No.5　　1988年2月8日発行

情報理論とその応用学会ニューズレター

第10回情報理論とその応用シンポジウム（SITA'87）報告

実行委員長　　森　真作
（慶応義塾大学）

第 10 回情報理論とその応用シンポジウムは1987年11月19日午後から21日午前まで藤沢市江ノ島の神奈川県立婦人総合センターで開催された．前夜には雨が降り出し天候が心配されたが，当日は雲一つない晴天に恵まれ，気温も上がり，また富士山がくっきりと見える絶好の天気となった．シンポジウムにさきがけて，19 日午前中電子情報通信学会情報理論研究会が開かれたが，この間に海外からのシンポジウム参加者のために三菱電機情報電子研究所（大船）の見学会が行われた．

シンポジウムは19日13:00から始まり，5セッション並列で進行された．参加者の総数（登録者）は約 300 名，発表論文数 175 編，セッション総数 40，この内英語セッションは 13（論文数 56 中欠席 3）であった．今回のシンポジウムは東京での世界電気通信会議(GLOBECOM '87)の直後の開催であったため，海外からの論文発表数が 30（内３件欠席），参加者 33 名に達した.19 日夕刻　IEEE IT-Group Tokyo Chapter 総会，本学会総会が開催されたが，この時間を利用して海外からの参加者のためにお茶会が催され，大変に好評であった．
19:00 から岩本楼で懇親会が立食形式で開かれ森実行委員長（慶大），堀内学会長（早大）の挨拶の後に海外参加者を代表して S. Lin 教授（ハワイ大学，本シンポジウム実行副委員長）の挨拶があり，この席で 1990 年にはこのシンポジウムをハワイで開きたい，さらに ISIT と肩を並べるような国際会議に育てたいとの提案があり，大拍手での賛同をえた．最後に次回の幹事大学である九州大学の古賀教授の挨拶があり，宴はいつ果てるともなく続いた．

翌 20 日は一般講演の後，安西氏（北大）の特別講演が行われた．題は”Contextual Information Processing in Japanese Dialog System”であり，実際の対話処理をヴィデオで見せながらの分かり易くしかもユーモアに富んだ説明がなされた．発表後の質疑では今後の情報理論と文脈処理の関係について活発な討論がなされた．特別講演の後の夕食会は前日と同じ岩本楼で宴会形式で行われたが，特に外国人にとって日本式の宴会は珍しく，好評であった．夕食後は同楼でワークショップが行われた。その詳細は本ニュースレターに記載されているが，それぞれ活発な意見交換がなされたようである。

21 日はすべてのセッションが日本語の発表で，昼食の後解散になった．

懇親会における S．Lin 先生のスピーチ

（上左）　懇親会風景
（上右）　一般講演における質疑応答

一般講演の中の日本語のセッションでは暗号関係のセッションが４セッションもあり注目されたが，特に若い優秀な研究者がこの分野で育っているように感じた．また最終日 21 日の故杉山康夫先生の追悼セッションには多くの参加者があり，先生の御功績の高さをあらためて示していた．英語のセッションでは変調と符号化さらにフェーディングチャンネルに関するセッションが注目され活発な討論がなされ，また多数の立席者まででた．

今回は積極的に英語のセッションを推進したが，初めての試みとして多くのセッションで座長を外国人に指名したこともあって，英語のセッションでの質疑は活発であった．また初めて参加する外国人からはこのシンポジウム全体の質の高さを賞賛すると同時に全ての論文をサマリーのみならずぜひ本文も英文にしてほしいとの声も聞かれた．さらに ISIT が純理論サイドに立つ会議であるのに対してこのシンポジウムが純理論から実際的な通信までをも広く含んでいるところに他に例を見ない大きな特徴があり，ぜひ国際会議化してほしいとの声もあった．

SITA'87 の写真入りの記事を IEEE IT News Letterに掲載したいとの依頼がEditorよりあったので，後ほど報告する予定である。

最後に本シンポジウムの参加者，実行委員各位，会場担当の学生諸君，会場を提供いただいた神奈川県婦人総合センターの各位，すべてにわったてお世話になった三菱電機の関係各位，また寄付をしていただいた３社，および広告に協力していただいた 30 社に深謝の意を表する次第である．

光通信理論ワークショップ

中川正雄（慶応義塾大学）

光通信理論のワークショップは山梨大学の高原先生の司会で開始され，今回は議題を限定せずに自由な議論がなされた．主な出席者と討論された議題を以下に示す．

出席者:

高原（山梨大，司会），広田（玉川大，世話人），末広（東京工科大），長岡（東京工科大），木田（東工大），山崎（慶大），日立の方，電通大，同志社大，横浜国大の学生の方，中川（慶大，世話人）

討論議題:

