キャンパス内の不正アクセスポイントを無線フレームの復号なく検出する手法

竹田　智洋[†a)]　大平　健司[††]　谷岡　広樹[††]　佐野　雅彦[††]
松浦　健二[††]　上田　哲史[††]

A Method to Detect Rogue Access Points in a Campus without Decrypting WLAN Frames

Tomohiro TAKEDA[†a)], Kenji OHIRA[††], Hiroki TANIOKA[††], Masahiko SANO[††], Kenji MATSUURA[††], and Tetsushi UETA[††]

あらまし　大学に無線 LAN アクセスポイント（以下，AP と呼ぶ）を導入するに当り，許可を得ず接続された AP や正規の AP を装った AP 等の不正 AP に関するセキュリティ上の課題が存在する．大学では，全学としてのネットワーク管理者（以下，全学ネットワーク管理者と呼ぶ）だけでなく，各サブネットワークごとに管理者を指定していることが多く，ネットワーク全体を把握している管理者が存在しない可能性がある．本論文では，全学ネットワーク管理者の視点で，サブネットワーク管理者との連携を追加で要することなく，検査対象 AP のキャンパスネットワークへの接続の有無を判断することにより不正 AP を検出する手法について提案する．提案手法では，Windows や Android 等の OS に導入されている，Captive Portal Detection（以下，CPD と呼ぶ）を利用する．キャンパスネットワークの上流と無線 LAN 通信区間の二箇所における CPD 用 HTTP 通信の時間差から，検査対象 AP のキャンパスネットワークへの接続を確認する．なお，本手法では無線 LAN での通信において，WPA2 等の復号を行わず推定している．評価実験では，提案手法によりネットワーク上流から見た各サブネットワークの IP アドレスと無線 LAN クライアントが接続した AP の紐付けが可能であることを確認した．

キーワード　キャンパスネットワーク，不正アクセスポイント，キャプティブポータル，無線 LAN

1. まえがき

大学に無線 LAN アクセスポイント（以下，AP と呼ぶ）を導入する際，許可を得ず接続された AP や正規の AP を装った AP がセキュリティ上の課題の一つになっている．これらの AP は不正アクセスの入り口になることがあり，情報漏洩等のセキュリティリスクを高めている．

大学は対外的には一つの組織であるが，その歴史的経緯の中で特に学問の自由や部局の自治への考慮が求められており，その結果，基幹ネットワークを管理する全学としてのネットワーク管理者（以下，全学ネットワーク管理者と呼ぶ）だけでなく，接続する各サブネットワークに対し，それぞれ管理者（以下，サブネットワーク管理者と呼ぶ）を指定し分散管理していることが多い．

大学では端末をキャンパスネットワークに接続する際に，一般的に不正アクセス対策や情報の機密性の保持といった一定の接続基準を設けているが，端末の接続についての基準の具体化は各サブネットワーク管理者に委ねられることが多い．よって，大学に対して不正アクセス関連の問合せがあった場合，全学ネットワーク管理者は，IP アドレスからサブネットワーク管理者を特定し，問合せを行うことにより原因を特定している．

全学ネットワーク管理者が不正アクセスを防止す

† 徳島大学大学院先端技術科学教育部，徳島市
Graduate School of Advanced Technology and Science, Tokushima University, 2–1 Minamijosanjima–cho, Tokushima-shi, 770–8506 Japan
†† 徳島大学情報センター，徳島市
Center for Administration of Information Technology, Tokushima University, 2–1 Minamijosanjima–cho, Tokushima-shi, 770–8506 Japan
a) E-mail: takeda@na3alf6.info
DOI:10.14923/transcomj.2017GTP0013

るべく，キャンパス内に接続された全ての AP の情報を得ようとすると，全てのサブネットワーク管理者との情報連携が追加で求められる．よって，全学ネットワーク管理者は，キャンパスネットワークを維持するための既存の管理コストとは別に，追加管理コストが発生する．

一般的に分散管理するに当り，役割をモジュール化し，各管理者の独立性を高めることにより，情報連携のコストを下げることができる．本提案手法では全学ネットワーク管理者がキャンパス内に接続された全ての AP を常に管理する必要性を排することで，全学ネットワーク管理者が手元のリストの維持に掛けなければならない労力を削減し，サブネットワーク管理者においてはより柔軟なネットワーク構成変更を可能とするものである．

全学ネットワーク管理者は，大学として接続している AP の管理と，所属不明の AP がキャンパスネットワークのセキュリティリスクを高めていないかどうかの監視を行う必要がある．また，サブネットワーク管理者は，各々が受けもつサブネットワークのみ監視を行う必要がある．近年，スマートフォンのテザリング機能などもち運び可能な AP の普及により，全学ネットワーク管理者は，管理外の AP を無条件に不正を行っている AP であると判断することはできなくなった．キャンパス内に設置された管理外の AP の中から，不正な AP を検出することは，両管理者が情報連携を行ったとしても，大変困難なものになった．

