平成 13 年度

学士学位論文

# 筆圧による個人認証システムにおける登録・認証処理の改善に関する研究

*Research on Improvement of Registration / Attestation Processing in the Individual Authentication System by Pen Pressure*

学籍番号：1020330　　氏名：森山　剛

指導教員：　竹田史章 教授

年月日：　2002 年 2 月 8 日

所属：　情報システム工学科

# 要旨

近年、インターネットなどのネットワークの普及、情報通信技術の進歩によってビジネス、あるいは情報交換の形態がオンライン化することにより大きく変化してきている。この形態が変わると同時に個人認証に対する技術が必要となる。そこで、本研究では数多くあるバイオメトリクスのなかでも筆圧による個人認証に着目する。筆圧認証でのシステムの核はニューラルネットワークで構成されている。また、これまでの研究の問題点として偽筆誤認証を起こす結果が得られたため、登録署名データの入力値と筆圧データの移動平均のみから移動平均に加えパターン間の分離情報を加えるなど改善を行い、実際に採取した筆圧データによりシミュレーションを行い、その有用性を確認する。

キーワード：筆圧、個人認証、ニューラルネットワーク、筆圧波形

# Abstract

Recently, the online information interchange is popular because business concern about telecommunication technology improvement and widely used internet and network. The personal certification technology became necessary in this kind of interchange. Then, in this research, the purpose is attending to use pen pressure in biometrics for personal certification. Main system of personal certification is organized by Neural Networks. However, this research still has problem about miss-certification. Input of signature data and pen pressure data. It improves only from a moving average by adding the separation information between patterns in addition to a moving average. In practice, simulation is used to collect the pen pressure data utility is confirmed.

Key Words: Pen Pressure, Individual Attestation, Neural Network, Pen Pressure Waveform

# 目次

# 図目次

# 表目次

# 第１章　はじめに

近年、インターネットや社内 LAN などのネットワークの普及、情報通信技術の進展によってビジネス、あるいは情報交換の形態が大きく変わりつつある。ビジネスそのものがオンライン化されることにより、迅速化、グローバル化などが容易に実現可能となる。しかしながら、非対面でのビジネスや情報交換が増加することによってこれまで人が行ってきた個人を特定する技術をコンピュータで実現することが必要となる。さらにコンピュータが関連する犯罪は増加の一途をたどり、「なりすまし」による犯罪を防止する意味からも個人を特定する技術である個人認証の必要性は高まっている。

個人認証とは、あらかじめ本人であることを登録し、その証拠を示すことにより本人であることを確認することである。現在の個人認証に用いられている認証手法は「所有物による認証」、「知識による認証」、「生体情報を利用した認証」の 3 種類の手法に分類することができる。1 つ目の手法として「所有物による認証」は本人であることを証明するものを発行し、それを携帯するものを本人とみなす方法である。その例として運転免許証やクレジットカードなどが挙げられる。2 つ目の手法として「知識による認証」は本人しか知りえない情報の提示により本人とみなす方法である。その例として暗証番号などが挙げられる。3 つ目の手法として「生体情報を利用した認証」は人間の身体、あるいは行動の特徴に基づいて、個人を自動的に認証する方法である[1]。その例として指紋、声紋、虹彩、筆圧などが挙げられる。

生体情報（以下バイオメトリクスと表記）とは「生体測定学」を意味し、バイオメトリクスを利用した個人認証とは、指紋、声紋、虹彩、顔、署名などさまざまな肉体的及び行動的特徴を個人認証に利用することを意味する。バイオメトリクスによる個人認証は、運転免許証やクレジットカードなどの「所有物による認証」や暗証番号などの「知識による認証」と比較して紛失しない、盗まれない、忘れない、偽造・変造されないといったメリットがある。この理由として、身体の一部あるいは行動による認証を行うため物を携帯する必要がほとんどない。また、本人であることを証明する情報を記憶する必要がない、1 次情報（身体の特徴など）を盗まれる心配がほとんどないという点が挙げられる。しかしながら、デメリットとして情報の提示に問題がある。例としてはバイオメトリクスを検出するまでに手間や時間がかかる。次に数多くあるバイオメトリクスについて例を示す。

はじめに、指紋は指先の皮膚紋様であり個別の特徴を持っている。この指紋による自動照合への試みは比較的長い歴史があり，従来の指紋の入力センシングのほとんどはプリズムの反射面に置いた指の凹凸を反射率の違いに反映させ，ディジタル画像化するという光学方式が用いられてきた。また、近年はこれに加え，半導体のチップの表面に直接接触させた指紋から静電容量の差などを用いてその凹凸をセンシングする素子も実用化されつつある。指紋認証のために用いる機器は小さく，自然な形で指紋認証の操作をすることができる。そのため、オペレーティングシステム（Operating System）などへログインする際のユーザ認証や，席を外す際のスクリーンセーバによる端末ロック、ワープロなどにおける一般アプリケーションのファイル内容秘匿のためのパスワード代替などが実現可能となる。

次に音声認識であるが、これは、声紋に現れる個人特性を利用する。指紋照合のよ

うに心理的抵抗が少ないため、広く利用される可能性がある。また、マイクなどの特殊な入力装置が不要である、音声ということで電話を通じての情報サービスなどの実用化が始まっている。他にも、顔による個人を認証するという方法もある。人間は個人ごとに異なった顔であるため、顔を見れば個人を認証できる。また、顔は常時露出しているため、心理的な抵抗感が少なく自然に画像を採取できるとされている。顔認識では、前処理として画像処理の対象領域を決定するために、肌の色、動き、形、大きさなどから顔の発見をする必要がある。この中で肌の色はよく利用されている。個人の顔を認証するには、顔の特徴的な部分の位置関係が重要な手がかりとなると考えられる。コンピュータで見つけやすい特徴としては、顔の輪郭や眉、目、口、鼻など顔固有の部分の位置と形状がある。また、動画像の場合は、顔の動き特徴を利用することができるため、さらに高精度の処理ができるが、それだけ計算量は膨大になる。このようにして、顔での個人認証は可能であり、現在の技術レベルは、眼鏡の着用、髪型あるいは加齢などによる見かけの変化にも対応できる[2]。

また、他のバイオメトリクスとして筆記による個人認証が挙げられる。これは人が自分の氏名を筆記する際に検出される筆圧や筆跡によって、個人を認証するものである。個人認証に筆記情報を用いるのは筆記された文字を他者が模倣することが困難であることによるものであり、欧米では古くから個人認証のための手法として用いられている。筆記された文字が模倣することが困難であるなら、文字を生成するための筆記という行為も他者による模倣が困難であると考えられるため、筆記行為を対象とした認証についてもいくつか手法が提案されている。筆記による個人認証にはオフライン方式とオンライン方式の 2 種類がある。オフライン方式には既に筆記された筆跡の静的情報を用いるものである。これは警察で用いられている筆跡鑑定のようなものである。また、オンライン方式は筆記動作に伴う動的情報を用いるものである。これは筆記を行った際に検出される筆圧をもとに個人を特定するものである。以上のことをふまえた結果より指紋、音声認識、顔画像による個人認証には心理的抵抗が大きいため心理的抵抗を少ないものや計算量を抑えたものによる個人を認証する必要がある。そこで、筆記という動作は日常的な行為であるため、虹彩や声紋のようなバイオメトリクスに比べて心理的な抵抗による拒否反応が少ないと報告されている。そこで、本研究では筆圧による個人認証を行う。

本研究では署名を行うことによって検出される筆圧というバイオメトリクスを用いて個人認証を行うことを目的とする。この筆圧を検出するために筆圧検知器を使用する。この筆圧検知器を使用した動的署名も，個人認証として考えられる。筆記行為はすでに日常化した行為であるため、指紋や網膜を用いる場合に比べ心理的な抵抗による拒否反応は小さく、また音声に比べればサンプル情報量も少ないため、計算量を減少させることが可能である。

現在、筆記情報を用いた個人認証システム実現のためにニューラルネットワークを用いて，筆圧による個人認証システムを実用可能な段階である。ニューラルネットワークは非線形識別能力を持ち、認証パターンの増加と新規認証パターンの登録を容易に実現することが可能である。本研究では筆圧による個人認証システムの構成を示し、これまでの課題であった他人が登録者を模倣した偽筆誤認証率の低下を目的とする。登録署名データにばらつきをもたせることにより、汎用性の向上につながる。認証の際にこれまでの研究では登録署名データとして筆圧データの移動平均をシステムの入力値として用いた。一方、本研究では移動平均に加えパターン間の相関係数と統計

的距離をシステムの入力値として用い個々の認証率向上を目指す。実際に採取された筆記データを用いたシミュレーションにより改善点の効果を定量的に示す。

# 第 2 章　問題点提起

本章ではこれまでの研究において認証率の低い偽筆による個人認証に対しての問題点を提起する。[4]

これまでの研究では、筆記という動的なバイオメトリクスを用いることに着目し、学習にニューロテンプレートマッチング識別手法を用いた個人認証システムの研究を行った。学習における抑制データの新しい作成手法として、本人の登録署名データから正規乱数を発生させ、それをもとに抑制データを生成することを提案し、実験では、シミュレーションにより従来手法と提案手法とで個人認証性能の比較を行い、提案手法の有効性を確認できる。ただし、抑制データとは本人以外と教師するデータである。しかしながら、他人が登録者を模倣した偽筆データについての誤認証率が高い問題も残されていた、そこで、現在の本人認証率、誤認証率を保つとともに、偽筆誤認証率を低下させることを目的とし、抑制データ生成手法、ニューラルネットワークへの入力筆記データの作成法を検討する必要がある。

表 2.1、表 2.2 の中では判定しきい値 TH は、0.4～0.9 としているが、実際の認証システムでは、0.6 か 0.7 で設定し出力判定を行っている。性能比較では TH が 0.6、0.7 の場合の認証結果をみることとする。表 2.1 では、本人認証率では平均 90％の認証率を得ることを確認できる。誤認証率においても 1.00%を切る程度の精度を得ることができ、共に高い認証精度を得ることができる。しかしながら、偽筆誤認証では約 50％の偽筆データに対して、本人であると誤認証して、良好な結果とはいえない。一方、表 2.2 の正規乱数で抑制データを作成した場合、本人認証率は表 2.1 に比べて若干向上している。また、偽筆誤認証率の値が 0.0%となればよいが、40%台の誤認証率であり、他人の登録署名データで抑制データを作成したときより偽筆誤認証率を抑えることに成功している。しかしながら、誤認証率は表 2.1 に比べて精度が低下してしまっている。特に、k0a の誤認証率が非常に悪いことがわかっている。これは、k0a のテンプレートに入力した k09 のテストデータ全てを、k0a と誤って認証したためである。

これまでの実験では、抑制データの作成法として他人の登録署名データから作成する場合と、本人の登録署名データから得られた正規乱数から作成する場合の 2 種類を用いて実験を行った実験結果から、認証精度は正規乱数を用いた方が、若干ではあるが性能は上であると考えられる。しかしながら、本章の最初に述べたように偽筆誤認証率が高くなってしまい、他人の署名でも本人と判定してしまう可能性がある。また、偽筆に対する誤認証も、しきい値を 1 番大きくしても 30%近くの値を示されている。表 2.1、表 2.2 に示す偽筆認証率では、どちらも本人と誤って認証した偽筆は、ほぼ同じ人物である。たとえば、表 2.1、表 2.2 の両方においても学生 k05 の偽筆認証率の結果では、k09 から採取した偽筆 9 回のほとんどすべてに対して本人と判断している。このことから、偽筆誤認証率を低下させるために改善を行う。

表 2.1　これまでの実験結果（他人の登録署名データから抑制データを作成した場合の本人認証率・誤認証率及び偽筆誤認証率）
登録者名：K05~K0b，TH：判定しきい値，登録データ数：10

本人認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 40 | 40 | 40 | 40 | 39 | 37 | 100.00% | 100.00% | 100.00% | 100.00% | 97.50% | 92.50% |
| K06 | 31 | 31 | 29 | 29 | 29 | 27 | 77.50% | 77.50% | 72.50% | 72.50% | 72.50% | 67.50% |
| K07 | 40 | 40 | 40 | 40 | 40 | 39 | 100.00% | 100.00% | 100.00% | 100.00% | 100.00% | 97.50% |
| K08 | 40 | 40 | 40 | 40 | 39 | 38 | 100.00% | 100.00% | 100.00% | 100.00% | 97.50% | 95.00% |
| K09 | 37 | 37 | 36 | 36 | 34 | 34 | 92.50% | 92.50% | 90.00% | 90.00% | 85.00% | 85.00% |
| K0a | 31 | 31 | 31 | 29 | 28 | 28 | 77.50% | 77.50% | 77.50% | 72.50% | 70.00% | 70.00% |
| K0b | 35 | 35 | 34 | 34 | 33 | 30 | 87.50% | 87.50% | 85.00% | 85.00% | 82.50% | 75.00% |
| 計 | 254 | 254 | 250 | 248 | 242 | 233 | 90.71% | 90.71% | 89.29% | 88.57% | 86.43% | 83.21% |

誤認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 1 | 1 | 0 | 0 | 0 | 0 | 0.42% | 0.42% | 0.00% | 0.00% | 0.00% | 0.00% |
| K06 | 1 | 1 | 1 | 1 | 0 | 0 | 0.42% | 0.42% | 0.42% | 0.42% | 0.00% | 0.00% |
| K07 | 1 | 1 | 0 | 0 | 0 | 0 | 0.42% | 0.42% | 0.00% | 0.00% | 0.00% | 0.00% |
| K08 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K09 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K0a | 8 | 6 | 6 | 4 | 3 | 0 | 3.34% | 2.50% | 2.50% | 1.67% | 1.25% | 0.00% |
| K0b | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| 計 | 11 | 9 | 7 | 5 | 3 | 0 | 0.65% | 0.54% | 0.42% | 0.30% | 0.18% | 0.00% |

偽筆誤認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 21 | 21 | 21 | 19 | 19 | 13 | 38.89% | 38.89% | 38.89% | 35.19% | 35.19% | 24.08% |
| K06 | 29 | 29 | 28 | 27 | 26 | 18 | 53.71% | 53.71% | 51.86% | 50.00% | 48.15% | 33.34% |
| K07 | 17 | 17 | 15 | 14 | 13 | 8 | 31.49% | 31.49% | 27.78% | 25.93% | 24.08% | 14.82% |
| K08 | 41 | 41 | 40 | 36 | 35 | 31 | 75.93% | 75.93% | 74.08% | 66.67% | 64.82% | 57.41% |
| K09 | 25 | 25 | 25 | 23 | 22 | 15 | 48.08% | 48.08% | 48.08% | 44.24% | 42.31% | 28.85% |
| K0a | 26 | 26 | 24 | 24 | 24 | 23 | 48.15% | 48.15% | 44.45% | 44.45% | 44.45% | 42.60% |
| K0b | 35 | 35 | 35 | 32 | 30 | 26 | 67.31% | 67.31% | 67.31% | 61.54% | 57.70% | 50.00% |
| 計 | 194 | 194 | 188 | 175 | 169 | 134 | 51.87% | 51.87% | 50.27% | 46.79% | 45.19% | 35.83% |

