端末自体の動きを用いた携帯端末向け個人認証

石原 進[†1] 太田雅敏[†3]
行方 エリキ[†2,☆] 水野忠則[†4]

携帯端末向けの手軽な個人認証手法として，携帯端末の動きを用いた個人認証手法「3D 動作認証」を提案し，その有用性について基礎的評価を行う．3D 動作認証では，動作計測用のセンサを搭載した小型端末でユーザの動きをとらえ，その個人特徴を認証に利用する．小型の加速度センサは腕時計や携帯電話に内蔵することができ，ユーザは特別な入力装置を用いずに，端末を動かすだけで手軽に認証操作を行うことができる．3 次元空間での動きは筆跡という目に見える形で残ることがなく，手首のひねりなどを利用した動作を肉眼でとらえることは難しいため，他人に動作をコピーされ悪用される危険性が低い．本手法では加速度センサで得られる加速度の DP マッチングにより認証判定を行う．加速度センサを搭載した実験用端末を用い，11 人の動作登録者および 27 人の成りすまし被験者による実験の結果を行った．この結果より，本手法に適した認証用動作の特性を確かめた．また，ユーザ自身のサインを動作パターンとして用いた場合，上記の特性に従って登録する動作の選別を行えば，本人拒否率を 1.5%未満，動作パターンを図示された条件下での成りすまし成功率を 1%未満とできることが確かめられた．

Individual Authentication for Portable Devices Using Motion of the Devices

Susumu Ishihara,[†1] Masatoshi Ohta,[†3] Eric Namikata[†2,☆] and Tadanori Mizuno[†4]

We propose an individual authentication scheme using motions of a portable device *3D motion authentication*. In this paper, we evaluated the fundamental properties of the scheme. The 3D motion authentication scheme measures motions with a small device equipped with an acceleration sensor for the authentication. The risk of misuse by others is low in the method, because the motion of a device in the air doesn't remain as handwriting and it is difficult to recognize the motion with the naked eye. The scheme uses DP matching to judge motions. We developed a prototype device like a mobile phone for the authentication scheme and tested it with 11 registered users and 27 attackers. We obtained a guideline for suitable motion patterns for this scheme from the results. We also obtained false rejection rate less than 1.5% and the false acceptance rate for vicious attackers who know the motion pattern show in the figure less than 1% with the user's own signature satisfying the guideline.

1. はじめに

近年普及している携帯電話や PDA などの小型携帯端末には，スケジュールやアドレス帳などの様々な個人情報を記録することができ，外出先でも手軽に多くの情報を取り出すことができる．このような携帯端末は，その持ち運びやすさゆえに，ときには机の上などに忘れてしまったり，紛失したりすることが多々ある．電子商取引などで用いる情報鍵などが端末に登録されている場合もあり，他人に悪用されるときわめて危険である．これらの情報を保護するために，一般的に物理的なキーやパスワードが用いられているが，情報を参照するたびに煩雑な操作を行うことは面倒であり，パスワードを設定しない原因にもなっている．本論文では，小型携帯端末向けの認証手法として，端末の動きを用いた手軽かつ高精度の個人認証を可能とする 3D 動作認証手法を提案する．

†1 静岡大学工学部
Faculty of Engineering, Shizuoka University
†2 静岡大学大学院情報学研究科
Graduate School of Information, Shizuoka University
†3 ソニー株式会社
Sony Corporation
†4 静岡大学情報学部
Faculty of Information, Shizuoka University
☆ 現在，ブラザー工業株式会社
Presently with Brother Industries, Ltd.

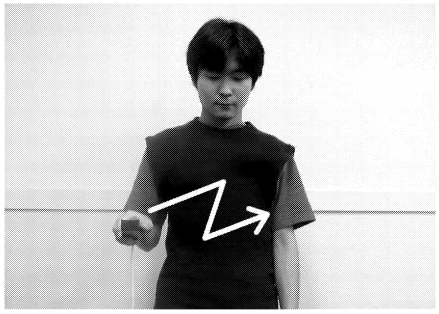

図 1 3D 動作認証のイメージ
Fig. 1 Image of 3D motion authentication.

3D 動作認証では，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することによって認証を行う．たとえば，端末を動かす速度や，タイミング，手首のひねりなどを特徴としてとらえ，認証処理に利用する．この考え方は，文字形状や筆圧などから個人特徴を抽出するオンライン署名認証[1),2)] に類似しているが，携帯端末の動きを用いる 3D 動作認証は，認証時にタブレットなどの特別な入力インタフェースを必要としない．したがって，3D 動作認証を，外部に複数の入力インタフェースを配置することが困難な腕時計型情報端末などの超小型端末に適用し，これら本体の認証に利用したり，これらの端末を外部機器の認証用装置として利用したりすることも可能である．また，3D 動作認証では，筆跡認証のようにペンを使ったり，携帯電話をペンやマウスのように持って動かしたりするのではなく，普段と同じ持ち方で認証動作を行うことができる．さらに，携帯端末に登録する動きは紙に書く筆跡のように跡が残ることがなく，ユーザが随時変更できるため他人に知られたり，正確に再現できたりする可能性が低いため，成りすましの危険が低いと考えられる．

本研究では，3D 動作認証の 1 つの形態として，3 軸加速度センサを搭載した小型の動作計測用端末を作成し，DP マッチング[3),4)] による動作照合機能を実装した．また，閾値の決定および，動作の経年変化に対応するための認証判定パラメータ自動設定機構を設計し，実機を用いた実験により本手法の有用性に関する基礎的評価を行った．

以下，2 章で 3D 動作認証の特徴を述べ，3 章で認証判定までの手順と，認証判定パラメータの自動設定手法について説明する．4 章で実機による本手法の有用性を確かめるための実験について述べ，5 章でその結果を基に検討を行う．最後に，6 章でまとめとする．

2. 3D 動作認証の特徴

3D 動作認証では，携帯端末の動きを個人認証に利用するため，認証時にペンや指紋読み取り装置のような特殊な入力インタフェースを必要としない．従来のパスワードによる認証のように，端末に配置された小さなボタンを何度も押す必要がなく，ユーザは携帯端末を空中で動かすだけで手軽に認証操作を行うことができる．