本論文では，ユーザがキャンパスネットワークに接続することを意図して使用される AP の内，キャンパスネットワークに許可を得ずに接続された AP を第一種不正 AP と定義する．また，大学が管理している AP の ESSID を発信しているが BSSID が管理外のものであるなど，大学が導入した正規の AP を装った AP を第二種不正 AP と定義する．この二つを不正 AP とし，検出すべき対象とした．検査対象 AP の通信内容を復号することなくキャンパスネットワークへの接続の有無を判断することにより，不正 AP を検出する手法について提案する．

本提案手法では，キャンパスネットワークへの接続の有無の確認にサブネットワーク管理者との常時の連携を要さないため，全学ネットワーク管理者の管理コストを抑えることが期待される．

2. 従来手法

不正 AP の検出方法として，大別して以下の 3 種類の手法が提案されている．

- 有線 LAN 側から検出する手法
- 無線 LAN 側から検出する手法
- 双方からのデータを用いて検出する手法

2.1 有線 LAN 側から検出する手法

有線 LAN 側でトラヒックを観測し，観測点より下流での無線 LAN の使用を推定する手法がある．

無線 LAN のアクセス制御には CSMA/CA 方式を用いる．CSMA/CA 方式により端末の通信が競合しないように制御しているが，この方式は他端末が通信をしていない場合でもすぐに通信を開始しないため有線 LAN に比べレイテンシが大きい．この特徴を利用し Beyah らは，レイテンシの特徴から無線 LAN で接続されている機器を推定している [1]．Xie らは，特にレイテンシの揺れに注目した検出手法を提案している [2]．また Watkins らは，RTT を用いた検出アルゴリズムを提案している [3]．これらの手法 [1]～[3] は，有線 LAN 側において，AP が接続されていないネットワークで無線 LAN の特徴をもったレイテンシが観測された場合，不正 AP が接続されているとみなすことができる．しかしながら，無線 LAN の高速化に伴い，レイテンシの縮小や揺れ幅の減少が原因で，正しく検知できない場合が増加している．また，パケットの TTL を確認し，AP を経由しているか確かめる手法もあるが，無線 LAN クライアントからネットワーク上流の観測点までのルータなどの接続数が既知のときのみ使用可能である．キャンパスネットワークはサブネットワークごとに管理者が異なることが多く，ネットワーク全体の構成を把握することが困難であるため，この手法は不適である．

2.2 無線 LAN 側から検出する手法

無線 LAN 側で検出する方法は，目的別に 2 種類存在する．

- 無線 LAN クライアント自身が検知を行う手法
- 暗号化されていない情報を元にして不正 AP を検出する手法

無線 LAN クライアント自身が検知を行う手法は，無線 LAN クライアントが偽装された AP に接続した際に，情報が流出するリスクを低減するために用いられる．Han らは，対象 AP への Probe Request と DNS の RTT を用いて検出している [4]．

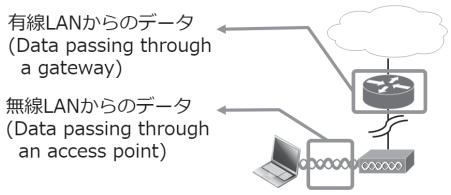

図 1　データ取得点
Fig. 1　Packet capture points.

暗号化されていない情報を元にして不正 AP を検出する手法は，無線 LAN による通信をキャプチャし，解析することで実現される．Thakur らは事前に正規 AP の SSID や BSSID，使用チャネル等を登録しておき，検査対象の AP の発する情報と比較することにより，不正 AP を検出している [5]．Jagtap らは，SSID や BSSID の他に信号強度の変化を監視し，不正 AP の判断材料にしている [6]．

しかしながら，これらの手法 [4]～[6] により不正 AP を検出するためには，事前にキャンパス内に接続された AP を全て把握する必要があり現実的ではない．また，Han らによる手法 [4] は，実際に AP に接続するため，正規の AP を装った AP を検出することは可能であるが，無許可で接続された AP を検出することができない．またこの手法は，検査対象 AP の通信を復号しなければならない．これはキャンパス内の全ての AP への認証情報を全学ネットワーク管理者が保持しなくてはならず，現実的ではない．

2.3　双方からのデータを用いて検出する手法

有線 LAN/無線 LAN の双方からのデータ（図 1）を用いて検出する手法として，川田らは無線 LAN/有線 LAN のトラヒックの相関から，両者のフローの比較によって識別する手法を提案している [7]．この手法は，検査対象 AP のキャンパスネットワークへの接続を判断できるが，無線 LAN による通信の内，有線 LAN 側の観測点を通過しない通信が多いと正しく検知できない．

3.　提 案 手 法

3.1　提案手法が解決する問題点と利点

本提案手法では，従来手法での問題点である以下の 5 点の問題を解決する．

（1）　レイテンシによる検出の難化
（2）　未知のネットワークに対する TTL による検出の困難性
（3）　ネットワーク全体を把握し検査する困難性
（4）　トラヒックの相関性による検出の困難性
（5）　無線の通信を復号する必要性

（1）と（2）の問題に対し，有線 LAN/無線 LAN 双方からのデータを用いた，レイテンシや TTL とは異なる指標により判断することで解決している．

（3）の問題に対し，全学ネットワーク管理者はネットワーク全体の把握を要することなく，検査対象 AP のキャンパスネットワークへの接続の有無を確認することにより解決している．

