

SITA

情報理論とその応用学会ニューズレター

企業から大学への転身組の雑感..... 岡本 栄司 (北陸先端大)
 成都旅行記..... 末広 直樹 (筑波大)
 第22回情報理論とその応用シンポジウム (SITA99) 開催案内..... 中川 健治 (長岡技科大)
 ISITA2000 Call for Papers
 情報理論とその応用学会 1998 年度役員
 国際会議のお知らせ
 会員情報
 次号のお知らせ

企業から大学への転身組の雑感

岡本 栄司 (北陸先端大)

SITA ニュースレターに寄稿をして下さいと編集担当の方に頼まれたのは、もう半年以上も前になります。まだまだ、回顧する年でもないし、一度はお断りしたんですが、SITA にはたいした貢献もしていないため、強いことも言えず引き受けることになりました。

しかし、引き受けたのはいいですが、人に読ませるような立派な題材を持ち合わせていないため、何を書いているのかさっぱりわかりません。仕方ないので、‘企業からの転身組で小さな大学に所属している一教官’としてエッセイ的に気がついたことを綴ることにしました。全くの雑文であり、研究の話はあまり出てきません。事実関係で間違いや勘違いも多いかとも思います。したがって、読者の皆さんは何も期待せずに読まなくてはいけません。

1 企業と大学

私は企業と大学の両方を経験しているどちらかという少数派です。企業の研究と大学の研究は目的研究と基礎研究の違いがあると、よく言われます。しかし、私の印象では、両者の違いは少なくなりつつあります。その主たる原因は大学側にあると思われれます。すなわち、文部省からの校費がどんどん少なくなることと、大学改革の一つの独立法人化の動きに伴って、研究費は各自の努力で稼げという傾向です。このため、大学人といえども世の中の役に立つ研究が求められているわけで、そうでないとなかなか研究費がつかえません。この点で企業経験者は有利だといえるでしょう。

しかし一方では、‘世の中の動きに迎合しているだけの多数派の研究はしない、少数派でも自分の気に入った研究を行う’という人もいます。これは、格好いいですが、企業ではなかなか難しい研究スタイルです。しかし企業にも全然ないわけではありません。大学でも少数派ですが、周囲の目を気にせず研究続けるには、それなりの宣伝が必要で、「おれはこれこれこういう理由でこの研究をし

ているんだ」と常々言っておかないといけませんからです。従って、確固たる信念を持っていないと難しいでしょう。かといって、多数派に生きるのが楽かといえば、そんなこともないと思います。多数の中で、頭角をあらわすのはそれなりの努力と運と才能が要求されるからです。

大学でも、私のような凡才が少なくとも人並みに研究活動をしようとする、結構大変です。先生一人一人が一城の主になるわけで、いわば社長兼技術者兼セールスマンを行わなくてはなりません。もし、ノーベル賞級の研究成果をあげれば、学生は最小人数だけ受け入れ、学会活動も積極的にには行わずに済ますことが許されるでしょうが。

2 これからの大学

大学の改革が叫ばれています。なかなか手厳しく今までの大学がまったくなくなってないという論調です。十年來の黄ばんだノートを用いて講義し、全然進歩がないとも言われています。でも、いまだそんな骨董品の人が本当にいるのでしょうか。少なくとも周りには見当たりません。確かに、授業のみ行い、卒論や修論学生を持たなければ、楽です。でも、われわれは学生を持たないわけにはいきませんし、持てばそれなりの成果を出さなければならぬので、自分で研究するよりよっぽど大変です。また学生に人気がなく誰も来ない研究室に対する白い目にも耐えなければいけません。ぬるま湯は幻想です。

大学として最も重要なことは教育と研究でしょう。価値あるアウトプットを生み出すには、やはりインプットとして優秀な人と資金が不可欠です。しかしながら、多くの大学は、なかなか優秀なインプットを得ることが難しい状況にあります。一方で、良質のインプットを得るには良質のアウトプットが必要で、これらは密接に関わっています。従って、何とか良いアウトプットを出して、正帰還がかかるようにしなければなりません。

このためには、変換過程が重要になります。すなわち、入学した学生を伸ばすことです。いわば、相対的なデルタを大きくするわけです。一方で、いい研究成果も出す必要があります。いい成果が出ればいい学生が集まるでしょう。このようにして、学生を伸ばしつついい研究成果をあげさせて、絶対値としてもアウトプットが高品質なものに近付ければ、遂には正帰還がかかるわけです。このために、優秀教員と使命感あふれる事務員、資金確保に知恵を絞っているわけです。

この場合、教官は学生を伸ばすことが求められるので、自分の研究だけして論文をたくさん書いていけば済むわけではありません。‘おれの背中を見て育つ奴だけ育てばいいんだ’、ということでは、もはや通用しません。研究ももちろん大切ですが、教育のプロという意識が求められます。このため、わがJAIST（北陸先端科学技術大学院大学）では、教育と研究がしやすい環境を整えています。学部がないので授業の負担が少なく済みませす。通常一人年当たり1.5科目で、私の場合今年は1科目です。年間を通してですよ。信じられないでしょう。さらに、やりやすい環境として、最近は珍しくなくなったのかもしれませんが、セメスター制を採用しています。すなわち、通常の2単位科目は週2回づつ講義して、2ヶ月で終了させてしまいます。年4セメスターのうち4-5月、6-7月、10-11月が実際に授業があるセメスターで、1月以降は授業はありません。その代わりに、その時期に修士1年生は副テーマ研究を行い、2年生は主テーマ研究を發表します。9月と12月は教養的な集中科目月間です。教える側からすると、担当教科が少ないとこの方が断然いいと思います。担当の時だけ集中すれば後は研究室での学生指導と研究に専念できるからです。

