Vol.2014-MBL-70 No.17
Vol.2014-UBI-41 No.17
2014/3/14

加速度センサ・ジャイロセンサを併用したスマートフォンの利用認証手法の提案

濵野 雅史[1]　新井 イスマイル[1]

概要：現在，スマートフォンの認証手法として，省作業性と高い強度を兼ね備えたバイオメトリクス認証が注目されている．バイオメトリクス認証の代表的な例として加速度センサを使用したジェスチャ認証があるが，加速度センサのみでは回転動作を取得することが出来ないためパスワードを盗難される危険性も高まる．そのため，強度を高くするためには複雑な動作で認証しなければいけないため省作業が失われる．本研究では，スマートフォンに標準搭載されているデバイスだけを使用することを目的とし，加速度センサに加えてジャイロセンサを併用したジェスチャ認証として一筆書き認証と単一動作組み合わせ認証を提案する．14 人の被験者によって実証実験を行った結果、一筆書き認証では，本人拒否率が 56.90[%]，他人受入率が 10.71[%]，単一動作組み合わせ認証では，本人拒否率が 44.05[%]，他人受入率が 30.71[%] という結果になった．また，開発者として十分に慣れている筆頭著者に対して同様の実験を行ったところ，一筆書き認証では，本人拒否率が 3[%]，他人受入率が 1.67[%]，単一動作組み合わせ認証では，本人拒否率が 11[%]，他人受入率が 71.67[%] という結果になった．

キーワード：スマートフォン，バイオメトリクス認証，加速度センサ，ジャイロセンサ，DP マッチング

1. はじめに

近年，スマートフォンの普及に伴い，誰でも手軽に多くの情報を持ち歩くことが出来るようになった．その反面，端末の利用認証を高い強度で設定しておかなければ，スマートフォンを紛失，盗難にあった際に悪用されるリスクも高まっている．

現在市販されているスマートフォンでは，数字入力や，点を結ぶなど，タッチパネルをタッチして解除を行う方法が主に使用されているが，指脂の軌跡からパスワードを解読される可能性がある．また，タッチパネルであるが故，解除を行うたびにディスプレイに注目する必要があり省作業性に欠ける．そこで現在，上記の問題を解決する省作業性かつ強度の高い認証手法としてバイオメトリクス認証が注目されている．バイオメトリクス認証を用いることによって，省作業性かつ強度の高い認証が出来るが，別途追加デバイスが必要になることがある．そのため，本研究ではスマートフォンに標準搭載されている入力インタフェースやセンサ類のみを使用したバイオメトリクス認証に注目する．

既存の研究に，スマートフォンに搭載されている加速度センサだけを用いてユーザが考えたジェスチャ動作から認証するもの [1]，加速度センサとタッチパネルを用いてそれぞれ単一動作を組み合わせて認証するもの [2] 等がある．しかし，加速度センサだけでは自由度が限られるため，強度を高めるにはジェスチャ動作を長くしなければならない欠点がある．

本稿では，加速度センサに加えてジャイロセンサを用いたジェスチャ動作による認証手法を提案する．ジャイロセンサを加えることにより，回転動作を取得することが出来るので自由度が高くなる．さらに，手首を使った回転動作は他人から見ても分かりにくいため，少ない動作でも強度を高めることが出来る．

本研究では，一筆書きのようにユーザが自由にジェスチャを登録し，同じジェスチャが再現出来るかどうかの認証手法，単一な動作 (上下左右・奥手前，ロール・ピッチ・ヨーの正負回転に端末を動かす) をパスワードのように組み合わせる認証手法の，2 種類の認証手法を提案し，本人拒否率と他人受入率を測る実証実験を計 4 日に渡って行った．一筆書き認証では，本人拒否率が 56.90[%]，他人受入率が 10.71[%] となった．また，既存手法との比較として，

[1] 明石工業高等専門学校 電気情報工学科, Department of Electrical and Computer Engineering, Akashi National College of Technology

Vol.2014-MBL-70 No.17
Vol.2014-UBI-41 No.17
2014/3/14

加速度のみを認証としたときの本人拒否率が 44.54[%]，他人受入率が 18.57[%] という結果になり，他人拒否率を約 8[%] 下げることが出来た．さらに，単一動作組み合わせ認証では，本人拒否率が 44.05[%]，他人受入率が 30.71[%] となった．さらに，約 2 週間練習し，また開発者として十分に慣れている著者に同様の実験を行ったところ，一筆書き認証では，本人拒否率が 3[%]，他人受入率が 1.67[%]，単一動作組み合わせ認証では，本人拒否率が 11[%]，他人受入率が 71.67[%] となった．

