AIST-PS-2003-002

情報産業とシステム検証

木下佳樹

産業技術総合研究所
情報処理研究部門
情報科学連携研究体

目次

はじめに　…… 1
システム検証産業にむけて　…… 3
情報産業のための科学技術研究、
　情報産業としての科学技術研究　…… 9

はじめに

独立行政法人産業技術総合研究所関西センターでは、2001 年の発足以来、毎年秋に研究講演会を開催している。2002 平成 14 年は、11 月 7 日に池田市民文化会館にて「情報産業と科学技術研究――くらしの中の頼れる技術」のテーマを設けて開催した。「システム検証産業にむけて」は、この研究講演会で著者が行った講演予稿である。システム検証技術への需要と数理的アプローチを説明、我々情報科学連携研究体での活動を紹介し、最後にこのような技術をもとに事業を起こすとすれば、必然的に情報産業的なものになろう、という主張を述べた。しかし、最後の部分は、講演会において一般的な情報産業そのものの紹介がなされなかったこともあって、十分主張できたとは思われない。今後とも考えていくべき主題でもある。

講演会に先立ち、「情報産業」の概念を共有することを目的として、2002 平成 14 年 7 月 2 日に産総研関西センター池田キャンパスにおいて、関西センター所属の研究員を対象とするワークショップが開催された。「情報産業のための科学技術研究、情報産業としての科学技術研究」はそのワークショップにおける講演記録である。梅棹忠夫氏によって提唱された情報産業の概念は、産総研研究者に必ずしも正確に理解されているとは限らず、情報機器産業、ソフトウェア産業などの狭い意味にとらえられている場合も多いからである。講演では、科学技術研究をすすめる立場からではあるが、できるだけ正確に情報産業の考えを紹介するよう努めたつもりである。

2003 年 2 月 7 日

尼崎にて　木下佳樹

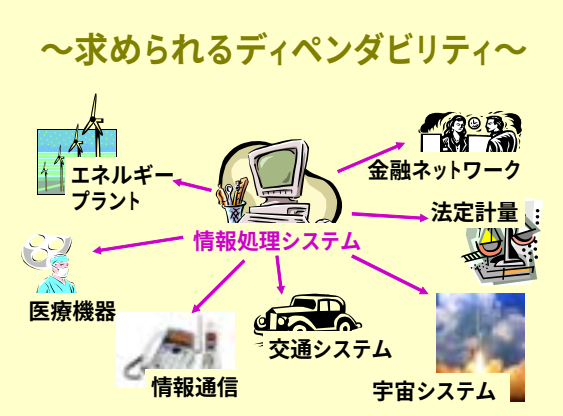
システム検証産業に向けて

2003平成15年1月24日

(独) 産業技術総合研究所
情報処理研究部門　情報科学連携研究体
木下佳樹

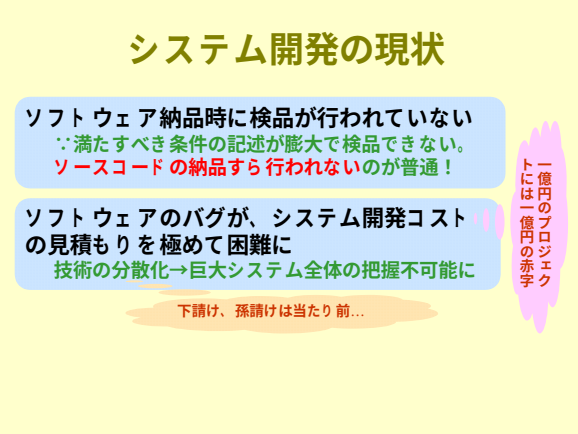
きょうは、「システム検証産業に向けて」と題しまして、数理的なシステム開発方式とそれに基づく検証の技術、さらにその技術を基盤とする産業の可能性について、お話するつもりでございます。