携帯端末向けの個人認証手法としては，**表 1** に示すように他にもいくつかの選択肢が考えられる．指紋や虹彩などの身体的特徴を用いたバイオメトリクス認証は，従来のパスワードや物理的キーによる認証に比べ，他人に不正利用される危険性が低い．しかし，これらの身体的特徴を用いた認証方式は，ユーザの心理的抵抗が強いという欠点がある．特に，指紋は容易に採取することが可能であり，採取されてしまった場合のトラブルに対処することが難しい．文献 6) では，ゼラチンにより作成したグミ製人工指が多くの指紋照合装置で受け入れられてしまうことが示されている．これに比べ，筆跡や声紋などの行動的特徴を用いたバイオメトリクス認証は，前者に比べ精度はやや落ちるが，ユーザへの受容性が高く，物理的コピーによる悪用の心配が少ない．3D 動作認証は，個人の行動的特徴を用いたバイオメトリクス認証の一種である．

オンライン筆跡認証では，タブレットなどの接触型の入力装置を使用するのが一般的[1),2)] だが，ビデオカメラを使った空中署名の研究も行われている[5)]．空中署名では，空中にサインを描く軌跡や速度が人により異なることを利用して個人認証を行う．

3D 動作認証もこれと同じ非接触型の認証方式の 1 つである．3D 動作認証では，内蔵の加速度センサを用いて動きを検出することで，空中署名で検出可能な端末の平行移動に加え，手首のひねりや回転などの動作も認証に用いることができる．これらの微妙な動きを肉眼でとらえることは難しく，たとえ他人に認証動作を見られたとしても，成りすましによって不正利用される危険性が低い．また，3D 動作認証では端末に内蔵されたセンサを用いるため，端末外部の機器を必要としない．これらの点で本論文で提案する 3D 動作認証は，携帯端末上の個人認証において，空中署名に比べて高い優位性を持つ．

声紋認証では追加で必要となるデバイスがマイクのみであり，特に携帯電話のように最初からマイクが搭載されている機器ではデバイスの追加が必要なく，組み込みが容易である．しかしながら，マイクを搭載し

表 1 認証方式の比較
Table 1 Comparison of authentication methods for portable devices.

		精度	コスト	盗難の危険性	精神的抵抗	外乱の影響	組み込みやすさ	必要デバイス
非バイオメトリクス	鍵，IC カード	高	低	高	低	低	中	鍵，カード
	パスワード	高	低	高	低	低	容易	入力用ボタン
バイオメトリクス（身体的特徴）	指紋	高	低	高	高	低	容易	指紋リーダ
	掌形	中	中	中	中	低	困難	カメラ
	虹彩	高	高	低	中	低	困難	虹彩リーダ
	顔	低	中	中	高	低	困難	カメラ
バイオメトリクス（行動的特徴）	筆跡	低	中	低	低	中	中	タブレット，ペン
	空中署名[5]	低	高	低	低	中	困難	カメラ，発光ペン
	声紋	低	低	低	低	高	中	マイク
	3D 動作認証	低	低	低	低	高	容易	加速度センサ

ていない機器へ適用する場合には，マイクを機器の表面に配置するためにフォームファクタ上の制限が生じる．一方，3D 動作認証では加速度センサを追加する必要があるが，そのサイズは十分に小さくかつ，配置先の制限が少ないため，比較的容易に携帯端末への組み込みが可能である．

3. 認証処理

3.1 認証処理の概要

以下，1 つの 3 軸加速度センサを利用して認証動作を計測することを前提として 3D 動作認証の認証処理手法について説明する．端末を利用しているユーザが正規のユーザであるかを確かめるには，システムにあらかじめ登録された本人の動作データと，認証時に計測された動作データの照合を行う．2 つの動作データの類似度が低い場合は，成りすましによる不正利用だと判定する．

登録された動作データと計測データの照合は，加速度の時系列データの DP マッチングによって行う．加速度センサの利用にあたっては，センサの出力に加わる外部振動などによるノイズの影響を少なくするために，加速度のピーク値の出現タイミングや，ゼロクロスタイミングのみを特徴量として利用する場合があるが，これらの値のみを利用すると，利用可能な情報量が少なくなり，高い認証精度が得られない可能性が高い．このため，本論文ではセンサから出力される加速度の値そのものを特徴量として利用することとした．

時系列データの照合手法としては，DP マッチング以外に，隠れマルコフモデル（HMM）が音声認識やジェスチャ認識などのアプリケーションで一般的に用いられている[7)~9)]．DP マッチングは，テンプレートマッチング法の一種で，時系列パターンを非線形伸縮しながら標準パターンとの比較照合を行う手法である．一方 HMM は確率モデルを用いたマッチング手法で，不特定者を対象にした場合に DP マッチングよりも高い認識精度が得られることが指摘されている．ただし HMM では，精度確保のために多量のデータ取得を必要とする．携帯端末へ登録されたユーザ個人の認証を行うという利用形態を考えると，HMM における不特定者を対象にした場合の優位性は重要ではない．また，認証パターンを登録するために多量のデータが必要となると，ユーザの利便性が低くなってしまう．この理由から本研究では DP マッチングを利用することとした．

加速度データのサンプリングは，ユーザの特定のアクション，たとえば認証が必要なドアの付近に立ったり，ボタンを押したりするなどの操作により開始される．データのサンプリングを開始してから，実際にユーザが認証動作を開始するまでの時間は毎回異なる．このため，ユーザが実際に認証を意図して端末を動かしている区間を検出する必要がある．そこで，認証動作の開始前と開始後に，一定時間その場に端末を静止させることで動作区間を検出することとした．なお，認証動作を行っている時間には毎回ばらつきがあるため，2 つのデータを照合するには，データ長の正規化などの処理が必要となる．

