Vol.2019-IOT-44 No.2
2019/3/7

ユーザの行動パターンに注目した無線LAN利用における認証

八切 有市[1,a)]　青木 茂樹[1,b)]　宮本 貴朗[1]

概要：既存の無線 LAN システムで広く用いられているセキュリティ技術は接続時のみ有効であり，接続済みの無線端末を第三者が利用する場合などには対応できなかった．本稿では，無線 LAN 利用ログ情報に注目することで，本人による端末の利用であるかを判別し，継続的に不正利用を監視する手法を提案する．まず，無線 LAN コントローラから SNMP を用いて無線 LAN 利用ログ情報を取得し，接続したアクセスポイント名および送受信パケット量の特徴量を抽出する．次に，端末ごとの位置情報の遷移と送受信パケット量の時系列変化をユーザの行動パターンとして確率モデルで学習する．その後，学習したモデルとテスト期間におけるユーザの行動パターンを比較して認証する．実験では，大阪府立大学における無線 LAN システムの無線 LAN 利用ログから行動パターンを学習し，認証した．

キーワード：無線 LAN，個人認証，行動認証，セキュリティ

Authentification Focused on User Behavior in Wireless LAN

Yuichi Yagiri[1,a)]　Shigeki Aoki[1,b)]　Takao Miyamoto[1]

Abstract: Existing security technologies in wireless LAN are effective only when connecting with wireless LAN. Thus, these technologies cannot detect unauthorized use of wireless device after connection. In this research, we focus on wireless LAN usage logs and propose a method to authenticate wireless device continuously. First, we acquire wireless LAN usage logs from a wireless LAN controller using SNMP. We extract connected access point name, transmitted packet quantity and received packet quantity from the wireless LAN usage logs. Next, we generate time-series variations of these extracted features as behavior pattern. We constract stochastic model of the behavior pattern. Finally we compare a behavior pattern in a test period with the stochastic model to authenticate wireless device. For experiment, we learned behavior patterns from wireless LAN usage logs at Osaka Prefecture University and authenticated wireless devices.

Keywords: wireless LAN, user authentification, behavior authentification, security

1. はじめに

近年，ノート PC やスマートフォン等のモバイル端末の普及に伴い，無線 LAN の利用が増加している．従来，組織においては個人や部署単位で独自に無線アクセスポイント（以下，AP）を設置し運営していることが多かったが，無線チャネルの枯渇や電波の干渉など管理の難しさから，今日では組織全体で統括された無線 LAN 環境（無線 LAN システム）を整備する動きが盛んになっている．これらの無線 LAN システムでは，無線 LAN の不正な利用を防ぐためにセキュリティ対策が講じられている．無線 LAN システムで一般に用いられるセキュリティ技術として，MAC アドレスフィルタリングや暗号化通信などが挙げられる．しかし，これらのセキュリティ技術は無線端末が無線 LAN システムに接続するまでの対策であり，接続済みの無線端末を第三者が利用する場合などに対応できない．

[1] 大阪府立大学大学院人間社会システム科学研究科
Graduate School of Humanities and Sustainable System Sciences, Osaka Prifecture Uniersity
[a)] sxa01296@edu.osakafu-u.ac.jp
[b)] aoki@kis.osakafu-u.ac.jp

本研究では，無線 LAN 利用ユーザが無線 LAN システムに接続した際に得られるログ（以下，無線 LAN 利用ログ）から特徴を抽出し，ユーザの認証を行う手法を提案する．具体的には，端末ごとの位置情報の遷移および送受信パケット量の時系列変化をユーザの行動パターンとして抽出する．抽出した行動パターンを確率モデルによりモデル化する．実験では，大阪府立大学（以下，本学）における無線 LAN 利用ログに対し提案手法を適用し，端末ごとのモデルを構築した．構築したモデルと抽出した行動パターンを比較することでユーザの認証を行った．

2. 関連研究

無線端末上で得られる位置情報を用いて認証を行う平岩らの研究 [1] では，Wi-Fi の情報から得られる行動の特徴が行動認証に有用であるかを検討することを目的とし，無線端末の位置情報から無線端末上で，行動モデルの構築およびテストデータとの認証を行っている．具体的には，Wi-Fi のネットワーク識別子である BSSID と RSSI(受信信号強度) に着目し，これらの特徴を一時刻ごとに一つの要素とし凝集型階層的クラスタリング [2] を行う．得られたクラスタを状態とみなすことで状態遷移列を生成し，単純マルコフモデルによりモデル化し認証を行っている．被験者の持つ端末上で Wi-Fi の情報を抽出し評価実験を行い，Wi-Fi の位置情報が認証を行う上で有用であることを示している．

