

フレーム解析に基づく認証解除攻撃脆弱性の診断手法の提案と評価

劉 宇軒¹ 小林 孝史^{2,a)} 喜村 栄太¹

概要：近年、無線端末の普及に伴い、アクセスポイントを標的とした認証解除攻撃（Deauthentication Attack）の脅威が増加している。しかしながら、実環境におけるアクセスポイントの認証解除攻撃に対する脆弱性を、効率的かつ非侵入的に診断する手法は未だ限られている。本研究では、無線アクセスポイントに対する認証解除攻撃の脆弱性を、事前にかつ非侵入的に診断可能な新たな手法を提案する。提案手法は、IEEE 802.11 の Beacon フレームに含まれる RSN 情報エレメントに着目し、対象アクセスポイントとの接続や通信への干渉を一切行うことなく、事前・非侵入・複数アクセスポイントの同時診断を実現できる点に特徴がある。また、実験許可を得た 55 台の無線アクセスポイントの Beacon フレームを収集し、提案手法に基づいて解析を実施した結果、各アクセスポイントの認証解除攻撃に対する脆弱性の有無を診断できた。これにより、提案手法の有効性および汎用性が実証された。

キーワード：認証解除攻撃、無線アクセスポイント、脆弱性診断、Beacon フレーム、複数同時診断

Proposal and Evaluation of a Vulnerability Diagnosis Method for Deauthentication Attacks Based on Frame Analysis

LIU YUXUAN¹ TAKASHI KOBAYASHI^{2,a)} KIMURA SHUTA¹

Abstract: In recent years, the spread of wireless devices has led to an increasing threat of deauthentication attacks targeting wireless access points. However, methods for efficiently and non-intrusively diagnosing the vulnerability of access points to such attacks in real-world environments remain limited. In this study, we propose a novel method that enables prior and non-intrusive diagnosis of vulnerabilities in wireless access points against deauthentication attacks. The proposed method focuses on the RSN information element contained in IEEE 802.11 Beacon frames, and is characterized by its ability to diagnose multiple access points simultaneously without requiring connection or interfering with communication. Furthermore, we collect Beacon frames from 55 wireless access points with prior permission and conducted analysis based on the proposed method. As a result, we are able to diagnose whether each access point is vulnerable to deauthentication attacks. These findings demonstrate the effectiveness and general applicability of the proposed method.

Keywords: Deauthentication Attack, Wireless Access Point, Vulnerability Assessment, Beacon Frame, Simultaneous Multi-Target Assessment

1. はじめに

無線通信技術の急速な普及に伴い、Wi-Fi は現代社会の日常生活において不可欠な重要な基盤インフラとなっている。家庭、学校、企業、公共の場など、あらゆる場所において Wi-Fi ネットワークが利用されており、ユーザに利便

¹ 関西大学大学院総合情報学研究科知識情報学専攻
Intelligent Informatics Major, Graduate School of Informatics, Kansai University

² 関西大学総合情報学部
Faculty of Informatics, Kansai University
a) taka-k@kansai-u.ac.jp

性の高いインターネット接続手段を提供し、情報社会の発展を大きく促進している。

しかしながら、無線ネットワークの大規模な展開に伴い、その安全上の問題も顕在化している。Wi-Fi通信は無線電波を介して行われ、データは物理的空間においてブロードキャスト形式で送信されるため、有線ネットワークと比較してさまざまな攻撃を受けやすい[1]。特に、一般的な無線通信環境においては、攻撃者が通信内容を傍受したり、偽造パケットを注入するなどの手段を用いて、中間者攻撃(MITM)、サービス拒否攻撃(DoS)などを実行し、ユーザのプライバシーおよびネットワークの可用性に深刻な影響を及ぼすおそれがある[2]。

総務省の調査[3]によれば、家庭における無線LANの普及率は88%に達しており、無線LAN利用者の約68%がセキュリティ上の不安を抱えている。そのうち、約36%は明確な理由を伴わない漠然とした不安を感じていると報告されている。

無線通信環境の安全性を確保することは、現代における喫緊の課題である。現在、多種多様な無線アクセスポイントが存在しており、その中には認証解除攻撃を受けてしまう可能性の高いものがあり、認証解除攻撃が成功した場合には、ユーザの通信切断やパスワードオフラインクラッキング攻撃といった大きなリスクがある。

近年、無線ネットワークのセキュリティに関する多くの研究が行われており、様々な攻撃手法に対する検出・防御方法が提案されている[4][5]。しかし、アクセスポイントにおける認証解除攻撃に対する脆弱性の有無を、事前かつ非侵入的に評価できる方法は依然として限られている。

