暗号とユビキタス社会

4・12 シンポジウム「電子社会の展望」から

シンポジウム「電子社会の展望」が4月12日、理工学部後楽園キャンパスで開かれた。
21世紀COEプログラムに選ばれた中央大学の
「電子社会の信頼性向上と情報セキュリティ」研究拠点の主催イベントである。
学外を含め研究者ら約500人が参加した。
ここでは、COEリーダーの辻井重男・中央大学教授と、
トロンの研究開発者として知られる坂村健・東京大学教授の、
興味深い2つの講演内容を中心に、当日の模様をレポートしたい。

講演「歴史にみる暗号、現代の暗号」

辻井重男　中央大学理工学部教授

シンポジウムの何かキャッチフレーズを、と聞かれて考えたのは「自由・平等・安心」だったそうである。電子社会、そして自身の専門である「暗号」研究のめざす社会理念となるだろう。

「ヘーゲルは……」と、話が始まった。「歴史（世界史）とは、自由の意思の発展の過程である、と言っているわけですが、確かに、それが歴史の法則だなと、私は思っています。自由の定義は難しいのですが、たとえば利便性の拡大という観点でみても、リアルスペース（現実空間）×サイバースペースで人間の行動範囲が広がる。自由のインフラ、自由の基盤を拡大する、そういうかたちでネット社会が開け、その安心・安全を保証する中核技術として私どもの研究もあるわけであります」

情報セキュリティの理念とは何か。4つの要素から成る、という。暗号を含め自由の拡大につながる「技術」、プライバシーの保護にかかわる「管理運営」、安全性の向上のための「法制度」、そして人間学でもある「モラル」。この4つが緻密な一体性をもち、欠けがあってはならない。従って、と教授は語る。「情報セキュリティとは学際的総合科学である」と。

講演の内容も、学際的な広がりで、多岐にわたっていく。

《暗号の歴史》 暗号といえば、まずは「情報を隠すもの」というのが一般的な理解だろう。事実、軍事・外交場面では切り離せない。

暗号通信と、そのまた敵陣営の諜報・解読の熾烈な戦い。いくつもの舞台裏のドラマや秘話は自著『暗号と情報社会』に詳しいが、史上、もっとも劇的なのは、ナチス・ドイツの「エニグマ暗号」だ。「イギリスがエニグマの解読に成功していなかったら、歴史はどうなっていたか。戦後史はまるで変わっていただろう、と言われるものですね」と、注釈が

入る（エニグマを解読したのはイギリスの数学者で、それを描いた同名の映画「エニグマ」も公開され話題になった）。

教授は戦史・歴史話もことのほかお好きなようである

暗号の歴史をめぐる。はじまりは、「シーザー暗号」だそうだ。ごぞんじ古代ローマの闘将、ヨコ書きをタテにしなければ意味が伝わらない「天地式」とよばれるもの。シーザーは奥方やかのクレオパトラへの付け文にも、これを使っていたらしい。

あるいは、上杉謙信の知将、宇佐見定行の「単文字換字暗号」、ほぼ同時期（１５００年）西洋では「多表式暗号」……と続く暗号発展略史。

ここまでは「暗号＝情報を隠すもの」という、第二次大戦までの旧来の暗号。暗号の理解としては、「半分だけ正しい。それが暗号のすべてではない」そうである。

《隠す暗号から見せる暗号へ》

軍事・外交場面で使われるのは味方同士が同じ暗号解読の乱数表などをもつことによって、情報をやりとりする方法である。

これを「共通鍵」という。

「情報をいかに隠すか」がすべて、だからむろん「秘密」を旨とする。

その暗号の歴史に、画期的な方式が登場する。

「公開鍵」

とよばれる。

１９７０年代に英・米で開発された。ネット時代の「電子暗号」である。

「隠す」から「見せる」へ。暗号の考え方においても「奇想天外な発想の転換」だったわけだ。アルゴリズムという演算法・解法はオープンにネット上に公開される。一方で個人はそれぞれに「秘密鍵」をもち、この二重の構造、二つの組み合わせで、ネット上の「認証」が行われる。

