スマートフォンにおけるタッチ操作の特徴を用いた継続的な個人識別システムの検討

渡邊 裕司† 市川 俊太†

†名古屋市立大学大学院システム自然科学研究科
467-8501 愛知県名古屋市瑞穂区瑞穂町山の畑 1
yuji@nsc.nagoya-cu.ac.jp

あらまし スマートフォンにおいてログイン認証後には一般的に不正アクセスが可能である．パソコンではキーボードやマウスの操作特徴を用いた個人識別研究が古くからあるが，スマートフォンに対する研究は最近始められつつある．スマートフォンには独特のタッチ操作があり，個人識別に使える特徴かを検討すべきである．本研究では，スマートフォンにおけるタッチ操作の特徴を用いた継続的な個人識別システムを検討する．操作履歴（指の接触時の座標位置と時刻）を記録する文章閲覧アプリを作成し，指の使用領域，移動距離，速度などの操作特徴を求めた．5人の被験者による実験の結果，操作特徴の組み合わせにより個人識別が可能であることを示唆した．

A study of continuous user identification using touch operational features on smart phone

Yuji Watanabe† Shunta Ichikawa‡

†Graduate School of Natural Sciences, Nagoya City University
1 Yamanohata, Mizuho-cho, Mizuho-ku, Nagoya 467-8501, JAPAN
yuji@nsc.nagoya-cu.ac.jp

Abstract After user authentication and identification for smart phone is passed on login, not only the legal owner but also illegal users freely use the smart phone. For the second protection, behavior-based user identification can continuously check the user activities after login. In this paper, we investigate continuous user identification using touch operational features on smart phone. We make a text browsing application to record fingers history on smart phone and extract characteristic operational features, for instance, the distribution of touched region, the speed and so on. Experimental results suggest the feasibility of user identification by combining operational features.

1 はじめに

最近のスマートフォンの普及は目覚ましく，携帯電話の総出荷台数に占めるスマートフォンの割合が 2012 年度には 68.7%になると予測されている[1]．スマートフォンを含む多機能な携帯電話にはアドレス帳だけでなく多くの重要な個人情報がパソコンと同様に含まれ，これらの情報は不正使用者から守られなければならない．そのために一般的に行われるの

がパスワードによる認証である．しかし，問題点として，(1)パスワードは忘れやすく，パスワードが一旦他人に漏洩するとパスワードを変更しない限り他人が容易に不正利用できてしまうこと，(2)パスワード認証はログイン時に一度だけ行うことが多く，ログイン後には正規ユーザだけではなく不正使用者も自由にアクセスできてしまうことが挙げられる．

指紋や顔画像など生体的特徴を利用したバイオメトリクス認証[2]には，認証精度が高い，パスワードを記憶する必要がない，生体的特徴ならば紛失しにくくコピーされにくいなどの利点があり，上述の問題(1)は解決される．しかし，ログイン後も絶えず認証することは煩わしく，問題(2)は残されたままである．さらにこの認証には一般的に指紋読み取り装置など特別な装置が必要となる．

そこで，パソコンにおいては，キー操作やコマンド列やマウス操作など他人が模倣することが難しい個人の特徴や癖を用いた認証方法が 1990 年代から広範に研究されている[3-12]．この行動的特徴による認証・識別では，特別な装置は不要である．また，この認証では，通常時の正規ユーザの振る舞いから特徴を表すプロファイルを作成し，そのプロファイルと現在の振る舞いとの間に著しい相違があれば，不正使用者として警告する．そのためログイン後も継続的に監視が行える．

一方，携帯電話，特にスマートフォンの行動的特徴による認証・識別の研究は最近始められつつある．例えば，キー操作に基づく認証[13,14]，加速度センサを用いた認証[15-17]，タッチパネルによる認証[18,19]，複数センサを用いた認証[20,21]などがある．加速度センサを用いた歩行や走行時の個人識別は高い精度を示している[17,20]が，静止時には使えない．タッチパネルや複数センサを使用した研究は比較的新しいため，文献[18,19,21]などはログイン時の認証であり，ログイン後の継続的な個人識別を扱った研究はまだ少ない．特にタッチパネル式のスマートフォンでは独特の操作（フリック（はじく），タップ（軽く叩く），ピンチ（つまむ）など）があるため，個人識別に利用できる特徴となりうるかを調べる必要がある．

