Wi-Fi偽APにおける利用者の意識調査

木田 伍[1,a)]　木村 悠生[1,b)]　石川 綾人[1,c)]　上原 哲太郎[2,d)]

概要：公共の場における無線 LAN の提供は普及し，多くの情報通信端末利用者が無線 LAN を無意識的もしくは意識的に利用している．総務省のガイドラインでは，公衆無線 LAN に接続する際利用者は，掲示などを確認し，偽のアクセスポイントに接続しないため注意することが必要とされている．しかし，偽のアクセスポイントに接続する契機や，特に注意の必要なタイミングがいつであるかは，必ずしも明らかではない．また総務省のガイドラインでは，公衆無線 LAN の提供者による，偽のアクセスポイントに対する対策は限られており，利用者側での対策が必須であるとしている．そこで本研究では実験的に偽のアクセスポイントを設置し，偽のアクセスポイントへ接続する利用者に関する検証を行った．また，アンケートおよびインタビューを行い，偽のアクセスポイントに接続する契機やアクセスしたタイミング，背景を明らかにし，利用者の意識すべき対策および提供者が新たに実施すべき対策を考察する．

キーワード：Wi-Fi，偽アクセスポイント，利用者行動，セキュリティ

Survey on User Awareness of Fake Wi-Fi APs

Kida Atsumu[1,a)]　Kimura Yuuki[1,b)]　Ishikawa Ryoto[1,c)]　Uehara Tetsutaro[2,d)]

Abstract: Providing public Wi-Fi has become commonplace, and many users now connect—knowingly or unknowingly—to these networks. According to guidelines from Japan's Ministry of Internal Affairs and Communications, users are expected to check posted information and exercise caution to avoid connecting to fake Wi-Fi access points. However, the specific situations in which users inadvertently connect to such fake access points, and the moments when heightened vigilance is required, remain insufficiently understood. Moreover, the guidelines offer only limited countermeasures for service providers, placing primary responsibility for protection on the user side. To address this gap, we experimentally deployed fake access points in public settings and examined the behavior of users who connected to them. We then conducted questionnaires and follow-up interviews to identify the triggers, timing, and background factors that lead users to connect to fake access points. Based on these findings, we analyze countermeasures that users should consciously adopt and propose additional measures that service providers can implement to mitigate the risk of fake access points.

Keywords: Wi-Fi, Fake Access Point, User Behavior, Security

1. はじめに

公共の場におけるインターネット利用のために，多くの情報通信端末（以下，端末）利用者が無線 LAN を利用している．特に IEEE 802.11 規格 [1] の無線 LAN は，スマートフォンなどの端末において，利用するための主要な規格であり，公共の場においても広く利用されており [2]，Wi-Fi の名称で知られる．他方，公衆 Wi-Fi を利用しない人のう

[1] 立命館大学大学院情報理工学研究科
Graduate School of Information Science and Engineering, Ritsumeikan University
[2] 立命館大学情報理工学部
College of Information Science and Engineering, Ritsumeikan University
[a)] kida@cysec.cs.ritsumei.ac.jp
[b)] ykimura@cysec.cs.ritsumei.ac.jp
[c)] ryoto@cysec.cs.ritsumei.ac.jp
[d)] t-uehara@fc.ritsumei.ac.jp

ち 60%以上が，公衆 Wi-Fi を利用しない理由として「セキュリティに不安がある」と回答しており [2]，公衆 Wi-Fi のセキュリティは利用者にとって重要な課題である．

総務省の Wi-Fi のセキュリティに関するガイドライン [3] では，利用者は，公衆 Wi-Fi へ接続する際に偽の Wi-Fi アクセスポイントへ接続しないため，掲示等から接続先の SSID を確認し，キャプティブポータル等の URL，HTTPS 表示等に注意することが必要とされている．また公衆 Wi-Fi 提供者側においても，偽の公衆 Wi-Fi アクセスポイント対策として，認証画面の HTTPS 化などの対策が求められている．

偽の公衆 Wi-Fi アクセスポイント対策のためには，提供者による認証画面の HTTPS 化などの技術的対策と，利用者への正確な接続情報の提示が求められる．しかし，利用者がどのような際に公衆 Wi-Fi を利用し，どのような点に着目して公衆 Wi-Fi の真贋を判断しているのか，また利用者がどのようなタイミングおよびシチュエーションで偽のアクセスポイントに接続するかは必ずしも明らかではない．さらに総務省のガイドラインでは，偽のアクセスポイントに接続しないための対策は利用者側で行うことが前提となっており，提供者側での対策は限られているとされている．加えて，一部の規格においては，利用者が偽のアクセスポイントを見分けることが不可能な場合もある [4]．

