No. 11 1991年7月25日発行

情報理論とその応用学会ニューズレター

巻頭言

会長 辻井重男
1991年7月9日

血液型に例えれば、A、B、O型すべての面の魅力を兼ね合わされた堀内先生の後を継いで、会長に選出され、非力の私に務まるか否か戸惑っている次第です。

１３年前に本学会の前身である研究会が組織され、泊まりがけのシンポジウムを開催してきたことは、電子情報通信学会と云う大学会の活性化にも良い刺激を与えたことは記憶に新しいところですが、学会設立後は滑川元会長、堀内前会長の下で組織も整備され、運営も軌道に乗り、小回りの効く小学会として活動の場を広げております。例えば、レクチャーノートシリーズの発刊企画もほぼ固まり、あとは執筆者の努力に待つと云った状況にあります。

本会のシンポジウムは国際的にも注目を集めており、好むと好まざるとにかかわらず、環太平洋にまたがる学会に育っていく宿命にあるように予想されます。開国政策を積極的に打ち出すか、なるべく鎖国の夢をむさぼるのが良いか皆様のお考えをお寄せ頂ければと存じます。

次に本学会は“応用”を冠していることもあって対象分野は可成り広いと云えますが、中核となる理論分野について現状のまま進めていけばよいか、あるいは、“情報学理論”とでも云うべきものに広げていくかについても御意見を頂ければ幸いです。

終りに、今年のシンポウムは嵩先生（阪大）を実行委員長に、田中先生（神戸大)、長沢先生（鹿児島大）等の御努力で、１２月の鹿児島開催に向けて準備が進められております。お目にかかれるのを楽しみにしております。

ＳＩＴＡ'９１にむけて

実行委員長　嵩　忠雄（大阪大）

本年の情報理論とその応用シンポジウム（ＳＩＴＡ'９１）は，平成３年１２月１１日（水）から１４日（土）まで，鹿児島県指宿市の指宿観光ホテルにて開催されます．平成３年３月に実行委員会が発足して以来準備を続けて参りましたが，開催要領が決定致しました．下記のような日程ですので奮ってご参加下さい．

７月　１日（月）	第１回案内送付開始
８月　９日（金）	発表参加申し込み締切
８月２６日（月）	第２回案内， 原稿用紙送付開始
９月３０日（月）	最終原稿締切
１０月３１日（木）	第３回案内送付開始

内容は，おおむね例年と同じで口頭発表形式を予定しております．最近のシンポジウムの論文の傾向としては英文での投稿が増えてきております．シンポジウムの国際化を一層進めるためにもこの機会に是非，英語での論文投稿をお願い致します．また，今回のシンポジウムでは，「２１世紀における情報基礎技術」をテーマに５件程度の招待講演を行うチュートリアルセッションを電子情報通信学会情報理論研究会との共催で予定しております．

当事務局の個人名簿に記載されている方には，７月初めに参加案内・講演募集案内をお送り致しました．名簿の不備，郵送費節約のため，資料をご所属ごとに一括してお送りしている場合もございますのでご了承下さい．尚，お手元に届いていない方は，お手数ですが事務局までご請求下さい．また，事務局の個人名簿の誤りにお気づきの方，あるいは変更のある方は，次回からの連絡を正確に行うために是非その旨ご連絡下さいますようお願いします．

連絡先:
〒560　豊中市待兼山町 1-1
大阪大学基礎工学部情報工学科
嵩研究室内　SITA'91 事務局
藤　原　　融
TEL.06-844-1151　　(内線 4806)
FAX.06-843-5943

大学院博士論文紹介

A Study on the Construction and Analysis of Substitution Boxes for Symmetric Cryptosystems

（対称暗号系のための置換関数の構成と安全性評価に関する研究）

金　光兆
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
韓国電子通信研究所

要旨

対称暗号系（特にブロック暗号系）における置換関数は暗号系の非線形性と安全性を決める非常に重要な構成要素である．ある置換関数において入力のどの１ビットの変化も全ての出力のビットを１／２の確率で変化させる場合，その置換関数は強なだれ規準(Strict Avalanche Criterion)を満たすという．

本論文では，強なだれ規準を満たす置換関数は暗号学的に望ましい性質を持っていることを証明すると同時に，そのような関数に多様な構成方法があることを示した．

例えば，強なだれ規準を満たす２進置換関数は二つの関数の連結，直積，Dyadic shift を用いることにより構成し，拡張することが可能である．更に，より詳細にその性質を論議するために，強なだれ基準に次数を定義し，最大次数の強なだれ規準を満たす全単射置換関数の構成方法を提案し

た.

また，これまで符号理論，論理構成，スペトル拡散通信等に利用されているベント関数の暗号学的性質を調べ，強なだれ規準を満たす２進置換関数と深い関係があることを明らかにした．つまり，最大次数の強なだれ規準を満たす２進置換関数は全てベント関数であることとベント関数は少なくとも零次強なだれ規準を満たす２進置換関数であることを示した.

