Title	位置情報を用いた偽無線LANアクセスポイントの検出
Sub Title	Detection of the rogue access point by physical location
Author	殷, 佳一(Yin, Kaichi) 加藤, 朗(Kato, Akira)
Publisher	慶應義塾大学大学院メディアデザイン研究科
Publication year	2016
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2016年度メディアデザイン学 第516号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40001001-00002016-0516

修士論文 2016 年度（平成 28 年度）

位置情報を用いた
偽無線 LAN アクセスポイントの検出

慶應義塾大学大学院
メディアデザイン研究科

殷　佳一

本論文は慶應義塾大学大学院メディアデザイン研究科に
修士 (メディアデザイン学) 授与の要件として提出した修士論文である。

殷　佳一

審査委員：

加藤　朗　教授　（主査）
砂原　秀樹　教授　（副査）
石戸　奈々子　准教授　（副査）

修士論文 2016 年度（平成 28 年度）

位置情報を用いた
偽無線 LAN アクセスポイントの検出

カテゴリー：サイエンス / エンジニアリング

論文要旨

近年、物理的なケーブルの代わりに電波だけで通信する手段として、有線 LAN より利便性が高い無線 LAN は通信、商業、旅行など様々な分野で用いられている。しかし、無線 LAN の普及と共に、今までにないセキュリティ問題が発生している。中間者攻撃、電波妨害など攻撃手法は情報漏洩に繋がる。無線 LAN には自動接続と言う利便性に優れた機能がある。この機能によって、ユーザがより快適にインターネットを利用できる。しかし、端末の自動接続機能を利用し、偽無線 LAN のアクセスポイントが正規無線 LAN に成りすまし、通信パケットを覗き、暗号化されていない情報を盗み取られることもある。現状では、偽無線 LAN に対して警戒していないことが多い。結果、偽無線 LAN 攻撃は通信情報を覗く成功率は高く、非常に危険な状態である。これに対し、教育によるセキュリティ意識を高めること以外では、適切なシステムで守らなければならない。偽無線 LAN アクセスポイント検出には幾つかの方法がある。ESSID、BSSID、IP などによる検出は一般的な方法であるが、本物に近い偽物には有効ではない。本研究は物理的な位置情報によって偽無線 LAN アクセスポイント検出方法を選択した。物理的な位置情報でアクセスポイントを特定するシステムを設計、実装を行った。物理的な位置情報による偽無線 LAN アクセスポイント検出の精確性且つ利便性を示す。

キーワード：

セキュリティ, 無線 LAN, 自動接続, 位置情報, 偽無線 LAN

慶應義塾大学大学院 メディアデザイン研究科

殷　佳一

Abstract of Master's Thesis of Academic Year 2016

Detection of The Rogue Access Point by Physical Location

Category: Science / Engineering

Summary

In recent years, Wi-Fi, which access to the Internet only use radio waves instand of the physical cables, is more convenient than LAN that to be recommended in many areas such as communications, business, tourism and so on. But now a days, we find more security problems which may disclosure our private infoemation than before. Such as Man in middle attack, communication interference and so on. There is a auto-connect function in Wi-Fi. Users can use Wi-Fi more convenient by this function. But on the other hand, a rough Wi-Fi accesspoint may be camouflaged with a regular one to peep our information take advantage of the auto-connect function. Unfortunately, there is no enough vigilance for it.As a result, you will have a high probability of peeping personal informations by a rough Wi-Fi accesspoint. So in my opinion, it is a rather dangerous situation. Of course, we can wake people up by education, or make a secure system to prevent this problem. There are many ways to find out a rough Wi-Fi accesspoint.May you can scean the status like ESSID, BSSID, IP address and so on to identify the accesspoint. But, this is not affective to a welldone rough Wi-Fi accesspoint. So in may system, I will use the physical locations. Because it has a high precision and easy to implement. And it has be proven by creating a core system on a smartphone.

Keywords:

Security, Wi-Fi, Auto connection, Physical Location, Rough Wi-Fi

Graduate School of Media Design, Keio University

Kaichi Yin

目　　次

図　目　次

表　目　次

第1章
序　　論

本章では、本研究の動機、研究対象の問題を解決する方法及び目標達成する基準について、本論文の構成について述べる。

1.1. 背景

近年のインターネットを利用する傾向は非常に高い。平成27年通信利用動向調査の結果により13歳～59歳のインターネット利用は9割を上回っており、60～79歳のインターネット利用は上昇傾向である。クラウドサービスを利用している企業の割合は年々上昇しており、平成27年末には4割を上回った [1]。その上、無線LANはLANと比べ優れた便利性を持っている。総務省では、公衆無線LANについて、2020年オリンピック・パラリンピックの東京開催を見据え、観光立国を推進する観点から、関係省庁、関係団体とも協力し、整備の促進に取り組んでいる [2]。

しかし、インターネットの発展と共に、セキュリティ問題に注目しなければならない。それは、インターネットを構成する重要なパーツの一つとして、無線LANは現在多岐にわたり利用されているからである。その優れた便利性と共にセキュリティ問題が浮かび上がった。無線LANを利用する際、あたかも正当な無線LANアクセスポイント（AP）と同じ挙動をする偽無線LAN APに接続すると、情報漏洩の危険性がある。それにも関わらずユーザの認証とは異なり、APの認証はあまり注目されず、放置されている。

無線LANには自動接続機能があり、この機能を利用しユーザが快適に無線LANを利用できるが、自動接続により、偽無線LANに繋がる可能性も高くなる。特に

携帯端末では、無線 LAN の接続が優先されている為、一般端末より危険である。そのため、偽無線 LAN に接続すると通信情報（通信内容、通信相手など）が漏洩する危険性が高まる。

1.2. 目的

本研究は、偽無線 LAN 問題を完全に解決するのは不可能である。偽無線 LAN が、正規無線 LAN から離れている場合の解決策を検討する。無線 LAN のセキュリティを強化し、その利便性を失わない前提で、一般ユーザが偽無線 LAN AP に接続しないことを目的とする。あるべからず処に存在する無線 LAN を怪しい無線 LAN に判定する。既に接続している怪しい無線 LAN に対して、正しい AP 情報と照合した上でその接続を制御する。正規無線 LAN AP であることを確認できない場合、ユーザに警告する。システムの実装によって、位置情報による偽無線 LAN AP の検出の信用性と便利性を実証する。

1.3. 方法

偽無線 LAN の検出より、被害を受けない方法がある。それは、全ての通信が VPN 経由で行うことである。また、その VPN サーバは認証されている、安全なサーバでなければならない。しかし、現状ではこれを実現するのは難しい。以上のことを踏まえた上で、AP の検出について検討を行った。AP の位置情報などの情報を特定し、事前に記録、接続することで情報を照合する。これにより、100% 確実ではないが、偽 AP を検出することが可能である。アプリケーションの実装により、検出された偽 AP への接続はユーザの同意の上で制御する。実装方法については第 5 章で示す。

1.4. 本論文の構成

本論文は本章以外、以下五章から構成される。

第 2 章は本研究と関わる様々な専門用語を説明する。第 3 章では現存の脆弱性を調査について述べる。主に無線 LAN のセキュリティ問題とその攻撃手法について説明する。第 4 章は偽無線 LAN と正規無線 LAN の位置関係を分けて、偽無線 LAN の対策を述べる。位置情報によって、解決できる場合と、難しい場合を分析する。その上で、本研究は最終的に物理的な位置情報を選択した理由を説明する。第 5 章は本研究の中核である。第 4 章で述べた解決方法でシステムを構築し、システムの流れと役割を述べ、現状で実装できるアプリケーションの動きを説明する。本章の最後に、得られた成果とまた足りない問題を説明する。第 6 章は本論文で述べている研究の内容と成果を総括し、残された今後の研究課題について述べる。

第2章
用　　語

本章では、本研究に関わる専門用語を説明する。本研究において専門的な用語を多々使用するため、本章では無線 LAN に関する専門用語を説明していく。本研究では、無線 LAN の仕組みを理解した上で、その通信を守るセキュリティを固めることに尽力する。

- 無線 LAN
  無線 LAN、通常では Wi-Fi と呼ばれる無線通信を利用し、データの送受信を行う LAN システムのことである。現在は IEEE の LAN/MAN 標準化委員会が規格化した IEEE 802.11 シリーズが標準として普及している [3]。無線 LAN の電波は最初 2.4GHz の帯域を使っている。国の法律によって、規定は変わるが、日本では 14 チャンネルが利用可能である。ただし、チャンネル 14 は 11Mbps モードのみ使用が許されており、転送性能が限られる。その原因で最近の製品や海外の製品はサポートしていないことから、ほとんど用いられない。その後、IEEE 802.11a により 5GHz の帯域が追加された。5GHz の無線 LAN はチャンネルが多く、通信速度が速いため好評を受けているが、電波の干渉により屋外での使用は法律で禁じられている場合がある。現在室内では、2.4GHz と 5GHz を併用することが多い。また、ESSID、BSSID、セキュリティ方式など無線 LAN のステータスについては後述する。

- ESSID
  ESSID（Extended Service Set IDentifier）、通常は SSID ともいう。IIEEE 802.11 シリーズの無線 LAN（Wi-Fi）におけるネットワークの識別子の一つ。無線 LAN では有線 LAN の様に通信線路を選べないことから、無線 LAN の

区別のために付けられるネットワーク名である。最大 32 文字までの英数字を任意に設定でき、ESSID が一致する端末としか通信しない [4]。通信時、SSID は無線 LAN の接続に重要な役を果たしているため、無線 LAN の分別には重要なステータスの一つである。

- 自動接続
  自動接続とは、端末が記録された ESSID を発見した時に、認証方式が同一の時に限り、自動的に再接続する仕組みである。この機能は利便性に優れており多用されている。これによって、無線 LAN がユーザの意思以外で切られても、通知なしで自動的に再接続する。しかし、これはセキュリティの面では問題であり、本研究が必要になる一因となっている。詳しくは第 3 章で述べる。

- BSSID
  BSSID は無線 LAN において、通信端末がアクセスポイントを識別するために使われる。長さ 48 ビットの ID のことである。通常はアクセスポイントの無線 LAN インターフェースの MAC アドレスが使われている [5]。MAC アドレスの偽造は可能だが、一般的には正しいものとして扱われている。アクセスポイントを偽造する為に、MAC アドレスを正規アクセスポイントの MAC アドレスと同一にすることで発覚の可能性を下げることができるが、一般的には BSSID のチェックはしていないことも多く、ここまでの対応はしなくても済む。

- WEP
  WEP は Wired Equivalent Privacy の略である、IEEE 802.11 無線ネットワークのセキュリティのためのアルゴリズムだったが、容易に解読されたため廃れた [6]。現在、WEP は推奨されていない。WEP に使われたストリーム暗号 RC4 は通信パケットを集めてパスワードの推定が可能となる。しかし、古いアクセスポイントか無線端末はハードウェア上新しい暗号化方式をサポート出来ないため、現在も WEP を使っている無線 LAN は少なくとも存在している。

- RC4

  RC4 は WEP に使われている暗号化方式である。この方式は公式的な発表はなく、通常は RC4 と呼ばれる。1987 年で Ron Rivest が設計し、30 年近く使われていたが、近年、この暗号化方式は破れ、安全ではないことが証明された。2015 年、TLS の中に RC4 の使用は RFC 7465 によって禁じられた [7]。攻撃者は通信の中間者になって、RC4 を使った HTTPS サイトの cookie 注入を成功した。

  RC4 は暗号化と復号に同じキーを使う。その上、XOR だけで暗号化を行っている。暗号化の時に使われたキーはランダムで生成されたものの、同じキーが使われる確率は通信パケットの生成と共に高まっている。同じキーを使う二つのパケットを見つければ、パスワードが容易に解析できる。現在では、短時間で RC4 を使っているサイトを解析できる [8]。