（4）の問題に対し，トラヒック量に着目せず，特定の HTTP 通信のレスポンスを推定し，リクエストとレスポンスの時間差をもとに検出することで解決している．

（5）の問題に対し，認証フレーム並びに無線フレームのサイズから特定の通信の推定を行うことにより，復号を要することなく検出する．よって全学ネットワーク管理者は，復号手段としての ID やパスワードといった情報を部局管理者に要求することなく検出可能である．

3.2　提案手法が依拠する通信

無線 LAN クライアントがインターネットへアクセスする前に，接続したネットワークから無線 LAN クライアントに対して特定のウェブサイトとの通信を要求する Captive Portal（以下，CP）と呼ばれる仕組みが存在する．一般的な公衆無線 LAN サービスでは，最初にインターネットに接続する際に，規約への同意や認証を行うためにこの仕組みが使用される．しかしこの CP が使用されていると，利用者が本来期待している TLS 証明書を正常に取得できず，TLS 証明書の検証が失敗する等，様々な問題を引き起こすことが知られている [8]．そのため Windows や Android 等の OS には CP を検出するための Captive Portal Detection（以下，CPD）と呼ばれる機能が搭載されている．本提案手法ではこの CPD により送出されるパケットを利用する．

CPD には様々な手法が存在する．Windows 10 を搭載した無線 LAN クライアントが AP に接続し，DHCP で IPv4 のアドレスを取得した場合，最初に DNS で特定のドメインの名前解決を行う．次に名前解決により取得した IP アドレスに対して，HTTP を用いて特定のファイルを取得する．最後に取得したファイルを検証し，正しいファイルであればインターネットに接続されているとみなす．Android 6.0 以前の場合も同

図 2　インターネット接続エラー表示（Windows 10）
Fig. 2　An error indication of Internet connection in Windows 10.

図 3　インターネット接続エラー表示（Android 6.0）
Fig. 3　An error indication of Internet connection in Android 6.0.

様である．インターネットに接続されていないと判断された場合の表示を，Windows 10 については図 2 に，Android 6.0 については図 3 に示す．

3.3 原　　理

本提案手法では，無線 LAN クライアントと AP の間の無線通信区間とキャンパスネットワークの上流の 2 箇所に観測点を設ける．CPD で流れる HTTP 通信のリクエストは，上流側観測点から取得する．CPD で流れる HTTP 通信のレスポンスは，無線通信区間側の観測点から取得するフレームを解析し推定する．このレスポンスに対応するリクエストを，上流側観測点から得られたリクエストより求めることにより，両者の検出時刻の差（以下，時間差）を計算することができる．時間差は，検査対象 AP がキャンパスネットワークに接続されていた場合，一定の範囲に集中する．よって，全学ネットワーク管理者は，提案手法により求まる時間差により，検査対象 AP のキャンパスネットワークへの接続の有無を判断することができる．

全学ネットワーク管理者は，不正 AP を検知するに当り，まずキャンパス内の無線フレームを監視する．無線フレームから，キャンパス内で動作している AP を把握することが可能である．それぞれの AP に関して，ESSID や BSSID を確認することにより，大学が導入したものか，それ以外かを把握することが可能である．また，提案手法により，その AP がキャンパスネットワークに接続されているかどうかを確認することが可能である．大学が導入していない AP であり，キャンパスネットワークに接続されている AP の場合，その AP は第一種不正 AP の可能性がある．大学が管理している ESSID を発信する AP であり，BSSID が管理外のものである場合，その AP は第二種不正 AP の可能性がある．

第一種不正 AP の可能性がある AP の場合，提案手法により，AP が接続されている IP アドレスが判明するため，その IP アドレスが所属するサブネットワークの管理者に，迅速に連絡を取ることが可能である．全学ネットワーク管理者は AP の物理的な位置を確認することなく担当のサブネットワーク管理者を特定することが出来，容易に問合せを行うことが可能になる．

第二種不正 AP の可能性がある AP の場合，キャンパスネットワークに接続されていれば，提案手法により求まる IP アドレスにより，キャンパス内の接続されているサブネットワークを把握できる．想定外のサブネットワークに接続されている場合は，その AP を第二種不正 AP であると判断し，第一種不正 AP と同様に，担当のサブネットワーク管理者に問合せを行うことにより対処を行う．キャンパスネットワークに接続されていなければ，第二種不正 AP である可能性はあるが，本提案手法では対処することができない．

3.4 データ取得

まずデータの取得について述べる．CPD で用いられる HTTP 通信のパケットを取得するため，無線 LAN クライアントと AP の間の通信区間とキャンパスネットワークの上流の 2 箇所に観測点を設ける．キャンパスネットワーク上流の観測点は，CPD で用いられる HTTP 通信のパケットが流れる経路上に設置する（図 4 の wired capture point）．キャンパスネットワークから外部ネットワークへの通信が全て通過する経路上に観測点を設定するのが望ましい．外部への通信が観測点を通過しないキャンパスネットワークが存在する場合，そのネットワークは検査対象外になる．無線 LAN クライアントと AP の間の通信区間に設けた観測点は，検査対象 AP とその AP に繋がる無線 LAN クライアントの通信を観測する（図 4 の wireless capture point）．検査対象 AP と物理的に距離が近い場所への設置が望ましい．距離が遠いと無線フレームを正しく取得できない可能性がある．