ついで，実際的な応用のために，強なだれ規準を満たす関数を用いて DES-like S-box を設計する方法を提案し，現在の DES に用いられている S-box より暗号学的性質が優れていることを実験的に確認した．設計した DES-like S-box を DES の S-box の代わりに用いて得られる暗号系と，FEAL 暗号系，Multi2 暗号系，DES 暗号系との暗号学的性質を比較し，総合的に見て新しい暗号系が優れているという結果を得た.

本論文の研究結果はブロック暗号系の設計と解析には直接的に有用であリ，ストリーム暗号系の設計と解析にも間接的に役に立つ思われる.

::::::::::::::::::::::::::::::::::

Principles for Designing Secure Block Ciphers and One-Way Hash Functions

（安全なブロック暗号及び一方向性ハッシュ関数の設計に関する研究）

鄭　玉良

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

The University of New South Wales

要旨

本論文では安全な情報システムの構成・運営に必要不可欠である共通鍵暗号及び一方向性ハッシュ関数の設計について研究する。共通鍵暗号を用いることによって情報の安全な交換や保存などの機能を実現することができ、情報の守秘性が達成できる。一方、一方向性ハッシュ関数は長いファイルを短い系列に圧縮し、かつ、この短い系列に圧縮される異なる長いファイルを見つけることが困難である性質を持っている。この性質を利用することによって、情報の認識の達成及び向上が実現できる。

本論文は PART 1 と PART 2 の二つの部分からなっている。PART 1 は安全な共通鍵暗号の設計法に関するもので、PART 2 は一方向性ハッシュ関数の構成法に関するものである。２つの部分の概要は以下に示す。

PART 1 では、まず１つのランダム関数から３段の DES-like 変換だけでは、疑似ランダム置換を構成することが出来ないことを示す。この結果によって、大西さんによって証明された２つの互いに独立なランダム関数から３段の DES-like 変換で疑似ランダム置換が構成できる結果が最適であることが明らかにされる。

続いて、PART 2 でいろいろな暗号学に役立つ変換を提案し、その中で TYPE-2 変換が最適なものであることを証明する。TYPE-2 変換を用いて安全性が保たれる暗号系を構成し、そのいくつかの実用的な変形版を提案する。これらの結果によって、理想的な暗号系を構成する目標に大きく一歩近づいたことになる。

PART 2 では一方向性ハッシュ関数に関して研究する。まず、具体例を用いて、疑似ランダム系列生成器の構成と一方向性ハッシュ関数の構成の間に双対性があることを示す。この双対性を利用して、任意の一方向性置換から、従来の構成法よりはるかに簡単な一方向性ハッシュ関数構成法を提案する。この簡単な構成法の応用として、DES 及び Rabin 関数から２つの実用的な一方向性ハッシュ関数を示す。

そして PART 2 では従来の一方向性ハッシュ関数を含めたいろいろなバーションの一方向性ハッシュ関数を定義し、それらの間の関係を考察する。ある種の弱い一方向性ハッシュ関数が強い一方向性ハッシュ関数に変換できることを示した上で、いくつかのバーションの一方向性ハッシュ関数の間に真の包含関係があることを明らかにする。

最後に本論文では解決できなかった問題をまとめ、これからの課題を言及する。

ミニワークショップ
符号理論とその応用
報告

森井　昌克　（愛媛大学）

１９９１年5月１４日から翌１５日にかけて，本学会主催のミニワークショップ「符号理論とその応用」が愛媛大学城北キャンパス（愛媛県松山市）にて開催された．今回の本ミニワークショップは符号理論，特にその中でも符号の構成法および復号法に関する研究，さらにその理論的応用に関する研究を中心課題として７件の講演を行い，その講演を題材に活発な議論が行われた．

本ミニワークショップの企画は，開催幹事である笹野博（近畿大学理工学部），常盤欣一朗（神戸大学工学部），森井昌克（愛媛大学工学部）の３氏であるが，そもそものきっかけは，その３氏の酒席での雑談から始まっている．３年前に開催された神戸でのＩＳＩT' 88 以来，本学会が主催，あるいは関与した情報理論に関する国際会議がいくつか開催され，また情報理論とその応用シンポジウム（ＳＩＴＡ）も回を増す毎に盛会となり，毎夏に開かれる情報理論とその応用ワークショップ（ＷＩＴＡ）も軌道に乗っている．しかしながら，情報理論の一分野である符号理論の分野に限ってみると必ずしも盛んとは言い難い．確かに毎回のＳＩＴＡでは複数のセッションが符号理論に割り当てられ（前回の蓼科でのＳＩＴＡでは３６セッション中６セッション，発表件数１３９件中２４件），活発な分野の一つと見なせなくはないのだが，ＩＳＩＴ 等に比較していま一つの感がある．特に代数的符号理論やその基礎理論は一時に比べて新しいテーマ（代数曲線上の符号等）がいくつか出てきているものの，研究がトーンダウンしているように感じられる．また，盛んとは言い難いもう一つの理由としては．　ＷＩＴＡが当初，その名が「符号理論とその応用ワークショップ（ＷＣＴＡ）」であり，1988 年から現在のＷＩＴＡに改名した経緯もある．そのようなことをブツブツと言いながら，結局，符号理論の活発な（元気な）研究者を集めて，情報を交換し，檄を飛ばし会うことが最良であろうという結論になり，この企画となったものである．

