平成21年度　特別研究報告書

SOMを用いたキーボード入力による個人認証

龍谷大学　理工学部　情報メディア学科

学籍番号 T060553　香島　健

指導教員　指導教員名 三好　力　教授

目次

第一章　はじめに

1.1研究目的

企業や一般家庭で急速にコンピュータが浸透してきた昨今、利便性や多様性が向上し様々な場所から手軽にネットワークに接続できるようになった。しかし、便利になった反面機密の情報や、個人情報などを盗み出そうとする人間が現れてきてしまう。そこでコンピュータにはパスワードシステムを代表とする本当に使用者本人かを識別するシステムが複数考えられている。しかしいずれも弱点があり万能ではない。

例えばパスワードであれば確かに予め文字列なり数列なりを登録しておき、次からは確認画面でコレを入力するだけで本人確認を取ることができるが、便利な反面悪意のある第三者に文字列を盗まれるとそれで全て通過されてしまう上、複数パスワード認証を用いる場合その全てを記憶していなければならない。記憶するのが困難だからと言ってメモなど目に見える形で置いておくと、セキュリティ能力が著しく低下する。またこれを解消するために複数の認証に共通の文字列を用いると、記憶が容易な分一つがばれると全てを通過されてしまうため、これもセキュリティ能力が著しく低下する要因になる。文字列を使い分けると記憶することが困難に成り、文字列をメモしておいたり、同じ文字列を使いまわしたりすると、セキュリティ能力が低下する。パスワード認証は簡単な分、解決できない問題をはらんでいる。以下にパスワードに対する意識調査を示す。

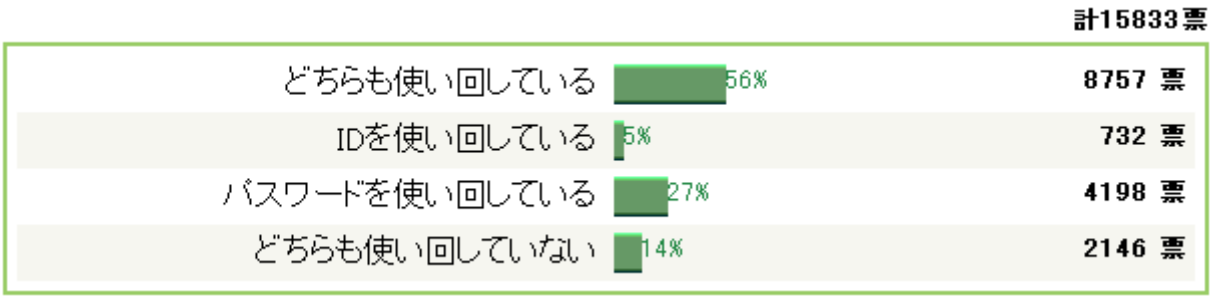

図1. パスワードおよびIDの意識調査

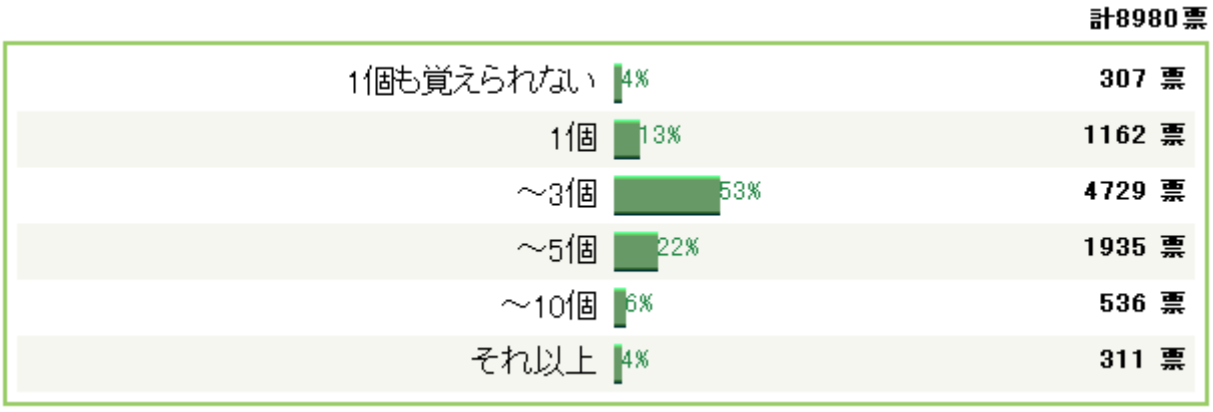

図2. パスワード暗記可能数の意識調査

（yahoo!ニュースより引用）

そこでパスワードに代わり近年用いられてきているのが人が持つ体の特徴を用いて個人の認証を行う生体認証である。パスワードとは違い他人と一致することのない生体の情報を用いることで、パスワードに比べセキュリティ強度が格段に上昇している。しかし生体認証はパスワード認証にはない問題を持っている。まず、基本的に生まれ持った不変の情報を用いる事になるため、一度不正アクセスを許してしまうと、同じセキュリティを用いることが不能になってしまう事が挙げられる。此の問題は他の部位や方法を用いる事でセキュリティを掛け直し情報を守ることが可能である。しかし二つ目の問題としてコスト・設備の問題がある。生体認証は往々にして認証に用いる機器にコストが大きく掛かってくる。個人などで用いる場合はコストは大きな問題にならないかもしれないが、コストを出きるだけ抑えていきたい企業等ではやはり採用しにくいだろう。

そこで本研究では、パスワードのように単純ではなくコストも控えめに出来るような認証方法として、文章入力による個人認証を提案する為の前段階として文章入力によって人間を識別可能であるかを自己組織化マップ（SOM）を用いて実験を行い、検証を行っていく。実験の方法としては、まず被験者に予め指定された文字列（今回は”私は学生です”と”青天の霹靂”を使用した）をローマ字で入力してもらう。このとき、キーボードの入力時にキーを押す、離す度に時間のデータを収集するプログラムを用いて時間のデータを収集する。収集したデータを SOM-PAC というツールを使用して二次元マップに変換し、キーボード入力で個人の識別が可能であるかを見る。

自己組織化マップを用いる理由として、SOMは多次元のベクトルにより表されたデータを、その特徴を残し他のデータとの相互関係を保ったまま 2 次元のマップに写像することが出来るため、多次元のデータ関係が 2 次元平面状の距離として表され視覚的に理解しやすいためである。

1.2 SOMとは

自己組織化マップ（Self-Organizing Map,以下 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、入力層と出力競合層の2つの層から成っている。SOMは、1980年代にコホーネンによって開発され、多次元データの分類、解析に効果的な技術として知られている。

SOMの特徴は、n次元のベクトルの集団を学習することにより2次元のマップにそれらのベクトルの関係を写像することが出来るのである。似ているベクトルは2次元のマップ上の近い位置に配置され、似ていないベクトルは遠い位置に配置される。認識、予測、分類など様々な分野に応用が利き、汎用性に優れていることから色々な分野での活躍が見込まれる。

1.2.1 基本のアルゴリズム

コホーネンは、生物の神経細胞、特に脳の情報処理の仕方を、以下のような簡潔な式に整理した。

$$m_i(t+1)=m_i(t)+h_{ci}(t)(x(t)-m_i(t)) \tag{1.1}$$

この式はおおむね次のようになっている。いま神経細胞（ノード）i が時刻 t で処理している情報処理能力を $m_i(t)$ とするとき、外部から入力信号 x(t)が入ってきたとする。細胞はこの入力信号を学習して次の時刻には入力信号により近い情報処理能力 $m_i(t+1)$ を持つようになる。

このとき x(t)が n 次元のベクトルだったとすると、参照ベクトルとも呼ばれる $m_i(t)$ もまた同じ n 次元の要素を持つ。そして $h_{ci}(t)$ は学習率係数を含めた近傍関数を意味する。

なお、t=0,1,2・・・は離散時間座標である。競合層のベクトルは参照ベクトル $m_i(t)$ で表され、入力層の次元に合わせて n 個の要素を持っている。出力を視覚的に見るために、普通2次元に配列されている、この様子を図3に示す。

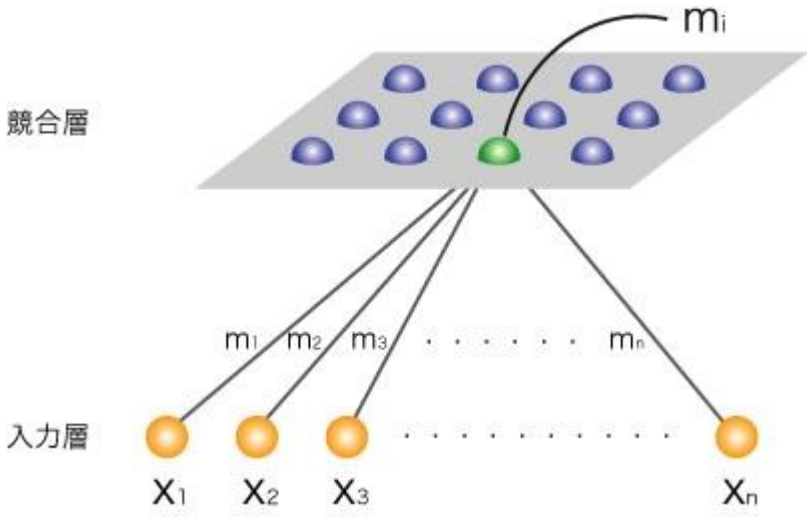

図3. SOM の構造

学習は次のようにして行われる。入力ベクトル x(t)は、ある測度、例えばユークリッド距離

$|x(t)-m_i(t)|$ を最小にするノードiを探し、それに添え字cをつけることにする。

$$|x(t)-m_c(t)|=min|x(t)-m_i(t)| \qquad (1.2)$$

式(1.2)で決められた参照ベクトル $m_c(t)$ を持つノードを勝者ノードと呼ぶこととする。上記の式(1.1)及び(1.2)の状態を図を用いて簡単に紹介する。まず入力信号が感知されると、まっさきにこの信号に一番近いノードが勝者ノードになる。そして勝者ノードの周りを正方形に囲った図では、円で囲われた領域を近傍領域として定義することにする。なお近傍領域の形は円ではなく正方形でも構わない。更に基本ノードの配列を六角形にすると、六角形近傍ともできる。

近傍内の全てのノードは入力されたベクトルを学習し、式(1.1)に従って学習を行った全てのベクトルが入力ベクトルの方向に少し傾く。学習を決められた回数繰り返していく。このときに、最初は近傍領域を大きくとっておき、学習を繰り返すごとに徐々に近傍領域のサイズを小さくしていく。

