# サイバーフィジカル空間における歩行者の日和見識別手法

天野 辰哉[1]　山口 弘純[1]　東野 輝夫[1]

**概要**：3 次元 LiDAR やデプスカメラにより 3 次元の物理空間内のモノや人の位置・状態を常時スキャンし構成されるサイバーフィジカル空間を活用することで，人々のソーシャルディスタンスや密集度，マスク着用や人とのモノとの接触などの状態を正確に捉え共有することが可能となる．このような空間内の歩行者に対して情報を共有・通知したり，あるいは歩行者同士がメッセージを送りあうためには，歩行者の保持する端末とスキャンされた物理的な歩行者の対応付け（ユーザ識別）が不可欠である．本研究では歩行者に対して事前の情報提供やその場でのタスクなどを要求しない自然な振る舞いから歩行者を日和見的に識別する手法を提案する．スマートフォン端末姿勢による識別と端末使用状況の遷移タイミングによる識別を提案・実装し評価を行った結果，本人拒否率 27.6%, 他人受け入れ率 5.1%の精度で識別を達成した．

## 1. はじめに

近い将来，拡張現実（AR）デバイスを常時着用する人々や高度なタスクを行うロボットの社会浸透が進むと予想される．これらの人々・ロボットは自身の持つセンサを通して，可視光や赤外線・電波などによる常時の 3 次元空間センシング能力をもつ．そういった複数の人やロボットが，センシングや状況理解技術により，人の混雑状況や屋内の空気質などを捉え，情報収集や共有することができれば，空気快適性の向上やスムーズな人の誘導，公衆衛生などの実現にもつながる．このような現実空間上に紐づけた仮想空間，いわゆる **AR クラウド**の実現のためには，空間上に実在する物体や人をシステムが識別・認識し，それに応じた仮想的なコンテンツの配置・表示が不可欠である（図 1）．特に対象空間上の，スマートフォンや AR デバイスを保持・装着する人への電子的な一時 ID の付与（人の識別）は，それらのデバイスを介したその人からの情報発信やその人への情報送信に必要である．人の識別方法として，事前に登録された顔や歩容（固有の歩き方）といった永続的特徴を用いる方法や，ユーザの保持・装着するデバイスによって動的に取得される行動やジェスチャなどの一時的な動きの特徴を，外部から取得されたものとマッチングする方法が存在する．様々な場所で展開されうる AR クラウドに対して，自己識別に関わる永続的な特徴を登録することは社会的に受容されない場合が多く，ユーザの自己情報コントロール権を確保する観点からも，そのような静的特徴に基づかない識別が要求される．

1　大阪大学大学院情報科学研究科

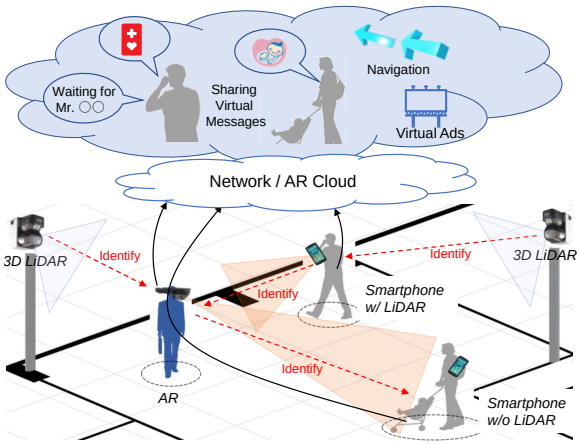



**図 1**　環境内の歩行者識別により実現する AR クラウド

本研究では，空間に設置された RGB，デプスカメラ，3 次元 LiDAR などによって捉えられる歩行者の保持するスマートフォン端末の姿勢と動きを利用したユーザ識別を提案する．提案手法を用いることで，ユーザによる事前の識別用情報や ID 登録なく，かつ自然なスマートフォン利用の様子のみから対象空間に侵入した歩行者を識別することができる．提案手法を実装し評価した結果，本人拒否率 27.6%, 他人受け入れ率 5.1%の精度で識別を達成した．

さらに，これまでに我々の研究チームが開発してきた，3 次元 LiDAR を用いた位置追跡システム「ひとなび」と，提案手法による人の識別手法を用いて AR クラウドのプロトタイプの実装を行った．AR クラウドを通して，識別された歩行者の遠隔地からの監視や設置されている LiDAR による 3 次元点群のモニタリング，機器の調整が可能な Micosoft Hololens2 用のアプリケーションを実装した．

