情報処理学会論文誌 Vol.58 No.9 1501–1512 (Sep. 2017)

無線LANアクセスポイントのベンダー構成比を用いた在宅/オフィス推定

鈴木 宏哉[1,a)] 山口 利恵[1,b)]

受付日 2016年12月5日, 採録日 2017年6月6日

概要：近年，スマートフォンに代表されるモバイル端末の普及により，利用者は場所を問わず，常時様々なサービスを享受することができるようになっている．一方で，モバイル端末と利用者行動との密接な結び付きから，プライバシ問題に注目が集まっている．特に，通信に端末固有のMACアドレスが含まれるWi-Fi無線通信は，利用者の追跡や位置情報の暴露といったプライバシ上の危険性を有している．本稿では，モバイル端末が収集した周辺のアクセスポイントのMACアドレス情報に着目し，アクセスポイント機器のベンダー構成比から，位置情報データベースなしでも居場所推定に有用な情報が得られることを示した．本稿では，16名の被験者から30日分ずつ収集した周辺アクセスポイントのMACアドレスデータを用い，在宅中や就業，就学中の時間帯におけるベンダー構成に有意に異なる相関比が得られることを実験により確認した．

キーワード：プライバシ，Wi-Fi，MACアドレス，モバイル端末，行動履歴

The Estimation for being in Home/at Office Using Vendor Composition Ratio of Wi-Fi Access Points

Hiroya Susuki[1,a)] Rie Shigetomi Yamaguchi[1,b)]

Received: December 5, 2016, Accepted: June 6, 2017

Abstract: In recent years, many people have wireless devices that can connect wireless network through Wi-Fi or Bluetooth connection. The information that is collected by these devices are useful, but invasion of privacy occurs. This risk raises concerns that user's privacy may be disclosed by gathering MAC addresses data. In this paper, we show the result of gathering MAC addresses of 30 days from 16 volunteers. We analyzed the gathered data and showed that there is a relationship user behavior and vendor composition ratio of wireless access points around user.

Keywords: privacy, Wi-Fi, MAC address, mobile devices, behavioral history

1. はじめに

近年，スマートフォンやウェアラブルデバイスの普及にともない，多くの人がGPSなどの各種センサ，Wi-Fi[*1]やBluetoothといったネットワーク通信機能を持つモバイルデバイスを日常的に携帯するようになった．これらのデバイスから収集される情報の履歴は，直接的，間接的に利用者の行動習慣や趣味嗜好といった特徴を含んでおり，各種レコメンドサービス [1] や個人認証技術 [2], [3] などに利用されている．一方で，これらの履歴情報でプライバシが侵害される事例も出ており，利用者の位置情報やスマートフォン内の情報を他者がチェックできるアプリケーション「カレログ[*2]」の事例などが知られている．カレログのように，ユーザの意図しない情報がアプリケーションを通じて外部に漏洩されるということは大きな問題である．この問

[1] 東京大学
The University of Tokyo, Bunkyo, Tokyo 113–8656, Japan
[a)] susuki.hiroya@sict.i.u-tokyo.ac.jp
[b)] yamaguchi.rie@i.u-tokyo.ac.jp

[*1] Wi-Fiとは無線LANの標準規格を保証された製品に与えられる認証のことであるが，本稿では無線LANと同義とする
[*2] http://klg2.com/

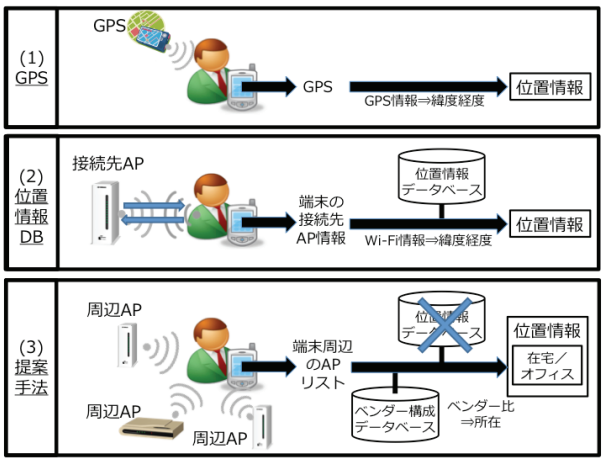


図 1 ロケーションプライバシに関する従来手法による情報漏洩と提案手法による情報漏洩．(1) GPS を用いた位置情報推定，(2) 位置情報データベース（DB）を用いた位置情報推定，(3) アクセスポイントのベンダー構成比を用いた提案手法

Fig. 1 The difference of three methods. (1) GPS Location, (2) Location Database, (3) Proposed method using vendor composition ratio of Wi-Fi access point.

題が近年，注目される背景として，環境の変化による問題の深刻化が大きい．まず，スマートフォンの普及により，多くの利用者がアプリケーションを自身でダウンロードして利用するようになったことがある．さらに，近年ではアプリケーション作成も容易になり，攻撃者による悪意あるアプリケーションの配布と，それによる情報漏洩リスクが高まっている [4]．

特に考慮すべき情報漏洩リスクとして，ユーザの位置情報に関するロケーションプライバシの問題がある．スマートフォンの利便性の高さから，スマートフォン利用者の多くは，入浴中などを除き常時身近に置くということが習慣化しつつある．このため，スマートフォンの位置情報は利用者の位置情報とおおよそ一致する．したがって，端末の位置情報を知られることはプライバシリスクにつながる問題である．本稿では，置き忘れやスマートフォンの利用頻度が低く手放すことが多い利用者については考慮せず，利用者と端末は同じ所にあるものとして論じる．

1.1 ロケーションプライバシリスクと対策

端末の位置情報を知るための攻撃手法として，**図 1** の (1) で示したように端末から GPS の位置情報を入手する方法がある．しかし，GPS のプライバシリスクについてはすでに認知されており，ユーザ自身のリテラシの向上だけでなく，アプリケーション側でも制約が設けられている．Android と iOS ともにパーミッション（機能へのアクセス権限）の設定により，アプリケーションが位置情報を収集する機能を利用するためにはユーザが明示的にアクセスを許可する必要がある．

端末本体の位置情報を使わずに，間接的に端末の位置情報を知るための従来手法として，図 1 の (2) のように，端末の接続先アクセスポイント（AP）の Wi-Fi 情報を利用するという手法がある [5]．Wi-Fi 情報とは AP の持つアクセスポイント機器を識別するための識別子のことである．Wi-Fi 情報の詳細については 1.2 節で述べる．AP の Wi-Fi 情報からユーザの位置情報を推定するためには，位置情報データベースが用いられている．位置情報データベースとは，アクセスポイントの Wi-Fi 情報と緯度経度などの位置情報を対応付けたものである [6]．このデータベースを用いると，接続先アクセスポイントの Wi-Fi 情報を知ることで，間接的にアクセス元端末の位置情報を推定することができる．また，接続先に限らず周辺のアクセスポイントの Wi-Fi 情報からも，同様に位置情報の推定が可能である．一方で，位置情報データベースを利用することは困難である．Google や Apple が持つような大規模な位置情報データベースは一般には公開されておらず，誰もが利用できるものではない．また，一般に公開されている位置情報データベースは網羅率が低く，アクセスポイントの未登録問題がある [7]．さらに，アクセスポイントは，新規の追加や削除などによる増減や移設による移動があるため，不変ではなく常時変化しているという問題もある．攻撃者自身が位置情報データベースを作成するには，データベースを更新し続けるコストが必要となる．このように位置情報データベースを用いた従来の攻撃手法には，制約があった．

