HSP を用いた
生体認証システムの開発

中頭達也[†1]　　堂薗浩[†1]

生体認証は身体的特徴や行動的特徴を利用した個人認証技術である．これらは物体やパスワードを用いた認証方式と比較すると，盗まれるリスクが低く，携帯電話や ATM のような様々な機器に用いられる．本研究では一筆書きにより抽出した，筆速の特徴を用いた生体認証アプリケーションの開発に HSP を用いている．HSP は windows 上で動作するスクリプト言語であり，追加セットの HSP3Dish を用いることで，開発したアプリケーションを様々な OS 上で動作させることが可能となる．

Development of the biometrics authentication system using HSP

TATSUYA CHUTO[†1]　HIROSHI DOZONO[†1]

Biometrics authentication is the personal authentication technology which uses physical feature or behavioral profile. Since the risks of theft and loss are lower than those of the authentic method using an object or a password, it is used in various devices like a mobile phone and ATM. In this research, HSP is used for Development of the Biometrics authentication application using the feature and speed of writing which were generated from the handwriting. HSP is a scripting language system that runs on Windows, and it is possible to operate on the various OSs developed by using an additional set of Hsp3Dish.

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で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より身近なものとなった．しかし身近になるにつれ，高くなるセキュリティの重要度に対して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多分に含んでおり，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．本研究では携帯端末の認証方式の 1 つとして，タッチパネル以外の専用機器を必要としない，筆跡から生成した特徴点や筆速といった行動的特徴量を用いた生体認証アプリケーションの開発を行った．[1]

更に開発したアプリケーションについて，利用形態や認証方法，正規ユーザーへの登録値最適化の有無といったいくつかの条件の下で認証データを収集，分析を行い，その実用性を評価した．

2. 生体認証

生体認証とは身体的特徴や行動的特徴を利用して，個人を特定する方法である．主にコンピュータのセキュリティや施設管理などに応用されており，最近では ATM や情報端末のログイン時等より身近に感じられるものとなっている．記憶認証や物体認証といった他の認証方式と比べ「なりすまし」が困難である事や認証方法が簡単である事がメリットとして挙げられる．また，本人が認証キーを忘れたり紛失したりと言うトラブルも回避する事ができる．

2.1 身体的特徴量を用いた生体認証

指紋，虹彩，声帯などの肉体的特徴の情報を利用した生体認証方法である．個人個人が肉体として持っている物なので盗難はほぼ不可能である上，それぞれの持っている情報量が非常に緻密で膨大であるため指紋を除いて，偽造も非常に困難である．しかし身体的特徴量を測定するにはそれぞれ専用のデバイスが必要になるため，システムの開発が複雑化する事やコストが掛かってしまうと言う問題がある．

2.2 行動的特徴量を用いた生体認証

筆速や筆跡といった特定の行動を行う際に現れる個々の癖を特徴量として利用し生体認証を行う方法である．

身体的特徴量とは違い，カメラやタッチパネルを応用し筆跡を測定するなど，必ずしも専用のデバイスが必要では無いためコストがかからない事が利点である．しかし癖は不変でない為，時間の経過とともに認証が上手くいかなくなる可能性がある他，他人に癖を真似されてしまう可能性なども有り，身体的特徴量を用いた生体認証に比べると個人の特定精度は低くなる傾向にある．

2.3 認証精度の評価

生体認証において認証の失敗は大きく二つに分類できる．一つは FAR（他人受入率）と呼ばれ他人を本人として認証してしまう場合である．生体認証は主に正規ユーザーの個人的特徴量登録し，それを基準として閾値を加えたものと入力されたデータの誤差を比較する事で本人であるかどう

†1 佐賀大学大学院工学系研究科先端融合工学専攻
Department of Advanced Technology Fusion, Graduate School of Science and Engineering Saga University

ⓒ2015 Information Processing Society of Japan

かを判断させる事が多い．

よって加える閾値の幅が大きくなるにつれ利便性は高くなるが非正規ユーザーを正規ユーザーと誤認して受け入れてしまい FAR は上がってしまう．もう一つは FRR（本人拒否率）と呼ばれ本人を本人として認証できない場合である．

こちらは FAR とは逆で上がると加える閾値の幅を小さくすることで安全性は高くなるが正規ユーザー本人も認証を失敗してしまう．つまり FAR と FRR は Fig1 に示すようにトレードオフの関係になっており両方を同時に下げるということが困難であることがわかる．

