Vol.2018-MBL-89 No.9
Vol.2018-ITS-75 No.9
2018/11/15

# 他者からの推測に頑健な視線軌跡を用いた個人認証手法の検討

藤本巧海 [1,a)]　白石陽 [1,b)]

**概要**：近年，個人認証の技術として，パスワード認証とバイオメトリクス認証が広く普及している．しかし，これらの認証技術には脆弱性がある．パスワード認証は入力を覗き見によって認証情報が漏洩する．バイオメトリクス認証は認証情報が偽造されるリスクがあり，加えて，認証情報の変更が困難である．これらの脆弱性を解決するために本研究では視線軌跡に着目する．視線を用いた既存研究として，あらかじめ設定された文字を視線で描画し，その軌跡から得られる特徴を抽出することで，個人認証を行った研究がある．この研究では，描画する軌跡があらかじめ設定されているため，認証情報が容易に推測されてしまう．そこで本研究では，他者から推測されにくい視線軌跡を用いた個人認証手法を提案する．提案手法では，ユーザ自身が認証に用いる視線軌跡を事前に登録し，認証時に描画した視線軌跡と登録した視線軌跡を比較することで個人認証を行う．提案手法では，視線軌跡の形状推定を行い，同時に，個人の描画特徴を抽出する．本研究では，個人利用の端末における 1 対 1 認証を想定しているため，提案手法では端末を保有する本人の特徴量のみを用いて学習を行う．

**キーワード**：視線軌跡，個人認証，１対１認証，描画特徴，認証情報

## 1. はじめに

近年，パソコンやスマートフォン，タブレットなどの普及している[1]．それらのモバイル端末ではロック解除や SNS へのログインなど，個人認証を行う機会がある．代表的な個人認証の技術としてパスワード認証とバイオメトリクス認証が挙げられる．パスワード認証は，利用者が事前に登録した文字列を認証情報に用いた認証手法であり，バイオメトリクス認証は，身体の一部の身体的特徴や行動的特徴を用いた認証手法である．現在，指紋や顔，虹彩を用いた認証は実用化され，パソコンやスマートフォンなどに適用されている．このようにパスワード認証とバイオメトリクス認証が個人認証技術として広く普及している．しかし，これらの認証手法には脆弱性がある．

パスワード認証は，覗き見により認証情報が漏洩するリスクがある．覗き見は攻撃者が専門的な知識を習得していなくてもできるソーシャル・エンジニアリングである．そのため，パスワード認証は認証情報が誰にでも漏洩してしまう危険性があると考えられる．また，パスワードを強固にするためには，パスワードを複雑にする必要がある．しかし，複雑なパスワードほど入力や記憶の負担が大きくなる．バイオメトリクス認証は，認証情報として登録している指紋や顔などの生体情報が偽造されるリスクがある．大久保らは，ゼラチンに指を押し付けて作成した擬似指紋を用いて指紋認証システムを突破した事例を取りあげ，バイオメトリクス認証は必ずしも安全な認証を行うことができるとは限らないという問題を指摘している[2]．また，認証情報として利用する指紋や虹彩などの生体情報は意図的に変更することができないため，認証情報を偽造された場合の対処が困難である．このようにバイオメトリクス認証では，認証情報が偽造された場合，攻撃者になりすまされ，その対処が困難である．より安全な認証を実現するためには，パスワード認証やバイオメトリクス認証の脆弱性である（1）覗き見により認証情報が漏洩すること（2）認証情報の変更が困難であることを解決することが必要であると考える．

そこで本研究では，これらの脆弱性を解決するために生体情報の一つである視線に注目した．視線は指紋や顔と同様に他者からは見えない．また，視線の動きの推測は困難である．よって，覗き見により視線の情報を盗むことは困難であると考えられる．さらに身体の一部を認証情報として用いていないため，認証情報が偽造されることがない．また，ユーザが視線で描画した軌跡（以下，視線軌跡と呼ぶ）を認証に用いると，認証情報として登録した視線軌跡を変更することで認証情報を変更することが可能になる．したがって，視線軌跡を用いることで，覗き見に頑健かつ認証情報の変更が可能である認証を実現できると考える．

