社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DPS－126（56）
2006－CSEC－32（56）
2006／3／17

自己組織化マップを用いたキーボード入力タイミング解析

村上　敦　　堂薗　浩
佐賀大学大学院　工学系研究科電気電子工学専攻

コンピュータシステムが現在我々の生活のほとんどすべての面に使われている。機密所持者のデータが盗まれる場合が増加する傾向にある現在では，セキュリティ技術は現在では非常に重要な問題となっている。端末のユーザー認証の主要な方法として，パスワードメカニズムが用いられる。しかしながら，静的な識別および認証は，悪意のある第３者によりパスワードを盗まれるか，推測されることがあり、安全性は不十分である。そこで，パスワードメカニズムに代わるものとして，バイオメトリクス認証が挙げられる。本研究では，キーボード入力のタイミングをバイオメトリクス認証として用いた，個人認証方式に関する研究を行った。

Keyboard input timing analysis using self-organization maps

Atsushi Murakami, Hiroshi Douzono

Computer systems are used for almost all the fields of our life now. The secret data are facing the dangerous to be stolen, thus the security technologie becomes an important problem now. The password mechanism is used as the main method of the user authentication of the computer systems, however, the the passwords may be hacked by irregular users moreover, it can share intentionally in a group, so safety of the password is inadequate. Then, to take the place of the password mechanism, a biometric authentication is used. In this research, the personal authentication method which uses the timing of keyboard input as a biometric authentication is proposed and the timing is analyzed using self organizing maps.

１．はじめに

近年，コンピュータシステムは現在の我々の生活のほとんどすべての面で使われており，パーソナルコンピュータから企業のユーザーシステムまでネットワークに接続されている。従って，機密所有者のデータを盗むことができる機会が増加する傾向にある現在では，セキュリティ技術は現在取り組むべき重要な問題である。

従来のコンピュータ・アクセス，端末のユーザの主要な方法として，パスワードメカニズムが挙げられる。しかしながら，静的な識別および認証は，悪意のある第3者によりパスワードを盗まれるか，推測されることがあり，また意図的に同じパスワードを共用することも可能で，安全性は不十分である。そこで，パスワードメカニズムに替わるものとして，バイオメトリクス認証[1]が挙げられる。

バイオメトリクス認証とは，人の生体的な特徴・特性を用いて行う本人認証方式である。従来からのパスワードなどの記憶による方式に比べ，失念，漏洩，偽造などのリスクが軽減できるため，パスワードなどにかわる安全度の高いセキュリティとして注目されている。バイオメトリクス認証には，指紋や顔や静脈，虹彩など身体的外観に基づくもの（身体的特徴）と，音声や署名など行動的特性に基づくもの（行動的特徴）がある。各認証方式にはそれぞれ長所，短所があり，一概にどの方式が優れているとはいえない。認証に際しては，指紋や顔などの全体像ではなく，特徴データと呼ばれる一部分の情報のみが求められる。認証時にインプットされた特徴データが，事前に登録された特徴データに一致するかどうかで，認証が行われる。

しかし、指紋認証のような一般的なバイオメトリクス認証では，何らかハードウェアの追加が必要となる。しかし，メインストリームのパソコン等ではコストダウンが最優先課題となっており，ハードウェアの追加が必要な認証方式は採用しにくいものとなる。そこで本研究では，バイオメトリクス認証に，キーボード入力のタイミングを用いた個人認証方式に関する研究を行った。キーボード入力のタイミングを用いた認証方式はすでに存在するが、本論文では様々な単語についてキー入力のタイミングデータを収集し、それらを自己組織化マップを用いて解析することで、認証に適した単語を選択し、システムが入力する単語を指定することで，パスワードを覚える必要のない認証方式を提案するものである。また、バイオメトリクスデータのような多次元情報の解析に自

己組織化マップが有用であることを示すことも、本研究の目的の一つである。前述のようにパスワードは最も一般的な認証方式であるが、単なるテキストデータであるため盗まれたり、あるいは、他人により推測されたりすることもあり、安全な方法とはいえない。また、最近では複数のシステムを使用するユーザも増えており、本来それぞれのシステムに別々のパスワードを設定すべきであるが、パスワードを覚えられないという理由で、同一のパスワードを設定したり、別々のパスワードをつけてもそれを忘れないようにメモしたりし、危険な状況を生み出している。本論文は、キーボード入力のタイミングという動的な情報を用いることで、パスワードを覚えなくてもシステムから指定された単語を入力することで認証を行う方法を提案するものである。研究の手順として，まず，キーボード入力のタイミングを記録するプログラムを作成した。次に，自己組織化マップを用いた解析プログラムを作成し，様々な単語から認証に適した単語を選択した。ここで選択した単語を用いて実験を行い，認証精度について議論する。

