PIN 入力タッチスクリーンバイオメトリクスにおける識別手法の影響

泉 将之[1]　西村 友佑[2]　柏木 まもる[3]　佐村 敏治[4]　西村 治彦[5]

概要：本研究ではスマートフォンを用いた PIN 入力タッチスクリーンバイオメトリクスについて検討を行なった．従来のキーストローク認証では得られなかったセンサやタッチスクリーンからの情報を利用した新たな特徴量を導入することにより認証精度の向上を図った．識別手法には統計的手法である Euclidean Distance（ED）法，Manhattan Distance（MD）法を，機械学習手法である Support Vector Machine（SVM），Back Propagation Neural Networks（BPNN），Learning Vector Quantization（LVQ）を用いる．21 名の被験者を対象に PIN 入力データを収集，解析を行い，特徴量の組み合わせによる認証率及びそのプロファイル数依存性について実験を行った．その結果，統計的手法では PIN4 桁において EER~ 6.7 %，PIN10 桁において EER~ 3.3 %，機械学習手法では EER~ 6.8–7.0 %，PIN10 桁において EER ~ 2.2–3.5 %という結果を得た．

Influence of Identification Methods by Touch-screen Biometrics for PIN Input

Izumi Masayuki[1]　Nishimura Yusuke[2]　Kashiwagi Mamoru[3]　Samura Toshiharu[4]　Nishimura Haruhiko[5]

1. はじめに

現在，スマートフォンの利用者は年々増加しており，それに伴い不正利用や情報漏洩の危険性も増大しつつある．従来のスマートフォンのセキュリティとして PIN（Personal Identification Number）入力（**図 1** 左）やパターン入力（図 1 右），パスワード入力などによる認証システムがあげられる．しかし，これらは総当たり攻撃やショルダーハッキング，画面に残った皮脂をなぞるなどの方法で比較的容易になりすましが可能である．一方で指紋認証を搭載したスマートフォン端末も登場しているが，複製された指紋によりなりすましができることが報告されている [1].

その対策の 1 つとして，PIN 入力やパスワード入力に対するキーストローク認証が注目されている．キーストローク認証は，主に PC のキーボードにおいて文字入力時のパターンを利用したバイオメトリクスである [2]．PIN 入力認証時のキーストロークデータによる認証の研究は 1980 年頃から行われていた [3]．PIN の照会とキーストローク認証を組み合わせることでより強固な認証システムを構築

図 1　スマートフォンで用いられる認証システム（左）: PIN ロック，（右）: パターンロック

Fig. 1　User authentication system on smartphone. (left): PIN lock, (right): pattern lock

[1] 明石工業高等専門学校 専攻科
Advanced Course, Akashi National College of Technology
[2] 大阪大学 基礎工学部
School of Engineering Science, Osaka University
[3] NTT スマートコネクト
NTT SmartConnect Corporation
[4] 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
[5] 兵庫県立大学 応用情報科学研究科
Graduate School of Applied Informatics, University of Hyogo

することが可能となるが，PC のキーボードにおけるキーストローク認証ではキーの押離時間のみしか特徴量にならない．

本研究ではスマートフォンを対象とした PIN 入力時のキーストローク認証を扱う．しかし，キーストロークとはキーボードのキー押下時にキーが押し込まれる深さのことであり，これをキーストロークと呼ぶことは適切ではないかもしれない．そこで本論文では，タッチスクリーンに対するキー入力による認証方法をタッチスクリーンバイオメトリクスと呼ぶ．スマートフォンを対象とすることにより，従来のキーストローク認証では得られなかったセンサやタッチスクリーンからの情報を利用した新たな特徴量の導入が可能となる [4]．

本研究では，実験によりスマートフォンにおける PIN 入力時のデータの収集と解析を行うことでタッチスクリーンバイオメトリクスの認証可能性についての議論を行う．従来のキーストローク認証では得られなかった特徴量を導入し，識別には統計的手法と機械学習の手法を用いて評価実験を行う．

2. 提案手法

2.1 特徴量抽出

タッチスクリーンバイオメトリクスでは従来より収集していた入力文字・押離の状態・時刻に加え，イベント発生座標と画面タッチ時の押下圧を取得することが可能であり，キーボードによるキーストロークダイナミクスと比較すると多様な特徴量を導入することができる．本研究で導入した特徴量を**図 2** に示す．PIN の入力桁数を n としたとき，特徴量の総数は $10n-3$ となる．

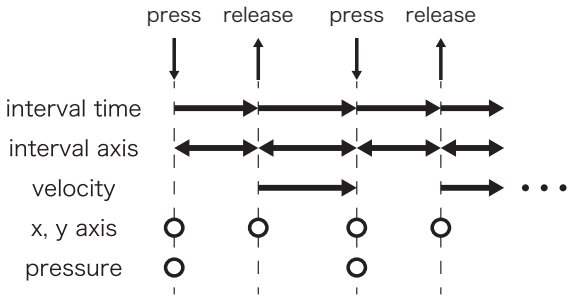

図 2 タッチスクリーンにおける PIN 入力の特徴量
Fig. 2 Feature indices for PIN input on touch-screen

特徴量ベクトルを $\boldsymbol{a} = (a_1, a_2, \cdots, a_i, \cdots, a_{10n-3})$ とし，本研究では以下の特徴量を用いる．

時間 $(a_i, i \in \{1, \cdots, 2n-1\})$
　タッチ操作における隣接時間間隔
　特徴量数: $2n-1$

距離 $(a_i, i \in \{2n, \cdots, 4n-2\})$
　タッチイベントの隣接座標間距離
　特徴量数: $2n-1$

速度 $(a_i, i \in \{4n-1, \cdots, 5n-3\})$
　キーを離してから押すまでの速度
　特徴量数: $n-1$

x, y 座標 $(a_i, i \in \{5n-2, \cdots, 9n-3\})$
　タッチイベント時の x 及び y 座標
　特徴量数: $4n$

押下圧 $(a_i, i \in \{9n-2, \cdots, 10n-3\})$
　キーを押した際の圧力
　特徴量数: n

2.2 認証の流れ

認証の流れを**図 3** に示す．本研究における認証プロセスはプロファイルを収集・生成するためのプロファイル登録フェーズ（Registration: 図 3 実線部）と入力ユーザが本人であるかを検証する認証フェーズ（Authentication: 図 3 破線部）に大別される．

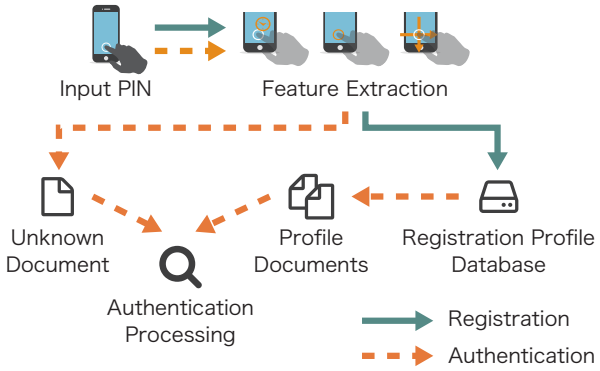

図 3 タッチスクリーンバイオメトリクスの認証の流れ
Fig. 3 Authentication process of Touch-screen biometrics

2.2.1 プロファイル登録

本フェーズでは，まず最初にユーザが PIN 入力を行う際にセンサやタッチスクリーンから得られる計測データを収集する．ユーザがプロファイル登録に必要な規定回数の入力を完了した後，特徴量抽出を行う．収集データの一例を**図 4** に示す．

登録プロファイル数を m としたとき，j 番目のプロファイルの特徴量ベクトルは $\boldsymbol{a}_j = a_{ij}$, $i \in \{1, 2, \cdots, 10n-3\}$, $j \in \{1, 2, \cdots, m\}$ となる．登録プロファイルにおける各特徴量の平均値 $\overline{a_i}$ と標準偏差 σ_i を次式に示す．

$$\overline{a_i} = \frac{1}{m}\sum_{k=1}^{m} a_{ik} \tag{1}$$

$$\sigma_i = \sqrt{\frac{1}{m}\sum_{k=1}^{m}(a_{ik} - \overline{a_i})^2} \tag{2}$$

