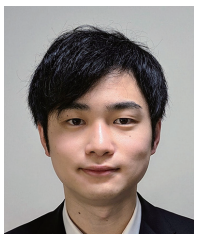
［研究助成（A）］

生体電位を用いたウェアラブルデバイス向け動作認証方式の開発

Development of a Biopotential-Based Motion Recognition Method for Wearable Devices

2221002



研究代表者　産業技術総合研究所　研究員　飯　島　涼

［研 究 の 目 的］

ウェアラブルデバイスによって人の生体データを取得し，活用する時代の到来にさきがけ，ウェアラブルデバイスのセンサで取得可能な生体電位を用いて，個人認証を行う技術の開発を目的とする。従来の認証に残されているセキュリティ問題・ユーザビリティ問題を解決するため，人の動作によって生じた電位から，個人ごとに生じる特徴を抽出し，認証に利用する。他の動作と同時に行える動作に着目し，(1) 早く，(2) 単純で，(3) 誰でも利用可能な動作認証システムを開発・評価する。本認証システムの開発により，従来の顔認証・音声認証と比べてより頑健なセキュリティ認証技術を確立するとともに，体が動かせない人，運転中・料理中など，他の動作中で手が離せない人，声が出せない人など，あらゆる人が動作認証を利用できる世界の実現を目指す。

［研究の内容，成果］

1　まばたきによって生じる電圧を用いたウェアラブルデバイス向け動作認証方式の提案

上記の目的を達成するため，申請の期間内では，「眼電位（ElectroOculoGram，以下 EOG）を用いたウェアラブルデバイス向け動作認証システムの開発と評価」を目標とし，研究・開発を実施した。EOG とは，眼球が動くことによって生じる電位で，両目の間に位置する電極によって取得することができる。VR 向けのヘッドマウントディスプレイや，JINS MEME，AR グラスなど，目の付近に装着するデバイスが普及しつつあるが，ウェアラブルデバイスに最適な認証方式が開発されておらず，認証システムが搭載されていない状態である。EOG の取得には，特別な医療機器を必要としないため，従来の生体電位認証に比べてより安価に実現することが可能である。具体的には，まばたき・ウィンクのような，300 ミリ秒以内に完結する動作によって，生じる EOG の特徴を認証に用いる。本認証方式を BlinkAuth と名づけ，認証方式のデザイン・ユーザスタディ・認証モデルの構築を実施した。

1.1　手法

認証方式のワークフローを図 1 に示す。認証に至るまでの流れは，（i）EOG 計測，（ii）前処理，（iii）特徴抽出，（iv）認証モデル構築の 4 つで構成されている。以下，簡単にそれぞれの手順を説明する。

（i）EOG 計測

データ取得には，JINS MEME Academic

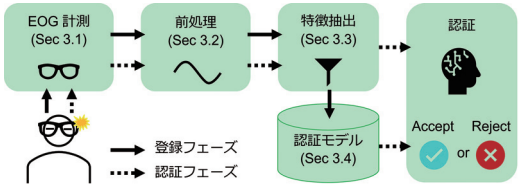


図 1　BlinkAuth のワークフロー

Pack を利用する。EOG 計測のイメージ図を図 2 に示す。JINS MEME においては，メガネの鼻パッド，ブリッジの部分がセンサとなっており，各センサで計測された電位をもとに右目，左目それぞれの電圧を計測する。電圧のうち，縦方向の電圧を EOG_v，横方向の電圧を EOG_h と表記する。本研究では主に，まばたき時に大きなピークを示す EOG_v を対象とし，単に EOG と呼ぶことにする。ユーザスタディによって，31 人を対象に，無意識なまばたき，意図的なまばたき，右目のまばたき，左目のまばたきをそれぞれ 180 回ずつ取得した。

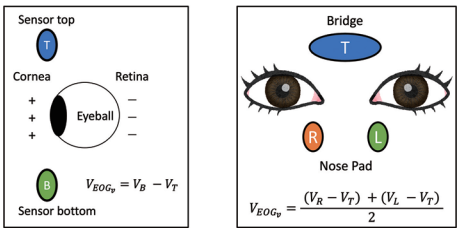


図 2　左：一般的な EOG 計測，右：JINS MEME による EOG 計測

（ii）前処理

（i）によって得られた EOG 波形に対して，まばたき箇所の抽出処理，エラー波形検出・除去処理を実装した。これにより，メガネに生じた振動や，まばたき以外の波形を取り除くことが可能となる。

