Vol.2017-CSEC-79 No.4
2017/12/4

特徴点を自動的に生成する認証システム-ダミー特徴点の追加

堂園　浩[1,a)]　中頭 達也[†1]　中國 真教[2,b)]

概要：近年、スマートフォン、タブレットなどタッチパネルを備えた通信デバイスが広く普及している。生体認証デバイスとして、ミドルレンジ以上のスマートフォンには指紋認証ユニットが搭載されたものがほとんどとなっているが、ローレンジのスマートフォン、タブレットデバイスでは搭載率がまだ低いものとなっている。以前からこのようなデバイスでは PIN コードや結線パターンを用いた認証方式が使われている。本研究室では結線パターンを手書き図形から自由に設定できる生体認証方式について研究を進めてきた、本報告では、この認証方式にダミーポイントを加え、知識認証としての強度を高めたものを紹介する。

キーワード：タッチパネル、知識認証、図形認証、生体認証

The Authentication System Automatically Generating Feature Points - Effect of Dummy Feature Points

Hiroshi Dozono[1,a)]　Tatsuya Chuto[†1]　Masanori Nakakuni[2,b)]

Abstract: Recently, the devices which are equipped with touch panels, such as smart phone and tablet, become widespread. As the biometric authentication device, the fingerprint readers are equipped to the smartphone upper than middle range, however the almost of smartphone in low range and tablet devices do not equip the fingerprint reader. For such devices, PIN or the pattern of connecting points are used as authentication methods. In our group, the authentication method which can generate the patten automatically from freehand pattern is researched. In this report, the authentication method which raises the strength as the knowledge authentication with adding dummy points to the generated pattern is introduced.

Keywords: Touch panel, Knowledge authentication, Pattern authentication, Biometric authentication

1. はじめに

近年，通信技術の向上や多様な情報端末の登場により，社会の情報化は加速度的な広がりを見せ，コンピュータやネットワークは私たちの生活にとって無くてはならないものとなった．しかし，そのような情報化社会の広がりに伴い高くなるセキュリティの重要度に対し，利用者のセキュリティへの意識はあまり変化がないのが現状である．中でも急激に普及したスマートフォン，タブレット端末は個人情報を大量に含んでおり，外出の際に持ち出すことが多い分，情報漏洩のリスクも高い．[1] 気づかないうちに検索の履歴から趣味や興味のある事を調べられたり，GPS を利用して自分の居場所を知られたり，メールやショートメールの送受信記録を見られたり，SNS から個人情報を抜かれたりする等プライベートが筒抜けになってしまう可能性も十分に考えられる．そこで本研究室では、情報を守る手段であるセキュリティについて注目し，それら携帯端末の特徴の 1 つであるタッチパネルを活用した生体認証システムの開発を行ってきた。本認証方式の特徴として，タッチパネル以外の専用機器を必要としない為，汎用性に優れること，筆跡から生成した特徴点を用いた結線パターンという知識認証と、特徴点感の筆速を用いた行動的特徴量を用い

1　佐賀大学
Saga University, 1-Honjyo, Saga 849–8502, Japan
2　福岡大学
Fukuoka University
†1　現在，京セラドキュメントソリューションズ
Presently with KYOCERA Document Solutions
a)　hiro@dna.ec.saga-u.ac.jp
b)　nak@fukuoka-u.ac.jp

ⓒ 2017 Information Processing Society of Japan

た生体認証のハイブリットであり，従来のパスワードを用いた認証や Android 端末等で用いられている結線パターンを用いた認証方法に比べ遥かに高いセキュリティ強度が見込めることが挙げられる．また、本報告では特徴点にダミーポイントを加え、知識認証の精度を高める方式を提案し、その実験結果を示す。

2. 特徴点を自動的に生成する生体認証システム

筆跡を用いた生体認証を行う際, 完全なフリーハンド曲線から認証を行う事は非常に難しいと考えられる. 理由は自由に曲線を描写出来てしまうと, 利用者が毎回同じ筆跡を画面上に描写する事が難しいからである. よって，筆跡による認証を行う場合, ある程度の制限を設けて元の筆跡に近い物を再現する事や書き慣れた慣れた図形，例えば署名などを用いることが多い. ただ，日本人にとっては，署名は日常的でないため，書きなれたとは言いがたいものである．本研究では作成しているシステムでは，各ユーザが登録したフリーハンド曲線から特徴点を抽出し，特徴点と特徴点を一筆書きの要領で結線する行動により元の曲線に近い状態を再現する方法を提案する．図 1 に手書き図形からの特徴点の生成の例を示す。

