平成 28 年度 修士論文

中継トラフィックデータの類似性に着目した悪性WiFiアクセスポイントの検出

Malicious WiFi AP Detection
Using the Similarity of Relayed Communication Traffic Patterns

指導教員　森 達哉 准教授

早稲田大学基幹理工学研究科情報理工・情報通信専攻

学籍番号 5115F052-2

原田　敏明

平成 29 年 1 月 30 日

概要

モバイル端末の普及に伴い，公衆無線 LAN サービスの需要が高まっている．国内では，訪日外国人向けサービスの整備が進められており，無料の公衆無線アクセスポイントに容易に接続できるスマートフォンアプリも公開されている．その一方で，正規の公衆サービスになりすまし，サービス利用者を攻撃する悪意のある無線アクセスポイントの運用が増加している．悪性 AP の実装は非常に容易であり，またユーザを悪性 AP へ誘導する手法は多彩である．多くの場合，利用者は悪性 AP だと気付かずに利用してしまい，個人情報を盗まれるなどの被害を受けることがある．本論文では，正規サービスの無線 AP とサービス利用者の中継を行う悪性 AP を，中継される無線 LAN フレームから得られる情報を基に検出する手法を提案した．また，提案手法を用いて都内における悪性 AP の実態調査を行った結果，悪性 AP が存在する可能性は低いが，暗号化の施されていないオープンな無線 LAN サービスが大量に存在することが明らかになった．

目次

図目次

表目次

第 1 章　序論

モバイル端末の爆発的な普及に伴い，公衆無線 LAN サービスの需要が高まっている．国内では，公衆無線 LAN サービス利用者が年々増え続け，スマートフォンユーザの 57% が WiFi サービスを利用している [1]．また，2020 年に開催される東京オリンピックに向けて，訪日外国人向けの公衆無線 LAN サービスの整備が進められている [2]．取り組みの一つとして，訪日外国人向けの無料 WiFi 接続アプリが挙げられる．NTTBP が提供するアプリである「Japan Connected-free WiFi」 [3] は，一度の利用登録で手軽に周辺の無料 WiFi スポットを検索，接続することができる．空港や新幹線主要停車駅においても無料 WiFi スポットが設置され始め，国内の公衆無線 LAN 環境は整いつつある．その一方で，公衆無線 LAN に潜在する脅威を熟知し WiFi サービスを利用しているユーザは少ない．WiFi サービスを利用したことがある国内のユーザが 75% であることに対し，無線 LAN ネットワークが安全かどうか区別できるユーザが，わずか 9% であった [4].

無線 LAN の脅威としてしばしば注目されるのは，通信が暗号化されていないオープンアクセスの無線アクセスポイント（以下，無線 AP と記述する）の利用による通信盗聴である．オープンな無線 AP を経由した通信は，Wireshark [5] などのフリーソフトで容易に盗聴できる．公衆 WiFi サービスの無線 AP の中には，未だにオープンアクセスで提供されているものもあり，利用者は個人情報を抜き取られている可能性もある．無料 WiFi スポット接続アプリは，暗号化されていないオープンな WiFi サービスのみと連携しているため，安全に利用できるとは限らない．さらに近年は，比較的容易に実装できる，ファームウェアを改変した汎用性の高い無線 AP（以下，そのような無線 AP を悪性 AP と呼称）を使用した攻撃が注目されている．

悪性 AP は，正規の公衆サービスの無線 AP になりすまし，利用したユーザの個人情報を盗聴したり，通信データの改竄を行うなどの目的で設置される．悪性 AP はインターネットへの接続を提供するために，隣接する通常の AP の中継機として動作することが多い．悪性 AP によるなりすましは，非常に巧妙である．無線 LAN に対する攻撃ツール群である Aircrack-ng [6] は，ネットワーク名（以下，SSID と記述する）や端末の MAC アドレスまで，正規の無線 AP と同一の悪性 AP を立ち上げることが可能なツールである．このようななりすましによるユーザの誘導を，通称 Evil Twin 攻撃と呼ぶ．近年のモバイル端末は，同一 SSID の無線 AP が存在する場合，受信電波強度の強い無線 AP に接続を切り替えるため，この攻撃を受けやすい．このような攻撃を行わずとも，悪性 AP の SSID を“FreeWiFi”のように，ユーザを引きつけやす

いものにすれば，容易にユーザを悪性 AP に接続させることができる．

このような悪性 AP への対策技術として，Passpoint [7] がある．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を提供可能とする．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おり，Web ブラウザ等による認証を必要としない．実際にサンフランシスコの公衆無線サービスが Passpoint を導入している [8] が，国内では認知度が低く，導入しているサービスは少ない．

本研究の目的は，正規 WiFi サービスの無線 AP とサービス利用者の中継を行い，通信盗聴や通信の改竄を試みている悪性 AP を，中継されるトラフィックデータの類似性から検出することである．本研究では，無線 AP を経由して，外部ネットワークと TCP による通信を行うユーザのトラフィックデータを利用する．

TCP パケットに着目した理由として，TCP，IP ヘッダの情報は，コネクションごとに異なることが挙げられる．通常，異なるユーザが同一サーバとコネクションを確立したとしても，ヘッダの情報が同一であることは無い．しかし悪性 AP は，送信元 IP アドレスや，802.11 ヘッダの情報のみを書き換え，それ以外のヘッダの情報は書き換えずにフレームを中継することが多い．特殊な攻撃を行っている悪性 AP も，中継フレームには攻撃時特有の特徴が現れる．よって，中継フレームのヘッダ情報の類似性や，特徴ある通信に着目することで，データの中継を行う無線 AP を検出できることを示す．また，提案手法を使用し都内の悪性 AP の実態調査を行い，悪性 AP の現状と顕在化した公衆無線 LAN サービスの課題を示す．

本研究の主要な貢献は下記のとおりである．

- 悪性 AP が中継する無線 LAN 通信の類似性から悪性 AP を検出する手法を提案し，有効であることを示した．
- 実地調査により，悪性 AP の現状と公衆無線 LAN サービスの課題を示した．

本論文の構成は以下の通りである．はじめに 2 章では悪性 AP の攻撃手段と，攻撃モデルについて述べ，次に， 3 章で本研究の関連研究を紹介する．つづいて 4 章では提案手法を紹介し，5 章では評価実験の結果と考察を示す． 6 章では都内における実態調査の結果と考察を示す． 7 章では本研究の制約を述べ， 8 章にて本論文をまとめる．

第 2 章　攻撃モデル

本章では，はじめに悪性 AP のユーザ誘導手段と，攻撃の危険性を示す．次に，本研究における悪性 AP の攻撃モデルを示す．

2.1　ユーザの誘導

攻撃者は様々な方法でユーザを悪性 AP に接続させる．ユーザの誘導手段としては，以下の 3 つが非常に脅威である．本節では，それぞれのユーザ誘導手段について述べる．

- Evil Twin 攻撃
- WiFi Honeypot
- Probe Response Spoofing

2.1.1　Evil Twin 攻撃

Evil Twin 攻撃（以下，ETA と記述する）は，悪魔の双子攻撃とも呼ばれ，正規の公衆無線 LAN サービスの無線 AP と同じサービス名（以下，SSID と記述する）で運用することで，ユーザを悪性 AP に誘導させる攻撃である．攻撃の概略図を，図 2.1 に示す．

クライアント端末は，同一 SSID の無線 AP が存在する場合，受信電波強度の強い無線 AP に接続を行う．またクライアント端末は，ビーコンフレームによる無線 AP スキャンの際に，無線 AP の MAC アドレスを区別しない．そのため，端末に表示される無線 AP のスキャンリストから ETA を行う無線 AP を確認することは困難である．よって，攻撃者は通常より強い電波，正規のサービスと同じ SSID で悪性 AP を運用すれば，正規の無線 AP に接続を試みるユーザを全て悪性 AP に誘導できる．

2.1.2　WiFi Honeypot

WiFi Honeypot は，“Free”などの利用料が無料であることを示す単語や，運用している場所に関連した単語を SSID にいれることでユーザを誘導する手段である．無料で利用できる公衆 WiFi サービスが無い環境でこの攻撃を行うと，ユーザが接続する可能性は高い．

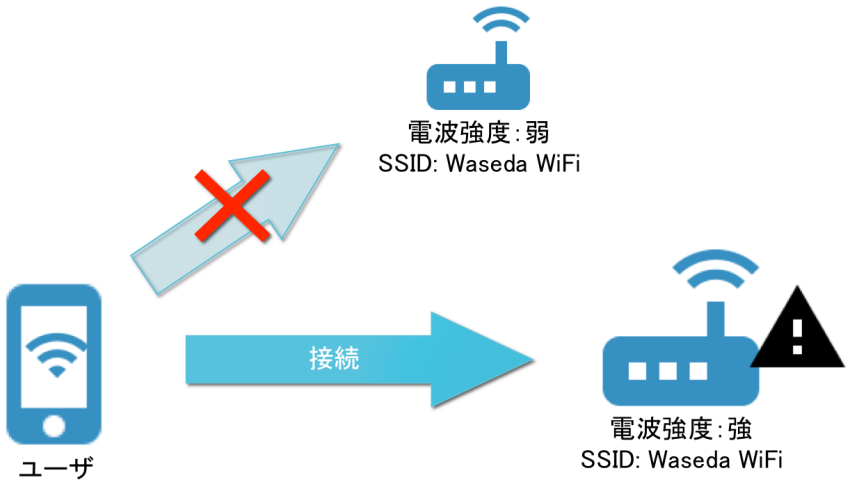

図 2.1　Evil Twin 攻撃の概要

実際に，チェコのセキュリティベンダーである AVAST Software [9] は，バルセロナ空港で複数のオープンな無線 AP を設置する実験を行った [10]．それらの SSID は，“Airport”や“Free”などの単語が含まれたものであった．結果として，わずか数時間で 2000 人以上のユーザが利用し，接続したユーザの 63.5% は，端末情報またはユーザ情報を確認できたとしている．

