打鍵タイミングを用いた4桁暗証番号による個人認証

納富 一宏[1]　山口 俊光[1]　石井 博章[2]　斎藤 恵一[3]　藤本 哲男[4]

[1] 神奈川工科大学情報工学科

[2] 神奈川工科大学福祉システム工学科

[3] 東亜大学経営学部経営学科

[4] 芝浦工業大学工学部機械工学科

Personal Authentication by 4 figure PIN using Keystroke Timing Pattern

Kazuhiro Notomi[1]　Toshimitsu Yamaguchi[1]　Hiroaki Ishii[2]
Keiichi Saito[3]　Tetsuo Fujimoto[4]

Abstract

In this article, we propose a personal authentication method with Self-Organizing Maps(SOM) for Web based application.

Information sharing on the World Wide Web(WWW), which is the most popular Internet service, is progressing rapidly today. Since WWW can cover the area crossed broadly, it is very effective as a means for information sharing. Unfortunately, with this global network access comes increased chances of malicious attack and intrusion. Traditional measures such as passwords and PINs are no longer adequate and we need to investigate more advanced safeguards against unauthorized access to Web based application.

We tesed the system ability to measure FRR(False Rejection Rate) and FAR(False Acceptance Rate) on the map which is learning with 56 input-vectors. For result of this ability test, our system keeps FRR and FAR 25%. Thus it seems that our method is available for personal authentication.

Keywords: Self-Organizing Maps, Personal Authentication, Biometrics Authentication, PIN with Keystroke Timing, False Rejection Rate, False Acceptance Rate, WWW

1　はしがき

コンピュータネットワークによる情報共有はここ数年で広く一般的に行われるようになった．インターネットは社会インフラとして多種多様な機能を果たすようになってきている．WWW(World Wide Web)による，広域をカバーする情報共有はその顕著な例である．社会インフラとしては，常に信頼感をもって使用することができる基盤形成が非常に重要となる．この基盤形成において，重要な意味を持つのがセキュリティ技術である．

インターネットのようなオープンなネットワーク上で医療情報に代表されるような個人情報を含む情報を共有するためには，不特定多数の人間がアクセスすることがないように個人認証手法を工夫する必要がある．

現在，広く行われている個人認証手法にIDとパスワード，または暗証番号を用いたものがある．しかしながら，この方法はユーザの記憶のみに依存する手法であり，パスワードの盗用などに対し，非常に脆弱であるといえる．

この弱点を補うための手法として，生体測定学を個人認証に応用したバイオメトリクス認証が多

数提案されている. 具体的な手法としては, 指紋や虹彩のパターンのようなユーザの生理学的特徴を用いた手法や, サインやキータイプのタイミングのような行動の特徴を用いる手法が広く知られている.

しかしながら, 指紋や虹彩, サインを用いた認証手法では専用のデバイスを用意しなければならないため, 導入コストが高くなってしまう. また, 指紋による個人認証の場合, 指紋が犯罪捜査に利用されることから心理的抵抗感を持っているユーザもおり, 導入に際しすべてのユーザの同意を得ることは難しい.[1] 法的に意味を持つ個人情報を扱うため, サンプルデータをいかに安全に保持するかという問題もある.

我々は, 導入コストがかからず, 利用者のユーザの心理的抵抗感の少ない打鍵タイミングによる個人認証手法に注目し, いくつかの提案を行ってきた.[2][3][4] これまでに提案してきたシステムでは, ユーザがパスワードを打鍵するタイミングを認証情報として用いる.

本稿では, 以前提案したシステムの評価結果をふまえ自己組織化マップ — Self-Organizing Maps : SOM — によるクラスタリングを用いてユーザの打鍵タイミングを分類し,4 桁暗証番号による個人認証を行う手法を提案する.

2 システム概要

2.1 自己組織化マップの概要

自己組織化マップはコホーネン (Kohonen) によって提案された競合学習型ベクトル量子化ニューラルネットワークである [5].