以下，本ミニワークショップの開催内容報告をその講演（講演者）にそって行う．

１．誤り訂正符号とその応用
（笠原正雄，京都工芸繊維大学工芸学部）

通信理論および誤り訂正符号の歴史的経緯について述べ，誤り訂正符号とその基礎となる数論およびアルゴリズムの他の分野への応用について詳細に解説を与えた．　講演後には，応用例を詳細に，しかも簡潔にまとめた表に関して，活発に討論がなされた．

２．代数符号の復号法とその周辺
（森井昌克，愛媛大学工学部）

ＢＣＨ符号やＲＳ符号の代数的復号法である Peterson 復号法や Berlekamp-Massey 復号法を説明し，さらに最近提案された新しい復号法である剰余復号法に対して詳細な解説を与えた．また暗号理論やディジタル信号処理への復号法の応用について説明を与えた．講演後には剰余復号法の利点について活発な議論が行われた．

３．誤り訂正符号の VLSI 自己テストへの応用
（岩崎一彦，千葉大学工学部）

ＶＬＳＩの組み込み自己テスト法について解説し，そのＶＬＳＩの故障がどのようなテスト応答での誤りを生成するかについて述べ，その誤りの見逃し確率（エイリアス確率）と符号理論の重み分布との関係について詳細な説明を与えた．　講演後，フォールトトレラントの問題と符号理論の関係が議論となり，互いに他の結果を応用することの重要性が指摘された．

４．直積ファイルの分散配置法
（藤原融，大阪大学基礎工学部）

データベースシステムにおける検索，更新を行うための基本操作の一つである部分照合質問，すなわち指定された属性に指定された値をもつレコードをファイルから検索する操作を効率的に行う問題に対して，符号理論の応用が極めて有効であることを指摘し，実際にその問題に対して有効な

解法を与え，解説を行った．　先の講演と同様，符号理論の応用に関して活発な議論が行われた．

５．逐次復号法に適した畳込み符号の構成の検討

(大橋正良，KDD 研究所)

最小自由距離が大きく，かつ列距離関数特性に優れた畳込み符号の探索を目的として，フィードバックを伴った畳込み組織符号に着目し，従来知られている符号よりも優れた符号を導出するとともに，その構成法について解説した．この構成法では，代数符号の復号法である Berlekamp-Massey アルゴリズムが用いられ，復号法の応用としての観点からも興味が持たれ，活発な議論が行われた．

６．一方向バイト誤り訂正/検出符号

(斉藤雄一，横浜国立大学工学部)

非対称通信路における誤り訂正/検出符号について概説し，特に一方向バイト誤りを訂正するための必要十分条件を示し，さらに具体的な符号構成法を与え，その解説を行った．講演後の討論では，非対称誤り訂正符号の現在の研究状況について，その直面している問題とともにその応用について議論が行われた．

７．代数幾何符号とその復号アルゴリズムについて

(三浦晋示，NEC C&C 情報研究所)

Varsharmov-Gilbert 限界を越える代数幾何符号の存在性と具体的な曲線上で構成される代数幾何符号の説明が与えられた．さらにその符号を復号するという意味と具体的な実現される復号アルゴリズムについて解説が行われた．特に復号アルゴリズムについては現在，必ずしも有効な一般的方法が与えられていないことが指摘され，その構成について議論が行われた．

以上の講演を中心とした討論会の他に，１４日夕刻から愛媛大学職員会館にて懇親会が行われ，符号理論やそれぞれの研究に対する考えや意見が和やかな雰囲気のもとで交わされた．

最後に，本ミニワークショップの参加者，特に活発に討論に参加して頂き，雰囲気を盛り上げて頂いた，横浜国立大学工学部　今井秀樹教授，ならびに神戸大学工学部　田中初一教授に感謝する．さらに会場の手配，設営等に関してご助力頂いた愛媛大学工学部　田崎三郎教授（本学会監事），同　山田芳郎助教授に深謝する．また，ミニワークショップの前日より開かれた電子情報通信学会情報理論研究会から引き続いて，会場設営等を助けて頂いた愛媛大学工学部電気電子工学科田崎・山田研究室，および同　情報工学科森井研究室の学生諸氏に感謝の意を表する．

