Vol.2015-CSEC-69 No.32
Vol.2015-IOT-29 No.32
2015/5/22

表面筋電位を用いた個人認証手法の実現に向けた基礎研究

山場 久昭[1,a)]　長友 想[1]　油田 健太郎[2]　久保田 真一郎[1]　片山 徹郎[1]　朴 美娘[3]　岡崎 直宣[1]

概要：近年，スマートフォンやタブレットのようなモバイル端末の普及に伴い，覗き見によって認証に必要な情報が第三者に取得されてしまてしまうことが問題となってきている．これを解決する技術として，指紋などの生体情報を用いた生体認証が注目されている．本論文では，そのひとつである筋電位を用いた個人認証について検討を行う．具体的には，前腕部の筋電位の波形が手首から先の手の動き（ジェスチャー）によって異なる波形を示すことを利用し，そのジェスチャーを組み合わせてパスワードとして用いる手法を提案する．今回は，個人認証に用いる生体認証として筋電位が利用可能であるのか，筋電位の波形からジェスチャーを判断することができるのか，また，それを計算機上に行わせるのが可能かどうかについて検討を行ったので，報告する．

キーワード：モバイル端末，ユーザ認証，覗き見攻撃，筋電図

Basic Studies for Realizing User Authentication Method Using Surface Electromyogram Signals

Abstract: At the present time, mobile devices such as tablet-type PCs and smart phones have widely penetrated into our daily lives. Therefore, an authentication method that prevents shoulder surfing is needed. We are investigating a new user authentication method for mobile devices that uses surface electromyogram (s-EMG) signals, not screen touching. The s-EMG signals, which are generated by the electrical activity of muscle fibers during contraction, are detected over the skin surface. Muscle movement can be differentiated by analyzing the s-EMG. In this paper, a series of experiments was carried out to investigate the prospect of an authentication method using s-EMGs. Specifically, several gestures of the wrist were introduced, and the s-EMGs generated for each motion pattern were measured. We compared the s-EMG patterns generated by each subject with the patterns generated by other subjects. As a result, it was found that each subject has similar patterns that are different from those of other subjects. Thus, s-EMGs can be used to confirm one's identification for authenticating passwords on touchscreen devices.

Keywords: mobile devices, user authentication, shoulder surfing attacks, electromyogram

1. はじめに

近年，スマートフォンやタブレットのようなモバイル端末の普及に伴い [1]，覗き見によって認証に必要な情報が第三者に取得されてしまい，容易に認証を突破されてしまうという問題が起きてきている．これらの端末には電話帳やメールといった個人情報が格納されている．そこでそれらの情報の漏洩を防ぐため，画面ロックをかけ，その解除にあたっては，それが所有者のみ可能とし，第三者によって解除がされないよう，個人認証が必要となるようにしている．しかし，既存の認証方式，PIN や Android 端末に採用されているパターン認証などは覗き見耐性が不十分である．

この問題を解決するためには，覗き見されてもユーザ以外が認証を突破できない，または，覗き見されない形で認証ができる認証システムが必要である．それを可能とする技術として指紋などの生体情報を用いた生体認証が注目されている．

本論文では，生体認証のひとつである筋電位 [2], [3] を用

[1] 宮崎大学
University of Miyazaki
[2] 大分工業高等専門学校
Oita National College of Technology
[3] 神奈川工科大学
Kanagawa Institute of Technology
[a)] yamaba@cs.miyazaki-u.ac.jp

ⓒ 2015 Information Processing Society of Japan

いた認証が実現可能かどうかの基礎的な検討を行った結果を報告する．近年，前腕部の筋電位の波形が手首から先の手の動き（以下，ジェスチャー）によって異なる波形を示すことを利用し，筋電位を用いてジェスチャーを判断して車椅子を制御するという試み [4] などが行われている．本研究ではそのジェスチャーを組み合わせてパスワードとして用いる手法について検討する．

今回は，個人認証に用いる生体認証として筋電位が利用可能であるか，筋電位の波形からジェスチャーを判断できるのか，また，それを計算機上に行わせるのが可能かどうかを調べた．具体的には以下の三つについて検討を行った．

