ゼミの風景

理工学部

辻井重男教授

Shigeo Tsujii

卒論演習

「暗号理論」の先端――ともに「研究」へ向かう視線

辻井重男教授――IT情報分野で「暗号理論」の斯界の第一人者である。世界のトップレベルの研究教育拠点を形成するための平成14年度21世紀COEプログラム、いわゆる「トップ30」に選ばれた、本学の「電子社会の信頼性向上と情報セキュリティ」研究グループを率いる。

と紹介しただけで、文学部・国文学専攻の私としてはもうダッシュで逃げだしたいような気持ちである。私のアタマではたして理解できるのかしら。おずおずと教室の扉を開けると……黒一色?! 部屋の中はみな、男性であった。ITやら暗号理論はオトコ向きなのかというと、もちろんそういうことはなくて、ゼミ生12人のなかに女性も1人。その日はたまたま欠席につき、文字通り紅一点の状況でゼミは始まったのだった。

やさしい?「電子投票」の話

ボードに、「電子投票」「共通鍵」「公開鍵」「楕円暗号」という4つのテーマと、それぞれにゼミ生3人の名前が書かれている。この日は、昨年末の最終講座――卒論の中間発表という大事な時間なのであった。それを中断して、「取材ということだから、前半はすこし分かりやすい話を」と、これは先生の優しい気遣いである。「ウサギの耳」でしっかり聞かねばと、ノートを広げる手がすこし震える……。

「電子投票の話がいいでしょうね。××君、資料を準備してくれるかな」と声をかけて、先生の講義が始まった。

選挙のたびに投票率の低下が話題になる。個人のパソコンや携帯電話から投票ができるようになって、直接投票所まで行かなくてもよくなったら便利で投票率も上がるだろう。しかし実用化するとなると問題も多々ある。最大は「個人のプライバシーを守りながらどう不正を防ぐか」という問題である。技術的にどう乗り越えるか。セキュリティに不可欠な、情報を暗号化する理論研究――その先端領域が先生の研究分野だ。

「TYKK方式による電子投票」。先生が他の研究者と共同で開発、目下研究段階中のものである（ちなみに「T」は辻井、以下共同研究者のイニシャル）。

「電子投票にも、3つの段階がありましてね」。図で示しながらの説明だ。第1、2段階は、「有権者が投票会場に出向いて端末機で投票する」形態、そして「自宅の端末機で投票、すべての回路が電子化される」第三段階へ。文字通りの「電子投票」になる。

第1段階は先の広島市長選など一部地域で試験的に実施されている。

「技術的な問題と同時にもちろん他面で、では投票率が高くなればそれでいいのか、ということも考えなければいけないわけですけどね」

そう、投票率の低さも有権者の政治意思の反映だとすれば……先端技術が人文系の学問分野とも離れてあり得ない、重要な指摘に思える。

講義のなかで、「デカルト」や「ヘーゲルの絶対精神」の言及もあった。「絶対精神の解釈や評価も変わってきている」というように。

情報分野の第一人者の講義の厚みである。

《つじい・しげお　1933年京都生まれ。東京工業大学卒。山梨大学助教授、東京工業大学教授などを経て94年から中大教授。情報セキュリティのスペシャリストとして、日本セキュリティ・マネジネント学会

会長など各種の団体・研究チームを率い、教学審議会委員なども。著書に『暗号と情報社会』など多数》

ゼミ生の卒論の中間発表に移った。まず、李潤喆（イ・ユンチュル）さん。

発表もさすが理工学部、ノートパソコンに入れたデータをオブジェクターでスクリーンに映し、ポインターで指しながら説明していくという形式である。全員の視線がスクリーンに集まる。

「ＴＹＫＫ方式による電子投票」の原理の説明から。「投票者がインターネットを使って投票する場合、有権者であるかの確認、また匿名性を守るための情報の暗号化を経て、最後に暗号を復号（元に戻す）してから開票結果として公表、という手順をふむやり方である」「このとき使う暗号をＲＳＡ暗号という」……簡単に説明すると、「素因数分解の定義を応用したもので」、不特定の人物が使用するための暗号・公開鍵暗号と呼ばれる中のひとつだそうだ。

「この暗号は本当に安全なのかを追求している段階である」

と、アタマに入ったのはこのへんまでだった。

卒論発表を聞きながら、専門的な応答がつづく（写真右が辻井教授）

数式の探検者たち

順に発表が続いたが、あとはお手上げ。難しい。だって、等号や不等号、数式がずらり並んで、「日本語」がないんですもの！　スクリーンに映した内容を印刷してもらってレジュメとしていただいたが、それ自体が「暗号」のごとく映るばかり。コンピュータの中は不可知のブラックボックス、彼らはその中に分け入る探検者たちである。

「この式、なんで成り立つか調べた？」

「ここ、逆数は計算できるだろ？」

「うーん、すごいよ。ＴＹＫＫ方式に君のイニシャル加えようか」

先生の指摘やゼミ生とのやりとりを聞きながら、思う。いわば同じ土俵にあるイクオール・パートナー、共に「研究者」同士である関係性のようなものを。文系の教室風景とは違う、それが新鮮な印象であった。もちろん担当者がウッとつまる場面も多かったけれども。

話が難しいので堅苦しそうな雰囲気に思えるが、そんなことはない。

「次の発表会は年明けになるなあ。1月初旬あたりで1時から5時くらいまで時間とってやろうか？　やってほしい人、手を挙げて！」（先生、手帳をひらきつつ提案）

「……」（ゼミ生沈黙）

「誰もいない！」（先生苦笑）

と、こんな具合で笑いが起きたり。

その日いただいた、先生がシンポジウムの際書いた原稿に〈現在この分野（情報セキュリティ）の人材育成が深刻な問題となっている〉との記述があった。その先生が「いや、ことしのゼミ生の卒業研究はレベルが高いよ」と語るのである。

テニスも先生を目標に

ゼミ生の権田正樹さんに聞いた。

「先生を目標にみんな頑張っているんですよ。先生は本当は僕たちを見てる暇なんてないくらい忙しい人なんです。日曜以外は全部研究、しかも朝は学生より早く学校に来られてますし。テニスが趣味で、学生より熱心で元気な方ですよ」

辻井ゼミの研究室にもおじゃました。このときは、部屋中にヒトとパソコンが蝟集する過密さだったが、それも4月、竣工成った新棟に引っ越した。教授研究室とゼミ生の研究室は少し離れた場所にあったが、これからは向かいの部屋の近さに。「共同研究者」の距離も縮まり、中大発のＣＯＥ研究も本格化するはずである。

「多摩キャンパスは女の子多いんだよね～、じゃあ今度は俺が取材に行こうかな～」

と言ってくださる方もいらっしゃったし、理工学部だからといって頭の固い人たちばかりということは決してないのである☆

これも発見！　と単純に嬉しい気持ちになった私でありました。ちょっとケーハクすぎるかもですが。

ＣＯＥの本論については、次ページの辻井教授の文章をお読みください。

（学生記者　酒井まりえ）