情報技術が社会のすみずみに浸透した結果、あらゆる機械がコンピュータによって制御されるようになりました。小はガスメータやタクシーメータなどの計量器、医療機器、クレジットカードから、大は航空や鉄道などの交通システム、原子力発電所の制御に至るまで、情報処理に無縁なシステムは今やありません。情報処理システムが誤動作して、甚大な影響を及ぼす様子は、今春のみずほ銀行事件、昨年のDoCoMo 携帯電話回収事件などの際に、新聞テレビの報道を通じて、つぶさに見聞したとおりでございます。また、EU のロケット Arian 5 が、ソフトウェアのバグが原因で発射後一分足らずのうちに墜落した事故は有名です。産業技術総合研究所が所掌する業務の一つであります法定計量の世界でも、計測器の電子化、コンピュータ制御化が進んだ結果、秤などの計量器の検定法をか

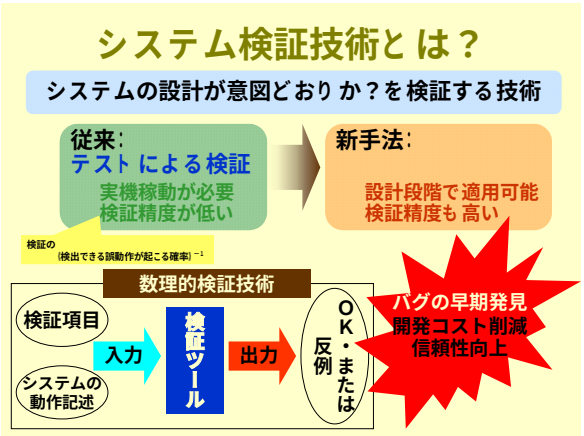


えていかなければならない、という問題がでてきております。

情報処理システムの誤動作、いわゆるバグは、システムを利用する側に大損害をもたらすわけですが、一方で、情報処理システムの開発者にも大きな影響をもたらしています。バグは、いつ何処で発生するか、前もってわかりませんし、発生した場合に、どれだけの労力とどれだけの時間をかければ退治できるのかも、よくわかりません。バグのせいで、開発コストの予測がほとんど不可能になっているのです。バグのせいで、一億円のプロジェクトには一億円の赤字、などという話もあります。LSIの開発では、開発工程の７０から８０％の期間は何らかの形でデバグ、つまり検証が行われているというデータがあります。システムを利用する側だけではなく、開発する側からも、システムを検証するための、より強力な方法が求められているわけです。



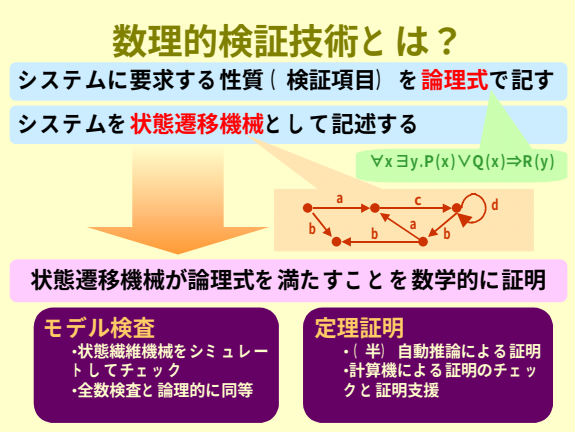
システム検証と申しますのは、文字通り、システムが誤りなく動くかどうか、を確かめることです。現在、検証のためにふつうに用いられている方法は、テストによるものです。この方法では、システムを実際に動かしてみて、意図どおりに動いているかどうかを観察します。昔から、機械システムに用いられてきた検証方法ですが、情報処理システムの検証にも、テストによる方法が主に用いられています。



テストによる方法には、滅多に起こらないのだけれど起こったら甚大な影響を及ぼすバグ、たとえば人の命にかかわったり、巨大な経済的損失を招くような種類の誤動作を見つけにくいという問題があります。あらゆる場合、あらゆる事象をつくしてテストできれば、このような問題は起こらないのですが、たいていのシステムでは、すべての場合の数をつくすと無限、あるいは非常に大きな天文学的数になってしまうので、「怪しそうな」境界条件を考えて、そのような場合を取り出して集中的にテストするのが普通です。しかし、この「怪しそう」という判断が問題です。情報処理システムの重大な誤動作の詳細な解