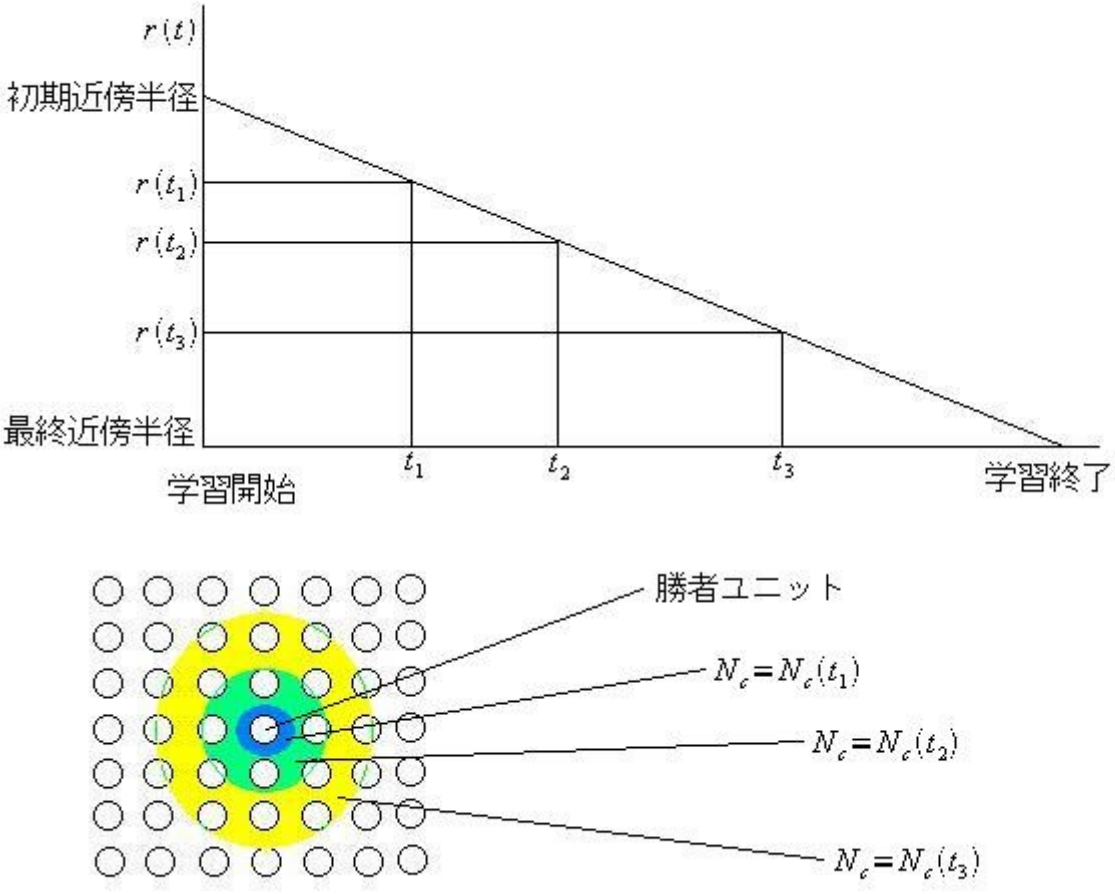

図4. 自己組織化マップの学習の進度 $(t_1<t_2<t_3)$ に伴う近傍サイズの変化

ここで式(1.1)において、 $h_{ci}(t)$ は学習率係数 a_t と近傍関数 $h(d,t)$ により、次のように表現することが出来る。

$$h_{ci}(t)=a(t)\cdot h(d,t) \qquad (1.3)$$

近傍関数は、学習される近傍領域を指定している関数である。出力競合層の勝者ノードの近傍を意味し、学習によって学習ベクトルが更新されていく領域になっている。学習をスタートさせるときには、近傍領域とするその範囲を大きめにとっておき、学習が進んでいくにつれ徐々にその範囲を狭くとっていく。近傍領域を減少させる関数には線形型とステップ型が存在するが、ここでは使用されることが多いガウス型近傍関数について簡単に紹介を行う。

$$h(d,t)=\exp(-d^2/k(r(t))^2) \qquad (1.4)$$

ここで d は式(1.5)で表される勝者ノードから参照ベクトルまでの距離、 $k(r(t))$ は学習時間 t のときの近傍領域のとる最大距離となっており、ガウス関数の波幅の係数である。

$$d^2=(x-a_i)^2+(y-b_i)^2 \qquad (1.5)$$

ここで、 $(a_i,b_{[i]})$ は勝者ノードの位置、(x,y)は半径 r(t)により成っている円形領域の内側にあるノードの位置を示している。近傍半径 r(t)は、学習の開始状態のときは大きく、学習が進むにつれて徐々に小さくなっていく。半径 r(t)の円の領域に含まれる範囲のノード、参照データは指数関数で決まるウェートを持って学習される、このことから勝者ノードに近いほど、その類似性が大きくなっていくように学習され、勝者ノードから遠ざかるほどその類似性が小さくなるように学習されていく。無論、近傍領域外のノードでは学習自体が行われない。

したがって、式(1.1)による学習中は近傍 N_c 内のノードに関しては、 $h_{ci}(t)=a(t)\cdot h(a,t)$ で、 N_c 外のノードに関しては、 $h_{ci}(t)=0$ である。これにより、近傍の外側に配置されているノードでは学習は行われない。

結局のところ、近傍関数は以下の式で表すことができる。

$$h_{ci}(t)=a(t)\cdot h(d,t)(i\subset N_c)$$
$$h_{ci}(t)=0 \qquad (\text{それ以外}) \qquad (1.6)$$

このとき、a(t)の値を学習率係数と呼び、0<a(t)<1 の値を持つ、a(t)と N_c の大きさは両方とも学習時間がたつにつれて普通は単純減少させる。a(t)は次のような式でたとえることが出来る。

$$a(t)=a_0(1-t/T) \qquad (1.7)$$

ここで a_0 は a の初期値になっており、通常 0.2~0.5 の値を選ぶ。Tは行われるべき学習での予定された全体の更新学習回数になっている。ただし、式(1.1)中、比例係数の a(t)は、学習の最初に大きな値を設定するようにしておき、学習が進んでいくにつれて、だんだんと小さい値に変化していくように設定しておく。また、近傍領域 $N_c=N_c(t)$ も式(1.6)と同様に減らしていくことが可能になっている。つまり、

$$N_c(t)=N_c(0)(1-t/T) \qquad (1.8)$$

ここで、 $N_c(0)$ は初期値である。

コホーネンの SOM アルゴリズムを整理すると、次のようになる。

1. 出力層にノードを配し、それぞれの持つ参照ベクトルをランダムな数値で初期化する。

2. 入力ベクトルと最もよく一致する競合層での参照ベクトルを探し、これを勝者ノードと定義する。

3. この勝者ノードの近傍のノードを式(1.1)に従って更新する。

SOM の学習を行うためには学習パラメータを設定する必要がある、以下で主要な学習に使うパラメータと簡単な解説を記す。

学習回数出力:競合層に対して学習を何回行うかをここで指定する。

学習係数:1 回の学習でノードをどれだけ更新するのかをここで指定する。

近傍半径:実験開始時の学習円のサイズをここで指定する。

マップサイズ:出力競合層のノードをいくつ並べていくかをX軸方向にいくつか、Y軸方向にいくつかという形式でここで指定する。

第二章　既存の技術と問題点

近年急速にコンピュータシステムは広がりを見せ、現在ではコンピュータシステムは我々の生活のありとあらゆる面で使用されており、家庭のパーソナルコンピュータから企業のシステムサーバにいたるまで同じネットワークに接続されている。以上の事より必然的に他のコンピュータやサーバーに接続し、個人情報や顧客情報などを盗み出す事ができる機会が増加した現在では、コンピュータのセキュリティの問題は非常に重要な問題になってる。そこで活躍してくるのが既に述べたパスワード認証やバイオメトリクス認証であるが、便利な点が多い反面問題点もやはり存在してくる、以下にそれぞれの認証方法の問題点を挙げる。

2.1 パスワード認証の問題点

今現在恐らく殆どの方が一度は触れたことがあり、かつ一番普及しているのがパスワード認証方式であろう。銀行の暗証番号も広義ではこれに含まれる。サーバー側のプログラムが難解ではなく、開発費用が他のシステムに比べて安価に抑えることができ、認証を行うに際して特別な装置が必要でない。認証を行うほうもあらかじめ登録しておいた文字列を入力するだけなので非常に簡単である。

たしかに利点も多いので普及しているのにも納得がいくが簡単に出来る分弱点も多い、以下に考えうる弱点を記す。

・攻撃者に推測されやすい

まず絶対的な条件として、登録した文字列を忘れずに覚え続けていなければならないということである。そのため殆どの人間が覚えやすい単語や数字の文字列をパスワードにしてしまうことが多い。辞書に載っている単語では、攻撃する側にとっても簡単に推測できてしまうし、またコレを実行するための違法ソフトウェアも存在する。利用者の家族やペットに関連した文字列にしたとしても、個人情報を取得されれば攻撃者に簡単に突破されてしまう。よく暗証番号に生年月日を設定する人がいるが、正直致命的である。

・漏洩しやすい

文字列を入力するだけで認証が可能になるということは、逆に文字列がばれてしまえばそれで終わってしまう。パスワード自体も通信回線を盗聴されたり、キー入力を記録するプログラムなどを秘密裏に起動されているといとも簡単に盗み取られ利用されてしまう。

・漏洩した場合の影響期間がながい

一度パスワードを盗まれてしまうと、その事に気がつくまではずっと不正利用されてしまう。更に盗まれた事に気がつくのは必然的に損害を受けてからになってしまう。

・パスワードを覚えられない

上記の対策として推測されにくい言葉を使用したり、短い期間でのパスワードの変更を行ったりしているとそれだけパスワードを記憶しておくことが困難になってくる。たった一種類のパスワードであれば覚えることは可能だが、キャッシュカードやクレジットカードなどそれぞれ何枚も存在し、別々のパスワードを設定していると、とても覚えておけるものではない。これを回避するために全部に同じパスワードなどを指定していると、一気に安全性が低下するし、盗まれた場合に損害が膨大になることもありうる。パスワードを覚えやすい文字列にしたり、同じパスワードを複数用いたりす

るとパスワードが盗まれたときの被害がすさまじい事になり安全性が著しく低下する。かといって、複数のパスワードをもちいたり、覚えにくい複雑な文字列を用いると覚えられなくなってしまう。パスワードをメモすればいいかもしれないが、メモという形で保存してしまうと安全性に問題が生じてしまう。どちらに比重をおいても片方が悪化するため、このもんだいには解決策は存在しない。

2.2 バイオメトリクス認証の問題点

パスワード認証に変わり最近色々なところで用いられているバイオメトリクス認証だが便利な反面コチラにも弱点は存在してくる。ここでは上で述べたそれぞれの認証方法の問題点を洗い出してみる。

・指紋認証の問題点について

人間の指に存在する紋様である指紋を用いて個人識別を行う指紋認証、たしかに個人固有の物を用いるのでセキュリティ強度は高いが、高めるに当たっていくつか弱点も存在してしまう。

・専用のハードウェアが必要

指紋で個人を認証するためには指紋を読み取るためのハードウェアと、認識した指紋を記録、処理し認証に必要な状態に持っていくためのソフトウェアがそれぞれ必要となる。これらを用意しようとするとどうしても資金が必要になってきてしまい、気軽に取り入れられるものではない。

・偽装の方法がある程度完成してしまっている

バイオメトリクス認証の中でも、最古参に相当する指紋認証ではやはり何点か偽装の方法が生み出されてしまっている。残留指紋をゼラチンに写し取って人工指を作成し、その人工指で認証を通過させることに成功しているので、安全性に疑問が残ってしまう。さらに、木工用ボンドを利用してスライド式の指紋認証を突破できると日本の学生が提唱している。また、実際に実システムに対して指に特殊なテープを張って指紋の変造を行った事件も発生している。。

・指が損傷すると認証不能になる

指紋認証は指紋を用いるので、指を傷つけると当然認証することは不可能になってしまう。修復可能な軽い損傷ならいいが、やけど等形が変形してしまう損傷だと永遠に認証する手段は失われてしまう。実際にゴルフで手が荒れてしまっただけで認証されなくなった例もそんざいする。

・網膜認証の問題点について

人間の目の部分に存在する網膜を用いた認証は、その網膜の終生不変性から高い認証精度を発揮するが網膜を利用するが故の弱点も存在する。

・装置が非常に高価

網膜認証に用いられる装置は非常に高価なものになっており、安易に採用できるものではない。なおこれは他のバイオメトリクス認証にも言えることである。

・疾患の影響を受けやすい

網膜は非常に疾患の影響をうけやすく、白内障や緑内障、糖尿病や高血圧症によって網膜パターンが影響を受け認証されなくなった例も報告されている。

・認証の方法が特殊

網膜認証を行うためには、網膜スキャナに対象者が顔を突き出し、目に赤外線を照射するという手順を踏まなければならない。そのために認証者には心理的なストレスが発生してしまう。

・照明の具合に影響される
　赤外線を用いるため、照明や他の光の影響を受けやすく、環境が変化すると認証が困難になる場合がある。

・虹彩認証の問題点について
　虹彩認証の認識力は、眼鏡やコンタクトレンズを装着していても低下することはなく環境にも左右されにくいが万能ではない。

・新しい技術であるが故の弊害
　虹彩認証は比較的新しい技術であり、既に指紋等を生体認証に利用している場合、新たに投資をする必要が出てくる。更に出入国手続きなどに用いる場合などは、最悪法律の改正等が必要になってくる。

