無しと判断する.
    CP有りなら、ポータルのアドレスを取得して、ミニブラウザでアクセスする.
  - ローカルのDNSサーバでアクセス先をひったくるように実装.
  - DNS over HTTPS (DoH)などの普及により、今後動かなくなる恐れ.

- 現在進行形 – Captive Portal Architecture (RFC 8952)
  - DHCPの option 114 や RA を使って、ポータルのアドレス(https)を配布.

現地情報ハンドラ
Venue Info Handler

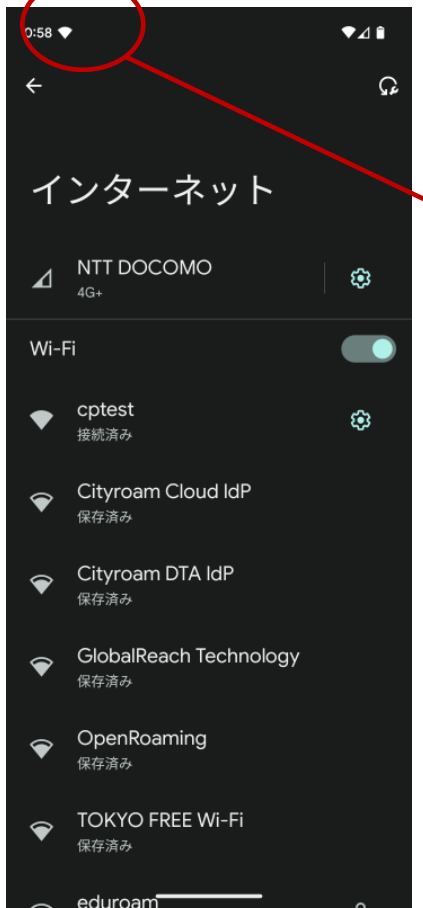
作りました！ 

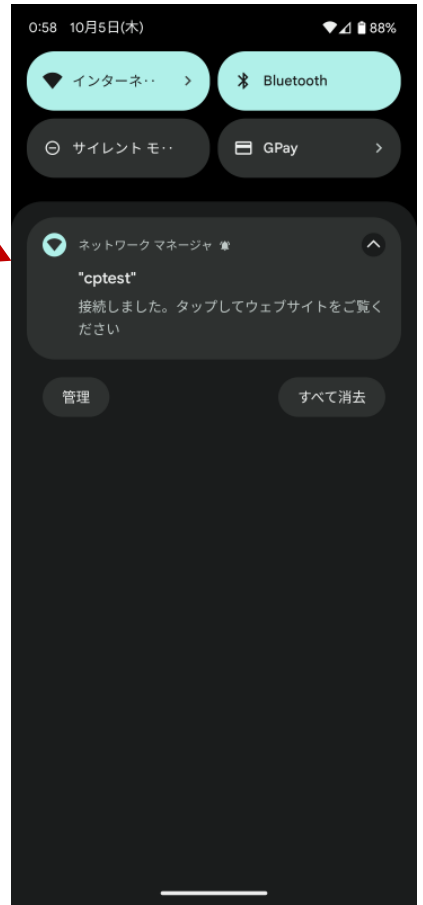
- WPA2/WPA3 Enterprise、PSK、オープン、なんでもOK.
  現地情報の「通知」を実現するプログラム群.　(GitHubにて公開)
- 設計方針:　自動接続の利点を殺さないよう、
  - 通信を極力ブロックしない
  - ポータルサイトへの誘導による「情報通知」を最優先として、
    画面のブロックも極力避ける
- 最近の主要なOSに対応
- 基地局システムに容易に組み込めるように、Captive Portal周りの技術情報を取りまとめた.

https://github.com/hgot07/VenueInfoHandler

Android 11+

- Capport API (RFC 8908)対応
- 通知機能がよく考えられている.
- 無線LANに接続されると、通知音が鳴り、通知欄にポータルサイトへのリンクが表示される.





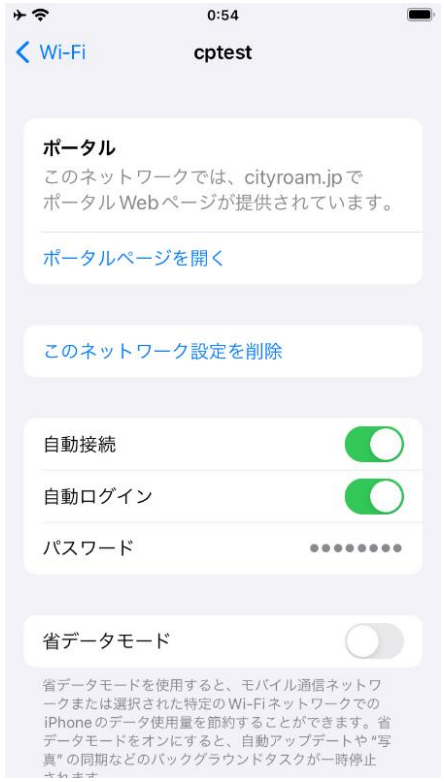
CP有効化も容易

ChromeOS, Android 10

- Capport API (RFC 8908) 非対応
- Google独自の仕組みを使って、キャプティブポータルが発動するように実装.
- ChromeOSの通知は、気付かれにくい.
- Android 10では、ミニブラウザの全画面表示. 通信はブロックされない.

