フリック入力を利用したスマートフォンの個人認証システム

沼沢 誠† 千石 靖‡

†‡金沢工業大学大学院工学研究科システム設計工学専攻
921-8501 石川県野々市市扇が丘 7-1
† makoto-n@jupiter.kanazawa-it.ac.jp
‡ sengoku@neptune.kanazawa-it.ac.jp

あらまし スマートフォンの利用者は若者を中心に増え続けている。しかし、多くのデータを保存することのできるスマートフォンの個人認証手段はいわゆるガラパゴス携帯電話の方法とほとんど同じであり改善が必要と考えられる。そこで、本研究では新たな個人認証手段としてキーボードで用いられているキーストロークダイナミクス認証をスマートフォンの一般的な入力方法であるフリック入力に応用する。この個人認証は入力者の指の移動量と文字入力にかかる時間を認証基準として本人確認を行う。このシステムはスマートフォンのフリック入力で認証を行うため特別な認証機器が不要であり、利用者の負担を増やさずにセキュリティを向上させることができる。

キーワード：スマートフォン、個人認証、キーストロークダイナミクス認証、フリック入力

The personal authentication system using a flick input of a smart phone

† Makoto Numazawa ‡ Yasushi Sengoku

†‡ Graduate Program in System Design Engineering, Graduate School of Engineering,
Kanazawa Institute of Technology
7-1 Ohgigaoka, Nonoichi, Ishikawa 921-8151, JAPAN
† makoto-n@jupiter.kanazawa-it.ac.jp
‡ sengoku@neptune.kanazawa-it.ac.jp

Abstract The users of a smart phone are continuing increasing in number focusing on a young man. However, it is thought that a personal authentication means of a smart phone by which many data can be saved is almost the same as the method of the conventional mobile phone, and needs to be improved. So, in this research, the keystroke dynamics attestation used by the keyboard as a new personal authentication means is applied to the flick input which is the general input method of a smart phone. This personal authentication performs personal identification by making time concerning the movement and character input of a finger into an attestation standard. This system can raise security, without special attestation apparatus being unnecessary in order to attest by the flick input of a smart phone, and increasing a user's burden.

keywords：smart phone, personal authentication, keystroke dynamics attestation, flick input

1　背景と目的

現在、スマートフォンは、若者を中心にシェアを伸ばしている。株式会社アイ・エム・ジェイのモバイル端末の保有動向に関する調査 [1] によると、20 代でスマートフォンのみを所有している人は 52.1%とガラパゴス携帯電話(日本独自で発展した携帯電話)のみを所有している人の 40.2%を上回っている。全年齢でもスマートフォンのみを所有している人は 40.9%とガラパゴス携帯電話のみを所有している人の 51.8%に近づいてきている。

しかし、スマートフォンでの個人認証システムはガラパゴス携帯電話とそれほど変わっていない。また、スマートフォンが高性能であるがために盗難にあった場合の被害はガラパゴス携帯電話より大きくなる恐れがある。そこで、本研究ではスマートフォンの個人認証システムのセキュリティを向上させるため、フリック入力を利用した個人認証システムの認証基準の考案と、その認証基準を作るためのプログラムとして Android の画面ロックシステムの構築を行う。

2　既存システム

既存システムについて述べる。

2.1　画面ロックシステム

現在の Android の画面ロックシステムは 3 つある。1 つ目は PIN と呼ばれる数字だけのロックシステムであり、4 ケタ以上 16 ケタまでを設定できる。2 つ目はパスワードと呼ばれる英数字､記号を 4 文字以上 16 文字まで使用できる認証方法である。3 つ目はパターンと呼ばれる認証方法であり、4 つ以上の点を通ること、点を通れる回数は各 1 度だけのルールで、縦に 3 つ横に 3 つの計 9 つの点から自分の決めたルートを描いて画面ロックを解除する方法である [2] 。

これらの画面ロックシステムはパスワードが短いと推測されやすく、長いと入力が手間になることや忘れてしまうという問題がある。しかし、これらの画面ロックシステムは Android 端末のみで行え、指紋認証などに必要な特別な装置が不要という利点もある。そこで、Android に標準で備わっている画面ロックシステムの持つ利便性を残しつつ、セキュリティの向上したシステムを提案する。