我々は，位置情報データベースを持たない攻撃者でも可能な攻撃手段として，自宅やオフィス，学校など特定カテゴリの場所に居ることを推定できる手法について提案する．本手法は，位置情報データベースを用いないため，緯度経度そのものを知ることはできないが，個人のプライバシに密接に結び付く自宅やオフィス，学校にいるかどうかを端末周辺のアクセスポイントの情報から推定する手法である．具体的には，自宅で利用されるアクセスポイントと，企業のオフィスや商業施設などで利用されるアクセスポイントには違いがあるという仮説に基づく．そこで，特定の場所に特定のベンダーの製品が使われているのであれば，Wi-Fi 情報に含まれるアクセスポイント機器のベンダー情報から，位置情報データベースなしでも，自宅やオフィス，学校などの場所であれば推定できると考えた．本稿では，（図 1 の (3)）で示す提案手法によるプライバシリスクの問題を提起し，その可能性について実験により評価した．

1.2 無線 LAN アクセスポイントと位置情報

従来，無線 LAN の利用は企業のオフィスや大学やその他公共機関といった特定の場所に限られていた．しかし，近年，家庭用無線 LAN ルータの普及により，自宅での Wi-Fi 利用が一般的になっている．さらに，公衆無線 LAN サービスの増加およびモバイル Wi-Fi ルータの普及，スマートフォンのテザリング機能の利用により，勤務先や自宅だけ

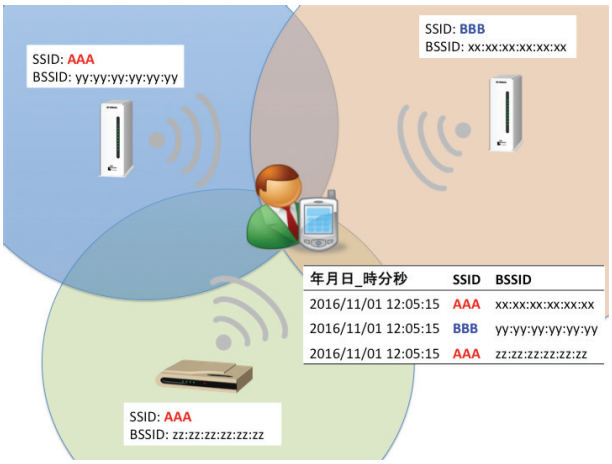


図 2 アクセスポイントにおける SSID と BSSID の関係
Fig. 2 The relation of SSID and BSSID of an access point.

でなく，外出時でも無線 LAN にアクセス可能である [8].

Wi-Fi 通信において，クライアント端末は無線 LAN アクセスポイントを経由してインターネットにアクセスする．各アクセスポイントは，自身を示す識別子として Service Set Identifier（SSID）と Basic Service Set Identifier（BSSID）を持ち，クライアント端末はこの 2 つの識別子をアクセスポイントの情報として利用する（**図 2** 参照）．モバイル Wi-Fi ルータやスマートフォンのテザリング機能などを除き，アクセスポイントは頻繁には移動されない．したがって，アクセスポイントは特定の場所から移動せず，逆説的に，ある場所から得られるアクセスポイントの情報は変動しないと考えることができる．また，ある場所が複数のアクセスポイントの通信可能範囲内であれば，それぞれのアクセスポイントから情報を収集することができる．すなわち，図 2 中の表のような，ある時間における SSID と BSSID のリストは，特定の場所と 1 対 1 に紐付けることが可能と仮定できる．

さらに，アクセスポイント機器はベンダーごとにその機能や価格帯に違いがあり，家庭用や業務用としてそれぞれ利用用途に合わせて設置される．そのため，利用されている機器を知ることができれば，設置場所の推定に有用な情報を得ることができると考えられる．同様に，アクセスポイント機器のベンダー情報にはユーザの行動に関連する情報が含まれるという仮説を立てることができる．

なお，場所に紐付かない性質を持つモバイル Wi-Fi ルータやスマートフォンのテザリング機能について，本稿では影響の少ないものとして扱っている．これらの移動するアクセスポイント（移動 AP と記す）を 1 人のユーザが複数持つことは少ないという前提の元で，周辺のアクセスポイント数が多数ある場合にはそのアクセスポイント情報が占める影響は少ないと仮定した．一方で，ネットワーク環境が整備されていない地域や場所の場合は，周辺アクセスポイントの数が少なくリストに占める移動 AP の比率が大きくなるため，考慮する必要がある．ただし，周辺アクセスポイント数の少ない場所については，アクセスポイント数が多い場所に比べ攻撃者が位置情報データベースを作成しやすいため，既存の攻撃手法が有効となる．さらに，ユーザ自身が持つ移動 AP 以外のアクセスポイントがない場合は，そのアクセスポイントがある場所に当該ユーザがいることが推測されるため，プライバシに対する別種の攻撃が可能と考えられる [9].

1.3 本稿の貢献

本研究では，モバイルデバイスの Wi-Fi 通信機能を用い，端末周辺のネットワーク環境を構成するアクセスポイントの機器ベンダーの構成と利用者の居場所に関係性があるという仮説から，在宅かオフィスや学校といった場所にいるかどうかの推定が可能な手法を提案した．場所の推定には，周辺アクセスポイントのベンダー構成比を用いた．ベンダー構成比とは，モバイル端末の周辺にあるアクセスポイント（AP）のリストからその AP 機器のベンダー構成の比率を求めたものである．ベンダー構成と場所の関係の有無については，日中はオフィスや学校，夜間は自宅にいるという仮定のもと，それぞれの時間帯とベンダー構成に相関があるかを示すことで評価を行った．

本稿の構成は次のようになっている．2 章では，位置情報とプライバシ，匿名化技術，個人認証に関する関連研究について紹介する．3 章では，Wi-Fi の持つ機能的特徴について説明する．4 章では，データ収集実験の方法と収集したデータの解析結果ついて述べる．5 章では考察を行い，6 章で結論を述べる．

2. 関連研究

2 章では，位置情報とプライバシ，プライバシリスクに対する対策，行動認証に関する関連研究について述べる．

2.1 位置情報サービスとロケーションプライバシ

位置情報と Wi-Fi 情報を紐付けた事例として，位置情報サービスがある．Google や Apple，Microsoft は，Wi-Fi のアクセスポイントと GPS の位置情報を対応付けた情報を収集し，位置情報データベースとして，それぞれが提供するサービスに利用している．また，Skyhook [10] や WiGLE [11] も，位置情報サービスを提供している [12]．日本ではクウジット株式会社の PlaceEngine が知られている [7].

Apple の Web サイトによると，アクセスポイントと位置情報の対応付けのための情報を，端末が定期的に収集していることが記載されている [6].

Apple 位置情報サービス

位置情報サービスがオンの場合，デバイスは，近くにある公衆 Wi-Fi アクセスポイントと携帯基地局のジオタグ付きの位置情報を，暗号化された匿名形式で Apple に定期的に送信します．この情報で，公衆 Wi-Fi アクセスポイントと携帯基地局の位置情報を記録する Apple のクラウドソーシングデータベースが拡充されます．

同様に，Google も位置情報データベースを保有しており，この情報を位置情報の精度向上のために利用している旨の記載がある [13]．

Google 位置情報サービス

Google は，位置情報サービスプロバイダとして位置情報ベースのサービスを改善するため，GPS や携帯電話の基地局からのデータだけでなく，ワイヤレスアクセスポイントからのパブリック Wi-Fi データも使用しています．

これらの Apple や Google などが作成する大規模な位置情報データベースは様々なサービスに活用され，ユーザの利便性を向上させている．一方で，これらの位置情報データベースが悪用された場合，容易に個人の居場所を特定可能である．

このような現状に対し，Wi-Fi 情報から端末所持者の位置や動きを推定される問題について指摘した研究も行われている [14], [15]．折尾らは Wi-Fi のロケーションプライバシについて言及し，モバイルデバイスの Wi-Fi や Bluetooth 利用におけるプライバシのリスクの低減・回避手法について考察している [5]．折尾らは，5 名の被験者に 10 日間スマートフォンを所持させた情報収集実験も行っているが，収集したデータ数の数えあげにとどまっており，具体的にそのデータと被験者の位置情報の関係性までは示していない．

