特別対談

今と昔の暗号の話、そして倫理学

鳥取環境大学学長　加藤尚武 *Hisatake Kato*
中央大学理工学部教授　辻井重男 *Sigeo Tujii*

戦争と外交の舞台は暗号の歴史でもある。長い「情報を隠す」暗号史から、「私」を認証する暗号の時代へ。電子社会の「ポストモダン暗号」とはそういうものらしい。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」研究拠点を率いる暗号理論の第一人者と、『戦争倫理学』などの著書で知られる哲学者が語りあう。情報社会を守り育てる暗号技術研究とモラル学。

構成＝編集室

――辻井先生の講演などを聞いていますと、「歴史は自由の意思の発展の過程である」というヘーゲルの言葉がよく出てきます。その「自由」の拡大発展として情報社会があるのだ、というふうに。すぐにヘーゲルの専門家である加藤先生を思い浮かべて、この対談をお願いすることになりました。

辻井　言わないでくださいよ。専門家だから、こちらは。

加藤　辻井先生の学識はもう森羅万象にわたっていますからね。

――辻井先生の暗号研究は「情報セキュリティ」の中核技術であり、加藤先生は哲学（倫理学）の立場から「情報社会の倫理学」を提唱されています。その点もクロスしてきますね。

加藤　そうですね。情報の倫理というか情報技術が社会を変えていく仕組みはどういうものなのか。

例えば革命で社会を変える、あるいは明治維新だとか戦争による社会の変化とは、全然違うかたちの変化をしている。長期的に見ると明治維新の影響と電話の影響とどちらが大きかったかわからない。それぐらい技術は大きな影響を持つわけです。すると技術が持っている社会を変える力を、我々はまだ十分わかっていないというか、全然わかっていないんじゃないか。

はっきり言うと、いままで政治による社会変化ばかり考えていたんじゃないかと思うんです。ヘーゲルは政治によって社会をどう変革するかということに目を向け始めた人で、その政治というのは経済が変えているんだというのがマルクスだったわけです。

辻井　何が技術革新の根源かを考えると、結局人間の好奇心、格好よく言えば真理の探究とか知的好奇心です。好奇心という点では、奥さんたちがワイドショーを見て芸能人がどうしたという好奇心もアインシュタインの好奇心も同じで、それは人

つじい・しげお

1933年生まれ。東京工業大学卒。山梨大学教授、東京工業大学教授をへて94年から現職。電子情報通信学会会長、総務省電波管理審議会会長などを歴任。電子情報通信学会功績賞、郵政大臣表彰など。著書に『暗号と情報社会』『暗号—ポストモダンの情報セキュリティ』など。

かとう・ひさたけ

1937年生まれ。東京大学卒。千葉大教授、京都大学教授をへて01年から現職。日本哲学会委員長。専攻・環境倫理学。94年和辻哲郎文化賞、00年紫綬褒章。著書に『ハイデガーの技術論』『倫理力を鍛える』『共生のリテラシー』『先端技術と人間』『ヘーゲル「法」哲学増補新版』など。

間が持っている一つの業みたいなものですね。もう一つは利便性へのあくなき欲求という、これも人間の業みたいなもので、この二つが原動力で止められないんです。止めたほうが人類の幸せにはいいのかもわからないけれど、止められないんじゃないかな。それが技術を動かして、技術がいろいろ世の中を変えていくのではないかと思うんです。

加藤　この電子化による社会的な変化は、今までの社会変化とも違う。違ったかたちの変化があり得る。それに対する対応という点からいうと、我々の理論はまだ随分手薄なのではないかというのが私が普段感じていることです。

暗号秘話あれこれ

——対論の入り口として、まず戦争や外交の舞台での暗号秘話をお聞きしたいのですが、辻井先生の著書『暗号と情報社会』にも多くの例が紹介されていますね。

辻井　世界的によく知られるのは、ドイツのエニグマ暗号ですね。第二次大戦の、アメリカがまだ参戦しない段階の、ドイツとイギリスの戦争です。エニグマが解かれなければドイツがイギリスに勝っていたかもしれないし、戦後の世界地図——冷戦構造はアメリカ対ナチスドイツという構図になっていたかもしれない、というぐらい大きい。エニグマが解かれたことで「ドイツの敗北を2年早めた」ともいわれています。

加藤　確か日本の暗号はエニグマのrevised version（改良版）というか、かなり似たものだと。

辻井　外務省と海軍は「紫暗号」で、エニグマの改良版というのか、エニグマより難しかったという説もありますけどね。九七式暗号というのが正式名称です。アメリカ読みで「パープル」といっているわけですが、昭和12年につくられて、1年9カ月後の14年に解読された。その後の日本の外務省の外交交渉は全部筒抜けになっている。ミッドウェー海戦（17年6月）の大敗、そして翌年ブーゲンビル島上空での山本五十六の撃墜死もその結果です。

しかし陸軍の暗号は解かれていたわけではないのです。負けたからみんな日本の暗号は解かれていたという話ばかりなんだけれど、向こうの暗号も解いている。いろいろな側面があって、どうも日本とアメリカの関係について言えば、結局暗号をやらなければよかったという感じが

します。平文で全部やったほうがよかった。というのは、正式文書が送られる、それからその暗号文が行くわけです。そこで食い違う。

加藤　外交の場合ですね。

辻井　そうですね。向こうが解くでしょう。そうすると暗号のほうを信用してしまう。二枚舌だと思ってしまうわけですから、使ったためにどうも損をしているなと。要するに外交交渉にはそういう駆け引きがつきものであるにもかかわらず食い違うと、不信感を増大してしまうわけです。