本研究では、Beaconフレームに含まれるRSN情報エレメントに着目し、RSN情報エレメントを解析することで、アクセスポイントにおける認証解除攻撃に対する脆弱性の有無を、事前かつ非侵入的に診断可能な手法を提案する。本手法は、通信内容への干渉やアクセスポイントとの実際接続を必要とせず、事前・非侵入・同時診断を可能とする点に特徴がある。

2. 関連知識

2.1 Access Point

無線アクセスポイント(Access Point: AP)とは、無線メディアを通じてSTA(無線端末)に分配サービス(Distribution Service)を提供し、無線端末がネットワークに接続できる環境を提供するデバイスである。

近年では、無線アクセスポイント機能を有するデバイスの多様化が進んでおり、ルータに加えて、さまざまなデバイスがAPとして動作可能となっている。本研究では、アクセスポイントを4種類に分類する。

- **ルータ型 AP (Router)**：ルータとは、複数のネットワークを相互に接続し、データの送受信を制御する機

器である。

- **テザリング型 AP (Tethering)**：スマートフォンやタブレットのテザリング機能により、当該端末自体がアクセスポイントとして動作し、他端末にインターネット接続を共有するものである。
- **モバイルホットスポット型 AP (Mobile Hotspot)**：パソコンが備えるモバイルホットスポット機能により、当該端末自体がアクセスポイントとして動作し、他端末にインターネット接続を共有するものである。
- **IoT デバイス搭載型 AP**：一部のIoT機器(例:監視カメラ、スマート家電、ドローンなど)は、初期設定やスマートフォンとの直接接続、あるいは端末からの直接制御を実現するために、自身が無線アクセスポイントとして動作するものである。

2.2 認証解除攻撃

認証解除攻撃(Deauthentication Attack)は、Wi-Fiネットワークに広く存在する攻撃手法の一つである。その目的は、ステーション(STA)とアクセスポイント(AP)間の接続を強制的に切断し、ネットワークサービスを中断させることである。この攻撃は、無線ネットワークに対する深刻な脅威となっている[6]。

IEEE 802.11標準において、認証解除フレーム(Deauthentication Frame)は管理フレームに分類され、接続を終了する際の通知に用いられる。例えば、STAが自発的に接続を切断する場合や、アクセスポイントが異常終了や電源オフにより通信を中止する場合に送信される。しかし、PMF(Management Frame Protection)が有効化されていない環境では、これらのフレームは暗号化や認証が施されておらず、攻撃者は容易に偽造することができる。その結果、攻撃者がSTAまたはAPを装い、偽造した認証解除フレームを注入し、接続を強制的に切断させることが可能となる[7]。

STAとAP間の接続状態は、通常以下の4段階に分類される：

未認証・未関連付け(Unauthenticated & Unassociated)
認証済み・未関連付け(Authenticated & Unassociated)
認証済み・関連付け済み(Authenticated & Associated)
認証済み・関連付け済み・802.1X認証済み(Authenticated & Associated & 802.1X Authenticated)

STAまたはAPのいずれかが認証解除フレームを受信すると、その接続状態は直ちに「未認証・未関連付け」に戻される。認証解除攻撃は攻撃者にとって容易に悪用できる脆弱性となっている。[8]

