Vol.2020-DPS-182 No.44
Vol.2020-CSEC-88 No.44
2020/3/13

視線軌跡描画における注視とサッケードの特徴を用いた個人認証手法の検討

藤本巧海 [1,a)]　渡辺泰伎 [1]　白石陽 [2,b)]

概要：近年，ノートパソコンやスマートフォン，タブレットなどのモバイル端末における個人認証の技術として，知識認証とバイオメトリクス認証が普及している．これらの認証情報が漏洩することで，ネットショッピングにおける不正購入や SNS におけるなりすましなどの不正利用の被害に遭う恐れがある．知識認証の脆弱性として，覗き見による認証情報の漏洩が挙げられる．また，バイオメトリクス認証の脆弱性として，認証情報の偽造による，なりすましへの対処が困難であることが挙げられる．これらの脆弱性を解決するために本研究では，視線の動きに着目する．視線の動きは覗き見による推測が困難であり，ユーザが意識的に再現することができる．そのため，ユーザ自身が認証情報として視線軌跡を登録，変更することで，他者からの推測に対して頑健な認証の実現が期待できる．本研究では，ユーザが視線で意識的に描画した軌跡を用いた個人認証手法の提案を行う．提案手法では，描画した視線軌跡の形状と描画特徴による認証を行う．著者らの先行研究では，視線軌跡の形状による軌跡の分類と描画特徴による個人分類を行うための特徴量の検討を行った．本稿では，個人分類の精度向上のための描画特徴として，局所的な視線移動である注視とサッケードに注目した．これらの特徴を用いて個人分類を行い，結果として著者らの先行研究と比較し，分類精度が向上した．また，学習アルゴリズムとして認証者本人のデータのみで学習できる Isolation Forest を用いて，認証者本人か否かの識別を行った．識別精度となる F-measure が 0.73，FAR(False Acceptance Rate)が 0.08，FRR(False Rejection Rate)が 0.27 となり，個人識別において Isolation Forest が有効であると示唆された．

1. はじめに

近年，ノートパソコンやスマートフォン，タブレットなどのモバイル端末が普及している．Web サービスやアプリへのログイン，ネットショッピングなど多くのユーザがモバイル端末による個人認証を行っている．様々な情報がモバイル端末経由で共有されているため，認証情報が漏洩すると不正利用の被害に遭う恐れがある．したがって，モバイル端末における認証の安全性を向上させることが重要となる．

個人認証方式として，知識認証やバイオメトリクス認証が普及しており，モバイル端末における認証にも用いられている．知識認証とは，パスワードや暗証番号などの本人のみが保有する知識を認証情報とした認証方式である．知識認証は，IC カードや鍵などの所有物を認証情報として用いていないため，認証情報を紛失することはない．しかし，駅やカフェなどの公共空間において，パスワードなどの認証情報を入力する際に覗き見される可能性がある．覗き見は攻撃者が専門的な知識を習得していなくても可能なハッキング行為である．そのため，知識認証の認証情報は誰に対しても漏洩する可能性がある．

バイオメトリクス認証とは，身体の一部（身体的特徴）や人間の行動（行動的特徴）を認証情報として用いた認証方式である．身体的特徴とは，指紋や顔などの固有性が高い身体の部位を示す．また行動的特徴とは，人間が持つ様々な行動の癖やパターンであり，本人であれば再現可能な特徴を示す．バイオメトリクス認証は，他者からの覗き見に対して頑健であり，認証情報を記憶する負担が少ない．しかし，身体的特徴を用いた認証では，認証情報として登録している身体的特徴が偽造されるリスクがある．また，認証に使用する指紋や虹彩などの身体的特徴は意識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．一方で，手の動きや歩行などの行動的特徴を認証に用いた場合，身体の一部を認証情報として用いていないため，認証情報の偽造が困難である．しかし，人の無意識な癖などを認証情報として扱う場合には，人が認証情報を意識的に変更することは困難である．よって，バイオメトリクス認証は，なりすましの被害に遭った際に対処が困難になることが考えられる．

