L-027

自己組織化マップを用いたキーストローク認証手法の提案 —覗き見によるリズムのなりすまし評価—

Proposal on Keystroke Authentication Method using Self-Organizing Maps —Evaluation of Rhythm Spoofing by Shoulder Surfing—

野口 敦弘† 高橋 雅隆† 納富 一宏† 斎藤 恵一‡
Atsuhiro Noguchi Masataka Takahashi Kazuhiro Notomi Keiichi Saito

1. はじめに

近年，銀行 ATM では，キャッシュカードの偽造・盗難などによる不正な払出し被害が横行している．この被害の本質は，暗証番号さえ知り得れば，誰でも払出しが行えてしまう点にある．

本研究では，暗証番号のみでの認証は脆弱であることを踏まえ，バイオメトリクス認証の 1 つであるキーストローク認証と組み合わせることを提案している．本人だけが知るキーストロークリズムを自己組織化マップにより学習・分類し，平均ユークリッド距離から認証精度を算出した[1]．

本稿では，暗証番号を覗き見される被害を想定し，覗き見によるキーストロークリズムのなりすましが可能であるか検証し，その結果に基づいてセキュリティ確保手段について考察する．

2. キーストローク認証と自己組織化マップ

2.1 キーストローク認証

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さまざまな打鍵動作を測定の対象として個人識別を行う，人間の行動的特徴を用いたバイオメトリクス認証の 1 つである[2]．既存の入力装置で実現が可能であり，特別な機器を必要としないため，導入費が安く済むという利点がある．

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）は，競合学習型ニューラルネットワークの一種であり，入力層と出力競合層の 2 層から成る[3]．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について学び，その原理を模した情報処理の仕組みである．SOM は，1982 年に T.Kohonen によって発表され，多次元データの分類，解析に効率的な技術として知られている．

3. なりすまし実験

3.1 第一実験～覗き見実験

キー被験者が暗証番号入力をする様子を，なりすまし被験者が後方から覗き見し，押下した番号とキーリズムを盗む．なりすまし被験者は，盗んだ番号とキーリズムを再現し，キーリズムによるなりすましが可能であるか検証する．

†神奈川工科大学大学院 Graduate school of Engineering , Kanagawa Institute of Technology
‡国際医療福祉大学情報教育センター Education Center of Medical Informatics , International University of Health and Welfare

3.2 第二実験～Web カメラによる覗き見実験

キー被験者が暗証番号入力する様子を Web カメラで録画し，その内容をなりすまし被験者が番号とキーリズムを覚えるまで観察する．そして，番号とキーリズムを覚えたところで，第一実験と同様に，再現してもらい，Web カメラを用いたキーリズムのなりすましが可能であるか検証する．

3.3 実験方法

3.3.1 実験方法

本学学生，20 代の男子，6 名(うちキー被験者 1 名，なりすまし被験者 5 名)に協力してもらった．実験の準備として，キー被験者に 4 桁の番号とキーリズムを覚えてもらうため，打鍵練習をしてもらう．第一実験では，キー被験者は 4 桁の番号にリズムを入れて 1 回だけ打鍵し，なりすまし被験者はその様子を後ろから覗き見し，キーリズムを再現してもらった．第二実験では，予めキー被験者 1 回分の打鍵の様子を Web カメラで録画する．なりすまし被験者は録画した映像を視聴し，キーリズムを再現してもらった．第一実験と第二実験では，4 桁の番号とキーリズムは異なる．

3.3.2 実験環境

銀行 ATM を参考に，以下のように機器の設置や人の配置を決めた．

・タッチスクリーンを高さ 70cm の平面上に配置し，画面の角度を高さ 5cm とした約 14.7° とした．
・覗き見はキー被験者後方から覗き込む(図 1 参照)．
・第二実験で使用した Web カメラは実際の被害状況などを参考にし，タッチスクリーンから 10cm 離した高さ 40cm の斜め左から録画した(図 2 参照)．

図 1 覗き見の様子

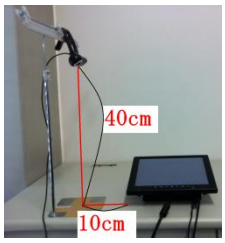

図 2 Web カメラの設置

3.4 分析

3.4.1 分析方法

SOM の学習により得られた学習用データと認証用データ間の距離をユークリッド距離という．分析には，各データ間のユークリッド距離を平均した平均ユークリッド距離を用いた．登録データの座標を(a_1, b_1)，(a_2, b_2)，(a_3, b_3)，

(a_4, b_4)とし，認証データの座標を(x, y)とすると，平均ユークリッド距離(n=4)は以下の式で表せる(3.1).

$$\bar{d} = \frac{1}{n}\sum_{i=1}^{n}\sqrt{(x-a_i)^2+(y-b_i)^2} \quad \cdots\cdots (3.1)$$

3.4.2 評価方法

評価には，本人拒否率（FRR：False Reject Rate）(3.2)と，他人受容率（FAR：False Accept Rate）(3.3)を用いた．定義式を以下に示す.

$$FRR = \frac{\text{本人拒否回数}}{\text{試行回数}} \quad (3.2) \qquad FAR = \frac{\text{他人受容回数}}{\text{試行回数}} \quad (3.3)$$

4. 実験結果

4.1 第一実験～覗き見実験結果

パスワードを 4186，キーリズムに長押しを 1 ヵ所入れた第一実験の結果を表 1 に示す．受入率とは，本人でない他人を受容してしまう確率である.

