その無線アクセスポイント安全ですか？ ～不正な無線 AP の分類とフィールド調査～

原田 敏明 †　　森 達哉 †　　後藤滋樹 †

† 早稲田大学 基幹理工学研究科
169-8555　東京都新宿区大久保 3-4-1
{t.harada,mori}@nsl.cs.waseda.ac.jp
goto@goto.info.waseda.ac.jp

あらまし　スマートフォンなどのモバイル端末による無線通信が普及し，それを利用した脅威も日々増加している．とくに近年は，既存の公衆無線 LAN サービスになりすまして，接続する利用者を攻撃する不正な無線アクセスポイントの運用が増加している．多くの場合，利用者は不正なアクセスポイントだと気付かずに利用してしまい，個人情報を盗まれたり，悪性攻撃を受けることがある．本論文では，不正 AP による攻撃手法を整理・分類し，それぞれの攻撃特有の挙動を基に検出する手法を提案する．また，フィールドで実地調査を行い，不正 AP の現状を分析した結果を報告する．

Is the Wireless Access Point Secure?: A Study on the Rogue Wireless AP in the Wild

Toshiaki Harada†　　Tatsuya Mori†　　Shigeki Goto†

†School of Fundamental Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, JAPAN
{t.harada,mori}@nsl.cs.waseda.ac.jp
goto@goto.info.waseda.ac.jp

Abstract　The spread of wireless communication increases the threat of wireless attacks. This paper deals with rogue wireless access points (APs) which attacks users by pretending to be an legitimate public WiFi service provider. It is reported that the number of rogue APs is increasing in recent years. When users mistakenly use rogue APs, they are damaged such as information leakage or malicious attacks. This paper analyzes various attack techniques of rogue APs and proposes a new method for rogue APs detection. It is based on the behavior of attacking rogue APs. We also conduct field researches for rogue APs and report the current status of real rogue APs.

1　はじめに

背景: モバイル端末が全世界に爆発的に普及し，モバイルトラフィックの増大が深刻化している．これにともない，無線 LAN サービスの需要が高まっている．国内では，キャリア系事業者だけでなく，施設が提供する公衆無線サービスも増え，スマートフォンユーザの過半数は公衆無線サービスを利用している調査結果も出ている [1]．その一方で，公衆無線 LAN に潜在する脅威を熟知し，対策を施しているユーザは少ない．特に国内では対策を施しているユーザは 2～3 割と著しく低い [2]．無線 LAN の脅威の中でもよく注目されるのは，オープンアクセスの無線 AP の利用による通信盗聴である．さらに，悪意のある汎用性の高いアクセスポイント (以下，無線 AP と記述する) を実装するのは比較的簡単であり，危険性が高い．本研究では悪意のある無線 AP を総称して**悪性** *AP* と呼ぶ．

悪性 AP は，正規サービスの無線 AP になりすます，通称 Evil Twin 攻撃 (以下，ETA と記述する)

で中間者攻撃を行い，ユーザの個人情報を盗聴したり，通信データの改竄を行いマルウェアを送り込むなどの目的で設置される．公衆無線サービスの無線 AP のほとんどはオープンアクセスで提供されている．ユーザが無線 AP が正規のサービスか見分けることのできる情報はネットワーク名 (以下，SSID と記述する) しかないため，ユーザは気づかずに悪性 AP に接続，情報が漏洩する可能性がある．また，近年のモバイル端末は，接続したことのある無線 AP に自動で接続する機能も実装されているため，ETA の攻撃を受けやすい．

国内では悪性 AP による事例はほとんど報じられていないが，2020 年に開催される東京オリンピックに向けて，訪日外国人のために公衆無線 AP を増設する予定もあり [3]，今後悪性 AP の運用は増加するとみられている．しかし，攻撃の挙動を示したとしても，それが確実に攻撃者であるとは言い切れない場合がある．実際に航空機内に無線 LAN サービスを提供しているプロバイダが，偽造した Google の証明書を利用し．YouTube などの動画配信サービスに対して帯域制限を適用していた事例も報告されている [4]．こうした事例は悪性とはいえないものの，正規のユーザがセキュリティレベルを落としたサービスの利用を強いられるため，不適切な運用である．本研究ではこのように悪性と断言できない無線 AP を**不正 AP** と総称する．