表 2.2　これまでの実験結果（正規乱数を抑制データとして使用した場合の本人認証率・誤認証率及び偽筆誤認証率）
登録者名：K05~K0b，TH：判定しきい値，登録データ数：10

本人認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 39 | 39 | 39 | 39 | 38 | 36 | 97.50% | 97.50% | 97.50% | 97.50% | 95.00% | 90.00% |
| K06 | 33 | 33 | 33 | 33 | 32 | 31 | 82.50% | 82.50% | 82.50% | 82.50% | 80.00% | 77.50% |
| K07 | 47 | 47 | 47 | 46 | 46 | 46 | 100.00% | 100.00% | 100.00% | 97.88% | 97.88% | 97.88% |
| K08 | 39 | 39 | 39 | 39 | 39 | 39 | 97.50% | 97.50% | 97.50% | 97.50% | 97.50% | 97.50% |
| K09 | 32 | 32 | 32 | 32 | 31 | 28 | 80.00% | 80.00% | 80.00% | 80.00% | 77.50% | 70.00% |
| K0a | 37 | 36 | 36 | 35 | 33 | 29 | 92.50% | 90.00% | 90.00% | 97.50% | 82.50% | 72.50% |
| K0b | 36 | 36 | 36 | 36 | 36 | 36 | 90.00% | 90.00% | 90.00% | 90.00% | 90.00% | 90.00% |
| 計 | 263 | 262 | 262 | 260 | 255 | 245 | 91.64% | 91.29% | 91.29% | 90.59% | 88.85% | 85.37% |

誤認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K06 | 1 | 1 | 1 | 1 | 1 | 1 | 0.42% | 0.42% | 0.42% | 0.42% | 0.42% | 0.42% |
| K07 | 3 | 3 | 2 | 1 | 1 | 0 | 1.25% | 1.25% | 0.84% | 0.42% | 0.42% | 0.00% |
| K08 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K09 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K0a | 51 | 51 | 50 | 49 | 46 | 41 | 21.25% | 21.25% | 20.84% | 20.42% | 19.17% | 17.09% |
| K0b | 21 | 21 | 17 | 11 | 7 | 5 | 8.75% | 8.75% | 7.09% | 4.59% | 2.92% | 2.09% |
| 計 | 76 | 76 | 70 | 62 | 55 | 47 | 4.56% | 4.56% | 4.20% | 3.72% | 3.30% | 2.82% |

偽筆誤認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 17 | 17 | 17 | 16 | 14 | 8 | 31.49% | 31.49% | 31.49% | 29.63% | 25.93% | 14.82% |
| K06 | 16 | 16 | 16 | 12 | 10 | 7 | 29.63% | 29.63% | 29.63% | 22.23% | 18.52% | 12.97% |
| K07 | 19 | 19 | 18 | 18 | 16 | 14 | 35.19% | 35.16% | 33.34% | 33.34% | 29.63% | 25.93% |
| K08 | 35 | 35 | 34 | 32 | 30 | 26 | 64.82% | 64.82% | 62.97% | 59.26% | 55.56% | 48.15% |
| K09 | 22 | 22 | 22 | 21 | 19 | 14 | 42.31% | 42.31% | 42.31% | 40.39% | 36.54% | 26.93% |
| K0a | 22 | 22 | 18 | 17 | 14 | 14 | 40.75% | 40.75% | 33.34% | 31.49% | 25.93% | 25.93% |
| K0b | 30 | 30 | 29 | 29 | 28 | 25 | 58.83% | 58.83% | 56.87% | 56.87% | 54.91% | 49.02% |
| 計 | 161 | 161 | 154 | 145 | 131 | 108 | 43.16% | 43.16% | 41.29% | 38.87% | 35.12% | 28.95% |

# 第 3 章　改善案の提示

本章では筆圧検知器の前バージョンと新バージョンとの比較を記述する。前バージョンとはこれまでの研究に用いていたシステム（以下バージョン A と表記）で、新バージョンとは本研究で使用したシステム（以下バージョン B と表記）である。

## 3-1　バージョン A とバージョン B の比較

① インターフェースとしてシリアルポート、USB ポートの両方のインターフェースに対応できるように改良
② 登録処理時での入力データの作成方法
③ 認証種類の変更
④ 認証判定方法

### 3-1-1　インターフェースの変更点

筆圧を検出するために筆圧検知器を使用している。この筆圧検知器には 2 種類のインターフェースがあり、シリアルポートを使用するタイプのインターフェースと USB ポート使用するタイプのインターフェースがある。シリアルポートを使用するタイプのインターフェースは AC 電源を必要とするため、使用場所が AC 電源を確保できる場所と限定される。USB ポートを使用するタイプのインターフェースは AC 電源を使用しないため、使用環境に依存せずに使用することが可能である。バージョン A では AC 電源を使用するシリアルポートタイプのインターフェースを採用した。しかしながら、バージョン B ではシリアルポートと USB ポートの 2 種類を使うことができる。このシリアルポートから USB ポート、USB ポートからシリアルポートへの変更はプログラムを変更することにより両方を使い分けることが可能となっている。これは、プログラムのインターフェースの部分をブロック化することにより実現することが可能である。

### 3-1-2　登録処理時での入力データ作成方法の変更点

登録処理時に筆圧データを登録する際に適性チェックを行う。これは、ニューラルネットワークに登録署名データを入力し、学習を行う場合、登録署名データにある程度ばらつきをもたせた方が認証率は向上する。しかしながら、ばらつきが大きくなれば学習の低下や本人認証率の低下を招く確率がある。そこで、登録処理を行う前に、登録署名データに対するチェック機構を設け、その署名データが登録するに値するかどうかをチェックする。このチェックの結果によって異常があると判断されたデータに対しては再登録処理を進める。ただし、すべての登録署名データを再登録させるのではなく、登録時にチェック機構を設けて異常が含まれると思われるデータを検出し、そのデータに対してのみ再登録を行う。

### 3-1-3　認証種類の変更

筆圧に必要なデータは本人署名データの登録署名データと本人以外を教師する抑制データの 2 種類のデータが必要である。

バージョン A では偽筆による登録署名データから作成した抑制データと登録者本人から正規乱数により抑制データを作成した2種類の抑制データを用いて実験を行い、両方の抑制データによる本人認証率、誤認証率、偽筆誤認証率の 3 項目について本人認証率は向上、誤認証率、偽筆誤認証率については低下させることを目的として認証実験を行っている。

本研究では抑制データの作成手法は偽筆によるものだけを使用し、実験を行う。

### 3-1-4　認証に用いる入力データの検討

認証の際にバージョン A では、登録署名データとして筆圧データの移動平均を入力値として用いた。バージョン B では、上記に加えパターン間の相関係数と統計的距離値のパターン間の分離情報を用い、偽筆誤認証率の低下を目指す。

# 第 4 章　提案システムの構成

## 4-1　提案システムの入出力機器構成

筆圧を検出するシステムが Windows95/98 上で動作するため、PC には Windows95/ 98 対応のパソコンを使用している。データ収集 BOX は H83048 マイコンを搭載し、PC とはシリアルポート(19,200bps)で接続されている。電源は AC アダプタによって得ている。データ収集 BOX に電子ペンが 5 芯ケーブルによって接続される。データ収集 BOX と電子ペンを図 4.1 に示す。また、本システムはシリアルポートと USB ポートの両方で動作可能となっている。筆圧情報は、電子ペンと呼ばれるペン状の入力装置を用いることにより採取される。

本研究で使用する電子ペンは、筆圧分解能 0.1g、時間分解能 4ms という高分解能の筆圧波形を得ることができる。筆圧波形とは、1 回の筆跡による筆圧の時間変動を表したものである。本研究で扱う筆圧認証は、この筆圧波形から抽出した特徴量により個人を認証するオンライン方式の個人認証である。電子ペンの構成図を図 4.2 に示す。

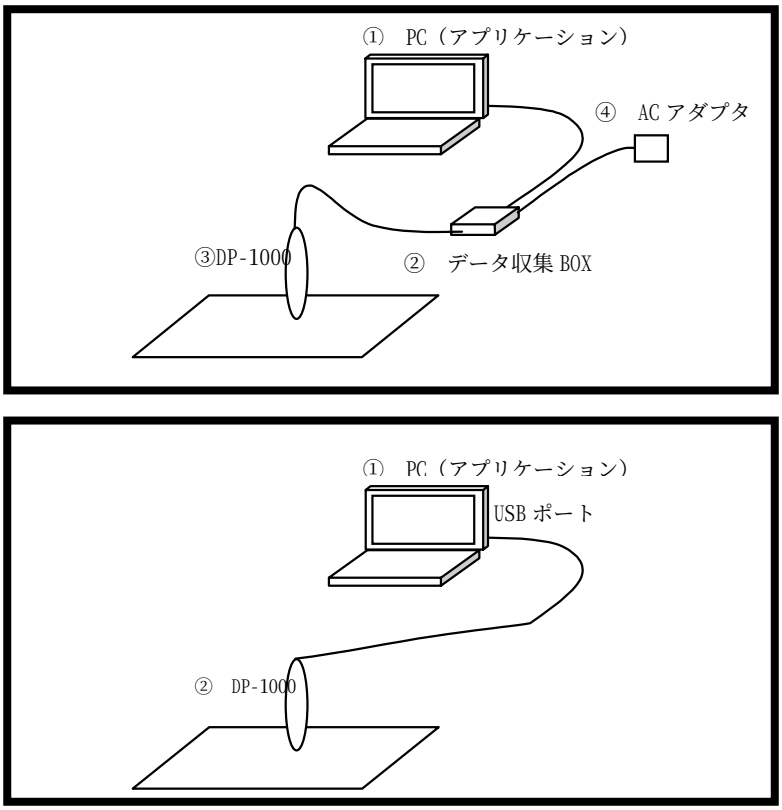



図 4.1　機器構成図（上図：シリアル版、下図：USB 版）

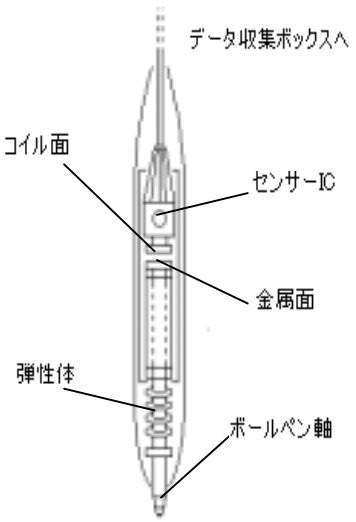



図 4.2　電子ペンの構成図

## 4-2　登録処理の概要

### 4-2-1　登録処理

登録セッションは、電子ペンによりサインを行い、前処理によって生成されたデータをニューラルネットワークに学習させることにより、本アプリケーションに登録を行う部分である。登録セッションには、「新規登録」、「追加登録」、「更新登録」の 3 種類がある。図 4.3 に登録セッションの流れを示す。

①新規登録とは未登録の人が認証システムに登録を行う。

②追加登録とは既に登録している人が、既存の登録署名データに新しい署名データを追加し、登録処理を行う。

③更新登録とは既に登録している人が、既存の登録署名データをすべて破棄し、新しく採取する署名のみで登録処理を行う。

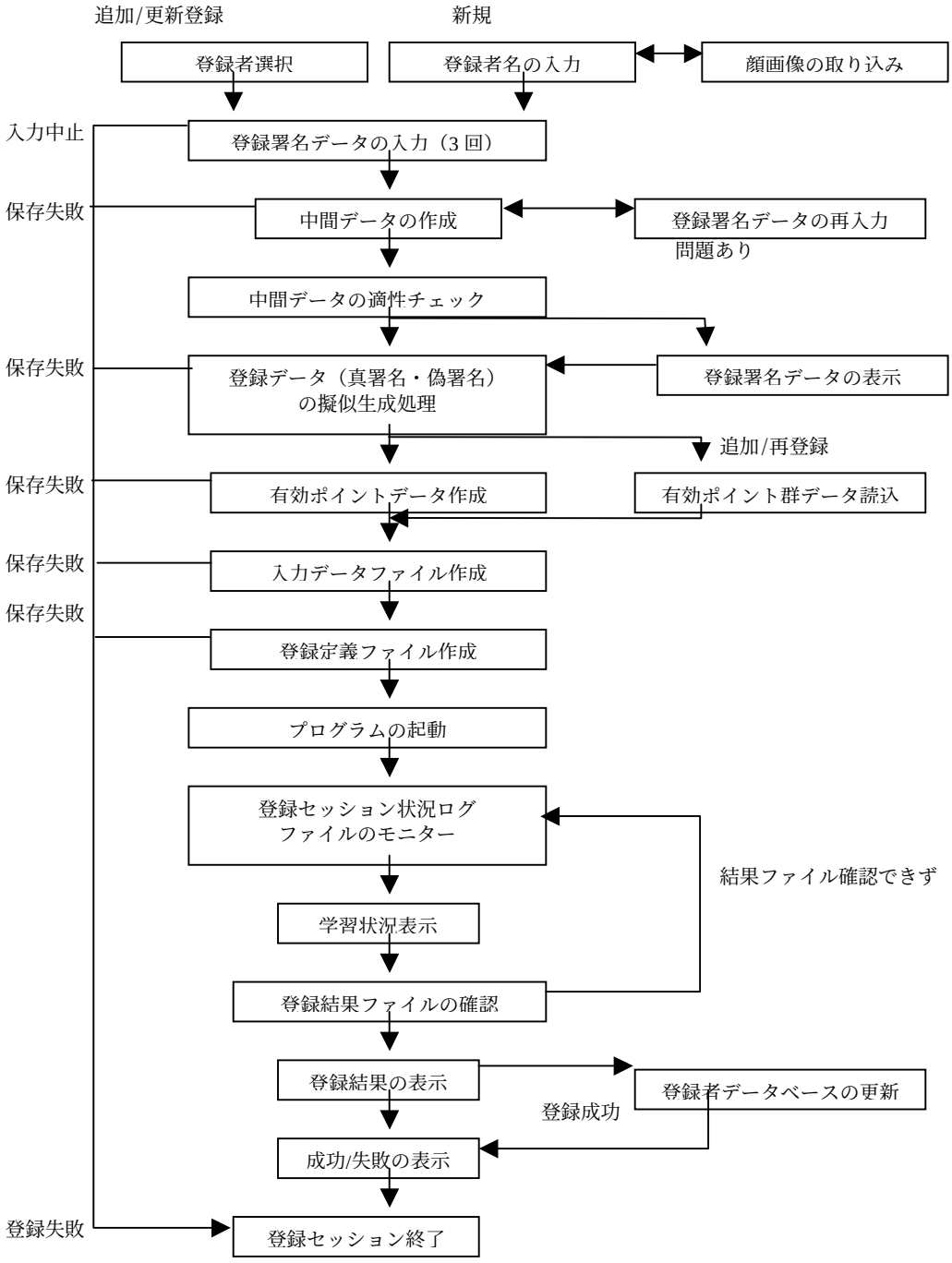



図 4.3　登録セッション処理の流れ

## 4-2-2　登録時における処理

新規登録時の場合、ID は自動で振り分けられるが、登録名は入力する必要がある。図 4.4 に登録時の処理を示す。

①登録者 ID の自動割当

登録者 ID を割り当てる。0001～1000 の 4 桁で、0000 は使用しない。ユーザによって登録者 ID を変更することはできない。

②登録者名の入力

登録者の氏名を入力する。

③登録者名の重複チェック
入力された登録者名が既存の登録者の名前と重複していないかをチェックする。
重複している場合は②へ戻る。
④署名データ入力処理
電子ペンから測定カウント値を受信し、署名データを採取する。