モバイル端末で安心して認証を行うためには，知識認証の脆弱性である覗き見により認証情報が漏洩すること，バイオメトリクス認証の脆弱性である認証情報が偽造された場合，認証情報の変更が困難であるため，なりすましへの対処が困難であることを解決することが必要である．これらの脆弱性を解決することを目的とした，身体的特徴を認証に用いた研究[1]，[2]や，行動的特徴を認証に用いた研究[3-5]が盛んに行われている．また，覗き見に対して頑健な行動的特徴を認証に用いた研究として視線移動を認証に用いた研究がある[6-9]．視線移動は腕の動きや脚の動きなどの行動的特徴とは異なり，他者が観測することが困難であり，覗き見に対する頑健性が高いと考える．また，視線移動は人が意識的に再現できるため，認証情報に用いる視線移動を変化させることで，認証情報の変更が可能である．

そこで本研究では，知識認証やバイオメトリクス認証の脆弱性を解決した認証を実現するために，ユーザがモバイル端末の画面上に視線で描画した軌跡（以下，視線軌跡と

1 公立はこだて未来大学大学院システム情報科学研究科
Graduate School of Systems Information Science, Future University Hakodate
2 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) g2119039@fun.ac.jp
b) siraisi@fun.ac.jp

ⓒ2020 Information Processing Society of Japan

呼ぶ）を用いた個人認証手法を提案する．著者らの先行研究[10]では，提案手法の要素技術として視線軌跡の形状の分類と描画特徴の特徴量の検討を行った．視線軌跡の形状の特徴量として，軌跡の画像と座標群データそれぞれから抽出できる特徴量を検討し，座標群データが提案手法に対して有効であることを示した．また，描画特徴として，描画軌跡から大域的な描画特徴を抽出し，個人分類の特徴量として利用したが，十分な分類精度は得られなかった．さらに，認証モデル構築のための学習アルゴリズムの検討が必要であることが課題として挙げられた.そこで本稿では，描画特徴による認証の精度向上のために，描画特徴の再検討を行った．さらに，提案手法の認証モデル構築のための学習アルゴリズムの検討を行った．

以降，2 章では行動的特徴や視線移動を認証に用いた関連研究について述べる．3 章では本研究で提案する視線軌跡の特徴を用いた個人認証手法について述べる．4 章では提案手法に用いる注視とサッケードに関する特徴と異常検知アルゴリズムの提案手法への有効性を評価するために行った実験について述べる．5 章では本論文についてまとめる．

2. 関連研究

2.1 行動的特徴を認証に用いた研究

小宮らは，キーボードの打鍵時間間隔の特徴を用いた認証手法を提案している[3]．打鍵時間間隔とは，キーの押下が開始された時間から，押下されたキーを離し次のキーの押下が開始されるまでの時間である．打鍵時間間隔に個人差が出るように，入力する機会が多いユーザ本人の氏名の入力を解析対象として認証に用いている．

濱野らは，ジェスチャ動作の個人の特徴を用いた認証手法を提案している[4]．この手法では，上下左右や回転させるように振るなどのジェスチャを対象としている．スマートフォン搭載の加速度センサとジャイロセンサを利用し，特定のジェスチャを行った際の特徴を認証に用いている．

伊藤らは，スマートフォンにおけるフリック入力方式の特徴を用いた認証手法を提案している[5]．テキスト入力時のフリック入力方式のタップ動作と上下左右方向のフリック動作を特徴として個人分類に用いている．また，スマートフォン搭載のセンサを用いてテキスト入力時の画面にかかる圧力や端末の揺れの特徴を抽出し，これらの特徴も個人分類に用いている．

文献[3]，[4]，[5]の手法は，ユーザそれぞれの行動に現れる無意識な癖やパターンを認証情報として用いているため，認証情報の変更が困難であり，なりすましへの対処が困難になると考える．

2.2 視線移動を認証に用いた研究

視線移動を認証に用いた研究として，無意識な視線移動を認証に用いた研究[6]と意識的な視線移動を認証に用いた研究[7]，[8]，[9]がある．

無意識な視線移動を認証に用いた研究として，Kinnunen らは，ビデオをディスプレイに表示し，それを見た被験者が行う無意識な視線移動の特徴を用いた認証手法を提案している[6]．字幕付きのビデオを表示し，その際に被験者が行う視線移動から特徴を抽出して認証を行う．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，意識的に認証情報を入力することは難しく，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．そのため，なりすましへの対処が困難であると考える．