そこで本研究では，スマートフォンにおいてユーザのタッチ操作の特徴を監視することによって継続的に個人識別を行い，不正使用者を発見することを最終的な目的とする．そのために，まずスマートフォン用に操作履歴を記録するアプリケーションソフトを作成し，個人識別のために抽出すべき特徴について検討する．具体的には，操作履歴としてユーザが画面にタッチしたときの座標位置とその時刻などを取得するための文章閲覧アプリ（テキストブラウザ）を作成する．そして，取得した座標位置・時刻から個人識別のための操作特徴として指の使用領域，移動距離，移動速度，移動角度などを求め，これらが個人識別として使えるかを検討する．

5 人の被験者による予備実験の結果，指の使用領域に関しては，ユーザがスマートフォン操作に慣れているかどうかがわかり，識別のための操作特徴として利用可能であることがわかった．また，単一の操作特徴からは個人識別を行うことは困難であるが，操作特徴の組み合わせにより個人識別が可能であることを示唆した．

2 関連研究

パソコンにおける行動的特徴による認証として，キーボードの打ち方によるキーストローク認証が 1990 年前後から始められ多く行われている[3-7]．また，コマンド列を用いた認証[8-10]やマウス操作に基づく認証[11,12]も 90 年代後半から行われている．本研究で取り上げるスマートフォンのタッチ操作はキー操作やコマンド列よりもマウス操作に近いため，ここではマウス操作に限って紹介する．文献[11]では簡単な図形をマウスでなぞらせて個人認証するが，パソコン利用中に認証のために何度も図形をマウス入力することは現

実的ではない．そこで，泉らはパソコン使用時の通常のマウス操作を継続的に監視する方法を提案していて[12]，本研究の目指す方向に近い．

一方，携帯電話やスマートフォンにおける行動的特徴による認証研究としては，キー操作に基づく認証[13,14]，加速度センサを用いた認証[15-17]，タッチパネルによる認証[18,19]，複数センサを用いた認証[20,21]などがある．文献[13]は，パソコンよりも計算能力や記憶容量が劣る携帯電話を考慮して，キーストロークの頻度を用いた簡便な認証方法を提案している．文献[14]では，スマートフォンにおいて 25 ユーザのキーストロークに対して様々な分類アルゴリズムの性能を評価し，約 2%の他人受入率（False Acceptance Rate: FAR）と 0%の本人拒否率（False Rejection Rate: FRR）を達成している．石原らの加速度センサを用いた 3D 動作認証[15]では，手に持った携帯端末の動きから個人的な動作特徴を抽出し，FRR を 1.5%未満，FAR を 1%未満にできることを示している．しかし，継続的な認証のためには端末を何度も動かす必要がある．文献[16,17]の加速度センサを用いた認証は，端末をベルトやポケットに入れた状態で歩行，走行，階段の昇降の動作から個人的な特徴を得て認証を行う．しかし静止時には識別できない．タッチパネルによる認証として，文献[18]では Android のロックパターンを使い，文献[19]では 5 本の指の動きを特徴としているが，これらは基本的にログイン時の認証である．見上らのタッチパネルと加速度センサを用いた認証[21]もログイン時である．本研究と同じような継続的な個人識別は，Shi らの SenGuard である[20]．SenGuard では，加速度センサ，マイク（使用せず），場所履歴，タッチスクリーンの複数センサを使用し，継続的な個人識別を目指す．文献[20]では，加速度センサと場所履歴の性能評価はあるが，タッチスクリーンの識別精度をまだ評価していない．また，複数センサの統合にもまだ至っていない．

3 タッチ操作履歴記録アプリケーション

3.1 文書閲覧アプリケーション

本研究では，iPhone，iPod touch，iPad 用に iOS 上で機能するタッチ操作履歴取得アプリケーションを開発する（現時点ではスマートフォン OS 別契約数シェアにおいて Android が iOS を上回っていることから[1]，筆者らは Android 上での開発も始めている）．実際にはユーザが通常利用するアプリのバックグラウンドで継続的に操作履歴を記録することが望ましい．しかし，現時点での iOS はマルチタスクになったものの，バックグラウンド実行は OS に組み込まれた 7 種類のプロセスのみ許可されるため，バックグラウンドで操作履歴を取得することができない．

そこで，ブラウジングは多くのスマートフォンアプリに備わった基本的機能の一つであることから，図 1(a)に示すような簡易な文章閲覧アプリ（テキストブラウザ）を作成し，ユーザが表示されたテキストを読むことでその操作履歴を継続的に記録する．ディスプレイの大きさは縦 480 ピクセル×横 320 ピクセルである．また，本ブラウザは縦方向のみのスクロール操作が可能であるため，以下の二つの操作によってスクロールする：