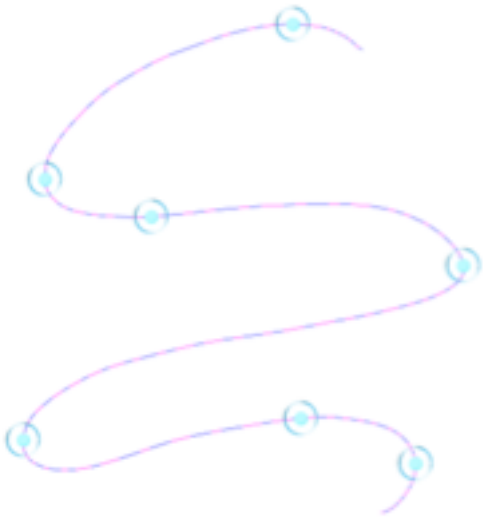

図 1 特徴点の生成
Fig. 1 Generated Feature Points

2.1 特徴点の検出

本研究で作成したシステムでは一筆書きされた曲線から特徴点を検出し，その点を結線する事で認証する．認証の際は検出された特徴点の順番で結線されないと認証成功にはならない．特徴点については，「点」と述べているが，結線の際は，特徴点の座標を中心として環境に応じた範囲を設けている．

2.1.1 特徴点検出

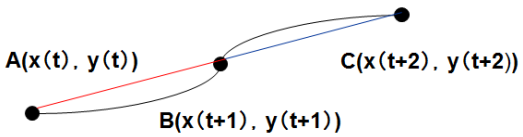

図 2 曲率計算に利用する座標
Fig. 2 Coordinate system for calculation of curvature

特徴点の検出には一筆書きされた曲線の連続する 3 点の座標から求められた曲率を用いる．曲率は図 2 に示すような 3 点 A,B,C が与えられている時，以下の式となる．[3]

$$d(t) = \frac{y(t+1) - y(t)}{x(t+1) - x(t)} \quad (1)$$

$$\text{曲率} = \left(\frac{1}{(1+(d(t))^2}\right)^{\frac{3}{2}} * (d(t+1) - d(t)) \quad (2)$$

今回この曲率が - 0.2 以下，又は 0.2 以上で特徴点のマーキングを行うが，更に（1），（2）の式に加え Y 座標と X 座標の値を入れ替えた計算も行い第 2 曲率も求めている．この理由としては [1]，[2] の数式のみでは X 座標の変化量が小さい垂線に近いような線を書かれてしまうと算出される曲率の変化が大きくなり過ぎてしまい，わずかな手ブレ等でも特徴点としてマーキングを行ってしまうので特徴点が増えすぎて生体認証を行う事が困難になってしまう事があげられる．最終的にそれぞれが - 0.2 以下，又は 0.2 以上の曲率を得る事でマーキングを行った．

2.1.2 一定距離における特徴点の検出

次に書かれた曲線が非常に緩やかであった場合，特徴点がなかなか検出されないという事態が起こりうる．そこで一定距離ごとに特徴点を表示するというアルゴリズムを追加した．このアルゴリズムにより，曲線の角度のある場所以外にも特徴点が生まれる為，システムを知っている非正規ユーザーでも認証が更に困難になることが考えられる．

2.1.3 内積を用いた特徴点の検出

実験を重ねると，上記 3 つの検出方法では，急な角度がついた時，例えばジグザグに一筆書きを行った場合にその各頂点を検出出来ない事がある事が分かった．そこで，上記 3 つの特徴点検出方法に加え，内積を用いた検出を行う．検出方法としては図 3 に示すようなある曲線が書かれる時，始点 O を定め，そこから一定距離進んだ座標 A までをベクトル a とすると，さらにそこから進んだ座標 B までをベクトル b とする．ベクトル b は書き進められ位置座標が更新される度に同じく更新されていき，ベクトル a とベクトル b が成す角が 70 度以上になった際に，座標 A から座標 B までを結んだ直線を考え，この直線を並行移動させた時，書かれた曲線の始点 O から座標 B までの範囲で交点が 1 つだけの点を特徴点としている．