以降，2 章でスマートフォン等の携帯端末の利用認証手法についての関連研究についてまとめ，3 章にて加速度センサ・ジャイロセンサを併用したスマートフォンの利用認証手法の提案を述べる．さらに，4 章に提案手法を実装した実験・結果および考察を述べ，5 章にて本論文をまとめる．

2. 関連研究

既存の認証手法の評価方法として次のようなことが挙げられる．まず，ユーザが認証手法に対して本人でないと判定されはじかれる度合い (本人拒否率)，他人がユーザに成りすまし認証し，本人であると判定され受け入れられる度合い (他人受入率) がある．本論文で「強度」という言葉も用いるが，これは他人受入率の逆の他人拒否率，つまり度合いが高い程性能が高いことを示す指標である．次に、追加機器の必要性である．追加機器が別途必要となると総じて評価が高くても普及しにくい傾向がある．代表例として指紋リーダや静脈リーダ等が挙げられる．次に，高強度時の作業量である．現在主に用いられている認証手法は強度を高くしようとすると作業量を多くしなければならないものが多い．最後に，公共空間等で利用する際の外乱の影響である．

本研究の第一要件として，スマートフォンを使用している人ならばだれでも追加コスト無しに利用出来るように，スマートフォンに標準搭載されている入力インタフェースやセンサ類だけを使用する．さらに，作業量を増やして強度を高くすると従来と同様の問題を抱えてしまうため，省作業性かつ強度が高いことを本研究の第二要件とする．

以上で述べたことを評価方法として，様々な認証手法をまとめたものを表 1 に示す．

現在スマートフォンの認証手法として主に使用されているパスワードロックのパターン数は，4 桁〜6 桁の数字パスワードだと 10,000〜1,000,000 通り，Android OS の，3 × 3 の点に配置された点をあらかじめ登録しておいた軌跡でなぞる「パターンで保護」だと 1,624〜389,112 通りで設定することが出来る．これらの現状を考慮して，最低でも 4 桁数字のパスワードよりも高い強度が要求される．単に強度だけを高めることが目的であれば，現状のパスワード入力手法ではパスワードの桁数を増やせばよいが，それでは省作業性が失われる．さらに毎回タッチパネルを確認しながら認証を行う煩わしさから省作業性が低いうえ，指脂の軌跡からパスワードを解読される可能性が高い．

そのため現在，上記問題を解決する認証方法としてバイオメトリクス認証が注目されている．バイオメトリクス認証として，キーボード入力の際のキーストロークの違いから個人識別をするキーストローク認証 [3] がある．この認証手法は従来のようにパスワードを覚える必要がなく，さらに強度も高い．しかし長い文章を打たなければ識別出来ないことからスマートフォン利用では省作業性が低い．他には，マイクを用いた声紋認証[*1]がある．省作業性も高くパスワードを解読される心配は少ないが，周囲のノイズの少ない場所でしか使用することが出来なく，例えば電車などの騒音を伴う公共空間では使用出来ないという制約がある．カメラを用いた顔認証 [4] では，省作業性は高いが，少しでもブレがあると認証出来ないので静止した状態で使用しなければならない．そのため省作業性に欠けている．また，暗闇では使用出来ない（外乱に弱い）という欠点がある．その他，声紋認証では他人に声を録音されていた場合，顔認証では顔を撮影されていた場合に成りすまされる恐れがある．

加速度センサを用いたジェスチャ認証 [1] であれば，周囲のノイズが多い場所や，暗闇でも使用することができ，外乱に強い．従来のパスワードによる認証手法のように，スマートフォンのタッチパネルをタッチする必要がないので，カバンやポケットの中から取り出す過程の一連の動作で認証することも可能である．しかし加速度センサだけを用いた認証手法では，6 自由度（端末を上下左右・奥手前に振る動作）によるジェスチャしか組み合わせることが出来ない．これではジェスチャの自由度が少ないので，ジェスチャのパターンを他人に覚えられる可能性があり，強度を上げるには入力を長くしなければいけない．

3. 加速度センサ・ジャイロセンサを併用した利用認証手法の提案・設計

3.1 提案手法

ジェスチャ認証の省作業性を向上させるには自由度を上げることが望ましい．そこで本研究はジェスチャ認証に利

[*1] 「AdvanceMediaInc.」http://www.advanced-media.co.jp/products/amivoiceverification.html(最 終 検索日：2014/2/10)