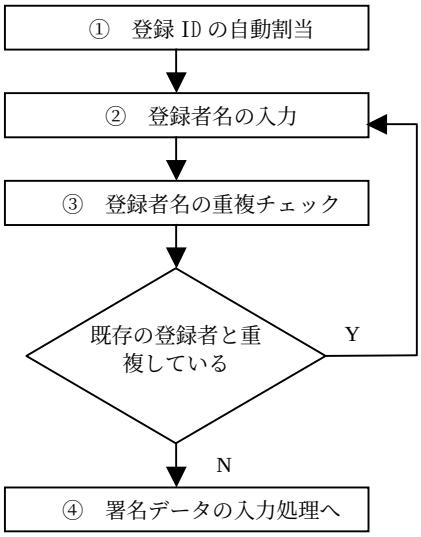



図 4.4　登録時の処理

## 4-2-3　登録署名データ入力

認証システムに登録を行うために、登録用のサインをおこなう。このサインは 3 回行う。図 4.5 に示す。

①書きはじめの検出
どの登録処理においても自動的に書きはじめの検出を行う。最新 10 個の筆圧カウント値データから、その分散値を計算し、分散値が 10.0 を超えれば書き始めとして次の処理へ進む。

②署名データへのサンプリング
書き始め検出直前のカウント値を基準カウント値とし、筆圧カウント値をソースデータ用配列に格納する。

③書き終わりの検出
書き始め同様、書き終わりも自動検出する。50 未満の筆圧カウント値が連続で何個サンプリングされたかを計算し、その連続数が規定値を超えれば書き終わりとして処理を行う。

④登録署名データ保存
署名データの採取が成功すると、署名データは WORK フォルダに一時的に保存する。登録処理に成功すればこのデータが登録署名データとして別フォルダに保存する。

⑤適正チェック処理へ
ニューラルネットワークモジュールへの学習を行う前に、採取されたデータに学習効率を低下させるようなばらつきの大きいソースデータの有無を調査する。

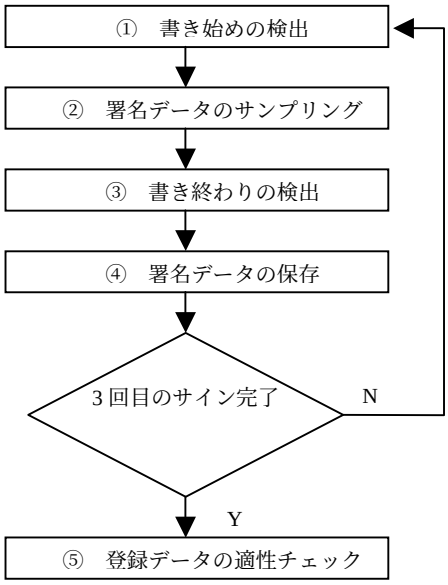



図 4.5　登録ソースデータの入力

## 4-2-4　登録署名データの適性チェック

登録ソースデータ中に、他の登録署名データとの相違点が多く、ニューラルネットワークモジュールの学習効率に影響を与えそうなものがある場合は、そのことを表示し、ソースデータの再入力を促す。このチェックには、各登録署名データから抽出した参照データを比較することで行う。図 4.6 に登録署名データとしての適正チェックを示す。

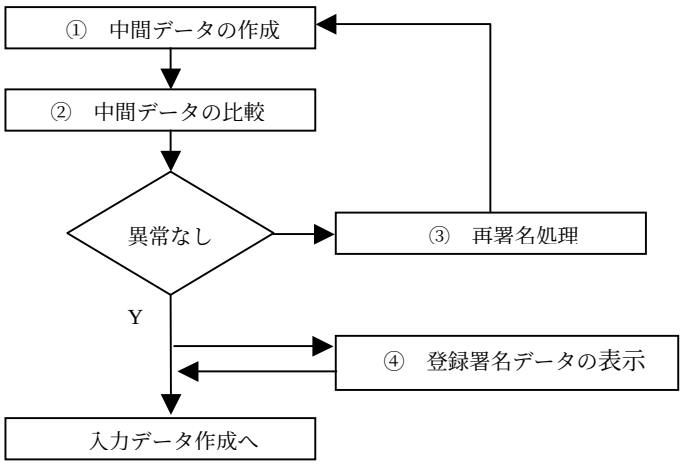



図 4.6　登録データとしての適正チェック

①中間データの作成

登録されたソースデータそのままでは、ニューラルネットワークに学習させることができない。ニューラルネットワークに渡すデータ（入力データ）を作成する為の中間データを作成する。中間データは、1,000 個以上の要素を持つ署名データを適当な数（現在 300 個）のデータに変換する。変換方法としては移動平均法を使用する。

②中間データ間の比較

登録署名データとしての適正を測る為に、中間データでの類似度を計算する。類似

度を示す為に抽出するデータは以下の 2 つがある。

1. データ間の相関係数

登録署名データから作成される中間データとの間で相関係数を求める。同一筆記者の署名間の相関が強いことが前提である。相関係数の計算式を式(4.1)に示す。2 つのデータ Data1(s,n)と Data2(s,m)(s=1～S)の相関係数は R(n,m)は、今、2 つのデータの平均値をそれぞれ、

$$Ave\ (n) = \frac{1}{S}\sum_{s=1}^{S} Data\ \ 1(s,n),\ Ave\ (m) = \frac{1}{S}\sum_{s=1}^{S} Data\ \ 2(s,m) \qquad (4.1)$$

とすると

$$R(n,m) = \frac{\sum_{s=1}^{S}(Data\ \ 1(s,n)\,Data\ \ 2(s,m)) - Ave\ (n)\,Ave\ (m)}{\sqrt{\sum_{s=1}^{S}(Data\ \ 2(s,n))^2 - S\cdot(Ave\ (n))^2}\ \sqrt{\sum_{s=1}^{S}(Data\ \ 2(s,m))^2 - S\cdot(Ave\ (m))^2}} \qquad (4.2)$$

となる。この相関係数の取りうる値は、[-1,1]である。1 に近いほど相関が強く、0 に近づく程相関が弱いということになる。

2. 統計的距離値（ユークリッド値）

登録署名データから作られる中間データ間で類似度を示すユークリッド距離値を求める。この距離値を求める式を式(4.3)に示す。

$$D(n,m) = \sqrt{\sum_{s=1}^{S}(Data\ \ 1(s,n) - Data\ \ 2(s,m))^2} \qquad (4.3)$$

0 に近いほどデータ間の距離が小さい、つまり類似していることになる。

相関係数は横軸方向への「ずれ」には敏感に反応するが、縦軸方向の値の「ずれ」にはあまり反応を示さない。逆に距離値は、縦軸方向の値の「ずれ」に敏感に反応するが、横軸方向への「ずれ」にはあまり反応を示さない。そういう意味で、この 2 つの要素両方を使用することで、登録署名データ間に異常が無いかどうかをチェックする。

③異常と思われる署名データの検出

中間データ間の比較によって得られた相関係数と距離値を用いて異常と思われるデータの選定を行う。3 個の登録署名データの場合、3 組の相関係数値と距離値が得られる。相関係数値を R(I),距離値を D(I)とし(I＝1～3),式(4.4)を用いて変数 Flag の値を設定する。但し、追加登録の場合、登録署名データ間で比較せず、既存の中間データの重心（平均）データと追加データそれぞれを比較した結果を式に適用する。図 4.7 に相関係数と距離値を示す。

$$\mathrm{Flag(I)} = \begin{cases} 1 & (R\ \ (I)\ > 0.3)\ \ \mathrm{AND}\ \ (D\ \ (I)\ < 1.9) \\ 0 & (R\ \ (I)\ \le 0.3)\ \ \mathrm{OR}\ \ (D\ \ (I)\ \ge 1.9) \end{cases} \qquad (4.4)$$

R,D の閾値(0.3,1.9)は設定ファイルにて変更可能である。

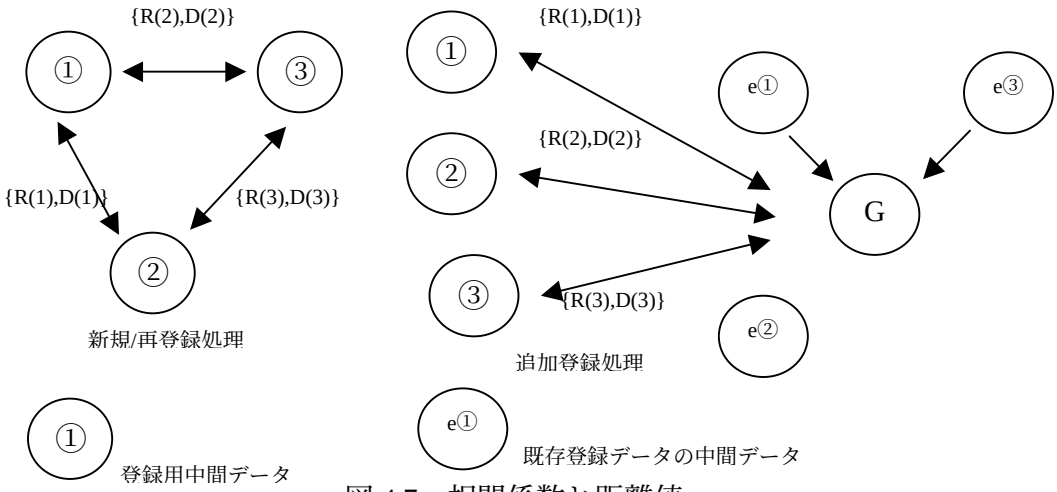



図 4.7　相関係数と距離値

求めたフラグに対し、以下の表 4.1 により、認証精度の低下を招くおそれのあるデータを決定する。

表 4.1　登録データの適正チェック

| Flag (1) | Flag (1) | Flag (1) | Data 1 | Data 2 | Data 3 | Check |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | NG | NG | NG | [000] |
| 1 | 0 | 0 | OK | OK | NG | [110] |
| 0 | 1 | 0 | NG | OK | OK | [011] |
| 0 | 0 | 1 | OK | NG | OK | [101] |
| 1 | 1 | 0 | NG | OK | NG | [010] |
| 1 | 0 | 1 | OK | NG | NG | [100] |
| 0 | 1 | 1 | NG | NG | OK | [001] |
| 1 | 1 | 1 | OK | OK | OK | [111] |

Data1～Data3 は登録ソースデータを指す
OK : 問題無し　NG : 問題あり

このチェックにより[111]（1 番下）になれば⑥以降へ進み、それ以外になれば④へ進む。

④適正チェック処理 2

チェック結果が[111]以外になり、「1」となっている数が 1 つしかない場合([100],[010],[001])に以下の処理を行う（それ以外は処理⑤へ進む）。

NG に 2 データ間の相関係数を ngR, 距離値を ngD とする。

1.ngR>0.3, ngD≧1.9 （距離値が条件を満たさずに NG）の場合
「1」となるデータとの距離値がより小さいデータを「1」にする。

2.ngR≦0.3, ngD<1.9 （相関係数が条件を満たさずに NG）の場合
「1」となるデータとの相関係数値がより大きいデータを「1」にする。

3.ngR<0.3, ngD≧1.9 （両方が条件を満たさずに NG）の場合
何も処理を行わず処理⑤へ進む。

⑤再署名処理

適正チェックにおいて問題ありと判断されたソースデータに関して再署名を行う。再

署名が終了すると、再び登録ソースデータの適正チェックをはじめ、すべての登録署名データに問題なしと判断したときに限り、次の処理へと進む。
⑥登録署名データの波形表示
採取した登録ソースデータを時間軸上に連続的に並べ、筆圧カウント値波形を表示する。

## 4-2-5　登録用の擬似データ作成

本システムが使用するニューラルネットワークを、マッチングにおけるテンプレートのように使用するには、学習という形でニューラルネットワークを構築させなければならない。そしてこの学習には、ニューラルネットワークに対して本人のデータを(1)と教師する「強化データ」と、本人以外を(0)と教師する「抑制データ」の 2 種類が必要である。強化データは登録署名から得られるデータを使用する。これに対し、抑制データには本人以外が模倣筆記した偽署名を使用するが、実用上この偽署名は使用できない（登録処理時にこの偽署名は存在しない）。そこで、強化データ、抑制データを擬似的に生成し、学習用の入力データに加える。
①登録署名データ間での対応付け
署名データは、筆記の際にサンプリングされるデータ（以下、実画と表記）と、文字と文字、又は画と画の間にサンプリングされるデータ（以下、空画と表記）に分けられる。図 4.8 に実画と空画を示す。

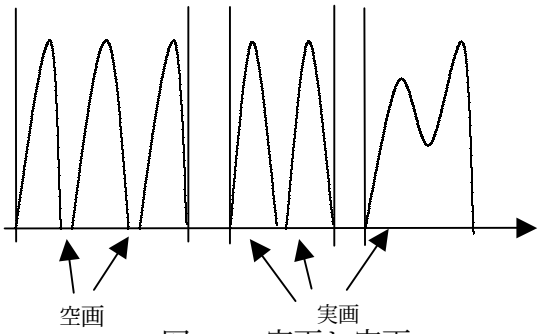


図 4.8　実画と空画

実画と空画に分離したデータに対し、登録署名データ間で対応付けを行う。対応付けは、登録署名データ A のある実画が登録署名データ B,C のどの実画にあたるかを推察し、割り当てる。組み合わされたデータ幅の標準偏差が最小になる組み合わせを検出する。図 4.9 に対応付けの処理を示す。