次に観測するデータについて述べる．キャンパスネットワーク上流の観測点では，CPD で流れる HTTP 通信の GET リクエストのみ観測する．キャンパスネッ

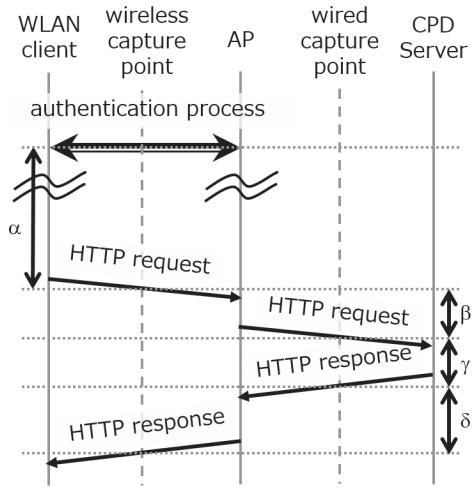

図 4　提案手法の時間差
Fig. 4　A time difference.

トワーク上流はネットワークトラヒック量が膨大であることが多く，全てのパケットの保存が困難であることが多いためである．HTTP 通信の GET リクエストに該当するパケットは，HTTP ヘッダを確認することにより容易に識別できる．CPD で流れる HTTP 通信の GET リクエストを観測することにより，そのパケットがキャンパスネットワーク上流の観測点を流れた時刻，OS，並びに観測点から見た IP アドレスが分かる．

無線 LAN クライアントと AP の間の通信区間に設けた観測点では，認証フレーム並びに，そのフレームが検出された後に流れるフレームの内，CPD で流れる HTTP 通信のレスポンスと推定されるフレームのみを取得する．近年，一般的に無線での通信内容は暗号化されているため，データを復号することは困難であるが，認証フレームは，無線フレームのヘッダにそのフレームの種類が記されているため，その他のフレームと識別可能である．CPD は無線 LAN クライアントが AP に接続した直後に実行されるため，認証フレームが流れた直後の数秒間（図 4 の α）フレームを解析する．一般に CPD で流れる HTTP 通信のレスポンスのデータ部のサイズは OS ごとに一定である．よって本提案手法は，認証フレームが流れた直後に，データ部が特定のサイズであるフレームが流れたかを確認することにより，CPD で用いられる HTTP 通信のレスポンスを推定している．推定したフレームにより，CPD で流れる HTTP 通信のレスポンスが無線 LAN クライアントと AP の間の通信区間に設けた観測点を流れた時刻，OS 並びに無線 LAN クライアントと AP の MAC アドレスが分かる．

3.5　データ解析

それぞれの観測点より得られた情報により解析を行う．まずはキャンパスネットワーク上流の観測点（図 4 の wired capture point）からのデータを，キャンパス内の通信元の IP アドレスに基づき分離し，それぞれを分離済み上流データとする．それぞれの分離済み上流データに対し，無線 LAN からのデータと比較を行う．比較は，無線 LAN クライアントと AP の間の通信区間に設けた観測点 (図 4 の wireless capture point）から得られた，CPD で流れる HTTP 通信のレスポンスと推定されるフレームを基準にする．

無線 LAN クライアントと AP の間の通信区間に設けた観測点で推定したフレームと同一の OS で，尚かつ最も時刻の近いパケットを分離済み上流データから選択し，基準のフレームと選択したパケットの時間差を求める．全ての推定したフレームに対して時間差を求め，その時間差が一定の範囲に集中していると，比較した分離済み上流データに対応するキャンパス内の IP アドレスに AP 接続されていると判断する．ただし各機器の時刻はできる限り同期されているものとする．

検査対象の AP がキャンパスネットワークに接続されていた場合は，提案手法の時間差は CPD で流れる HTTP 通信の，送受信に掛かる時間に対応する（図 4 の $\gamma+\delta$）．よって無線 LAN クライアントではなく CPD で用いられるサーバーに依存し，一定の範囲に集中する．

AP がキャンパスネットワークに接続されている場合，無線での通信区間で CPD で用いられる通信が検出されると，おおよそ同時刻にキャンパスネットワークの上流でも検出される．よって，双方で検出された CPD で用いられる通信の時間差が一定の範囲内であれば，検査対象 AP がキャンパスネットワークに接続されているとみなすことができる．

なお，キャンパスネットワークに接続され高頻度に CPD パケットを送受する AP（以下，AP′）が存在した場合，AP′ の IP アドレスと対応関係があると誤って結論する可能性がある．この可能性を除去するべく，AP′ が一様な確率分布で τ 秒に一つ CPD パケットを送受するものとして，その時間差の標準偏差 σ' を算出し，これと観測結果から得られる時間差の標準偏差 σ を比較する．何らかの有意水準において，σ の信頼

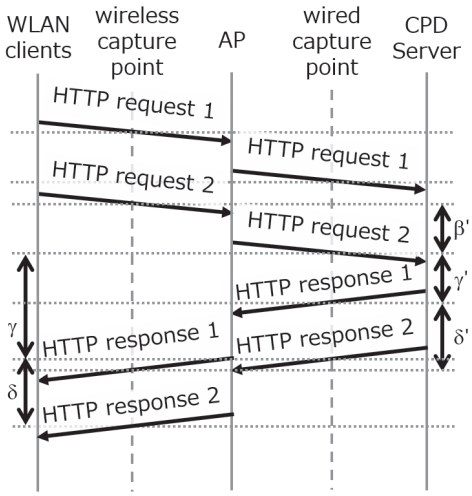

図 5　想定される誤差
Fig. 5　An expected error.