次に，特徴量の正規化を行う（式 (3)）．登録プロファイ

```
0105,0,0,122.2547,51.319153,0.20392159,1355732241576
0105,0,1,114.238,61.331665,0.12941177,1355732241666
0105,1,0,76.49271,84.698364,0.14509805,1355732241813
0105,1,1,70.48018,88.70337,0.16078432,1355732241882
0105,0,0,100.542816,29.404266,0.13333334,1355732242110
0105,0,1,85.51149,25.399261,0.16078432,1355732242202
0105,5,0,110.229645,71.68213,0.18039216,1355732242430
0105,5,1,108.22547,71.68213,0.15294118,1355732242534
0105,OK,0,74.488525,72.68335,0.15686275,1355732243016
0105,OK,1,68.476,72.68335,0.11764707,1355732243105
```

図 4 収集される PIN 入力データの例
Fig. 4 Example of collected PIN input data

ルの平均（$\overline{a'_i}$）をとることによりプロファイルとする（式 (4)）．

$$a'_{ij} = \frac{a_{ij} - \overline{a_i}}{\sigma_i} \tag{3}$$

$$\overline{a'_i} = \frac{1}{m}\sum_{k=1}^{m} a'_{ik} \tag{4}$$

2.2.2 認証

入力者の特徴量を u_i とするとき，式 (3) と同様に正規化を行う（式 (5)）．

$$u'_i = \frac{u_i - \overline{a_i}}{\sigma_i} \tag{5}$$

その後，節 2.3 で述べる認証手法を用いて入力者が本人であるかの判別を行う．

2.3 認証手法

本研究では認証手法として統計的手法（節 2.3.1）と機械学習手法（節 2.3.2）の 2 手法を用いる．統計的手法ではユークリッド距離（ED: Euclidean Distance）法及びマンハッタン距離（MD: Manhattan Distance）法を用いて評価を行う．機械学習手法ではサポートベクターマシン（SVM: Support Vector Machine），三層バックプロパゲーションニューラルネットワーク（BPNN: Back Propagation Neural Networks），学習ベクトル量子化（LVQ: Learning Vector Quantization）による評価を行う．

2.3.1 統計的手法

統計的手法では，認証フェーズ（節 2.2.2）においてユーザ入力より抽出し式 (5) で正規化したユーザ入力の特徴量 u'_i と登録プロファイル間の距離を計算する．その距離があらかじめ設定しておいた閾値以下となれば本人であるとし，そうでなければ他人の入力であると判断する．

2.3.1.1 ED 法

ED 法における距離と閾値の関係を**図 5** に示す．

ED 法のプロファイル特徴量の距離 d^{ED} は式 (6) になる．

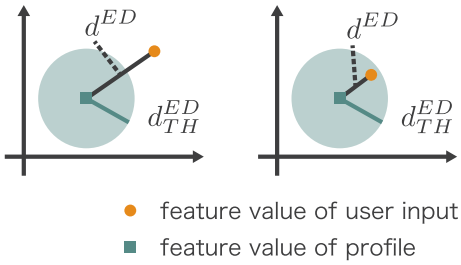

図 5 ED 法による本人認証（左）：入力者が他人の場合，（右）：入力者が本人の場合
Fig. 5 Authentication by ED method (left): correct user, (right): incorrect user

$$d^{ED} = \frac{1}{10n-3}\sqrt{\sum_{i=0}^{10n-3}(u'_i - \overline{a'_i})^2} \tag{6}$$

認証に際しては閾値 d^{ED}_{TH} を設定し，次式により認証を行う．

$$\begin{cases} d^{ED} \le d^{ED}_{TH} & (\text{本人}) \\ d^{ED} > d^{ED}_{TH} & (\text{他人}) \end{cases} \tag{7}$$

2.3.1.2 MD 法

MD 法における距離と閾値の関係を**図 6** に示す．

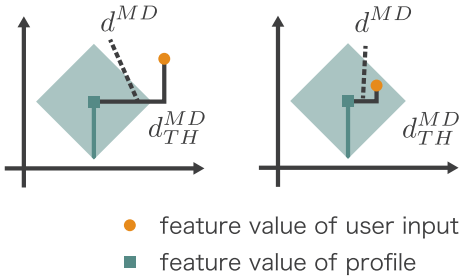

図 6 MD 法による本人認証（左）：入力者が他人の場合，（右）：入力者が本人の場合
Fig. 6 Authentication by MD method (left): correct user, (right): incorrect user

MD 法のプロファイル特徴量の距離 d^{MD} は式 (8) のようになる．

$$d^{MD} = \frac{1}{10n-3}\sum_{i=0}^{10n-3}|u'_i - \overline{a'_i}| \tag{8}$$

認証に際しては閾値 d^{MD}_{TH} を設定し，ED 法と同様に認証を行う．

$$\begin{cases} d^{MD} \le d^{MD}_{TH} (\text{本人}) \\ d^{MD} > d^{MD}_{TH} (\text{他人}) \end{cases} \tag{9}$$

2.3.2 機械学習手法

機械学習手法では登録プロファイルに加え，他人の特徴量データを用意することにより，教師あり学習によってあらかじめ識別器を構築しておく必要がある．認証フェーズ（節 2.2.2）で正規化されたユーザ入力の特徴量 u'_i を識別器に与え，本人と他人を分類させる． 本研究では 1 人で 1 つの識別器を構成する．

2.3.2.1 SVM

サポートベクターマシン（SVM: Support Vector Machine）はクラス分類，回帰，新規性検出などに用いられるデータ解析手法である [5], [6]．低次元な特徴ベクトルを高次元空間へと写像を行うというアプローチを取ることで線形分離可能性を高め識別超平面を求める．ここで線形分離可能であるとは**図 7** のように線形関数による超平面（2 次元の場合は直線）で対象データをもれなく分類することが可能である状況を指す． 線形分離可能な問題で 2 クラスの分類

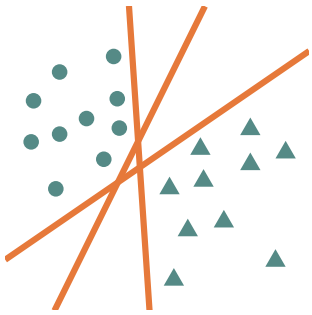

図 7 複数の超平面で線形分離可能な状態

Fig. 7 Samples that are linearly separable by hyperplane of multiple

を行うとき，決定境界となる超平面は複数存在する．

学習データの集合を $(\boldsymbol{x}_1, y_1), (\boldsymbol{x}_2, y_2), \cdots, (\boldsymbol{x}_n, y_n)$ と定義する．ここで，$\boldsymbol{x}_i$ $(X = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n\})$ は特徴量ベクトル，y_i はクラスラベルである．クラス 1 である場合に $y_i = 1$，クラス 2 である場合に $y_i = -1$ とすると，y_i における線形閾値関数は式 (10) のように表現される．

$$y_i = \begin{cases} 1 & ({}^t\boldsymbol{\omega}\boldsymbol{x}_i + \omega_0 \geq 0) \\ -1 & ({}^t\boldsymbol{\omega}\boldsymbol{x}_i + \omega_0 < 0) \end{cases} \tag{10}$$