国際会議報告

1991 IEEE International Symposium on Information Theory

斎藤　雄一（横浜国大）

本会議は 1991 年 6 月 24 日(月)から 28 日(金)にわたって Hungary, Budapest にある Budapest Convention Centre で開かれました．会議に先立ち 23 日には Registration と Welcome Reception が行われ，26 日(水)は朝の Plenary Session のあと参加者たちは Excursion を楽しみました．他の４日間は，朝 8 時からの Plenary Session に始まり，前半は 12 時 20 分まで，3 時 40 分の長い昼休みをはさんで，後半は 4 時から 7 時まで，というスケジュールで論文発表が行われ，25 日（火）夜には Recent Result Session, 27 日（木）には Banquet が催されました．

従来の ISIT の Proceedings は Abstract のみという簡単なものでしたが，今回は 1 ページの Extended Abstract （信学会全国大会程度のもの）になりました．従来形式が良いか，今回の形式か，という投票も行われました．投票結果はまだ発表されていませんが，発表論文に関する情報を少しでも多く得たいという意味で，筆者は今回の形式に賛成しています．

正確な数字はわかりませんが，参加者は約 500 名で，例年と異なる点はソ連からの参加者が 30 名程度と多かったことでした．407 件の論文が並列に 7 セッションに分かれて発表され，全セッション数は 53 でした．なお，毎回恒例の Plenary Session として今回は以下のような招待講演が行われ

ました．参加者たちは熱心に聞き入り，時にはメモをとる姿も見受けられました．

Monday, June 24
  Janos Korner: A Generalized Shannon Theory for Zero Error
Tuesday, June 25
  Donald Ornstein: Universal Data Compression from Ergodic Theory Point ov View
Wednesday, June 26
  Murat Kunt: HDTV
Thursday, June 27
  A. J. Viterbi: Shannon Theory from a Communication Engineering's Perspective
Friday, June 28
  Ronald Graham: Aspects of Randomness in Graphs and Hyergraphs

さて，今回プログラムにあった論文の中で最も注目をあびたのはソ連の A. L. Turkin and V. I. Korzhik による“The practically Optimal decoding algorithm of arbitrary linear codes over BSC, having polynomial-time complexity”であると思います．タイトルを見ただけで符号理論の研究者なら興味深く感じるはずですが，この発表は暗号研究者にとっても非常に重要な意味を持っています．タイトルに書かれていることが本当ならば McEliece の公関鍵暗号系が多項式時間で解読できることになるからです．さて内容はというと，筆者には全く理解できず，残念ながら読者の期待に沿う報告はできません．雰囲気だけを伝えると，講演はロシア語で行われ，通訳が逐次英語に訳すという形式でした．しかし，発表後通訳が正しくないというコメントもあリ，ほとんどの参加者が理解できずに終わったという印象です．

なお，次回は 1993 年 1 月 17 日から 22 日にアメリカ，テキサス州 San Antonio で開催される予定です．

最後に，開催地の Hungary, Budapest の印象を伝えておきます．日本との時差は，日本を基準にして-7 時間，６月後半の Budapest の気候は，晴れれば今の日本と変わらず暑く，曇ると寒く上着が必要になります．雨が降った日もありましたが，空気は乾燥しています． Budapest 市は，市の中央を流れるドナウ川を境に西側の Buda 地区，東側の Pest 地区に分かれています．Buda 地区は旧王宮があり東京でいうと山の手，Pest 地区は繁華街があり下町といったところでしょう．旧王宮のある丘の上からは美しい町並みを一望することができます．ちなみに会場の Budapest Convention Centre は Buda 地区にあります．Budapest の街には自動車があふれ，排ガス規制がないのか，空気は汚れています．しかし，Budapest は飲食費，交通費の安い街です．ホテルのレストランでは 1000 円，街の普通のレストランだと 500 円も出せばお腹いっぱい食べられます．ワインも安くスーパーでは 200 円以下からあります． Budapest には地下鉄，市電，トロリーバス，バスが網の目のように走っていて料金は 30 円以下．慣れれば非常に便利な街です．

末筆ながら，この報告の仕事を笑顔で押しつけて頂いた今井先生と坂庭先生に感謝します．

随筆

『偶然の不思議』

京都工芸繊維大学
笠原　正雄

偶然とは言え、余りにも稀なことが現実に起こると、神秘的な感情におそわれるのは私だけであろうか？
Shannon のいう“十分に低い確率”とは本質的な差があるのではないかと考え込んだりしてしまう。

いま思い出すことのできる“不思議な偶然”の幾つかを紹介しよう。勿論これらのことは全て真実であるが、忙しさに取り紛れて登場者に一々お許しを頂くことができなかったので、ご氏名は全て“暗号化”させていただくことにしよう。

