L-018

模擬環境を利用した eduroam に対する Evil Twin 攻撃の評価

Evaluation of Evil Twin Attack on eduroam in a Simulated Environment

土山 大征† 岡崎 裕之† 鈴木 彦文‡
Daisei Tsuchiyama Hiroyuki Okazaki Hikofumi Suzuki

1. はじめに

近年，学術機関を標的としたサイバー攻撃が増加しており，学内システムの認証情報を窃取する事例も報告されている．多くの学内システムは，基本的なセキュリティが講じられているため，攻撃者がサーバ側を直接狙うには高いコストがかかる．

そこで攻撃者は，より攻撃しやすいユーザー端末側を補標的とし，フィッシングなどを用いて，認証情報の窃取を試みる．その中で，攻撃者の標的となるのが，無線 LAN ローミング基盤「eduroam」である．

eduroam は，大学や高専で多く利用されており，2025 年 6 月時点で国内 462 機関が参加している[1]．学生や教職員の学習や研究活動の場として利用されている．eduroam は，IEEE802.1X 認証を用いた WPA2/WPA3-Enterprise 方式を利用している．家庭用無線 LAN で一般的に利用される Personal 方式は共通のパスフレーズ（PSK）を用いた簡易な認証方式であるが，Enterprise 方式ではユーザー名やパスワードを用いたユーザー認証のほか，証明書を用いた認証を行う．Enterprise 方式の特徴として，ユーザーの認証情報を RADIUS サーバに登録することで，ユーザーごとのアクセス制御が可能であることや，ユーザーごとに認証情報が異なるため，なりすましが困難であることが挙げられる．そのため，eduroam では利便性とセキュリティを両立するために Enterprise 方式が採用されており，ユーザーは所属機関の認証情報を用いて，他機関の無線 LAN にも安全に接続できるようになっている．

しかし，この構造には問題がある．eduroam で利用される認証情報は，学内ポータルやクラウドサービスと共通であることが多いため，一度の情報漏洩が複数サービスへの不正アクセスにつながるリスクがある．このため，eduroam のセキュリティ対策は十分であるべきだが，eduroam で利用される Enterprise 方式にはユーザー端末側が正しい証明書検証設定を行っていることが前提であり，設定不備や注意不足がある場合，Evil Twin へ接続してしまい，認証情報を盗まれる危険性がある．

Evil Twin 攻撃では，正規の eduroam に似せたアクセスポイント（以後，AP）を用意し，ユーザーを誘導し，偽のキャプティブポータル画面を表示させて入力を促すことにより，認証情報を窃取する手法がある．加えて，ユーザー端末が Evil Twin の接続した際に発生する通信を傍受・解析することで認証情報を窃取する手法も存在する．後者は端末の自動接続機能が有効になっていると，ユーザーの入力なしで認証情報を窃取可能である．

このような背景から，eduroam に対する Evil Twin 攻撃に対して，認証情報をどの程度窃取する可能かを評価することは重要である．そこで本研究では，Evil Twin 攻撃における認証情報の窃取が，端末の設定状況や種類によってどの程度成功するかを実験的に評価した．実験の結果，証明書検証が適切に行われていない端末では，認証情報が容易に窃取されることが確認された．これらの結果から，eduroam の安全な利用には，サーバ証明書の適切な設定の徹底に加え，ユーザーへのセキュリティリテラシー教育が不可欠である．本研究は，eduroam 運用における課題を明らかにし，その改善に向けた具体的な方向性を示すものである．

2. 前提知識

2.1 eduroam

eduroam は，学術機関の間で無線 LAN の相互利用を実現する，国際的な無線 LAN ローミング基盤である．無線 LAN ローミングとは，認証連携技術により，利用者が所属機関のアカウントを利用して，他機関の無線 LAN インフラを利用可能とする仕組みである． eduroam は，欧州の教育研究ネットワークを運用する GÉANT によって開発・運用されている．日本では，国立情報学研究所（NII）が eduroam JP の名称で高等教育機関や研究機関を対象に展開している．近年では，市街地においても eduroam を提供する企業があるなど，普及が進んでいる[1].

eduroam が誕生した背景として，従来のキャンパス無線 LAN が学内機関者のみを対象としており，国内・国際会議など，他機関の関係者が現地でインターネットを利用することが難しい場合があったという課題がある．この対処として，各機関がゲスト用ネットワーク構築，ID 発行などを個別にしていた．このようにして，学術機関の間で無線 LAN の相互利用を実現したのが eduroam である．

eduroam にはいくつか問題点がある．ひとつは運用・技術基準は存在するが，細かな取り決めはなく，その多くが各機関の裁量に委ねている点である．このため，安全性の根拠が技術依存しており，また，監査機関の存在も明確でないことから，全ての eduroam ネットワークが安全であるという保証もない[2]．第二に，eduroam 接続時には所属機関のアカウントを利用するため，同一 ID で様々なサービスにアクセス可能となり，情報漏洩時のリスクが高い点である．したがって，eduroam におけるセキュリティ対策は十分である必要がある．しかし，eduroam のユーザー認証で用いられている IEEE802.1X には，ユーザー側の証明書検証不徹底や接続設定の多様性により，Evil Twin 攻撃への脆弱性が存在する．本研究では eduroam の模擬環境でこの攻撃を実施し，接続設定の違いが攻撃成功に与える影響を分析した結果を示す．