ネット世界の電子商取引、さらには電子マネーとなると、「何が本物であるか」という、人間や文書の「真正性」の保証が最重要になる。サイバースペース特有の、なりすましや偽造、改ざん。教授の表現では「端末機で指先が震えていても相手には分からない」し、しかも一瞬に思わぬ場所まで「悪事千里を走る」。それをどうチェックするか。それが同時に新しい社会をつくり出す。「守り」と「攻め」が一体化した技術が現在の暗号理論研究であり、中大・辻井チームはこの先端分野で唯一のＣＯＥ研究拠点である。

現在の主流は「ＲＳＡ暗号」とよばれるものだが、目下辻井チームが取りくんでいるのはさらに進化した「楕円暗号」「超楕円暗号」……などと聞いても、専門家以外には手が出ない。中身は数学・整数論の世界だ。ピタゴラスやガウス、フェルマーの定理などを例に、整数論が、素数が、といった説明が続いたけれど、この部分はあっさり素通りしよう。

ともあれ教授によれば、暗号理論の体系は、「深い数学的構造をもった美しい体系」だそうである。「だからこそ、暗号研究に惹かれた」とも。

「暗号」が、真偽を峻別する「真正性」と、同時にそれが安全なものだという「安全性」を担保しているか。「われわれ（の研究）は、それを数学的にキチンと厳密に証明しましょう、としている」と、教授は話した。

昨年４月、電子署名法が施行され、議論もあった住基ネットも８月スタートする。

公開鍵とは別に個人が所有する「秘密鍵」は実印に相当するが、これまでは５１２ビット、１６０ケタの数字だった。見破ろうとしても「コンピュータを８００台つないでも何カ月もかかる」そうだから安全面でまず問題なさそうだが、電子政府の内実を備えるには不十分で、わが国ではその倍、１０２４ビットに高める方針だという。「今後10年は、これで完璧でしょう」

《孫子の兵法に曰く……》

孫子が引用される。

「明君賢将……必ズ人ニ取リテ敵

「暗号」からIT日本社会論を語る
辻井重男教授

ノ情ヲ知ル者ナリ」

情報が重要、「人ニ取リテ、というところも大事ですね」と、第二次大戦下、独ソ不可侵条約を破ってナチスがソ連に侵攻（１９４１年）した場面の秘話を披露する。

ヒトラーらの信任の厚かった時の大島浩駐独大使の暗号電文はソ連侵攻を2週間前に打電するなど重要なものも多かったが（連合軍はそのほとんどを解読していたとされる）、侵攻から半年後モクスワ撤退の段階でも「ドイツ優勢」を伝えた。それが日米開戦の戦況判断に重大な影響を与えた、ともされる秘話だ。

「情報は、多元的に集め、願望に基づかず、既定路線にとらわれず、冷厳・客観的に分析されなければならない」

学ぶべきは歴史の教訓だ、と教授は強調した。

「情報国家」へ向けて、歴史の教訓は生かされているのか、情報についての認識に甘さはないか、という話に移っていく。

講演のレジュメには、西田幾多郎（１８７０―１９４５年）についての本（『物語「京都学派」』）の紹介もあった。京都学派を率い、西洋との理念的な対決とその超克を説いた「近代の超克」論で知られる。その意義を一面で評価しつつ、では本当に「近代の超克」を日本は果たせたのか、逆に西洋との真の対決を避け、真剣に考えてこなかったのではないか――教授はそう問うのである。

《ＩＴ日本は大丈夫？》

「内部規範社会」と「集団志向性」。日本の特徴をそう指摘する。

農業社会から大量生産の工業社会への離陸――戦後のめざましい高度成長は日本的特性がみごとに奏功した結果である。

同時に、農業社会から工業社会への移行は、歴史必然的な連続性といえるだろう（教授の表現では「解析接続的連続性があった」）。が、ＩＴ社会は、これまでとは「非連続的」に、一気に次のステージにジャンプするような、実線ではなく点線でしか表せない未知の社会にちがいない。

「個の時代」といわれる。「新しい理性」も要求される。そういうなかで、ＩＴ社会を日本的特性だけでやっていけるのか、という問いかけだ。

「福沢諭吉は……」という話になった。明治初年、「（電信や蒸気機関車などの）西洋の大発明は、人々の内部の精神を動かして……」と語ったそうだ。明治の晩年になると、漱石が「我々も内発的に変わっていかざるをえないが、急には変われない。神経衰弱にならない範囲でやろう」という趣旨の演説しているという。戦中の京都学派や小林秀雄らの雑誌『文学界』座談会では「アメリカの機械は日本の精神には勝てない」といった発言も飛び出した。

