No. 20　　1995年4月26日

SITA　情報理論とその応用学会ニューズレター

ごあいさつ(新会長挨拶)

笠原正雄(京都工芸繊維大学)

史上初めてという猛暑を記録した昨夏の７月 20 日頃だったと思う。東京大学で開催された「情報理論とその応用学会」理事会で、次期会長候補の推薦という議題に移ったとき、しばしの沈黙のあと、有本会長から「笠原さん如何がですか？」という御指名があった。このとき瞬間的に私の脳裏をよぎったのは 20 年近くも前の昭和 52 年３月３日の大阪大学入学試験のときの風景である。昭和 52 年当時は、まだ学園紛争の名残りで、講師以上の若手教官が学内警備班を勤め試験妨害を警戒するという状況であった。私が警備を担当した日は３月というのに、厳しい寒波が近畿地方を襲い、建物の外は銀世界、時折、粉雪が舞うという有様であった。いくら下着を重ね、マフラーをし、オーバを着込んでも寒さを防ぐことはできない。警備拠点に 30 分間も外に立ち尽くしていると身体の芯まで氷りついてしまう。実際、こんな寒い目に遭うと、帰宅後、湯舟に 30 分近く浸かってみても、なお且つ身体の芯が冷え込んでいるように感ずるということを私は初めて経験したのであった。このとき警備作業をともにしていたM氏が、

降りしきる雪の中でふと思い出したように「基礎工学部の有本先生が笠原さんに話をしたいとおっしゃっていましたよ。」と話しかけてきたのである。有本先生については、最近東大から来た人、制御理論、ロボットあるいは情報理論等々の幅広い分野で活躍されている新進気鋭の研究者といったイメージは持っていたけれど、直接お会いしたことはなかった。当時、私のグループは藤原謙一氏の率いる三菱電機の俊才グループ(平澤茂一氏(現早大教授)、山内才胤氏(現三菱電機(株)通信システム研究所長)、杉山康夫氏(元摂南大学助教授で昭和 62 年夏に惜しくも他界された))との熱心な研究討論活動によって情報理論、符号理論に関する研究成果が内外にようやく認められつつあったものの、基礎工学部には嵩先生という符号理論における世界の秀峰が聳えている。嵩先生、有本先生を中心とする基礎工学部のレベルに追い付くには自ら努力、勉励するしかないと考え、学部の壁を越えるような努力をすること等は、当時殆ど考えていなかった。基礎工学部の位置する豊中キャンパスとの 10㎞ ほどの距離は実際の物理的距離よりも遥かに遠い所にあったのである。そのような状況の中、記憶に残る雪景色の中で、初めて人伝てに有本先生からの呼びかけの声を聞いたのである。私自身の記憶に誤りがなければ、これが情報理論とその応用学会への動きの第一歩であった。電話等での話し合いの後、基礎工学部に有本先生を訪ねたが、そのとき「笠原さん、何かやりませんか？今のままでは日本には情報理論は育ちませんよ。」、「是非、頑張りましょうよ。」というような会話が交わされたと思う。理事会の席での「笠原さん、会長をやりませんか？」という声が、20 年前の「何かやりませんか？」という呼びかけの声と、20 年近い歳月を完全に短絡して、二重にダブって聞こえたような錯覚を私は覚えたのであった。

さて、ここで少し思い出話になることを許していただこう。20 年前の呼びかけの輪は順調に広がり、第１回の情報理論とその応用研究討論会(SITA)が昭和 53 年 11 月に神戸市の六甲荘で開催された。滝保夫東大教授を理事長とし、滑川敏彦(阪大)、重井芳治(東北大)、宮川洋(東大)、嵩忠雄(阪大)という著名な先生方を理事、辻井重男(東工大)、韓太舜(相模工大)、今井秀樹(横浜国大)、原島博(東大)の各先生方を東の幹事、そして有本卓(阪大)、平澤茂一(三菱)、杉山康夫(三菱)、笠原正雄(阪大)を西の幹事とする運営組織であった。第１回は主として西の幹事がお世話をし、ホテルに泊り込んで研究討論をするという形式を選んだ。当時、電気系の研究集会活動をこのような形式で行うことは非常に珍しいことであった。何故このような泊り込み形式での研究討論会を企画したのであろうか？古い記憶は当てにならないので、間違っていればお許しいただきたいが、この理由は有本先生が京大の数学科出身、平澤先生が早大の数学科出身、そして私自身も昭和 40 年代の初めに京大の数学科で永田雅宜先生の抽象代数学の講義を聴講させていただいたことがあったために、４人の西側幹事から成る“実行委員会”はいつも数学的雰囲気に終始したことによる。昭和 50 年代に入っても、電気系学会の研究発表の場は依然として国立大学の寒々とした殺風景な教室が主要な“ひのき舞台”であった。プリズンのような雰囲気のただよう廊下を歩いていくと、教室にたどりつくまでに研究発表意欲はしぼみ、意気消沈してしまう。私自身、京大の数学科の掲示板で、浅虫温泉でシンポジウム開催予定、等の貼り紙を見てカルチュアの差を感じ、電気系研究集会に比べ誠に羨ましい限りと考えていたが、このような思いはその後もずっと持ち続けていたのである。数学的雰囲気にあった実行委員会では、泊り込み形式は議論らしい議論もなく、すんなりと決定されたと思う。理事会の席ではこんな思いが私の胸中を去来したが、同時に、会長職をバトンタッチさせていただくこれからの１年間、「初心忘れずで頑張らねばならない。」と強く感じた次第であった。

情報理論とその応用研究会は、昭和 58 年頃より、学会化のための作業が精力的に進められたが、昭和 59 年に情報理論とその応用シンポジウムの実行委員長を勤められ、回路とシステムの分野における重鎮、堀内和夫早大教授のリーダシップのもと現学会がスタートした。滑川敏彦初代会長からはじまって堀内和夫会長、辻井重男会長、嵩忠雄会長、有本卓会長とバトンタッチされてきたが、歴代会長の先生方は電子情報通信学会、IEEE 等々の学会で重責を担われ、研究面でも数々の功績、業績を挙げられた方々である。会長職をお引き受けして３ケ月が経過したが、「本当に私のような者で良かったのか？」という戸惑いの気持ちにある。

情報理論とその応用学会は、昭和 53 年に研究会としてスタートして以来、多くの方々からご指摘をいただいているようにさまざまな形でのインパクトを電子情報通信学

会に与えてきている。その理由は本会会員のほとんどが電子情報通信学会の会員でもあり、しかもこれらの方々が電子情報通信学会の運営面あるいは研究活動面で大いに寄与されていたことによる。例えば昭和 50 年代後半から 60 年代前半にかけて、電子情報通信学会に情報理論、情報セキュリティ、スペクトル拡散等の専門委員会が相次いで誕生したが、これらの研究専門委員会の委員の多くが本学会でアクティブに活躍されている方々であった。時間に制約されずにより突っ込んだ議論をするために、昭和 53 年に SITA 実行委員会が選択した“泊まり込み形式”は電子情報通信学会に第２種研究会活動をスタートさせる大きな力の一つになったように思われる。実際、沢山の方々からそのようなご指摘を受けたし、我国における情報理論とその関連分野の活性化のために SITA 活動が大いに寄与したとのおほめの言葉をいただくこともしばしばであった。

ここ数年、情報理論とその応用シンポジウムの国際化が活発に進められている。国際化のために尽くされた先生方に感謝の気持ちを表すには、国内外の余りにも多数の先生方に貴重なお時間を割いていただいたために、与えられた紙幅ではとても足りない。このため、ここでは一々お名前を挙げて感謝の気持ちを表すことは控えさせていただくが、やはり ISITA ということになると、慶應大学森真作先生の多大のご尽力ぶり、そして理事会の席上で、いつも満面の笑みを浮かべながら海外シンポジウムの進捗ぶりを報告されるご様子が目に浮かんでしまう。深く感謝申し上げたい。

国際化を含めた本学会の益々の発展によって、情報理論とその応用に関する研究分野に若い芽が着実に育っている。このような趨勢の中、電子情報通信学会は平成７年度からソサイエティ制が本格的にスタートする。勿論、本学会にも大きな影響があると思われるが、過去 20 年近い歴史の中で築いてきた相互発展の道を振り返って、相方がより大きな、そしてより新しい発展の方向を模索していかねばならないと思う。

平成６年 12 月に広島市で SITA'94 が、広島大学吉田典可先生を委員長とする実行委員会の先生方の創意と誠意に溢れたご努力によって成功裡に開催された。この SITA'94 会期中に開催された理事会において、電子情報通信学会のソサイエティ制に、本学会が如何に対処すべきかについて活発な議論がなされた。この席で有本会長から「数学者が浴衣掛けで気楽に参加できるような雰囲気を本学会はいつまでも持ち続けて欲しい。」とのご発言があった。これは「初心忘るべからず」ということであろう。昭和 53 年 11 月に開催された第一回研究討論会実行委員会が持っていた数学的雰囲気、そしてその頃持っていたに違いない未知への挑戦の気風を忘れてはならないと、強く自分自身に言い聞かせねばならない言葉でもある。

私自身、情報理論とその応用研究会に始まる本学会活動の中で得たものはとても大きい。その第一は“人とのつながり”である。すなわち、年齢不問の良き友、良きライバルを見い出すことができたことである。昭和 53 年当時の東の幹事であった辻井、韓、今井、原島の各先生、それに西の幹事の有本、平澤、杉山の各先生に巡り合うことがなかったら、私が現在、情報理論、通信方式等の研究を続け、また情報セキュリティ、情報通信倫理等の新しいテーマを見い出し得たかどうか、大いに疑問である。

SITA 活動を通して、著名な先生方と直接お話をさせていただいたことも研究遂行上の大きな励みになったと思う。 53 歳というお若さで惜しくも他界された東京大学教授宮川洋先生には多忙なお時間を割いていただいて、学士会館で色々お話をさせていただいたことがある。話題が情報理論とその応用研究会の学会化の問題に移ったとき、慈愛に満ちた眼差しで「学会化によって今までの良さを失わないように」とおっしゃった。このときの先生のお言葉は、今も強く心の中に残っている。本会の理事を長らく勤められ、現在は顧問をしていただいている重井芳治先生にも私を含めた若い会員の研究意欲を大いに鼓舞していただいた。重井先生は誠に豪放磊落、しかも誠実溢れたお人柄であり、しばしば心を打たれた。研究者としてパーソナリティの大切さを感じたものである。