目的: 本研究の目的は，悪性 AP による攻撃を目的ごとに分類し，各々の悪性 AP クラスの特徴に基づいた悪性 AP 検出手法を確立することにある．ここで利用する特徴とは，無線 LAN 通信におけるアソシエーション確立後の HTTP 通信における挙動として，リダイレクトのパターンや SSL/TLS 通信の有無，正規の公開鍵証明書の有無である．

また，本研究では国内外の公衆無線 LAN サービスの実態調査を行い，悪性 AP は存在するのか，果たして検出された悪性 AP は，攻撃者により設置されたものだと断言できるのか，という Research Question を考察する．調査では，国内 500 以上の公衆無線 AP に加え，国外の空港などでも調査を行い，国内外の公衆無線サービスの比較も行う．

さらに本研究では．上述の悪性 AP 検出手法を実装したモバイルアプリを開発した．このようなアプリを普及させることにより，ユーザが安全に公衆無線 LAN サービスを利用できることが期待できる．

貢献: 本研究の貢献は以下のように要約される．

- **悪性な挙動を示す無線 AP の検出手法を提案した．**
- **提案手法を組み込んだアプリを開発した [1]．**
- **国内外の無線 AP の危険性を実地調査した．**

本論文の構成は以下の通りである．はじめに 2 章で関連研究を述べる．次に 3 章で悪性 AP による攻撃手法とその挙動について述べ，4 章で検出手法について述べる．5 章では実地調査の内容と結果を示し，6 章で今後の課題と悪性 AP への対策技術について述べた後，7 章にて本論文をまとめる．

2 関連研究

本章では，悪性 AP の検出に関するいくつかの研究を述べる．Jana らは文献 [5] で，無線 AP から発せられるビーコンやプローブ応答に記載された TSF タイマ値から計算されるクロックスキューを利用し，ETA を行う悪性 AP を検出できることを示した．端末ごとに独自のスキュー値を持つため，なりすましを検出することができる．Lanze らは文献 [6] で，ツールを使用したソフトウェアベースの無線 AP と，ハードウェアベースの AP の挙動の差異から，悪性 AP の検出が可能であることを示した．ソフトベースの AP の場合，ビーコン記載のタイムスタンプ値に外れ値が多く存在するなどの特徴から，ツールで AP を運用している危険な無線 AP を検出する．Nakhila らは文献 [7] で，SSL/TLS プロトコルの特徴を利用した検出手法を提案した．同じ SSID の異なる無線 AP に接続した際に通信が切断される場合には，正規の AP と ETA を行う悪性 AP が，それぞれ異なるゲートウェイを利用していると判断できるため，検出できると主張している．

3 攻撃の分類とその特徴

本章では，はじめに正規の公衆無線 LAN サービスの挙動を示す．つぎに悪性 AP による攻撃を整理し，正規 AP との差異を示す．

[1] https://play.google.com/store/apps/details?id=org.morilab.wifi.wifiguardian&hl=en で公開中．

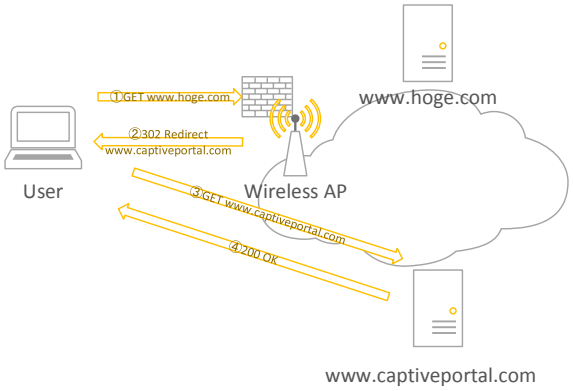

図 1: プロキシ型のキャプティブポータル

表 1: HTTP ステータスコード

Code	Detail
200	正常に処理され，レスポンスを受信
301	リソースの場所が恒久的に変更 または HTTPS での通信を強要
302	リソースが一時的にいつもと異なる場所