ここで $\boldsymbol{x}_i$，$\boldsymbol{\omega}$ ともに d 次元である．$\boldsymbol{\omega}$ は重みベクトルであり，ω_0 はスカラーで閾値を表す．2 つのクラスを区別する超平面は式 (11) のように表される．

$${}^t\boldsymbol{\omega}X + b = 0 \tag{11}$$

式 (11) より，2 クラスを区別する超平面は $\boldsymbol{\omega}$ と ω_0 に応じて複数存在することがわかる．学習データを用いて，あらゆる未知のデータに対し適切に分類を行う超平面を構成する必要がある．SVM はこの超平面のうち，決定境界を決める学習データ（サポートベクトル）と決定境界との距離（マージン）が最大になるような超平面を求め，2 クラスの区別を行う超平面とするアルゴリズムである．ここでマージンは ${}^t\boldsymbol{\omega}\boldsymbol{x}_i + \omega_i = 1$ と ${}^t\boldsymbol{\omega}\boldsymbol{x}_j + \omega_i = -1$ の間隔として表される（**図 8**）． マージンを最大化するということは

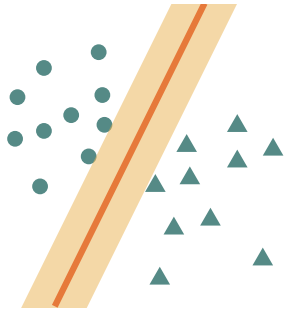

図 8 マージンが最大となる超平面

Fig. 8 Maximum margin hyperplane and margins with samples from two classes

$\boldsymbol{x}_i - \boldsymbol{x}_j = 2/\|\omega\|$ を最大化，もしくは $\|\omega\|$ を最小化する問題となる．この問題はラグランジュの未定乗数法により式 (12) のような問題設定として解くことが可能である．

$$\begin{cases} \frac{\|\omega\|^2}{2} & (\text{目的関数}) \\ y_i({}^t\boldsymbol{\omega}\boldsymbol{x}_i + \omega_0) \geq 1 & (\text{不平等制約}) \end{cases} \tag{12}$$

図 8 ではマージン内にデータが存在せず誤分類も発生していない．しかし，実際の問題では一部のデータの存在により線形分離不可能になる場合も多い．マージン内にデータが存在せず，誤分類ないマージンをハードマージンという．このような状況に対応するため，若干の学習データの誤分類を許すように SVM を修正する必要がある．その場合，式 (13) で表される不平等制約を考える．

$$y_i({}^t\boldsymbol{\omega}\boldsymbol{x}_i + \omega_0) \geq 1 - \xi_i \quad (\xi_i \geq 0) \tag{13}$$

ξ_i は各学習データごとに定義され，データが正しく分類されかつマージン境界の上または外に存在するかどうかを表す変数であり，スラック変数と呼ばれる．式 (13) のような制約を持つマージンをハードマージンに対しソフトマージンと呼ぶ．この場合のラグランジュの未定乗数法の目的関数は式 (14) のようになる．C は境界面からの逸脱度を伝える母数で，ペナルティ母数やコストなどと呼ばれる．

$$\frac{\|\omega\|^2}{2} + C\sum_{i=1}^{N}\xi_i \quad C > 0 \tag{14}$$

ここまでは線形分離可能な問題についてのみ述べた．線形分離不可能な問題に SVM を適用する場合，データの高

次元への写像を行うことで線形分離可能な状態に変換する必要がある．ここで問題となるのは適切な写像関数の選定と，元の空間のデータ間の距離関係を破壊しないような計算方法である．ここで写像関数 $\phi(\boldsymbol{x}_i)$ の内積として表現されるカーネル関数 $K(\boldsymbol{x}_i, \boldsymbol{x}_j)$ を利用することで，計算方法の問題は回避できる．データ解析や研究などで利用頻度の高いカーネル関数には以下の様なものがあげられる．

$$
\begin{aligned}
&{}^t\boldsymbol{x}_i\boldsymbol{x}_j && \text{（線形カーネル）} && (15)\\
&(\gamma\,{}^t\boldsymbol{x}_i\boldsymbol{x}_j + \delta)^p && \text{（多項式カーネル）} && (16)\\
&\exp(-\gamma\|{}^t\boldsymbol{x}_i - \boldsymbol{x}_j\|) && \text{（ガウシアンカーネル）} && (17)\\
&\tanh(\gamma\,{}^t\boldsymbol{x}_i\boldsymbol{x}_j - \delta) && \text{（シグモイドカーネル）} && (18)
\end{aligned}
$$

上記のカーネルには γ や p などの未知のパラメータが存在する．これらは識別器の性能に大きく影響するため，モデルの交差妥当性に配慮しつつ適切な値に設定する必要がある．また，カーネルを用いた非線形 SVM にソフトマージンを併用することも可能である．

SVM はマージン最大化学習則を用いているため，識別に用いる変数が多くなっても過学習を生じにくいという特性がある．一方で適切なカーネル選択やパラメータ調整に多大な計算コストを生じる可能性がある．

2.3.2.2 BPNN

ニューラルネットワーク（NN: Neural Networks）は，生物の脳の神経回路を模した数理的モデルである [5], [7]．神経回路を構成する最小単位はニューロンと呼ばれる神経細胞である．ニューロンは受け取った信号に処理を行い，条件をみたすと次のニューロンに処理済みの信号を送る．ニューロンのモデルを**図 9** に示す．　ここで $x_1, x_2, \cdots, x_n$

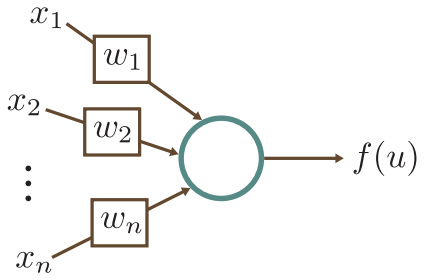

図 9　ニューロンのモデル
Fig. 9　Neuron model

は入力信号であり，$w_1, w_2, \cdots, w_n$ はそれぞれの入力信号に対応する結合の重みである．それぞれの入力信号 x_i に重み w_i をかけた $u = w_i x_i$ を求め，出力信号 $f(u)$ を生成する．モデル化されたニューロンの入力と出力の関係は式 (19) で表される．

$$
y = f(u) = \frac{1}{1 + \mathrm{e}^{-u}} \quad (\text{ただし } u = \sum_{i=1}^{n} w_i x_i) \qquad (19)
$$

図 9 のようなニューロンが多数並列に接続されたシステムがニューラルネットワークである．ニューラルネットワークのモデルを作成する場合，この重み w_i をどのように決定するかが問題となる．

ニューラルネットワークはニューロンの結合の仕方によりいくつかのモデルに分類される．その中でもよく使われているモデルの 1 つが**図 10** のような階層型ネットワークモデルと呼ばれるものである．2 つのクラスを識別するため

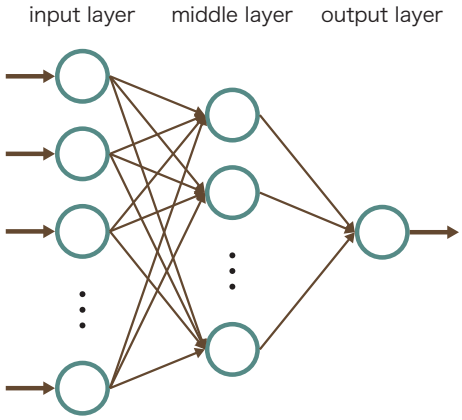

図 10　3 層の階層型ニューラルネットワークモデル
Fig. 10　Hierarchical neural network of three layers

のニューラルネットワークでは，入力層のニューロンの数は個体の特徴量数であり，出力層の形式ニューロンの数はクラスを表すニューロンただ 1 つである．中間層のニューロンの数は入力のデータ構造に適した数に設定する必要がある．

階層型ネットワークモデルの学習アルゴリズムとして最もよく使われるのが逆伝播法（BPNN: Back Propagation Neural Networks）である．BPNN は教師ありの機械学習法で，重み w_i に初期値としてランダムな値を与えたモデルに個体の特徴量である x_i を入力する．得られた結果が教師信号と違うものであれば，結果が目標値に近づくように重みを置き換えて計算を繰り返し，最適値を求めるものである．

