eduroam/OpenRoaming における現地情報通知

後藤英昭 [1)]，　原田寛之 [2)]，　漆谷重雄 [3)]

1) 東北大学 サイバーサイエンスセンター
2) 札幌学院大学 情報処理課
3) 国立情報学研究所

Venue Information Notification on eduroam/OpenRoaming

Hideaki Goto[1)], Hiroyuki Harada[2)], Shigeo Urushidani[3)]

1) Cyberscience Center, Tohoku University
2) Information Processing Division, Sapporo Gakuin University
3) National Institute of Informatics

概要

教育・研究機関向けの無線 LAN ローミング基盤である eduroam や，市民一般向けの OpenRoaming では，WPA2/WPA3 Enterprise による利用者認証と無線接続が行われる．この方式では，高いセキュリティと自動接続によって利便性の高い無線 LAN 利用環境が実現されるが，現地に固有の利用規約や注意事項，現地案内などの情報を利用者に提示する手段が十分に整備されていない．eduroam の参加機関や，OpenRoaming を導入する店舗・施設などから，このような情報提示を行いたいという要望が出ることがある．一方，公衆無線 LAN で現在主流のウェブ認証方式は，キャプティブポータルの仕組みを利用した情報提示が可能であるが，セキュリティ上の問題が多く，Enterprise 型のような自動接続が難しい．近年の OpenRoaming の普及に伴い，現地情報の提示が重要視されるようになり，そのための仕様が幾つか現れている．本研究では，現地情報の提供方法と，主要なオペレーティングシステム (OS) によるサポート状況を調査した．また，新しい仕様に対応できていない OS もサポートできるように，キャプティブポータル技術の併用・応用の技術を含めて，情報提示の仕組みとソフトウェアを開発した．Enterprise 型でも，利用者が容易にポータルサイトを見つけ，有益な情報を得ることができ，サービスの利便性向上が期待される．

1　はじめに

教育・研究機関向けの無線 LAN ローミング基盤である eduroam [1] や，市民一般向けの OpenRoaming [2] では，WPA2/WPA3 Enterprise [3] による利用者認証と無線接続が行われる．この方式では，高いセキュリティと自動接続によって利便性の高い無線 LAN 利用環境が実現されるが，現地に固有の利用規約や注意事項，現地案内などの情報を利用者に提示する手段が十分に整備されていない．eduroam の参加機関や，OpenRoaming を導入する店舗・施設などから，このような情報提示を行いたいという要望が出ることがある．一方，公衆無線 LAN で現在主流のウェブ認証方式では，キャプティブポータル (Captive Portal) の仕組みを利用した情報提示が可能であるが，セキュリティ上の問題が多く，Enterprise 型のような自動接続が難しい．

一般にキャプティブポータルは，利用者の通信を遮断し，利用者のログイン後に開放するという利用形態である．このため，自動接続を至上とする無線 LAN システムとは相反するものであり，eduroam や OpenRoaming でキャプティブポータルを併用することは強く非推奨とされている．近年，OpenRoaming の普及に伴い，現地情報の提示が重要視されるようになった．無線 LAN の接続時に，利用者の操作がなくても通信が遮断されないような，情報提示のための仕様が幾つか現れている．

本研究では，現地情報の提供方法と，主要なオペレーティングシステム (OS) によるサポート状況を調査した．また，新しい仕様に対応できていない OS もサポートできるように，キャプティブポータル技術の併用・応用の技術を含めて，情報提示の仕組みとソフトウェアを開発した．これを用いると，WPA2/WPA3 Enterprise のネットワークにおいても，利用者が容易

にポータルサイトを見つけ，有益な情報を得ることを支援できる．サービスの提供者の視点では，利用規約を提示したり，ポータルサイトや車内・機内 Wi-Fi サービスのメニューなどに利用者を誘導できるようになる．これにより，様々な無線 LAN サービスの利便性向上が期待される．