（iii）特徴抽出

前処理を行った波形から，個人ごとに異なると考えられる特徴を抽出する。特徴抽出の種類として，波形を時間軸でとらえたときに生じる特徴を時系列特徴，FFT による周波数解析によって得られる特徴を周波数数特徴と定め，それぞれ抽出処理を実装した。図 3 に，得られた波形と，波形から得られる時系列特徴のイメージ図を示す。

（iv）認証モデル構築

認証用に用いるモデルは，古典的な非線形モデルとして SVM，決定木を利用したモデルとして Random Forest と XGBoost（以下 XGB），深層学習モデルとして単純な MLP を用いた評

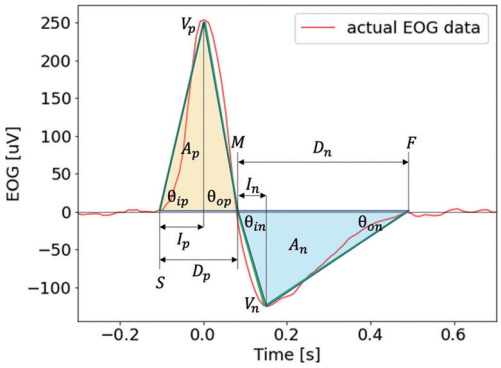


図 3　EOG の波形例と時系列特徴

価を実施した。（iii）で抽出した特徴量を用いて，本人と他人のデータ割合が等しくなるようにアンダーサンプリングを実施した後，学習データ：テストデータ＝8:2 となるように分割した。それぞれのモデルについて，5 段階の交差検証を実施し，さらにグリッドサーチにより，ハイパーパラメータチューニングを実施し，最適なパラメータ条件での評価を行った。

1.2　評価結果

バイオメトリクス分野において，精度・エラー率の計測の際にスタンダードとなっている，ROC（Receiver operating characteristic），AUC（Area under the curve）スコア，EER（Equal Error Rate）によって評価を実施した。AUC，EER はそれぞれモデルのトレードオフを考慮した指標であり，AUC は精度，EER はエラー率を表す。

図 4 に，検証した各モデルの ROC を，表 1 に AUC，EER，F1 スコアを示す。表 1 より，すべてのモデルにおいて，AUC＝95% 以上を達成しており，高精度に認証が可能なモデルを

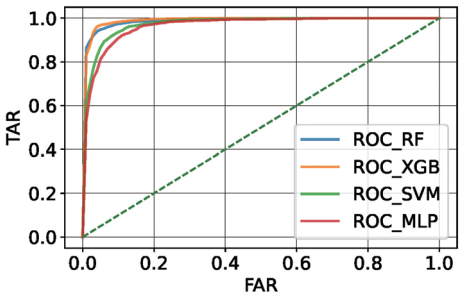


図 4　各認証モデルの ROC

表 1　各認証モデルの評価値

Model	AUC	EER	F1
SVM	0.967	0.0730	0.926
XGB	0.992	0.0347	0.967
RF	0.990	0.0463	0.956
MLP	0.973	0.0632	0.930

構築することが可能である。EER を比較すると，EER＝3.47% となる XGB が最も高精度に認証を行えるモデルであることがわかる。さらなる精度向上のために，まばたき検知アルゴリズムの精度向上，個人間の特徴をとらえた特徴量の増加などが考えられる。

2　EOG 認証　BlinkAuth のユーザビリティ検証

前章までで認証デザイン・基礎評価を実施した EOG 認証方式 BlinkAuth の，リアルタイム認証システムを開発し，パフォーマンス・ユーザビリティ検証を実施した。

2.1　手法

図 5 に，リアルタイム認証方式の実装概要を示す。JINS MEME から EOG データを受け取るソフトウェアを開発し，リアルタイムでまばたき波形検知が行えるよう，queue によるバッファ処理を実施した。バッファ上で検知したまばたき波形に対して，1.1 章で説明した前処理・特徴抽出を行う。認証モデルは，すでに存在する学習データと，あらたに応募した参加者のデータの一部を混ぜることで作成する。