3.2 認証処理手順

認証処理の手順は次のとおりである．

(1) 加速度データのサンプリング
(2) 動作区間の抽出
(3) 加速度の正規化
(4) データ長の正規化
(5) データ間距離の算出

以下，それぞれの処理内容について述べる．

(1) 加速度データのサンプリング

携帯端末内の 3 軸加速度センサにより，ユーザの認

証動作の計測を行う．

(2) 動作区間の抽出

加速度データのサンプリングを開始してから，実際にユーザが認証動作を始めるまでの時間は毎回異なるため，ユーザが実際に認証を意図して端末を動かしている区間を検出する必要がある．そこで，加速度が急激に変化したときに認証動作の開始時刻を決定し，動作開始後に一定時間，加速度の変化がなかった時点で認証動作の終了時刻を決定することとした．この方式を用いることで，認証動作中にリアルタイムに動作開始時刻／終了時刻を検出することが可能となり，ユーザが認証動作を終了すると，システムは自動的に加速度のサンプリングを停止することができる．また，この仕組みによって，端末の無駄な電力消費を抑えることができる．特に小型の携帯端末は電池の持続時間が問題となるため，このような配慮が大切である．

次に動作区間抽出アルゴリズムの詳細を示す．

(1) 各軸の過去 T 時間の加速度サンプルの最大値と最小値の差 d_x，d_y，d_z を求める．**図 2** (a) は，X 軸における加速度変化の例を示している．

(2) a) 認証動作開始前の場合
$\sqrt{d_x^2+d_y^2+d_z^2}$ が閾値 E を上回った時点より P_{start} 時間前を動作開始時刻と見なす．

b) 認証動作開始後の場合
$\sqrt{d_x^2+d_y^2+d_z^2}$ が閾値 E を下回った時点より P_{end} 時間前を動作終了時刻と見なす（図 2 (b)）．

T を小さくしすぎると，認証動作中に端末を動かす速度が小さくなったときに，誤って認証動作が終了したと判断してしまう．逆に T を大きくしすぎると，動作終了点を検出するまでに時間がかかる．

E は，端末が静止状態にあるかを判別するための加速度の閾値である．E を小さくすると，わずかな動きでも端末を動かしていると判断する．

P_{start} と P_{end} は，動作区間の検出誤差を吸収するために設けた値である．

動作を登録したユーザが正確に登録した動作を再現したとしても，動作区間の検出の精度によってはこれらが同じデータとして切り出されない恐れがある．しかし，本節で示したアルゴリズムでは，加速度の大きさが閾値以上となる前後に P_{start}，P_{end} の時間的余裕を設けているため，実際に検出される加速度の時系列データの冒頭と末尾には 0 に近い値が連続することになる．DP マッチングによる加速度時系列データのマッチング時には，実際の動作開始前後の 0 に近い加速度値に合わせて時間軸上のずれが吸収されるので，加速度の閾値検出時刻のずれがあっても，認証精度への影響は少なくなる．

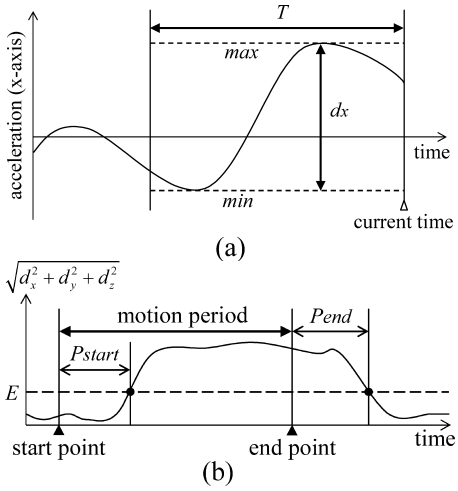

図 2 動作区間抽出アルゴリズム
Fig. 2 Algorithm of motion period identification.

(3) 加速度の正規化

ユーザが前回と同じ動作を意図して認証動作を行ったとしても，端末を動かす速度が異なると，加速度の振幅量が変化するため，別の動作だと見なされてしまう可能性が高い．そこで，加速度の絶対値の最大値が 1 になるように加速度の正規化を行い，このような相対的な速度差を吸収する．

携帯端末の持ち方が違うと，加速度センサが検出する加速度が変わるので，認証精度に大きな影響が出ると予想される．しかしながら，端末の持ち方も個人の特徴であると解釈するならば，認証アルゴリズムによって端末の持ち方の違いを吸収してしまうよりも，違いをそのまま利用する方が成りすまし成功率を小さくすることが可能である．この見地から，本研究では，端末の持ち方に関する補正は行っていない．

(4) データ長の正規化

長さの異なる 2 つの加速度データを比較するための前処理として，データ長の正規化を行う．ここでは，自然 3 次スプライン補間を用いて，観測データのサンプル系列から，照合対象となるマスタデータのサンプル数と同じ数のデータを生成することとした．

(5) データ間距離の算出

正規化後の観測データを，システムに登録されている本人のマスタデータとマッチングする．求められたデータ間距離が，設定された閾値よりも低ければ登録者本人の動作であると判断する．マスタデータと観測データの照合には DP マッチングを用いる．DP マッ

チングの距離尺度には加速度ベクトル間のユークリッド距離を用いる．時系列データ A の i 番目の x 軸加速度を $\ddot{x}_A(i)$ と表した場合，時系列データ A の i 番目の加速度ベクトルと，時系列データ B の j 番目の加速度ベクトル間のユークリッド距離 $d(i,j)$ は次のようになる．

$$d(i,j) = \sqrt{d_x^2(i,j) + d_y^2(i,j) + d_z^2(i,j)} \quad (1)$$
$$d_x(i,j) = \ddot{x}_A(i) - \ddot{x}_B(j) \quad (2)$$
$$d_y(i,j) = \ddot{y}_A(i) - \ddot{y}_B(j) \quad (3)$$
$$d_z(i,j) = \ddot{z}_A(i) - \ddot{z}_B(j) \quad (4)$$

このとき，時系列データ A と B の DP マッチング距離 $D(A,B)$ は次の漸化式で求められる．

$$Initialize: \quad g(1,1) = 2d(1,1) \quad (5)$$
$$For\ i = 1\ to\ I,\ j = 1\ to\ J$$
$$g(i,j) = \min \begin{bmatrix} g(i-1,j) + d(i,j) \\ g(i-1,j-1) + 2d(i,j) \\ g(i,j-1) + d(i,j) \end{bmatrix} \quad (6)$$
$$D(A,B) = \frac{g(I,J)}{I+J} \quad (7)$$