ユーザの意識的な視線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う研究[7]，[8]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う研究がある[9]．De Luca らは，視線で PIN(Personal Identification Number)コードを入力する認証手法を提案している[7]．この手法では，ディスプレイ上に表示されたキーパッドの数字を一定時間注視することで PIN コードを順番に入力し，認証を行う．Rajanna らは，ディスプレイ上に表示される記号の中から入力したい記号を一定時間視線で追跡することでパスワードを入力する認証手法を提案している[8]．この手法では，ディスプレイ上に表示された記号を一定時間視線で追跡することで認証を行っている．一方，向井らは，あらかじめ与えられた文字を視線で描画し，その視線軌跡から得られる特徴を用いて，個人識別を行っている[9]．この手法では，認証情報として登録できる文字としてアルファベットと○記号を用いている．登録されている文字を一つ選択し，その文字をユーザが視線で描画する．描画された文字から抽出した特徴を用いて認証を行っている．この手法では，認証情報として登録された文字を変更することで認証情報の変更が可能になる．

文献[7]，[8]，[9]の手法は，認証情報の変更が可能でありなりすましへの対処が可能である．しかし，文献[7]，[8]の手法では桁数が少ないパスワードを認証情報とした場合，攻撃者に推測されやすいと考えられる．文献[9]の手法では，認証情報として利用できる視線軌跡が限られており，他者から認証情報が推測されやすいことが考えられる．

3. 提案手法

3.1 研究目的

本研究の目的は，知識認証とバイオメトリクス認証の脆弱性を解決する視線軌跡を用いた個人認証手法の提案である．視線は目に見える情報ではないため，覗き見や偽造により漏洩するリスクが低いと考える．また，ユーザにより

意識的に視線を再現することができるため，認証情報の変更が可能になる．よって，認証情報の偽造によるなりすましへの対処が可能になると考える．

提案手法は，入力された視線軌跡の形状による認証と視線で描画した際の個人の特徴（以下，描画特徴と呼ぶ）による認証から構成される．視線軌跡の形状は入力するユーザにより意識的に変更が可能であるため，認証情報の要素として視線軌跡の形状を用いることで，認証情報の変更が可能になる．視線軌跡の形状のみを認証情報とする場合，同一の軌跡を描画した異なるユーザが同一のユーザとして識別され，なりすましの被害に遭う恐れがある．よって，描画特徴を用いることで，軌跡の形状の偽造によるなりすましに対して頑健になると考える．

本稿では，先行研究における課題を踏まえて，局所的な視線移動の抽出と 1 対 1 認証を想定した学習アルゴリズムの検討を目的とする．

3.2 提案システム

本節では，提案システムの構成について述べる．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，各フェーズにおいて入力された視線軌跡から特徴量を抽出し，認証情報の登録や認証などを行う．

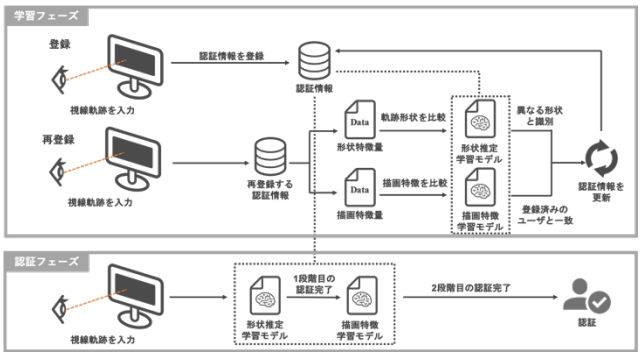


図 1 提案システムの全体像

学習フェーズは視線軌跡を入力し，認証情報を登録するフェーズである．視線軌跡を複数回入力し，軌跡の形状と描画特徴を抽出し認証情報として登録する．また，認証情報の更新も学習フェーズにおいて行う．認証情報の登録時と同様に新たに登録したい視線軌跡を複数回入力することで認証情報の変更を行う．