本研究では，利用者の偽のアクセスポイントに対する接続状況を調査するために，立命館大学において実験的に偽のアクセスポイントを設置し，偽のアクセスポイントに接続する利用者に関する検証を行った．また，Wi-Fi 利用者に対して Wi-Fi アクセスポイントに接続する契機や公衆 Wi-Fi の真贋を判断する際の着眼点に関してアンケートおよびインタビューを行った．実験および調査の結果から，偽アクセスポイントに対する利用者の意識や，既存の偽アクセスポイント対策の課題が明らかになった．これらの結果を踏まえ，利用者が注意すべき点や，効果的な周知啓発のあり方，さらには提供者が講ずべき具体的な対策について考察する．

2. 研究背景

2.1 Wi-Fi

Wi-Fi は，無線 LAN の普及促進を行う業界団体である Wi-Fi Alliance から認証を受けた，IEEE 802.11 規格に準拠する通信を行う機器を指す．認証を受けた機器が増えたことから，無線 LAN 全般を指して Wi-Fi ということもあり，本研究では無線 LAN 全般を指して Wi-Fi として使用する．

2.2 SSID

Wi-Fi の SSID（Service Set Identifier）は，Wi-Fi ネットワークを識別するための値であり，ESSID（Extended SSID）と BSSID（Basic SSID）の 2 種類がある．ESSID はネットワーク全体を識別するための文字列であり，一般的に SSID と呼ばれることが多い．BSSID は特定のアクセスポイントを識別するための値であり，通常はアクセスポイントの MAC アドレスを指す．本研究では，ESSID を単に SSID と表記する．

表 1 立命館大学の学内 Wi-Fi
Table 1 Ritsumeikan University Wi-Fi

SSID	認証方式
Rits-1Xauth	WPA/WPA2-Enterprise
5GHz-Rits-1Xauth	WPA/WPA2-Enterprise
Rits-Webauth	WPA/WPA2-Personal
edurome	WPA/WPA2-Enterprise

2.3 偽アクセスポイント

偽アクセスポイント（Fake Access Point, 偽 AP）とは，正規のアクセスポイントと同じ SSID を持つアクセスポイントであり，利用者が意図せず接続してしまう可能性がある．偽 AP のうち，AP の MAC アドレスの偽造を行うものを，特に Evil Twin [4] と呼ぶ場合がある．また Evil Twin を用いた攻撃を Evil Twin Attack と呼ぶ．2024 年 7 月には，オーストラリアにて複数の偽 AP を設置し個人情報を盗んだとされる事件が発生しており [5]，偽 AP は実際の攻撃に利用されている．

2.4 キャプティブポータル

キャプティブポータル（Captive Portal）は公共 Wi-Fi などに接続する際に，Web ブラウザを通じて認証や利用規約への同意を求める仕組みである．キャプティブポータルに対応した AP へ接続すると，キャプティブポータルのページが自動的に表示ないしは Web ブラウザ利用時強制的に表示され，利用者はこのページを通じて認証や利用規約への同意を行う．

2.5 立命館大学の Wi-Fi 環境

立命館大学は，所属する学生向けに 4 種類の学内 Wi-Fi を提供している．立命館大学において提供されている学内 Wi-Fi を表 1 に示す．Rits-1Xauth および 5GHz-Rits-1Xauth，Rits-Webauth は，同じネットワークに接続している．また，Rits-1Xauth と Rits-Webauth は，ペアで設置されており，大学内において同様の密度で設置されている．Rits-1Xauth および 5GHz-Rits-1Xauth，edurome は，IEEE802.1X 認証を用いた Wi-Fi である．IEEE802.1X 認証を用いた Wi-Fi では，ID とパスワードによる認証後，端末は電子証明書を受け取り，Wi-Fi ネットワークに接続する．Rits-Webauth は，暗号化キーを入力して AP に接続後，キャプティブポータルによって ID とパスワードによる認証を行い，Wi-Fi ネットワークに接続する．

3. 関連研究

原田 [6] らは，キャプティブポータルや SSL 証明書を用いた偽 AP 検出アプリを開発し，東京都内複数箇所の公衆 Wi-Fi において，偽 AP 検出アプリを用いて調査した．調査の結果，攻撃を企図している偽 AP は発見に至らなかったが，多くの AP において偽造可能な状態であることが示唆された．一方，実際の利用者が偽 AP に接続するかどうかは研究対象としていない．

Qian ら [7] や森田ら [8] は，Evil Twin Attack に着目し，偽 AP の検出方法を提案し，技術的な検知の有効性を示した．一方で，検知技術が存在しても，利用者自身が「偽 AP に遭遇し得る」という脅威を認知していなければ，実際の利用場面で対策を講じることは難しい．Qian らや森田らの研究はネットワーク側の検出に焦点を当てており，利用者が日常的に偽 AP という脅威を認知し，接続を回避するかどうかといった認知的側面や行動様式は対象としていない．

