福井大学 大学院工学研究科 研究報告 第64巻 2016年3月
Mem. Grad. Eng. Univ. Fukui, Vol. 64（March 2016）

Android端末上の加速度センサを用いた新しい生体認証システム

古賀 堯志*　小高 知宏*　黒岩 丈介**　白井 治彦***

New Biometric System Using Accelerometer on Android Terminals

Takashi KOGA*, Tomohiro ODAKA*, Jousuke KUROIWA** and Haruhiko SHIRAI***

(Recieved February 5, 2016)

In this paper, we developed the wrist motion-based authentication system using accelerometer on Android terminals. In the previous researches, hand moving of writing the letter in field was set to target, although our system is using the wrist motion to improve visual silence and availability. Our system requires the moving after the vibration to improve the accuracy of authentication. We got characteristics of motion in 8 subjects. As the result, we got 11.25% of FRR at 10.357% of FAR on change the threshold estimation value.

Key Words: Authentication, Biometrics, Wrist Motion-based System, Android Terminals, Time Lag of Reaction

1　はじめに

近年，スマートフォンやタブレット型端末といった携帯端末が急速に普及してきており，特に日本国内においてスマートフォン所有率は2010年と比較して6倍以上に増加している [1]．これらは従来の携帯電話と比較して大容量・高機能化しており，パソコンと比肩するまでに性能や用途を広げる一因にもなっている．しかしこれに伴って，紛失に因る個人情報データの流失のリスクも上がっており，実際に流失した場合は損失・損害も増加する可能性もある．その対策として端末本体の個人認証技術の強化が不可欠となっている．

従来から用いられている認証手法としては，ログイン時にパスワードを使用する方法や，画面をスワイプするパターンを要求する方法がある．これらの方法は特別な装置無しに認証を行う事ができるが，その反面，入力する内容を亡失すると使用できなくなる，また入力内容その物を見られてしまうと効力が完全に失われてしまうという欠点もある．更に表1や表2に示す通り，これらの手法を用いた場合のパターンの組み合わせは有限である事も計算上明らかであり，計算機的な総当たり解析 (Brute-force attack) により侵入を許してしまう可能性もある．これらの事から，セキュリティ上は一定回数間違えた場合の再試行の禁止や，文字列等の組み合わせの定期的な変更等の対策が必要となる．

以上を踏まえると，セキュリティの面においては見ただけでの複製が困難な各個人特有の特徴を用いる生体認証が優れていると言える．一例として，指紋，指静脈の透視イメージを用いる物が挙げられ [2]，実用化されている物も多数ある．しかし，検出する対象によっては特殊な機器を使用しなければ読み取る事ができず，読み取り・データ登録に抵抗感を示しうる特徴もある等，即時の導入が難しいという欠点もある．

その為，一般的な民生端末に搭載されているセンサ等を用いて人の行動の特徴を検出し，それを生体的な特徴として認証に用いる手法が提案されている．検出する行動として，歩行動作や画面のスクロール速度等が用いられている．また前述のパスワード・パターン認証と組み合わせた研究も行われてきているが，本研究では人の手首の動きの特徴の個人差を用いる事にする．具体的には，多くのAndroid端末に搭載されている加速度センサを用いて使用者の端末を持った手の手首を動かす動作を検出し，その動きの速さや方向を用いて個人を識別する [3]．

本稿では，以前から研究が行われてきた生体認証手法と比較しながら有用性を検証していく．第2章では生体認証技術の歴史と本研究のシステムの特徴につい

*大学院工学研究科原子力・エネルギー安全工学専攻
**大学院工学研究科知能システム工学専攻
***工学部技術部
*Nuclear Power and Energy Safety Engineering Course, Graduate School of Engineering
**Human and Artificial Intelligence Systems Course, Graduate School of Engineering
***Technical Division

表 1　各種文字列における 8 文字の組み合わせ総数と計算時間 [4]

文字の種類	組み合わせ総数	秒間 100 万回	秒間 1000 万回	秒間 1 億回	秒間 10 億回
数字 (10 種)	10^9	約 1.5 分	約 10 秒	瞬時	瞬時
英字 (大小)(52 種)	約 53×10^{12}	約 1.5 年	約 62 日	約 6 日	約 15 時間
英数字 (62 種)	約 218×10^{12}	約 7 年	約 253 日	約 25.25 日	約 60.5 時間
英数字及び記号 (96 種)	約 7.2×10^{15}	約 229 年	約 23 年	約 2.25 年	約 83.5 日

