高知大学大学院理学研究科

数理情報科学専攻情報科学講座

2008年度修士論文要旨

擬似乱数と物理乱数の比較研究

数理情報科学専攻　情報科学講座　　赤　松　将　之

本研究では、擬似乱数で主に使用されている線形合同法の周期性の問題をランダムウォークにより視覚的に明らかにし、RandomStreamer という装置から生成する物理乱数との比較研究を行い、Java 言語環境での物理乱数の使用法を開発した。

シミュレーションや暗号、ゲームといった様々なところで乱数（random number）が取り扱われている。しかし、現在使われている乱数の殆どが擬似乱数を使用していて、規則的であり、周期も存在する。特に一般的に使用されている線形合同法では周期性の問題が大きいとされる。ときに、シミュレーションでは大量の乱数が必要な時や、暗号では推測される可能性があり、擬似乱数では不適当な場合がある。一方で物理乱数と呼ばれる一定のアルゴリズムによって生成されない乱数がある。この物理乱数の発生装置が最近では、比較的に安価で手に入るようになってきた。しかし、まだ物理乱数の使用頻度は低い。それは、擬似乱数の危険性を十分に認識しておらず、また物理乱数の簡便な使用法が確立されていないことが考えられる。

そこで、本研究では、擬似乱数に周期がある欠点を明らかにし、真の乱数（真性乱数）である物理乱数と比較する。擬似乱数は、主に使用されている線形合同法により生成する。物理乱数は熱雑音より生成する RandomStreamer と呼ばれる装置を使用する。この装置は Windows 用ドライバが付属しているが Java 言語には対応していないので、Java の JNI（Java Native Interface）という機能を用いて C++ 言語を介して使用できるようにした。RandomStreamer の物理乱数の生成速度は 1 MByte/sec である。しかし、1 回の通信で６５５３６ Byte しか使用できず、通信速度に時間がかかるために、生成された物理乱数を十分に使いきれていなかった。そこで、Java でスレッドを立ち上げて一方で乱数の取得を行い、一方で乱数を使用するといったアルゴリズムにすることによって、使用する速度の改善を行うことができた。

比較には擬似乱数の欠点を視覚的に捉えるためにランダムウォークを作成した。また、数値的にも比較できるように分散、出発点に戻る回数も計測しグラフ化した。これによって、擬似乱数の周期があるという欠点を視覚的に、また数値的にも明らかにすることができた。一方の物理乱数は、擬似乱数で見られた欠点はなく、速度も擬似乱数とほとんど変わらない程度で使うことができた。

QR コードと携帯電話を活用した大学教育支援システム

数理情報科学専攻　情報科学講座　　石川　善幸

大学教育においては単位制をとっているため、学期当初において履修登録を行う必要がある。近年、大学教育の質が問われるようになって授業時間の確保が厳密にチェックされるため、迅速な履修登録の完了が要求されるようになってきている。高知大学では現在、履修登録を行うにあたって、OCR シート提出という手段をとっているが、毎学期の履修登録期間には窓口が非常に混雑しており、そのため登録ミスも頻繁に発生している。窓口混雑の問題を解決するには、履修登録のオンライン化が必要であるが、PC インターネットの利用についてはいくつかの問題が予想される。つまり、学内のネットワーク接続環境が限られているため、全員が短期間に集中して利用することが難しいこと、また授業コードの入力ミスなどによる登録ミスの発生などである。

授業コードの問題については、吉田が 2006 年度卒業研究の「ネットワークを利用した大学教育支援システム (2) — 履修登録支援システム — 」において、ショッピングカートモデルを用いたシステムを提案し一定の進展が見られたが、多数の学生が短期間に同時にネットワークを利用できるかどうかについては問題が残されていた。

本研究では、PC よりも持ち運びが便利で、学生の間にも普及している携帯電話を用いることによって、短期間に集中する履修登録アクセスの問題を解決できないかを検討した。携帯電話によるウェブページへのアクセスについては、携帯キャリアによって一意的に決められている「個体識別番号」が付加されるため、一度ユーザ ID とパスワードで認証できれば、以後の認証を省略しても個人を特定することが可能である。但し、識別番号の形式はキャリアによって異なるため、その取得と利用には、個別に対応する必要がある。