2.1.3　Probe Response Spoofing

プローブとは，クライアント端末が以前つないだことのある SSID が周りに存在しているか，能動的にスキャンする機能である．クライアントが発するプローブ要求に対して，無線 AP がプローブ応答を返すことで接続を行う．しかし，特定のプローブ要求に対して悪性 AP が偽のプローブ応答を返せば，悪性 AP がその SSID になりすますことができる．この攻撃を行った場合，クライアント端末の無線 AP スキャン結果には，出先であるのに自宅の無線 AP の SSID が表示されるなどの特徴が出る．また，端末の設定によっては，接続したことのある無線 AP に自動で接続する場合もあるため，ユーザは細心の注意を払う必要がある．

2.2　悪性 AP の攻撃分類

悪性 AP による攻撃を，主に以下の 3 つの目的に大別する．本節では，それぞれの攻撃目的の概要を述べる．

- 通信盗聴
- 通信の改竄
- サービス妨害攻撃

2.2.1 通信盗聴

悪性 AP による攻撃が危険である理由の一つに，ネットワーク内の位置関係が挙げられる．悪性 AP がインターネットアクセスを提供していれば，悪性 AP はクライアントとサーバの間に位置することになる．従来の中間者攻撃に比べて，物理的な制約などが極めて少ないため，容易に中間者攻撃によって通信を盗聴できることが，悪性 AP の脅威となっている．悪性 AP による通信盗聴は，WPA2 などで無線 LAN が暗号化されていない場合，平文通信盗聴と暗号通信盗聴に分けられる．

前者は，特別な攻撃ツールは必要無く，Wireshark などの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．また，無線 LAN が WPA2 などで暗号化されていない場合，悪性 AP を用いずとも，盗聴することが可能である．実際にオープンな無線 AP を経由した通信を，Wireshark にて盗聴した様子を，図 2.2 に示す．

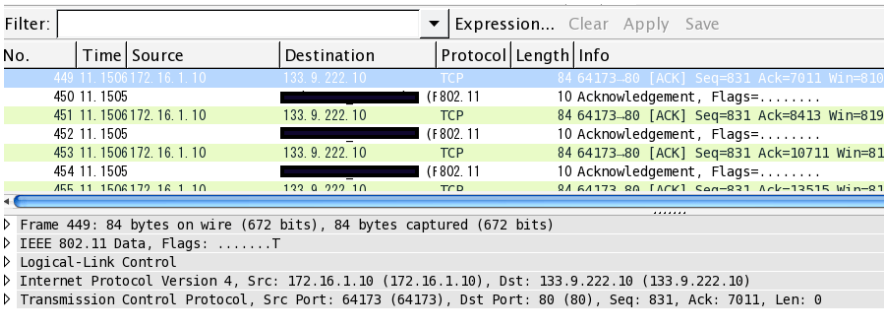

図 2.2　wireshark による平文盗聴

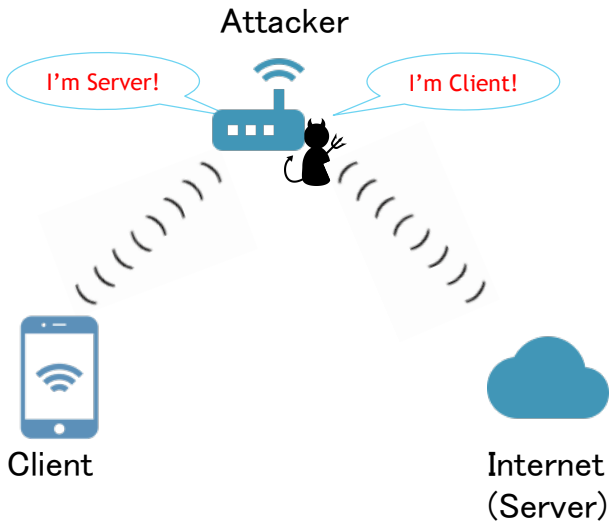

図 2.3　sslstrip の概要

後者は，sslstrip と呼ばれる攻撃が有名である．攻撃の簡略図を図 2.3 に示す．この攻撃は，悪性 AP がクライアントになりすまして，サーバと SSL による暗号通信を行う．さらに悪性 AP はサーバにもなりすまし，本物のクライアントに通信内容を平文で送信する．SSL により秘匿化されている情報も漏洩する可能性がある，非常に致命的な攻撃である．この攻撃は，HTTPS での通信を強制する HSTS 機能 [11] を使用することで，回避が可能である．HSTS は，初回通信の際に Web サーバから Web ブラウザに，次回以降の該当ドメインに対するアクセスを HTTPS にするように伝達する機能である．Google や Twitter などの主要なサイトは，ブラウザごとに事前に HSTS のリストに登録されている [12]．ただし，事前にドメインが登録されていない限り，初回の該当ドメインとの通信は HTTP での通信になるため，注意は必要である．

2.2.2　通信の改ざん

公衆無線 LAN サービスは，キャプティブポータルという認証機能を使用していることが多い．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．認証は，事前に登録した情報や，ユーザのメールアドレスを入力するケースなどがある．実際に，公衆無線 LAN サービスを提供している Wi2 [13] の無線 AP に接続した際のインターネットアクセス時の画面を図 2.4 に示す．この仕組みを利用し，攻撃者はユーザを偽のポータルサイトに誘導することができる．

誘導の目的の一つとして，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れば，ユーザに認証情報を入力させることは容易である．また，マルウェア感染も目的として挙げられる．インターネット利用に必要なアプリという名

図 2.4　wi2 サービスのキャプティブポータルサイト

目でダウンロードを誘導すれば，サービス利用者に次々と感染を拡大させることが可能であると言える．実際に，2005 年に公共の場に悪性 AP が設置されていた事案 [14] では，偽のポータルサイトにマルウェアが仕込まれていた．

2.2.3 サービス妨害

妨害の対象は，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 とインフラストラクチャへの攻撃には，DoS 攻撃が用いられる．前者には，プローブ要求フレームを大量に送りつけることで，応答処理の負荷をかけることができる．後者には，無線 AP が自身の存在を知らせるビーコンフレームを大量に発することで，電波の混信や，正規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，de-auth パケットなどが使用される．de-auth パケットは，不正な無線ネットワーク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，攻撃者はこれを悪用し，悪性 AP に接続させるためにユーザを正規の無線 AP から切断させることが可能である．サービス妨害の攻撃を組み合わせれば，容易にユーザを悪性 AP に誘導できる．

2.3 悪性 AP の攻撃モデル

悪性 AP はインターネット接続を攻撃対象のユーザに提供することで，sslstrip 等のリアルサービスに紐づく攻撃が可能となる．悪性 AP をインターネットに接続する方法は以下が挙げられる．

- 公衆無線 LAN に接続する
- 有線 LAN で接続する
- テザリングで接続する

有線 LAN での接続は，施設が有線を提供していない場合，第三者が利用するのは困難である．スマートフォンのテザリングによる悪性 AP の実装は非常に容易だが，sslstrip などの各種攻撃を行うことができない．よって本研究では，公衆無線 LAN に接続し，インターネット接続を提供している悪性 AP を考える．本研究における悪性 AP の攻撃モデルを図 2.5 に示す．

クライアントは，フレームの中継を行う無線 AP と無線通信を行う．クライアントと中継 AP 間のフレームを，C-PB フレームと称する．また，中継 AP はクライアントとして，正規サービスの無線 AP と無線通信を行う．中継 AP と正規 AP 間のフレームを，PB-AP フレームと称

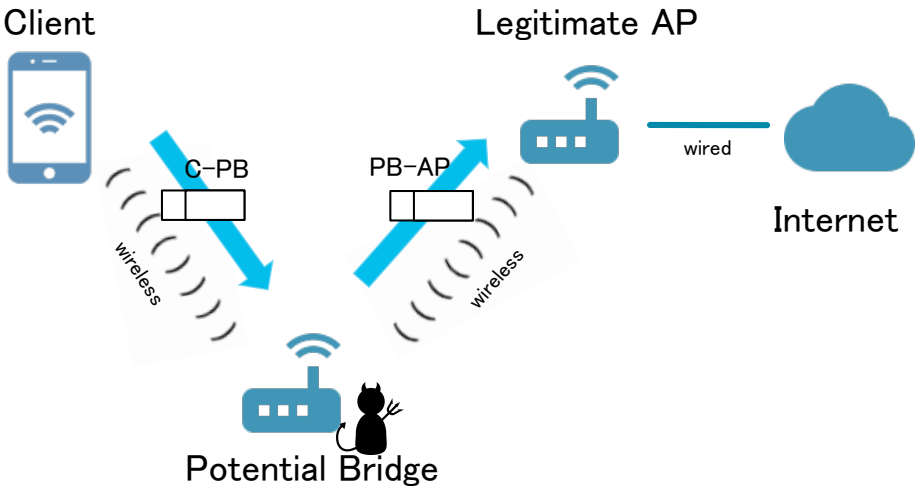

図 2.5　攻撃モデル

する．

また，この中継 AP はルータ，ブリッジのどちらかの挙動を示す．前者の場合は，DHCP サーバとしてクライアントに IP アドレスを割り当て，NAT または NAPT の機能を有する．後者の場合は，データリンク層での処理となり，宛先/送信元 MAC アドレスの書き換えなどを行い，中継する．