BPNN は関数近似能力が優れており，3 層型で多くの問題をとくことができる．一方で中間層の最適なニューロン数の決定法が確立していないことや，学習データにより局所解に陥ってしまうといった欠点がある．

2.3.2.3 LVQ

学習ベクトル量子化（LVQ: Learning Vector Quantization）は学習データありの自己組織化マップ（SOM: Self-Organizing Maps）であり，ニューラルネットワークの一種である [8]．学習のアルゴリズムとして LVQ1，LVQ2，LVQ3 があり，LVQ とはそれらのアルゴリズムの総称である．LVQ は予めクラスの判明している学習データを元に代表ベクトルを作成し，逐次型学習によって代表ベクトルの更新を行い，入力空間を適切に分割する．その後，入力

データを与えた時にデータがどのクラス空間に含まれるかの判定を行い，クラスを識別する．

2.3.2.3.1 LVQ1

LVQ1 では新規学習データ $(\boldsymbol{x}, y)$ から最も近くにある代表ベクトル $\boldsymbol{c}$ を選び，学習データのクラスラベル y と代表ベクトルのクラスラベル l_c を比較する．これらが等しいならば代表ベクトルを学習データのベクトルに近づけ，異なるならば遠ざける．代表ベクトルは式 (21) に表される式により操作される．

$$\boldsymbol{c} = \arg\min \|\boldsymbol{x} - \boldsymbol{m}_i\| \quad \text{（代表ベクトル）} \tag{20}$$

$$\boldsymbol{c}(t+1) = \begin{cases} \boldsymbol{c}(t) + \alpha(\boldsymbol{x} - \boldsymbol{c}(t)) & y = l_c \\ \boldsymbol{c}(t) - \alpha(\boldsymbol{x} - \boldsymbol{c}(t)) & y \neq l_c \end{cases} \tag{21}$$

2.3.2.3.2 LVQ2

LVQ2 は，LVQ1 から更新する代表ベクトルを 2 つに増やしたアルゴリズムである．更新する代表ベクトルは学習データとクラスラベルが同じもので，最も近傍にある代表ベクトル $\boldsymbol{c}_1$ と，学習データとクラスラベルが異なるもので，最も近傍にある代表ベクトル $\boldsymbol{c}_2$ である．

$$\boldsymbol{c} = \arg\min \|\boldsymbol{x} - \boldsymbol{m}_i\| \tag{22}$$

$$\boldsymbol{c} = \arg\min \|\boldsymbol{x} - \boldsymbol{m}_j\| \tag{23}$$

代表ベクトル $\boldsymbol{c}_1$，$\boldsymbol{c}_2$ の中間の位置に 2 つのベクトルの距離の 10 ~ 20% の幅を持ったウィンドウを設定し，学習データがそのウィンドウに存在する場合，式 (24) 及び式 (25) により代表ベクトルを更新する．

$$\boldsymbol{c}_1(t+1) = \boldsymbol{c}_1(t) + \alpha(\boldsymbol{x} - \boldsymbol{c}_1(t)) \tag{24}$$

$$\boldsymbol{c}_2(t+1) = \boldsymbol{c}_2(t) - \alpha(\boldsymbol{x} - \boldsymbol{c}_2(t)) \tag{25}$$

2.3.2.3.3 LVQ3

LVQ3 は，LVQ1 と LVQ2 を組み合わせたアルゴリズムである．まず，学習データから最も近傍にある代表ベクトルを順に 2 つ選択する．

$$\boldsymbol{c}_i = \arg\min \|\boldsymbol{x} - \boldsymbol{m}_i\| \tag{26}$$

$$\boldsymbol{c}_j = \arg\min \|\boldsymbol{x} - \boldsymbol{m}_j\| \tag{27}$$

次に，2 つの代表ベクトルのクラスベクトルを l_i 及び l_j，学習データのクラスラベルを y としたとき，以下の条件のもとで代表ベクトルの更新を行う．

- $l_i = l_j = y$ である

$$\boldsymbol{c}_{i,j}(t+1) = \boldsymbol{c}_{i,j}(t) + \alpha(\boldsymbol{x} - \boldsymbol{c}_{i,j}(t)) \tag{28}$$

- $l_i \neq l_j$ であるが，$l_j = y$ かつウィンドウ内に学習データが存在する

$$\boldsymbol{c}_i(t+1) = \boldsymbol{c}_i(t) - \alpha(\boldsymbol{x} - \boldsymbol{c}_i(t)) \tag{29}$$

$$\boldsymbol{c}_j(t+1) = \boldsymbol{c}_j(t) + \alpha(\boldsymbol{x} - \boldsymbol{c}_j(t)) \tag{30}$$

LVQ は識別に用いる変数が多くなる場合などで有効である．一方，学習データだけでなくその読み込み順によっても結果が変わってしまうという性質を持つ．

3. 実証実験

3.1 実験概要

提案手法の有効性を検証するため，スマートフォンを用いた実証実験を行う．15 歳から 48 歳の男性 21 名を被験者として，被験者が普段から使用しているスマートフォン端末を利用する．被験者は 4 桁及び 10 桁の PIN を実際に入力し，図 3 のような収集データをデータベースサーバに送信する．PIN 入力，データ収集のために我々は Android 端末上で動作するアプリケーションを開発した（**図 11**）．

図 11 PIN 入力データ収集アプリケーションの動作画面（左）：PIN 入力画面，（右）：データ送信確認画面

Fig. 11 Screenshot from interface of pin input data collecting system. (left): PIN input screen, (right): data transmission confirmation screen

認証システムの検証を行うにはプロファイルデータとテストデータを用意しておく必要がある．本実験では本人の PIN 入力データとして，10 ファイルをプロファイルデータとして用いた．一方，テストデータには本人の PIN 入力データとして 15 ファイル（但し，プロファイルデータとして用いた 10 ファイルを除く）を，侵入者データとして他の被験者の PIN 入力データの 48 ファイルを用いた．

認証精度の評価指標として，本人拒否率（FRR: False Rejection Rate）と他人受入率（FAR: False Acceptance Rate）を用いる．また，FRR と FAR が等しくなる誤り率を等誤り率（EER: Equal Error Rate）とする．

本研究では以下の解析を行う．

- 特徴量の組み合わせについての認証率
- 認証率のプロファイル数依存性

統計的手法では閾値の調整により認証率が変化するため，EER を用いる．一方，機械学習手法は非線形なパラメータであるため EER を求めることは困難なので，FRR と FAR をそれぞれ求めた．

機械学習手法には R 言語のパッケージを用いた．SVM には”e1071”パッケージに含まれる svm 関数を使用し，カーネルにはガウシアンカーネルを選択した．パラメータ調整には関数 tune.svm を使用し，$C = 10^i$ $(i \in 0, 0.2, \cdots, 2.0)$, $\gamma = 10^j$ $(j \in -3.0, -2.8, \cdots, -1.0)$ の範囲でグリッドサーチを行い最適値を用いた．BPNN には”nnet”パッケージに含まれる nnet 関数を使用し，中間層のニューロンは 5 個とした．LVQ には “nnet” パッケージに含まれる lvq3 関数を使用し，アルゴリズムには LVQ3 を使用した．学習データは学習データ依存性を考慮した最適なプロファイル数と他人データ数に設定した．

また，座標や距離の特徴量は使用するスマートフォンの解像度の違いにより大きく影響を受ける．そこで本実験ではこの機種依存性による影響緩和のため，通常の pixel 値ではなく dp（Density-independent Pixel）を使用した． dp 値は画面解像度 160dpi（dots per inch）を基準とし，次式により求められる [9].

$$\mathrm{dp} = \mathrm{pixel} * (160/\mathrm{dpi}) \tag{31}$$

3.2 実験結果

3.2.1 特徴量の組み合わせについての認証率

3.2.1.1 統計的手法

4 桁の PIN 入力における実験結果を付録**表 A·1** に，10 桁の PIN 入力における実験結果を付録**表 A·2** に示す．1 つの特徴量及び特徴量の組み合わせにおいて，最も EER の精度が高いものを太字で示す．