表 2　3×3 格子のパターンロック認証の組み合わせ [5]

通る点の数	組み合わせ総数
4	1,624
5	7,152
6	26,016
7	72,912
8	140,704
9	140,704
参考:英字大小 52 種から 3 文字	140,608

て述べ，システム構成や実験方法について第 3 章で述べる．第 4 章で述べる実験で，被験者夫々の動作の特徴を確認した上で FAR/FRR を検証する．そして第 5 章でこれらの結果を考察し，総括する．

2　生体認証

本節では，生体認証の特徴と既知の問題点，及び本研究で用いる解決手法について述べる．

2.1　従来の研究における生体認証技術

2.1.1　歴史的背景

[6] によれば，各個人固有の特徴を用いた個人同定は古くから行われており，例えば指先の表皮紋様である指紋は,「万人不同」「終生不変」の特徴が経験的に理解されてきていた．この特徴は日本でも利用されており，拇印を本人筆の書面に押すという習慣もある．英国の N.Grew は 1684 年にこれの科学的研究を行ったと言われている．また，インドに派遣された英国政府職員の W.J.Harschel はこれを個人認証手法として実用化し，英国医師 H.Faulds は 1874 年の来日時に前述の習慣に着目した研究を行なっている．後に，英国の F.Galton によって弓状，渦状，蹄状の 3 種類に指紋を大別した上で，古くから経験的に得られていた特徴を裏付けた．日本国内では 1908 年に施行された刑法において，再犯者を厳罰化すべくこれの識別に指紋法を用いた事が始まりで，以降前科者の管理手法としての利用が試みられてきた．1971 年に運用開始された犯罪者管理システム AIFS ではより実用的なものとなっている．現在，指紋は犯罪捜査のみでなく，様々な場面での本人認証の手法に用いられている．

2.1.2　生体認証の様々なモダリティ

我々の社会生活の中では，見覚えのある「顔」や聞いた事のある「声」だけで本人か否かを判断する事が多く，これらの曖昧且つ主観的な特徴のみで本人であると認めた上で金品の授受を行う事は現実的には不安が残る．ネットワーク上においてはこの危険度が更に増しており，より厳密且つ客観的な尺度で本人認証を行う事が推奨されている．即ち，本人以外が知り得ない事や所持し得ない物で紛失・忘却・盗難の危険性がより少ない物による認証を行う必要がある．本人の記憶にある暗証番号やパスワード，及び各個人の生体的及び行動的特徴でこれらの認証を行う事は，セキュリティ上において理に適っているとされる [7]．

生体認証に用いられる特徴の大分類をモダリティと呼び，一般的には表 3 に示す様な物が挙げられる．

生体認証においては，全ての人に一般的に存在する「普遍性」，ある人と同じ特徴を持つ人が誰もおらず，複製も不可能な「唯一性」，加齢によって減少あるいは滅失する事の無い「永続性」が特に重要視されている．指紋や顔，虹彩，静脈といったモダリティは個人を直接特定するもので身体的特徴と呼ばれ，認証誤差が比較的少なく，経時変化が少ないのが特徴である．現在，身体的特徴を利用した方法は図 1 に示す様な各種端末における指紋認証，金融機関 ATM における指静脈認証等が実用化されており，近年では顔認証も携帯端末に実用化されてきている．

しかし，これらには夫々に短所が存在し，それらを解決する手法の確立が急がれている．例えば，指紋を用いる場合は人工手指でのログインが可能である事，また顔認証においては照明，顔の角度，表情によって認証結果が変化するという課題が知られている．特にここまでに挙げた方法で本人拒否が発生してしまった場合に，それ単独での認証となっているとログインが不可

表 3　各種生体認証手法の特徴 [6][7][8]