本稿では，初めに，現行のキャプティブポータルの動向と，新しい情報提示の仕組みを説明する．本研究で目標とするシステム要件を明らかにする．続いて，最近の各種 OS における現地情報 (Venue Info) 提示のサポート状況，および，キャプティブポータルの仕組みを利用した代替手段について解説する．最後に，各機関において極力小さなシステム変更で導入できることを目指して開発した，情報提示のためのソフトウェアを紹介する．

2　キャプティブポータルと現地情報提示

公衆無線 LAN で広く使われているキャプティブポータルは，基本的には利用者認証ないし利用規約提示・同意取得，および，アクセス制御を目的としたシステムである．このため，利用者が認証情報を入力するか，利用規約に同意するための操作を行うまでは，ポータルサイト以外への通信は遮断される．

キャプティブポータルの初期の実装では，ルータで ARP (Address Resolution Protocol) テーブルの値を書き換えたり，ポート 80/TCP をリダイレクトすることによって，利用者が任意のウェブサイトにアクセスしようとする通信経路を捻じ曲げて，ポータルサイトに誘導していた．この手法は広く使われているものの，HTTPS (Hypertext Transfer Protocol Secure) の利用が一般的になった現在では，利用者が明示的にウェブブラウザに HTTP のアドレスを入力するまで機能しないという，実用性に乏しいものである．原理的には中間者攻撃 (Man-In-The-Middle (MITM) Attack) と変わらず，HTTPS に適用すると不正な証明書のエラーが表示されるという，セキュリティ上の問題もある．

利便性とセキュリティの向上のために，現在は主要な OS に独自のキャプティブポータル検出 (Captive Portal Detection, CPD) の仕組みが組み込まれており，ネットワークの接続時に自動的に 80/TCP の通信が開始される．基本的な原理としては，OS が特定のウェブページにアクセスして，規定の応答があればキャプティブポータルなしと判断する．もし特定アドレスの通信先が変更されていて，規定と異なる応答があれば，キャプティブポータルありと判断して，接続先のシステムから提示されるページを利用者に提示する．ただし，OS ベンダごとの独自手法に依るため，各種 OS に対応したシステムを構築するのは容易ではない．オープンソースの実装としては，CoovaChilli [4] や openNDS [5] などがある．

キャプティブポータルの仕組みの標準化が推進されて，現在は RFC 8908, 8910 としてまとめられている [6, 7]．OS 側の基本的な動作は，以下のようになる．端末が無線 LAN に接続され，DHCP (Dynamic Host Configuration Protocol) によって IP アドレスを取得する際に，DHCP option 114 (DHCPv4) または Router Advertisement option 37 (DHCPv6) によって Captive Portal API のアドレスを受け取る．OS はこの API とやり取りをして，ポータルサイトのアドレスなどを受け取り，必要に応じて利用者に通知したりポップアップ画面を出す．また，必要に応じて，ポータルサイト側で利用者認証や利用許諾の手続きを進める．API では venue-info-url というパラメータが定義されており，これらの処理を省略しても，任意のウェブサイトのアドレスを利用者に通知することができる．現地情報の通知だけが目的で，OS がそのような機能を提供しているなら，僅か数個の固定パラメータを JSON (JavaScript Object Notation) 形式で返すスクリプトと，DHCP サーバへのオプション追加のみで実装できる．

OpenRoaming では，WPA2/WPA3 Enterprise に加えて，Passpoint [8] による基地局自動選択の仕組みが使われている．Passpoint Release 3 で Venue URL と呼ばれる属性値が追加された．この属性値を使うことで，現地情報 (Venue Info) などを含むウェブサイトのアドレスを利用者に通知できる．しかしながら，執筆時点において，この属性値は有効に利用されていないようである．また，Passpoint を使わない eduroam などの無線 LAN では，利用できない．

