Journal of the Faculty of Management and Information Systems,
Prefectural University of Hiroshima
2016 No.8 pp. 89 - 101

論　　文

計画型数理管理のための大規模ソフトウェア製作によるシミュレーション

錦　織　昭　峰

Simulation by Developing Large-Scale Management Software System of Mathematical Planning

Akimine NISHIKORI

Abstract

The research topics of this paper are constructed by the followings of simulation. 1). Development of an approximation method using search trees and its large-scale software for solving large-scale constraint satisfaction and assignment problems with priority order 2). Study on constrained load (power) flow of electric power systems, and on the development of its large-scale software 3). Study on display expression of sparse data structure for a large-scale spread sheet 4). Study on competitive voting and budget distributing algorithm for selecting the 21st century COE programs 5). Study on the necessary and sufficient condition on subtour elimination constraints in the formulation of symmetric traveling salesman problem 6). Study on developing the software using the incremental method by constant time for solving (modified) job shop scheduling problems 7). Study on logistics and facility location for cities in all prefectures of Chugoku and Shikoku regions 8). Study on repeated bids for many articles by combinatorial auction 9). Study on subjective distances in trade area model around the new Hiroshima baseball stadium 10). Study on algorithmic expression of neural network optimization using augmented Lagrangean function 11). Application for a simple patent on structures of systems 12). Security for the internet 13). Study on multiple encryptions and on encrypted redundant letters of a command

第１章　まえがき

今日では，コンピュータによる情報システムは実際に多数開発されている。システムを現実に開発する際に問題となる点として，実際のシステムは開発すると大規模になることがある。最終製品である情報システムは大規模でスパースとなるが，その基本的なデータ構造をどのように構成するのかは重要な問題である。従来，経営の問題として現れる計画，設計，運用に適用される最適化技法は，小規模なシステムに限定されている場合が多い［1，2］。

本研究では，実際の情報システムの事例を取り上げて，大規模でスパースな基本データの構造

を取扱う方法を考察している。特に，基本の構造として，行と列を整列させる「行列の構造」と「スプレッドシートの構造」，及び，行と列を整列させない「木の構造」を取り上げている。

本論文では，下記のようなテーマを挙げている。

1）ある期間帯（あるいは場所）に，ある資源（人数，設備，資金など）を割当てるための大規模でスパースな探索木［3 ～ 7］，

2）電力システムのスパースな大規模行列［8 ～ 13］，

3）大規模でスパースなスプレッドシート［14 ～ 16］，

4）競争的研究資金プログラムのための複数選出のアルゴリズムで用いる大規模スパースなスプレッドシート［17］，

5）巡回距離を最小化する巡回セールスマン問題の定式化［18 ～ 20］，

6）固定時間増分法によるジョブ・ショップ・スケジューリングに関する研究［21］，

7）中国・四国の都市における施設配置に関する研究［22 ～ 25］，

8）組合せオークションのための繰返し入札に関する研究［26］，

9）広島新市民球場周辺の商圏モデルの主観的距離に関する研究［27，28］，

10）拡張ラグランジュ関数を用いたニューラルネットワークによる最適化［29］。

以上の研究テーマ以外には，次の三つのテーマを考察している。

11）として，設備配置及び設備・装置の構造などの改善について考察する［30，31］。メモリのデータ構造と同様に，実際の構造物を簡単に抽象的に考えてシンプルなモデリングをして，新しいアイデアを創出して物づくりにおいて改善案を開発して，特許を取得する。そのために，システムとして捉えて，関係式によってモデリングして考察する。システムの構造について，過去に公開したアイデアの実績として，ガソリンなどの注入方法による大幅な改善，飛行機の翼の改良による機体振動の大幅な減少，船舶の先端構造を模擬した防波堤の改善，などがある。すなわち，エンジンの内部は高温・高圧で改造は難しいが，これに吹き込む気体を，内部でできるだけ拡散させて混ぜるモデリングを考察する。飛行物体の，例えば羽根の形状を，円弧の一部であるアークにする構造を検討する。海岸にある堤防の構造を，押し寄せる波を跳ね返る波で打ち消し合う構造を検討する。

このようなシステム的なモデリングを用いて，その改善を務めるための基本的な考え方を MOT 教育［30］として考察する。MOT 教育には情操教育を指摘しているが，その具体的な内容については吟味して公開することが必要である。

12）として，インターネットを利用して，遠隔地点と共同でシステムを構築してシミュレーション実験を行うことが重要である。この際に，ネットワークの頑強（ロバスト）性について考慮して，ネットワーク攻撃による妨害やデータ破壊・奪取を防ぐための情報セキュリティを開発して，各地点に独立した二重で 2 倍の情報システム［32］を構築することを考察する。

13）として，普通に暗号をかけることは既に行われているけれども，ユビキタス暗号化社会においては，未だに考察されていない事項を検討する［33，30，31］。社会のいたるところで暗号をかけると，「ユビキタスな暗号化社会」となる。一個の暗号化に脆弱性があっても，多数の暗号化を繰り返すならば，どのようなハード・ソフトでも，暗号を破ることが不可能になる。当然，この逆順に解読すれば，正規の解読は必ずできる。