†信州大学大学院総合理工学研究科，Graduate School of Science and Technology, Shinshu University

‡国立情報学研究所 トラスト・デジタル ID 基盤研究開発センター，Center for Trust & Digital Identity

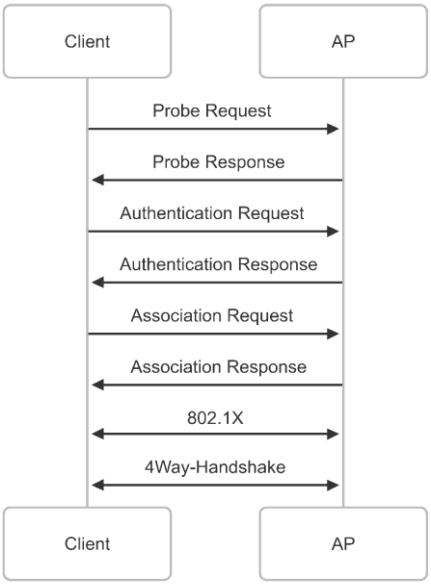

図 1　WPA2/3-Enterprise 接続シーケンス

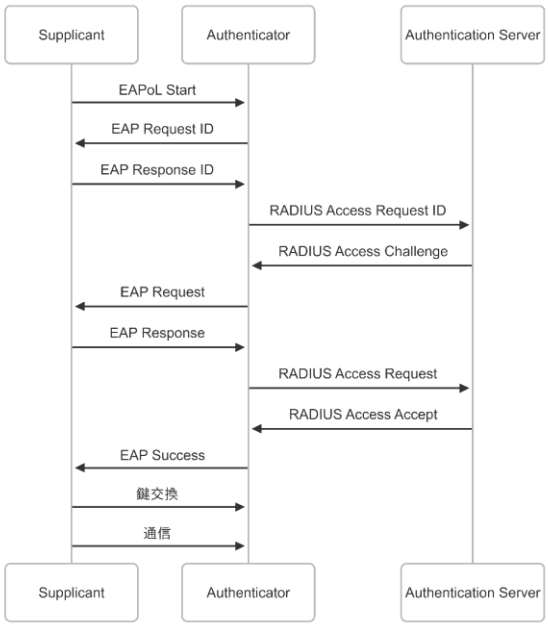

図 2　802.1X 接続シーケンス

2.2 WPA2/WPA3-Enterprise

WPA2/WPA3-Enterprise は無線 LAN におけるセキュリティ規格 WPA2/WPA3 にあるモードのひとつであり，認証サーバを利用した IEEE802.1X 認証を行う．接続シーケンスを図 1 に示す．ユーザーはあらかじめ ID・パスワードを認証サーバに紐づけておき，アクセスポイント（以後，AP）の接続時にはこの情報を利用して認証を行う．WPA2/3-Enterprise は企業や学術機関のように多数の利用者を収容するネットワークで利用することを想定したモードであり，eduroam では利用が義務付けられている．

同じセキュリティ規格のモードである PSK と違い，ID とパスワード，さらにはクライアント証明書を用いることができるため，高い安全性を確保できるとされている．

WPA3-Enterprise は WPA3 のモードであるため，通信の確立・切断に用いるフレームに対して認証をする PMF(Protected Management Frames)[3]を標準採用し，2.3 節のような認証手続きに対する攻撃に対策をしている．

2.2.1 IEEE802.1X

eduroam ではユーザーの認証方式として，IEEE802.1X(以降，Dot1X)に対応した RADIUS を使用する．Dot1X は IEEE が制定した LAN における認証規格である． Dot1X は，Supplicant， Authenticator， Authentication Server の 3 つから構成される．Supplicant は認証を受ける Client であり， 通常，PC やスマートフォンまたはネットワークへの接続を試みるデバイスが該当する．Authenticator は Dot1X に対応した Switch や AP であり，Authentication Server と Supplicant の中継を行う．Switch や Authentication Server は認証を行うサーバであり，一般的に RADIUS が該当する． Dot1X では EAP を用いた認証を行う．EAP は Extensible Authentication Protocol の略で，PPP（Point-to-Point Protocol）を拡張したプロトコルである．EAP の認証タイプには複数の種類があり，特に， eduroam で用いられる EAP には，主に EAP-PEAP や TTLS がある．PEAP は，クライアントと RADIUS の間で TLS 接続を確立する Phase1 と，ユーザー認証を行う Phase2 の二段階の認証を行う．TTLS も TLS 接続を確立した後，ユーザー認証を行う[4]．どちらも，ID とパスワードのやりとりは，TLS トンネルで保護された通信路で行われるため，通信をする AP と認証サーバが正規のものであれば，攻撃者に通信を傍受される危険性はなくなる．ここで，クライアントは，Phase1 において，サーバ証明書を検証することで，クライアントからサーバ認証を行うことができ，これにより，偽 AP への接続を防いでいる．しかし，クライアントによっては，サーバ認証を実施しない設定も可能であり，この場合，2.5 節の EvilTwin のような，正規の AP に偽装した AP に接続してしまうと，ID・パスワードを窃取される危険性がある．

2.3 Deauthentication 攻撃

クライアントおよび AP が通信の切断に利用する De-authentication フレームを端末および AP に送り続け，クライアントを AP から切断させる攻撃である．De-authentication フレームのフォーマットを表 1 に示す．MAC Header は MAC アドレスなどの情報を 24byte，FCS は誤り検出符号として 4byte を設定する．このフレームは平文でやりとりされるため，通信を傍受することで偽造することができ，そのため，クライアントを AP から不正に切断させることが可能である．この攻撃を続けることで，クライアントと正規 AP 間の通信を不能にすることができるため，2.5 節に示す Evil Twin のような，正規の AP に偽装した AP に誘導する手段としても利用される．ただし，WPA3 では PMF が標準採用されたことにより，この攻撃が困難になった[5].