視線情報を用いた認証に関する研究として，ビデオを刺激として被験者に与え，その際に計測される視線の移動を認証に用いた研究がある[3]．この手法では，無意識な視線の移動を認証情報として扱っているため，ユーザが意図的に認証情報を変更することが困難である．また，アルファベットや○記号を視線で描画し，描画軌跡から得られる特徴量を認証に用いた研究がある[4]．この手法は，あらかじめ設定された文字や記号を視線で描画した軌跡を認証に用いているため，認証情報が推測されることについて十分に

1　公立はこだて未来大学システム情報科学部
School of Systems Information Science, Future University Hakodate.
a)　b1015149@fun.ac.jp
b)　siraisi@fun.ac.jp

Vol.2018-MBL-89 No.9
Vol.2018-ITS-75 No.9
2018/11/15

考慮されていない．本研究では，他者からの推測に頑健な個人認証手法の提案を最終目的とするが，本稿では，認証情報の変更を可能にするための要素技術として，視線軌跡の形状推定に有効な特徴量の検討を行う．

## 2. 関連研究

視線情報を用いた認証に関する研究として，無意識な視線移動を認証に用いた研究とユーザの意識的な視線移動を認証に用いた研究がある．

### 2.1 無意識な視線の移動を認証に用いた研究

無意識な視線の移動を認証に用いた研究についてKinnunenらは，タスク中の視線の移動から抽出した特徴を用いた認証を行っている[3]．この研究では，字幕付きのビデオを刺激としてディスプレイに表示し，事前に被験者に対して視線計測に関する指示テキストを提示している．ビデオと視線計測に関する指示テキストの表示中に観測される視線の移動から抽出した特徴量を用いて認証を行っている．この手法では，ユーザに意識させず認証を行うことができる．しかし，無意識な視線の移動を用いており，一度登録した認証情報の変更が困難であると考えられる．

### 2.2 ユーザの意識的な視線移動を認証に用いた研究

ユーザが意識した視線の移動を認証に用いた研究として，視線でパスワードを入力する認証を行った研究[5][6]と，視線軌跡を描画し，描画時間や描画速度などの特徴量を抽出することで認証を行った研究[4]がある．De Lucaらは，ディスプレイに表示されたキーパッド上で入力したい数字を一定時間注視することでPIN（Personal Identification Number）コードを入力する認証手法を提案している[5]．また，Rajannaらは，ディスプレイ上に表示される複数の記号の中からパスワードとして入力したい記号を一定時間視線で追跡することで記号を入力する認証を行った[6]．この手法では，3桁の入力記号をパスワードとして設定し，それらの記号を順に注視することでパスワードの入力を行っている．文献[4][6]の手法は，認証情報の変更が可能である．しかし，入力するパスワードの桁数や文字数が少ない場合には攻撃者に推測される可能性がある．パスワードの桁数や文字数を多くすると入力にかかる時間が増え，入力に対する負担が大きくなる．一方，向井らは，あらかじめ設定された文字や記号を視線で描画し，その視線軌跡から得られる特徴を抽出することで，個人の識別を行っている[4]．この手法で認証情報として登録できる視線軌跡はアルファベットのA~F，○記号の7種類である．これらのアルファベットと記号のうち1文字を選択し，認証情報として扱う．この手法では，ユーザが利用できる複数の視線軌跡が設定されており，認証情報として登録されている視線軌跡が限られている．そのため，認証情報の推測が容易であるが，他者から記号のパターンを推測されやすい．

### 2.3 まとめ

視線の移動を個人認証に用いる場合，文献[3]から無意識な視線の移動を用いる場合は認証情報の変更が困難になることが問題となる．文献[5][6]では，桁数が少ない場合において認証を行った．しかし，桁数が多くなると認証にかかる時間が増え，認証時にユーザに与える負担が大きくなることが考えられる．また，文献[4]より認証情報として登録できる軌跡に限りがあり，種類が少ないと文献[5][6]の手法と同様に認証情報を推測されるリスクがある．視線の移動を個人認証に用いる場合，認証情報が変更かつ他者からの推測が困難であることが求められる．そこで本研究では，認証情報の変更を可能にするためにユーザが視線で描画した軌跡を認証情報として用いる．また，パスワード認証と比べて他者からの推測に対して頑健な認証を実現するために，ユーザ自身が視線軌跡を定義し，認証情報として登録する．本稿では，ユーザが定義する軌跡の例をあらかじめ複数用意し，これらの軌跡間の類似度の算出を行う．