Mariano ら [9] は，偽 AP を設置し，偽キャプティブポータルを通して利用者のセキュリティ意識を測定する仕組みを提案・実装した．実験はブラジリア大学キャンパスで実施され，利用者が偽ネットワークに接続すると教育的な認証画面に誘導し，アンケートによってフィッシングや MITM 攻撃などに関する認知度・行動傾向を測定した．調査の結果，多くの利用者が公衆 Wi-Fi を「不安」または「非常に不安」と認識していたが，証明書確認や VPN 利用といった具体的対策には結び付いていないことが明らかとなった．Mariano らは，実際の攻撃を伴わず，ユーザ行動を模擬的に観察しつつ，啓発を行う教育的アプローチを採用している点に特徴がある．一方，行動背景や意識の詳細な分析は行われておらず，利用者が偽 AP に接続する契機や，どのような点に着目しているかは明らかにされていない．

関連研究を踏まえ，本研究では，実験的に偽 AP を設置し，偽 AP へ接続する利用者に関する検証を行う．加えて，Wi-Fi 利用者の行動背景や意識の詳細な分析を行うために，アンケートおよびインタビュー調査を実施する．

4. 予備調査

利用者の偽 AP に対する接続状況を調査するために，実験的に偽 AP を設置し，偽 AP に接続する利用者に関する検証を行った．立命館大学大阪いばらきキャンパス [10]（以下，OIC）内の飲食店である OIC FOOD PARK（以下，調査エリア）において，2025 年 5 月 27 日から 2025 年 5 月 30 日までの 4 日間と 2025 年 6 月 24 日から 2025 年 6 月 27 日までの 4 日間の期間，12:30 から 13:00 の 30 分間調査を行った．前半 4 日間は立命館大学が設置している IEEE802.1X 認証の AP（以下，1XAP）を対象に調査した．後半 4 日間は立命館大学が設置しているキャプティブポータルによる Web 認証の AP（以下，WebAP）を対象に調査した．偽 AP に接続した利用者の要因を明らかにするため，偽 AP 接続後のキャプティブポータルによって表示される Web ページにアンケートへのリンクを設置した．調査に使用した偽 AP の機器およびソフトウェアを表 2 に示す．調査で設置した 1XAP と WebAP の偽 AP を表 3 に示す．同名 SSID は対象の SSID と同様の文字列を偽 AP に使用し，似た SSID は対象となる SSID の文字列の 1 文字を改変もしくは追加した SSID を偽 AP に使用した．また，偽 AP の認証方式はすべて OPEN である．調査エリア内での大学が設置している Wi-Fi 利用端末数を把握するため同時に Wi-Fi パケットキャプチャを行った．大学が設置した AP へ接続している端末数をパケットキャプチャにより推定した．

表 2 機器およびソフトウェア
Table 2 Equipment and Software

Raspberry Pi	3 Model B+
Ubuntu	24.04.1 LTS / 6.8.0-63-generic
hostapd[11]	2.10
NoDogSplash[12]	5.0.2

表 3 偽 AP の SSID
Table 3 Fake AP SSIDs

対象 AP	同名 SSID	似た SSID
1XAP	Rits-1Xauth	Rits-lXauth
WebAP	Rits-Webauth	Rits-Webauthn

4.1 研究倫理

本調査では，調査エリア滞在者の Wi-Fi 利用に影響を与える可能性があるため倫理的配慮に基づいて実施した．本調査の実施にあたり，調査で収集した情報に関するプライバシーポリシー [13] を定めた．Wi-Fi 利用者の端末が偽 AP に接続した際，キャプティブポータルにより，偽 AP に接続したことを Wi-Fi 利用者に対して即時提示するようにした．大学の授業への影響を避けるため，授業が実施されていない時間帯に短時間で実施した．また，端末が偽 AP に自動接続しないよう，本来の AP と異なる認証方式を設定した．調査中は実施者が調査エリアに常駐し，問題が起きた場合，即座に対応できるよう待機した．調査エリア内に掲示物を設置し，調査を回避しインターネットを利用する方法および問い合わせ窓口を告知した．本調査の実施にあたり，施設管理者および施設情報システム管理者に許可を得た．また，我々は本調査に対して情報処理学会 CSEC 研究会が運用する「サイバーセキュリティ研究における倫理的配慮のチェックリスト」[14] によるセルフチェックを実施した．

表 4　実験結果
Table 4　Experiment Results

	学内 Wi-Fi 利用端末数		偽 AP 接続数	
	1XAP	WebAP	1XAP	WebAP
1 日目	374 種類	398 種類	0 件	1 件
2 日目	508 種類	386 種類	0 件	0 件
3 日目	545 種類	487 種類	0 件	0 件
4 日目	394 種類	457 種類	0 件	0 件

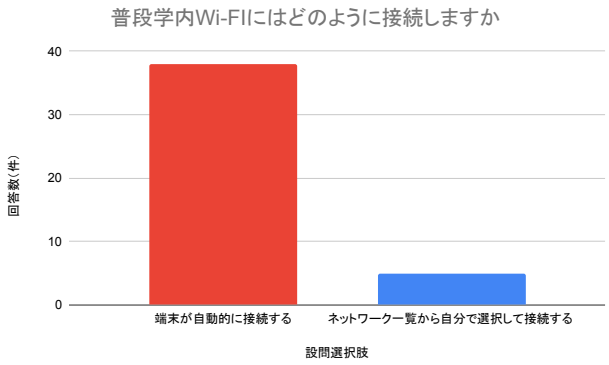

図 1　アンケート結果 1
Fig. 1　Questionnaire Results 1

4.2　結果

調査結果を表 4 に示す．調査エリアでは大学が設置する Wi-Fi の利用は確認されたが，偽 AP への接続はほとんどなかった．アンケートへの回答は 0 件であり，偽 AP に接続する利用者の要因は不明である．

