沖縄県域公衆無線 LAN-AP 認証方式の検証
Proposal of Okinawa prefecture public wireless LAN-AP authentication method

苑田 征弥 [*1]，谷口 祐治 [*2]
Seiya Sonoda[*1], Yuji Taniguchi[*2]
[*1] 琉球大学情報工学科
[*1]Department of Information Engineering and Science,University of the Ryukyus
[*2]琉球大学 総合情報処理センター
[*2]Computing and Networking Center,University of the Ryukyus
Email: e135750@ie.u-ryukyu.ac.jp, taniguchi@cc.u-ryukyu.ac.jp

あらまし：沖縄県域における公衆無線 LAN，特に「Be.Okinawa Free Wi-Fi」に着目し， 暗号化通信の有無，フィルタリングの有無を解析，考察し，問題点を示す。問題点の対策に基づいたアクセスポイントを試作し，信頼性の高い認証方式を提案する。
キーワード：公衆無線 LAN，暗号化通信，アクセスポイント構築

1. はじめに

公衆無線 LAN とは，無線 LAN を使用して，インターネットへの接続を提供するサービスのことであり, 主に空港や観光地, 主要都市に設置されている。

その設置目的の多くは観光客向けの提供で，現在も設置施設の増加が進んでいる。一方，公衆無線 LAN のセキュリティにおいて数多くの危険性が指摘されており [(1)]，単に無認証のアクセスポイントを設置すると，なりすましや，盗聴による情報漏えいのリスクが高まる。

本研究では, 沖縄県における公衆無線 LAN から，2017 年現在，沖縄県が推奨する無料 Wi-Fi サービス事業である「Be.Okinawa Free Wi-Fi」[(2)](以下，「BoF-Wi-Fi」と呼ぶ。)に焦点をあて, 公衆無線 LAN の問題点の調査と対策及び，対策に基づいたアクセスポイントを試作し，信頼性の高い認証方法を提案する。

2. 「BoF-Wi-Fi」の解析

公衆無線 LAN である「BoF-Wi-Fi」に対し，実際に公衆無線 LAN が設置されている施設へ訪れ，認証方式，暗号化形式，ポートの開放状況を Nmap と Wi-Fi Explorer を用いて調査を行った。

(a) 解析環境の構築，およびポートスキャン

開いていると危険なサービス・ポートが開いた状態である外部に公開されている VM を作成し，「BoF-Wi-Fi」に接続した PC から外部に公開されている VM に Nmap によるポートスキャンを行った。

(b) 那覇空港における電波干渉の調査

複数の公衆無線 LAN サービスが存在する施設として那覇空港を調査場所として選択し，Wi-Fi Explorer による電波干渉の調査を行った。

表 1: フィルタリングポート

PORT	STATE	SERVICE
25/tcp	filtered	smtp
1720/tcp	filtered	h323q931
2000/tcp	filtered	cisco-sccp

3. 解析結果

(a) Nmap によるポートスキャンの結果

「BoF-Wi-Fi」 の Nmap ポートスキャンを行った結果のフィルタリングポートは表 1 の通りである。

「BoF-Wi-Fi」 は，smtp，h323q931，cisco-sccp に対してルータ上でパケットフィルタリングを行っていた。一方で，外部 VM で起動しているサービスに対しては smtp 以外, フィルタリングは行われていなった。

smtp は，オープンリレーを防ぐため，h323q931，cisco-sccp は，VoIP を使用したインターネット通話アプリをフィルタリングするためであると考えられる。

(b) 那覇空港の現状調査の結果

那覇空港で Wi-FiExplorer による解析を行った結果を図 1 に示す。

那覇空港では，様々な公衆無線 LAN が設置されているため, 電波干渉が起こっている。「BoF-Wi-Fi」同士がチャンネルの競合を起こしていないか調査するため，「BoF-Wi-Fi」のみに絞った結果を図 2 に示す。「BoF-Wi-Fi」のみに絞った結果から,「BoF-Wi-Fi」のアクセスポイント間では，電波干渉が置きていないことを確認した。また，調査を進めると，「BoF-Wi-Fi」は，暗号化なしの通信を行っていることが判明した。