3.3 研究課題とアプローチ

本研究の研究課題を以下の 4 つとする．

a) 計測デバイスの選定
b) 形状による認証に有効な特徴量の検討
c) 描画特徴による認証に有効な特徴量の検討
d) 1 対 1 認証を想定した学習

課題 a に対するアプローチとして，非接触型デバイスを用いる．視線計測装置としてメガネ型の接触型のデバイスと，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[11]．接触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とってメガネをかけた際の視線の遮りや装着感などが負担になると考えられる．また，本研究では提案システムが将来的にモバイル端末に適用され，端末搭載のカメラを用いて非接触で視線計測を行うことを想定している．非接触で計測を行った場合，デバイスを装着する必要がないため，認証時のユーザの負担が少ないと考える．以上の理由により，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，視線軌跡の座標群データから抽出可能な特徴量を用いる．提案システムでは，ユーザ自身が定義した視線軌跡を用いるため，ユーザがどのような軌跡を描画したかの推定を行う必要がある．著者らの先行研究[10]において，視線軌跡の形状推定に有効な特徴量の検討として座標群データと軌跡画像から抽出可能な特徴量の比較を行い，実験結果から視線軌跡の形状推定においては座標群データが有効であることを示した．座標群データの特徴量を用いた際，分類精度である F-measure が 0.96 となった．よって，座標群データが視線軌跡の形状による認証において有効であることが示唆された．

課題 c に対するアプローチとして，視線軌跡から局所的に抽出した注視とサッケードの特徴を個人分類に用いる．なりすましに対して頑健にするために登録されたユーザが本人か否かを識別するための要素技術として個人分類を行う．著者らの先行研究において，座標群データから視線軌跡の描画の全フレームの座標の変化量を特徴量として用いて個人分類を行った．しかし，特徴量の中に個人分類に有効でない特徴が含まれていた．そこで本稿では，視線移動から注視やサッケードを検出し，特徴量を抽出する．局所的に視線移動を検出することで，個人の特徴がより現れる特徴量が抽出できると考える．

課題 d に対するアプローチとして，異常検知アルゴリズムを用いる．異常検知とは，正常なデータのみを学習し未知のデータを正常か異常か識別する手法である．認証方式として，本人のデータのみを学習し本人か否か識別する 1 対 1 認証と，登録されているユーザのうちの誰なのかを識別する 1 対 N 認証がある．提案手法は個人が保有するモバイル端末に適用することを想定している．よって，提案手法では学習に本人のデータのみを用いる 1 対 1 認証を行う．そこで，異常検知アルゴリズムが提案手法の学習アルゴリズムとして有効であると考える．

本稿では，課題 c と課題 d に着目する．注視とサッケードの局所的な抽出を行い，個人分類に用いることで有効性の評価を行う．また，異常検知アルゴリズムである One Class SVM(Support Vector Machine)と Isolation Forest を用い

て，個人識別への有効性の評価を行う．

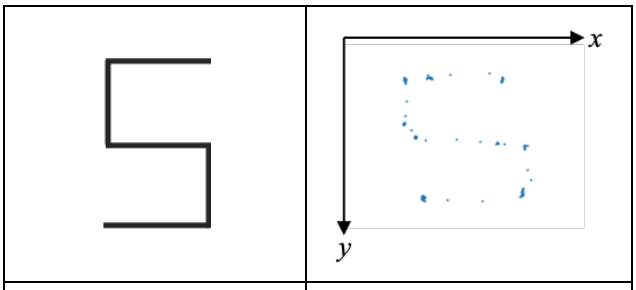
3.4 視線計測デバイスと得られるデータ

本研究では視線計測デバイスとして非接触型のデバイスを用いる．視線計測には機材として Tobii Pro Tx-300（図 2）を用いる．また，計測環境については図 3 に示す．

図 2 実験機材（Tobii Pro Tx-300）

図 3 計測環境

また，収集されるデータの一例を図 4 に示す．



(a) 定義した図形	(b) 座標群データ

図 4 収集したデータの一例

座標群データは座標とそのタイムスタンプが時系列順に記録されたデータを示す．提案手法では，この座標群データに対して前処理を行い，形状による認証に用いる特徴量と描画特徴による認証に用いる特徴量の抽出を行う．

3.5 データの前処理

収集される座標群データをそのまま用いると，視線のブレや注視点などがあり，形状による認証においてノイズになると考えられる．個人識別に用いる描画特徴としては視線のブレや注視が有効であると考えられる．しかし，生データを用いる場合，描画時の視線の大きな乱れが含まれていることもあり，それが外れ値となりノイズになると考えられる．よって，形状推定と個人識別を行う前に座標群データの前処理を行う．

