ユーザの慣れによる認証精度の低下を考慮したリズム認証方式の提案

喜多 義弘 †　　朴 美娘 †　　岡崎 直宣 ‡

† 神奈川工科大学
243-0292 神奈川県厚木市下荻野 1030

‡ 宮崎大学
889-2192 宮崎県宮崎市学園木花台西 1-1

あらまし　スマートフォンなどに搭載されている画面ロック機能には，暗証番号やパターンなどの認証方式が利用されている．しかし，これらの認証方式は，第三者やカメラなどによる覗き見攻撃に対して脆弱である．そのため，我々は以前より覗き見攻撃への対策として，自己組織化マップを用いたリズム認証方式を提案してきた．しかしながら，この認証方式をユーザが使い続けることによって慣れによる誤差が生じ，認証精度が低下し続ける問題がある．そこで本論文では，認証回ごとにユーザの入力情報を基に閾値の中心を移動し，自己組織化マップを定期的に更新することによって，ユーザの慣れによる認証情報の変化に対応したリズム認証方式を提案する．この手法により，認証精度を保持し，認証方式の長期利用が可能になることが期待される．

Proposal of Rhythm Authentication Method for lowering prevention of authentication accuracy by user's practice

Yoshihiro Kita†　　Mirang Park†　　Naonobu Okazaki‡

†Kanagawa Institute of Technology
1030, Shimo-Ogino, Atsugi, Kanagawa 243-0292, JAPAN
‡University of Miyazaki
1-1, Gakuen-Kibanadai-Nishi, Miyazaki 889-2192, JAPAN

Abstract　Existing authentication methods for display lock system, e.g. PINs and Android password pattern, have a common problem called "shoulder-surfing," that means inferring authentication information by watching the authentication sequence. We proposed the rhythm authentication method using Self-Organizing Map (SOM) for countermeasure of shoulder-surfing. However, this method has a problem that authentication accuracy is influenced by user's practice. In this paper, we propose the method that center of threshold is moved by the user's input information every authentication, and SOM is learned periodic by server. It expects that long-term using of the authentication method by proposed method.

1　はじめに

近年，BYOD（Bring Your Own Device）によるビジネスモデルのツールや個人のライフアイテムとして，スマートフォンをはじめとするモバイル端末が普及してきており，端末内の社内情報や個人情報の守秘への意識が高まりつつある [1]．多くのモバイル端末には，他人から端末を操作されないように画面ロック機能が搭載されており，そのロック解除に暗証番号やパターンなどの認証方式が利用されている．しかしながら，人通りの多い場所や公共施設などで画面ロックを解除する際には，第三者や監視カメラなどにより肩越しから認証動作を覗き見ら

れ，認証情報が漏れてしまうこと（以下，覗き見攻撃）が考えられる．

覗き見攻撃への対策として，従来から様々な研究が行われている [2]〜[4]．しかし，これらの研究は認証動作をカメラによって覗き見され，認証動作を解析される攻撃（以下，録画攻撃）に対して，十分な耐性を有していない．そのため，利用者が画面を見ながら認証動作を行う以上，その認証画面を録画されていないことが保障されない限り，十分な安全性を確保できない．

録画攻撃対策の先行研究として，自己組織化マップ（Self-Organizing Maps，以下，SOM）を用いたリズム認証方式 [5, 6] が行われている．この認証方式は，タッチスクリーンをタップし，そのタップのイベント時間を SOM に入力し，学習・分析によりその類似度に応じて個人認証を行う．そのため，利用者は画面上のタップのみで認証を行うことができるため，鞄やポケットの中などに端末を入れたまま画面を見ずに認証情報を入力でき，認証画面を録画されることはなくなる．我々も以前に，マルチタッチ操作に対応したリズム認証方式 [7] について提案した．マルチタップ操作により，従来のリズム認証方式より認証精度が向上したが，リズム認証方式をユーザが使い続けることによって慣れによる誤差が生じ，認証精度が低下し続ける問題が出てきた．