本研究で開発するシステムでは，現地情報の提示が主目的である．Captive Portal API が利用できない環境では，古いキャプティブポータルの仕組みを使うこともやむを得えないと考えられる．目標とするシステム要件を以下に示す．

- 情報提示を主目的として，利用者の操作をできるだけ排除できること．
- やむを得ず利用者の操作が必要となる場合でも，僅かの操作に留められること．

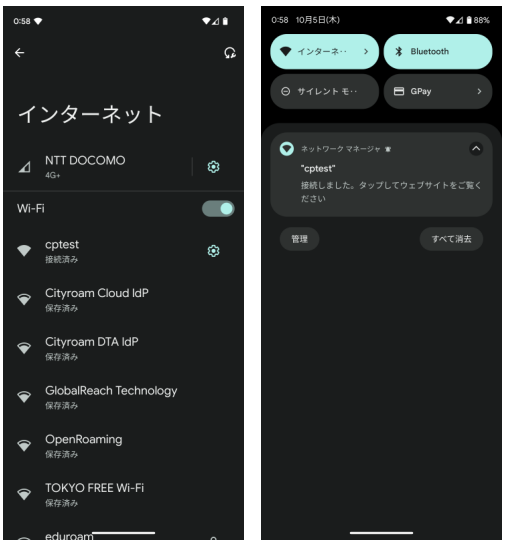

図 1　Android の Venue Info 通知（左上に扇型のアイコン）.

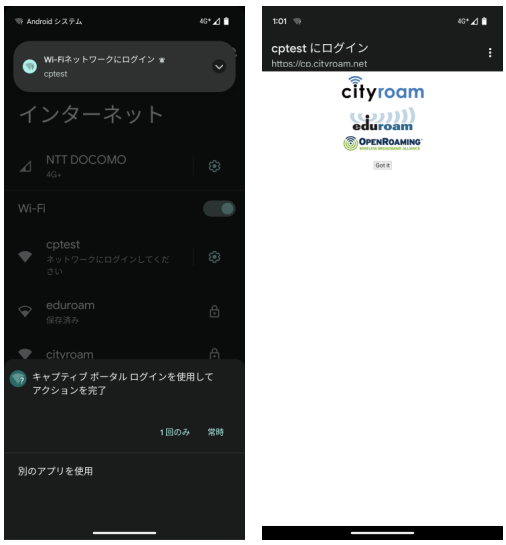

図 2　Android のキャプティブポータルの例.

- ネットワーク接続の際に利用者に気付かれやすい通知を出しつつ，あまり邪魔にならないようにできること.
- 新しい Captive Portal API の利用を優先すること.
- モバイル端末で用いられる多様な OS に対応できること．特に，学校・大学で利用されることの多い Android, iOS/iPadOS, macOS, Windows, ChromeOS に対応することが望ましい.
- 極力，実装が容易であり，既存システムに組み入れやすいこと.

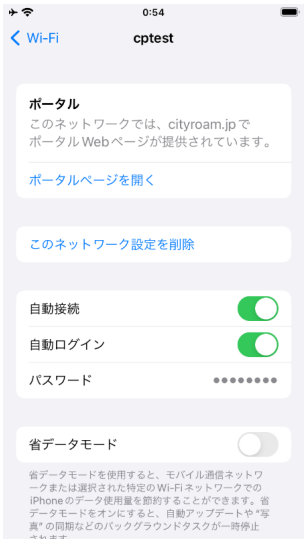

図 3　iOS のポータルページ通知.

3　各種 OS のキャプティブポータル/現地情報通知の対応状況

3.1　Android

Android 11 以降で，Captive Portal API に対応している．API で ”captive”: false とした JSON データを端末に返すことで，ポータルサイトへのリンクを端末に通知できる．Android 10 以前では，Google の独自仕様によるキャプティブポータルしか利用できない.

Android 11 以降では，無線 LAN に接続されると通知音が鳴り，ステータスバーに通知アイコンが追加される（図 1）．この通知は venue-info-url と関連付けられており，利用者は随時この通知をタップするだけでポータルサイトに移動できる.