© 2021 Information Processing Society of Japan

## 2. 関連研究

### 2.1 無線・近接情報に基づくユーザ識別

ユーザの近接情報は空間内のユーザ識別や認証に幅広く用いられている．文献 [1] は LiDAR とウェアラブル RFID タグの組み合わせによる歩行者マッチング手法を提案している．LiDAR を用いて歩行者の位置を追跡し，RFID タグを持った歩行者が環境内に配置された RFID リーダーの近くを通過した際に，移動軌跡と RFID タグとの関連付けを行う．歩行者との移動軌跡を高精度に一致させるためには，環境内に多数の RFID リーダを配置する必要があり，インフラの設置コストが課題となっている．

### 2.2 振る舞いに基づくユーザ識別

人の歩き方やジェスチャなど振る舞いをセンサにより取得して，人の識別や IoT デバイスのユーザ認証に活用する研究がなされている．文献 [2] はディスプレイ上での空中ジェスチャーや視線，タッチによるユーザ認証手法を設計し，公共の場での認証手法としてユーザビリティやセキュリティの観点でどれが適しているかを評価している．P2Auth [3] はノブやボタンなどの IoT デバイスが備えるインターフェースの操作タイミングによってユーザ認証を行う手法であり，詳細な動きを捉えることで模倣攻撃に対する耐性を持つ．また近年では AR や VR デバイスのユーザ認証にジェスチャを用いる試みもなされている．また，Wi-Fi や RFID などの電波によって空間内の人間の行動を認識するワイヤレスセンシングを用いたユーザの識別や認証を行うシステムも注目されている．例えば Wi-Sign [4] は任意のパネル上での指による署名動作を Wi-Fi の Channel State Information (CSI) により捉えることで認証するシステムである．

### 2.3 歩行者の移動軌跡とスマートフォン端末のマッチング

スマートフォンユーザへの屋内位置情報サービスの提供を目的として，カメラ映像や LiDAR など環境設置センサから推定された歩行者の移動軌跡と歩行者の保持するスマートフォン端末をマッチングする手法がこれまでにも研究されている．代表的な手法は端末内蔵の加速度・ジャイロセンサによる Pedestrian Dead-Reckoning（PDR）を用いて，端末が自身の移動軌跡を推定しシステムに報告，システムが環境センサによる移動軌跡との類似性に基づいてマッチングするものである．文献 [5] では LiDAR により推定される歩行者軌跡とモバイル端末に搭載されているモーションセンサの計測情報とのマッチングによって端末保持者を特定する手法を提案している．[6] も同様に LiDAR による群衆の移動軌跡を用いて，その群衆内の歩行者がモバイル端末のカメラで撮影した映像内の人物の位置特定手法を提案している．またポケットに入れたスマートフォンの内蔵センサを用いて保有者の歩容を推定し，認証に用いる手法 [7] も存在する．

### 2.4 提案手法の立ち位置

動作に基づく識別・認証の既存手法の多くはユーザに特定動作を求める．これらは外部からの模倣攻撃に対して堅牢である場合が多いものの，ユーザの負担が大きく実用的ではない．移動軌跡による識別はユーザの自然な動きを利用しユーザ負担は小さいものの，現実的に屋内においては移動軌跡はパターン化されることが多く，さらに複数人が同時に部屋に入ってきた場合など高い確率軌跡が重複するため実応用的なシナリオでの活用は難しい．これらに対して本研究では能動的でない自然なスマートフォン使用動作からのユーザ識別手法を提案する．

## 3. 想定環境

### 3.1 想定環境

提案システムのアーキテクチャを図 2 に示す．環境内部には，3 次元 LiDAR やデプスカメラが複数台設置されており，計測可能範囲内の物体形状がスキャンされているものとする．スキャン結果として得られる 3 次元点群はネットワークを介して定期的にクラウドサーバ（あるいはエッジサーバ）上に集約され，3 次元点群解析による人検知および追跡システム『ひとなび』により，空間内の歩行者の位置座標と移動軌跡がリアルタイムに推定されている．歩行者の位置推定・追跡可能な領域を**追跡可能領域**とする．一般に追跡可能領域は LiDAR やデプスカメラが設置されている壁で区切られた部屋である．一方で，環境内の一部の歩行者はスマートフォンを保持しており，環境内に設置されている Wi-Fi アクセスポイントを通してのみアクセス可能な提案システムによる専用 Web アプリケーションに接続できる．この Web アプリケーションに接続可能な領域を**接続可能領域**とする．