1）先ず司会の高原先生より光通信理論の役割に関してのお話があり，特に現実のシステムの設計と未来のシステムにおける役割に関してのお話があった．

2）玉川大学の広田先生への質問として，不確定性原理の意味に関する質問があり，スクイーズド状態を中心に先生の分かりやすくしかも含蓄あるお話が聞かれた．

3）回路理論の権威である東工大の木田先生からフーリエ変換における不確定性原理と光の不確定性原理に関する類似点，さらに標本化定理に関するお話があった．

4）光子通信と Z-Channel の関係に関して質問

があり，主に広田先生が説明をなさった．以上光通信に専門を持たない参加者の違った角度からの意見がおおいに専門家の参考になるような自由な雰囲気の中での議論（まじめな議論もあり，くだけたよもやま話やジョークもあり）は参加者のこれからの研究意欲を強くあおったであろう．

暗号ワークショップ

松本　勉(横浜国立大学)

暗号のワークショップは，主として
(1)Zero-Knowledge Protocol
(2)暗号をどう捕らえるか
について，約 30 名の参加者により２時間にわたる熱心な討論が行われた．

話題(1)の提供者は東工大の黒沢馨先生で，最近盛んに研究されている魅力的なテーマ: Zero-Knowledge Interactive Proof 及び Zero-Knowledge Protocol について，議論の材料が発表された．はじめに，難解とされている， Zero Knowledge に関する代表的ないくつかの論文について，その証明を含めて，大変分かりやすい解説がなされ，また，最近破られた和田-黒沢 Zero-Knowledge 認証プロトコルとそれらの論文の比較も示された．

まず，“なりすまし”に焦点を当てると，鍵共有法，個人情報に基づく鍵共有法，ならびに，Zero-Knowledge 認証プロトコルの流れが自然に理解できることが示された．

次に，和田-黒沢 Zero-Knowledge 認証プロトコルの Zero-Knowledge 性の証明は，３色問題に関する Zero-Knowledge Proof および平方剰余性を利用した Zero-Knowledge 認証プロトコルの証明と，形式上同一であることが示された．これを通じ，それらの証明法に関する疑問が提起された．

従来の Zero-Knowledge 性の証明法を熟知している参加者が少なかったので，黒沢先生は大変ご苦労されたようであるが，活発な質疑応答が交わされ，約 90 分が瞬く間に過ぎてしまった，興味深い研究課題も生まれ，たいへん有意義であった．

話題(2)は，松本の私見で始まった．私はもともと「暗号とは，ある知識をエンエィティが持っているかいないかによって，ある操作をそのエンエィティが効率よく行えるか行えないかを制御し，守秘性や認証性などの情報セキュリティを達成する方法の総称である．」と考えていた．

しかし，今日のように，ＩＣカードなどの携帯可能で物理的・機構的に保護された小型計算デバイスが簡便に利用できる時代では，上記の意味での暗号が実現する情報セキュリティは，「“知識”そのものはエンティティ自身には知らせず，その“知識”の詰まったＩＣカードをエンティティが利用できるか否かを制御する」という方法によっても実現できるし，この方法によれば，上記の意味の暗号では不可能もしくは困難であったことも簡単に達成できる例が多い．

そこで，上記の＿＿＿＿部分を取り除いたものを“暗号”（より適切な言葉があればそれに置き換えても良い）と考えて総合的に研究すると良い成果が期待できるのではないか，という意見を述べた．

これに対し，賛否両論が色々と出されたが，時間の都合もあり明確な結論には至らなかった．しかし，この種の問題の存在を認識するきっかけになった点では意義があったと思う．

なお，本報告の話題(1)の部分をまとめる際に黒沢先生にご協力いただいたことをここに記し，感謝する．

情報源符号化

山本博資（電気通信大学）
佐藤　創（専修大学）

本ワークショップには 30 名近くの方が集まり，活発な議論が行われた．データ圧縮関係のセッションは最終日に設定されており，ワークショップ当日まだ講演が一件も成されていなかったため，翌日の講演予定者にお願いし，フリートーキング形式で講演内容を説明して頂いた．今回は特に無歪データ圧縮を取

り上げ，下記のような算術符号，Huffman 符号，Ziv-Lempel 符号などに関する話題について討論を行った．

【内容】

(1) 隠れマルコフ情報源モデルを用いた算術符号化　　（長岡技術大学　荻原春生）

(2) 2 重マルコフ情報源への Lynch-Davisson 符号の適用及び Huffman Tree の表現法について　　（神戸大学　若野勝巳）

(3) Ziv-Lemple 符号の改良について　　（横浜国大　パクジファン）

通常の講演と異なり，途中でいろいろ質問ができ，参加者各自にとって得ることが多かったと思われるが，当日の熱気は 1 月 15 日～17 日に開かれるワークショップ【データ圧縮ー理論と実際】に引き継がれることと思う．

なお最近，ユニバーサル符号の発表及び質問に関して若干の混乱が見受けられる．この原因は，研究目的及び方法などについて各自曖昧なまま，討論に参加するためと思われるので，いかに注意点を書き留める．