この実装は，大きなポップアップ画面で操作を邪魔するようなことがなく，ほぼ確実に利用者にポータルサイトを知らせることができるという点で，現時点で最も用途に合致していると考えられる.

Android 11 以降では，Captive Portal API に準拠したログイン画面を表示することもできる．実装例を図 2 に示す．ログイン画面に置かれたリンクをタップすることで，ウェブブラウザがポータルサイトを表示するようにできる.

3.2　iOS/iPadOS

実機で調査した限り，iOS/iPadOS 15 以降が Capport API に対応しており，実際に API へのアクセスが確認された.

API で ”captive”: false を返した場合，15 と 16 では利用者への通知が一切ない．iOS/iPadOS 17 では，Wi-Fi 設定の SSID をタップしたところに「ポータル

図 4　iOS のキャプティブポータル.

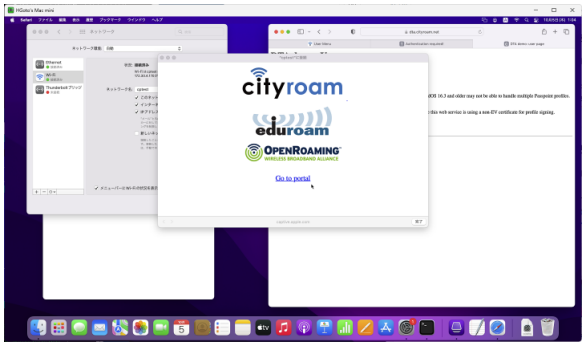

図 5　macOS のキャプティブポータル.

ページを開く」という表示が追加された（図 3）．しかしながら，通知アイコンも通知音もないため，利用者がこれに気付くのは難しいと考えられる．

API で ”captive”: true を返した場合，ネットワーク接続時に端末に全画面のポップアップが表示される（図 4）．利用者には邪魔になるかもしれないが，ほぼ確実に利用者に見て欲しい情報がある場合には，このような通知方法を採用するしかなさそうである．僅かのタップ数でキャプティブポータル画面を抜けられるような実装が望ましい．

なお，iOS/iPadOS はキャプティブポータルを抜けた後でも，定期的に API をポーリングして，ネットワーク接続状況を確認する．API は端末の接続中に ”captive”: false を返し続けるように実装する必要がある．

3.3　macOS

macOS 13 (Ventura) 以降が Capport API に対応しており，実際に API へのアクセスが観測された．

しかしながら，API で ”captive”: false を返した場合は利用者への通知がない．API で ”captive”: true を返した場合，画面中央に Captive Network Assistant（CNA）の大きな画面が表示される（図 5）．iOS/iPadOS と同様に，利用者に見て欲しい情報がある場合には，このポップアップ画面に頼るしかなさそうである．

macOS 12 (Monterey) では，Capport API へのアクセスがなかった．Apple 独自のキャプティブポータル機能を実装することで，上記と同様の CNA 画面を表示させることは可能である．

Apple からは，2020 年に Captive Portal API の紹介記事 [9] が出ている．今後，情報通知のみのユーザインタフェースが洗練されることを願っている．

3.4　Windows

Windows 10, 11 はいずれも Captive Portal API に非対応である．

Microsoft 独自のキャプティブポータルの実装では，ネットワーク接続の際にまず http://www.msftconnecttest.com/connecttest.txt を読み込む（Windows 10 Version 1511 以前では動作が異なる）．規定の文字列 “Microsoft Connect Test” が返ってきた場合はキャプティブポータルなしと判断する．基地局まわりのネットワークでこの接続を乗っ取り，別の文字列を返す．OS はキャプティブポータルありと判断して，別のファイルからポータルサイトのアドレスを読み取り，ウェブブラウザでそのサイトを自動的に開く．