また、携帯電話のキーからでは、授業コードの入力が難しく入力ミスが予想される。この問題については、最近広く利用されている QR コードを利用することが考えられる。QR コードは、1994 年に株式会社デンソーによって開発された 2 次元コードであり、1999 年に JIS X 0510 として標準化されている。21x21 から 177x177 までの白黒のマトリックスによって情報を表現するが、位置検出パターンや誤り訂正符号を利用することによって高い信頼性を持つことが特長である。また、現在利用されているほとんどの携帯電話が、カメラ付きで QR コード読み取りに対応している。

本研究では、以上のような考察に基き、識別番号を用いた認証と QR コードを利用したオンライン履修登録システムを試作した。QR コードの作成については、Web サービスとして、あるいはフリーソフトが出ているが、多くは GUI を用いるものであるため、数 100 におよぶ授業科目について個々にキーボードから入力するのは非現実的である。このため、プログラム言語 Python を用いて QR コードを作成できるようなライブラリを構築した。以上の研究を通じて、携帯電話を活用した履修登録システムの開発に展望を開くことができた。今後、さらに総合的な大学教育支援システムへの、モバイル環境の応用も展望することができるものと思われる。

手話入力装置の開発

数理情報科学専攻　情報科学講座　　氏名　牛田吉章

近年では聴覚障害者とのコミュニケーションを円滑にするために，手の動きを読み取り言葉に変換するための手話変換システムの研究が進められている．手話変換システムに利用される手の動作を読み取る装置はカメラで手を撮影し，画像処理やモーションキャプチャ等で手の動きを読み取る手法と，手袋状になっていて各関節部分などに直接取り付けられた曲げ抵抗等から情報を取得し手の状態を読み取る手法の２つに大きく分類され，これらを総称してデータグローブと呼ぶ．現在は手話の入力，人間の手の動きを３次元空間での表現，またロボットの遠隔操作などの研究が進められている．

前節で述べたように，前者であるカメラを用いる装置では複数のカメラを用い別々のアングルから撮影することで比較的容易に３次元での情報取得が可能となるが，それなりのスペースが必要となるため一定の場所に固定する場合には有効的であるかもしれないが持ち運びには適さないと考えた．後者は手に装着するデバイスのみで構成することが可能で，設置スペースを必要とせず容易に持ち運ぶことができるが，曲げ抵抗等を利用した装置では指の状態を伸びているのか曲がっているのかの状態しか読み取れないので，３次元的な手の動きや流れを取得することがやや難しい．しかし「手話」は手の静止状態だけでなく，その前後の動作も含めて言葉を表現する言語であるので３次元での情報取得が必要不可欠であると考えられる．よって各指や手の状態だけでなく，手全体の動きや流れの情報も取得することを目標とし，本研究では加速度センサに注目し，データグローブの製作を行った．また本研究は動きや流れを取得するための初期段階と位置付けし，まず静止状態での情報取得を試みることにした．

本研究の実験では静止状態に限定された日本語の「指文字」40音のそれぞれに特徴を見出すことができ，この特徴を用いて「指文字」を区別し，認識できることを確認した．「指文字」の認識まで可能となったので，今後は手の動きや流れを読み取り，「手話」の認識へと進めてゆく予定である．動作を取得する際に各センサの変化を随時読み込むのか，それとも一定の間隔でサンプリングするのか，それからどのように変化の流れを抽出するかが重要であると考えられる．また，静止状態の「指文字」に限定しているために照合するためのデータベースが小さく済ませることができたが，動作を含めたデータとなると１動作あたりのデータの大きさも比較にならないほど大きなものになってしまい，照合するためのデータベースもおのずと大きなものになってしまうと考えられる．このためデータベースの作成や，動作をどのように照合するのかが当面の課題点である．

高性能ＳｏＣを目指したクロックツリー規模改善法の研究

数理情報科学専攻　情報科学講座　　海老江　光

情報化社会を支えるコンピュータの基幹部品であるＬＳＩは，大規模化と高速化を求められ微細化が進められてきた．近年のＬＳＩは，システム全体を１チップにまとめたＳｏＣへと進化しており，素子数も飛躍的に増大している．一方，ＬＳＩの微細化・高速化が進むにつれ，設計面で新たな問題を生む．ＬＳＩのクロック回路設計の微細化問題もその一つである．クロックは，ディジタル回路のタイミング調整のための周期的信号である．