ユーザの位置情報に着目し無線 LAN や画像センサー，GPS，カメラやレーザを用いた測位から得られた動線を解析した研究として，鈴木らの研究 [3] や淺原らの研究 [4] が挙げられる．鈴木らは，人物の動線データのパターン分類および分類されたパターンのどれにも当てはまらない人物の検出手法を提案している．ここで，k-means クラスタリングを行うことで人物動線データを分類できることや，隠れマルコフモデル (HMM) および固有値分解により位置情報の時系列データから人物の行動パターンの傾向を安定的に学習できることを示している．淺原らは，歩行者の位置情報から歩行者の行動を予測することや例外行動を検出することなどを目的とし，測位機能付きの携帯端末から抽出した動線データに混合確率分布によるクラスタリングを適用し遷移や移動などの状態を示す記号列に変換することで HMM の一種と見なせる混合マルコフモデル (MCM) によるモデル化を行っている．実験では，シミュレーションによる仮想的なデータを用い，学習モデルによる高い行動予測精度を達成している．これらの研究 [1,3,4] で用いられている手法は，位置情報のみを考慮したモデル化を行っているため，別のユーザの同じ場所における無線端末の不正利用などを検出することができないという問題点がある．

本研究では無線 LAN コントローラから接続している無線端末群のそれぞれの端末の位置情報と送受信パケット量を取得し，これらの特徴量を用いて端末ごとのモデルを構築することで，無線 LAN システムに不正に接続している端末が存在していないかを継続的に監視するシステムを提案する．

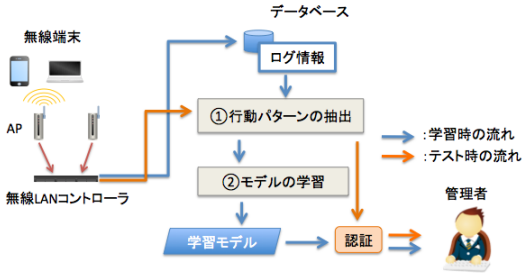

図 1 提案システムの構成

表 1 提案手法に用いる情報

情報	説明
MAC アドレス	端末を一意に示す文字列.
接続した AP 名	AP を識別する一意な文字列.
送信パケット量	端末が送信した単位時間ごとのパケット量.
受信パケット量	端末が受信した単位時間ごとのパケット量.

3. 提案手法

手法のおおまかな流れを図 1 に示す．まず組織に設置してある各 AP から，無線 LAN に接続した端末の無線 LAN 利用ログ情報を無線コントローラにおいて単位時間ごとに収集し，これらのログ情報および収集した時刻をデータベースに保存する．次にデータベースから特徴量を抽出し，特徴量の時系列変化を行動パターンとして抽出する．そして，抽出した行動パターンを確率モデルで学習する．テスト期間に得られた無線 LAN 利用ログから同様に行動パターンを抽出し，端末の確率モデルを用いて抽出した行動パターンをどのくらいの確率で再現できるかを算出する．算出した確率がしきい値を下回る場合，不正利用端末として管理者に通知する．この処理をテスト期間に接続している全ての端末に対して行う．以下の節では，それぞれの処理について詳細に述べる．

3.1 無線 LAN 利用ログの収集

無線 LAN コントローラから SNMP を用いて単位時間ごとの無線 LAN 利用ログを取得する．得られる無線 LAN 利用ログには，IP アドレス，MAC アドレス，接続した AP 名および送受信トラフィック量などが含まれている．本手法では，ログに含まれる情報のうち，MAC アドレス，接続した AP 名，送信パケット量および受信パケット量を用いる．これらの情報の説明を表 1 に示す．接続した AP 名，送信パケット量，受信パケット量および取得した時刻情報をデータベースに登録する．