## 3. 提案手法

本章では，まず3.1節で本研究の目的を述べ，3.2節では本研究で提案するシステムについて述べる．3.3節では研究課題とアプローチについて述べる．3.4節以降では本稿で取り組んだ提案手法の詳細について述べる．

### 3.1 研究目的

本研究の最終目的は，視線軌跡を用いた他者から推測がされにくい個人認証手法の提案である．認証情報を他人からの推測に対して頑健なものとするために，本研究では認証情報である視線軌跡をユーザ自身が登録する．また，認証情報の変更を可能にするために，ユーザがどのような視線軌跡を描画したかを推定する必要がある．あらかじめ登録した軌跡と新しい認証情報として登録する視線軌跡の形状を推定する．異なる視線軌跡の形状であると識別することで認証情報の変更が可能になる．軌跡の形状を推定するためには視線軌跡から推定に有効な特徴量を選定する必要がある．また，提案手法では，認証情報として軌跡形状と軌跡の描画の特徴を用いる．よって，軌跡の形状推定のための特徴量だけでなく，描画特徴量の抽出も行う．本稿では，視線軌跡の形状推定に有効な特徴量を選定するための初歩的な検討として，簡易な視線軌跡を設定し，描画された視線軌跡から特徴量を抽出し，視線軌跡間の類似度の比較を行った．

Vol.2018-MBL-89 No.9
Vol.2018-ITS-75 No.9
2018/11/15

### 3.2 提案システム

本研究の提案システムの全体像を図 1 に示す．提案システムは学習フェーズと認証フェーズから構成される．まず学習フェーズにおいて，軌跡の形状推定と個人描画特徴の学習モデル作成を行う．まず，視線軌跡の入力後，前処理を行い形状推定に用いる特徴量の抽出を行う．その後に軌跡の形状のための学習モデルの作成を行う．また，個人描画特徴の学習モデル作成は，入力された視線軌跡から個人描画の特徴量の抽出後に行う．認証フェーズにおいて，学習フェーズで作成した学習モデルを用いて作成した個人識別のための学習モデルから認証を行う．本稿では，学習フェーズにおける軌跡の形状推定のための特徴量抽出について検討を行った．

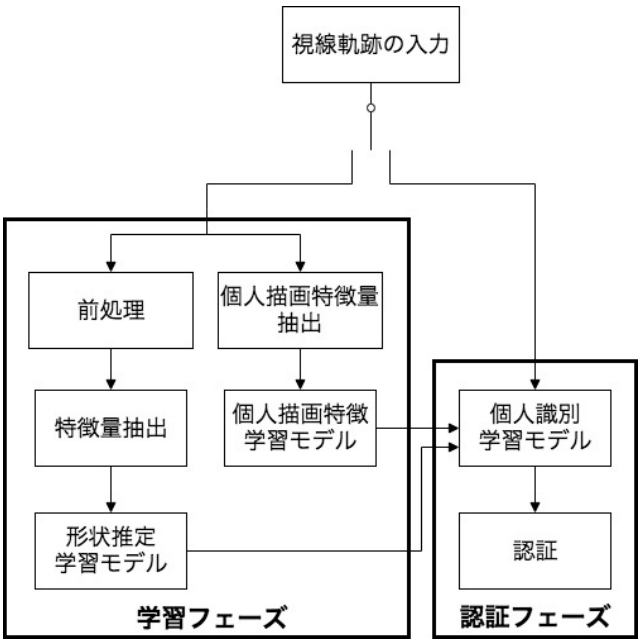



図 1 提案システムの全体像

### 3.3 研究課題とアプローチ

本研究では，以下の 4 つを研究課題とする．

a) 視線計測デバイスの検討
b) 認証情報の変更
c) 個人識別のための特徴量の検討
d) 学習モデルの検討

課題 a に対するアプローチとして，非接触型デバイスを計測デバイスとして用いる．視線計測装置はメガネ型の接触型と，据え置き型やディスプレイ一体型の非接触型のデバイスがある．メガネ型のデバイスを用いた場合，普段メガネをかけないユーザに対する装着の負担が大きくなると考えた．非接触型デバイスは装着などの負担を与えないため，ユーザが制限されることがない．これらの理由により，本研究では，計測デバイスとして非接触型デバイスを用いる．

