

情報理論とその応用学会ニューズレター

SITA' 90のお知らせ

大学院博士論文紹介

暗号鍵共有方式KPSの実現に関する研究

ユニバーサルデータ圧縮とその応用に関する研究

A STUDY ON QUANTUM COMMUNICATION SYSTEMS

可変レートによる高効率音声符号化方式に関する研究

情報縮約理論を用いた情報システムの評価に関する研究

情報系新学科紹介(明治大学理工学部情報科学科)

コーヒープレイク~Shannon は越えられるか~

会合案内

ISITA' 90

VISICOM'91 Fourth International Workshop on PACKET VIDEO

VISICOM'91 1991 Picture Coding Symposium

SITA' 89報告

情報理論とその応用学会1989年度総会報告

役員立候補の受付

投稿募集

編集後記

佐藤 洋

高嶋 洋一

朴 志煥

山崎 浩一

水井 潔

稲積 宏誠

荒川 薫

広田 修

畑 雅恭

今井 秀樹, 森 真作

SITA' 90のお知らせ

実行委員長 佐藤 洋 (電気通信大学)

今回のシンポジウムは東京近郊で行なわれることが決定され、電気通信大学が中心となってお世話をすることになりました。

日程 1991 年 1 月 23 日(水)~1 月 26 日(土)

会議場 蓼科パークホテル(長野県茅野市)

論文締切 11 月 17 日

(参加申込を頂いた方には近く詳細御案内を
お送り致します)

会場は、八ヶ岳中信高原国定公園の中の蓼科温

泉にあります。近くにはスキー・スケート場もたくさんあり、絶好の保養地でございます。あいにく冬季の開催で外は寒いですが、温泉気分を満喫して頂けるのではないかと存じます。参加費の高騰をなるべく押えて、学生の皆さんにも参加し易いようにいたしたいと思います。本年 11 月 27 日~30 日にはハワイで ISITA が開かれますが、実行委員は一同、内容の充実したシンポジウムになりますよう張り切って準備に取り組んでおりますので、ISITA と同様に定例の SITA の方にも、振るって御参加下さるようお願いいたします。

実行委員会の事務局は

〒182 調布市調布ケ丘 1-5-1

電気通信大学 情報工学科

(小林 欣吾, 山口和彦)

電話 0424-83-2161 内線 4380, 4379

Fax 0424-82-3055

Email sita-office@cs.uec.ac.jp

です．なお関係の諸組織におかれましてはシンポジウムの開催に向けて何かとお力添えを下さいますよう、よろしくお願い申し上げます．

大学院博士論文紹介

暗号鍵共有方式 KPS の実現に関する研究

高嶋 洋一

学位取得大学：

横浜国立大学(指導 今井 秀樹 教授)

現在の所属：

NTTヒューマンインターフェース研究所
画像メディア研究部

要 旨

現在、大規模で複雑なネットワークにおいて不特定多数のエンティティ(entity:ユーザ、加入者)と暗号通信を可能とすることは、現代社会で情報機器を安心して利用できるようにするために必要とされている．そこで問題となるのは、利用する鍵の配送(共有)を安全かつ簡単に行なうにはどのようにすればよいかということである．この鍵配送(共有)問題の1つの解決方法として公開鍵暗号化方式が考えられている．公開鍵暗号化方式は暗号化鍵を公開しても良いので鍵配送に秘密通信路を使用しなくてすむという画期的な特長を有しており、具体的方式として1978年にRivest, Shamir, Adlemanにより提案されたRSA暗号方式があるが、残念ながら現在の技術では、暗号化/復号の計算量が大きいためリアルタイム通信など高速処理には適していない．他の公開鍵暗号化方式もいろいろと研究されてはいるが、まだ実用にいたっていないのが現状のようである．

そこで、鍵配送(共有)問題を解決し、共通鍵暗号方式の簡便な利用を可能にする鍵共有方式 KPS (Key Predistribution System)が重要な意味を持つてくる．共通鍵暗号化方式は過去に莫大な研究資産があり、一般に暗号化/復号速度も高速である．

これを利用できれば、公開鍵暗号化方式では実現できない高速処理にも暗号を適用することが可能となる．KPSの具体的方式として、線形スキームと呼ばれる方式が提案されている．KPSは、信頼できるセンタの存在を仮定しているものの、エンティティが暗号通信しようとしているとき、鍵共有のためにセンタや他のエンティティと打ち合わせする必要がないという特長を有している．したがって、宛先だけが分かっている相手エンティティに対し、いきなり暗号通信を始めることができる．言い換えれば、暗号を利用したメール通信ができるということである．またこの特長を利用して、様々な電子取引等にも暗号を応用することが可能である．さらに安全性の面では、

- (1)信頼できるセンタの存在を前提としている
- (2)ICカードの物理的セキュリティが十分でない場合、エンティティの結託によるセンタ秘密の暴露という問題があるが、1つのエンティティに配られた情報(秘密アルゴリズム)だけでは他のエンティティ間で利用される鍵や、他のエンティティの秘密アルゴリズムを完全に求めることが、理論的に不可能であるということがある．

このような特徴を持つKPSが、本当に理論通りに真に実用的であるかどうかを調べることを目的として、KPSを利用して鍵共有を行う装置を具体的に実現する．本論文は、この実現に関する技術、方法についてまとめたものである．