(1) 同一人物が同じジェスチャーを行ったときに得られる各筋電位が，全て同じような波形になるのか，また，同じジェスチャーでも人物が変われば異なる波形になるのか？
(2) ある人間がいくつかのジェスチャーをとったときの筋電図が与えられた状態で，当該の人物の新たな筋電図が提示されたときに，それがどのジェスチャーによるものだったのかを判定できるか？
(3) 波形の特徴を何らかの数値として抽出し，その数値を用いることで，上の (2) の判定を計算機上で実現できるか？

以下，モバイル端末の個人認証の課題，筋電位，筋電位を用いた個人認証手法，実験，考察の順に述べる．

2. モバイル端末の個人認証

本章では，モバイル端末の個人認証の課題と，本論文で対象とする攻撃手法の録画攻撃について述べる．そして，従来の認証方式と，近年注目を浴びている生体認証についての特徴について，いくつか説明する．

2.1 モバイル端末の個人認証の課題

現在，モバイル端末の個人認証として広く用いられている PIN 認証やパターン認証などは，覗き見攻撃に弱い．すなわち，第三者に覗き見られた場合パスワードなどの認証情報を盗まれやすく，容易にロックを解除されてしまう．

近年では，特に，録画攻撃にどう対応するかが問題となっている．録画攻撃とは認証画面と操作盤を撮影し，後でその映像記録から秘密情報を解析，取得するという方法である．人間による覗き見攻撃については認証操作を複雑にすることで対応が可能であるが，録画攻撃への対策は容易ではない [5].

録画攻撃への対策として，生体認証情報の効果が期待される．生体認証とは指紋や虹彩，筋電位などの人間の特徴をパスワードとして用いる認証方法である．生体情報は個人に特有のものであり偽ることが困難なので，個人認証の手法として有効である．

2.2 覗き見攻撃

覗き見攻撃とは，正規ユーザの認証行為を覗き見ることで暗証番号やパスワードといった秘密情報を不正に取得する方法である．近年この攻撃はその実行主体が人間からビデオカメラを用いた手法に変わりつつある [5]．例えば，ビデオカメラを用いて認証画面と操作盤を撮影し，後でその映像記録から秘密情報を解析，取得するという方法がある．認証を行う際の対策が必要とされている．録画攻撃への対策としては他人に覗き見られることのない環境で認証動作を行うという事が挙げられる．しかし我々の生活環境にはいたる所に監視カメラが設けられており，意図的でなくとも認証動作を録画されてしまう恐れがある．以上のことから，覗き見攻撃への対策手段としては，覗き見を困難にさせることの他にも，覗き見をされた場合にも安全性の確保ができるようにする対策が必要であると言える．

2.3 従来の認証方式

2.3.1 パスワード認証

従来，計算機の認証方式には主にパスワード認証が用いられてきた．パスワード認証とは，数字やアルファベットを組み合わせたものをパスワードとして用いる認証方法である．この認証方式は，文字列の長さによってセキュリティの向上を図ることができるが，長くなるにつれ，ユーザビリティが下がってしまう．また，自分の誕生日や覚えやすいパスワードを設定すると，攻撃者による推測が容易になり，認証を解除されてしまう恐れがある．そのため，一般には英数字を組み合わせた 8 文字以上のパスワードが推奨されている [6].

2.3.2 PIN コード認証

Personal Identification Number(PIN) とは，本人確認のために用いられる秘密の識別番号である [7]．あらかじめ設定しておいた PIN と入力が一致した場合に認証を成功させる認証方式 PIN コード認証と呼ぶ．スマートフォンの画面ロックをする際に用いられる他にも，銀行やインターネット上での個人認証を行う際の認証など幅広く利用されている認証方式である．PIN コード認証には，認証動作を他者にのぞき見られた場合に容易に突破されるという問題がある．

2.3.3 パターン認証

パターン認証とは，Android に標準搭載されている認証方式で，画面上の 9 つの点を指でなぞり，点と点とを結ぶパターンを認証情報とする認証方式である．使用するパターンは，9 つの点のうち 4 つ以上の点を通過しなければならない，同じ点は 1 度しか通過できない，というルールの下で，自由に設定することができる．そのため，単純なパターンであればユーザビリティが高めることも，複雑なパターンであればセキュリティを高めることもできる．