ⓒ 2017 Information Processing Society of Japan

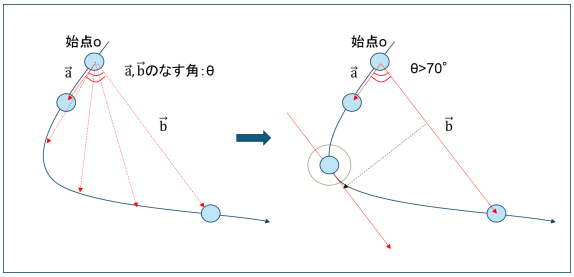

図 3 特徴点の検出方法
Fig. 3 Detection of feature points

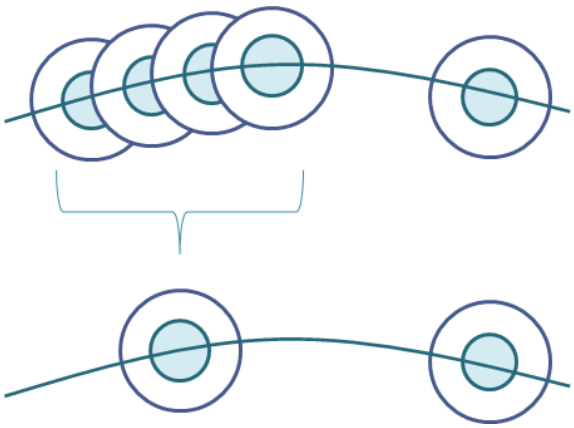

図 4 特徴点の統合
Fig. 4 Integration of feature points

2.1.4 特徴点統合

描いた曲線の曲率が一定以上，以下の状態が続くとき，特徴点が密集して表示されてしまい認証精度が下がってしまう．この問題に対して特徴点を中心とした円が重なった場合，特徴点のX，Y座標全てを合計し，それを特徴点数で割ることにより新たな特徴点を求めた．これにより認証に適した４～８の特徴点数に絞ることが可能となった．更にユーザーによっては，丸やハート型，多角形といった始点と終点が重なる図形を描くことがある為，そのような場合は図５に示すように始点と終点を統合し，統合された特徴点は始点と終点両方の特性を併せ持つようになっている．

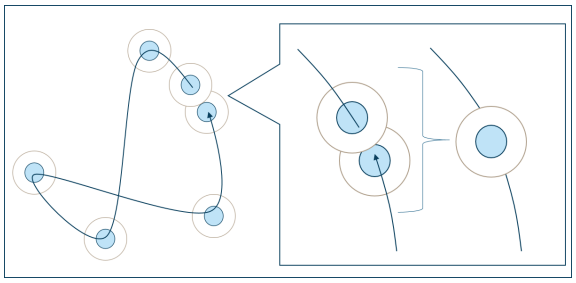

図 5 始点と終点の統合
Fig. 5 Integration of starting and ending points

2.2 筆速を用いた生体認証

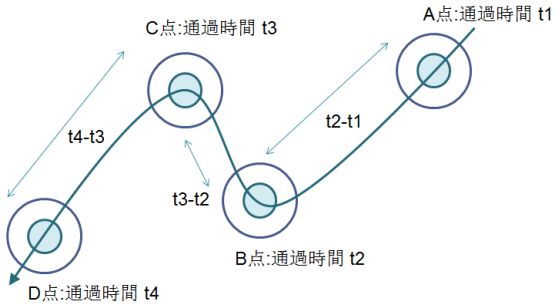

図 6 筆速の取得
Fig. 6 Acquisition of writing speed

生体認証に用いる筆速は上記の特徴点を利用して作成した認証点同士を結線する際に取得する．図６に示すように特徴点 A，B を中心とした円を通過した時間を t1，t2 とすると，t2-t1 を保存値と比較する．これを BC 間，CD 間と繰り返し，全セクションにおいて認証値と保存値の誤差が点間の距離に応じて設けられている閾値の範囲内であるとき認証成功となる．仮に，一筆書き開始位置，終了位置が円の範囲内であっても円に侵入した位置同士を比較する為，設定上問題はないが速度自体に違いが出やすいので非推奨としている．