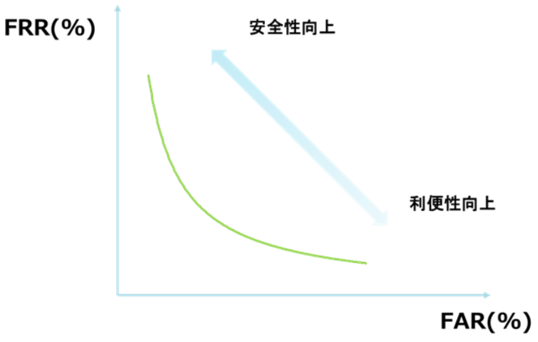

Fig.1　Relation of FAR and FRR

3. HSP

HSP は Windows 上で動作するスクリプト言語システムである．文法が簡潔であることや，多彩な命令セットがあるため，比較的簡単に本格的なアプリケーションソフトの開発を行うことが可能で，主に実用ツール，ゲーム，スクリーンセーバーなどの作成に用いられている．DLL をプラグインとして利用することができ，それによって DirectX や OpenGL などの 3D グラフィックスを扱うこともできる．

3.1 HSP3Dish

HSP3Dish は，HSP3 のスクリプトを iPhone や android 端末といったスマートフォンで動作させることのできるマルチプラットフォーム向けランタイムのセットである．

これにより，iPhone, iPad 始めとする iOS デバイスや，Galaxy, Nexus7 などの android OS を使用した携帯機器，タブレット上で動作するソフトウェアを HSP で開発することが可能になる．android 上で起動させるための環境設定として Android SDK，Android NDK，Java Development Kit，Apache Ant が必要である．[2]

4. 特徴点を自動的に取得する認証システム

今回作成した生体認証方式は特徴点の取得，筆速の取得，認証の 3 ステップに分かれている．

初めて利用するユーザーは一筆書きを行うことにより，特徴点を取得，次に 3 回初めと同じ形をなぞり書きすることにより筆速を取得し，最終的に認証画面で再度初めの一筆書きと同じ形をなぞることによって認証するという流れをとる．アプリケーション起動時は認証画面が最初に立ち上がり，そこからユーザーの変更，初回登録や筆速の再設定を行うことが出来る．

本認証システムの認証時の画面を，Fig.5，7，8 に示している．

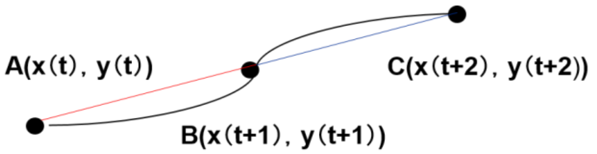

Fig.2　Feature point

4.1 特徴点の取得

一筆書きから特徴点を検出する条件は曲線の始点と終点，曲線が一定距離を経た時，連続する 3 点の曲率が一定値以上もしくは以下の時，座標間毎の内積によって導き出された角度が一定以上の時としている．取得した特徴点はユーザー情報として保存される．

Fig.2 に示した 3 点が与えられたとき，曲率を求める際に利用した計算式を以下に示す．[3]

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

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

Fig.3 に示すように，内積 $\vec{a}\cdot\vec{b}$ がなす角 θ がある一定以上の時は，$\vec{b}$ を平行移動させぶつかる筆跡座標が一つだけの点に特徴点を置く．

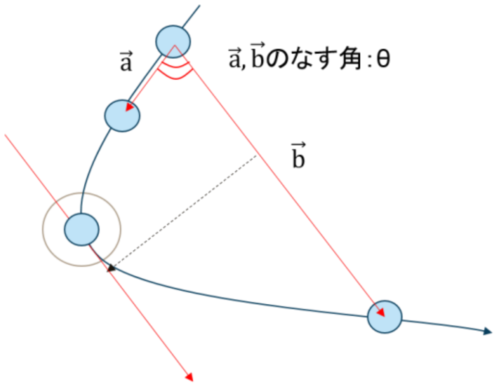

Fig.3　Detection using the inner product

検出した特徴点は描いた曲線の曲率が一定以上もしくは以下の状態が続くとき， Fig.4 に示すように密集して表示される．そこで，特徴点が重なった場合，重なった全ての点の重心に新しく統合点を表示することでこれを解決している．円形やハートの形のような始点と終点が接するような図形が描かれた場合は始点と終点を統合し，その統合された点には認証時，始点と終点のどちらの性質も兼ねそろえた点としている．なお，内積によって検出された特徴点と