それからもう一つ非常に大きな問題がありましてね。最近出た小松啓一郎さんの『暗号名はマジック』という本に出ているんです。お読みになりましたか。あれはものすごく面白くて、「誤訳」が日米戦争を起こした原因だと書いてある。

単純な例で言うと「御前会議」。これを「meeting in the morning」と訳してしまう。「甚だ恐懼に堪えざるも」は、天皇陛下に申し上げるのは「大変恐れ多いことながら」という言葉ですが、それを「大変懸念すべきことである」と訳している。

一番大きいのは日独伊三国同盟ですね。ドイツとアメリカが戦争を始めたら日本はどうするか、日独伊三国同盟があるから日本は自主的に参戦するかどうかを決めるという電報を打ったんです、「自主的に」と。それを「automatically」と向こうは訳した。「自動的に」と訳してしまったんです。

加藤　これは大変なことになる。

辻井　これはかなり影響があったと。他にも「天聴に達せられあり」なんて、今の日本の若い人でもわからないような言葉が向こうにわかるわけはない。そのようにかなり誤訳もあるし、二重にいろいろ間違いを起こしていて不信感を増大した。これだったらむしろもう暗号文をやめて全部平文でやっておいたほうがよかったぐらいなんですよ。

加藤　暗号も完全に習熟していればいいんだろうけれども、暗号を習熟する人が大量にいるということはちょっと考えられませんからね。ですからトップシークレットが暗号になるわけで……。

暗号から情報のセキュリティという問題になると、相変わらず情報というのは漏れたら価値がなくなるというかたちが多いわけですよね。

辻井　私たちが研究している電子暗号も、第二次大戦までの暗号と共通する面はいろいろあります。最近も軍事・外交に使うこともあるし産業機密みたいな話もありますから。しかしＩＴ社会になって全く違う使われ方があるというところをわかってもらいたいと思うんですね。

「公開鍵」――電子時代のポストモダン暗号

――電子社会の暗号、「ポストモダン暗号」という言い方もされてますね。

加藤　「公開鍵方式」という、暗号の基礎的な方式そのものが革命的に変化したわけですね。暗号の用途もトップシークレットだけが暗号化されるのではなくて、あらゆる情報は常に傍受可能な状態になると、あらゆる情報が同時に暗号化されないとプライバシー、セキュリティが保たれないという状況にもなってきているんではないでしょうか。

辻井　要するに用途からいうと、機密守秘というか「秘密を守る」というのが数千年来暗号の役割で、これは今でもプライバシーを守ったりということで大事なわけですが、もう一つ自分を自分であると主張する「認証」という、人に限らず文書でもお金でもこれが本物ですよという真正性の保障、こっちのほうがむしろサイバー世界では大きな役割で、それが主に公開鍵暗号の担っている役割ですね。

加藤　例えば電子投票をする場合には二重投票を防ぐというのがまず

ありますね。それから投票の秘密というのを守らなければならない。例えば、なりすましというのはしょっちゅう情報の世界ではあるわけだけど、なりすましの防止策の決め手は何なんですか。

辻井　決め手は公開鍵暗号で、公開鍵暗号というのは内側に秘密鍵を持っていて外側に公開鍵があるという二重構造になっている。内側の秘密鍵は大事に自分だけの秘密にして外側の公開鍵はみんなに使ってもらうという構造になっていて、秘密鍵で署名を付けるということです。

例えば1万円札は上質な紙に透かしを入れて物質的な属性と金額情報をうまく融合させて、金額としてのお金の価値を持たせている。これをサイバー世界というネットワークとコンピューターの世界でやるには、物質的な属性は使えないので暗号という数理的な手段で証明を付ける。

加藤　それはいままでのセキュリティの考え方からすると、全く革命的なことですね。つまり素材に一切依存しないわけですね。いままでは、例えば紙に署名をするとか金のハンコを押すとか指紋を押すとか、全部モノの素材そのものがこの人のものだということに結び付いていた。それが最終的には数値というかたちになると、その数値は電子で表現しても電球で表現しても何で表現してもいいわけで、素材には一切依存しない。

辻井　そうですね。基本的に依存しない。ただ、どう守るかというときにICカードに入れて守る。そういう意味では物理的な耐タンパー性みたいなものは必要ですが、基本的な証明は数学的な証明を付けるわけです。

「私」を認証する「素数」の世界

加藤　すると私のID番号というのは公開鍵方式の中の、例えば素数の一つか何かが私を証明する……。

辻井　IDを秘密にするという考えもあるんですが、私はパブリサイズドIDといいましょうか、IDというのはみんなに使って見せるものだと基本的に思っているんです。

加藤　ハンコみたいなものですね。机にしまってあるけれども時々人が見ている。

辻井　それを三文判としましょうか。それで実印になるのが公開鍵暗号の秘密鍵なんです。

加藤　でも一人ひとり素数を使っていったら、素数不足になりますね。素数のケタ数が次の素数となるともののすごい飛びがあるわけですね。

辻井　大丈夫なんです。素数ってそんなにあるのかと心配されるんですが、例えば100以下の素数は25あるんです。10000以下の素数は2000ぐらいある。

今どれぐらいのところを使っているかというと、素数の大きさは十進数で150ケタです。宇宙全体の素粒子の数は50ケタなんです。その150ケタの中に素数がどれぐらいあるかというと147ケタぐらいある。もうちょっとかな。素数っていっぱいあるんですよ。