- WPA-PSK

  WPA は Wi-Fi Protected Access の略である。Wi-Fi Alliance の監督下で行われている認証プログラムである。WPA プロトコルは、それ以前の WEP に対して脆弱性を指摘されたため、その対策として策定された。WPA では、TKIP（WPA とも呼ばれる）もしくは CCMP（WPA2 とも呼ばれる）による暗号化が提供されている。個人や小規模のネットワークには事前共有鍵モード（PSK、またはパーソナルモード）が使われている [9]。

- IV

  Initialization Vector、初期化ベクトル、同じ暗号鍵でストリームを生成しても毎回異なるストリームを生成する為に必要とされるビット列である。これにより、毎回暗号鍵を替えるといった時間のかかる作業を省くことができる [10]。

- HTTPS

  HTTPS（Hypertext Transfer Protocol Secure）は、HTTP による通信を安全に行うためのプロトコルである。実際では、SSL/TLS プロトコルによって提供されるセキュアな接続の上で HTTP 通信を行うことを HTTPS と呼

んでいる。現在 TLS1.2 が多く用いられている。幾つかの暗号化方式が決められており、セキュリティレベルが以前より遥かに高まっている。通常は、安全性が高い RSA 暗号を使ってセキュアな通信を確立し、計算速度が速い AES 暗号で通信内容を暗号化する。

- 認証
  認証は、対象の正当性を確認することである。インターネットにおいて、Certification と Authentication の二種類の認証方式が多く使われている。パスワード、証明書など相手に認証して貰うのは Certification に該当され、デジタル署名などは Authentication に当たる。本研究にとって、証明書認証はシステム構成中、重要な要素である。
  証明書（デジタル公開鍵証明書）は認証局（CA、Certificate Authority）から発行される。証明書には公開鍵と持ち主の記載があり、記載の個人、組織、サーバその他の実体がこの公開鍵に対応した私有鍵の持ち主であることを証明する。認証局は証明書の申請者の身分を確認することを義務付けている。したがって、利用者はその証明書を信用することができる（図 2.1）。

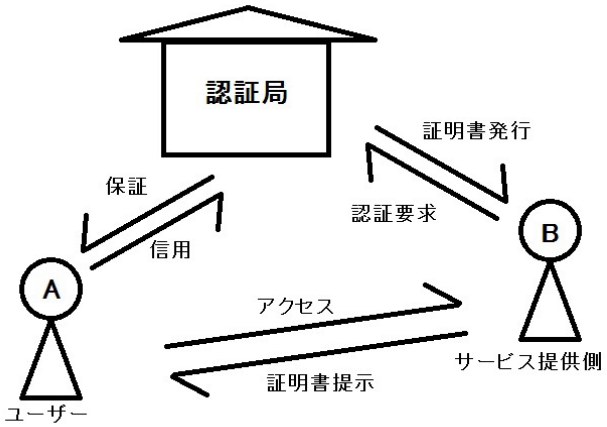

図 2.1: デジタル証明書による信頼関係

- 辞書攻撃
  プログラムにより辞書ファイルを使って、順次辞書に含まれる候補に対して

パスワード検証を行う攻撃である。辞書を用いることで、総当たり方式に比べて探索効率を上げることができるが、辞書に含まれていないものを発見することはできない。

- 中間者攻撃
  中間者攻撃は通信に介在することによって、通信データを盗聴または改竄することである。無線 LAN は電波を用いることから有線 LAN より中間者攻撃は容易である。本研究の対象である偽無線 LAN も中間者攻撃の一種である。端末は偽のアクセスポイントを経由し、インターネットにアクセスした時、全ての通信パケットは偽のアクセスポイントによって監視される（図 2.2)。詳細は第 3 章で述べる。

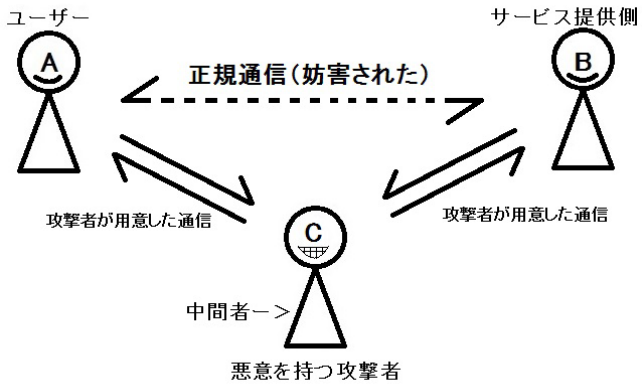

図 2.2: 中間者攻撃

- 偽無線 LAN
  偽無線 LAN、Evil Twin Attack とも呼ばれている。正規無線 LAN と同じステータスの偽物アクセスポイントを作って、正規無線 LAN のフリをして通信端末をアクセスさせ、中間者として通信データを盗聴あるいは改竄する。ステータスを完全一致させることにより、一般的に無線 LAN で用いられている情報だけでの検知は難しいと考えられる。例として、渋谷駅で KMD と同じ無線 LAN を作ると図 2.3 に示すようになる。。

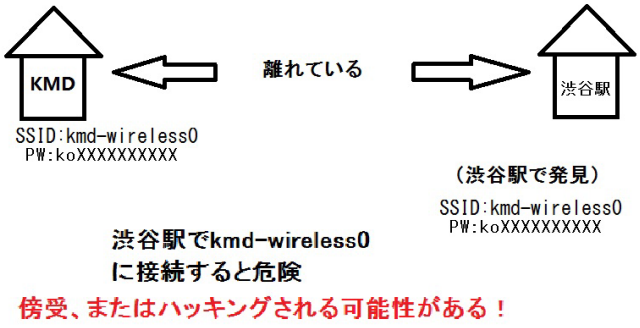

図 2.3: 偽無線 LAN の図例

- 位置情報
  位置情報とは、地理座標（または地図座標）で表示された位置のことである。本研究では、二次元座標の上で位置情報を特定する。すなわち、緯度と経度で位置情報を得るが、より精度の高い位置情報を取得する場合には、標高を加えて三次元位置情報を判断することが望ましい。

- GPS
  GPS（Global Positioning System）、全地球測位システムである。アメリカの衛星から出した電波を分析することによって、現在の緯度と経度を知ることができる。衛星電波を受信しにくい場所、特に室内では十分な電波を受信できず、必要な精度が得られない場合も多い。現時点では、最も汎用性の高い位置測定システムである。

- 基地局情報
  基地局情報とは、携帯基地局から電波で通知される情報である。都市では同時に複数の基地局から電波を受信できることが多い、それによって端末の位置をある程度絞ることができる。基地局は通常広い範囲に送信しているので、基地局情報によって得られる位置情報の精度は高くないが、本論文の目的では十分な精度があると考えられ、この情報も併用することが望ましい。

第3章
無線LANの脆弱性

無線LANの通信では、ケーブルは不要であるため電波だけでデータを転送している。これは無線LANの最大の利点であり、弱点でもある。ケーブルというデータを守る物理的なトンネルがなくなり、通信時にはデータは近傍の空間全体に届くことになる。情報が盗まれる可能性が生じる。

本章では無線LANの脆弱性について調査し、分析する。先ずは無線LANの脆弱性とその攻撃手段を述べる。次に、本研究と関わり深い自動接続の脆弱性について説明する。また本章の最後に、これらの脆弱性による深刻な被害を述べ、これらの脆弱性が生まれた原因について考察する。

3.1. 無線LANの仕組みによる脆弱性

無線LANの通信パケットは近傍の空間全体に届いているため、誰でも受信することができる（図3.1）。さらに、通信パケットには、アクセスポイントと端末両方のMACアドレスが含まれており、MACアドレスは通常変わらないため、受信する端末を特定することが出来る。特に攻撃を仕掛けず、端末（ユーザ）の情報が漏れる場合もある。これは無線LANの仕組みによる脆弱性である。その上、人為的な攻撃を用いて無線LANの脆弱性がさらに突かれる。

無線LANではユーザのプライバシやセキュリティを確保するため、古くはWEPが用いられていた。また最近では、WPAあるいはWPA2というパケットを暗号化する手段が用いられている。しかし、WEPでは第2章で述べた通り使用する暗号の強度が不十分であるため容易に解読されてしまう。またWPA/WPA2は、暗号は比較的強いものの、鍵を共有するPSK方式が多く用いられている。そのた

め、多くの人がアクセスしている公衆無線 LAN では、WPA を用いていたとしても、事実上暗号は意味をなさない。

本格的な対策は、ユーザ毎に異なった鍵を使うことができる WPA/Enterprise 方式を使うことである。この方式は、ユーザ毎に認証を行う必要がある。そのためユーザ毎に個人証明書やパスワードを生成し、ユーザにセキュアに配布する。そしてユーザはその情報をそれぞれの機器に正しく組み込むことが必要になる。従って、誰でも簡単にできる方式とは言えず、企業内部などサポートが得られる環境以外ではあまり用いられていない。

つまり、多くの無線 LAN では、共有鍵さえ入手できればパケットの復号は可能であり、特に公衆無線 LAN では、VPN や SSH などの、別に提供される暗号化を併用することが重要である。

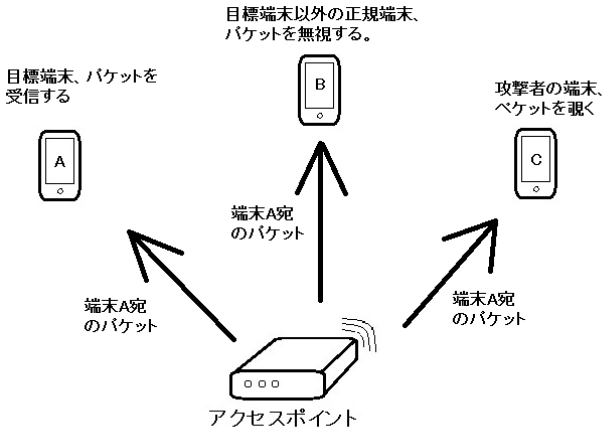

図 3.1: 通信パケットは同じ空間中全ての端末に送る

3.2. 無線 LAN に対する様々な攻撃目的とその手法

一般的には、通信に対する攻撃目的は以下となる。それぞれの攻撃目的に対して、攻撃手法も異なる。

- 通信の妨害

- 通信の盗聴と改竄
- ユーザの行動分析による個人情報の漏洩

3.2.1 通信の妨害

通信の妨害、つまりユーザが無線 LAN を利用できなくなることである。妨害の前提として、目標とする無線 LAN の情報を事前に入手しなければならない。妨害によって、公衆無線 LAN や無線 LAN の提供者の信用性が下がる。その上、この通信の妨害から利益を得る場合がある。

- 物理的な攻撃
  無線 LAN に対する攻撃の中では、一番分かりやすいのが物理的な攻撃である。無線 LAN のアクセスポイントの位置情報を知る前提で、アクセスポイントを破壊すれば通信は止まる。通信を妨害する目的は簡単に達成できる。しかし発覚リスクも高く、現地に行かなければならない。潜入ルートと逃走ルートを用意して、一撃でアクセスポイントを仕留める手段を準備する必要がある。この種の攻撃に対して、アクセスポイントを関係者以外アクセス出来ない様にすることが挙げられる。また、無線 LAN アクセスポイントへのケーブルも攻撃対象になりやすいので、保護する必要がある。

- 電波妨害
  電波による妨害は、物理的な攻撃より遥かに安全且つ高効率である。無線 LAN の通信は電波で行っている。同じエリアでは無線 LAN と同じ周波数の電波が存在していると、無線 LAN の通信に干渉し、データの転送が出来なくなる。攻撃者は正規無線 LAN が使用している電波の周波数を簡単に調べることができる。それに合わせて妨害電波を発射すれば良い。また、電子レンジなど他の電波を出す設備も電波妨害の原因になる可能性がある。

3.2.2 通信の盗聴と改竄

通信の盗聴は妨害より難易度は高く、改竄であればさらに難易度が高い。

無線 LAN は近傍の空間全体に電波を送出しているため、その電波を受信出来る端末があれば、通信データの盗聴は可能となる。WEP や WPA で暗号化していても、共有鍵を入手すればパケットの復号は可能である。これを防ぐために、パケットをこれらとは異なったレベルで暗号化する必要がある。