析がいくつか行われていますが、思いもよらない、想定外の事象に関する動作に問題があったという場合が多いのです。

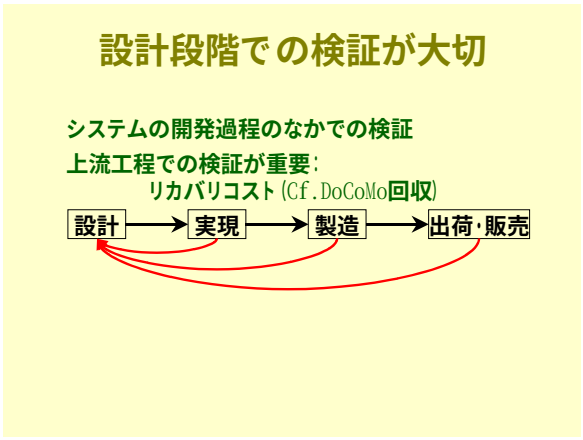
テストによる検証を補う方法として研究されてきたのが formal method、日本語で形式的技法あるいは数理的技法と呼ばれるものです。数理的技法では、まず情報処理システムの動作仕様を、日本語や英語ではなく、論理式で記述します。一方、情報処理システム自体を、状態遷移機械、いわゆるオートマトンとして記述して、これが、動作仕様の論理式を満たすことを示します。



数理的技法には、大きく分けて二つのアプローチがあります。一つは、論理的な推論を積み重ねて証明する定理証明法で、これにはさらに、計算機によって 100%自動的に定理証明しようとするアプローチと、人間が証明するのを計算機が手助けするというアプローチの二つがあります。完全な自動証明をするには、論理体系の記述力をある程度制限する必要があることが原理的に知られています。

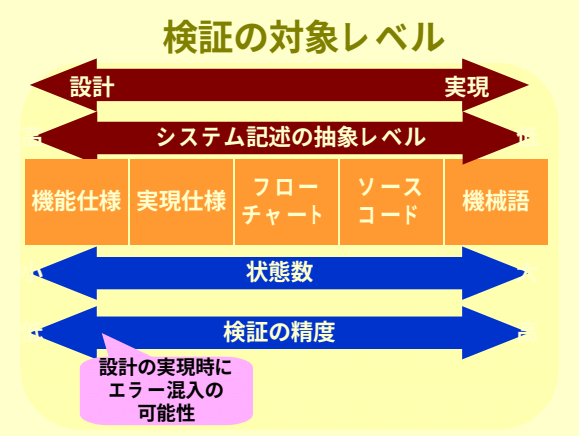
もう一つは、設計図にもとづいて情報処理システムを計算機によって模倣、つまりシミュレートし、計算機のパワーをつかってしらみつぶしに調べようという方法で、モデル検査とよばれるものです。これは場合の数が有限個でないと使えない方法ですが、LSI 設計など、随分広い範囲の問題に対して実用化されつつあり、現在注目を集めている手法です。

定理証明にしろ、モデル検査にしろ、境界条件だけを抜き出す必要がなく、あらゆる条件のもとでの検証が行われます。また、テストの場合、設計→試作→検証→バグ発見→設計というサイクルで検証が進められますが、数理的技法では実機を動作させる必要がないので、このサイクルから試作段階を削ることができ、効率よくすることができます。これらはテスト法に比べてよい点ですが、不利な点もいくつかあります。



設計そのものが矛盾なく、意図どお

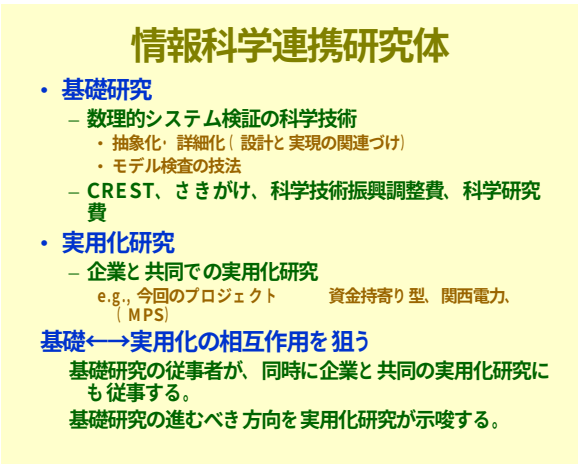
りになされているか、という、設計段階での検証には、数理的技法はうまく働きますが、設計を正しく実現したかどうか、という実現段階の検証には数理的技法はあまり向きません。数理的技法では、計算機の中に、対象となるシステムの記述をいったん作り上げてしまう必要がありますが、状態遷移機械は仕様記述に比べて、格段に記述量が多く、計算機がパンクしてしまう、という問題が生じるのです。