課題 b に対するアプローチとして，視線軌跡の形状の推定を行う．提案手法では，他者からの推測に頑健な認証を実現するためにユーザ自身が登録した視線軌跡を認証情報として用いる．認証情報を変更したい場合，視線軌跡を再登録すれば良い．再登録したい軌跡と既に登録されている軌跡を比較し，識別を行う．したがって，軌跡の識別を行うために視線軌跡の形状を推定することが必要となる．

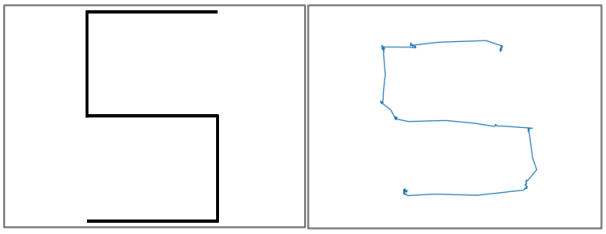
課題 c に対するアプローチとして，視線軌跡の描画時の視線のブレや注視時間などの描画特徴を用いることを検討している．提案手法では，認証情報として軌跡の形状と軌跡から得られる描画特徴量を用いる．軌跡の形状のみを認証情報として扱うと，複数のユーザで同じ形状の軌跡を定義した場合，同一のユーザとして識別する可能性があるため，なりすましに対して脆弱になると考えられる．以上の理由により，視線のブレや描画速度などの個人の描画特徴量を用いることが必要である．

課題 d に対するアプローチとして，OCSVM(One Class Support Vector Machine)を用いることを検討している．文献[5]の手法では，認証システムに登録されているユーザのうちの誰であるかを識別する 1 対 N 認証を想定しており，SVM による多クラス分類を用いて分類を行っている．しかし，本研究で提案する認証手法は，個人の利用端末における 1 対 1 認証を想定している．よって本人のデータを正常なデータとして学習させ，他人のデータを異常なデータとして扱うことで本人のみを識別できると考える．

本稿では，課題 a と課題 b に注目し，非接触型デバイスを用いて視線軌跡の収集を行い，視線軌跡形状の推定に有効な特徴量選定のための検討を行う．

### 3.4 視線軌跡のデータの分析

視線軌跡のデータは，ディスプレイの左上端を原点とした 2 次元座標空間上の時系列データとして表現される．描画時刻順にしたがって，各点を線で結ぶことで軌跡データが構成される．収集した視線軌跡のデータの例を図 2（左図はユーザが登録したい軌跡であり，右図は計測された視線軌跡である）に示す．



Vol.2018-MBL-89 No.9
Vol.2018-ITS-75 No.9
2018/11/15

図 2　収集した視線軌跡のデータの一例

図 2 の右図の軌跡上の点が集中して描画されている部分は注視箇所を表す．この注視箇所は，形状の推定においてはノイズになると考えられる．3.5 節ではノイズを取り除くための前処理について述べる．

### 3.5 軌跡データの前処理

軌跡の形状推定を行うための手法として座標データを用いた手法と軌跡の画像データを用いる手法があると考える．座標データを用いる場合，形状推定のために抽出できる特徴量が少なく，軌跡の形状推定において座標を線で結んだ画像データを用いることで座標データよりも多くの特徴量を抽出できると考えた．そこで本研究では，形状推定を行うためにまず視線で描画した軌跡を画像データとして扱う．すなわち，点列データを画像データに変換し，前処理を行う必要がある．本研究では，視線軌跡データの前処理を行う．具体的な処理の手順を以下に示す．