まず，描画された軌跡の全フレームを時系列順に分割する．次に分割された区域ごとに座標の平均化を行い，平均座標群データを算出する．これにより，視線のブレが除去されると考えられる．また，注視による複数の集中した座標が含まれる区域において，平均座標群データを算出することで注視点を除外することが可能であると考える．平均座標群データを算出する際の分割数は，多いほど元の軌跡データの形状情報を維持しつつ大きな外れ値を除外することができる．また，分割数が少ないほど元の軌跡データの概形を維持し視線のブレの削除が可能である．よって，視線軌跡の形状による認証においては分割数を少なく，描画特徴による認証においては分割数を多くした状態で平均座標群データの算出を行う．それぞれで算出した平均座標群データから形状による認証と描画特徴による認証に関する特徴量の抽出を行う．

3.6 抽出する特徴量の検討

本節では，3.5 節で述べた平均座標群データから個人識別に用いる描画特徴について述べる．

3.6.1 個人識別に用いる特徴量の検討

本稿では，局所的な視線移動である，注視とサッケードに関する特徴量を用いる．注視とは視線を固定するために行う視線移動である．また，サッケードとは，ある点からある点へと視線を向ける際の断続的に行われる高速な眼球運動である[12]．提案手法では，これらの視線移動に個人の特徴が現れると考え，特徴量の抽出を行う．

3.6.2 局所的な注視とサッケードの抽出

前処理を行い，算出された平均座標群データから注視とサッケードの特徴量の抽出を行う．

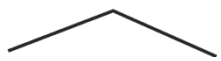
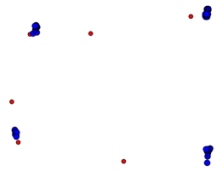
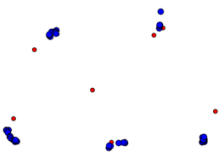
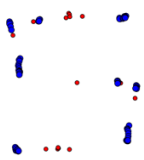
まず，注視の特徴量抽出のために注視の検出を行う．平均座標群からスライディングウィンドウを用いて注視箇所の検出を行う．スライディングウィンドウにより任意の大きさの検出窓を一定のフレーム数ずらしながら注視箇所の検出を行う．検出窓内において，計測された視線の座標が密集している箇所を注視箇所とする．本稿では，5 個以上の点が密集している箇所を注視箇所として検出を行った．検出された注視箇所ごとに注視の特徴量の抽出を行う．

次に，サッケードの検出は，注視箇所ごとに平均座標を算出し，注視箇所のみで形成される注視座標群データを算出する．軌跡描画に伴い，注視とサッケードは繰り返し行われていると考えられるため，注視座標群データの連続す

る 2 フレーム間の座標の変化量を算出することでサッケードの抽出を行う．

提案手法を用いて注視箇所が検出できているか予備分析を行った．提案手法を用いて 4 種の軌跡の平均座標群データから注視を抽出した結果を表 1 に示す．

表 1 軌跡から抽出された注視

描画した軌跡	抽出した注視
	
	
	
	

青の点が注視と判定された視線の計測点を示す．軌跡の開始点，終了点，転折箇所に青の点が密集している．よって，注視箇所が検出できていることが示される．提案手法では，このように抽出された注視箇所を用いてサッケードの検出と，特徴量の抽出を行う．

3.6.3 個人分類に用いる特徴量

提案手法で用いる特徴量と先行研究で個人分類に用いていた特徴量を表 2 に示す．

表 2 個人分類に用いる特徴量

特徴量	提案手法	先行研究
平均座標群データの変化量	○	×
x，y 座標の分散	○	○
x，y 座標の標準偏差	○	○
描画時間	○	○
注視時間	×	○
注視の分散	×	○
注視の標準偏差	×	○
注視の回数	×	○
x，y 方向のサッケードの速度（最大値，最小値，平均）	×	○
サッケードの回数	×	○

提案手法では先行研究と比較し，平均座標群データの変化量を用いない．また，新たに注視とサッケードの特徴量を用いる．平均座標群データの変化量は視線軌跡を描画した全フレームのデータを用いているため，個人分類において冗長な情報が含まれていると考える．そこで，注視とサッケードの特徴量を用いることで，冗長な情報が含まれない視線移動の特徴を抽出できると考える．