現在の思想・論壇では、環境破壊等にみる西洋近代批判から、日本からの「共生の思想」発信を、とする論も盛んである。

「それもいいのですが、それだけでいいんでしょうか」と疑問を投げかけ、教授は一昨年訪ねたドイツの「計算機博物館」の印象を語った。ソロバンもむろんあった。しかし歴史的に展示されたほとんどは西洋が生み出した機器の集積である。「それを眺めてこれが機械を作った精神なのか、と改めて圧倒されました」

欧米の底力、といえばいいのだろうか。ほとんど日本文化論、東西文明論に踏みこんだ発言である。

欧米に伍して、あるいは対しつつ、日本が「ＩＴ国家」「情報国家」として生きていくうえで重要なことは、と述べる。

「技術面と同時に、精神構造改革――日本人の意識改革がどうしても必要だと思います。それに人材が決定的に足りない。パネル討論のテーマでもありますが、人材育成が急務なのです」

メッセージをこめた問題提起で締めくくった。

（学生記者　吉野仁美＝総３）

講演「ユビキタス社会と私たちの生活」

坂村健　東京大学教授

《どこでもコンピュータ》

「ユビキタス（コンピューティング）」？　ｗｈａｔ？という向きが多いだろう。教授もその説明からはじめた。

「ユビキタスコンピューティング」とはあらゆるものにコンピュータを内蔵し、全てのコンピュータ同士をネットワークでつなぐ、という考え方。これからの電子社会のビジョンとして坂村教授が提唱しているものである。

さて、コンピュータと言われてあなたはどんなものを想像するだろうか？　ほとんどの人がパソコンや携帯電話などと答えるだろう。炊飯器や洗濯機、と答える人は少ない。しかし、坂村教授が定義するコンピュータとは世間一般の定義とは明らかに異なる。

「携帯電話やパソコンはもちろん、炊飯器、冷蔵庫、コピー機、ラジオにエアコンと、マイクロコンピュータを組み込まれている全てのものはコンピュータである」と定義する。ユビキタスコンピューティングという考え方では、家電製品のほかに衣服や文房具などありとあらゆるものにコンピュータを組みこみ相互に交信させることである。

「どこでもコンピュータ」の近未来を語る坂村健教授

84年、今から約20年前に、坂村氏は「実時間ＯＳ（オペレーティング・システム）」の製作を提唱し、ＴＲＯＮ（the real-time operating system nucleus）プロジェクトを発足させた。

そのときから「未来はあらゆるモノの中にコンピュータが入りそれらがネットワークで結ばれる」というビジョンを語ってきた。それがユビキタスコンピューティングのコンセプトにつながっている。もっとも聞き慣れないラテン語の「ユビキタス」では理解しづらいだろうからと、教授は端的にこう表現してみせる。

「どこでもコンピュータ」

なるほどこのほうが一般には分かりやすい。

ではこの考えを導入することで、われわれの生活にどのような恩恵があるのだろうか？

ビンを取り出して、「ここに２つの薬があるとしましょう」と、説明も具体的だ。

個々の薬を単独で服用することに問題はないが、一緒に飲用すると深刻な副作用を引き起こす場合、もし、薬のビン自体にマイクロコンピュータを内蔵させることができれば、「どういう薬と飲むと副作用を起こすのか」とか、「何が危険なのか」といったことが入力できる。それに加え、もし、薬のビン同士が会話をすることができれば、「一緒に服用すると危ないよ」と薬のビン同士が副作用の危険性を認識することもできる。その結果として、服用しようとする人間がいた場合、携帯電話に薬のビンから電話がかかってきて、「死んでしまいますよ」と警告することもできるだろう。

薬のビンにコンピュータを内蔵するだけで日常の安全性を高めるメリットにつながり、医療ミスの減少にも多大な貢献をすることができるというわけだ。

持参のビンにもコンピュータが内蔵されていて、読み取りのセンサーを近づけると「コノクスリハ……」とビンが語るサマに会場は軽いざわめき。「ほう」「へェ」という声がもれた。