実際にソフトウェアシステムの開発にあたった経験をお持ちの方であれば、設計段階で意外に多くのバグが出てしまい、しかも設計でのバグは設計のやり直しを迫りますから、とり除くのに手間暇がかかる、ということに同意していただけるのではないかと思います。設計を実現するときに混入するバグも、確かにありますが、それはいわゆるケアレスミスで、見つかれば除くのは簡単な場合が多いのです。

設計のバグを数理的方法でみつけ、実現のバグをテストで見つける、と大まかに考えるのがよいようです。

私ども情報処理研究部門情報科学連携研究体では、数理的方法にもとづく検証法の研究を行っております。モデル検査の研究、抽象化と呼ばれる、モデルの変換の方式の研究などの、基礎研究が、研究グループとしての中核となる活動で、本年度より科学技術振興事業団の戦略的創造研究推進における研究プロジェクトを５年計画で開始することとなり、ほかに、同じく科学技術振興事業団のさきがけ２１、科学技術振興調整費、科学研究費補助金など、最近、「競争的研究資金」と呼ばれておりますような種類の研究予算で活動しています。



一方で、基礎研究に携わる研究者が同時に実用化プロジェクトにも関係する、という方針をたてまして、企業と共同で、数理的技法の実用化プロジェクトを四つばかり進めております。相手の企業からは資金提供を得たり、技術的な協

力を得たりと、積極的な参加をいただいております。おかげで大変忙しい思いをしておりますが、実用化の試みから基礎研究の新しい問題が見つかるのではないかと期待しております。

この実用化研究の試みを始めて、私どもが身にしみてよくわかったことが一つございます。理屈ではわかっていたのですが、実際に現場に近い方々と一緒に仕事してみて、数理的技法は、検証段階だけに導入できるものではない、ということがよくわかりました。仕様を論理式で記述することが数理的技法による検証の大前提なのですが、実際には、論理式どころか、日本語で書いた仕様も全く存在せず、ただソースコードだけ、ひどいときにはオブジェクトコードだけがあり、仕様は開発者の頭の中にだけあったのだが、開発者の移動とともにどこかへ行ってしまった、あるいは忘れられてしまった、という例が多く見られます。これでは数理的技法を使おうにも手も足も出ないわけです。

実用化研究からの教訓

- 数理的技法導入には開発過程全体の変更が必要
  - 仕様書が頭の中だけにしかない場合も！
- 企業に理解していただくことの必要
  - 産総研コンソーシアム「システム設計検証技術研究会」

数理的技法は、欧米では 20 年以上前から研究分野として確立し、産学にまたがる大きなコミュニティができていますが、日本では、企業に知られていない場合も多いようです。数理的技法を企業で導入していただくには、ソフトウェア開発過程全体の変更を求めなければならず、そのためにも、数理的技法の存在を企業に対してアピールすることが必要だと考えまして、システム設計検証技術研究会なるものを始めました。

最後にシステム検証の科学技術に基づく産業のお話をしてみようと思います。産業につきましては私は全くの素人でございますので、これまでの話とちがって、以下の話はどうぞ眉にツバつけてお聞き願いたいと存じます。

システム検証産業に向けて

- 独立検証・実証 （IV&V）
  - NASA IVV
  - 日本：コンパイラの第三者検証
- IV&Vの産業化
  - 開発費の2%でバグがとれる？
  - Cf. 一級建築士
  - お墨付きを扱う ⇒ 情報産業

独立検証・実証という言葉がございます。英語で Independent Verification and Validation、アメリカ流に縮めて IV&V などと呼ばれています。これはシステムの検証を、