提案システムの目的は，トラッキング中の歩行者とアプリケーションに接続しているユーザのマッチングである．タイムステップ $t$ において追跡可能領域にいる歩行者の集合を $P_t = \{p_{i,t}\}_i^N$，識別待ちの Web アプリケーションユーザ（セッション）の集合を $S_t = \{s_{j,t}\}_j^M$ とする．ユーザ $s_{j,t}$ は自身を識別するための情報として，端末内蔵センサによって捉えられる自己の状態・シグネチャ（端末姿勢など）をシステムの識別サービスに常時報告する．識別サービスは歩行者集合 $P_t$ のうち $s_{j,t}$ の報告するシグネチャと一致する歩行者をカメラなどの環境センサによって捉えられる情報をもとに探索し，合致するものがいればその物理的歩行者とセッションを紐づけ識別完了として以降の $P_t$，$S_t$ から除外する．

なお追跡可能領域と接続可能領域は基本的に一致しない．接続可能であるが追跡可能でない領域では，接続可能

© 2021 Information Processing Society of Japan

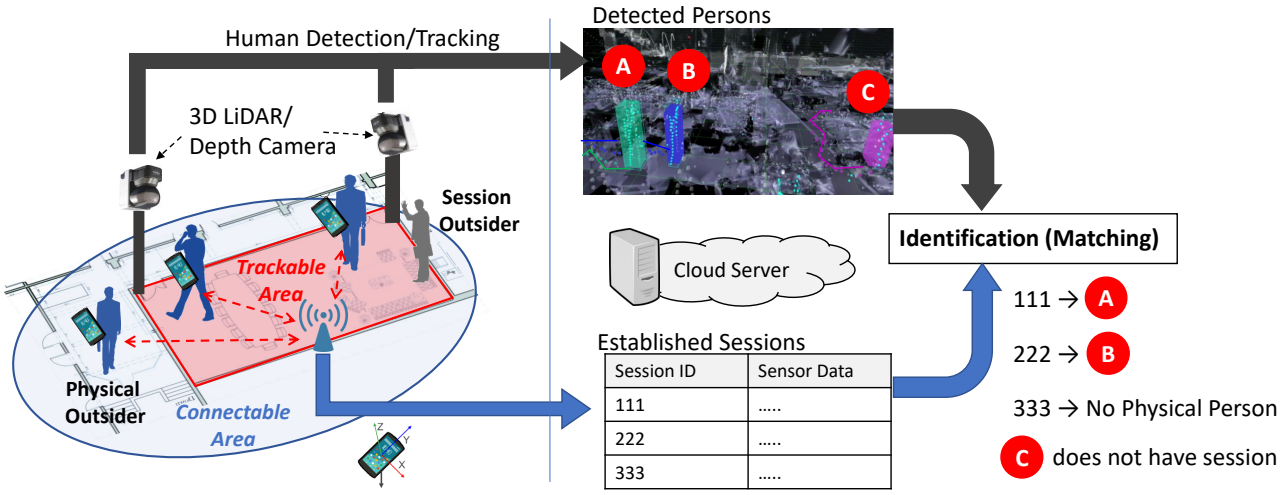



**図 2**　システムアーキテクチャ

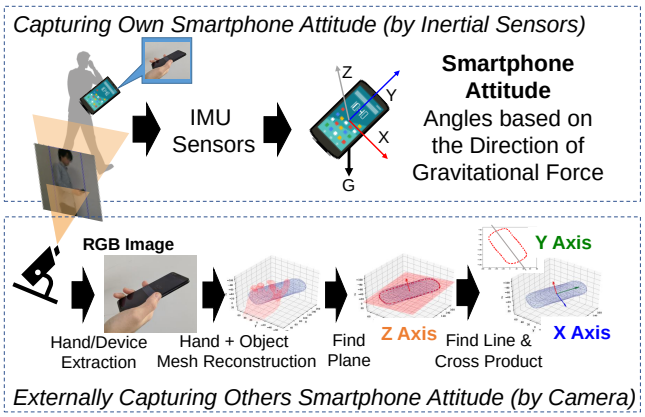



**図 3**　端末姿勢によるユーザ識別

領域にいて Web アプリケーションに接続しているものの，追跡可能領域にいない物理的な部外者が発生しうる．追跡可能であるが接続可能でない領域および重複領域では，追跡されているものの Web アプリケーションに接続しないサービス上の部外者が存在しうる．したがって識別処理が一切行われていない状況であっても $M$ と $N$ は一致しない場合がある．

## 4.　端末姿勢によるユーザ識別手法

環境センサとしてカメラ映像を使用可能な場合は画像中の端末の姿勢を直接推定し，端末自身のセンサによる自己姿勢推定値とマッチングすることでユーザ識別ができる．

被識別ユーザ $s_{j,t}$ は端末内蔵センサによって捉えられる自己の端末姿勢を識別サーバに送信する．一方環境センサ（RGB カメラ）は Yolo-v3 [8] を用い，環境内の歩行者 $P_t$ を検出し，さらに各歩行者の持つスマートフォン端末をカメラ映像から検出する．切り出した画像をもとに端末の姿勢を推定し，$S_t$ からの受信姿勢との類似性が一定の閾値を超えているか判定することで，ユーザ識別が実現できる．