図1および図2に示すように、攻撃者は主に次の2通りの手法によって認証解除攻撃を行う。

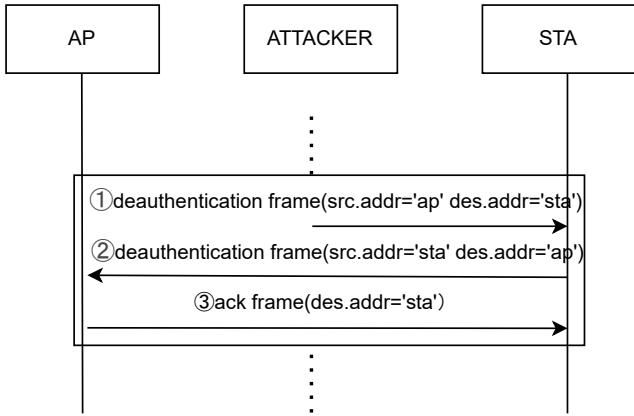


図 1 STA に対する認証解除攻撃の概略

Fig. 1 Overview of Deauthentication Attack Targeting STA

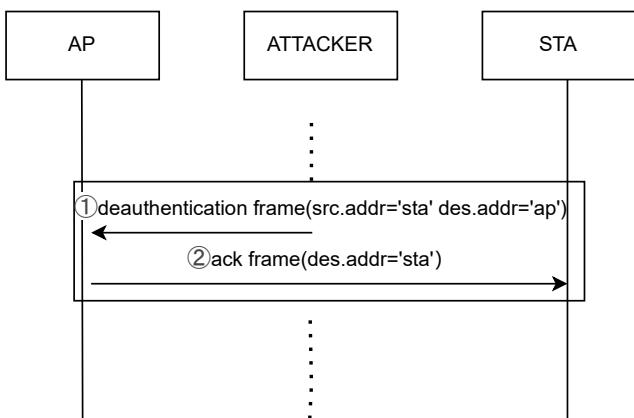


図 2 AP に対する認証解除攻撃の概略

Fig. 2 Overview of Deauthentication Attack Targeting AP

- STA の MAC アドレスを偽装して AP に 認証解除フレームを送信する
- AP の MAC アドレスを偽装して STA に 認証解除フレームを送信する

これらの手法はいずれも高い危険性を持ち、実行に必要な知識や装置も少なく、極めて低コストで実現可能である。

図 1 に示すように、攻撃者が送信元 MAC アドレスを AP の MAC アドレスに偽装した認証解除フレームを送信すると、PMF が無効な環境では当該管理フレームの真正性は検証されない。状態機械を「未認証・未関連付け」へ遷移させて接続を直ちに失効させる。さらに、STA は内部の接続制御により AP への再接続を自動的に試みるため、攻撃者が認証解除フレームを継続注入すると、当該 STA は再接続に失敗し続ける。図 2 に示すように、攻撃者が送信元 MAC アドレスを STA に偽装した認証解除フレームを AP へ送信した場合も同様である。AP は ACK を返した後に当該 STA との関連付け状態を破棄し、STA 側は切断を検出して再接続を試みる。攻撃が継続すると、STA は接続失敗ループに陥る。

さらに、この攻撃は以下のような他の攻撃手法と組み合

わせることで、より大きいリスクをもたらす：

Dos (サービス拒否) 攻撃：認証解除フレームを連続的に注入し、STA が接続を完了できない状態を恒常に維持することで、ネットワークの利用を妨害する。STA が認証フレーム（Authentication frame）を再送信しても接続が完了せず、STA は常に再接続に失敗し、結果としてネットワークは実質的に利用不能となる。

ハンドシェイク情報傍受：STA を強制的に切断し、WPA/WPA2 ネットワークに再接続させることで、4-way ハンドシェイクを誘発し、その通信を傍受する。これにより、PTK (Pairwise Transient Key) の生成に必要な情報を取得し、オフラインで PSK に対する総当たり攻撃を実行することが可能となる。

認証解除攻撃は現在の無線セキュリティにおける重要な脅威の一つとして広く認識されている。

2.3 Management Frame Protection

管理フレーム保護 PMF (Management Frame Protection) は、IEEE 802.11w 修正案によって導入され、2012 年に IEEE 802.11 標準に統合された無線 LAN 向けのセキュリティ拡張機能である。その目的は、管理フレームを悪用した中間者攻撃 (MITM) やサービス拒否 (DoS) 攻撃を防止し、無線 LAN の信頼性を高めることにある。

PMF が無効な環境では、Deauthentication フレームや Disassociation フレーム、さらには一部の Action フレームが平文で送信されるため、暗号化や真正性検証が行われない。この結果、攻撃者による偽造ができ、接続断や通信の乗っ取りなど深刻な被害を引き起こす可能性が高い。この問題に対処するため、PMF では管理フレームに暗号化および完全性保護を導入し、偽造フレームによる不正操作を防止している。主な機能は次のとおりである。

- (1) 完全性保護：メッセージ完全性コード (MIC) を用いてフレーム内容の改ざんを防ぐ。
- (2) 送信元認証：管理フレームが正当な通信相手から送信されたことを保証する。
- (3) リプレイ防止：シーケンス番号と確認機構によりリプレイ攻撃を防止する。
- (4) 以下のフレームの暗号化する：Disassociation, Deauthentication, Robust Action Frames, Directed Channel Switch Announcement

IEEE 802.11 標準において、無線 LAN 通信は階層構造に基づいてデータをカプセル化している。その中で、自身情報のブロードキャストを担う Beacon フレームは、IEEE 802.11 Wireless Management Frame (無線管理フレーム) に分類される管理フレームの一種であり、アクセスポイント (AP) が定期的に送信し、存在や情報を周囲に通知する役割を果たす。Beacon フレームは、複数の固定フィールドと拡張フィールドで構成されており、後者の Tagged