事務職員については、公立と私立では、かなり様相が違います。国立では、基本的に2,3年でローテーションするので、せっかく大学のカラーに慣れて仕事を覚えてもらっても異動してしまいます。特にJAISTのようなちょっと変わった大学では、新しい人にまた最初から覚えてもらうこととなります。スタッフというのは、一人非協力というかあまり熱心でない人がいると、全体がその人のペースになってしまうという性格と持っています。従って、理解あるスタッフ、特に課長以上の理解が決定的に重要です。一方、私立では、大学への貢献による評価も徹底しているし、周りから見てもかなり理解を持っているというか、使命感にあふれているように見えます。

再びJAISTを引合に出して恐縮ですが、本学ではスタッフの協力体制が非常に行き届いています。国際会議を開催すると、研究協力課が全面的に支援してくれて、事務局を引き受けてくれます。他に海外から研究員を招聘する時も、事務手続きを相手方と直接英文で電子メールのやり取りしてくれます。誠に助かりますが、しかし、いいことばかりではありません。というのも、秘書を雇えないことになっているからです。人員削減の線にのっとった施策で、その代わりに計算機を充実させて、それで済ませるようにしています。スタッフの協力体制もその一環です。

3 研究室体制

わが研究室の運営方針は、基本的には、人的にも資金的にも大規模にし、各人には自立精神を持たせるという考え方です。この方が、就職に際しても自分の言葉で研究内容を述べられるため有利となるからで、将来自分のためになります。それから、修了までに必ず国際会議に発表させるということもルールに課しています。JAISTではいろいろなレベルの学生がいますが、どんな学生でも国際会議で発表すると自信を持ち、大きく成長します。発表場所は海外でなく、国内でも構いません。中には、成長しすぎて、調子に乗って何度でも発表したがる学生も出てきますが、

研究室の規模を大きくするのは、その方が活気にあふれるからです。私の場合、一人の教官に修士課程1学年5人、博士課程一人で合計13人ぐらいいた方が、生産性が上がるような気がします。一見多いような気がするかもしれませんが、助手もいるので、何とかなるものです。あまり、手取り足取り面倒見るより、自分で進めさせることが重要で、自分の研究成果をあげることも、弟子が成長することに価値を見出す研究者向けのスタイルといえましょう。こうなると、学生と我慢比べの様相を呈してきます。学生が研究にやる気を起こして実行するのを待つか、あるいは手助けをしてしまうか、です。学生から出てくるのがわかっていれば待てるでしょう。しかし、必ずしもそうはいきません。そこで、我慢比べになるわけです。学生といってもいろいろで、細かく指導した方が成果を出す学生も確かにいます。それをあえて出させるのですが、これはなかなかつらいものです。

大規模研究室にするには、結構研究資金が必要となります。大規模だと先ほど述べたように、自主性を大切にするので、情報収集が学生といえども大切になります。すると、学会にも参加させるので、学生が多くなるとその旅費が馬鹿になりません。国内でもちょっと離れると一人5,6万円はかかりますので、一回に百万円近くなります。しかも、旅費ですのでいわゆる校費は使えません。どうみても、科研費、研究助成、受託研究、共同研究、奨学寄付等がないと、確保できません。従って、これらを稼ぐ算段も教官には求められるわけです。

4 学会とのかかわり

最近は学会も増えてきて、どこで話して発表していいものやら迷うくらいです。私の専門の暗号や情報セキュリティ関連の発表では、

情報理論とその応用シンポジウム (SITA, 年1回)
情報理論とその応用学会

情報セキュリティ研究会 (ISEC, 年数回)
電子情報通信学会

暗号と情報セキュリティシンポジウム (CSIS, 年1回)
電子情報通信学会

コンピュータセキュリティ研究会 (CSEC, 年4回)
情報処理学会

コンピュータセキュリティシンポジウム (CSS, 年 1 回) 情報処理学会

があり、われわれは、時期や進捗状況をかながみて適当に選んで研究室から発表しています。研究室が大きいと、発表機会があるということはありません。他に、国際会議がありますが、Crypto や Eurocrypt は質も競争率も高くして学生にはなかなか採択されるのが難しいのが現状です。今まで発表した日本人は 30 人までいってないのではないかと思います。まして、複数回発表した人はかなり少ないと思います。しかし、前述したように、国際会議で英語で発表するというのは学生たち若い人には非常にいい経験になり、その後良く伸びます。この意味で最近学生が発表できる機会が増えてきたのは助かります。わが国主体で行われているか、わが国から始まった学会で

Asiacrypt (毎年)

International Symposium on Information Theory and Its Application (ISITA, 隔年)

International Workshop on Practice and Theory in Public Key Cryptography (PKC, 毎年)

Information Security Workshop (ISW, 隔年)

International Conference on Information and Communications Security (ICICS, 隔年)

などは Springer から Lecture Note in Computer Science シリーズとして予稿集も出る有用な会議です。ISITA は出ませんがもちろん最も有用です。