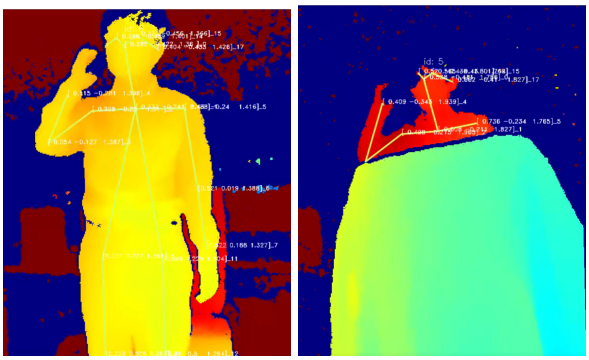
端末の画像からの姿勢推定は以下のように行う．切り出された端末画像領域をもとに，スマートフォンの形状およびそれを保持する歩行者の手を図 3 に示すように 3 次元のメッシュとして再構成する．この再構成においては人の手・指先の構造とその保持する物体の形状を含む大規模なデータセットである ObMan [9] と ObMan の製作者により公開されている学習されたモデル [10] を利用する．これにより入力画像における手首の位置を原点とする 3 次元空間上の手のメッシュ構造および物体のそれぞれのメッシュ構造が取得できる．

生成された 3 次元の手と物体それぞれのメッシュ構造による物体形状から，物体，つまりスマートフォンの X，Y，Z 軸を推定する．スマートフォンのメッシュを構成する 3 次元の点群に対して，1 枚の平面検出アルゴリズムを適用し，得られた平面の法線ベクトル方向を Z 軸とする．スマートフォンを保持する人はスマートフォンの背面を握っているものとし，手からスマートフォンへ向かう方向を Z 軸の正方向とする．また検出された平面とスマートフォンのメッシュが交差する点を，平面上の 2 次元の点群として抽出し，それら点群に対して最小二乗法による直線検出を適用し，得られた直線の方向を Y 軸，平面上での直線の法線方向を X 軸とする．X 軸，Y 軸の向きはすでに正方向が確定している Z 軸を基準に右手系座標系が成立する方向にする．最後に生成された物体のメッシュに対する重力方向を推定する．物体のメッシュは 3 次元空間上において，入力画像が構成する平面が，Y-Z 平面と平行になるような向きで生成され，入力画像上で上方向は 3 次元座標上で Y の正方向であり，下方向は Y の負の方向になる．したがってカメラの仰角（Elevation）$\phi$ およびロール（Roll）$\lambda$ がともに 0 である場合は，生成された 3 次元座標系において Y の負の方向が重力方向となる．

## 5.　端末使用状況の遷移検出によるユーザ識別

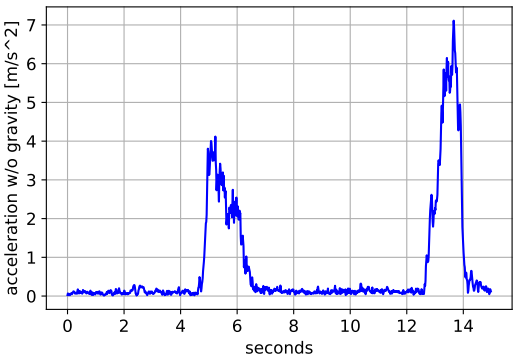
RGB/Depth カメラによって捉えられる歩行者のジェス

© 2021 Information Processing Society of Japan

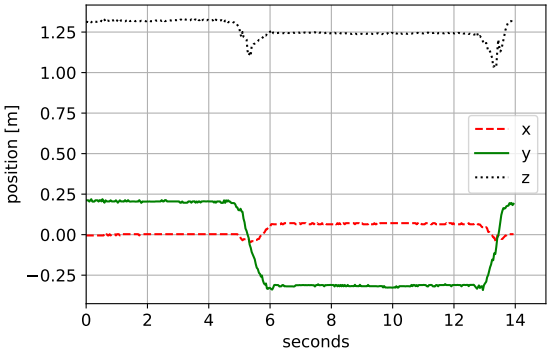


(a) 遮蔽物なし　　(b) 遮蔽物あり

**図 4**　RGB-D カメラによる骨格検出の例




(a) 端末加速度ノルム




(b) RGB-D カメラ映像による手首関節推定位置

**図 5**　右手に保持する端末を持ち上げて顔の前で確認し，またもとに戻す動作を行った際の，端末センサの値と環境センサ（RGB-D カメラ）による関節推定位置

チャと歩行者の保持するスマートフォンが捉える歩行者のジェスチャのマッチングによるユーザ識別手法を提案する．端末に大きな加速度変化をもたらすのは保持者によるスマートフォン操作や収納のタイミングであることに着目し，それらのジェスチャによりマッチングを行う．端末加速度に大きな変化があった際に，そのタイミングがカメラが捉える歩行者の手首の移動のタイミングと一致するユーザを見つけ，存在すればその探索の保持者とする．