2.2 スマートフォンにおける対策

iOS，Android それぞれのスマートフォンで，Wi-Fi 情報によるプライバシリスクに対する対策が進んでいる．攻撃者による外部からの Wi-Fi の観測に対しては，iOS8 で MAC アドレスのランダム化の機能が追加されるなど，OS レベルでの対策がなされている．Android6.0（API Level23）でもスキャン時，外部デバイスに対してはランダムな MAC アドレスを返す [16]．さらに，アプリケーションによる端末内部からの観測に対しても，Android では 6.0 から匿名化が行われている．API を使用して端末内の識別子（BSSID）にアクセスすると，Wi-Fi と Bluetooth ともに 02:00:00:00:00:00 が返ってくる．結果，現在はアプリケーションにより端末内で収集可能な情報は，周辺アクセスポイントの Wi-Fi 情報のみである．従来の端末自体の情報を利用して端末の位置推定を行う手法に対しては対策が進んでいる．しかし，対策に影響されない攻撃手法として，提案の周辺アクセスポイントの情報を利用した攻撃が考えられる．

2.3 位置や Wi-Fi の履歴情報を用いた認証

位置や Wi-Fi の履歴情報を用いた既存研究の 1 つとして，行動的特徴を用いた認証がある．行動的特徴を用いた認証とは，移動にともなう位置情報の変化 [3] や人間の動作 [17]，購買行動など人間の行動履歴に含まれる個人差を用いた認証手法である．入力手段の限られるモバイルデバイスでは特に，利用者が明示的な操作を必要としない手法として，位置情報や利用中のアプリケーションを元にした暗黙的な認証が提案されている [18], [19]．

Hayashi らは，GPS を用い，安全であると仮定できる環境（自宅）では簡易な認証を用い，安全性が低い環境（公共の場）では安全性の高い認証を用いる 2 段階の多要素認証を提案している [20]．Hayashi らの実験によると，被験者 36 名が 1 日に滞在する場所と時間の内訳として，平均で 38.9%が自宅，18.7%が学校職場となり，上位 2 カ所で 6 割近い時間を過ごしているという結果が得られている．これは，本稿の対象である自宅やオフィスを推定できれば，6 割の居場所の推定ができる可能性を示している．

Wi-Fi を用いた研究として，Albayram らが MAC アドレスをフィンガプリントとして確率的 n-gram モデルにより個人認証を行う手法を提案している [21]．MAC アドレスのリストを過去の行動履歴として学習し，正常な行動か異常な行動かを推定することで認証を行う手法である．この手法も被験者の所在を推定しているが，教師あり学習のために事前に MAC アドレスリストと場所の対応付けがなされたデータを必要としている．これは攻撃者が MAC アドレスに対応した位置情報データベースを事前に持っている必要がある．未知の MAC アドレスが入力されることを想定しておらず，位置情報データベースを持たない攻撃者にとっては困難である．また，利用者の行動履歴を用いた事例として，リスクベース認証がある．Google では，利用者のアクセス元 IP アドレスを位置情報に相当する情報として利用し，記録したアクセス履歴（アカウントアクティビティ）を元に，不審なアクセスに対して警告を行う機能を提供している [22]．Google は経度，緯度といった位置情報の代わりに IP アドレスを用いているが，クライアント端末自身の情報の提供が必要である．

Sapiezynski らは，1 人あたり 1 日 1 つの GPS の観測を使うことで，Wi-Fi のアクセスポイント情報を用いて 80%を占める人間の位置情報の推定ができるという報告をしている [23]．この結果は，モバイルルータを用いて屋外での位置情報の特定ができる可能性を示すとともに，本稿で指摘するプライバシ上の問題を引き起こす可能性も示している．

3. Wi-Fi 履歴に関する用語の定義と周辺知識

3 章では，Wi-Fi 履歴に関連する用語と Wi-Fi で用いられる識別子の詳細について述べる．

3.1 用語の定義：SSID と BSSID，MAC アドレス

図 2 は，Wi-Fi アクセスポイントと SSID，BSSID の関係を示している．SSID とは，Wi-Fi におけるアクセスポイントの識別名である．SSID は任意に設定可能であり，同一の識別名の SSID を複数のアクセスポイントに割り当てることができる．これにより，図 2 で SSID「AAA」が割り当てられた 2 つのアクセスポイントのように，複数台が通信可能範囲をカバーし合うことで，広範囲の Wi-Fi アクセスエリアを実現することも可能である．

他方，BSSID は端末ごとに設定される識別子であり，そのアクセスポイント端末の MAC アドレスが割り当てられる．MAC アドレスには一意性があり，グローバルな MAC アドレスは基本的に衝突しない．ただし，MAC アドレスを変更可能な機器もあり，必ずしも一意とは限らない．たとえば，Apple の iOS8 以降には，プライバシ保護のため，MAC アドレスをランダム化する機能が搭載されている．ランダム化を行うことで，スキャン時の MAC アドレスが偽装される．本稿では以後，BSSID と MAC アドレスは同じものとして扱う．

3.2 MAC アドレスと OUI

MAC アドレスは，前半 24 ビット部分が OUI（Organizationally Unique Identifier）と呼ばれるベンダー識別子になっており，IEEE Standards Association により各ベンダーへの割り当てが行われている [24]．

現在，IEEE において割り当てられている OUI の総数は 16,215 個あり，1 組織で 2 個以上の OUI を取得している組織が 520 ある．ここでは，登録ベンダー名の表記が異なるものはすべて別組織として計上した．100 個以上の OUI を取得している組織は 6（Cisco 518，Apple 340，Samsung 191，ARRIS 170，Intel 141，Cisco 131 *3）ある．

3.3 ローカル MAC アドレス

IEEE の OUI に関するガイド [25] に記載されているとおり，第一オクテットの 2 ビット目は Universal/Local ビットとして定義されている．Universal/Local ビットが 1 になっているローカル MAC アドレスには特定のベンダーが割り当てられておらず，ローカルネットワーク内でユニークに割り当てられていれば利用可能である．今回実験で収集したデータにもローカル MAC アドレスが観測されている．

*3 Cisco の登録には「CISCO SYSTEMS, INC.」「Cisco Systems」など複数の表記がある

4. データ収集およびその解析

4 章では，データ収集実験の目的，およびデータ収集の方法と収集したデータの解析結果ついて述べる．

4.1 Wi-Fi 履歴収集実験の目的と仮説

本実験の目的は，利用者の周辺にあるアクセスポイントのベンダーの分布と人間の行動，時間に関係があるという仮説を評価するためである．

本研究における前提として，場所によって利用される無線 LAN アクセスポイントに違いがあるという仮説を立てた．一般に，自宅では家庭用の機器が使われ，オフィスや学校といった場所では業務用の機器が使われると考えた場合，ある時点で観測された周辺のアクセスポイントの一覧からそのベンダー構成を調べることで，自宅かオフィスかといった傾向に違いが現れると考えられる．ベンダー構成と場所に関係性があるということを示せれば，時間や BSSID の一覧，過去の行動履歴といった情報を必要とすることなく，ユーザの行動推定が行える可能性がある．本稿では，この仮説が適切かどうかの評価を行った．なお，本稿では被験者は日中に学校や勤務先に外出し，夜間は在宅で睡眠などを取るという仮定を置いたうえで評価を行っている．

4.2 データ収集実験

本実験では，スマートフォン（Softbank ARROWS A 202F *4）を用いたデータ収集を行った．被験者には，周辺にある Wi-Fi アクセスポイントの情報（SSID，BSSID）を 5 分に一度収集するロガーを入れた実験端末を携帯させ，30 日分のデータを収集した．データ収集の開始日と終了日は被験者ごとに異なるが，いずれも 2014 年 9 月上旬〜11 月上旬に実施した．被験者は男女を含む 20 歳以上の大学職員および学生の 16 名からなる．

なお，端末には SICT01 から SICT20 までの ID を割り当てており，予備実験に用いた SICT01，SICT02 の 2 台，およびデータ収集に不備のあった SICT13，SICT17 を除く 16 台を使用した．

表 1 は各被験者から収集したデータのサンプルである．

表 1 データ収集項目のサンプル
Table 1 Sample of collected data.