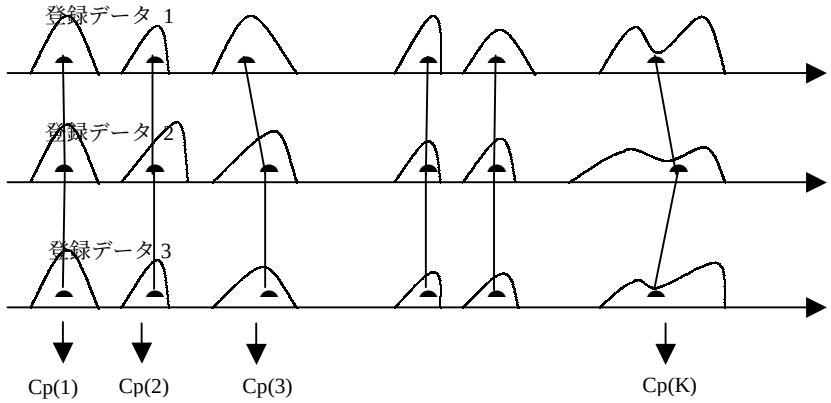



図 4.9　対応付け処理

②対応付け結果から本人署名（強化データの元）を擬似生成し、中間データを作成する。強化データは、本人に限りなく近い擬似データとして作成する。

1.組み合わせ単位で登録署名データを組み替えて作成する。図 4.10 に組み合わせ単位での擬似データ生成を示す。

| | | | | |
|---|---|---|---|---|
| $R_1(1)$ | $R_2(2)$ | $R_3(3)$ | ・・・ | $R_{mod(K.3)+1}(K)$ |
| $R_2(1)$ | $R_3(2)$ | $R_1(3)$ | ・・・ | $R_{mod(K+1.3)}(K)$ |
| $R_3(1)$ | $R_1(2)$ | $R_2(3)$ | ・・・ | $R_{mod(K+1.3)+1}(K)$ |

Rn(t) : n 番目登録データの t 番目登録データ、K : 組み合わせ数

図 4.10　組み合わせ単位での擬似データ生成

2.筆圧カウント値を等倍する（±2～3%）。図 4.11 に筆圧カウント値の変化を示す。

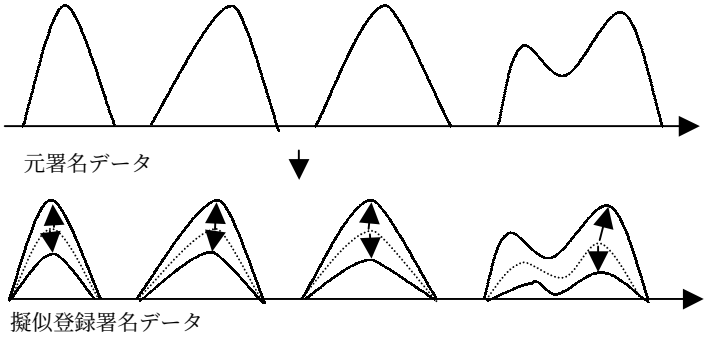



図 4.11　筆圧カウント値の変化

③対応付け結果から偽署名（抑制データの元）を議事生成し、中間データを作成。抑制データは、第 3 者が模倣した擬似データとして作成する。

1.データの組み合わせは、図 4.10 と同じように行う。

2.データ幅の倍率は、それぞれの実画に対して設定して変化させる。図 4.12 にデータの縮小、伸張を示す。

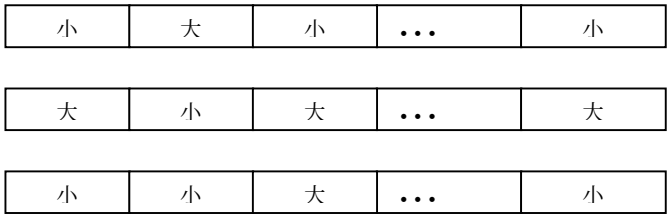



図 4.12　データの縮小、伸張

3.筆圧カウント値の変成は登録署名データを擬似生成する場合は、単に筆圧カウント値を等倍する。偽署名を想定した場合、署名という行動で最も他人との違いが出るのは、リズムや筆記速度である。そこで、筆記速度、リズム等を擬似的に変性させる事で偽署名を生成する。本プログラムは、適当な線形関数を筆圧カウント値に乗算させる方法を使用している。図 4.13 に偽署名の擬似データ生成を示す。

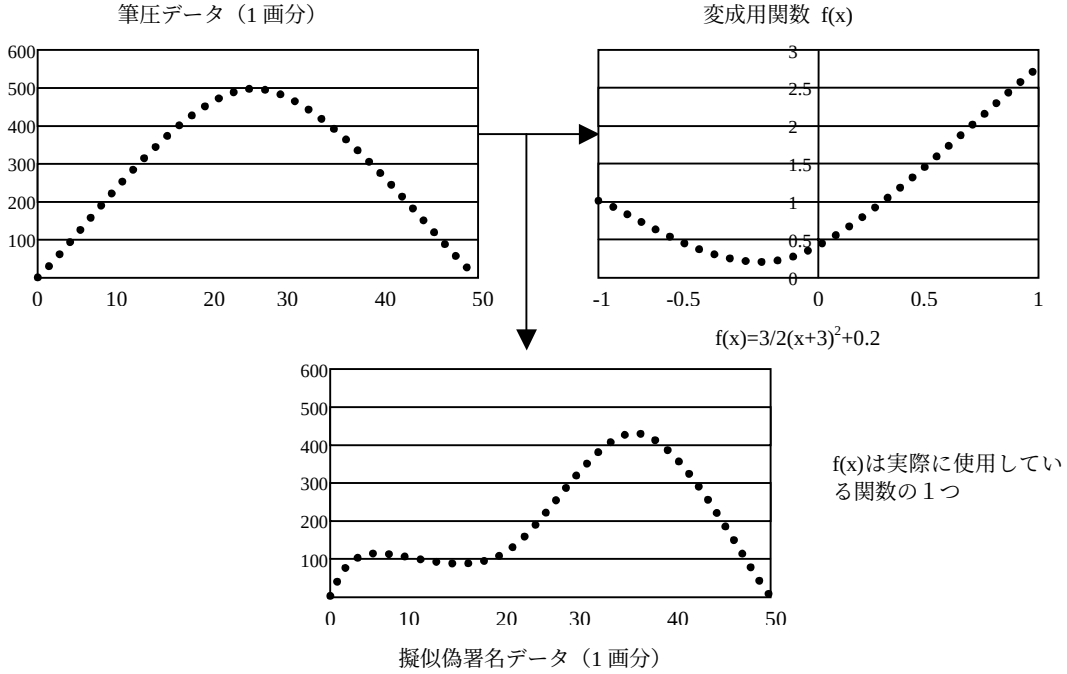



図 4.13　偽署名の擬似データ生成

## 4-2-6　有効ポイント群データの作成

300 個の要素を持つ中間データから、有効と思われるデータ 50 個を抽出する。登録署名データから作られる中間データ間で、各要素（1～300）について標準偏差と平均値を求める。図 4.14 に中間データ各番号の標準偏差（σ）と平均値（μ）の計算を示す。

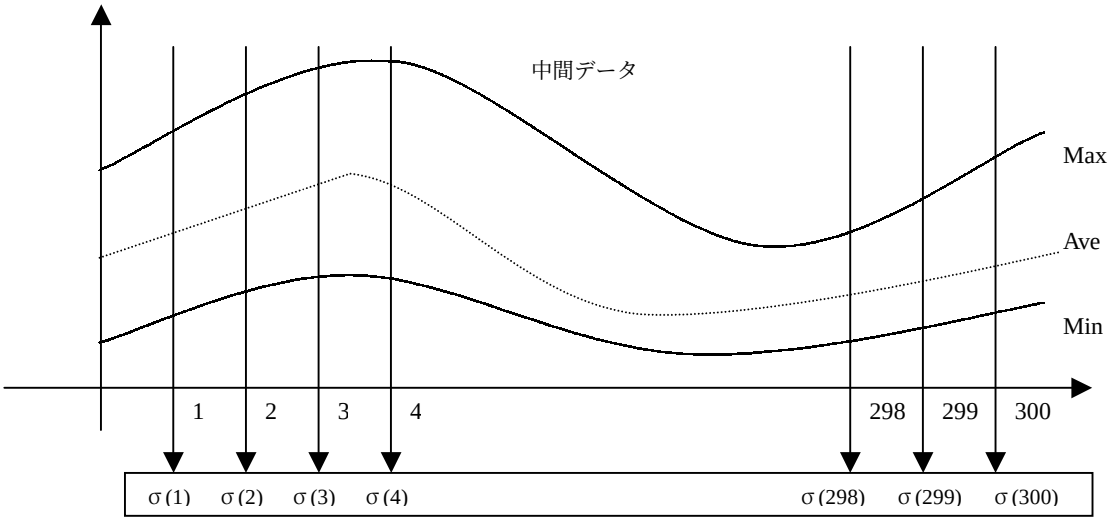
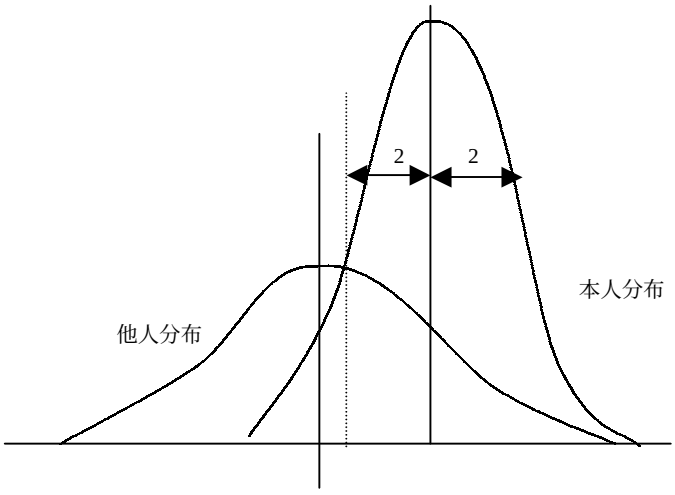



図 4.14　中間データ各番号の標準偏差（σ）と平均値（μ）の計算

また擬似生成した偽署名の中間データからも同様に求める。中間データの各要素は、正規分布に従うことを前提に、他人と本人の分布が重ならないと思われるポイント 50 個を抜き出す。図 4.15 に有効ポイント群の抽出基準を示す。そのために使用する要素番号に 1、使用しない番号に 0 が割り当てられた有効ポイント群データを作成する。図 4.16 に有効ポイントビット情報の作成を示す。




※　本人データの平均±σに存在する他人データの分布

図 4.15　有効ポイント群の抽出基準

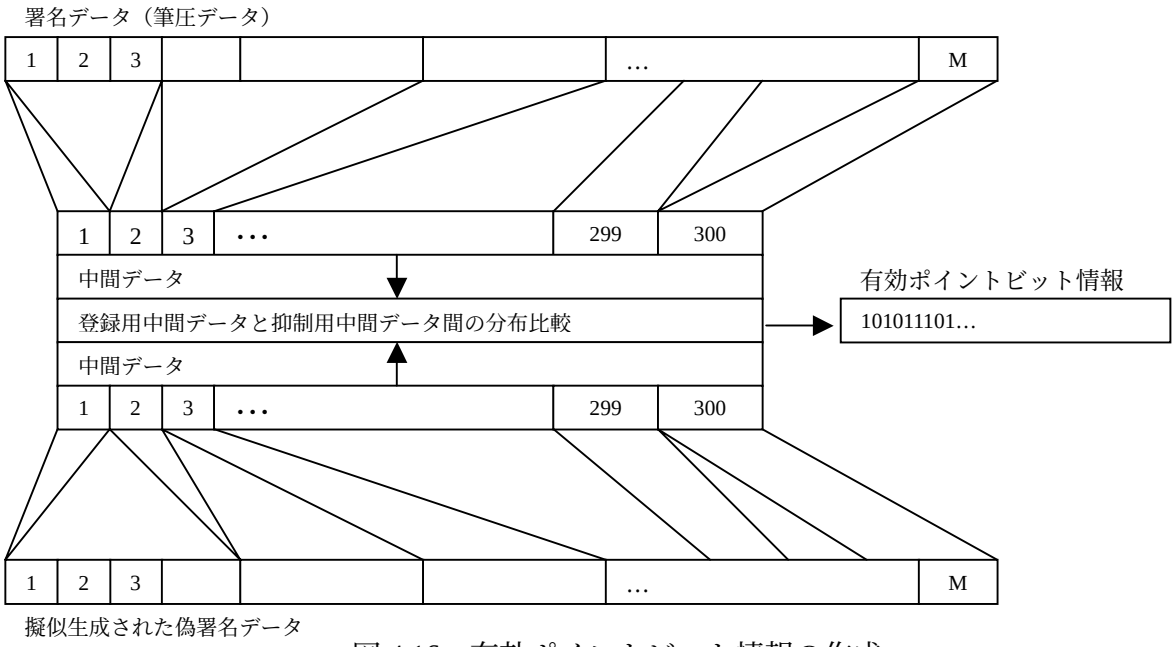



図 4.16　有効ポイントビット情報の作成

## 4-2-7　入力データ（ニューラルネットワーク入力用）の作成

4-2-6 で作成した有効ポイントビット情報と中間データを使用して入力データを作成する。有効ポイントビット情報において、「1」とされている有効ポイントを抽出し、ニューラルネットワークに入力するデータを作成する。現在のデータサイズは 50 に設定されている。これに、ヘッダをつけ、「WRITE.DAT」というファイル名で WORK フォルダに保存する。本システムでは、抑制データ側の入力データ（Unknown.Slb）も作成する。このファイルは、フォルダに保存する。ただし、「WRITE.DAT」とは違うフォーマットで保存する。図 4.17 に登録用入力データの作成を、図 4.18 に抑制用入力データの作成を示す。