加藤　同じ素数が配分される危険というのはないんですか。

辻井　ないね。それは全くないわけじゃなくて、数学的にはないんです。

加藤　確率論的にはゼロではない。

辻井　いや、それはゼロと言うんです。地球があした滅ぶ確率よりも低いわけですから。ゼロと言わないと駄目なのですが、別の原因で、熱雑音による素数発生とか、電源が入っていなかったとか電圧が下がっていたとかで起きる問題はある。

加藤　もっとローテクレベルでの失敗？

辻井　そうなんです。ローテクレベルで同じような素数が続けて出るかどうか。しかしこれは公開ですからチェックできる。

加藤　ものすごくケタ数の高い素数になると、もう暗記はできないね。

辻井　公開鍵は300ケタですから。これは自分で暗記するんじゃな

くて、ICカードが覚えているわけです。

加藤　でも宇宙というか、数の世界に存在する素数の中でたった一つの素数が自分の素数だなんてなると、何か「愛する素数」なんて感情が出てくるんじゃないでしょうかね(笑)。その素数が無限に存在することの証明というのは高校時代にやりましたけれどね、帰納法で。

ギリシャ人の「厳密値」と「さしがね術」の「近似値」

辻井　そういう話を先生に聞きたかった。素数が無限にあるということをギリシャ人が証明しているわけです。

加藤　背理法の例としてね。

辻井　背理法なんですよ。例えば素数は2，3，5といきます。5までしか素数がないと仮定しましょうというわけです。そうすると2，3，5、素数を掛けます。2×3が6、5×6、30。それに1を足してごらんなさいというわけです。31。これはたまたま素数なんですが、別に31が素数かどうかは問題じゃない。2と3と5しかないと言ったではないか。ところが2，3，5を掛けて1が余るということは、2でも割り切れない、3でも5でも割り切れない。じゃあ31は素数になってしまう。それは最初の仮定と反するではないかという背理法なんです。

それで先生に伺いたいのは、どうも中国人、日本人というのはそこまで論理的に考えない民族じゃないかという気がしてしょうがない。

加藤　そう思います。私はこの間、日本の大工さんの『大工さしがね術』という本を読んだんです。読んでもよくはわからないけれども、ものすごく精密な、例えば屋根の削り方や角度を全部さしがね、金尺だけでもって計算する。そこで最も驚いたのは「近似値」と「厳密値」の区別がないということです。

だからギリシャ人だったら絶対に認めない体系なんです。ギリシャ人なら、さしがね術というのは近似値であって厳密値ではないと、近似値のデータの取り方と厳密値の取り方を全部別系統にすると思うんです。さしがね術は大体これでやればもう実用的には十分というのと、厳密にこれでもってやれるという区別が全くない。

辻井　ある意味でディスクリート(分離的、抽象的)な考え方というのか、ピタゴラスは2400百年ぐらい前、数は有理数（いわゆる大学生ができないという分数ですが）しかないと思っていた。ところがタテ・ヨコ1メートルの対角線はルート2と無理数を発見してしまって、これは神様の失敗作だ、神様は間違ってこういう数をつくったんだから、口外しちゃダメだと弟子に言ったわけです。だけど弟子は漏らしてしまって、その弟子はそのたたりで……。

加藤　死刑にされたっていうか、破門にされたというかね。

辻井　船に乗って沈んだとか。だから今の数学ではやはり有理数のほうが実数より偉いんです。有理数を完全にしていくと実数になったり、p進数体というんですがいろいろな数が出てくるんです。有理数のほうが何か上だというのを直感的に考えていた。

とにかく先生もおっしゃられたように厳密値、つまり3というのと3・14は明らかに違うんだという考え方は、やはりギリシャ人の思考かなと思います。

ピタゴラス、プラトン、アリストテレス……

加藤　それはすごいものだと思うんです。ピタゴラスの体系ができ上がったときにユークリッド幾何学ができ上がっていくわけです。プラトン、アリストテレスとユークリッド幾何学の成立はいわば並行しているんです。

辻井　そうなんですか。プラトンとアリストテレスはだいぶ年が違いますよね。30ぐらいですかね。おじいさんと青年ぐらいですよね。

加藤　プラトンのお弟子さんの若手のトップがアリストテレスですね。しかし、発想法は違う。アリストテレスの場合には数学的な厳密値以外のものに対する関心が強かった。生物を集めて全部胎児の解剖をして、それで胎児の形態と親の形態が似ているということを発見して、親子関係というのは形態を決定する一番大きな要因だというようなことを言うわけです。

そこから物の中にはすべて将来を決定する要因が内在しているという、今で言えばＤＮＡだけれどもそれ式の考え方をしているんですが、もしユークリッド幾何学が完成していてこれこそが学問の典型だということになった場合に、解剖学までやる気、迫力は出なかったかもしれない。だからユークリッド幾何学の完成度が弱かったからアリストテレスが出たという可能性があると思います。

辻井　そういうものですか。

加藤　プラトンのほうは無理数のないユークリッド幾何学的なものに、ピタゴラス派の数学にのめりこんでいた。そして結局ヨーロッパの学問はあらゆる原型がユークリッド幾何学になるんです。ですからニュートンが『プリンピキア』を書いたときも、完全にユークリッド幾何学と同じかたちで書くわけです。それで数千年間、ヨーロッパの合理性というのはユークリッド幾何学を原型とするという考え方になった。