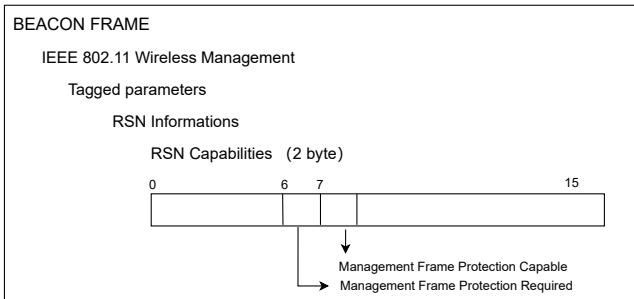


図 3 Beacon フレームに含まれる PMF 関連ビットの位置関係
Fig. 3 Bit Layout of PMF-Related Fields in the Beacon Frame

Parameters フィールド（可変長フィールド）は「タイプ - 長さ - 値 (TLV)」形式で記述される。このフィールドには SSID, 対応データレート, セキュリティ関連情報などの情報要素が格納される。

可変長フィールドの中で、セキュリティ構成を示す重要なフィールドが RSN 情報エレメント (Robust Security Network Information Element) である。これは IEEE 802.11i にて定義され、後に標準へ統合されたもので、使用中の暗号アルゴリズム、認証方式、および管理フレーム保護機能の有無を記述する。

RSN 情報エレメントには複数のサブフィールドが含まれており、特に、RSN Capabilities フィールドには、2 バイトの PMF に関する機能ビットが含まれており、MFPC および MFPR の値もここに格納されている。MFPC (Management Frame Protection Capable) は、当該デバイスが PMF に対応していることを示す。MFPR (Management Frame Protection Required) は、当該 AP が接続に際して PMF の使用を必須とすることを示し、PMF をサポートしない STA は当該 AP に接続できない。

2.4 PMF の実装および普及状況

近年、Wi-Fi Alliance は、Wi-Fi Certified を取得する新規機器に対して、PMF 対応を必須条件として定めている [9][10]。Apple, Microsoft, IODATA, Qualcomm (Atheros), TP-LINK などの主要メーカーはすでに実装を完了している。一方で、未対応の事例も依然として存在している。

2021 年 10 月および 12 月に実施された調査 [11] によれば、PMF を有効にしているものは約 4.84 % にとどまり、PMF を強制使用している無線アクセスポイントはわずか 0.01 % であることが報告された。この普及率の低さの背景には、PMF に非対応の旧型機器が依然として広く使用されていることに加え、低コストや省電力性を優先する IoT 機器などにおいて PMF 機能が実装されていないケースが多いことが挙げられる。

3. 関連研究

現在、商用および研究のいずれにおいても、無線アクセスポイントにおける認証解除攻撃に対する脆弱性を診断する手法としては、認証解除フレームを偽造して対象アクセスポイントに対して実際に攻撃を行うアプローチが主流である [12]。

このような手法では、テスト用 STA が実際に対象アクセスポイントに接続するか、または当該アクセスポイントを利用中の実機端末に対して直接攻撃を行う必要があるため、正常な通信に干渉や影響を引き起こし、安全性の観点から問題がある。

さらに、認証解除攻撃を実行可能なツール [12] は存在しているが、これらを用いるには、対象アクセスポイントの BSSID やチャネルなどの情報を事前に収集し、さらに当該アクセスポイントに接続中の STA の MAC アドレスを特定する必要がある。加えて、複数のアクセスポイントを対象とした同時診断は困難であり、拡張性や効率性の面でも大きな制約を伴っている。

現在、多くの研究者は認証解除攻撃が発生したことを検出する手法に取り組んでいる。Domien ら [6] は、フレームの物理信号に基づく検出手法を提案した。Roman ら [13] は、統計的閾値判定に基づく検出手法を提案した。しかし、これらの手法はいずれも攻撃が発生した後に異常を検出する「事後的な検知手法」である。

以上のように、現行手法は通信への干渉、手順の煩雑さ、拡張性の欠如といった課題を抱えており、大規模な実環境への適用には限界があると言える。加えて、攻撃が発生する前の事前診断も、無線ネットワークの安全性向上における重大な課題である。

4. 提案手法

本研究は、アクセスポイント (AP) が送信する Beacon フレームを収集し、RSN 情報エレメント内の RSN Capabilities から MFPC / MFPR を抽出することで、接続や攻撃を伴わずに認証解除攻撃に対する脆弱性を事前に判定する手法を提案する。本手法は無線 LAN の運用通信に干渉せず、標準仕様に依拠するためベンダ非依存であり、チャネル走査により同時に多数の AP を対象とできる。

4.1 設計方針

本手法は以下の設計方針に基づいている：

- **非侵入性**：検出過程においてフレームを送信せず、攻撃を行わない、対象ネットワークに一切の影響を与えない。
- **非接続型**：通信の確立を必要とせず、AP への接続を必要としない、ブロードキャストされるフレームのみ