正規のネットワーク管理者が設置した中継 AP である場合，中継 AP の SSID は接続している親機と同一の SSID であることが通例である．もし，中継 AP の SSID が親機と異なっていたり，MAC アドレスが親機と同一である場合は，悪性の可能性が高い．前者は，ビーコンフレームの情報から存在を検出できるが，後者はビーコンの情報のみでは検出できない．ただし，悪性 AP が中継するデータフレームは，非常にヘッダの情報が類似していたり，顕著な特徴が存在する．本研究では，C-PB フレームと PB-AP フレームに着目し，攻撃を行っているか否かに関わらず，トラフィックの中継を行っている無線 AP を検出する手法を提案する．

第 3 章　関連研究

- Jana ら [15] は，無線 LAN マネジメントフレームに記載された TSF タイマ値から計算できるクロックスキューを，無線 AP のフィンガープリントとして使用することで，ETA が検出できることを示した．この研究では，クロックスキューの計算手法の違いによる精度の差異，環境の温度変化による，TSF タイマ値のばらつきを考慮した手法を提案している．
- Nakhila ら [16] は，SSL/TCP プロトコルの特徴を利用して，ETA を検出できることを示した．狭い範囲で無線 AP を展開している公衆無線 LAN サービスの場合，それらの無線 AP は 1 つのネットワークのゲートウェイを共有していることが多い．この研究では，外部ネットワークと TCP のコネクションを確立した状態で，ローミング機能により，同一の SSID である他の AP に接続を切り替える．その際に，外部ネットワークとの TCP コネクションが切断された場合，その無線 AP は正規のサービスとは異なるゲートウェイを使用していると言えるため，ETA が検出可能だとしている．
- Han ら [17] は，Round Trip Time（RTT）を利用した手法で ETA が検出可能であるとした．悪性 AP は正規の AP に接続してインターネット接続を提供している場合，通常と比べて RTT が大きくなる．その特徴を利用し，ETA を行っている悪性 AP を検出可能だとしている．
- Lanze ら [18] は，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無線 AP の挙動の際から悪性 AP が検出可能であるとした．ソフトウェアベースの無線 AP には以下の 3 つの特徴が存在することを示した．
  - ビーコンフレームに記載された TSF タイムスタンプの外れ値が大量に存在する．
  - 隣接チャネルのプローブ要求に応答する．
  - プローブ要求の接続先無線 AP の BSSID を異なる値に変更しても応答する．

  上記の特徴を用いて，ソフトウェアベースの悪性 AP が検出可能であるとしている．

文献 [15] [16] [17] は，ETA の検出に特化したものであるため，WiFi Honeypot は検出できない．文献 [17] では，本研究と同様の攻撃モデルを想定している．しかし，多数のユーザが利用する公衆無線 LAN サービスでは，フレーム衝突や電波干渉などによる遅延が大きいため，誤検出を招く恐れがある．文献 [18] の手法は，ツールにて実装した悪性 AP を全て検出可能だが，

ハードウェアベースの WiFi ハッキング機器 [19] も市販されているため，検出できない可能性もある．

本手法は想定する攻撃モデルで実装された悪性 AP であれば，悪性 AP に接続して検証を行う必要は無く，ETA だけでなく WiFi Honeypot も検出可能である点で優位性がある．

第 4 章　悪性 AP の検出手法

本章でははじめに，C-PB フレームと PB-AP フレームの類似性の判定に使用するデータフレームのヘッダ情報について論ずる．次に，そのヘッダ情報を利用した悪性 AP 検出手法を提案する．また提案手法では，上記いずれかのフレームに WPA2 などの無線 LAN 暗号化手法が施されているか否かで，検出アルゴリズムが異なる．よって，それぞれのケースにおける検出アルゴリズムを記述する．

4.1　類似性判定

提案手法では，ノードが送受信する TCP パケットに着目し，類似性の判定を行う．判定に利用するヘッダのフィールドを，表 4.1 に示す．

表 4.1　使用するフィールド

レイヤ	フィールド
TCP	送信元/宛先ポート番号，SEQ 番号，ACK 番号， ヘッダ長，TS Value，TS Echo Reply
IP	データグラム長，フラグメント ID，TTL， 送信元/宛先 IP アドレス
802.11	Receiver アドレス，Transmitter アドレス， シーケンス番号，FCS，Retry フラグ

TCP ヘッダにおいて使用するフィールドは，TCP コネクションごとに値が基本的に異なるものを選択している．異なる TCP ストリームのフレーム間で，これらの全ての値が一致する確率は極めて低い．特に，TCP レイヤの TS Value 及び TS Echo Reply [20] は，送受信端末のクロックを参照しているため，ほとんど一致することは無い．

802.11 ヘッダの送信元，宛先 MAC アドレスのフィールドは合わせて 4 つ存在する，Receiver アドレス，Transmitter アドレスは，それぞれ直前，直後の送受信ノードの MAC アドレスが記載されている．また Retry フラグは，無線 LAN における再送が起きたか否かを判定するために使用する．

悪性 AP がフレームを中継することで，IP アドレスやポート番号など，いくつかのフィールド値は書き換えられる．よって，それらの値が異なるフレーム間にて，他のフィールドが一致していることは極めて少ない．本研究では，悪性 AP にて書き換えが行われないフィールド値の一致を確認することで，フレームの類似を判定する．

4.2 暗号化されていない悪性 AP の検出

本節では，C-PB，PB-AP 双方とも暗号化されていない，オープンな悪性 AP の検出アルゴリズムを示す．提案手法はまた，sslstrip などの盗聴型攻撃が行われているか否かにより，注目すべき点が異なる．盗聴型攻撃の有無それぞれの検出について記述する．

4.2.1 盗聴攻撃なし

検出フローチャートを図 4.1 に示す．はじめに，モニター端末でキャプチャした無線 LAN フレームから，TCP のストリームを全て抽出する．次に，抽出した各ストリームから，送受信ノードの MAC アドレスのペアを抽出する．

悪性 AP がブリッジとしてフレーム中継すると，TCP 及び IP レイヤのフィールドは完全一致となるが，802.11 ヘッダのフィールドが書き換えられる．その場合，TCP 及び IP レイヤの情報が完全一致であるにも関わらず，別のパケットとして認識されるため，類似パケットが同一のシーケンス内に現れる．これは，ETA により MAC アドレスを変更しても，他の 802.11 ヘッダの情報から検出できる．そのため，同一シーケンス内に送受信ノードのペアが複数ある場合，ブリッジとして動作する悪性 AP により中継されたフレームがあると考えられる．よって，TCP 及び IP レイヤのフィールドが全て一致し，802.11 レイヤのフィールドが異なる類似パケットが，ストリーム内に存在するか検証する．存在した場合は，該当ノードを悪性の疑いがある中継 AP と判定する．

ペアが 1 組であった場合は，宛先 IP アドレスごとにストリームをグループに分ける．グループ内のストリームは，送信元 IP アドレスとストリームのペアで管理する．なお，ここでの宛先 IP アドレスとは，外部ネットワークの IP アドレスを指す．グループ分けの例を図 4.2 に示す．

グループ内に複数のノードのストリームがあった場合，グループ内のノード間の類似性判定を行う．悪性 AP がクライアントからのフレームをルータとして中継すると，NAT/NAPT 機能により，送信元 IP アドレス及びポート番号は書き換えられる．よって，それ以外のフィールドは，一致または類似する．その場合，異なる送信元から同一の宛先グローバル IP アドレスに送信された TCP ストリーム間で，類似パケットが存在するはずである．図 4.2 の例では，宛先 IP が z.z.z.z のグループが検証の対象となる．宛先 IP が y.y.y.y のグループは，送信元ノードがノード C のみであるため，検証の対象ではない．その後，異なるノード間のフレームの，ポート番号，IP アドレス，TTL 以外の TCP，IP 層の要素を参照する．もしそれらの値が一致していた場合，該当ノードを悪性の疑いがある中継 AP と判定する．

