

スマートフォンのモーションセンサを利用した
個人認証アプリケーションの開発に関する研究

総合情報学研究科

知識情報学専攻

マルチメディア情報システムの基礎と実際

15M7112

高坂 賢佑

要旨

スマートフォンの普及により，従来型のフィーチャーフォンと呼ばれる端末と比較して多種多様なサービスを利用できるようになった．例えば，スマートフォンはパーソナルコンピュータ向けに設計された **Web** サイトを閲覧できるフルブラウザが利用できる．これを用いることで，オンラインショッピングを含むサービスをどこでも手軽に利用できるようになった．またスマートフォンは，様々な企業や個人が開発した多種多様なアプリケーションを自由にインストールし利用できる．例えば国内銀行各社からスマートフォン向けアプリが提供されているが，これを用いることでアプリ内で口座残高の確認や入出金明細の確認はもちろん，振り込みや振り替えなども行える．このようなサービスを利用する際には，あらかじめ登録したユーザ名とパスワードを用いた個人認証を行うのが一般的である．だがこれら情報をアプリ内に記憶しておくことで，利用毎に再入力する手間を省けるような仕組みを持つ場合もある．

このようにスマートフォンによって日々の生活がより豊かになった一方で，端末がより多くの個人情報を内包するようになった．このことから，第三者によって不正に個人情報にアクセスされたり，インストールされたアプリを通じて様々なサービスをなりすまし利用された場合の危険性は高くなった．そのため，端末利用時にはパスコード認証や指紋認証などを用いて本来の端末所有者であるか認証するよう設定することが推奨されている．

現在スマートフォンにおいて個人の認証方式として広く使われている方法として，パスコード認証と指紋認証が挙げられる．しかしながらこれら認証方式にはいくつかの問題点が考えられる．まずパスコード認証では認証作業が煩雑であったり認証に用いる鍵情報の自由度が低いという点がある．また指紋認証では指紋を読み取るためのハードウェアが必要である点や，指紋情報は変更ができないため，何らかの原因でこの情報が第三者に漏洩した場合はその指紋を用いた個人認証ができなくなるという点がある．

そこで本研究ではスマートフォンに一般的に搭載されている加速度センサと角速度センサを利用し，人間の動きを用いて端末を振ることで個人を認証するシステムを開発した．本シス

テムでは，認証時に入力されたデータが本来の端末所有者本人によるものを識別するために，人工ニューラルネットワークを利用した．端末所有者はあらかじめ認証時に利用したい動きをシステムに入力し，登録処理を行う．登録処理では，まず **Denoising Autoencoder** を用いて入力されたデータの特徴を学習し，その後 **Denoising Autoencoder** の後ろに識別を行うニューロンを繋いで学習を行う．認証時には，登録処理で得られた識別器を用いて入力されたデータが端末所有者本人のものであるかを識別する．

評価の結果，云々．本システムにより，パスコード認証が抱える認証の煩雑さと鍵情報の自由度といった問題点を軽減した．また指紋認証における鍵情報が変更できないという問題点を解消し，直感的に個人認証を行うことが可能になった．

目 次

第 1 章 序論	1
1.1 研究背景	1
1.2 研究目的	2
1.3 本論文の構成	2

图 目 次

表 目 次

第1章 序論

1.1 研究背景

近年，スマートフォンと呼ばれる携帯端末が急速に普及しつつある．スマートフォンとは，パーソナルコンピュータ向けに設計された Web サイトを閲覧できる機能を持つフルブラウザを搭載し，様々な企業や個人が開発した多種多様なアプリケーションをインストールし利用できる携帯端末のことを指す [1]．平成 28 年版の情報通信白書によるとスマートフォンの世帯普及率は 2015 年末時点で 72.0%とあり，また前年比で 7.8 ポイント増となっている [2]．スマートフォンの普及によりどこでも手軽にオンラインショッピングやネットバンキングをはじめとする多種多様なサービスを利用できるようになった．