まず、KPSの実現に当たり、KPSのプロセスの一つにセンタが各エンティティの秘密アルゴリズムを秘密に配布するプロセスがあることから、個別に秘密通信路として、ICカードを利用することを考えた．ICカードの中に秘密アルゴリズムをいれて配布(または本人が取りにいくことを)すれば、本人ですら秘密アルゴリズムは知らないというようにすることが可能である．ICカードはキャッシュカードのような磁気カードとは異なり、磁気カードが単なるメモリだけであるのに対し、ICカードはメモリにCPUを組み合わせた新しいデバイスである．ICカードはメモリのアクセスをCPUに管理させることができるので、情報セキュリティの点で磁気カードより優れており、この長所を活かした応用がいろいろと考案されているところである．

一方、KPSの1具体例である線形スキームは、あるしきい値以上の結託があるとシステム全体の秘密がばれてしまうという欠点を持っている．しか

し、そのしきい値を自由に設定して個別の方式を設計できるという広いクラスであり、他の鍵共有方式では、このしきい値を大きくすることが難しい。

つぎに、実現するための設定条件として、しきい値を 8192 にし、ID 変換アルゴリズムを検討する。ID 変換アルゴリズムは、短いベクトル(ID)を長いベクトルに変換する一方向性のアルゴリズムである。線形スキームによる鍵共有は、行列とベクトルの乗算とこの ID 変換アルゴリズムとから構成され、安全性の面でのキーポイントを担っている。ID 変換アルゴリズムは IC カードでも簡単に計算でき、単射を実現し、一方向性でランダム性であることも望まれる。このような条件を満たす構成法として既存の暗号アルゴリズムを一方向性アルゴリズムの部品として用い、それらをうまく組み合わせる方法を検討する。ID 変換アルゴリズムを実際にある 8bitCPU で実現し、統計的な実験の範囲では、単射性、ランダム性の条件は十分に満足されていることが示された。

ID 変換アルゴリズム、IC カード利用といった方針が固まったところで KPS を実現する IC カード(KPS カード)を実際に制作する。完成した IC カードを KPSL1CARD と呼ぶが、この KPS カードは、既存のネットワークにおいて暗号通信をたやすく行えるようにしたカードであり、例えば、ファクシミリ端末に KPS ファクシミリアダプタを組み込み、この KPS カードをアダプタに差し込むことによってネットワーク上では暗号化されたデータが流れるように暗号通信ができる。それぞれ通信メディア毎のアダプタさえ用意すれば、コンピュータネットワーク等にも適用できる。

KPSL1CARD は、KPS アダプタに差し込んで利用するだけでなく、KPSL1CARD 単独でもいくつかの機能(オフライン機能)を有している。オフライン機能として電卓、持ち主確認、電話帳、KPSID 帳、パスワード変更、ログ、ロック、ロック解除があり、またハードウェア的な特徴として発振器(450KHz)、乱数発生器が内蔵されているということがある。

現在、ファクシミリ通信に適用することができる KPS facsimile adaptor と KPS センタ、KPS ロック解除センタがある。アダプタは、適用する通信メディアに対してそれぞれ用意する必要があるが、KPS センタや KPS ロック解除センタは KPSL1CARD を利用する限り、共通である。

最後に、実現したプロトタイプシステムの評価をおこなう。KPSL1CARD は、まだプロトタイプであり、カード厚が厚い、構造が複雑、等のいくつかの欠点が挙げられる。しかし、従来にない鍵共有法を実際に具体的に実現したカードであり、アダプタさえ用意すればどんな通信メディアにも暗号通信が可能となることを、実際に示したという点で、評価できるであろう。将来、技術が進んでいくにつれ先の欠点はすぐに解決できるめどが立っており、将来このようなカードは必要不可欠となっていくであろうと思われる。

ユニバーサルデータ圧縮とその応用に関する研究

朴 志煥

学位取得大学：

横浜国立大学(指導 今井 秀樹 教授)

現在の所属：

大韓民国国立釜山水産大学電子計算学科

要 旨

データ処理技術の発達に伴い、多種多様なデータを効率よく保存・伝送するデータ圧縮の重要性が高まっている。Shannon 理論の一分野として研究されてきたデータ圧縮は、対象情報源をそれが含んでいる冗長性(redundancy)を削除してより短い出力データ系列に変換することを言う。その効果は、データ通信における伝送効率を上げることやデータベース等の蓄積における記憶容量の削減および情報セキュリティを高めることにある。現在、データ圧縮技術は、計算機上のファイル系、データおよび画像通信などの分野で多く応用され、実用化されつつある。

最適符号としてよく知られているハフマン符号を始め、従来の多くの符号は対象情報源の性質が予め分かるという前提の下に効率的な圧縮が行われる。これに対して近年注目を浴びている“ユニバーサル符号”は、対象情報源に対する事前知識を前提とせずに、その平均符号長が圧縮の限界であるエントロピーまで限りなく近づくという漸近的最良性を持つ強力な符号である。この様なユニバーサル符号は、Ziv-Lempel 符号および Rissanen 符号を契機として大きな成長を見せてきた。その中でも、系列の複雑さを有限オートマトン上で定義した計算論的情報量に基づく Ziv-Lempel 符号は