LiDAR や深度センサによる 3 次元点群のみを環境センサデータとして利用する場合，スマートフォン端末のような小さな物体の形状を捉えることは容易ではない．一方でそのようなセンサデータのみから人間の骨格を推定する手法

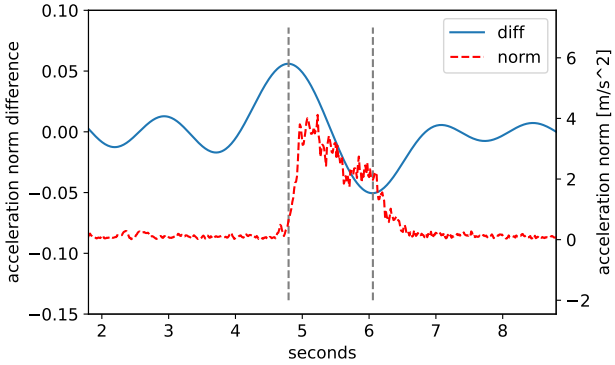



**図 6**　加速度変化の最大・最小ピーク検出による遷移開始・終了の検出

が存在し適用可能である [11]．RGB-D カメラからの歩行者骨格検出の例を図 4 に示す．ここではカメラとして Intel Realsense L515，検出には，深層学習に基づく 3 次元骨格検出・追跡手法である Cubemos Skelton Tracking [12] を利用している．図 4(a) のようにオクルージョンや RGB-D カメラの特性などから歩行者の保持する端末そのものを検出することが難しい場合であっても，骨格検出は可能な状況も多く，また図 4(b) のようにオクルージョンによって人の体全体が捉えられていない状況でも，部分的な骨格を検出できる．なお例で使用している Cubemos はカメラを基準とする 3 次元座標系における関節の座標を出力しており，以降でも環境センサによって捉えられる全歩行者の両手首の関節位置がユーザ識別プログラムにリアルタイムに入力されているものとする．

### 5.1　スマートフォン使用状況の遷移検出

提案手法では「電話を掛ける」，「顔の前で端末を操作する」，単に「手に保持する」，「ポケット・カバンに収納」といった日常的なスマートフォン使用動作・状態の遷移は基本的に手の移動とともに発生するとして，これらの遷移が発生したときに，環境センサが捉える手の移動の中で動作タイミングが合致するものを発見することでユーザ識別を行う．例として右手に保持する端末を持ち上げて画面を確認し，また戻すという動作行った際の端末加速度ノルムと環境センサによって捉えられる手首関節位置の変化を図 5 に示す．

図 5(a) に示すように端末の移動時には大きな加速度が加わるため，内蔵センサの加速度ノルムが一定閾値 $l$ を超えた場合に遷移イベントが発生したとする．図 6 に示すように閾値を超えた時刻 $t$ を基準に一定の $t-a$，$t+b$ 間の加速度ノルム系列データにローパスフィルタを適用し，その差分が最大値・最小値をとる時刻（加速度変化が最小・最大となる時刻）で挟まれる区間を遷移区間とする．なお閾値 $l$ や $a$,$b$ の値は歩行者の移動状態により変更する．Google API Activity Recognition などの既存の歩行者状態識別手法により歩行者が静止状態・歩行・走行のいずれであるか

© 2021 Information Processing Society of Japan

を取得する．

### 5.2 遷移タイミングに基づく尤度

あるユーザ $s_{j,\hat{t}}$ から送られる加速度センサデータに対してタイムステップごとに上記のアルゴリズムで遷移発生検出を行う．$\hat{t}$ 番目のタイムステップに遷移が検出されると各物理的歩行者 $i$ に対して $s_{j,\hat{t}}$ が物理的歩行者 $p_{i,t}$ が生じさせたユーザ（セッション）である尤度 $\mathcal{L}_{i,j,\hat{t}}$ を導出する．検出された遷移時間を $D_{\hat{t}}$ とする．さらに環境センサが捉える歩行者 $p_{i,\hat{t}}$ の右手あるいは左手が $T_{\hat{t}}$ 中に遷移していた場合，該当する環境センサが捉えた遷移時間を $T_{\hat{t},p}$ とする．尤度は以下のように定義する．

$$\mathcal{L}_{i,j,\hat{t}} = \frac{1}{\hat{t}} \sum_{t=0}^{\hat{t}} \mathrm{IOU}(D_t, T_t) \frac{1}{\mathrm{COUNT}(T_t, P_t)} \mathrm{CONF}(T_t) \quad (1)$$