（その 1）

同志社中学時代、私が最も親しくしていた友人の一人であり、現在美術商を営んでいる L 氏はご両親とともに京都の下鴨から宝塚市に転居されたが、全く偶然に、私の大阪大学大学院時代以来の親友の一人である神戸大学の L 教授と閑静な住宅街で、隣り合わせに住んでおられるのである。

（その２）

緑の窓口で指定席券が二重に販売されることは新聞紙上等では見聞しても自ら経験することは極めて稀なことである。昭和 51 年 7 月のある日、私は研究室の夏季合宿に参加するために、京都の実家に立ち寄った後、京都駅始発の急行「丹後３号」に一人で乗り込んだ。この時、私は二重販売の指定券を買わされていたのであったが、そんな事とは露知らずにシートに腰を掛けていた私に、不審顔で切符の提示を求めた初老の紳士は、何と同志社高校時代のクラス担任で、お会いするのは卒業以来初めてかなと思う Y 先生であった。Y 先生は剣道部の夏季合宿のために大勢の部員を引率しておられたのであったが、神様が仕組まれたような“再会”にお互いに気付いた後は、仲良く一つの席を譲り合い、後輩諸氏に囲まれて楽しくミニ同窓会を開くことになった次第である。

（その３）

今から 10 年程前、京阪神在住のＸ先生に新幹線のひかり号のほぼ同じ席に偶然に乗り合わせたことがあった。しかも３日後の帰りの新幹線でまたまた偶然に同じような席に乗り合わせ、お互いに予め打合わせておいてもこううまくはいくまいと驚いたのであった。以後、新幹線に乗るたびにＸ先生がお乗りになっていないかと些かノイローゼになったが、勿論Ｘ先生も同じ思いであったことと思う。そんなことも忘れかけたある日、Ｘ先生からお電話があり、「…この間、親戚の結婚式に出席したら、花嫁さん、何と笠原先生の遠縁の方でしたよ！」と仰ったのである。あゝ、やはりＸ先生とは何かの“つながリ”があるに違いない、と私は思った。

海外でも同じような経験がある。20 年程前に２年間滞在した Bell 研究所の Foster 博士とも不思議なつながりがあった。ＢＳＴＪに投稿された Foster 博士の論文をたまたま査読したことがきっかけとなって、研究部門を異にする彼と親しくなったが、色々の機会に“縁”を感じさせられる人であった。そのハイライトは 1969 年 2 月 16 日、私の長女がニュージャージ州のリバー・ビュー病院で誕生した同じ日に、同じ病院で Foster 博士の長男が産声をあげた時であった。我が娘と彼の息子とが新生児室で仲良く隣り合わせになっていたのである。

さて、この話には続きがある。19XY 年の秋、くだんのＸ先生から長期海外出張のご挨拶状をいただいた。その文面を見て私は我が目を疑った。Ｘ先生の長期訪問先の一人は Bell 研究所を退職し、今や大学教授となっておられる Foster 博士であったからである！

（そして蛇足）

情報理論とその応用シンポジウムも来年で 15 回目を迎える。同じ時代に同じ分野の研究ができるのもお互い何かの不思議な“縁”があるからであろう。「シンポジウムに出てみても何時も同じ顔ぶれだ。マンネリだ！」と嘆く前に、共に議論し合える“つながリ”をより大切なものにしていきたいと願う昨今である。

第８回応用代数・代数的アルゴリズム・誤り訂正符号国際会議（AAECC-8）論文集発刊のお知らせ

阪田省二郎（豊橋技術科学大学）

前回の SITA ニューズレター（No.10）の中で紹介のありました，ＡＡＥＣＣ-8 の論文集が， Springer Verlag より Lecture Notes in Computer Science シリーズの Vol.５０８として６月に出版される予定です.

２篇の招待論文と３１篇のフルペーパからなり，その内容は，誤り訂正符号の理論・応用及び計算代数・幾何に関するテーマを中心に，符号化変調，よい相関をもつ系列，グレーブナ基底，記号・代数計算アーキテクチャ，暗号化も含んでいます.

この AAECC-8 は.１９８３年にフランス，トゥールーズで第１回が開かれてから，毎年ヨーロッパ各地で開催されてきた AAECC の第８回会議で，昨年８月初めて日本（東京）で開催されたものです. ヨーロッパ，アメリカからの参加者と共に，国内からも多数の研究発表と論文投稿がありました. また，今回の論文集の編集は日本側に任され，多数の SITA 関係者に査読等に関し多大のご協力を戴きました.