①ある特定の符号の特性を調べることが研究目的の場合

その符号のユニバーサル性（つまり，適用可能な情報源の範囲）を明確にする必要がある．次に，その符号に対して，理論的に性能評価する必要がある．シミュレーションによる評価だけではその符号の普遍的性能が分からない．また，性能比較を行う場合は，ユニバーサル性の異なる他の符号とある特定の情報源に対してのみ，比較しても意味がない場合が多い．比較するときは同じユニバーサル性を有する符号と適用可能ないろいろな情報源で，性能を比較すべきであり，その時には，圧縮率ばかりでなく，必要とする記憶容量（space complexity），符号化時間(time complexity)等の他の重要な条件も明確にして比較することが望ましい．

②ある特定のクラスの情報源に対する圧縮が研究目的の場合

あるクラス（例えばファイルや画像など）の情報源を圧縮することが目的の場合には，そのクラスに適用可能な有望な符号を選び出し，各符号のそのクラスに対する性能を理論的またはシミュレーションなどで評価する．その時には，符号そのものの善し悪しよりは，そのクラスにはどの符号がどのような理由で適しているか，あるいはそのクラスに適した符号化法は何かを議論すべきである．また，この場合も記憶容量，符号化時間も含めて比較されることが望まれる．

最近，算術符号， Ziv-Lempel 符号以外に，いろいろな特徴を持つユニバーサル符号が多数考案されている。今後，各種のユニバーサル符号やその改良型の性能比較に関する研究発表も増加すると思われるが，上記①②のどの立場で発表するかを明確にして議論すれば，無用な混乱は避けられるものと思われる．

通信路符号化

橋本　猛（東京電機大学）

このグループの主題は通信路符号化であったが，総数 27 名の参加者は符号理論関係の方が多数を占めた．このワークショップのテーマを決めるに当り，常盤（阪大），山田（宇宙研），橋本（電機大）の３人の世話役は符号理論，及びそれの応用において最近の話題になっているものをということで，代数幾何符号と符号化変調を取り上げることを決め，当日は符号化変調の３人の（自称）新人，笠原（阪大），山口（横国大），後川（東大）の方々の話題提供から始めることにした．符号化変調は符号理論と通信路符号化理論とが非常に接近している所であり，これからの理論的な進展が期待される分野である．ところが，優秀な研究者のねばり腰と言うべきか，意外に話の時間が延びたので討論は適当に切り上げて，山西（日電）による代数幾何符号の解説を聞かせていただくことになった．この代数幾何符号は良好な距離構造をもつ符号のクラスとして最近注目を集めており，その解説には事前からかなりの感心が持たれていたようであった．この分野で多くの（自称，他称の）若手が続くことが望まれる．ただし，代数幾何符号の解説には数時間を要するとの解説者のコメントもあるように，ワークショ

ップの僅かな時間内で満足のいく理解は望めないというのは世話人の言い訳であろうか．今回のワークショップでは，欲張りな世話人のせいもあるが，会場や門限などの制約が重なり時間に不自由することとなった．次回には会場や時間帯のセッティングの面での配慮をお願いしたい．　　（文中敬称略）

ENGLISH　WORKSHOP

笹瀬　巌（慶應義塾大学）

ENGLISH WORKSHOP には，米国，カナダ，フランス，西ドイツ，イタリア，中国からの SITA 参加者および留学生を含め約 15 人の参加があった．　まず，簡単な自己紹介のあと，SITA'87 に対する感想および今後の SITA への期待や要望についてのフリーディスカッションを行った．まず，SITA'87 については，極めて好評で，次のような感想が寄せられた．まず，英語でのセッションが並列してあり興味深い論文が数多く発表されたこと，また，サマリー集により日本語での論文の概略を知ることができ有用であったこと，日本人研究者がとても親切で，楽しく討論することができたこと，旅館や夕食が日本的でよかったこと，時期が東京で開かれた世界通信会議の直後であり，会場が東京からの交通が便利な景色の良い場所であったこと，三菱電機への見学ツアー，特別講演が有意義であったこと，お茶の会や鎌倉への観光案内など外国人に対する配慮がいきとどいていたことなどが挙げられる．今後の SITA への期待および要望としては，次のような意見が寄せられた．まず，SITA の存在をもっと外国に知らせるべきだとの意見が強く，そのためには，論文募集の手紙をできるだけ早く準備し，関連ある学会誌に掲載したり，国際会議などで配布したり，ダイレクトメールで知らせたりすることが極めて大切であるとの意見が出された．また，来年も是非参加したい，友人にも参加を依頼したいとの意見が大勢を占め，そのためにも，これまでの SITA 参加者に論文募集の手紙を確実に郵送してほしいとの強い要望があった．さらに国際化を一層進めるためにも，より多くの英語での発表を期待したい，日本語での発表の論文もできるだけ英語で書いて欲しい，興味ある日本語での発表をきくために OHP に英語での説明を加えて欲しいなどの意見が述べられた．最後に，海外から，特に，東南アジアからより多くの若手の研究者の参加者を迎えることができるように，ICC，GLOBECOM，ISIT などの国際会議にみられるような奨励援助制度が，SITA にも取り入れられないかとの要望があったが，私も大賛成であり，SITA がさらに情報理論の発展および国際交流に寄与することを心から願っている．