種別	生体情報	特徴量	普遍性	唯一性	永続性	問題点
身体的特徴	指紋	指紋の特徴点等	高	高	高	指の状態により結果変化
	虹彩	虹彩領域の模様	高	高	高	回転変化への対応，ピント調整
	顔	顔面の特徴	中	低	中	顔の向き，表情等への対応
	(指) 静脈	静脈の透視撮影	中	中	中	撮影機器が別途必要
行動的特徴	動的署名	座標等の時間変化	低	低	低	動作の経年変化
	声紋	音声の個人差	中	低	低	ノイズ，声の変化等
	歩行	端末本体の加速度等	中	低	低	動作の経年変化

図 1　生体認証の民生端末での使用例，中央部が指紋センサ

能になってしまう為，PIN 入力やパターン認証といった非生体的方法と組み合わせて利用している．これらの様に，身体的特徴を利用した方法では「物」を認証対象としている以上，複製物による認証の対策を行う必要があると言える．

一方で音声，署名といった，何らかの行動に伴って現れる生成物から抽出した特徴を行動的特徴と呼び，採取されても心理的負担が比較的少ないという特徴がある．これらは複製の対象が「行動」であり，関節の可動域や動きの癖が人間夫々にある以上完全な複製が困難である為，普遍性及び唯一性においては理論的には優れていると考えられる．しかし永続性については，練習や外界の状態，あるいは病気等によって動作が変化する可能性もあり，何らかの方法で常時更新されたデータを用いる必要がある．

2.2　行動的特徴と既知の問題点

行動に伴う生起物を利用し，それの個人差を用いた認証手法を行動的特徴と呼ぶ [8]．例えば音声認証においては，発声時の音声をマイクロホンを用いて録音し，その際に得た音声波形を FFT 等を用いて周波数領域による変換を行い，予め録音したテンプレートと照合する．その結果がある一定の閾値以内である場合に認証成功としている．身体的特徴と比較すると，特殊な外部装置を用いずとも比較的入手が容易なセンサを導入する事で受容性を維持しつつある程度の認証精度が得られる長所があり，特にスマートフォンの様な，拡張性よりも携帯性を重視する事の多い小型端末においては特に重要な要素であると言える．

また，終生不変な身体的特徴と違い，利用者が意図的に認証に利用するパターンを任意に変更する事も可能であり，模倣されにくいパターンを作成する事が重要視されている．これは既存の認証手法であるパスワードやスワイプパターン認証と同様に，一度そのパターンが盗まれても登録している内容を変更する事で再度利用可能となる事が利点である事を意味している．即ち，個人差の出る行動的特徴を利用しつつユーザが自身で任意の動作を手軽に登録できる利便性を併せ持つ特徴がある．

既知の短所としては外乱等の作用に弱い事や，動作その物を記録されてそれを認証に使用される事が挙げられる．前述の音声認証においては，静粛な場所では成功した認証が騒音の中では失敗するという事も考えられる．これは一定の周波数の音声をカットするフィルタを通す事で解決可能だが，発話側の問題，例えば風邪等で声が変化している場合には対応できない．また，録音された音声を認証で使用された場合，特に認証基礎データの登録時の音質が悪い場合には二つの音声の差が小さくなってしまう事が考えられる．

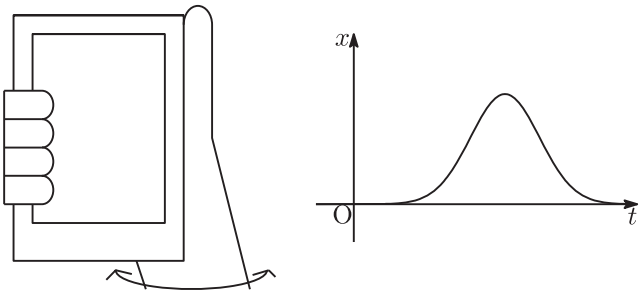
2.3　本研究での着目点

本研究では，スマートフォンにおいて標準搭載されているセンサを用いて生体認証を行うという目標から，それらのセンサで収集可能な行動的特徴をモダリティとして扱う．スマートフォンに搭載されるセンサとして，加速度センサ，重力センサ，ジャイロセンサ等が挙げられるが，本研究では加速度センサを用いる．加速度センサを用いる手法は，スマートフォン普及以前より行われてきていた [9] が，認証に用いる動作の大きさ

