「マルチメディア，分散，協調とモバイル
(DICOMO2013)シンポジウム」 平成25年7月

スマートフォンにおけるキー操作熟練度の違いによるキーストローク認証手法の検討

山田健一朗[†1] 納富一宏[†1] 斎藤恵一[†2]

近年，スマートフォンやコンピュータを利用したオンラインゲームが流行している．それに伴い，不正アクセス被害も多発している．ログイン時の認証動作を突破できれば，その後は誰でも自由に操作できることから，不正アクセスの被害が減らないと考えられる．本研究では，オンラインゲームにおける不正アクセス被害の対策として，ゲーム操作情報を使用したキーストローク認証手法を提案している．先行研究では，マルチタッチやフリック操作といったスマートフォン独自のキー操作を用い，最高 86.39%の認証精度が確認された．また，検証結果から高い認証精度を得るためにはキー操作の安定性が必要であることも確認された．本稿では，継続的にキー操作実験を行い，被験者のキー操作熟練度を高めた状態でキー操作実験を行った結果について述べる．具体的には，キー操作実験を行う期間を変更した 3 グループで実験を行い，分析結果からキー操作熟練度の違いによる認証精度の変化について比較検証を行った．結果，高い確率で 2 日目以降の認証精度が向上し，最高 98.89%の認証精度を確認した．キー操作熟練度を高めることにより，認証精度の向上を期待できることが確認された．

Analysis of Keystroke Authentication based on the Difference in Operational Skill like a Gamepad Style

KENICHIRO YAMADA[†1] KAZUHIRO NOTOMI[†1] KEIICHI SAITO[†2]

1. はじめに

近年，スマートフォンやコンピュータを利用したオンラインゲームが流行している．それに伴い，他人の ID やパスワードを利用し，ゲーム内通貨やアイテムなどを違法に入手する不正アクセスの被害も多発している [1)]．ログイン時の認証動作を突破できれば，その後は誰でも自由に操作できることから，不正アクセスの被害が減らないと考えられる．

そこで，不正アクセスの被害を減らすには，ログイン時のパスワード認証だけでなく，ログイン後のゲーム操作時にも本人か他人かを見分ける必要があると考えた．その中でゲーム操作時のキー操作には，使用者独特の癖があると推測でき，個人識別に十分な特徴の差を観測できると考えられる．

先行研究 [2)]では，マルチタッチを用いた操作パターン，フリックを用いた操作パターン，単純な操作パターン，複雑な操作パターンの検証を行い，最高 86.39％の認証精度が確認されている．検証結果から，高い認証精度を得るには入力動作の安定性が必要であることが確認された．これまでの実験では，実験開始前に行っているキー操作の事前練習のみで実験データを取得していたため，キー操作の熟練度が低く，入力動作の安定性も低いと考えられる．しかし，実際にオンラインゲームをプレイしている時のキー操作は熟練度が高い状態でのキー操作となる．そのため，入力動作の安定性も増し，認証精度の向上が期待できる．

本稿では，継続的にキー操作実験を行い，被験者の熟練度を高めた状態でキー操作実験を行う．キー操作実験を行う期間を変更した 3 グループで実験を行い，分析結果からキー操作熟練度の違いによる認証精度の変化について比較検証を行う．

2. 関連技術

2.1 バイオメトリクス認証

バイオメトリクス認証とは，「人間の身体的あるいは行動的特徴を用いて個人を特定する技術」[3)]である．パスワードや物による認証では，忘却や紛失の恐れがあり，本人でも認証できなくなることがある．また，盗難や漏洩によって他人が認証される恐れもある．バイオメトリクス認証の場合は，それらの可能性が低いというメリットがある．バイオメトリクス認証には，身体的特徴を情報として用いる認証と行動的特徴を情報として用いる認証の二種類があり，本研究で扱うキーストローク認証は，後者の行動的特徴に含まれる．