今年もまた恒例のシンポジウム、SITA'95 が東北大学樋口先生、川又先生、岩手大学三浦先生を中心とする先生方のご努力によって花巻温泉で開催される予定である。実行委員会の先生方の貴重なお時間を何百時間と取り、またさまざまな御心労をおかけすることとなろう。深い感謝の気持ちで一杯である。 SITA'95 を通して若い会員諸氏が研究面での収穫と人との繋がりを得られんことを切に祈願する。

平成７年３月吉日
情報理論とその応用学会の発展を祈りつつ。
会長、笠原正雄

暗号研究と私
－私の Key Paper－

小山謙二(ＮＴＴコミュニケーション科学研究所)

はじめに

私はこの「私の Key Paper」シリーズの愛読者である。特に、田中初一先生、嵩忠雄先生、笠原正雄先生の書かれた含蓄のあるエッセイを読んで感動した。最近、橋本猛、今村恭己両先生から執筆依頼がきた。とまどったが、一大決心をして、私の暗号研究にまつわる半生記をスケッチ風にまとめることにした。

ＮＴＴの研究所に入って今年で 20 年、情報セキュリティと暗号理論の研究を行なって 15 年が経つ。この間に約 50 件の査読付き論文（内 19 件が単名論文）を著した。このエッセイでは、私の研究に深い影響を与えた人達やその著作、あるいは私の論文の中でカギとなる作品についてエピソードを交えて記そう。

暗号研究の伏線

1970 年代、数理パズル愛好家にとって毎年１月上旬は忙しい季節であった。中村義作氏（元ＮＴＴ基礎研究部第一研究室長、現静岡県立大学教授）から出された年賀状パズルを競って解いていたからだ。正解者には先着 10 名まで図書券の賞品がもらえるので、ハングリーな私は熱中したものだ。たとえば、1975 年（昭和 50 年）の問題は以下の通り。「a,bをそれぞれ自然数とするとき、$a^2 - 1975b^2 = 50$ を満たす１組の解は、a = 45,b = 1 です。このような解をあと 3 組求めてください」。問題の意味は中学生でもわかるが、コンピュータで総当たり的に解こうとすると時間がかかりすぎる。この問題は Pell 方程式の解法を知っていると比較的やさしい。中村さんの出題した一連のパズル問題と解答は「続数理パズル」（中公新書）で紹介されている。入社後５年間は、私はプロジェクト研究のかたわら、高木貞治の名著「初等整数論講義」などを輪講で読み、基礎体力をつけていた時代といえる。

暗号研究を始めたキッカケ

1978 年の Rivest-Shamir-Adleman の論文は、公開鍵暗号のアルゴリズムを初めて示したものであり、私に限らず多くの人々に大きなインパクトを与えた。このＲＳＡ公開鍵暗号は現在でも最も有名であり、フェルマーの小定理が見事に暗号化と復号化に反映されている。大きな数が素数かどうかを直接的に判定するのは簡単だが、大きな数を素因数分解するのは非常に難しい。この性質を鍵生成に利用し、暗号の計算量的安全性の根拠にしている。

私がこの論文の存在を知ったきっかけは、1979 年(正月号)の「ＮＴＴ研究所所内ニュース」に載った新しい暗号の紹介記事である。この記事を書かれたのは、池野信一氏(当時特別研究室長、後電気通信大学教授、故人)であり、私の入社時の直属の上司であった。スジのいい研究をいち早く見抜き、本質を分かりやすく解説する筆力には感服した。１月下旬池野さんに部屋に呼ばれ、「この分野の研究をしてみる気はないか」と打診された。数学パズル好きの私は「とにかくやってみたいです」と答えた。

Shamir の功績

現代暗号の推進者を一人だけ挙げるとすると、間違いなく Shamir（シャミア）であろう。情報理論の大家 Shannon(シャノン)、大劇作家 Shakespeare（シェークスピア）など時代を画する偉大な人にはなぜか Sha･･･のつづりが多い。研究社の新英和中辞典をひくと、Shannon という単語がでていた。しかし、その意味はイギリスの最長の川とある。やはり偉大だ。 SITA の会員ならば 100%人名を連想するが、英文学者は上記の地名を連想するようだ。もちろん Shakespeare は人名で出ていたが、Sliamir は未だ出ていない。 Shamir の論文はすべて大きな影響力があり、代表的なものでも次の５つがある。

1. RSA 暗号アルゴリズム(Rivest、Adleman と共著 1978)
2. 秘密分散共有のアルゴリズム(1978)
3. ナップザック暗号の解読(1982)
4. 名前に基づく(ID-based)のゼロ知識認証法(Fiat と共著 1985)

5. DES タイプ暗号に対する差分攻撃法(Biham と共著 1985 から 1991)

これらの論文は論理の流れがよどみなく、記述が簡明であり、技術的内容も分かりやすい。それゆえに、一字一句がズシリと重い。Shamir は現在イスラエルの Weizman Inst.の教授である。いつもサンダルシューズを履き、ブルーのＴシャツとジーンズ姿で国際会議にサッソウと現れる。 ＮＴＴの招聘教授として来日されたときもこの「正装」であった。彼の発想力と解析力の源泉は何か。彼の頭脳を映し出した研究ノートには、「並の論文」になるネタが一杯書き込まれているそうだ。しかし、その中で厳選し、本当に重要と思われる論文しか発表しない。性格は穏やかであり、チュートリアル講演も気軽に引き受けてくれる。ただし、専門書や教科書は書かないのが彼の主義である。

Shamir のＭＩＴ時代の同僚である Rivest は 1991 年に来日された。 ASIACRYPT 国際会議とＮＴＴの CS 研で学習理論と暗号の関係について招待講演を行なった。彼は米国西部風のラフなスタイルと米国東部風のネクタイにスーツという服装の両方を着こなす。彼が社長をしている RSA Data Security 社はレッドウッド(カリフォルニア州)にあり、教授をしているＭＩＴはボストン(マサチューセッツ州)にある。RSA 暗号の誕生秘話も伺った。 Diffie-Hellman の公開鍵暗号の概念などは実現できないと予測し、それを証明しようとしているうちにＲＳＡ暗号が生まれたそうだ。 Rivest は Micali や Goldwasser らの弟子を育てるとともに、最近は計算量的学習理論の分野で活躍している。

最初の暗号論文

公開鍵暗号の研究をやると私が決意してからしばらくすると、一松信先生や土居範久先生の優れた解説がブルーバックスや情報処理学会誌に載った。いくら筋のいいテーマでも、その水脈から水を汲まなければ何にもならない。新しい分野の研究テーマを組織内で正式に提示し、認知されるには、本人が論文を書いて実績を示さなければならない。1980 年前後の数年間は、緊張感と高揚感の入り混じった熱い青春期であった。この時期にたまたま見つけた論文が Shamir の秘密分散共有法である。

秘密(宝島の地図)を分割してｎ人で共有し、ｋ人集まれば元の情報が復元され、ｋ－１人以下ならば元の情報は全くわからない。いわゆる(k,n) threshold scheme を Shamir は整数多項式を使って実現する方法を明らかにした。私はそのうまい実現法と美しさに感心した。私が最初に書いた暗号関係の論文は、秘密分散共有法のアクセス構造を階層構造に拡張したものである。つまり上司と部下の２階層では必ず上司の許可が必要となるようなアクセス構造について、その実現法を明らかにした。この論文は情報処理学会論文誌に 1982 年に掲載された。しばらく後に、西関隆夫先生らはアクセス構造をより一般化した場合の実現法を明らかにされた。エントロピーとの関係を研究する論文も現れ、Simmons がサーベイ論文を盲いているように、その後の一つの大きな研究の流れとなった。

明るい暗号研究会と仲間達

80 年頃、わが国の学会で暗号研究を発表している人は皆無であった。82 年に私的な研究会「明るい暗号研究会」を創った。なぜ明るいかと言うと、公開鍵暗号は鍵管理に限らず学問的にもオープンだからである。この明るい暗号研究会は月に一回土曜日の午後に開かれた魅力的な会合であった。暗号に関する話題について明るく雑談したり、研究の中間結果報告に対して遠慮のないコメントをしたり、最新情報の交換などを行なってきた。当初の参加メンバーは、松本勉氏(横浜国大)、藤原良氏(筑波大、[ウォータルー大学の先輩])、西村和夫氏(当時慶応大、現駒澤大)と私の４人である。この会合は幹事の松本さんのご努力や、会場を提供してくれた東大の原島博教授のご協力もあって、91 年まで約 10 年間続いた。この間に積極的に参加いただいた主なメンバーは以下の通り。辻井重男氏(当時東工大、現中央大)、今井秀樹氏(当時横浜国大、現東大)、岡本栄司氏(当時 NEC、現北陸先端大)、岡本龍明氏(NTT)、太田和夫氏(ＮＴＴ)、黒沢馨氏(東工大)、伊東利哉氏(東工大)、佐古一恵氏(ＮＥＣ)、静谷啓樹氏(東北大)、桜井幸一氏(当時三菱電機、現九州大)、小林邦勝氏(山形大)。

この私的な勉強会と並行して、信学会の ISEC 研究会や SCIS シンポジウムが軌道に乗っていった。 Proceedings が正式に保存される組織(ISEC 研究会など)が整備されるにしたがって、率直で徹底した討論が少なくなっているのはやや残念である。参加者が国際的にも一流になってきたこと、暗号研究が成熟期に入ったこと、および私の関西

への転勤などの理由で、明るい暗号研究会は現在、自然休会となっている。

最も評価の高かった論文

「アパートやホテルの部屋に共通の合い鍵(マスター鍵)があるように、暗号にも個別鍵に共通に代替できる鍵があるといいな」このアイデアを RSA 暗号に適用したのが私の代表的な論文(1982 年)である。

このアイデアは従来の秘密鍵暗号でも存在するのかどうか不明であったので、その道の権威である釜賀一夫氏(ペンネーム加藤正隆:当時「数理科学」誌に連載された暗号の解説記事および単行本「基礎暗号学」の著者)に手紙を書いて問い合わせた。「似たアイデアは秘密鍵暗号でもあるが、RSA 暗号で存在するとは面白い」という丁寧なお返事をすぐにいただき感激した。

RSA 暗号のマスター鍵の存在条件を明らかにし、具体的な導出法を示した。さらに、マスタ鍵のサイズが個別鍵のサイズの単純和よりも小さくできることも実験で確かめた。この論文で信学会の論文賞と米澤ファウンダーズ・メダル受賞記念特別賞(最優秀論文賞)を受賞した。この受賞をきっかけに SITA 事務局から講演依頼がきて、松山で開かれた大会で「招待講演」を行なった。講演料はいただかず、資料代１万円を自費で払った。何か変だなと思ったが、松山城の茶店で甘酒を飲みながら天主閣をながめていると、やっと一人前になりつつある自分に満足感を覚えていた。SITA のコミュニティの雰囲気が気に入り、それ以降大会には自主的に参加するようになった。

1983 年には、この RSA 暗号のマスタ鍵の成果と分散型通信制御の研究成果をまとめて京都大学で博士号の学位を取った。暖かく声をかけてくださり、学生時代からご指導を賜わった桑原道義先生、西川偉一先生、三根久先生に感謝したい。

その後、ラビン暗号にもマスタ鍵があること、同報通信の暗号化に適用できることを明らかにした一連の論文を書き、1984 年に科学技術庁から研究功績者賞(長官賞)をいただいた。私にとって第一次黄金期だったかもしれない。(第二次黄金期は未だ訪れていない....)

