M-039

フリック入力における個人特性を利用した認証強化方法の検討

A Study of Authentication Improvement with Individual Characteristics for Flick Input

岡田 春菜 † **鬼木 明日香** ‡ **佐藤 健哉** ‡
Haruna Okada Asuka Oniki Kenya Sato

1 はじめに

近年，メールやインターネットショッピングなどで個人の認証にパスワード認証が使われる機会が多くなっている．パスワードを他人に知られてしまうことや，パスワードの忘却，使いまわしなど，パスワード認証の問題点が多くある．そこで，指紋や静脈など，個人で固有のものとされるものや動作で認証を行う生体認証が注目されている．

スマートフォンは我々にとって欠かせない存在となっている．今回，スマートフォンで文字を入力する際の個人の特徴を用いた，新たな認証方法を提案する．多くの人が日本語入力の時にフリック入力 [1] を使うだろう．フリック入力の際，どのくらい指を移動させるか，どの程度スマートフォンが動くのか，個人で違いがあるので，この特徴量を認証に使用することができる．

また，スマートフォンにはさまざまなセンサーが搭載されている．そこで，文字を入力した時に関係するフリック入力の特徴量と加速度センサー・ジャイロセンサーの二つのセンサーで検知できる手の動きの特徴量により認証する．

2 提案システム

2.1 概要

今回提案するシステムは，文字入力時にフリック入力の特徴と加速度センサー及びジャイロセンサーで検知した特徴量から個人を判別する．

まず，フリック入力の特徴は，フリック入力の速さ，どの程度はじくか，を算出する．

次に加速度センサー・ジャイロセンサーの特徴量は，ある文字を入力したときに，スマートフォンがどの程度空間移動をするか，どの程度回転移動するか，を算出する．

ユーザが入力している間，画面上の軌跡・加速度センサー・ジャイロセンサーのセンサー値の検出をする．そのデータの特徴量と事前に算出した本人の特徴量データを照らし合わせ，認証する．

2.2 システムの構成と条件

システムの動作手順を図 1 に示す．

- **スマートフォン**
  画面上の軌跡・加速度センサー値・ジャイロセンサー値をとる．

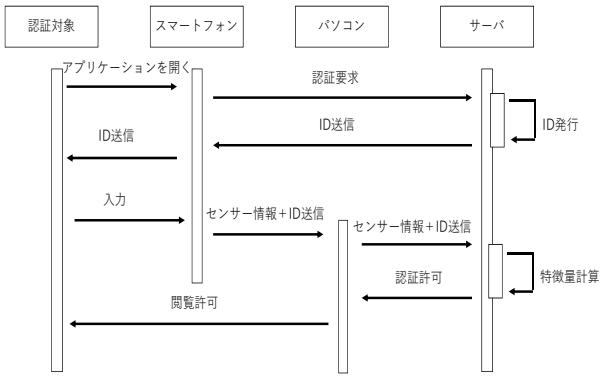

図 1 システムの動作手順

- **パソコン**
  スマートフォンで検出したセンサー値から特徴量を受け取り，サーバに送信する．
- **サーバ**
  パソコンから受け取ったセンサー値から特徴量を算出し，認証をする．

2.3 認証の手順

システムの動作手順を図 1 に示す．

(1) スマートフォンのアプリケーションからサーバにアクセスする．
(2) サーバから認証要求と ID をスマートフォンに送る．
(3) スマートフォンで文字入力を行う．
(4) スマートフォンからパソコンにセンサー値を Blootooth で送信する．
(5) パソコンからサーバにセンサー値と ID を送信する．
(6) サーバで特徴量計算と認証を行う．
(7) サーバからパソコンに閲覧許可を発行．
(8) パソコン側でログイン可能となる．

2.4 認証アルゴリズム

以下の項目を特徴量として計算する．

- **画面上の軌跡**
  画面上の軌跡のデータを一文字ずつに区切り，始点と終点の座標の平均と 2 点間の距離を算出する．

$$x_i\ ,\ y_i \quad (i = 1, ...N)$$

† 同志社大学 理工学部 情報システムデザイン学科
‡ 同志社大学大学院 工学研究科 情報工学専攻

- **加速度センサー**
  3 軸方向の加速度データを 1 文字ずつに区切り，0.01 秒ごとに N 個取得して，加速度の向きを 3 軸ベクトルとして，算出する．

$$x_i\ ,\ y_i\ ,\ z_i \quad (i = 1, \ldots N)$$

平均 (2・3 軸方向)

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

- **ジャイロセンサー**
  ジャイロセンサーは，1 文字ごとの 3 軸方向のジャイロデータを 0.001 秒ごとに N 個取得して，最大値と最小値の差を算出する．

$$x_i\ ,\ y_i\ ,\ z_i \quad (i = 1, \ldots N)$$

最大値の平均

$$\begin{cases} x_i > \bar{x}\ ,\ x_i > x_{i-1}\ ,\ x_i > x_{i+1} \\ x_{i,Max} =, max\{x_{i-5}, x_{i-4}, \ldots, x_{i+5}\} \end{cases}$$

を満たす $x_{i,Max}$の平均値.