まず，1 つの特徴量では座標特徴量が最も精度が高いことがわかる．ボタンのどこをタッチするかということに個人差が見られることがわかる．

特徴量を組み合わせた場合は，PIN4 桁，PIN10 桁とも「時間，座標，押下圧」の組み合わせが高精度であることがわかる．

「時間」「座標」「押下圧」以外の特徴量を加えても精度が向上しない原因として，「距離」は「座標」の関数であり，「速度」は「距離」と「時間」(即ち「座標」と「時間」) の関数となっていることがあげられる．「距離」「速度」の 2 特徴量に関しては「時間」「座標」と相関を持つため新たな特徴量としての寄与はほとんどないといえる．従って，「距離」「速度」を特徴量として組み込んだとしても，認証率において優位性は見られないと考えられる．

「時間，座標，押下圧」の特徴量の組み合わせを用いて，識別率（FRR，FAR）の閾値依存性について述べる．4 桁の PIN において MD 法を用いた場合の閾値 d_{TH}^{MD} を**図 12**，10 桁の PIN においても同様に MD 法を用いた場合の閾値 d_{TH}^{MD} を**図 13** に示す．PIN の桁数による大きな変化は見られず，$d_{TH}^{MD} = 1.5 \sim 1.8$ のときに FRR と FAR が同じ値（EER）となっている．

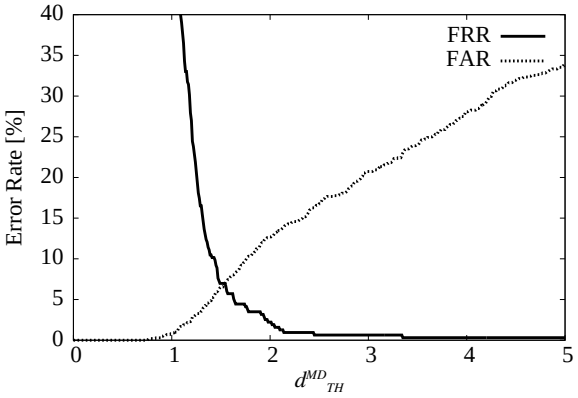

図 12 認証率における閾値依存性（PIN4 桁，MD 法）

Fig. 12 Dependence on threshold of recognition accuracy (4-digits PIN, MD method

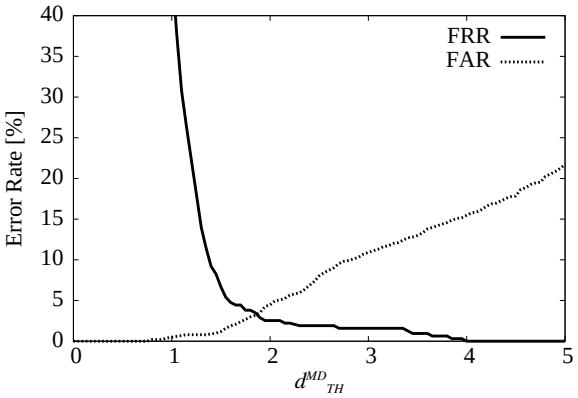

図 13 認証率における閾値依存性（PIN10 桁，MD 法）

Fig. 13 Dependence on threshold of recognition accuracy (10-digits PIN, MD method

3.2.1.2 機械学習手法

4 桁の PIN 入力において SVM を用いた場合の結果を付録**表 A·3**，BPNN を用いた場合の結果を付録**表 A·4**，LVQ を用いた場合の結果を付録**表 A·5** に示す．また，10 桁の PIN 入力において SVM を用いた場合の結果を付録**表 A·6**，BPNN を用いた場合の結果を付録表 A·6，LVQ を用いた場合の結果を付録**表 A·8** に示す．1 つの特徴量及び特徴量の組み合わせにおいて，最も精度が高いものを太字で示す．

1 つの特徴量については統計的手法（節 3.2.1.1）と同様に「座標」特徴量が優位である．一方で特徴量の組み合わ

せに関しては，手法や PIN の桁数により最適な特徴量の組み合わせは異なっている．これは，認証率に良い影響を与えない特徴量を含んでいたとしても，学習による重みの調整で精度が変化しやすくなるからだと考えられる．また，特徴量の数（入力層の数）が多いほうが学習に良い結果が出やすいことがわかった．

3.2.2 認証率のプロファイル数依存性

3.2.2.1 統計的手法

登録プロファイル数を 3，5，7，10 と変化させた場合の認証精度の変化について解析を行った．4 桁の PIN 入力における MD 法の結果を**図 14** に，10 桁の PIN に MD 法を用いた場合の結果を**図 15** に示す．

プロファイル数の増加により EER の値が向上していることが確認できる．しかし，プロファイル数が 5 以上では認証精度の向上はそれほど大きくない．プロファイル数は 10 もあれば安定することがわかる．

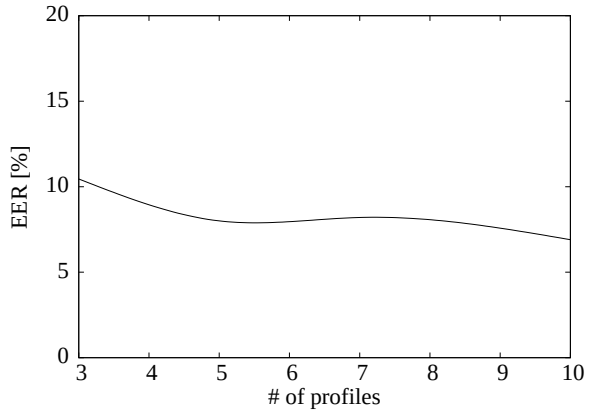

図 14 認証率の EER 曲線におけるプロファイル数依存性（PIN4 桁，MD 法）

Fig. 14 Dependence on the number of profiles in the EER curve of recognition accuracy(4-digit PIN, MD method)

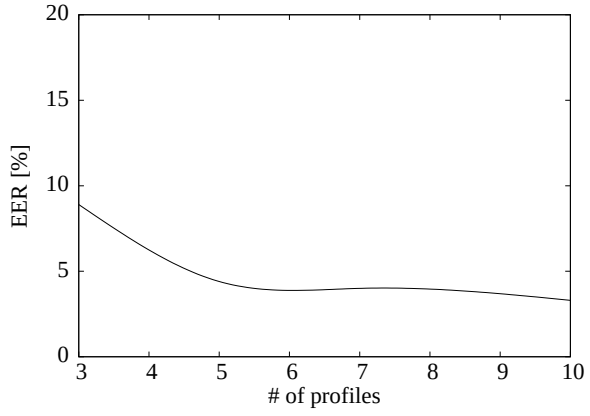

図 15 認証率の EER 曲線におけるプロファイル数依存性（PIN10 桁，MD 法）

Fig. 15 Dependence on the number of profiles in the EER curve of recognition accuracy(10-digit PIN, MD method)

3.2.2.2 機械学習手法

教師あり学習を行う SVM，BPNN，LVQ では学習データのうち，プロファイル数が 3，5，7，10 の場合について，それぞれ他人データの数を 3，5，7，10，15，17，20，23 と変化させたときの FRR と FAR を調べた．4 桁の PIN において SVM を用いた場合の結果を付録**表 A·9**，BPNN を用いた場合の結果を付録**表 A·10**，LVQ を用いた場合の結果を付録**表 A·11** に示す．10 桁の PIN も同様に SVM を用いた場合の結果を付録**表 A·12**，BPNN を用いた場合の結果を付録**表 A·13**，LVQ を用いた場合の結果を付録**表 A·14** に示す．

機械学習手法については，学習データに用いるプロファイル数が多くなれば全体的に精度が向上することがわかる．

PIN 桁数や識別手法を問わず，教師あり学習を行う手法においてはプロファイル数が増加すれば FRR が減少し FAR が増加する傾向が見られる．また，他人データ数が増加すれば逆に FRR が増加し FAR が減少する傾向が見られる．