初めての国際会議

CRYPTO(米国)、Eurocrypt(欧州)の国際会議が始まったのは 80 年代の初めである。暗号研究者の端くれとしてやや自信の付き始めた私は、世界の第一線の研究状況を知りたくて、年休をとり、自費で Eurocrypt84(パリ)に参加した。良き理解者であった女房と当時の上司(山下紘一氏、塚本克治氏、好田正紀氏)に感謝したい。会場はソルボンヌ大学(パリ大学)の中の一教室である。事前に地図は送られて来ず、当日学内にも案内掲示板がない。あったとしてもフランス語だから分からない。学内を歩いていた暗号研究者らしき人に英語で声をかけ、やっとの思いで会場にたどり着いた。D. Denning らと会い、研究発表の雰囲気を楽しんだ。第一線の暗号研究もこんなものかという妙な自負心が湧いた。しかし、日本でいくらいい論文を発表しても世界には届かないという苛立ちも感じた。また会場案内など会議運営に対する教訓は、後に ASIACRYPT 国際会議(1991 年に日本で開催)の運営に役立った。

専門書を執筆するための雌伏

1980 年代中頃、公開鍵暗号およびそれに関連した計算機数学が広く急激に進展しているのに、内外ともに適切な教科書がないことが不満だった。「誰か書いてくれればいいのに」と思っていた頃、信学会から執筆依頼があった。論文リストが充実した第一級の入門書を兼ねた専門書を著す決意をたてた。２年間は論文は書かずに、本の執筆に専念した。数千の暗号関連の論文を集めて通読した。しかし、重要論文リストに載せる価値があるのはその 1/10 程度であることも分かった。1985 年から１年間、カナダのウォータルー大学に客員助教授として滞在したが、約半分の時間を原稿の改訂に充てた。共著者の池野先生にも励まされながら、1986 年に完成した単行本「現代暗号理論」は、予想以上に好評であった。幸い、1988 年に著し述賞をいただいた。現在までに、専門書としては異例の 5000 部の売上があったそうだ。もし改訂新版を著す機会があれば、ゼロ知識証明、ID-based システム、差分(線形)解読法、数体ふるい法に基づく素因数分解法、楕円曲線暗号などの項目を追加したい。

究極の２次元暗号を求めて

RSA 暗号やラビン暗号は１次元暗号である。２ブロックの平文をからませて２ブロックの暗号文を生成するのが２次元暗号である。１次元暗号を２回適用するのと、２次元暗号を１回適用するのとどちらが得策か。安全で高速な

究極の２次元暗号を構成できるだろうか。

２次元暗号の原型は小林邦勝氏らが 1989 年に提案した２次元ラビン暗号だと思う。 90 年に私は一般化２次元ラビン暗号に拡張したが、一意復号性で不満があった。一方、私は楕円曲線($y^2=x^3+\alpha x+b$なる２次元上の非特異な３次曲線)に基づく素因数分解の数値実験を行なってきた。 1990 年に Vanstone 教授と議論していると、一意復号可能な RSA 型楕円暗号が実現できると思い至った。特殊な素数 p を法とする特定の楕円曲線の位数は$p+1$になることを見い出した。この性質が楕円暗号の鍵生成に使えるのだ。岡本龍明氏との討論結果を含めて、早速 Eurocryt91 国際会議(春)に投稿した。結果は reject だったが、めげずに CRYPTO91 国際会議(夏)に再投稿した。
プログラム委員会から「内容は非常にすばらしいが、同様な内容の投稿が Maurer から出ているのでマージすれば(合作とすれば)、発表を認める」との返事がきた。２つの投稿論文を見比べた。解析の広さと深さともこちらの方が優れていると思った。しかし、同時期に同じアイデアが独立して出現することもあろうと思い直して、共著とした。

1991 年に私は武蔵野の基礎研究所から京都のコミュニケーション科学研究所(CS 研)に移った。ＣＳ研は情報科学の基礎研究を行なうために新設されたＮＴＴの研究所である。 CS 研では、私のテーマは変わらず、RSA 型楕円曲線暗号(CRYPTO91 で発表)を発展させることにした。幸い、新しい同僚に恵まれ、以下の成果が得られた。

1. 楕円曲線上の演算を高速化するアルゴリズムの開発(鶴岡行雄氏と共著 1992 年)、

2. 同報通信において楕円暗号が RSA 暗号より安全であることを示す厳密かつ一般的な解析(桑門秀典氏と共著 1994 年)、

3. １対１通信において RSA 暗号よりも安全または高速な、特異な３次曲線($y^2 = x^3+axy+bx^2$)に基づく暗号の提案(桑門氏と共著 1994 年～1995 年)。

新作の数学パズル懸賞問題

中村先生にならって私も今年初めて、数理パズルを創った。昨年ワイルスが証明したとして話題になったフェルマー予想に関連したものである。問題は以下の通り。

「$x^7+y^7+z^7 = 1995$ を満たす整数解x、y，zは存在するか。ないなら、それを証明してください。あるなら、具体的に数値解を示してください」

今年の年賀状の片隅にこの問題を記入して友人知人に送ったが、3 月 20 日現在、まだ回答がない。年賀状には賞品に関して一切述べなかったが、ある知人が熱心に取り組んでいるらしい。今回、激励と挑戦の意味を込めて懸賞金をつけることにした。辻井先生は自ら考案された ID-based 鍵共有法の解読問題に賞金 3000 ドルを懸けられている。その金額には及ばないが、2000 円分の図書券を先着正解者１名に進呈します。(ポケットマネーで出す懸賞金の額の設定は難しい。お布施のように授ける人の格によって定まる)。なお、私の問題に対する回答期限は、問題の寿命と同じく今年限りです。

2000 円よりも一流誌に論文が掲載されることに価値をおく人には、次の未解決問題をお勧めします。$x^3+y^3+z^3=30$ の整数解を求める問題です。解の発見または非存在証明に成功すれば、J. of Math. Comp.に投稿してください。きっと採録されるでしょう。一般に$x^3+y^3+z^3 =n$, $0 < n < 1000$ の整数解に興味のある方は私の最近の Letter(信学論ＥＡ３月号 1995)が参考になるでしょう。

あとがき

やや自慢話めいたエッセイになってしまった。しかし、一人の人間は周りの人々のお蔭で成長していることが改めて分かった。熱意をもって楽しく持続させる志があれば、一人前の専門家として自立できる。このメッセージが解読されて、若い人々に伝われば幸いである。私自身、未だ「自叙伝」を書く歳ではないと思っている。第２次黄金期を目指して頑張りたい。

電子情報通信学会のソサイエティ制移行と情報理論とその応用学会

－ライバルなのか、パートナーなのか、それとも･･･－

原島 博(東京大学)

はじめに

この４月に、電子情報通信学会がソサイエティ制に移行し、４つのソサイエティと１つのグループが発足した。このうち、情報理論に最も関係が深いのが基礎境界ソサイエティである。そもそもソサイエティ制とは何なのか。今までのグループ制とどこが違うのか。基礎境界ソサイエティの中で情報理論グループは、どのように位置づけられているのか。情報理論とその応用学会とソサイエティの関係はどうなるのか。何よりも、一般の研究者にとって具体的に何がどう変わるのか･･･。このような疑問をお持ちの方も多いと思われる。ここでは、この問題に対しての筆者なりの回答、そして私見を述べてみたい。

筆者のソサイエティ制とのかかわり

まず、ここでの筆者の立場を明らかにしておかねばなるまい。ソサイエティ制に関して言えば、実は筆者にはいろいろなかかわりがある。

電子情報通信学会(以下では通信学会と略称する)においてソサイエティ制の検討が始まったのは、今から 15 年前の 1980 年の５月である。理事会のもとに基本問題検討委員会が設立され、筆者はソサイエティ制を検討する分科会(第１分科会)の幹事を拝命した。初期の頃のソサイエティ制に関する検討報告書は、ほとんど筆者が中心になって執筆している。その後も一種の学識(?)経験者として、ほぼすべての関連の委員会に関係している。

第２は、通信学会の情報理論専門委員会の前専門委員長としてのかかわりである。筆者が委員長を務めた 1993 年度(平成５年度)は、ちょうど研究専門委員会としてソサイエティ制へどう対応するか決断が迫られたときであった。

そして、その次の 94 年度(平成６年度)には、基礎境界研究グループの運営委員長としてソサイエティ制へ向けての準備作業にあたり、引き続いて 95 年度(平成７年度)には、基礎境界ソサイエティの初代会長として、ソサイエティの出発作業を担当することになった。これが第３のかかわりである。

そして第４は、言うまでもなく情報理論とその応用学会のメンバーとしてのかかわりである。筆者は、情報理論とその応用シンポジウムの発足時(1978 年)の幹事の一人であり、学会設立後もいろいろと関係が深い。その意味で情報理論とその応用学会の立場からも、形式的には他学会である通信学会のソサイエティ制発足に強い関心を持っている。

ソサイエティ制とは何か

そもそも通信学会のソサイエティ制とは何であろうか。簡単に言えば、学会の中にある程度独立したミニ学会を作ることである。

基本問題検討委員会が設立された 1980 年当時は、通信学会の会員数は３万人(現在は約４万人)近くになっていた。ところが、その組織は昔のままで、すべてを学会の中央が一元的に管理していた。例えば、研究専門委員会は技術委員会に属していたが、その総数の規制がかかっていたために新しい研究専門委員会を設立することは困難であった。また、論文誌の編集と研究会の活動が別々の組織でおこなわれ、その間の有機的な連携は皆無に近かった。当然会員から見ても、学会の運営組織は自分とは無縁な存在であった。

このような当時の状況に対して、基本問題検討委員会でその当初から構想していたのがソサイエティ制である。専門が比較的近い会員だけでミニ学会を構成し、その中で論文誌編集や研究会、大会活動の有機的な連携をはかる。あわせて会員登録をおこない、ソサイエティ役員を直接選べるようにする。会計的にも原則独立採算にして、収益事業も含めてそれぞれ独自の活動が保証されるようにする。これがソサイエティ制の基本思想であった。