開発者の立場からではなく、システムの内部を知らない第三者が行うようでないと十分な結果が得られない、という話です。NASA では常勤研究者が 130 名規模の IV&V の研究所を十年来運営して、宇宙機器制御ソフトウェアの信頼性向上を図っています。日本でもコンパイラを作るところなどでは、検証専門の部署を作って第三者検証を昔から行っているようです。しかし、そのほかの殆どのソフトウェアについては、第三者検証は全くといっていいほどなされていません。

はじめに申しましたように、ソフトウェアの信頼性は、ユーザ側からも開発側からもますます大きな問題になっております。そこで、近い将来、第三者検証を専門に請け負う仕事が産業として成立するのではないかと考えておる次第です。ちょうど、建築における一級建築士の仕事にあたるものです。建築の場合、建設業者でも施主でもない、第三者の一級建築士が出来上がった建物を検査することになっています。そのような仕事の情報処理システム版ができていくのではなかろうか、というわけです。そのような仕事があれば、これはまさに、情報産業の一つといえるでしょう。「ちゃんとできている」というお墨つきは一種の情報だからです。開発費の２％を投入することによってバグ発見の効率が飛躍的に上がり、開発コストがある程度予測できるようになるとすれば、積極的に検証に投資しようとする企業が多数でるのではないかと思うのですが、この辺、どうお考えになるかは産業で実務に携わっておられる方々に伺ってみたいところです。

このようなシステム検証産業の基盤となるのが、今回お話したシステム検証の技術です。システム検証の技術を、数理科学をもちいてできるだけ客観的に記述し、一部の熟練技術者だけではなく、勉強さえすれば誰でも身につける技術にしたてていこう、というのが我々が現在格闘している実用化研究の意図でございます。

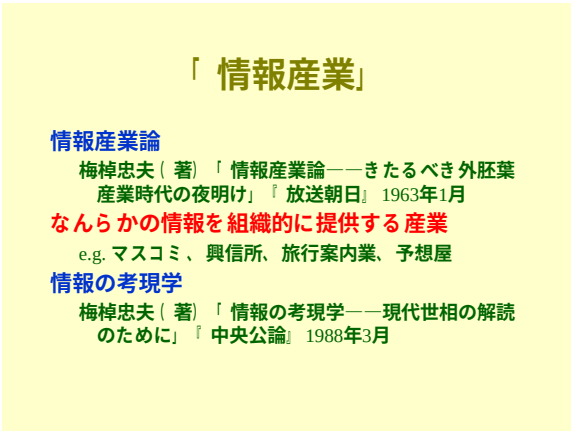
どうもありがとうございました。

情報産業のための科学技術研究、情報産業としての科学技術研究

木下佳樹
情報科学連携研究体

「情報産業」をキーワードにして秋の講演会を企画してはどうか、と提案した者として、情報産業ということばの由来と正確な意味を説明するオブリゲーションを感じています。また、今回のワークショップのテーマで情報産業と科学技術研究がどんな意味合いで並べられているのか、も説明しなければならないと考えています。15 分では、副題の「暮らしの中の頼れる技術」までは説明できそうにありません。

さて、この情報産業というコトバは、日本で使われはじめたものでして、英語に information industry というコトバがあって、それを翻訳した、というようなものではありません。1963 年、いまから 39 年前に梅棹忠夫教授が放送朝日という、朝日放送の社内報に「情報産業論」という論文[1)]を書かれたのがはじめのようです。梅棹忠夫さんは、ご承知のように民族学博物館を作った学者ですが、一方で、情報に関する考察も少なからず行っておられまして、岩波新書の「知的生産の技術」[2)]が広く読まれたことは、現在 40 歳以上くらいの方ならよくご存知かと思います。