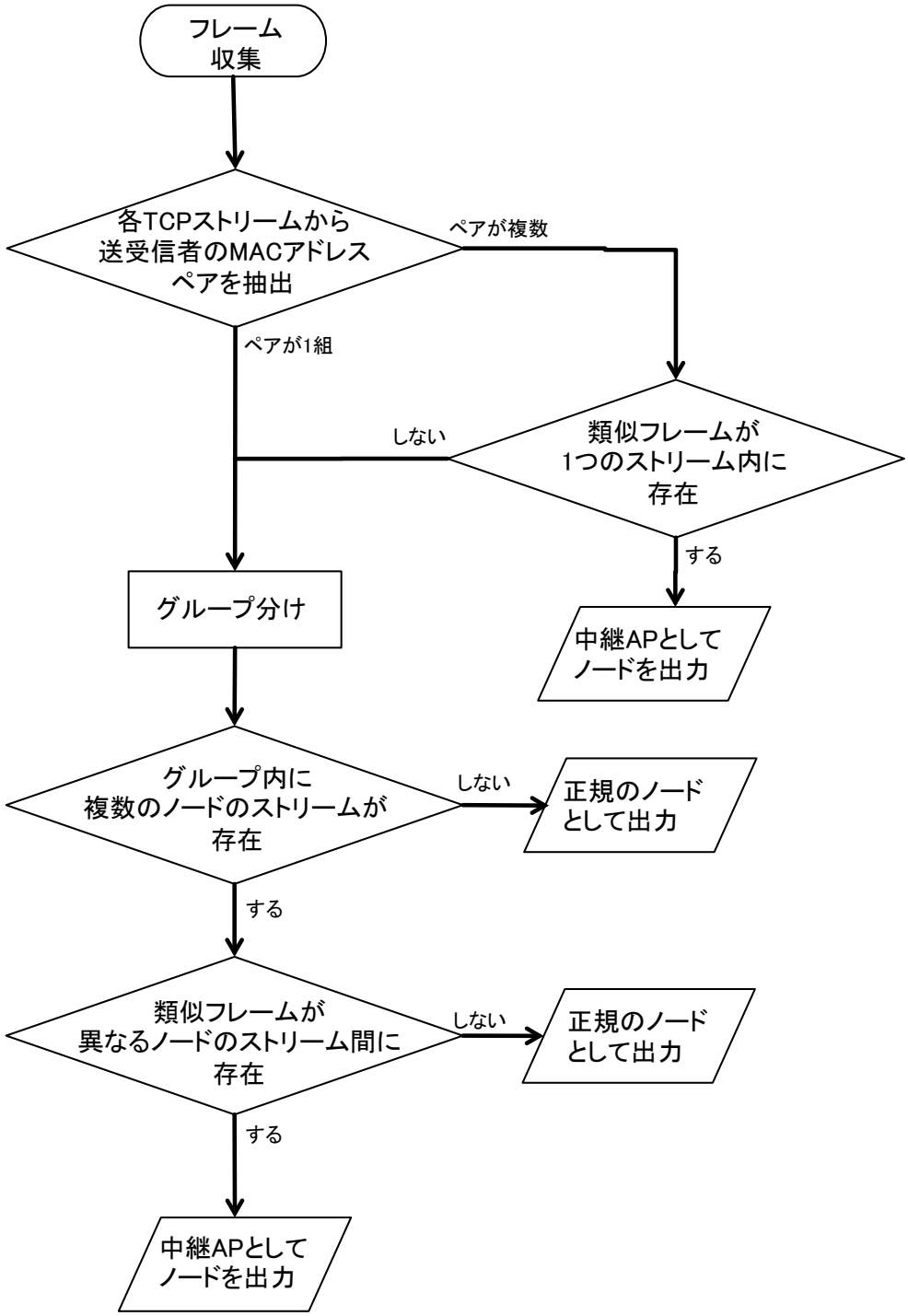
フレーム
収集
各TCPストリームから
送受信者のMACアドレス
ペアを抽出
ペアが複数
ペアが1組
しない
類似フレームが
1つのストリーム内に
存在
する
グループ分け
中継APとして
ノードを出力
グループ内に
複数のノードのストリームが
存在
しない
正規のノード
として出力
する
類似フレームが
異なるノードのストリーム間に
存在
しない
正規のノード
として出力
する
中継APとして
ノードを出力

図 4.1　検出手法の概要

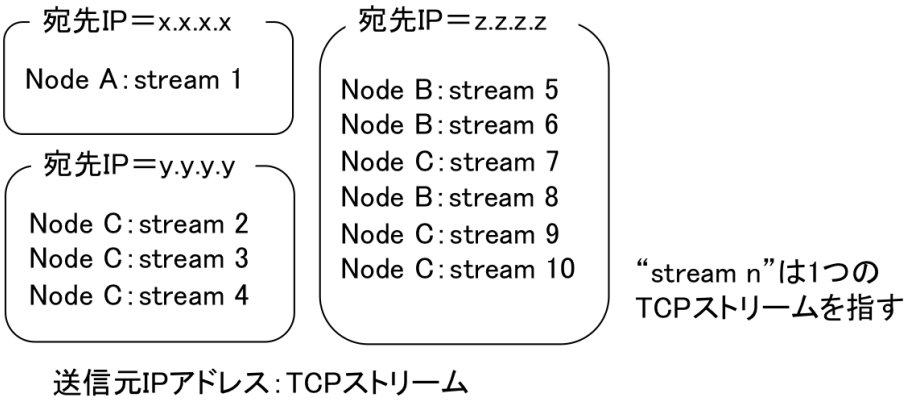

図 4.2　グループ分けフェーズ

4.2.2　盗聴攻撃あり

sslstrip をはじめ，中間者攻撃が実装されている悪性 AP は，攻撃を実装していない場合と中継の仕方が異なる．中間者攻撃の際悪性 AP は，暗号通信を自身で終端させるために，クライアントと悪性 AP 間，悪性 AP とサーバ間でそれぞれ異なる TCP コネクションを確立する．よって，C-PB フレームと PB-AP フレームそれぞれのフィールド値には類似性が無い．しかし，クライアントは悪性 AP とルータを経由せずに通信を行うため，IP レイヤの TTL の値が最大値から減らない．提案手法では，各ストリーム内の全パケットの TTL を確認する．もし双方向のパケットの TTL が最大値であった場合，中間者攻撃による攻撃を受けていると判断できる．なお，キャプティブポータルサイトが存在する無線 AP を検証した場合，C-PB 間での通信のみで認証が行われる可能性があるため，誤検出を招く恐れがある．その場合は，事前にポータルサイトを運用しているサービスのドメインや IP アドレスをホワイトリストに登録しておくことで，誤検出を防ぐことができる．

4.3　暗号化された悪性 AP の検出

WPA2 などの暗号化が通信に施されていた場合，IP レイヤ以上のフィールドは参照できない．ただし，悪性 AP がクライアント，サーバ間のトラフィックを中継する性質は変わらない．よって本研究では，悪性 AP が中継する通信量の時系列データに着目する．ある送受信ノードが時間 T 秒で行った通信量の時系列（例えば 1 秒間隔の計測値）を観測する．送受信ノードペアごとに時系列データ間の相関係数を算出し，相関係数が 1 に近い場合は，その通信の中間に位置するノードを中継 AP と判定する．

第 5 章　評価実験

本章では，第 4 章で提案した手法により，中継トラフィックデータから悪性 AP を検出できるかの評価を行い，得られた評価結果について考察する．

5.1　オープンアクセスの悪性 AP

評価実験における実験環境と使用した機材を，それぞれ図 5.1， 5.2 に示す．ペネトレーションテスト用に市販されている WiFi ハッキング機器の WiFiPineapple **??**を悪性 AP として動作させ，研究室の無線 AP に接続させる．ASUS の Zenfone1 台（Victim）を悪性 AP 経由で，他 2 台（Host A/B）を研究室の無線 AP（正規 AP）経由で外部ネットワークにアクセスさせ，LinuxOS を搭載したモニター端末で無線 LAN パケットを全てキャプチャする．なお，本研究では全ての通信を同一チャネルで行っている．また，悪性 AP 上で sslstrip を動作させたケースと，動作させていないケースそれぞれの実験を行った．

結果として，攻撃の有無に関わらず，提案手法による悪性 AP 検出率は 100% であった．また，同一の web サイトを訪問し，検証対象のグループに存在した正規のクライアント端末も，誤検出されることは無かった．よって，中継トラフィックの類似性に着目した本手法は，悪性 AP 検出に有効であると言える．

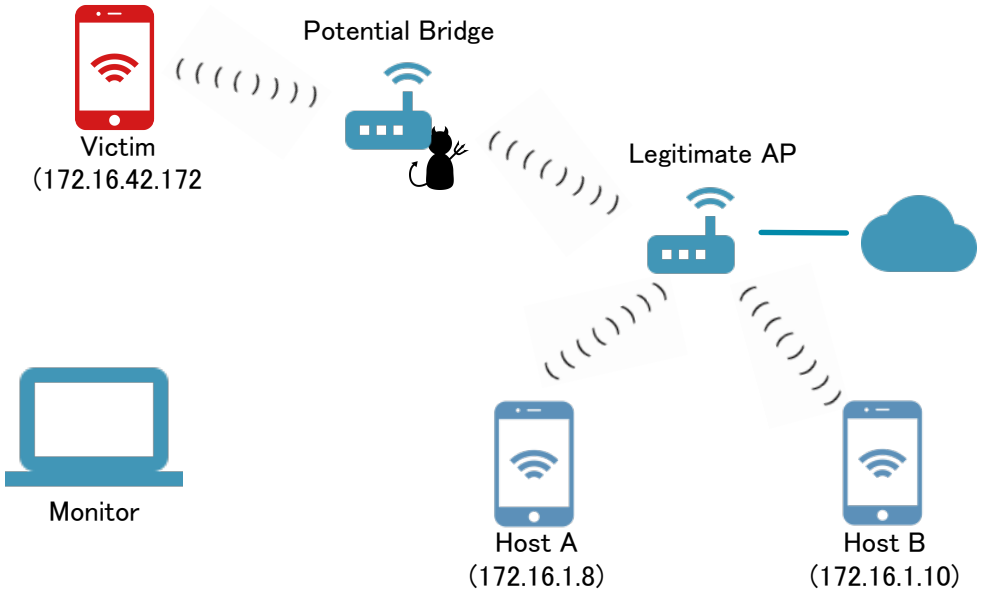

図 5.1　実験環境

図 5.2　評価実験に使用した機材

5.2 暗号化された悪性 AP

本節では，無線 LAN を WPA2 などで暗号化した悪性 AP の検出手法が有効であるかどうかを検証する．

5.2.1 提案手法の有効性

第 5.1 節と同じ環境で，暗号化された中継トラフィックから悪性 AP を検出できるか検証を行った．悪性 AP に接続した被害者端末で，森研究室の HP，google トップページ，amazon トップページ，youtube トップページ，動画視聴の順序で，インターネットとの通信を合計 150 秒間行った．また，正規の AP に接続した Host A にて，上記 Web サイトにランダムにアクセスを行う．その際の C-PB フレーム，PB-AP フレーム，Host A と正規 AP 間の 1 秒あたりのそれぞれのトラフィックデータ量を，それぞれ図 5.3， 5.4， 5.5 に示す．