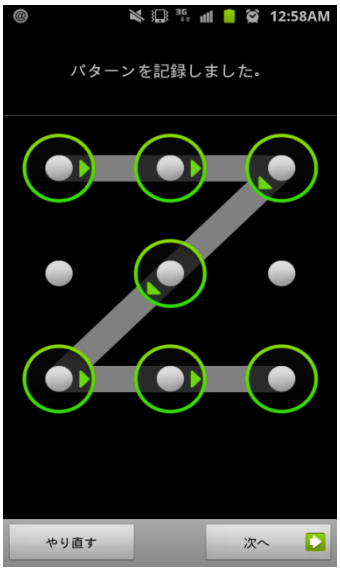

図 1　パターンによる画面ロック

2.2　フリック入力

フリック入力とは、スマートフォンなどのタッチスクリーンで採用されている日本語入力方式である。見た目はテンキーのように、あ段（あかさたなはまやらわ）が配置されており、各キーの上下左右に（い段、う段、え段、お段）が隠れて配置されている。あ段のキーから上下左右にスライドさせる（弾く）ことで､文字を入力ができる機能 [3] である。

フリック入力はガラパゴス携帯電話で多く使われていた入力方法であるトグル入力に比べ慣れれば高速で文字を打つことができるため、スマートフォンユーザーに利用者が多い入力方法である。

図 2　フリック入力

3　関連研究

佐村敏治氏がスマートフォンを用いた日本語入力によるキーストローク認証という研究を行っている [4] 。また、梅津亮氏、ベッド B.　ビスタ氏、高田豊雄氏がスマートフォンにおけるキーストロークダイナミクスを用いた個人認証方式に関する一検討という題名で暗号と情報セキュリティシンポジウム [5] で発表を行っている。本研究はこれらとは独立して開発を進めており、後日比較検証を行う予定である。

4　提案システム

提案システムのデータの説明や画面ロックシステムの要件について述べる。

4.1　認証基準のためのデータ

認証基準はフリック入力に、キーボード入力で存在しているキーストロークダイナミクス認証を応用し、作成する。キーストロークダイナミクス認証とはキーボードで文字を入力する際の癖で、登録した本人が利用していることを連続的に確認する技術 [6] である。フリック入力がキーボード入力と同じく個人によって入力の癖があると仮定し、フリック入力によって本人確認を行う。

具体的にはフリック入力時に指の移動により取得することのできる座標と指がキーを押してから離すまでの時間や次のキーを押すまでの時間の 2 つを認証基準とする。

初回に認証基準となる情報を登録し、以降の認証成功時には成功した情報を最も新しい認証基準として登録し、最も古い情報を破棄する。これにより利用者の入力の変化に対応する。

この認証システムは通常のパスワードのメリットである特別な機器が不要な点や変更が容易であるという利点を持っている。なおかつ、パスワードの情報が漏れてしまっても本人と同じ入力をすることが難しいという利点がある。

認証基準の詳細は 4.5 節で述べる。

4.2　画面ロックシステムの要件

画面ロックシステムの要件を以下に示す。

- Android の画面ロックでの使用を想定して構築する。
- パスワードは 8 文字以上 16 文字以下とする。
- パスワード入力はひらがなで行う。
- パスワードのあ段を 1 文字までとする。
- 認証基準はフリック入力時に取得する座標とキーを押す時間とする。
- パスワード入力に失敗した場合は最初からやり直さなければならない。
- 初回に 10 回の入力を行い認証基準とする。
- パスワードは任意で変更可能であり、変更時に再度 10 回入力を行う。
- 認証成功時に取得したデータを次回の認証データとし、最も古いデータを削除する。

パスワードの入力をひらがなにするのは、実験を行う際に被験者の多くが普段から入力することの多いフリック入力の入力方法がひらがなだと想定したからであり、英字入力でも認証は可能である。

あ段を 1 文字までとするのは、あ段は指を動かさずに入力するので座標が変わらず、タッチする時間も他人と違いが出にくいため、個人を判別することが難しいからである。

パスワード入力に失敗した場合に最初からやりなおさなければならないのはキーを押す時間を認証基準としているため、入力に失敗した場合に時間の取得ができないためである。

これらの要件を元にシステムの構築を行う。

4.3　画面ロックシステムの入力画面

図 3 は現在構築中の画面ロックシステムの入力画面である。

図 3　画面ロックシステムの入力画面

この画面でパスワードを入力した際にパスワードが一致し、かつパスワード入力時に指の移動により取得することのできる座標データと指がキーを押してから離すまでの時間や次のキーを押すまでの時間があらかじめ登録していたデータの認証基準を満たせば認証成功となる。

4.4　認証基準のためのデータ

表 1 はパスワード入力時に取得することのできるデータを表にしたものである。

表 1　パスワード入力時のデータ(例)

	X移動値/dp	Y移動値/dp	押すまで/ms	離すまで/ms
1文字目	56	3		69
2文字目	74	23	314	82
3文字目	9	140	349	103
4文字目	30	107	225	119
5文字目	1	2	253	117
6文字目	59	20	253	92
7文字目	0	0	227	45
8文字目	94	27	278	94