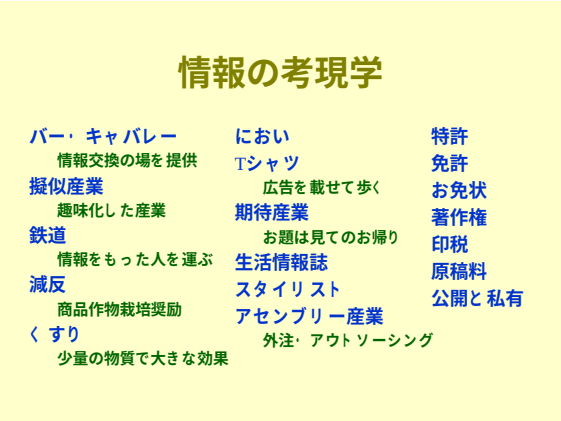


「情報産業論」では、情報産業は「なんらかの情報を組織的に提供する産業」と規定されています。そうして、

> 情報のさまざまの形態のものを「売る」商売は、新聞、ラジオ、テレビなどという代表的マスコミのほかに、いくらでも存在するのである。出版業はいうまでもなく、興信所から旅行案内業、競馬や競輪の予想屋にいたるまで、おびただしい職種が、商品としての情報をあつかっているのである。

と、いかにも民族学者らしい観察を述べておられます。

その後、1988 年の論文「情報の考現学――現代世相の解読のために」[3]では、



情報交換の場所を提供しているバーやキャバレー、一坪農園などの趣味に資する擬似産業、情報を持った人を運ぶ鉄道、商品作物の栽培を奨励する減反、微量でおおきな作用をもたらす薬、においを売り物にする産業、ブランドネームなどの広告を載せたＴシャツ、音楽会などの興行における期待産業、生活情報誌、スタイリスト、アウトソーシングを徹底したあとに最後まで残るであろうアセンブリー産業などの例をあげておられます。

また、特許、免許、お免状、著作権、印税、原稿料、公開と私有など、情報産業特有の現象についても考えておられます。

これらの論説は中公文庫「情報の文明学」[4]に収められていて、手に入りやすく、またどちらも短い文章なので、是非ご一読をお勧めいたします。内胚葉産業である農業、中胚葉産業である工業に対して、外胚葉産業の情報産業は脳神経系への刺激に関する営みなのだ、とか、情報はコミュニケーションとは独立に存在する、などの興味深い観察がいくつも述べられています。

農業、工業、情報産業と並べると、アルビン・トフラーの「第三の波」[5]、ダニエル・ベルの「脱工業社会の到来」[6]などを思い出す方もおられるでしょうが、梅棹忠夫の「情報産業論」は第三の波の十数年前に発表されています。

情報産業についての説明はこれくらいにして、次に「情報産業」と「科学技術研究」をどんなつもりで並べたのかについてお話いたします。そのために、先ほど出てまいりましたアセンブリー産業に注目いたします。

アウトソーシング、つまり外注化を行った究極にあるもの典型例として、梅棹さんは出版業をあげておられます。たしかに、出版社で印刷所や製本所まで持っているところは少ないでしょう。なかには企画、編集、レイアウトまで外注する出版社もあるそうです。外注を徹底的にすすめて、最後まで残るのは製作過程の管理機能だけということになるようです。

アセンブリー産業は出版業に限りません。「情報の考現学」から少し引用します。

> そういえば、今日の工業自体がかなりの程度にアセンブリー産業である。巨大な自動車会社といえども、下請企業から部品のアセンブリーによって最終製品をつくりだすのである。その点では、現代の代表的機械工業である自動車会社も、出版業や織物業とかわらない。
>
> ただ決定的に違うのは、出版業や織物業では、その中心に代がえのきかない個別的な情報が鎮座しているのである。関連する工業的部品産業が、いかに高度の生産能力をそなえていても、この情報という一点をぬきにしては、なにものも生産することができない。出版元や織元は、この情報というかなめの一点をおさえているのである。
>
> 近代機械工業は、その生産の過程から、かなりの部分を分離して外注化した。しかし、おそらくは最後の組みたての工程だけは、自社内に保有するであろう。出版業や織物業のように、徹底した発注産業になれば、これはもう工業としての顔がたたなくなるであろう。

こんな引用をすることによって、工業生産を軽くみよう、と主張したいのではありません。外注化を徹底し、工業生産的要素を全く除いたあとに、まだ、一つの会社を営んでいくに足る仕事が残っている、しかも、その部分が他の部分を決定的に支配しうるという事実に注目したいのです。