Vol.2014-MBL-70 No.17
Vol.2014-UBI-41 No.17
2014/3/14

表 1 既存認証手法の比較

		本人拒否率	他人受入率	追加機器の必要性	高強度時の作業量	外乱の影響	必要デバイス（追加必要性）
非バイオメトリクス	鍵，IC カード	低	低	有	少	低	鍵，カード（有）
	パスワード	低	低	無	多	低	入力用ボタン，タッチパネル（無）
バイオメトリクス (身体的特徴)	指紋	低	低	有	少	低	指紋リーダ （有）
	顔	高	中	無	少	高	カメラ（無）
	声紋	中	低	無	少	高	マイク（無）
バイオメトリクス (行動的特徴)	キーストローク	中	低	無	多	低	キーボード（無）
	筆跡	中	低	有	多	中	タブレット，ペン（有）
	ジェスチャ動作	中	低	無	多	中	加速度センサ（無）

用するセンサとして加速度センサに加えてジャイロセンサを活用することを提案する．加速度センサでは回転動作が取得出来ないがジャイロセンサで取得することができ，これによって自由度を上げることが出来る．

また，回転動作は周りから見てもわかりずらいので，少ない動作でも強度を高めることが出来るのではないかと考えている．

本研究で加速度・ジャイロセンサを併用した認証手法として以下の 2 通りを提案する．

(1) ユーザが自由にジェスチャを考えて登録し，同じ動きが出来れば認証
(2) 単一動作（上下左右・奥手前，ロール・ピッチ・ヨーの正負回転に端末を動かす）をパスワードのように組み合わせて認証

便宜上，前者の認証手法を「一筆書き認証」と名付け，後者の認証手法を「単一動作組み合わせ認証」と名付ける．

一筆書き認証は一筆書きのように，一連の動作をユーザが自由に考えて登録する．このとき加速度センサから得られる値とジャイロセンサから得られる角速度をサンプリングしておき，認証の際に得られる入力サンプリングデータと，あらかじめ登録されているマスタデータを DP マッチングによって同一のジェスチャであるかを判断し認証する．この認証手法はジェスチャをユーザが自由に考えて登録するので，動作に個人の特徴が出るため，他人に見られても真似され成りすまされる可能性は低いが，複雑な動きにすればするほど本人拒否率が高くなる可能性がある．

単一動作組み合わせ認証は，端末を「上下左右・奥手前に振る，ロール・ピッチ・ヨーの正回転と逆回転」といった 12 種類のジェスチャパターンを定めておき，ユーザがこれらのジェスチャパターンを最低 4 桁以上，最高 12 桁以下パスワードのように組み合わせて認証する．この認証手法は単一な動作であるので，本人拒否率は低くなると予想されるが，動作に個人の特徴が出にくいため，他人に見られたときに真似され成りすまされる可能性が高い．

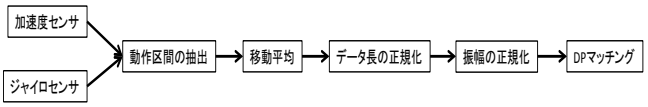

図 1 一筆書き認証データフロー

3.2 設計

3.2.1 一筆書き認証

認証の時に使用する入力サンプリングデータとして，合成加速度 (式 1), および合成角速度 (式 2) をマッチングの対象としている．加速度の値をそれぞれ，a_x，a_y，a_z としたとき合成加速度を

$$a = \sqrt{a_x^2 + a_y^2 + a_z^2} \tag{1}$$

で表し，角速度の値をそれぞれ，ω_x，ω_y，ω_z としたとき合成角速度を

$$\omega = \sqrt{\omega_x^2 + \omega_y^2 + \omega_z^2} \tag{2}$$

で表す．

この認証手法のデータフローを図 1 に示す．

3.2.2 単一動作組み合わせ認証

本認証手法でのジェスチャパターンの識別はセンサから得られる加速度データ・ジャイロデータのそれぞれ x, y, z 軸の 6 つのラベルから分散をとり，一番分散が大きいものをジェスチャパターンとして識別している．識別したジェスチャパターンをパスワードのように 4 桁以上 12 桁以下組み合わせて羅列し，登録されたジェスチャパターン列と一致しているかを判定する．ジェスチャパターンを 4 桁以上 12 桁以下組み合わせるため，ジェスチャパターンの識別までを 3 回〜11 回繰り返している．この認証手法のデータフローを図 2 に示す．