ニューロンは層状をなし, 入力データは各ニューロンに並列的に伝達される. 学習を行う前の状態のニューロンは乱数で初期化される. 入力データ $\boldsymbol{x}_i$ が投入されると各ニューロンは次式により内部ポテンシャル net_i^j を計算する.

$$net_i^j = \frac{1}{D(\boldsymbol{w}_i, \boldsymbol{x}_j)} \tag{1}$$

ここで,$\boldsymbol{w}_i = (w_{i1}, w_{i2}, w_{i3}, ..., w_{in})$ は各ニューロンの結合重みベクトルである. D は入力と結合重みベクトルとの相違を示す距離関数であり, ユークリッド距離が一般的に用いられている.

$$D(\boldsymbol{w}_i, \boldsymbol{x}_j) = |\boldsymbol{w}_i - \boldsymbol{x}_j| \tag{2}$$

この式により最大の内部ポテンシャルを示す結合重みベクトルが競合に勝ち残ったニューロンとなる. そのニューロンの近傍のニューロンを巻き込みながら, 次式に示すコホーネンの学習則にしたがって結合重みベクトルの修正を行なう.

$$\boldsymbol{w}_k^{new} = \boldsymbol{w}_k^{old} + \alpha(\boldsymbol{x}_j - \boldsymbol{w}_k^{old}) \tag{3}$$

α は学習係数と呼ばれる値で, 学習回数 t の関数で表される.

2.2 認証情報としての打鍵タイミング

本システムでは自己組織化マップ (SOM) によるクラスタリングを用いて個人の打鍵特性を抽出する. 以前提案したパスワードの打鍵タイミングを認証に用いるシステムでは Fig.1 に示す,$t_n^{press-press}$ のみを打鍵タイミングとして取得し, 認証データとして用いていた.

今回は, より精度の高い認証を行うため, より細かくタイミングを取得し入力ベクトルを生成する. ユーザがキーを打鍵するタイミングとして, ユーザがキーを押す時刻, ユーザがキーを離す時刻を記録する. 記録したタイミングをもとに, キー α を押してから次のキー β を押すまでの時間 ($t_n^{press-press}$), キー α を押してからキー α を離すまでの時間 ($t_n^{press-release}$), キー α を離してからキー次のキー β を押すまでの時間 ($t_n^{release-press}$) を計算し,SOM への入力ベクトル $\boldsymbol{x}$ として用いる.(Fig.1 参照)

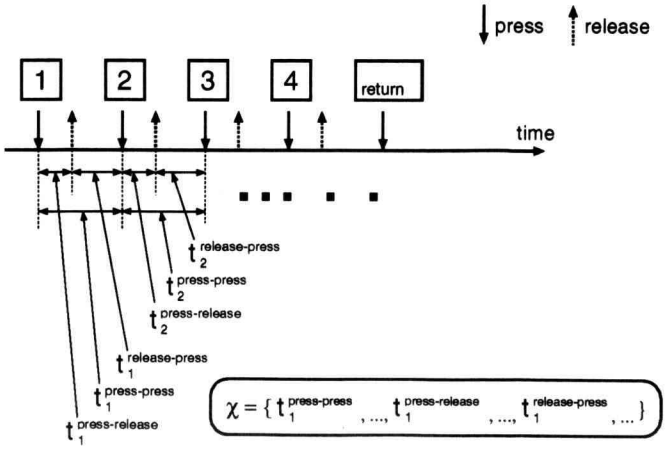

Fig 1: Keystoke Timing

本システムでは,4 桁の暗証番号を用いるので SOM への入力ベクトルの属性数は 13 となる. 具体的な入力ベクトルの例を Fig.2 に示す.

入力ベクトルの中にマイナス値の属性がある. キー入力をする際,Fig.3 に示すように, キー α を

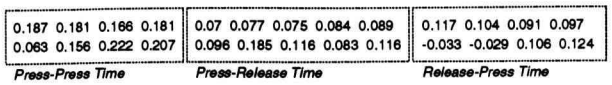

Fig 2: Input Vector

離してからキー β を打鍵する場合とキー α を離す前に, キー β を押す場合がある. キーが何も押されていない時間 ($t_n^{release-press}$) は次のキーを押した時刻と前のキーを離した時刻の差によって求めている. そのため,$t_n^{release-press}$ はマイナス値となる.