情報産業のための科学技術研究

工業内部でも外注化がすすんでいる
　下請け
外注化の徹底　→　アセンブリー産業
　e.g., **出版社、放送会社**
「外注化」＝「工業から情報産業への移行」
∴
　Cf.　**研究の出口論**

さいごに残る仕事は、生産過程を管理する情報の処理だといえます。外注化とは工業から情報産業への移りかわりの過程といってもいいでしょう。だ

とすれば、工業が進む道しるべを与える使命を負っている我々としては、きたるべき情報産業的仕事がどうあるべきかの研究をするべきではないだろうか。このような考えから、スローガンとして

　情報産業のための科学技術研究

というものを掲げてみました。つまり、工業や農業などの今までの産業の中に、全体をコントロールしている情報産業的要素を見出し、そこをすすめるための科学技術を研究する、ということです。

これは、少し前に研究所内で盛んに言われた「研究の出口論」と殆ど同じ事を、情報産業の考えを使って述べただけといえるかもしれません。ただ、情報産業としての面に着目することによって、事の本質が情報の操作、処理にあるのだ、ということが浮き彫りになると思います。例えば材料を研究するにしても、どのような材料がどのように使われるかを考えて、そこから新しい材料づくりに向かうべきである、というのが研究の出口論でしょう。ここで考えるべき内容がほかならぬマーケティングであり、生産管理である、そうしてそれらは情報の処理であるというわけです。

一方、情報産業のなかに研究所も当然ながらはいります。民族学博物館をたてられた梅棹氏は情報を蓄積する情報産業としての博物館を強調しておられますが、研究所も新しい学術情報、技術情報をつくったり、蓄積したり、既存の情報から二次情報を作り出したりするところだから、その業務は情報産業の一つの典型です。この研究所業務遂行で中心になるのが知的基盤ということになるでしょう。そうして、梅棹さんが既に情報考現学でとりあげている特許、著作権、印税、公開と私有などが、知的基盤を扱う我々研究所が直面している問題であることは皆さん御承知のとおりです。

また研究所業務が情報の生産や蓄積である、ということから、情報処理のテクニックを研究所業務に使える、というあたり前のこともでてきます。さらに、理論とシミュレーションによる情報科学の方法論が、伝統的な理論と実験による物理学の方法論に取って代わる事例がいくつか出てきています。実験科学の対象とするには、その現象が再現可能である、ということが前提になるわけですが、生命現象やビッグバ

情報産業としての科学技術研究

- 研究所業務は情報産業
  - 学術情報、技術情報の生産と蓄積
  - 知的基盤の整備
  - 特許、著作権、印税、公開と私有
- 実験からシミュレーションへ
  - 再現不能な現象への適用

ンなどの再現可能性が得られないような現象に関する理論の検証に、シミュレーションが使われ始めている、という点は、大いに注目に値するのではないでしょうか。

とまあ、話はどんどん大きくなるわけですが、「科学技術研究」という一つの業務を、情報産業としてみることによって、研究所が進むべき道が見えてくるのではないか、という意味をこめて、

　情報産業としての科学技術研究

というスローガンをたててみました。

以上、情報産業のための科学技術研究、情報産業としての科学技術研究といった二つの意味合いで、情報産業と科学技術研究を並べたことをお話いたしました。

参考文献

1) 梅棹忠夫:「情報産業論――きたるべき外胚葉産業時代の夜明け」,放送朝日,1963 年 1 月号,pp.4-17,1963.

2) 梅棹忠夫:知的生産の技術,岩波新書,1983(原著　岩波書店,1969).

3) 梅棹忠夫:「情報の考現学――現代世相の解読のために」,中央公論,1988 年 3 月号,1988.

4) 梅棹忠夫:情報の文明学,中公文庫,1999(原著　中央公論社,1988).

5) アルビン・トフラー;徳岡孝夫監訳:第三の波,中公文庫,1982.

6) ダニエル・ベル;内田忠夫ほか訳:脱工業社会の到来:社会予測の一つの試み(上)(下),ダイヤモンド社,1975.