日時	SSID	BSSID
2014/10/05 00:00	0000docomo	00:80:f0:xx:xx:xx
2014/10/05 00:00	au_Wi–Fi	c0:8a:de:yy:yy:yy
2014/10/05 00:00	0001softbank	04:c5:a4:zz:zz:zz
2014/10/05 00:05	0000docomo	00:80:f0:xx:xx:xx
2014/10/05 00:05	au_Wi–Fi	c0:8a:de:yy:yy:yy

*4 http://www.softbank.jp/mobile/products/list/202f/

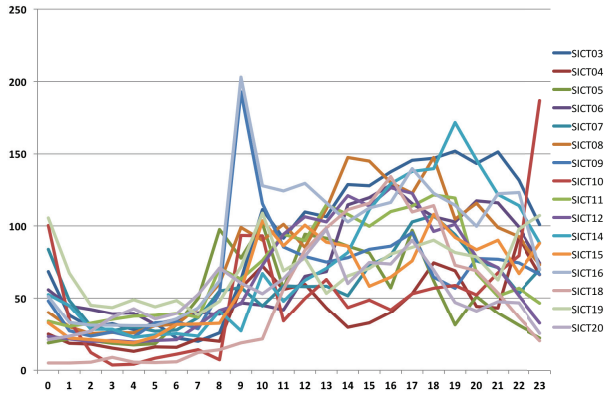


図 3 時間ごとの MAC アドレス数の平均（横軸：時間［0 時から 23 時］，縦軸：BSSID 数）

Fig. 3 Hourly number of average BSSID (horizontal axis: hour, vertical axis: the number of BSSID).

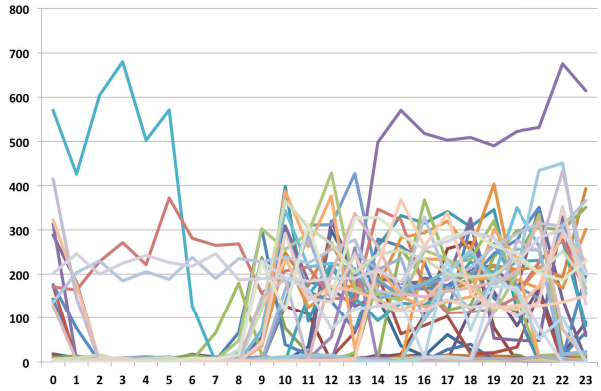


図 4 SICT03 の時間ごとの BSSID 数（横軸：時間［0 時から 23 時］，縦軸：BSSID 数）

Fig. 4 Hourly number of BSSID (SICT03) (horizontal axis: hour, vertical axis: the number of BSSID).

収集したデータは，時間，SSID，BSSID をリストにしたもので，表 1 は 2014 年 10 月 05 日の 00 時 00 分と 00 時 05 分の 2 回分のデータを表したサンプルである．なお，本稿では被験者の個人情報への配慮から匿名化のため，例として掲載するデータについては BSSID の後半 24 ビットを置き換えて記載している．16 名の被験者全体で 55,109 種類の SSID と，106,020 種類の BSSID を観測した．

4.3 各被験者から得られた BSSID に関する評価

図 3 は，各被験者ごとに 0 時から 23 時までの 1 時間で観測した BSSID 数 30 日分の平均を折れ線グラフで表している．この図から被験者全体に共通する時間帯と BSSID 数に関する評価を行う．

すべての被験者で 2 時から 6 時の時間帯の平均 BSSID 数が少ないことが分かる．1 時と 7 時については，2 時から 6 時を除く他の時間と比べると少ないが，MAC アドレス数が増えている被験者がいる．これは各被験者 30 日分のデータの中に 1 時頃に帰宅した日などが含まれるため，平均された結果として増えているものと考えられる．同様に 7 時や 8 時も外出が早い日が影響しているものと考えられる．したがって，本実験の被験者は多くの場合，1 時から 7 時または 8 時が在宅の時間と考えられる．一般に自宅のような私的空間が多数のアクセスポイントの範囲内になることは少なく，夜間帯は自宅で過ごすという仮定に合致する結果となっている．

また，9 時の平均 BSSID 数が多い被験者が 2 名おり，他の多くの被験者も 9 時前後を境にして観測される BSSID 数が増加している．これは通勤通学にともない，観測される周辺のアクセスポイントが増えるためである．さらに，午後から夜にかけての時間帯は被験者ごとのばらつきが大きいという結果も，退勤下校後の行動習慣が 1 人 1 人異なるということを示している．

図 4 は，SICT03 が 0 時から 23 時までの各時間ごとに観測した BSSID 数の合計を，日別にグラフにしたものである．この SICT03 の例と同様に各被験者の 1 日の行動も日によって大きく異なっている．このようにばらつきがある一方で，BSSID 数が明らかに異なる 4 日分を除き，1 時から 7 時の時間帯は在宅と推定できる．1 時については BSSID 数が多い日もあり，日によって在宅でない場合もあるが，2 時以降は他の時間帯と比べ BSSID 数が少ないことが分かる．

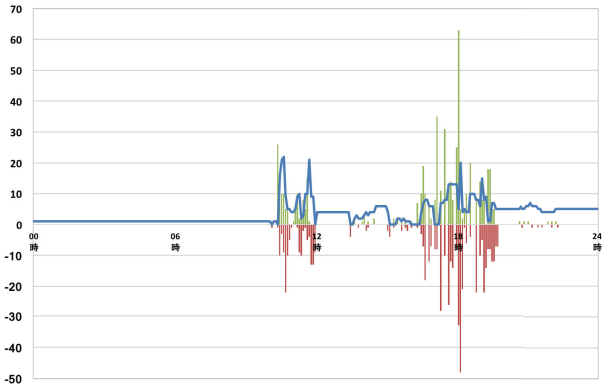


図 5 SICT03 の時間ごとの MAC アドレス数の変化 09/20（横軸：時間，縦軸：MAC アドレスリストの増減数），折れ線グラフ（青）：前後の時間で継続して観測された MAC アドレス数，正の棒グラフ（緑）：新しく観測されたアドレス数，負の棒グラフ（赤）：観測されなくなったアドレス数

Fig. 5 Hourly number of MAC address (SICT03) 09/20 (horizontal axis: hour, vertical axis: the changed number of BSSID).

図 5 は，SICT03 のある日の時間ごとの BSSID 数の増減を示している．折れ線グラフが，前後の時間で継続的に観測されている BSSID 数を示し，正負の棒グラフがそれぞれ前後の時間での BSSID 数の増減を示している．

移動しない場合，同一のアクセスポイントの範囲内に居続けることになり，同じ MAC アドレスが前後の時間で 5 分ごとに検出され続けるはずである．一方，移動すると前

表 2 SICT03 の自宅で観測される BSSID リスト
Table 2 In home BSSID list (SICT03).

BSSID	OUI	ベンダー名
00:1d:6a:xx:xx:xx	001D6A	Alpha Networks
06:1d:6a:xx:xx:xx	001D6A	Alpha Networks
00:22:cf:yy:yy:xx	0022CF	PLANEX
00:22:cf:yy:yy:yy	0022CF	PLANEX
00:24:a5:zz:zz:zz	0024A5	Buffalo

表 3 SICT03 の自宅以外で観測された BSSID リストの一例
Table 3 Out of home BSSID list (SICT03).