最も多く研究され、LZW(Lempel-Ziv-Welch)符号の様な実用的な符号にまで至っている。

また、計算機科学の分野でよく使われている Self-Organizing Rule(SOR)をデータ圧縮へ応用した例が Bentley-Sleator-Tarjan-Wei(BSTW)により考案され、新たなユニバーサル符号として注目されている。それに関連した整数表現法に関する研究も活発である。BSTW 符号に代表される Recency Rank 型ユニバーサル符号と類似したインターバル型符号は実現が簡単であり、しかも、その漸近的最良性が保障されるユニバーサル符号の一つである。

一方、Rissanen は情報源の文脈情報を収集する情報源モデリングに着目し、MDL(Minimum Description Length)規準と算術符号(Arithmetic Code)を独立に発展させ、新たなユニバーサル符号への指針を与えている。算術符号はデータ系列の圧縮をはじめ画像符号化に至る多くの分野に応用されつつある。

これらのユニバーサル符号はそれぞれ独立に研究され、理論的には漸近的な最良性が示されている強力な符号である。しかし、有限長のデータを圧縮率、収束性、計算量および所要メモリの面で効果的に処理できる段階にまでは至っていないものが多い。そこで、本論文ではこの問題を踏まえたより実用的な圧縮法を構成する立場で各方式の検討を行い、その性能を明かにすると共に、より有効なデータ圧縮法の設計を目指す。本論文は 6 章で構成され、2 章～5 章で上記の各ユニバーサル符号について検討している。これらの各符号を用いて適応圧縮法を構成する際の問題点を指摘し、その解決策となる具体的な四つの方式を提案している。

まず、2 章では“ポインタ型ユニバーサル符号”に代表的される ZL-U(Ziv-Lempel's Universal Algorithm)法の性能を分析し、その問題点を明かにする。その解決策として提案する符号化法は、ZL-VF(Ziv & Lempel's Variable to Fixed)符号を可変長の W(Variable to Variable)に拡張を行い、それによって得られる各パラメータに算術符号化を行う方式である。また、算術符号化の前提となる出現確率の推定はリングバッファを用いて適応的にを行い、確率更新に伴う計算量の増加を線形オーダーで抑えている。提案方式の性能は LZW 符号に比べて、符号化速度では少し劣るものの、ポイン

タ型であるので増分分解型の LZW 符号より復元は早く、かつ圧縮率でも平均 9%良い結果が得られる。

Recency Rank 型符号は、現在符号化しようとする部分系列とその最終出現との間に存在する異なる部分系列の個数で符号語が決まるものである。3 章では Recency Rank 型ユニバーサル符号の一つである BSTW(Bentley-Sleator-Tarjan-Wei)アルゴリズムを適応的に構成するときの問題点を指摘し、それを解決した新たな適応データ圧縮法を示す。そこで、計算機科学分野で応用されている SOR の中で MTF(Move To Front)と Transpose を中心に検討を行っている。また、符号化においては 2 パスとなるハフマン符号の代わりに、Elias の ω 符号に基づいた新しい整数表現法を用いている。提案方式を計算機上の各種のファイルに施した場合、その圧縮率は Dynamic Huffman 符号、算術符号(1 重マルコフ)と LZW 符号に比べてそれぞれ 27%、13%、7% 程度良い圧縮率が得られる。

4 章は“Interval 型ユニバーサル符号”を取り上げ、その性能向上を図ると共に 2 章で提案した ZL-VV(Ziv-Lempel's Variable to Variable)符号との関係を明かにする。また、リスト構造(List Structure)を用いた新しいインターバル符号を提案し、それらの性能を比較検討する。5 章ではディジタル化された階調画像(Gray scale images)の無歪圧縮(可逆符号化)について検討を行っている。符号化方式としては“多値算術符号”を用いているが、符号化の前提となる情報源モデリングはより汎用的なマルコフモデルと画像データに適した差分モデルを用いている。モデリングの際に、次数(order)と階調数の増加に伴う符号化の劣化が大きな問題となるので、状態の縮退を行っている。その基本的考え方は、出現頻度が少ない状態をグループ化することであるが、その際に計算量と所要メモリなどを考慮した最適な方法が必要である。提案する縮退法は、従来法より少ない計算量と所要メモリで、同程度以上の圧縮率が得られる特長を持つ。また、提案方式は画像符号化の標準化における階層的な符号化にも適する。さらに、多値算術符号化の処理速度を向上させるために、確率区間の並べ換えによる高速化アルゴリズムの一手法を提案している。

山崎 浩一

学位取得大学：

慶應義塾大学（指導 中川 正雄 教授）

現在の所属：玉川大学情報工学科

要 旨

本研究は、光を情報伝送媒体とした通信系の性能限界を、物理的および通信方式的に改善することを目的とするものである。

物理的改善とは、光の性質を変えることによりその量子雑音の情報成分に与える影響を低減するものであり、これは通信系の本質的な特性改善をもたらす。現在、光通信系は量子雑音以外の雑音の影響はほぼ無視しでき、量子雑音が系の性能に限界を与えるところまできている。ここでは、新しい性質の光として、従来広く用いられているコヒーレント状態光に比べ、複素振幅の二つの直交成分のうちの一方の量子雑音が少ないスクイズド状態光、および光子数揺らぎの少ないサブポアソン状態光を対象とする。まず初めに、これらの非標準状態光を用いることにより、コヒーレント状態光の量子雑音限界を大幅に改善することを示し、非標準状態光の有効性を明らかにする。次に、これらの非標準状態光がエネルギー損失の影響を受けやすく、その特徴が破壊されやすいことを示す。特に、スクイズド状態光では、送信側で信号対雑音比（ S/N ）を最大にしても、受信側における S/N は、3 dB以上のエネルギー損失がある場合ではコヒーレント状態光よりも悪くなることを示し、通信系に与える損失の影響の重大さを示す。そのために、損失の影響を考慮した最適なスクイズド状態光の条件を求め、この最適化により任意の損失量に対しコヒーレント状態光より S/N の優れたスクイズド状態光が得られることを示す。さらに、上述の最適スクイズド状態光と光子数状態光を用いた二種類の通信系に対する損失の影響を考察し、スクイズド状態光を用いた方が影響が小さいことを示す。