２．自己組織化マップ

自己組織化マップ(SOM:Self Organizing Maps)[2]は，1981年にKohonenによって提案された教師なし競合学習型ニューラルネットワークであり，多次元からなるデータの解析に用いられる。世の中には多くの情報があり，その情報の分析を行うことにより情報が持つ意味を把握することは非常に重要である。SOMは，データマイニング手法の一種であり，多変量情報を持ったデータどうしの相関を可視化することが可能という特徴を持っている。。一般に，データの解析には，各データ間の特徴を抽出するためのデータの可視化が重要となる。データの可視化は，各データ間の類似性などの相関の把握を容易にし，効率的なデータの統計的解析を可能にする。しかし，多次元からなるデータでは可視化が困難である。SOMは，そのような多次元のデータの統計的性質を学習し，類似した性質を持ったものどうしが近接するように低次元化を行い，データの可視化を可能とする。本論文では、キーボード入力のタイミングを入力ベクトルとし二次元平面上に単語間の関係やユーザ間の関係を可視化した。

３．キーボード入力タイミング取得方法

キーボード入力のタイミングを取得するためにはオペレーティングシステムやウインドウシステムにより別々の方法を用いる必要がある。本研究ではWindowsXP上で実験を行った。

まず、個人認証に用いるキーボード入力を取得するプログラムを作成した。キーボード入力情報はGetAsyncKeyState関数を用いて取得した。

GetAsyncKeyState関数は，キーボードの状態を非同期的に取得するWindows APIで、特定のキー（１つ）が現在押されているか、押されていないかを戻り値として返してくる。この関数を用いて英字と数字キーおよびシフトキーのスキャンを行い、キー入力を取得した。また、RDTSC命令でシステムクロックを取得することでWindowsXPで測定可能な最小の単位で時間の測定を行った。

キーボード入力を取得するプログラムは図１のような形でファイル出力を行い，それぞれのデータの意味は図２のようになる。

```
13 0.08443 0.08798 0.09755 ..... 0.04580 sagadai
15 0.10785 0.21153 0.10802 ..... 0.08984 0.14006 0.07667 arigatou
15 0.08712 0.02276 0.12870 ..... 0.08134 0.05537 0.07166 kangaeru
```

図 １：ファイル出力形式

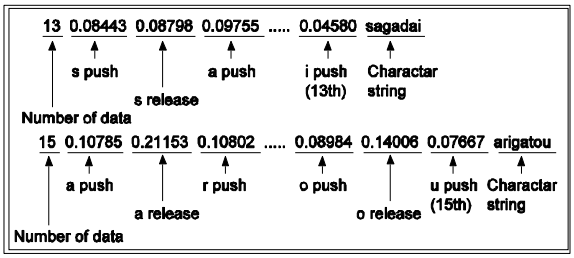

図 ２：ファイルの意味

４．自己組織化マップの解析結果と検証

まず、'sdfghjkl', 'SdFgHjKl', 'sagauniv', 'SagaUniv', 'datafile', 'Datafile', 'Ht%n&MkA'のパターンについて解析結果を述べる。Sdfghjklはホームポジションのキーを順に入力するもので、sagauniv,datafileは簡単な英単語、Ht%n&MkAはパスワードに適しているという記号入りの文字列の一つである。これらの単語について１０人の被験者から７個の単語を順に６回ずつ入力を行い、計４２０個のキー入力データを取得した。

図３は，自己組織化マップを用いて全てのユーザの全ての単語を 32x32 のサイズのマップに学習し、学習後のキー入力のタイミングをグラフとして表したものの一部（8X8 の領域）である。学習回数はデータ数の５０倍とした。各グラフの横軸がキーボードを押す離すの順番、縦軸が押していたあるいは離していた時間を表す。各グラフは形の近いものがマップ上でクラスタ化され、SOMの学習がうまく行われていることがわかる。