3.2.3 関連研究との比較

本研究の関連研究として，スマートフォンだけでなく従来型の携帯電話や PDA のモバイル端末による実験が多く行われている．特にモバイル端末による PIN やパスワードにおけるバイオメトリクスの研究を**表 1** に示す．

Clarke と Furnell[10] は 4 桁ないし 11 桁の PIN と 6 文字のパスワードにおける携帯電話でのキーストローク認証を扱っている．特徴量は押離時間のみ利用している． 識別手法には FF-MLP（Feed Forword Multi-Layer Perceptron）や RBF（Radial Basis Function）Networks，Generalized Regression Neural Network（GRNN）の機械学習を用いている．我々の結果のほうが精度が向上していることがわかる．また，本研究では被験者全員が同一のパスワードしか扱っていない．Saevanee と Bhatarakosol[11] は PDA（Personal Digital Assistant）を対象としている． 特徴量は隣接時間と押下圧を利用している．識別手法にはユークリッド距離における k 近傍法（k-NN: k-nearest neighbors algorithm）を用いている．高精度の結果が得られはしているが本研究も被験者全員が同一のパスワードしか扱っていない．Hwang ら [12] は意識的にリズムを刻みながら入力を行うことにより認証率の向上を実現している．認証率の向上には有効であるが，我々の研究についても本手法を用いれば認証率は向上すると考えられる．

4. おわりに

本研究ではスマートフォン端末において PIN 入力を行った場合のセンサなどの入力データから認証を行うタッチスクリーンバイオメトリクスを提案し，実証実験を通してその有効性を示した．特徴量としてキーストローク認証で用いられてきた特徴量である隣接時間間隔に加え，従来では得られなかったタッチスクリーンバイオメトリクス独自の

表 1 関連研究との比較

Table 1 Comparison with related research

	PIN 桁数	被験者数	プロファイル数	PIN の種類	識別手法	EER [%]
Clarke and Furnell[10]	4	30	20	1	ニューラルネットワーク	9 ~ 16
	11					5 ~ 13
Saevanee and Bhatarakosol[11]	10	10	20	1	k 近傍法	1
Hwang et al.[12]	4	25	5	25	統計的手法	4
本研究	4	21	10	21	統計的手法	6.7
	10					3.3
	4				機械学習手法	6.8 ~ 7.0
	10					2.2 ~ 3.5

特徴量（距離，速度，座標，押下圧）を導入を検討した．また，識別手法として統計的手法（ED 法，MD 法）と機械学習手法（SVM，BPNN，LVQ）を用いて認証実験を行った．その結果は以下のとおりである．

- スマートフォンのセンサやタッチスクリーンから得られる特徴量を追加することで精度の向上が確認された
  - 統計的手法では「時間，座標，押下圧」が最適な特徴量の組み合わせとなった．登録プロファイル数が増加すると認証精度も向上するが，プロファイル数 7 以上では精度が安定した．
  - 機械的手法では手法や PIN の桁数により最適な特徴量の組み合わせが変化した．最適な認証率となる学習時のプロファイル数と他人データ数の関係を示すことができた．

今後は個人の閾値決定手法など実用化における課題を解決しつつ，認証率のさらなる向上をはかりより強固で安心，使いやすいシステムの開発を目指していく．

参考文献

[1] : CCC — Chaos Computer Club breaks Apple TouchID, Chaos Computer Club (online), available from ⟨http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid⟩ (accessed 2014-05-04).

[2] Samura, T. and Nishimura, H.: Personal Identification and Authentication Based on Keystroke Dynamics in Japanese Long-Text, *Continuous Authentication based on Biometrics: Data, Models, and Metrics, I. Traore et al.(Eds.), IGI Global*, pp. 212–231 (2011).

[3] Banerjee, S. P. and Woodard, D. L.: Biometric authentication and identification using keystroke dynamics: A survey, *Journal of Pattern Recognition Research*, Vol. 7, No. 1, pp. 116–139 (2012).

[4] 泉　将之，佐村敏治，西村治彦：スマートフォンにおける日本語非定型文でのフリック入力認証，第 3 回バイオメトリクスと認識・認証シンポジウム，pp. 85–90 (2013).

[5] 荒木雅博：フリーソフトでつくる音声認識システム: パターン認識・機械学習の初歩から対話システムまで，森北出版 (2007).

[6] C. M. ビショップ：パターン認識と機械学習下:ベイズ理論による統計的予測，シュプリンガージャパン (2008).

[7] C. M. ビショップ：パターン認識と機械学習上:ベイズ理論による統計的予測，シュプリンガージャパン (2008).

[8] T. コホネン：自己組織化マップ，シュプリンガーフェアラーク東京 (2005).

[9] : Supporting Multiple Screens — Android Developers, Google Inc. (online), available from ⟨http://developer.android.com/guide/practices/screens_support.html⟩ (accessed 2014-05-16).

[10] Clarke, N. L. and Furnell, S.: Advanced user authentication for mobile devices, *computers & security*, Vol. 26, No. 2, pp. 109–119 (2007).

[11] Saevanee, H. and Bhatarakosol, P.: User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device, *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*, IEEE, pp. 82–86 (2008).

[12] Hwang, S.-s., Cho, S. and Park, S.: Keystroke dynamics-based authentication for mobile devices, *Computers & Security*, Vol. 28, No. 1, pp. 85–93 (2009).

付　　録

A.1　特徴量の組み合わせについての認証率

表 A·1　PIN4 桁における特徴量の組み合わせごとの統計的手法による認証率（EER）

Table A·1　EER for combination of features by statistics method in 4 digits PIN

特徴量	ED 法 EER [%]	MD 法 EER [%]
時間	24.4	24.5
距離	17.2	17.8
速度	23.2	23.9
座標	**11.8**	**11.9**
押下圧	21.2	20.6
時間，距離	14.3	14.5
時間，速度	16.3	16.0
時間，座標	9.5	8.7
時間，押下圧	14.3	13.5
距離，速度	16.2	16.0
距離，座標	10.2	10.7
距離，押下圧	10.6	10.4
速度，座標	11.8	11.5
速度，押下圧	14.0	13.1
座標，押下圧	8.3	8.6
時間，距離，速度	14.0	14.0
時間，距離，座標	9.2	8.8
時間，距離，押下圧	11.1	9.6
時間，速度，座標	8.9	9.1
時間，速度，押下圧	10.8	10.3
時間，座標，押下圧	**6.8**	**7.0**
距離，速度，座標	10.2	10.7
距離，速度，押下圧	10.5	10.2
距離，座標，押下圧	7.6	7.8
速度，座標，押下圧	8.5	8.2
時間，距離，速度，座標	9.0	9.0
時間，距離，速度，押下圧	11.1	9.0
時間，距離，座標，押下圧	7.6	7.3
時間，速度，座標，押下圧	7.0	7.1
距離，速度，座標，押下圧	8.0	8.0
全特徴量	8.1	8.2

表 A·2　PIN10 桁における特徴量の組み合わせごとの統計的手法による認証率（EER）

Table A·2　Recognition accuracy for combination of features by statistics method in 10 digits PIN

特徴量	ED 法 EER [%]	MD 法 EER [%]
時間	14.9	14.7
距離	24.8	25.2
速度	16.0	15.8
座標	**7.1**	**7.5**
押下圧	22.5	21.4
時間，距離	12.8	11.5
時間，速度	11.6	10.2
時間，座標	5.1	4.3
時間，押下圧	10.8	10.1
距離，速度	16.9	17.2
距離，座標	7.2	6.3
距離，押下圧	14.3	14.6
速度，座標	6.3	6.5
速度，押下圧	12.8	12.5
座標，押下圧	5.1	4.7
時間，距離，速度	12.4	10.4
時間，距離，座標	5.1	4.3
時間，距離，押下圧	10.7	9.5
時間，速度，座標	5.2	4.1
時間，速度，押下圧	9.2	8.8
時間，座標，押下圧	4.2	**3.4**
距離，速度，座標	6.8	5.9
距離，速度，押下圧	12.7	11.6
距離，座標，押下圧	5.4	4.9
速度，座標，押下圧	**4.2**	4.2
時間，距離，速度，座標	5.4	4.6
時間，距離，速度，押下圧	10.8	8.9
時間，距離，座標，押下圧	4.8	4.3
時間，速度，座標，押下圧	4.4	3.4
距離，速度，座標，押下圧	5.4	4.4
全特徴量	6.8	3.9