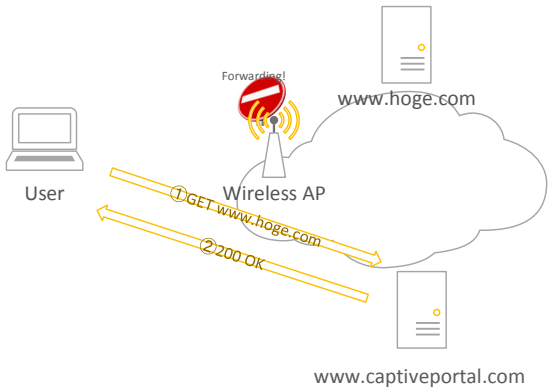

図 2: フォワーディング型のキャプティブポータル

3.1 公衆無線 AP の正規の挙動

公衆無線 LAN サービスは，オープンアクセスで誰でも接続可能であるがゆえに，キャプティブポータルという認証機能を使用している場合がほとんどである．本節では，認証がない場合とある場合それぞれの挙動について論じる．

3.1.1 認証あり公衆無線 AP

キャプティブポータルとは，ルータを経由してインターネットに接続を試みる端末が認証済みでない場合に，通信を強制的にブロックし，認証画面を端末のブラウザに表示させる仕組みである．キャリア系のサービスである場合，登録情報を利用して認証を行うことが多いが，空港などの施設が提供するサービスの場合は，ユーザのメールアドレスを入力するのみであるケースや，短時間であれば誰でも無料で接続できるケースがある．キャプティブポータルの実装には，プロキシ型の処理と，フォワーディング型の処理の 2 つがある．プロキシ型の処理を図 1 に，フォワーディング型の処理を図 2 に示す．

前者は，ユーザが HTTP リクエストを特定のサーバに送った際に，リダイレクトを指示する 302 のステータスコードが返ってくる．本論文で現れる HTTP のステータスコードの詳細を，表 1 に示す．302 のステータスコードは，一時的にいつもと異なる場所にリソースがある際に使用するもので，キャリアが提供するサービスのキャプティブポータルはこの挙動を示すことが多い．

後者は，HTTP のリクエストが無線 AP を通る際に，強制的にポータルサイトのサーバにパケットをフォワーディングする実装方法である．前者の場合と違って，クライアント側にリダイレクト先を明示したわけではないため，クライアント側のブラウザのアドレスバーには，ポータルサイトの URL ではなく，リクエストした URL が表示されている．フォワーディングの方法としては，iptables による経路制御や，DNS の名前解決応答などがある．HTTP リクエストに対して返されるステータスコードは 200 となるが，ほとんどの場合レスポンスと同時に送信される HTML 内に自動リダイレクトのコードが埋め込まれており，無線サービスのポータルサイトに自動転送される．

3.1.2 認証なし公衆無線 AP

オープンアクセスにもかかわらず，キャプティブポータルなどの認証を実装していない無線 AP を，本論文では「**認証なし AP**」と記述する．運用上非常に不適切ではあるが，利便性のためにこのような設定を施している管理者もいる．この場合 HTTP リクエストを送れば，リクエスト先のサーバから 200 のステータスコードとともに応答が返ってくる．しかし主要な web サービスにおいて，ユーザの個人情報を扱うページにリクエストを送った場合は，301 の

ステータスコードとともに HTTPS の URL が返ってくる．現在このような実装を施している web サービスは数多く存在するため，危険性は低いと考えられるが，認証のないの無線 AP の利用が危険なことには変わりない．

3.2 攻撃の分類と特徴

悪性 AP による攻撃を主に以下の 3 つに大別する．

- 通信盗聴
- 通信の改ざん
- サービス妨害攻撃

本節では，それぞれの攻撃を目的ごとに整理し，HTTP 通信時の挙動の特徴とともに論じる．

3.2.1 通信盗聴

クライアントとサーバの間に位置する無線 AP を最大限に利用できるのが，中間者攻撃による通信盗聴である．攻撃の際は無線 AP が送信者と受信者の両方になりすますが，物理的な距離などによる制約が通例と比べて少なく，成功の可能性は非常に高い．