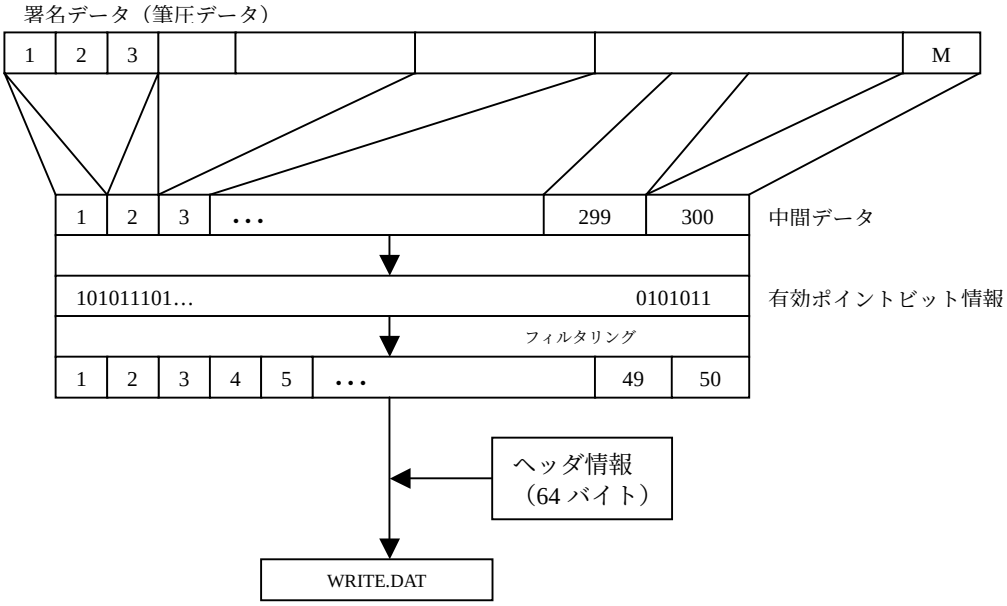



図 4.17　登録用入力データの作成

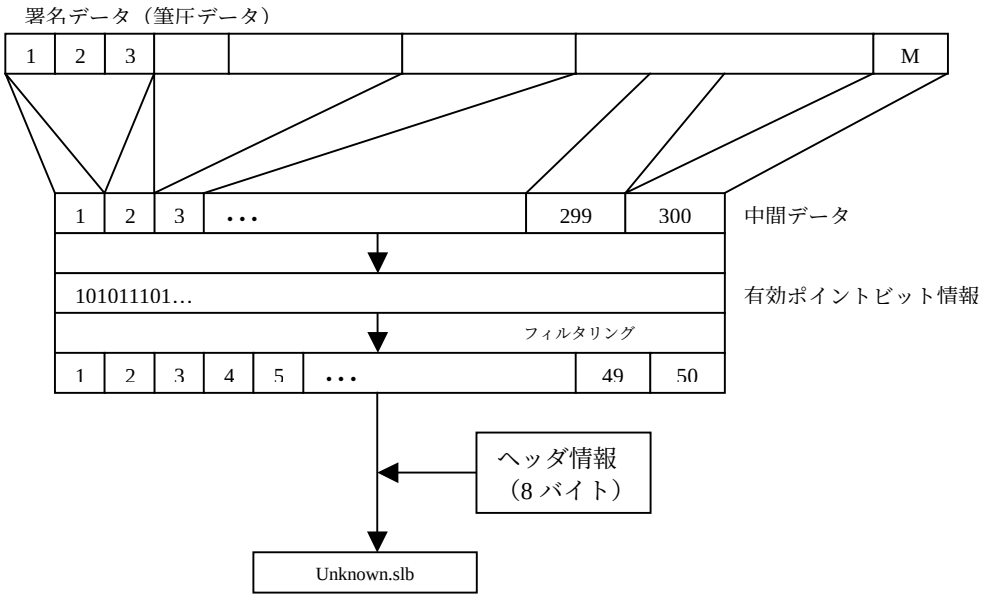



図 4.18　抑制用入力データの作成

WRITE.DAT、Unknown.Slb の 2 つのフォーマットはともにバイナリ形式で保存する。また、ヘッダのサイズは、指定サイズでなければ正常に動作しない。Unknown.Slb は登録者ごとに用意する。1 度作成したデータを再度作成しないように、使用しないファイルは別名で保存する。

## 4-2-8　登録セッションモニタ

本システムの登録（学習）処理は、登録用データを増加させた倍率分だけ発生する（3 個単位で学習させるため)。例えば、3 個から 12 個にした場合、増加倍率は 4 となり、登録処理は 4 回発生することになる。登録処理が終わるたびに結果を確認し、規定回数の学習を終えた時点で終了とする。図 4.19 に登録結果ファイルモニタを示す。

①入力データファイルと登録セッション定義ファイルを WORK フォルダに作成する。
　一旦すべてのファイルを作成し、別名で保存する。使用する際にリネームして使用する。
②登録処理を行う実行ファイルを起動する
③登録結果ファイルの作成し、ファイルがあることを確認後、そのファイル内容を読み込む。
④登録処理が成功していれば、次の入力データファイルと定義ファイルを作成し、次の登録処理に進む。
⑤すべての登録署名データを学習したら、終了する。
⑥最後の登録結果ファイルの存在を確認したら結果の内容を確認し、その結果を表示する。

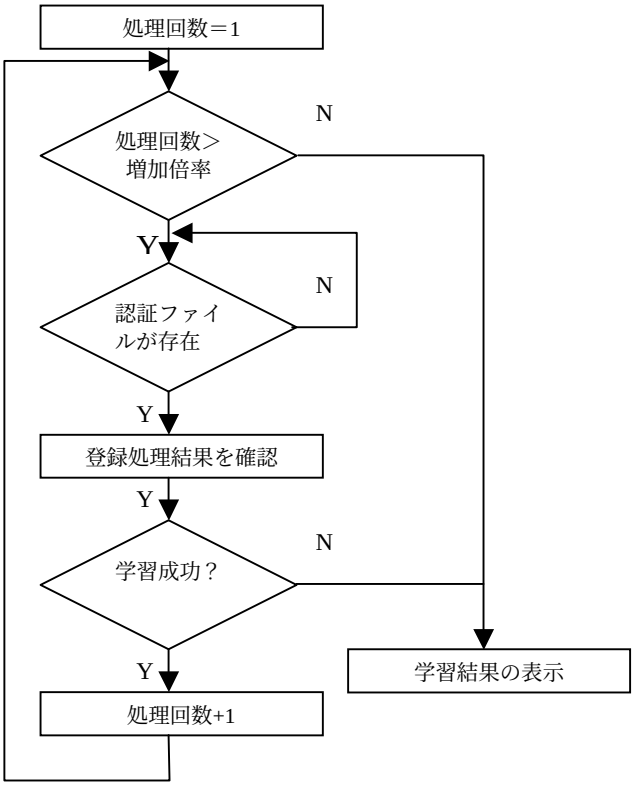



図 4.19　登録結果ファイルモニタ

## 4-2-9　登録結果表示

登録終了時と同様にニューラルネットワークが登録結果ファイルを作成する。

## 4-2-10　登録者データベースへの登録

登録処理が成功した場合にのみ、その登録者情報を登録者データベースに格納する。格納する情報は登録者 ID、登録者名、登録署名データ数、アクティブフラグの 4 つである。アクティブフラグは、その登録者が追加/更新登録、及び認証処理が許可されているかどうかを認識するためのフラグである。

# 4-3　認証処理の概要

## 4-3-1　認証処理

認証セッションは、提示用に登録した時と同様の署名を行い、登録されているデータとの照合により、本人かどうかの確認を行う。認証セッションでは、提示用署名データをニューラルネットワークモジュールに入力し、その出力によって判定を行う。以下、認証セッション時の概要を図 4.20 に示し、各処理について述べる。

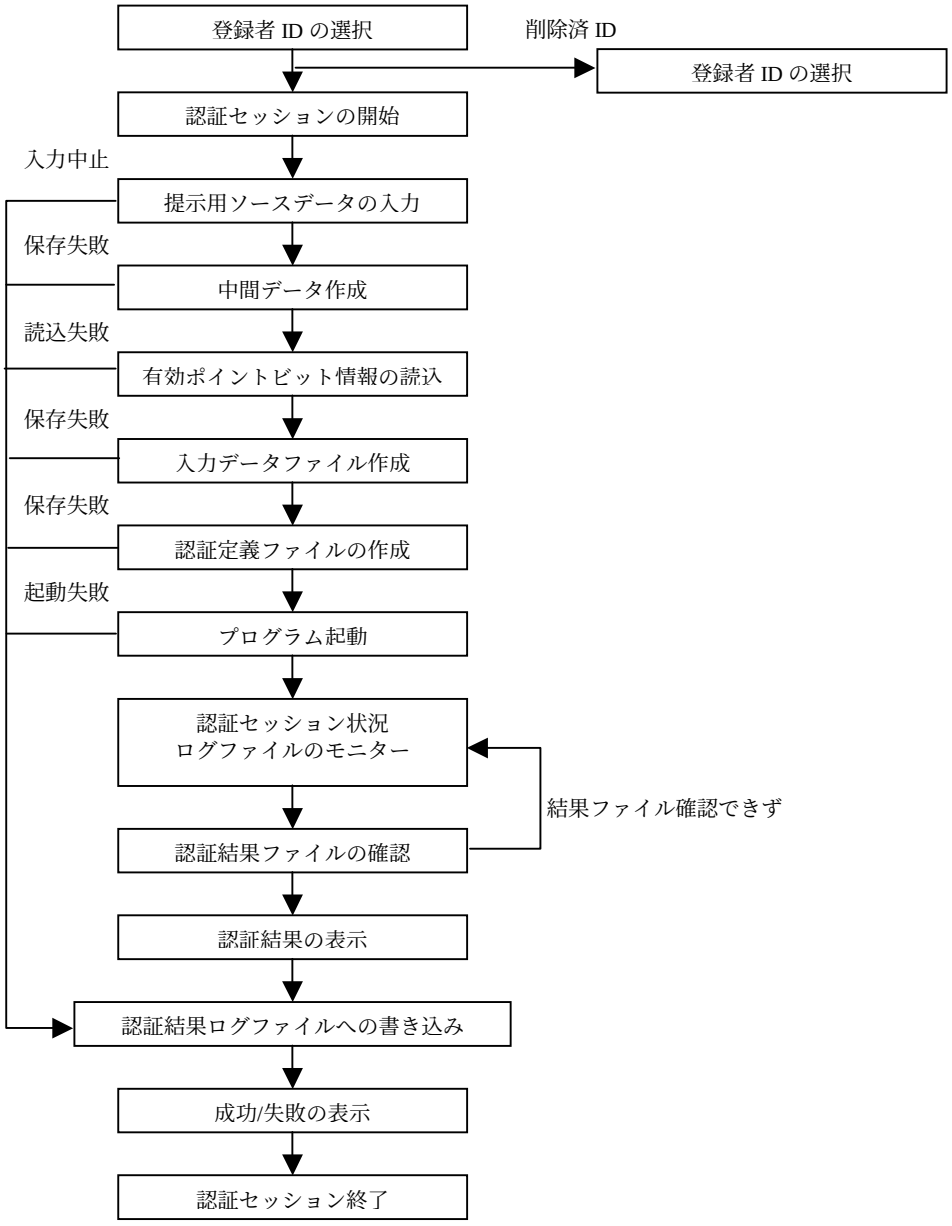



図 4.20　認証セッションの処理の流れ

## 4-3-2　登録者 ID、登録者名の選択

どの登録者として提示ソースデータ（以下、テストソースデータと表記）を入力するかを選択する。対象となる登録者 ID を選択しない限り次の処理へ進むことはできない。

## 4-3-3　テスト署名入力データの入力

提示用の署名は 1 回のみである。筆記を途中で失敗してもそのまま次の処理へ移行する。図 4.21 に登録ソースデータの入力を示す。電子ペンからの送信データが確認できない場合に限り入力中止となる。

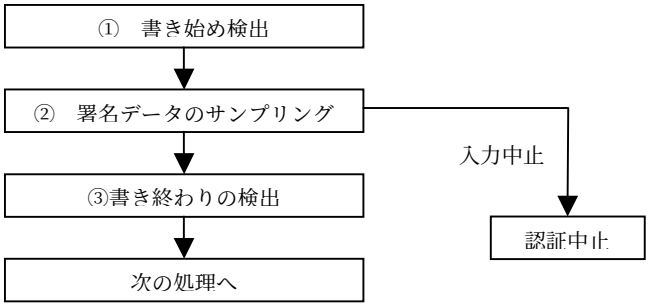



図 4.21　登録ソースデータの入力

## 4-3-4　中間データの作成

4-2-4 に述べた中間データと同じ処理で作成する。有効ポイントの読み込み対象となる登録者が、中間データ中において、どの要素を使用しているかを示す有効ポイント群データを読み込む。

## 4-3-5　入力データの作成

4-3-4 で作成した有効ポイント群と中間データを使用して入力データを作成する。有効ポイント群データにて、使用する事を示す「1」を持つ要素を抽出する。現在は 50 に設定する。WRITE.DAT というファイル名で WORK フォルダに保存される。
登録セッション時に作成されるデータと違う点は、保存されるデータは 1 個、登録者 ID が ”1001”、通し番号は「1」のみを使用の 3 つである。

## 4-3-6　認証セッション状況ログファイルモニタ

認証セッションは、認証対象となった登録者に対してのみ行われる。従って、認証結果ファイルの存在を確認し、認証結果ファイルの内容に従って結果を表示する。図 4.22 に認証結果ファイルモニターを示す。認証セッション時においては、ニューラルネットワークの出力値が認証結果となるため、進行状況を示すプログレスバーを表示する。

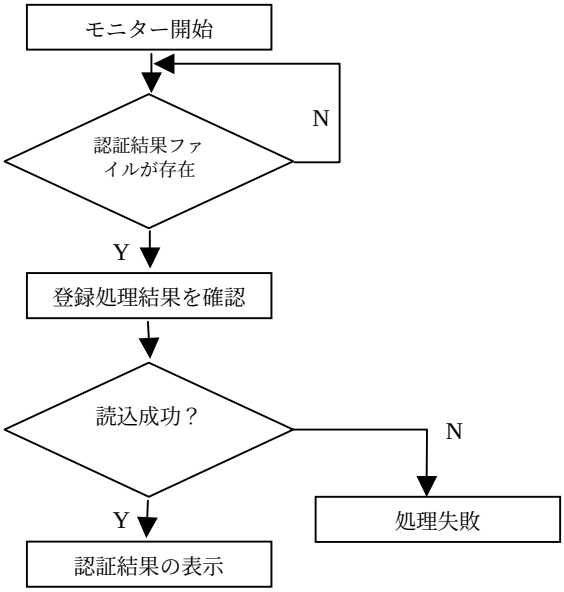



図 4.22　認証結果ファイルモニタ

### 4-3-7　認証結果の表示

認証終了時と同時にニューラルネットワークが認証結果ファイルを作成する。これを本アプリケーションが読み込む。結果ファイルの中には、認証定義ファイルに列挙された各候補者用のニューラルネットワークからの出力値を格納する。ニューラルネットワークには、1 つの値を出力する（出力層ユニット数：1）ものと、2 つの値を出力する（出力層ユニット数：2）のものがあり、本研究では 2 つの値を出力するニューラルネットワークを使用する。この 2 つの出力値をそれぞれ、OUT1,OUT2 とした場合、以下の条件を満たす候補者をテストソースデータの提示者本人とする。

$$(OUT1 > THREAD1) AND ((OUT1 - OUT2) > THREAD2) \quad (4.5)$$

THREAD1,THREAD2 は、認証における判定基準となる値で、設定ファイルから読み込む。ただし、対象者の登録用中間データの重心データと比較した場合の相関係数と距離値が、式（4.5）を満たさない場合は、本人以外となる。