「X 移動値」はパスワードを入力する際にキーを押してから離すまでに移動したX座標の値、「Y 移動値」はキーを押してから離すまでに移動した Y 座標の値である。「押すまで」は前のキーを離してからキーを押すまでの時間、「離すまで」はキーを押してからキーを離すまでの時間である。1 文字目の「押すまで」にデータがないのはシステムが 1 文字目を押してから時間の取得を行うからである。

4.5　認証基準

認証基準はあらかじめ登録してある10個のデータで作成する。このデータの平均と標準偏差を求める。xは認証のために入力したX移動値とし、μ は登録しておいた1文字目のX移動値10個の平均の値、σ は登録しておいた1文字目のX移動値10個の標準偏差とする。xが

$$\mu - K\sigma \ < \ x \leqq \ \mu + K\sigma \quad (1)$$

であった場合に1文字目のX移動値が登録してある本人と判断する。なおKは今後行う計測実験で本人拒否率、他人受入率のデータを収集し決定する。

この方法を座標データ16個、時間のデータ15個全てに行う。そして、座標データ16個中L個入った場合と時間データ15個中M個入った場合の両方を満たした場合に本人と判断し認証成功とする。L、Mも今後行う実験により決定する。

5　今後行う実験

実験により本人拒否率、他人受入率と 4.5

節の認証基準 K、L、M を決めるためのデータを収集する。

- 実験はスマートフォンでフリック入力を普段から利用している人､複数を対象とする。
- パスワードは全員「せいろくめんたい」で固定する。
- 最初に10回入力し､データを登録してもらう｡その後､認証のために10回パスワードを入力してもらう。

本人拒否率は自分で登録したデータに10回認証した際の認証失敗率とする。また、他人受入率は図4のように本人拒否率を計測する際に入力した10回の入力を他の人の登録してあるデータから計算した認証基準で認証させた場合の認証成功率とし、自分以外の実験者のデータ全てで行う。

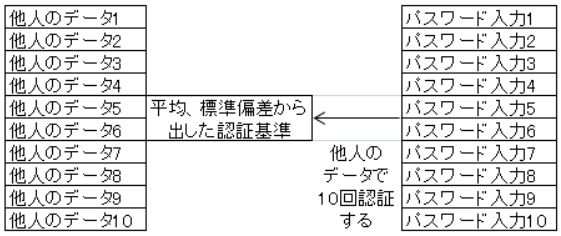

図4　他人受入率の計算方法

データ収集後に認証基準のK、L、Mを変更した場合の本人拒否率、他人受入率を計算する。

6　まとめ

スマートフォンの個人認証システムのセキュリティを向上させるために、フリック入力を利用した個人認証システムの認証基準の考案と、その個人認証システムを作るための実験として Android の画面ロックシステムの構築を行っており、今後実験を行う。

認証基準が指でキーを押してから離すまでの時間だけではなく指の移動により取得することのできる座標も認証基準にしているため、通常のキーボードにおけるキーストロークダイナミクス認証よりも個人を識別しやすいのではないかと考えている。

また､この個人認証システムは Web やアプリなどのログインシステムなどにも利用可能であり、セキュリティをより高めるために管理者側に認証サーバを置き、端末からは入力されたデータを送り、認証サーバで個人認証を行うという方法も可能である。

もし、この認証システムが高い精度で本人の認証、他人の識別を行うことができるなら利用者の負担を増やさずにセキュリティを向上することが可能となる。

参考文献

[1]　株式会社アイ・エム・ジェイ
モバイル端末の保有動向に関する調査
http://www.imjp.co.jp/press/assets/201304/imj20130418.pdf

[2]　andronavi
こだわりのパターンで Android を画面ロック！セキュリティ対策も安心。
http://andronavi.com/2011/06/94849

[3]　APP max
スマホ使い必須の文字入力フリックとは？
http://appmax.jp/archives/65688015.html

[4]　佐村敏治, 「スマートフォンを用いた日本語入力によるキーストローク認証」, 明石工業高等専門学校研究･教育シーズン(2010)
http://www.akashi.ac.jp/contents/Techno/pdf/23.pdf

[5]　梅津亮, ベッド B.ビスタ, 高田豊雄, 「スマートフォンにおけるキーストロークダイナミクスを用いた個人認証方式に関する一検討」
暗号と情報セキュリティシンポジウム, 3D1-5 (2013)

[6] J-Net21
「キーストローク・ダイナミクス認証」
とは
http://j-net21.smrj.go.jp/develop/digital/entry
/001-20110126-01.html