3.7 認証モデル構築に用いる学習アルゴリズムの検討

提案手法では，異常検知アルゴリズムを用いて学習を行う．異常検知アルゴリズムを個人認証に用いている研究として，One Class SVM と Isolation Forest を用いた研究がある[5]，[13]．One Class SVM とは，SVM において，正常なデータを 1 クラスとして学習に用いて，未知の入力データが正常か否かを識別する異常検知アルゴリズムである．Isolation Forest とは，ランダムに特徴量と分割点の選択を繰り返し，孤立したデータを異常データとする異常検知アルゴリズムである．本稿では，本人のデータを正常なデータ，他人のデータを異常なデータとして，前述の異常検知アルゴリズムを用いて個人識別を行う．

4. 実験および考察

本章では，4.1 節において視線移動の局所的な特徴を用いた個人分類に関する実験とその考察について述べる．また，4.2 節では異常検知アルゴリズムを用いた個人識別に関する実験とその考察について述べる．

4.1 局所的な特徴を用いた個人分類

注視とサッケードに関する特徴の個人分類に対する有効性を評価するために，Random Forest による 10-分割交差検証を行い，被験者 5 名の分類を行った．各被験者に図 5 に

示す図形を 30 回描画するように指示した．表 2 に，提案手法と先行研究の個人分類に用いる特徴量を挙げる．これらの特徴量を用いて分類を行い F-measure を算出し比較することで，分類精度の評価を行う．加えて，変数重要度を算出することで，有効な特徴量を検討する．実験環境を表 3 に示す．

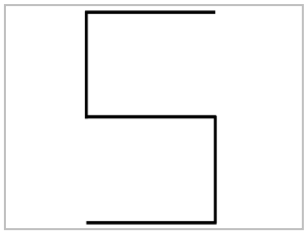


図 5 被験者に描画を指示した図形

表 3 実験環境

項目名	仕様
CPU	Intel Core i5 2.4GHz
OS	macOS Catalina10.15.2
言語環境	Python3.4.5
使用ライブラリ	scikit-learn0.18.1

提案手法と先行研究のそれぞれの分類結果を図 6 に示す．

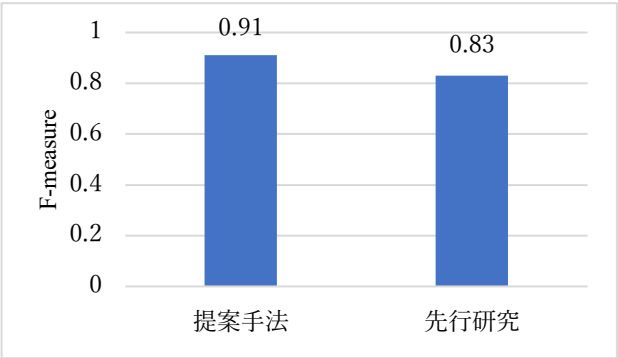


図 6 個人分類結果

提案手法の分類精度は，F-measure が 0.91，先行研究の手法で行った分類精度は 0.83 となり，分類精度が向上した．提案手法で抽出した注視とサッケードに関する特徴量は，冗長な情報が含まれていない．そのため分類精度が高くなったと考えられる．

提案手法の変数重要度が高い上位 10 個の特徴量を表 4 に示す．

表 4 個人分類に用いた特徴量の変数重要度

特徴量	変数重要度	
	提案手法	先行研究
x 座標の標準偏差	1.99	0.56
x 座標の分散	1.69	0.30
x 方向のサッケードの最小速度	1.48	-
x 方向のサッケードの平均速度	0.62	-
描画時間	0.61	0.15
x 方向のサッケードの最大速度	0.55	-
y 方向のサッケードの平均速度	0.45	-
y 方向のサッケードの最小速度	0.44	-
y 座標の分散	0.36	0.17
y 方向のサッケードの最大速度	0.35	-