3.3 特徴量の抽出

3.2 節でブロックの記述に留まっていた各動作の詳細な設計を以下に述べる．

Vol.2014-MBL-70 No.17
Vol.2014-UBI-41 No.17
2014/3/14

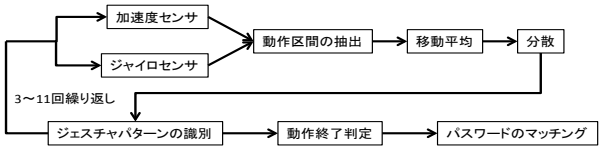

図 2 単一動作組み合わせ認証データフロー

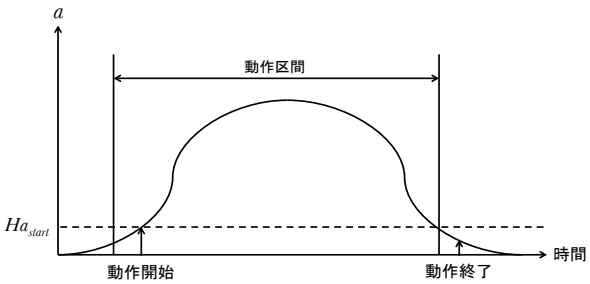

図 3 動作区間抽出概要

3.3.1 動作区間の抽出

本研究で使用する認証手法では，システムを起動してから常に加速度と角速度の値をサンプリングし，随時合成加速度および合成角速度を導出している．そのため，システムを起動してからジェスチャに移るまでの時間は毎回異なるので，認証に使用するジェスチャの動作区間を抽出する必要がある．

ここで，加速度の場合の動作区間抽出の概要を図 3 に示す．あらかじめ動作開始の合成加速度の閾値 Ha_{start}，合成角速度の閾値 $H\omega_{start}$ と，動作終了の閾値 Ha_{end}，$H\omega_{end}$ を設定しておく．合成加速度か合成角速度の値が Ha_{start}，$H\omega_{start}$ を超えたところを動作の開始とみなし，それぞれの値が数秒間 Ha_{end}，$H\omega_{end}$ 下回ったところを動作の終了とみなす．閾値を超えた瞬間のところからを動作開始とすると動作の途中からサンプリングする可能性があり，数秒間下回ったところまでを動作終了とするとデータ長の最後に 0 に近い値が連続するため，動作の開始から数サンプル手前から動作終了の数サンプル手前までを動作区間としている．[1]

なお，一筆書き認証の認証手法では，一筆書きのようなジェスチャを想定しているので，一度止まってまた動きだすようなジェスチャは想定していない．

3.3.2 移動平均

双方の認証手法で認証の際に使用するデータについては，センサから得られた生データを用いるのではなく，手振れなどの微小なノイズを除去するため，移動平均 [5] を施したデータを用いてマッチングを行う．

8 の字を描くジェスチャを 5 回行った時の合成加速度の

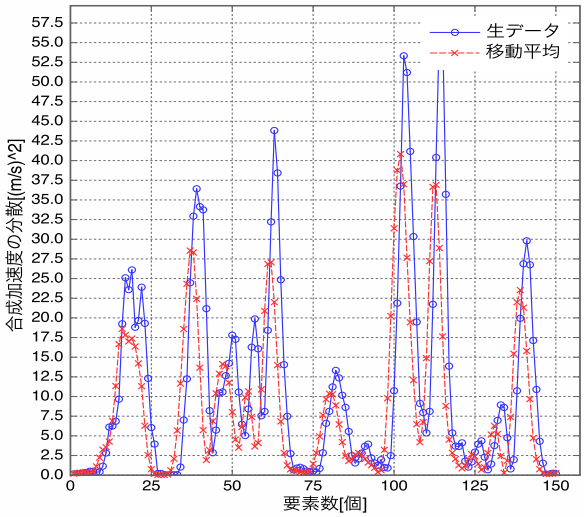

図 4 合成加速度の分散の生データと移動平均の比較

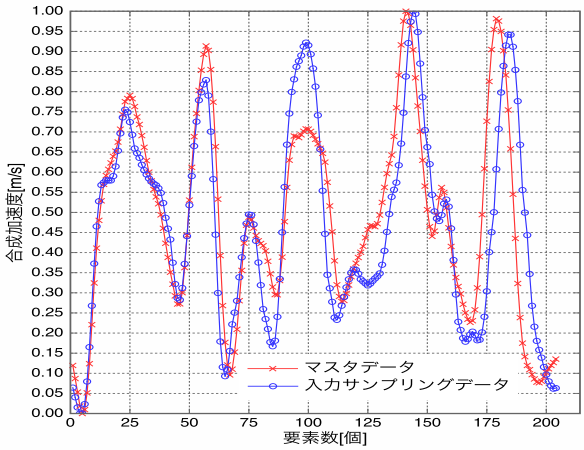

図 5 正規化後の入力サンプリングデータとマスタデータの比較

生データと，要素数 5 個で移動平均を施したデータの分散をとり，比較したグラフを図 4 に示す．

図 4 において，横軸 20 付近での振幅の増減が滑らかになっている．このように，移動平均を施すとデータのばらつきを抑えることが出来るので，微小なノイズを除去出来ているといえる．