そこで本研究では，認証回ごとにユーザの入力情報を基に閾値の中心を移動し，SOM を定期的に更新することによって，ユーザの慣れによる認証情報の変化に対応した認証リズム認証方式を提案する．具体的に，閾値の中心の移動については，SOM 上において認証ごとに得る入力情報の勝利ノードを探索し，その勝利ノードと従来の勝利ノードとの重心を新たな閾値の中心として決定する手法を提案する．SOM の定期更新については，SOM の学習時間を考慮した，効率的な更新手法について提案する．また，SOM を用いた認証方式は従来のリズム認証方式 [7] と同様であり，本人拒否率（False Reject Rate，以下，FRR）および他人受入率（False Accept Rate，以下，FAR）の低減を考慮し，全ての特徴のうち利用者本人の再現率が高い特徴，および，他人との特徴差が大きい特徴をそれぞれ用いる．

2 関連研究

2.1 覗き見耐性を持つ認証方式

覗き見耐性を持つために，端末の振動機能を用いた認証方式 [2] や fakePointer[3] がある．この認証方式は，暗証番号を入力する際に，入力カーソルを複数表示し，正解の入力カーソルを振動で通知する方法である．正解の入力カーソルは認証のたびにランダムで変化するため，認証動作を覗き見られても認証情報が露呈しない特徴を持つ．

覗き見耐性を持つ認証方式として，アイコンと移動法則を用いた STDS 認証方式 [4] もある．この認証方式は，まずユーザがパスワードとなるアイコンと独自の移動法則を登録する．そして，表示されたアイコン群から登録したアイコンを探し出し，そこから移動法則に従って移動した先のアイコンをタップすることによって認証を行う．登録したアイコンの位置は認証のたびにランダム変わるため，覗き見られても登録したアイコンが露呈しない特徴を持つ．

これらの認証方式は，覗き見に対して有用ではあるが，カメラなどの録画機器に対して耐性が十分ではなく，認証動作や端末の画面を複数回録画された場合，認証情報が解析されてしまうことが考えられる．そのため，利用者が画面を見ながら認証動作を行う以上，その認証画面を録画されていないことが保障されない限り，十分な安全性を確保できない．

2.2 自己組織化マップ

自己組織化マップ（Self-Organizing Maps: SOM）とは，競合学習型ニューラルネットワークの一種であり，与えられた入力情報の類似度を 2 次元空間のマップ上での距離で表現するモデルである [8, 9]．

SOM は入力層と競合層の 2 つの層から成る．入力層には入力ベクトルが割り当てられたノードを，競合層には入力ベクトルと同次元の参照

ベクトルを割り当てられた，2 次元空間上で規則的に配置したノードをそれぞれ持つ．まず，入力ベクトル $\vec{i}$ が入力層に与えられたとき，競合層において $\vec{i}$ との内積が最も大きい参照ベクトルを持つノードを探索する．この探索により特定したノードを，勝利ノードと呼ぶ．勝利ノード v が決定したとき，勝利ノードとその周辺のノードに対して，以下の式 (1)〜(3) を適用し，勝利ノードを含むノード n の参照ベクトル $\vec{r_n}$ を $\vec{i}$ へ近づけるための学習を行う．式において，2 次元空間上での勝利ノードの座標を $L_v = (x_v, y_v)$，近傍半径 θ 内のノード n の座標を $L_n = (x_n, y_n)$ とする．また，T は予め設定した学習の総回数，t は学習回数，σ は近傍の広がりを表す正規分布の標準偏差に対応した正の定数とする．

$$\vec{r_n}(t+1) = \vec{r_n}(t) + H_n(t) \cdot (\vec{i}(t) - \vec{r_n}(t)) \quad (1)$$

$$H_n(t) = \alpha(t) \cdot exp(-\frac{|\vec{L_n} - \vec{L_v}|^2}{2\sigma^2}) \quad (2)$$

$$\alpha(t) = 1 - \frac{t}{T} \quad (3)$$

これらの式を用いて学習を行うことにより，特徴が似たデータは近い場所に，異なる特徴のデータは遠い場所にマッピングされるため，複数の多次元データを視覚的に解りやすく分類することができる．また，ある勝利ノードとそれに特徴が似たデータとが集合した領域を，以降では近傍領域とする．