図４は，ある個人のキー入力のタイミングをSOMを用いて学習し、入力データをマップ上に再写像した解析結果を、入力データの単語で表したものである。マップサイズは16x16とした。なお、本論文で用いたマップは上下、左右がつながった環状マップである。各個人については、それぞれ単語毎に集まる傾向にあり、単語ごとには、ほぼ同じタイミングで入力していることがわかる。

図５は単語datafileについてキー入力のタイミングをSOMを用いて学習し、入力データをマップ上に再写像した解析結果を、ユーザ番号を用いてラベル付けしたものである。図５のマップでも同じユーザ番号が二次元平面状でクラスタ化されているのが見て取れるが，よりわかりやすくするために全ユニットにラベル付けを行った図６のような形で，これ以後解析結果を表示する。図６から図９では，各ユニットに対して，最も近いキー入力タイミングのユーザー番号でラベル付けをした。前述の７個の単語に関して、最も良い場合の結果と、最も悪い場合の結果を図６と図７にそれぞれ示す。

良好な結果であると個人毎にクラスタ化されたマップが出力される。図６ではユーザによってはある程度クラスタ化された結果になったが，図７では，ほとんどのユ

ーザに関してクラスタ化されているとは言えず，良好な結果は得ることができなかった。

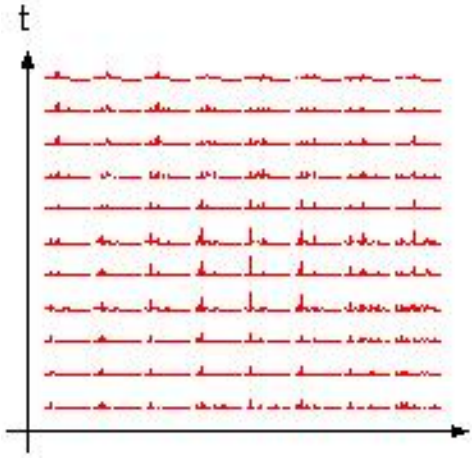

図３　全体の入力データのマップの一部

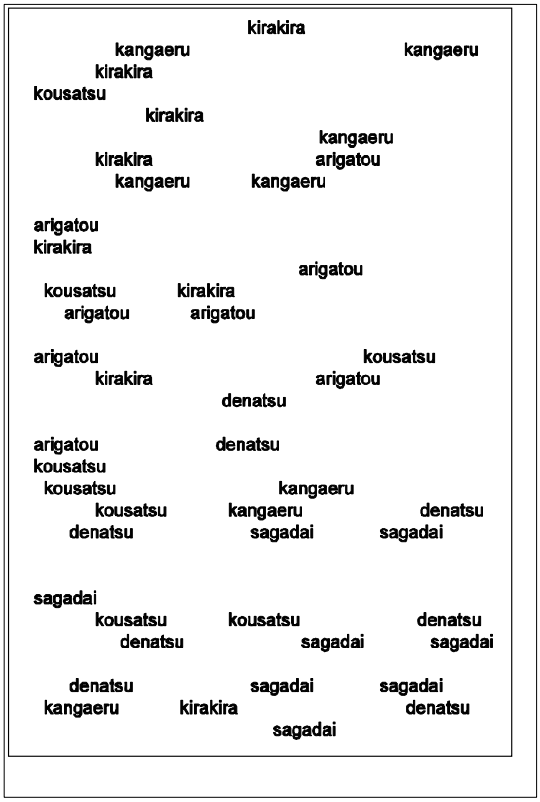

図４：ある個人の単語マップ

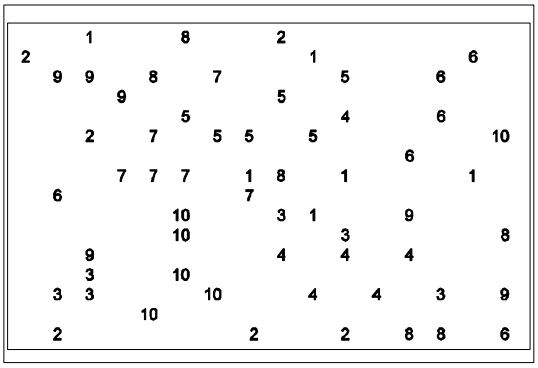

図 3：datafile のユーザマップ(1)