2.4 CSA 攻撃

攻撃者がクライアントに対して，CSA（Channel Switch Annoucement）フレームを送り続け，端末を AP から切断さ

せる攻撃である．CSA は AP が端末に対して通信に使うチ

表 1　Deauthentication フレームのフォーマット

MAC Header	Reason Code	FCS
24byte	2byte	4byte

表 2　CSA のフォーマット

Element ID	Length	Channel Switch Mode	New Channel Number	Channel Switch Count
1byte	1byte	1byte	1byte	1byte

ャネルの変更を通知するフレームであり，IEEE802.11h で定義されている[5]．AP は 5GHz 帯で通信中に使用しているチャネルで気象衛星などの電波を受信した場合，別のチャネルに移動する必要がある．この際に通信を続けるために，AP は CSA を送信し，クライアントにチャネル切り替えを通知する．CSA を受信したクライアントはチャネルを切り替えて通信を再開する仕組みとなる．

CSA のフォーマットを表 2 に示す．Element ID はビーコンのオプション情報を識別するための ID であり，CSA では 37 が入る．Length は CSA 情報の長さであり，3byte が設定される．Channel Switch Mode は，クライアントが CSA 受信後チャネルを移動するまでに通信を続けるかを指定する．1 がセットされている場合は，クライアントがチャネルを切り替えるまで通信を停止する．New Channel Number は移動先のチャネルが入る．Channel Switch Count はチャネル移動までに送信されるビーコン数であり，ビーコンを送信するたびに減り，0 になるとチャネルの移動が起こる．

これらの情報は PMF による暗号化の対象にならないため，通信を傍受し，偽造することができる．そのため CSA を悪用した DoS 攻撃が可能である．先行研究[5]では，Channel Switch Mode を 1，New Channel Number を実際の AP と異なるチャネル，Channel Switch Counter を 0 に設定した CSA 入りのビーコンフレームを偽造して，通常のビーコンと同じ間隔で送信し続けることで，クライアントと AP 間の通信を不能にできることが示されている．

2.5 Evil Twin 攻撃

Evil Twin は，攻撃者が正規 AP に偽装した悪意のある AP（以後，偽 AP）であり，それを用いて通信を傍受し，フィッシング等により，ユーザーの秘密情報を窃取する攻撃が Evil Twin 攻撃である．攻撃者がユーザーを Evil Twin に誘導する方法として，Evil Twin を正規 AP と同じ名前にし，電波強度の高い状態で利用者の多いところに設置する方法がある．すると，クライアントは同じ基地局が存在する場合，電波強度の高い方に接続するため，Evil Twin に誘導することが可能である．ただし，Evil Twin の電波強度に依存するため，クライアントを正規 AP から不正に切断させて Evil Twin に誘導する攻撃手法も一緒に取られる．そのための攻撃手法には，2.3 節，2,4 節で述べた Deauthentication 攻撃と CSA 攻撃がある．本研究では，両手法を利用した Evil Twin 攻撃を行う．

Evil Twin を設置して，秘密情報を窃取するまでの流れを WPA のモード毎に示す．

フリーWiFi をはじめとした PSK 方式では，同一のパスフレーズ（PSK）を使用するため，以下のような手順で攻撃が行われる．

1. 何らかの形でパスフレーズを入手
2. 入手したパスフレーズを使って，Evil Twin を構築
3. ユーザーが誤って Evil Twin に接続．
4. ユーザーを偽のキャプティブポータルなどに誘導
5. ユーザーが入力した認証情報などの秘密情報を窃取

一方で，eduroam をはじめとした Enterprise 方式では，ユーザーによって，接続に使う ID・パスワードが違うため，ユーザーを Evil Twin に誘導にしようとすると，Dot1X 認証に失敗し，ユーザーを偽のキャプティブポータル等に誘導できない．そのため，攻撃者は以下のような手順で攻撃を成立させようとする．

1. まず，ユーザーの初回接続時に，偽 AP を用いて ID・パスワードを窃取（偽の RADIUS サーバで認証情報を取得）
2. 盗んだ ID・パスワードを RADIUS サーバに登録し，次回以降，Evil Twin での接続を接続が成功させる
3. ユーザーが誤って Evil Twin に接続
4. ユーザーを偽のキャプティブポータルなどに誘導
5. ユーザーが入力した認証情報などの秘密情報を窃取

2.2.1 節で述べたように，端末はサーバ検証が無効な場合，ID・パスワードを窃取可能である．特に，2.1 節で述べたように，eduroam で利用される ID・パスワードは情報漏えい時のリスクが高い．そのため，本研究では，Evil Twin 攻撃による ID・パスワードの窃取を攻撃者の目標とした Evil Twin 攻撃の評価を行う．

2.6 関連研究

本節では本研究に関連する研究について説明する．eduroam に対する Evil Twin 攻撃の研究として，Ivan [6]らは Enterprise 方式への攻撃と脆弱性を評価するために，認証情報窃取攻撃実験によるユーザーセキュリティ意識評価を実施した．この研究では，EAP で使われるほとんどの方式が，決して安全とは言えず， また，iPhone は、ユーザーが端末を誤って構成する可能性が低く，ユーザーが明示的に設定を変更しない限り、本研究で用いた攻撃の影響を受けないこと，さらには、比較的熟練したエンドユーザーであっても，Wi-Fi に関するセキュリティ認識はほとんどなく，極めて低いことが示されている．青山ら[7]はクラウド GPU サービスを活用した 2 段階 Evil Twin 攻撃を提案した．青山らの手法は，1 段階目に認証情報の取得と RADIUS への登録，2 段階目に Evil Twin によるフィッシングを行い，認証情報の取得に GPU を用いた場合，8 文字以下であるとき現実的な時間で解析可能であり，本攻撃が有効であると評価した．