ＬＳＩの高速化は，クロック周波数を高めることで実現する．しかしクロック周波数を高めると，クロックの消費電力を大きくしてしまう．現在，クロック回路による電力消費は全体の40％近くといわれており，消費電力面で深刻な問題となる．また，膨大な電力消費は，ノイズの原因ともなる．高性能で低消費電力の回路設計には，クロック回路規模の削減が必要である．

クロック回路の規模は，クロックを供給する配線本数と信号を伝えるトランジスタ素子数の総和で決まる．従来のクロック回路の構成は，２分木構成が中心であった．クロック信号の供給先の素子をペアにして分岐点からの均等距離の実現が容易なためである．ｎ分木であれば２分木に比べ，階層数や分岐数でより小さくすることができる．しかし，ｎ分木では厳密な均等距離となる分木点の算出法や，構成法がないため，いままで研究されてこなかった．

本論文で，著者は，より小規模なクロック回路をつくるｎ分木クロックツリー構成に注目し，その構成方法を提案する．ｎ分木における最適な数ｎを，各分岐数の階層数，分岐点数をプログラムの実装により比べ追及する．さらに，ｎ分木のゼロスキューを可能にするための均等距離点（分岐点）の算出の可能性の研究について述べ，最後に具体的な均等距離点構成アルゴリズムを提案する．本研究から，ｎ分木のｎとして３が，各ｎ分木の階層数，分岐点数より格段に削減が可能で大幅な総配線長の削減が可能であることを示す．さらに，３端子において，均等距離点を高い確率で決定可能であること，また，提案アルゴリズムが，同均等距離点を効率よく求めることができることを示す．

タッチパッドを利用した個人認証について

数理情報科学専攻　情報科学講座　　栗田　了輔

現在のセキュリティ技術にはさまざまなものがある．個人認証の分野では，暗証番号などを用いた最も基本的な認証方法から，指紋や顔，静脈などといった本人しか持ち得ない情報であるバイオメトリクス認証（生体認証）などがある．

バイオメトリクス認証には指紋や静脈などの身体的特徴，声紋や署名などの行動的特徴があり，これらの特徴を用いて本人確認を行う認証方式のことである．比較的利用しやすい指紋や静脈を利用する身体的特徴を用いた研究が進んでいるのに対して行動的特徴を用いた認証は製品としての開発が困難であり，最大の欠点として体調の変化によって特徴が異なることである．

しかし身体的特徴に比べ，行動的特徴を用いるメリットとしては本人の意識や意思が確かな時にしか認証ができないことである．例えば，指紋認証を行う時に，本人を眠らせて他人が認証を行ったり，認証する部分を切断するというような危険性も高く，一度認証されると，基本的には，その後は本人であることを確認することは行われない．この方法では何らかの手段で認証された場合，他人が本人となりすましてしようすることが可能となる．

この問題に対して，認証後も引き続きユーザを常時監視する「追認証」という方法を行うことによって，セキュリティを高めることが可能である．また追認証は本人が無意識のうちに認証が行われ，ユーザに負荷がかからないというメリットもある．当研究室ではこれまでマウスの操作やキー入力を用いた追認証が先行研究として行われてきた．

本研究ではタッチパッドの操作における指の動作に注目し様々な情報を得られることがわかった．タッチパッドをタップしたり，滑らせたりしたときには，指の圧力または面積，タッチパッドに触れた場所，触れていた時間などである．

それらの中から今回はタッチパッドを操作する時の“速さ”に着目し，そこから得られる情報を元に分析した．例えば，ある点から次の点へのカーソル移動動作においては，速度情報に関してだけでも一定の早さで目的の場所に移動する人や一気に目的の場所周辺に近づけ，徐々に調節する人，また滑らせる回数が多い，少ない，タッチパッドに触れている時間などに特徴がみられた．これらのデータからどれくらいの精度で本人認証が可能かを，無作為に選んだ30人を対象に検証を行い，比較的高い精度で本人確認が可能であることがわかった．しかし対象人数をより多くした場合，この手法だけでは限界があることも予想される，特定マシンにおける個人認証という観点では，ある程の有効性は確認できるが，その限界と今後の発展性についての考察も行った．