## 4-4　個人認証システムにおけるニューラルネットワーク

### 4-4-1　ニューラルネットワーク選択機構

筆圧による個人認証システムにおけるニューラルネットワーク選択機構では、認証処理において駆動するニューラルネットワーク数をできるだけ少数に抑えることを目的とする。理由としては、各ニューラルネットワークの規模が小さくとも、登録者の増加に伴いニューラルネットワークの数が増加すれば、それに伴い動作に必要とされる時間を無視することはできないからである。

従来のニューラルネットワークのみの認証手法では困難である、認証パターンの増加と新規認証パターンの登録を実現するために、ニューラルネットワークとテンプレートマッチングを融合したものを使用する。基本的な構成は個々の認証パターン毎にテンプレートをニューラルネットワークによって作成し、本来線形処理であったテンプレートをニューラルネットワークとの融合により、非線形処理による判定を行うテンプレートによるマッチング処理を行うというものである。ニューラルネットワーク選択機構により駆動するニューラルネットワークを選択することで、不要なニューラルネットワークの駆動が抑制される。また、それによって学習時間の短縮化が期待できるとともに異常な入力が与えられた場合に、システムが異常動作し、誤った認証を行うという可能性の低減を図ることができる。テンプレートは学習データを用いることで作成され、学習データの追加毎に更新されるものとする。筆圧波形から画数及び筆記時間を求め、テンプレートに格納された画数及び筆記時間と比較することにより駆動するニューラルネットワークの決定を行っている。

### 4-4-2　ニューロテンプレートマッチング識別手法[3]

ここでは、本研究で用いた筆圧データによる個人認証用テンプレートマッチング識別手法について説明する。実際に筆記データを使用しての個人認証では、登録者数は多大な人数が必要となる。そこで、本研究で提案するニューラルネットワークによる識別手法は、ニューラルネットワークとテンプレートマッチングを融合させたニュー

ロテンプレートマッチング識別手法を用いる。この手法では、認証パターンの増加と新規認証パターンの登録を容易に実現することが可能である。その基本的な構成は、個々の認証パターン毎のテンプレートをニューラルネットワークで構成し、非線形テンプレートによるマッチング処理を行う。なお、各テンプレートに対応するニューラルネットワークは、目的とする認証パターン（目的パターン）と目的としない認証パターン（目的外パターン）の 2 つに分類する機能を有する。また、ニューラルネットワークの出力層の素子の構成法は 2 種類あり、1 つは、出力層は 1 つの素子を持ち、出力値がある設定したしきい値より大きければ目的データ、それより小さければ目的外データと判定する手法である（以下 NN1 と略記）。もう 1 つは、出力層の素子に目的素子と目的外素子の 2 つの素子を設定する方法である（以下 NN2 と略記）。

ニューラルネットワークでの学習を行うためには、教師される信号が 1 となる場合と、0 となる場合のそれぞれの入力が必要となる。この教師信号が 1 となる入力を強化データ、0 となる入力を抑制データとそれぞれ表記することにする。

## 4-4-3　NN1 の構成

NN1 の基本構成については図 4.23 で示す。NN1 の学習において、目的パターンに対して目的パターンを提示した場合は“ 1 ”と教師し、目的外パターンを提示した場合は“ 0 ”を教師する。認証結果の提示にはしきい値を設定し、そのしきい値を用いて目的パターンか目的外パターンかを判定する。

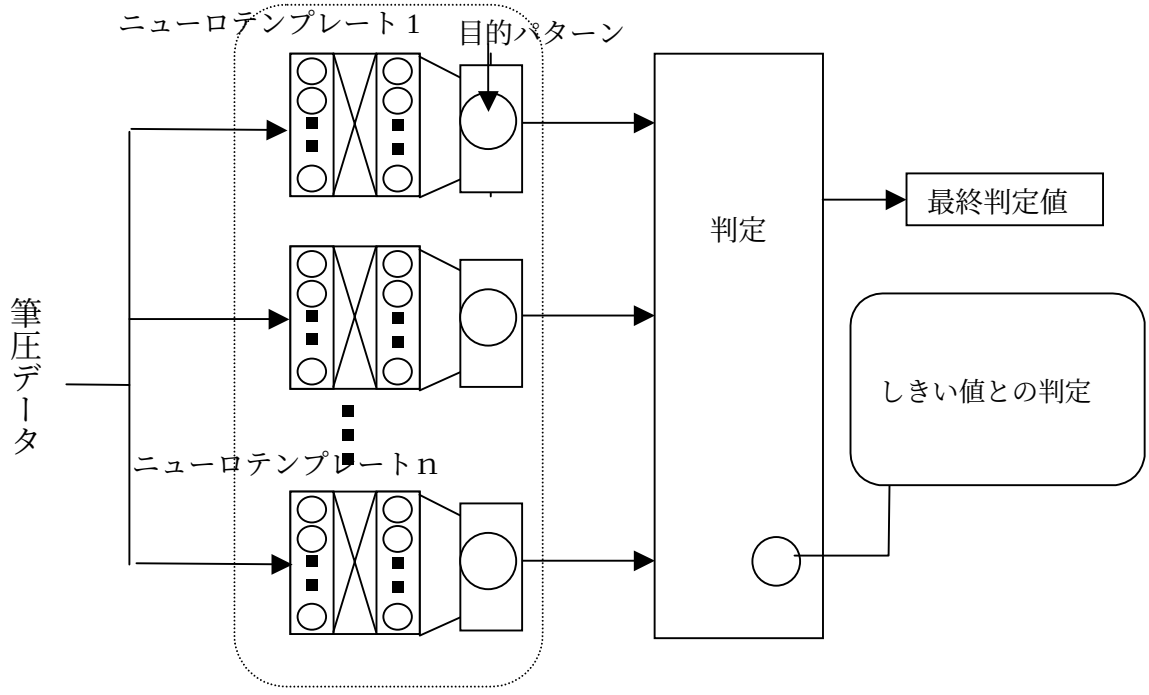



図 4.23　NN1 の構成図

## 4-4-4　NN2 の構成

筆圧による個人認証システムにおける登録処理中に使用するニューラルネットワークは、NN2 を使用する。出力層にある 2 つのユニットの 1 つは目的パターンの提示

に反応するユニットであり、もう 1 つは目的外のパターンに反応するものである。学習において、目的パターンのデータ（本人の筆記データ）を提示した場合には目的パターンに対応するユニットには“ 1 ”を、目的外に対応するユニットには“ 0 ”を教師する。目的外パターンのデータ（他人による偽筆等）の提示に対しては目的パターンユニットには“ 0 ”、目的外パターンユニットに“ 1 ”を教師する。

筆圧による個人認証で使用されている NN2 は入力層・中間層・出力層の 3 層からなり、各層の素子数を入力層が 50 個、中間層が 35 個、そして出力層が 2 個となる。図 4.24 に構成図を示す。

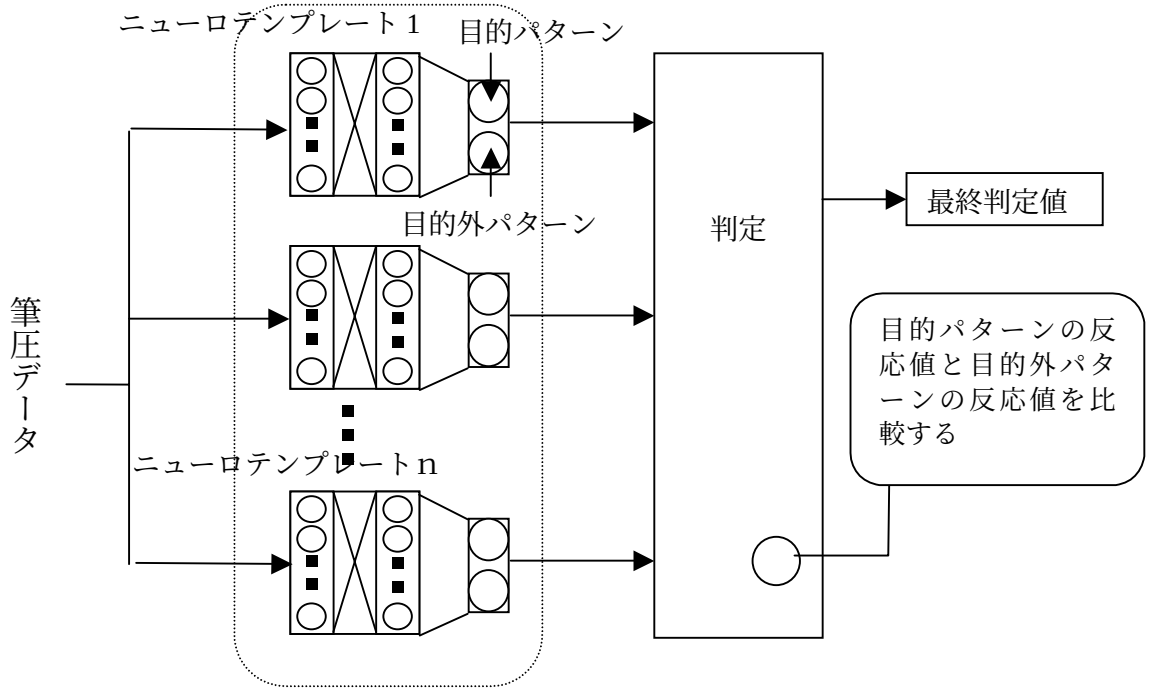



図 4.24　NN 2 の構成図

複数のテンプレートの結果から最終判定を得る手続きは以下の通りである。まず、目的パターンの出力ユニット値にしきい値を設定する。さらに、目的外パターンの出力ユニット値と目的パターンの出力ユニット値との差分にも別のしきい値を設定する。この 2 つのしきい値を満たしたすべてのニューロテンプレートからの出力ユニット値の最大値に対応するカテゴリを最終判定候補とする。この候補となる入力値を同じカテゴリの学習データから統計的に作成した上下限値で確認し、この上下限値の範囲内に入力値のすべてが収まっていれば、そのカテゴリを最終判定とする。

## 4-4-5　ニューラルネットワーク

筆圧認証システムで用いるテンプレートとなるニューラルネットワークは、図 4.25 に示すような 3 層の階層型ネットワークを使用する。各層の素子数は最大 50 個までとなる。図 4.2 では例として入力層、中間層、出力層の素子数（図 4.2 中の各層の“ ○ ”の数）がそれぞれ 5 個、3 個、4 個と示してあるが、本システムは、各素子数をそれぞれ 50 個、35 個、2 個で構成する。各素子は、それぞれ独立した層に配置している。各層の素子はそれよりひとつ前の層の素子から入力を受け、また、各層間ではすべて

の素子が結びついている。情報の流れる方向は、入力パターン（図 4.2 では 5 つの入力値）が入力層の各素子に与えられ、中間層で変換し、出力層の各素子から出力パターン（図 4.25 では 4 つの出力値）が得られる。

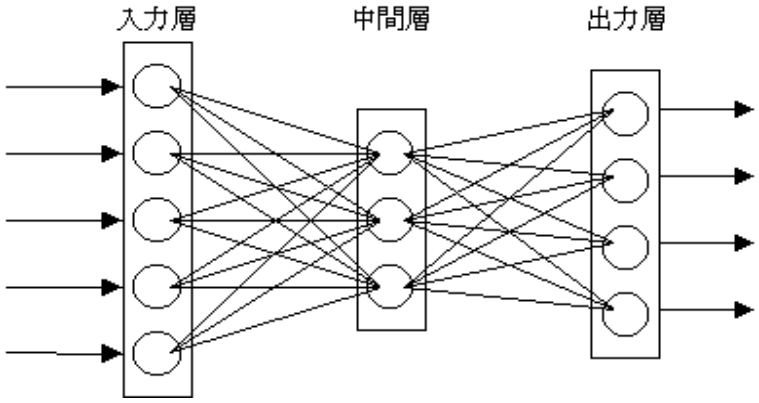



図 4.25　階層型のニューラルネットワークの例

## 4-4-6　学習

筆圧による個人認証システムでは、登録処理の中でニューラルネットワークを用いた学習を行う。このシステムでは登録対象のカテゴリ数と同数のニューラルネットワークを並列に配置したシステムを用いる。このシステム構成を図 4.26 に示す。図 4.26 では分類を行うカテゴリ数のニューラルネットワークと前処理機構としてニューラルネットワーク選択機構、そしてニューラルネットワークの出力値の比較部から構成される。登録処理において各筆記者には 1 個ずつのニューラルネットワークが対応し、ニューラルネットワークにはそれぞれ独立した ID を付与する。

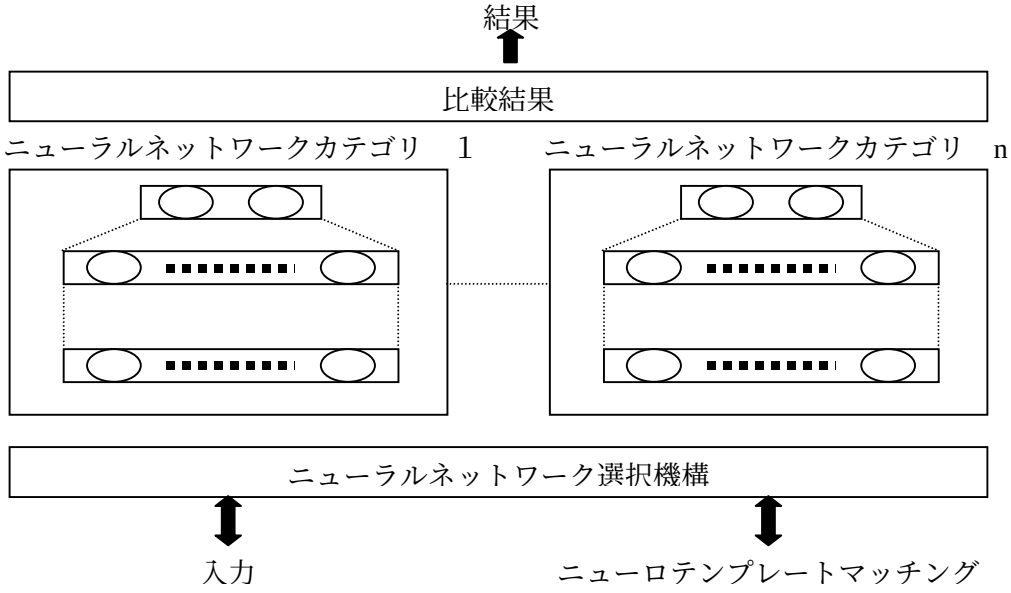



図 4.26　提案システムの構成

カテゴリごとにニューラルネットワークを独立させることによりそれぞれのニューラルネットワークの規模は小さくなるため、学習に用いられる時間は大きく短縮さ

れる。また、カテゴリ同士が独立したものであるため、新規にカテゴリ追加のために学習を行う場合にも、他の学習済みカテゴリの分類能力に影響をおよぼすことなく実行できる。