この中で Asiacrypt はわが国から始まった暗号の国際会議で、2000 年からは Crypto, Eurocrypt と並んで 3 大 Crypto となるのが International Association for Cryptologic Research (IACR) の会員による投票で昨年暮れに承認されました。これは、わが国ばかりでなくアジアやオセアニア諸国の以前からの悲願で、暗号研究を海外に広めてきた諸先輩の努力が実ったものといえます。この実現のために、今井秀樹先生 (初代委員長) を中心として、松本 勉先生らと協力して、各国の代表からなる Asiacrypt Steering Committee を設立し、IACR と協力する姿勢を打ち出したのが理解されたといえます。IACR の Dr. Kevin McCurley 会長と Dr. Thomas Berson 理事に協力を感謝したいと思います。この ASC にはオーストラリア、ニュージーランド、インド、シンガポール、中国、台湾、韓国、日本から各々 3 人を上限としてメンバーが出ています。毎年 2 回ぐらい会合を持っており、Asiacrypt の開催地の決定、アジア太平洋地域の研究レベルの向上を図っています。現在、2 期目に入っており、私が委員長を務めています。

私自身が学会で初めて発表したのは大学 4 年の沖縄で、電気通信学会の回路とシステム研究会でグラフ理論の発表でした。それ以来、多くの学会で発表していますが、海外で最初に発表した時の経験は忘れられません。1981 年の Alerton Conference で、31 歳の時でした。これは、アメリカのイリノイ大学で毎年行われる国際会議で、暗号の発表でしたが、外国に渡るのが始めてだったために、非常に緊張した覚えがあります。

ニューヨークの JFK 国際空港に飛行機が降下しはじめ、窓の外に郊外の家々が見え始めた時、「いよいよ来てしまった」と体が異常に硬直してしまい、お陰で空港でいきなり雲助タクシーに騙されるという洗礼を浴びてしまいました。JFK 空港は単なる中継地でその日のうちにボストンに行くことになっていました。次々にタクシー運転手が「どこへ行くんだ」と声をかけてきて「ボストン」と答えて振り払っているうちに不安になり、ひょっとするとボストン行きの飛行機は別空港から出るのかと思い、つい「いくらか」ときいたら 10 ドルといわれて、なんか安い気がして乗ってしまったのです。ところが実際は隣のターミナルで、ほんの 2, 3 分しか乗らなかったのですが、カーツとなっていたために、騙されたことに気がつきませんでした。あまつさえ、「アメリカでは 15% のチップをあげないといけない」ということだけはしっかり覚えていて、チップまであげてしまい、偉く喜ばれてしまいました。降りた時点でも騙されたことに気づかず、ターミナル内で歩いている時に 10 ドルといえば 2000 円以上だなあと思い出して、やっと騙されたことに気づきました。まったく、情けない限りです。

5 今までの研究

このように失敗を重ねながら、いくつか学会発表をしてきましたが、今までの研究を振り返ってみると、自信作はあまりありません。今までの研究として

- グラフ理論
- 通信理論
- 暗号理論
- 情報セキュリティ

を対象にしてきました。グラフ理論は、東京工業大学の大学院時代に電子工学科の梶谷洋司教授のもとで行なった回路理論的グラフ理論といわれるもので、集中定数回路の素子接続条件から導かれる性質を探ったものです。また、通信理論は NEC の通信研究部時代に行なったデジタルマイクロ波通信における非線形通信理論と呼ばれるものです。暗号理論は NEC の情報基礎研究部時代に主に研究したもので、現在も続いています。JAIST に来てからは、暗号理論だけでなく、耐タンパーソフトウェアやウイルス対策、個人識別などの情報セキュリティに広がってきています。

主な結果を簡単に述べましょう。

グラフ理論： グラフの木集合はグラフ構造から規定されていて、逆に木集合からグラフ構造が規定されます。その関係はさまざまな形態に現れています。そこで、いくつかの主な関係を調べました。たとえば、枝にラベルがついているとして、それらのいくつかのラベルが同一になっている場合でも、木集合からグラフ構造を決定できる場合があり、それらを調べました。また、グラフ理論にはいくつかの著名な定理がありますが、逆にそれらの定理が成立す

るのはグラフのどの性質によるものかを調べ、成立するための必要十分条件を検討しました。

通信理論：ふつう伝送路は線形と仮定されることが多いのですが、実際は電力増幅器を効率的に使うために非線形部分までも用います。そこで、このような非線形伝送路で信号を送った場合に、デジタル通信波形がどのように歪を受けるか、そして誤り率がどのくらい悪化するかなどを研究しました。

暗号理論：暗号は一番長い間研究しており、NECの3年目から今まで18年間研究しています。暗号のみを集中して行ったのはNEC時代で、鍵管理やそれに関連する実装なども行いました。ID情報に基づく鍵配送方式では佐古和恵氏と共に論文賞を受賞しました。暗号に関しては研究ネタがゴロゴロしていた時代で、私のような凡人でも十分にやれたので、運が良かったと思います。また、早い者勝ちだった証拠に、RSA公開鍵暗号の復号に中国人の剰余定理を用いる方式の特許出願し、登録されました。当然、出願人は会社なので今の私には何の権利もありません。他にも多数特許出願しましたが、これほど印象的なものはありません。大学に移ってからは解読手法や秘密分散法、署名方式のほか、応用システムの研究も行っています。解読は企業にはなかなかやれない題材で、評価してもらうのは相当な成果でないと難しいと思います。この点、線形解読を提案し世界で始めてDESの解読に成功した三菱電機の松井充氏はすごいと思います。

情報セキュリティ：情報セキュリティというと暗号も含むのが通例ですが、ここではそれ以外という意味で使います。コンピュータウイルス対策が最初の関わりで、1988年から2年間情報処理振興事業協会(IPA)に非常勤研究員として兼務してその研究を行いました。デジタル署名をプログラムに付加することにより、未知ウイルスでも効ねつける方式を開発しました。これは今IPAから配布されています。その後も、耐タンパーソフトウェア、著作権保護方式などのソフトウェア保護、個人識別等は、主に大学に移ってから行ったものです。これは研究室に学生が多くいるために様々な研究ネタを扱わなくてはいけないことも関係しています。