中間者攻撃による通信盗聴は，平文通信盗聴と暗号通信盗聴の 2 つに分けられる．前者に関しては，無線ネットワークの性質上，中間者攻撃を行わずともパケットキャプチャツールで盗聴することが可能である．後者は，sslstrip と呼ばれる攻撃が有名であり，非常に致命的な攻撃である．攻撃の簡略図を図 3 に示す．この攻撃は，受信者になりすました AP とサーバは暗号通信を行うが，AP はその内容をクライアントに平文で送信する方式である．また，ユーザと AP 間を SSL で暗号化する sslsplit と呼ばれる攻撃も存在する．

sslstrip の攻撃の特徴として，特定のサーバに HTTP のリクエストを送った際に，通常の場合と挙動が異なるという点がある．個人情報などを扱うページに HTTP でリクエストを送信した場合，大半の web サービスは 301 のステータスコードとともに HTTPS の URI を返す．しかし，sslstrip を行っている AP 経由でこのリクエストを送信すると，HTTP の URI を返すという特徴がある．また攻撃の際，クライアントのブラウザのアドレスバーには HTTPS の表記はない．sslsplit の場合，認可されたサーバ証明書を用意しなければクライアント側に自己署名証明書の危険性を表すポップアップが表示される．現在の主

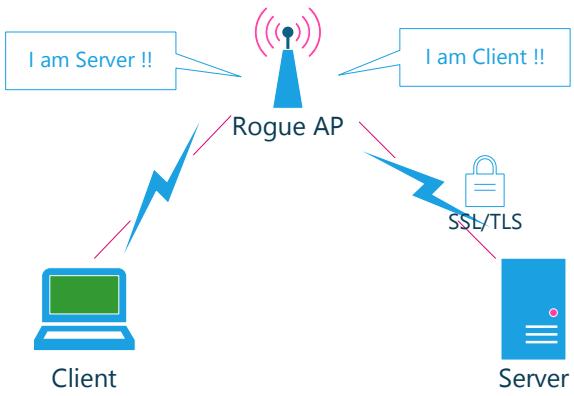

図 3: sslstrip の概要

要なブラウザは自己署名証明書の場合巨大な警告を出すため，ユーザが無線 AP の利用に懐疑的になる可能性が高い．

3.2.2 通信の改ざん

クライアントの通信を改ざんし，偽のポータルサイトに誘導する手口がある．DNS 偽装攻撃や，キャプティブポータルのようにリダイレクトを実装すれば誘導可能である．攻撃目的の 1 つとして，ユーザの個人情報の流出が挙げられる．大手の公衆サービスのポータルサイトのクローンを作成することは容易であり，ユーザが認証情報を入力し送信ボタンを押すと，攻撃者にその情報が送信される，という実装も比較的容易である．ログイン後にインターネット接続を提供すれば，ユーザは気づかずに利用する可能性が高い．

また，他の目的としてはマルウェア感染が挙げられる．正規のポータルサイトを装った偽サイトにマルウェアを仕込んだり，利用するためには特定の証明書のダウンロードが必要だ，という通知を表示させるという手法がある．マルウェアの挙動によって攻撃者の目的は異なるが，ページにマルウェアを仕込むことは容易であるため，サービス利用者に感染が拡大する可能性がある．

この攻撃目的の無線 AP の挙動は，DNS 偽装攻撃を実装している場合は，証明書の正当性の検証で検出可能である．しかし，正規の公衆無線 AP と同じくキャプティブポータルを実装している場合は，HTTP 通信の挙動からは特定することはできない．しかし，フィッシング用ポータルサイトの実装時に，サーバ証明書を用意しない，または自己署名証明書