辻井　プラトンのほうが思弁性が高いという感じになるんでしょうか。

加藤　ええ、そうですね。

西欧の「思弁性」中国の「即物性」

辻井　狩野直喜という京都大学の昔の哲学者がいますね。あの人は中国文学、中国哲学の人で、「中国は即物性で、西欧は思弁性」といったことを西田幾多郎に言ったらしい。中国人は漢方にしても天文学にしても経験を集大成していきますが、あまり公理論的に理論体系を築くというのではないですね。

加藤　墨子という「兼愛説」（人類愛）を唱えた思想家がいますね。孔子とは違うタイプの思想家です。孔子の集団はお祭りの専門家、お葬式などを取り仕切ったりする宗教儀式の集団で、何十人も隊を成して鐘と太鼓をたたいて移動していろいろ引き受けていた。一方、墨子の集団は土木事業の集団だったんです。中国の土木工学というと将来万里の長城を建てたりするわけで、ヨーロッパの土木工学の技術と比べてかなり進んだものをたくさん持っていた。

ところが墨子の思想の中に工学思想は入っていないんですよね。

辻井　工学？

加藤　工学。テクノロジーの思想はないわけです。「人を大事にしましょう」だとか「人間のお葬式ばかりに金を掛けるんじゃありませんよ」とか、人間についての墨子の言

葉は残っているけれども、一体工学とは何であり、物をつくるとはどういうことであり、正方形とは何であるかという思想は残っていない。

辻井　あのころいろいろな思想家がいて「法家」と言うんですか、あの人たちはさっきの背理法みたいなものを考えたのかどうかぼくは知らないんですが、プラトンやピタゴラス……ギリシャというのはとにかく面白いなという感じがします。

加藤　ギリシャ人の持っていた純粋値に対するあこがれは、ちょっと突出していますね。

辻井　私はこれを卒業研究で、これから実際に納得するまでちょっとやってみようと思うんですが、本当の円・マルは誰も書けませんよね。幅はゼロでなければいけないし、ちょっとでも歪んでいたら円と言わないわけです。だから普通は何か変なものになる。楕円はちょっと長径と短径が異なる。ちょっとと言ったって、さっき言った宇宙の全体のうちの素粒子1個、10の50乗分の1、それぐらいの誤差。こんなものは誰も見分けられないんですが、円からつくった暗号は弱くて、楕円からつくった暗号が強い。

加藤　ケプラーの楕円軌道も、描けと言われたら見分けはつかないですよね。

辻井　本当に宇宙全体と素粒子1個ぐらいの誤差で楕円にします。そうすると強い暗号がつくれるはずなんです。それはp進数体という数の世界を考えるとそういうことになってしまう。だけど何かわれわれの実感からは納得できないので、これは今年の卒業研究のテーマでやってみようと思う、本当につくれるのかというのはね。

暗号の数学的構造

加藤　だからやはり実感型世界とは全然別世界のロジックがあるという考え方がないと、完全な円という考え方は出てこないと思うんです。つまり経験的に見ればこれはもう完全な円というコンセプトがないとできない。材木の切り口を直径何寸なんていうのは、完全な円から現実的なものを考えるわけでしょう。そのときに完全な円はどこから考えたかというと材木から考えたわけじゃないわけです。

辻井　数学はそういう意味では完全な円を抽象的に式の上で考えるんですよね、円は描けないけれども。だけど生活実感とそれほど離れたことが、また現実に力を及ぼすということがあるのかというのがちょっと興味があって、実際に確かめてみないとまだ納得できないなという感じもするんです。

　というのは、要するにデジタル技術はアナログのあくまで近似なんです。これに対して、大小性とか連続性とかいう概念は捨て去って、単に足し算、引き算、掛け算、割り算ができる数の世界を考えましょうと。そういうものを暗号で使うんです。だから実数的な半端な数は一切使わない。そういう数の世界で、観念の世界のものが現実にプライバシーを守ったり電子マネーをつくったりできるとすれば、面白い話だなと思うんです。

加藤　複素数だって工学的に使われるわけですからね。

辻井　人類の歴史というのは数の世界の拡大の歴史でもあるんです。公開鍵暗号の数学的な構造に非常に魅力があって、それで私は79年から暗号の研究を始めたんですよ。その頃セキュリティが大事だという意識も少しはあったけれど、今みたいにセキュリティ、セキュリティと言いませんし、むしろ公開鍵暗号というのが出てきて、それで非常に面白いなと思ったんです。

加藤　むしろ実用を離れて暗号の公開鍵暗号方式というそれ自体に関心があったと。

辻井　米・スタンフォード大学で76年に「公開鍵」という概念が出て、

78年には代表作の「ＲＳＡ暗号」が出ました。デジタル・シグネチャーということで、これから紙に代わってネットワークの世界で、ハンコや手書き署名に代わるものはどうしたらいいかという問題になっていますから、実用的なことも考えましたが、公開鍵暗号というのが今までの暗号と違って数学的にきれいにできているので、それでやり出したんです。

公開鍵暗号という概念を最初に考えた人はすごいんですが、実はイギリスがその４―５年前に全部やっているんです。これは諜報機関なんです。それで30年隠していた。イギリス人というのはしたたかだなと思います。アメリカの場合はもうちょっと現代意識なんでしょうが。ミッドウェーの海戦などで鍵の配送が間に合わなかったために帝国海軍は大打撃を受けた。公開鍵は、要するに鍵の配送をなくそうということなんです。