・認証の面倒さ
　数メートル以上はなれると認識できないうえに、対象者が頭を動かしていたりカメラに目を向けていなかったりすると認識できない、更に普段行わないような行動を取らなければならないため、精神的負荷も掛かってくる。

・画質の問題
　他の画像を用いるバイオメトリクス認証にも言えることだが、画像の品質が悪いと認証が上手く働かない。鮮明な画像を用意するためにもハードウェアに掛かってくる資金はやはり大きなものになってくる。

・顔認証の問題点について
　対象者に協力を仰がなくても画像を用意できさえすればいいので、楽に認証を行うことが可能な顔を使用した認証だが、顔認証特有の問題として、プライバシーの問題が出てくる。

・プライバシーの問題について
　顔を用いた識別自体は、私たちが普段日常生活を送るに当たって普通に行っていることなので抵抗は少ないのだが、認証を行うと言うことは顔を記録しなければならないということである。大げさだが、プライバシーの侵害ではないかとする声も一部で上がっている。

・静脈認証の問題点について
　静脈認証独特の問題点というのは特にないのだが、やはり装置にコストが掛かる等、問題は存在している、また生体以外（大根）で作った人工指でセキュリティを突破できる装置も存在していたなど100％安全とはいえない。

・音声認証の問題点について
　音声を用いるため、声帯や声を出すための器官に損傷があれば勿論認証は不可能になってくる、さらに録音機材によって認証精度が左右されてしまうのも無視できない。精密な装置を作ろうとするとやはりコストのもんだいが発生する。

・DNA認証の問題点について
　人間の設計図ともいえるDNAを用いた個人識別は、非常に精度の高いものとして知られている。だが例に漏れずコストがかなり掛かる上にDNA認証特有の問題も抱えている。

・情報の抽出・分析に時間が掛かる
　最新の設備を用いてもサンプルを採取してからDNAを抽出しIDを生成するまでにどうして 3 時間以上の時間を要する。使用する試薬も高価なため安易に採用できないのも問題である。

・筆跡認証の問題点について
　バイオメトリクス認証の中ではコストは掛からず、安易に採用できる点が優秀だが、筆跡自体は模倣することがかのうで信頼性はあまり高くない。書いている過程の動作なら模倣されることは少ないが、圧力測定器などのハードウェアの追加が必要になってくるため、ここでもコストの問題が発生してしまう。

　いろいろ種類によって問題点は異なるが共通して主に以下のものが存在している。

・体の一部をキーとして使用している場合、怪我や病気などで損傷してしまうと認証が不可能になってしまう場合がある。

・おなじく体のパーツがキーの場合、対象者が成長期だった場合サイズ自体が変わってしまい、本人で有るにも関わらず、認証されなくなってしまう可能性がある。

・DNAなどの生涯不変な情報を使用している場合、一度複製などでセキュリティを破られると一生安全性を回復することが出来ない。更に、生涯不変であるがゆえにシステムから脱却する時にも無効化することはできない。

・指紋等の生体情報をプライバシーそして捉えた場合、システム管理者に情報を公開することになってしまう。

・全てのシステムに同じ情報を用いることになってしまうため、管理者が悪用すると、おなじ生体情報を用いたシステムは全て破られてしまう可能性がある。

・専用のハードウェアやソフトウェアに相応のコストが掛かってくる

　それぞれに弱点があるのは仕方がないことだが、やはりそのシステムの採用の可否を左右する一番の問題点はコストになってくるだろう。逆にコストの問題がないシステムであれば実験的にでも投入しやすいのではないだろうか。

第三章　提案手法

ここで前章で示した問題点を解決するために、キーボード入力を用いた個人認証を提案する。

・まず使用者本人の文章入力のデータ、キーボードを打つ際のキーを押してから離すまでの時間、更に離してから次のキーを押すまでの間隔の時間を採取する。

・それを自己組織化マップを用いて学習を行いそれをサンプルとして保存しておく。

・秘密裏にプログラムを走らせておき、常に使用者のデータを採取しサンプルと比較する。

・予め採取しておいた使用者のサンプルと比較を行い、採取したデータと予め採取しておいたサンプルとが一定以上で異なる場合、管理者に連絡する。

この方法は主に以下の利点が存在する。

・まずパスワードなどの決められた文字列などとは違い、人間の行動を用いて識別を行うものなので、他人に偽装されることが非常に少ない。

・判定に用いる要素のなかに細かい時間のデータ（今回の実験では小数点第6位まで）がかなりの数含まれることになる。”青天の霹靂”であればローマ字入力で”seitennohekireki”となりプログラムによりキーを押す時、離す時のデータを取ってくるため、31ものデータで要素が構成されることになり、まず他人と重なることはない。よって識別能力は良好だと思われる。

・この方法も文字列や暗号ではなく人間の要素を用いて認証をおこなっていくため分類的には生体認証になるのだが、体の一部を用いるほかの生体認証と違い、生体情報の登録や認証自体に専用のハードウェアを用いる必要がなく、入力情報を採取するプログラム等があれば可能になるため、他の認証方法よりコストを大幅に抑えることが出来る。

・従来の方法はそこに認証があることが意識できてしまうため、悪意のある第三者には警戒されてしまう。また、いくらコストを無視して頑丈なセキュリティを敷いていたとしても、一度破られてしまうとどんなに優れたものでも無力になってしまう。今回の手法は今までの”門番”の位置にあるセキュリティとは異なり、鍵が破られた後の”警備”としての使用になるため、門番より意識されにくい。よって警戒されにくいため結果としてセキュリティ能力の向上が見込める。

・他の生体認証のように登録時に特殊な行動を必要とせず、キーボードを打つという普段の行動でデータを記録できるため、使用者の精神的な負担が非常にかるい。

第四章　実験と考察

4.1 実験方法

今回の実験では、今回の提案手法の前提となるキーボード入力のデータと自己組織化マップを用いて個人の認証が可能かどうかの検証を複数のデータを用いて行っていく。

実験方法としてまず文章を入力するときに用いるキーを押すときと離すときの時間を採集するためのプログラムを作成する。今回は 1/1000000 秒までの時間をデータとして収集できるようにした、その収集したデータをプログラムによってファイルに出力できるようにしておく。

次にデータを収集するために被験者に決められた文章を入力してもらい時間データを収集する。今回は学校の演習室で用いることを想定したため同じ学科の人 9 人に協力してもらいデータを収集した。

まず普段打ちなれている文章とそうでない文章の本人確認の精度の確認を行うために二通りの文章を用意し入力を行ってもらった。打ちなれた文章として”私は学生です”という文章、普段使わないであろう文章の代表として”青天の霹靂”という文章をそれぞれローマ字で各自五回ずつ入力してもらう。その際プログラムを作動させておき入力時のデータを収集する。データの収集が完了したら今回使用するSOM_PACに入力するために整理し、マップを作成する。今回は初期値はランダムでマップの生成を行った。以下にSOM_PAC の簡単な紹介を記す。

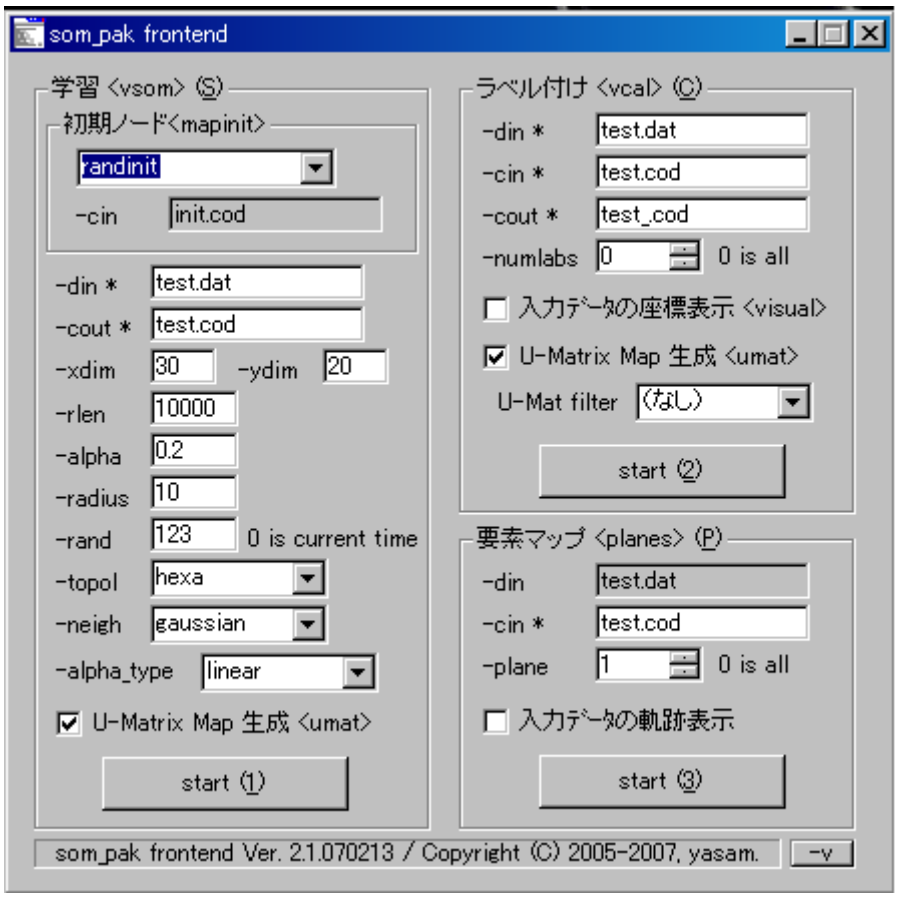

図5. SOM設定画面

・初期ノード　学習を開始する前のコードブックの状態をここで設定する。ノードの値をランダムで決定する randinit、入力データの主成分を計算し、その第一第二要素を基にノードの値を決定する lininit、-cin の部分に与えられたファイルを初期のコードブックとして読み込む cin の 3 種類が存在する。今回は randinit を使用した。

・-din 入力データのファイル名。
・-cout コードブックを保存するファイル名。
・-xdim-ydim 生成するマップの縦幅と横幅の値。
・-rlen ここで学習回数を設定する。今回は10000を回数として設定した。
・-alpha 学習率係数を0～1の範囲で設定する。
・-radius 近傍半径を此処で決定する。
・-rand SOM_PAK のプログラムで使用される乱数の種、今回は初期の値を使用する。
・-topol 近傍ノードとの位相関係、六角形格子か直角格子から選択する。
・-neigh 近傍関数の選択。
・-alpha_type 学習率係数の減少方法を選択する。

4.2 結果と考察

今回は結果として普段打ちなれた文章とそうでない文章のマップ、またそれぞれの要素を全体の時間で割り打つリズムのみを抽出したもの、そしてそれぞれを入力するときの押すときのみ、離すときのみの特徴のマップを結果として出力した。それぞれを見比べつつ考察していく。

図 7, 8 はそれぞれの文章のデータをそのまま使用して作成したマップ、図 9、10 は各々の要素を全体の時間で割ることによって時間的要素を取り去ったデータを使用したマップ、図 11～14 はデータ入手時に発生する”押してから離したとき”、”離してから押したとき”に発生するデータのみを抜き出してマップを作成したものになっている。

37

0.101095	0.122152	0.117094	0.102500	0.090579
0.096484	0.137508	0.117674	0.136502	0.091117
0.091147	0.118453	0.101852	0.143405	0.075373
0.085795	0.125102	0.112480	0.123089	0.080541
0.091147	0.118453	0.101852	0.143405	0.075373

図6. 入力データ一部抜粋

データは図6のようになっており、青枠の列が”押してから離すまで”のデータ、赤枠が”離してから次のキーを押すまで”のデータとなっている。入力データを全て利用した図 7,8 はこのように二種類のデータが交互に並ぶようになっている。図 11~14 はこのデータの中から赤枠のみ、もしくは青枠のみのデータを抜き出して作成したマップになる。マップ上に通し番号がある部分にそれぞれの要素が分布していることを表している。通し番号の前の数字は被験者の番号、後ろの番号が何回目の入力かを示している。また此のマップは基本的に近いほうが特徴が近いことを示している。ただし、色が黒に近ければ近いほどその部分は距離が開いていることを示している、コレを踏まえてそれぞれを見ていく。