を利用した暗号化を施している可能性があるため，攻撃の危険性評価の指標の 1 つになる．また，通信挙動のみに着目するならば，前節で論じたフォワーディング型のキャプティブポータルの挙動を示した際に，自動リダイレクトが実装されていない場合も，攻撃である可能性がある．

3.2.3 サービス妨害攻撃

DoS 攻撃がこの攻撃目的に用いられる．DoS 攻撃の対象として，以下の 3 つが挙げられる．

- 無線 AP
- インフラストラクチャ
- クライアント端末

無線 AP への DoS 攻撃は，例として probe request flood がある．probe request とは，クライアントから発せられる無線 AP の存在確認のためのフレームであるが，このフレームを大量に送りつけることで，無線 AP に負荷をかけるという意図である．

インフラストラクチャへの攻撃は，例として Beacon Flood がある．Beacon は無線 AP が発する自身の存在を知らせるフレームであるが，大量に異なる SSID の Beacon フレームをブロードキャストすることで，電波の混信や，正規のサービスの存在を隠すことができる．

クライアント端末への攻撃は，例として de-auth flood がある．de-auth パケットは本来，不正な AP に接続を試みているユーザに対して送ることで，ユーザを攻撃から守るためなどに利用される．しかしこれを悪用し，無線 AP を利用しているユーザを強制的に切断させることができる．

本研究で提案する手法では，サービス妨害攻撃は考慮していない．しかし，これらの攻撃はサービス妨害という目的だけでなく，自身の悪性な無線 AP に誘導する手段として使われる可能性もあるため，非常に危険である．

4 悪性 AP の検知

本章では，はじめに悪性 AP を想定されるリスクごとに分類する．つぎに悪性 AP の分類を利用した検出手法を提案し，それを利用したモバイルアプリの概要を示す．

4.1 検出手法

第 3 章で述べた攻撃とその特徴から，CUI で悪性 AP を検出する手法を提案する．検出のプロセスは，**HTTP レスポンス検証**と**証明書検証**の 2 つに分かれている．

最初に行う HTTP レスポンス検証では，まず無線 AP 経由で，特定の Web サービスのログインページに HTTP のリクエストを送信する．なお，このログインページは自動で HTTPS の URL にリダイレクトさせる設定とする．また，そのサーバは正当な証明書をインストールしている．レスポンスのステータスコードが，302 または 200 の場合，キャプティブポータルが存在すると言えるため，リダイレクト先の URL を取得し，証明書検証のプロセスを実行する．301 の場合は認証なし AP であるので，sslstrip が行われていないかを判断するために，リダイレクト先の URL を確認する．もし URL が HTTPS であったら証明書検証へ，そうでない場合は sslstrip を行う悪性な認証なし AP である．

証明書検証では，サーバ証明書が信頼された証明機関から発行されたものかどうか検証する．認証なし AP であった場合は，HTTP レスポンス検証でリクエストを送信した Web サーバの証明書を検証し，sslsplit 攻撃が行われているか判断を行う．キャプティブポータルが実装されている無線 AP の場合は，最終的なリダイレクト先のサーバのサーバ証明書の信頼性を検証する．この際，リダイレクトを多段階にしているサービスでは，途中のリダイレクト用のサーバの証明書の信頼性は考慮しない．また，受信した HTML に自動リダイレクトのメタデータが埋め込まれている場合は，そのリダイレクト先サーバの証明書を検証する．

以上の検出手法を用いて検証される無線 AP の危険性を表 2 に示したカテゴリーで評価する．sslstrip と sslsplit の挙動は，攻撃以外に実装する可能性が極めて低いため，非常に危険なカテゴリ A と判定する．ポータルサイトが存在するにもかかわらず，SSL に対応していないサーバの場合は，第三者にも情報流出の危険性があるため，攻撃でない場合も危険性は高いとしてカテゴリ B と判定する．また，ポータルサイトが SSL に対応してはいるが，信頼できないサーバ証明書を使用している場合は，攻撃でないとしても不適切な設定であると言えるため，カテゴリ C とする．カテゴリ E，F の問題発生とは，サーバからのレスポンスが不到達だった場合を指す．以上をふまえ，提案手法を図 4 に示す．