ⓒ 2017 Information Processing Society of Japan

2.2.1 認証の最適化

生体認証，とりわけ行動的特徴量を用いる場合考慮しなければならない問題の一つが特徴量の変化である．経年変化はもちろん，怪我やユーザーを取りまく環境からユーザー自身の感情の状態という些細なことであっても認証値に影響してしまう．このようなことに対して，初めに取得した登録値を基に認証を行い続けていればいずれ認証できなくなることは必然である．従って認証に用いるユーザーの登録値は一定不変ではなく，ユーザーの認証値に応じて変化することが望ましいと考えられる．そこで今回のアプリケーションでは，認証成功する度に認証成功したユーザーの登録値を認証値に応じて変化させていくというアルゴリズムを加えた．これにより，認証するほどにより自分になじんだ認証アプリケーションになっていく．

2.3 ダミーシステム

本システムでは認証に用いる特徴点数を 5〜8 とすることを推奨しているが，検証結果より特徴点数 8 個は FRR が高くなってしまうことから，やや再現性に欠けることが分かった．さらに今回は検証を行っていないが，特徴点数 5 個の場合に偶然に認証が破られることが何度か見受けられたことから，特徴点数を 4 個以下とする場合はより FRR が増加することが想定される．そこで，自ら任意の場所にダミーの特徴点を配置できるシステムを追加した．なお，ダミー特徴点を配置するタイミングは筆速を取得後とし，配置可能数は最大 5 つまでとしている．認証時の判定は指を離した際に行われ，判定後に認証の成功と失敗，失敗の際は更に，ダミーを通過しての失敗，結線順を間違えることによる失敗，閾値を外れたことによる失敗とどのような失敗内容であるかを保存しておくシステムになっている．

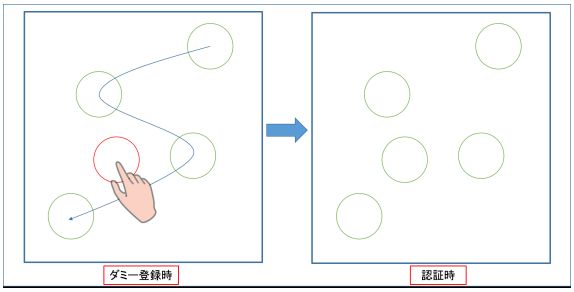

図 7 ダミー特徴点登録画面
Fig. 7 Screen image of registration of dummy feature points

3. 認証実験結果

3.1 結線パターンによる知識認証の実験

まず、結線パターンを用いた知識認証の実験結果を示す。．図 8 は検証に用いた特徴点数 4〜8 の結線パターンである．検証の際は図中の線が消えて円だけが表示された状態で一筆書きを１０人の被験者に各特徴点数 3 回ずつ計 15

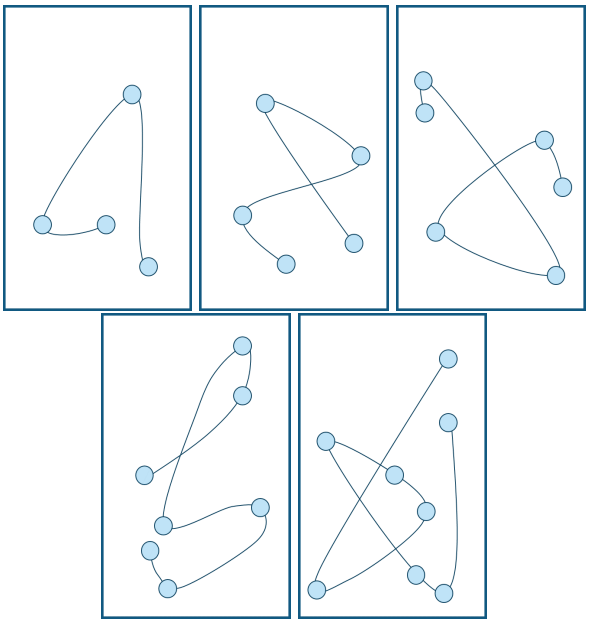

図 8 知識認証の検証に用いた結線パターン
Fig. 8 The connection patterns used to examine the knowledge authentication

ⓒ 2017 Information Processing Society of Japan

回行ってもらった．なお，本実験の参加者は全て，以前も同様に本システムの実験に参加してもらい，本認証アプリケーションを使用したことがある者である．検証結果を表 1 に示す．この表を見ると，特徴点が 4 つの場合 1 度認証が破られている．このことから特徴点は 5 以上あるほうが好ましいことがわかる．次に始点が正解であった人数と回数について考えると特徴点数 8 の場合に多くなっている．これは円が表示された時に一番上にある場所が始点であったためだと考えられる．よって，一筆書きの際の書き始める位置は出来るだけ画面上部を避けるべきであることがわかった．