表 A·3 PIN4 桁の SVM による特徴量の組み合わせについての認証率
Table A·3 Recognition accuracy for combination of features by SVM in 4 digits PIN

特徴量	SVM FRR [%]	SVM FAR [%]
時間	30.5	15.9
距離	20.3	16.1
速度	32.3	19.0
座標	**7.6**	**14.3**
押下圧	12.7	21.7
時間，距離	18.4	10.2
時間，速度	20.0	13.8
時間，座標	13.0	9.6
時間，押下圧	16.5	12.3
距離，速度	15.6	15.9
距離，座標	12.7	13.4
距離，押下圧	11.4	11.9
速度，座標	6.7	14.7
速度，押下圧	7.0	13.1
座標，押下圧	0.3	11.9
時間，距離，速度	14.0	10.0
時間，距離，座標	13.0	9.6
時間，距離，押下圧	13.0	6.1
時間，速度，座標	14.0	7.7
時間，速度，押下圧	14.6	9.7
時間，座標，押下圧	6.7	9.6
距離，速度，座標	10.2	13.1
距離，速度，押下圧	8.6	11.9
距離，座標，押下圧	5.4	11.2
速度，座標，押下圧	1.6	11.5
時間，距離，速度，座標	12.1	8.1
時間，距離，速度，押下圧	12.1	8.1
時間，距離，座標，押下圧	9.2	9.3
時間，速度，座標，押下圧	7.0	6.9
距離，速度，座標，押下圧	7.6	11.6
全特徴量	**5.1**	**8.2**

表 A·4 PIN4 桁の BPNN による特徴量の組み合わせについての認証率
Table A·4 Recognition accuracy for combination of features by BPNN in 4 digits PIN

特徴量	BPNN FRR [%]	BPNN FAR [%]
時間	34.0	15.6
距離	30.8	13.3
速度	40.0	15.4
座標	**19.1**	**11.2**
押下圧	27.3	14.7
時間，距離	22.9	12.8
時間，速度	26.0	14.4
時間，座標	13.3	12.5
時間，押下圧	20.6	11.4
距離，速度	24.4	12.7
距離，座標	21.0	13.8
距離，押下圧	20.3	9.3
速度，座標	14.6	10.2
速度，押下圧	10.5	12.9
座標，押下圧	7.0	8.3
時間，距離，速度	20.6	12.8
時間，距離，座標	14.9	12.3
時間，距離，押下圧	18.1	10.0
時間，速度，座標	14.6	12.7
時間，速度，押下圧	17.8	11.1
時間，座標，押下圧	9.8	9.1
距離，速度，座標	16.2	11.2
距離，速度，押下圧	17.8	8.8
距離，座標，押下圧	11.1	10.0
速度，座標，押下圧	**7.3**	**7.1**
時間，距離，速度，座標	14.6	12.3
時間，距離，速度，押下圧	16.8	11.1
時間，距離，座標，押下圧	12.1	10.7
時間，速度，座標，押下圧	10.8	9.3
距離，速度，座標，押下圧	9.5	10.3
全特徴量	10.8	10.5

表 A·5 PIN4 桁の LVQ による特徴量の組み合わせについての認証率

Table A·5 Recognition accuracy for combination of features by LVQ in 4 digits PIN

特徴量	LVQ FRR [%]	LVQ FAR [%]
時間	42.2	15.2
距離	35.2	12.4
速度	35.9	27.0
座標	**8.3**	**17.7**
押下圧	14.3	41.8
時間，距離	23.5	9.9
時間，速度	33.0	11.0
時間，座標	19.1	11.0
時間，押下圧	24.1	13.2
距離，速度	20.0	17.9
距離，座標	9.2	16.6
距離，押下圧	13.7	15.6
速度，座標	4.8	22.5
速度，押下圧	6.0	16.1
座標，押下圧	1.6	15.0
時間，距離，速度	20.0	10.9
時間，距離，座標	17.1	9.4
時間，距離，押下圧	14.3	8.7
時間，速度，座標	15.2	13.4
時間，速度，押下圧	18.7	11.6
時間，座標，押下圧	6.0	10.9
距離，速度，座標	8.9	14.5
距離，速度，押下圧	7.9	11.9
距離，座標，押下圧	2.2	15.4
速度，座標，押下圧	2.2	12.1
時間，距離，速度，座標	17.1	10.1
時間，距離，速度，押下圧	9.5	9.4
時間，距離，座標，押下圧	**7.6**	**8.8**
時間，速度，座標，押下圧	5.7	9.3
距離，速度，座標，押下圧	5.1	12.4
全特徴量	8.9	8.8

表 A·6 PIN10 桁の SVM による特徴量の組み合わせについての認証率

Table A·6 Recognition accuracy for combination of features by SVM in 10 digits PIN

特徴量	SVM FRR [%]	SVM FAR [%]
時間	18.7	13.4
距離	15.9	14.7
速度	14.0	18.0
座標	**6.3**	**7.9**
押下圧	5.4	19.3
時間，距離	9.2	5.1
時間，速度	19.4	7.3
時間，座標	7.9	4.8
時間，押下圧	9.8	9.6
距離，速度	9.5	8.0
距離，座標	4.4	7.5
距離，押下圧	7.9	9.3
速度，座標	7.0	5.1
速度，押下圧	10.5	7.2
座標，押下圧	4.4	6.5
時間，距離，速度	9.5	4.1
時間，距離，座標	6.7	5.2
時間，距離，押下圧	8.6	4.9
時間，速度，座標	8.3	4.4
時間，速度，押下圧	9.5	4.0
時間，座標，押下圧	4.4	5.4
距離，速度，座標	7.3	4.5
距離，速度，押下圧	5.7	3.3
距離，座標，押下圧	3.8	7.7
速度，座標，押下圧	6.0	3.4
時間，距離，速度，座標	7.6	3.7
時間，距離，速度，押下圧	8.6	3.3
時間，距離，座標，押下圧	3.8	5.8
時間，速度，座標，押下圧	5.7	5.5
距離，速度，座標，押下圧	**4.4**	**3.5**
全特徴量	4.8	5.8

表 A·7 PIN10 桁の BPNN による特徴量の組み合わせについての認証率

Table A·7 Recognition accuracy for combination of features by BPNN in 10 digits PIN

特徴量	BPNN FRR [%]	BPNN FAR [%]
時間	18.4	7.7
距離	24.1	8.5
速度	24.1	9.4
座標	**9.8**	**4.7**
押下圧	23.2	10.0
時間，距離	13.3	6.0
時間，速度	13.3	6.3
時間，座標	7.9	4.0
時間，押下圧	10.8	6.8
距離，速度	15.2	6.4
距離，座標	14.0	4.1
距離，押下圧	12.7	6.9
速度，座標	6.3	3.6
速度，押下圧	10.5	5.4
座標，押下圧	4.8	2.8
時間，距離，速度	11.1	5.6
時間，距離，座標	9.2	4.6
時間，距離，押下圧	9.5	5.4
時間，速度，座標	7.9	4.7
時間，速度，押下圧	7.0	5.8
時間，座標，押下圧	5.4	4.3
距離，速度，座標	9.5	4.1
距離，速度，押下圧	7.6	6.0
距離，座標，押下圧	9.5	4.6
速度，座標，押下圧	**4.1**	**2.2**
時間，距離，速度，座標	7.9	4.9
時間，距離，速度，押下圧	4.8	6.0
時間，距離，座標，押下圧	5.4	4.2
時間，速度，座標，押下圧	5.1	4.4
距離，速度，座標，押下圧	6.0	4.5
全特徴量	4.4	4.9