ⓒ2015 Information Processing Society of Japan

重なりがあった場合は内積によって検出された特徴点を優先として表示している． Fig.5 に特徴点取得後の画面を示す．

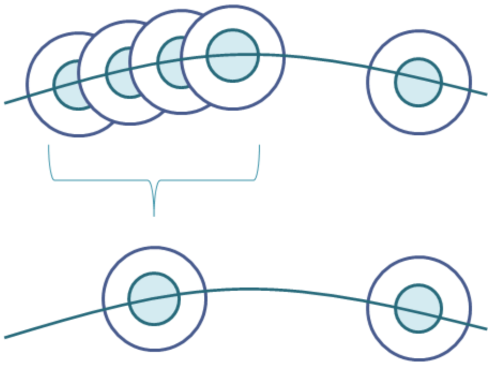

Fig.4　Integration of feature points

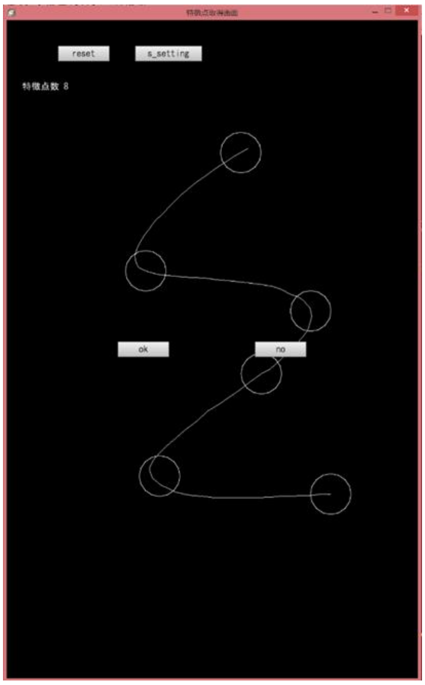

Fig.5　Feature point acquisition screen

4.2 筆速の取得

生体認証に用いる筆速は 3.1 で取得した特徴点のみをユーザー情報をロードすることによって表示し，初めと同じような曲線を 3 度書くことによって取得する．Fig.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 の値を求める． これを BC 間，CD 間と，全セクションにおいて繰り返し，各セクションの 3 回書いた平均値が登録値としてユーザー情報に上書き保存される．Fig.7 にロード画面と 3 回の筆速登録後の画像を示す．

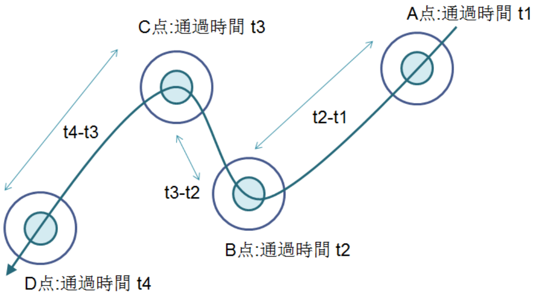

Fig.6　Writing speed

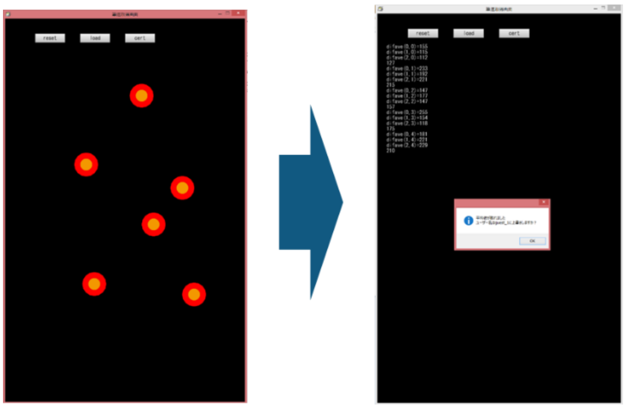

Fig.7　Writing speed acquisition screen

4.3 認証

認証は再度，3.1 で取得した特徴点のみを表示し，初めと同じ曲線を 1 度書く． 全ての点間において時間差の認証値が保存されたユーザーの平均の閾値内に収まれば認証成功となる． 特徴点と筆速まで登録していた場合は登録しているユーザー名をロードすることによって始めから認証を行える． Fig.8 に認証画面を示す．

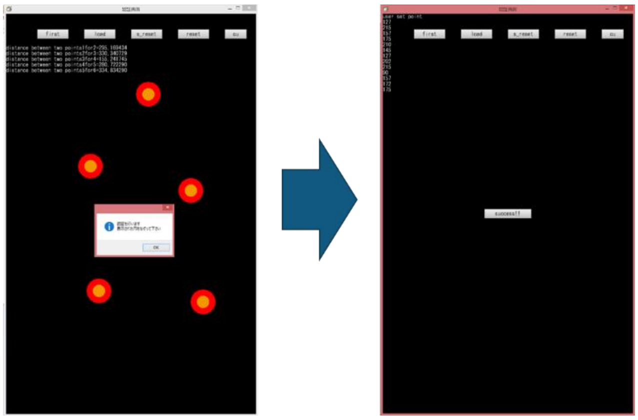

Fig.8　Authentication screen

4.4 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

ⓒ2015 Information Processing Society of Japan

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．

5. 認証システムの実験

今回開発した生体認証アプリケーションの実用性の評価の為に 2 つの実験を行う．

5.1 実験 1

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 6 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．