(i)　2 値化
(ii)　膨張処理
(iii)　細線化処理

以下，それぞれの処理について述べる．

膨張処理と細線化処理をするにあたって，あらかじめ軌跡画像データの 2 値化を行う．膨張処理は，2 値画像において注目画素の周辺に白い画素が 1 画素でも存在する場合に白に置き換える処理である．膨張処理を行うことにより視線の細かいブレを削除することができると考える．

細線化処理とは 2 値画像を幅 1 ピクセルの線画像に変換する処理である．膨張処理を行うことで，注視箇所の部分の幅が大きくなる．膨張処理を行った際，注視箇所や視線のブレにより凹凸が生じる．それらの凹凸により形状が正しく推定されないことが考えられる．そこで，膨張処理を行った軌跡の幅を統一するために細線化処理を行った．これらの処理を用いることで軌跡画像のノイズを削除することができると考える．

### 3.6 軌跡形状のための特徴量の検討

#### 3.6.1 局所特徴量を用いた軌跡の形状推定

視線軌跡のような線図形において特徴が際立って見られるのは転折である．転折は図形全体ではなく局所的に観測される特徴である．よって，局所的に特徴量を抽出することで，効率的に形状推定を行うことができると考えた．本稿では，形状推定のための特徴量として局所特徴量を用いることを検討する．

#### 3.6.2 Accelerated-KAZE 特徴を用いた軌跡の類似度算出

Accelerated-KAZE(AKAZE)特徴とは，局所特徴量である KAZE 特徴に比べ，ロバスト性が高い特徴量であり，算出にかかる計算コストが少ない[7]．KAZE 特徴とは SIFT(Scale-Invariant Feature Transform )や SURF(Speeded-Up Robust Features)の欠点を解決した特徴である[8].

比較に用いる軌跡画像から AKAZE 特徴点を抽出し，マッチングする特徴点のユークリッド距離を求めることにより，登録されている軌跡と再登録したい軌跡の類似度を算出する．ユークリッド距離は距離が短いほど画像の類似度が高いため，値が小さくなるほど画像が類似していると言える．

## 4. 予備実験と考察

本章では，3 章で述べた提案手法に基づき行った予備実験について述べる. 4.1 節では軌跡データの前処理について述べる．次に 4.2 節では前処理を行ったデータを基に行った軌跡の形状の分類について述べる．最後に 4.3 節では考察について述べる．

### 4.1 軌跡データの前処理

本節では，軌跡データの前処理を行った結果を述べる．表 1 に，予備実験の実験環境を示す．また，視線計測装置として Tobii Pro Tx-300 を用いて視線軌跡のデータ収集を行った. 視線の座標のサンプリング周波数は 60Hz である．

表 1　予備実験の実験環境

| | |
|---|---|
| CPU | Intel Core i5 2GHz |
| OS | High Sierra10.13.6 |
| 言語環境 | Python2.7.15 |
| 使用ライブラリ | OpenCV3.4.3 |

図 2 で示した視線軌跡の画像を 2 値化し，膨張処理を行った画像を図 3 に示す．視線軌跡の注視箇所のブレは軌跡ごとに異なるため，どのようなブレにおいても均等に滑らかにするために膨張処理を 30 回行った．

図 3　図 2 の描画軌跡を 2 値化・膨張処理した画像

膨張処理を行った際，注視箇所の視線のブレにより複数

Vol.2018-MBL-89 No.9
Vol.2018-ITS-75 No.9
2018/11/15

の軌跡間で膨張した軌跡の幅が異なる．軌跡の幅の差により形状が正しく推定されないことが考えられる．そこで，膨張処理を行った軌跡の幅を統一するために細線化処理を行った．細線化処理を行った画像を図 4 に示す．また，図 4 は本原稿における見えやすさを考慮し，白黒を反転させて表示をしている．