2	2	1	1	8	8	8	2	2	1	2	2	8	8	6	6
2	9	2	9	8	8	7	8	2	1	5	1	8	6	6	6
9	9	9	9	8	8	7	2	5	5	5	5	8	6	6	6
9	9	3	9	9	5	8	2	5	4	5	5	6	6	6	6
10	2	2	9	5	5	5	5	5	5	4	1	6	6	6	10
10	2	2	1	7	5	5	5	5	5	4	2	6	6	10	10
10	2	2	1	7	7	1	1	8	1	1	1	6	6	1	10
6	6	6	7	7	7	1	1	8	1	1	3	6	1	1	1
6	6	6	7	7	1	1	7	1	3	1	1	9	1	1	1
1	6	6	10	10	10	10	1	3	1	3	9	9	9	9	8
8	9	9	9	10	10	10	1	4	3	3	3	4	9	8	8
9	9	9	9	10	10	10	4	4	4	4	4	4	4	8	8
9	3	3	3	10	10	10	2	4	4	4	4	4	3	9	9
3	3	3	3	10	10	10	10	4	4	4	4	3	3	3	9
9	9	3	10	10	10	10	2	2	4	2	2	8	3	9	9
9	2	2	2	10	8	2	2	2	2	2	8	8	8	6	6

図 4：datafile のユーザマップ(2)

5	4	4	4	5	4	1	7	7	7	2	2	8	8	8	5
5	5	4	8	4	4	4	7	7	7	7	2	8	8	5	5
5	5	8	8	4	4	4	7	7	7	1	9	9	3	3	5
1	1	1	8	4	4	5	5	1	1	9	9	9	2	2	3
1	1	1	4	4	4	5	1	1	1	8	9	2	10	10	10
1	1	1	9	4	2	5	1	1	8	8	8	10	10	10	10
1	9	9	9	9	2	2	10	10	10	8	9	9	10	10	10
6	6	6	9	9	2	8	8	10	10	9	9	3	10	10	10
9	6	6	8	8	9	8	8	10	10	10	3	3	3	10	9
9	6	6	8	8	8	8	3	6	10	6	6	3	3	3	9
9	6	6	8	2	2	7	3	6	6	6	6	6	3	3	3
4	4	9	2	2	3	7	7	7	7	6	6	6	6	6	6
4	9	9	2	2	10	3	5	7	7	7	8	6	6	6	6
3	9	9	2	5	10	5	5	5	7	9	1	6	6	7	7
5	2	2	5	5	5	1	5	9	9	1	1	1	7	7	7
5	5	4	4	5	1	1	1	7	7	7	1	1	8	7	5

図 7：Ht%n&MkA のユーザマップ

要因としては，入力してもらった文字列が、単純な単語であっても、普段使い慣れていない文字列だったために，このような結果になったのではないかと思われる。その中でもシフトを押す文字列の場合は，シフトキーを押しながらキーボード入力する機会が少ないのが理由に挙げられる。

また，'Ht¥%n¥&MkA'のようにパスワードには適しているると適していると言われている記号が混じった文字列の場合，記号は普段使わないためキーボードを見て入力をしているようで取得している時間にばらつきが出て，そのため解析結果のマップがクラスター化されていないと推測できる。

以上より，普段使い慣れていない単語や、シフトキーを押す大文字や，記号が混じった文字列であると個人認証は難しいことがわかった。

日本人の場合，多くのユーザは日本語入力にローマ字を用いており，また，ワープロでの文章作成から，WEBでの検索まで，日本語を入力する機会は非常に多い。そこで，'arigatou'，'denatsu'，'kangaeru'，'kirakira'，'kousatsu'，'sagadai'のパターンについて解析結果を述べる。入力を取得する際は日本語（ひらがな）での記述と、入力を行うローマ字の記述方法を表示してユーザに入力してもらった。また、この実験をおこなった被験者は 10 人であるが、前回の被験者と全員が同じではない（同一ユーザをあつめることができなかったため）。また、今回は認証実験にもちいることも考えて、１人あたり８回ずつ入力をおこなってもらった。

前述の実験と同様に単語ごとにマップを作成し、最も良い結果の場合と、最も悪い場合の結果を図８と図９にそれぞれ示す。結果を見ると図８，図９ともに、図６と比較してもユーザごとに、よりクラスタ化されており，良好な結果は得ることができた。

その中で入力方法が複数存在する，'denatsu'，'kangaeru'，'kousatsu'の 3 パターンは，人によっては普段の入力方法と異なるためか，クラスタ化されていないユーザもいた。