区間上限が σ' より小さい場合のみ，AP′ が一様な確率分布で τ 秒に一つ CPD パケットを送受するという仮説が成立する範囲内で，検査対象 AP がキャンパスネットワークに接続されているとみなす．

3.6　想定される誤差

提案手法では，複数の無線 LAN クライアントが同一の AP に対し，ほぼ同一の時刻に接続した場合，CPD で流れる HTTP 通信の GET リクエストとレスポンスの対応関係に齟齬が生じる可能性がある．実際の提案手法による時間差（図 5 の $\beta'+\gamma'+\delta'$）が，提案手法により求めたい時間差（図 5 の $\beta'+\gamma+\delta$）より短い時間を導き出す可能性がある．提案手法では，求まる時間差のばらつきにより検査対象 AP がキャンパスネットワークに接続されているかを判断しているため，実際の時刻より短い場合でも判断可能である．また，各機器の内部時計のズレにより，求まる時間差が負の値になる場合がある．内部時計のズレは固定長であり，提案手法で求める時間差が負の値になっても，一定の範囲に集中するため判断可能である．

また提案手法では，無線 LAN クライアントから AP へ認証後に流れる無線フレームのうち，CPD で用いられる HTTP 通信のレスポンスを，無線フレームのデータ部のサイズから推定している．よって，間違ったフレームを推定した場合，提案手法による時間差は，他の時間差が集中している一定の範囲から大きく離れる可能性がある．

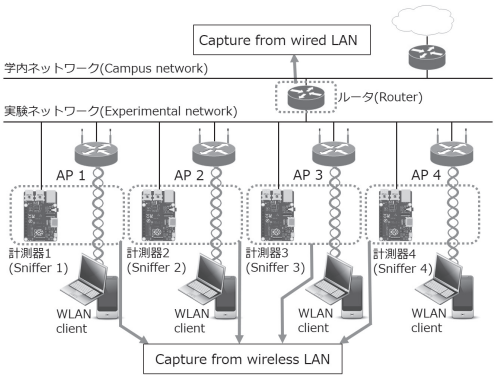

図 6　評価実験ネットワーク
Fig. 6　The network diagram of the evaluation.

4. 評 価 実 験

NAPT を兼ねた AP を 4 台用い，四つのプライベートサブネットを含む実験ネットワークを用意した．実験ネットワークからキャンパスネットワークへの接続点にルータを接続し，ネットワーク上流の観測点とした．ネットワーク上流の観測点を流れる通信と，無線 LAN クライアントと AP の間の通信区間に設けた観測点で得られるフレームから，提案手法を用いて推定・比較を行うことで，ネットワーク上流の観測点から見た IP アドレスと無線 LAN クライアントが接続した AP の紐付けが可能であるか確認した．なお本実験では，無線通信区間での HTTP レスポンスの推定に当り，認証パケットが流れてから 15 秒以内（図 4 の α）に流れたパケットに範囲を絞り推定を行った．本実験で構築したネットワークを図 6 に，使用した機器の詳細を表 1 に示す．

4.1　評価実験の手順

各無線 LAN クライアントは，提案手法による時間差を大量に得るため，AP への接続/切断を約 20 分間繰り返した．また，接続直後に CPD により流れる通信を取得したいため，接続が完了してから数秒間は切断を行わないようにした．接続完了から切断までの時間は，Windows ではランダム関数を用いることにより，4 秒から 8 秒の間でばらつきをもたせた．また，Android では手動で接続と切断を繰り返すことにより一定のばらつきをもたせた．

評価実験は，無線 LAN クライアントと AP の接続の組合せを変更して 4 回実施した．それぞれの実験を Case 1〜Case 4 とする．実験ごとの無線 LAN クライ

アントの接続先を表 2 に示す．また，各無線 LAN クライアントの詳細は表 1 に示す．

Case 1 では，1 台の AP に対して 4 台の無線 LAN クライアントを接続させた．これは，複数の無線 LAN クライアントが同一の AP に接続した場合の提案手法の有効性について，評価することを目的とした．

Case 2 では，4 台の AP それぞれに 1 台の無線 LAN クライアントを接続させた．これは，CPD で流れる通信が複数のネットワークから検出された場合の提案手法の有効性について，評価することを目的とした．

Case 3 では，2 台の AP それぞれに 2 台の無線 LAN クライアントを接続させた．これは，OS が異なる無線 LAN クライアントが AP に接続していた場合の提案手法の有効性について，評価することを目的とした．