SOM の特性を活かしたリズム認証の先行研究 [5, 6] が行われており，認証の判定における SOM の有用性が報告されている．本研究においても認証の判定に SOM を用いる．

2.3 リズム認証

リズム認証とは，連続した入力の時間差を認証情報として用いる認証方法であり，利用者個人の行動的特徴を活かしたバイオメトリクス認証の一つである．リズム認証は，従来からキーボードなどの入力装置を対象とした研究 [5]〜[7],[10]〜[12] が行われており，現在は，モバイル端末向けにタップ入力を利用した研究が行われている [6, 7]．リズム認証を用いることにより，利用者は認証画面を見ずに，タッチスクリーンへのタップ入力によって認証を行うことができる．そのため，他人や監視カメラに認証画面を露呈することがなくなり，認証情報の漏洩を防ぐことが期待できる．しかし，現在のリズム認証の認証情報は入力の時間差のみであるため，FRR や FAR が増えやすく，認証精度が十分ではない．

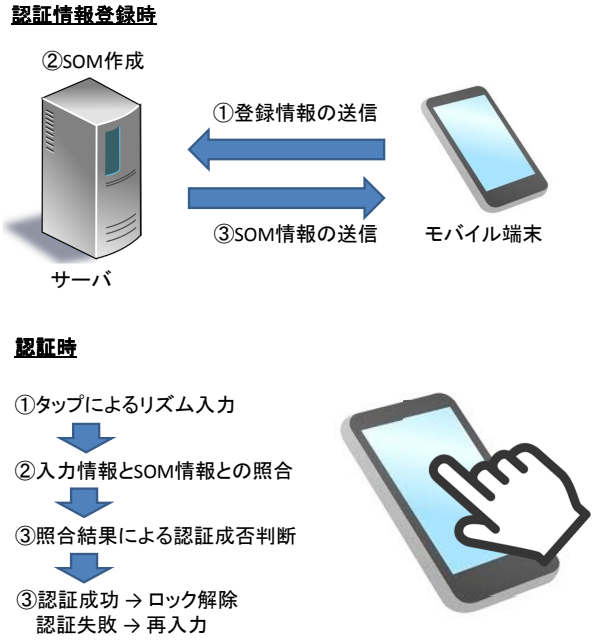

図 1: 認証情報登録および認証の手順

野口らによって，シングルタップ操作によるリズム認証方式 [6] が提案されている．この方式は，使用する指に関わらず，タップしたリズムを認証情報にする認証方式である．この方式は SOM 利用しており，タップのイベント発生時間および終了時間を入力データにしている．リズムのみであるため，画面が小さいモバイル端末でも適用しやすい利点がある．しかし，指の識別は行わないため，認証の際に画面をタップする音を他人が聞くことで，認証情報であるリズムが漏れ，他人が同様のリズムでタップすることで画面ロックを解除されてしまうことが考えられる．

我々は以前に，マルチタップ操作を利用したリズム認証方式 [7] を提案した．この認証方式

は，認証方式 [6] を基に，タップのイベント時間による特徴量を追加し，さらに指の識別や指間の距離など計 6 項目の入力データから SOM を作成し，その SOM を認証に利用した方式である．

図 1 に，この認証方式の認証情報登録および認証の手順について示す．モバイル端末は個人で所有している場合が多く，複数のユーザで 1 つの端末を共有することは少ない．そのため，ユーザは端末 1 台につき 1 名であることを想定する．

認証情報の登録では，ユーザが端末上でタップした認証情報はサーバへ送信され，サーバで SOM を作成する．サーバは作成した SOM のデータを端末へ送信し，登録は完了する．