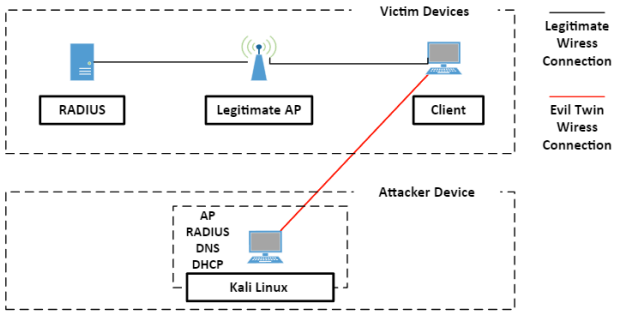

図 3　本研究における Evil Twin 攻撃の概要図

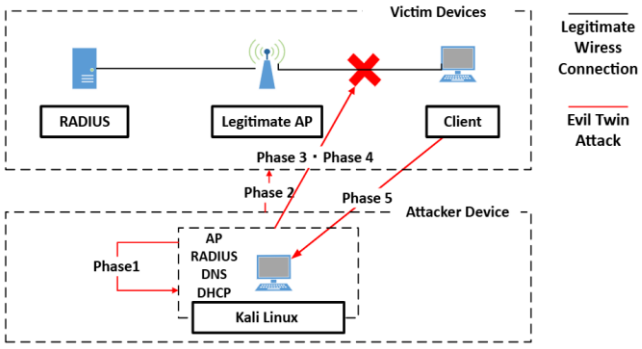

図 4　本研究における Evil Twin 攻撃のフロー

3. 実験方法

本研究では，正規の eduroam の電波が届く範囲内（以後，ケース 1）と届かない範囲外（以後，ケース 2）の双方において，Evil Twin 攻撃が実施される状況を想定し，それぞれのケースにおける攻撃の成功率や影響の違いを評価する．具体的には，ケース 1 では，正規の eduroam に接続中のクライアントが，攻撃者によって Evil Twin に誘導されるケースを想定し，ケース 2 では，正規の eduroam が存在しない状況下で，クライアントが Evil Twin を正規のものと誤認して接続してしまうケースを想定する．

加えて，クライアント端末側のサーバ証明書の検証有無によって，攻撃に対する耐性にどのような差異が生じるかを明らかにするため，各ケースについて「サーバ証明書を検証する設定」と「サーバ証明書を検証しない設定」の両方で実験を行う．これにより，現実的な運用における設定の違いがセキュリティに与える影響を検証する．

3.1 実験環境

実験に用いた端末構成を図 3 に示す．攻撃者の端末として仮想環境上に Kali Linux をインストールしたノート PC を準備した．また被害者の端末としてクライアントとなる PC やスマートフォンと正規 AP を準備した．図には省略しているが，正規の eduroam ネットワークは，AP と RADIUS サーバの他，L3 スイッチおよびルーターを用いて構築しており，外部ネットワークとは遮断されているため，インターネット接続はできない．RADIUS の設定は eduroam JP が提供する手引き[8]をもとに設定している．

表 3　実験で用いた端末

Attacker	CPU	Intel Core i7-10510U 1.80GHz
	Memory	4GB
	OS	Kali Linux
	WiFi Adapter	tp-link Archer T4U Plus Elecom WDC-867DU3S
ハッシュ解析端末	Memory	32GB
	GPU	NVIDIA GeForce RTX 3060Ti
	GPU Memory	8GB
Client	Windows 10（本体内蔵アダプター）	
	Windows 11（本体内蔵アダプター）	
	Android 8	
	Android 12	
	Fire 7	
	MacBook Pro（macOS Sequoia 15.5）	
Access Point	業務用Access Point（WPA2/3-Enterprise）	
RADIUS	FreeRADIUS（AlmaLinux 8）	

本実験で使用した端末のリストを表 3 に示す．Kali Linux は Virtual Box 上に導入した．memory は仮想環境上に付与した量である．WiFi Adapter は USB 接続している．クライアントには Windows10・11，Android8・12，Fire 端末，MacBook Pro を使用した．Access Point には業務用アクセスポイントを使用し，2.4GHz 帯と 5GHz 帯の両方を展開した．ただし，本実験では基本的にクライアントは 5GHz 帯に接続することを想定し，5GHz 帯のみに接続させている．なお，PMF は有効に設定している．

3.2 実験手順

実験の主な手順は以下の通りである．

(1) EAP Hammer と自作スクリプトを用いて，Evil Twin 攻撃を実施
(2) Evil Twin 攻撃による窃取したパスワードハッシュを解析

3.3 ケース 1 における Evil Twin 攻撃の流れ

ケース 1 では，正規の eduroam に接続中のクライアントが，攻撃者によって Evil Twin に誘導される状況を想定し，再現する．

本研究で実施したケース 1 における Evil Twin 攻撃の詳細な流れを図 4 に示す．図中の「Phase」は，以下に示す各段階と対応している．

Phase 1 : EAP Hammer を用いて Evil Twin 設置
Phase 2 : AP およびクライアントスキャン
Phase 3 : Deauthentication 攻撃の実施
Phase 4 : CSA 攻撃の実施
Phase 5 : クライアントが Evil Twin に接続