3.3.3 データ長の正規化

ユーザが認証時に行ったジェスチャの入力サンプリングデータと，あらかじめ登録しておいたマスタデータの長さが異なる場合が多いので，比較するための前処理としてデータ長の正規化を行って，入力サンプリングデータ長をマスタデータ長に揃える．元々要素数 190[個] であったサンプリングデータを要素数 204[個] のマスタデータに正規化したグラフを図 5 に示す．このように，正規化前はデータ長が短かったのだが，マスターデータ長に合わせて正規

化することにより，データ長が長くなっている．

3.3.4 振幅の正規化

ユーザが登録したジェスチャと同じ動作を意図して認証動作を行っても，端末を動かす速度が異なると，加速度および角速度の振幅値が変化するため，別のジェスチャだとみなされてしまう可能性が高い．そのため，加速度および角速度の最大振幅値が 1 になるように正規化した．入力サンプリングデータの正規化後のグラフを図 5 に示す．このように，最大振幅値が 1 に，最小振幅値が 0 に正規化されている．

3.3.5 DP マッチング

一筆書き認証のマッチング手法として，本研究では DP マッチング [6] を使用した．DP マッチングは，時系列になっているデータ同士の類似度を比較する手法で，2 つのデータの要素間の整列化を行いながら，一度計算した結果を利用して，効率的に類似度 (DP マッチング距離) の計算を行う方法である．マスタデータと入力サンプリングデータの各値を整列化する際に各値の差に対する閾値を定め，閾値以内であれば同じ値とみなしている．マスタデータ系列を M，入力サンプリングデータ系列を I とし，DP マッチング距離 $D(M,I)$ を算出する際の漸化式を以下に示す．

$$g(j,k) = min \begin{cases} g(j-1,k) + d(j,k) + 1 \\ g(j-1,k-1) + d(j,k) \\ g(j,k-1) + d(j,k) + 1 \end{cases} \quad (3)$$

$$g(0,0) = d(0,0)$$
$$j = 1 \sim l_m,\ k = 1 \sim l_i$$

$$D(M,I) = g(j,k) \quad (4)$$

マスタデータと入力サンプリングデータの各値を整列化した際に，同じ値であるとみなされた場合に $d(j,k) = 0$，違う値であるとみなされた場合に $d(j,k) = 3$ としている．DP マッチングを合成加速度および合成角速度に対して使用し，上式によって算出された $D(l_m - 1, l_i - 1)$ が両方ともあらかじめ定めておいた閾値以内であれば同じジェスチャであるとみなしている．

3.3.6 分散

単一動作組み合わせ認証では，センサから得られた生データに移動平均を施した後，分散を求めることによりジェスチャパターンの識別を行っている．分散を求めることによって，加速度および角速度の x, y, z 軸の分散が最大

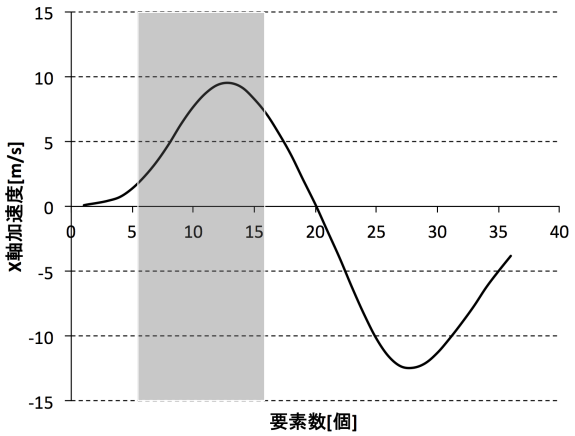

図 6 端末を右に振った時の加速度

の軸への動作を行っていることが分かる．例えば x 軸が最大であれば左右のどちらかに端末が動いている．左右の正負判定としては入力サンプリングデータ長の $\frac{1}{4}$ のところから $\frac{1}{2}$ のところまでの入力サンプリングデータの生データの総和が，正か負かで判断している．