一方、光子計数通信系の特性を変調方式や誤り訂正符号など通信理論的立場から改善し、情報理論により考察する。この通信方式はエネルギー制限の非常に厳しい深宇宙通信への適用が期待されている。そこで、ここでは情報伝送のエネルギー

効率の改善を目的とし、その評価基準として“光子一個で伝送可能な情報量（情報効率）”を用いる。まず、変調方式として On-Off Keying（OOK）を提案し、すでに提案されているパルス位置変調（PPM）との比較を通信路容量を用いて行う。その結果、OOKの方が情報効率で約 $1.44/n$ bit/Photon 優れ、伝送帯域はPPMの約3分の1であることを示す（ n は信号の平均光子数）。次に、OOKを用いた光子計数通信路は完全非対称二元通信路であるため、従来の誤り訂正符号ではその性能が十分発揮されないことを示し、従来の誤り訂正符号を光子通信路に適した符号に改良した“重み分布制御符号”を提案し、その有効性を示す。次に、要求される情報効率に対し準最適な誤り訂正符号の条件（情報速度、入力シンボルの生起確率）を信頼性関数により求め、また従来の誤り訂正符号では 1 bit/photon 以上の通信が保証されないことを示す。さらに、光子計数通信路における背景光雑音の影響を考察し、しきい値決定法を用いる。OOKの方が最尤決定法を用いるPPMよりその影響は大きい、PPMではブロック長が長くなるにつれて影響が大きくなることを明らかにする。

以上、本研究では従来の光通信で知られる量子限界を、物理的及び通信方式的に克服する方法を提案したものであり、今後の光通信系への応用上有用であることを示した。

可変レートによる高能率音声符号化方式 に関する研究

水井 潔

学位取得大学：

慶應義塾大学（指導 中川 正雄 教授）

現在の所属：関東学院大学電気工学科

要 旨

近年、音声・画像・データといった様々な情報形態を同時に取り扱える統合通信網の研究・開発が行われている。統合通信網では、時々刻々と変化する情報源の持つ情報量に合わせた可変レート符号化方式が使用できる。

本論文では、「可変レートによる高能率音声符号化方式」として「可変ビットレート Modulo-PCM 方式」と「可変ビットレート PARCOR-VQ 混成ボコー

ダ」を提案している。

第1章では、音声の高能率符号化方式について概観し、本研究の位置づけを行っている。

第2章では、Modulo-PCM方式、PARCOR方式、ベクトル量子化、可変レート符号化を中心に従来の高能率音声符号化方式を説明している。

第3章では、新しい波形符号化方式のModulo-PCM方式に可変レート符号化方式を適用した可変ビットレートModulo-PCM方式を6種類提案し、その特性を計算機シミュレーション及び主観評価試験によって評価している。特に、3 - 6.で提案している方式は、簡単な回路構成で量子化ビット数とステップ幅をそれぞれブロックごとに適応的に変化させるModulo-PCM方式で、平均ビットレート30.96kbit/secで、CCITTで標準化された32kbit/secのADPCM方式より良好な再生音が得られることがわかった。

第4章では、分析・合成系符号化方式のPARCOR方式とベクトル量子化法を可変レート符号化方式で組み合わせた可変ビットレートPARCOR・VQ混成ボコーダを提案している。本方式は、有声音部では高い情報圧縮効果を得るためにベクトル量子化を用い、無声音部では合成音の了解性を高めるためPARCOR符号化を用いる。すなわち、フレームの形態に合わせて使用するビット数を変える可変レート符号化方式である。計算機シミュレーション及び主観評価試験により、平均ビットレート919bit/secで、従来の2.4kbit/secのPARCOR方式と同程度の了解性の高い合成音声を得られることを確認している。

第5章は結論であって、本論文で得られた成果を総括的にまとめ、今後の課題について述べている。

以上のように、本論文では「可変レートによる高能率音声符号化方式」として「可変ビットレートModulo-PCM方式」6種類と「可変ビットレートPARCOR・VQ混成ボコーダ」を提案し、計算機シミュレーション及び主観評価試験によってその有効性を確認している。

情報縮約理論を用いた情報システムの評価に関する研究

稲積 宏誠

学位取得大学：

早稲田大学（指導 平澤 茂一 教授）
現在の所属：湘南工科大学情報工学科

要 旨

近年の情報化社会の進展にともない情報を取り扱うシステムは益々大規模化、複雑化しつつある。しかしながら、このような情報システムは明確な評価基準を持たないままいくつかの要因を総合して経験的或は直観的に設計、評価されているのが現状である。さらに、人間を系に含むような情報システムに於ける曖昧性の評価、互いにトレードオフ関係にある要因の相互関係の評価は非常に難しい課題とされている。特に、従来許されなかった曖昧さに注目し、これを積極的に許容することによって「柔らかい」システムを構築する問題が多く存在している。例えば、大規模情報検索システムにおいて、検索結果の曖昧さを許容することによって検索効率を向上させるような問題などはその典型といえる。従って、理論的な裏づけを持った評価基準を確立し、これを情報システム構築のための指針にすることは極めて重要な問題である。