現在では米粒より小さなマイクロコンピュータがすでに開発されているそうだ。電力は外部から供給し、記憶素子としての機能を持たせたこのコンピュータをビンに組みこむことは技術的には容易だという。しかし、問題点もある。情報の安全性と電力の供給方法である。

「情報の安全性についてはセキュリティをしっかり構築してから、モノと人間、モノとモノとの通信ができうるように研究を進めている」と教授は現状を語る。電力を送るための電波の人体に及ぼす影響についてはどうだろうか？　「強力な電波を出せばいいという問題じゃない。危険性がないように解決していくという研究が重要なんですね。微小な電波を長く飛ばすという研究も必要だ。

アメリカでは軍事利用を目的で開発が進められているが、日本では民間利用でやっていかなければならない」と話した。

坂村教授は著書『ユビキタス・コンピュータ革命』の中でもしきりに民間利用を唱えている。なぜ民間利用にこだわるのだろうか？「民間で行わなければユビキタス社会は夢物語で終わってしまう。あらゆるものが通信するためには同じ通信方式でないといけない」と語る。通信方式の統一――異なる通信方式では、お互いが異なる言語で話をしているのと同じこと。「セキュリティを高めるにはソフトの中身をオープンにしたほうがいい。なぜなら、世界中のソフト開発者の目にさらされ、開発者とは違った切り口からそのソフトを診断できる。迅速で効率的に誤りをチェックできる」

開かれたネットワーク――これこそ坂村教授の持論であろう。

もし、これがマイクロソフトのWINDOWSのように大変普及しているソフトにもかかわらず、中身を公開していなければ間違いに対応できない。「ある会社が独占したり、一つの国家が秘密にやっても意味がないんです。みんなで使うのだから、みんなでやらなければならない。これは今後の日本、世界の課題である」と強調した。

TRONは、オープン・フリーのOS――坂村思想の結晶である。

《小柴先生がウラヤマシイ》

ノーベル物理学賞を受賞した小柴昌俊・東大名誉教授の話も飛び出した。

アメリカのチームに実験を一緒にしようと声をかけられたときに、小柴さんは、「戦って勝たねばならん！」と胸にたぎるものを感じた、というエピソードがある。それを聞いて、「そりゃぁ、うらやましいと思いました」と語る。「コンピュータをやっている人間はアメリカと戦おう、なんて言えません。言っただけで、たたかれてしまいます。これには腹が立ちますよ。研究や独創性というものは戦いの末に得られるものです。アメリカがもう研究をやっているから戦わないでアメリカのものを使っていたら、独創性なんてありえない」

情報技術分野の日米戦争、対日圧力。私は民族派ですから、と笑って添えた。

「小柴先生はアメリカと戦って勝利して、ノーベル賞を受賞されました。私は戦えないうえにノーベル賞なんてもらえないですよ。存在しないのですから。日本は画一的で、ノーベル賞が一番だと思っている方がたくさんいらっしゃる。がんばってノーベル賞とってくださいね、なんてよく言われるんです。でも、ノーベル賞にコンピュータの分野なんてないんです」とユーモアまじりのぼやき節。

（僕もノーベル賞が一番だと思っていました。でもなるほどノーベルはコンピュータ社会など予測しようもなかった、わけですね）

「物理をやっている人たちは実験のためにはカミオカンデのような数百億もするような実験装置にもポンとお金が出てくる。コンピュータをやっている人間にはその１０分の１も降りてきませんよ」と、独特の語り口にまた会場がわいた。

《今後の研究と日本の未来》

TRONの民間利用を唱え続け、結果として、世界中で利用されているOSとなった今、坂村教授が見る今後の日本とは？

「日本は家電を作ったり、既存のものを小さくしたり既存の物質にコンピュータを組みこんだりする技術に長けている。アメリカには家電製品を作っているところは少ない。だから日本にもこの分野の未来は十分ある。ハードや大きいシステムを作るのは得意じゃないが、小さいものや既存の物をより良くするための改良に関しては得意分野ですよ」

「基本OSなどのソフトにいちいち料金を課していたら、成長するための土台ができない。そこはオープンにソフトを配布してよりよい未来のために貢献するべきなんです。携帯電話、デジタルカメラ、組みこみ型コンピュータなどは日本が最も進んでいる立場にある。今後も、日本がより発展するように我々は研究を続けていきます」