を解析対象とする。

- **軽量かつ高速**：一般的な無線 LAN モニタリングデバイスのみで構築可能であり、高速な収集と一括解析を実現する。
- **ベンダ非依存**：IEEE 802.11 標準に準拠したファイル構造を基にしており、特定メーカーや製品に依存せず、汎用性が高い。
- **同時多 AP**：BSSID ごとに複数 Beacon を収集して、広域環境の多数 AP を同時に診断できる。

この手法は、大規模な無線ネットワーク環境で、事前に複数のアクセスポイントの認証解除攻撃に対する脆弱性を診断することを可能にし、実際の攻撃を行うことなく、認証解除攻撃に対する脆弱性のあるアクセスポイントを診断できる点で、既存の診断手法とは異なる視点からの新たなアプローチである。

4.2 実行環境



図 4 実行環境

Fig. 4 experimental environment

表 1 実行環境

| | |
|------------------|-------------------|
| OS | Linux Kali 6.6.15 |
| Wireless adapter | ENTGD mt7921u |
| Python | 3.11.8 |

本システムは Linux (Kali, 6.6.15) 環境を基盤とし、Python 3.11.8 とモニターモード対応の無線インターフェースアダプタ（ドライバ：mt7921u）上で動作する。解析には Scapy を用い、チャネル制御には iw を用いる。動作環境の規制ドメインに従い、2.4GHz 帯および 5GHz 帯の使用可能なチャネルを監視対象とする。システムの構成例は図 4 および表 1 に示す。チャネル走査および解析手順の詳細は 4.3 節に示す。

4.3 検出ロジックと実現方法

(1) フレーム収集とチャネル切り替え

無線アダプタは同時に一つのチャネルしか監視できないため、コマンド `iw dev <interface> set channel <channel_number>` を用いて順次チャネルを切り替え、2.4GHz 帯（チャネル 1～13）および 5GHz 帯の使用可能なチャネル（チャネル 36, 40, 44, 48,

52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144）を対象に、計 33 チャネルを順次切り替え、各チャネルを約 5 秒間監視する。監視中には Scapy を用いて無線フレームを取得し、解析用にメモリへ格納する。

(2) Beacon フレームの抽出

IEEE 802.11 フレームヘッダ内の `type` フィールドおよび `subtype` フィールドの値を基に、(`type=0`, `subtype=8`) の Beacon フレームを抽出する。

(3) RSN 情報エレメントの解析

Beacon フレームに含まれる Tagged Parameters の中から、Element ID 48 に対応する RSN 情報エレメントを抽出し、その内部構造を解析する。特に、第 10～11 バイトにあたる RSN Capabilities フィールドに着目する。

(4) PMF 関連情報判断

RSN Capabilities フィールド内のビット 6 およびビット 7 には、以下の 2 つのビットフラグが含まれる：

- **MFPC (Management Frame Protection Capable)** : PMF をサポートする
- **MFPR (Management Frame Protection Required)** : PMF 必須とする

これらをビットマスク (0x40, 0x80) によって抽出し、以下のように判断する：

- (a) MFPC = 0 かつ MFPR = 0 の場合：すべての接続中で管理フレームが暗号化されずに送信されるため、攻撃者によって容易に偽造され、認証解除攻撃を受ける可能性が高い。
- (b) MFPC = 1 かつ MFPR = 0 の場合：PMF には対応しているが、無線接続時に PMF の使用が強制されていないため、PMF が未使用の接続では認証解除攻撃を受ける可能性が高い。
- (c) MFPC = 1 かつ MFPR = 1 の場合：アクセスポイントが STA に対して PMF を有効にした状態での接続を強制するため、単独での認証解除攻撃を受ける可能性は極めて低い。

(5) 未対応ケースの判定処理

一部の AP において、メーカーによる PMF 機能の未実装または実装ミス、もしくは 2012 年以前の旧型ファームウェアや IEEE 802.11w が普及する以前の機器などでは、Beacon フレーム内に RSN 情報エレメントが存在しない、または RSN Capabilities フィールドに MFPC・MFPR が含まれないケースがある。このような場合には、当該 AP を PMF に非対応と判定する。

(6) 結果出力

解析結果は SSID, BSSID, チャネル, MFPC, MFPR に加えて 判定クラス (A / B / C) を付与したテキ

ストとして出力し、原始フレームは pcap 形式で保存する。

5. 実験結果と評価

5.1 データ収集概要

本研究におけるデータ収集は実測を基盤としており、事前に被調査者に対して研究目的および収集内容を説明し、同意書への署名を得たうえで、実環境下において無線アクセスポイントのデータを収集した。すべてのデータ取得は明示的な許可を得た上で行われ、倫理的および法的要件を満たすよう配慮されている。