情報システムに関する従来の研究は、そのサブシステムの解析評価可能な部分について詳細に考察したミクロな立場からの研究、あるいは近似的な解析モデルやシミュレーション技法を用いたマクロな立場からの研究は数多く存在する。しかしながら、いずれもほとんどの研究は特定の変数に着目したシステムの挙動について解析されており、共通の視点からシステム規模をパラメータとして統一的に解析、評価する方法は未だ研究されていない。

本研究では、このような情報システム構築の際生じる問題に対して、新しいモデル化と評価方法を提案し、具体的な情報システムに適用する。すなわち、曖昧さやトレードオフ関係にある要因を含む情報システムが、システム規模増大時に示す特性を評価するためのモデルである。このモデル提案のためには、情報を扱うための基礎理論である情報理論に基礎をおいている。情報源符号化のモデル、特に歪を許容した情報源圧縮の基礎理論である情報縮約理論に基づいて、互いにトレードオフ関係にある圧縮効率と歪の関係の評価を応用し、大規模化を前提とした情報システムに適用したものである。このように本研究では、一貫して

種々の情報システムを対象とし，かつ情報縮約理論による解析，考察を展開する．

第1章においては，情報縮約理論，特にその根幹をなす源符号化定理の性質を要約するとともに，本研究の出発点であり主たる背景となっている質問応答システム(Question-answering Systems；以後QAシステムと呼ぶ)の視点を明らかにする．これは，情報を蓄積し，検索を行う過程において，ユーザの発する質問に対する回答の誤りを許容することにより情報の蓄積効率向上を狙いとしたものである．そこで，データの蓄積容量と質問に対する回答の誤り確率の関係を，正規化されたレート歪関数を用いて定量評価され，その結果，ある種の誤り確率を許容することにより情報蓄積効率向上の可能性の存在を示唆している．しかしながら，このモデルにおいては，対象とする情報システムが質問応答によるものに限定されている点，適用条件の厳しさなどから広範囲な応用がなされていない．その結果，システム規模をパラメータとしたトレードオフ関係の変化を論じるための情報システムの統一的なモデル化の必要性を示すとともに，本研究の視点，位置づけを明らかにする．

第2章においては，情報縮約理論に基礎をおくQAシステムのモデルを再構築することにより，その拡張と一般化を行なう．まず，対象とする情報システムに投入すべき投入資源とそれによって変化するシステム歪を定義し，それらの関係を評価するモデルとしてトレードオフ評価モデル(Trade-offs Evaluation Model)を提案する．次に，従来のQAシステムとの比較においてその応用範囲の拡大とそれによって得られる有効性を示す．まず，トレードオフ評価モデルは対象とする情報システムに対して，投入資源と歪が定義でき，システム規模増大時の両者のトレードオフ関係の変化に注目する．対象とする情報システムの特徴はそのシステムの規模により表現されたトレードオフ関係のみで表わすことができない．その結果，情報システムの優劣は，システム規模増大時にもたらされる僅かな劣化を許容することにより，システムに投入されるべき投入資源の大幅な削減が実現できるか否かにより評価される．評価基準として，柔軟性(Elastic Condition)，自明的柔軟性(Trivial Elastic Condition)を定義し，その解析，評価の方法を明らかにする．すなわち，対象とするシステムが柔軟性もしくは自

明的柔軟性を満足するときのみシステム規模に対してトレードオフ関係が効果的に変化し，そのシステム構築の有効性が保障されることを示す．さらに，多くの情報システムに於て，僅かな投入資源の付加によりシステムの歪の大幅な改善が実現できるか否かによって評価される問題にも適用できるようにモデル化の条件を拡張する．その結果，歪の増大，すなわちシステムの劣化を許容することによる投入資源の削減を図る「圧縮モデル」と，投入資源を付加することを許容することによる歪の減少，すなわちシステムの改善を図る「付加モデル」に分類される．また，レート歪関数導出において，情報縮約理論の基本的視点であるランダム符号化による写像関係に限定せず，その対象とするモデル化の条件を緩和することのできることを示す．従って，本研究においては情報システムは4種類のタイプに分類し解析を行い，3章以降の具体的なシステム解析と対応づける．

第3章においては，システムの劣化を前提としての投入資源削減を目的として，データ蓄積効率と検索時の誤りが問題となる典型的な2値検索問題を取りあげる．そこで検索問題に於てデータ数が増大するとき記憶容量と誤りとの関係がどのような特性をもつか明らかにする．典型的な2値検索問題とは，答え方を{Yes, No}に限定した

テーブル探索問題(Table look-up problem)，完全符合問題(Exact match problem)，全2値問題(A11 binary-valued problem)の基本的ではあるが適用範囲の広い3種類の問題を指す．その結果，データ数増大時にのみが自明的柔軟性をもつことを明らかにする．さらに，各々に対して論理演算によって合成された質問を定義して同様の解析を行い，質問の合成方法によってシステムの特性が逆転することを示す．