表 1　パターン毎の検証結果
Table 1　Experimental result for each pattern

	4	5	6	7	8
正しい結線順で結べた人数	1	0	0	0	0
正しい結線順で結べた回数	1	0	0	0	0
始点が正解であった人数	4	1	2	2	4
始点が正解であった回数	5	1	4	2	6

3.2　筆速を用いた生体認証実験

3.2.1　実験方法

本システムの評価の為に，2 つの実験を行う．実験 1 は登録者である正規ユーザー含め 16 人で行う．初めに登録者が 20 回試行した後の登録データを登録者以外の 15 人が 20 回ずつ認証を行い，これを特徴点数 5〜8 毎に結線順未知，既知の場合で繰り返す．但し結線順が未知か既知の場合で特徴点数は同じだが書かれた曲線は異なるものとする．2 つ目の実験は特徴点毎で登録者を変更し 12 人で行う．登録者が 3 回認証成功した後にその認証の様子を見た登録者以外の 3 人が 5 回認証を行い，再度登録者が 5 回認証を行う．これを 3 人で特徴点数 6〜8 の場合に分けて行う．但しこの検証を行った 12 人は全て別人である．

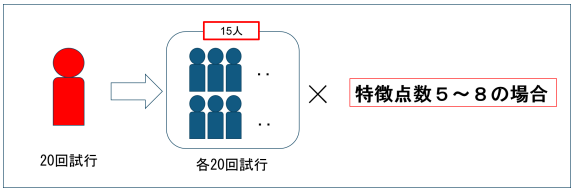

図 9　実験 1 のイメージ図
Fig. 9　Image of experiment 1

3.2.2　結線順を伝えていない場合の検証

先ず，FRR と FAR の試行結果の平均値の比較の内，結線順を伝えていない場合の実験 1 の結果を図 11 に示す．被験者は限られた試行回数の内様々なパターンで認証を試みていたが認証が破られる様子は無く，数値的に見た場合であってもほぼ FAR は 0 %であることがわかる．

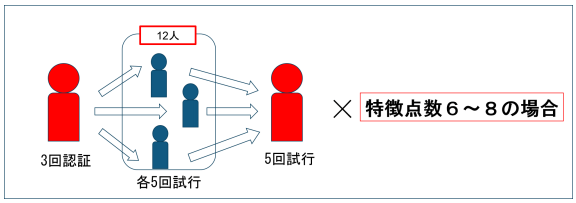

図 10　実験 2 のイメージ図
Fig. 10　Image of experiment 2

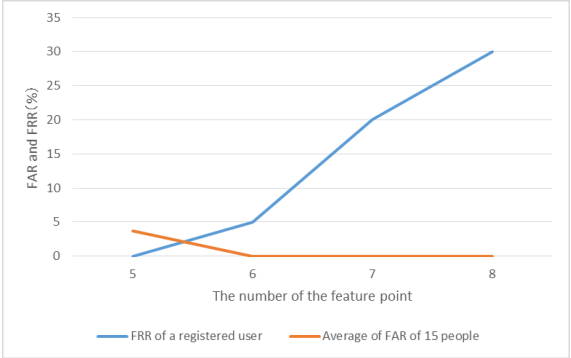

図 11　結線順を伝えていない場合の実験結果
Fig. 11　Experimental results without prior knowledge of connection order

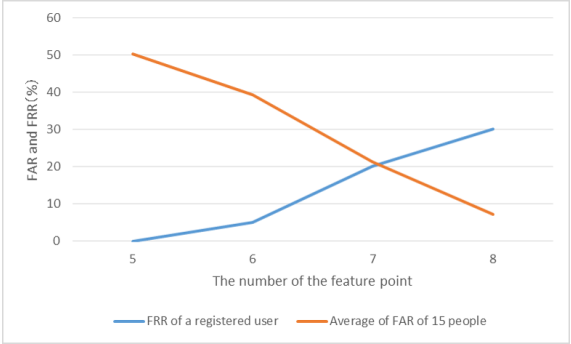

図 12　結線順を伝えた場合の実験結果
Fig. 12　Experimental results with prior knowledge of connection order