キーストローク認証とは，キーを押している時間，次のキーが押されるまでの時間，タイピングエラー率などの打鍵動作を測定の対象として，個人識別を行うバイオメトリクス認証の一つである．

†1 神奈川工科大学大学院工学研究科情報工学専攻
Dept. of Information and Computer Sciences, Kanagawa Institute of Technology
†2 国際医療福祉大学情報教育室
Education Center of Medical Informatics, International University of Health and Welfare

2.2 自己組織化マップ

自己組織化マップ（SOM：Self-Organizing Maps, 以下 SOM という）とは，入力層と競合層の 2 層で構築された，ニューラルネットワークモデルの一つである．競合学習を基礎とし, 教師信号を必要としない教師なし学習を行う. また，多次元の属性ベクトルで表現されたデータを属性の類似度によって 2 次元平面上に配置する能力を持つ．ニューラルネットワークとは，脳・神経系による情報処理方式の原理を模した情報処理の仕組みである [4].

通常使用されている基本 SOM は，学習を行う際に入力データが学習される位置によって学習量が変化するため，ベクトル同士の関係が正常な位置に配置されないという問題点がある．その問題を解消する方法として，トーラス型 SOM がある．トーラス型 SOM は，マップの上下左右のノードが相互に結合しており，学習円がはみ出した場合はマップの対称な位置が学習される．このため，入力ベクトルは均等に学習され，基本 SOM よりも正確なマップを生成することが可能である．以上の点より，本研究では，トーラス型 SOM を採用した.

2.3 マルチタッチ

マルチタッチとは，タブレット端末やスマートフォンの画面で利用されている静電容量方式のタッチパネルにおいて，複数のポイントに同時に触れて操作することができる入力方式である. 大画面を複数人が同時に利用することや，複数の指による操作で，対象の移動や回転，ズームなどの動きを直感的に入力することができる.

フリック操作とは，タッチパネルにおける操作方法の一つで，画面を軽く払うように指やタッチペンを動かし，画面内のページや項目を移動する操作である．フリック操作を用いた機能のうち，スマートフォンにおける日本語入力機能で採用されている入力方式は，フリック入力と呼ばれている.

3. キー操作計測実験

3.1 実験条件

本学男子学生 15 名を被験者として実験を行った．被験者 15 名を 5 名ずつ 3 グループに分け, それぞれ 1 日計測を行うグループ，5 日間計測を行うグループ，10 日間計測を行うグループとした．スマートフォンを両手で横向きに保持し，椅子に座った状態で表 1 に示す 2 パターンのキー操作を行った．オンラインゲームで想定されるキー操作パターンが不明なため，キー操作パターンには熟練度の違いが現れやすいと想定される，格闘ゲームで使用されるパターンを参考にした．キー操作には両手の親指を使用し，30 回のキー操作練習後, 本登録として 15 回のキー操作を行った. 2 日目以降のキー操作練習は自由とした. 被験者情報を表 1 に，実験風景を図 1～2 に，実験に使用したキー操作パターンを表 2 に示す.

表 1　被験者情報

グループ	被験者数	キー操作計測期間
A	5 人	1 日
B	5 人	5 日
C	5 人	10 日

図 1　実験風景

図 2　実験機器の持ち方

表 2　実験に使用したキー操作パターン

桁数	パターン 1	パターン 2
1	←	△
2	↓フリック→	×フリック□
3	□	→
4	←○同時押し	↓○同時押し

3.2 実験環境

実験では, 表 3 に示す性能のスマートフォンを使用した. 計測プログラムは，HTML5，PHP，JavaScript を使用して作成した．ゲーム操作を想定したため，図 3 のような入力ボタン配置とした．なお，ボタンサイズは直径約 0.9cm となっている.