4.2.1 全データによるマップ

”私は学生です”入力時のデータをそのまま用いて作成した図7を見ると、まずマップ左側にある被験者1、左上にある5と7は同じ被験者のデータが非常に整っておりかつ近いのでほぼ本人を識別することは可能になる。また左下に固まっている被験者6は一つ一つの要素自体は少し離れているものの他の被験者の結果からかなり離れた位置に分布されているので、認証は十分可能である。各々の要素が分散している被験者4、2、8、9も他との要素の重なりが少ないため認証自体は行えるものと思われる。認証を行う上では要素のまとまりよりも、違う被験者同士の要素が重ならないことが重要になってくるので、此のくらいの人数であれば認証は可能だと思われる。

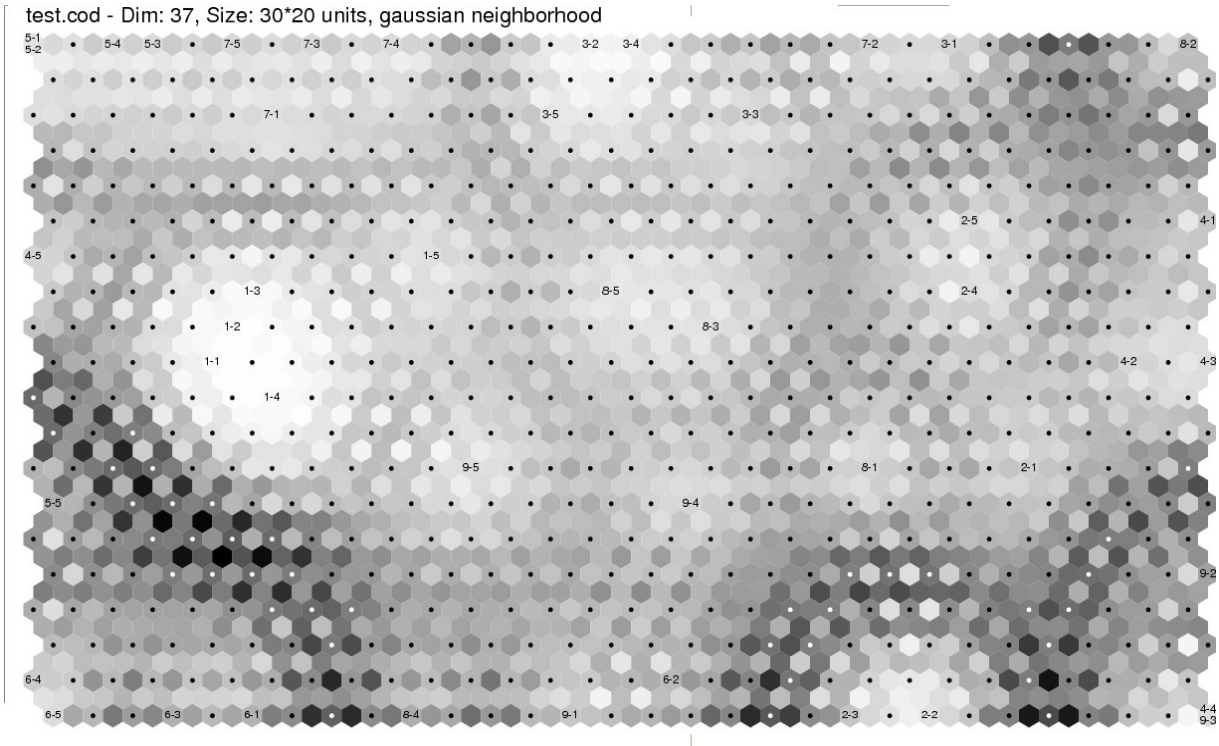

図7. ”私は学生です”入力マップ

次にこのマップと”青天の霹靂”の入力によって出力したマップ図8とを比較していく。

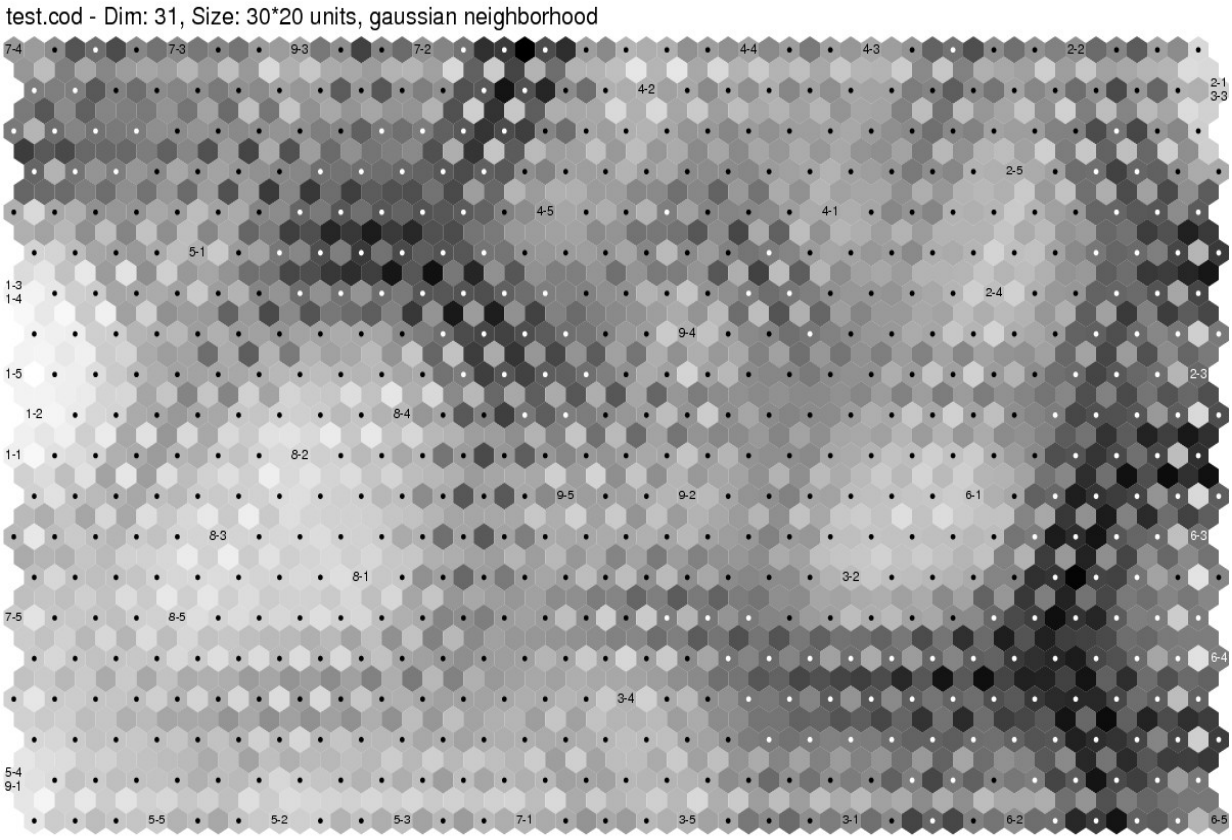

図8. ”青天の霹靂”入力マップ

こちらのマップも1と8は綺麗に分類されまとまっており、ほかの被験者の要素も判別が不能になる程重なっているところはないので、判別自体にはこちらも問題はない。図7のマップと見比べてすぐに分る違いとしては、図7のマップと比べて図8は色の濃い部分が非常に多い事である。黒い部分が多いということは距離がそれだけ離れているということなので図7より他人の要素と被りにくいことになる。

ここで立ち戻って”私は学生です”と”青天の霹靂”という題材を見直してみる。これらをローマ字表記に直すと”watasihagakuseidesu”と”seitennohekireki”となる(他にも入力の方法はあるが今回はこれに統一してもらった)。たしかに後者の文は日常生活では使うことがないので入力する機会はほぼないと思われるが、文を構成しているｱﾙﾌｧﾍﾞｯﾄに注目すると”私は学生です”と比較して、”青天の霹靂”のほうは同じｱﾙﾌｧﾍﾞｯﾄを使用している比率が大きい、更に打つキーの量も後者の方が短い。ここで考えられることは、普段よく目にするような文章ではなく文章自体が打ちやすいものであればより特徴が出て認証がしやすいのではないかということである。更に普段打ちなれるというのは環境によって人それぞれ違うので一概には特徴とは言えないが、文章自体が簡潔なもののほうが特徴が出るということになれば対象者の環境は関係なく満遍なくよい結果が出るのではないか。