BSSID	OUI	ベンダー名
3c:ce:73:xx:xx:xx	3CCE73	Cisco
3c:ce:73:xx:xx:yy	3CCE73	Cisco
2c:36:f8:yy:yy:xx	2C36F8	Cisco
2c:36:f8:yy:yy:yy	2C36F8	Cisco
2c:36:f8:yy:yy:zz	2C36F8	Cisco
2c:36:f8:yy:xx:xx	2C36F8	Cisco
2c:36:f8:yy:xx:yy	2C36F8	Cisco
2c:36:f8:yy:xx:zz	2C36F8	Cisco
20:c9:d0:zz:zz:xx	20C9D0	Apple
00:24:a5:zz:zz:zz	0024A5	Buffalo

回のデータ収集タイミングのアクセスポイント範囲から離れ，新しいアクセスポイントの範囲内に入ることになるため，観測される BSSID リストに増減が発生する．すなわち，移動中は前後の時間での BSSID 数の増減が大きくなると考えられる．図 5 の例では，0 時以降の深夜時間帯は MAC アドレス数が変動しておらず，移動していないと考えられる．

表 2 は，図 5 で BSSID 数の増減が観測されない在宅中に観測された BSSID のリストを示している．他方，**表 3** は 1 時から 7 時の時間帯に在宅していなかった日の BSSID リストである．表 2 と，表 3 からは自宅にいる日といない日で観測される BSSID 数とそのベンダーの構成が異なることが確認できる．

4.4 Wi-Fi 履歴のベンダー構成比に関する評価

我々は，周辺の Wi-Fi アクセスポイント履歴の中で，特にアクセスポイント機器の利用傾向に着目した．現在，比較的安価な家庭用 Wi-Fi ルータなどの普及が進んでいるが，一定の規模以上のサービスには業務用のアクセスポイント機器が使われる．すなわち，在宅中や勤務中，移動中などで周辺にあるアクセスポイント機器の種別分布に差があると仮定した．

4.4.1 データ収集実験で得られた OUI 情報

今回のデータ収集実験で観測された全 OUI の異なり数は，2,270 個あった．観測された全データのうち，1,000 回以上観測した OUI は 33 あり，最も観測回数の多かった OUI は「Buffalo Inc.」の「106F3F」で 3,707 回である．

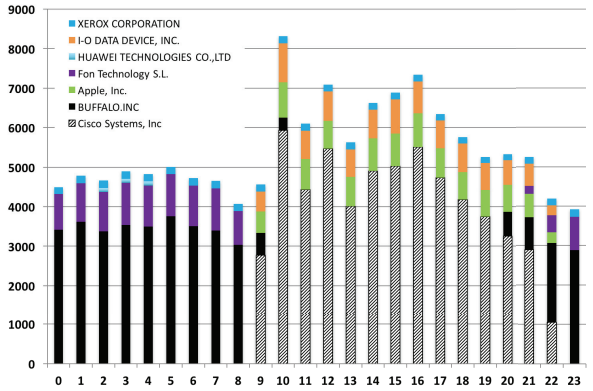


図 6 SICT16 の時間ごとのベンダー構成比（横軸：時間［0 時から 23 時］，縦軸：合計 BSSID 数）
Fig. 6 Vendor composition ratio of SICT16 (horizontal axis: hour, vertical axis: the total number of BSSID).

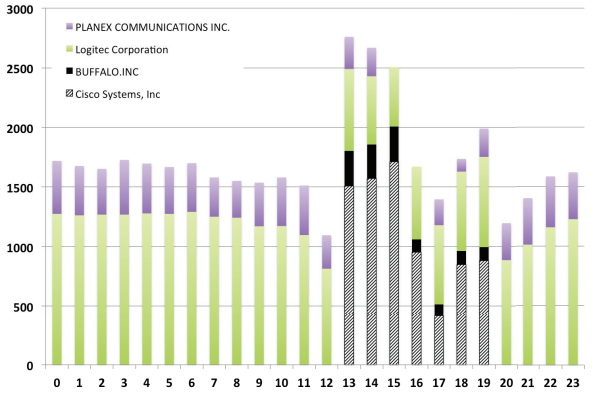


図 7 SICT18 の時間ごとのベンダー構成比（横軸：時間［0 時から 23 時］，縦軸：合計 BSSID 数）
Fig. 7 Vendor composition ratio of SICT18 (horizontal axis: hour, vertical axis: the total number of BSSID).

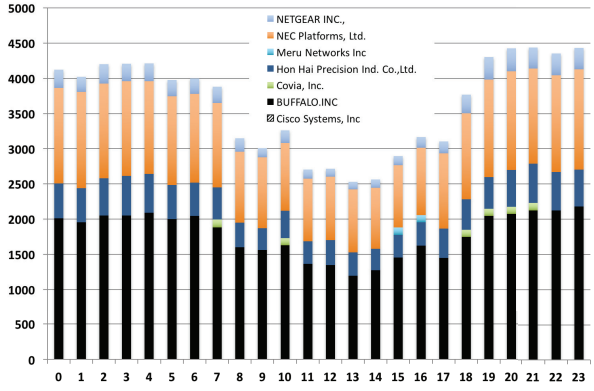


図 8 SICT20 の時間ごとのベンダー構成比（横軸：時間［0 時から 23 時］，縦軸：合計 BSSID 数）
Fig. 8 Vendor composition ratio of SICT20 (horizontal axis: hour, vertical axis: the total number of BSSID).

4.4.2 被験者の時間帯ごとのベンダー構成比

図 6 と**図 7**，**図 8** は，SICT16 と SICT18，SICT20 の被験者の各時間における BSSID の観測数の合計を示した

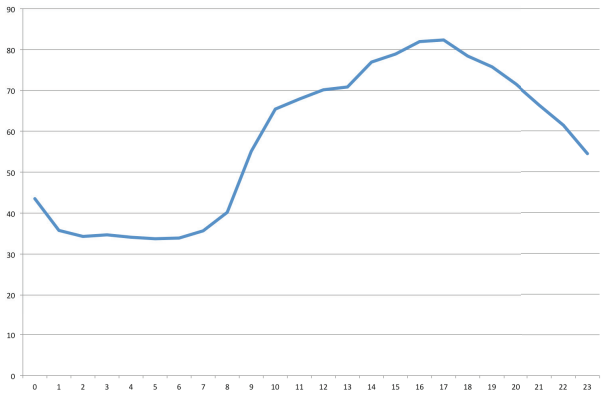


図 9 時間ごとの全被験者データの平均 MAC アドレス数（横軸：時間［0 時から 23 時］，縦軸：平均 MAC アドレス数）

Fig. 9 The number of hourly average MAC address of all volunteers (horizontal axis: hour, vertical axis: the average MAC address).

図である．棒グラフは，観測された BSSID をベンダーごとに合計しており，この図が各時間におけるアクセスポイントのベンダー構成比を表している．

SICT16 の例で示すと，30 日分のデータの合計として 7,490 種類の BSSID が観測され，その全観測回数の合計は 229,282 回であった．そのうち，全観測回数の約 75%に相当する数が観測回数上位の 91 種類の BSSID のみで計上されており，残りの約 7,400 種類は観測回数が低頻度の BSSID となる．各図からは，出現回数が低頻度の BSSID を除いている．

図 6 と図 7 はいずれも日中帯に Cisco の BSSID が多数観測されていることが分かる．さらに，いずれも日中帯は観測される BSSID 数が増加し，夜間帯とベンダー構成が明確に異なっていることが分かる．一方，16 名の被験者のうち，図 8 の SICT20 のみ，日中と夜間で全体的に BSSID の観測数が多く，日中と夜間でベンダー構成がほとんど変わらない結果となった．SICT20 のような被験者の場合，ベンダー構成比のみでは行動を推定することが困難である．

図 9 は，全被験者が収集した時間ごとの平均 MAC アドレス数を示している．平均値のため必ずしもすべての日で同じ傾向となるわけではないが，大部分の被験者にとって MAC アドレスが少ない時間帯が 2 時から 6 時にあり，10 時に急激に増加し，17 時をピークに減少していることが分かる．これは，1 日の生活習慣の検証で得た結果（図 3）と組み合わせると，在宅していると推定される時間帯とそれ以外の時間帯と一致しており，在宅中はアクセスポイントが少ない傾向にあることも分かる．