ここで，I と J はそれぞれ，時系列データ A と B のサンプル数である．4 章で述べる実験に用いた実装では，本人のわずかな動作速度のずれのみを許容するために，整合窓幅の半径を 50＋(マスタデータ長/20) としている．

3.3 認証判定パラメータの自動設定

3.3.1 初期マスタデータと初期閾値の決定

手書き文字と同様に，3 次元空間における動作には毎回バラツキがあり，動作の再現に失敗することがあるため，複数の動作データの中からユーザの動きを最もよく反映しているものをマスタデータとして採用するのが望ましい．また，ユーザが登録する認証動作は多種多様であり，最適な認証判定用の閾値が動作パターンごとに異なると考えられる．オンライン筆跡認証では，署名者に依存した閾値を別々に設けることにより，認証精度を数%改善できるという報告がある[10]．そこで，最初に認証動作を登録する際に，同じ動作を複数回入力し，そのデータをもとに認証判定用のマスタデータと閾値を決定することにした．次に，初期マスタデータと初期閾値の決定手順を示す．

(1) 初期データの登録 ユーザが N 回認証動作を登録する．これらの動作データは有効動作履歴としてシステムに保持される．i 番目に登録された動作データを $M_i(i = 1,2,\cdots,N)$ と表す．

(2) マスタデータの決定 動作データ M_i と $M_j(j = 1,2,\cdots,N)$ の DP マッチング距離を D_{ij} とする．M_i と有効動作履歴中の各動作データとの DP マッチング距離の二乗和 $(\sum_{j=1}^{N} D_{ij}^2 (i \neq j))$ を求め，この値を最小にする M_i をマスタデータとする．

(3) 無効動作の除去 ユーザがまだ認証動作に慣れていない場合，(1) での動作登録時に不安定な動作が登録されてしまうことがある．このような動作データが有効動作履歴として保持されると，後の認証判定に悪影響を及ぼす恐れがある．そこで，この不安定な動作データを無効動作として有効動作履歴から削除する．有効動作履歴中の各動作データとマスタデータとの DP マッチング距離 D_i を求め，これらの中央値を D_m とおく．$D_i > bD_m$ となる動作データ M_i を無効動作とし，有効動作履歴から削除する．b は $b > 0$ となる定数である．

(4) 閾値の決定 D_i の平均値 μ と，D_i の標準偏差 σ を求め，$\mu + a\sigma$ を D_i に対する閾値とする．a $(a > 0)$ は閾値制御のためのパラメータである．すなわち，マスタデータと認証判定対象データの距離 D に対して，$D < \mu + a\sigma$ のとき，この認証判定対象データを認証成功と判定する．ユーザが認証動作に慣れて動作が安定しているほど，閾値はより低く設定される．

3.3.2 マスタデータと閾値の自動更新

認証時に計測された動作データは，システムにあらかじめ登録されている本人のマスタデータと照合される．マスタデータを登録して間もない時期に正常な認証判定ができたとしても，時間の経過とともにユーザの動作は少しずつ変化し，正常な認証判定ができなくなると予想される．オンライン筆跡認証の場合，9 週間マスタデータを更新しないと，認証精度が約 50%低下するという報告がある[11]．3D 動作認証の場合，ユーザが行った動作が筆跡という目に見える形で残らず，自分自身の動作の微妙な変化をとらえることが難しいため，経年変化の影響がより顕著に現れると考えられる．そこで，ユーザの認証が成功するごとに，マスタデータと閾値を更新して動作の経年変化に対応することにした．更新手順は以下のとおりである．

(1) 有効動作履歴の更新 認証に成功した動作データを有効動作履歴に追加登録する．登録されているデータ数が有効動作履歴最大数 $H_{\max}$ を超える場合は，履歴中の最も古い動作データを削除する．

(2) マスタデータの更新 3.3.1 項 (2) と同様に，有効動作履歴として登録されている動作データからマスタデータを選出する．

(3) 閾値の更新 3.3.1 項 (4) と同様に，有効動作履歴から閾値を再計算する．ユーザの動作が安定し

図 3 実験用端末の外観
Fig. 3 Device used in experiments.

表 2 実験端末仕様
Table 2 Spec of a device for experiments.

サイズ	13 × 4 × 2.5 cm
重量	68.5 g
加速度センサ	MA3-04 c（MicroStone 社製）
加速度検出軸数	3 軸
加速度検出範囲	−4〜4 G（重力測定不可）
サンプリングレート	200 Hz

表 3 解析用 PC の仕様
Table 3 Spec of PC for data analysis.

CPU	Pentium 4 2.00 GHz
RAM	512 MB
OS	Windows XP Professional

てくると，閾値は今までより低い値に更新されるため，成りすまし成功率を下げることができる．

4. 評価実験

提案手法の有効性を検証するため，加速度センサを内蔵した実験用の端末を利用した実験を行った．まず，11 人の動作登録者に対する 1 カ月間の継続的な動作データの測定を行い，経年変化への追従性を確かめた．さらに，動作登録者以外の 27 人による成りすまし実験を行い，提案手法の成りすましに対する耐性，ならびに本手法に適した動作について調べた．

4.1 実験環境

実験では形状および重量を現行の携帯電話と同等となるようにしたデータ取得用の端末を作成した．実験用端末の外観，仕様を**図 3**，**表 2** に示す．実験用端末は加速度センサとその補助回路のみを搭載しており，信号をシリアルケーブルを通して PC に送信する．データの解析はすべて PC 側で行った．データ解析用 PC の仕様を**表 3** に示す．また，**表 4** に 3.2 節で述べた動作区間抽出パラメータ，および 3.3.2 項で述べたマスタデータと閾値の自動更新パラメータを示す．

すべての測定は無風の室内で行った．各被験者には立位で，静止した状態で認証動作を行ってもらった．また，ノイズの影響を抑えるため，認証動作を行う際には，実験端末と解析 PC を接続するシリアルケーブルが他のものと当たらないよう各被験者に口頭で注意を促した．

4.2 実験方法

4.2.1 本人の認証動作の追跡実験

21 歳から 25 歳の大学生・大学院生男女からなる被験者 11 人にシステムへ認証動作を登録してもらい，1 日に 3 回，週 5 日の頻度で 1 カ月間その動作を行ってもらった．動作の初期登録時，初期マスタデータ・

表 4 実験に使用したパラメータ
Table 4 Parameters used in experiments.