5.　インタビュー調査

Wi-Fi 利用者の AP 接続への契機や公衆 Wi-Fi の真贋を判断する際の着眼点を明らかにするため，OIC を利用する学生にアンケート調査およびインタビュー調査を実施した．

5.1　アンケート調査

偽 AP 実験の結果より，認証方式が OPEN で同名および似た SSID の偽 AP にはほとんど接続されないことが確認された．結果の要因を明らかにするため OIC を利用する学生にアンケート調査を実施した．アンケート参加者の募集は大学内ポータルサイトで行った．アンケートの設問は付録 A.1 に示す．

5.1.1　結果

43 人からアンケートの回答を得た．抜粋したアンケートの結果を図 1，2，3，4，5，表 5 に示す．自由記述の回答は SCAT（step for cording and theorization）[15] を用いて分析した．SCAT により，理論記述と呼ばれる，利用者の行動や意識を説明する記述を抽出した．アンケートの自由記述の分析は筆頭著者が実施した．SCAT により得られた理論記述を表 6 に示す．

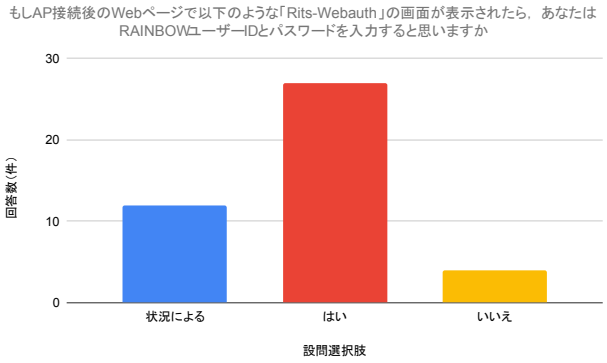

図 2　アンケート結果 2
Fig. 2　Questionnaire Results 2

表 5　アンケート結果 3
Table 5　Questionnaire Results 3

どのような場合に ID とパスワードを入力しますか	
設問選択肢	回答数（件）
大学構内で表示されたとき	3
「Rits-Webauth」に接続していることが確認できたとき	2
上記の両方を満たすとき	3
端末が自動で接続したとき	4

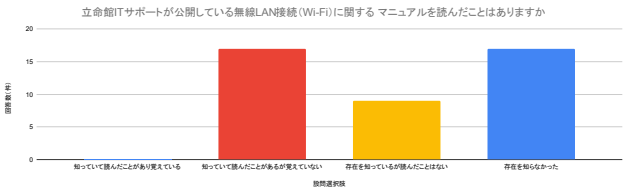

図 3　アンケート結果 4
Fig. 3　Questionnaire Results 4

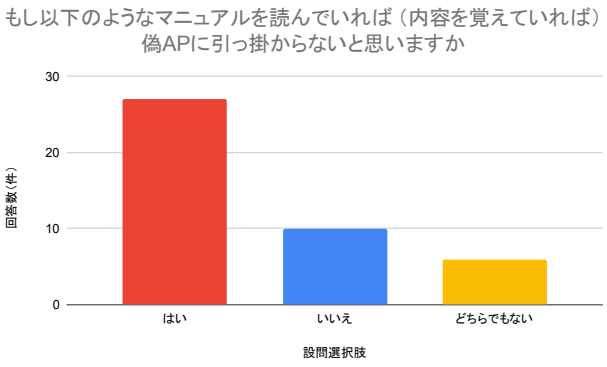

図 4　アンケート結果 5
Fig. 4　Questionnaire Results 5

5.2　インタビュー調査

アンケート回答者のうち，インタビューの同意を得られた 20 人にインタビュー調査を実施した．2025 年 7 月 9 日から 2025 年 7 月 18 日の期間，対面およびオンラインで，説明および諸手続きを含む約 30 分間のインタビューを実施した．本研究では，筆頭著者がインタビューを実施した．