図 10 は，図 9 における特徴的な時間（0 時，4 時，10 時，17 時）のベンダー分布（図 6〜図 8 と同様に観測数が低頻度のベンダーを除いた分布）を示している．上下にある 2 つずつの図は夜と日中を表しており，上段の 0 時と 4 時の結果からは明らかに Buffalo の比率が高いことが分かる．一方，下段の 10 時，17 時は Buffalo の比率が小さくなり，Cisco の比率が大きくなっていることが分かる．これは，Buffalo が家庭用を中心に業務用まで取り扱うベンダーである一方，Cisco は業務用アクセスポイント製品を取り扱うベンダーとして一般家庭での利用が少ないためである．同様に，夜間帯に見られるベンダー名には Logitec，PLANEX などの同じく家庭用製品を主に取り扱っているベンダーが見られる．

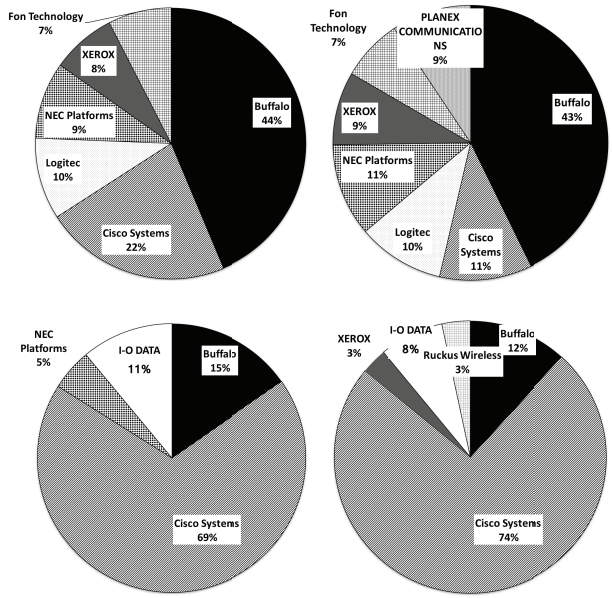


図 10 00 時（左上），04 時（右上），10 時（左下），17 時（右下）における各ベンダーの割合

Fig. 10 Vendor composition ratio: 0 am (top left), 4 am (top right), 10 am (bottom left), 5 pm (bottom right).

アクセスポイント製品の利用に明確な区分があるわけではなく，業務用を家庭で，家庭用を業務で使用することはできる．しかし，各製品の価格帯の違いとベンダーごとの製品ポートフォリオの差から，BSSID に含まれる OUI から得られるベンダー名の構成を確認することで，場所の傾向を推測できる可能性があることを本実験で確認できた．この結果から，夜間自宅に帰らずにオフィスや学校にいるような状況でも，BSSID リストからベンダーの構成比を知ることで，ある時間における居場所の推定を行うことが可能と考えられる．

5. 考察

5 章では，本実験で得られた結果についてベンダー構成比とユーザ行動の関係に関する考察を行う．

図 9 より時間帯ごとにベンダー分布が変わることが傾向が確認できた．本章では特徴的なベンダーのうち，特に Cisco と Buffalo の 2 つのベンダーに着目し，評価には相関比を用いた．

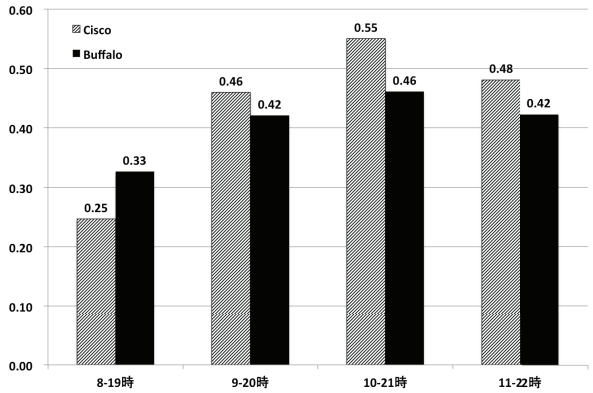


図 11 Buffalo および Cisco の日中と夜間の相関比の全被験者平均（横軸：日中とした時間帯，縦軸：相関比）

Fig. 11 Correlation ratio between Cisco and Buffalo during daytime and nighttime (horizontal axis: hours of daytime, vertical axis: correlation ratio).

5.1 相関比の定義

5 章で評価に用いる相関比の定義を示す．

対象となるデータを相関の有無を評価したい n 個のグループに分ける．各グループ内のデータ 1 つ 1 つをそれぞれのグループの平均から引いたものを 2 乗し合計した偏差平方和 S_1，S_2，S_3，...，S_n を求める．さらに，この各グループの偏差平方和を合計したものを級内変動 S_w とする．

$$S_w = S_1 + S_2 + S_3 ... + S_n$$

続いて，級間変動 S_b を求める．各グループ内のデータの個数を N_1，N_2，N_3，...，N_n とする．各グループのデータの平均を $\overline{X}_1$，$\overline{X}_2$，$\overline{X}_3$，...，$\overline{X}_n$ とし，全体平均を $\overline{X}$ と表す．

$$S_b = N_1 \times (\overline{X}_1 - \overline{X})^2 + N_2 \times (\overline{X}_2 - \overline{X})^2 + N_3 \times (\overline{X}_3 - \overline{X})^2 + ... + N_n \times (\overline{X}_n - \overline{X})^2$$

S と S_w，S_b の関係は次のように表せる．S は全体の偏差平方和である．

$$S = S_w + S_b$$

相関比 η^2 は次の式で表される．

$$\eta^2 = \frac{S_b}{S_w + S_b} = \frac{(S - S_w)}{S}$$

関係が最も強いとき，$S_w = 0$ で $\eta^2 = 1$ となる．逆に，$S_w = 1$ のとき，$\eta^2 = 0$ となる．本稿では，相関比 0.4 以上で相関があり，0.6 以上でやや強い相関，0.8 以上で強い相関があると考える．

5.2 日中と夜間とベンダーの相関

日中と夜間の Cisco と Buffalo の相関比は，**図 11** に示したとおり，相関が見られた．**表 4** は，図 11 で特徴的な相関を示した被験者の結果の比較である．

表 4 SICT16 と SICT18 の半日ごとの平均相関比の比較

Table 4 Comparison of average half day correlation ratios of SICT16 and SICT18.

ID	Buffalo	Cicso
SICT16	0.73	0.72
SICT18	0.30	0.31

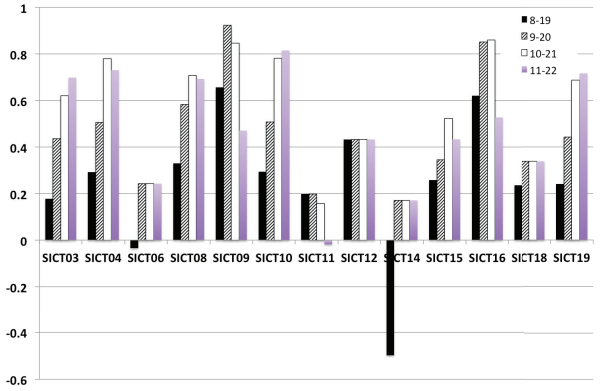


図 12 Cisco の半日の相関（8 時，9 時，10 時，11 時）（横軸：被験者 ID，縦軸：相関比）

Fig. 12 Correlation ratio of Cisco during half day (horizontal axis: volunteer id, vertical axis: correlation ratio).

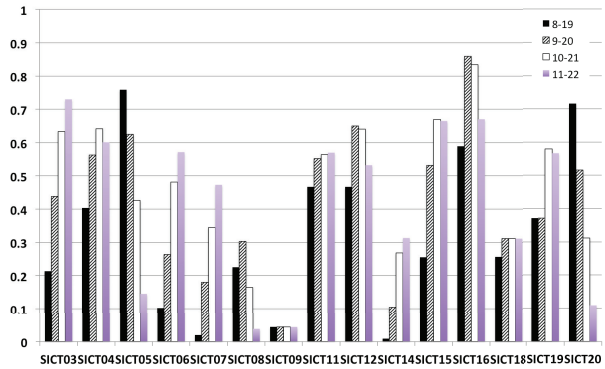


図 13 Buffalo の半日の相関（8 時，9 時，10 時，11 時）（横軸：被験者 ID，縦軸：相関比）

Fig. 13 Correlation ratio of Buffalo during half day (horizontal axis: volunteer id, vertical axis: correlation ratio).