まず，Phase 1 では，EAP Hammer[9]を用いて Evil Twin を設置する．ここでは，正規 AP と同一の SSID，同一の MAC アドレス，同一のチャネルを設定した偽の AP を構築し，ユーザー端末を誘導する準備を行う．

表 4　サーバ証明書の検証を行った場合の攻撃結果概要

クライアント	Deauthentication 攻撃	CSA 攻撃	Evil Twin 攻撃（正規APあり）	Evil Twin攻撃（正規APなし）
Windows 10（本体内蔵アダプター）	○ 成功	○ 成功	× 失敗	× 失敗
Windows 11（本体内蔵アダプター）	× 失敗	○ 成功	× 失敗	× 失敗
Android 8	× 失敗	○ 成功	× 失敗	× 失敗
Android 12	× 失敗	○ 成功	× 失敗	× 失敗
Fire 7	○ 成功	× 失敗	× 失敗	× 失敗
MacBook Pro（macOS Sequoia 15.5）	× 失敗	○ 成功	× 失敗	× 失敗

表 5　サーバ証明書の検証を行わない場合の攻撃結果概要

クライアント	Deauthentication 攻撃	CSA 攻撃	Evil Twin 攻撃（正規APあり）	Evil Twin攻撃（正規APなし）
Windows 10（本体内蔵アダプター）	○ 成功	○ 成功	○ 成功	○ 成功
Windows 11（本体内蔵アダプター）	× 失敗	○ 成功	× 失敗	× 失敗
Android 8	× 失敗	○ 成功	○ 成功（※条件つき）	○ 成功
Android 12	× 失敗	○ 成功	○ 成功	○ 成功
Fire 7	○ 成功	× 失敗	× 失敗	○ 成功
MacBook Pro（macOS Sequoia 15.5）	× 失敗	○ 成功	× 失敗	○ 成功

続く Phase 2 では，周囲に存在する AP およびクライアントのスキャンを実施し，正規 AP の詳細情報（MAC アドレス，チャネル等）や攻撃対象となるクライアント端末の MAC アドレスを取得する．

Phase 3・Phase 4 では，正規 AP とクライアント間の接続を強制的に切断するため，Deauthentication 攻撃と CSA 攻撃を行う．これにより，クライアント端末は再接続先を探し始める．CSA 攻撃は Deauthentication 攻撃で Evil Twin に誘導できなかった場合に行う．

最終的に Phase 5 では，Deauthentication 攻撃および CSA 攻撃の効果により，クライアント端末が Evil Twin へ接続しようとする．これによって，Evil Twin に接続したクライアントの認証情報を窃取する．

3.4 ケース 2 における Evil Twin 攻撃の流れ

ケース 2 では，正規の eduroam が存在しない環境を想定し，ユーザーが Evil Twin に自発的に接続してしまう状況を再現する．

Phase 1: Evil Twin 設置（EAP Hammer を使用）
Phase 2:AP および クライアントのスキャン
Phase 3: クライアントが自動的に Evil Twin に接続
Phase 4: 認証情報の送信とハッシュの窃取

このケースでは，Deauthentication 攻撃や CSA 攻撃のような強制的な誘導手法は用いず，クライアントが既知の SSID に対して自動接続を試みる性質を利用している．特に，eduroam のような学術ネットワークにおいては，一度接続したことのあるネットワークに自動的に再接続する設定となっていることが多く，Evil Twin によるなりすまし接続が成立しやすい．

3.5 パスワードハッシュの解析手法

攻撃によって窃取されたパスワードハッシュは、EAP 認証の過程で取得されたものであり、主に MSCHAPv2 に由来するチャレンジ-レスポンスの形式（NetNTLM）である。以下の手順で解析を実施した．

1. EAP Hammer により取得されたパケットから，チャレンジとレスポンスの情報を抽出
2. 抽出した情報を hashcat に対応する形式に変換
3. オフライン環境にて，hashcat を用いて総当たり攻撃を実施
4. 解析の成否および処理時間を記録し評価

本研究では，本学の eduroam における認証で使用されるパスワードの要件に基づき，試験的に英数字 8 桁のパスワードを想定し，オフライン環境におけるパスワード解析に要する時間を計測した．

パスワードの解析は総当たり攻撃（ブルートフォース）により実施し，解析時間の短縮を図るため，hashcat のオプションを用いて「英数字 8 桁」の形式に限定して実行した．

なお，本学が定める eduroam のパスワード要件は「英小文字・英大文字・半角数字・半角記号のうち，少なくとも 3 種類以上の文字種を 1 文字以上含めること，かつ，8 文字以上 31 文字以内で構成すること」とされている．本研究では，ユーザーが設定しやすく，かつ本学が配布する初期パスワードのパターンとして一般的に用いられている「英数字 8 桁」の形式に限定して検証を行った．

4. 実験結果

本章では，ケース 1（正規の eduroam が存在する環境）およびケース 2（正規の eduroam が存在しない環境）において，各種攻撃手法がクライアントに対して成功したかどうかをまとめ，またサーバ証明書の検証有無が接続挙動に及ぼす影響について評価した．

4.1 ケース 1 の実験結果

このケースでは，正規 AP の電波が届いている状況で Evil Twin 攻撃を実施した．表 4 および表 5 に結果を示す．

4.1.1 サーバ証明書検証を有効している場合

表 4 にサーバ証明書検証を有効にしている場合の結果を示す．クライアントはいずれも Evil Twin への接続を試みたものの，サーバ証明書の検証に失敗した．したがって，サーバ証明書の検証が有効な防御機構として働いていることが確認できた。