無線 LAN 通信の改竄は盗聴の上で通信パケットの内容を変更し、正規端末に送ることである。無線 LAN 通信のパケットには一定なフォーマットがあり、通信内容以外のデータは暗号化を行わないことも多い。例え通信内容が暗号化されて分からなくても、パケットの部分を改竄できれば、一定な攻撃になれる。これを防ぐにはかなり難しいことになる。何故なら、通信パケットのパケット部分は手紙の宛先のように、暗号化されたら不便が生じることがある。

世の中には無線 LAN のセキュリティを確認するため、様々なソフトウェアが開発されており、それらのソフトウェアは同時に、攻撃者に利用され兼ねない。攻撃者は盗聴によって秘密情報を手に入れるか、通信データの改竄によって偽情報の配布が出来る。

- Aircrack-ng

  Aircrack-ng は攻撃手法ではなく、Thomas d'Otreppe de Bouvette たちが開発した無線 LAN 評価ツールである [11]。2006 年以来、Aircrack の新しいバージョンとして、無線 LAN を評価するプログラムである。無線 LAN を攻撃するより、管理者がこのプログラムを使って、無線 LAN の安全性を確かめる。無線 LAN セキュリティ、特に古いセキュリティタイプの WEP に対して、抜群な攻撃力を持っている。WEP は不安全な RC4 を使っており、攻撃者が暗号化されたデータを含まれている通信パケットを大量入手すると、暗号の解析が可能になる。Aircrack-ng は通信パケットを偽造することにより、ARP パケット（有効な暗号文データが含まれている）を増やすこともできる。その上で、WEP への攻撃を行う。このような欠陥を利用し、Aircrack-ng はすべての WEP にパスワードを解析できる。また、現在多く使われている WPA-PSK2 に対し、辞書攻撃もできる。

Aircrack-ng を利用して無線 LAN のセキュリティテストをする場合は、Aircrack-ng の付属コマンド airmon-ng でアダプタをモニタモードに変更し、airodump-ng で周囲の無線 LAN 情報を知ることができる（図 3.2）。詳しい攻撃手順は付録 A に示す。

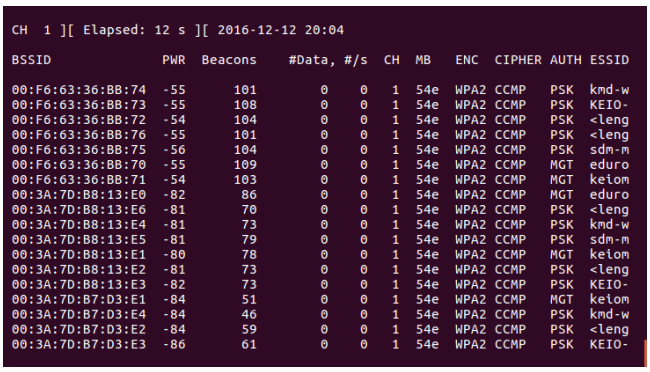

図 3.2: airodump-ng で無線 LAN 情報を見る

- 無線 LAN における中間者攻撃
  攻撃者は正規無線 LAN の電波を妨害し、正規無線 LAN のフリをして端末に電波を出すことによって、攻撃者と正規無線 LAN の間に新しい通信が始った場合、正規通信の中間者攻撃が可能である。その場合、端末はただ一瞬の断線と再接続を行っただけであり、無線 LAN 環境ではこの様なことは定常的に発生しているため、検知するのは難しい。
  また、インターネット上中間者攻撃を防ぐためには、サーバに証明書を発行し認証を行う必要がある。しかしながら現時点では、アクセスポイントを認証する標準的な方法はないため、中間者攻撃されやすい環境になっている。無線 LAN での中間者攻撃を防ぐ方法として、全ての通信を暗号化し、VPN 経由で通信する。この時、VPN の対地機器を正しく認証することが、中間者攻撃を防ぐためには必要である。インターネット上、このようなサービスを提供する業者がいることも確認されたが、それらの機能を使用するにはか

なりの費用が必要であるため、一般ユーザに向いていない。

3.2.3 ユーザのアクセス情報による個人情報の漏洩

前述のことから、MAC アドレスによって端末を特定することが出来る。ユーザが使用している端末数は数台程度のことが多く、ユーザを特定することは必ずしも容易ではないが、端末で人を推定できることになる。無線 LAN を管理者は、管理下の無線 LAN の接続情報を取得することができる。無線 LAN の接続情報からは、ユーザが誰であるかは特定できないものの、ユーザが特定の無線 LAN アクセスポイントの近傍に出現したことや、その傾向などについて、パケットの内容を覗くことなく知ることができる。また、接続先の IP アドレスの記録はある条件では法令上必須である。その記録を分析することは必ずしも法令で許されている訳ではない。しかし、接続条件などに記載しユーザが承認した場合は、個人の特定までは必ずしもできないが、パケット本体を覗かなくても、ユーザの学校や会社などの属性についてかなり細かく知ることができる場合が多い。暗号化されていないパケットを覗くことは、日本では通信の秘密という憲法に規定されている規約によってできないが、悪意を持った管理者の行動まで縛ることはできないことも事実である。

暗号化されていない通信の危険性を示す一例を挙げる。HTTPS が使われていないページがあるとする。このページにアクセスした時、当然、通信内容は暗号化されていない。図 3.3 に示すように、暗証番号を入力しないと次のページには進まないページがあったとする。ユーザはとある公衆無線 LAN を利用してこのページにアクセスしている時、同じ公衆無線 LAN を利用している攻撃者は通信相手が分かる。これによって、ある大学のメールサーバにアクセスしていると、その関係者と推定できる。さらに、暗号化されていないパケットの本体を観測することにより図 3.4 及び図 3.5 に示すように平文のパスワードも知ることができてしまう。

図 3.3: 暗号化されていないパスワード入力ページ

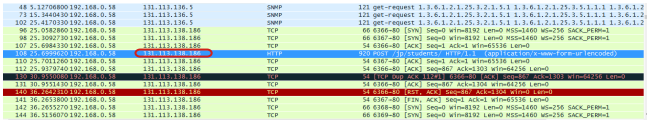

図 3.4: パスワードが含まれる可能性があるパケット

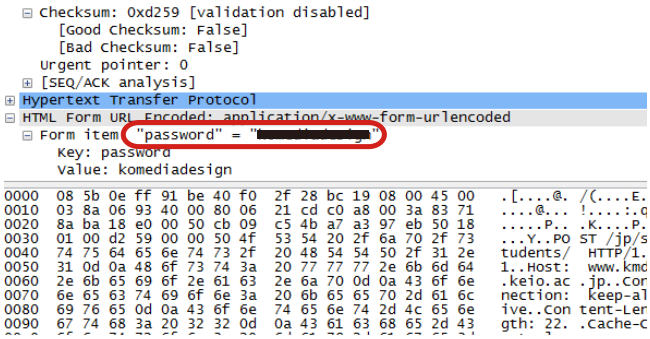

図 3.5: パスワードが表示された通信パケット

3.3. 偽無線LANの構築

偽無線 LAN というと複雑に聞こえるが、それを構築する為に必要なのは小型コンピューター台と無線 LAN 親機機能付きのアダプター一つだけである。本研究では Dell のコンピュータに Ubuntu 16.04.1 システムを入れて、無線アダプタについては Buffalo WLI-UC-GNM を用いた。偽アクセスポイントを作るソフトウェアとして、hostapd 2.5 と isc-dhcp-server を採用した（表 3.1）。hostapd 2.5 はコンピュータを使い、無線 LAN のアクセスポイントを立ち上げるソフトウェアである。isc-dhcp-server は立ち上がったアクセスポイントに DHCP 機能を付けるソフトウェアである。また、Cisco Systems のアクセスポイントに MAC アドレスを設定できれば、それも使用可能となる。本研究では必要な設定を設定ファイルに保存して、hostapd を立ち上げ、無線 LAN をブロードキャスタする。具体的な設定手順は付録 B に示す。

偽無線 LAN は正規無線 LAN と同じステータス（ESSID、BSSID、暗号化方式と暗号鍵など）を持っているからこそ端末を騙せる。通常、ESSID、暗号化方式と暗号鍵が同一なら接続が可能である。しかし、既にアクセスポイントの偽造に対策しているソフトウェアがインストールされていた場合、BSSID が異なると、偽造が検知される。そのため、市販されているアクセスポイントは基本項目しか

表 3.1: 偽無線 LAN アクセスポイントの構築環境

コンピュータ	Dell Latitude E5440
システム	Ubuntu 16.04.1
アダプタ	Buffalo WLI-UC-GNM
AP ソフトウェア	hostapd 2.5
DHCP ソフトウェア	isc-dhcp-server

設定できない為、偽造無線 LAN には適していない。

一例として、IODATA の WN-AC583RK では基本項目として ESSID、暗号化方式とパスワードがある。その中、MAC アドレス (BSSID) はステータス画面で調べることができるが、それを設定する機能は無いことが多い（図 3.6）。その為、偽造には向いていない。アクセスポイントの偽造には、Cisco のアクセスポイント或は特定のソフトウェアが必要とされる。Cisco のアクセスポイントを使い、アクセスポイントの偽造をする場合、コンソールで設定する場合が多い（図 3.7、図 3.8、図 3.9、図 3.10）。ソフトウェアを使って、アクセスポイントの偽造を実現する場合、ESSID、暗号化方式とパスワードが設定ファイルに既に含まれている（図 3.11）。BSSID だけはソフトウェアがアダプタの MAC アドレスを参照し自動で生成される。それを変更する為には、アダプタの MAC アドレスを偽造しなければならない。多くのアダプタでは MAC アドレスが設定可能である。Ubuntu の場合、ifconfig を使えば簡単に偽造出来る。偽造アクセスポイントの MAC アドレスを前文で述べた市販アクセスポイントに偽造した。変更前後の MAC アドレスは明らかに異なっている（図 3.12）。また、この変更は通信に反映される。直観的に表現するために、明らかに偽造の MAC アドレス 00:aa:bb:cc:dd:ee を使い、通信を行った（図 3.13）。

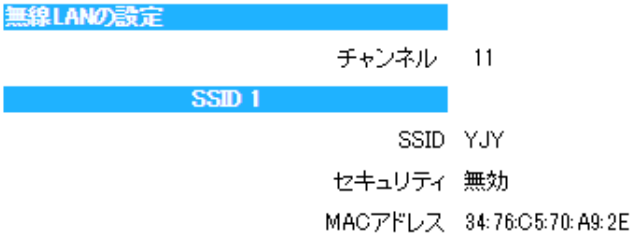

図 3.6: MAC アドレスのページ、変更は出来ない

```
dot11 ssid YJYtest
   authentication open
   guest-mode
```

図 3.7: Cisco のアクセスポイントの認証方式の設定

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid YJYtest
 !
 channel 2447
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
```

図 3.8: Cisco のアクセスポイントのチャンネル設定