が問題になる場合もある．特に実際の使用時に取得する動作が大きい場合には心理的負担が掛かる可能性もある．

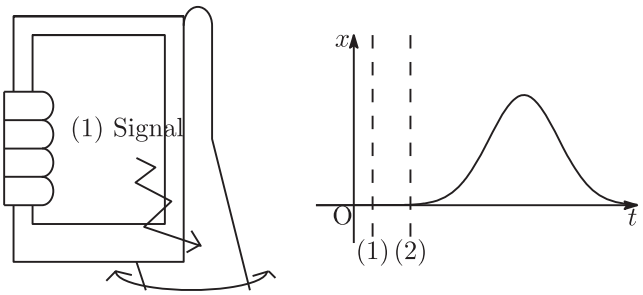
ユーザの癖を検出する行動的特徴を用いる際には「正確」「静粛」「迅速」の 3 つの要素を前提として，精度や遅れ，消費電力とのバランスを考慮する事が重要であると言える [10]．本システムでは，端末を持った側の，大きな動きを伴わない静粛な数回の手首動作を対象とし，短時間で正確な特徴抽出を行う．これにより前述の 3 要素を満たしつつ，高精度での認証を行えると予想される．

対象動作を小さくする事に伴うデメリットも考えられる．例えば，図 2 の様に手首動作のみを特徴量とした場合，加速度の変化が小さく動作を侵入者に模倣され易いというリスクが挙げられる．これは認証精度に関わる重大な欠点となり得る．これの解決策として，複数の生体認証技術のインテグレーション手法が提案されている．表 4 に示す通り，これらはアンサンブルモデル，マルチサンプルモデル，マルチモーダルモデル [6] に大別される．本システムにおいては，マルチサンプルによって認証を行う際の基礎データを作成しているが，更にマルチモーダル化する事による高精度化を目標とする．原理を図 3 に示す．先ず，(1) のタイミングで端末本体から何らかの信号が発生する．利用者はこれを受け取りその後に (2) のタイミングで動作を行う．これにより，「動きの初動までの時間」をモダリティとして追加する事が可能になる．初動までの時間は，得られた手首動作の加速度データから導出が可能であり，受容性を維持したままでの認証精度の向上が期待できる．以上の 2 つのモダリティを併用し，手首の可動域，動作速度だけでなく信号を受けてからの反応までの時間を動きの個人差として取り扱う．



Motion only

図 2　従来の動作認証の手法



Motion after Signal

図 3　本研究で利用するマルチモーダル認証

3　実験方法

本研究では，Android 端末に認証用アプリケーションをインストールし，それを用いて各ユーザの動きデータを取得する．得られた動きは軸毎に分けられた CSV ファイルに加速度の変化として記録する．そのデータを用い，パソコンを用いて数値的に比較検討する．システムの構成を図 4 に示す．また，アプリケーション構築の環境を表 5 に示す．

Android アプリケーション上では，SensorManager クラスを呼び出す事で，センサ数値が変化した際に実行される onSensorChanged メソッドが利用可能になる．また，加速度センサの精度はプログラム内で指定可能で，今回はリアルタイムに動作を取得する為，端末搭載センサの最小遅延時間ですぐ取得する `SENSOR_DELAY_FASTEST` を指定した．

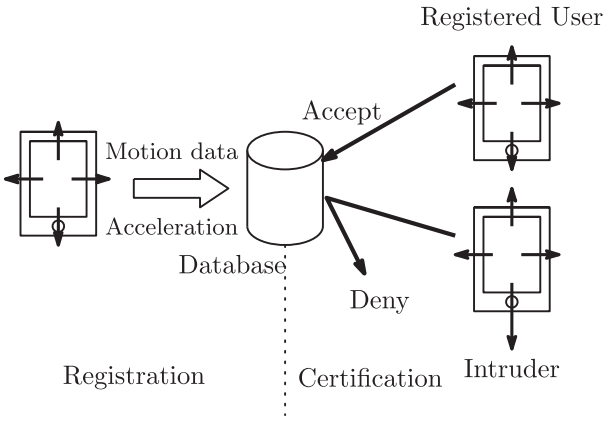


図 4　システム構成

表 4　インテグレーションモデルの分類 [6]