確立過程ワークショップ

井原俊輔（高知大学）

このワークショップは参加者が少なく開会に至らないのではとの予想のもとに責任者の役を引き受けたのですが，少人数（10 名程度）ながらも予想よりははるかに多く無事開会されました．

現在，ガウス型通信路の容量がフィードバックによりどう変わるかに関し，いくつかの結果が得られつつある．例えば，(1)フィードバックにより容量が増加するための条件，（2）フィードバックの無いときの容量に対し有るときのそれは高々２倍である(Cover et al.)，(3)この”２倍”が達成される例，等である．責任者としては，議論のひとつの材料として上のような話題の提供の準備を一応していた．

しかるに，このような小さな話題で包むには参加者の顔ぶれがあまりに豊かすぎ，このような話題提供抜きで話はたちどころに情報理論全般へと広がっていった．さらに話は広がり，時間切れとなるころには無限大へと発散してしまった．

議論の中で，今回のシンポジウムにおいて I - divergence (Kullback - leibler の情報量）の登場する報告が幾つもあったことが話題になった．このこと自身は I - divergence のような基本的な量はいつの世でも重要な役

割を果たすと言うことを物語っているのであろう．これにちなんだわけではないが，確率過程のワークショップは話はまとまらず，完全に diverge してしまった．

■SITA87 関連記事はここまで■

1987年符号理論とその応用 ワークショップ（WCTA'87）報告

企画理事　今井秀樹（横浜国大）
企画幹事　河野隆二（東洋大学）

日時:　　昭和 62 年 7 月 30 日～31 日
場所：　　東京理科大学特別教室
　　（セミナー　ハウス）
合同開催:1987 年暗号と情報セキュリティワークショツプ(WCIS'87)　(暗号と情報セキュリティ研究会及び電子通信学会情報セキュリティ時限専門委員会主催)
参加者:　150 名

昭和 61 年度に引続き暗号と情報セキュリティワークショツプと合同開催という形式で，東京理科大学の金子先生のご協力により緑豊かな庭園に囲まれた千葉県野田市のセミナーハウスで開催された．「畳込み符号とその復号法」と「Combined Coding and Modulation」をテーマとして 11 名の専門家により，概論から装置化，最近の動向等について講演が行われ，連日活発な討論が交わされた．

各講演の内容及び議論の対象となった話題について，簡単にまとめると次の通りである．

WCTA87-1　　岩垂　好裕（日本電気）
「畳込み符号とその復号法（概論)」
Wyner 符号，Haagelbarger 符号，岩垂符号などの各クラスの畳込み符号の関係について統一的な解説が行われ，復号の容易な畳込み符号の構成などについて議論が行われた．

WCTA87-2　　平澤　茂一(早稲田大学)
「畳込み符号とその E(R)関数」
符号化方式に関する特徴を理論的に比較する上で有用な信頼度関数 E(R)に基づくブロック符号と畳込み符号の比較や，復号法の複雑さについて分かり易く解説された．

WCTA87-3　　安田　豊，大橋　正良(KDD)
「ビタビ復号器の装置化と復号アルゴリズム」
ビタビ復号器の装置化に関わるポイントを整理し，装置の簡単化という観点から有効である符号構成や復号法が紹介され，衛星通信を中心とした応用について議論された．

WCTA87-4　　笹野　博（近畿大学）
笠原　正雄（京都工芸繊維大学）
「Viterbi 復号法とその符号間干渉のある通信路への応用」
符号間干渉のある通信路に対する Viterbi アルゴリズムを用いた最尤復号器の構成法やその復号誤り確率の上界式などについて，具体的な例を用いて解説された．

WCTA87-5　　橋本　猛（東京電機大学）
「通信路等化と簡略アルゴリズム」
前講演に引き続いて，記憶のある通信路に対する符号化・復号と等化の同等性や統合的最適化について説明され、 Viterbi アルゴリズムとその簡略化について論じられた．

WCTA87-6　　笠原　正雄（京都工芸繊維大学）
「符号化変調方式とその動向」
ディジタル変調方式の始まりから，その一つの発展形式としての符号化変調方式の動向に至る歴史的な研究の流れを，新しい視点から解説され，今後の展望について議論された。