時系列グラフから，各 web サイトを訪れた際のスパイクが，C-PB フレームと PB-AP フレームでは類似していることがわかる．この C-PB フレームと PB-AP フレームの時系列データの相関係数は，0.9580 と非常に高い数字であった．しかし，C-PB フレームと Host A のグラフは類似点が少なく，相関係数も 0.1597 と非常に低い結果となった．この結果から，フレームが暗号化されていたとしても，クライアントと無線 AP 間の通信量の相関からトラフィックを中継している無線 AP を検出できることがわかる．

また，観測した合計 150 秒のトラフィックデータを 10 秒ごとに分けた際のそれぞれの相関を，CDF で図 5.6 に示す．中継されたフレーム間では，短時間でも比較的高い相関があることが見て取れる．しかし Host A のフレームとの相関は，短時間ではほとんど相関がない．この結果から，もしクライアントが悪性 AP と短時間の通信を行っていた場合でも，トラフィックの相関から悪性 AP を検出できる可能性がある．

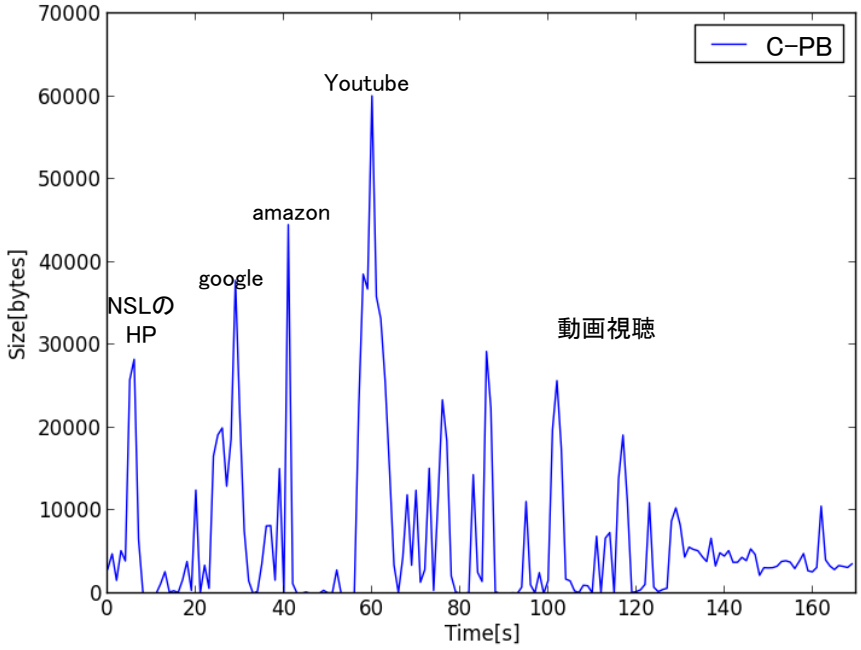

図 5.3　C-PB フレームの時系列データ量

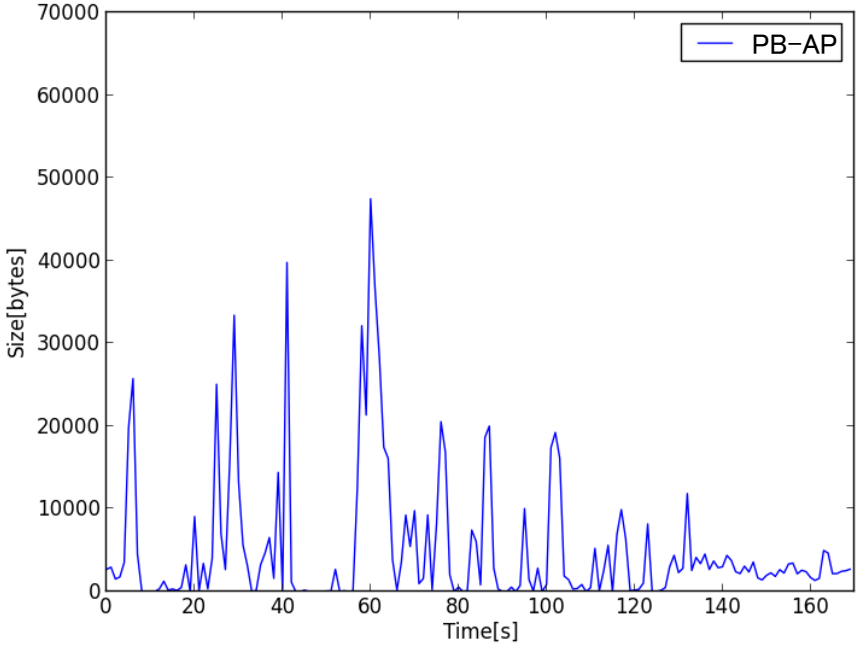

図 5.4　PB-AP フレームの時系列データ量

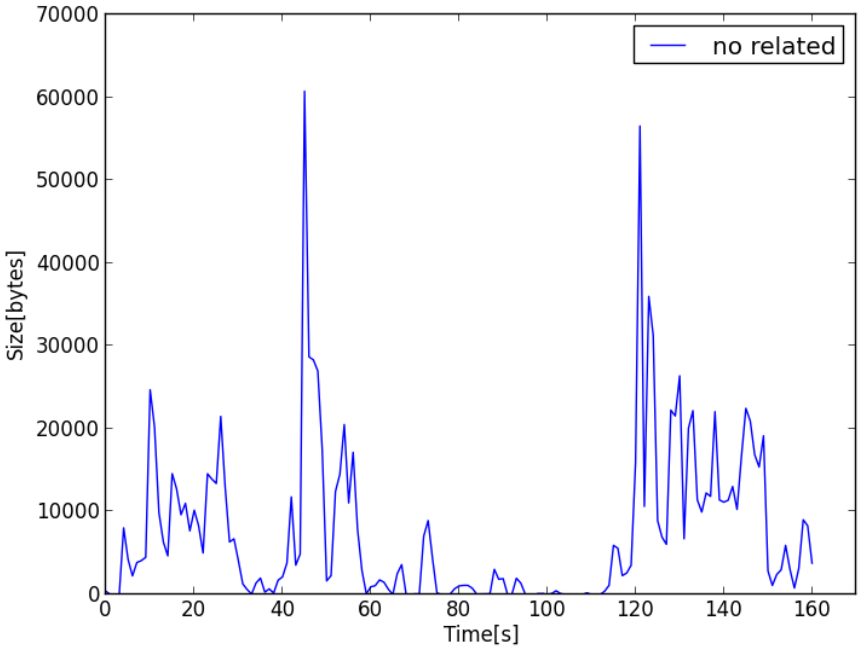

図 5.5　Host A の時系列データ量

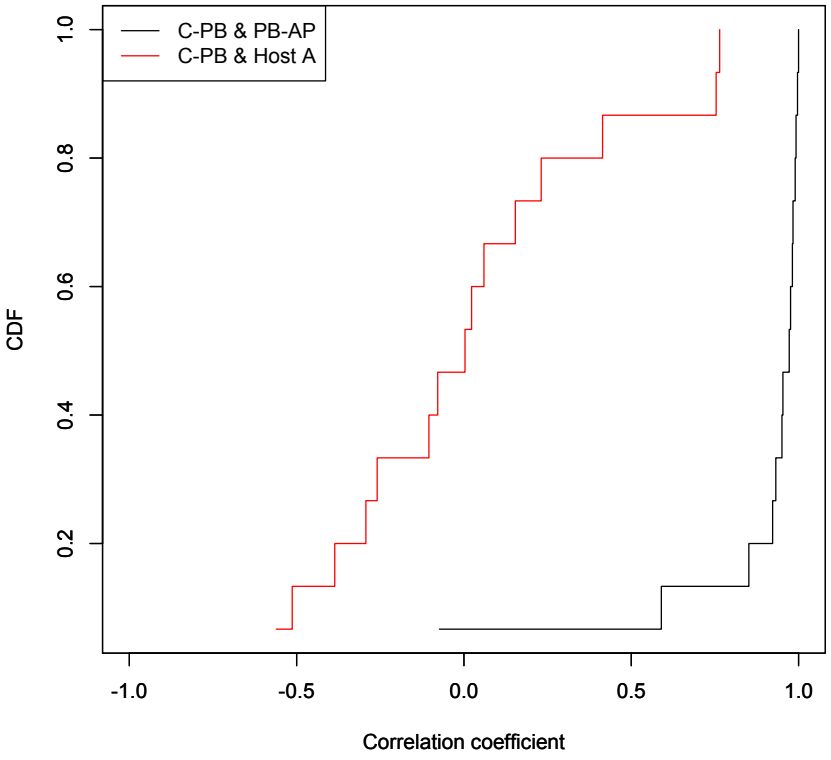

図 5.6　10 秒あたりの相関係数の累積分布

5.2.2 誤差因子の影響度

提案手法は，無線通信におけるデータフレームの通信量を利用した手法であるため，悪性 AP を設置した攻撃者が意図的に PB-AP フレームを増やすことで，検出を回避する可能性も考えられる．また，データフレームの再送による通信量の増加も結果に影響を与えると考えられる．よって，そのような誤差因子がどれだけ結果に影響を及ぼすかの評価を行った．