6 在外研究の思い出

最後に、在外研究の思い出で締めくりたいと思います。1993年の11月1日から1994年8月31日まで、アメリカのテキサスA&M大学数学科に文部省在外研究として滞在しました。秘密分散法で有名なG.R.Blakley教授の招待でしたが、いろいろな意味でいい経験になりました。研究では、Permutation Polynomialというものをいろいろな面から調べました。Permutation Polynomialというのは、有限体 F 上の多項式 $f(x)$ を F から F への関数と見た時に、それが一対一対応になるような多項式をいいます。 x を入力アドレスとみて、 $f(x)$ を出力アドレスとみなせばデータの入れ替えができるので、いろいろな応用は広いものです。多項式がPermutation Polynomialとなるための条件、代数的性質、幾何学的性質などをBobと調べました。

40歳過ぎてからアメリカに滞在したのですが、このような時期が人生にはあってもいいと思いました。面白いことはいろいろありましたが、中でも車にまつわる出来事が忘れられません。それを含む詳しい滞在記は共立出版の蟻塔に連載しました。免許取得、中古車購入、レッカー車移動、盗難、交通違反、交通裁判、売却などを通じて、違う文化をずいぶん味わいました。特に、車の盗難の被害にあったのには驚きました。これについては、蟻塔のほかにも何人かの人にも話してありますが、あらためて書かないではいられません。これから滞在する人には何らかの役にたつかも知れませんし。

滞在を始めて1週間でOldmobileの中古車を購入し、更に2週間目にヒューストンで行われたGlobecom'93に参加するため車で行って被害に会いました。ガレリア地区という、新興の繁華街にある決して安くはないHoliday Inn, Crowne plazaに泊まって、ホテルの駐車場に自分で停めたのですが、翌日見てみるともうそこにはありませんでした。隣にいい車があるのに、なぜ中古車を盗むのかと思いましたが、要するに盗み易いものを盗むのが鉄則らしいです。Globecom開始の初日に盗難が発覚し、その処理のために学会どころではなくなっていました。古い車なので、盗難保険には入ってなかったので3300ドルが一気に消えた感じです。警察に電話すると、「車を盗まれた間抜けな奴」という感じで横柄に聞きとり調査して、最後にCase Numberを付与しておしまいでした。来もしませんでした。実は、このCase Numberが重要で、保険でも何でもすべてはこのCase Numberで処理されます。

ホテルは、駐車場に「盗難その他の一切の責任はとらない」という看板を出してあるので、知らんぷりです。でも、悔しいのでフロントに食い下がると、マネージャーが出てきて、1日の宿泊代をただにしてくれると言ってくれました。それでは引き下がれないので、トップに話しに言ったら、すべての宿泊費用をとらないと言ってくれました。それ以上は、そのホテルでは何もできないので、それであきらめました。アメリカでは、食い下がるとそれだけの見返りがあるものです。

Globecomの最終日の前日に、10マイルほど離れたところに乗り捨てられていたのを発見したと、警察から電話がありました。窓ガラス1枚の破損、ハンドルの付け根付近のカバー破損、1つのタイヤのパンクが損傷のすべてで、たぶん、若いチンピラが盗んで乗り捨てたんだらうとのことでした。すでに、修理工場に運ばれていたもので、応急手当をして、乗って帰りました。お蔭で私は今でも古い車なら鍵がなくても簡単にエンジンをかけられます。すべてにかかった修理費用は400ドルぐらいで、宿泊費用の方が高かったような気がします。しかし、学会はほとんど聞けませんでした。今思い出しても、あの時は本当に心細いというか、情けない気分になりました。

在外研究中は、Bobのおかげで、結構いろいろなところから招待を受けて交流を深められました。

Brian Snow, National Security Agency(NSA)

Andrew Odlyzko, AT&T Bell Lab.

Martin Hellman, Stanford University

Cathy Meadow, Naval Research Lab.(NRL)

Mile Smid, National Institute of Standards and Technology(NIST)

Lalf Swanson, Jet Propulsion Lab.(JPL)

これら招待の招待はすべて受けましたが、割と公的な機関が多いと言えます。他にも、IBM Watson Lab. の Copersmith 博士や University of Wisconsin, Milwaukee の Davida 教授にも招待されたが、都合がつかないので、断念しました。

NSA は日本からだとなかなか入れないところですが、実際に行ってみると、何の変哲もないビルディングで拍子抜けしました。暗号博物館があって、ドイツの Enigma や日本の Purple が置いてありました。また、館長の好意で、普通は入れない部屋まで案内してもらい、第2次世界大戦時の日本の海軍 Code Book を見せてもらいました。表紙に鉄板を入れてあって、海に投げ込めば浮かんでこないようになってました。

在外研究中は夏休み以外単身だったので、趣味の方にも時間が取れました。まず、夕方が暇だったので、ゴルフの練習場に良く行きました。アメリカでは5時以降が長いので、グリーンも回ることができます。Texas A&M 大にはゴルフ場があり、8ドルでプレイできました。また、みんなと囲碁もけっこう楽しみました。私は10年ぶりぐらいなので、かなり腕は落ちてましたが、遊びなので十分でした。夏休みには家族が来たので、車でテキサスからフロリダまで片道丸2日かけてドライブしました。往復では、4日間運転だけしていたことになり、今考えると信じられませんが、よくやったものだと思います。