この実装では，端末が新しいネットワークに接続されるたびにウェブブラウザのタブが増えていくという鬱陶しさがある．しかしながら，確実に情報提示できる上に，利用者が随時参照できるという点では好ましい．

Windows は，ネットワークの利用中に，上記の確認用ページを 20〜30 秒間隔程度でポーリングする．これは NCSI (Network Connectivity Status Indicator) の機能であり，もし規定の文字列が得られなかった場合はネットワーク切断状態と判断して，画面上のアイコンが地球儀の表示になる．ネットワークが利用可能な状態であっても，このような表示は利用者に不安を与えるため，Windows 向けの実装では正常接続の表示を出すような工夫が必要になる．

3.5　ChromeOS

ChromeOS は，学校向けの Chromebook 端末として採用例が多いことから，十分な利便性の確保が必要である．しかしながら，Android と同じ Google 発でありながら，現行のバージョン 117 でも Captive Portal API には対応していない．

ChromeOS では，Google 独自のキャプティブポータル機能が利用できる．ネットワーク接続の際に，端末はまず http://www.gstatic.com/generate_204 にアクセスする．ステータスコード 204 No Content

図 6　ChromeOS のポータルサイト通知.

が返ってきた場合は，キャプティブポータルなしと判断する．HTTP のコンテンツが返された場合は，それをウェブブラウザ開くための通知が表示される（図 6）.

4　Venue Info Handler による通知機能の実装

現地情報を通知する機能は，基地局を提供する事業者ごとに実装する必要がある．大学や中小事業者，あるいは個人でも容易に実装できるように，現地情報の提示を主目的とする API プログラム群を開発して，Venue Info Handler という名前でパッケージ化した．このプログラム群は，オープンソースソフトウェアとして GitHub で公開予定である.

openNDS [5] などの既存のキャプティブポータル実装と異なり，Venue Info Handler にはアクセス制御関係のコードが含まれていない．このため，ファイアウォールとの組み合わせを考える必要がなく，HTTP サーバと DHCP サーバ，および，DNS サーバの設定変更のみで実装が可能である．唯一，データベース機能として Redis [11] を用いているが，他のデータベースシステムと比べて，Redis サーバの設定と起動は容易である.

Venue Info Handler では，まず RFC 8908/8910 を利用する情報提示のための API を実装した．具体的には，venue-info-url を含む JSON データを返すだけの，簡便な CGI (Common Gateway Interface) プログラムが主体である．端末に API の所在を知らせるために，DHCP option 114 や RA option 37 を追加するが，これは多くの DHCP サーバで容易に設定できる.

前章で説明したように，最近の主要な OS であっても，Captive Portal API (RFC 8908) のみでは十分な情報提示が難しい．Apple 製の OS（iOS/iPadOS, macOS）では，RFC 8908 に準拠したバージョンであっても，利用者のポータルサイトへの誘導が難しい．このため，Apple 独自のキャプティブポータル機能を追加した.

Windows と ChromeOS は，いずれも現行バージョンが RFC 8908 に非対応のため，Microsoft と Google のベンダ独自仕様のキャプティブポータル機能も追加した.

多くのキャプティブポータル実装では，特定の HTTP アクセスを横取りする仕組みが必要である．端末に対して正規と異なる A/AAAA レコードを返すために，手元の実装では Dnsmasq [12] を用いている．Venue Info Handler は DNS サーバの種類に依存しないため，同様のアドレス書き換えが実現できるならば，他の DNS サーバを組み合わせることもできる.

RFC 8908 による venue-info-url の通知を除き，他の手法では，API が個々の端末を識別し，状態を把握しながら応答を返す必要がある．現状の OS の仕様では，OS 内部のキャプティブポータル機能が HTTP サーバにリクエストを送る際に，端末の識別・追跡に利用できるようなユニークな属性値を送出しない．API 側は，IP アドレスを頼りに端末を識別する以外にない．従って，Venue Info Handler の CGI プログラムは，NAT (Network Address Translation) を越えると正常に動作しない．Venue Info Handler は，基地局と同じネットワークセグメントに設置する必要がある．この制約は実装の手間につながるが，現行の OS の仕様では致し方ない.