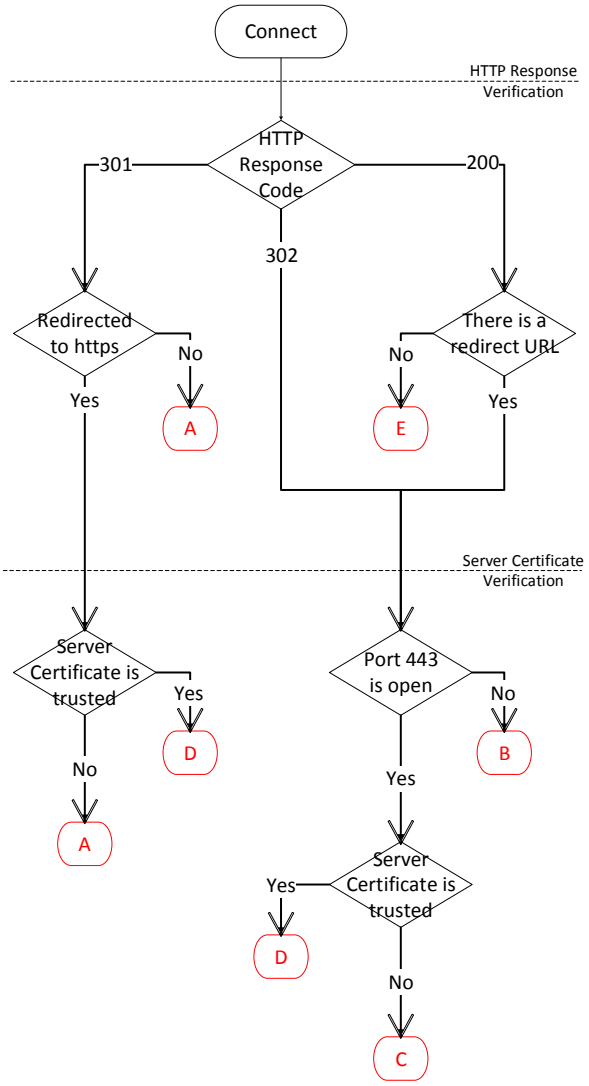

図 4: 検出手法

4.2 モバイルアプリの開発

前節で提案した検出手法を用いて，オープンな無線 AP の安全性を検証する Android OS 用アプリを開発した．このアプリは，ユーザの周りにあるオープンな無線 AP をスキャンし，安全性を検証する．実際にアプリを使用し，周辺の無線 AP の安全性を検証した結果の画面例を図 5 に示す．無線 AP の危険性の評価は，表 2 で提案したものを使用し，それを表情と色を用いて危険性を可視化している．この例では SSID を Pineapple として設置した不正 AP が正しく検知されていることがわかる．このアプリを用いることにより，公衆無線サービスを利用する

表 2: 無線 AP のリスク

Risk	Level	Detail
A	critical	攻撃を意図している可能性が非常に高く，また第三者にも情報が流出する可能性あり
B	high	攻撃とは断言できないが第三者に情報が流出する可能性が高い不適切な設定
C	medium	攻撃の可能性は低いがサービス運用上不適切な設定
D	low	攻撃を実装している可能性は低いと言えるが，オープンアクセスであるため注意が必要
E	error	手動での検証不能または証明書検証で問題発生
F	error	HTTP レスポンス検証で問題発生

ユーザは自己判断で安全な無線 AP を選択できるようになる．また，このアプリを用いてより広範囲な調査を実施することが出来ると期待される．

5 実態調査

本章では，国内外の主要都市において行った，オープンアクセスの無線 LAN の実態調査の結果を示す．

5.1 都内無線 LAN 調査

都内の複数箇所において，悪性 AP が存在するかの実態調査を行った．第 4 章で提案した手法とアプリを使用し，ラップトップ型 PC と Android 端末で検証を行った．調査の場所は，訪日外国人が多い街，オフィスが多い街などから総合的に判断し，羽田空港，新橋，浅草，池袋，渋谷の 5 地点とした．本実験では，端末の周辺にあるオープンアクセスの無線 AP を全てスキャンし，電波強度が低いものを除いてそれぞれ自動で検証を行う．検証の結果を表 3 に示す．ただし，リスクのカテゴリ E の括弧内の数字は検出数の内，自動検証不可と判定された AP の数を示している．