第4章においては，投入資源付加によるシステムの歪の改善を目的とする情報システムとして，重複ファイル配置の問題について新しい評価方法を提案する．すなわち，分散型ネットワークにおけるノード数が増大するとき重複ファイルコストと検索に要する通信コストの関係がどのような特性をもつかを明らかにする．特に，ネットワークの基本トポロジであるバス型，リング型，スター型を基礎としたサブシステムに対して，両者のコスト関係がどのような特性をもつかを評価し，システム全体の構築方法を示す．その結果，柔軟

性を有する条件のもとにスター型を基礎とするサブシステムをバス型およびリング型などの構造の中に分散させる基本設計が望ましいことを明らかにし、同時に、現実のネットワークの効率評価との整合性も実証する。

第5章においては、大規模マスクファイルにおいて、質問検索用索引ファイルを2次ファイルとして構成するか否かの問題に対して、マスクファイルの再構成による検索効率維持の問題を扱う。ここで、ファイルはできるだけレコードの一連検索性を有するように編成される。一連検索性を有するファイルとは、任意の質問項目に対して該当するレコードを逐次に取り出すことの可能な、有用で検索時間の面で最も効率のよいファイル編成を指す。これは任意の質問項目に対して実現することは不可能であるが、全体のファイル構成に冗長性付加、すなわち記憶容量の増加を許容してその特長を保持しようというものである。そこでレコード数が増大するとき、その冗長構成と検索時間との関係がどのような特性をもつかを明らかにする。その結果、レコード数の増大に対して柔軟性をもつ方式を明かにし、ある検索時間以内という条件のもとでの有効な構成方法を提案する。

第6章においては、情報システムが多種多様な検索要求に対して、真に必要な情報が出力されない検索もれと、不必要な情報が出力される検索ノイズをいかにして抑制するかという出力制御問題をについて考察する。一般には、これらを同時に解消する方法を見いだすことは極めて困難な問題とされている。これら2つの相反する制御を行なうために、検索対象を下位レベルのカテゴリと、それらのグループとしての特徴を示すクラスタという上位レベルの階層を導入し、そのクラスタサイズを可変にする情報システムを提案する。その結果、記憶データ数を増大させたとき、クラスタを可変にすることによる記憶容量の増大と検索もれ及び検索ノイズとの間の関係がどのような特性をもつかを明かにし、柔軟性の視点から提案モデルが有効であることを示す。特に、重複を許した階層構造が、検索もれに対して有効に機能する。

第7章においては、全体を総括し、本論文で提案したモデル化が、情報を取り扱うシステムの中に存在する基本的なトレードオフ関係を明確に評価することのできる有効な手段であることを示す

とともに、情報理論の適用範囲の拡大とその制約について展望する。

モデル化について、別の視点からの考察も含めたものを、早稲田大学システム科学研究所紀要に早稲田大学平澤茂一教授との連名でまとめました。(1990, No. 21, pp. 147-190)

情報系新学科紹介
明治大学理工学部情報科学科

荒川 薫（明治大学）

明治大学理工学部には、1989年4月に、新しく情報科学科が新設されました。場所は、川崎市多摩区の明治大学生田キャンパス（小田急線生田駅下車）です。このキャンパスは、緑豊かな高台に位置し、環境も快適です。

本学科では、主として情報科学のための基礎理論、コンピュータのソフトウェアとハードウェア、情報システムとその応用、そして他分野との境界領域に関する教育・研究を行なっています。さらに、コンピュータを十分に活用した演習と実習を重視しています。写真は、実習室で、学生たちがワークステーションを用いた実習に励んでいる様子を写したものです。また、これらの教育・研究を通して、国際性豊かで創造性に富んだ、幅広い視野を有する情報科学の専門家を育成することを目的としています。

現在、この学科には、次のような研究室があり、活発に研究が行なわれています。

- 1) コンピュータ基礎研究室（駒宮安男教授）
コンピュータの基礎を論理的に解明。特に、論理数学や新しい喋れるプログラミング言語などを開発。
- 2) 情報基礎研究室（中村昭教授）
情報の基礎について数学的に解明。例えば、言語理論やグラフ理論などを研究。
- 3) 論理デバイス研究室（富沢一隆教授）
コンピュータの素子の開発を理論的に研究。特に、物性理論に基づく論理デバイスのシミュレーションを研究。
- 4) システム科学研究室（向殿政男教授）

システムの基本的性質について研究．特に，あいまい（ファジイ）な情報の処理システムを研究．

5) ソフトウェア基礎研究室（疋田輝雄教授）

ソフトウェアのための基礎理論とソフトウェアの構成について研究．例えば，人工知能用プログラムの開発など．

6) コンピュータ設計研究室（藤原秀雄教授）

コンピュータのハードウェアの設計．特に，故障のテストが容易で，少しぐらいの故障に耐えられるコンピュータの設計．

7) 設計自動化研究室（山田輝彦助教授）

コンピュータのCADと，そのための新しい手法の開発．

8) ソフトウェア科学研究室（石畑清助教授）

コンパイラやOSの研究を行い，各種実用的なソフトウェアシステムを開発．

9) ロボット科学研究室（武野純一助教授）

ロボットに関する研究．小型ロボットの制作と制御．

10) 情報理論研究室（荒川薫講師）

情報理論とそれに基づく各種の応用研究．例えば，医療情報処理やニューラルネットワークの研究．



写真 学生実習室

コーヒーブレイク

Shannon は越えられるか

話を進める前に Shannon を越えるとは何を意味するかを述べておく必要がある．周知のように Shannon は通信の過程の科学的及び技術的設計理念とも言えるべき数学的理論を体系化した．その理論体系は直接，現実の通信システムの設計に適用されるわけではない．むしろ設計理論のための哲学