```
interface BVI1
 ip address 192.168.99.1 255.255.255.0
 no ip route-cache
```

図 3.9: Cisco のアクセスポイントの IP アドレス設定

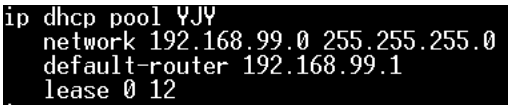

図 3.10: Cisco のアクセスポイントの DHCP 設定

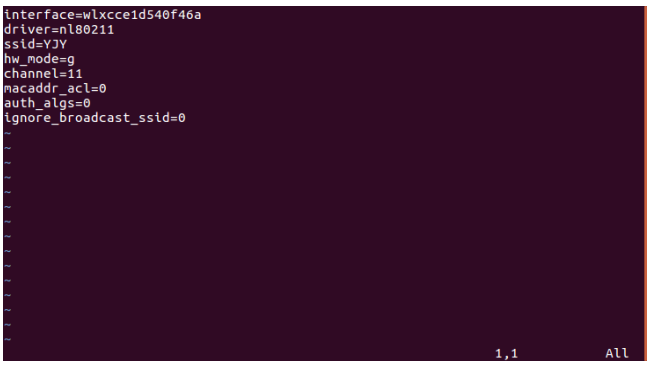

図 3.11: HOSTAPD における設定ファイル

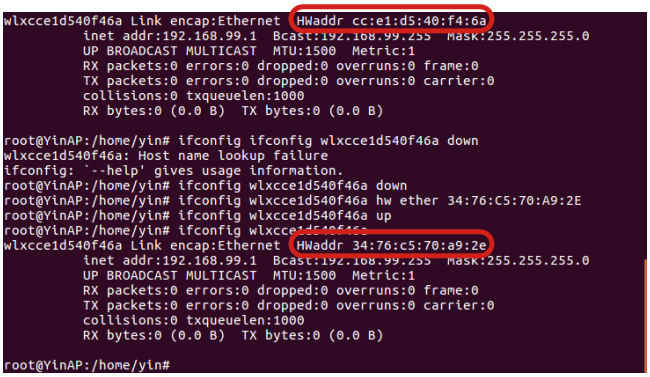

図 3.12: 偽アクセスポイントの MAC アドレス変更例

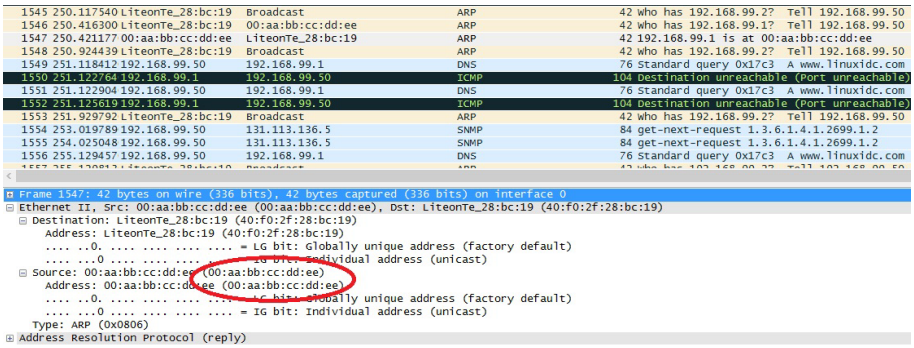

図 3.13: MAC アドレスを偽造した偽アクセスポイントとの通信パケット

3.4. 自動接続の脆弱性

自動接続について 5 ページで述べたが、端末が無線 LAN に接続を行う時、セキュリティを含めたステータスが過去に接続したものと一致している場合、ユーザには通知せずに接続する。接続したことがある無線 LAN について、Windows 8.1 では図 3.12 に示しているように表示させることができる。これは実用性を考えた上で、合理的な仕組みになっている。

無線 LAN では短時間の断線と再接続はごく普通な状況として考えられる。また、複数のアクセスポイントが設置されている場合、アクセスポイントの切り替え時には、断線と再接続を行う。端末が一々ユーザに指示を仰いだ場合、無線 LAN の利便性に大きな影響を与えることになる。

しかし、これが原因でセキュリティ上の問題も発生する。端末が偽の無線 LAN アクセスポイントに自動接続する時も、ユーザには通知しない。利用している無線 LAN の ESSID や BSSID を注意すれば良いが、いちいちそこに注意すると、無線 LAN の利用が不便になる。

図 3.14: Windows8.1 の無線 LAN 記録リスト

また、携帯端末において、無線 LAN はデータ通信より優先度を高く設定することが多い。何故なら、無線 LAN はほぼ無料で利用できるが、データ通信は比較的に高い料金が必要である。ユーザが無線 LAN 機能を消し忘れた場合、携帯端末は

利用できる無線 LAN を発見した時には自動で接続し、利用中のデータ通信を無線 LAN に切り替える。この場合は無線 LAN のマークが携帯端末の上に表示されるだけで、ユーザに分かりやすい通知は行わないことが多い。重要なデータをやり取りしている最中に怪しい無線 LAN に切り替わった場合、情報が盗まれる可能性がある。

3.5. 無線 LAN に対する攻撃の危険性

無線 LAN の攻撃で、一番危険なのは情報漏洩である。攻撃者はセキュリティが不完全な場合、正規端末に対して個人情報を盗み、場合によってはウィルスに感染させることも可能である。ウィルスに感染された端末は、重要なデータを盗むバックドアになり、悪事の踏み台にされる恐れがある。

3.6. 本章のまとめ

無線 LAN の脆弱性が生まれる原因は二つある。一つは無線 LAN 自身の仕組みがまだ未熟なことである。無線 LAN はその利便性を持って、迅速に発展したが、それと共に深刻になっているセキュリティ問題はすぐに解決されなかった。仕組み上、有線 LAN と比べて、無線 LAN の通信には、より強固な暗号化と双方向の認証が必要である。現在使われているセキュリティプロトコルも何時までも安全であるとは考えられない。

もう一つは無線 LAN を使う人のセキュリティ意識が不十分なことである。セキュリティ問題に一番重要なのはユーザである。ユーザにセキュリティの意識がなければ何も守ることはできない。

第4章
偽無線LANアクセスポイントの検出

無線LANは電波による通信を行っており、電波には有効範囲がある。電波の発信源から離れるほど、電波強度は弱くなる。端末は同じ無線LANの中で二つのアクセスポイントが出した電波の中、電波強度が強い方を優先的に接続する仕組みになる。そこで確認の為、切り替える動作実験を行った。L字の廊下の中に、二つの同じESSIDのアクセスポイントを設置する（図4.1）。先ずはポイント1でMACアドレスが00:25:45:22:a7:6cのアクセスポイントに接続する。そして、ポイント1からポイント2に移動する。この時信号はだんだん弱くなったが、端末は別のアクセスポイント（MACアドレスが00:26:0b:62:b2:02のアクセスポイント）には切り替わらなかった。ポイント3まで行くと、最初のアクセスポイントの電波が極めて衰弱になり、端末が自動で回線を切って、電波が強い二つ目のアクセスポイントに切り替えた。この実験により、正規無線アクセスポイントと偽無線LANアクセスポイントの物理的な位置関係により、攻撃を防ぐ方法は変わることが分かった。本章では偽無線LANアクセスポイントと正規無線LANアクセスポイントの位置関係について分析し、その対策を検討する。

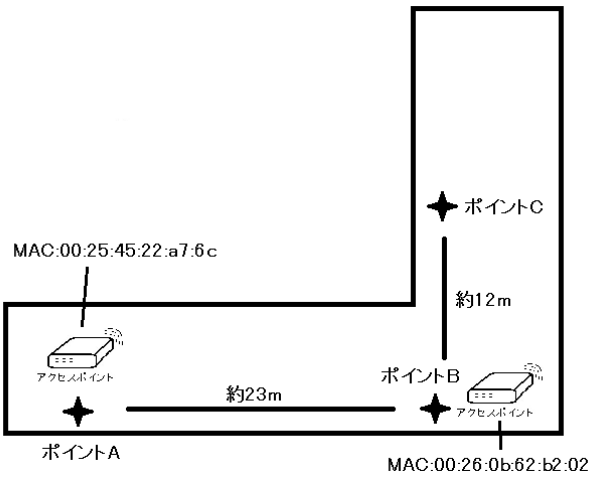

図 4.1: とある廊下で無線 LAN 接続テスト平面図

4.1. 位置情報との関係

無線 LAN の接続は、位置情報と大きく関わっている。本研究では正規無線 LAN の受信範囲と偽無線 LAN アクセスポイントの位置関係を三つの状況に分けて、一つ一つ分析する。その中で本研究の対象である場合の偽無線 LAN アクセスポイントの検出方法を議論する。三つの位置関係は以下となる。

- 偽無線 LAN が正規無線 LAN の受信範囲内の場合
- 偽無線 LAN が正規無線 LAN のアクセスポイント受信範囲外近傍の場合
- 偽無線 LAN が正規無線 LAN の受信範囲外近傍ではない場合

4.1.1 偽無線 LAN が正規無線 LAN の受信範囲内の場合

本研究は、正規無線 LAN の範囲内で偽無線 LAN が存在している場合を検証する為に、実際に環境を作って、テストを行った。その結果、正規無線 LAN と完全に一致している偽無線 LAN の存在が正規無線 LAN の通信を妨害することが確認できた。この結果を踏まえ、無線 LAN の通信とハンドシェイクについて調査を行った。[12]。そして端末は、両方のアクセスポイントが正規アクセスポイントで

あった場合、両方の認証パケットを同時に受け取り、認証を行ったのである。片方の認証は通り、もう一方の認証はハンドシェイク時のIVが違うため、再認証のパケットを提示する。端末は、二つの無線LANの認証を振り返り、永遠に繋がることはない（図4.2)。もし偽無線LANのステータスが正規無線LANのステータスと完全に一致していない場合、記録された正規無線LANのステータスと比べれば偽無線LANを検出できる。この点については、”EvilAP Defender-master”などオープンソフトがすでにgithub上共有されている [13]。

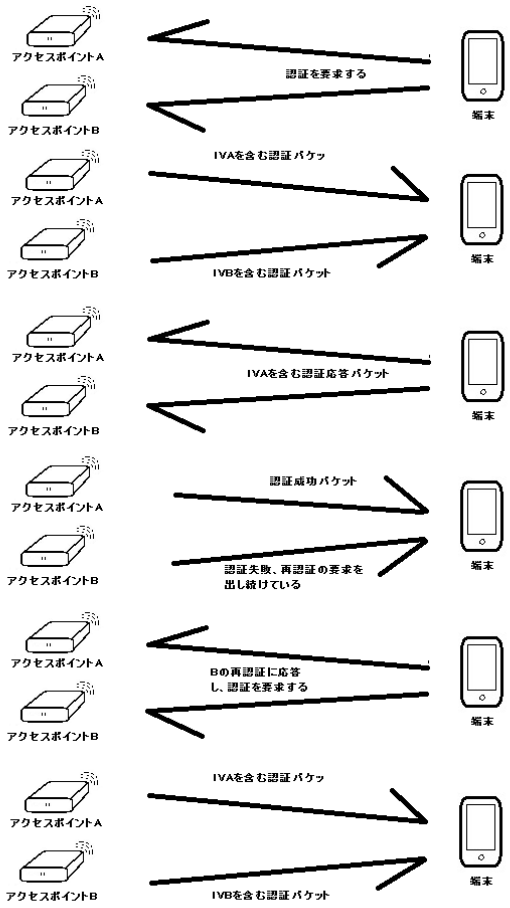

図 4.2: IVの違いによる認証の振り返す

4.1.2 偽無線LANが正規無線LANのアクセスポイント受信範囲外外近傍の場合

アクセスポイントの個体差を除いて、正規範囲近傍は一番判断し難いである（図4.3）。この範囲では、正規無線LANの電波が極めて弱くなっていくにも関わらず、端末はそれを認識出来て、通信を切断しない。この場合、もし偽無線LANアクセスポイントが立ち上がって、正規無線LANの電波より遥かに強い電波を出すと、端末はそれに接続する。この範囲は、正規無線LANにとって決して怪しい範囲でないが、偽無線LANにとって絶好な場所である。本研究でこの範囲内の偽アクセスポイントの特定は困難である。

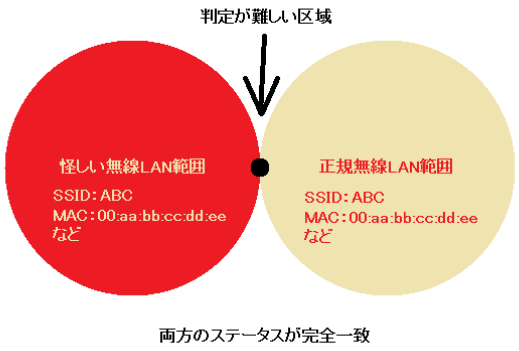

図 4.3: 正規無線LANの近傍で判定困難の区域

4.1.3 偽無線LANが正規無線LANの受信範囲近傍ではない場合

正規無線LAN受信範囲近傍ではない場合、正規無線LANの電波は既に届かないと判断する。そこで同じ無線LANが発見された場合、怪しい無線LANと判断してもよい。本研究では、この種の正規無線LANと離れている偽無線LANを位置情報で判断し、それを検出し、端末が接続しないようにする方法について研究を行う。

4.2. 検出可能な方法

偽無線LANの検出については、幾つかの方法が存在している。

- ステータス検知による偽無線の検出
- 証明書によるアクセスポイントの認証
- 周辺の電波情報による無線LANの判別
- IPアドレス検証して無線LANの区別
- 位置情報による無線LANの特定

4.2.1 ステータス検知による偽無線の検出

既存方法として、ステータス検知による検出が多く利用されており、EvilAP Defenderの様なソフトウェアも簡単に入手できる。通常偽無線LANアクセスポイントは正規無線LANアクセスポイントと比べ、ステータスの違いは以下となる。

- BSSIDが違う
- BSSIDが同じが、チャンネル、認証方式などが違う
- BSSID、チャンネル、認証方式など同じが、ビーコンに含まれている情報が違う

これらのステータスを正規無線LANに接続する時に記録し、再接続時は記録と比べ、無線LANアクセスポイントの真偽を判断する。しかし、無線LANのステータスは何らかの方法で偽造可能である。ステータスが正規無線LANアクセスポイントと完全一致であると、偽無線LANアクセスポイントの検出は不可能である。

4.2.2 証明書によるアクセスポイントの認証

現在、証明書が一番使われているのはウェブサイトである。特に商業用ウェブサイトは証明書を使用し、偽造されないようにしている。本研究において、ウェブサイトのように、アクセスポイントごとに証明書を発行し、そのアクセスポイントを認証することが望ましい（図 4.4）。