5.2 法令・倫理的配慮

本研究のデータ収集および解析は、以下の法令および倫理指針に則り、適切に実施した。

- **電波法 [14]**：本研究では暗号化通信の復号を一切試みておらず、偽造フレームの送信や干渉行為も行っていない。合法な周波数帯において、明文のブロードキャストフレームのみを受信しており、法令上の要件を満たしている。
- **個人情報保護法 [15]**：収集対象となったデータ（SSID や MAC アドレスなど）は、それ単独では個人を特定できない情報であり、「個人情報」の定義に該当しない。また、氏名や住所などの関連付けも行っていない。
- **倫理問題 [16]**：全てのデータ取得は、機器の所有者または管理者の明示的な同意を得たうえで実施されており、研究目的と使用範囲についても事前に説明を行った。これにより、情報処理学会（IPSJ）の倫理指針に則して実施した。

5.3 結果分析

本研究で対象とした無線アクセスポイント（AP）は合計 55 台であり、ルータ 32 台、テザリング 14 台、モバイルホットスポット 8 台、IoT デバイス 1 台である（表 2）。

| アクセスポイント種別 | 台数 |
|--------------|----|
| ルータ型 | 32 |
| テザリング型 | 14 |
| モバイルホットスポット型 | 8 |
| IoT デバイス型 | 1 |

表 2 収集した合計 55 台無線アクセスポイントにおける種類の構成

調査対象においては、特定の種別のアクセスポイントに偏りが見られたが、全体としては現代の無線環境における多様性を反映した構成となっていた。

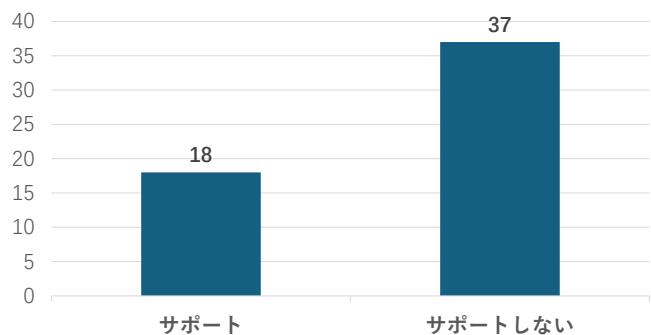


図 5 収集した全アクセスポイントにおける PMF サポート状況

Fig. 5 PMF Support Status of Collected Access Points

図 5 に示すように、55 台のうち 18 台（約 32.7%）が PMF をサポートし、37 台（約 67.3%）はサポートしていない。この「サポートしない」AP には、PMF 機能自体が未実装の AP と、PMF 機能はあるが設定が無効の AP の双方が含まれる。

この結果は、PMF が 2012 年以降に IEEE 802.11 標準に正式導入されたにもかかわらず、現場においてその利用が十分に普及していない実態を示しており、認証解除攻撃に対する脆弱性が依然として残存していることが示唆される。

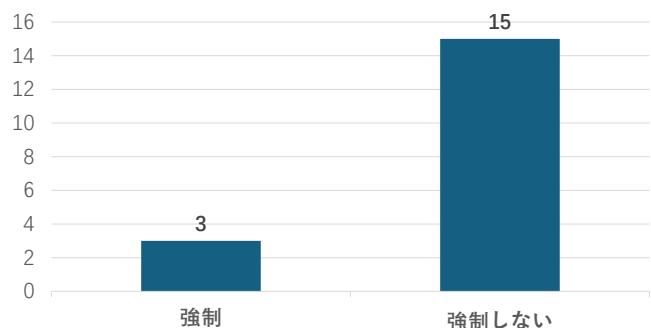


図 6 収集した 18 台 PMF をサポートするアクセスポイントにおける PMF 強制状況

Fig. 6 Enforcement Status of PMF Among the 18 Collected Access Points That Support PMF

さらに、図 6 に示すように、全 55 台の AP のうち、PMF をサポートしているのは 18 台であり、その中で PMF の使用を強制しているものは 3 台（5.5%）にとどまった。

PMF 接続を強制する 3 台はいずれもルータ型アクセスポイントであり、確認の結果、テザリング、モバイルホットスポット、IoT デバイスの各カテゴリに属する AP では、いずれも PMF 接続を強制する機能が実装されていないことが確認された。したがって、少なくとも本観測範囲においては、PMF の強制機能はルータ型に偏在しており、非ルータ型デバイスにおけるセキュリティ強度の向上が今後の課題である。