WCTA87-7　　山田　隆弘（宇宙科学研究所）
「位相連続変調方式と Viterbi アルゴリズム」
CPFSK やパーシャルレスポンス FSK などの位相連続変調方式と，その Viterbi アルゴリズムによる復調法について紹介され，応用に関する議論が行われた．

WCTA87-8　吉田　進，池上　文夫（京都大学）
「耐多重波変調方式」
多重波伝搬とフェージングによって特徴づけられる移動体通信の高信頼化を実現する耐

多重波変調方式について解説され，符号化変調方式の応用の可能性が議論された．

WCTA87-9　　山口　和彦，今井　秀樹（横浜国立大学）

「多値変調に適した高信頼トレリス符号化復号方式」

今井・平川法に基づく畳込み符号と軟判定ビタビ復号法を用いた符号化多値伝送方式と，Ungerboeck 方式の比較に基づく新しい符号構成の提案とその評価について報告された．

WCTA87-10　　笹瀬　巌（慶応大学）　河野　隆二（東洋大学）

「海外における最近の Combined Coding and Modulation」

符号化位相連続変調方式とトレリス符号化変調方式の様々なバリエーションに関する最近の興味深い論文がサーベイされ，相互の関連や今後の研究動向について紹介された．

1987年暗号と情報セキュリティワークショップ（WCIS'87）報告

植松友彦，藤岡淳（東京工業大学）

7月29日から31日まで，野田市にある東京理科大学のセミナーハウスにおいて，表記のワークショップが WCTA'87 と同時開催された．今年のワークショップの形式は，パネル討論・招待講演・公募論文の３通りで，それぞれ活発な議論が展開された．

［パネル討論］

テーマは，ID-Based システムの諸方式についてであり，神戸大学の田中先生を司会者として， NTT の小山氏，日本電気の岡本氏，横浜国立大学の松本先生の三名をパネラーに招いた．まず，パネラーによる，ID-Based システムの概念とその現状についての講演・報告が行なわれた．続く討論会では，会場からの質問・意見などが相次ぎ，このテーマへの関心の高さが感じられた．今後の研究に対して非常に有益な示唆に富むパネル討論であった．

［招待講演］

講演題目は，

「計算量理論の最近の話題 ”P=NP? ”」　大阪大学　中野先生

「Zero-Knowledge Proof」　東京工業大学　渡辺氏

「ガロア体上の演算アルゴリズム」　東京工業大学　伊東氏　大阪大学　森井氏

「情報システムにおけるセキュリティ評価技法」　日立製作所　宝木氏

の４つで，暗号・情報セキュリティの分野で，最新かつホットな話題に対するものであった．

特に，中野先生の講演は，計算量理論の初歩を平易に解説したもので， Swart の論文についての解説もあり，非常に分かりやすいものであった．

［公募論文］

公募論文の主たるテーマは『暗号技術の応用』であり，セキュリティチェックに関するもの１件，電子手形取引に関するもの２件，LSI に関するもの１件，装置化に関するもの１件など，計９件の発表が行なわれた．なかでも，NTT の小山氏による“公開鍵暗号を解読したことを秘密情報を漏らさずに納得させる方法”は．Interactive Proof の一つの応用として大変興味深いものであった．

以上，簡単ではあるが，WCIS'87 についての報告をまとめてみた．次回は関西地区で開催される予定である．

両ワークショップ一括の会計報告

［収入］

参加費一般￥8,000×76（人）＝￥608,000

学生￥5,000×46（人）＝￥240,000

計￥848,000

但し，講演者参加費無料

［支出］

セミナーハウス	￥217,800
資料印刷製本代	￥293,300
事務通信費	￥169,445

懇親会補助	￥7,455
アルバイト代	￥160,000
	計￥848,000

ISSPA87 (International Symposium on Signal Processing and its Applications) 参加報告

河野隆二（東洋大学）

主催:IASTED
(lnternational Association for Science and Technology for Development)
共催:IEEE, IREE, lEAust
日時:1987 年 8 月 24 日～28 日
会場:Mayfair Crest International Hotel, Brisbane, Australia
参加者:
約 230 名（日本人 12 名）
主要参加国：
オーストラリア，ニュージーランド，米国，カナダ他計 20 カ国
セッション数：
５（チュートリアル），
３（招待），
24（一般，内 6 ポスターセッション）
発表論文数:
190 件（日本 9 件）
テーマ:

(1) ディジタル信号処理（20 件）
(2) ディジタルフィルタ（19 件）
(3) スペクトル推定（8 件）
(4) 時変スペクトル解析（7 件）
(5) 適応信号処理（18 件）
(6) アレイ信号処理（12 件）
(7) レーダ・ソナー・地震信号処理（11 件）
(8) 音声解析（18 件）
(9) 画像処理・パターン認識（25 件）
(10) ＶＬＳＩ信号処理（7 件）
(11) 光信号処理（2 件）
(12) 生医学信号処理（7 件）
(13) ディジタル通信（6 件）
(14) 信号処理応用（9 件）

信号処理に関する国際会議がオーストラリアで開催されるのは，この ISSPA87 が最初であるということで， ICASSP 等と比べてオセアニア，アジア，の研究者が多く小規模であったが，討論などの時間的余裕があり有意義であった.