本論文の構成は以下のとおりである。第 2 章においては 1）～ 11）の研究の概要を記している。第 3 章では 12）の研究において考察すべき項目を列挙している。第 4 章では 13）の研究について

考察している。第 5 章ではまとめを述べている。

第 2 章　研究内容の概要

1）～ 11）に挙げた研究テーマについては，以下のような考察を行っている。

1）割当問題では，ある期間帯にある資源を割り当てたときの「利益」を，目的関数の利益係数として用いている。この係数が「利益」という明確な金額で表すことができず，単に，ある期間帯にある資源を割り当てる「重要度」あるいは「優先度」という「重み付け」を表している場合がある。この優先度は本来数値化すること自体が困難であり，優先度をどのように重み付けしたらよいという明確な基準がない。

本研究では，利益あるいは費用が金額として明確に与えられていない割当問題を解く際に，割当を行う順番を表す優先順位を設定し，その優先順位に従った割当を行って実行可能解を求めるアルゴリズムを提案する。提案法によって，全ての要望ができるだけばらつくことなく，各々の要望を表す優先順位すなわち要望の順位をできるだけ満足させて，専門家のエキスパートよりも良い近似最適解を求める。この提案法を用いたソフトウェアを開発する。

一例として，各先生の所望する時間帯を考慮して，大学時間割を自動的に作成する。大学における時間割カリキュラムは，学生数の変動，学科の新設などの理由により毎年新しく作成されている。これらの時間割作成には，各種の条件が満たされなければならない。現状では時間割作成者は，各種のデータを参照しながら時間割作成を手作業で行っているために，それにかなりの時間を割いている。更に，その提案法を用いて大学の時間割作成に適用して，大学の全教員の要望をできるだけ満足する時間割を作成する。

本研究では，研究対象を大規模な割当問題として，解を探索するために探索木を構成して，探索を進めた結果不要となったデータを削除する際には，メモリの断片化を避けるために二重の「ごみ集め」を採用している。

開発したデータ構造を用いて，データの挿入，削除，アクセスの仕方，ごみ集め（garbage collection）等を考慮するアルゴリズムを提案する。更に，複数の探索木が交叉している場合には，ある探索木を用いて割当を変更すると，別の探索木のアークが削除されて不要となることを考慮するアルゴリズムを構築する。

2）電力系統における原子力発電が見直されており，代替エネルギー源として，再生可能エネルギー（Renewable Energy）が脚光を浴びている。これには，太陽光発電システム（Photovoltaic Power Generation System）及び風力発電システム（Wind Power Generation System）等がある。再生可能エネルギーが大量に導入された場合には，天候などの影響によって出力が大幅に変動する可能性があることから，従来にはなかった潮流変動の課題が指摘されている。また，他の隣合せの電力会社への融通電力を増加させると，電力潮流が変化してしまう。

ループが在る地域で電力潮流が変われば，ループの両方向の内で，どちら向きにどれだけの量の電力が流れるかは，予め予測が難しいことがある。この際に，いくつかの地点で，無効電力と電圧が変動する場合がある。ここで電圧低下が起きるとすると，その電圧を上げるために，現場のどの地点に無効電力を投入する設備を設けるかは重要な問題となる。

実際に電力系統では，システム内の各制御機器には調整が容易である機器と，そうでない機器がある。それ故，容易な順に優先順位を設定して，その順位に従って調整を行うアルゴリズムを開発することは意義がある。

従来，潮流計算問題はその設定の仕方にもよるけれども，得られた解を現実の運用に用いるために，電力システム内のすべての指定値を同時に制御する解を求めると，中枢の情報をシステム内のすべての地点に送る必要がある。本研究では，ある地点あるいはその付近の地点だけで無効電力の調整を行うという単純な解を自動的に求めるソフトウェアを開発する。

制約付き潮流計算ソフトウェアの開発では，計算方法の理論的構築のみならず，実際の規模をもつ系統を用いた数値計算による実証を行なう。この実証に必要であるプログラムを開発する際には，効率的な計算が行なえること，正確に作成すること，系統技術者が簡便に使用できることを考慮するので，多大の労力と時間を必要とする。本研究では，ソフトウェアの開発過程において，効率，正確，簡便を考慮するために留意する点に関して考察する。

ここで，効率的な計算を行なうということは，計算時間をできるだけ短くするために，プログラムを複雑にすることである。また，正確に作成するということは，例えば，効率は悪いけれども作成が容易である別の方法で同じ計算を行ない，その計算結果と照合することにより，プログラムが正しく作動しているかどうかを調べて，もしエラーがあればプログラムを修正することである。更に，簡便に使用できるということは，プログラムの内容に習熟していない系統技術者でも容易に使用できるようにするために，入出力形式を簡単にしたり，入力データのエラーを排除したりする機能を設けることである。

3）Excel などで代表される表計算ソフトウェアでは，多数の縦横の線で区切られたセルと呼ばれる四角の「欄」をもち，この中にデータを格納したスプレッドシート（あるいはワークシート）と呼ばれる「表」を使っている。