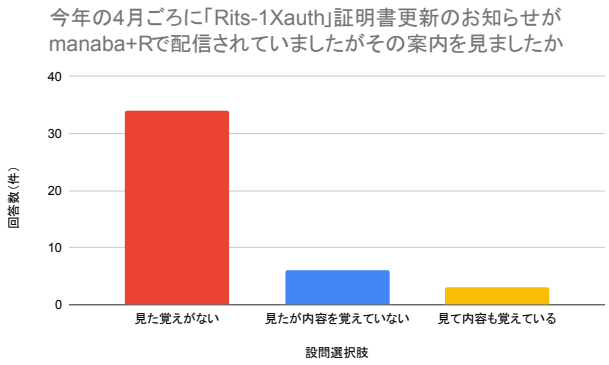

図 5 アンケート結果 6
Fig. 5 Questionnaire Results 6

表 6 自由記述から抽出した理論記述
Table 6 Theoretical descriptions extracted from free text

学内 Wi-Fi 利用方法のマニュアルを読んでいたとしても 偽 AP に引っかかると考える理由
・マニュアルを覚えていたとしても面倒くさいため， 毎回の接続時に注意しない
・手間がかからずに AP に接続できることを利点に感じており， その利点をつぶすような追加の確認はしない
・すぐに AP に接続したいときは確認せずに接続する
・AP から切断されて再接続するときは， 気持ちの余裕がないため注意しない
・マニュアルを覚えていれば一定の効果があると考えている
・マニュアルを覚えていても気にしない人や知識のない人は， わざわざ確認しない
・マニュアルの内容を忘れてしまう
・大まかに接続時に確認するが詳細までは確認しない
・そもそもマニュアルに目を通すのが面倒くさい
・インターネットに出るまでの過程に興味がないため注意しない

インタビューは半構造化インタビューで実施した．インタビュイーの属性を表 7 に示す．インタビューの構造化部分を付録 A.1 に示す．

5.2.1 分析

インタビューデータの分析手法として，アンケート自由記述の分析と同様に SCAT を用いた．筆頭著者および共著者 1 人の 2 人で SCAT を実施した．SCAT によって得られた理論記述から重複した意味を持つものを削除し，AP 接続の契機と Wi-Fi の真贋判断に関する理論記述を抽出した．抽出した結果をそれぞれ体形的に理解するため，抽出結果を新原らが定義した m-SHEL[16] を参考に，Wi-Fi 利用分類用に拡張したものを用いて分類した．拡張した m-SHEL（以下，Wm-SHEL）を表 8 に示す．

5.2.2 結果

分析し，分類した結果を表 9 に示す．SCAT により，373 種類の理論記述が得られた．AP 接続の契機に関する理論記述は 87 種類，Wi-Fi の真贋判断に関する理論記述は 114 種類抽出された．AP への接続の契機として，E（環境）がもっとも多く，39 種類であった．また，Wi-Fi の真贋判断

表 7 インタビュイー属性一覧
Table 7 Interviewee Attributes

学部・研究科	回生	性別
経営管理研究科	修士 1 回生	男性
経営学部	4 回生	男性
経済学部	4 回生	男性
経営学部	3 回生	男性
経営学部	2 回生	女性
経営学部	2 回生	男性
経営学部	2 回生	女性
経済学部	2 回生	女性
情報理工学部	4 回生	女性
情報理工学部	3 回生	男性
情報理工学部	3 回生	男性
情報理工学部	2 回生	男性
情報理工学部	2 回生	男性
情報理工学部	1 回生	男性
政策科学部	4 回生	男性
政策科学部	4 回生	男性
政策科学部	4 回生	女性
映像学部	4 回生	女性
映像学部	2 回生	女性
総合心理学部	3 回生	男性

表 8 本研究で使用した Wm-SHEL
Table 8 Wm-SHEL used in this study

要素	カテゴリ
m：マネジメント	組織・管理・制度・指導・方針
S：ソフトウェア	ルール・手順・教育・認証・知識・暗号
H：ハードウェア	端末・インターフェース
E：環境	利用場所・状況・制約
L1：本人	意識・態度・個人の認識・行動
L2：周りの人	他者・コミュニティ影響

として，L1（本人）がもっとも多く，42 種類であった．接続の契機の E（環境）と真贋判断の L1（本人），S（ソフトウェア）それぞれの理論記述から契機と真贋に関する記述を抜き出した結果を，表 10，11，12 に示す．AP の真贋判断の L1（本人）において，SSID に関する内容は 12 種類あり，40%を占めた．携帯電話回線において大容量通信プランがあることから，公衆 Wi-Fi をほとんど利用しない場合もインタビュー結果から確認された．しかし，表 10 に示すように，公衆 Wi-Fi を利用する場合も確認された．

6. 考察

6.1 予備調査実験において Wi-Fi 利用者が偽 AP に接続しなかった要因

4 章において，実験的に偽 AP を設置したが，学内 Wi-Fi 利用者（以下，Wi-Fi 利用者）による偽 AP への接続は 1 件しか確認されなかった．図 1 より，Wi-Fi 利用者は Wi-Fi を端末の自動接続で利用していることがわかる．表 12 よ

表 9 分類結果
Table 9 Classification Results

	接続の契機	真贋判断
m	5 種類	10 種類
S	0 種類	24 種類
H	19 種類	6 種類
E	39 種類	31 種類
L1	23 種類	42 種類
L2	1 種類	1 種類
合計	87 種類	114 種類

表 10 Wi-Fi 接続の契機（環境）
Table 10 Triggers for Connecting to Access Points (Environment)