8 月 24 日～25 日は信号処理，適応並列処理，２次元処理，フィルタ設計，適応アルゴリズムのチュートリアルセッションがクイーンズランド大学で、 MIT の J.S.Lim， UC Santa Barbara の S.K.Mitra らにより行われ 8 月 27 日～29 日は会場をホテルに移してテクニカルセッションが行われた.

オープニングアドレスでは，オーストラリア防衛庁の H. d'Assumpcao が防衛における信号処理の概要について講演し，OTH レーダなどの最新の話題を写真などを折り混ぜながら紹介した． また，オーストラリア国立大学の B. D. O. Anderson による判定帰還等化器に関する招待講演と西オーストラリア大学の J. Imberger による海洋学における信号処理に関する招待講演が行われた.

一般講演においては，上記の 14 のテーマに分類され広範囲のトピックスをカバーするもので，特にテーマを絞ったものではなかった. オーストラリアにおける信号処理研究では応用分野として軍事の占める比重が大きいことが感じられた.

また，会期中に知り合ったシドニー大学の研究者を本学会主催の SITA87（江ノ島）に招くことができ，交流を深めることができた.

ワークショップ データ圧縮ー理論と実際

小倉久直（京都工芸繊維大学）
小林欣吾（大阪大学）

この 1 月 15 日から 17 日にかけて表記のワークショップが本学会の主催で専修大学箱根セミナーハウスに於て開催されました. このワークショップのために正月を返上して原稿を用意された 18 名の講演者の興味津々な話題と

連休をものともせず駆けつけた 70 名の参加者による熱烈な討論によって二日目には予定を大幅に狂わされ（大方の思惑どうり）終了が夜の 10 時近くになってしまうほどであった．ランダムな列とはどのようなのものであるべきかにはじまる純粋に数学的興味に始まって，貿易摩擦までからむ技術の標準化といった，斬れば血が奔ばしる話題にまで至る広範囲のスペクトルを備えた研究活動がデータ圧縮をテーマとしていま正に行われているのだと実感させるワークショップでありました．

数学的には，ランダム列の概念は Martin-Lof で尽くされているが，情報科学で有用なものとするには，time-complexity，space-complexity の概念を導入して algorithm のクラスを限定して，学習とか暗号といった実際の応用に有効な構成的な仕方で complexity の定義を考えてゆかねばならないという主張が山田氏からなされた． Algorithmic な complexity に関する研究は，計算機科学に多大の影響を与え，データ圧縮の種々の技法を生んできている．さらに，それにからんで，情報源の構造を調べるという共通のテーマを通して，情報理論と統計学がまた歩み寄ってきている，このことは多端子情報理論の視点からみると更に明確となるといったことなどの興味深い話題も提供された．

データ圧縮の実際的側面は，計算機科学を除けば音声圧縮と画像圧縮にほとんど代表されるといっても良い．これらの研究分野の息の長い歴史の中で消え去った技術と，生き残った或は再生した技術に対する解説の後，これからの技術的理論的可能性についての展望，例えば，知識ベースを構築しながら低レートで品質の高い動画像圧縮に適用する知的符号化，HDTV などの高品質放送，ISDN 構築への対応などが語られた．

世界を相手に標準化に携わる研究者たちが，より性能の優れた方式であっても諸般の事情で採用が見送られるといった苦渋を経験すると共に，最後は結局のところ理論的に確固と性能の保障された原理が勝つのだという信念に従って努力を積み重ねていることが印象的であった．それはまた，彼らが，進化する標準化あるいは新しい考え方を許容する標準化といった方向を探っていることを裏付けている．したがって，標準化に携わる当の研究者たち自身が，標準化が原理的に斬新なアイデアを阻害することを恐れ，若い野心のある理論家の出現を期待していることが理解された．一方，標準化とは別の土俵，例えば CD-I など，を設定して戦略を練っている人々の存在することもまた興味深いことであった．