この考え方は、当時の理事会にも比較的好意的に受け入れられた。しかし、急な改革には慎重論もだされ、段階的に移行することになった。こうして、とりあえず 1985 年に研究グループ制がスタートしたのである。

研究グループ制は、学会内部の運営形態だけを分野ごとにある程度独立させようとするものである。その結果、たとえば研究専門委員会は、それぞれの関連のグループ運営委員会に属すようになった。一方で、グループごとの会員登録はおこなわないので、一般会員からは学会がそれほど変ったようには見えなかった筈である。また、独立採算ではなく、論文誌や研究会活動の経費は学会が一括して管理していた。そしてグループの独白の活動は、その運営費(150 万円程度計上)の範囲に限られていた。

本年度(1995 年度)よりスタートしたソサイエティ制は、これをさらに一歩進めたものである。ソサイエティごとの会員登録をおこない(昨年秋に実施)、その登録会員が次期のソサイエティ会長を選挙できるようになった(本年春に実施)。会計も、当初は仮想独立採算とするが、次第に完全な独立採算に移行することになった。仮想独立採算制とは、経理の大部分は学会本部が一括担当するが、項目をソサイエティごとに別に分けて、それぞれの収支がわかるようにすることである。

基礎境界分野のソサイエティをどう考えるか

基礎境界分野は、回路、信号処理、情報理論、音響、さらには信頼性理論なども含めた広い領域をカバーしている。アメリカの IEEE では、このそれぞれの分野に対して異なるソサイエティがある。通信学会でソサイエティを作るとしたら、どのような単位で組織化したらよいのであろうか。基礎境界分野に関連するソサイエティの設立に際して、これがまず問題になった。

もともとソサイエティ制の趣旨は、学問領域を同じくする研究者や技術者の集まりである。その意味では、分野としてまとまりのよい IEEE なみの単位でソサイエティを構成することが望ましい。しかし、一方で IEEE とは会員規模が異なり、もうすこし大きな単位でないと難しいかもしれない。

実は、筆者はソサイエティの大きさ、およびその具体的な組織のイメージとして、情報理論とその応用学会をモデルに考えていた。単独である程度の規模のシンポジウム(大会)を持て、国際会議開催の能力もある。しかも、研究者のネットワーク(人脈)のまとまりがよい。それがソサイエティの条件であり、情報理論とその応用学会はそれを満たしている。

しかし、通信学会においては、ソサイエティ制の検討が思想レベルから実務レベルへ進むにつれて、次第にソサイエティ設立の条件が厳しくなってきた。その代表的な条件は、単独で論文誌を(できれば毎月)発行できること、そして論文誌発行費用まで含めて独立採算が可能であることである。

実務レベルでの検討では、IEEE のソサイエティ制が手本となった。さらに、通信学会には、IEEE の Communications Society と馴染みがある関係者が多く、知らず知らずのうちに、会員数万人のソサイエティ規模を想定してしまったのかも知れない。

いずれにせよ、この条件は基礎境界分野には、きわめて重くのしかかってきた。 93 年度に筆者が情報理論研究専門委員長であったときのことである。

基礎境界ソサイエティ設立前夜

当時は、情報理論の関係者の多くは、情報理論に比較的近い分野だけでソサイエティを作りたいと思っていた。研究専門委員会名でいえば、情報理論、情報セキュリティ、スペクトル拡散などである。情報通信基礎ソサイエティなる名称も、関係者の間ではほぼ合意されていた。これとは別に回路・システム・信号処理分野でも、まとまってソサイエティを設立する準備が進められていた。

しかし、残念ながら結果的にはこの構想は実らなかった。単独で論文誌を発行できること、そして論文誌発行費用まで含めて独立採算が可能であることという条件がネックになったからである。あわせて、基礎境界分野には、信頼性理論や非線形理論など他と組みにくい独立した分野があり、その処遇が問題になった。

さらには、基礎境界分野が、IEEE 的なソサイエティ制に馴染むのかという本質的な問題も提起された。基礎境界分野は、回路や情報理論などの固有の学問を抱えているが、同時にまだ一人立ちができていない新分野や境界分野の育成という任務も担っている。この分野の独立採算は当然ながら期待できない。通信学会でのソサイエティ制の検討に際して、新分野と境界分野の育成策は、実務レベルの検討ではほとんどおこなわれなかったように記憶している。

こうして、基礎境界研究グループは全体として一つのソサイエティを作るべきか、情報通信基礎ソサイエティを独立させるべきか。 93 年 11 月の基礎境界研究グループの運営委員会は、その意志決定の最終期限であったが、筆者

は情報理論研究専門委員長としてぎりぎりまで迷っていた。専門委員の先生方にアンケートで意見を伺ったが、その分布はかなりばらついていた。

繰り返すようであるが、筆者としては情報理論関係だけで一つのソサイエティを作ることが、本来の形であろうと考えていた。その気持ちは今でも変らない。しかし、一方で単独で独立採算で論文誌が発行できるという自信はなかった。また、新分野や境界分野の育成をどうするかという点が最も気になっていた。

回路関係の分野も同じ悩みをもっていたのであろう。筆者の耳に間接的ではあるが、回路関係はそのまま基礎境界に残って、基礎境界ソサイエティを名乗りたいとの意向が伝えられた。もしそうなると、少なくとも形の上は情報理論関係だけが独立して、小規模のソサイエティを勝手に作ったような印象を与えてしまう。

当時の基礎境界研究グループの委員長は篠田庄司先生(中央大)、ソサイエティ制の準備の責任者は副委員長の笠原正雄先生(京都工繊大)であった。両先生とも、少なくとも喧嘩別れの形になることは避けたいと事態を苦渋しておられた。特に笠原先生は、立場は中立であられたが、内心では情報理論分野の将来を真剣に心配しておられた。

結局、筆者はぎりぎりになって情報通信基礎ソサイエティの独立は断念し、基礎境界分野の一本化を決断した。そして、筆者の独断でその旨グループ運営委員会で発言した。実はもう少し情報理論関係者のご意見をお聞きしたかったのであるが、その時間的余裕がなかったことは残念である。もし、なんらかの後遺症が残ったとしたら、それは筆者の責任である。

実は、筆者自身はかなりの後遺症が残ってしまった。最後の基礎境界研究グループ運営委員長として、そして初代の基礎境界ソサイエティ会長として、運営委員会での発言の責任をとらされることとなったのである。

基礎境界ソサイエティの新しい組織

結局、ソサイエティ制は、他の通信、エレクトロニクス、情報・システム分野も含めて、当時の４研究グループがほとんどそのままソサイエティへ移行することとなった。移行は最も簡単であるが、筆者としては、15 年間の検討はいったい何であったのかという無力感だけが残った。

しかし、そう言ってもいられない。次善の策を講じなければならない。94 年度の副委員長の藤井信生先生(東工大)を中心に、基礎境界分野にふさわしいソサイエティ組織の検討に着手した。

その結果、基礎境界ソサイエティの中に分野ごとにミニソサイエティをおくこととした。学会からはソサイエティが一つに見え、実際には研究者グループとしてまとまりがよいミニソサイエティレベルで独立して活動できる、そのような組織を目指すこととしたのである。そして、それぞれのミニソサイエティの代表者は、基礎境界ソサイエティの副会長に就任していただき、ソサイエティ会長のかなりの権限をその副会長に委譲することとした。

このミニソサイエティは規定上はサブソサイエティと呼ばれ、システムと信号処理(回路とシステム、VLSI 設計技術、ディジタル信号処理、コンカレント工学)、情報通信基礎(情報理論、情報セキュリティ、スペクトル拡散)、音響・超音波(応用音響、超音波)の３サブソサイエティが組織化された。信頼性、非線形問題、思考と言語、それに新しく発足した情報通信倫理の各研究専門委員会は、単独では活動が困難であるので、基礎境界ソサイエティ会長に組織上は直結することになった。

このような組織になれば、研究会やシンポジウム、セミナーなどの研究活動は、それぞれのサブソサイエティが独自に実施できる。これに対して、ソサイエティ論文誌の編集、ソサイエティ大会の開催などは、基礎境界ソサイエティ全体で面倒を見ることになろう。

経理はサブソサイエティ単位でおこなうが、独立採算についてはソサイエティ全体でとれていればよことにする。また、ソサイエティとして、新分野や境界分野の育成に力を注ぐこととする。もちろん、そのためには何らかの資金が必要である。そこで、ソサイエティに特別に事業委員会を設け、事業担当副会長を中心に講習会などの各種事業をおこなうこととなった。

ソサイエティにおけるもう一つの重要な活動は、ニューズレター発行などの会員に対する情報提供サービスである。これは、ソサイエティ誌編集担当副会長のもとで責任をもつことになった。

こうしてできあがった基礎境界ソサイエティの組織を図１に示す。結果として、他のソサイエティとは異なる特色のあるものになった。

なお、95 年度の基礎境界ソサイエティ初代会長は、筆

者が引き続いて担当することになり、次期会長すなわち96 年度会長は、登録会員の選挙により笠原正雄先生が選ばれた。

また、情報通信基礎サブソサイエティの委員長(ソサイエティ副会長)には、今井秀樹先生(東大)が関連の研究専門委員会から推薦されて就任した。

情報理論とその応用学会との関係

以上のべたように、通信学会において基礎境界ソサイエティが発足し、その中に情報通信基礎サブソサイエティが組織化された。一方、これとは別に、情報理論とその応用学会(以下、SITA と略称する)が 1986 年より活動を続けている。

この２つの組織の関係はこれからどうなるのか。通信学会会員でない SITA 会員も多数おられるであろう。もしかしたら、SITA は通信学会に吸収されてしまうのではないかと心配される方もあろう。

この問いに対する筆者の回答は簡単である。情報理論研究者の真の意味での日本のソサイエティは、SITA(情報理論とその応用学会)のみである。それは、部分的に通信学会の情報通信基礎サブソサイエティとしての顔も持っているが、両者は基本的には一体である。

情報理論のみならずほとんどの学問分野は、いまや既存の学会の枠を超えて横断的に発展している。注目されている分野は、それぞれの学会が競って学会誌に特集を組んだり、シンポジウムを企画したりしている。しかし、そこに登場する研究者は、ほとんど共通していることが多い。何のことはない。学問分野の啓蒙のために出張サービスをおこなっているのである。

真の意味でのソサイエティは基本的には、志を同じくする研究者・技術者の集団であり、その意味では同好会である。同じメンバーの同好会すなわちソサイエティを、学会ごとに作ることはばからしい話である。