従来，表計算ソフトウェア Excel などで用いられるスプレッドシートにおいて，取り扱うデータがまばらにしか存在しない場合でも，対象とする区画中にデータの有るセルが 1 件でもあれば表示をするので，ディスプレイ上の 1 行あるいは 1 列にデータの無いセルのみがディスプレイに表示されることが起こる。すなわち，コンピュータのディスプレイ上にデータを表示する際には，セルの並んだ順番にそのままに表示するか，あるいは，使用者が指定した行あるいは列のみを表示していた。しかしながら，スプレッドシートが非常に大きく，しかも，データがまばらな場合（すなわち，スプレッドシートで表されたマトリックスが希薄配列である場合）には，閲覧すべきデータが少数であるにもかかわらず，何度も画面を切り替えてディスプレイに表示するしか表示法がなかった。

本研究では，表計算ソフトウェアなどで用いられるスプレッドシートにおいて，取り扱うデータがまばらにしか存在しない場合に，データがない部分を省略して記憶し，データのある部分のみを自動的に表示させる方法を提案する。本研究では，この方法を，大規模なスプレッドシートを用いた大学成績処理に適用する。すなわち，データの無いセルは取り除いて，データの有るセルのみを「圧縮順配列」によって記憶させておき，データの無いセルは自動的に省略して，データの有るセルを表示する画面を構成するアルゴリズムを開発する。

4）競争的研究資金の審査委員会において資金プログラムを選出する際には，少数の委員ではなく，全委員で素案を作成すべきである。そのため，全委員が投票を行い，賛同を示す賛成票が多い資金プログラムを選出することになる。この投票システムにおける，投票及び予算入札を管理する大規模なスプレッドシートを開発する。

従来では選挙方法は，投票システムあるいはゲーム理論として研究されている。審査委員会において，審査委員は何人であるかは重要である。執行する国費の金額の多寡によって審査委員の人数を試算してみると，数百人の委員が必要となる。この投票システムにおける，投票及び予算入札を管理する大規模なスプレッドシートを開発する。例えば，1 分野で予算総額が 32 億円であるとすると，委員 1 人に付き 1 千万円の予算執行を認めるならば，1 分野当り 320 人の委員が必要となる。または，委員 1 人で 3 千万円までの予算執行ならば，1 分野当り 107 人の委員が必要となる。もし 2 年間再審査は無しで毎年同額程度の国費を執行できるならば，この人数の 2 倍となり，640 人または 214 人の委員が必要となる。

5）従来は，巡回セールスマン問題の目的関数と制約条件を線形式で表す場合に，どのような定式化になるのかが明確に示されていない。特に，部分巡回路除去条件は，数式で厳密に示されてはいない。部分巡回路除去条件は，そのまま制約条件式にすると組合せ爆発が起こり，現実には使えなくなる。最近海外の OR 関係の雑誌でほぼ妥当な個数を公表しているが，本研究では必要十分な制約式を明確にする。

巡回セールスマン問題の部分巡回路除去条件はそのまま取り扱うと非常に数が多くなる。従来は，近似最適解を求めるために近似解法が研究されてきた。本研究では，巡回セールスマン問題の厳密な定式化を緩和して，近似的な定式化を開発する。すなわち，どのような制限や条件を設けると，どの程度の制約条件式が減少して，数理計画システムで実際に解くことができるのかを研究する。その定式化を用いて，現実的な規模の巡回距離最小化問題を解いて考察を行う。

6）時計時の単位毎にモデルが動いて事象が処理される方法である固定時間増分法を用いる。ジョブ・ショップ・スケジューリング問題をディスパッチング・ルールを用いて解く際に，一般的に用いられるモデルの時間処理は可変時間増分法である。本研究では，固定時間増分法を用いている提案法のソフトウェアを簡単に修正して，作業の先行・後続作業の関係が一つではなくて複数あるジョブ・ショップ・スケジューリングを行う。

7）物流費用を考慮して，輸送計画と施設配置を考察する。物流費用はその性質の違いから，物流施設コストと輸送・配送コストに大きく分類できる。ここで前者は物流施設を集約統合化したほうがコストを低減でき，それに対して後者は物流施設を多く分散したほうがコストを低減できるという相反する関係にある。最適な物流施設計画はその両者の和を最小化するものでなければならない。本研究では，中国地方と四国地方の全ての都市を対象として，どの都市に施設を置くかを考察する。この際に，施設の処理能力は複数から選択して，施設を配置する都市数に上限を設けてシミュレーションを行う。

8）組合せオークションにおける，売上総額を最大にするような財の割当を考察する。本研究では，入札が繰り返される度に入力データをその度に入れ替える方法を考察する。この際に，財が

すべて売買されなかったときに，売手と買手が要望価格を変えていくケースを想定する。すなわち，売れなかった財に対しては，これらの複数人の買手と売手が再度オークションに参加して，買手の価格を上げる，あるいは，売手の価格を下げて，再度入札を行う。このように入札を繰返して，オークションに出品されたすべての財を売買する。入札をする度に最適化ソフトウェアを用いて，全ての売上総額を最大化する組合せを考察している。