端末を右に振っているときの加速度のグラフを図 6 に示す．このとき，網掛けにしているところの総和から，正負判定をしている．

さらに，加速度センサから得られる値より，角速度センサから得られる値が弱く，回転の動作を加速度と平等に扱うことが出来なかったため，角速度を 5 倍に増幅することによって解決した．増幅する定数を複数のパターン検証し，5 倍が一番回転動作を加速度と平等に扱うことが出来たため，5 倍に増幅している．

4. 実験・結果および考察

本研究では，一筆書き認証と単一動作組み合わせ認証の双方で，本人拒否率と他人受入率を測る 2 通りの実験と，アンケート調査からどちらの認証手法が優れているかを検証した．被験者としては，15 歳から 19 歳の高専生男女 14 名を対象とした．本実験で使用した端末は Samsung 社の Android 端末，Galaxy Nexus で統一し，端末による個体差を除くため，被験者には各日同じ端末を使用してもらった．実験時の加速度・角速度のサンプリングレートは 100[Hz] とした．

本実験で開発した 2 種類のアプリケーションの画面遷移図を図 7，図 8 に示す．

両認証手法で，まずユーザ登録を行ってから，ジェスチャまたはジェスチャパターンの組み合わせを登録してもらい，練習画面で練習してもらってから，認証実験を開始

Vol.2014-MBL-70 No.17
Vol.2014-UBI-41 No.17
2014/3/14

表 2 実験使用端末仕様

サイズ (h × w × d [mm])	135.5 × 67.94 × 8.94
重量 [g]	135
OS	Android 4.2.1
CPU	Texas Instruments OMAP 4460 1.2GHz
メモリ	1GB

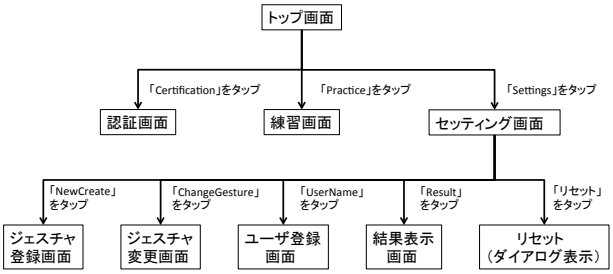

図 7 一筆書き認証の画面遷移図

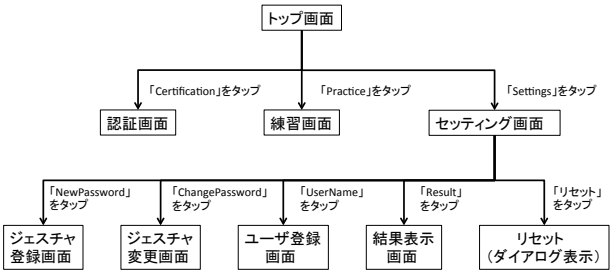

図 8 単一動作組み合わせ認証の画面遷移図

してもらった．

4.1 本人拒否率 (FRR)

一筆書き認証および単一動作組み合わせ認証での実験方法は，被験者に登録したいジェスチャまたはジェスチャパターンの組み合わせを練習してもらい，ある程度慣れてからジェスチャまたはジェスチャパターンの組み合わせを登録し，認証動作を 10 回繰り返す実験を 3 日に渡って行った．そのときに得られた成功数および失敗数から本人拒否率を算出した．一筆書き認証はある程度習熟が必要であると考えられるので，初日は本人拒否率は高くなるが，日を重ねるごとに本人拒否率は低くなると予想する．単一動作組み合わせ認証は初日から一筆書き認証と比べて本人拒否率は低いと予想する．

4.2 他人受入率 (FAR)

一筆書き認証および単一動作組み合わせ認証での実験方法は，ある程度双方の認証手法に慣れた状態で，2 人 1 組になってもらい相手に自分の登録したジェスチャおよび，

表 3 一筆書き認証 FRR

	1 日目	2 日目	3 日目
	FRR [%]	FRR [%]	FRR [%]
被験者 1	70	0	50
被験者 2	40	40	60
被験者 3	90	90	100
被験者 4	10	40	50
被験者 5	10	10	80
被験者 6	100	90	80
被験者 7	40	40	40
被験者 8	60	70	90
被験者 9	40	40	70
被験者 10	100	70	40
被験者 11	40	30	90
被験者 12	90	0	50
被験者 13	70	10	10
被験者 14	100	100	90
平均	61.43	45.00	64.29