パラメータ		値
T	（動作計測時間）	500 msec
E	（停止判定閾値）	1 G
P_{start}	（動作開始時刻誤差）	100 msec
P_{end}	（動作終了時刻誤差）	400 msec
b	（無効動作除去パラメータ）	2.0
a	（閾値制御用パラメータ）	1.5
$H_{\max}$	（有効動作履歴最大数）	10

閾値を決定する必要がある．そのため，被験者に十分に（各被験者 10 回以上）動作の練習を行ってもらってから，データ初期登録のために 10 回動作を行ってもらった．

被験者が提案手法に早く馴染むことができるように，認証動作は，筆記で書き慣れた自分の名前を空中で描く動作のみにした．具体的には，自分の苗字もしくは下の名前を，漢字もしくは平仮名で空中で描くパターンである．また，被験者には自分の名前を空中で書いているイメージで動作を行うようにしてもらった．動作の長さに関しては特に制限を設けなかった．なお，被験者は全員右利きである．

この実験では，初期登録時を含め，動作のデータ測定時には認証判定の成否，およびマスタデータと認証動作間の DP マッチング距離を被験者に伝えていない．これは，これらの実験で得られた同一データからマスタデータの更新時，非更新時の両者の場合の認証精度を確認することを意図したためである．このようなフィードバックを与えようとすると，更新版，非更新版のいずれかのマスタデータに基づいてフィードバックする値を決定する必要があるが，更新版，非更新版の比較をする以上，これらのいずれかのみをフィードバック時に使用することは避けられるべきである．

システム側からユーザの認証動作の良否に対する情

表 5 実験結果
Table 5 Experiment results.

	Transition of FRR				FRR		成りすまし成功率		加速度 [G]						動作長	
	(非更新)		(更新)		(全体)		(全体)		標準偏差			ダイナミックレンジ			[sec]	動きの傾向
User	First 3 days	Last 3 days	First 3 days	Last 3 days	No update	Update	No update	Update	x	y	z	x	y	z		
1	0.44	0.66	0.22	0.11	0.57	0.09	0.08	0.00	0.87	0.47	1.70	6.41	3.55	7.88	2.97	腕全体
2	0.00	0.11	0.11	0.11	0.05	0.10	0.00	0.03	1.49	0.40	1.09	7.90	2.06	6.93	2.34	腕全体
3	0.00	0.22	0.00	0.00	0.13	0.00	0.00	0.00	1.05	0.37	1.36	6.79	2.29	7.33	3.89	腕全体
4	0.44	0.44	0.22	0.11	0.43	0.10	0.00	0.00	1.33	0.65	1.33	7.53	3.56	7.33	1.72	腕全体
5	0.66	0.00	0.11	0.00	0.00	0.00	0.18	0.06	1.14	0.42	1.29	6.80	2.23	7.36	3.05	腕全体
6	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	1.34	0.45	1.51	7.60	2.60	7.74	3.06	手首のみ
7	0.00	0.00	0.00	0.00	0.00	0.04	0.42	0.30	0.75	0.20	0.60	4.28	1.20	3.59	3.32	手首のみ
8	0.00	0.00	0.00	0.00	0.00	0.00	0.29	0.10	0.78	0.25	0.96	4.98	1.55	5.49	3.37	手首のみ
9	0.00	0.00	0.00	0.00	0.00	0.00	0.98	0.17	0.66	0.18	0.73	3.55	1.01	3.87	4.32	腕全体
10	0.22	0.55	0.22	0.33	0.39	0.17	0.00	0.05	1.08	0.43	1.18	6.17	2.57	6.74	2.83	腕全体
11	0.00	0.22	0.00	0.22	0.08	0.04	0.00	0.13	1.14	0.56	1.51	6.98	3.55	7.64	4.52	腕全体
Average	0.16	0.2	0.08	0.08	0.15	0.05	0.18	0.08	1.06	0.40	1.20	6.27	2.38	6.54	3.22	
Average (User 1–6)	0.26	0.24	0.11	0.06	0.20	0.05	0.05	0.01	1.20	0.46	1.38	7.17	2.71	7.43	2.94	

報が得られないと，ユーザや登録した動作によっては，1 カ月の間に，初期の登録動作からかけ離れた動作を行うようになったり，動作が収束しなかったりすることも予想される．このため，このフィードバックを行わないという条件は認証手法の精度を正確に評価するという観点からは理想的とはいえないものである．しかし，特にユーザの動作を強制する指示を行わない条件下で，ユーザが同一動作を維持できるかどうかを判別することができるため，本手法の実運用に対する適性の基礎的な評価には適当であると考える．

4.2.2 成りすまし実験

27 人の被験者に前述の 11 人のマスタデータ登録者の動作を真似してもらった．被験者は全員右利きである．成りすましを行う被験者には，成りすまし対象の動作が正面から映っているビデオ，およびそれぞれの動作が空中でどんな字を描いているものかを示した図を被験者が納得するまで見せた．この間，被験者には動作の練習を認めている．これらの過程の後，被験者が自分で成りすましが可能と判断した直後に，成りすましの動作を各動作に対して 4 回ずつ行ってもらった．なお，図による動作の掲示を省いた場合の成りすまし試行に対しては測定を行っていないが，ビデオを一見しただけで動作を納得できた被験者は，見られなかった．

5. 実験結果と検討

以降の説明では，3.3.2 項で述べた手法に従って，マスタデータ・閾値を更新したデータを用いた場合に得られた結果を更新版と呼び，逆に更新させなかった場合の結果を非更新版と呼ぶこととする．

5.1 実験結果

表 5 に全被験者の更新・非更新版の実験開始後 3 日間と実験終了前の 3 日間における FRR（False Rejection Rate：本人拒否率），実験期間を通じての更新・非更新版の FRR と成りすまし成功率（意図的な成りすましユーザに対する FAR（False Acceptance Rate：他人許容率））を示す．更新版の FRR は，操作時における最新の更新済みマスタデータおよび判定用閾値に対する認証の成否をもとに計算した．また，更新版の成りすまし成功率は，1 カ月間の各被験者の動作測定値をもとに各認証動作終了時のマスタデータおよび判定用の閾値を計算し，これらの値に基づいて認証の成否を判定することにより計算した．