9）本研究では，広島新市民球場周辺にある大型ショッピング・センターの二つの店舗（広島駅の複合店舗及び広島府中ソレイユ）の小売店についての商圏モデルを考察する。人口が二千人以上の町を十か所だけ選んで，野球観戦に集まる観客が試合前後に買い物をする球場を含めて考察する。本研究では，心理的要因の一つである交通信号機に着目して，消費者が店舗に到着するための所要時間，信号機のサイクル時間，町の人口などのデータを基にして数値シミュレーションを行う。これにより，両方の店舗に出向するのに必要な時間を算出して，ハフモデルによって各町から各店舗へ買い物に行く出向人数とその確率を推定する。自動車または自転車による移動にかかる所要時間の変更を考察する。すなわち，各移動ルートにある信号機を調整して，予め定められた許容時間内に店舗に到着させるために信号機のサイクル時間を改善できるかどうかを試算する。このシミュレーションでは，現状の設定において赤色で実際に停止させている信号機に着目して，制約条件式を 2 次関数として EXCEL のソルバー機能を用いている。

10）本研究では，カオス及びニューラルネットワークによって最適化問題を解く際に，拡張ラグランジュ関数を用いることを提案している。すなわち，最適化問題の制約条件を目的関数に組込む際に，従来はペナルティ定数をつけた 2 次項のみであったけれども，本研究ではラグランジュ乗数を係数に持つ 1 次項もまた付加している。本研究では，従来定式化で用いられているペナルティ関数を用いる方法と，拡張ラグランジュ関数を用いる方法の比較を行っている。

11）エンジンの構造で最も良いのは，吹き込む直前に，らせん状になった通り道を通して，内部に吹き込む構造である。すなわち，ガソリンがエンジンの内部に入ると直ぐに，入口付近から周囲に広がらせる。単にらせん状にするよりも，更に複雑な構造にすると，更に複雑に周囲に広がる。

飛行物体の羽根の形状は，円弧の一部であるアークとして，この円弧の中心を飛行物体の胴体を前方から貫く中心線上に置く位置を検討する。普通には，気体や液体などの流体は，丸い菅である円柱の中を流す。例えば四角柱の中を流すと，四方の隅で乱流になる。飛行機で高速で飛ぶ場合にはこれを応用して，飛行機の周辺で空気が流れる形状は円柱にする。

海岸にある堤防の構造を，ぶつかって来る波と，その反射波が，お互いに打ち消し合うようにする。このために，堤防の水面より数メートル下を円柱状にするモデリングを検討する。

第 3 章　ネットワーク社会のセキュリティに関する基本的な構造，運用，制度等

12）の研究として，日本独自の情報ネットワークシステムを構成する際に必要となる，下記の項目を検討することを提案する。この際に，当然の事であるけれども，ネットワークアーキテクチャ，分散あるいはユビキタスコンピューティング等の，既存の固有技術を使用することになる。

インターネットを基盤とするIT（情報技術）に関する研究が盛んに行われている［34 ～ 38］。インターネットを代表とする高度情報通信ネットワークによって形成されるIT国家の建設が推進されている。これに伴って，ウイルス対策，不正アクセス対策，暗号技術等のセキュリティに関連する情報技術全般の研究が行われている。

日本では，内閣サイバーセキュリティセンター（NISC）を組織して，中央省庁や電力などの重要な施設をサイバー攻撃から守ることを使命としている。米国では，（当時の）クリントン米大統領は，コンピュータネットワークが，ハッカーの侵入や「サイバー（電脳）テロ」にさらされているので，社会的な混乱が起きないようにするために，「サイバースペース（電脳空間）防衛計画」を実施すると発表している。発電から航空管制までコンピュータ網が張り巡らされている現代において，コンピュータの前に座ったハッカーは，企業や自治体，国家を麻痺させることができる。それ故，ネットワークの防衛は，国の安全保障につながる。現存するインターネット等は，ユーザの使用権利を保護するという観点から，セキュリティ対策等の規制ができないので，民間でホビー用等に使用されるべきものである。日本独自の情報ネットワークを構築して，電子政府や商業活動等に容易に有効利用できるようにする必要がある。新設する情報ネットワークにおいては，この情報ネットワークの管理者によって，一般の使用者に対して使用制限や使用停止を，通知をしないで一方的に行うことができる規則で運用できることを原則とするべきである。

考察の対象となるのは，次の10項目である。これらの項目については，ネットワーク，インターネット，ソフトウェア，コンピュータOS，セキュリティ，ウイルス，不正アクセス，暗号技術，ルーティング，情報家電，スマートハウス，情報管理，データ構造，電子投票，住民基本台帳，バックアップ電源，電力システム等，あるいはこれらに伴う法規制等に関する文献を渉猟する必要がある。

「項目1」インターネットとしてのネットワークの構造及びその運用に関して考察し，ネットワーク内の回線の接続の仕方を工夫することによって，新しい運用方法を提案する。ネットワークを構成している回線の接続に関して述べると，パケットを転送する技術の一つであるルーティングを容易に行えるように，ケーブルを敷設する必要がある。これにより，不正なアクセスを防止することができる。従来は，東と西を結ぶバックボーンとなる幹線を基幹として，他の地点はそれにぶらさがった構造をしている。また，ルーティングのためのアルゴリズムとして幾つかあるが，ユーザ間で送受信されるパケットの転送が未だに容易でないという問題点がある。