ただし，そのパターンを見ることができれば，それを記

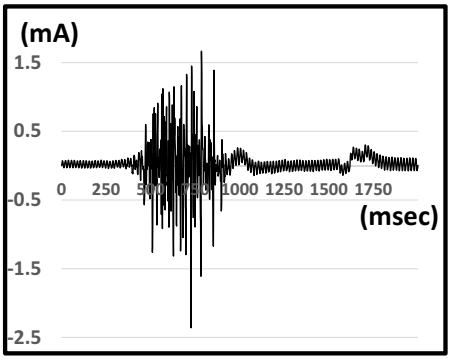

図 1 筋電図の例
Fig. 1 A sample of electromyogram signals.

憶するのが比較的容易であるため，第三者にのぞき見られた場合に，認証情報が容易に奪われてしまうという欠点がある．

2.4 生体認証方式

生態認証技術とは人間の身体的特徴や行動的特徴を用いて本人認証を行う技術であり，バイオメトリクス認証とも呼ばれる．上記した PIN コードのような暗証番号やパスワードに比べてなりすましが困難であることから，より強固なセキュリティを有した認証技術であると期待されている [8].

2.4.1 指紋認証

指紋認証とは現在用いられている生態認証技術の中で最も普及している認証技術であり，幅広い場面に用いられている認証手法である．指紋を構成している凹凸の高さや形状といった要素を個人の特徴として認証を行う．指紋の形状は千差万別であり高い認証精度を誇りながら，認証に用いる機器のコストが比較的安価で済むという特徴がある．しかし，指が荒れていたり乾燥していることで認証がうまくいかない場合がある [9]．また，ゼラチンで偽造した指紋つきの指で認証を突破することが可能であるという報告もされており課題が残っている．

2.4.2 虹彩認証

虹彩とは角膜と水晶体の間にある環状の領域であり，生まれてから約 2 年で形成され，それから変化することはない．そのため，認証に用いる際に，経年劣化による認証の不具合が生じることはない．また虹彩には個人差があり複雑な模様であるため，偽造が困難であることから高い認証精度を誇る．これらの特徴から，既にオランダやイギリスの空港では虹彩認証を用いた出入国手続きが行われている [10]．しかし，認証中に動いたり目を逸らすと認証できない場合がある．また，虹彩認証は認証の際に動いたり目を逸らすと認証できない場合があるなど，取り扱いのしやすさの点で課題がある．

3. 筋電位

筋電位とは，脳から送られた信号が筋線維に伝達された際に生じるものであり，ニューロン（神経細胞）が細胞内外の電位を変化させることで生じる一時的な細胞内外の電位差の逆転のことである．筋電位は筋電計を用いることで測定することが可能であり，皮膚表面で計測した筋電位のことを表面筋電位と呼ぶ．観測された電位の変化は図 1 のような筋電図として記録できる．これを surface electromyogram(s-EMG) という [11].

さて，観測される筋電位はどの筋肉をどのように動かすかによって異なるものをとる．例えば，前腕部で観測される筋電位は，「どの指を動かすのか」などによって変化する．筋電位を記録することで運動のパターンを分析して筋肉の状態が異常であるか正常であるかの診断をしたり，筋の張力の状態を知ることが可能である．

この性質から，筋電位は障がい者を支援するヒューマンインターフェイスの開発にも活用されている．例えば Tamura 等は，顔の皮膚表面から得られた筋電位を表面筋電計を用いて測定・解析して表情筋の動作を推定し，その動作を入力として用いることで車椅子を制御する，ハンズフリー車椅子の開発 [4] を行っている．

4. 筋電位を用いた個人認証手法

4.1 提案する認証手法の基本的な考え方

本論文では，手首から先を動かした時に観測される筋電位を筋電計で測定し，得られた波形を用いて個人認証を行う手法について検討を行う．具体的には，ジェスチャーごとに得られる筋電位の波形が異なることを利用して，いくつかのジェスチャーを連続して行うことをパスワード（認証情報）として用いる．この時，筋電計で測定して得られた波形には個人差があるので，認証動作を見られて，その攻撃者がまったく同じジェスチャーを再現したとしても，認証突破することができない．