4.1.2 サーバ証明書検証を無効にしている場合

表 5 にサーバ証明書検証を 無効にしている場合を示す．Android 系端末や Windows10 は，CSA 攻撃をきっかけに Evil Twin に接続する挙動が確認された．Android8 に関しては，5.4 節でも述べるが，Evil Twin の MAC アドレスを正規 eduroam （5GHz） と同じにした場合のみ成功した．Windows11 では CSA 攻撃の成功後にも Evil Twin への接続は行われなかった．Fire 7 では Deauthentication 攻撃の成功後にも Evil Twin への接続は行われなかった．以上より，サーバ証明書検証が無効な設定では，正規の eduroam の存在下でも Evil Twin に接続してしまう可能性があることがわかった．

4.2 ケース 2 における実験結果

このケースでは，クライアントが正規の eduroam の電波を受信できない環境下に置かれた状態で，Evil Twin 攻撃を実施した．表 4 および表 5 に結果を示す．

4.2.1 サーバ証明書検証を有効している場合

クライアントはいずれも Evil Twin に接続を試みるものの，サーバ証明書の検証に失敗したため，すべての接続が拒否された。したがって，サーバ証明書の検証が有効な防御機構として働いていることが確認できた。

4.2.2 サーバ証明書検証を無効にしている場合

Windows11 以外のクライアントが Evil Twin に自動的に接続し，攻撃が成功した．特に，正規の eduroam が存在しない環境ではクライアントが接続先の AP を選定する基準が弱まるため，サーバ証明書の検証が無効である設定では攻撃が極めて有効となる．

以上のように、サーバ証明書検証が無効である場合，正規 AP の有無に関わらず Evil Twin 攻撃が成功する可能性があることが確認された．一方で，証明書検証を有効にすることで，CSA 攻撃や Evil Twin 攻撃による接続の乗っ取りを防げることが示された．

4.3 パスワード解析結果

本研究では，パスワードの解析は総当たり攻撃（ブルートフォース）により実施し，解析時間の短縮を図るため，hashcat のオプションを用いて「英数字 8 桁」の形式に限定した．その結果，6 回平均で 56 分 24 秒であった．

5. 考察

本実験では，正規の eduroam が存在するケース（ケース 1）および存在しないケース（ケース 2）それぞれにおいて，クライアント端末が Evil Twin に接続するかどうかを観察した．また，クライアント端末のサーバ証明書検証設定の有無による差異も検証した．

5.1 ケース 1（正規 AP の電波が届く範囲内）

サーバ証明書の検証を無効にしている場合，CSA 攻撃や Deauthentication 攻撃によってクライアントが正規の AP から切断され，Evil Twin へと接続してしまうことが確認された．このとき，サーバ証明書の検証が行われないため，ユーザーは偽の AP に気づかず，認証情報が窃取されるリスクが高い．ただし，サーバ証明書の検証が無効な端末であっても，Evil Twin に容易に接続されるケースは少なく，Evil Twin の電波強度が正規 AP よりも弱い場合，Evil Twin に接続しづらく，図 1 に示す EAP 通信の初期処理（Authentication request/response）までは完了するものの，その後の認証に失敗するケースなどが散見された．

一方，サーバ証明書検証を有効にしている場合，Evil Twin への接続を試みた際に接続が拒否されたりする挙動が見られた．したがって，サーバ証明書の検証設定は，ケース 1 において攻撃の成立を防ぐ重要な要因であることが示された．

表 6　CSA 攻撃の成否 : 環境条件および パラメーターごとの比較

指定チャネル	Evil Twinの有無	成否	備考
正規AP(2.4GHz)と同じチャネル	あり	○ 成功	Evil Twinは任意のMACアドレス
	なし	× 失敗	
正規AP(5GHz)と同じチャネル	あり	検証不可	Evil Twinは任意のMACアドレス
	なし	×失敗	
正規APが存在しないチャネル	あり	○ 成功	
	なし	× 失敗	

表 7　Evil Twin 攻撃の成否 : MAC アドレスとチャネルの関係による比較

No.	MACアドレスの関係	チャネルの関係	例（MAC, ch）	成否	備考
1	正規AP（2.4GHz）と同一	正規AP(2.4GHz)と同一	○○:c8, ch:1	○成功	Windows10・Android12で Evil Twin 攻撃が成功
2	正規AP（2.4GHz）と同一	正規AP(2.4GHz)と異なる	○○:c8, ch:11	×失敗	オープン認証までは完了
3	正規AP（5GHz）と同一	正規AP(2.4GHz)と同一	○○:cc, ch:1	○成功	Android8・MacBook Proで Evil Twin が成功
4	正規AP（5GHz）と同一	正規AP(2.4GHz)と異なる	○○:cc, ch:11	×失敗	
5	異なるMAC	正規AP(2.4GHz)と同一	○○:10, ch:1	×失敗	
6	異なるMAC	正規AP(2.4GHz)と異なる	○○:10, ch:11	×失敗	

5.2 ケース 2（正規 AP の電波が届かない範囲）

この環境では，クライアントが受信可能な SSID が Evil Twin のみであるため，サーバ証明書検証を無効にしている設定では，クライアントが Evil Twin を正規の AP と誤認し，自動的に接続してしまうケースが確認された．このことは，学外や公共の Wi-Fi 環境など，正規の eduroam が存在しない場所においても，同様のリスクが存在することを示唆する．

Evil Twin に接続してしまった端末の内，Android12 と MacBook Pro においては，PEAP-MSCHAPv2 で正規 eduroam に接続したにもかかわらず，PEAP-GTC で Evil Twin に接続してしまい，平文パスワードの入手に成功してしまうケースがあった．この事から，たとえ，Phase2 認証を強固な方式に設定していても，クライアントが Evil Twin に対しては脆弱な認証方式で接続してしまう可能性があると考える．