公開鍵というのは鍵の半分を見せまして相手に使わせるわけですから、敵に盗まれたって構わない。片割れの秘密鍵さえ大事にしていればいいわけです。だから鍵の配送がものすごく楽になるわけです。そういう意味で考えたらしい。

加藤　それは軍艦に暗号帖というのがあって、軍艦が沈むときには艦長は責任を持って焼却するとか爆破するとか、そういう責任があったんでしょう。

辻井　何か本のカバーが鉄でできているから、それで沈むようにしてあるとかいろいろ説はありますけれどね。

――北朝鮮の工作船からも乱数表のようなものが見つかった、という報道がありましたね。

加藤　そうでしたね。

辻井　公開鍵は使っていないんじゃないですか。

加藤　古いタイプ、乱数表を使っているのかもしれませんね。

辻井　今でも外交上はほとんど公開鍵じゃなくて共通鍵方式なんでしょうけれどね。鍵をしっかり持っていきますし……。クーリエ（外交伝書使）じゃないけれども、外務省でも手錠を夜寝るときも外さないで行っていたらしいですよ。

コンピュータでも解読不能

――電子時代の公開鍵や秘密鍵が数学的構造をもつとすれば、数学者によってまた解読される、という可能もあるわけですか。

辻井　共通鍵はあまり数学的じゃない。共通鍵と公開鍵はそういう意味でもタイプが違うんですが、公開鍵の場合は仮定はあるんです。

素因数分解という問題は難しいと仮定しましょう、ということなんです。21を3と7に分けるのは難しいとしましょう。この21という長さがさっき言ったように３００ケタぐらいになるわけです。そうするとコンピューターを何年回しても解けません。ただこれは解けないという数学的証明はできないんです。

加藤　数学的にはできないんですか。

辻井　数学的証明はできなくて、経験的に数学者、暗号学者がもう何十年かかってやっても解けない。つまり現実時間と我々は言うんですが。原理的には解けるんです。原理的には解けるけれども効率よくは解けないということをみんな信じているわけです。

加藤　ぼくたちが、例えば１００ケタぐらいの数を与えられてこれが素数か素数でないか言いなさいと言われた場合には、2で割れるか3で割れるか5で割れるか7で割れるかと、割れるか割れないかというのをずっとやっていく。それで自分で次の素数をつくってはまたそれで割れるかというようにずっとやっていくわけでしょう。その計算をするのにどれぐらい時間がかかるかというのをコンピューターにやらせた場合の時間を計算する。それは厳密とは言えないかたちの計算なんですか。

かもしれません。だから「絶対ですか」と櫻井よしこさんに言われると困ってしまうんだけれども（笑）。我々は絶対と言うんです。

――つまり、「絶対に破られない暗号」は作成可能である……。

辻井　だからこういうことなんです。素因数分解、その素数の積に分けるのは難しいと仮定しましょう。そこから後はきちんと厳密に証明していくんです。それでいかなる強い攻撃に遭っても平文のいかなる部分情報も、つまり１０００ビットの平文だと１ビットも漏らさないということを厳密に証明しないと、電子政府には使わない。非常に厳密にやっているんですね。わりと簡単に、暗号は破られるなんて言われると、違うと言いたい。

加藤　古いタイプの暗号と新しいタイプの暗号を混同した議論がものすごく多いですね、どんな暗号も破られるだろうというのは。

辻井　それもありますし、暗号が破られるにもレベルがいろいろある。いま私が言っているのは理論的なレベルです。コンピューターに忍びこんで鍵を盗むというのも、破られるって言えば破られるわけです。一般の人から見れば原因はどうでも破られたんでしょうということになる。だから別の防御が必要なわけです。その理論構築の話と、破れるかという話はちょっと切り分けないといけない。管理運営の問題とかパソコンをどう管理するかともかかわってきますから。ＩＣカードに入っているのをＩＣカードをこじ開けてそれを盗み出すような技術だってないわけではない。それはしかし何億円かけてそういうのをやる必要が、それだけの価値があるかとか、そういうことにもなるわけです。少なくとも理論的にという意味では、厳密に証明を付けようというのがわれわれ学会での研究の仕方なんです。

電子投票――「国民投票」の功罪

――電子商取引は一般化して、電子投票も全国で2か所ぐらいで実施されましたね。

加藤　あれは電子投票というか電子集計で、投票そのものは現場に出向いて手でやっているんでしょう。

辻井　電子投票には3つの段階がありまして、今やっているのはまだ第1段階です。岡山県新見市などでやったのは、投票所に出向いて紙の代わりにタッチパネルを使ったもの。第2の段階は中で投票所同士がネットワーク化される。第3段階というのは家庭や、あるいは携帯端末からも可能になる。

電子投票なんて口が腐っても言うなと言われたりするんですよ。なぜかというと政治家が一番困るということなんです。日本の政治構造を変えてしまいますから。

加藤　国民投票はいままで行われ

辻井　ギリシャ時代から「エラトステネスの篩（ふるい）」とかありましてね。今はもうすこし効率のいい方法がいくつかあるんです。しかし、それでやっても今のコンピューターで何万年とかかかります。