ⓒ 2017 Information Processing Society of Japan

3.2.3 結線順を伝えた場合の検証

結線順を伝えた場合の実験 1 の結果を図 12 に示す．前節の結線順を伝えていない場合における結果に対して，被験者によっては何度も誤認して認証成功させてしまうという場面が多くみられた．数値として見た場合においても全体的に FAR は高く，特徴点数 5，6 の場合 FAR は 40 %を超えるという結果になった．これらに対しなりすまし対策を講じる必要がある．

3.2.4 最適化システムの検証

表 2 実験 2 の実験結果
Table 2 Experimental results of experiment 2

	認証者	A	B	C
登録者 1 特徴点数 6	本人以外	1	4	1
	本人	5	2	4
登録者 2 特徴点数 7	本人以外	0	3	2
	本人	3	0	0
登録者 3 特徴点数 8	本人以外	0	0	0
	本人	4	4	5

表 2 では登録者以外が認証に成功してしまった場合にその後の登録者が認証に失敗してしまうことが分かる．これは認証成功するたびにユーザーの登録値を登録者に最適化していくシステムが逆効果となってしまった結果であると推測できる．実験 2 の結果よりユーザーに最適化するシステムが悪い方向へ働いてしまう場合があることが分かる．そこで，最適化のシステムを外した場合において検証 2 と同様の試行を行った結果を表 3 に示す．結果を見ると，表 2 の結果に比べ，登録者本人が安定した認証率を誇っていることが分かる．しかし，特徴点 8 個の際の認証に成功するといったように，本人以外の認証率も上がっている事が分かった．

表 3 実験 2 の実験結果
Table 3 Experimental results of experiment 2

	認証者	A	B	C
登録者 1 特徴点数 6	本人以外	2	3	3
	本人	5	5	5
登録者 2 特徴点数 7	本人以外	1	3	3
	本人	4	5	4
登録者 3 特徴点数 8	本人以外	0	1	1
	本人	5	4	4

3.3 ダミーシステムを加味した結果

次にダミーシステムを加味して実験を行い，ダミーシステムの評価を行う．実験内容として，特徴点数 4〜6 の場合にダミーの特徴点を 1 つ加え，登録者含めて 6 人それぞれに各特徴点数で 10 回の試行を行う．それをダミーシステム存在を初め伝えず，その後伝えて繰り返す．但し，本実験ではダミーがどの程度認証に影響を与えるかの確認が第一である為，ユーザーに最適化するシステムは無効としており，被験者はダミーシステムを実装していない通常のアプリケーションでの認証を経験したことのある者に限って選別を行っている．表 4 と 5 に実験結果を示す．表 4 の結果より特徴点数が 5，6 個の場合だけでなく 4 個であっても非正規ユーザーは認証成功しないことが分かった．1 つ目の実験では，非正規ユーザーは表示されている特徴点全てをなぞってしまうために失敗の種類が全てダミーを踏んでしまうことによる認証失敗であった．そのため，ダミーを意識した非正規ユーザーの考慮がまだ十分とは言えない．そこで，2 つ目のダミーを意識した実験での結果を見ると，図 5 より，ダミーを意識していても 1 つ目の実験と同様の結果が得られる形になった． 図 14〜16 に示すのは各ユーザー総試行回数の失敗内容の内訳を表すグラフであるが，特徴点数が 5 個，6 個の場合は 90%以上がダミーを踏むことが分かった．このことから，認証の様子を見られていない限りではダミーを配置することは非常に有効なセキュリティ能力を発揮することが分かった．しかし，ダミーの配置場所によっては，認証からしばらくするとダミーを配置した本人でも見分けがつかなくなったり，システムでは指を離した際に認証終了となっており，離すまでにダミーを少しでも通過したら認証失敗となる為，思いがけないうちにダミーに接してしまうという課題がある．