最後に，どうしても都合がつかず参加されなかった方々の参考のために講演のタイトルとその演者を以下に挙げておく．

(1) データ圧縮技術の現状と動向
－画像符号化－　安田靖彦（東大）
(2) 線形予測分析による音声情報圧縮
板倉文忠（名大）
(3) 画像情報圧縮技術の変遷と展望
原島　博（東大）
(4) 計算機科学におけるデータ圧縮
－アルゴリズム的ユニバーサル符号について－　山本博資（電通大）
(5) データ圧縮・統計的推論・チユーリング機械　韓　太舜（専修大）
(6) 歪・レート関数のプロセス表現，エルゴード分解，そして定常符号化
橋本　猛（東京電機大）
(7) データ・コンパクション　その１
佐藤　創（専修大）
(8) 動画像圧縮技術の標準化と研究動向
大久保　栄（ＮＴＴ）
(9) 静止画像圧縮技術の標準化と研究動向
安田　浩（ＮＴＴ）
(10) 蘇ったＴＶ圧縮技術
－３次元周波数領域の活用による－
吹抜敬彦（日立）
(11) 動画像信号のフレーム間予測とエントロピー符号化
古閑敏夫（日本電気）
(12) テレビ会議／テレビ電話におけるビデオ符号化技術－画像圧縮技術の実用化動向－　村上篤道（三菱電機）
(13) 計算論的情報理論概説－有限記号列の情報理論とそのデータ圧縮への応用－
山田真市（早稲田大，日本ユニバツク）
(14) データ・コンパクション　その２
－算術符号と線図形データの符号化－

森田啓義（豊橋技科大）

(15)データ・コンパクション　その３
－情報源モデルの推定と MDL 基準－
伊藤秀一（電通大）

(16)音声符号化の標準化と研究動向
八塚陽太郎（ＫＤＤ）

(17)ＣＤＩへの圧縮技術の応用
赤桐健三（ソニー）

(18)音声圧縮技術の実用化動向
荒関　卓（日本電気）

また，このワークショップは，佐藤洋（電通大），佐藤創（専修大），山本博資（電通大）の諸氏に世話人としての御協力を頂いて行われました．そのほか多数の人々の御協力によりこの企画が成功を納めましたが，なかでも，素晴らしい会場を提供して頂いた専修大学の御好意に篤く感謝いたします．

なお，本ワークショップの講演資料(258 ページ）は当学会事務局において送料込みで一部 4000 円にて販売いたしております．データ圧縮の理論的な側面と実際的な側面の最新の情報が詰め込まれたこの資料の残部は限られておりますので興味をお持ちの方はお早く申し込み下さい．

1988 年暗号と情報セキュリティ シンポジウム開催の御案内

開催担当幹事　　富永英義（早稲田大学）

1988 年暗号と情報セキュリティシンポジウムを下記のとおり開催致しますので御案内申し上げます．

昭和 62 年 12 月末現在で，参加予定者約 90 名，また発表予定件数 32 件となっております。尚，今回は一般講演とともに「暗号処理ハードウェア」に関するパネル討論を企画致しました．

現在，若干ではございますが宿泊設備等に余裕がありますので，参加を希望される方は事務局までお問い合わせ下さい．

記

主催　：　暗号と情報セキュリティ研究会
(CIS 研究会）

協賛　：　電子情報通信学会情報理論研究会
情報理論とその応用学会

日程　：　昭和 63 年 2 月 22 日（月）～24 日（水）

2 月 22 日（月）

10:00～	受付開始
10:30～12:10	機密管理方式の基礎理論
13:30～15:30	認証システム
15:50～16:50	1D を用いた暗号方式とその安全性
17:00～18:00	1D を用いた暗号方式とその安全性
19:30～21:30	情報通信の安全性とその対策

2 月 23 日（火)

8:40～ 9:55	有価情報の安全性確保
10:15～12:00	暗号アルゴリズム
13:00～14:10	個人識別情報とその利用
14:30～15:15	暗号システムのハードウェア
15:35～18:00	暗号処理ハードウェア（パネル討論）
18:30～20:00	懇親会

2 月 24 日（水）

9:00～ 9:45	伝送路及び端末
10:00～11:00	支援システム
11:20～12:20	安全性評価

会場　：
生産性研修会館
静岡県田方郡函南町平井
宇南谷下 1753-11　(〒419-01)
TEL　(05597)4-0311

交通　：　JR 熱海，三島駅より
約 30 分（タクシー）
約 50 分（バス）
伊豆箱根鉄道大場駅より
約 20 分（タクシー）

尚，チャーターバスを以下のとおり用意致します．

2 月 22 日（月）熱海駅～生産性研修会館
9:00 及び 9:20 発

2 月 24 日（水）生産性研修会館～熱海駅
13:30 発

参加費:　一般　　会社関係者　7,000 円
大学関係者　5,000 円
学生　　4,000 円

宿泊費:
幾つかのタイプを用意致しました.
例えば，２泊（ﾂｲﾝﾙｰﾑ）で 21,000 円（懇親会費含む）となっております．申し込み方法と共に詳細は，事務局までお問い合わせ下さい.