例えば，図 2 の一連のジェスチャーを認証のパスワードとして選んだとする．そして，そのジェスチャー毎に得られる波形（図 3）をモバイル端末上に登録しておく．すると，ジェスチャーを登録した所有者が認証操作を行った場合，図 4 に示すような，登録されている（一連のジェスチャーの）筋電位の波形と似た波形が測定され，認証に成功する．しかし，第三者が同じジェスチャーで認証動作を行ったとしても，筋電計で測定して得られた波形には個人差があるので，図 5 のような異なる波形が測定され，ロックを解除することができないことが期待できる訳である．

さらに，認証に筋電位を用いることには，覗き見をされずに認証操作を行うことができるという利点もある．すなわち，タッチパネルを目視して確認しながら認証動作を行

ⓒ 2015 Information Processing Society of Japan

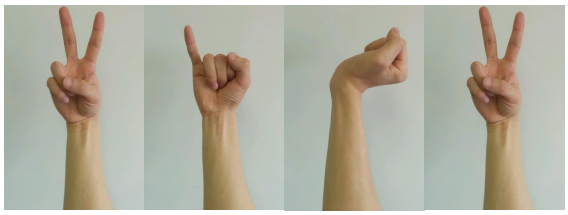

図 2 登録したパスワード（ジェスチャー列）例
Fig. 2 An example of a registered password (a list of gesterus).

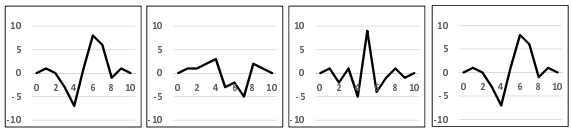

図 3 対応する筋電図
Fig. 3 The correspoinding electromyograpms.

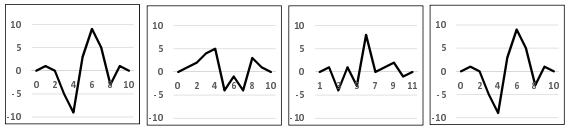

図 4 所有者が入力した認証動作を測定した波形の例
Fig. 4 An example of input electromyograms generated by the owner.

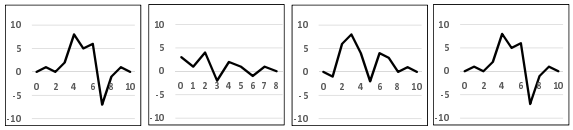

図 5 攻撃者が入力した証動作を測定した波形の例
Fig. 5 An example of input electromyograms generated by another.

う（例えば，パスワードや PIN 入力する）必要がないので，ポケットの中のような人目にふれない環境での認証が可能になる．これによって，更に覗き見攻撃に対する安全性を確保することができると考えられる．

4.2 認証のための計算機システムへの課題

筋電計で測定して得られた波形の識別を人間が行うのが容易であったとしても，それを利用した認証システムをモバイル端末上で実現するには，その識別を実現できる計算機システムを開発しなければならない．そのためには，(1) 表面筋電図の特徴を的確に捉えた特徴量の抽出と，(2) 抽出された特徴量同士を比較して，二つの波形が似ているか否か，すなわち，同じジェスチャーであるか否かを判定する手法が必要となる．一般には高速フーリエ変換を用いて表面筋電位の特徴抽出を行い，ニュラルネットワーク等を利用してた得られた特徴量の比較を行い、ジェスチャーを特定しようとする接近法が多い．ただしその弱点として，計算のコストが大きいことが挙げられる．

Tamura 等は，波形が取る最大値と最小値との差 (Peak to Peak) を筋電位の特徴として用いる手法が，算出は容易であるにもかかわらず，高い識別率を示すことを報告している [4]．そこで本研究でも，これを参考にして，各筋電図の持つ特徴量としてこの Peak to Peak を採用し，検討を進めている．