32台のルータ型APのうち、14台(43.8%)がPMFをサポートしていたが、残り18台(56.2%)はサポートしていない。さらに確認を行った結果、これらの多くはPMF機能自体はサポートしているが、初期設定では有効化されていないケースが多く、ユーザーによる手動設定がなければ、認証解除攻撃を防御できない。

したがって、ハードウェアレベルで一定のPMF機能が存在していても、運用段階では設定ポリシーに強く依存することが示唆される。

次に、14台のテザリング型APについて分析を行ったところ、4台(28.6%)のみがPMFをサポートしている、これはiPhone 15、iPhone 16がそれぞれ1台、Sony Xperia 1Vが2台の構成であった。一方、さらに確認を行った結果、残り10台についてはPMF機能が実装されていないことを確認した。

この結果から、一部の最新機種ではPMFが導入されているものの、大多数のスマートフォンやタブレットによって設置されたAPでは、PMFが実装していないことが明らかになった。

同様に、PCのインターネット共有機能により設置されたモバイルホットスポット型AP(8台)では、全てのAPにおいてMFPCおよびMFPRの値が0であり、これらのAPではPMFを有効にした状態での接続が全く不可能であることが明らかになった。

この結果は、当該種別のAPではPMFによる保護機構が備わっておらず、認証解除攻撃に対して脆弱であることを示唆する。

最後に、IoTデバイスによって設置したAPでは1台のみが対象となったが、MFPC・MFPRともにBeacon内に含まれていない、PMFが未実装であることが確認された。

また、Gordonらの研究[17]では、ドローンやスマートスピーカー等のIoTデバイスによって設置された無線APにおいて、PMF機能が実装されていないことが報告されている。

これらのIoTデバイスは、省電力性・即時接続性を優先して設計される傾向があり、セキュリティ機構が簡略化されることが多いとされている。

したがって、先行研究の指摘と本研究の観測は整合しており、IoTデバイス型のAPではPMF等の保護機構が未導入である事例が一定程度存在し、認証解除攻撃に対する潜在的リスクが残存していることが示唆される。

6. 提案手法の限界と今後の課題

本研究で提案した手法は、IEEE 802.11 Beaconフレームに含まれるRSN情報エレメントに基づき、無線APのセキュリティ設定を静的に解析し、認証解除攻撃に対する脆弱性を診断するものである。本手法は、非接続型・非攻撃型・通信非干渉という特性を有し、大規模な無線ネット

ワーク環境における短時間で大量APに対する脆弱性診断に適している。しかしながら、以下のような限界も存在する。

- 第一に、実際の通信においてPMF機能が使用されているかを確認することはできない点である。BeaconフレームはあくまでAPの設定情報を公開するものであり、実際接続でPMFを使用されたかどうかまでは判断できない。
- 第二に、RSN情報エレメントにMFPCまたはMFPRのビットがない場合、本手法はPMF未対応と判定する。これはIEEE 802.11標準の仕様に基づいて判断するが、IEEE 802.11の標準に準拠していない一部実装では過度に保守的な判定となる可能性がある。
- 第三に、本手法は、認証解除攻撃に対する脆弱性がある無線APを正確に診断することはできるが、脆弱性がないと断定することには限界がある。無線通信の特性上、攻撃者はフレーム偽装に加え、無線干渉やSAQueryタイムアウトの悪用など、複合的な手法によってPMFの防御を回避する可能性がある。そもそも、攻撃手法は日々進化しており、APが将来的にも認証解除攻撃を受けないと保証することは困難である。

今後の研究課題としては、実際の通信を対象に、非侵入的な方法で当該接続が認証解除攻撃に対して脆弱であるか否かを判定する手法を確立することである。また、本手法を他の無線セキュリティ分析手法と組み合わせることで、多層的かつ複合的な無線セキュリティ診断を実現することも期待される。

7. 結論

本論文では、フレーム解析に基づく認証解除攻撃脆弱性の診断手法を提案し、実環境で評価した。本手法はBeaconフレームを解析対象とし、RSN情報エレメント、特にMFPCおよびMFPRビットの有無を確認することで、当該APがPMF機能に関する内容を判断する。このようにして、接続や攻撃を伴わない非侵入型の認証解除攻撃に対する脆弱性評価を実現した。

複数の実環境において合計55台の無線APを対象に検出を実施した結果、現在のネットワーク環境においては、依然として多くの機器がPMFを有効化しておらず、また、多くの無線APがそもそもPMF機能を備えていないことも確認した。特にスマートフォンのテザリング、PCにより設置されたモバイルホットスポット、IoT機器により設置されたAPにおいてこの傾向が顕著であり、現行の無線ネットワークインフラが認証解除攻撃に対して顕著な脆弱性を抱えていることが示唆された。