表 3　実験に使用したスマートフォン

機器名	iPhone4
OS	iOS5.1.1
タッチパネルサイズ	3.5 インチワイド

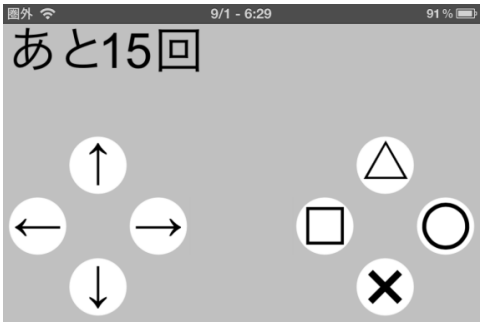

図 3　表示されるボタン配置図

3.3 計測値と属性ベクトル

本実験では，キー操作パターンを計測し，SOM 学習用の属性ベクトルを構成し，分析に用いた．各キーの押下，フリック，解放イベントから，その直後のイベントとの時間差 t1～t10 をそれぞれ計測し，分析に用いた．計測属性を図 4 に示す.

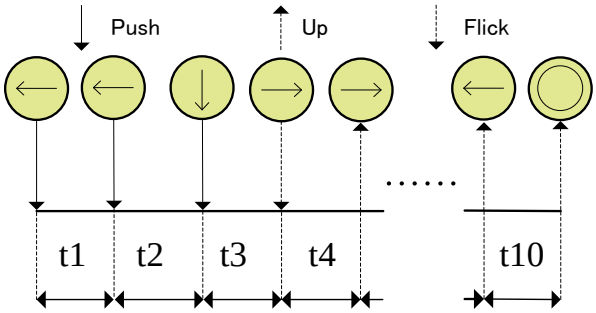

図 4　計測属性

3.4 分析

本実験で得た 15 回分の計測データを最大値 1，最小値 0 に正規化する．それらのデータから，操作ミス時のデータを取り除いた 10 回分の計測データを学習用に 7 回, 認証用に 3 回に分け，SOM を用いて分析を行った．SOM の学習条件として，グループ別で分析を行う場合はマップサイズ 50×50（ユニット数 2,500），学習回数 50,000 回と設定し，被験者グループを分けずに分析を行う場合は，マップサイズ 100×100（ユニット数 10,000），学習回数 70,000 回と設定した．マップ上の学習に使用したベクトルと認証時のベクトルとのユークリッド距離の平均を求め，その値が設定した閾値以内であれば認証成功とした．

評価には，他人受容率（FAR：False Accept Rate）と，本人拒否率（FRR：False Reject Rate）を用いた．これらの定義式を以下に示す．

$$\mathrm{FAR} = \frac{\text{他人受容回数}}{\text{試行回数}} \qquad \mathrm{FRR} = \frac{\text{本人拒否回数}}{\text{試行回数}}$$

なお, FAR と FRR が等しい値を等価エラー率(EER：Equal Error Rate)とし, EER を 1 から引いた値を認証精度とする．

4. 実験結果

SOM は初期値が乱数で決定されるため, 毎回異なるマップが作成される．本実験では 5 回ずつマップを作成し，その平均値を本実験の認証精度とした．各グループ，パターンごとの認証精度を表 4～6 に, 作成された認証精度グラフの 1 枚を図 5～10 に示す．

表 4　認証精度（グループ A）

グループ A・パターン 1		グループ A・パターン 2	
日数	認証精度	日数	認証精度
1	93.05%	1	87.56%

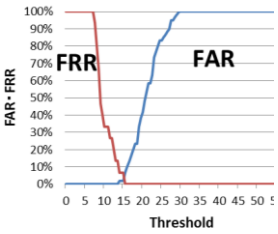

図 5　認証精度グラフ
（グループ A・パターン 1）

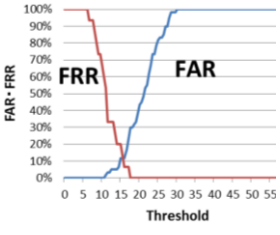

図 6　認証精度グラフ
（グループ A・パターン 2）

表 5　認証精度（グループ B）

グループ B・パターン 1		グループ B・パターン 2	
日数	認証精度	日数	認証精度
1	84.94%	1	87.22%
2	87.33%	2	91.44%
3	86.72%	3	87.67%
4	92.95%	4	91.00%
5	86.28%	5	85.56%