その一方で，これらサービスの利用にはユーザ ID やパスワード等を含む個人情報を用いた個人認証を必要とする場合が多い．また，利用しているブラウザやアプリケーションによっては，サービスにログインすれば一定期間ログイン状態を保持し再ログインの手間を省くような機能を持つものもある．この機能により，ユーザはサービスを利用するたびに再ログインする手間が無くなることから利便性が向上する．しかしながら，悪意のある第三者がサービスへのログインに必要な情報を知らずとも，本来のユーザになりすましてサービスを利用できてしまうという危険性がある．

このように，スマートフォンは従来型のフィーチャーフォンと比較してより多くの個人情報を内包しており，第三者からのこれら情報への不正なアクセスを防ぐための仕組みが不可欠となっている．現在この仕組みを実現する方法として広く採用されているのが，端末利用時にあらかじめ登録したパスコード情報や指紋情報をもとに，現在の利用者が本来の端末所有者であるかを確認する個人認証システムである．パスコード認証方式では，あらかじめ端末所有者が特定の文字種からパスコードを構築し，これを端末に登録しておく．そして，端末利用時に入力されたパスコードと登録されたパスコードを比較して同一であれば端末所有者であるとみなして，その後の端末利用を許可する．指紋認証方式では，あらかじめ端末所有者が端末に搭

載された指紋読取機を通じて自らの指紋をスキャンし、これを端末に登録しておく。そして、端末利用時に指紋をスキャンして登録された指紋との比較をし、同一であれば端末所有者であるとみなしてその後の端末利用を許可する。これらの個人認証システムを利用することにより、第三者によって不正に端末内の個人情報へアクセスされる危険性のある程度軽減できる。しかし、これらの認証方式にはそれぞれいくつかの問題点が挙げられる。

まずパスコード認証方式だが、これは個人認証を行う際にスマートフォン画面上に表示されたソフトウェアキーボードを目視し指でタッチして操作する必要がある、ユーザにとっては煩雑である可能性があるという点がある。またあらかじめ決められた文字種の中から一つずつ選んだ文字を並べてパスコードを構築することから、パスコードのパターン数が限られ、認証に用いる鍵の自由度が制限されてしまうという点がある。

指紋認証方式については指紋をスキャンするためのハードウェアをスマートフォンに搭載しなければならないという点がある。また指紋情報は変更ができないため、何らかの原因でこの情報が第三者に漏洩した場合は、今後その指紋を用いた個人認証ができなくなるという点がある。さらに、ドイツのハッカー集団である **Chaos Computer Club** の生体認証チームが、一般的なカメラで撮影された写真に写り込んだ指から指紋を複製することに成功している [3]。このことから、指紋情報が漏洩する可能性が十分にあり個人認証システムが担う機密性の確保が難しいといえる [4]。

1.2 研究目的

本研究では、一般的なスマートフォンに搭載されている加速度センサと角速度センサを利用し、端末を振る動き（以下、モーション）で個人認証を行うシステムを開発する。これによりパスコード認証方式における認証作業の煩雑さと鍵情報の自由度が制限されるという課題点を軽減し、指紋認証方式における指紋情報が漏洩した場合に鍵情報の変更ができないという課題点を解消した生体認証システムの実現を目指す。

1.3 本論文の構成

第2章にて本研究に関連する先行研究について述べる。第3章では本研究で開発した個人認証システムを提案するにあたり必要となる知識について説明する。第4章では本研究で開発した個人認証システムの実装について、その詳細を述べる。第5章では本研究で開発した個人認証システムの評価実験とその結果を示し、第6章で結論と今後の課題を述べたあと、本論文を総括する。

参考文献，参考URL等

- [1] 総務省 | 電気通信サービスF A Q（よくある質問） | スマートフォンとはなんですか？，
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_faq/faq01.html，2017 年 1 月 27 日確認.
- [2] 総務省，“平成 28 年版情報通信白書”，2016 年.
- [3] CCC — Fingerprint Biometrics hacked again,
<https://www.ccc.de/en/updates/2014/ursel>，2017 年 1 月 27 日確認.
- [4] Chaos Computer Club claims to have “cracked” the iPhone 5s fingerprint sensor Naked Security, <https://nakedsecurity.sophos.com/2013/09/22/chaos-computer-club-claims-to-have-cracked-the-iphone-5s-fingerprint-sensor/>，2017 年 1 月 27 日確認.