検証した無線 AP のうち，認証なし AP は 2 つのみであった．国内では，認証なし AP を利用いたサイバー犯罪が多い為 [8]，非常に良い傾向であると言える．ただし，認証があるとはいえ，オープンな

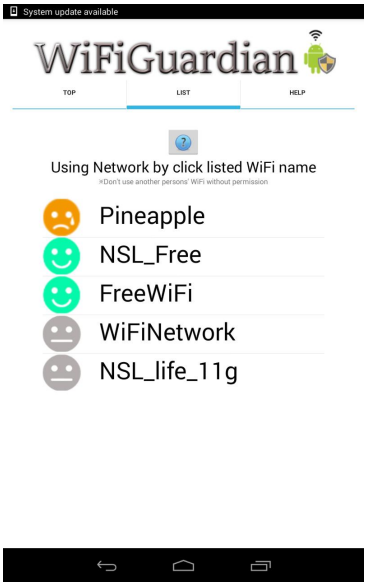

図 5: アプリの使用画面例

表 3: 実態調査結果

risk	羽田	新橋	浅草	池袋	渋谷
A	0	0	0	0	0
B	0	0	0	0	0
C	0	0	0	0	0
D	62	14	46	48	58
E	12	14	29(5)	23(1)	13
F	27	37	63	55	31
計	101	65	138	126	102

無線 AP が 500 以上観測されたことは良いことではない．オープンな無線 AP は，クライアント端末と無線 AP 間の通信を暗号化しないため，第三者による盗聴の危険性がある．多くの公衆無線サービスは，マルチ SSID と呼ばれる機能を使用し，暗号化されたネットワークも同時に提供しているが，利便性を求めてオープン認証の SSID を使用するユーザも存在する．したがって，暗号化された無線 AP の利用を普及させることが求められる．

5.2 国外無線 LAN 調査

航空機内や，アメリカ，カナダの施設の無線 LAN サービスの実態調査を行った．結果として，38 個のオープンな無線 AP が検出されたが，ほとんどが自己署名証明書の利用，または手動により検証不能と判断され，カテゴリ C または E に分類された．

手動により検証不能であった無線 AP は，リダイレクトをメタタグで実装するのではなく，javascript で実装していたためであったり，個々のサービスで実装が異なっていた．また，本調査で検出した無線 AP は全てフォワーディング型のキャプティブポータルを実装しており，またプロキシ型とフィルタリング型を組み合わせているものも多く見受けられた．地域によっては悪性 AP や，不正 AP が多いと言われているが，本調査は公衆無線サービスが比較的整備された，狭い範囲であったため，このような結果になったと思われる．

6 議論

本章では，調査結果から得られる今後の課題と，公衆無線 AP に施すべき不正 AP 対策技術について議論する．

6.1 今後の課題

実態調査により，国や地域ごとでキャプティブポータルの実装がかなり異なることが判明したため，そのような差異にも対応できるように検出手法のスクリプトを修正する必要がある．検証に GUI のブラウザを使用していないため，HTML や javascript などにリダイレクトが埋め込まれていても，確実にリダイレクト先にジャンプできるかは，現在の手法では保証できない．開発したアプリを様々な国や地域のユーザが使用するためには，非常に重要なことである．実装の違いによる検証エラーを減らし，且つモバイル端末で動作する範囲内での開発が今後の課題である．