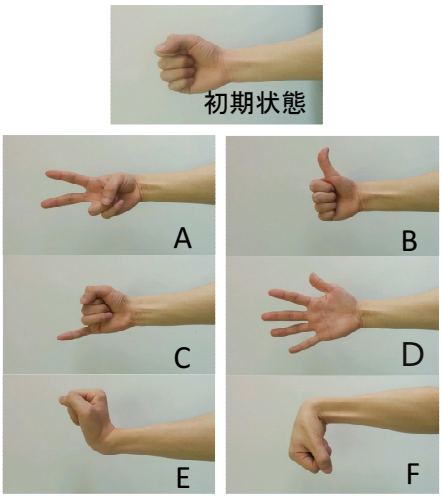

図 6 実験に用いたジェスチャ
Fig. 6 The gestures introduced into the experiments.

5. 実験

本節では，以下の二つについての実験を行う．

(1) 同一人物が同じジェスチャーを行ったときに得られる各筋電位が，全て同じような波形になるか
(2) ある人物のいくつかのジェスチャーをとったときの筋電図が与えられた状態で，当該の人物の別の筋電図（ただし，当該ジェスチャーのいずれか）が提示されていたときに，それがどのジェスチャーによるものか判定できるか

5.1 筋電位の測定

今回の実験で必要となるデータとして，筋電位の測定を以下のように行った．

今回はでは図 6 に示す A〜F の 6 パターン（チョキ，親指，小指，パー，手の甲側に向けてひねる，手の平側に向けてひねる）のジェスチャーの測定を行った．

拳を軽く握った状態を初期状態として，そこからそれぞれのジェスチャーを取る，という動作を行った時の筋電位を測定した．各ジェスチャー毎に，この動作を 5 回ずつ繰り返した時の筋電位を測定し，それを 1 セットとして，同じ実験を 1 週間の間隔を空けて 2 回行った．すなわち，被験者 1 人の 1 つのジェスチャーにつき 2 セット，合計 10 回ずつの筋電位を測定した．この測定では，宮崎大学工学部生 12 名を被験者として採用した．

測定の様子を図 7 に示す．筋電計を机に置き，椅子に座った状態で筋電位の測定を行った．電極は，手のひらを

ⓒ 2015 Information Processing Society of Japan

表 1　実験に用いた機器とソフトウェア
Table 1　The instruments and the software used in the experiments.

電極	筋電センサ（DL-141）
データロガー	バイオログ（DL-3100）
計測ソフトウェア	m-Biolog

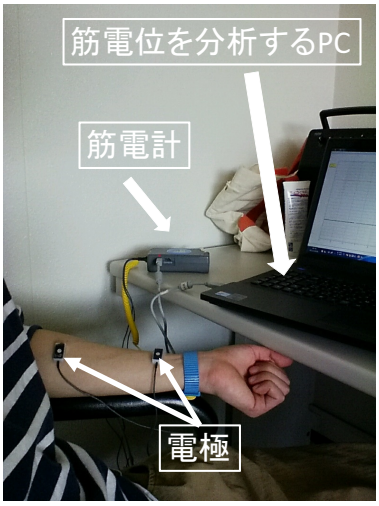

図 7　実験を行っている様子
Fig. 7　A scene of the experiment.

上に向けた状態で手の付け根から腕に向かって 6cm の位置と手の付け根から 18cm の位置にそれぞれ 1 つずつ貼った．この位置は，どの位置に電極を貼ると波形が表れやすいのか，予備実験に基づいて決定した．また電極を貼る際に専用のクリームで皮脂を除去し，アルコール綿でクリームをふき取ることで皮膚と電極の接触抵抗を小さくした．

実験で用いた機器を表 1 に示す．いずれも S&M 社の機器である．

5.2　筋電位を認証に用いる可能性の確認

同じ被験者の同じジェスチャーの波形が互いに似ているかどうか，5.1 で得られた筋電図を用いて比較を行った．72 組のデータ（12 名× 6 ジェスチャー）それぞれについて，1 回目に計測した波形と 1 週間後に計測した 2 回目の波形を実験者が見比べ，形状に着目して，似ているかどうかの判定を行った．判定は人間の目で比較し，行った．ただし，計測した波形のうち，大きなノイズを含んだ波形は測定失敗として判定の対象外とした．その結果を表 5.2 に示す．正しく計測された波形のうち，約 84.6%が似ているという結果になった．