## 4-4-7　学習アルゴリズム

前項の情報の伝達において、入力層に与えられた入力パターンが中間層を経て変換され、出力層から出力パターンが得られることを示したが、入力パターンに対して期待する出力パターンを得るためには、各ユニット間の結合重み（ウェイト）を適切な値しなければならない。このウェイトを適切な値に設定にするために学習を行う。

学習方法としては、≪誤差逆伝搬（Error Back Propagation）アルゴリズム)≫を使用する。具体的には、いくつかの入力パターンの例（学習パターン）を与え、その時の出力パターンと期待する出力パターン（教師値）との誤差が減少するようにウェイトを修正する。ある入力パターンを与えた時、出力層の第 j ユニットの出力値を Oj、この時における出力層の第 j ユニットの期待値を Tj とすると、第 j ユニットの誤差 Ej は式(4.6)にて求められる。

$$E_j = \frac{1}{2}\left(T_j - O_j\right)^2 \tag{4.6}$$

したがって､1 つの学習パターンＰにおける出力層の誤差 Ep は式(4.7)にて求められる

$$E_j = \frac{1}{2}\sum_j \left(T_j - O_j\right)^2 \tag{4.7}$$

全学習パターンの誤差の総和を E とし、これを総合誤差と記述する式(4.8)。

$$E = \sum_p E_p = \frac{1}{2}\sum_p \sum_j \left(T_j - O_j\right)^2 \tag{4.8}$$

上記の総合誤差 E が最小になるように各ユニット間の結合重み（ウェイト）を修正する。修正の方法としては最急降下法を用いる。具体的には、それぞれの学習パターンごとに各ユニットの誤差 Ej が最小になる方向へ微妙な変更を加えていく。第ｔ回目の学習における、ｋ－1 層の第 I ユニットからｋ層の第 j ユニットへのウェイト Wij の修正量⊿Wij(k-1,k)(t)は式(4.9)にて求められる。

$$\Delta W_{ij}^{k-1,k}(t) = -\varepsilon\delta_j^k O_j^{k-1} + \alpha\Delta W_{ij}^{k-1,k}(t-1) + \beta\Delta W_{ij}^{k-1,k}(t-2) \tag{4.9}$$

上の式において、“ ε ”は学習定数、“ α ”は慣性定数、“ β ”は振動定数をあらわす。また、”δj(k)”はｋ層の第 j ユニットの一般化誤差で、ｋ層が出力層の場合と中間層の場合によって算出方法が異なる。式(4.10)、式(4.11)に一般化誤差の算出方法を示す。

k 層が出力層の場合、（Ij(k)は k 層の第 j ユニットの入力総和）

$$\delta_j^k = \left(T_j - O_j^k\right) f'\left(I_j^k\right) \tag{4.10}$$

k 層が中間層の場合、（ただし、m は出力層のユニット番号）

$$\delta_j^k = \left(\sum_m W_{jm}^{k,k-1}\delta_m^{k+1}\right) f'\left(I_j^k\right) \tag{4.11}$$

以上が誤差逆伝搬法によるウェイト修正の説明とする。
前項で記述したウェイトの修正式

$$\Delta W_{ij}^{k-1,k}(t) = -\varepsilon\delta_j^k O_j^{k-1} + \alpha\Delta W_{ij}^{k-1,k}(t-1) + \beta\Delta W_{ij}^{k-1,k}(t-2) \tag{4.12}$$

における、学習定数 ε、慣性定数 α、振動定数の β は環境設定ファイルで設定する。ε は大きな値にするとウェイトの修正量が大きくなり、学習は早くなるが、あまり大きくすると逆に学習が収束しなくなる。総合誤差が上下に振動するときは、学習定数を小さくし、誤差の減少速度が小さい時は学習定数を大きくする必要がある。この操作は学習プログラムが自動的に行う。ユーザは学習開始時の学習定数の初期値を設定する。初期値は（0.1< ε <1.0）の範囲で設定する。デフォルト値は 0.5 である。
慣性定数 α は総合誤差の振動を減らし、学習の収束を加速させる働きをする。振動定数 β は総合誤差を上下に振動させて極小値から脱出させる働きをする。α と β には関連性があり、以下の図 4.27 の範囲内（塗りつぶした部分）で設定する。慣性定数のデフォルト値は 0.95、振動定数のデフォルト値は - 0.1 である。

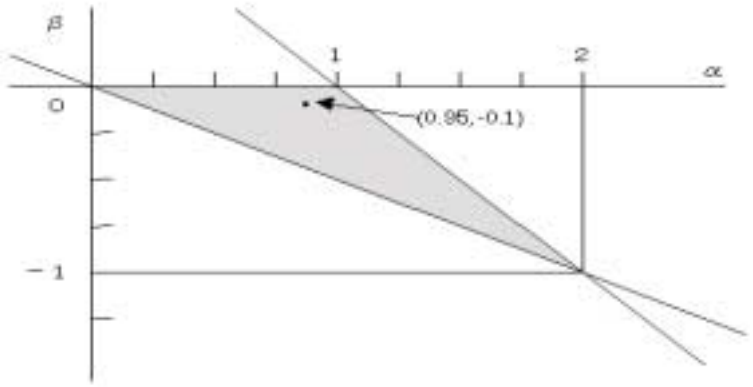



図 4.27　慣性定数と振動定数の範囲

## 4-4-8　入力層の入出力関数

本項では、ニューラルネットワークにおいて、入力層に与えられた入力パターンの伝達手段、出力層の出力方法について記述する。

図 4.28 において s1、s2、s3 はそれぞれの入力層の第 1，2，3 ユニット、a1，a2 はそれぞれ中間層の第 1，2 ユニット、 r 1，r2，r3 はそれぞれ出力層の第 1，2，3 ユニ

ットを表す。また、S1，S2，S3 は入力層への入力値（スラブ値)、R1，R2，R3 は出力層の出力値を表す。入力層の第 i ユニットから中間層の第 j ユニットへの結合の重み（ウェイト）を Wij とする。中間層と出力層の間の情報伝達方法もまったく同じであるので、入力層と中間層を例として説明する。

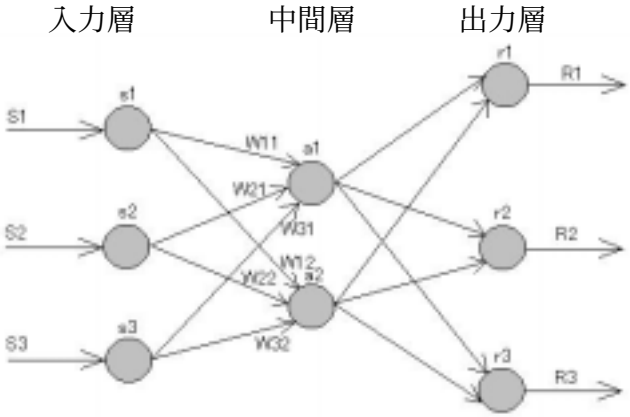



図 4.28　ニューラルネットワークの入出力

＜ユニットの入力値＞

入力層の第 i ユニットの出力値を Si とすると（入力層のユニットは入力値と出力値が同じ)、中間層における第 j ユニットの入力の総和 Ij は式(4.13)にて求められる。

$$\begin{aligned} I_1 &= W_{11}S_1 + W_{21}S_2 + W_{31}S_3 \\ I_2 &= W_{12}S_1 + W_{22}S_2 + W_{32}S_3 \end{aligned} \tag{4.13}$$

となり一般的に、

$$I_j = \sum_i W_{ij}S_i \tag{4.14}$$

と表すことができる。

＜ユニットの出力値＞

中間層における第 j ユニットの入力の総和を Ij とすると、中間層の第 j ユニットの出力値 Oj は式(4.15)にて求められる。

$$O_j = f(I_j) \tag{4.15}$$

(f は入出力関数)

このようにして、入力層の各ユニットの出力値と、入力層と中間層の各ユニット間のウェイトから中間層の各ユニットの出力値を得ることができる。同様にして、中間層の各ユニットの出力値と、中間層と出力層の各ユニット間のウェイトから出力層の各ユニットの出力値を得ることができる。

## 4-4-9　中間層･出力層の入出力関数

中間層と出力層の各ユニットの入出力関数として使用される、ロジスティック関数（シグモイド関数）を式(4.16)に示す。

$$f(x) = \frac{1}{1 + \exp\left(\frac{-x + \theta}{T}\right)} \tag{4.16}$$

式（4.4）において、ｘは各ユニットへの入力値で、f(x)はそのユニットの出力値である。Ｔはネットワークの温度と呼ばれる正の数で、Ｔが大きくなるほどグラフはなだらかなものとなる。θはユニット単位のしきい値である。図 4.29 にシグモイド関数のグラフを示す。このグラフでのしきい値θは０とする。Ｔは総合誤差に応じて、1.3 から 0.7 まで変化させる。この操作は学習プログラムが自動的に行う。

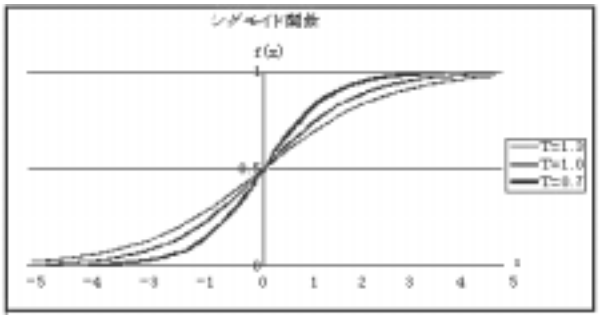



図 4.29　シグモイド関数

## 4-4-10　初期学習と継続学習

学習時には、初期学習か継続学習のどちらを行うかを選択することができる。初期学習では、最初に乱数を用いることでウェイト値の初期化を行う。それに対して継続学習では、既に存在しているウェイト値を初期値として使用する。継続学習は学習データを追加した時など現状のウェイトを利用時に実行する。

# 第５章　認証実験

現状の筆圧検出システムによって採取された筆記データを元に学習を行う。学習に用いられる抑制データの作成手法は、他人の登録署名データによって作成されるものを用いる。そして、抑制データを用いての学習を行った後に、認証実験を行い、その認証結果を示す。

## 5-1　実験手順

### 5-1-1　実験条件

認証実験は、以下に示すような条件下で行うものとする。

①実験対象データ

竹田研究室に所属する学生の内、任意に選定した 9 名から採取された本人署名データを使用する。採取されたデータ数は各人 81 個ずつ採取する名前はフルネームで書かれたものを使用する。

また、本人署名の他に、各人が自分以外の署名を単純に模倣した偽筆署名（9 個/人×9）を採取する。偽筆署名の内訳は、自分以外の 8 名に対し、1 人につき 9 個の偽筆を採取したということになる。

②筆記データ採取方法

電子ペンを用いて筆記データを採取する。筆記環境を同じにするため筆記者は椅子に座った状態で署名を行う。図 5.1 にデータの採取風景を示す。用紙は図 5.2 に示すような同じ大きさの記入枠が並んだ筆記データ採取シートを使用する。氏名は 1 つの枠に 1 回のみ記入する。図 5.3 に実際に記入枠に書かれた氏名と、それにより得られた筆圧波形を示す。なお、筆記者には、普段書き慣れた書き方での署名を心がけるようにする。

③登録署名データ数

最初に本人より採取された 9 個のソースデータの内、無作為に選んだ 3 個のデータを学習登録署名データとしてニューラルネットワークに入力し、学習を行う。残りの 6 個のデータは認証テストを行う際に、入力されるテストデータとする。

④筆記データ作成手法

採取されたソースデータをニューラルネットワークに入力できる状態にするため、筆圧波形筆圧軸に対し、筆圧値の最大値でデータを除算することにより、0.0~1.0 までの値に正規化を行う。

図 5.1　データの採取風景

筆圧波形データ採取シート　　月　日（　）　筆者コード　　筆者

朝

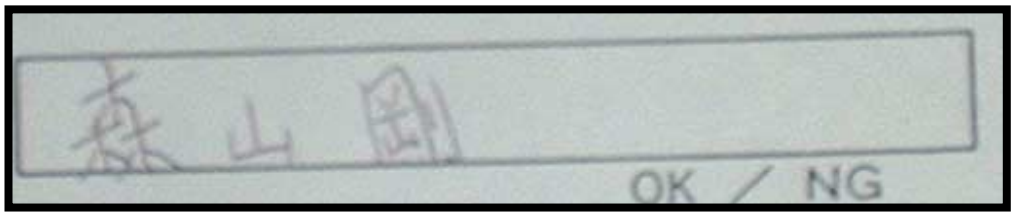
昼

夕

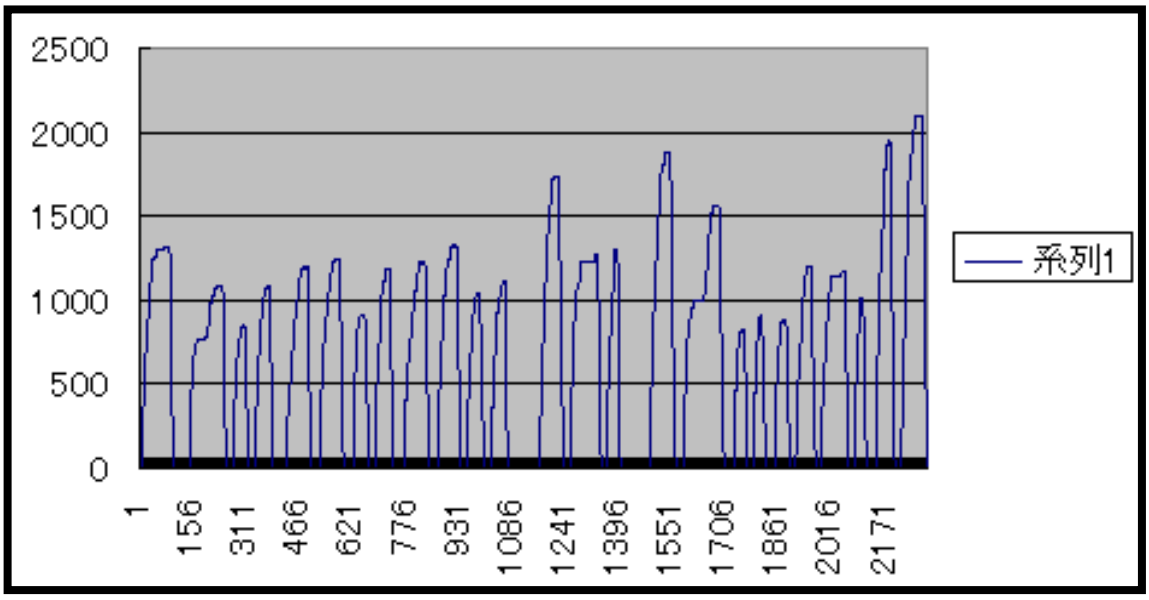
OK ／ NG

備考

図 5.2　署名データ採取シート




(a)