IOU() は 2 つの時間の和集合を共通時間で割ったものであり，遷移タイミングの一致度を表す．$\mathrm{COUNT}(T_t, P_t)$ は $P_t$ のうち右手あるいは左手が $T_t$ と重複する遷移を示すをもつものの数である．重複する遷移が存在しない場合は，1 を返すものとする．これによって例えば 2 人の歩行者が同じタイミングで同じ動作をしているのを環境センサが捉えられた場合はそのステップで加算される尤度を半分に捉える．$\mathrm{CONF}(T_t)$ は $T_t$ の導出に利用した骨格推定の確信度の時間 $T_t$ 間の平均値である．骨格がはっきりと検出されている場合は 1 に近づき遮蔽物などにより推定精度が低下している場合はより低い値になる．これらで表現される開始時から $\hat{t}$ までの各タイムステップで遷移タイミングの一致度，珍しさ，確信度の積の平均値をタイムステップ $\hat{t}$ における尤度とする．尤度が一定の閾値を超えた際に，その $s_{j,\hat{t}}$ と $p_{i,t}$ が同一ユーザであると識別する．

## 6. 実験と評価

### 6.1 端末姿勢による識別精度

端末姿勢によるユーザ識別の精度を評価するため端末姿勢データを取得した．1 つ目のデータセットとして，様々な角度でのスマホを保持する画像と，その時のセンサによる端末姿勢の真値を 2 種類の大きさの違うスマホ（Google Pixel 3 と Lenovo Phab 2 Pro）で収集したものを合わせて計 360 サンプル取得した．また 2 つ目のデータセットとして 3 人の被験者が座って 5 分間 Web ブラウジングしている際の端末姿勢とそれを撮影したカメラ映像からの推定端末姿勢を取得した．

ユーザ識別のマッチングの閾値として，すべての軸の誤差が± 10 度以下であれば一致しているとみなし識別を行い，その精度を評価した．ただし一般的な識別と比べて識別情報である端末姿勢というのは取りうる範囲が狭く，複数ユーザが同時に同一の端末姿勢をとる，つまり識別情報の衝突が頻繁に発生する．これらはシステム上で検知可能であるため，その際は識別拒否が発生したとする．まず識別情報の衝突が起こらないよう 1 つ目のデータセットからサンプルの除外を行ったうえで識別精度を評価した．その結果，識別の正解率（正しく識別されたものの割合）は 72.4 % であった．また識別に失敗した 27.6 % の内訳として，誤ったユーザと識別されたもの（他人受入率）が 5.1 %，すべてのユーザとの類似度が閾値 $\mathrm{TH}_o$ を上回り該当なしとなったもの（本人拒否率）が 22.4 % であった．その結果本人拒否率 27.6 %，他人受け入れ率が 5.1 %であった．ユーザの識別としてはこの数値は高い精度とは言えないが，これは網羅的に生成したデータセットであり，例えば，多様なスマホの持ち方をする 360 人の群衆の中から一人の人間を見つけようとするような最悪のケースに該当する．ユーザ識別の観点では，他人受入率の低さが重要であり，これは類似度の閾値によって変動し，本人拒否率の低さとのトレードオフの関係にある．

またより現実的な環境下においたユーザ識別性能の評価を行った．シナリオとして座りながら保持しているスマートフォンでウェブブラウジングしている 3 人のユーザを識別する状況を想定し，その際の識別性能を評価する．5 分程度 3 人の保持するスマートフォン端末姿勢を推定しつづけ，それを基に各同一時刻における相互の正解率を求めた．なおカメラ画像にピンぼけが発生していたり，スマートフォンが見切れているようなタイミングの映像フレームはあらかじめ手動で映像から除外し，全 300 秒のカメラ映像を入力とした．そのような全 300 秒間のうち，センサによる 2 つ以上の端末姿勢の類似度が閾値 $\mathrm{TH}_o$ を上回り，認証情報（端末姿勢）の衝突が発生したのは 10 % に相当する 31 秒間であった．また 300 秒間のうちの 74 % である 223 秒間は識別の正解率が 100 % ととなり，残りの 43 秒間では 3 人のうちの 1 人の識別に失敗し，正解率が 66 %，さらに残りの 3 秒間では 3 人のうちの 2 人の識別に失敗し，正解率が 33 % となった．なお識別の失敗はすべて，カメラによる端末姿勢に該当する端末姿勢が存在しない，本人拒否の失敗であり，セキュリティ上の脅威である他人受入は発生しなかった．