表 4 より，サッケードに関する特徴量の変数重要度が高く，サッケードが分類に寄与していることが示された．しかし，注視に関する特徴量の変数重要度が低く表 4 に示す上位 10 個に含まれていないため，注視が分類精度に寄与していない結果となった．本稿では，3.6.2 項で述べたように，注視の特徴量を抽出する際に 5 フレーム以上視線が密集していた箇所を注視箇所とした．よって，短時間の注視の場合，5 フレーム未満の注視は注視箇所として検出されないため，注視の個人特徴が十分に抽出できず，変数重要度の値が低くなったと考える．また，x 座標の分散や標準偏差などの提案手法と先行研究の両方で用いている特徴量において，提案手法の変数重要度が高くなっている．先行研究で用いていた平均座標群データの変化量は提案手法では用いていないため，その他の特徴量が分類に寄与したためであると考えられる．

F-measure と変数重要度による評価の結果から，局所的な視線移動の特徴が個人分類に対して有効であることが示唆された．よって分類精度を向上させるために，視線軌跡の局所的な転折部分などの描画特徴を抽出し，追加する必要があると考える．

4.2 異常検知アルゴリズムを用いた個人識別

異常検知アルゴリズムの提案手法への有効性を評価するために，One Class SVM と Isolation Forest を用いて個人識別を行う．各被験者 5 名には図 5 の図形を 30 回描画するように指示した．本実験に用いる特徴量は表 2 に示した提案手法の特徴量を用いる．前述の異常検知アルゴリズムを用いて本人か否かを識別し，識別精度を F-measure，FAR(False Acceptance Rate), FRR(False Rejection Rate)により評価を行う．FAR とは他人を誤って本人と識別する確率であり，FRR は本人を誤って他人と識別する確率である．識別精度の算出として，まず被験者一人のデータを学習データとして，その他の被験者のデータを評価データとし，他

人を他人であると識別するテストを行う．次に，同様の被験者のデータを用いて 10-分割交差検証を行い，本人を本人であると識別するテストを行う．これにより，被験者一人のデータを用いた際の F-measure，FAR，FRR を算出し，同様の手順を各被験者分行う. 最後に F-measure, FAR, FRR それぞれの平均を算出することで識別精度を算出する．識別結果を図 7 に示す.

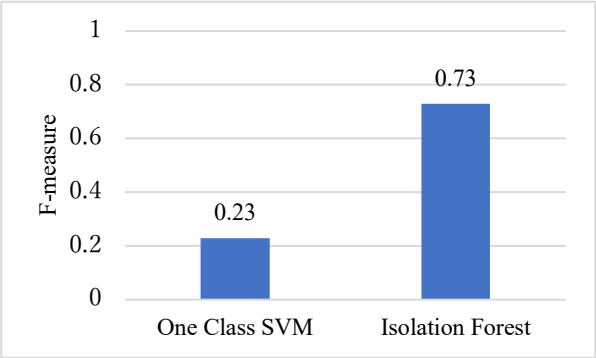


図 7 異常検知アルゴリズムによる個人識別結果

識別精度として F-measure は One Class SVM を用いた場合に 0.23，Isolation Forest を用いた場合は 0.73 となった．

また，それぞれの異常検知アルゴリズムを用いた際の FAR と FRR を示す.

表 5 識別器ごとの FAR と FRR

アルゴリズム	FAR	FRR
One Class SVM	0.00	0.87
Isolation Forest	0.08	0.27

One Class SVM を用いた際の FAR は 0.00，FRR は 0.87 となった．この結果から，FRR の値が 0.00 であるため他人を拒否できているが，FAR の値が高いため本人を他人であると高確率で誤識別していることが示された．また，Isolation Forest を用いた際，FAR が 0.08，FRR が 0.27 となった．この結果から，FRR の値が低いため高確率で他人を拒否している．また，FRR の値は，One Class SVM を用いた場合と比較し低くなっているため，比較的高精度で本人を受け入れている．このような識別精度になった理由として，学習させる本人のデータが少なく，識別に有効な学習モデルが作成できなかったと考えられる．よって，学習データのサンプル数を増やすことが課題となる．F-measure，FAR，FRR を用いた評価から，比較的識別精度が高くなった Isolation Forest が提案手法の学習アルゴリズムとして有効であることが示唆された.

5. まとめ

本研究では，知識認証とバイオメトリクス認証の脆弱性を解決する認証の実現を目的として，視線軌跡を用いた個人認証手法の提案を行う．提案手法では，視線軌跡の形状による認証と描画特徴による認証を行う．本稿では，個人分類の精度向上のために局所的な視線移動である注視とサッケードの特徴量の抽出を行い，新しい特徴量を導入し，個人分類の精度の観点から特徴量の検討を行った．また，提案手法における認証モデル構築に利用する学習アルゴリズムを検討するために，異常検知アルゴリズムを用いて個人識別を行った.