3.2 特徴量の抽出および抽出した特徴量を用いた行動パターンの生成

一般に，ユーザの行動は滞在場所での無線利用や会議場所への移動，昼食・夕食時の移動など，1 日ごとにある程度類似した遷移やネットワークの利用が多いと考えられる．そこで，データベースからある端末の接続した AP 名，送信パケット量および受信パケット量の 1 日の時系列データを抽出する．そして，抽出した時系列データを記号列に変換し，ユーザの 1 日の行動パターンとする．以下では，時系列データの記号列への変換方法について述べる．

- 接続した AP 名

  一般的に組織で運用されている AP は，それぞれを識別するために一意な AP 名が付けられており，組織はそれぞれの AP の位置情報を保有している．無線端末は基本的にその場所で一番電波強度が強い AP に接続されるように設計されており，端末が AP に近いほど電波強度が強くなる．したがって，接続した AP 名がユーザのおおよその位置情報を示す．AP 名を基に取得した位置情報のそれぞれに対して，一意な位置記号 v を与える．位置記号 v は次式の有限集合で表す．ここで，m は設置されている AP の総数である．

  $$V = \{v_1, v_2, ..., v_m\} \tag{1}$$

  得られた位置記号 v の記号列を位置情報の遷移を示す位置の行動パターンとする．

- 送受信パケット量

  送受信パケット量は，ネットワークの利用方法により大きく異なる．同一ユーザによって同じ様に利用された時に，同じ記号が割り当てられるように，送信パケット量および受信パケット量をそれぞれ一定の区間ごとに分割し，各区間に一意な記号を付与する．これを送信記号 h および受信記号 c とする．送信記号 h および受信記号 c は次式の有限集合で表す．ここで，q は送信パケット量の区間の総数であり，z は受信パケット量の区間の総数である．

  $$H = \{h_1, h_2, ..., h_q\} \tag{2}$$

  $$C = \{c_1, c_2, ..., c_z\} \tag{3}$$

  送信記号および受信記号の区間の総数が設置されている AP の総数と等しくなるように，送信パケット量および受信パケット量の区間の幅を決定する．データベースに登録されている全ての端末における送信パケット量および受信パケット量の最大値を設置されている AP の総数で割り小数点以下を切り上げた値を送信パケット区間幅 u および受信パケット区間幅 y とする．ここで，送信記号 h_1 は 0 パケットから始まる区間であり，送信記号 h_d は $((d-1)u)$ パケットから $(du-1)$ パケットの区間である．また，受信記号 c_1 は 0 パケットから始まる区間であり，受信記号 c_d は $((d-1)y)$ パケットから $(dy-1)$ パケットの区間である．

  抽出した送信パケット量および受信パケット量を送信記号 h および受信記号 c に変換する．ここで，送信記号 h および受信記号 c は，抽出した送信パケット量および受信パケット量が含まれている区間を示す．得られた送信記号および受信記号の記号列をそれぞれ送信パケットの行動パターンおよび受信パケットの行動パターンとする．

3.3 行動パターンの学習フェーズ

3.3.1 ユーザの行動パターン

時刻 i に得られた端末の位置記号を b_i，送信記号を a_i，受信記号を r_i，1 日の位置の行動パターンを B，送信パケットの行動パターンを A，受信パケットの行動パターンを R とし，B，A，R を次式の記号列で表す．

$$B = b_1 b_2 ... b_i ... b_T \tag{4}$$

$$A = a_1 a_2 ... a_i ... a_T \tag{5}$$

$$R = r_1 r_2 ... r_i ... r_T \tag{6}$$

ここで，T は記号列長である．そして，時刻 i に注目している端末の情報が無線 LAN 利用ログに記録されていない場合，記号を出力しない．そのため，日によって記号列長 T は異なる．

3.3.2 滞留と移動の識別

学習の前段階として，端末の滞留と移動を識別する．滞留と移動の識別には端末の位置の行動パターンを用いる．時刻 i における端末の滞留 S および移動 M を示すラベルを l_i とする．l_i を次式のルールにより識別する．

$$l_i = \begin{cases} S & if \quad i = 1, b_{i-1} = b_i \\ M & otherwise \end{cases} \tag{7}$$

端末が常に同じ場所に置いてある場合，異なるユーザによる同じ場所での不正利用を検出することは難しい．そこで，滞留時の学習では，位置の行動パターン，送信パケットの行動パターンおよび受信パケットの行動パターンを用いる．