ロボットのバランス制御に関する研究

数理情報科学専攻　情報科学講座　　島村　圭

現在，ロボットに関する技術は，社会ニーズにより従来ロボットが活躍していた産業から，医療・福祉，日常生活支援などの非産業分野に展開している．そしてロボットに複雑な動作を行わせるには，ロボット本体の姿勢制御技術が重要な要素となっている．
人間の場合, 動作は感覚的に行いきわめて質のいいバランス動作を実現している. これは，複合動作であり，常に適切な動作を複数選択し組み合わせることで動作を行い，様々な状況・環境への対応をしている．しかし，ロボットの場合はセンサを用いてバランス制御を行わないといけない．ロボットにとってのセンサは人間の五感に相当するもので，ロボット制御全体で大きな役割を果たしている．そこで，本研究ではロボットのバランス制御センサとして一般的な，加速度センサとジャイロセンサを比較し，センサと制御の関係を調べ，より安定したバランス制御の検討を目的とした．
それにより，医療・福祉・介護などの日常生活支援ロボットへの応用が期待できる．

本研究室ではバランス制御を倒立振子装置の観点から考えています．
倒立振子には振り上げ式・自走式・自立式など多くの種類があり，本研究室の先行研究では自走式の倒立振子装置を製作し実験を行っている．
装置の主要部分は加速度センサ・ジャイロセンサ・ロータリエンコーダ，出力としてモータ・ギヤを使用，CPU には H8-3069 を使用した．

先行研究では加速度センサの情報のみを利用して実験を行っていたが，加速度センサ・ジャイロセンサを組み合わすことで正確な姿勢情報の取得が可能となる．
制御プログラムは先行研究と同じくファジィ推論により算出した LUT 方式の制御を使用した．LUT の作成には FDL を用いたファジィ推論演算プログラムを用いて行った．

結果として，以前の制御より改善が確認することができたが，今後も改善する点が明らかとなった．
今回はハードウェア・制御プログラム共に改善し実験を行ったが軽量化・プログラムの効率化をし，より強いバランス制御を行えるようにしたい．

配線長推定法とレイアウトブラウザの研究

数理情報科学専攻　情報科学講座　　張　帆

最先端の電子･情報処理機器にVLSIが多数搭載されるようになったが、微細加工技術の進歩によりVLSIの1チップに搭載できる素子数は飛躍的に増大し，性能向上も進められている．

一方，微細化によって，設計の質的課題，量的課題が生じている．設計の質的課題としては,信号処理のタイミングや高性能の保障の問題,また，設計の量的課題としては，設計効率の改善などが挙げられる．

設計の量的課題は，微細化により1チップに搭載される機能や素子数が増大したことが原因で，より抽象度の高い機能設計やRTL設計等の上流DA研究により設計効率の改善することで解決されてきた．しかし，質的課題は，微細加工により配線抵抗，配線間近接にともなうクロストーク，歩留まり等の問題が顕著化してきたことが原因であり，物理設計の詳細に関わるため，高度な抽象化が困難となり設計の終段階まで判明しない．そのため，タイミング問題などが判明した場合には，再度，上流設計に戻って修正するなどの問題が残ってしまう．

そこで，著者は，設計において重要な項目となるタイミングについて，特に配線遅延を見積もるための配線長推定手法の研究と高速なレイアウト設計(配置・配線)を開発するための環境となる物理設計ブラウザの開発の研究を行った．

著者の提案する配線長推定法は，ネット端子の配置位置の広がりの中心位置を原点とした，4象限分布としての場合分けして推定する．端子が3つ以下の象限に分布される場合，半周囲長で配線長を推定し，端子が3つ以上の象限に分布される場合は半周囲長をL1とする，半周囲矩形内部の同矩形の辺から残りの端子を矩形までの距離をそれぞれX方向とY方向に最短距離で結んだ長さの最小をL2とし，これら2つの配線長L1とL2の総和を推定配線長とする．