表 A·8 PIN10 桁の LVQ による特徴量の組み合わせについての認証率

Table A·8 Recognition accuracy for combination of features by LVQ in 10 digits PIN

特徴量	LVQ FRR [%]	LVQ FAR [%]
時間	21.9	8.1
距離	25.1	10.6
速度	28.3	9.6
座標	**5.4**	**9.7**
押下圧	8.9	27.2
時間，距離	12.1	4.9
時間，速度	13.7	5.6
時間，座標	6.7	4.3
時間，押下圧	9.8	5.4
距離，速度	13.0	6.3
距離，座標	9.5	8.4
距離，押下圧	6.3	9.3
速度，座標	8.3	5.3
速度，押下圧	8.3	9.6
座標，押下圧	1.9	7.1
時間，距離，速度	13.0	5.0
時間，距離，座標	7.3	4.2
時間，距離，押下圧	7.9	2.6
時間，速度，座標	5.1	4.7
時間，速度，押下圧	4.8	5.8
時間，座標，押下圧	1.9	4.1
距離，速度，座標	9.2	4.7
距離，速度，押下圧	6.0	4.4
距離，座標，押下圧	3.8	9.3
速度，座標，押下圧	2.9	5.0
時間，距離，速度，座標	4.8	3.8
時間，距離，速度，押下圧	7.6	3.0
時間，距離，座標，押下圧	3.5	4.0
時間，速度，座標，押下圧	2.2	3.4
距離，速度，座標，押下圧	4.8	5.1
全特徴量	**2.2**	**3.3**

A.2 認証率のプロファイル数依存性

表 A·9 SVM を用いた認証率における学習データ依存性（PIN4 桁）
Table A·9 Dependence on the number of training data of recognition accuracy using SVM (4-digits PIN)

	プロファイル数 5		プロファイル数 7		プロファイル数 10	
他人データ数	FRR [%]	FAR [%]	FRR [%]	FAR [%]	FRR [%]	FAR [%]
3	1.9	46.5	0.6	47.7	0.0	46.1
5	8.6	16.5	3.5	18.4	1.6	22.2
7	**9.5**	**13.9**	4.8	15.4	1.9	20.1
10	**14.6**	**8.6**	**8.9**	**11.0**	5.1	12.5
13	19.1	6.5	**8.6**	**7.6**	5.1	8.7
15	20.0	476	14.6	6.1	5.7	8.3
17	18.4	3.5	12.7	5.4	**4.4**	**7.8**
20	26.7	1.7	17.5	4.1	**10.5**	**5.4**
23	29.2	1.4	23.5	2.2	12.4	3.5

表 A·10 BPNN を用いた認証率における学習データ依存性（PIN4 桁）
Table A·10 Dependence on the number of training data of recognition accuracy using BPNN (4-digits PIN)

	プロファイル数 5		プロファイル数 7		プロファイル数 10	
他人データ数	FRR [%]	FAR [%]	FRR [%]	FAR [%]	FRR [%]	FAR [%]
3	4.1	26.3	1.6	26.2	1.0	25.6
5	3.8	23.4	2.5	23.3	1.9	22.8
7	5.1	24.3	3.8	24.3	2.2	23.4
10	**9.5**	**19.7**	6.3	21.3	3.8	20.8
13	**13.3**	**12.5**	9.5	13.4	6.3	14.7
15	15.2	10.9	11.1	11.6	7.3	13.0
17	15.6	9.6	**10.5**	**11.6**	**7.3**	**12.5**
20	18.7	6.4	**12.7**	**9.5**	**10.8**	**10.5**
23	21.6	5.5	12.7	7.0	10.2	8.7

表 A·11 LVQ を用いた認証率における学習データ依存性（PIN4 桁）
Table A·11 Dependence on the number of training data of recognition accuracy using LVQ (4-digits PIN)

	プロファイル数 5		プロファイル数 7		プロファイル数 10	
他人データ数	FRR [%]	FAR [%]	FRR [%]	FAR [%]	FRR [%]	FAR [%]
3	0.0	100.0	0.0	100.0	0.0	100.0
5	6.0	50.7	0.0	62.2	0.0	62.6
7	6.3	23.1	1.3	34.9	0.6	38.2
10	**9.2**	**14.8**	2.5	23.3	5.4	23.5
13	**11.7**	**9.4**	6.7	14.2	7.0	16.4
15	14.3	7.7	**5.7**	**11.5**	4.4	14.0
17	14.3	7.1	**8.9**	**8.7**	**7.0**	**12.8**
20	15.9	6.2	8.6	7.7	**8.9**	**8.8**
23	15.9	3.8	15.2	3.8	9.8	6.0

表 A·12　SVM を用いた認証率における学習データ依存性（PIN10 桁）

Table A·12　Dependence on the number of training data of recognition accuracy using SVM (10-digits PIN)

	プロファイル数 5		プロファイル数 7		プロファイル数 10	
他人データ数	FRR [%]	FAR [%]	FRR [%]	FAR [%]	FRR [%]	FAR [%]
3	2.2	27.6	2.2	34.5	1.0	38.6
5	**4.1**	**10.9**	4.4	13.1	2.5	13.4
7	**8.9**	**7.1**	6.0	8.9	3.2	11.4
10	10.2	5.9	**6.3**	**7.1**	7.0	7.3
13	9.8	3.0	**8.3**	**4.0**	**4.8**	**5.3**
15	11.7	1.9	7.6	4.0	**6.7**	**2.9**
17	12.4	0.9	11.7	1.4	7.9	1.7
20	10.8	0.9	11.7	1.5	7.6	0.9
23	11.4	0.6	9.2	0.7	7.9	0.6

表 A·13　BPNN を用いた認証率における学習データ依存性（PIN10 桁）

Table A·13　Dependence on the number of training data of recognition accuracy using BPNN (10-digits PIN)

	プロファイル数 5		プロファイル数 7		プロファイル数 10	
他人データ数	FRR [%]	FAR [%]	FRR [%]	FAR [%]	FRR [%]	FAR [%]
3	2.5	32.4	1.0	31.2	0.3	29.0
5	1.9	29.0	0.6	27.6	1.0	25.6
7	3.5	29.5	1.9	29.2	1.6	28.0
10	5.4	24.3	4.1	24.5	1.9	23.5
13	5.7	15.6	4.4	15.8	3.2	15.3
15	7.3	9.7	4.8	9.7	1.6	9.8
17	**7.6**	**8.8**	6.0	7.9	2.2	8.7
20	**8.6**	**6.4**	**6.3**	**6.3**	4.1	6.1
23	8.6	4.0	6.7	4.9	**4.4**	**4.9**

表 A·14　LVQ を用いた認証率における学習データ依存性（PIN10 桁）

Table A·14　Dependence on the number of training data of recognition accuracy using LVQ (10-digits PIN)

	プロファイル数 5		プロファイル数 7		プロファイル数 10	
他人データ数	FRR [%]	FAR [%]	FRR [%]	FAR [%]	FRR [%]	FAR [%]
3	0.0	100.0	0.0	100.0	0.0	100.0
5	0.6	56.6	0.3	64.3	0.0	68.3
7	5.4	31.2	0.6	36.2	0.3	37.8
10	8.3	15.6	7.6	18.6	2.2	21.5
13	**9.2**	**11.4**	5.4	13.6	1.0	17.8
15	**12.1**	**4.9**	**6.7**	**6.5**	1.3	12.0
17	5.4	3.7	**5.7**	**5.2**	1.9	7.3
20	5.1	1.9	1.3	4.1	1.9	6.0
23	4.4	1.6	2.2	2.4	**2.2**	**3.3**