第 5.2.1 項で得られた暗号化された PB-AP フレームを使用する．150 秒の観測データに，ノイズデータを単位時間の通信量にそれぞれ加える．一様分布に従ったノイズを加えた際の，乱数の最大値と相関係数の関係を，図 5.7 に示す．また，正規分布に従ったノイズを加えた際の，乱数の平均と相関係数の関係を，標準偏差が平均の 1/10，1/5，1/2 である場合に分けて図 5.8 に示す．

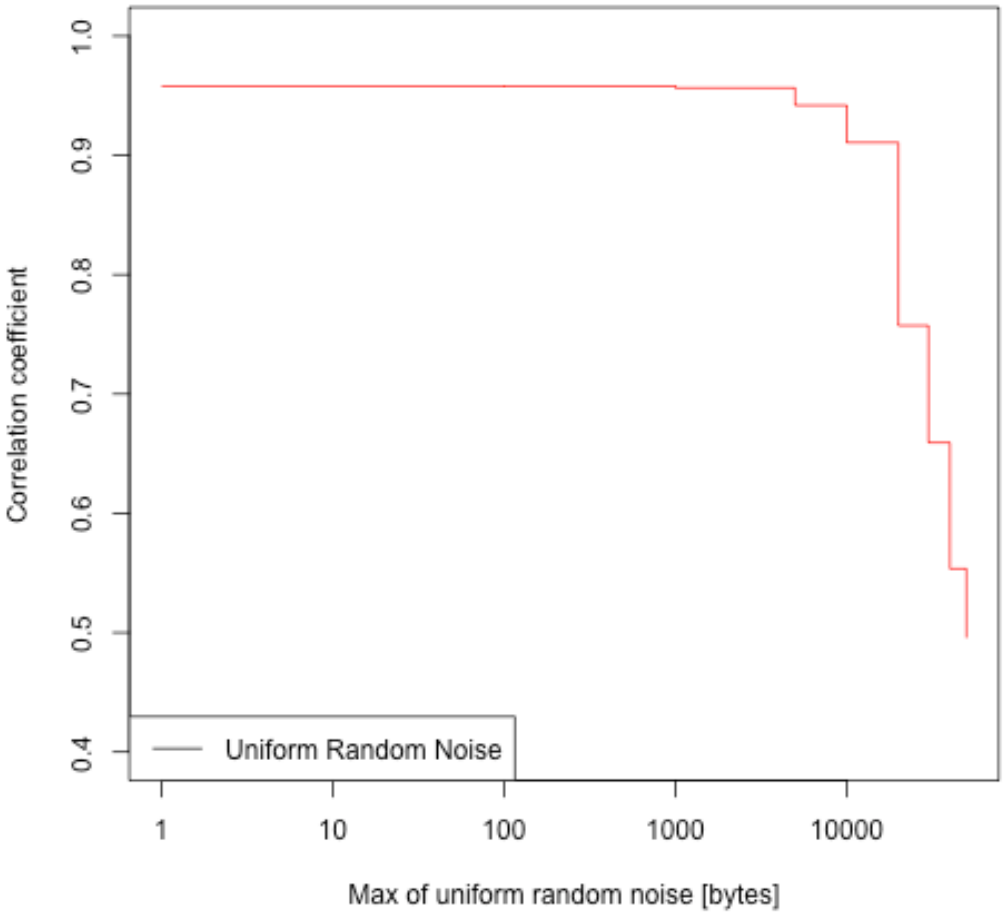

図 5.7　一様分布に従ったノイズと相関の関係

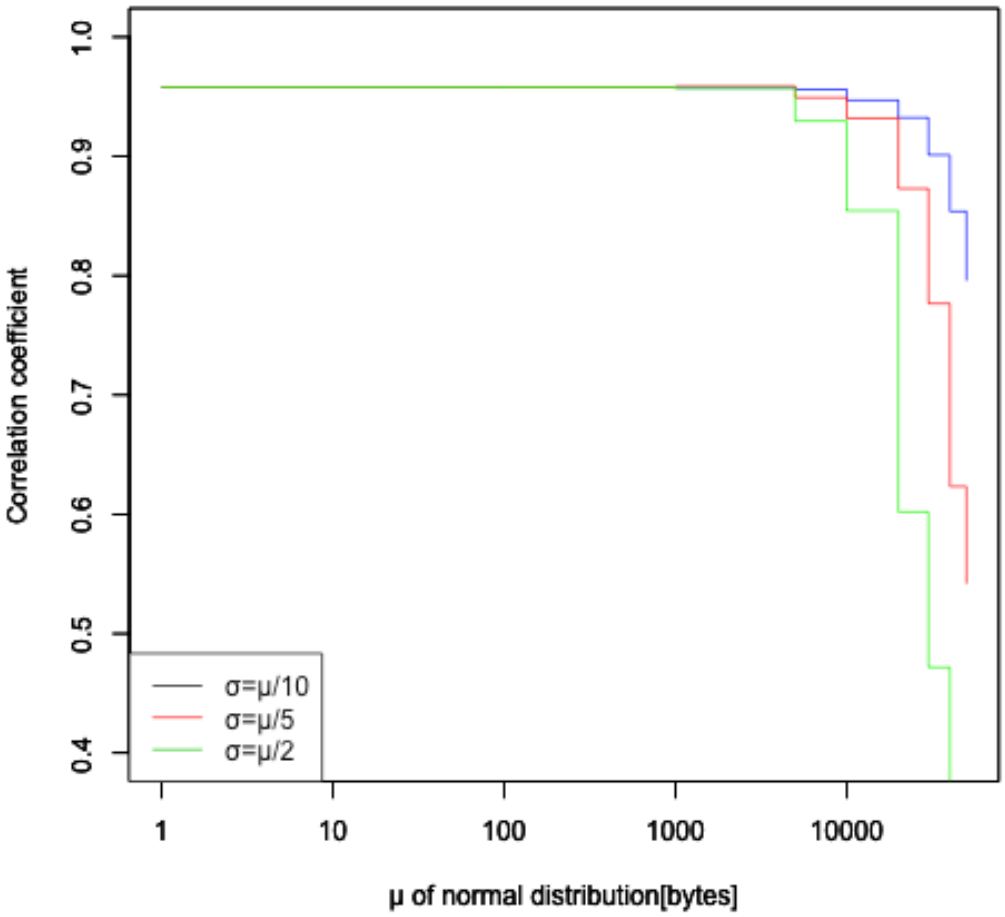

図 5.8　正規分布に従ったノイズと相関の関係

図 5.7，5.8 から，分散の小さいノイズであればノード間の通信量の相関に影響はあまり見られない．攻撃者が一定サイズのノイズを周期的に加えた場合は，検出精度には影響がないと言える．ただし，分散とともにノイズのデータサイズが大きくなると，相関は低くなることがわかる．図 5.3 から，Youtube などの Web ページアクセスのみでも通信量は数万 byte に及ぶことがわかる．攻撃者がランダムに上記の Web サイトと通信を行った場合，フレーム間の相関に大きな影響を与える．これらの結果から攻撃者にとって C-PB，PB-AP フレーム間の相関を低くすることは容易であると言える．よって，提案手法はこのようなシナリオに対する耐性は低い．

またデータフレームの再送制御により相関が低くなる場合も考えられる．無線 LAN におけるデータフレームの再送は，無線クライアントの増加や電波の混信によって増加する．しかし，再送フレームである場合には 802.11 ヘッダの Retry フラグが立つため，無線 LAN における再送フレームを除くことができる．よって無線 LAN における再送は結果に大きな影響を与えることは無い．ただし TCP レイヤにおける再送は，フレームが暗号化されている以上判断が不可

能である．ネットワーク環境の悪化に伴い，短時間に連続した再送が行われた場合，少なからず結果に影響を及ぼすと考えられる．

第 6 章　実地調査

本章では，提案した悪性 AP 検出手法を用いて，東京都渋谷駅周辺の悪性 AP 実態調査を行った結果を示す．またその結果から考察できる悪性 AP の現状，公衆無線 LAN サービスの課題，本手法による調査のスケーラビリティについて述べる．

6.1　調査概要

東京都の渋谷駅周辺において，無線 AP が比較的多いと考えられる 8 地点で，通信が暗号化されているか否かに関わらず，無線 LAN 通信のモニタリングを行った．実地調査に使用した機材を図 6.1 に示す．LinuxOS を搭載したノートパソコンをモニター端末として使用し，LinuxOS 上で動作するフリーのパケットキャプチャツール，airodump-ng により無線 LAN 通信を観測した．無線 LAN 通信は 802.11g 規格であると想定し，全１３チャネルのモニタリングを行う．なお，C-PB フレームと PB-AP フレームは同一チャネルを使用しているとは限らないため，類似フレームの観測には全チャネルを同時にモニタリングする必要がある．そのために無線 LAN カードを１３枚用意することが理想であるが，今回の調査ではモニター端末に内蔵されているものも含め，合計 4 枚の無線 LAN カードで調査を行った．

実地調査における無線 LAN 通信モニタリングのフローチャートを図 6.2 に示す．まず，観測地点周辺に存在する無線 AP をスキャンし，使用しているチャネルのリストを取得する．1 つの悪性 AP は，最大で 2 つのチャネルを使用しフレームを中継するため，2 つのチャネルを同時に観測する必要がある．観測地点周辺にて N 個のチャネルが使用されていた場合，${}_NC_2$ 個のチャネルのペアが作成できる．作成したペアの集合を 2 つに分け，4 枚 2 組の無線 LAN カードで並列にチャネルのペアを 10 秒間モニタリングする．観測時間を 10 秒に設定した理由は，第 5 章で述べたように，類似フレームが存在した場合は 10 秒間の通信でも十分に相関が高いためである．観測時間は全 13 チャネルが使用されている場合で，最大約 390 秒となる．観測が終わり次第，次の観測地点に移動し，同じ操作を行う．その後提案手法にて，全 8 地点で観測したデータから悪性 AP が検出できるか検証を行う．