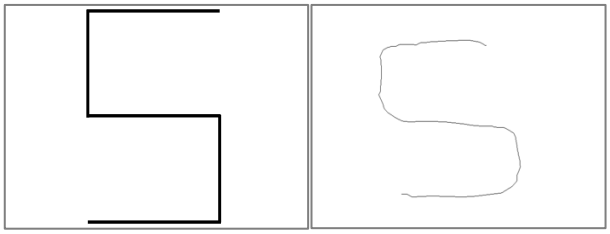


図 4 図 3 に対し細線化処理した画像

### 4.2 Accelerated-KAZE 特徴を用いた軌跡の類似度算出

図 4 の AKAZE 特徴点と，異なる形状の軌跡を前処理した画像の AKAZE 特徴点を抽出し，最近傍点のユークリッド距離を求めた．特徴点を抽出した軌跡の画像を図 5，図 6，図 7，図 8，図 9（左図はユーザが登録したい軌跡であり，右図は計測された視線軌跡に対し前処理を行った画像である）に示す．これらの図は図 4 と同様に白黒を反転させて表示している．図 4 と異なる形状の軌跡として図 5，図 6，図 7，図 8 を用いた．また，図 9 は図 4 と同じ形状を想定し描画した軌跡である．

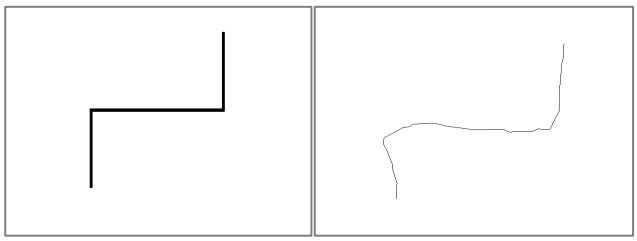


図 5 比較軌跡 1

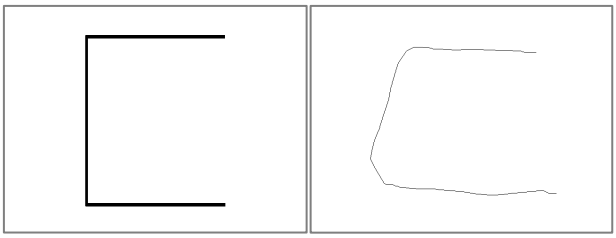


図 6 比較軌跡 2

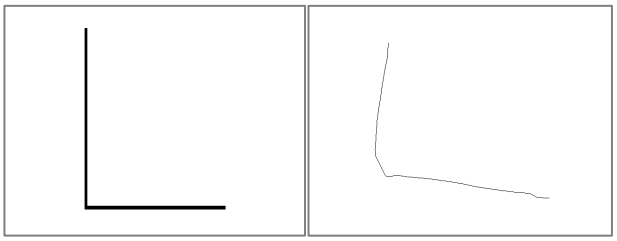


図 7 比較軌跡 3

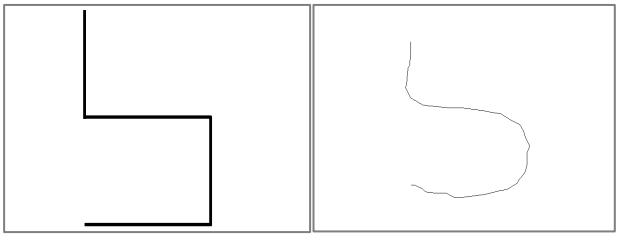


図 8 比較軌跡 4

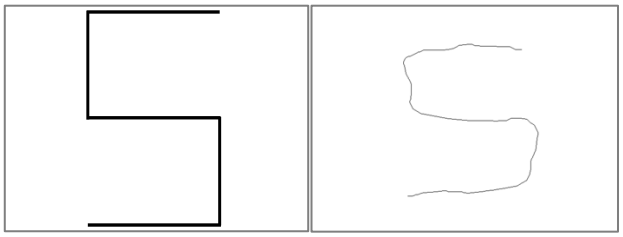


図 9 比較軌跡 5

図 4 とそれぞれの軌跡間のユークリッド距離を算出した結果を表 2 に示す．

図 7 のユークリッド距離の値が大きく，もっとも類似していない．しかし，図 4 と同様な形状を想定した軌跡である図 9 の値と図 5，図 6，図 8 の値が類似した．よって図 4 と図 5，図 6，図 8，図 9 が図 7 より類似している．