しかし、アクセスポイントは現在認証されていない。そのため、既存のプロトコルは通用しない。アクセスポイントに証明書を発行するには、ベンダと交流し、アクセスポイントのシステムを変更する必要がある。その上、現在広く使われている無線 LAN プロトコルを改訂しなければならない。つまり、アクセスポイントの証明書を実装するためのコストは非常に高い。

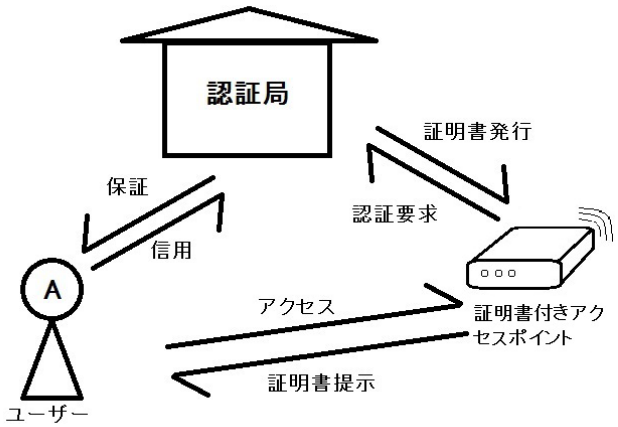

図 4.4: 証明書付きアクセスポイントの認証

4.2.3 周辺の電波情報による無線 LAN の判別

周辺の電波情報とは、そのアクセスポイントの受信範囲の中で共存している他の電波の情報である（図 4.5）。通常、同じ場所に対して同時に受信できる電波は予想できる。携帯端末において、同時に受信できる電波の基地局情報により位置を特定できる。アクセスポイントにも幾つか常に周辺に存在している電波がある。

これに基づいて、アクセスポイントの真偽を検証する。しかし、基地局情報と違い、アクセスポイント周辺の電波情報は変動しやすい。これにより、周辺の電波情報の信用性が低くなる、検証や検出には向いていない。判別の参考になるが、根拠にはならない。

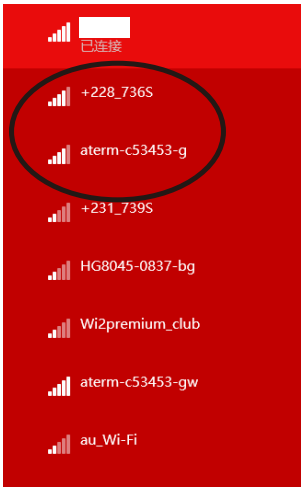

図 4.5: 周辺無線 LAN の情報例

4.2.4 IP アドレス検証して無線 LAN の区別

DHCP 機能により、無線 LAN から受け取ることができる IP アドレスは一定の範囲である。その無線 LAN からいつもと違う IP アドレスを受け取ると、怪しい無線 LAN と判断することができる。また、その無線 LAN の範囲の中、プリンタなど常に存在している機械の偽造は非常に繁雑である。その為、偽無線 LAN でそれらの機械にアクセス出来ない時点で、偽無線 LAN であると考えられる。しかし、接続毎に、無線 LAN にある機械を確認する機能はなく、その上それらの機械が故障により停止する時もあるため、確実な検証手段であるとは言えない。

4.2.5 物理的な位置情報による無線LANの特定

物理的な位置情報は、9ページにより、緯度と経度が含まれている。この情報は、二次元地図上にある一点に対して唯一の情報である。しかし、現実は三次元であり、標高と言う数値が存在している。同じビルの中、違う高さで正規無線LANと偽無線LANが存在していると、位置情報による分別は可能が、通常より難易度が遥かに高い。そのため、本研究において上記で記述したことは、特例として扱い、個別で対応する。この特例以外の場合、正規無線LANアクセスポイントが盗難、すり替え、破壊されない限り、無線LANアクセスポイントの物理的な位置情報でそのアクセスポイントを特定できる。また、そのアクセスポイントの正規な電波範囲も割り出す。同時に、端末の物理的な位置情報をGPSなどから得ることで、端末が正規な無線LANの受信範囲にあるかどうかを判断できる。

4.3. 現存の対策

偽無線LANアクセスポイントの検出問題は既に長い間問題視されていた。この問題は完璧に解決されていないが、幾つかの解決策が考えられている。

- 一つ目に電子情報通信学会による無線LANアクセスポイントやネットワークの情報を収集し、その情報を検証することで、不正なアクセスポイントを判定する手法 [14] がある。ステータス検知は一番使われている方法であるが、ステータスの偽造など問題があるので、本研究では採用しない。

- 二つ目にCisco Wireless LAN Controller(WLC)の自動電波調整機能がある。WLCにより、不正なアクセスポイントの電波干渉を自動的に回避でき、不正アクセスポイントも検知できる。さらにClean Airがあればサイトマップで干渉源や無線デバイスの位置検知と外部電波の干渉状態の可視化まで可能になる [15]。Cisco社独自の技術を使うアクセスポイントなので、普及には向いていない。本研究は無線LANの便利性を生かして偽無線LANの検出を行う研究である。

4.4. 本研究の検出方法

本研究は偽無線LANが正規無線LANの受信範囲近傍ではない場合の、偽無線LANアクセスポイントの検出方法について研究を行う。この場合、周辺電波、IPアドレスなどによる検出方法は突発的な状況の対応能力が低いため、結果の精確性が低い。また、ESSID、BSSID、暗号化方式などのステータスは偽造されやすいので、使用しないこととした。アクセスポイントに証明書を実装することも時間とコストをかかるため、推奨はできない。ゆえに、提案された方法は物理的な位置情報による無線LANの特定である。

この方法では、物理的な位置情報を要求するが、現存する携帯端末は簡単に取得可能である。また、現存のアクセスポイントに対し、特に変動する箇所がない。携帯端末に相応のアプリケーションをインストールするだけで実装は容易にできる。

4.5. 本章のまとめ

端末が正規な無線LANの受信範囲の中、或は周辺70m以内にあるの場合、別の方法で無線LANの真偽を確かめるため、ここでは討論の範囲外となる。端末が正規な無線LANの受信範囲から70m以上離れている場合、物理的な位置情報による偽無線LANの検出は実行の難易度、実行のコスト、情報の信用性など角度から考慮して一番妥当である。この考えを踏まえ、具体的な実行方法やシステムの構築は次章で詳しく述べる。

第5章
システム構築及び実装

前章より、位置情報による偽無線 LAN の検出は信用性があり、実現性が一番高い方法であることがわかった。本章では、位置情報による偽無線 LAN アクセスポイントの検出システムを構築する。しかし、時間や資金の制限によって、現状では完全なシステムを設計が完成しても、実行するには困難である。そのため、完全なシステムを構築した上で、システムの効果とその便利性を核となるシステムのみを実装し評価する。

また、世の中には無線 LAN やアクセスポイントに関する既存システムが多数存在しているため、それらのシステムと本システムの相違性についても述べる。

5.1. システムの仮定

本システムは、幾つかの仮定から構築されたものである。

- 偽無線 LAN アクセスポイントの物理的な位置は正規無線 LAN の周辺から十分遠いところにある。
- 端末の通信は全て認証された VPN を経由しないと同時に本システムだけ認証された VPN サーバでデータを転送する。
- ユーザの端末は GPS などを利用し、正確な位置情報を取れる。

5.2. システムの構築

物理的な位置による偽無線 LAN の検出のシステムは管理者側、サーバ側、端末側三つ構成要素がある（図 5.1）。

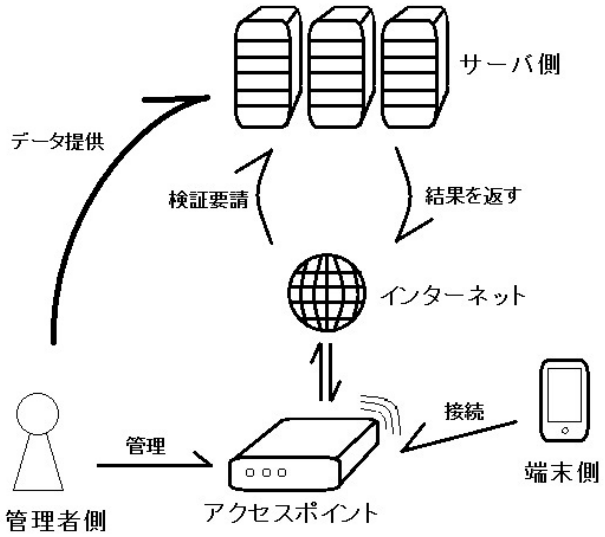

図 5.1: システムの構成図

システムの流れとして、管理者側からサーバ側に正規無線 LAN アクセスポイントのデータを提供し、端末側からサーバ側に向けて、検証要請を出す。そして、サーバ側から結果を受け取り、アクセスポイントの真偽を判断し、アクセスを制御する（図 5.2）。

- 管理者側
  管理者側は正規な無線 LAN とそのアクセスポイントを管理している側のことである。個人あるいは組織のインターネット担当者に当たる。管理者側において、一番重要ことは正しい無線 LAN 情報を安全なルートで提供されることである。具体的な方法について、本章の後で述べる。

- サーバ側
  サーバ側は、システムの中心である。無線 LAN とそのアクセスポイントの情

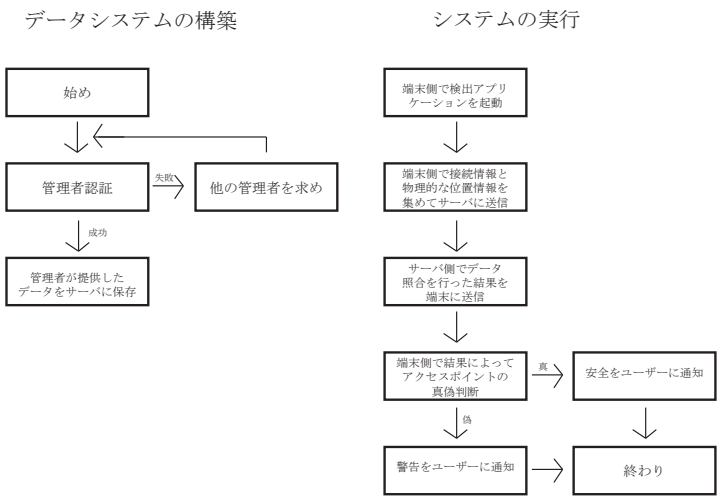

図 5.2: システムの流れ

報をデータとして保存する。データの詳しさによって、システムの精度が変わる。物理的な位置情報で無線 LAN アクセスポイントを特定するには、最小限更新日付、緯度、経度、ESSID 四つの情報が必要とされる。このデータは本システムに対して一番重要なデータである。その中、無線 LAN の ESSID 情報に対して、緯度と経度情報は複数存在可能である。その原因は、違う場所に同じ ESSID の無線 LAN が存在する可能性があるためである。しかし、二次元地図上にある緯度と経度の点に対して、ESSID は一つしかない。よって、データを保存する時、新旧データに緯度と経度の重複を確認しなければならない、表の中の更新日付が 20161204 のデータの緯度と経度は更新日付が 20161201 のデータですでに使われたため、これを発見した場合、古いデータを無効化させ、新しいデータの参考基準となっている（表 5.1）。無効化された古いデータについては本章で後述する。

更新日付、緯度、経度、ESSID 以外、補佐として使われた情報も幾つかある。これらの情報の数が多いほど、システムの精度は上がる。ESSID の違う二つの無線 LAN アクセスポイントが同じビルの中に存在している場合、二次元地図上だけでは特定出来ないため、標高が必要とされる。しかし、標

表 5.1: 基本データの保存例

更新日付	緯度	経度	ESSID
20161201	35.552144	139.647188	kmd-wireless0
20161202	35.713840	139.700940	kmd-wireless1
20161203	35.552100	139.647100	kmd-wireless0
20161204	35.552144	139.647188	kmd-wireless2

高は緯度や経度と比べて測定が困難である。そのため BSSID、IP、併存の ESSID 情報などが参考になる。ただし、これらの情報は不安定であるため、これだけで判断するのは避けるべきである。データを保存する時、使う可能性がある情報もデータベースに入れておくことで、現在では参考にならない情報も、将来には参考する価値が隠されている可能性があるので、その情報を入れる場所を EXTRA 情報として保持する（表 5.2)。