開催案内

ミニワークショップ「顔」

実行委員長　原島博（東大）

１．日時：
1991年８月２６日午後－２７日午後

２．会場：　加藤科学振興会　軽井沢研修所
住所　長野県北佐久郡軽井沢町
大字長倉字大日向５６０７－４
電話　０２６７－４５－５３１５
交通　信越線中軽井沢よりタクシー10分

３．参加登録費：
一般１０，０００円、学生５，０００円
なお、参加登録費は当日受付でお払いください。

４．参加申込締切８月１５日

５．宿泊：会場は宿泊施設が限られていますので、発表者、関係者を優先させていただきます。各自軽井沢周辺でご確保ください。

６．主催：
情報理論とその応用学会
電子情報通信学会
（情報理論研究専門委員会、ヒューマンコミニュケーション研究専門委員会)、
画像符号化シンポジウム運営委員会

７．定員：発表会場約１００名、
宿泊約５０名

８．プログラム

顔と文化：
顔と文明　香原　志勢（立大、一般教養）
顔と犯罪　市川　和義（日大、歯）

顔と心：
顔と認知　吉川佐紀子（追手門大、文）
顔と感情　千葉　浩彦（淑徳大、社会福祉）

顔とコミュニケーション：
顔と感性　宮内　淑子
（兵庫県､主任広報専門委員）
顔の演出　村沢　博人（ポーラ文化研）

顔と情報システム：
顔の自動識別　増田　功（セコム）
顔の符号化　金子　正秀（ＫＤＤ）
顔によるインターフェース
赤松　茂（ＮＴＴ）
顔のコンピュータ合成
表情の分析・合成
森島　繁生（成蹊大、工）
似顔絵の合成
輿水　大和（中京大、情報科学）
顔のグラフィックス（ビデオ放映）

９．申込先：
〒１６９　東京都新宿区大久保３－４－１
早稲田大学理工学部応用物理学科
橋本周司
Tel．03-3812-2111 EX．7776
Fax．03-5689-4637

ミニワークショップ
「データ圧縮理論：現状と展望」
「情報理論における基本的未解決問題」

川端　勉　（電気通信大学）

「データ圧縮理論：現状と展望」と「情報理論における基本的未解決問題」の二つのミニワークショップを、合同して以下のように開催致します。どうか、奮って御参加下さい。

期日：　平成３年８月２９日（木）１３時
～３１日（土）１５時３０分

会場：　ホテル新定山渓（北海道・札幌市）

内容：
前半にデータ圧縮理論関係、後半に未解決問題のテーマで、２０人前後の方に招待講演をお願いしています。初日のスケジュール終了後、懇親会を行います。また、参加者から自由に未解決問題を提示して頂く即興セッションや、特別講演も企画しています。

連絡先:
〒182　東京都調布市調布ケ丘 1-5-1
電気通信大学情報工学科
ワークショップ事務局
小林欣吾、森田啓義
TEL.　0424-83-2161 (内線 4380)
(会場、宿泊に限りがあるため電話で
確認をおとり下さい)

昼食, レセプション, バンケットの
費用が含まれます.

宿泊費　シングル 14,000 円,
ツイン　10,000 円／人・泊

ｵﾌﾟｼｮﾅﾙﾂｱｰ　浅間神社, 郷土館, 河口湖を訪れる
バスツアー. 昼食(炉端焼き)込み 2,000 円／人

参加申込締切　1991 年 9 月 30 日
問い合わせ先　〒180 東京都武蔵野市緑町 3-9-11
NTT 基礎研究所　小山　謙二
電話　0422-59-2189
FAX　0422-59-3240
主催　電子情報通信学会,
IACR　(International Association
for Cryptologic Research)

ASIACRYPT'91

期日　1991 年 11 月 11 日(月)～14 日(木)
会場　ホテルハイランドリゾート
(山梨県富士吉田市)
新宿より高速バスで 100 分
電話 0555-22-1000
FAX　0555-22-3115

内容
情報・通信システムのセキュリティ確保に有効な暗号理論及びその応用技術に関して, アジアで初めて開催される国際会議です. 内外の第一線の研究者と意見の交流や最新の交換が図れる貴重な機会を提供します. ＭＩＴの Rivest 教授らの招待講演をはじめ, 約 40 件の発表が予定されています(プログラムの詳細は 9 月に決定).

実行委員長：辻井重男(東工大)
組織委員長：笠原正雄(京都工繊大)
ﾌﾟﾛｸﾞﾗﾑ委員長：今井秀樹(横国大)

併設技術展示会
下記 9 社による, 暗号装置, 指紋判別機などのセキュリティの展示が行なわれます.
出展会社：アドバンス, ＮＴＴ, セコム, 東芝, 日本電気, 日立製作所, 富士通, 松下電気産業, 三菱電機(五十音順)

参加費　一般 50,000 円, 学生 30,000 円
(9 月 20 日以降の申込はそれぞれ１割増しになります)
予稿集及び論文集(後日発送予定),

ISSSTA'92

(IEEE International Symposium on Spread Spectrum Techniques and Applications)