5.2 実験 2

実験 2 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．

6. 実験結果

Fig.9,10,11,12 に実験 1，Table.1 に実験 2 の結果を示す．

6.1 実験 1 の結果

Fig.9,10 は FRR と FAR の試行結果の平均値の比較を結線順未知と既知の場合で表している．Fig.9 より結線順未知の場合，ほぼ FAR は 0%である事が分かる．それに対し結線順既知の場合である Fig.10 では全体的に 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．次に FRR の値は特徴点数が 5，6 個の場合は 0%であるが 7 個以上になってくると次第に数値が上がっていっている為，極力特徴点数は 7 個以下が望ましいことがわかる．Fig.11,12 は 15 人の個別の FAR とその平均値を結線順未知と既知の場合で表している．Fig.11 を見ると，特徴点数が 5 個の場合の平均 FAR は 5%未満であるが，一人だけ 40%を超える被験者がいる事が分かる．これは 1 度認証に成功してしまうとそれ以降の認証が比較的容易になることが，原因であると考えられる．Fig.12 では個人による FAR の差が見られ，今回の認証に成功しやすい人，失敗しやすい人が分かりやすく露見する結果になったといえる．

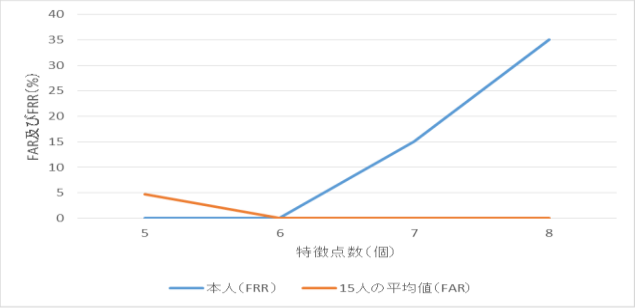

Fig.9 Comparison of FAR and FRR (Unknown)

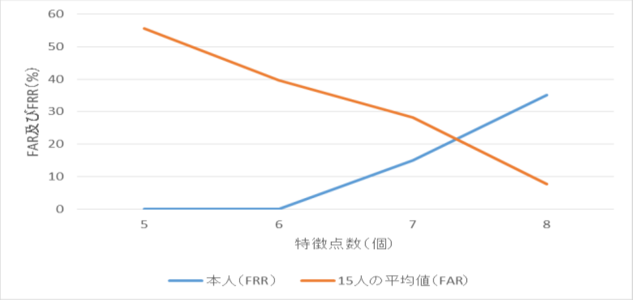

Fig.10 Comparison of FAR and FRR (Known)

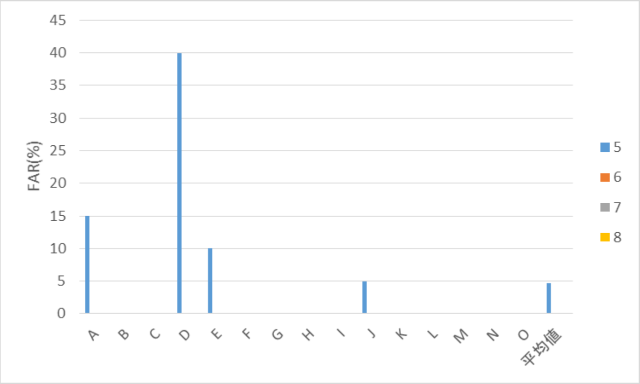

Fig.11 FAR for 15 people (Unknown)

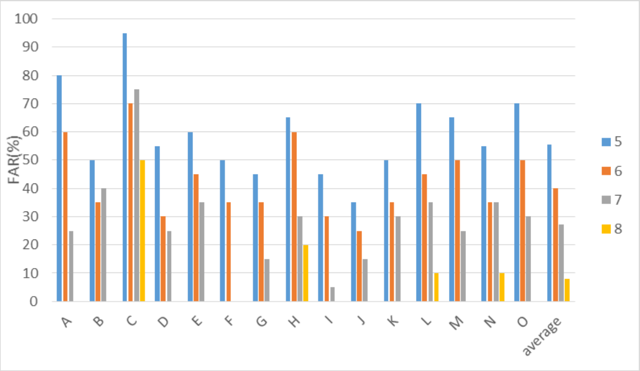

Fig.12 FAR for 15 people (Known)