加藤　たまたま解けてしまうという可能性はないんですか。当てずっぽうでやったら当たっちゃった。

辻井　たまたま当てずっぽうで当たる確率は宇宙の中でこの素粒子を見つけてこいというぐらいの確率だと。だからそれを我々は絶対と呼ぶ。数学者はそういうのを絶対と言わないんですけれどね。市民も言わない

ていなくて、国民投票についての法制的なバックアップもないわけです。ただ憲法改正などはあるかもしれませんが。それが、毎日やっても大丈夫になる。外務大臣はどうも田中さんは駄目だね、川口さんにするかね、いや、どっちにするかモメているようだね。じゃあ投票しましょうということになったり、毎日が投票日ということになるとこれは……。技術というのはそうだと思うんです。最初は例外的で特権階級だけが乗っていた自動車に、やがてすべての人が乗るようになるというようにして、最初は極めて少数の例外的なものであったのが今度は逆にやらないほうが例外になっていくという転換だと思うんです。国民投票はもう伝家の宝刀みたいなもので、百年に1度やるかやらないかだと思っていたのが毎日でもできるというのは画期的な変化です。

辻井　何でも投票で決めてしまうと、政策の整合性も長期的な展望もなくなってしまうからそれはまずいんでしょうけれども、今の選挙を本当に任意の端末からやると投票率はものすごく上がります。上がるのは浮動票です。すると例えば土建関係などに支えられている票というのは相対的に減って、がらりと政治の構造を変えてしまうからみんなやりたがらないわけです。

加藤　今の政治は投票率が下がってきている。下がってきているから逆に安定していて、投票率が高くなると政治が不安定になるというのは、実際にもう既に起こっているわけです。投票率が上がると大体予測を外れるような当選者が出てくる。

　今はパソコンのネットワークに加入している人が44％ぐらいでしょうか、これが88％ぐらいになってこの電子投票を実際に第3段階でやっても構わないということになると、ものすごく不安定になるという話があります。ちょっとしたうわさだけで総理大臣の首が飛んだりすることになります。そうするとデマをつくる技術なんていうのは絶大なる効用があることになる。

辻井　だから投票ではなくてアンケートかなと思っているんです。いわば世論調査的なものをプライバシーを守りながら聞く。ビジネスでもプライバシーを守るから本当のことを言えというと、相当上がるらしいんです。それを今ちょっと考えているんです、私の方式では。

少数者の権利はどうなる？

加藤　ただ、そういう電子投票時代になったときに、本当に投票にかけることがいいかどうかという問題もあるんです。例えば10万人に1人しか病人がいないような病気というのはざらにあるわけです。ほとんど誰もがかかるような病気もある。研究開発費の予算配分を投票で決めるとするんです。すると5万人に1人とか10万人に1人の人の研究費の配分というのは、ゼロに限りなく近づいていくと思う。実際問題としていま「オーファンドラッグ」とか「オーファンデバイス」といって患者の数の少ない医療機器については、前は薬品会社がサービスで提供していたんですが、それではあまりかわいそうだというので法律的にバックアップして税金から補助金を出しているんです。

　ところがそういう少数者であるものについての配慮が行き届かなくなる危険がある。今はすべての人が自分が将来どういう病気になるかわからない、それを「ベール・オブ・イグノラン

ス」と言います。ベール・オブ・イグノランスが機能するからいわば公正性というものが保たれて、自分のことはわからないからやむを得ず公正な判断になってしまうわけです。

ところが遺伝子解読時代となると自分がどういう病気になるかが分かる、ベール・オブ・イグノランスがなくなってくる時代なので、その時代に国民投票で予算配分をしたら少数者の不利益というのはとても大きくなります。

辻井　多数決でいくと、そういう問題がありますね。

加藤　ですからそもそも公共的な合意形成、意思決定の方式について、一体どういう意思決定の方式を取ることが最善かという問題があって、今のまま直接投票をすればいろいろなコンフリクトを生み出す原因になっていく。いわゆる「投票のパラドックス問題」です。直接民主主義というのが本当にうまく機能するかどうかですね。

辻井　それはやっぱりいろいろな整合性とか長期的な展望とか大局的な判断を誰に任せるか、を投票するというかな。

加藤　私の感じでは、そういう国民的な合意形成の方法論はほとんど理論的な解明が行き届いていなくて、このまま電子化していくというと、合意形成の原則的な方法論がほとんど研究されないままでなし崩し的に電子化されていくことの恐ろしさ、そのほうが怖いんじゃないかと思います。

辻井　合意形成の方法論と電子化の関係ですね。これはどういう分野の人が研究するんですか。

加藤　統計学で決定理論なんていうのがありますね、投票のパラドックスなどを研究する人たち。政治学でも投票のパラドックスなどの数学的な問題を授業で扱うようにだんだんなってきていますけれどね。今は全然バラバラです。

辻井　この問題は真剣に研究してもらわないといけない。

平均値主義が研究を阻む

辻井　例えば研究費の配分とか研究を決める話だったら我々も議論に参加できるんです。というのは今の日本の評価方法は駄目だと思う。平均値主義なんです。いつも言う例は、10人の評価者がいてAとBという研究テーマがある、あるいはAという研究者、Bという研究者のどっちに研究助成をするか10人でそれを決める。Aという人については10人が投票で全員70点を付けた。平均点は70点です。Bという人については2人は90点を付けたけれど残り8人は60点を付けた。こっちは平均66点。すると、じゃあ皆さんAのほうが70点だからこっちを取りましょう、となる。