本実験のために新たに 12 人の参加者を募集し，認証にかかる時間，および，認証後に調査したユーザビリティ評価について報告する。ユーザビリティの指標は，HCI 分野でデファクトとなっている SUS（System Usability Scale）を用いて行う。これは，実際にユーザがシステムを利用後に，10 個の質問によってユーザビリティを 100 点満点で評価するものである。さらに，自由記述回答として，Q:「もし BlinkAuth を日常生活の中で使うとしたらどんな場面で利用ができると考えられるか？」を調査した。

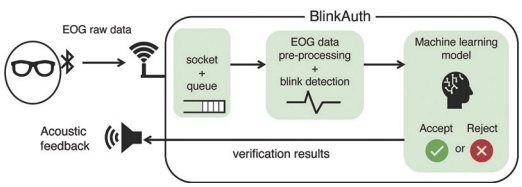
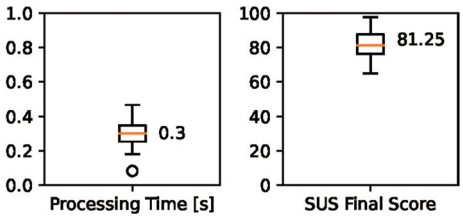


図 5　リアルタイム認証方式の実装

2.2　評価結果

リアルタイム認証による評価結果を図 6 左に示す。認証の処理時間の中央値は 0.3 秒であり，まばたき動作そのものの動作が 0.3 秒であることを考えると，全体で 0.6 秒で完結する認証方式であるといえる。従来ウェアラブルデバイスで用いられている認証方式は，現状 PIN やパスワードの認証が主であるが，その認証時間は，PC 上で 7.5 秒，スマートフォンやタブレット上で約 12.8–13.2 秒かかることがわかっている。ほかの動作認証方式と比較しても，1 秒未満に認証が完結するものは前例がなく，本研究は最も早く完結する動作認証方式と位置づけることができる。図 6 右に，SUS の結果を処理し，100 点満点で評価した場合の結果を示している。SUS の最終スコアは中央値が 81.25 となった。SUS 最終スコアの統計値によれば，SUS が 80.3 を上回るシステムは最上位のユーザビリティとして Rank A とされている。本研究で実装した認証方式は，高精度かつ，ユーザにとっても利用しやすいユーザ認証方式であることが示された。



左：認証の処理時間，右：SUS Final Score の箱ひげ図。
数値はそれぞれ中央値を示している。

図 6　リアルタイム認証の評価結果

さらに，自由記述式回答で得られた認証方式 BlinkAuth の課題と，今後有望であると考えられる利用ケースをまとめる。

Q:「もし BlinkAuth を日常生活の中で使うとしたらどんな場面で利用ができると考えられるか？」

著者らが示した利用例以外に，ユーザの手がふさがった状況下での利用例について提案が多く見受けられた。例えば，「スマートフォンやカードをタッチする代わりに，まばたきで改札やチケットゲートを通れるようにしてほしい」(User ID 58)，「手がふさがっているときに，家やホテルのオートロックをまばたきで解除したい」(User ID 44) といったコメントがあった。そのほか，お年寄りや子どもなど，パスワードに理解のない・覚えることが難しい層への普及などが含まれていた。その他の自由記述回答に対する考察は成果 [2] および投稿中の国際会議論文に示している。

3　EOG 認証のロバスト性検証

前章までで，基礎評価，ユーザビリティ評価により，BlinkAuth の実現可能性を評価した。本章では，実世界で生じうる利用上の変化に対してどの程度ロバストであるかを確認するための追加検証を実施した。具体的には，(1) 時間による経時変化の影響，(2) なりすまし攻撃の評価，(3) 肌状態の変化による影響 (4) 運転中など，動作中に BlinkAuth を利用した場合の影響，の 4 つの観点から調査した。本報告書では，ページの都合上 (1) の結果を掲載する。

3.1　時間による経時変化の影響

動作によって得られる生体信号は，時間によって変化することが指摘されている。時間経過によって生体信号に変化があると，認証する際の誤り率の増加につながるため，そのような現象が起こりうるかをあらかじめ計測する必要がある。本研究では，同じ日付中に，時間を変えて計測した場合を Short period，異なる日付で後日計測した場合の評価を Long period とし，評価を実施した。