移動時の位置情報の遷移にはユーザの特性が出やすく，移動時の学習において位置の行動パターンに加えて送信パケットの行動パターンおよび受信パケットの行動パターンを用いると，確率モデルの精度が下がる可能性がある．そこで，移動時の学習では位置の行動パターンのみを用いる．

3.3.3 滞留時の学習

滞留時におけるパラメータとして，出現頻度 F を考え

る．F_{v_k} は学習期間に観測された全ての位置の行動パターン B において，$l_i = S$ を満たす全ての b_i のうち，位置記号 v_k が出現する（記録されている）回数を表す．F_{h_k} は端末の学習期間に観測された全ての送信パケットの行動パターン A において，$l_i = S$ を満たす全ての a_i のうち，送信記号 h_k が出現する回数を表す．F_{c_k} は学習期間に観測された全ての受信パケットの行動パターン R において，$l_i = S$ を満たす全ての r_i のうち，受信記号 c_k が出現する回数を表す．位置記号の有限集合 V，送信記号の有限集合 H および受信記号の有限集合 C における全ての要素に対して，出現頻度をカウントし，それぞれ $\{(v_1, F_{v_1}), (v_2, F_{v_2})...(v_m, F_{v_m})\}$，
$\{(h_1, F_{h_1}), (h_2, F_{h_2})...(h_q, F_{h_q})\}$，
$\{(c_1, F_{c_1}), (c_2, F_{c_2})...(c_z, F_{c_z})\}$ として保存する．

3.3.4 移動時の学習

移動時におけるパラメータとして，位置記号と 1 時刻前の位置記号を考慮した遷移の出現頻度 Z を考える．$Z_{v_g v_k}$ は学習期間に観測された全ての位置の行動パターン B において，$l_i = M$ を満たす全ての b_i のうち，時刻 i に位置記号 v_k，時刻 $i-1$ に位置記号 v_g が出現する回数と定義する．位置記号の有限集合 V における時刻 i の位置記号を表す要素と時刻 $i-1$ の位置記号を表す要素の全ての組み合わせに対して出現頻度をカウントし，$\{(v_1v_1, Z_{v_1v_1}), (v_1v_2, Z_{v_1v_2})...(v_mv_m, Z_{v_mv_m})\}$ として保存する．

3.4 行動パターンの認証フェーズ

新たに観測された行動パターンをテストデータとして，認証処理を行う．ここで，テストデータの行動パターン (位置の行動パターン $\tilde{B}$，送信パケットの行動パターン $\tilde{A}$，受信パケットの行動パターン $\tilde{R}$) を以下のように表す．

$$\tilde{B} = \tilde{b}_1\tilde{b}_2...\tilde{b}_i...\tilde{b}_{\tilde{T}} \tag{8}$$

$$\tilde{A} = \tilde{a}_1\tilde{a}_2...\tilde{a}_i...\tilde{a}_{\tilde{T}} \tag{9}$$

$$\tilde{R} = \tilde{r}_1\tilde{r}_2...\tilde{r}_i...\tilde{r}_{\tilde{T}} \tag{10}$$

ここで，$\tilde{T}$ はテストデータの行動パターンの系列長である．

まず，位置の行動パターン $\tilde{B}$ を参照して，式 (7) に基づいて滞留と移動を識別し $\tilde{l}_i$ を求める．そして，時刻 i の行動パターンのそれぞれの記号 $\tilde{b}_i, \tilde{a}_i, \tilde{r}_i$ の出現確率 P_i を次式で算出する．

$$P_i = \begin{cases} \sqrt[3]{\frac{F_{\tilde{b}_i}}{\sum_{j=1}^{m} F_{v_j}} \frac{F_{\tilde{a}_i}}{\sum_{j=1}^{q} F_{h_j}} \frac{F_{\tilde{r}_i}}{\sum_{j=1}^{z} F_{c_j}}} & if \ \ \tilde{l}_i = S \\ \frac{Z_{\tilde{b}_{i-1}\tilde{b}_i}}{\sum_{j=1}^{m} Z_{\tilde{b}_{i-1}v_j}} & otherwise \end{cases} \tag{11}$$