問い合わせ・連絡先:
開催担当事務局・小松　尚久
早稲田大学理工学部電子通信学科
新宿区大久保 3-4-1(〒160)
TEL　(03)203-4141（理工 3419)
FAX　(03)200-6735

1988年IEEE情報理論国際シンポジウム (1988 IEEE International Symposium on Information Theory)

広報委員長　小林欣吾（大阪大学）

いよいよ，あと半年足らずで（6 月 19 日より 6 月 24 日まで）表記のシンポジウムが国際会議センター神戸に於て開催されます．組織委員会，諮問委員会，プログラム委員会，実行委員会等の活動も大詰めを迎え，準備万端滞りなく進行しています．既に，原稿の締切日も過ぎてしまいましたが，我々のシンポジウムに多大な関心を寄せられた方々から多数の投稿を頂き深く感謝いたします．また，当学会の会員に限らず関心をお持ちのかたをお誘いの上ご参加下さるようお願い申し上げます.

昭和62年度通常総会

総会報告:
本学会昭和 62 年度通常総会は，昭和 62 年 11 月 19 日（木）17 時 45 分より，第 10 回情報理論とその応用シンポジウム(SITA87)開催中の神奈川県立婦人総合センターにおいて開催されました．会長の挨拶に引き続き下記の議題が審議され承認されました.

・昭和 61 年度事業報告
・昭和 62 年度事業中間報告と中間収支決算
・昭和 63 年度事業計画と収支予算
・会則一部改訂の件
・第 10 回情報理論とその応用シンポジム(SITA87)中間報告
・第１１回情報理論とその応用シンポジム(SITA88)開催計画
・情報理論とその応用国際シンポジウム(IFITA88)開催計画

会計報告：
昭和 62 年度通常総会で承認されました昭和 61 年度会計決算および昭和 63 年度一般会計予算は下記のようになっています.

情報理論とその応用学会
昭和 61 年度　会計報告

収入		
項目	予算	決算
会費収入　正会員	0	0
学生会員	0	0
雑収入（利息等）	0	567
繰越金収入	700,000	700,000
計	700,000	700,567

支出		
項目	予算	決算
ニューズレター		
印刷費	50,000	54,370
会員名簿　印刷費	50,000	30,000
会則　印刷費	30,000	0
資料コピー代	20,000	1,800
入会案内資料		
印刷郵送費	100,000	0
通信　郵送費	64,000	53,030
会議費	110,000	74,670
事務用品費	10,000	17,000
消耗品費	0	4,530
雑費	0	1,000
予備費	266,000	0
次年度繰越	0	464,167
計	700,000	700,567

情報理論とその応用学会
昭和 63 年度　一般会計予算案

収　　入	
項　　目	金　額
会費（正員 165名）*1	330,000
会費（学生員　20名）*1	20,000
繰越金*2	270,000
合　　計	620,000

支　　出	
項　　目	金　額
ニューズ・レター印刷費（３回）	90,000
ニューズ・レター郵送費（３回）	60,000
会費請求書印刷郵送費	25,000
総会費	30,000
会議費	70,000
会議資料印刷費	10,000
事務局経費	50,000
事務局通信費	100,000
事務用品費	10,000
雑費	10,000
予備費	165,000
合　　計	620,000

注　*1　昨年度実績をもとに概算.
　　*2　今後の支出予定を想定して概算.

昭和63年度事業計画カレンダー

1月15日～17日　1988年情報理論とその応用ワークショップ・データ圧縮（専修大学箱根セミナーハウス）
5月　（ニューズ・レター発行）
6月19日～24日　1988年情報理論国際会議(ISIT'88)
（神戸国際会議場）
27日～29日　1988年情報理論とその応用国際フォーラム(IFITA88)
（東京郵便貯金会館）
7月27日～29日　1988年符号理論とその応用ワークショップ(WCTA88)および1988年暗号と情報セキュリティワークショップ(WCIS88)
（六甲山スカイビラ）
9月　（ニューズ・レター発行）
12月1日～3日　第11回情報理論とその応用シンポジム(SITA88)
（別府温泉）

会員名簿発行のお知らせ

会員名簿が出来上がりました.　会員の皆様には，個人宛てに，あるいは多くの会員がいる箇所には一括してお送りしましたが，まだ届いていない場合は事務局までご連絡下さい.

会費納入のお願い

会費納入が振替払込という形で出来るようになり，先に，会員の皆様へ63年度会費の払い込みをお願いいたしました．まだお済みでない方は，ぜひ早い機会に払い込みをお願いいたします.

編集後記

本号は幹事会が編集部となって発行する第1号のニューズレターとなります．今後もこの体制を充実させて行きたいと思っています．皆様のご支援，ご協力をお願い致します．また，今回からニューズレターへの投稿は，原則として，一太郎の文書ファイルまたはMS-DOS標準テキストファイルでお願いすることになりました．メディアは，5'2HD,5'2DDまたは8’2DDが利用可能です．投稿並びに内容についてのお問い合わせは，編集理事または編集幹事までお願い致します.（編集幹事:山田）

情報理論とその応用学会事務局
早稲田大学理工学部堀内研究室内
東京都新宿区大久保3-4-1（〒160）
PHONE:03-209-3211　FAX:03-200-2567