4.2.2 時間要素を取り去ったマップ

次に全体の時間で各要素を割ることにより、打つ時間による特徴を消し入力のリズムのみによって生成したマップをみて検討していく。

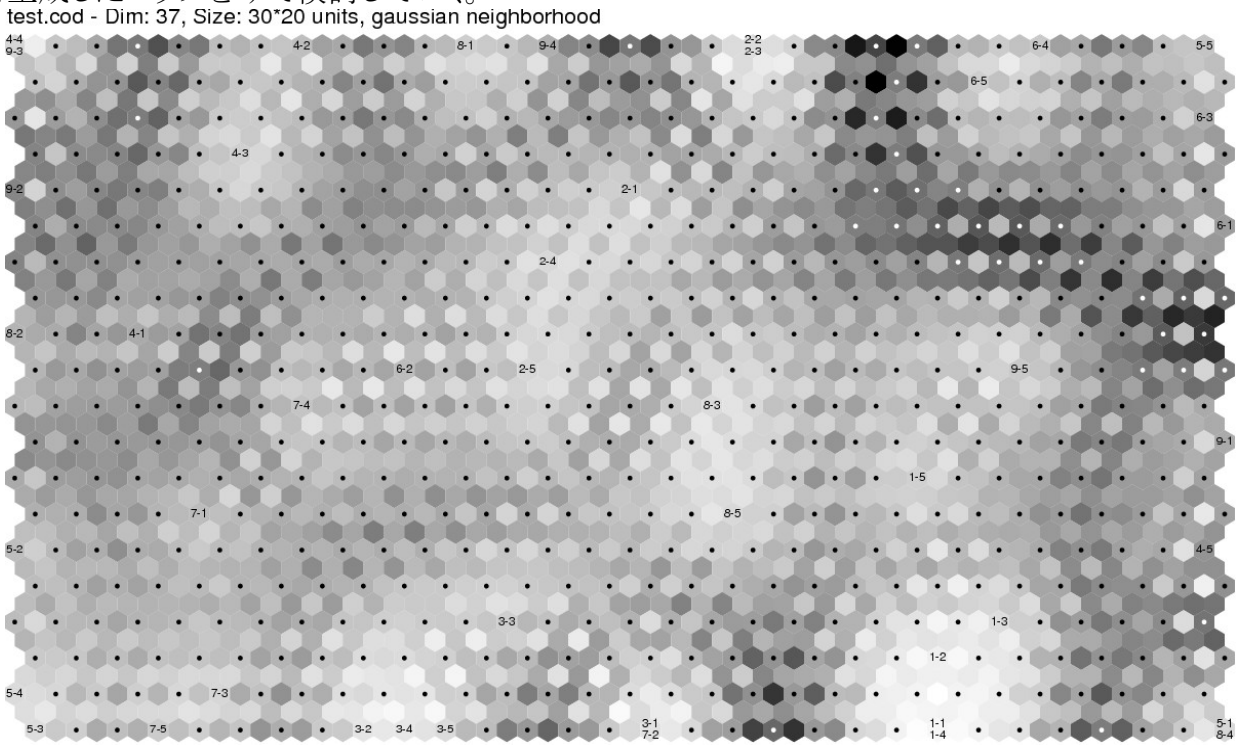

図9.”私は学生です”リズムマップ

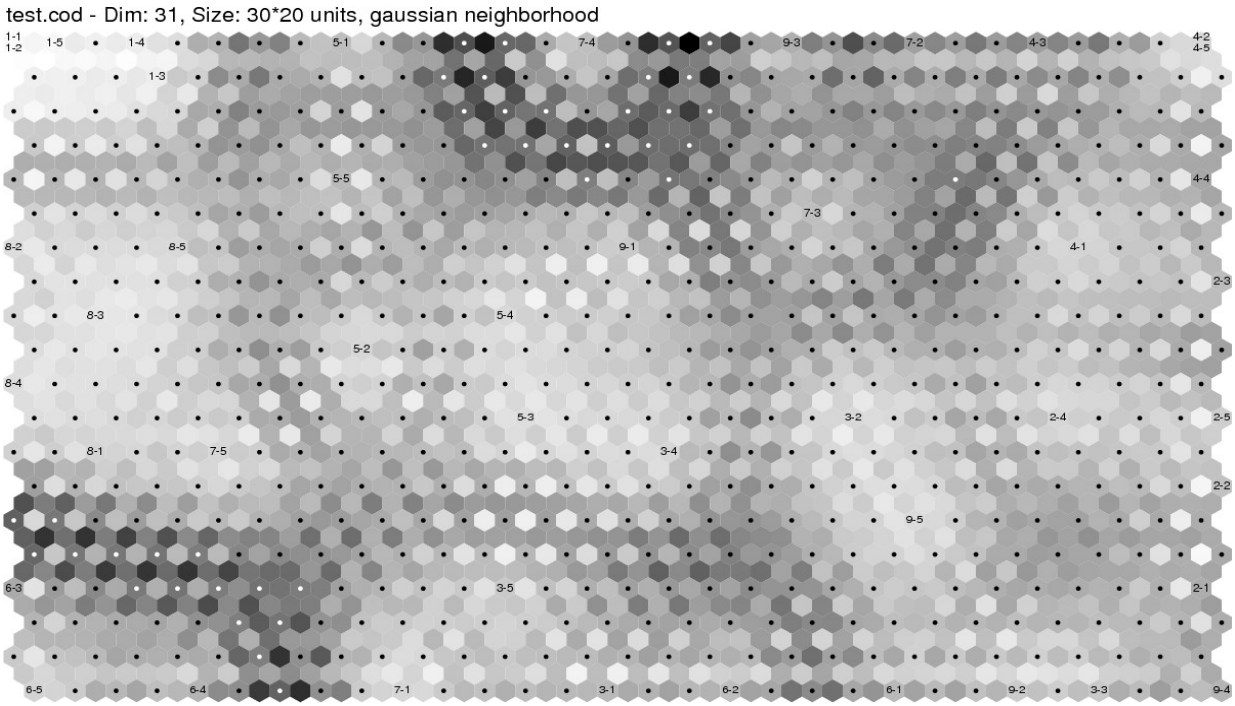

図10.”青天の霹靂”リズムマップ

各々の要素を全体の時間で割ることによって、データに存在する時間的要素を消去ることが出来る。図9の方が”私は学生です”を入力してもらったときのリズムのみを抽出したものになっている。図10の方が”青天の霹靂”となっている。時間要素を消すことによって各入力の要素の重なりは発生していないので、打つリズムだけでは認識できないということはない。ただし図10と図8を見比べると判るが、全体的に色が薄くなっている。ここで考えられるのは、リズムだけでも一応判別は可能になるが、時間要素が入ったものに比べて精度は弱くなってしまうということである。ただ逆にリズムにも人間ごとの特徴が出ることも確認できるので、重要な要素として用いることは十分可能である。

次に押してから離す時のみの要素、離してから押すときのみの要素で構成されたマップを見ていく。

4.2.3 ”押す”のみのデータ、または”離す”のみのデータによるマップ

図6のようになっているデータを、青枠で囲まれている”押してから離すまで”に発生する要素を取り出し生成した図11が、”私は学生です”を入力したときのキーを離すまでの間の要素のみのマップ、図12が赤枠の”離してから次のキーを押すまで”に発生する要素を用いて生成したマップになっている。図13が”青天の霹靂”のキーを離す間の要素のみのマップ、図14がその逆になっている。