- フリック：指を「はらう」ように，指をスライドしながら離すこと
- ドラッグ：画面を押しっぱなしにしたまま，指をスライドさせること

なお，スマートフォンの操作には他にもタップ(画面の任意の場所をポンと押すこと)，ピンチ操作（2 本の指で画面を押さえて，摘むように指を近づけることをピンチイン，遠ざけることをピンチアウト）などがあり，それらの操作も取得可能な横方向スクロールも含めたブラウザの開発も進めている．

一方，既存のクラスを用いてスクリーン上の座標位置を取得することが困難であるため，

UITextView クラスを用いてテキスト上の座標位置を取得する．図 1(b)に示すように，原点は左上に存在し，X 軸と Y 軸の範囲はともに用意するテキストの量に依存する．図 1(a)のテキストの場合，X 軸の範囲は[0, 320]，Y 軸の範囲は[0, 20000]となる．

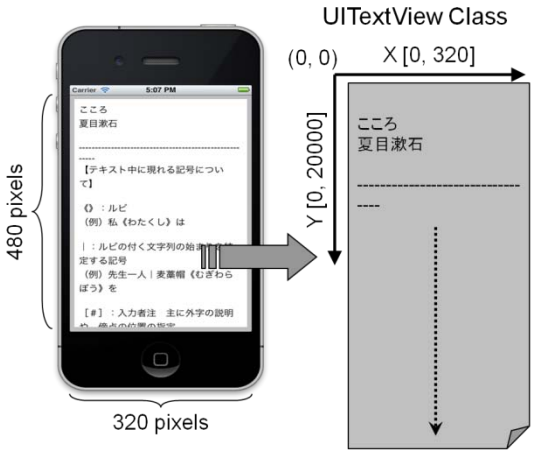

図 1：(a)操作履歴を取得するための簡易テキストブラウザと(b)テキスト上の原点と X 軸と Y 軸

3.2　操作履歴と操作特徴の抽出

前節の簡易テキストブラウザによって継続的に取得する「操作履歴」は，$\{event, (x, y), t\}$ の形式である．ここで，*event* はタッチパネルに指が触れているときに呼び出されるタッチイベントのことであり，以下の三つのタッチイベントを検出できる．

1. 指をタッチした瞬間
2. 指を動かしたとき
3. 指を離したとき

そして，(x, y)はタッチイベントを検出したときの座標位置であり，t はその検出時刻である．例えば，開始から 20 秒後に指でタッチパネルに触れ，25 秒後に離した場合は，{{1, (200, 15), 20}, {2, (200, 16), 22}, {3, (200, 18), 25}}という操作履歴が得られる．

得られた操作履歴から個人識別を行うための「操作特徴」を抽出しなければならない．

そこで，パソコン上のマウス操作から操作特徴を抽出する既存研究[12]を参考にして，以下の基本的な操作特徴を求める．

1. 指の使用領域：ユーザが触れた指の座標位置を集計し分布図を作成
2. 指のX座標：縦スクロールであるためX座標を集計
3. 指の移動距離:指をタッチした瞬間（始点）と指を離したとき（終点）の2地点間の距離を計算（図2）
4. 指の移動速度:2地点間の距離を時間で割って速度を計算
5. 指の移動角度:2地点間の移動角度を計算（図2）

そして，実験によりそれぞれが個人識別として使えるかを検討する．

図 2：指の移動距離と移動角度

4　予備実験結果

5 人の被験者(内スマートフォン所持者は 4 人）に作成したテキストブラウザを iPod touch で使用してもらい，操作履歴を取得する予備実験を行った．実験手順としては，まず被験者に iPod touch とテキストブラウザの操作方法を説明し，テキストブラウザを使っ

て自由に文章を読んでもらった．そして，読み終わったらiPod touchを回収して操作履歴をiTunes経由で取得した．

表1は各被験者に対して検出できたイベント数と検出できた移動距離の数である．また，図3に各被験者に対して検出できたイベント全ての座標位置の分布図つまり指の使用領域を示す．移動距離の計算には，三つのタッチイベントの連続が必要である（移動時の *event* = 2 は除いてもよいため，*event* 列に対して正規表現を使うと 12*3）．しかし，実際に実験してみると離脱時の *event* = 3 が検出されにくかったため，離脱時が含まれない場合も移動距離に含めた（*event* 列に対して正規表現を使うと 12*3 または 12+）．