「項目2」インターネット上において，多数のソフトウェアを一ヶ所で登録・管理する機能を持つ施設であるソフトウェアセンターに関して考察する。各研究分野で対象とされている現実の問題に対して，統一的なベンチマークテスト問題を処理した結果により，開発された方法論，及びそのソフトウェアを評価する制度を設ける。そのために，ソフトウェアセンターという設備を設けることを提案する。また，そのために必要となる事項を列挙する。現状では，（旧）学術情報センターである「国立情報学研究所」が，情報分野における総合的な研究機関，及び，情報発信機関として創設されている。このような機能に加えて，ソフトウェアの開発，登録，保守，整備をインターネット上で行うことになる。

「項目3」インターネットの運用を行うのに必要な法整備，及び，それに伴う運営体制を考察する。現状では，インターネットに各個人が接続して自由に各人がアクセスできるけれども，不正を行うサイトを法律によって治めることを考察する。また，災害等の考察をあらかじめ行う必要がある。規則によって，ユーザの利用制限と禁止することは，現状では迅速に遂行できるとは言

い難い。

「項目 4」コンピュータ OS のためにセキュリティ対策をする。カーネルと呼ばれるコアのファイルへの不正アクセス対策を考察し，新しい対策を考案する。現在は，ウイルスの種類毎にワクチンとなるソフトウェアを開発しているので，対策が後手に回りがちである。

「項目 5」インテリジェント・ハウスのための基本的なネットワーク構造を考察し，回線の接続の仕方を工夫することによって，新しいネットワーク構造を提案する。コンピュータ等の事故，取り扱いミス，停電等のアクシデントにも耐える安全なホーム・ネットワークの基本的な構造を考察する。現状では，情報家電やスマートハウスとして研究されている。

「項目 6」インターネット上での情報管理に関する基本的なデータ構造を考察する。インターネット上で情報を提供するためには，ある程度，規格化された形状を持たせる方が良い。本考察では，スパースで大規模なスプレッドシート構造，及び，動画像の転送を対象とする。現状では，各サイト毎の情報は，ホームページ等により文章で提供されている。

「項目 7」国政選挙の電子投票システムの不正に関する対策を考察し，問題点を列挙する。電子投票システムは，事故等のトラブル以外に，現場の電子投票の管理人による不正，あるいは，コンピュータシステム開発者等によるソフトウェアの改ざん等が考えられる。これへの対応策を検討する。現在行われている電子投票システムの問題点が洗い出しされていない。すなわち，投票機を用いた場合に，どのようなトラブルや改ざん等の不正が起こるかが列挙されていない。

「項目 8」住民基本台帳ネットワークの侵入と漏洩に関して対策を練り，新しい対応策を提案する。他地点からの不正なアクセスにより，個人情報を盗まれることを防ぐためには，住民基本台帳ネットワークに対して，セキュリティ対策をする必要がある。項目 1 と同様に，ネットワークの基本的な構造を変更する必要がある。

「項目 9」情報ネットワークを不断に使用するために，大切な電源，及びそのバックアップ電源を考察する。現状では，工場等で使用している電源は，停電の際に迂回される復旧のスイッチ操作により，一時的にオフになることがある。このような場合にも，安定して電力を供給するための自衛手段を検討する。緊急を要する病院等ではバックアップ電源を設置しているけれども，工場等では必要性を感じて対応しているとは言い難い。

「項目 10」電源を安定して使用するための電力システムを考察し，制約付き潮流計算の有効性を示す。電力を長距離送電する主要幹線が，事故やテロによって使用できなくなったときに，他にどのような主要幹線をあらかじめ設けておくかを考察する。現状では，原子力発電等の主要電力源と都市部を結ぶ幹線は，普通は一本のルートしか敷設しない場合が多い。

第 4 章　情報セキュリティに関する考察

13）の研究として，アナログ社会からデジタル社会に変換した「縮約した擬似社会」の考察がある。アナログの情報をデジタルに変換しているが，最も近いデジタル情報に縮約化している。そのデジタルに最も近いアナログは多数あるが，全ては縮約して同じデジタル情報としている。このようなデジタル社会は，人々を社会的に不安に陥れる。安心・安全な社会にするには，頑強な暗号化が必要になる。

インターネットで暗号化し，ネットワーク全体で暗号化し，コンピュータの OS で暗号化し，例えばメール・ソフトで暗号化するためのアーキテクチャを構築する。更に，暗号をかけるソフ

トを数社から選んで，その数個のソフトでそれぞれ暗号をかける，また，ユーザ自身が暗号をかけることを考察する必要がある。

現状の暗号化は，公開鍵と秘密鍵によって共通鍵だけを相手先に送付して利用させている。これを，全ての文字列の暗号化に代える。また，OS のコマンドを暗号化することにより，インターネットによるコンピュータの破壊を未然に防止できる。これにより，ネットワークのセキュリティの問題点，すなわち，ネットワークに接続された OS の脆弱性を消すことができる。従来マイクロソフト社などが行っていたセキュリティ・ホール改善のための Windows の更新をする必要がなくなる。