一方で、多くの研究者はホームグランドを持っている。電気系出身者ならば通信学会や電気学会、機械系ならば機械学会、数学系であれば数学会。自分の出身分野以外の学会に多く入会することには、経済的にも限度がある。そのような場合にはそれぞれのホームグラウンドに新しいソサイエティができて、そこで活動できることが望ましい。

この一見矛盾する要求に対する解決策は、「それぞれの学会にソサイエティを作って、それを共通にしてしまうこと」である。学会は沢山あってもソサイエティは一つ、逆に言えば一つのソサイエティの活動が、それぞれの学会から自分の活動のように見えるような仕組みをつくればよい。

SITA についても、その活動が通信学会の情報通信基礎サブソサイエティの活動としても見えるようにしておけば、宣伝効果も抜群である。色々な活動を共催にすれば、通信学会の活動費を使って SITA の活動を活性化できる。会計をきちんとすれば、これは悪いことではない。一石二鳥の考え方だと思うが、いかがだろうか。

むすび

筆者は、SITA も含めてソサイエティはもっとたくましく、しぶとくあって欲しいと願っている。他学会に大きな組織ができたら、それを積極的に利用すればよい。会員４万人の通信学会は、それこそ利用しがいがある。通信学会のソサイエティ制は、それを可能にするための改革なのである。

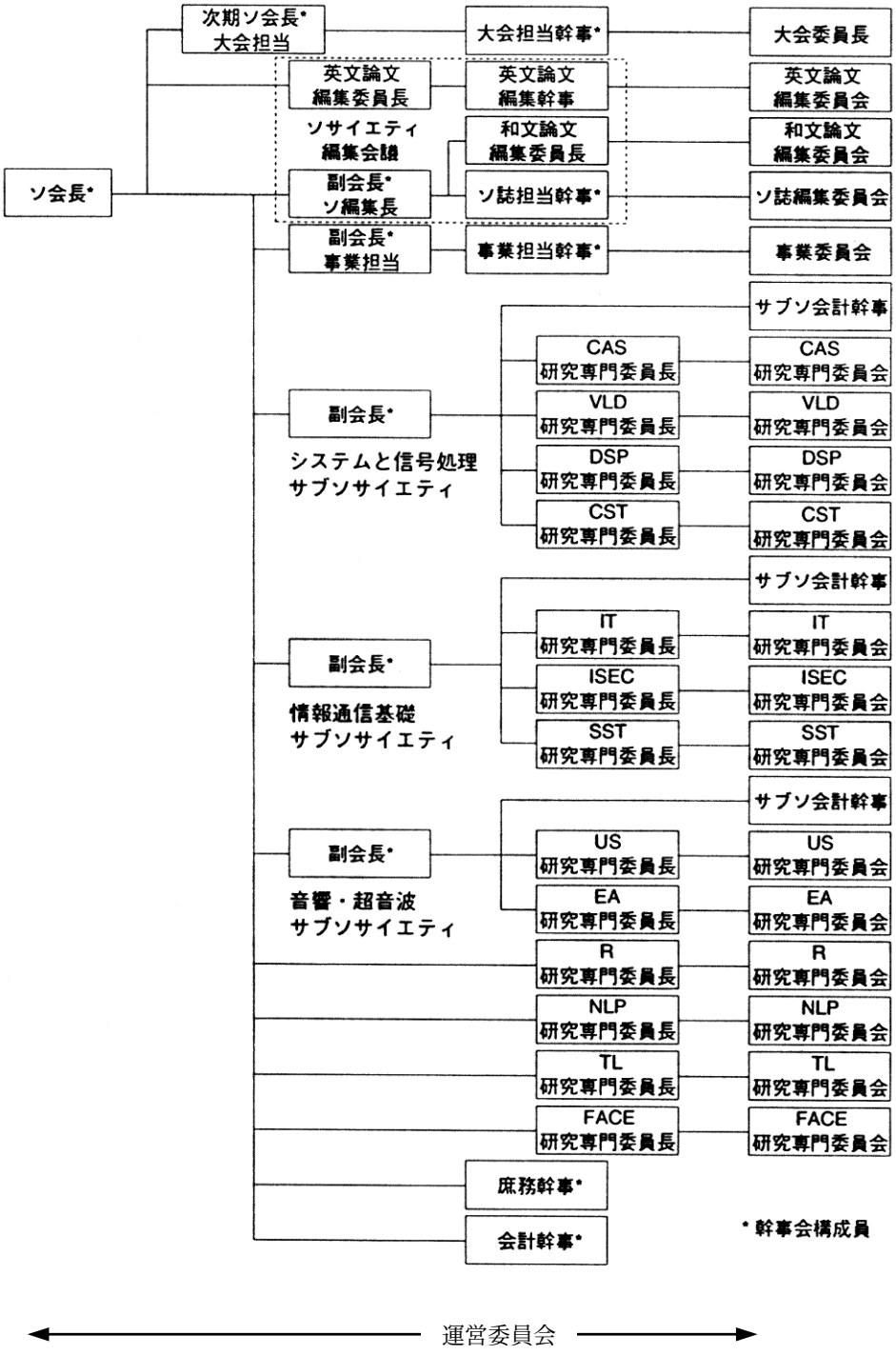

図 1:基礎・境界ソサイエティの組織

SITA における電子メールの活用

企画幹事　山口和彦(電気通信大学情報工学科)

情報理論とその応用学会では、学会会員を対象にしたメーリングリストの運用を開始しました。このメーリングリスト、以下 sita-ml では、

1.ワークショップ等の催しに関する情報の提供

2.会員相互の情報交換

3.会員の個人情報の検索

4.ニューズレターの電子的配布・管理

のサービスを行います。以下では、こうしたサービスを行う経緯と諸問題、実際の利用法について説明いたします。既に sita-ml サービス開始のメールが皆さんに届いている事と思いますが、

1.利用を希望するがメールが届いていない、

2.メールを受け取ったが利用を希望しない、

3.メールアドレスを持っているが、使っていないので
登録を取り消して欲しい、

4.その他の事情がある

などの方は E-mail(sita-admin@lit.cs.uec.ac.jp)又は Fax(0424-82-3055)等にて、管理者(現在は電通大山口が行っています)までご連絡下さい。なお、まだ行き届かない面は多々あると思いますが、メールアドレスをお持ちの方は sita-ml に参加下さるようお願いします。

sita-ml のサービス開始について

最近のネットワーク環境の発展に伴い、私たちの研究環境も電子メール、匿名 ftp (anonymous ftp)、WWW などを利用する機会が多くなりました。情報理論とその応用学会の会員の間の情報の交換がより簡便に行われれば有益であろうという観点から、最も基本的な方法である、メーリングリストのサービスをスタートさせようというものです。

sita-ml(SITA mailing list)は、「情報理論とその応用学会」(Society of Information Theory and Its Applications)の会員の連絡のために作られたものです。

既に、いくつかのメーリングリストに参加されている方も多いと思いますが、簡単に説明します。ある登録されたメンバが、sita-ml@lit.cs.uec.ac.jp というメールアドレスにメールを送ると、自分自身を含む登録されたメンバ（利用休止中のものを除く）に送ると同時に、メールを番号をつけて保存管理するものです。ですから、学会からの連絡案内を伝えると同時に会員の皆さんが情報の発信者になる、それをもとに議論をするなどが可能です。そして、その情報は必要なときに皆さんが取り出す事が出来ます。

もちろん、匿名 ftp、WWW 等のサービスは、さらに多くの利点を有しています。本学会や会員が外部に対してその活動を伝えたり、我々の研究する分野の発展のためにある種の宣伝を行う事も可能です。今後、そうしたサービスを拡充していく事は多くの方が賛成されると思いますが、方針を定めー定の合意を取るべき問題が少なくありません。例えば、現在印刷、郵送で発行しているニューズレターや、情報理論とその応用シンポジウムの論文、その目次などを匿名 ftp で閲覧できれば便利であるという話がある一方で、会員を対象としたニューズレターを会員外に提供することの是非や、論文の著作権の管理などを考えねばなりません。そうした、本学会におけるより進んだサービスの方針について意見を交換するためにも sita-ml を利用できます。

すでに、情報理論とその応用シンポジウムの連絡などにもメーリングリストが利用されていますが、適切なメーリングリストソフトウエアを用いることで、情報を保存し、会員が検索、閲覧を行うことができます。もちろん匿名でない ftp によるサービスを利用する方法もありますが、会員全員にユーザアカウントとパスワードを設定するのは管理が煩雑です。そこで、現段階ではメーリングリストを利用する事としました。

Sita-ml の提供するサービス

既に、いくつかのメーリングリストに参加されている方も多いと思いますが、これから、ネットワークの利用を検討されている方に対する積極的な参加を勧誘の意味を込めて sita-ml のサービスを紹介します。より詳しい説明や変更情報などは、メールリストを通してまた、今後のニューズレタ等の文書を利用してご連絡します。

以下に sita-ml について簡単に説明します。この利用に関する大まかな注意は以下の点です。

・sita-ml から皆さんに届いたメールに対し返事(reply)を行うと、sita-ml@lit.cs.uec.ac.jp 宛に送信されるので議論を始める事が出来ます。

・逆に情報発信者のみに問い合わせ、連絡等を行いたい場合には、返事(reply)ではなく、Sender：の行にあるメールアドレスにメールを出して下さい。sita-ml@lit.cs.uec.ac.jp に送ると登録会員全員に届いてしまいます。十分注意下さい。

・sita-ml@lit.cs.uec.ac.jp に出すメールには Subject 欄に本文の内容がよく分かる様に記入して下さい。後で、あの記事が読みたいという人が検索する時に重要になります。

・利用に関する相談、登録削除、一時離脱などは sita-admin@lit.cs.uec.ac.jp にご連絡下さい。(なお、登録削除、一時離脱は参加者自身によっても可能です。以下に説明します。)

sita-ml では、少し古いソフトウエアですが平野はるか氏による hml と呼ばれるメールリストプログラムを利用しています。先に述べた過去の記事や個人情報の検索なども以下の様に sita-ml@lit.cs.uec.ac.jp にコマンドをメールとして送ることで実行されます。コマンドは、メール本文の第１行目が＃で始まるメールです。すなわち本文が

```
#cmd
^D                              (end of file)
```

という形をしており、cmd には、

help	コマンドのヘルプをメールで受け取る
summary	記事の一覧(記事番号と発信者、Subject)を得る
get ID	ID 番目の記事を得る
off	メール網への参加を休止する(長期不在時等に利用)
on	休止状態からメール網へ参加を復帰する
bye	メール網のメンバから登録を削除する
members	全登録メンバのメールアドレスを得る
actives	休止状態でない全メンバのメールアドレスを得る
Iam	個人情報を登録する(個人情報は続く行に記述)
whois mail-address	メールアドレスが mail-address の個人情報を得る
who	個人情報登録者のメールアドレス一覧を得る