サーバで SOM を作成する理由として 2 つ挙げられる．まず，SOM 作成の膨大な処理への対応である．SOM は，1 つのノードにつき n 次元を扱い，1 つのマップは数千〜数万のノードによって構成されている．それらのノードにつき，探索および学習を数万回行うため，その処理は膨大である．その処理をモバイル端末上で行うには負荷が大きく，端末の動作が不安定になることが考えられるため，処理能力が高いサーバで SOM を作成する．次に，端末間での認証情報の共有によるユーザの負荷軽減がある．複数台の端末を有するユーザが各端末上で本人認証を行う際，ユーザ本人の既存 SOM を端末へ送信して認証情報を共有することにより，各端末で認証情報の新規登録や変更を行う必要がなく，普段通りに認証を行うことができる．これによりユーザは，新たに認証情報を覚えたり，複数の認証情報を管理したりする必要がない．

認証時では，まず，ユーザは端末上をタップしてリズムを入力する．次に端末内では，入力情報と SOM とを照合し，入力情報の勝利ノードと近傍領域の中心とのユークリッド距離を求める．そして，その距離が予め定義した閾値内であるか否かによって認証の成否を判断する．認証が成功した場合は画面ロックを解除し，失敗した場合はユーザに対し再度入力を求める．

指の識別や指間の距離も特徴として加えることにより，ユーザ本人と他人との区別がつきやすくなり，従来のリズム認証方式よりも認証精度が向上した．しかし，ユーザの慣れによって発生する認証動作の誤差により，FRR が上がり，認証精度が徐々に下がることが考えられる．

3 提案手法

本論文では，ユーザの慣れによって発生する認証動作の誤差による認証精度の低下を抑えるため，ユーザ登録時だけでなく認証入力時の入力情報も考慮し，次の 2 手法に基づいたリズム認証方式を提案する．リズム認証方式は，以前我々が提案した認証方式 [7] を用いる．

- 閾値の中心移動による SOM 上の認証判定位置の変更
- SOM の定期更新

3.1 閾値の中心移動による SOM 上の認証判定位置の変更

認証判定は，近傍領域の中心からの距離が閾値内であるか否かによって決定する．近傍領域の中心は，ユーザが登録した複数の入力情報を SOM に入力した際，各入力情報の勝利ノード間の重心である．ユーザが認証手法に慣れてくると，リズムの速さや指の距離などが登録時と比べて変わってくるため，認証入力時の勝利ノードが，近傍領域の中心から徐々に離れ，閾値外へマッピングされることが考えられる．

そこで，ユーザ登録時や認証入力時の各勝利ノードの重心を閾値の中心とし，認証回を重ねるごとに閾値の中心を移動することによって認証判定の位置を変更する手法を提案する．

図 2 に，勝利ノード間の重心の移動について示す．この図では，例として 3 つのノード間の重心を閾値の中心としている．また，図中のノードに記した数字は登録順（または入力順）を示す．まず，ユーザ登録時において，ユーザは一連のリズムのタップ情報を複数回分（図 2 の例では 3 回分）登録する．端末は，これらのタップ情報を認証サーバへ送信し，認証サーバでは送信されたタップ情報を基に SOM を作成する．