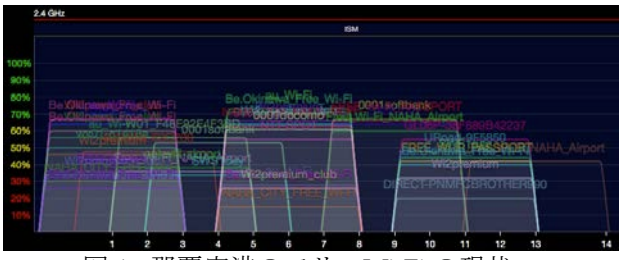

図 1: 那覇空港のフリーWi-Fi の現状

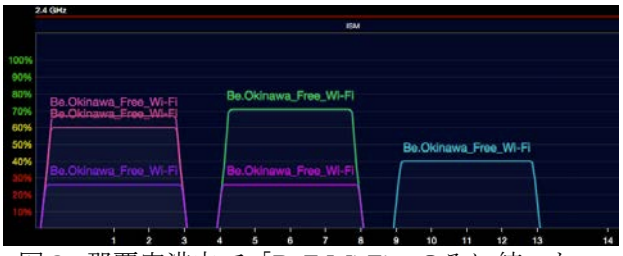

図 2: 那覇空港内で「BoF-Wi-Fi」のみに絞った結果

3.1 解析結果の考察

開いていると危険とされているポートの内, smtp, h323q931, cisco-sccp へのフィルタリングは適切である。一方，その他サービスのフィルタリングは行われていなかった。「BoF-Wi-Fi」のアクセスポイント間のチャンネル設定も適切であり，電波同士の競合が起こらない設定になっていた。しかし，暗号化通信を行っていないため，盗聴，なりすましの危険性がある。

4. アクセスポイント(AP)の試作

前節で得られた結果から，信頼性の高い認証方式を用いたアクセスポイントを試作する。

作成した AP の特徴は以下の通りである。

(a) 信頼性の高い認証方式を用いる
- 二段階認証を採用

(b) 暗号化通信を行う
- WPA2-エンタープライズ(EAP)
- 複合はほぼ不可能

(c) パスワードに有効期限を設定する

(d) サーバにユーザ情報を格納する
- 再接続の際に再利用可能

4.1 作成した AP と「BoF-Wi-Fi」の比較と考察

「BoF-Wi-Fi」 と作成したアクセスポイント(AP)を比較した結果を表 2 に示す。

表 2: 2 つの AP を比較した結果

無線 AP	暗号化通信	再認証	接続時間
Be.Okinwa Free Wi-Fi	×	×(有)	○
作成した AP	○	○(無)	△

「BoF-Wi-Fi」は、通信の暗号化を行っておらず，ユーザの情報も記録していないため再接続する際に再認証が必要になる。しかし，SNS 認証を利用しているので接続までの時間は早い。

一方，作成したアクセスポイントは，通信の暗号化を行っており，再接続の際に，サーバに格納された情報を参照するので再認証の必要がない。しかし，「BoF-Wi-Fi」に比べメール確認などの工程が多いため，接続まで時間はかかる。

5. まとめ

本研究では，沖縄県内における公衆無線 LAN の一つである「BoF-Wi-Fi」に対して調査, 解析を行い，現状の「BoF-Wi-Fi」の問題点を指摘した。

そして，問題点を受け，信頼性の高い認証方式を用いた暗号化された通信を行う無線 LAN アクセスポイントを試作し,「BoF-Wi-Fi」との比較を行った。

信頼性の高い認証方式を用いてる点，通信の暗号化を行っている点，再認証が不要な点から，本研究で作成した AP は有意である。

今後の課題として，沖縄県内のその他公衆無線 LAN の解析を行うこと, 試作したアクセスポイントは，事前にユーザ情報をサーバに登録しなければならないため，サーバに登録を行うためだけのフリー Wi-Fi アクセスポイントを構築すること，ルータ上で，不要なサービスはフィルタリングすることが挙げられる。

参考文献

(1) 清水渉，小林稔幸:“無線ホットスポットサービスのセキュリティ", 情報処理学会研究報告マルチメディア通信と分散処理(DPS), 2002(32(2001-DPS-107)), 1-6, 2002-03-28

(2) 文化観光スポーツ部観光振興課:“沖縄県が推奨する無料 Wi-Fi サービス事業の実施事業者の募集について”, http://www.pref.okinawa.jp/site/bunka-sports/kankoshinko/ukeire/28wifi_bosyu.html, 最終閲覧日：2017 年 2 月 5 日