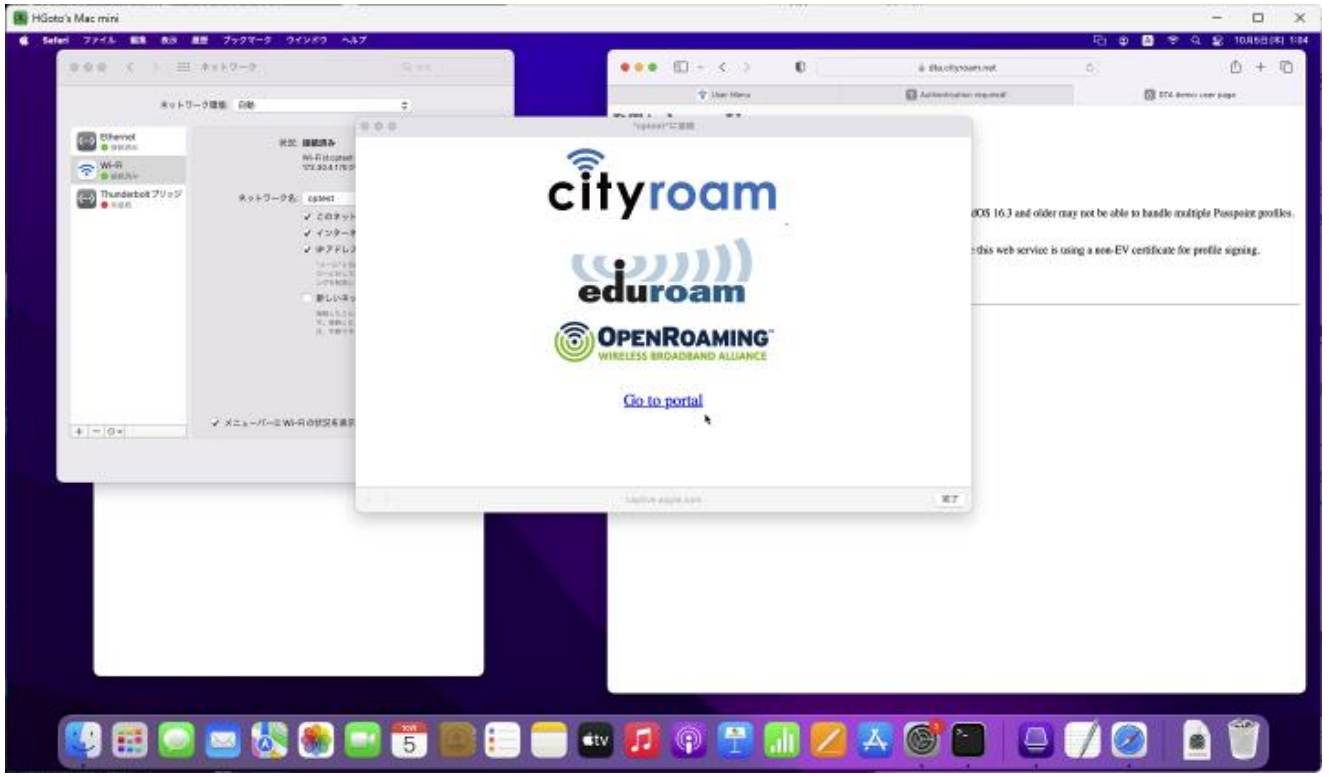
iOS/iPadOS

- iOS/iPadOS 14以前はCapport APIに非対応.
- 15, 16では、Capport APIで captive=false の設定だと、通知が一切出ない.
- 17では、Wi-Fi設定の中にひっそりと通知が出るのみ. 動作しないことが頻発.
- Apple独自の仕組みを使って、Captive Network Assistant (CNA)が必ず動くように実装して、ワークアラウンド. 通信ブロックを自動解除する実装とした.



macOS

- macOS 13 (Ventura)以降で、Capport APIに対応.
  ただし、通知機能がない.
- Apple独自の仕組みを使って、Captive Network Assistant (CNA)が必ず動くように実装して、ワークアラウンド. 通信ブロックを自動解除する実装とした.
- 無線LAN接続のたびに900px幅の大きなCNA画面が表示されるのが鬱陶しい.



Windows 10/11

- Capport APIに非対応.
- Microsoft独自の仕組みを使って、キャプティブポータル機能が必ず動くように実装して、ワークアラウンド.
- サンドボックスもなしにいきなり「規定のブラウザ」でポータルにアクセスする仕組みなので、セキュリティ上の懸念がある.
  (Windowsの仕様であって、開発したツールの問題ではない)
- 通信はブロックされないが、NCSI (Network Connectivity Status Indicator)の機能が組み合わさっているので、接続アイコンの表示が少しおかしくなる.

まとめ

- WPA2/WPA3 Enterpriseの無線LANでは、利用者をポータル画面に誘導する手段がない問題があった.
- アクセス制御が前提だった従来のキャプティブポータルに代わり、現地情報の通知が重要なことを説いた.
- 現地情報通知を実現するためのプログラム群を開発した.(最近の主要なOSに対応)
- eduroamやOpenRoamingでも、利用者に通知を出したり、ポータルサイトに誘導したりできるようになった.

- OS側の対応に未熟なところがあり、Wireless Broadband Alliance (WBA)を通じてベンダに改善を呼びかけている.