モデル分類	融合する情報	精度向上	利便性・可用性・受容性	その他特徴
アンサンブル	照合アルゴリズムの複合	中	一般的なシステムと同様	UI 変更不要
マルチサンプル	複数回サンプルの照合	低	利便性低下	システム構成変更不要
マルチモーダル	複数種の生体情報の照合	高	可用性・受容性向上	高精度化

認証に用いる加速度データは，一連の動作 1 サイクルにつき 440 サンプル分取得する．本システムでは，図 5 の様な，椅子に座り携帯端末を利き手で持ち，画面を見ている状態での認証操作を想定しており，また単純な動作での認証操作が行えるかを検証する為，認証に用いる動作は手首を左 → 上 → 右 → 下に返すものとした．振動のタイミングは 50，150，250，350 サンプル目とし，以降掲載の測定結果には縦軸と平行な線で示してある．

表 5　構築環境

作成環境	Eclipse(Kepler SR2)
ADT バージョン	22.6.1
使用端末	Sony Ericsson 製 SO-03D
Android バージョン	4.0.4

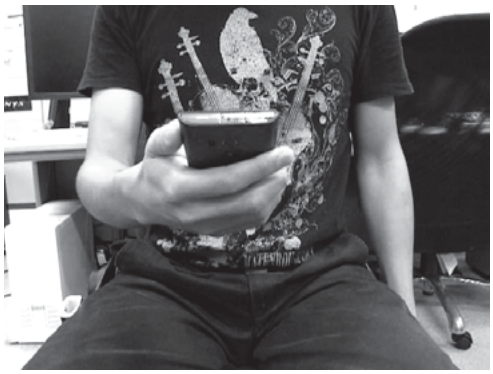


図 5　測定の様子

マスタデータ登録を行う前に，登録方法の習熟の為 1 サイクル練習を行う．その後に元データを 1 サイクル分連続で取得し，各サンプルでそれらの平均を取りこれを認証のマスタデータとする．認証においてはこのマスタデータと認証データとを，各点において誤差の自乗を取り，それらの総和を評価値とし，ある閾値を下回った場合のみ認証成功とする．

4　実験

前節の条件のもと，実験を行った．被験者は 8 名で全員右利きである．

4.1　各被験者の測定結果

表 5 の環境で作成したソフトウェアを使用し，動作における各軸の加速度データを 8 名分取得した．取得したデータの例として，図 6 に被験者 4 の測定結果，図 7 に被験者 6 の測定結果を夫々3 軸分示す． 図 6 より，被験者 4 では全ての軸において 10 回分の測定データ波形にバラつきが大きいことが確認できる．一方，図 7 より，被験者 6 では 10 回分の波形が概ねまとまっていることが確認できる．また，動作時においては各軸で何らかの加速度変動が発生している．これは [9] と異なる結果となっているが，この理由として，[9] での実験方法による動作が概ね平面上となっているのに対して，本システムでの方法は 3 次元各方向での動作であることが挙げられる．

前節での評価方法を用いて 10 回分の動作の平均を求め，それを認証マスタデータとした場合の，10 回分の動作の評価値の平均を求めたグラフを図 8 に示す．特に評価値の大きい被験者 4 を除くと，他の被験者は各軸 1000 以内に収まっており，また y 軸方向の評価値は 500 以下に収まっていることが確認できる．これらの結果より，10 回の平均では認証に用いるマスタデータとしての使用が難しいユーザも出る場合がある為，練習回数の増加又はマスタデータ作成に用いるデータ数の増加が必要と考えられる．

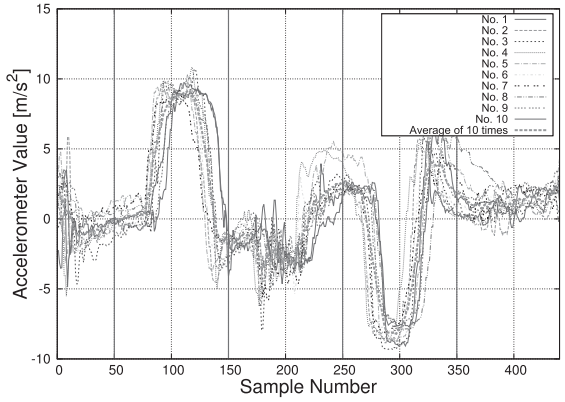
4.2　全被験者の動作の平均

10 回分の動作の平均を各被験者データに対して求めた結果を図 9 に示す．この図より，加速度数値の増加が急峻になる点，即ち動作開始点の差が 3 軸で最も大きい方向は x 軸と考えられる．