最小値の平均

$$\begin{cases} x_i < \bar{x}\ ,\ x_i < x_{i-1}\ ,\ x_i < x_{i+1} \\ x_{i,min} =, min\{x_{i-5}, x_{i-4}, \ldots, x_{i+5}\} \end{cases}$$

を満たす $x_{i,min}$の平均値.

最大値の平均－最小値の平均

$$X = x_{i,Max} - x_{i,min}$$

上記の項目ごとに，事前登録データとの誤差を算出し，各誤差を重み係数を掛けて足し合わせることで全体誤差を算出する．全体誤差が設定した閾値よりも低ければ，正規ユーザと判定する．

3 評価

事前条件として，「ふりっく」という文字を 5 回入力し，特徴量を算出しておく．今回 5 名のデータを用いて，特徴量を算出した．本評価では，スマートフォンを右手に持った状態で行う．画面上の軌跡は，図 2 で示したように 5 名の個人の特徴が表れていた．加速度センサー値から，図 3 のようにデータをまとめることができる．同様に”り”，”っ”，”く”の 3 文字からも個人の特徴が現れ，個人を特定することができた．ジャイロセンサー値からは各文字のセンサー値の最大値と最小値を算出すると，個人の違いが表れた．5 回の事前登録情報との誤差に重み付けをし，閾値を決定し，個人の認証を行った．

4 まとめ

- **ユーザの認証時の動作負担**
  スマートフォンで文字入力をするだけで認証が完了する．
- **不正アクセス**
  提案システムを利用すると，スマートフォンを覗き見されることや，パスワードを忘れて困ることもなくなる．また，パスワードの使いまわしの問題も解決できる．

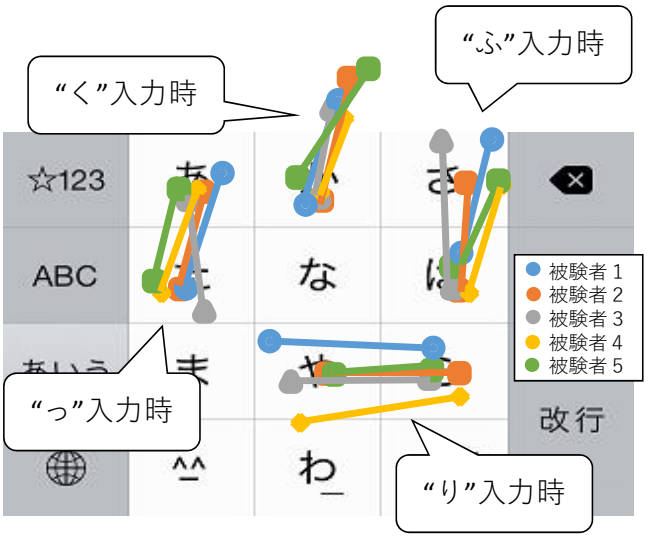

図 2　画面上の軌跡

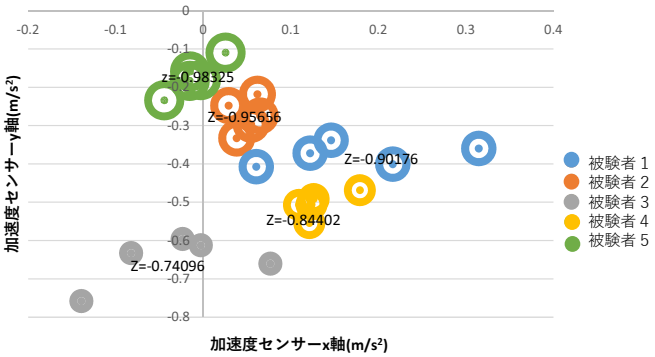

図 3　加速度センサー値（”ふ”入力）

データベースの情報が漏えいした場合でも，登録特徴量を直接使用して認証はできず，指定されたスマートフォンによるセンサ入力を行うことでのみ認証される．

今回の提案システムを用いることで，手の動きと端末の動きにより，個人によって差が認められた．この差を用いることで，個人の特定が可能であることが確認された．今後は機械学習を用いることにより，認証ができることを目標とする．

スマートフォンで文字入力をするという日常的な行為を認証に活用することで，ユーザの動作負担を解消するとともに，セキュリティの向上を考えた．

参考文献

[1] 平岡, 佐村, 西村，テキスト入力によるキーストロークダイナミックス, 情報知識学会誌, pp.63-68, 2006.