Case 4 では，Windows と Android の無線 LAN クライアントの両方が接続した AP と，それぞれが接続した AP を用意した．これは，複数種類の OS が通信を行ったデータとそれぞれの OS が通信を行ったデータを比較した場合の，提案手法により求まる時間差への影響を確認することを目的とした．

各 Case でルータから取得したデータを通信元の AP の IP アドレスに基づき分離し，それぞれを分離済み上流データとした．それぞれの分離済み上流データとそれぞれの AP が送受信する無線フレームを比較し，提案手法により時間差を求めた．またその時間差を，比較したデータと OS ごとにヒストグラムに表した．

表 1　使 用 機 器
Table 1　Equipment.

name	role
Router	NAPT
AP 1	NAPT/AP
AP 2	NAPT/AP
AP 3	NAPT/AP
AP 4	NAPT/AP
Sniffer 1	Capturing packets passing through the AP1
Sniffer 2	Capturing packets passing through the AP2
Sniffer 3	Capturing packets passing through the AP3
Sniffer 4	Capturing packets passing through the AP4
Client 1	A wireless LAN client ・MacBookPro 13-inch, Mid 2012 ・Windows 10 Pro 64bit (Boot Camp 使用)
Client 2	A wireless LAN client ・Gigabyte GB-BXCE-2955 ・Windows 10 Enterprise 64bit
Client 3	A wireless LAN client ・Xperia X Performance ・Android 6.0
Client 4	A wireless LAN client ・Xperia Z4 ・Android 5.0

表 2　無線 LAN クライアント接続先
Table 2　The pattern of WLAN associations.

	Client 1	Client 2	Client 3	Client 4
Case 1	AP 1	AP 1	AP 1	AP 1
Case 2	AP 1	AP 3	AP 2	AP 4
Case 3	AP 3	AP 4	AP 3	AP 4
Case 4	AP 1	AP 3	AP 1	AP 2

4.2　システムの実装

実験ネットワークからキャンパスネットワークへの接続点のルータは，ソフトウェアルータ（VyOS 1.1.7）を導入した．このルータは NAPT として動作させており，NAPT の内側のネットワークインタフェースに対して，tcpdump を用いて通信を取得した．全ての通信について取得するとデータ量が膨大になる．よって，tcpdump でパケットを取得する際にフィルタを掛け，ルータを通過するパケットの内，HTTP 通信の GET リクエストのみを保存した．AP の暗号化方式は，WPA2 Personal の CCMP を使用した．また，AP は 2.4GHz 帯で IEEE 802.11g の規格で通信を行った．それぞれの AP に対して，無線 LAN クライアントと AP の間の無線フレームを取得するため，RaspberryPi B+と無線 LAN ドングルを計測器として用いた．無線 LAN ドングルは Planex GW-900D を用いた．各計測器は有線で実験ネットワークに接続し，SSH により操作した．

4.3　評価実験の結果

ヒストグラムは，データが集中したものとそれ以外の 2 種類に大別された．データが集中したヒストグラムの内，Windows の代表例を図 7 に，Android の代表例を図 8 に示す．これらは，Case 1 により得られた時間差について，OS 別にヒストグラムにしたものである．また，それ以外のヒストグラムの内，Windows の代表例を図 9 に，Android の代表例を図 10 に示す．

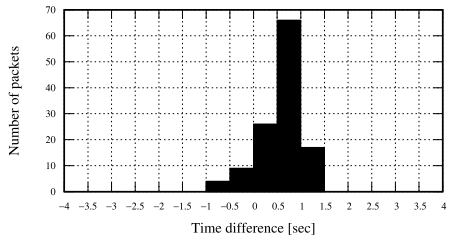

図 7　一致時の時間差（Windows）
Fig. 7　The time differences in the matched data (Windows).

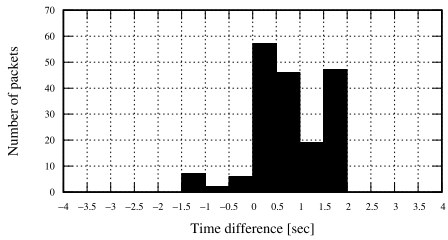

図 8　一致時の時間差（Android）
Fig. 8　The time differences in the matched data (Android).

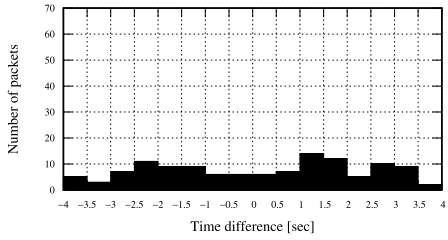

図 9　不一致時の時間差（Windows）
Fig. 9　The time differences in the unmatched data (Windows).

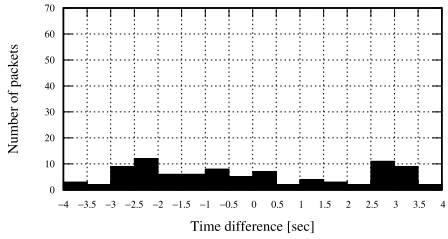

図 10　不一致時の時間差（Android）
Fig. 10　The time differences in the unmatched data (Android).