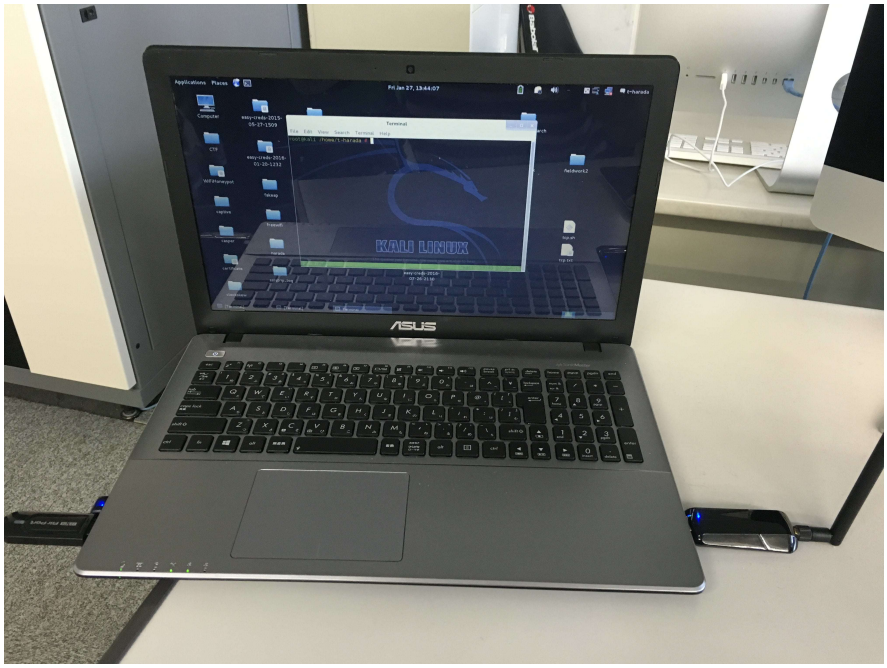

図 6.1　実地調査に使用した機材

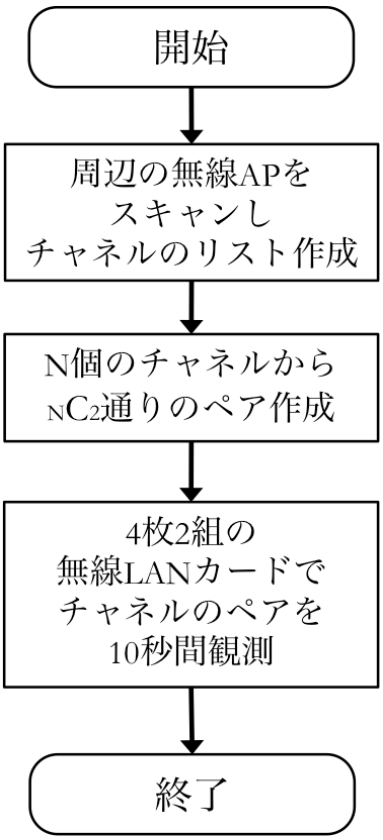

図 6.2　実地調査のフローチャート

6.2 調査結果

結果として，フレームを中継しているとみられる無線 AP は，暗号化されているか否かに関わらず検出されなかった．チャネルのペアごとに観測したデータには，データフレームが含まれていないことがあり，類似性を検証できていないペアが多く存在した．

全 8 地点において観測された無線 AP の数を，SSID（サービス名）と BSSID（MAC アドレス），無線 LAN の暗号化方式ごとに，表 6.1 に示す．また，観測を行った 8 地点と，数箇所の無線 AP の内訳を示した図を，図 6.3 に示す．

表 6.1　観測された無線 AP の内訳

暗号化方式	SSID	BSSID
WPA2	506	803
WEP	97	240
OPEN	48	354
不明	28	101
合計	679	1498

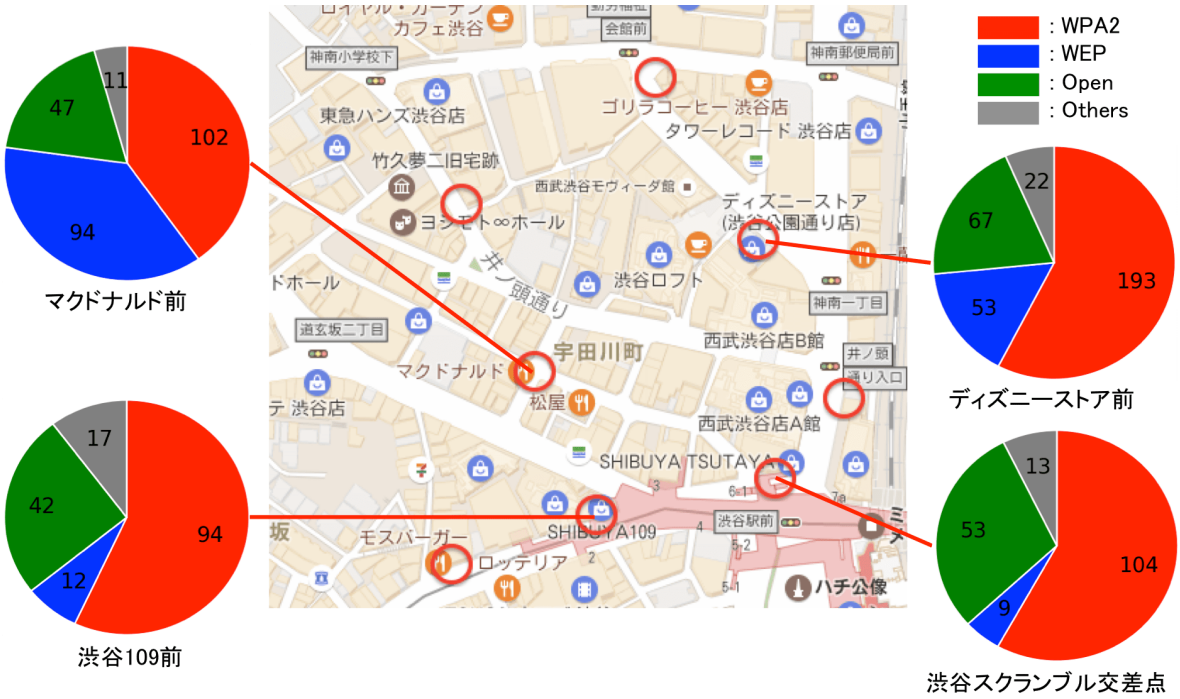

図 6.3　実地調査の観測地点

6.3 考察

本節では実地調査により得られた結果について，悪性 AP の現状と，実地調査を通して顕在化した公衆 WiFi サービスの課題と対策，検出手法を用いた実地調査のスケーラビリティについて考察する．

6.3.1 悪性 AP の現状

結果として悪性 AP は検出されていないため，渋谷駅周辺にて複数の悪性 AP が常駐しているという最悪のケースはないと言える．ただし，本調査では全チャネルを同時にモニタリングすることができず，また観測時間も 10 秒間であった．そのため，悪性 AP の通信と観測端末のモニタリングのタイミングが合わずに，悪性 AP の通信を見逃している可能性も考えられる．現に，比較的人通りの多い日中に調査を行ったにもかかわらず，データフレームを大量に受信することができなかった．よって正確な調査を行うためには，長期間にわたり無線 LAN を全チャネル同時に監視する必要がある．

6.3.2 公衆 WiFi サービスの在り方

実地調査を通して，表 6.1 に示したように大量の無線 AP を観測した．その中でも安全でない WEP の暗号化方式や，暗号化を施していない無線 AP が多く存在したことは，無線 LAN の脅威が浸透していないためと考えられる．表 6.2 に，受信したビーコンフレームから得た，暗号化されていない公衆 WiFi サービスの SSID の一例を挙げる．

暗号化されていない無線 AP は，半数以上が SSID のステルス機能を使用していた．ステルス機能とは，ビーコンフレームに SSID を記載せずに，無線 AP の存在を秘匿する機能である．無線 AP の不正利用を防ぐために機能を使用していると考えられるが，通信が暗号化されていない以上，盗聴の危険性がある．クライアントが発するプローブ要求フレームには SSID が平文で記載されているため，ステルス機能を使用していても不正利用の危険性がある．

また他の SSID には，有料無料を問わずキャリア系事業者の提供する WiFi サービスが多く見受けられた．特に"Free"という文字列が入っているサービスや，多くの利用者が来店するスターバックスの提供する無線 AP は，Twitter などのサービスと連携することで手軽に WiFi サービスを利用できるものが多い．サービス連携の際は認証のための通信が暗号化されているはずだが，オープンな無線 AP である以上，認証画面が攻撃者により偽装されている可能性も否めない．よって公衆 WiFi サービスの通信を，より安全な WPA2 による暗号化方式に統一すべきだと考える．

これらの課題に対する対策として，第 1 章で述べた Passpoint の導入が挙げられる．公衆 WiFi サービス業者間で連携を取り，異なる WiFi サービスのセキュアな無線 AP 間をローミングさせ