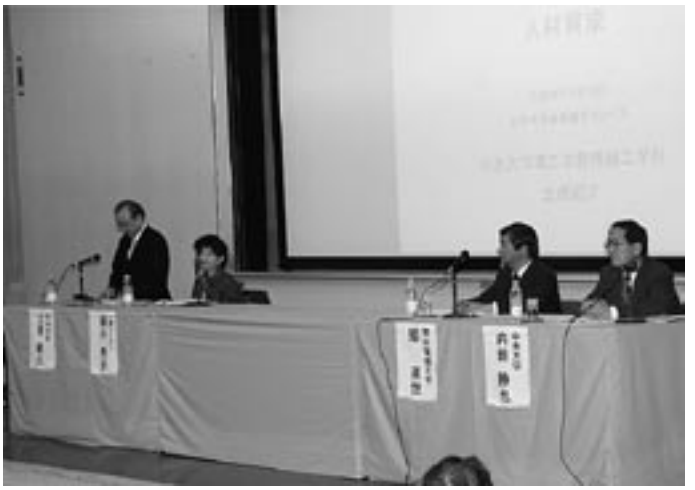
日本の技術的な力量、その自信をのぞかせる講演となった。

（学生記者　古賀清人＝理２）

講演とパネル討論

充実したCOEシンポジウム

シンポジウムは午前と午後の二部構成で開かれた。本学今井桂子教授の司会で始まった午前の部では、風間重雄理工学部長のあいさつのあと前科学技術政策担当大臣の尾身幸次衆院議員が特別講演。尾身氏は、現在の日本の情報技術政策をハード、ソフト、ネットワークという切り口で整理した後、電子社会の実現に向けて、特に情報セキュリティ分野については「国として個人としてやらなきゃいけないことが、この分野に関しては無限にある」と指摘した。



午後のパネル討論も活発に。会場には研究者らの姿が目立った＝理工学部５号館で

前ページで詳述の、本学ＣＯＥプログラム拠点リーダーの辻井重男教授の「歴史にみる暗号、現代の暗号」、坂村健東京大学教授の「ユビキタス社会と私たちの生活」は、このあと行われた午前中の講演である。

午後の部は角田邦重本学学長の挨拶で始まり、「人材育成」をメーンテーマに、講演やパネル討論に移った。

「電子政府・自治体からみた人材育成への期待」と題した講演のなかで、大野慎一・総務省大臣官房政策統括官は、電子政府・自治体のシステム作りには、制度、技術、運用の三点がどれも不可欠とし、なによりも「国民の皆様に安心して使っていただけることが一番大切」と強調した。また池上徹彦会津大学学長は、「日本の科学技術政策」について講演。ソフトウェア分野特有の「目に見えないもの、重さの無いもの」ゆえの政策決定の困難さにふれながら、科学技術政策への提言を行った。

パネル討論は、本学の土居範久教授がコーディネータをつとめ、「ソフトウェアの人材が極めて薄い」という現状認識にたって問題を提起、それを受けて、パネリストの熱心な討議が続いた。國井秀子・リコーソフトウェア研究開発本部長は、「アジア各国が国家の重点施策としてソフトウェアの人材育成に取り組んで成果を上げている」ことを実例をあげて解説し、特にこうした国々とわが国とのギャップが大きいことも問題だと指摘。脇英世東京電機大学教授は育成すべき人材には平均的技術者と「平均値から大きく離れた人間」が要る現状の問題点に言及した。本学の内田勝也助教授は、本年度からスタートした本学大学院理工学研究科の情報セキュリティ副専攻を紹介しながら、技術者や管理者向けの情報セキュリティ教育だけでなく「利用者が加害者にならないための教育」の必要性も強調した。

締めくくりに鶴保征城・ＮＴＴソフトウェア代表取締役社長による総括。情報が溢れる時代の要請として大学に「情報濾過能力を持った人材の輩出を期待する」と語るとともに、ハイテクなものだけでなく、「ハイセンスなものでいこう」と発想の柔軟さをも要請した。

会場には研究者や産業界、自治体関係者の姿も多く、午前と午後の部合わせて参加者は５４０人にのぼった。参加者からは、電子社会実現へ向けた本学の取り組みへの評価の声が聞こえるなど、内容面でも充実したシンポジウムとなった。

（21世紀ＣＯＥプログラム　ポスト・ドクター　加藤研太郎）