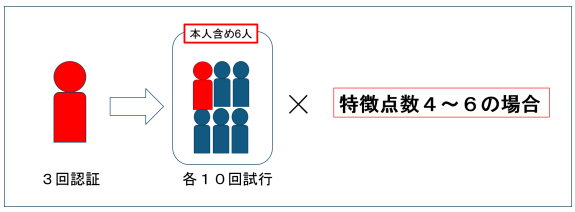

図 13 ダミーシステムの実験イメージ
Fig. 13 Image of the experiment of dummy system

表 4 ダミーシステムの実験結果
Table 4 Experimental results of dummy system

特徴点数	登録者	A	B	C	D	E
4	10	0	0	0	0	0
5	10	0	0	0	0	0
6	10	0	0	0	0	0

表 5 ダミーシステムの実験結果 2
Table 5 Experimental results of dummy system

特徴点数	登録者	A	B	C	D	E
4	10	0	0	0	0	0
5	10	0	0	0	0	0
6	10	0	0	0	0	0

ⓒ 2017 Information Processing Society of Japan

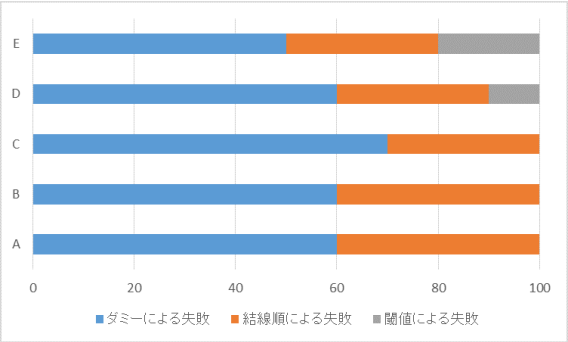

図 14 特徴点数 4 個での失敗内容の内訳
Fig. 14 Samples of failures for the patterns of 4 feature points

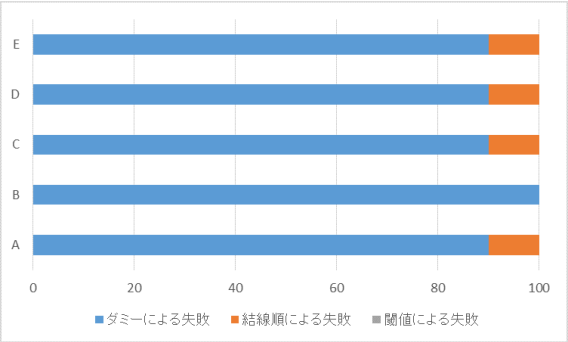

図 15 特徴点数 5 個での失敗内容の内訳
Fig. 15 Samples of failures for the patterns of 5 feature points

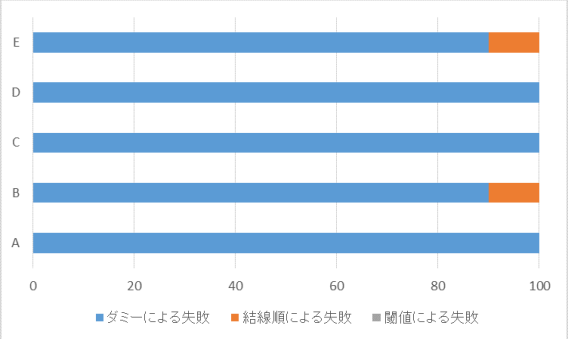

図 16 特徴点数 6 個での失敗内容の内訳
Fig. 16 Samples of failures for the patterns of 6 feature points

4. 結論

まず本研究において開発した認証システムについて，先行研究に加え，より正確な特徴点の検出，ダミーシステムの実装より，認証の様子を見られていない時はセキュリティはより強固となった．しかし，認証をする様子を見られた際の対策が未だ乏しく，有効円の設定の際の円の半径や通過率の考察，加えて円内における曲率を認証に用いることにより，認証精度の向上が見込めるのではないかと考えられる．実験結果に対しては，実験に協力していただいた被験者が，以前から今回の認証システムを知っており何度も認証実験に協力をしていただいた方々と，全く初めてこのような認証を行う方々が混じっていたために，その面においても認証率に変化があったのではないかと考えられる．いずれにせよ，全体として実験データの量不足を感じる結果になった為，実験データの効率的な収集方法も考える必要がある．

参考文献

[1] 稲葉　勇希/特徴点を自動的に抽出する個人認証システムに関する研究/佐賀大学大学院修士論文/2013
[2] 山崎　尚人/HTML5 を用いたオンライン生体認証システム/佐賀大学大学院修士論文/2015
[3] 梅原　雅顕　山田光太郎　共著/曲線と曲面―微分幾何的アプローチ―/裳華房/2002

ⓒ 2017 Information Processing Society of Japan