共通鍵では，複数回暗号化するとしても，文字を複数回ずらすことを一度に行うと，ある共通鍵で 1 回ずらして暗号化した結果と同じ文字列になる。それ故，多重に暗号化するには，複数組の公開鍵・秘密鍵を使うことになる。

10 進数の数値を暗号化する場合には，暗号化した数値は 1 桁だけ多くなることがあり，これを考慮する必要がある［33］。（暗号化した数値が同じ桁数になるならば，先頭に零を付けて，1 桁増やすことにする。）8 ビット（または 16 ビット）で表される文字（または漢字）などを，2 進数の数値として取り扱うならば，1 個多くなることを考慮する必要がある。

公開鍵と秘密鍵による RSA 暗号［39］において，非常に大きな二つの素数を掛けた数値を n とする。n で割った余りの数値を暗号化している。偶数（n － 1）を 2 進数で表すと，最上位は 1 であり，全てのビットが 1 となることは無い。下位の方から順番に 8 ビット（または 16 ビット）ずつ区切り，合計 k 個あるとする。ただし最上位に，1 ～ 7 ビット（または 1 ～ 15 ビット）が残っているならば，残っているこのビットは無視して含めない。最上位に 1 ビットも残っていないならば，k ← k － 1 として k を 1 だけ減らす。暗号化する文字の列は，k 個ずつ区切って，それぞれの区切り毎に暗号化する。ただし，暗号化すると（k ＋ 1）個となる場合があるが，復号すると元の長さの k 個に戻る。

他者が暗号を使用していて，それが RSA 暗号だということが予め分かるならば，不正に解読する方法がある。復号して解読するときには，復号したい数値に対して d 乗して，公開された n で割っている。それ故，d に対して，d ＝ 2，3，4，・・・と順番に入れて，それぞれに対して復号しているかどうかを調べる，という総当たりをする方法である。各々を人間の目で見て調べると膨大な手間がかかるので，調べる際にはエディタの検索機能を使う。普通には頻繁に出てくる a，the，this（または，「これ」，「その」，「ます」，「です」）などの文字列が多数出現しているかどうかを，コンピュータで検索して自動的に調べる。このような文字列が多い場合には，人間が実際に目で見て調べて，解読されているかどうかを判定する。これは簡単な方法であるので，これによって不正に解読されないように注意が必要である。共通鍵などと一緒に，多重に暗号化しておくとよい。

将来にはどんな情報データでも暗号化をするユビキタス暗号化の時代が来ると予想されるが，暗号化・復号を行うプロセッサを開発するためには，それを行うソフトによる暗号命令を作成する必要がある。この暗号命令をハード回路でチップ化する。

利用目的や利用環境が異なれば，想定されるリスクも異なってくるので，必要とされる対策も異なってくる。新規に独立した情報システムを構築する際に，ネットワークに独自のサーバを接続して，パソコンにクライアント・ソフトを新規に導入して，遠隔地間で新たな独立した情報システムを構築することを考察する必要がある。情報セキュリティのための技術を構築して，多数

の研究者によるグリッド環境のためのグリッドミドルウェアを製作することが将来の課題である［40］。

インターネットによるデータ伝送において，現行のイーサネット･ヘッダと IP ヘッダ［41］の次に，（例えば，これと同数の固定長ビットによる）付加データを入れることにして，そのようにプロトコルを変更することを提案する。この付加データは，後続のデータに関する情報であり，例えば，暗号化されたデータを解読するための情報である。（この付加データを，区切りがよい 10 ビット単位で構成してもよい。）これ以外には，この付加データを IP アドレス枯渇問題にも使用することができる。すなわち，現行の IP アドレスは 32 ビットとしている IPv4 であるので，ビット数を拡張して，このビットのデータをここに記憶させて使用する方法が考えられる。

情報セキュリティ体制の確立のために，情報セキュリティ・マネジメントを実行することで，情報セキュリティ・レベルの維持を図る対策の検討が必要である。情報セキュリティ・マネジメントを実行するために，情報セキュリティ対策の具体的計画・目標の策定，計画に基づく対策の導入・運用，実施した結果の監視・見直し，改善・処置という一連のサイクルを継続して実施することになる。

第 5 章　あとがき

大規模なソフトウェアを製作する際に決定すべきスパースなデータ構造は様々な分類の仕方があるが，本研究ではデータ構造を二つに分類して，行と列を整列させるデータ構造と，整列させないデータ構造としている。このような最新の研究成果を用いて，大規模なソフトウェア開発あるいは大量データによる数値シミュレーションの事例を取り扱った研究を行い，更には検証を行う。

本研究では，一般的な問題の一例として一般化割当問題を選んで，エキスパートよりも良い結果を得ることができることを例証する。本研究は，スパース性を考慮して効率的な探索木を作成すれば，エキスパートよりも更に深い探索を行って近似最適解を改善できることを示す。これを，本研究では実用性を考慮した人工知能の機能の一つとして研究している。すなわち，スケジューリング表を表す状態空間を探索して，制約及び拘束を表す条件式を連続的に変形させて充足させる知能を研究する。