- やむを得ない事情
- モバイル回線の通信量削減
- 普段利用する AP が利用できない場合に切り替え
- 通信容量の上限に達しているとき
- 誰かと連絡を取りたい場合
- AP が不調な場合に切り替え
- 大容量通信を行うとき
- 利用者が少ない Wi-Fi に切り替え
- 1 日に複数回 Wi-Fi を利用する予定がある場合
- 飲食店で作業をする場合
- 長時間同じ場所に留まる場合
- 公共交通機関利用時
- モバイル回線が利用できない場所
- 勤務先では自動接続でその他は手動接続
- 素早く接続したい場合
- インターネットが利用できないとき
- 回線速度が速い Wi-Fi に切り替え
- 飲食店の公衆 Wi-Fi
- 学内と自宅内のみ

り，Wi-Fi 利用者は，AP の暗号化の有無に真贋判断の上で着目してることがわかる．また，そのほかの理論記述から，Wi-Fi 利用者は IEEE802.1X 認証の学内 Wi-Fi を優先して利用していることが確認された．今回の実験で設置した偽 AP は，認証方式が OPEN であった．本来の学内 Wi-Fi と認証方式が異なるため，端末は偽 AP に自動接続しない．したがって，Wi-Fi 利用者は偽 AP に接続しなかったと考えられる．前述した理由と実験結果から，Wi-Fi 利用者は，普段から偽 AP の対策として一定の効果がある Wi-Fi 利用を行っていると考えられる．

6.2 Wi-Fi 利用者の偽 AP 接続リスク

6.1 節より，Wi-Fi 利用者は，偽 AP の対策として一定の効果がある Wi-Fi 利用を普段行っていると考えられる．しかし，Wi-Fi 利用者の端末が自動接続してしまう偽 AP を設置された場合，Wi-Fi 利用者は偽 AP に接続してしまう可能性があるため，そのリスクについて本研究の結果より考察する．以下では偽 AP の認証方式が WPA/WPA2/WPA3 Personal である場合と，WPA/WPA2/WPA3 Enterprise である場合に分けて考える．

表 11 Wi-Fi の真贋判断（本人）
Table 11 Authenticity Judgment (User)

- できるだけ公衆 Wi-Fi を利用しない
- 分からない画面が出てきたら疑う
- 信頼できないものには接続しない
- SSID が見覚えのあるパターンだと信頼
- SSID に日本語が含まれていると怪しい
- SSID が単語のみだと怪しい
- 学内 Wi-Fi 以外は認証情報を入力しない
- メールアドレス等であれば入力
- SSID で判断
- SSID から大学の Wi-Fi だと推測
- ユーザ名とパスワード入力後の証明書は信頼
- 公衆 Wi-Fi はあまり利用しない
- SSID を正確に記憶していない
- 雰囲気で選択
- 積極的に公衆 Wi-Fi を利用
- 「Free」という文字列は信頼できない
- 怪しくてもインターネット利用のために接続
- Wi-FI 利用案内を確認
- Web 検索で確認
- 公衆 Wi-Fi は危険
- よくわからない SSID は怪しい
- 見慣れた SSID は信頼
- SSID に施設名が含まれていないと怪しい
- Web 検索でわざわざ確認しない
- SSID はユニークである
- 学内 Wi-Fi は信頼
- 素早い接続を優先し確認しない
- 公衆 Wi-Fi アプリ
- 何かの SSID 似せている AP は怪しい
- 信頼する SSID を記憶

表 12 Wi-Fi の真贋判断（ソフトウェア）
Table 12 Authenticity Judgment (Software)

- 暗号化キーが必要な Wi-Fi をより信頼
- 証明書はよくわからないがマニュアルに従い端末に信頼させた
- 証明書はよくわからないが端末に信頼させた
- 学内 Wi-Fi はマニュアル通りに接続した
- 暗号化されていない Wi-Fi は怪しいと感じる
- 学内 Wi-Fi のマニュアルを読んでいないため，暗号化キーがわからない AP がある
- 証明書を接続のため仕方なく端末に信頼させた
- 学内 ID とパスワードは大学敷地内で求められた場合は入力
- 初めて行く場所での証明書は受け入れない
- 公式アプリ経由のみで接続可能な公衆 Wi-Fi は信頼
- ガイダンスの説明を覚えていたので，学内 Wi-Fi マニュアルを読んでいない
- 信頼している Wi-Fi であれば証明書の更新を受け入れる
- 安全に利用可能な公衆 Wi-Fi が存在することを知っている
- 公衆 Wi-Fi の利用規約に日本で使わない漢字が，含まれている場合は怪しい
- 携帯キャリアが提供している Wi-Fi は安全性が高い
- 学内 Wi-Fi は信頼できるのでの証明書は無条件で端末に信頼させる

偽 AP が WPA/WPA2/WPA3 Personal の認証方式を用い，本来の AP と同一の SSID と暗号化キーが設定されている場合，Wi-Fi 利用者の端末は偽 AP に自動接続する．不特定多数が利用する公衆 Wi-Fi においては，SSID や暗号