を与えるものと考えらるべきである．したがって Shannon を越えるとは Shannon の思想を越えねばならない事を意味する．

Shannon の思想の根元はエントロピーと符号化である．エントロピーで測られる情報は符号化，いわゆる情報の加工に直結されている．この2つの定理を基本思想として数多くの通信系の設計理論が構築され，また構築され続けている．本学会の多くの方々はこの分野で活躍されている．

Shannon を越えようとする試みもまた少なくない．その代表は意味論である．

Shannon はむしろ情報の意味を除く事によって情報を定量化した。したがって最も身近な "Shannon を越える" はこの意味を公式化することである。これは Shannon の公式化の直後から試されているが、成功の例はまだ聞かれない。しかし、これは研究すべき重要なテーマである事はまちがいない。

第2はエントロピー測度の拡張である。このテーマも数え切れない程の研究が行われている。これらの大半は Shannon が最も重視する符号との対応を無視して進められる。これらの理論がたとえ Shannon のエントロピーを拡張し、Shannon エントロピーの適用外を記述したとしても、符号との対応原理がない限り通信過程として Shannon を越えることにはならないであろう。

第3は物理過程との融合である。初期の試みは熱統計力学と Shannon エントロピーとの一体化であった。特にブリュリアンの負エントロピーと熱力学の研究は多くの成果をもたらした。しかし現在、その理論は Shannon 理論以上の何ものをも創生していない。

それは、物理学が自然界の記述を目的とした理論体系であることによるものと思われる。事実、ブリュリアンの理論はむしろ物理学に Shannon 理論を取り込もうとした試みであることから結論づけられる。

以上の簡単な解説からでも Shannon を越える事は極めて困難である事がうかがい知れる。Shannon の理論は情報の科学の出発点における最も堅固な基盤である事は疑いのない所であろう。といって万人が満足しているとも言えない。

上記3つの側面からのアタックで第3の物理学との融合が近年、新しい成果を挙げつつある。それは Shannon の基本理念は変更せず、情報と物理現象を不可分とする試みである。これによって、Shannon の理論以上のものが創生されるとすればそれは Shannon を越えたと言えるであろうが、単に適用範囲を広げたのみではそうとは言えない。

ここにその一例を示そう。“光通信過程の受信端でその光通信過程の伝送情報量は0から無限大まで自由に制御できる。”すなわち伝送情報量は送信側と通信路には強く依存しない。これは拡張とみなすか、越えたのかは読者の判断におまかせする。

(広田 修)

会合案内

I S I T A ' 9 0

開催期間:1990年11月27日~30日

Reception(Welcome Party):

11月26日18:00~20:00

Evening Special Session:

11月27日16:00~18:00

(Guest Speakers;Dr.Forney and Prof.Massey)

Banquet:

11月28日19:30~22:30

Social Activity:

11月29日夕 Sunset Cruizing & Soft dance

開催場所:SHERATON WAIKIKI HOTEL, HAWAII, USA

発表件数:295件(内、日本から110件)

セッション数:72セッション

参加国数:22ヶ国

組織委員長:堀内 和夫(早大)

実行委員長:森 真作(慶大)

Shu Lin (ハワイ大)

プログラム委員長:今井 秀樹(横浜国大)

参加申込先:小沢 慎治(慶大)

Phone: 045(563)1141 Ex.3321

Fax: 045(563)3421

E-mail: ozawa@ozawa.elec.keio.ac.jp

VISICOM'91 Fourth International Workshop or PACKET VIDEO

開催期間:1991年3月18日~1991年3月19日

開催場所:京都

連絡先:

Secretariat of PACKET VIDEO'91

c/o Inter Group Corp.

Akasaka Yamakatsu Bldg., 8-5-32

Akasaka, Minato-ku, Tokyo 107, Japan

Phone: +81-3-479-5311

Fax: +81-3-479-2475

VISICOM'91 1991 Picture Coding Symposium

開催期間:1991年3月21日~1991年3月23日

開催場所:東京

連絡先:

Secretariat of PCS'91

c/o Inter Group Corp.

Akasaka Yamakatsu Bldg., 8-5-32

Akasaka, Minato-ku, Tokyo 107, Japan

Phone: +81-3-479-5311

Fax: +81-3-479-2475

SITA' 89 報告

実行委員長 畑 雅恭 (名古屋工業大学)

第 12 回の情報理論とその応用シンポジウムを愛知県犬山市の名鉄犬山ホテルにおいて、1989 年 12 月 6 日より 9 日まで開催し、154 編の論文発表とアジア、北米、ヨーロッパの 7 ケ国からの参加を含め 300 名を超える参加者が得られ盛会裏に終了した。このことは、本シンポジウムが諸先生方の御努力により発足して以来、この 12 年間にいかに重要な集まりとして産・学の間に根付き、また国際化しているかを如実に物語るものであり、同慶のいたりである。

とりわけ国際化については、1988 年神戸で開催された I S I T を契機として、第 10 回江ノ島における会議より急速に進展し、本年度の I S I T A の開催に引き継がれてきていることは御存知の通りである。なお、おりしも開催地である犬山市では市制 35 周年を迎え国際文化、国際観光都市を標榜されており、この面から松山犬山市長をはじめとして開催地域より多大の協力が得られたことも幸いであった。