一方，サーバ証明書の検証が有効である場合には，サーバ証明書の検証失敗により，Evil Twin との接続が阻止され，ユーザーの認証情報が保護される結果となった．ただし，実験で使用した macOS におけるサーバ証明書の検証とは，ユーザー自身が提示された証明書のドメイン名や発行元を目視で確認し，正当な接続先かどうかを判断する行為であった．そのため，ユーザーが証明書の内容を正しく理解していない場合や確認を怠った場合には，誤って Evil Twin に接続してしまう可能性がある．

したがって，両ケースともに，証明書検証が有効であれば攻撃を未然に防ぐことが可能であり，その重要性が再確認された．

5.3 CSA 攻撃の成功条件

表 6 に示すように，CSA 攻撃は，Evil Twin が正規 AP と同一チャネルに存在し，かつ同一の MAC アドレスを使用している場合において，特に高い成功率を示した．なお，表 6 にある検証不可とは， 使用した Wi-Fi アダプターで 5GHz 帯の Evil Twin を立てることができなかったため，検証不可能だったことを示す．

表 6 に示す結果について，詳細は以下の通りである．

移動先チャネルに Evil Twin が存在しない場合，クライアントが CSA を受信しても，正規 AP が提供するもう一方のバンド（例:2.4GHz 帯→5GHz 帯）へとチャネルを切り替えてしまう挙動が確認された．このように，CSA をトリガーとしてチャネルを変更しても，それが Evil Twin の存在する．

このことから，CSA 攻撃の成功にはチャネルの移動先に，「正規 AP と同一チャネル&SSID の AP」が存在することが鍵であるといえる。

特に，正規 AP と同じ SSID の AP が同一チャネル上に存在しない場合，CSA を受信したクライアントが Evil Twin のチャネルではなく，正規 AP が提供する別バンドのチャネルへと移動する挙動が観測された．これは，eduroam のように 2.4GHz 帯と 5GHz 帯の両方を提供する環境では，CSA 攻撃の成功を困難にする要因の一つであるといえる．

一方で，2.4 節に示したように，CSA 攻撃に関する先行研究では，CSA を含む偽ビーコンを通常のビーコンと同じ間隔で送信し続けることで，クライアントが New Channel Number に従ってチャネルを切り替え，通信不能に陥ることが報告されている．この攻撃は Channel Switch Mode を 1、Channel Switch Counter を 0 とした CSA パケットを利用している．

しかしながら，本研究の環境では，正規 AP が 2.4GHz 帯と 5GHz 帯の両方で電波を提供しているという構成の影響もあったのか，先行研究どおりに CSA 攻撃が常に成立するわけではなかった．特に， 複数バンドの存在が，クライアントのチャネル選択アルゴリズムに影響を与えた可能性が考えられる．

以上のことから，CSA 攻撃は理論上の成立条件を満たしていても，実際の環境におけるバンド構成やクライアント側の挙動により大きく成功率が左右される攻撃手法であると結論づけられる．

5.4 Evil Twin 攻撃の成功条件（MAC アドレス・チャネルの関係）

表 7 に示すように，Evil Twin 攻撃において，様々なパターンを検証した結果，Evil Twin が正規 AP と同一のチャネル・MAC アドレスを模倣しているかどうかが成功可否に大きく影響することがわかった．

正規 AP の MAC アドレスは下位 2 桁のみ異なっており，「2.4GHz 帯が C8」，「5GHz 帯が CC」となっていた．チャネル設定は自動であったが，表 7 との対応を明確にするため，「2.4GHz 帯のチャネルは 1」であると仮定する．なお，表 5 には，「正規 AP（5GHz 帯）と同一のチャネル」の項目が存在しないが，これは 5.3 節でも述べた通り，使用した Wi-Fi アダプターでは 5GHz 帯の Evil Twin を構築できなかったためであり，検証不可能であったことによる．

検証の結果，正規 AP と同じ MAC アドレス・同じチャネルを使用した場合，多くの端末で Evil Twin への接続が成立，またはオープン認証まで進んだ．

一方で，正規 AP と異なる MAC アドレスを使用した場合，同じチャネルであっても，端末は Evil Twin に接続しなかった．

また，Evil Twin 攻撃が成功した端末においても，すべてが同一条件で成功したわけではなく，端末ごとに挙動の違いが見られた．

以上から，Evil Twin 攻撃の成否は，端末の仕様による差異も影響するが，特に Evil Twin の MAC アドレス・チャネルの設定が主要な成功要因であると考えられる．

5.5 パスワード解析

本実験では，「英数字 8 桁」のパスワード解析を実施した．その結果，6 回分の平均解析時間は 56 分 24 秒であり，この程度の複雑性であれば，条件を限定したうえで hashcat を用いることで，安価な GPU でも比較的短時間で解析が可能であり，極めて脆弱であることが明らかとなった．なお，hashcat の試算では，全探索に最長約 2 時間を要すると出力された．

また，本実験では実施していないが，同条件に記号を加えた場合，hashcat の試算では解析に約 4 日を要すると出力された．このことから，攻撃者視点においては，まず英数字など強度の低い組み合わせを優先的に試行することで，解析時間を大幅に短縮できると考えられる．

なお，青山らの研究では，小文字 8 桁のパスワードに対し，NVIDIA V100 Tensor Core GPU を用いた実験で，2 回平均 21 分 45 秒で解析を完了したと報告している．本研究では小文字 8 桁で解析をしていないが，両者の結果を踏まえると，安価な GPU であっても青山らの結果と大きく変わらない解析性能を示す可能性があると考えられる．ただし，青山らの研究で使用された hashcat コマンドの詳細設定が不明なため，この推測には一定の留保が必要である．