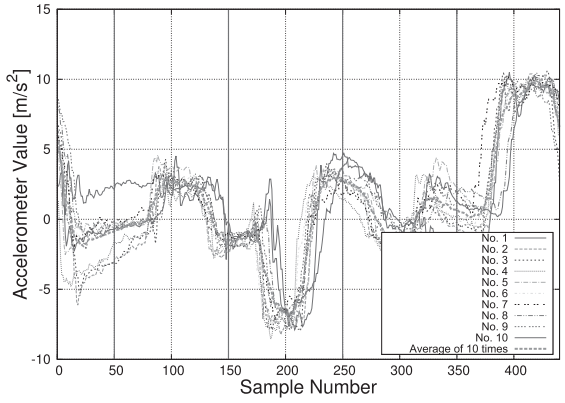
4.3　FAR/FRR 比の検討

各被験者のマスタデータに，別の被験者のデータを当てはめた場合の評価値を求め，閾値を変化させた場合に他人受入率 (FAR) がどの様に変化するかを求めた．また，同じ閾値に設定した場合の本人拒否率 (FRR) の変化を求め，本システムでの認証精度を評価した．

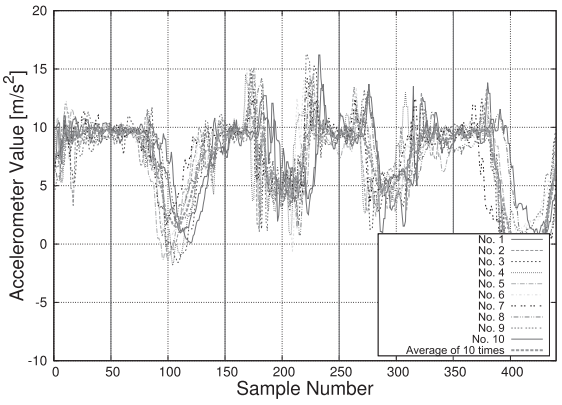
閾値は 0〜2000 まで 50 刻みで変化させ，各軸にこれらを適用し，全ての軸で適用した閾値未満となった場合