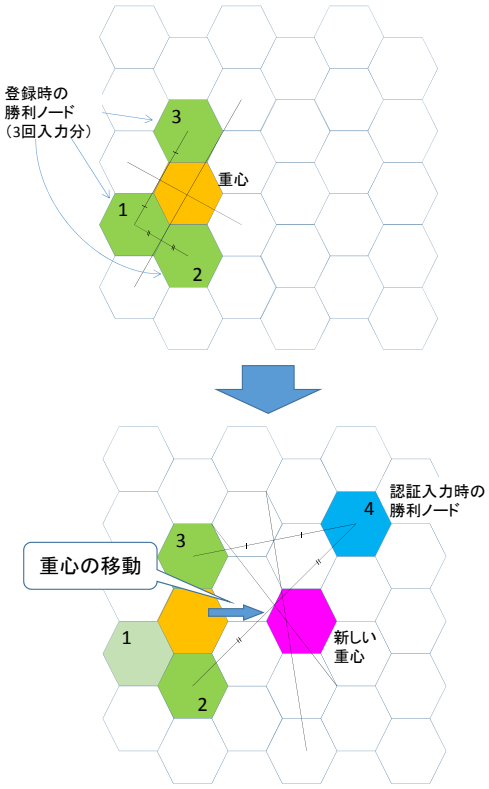

図 2: 勝利ノード間の重心の移動

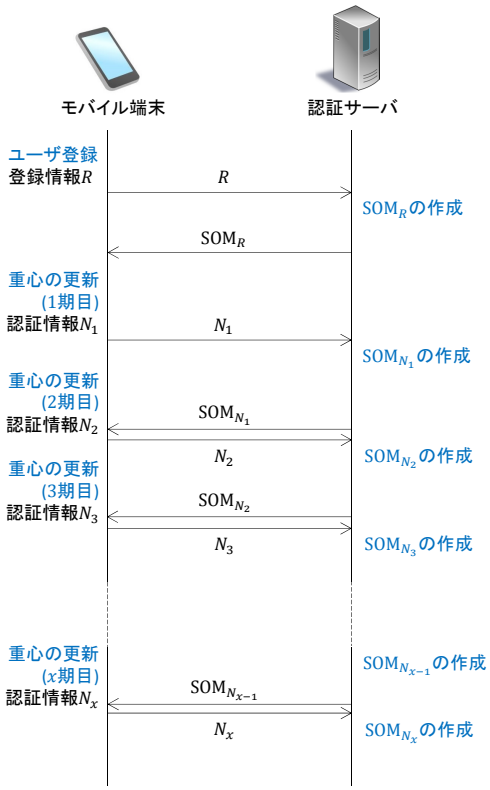

図 3: 端末と認証サーバ間の相互通信による SOM の定期更新

このとき，送信された全てのタップ情報の勝利ノード間の重心を求め，その重心となるノードを閾値の中心とする．

重心測定の対象になるノード数を r，SOM において m 番目に入力されたタップ情報の勝利ノードの座標を (x_m, y_m) とするとき，閾値の中心となるノード C の座標 $C(x, y)$ を求める式を，以下に示す．

- $m < r$ のとき

$$C(x,y) = (\sum_{i=1}^{m} \frac{x_i}{m}, \sum_{i=1}^{m} \frac{y_i}{m}) \quad (4)$$

- $m \geq r$ のとき

$$C(x,y) = (\sum_{i=m-r}^{m} \frac{x_i}{r}, \sum_{i=m-r}^{m} \frac{y_i}{r}) \quad (5)$$

次に，認証時において，ユーザは一連のリズムをタップし，認証を行う．認証に成功した場合，重心の対象となっているノードのうち最も古いものを対象から外し，認証時のタップ情報の勝利ノードを重心の対象に加え，新たな重心を求める．(図 2 の下部参照) 新たな重心を閾値の中心とする．

閾値の中心が移動することにより，ユーザの慣れによりタップ情報の勝利ノードが変わっても，従来のタップ情報の勝利ノードと併せて閾値内に収めることができるため，本人拒否率が上がりにくくなることが考えられる．

3.2 SOM の定期更新

閾値の中心を移動しても，重心の対象になる全ての勝利ノードが閾値内に必ず入るとは限らない．そこで，認証サーバで SOM を定期的に学習しなおし，閾値の中心を改めて定義する手法を提案する．SOM は学習に多くの時間を要するため，端末は認証サーバで SOM を作成している間，SOM データが更新されるまで待機