図 12，**図 13** は Cisco と Buffalo の 12 時間（半日）ごとの相関を 8 時から，9 時，10 時，11 時と開始時間を変えて 4 種類求めたものである．5.1 節の相関の定義と算出方法について，図 11 の Cisco の例を用いて示す．ここでは 1 日を 12 時間ごと半日に区切った場合に Cisco が有意に相関を持つかを評価することが目的である．したがって，グループ数は $n = 2$ 個となる．偏差平方和 S_1 と S_2 は，各時間の Cisco の BSSID の観測数の和から求める．S_1 と S_2 のグループについて，図 11 では 4 パターンの分け方で比較しているが，ここでは 8 時から 19 時を例に取る．S_1 では 8 時～19 時の各時間の Cisco の BSSID の観測数から偏差平方和を求め，S_2 では残りの時間の偏差平方和を求める．級内変動は $S_w = S_1 + S_2$ となる．各グループ内のデータ

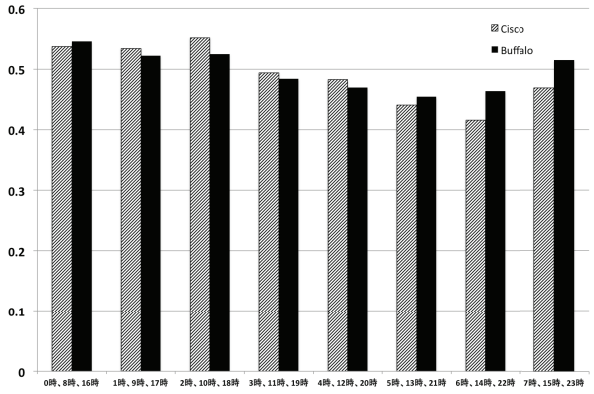


図 14 Cisco と Buffalo の 8 時間ごとの相関（横軸：各時間帯の開始時間，縦軸：相関比）

Fig. 14 8 hour correlation ratio between Cisco and Buffalo (horizontal axis: hours of daytime, vertical axis: correlation ratio).

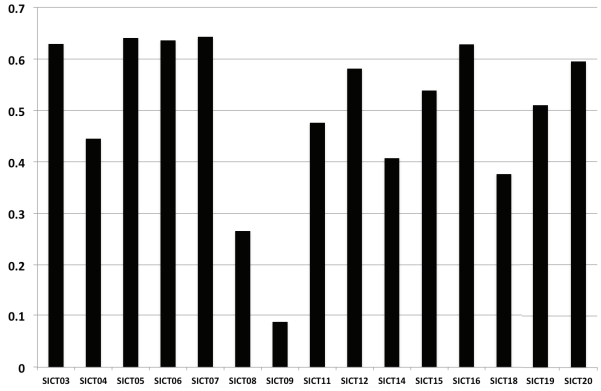


図 15 被験者ごとの Buffalo の 8 時間区切りの相関（横軸：被験者 ID，縦軸：相関比）

Fig. 15 8 hour correlation ratio for each volunteer (horizontal axis: volunteer id, vertical axis: correlation ratio).

の個数は 12 時間ごとであり，$N_1 = 12$，$N_2 = 12$ となる．各グループのデータの平均 $\overline{X}_1$，$\overline{X}_2$ は，それぞれ 8 時〜19 時とその残りの 1 時間ごとの Cisco の BSSID の観測数の平均である．全体平均 $\overline{X}$ は，1 時間ごとの Cisco の BSSID の観測数の和を，1 日の 24 時間で割った平均である．以降，定義のとおり相関比 η^2 を求める．図 11 では全被験者の相関比の平均を求めるため，同様に 16 名の被験者ごとの相関比を求めた結果，$\eta^2 = 0.25$ が得られた．相関比が低いことから，全体として 8 時から 19 時の時間帯に Cisco の BSSID が観測される事象の間の相関は弱いと考えらえる．裏を返すと，Cisco の BSSID の観測と 8 時から 19 時の時間帯との間に関係があると判断はできないということになる．以後，**図 14**，**図 15** までの相関比は同様に求めた．

図 12，図 13 で高い相関が見られた SICT16 のベンダー構成は，図 6 に見られるように，大きく 2 種類のベンダー構成に分けられるため，高い相関比を示したと考えられる．一方，SICT18 も，時間ごとのベンダー構成を 2 種類に分けることが可能であるが，日中帯のベンダー構成を示す時間は 14 時から 20 時の 7 時間分と短くなっているため，12 時間分のデータで相関を求める半日では高い相関が得られなかった．

5.3 8 時間ごとの時間帯とベンダーの相関

一日を 8 時間ごとに 3 分割した場合の各時間帯とベンダーの相関比を評価した．ここでは S_1 と S_2 のグループを，8 時間分のデータから求める S_1 と残りの 16 時間分から求める S_2 に分けた．

図 15 は，8 時間ごとに区切りとした場合の Buffalo の相関比を被験者ごとに示した図である．SICT09 は 0.087 とほとんど相関がないことを示している．これは SICT09 で観測される Buffalo が観測された時間が 23 時のみで，観測数も少ないためである．SICT09 のデータを除外した場合の Buffalo の平均相関は，0.50 から 0.53 に 0.03 向上する．

5.4 被験者の周辺環境による偏り

本実験の被験者は東京大学の学生および職員からなっており，都市圏に生活する被験者の情報で評価を行っている．公衆無線 LAN アクセスポイントなどは，都市圏での普及が進んでいる一方，その他の地域ではまだまだ普及が進んでいない現状がある．また，アパートなどの集合住宅と一軒家とでは自宅周辺のアクセスポイントの傾向も変わることが予想される．このように，地域や環境によって得られる情報が異なるため，より多くの被験者からデータを収集し，評価を行う必要がある．ただし，アクセスポイント数が少ない環境にいる被験者の場合，そもそも特定の BSSID を観測した段階で個人特定がなされてしまう可能性もあり，本稿におけるプライバシの検討とは異なる方針での検討が必要と考えられる．

5.5 ベンダー構成比の行動推定への適用

16 名の被験者 30 日分のデータを収集することで，自宅とオフィス・学校に相当する場所では周辺アクセスポイントのベンダー構成や観測される BSSID 数が異なることが分かった．これにより，従来の行動履歴を用いた研究のように GPS の位置情報や位置情報データベースの利用なしに，行動推定ができる可能性を示すことができた．一方で，ベンダー構成は被験者ごとに違っており，時間帯におけるベンダー構成比の違いだけでなく，その内訳についても検討することでより的確に BSSID と行動の関係を評価できると期待される．

5.6 提案手法による攻撃の可能性と対策について

提案手法は，ユーザの位置情報を直接取得できる既存手法と比較し，家やオフィス，学校などの位置情報の種類の判別にとどまっており，深刻なプライバシ侵害に直結する

ものではない．しかし，位置情報データベースの有無の制約を受けないという点で攻撃の種類を広げるものである．たとえば，Hayashi らの研究結果 [20] に従えば，提案手法により 1 日の居場所のうち 6 割に該当する時間を推定できる可能性が示されている．逆説的に，残り 4 割の時間がそれ以外の場所であることを推定できる可能性があり，各時間帯の種別ごとに有効な攻撃手法が提案されれば，攻撃対象者の実際の場所を知らなくても攻撃できる可能性が広がる．また，Hayashi らの提案手法は，自宅などの安全な場所と，職場などの比較的安全な場所，そのほかの公共の場所で認証の種類を変えることで，場所の種別によって安全性と利便性を調整可能な認証手法である．この手法に対して，我々の提案手法を用いると Wi-Fi 情報だけでどの認証手法が使われるかを推定でき，攻撃者は自身が有利な認証手法をユーザが利用しているタイミングを選択的に攻撃できる可能性もある．