6. まとめと今後の課題

本研究では、模擬環境 eduroam における Evil Twin 攻撃の有効性とそれに対する防御策としてのサーバ証明書の検証の重要性について検証を行った．

第一に，サーバ証明書の検証の有無が Evil Twin 攻撃の成否に直結することを，複数のクライアント端末を用いた実験により確認した．これにより，サーバ証明書の検証が，

Evil Twin 攻撃を防止する有効な防御手段であることを再確認した．

第二に，CSA 攻撃については，その成功条件を実験的に明らかにした．具体的には，正規 AP が複数バンドを提供している場合，Evil Twin が正規 AP と同一のチャネルに設置されている場合に限り，攻撃が成立することを確認した．逆に，これらの条件が揃わない場合にはクライアントは CSA 情報を無視し，攻撃は無効化されることがわかった．

また，クライアントの種類や OS バージョンによって，Evil Twin 攻撃や CSA 攻撃に対する耐性に違いが見られたことも重要な発見である．例えば，Android 12 と MacBookPro では GTC 方式で接続処理が進むケースがあり，結果として平文でのパスワード窃取が可能となった．一方で，EAPHammer によって生成される Evil Twin が EAP-SHA1-TKIP を使用するため，それをサポートしないクライアントが接続できないケースも確認された．

これらの結果は，eduroam を運用する学術機関および研究機関において，「サーバ証明書検証の徹底を端末側で確実に行わせること」および「端末側でのセキュアな CSA の実装」が極めて重要であることを示す．

今後の課題としては，まず，Android や Windows といった異なる OS において，Evil Twin 攻撃において挙動が異なるが，その挙動の根拠が明確でないため，さらなる挙動分析が必要である．加えて，本研究では Evil Twin による認証情報の窃取に EAPHammer を使用したが，airgeddon など他のツールによる攻撃との違いについても検証することで，攻撃成立条件の一般化が進むと期待される．さらに，パスワード解析についても，より多様な条件下での検証を行う必要がある．最後に， Enterprise 方式のネットワークに対して，自動検出・選択およびシームレスなアクセス・ローミングを可能とする技術に Passopoint[10]がある．これの技術は，安全な Wi-Fi 自動接続の仕組みとして注目されており，将来的には，eduroam にも導入が進むと予想されているため，Passpoint 対応環境における Evil Twin 攻撃の可能性についても検討を進めていきたいと考える．

謝辞

本研究の一部は，JSPS 科研費 JP22K11982 の助成を受けたものです．

参考文献

[1] 国立情報学研究所 学術基盤推進部 学術基盤課 eduroam 担当，“eduroam JP の概要 | eduroam”， 国立情報学研究所 学術基盤推進部 学術基盤課 eduroam 担当，https://www.eduroam.jp/about，参照 June．1，2025.

[2] 国立情報学研究所 学術基盤推進部 学術基盤課 eduroam 担当，“国立情報学研究所 eduroam JP サービス技術基準・運用基準”，国立情報学研究所 学術基盤推進部 学術基盤課 eduroam 担当，https://www.eduroam.jp/sites/default/files/2024-08/%E5%9B%BD%E7%AB%8B%E6%83%85%E5%A0%B1%E5%AD%A6%E7%A0%94%E7%A9%B6%E6%89%80%20eduroam%20JP%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E6%8A%80%E8%A1%93%E5%9F%BA%E6%BA%96%E3%83%BB%E9%81%8B%E7%94%A8%E5%9F%BA%E6%BA%96.pdf ， 参照 June．1，2025.

[3] Cisco，” WLC での 802.11w 管理フレーム保護の設定”，Cisco，https://www.cisco.com/c/ja_jp/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html. 参照 June．1，2025.

[4] NPO 日本ネットワークセキュリティ協会 2002 年度 相互接続ワーキンググループ，” 802.1X 相互接続実験報告書”，NPO 日本ネットワークセキュリティ協会，https://www.jnsa.org/houkoku2002/musenlan2002.pdf, 参照 June．1，2025.

[5] 窪田恵人，五十部孝典，森井昌克，無線 LAN 機器に対する DoS 攻撃の実装と評価，コンピュータセキュリティシンポジウム 2019 論文集，p. 1079-1085，（2019）．

[6] Ivan Palamà，Alessandro Amici，Gabriele Bellicini，Francesco Gringoli ，Fabio Pedretti ，Giuseppe Bianchi,Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments,Computer Communications，Volume 212，（2023）．

[7] 青山 諒仁，鈴木 彦文，岡崎 裕之，クラウド GPU サービスを活用した 2 段階 EvilTwin 攻撃の実装と評価，学術情報処理研究,2024, 28 巻, 1 号, p. 23-29,（2024）．

[8] 国立情報学研究所 学術基盤推進部 学術基盤課 eduroam 担当，“利用者向け情報”，国立情報学研究所 学術基盤推進部 学術基盤課 eduroam 担当，https://www.eduroam.jp/for_users．参照 June．1，2025.

[9] s0lst1c3，“GitHub - s0lst1c3/eaphammer: Targeted evil twin attacks against WPA2-Enterprise networks. Indirect wireless pivots using hostile portal attacks.”，https://github.com/s0lst1c3/eaphammer．参照 June．1，2025.

[10] Wi-Fi Alliance，”Passpoint | Wi-Fi Alliance”，https://www.wi-fi.org/ja/access，参照 June．1，2025.