また、特別講演については、本シンポジウム名誉顧問の本多波雄豊橋技術科学大学長より情報理論研究の歩みと将来について、またハンガリー科学アカデミーのシザール博士の有意義な講演と、さらに犬山市にある京都大学霊長類研究所の久保田教授より脳の神経情報処理について講演頂き、それぞれ大きな反響と好評を得た。また、恒例になった夜のワークショップでも 7 会場から遅くまで熱気ある討論が続けられた。

東海地域で当シンポジウムが開催されたことは、地域にとっても意義の深いことであった。御指導、御支援頂いた堀内会長をはじめ多くの関係各位に

深く御礼申し上げる次第である。

情報理論とその応用学会 1989 年度総会報告

平成元年度庶務理事 今井 秀樹 (横浜国立大学)
森 真作 (慶應大学)

平成元年 12 月 8 日 (金) より犬山市「名鉄犬山ホテル」にて情報理論とその応用学会 1989 年度総会が実施された。議事は次の通りであり、議事 2~8 についてすべて承認された。

1. 会長あいさつ (堀内和夫本会会長より)
2. 1988 年度事業報告・収支決算報告
(SITA'88 を含む)
3. 1989 年度事業中間報告・中間収支決算
4. 1990 年度事業計画・収支予算案
5. SITA'89 中間報告
6. SITA'90 開催計画
7. 1990 年度役員承認の件
8. その他 (SITA'87 決算報告を含む)

なお総会に先だって 1990 年度役員の選挙が実施され、1990 年度役員構成は下記の通りとなった。

1990 年度役員

	氏 名	所 属	
会長	堀内 和夫	早稲田大学	留
副会長	辻井 重男	東京工業大学	留
	有本 卓	東京大学	新
理事			
(無任所)	原島 博	東京大学	留
	丸林 元	長岡技術大	新
(庶務)	森 真作	慶應大学	留
	中川 正経	慶應大学	留
(会計)	田崎 三郎	愛媛大学	留
	藤原 謙一	三菱電機	留
(編集)	田中 初一	神戸大学	留
	畑 雅恭	名古屋工業大	留
(企画)	韓 太舜	専修大学	留
	小林 欣吾	電気通信大学	留
監事			
	岩垂 好裕	日本電気	留
	古賀 利郎	九州大学	留

(留：留任，新：新任)

本総会開催にあたって多大のご尽力，ご支援を
頂いた畑 雅恭実行委員長をはじめとする SITA'
89 の実行委員会各位，ならびに細かく気を配って
頂いた本会事務局余語菜穂子さん（早稲田大学堀
内研究室）に感謝致します．

役員立候補の受付

当学会では毎年役員の交代に伴う役員選挙を実施
しております．次回の選挙は 1991 年 1 月の予定で
すが，次回から理事会推薦の候補以外に立候補者
も候補になることが可能になりました．但し，正
会員であることが資格になります．立候補希望の
方は本年 11 月末日までに学会事務局宛に文書によ
ってその意志をお伝え下さい．なお，立候補可能
な役員は会長，理事，監事のいずれかであり，希
望の役職名もこの中から一つ選択してその時にお
伝え下さい．

投稿募集

ニューズレターの投稿を大いに歓迎致します．
原稿をフロッピーディスクで送って下されば幸い
です．この場合は，編集の都合上，一太郎 Ver.3 に
よる文書ファイルか MS-DOS の標準テキスト・フ
ァイル(5'2HD または 5'2DD)でお願い致します．フ
ロッピーディスクはお返し致します．

投稿並びに次号のニューズレターに関するお問
い合わせは下記宛にお願い致します．

田中 初一（編集理事）

〒657 神戸市灘区六甲台町 1-1

神戸大学工学部電気工学科

Phone: 078(881)1212 EX5086

Fax : 078(861)7679

畑 雅恭(編集理事)

〒466 名古屋市昭和区御器所町

名古屋工業大学電気情報工学科

Phone: 052(732)2111 EX454

Fax : 052(733)6589

吉田 進(編集幹事)

〒606 京都市左京区吉田本町

京都大学工学部電子工学科

Phone: 075(753)5317 (直通)

Fax : 075(751)1576

大石 進一(編集幹事)

〒169 新宿区大久保 3-4-1

早稲田大学理工学部電子通信学科

Phone: 03(203)4141 EX73-3424

Fax : 03(200)2567 (理工学部)

編集後記

今回は幹事会で企画検討した学位論文紹介，コ
ーヒーブレイク，学科紹介を中心に編集致しまし
た．この他に，今年度の行事カレンダーを作成す
る予定でしたが，幹事（大石）の怠慢により発行
が大幅に遅れたため，この企画はうまく生かせま
せんでした．情報をお寄せ頂きながら掲載できな
かった会合案内がいくつかありましたことを深く
お詫び申し上げます．なお，コーヒーブレイクの
テーマとしてふさわしいものがございましたら投
稿募集先宛お送り頂ければ幸いです．（大石 記）

情報理論とその応用学会事務局（早稲田大学理工学部内研究室内）

〒169 新宿区大久保 3-4-1 早稲田大学理工学部電子通信学科

Phon : 03(203)4141 EX73-3420

FAX:03(200)2567(理工学部)