表 5.2: 拡張データの保存例

更新日付	緯度	経度	ESSID
20161201	35.552144	139.647188	kmd-wireless0
BSSID	Gatway	DNS Server	併存 SSID1
00:aa:bb:cc:dd:ee	131.113.136.0	131.113.136.64	keiomobile2
併存 SSID2	EXTRA1	EXTRA2	
sdm			

端末から検証待ちの情報を受け取り、無線 LAN のデータと照合し、結果を端末に返すまでがサーバの役割である。端末側でデータを照合することは安全ではない。端末がウェルスに感染したり、データ転送中に盗聴されたり、データが悪事に利用され兼ねない。しかし、検証待ちの無線 LAN をユーザ自身が作った個人無線 LAN の場合、個人の情報をサーバに転送し、毎回サーバに聞いて検証するのは効率が悪いため、サーバ側ではなく、端末側でユーザ自身入力してもらい検証する方が効率が高いと考えられる。勿論、ユーザ自身が作ったホワイトリストにもセキュリティをかけなければならない。

- 端末側

端末側は、システムがユーザと直接交流を行う部分である。プログラムを工夫して、ユーザの同意を得た前提で、GPS と基地局情報を利用して実際の位置情報と繋いでいる無線 LAN の情報を受け取る。具体的な獲得方法は本章の後で述べる。端末側はユーザの位置情報と無線 LAN 情報をサーバ側に送って認証する。そして、サーバ側から帰ってきた結果をユーザに通知し、無線 LAN の制御をユーザに判断させる（図 5.3）。

5.3. システムの実装

本システムは管理者側、サーバ側、端末側の三か所を実装する。管理者側では各公衆無線 LAN の担当者の情報提供が必要とされる。担当者に認証をかけて、情報の信用性を保つ。現段階では、システムを評価するため、環境構築を含め本研究が管理者側の役目を果たす。サーバ側は、インターネット上証明書付きのサーバを購入し、認証システムとデータ照合システムを実装する。現状では、資金、時間などの原因で、端末側でデータ照合を行う。端末側は現在の無線 LAN をスキャンすることが可能であるため、GPS で位置情報を取得できる機能が付いたアプリケーションを実装する [16]。現在は、サーバ側の認証を含め、入力した無線 LAN アクセスポイントデータと実際繋がっている無線 LAN の情報 [17] を照合し、ユーザに結果または警告を出す Andriod アプリケーションを作った。そして、このアプリケーションを用いて個人無線 LAN の真偽の検出を行う。また、検出を行う時、無線 LAN には受信範囲があるため、正規無線 LAN の範囲は一つだけではない。アクセスポイントの受信範囲は約 25m と経度一秒の差である 31m から計算した。結果、GPS 座標上は約 0.0002 度（十進数）であった。本研究は、正規無線 LAN の範囲を二次元地図上一つの四角を仮定し、その範囲はアクセスポイントの座標から上下 0.0002 度（十進数）に設定した。

先ずは実装環境について説明する。携帯端末には GPS、無線 LAN、基地局情報などの機能がついており、本システムに対して、実装しやす環境である。IOS 端末にアプリケーションを入れるため、様々な手続きが必要なため、小規模な実装には向いていない。そこで、実装は Andriod 端末を選択した。システムバージョ

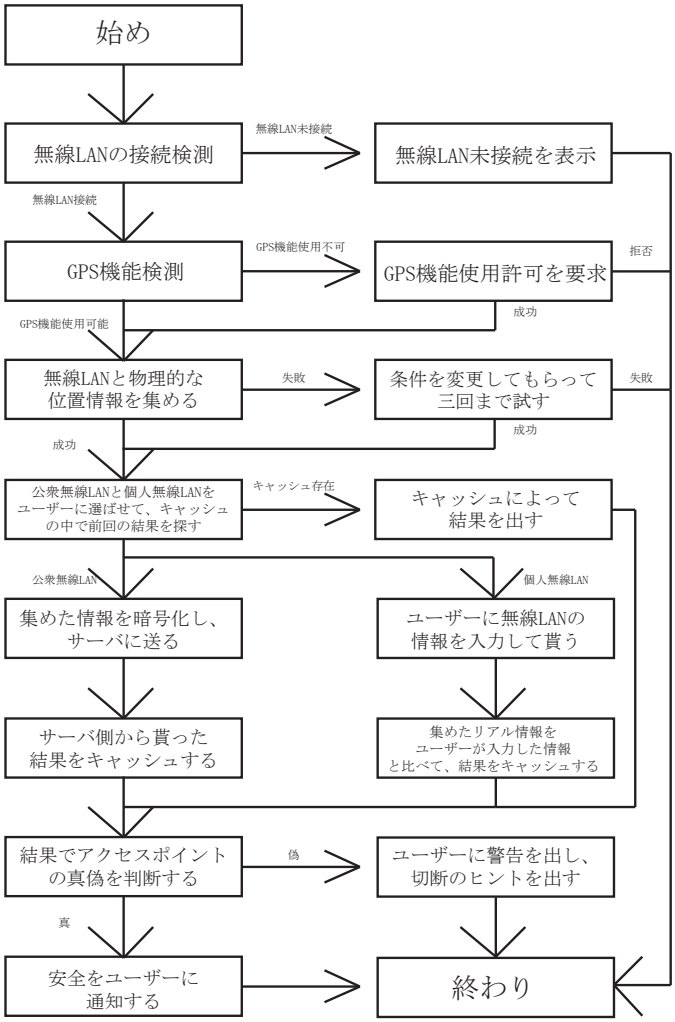
始め
無線LANの接続検測
無線LAN未接続
無線LAN未接続を表示
無線LAN接続
GPS機能検測
GPS機能使用不可
GPS機能使用許可を要求
拒否
成功
GPS機能使用可能
無線LANと物理的な
位置情報を集める
失敗
条件を変更してもらって
三回まで試す
失敗
成功
成功
公衆無線LANと個人無線LANを
ユーザーに選ばせて、キャッシュ
の中で前回の結果を探す
キャッシュ存在
キャッシュによって
結果を出す
公衆無線LAN
個人無線LAN
集めた情報を暗号化し、
サーバに送る
ユーザーに無線LANの
情報を入力して貰う
サーバ側から貰った
結果をキャッシュする
集めたリアル情報を
ユーザーが入力した情報
と比べて、結果をキャッシュする
結果でアクセスポイント
の真偽を判断する
偽
ユーザーに警告を出し、
切断のヒントを出す
真
安全をユーザーに
通知する
終わり

図 5.3: 端末側の流れ

ンは Andriod5.0.2 である。実装用アプリケーションを作る上で、Andriod Studio 2.1.3 を使用した。GPS 利用、偽無線 LAN 照合、無線 LAN 接続制御などの機能を実装した。端末が無線 LAN に接続し、本アプリケーションを起動し、無線 LAN の真偽を判断でする（図 5.4）。

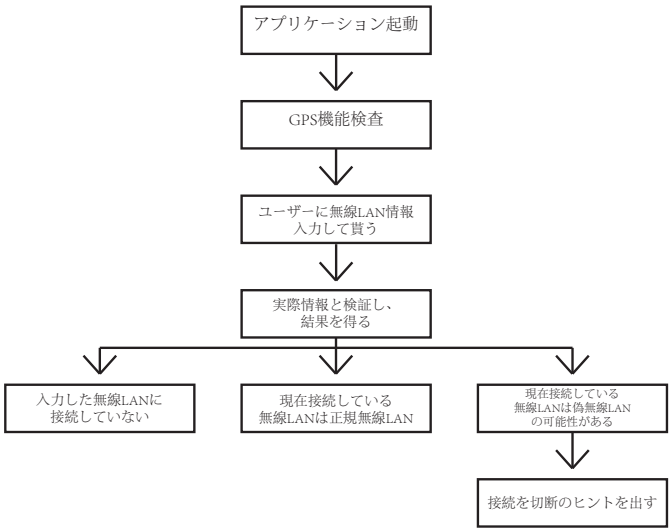

図 5.4: 実装システムの流れ

アプリケーションを起動し、GPS 機能を使用可能にする（図 5.5）。GPS 機能は電力消耗が激しいため、通常は OFF の状態になっているため、本アプリケーションが機能を使用する前に、GPS 機能の確認を行う。

ユーザに無線 LAN の情報を入力する。情報には必須な ESSID、緯度、経度が含まれている（図 5.6）。ここに入力した情報は、本来サーバ側に保存された正規無線 LAN の情報である。個人無線 LAN の場合は、このような形で正規無線 LAN の情報を貰う。

START ボタンを押して、検証を行い結果を得る。結果により、ユーザに相応な報告を出す。

入力した ESSID が違うは場合は画面下方にメッセージが出る（図 5.7）。その後、ユーザは無線 LAN 情報を再入力することができる。

現在接続している無線 LAN が正規無線 LAN の場合も画面下方にメッセージが

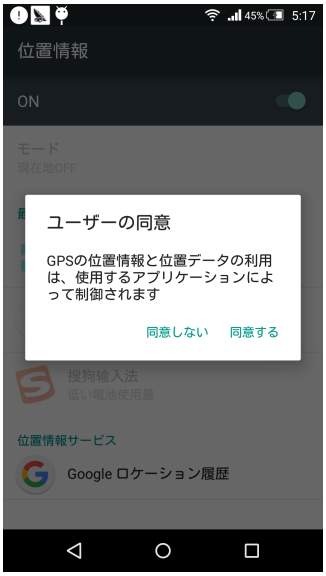

図 5.5: GPS 機能の使用確認

図 5.6: 情報入力画面

図 5.7: ESSID が見当たらない場合

出る（図 5.8）。その後は再検出可能である。

実験中、無線 LAN 受信範囲外に移動するのは不便なため、入力した正規無線 LAN 情報を変更することで、正規無線 LAN の範囲を変更する。これにより、実験端末が正規無線 LAN 範囲内から正規無線 LAN 範囲外に移動した。この時、元々正規無線 LAN として認識された無線 LAN は、怪しい無線 LAN になった（図 5.9）。

この場合、画面下方にメッセージを出す代わりに、ユーザに警告を出す（図 5.10）。この結果は本研究の目的である偽無線 LAN アクセスポイントの検出に対して重要な結果なため、ユーザに目立つな警告を出すことが役割である。また、接続している無線 LAN を遮断するか否かの判断はユーザに任せて選ばせる。

警告によって、無線 LAN の接続を制御する（図 5.11）。ユーザが「接続を遮断する」を選択した場合、携帯端末の無線 LAN 機能を OFF 状態にする。

5.4. システムの評価

本システムの実装結果により、位置情報で偽無線 LAN 判別の適合性と利便性が示された。

図 5.8: 安全な無線 LAN と判定された場合

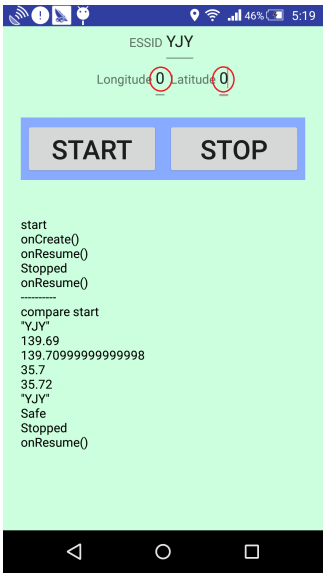

図 5.9: 入力情報を変更

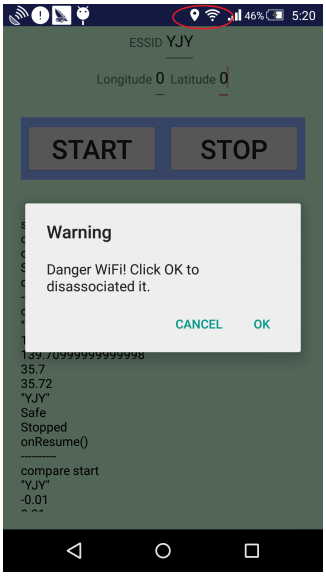

図 5.10: ユーザに警告と選択

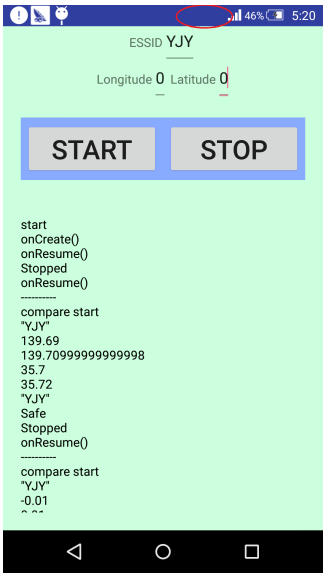

図 5.11: 無線 LAN 機能を OFF 状態にさせる

本実装は、Andriod システム上偽無線 LAN アクセスポイントの検出システムの核となる部分を実現した。位置情報は Android のシステムコールで取得し、ユーザのデータと照合した。インターネットとサーバを利用していないため、GPS のデータを取り次第、1 分以内で照合することが可能である。室外や窓口など GPS 情報を取得しやすい環境では、効率的な効果を発揮できる。

5.4.1 実装の適合性

本実装は、照合結果によりユーザへの通知が変わる。結果が安全な無線 LAN の場合、ユーザに Safe を表示する以外、無線 LAN への変更は行わない。結果が判定困難な無線 LAN か偽無線 LAN の場合は、ユーザに警告を出して、Android のシステムコールで接続している無線 LAN を切断させるか否かをユーザに洗濯してもらう。

5.4.2 実装の利便性

ユーザは、端末側のアプリケーションをインストールするだけで本システムを利用でき、自分でホワイトリストを管理することも可能である。個人や団体はグループ内専用の正規無線 LAN アクセスポイントのデータベースを作り、グループに対して悪意がある偽無線 LAN アクセスポイントの検出システムを簡単に実装できる。また、データベースを事前に用意できれば、通信端末を持っている取引相手や一般人に、アプリケーションを配るだけで、偽無線 LAN アクセスポイントの検出が可能である。例えば、客にグループ内の無線 LAN アクセスポイントを検出できるアプリケーションを配れば、客がその無線 LAN を利用する時のセキュリティが高まる。

5.5. 完全なシステムについて

本研究は現在、システムの核となる部分を実装したが、完全なシステムは時間や資金などが要因となり、実装しなかった。完全なシステムを実装する場合、先

ずは管理者から正規アクセスポイントのデータを集める。一定な量か一定範囲のデータを集まれば、ユーザにサービスを提供できる。ユーザは端末を用いて、検出アプリケーションをインストールし、繋がっている無線LANの真偽を検出できる。時間の経過と共に、サーバ側のデータ量が増えることになるが、古いデータの処理によって、一つの物理的な位置情報は五つまでデータが存在することになる。同じ容量のサーバでは、一つのデータの量が大きくないため、位置情報の数は有効的に増やすことが出来る。