などが利用できます。(注：＃と cmd の間には空白があります。^D は end of file を意味します。) #help を sita-ml@lit.cs.uec.ac.jp に送れば、もう少し詳しい説明が返送されるというわけです。

この sita-ml を利用して、情報理論とその応用学会ニューズレターの配布を試みます。配布形式は、現在は LaTex のテキストファイルとします。その他の形式の是非等はこれから検討したいと思います。ご意見をお待ちています。将来的には印刷物によるニューズレターの配布を希望しない方に申し出ていただく事で印刷費、郵送費等を軽減できるでしょう。なお、管理の分散化にご協力いただけるとたいへんうれしいので、管理運営にご興味がある方の連絡もお待ちしています。

なお、会員の個人情報の検索は、電子メールアドレスに対する、個人名・所属・連絡先等の情報を指しますが、本人の承諾無しに検索可能な状態にするつもりはありません。また、現時点では本人が登録処理をする形にしています。

【編集部より】

計算機ネットワークは情報交換等の手段として研究上欠かせないものとなりつつあります。会員の皆様の中にも既にご存知の方がいらっしゃるかもしれませんが、情報処理学会の学会誌が学術情報センターによって試験的に公開されています。

我が情報理論とその応用学会でも、この様な時代の趨勢に遅れじとニューズレターの電子化の試みが始まりました。会員の皆様にはまず、上記の山口企画幹事の記事を読んで頂いて、お気軽に使ってみることをおすすめします。

今後期待したいサービス、サービス利用に伴う不明な点等この記事に関する御意見、御質問がございましたら是非、高田豊雄(編集幹事、連絡先はニューズレター最終ページ)までお寄せ下さい．今後の記事作りならびに電子化されたサービスのありかたに反映していきたいと思います。

また、電子メールを利用できない、あるいはメーリングリストに加入できない環境にいらっしゃる会員の方の御意見の取り継ぎも行ないたいと思います。

講演会報告

「Wavelet とその応用に関する講演会」報告

佐藤後輪(大阪大学基礎工学部)

標記の講演会を以下のように開催した。

日時:平成６年 10 月１日（土）13:00 - 17:00

場所:京都大学工学部電気系総合館 3F 中講義室

共催:「情報理論とその応用学会」,「電子情報通信学会 変動現象の確率過程モデルと応用に関する時限研究会」

演者・演題:

新島耕一（九州工業大学）「Wavelet の数学的基礎と画像データ圧縮について」

葛目幸一（弓削商船高等専門学校）「Wavelet による心電図信号の圧縮」

伊藤秀一（電気通信大学）「Wavelet 変換による再生歪みを保証する高能率符号化方式」

吉川昭（近畿大学）「Wavelet と時間周波数分布について」

講演の内容を各講師の先生にまとめていただいたので、それを紹介する。

（1）数学的基礎と画像データ圧縮について

ウェーブレットは、最近、画像を解析する手段として注目されている。それは、ウェーブレットが多重解像度解析であることに起因している。 $L^2(R^2)$空間の中に、それに近づく単調増大な部分空間列$\cdots \subset V_j \subset V_{j+1} \subset \cdots \subset L^2(R^2)$を設定し、各ｊに対して、$V_{j+1}$を

$$V_{j+1} = V_j \oplus W_j, \qquad V_j \perp W_j$$

のように直交分解する。W_jの正規直交基底のもとになる関数をウェーブレット関数とよぶ。この分解は、V_{j+1}に属する画像を低周波成分$\in V_j$と高周波成分$\in W_j$に分けることを意味し、ある意味で画像の高圧縮を保証する。多重解像度解析という言葉は、このように、多段階にわたって画像を分解し解析することからきている。この解析にもとづくと、画像圧縮のみならずエッジ検出もできることがわかっている。筆者は、この解析によって画像の鮮明化も可能であると考えている。シミュレーションでは、Ｘ線撮像やＣＴ画像にウェーブレットの多重解像度解析を適用し、画像圧縮や画像の鮮明化を試みた。(新島耕一)

(2) Wavelet による心電図のデータ圧縮

ウェーブレット変換(ＷＴ)による心電図信号(ECG)の圧縮に関し(1)データ圧縮率のウェーブレット関数依存性(2)ECG のＲ波の検出法(3)雑音除去法についての検討を行なった。ＷＴによるデータ圧縮率は用いるウェーブレット関数に大きく依存するが、標本点圧縮率で 13 以上の高圧縮率が得られた。また ECG のＲ波は S/N＝20［dB］の雑音付加時においてもＷＴ逆変換時のウェーブレット係数の適切な選択により容易に検出できることを確認した。またデータ圧縮率は信号に含まれる雑音レベルに大きく依存するが、雑音のない場合のＷＴ変換係数の大

きさ分布のエントロピーが非常に小さいので復元精度を確保するために、同値を小さく設定してもデータ圧縮率は低下しない。しかし雑音が重畳した時には、雑音が除去できないばかりでなくデータ圧縮率の低下を招く恐れがある。本研究では、ＥＣＧのＷＴスペクトルの周期性を利用した雑音除去システムを提案し、雑音が重畳した場合でも閾値を一定に保ったまま圧縮率を低下させることなく雑音を除去できることを示した。(葛目幸一)

(3)Wavelet 変換による再生信号品質を保証する高能率符号化方式

歪みを許したデータ圧縮においては、再生信号の品質を保証した上でなるべく符号化能率を良くする必要のある応用が考えられる。ここではデータ圧縮に Wavelet 変換を適用し、最適なビット割り当てに基づいた符号化アルゴリズムを紹介した。まず信号圧縮において系列依存性に対する対処の方法として、予測符号化、変換符号化(主軸分析、Karhunen-Loève 展開、サブバンド符号化)、ベクトル量子化(ブロック符号化)などを述べ、それぞれの特徴を明らかにした。ついで独立な並列ガウス性情報源に対する合計のレート歪み関数問題の解から reverse water filling の定理を示し、最適なビット割り当て問題の考え方を述べた。さらに、Wavelet 変換による信号圧縮問題の定式化に触れ、最適なビット割り当てに基づくアルゴリズムの提案とその実験結果について述べた。心電図のデータ圧縮に適用した場合に、設計目標として与えられた許容歪みと実際の符号化によって得られた再生歪みの数値とが良く一致していることが示された。心電図のデータ圧縮としてみた場合も、既存の方式に対して優位にあることを主張した。(伊藤秀一)

(4) Wavelet と時間-周波数分布

確定的信号の時間-周波数平面上及び時間－スケール平面上の双線形表現について解説した。双線形表現は信号エネルギーの時間－周波数密度分布を知るために有用である。本解説ではまず、短時間 Fourier 変換と Wavelet 変換の関連を述べた。次いでこれらの２乗として定義される Spectrogram と Scalogram が Wigner 分布を介して密接な関係を持つことを述べた。さらに、Spectrogram と Wigner 分布を要素として含む Cohen のクラス(Ｃ)及び Scalogram と Wigner 分布を要素として含む Rioul-Flandrin のクラス(Ｒ)について説明し、両者の共通部分のクラスが、実は Cohen のクラスの中でも重要な積型の核関数をもつ双線形表現のクラス(P)に他なら無いことを述べた。また、一般に双線形表現のサブクラスとして、時間シフト不変なクラス(Ｔ)、周波数シフト不変なクラス(Ｆ)及びスケール不変なクラス(S)を考えると、Ｃ ＝ Ｔ∩Ｆ,Ｒ＝ Ｔ∩Ｓ,Ｐ＝ Ｔ∩Ｆ∩Ｓ ＝ Ｃ∩Ｒなる明快な関係が成立すること、そして積型関数のクラス(Ｐ)は、時間シフト、周波数シフト及びスケーリング、のいずれに対しても不変な表現のクラスであり、シフト－スケール不変なクラスと呼ばれことを述べた。(吉川昭)

開催日が土曜日であったにもかかわらず、講演会には約 30 名の出席者があり、各講演に対して密度の濃い質疑応答がなされた。開催にあたって新島耕一氏(九州工業大学情報工学部)にお世話になった。ここに記して謝意を表する。

国際会議報告

International Symposium on Information Theory and lts Applications (ISITA‘94)

オスカル(Oscar Yasuo Takeshita)(東京大学)

昨年の 11 月 20 日から 24 日の５日間にわたってシドニーで開かれた International Symposium on Information Theory and Its Applications ISITA '94 は、私にとって様々な点で、充実した国際会議でした。会議はシドニーの Sheraton Wentworth ホテルで行なわれ、国際会議を行なう会場としては、非常に適した環境だと感じました。

“情報理論とその応用”は広い分野なので他の専門分野でも同様であったと思いますが、少なくとも私の専門分

野の“通信システムと符号理論”については高いレベルの研究者が集まっており、興味深い研究内容を聞いたり、また、私自身も一発表者として他の参加者から貴重な意見を受け、有意義な情報の交換ができてとても有効でした。

シドニーは様々な風景をもつ奇麗な街です。連日の恵まれた晴天のおかげで、有名な Opera House、Harbour Bridge、その他様々な所へ観光することができました。シドニーの人々は心がとても暖かく、気軽に雑談したり、街の事を聞いたりすることができました。私を含む同じ研究室の三人の学生は、学会が用意してくれた一番安いホテルに泊まりました。私以外の二人はシャワーがついているツインルームに泊まりましたが、私が泊まったシングルルームには、シャワーとトイレが部屋の中にはなく、廊下をはさんで部屋の反対側にありました。宿泊費が安いのでそれくらいのことは覚悟していましたが、廊下に面したシャワーとトイレのドアは、互いに反対側が見えてしまうような隙間だらけのドアだったのには驚きました。このような意外な点もありましたが、一階にあったバーには私が大好きなビリヤードのテーブルが置いてあり、楽しむことができました。

全体として、とても良い国際会議だと思いました。本シンポジウムの委員の方々に感謝致します。

講演会のお知らせ

第２回若手研究者のための講演会開催のご案内

情報理論とその応用学会(SITA)
非線形理論とその応用学術研究集会(NOLTA)
電子情報通信学会情報理論研究会
電子情報通信学会回路とシステム研究会
電子情報通信学会非線形問題研究会

情報理論、回路理論、非線形理論、制御理論の分野でご活躍の大先輩の先生方より、研究テーマ、研究活動とその感想などについて経験談を交えながらご講演いただきます。奮ってご参加下さいますようご案内申し上げます。

