第2日目　総括討論

司会(早田)：高橋さんから全体に関するコメント・質問等お願いします.

高橋：札幌学院大学の高橋です．終盤の時間帯でありますので，技術的な問題から社会的な問題にコンテクストを移して質問をさせていただきたいと思います.

特にセキュリティ技術が実用化段階に達して,それが具体的な社会制度,社会情報のツールとして使われる段階に達したときに起こりうる問題をどのような技術外的な仕組みでカバーしながら使っていくか，という問題に関してです.

森田先生のお話でいいますと，暗号技術には暗号をかける者と破ろうとする者のイタチごっこがあって，暗号が破られる可能性というのがたえずある．それに対する一番確実な方法は，たとえばユーザーの体にチップを埋め込むことだというお話があるそうです．ですが，社会制度の中では人間のなすことの不完全性というものをはじめから折り込んで,その結果が最悪なものになることだけは回避するという発想があります．たとえば裁判制度でいうと,疑わしきは罰せずとすることで,無実の人を罰することだけは回避するために，あえて罪人を放免する可能性を残す方を選ぶということがあります．最悪のものを回避するために，それに準ずる悪をあえて選ぶ場合もあるわけです.

体にチップを埋め込むというのは，技術的にはこれ以上ない最高の選択であったとしても，心理的な抵抗はかなりあると思います．ですので，そこまでやるくらいなら，何かセキュリティ上の問題があって損害が生じたときにそれを補償できるような保険制度を用意して，技術的な不完全性を補うという選択肢がありうると思います．そこで，このような

セキュリティ技術と社会制度の補足関係のあり方について，技術者の間でどのようなご議論がおありなのかについてお聞きしたいと思います.

それと関連して，吉村先生におうかがいしたいと思います．昨日のお話の中で銀行の小切手のサインを判定するというような場面で実用化したいというのがありました．そのようなかたちで製品として実用化された場合,これが万一誤読をおかして経済的な損害が生じたときに，誰がこの責任を負うのかという問題があります．製造物責任ということが家電製品なんかでは認められるようになりました．鑑定家と機械との関係でいったとき，鑑定家にできて機械にできないことが，はっきり1つあります．それは責任をとることだと思います．ですので，そこをどのような社会制度で補ってゆくかという点について，どのような展望をお持ちなのかについてうかがいたいと思います.

司会：それでは森田先生から何か.

森田：イタチごっこという話を昨日してしまいましたが，簡単にいいますと，確かにある面でそれは日常的な事態なのです．たとえば昨日よりは今日の方がパソコンの能力が上がっていくと，暗号の処理が早くなります.

ですから当然アタックの能力もどんどん上がっていきますから，その分暗号の方も強くしなければならない．

ただ，それについてみますと，今から15年くらい前の研究発表では，ほとんど安全性をイメージさせる思惑だけで案を作っていた人が多いんです．そういう思惑で何となく安全だという人がいて，全体的にもなんとなく大丈夫かなというような状況だったのです．

ここ1～2年の流れでいきますと，――昨日いった流れと逆のことをいっているような感じもあるのですが――安全性の保証をつけた暗号というのがトレンドになっています．素因数分解とか，そういうベースになる問題自体は，当然先程いいましたようにだんだん短いものを長くしなければならないとか，そういう差はあります．けれども，実はその枠組みの中ではほとんどそういう問題と等価であるという考え方もあるのです．いわゆるDLPとかFPとかという計算上の問題でベースになっている安全性の指標とほぼリンクするようなかたちの安全性証明がついている，というのが結構あります．ですから，ある面では情報セキュリティの分野ではかたがついてしまって，安全性についてはもう100%保証されている．あとはそのベースになっている問題が人類にとってだんだん既知になり，ノウハウがたまって，解読が簡単になりつつあるという問題だけなんですね．そのよい例が共通鍵暗号DESです．有名なAESはちょっとまだ古いタイプのものなんですが，たとえばパブリックキーでRSAとか，その流れのものにはOAEPとか，いろいろそういうのが出てきてますし，我が社からも結構いろいろ安全性の証明については出しております．ですから補足しますと，イタチごっこといいながら，意外と情報セキュリティの中でのイタチごっこはそんなになくて，だんだんと錨がきっちりと降りて安全性が実現されつつあるということなのです．