6.2 必要な対策

第 5 章で述べた，国内の公衆無線サービスの現状に対する対策として，公衆無線 LAN に適用できる Passpoint[9] と呼ばれる技術の導入が挙げられる．

Hotspot2.0 規格のサービス名である Passpoint は，セキュアな無線ネットワークに，自動で認証と接続を行う技術であり，シームレスなサービスの提供を可能とする．Passpoint では従来サービスと異なり，Web ブラウザ等による認証を必要としない．端末の SIM カードによる認証や，電子証明書によるクライアント認証などが実装されている．実際にサンフランシスコの公衆無線 AP では，後者による Passpoint 技術の実装を行っている [10]．このサンフランシス

コのサービスでは，電子証明書などの接続に必要なプロファイルをインストールできるオープンな無線 AP を提供している．プロファイルをインストールすることで，周辺にある Passpoint 対応の無線 AP に自動で接続することができる．現在 Passpoint 対応端末は増加しており，Passpoint 機能を動作させている無線 AP が存在すれば，サービスの利用が可能である．

この技術により，携帯キャリアと契約しているユーザは，携帯キャリアが提供している公衆 AP に，SIM 認証で自動で接続することができるため，オープンアクセスの SSID を用意する必要がない．また，キャリアと契約していない訪日外国人は前述したような，電子証明書によるクライアント認証を利用すれば良い．そのためには，全国の無線インフラを整備する必要がある．

ただし，注意すべき点として，サンフランシスコの Passpoint サービスのように，プロファイルをインストールするための無線 AP をオープン認証で実装すると，ETA 攻撃によって偽のインストールページに誘導する攻撃を受ける可能性がある．今後の国内の無線サービスのセキュリティレベル向上のためには，Passpoint 導入は必須である．しかし導入の際には，このような脅威が存在することを考慮に入れなければならない．

7 まとめ

ユーザを攻撃する悪性な無線 AP の通信挙動の特徴を用いて，それらを検出する手法およびアプリを開発した．その検出手法を用いて，国内の公衆無線 AP の実態調査を行った結果，現状で国内では，悪性な無線 AP の運用は少ない．しかし，悪性ではないものの，第三者により通信を盗聴される危険性のあるオープンな無線 AP が大量に存在する現状を示した．自動でセキュアな無線 AP に接続と認証を行う技術である Passpoint を普及させることで，盗聴やなりすまし攻撃などの脅威を取り除くことができると期待している．

また，開発した不正 AP 検出アプリでは，使用するオープンな無線 AP の危険性を可視化することにより，ユーザが自己判断で安全なサービスを利用することが期待される．しかし，国内外での公衆無線 LAN サービスの実装方法の差異により，不正の検証が困難な場合があることが実地調査により確認された．アプリを様々な地域のユーザが使用できるよう，これらの例外的な実装に対応できるよう手法を改善していくことが今後の課題である．

参考文献

[1] ICT 総研, “2015 年 公衆無線 lan サービス利用者動向調査.” http://ictr.co.jp/report/20150416000081.html.

[2] 総務省情報セキュリティ対策室, “公衆無線 lan 利用に係る調査結果.” http://www.soumu.go.jp/main_content/000347651.pdf.

[3] 国土交通省観光庁, “公衆無線 lan の整備状況について.” http://www.mlit.go.jp/common/000987046.pdf.

[4] ZDNet, “Gogo in-flight wi-fi serving spoofed ssl certificates. .” http://goo.gl/p2wWu5.

[5] S. Jana and S. K. Kasera, “On fast and accurate detection of unauthorized wireless access points using clock skews,” in *Proc. Mobicom’08*, 2008.

[6] F. Lanze, A. Panchenco, I. Ponce-Alcaide, and T. Engle, “Detecting software-based 802.11 evil twin access points.,” in *Proc. IEEE CCNC 2015*, 2015.

[7] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou, “User-side wifi evil twin attack detection using ssl/tcp protocols.,” in *Proc. IEEE CCNC 2015*, 2015.

[8] 総務省情報セキュリティ対策室, “無線 lan ルータの不正利用に関する注意喚起.” http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000192.html.

[9] “Passpoint.” http://www.arubanetworks.co.jp/solutions/pdf/WP_Passpoint_Wi-Fi_r1.pdf.

[10] “Hotspot2.0 announcement.” http://www6.sfgov.org/index.aspx?page=255.