(b)

図 5.3　記入された実際の署名(a)と得られた筆圧波形(b)

⑤　学習方法

本人以外の 9 名の登録署名データ（計 81 個）を元に作成したものを抑制データとして使用し、学習を行う。

⑥　認証結果判定用しきい値

認証実験後、ニューラルネットワークからの出力値から本人か、そうでないかを OK/NG で判定するためのしきい値により判定を行う。しきい値は 0.4~0.9 までの範囲で、0.1 単位で増減させて検証を行う。OK か NG かの判定方法は、ある筆記者の署名データをニューラルネットワークに入力した場合、出力値 Out が、Out≧Th1（Th1 は判定用しきい値）を満たすとき、その筆記者は登録者本人であると判断するものとする。しきい値の値が大きいほど、ニューラルネットワークからの出力に対する判断が厳しいことになる。

## 5-1-2　実験結果表示内容

表 5.1　認証種類

| 認証種類 | 筆記者 | 筆記文字 | 判定結果 | 理想値 |
|---|---|---|---|---|
| 本人認証率 | A | A | A | 100.00% |
| 誤認証率 | A | B（A以外） | A | 0.00% |
| 偽筆誤認証率 | B（A以外） | A | A | 0.00% |

①　本人認証率とは A が A と書いて A と判定した割合である。本人認証率は、登録者本人の登録署名データによって学習を行ったニューラルネットワークに、登録者本人が筆記した署名を入力した結果、本人として受理された割合をパーセンテージで表したものである。値が高いほど登録者本人の署名データであるということになる。
②　誤認証率とは A が A 以外と書いて A と判定した割合である。上記と同様に、学習を行ったニューラルネットワークに、本人以外が署名した他筆署名を入力する。誤認率は、この他筆署名を登録者本人と誤って認識し、受理した割合を表したものである。値が低いほど登録者以外の署名データを棄却していることとなる。
③　偽筆誤認率とは A 以外が A と書いて A と判定した割合である。本人登録署名データによって学習されたニューラルネットワークに、登録者本人以外の 8 人が 9 個ずつ系 72 個登録者の氏名を簡単に模倣した署名（偽筆）を入力する。この入力データを登録者本人と判断し、受理された割合を示したものである。この値が大きいほど偽筆データを誤って受理していることになる。

## 5-2　実験結果

表 5.2 は上の表から、本人認証率、誤認証率、偽筆誤認率を表している。表中の TH は反応値を判定するしきい値を表しています。この反応値がしきい値以上である場合は本人、しきい値以下である場合は本人以外を表している。これまでの研究では抑制データの作成手法を偽筆によるものと、本人登録署名データから正規乱数によるものの、2 種類を用いて実験を行ったが、本研究では他人による偽筆をもとに抑制データを作成するものでの実験を行った。その結果、本人認証率では K06 においては理想値に近い 100%の結果が得られた。しかしながら、K07 においては理想値の 50%前後の結果であるため認識率がよいとはいえない。誤認証率では K06、K07、K08、K0a においては理想値に近い 0.0%という結果が得られた。また、偽筆誤認証率の結果についてはこれまでの実験よりも理想値に近いため良好な結果であるといえる。

表 5.2　実験結果（偽筆署名を抑制データとして使用した場合の本人認証率・誤認証率及び偽筆誤認証率）
登録者名：K05~K0b，TH：判定しきい値

本人認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 28 | 28 | 28 | 28 | 28 | 24 | 84.85% | 84.85% | 84.85% | 84.85% | 84.85% | 72.73% |
| K06 | 37 | 37 | 37 | 36 | 35 | 35 | 100.00% | 100.00% | 100.00% | 97.30% | 94.60% | 94.60% |
| K07 | 18 | 18 | 17 | 16 | 16 | 14 | 54.55% | 54.55% | 51.52% | 48.49% | 48.49% | 42.43% |
| K08 | 28 | 28 | 28 | 28 | 27 | 24 | 93.34% | 93.34% | 93.34% | 93.34% | 90.00% | 80.00% |
| K09 | 38 | 38 | 36 | 33 | 30 | 20 | 95.00% | 95.00% | 90.00% | 82.50% | 75.00% | 50.00% |
| K0a | 28 | 28 | 27 | 27 | 26 | 22 | 82.36% | 82.36% | 79.42% | 79.42% | 76.48% | 64.71% |
| K0b | 25 | 25 | 21 | 20 | 19 | 15 | 75.76% | 75.76% | 63.64% | 60.61% | 57.58% | 45.46% |
| 計 | 202 | 202 | 194 | 188 | 181 | 154 | 84.17% | 84.17% | 80.83% | 78.33% | 75.42% | 64.17% |

誤認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 4 | 4 | 3 | 2 | 1 | 1 | 1.94% | 1.94% | 1.45% | 0.97% | 0.49% | 0.49% |
| K06 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K07 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K08 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K09 | 7 | 7 | 6 | 5 | 3 | 3 | 3.50% | 3.50% | 3.00% | 2.50% | 1.50% | 1.50% |
| K0a | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K0b | 9 | 9 | 7 | 4 | 2 | 1 | 4.35% | 4.35% | 3.39% | 1.94% | 0.97% | 0.49% |
| 計 | 20 | 20 | 16 | 11 | 6 | 5 | 1.39% | 1.39% | 1.11% | 0.76% | 0.42% | 0.35% |

偽筆誤認証率

| TH | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K05 | 8 | 8 | 7 | 6 | 4 | 3 | 14.81% | 14.81% | 12.96% | 11.11% | 7.41% | 5.56% |
| K06 | 8 | 8 | 5 | 3 | 3 | 2 | 14.81% | 14.81% | 9.26% | 5.56% | 5.56% | 3.37% |
| K07 | 9 | 9 | 8 | 6 | 5 | 4 | 16.67% | 16.67% | 14.81% | 11.11% | 9.26% | 7.41% |
| K08 | 26 | 26 | 25 | 23 | 20 | 15 | 48.15% | 48.15% | 46.30% | 42.59% | 37.04% | 27.78% |
| K09 | 8 | 8 | 6 | 5 | 5 | 5 | 15.38% | 15.38% | 11.54% | 9.62% | 9.62% | 9.62% |
| K0a | 0 | 0 | 0 | 0 | 0 | 0 | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% |
| K0b | 1 | 1 | 0 | 0 | 0 | 0 | 1.92% | 1.92% | 0.00% | 0.00% | 0.00% | 0.00% |
| 計 | 60 | 60 | 51 | 43 | 37 | 29 | 16.04% | 16.04% | 13.64% | 11.50% | 9.89% | 7.75% |

## 5-3　考察

これまでの研究と本研究を比較すると偽筆誤認証率を低下させることができた。しかし、本人認証率が低下した結果となった。これは登録時における入力データの追加により偽筆誤認証率を低下させることができた。これまでの研究では筆圧データの移動平均を使用していたが、本研究では移動平均に加えパターン間の相関係数、統計的距離のパターン間の分離情報を追加することにより偽筆誤認証率を低下させることができた。これまでの研究では抑制データの作成手法が 2 種類あり、偽筆署名データからと正規乱数によるものの 2 種類あったが、本研究では偽筆署名データからのみに設定し、認証を行った。これまでの研究の実験結果と本研究の実験結果を比較する。本研究と同じように偽筆による抑制データ作成手法での比較を行う。比較のために用いる表は表 2.1 と表 5.2 である。本人認証率、誤認証率、偽筆誤認証率の 3 項目について比較を行う。

本人認証率においてはこれまでの研究では 90.71%、本研究では 84.17%と低下した結果となった。筆圧データの違いもあるが、95.00%以上の認証制度を向上させる必要があると考えられる。

誤認証率においてはこれまでの研究では 0.54%、本研究では 1.39%と低下した結果となった。筆圧データの違いもあるが、認証率が低下しているため認証精度を向上させる必要があると考えられる。

偽筆誤認証率においてはこれまでの研究と比較し、大幅に認証制度を向上させることができた。これは本項の最初にも述べたがパターン間の分離情報を追加することにより認証制度を向上させることができた。

筆圧による個人認証において筆記者が自分の署名を書き慣れていて、特徴がある筆記者がそれぞれの認証について認証精度がよいと考えられる。偽筆誤認証についても筆記者本人と本人以外であれば筆圧、筆記スピードはそれぞれ異なり判定結果が明白であると考えられる。そこで本人署名と偽筆署名との 2 つの筆圧波形を示す。筆記文字は著者である「森山剛」と筆記を行う。本人の筆圧波形と本人以外が模倣した筆圧波形を示す。図 5.4 が本人の署名を行った際に検出された筆圧波形を示している。また、図 5.5 は本人以外が模倣をして署名を行った際に検出された筆圧波形を示している。同じ文字を筆記しているのにもかかわらず波形が違うことがわかる。このことから、偽筆署名のように模倣を行い「なりすまし」をするということは難しいと考えられる。

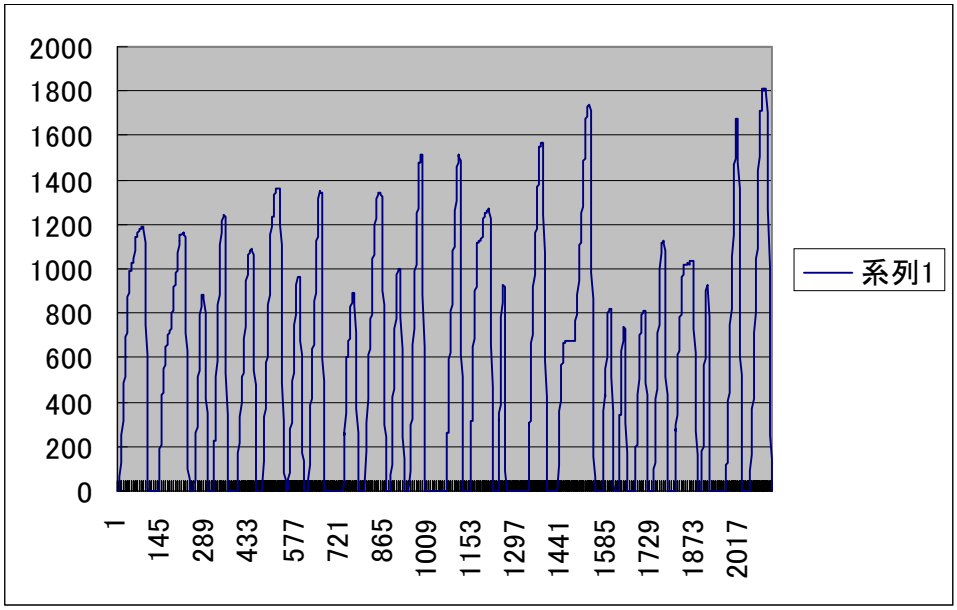



図 5.4　本人署名の筆圧波形

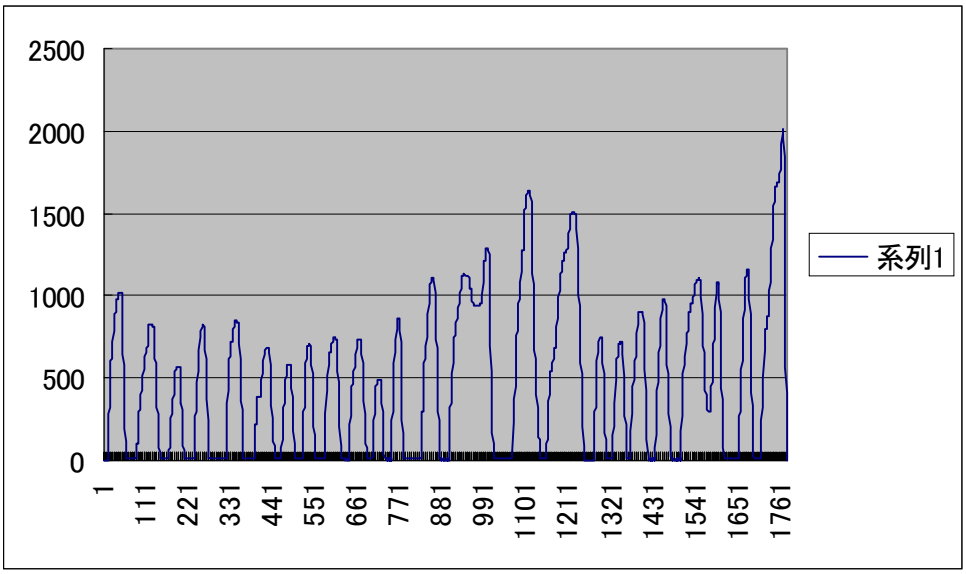



図 5.5　偽筆署名の筆圧波形

# 第６章　まとめ

本研究では筆圧により個人認証システムの開発を行うことを目的とし研究を行った。

これまでの研究での問題点である、偽筆誤認証を抑えるために処理の改善案を提案した。改善点は登録時の入力データの入力値としてこれまでの研究でははは筆圧データの移動平均を用いていたが、本研究では移動平均に加え、パターン間の相関係数、統計的距離のパターン間の分離情報を追加することにより、偽筆誤認率についてこれまで以上の結果をえられた。

今後の課題としては登録署名データ数が大幅に増加した場合、本人認証率が低下してしまうため、改善を行う必要がある。

# 第 7 章　謝辞

1 年半にわたり、御指導いただきました竹田史章教授に深く感謝いたします。本研究を進めるにあたり、研究用資料の提供および貴重な助言を賜りました日本システム開発株式会社仁木章人様ならびに、実験データ採取に協力していただいた、高知工科大学工学部情報システム工学科竹田研究室所属の学生一同に感謝いたします。

# 第８章　参考文献


[1]　「HITACHI」、http://www.hitachi.co.jp/Prod/comp/ic-card/outline/certification.htm

[2]　佐伯久弥、“ ニューロボードを用いた掌紋による個人認証に関する研究 ”、平成 12 年度高知工科大学学士学位論文、2001

[3]　竹田史章、西陰紀洋、“ 紙幣用ニューロテンプレートマッチング識別手法の開発 ”、電学論Ｃ、121 巻 1 号、2001

[4]　長尾　崇、“ 電子ペンによる個人認証システムにおける前処理の改善に関する研究 ”、平成 12 年度高知工科大学学士学位論文、2001

[5]　森山　剛、竹田史章、“ 電子ペンによる個人認証システムにおける前処理 ”、高速信号処理応用技術学会、春季研究会論文集、pp.124-125、2001

[6]　森山　剛、竹田史章、“ 電子ペンによる個人認証システムにおける前処理の改善 ”、システム制御情報学会論文集、pp.111-112、2001