化キーが攻撃者に容易に取得され得るため，利用者端末が自動接続する偽 AP を攻撃者が設置可能である．Wi-Fi 利用者が攻撃者の設置した偽 AP に接続すると，キャプティブポータルを用いたフィッシングサイトに誘導され，ID やパスワード，クレジットカード情報などが攻撃者に漏洩する可能性がある．キャプティブポータルを用いてフィッシングサイトが設置された偽 AP による攻撃を図 6 に示す．Wi-Fi 利用者は，キャプティブポータルを用いたフィッシングサイトの対策として，キャプティブポータルで表示された Web ページの URL の確認が挙げられる．本来の AP がキャプティブポータルで用いる Web ページを HTTPS で提供している場合，偽 AP が同様の HTTPS の URL を用いてフィッシングページを設置することは難しい．したがって，Wi-Fi 利用者の端末 Web ブラウザは，偽 AP のフィッシングページ上で，ログイン情報の自動補完を行わず，Wi-Fi 利用者の手動入力が必要であり，Wi-Fi 利用者の判断に委ねられる．Wi-Fi 利用者はキャプティブポータルで提供される Web ページの URL を確認することで，偽 AP のフィッシングページに情報を入力しないようにする必要がある．

また，接続時にログインを要求する Wi-Fi においてキャプティブポータルによる Web 認証が用いられている場合も，キャプティブポータルによって表示された Web ページの URL を確認することが重要である．しかし，図 2 より，学内 Wi-Fi のキャプティブポータル Web 認証において，ログイン画面の外観のみを基準としてログイン情報を入力すると答えたのは，回答者の 62.8%であり，半数以上は URL などその他の情報を確認していなかった．ログイン情報は複数のサービスにおいて共通して利用されている場合があり，またパスワードが Wi-Fi 利用者によって使い回されている場合もある [17]．したがって，偽 AP の接続によってログイン情報が漏洩することは，Wi-Fi 利用者にとって重大なリスクとなり得る．

偽 AP が WPA/WPA2/WPA3 Enterprise の認証方式を用いている場合 IEEE802.1X 認証が使用され，Wi-Fi 利用者の端末は自動接続を試みるが，端末が本来の AP から受け取り保存している電子証明書による検証に失敗するため接続されない．しかしその場合，偽 AP に自動接続を試みた端末が，Wi-Fi 利用者に電子証明書の検証が失敗したことを知らせるとともに，偽 AP への接続を続行するかの判断を求める場合がある [18]．端末に判断を求められた際に，Wi-Fi 利用者が接続の続行を選択すると，端末は偽 AP に接続し，偽 AP の電子証明書を保存する．その場合，Wi-Fi 利用者は偽 AP に IEEE802.1X 認証の ID とパスワードを送信し，偽 AP を設置した攻撃者に漏洩する．アンケートの結果および表 12 より，Wi-Fi 利用者は，IEEE802.1X 認証の電子証明書を十分に理解しておらず，軽率に端末へ保存させていることが確認された．Wi-Fi 利用者は，WPA/WPA2/WPA3 Enterprise の認証方式を用いた AP を利用していても，電子証明書へのリテラシー不足により偽 AP に接続し，ID とパスワードを漏洩する可能性がある．したがって，WPA/WPA2/WPA3 Enterprise の認証方式を用いた偽 AP への誤接続を防止するためには，Wi-Fi 利用者における電子証明書の理解度向上が必要である．

図 6 偽 AP によるフィッシング
Fig. 6 Phishing via Fake Access Point

6.3 Wi-Fi 提供者が講ずべき対策

Wi-Fi 提供者は，偽 AP の対策として IEEE802.1X 認証を導入することが有効であるが，Wi-Fi 利用者の電子証明書に対するリテラシー不足により，偽 AP への接続を防げない可能性がある．したがって，IEEE802.1X 認証を用いた Wi-Fi の提供者は，Wi-Fi 利用者に対する教育や啓発活動を通じて，電子証明書の重要性や確認方法について周知徹底を図る必要がある．しかし，不特定多数が利用する公衆 Wi-Fi おいては，それぞれに対して事前登録が必要な IEEE802.1X 認証を導入することは現実的でない．Wi-Fi 提供者が講じる偽 AP への有効な対策として，OpenRoaming[19] の導入が挙げられる．OpenRoaming は，事前登録が必要であるが，Wi-Fi 利用者が 1 つのアカウントで OpenRoaming に参加している AP すべてに IEEE802.1X 認証を用いて接続可能なサービスである．Wi-Fi 提供者は，OpenRoaming に参加した AP を設置することで，Wi-Fi 利用者に IEEE802.1X 認証を用いた Wi-Fi を比較的簡単に提供できる．

7. おわりに

本研究では，偽のアクセスポイントに接続する利用者に関する調査を行なった．実験的に偽のアクセスポイントを設置したが，学内 Wi-Fi 利用者は偽 AP に接続しなかった．また，アンケート調査とインタビュー調査を実施し，

Wi-Fi 利用者の Wi-Fi アクセスポイントへの接続契機や Wi-Fi アクセスポイントの真贋を判断する着眼点を分析した．それらの結果から，Wi-Fi 利用者の接続契機や真贋判断の着眼点が一部明らかになり，Wi-Fi 利用者の日常的な利用方法において，偽のアクセスポイントへの接続リスクはある程度低いことが確認された．しかし，不十分な点も確認され，それに対する Wi-Fi 利用者と提供者それぞれのが講ずべき対策を考察した．

謝辞

本研究は立命館大学情報基盤課および株式会社 nadeshico の協力を得て実施した．ここに謝意を表する．

参考文献

[1] IEEE: IEEE 802.11, The Working Group Setting the Standards for Wireless LANs, https://www.ieee802.org/11/. [Online; accessed 2025-08-02].