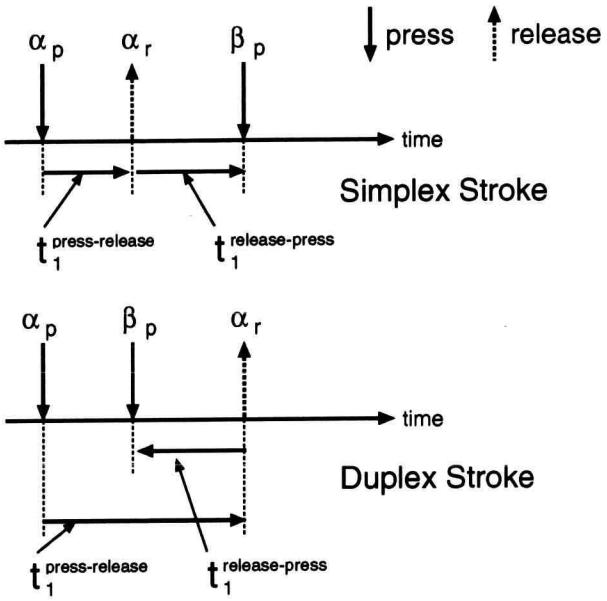

Fig 3: Simplex Stroke and Duplex Stroke

2.3 自己組織化マップによる個人認証

打鍵タイミングによって生成された入力ベクトルを用いて個人認証を行う. 新規ユーザを登録する際には, その入力ベクトルを用いてSOMの学習を行いマップを生成する. そして, ユーザの個人認証は, ログインしようとして入力した暗証番号の打鍵タイミングを先に生成したマップに配置する.

学習の用いた各ベクトルと新たに配置したベクトルの2次元平面上におけるユークリッド距離を測定する. その平均値を距離関数として定義する. 定義式を以下に示す.

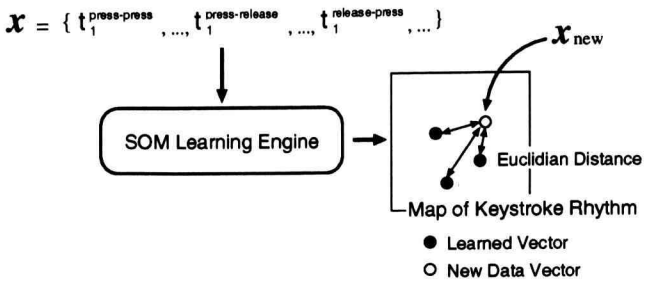

Fig 4: Map Making and Authentication

$$d = d_{userID}(s) = \frac{1}{n}\sum_{i=1}^{n}\|s - s_i\| \qquad (4)$$

その値があらかじめ設定した閾値より小さければ認証成功とし, 大きければ認証失敗とみなす. 認証関数 $Auth(d, Th.)$ を以下に示す.

$$Auth(d, Th.) = \begin{cases} Accept, & for \quad d_{userID}(s) \leq Th. \\ Reject, & for \quad d_{userID}(s) > Th. \end{cases}$$

2.4 実装システムの構成

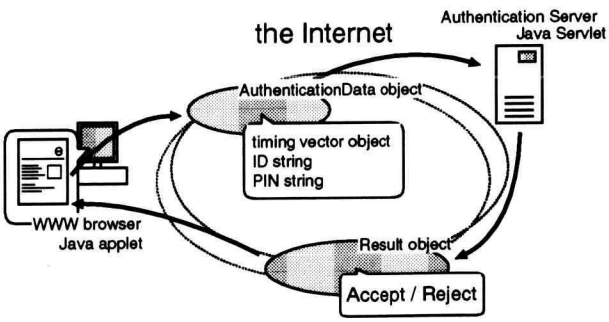

Fig 5: System Structure

実装したシステムはFig.5に示すようにクライアント/サーバで構成される2層システムの構成をとっている. クライアントはJava Appletとして実装されており, 一般的に用いられているwebブラウザ上で動作する. それゆえユーザは本システムを利用するため, あらたにソフトウェアをインストール必要はない. サーバはJava Servletとして実装されており,webサーバ上で動作する. Java ServletはCGIのようにアクセス毎にプロセスが立ち上がるのではなく,JavaVMのスレッドとしてプログラムは動作するため一般に高速で動作するという特徴がある. また,Java Appletと

Java Servlet 間の通信には HTTP を用いるという特徴がある. そのためプロキシサーバ越しに使用できるので既に構築済みのファイアウォール等のネットワーク構成を変更する必要がない.