ジェスチャパターンの組み合わせを数回見てもらってから相手に端末を渡し，成りすまして認証可能かどうかを 10 回繰り返す実験を行った．そのときに得られた，成功数および失敗数から他人受入率を算出した．本実験は本人拒否率の実験が終了した後日に行ったため，一部被験者が入れ替わっている．本実験では一筆書き認証の他人受入率は低く，単一動作組み合わせ認証の他人受入率は一筆書き認証よりも高くなると予想する．

4.3 本人拒否率 (FRR) 結果

一筆書き認証での本人拒否率を表 3 に示す．一筆書き認証での本人拒否率を表 3 に示す．予想通り，初日の本人拒否率が高く，2 日目の本人拒否率は低くなっている結果となった．しかし，3 日目の本人拒否率が高くなっている結果となった．2 日目の実験から少し日が空いてしまった為，以前の感覚を忘れてしまい本人拒否率が高くなったと考えられる．

さらに，既存研究との比較として，提案手法の 3 日間の合計から出した本人拒否率と，加速度のみを認証の対象としたときの本人拒否率を比較したものを表 4 に示す．加速度のみを認証の対象としているので，端末の細かな回転は無視でき，動作の速さだけがポイントになる為本人拒否率は低くなっている．

単一動作組み合わせ認証での本人拒否率を表 5 に示す．初日から一筆書き認証より本人拒否率が低い結果になった

Vol.2014-MBL-70 No.17
Vol.2014-UBI-41 No.17
2014/3/14

表 4 提案手法と既存手法の FRR の比較

	提案手法	既存手法
	FRR [%]	FRR [%]
被験者 1	40	40
被験者 2	46.67	43.33
被験者 3	93.33	70
被験者 4	33.33	23.33
被験者 5	33.33	30
被験者 6	90	73.33
被験者 7	40	33.33
被験者 8	73.33	60
被験者 9	50	33.33
被験者 10	70	66.67
被験者 11	53.33	33.33
被験者 12	46.67	26.67
被験者 13	30	23.33
被験者 14	96.67	66.67
平均	56.90	44.52

表 5 単一動作組み合わせ認証 FRR

	1 日目	2 日目	3 日目
	FRR [%]	FRR [%]	FRR [%]
被験者 1	50	20	70
被験者 2	30	50	60
被験者 3	60	70	60
被験者 4	20	70	70
被験者 5	10	30	30
被験者 6	100	50	20
被験者 7	50	20	90
被験者 8	100	10	90
被験者 9	40	10	30
被験者 10	80	0	10
被験者 11	100	0	30
被験者 12	20	50	40
被験者 13	30	70	20
被験者 14	50	20	20
平均	52.86	33.57	45.72

が，3 日間の合計から出した本人拒否率は 44.05[%] と，予想していた結果よりも本人拒否率が高い．被験者が認証の際に入力したデータを調べてみると，登録した動作の組み合わせと全く違う組み合わせが入力されていることは無かったのだが，登録した動作の逆の動作が一部入力されていることが多々あった．

表 6 一筆書き認証・単一動作組み合わせ認証 FAR

	一筆書き認証	単一動作組み合わせ認証
	FAR [%]	FAR [%]
被験者 1	0	0
被験者 2	0	50
被験者 3	20	30
被験者 4	0	0
被験者 5	0	50
被験者 6	0	70
被験者 7	0	30
被験者 8	30	80
被験者 9	0	10
被験者 10	0	0
被験者 11	0	20
被験者 12	30	0
被験者 13	70	90
被験者 14	0	0
平均	10.71	30.71

約 2 週間ほど練習し，また開発者として十分に慣れている筆頭著者についても評価してみたところ，一筆書き認証の本人拒否率は 3[%]、単一動作組み合わせ認証の本人拒否率は 11[%] という結果になった．このことから，本人拒否率を下げる為には，十分に慣れる必要があることが分かる．

4.4 他人受入率 (FAR) 結果

一筆書き認証および単一動作組み合わせ認証での他人受入率を表 6 に示す．予想通り，一筆書き認証の他人受入率は低く，相手のジェスチャを数回見ただけでは成りすますことが難しいことが分かった．被験者 13 については他人受入率が高いが，この被験者のジェスチャは端末を 1 回下に振るだけの簡単なジェスチャであった為，他人受入率が高くなっていると考えられる．単一動作組み合わせ認証では，数回相手の動作の組み合わせを見ただけで成りすまされ易いことが分かった．