状態になることが考えられる．そのため，効率的にSOMの更新を行う必要がある．

図3に，端末と認証サーバ間の相互通信によるSOMの定期更新を示す．以下にその更新手順について述べる．また，図3内および手順内で用いる記号を，以下に示す．

R: ユーザ登録情報

N_x: x期目で新たに得た認証情報．ここでの1期間は，認証サーバに前回の認証情報を送信してから再び新たな認証情報を送信するまでの期間を指す．

SOM_R: Rを基に作成したSOM

SOM_{N_x}: Rを併せてx期までに得たN_xを基に作成したSOM．基にする情報の数は，3.1節における重心測定の対象になるノード数rとする．

T: 端末

S: 認証サーバ

$A \to B$: AからBへ送信する．

端末および認証サーバでの通信手順

1. $T \to S : R$

   端末から認証サーバにユーザ登録情報Rを送信する．

2. $S : \mathrm{SOM}_R$

   認証サーバはSOM_Rを作成する．

3. $S \to T : \mathrm{SOM}_R,\ x = 1$

   認証サーバから端末にSOM_Rを送信する．ここより1期目を開始する．

4. $T \to S : N_x,\ x = x + 1$

   端末から認証サーバにN_xを送信する．

5. $S : \mathrm{SOM}_{N_x}$

   認証サーバはSOM_{N_x}を作成する．

6. $S \to T : \mathrm{SOM}_{N_x}$

   認証サーバから端末にSOM_{N_x}を送信する．

7. 手順4〜6を繰り返す．

表 1: 認証に用いたSOMの定数および閾値

ノード数 (マップサイズ：横×縦)	8,000 (100×80)
学習係数 σ^2	160.0
初期近傍半径 θ_0(ノード数)	50
学習総回数 T	30,000
閾値半径 (ノード数)	21
重心測定の対象ノード最大数 r	10
SOMの定期更新	認証100回ごと

認証サーバで$\mathrm{SOM}N_x$を作成している間に，端末では$\mathrm{SOM}_{N_{x-1}}$を用いて認証を行う．そして，端末と認証サーバとで相互通信を行う際に，それぞれから認証情報とSOMデータを交換することにより，ユーザ登録時のSOM初回作成以外でSOMの更新にかかる時間を抑えることができる．

4 評価および考察

ユーザの慣れによる認証精度の低下および本提案手法の有用性を確認するために，認証回数ごとにFRRの測定を行った．

従来手法として，以前我々が提案した認証方式[7]を用いて，従来手法および提案手法でそれぞれ400回の認証入力を行った．そして，25回ごとの認証失敗数を計測し，FRRの推移についてまとめた．表1に，認証に用いたSOMの定数および閾値を示す．閾値は，認証成功になる勝利ノードからユークリッド距離（ノード数）であり，文献[7]において最も認証精度が高かった値を用いている．

図4に，従来手法および提案手法によるFRRの推移を示す．図より，提案手法の方が従来手法よりもFRRの低減を維持していることが確認できる．また，認証100回ごとに行われるSOMの更新によってFRRが低減していることも確認できる．これにより，本提案手法は有用であり，FRRの低減を維持することで長期にわたる運用でも認証精度を維持できることが考えられる．

今後の課題として，勝利ノードの更新により

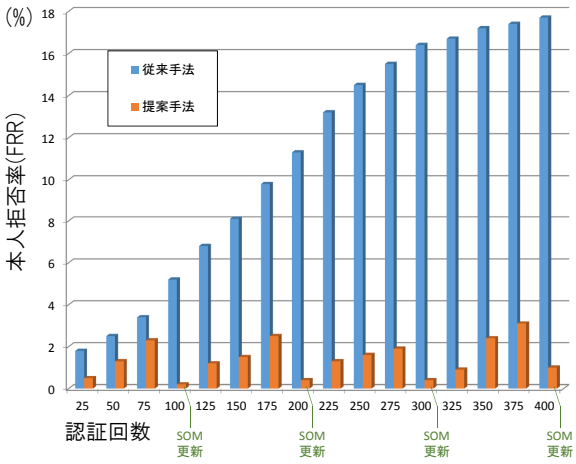

図 4: 従来手法および提案手法による FRR の推移

近傍領域になるノードが認証ごとに異なるため，それに併せて FAR も変動することが考えられる．そのため，リズム認証を長期的に運用する場合，FRR だけでなく FAR も低減し，かつ，それを維持する手法を提案する必要がある．