表 5 には，さらに初期マスタデータにおける各軸の加速度の標準偏差，各軸の加速度のダイナミックレンジ，初期とマスタデータの動作の長さ，認証動作を行ったときの実験端末の動かし方の傾向を示している．なお，これらのうち加速度に関するデータは正規化を行う前の値である．

5.2 認証精度

1 カ月の本人動作の追跡実験後の平均 FRR はマスタデータおよび判定用閾値の更新を行った場合に平均 5%となった．また，こうして得られたマスタデータと判定用閾値を使ったときの成りすまし成功率は平均 8%となった．

詳細については後述するが，被験者 11 人中，登録動作自体に問題がある被験者 2 人（7，8，9），動作習熟過程で動作が収束しない被験者 2 人（10，11）が認められた．これらを除けば，FRR と成りすまし成功率の最大値はそれぞれ 10%，6%であり，平均ではそれぞれ 5%，1%となった．うち 2 人の被験者では，FRR，成りすまし成功率はいずれも 0%となった．ただし，今回の実験では，FRR に関しては，それぞれ試行回数が 66 回前後であり，精度は 1.5% である．また成りすまし成功率に関しては，1 つの成りすまし対象の動作に対して，27 人の被験者が 4 回ずつ動作を

表 6 認証精度の比較
Table 6 Comparison of accuracy of authentication.

認証技術	本人拒否率（FRR）[%以下]	他人受入率（FAR）[%以下]
指紋認証（光学式）	0.01	0.001
指紋認証（真皮検出半導体式）	0.001	0.0001
静脈認証	0.1	0.00001
顔認証	1	0.1
虹彩	0.0001	0.0001
オンライン署名認証	0.2	0.6

行ったため，精度は 0.93% である．

表 6 に代表的なバイオメトリクス認証手法における FRR と他人受け入れ率（FAR) の水準を示す．この表から分かるように，提案手法における FRR および成りすまし成功率は，他の手法と比べて大きい．特に，本方式と同じくユーザの意志を持った動作を認証に用いるオンライン署名認証と比べても，FRR に関して 10 倍以上の差がある．FAR に関しては，登録動作に問題があるとされる被験者の分を排除しても 2 倍近い差がある．

ただし，今回の成りすましの実験では，成りすましを行う被験者に真似をする動作パターンを紙面で見せ，さらにその動作のビデオを被験者が納得するまで見てから成りすましを行ってもらっている．このためにあえて FAR という一般的な用語を使わず，成りすまし成功率という言葉を本論文では使用している．実際の利用環境を想定した場合，動作パターンは見ただけでは何を書いているのかを判断するのが難しく，さらに，他人の動作をじっくり見る機会も少ないと考える．今回の実験では，成りすまし被験者が図示された動作を見ない限りどのような動作をしているかが理解できなかったこと，成りすましを行う側にきわめて有利な実験条件を鑑みると，今回得られた 2 人の被験者の 1% という成りすまし成功率は十分に実用的な範囲にあると見なしてよいと考える．しかしながら，FRR が大きい問題は依然として残る．これには，成りすまし成功率の実質的小ささを考慮しながら認証用パラメータを甘めに設定する，経年変化への対応アルゴリズムの改善，認証登録時に不適な動作を排除するなどの対策が必要になろう．

以下，認証精度について詳しく検討する．

5.2.1 経年変化への対応

図 4，**図 5** に，それぞれ実験の最初の 3 日間と最後の 3 日間における，各被験者の非更新版と更新版の FRR の変化を示す．図 4 の非更新版グラフを見ると，

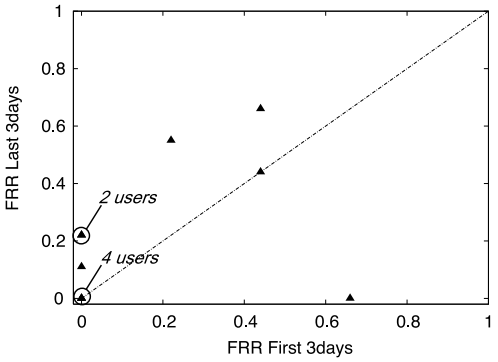

図 4 FRR の変化（非更新版）
Fig. 4 Transition of FRR (without parameter update).

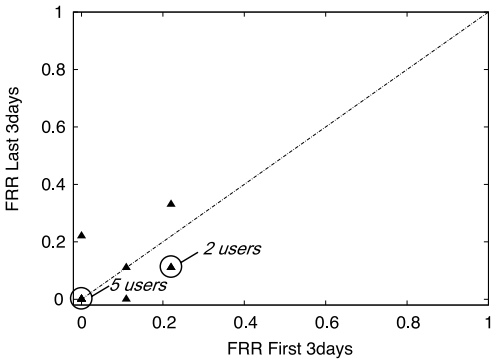

図 5 FRR の変化（更新版）
Fig. 5 Transition of FRR (with parameter update).

認証判定に初期マスタデータ・閾値を使い続けるため，被験者 11 人中 5 人の FRR が悪化していることが分かる．これに対し，図 5 に示す更新版では，FRR の悪化があったのは 2 人の被験者（10，11）のみであった．

5.2.2 成りすましに対する耐性

図 6 に，各動作登録者における更新版・非更新版の成りすまし成功率の変化を示す．マスタデータと判定用閾値の更新により，被験者 11 人中，6 人に成りすまし成功率の改善が見られた．特に，初期の成りすまし成功率が大きかった被験者 7，8，9 に効果が顕著に見られる（表 5)．

成りすましに対する耐性の高い動作の特徴を調べるため，初期マスタデータの加速度と動作の長さの 2 つの観点から検討する．

図 7 に，被験者ごとの各軸の加速度のダイナミックレンジのうち最大の値と更新版の成りすまし成功率および FRR の相関を示す．この図より，加速度のダイナミックレンジが小さいと成りすまし成功率が大きくなり，成りすましが容易になっていることが分かる．つまり，動作が緩慢な動作は 3D 動作認証に適さない．

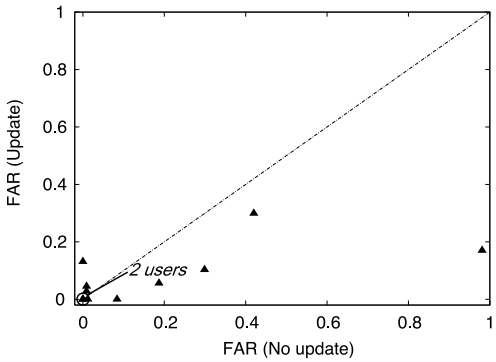

図 6 パラメータの更新による成りすまし成功率の変化
Fig. 6 Transition of FAR for vicious attackers with update of parameters.