それに対して，'arigatou'，'kirakira'，'sagadai'の 3 パターンは，ローマ字の入力方法が 1 パターンしか存在しないことと，入力が簡単であるため，一部のユーザを除いてキーボード入力が安定して良好な解析結果が得られたと考えられる。ただ、コンピュータの使用時間が短くキーボード入力が苦手なユーザ（例えばユーザ５）はクラスタ化されなかった。

全体の実験で、最も良好なデータとしては、図８の文字列'kirakira'の結果と思われ，クラスタ化の状況を考えると、同じ文字列を用いてもキーボード入力のタイミングにより，個人を認証することは可能ではないかと考えられる。これらの結果を踏まえて以下の個人認証実験を行った。

5	5	3	3	3	3	4	4	4	7	7	7	7	10	7	7
1	1	3	3	3	3	3	4	10	10	10	10	10	7	7	7
1	1	1	3	3	3	3	3	10	10	10	2	10	10	7	7
1	1	1	3	3	6	3	10	10	10	10	2	10	10	10	7
6	6	3	6	6	6	3	10	10	10	10	2	2	2	7	6
6	6	6	6	6	6	10	10	10	8	8	10	2	10	6	6
6	6	6	6	6	6	10	10	2	2	6	8	8	6	6	6
6	9	6	6	6	6	2	2	2	2	8	8	1	1	6	6
9	9	6	6	6	2	2	2	2	6	6	8	1	1	1	1
1	9	9	6	6	2	2	2	2	8	8	8	3	3	1	1
1	9	9	9	6	6	2	2	8	8	8	8	3	3	1	1
1	9	9	9	6	6	6	8	8	8	8	8	3	3	1	1
1	9	9	9	8	8	8	4	4	8	8	10	3	1	1	1
1	9	9	4	4	4	4	4	4	4	7	7	7	7	7	1
6	6	6	4	4	4	4	4	4	7	7	7	7	7	7	7
6	6	6	3	4	4	4	4	4	7	7	7	7	7	7	1

図 8：kirakira のユーザマップ

3	1	3	3	3	3	6	4	7	7	7	10	10	7	10	2
3	1	5	1	1	3	9	4	8	7	7	10	10	9	2	2
3	5	1	1	1	1	9	8	8	8	7	10	10	2	4	3
5	5	5	1	1	1	5	6	8	8	9	9	2	4	4	8
8	5	5	1	1	1	5	6	6	6	9	2	2	4	4	8
9	9	5	5	1	5	5	6	6	6	2	2	2	6	4	9
9	5	5	5	5	5	5	3	3	6	2	2	2	6	4	4
4	4	4	8	8	8	3	3	3	3	2	2	2	6	4	4
4	4	5	8	8	3	10	3	3	6	6	9	3	8	8	4
4	4	5	8	3	10	2	10	4	6	6	9	3	4	8	6
6	7	7	6	3	10	10	10	4	6	6	4	2	4	8	6
7	7	7	6	6	3	3	4	4	4	10	3	3	5	5	6
6	7	7	6	10	10	6	6	4	10	7	7	2	3	5	10
10	7	7	7	10	6	6	7	10	10	10	2	2	2	10	10
10	7	7	3	10	6	6	7	10	10	10	2	2	7	10	10
2	1	3	3	3	3	6	4	7	10	10	10	7	7	7	10

図 9：denatsu のユーザマップ

５．個人認証実験

次に個人認証実験の結果を述べる。前節での解析により単語'kirakira'が認証には適していると考えられるが、比較のためその他の単語についても認証実験を行った。

また、前節では取得したデータを全て用いてマップを学習させたが、この節では取得したデータの半分を学習用に、残り半分を認証用に用いた。認証はSOMを用いて行い、検証用のデータに一番近いユニットにラベル付けされユーザ番号が、入力したユーザと等しいとき認証されたものとした。

まず、最初に取得した英単語、記号混じりの単語に対して、SOMで解析した際，最も悪かった'Ht%n&MkA'と，最も良かった'datafile'の個人認証を行った。それぞれ表１，表２に示す。表１では本人受入率が１００％になる人がおらず０％の人が多かった。表２に示す'datafile'は本人受入率が１００％の人が２名おり，SOMでの解析結果が反映されていると考えられる。