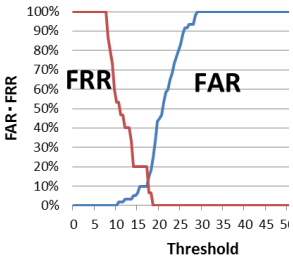

図 7　認証精度グラフ
（グループ B・パターン 1）

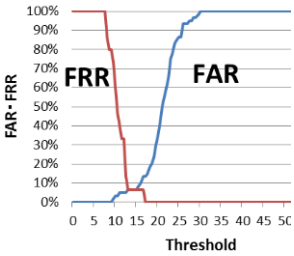

図 8　認証精度グラフ
（グループ B・パターン 2）

表 6　認証精度（グループ C）

グループ C・パターン 1		グループ C・パターン 2	
日数	認証精度	日数	認証精度
1	94.56%	1	88.05%
2	88.06%	2	96.39%
3	87.00%	3	97.50%
4	98.67%	4	89.50%
5	83.83%	5	93.56%
6	77.50%	6	85.78%
7	87.33%	7	83.89%
8	89.44%	8	92.56%
9	98.89%	9	90.39%
10	95.22%	10	87.67%

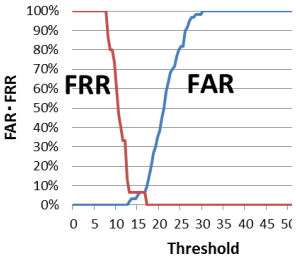

図 9　認証精度グラフ
（グループ C・パターン 1）

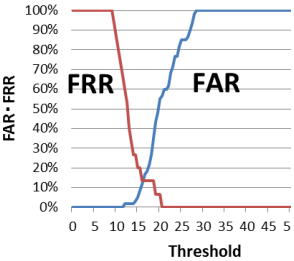

図 10　認証精度グラフ
（グループ A・パターン 2）

被験者をグループ分けせずに分析を行った場合に使用したデータ一覧を表 7 に示す．グループ D は，各グループのキー操作計測 1 日目のデータを使用した. グループ E は，各グループのキー操作計測最終日のデータを使用した．グループ F は，各グループの最も高い認証精度が確認された

キー操作計測日のデータを使用した．各グループ，パターンごとの認証精度を表 8 に，作成された認証精度グラフの 1 枚を図 11～16 に示す．

表 7　使用データ詳細

グループ	パターン	使用データ日数		
		A	B	C
D	1・2	1 日目	1 日目	1 日目
E	1・2	1 日目	5 日目	10 日目
F	1	1 日目	4 日目	9 日目
	2	1 日目	2 日目	3 日目