本研究における第一の特長は，実規模であるが故に大規模なシステム（すなわち，変数の次元が大きく，式の数が多い問題）を対象としていることである。大規模でスパースな 2 次元配列変数 x[i,j] に対して，キャッシュメモリのヒット率を向上させることができるデータ構造を決定して，実規模の大規模数値シミュレーション実験において，計算時間の大幅な短縮を行うことになる。著者は，このデータ構造を動画像に応用する特許を申請している［42，43］。

開発するソフトウェアは，大規模でスパースな行列を効率良く取り扱うことを考慮すべきである［44］。研究として作成したのは，電力システムの最適化のために約 2 万ライン，スケジューリング及び割当問題等のために約 1 万ライン，合計約 3 万ラインである。ここで，大規模な一般化した割当問題に関する研究においては，優先順位に従った割当てを行った解を求めるために，探索木を用いた最適化法を提案している。提案法による約 1 万ラインの大規模な経営のためのソフトウェアを，Fortran により一個人で作成して，数値シミュレーション実験を行い，十数万個程度の整数変数をもつ非常に大規模な割当問題を扱っている。

本研究の提案法を用いた大規模なソフトウェアを作成して数値シミュレーション実験を行っている。シミュレーションを行うにあたって，業務の委託や共同実施などの形で遠隔地点と共同でシステムを利用するために，新たなシステムをインターネット上で構築する必要がある。

また，システムの構造をアイデアで改善して，特許を取得することを提案している。過去に公開したアイデアの実績と伴に，この基本的な考え方を MOT 教育として公開する方がよい。特許のアイデアまでの開発ならば，個人または少人数の能力に帰するところが大きい。

参考文献

［1］錦織昭峰「大規模な数理情報システムのスパースなデータ構造」，県立広島大学経営情報学部論集，第 2 号，pp.11-24，平成 22 年。

［2］茨木俊秀，福島雅夫「FORTRAN77　最適化プログラミング〈岩波コンピュータサイエンス〉」，岩波書店，1991 年。

［3］錦織昭峰「割当問題の制約充足のための探索木のデータ構造」，日本シミュレーション学会第 19 回シミュレーション・テクノロジー・コンファレンス，pp.313-317，平成 12 年。

［4］錦織昭峰，渡辺展男，青木兼一，金指正和「大規模な優先順位付き割当問題のための探索木を用いた近似解法」，電気学会論文誌，第 115 巻Ｃ分冊，第 12 号，pp.1521-1531，平成 7 年。

［5］錦織昭峰，渡辺展男，一森哲男，青木兼一，金指正和，伊藤雅「優先順位付き割当問題のための大規模数値求解に関する考察」，日本応用数理学会論文誌，Vol.6，No.4，pp.329-351，平成 8 年。

［6］錦織昭峰「優先順位を考慮した大規模な一般化割当問題のためのデータ構造とアルゴリズム」，電子情報通信学会論文誌Ｄ－Ⅰ，Vol.J85-D-I，No.2，pp.122-131，平成 14 年。

［7］A. Nishikori, Data Structure and Algorithm for Large-Scale Generalized Assignment Problem Which Considers Priority Orders, *Systems and Computers in Japan*, Vol.38, No.3, pp.83-91, 2007.

［8］K. Aoki and A. Nishikori, An Algorithm for Constrained Load Flow, *IEEE Trans. Power App. Syst*., Vol.PAS-103, No.5, pp.963-973, 1984.

［9］K. Aoki, A. Nishikori and R. Yokoyama, Constrained Load Flow Using Recursive Quadratic Programming, *IEEE Trans. Power Systems*, Vol.PWRS-2, No.1, pp.8-16, 1987.

［10］青木兼一，錦織昭峰「非線形計画を用いた制約付き潮流計算」，電気学会論文誌，第 106 巻Ｂ分冊，第 8 号，pp.678-684，昭和 61 年。

［11］範明天，青木兼一，錦織昭峰，奈良宏一「An Algorithm for Discrete Optimal Power Flow」，*Electrical Engineering in Japan*, Vol.112, No.1, pp.114-123, 1992 年。

［12］錦織昭峰「電力系統の制約付き潮流計算に関する研究」，工学博士論文，広島大学，昭和 62 年 3 月。

［13］錦織昭峰「Lagrange 乗数の許容限界を調節した制約付き潮流計算」，電気学会全国大会，6-100，pp.173-174，2012 年。

［14］錦織昭峰「スプレッドシートのためのまばらなデータの表示法」，日本シミュレーション学会第 17 回シミュレーション・テクノロジー・コンファレンス，pp.279-282，平成 10 年。