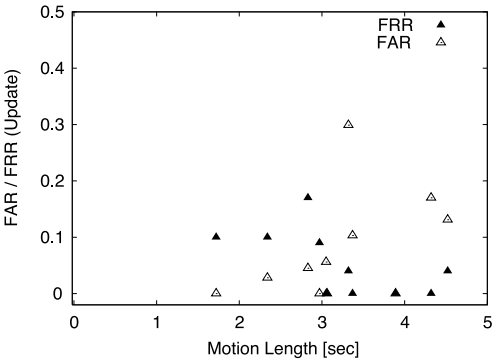

図 8 初期マスタデータの長さと FRR，成りすまし成功率の相関
Fig. 8 Correlation between initial master data and FRR, FAR for vicious attackers.

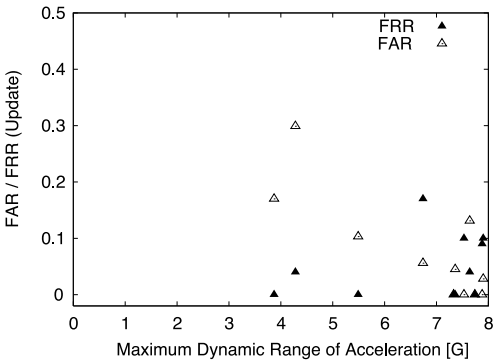

図 7 加速度のダイナミックレンジの最大値と更新版 FRR，成りすまし成功率の相関
Fig. 7 Colleration of FRR / FAR for vicious attackers with parameter update and maximum value of dynamic range of each axis.

成りすまし成功率が特に大きい被験者 7，8，9 はこの条件に該当する．また，これらの被験者は各軸の加速度の標準偏差も小さかった（表 5）．特に，被験者 7，8 は端末を手首のみで動かしており，十分に大きな加速度を端末に与えにくかったと推測される．なお，FRR と加速度のダイナミックレンジに関しては今回の実験に関する限り，相関は見られなかった．

図 8 に，被験者の初期マスタデータの長さと成りすまし成功率，および FRR との相関を示す．この図より，マスタデータが長いほど FRR が向上する一方で，成りすまし成功率が悪化していることが分かる．このような相関が得られるのは，マスタデータが長いほど，認証対象のデータとの DP マッチング距離が総じて大きくなり，DP マッチング距離の標準偏差によって決められる判定用の閾値が大きくなるためである．生体認証においては，FRR，成りすまし成功率いずれもが低いことが要求される．今回実験した条件では，両者の増加曲線が動作の長さ 3 秒付近で交わっており，この程度の長さの操作が適当と考えられる．

以上の検討より，成りすましに対する耐性の高い動作の条件は，

- 加速度の変化，絶対値がいずれも大きい，
- 動作時間は 3 秒程度，

とまとめることができる．これらの条件に適合するように，初期のマスタデータの登録時にシステムが許容する動作を制限することにより，実用的な成りすまし耐性が得られると期待できる．

5.2.3 パラメータ更新が効果的に働かない場合

表 5 を見ると，被験者 10，11 は，更新版において成りすまし成功率が悪化している．さらに，この両被験者は，表 5 を見ると分かるように，更新版・非更新いずれにおいても測定実験初期と比べて実験終盤で FRR が増加している．これは登録者本人が最初に登録した動作を再現できなくなっていることを意味している．特に，被験者 11 はマスタデータが他の被験者に比べて長い．これが本人の動作のばらつきを招いていると考えられる．この結果，パラメータの更新をしていた場合，実験終盤では入力動作のばらつきが大きいために，認証の成功判定のための閾値が大きくなり，成りすましに対する耐性の悪化を招いている．

ユーザの動作のばらつきの一因として，今回の測定では被験者に認証の成否および DP マッチング距離をフィードバックしていないことが考えられる．通常の使用においては，最低限利用者には認証の成否が分かるので，動作登録者本人は動作を改善するよう意識することが予想される．このような場合，動作登録者本人による動作のばらつきが抑制され，パラメータの更新を行うことによって FRR が改善されると推測される．

5.3 処理速度

PC を用いた実験環境においては，認証処理自体にかかる時間が 0.12 秒，10 個の動作履歴をもとにマスタデータを更新する処理に関しては 0.80 秒を要した．マスタデータの更新処理は，過去に比較した動作履歴間の DP マッチング距離を保存しておくことで，その処理時間を履歴長 L に対し $O(L)$ で実行できる．また，認証操作 1 回あたりにセンサから送信されるデータは，今回の実験で用いた認証動作では，最大 4,000 バイト程度である．

これらの値は，PC 上での処理を行うには十分に実用的な値である．しかしながら，携帯電話や PDA などの携帯端末で用いると，処理時間は大幅に大きくなると考えられる．最新の PDA でのプロセッサの動作クロックが数百 MHz であることを考えると，処理時間は PC 上の数十倍となると考えられる．これより携帯端末での認証処理時間は数秒から十数秒程度，有効動作履歴の更新には数十秒を要すると推測できる．携帯端末での実用にあたっては，有効動作履歴上で保持するデータ数の削減，サンプリングレートの削減，マスタデータの長さの制限などのチューニングを行い，処理時間および必要メモリサイズの削減を行う必要がある．