### 6.2 端末状態遷移検出による識別精度

「ポケットにスマホを入れる」「スマホを持つ」「通話する」「顔の前で端末を操作する」の 4 状態による計 12 の遷移時の環境センサによる手首関節推定位置と内蔵センサの値を取得した．各遷移は約 5 秒で行われる．データ取得には RGB-D カメラである Intel Realsense L515，RGB-D 画像からの骨格検出には Cubemos を利用した．またスマートフォン端末として Pixel 5 を利用し，Realsense によりスキャンされているタイミングでの内蔵センサによる端末加速度を取得した．

初期状態として上記の 4 つのいずれかをランダムにも

© 2021 Information Processing Society of Japan

ち，5〜10 秒に一度他の状態に遷移する，あるいは現在の状態にとどまるを繰り返す歩行者をシミュレーションし，対応する実測データを利用して，5 人の歩行者がいる環境でのセンサデータを再現した．その結果最大 45 秒ですべてのユーザが識別可能であることが確かめられた．

## 7. 議論

追跡しているがセッションを持たないサービス上の部外者および追跡できないがセッションを持つ物理的部外者の存在について考察する．物理的部外者が多数存在する場合，追跡可能領域にいる歩行者と物理的部外者が偶然同じ行動をとる可能性を排除することができない．しかしこれはセッションを通して受信する各端末センサの類似性を確認し，識別拒否とすることで，もっとも深刻な他人受け入れを防止することができる．

サービス上の部外者の存在は想定する AR クラウドアプリケーションによっては深刻である．あるユーザがサービス上部外者の振る舞いに偶然似た端末姿勢や動作をとった場合に，物理的なその部外者であると識別される可能性があるためである．物理的部外者の対策と同様に，環境センサが捉えるユーザの振る舞いの類似性を確認し，同様の振る舞いをして言いるユーザが存在する場合は識別拒否とすることができればよいが，環境センサは内蔵センサとはことなり，オクルージョンなどによるデータの欠損が発生しうる．また能動的な攻撃者の存在を考慮する場合，攻撃者が偽の Wi-Fi アクセスポイントを利用するなどして，意図的に被害者をサービス上部外者にする攻撃が考えられる．環境センサによるユーザの動作を捉える精度の向上と他レイヤーの攻撃防止が重要である．

また今回は模倣攻撃について考慮していない．文献 [13] では攻撃者が AR デバイスを装着し，被識別中のユーザの振る舞いを予測することで，被害者ユーザに成りすます模倣攻撃の可能性が指摘されている．識別のためのジェスチャの模倣困難性を高めることなどがこれらの攻撃の防止策として挙げられているが，動作の複雑化はユーザの自然なふるまいからの識別を目指す日和見的なマッチングの目指す利便性とのトレードオフの関係にある．したがって，提案手法は能動的な攻撃者の居ないオフィスなど限定された空間での AR クラウドでの活用が有効であると考えられる．

## 8. AR クラウドのプロトタイプ実装

提案システムによる AR クラウドシステムをプロトタイプ実装した．AR クラウドを通して通路を歩く識別した歩行者を遠隔監視するアプリケーションおよび LiDAR の設置調整を可能にするアプリケーションを Micosoft 社の Hololens2 を利用して実装した 7．また AR クラウド内の検出歩行者の確認やメッセージ・コンテンツ配置のためのビューアアプリケーション 8 を実装している．