クライアントは, フォームからユーザ ID と暗証番号を受け付け, 認証情報を AuthenticationData Object として, サーバに送信する. 暗証番号をユーザが入力する際のタイミングを同時に計測する. そのため, 通常の認証システムを使用する場合とユーザの作業は変わらない. Fig.6 に本システム, クライアントのスクリーンショットを示す.

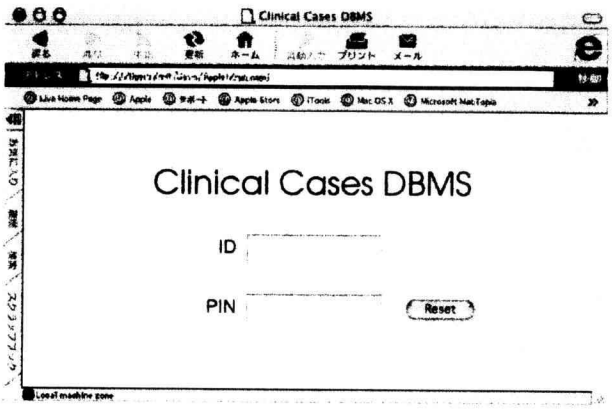

Fig 6: Screen Shot

3 評価・考察

3.1 認証精度評価

被験者 7 名を対象に認証実験を行った. 同じ暗証番号を 50 回以上打鍵させ, 各被験者のデータから, マップ生成用に 8 回分, 試行用に 40 回分をランダムに選択した. 打鍵タイミングの計測には,Sun Microsystems 社製ワークステーションに付属する日本語 Type 6 キーボードのテンキーを使用した. マップ生成用入力を用いて 2000 回の学習を行いマップを生成する. 生成するマップのサイズは 50×50 ノードである.

評価項目としてバイオメトリクス認証の評価値として広く用いられている本人拒否率 (FRR : False Rejection Rate) と他人受容率 (FAR : False Acceptance Rate) を用いる. この 2 つの項目はともにシステムのエラー率なので, 各項目の値が 0 に近ければ近いほど優れた認証システムであると言うことができる.

FRR,FAR の定義式を以下に示す.

$$FAR = \frac{\text{他人受容回数}}{\text{試行回数}} \quad (5)$$

$$FRR = \frac{\text{本人拒否回数}}{\text{試行回数}} \quad (6)$$

認証精度評価実験の結果を Fig.7 に示す.

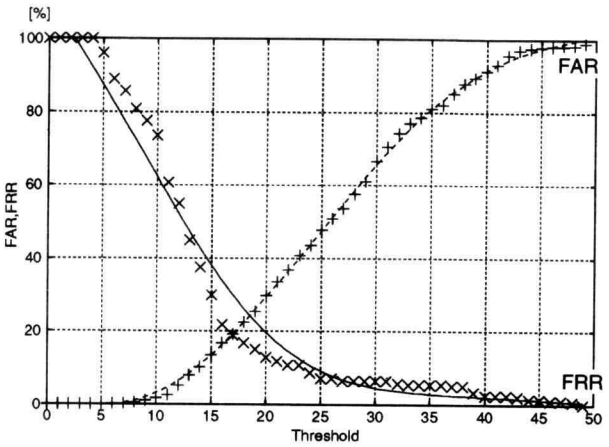

Fig 7: Result

結果は, 評価実験用の入力ベクトル 40 回分を各被験者について SOM による認証を行い, 各被験者ごと FRR,FAR を計算し, それを平均したものである. 同じ, 暗証番号を用いているので打鍵タイミングを考慮しない通常の認証システムでは,FAR は 100%になってしまう. しかしながら, 本システムを用いて閾値を 15〜20 に設定することで FAR,FRR を 25%程度に抑えることが可能となる. また, ユーザの利便性を優先し FRR を 10%にした場合でも,FAR が 50%以下に抑えることが可能となる.