表 8　認証精度（グループ D・E・F）

グループ	パターン	認証精度
D	1	81.59%
	2	78.31%
E	1	81.73%
	2	81.92%
F	1	88.80%
	2	86.52%

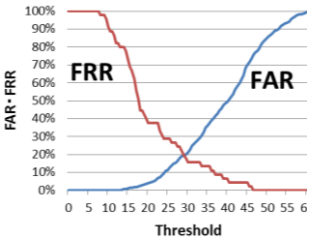

図 11　認証精度グラフ
（グループ D・パターン 1）

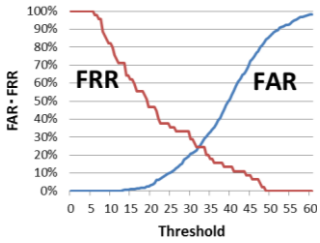

図 12　認証精度グラフ
（グループ D・パターン 2）

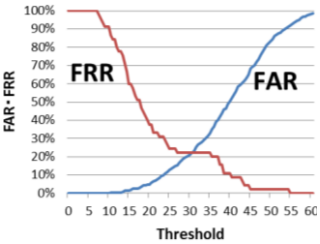

図 13　認証精度グラフ
（グループ E・パターン 1）

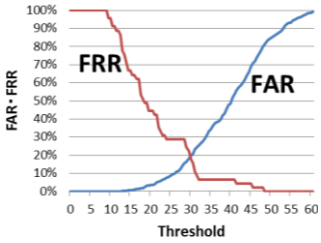

図 14　認証精度グラフ
（グループ E・パターン 2）

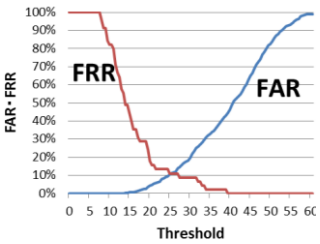

図 15　認証精度グラフ
（グループ F・パターン 1）

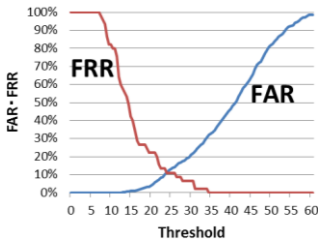

図 16　認証精度グラフ
（グループ F・パターン 2）

5.　考察

表 5～6 より，計測 1 日目とその他の日を比較すると，グループ B の両パターン，グループ C・パターン 2 では，高い確率で 2 日目以降の認証精度の向上が確認された．グループ C・パターン 1 では，計測 1 日目の認証精度が他のグループ，パターンに比べて高かったため，2 日目以降の認証精度が高くなる確率は低下したと考えられる．しかし，9 日目には本実験で算出した認証精度の中で最も高い 98.89%が確認され，熟練度による影響が現れたと考えられる．また，認証精度が低下した要因として，キー操作計測期間が空いてしまったことが考えられる．被験者の中でキー操作が安定していない状態で計測期間が空いてしまったため，キー操作熟練度が低下したと考えられる．

表 8 より，グループ D とその他のグループを比較すると，グループ E・F どちらの場合でも認証精度の向上が確認された．被験者数が増え，計測期間がそれぞれ異なる状況で認証を行った場合でも，熟練度による影響は現れると考えられる．

以上の点から，キー操作計測を継続的に行い，キー操作熟練度を高めることにより，認証精度の向上を期待できることが確認された．

6.　おわりに

本実験では，スマートフォンにおけるキーストローク認証手法において，キー操作熟練度の違いにより認証精度が変動するか検証を行った．結果，高確率で計測 1 日目よりも 2 日目以降の認証精度が高くなり，計測 9 日目に本実験で最高精度となる 98.89%の認証精度を確認した．キー操作熟練度を高めることにより操作の安定性が増し，認証精度の向上を期待できることが確認された．

今後の課題として，数時間毎に実験を行った場合の熟練度の検証，また，その場合における日数経過後の認証精度変動を検証することが考えられる．さらに，実際にスマートフォンでゲームをしているときのキー操作情報の取得を可能にすることで，直感的なキー操作となり，個人差が大きく現れると考えられる．また，ゲームジャンルの違いによるキー操作の分類が可能になり，より詳細なキー操作の分析が可能になる．

参考文献

1)　総務省：不正アクセス行為の発生状況，入手先 <http://www.soumu.go.jp/main_content/000215184.pdf> (2013.05.16)
2)　山田健一朗，野口敦弘，納富一宏，斎藤恵一：スマートフォンにおけるゲームパッドを意識したキーストローク認証手法 -フリック操作の対応-，情報処理学会 第 75 回全国大会講演論文集 第 3 分冊,4Z-7, pp.565-566, (2012.03).
3)　バイオメトリクスセキュリティコンソーシアム：バイオメトリックセキュリティ・ハンドブック，オーム社 (2005).
4)　大北正昭，徳高平蔵，藤村喜久郎，権田英功：自己組織化マップとそのツール, pp.1-7, シュプリンガージャパン株式会社 (2008).