［15］錦織昭峰，柳沢典子「大規模なスプレッドシートを用いた大学成績処理のデータ構造に関

する一考察」，広島県立大学紀要，Vol.6，No.1，pp.79-89，平成 6 年。
［16］錦織昭峰「スプレッドシートによる，まばらなデータの表示」，特許出願番号　特願平 6-113326，特許公開番号　特開平 7-287734，出願日　平成 6 年 4 月。
［17］錦織昭峰「競争的研究資金プログラムのための複数選出のアルゴリズムに関する考察」，電気学会論文誌Ｃ，Vol.133，No.10，pp.1957-1968，2013 年。
［18］錦織昭峰「数理計画における巡回セールスマン問題の定式化」，広島県立大学紀要，Vol.15，No.1，pp.25-30，平成 15 年。
［19］錦織昭峰，石橋悠毅「配送のための巡回距離最小化問題 TSP の定式化に関する一考察」，電気・情報関連学会中国支部連合大会，pp.306-307，平成 18 年。
［20］A. Nishikori, Necessary and Sufficient Condition on Subtour Elimination Constraints in the Formulation of Symmetric Traveling Salesman Problem, *Proceedings of the International Conference on Electrical Engineering*, No.SI-1, pp.72-76, 2012.
［21］A. Nishikori, Incremental Method by Constant Time for Solving Job Shop Scheduling Problems, *Proceedings of the 10th International Conference on Industrial Management (ICIM2010)*, pp.38-42, 2010.
［22］錦織昭峰「ロジスティクスに関する考察」，広島県立大学紀要，Vol.16，No.1，pp.27-35，平成 16 年。
［23］錦織昭峰，石橋悠毅「中国 5 県都市の施設配置に関する一考察」，日本シミュレーション学会第 25 回大会，pp.199-205，平成 18 年。
［24］錦織昭峰「四国地方 4 県都市の施設配置に関する一考察」，第 56 回システム制御情報学会研究発表講演会，T23-4，pp.337-338，2012 年。
［25］A. Nishikori, Consideration on Facility Location for Cities in Four Prefectures of Shikoku Region, *Proceedings of the 11th International Conference on Industrial Management (ICIM2012)*, pp.39-43, 2012.
［26］錦織昭峰「組合せオークションにおける複数財のための繰返し入札に関する考察」，日本シミュレーション学会第 28 回大会，pp.443-447，平成 21 年。
［27］錦織昭峰「広島新市民球場周辺の商圏モデルの主観的距離に関する研究」，県立広島大学経営情報学部論集，第 3 号，pp.131-142，平成 23 年。
［28］錦織昭峰「広島新市民球場周辺の商圏モデルの主観的距離に関する研究」，電気学会 ITS 研究会資料，ITS-12-16，pp.29-34，平成 24 年。
［29］錦織昭峰，日野智崇　研究ノート「拡張ラグランジュ関数を用いたニューラルネットワークによる最適化」，広島県立大学紀要，Vol.14，No.1，pp.167-177，平成 14 年。
［30］錦織昭峰「「システム管理最適化論」のシラバスに関する一考察～工業特許のアイデアを生み出す MOT 教育～」，県立広島大学経営情報学部論集，第 6 号，pp.23-34，2014 年。
［31］錦織昭峰「工業特許のアイデアを生み出す MOT（Management of Technology）に係る実践例」，電気学会産業応用部門大会，5-54，pp.V327-V332，2015 年。
［32］錦織昭峰，特集：21 世紀の扉を開く記念部門誌　特集解説「日本の情報ネットワークおよびソフトウェアセンターに関する提言」，電気学会論文誌，第 121 巻Ｃ分冊，第 1 号，pp.56-57，平成 13 年。
［33］錦織昭峰「四国地方の都市毎の施設配置とその情報の多重暗号化に関する研究」，日本ロジ

ステックスシステム学会第 16 回全国大会予稿集，pp.15-18，2013 年。
［34］宮地利雄「ネットワーク・セキュリティの現状と課題」，電気学会論文誌，第 124 巻 C 分冊，第 8 号，pp.1521-1526，2004 年。
［35］村瀬一郎，鈴木裕信「国外の政府レベルのネットワークセキュリティ確立への取り組み」，情報処理，第 42 巻，第 12 号，pp.1181-1185，2001 年。
［36］戸村哲，三輪信介，大野浩之「我が国政府におけるネットワークセキュリティ確立への取り組み」，情報処理，第 42 巻，第 12 号，pp.1186-1190，2001 年。
［37］武田圭史「多様化するネットワーク環境における情報セキュリティ対策」，システム／制御／情報，Vol.51，No.4，pp.158-163，2007 年。
［38］薄田昌広「非定型な情報システムへの情報セキュリティ対策の検討」，システム／制御／情報，Vol.51，No.4，pp.175-180，2007 年。
［39］飯島淳一「入門　情報システム学」，日科技連，2005 年。
［40］鶴澤武士「グリッドを実現するグリッドミドルウェア基盤」，情報処理，Vol.51，No.2，pp.120-126，2010 年。
［41］坂和正敏，矢野均，西崎一郎「情報科学入門」，朝倉書店，1995 年。
［42］錦織昭峰「3 原色あるいは 3 属性による動画像のためのスパース性を考慮したデータ構造」，広島県立大学紀要，Vol.13，No.1，pp.47-58，平成 13 年。
［43］錦織昭峰　特許「動画像における映像情報のスパース性を考慮したデータ構造」，特許出願番号　平成 7 年　特許願　第 192402 号，特許公開番号　特開平 9-9292，特許第 3194005 号，査定日平成 13 年 3 月。
［44］錦織昭峰「情報科学及び経営科学の初学者用教材に関する一考察」，第 57 回システム制御情報学会研究発表講演会，No.215-6，pp.1-6，2013 年。