表 2 Accelerated-KAZE 特徴点のユークリッド距離

| 図 3 と比較した軌跡 | ユークリッド距離 |
|---|---|
| 図 5 | 18.8547 |
| 図 6 | 18.6837 |
| 図 7 | 21.5042 |
| 図 8 | 17.3418 |
| 図 9 | 17.2991 |

### 4.3 考察

本稿では，局所特徴量を用いることで有効的に特徴量を抽出できると考え，局所特徴量を用いた軌跡の類似度算出を行った．しかし，4.2 節の結果から，図 4 と同様な形状を想定して描画した図 9 と，図 5，図 6，図 8 のユークリッド距離の値が類似した．局所特徴は画像の一部に際立って見られる特徴であるため，対象となる軌跡の一部分を含む軌跡は，局所的に見ると同じ軌跡であると判定された．この結果より，局所的な形状よりも大域的な形状から軌跡の形

状を推定するために大域特徴量を用いることを検討する必要があると考える．また，今回は視線計測装置から収集される，座標群を線で結んだ軌跡の画像を用いて類似度を算出した．座標群のデータを用いて，座標の変化量から形状を推定する手法について検討する必要がある．

## 5. まとめ

本研究の最終目的は，視線軌跡を用いた他人からの推測に対して頑健な個人認証手法の提案である．そのための要素技術として，ユーザが描画した軌跡の形状を推定する．関連研究における視線を認証に用いると認証情報の変更が困難になるという問題に対して，ユーザが視線で描画した軌跡を認証情報に用いた認証を行う．また，認証情報が推測されるという問題に対して，認証情報に用いる視線軌跡はユーザが自身で定義した軌跡を用いる．本稿では，軌跡の形状の推定に有効であると考えた特徴として Accelerated-KAZE 特徴を挙げ，特徴点を抽出し類似度を算出した．

今後は，画像を用いた形状の推定手法だけでなく，座標の変化量を用いた形状推定手法の検討を行う．形状推定を行ったのち，個人描画特徴の抽出の手法を検討する．個人描画特徴と形状推定の結果を用いて個人の認証を行い，評価を行う．

**謝辞**　本研究の一部は東北大学電気通信研究所共同プロジェクト研究による．

## 参考文献

[1] 総務省，情報通信白書平成 29 年，第 1 章第 1 節「スマートフォン経済の現在と将来」，p.2，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/n1100000.pdf，(参照　2018-06-18).

[2]大久保誠也，湯瀬裕昭，指紋認証実験を取り入れた情報セキュリティ教育の試行，情報処理学会研究報告コンピュータと教育(CE)，Vol.2010-CE-103，No.13，pp.1-7 (2017).

[3]Tomi Kinnunen, Filip Sedlak and Roman Bednarik, Towards Task-Independent Person Authentication Using Eye Movement Signals, Proceedings of the 2010 ACM Symposium on Eye-Tracking Research & Applications, ETRA ’10, pp.187–190 (2010).

[4]向井寛人，小川剛史，個人認証を目的とした視線の軌跡情報からの特徴抽出，情報処理学会論文誌デジタルコンテンツ(DCON), Vol.4，No.2，pp.27-35 (2016).

[5]Alexander De Luca, Roman Weiss and Heiko Drewes, Evaluation of Eye-Gaze Interaction Methods for Security Enhanced PIN-Entry,Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces, OZCHI’7, pp.199-202 (2007).

[6]Vijay Rajanna, Polsley Seth and Tracy Hammond, A Gaze Gesture-Based User Authentication System to Counter Shoulder Attacks, Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp.1978-1986(2017).

[7]Laster Kalms, Khaled Mohamed, Diana Gohringer, Accelerated Embedded AKAZE Feature Detection Algorithm on FPGA, HEART2017 Proceedings of the 8th International Symposium on Highly Efficient Accelerators and Reconfigurable Technologies, No10, pp.1-6 (2017).

[8]Pablo Fernadez Alcantarilla, Adrien Bartoli, Andrew J. Davison, KAZE Feature, European Conference on Computer Vision (ECCV) 2012, pp.214-227 (2012).