提案する配線推定法は従来のネット端子の配置位置の広がりの半周囲長推定に比べて,より実際の配線長に近い推定方法を提供することができる．

配置、配線手法の検証環境の開発として，豊永研究室で統合されているYAT形式で出力された配置配線データを読み込み，高速に表示するブラウザ(YatViewII)をVisualBasic2008で開発を行った．YatViewIIは，セルの物理形状，端子位置，配線層，接続情報を様々な切り替えにより表示する機能を持たせた.微細な状況から全体の概観まで,図サイズの拡大と縮小や，多層配線で用いるレイヤの表示色の指定や変更などの機能を持たせた。統計情報として，セル数，ネット数，ビア数なども表示する．特記すべき機能として，著者が開発した配線長推定等の見積もり機能も持たせた．

以上の研究により，まず，配線推定法として，ベンチマーク回路等から精度高い配線長推定ができることが確認された．また，配置配線環境として，接続数が一万を超える配線表示や，約十万素子程度の大量な配置情報を比較的高速に表示可能なブラウザを提供できることが判明した．

本研究により配線推定の高精度化と配置・配線機能の確認の容易化を確立することができた．

自律型ロボットの移動経路の改善

数理情報科学専攻　情報科学講座　西野圭一郎

卒業論文では自律型ロボットの移動経路の改善について、２つの凸包アルゴリズムをベースとした改善案を提案した。修士論文では、それらのアルゴリズムがそれぞれどの程度の成果を得ていたのかを実際に検証し評価すること、そして十分な成果が得られていない場合はより改善できる手法を提案することを目標として研究を行う。

卒業論文において基礎としていた自律型ロボットの移動計画問題の概要は以下のようなものである。まず、ロボットの動作を限界長方形のなかに制限する。そして障害物が含まれた空間を台形分割し、各線分の中点と台形の中心にそれぞれ節点を置く。そしてそれらの節点の中で、一方の節点が台形の中心で、他方の節点が同じ台形の境界上にあるもの同士を枝で結び、道路地図を作成する。このようにして移動計画問題を節点と枝のグラフ問題に置き換えて移動経路を探索する。そして、その道路地図から幅優先探索により１本の経路を得る。この経路において、節点を削除し効率よく目標点まで移動することができる手法として、卒業論文では右回り凸包アルゴリズムと左回り凸包アルゴリズムという２つの案を提案し、ある程度の成果を得た。しかしこれが、最短であるベスト解にどの程度近いものなのかは不明であった。

そこで修士論文では、ベスト解を決定するプログラム **distance.c** を作成した。これは、出発点から目標点までに経由する節点の数・順番などのすべての組み合わせを考え、それらのうちの無衝突経路について合計距離を計算し、その最小値を求めるプログラムである。

プログラム作成において問題となったのが、多重繰り返し処理の問題である。今回具体的に検証した図においては、経由する節点は 11 個存在するので 11 重の **for** ループ処理が必要となる。**distance.c** では制御変数を 1 次元的に 1～11^{11} まで変化させる 1 重の **for** ループを準備し、その中で制御変数を 11 進数に変換し、その 1 桁目が第一節点、2 桁目が第二節点といった具合に割り振ることにより解決した。

こうしてできたプログラムにより、凸包アルゴリズムでは 50％ほどの改善が得られていることがわかった。本研究では多くの場合ベスト解を O(n) の計算量で求めることができる **StraightLine(P)** というアルゴリズムを開発することができた。これは、経路において、連続する３点のうち、最初と最後の点を直線で結び、障害物に衝突する経路でなければ中央の点を削除していくという方法である。

決定木を用いた医療データの解析手法

数理情報科学専攻　情報科学講座　　林　佳宏

近年、大規模病院では電子カルテの導入が進められるなど医療データ(診療データや検査データ)の電子化が進み、長期間にわたり検査結果や診療情報が収集・蓄積されてきた。

本研究では、情報科学分野で使用されているデータベース技術やデータ解析技術を医療データに適用することにより、従来では見逃されていたルールや新たな知見を発見するとともに、そのための解析手法を提案することを目的とする。研究アプローチは、うつ病患者に投薬される抗うつ薬SSRIの一種であるデプロメールの薬効についてデータマイニングを行い解析する。なお、本研究は高知大学医学部神経精神科学教室および医学情報センターとの共同研究として推進した。