１９９２年１１月２９日～１２月２日
会場：Pacific Convention Plaza Yokohama
主催：ＩＥＥＥ東京支部
電子情報通信学会スペクトル拡散
研究専門委員会
協賛：ＩＥＥＥ　ＣＯＭＳＯＣアジア
パシフィック委員会
ＩＥＥＥ　Information Theory
Society
電子情報通信学会通信方式
研究専門委員会
電子情報通信学会情報理論
研究専門委員会
Communication Chapter of IEEE UK
and Republic of Ireland Section

名誉委員長　：　丸林　元（長岡技科大）
実行委員長　：　中川　正雄（慶大）
プログラム委員長：　河野　隆二（横国大）

目的：スペクトル拡散は通信分野、特に衛星系、移動系の新しい方式として注目されるのみならず、距離測定やナビゲーション分野の新しい方式としても注目され、付加価値の高いものである。従来の方式とはかなリ原理を異にするが故に未来指向の価値観を持つ方式であり、公共的な通信網だけでなく、ユーザ主体のコンシューマ通信網にも有望と見られている。この様なスペクトル拡散技術の基礎理論から応用技術までを、内外の研究者を集めて研究発表と討論をし、この分野の発展に寄与しようというものである。

トピックス：
１．基礎理論と基礎技術
　変調・復調、同期、拡散符号、干渉信号除去、ＣＤＭＡ、情報セキュリティー、誤り訂正、アンテナ、その他
２．測距とナビゲーション
　ＧＰＳ、レーダ、その他
３．デバイスと回路
　ＳＡＷフィルタ、シンセサイザ、その他
４．応用技術
　移動通信、衛星通信、コンシューマ通信、放送、医用、その他

スケジュール：
　論文提出（２０００ワード以内）
　　１９９２年5月１日
　採否通知
　　同　　7月３１日
　カメラレディーコピー提出
　　同　　9月３０日

論文提出先：
　横浜国立大学工学部電子情報工学科
　河野隆二
　〒２４０　横浜市保土ヶ谷区常盤台１５６
　Tel. 045-335-1451, Fax. 045-338-1157
　E-mail kohno@kohnolab.dnj.ynu.ac.jp
その他の案内：
　慶應義塾大学理工学部電気工学科
　中川正雄
　〒２２３　横浜市港北区日吉３－１４－１
　Tel. 045-563-1141, Fax.045-563-3421
　E-mail nakagawa@nkgw.elec.keio.ac.jp

電子情報通信学会
「情報理論の通信システムへの応用」
小特集号（和文誌Ａ）論文募集

情報理論の通信システムへの応用
論文小特集編集委員会

通信網のディジタル化が進む今日、コンピュータのデータばかりか、本来はアナログである音声や画像などの情報もディジタル化され、伝送、記憶、処理されています。ディジタル化により、異種類の情報を統合できるばかりでなく、情報の信頼性を向上できる誤り訂正符号などのディジタル技術が応用できるからであります。特に、情報の高信頼化を直接的に実現できる誤り訂正符号は、情報通信システムの高度化を支える基本技術の一つとなっています。近年、誤り訂正符号を体系づける情報理論、特に符号理論が数多くの方面に応用され着実に成果を挙げつつあります。例えば、ファアクシミリ、CD、計算機メモリ、データ伝送、衛星通信、移動通信など多方面にわたっています。この様な状況で、情報理論や符号理論の開花しつつある通信システムへの応用に的を絞り、和文誌A 分冊において「情報理論の通信システムへの応用」論文小特集号(平成４年８月)を計画致しました。趣旨をご理解いただき、奮って御寄稿下さいますようお願い申し挙げます。

１．対象分野:
(1)情報理論、符号理論の基礎
(2)各種通信・記録システムのための誤り検出・訂正符号
(3)符号化変調方式
(4)復号アルゴリズム
(5)符号化・復号用 LSI

2.論文の執筆と取り扱い
　通常の論文と同一とします。但し、刷上り８ページ以内。査読後の再提出(条件つき査読の場合)は

通常の 60 日以内か短縮される場合があります。小特集号の予定総ページ数を越えた場は、一般論文にまわす場合もありますのでえ、あらかじめ御了承下さい。論文寄稿時には、「情報理論の通信システムへの応用小特集号」と論文の表紙に朱記して下さい。

３．論文寄稿締切日：
平成 3 年 12 月 20 日（金）必着

４．原稿送付先:
〒105 東京都港区芝公園 3−5−8
機械振興会館　電子情報通信学会論文課

５．問い合せ先:　河野隆二　横浜国立大学
電話 (045)335-1451 内線 2813
FAX (045)338-1157

平成３年度 情報理論とその応用学会役員一覧 （平成３年５月３１日現在）

顧問
重井芳治（東洋大）　滑川敏彦（姫路独協大）
嵩　忠雄（阪大）　堀内和夫（早大）

会長
辻井重男（東工大）

副会長
有本　卓（東大）　森　真作（慶大）

理事
（無任所）　丸林　元（長岡技術大）
大石進一（早大）
（庶務）　中川正雄（慶大）
坂庭好一（東工大）
（会計）　山内才胤（三菱）
平田康夫（ＫＤＤ）
（編集）　畑　雅恭（名工大）
青山友紀（ＮＴＴ）
（企画）　小林欣吾（電通大）
阪田省二郎（豊橋枝科大）