しかし、完璧なシステムを実装することは容易ではない。端末機種によって、取れる情報と取れない情報がある。その場合はシステムに合わせて個別対応を行うしかない。また、管理者側で担当者の本人認証について、協力を貰えない場合もあり、全ての公衆無線LANの情報を取得することはほぼ不可能である。それと同時に、偽情報を識別する能力も必要とされる。サーバ側では、サーバのデータ容量の大きさや、サーバのセキュリティも考慮しなければならない。何より重要なのは、サーバとの通信時、情報の受け渡しは安全であるかを確認すること。端末側として、現在の機能の上に、基地局情報や周囲の無線LAN情報も位置情報を取得する際の参考として使いたい。また、悪意を持つ人が端末のアプリケーションを改竄して、偽情報を出すことなども防ぐ必要がある。

5.5.1 管理者側から無線LANの正しい情報を取る方法

無線LANの正しい情報は管理者側から取得することが一番妥当だと考える。よって、管理者が本物であれば、この無線LANの情報が正しいといえる。つまり、管理者を認証するシステムが要求される。

管理者の認証は個人の身分証明と繋がる。通常は一人ひとりにIDとパスワードを発行し、データの更新時、そのIDとパスワードを照合することにより、データを更新した人物が本人であることを証明できる。本システムでは、IDとパスワードの代わりに管理者毎にデジタル署名を発行する。管理者がサーバにデータを更新する際、その人専用のデジタル署名がないと、そのデータを本人に認めない。同時に、管理者もサーバの証明書を検証し、サーバを認証する（図5.12）。もちろん、本物の管理者が嘘をつかないことを信じることも重要である。無線LANのセ

キュリティの為に、管理者の協力は欠かせないものである。

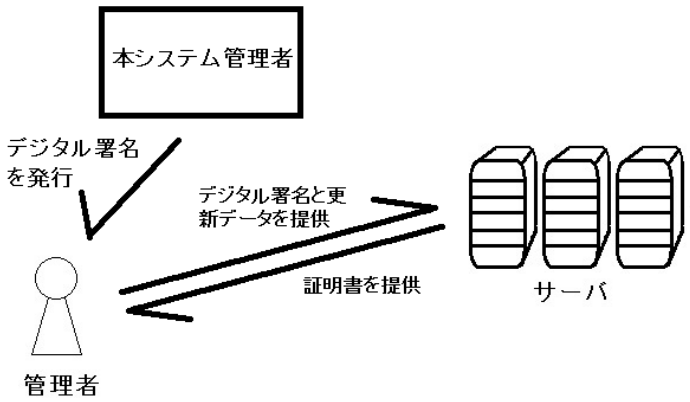

図 5.12: 管理者とサーバの双方認証

5.5.2 データを管理する方法

セキュリティのレベルを高めるためには、サーバのデータを常に更新しなければならない。その頻度は約一ヶ月一回である。データの更新は更新日付によって、自動管理する。緯度と経度が一致するデータは日付が新しい方が古い方を更新する。一ヶ月以上更新されていないデータは管理者に知らせ、更新を催促する。

更新されたデータは古いデータと呼び、古いデータを無効化するだけで、古いデータ自体は削除されない。もし、新しいデータが間違っている場合、何時でも一つ前の古いデータに戻すことが出来る。しかし、一つ前の古いデータも間違っている可能性があるため、一番新しいデータから、三つ前の古いデータまで全部を無効化して保存するのが安全である。これで一つの物理的な位置情報に対して、アクセスポイントのデータは少なくとも四つになる。サーバの容量を考慮すると、それ以外の古いデータは削除しても良い。

また、個人無線 LAN のデータはユーザ自身で設定するので、ユーザが再設定で

きるようにデータを管理すれば、古いデータを残す必要がないと考える。携帯端末の容量がサーバより遥かに少ないため、データが少ない程使いやすい。

5.5.3 端末側で位置情報を取る方法

位置情報を取得するのは、端末が現在の位置情報を取ることである。この情報を得るためには、幾つかのルートがある。そして、一番よく使われているのはGPSである。本研究もGPSを位置情報を取る基本ルートとして使うが、GPSだけで位置情報を取るには、幾つかの欠点が存在している。まず初めに、GPSが起動してから位置情報を取るまでに時間がかかる。数分〜数十分という少々長い時間が要求されることはユーザ体験にとって決してよろしいとは言えない。また、GPSは衛星の電波を拾って分析して位置情報を割り出すため、室内では誤差が大きいか、そもそも位置情報が取れない場合もある。その為、GPSだけで物理的な位置情報を取るのは好ましくない。これを改善するために、GPSを利用した上で、基地局情報と無線LANを併用させることが一番効率が良い。携帯端末では、一般的にGPSと基地局情報などを併用する機能が付いているため、実現することは難しくない。本研究では、周囲の無線LAN情報を集める必要があるため、特定の無線LANの物理的な位置情報を検証する時、周囲の無線LAN情報も補佐として使えると信用性が高くなると考える。

5.5.4 端末側とサーバ側の間セキュアな情報転送方法

セキュアな情報転送方法は本研究において必要不可欠である。繋がっている無線LANを検証する時は、既に危険なネットワークの中にいる可能性がある。そのため、端末とサーバの間の通信は、HTTPSを用いて、認証されたVPNサーバを経由する必要がある。また、サーバのアドレスが偽無線LANアクセスポイントによって偽造されて、偽サーバに繋がる可能性があるため、サーバ側の証明書を検証する必要がある。

サーバ側から受け取った問い合わせ結果はキャッシュとして保存するため、通信時の結果キャッシュの真偽を確かめなけらばならない。結果キャッシュが改竄

されないため、問い合わせごとにランダムで 32 ビットの番号を割り当て、結果のキャッシュを読み込む前に照合する。この番号は結果キャッシュの暗号化に利用するため、通信途中にパケットを覗いても、シリアル番号が分からない限り、結果キャッシュの偽造は出来ない（図 5.13）。

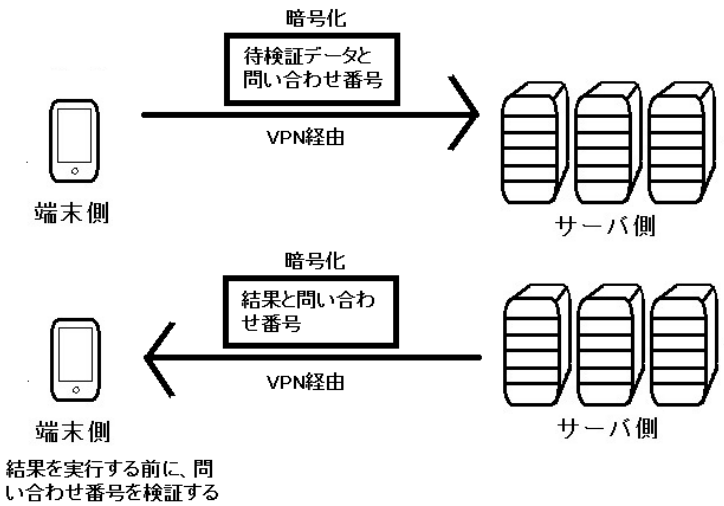

図 5.13: セキュアな問い合わせ方法

また、問い合わせのサーバは一つとは限らない場合がある。その場合は、端末から取れた位置情報で一番近いサーバを選択し、通信と認証を行う。サーバの位置情報は特定のサーバで管理し、その特定のサーバを最初の問い合わせサーバにする。

5.6. 既存の無線 LAN サービスとの相違性

世の中には、公衆無線 LAN 関係のサービスやアプリケーションが多く存在している。その中に、無線 LAN アクセスポイントの情報を集めているサービスがある。

- Wigle
  Wigle は世界的な無線 LAN アクセスポイント情報を集めるウェブサイトで

ある。そのデータベースの中は、位置情報と無線 LAN のステータスを繋ぎ、世の中の人に無線 LAN の情報を提供している。その提供者はユーザであり、使用者もユーザである。ユーザは Wigle を使い、無料で公衆無線 LAN の情報を探して利用できる。このサービスは本研究と相違性を持っている。一つ目は、Wigle の無線 LAN 情報量が多いが、信頼性が欠けている。ユーザから提供された情報は、管理者を通して確認せず、管理者に知らされていない状態で公開されている偽物の情報の可能性がある。二つ目は、ユーザが他人の無線 LAN を勝手に使う為に Wigle を利用している。これはセキュリティ上決して良くない状態である。本研究は情報を守るために無線 LAN の情報を集め、セキュリティを高める研究であり、無線 LAN を使う時に、もっと安全に使うことに着目している。その為、アプリケーション一つで簡単に、セキュリティ問題の解決に尽力している。

- EvilAP Defender-master
  このソフトは Evil Twins Attack の対策として、前文ですでに述べた。EvilAP Defender-master は接続したことがある無線 LAN のステータスを記録し、二回目に接続する時、新たに受け取ったステータスを一回目に記録したステータスと比べ、変更されたかどうかを判断する。この方法で、完全に同じ無線 LAN を区別することは不可能である。前章から、偽無線 LAN アクセスポイントが正規無線 LAN の範囲内の場合、完全一致のステータスが通信妨害を誘発するため、偽無線 LAN を見つけやすい。この場合、EvilAP Defender-master を利用する方が精度が高い。本研究は、物理的な位置情報を利用して、無線 LAN アクセスポイントを特定する方法を実装したので、EvilAP Defender-master とは完全に別のツールであると言える。

第6章
結　　論

本研究は、位置情報による偽無線 LAN アクセスポイントの検出である。無線 LAN のセキュリティ問題及び、偽無線 LAN による脆弱性について述べてきた。幾つかの偽無線 LAN の検出方法を研究し、その中で信用性かつ利便性が高い物理的な位置情報による検出方法を採用した。

6.1. 総括

本研究は、無線 LAN のセキュリティ問題の中で、偽無線 LAN アクセスポイントが正規無線 LAN アクセスポイント範囲周辺から離れている場合の検出方法について、位置情報による検出方法を採用し、そのシステムを構築した。様々な制限により、システムの完全な実装までは至らなかったものの、核となるシステムを実装し、物理的な位置情報による偽無線 LAN アクセスポイント検出の適合性と利便性を示した。

本研究は個人、組織の無線 LAN セキュリティに一定の補助効果を認める。また数多くの無線 LAN のデータをサーバ側に保存すると、HTTPS 通信により、広範囲の無線 LAN アクセスポイント検出システムが実装できる。組織全体の無線 LAN アクセスポイントのデータベースを作ることで、セキュアな公衆無線 LAN を簡単に提供できる。喫茶店、ホテルなど無線 LAN サービス提供側として、より安全な公衆無線 LAN サービスも簡単に提供できる。通信情報を守ることで、個人情報やプライバシの流出を避けることとが可能である。これにより、生活の質を上昇させる。

今まで本研究に関する内容は少ない。その原因を以下に示す。

- 無線 LAN の問題が多く存在する
  無線 LAN の歴史は長くない。その利便性と突拍子な発展に人々は驚いた。しかし、無線 LAN のセキュリティ強化はその発展の速さに追いついていないのが現状である。その為、無線 LAN のセキュリティ問題は未だ数多く存在している。この偽無線 LAN アクセスポイントの問題について、心配している人は多いが、システム構築まではまだあまり行われていない。このようなことが原因で、関連する研究が少ないのである。