これらは，Case 3 により得られたデータの内，AP 4 がもつ IP アドレスに対応する分離済み上流データと，AP 3 が送受信した無線フレームを比較した場合の時間差について，OS 別にヒストグラムにしたものである．

データが集中したヒストグラムの比較元のデータを分析した結果，無線フレームを送受信している AP と分離済み上流データの通信元の AP が一致していた．また，計測器からのデータと，その観測している AP の IP アドレスと対応していない分離済み上流データを比較した場合は，時間差が一定の範囲に集中しないヒストグラムが作成されるか，無線フレームで推定したクライアントと同一の OS の通信を，分離済み上流データから見つけることができなかった．

表 3　時間差の標準偏差一覧 [秒]
Table 3　The list of standard deviation of time differences [sec].

Windows		Android	
一致群 (Group A)	不一致群 (Group B)	一致群 (Group C)	不一致群 (Group D)
0.4689	2.1646	0.7684	5.2711
0.1454	2.1501	0.6191	3.7761
0.2760	1.8913	0.7712	3.5256
0.9849	3.2387	0.8275	4.7080
0.1774	1.9058	0.6040	5.6657
0.2857	1.7357	0.6225	5.6248
0.1369		0.7088	

CPD で流れる HTTP 通信のレスポンスの推定に関して，本評価実験で得られた無線フレームを復号して解析した結果，偽陽性の推定はなかった．また，提案手法による時間差のサンプル数が十分取得できているため，偽陰性の推定による時間差のサンプル数の減少は影響がない．

計測器からのデータと，その観測している AP の IP アドレスと対応した分離済み上流データを比較した場合の時間差を一致時の時間差とし，それ以外の場合の時間差を不一致時の時間差とする．一致時の時間差の標準偏差の集合を一致群とし，不一致時の時間差の標準偏差の集合を不一致群とする．一致群と不一致群の明確な差を確認するため，ウィルコクソンの順位和検定を実施した．OS ごとに一致群/不一致群を求め，まとめた表を表 3 に示す．Windows のデータに関して Group A は一致群，Group B は不一致群である．また，Android のデータに関して Group C は一致群，Group D は不一致群である．帰無仮説は，「一致群と不一致群に差がない」である．検定により，有意水準を 0.05 とした場合，各 OS で帰無仮説が棄却された．よって，提案手法による時間差について，一致群と不一致群の標準偏差の比較において，群間に差がないとはいえない，つまり差があるとみなせることが示唆された．

よって，提案手法により求まる時間差が一定の範囲に集中していれば，検査対象 AP がネットワークに接続されていたとみなすことができるので，**3. 3** で述べたとおり，第一種不正 AP 並びに第二種不正 AP を識別可能であるといえる．

4. 4　考　　察

評価実験では，一致時の時間差が，おおよそ −1.5 秒から 2.0 秒の範囲に集中した（図 7，図 8）．時間差として負の値が算出されている．これは，短い間隔で

複数の CPD が送受信された場合，推定した HTTP 通信のレスポンスに最も近い HTTP 通信の GET リクエストとの時間差を求めているため，GET リクエストとレスポンスの対応関係に差異が生じ，誤差が生じたものと考えられる．

不一致時の時間差は，一定の範囲に集中しなかった．時間差は −4 秒から 4 秒の範囲外にも多数のデータが見受けられた（図 9，図 10）．この不一致時の時間差は，無線 LAN クライアントが AP へ接続/切断を繰り返した時間の間隔に依存していると考えられる．

評価実験では無線 LAN クライアントの再接続間隔は 4 秒以上であった．すなわち **3. 5** に述べた τ は $\tau > 4$[秒] とでき，$\sigma' = \tau/2\sqrt{3} > 1.15$ となる．一方，有意水準を 0.05 とすると，σ の信頼区間上限は図 7 から図 10 の例に対して，それぞれ 0.5387, 0.8000, 3.4888, 5.3537 であった．このことから，評価実験の範囲においてはデータが集中しているか否かを **3. 5** に記述したしきい値を用いて区別でき，「データが集中している」と判断されたものは「一致時」のもののみとなっている．

5. むすび

本論文では，全学ネットワーク管理者の視点で，セキュリティリスクを高めるキャンパス内の不正 AP の排除のために，検査対象 AP のキャンパスネットワークへの接続の有無を判断することによる不正 AP 検出手法を提案した．本提案手法は，検査対象 AP の通信内容を復号することなく判断する．本提案手法では，川田らによる従来の有線 LAN/無線 LAN の双方を用いて検出する手法 [7] の，無線 LAN のトラヒックについて，有線 LAN 側の観測点を通過しないトラヒックが多いと正しく検知できない問題点を，トラヒック量に依存しない手法により解決している．

評価実験では，ネットワーク上流の観測点を流れる通信と無線フレームを取得し，提案手法を用いて推定・比較を行うことで，ネットワーク上流から見た IP アドレスと無線 LAN クライアントが接続した AP の紐付けが可能であることを確認した．

評価実験では CPD で流れる通信を一定量取得するため，高頻度で無線 LAN クライアントの AP への接続/切断を繰り返したが，無線 LAN クライアントが AP に接続を行う機会は極めて少ない．よって，検査対象 AP のキャンパスネットワークへの接続の有無を確認するためには，数日間ネットワーク上流の観測点を流れる通信と無線フレームを取得しなければならない．評価実験の取得方法では，無線フレームの取得データ量が膨大になる．これは運用面から見て非現実的である．実際の運用に当り，逐次無線フレームを解析し必要なデータのみをリアルタイムでやり取りを行うシステムが必要不可欠となる．

文　献

[1] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, “Rogue access point detection using temporal traffic characteristics,” Proc. IEEE GLOBECOM 2004, vol.4, pp.2271–2275, 2004.