それから先程のご質問の後半で，責任の所在をどうするかというお話がありました．それは要するにペナルティーをどう与えるかという話だと思います．昨日の中野先生のお話だと，ある程度の基準を設けて，その基準に達しない人は，最悪の場合，退学にするというのがあるわけです．私どもの電子マネーとかそういうところでもやっぱり同じような問題がありまして，今はとりあえず仮名の状態で匿名性を確保しながら，普通の現金と同じように電子的な世界でショッピングができるというのを普通の状態とします．それで何か起こったときに，たとえば何か悪さを働いたという段階では，逆に匿名性が破壊されて本名がパッとでてくるようなかたちのペナルティーを与えています．電子マニュアルとか，新しいものを作ろうという人間たちの中には，非常時に備えてそういう枠組みを作ろうとしている者もおります．

電子チップを埋め込むとかいう話は，冗談半分で言ったつもりですが，学会でもそういう話の方が楽しいとか，極端な方がよくわかるということで何人かと話をしたことがあります．ただ現実はそれに近いわけです．電子チップではなくても，ある面で監視されていて，どこかで悪いことをしたら，いきなり指名手配されてしまうと．「ビッグブラザー」というのがいて，いわゆる全体のシステムを支配している人が，その心の持ちようによってすぐに誰かを責めるような状況ができあがってしまう．オーソン・ウェルズの『1984』でしたか，あの小説の話にあるようなことは結構セキュリティの分野でも「ビッグブラザー」という固有名詞で利用されています．そういうところは仕組みとして多少は入れる必要はあるとは思いますが，最後はコンセンサス，いわゆる我々の社会の中でどの程度受け入れるかということになります．

そういう意味では全体を管理するシステムを徐々に入れましょうという方向だと思いま

す．経済的な例でいうと，今一番ティピカルなものは我々がよく使っているクレジットカードです．これは，いろいろな人が偽造を働いていて，一説には氷山の一角のみわかっていて，4～500億円くらいの損失があるそうです．本当はもっとその10倍くらい多いのではないかという人もいますが，そのためにかかるお金は保険料でまかなっているのです．このように偽造による損害は保険で補っているわけですが，その代替案がない．クレジット会社は手数料で儲けていますから，その手数料から保険料をごそっと引かれるのは嫌だというので，SETという電子的な規格を入れたりしているわけです．ですから，流れとしては，保険と我々の持っている技術とのバランスを取りながら，我々の社会のそれぞれの人が――指紋押捺問題ではないですが――あまり拒絶しないところを見ながら徐々に全体を管理するシステムを入れていくというのが一番良いかなというふうに思っています．

司会：ありがとうございました．

田中：イタチごっこに関係して，今実はセキュリティというのは技術的にはかなり完成度が高くなっていると，そういう意味のお話をうかがったと受け取りました．それはそうではないかと思うのですが，実は安全工学のところでMTBAという概念が提出されたことがあります．MTBAというのは，mean-time between accidentsです．たとえばボイラーといいますと技術的には完成されたものだというふうに考えられていますが，そのボイラーの事故が決してないわけではありません．その事故を計るのに，たとえばその現在のボイラーのうち，1年で1,000台に1台が事故を起こしたといたしますと，ワンセットのボイラーを1000年使っていますと，必ず事故が起こるということになります．それで1台のボイラーが何年続けて使用されたときに事故を起こすかという，その時間に換算したもの，それがMTBAなんです．不思議なことに，そのMTBAをボイラーだけではなしに，たとえばダムのようなものにまで拡張しましても，ほぼ一定でした．現在ではその値が約2万4千時間から2万8千時間ぐらいになると考えられているらしいのです．もちろん，技術的にボイラーはほとんど完成しておりました．にもかかわらず，そのような事故が起こるというのは，これはやはり人が使うからだと思うのです．1つの機械的存在としてのボイラーと，社会的存在としてのボイラーとは安全性が違ってくるのではないだろうか．したがって，技術的な安全性というのがほぼ100%近くなったとしても，しかしそれでその問題がなくなるわけではなくて，MTBAのような考え方は，やはり成り立つのではないか，新しいセキュリティの問題がそれに関連してやはりずっと出てくるのではないかという気がしたものですから一言申し上げました．