[2] 総務省：令和 7 年版 情報通信白書 | データ集，https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html. [Online; accessed 2025-08-02].

[3] 総務省：無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について，https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/. [Online; accessed 2025-08-02].

[4] Kaspersky: 悪魔の双子攻撃とは？ Wi-Fi に潜む悪魔の双子の説明，https://www.kaspersky.co.jp/resource-center/preemptive-safety/evil-twin-attacks (2017). [Online; accessed 2025-08-02].

[5] Convery, S.: WA man set up fake free wifi at Australian airports and on flights to steal people's data, police allege — Cybercrime — The Guardian, https://www.theguardian.com/technology/article/2024/jun/28/wa-man-fake-free-wifi-airports-data-theft-ntwnfb (2024). [Online; accessed 2025-08-18].

[6] 原田敏明, 森達哉, 後藤滋樹, Toshiaki, H., Tatsuya, M., Shigeki, G.: 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〜，Vol. 2015, 情報処理学会，pp. 931–938 (2015).

[7] LU, Q., QU, H., ZHUANG, Y., LIN, X.-J. and OUYANG, Y.: Client-Side Evil Twin Attacks Detection Using Statistical Characteristics of 802.11 Data Frames, *IEICE TRANSACTIONS on Information*, Vol. E101-D, No. 10, pp. 2465–2473 (online), DOI: 10.1587/transinf.2018EDP7030 (2018).

[8] 森田雅也, 金井敦, 谷本茂明, Masaya, M., Atsushi, K., Shigeaki, T.: ユーザアクセス情報を用いた Evil Twin 攻撃検出手法，情報処理学会，pp. 808–814 (2020).

[9] Mariano, H. S. and Café, D. C.: Measuring Public Wi-Fi Security Awareness via Captive Portal Connections Using a Microcontroller, *2024 Workshop on Communication Networks and Power Systems (WCNPS)*, pp. 1–6 (online), DOI: 10.1109/WCNPS65035.2024.10814259 (2024).

[10] 立命館大学：大阪いばらきキャンパス | アクセス，https://www.ritsumei.ac.jp/accessmap/oic/. [Online; accessed 2025-08-05].

[11] Malinen, J.: hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/WPA3/EAP/RADIUS Authenticator, https://w1.fi/hostapd/ (2013). [Online; accessed 2025-08-05].

[12] Contributors, T. N.: Welcome to Nodogsplash's documentation!, https://nodogsplash.readthedocs.io/en/latest/. [Online; accessed 2025-08-05].

[13] 立命館大学情報理工学部サイバーセキュリティ研究室：Wi-Fi 偽アクセスポイント設置調査におけるプライバシーポリシー，https://cysec.ise.ritsumei.ac.jp/fakeap_privacy_policy/. [Online; accessed 2025-08-05].

[14] 情報処理学会 CSEC 研究会：サイバーセキュリティ研究倫理に関するチェックリスト，https://www.iwsec.org/csec/ethics/checklist.html. [Online; accessed 2025-08-05].

[15] 大谷尚：4 ステップコーディングによる質的データ分析手法 SCAT の提案 —着手しやすく小規模データにも適用可能な理論化の手続き—，名古屋大学大学院教育発達科学研究科紀要. 教育科学, Vol. 54, No. 2, pp. 27–44 (2008).

[16] 新原功一，原田要之助：情報セキュリティインシデントに対するヒューマンエラー対策の提案，情報処理学会論文誌, Vol. 55, No. 10, pp. 2318–2326 (2014).

[17] トレンドマイクロ株式会社：パスワードの利用実態調査 2023，https://www.trendmicro.com/ja_jp/about/press-release/2023/pr-20230831-01.html (2023). [Online; accessed 2025-08-21].

[18] Apple: Apple デバイスを 802.1X ネットワークに接続する，https://support.apple.com/ja-jp/guide/deployment/depabc994b84/web. [Online; accessed 2025-08-18].

[19] Inc, W. B. A.: Open Roaming, https://wballiance.com/openroaming/. [Online; accessed 2025-08-18].

付　　録

A.1 アンケート設問およびインタビュー構造部分

本研究で実施したアンケートの設問およびインタビュー構造部分は GitHub 上（https://github.com/cysec-lab/css2025-FakeAP-questionnaires）に公開している．