表 1：各被験者に対して検出できたイベント数と検出できた移動距離の数

被験者	検出できたイベント数	検出できた移動距離の数
A	120	7
B	2420	339
C	250	72
D	270	52
E	110	24

表1の各被験者のイベント数および図3の分布図からA，C，D，Eはスマートフォンの操作に慣れていて，Bはスマートフォンを使って文章を読むことに慣れていないといえる．また，AとEは，他の被験者と比べてイベント数が少なく，分布が散らばっていないことから，スマートフォンを使用することに特に慣れているといえる．実験後，AとEがスマートフォンを2年以上所持していることを確認した．このことから座標位置の分布は，個人識別を行うための操作特徴の1つになりえると考えられる．そこで，分布図の横方向の位置とばらつきが各被験者で異なるようにみえるため，各被験者のX座標に対して基本統計量の平均値，最小値，最大値，標準偏差を求めた(表2には平均値と標準偏差を示す)．標準偏差から各ユーザのX座標にばらつきが生じていることがわかる．平均値に対して被験者間に有意差があれば，この平均値を個人識別の特徴とできる．しかし，BとCの平均値が同程度の値を示しており，ウェルチの検定を行った結果からもBとCの間では有意差が現れなかった．

表 2：指のX座標の平均値と標準偏差

被験者	平均値	標準偏差
A	231.6	29.6
B	**169.6**	51.8
C	**163.0**	83.0
D	197.4	39.9
E	251.1	15.7

次に，各被験者の指の移動距離，移動速度，移動角度に対して同様に基本統計量の平均値，最小値，最大値，標準偏差を求めた（表3には平均値と標準偏差を示す）．まず移動距離の平均値が個人識別の特徴となりうるかを検討してみると，BとCの値が同値であり，ウェルチの検定結果からもBとCの間では有意差がなかった．次に移動速度の平均値については，今度はAとBの値が同程度の値を示しており，ウェルチの検定結果からもAとBの間では有意差が現れなかった．最後に移動角度の平均値に関しては，CとDの値が同程度の値を示し，ウェルチの検定結果からもCとDの間では有意差がなかった．

以上の結果から単一の操作特徴だけでは，個人識別を行うことが難しいとわかった．しかし，操作特徴を組み合わせ，複合的な観点からみれば個人識別が可能であると考えられる．例えば，指の移動距離の平均値においてBとC間には有意差がないが，指の移動速度の平均値ではBはCよりも大きく，Cの移動速度の平均値は一番小さいことがわかる．これら複数の操作特徴を分類アルゴリズムに入力すれば，適切なユーザを出力するような個人識別が可能であると考えられる．