記

日　時：　平成７年７月 14 日(金)13 時-18 時
場　所：　早稲田大学　国際会議場　井深　大 記念ホール(TEL.03-3203-4141)
　　JR 山手線高田馬場駅よりスクールバス 10 分、西早稲田下車徒歩 3 分
参加費：　会員、学生無料。その他 1000 円

プログラム:

(1)講演　笠原正雄(京都工芸繊維大学)　「情報通信の夢」
(2)講演　辻井重男(中央大学)　「現代暗号の不思議」
(3)講演　甘利俊一(東京大学)　「情報幾何学とニューラルネット」
(3)パネル討論　「企業における研究者の育成」

司会　下村尚久(東芝)
パネラー　藤原謙一(元三菱電機)、江尻正員(日立製作所)、青山友紀(NTT)

なお講演会終了後、懇親会を開催いたします。

連絡先	早稲田大学	平澤茂一	TEL.03-3203-4141(73-3451)	FAX.03-5273-7215
		大石進一	TEL.03-3203-4141(73-3424)	FAX.03-5272-5742
		松嶋敏泰	TEL.03-3203-4141(73-3460)	FAX.03-5273-7215
	京都工芸繊維大学	若杉耕一郎	TEL.075-724-7481	FAX.075-724-7400
	法政大学	西島利尚	TEL.0423-87-6342	FAX.0423-87-6126

国際会議のお知らせ

IEEE ITW '95 (INFORMATION THEORY WORKSHOP)
Sunday, June 25 — Thursday, June 29, 1995 Rydzyna, Poland

Invited Sessions and Their Co-Organizers:

Coded Modulation (E. Biglieri, W. Holubowicz)
Communication Theory (B. Vucetic, R. Kohno)
Error Correcting Codes (S. Lin, K. Zigangirov)
Multiple Access (S. Verdu, S. Shainai (Shitz))
Neural Networks (M. Pawlak, N. Tishby)
Shannon Theory (A.D. Wyner, I. Csiszar)
Source Coding (D. Neuhoff, K. Kobayashi)

Organizer of Contributed Papers Session (Evening Session):

Prof. Tom E. Fuja Department of Electrical Engineering, University of Maryland, College Park, MD 20742 Fax: 301-314-9920 E-mail: fuja@eng.umd.edu

Program Committee Members:

E. Biglieri, Politecnico di Torino, Italy
T. Fuja, University of Maryland, USA
A. Jajszczyk, EFP, Poland
R. Kolmo, Yokohama National University, Japan
D. Neuhoff, University of Michigan, USA
S. Shainai (Shitz), Tcchnion, Israel
N. Tishby, Hebrew University, Israel
S. Verdu, Princeton University, USA
S. Wilson, University of Virginia, USA
K. Zigangirov, Univ. of Lund, Sweden
A. Csiszar, Hungarian Academy of Science, Hungary
W. Holubowicz, EFP, Poland
K. Kobayashi, Univ. of Electro-Communications, Japan
S. Lin, University of Hawaii, USA
M. Pawlak, University of Manitoba, Canada
P. Siegel, IBM Research, San Jose, USA
A. Vardy, University of Illinois, USA
B. Vucetic, University of Sydney, Australia
A. Wyner, ATT Bell Lab., Murray Hill, USA

Registration Fees (Proceedings, Room for 5 nights, Meals, Social program):

Fee (single/double)	IEEE members	Non-members
Before May 1, 1995	$ 650/540 ($ 550/440)	$ 720/610 ($ 620/510)
After May 1. 1995	$ 750/640 ($ 630/520)	$ 820/710 ($ 700/590)

ITW-95 Secretariat;

EFP, Mansfelda 4, P.O. Box 31, 60-854 Poznan 6, Poland
Tel: +48 61 483406 Fax: +48 61 483582 E-mail: itw@efp.poznan.pl

ITW '95 Technical Program:

Date	9:00-12:30	14:30-18:00
Monday, 26 June	Session 1 (Error Correcting Codes)	Session2 (Communication Theory)
Tuesday, 27 June	Session 3 (Multiple Axxess)	Session 4 (Coded Modulation)
Wednesday, 28 June	Session 5 (Shannon Theory)	
Thursday, 28 June	Session 6 (Neural Networks)	Session 7 (Source Coding)

1-1 R.Blahut, "On the decoding of codes on curves"
 -2 D.J. Costello, "Are castrophic encoders really bad?"
 -3 R.Johannesson, "On the error probability for list decoding of convolutional codes"
 -4 J.Snyders, "Soft decoding methods of block and convolutional codes"
 -5 A.Vardy, "New results on trellis complexity of block codes"
 -6 V.Zyablov, "Some constructions of concatenated codes based on convolutional codes"
2-1 P.V. Kumar, "Quaternary and binary sequences with low correlation"
 -2 S.Maric, "Performance analysis of families of algebraically designed FH code in various CDMA systems"
 -3 R.W. Yeung, "Multilevel diversity coding with symmetrical connectivity"
 -4 Y.Sato, "Blind carrier phase control in 256-QAM and its joint system to the constant modulus blind equalizer"
 -5 B.Vojcic, "Joint transmitter receiver optimization in synchronous multiuser communications"
 -6 R.Kohno, "Information theoretical aspect of adaptive array antenna systems"
3-1 J.Massey, "Spectrum spreading and multiple accessing"
 -2 T.Cover, "Multiple access investment"
 -3 B.Hughes, "Information theory, coin weighing, and multiuser coding"
 -4 M.Honig, "Rapid detection and suppression of multiple-access interference in DS-CDMA"
 -5 A.Lapidoth, "The effect of mismatch on the multiple access channel and on lossy source compression"
 -6 S.Shamai (Shitz), "Information theoretic considerations for intra and inter cell multiple access protocols in mobile fading channels"
4-1 G.Battail, "Direct combination of Reed-Solomon encoding over GF(q) and q-PSK modulation"
 -2 C.Heegard, "Modulation and FEC for digital cable TV"
 -3 B.Vucetic, "Iterative decoding of block codes"
 -4 M.Trott, "Big non abelian trellis codes"
 -5 J.Huber, "Design of multilevel codes"
 -6 H.Imai, "Perfectly geometrically uniform trellis codes"
5-1 A.Ahlswede, "Theory of information transfer"
 -2 T.S.Han, "Nonserial source coding"
 -3 G.Simonyi, "Information theory and combinatorics"
 -4 P.Narayan, "Channel capacity and the role of the decoder"
 -5 E.Telatar, "Zero-error list capacities discrete memoryless channels"
 -6 A.Wyner jr., "Entropy estimation and patterns"
6-1 J.(Shuki) Bruck, "Neural networks and circuit complexity"
 -2 A. Krzyzak, "On nonparametric classification and nonlinear function estimation using radial basis networks"
 -3 S.Kulkarni, "Consistent regression estimation under arbitrary sampling"
 -4 G.Lugosi, "Concept learning using complexity regularization"
 -5 R.Meir, "Stochastic complexity of learning realizable and unrealizable rules"
 -6 M.Opper, " Supervised learning: information theoretic bounds on predictive errors"
7-1 G.Nelson, "An interesting hierarchical lossless data compression algorithm"
 -2 M. Feder, "Strong lower bounds in universal coding for general classes and for hierarchies of source classes"
 -3 F.Willems, "Weighting algorithms"
 -4 R.Ahlswede, "Rate distortion theory and identification"
 -5 Z.Zhang, "The redundancy of source coding with a fidelity criterion"
 -6 H.Koga, "Estimation of ideal sequences for data compression with fidelity criterion"

SITA レクチャーノート・シリーズのお知らせ

第２分冊「確率課程－応用と話題」出版のお知らせ

小倉久直（京都大学）

本書は本学会のレクチャー・ノートシリーズ全５冊のうちの１冊として昨年６月に出版されました。本学会編集の出版物でありながら、出版をご存知ない学会員の方が多いようなので改めて紹介いたします。

本書は情報理論に関係のある分野で全般的な応用の立場から見た確率過程の話題をとりあげたもので、SITA などで発表された話題も含まれています。執筆には渡辺寿夫・岡部靖憲先生ら数学の専門家も加わっておられますが、全体としては工学・物理学・生物学・医学などへの応用・実用を意図した記述・直観的モデリング・シミュレーション・応用例等が多く与えられています。これらの内容・話題には他の既刊書に見られない新しいものを多く含んでいますが、いずれも応用上重要性の高いもので、現在までかなり研究され将来的にも意味があり、かつ他分野の研究者への問題の提示も含むものです。内容を以下に要約します。

第１章(小倉・八名)はパルス列・ランダム点などの点過程の理論を既設し、最近応用の進んでいる点時系列解析・応用を述べています。第２章(小倉・吉田)では確率場のスペクトル表現・予測理論ならびに確率場システムとしての画像の統計的処理の話題を取り扱っています。第３章(渡辺)では確率微分方程式の記述する解と、計算機などで発生する実際の揺動過程との近似の数学的意味が述べられています。第４章(岡部)は時系列データ問の統計的な因果性、および定常性のテストの理論・解析例がを与えられています。第５章(本田・酒井)では最近応用分野が多くなりつつある周期的な相関を持つ確率過程すなわち周期定常過程の理論と時系列解析の実際の取り扱いを述べています。第６章(小倉・佐藤)では Wiener 過程の非線形汎関数理論の解説と非線形システムへの各種の応用を述べています。第７章(佐藤)は確率過程のあるレベルへの初通過時間・レベルクロスの数学理論・モデルと応用例について広く紹介しています。第８章(添田・佐藤)では待ち行列問題の最近の話題として拡散過程による近似理論を述べています。第９章(吉川)ではデータの時変スペクトルの表現、ウエーブレット解析との関連などの新しい方法を紹介しています。第 10 章(鎌部)では位相力学系の１つである記号力学系の理論とその情報理論・符号理論への応用を取り扱っています。

本書は当初 13 章を予定していましたが、著者の都合で残念ながら 2、3 の興味ある話題を割愛せざるを得なくなりました。また確率過程と必ずしも直接の関係はありませんが情報理論で重要と思われる関連話題(第 9・10 章)も含んでいます。本書は確率過程のすべてをカバーする応用・話題を含むわけではありません。例えば確率過程論の重要な応用分野である確率システム制御・推定理論・時系列解析などのついては他の良書に譲ります。話題によっては内容が一冊の著書となるべきものもあり、ページの限られた本書の記述だけでは十分でない場合もありますが、本書は話題の概観を与えるもので、これによって、学会員諸氏が少しでも確率過程の方向の研究に関心を向けて下されば幸いです。