(a) x 軸

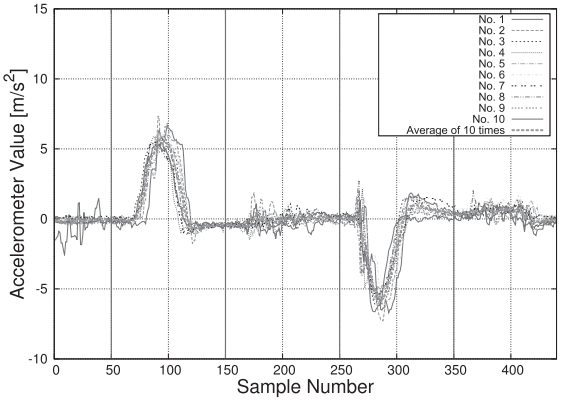


(b) y 軸

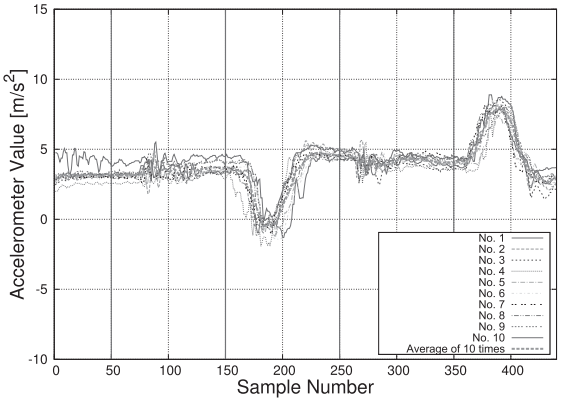


(c) z 軸

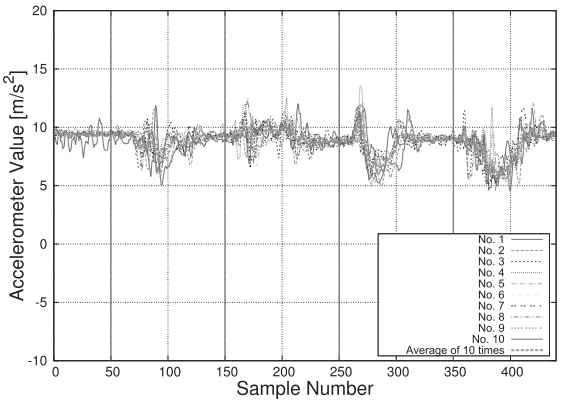
図 6　被験者 4 の測定結果



(a) x 軸



(b) y 軸



(c) z 軸

図 7　被験者 6 の測定結果

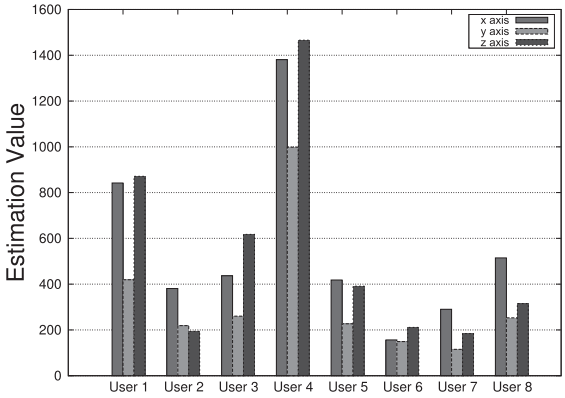


図 8　各被験者の評価値平均

のみ認証成功とする．その結果を図 10 に示す．閾値を 1400 に設定した際に，FAR = 10.357，FRR = 11.25 となった．

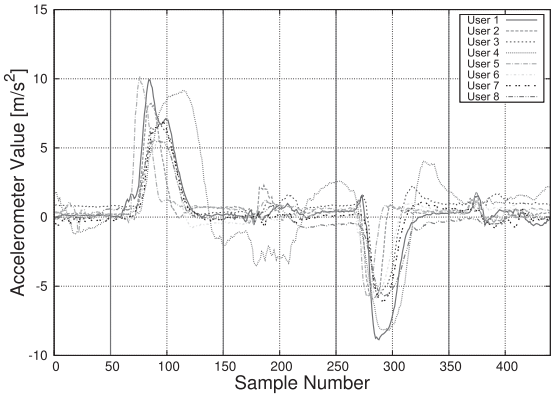
FAR，FRR 共に 10%を超える結果となったが，この理由として，事前の練習回数が 10 回，その後の測定回数が各 10 回と少なく，被験者の動作習熟が不十分だった事や，[9] よりも単純な動作を認証対象としている事が挙げられる．後者については，初動までの時間等，認証の次元を増やす事で改善されるのではないかと考えられる．また，今回は全ての軸で同じ閾値を設定して FAR/FRR 比を求めたが，図 8 より，y 軸の評価値のみ被験者 8 名中 7 名で 3 軸中最低となっている．この事から，3 軸夫々に独立した閾値を設定する事で，特に FAR の低下を図れるのではないかと考えられる．

5　考察・まとめ

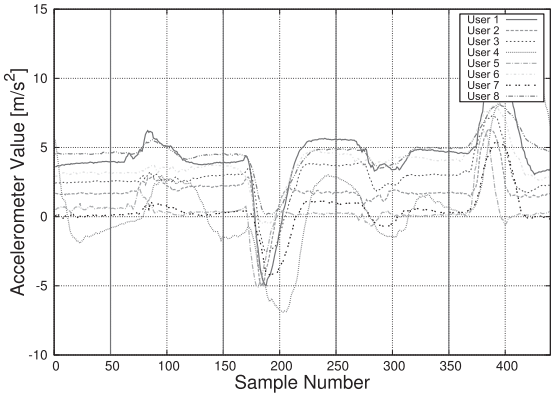
今回，振動のタイミング毎に手首を指定した順番に返すという動作を用い，その動作の変化を認証に用いるシステムを作成し被験者 8 名に対してその有効性を検討した．その結果，各被験者に対して動作の変化が確認でき，特に x 軸においては初動の速度も認証の対象にできる可能性がある事を確認した．