解析手法には決定木分析を用いて、うつ病患者に対するデプロメールの投薬による血液検査データの変化を解析した。対象データは1検査当たりを1件(データベース内の1レコードに対応)とし、全130件であり、それぞれが31属性を有した。その内訳としては投薬前のものが78件、投薬中のものが52件であった。なお、本データは神経精神科学教室の医師がカルテとの照合を行い、病名を確認した教師データである。また、医療データの特徴として、患者により検査回数や検査間隔が異なるという問題があるため、そのまま解析を行ったのでは有効な結果を得ることができないと考えられる。そこで、患者一人毎の投薬を開始する直前の検査データと投薬を終了する直前の検査データのみを抽出することによりデータを統一した。このデータ統一により、データ数は38件(投薬前が23件、投薬中が15件)になった。データ統一を行った場合と行わなかった場合のデータに対して解析を行った。解析結果として、投薬により値が変化している検査項目を比較すると、データ統一前はUAが増加し、CRPが減少したのに対して、データ統一後はCPK(CK)が増加し、CRPが減少するという違いが見られた。その中で、CRP(蛋白の一つであり、炎症性病巣の存在や病変の活動性、障害程度を鋭敏に反映する代表的な炎症マーカー)という検査項目については、データ統一を行った場合と行わなかった場合のどちらにおいても抽出されたので、評価できる結果であると考えられる。また、うつ病患者はストレスで炎症が酷くなると最近になって指摘がされており、医学的な観点からも有効な結果であると考えられる。

FFT 法による相関解析を利用した雲画像からの風速取得の試み

数理情報科学専攻　情報科学講座　東　康敬

高知大学地球環境情報学研究室が運用する「高知大学気象情報頁」には 1994 年以来大量の気象衛星画像データが保管されている。現在のところ、画像の幾何補正や背景画像（地理情報）を付加した一般向け画像の作成など基本的処理のみが行われているが、その画像から温度・風向・風速といった情報を取り出して整理されてはいない。

そこで本研究では、時系列として存在する気象衛星画像の相関関数を求め、それから雲の動き、つまり高層における大気の流れを表す風向･風速を求めることを試みた。

相関関数とは、時系列をなす二つの関数の類似度（相関係数）を座標の差の関数で表したものである。この相関関数を求めるための計算手法として、本研究では FFT 法を採用した。FFT とは高速フーリエ変換のことであり、有限離散デジタルデータの信号周波数成分(スペクトル)を高速に演算処理するアルゴリズムである。一般にデータ数 N が 2^n になっているとき、相関係数を直接計算する場合（$O(N^2)$）に比較して計算量が $O(Nn) = O(NlogN)$ となって計算の高速化を計ることができる。

本研究で扱う画像は全て「ひまわり 6 号」(MTSAT-1R) によって観測されたもので、北緯 70 度から南緯 70 度、東経 70 度から西経 150 度の範囲について 4pixel/degree の緯度経度格子にマッピングされている。また画像データは 1 時間毎に 1 つの PGM 形式画像ファイルとして保存されている。この画像を縦横 14 個ずつのセクション（各セクションは緯度経度 10 度)に分け､それぞれの中央部分の 32×32 pixel を相関解析の対象とした。各セクションについて、1 時間の観測時間間隔をおいた 2 つの画像から相関関数を求め、その最大値を示す位置(差)がそのセクションにおける対象物(雲)の移動量であるとすることができる。実際の計算においては、最大値の周辺 3×3 の格子点における相関値を追加して 2 次関数による内挿で最大となる位置を求めている。また各セクションにおける相関関数を等高線グラフ化することで、計算の有効性を確認している。

以上の結果として、風向・風速を表す矢印を元の雲画像に重ねて表示することができた。この結果をアニメーションに表すことなどにより、雲の動きから求まる風向・風速を視覚的に容易に捉えることができ、今後の研究に有効であると思われる。

主成分分析による MTSAT 広域データの解析

数理情報科学専攻　情報科学講座　森山賢太朗

アジアは一年を通して季節の移り変わりや台風、雨期・乾期など、天候が変わりやすい地域の一つである。その様子を表した画像を、MTSAT(運輸多目的衛星)の気象観察機能を用いて、多量の気象衛星画像として得ることができる。そこで、その画像データを特徴別に分類し、DB 整理などに利用出来ないかと考えた。