私は大学に移るときに、‘これからはのんびりできるか’と思いましたが、実際はできませんでした。忙しくしていないとやっていけないのが悲しいかな小さい大学の現実です。とはいいいながら、私のような何の取り柄もない人間がこうしてやってこられたのは大変幸運で、ひとえに皆様のお蔭と感謝しております。この場を借りてお礼申し上げます。

成都旅行記

末広直樹 (筑波大学)

1998年7月に日本学術振興会と中国自然科学基金の共同助成による「日中科学協力」(チャンネル間干渉の無いCDMA方式の性能評価)によって、四川省成都市(Chengdu, Sichuan)の西南交通大学に約半月滞在しました。

Fan Pingzhi 教授とのディスカッションは非常に意義深いもので、連日のディスカッションによってチャンネル間干渉の無いCDMA方式(末広方式)の性能評価について定量的に考察するために十分な準備ができました。(この方式は、今では、W-CDMA方式より約10倍の性能が出ることがわかったと確信しています。)しかし、ここでは、テクニカルな議論は別の機会にゆずって、エクスカージョンの話を楽しみましょう。

半月も居れば、ディスカッションばかりというわけにいかないのは中国でもどこでも同じことだというわけで、まず、諸葛孔明の廟(本当は劉備の墓がメインなはずだが)に連れていってもらいました。この人は三国時代の蜀の丞相で、中国で一番人気のある歴史上の人物です。成都が蜀の都だったのでこれがあるわけです。三国時代は日本でいえば弥生時代の終わりころにあたり、そもそも弥生時代が終わったのは、三国時代の大動乱に耐えかねて一族郎党で海を渡って未開の地に住みついた人たちが日本の歴史を動かしたことによるのです。この時代に中国大陸の人口が9割減ったと言われていました。9割も減った理由は、殺されたよりも食料不足によるものがほとんどだと思います。つまり、農業というのは治安が確保されてはじめて成立する産業ですから、大動乱のときには、収穫した農作物を自分で守る自信のある人たちしか農業をしないわけです。農業生産が9割以上減ったために人口が9割減ったのだと思います。三国時代の後に北方民族が住み着いて、中国語の発音すら変わったようです。日本で使っている発音はこの発音変化以前の発音です。そんなことを思いながらたくさんの人物像(立体的な)を見るとぼくが知っているのはほとんど武将ばかりで、文官はほんの少ししか知らないということに気がつきました。人物像は蜀帝国の文官が半分を占めていました。

次に、三星堆遺跡の博物館に連れていってもらいました。ここは「長江文明」といわれる約3500年前の遺跡で、黄河文明の殷(商)と同じ時代です。十数年前に発見され

たばかりで、古代の四大文明が五大文明になったというほどの大発見です。殷の青銅器文明と大きく異なるところは、青銅器は青銅器でも殷にはほとんどない仮面がほとんどを占めるということです。特に印象的なのは両目に杭を打ち込まれたように見える仮面で、歴史学者たちはこれを古代文献にある「縦目の王」にあてはめようとしているようですが、ぼくのアマチュアの直感によれば、これは悲惨な死に方をした英雄の崇りを鎮めるために神として祭っているもので、こういう考え方は日本にもあります。たぶん梅原猛さんならぼくの考えに賛成してくれると思います。このあたりからはまだまだたくさんの同時代の遺跡が見つかる可能性があり、特に文字を書いたものが見つかるとおもしろいと思うのですが、文字があったのかどうかはわかりません。

成都是食べ物もおいしいです。ほんとうは辛いものが多いらしいのですが、ぼくは辛いものは食べられないので、辛いものを選んで食べましたが、皮付き豚肉の煮込みがおいしかったです。また、西瓜がおいしくて、1個30円くらいの西瓜を毎日食べました。道ばたで西瓜を並べて売っているのですが、客が「これを切ってみる」というと2つに切って、もし客が満足するほど熟れていなければ、別のを切ります。熟れていなかった西瓜はもう売り物にはならないわけですが、客は最後には必ず買うので、(これで1個も買わなければ、喧嘩になってしまいます。)ちゃんと経済が成り立っているようです。

全体として、日本の基準では相当貧乏なような人たちでも幸せそうな顔をして生活しているので、日本の基準が変なのかな?という気がしてきます。おいしいものが非常に安く食べられるので、ほとんどの人は貧乏でも(テレビなどを買えない)不幸ではないと思っているようです。

北京では、おみやげ屋の女店員が「テレビと本で日本語を勉強した」といって、ぼくの英語よりずっとじょうずな日本語をしゃべるので、感心してしまいました。なにしろ人口が日本の10倍いるので、有能な人材も日本の10倍いるわけです。中国からの留学生を多数招聘するのが、長期的に見て日本経済のジリ貧を避ける良策ではないでしょうか?