研究というのはブレークスルーを出さないと意味がないんです。70点ではブレークスルーは絶対といっていいぐらい出ないわけです。ところが90点を2人付けたということは2割ぐらいの可能性でブレークスルーが出せる。駄目かもしれない確率も8割あるかもしれないけれど。そういう決定をしないと研究の場合は駄目だと。

加藤　そうです。オリンピックのフィギュアスケートのジャッジペーパー方式で、飛び跳ねた点数を付けた人は削るという方式でやると、凡庸な人のほうが点数が高くなるという可能性が高いんです。

辻井　ユダヤ人は全員が賛成した案は採らないという話ですね。平均値主義はまずいと。この間、私が司会をしていまして、最後に一人ずつこれはいいというのをみんな言ってくれといってそれで決めたんです。後でわかったのは、自分の組織の出身者で知っている人を推したりとか、日本人はやっぱり情緒的でね。

加藤　かなり親分子分的なのが強いですね。

辻井　だからなかなか客観的にやるのは難しいなと思いました。いず

れにしても合意形成の方法論と電子化の関係は確かにそうですね。技術が変わってどう変わるかというときに、いろいろな意味で前もって考えておかないといけない。

プライバシーとモラル

――住基ネットが8月本格稼働しました。個人情報保護法も成立しましたが、国民の関心と議論は自分のプライバシーがどう守られているかという点にあります。専門家としてどのようにお考えですか。

辻井　9・11米国多発テロ（01年）以降、アメリカなどでは個人の自由・プライバシーよりは国家社会の安全、危機管理のほうに重点が置かれてきたようにみえますが、それをめぐってイデオロギー論争や、あるいはバランス論などもある。その点では、われわれ情報セキュリティをやっている者はバランス論ではなくて、目標としては自由の拡大、利便性や効率性等の向上ということと、安全性の向上、プライバシーの保護、それから監視社会への恐れの極少化というものを同時に達成しなければいけない。そのために「技術管理」と「マネジメント」と「法制度」と「モラル」を強く連携させた、完結した社会システムをつくっていくというのが情報セキュリティシステムだと思っているんです。情報セキュリティ科学はそれが緊密に一体化した学際的総合科学なのだ、と私はよく言うんです。

　プライバシーか安全性かは、確かに矛盾するんですが、それをなるべく両立させたい。例えばさっき言った電子投票などで使っている技術は、プライバシーを守りながら、言い換えれば自分の秘密は見せないで自分は不正な処理はしていないということを証明できる、それは零知識相互証明、プロトコルと言うんですが、技術的にはそういう暗号の手法があります。

　先生のご専門の倫理――モラルが現実世界でどれぐらい力を持ち得るのかというのに私は興味があるんです。

加藤　現代社会は一人当たりの労働生産性はものすごく高くなっている。これだけ豊かな社会になると他人様の労働に依存して食ったりバクチだけで生活したりとかという、いわば実質的に社会的に貢献しないでも生きる可能性も増えてくるわけなんだけれども、それがそんなに悪く、ひどくなっていないというのは、ものすごく複雑ないろいろな仕組みをつくっていくからです。

　社会的なサンクション（制裁）というのも、イスラム社会では泥棒をした人の両手を切るという極端なサンクションをやるわけだけれども、泥棒に対するサンクションの程度は弱くなっている。19世紀あたりから見せしめ型の処罰というのは少なくなって、20世紀はだから犯罪が増えたという説もあります。

　でもサンクションによる予防効果のほうが高くて、おかげでみんなが不幸な目に遭っているというのは少なくなってきている。そういった意味では人間がいわゆる物理的な刑罰を受けなくても社会的な評判を落とすのを避けたいというような気持ちの働きが、事実上犯罪を防止するのに十分な力を持つようにはなってきている。

　ところがこれから例えば自分で稼がないで、コンピューターの中でお金の変動だけで金を稼ぐ人がたくさん増えてくる。またソビエトの軍事力がなくなったのでアメリカの軍事力を減らして軍事力を使わないようにしようというのではなくて、アメリカの軍事力があればどこの国でも必ずやっつけることができるから、世界支配をやってしまおうというように考えたりするとなると、世界全体が情報によって結ばれた社会は安全性とか、将来の予測について妥当で合理的な判断をする方向に向かっているのか、むしろ非合理な方向に

動こうとしているのか。それが、20世紀の冷戦以後の新しい問題じゃないかと思います。

辻井　見えない世界での倫理観というんですか、それがどの程度なのか。さっき体面と言われたけれども、日本でも「旅の恥はかき捨て」と昔から言ったわけで、「コンピューターの恥はかき捨て」みたいに、どれくらい抑止力があるのかが心配ですね。

でも日本人というのは不思議だなと思うのは、神様が見ているという意識はなくても、まあまあ道義観を持っていますね。そんなに悪いことを人が見ていなくてもしない民族でもある。

加藤　大体キリスト教国よりも儒教国のほうは犯罪率が少ないんじゃないでしょうか。

辻井　だからそういう何かＤＮＡのようなものがあるんだけれども、モラル、難しく言えば情報倫理はどれぐらい効果を発揮してくるのかというのが、ちょっと興味のあるところなんですけれどね。

加藤　あまり大胆なものじゃなくて、やっぱり微調整型になるんじゃないでしょうか。適当にサンクションを決める、それから適当に体面が悪くなってみんなの前でさらし者にされるのは嫌だというような、いろいろな要素を複合的に使った微調整型のモラルで、画期的にこれでいい方法があるというのは出ないんじゃないかと思います。