また取得したデータを用いて FAR/FRR 比を求めた結果，閾値 1400 の時に FAR = 10.357%，FRR = 11.25% となった．これは動作習得回数の増加，前述した認証の次元の増加，及び 3 軸で独立した閾値の設定によって改善される事が予想される．

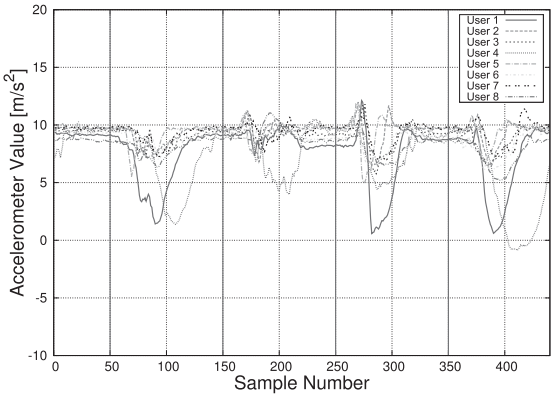
このシステムの様な本人の行動的特徴を用いた生体認証では，行動の経年変化によって特に FRR が増加する可能性も懸念されており，その対策としてマスタデータの更新機能の実装も検討されている [9]．以上を踏まえた上で，今後は認証の次元の増加と共にマスタデータの経年変化への対応を行い，誤認証の減少を目指す事を検討していく．



(a) x 軸



(b) y 軸



(c) z 軸

図 9　各被験者の動作の平均

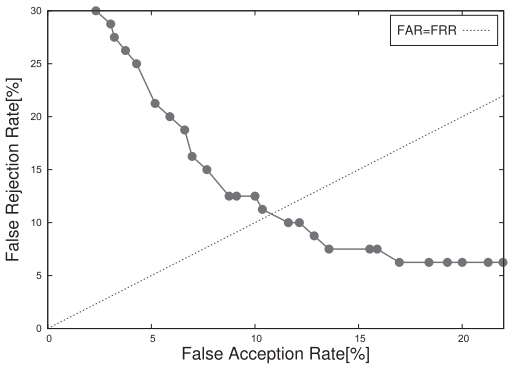


図 10　本システムの FAR/FRR 比

参考文献

[1] 総務省. 平成 26 年通信利用動向調査の結果 (Jul 2015). http://www.soumu.go.jp/johotsusintokei/statistics/data/150717_1.pdf.

[2] 鷲見和彦. 進化する生体個人認証技術とシステムの未来展望. 高精度化する個人認証技術. 株式会社エヌ・ティーエス (2014).

[3] 古賀尭志, 小高知宏, 黒岩丈介, 白井治彦. 携帯端末のセンサを用いる新しい個人認証システム. 平成 26 年度電気関係学会北陸支部連合大会 (Sept 2014).

[4] Ivan Lucas. Password recovery speeds. http://www.lockdown.co.uk/?pg=combi.

[5] delight.im. https://github.com/delight-im/AndroidPatternLock.

[6] バイオメトリクスセキュリティコンソーシアム. バイオメトリックセキュリティ・ハンドブック. オーム社 (2006).

[7] 映像情報メディア学会, 半谷精一郎. バイオメトリクス教科書 : 原理からプログラミングまで. コロナ社 (2012).

[8] 小松尚久, 内田薫, 池野修一, 坂野鋭. バイオメトリクスのおはなし : あなたの身体情報が鍵になる. おはなし科学・技術シリーズ. 日本規格協会 (2008).

[9] 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 (モバイルアプリケーション, ＜特集＞ ユビキタス ITS とモバイルアプリケーション). 情報処理学会論文誌, Vol. 46, No. 12, pp. 2997–3007 (2005).

[10] Cheng Bo, Lan Zhang, and Xiang-Yang Li. Silentsense: Silent user identification via dynamics of touch and movement behavioral biometrics. *CoRR*, Vol. abs/1309.0073 (2013).