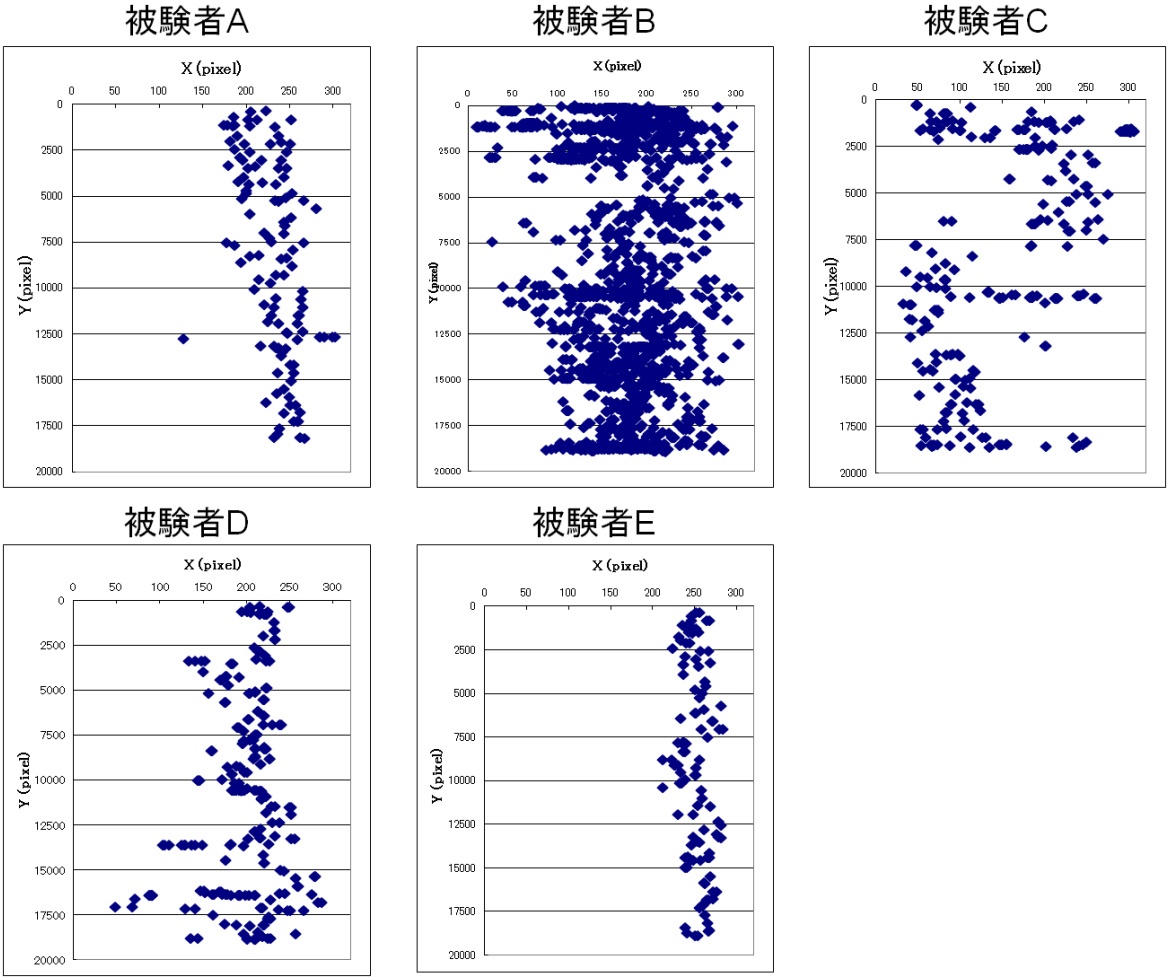

図 3：各被験者の使用領域

表 3：各被験者の指の移動距離，移動速度，移動角度に対する平均値と標準偏差

被験者	移動距離（pixels）		移動速度（pixels/s）		移動角度（°）	
	平均値	標準偏差	平均値	標準偏差	平均値	標準偏差
A	7.4	2.0	**104.1**	98.0	−33.7	102.5
B	**7.9**	8.4	**119.4**	606.9	22.2	94.8
C	**7.9**	6.2	53.1	56.1	**−18.3**	83.1
D	7.6	3.2	86.9	88.9	**−20.9**	101.7
E	9.2	1.5	168.0	75.0	−42.6	84.6

5　検討事項

本研究はまだ始めたばかりであるため，多くの課題が残されている．以下に検討事項を挙げる．

複数の操作特徴を用いた継続的な個人識別：前節で述べた操作特徴の組み合わせにより個人識別が可能かどうかをまず調べなければならない（発表時には報告予定）．また，操作特徴は時間にも依存するため，全データに対する統計量ではなく，オーバーラップを許

した適当なサイズのウィンドウに対して平均値などを求める必要がある．そして，過去いくつかの操作特徴に対して現在の操作特徴に相違があるかどうかを検査する継続的な個人識別システムを構築する．なお，分類アルゴリズムには，WEKA のデータマイニングソフト[22]を使う予定である．

被験者を増やした本実験：例えばマウス操作を用いた既存研究[12]の被験者は 5 人であり，本研究の予備実験も 5 人で行った．しかし，行動的特徴の認証手法の問題点として，識別する人数が増えるにつれて認証が難しくなるということが挙げられている．その検証を行うために被験者の人数を増やし再度実験を行う必要がある．

他の操作も取得可能なアプリの開発：本研究ではテキストブラウザを作成し，そのブラウザ上でフリックやドラッグによりテキストを読むことで操作履歴を取得した．しかし，フリックやドラッグ以外にもタップやピンチ操作などスマートフォン独自の操作がある．またスマートフォンの操作にはブラウジングだけでなくキー入力もある．そこで，他の操作も含めた操作履歴を取得するアプリケーションの開発も必要である．

複数センサを用いた個人識別：タッチ操作だけでは個人識別の精度が悪いと予想されるため，文献[20,21]のようなタッチパネルだけでなく加速度センサなど複数センサを用いた個人識別システムを検討すべきである．