表 6.2　暗号化されていない公衆 WiFi サービス一覧

SSID	観測数
SSID なし	183
Wi2Premium	48
SWS1day	25
.FREE_Wi-Fi_PASSPORT	21
0001softbank	20
0000Visit_SHIBUYA	6
7SPOT	6
OlOl_marui_Free_Wi-Fi	5
Wi2	4
0000FLETS-PORTAL	4
0000Shibuya_City_01	3
rakuten-cafe	3
FREE_Wi-Fi_and_TOKYO	3
QFRONT Free Wi-Fi	3
Famima_Wi-Fi	3
at_STARBUCKS_Wi2	2
Bic_Wi2_WiFi	2
SHIBUYA109_Free	2
Wi2_free	2
wifi_square	2

ることで，セキュリティとアクセシビリティが向上すると考えている．実際にサンフランシスコの公衆 WiFi サービスはこの技術を導入しており，プロファイルを端末にインストールすることで，異なる WiFi サービス事業者間でもローミング可能である．現在流通している無料 WiFi スポット接続アプリは，暗号化されていない無線 AP にのみ接続を行うため，セキュリティの面で劣っている．最低限，利用者の多い国内の観光地などの公衆 WiFi サービスに Passpoint を導入することがサービス全体の課題であると考えている．

6.3.3　実地調査のスケーラビリティ

本調査では，全チャネルを同時にモニタリングすることができず，観測時間も短秒間であったため，正確な調査を行うことはできなかった．よって，モニター端末が全チャネルを同時に数分単位でモニタリングし，それを継続することにより，正確に悪性 AP の挙動を監視できる

と言える．また，そのようなモニター端末を複数用意し同期させることで，大規模な調査が可能である．数分間モニター端末に周辺の無線 LAN 通信を監視させ，得られたデータをモニター端末，またはそれらをコントロールするサーバなどに送り，検出手法によりデータを解析する．解析の結果，フレームを中継する無線 AP を発見した場合は，悪性 AP が接続している正規の公衆サービスの管理者に通知する．このようなモデルで調査を行うことで，より広いエリアでも悪性 AP の動向を監視することができる．ただし，無線 LAN の電波強度や電波干渉を考慮すると，100m 間隔程度でモニター端末を配置しなければならないため，費用対効果の評価が必要である．

第 7 章　制約

本研究の制約は，主に以下の 3 つである．

- 正規の公衆 WiFi サービスが提供している中継無線 AP を誤検出する
- 攻撃モデルが異なる悪性 AP を検出できない
- C-PB，PB-AP フレーム間の相関を意図的に低くする悪性 AP を検出できない

一つ目の制約は，検出した中継無線 AP が悪性であるか否かを判断することができないということである．実際に無線 LAN 中継機は市販されており，公衆 WiFi サービスが中継機を使用している可能性もある．．本研究の調査で検出した無線 AP 及び公衆 WiFi サービスは中継機を使用していないと考えられるが，施設の提供する WiFi サービスなどでは，中継機を使用している可能性がある．本手法を実地で常時運用する場合，あらかじめ周辺の WiFi サービスにて使用されている無線 LAN 中継機調査し，ホワイトリストに登録するなどの対策が考えられる．

二つ目の制約は，第 2.3 節で想定した攻撃モデル以外の悪性 AP を検出することができないことである．本研究は，インターネット接続を攻撃対象のユーザに提供するために，正規の公衆 WiFi サービスの無線 AP に無線接続をしている悪性 AP を検出対象としている．よって，悪性 AP が PB-AP 間を有線接続，テザリングで接続している場合，本手法では検出できない．また第 2.2.3 項で述べた，偽のポータルサイトへ誘導する通信改竄攻撃は，攻撃者が通信を悪性 AP で終端させる可能性もあるため，PB-AP フレームが存在しない．他の攻撃モデルで実装された悪性 AP への対策として，我々の過去の研究 [21] で提案した手法を組み合わせることが挙げられる． [21] で我々は，悪性 AP による攻撃時の通信の特徴から悪性 AP を検出する手法を提案した．この手法では攻撃モデルに関わらず，sslstrip などの各種攻撃を行っている悪性 AP を検出可能である．

三つ目の制約は，第 5.2.2 項で述べた，ノイズデータの混入による悪性 AP の誤検出，見逃しである．暗号化された通信では参照できるフレームのヘッダは限られているため，ノイズデータの除去は困難である．このような場合の悪性 AP 検出は本研究の今後の課題である．

第 8 章　まとめ

本研究では，大半の悪性 AP が隣接する通常の無線 AP の中継機として動作することに着目し，中継されたトラフィックデータの類似性から悪性 AP を検出する手法を提案した．

検出手法を用いて渋谷駅周辺の悪性 AP 実態調査を行い，約 1500 個の無線 AP を調査したが，悪性 AP が存在する可能性は低かった．しかし調査の中で，公衆 WiFi サービスの約 4 割が通信を暗号化していない，または安全でない暗号化を施した無線 AP を使用していた．これらの無線 AP をユーザが利用した場合，通信が盗聴され個人情報が漏洩する可能性がある．セキュアな無線ネットワークをローミング可能とする Passpoint 技術を公衆 WiFi サービスに導入し，安全な公衆 WiFi サービスを提供すべきである．

本手法は，全チャネルを同時に長時間モニタリングできる端末に適用することで，悪性 AP の動向を常時監視することができる．また，それらの機能要件を満たしたモニター端末を複数用意し，それらから得られたデータを同期することで，非常に大規模なエリアで調査が可能である．

本手法は通信が暗号化されているか否かに関わらず，悪性 AP の検出に有効である．ただしノイズデータが混入された場合は，暗号化された悪性 AP の検出精度が著しく低下する．また，正規の中継無線 AP を悪性 AP として検出してしまうこと，想定した攻撃モデルと異なる悪性 AP を検出できないことが本手法の制約である．今後の展望として，これら制約への対策，全チャネル同時モニタリングによる正確な悪性 AP 実態調査の実施が挙げられる．

第９章　研究業績

国際ポスター発表（査読付き）

1. T.Harada，T.Mori，S.Goto，"Detecting Malicious Wireless APs: Methodology and Field Studies"，The 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2015)

国内研究会

1. 原田 敏明，森 達哉，後藤滋樹，"その無線アクセスポイント安全ですか？～悪性無線 AP の分類とフィールド調査"，コンピュータセキュリティシンポジウム 2015 論文集，vol.2015，No.3，pp. 931-938，2015 年 10 月
2. 原田 敏明，森 達哉，"中継トラフィックデータの類似性に着目した悪性 WiFi アクセスポイントの検出"，信学技報 vol.116，no. 251，IN2016-52．pp.19-24．2016 年 10 月

開発ソフトウェア

1. WiFiGuardian，
   https://play.google.com/store/apps/details?id= org.morilab.wifi.wifiguardian&hl=en

参考文献

[1] ICT 総研. 2016 年 公衆無線 lan サービス利用者動向調査. http://ictr.co.jp/report/20160913.html.

[2] 観光庁総務省. 無料公衆無線 LAN 整備促進協議会整備促進 PT の報告. http://www.mlit.go.jp/common/001115688.pdf.

[3] NTTBP. Japan Connected-free Wi-Fi. http://www.ntt-bp.net/jcfw/about/ja.html.

[4] Norton. The Norton Wi-Fi Risk Report. http://www.slideshare.net/NortonSecurity/norton-wifi-risk-report-global.

[5] Wireshark. https://www.wireshark.org/.

[6] Aircrack-ng. https://www.aircrack-ng.org/.

[7] passpoint. http://www.wi-fi.org/ja/discover-wi-fi/wi-fi-certified-passpoint.

[8] Hotspot 2.0 Announcement by San Francisco. http://www6.sfgov.org/index.aspx?page=255.

[9] AVAST Software. https://www.avast.co.jp/.

[10] Most will connect to an unsecured Wi-Fi hotspot if it's free. http://www.zdnet.com/article/most-will-connect-to-an-insecure-wi-fi-hotspot-if-its-free-stu

[11] HTTP Strict Transport Security. https://tools.ietf.org/html/rfc6797.

[12] Preload HSTS. https://www.chromium.org/hsts.

[13] Wire & Wireless. https://wi2.co.jp/jp/300/.

[14] 無線 LAN フィッシング. http://internet.watch.impress.co.jp/cda/news/2005/05/12/7562.html.

[15] Suman Jana and Sneha K Kasera. On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews. In *IEEE Transactions on Mobile Computing*, Vol. 9, pp. 449–462, March 2010.

[16] Omar Nakhila, Erich Dondyk, Muhammad Faisal Amjad, and Cliff Zou. User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols. In *Military Communications Conference MILCOM 2016 - 2016 IEEE*, pp. 1243–1248, 2016. ISSN 2155-7586.

[17] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li, and Sanglu Lu. A Measurement Based Rogue AP Detection Scheme. In *IEEE INFOCOM 2009*, pp. 1593 – 1601, 2009.

[18] Fabian Lanze and Andriy Panchenco and Ignacio Ponce-Alcaide and Thomas Engel. Detecting Software-Based 802.11 Evil Twin Access Points. In *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*, pp. 225–232, 2015.

[19] WiFi Pineapple. `https://wifipineapple.com/`.

[20] V. Jacobson. TCP Extensions. `http://www.networksorcery.com/enp/rfc/rfc1323.txt`, May 1992.

[21] 原田敏明, 森達哉, 後藤滋樹. その無線アクセスポイント安全ですか? 悪性無線 AP の分類とフィールド調査 . コンピュータセキュリティシンポジウム 2015 論文集, 第 2015 巻, pp. 931–938.

謝辞

本研究を進めるにあたりご指導を頂いた，早稲田大学森達哉准教授に感謝致します．また，研究に関する議論に付き合っていただき，研究に必要な機材を貸していただいた早稲田大学嶋本薫教授，大河内志彦さんに感謝致します．