周辺のアクセスポイント情報を収集する手段について具体的に定義しないが，起こりうる攻撃としては悪意あるアプリケーションが漏洩した Wi-Fi 情報を利用することが考えられる．提案手法に対しては，OS レベルで BSSID に対するアクセス制限を設けることで防止が可能である．しかし，現在も適切なアクセス権の設定がなされていないことから，位置情報のリスクに比べ，Wi-Fi 情報のプライバシリスクに関する認識が低いことが分かる．現在，Pokemon GO [*5]，Ingress [*6] などの位置情報を用いたゲームが普及しており，ユーザはこれらのアプリケーションに対して自身の端末の位置情報アクセスを許可している．これらのゲームが攻撃者により配布された悪意あるアプリケーションだった場合，「カレログ」の事例のような情報漏洩などのリスクが存在する．同様に今回提起した Wi-Fi 情報のリスクについても，十分なリテラシーがなければ容易にアクセスを許可してしまう可能性があり，システムのみの対策で対応することは難しいと考えられる．

6. まとめ

本研究では，ユーザ周辺のアクセスポイントの Wi-Fi 情報からベンダー情報を用いることで，ユーザの所在に関する情報を推定する攻撃手法の提案を行った．提案手法の評価として，日中はオフィスや学校，夜間は在宅といった時間と場所の関係を仮定し，16 名の被験者から収集したデータからベンダー情報と時間の相関を求めた．実験結果から Cisco，Buffalo などが相関比 0.5 以上の相関を示すことを確認し，時間ごとに観測されるベンダーに相関があることを示した．結果，ベンダー構成比が，自宅や職場といったユーザの場所のカテゴリを推定するために有用な情報であることが確認でき，従来手法のような位置情報データベースがなくとも攻撃が可能ということが分かった．提案した攻撃手法に対しては，BSSID のベンダー情報をランダム化する対策，または OS レベルでアクセス制限を行うなどの対策が考えられる．また，位置情報のプライバシリスクと同様にシステム的な対応だけでなく，Wi-Fi 情報のリスクについても今後ユーザのリテラシー向上が望まれる．

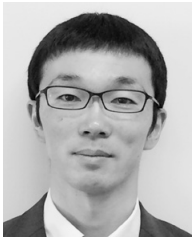
謝辞 本稿の研究は，次世代個人認証技術講座（三菱 UFJ ニコス寄付講座）による．

[*5] http://www.pokemongo.jp
[*6] https://www.ingress.com

参考文献

[1] 手塚博久，伊藤浩二，村山卓弥，瀬古俊一，西野正彬，武藤伸洋，阿部匡伸：ライフログを活用したレストランレコメンド，NTT 技術ジャーナル，Vol.22, No.7, pp.29–32 (2010).
[2] Kobayashi, R. and Yamaguchi, R.S.: A behavior authentication method using wi-fi bssids around smartphone carried by a user, *2015 3rd International Symposium on Computing and Networking* (*CANDAR*), pp.463–469, IEEE (2015).
[3] Zhang, F., Kondoro, A. and Muftic, S.: Location-based authentication and authorization using smart phones, *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), pp.1285–1292, IEEE (2012).
[4] トレンドマイクロ：スマホを狙う不正アプリの最新事情，トレンドマイクロ is702（オンライン），入手先 ⟨https://www.is702.jp/special/1938/⟩（参照 2017-04-03）．
[5] 折尾彰吾，上田 浩，上原哲太郎，津田 侑：ワイヤレスデバイスのもたらすロケーションプライバシー問題に関する一考察，コンピュータセキュリティシンポジウム 2012 論文集，pp.262–269 (2012).
[6] Apple：プライバシーと位置情報サービスについて，Apple（オンライン），入手先 ⟨https://support.apple.com/ja-jp/HT203033⟩（参照 2016-06-09）．
[7] クウジット株式会社：PlaceEngine, クウジット株式会社 (online), available from ⟨http://www.placeengine.com⟩ (accessed 2016-06-09).
[8] NTT ドコモ：株式会社 NTT ドコモ，NTT docomo（オンライン），入手先 ⟨https://www.nttdocomo.co.jp/service/wifi/docomo_wifi/area/index.html⟩（参照 2017-04-03）．
[9] 中村暢宏，上原哲太郎ほか：Wi-Fi モバイルルータにおける位置トレーサビリティの検討と対策，研究報告インターネットと運用技術（IOT），Vol.2016, No.11, pp.1–7 (2016).
[10] Skyhook：Skyhook 社，Skyhook（オンライン），入手先 ⟨http://www.skyhookwireless.com⟩（参照 2016-05-18）．
[11] WiGLE: WiGLE, WiGLE (online), available from ⟨https://wigle.net⟩ (accessed 2016-05-18).
[12] Skyhook：WIFI 及び携帯基地局信号のデータベース，Skyhook（オンライン），入手先 ⟨http://www.skyhookwireless.com/coverage-japan⟩（参照 2016-05-18）．
[13] Google：位置情報サービスでアクセスポイントを設定する，Google（オンライン），入手先 ⟨https://support.google.com/nexus/answer/1725632⟩（参照 2016-06-09）．
[14] Peng, Z., Kaji, K. and Kawaguchi, N.: Privacy protection in WiFi-based location estimation, *2014 7th International Conference on Mobile Computing and Ubiquitous Networking* (*ICMU*), pp.62–67, IEEE (2014).
[15] Krumm, J.: A survey of computational location privacy, *Personal and Ubiquitous Computing*, Vol.13, No.6,

pp.391–399 (2009).
[16] Google: Android 6.0 Changes, Google (online), available from ⟨https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html⟩ (accessed 2016-06-10).
[17] Riva, O., Qin, C., Strauss, K. and Lymberopoulos, D.: Progressive Authentication: Deciding When to Authenticate on Mobile Phones, *USENIX Security Symposium*, pp.301–316 (2012).
[18] Shi, E., Niu, Y., Jakobsson, M. and Chow, R.: Implicit authentication through learning user behavior, *Information Security*, pp.99–113, Springer (2011).
[19] Khan, H. and Hengartner, U.: Towards application-centric implicit authentication on smartphones, *Proc. 15th Workshop on Mobile Computing Systems and Applications*, p.10, ACM (2014).
[20] Hayashi, E., Das, S., Amini, S., Hong, J. and Oakley, I.: Casa: context-aware scalable authentication, *Proc. 9th Symposium on Usable Privacy and Security*, p.3, ACM (2013).
[21] Albayram, Y., Kentros, S., Jiang, R. and Bamis, A.: A method for improving mobile authentication using human spatio-temporal behavior, *2013 IEEE Symposium on Computers and Communications* (*ISCC*), pp.000305–000311, IEEE (2013).
[22] Google：アカウントアクティビティ，Google（オンライン），入手先 ⟨https://support.google.com/mail/answer/45938?hl=ja⟩（参照 2016-06-09）.
[23] Sapiezynski, P., Stopczynski, A., Gatej, R. and Lehmann, S.: Tracking Human Mobility Using WiFi Signals, *PloS one*, Vol.10, No.7, p.e0130824 (2015).
[24] IEEE: IEEE Standards Association (online), available from ⟨http://standards.ieee.org/develop/regauth/oui/public.html⟩ (accessed 2016-06-09).
[25] IEEE: Standard Group MAC Addresses: A Tutorial Guide (online), available from ⟨http://standards.ieee.org/develop/regauth/tut/macgrp.pdf⟩ (accessed 2016-06-09).



鈴木 宏哉 （正会員）

東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター学術支援専門職員．慶應義塾大学理工学部情報工学科卒業．同大学大学院修士課程修了．日本サード・パーティ株式会社勤務．2014 年 5 月より現職．電子情報通信学会，言語処理学会，各会員．

山口 利恵 （正会員）

東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター特任准教授．博士（情報理工学）．産業技術総合研究所研究員，内閣官房情報セキュリティセンター員を経て，2013 年 6 月より現職．電子情報通信学会，人工知能学会，各会員．