Fig.8 に以前提案したパスワード打鍵タイミングによる個人認証システムの認証精度評価結果を示す. 以前のシステムでは FAR,FRR をともに最も低く抑えた 2 曲線の交点が 50%近くになっている. また,FRR を 10%以下にした場合, 以前のシステムでは FAR が 90%以上になってしまい打鍵タイミングを認証に用いる意味がほとんどなくなってしまう.

本稿で提案したシステムを用いることで, エラー率を半分ほどに抑えることが可能となった.

3.2 基本性能評価

実際にシステムを運用する上で重要なマップ生成時間, および認証にかかる時間を基本性能の評

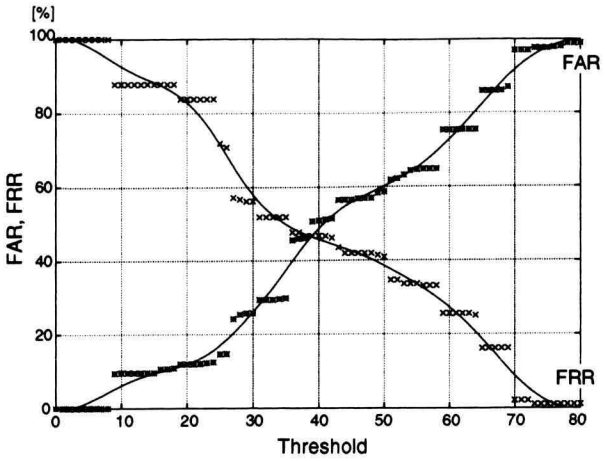

Fig 8: Result of Password Authentication with Keystroke Timing Pattern

価項目として評価実験を行った．評価実験に用いたコンピュータの仕様を Table.1 に示す．

Table 1: System Requirements

OS	SunOS 5.8
CPU	UltraSPARC IIi
RAM	256 MB
HDD	20GB
Java VM	Sun J2RE Standard Edition 1.3.0

計測結果はマシンのプロセス状況によって若干ことなるため,5 回計測をおこないその平均値を評価結果とした．評価結果を Table.2 に示す．

Table 2: Fundamental Performance of the System

マップ生成時間 [sec]	27.49
認証時間 [sec]	0.053

マップの生成に,30 秒近くの時間がかかっているがマップを生成するのは,新規ユーザ登録時だけなので,問題はないと考える．認証時間はネットワークを介して使用することを考慮に入れても,十分に短い時間で行われているといえる．

4 むすび

打鍵タイミングを用いた4桁暗証番号による個人認証について述べた．とくに,より詳細に打鍵タイミングを取得し自己組織化マップ (SOM) への入力とすることで認証精度の向上をはかるという点について,実際にシステムを構築し認証実験を行うことで検討した．以前提案したシステムに比べ認証精度が向上し,簡易な認証システムとしての有効性が示唆された．

FAR,FRR で示されるエラー率は各ユーザごとにばらつきがあり,結果として示したグラフよりかなり低い位置に交点があるユーザがいると同時に,40%近くの位置に交点があるユーザもいた．ユーザごとの結果のばらつきを抑え,認証精度を高めることが今後の課題である．

参考文献

[1] 財団法人社会安全研究財団情報セキュリティ調査委員会：情報セキュリティ調査研究報告書 (1997).

[2] 山口, 納富, 他：WWW による臨床症例検索システムの開発 — 自己組織化マップを用いた打鍵タイミングによる個人認証 (2000), 情報処理学会第 61 回全国大会講演論文集、4R-4.

[3] 山口, 納富, 他：臨床症例検索データベースの構築 — 自己組織化マップを用いた打鍵タイミングによる個人認証の改良 (2001), 情報処理学会第 62 回全国大会講演論文集、6Q-2.

[4] 山口, 納富：自己組織化マップを用いた打鍵タイミングによる個人認証 (2001), 神奈川工科大学研究報告、B 理工学編、第 25 号、pp.77-82.

[5] 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 訳.

[6] Fabian Monrose, A. R.: Authentication via Keystroke Dynamics (1997), ACM Conference on Computer and Communications Security.

[7] Fabian Monrose, A. D. R.: Keystroke Dynamics as a Biometric for Authentication (1999).

[8] Polemi, D.: Review and evaluation of Biometric Techniques for Identification and Authentication — Final Report (1997).