この式では，テストデータの行動パターンにおいて，滞留と判断した時刻については，位置の行動パターンの発生確率，送信パケットの行動パターンの発生確率，受信パケットの行動パターンの発生確率をそれぞれ求め，それらの積の立方根を求めて発生確率とし，移動と判断した時刻については位置の遷移情報の発生確率を用いている．ここで，ゼロ頻度問題の発生を回避するため，$F_{\tilde{b}_i}$，$F_{\tilde{a}_i}$，$F_{\tilde{r}_i}$ または $Z_{\tilde{b}_{i-1}\tilde{b}_i}$ が 0 である場合，$F_{\tilde{b}_i}$，$F_{\tilde{a}_i}$，$F_{\tilde{r}_i}$ または $Z_{\tilde{b}_{i-1}\tilde{b}_i}$ に十分小さい数 ε を与える．

そして，テストデータの行動パターンが学習モデルから生成される確率を示す対数尤度 U を次式で算出する．

$$U = \log_{10} \prod_{i=1}^{\tilde{T}} P_i \tag{12}$$

算出した対数尤度 U の値は，記号列長 $\tilde{T}$ の影響を受けるため，次式で正規化する．

$$D = \frac{U}{\tilde{T}} \tag{13}$$

正規化した対数尤度 D がしきい値未満の場合にテストデータの行動パターンは，不正利用端末であると識別し，管理者に通知する．

4. 評価実験

4.1 実験環境

4.1.1 実験のログデータ

実験では，本学の 2017 年 4 月 1 日 0 時から 2018 年 9 月 31 日 23 時 59 分までの 18 ヶ月分の無線 LAN 利用ログを用いた．このうち，2017 年 4 月 1 日 0 時から 2018 年 3 月 31 日 23 時 59 分までの無線 LAN 利用ログを学習データに利用し，2018 年 4 月 1 日 0 時から 2018 年 9 月 31 日 23 時 59 分までの無線 LAN 利用ログをテストデータに利用した．単位時間は 5 分とした．モデル構築には一定の学習データ量が必要である．また，テスト期間に利用されている端末を用いて認証するため，一定のテストデータ量も必要である．したがって，実験では学習期間内に 120 時間以上かつテスト期間内に 24 時間以上無線 LAN に繋がっている無線端末の無線 LAN 利用ログを利用した．

4.1.2 学習に用いる位置情報

本学の無線 LAN 利用ログでは，AP 名から AP が設置された棟 (棟情報とする) および階数，同じ階のどの AP であるか (AP 情報とする) を識別できる．AP の周辺に障害物がある場合や複数の AP が密集している場合などに，無線端末が必ずしも最寄りの AP に接続されるとは限らない．そこで，端末のおおよその現在地である棟情報に注目する．そして，棟情報を用いて端末が移動状態か滞留状態かを識別する．移動時の学習では，位置情報として棟情報に割り当てた記号を用いる．滞留時の学習では，位置情報として AP 情報に割り当てた記号を用いる．

4.2 評価手法

手法の評価において，端末のモデルを学習し，その端末のテストデータにおける行動パターンの正規化した対数尤度 D および他の端末のテストデータにおける行動パターンの正規化した対数尤度 D を算出する．この処理を全ての端末に対し適用する．これにより本人による利用を正しく判断する真陽性 (True Positive，TP) および他人による利用を誤って本人による利用であると判断する偽陽性 (False Positive，FP) のしきい値による変動を示す受信者動作特性曲線 (Receiver Operatorating Characteristic curve，ROC 曲線) を描く．そして，ROC 曲線を数値として評価し，1 に近ければ近いほど良いモデルであると判断できる AUC(Area Under the Curve) を算出する．実験では，提案手法の評価と，特徴としての送受信パケット量 (送受信パケット量特徴) が認証に有用であるかの評価を行う．ここでは，$\varepsilon = 0.5$ とする．

4.2.1 提案手法の評価

比較手法は単純マルコフモデルと HMM とする．提案手法，単純マルコフモデルおよび HMM の ROC 曲線を描き，それぞれの AUC を算出し比較することで提案手法を評価する．ここで，単純マルコフモデルおよび HMM は，棟情報の遷移を行動パターンとして確率モデルで学習した．