6.2 実験 2 の結果

Table.1 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．

Table.1 The authentication result in experimentation 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

6.3 ユーザーに最適化するシステムの有無について

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実験 2 と同様の試行を行った結果を Table.2 に示す．結果を見ると，Table.1 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．

Table.2 The authentication result in experimentation 2（removed optimization system）

	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

7. ダミーシステムの導入

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．

7.1 ダミーシステムの実験

特徴点数 4，5，6 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 回の試行を行ってもらった．更にダミーが 1 つ追加されていることを伝えた上で同じ試行を行った．なお，認証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．

7.2 ダミーシステムの実験結果

ダミーシステムの実験結果を Table.3，4，Fig.13，14，15 に示す．Table.3 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，Table.4 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．Fig.13，14，15 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．

Table.3 The authentication result of the dummy system in experimentation 1

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

Table.4 The authentication result of the dummy system in experimentation 2

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

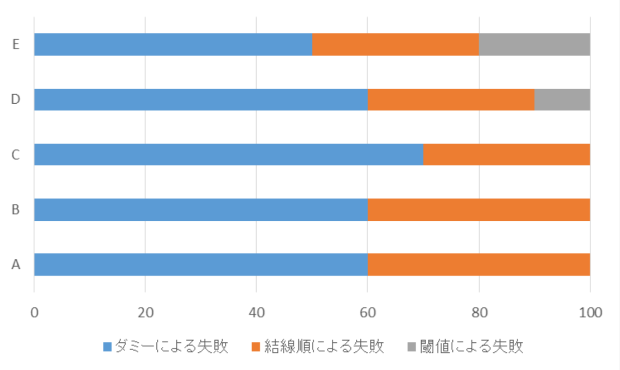

Fig.13 Try classification of the failure (Feature point 4)

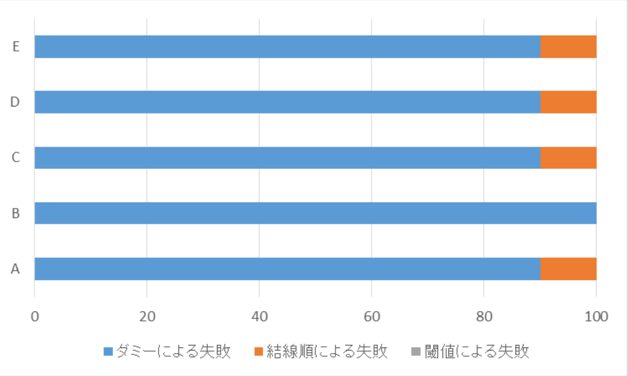

Fig.14 Try classification of the failure (Feature point 5)

ⓒ2015 Information Processing Society of Japan

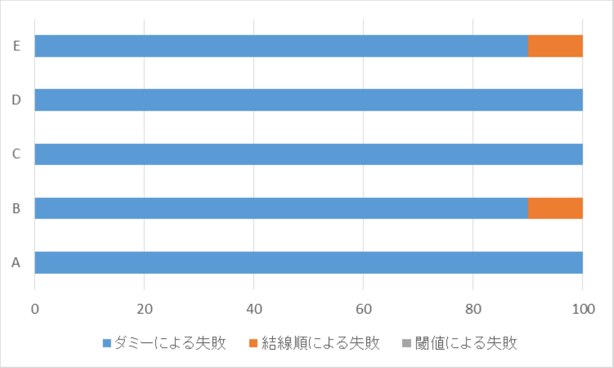

Fig.15 Try classification of the failure (Feature point 6)

8. おわりに

今回の実験結果より認証をしている様子を見られた後のなりすまし対策を早急にとる必要があることが分かった．更に，今回の認証システムの実験に協力していただいた被験者は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，このような認証をする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．

今後はそれらをふまえ，これまで以上に正規ユーザーが自ら最適な認証が可能となるような UI の開発を行っていきたい．

謝辞

本研究を行うにあたって，日頃から丁寧で親切な御指導，御鞭撻をいただいた，堂園浩准教授，築地浩技術職員　並びに諸先生方に厚くお礼申し上げます．

また，本研究について御助言や御協力いただいたグループ F 研究室の学部生，大学院生の皆様に深く感謝致します．

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
2)　おにたま: はじめてつくるスマホアプリプログラミング―HSP3Dish 入門
3)　山田　光太郎，梅原　雅顕：曲線と曲面

ⓒ2015 Information Processing Society of Japan