本書の編集企画は小倉、佐藤(俊)が行ないましたが、計画当初には電気通信大学の御牧義先生が執筆・編集に携わられる予定のところ大変残念なことに急逝されました。本学会の確率過程の研究の重要メンバーであった先生の御業績を偲びつつ御冥福をお祈りしたいと思います。

SITA 事務局時代の思い出

小林(旧姓:余語)菜穂子

情報理論とその応用学会の会員の皆様、お元気でいらっしゃいますか。突然ですが、私のことを覚えていて下さる方はいらっしゃるでしょうか。元事務局の余語菜穂子です(今の姓は小林と言います)。

早稲田大学退職後は、情報理論とはかけ離れた世界におりますが、先日今井秀樹先生(東京大学生技研)と再会する機会に恵まれまして図々しく登場している次第です。

事務局時代は皆様方には大変お世話になり、楽しい思い出が一杯です。特に三回のシンポジウムは心に残っております。まず、一年目は江ノ島の旅館でカナダの女性の方と同室になり、舞い上がってしまいました。二年目は別府の温泉を独り占めできて満足！（九州大学の方には本当によくしていただき、あれ以来九州が大好きになりました）三年目は実家の近くということもあって（犬山）余裕でした・・・？

私事で恐縮ですが、近況を報告いたします。現在私は東京大学薬学部薬品製造工学教室というところで秘書をしております。情報理論のようにスマートな分野ではなく、教室にはシビレエイやなめくじがいます。でも、若く明るい研究室で、元気に働いております。東大にお越しの際は是非お立ち寄り下さい。(内線 4800)

末筆となりましたが、情報理論とその応用学会の益々のご発展をお祈り申し上げます。

次号のお知らせ

「博士論文特集号」

博士論文要旨募集

昨年同様に、次号(6 月発行予定)では博士論文特集を予定しています。本学会に関係ある分野でどのような学位論文が生れているかは多くの会員が知って祝福したいと考えていることだと思います。

学位を最近取得された方の博士論文要旨の投稿をお待ちしています。

投稿は以下の要領で受け付けます。

投稿原稿: 大学に提出する時の要旨のサイズが基本です。昨年のニューズレタ-No.18, 19 の博士論文要旨を参考にして下さい。

原稿形式: LaTeX のソースの形であるのが最も望ましいのですが、印刷したものでも受け付けます。但し、その場合でも文章の部分はテキストファイルの形であることが望ましい。

原稿〆切: とりあえず５月下旬頃です。詳しくは編集理事・幹事にお尋ね下さい。

連絡先: 巻末を御覧下さい。

報告とお知らせ

平成６年度第２回情報理論とその応用学会理事会
日時:1994 年 7 月 22 日(金)，16:00-18:00，　場所:早稲田大学理工学部

平成６年度第３回情報理論とその応用学会理事会
日時:1994 年 12 月 7 日(金)，12:30-14:30，　場所:広島ロイヤルワシントンホテル

平成７年度第１回情報理論とその応用学会理事会
日時:1995 年 2 月 4 日(土)，14:00-17:00，　場所:早稲田大学理工学部

SITA ‘ 94 開催報告
期日:1994 年 12 月 6 日(火)-9 日(金)、　会場:広島ロイヤルワシントンホテル
参加者数:一般(182 名)、学生(147 名)、(外国人:3 名－アメリカ、韓国、イタリアー)、　講演件数:212 件

ISITA ‘ 94 開催報告
期日:1994 年 11 月 20 日(日)-25 日(金)、　会場:Sheraton Wentworth Hotel,Sydney,Australia
参加者数:一般(209 名)、学生(83 名)、講演件数:293 件

SITA ‘ 95 開催案内
期日:1995 年 10 月 24 日(火)-27 日(金)、会場:岩手県花巻温泉ホテル千秋閣
参加・発表申込み締切(予定):1995 年７月１日
問い合わせ先:川又政征(東北大学大学院情報科学研究科、SITA‘ 95 実行委員会事務局、
Tel: 022-263-9411, Fax: 022-263-9411, Email: sita95@higuchi.ecei.tohoku.ac.jp

ISITA ‘ 96 開催案内
期日:1996 年９月 19 日(木)-21 日(土)、会場:Victoria Conference Centre, Victoria, Canada

入会希望者	石田賢治(広島県立大学)	井上晶子(追手門学院大学)	大村道郎(広島工業大学)
	岡野博一(広島工業大学)	川又政征(東北大学)	鴻巣敏之(早稲田大学)
	新家稔央(早稲田大学)	樋口龍雄(東北大学)	堀越淳(群馬大学)
	菊政勲(山口大学)	小田弘(神戸大学)	古賀弘(東京大学)
	後藤正幸(早稲田大学)	中澤真(早稲田大学)	
退会希望者	青木由直(北海道大学)	遠藤一郎	片山徹(京都大学)
	小泉寿男(三菱電機)	坂井義高(ＮＴＴ基礎研究所)	移動通信システム開発(株)

情報理論とその応用学会　1995 年度役員

顧問	滑川敏彦(姫路独協大学)	堀内和夫(早稲田大学)	辻井重男(中央大学)
	嵩忠雄(奈良先端科学技術大学院大学)	Shu Lin(ハワイ大学)	有本卓(東京大学)
会長	笠原正雄(京都工芸繊維大学)		
副会長	平沢茂一(早稲田大学)	今井秀樹(東京大学)	
無任所理事	中川正雄(慶應義塾大学)	畑雅恭(名古屋工業大学)	
庶務理事	山本博資(東京大学)	若杉耕一郎(京都工芸繊維大学)	
会計理事	村上篤道(三菱電機)	小松尚久(早稲田大学)	
編集理事	今村恭己(九州工業大学)	河野隆二(横浜国立大学)	
企画理事	岡本栄司(北陸先端科学技術大学院大学)	古賀敬一郎(ＫＤＤ)	
監事	丸林元(創価大学)	田中初一(神戸大学)	
評議員	磯道義典(広島市立大学)	岩垂好裕(名古屋大学)	大石進一(早稲田大学)
	小沢慎治(慶應義塾大学)	金谷文夫(NTT)	金子敏信(東京理科大学)
	阪田省二郎(電気通信大学)	坂庭好一(東京工業大学)	鈴木孝夫(沖電気工業)
	鈴木秀夫(東芝)	武部幹(金沢工業大学)	塚田啓一(松下電器産業)
	津田俊隆(富士通研究所)	中野幸男(日立製作所)	中村勝洋(NEC)
	荻原春生(長岡技術科学大学)	橋本猛(電気通信大学)	原島博(東京大学)
	韓太瞬(電気通信大学)	樋口龍雄(東北大学)	平田康夫(ＫＤＤ)
	広田修(玉川大学)	森真作(慶應義塾大学)	山内才胤(三菱電機)
	古田典可(広島大学)	吉田進(京都大学)	B.S. Vucetic(シドニー大学)
	V.K.Bhargava(ビクトリア大学)		
無任所幹事	藤原融(大阪大学)	常磐欣一朗(神戸大学)	
	植松友彦(北陸先端科学技術大学院大学)	西島利尚(法政大学)	
庶務幹事	山崎浩一(玉川大学)	稲葉宏幸(京都工芸繊維大学)	
会計幹事	森井昌克(愛媛大学)	松崎敏泰(早稲田大学)	
編集幹事	高田豊雄(奈良先端科学技術大学院大学)	稲積宏誠(青山学院大学)	
企画幹事	鈴木寿(中央大学)	山口和彦(電気通信大学)	

編集後記

今年の第１号をお届けします。編集担当者４人が力を合わせて何とか発行出来ました。私白身は、橋本猛前理事と研究室の上原聡助手との協力により、不慣れな作業を行なうことが出来ました。ニューズレターの価値は掲載記事によって決まると思います。今回も充実した原稿を執筆下さった執筆者の皆さんにお礼を申し上げます。

橋本前理事の発案の「私の Key Paper」シリーズと「学位論文特集号」は好評ですので、今後も続けたいと考えています。今年からの企画としては（1）本学会における電子メールの活用と(2)電子情報通信学会の Society 制移行に伴う課題とを新しいシリーズとして取り上げます。会員の皆さんのご意見を編集担当者にお送り下さい。次号(21 号)からは郵送でなくて電子メールでの配布(LaTeX のテキストファイルの配布)を希望する会員が増えることを期待しています。電子メールでの配布を希望される方は、メールで sita-admin@lit.cs.uec.ac.jp 宛てか編集担当者宛てにご連絡下さい

１月 17 日早朝の地震による阪神大震災は痛ましい事件

です。被災者の皆さんに心からお見舞い申し上げます。(今村)。

本年度より、編集理事としてニューズレターの編集・発行に参加させて頂きます。ニューズレター発刊当初より、幹事として協力させて頂きましたが、気持ちを引き締めて、本学会の機関誌としてニューズレターが会員各位に有効に活用して頂けるように努力致します。面白いアイデアや役に立つ記事をお持ちの方は、お気楽にご連絡下さいますようお願い申し上げます。(河野)

今号よりニューズレターの編集に参加することとなりました。昨今、情報処理学会の学会誌や内外の研究機関のテクニカルレポート、学位論文等が当り前のごとく電子的に公開されるようになっています。 SITA がそのような動きに遅れをとらないよう、私も編集幹事として活発に活動していきたいと思います。(高田)

編集担当者

今村 恭己(編集理事)
〒820 福岡県飯塚市大字川津
九州工業大学情報工学部電子情報工学科
Tel. 0948-29-7662
Fax. 0948-29-7651
E-mail imamura@cse.kyutech.ac.jp

河野 隆二(編集理事)
〒240 神奈川県横浜市保土ケ谷区常盤台 156
横浜国立大学工学部 電子情報工学科
Tel. 045-335-1451,ext.2813
Fax. 045-338-1157
E-mail kohno@kohnolab.dnj.ynu.ac.jp

稲積 宏誠(編集幹事)
〒157 世田谷区千歳台 6-16-1
青山大学理工学部経営工学科
Tel. 03-5384-1111,ext.3507
Fax. 03-5384-6500
E-mail hiro@ina-lab.ise.aoyama.ac.jp

高田 豊雄(編集幹事)
〒630-01 奈良県生駒市高山町 8916-5
奈良先端科学技術大学院大学情報科学研究科
Tel. 07437-2-5211
Fax. 07437-2-5219
E-mail takata@is.aist-nara.ac.jp

情報理論とその応用学会事務局
〒606 京都府京都市左京区松ケ先御所海道町
京都工芸繊維大学工芸学部電子情報工学科
笠原研究室内
Tel. 075-724-7471　　Fax. 075-724-7400　　E-mail kasahara@paylia.dnj.kit.ac.jp