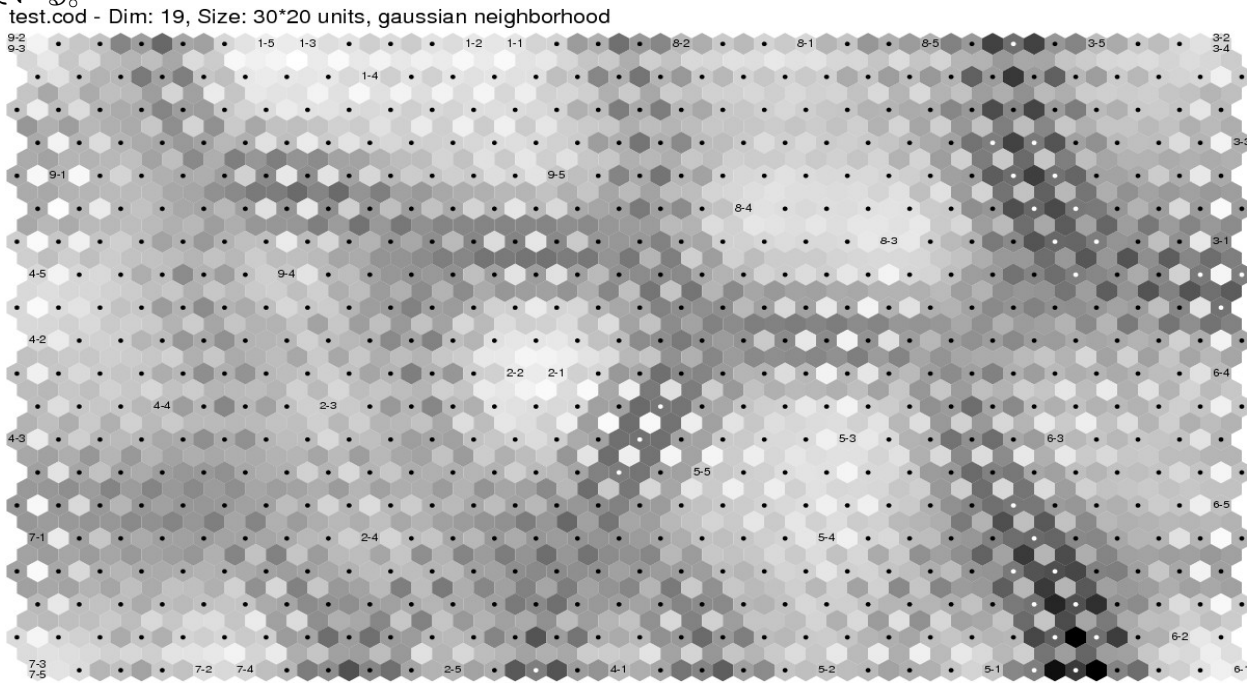

図11．”私は学生です”押した状態から離し終わるまでの時間によるマップ

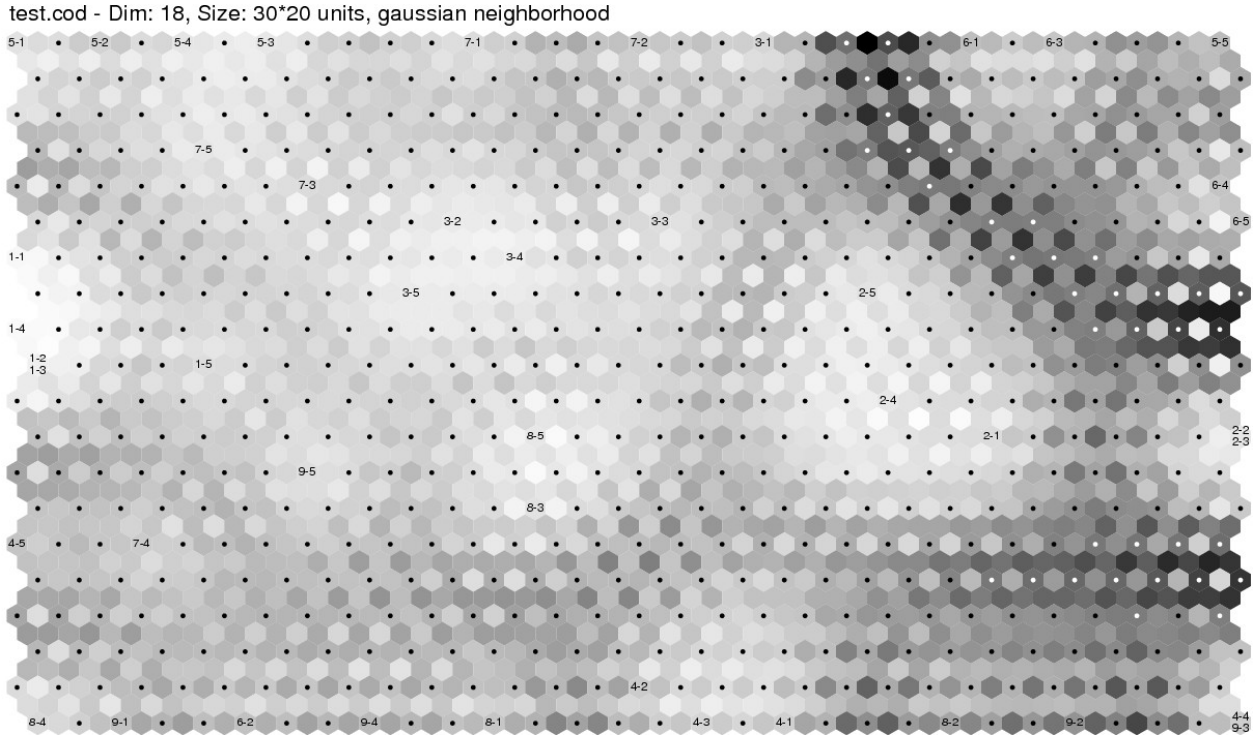

図12．”私は学生です”離した状態から押し終わるまでの時間によるマップ

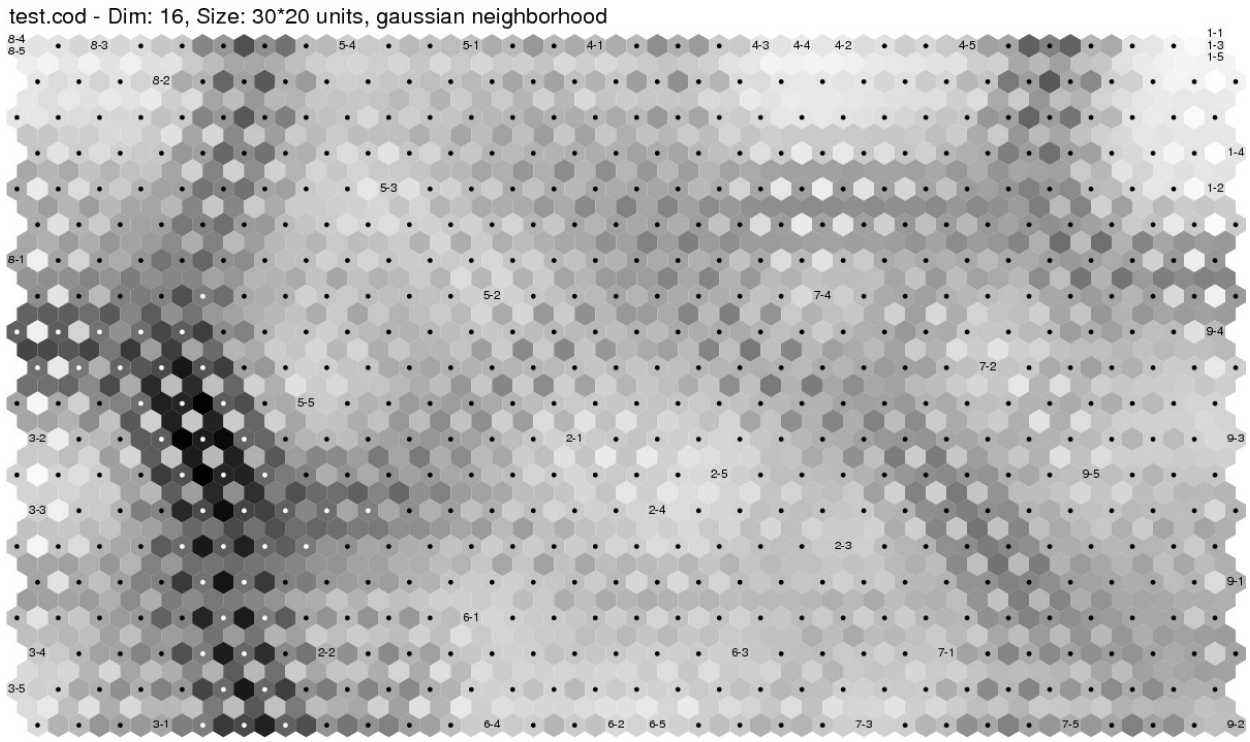

図13. ”青天の霹靂”押した状態から離し終わるまでの時間によるマップ

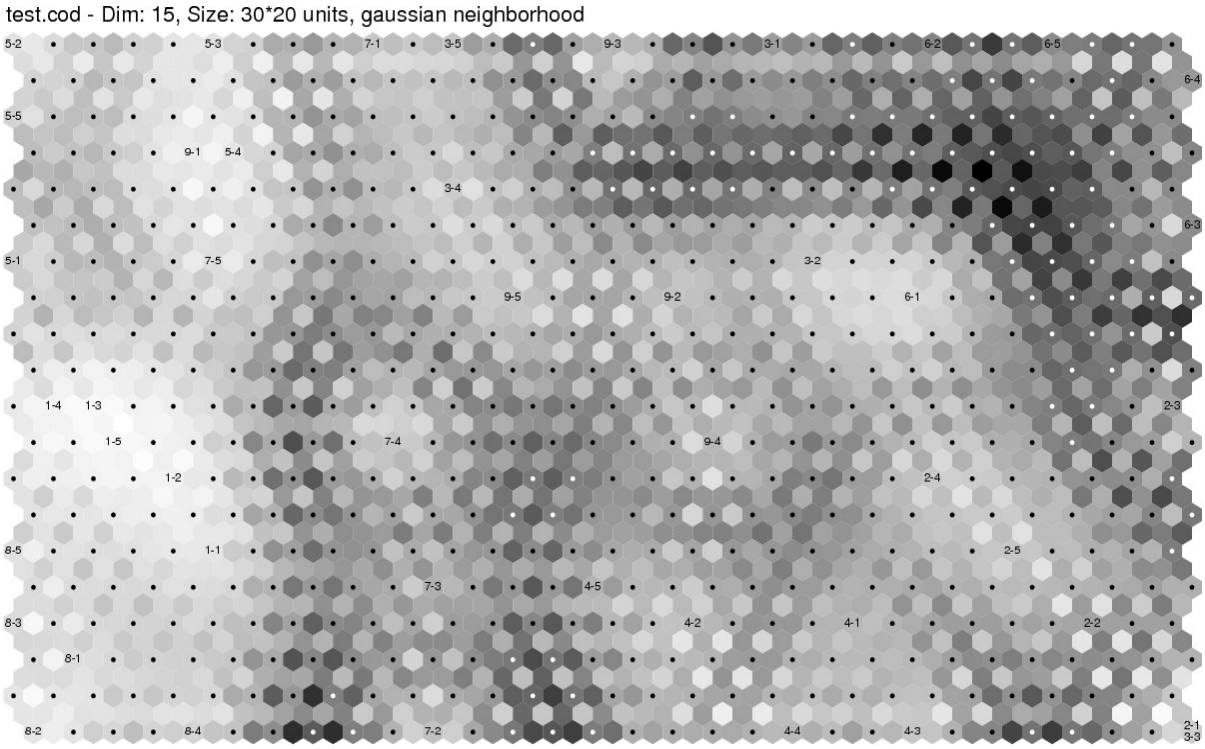

図14. ”青天の霹靂”離した状態から押し終わるまでの時間によるマップ

まず”私は学生です”の要素である図11と図12を見比べていく。まずどちらも一応特徴が出て判別は出来るのだが、離す動作の方が他人との距離が離れており、押す動作に比べてより特徴が出るものになっている。次に”青天の霹靂”の方の図13と図14を見比べていく。押したときの方が一見特徴が出てるようにも見えるが、左上や右下あたりに要素が被ってしまっている点が見受けられる。逆に図13のほうは全体の距離こそ近いものの、わりかし綺麗に分類できている。よってそれほど大きな差ではないにしても押す動作よりも離す動作の方がより個人の個性がでやすいと考えられる。

4.2.4 考察

以上より慣れや環境ではなく、打ちやすい簡潔な文のほうが各々の特徴が出やすいことが分った。また含まれている要素は多ければ多いほど良いことが判った。よって今回では文が簡潔であり、かつ”押す要素”、”離す要素”、”リズム要素”に加え”時間的要素”も含んでいる図7が一番個人を識別するのに向いているマップということになる。

4.3 まとめ

今回の実験で分ったことをまとめてみると以下の事が言える。

・特徴は普段用いられる単語で構成されている文章より、ローマ字入力で見たときに同じキーが使われていたり、短いもののほうがより特徴が出やすいことが図7、8より確認できた。文章自体が打ちやすいもののほうが特徴が出やすいと考えることが出来る。

・入力要素から時間的要素を取り払っても人を識別することは今回は可能であったが、やはり単体では弱い。時間的要素やそれ以外にも複合できるものがあれば複数組み合わせて用いることが望ましい。ただしコレ自体も重大な識別要素として十分運営可能である。

・押す動作よりも離す動作の方が特徴が出やすいことが分った。ただどちらも複合して使う場合の要素としては十分機能すると思われる。

今回の実験の範疇では人の判別は可能であるといえる。少人数で可能だったということはさらに様々な要素を複合させ洗練させることができれば最終的に十分実用に耐えうるものができるのではないか。

今回は時間要素やリズム要素を主に考え、個人個人で特徴が出ることは分ったが、最終的に強固なものにするには更に複数の要素を組み合わせる必要が出てくる。動作からでる要素ではなくsi や shi などの、同じローマ字でもｱﾙﾌｧﾍﾞｯﾄによる癖の違いや、かなり難解だが誤字なども個人の判別材料に出来ると考えている。

今回の実験では二パターンの文を入力してもらう事で人を判別できるかどうか、どのような要素が識別材料として使用可能か検討を行った。今後の発展としては上に挙げたように更なる識別要素の発見や入力文のパターンを増やし被験者の人数や年齢層などを大きくすることでより実用的な記録を得ることがある。

謝辞

本研究を行うにあたり、様々な助言、指導等をして下さった三好教授に心より御礼申し上げます。また様々なコメントを頂きました研究室諸氏に御礼申し上げます。

参考文献

1)BIOMETRICS
http://www.jaisa.jp/action/group/bio/shoukai.html

2)【調査】自己組織化マップ（SOM）
http://mikilab.doshisha.ac.jp/dia/research/report/2003/0604/003/report20030604003.html

3)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”、(2008)

4)T.ｺﾎｰﾈﾝ:”自己組織化マップ（SELF-ORGANIZINGMAPS）”,(1996)

5)村上　敦、堂薗　浩
自己組織化マップを用いたタイミング解析

付録

パスワード認証について

今現在もっとも用いられている認証方法で、通常はユーザーIDに用いる。あらかじめ登録されているそのユーザーIDのパスワードと、操作者によって入力されたパスワードが一致していることによって、その操作者がIDの使用者本人であると認証を行う方法である。

生体認証について

生体認証とは、我々人間の持つ身体的特徴や行動的特徴の情報を用いて行う個人認証技術であり、通常テンプレートとよばれる情報を事前に採取及び登録を行い、認証時にセンサーで取得した情報と比較することで認証を行っていく。上記で述べたパスワード認証とは違い、忘却や紛失によって本人でも認証できなくなったり、漏洩や盗難などの不慮の事態によって他人が認証されてしまうような危険性が低いと考えられている。よって、認証自体は手軽なものが多い事と、あるいは本人以外の第三者が認証されるリスクが低いことから集合住宅の入り口や入国手続きなどの認証手段に採用されている。

以下で現在使用されている主な認証素材を紹介する

・指紋　人や指ごとに指の紋様である指紋は全て異なり、薬品等で指先が焼けるなどの事故がない限り一生を終えるまで変わることはない。

照合方法としては、比較を行う資料を用意し、それぞれの内まず遺留指紋等の対象となる指紋中の線が時計回りに見て線の開始点と、線が途切れている終始点、線が分かれている分岐点、線が交わっている接合点、これら4つを特徴点という。これらが鮮明に確認できる部位を 8 点以上抽出する。次に対象者の指紋から同じ部位の特徴点を抽出する。抽出後、双方の特徴点の位置と方向を比較して合致する点の確認を行う。このとき、特徴点と特徴点の間を横切る形で存在する隆線の数（これをリレーションと呼ぶ）を照合に使用することで、更に精度の高い鑑定を行うことが可能になる。

通常の判定基準とは違い、刑事事件で用いるために設けられている警視庁の判断基準では、原則として特徴点 12 点以上の合致が必要になってくる。しかし、防犯ビデオの映像など併用できる証拠が存在する場合には12点以下でも証拠能力を持つことも可能になる。

指紋には主に以下のものが存在する

・渦状紋　円形または渦巻き状の線で構成されている指紋。日本人の約半数が渦状紋の指紋をもつとされている。

・蹄状紋　右もしくは左のどちらかの方向に蹄の形をして線が流れている指紋。日本人の約 4 割がこの指紋をもつといわれる。

・弓状紋　弓なりになった線のみで構成されている指紋。片方よりもう一方に線がながれ、線が逆方向に流れることがない。日本人には非常に少ない。

・変体紋　上記のどれにも属していない指紋。上下に流れる線で形成されている物や、点や短い線だけで形成されているもの等非常に稀な指紋。また上記に記した薬品などで指先が焼け、指紋

がなくなった状態もここに分類される。

・網膜　網膜は、眼球の構成要素の内の一つ。眼球の後ろ側の内壁を覆う薄い膜状の組織であり、神経細胞が規則的に並ぶ構造をしている。視覚的な映像を電気信号に変換する働きを持ち、視神経を通して脳中枢へと電気信号を伝達する。

認証を行う素材として網膜による識別は非常に正確に行うことが出来る。これは、網膜上の血管パターンが識別手段として非常に優れた独自性と安定性を持つことが背景にある。内耳の骨もそうだが、網膜は脳の感覚プロセス機能の必要性から安定することが必然になってくるので、人間の一生の中で変化することはなく、例え同一人物でも左右の眼で網膜の形状は異なってくる。また、人間の目という機関は高い反射的特徴を有しているため、物自体に接触しなくても簡単に測定することが出来るうえ（無論測定を行うためのハードウェアなどの準備は必要）、網膜のパターンは外面的な特徴とは異なり、目の中に保持されているので不安定要素も低く、外部的にも晒されていないので、人間が生まれてくる上で持って生まれた天然のサインとも言える

網膜認証には網膜識別機を用いる、光源としてパルス変調された直流電流を用いた小さめの白熱タングステンランプを用いる。この光源より、眼に見えるイメージと網膜の血管のパターンを取り込むための近赤外線を発生させる。この光で眼の瞳を中心にして回転する近赤外線を円柱状に作成する。この弱い光は虹彩を通り、各個人によって異なる網膜の血管パターンにより反射され、また吸収される。同一の発光経路に戻ってきた光はビームスプリッターという受け皿に当たりそこから検出装置に向かう。受け取ったアナログ信号を A/D コンバータに送りデジタル信号に変換する。このようにして個人のデータの登録を行い個人認証を行っていく。

・虹彩　虹彩とは黒目の内側で、瞳孔より外側のドーナツ状の部分のことを言い、瞳孔の開き具合を調節する筋肉から構成されている。つまるところ虹彩は外界から眼球内部へ入射される光の量を調節する部分であり、カメラの絞りに相当する。