まず，局所的な視線移動である注視とサッケードが個人分類に有効であるかを評価するために，注視とサッケードに関する特徴量を抽出し，個人分類の実験を行った．提案手法と著者らの先行研究の分類精度を比較し，評価した．今回新たに導入した注視とサッケードに関する局所的な特徴量を用いた場合の分類精度は，F-measure が 0.91，先行研究における特徴量を用いた場合の分類精度は F-measure が 0.83 となり，分類精度が向上した．また，変数重要度を算出した結果，サッケードに関する特徴量の変数重要度が高くなっていることが示された．よって，局所的な視線移動に関する特徴が個人分類において有効であることが示唆された.

次に学習アルゴリズムを検討するために，異常検知アルゴリズムである One Class SVM と Isolation Forest を用いて，個人識別の実験を行った．F-measure，FAR，FRR を用いて精度の評価を行い，識別精度が比較的高くなった Isolation Forest が提案手法の学習アルゴリズムとして有効であることが示唆された.

今後の課題として，局所的な視線移動を再検討し，新たな特徴量を追加することで，個人分類精度を向上させる必要がある．また，個人識別において，識別精度を向上させるために学習データの不足を補完する手法の検討が必要であると考える．提案手法の認証精度を評価するために，認証の評価指標である EER(Equal Error Rate)を用いて評価を行う必要がある.

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] 白川功浩，吉浦裕，市野将嗣，虹彩および目の周辺の分割画像を用いた個人認証，情報処理学会論文誌，Vol.59，No.9，pp.1726-1738 (2018).
[2] 藤田真浩，眞野勇人，佐野絢音，高橋健太，大木哲史，西垣正勝，肌理を利用したマイクロ生体認証：ユーザビリティ向上のためのプロトタイプシステム改良，情報処理学会コンピュータセキュリティシンポジウム 2017 論文集，Vol.2017，No.2，pp.704-711 (2017).

ⓒ2020 Information Processing Society of Japan

[3] 小宮崚輔，櫻田ユカリ，中國真教，氏名入力時における打鍵時間間隔の特徴を利用した個人認証，情報処理学会火の国情報シンポジウム 2017，C2-1 (2017).
[4] 濱野雅史，新井イスマイル，加速度センサ・ジャイロセンサを併用したスマートフォンの利用認証手法の提案，情報処理学会研究報告モバイルコンピューティングとユビキタス通信(MBL)，Vol.2014-MBL-70，No17，pp.1-8 (2014).
[5] 伊藤駿吾，白石陽，スマートフォンのフリック入力方式の特徴に注目した継続認証手法の提案，情報処理学会第 25 回マルチメディア通信と分散処理ワークショップ論文集，Vol.2017，pp.1-8 (2017).
[6] 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).
[7] 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).
[8] Vijay Rajanna，Polsley Seth and Tracy Hammond，A Gaze Gesture-Based User Authentication System to Counter Shoulder Attacks，Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems，pp.1978-1986 (2017).
[9] 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).
[10] 藤本巧海，白石陽，視線軌跡の形状と描画特徴を用いた個人認証手法の検討，情報処理学会マルチメディア，分散．協調とモバイルシンポジウム論文集，Vol.2019，pp.1423-1432 (2019).
[11] Tobii Pro アイトラッカーの仕組み，tobii pro，https://www.tobiipro.com/ja/service-support/learning-center/eye-tracking-essentials/how-do-tobii-eye-trackers-work/ (参照 2019-05-06).
[12] 鵜飼一彦, 眼球運動とその種類, 光学(Japanese Journal of Optics)，Vol.23，No.1，pp.2-8 (1994),
[13] 渡辺一樹，長友誠，油田健太郎，岡崎直宣，朴美娘，スマートロックにおける異常検知を用いた二つの端末の加速度における歩行認証の提案，情報処理学会マルチメディア，分散，協調とモバイルシンポジウム論文集，Vol.2019，pp.1155-1160 (2019).

ⓒ2020 Information Processing Society of Japan