6　おわりに

本論文では，スマートフォンにおけるタッチ操作の特徴を用いた継続的な個人識別システムを検討した．操作履歴として指の接触時の座標位置と時刻を記録する文章閲覧アプリを作成し，指の使用領域，移動距離，速度などの操作特徴を求めた．5 人の被験者による実験の結果，操作特徴の組み合わせにより個人識別が可能であることを示唆した．今後は，前節であげた課題に取り組む予定である．

参考文献

[1] （株）MM総研［ 東京・港 ］，“スマートフォン市場規模の推移・予測（12 年 3 月）”，2012. 3. 13

[2] A. Jain, R. Bolle, and S. Panakanti, “Biometrics: Personal Identification in Network Society,” Kluwer Academic Publishers, 1999.

[3] R. Joyce and G. Gupta, “Identity Authentication Based on Keystroke Latencies,” *Communications of the ACM*, 33(2), pp.168-176, 1990.

[4] J. Leggett, G. Williams, M. Usnick, and M. Longnecker, “Dynamic Identity Verification via Keystroke Characteristics,” *International Journal of Man-Machine Studies*, 35(6), pp.859-870, 1991.

[5] 粘川正充，角田博保，森裕子，“アルペジオ打鍵列を利用した個人認証手法の提案”，情処学論，34(5), pp.1198-1205, 1993.

[6] F. Monrose and A. Rubin A, “Authentication via Keystroke Dynamics,” *Proc. of the 4th ACM conference on computer and communications security*, pp.48-56, 1997.

[7] F. Bergadano, D. Gunetti, and C. Picardi, “User Authentication through Keystroke Dynamics,” *ACM Trans. on Information and System Security*, 5(4), pp.367-397, 2002.

[8] 白井治彦，西野順二，小高知宏，小倉久和，“対話的計算機環境におけるコマンド入力連鎖を用いた認証手法の提案”，信学論 A，J82-A(10)，pp. 1602-1611，1999.

[9] M. Schonlau, W. DuMouchel, W. Ju, A. Karr, M. Theus, and Y. Vardi, “Computer Intrusion: Detecting

Masquerades," *Statistical Science*, 16(1), pp.58-74, 2001.

[10] T. Okamoto and Y. Ishida, "An Immunity-Based Anomaly Detection System with Sensor Agents," *Sensors*, 9(11), pp.9175-9195, 2009.

[11] 林賢一，岡本栄司，満歩雅浩，植松友彦，"マウスを用いた新しい個人識別方式の提案"，暗号と情報セキュリティ・シンポジウム SCIS97-19A，1997.

[12] 泉正夫，長尾若，宮本貴朗，福永邦雄，"マウス操作の特徴を用いた個人識別システム"，信学論 B，J87-B(2)，pp. 305-308，2004.

[13] T. Isohara, K. Takemori, and I. Sasase, "Anomaly Detection on Mobile Phone Based Operational Behavior," *IPSJ Journal*, 49(1), pp.436-444, 2008.

[14] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, "Keystroke-Based User Identification on Smart Phones," *Proc. of the 12th International Symposium on Recent Advances in Intrusion Detection*, pp.223-243, 2009.

[15] 石原進，太田雅敏，行方エリキ，水野忠則，"端末自体の動きを用いた携帯端末向け個人認証"，情処学論，46(12)，pp.2997-3007，2005.

[16] J. Mantyjarvi, M. Lindholdm, E. Vildjounaite, S. M. Makela, and H. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," *Proc. Of IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp.973-976, 2005.

[17] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Cell Phone-Based Biometric Identification," *Proc. of the 4th IEEE International Conference on Biometrics: Theory Applications and Systems*, pp.1-7, 2010.

[18] J. Angulo and E. Wastlund, "Exploring Touch-screen Biometrics for User Identification on Smart Phones," *IFIP Summer School*, 2011.

[19] 井芹隼人，岡本栄司，"タッチパネルを用いた行動的特徴に基づくバイオメトリクスに関する一考察"，CSS，pp. 84-88，2011.

[20] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, "SenGuard: Passive User Identification on Smartphones Using Multiple Sensors," *Proc. of IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications*, pp.141-148, 2011.

[21] 見上一憲，林原尚浩，"タッチパネルと加速度センサを用いた携帯端末向けジェスチャ認証とその入力方式の提案"，情報処理学会研究報告，CSEC-56(8)，2012.

[22] I. Witten and E. Frank, "Data Mining: Practical Machine Learning Tools and Techniques," Morgan Kaufmann Publishers, 2005.