第 22 回情報理論とその応用シンポジウム (SITA99) 開催案内

開催期間： 平成 11 年 11 月 30 日 (火) ~ 12 月 3 日 (金)
(11 月 30 日午後に電子情報通信学会情報理論研究会)

開催場所： 新潟県湯沢町 NASPA ホテルニューオータニ
(JR 上越新幹線 / 上越線 越後湯沢駅下車 車 3 分)

宿泊施設： 同上 (ホームページあり <http://www.naspa.co.jp/>)
宿泊費 一泊 9,500 円 (4~5 人部屋) ~ 12,000 円 (個室)

シンポジウム日程 (案):

11 月 30 日 (火)

情報理論研究会, レセプション

12 月 1 日 (水)

一般講演, 特別講演, ワークショップ

12 月 2 日 (木)

一般講演, 特別講演, 情報理論とその応用学会総会,
IEEE 東京チャプター総会, 懇親会

12 月 3 日 (金)

一般講演

運営組織： 実行委員長 荻原春生 (長岡技術科学大学)
プログラム委員長 小松尚久 (早稲田大学)

S I T A 9 9 実行委員会事務局

〒 940-2188 新潟県長岡市上富岡町 1603-1

長岡技術科学大学電気系

SITA99 実行委員会事務局 中川健治

TEL.0258-21-4263

FAX.0258-47-9500

E-mail: sita99@comm.nagaokaut.ac.jp

URL: <http://comm.nagaokaut.ac.jp/SITA99/>

今後の主な日程 (案)

発表申し込み〆切 8 月 31 日 (火)

参加者事前申し込み〆切 8 月 31 日 (火)

参加費早期支払い〆切 10 月 15 日 (金)

原稿受付〆切 10 月 20 日 (水)

宿泊申し込み〆切 10 月 31 日 (日)

書類送付に関する注意事項

例年と異なり今年度は S I T A 9 9 に関する書類は郵便ではお送りしません。すべて上記のホームページから必要書類をダウンロードして、それをプリントアウトして使用していただくこととなります。ただし、ニュースレターを郵便で受け取っている方に限り、7 月頃にお送りする申込書類を郵便で送付いたします。その後の書類に関しては申込書類の中のお知らせを参照して下さい。

Preliminary Call for Papers – ISITA'2000

The 2000 International Symposium on
Information Theory and its Applications
Honolulu, Hawaii, U.S.A., November 5–8, 2000

<http://isita2000.soft.iwate-pu.ac.jp/>

International Advisory
Committee Chair
Hideki Imai (Japan)

Symposium General Chairs
Shu Lin (USA)
Eiji Okamoto (Japan)

Technical Program
Committee Chairs
Toru Fujiwara (Japan)
Marc Fossorier (USA)

Treasurer
Kaoru Arakawa (Japan)
Shoichiro Yamasaki
(Japan)

Local Arrangement
Marc Fossorier (USA)

Publicity
Toyoo Takata (Japan)

Registration
Kazuhiko Yamaguchi
(Japan)

Secretariat
Atsuko Miyaji (Japan)
Kanta Matsuura (Japan)

Sponsored by *the Society for Information Theory and Its Applications*.

The first International Symposium on Information Theory and its Applications (ISITA) was held in Honolulu in November 1990. Ten years later, the sixth ISITA symposium is back to its birthplace, in conjunction with the 2000 IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2000).

Authors are invited to submit original papers to the 2000 International Symposium on Information Theory and its Applications, to be held in Honolulu, Hawaii, U.S.A., November 5–8, 2000.

Categories of Interest include (but are not limited to) the following:

- Error Control Coding
- Coded Modulation
- Communication Systems
- Optical Communications
- Detection and Estimation
- Mobile Communications
- Spread Spectrum Systems
- Pattern Recognition
- Signal Processing
- Speech/Image Processing
- Source Coding
- Shannon Theory
- Neural Networks
- Distributed Information Networks
- Data Networks
- Stochastic Processes
- Data Security
- Cryptography
- Chaos and Fractals
- VLSI Communications

Important Dates

- Extended summaries due: March 15, 2000
- Notification of acceptance: June 15, 2000
- Camera ready papers due: August 1, 2000

Author Information

Prospective authors should submit an extended summary of their manuscript. The details of the submission will appear in the web page of the symposium. The proposal should be submitted to:

Prof. Toru Fujiwara
Department of Informatics and Mathematical Science
Graduate School of Engineering Science
Osaka University
1-3 Machikaneyama, Toyonaka, Osaka 560-8531 JAPAN
E-mail: fujiwara@ics.es.osaka-u.ac.jp

国際会議のお知らせ

EUROCRYPT '99

日時 1999年5月2日 - 5月6日
場所 Hotel Hilton, Prague, Czech Republic
連絡先 Jaroslav Hruby, General Chair Eurocrypt '99
Konevova 41, 130 00 Praha 3, Czech Republic
Email: hruby@gcu.cmp.cz
原稿 締切終了 (1998年10月12日)

IEEE International Conference on Communications (ICC '99)

日時 1999年6月6日 - 6月10日
場所 Pan Pacific Hotel, Vancouver, B.C., Canada
連絡先 Ms. Peggy Shepard
Venue West Conf. Services Ltd.
#645-375 Water St.
Vancouver, BC, V6B 5C6, Canada
Tel: +1-604-681-5226
Fax: +1-604-681-2503
Email: congress@venue.west.com
原稿 締切終了 (1998年8月15日)

5th International Symposium on Communication Theory and Applications (ISCTA'99)

日時 1999年6月11日 - 6月16日
場所 Charlotte Mason College, Ambleside, Lake District, UK
連絡先 Prof. B. Honary
Lancaster University
Communications Research Centre
Lancaster LA1 4YR, UK
Email: B.Honary@lancaster.ac.uk
Tel: +44 1524 593015
Fax: +44 1524 594207/381707
原稿 締切終了 (1999年2月8日)

1999 IEEE Information Theory Workshop

日時 1999年6月20日 - 6月25日
場所 Kruger National Park, South Africa
連絡先 Prof. Hendrik Ferreira
Dept. of Electrical Engineering
Rand Afrikaans University
P.O. Box 524, Auckland Park, 2006, South Africa
Email: hcf@ing1.rau.ac.za
Tel: +27 11 489-2463
Fax: +27 11 489-2357
原稿 締切終了 (1999年1月31日)