4.2.2 送受信パケット量特徴の評価

送受信パケット量特徴が認証に有効であるかを確認するため，提案手法の学習において送受信パケット量特徴を用いる場合と用いない場合の ROC 曲線を描き，それぞれの AUC を算出し比較する．送受信パケット量特徴を用いない手法をパケット非使用手法とする．パケット非使用手法では，滞留時と移動時に位置記号が出現する確率 P_i は，

$$P_i = \begin{cases} \frac{F_{\tilde{b}_i}}{\sum_{j=1}^{m} F_{v_j}} & if \quad \tilde{l}_i = S \\ \frac{Z_{\tilde{b}_{i-1}\tilde{b}_i}}{\sum_{j=1}^{m} Z_{\tilde{b}_{i-1}v_j}} & otherwise \end{cases} \tag{14}$$

となる．

4.3 実験結果

本学の無線 LAN に学習期間内に 120 時間以上繋がり，テスト期間内に 24 時間以上繋がった端末は 388 端末であった．送信パケット区間幅 u は 787000 パケットであり，受信パケット区間幅 y は 673000 パケットであった．

4.3.1 単純マルコフモデルおよび HMM との比較結果

提案手法，単純マルコフモデルおよび HMM の ROC 曲線を図 2 に示す．提案手法，単純マルコフモデルおよび HMM の AUC を表 2 に示す．図 2 より FP 値によって最も高い TP 値を示す手法が変わることがわかる．本研究では，不正利用を監視することを目的としているため，可能な限り FP 値を下げることを目指している．したがって，図 2 より FP 値が低い場合に最も高い TP 値を記録した提案手法が，不正利用を監視する手法として最も良い手法であることがわかった．また，表 2 より提案手法の AUC は単純マルコフモデルおよび HMM の AUC に比べ高く，提案手法が認証精度の高い手法であるといえる．このような結果が得られた原因として，提案手法では，端末の滞留と移動を分けて学習することで，滞留と移動を区別しない単純マルコフモデルおよび HMM と比べ，ユーザの特性がでやすいためと考えられる．また，別の原因として，提案手法は位置の行動パターンに加え送信パケットおよび受信パケットの行動パターンを確率モデルとして学習したことで，位置の行動パターンのみを考慮した単純マルコフモデルおよび HMM よりも，移動があまり見られない端末の学習モデルを高精度で構築できたためと考えられる．

表 2 提案手法，単純マルコフモデルおよび HMM の AUC

手法	AUC
提案手法	0.9128221
単純マルコフモデル	0.8553775
HMM	0.8956679

4.3.2 送受信パケット量特徴の有無の比較結果

送受信パケット特徴量が認証の要素として有用であるかを検証する．提案手法とパケット非使用手法の ROC 曲線を図 3 に示す．提案手法とパケット非使用手法の AUC を表 3 に示す．図 3 より提案手法は FP 値が低い場合にパケット非使用手法よりも高い TP 値を記録した．また，表 3 より提案手法の AUC はパケット非使用手法の AUC よりも高くなった．この結果より，適切な送信パケット区間幅および受信パケット区間幅を定めた上で送受信パケット量特徴を用いることで，認証精度は高くなることがわかる．

実験で用いた送信パケット区間幅および受信パケット区間幅において，送信トラフィック量および受信トラフィック量を送信記号および受信記号にどのように変換したかを調べる．ここでは，提案手法における学習データおよびテストデータの全端末の送信記号および受信記号の観測回数を調べた結果を表 4，5，6，7 に示す．表 4，5，6，7 では観測回数が上位 5 位のもののみを示している，表 4，5 より学習データ，テストデータ共に送信記号 h_1 の出現回数が多く，表 6，7 より学習データ，テストデータ共に受信記号 c_1 の出現回数が多かった．したがって，送信記号 h_1，受信記号 c_1 以外の記号の出現が行動パターンの特徴を反映しており，その特徴を学習できていると考えられる．