虹彩がなぜ認証に向いているかというと以下の理由がある。人間の目はおよそ妊娠6ヶ月までに形成され、その時点で瞳の部分に孔が開き、その開口部、すなわち瞳孔から外側に向かってカオス状の皺が発生することが研究などを通して知られている。この皺の成長は生後二ヶ月ほどで止まり、それ以降変化することはない。この皺の形状は遺伝的影響度が少ないことが知られている。そのため、虹彩の模様は指紋などと同様にその人固有のパターンとなり、同一人物の左右の眼でも異なり、更に一卵性双生児でも異なったパターンになる。何かしらの病に苛まれたとしても、虹彩自体が眼の表面の存在することら、眼球内部の疾病などの影響を受けることは殆どなく、眼の充血などにも影響を受けることはない。たとえ眼が不自由だったとしても、眼の不自由な方の多くは視神経の障害であり、殆どの場合は虹彩には何の影響もない。

次にどのようにして認証を行うかを紹介する。虹彩での認識は上記に述べたような虹彩の特徴を利用して、デジタルカメラで撮影した虹彩のパターン画像をデータ化し、予め登録してある本人の虹彩データと比較照合することにより、個人を特定していく。個人認証に虹彩を用いることの技術面での利点は以下のようなものがある。

① 認証精度が非常に優れている。

② 非接触での認識が可能になる。

③ 対象者の目を持ってくるなどの非常に極端な事を行わない限り、偽証が非常に困難。

④ 上記でも述べたが、虹彩自体が非常に安定しており生涯において変化しないため、再登録が基本的に不要。

良好な虹彩パターンの画像が得られたあとは画像に処理を施していく。

・局部化処置
得られた眼の画像から虹彩部分を切り出す。これは、虹彩の外側の境界と虹彩内側の境界とを、明るさの違いなどを用いて検出することにより行われる。

・特徴抽出
まずは分析帯の決定を行う。虹彩の外側境界から内側境界までを 8 層に分割した分析帯を決定する。この時、目蓋やまつ毛等により虹彩の一部が隠れてしまい誤った虹彩データになってしまうことを防ぐため、特徴抽出を用いて使用する範囲を制限する。周囲の明るさ等によって瞳孔の大きさが変化し、虹彩部分の形状がかわり虹彩データが変化することもありえるのではないかと思うが、虹彩は瞳孔の大きさを調節するための筋肉の模様に過ぎないため、その大きさ自体が幾ら変化しようとも、模様が相対的に変化するだけで取得できる虹彩データ自体になんの代わりもない。

次に分析を行う。これはまず、虹彩の中心を原点とした極座標を考える。特殊なフィルターにより各分析帯の虹彩の濃淡の変化を抽出する。濃淡の変化をデジタルコード化することにより 256 バイトのアイリスデータが生成される。

・マッチング
このコード化されたデータを入力された虹彩のデータとし、予め登録されている本人の虹彩データとマッチングを行うことにより、ハミング距離値を算出する。

・本人判定
正規化された距離値が所定の値より小さいならば本人と判断し、大きいならば他人と判定する。この判定のための閾値は、大量の虹彩データを収集し統計的に処理することにより決定されている。この事を図3に示す。

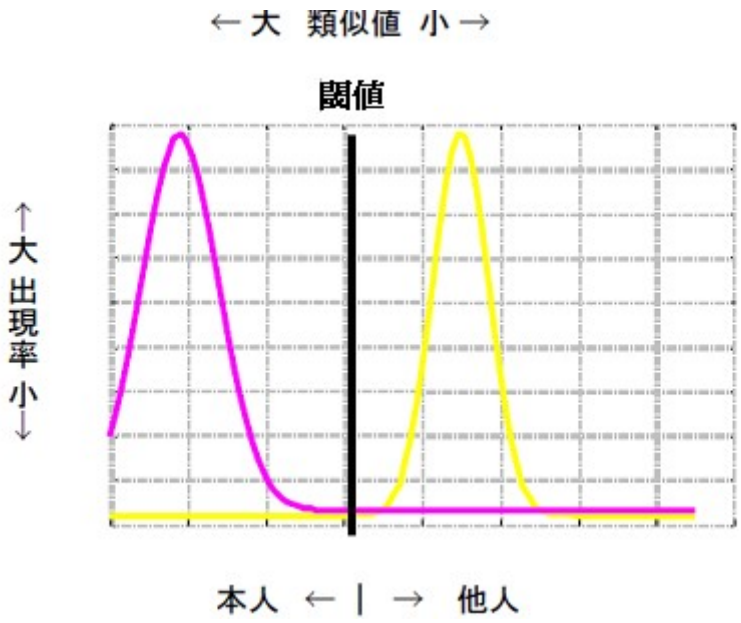

図. 閾値による本人判定の分岐

閾値より左側の山は本人同士の虹彩パターンで照合した結果の分布、右側の山は他人同士の虹彩パターンで照合をした結果の分布を示したものになっている。ハミング距離は排他的論理和の計算になっているため、他人同士が全くバラツキを持っていれば 0.5 を中心として分布する。
本人同士のハミング距離は全く同じであれば0になるが、データ取得時の状況などで全く同じというのはなかなかおこらないので、0.1 程度を中心に分布する。これらの分布は 2 項分布に合致することが確認されており、通過エラーや阻止エラーとも 120 万分の 1 の精度が得られている。ちなみに認証時に眼鏡等をつけていたとしても、虹彩認識では赤外線を用いているため角膜と反射率が異なる、これにより処理段階で排除可能である。

・顔　私たちは通常人と出会ったとき、視覚により相手のかをを捕らえ誰であるかを認識している。これと同じように機械にもこれらを簡易的に認識できるようにしたものが顔認証である。顔を用いて認証を行うことの利点を以下に示す。

①　顔を見て誰かを判断すること自体は我々が普段から行っている自然な認識方法である。よって他の認証方法と比べて心理的な抵抗が少なく親しみやすい。

②　距離が多少離れていても認識することが可能。

③　ユーザーが何も身に着けず、かつ自主的に意識して認識されるように行動しなくても、自然に歩いているだけで認証がかのうなのは顔だけである。

④　顔画像や映像で記録できる、または記録されているかもしれないということから、不正行為に対する心理的な抑止効果も期待できる

⑤　同じカメラを用いて、顔認証以外の認証（視線認証など）を兼用して行うことが可能。

以下に実用化されている顔認証の方法を紹介する。

・Gabor Wavelet 変換＋グラフ・マッチング
　顔器官上の特徴点間の弾性的な位置関係を持つ顔グラフと、その特徴点周辺における Gabor フィルタにおける濃淡特性の周期性と方向性を特徴量としてにんしきする。顔画像上に多くの特徴点を配し、詳細に位置決めを行い特徴量を比較しているため、位置がずれることによっておきる誤差や、表情変化、顔向き変化に強いという特徴をもっている。また、斜めからも高速に認証することが可能であるため、他の手法では難しいとされていた歩行中の人の顔を認証することを実現している。

・主成分分析による固有顔
　まず多数の顔画像パターンの集合に対して主成分分析を行い、固有ベクトルを決定します。次に、入力顔画像を固有ベクトルの空間に射影し、登録された顔の射影との類似度により確認を行う方法である。

・Local Feature Analysis
　固有顔の考え方を基本的には踏襲しているが、顔全体のパターンではなく、鼻、眉、目、口、頬、などのかおの器官の局所的なパターンに対して主成分分析を行うことによって表情や顔向きなどに比較的安定した認識を実現している。

・動画像ベースによる制約的相互部分空間法
　文字認識で用いられている部分的空間法をベースとしているが、入力を静止画像でなく、動画像を用いることにより複数の顔パターンの分布の類似度に基づいて識別することが出来る。また制約的部分空間に射影することにより、照明への影響を受けにくい効果がある。

・ニューラルネットワーク
　ニューラルネットワークを用いて顔検出、顔器官特徴点検出、認証を行っていく。目・鼻の側面口・眉・頬など濃淡コントラストのある領域を顔特徴として抽出し、数値化及び正規化を行い、ニューラルネットワークを用いて学習を行っていく。

・静脈　静脈とは、毛細血管から発生した静脈血を心臓に送るために使用される血管である。毛細血管の吻合により細静脈に至り、静脈になる。ただし、肺静脈には他の静脈とは機能が異なり動脈血が流れている。全身の静脈は肺静脈系と大静脈系に二分されている。大静脈系は腸などからの血液を肝臓に運ぶ門脈系を含む。静脈は皮膚からの位置によっていくつかに分類することが出来る。筋膜よりも皮膚よりを走行する皮静脈、筋膜下を走っている深静脈、この二つの静脈をつないでいる貫通静脈とある。

　静脈の認証に用いるのは主に手の甲や指に走っている皮静脈を用いる。理由としては、皮静脈の位置は個人個人によって差があり、更に年月がたっても形状が変化することがないからである。

　静脈の認証の方法も様々あるが、そのうちの指の静脈を用いた認証の方法を簡単に紹介する。

①　まず指の第一関節と第二関節の間付近に赤外線LEDを使用して近赤外線をあて、一定以上の太さ以上の静脈を浮き上がらせて記録する。

② 採取した画像データに処理を施しノイズを除去してパターン画像を生成する。

③ 生成したパターン画像をハードウェアに登録しておき、認証時に読み込まれた静脈のパターンと照らし合わせて認証を行う。

赤外線LEDの近赤外線の光を当てることで静脈の形が読み取れるのかというと、血液中のヘモグロビンが近赤外線を吸収するために静脈が陰になって浮き出るからである。

・音声 指紋認証などの場合はサンプルや画像などを予め採取しなければならないため、認証を行うのに心理的に抵抗を感じる人が多い。しかし、音声を用いる音声認証ではこのような心理的な抵抗は非常に少ない。また、電話などを用いれば遠隔地からでも認証を行うことが可能になる。さらに、他の生体認証に比べ標準的なパーソナルコンピュータに搭載されているハードウェアがあれば音声認識が可能であり、音声認識のためだけの特別なハードウェアを予め準備しておく必要はない。

音声認証には、サウンドスペクトログラム、あるいはこれと同じレベルの価値を持つ音声特徴を用いる。サウンドスペクトログラムの例を図4に示す。

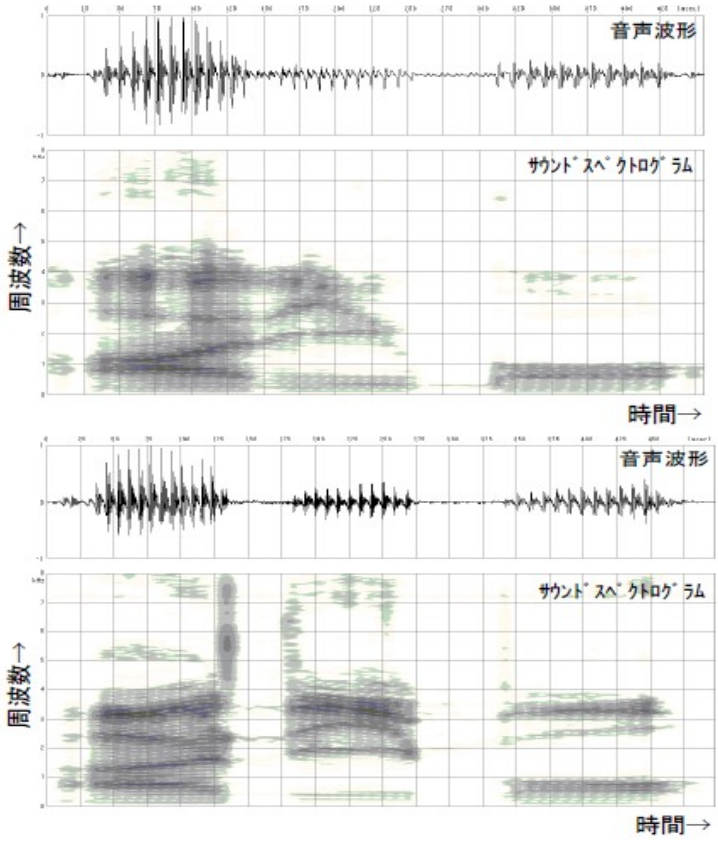

図. サウンドスペクトログラムの例

このサウンドスペクトログラムは上下でそれぞれ違う人物のものとなっており、横軸が時間、縦軸は周波数を示している。サウンドスペクトログラムの色の濃い部分は、そこに音声による信号が集中していることを示している。逆に色の薄い部分は音声信号の成分がそこには存在していないことを示している。