既存研究との比較として，一筆書き認証での提案手法と加速度のみを認証の対象としたときの他人受入率の比較を表 7 に示す．やはり，加速度のみであると，細かな回転の動きは無視されるので成りすまされ易いことが分かる．

被験者を本人拒否率の低い順に 3 つのグループに分け，各グループからそれぞれ数名ずつ選出し合計 5 名に対して，十分に慣れている筆頭著者についても同様の実験を行った．そのときの結果を表 8 に示す．被験者による他人受入率と比べ，一筆書き認証において約 2[%] 増加しているが，

表 7 提案手法と既存手法の FAR の比較

	提案手法	既存手法
	FAR [%]	FAR [%]
被験者 1	0	0
被験者 2	0	10
被験者 3	20	50
被験者 4	0	0
被験者 5	0	0
被験者 6	0	20
被験者 7	0	0
被験者 8	30	30
被験者 9	0	0
被験者 10	0	60
被験者 11	0	0
被験者 12	30	0
被験者 13	70	90
被験者 14	0	0
平均	10.71	18.57

表 8 筆頭著者が成りすましたときの FAR

	一筆書き認証	単一動作組み合わせ認証
	FAR [%]	FAR [%]
被験者 1	0	80
被験者 2	0	40
被験者 3	40	0
被験者 4	20	0
被験者 5	0	0
平均	12.00	24.00

単一動作認証においては約 6[%] 減少しているので，他人に成りすますときの習熟度はあまり関係ないことが分かる．

さらに，先ほど選出した 5 名にランダムで 1 名加え，合計 6 名に筆頭著者のジェスチャや動作の組み合わせを，多くの回数見てもらい成りすましてもらったところ，一筆書き認証において，他人受入率が 1.67[%]，単一動作組み合わせ認証において，他人受入率が 71.67[%] という結果になった．このことから，一筆書き認証においては習熟度が高いと，何回見られても他人に成りすまされる可能性は極めて低く，単一動作組み合わせ認証においては，習熟度が高くても多くの回数見られると他人に成りすまされ易いことが分かった．

4.5 アンケート調査

全ての実験が終了してから，一筆書き認証と単一動作組み合わせ認証のどちらが使い易かったかアンケートしたところ，一筆書き認証 7 票，単一動作組み合わせ認証 7 票のどちらも同数であった．どちらの認証手法も習熟度に個人差があり，また期間が短かったため、以上の結果から一概にどちらの認証手法が使い易いかを判断することは難しい．筆頭著者は一筆書き認証の方が使い易いと感じた．

5. おわりに

本論文では，現在使用されているスマートフォンの利用認証手法の強度と省作業性が低い問題を解決するために，加速度センサとジャイロセンサを併用したスマートフォンの利用認証手法について，一筆書き認証と単一動作組み合わせ認証の 2 種類の手法を提案した．今回の 4 日間に渡った実験において，本人拒否率は単一動作組み合わせ認証の方が優れており，他人受入率は一筆書き認証が優れている結果になった．一筆書き認証は習熟度が高いほど，本人拒否率が低くなることが確認出来たので，長期間で実験を行うともう少し本人拒否率が下がるのではないかと予想する．さらに，本研究ではマスタデータの更新を考慮していなかったので，マスタデータの更新を行うとさらに，本人拒否率が下がると推測する．単一動作組み合わせ認証においては，登録された動作の正負が逆の入力を多く確認したので，正負判定のアルゴリズムを変える必要がある．今後，一筆書き認証においてはマスタデータの更新を実装し，単一動作組み合わせ認証においては正負判定のアルゴリズムを変更したものを実装し，さらに本人拒否率を下げることを目指していきたい．

参考文献

[1] 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 ”，情報処理学会論文誌，46(12), pp. 2997-3007, Dec, 2005.
[2] 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，Vol.2012-CSEC-56 No.8, Feb, 2012.
[3] 佐村 敏治， 西村 治彦：”テキスト入力によるキーストロークダイナミックス”，情報知識学会誌 Vol. 16 , No.2, pp.263–268 , Dec, 2006.
[4] 佐藤 俊雄：”顔による個人認証”，生体医工学，44(1) : pp. 40-46, 2006.
[5] 山本 健太郎， 上岡 英史 :“ 忠実な動作抽出アルゴリズムを用いた手振り個体識別 ”，電子情報通信学会，モバイルマルチメディア通信 112(44), 15-20, May, 2012.
[6] 藤井 亮介 :“ DP マッチングによる文字認識の手法を応用したヒトの動作のパターン認識 ”，大学院研究年報 理工学研究科篇, 第 43 号/2013，Jul, 2013.