これらの結果より，送受信パケット量特徴は，認証に有効な特徴であると言える．

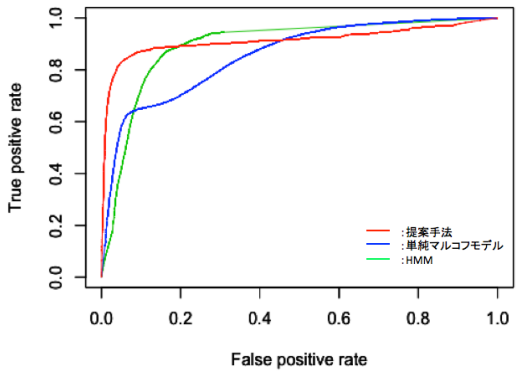

図 2 提案手法，単純マルコフモデルおよび HMM の ROC 曲線

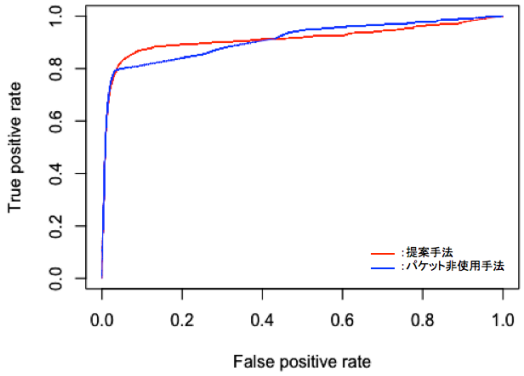

図 3 提案手法およびパケット非使用手法の ROC 曲線

表 3 提案手法およびパケット非使用手法の AUC

手法	AUC
提案手法	0.9128221
パケット非使用手法	0.9104903

表 4 学習データにおける送信記号の観測回数上位 5 位

記号名	観測回数
送信記号 h_1	3528612
送信記号 h_2	1791
送信記号 h_3	258
送信記号 h_4	76
送信記号 h_6	50

表 5 テストデータにおける送信記号の観測回数上位 5 位

記号名	観測回数
送信記号 h_1	2465341
送信記号 h_2	800
送信記号 h_3	104
送信記号 h_4	54
送信記号 h_5	24

表 6 学習データにおける受信記号の観測回数上位 5 位

記号名	観測回数
受信記号 c_1	3530105
受信記号 c_2	505
受信記号 c_3	154
受信記号 c_6	41
受信記号 c_4	40

表 7 テストデータにおける受信記号の観測回数上位 5 位

記号名	観測回数
受信記号 c_1	2465837
受信記号 c_2	371
受信記号 c_3	51
受信記号 c_4	49
受信記号 c_5	28

5. おわりに

本論文では，無線 LAN に接続済みの無線端末が不正に利用されていないかを継続的に監視することを目的とし，端末の位置情報，送信パケット量および受信パケット量を記号列に変換した行動パターンを確率モデルで学習する認証手法を提案した．また，提案手法が実際のユーザの認証に有用であるかを確認するため，実稼働している無線 LAN の無線 LAN 利用ログを用いた実験を行った．

評価実験では，ROC 曲線において提案手法が従来手法の単純マルコフモデルや HMM より FP 値が低い場合に最も高い TP 値を達成し，また提案手法がこれらの手法に比べて最も高い AUC を達成した．その結果より，本手法は単純マルコフモデルや HMM よりも認証精度の点で優れており，滞留時と移動時で位置情報の学習の仕方を変えることが有効であることを確認した．また，提案手法がパケット非使用手法より FP 値が低い場合に高い TP 値を達成し，また提案手法がパケット非使用手法よりも高い AUC を達成した．その結果より，送受信パケット量特徴が認証の要素として有用であることを示した．

今後の課題としては，より短期間の無線 LAN 利用ログから一定の識別精度を持った確率モデルを構築できるように提案手法を改良することなどが挙げられる．

参考文献

[1] 平岩 啓，満保 雅浩：行動認証への無線 LAN 情報の活用，コンピュータセキュリティシンポジウム 2017 講演論文集，3E4-3，pp.1506-1513，(2017)．
[2] 神 嶌 敏 弘：クラスタリング Clustering，入手先〈http://www.kamishima.net/archive/clustering.pdf〉(2019.1.21)
[3] 鈴木 直彦，平澤 宏祐，田中 健一，小林 貴訓，佐藤 洋一，藤野 陽三：人物動線データ分析による逸脱行動人物の検出，情報処理学会研究報告，2007-CVIM-158，Vol.2007，No.31，pp.109-115 (2007)．
[4] 淺原 彰規，丸山 貴志子，佐藤 暁子：混合マルコフモデルに基づく歩行者動線解析方式，情報処理学会論文誌，Vol.52，No.1，pp.187-196，(2011)．