CRYPT '99

日時 1999年8月15日 - 8月19日
場所 Santa Barbara, California, U.S.A.
連絡先 Donald Beaver, General Chair, Crypto '99
Transarc Corp.
707 Grant St.
Pittsburgh, PA 15219 USA
Tel: +1-412-338-4365
Fax: +1-412-338-4404
Email: crypto99@iacr.org
原稿 締切終了(1999年2月8日)

The Twentieth IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'99)

日時 1999年9月12日 - 9月15日
場所 Asia and Pacific Trade Center, Osaka, Japan
連絡先 Email: PIMRC99@pimrc99.kuee.kyoto-u.ac.jp
原稿 締切終了(1999年2月2日)

37th Annual Allerton Conference on Communication, Control, and Computing

日時 1999年9月22日 - 9月24日
場所 Allerton House, UIUC, Urbana, Illinois, USA
連絡先 Becky Lonberger
Email: becky@bode.csl.uiuc.edu
<http://www.comm.csl.uiuc.edu/allerton/>
原稿送付先 37th Annual Allerton Conference,
University of Illinois at Urbana-Champaign,
Cordinated Science Laboratory
1308 West Main St.
Urbana, Illinois 61801-2307, USA
Email: allerton@csl.uiuc.edu
締切日 1999年7月14日 (3-5 ページ投稿)

1999 Information Security Workshop (ISW '99)

日時 1999年11月6日 - 11月7日
場所 Kuala Lumpur, Malaysia
原稿送付先 isw99-sbm@ecip.tohoku.ac.jp
連絡先 Email: isw99-gen@musm.edu.my
<http://www.musm.edu.my/BusIT/isw99>
締切日 1999年6月4日 (15 ページ以内, 電子メール投稿のみ)

13th AAEECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes

日時 1999年11月14日 - 11月19日
場所 Honolulu, Hawaii, USA
連絡先 Prof. Marc Fossorier
University of Hawaii
Dept. of Electrical Engineering
2540 Dole St., #483
Honolulu, HI 96822, USA
Email: marc@spectra.eng.hawaii.edu
<http://www.irit.fr/ACTIVITES/AAEECC/aaecc13.htm>
原稿 締切終了(1999年1月15日)

ASIACRYPT '99

日時 1999年11月15日 - 11月18日
場所 Singapore
原稿送付先 Dr. Kwok Yan Lam, Co-Chair Asiacrypt '99
School of Computing
National University of Singapore
Kent Ridge Crescent, Singapore 119260
Email: lamky@comp.nus.edu.sg
Tel: +65-8746613
Fax: +65-7794580
連絡先 Dr. Chaoping Xing, Organizing Chair Asiacrypt '99
School of Computing
National University of Singapore
Kent Ridge Crescent, Singapore 119260
Email: xingcp@comp.nus.edu.sg
Tel: +65-8742790
Fax: +65-7794580
http://www.comp.nus.edu.sg/asia99/
締切日 1999年5月10日 (15 ページ以内)

GLOBECOMM '99

日時 1999年12月5日 - 12月9日
場所 The Intercontinental and Sheraton Hotels, Rio de Janeiro, Brazil
連絡先 Professor Raimundo Sampaio Neto
PUC-Rio/CETUC
Rua Marques de Sao Vicente
225-22453-900
Rio de Janeiro, RJ
BRAZIL
Tel: +55-21-274-3664
Fax: +55-21-274-3664
Email: raimundo@cetuc.puc-rio.br
http://www.globecom99.mhw.com.br/
原稿 締切終了 (1999年3月12日)

ISPACS '99

日時 1999年12月8日 - 12月10日
場所 Phuket Arcadia Hotel & Resort, Phuket Thailand
原稿送付先 ISPACS'99 Secretariat
Research Center for Communications and Information Technology (ReCCIT)
King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520, THAILAND
Tel: +662-7372500-47 Ext 5023,5024
Fax: +662-7392350
連絡先 同上
http://ispacs99.kmitl.ac.th/~reccit
Email: ispacs99@kmitl.ac.th
締切日 1999年4月15日 (2-3 ページの拡大アブストラクト)

IEEE International Conference on Communications (ICC 2000)

日時 2000年6月18日 - 6月22日
場所 New Orleans Marriott, New Orleans, LA, USA
連絡先 Mr. Richard W. Miller
Bell South Telecommunication Inc.
Rm. 1050
365 Canal St.
New Orleans, LA 70130
Tel: +1-504-528-2553
Fax: +1-504-528-2387
Email: c.w.miller@ieee.org

2000 IEEE International Symposium on Information Theory

日時 2000年6月25日 - 6月30日
場所 Sorrento Palace Hotel, Sorrento, Italy
原稿送付先 Prof. Thomas Ericson
Linköpings Universitet
ISY, Datatransmission
SE-581 83
Linköping, Sweden
連絡先 Prof. Giorgio Taricco
Dipartimento di Elettronica
Politecnico di Torino
Corso Duca Degli Abruzzi, 24
I-10129, Torino, Italy
Email: taricco@polito.it
Tel: +39-11-564-4084
Fax: +39-11-564-4099
<http://www.unisa.it/isit2000>
締切日 1999年9月15日 (拡大アブストラクト (short paper)/
原稿 (long paper) 送付)

The Eleventh IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC 2000)

日時 2000年9月18日 - 9月21日
場所 Stakis London Metropole, London, U.K.
連絡先 <http://www.pimrc2000.com/>
原稿送付先 Dr. Shuzo Kato
5-25-16
Hinominami, Kounan-ku,
Yokohama 234-0055, Japan
Fax: +81 45 846 8319
Email: skato@ibm.net
締切日 2000年2月25日 (3000 ワードアブストラクト投稿, PDF 電子メール投稿)

GLOBECOMM 2000

日時 2000年11月27日 - 12月1日
場所 San Francisco, CA, USA

情報理論とその応用学会 1999 年度役員

1998 年度第 3 回理事会, 1998 年度通常総会, 1999 年度第 1 回理事会の決議を経て, 1999 年度役員は次の通り決定しました.