一方，同一の被験者の異なるジェスチャー同士の比較も同様に行った．被験者 1 人につき，異なるジェスチャー同士の組み合わせが 60 組あるので，被験者全員で 720 組の波形の比較を行った．その結果，ジェスチャーが異なるにも関わらず，似た波形になったものは全体の約 1%程度であった．

表 2　同一人物の同じジェスチャーの波形の比較結果
Table 2　The comparison of electromyograms generated by the same people.

似ている	55/72
似ていない	10/72
計測失敗	7/72

さらに，異なる被験者間での，同じジェスチャーの波形同士の比較も同様に行った．各被験者それぞれの各ジェスチャーについて 22 組（自分以外の被験者 11 名×実験数 2）の波形と比較したところ，結果として，ほとんどの波形の形状に個人差があり，似ている形状の波形は全体の約 1 割程度であった．

5.3　筋電図からのジェスチャーの予測実験

対応するジェスチャーが不明な筋電図を，それが既知の筋電図群と比較することにより，当該のジェスチャーを予測できるかを調べる実験を行った．具体的には，学生 7 人を被験者として次の実験を行った．被験者には，図 6 のジェスチャー A，B，C（チョキ，親指，小指）の 3 パターンのジェスチャーの波形の 1 回目に測定した波形（図 8）を見せておく．その上で，その 3 つのジェスチャーの中から 1 つのジェスチャーの 2 回目の波形（図 9）を提示し，そのジェスチャーが最初に見せたどのジェスチャーのものであるか判定してもらった（正解は小指）．この実験は各被験者に対して 2 回行った．結果として，7 名全員が 2 回とも正しい答えを出すことができた．以上から，筋電位を用いた個人認証が原理的には十分可能であることが示された．

6.　考察

筋電位の測定から得られた筋電図同士を比較することにより，以下が確認できた．

- 同一人物の同じジェスチャーからはほぼ同じ波形が得られる．
- 同一人物であっても，異なるジェスチャーからは異なる波形が得られる．
- 同じジェスチャーであっても別の人物からは異なる波形が得られる．
- 筋電図の波形パターンの情報から，限定された条件の下でではあるが，人間はその筋電図の元のジェスチャがなんであったかを判定することができる．

この判定を機械に行わせるという点については，特徴量には波形の最大値と最小値の差（P to P）を採用した上で，被験者の測定データ群に重回帰分析を施し，そこから得られた係数と切片を用いて，ジェスチャの判定を行う手法を試行しているが，十分な性能出すまでには至っていない [12]．その理由としては，重回帰分析を行う際に目的変

ⓒ 2015 Information Processing Society of Japan

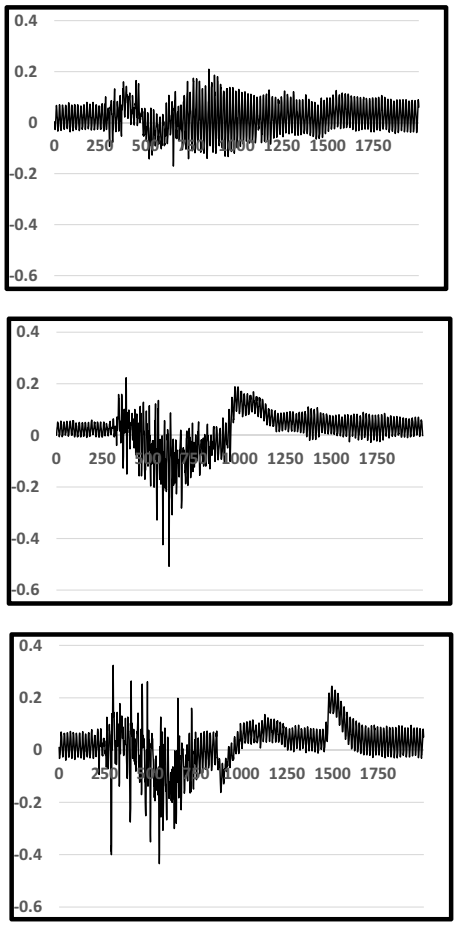

図 8 被験者に事前に示しておいた筋電図（上：チョキ　中：親指　下：小指）

Fig. 8 The s-EMGs shown to the experimental subjects in advance.