- 携帯端末の普及
  携帯端末の普及は無線 LAN の発展に劣らない速さである。携帯端末の場合、無線 LAN と自動接続機能はコンピュータ端末より多く利用されている。また、携帯端末では料金などが原因で、無線 LAN がデータ通信よりも優先されている。その分、危険性も増し、携帯の普及率が高くなった今、偽無線 LAN アクセスポイントの問題を重視すべき時である。

6.2. 未来への展望

本研究は偽無線 LAN が正規無線 LAN の範囲周辺から離れている場合を研究対象として、その偽無線 LAN アクセスポイントの検出システムを設計し、一部を実装した。正規範囲の偽無線 LAN アクセスポイントの検出は一番困難であるため、物理的な位置情報を使った場合の、精度誤差が 1m 以内の物理的な位置情報を取れる手段が欲しい。現状では、物理的な位置情報を取る手段として、GPS などが使われているが、GPS には室内で物理的な位置情報を取り難い欠点がある。本システムのように、無線 LAN を利用せず、どこでも位置情報を取る手段が好ましい。また、二次元地図上で同じ点の存在する二つの正規無線 LAN アクセスポイント、つまり、高低差 70m 以上離れている二つの正規無線 LAN アクセスポイントででは、もっと簡単な区別方法が必要である。現在は、GPS だけで標高を取っているが、アメリカの都合で誤差が生じる。その為、標高値の信用性が高くないと判断する。標高を測量する為一番の計測方法は気圧である。しかし、現在のスマホ端末に気圧を測定するセンサはほとんどついていないため、スマホ端末だけで標高

を正確に取る手段はない。もし将来でスマホ端末に気圧センサが付けられるまらば、もっと精確に無線 LAN アクセスポイントを検出できるはずである。

情報転送のセキュリティについては、暗号化されたものの怪しい無線 LAN を使用し、データ転送時の妨害を受ける可能性が存在している。本システムとして、怪しい無線 LAN を利用せずに、安全な通信ルートを要求している。しかし、スマホ端末はデータ通信に利用された別の電波が使っているが、現在の仕組み上、無線 LAN を接続している状態で、データ通信のみでデータを転送することは不可能である。無線 LAN が接続中、データ通信も使えるスマホ端末が今後の将来性としてはふさわしい。これが実現された場合、怪しい無線 LAN を通らなくても、その無線 LAN の真偽を検出することができる。

また、物理的な位置情報以外の検出方法として、IP アドレスや MAC アドレス、或は専用のステータスによる検出とアクセスポイントに証明書を発行する検出は望ましい。しかし、これらの検出にはアクセスポイントを認証できるフレームワークの標準化と導入が必要とされる。第 4 章で述べた通りに、フレームワークの変更は容易にできることではないため、これからの無線 LAN セキュリティ問題の検討の最中、この様なフレームワークの標準化と導入が議論される。新しいフレームワークが構築可能であれば、偽無線 LAN アクセスポイントの検出の効率はさらに高まる。

謝　　辞

筆者は留学生として、慶應義塾大学大学院メディアデザイン研究科で二年の時間に渡り研究し、本論文を作成しました。ここで、この二年間私の学業に協力してくれた人たちに心からの感謝を申し上げます。

先ずは、本研究の主指導教員であり、慶應義塾大学大学院メディアデザイン研究科の加藤朗教授に深謝の意を表します。加藤朗教授から幅広い知見から的確な指導をして頂きました。留学生として、日本の論文の書き方がよく分からず、深く悩みましたが、加藤朗教授の親切な指摘によって何とか困難を乗り越えることができました。

また本研究の副指導教員であり、慶應義塾大学大学院メディアデザイン研究科の砂原秀樹教授に心から感謝いたします。砂原秀樹教授から専門的な見解と確実な意見を多く頂き、本研究にとって一つの大きな力になりました。

本研究の副査であり、研究に関して助言をいただいた慶應義塾大学大学院メディアデザイン研究科の石戸奈々子副教授に感謝の意を表します。

また、研究のインスパイアを与えてくれた同プロジェクトの橋本真太郎先輩に謝意を申し上げます。研究分野に関する様々な情報を与えてくれたメディアデザイン研究科の林達也さんに謝意を申し上げます。

最後、筆者の学業に資金援助をしてくれた「公益信託 大槻記念アジア ー アフリカ留学生奨学基金」に深く感謝を申し上げます。

参 考 文 献

[1] 総務省. 平成 27 年通信利用動向調査の結果, 2016.7.22.

[2] 総務省. 公衆無線 lan の整備の促進. http://www.soumu.go.jp/menu_seisaku/ictseisaku/public_wi-fi/, 2014.8.

[3] Wikipedia. 無線 lan. https://ja.wikipedia.org/wiki/無線 LAN, 2016.9.28.

[4] e Words. Essid. http://e-words.jp/w/ESSID.html, 2003.6.18.

[5] Wikipedia. Bssid. https://ja.wikipedia.org/wiki/BSS-ID, 2016.3.9.

[6] Wikipedia. Wep. https://ja.wikipedia.org/wiki/Wired_Equivalent_Privacy, 2016.5.9.

[7] Andrei Popov. *Prohibiting RC4 Cipher Suites*.

[8] Frank Piessens Mathy Vanhoef. Rc4 nomore. http://www.rc4nomore.com.

[9] Wikipedia. Wpa. https://ja.wikipedia.org/wiki/Wi-Fi_Protected_Access, 2015.10.3.

[10] Wikipedia. 初期化ベクトル. https://ja.wikipedia.org/wiki/初期化ベクトル, 2015.10.31.

[11] mister x. Aircrack-ng. https://www.aircrack-ng.org/doku.php?id=Main, 2016.11.30.

[12] William A. Arbaugh Jon Edney. 無線 LAN セキュリティ : 次世代技術 IEEE 802.11i と WPA の実際. 構造計画研究所, 2006.

[13] Moshe Kaplan. Evilap defender. https://github.com/moha99sa/EvilAP_Defender/wiki, 2016.6.16.

[14] 保要隆明, 金井敦. 無線 lan 不正アクセスポイント判定手法の検討. 電子情報通信学会技術研究報告, Vol. 115, No. 334, 2015.

[15] 藤重雄喜. Cisco 無線 lan コラム第 2 回 : 不正アクセスポイントによる無線 lan 環境への影響をどのように防ぐか.

[16] Android アプリ開発. [android] gps で位置情報を取得するアプリを作る. https://akira-watson.com/android/gps.html, 2016.12.13.

[17] Andriod Developers. Wifiinfo. https://developer.android.com/reference/android/net/wifi/WifiInfo.html.

付　　録

A. Aircrack-ngのコマンド

- ネットワークアダプタをモニターモードに変更する
  $airmon-ng start wlan0
- モニタモードのテストを兼ねて近くの無線LAN情報を見る
  $airodump-ng mon0
- 特定のBSSIDの無線LANパケットをivsファイルに保存する
  $airodump-ng –ivs -w filename –bssid BSSID mon0
- 　さっき保存したivsファイルを解析してパスワードを入手する
  $aircrack-ng filename.ivs

B. 偽無線LANの設定

- ソフトウェアを使う場合
  設定ファイル：/etc/hostapd/hostapd.confにSSID、認証方式などを編集する
  設定ファイルを設置完了後
  $service hsotapd　 stop
  $hostapd /etc/hostapd/hostapd.conf

- Cisco の AP を使う場合
  console で接続して、コマンドを入力する
  $enable
  ターミナルに入る
  $configure terminal
  DHCP を起動する
  $(config)# service dhcp
  インタフェースの設定に入る
  $(config)# interface dot11
  MAC アドレスを偽造する
  $(config-dot11)# mac-address 00:aa:bb:cc:dd:ee
  チャンネルを設定する
  $(config-dot11)# channel 2462
  IP アドレスを設定する
  $(config-dot11)# ip address 192.168.99.1 255.255.255.0
  SSID を設定する
  $(config-dot11)# ssid YJY
  認証方式を認証無しに設定する
  $(config-ssid)# authentication open
  ブロードキャスタをする
  $(config-ssid)# guest-mode
  インタフェースを起用する
  $(config-dot11)# no shutdown