評価用の無線 LAN システムを研究室内に構築して，Venue Info Handler を追加した．各種 OS を用いて，OS ごとの挙動を分析しながら，動作確認を行った．図 1〜6 は，構築したシステムを利用して実際の画面をキャプチャしたものである.

5　むすび

eduroam や OpenRoaming などの WPA2/WPA3 Enterprise の無線 LAN では，接続が自動化されているため，現地に固有の利用規約や現地案内などの情報を利用者に提示する仕組みが十分に整備されていなかった．ポータルサイトへの誘導のために，キャプティブポータルを併用した場合，利便性の大幅な低下を招く問題があった．本研究では，なるべく利用者に負担を強いないように，ポータルサイトへのアクセス手段を提供する仕組みを検討した.

現地情報の提供方法と，主要 OS によるサポート状況を調査した．また，新しい仕様に対応できていない

OS もサポートできるような，情報提示の仕組みとソフトウェアを開発した．これにより，Enterprise 型でも利用者が容易にポータルサイトを見つけ，有益な情報を得ることができるようになり，無線 LAN サービスの利便性向上が期待される．

現時点では，OS ベンダの独自実装によるキャプティブポータルの仕組みに頼らざるを得ないことが多い．今後，Captive Portal API (RFC 8908/8910) の普及に伴って実装の煩わしさは減っていくものと考えられるが，現地情報の提示という観点では必ずしも使いやすいユーザインタフェースにはなっていないことから，OS ベンダや無線 LAN 業界に対して改良を働きかけていく予定である．

なお，キャプティブポータルの画面を強制表示する仕組みは，Enterprise 型の自動接続という利点を少なからず犠牲にする．eduroam や OpenRoaming への採用は慎重に行うべきである．

本研究の一部は，令和 5 年度国立情報学研究所公募型共同研究の助成を受けた．

参考文献

[1] eduroam JP: https://www.eduroam.jp/
(2023 年 10 月 5 日参照)

[2] WBA OpenRoaming:
https://wballiance.com/openroaming/
(2023 年 10 月 5 日参照)

[3] Wi-Fi Alliance, “Discover Wi-Fi, Security.”
https://www.wi-fi.org/ja/
discover-wi-fi/security/
(2023 年 10 月 5 日参照)

[4] CoovaChilli: https://coova.github.io/
(2023 年 10 月 5 日参照)

[5] openNDS:
https://github.com/openNDS/openNDS/
(2023 年 10 月 5 日参照)

[6] T. Pauly and D. Thakore, “Captive Portal API.” https://datatracker.ietf.org/doc/html/rfc8910
(2023 年 10 月 5 日参照)

[7] W. Kumari and E. Kline,
“Captive-Portal Identification in DHCP and Router Advertisements (RAs).”: https://datatracker.ietf.org/doc/html/rfc8910
(2023 年 10 月 5 日参照)

[8] Wi-Fi Alliance, “Passpoint – Wi-Fi ホットスポットネットワークへのシームレスでセキュアな接続を実現.” https://www.wi-fi.org/ja/discover-wi-fi/passpoint/
(2023 年 10 月 5 日参照)

[9] Apple, “How to modernize your captive network.” https://developer.apple.com/news/?id=q78sq5rv
(2023 年 10 月 5 日参照)

[10] Venue Info Handler: https://github.com/hgot07/VenueInfoHandler/
(2023 年 10 月 5 日参照)

[11] Redis: https://redis.io/
(2023 年 10 月 5 日参照)

[12] Dnsmasq: https://thekelleys.org.uk/dnsmasq/doc.html
(2023 年 10 月 5 日参照)