表 1　パスワード 4186 とした第一実験の結果

認証方法	受入率[%]
パスワード認証	80.0
キーストローク認証	33.3

次に，番号を 1765 に変え，キーリズムに長押しを 2 ヵ所入れた結果を表 2 に示す.

表 2　キーリズムを複雑にした第一実験の結果

認証方法	受入率[%]
パスワード認証	100.0
キーストローク認証	13.1

4.2 第二実験～Web カメラによる覗き見実験結果

パスワードを 3951，キーリズムに長押しを 2 ヵ所入れた第二実験の結果を表 3 に示す.

表 3　Web カメラによる覗き見実験の結果

認証方法	受入率[%]
パスワード認証	100.0
キーストローク認証	18.1

5. 考察

第一実験では，背後から覗き見され，暗証番号とキーリズムが盗まれることを想定して実験を行った．その結果，パスワード認証の受入率は 80.0%となった．なりすまし被験者 5 名中 1 名がパスワードを 4186 でなく，4153 とキー押下をした．ボタン配置を見ると，8 の上が 5 であり，6 の上が 3 である．キー押下の軌跡はある程度辿れていることを表しているが，番号の誤認識であることには変わりはない．番号認識に関しては，背後からかなり近い位置で覗き見しているため，すべての被験者がクリアできるものと推測していた．しかし，個人により，必ずしも認識できるものではないということが分かった.

キーストローク認証の受入率は 33.3%の結果を得た．パスワード認証は番号さえ知り得てしまえば，誰でも受け入れてしまう．しかし，キーストローク認証では，パスワード認証に加え，キーリズムを再現できなければ認証されない．したがって，受入率に大きな違いが出たと考える.

表 2 の通り，キーリズムに長押しを 2 ヵ所入れた際，キーストロークの受入率は 13.1%と 20%ほど低下した．この低下の度合いはキーリズムが認証に与える影響の大きさを表すものである．また，すべてのなりすまし被験者も，この影響の大きさを理解していた．そのため，キーリズムの再現性の度合いが，なりすましが成功するかのキーポイントになる．したがって，キーリズムが複雑になるにつれて，他人による再現性が難しくなると考えられる.

背後からの覗き見によって番号を盗まれた際に，キーストローク認証によって受入率を 13.1%まで低下させることができた．したがって，キーストローク認証は覗き見によるなりすまし対策に効果があることが示された.

第二実験では，ATM にカメラが仕掛けられるという実被害の状況を想定し，録画した情報からなりすましが可能であるか実験を行った．その結果，パスワード認証の受入率は 100.0%であった．録画情報であるため，繰り返し確認ができる．したがって，この結果は妥当であるといえる.

キーストローク認証の受入率は 18.1%の結果を得た．第一実験の 2 ヵ所長押しを入れた受入率と比べると，5%向上していることが分かる．Web カメラで録画したものを覚えるまで繰り返し見ることができるので，受入率が向上したものと考えられる.

Web カメラによる覗き見でも第一実験と同様に，キーストローク認証によって受入率を 18.1%まで低下させることができた．したがって，キーストローク認証は Web カメラを用いた覗き見によるなりすまし対策にも効果があることが示された.

6. 今後の課題

現在，銀行 ATM では，覗き見防止対策がなされている．例えば，左右方向からは見えないように画面にフィルターが添付されている，正面に覗き見防止用の鏡が設置されている，順番待ちの場所は ATM から離れたところに設置する，などがある．覗き見されないことが一番望ましいが，しかし現状，覗き見被害は後を絶たない[4]．今後の課題として，システム的にセキュリティを確保できるような対策を考えることが被害拡大を防ぐ上で重要である.

7. おわりに

本稿では，覗き見によるリズムのなりすましについて検証を行った．キーリズムは本人特有のものであり，他人が再現するには難しいことが本実験から分かった．キーストローク認証は，今までの入力動作にリズムを加えるだけで済むので，煩わしさが少ない．銀行 ATM における生体認証の利用が進まない要因は，この煩わしさであると考える．今後，ユーザの利便性向上が求められる.

参考文献

[1] 野口敦弘，高橋雅隆，納富一宏，斎藤恵一：“タッチスクリーンによるキーストローク認証手法ーリズムの再現性と長押しの効果ー”，情報処理学会 マルチメディア，分散，協調とモバイル(DICOMO2011)シンポジウム，2G-3(2011.07) [発表予定].

[2] バイオメトリックセキュリティコンソーシアム，佐藤政次：バイオメトリックセキュリティ・ハンドブック，第 1 版第 1 刷発行，p.2-3，(2006).

[3] T.Kohonen：自己組織化マップ，シュプリンガー・フェアクラーク東京(1996)，徳高平蔵 他.

[4] 金融庁，“偽造キャッシュカードによる預金等不正払戻し（被害発生状況・補償状況）”，(2011. 04). http://www.fsa.go.jp/news/22/ginkou/20110421-1/01.pdf