また，他人による認証の判定が成功になった場合，その認証情報で SOM の学習が行われるため，FRR や FAR が上がることが考えられる．このような事態を防ぐために，SOM の学習に用いる認証情報がユーザ本人の情報であるかどうかの判定が必要になる．

5 おわりに

本研究では，認証回ごとにユーザの入力情報を基に閾値の中心を移動し，SOM を定期的に更新することによって，ユーザの慣れによる認証情報の変化に対応したリズム認証方式を提案した．閾値の中心である各認証情報の勝利ノード間の重心を認証ごとに変化させることにより，ユーザの慣れによる認証動作の変化に即時対応できる．そして，端末と認証サーバとの相互通信により，効率的に SOM の更新を行うことができ，常に一定の認証精度を得ることができる．また，FRR 測定による評価実験により，提案手法は従来手法よりも FRR を長期的に低減できることを確認した．これにより，本提案手法によってリズム認証方式を長期的に運用できると考えられる．

以下に，今後の課題を示す．

- FAR の長期的な低減

  本論文では，FRR の長期的な低減について提案したが，FAR についても同様に対策を講じる必要がある．具体的な対策として，中心移動後の閾値の調整や認証失敗となったタップ情報も考慮した SOM の作成などが挙げられる．

- 登録時の SOM 初回作成による待機時間の削減

  登録時，認証サーバで SOM 初回作成が終了するまで，端末では認証を行うことができない．SOM の学習回数を削減することで認証時間の短縮を行うことも考慮しているが，学習が不十分になり，認証精度が低下することが考えられる．そのため，SOM 初回学習待機中におけるリズム認証方式の代替手法について検討する必要がある．

参考文献

[1] “スマートフォン&タブレットの業務利用に関するセキュリティガイドライン，” 日本スマートフォンセキュリティフォーラム（JSSEC），2012.

[2] 石塚正也，高田哲司，“振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案，” Computer Security Symposium 2013, pp.708-715, 2013.

[3] 高田哲司，“fakePointer：映像記録による覗き見攻撃にも安全な認証方式，” 情報処理学会論文誌，Vol.49，No.9，pp.3051-3061，2008.

[4] 喜多義弘，菅井文郎，朴美娘，岡崎直宣，西村広光，鳥井秀幸，岡本剛，“STDS 認証方式における録画解析による攻撃への耐性に関する一検討，” 第 12 回情報科学技術フォーラム，RL-002，pp.1-8，2013.

[5] 市村亮太，納富一宏，斉藤恵一，“覗き見攻撃耐性を考慮したスマートフォンにおけるリズム認証手法，” マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2013），pp.230-233，2013.

[6] 野口敦弘，納富一宏，斉藤恵一，“ボタンレスで行うリズム認証手法〜ピアノ経験者との比較によるリズムの個人差検証〜，” マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2012），pp.192-196，2012.

[7] 喜多義弘，神里麗葉，朴美娘，岡崎直宣，“自己組織化マップを利用したリズム認証方式とその認証精度に関する考察，” マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2014），pp.1011-1017，2013.

[8] T. Kohonen., “Self-Organizing Map,” Springer, 2001.

[9] 徳高平蔵，大北正昭，藤村喜久郎，“自己組織化マップとその応用，” Springer，2007.

[10] T., Chang, C., Peng, C., Tsai, Y., Chen, and P., Cheng, “Personalized Rhythm Click Based Authentication System Improvement using a Statistical Classifier,” Proceedings of 2nd International Conference on Information Communication and Management (ICICM 2012), pp39-43, 2012.

[11] T., Chang, C., Tsai, Y., Yang, and P., Cheng, “User Authentication using Rhythm Click Characteristics for Non-Keyboard Devices,” Proceedings of International Conference on Asia Agriculture and Animal, pp.167-171, 2011.

[12] Jacob, O.W., “TapSongs: Tapping Rhythm-Based Passwords on a Single Binary Sensor,” Proceedings of the 22nd Annual ACM Symposium on User Interface Software and Technology, pp.93-96, 2009.