提案手法は、通信環境に影響を与えることなく、無線アクセスポイントを対象として、認証解除攻撃に対する脆弱性の有無を判断できる情報を収集した、リスクの早期発見

と対応判断を支援するものであり、ネットワーク資産管理やセキュリティ監査といった用途において有効である。

参考文献

- [1] Thomas, A. M., Kumaran, G. A., Ramaguru, R., Harish, R. and Praveen, K.: Evaluation of Wireless Access Point Security and Best Practices for Mitigation, *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, pp. 422–427 (online), DOI: 10.1109/ICEECCOT52851.2021.9707914 (2021).
- [2] Lounis, K., Ding, S. H. and Zulkernine, M.: Cut It: Deauthentication attacks on protected management frames in WPA2 and WPA3, *International symposium on foundations and practice of security*, Springer, pp. 235–252 (2021).
- [3] Ministry of Internal Affairs and Communications: 令和4年度無線LAN利用者に対するアンケート調査集計資料, https://www.soumu.go.jp/main_content/000897265.pdf (2024). Accessed on 2025-04-17.
- [4] Amoordon, A., Deniau, V., Fleury, A. and Gransart, C.: A single supervised learning model to detect fake access points, frequency sweeping jamming and deauthentication attacks in IEEE 802.11 networks, *Machine Learning with Applications*, Vol. 10, p. 100389 (online), DOI: <https://doi.org/10.1016/j.mlwa.2022.100389> (2022).
- [5] Agarwal, M., Biswas, S. and Nandi, S.: Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach, *2015 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 246–251 (online), DOI: 10.1109/SMC.2015.55 (2015).
- [6] Schepers, D., Ranganathan, A. and Vanhoef, M.: On the Robustness of Wi-Fi Deauthentication Countermeasures, *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '22, New York, NY, USA, Association for Computing Machinery, p. 245–256 (online), DOI: 10.1145/3507657.3528548 (2022).
- [7] IEEE: IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks—Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pp. 1–4379 (online), DOI: 10.1109/IEEESTD.2021.9363693 (2021).
- [8] Reen, R. S., Dharmani, G., Gothwal, R. and AbdAllah, E. G.: Evaluation of Wireless Deauthentication Attacks and Countermeasures on Autonomous Vehicles, *2023 10th International Conference on Dependable Systems and Their Applications (DSA)*, pp. 494–501 (online), DOI: 10.1109/DSA59317.2023.00069 (2023).
- [9] Alliance, W.-F.: Wi-Fi® security technologies, <https://www.wi-fi.org/discover-wi-fi/security>. Accessed on 4 July 2025.
- [10] Ebbecke, P.: Protected Management Frames enhance Wi-Fi network security, <https://www.wi-fi.org/beacon/philipp-ebbecke/protected-managementframes-enhance-wi-fi-network-security>. Accessed on 4 July 2025.
- [11] Schepers, D., Ranganathan, A. and Vanhoef, M.: Let numbers tell the tale: measuring security trends in wi-fi networks and best practices, *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '21, New York, NY, USA, Association for Computing Machinery, p. 100–105 (online), DOI: 10.1145/3448300.3468286 (2021).
- [12] Aircrack-ng Team: Aircrack-ng - Wireless Security Tools Suite, <https://www.aircrack-ng.org/>. Accessed on 8 July 2025.
- [13] Bansal, R., Tiwari, S. and Bansal, D.: Non-cryptographic methods of MAC spoof detection in wireless LAN, *2008 16th IEEE International Conference on Networks*, pp. 1–6 (online), DOI: 10.1109/ICON.2008.4772621 (2008).
- [14] 総務省: 電波法, [https://laws.e-gov.go.jp/law/325AC00000000131](https://laws.e-gov.go.jp/law/325AC0000000131). Accessed on 4 July 2025.
- [15] 個人情報保護委員会: 個人情報の保護に関する法律, <https://laws.e-gov.go.jp/document?lawid=415AC000000057>. Accessed on 4 July 2025.
- [16] 情報処理学会倫理綱領委員会: 情報処理学会倫理綱領・行動規範, <https://www.ipsj.or.jp/ipsjcode.html>. Accessed on 4 July 2025.
- [17] Gordon, J., Kraj, V., Hwang, J. H. and Raja, A.: A Security Assessment for Consumer WiFi Drones, *2019 IEEE International Conference on Industrial Internet (ICII)*, pp. 1–5 (online), DOI: 10.1109/ICII.2019.00011 (2019).