次に，ローマ字の単語について，SOMの解析結果が、最も悪かった'denatsu'と，最もよかった'kirakira'の個人認証を行った。それぞれ表３，表４に示す。表１，表２と比べ，本人受入率も上がりより良い結果になっている。ただし、表４においても、本人受入率が100%となっているものは２人であり、本人受入率が75%のユーザに関しては２回入力してもらえば認証可能ではないかと考えられる。他人受入率も本人受入率が高いユーザでは5%以下と十分低くなっている。このような結果になった原因のひとつとして実験方法が考えられる。今回の実験では、全ての単語を順番に全て入力することを８回繰り返してデータを取得したが、自分自身が被験者になったときでも最初の数回で飽きてしまい、最後の方は入力が乱れてきた。今回の認証実験では、最初の半分を学習用に、残りの半分テスト用に用いたため、テスト用のデータの方が質が悪かったのではないかと考えられる。

表 1：Ht%n&MkA を個人認証に用いた結果

	本人受入率[%]	本人拒否率[%]	他人受入率[%]
User1	66.7	33.3	0.0
User2	0.0	100.0	22.2
User3	0.0	100.0	16.7
User4	33.3	66.7	5.6
User5	33.3	66.7	22.2
User6	33.3	66.7	33.3
User7	0.0	100.0	5.6
User8	0.0	100.0	16.7
User9	0.0	100.0	0.0
User10	0.0	100.0	16.7

表 2：datafile を個人認証に用いた結果

	本人受入率[%]	本人拒否率[%]	他人受入率[%]
User1	0.0	100.0	0.0
User2	0.0	100.0	44.4
User3	0.0	100.0	16.7
User4	33.3	66.7	5.6
User5	0.0	100.0	0.0
User6	66.7	33.3	0.0
User7	100.0	0.0	0.0
User8	33.3	66.7	33.3
User9	0.0	100.0	5.6
User10	100.0	0.0	0.0

表 3：denatsu を個人認証に用いた結果

	本人受入率[%]	本人拒否率[%]	他人受入率[%]
User1	100.0	0.0	0.0
User2	25.0	75.0	23.8
User3	0.0	100.0	9.5
User4	50.0	50.0	4.8
User5	25.0	75.0	9.5
User6	0.0	100.0	9.5
User7	50.0	50.0	14.3
User8	50.0	50.0	9.5
User9	25.0	75.0	4.8
User10	75.0	25.0	9.5

表 4：kirakira を個人認証に用いた結果

	本人受入率[%]	本人拒否率[%]	他人受入率[%]
User1	50.0	50.0	0.0
User2	100.0	0.0	4.8
User3	25.0	75.0	19.0
User4	100.0	0.0	4.8
User5	0.0	100.0	4.8
User6	75.0	25.0	4.8
User7	75.0	25.0	9.5
User8	75.0	25.0	9.5
User9	75.0	25.0	4.8
User10	75.0	25.0	4.8

最後に新たに被験者１０名のログイン名を表示させ、被験者１０人全員に８回ずつ入力してもらったデータを用いて認証実験を行った結果を表５に示す。

表 5：各自の名前を個人認証に用いた結果

	本人受入率[%]	本人拒否率[%]	他人受入率[%]
User1	100.0	0.0	0.0
User2	100.0	0.0	0.0
User3	100.0	0.0	2.8
User4	75.0	25.0	2.8
User5	75.0	25.0	11.1
User6	50.0	50.0	2.8
User7	100.0	0.0	5.6
User8	100.0	0.0	5.6
User9	0.0	100.0	5.6
User10	50.0	50.0	11.1

一人を除けば本人受入率は５０％を越え，他人受入率も低く、キーボード入力のタイミングを用いた個人認証方式ができる可能性を示すことができたと言える。また、今回の実験ではSOMを用いて認証実験をおこなったが、全ての入力データがどれかのユニットに写像されると言う点で、本来、SOM自体は認証には向いているネットワークではないといえる。そのため、SOMの学習結果から標準パターンと認証を行える誤差の範囲を自動的に決定し、認証システムを構築する必要があると考えられる。

６．まとめ

本論文では，キーボード入力のタイミングを用いた個人認証方式に関する研究を行い，同じ文字列を用いてもキーボード入力のタイミングにより，個人を認証できる可能性を示した。課題として。認証の識別が付きやすい単語など，さらにデータを収集し、解析することがが挙げられる。また，キーボードに加速度センサーなどを取り付け識別情報を多くすることなどが，今後の課題である。

参考文献

1) http://www.biometrics.org/
2) T.コホネン:'' 自己組織化マップ(SELF-ORGANIZING MAPS) '',(1996)