顧問

滑川 敏彦	(姫路獨協大学)	堀内 和夫	(早稲田大学)
辻井 重男	(中央大学)	Shu Lin	(ハワイ大学)
嵩 忠雄	(広島市立大学)	有本 卓	(立命館大学)
笠原 正雄	(京都工芸繊維大学)	平澤 茂一	(早稲田大学)
今井 秀樹	(東京大学)	田中 初一	(神戸大学)

会長

原島 博 (東京大学)

副会長

中川 正雄 (慶應義塾大学) 韓 太舜 (電気通信大学)

理事

無任所

山本 博資 (東京大学) 森井 昌克 (徳島大学)

庶務

植松 友彦 (東京工業大学) 笹瀬 巖 (慶応義塾大学)

会計

常盤 欣一朗 (神戸大学) 荒川 薫 (明治大学)

編集

内匠 逸 (名古屋工業大学) 笹野 博 (近畿大学)

企画

山口 和彦 (電気通信大学) 鈴木 讓 (大阪大学)

監事

岡本 栄司 (北陸先端科学技術大学院大学) 畑 雅恭 (愛知県立大学)

評議員

秋山 良太	(富士通)	今村 恭己	(九州工業大学)
岩垂 好裕	(多摩大学)	岩村 恵一	(キヤノン)
大橋 正良	(KDD)	荻原 春生	(長岡技術科学大学)
金谷 文夫	(湘南工科大学)	金子 敏信	(東京理科大学)
河野 隆二	(横浜国立大学)	小松 尚久	(早稲田大学)
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)
高田 豊雄	(岩手県立大学)	田崎 三郎	(愛媛大学)
塚田 啓一	(松下電器)	中野 幸男	(Hitachi Telecom (USA))
中村 勝洋	(NEC)	樋口 龍雄	(東北大学)
藤原 融	(大阪大学)	松嶋 敏泰	(早稲田大学)
丸林 元	(創価大学)	三浦 守	(岩手大学)
村上 篤道	(三菱電機)	森 真作	(日本工業大学)
山内 才胤	(大井電気)	山岸 篤弘	(三菱電機)
若杉 耕一郎	(京都工芸繊維大学)	V.K. Bhargava	(ピクトリア大学)
B.S. Vucetic	(シドニー大学)		

幹事

無任所

山田 功 (東京工業大学) 稲葉 宏幸 (京都工芸繊維大学)

大濱 靖匡 (九州大学) 三宅 茂樹 (NTT)

庶務

渋谷 智治 (東京工業大学) 佐波 孝彦 (千葉工業大学)

会計

伊丹 誠 (東京理科大学) 地主 創 (青山学院大学)

編集

佐古 和恵 (日本電気) 新家 稔央 (神奈川工科大学)

企画

古賀 弘樹 (東京大学) 鴻巣 敏之 (大阪電気通信大学)

会員情報

新入会会員

(正会員) 宮城 茂幸 (京都大) 相良 和彦 (日立) 内田 智久 (LSI ロジック)
高木 清 (LSI ロジック)
(学生会員) 井坂 元彦 (東京大)

退会会員

(正会員) 石橋 義人 (ソニー) 難元 孝夫 (広島大)
(賛助会員) 東洋通信機株式会社 沖電気工業株式会社 日立製作所

会員数 名誉会員 3 名 正会員 425 名 学生会員 22 名
(99/2/10 現在) 賛助会員 16 社

編集後記

ニューズレター第 73 号をお届けします。年度末に発行の予定が 2 ヶ月近くも遅れてしまい申し訳ございません。次号より新スタッフにてニューズレターが発行されます。

(高田)

編集担当者

高田 豊雄 (編集理事)

〒 020-0173 岩手県滝沢村滝沢字巣子 152-52
岩手県立大学ソフトウェア情報学部
Tel. 019-694-2606
Fax. 019-694-2657
E-mail takata@soft.iwate-pu.ac.jp

佐古 和恵 (編集幹事)

〒 216-8555 神奈川県川崎市宮前区宮崎 4-1-1
NEC C& C メディア研究所
Tel. 044-856-2141
Fax. 044-856-2235
E-mail sako@ccm.CL.nec.co.jp

内匠 逸 (編集理事)

〒 466-8555 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. 052-735-5472
Fax. 052-735-5477
E-mail takumi@ics.nitech.ac.jp

松嶋 智子 (編集幹事)

〒 229-1196 神奈川県相模原市橋本台 4-1-1
職業能力開発大学校情報工学科
Tel. 0427-63-9182
Fax. 0427-63-9186
E-mail tomoko@uitec.ac.jp

情報理論とその応用学会事務局
〒 223-8522 横浜市港北区日吉 3-14-1
慶應義塾大学 理工学部 情報工学科
笹瀬 研究室内
TEL: 045-563-1141 ext.3376,3319
FAX: 045-563-2773
E-mail: sita@sasase.ics.keio.ac.jp