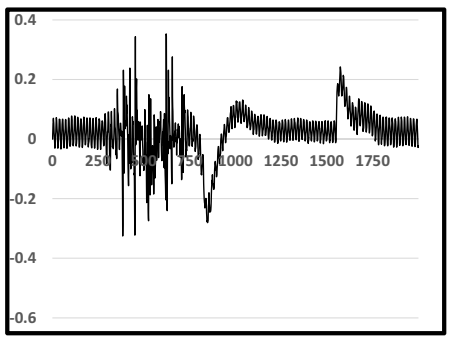

図 9 判定対象とした波形

Fig. 9 The s-EMG required to be identified.

数をすべての P to P の平均値としたことや，特徴量に P to P のみを用いたこと，重回帰分析を適応することそのものの限界などをあげられており，今後は主成分分析やニューラルネットを用いた手法を検討することが考えられる．

7. おわりに

本論文では，表面筋電位を用いた個人認証手法の検討を行った．筋電位を認証に用いることがそもそもの可能なのか，筋電図からジェスチャーを予測できるか，機械上でジェスチャーの判断ができるかの 3 つについて検討した．実験の結果，筋電位を認証に用いることの可能性と，筋電図からジェスチャーを判断することができることは示されたが，機械上でその判断を行わせる時の性能は，今回用いた手法の範囲では不十分であることが分かった．今回は筋電位を認証に用いることが可能かどうかの検証を行ったので，今後は機械上でジェスチャーの識別ができるシステムの構築に努めたい．

参考文献

[1] インターネットの普及状況
入手先 ⟨http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc253110.html⟩
[2] 宮川大毅，朝倉義裕：簡易表面筋電位測定システムに関する研究，神戸高専研究紀要第 48 号, pp.51-56 (2010).
[3] 神経細胞と静止膜電位,
入手先 ⟨http://www7b.biglobe.ne.jp/~homunculus/neuro/neurophysiology/S1.html⟩
[4] Tamura, H., et al：A Study of the s-EMG Pattern Recognition Using Neural Network, International Journal of Innovative Computing, Information and Control, pp.4877-4884, 2009.
[5] 和斉薫：モバイル端末向け個人認証方式における柔軟な安全性強度の実現手法に関する研究, 宮崎大学大学院修士論文 (2015).
[6] 石黒司，福島和英，清本晋作，三宅優：モバイル端末のロック解除向けパターン認証の安全性評価，電子情報通信学会技術研究報告．ICSS，情報通信システムセキュリティ．pp.272-278 (2012).
[7] 西坂健太郎，寺田真敏，土居範久：携帯電話を対象とした PIN 認証向け日本語パスワードの提案．情報処理学会研究報告．IPSJ，マルチメディア通信と分散処理研究会報告．pp.1-8 (2010).
[8] 妹尾一郎，厚井裕司，貞包哲男，中谷直司，馬場義昌，鹿間敏弘：生体認証によるネットワーク個人認証システム，情報処理学会論文誌．pp.1111-1120 (2003).
[9] 指紋認証装置によるテスト環境対策および偽造指紋への耐性試験
入手先 ⟨http://www.cac.co.jp/softechs/pdf/st2601_10.pdf⟩
[10] もうすぐ「目」が「パスポート」の時代が来る…!?
入手先 ⟨http://www.senju.co.jp/consumer/resteye/zatsugaku/007.html⟩
[11] 新・筋電センサ MiniBioMuse-iii,
入手先 ⟨http://nagasm.org/ASL/SIGMUS0108/⟩
[12] 長友想：表面筋電位を用いた個人認証手法の検討, 宮崎大学工学部卒業論文 (2015).

ⓒ 2015 Information Processing Society of Japan