情報の秘匿権の範囲とは

辻井　プライバシーの感覚、プライバシーの定義もlet me aloneだと言っていたのから「自己情報コントロール権」だというように変わってきたんだけれども、自己情報コントロール権というそんな格好いいことができるのか。これだけもう情報をみんな取られて、どこに自分の情報があるかわからないじゃないかと。結局どこで漏れているかわからないということにだんだん人間は慣れてくるのか。

加藤　慣れてくるよりしようがないんじゃないでしょうかね。つまり自己情報の完全な管理というのは不可能ですよね。

私は東京にいるときと鳥取にいるときでは全然違うんです。鳥取にいるともう町中の人は全部私の顔を知っているわけです。ですから飲み屋で飲んでいてもそのうち隣のお客さんが「学長、これからどこに行くんですか」なんてすぐ聞きますからね。

辻井　京都でも京大の長尾総長が、やっぱりホテルなんかに行くとちゃんとホテルのボーイさんが京大総長の顔を知っていて声をかけるというんです。

加藤　辻井先生もインターネット検索すれば山ほど情報が集まってきます。それはどうしようもないというか、それを全部自分で管理するのは無理だと思います。すると結局情報の管理権が成立する範囲、情報の秘匿権が成立する範囲をちゃんと決めるというか、それが成り立つか成り立たないかという問題になると思うんです。

その意味では自分がこれは知られたくないんだという情報を、一人ひとりが守れる、出さずに済むということですよね。よく自分の情報は全部自分で管理すると言うけれど、自分の情報を自分で管理し切れないです。

辻井　し切れませんね。だから出さないようにする。プライバシーというのは国によって感覚が違うし、時代によっても変わっていく。だから自分で出したくないものはとにかく紙で、と。だけど紙も今スキャンされて載せられてしまったりするし、情報漏えいというのはものすごく大きな問題です。結局住民基本台帳の問題も個人情報保護法も、うちの堀部先生（政男・法学部教授）が言っていたけれど、結局突き詰めて議論すると行政不信になってしまうと言うんです。

加藤　昔は人様の戸籍謄本を取ることができて、それで「おまえ、離婚した経験あるね」なんてすぐばれてしまったりしたわけです。今はそういう個人の住民の戸籍などを他人が取得することについての制限が随分強くなってきましたが、昔はかなり大っぴらに漏れていた。あの大っぴらに漏れていた体制がそのまま電子化されると、すごく大っぴらになってしまう。

辻井　そうです。電子化されるとすごく大げさになる。だから紙の世界でいったんまず少し固くしたんです。

加藤　紙の世界でいま絞り込んできていて、それが電子化されるというときに、電子化するならもうちょっと絞ったほうがいいということになるのか、それとも大体ここまで絞ったんだからこのレベルで電子化すればいいのかという、そういうかたちの議論をしないといけないんじゃないかと思うんです。

辻井　今の紙のレベルと電子のレベルとを比較してみようと思っているんです。紙も結構危ない面もあるわけです。ただ電子の場合は一瞬にしてみんなにわかってしまうから、確かに被害は大きくなりやすい。そこで国際比較をもう少し厳密にやってみなければいけないなと思って、「セキュアーな電子政府を推進する会」というのをつくりつつあるんです。

加藤　それは主として個人情報についての政府の管理能力を検討するものですか。

辻井　個人情報だけじゃなくて全体です。最近どうしても住基ネットのほうに話がいきますが、住基ネットだけではなくて全体に安全性を高めていこうと。行政と少し距離を置き、それから産業界とも距離置く。距離を置きつつ、産業界や行政の人とも話をし、というような形で会をつくっているんです。加藤先生にもぜひお加わりいただければと思うんですけれどね。

加藤　重要な問題ですね。

技術研究と倫理学の確立

加藤　技術は自然の中にあるものの機能の拡大、あるいは人間の身体機能の拡張説というのがあったんですが、電子社会はそれとも違う新しさがある。だからセキュリティの技術や新しい倫理学が重要になる、ということですね。

辻井　そうですね、住基ネットなどでも評判が悪い面があります。しかし考え方を変えれば、この電子社会で自分を主張できるものというように考えているんです。何かに価値を付ける。したがって電子マネーというのは、暗号でお金を守っているんじゃないんです。暗号でお金に価値を付けている。技術的には暗号技術によって初めて電子マネーというのはつくられる。これは今はまだそれほどではないけれども、経済のボーダレス化などを進める大きな道具として将来国際経済社会に地殻変動をもたらすかもしれない。そういう単に守りというよりは積極的に社会を変えていくようなところがあるということを言いたいわけです。

サイバー世界というのは真と偽が峻別しがたい世界ですから、何が本物であるか、真正性の保障、真と偽の区別をきちんとすることによってサイバー世界は成り立つ。それが結局サイバー世界では素数です。本物を瞬間に見分ける力を持っている。それは単に情報を隠すというより、もっと積極的な意味を持っていると、そういう方向でわれわれは研究を続けているんです。

（おふたりは各種委員会や会合などで旧知の間柄だが、直接の対談はこれが初めて。哲学・文明論ではピタゴラス＝プラトンの「数の世界」に基礎づけられた西欧社会の成立とその評価、さらに一神教と多神教をめぐる問題など熱を帯びて続いたが、紙数の関係で一部割愛した）