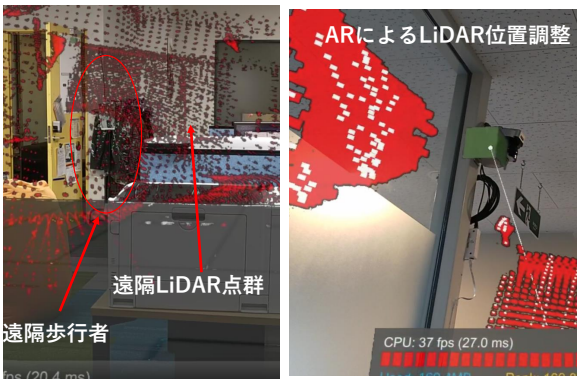



**図 7** ひとなびと Hololens2 による AR クラウドアプリケーション: Hololens を通して遠隔の歩行者や LiDAR センサをモニタリング

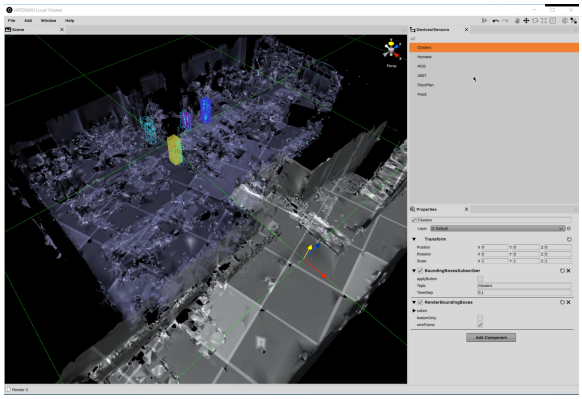


**図 8** AR クラウド内の検出歩行者の確認やメッセージ・コンテンツ配置のためのビューアアプリケーション

## 9. おわりに

本研究では AR クラウドの実現を目指し，環境に設置された RGB/Depth カメラや LiDAR により検出された歩行者と歩行者が保持するスマートフォン端末のマッチング（ユーザ識別）手法を提案した．提案手法は既存手法が要求する能動的なアクション（特定の空中ジェスチャーなど）を用いずに，日常的生活の中でのスマートフォン使用の様子からユーザ識別を実現する．また提案手法をもとに Hololens2 と LiDAR による人流解析システム「ひとなび」を用いて AR クラウドのプロトタイプを実装した．

今後の課題としてより現実的な長期間にわたる日常的環境下での識別精度の調査および模倣攻撃など能動的な攻撃への耐性調査に取り組む予定である．

## 謝辞

本研究成果は国立研究開発法人情報通信研究機構（NICT）の委託研究「ウイルス等感染症対策に資する情報通信技術の研究開発（課題番号 222）」により得られたものです．

© 2021 Information Processing Society of Japan

## 参考文献


[1] Dirk Schulz, Dieter Fox, and Jeffrey Hightower. People tracking with anonymous and id-sensors using rao-blackwellised particle filters. In *Proceedings of the 18th International Joint Conference on Artificial Intelligence*, IJCAI’03, p. 921–926, San Francisco, CA, USA, 2003. Morgan Kaufmann Publishers Inc.

[2] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 2, No. 4, pp. 1–22, 2018.

[3] Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices. *Proceedings of the 25th Annual International Conference on Mobile Computing and Networking (MobiCom’19)*, pp. 1–17, 2019.

[4] Syed W. Shah and Salil S. Kanhere. Wi-sign: Device-free second factor user authentication. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MobiQuitous ’18, p. 135–144, New York, NY, USA, 2018. Association for Computing Machinery.

[5] 高藤巧, 藤田和久, 樋口雄大, 廣森聡仁, 山口弘純, 東野輝夫, 下條真司. トラッキングスキャナとモーションセンサを用いた高精度屋内位置推定手法の提案. 情報処理学会論文誌, Vol. 57, No. 1, pp. 353–365, 2016.

[6] 岩橋宏樹, 樋口雄大, 山口弘純, 東野輝夫. 歩行者群の移動軌跡情報を用いたモバイルカメラ画像内の人物位置推定手法. 情報処理学会論文誌, Vol. 56, No. 2, pp. 470–482, 2015.

[7] Muhammad Muaaz and René Mayrhofer. Smartphone-Based Gait Recognition: From Authentication to Imitation. *IEEE Trans. on Mobile Computing*, Vol. 16, No. 11, pp. 3209–3221, 2017.

[8] Joseph Redmon and Ali Farhadi. Yolov3: An incremental improvement. *arXiv*, 2018.

[9] Yana Hasson, Gül Varol, Dimitris Tzionas, Igor Kalevatykh, Michael J. Black, Ivan Laptev, and Cordelia Schmid. Learning joint reconstruction of hands and manipulated objects. In *CVPR*, 2019.

[10] Yana Hasson, Gül Varol, Dimitris Tzionas, Igor Kalevatykh, Michael J. Black, Ivan Laptev, and Cordelia Schmid. Learning joint reconstruction of hands and manipulated objects. ”`https://hassony2.github.io/obman.html`”, 2019-. [Online; accessed 17-May-2020].

[11] Yufan Zhou, Haiwei Dong, and Abdulmotaleb El Saddik. Learning to estimate 3d human pose from point cloud. *IEEE Sensors Journal*, Vol. 20, No. 20, pp. 12334–12342, 2020.

[12] Cubemos. Cubemos skeleton tracking sdk. ”`https://www.cubemos.com/skeleton-tracking-sdk`”, 2020-. [Online; accessed 09-May-2021].

[13] Hassan Khan, Urs Hengartner, and Daniel Vogel. Augmented reality-based mimicry attacks on behaviour-based smartphone authentication. *MobiSys 2018 - Proceedings of the 16th ACM International Conference on Mobile Systems, Applications, and Services*, pp. 41–53, 2018.


© 2021 Information Processing Society of Japan