[2] G. Xie, T. He, and G. Zhang, “Rogue access point detection using segmental TCP jitter,” Proc. 17th international conference on World Wide Web, pp.1249–1250, Beijing, China, April 2008.

[3] L. Watkins, R. Beyah, and C. Corbett, “A passive approach to rogue access point detection,” Proc. IEEE GLOBECOM 2007, pp.355–360, 2007.

[4] H. Han, B. Sheng, C.C. Tan, Q. Li, and S. Lu, “A timing-based scheme for rogue AP detection,” IEEE Trans. Parallel Distrib. Syst., vol.22, no.11, pp.1912–1925, 2011.

[5] S. Thakur and A. Bodhe, “RAPD algorithm: detection of rogue access point in wireless network,” Int. J. Emerging Technology and Advanced Engineering, vol.3, no.6, pp.85–89, 2013.

[6] S.V. Jagtap and K.N. Honwadkar, “Rogue access point detection in WLAN by analyzing network traffic and behavior,” Int. J. Comput. Appl., vol.1, no.22, pp.27–29, 2010.

[7] 川田丈浩，矢田　健，“無線/有線 LAN トラヒック分析による不正アクセスポイント検出法の提案，” 信学技報，IN2014-91, 2014.

[8] M. Nottingham, “draft-nottingham-capport-problem-01 - Captive Portals Problem Statement,” IETF, https://tools.ietf.org/html/draft-nottingham-capport-problem-01, April 2016.

（平成 29 年 5 月 25 日受付，9 月 26 日再受付，
11 月 2 日早期公開）

竹田　智洋

徳島大学大学院博士前期課程．2017 年徳島大学工学部知能情報工学科卒業．現在，2017 年 4 月より同大学大学院に在籍．ネットワーク・セキュリティに関する研究に従事．情報処理学会学生会員．

大平　健司　（正員）

徳島大学情報センター講師．2002 年京都大学理学部卒．2004 年同大大学院修士課程了．2007 年同大大学院博士後期課程単位取得認定退学．(株) オクトパス．2008 年京都大学学術情報メディアセンター特定助教．2012 年奈良先端科学技術大学院大学情報科学研究科特任助教．博士（情報学）．2015 年 12 月より現職．公衆 WLAN，認証，セキュリティ，IPv6，トラヒック制御などの研究に従事．電子情報通信学会，情報処理学会，システム制御情報学会，IEEE 各会員．

谷岡　広樹

徳島大学情報センター助教．1997 年千葉大学工学部電気電子工学科卒．2004 年信州大学大学院博士前期課程了．2008 年同大大学院博士後期課程了．博士（工学）．1997 年から IT 系企業での勤務を経て，2016 年 4 月より現職．情報検索，自然言語処理，機械学習などの研究に従事．情報処理学会，人工知能学会，IEEE，ACM 各会員．

佐野　雅彦　（正員）

徳島大学情報センター准教授．1990 年徳島大学工学部情報工学科卒．1992 年同大大学院博士前期課程了．1995 年同大大学院博士後期課程了．博士（工学）．同年同大工学部助手．改組を経て 2014 年 4 月より現職．配線問題の並列処理方式，ネットワーク，セキュリティなどの研究に従事．電子情報通信学会，情報処理学会，IEEE 各会員．

松浦　健二　（正員）

徳島大学情報センター教授．1994 年徳島大学工学部知能情報工学科卒．1996 年同大大学院博士前期課程了．2002 年同博士後期課程了．博士（工学）．1996 年 4 月から 1999 年 3 月，日本電信電話株式会社勤務，2002 年からドイツ KMRC 研究員，2003 年より徳島大学高度情報化基盤センター助手，2009 年 8 月同准教授，2015 年 11 月より現職．身体の学習支援，グループ学習支援，認証連携と情報基盤などの研究に従事．電子情報通信学会，情報処理学会，人工知能学会，教育システム情報学会，日本教育工学会各会員．

上田　哲史　（正員）

徳島大学情報センター教授．1990 年徳島大学工学部電子工学科卒．1992 年同大大学院博士前期課程了．同年同大学工学部知能情報工学科助手．博士（工学）．2009 年高度情報化基盤センター教授．改組を経て 2014 年 4 月より現職．非線形力学系の解析などの研究に従事．電子情報通信学会，計測自動制御学会，IEEE，情報処理学会，可視化情報学会，信号処理学会各会員．