画像データの特徴を分類するのに多次元データ解析を行う。多次元データ解析にはいくつかの手法があるが、本研究では主成分分析を用いる。この手法は、多変量データを統合し、新たな総合指標を取り出すためのもので、相関関係にあるデータの総合力や特徴を表すことに優れているためである。元のデータの変数に重みをつけ、少数の合成変数を作る。このとき合成変数ができるだけ元のデータの多くの情報をもつようにするため、データの散らばり具合（分散）に着目する。分散＝情報量と言えるからである。分散の大きいものから順に第一主成分、第二主成分、・・・となり、このようにして求めたそれぞれの主成分について特徴を見いだしていく。

高知大学気象情報頁では気象庁が運営する気象衛星ひまわりによって観測された画像を気象業務支援センター経由で入手し、画像処理をほどこした後インターネットによって提供している。また保存書庫には過去に取得された気象衛星画像を保存していて、教育や研究の目的で自由に利用することができるようになっている。本研究で用いる画像はその中の「ひまわり 6 号」（MTSAT-1R）によって観測されたもので、その範囲は北緯 70 度から南緯 70 度、東経 70 度から西経 150 度である。この一時間ごとの気象衛星画像データを三年間分、約 26280 のデータを解析する。画像データのサイズは計算時間の問題から 560×560 のサイズを 28×28 のサイズに縮小して行う。

本研究では元の画像と主成分分析を行った画像を時系列的に見比べることで、説明変量の圧縮により細かい成分の動きは失ったが、全体の大きな動きは再現できた。これは衛星画像にも主成分分析を使える可能性があることを示している。また、それぞれの主成分ベクトルを時系列的に見ることで、その変化を地域ごとの特徴として捉えることが出来た。

Web シラバスシステムにおける OpenID 利用の試み

数理情報科学専攻　情報科学講座　　吉田 俊雄

高知学園短期大学においては，授業シラバスの公開手段として Plone/ArchTypes を応用したコンテンツ管理システム(CMS)を導入し，Web シラバスシステムとして利用している．このシステムはインターネット経由でその設置場所を意識せずに利用できる点や，学生の資格取得のための単位確認インタフェースを CMS 機能を応用して導入するなどの拡張性を持っている点が特徴である．しかし，今後利用拡大に伴って予想される，学生の個人認証によって履修歴を確認するなどの機能拡大には対応できていない．

Plone/ArchTypes 標準の認証機能を用いて学生の認証を行う場合，CMS データベースへ在学生や新入生の個人情報・ID を登録しつつ管理する必要がある．しかし，この作業は膨大な量となる恐れがあり，現状のように CMS が学外に設置されている場合は情報漏えいが懸念される．また，学内においては，メールの利用など登録済みの全学認証 ID があるため，これを再利用できればパスワードの管理上も有効である．

インターネットを介して，学内認証結果を安全に学外で利用するための手段として，本研究では OpenID を用いて試験環境を構築した．OpenID は，URL を ID として Web 上でシングルサインオンを実現する認証技術で，ID 発行と認証を行う OP(OpenID Provider) と，その認証を外部から利用する RP(Relying Party)という両サービス機能を定義している．この技術を採用する利点には，シラバスシステムを実装する Plone が標準採用しているため導入コストが低い点，比較的シンプルなプロトコルであり，ソースコードが公開されているためカスタマイズしやすい点がある．

試験環境においては，OP に UNIX 認証を利用する Gracie を用いて実際に運用中の高知大学情報科学コース教育用システムのユーザデータベースから OpenID を提供させ，RP は Plone の標準プラグインで実装した．

比較的簡単であると言われるプロトコルではあるが，実装上にはいくつかの問題点があることがわかった．Gracie や Plone は Apache httpd の ReverseProxy 機能を用いてインターネットに公開する必要があるが，認証情報を入れることで長くなった URL を適切に処理することが難しいなどである．

本研究においては，httpd の設定を調整することで，問題点を解決でき，実際に OpenID を使ってログイン可能なことが確認できた．今後，OP の機能を拡張し，認証に加えて学習記録などの個人データを提供させることで，各学生の環境や状況やニーズに沿った細やかなサービスを提供できるようになる．一方で，利用できる RP を制限するなどの方法でセキュリティを強化することも必要である．