6. まとめ

携帯端末向けの簡便な個人認証手法として，端末の動きを用いた 3D 動作認証と，その認証判定用パラメータの自動設定機構，経年変化への追従機構を提案した．また，実機と 11 人の動作登録者および 27 人の成りすまし被験者による実験により有用性の基礎評価を行った．

実験の結果，正規ユーザ本人に認証動作の良否を通知しない状態で 1 カ月間にわたって動作を行った場合，FRR を 10%以下にできることが確かめられた．また，登録した認証動作の大まかな軌跡とその軌跡の表す意味を被験者に提示し，その動作のビデオと書面による説明および練習後に成りすましを試みるという，成りすましを受ける側に不利な条件下で，成りすまし成功率を 5%以下とすることが可能であることが確かめられた．なお，ビデオを一見しただけで動作を納得できた被験者は，見られなかった．被験者の登録した動作パターンによっては FRR を 1.5%未満，成りすまし成功率を 1%未満にまで抑えることができた．これら良好な登録動作に共通する特性として，各軸の加速度の大きさおよびその変化がいずれも大きいことが確かめられた．このような特性を持つ動作のみを認証システムに登録可能とすることで，認証精度の向上が期待できる．

今回の実験では，認証用動作に名前の筆記操作を用いたが，本手法による認証に適した操作は筆記操作に限らないと考える．認証用の動作としては，より短く簡単な動作でかつ，個人の身体上の特徴や習癖を反映して高い認証精度が得られるようなものが望ましい．個人の習癖が出るような動作としては，指揮棒を振るような動作，ゴルフや野球などのスイングなどが考えられる．また，簡単な動作として日常的な携帯電話に出る動作などが考えられる．今後多量のサンプルに基づく実験を行い，個人の習癖が多く含まれるような動き，およびその特徴を明らかにしたい．

なお，本論文における実験はすべて振動のない安定した場所でユーザが静止し，動作登録時と同じ姿勢で動作を行っている．しかし，電車や自動車などの乗車時の利用，歩行時の利用など，実利用条件を想定すると，加速度センサにユーザの意図しない加速度が多く加わることが予想される．このような場合には，本論文で提案した動作区間の切り出し，DP マッチングによる加速度データの照合が必ずしも正常に機能する保証はない．今後様々な条件での本方式の有効性の検証ならびに改善手法の検討を行う必要がある．

参考文献

1) Cyber-SIGN. http://www.cybersign.com/
2) 西村広光，堤　正義：筆圧情報を含むオンライン文字情報を利用したオフライン文字認識性能の向上，電子情報通信学会技術研究報告，PRMU, Vol.102, No.55, pp.45–50 (2002).
3) Zhao, P., Higashi, A. and Sato, Y.: On-Line Signature Verification by Adaptively Weighted DP Matching, *IEICE Trans. Information and Systems*, Vol.E79-D, No.5, pp.535–541 (1996).
4) Rhee, E.J., Kim, T.K. and Nakajima, M.: On-line Recognition of Cursive Hangul by DP Matching with Structural Information, *IEICE Trans. Information and Systems*, Vol.E78-D, No.8, pp.1065–1073 (1995).
5) 片桐雅二，杉村利明：空中署名画像を使った移動環境に適する個人認証，映像情報メディア学会技術報告，Vol.25, No.85, pp.59–64 (2001).
6) 遠藤由紀子，平林昌志，松本　勉：指紋照合装置は人工指を受け入れるか（その 5），情報処理学会研究報告，DPS, Vol.2003, No.18, pp.251–256 (2003).
7) Gales, M.J.F., Knill, K.M. and Young, S.J.: State-based Gaussian Selection in Large Vocabulary Continuous Speech Recognition Us-

ing HMMs, *IEEE Trans. Speech and Audio Processing*, Vol.7, No.2, pp.152–161 (1999).
8) Nakagawa, S.: A Survey on Automatic Speech Recognition, *IEICE Trans. Information and Systems*, Vol.E85-D, No.3, pp.465–486 (2002).
9) Yoon, H.-S., Soh, J., Min, B.-W. and Yang, H.S.: Recognition of Alphabetical Hand Gestures using Hidden Markov Model, *IEICE Trans. Fundamentals of Electonics, Communications and Computer Sciences*, Vol.E82-A, No.7, pp.1358–1366 (1999).
10) Griess, F.D.: Project Report: On-line Signature Verification (2000).
11) Yamanaka, S., Kawamoto, M., Hamamoto, T. and Hangai, S.: Signature Verification Adapting to Intersession Variability, *IEEE ICME2001* (2001).

(平成 17 年 3 月 31 日受付)
(平成 17 年 10 月 11 日採録)

石原　進（正会員）

昭和 47 年生．平成 6 年名古屋大学工学部電気学科卒業．平成 11 年同大学大学院工学研究科博士後期課程修了．平成 10 年日本学術振興会特別研究員．平成 11 年静岡大学情報学部助手．平成 13 年より同大学工学部助教授．博士（工学）．平成 9 年電気通信普及財団テレコムシステム技術学生賞受賞．モバイルコンピューティング，無線環境用 TCP/IP，アドホックネットワークに関する研究に従事．電子情報通信学会，IEEE，ACM 各会員．

太田　雅敏

昭和 54 年生．平成 14 年静岡大学情報学部情報科学科卒業．平成 16 年同大学大学院情報学研究科修士課程修了．同年ソニー（株）入社．CE 機器関連のアプリケーション開発に従事．

行方エリキ

昭和 55 年生．平成 15 年静岡大学情報学部情報科学科卒業．平成 17 年同大学大学院情報学研究科修士課程修了．同年ブラザー工業（株）入社．工作機械の開発に従事．

水野　忠則（フェロー）

昭和 20 年生．昭和 43 年名古屋工業大学経営工学科卒業．同年三菱電機（株）入社．平成 5 年静岡大学工学部情報知識工学科教授，現在，情報学部情報科学科教授．工学博士．情報ネットワーク，モバイルコンピューティング，放送コンピューティングに関する研究に従事．著訳書としては『コンピュータネットワーク概論』（日経 BP），『モダンオペレーティングシステム』（ピアソン・エデュケーション）等がある．電子情報通信学会，IEEE，ACM 各会員．当会フェロー，監事．