監事
岩垂好裕（名大）　田崎三郎（愛媛大）

評議員
青木由直（北大）　秋山　稔（東大）
浅川　繁（東芝）　磯道義典（広大）
稲垣康善（名大）　今井秀樹（横浜国大）
今村恭己（九工大）　小倉久直（京大）
小沢慎治（慶大）　笠原正雄（京都工繊大）
畔柳功芳（東京工科大）　古賀利郎（九大）
佐藤　洋（電通大）　高橋磐郎（筑波大）
高崎喜孝（日立）　田中初一（神戸大）
手塚　集（日本 IBM）　富永英義（早大）
長尾　真（京大）　野口正一（東北大）
原島　博（東大）　韓　太舜（専修大）
平澤茂一（早大）　福島邦彦（阪大）
八重礼剛（富士通）　Shu Lin （ハワイ大）

幹事（無任所）
吉田　進（京大）　河野隆二（横浜国大）
笹野　博（近畿大）　橋本　猛（電通大）
（庶務）
広田　修（玉川大）　荒川　薫（明治大）
（会計）
山田芳郎（愛媛大）　小松尚久（早大）
（編集）
内匠　逸（名工大）　笹瀬　巌（慶大）
（企画）
森田啓義（電通大）　川端　勉（電通大）

幹事補佐
地主　創（東工大）　山崎浩一（玉川大）

オブザーバ
長瀬庸二（鹿児島大）　藤原　融（阪大）

事務局　谷口房江（東工大辻井研）

（順不同）

平成3年度 第1回情報理論とその応用学会理事会 議事録（要約）

1.開催日　:　1991 年 5 月 31 日　18:00〜21:00
2.開催場所：東京工業大学大岡山
南 3 号館 2 階 201 会議室
3.出席者　:　辻井会長以下 21 名
4.議事要約
4.1 小林理事より 1990 年度情報理論とその応用学会シンポジウムの実施報告がなされた.

4.2 前回総会(平成3年1月24日)で選出された役員(理事，監事)に加えて，会長の推薦・任命による新役員を新しく承認した．
4.3 藤原オブザーバ，長澤オブザーバより，　SITA '91の計画・準備状況が報告され，承認された．
4.4 賛助会員募集に関する基本的な活動方針のスケジュールが了承された．
4.5 各担当幹事より，年間計画が報告された．
4.6 ISITA'92を，Singapore ICCS/ISITA' 92 の形で1992年11月16〜20日に開催することを承認した．
4.7 森副会長(WG委員長)より，学会の活動に関するワーキンググループの中間報告がなされた．WGとしては引き続き検討を行ない，いずれ最終的な答申を出す．
4.8 その他(次回理事会は9月7日(土)玉川大学で開催)

投稿募集

ニューズレターへの投稿を大いに歓迎いたします．原稿をフロッピーディスク（5 or 3.5インチ，2DD または 5DD）に入れて送っていただければ幸いです．この場合，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でお願いします．なお今後，電子メールによる原稿送付も歓迎します．

投稿なら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いたします。

畑　雅恭（編集理事）
〒466 名古屋市昭和区御器所町
名古屋工業大学知能情報システム学科
Tel.052-732-2111 ext．2454
Fax.052-733-6589
青山　友紀（編集理事）
〒100 東京都千代田区内幸町1-1-7
大和生命ビル１０Ｆ
日本電信電話株式会社　研究開発技術本部
Tel.03-3509-2415
Fax.03-3595-4521
笹瀬　巌（編集幹事）
〒223 横浜市港北区日吉3-14-1
慶應義塾大学　理工学部電気工学科
Tel.045-563-1141 ext.3318
Fax.045-563-3421
内匠　逸（編集幹事）
〒466 名古屋市昭和区御器所町
名古屋工業大学　知能情報システム学科
Tel.052-732-2111 ext.2850
Fax.052-733-6589
E-mail:takumi@babel.elcom.nitech.ac.jp

編集後記

今回のニューズレターは新会長あいさつ，博士論文の紹介，随筆，ミニワークショップ報告，国際会議報告などを中心に編集を行なうことができました．ご多忙のなか原稿をお寄せ頂きました方々に厚くお礼申し上げます．

今後，さらに豊かな内容にして行きたいと思いますので，若手の学会員の皆様には，ふるってご投稿頂くよう期待致しております．

(畑)

情報理論とその応用学会事務局
〒152　東京都目黒区大岡山2-12-1
東京工業大学　工学部　電気電子工学科　辻井研究室内
Tel.03-3726-1111　ext.2503　Fax.03-3729-0685