サウンドスペクトログラムのパターンは個人によって異なってくる。これは、サウンドスペクトログラムが個人ごとの発声器官の形や大きさの違い、さらには調音の違いを明確に表すことが可能になっているためだ。調音とは、母音や子音を発声する場合に発声器官内での狭くなっている位置や、その狭くなっている位置の時間的な変化のパターンのことを言う。調音はその個人の体格や、方言などのその個人個人が今まで育ってきた言語環境に大きく影響を受けている。音声認証ではこういった個人個人の調音の違い、すなわちサウンドスペクトログラムの違いを利用して認証を行っている。

音声認識には主に3つの方式が存在する、以下で簡単に紹介を行う。

・テキスト従属方式

テキスト従属方式は、発話内容があらかじめ決められている方式になっている。パスワード方式、キーワード方式、またはキーフレーズ方式と呼ばれていることもある。一般には Dynamic Programming 法（以下 DP 法）や Hidden Marcov Model 法（以下MMD法）と呼ばれる手法を用いた単語音声認識の技術が用いられている。DP法はHMM法に比べて実装が簡単になっている。HMM法は一般的にDP法に比べて精度が高いが、話者のモデル作成に多くの発生が必要で、実際の場面では利用できないことがある。そのため利用の最初期では不特定話者認識による単語認識により、話者がそのキーフレーズを知っているかだけをチェックし、数回使ううちにその単語の発声が複数回得られるためその発声によりHMM法の話者モデルを作成するという発声内容照合法が提案されている。テキスト従属方式では発声内容をしっているか、かつその音声がその話者の声質であるかの二十チェックが行われることになる。氏名や電話番号など比較的短い音声で認証が可能になるが、詐称者にテキスト自体が知られてしまうと話者の声質だけのチェックに変わってしまいセキュリティの強度が著しく低下してしまう。

・テキスト独立方式

テキスト独立方式は、発話内容を特に限定しない音声を用いる方式になっている。フリーワード方式、自由発話方式などと呼ばれることもある。Vector Quantization 法（以下VQ法）、エルゴーディックHMM法、Gausian Mixture Model 法（以下GMM法）などが用いられている。VQ方式はGMM方式よりも実装は簡単になっているが、一般的にエルゴーディックHMM法やGMM方式よりも認証制度は劣っている。エルゴーディックHMM法はGMM法よりも多くの登録発声が必要になってくるので実際はGMM法が使われることが多くなっている。テキスト独立方式では話者の声質だけがチェックされるために、十分な認証制度を得るためには比較的長い音声が必要になってくる。最低でも話者モデルの登録に20秒以上、称号には 5 秒以上の音声が必要になる。長い音声を得るのが難しいアプリケーションでの適用には向いていないが、音声対話技術を用いた電子商取引システムなどでは全体で十分な音声が得られる場合があり適応可能になっている。

・テキスト指定方式
テキスト指定方式は、システムが発話内容を指定する方式になっている。自由なテキストを指定する方式と、あらかじめ決められたテキストの番号を指定する方式がある。テープレコーダーなどに録音された音声による詐称を防ぐのに有効になっており、システムの信頼性をあげることができる。自由なテキストを指定する方式は、話者認識技術と不特定話者音声認識技術を組み合わせることで可能となっている。

・DNA　人間のDNAは約30億個の塩基配列から成り、人体の設計図とも言われている。人間一人一人が少しずつ異なっているように、このDNAの塩基配列も人によって異なる部分があり、その情報を上手く抽出して扱うことが出来れば他の生体認証の題材と同じように個人認証に用いることが可能になる。塩基配列とは、アミン、グアニン、シトシン、チミンの４種類の塩基の文字列になっている。DNAの塩基配列は二重化されて細胞核に畳み込まれている。人体は50～60兆の細胞で出来ているが、どの細胞を取り出してもDNAの塩基配列はどれも同じになっており、終生変わることはないとされている。またDNAは無機質で安定した水溶性の物質なので、簡単にインクなどに溶かしこむことが可能になっている。DNAの情報分類を以下の図5に示す。

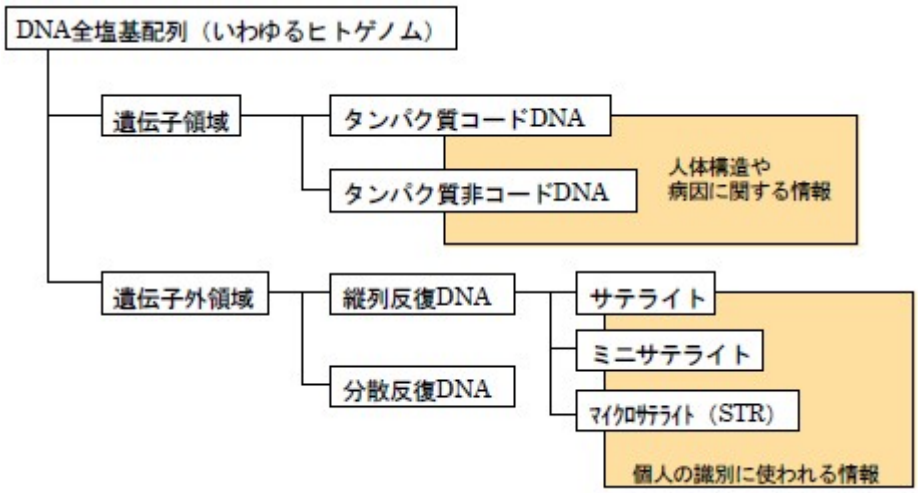

図. DNA全塩基配列の分類

以下にDNAを用いた認証の特徴を簡単に紹介する

・識別精度の高さ
指紋などのようにDNA以外のアナログ情報に基づくバイオメトリクス認証では、50 万～100 万分の1の認証制度となっているが、DNA情報を用いた場合、現状の抽出技術による同値確率が10の21乗程度にすることが可能で、識別精度が非常に高い。

・照合アルゴリズムが不要
DNA情報からIDを生成するアルゴリズムを国際的に定義すればIDは一意に定まってくるので、照合はデジタル情報同士の直接的な比較によって行えばいい。アナログ情報のように特徴抽出

点やパターンマッチングによる難しい照合アルゴリズムは特に必要としていないところが他の手法に比べて大きい。

・生体情報の抽出・分析に時間と費用が大いに掛かる
　口腔を綿棒などで軽く擦り、粘膜の細胞からDNAを抽出し、DNA-ID を生成するのに最新の設備を用いても 3 時間以上を必要とする。またIDとなる個人情報を生成するのに高価な試薬を必要とするので、DNAを用いたバイオメトリクス認証については特別な用途に限定されているのが現状である。

次に実際に用いられているDNA認証マークについて簡単に紹介を行う。

・DNA認証マーク
　ブランド商品やグッズの真贋識別に用いられ実用化されているのがDNA認証マークである。この認証マークの印刷インクには、当事者のIDとなるDNAの一部が溶解されており、DNA入りのインキを使った特殊印刷が施されている。当事者のDNAはかなり特殊な物であり、細胞を盗まれない限り認証マークの複製は非常に困難である。真贋性の判定はマークのインキに溶解されているDNA断片を解析に、当初のIDが生成できるかどうかで判定される。なお、補助的な確認手段として、インキに特別な波長に対して発光する蛍光剤を混入し、手持ちの赤外線レーザスキャナーを使って正規の認証マークであることを見分ける。

・筆跡
　筆跡とはワードプロセッサなどを介さずに、筆やペンなどの筆記用具を用いて人の手によって直接掛かれた文字やその書き方の癖を利用して認証を行う方法である。なぜ筆跡に識別能力があるのかを簡単に説明する。

・筆跡のもつ個性
　文字は人が相互に意思を伝達するために、統一的に定めた記号になっている。この文字をパーソナルコンピュータなどを使用せずに手書きで記載する際には、書き始めから終わるまでに動きが確実に発生する。この動きに記載者ごとに所謂癖が発生する、これが他人には見ることが出来ない筆跡上の個性というものであり認証に利用できる。

・筆跡の恒常性
　個人個人の筆跡は常に何かしらの個性を持っているのだが、残念ながら完全に不変不動というものではない。人間のアナログな動きがダイレクトに反映されてしまう部分なので、記載時の客観的な環境や記載者の心理低条件によって少ないながらも変化が起こってしまうことがある。しかし一個人の筆跡としてどの程度の変化が起こるのかを検査した場合、よほどのことがない限り許容の範囲内にあり認証上は無視できるものになっている。

次に筆跡において個人認証を行う場合にどのような特徴が使用されるのかを間単に紹介する。

・筆順
　文字を書く時に筆を入れる順序自体は、文部科学省によって所謂書き順として順序自体は定められている。しかし、実際には万人が必ずしも書き順にしたがって文字を書いているわけではない。

ただ、書き順に従って記載する人のほうが多くなっているので、これも個人を識別するための大切な要素の一つになってくる。

・字画の構成
　個々の文字における字画線の交差する位置や角度や配置など、組み合わせられた字画線間に見ることが出来る関係性によって個人の癖の特徴を見出すことが可能になっている。

・字画形態
　個々の文字における画線の長辺、歪曲度、直線性や断続の状態、点画の形態などに見られる筆跡の特徴には、筆者個人の特徴を明確に確認することが可能になっている。

・筆勢
　文字を書く場合に見られる書く勢い、速さ、力加減、滑らかさなどの筆記用具の使用加減のことを筆勢という。外部のハードウェアを用いて蓄積され、実験的データを基に比較されそこから評価を行っていく。

・筆圧
　文字を書く際に筆記用具で記載面に対して加えられる圧力の事。 重にハードウェアを用いてコンピュータによって解析される。

・誤字や誤用
　といっても単純なミスのことではない。誤用や誤字に長い間気がつかず、正しくない字や字画を癖として覚えこんでしまった場合のものである。大体の場合は記載者独自のものとなってくるので、識別上かなり強力な材料になりうる。

・個人内変動
　筆跡は書く人それぞれに個人差が存在するために筆者識別の題材となりうるが、同一筆者でも変化は小さいながら変動が生じてしまう。しかしこの同一人物でおこる変動自体も筆者によってそれぞれ生じる位置や状態が異なってくる。個人変動はどこで発生するのか自体は固定できないので一定の位置で判別を行うことは出来ないが、これも十分に識別材料になりえてくる。

ソースコード

```
#include<stdio.h>
#include<stdlib.h>
#include<windows.h>
#include<time.h>


class TimeCounter
{
public:
	TimeCounter():flg(false)
	{
		QueryPerformanceFrequency(&freq_);
	}

	void begin()
	{
		QueryPerformanceCounter(&before_);
      flg=true;
	}

	double end()
	{
      if(!flg)
				return 0;

		LARGE_INTEGER after;
		QueryPerformanceCounter(&after);

		return (double)( after.QuadPart -
before_.QuadPart )/freq_.QuadPart;
	}

private:
	LARGE_INTEGER freq_, before_;
   bool flg;


};


int main(void){

	char filename[]="data.txt";
   FILE *fp;
	char i;
	int flag;
	flag=0;
   TimeCounter t;

	if((fp=fopen(filename,"w"))==NULL){
		printf("色々と残念なので終了します/n");
		exit(1);
	}

	while(1){
		for(i='0';i<='Z';i=i+1){
if(GetAsyncKeyState(i) & 0x8000){



		if(flag==0){
double result_time=t.end();
printf("%f\n",t.end());
			fprintf(fp,"%f\n",t.end());
t.begin();
			fprintf(fp,"%c\n",i);
			flag=i;
			break;


}
			 }
else if(flag==i){
		printf("%c\n",i);
			fprintf(fp,"%c\n",i);
			flag=0;
double result_time=t.end();
printf("%f\n",t.end());
			fprintf(fp,"%f\n",t.end());
t.begin();
			break;
		}

		}
if(GetAsyncKeyState(VK_ESCAPE) & 0x8000){
		break;
	}
	}

	return 0;
}
```