Short Period：13 人の実験参加者に対して，10:00, 12:00, 14:00, 16:00, 18:00 の 5 回に分けて，180 個ずつのまばたきデータを収集する。その際の認証モデルのエラー率の変化を見ることで，時間ごとの傾向を明らかにする。図 7 に，各時間のエラー率を示している。Time は時系列特徴のみ，Frequency は周波数特徴のみ，All は両方を合わせて利用した場合のエラー率となっている。All に着目すると，10:00 から 16:00 にかけて徐々にエラー率が下がり，18:00 に 0.5–1 % 程度エラー率が上昇していることがわかる。10:00–16:00 にかけては，ユーザが認証動作に慣れることにより，動作が安定し，結果として精度向上につながったと考えられる。この結果から，ユーザが早く動作になれるための認証データ登録インタフェースデザインが重要となる。さらに，18:00 のエラー率上昇からは，遅い時間帯となり，ユーザの疲れがまばたき動作に影響を及ぼす可能性が示唆される。

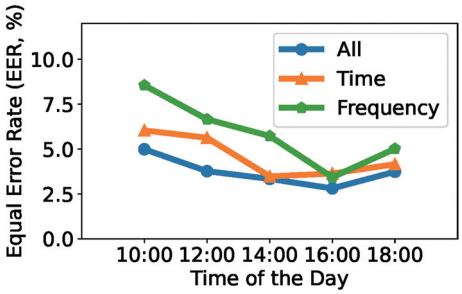


図 7　Short period 評価におけるエラー率の変化

Long Period：1 章で募集した 31 人に対して，7–10 日後に，1 章と同様のデータ計測を行い，その際のエラー率を検証する。図 8 に，1 回目のデータ計測の結果（Base，1 章参照）と，後日行った 2 回目の結果（1 week later）を示す。結果より，2 回目の計測では，5.42% 程度 EER が増加していることがわかる。これは，参加者が 7–10 日間の間，一度も認証を意識したまばたき動作を行わなかったためであると考えられる。

精度向上のための対策：疲れ目や，長時間認証を行わないことにより，精度が低下する可能性について言及した。対策として，ユーザが認証動作を行うたびに，試行データをもとに認証モ

デルを更新する incremental learning や online training を行うことが考えられる。疲れている状態や，風邪等の状態で同様の動作が行えない場合，長時間認証動作を行わなかった場合のデータなど，あらゆる状況でデータ取得が行い，逐次学習により認証モデルを改善することが望ましい。

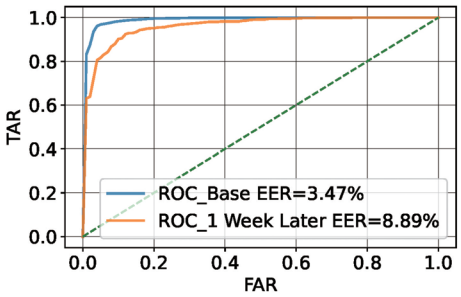


図 8　1 回目の計測と，2 回目の計測での ROC，EER 結果

4　認証方式のフレームワーク化・筋電位認証への応用

BlinkAuth で作成した認証ワークフロー（図 1）について，ほかの生体電位でも利用できるよう一般化・フレームワーク化を行い，筋電位（EMG）による認証においても同様に利用可能であることを示している（成果 [3] 参照）。今後，フレームワークの公開，BlinkAuth の実利用化，EMG 認証のロバスト性・ユーザビリティ評価などが課題となる。本研究で得られた生体信号処理の知見にもとづき，生体信号周辺に存在するセキュリティ・プライバシー問題の解決に向けた研究開発を今後も推進する予定である。

最後に，本研究に対する立石科学技術振興財団の研究支援に心より感謝申し上げます。

［成果の発表，論文など］

［1］ **Ryo Iijima**, Tatsuya Takehisa, and Tatsuya Mori. 2022. Cyber-Physical Firewall: Monitoring and Controlling the Threats Caused by Malicious Analog Signals. In the proceedings of 19th ACM International Conference on CF '22, May 17–19, 2022

［2］ 飯島 涼，竹久達也，大木哲史，森 達哉，まばたきによって生じる電圧を用いた認証方式の提案，コンピュータセキュリティシンポジウム 2022, 2022 年 10 月　**CSS2022 優秀論文賞受賞**

［3］ 渡部晃久，飯島 涼，森 達哉，手首の表面筋電位を用いたスマートウォッチ向けジェスチャ認証方式，情報通信システムセキュリティ研究会（ICSS2023），2023 年 3 月

その他，[2] をセキュリティ系国際会議に投稿中.