森田：どうもありがとうございます．まさにおっしゃるとおりで，この前も私どものプロジェクトをやっていて直面したのは，まさにその問題ばっかりなんです．ヒューマンファクターというのがまさにそのとおりで，特によくいわれていることは，ほとんど犯罪的なことの9割以上は内部の者の犯行で，そのうえ我々が思いもしないことが起こる．そういうものが何かの過程から入ってくるわけです．先程，中野先生のダブルクリックの話とシングルクリックの話は面白かったです．要するに想定しているものが全部自分中心に，自分ができることはみんな知っているんだっていうのが作り方の当然になっちゃうわけですね．技術者のおごりなのかもしれませんけれども．やはり今，我々が特に心をさいているのは，ヒューマンファクターにどう対処するのかということですね．たとえばICカードにその人の個人情報を入れておく場合，それはそのカードをなくさないという前提があ

るわけです．ところが，よくなくしたり，落としたり，壊したり，そういうことがしょっちゅう起こっているわけです．それはそれを使う前と比べてみると，当然セキュリティは上がっているのだからいいだろということもいえますが，どうもそれでかえって従来よりも面倒くさい社会になってしまったともいえるわけです．まさにおっしゃるとおりです．

信頼性という場合，自然対象だけではなくて，要するに人間も含めてセキュリティの管理とか，そういう問題にどう取り組むかが，まさにこれから重要になってくると思います．

野川：厚生省がセキュリティを非常に重視していまして，たとえばエイズの問題に関連したデータが，ネットワークから漏れてはいけないということで暗号をかけているのです．厚生省が言っているのがいわゆる電子的な暗号だけというのが問題で，まず物理的セキュリティをしっかりしないといけません．物理的なセキュリティを破られると，どんなに良い暗号をしていても，コンピューターの前に座られると，セキュリティが守れないというわけです．診察室とかに端末を置くのですが，そこはカードで入れる部屋にするんですね．サーバーはちゃんとカード管理のサーバー室で，他の人間，関係ない人はコンピューターの前に座れないというふうにするわけです．ですから，電子的なセキュリティに関する議論は非常に多いのですが，進んでいるようでいて，実際にシステムで活用されているのが物理セキュリティなのですね．ところが実は，その物理セキュリティを確保するのに，とてもお金がかかる．たとえばドア１つひとつに全部 ID カードを付ける，それも全部特別に回線を引いて，中央の警備室で全部危ない人が来たら全部自動的に閉めるとか，そこまでやるとえらいお金がかかってしまう．

田中：今の物理的セキュリティに関係して前から非常に気になっていることが１つあるんです．自然現象にエアシャワーというのがあります．非常にエネルギーの高い宇宙線がやってきて，ごく短い範囲，実際には半径１ミリメートルくらいの範囲で何万という粒子がつくられている．そういうふうなエアシャワーがたまたま重要な素子にぶつかったりしたときに，何らかの影響が出ないのかと．そのエアシャワーは地上地下のどこにも必ずきていますので，おそらく今まで起こったコンピューターの事故のうち，全く原因不明のものの中にはそういう場合があるのではないかということなのです．これはしかし，防ごうと思いますと，上空に厚さキロメートル単位のカバーで地球を覆わなければなりませんから，そういうことはまず不可能なんですね．ですから，そういう部分はやはり残るのではないかという気がしないでもありません．

野川：それに関しては，最後の最後は人間がかかわるんでしょうね．

照合の話で最終的に誰が責任をもつかということですけれど，よく似た話がすでに医療系にありまして，心電図の自動診断というのがあります．今，心電計は賢くて，全部診断が出てくるのです．その診断が間違っているときの最終責任者は誰だというと，結局医者なんです．結局，それをうのみにして患者の治療をして，間違ったらその医者が悪いという原則が一応医療系でできています．

銀行の場合でも，最終的には人間が判断するということになるでしょうかね．そのときの機械のつくり方にもよりますが，問題があるときははじく，あるいは全部人間にまわすとか，それで最終的に人間がセキュリティを守ることになるんだと思います．

司会：どうもありがとうございました．

それでは先程の高橋さんのコメントの後半の方で，吉村先生への質問がありましたので，吉村先生，お願いします．

吉村：私の考えは，できればタイプＩのエラーは，なるべく小さくする．そしてタイプ

IIのエラーを大きくしても，やむを得ないという考えでたぶん昨日もお話ししましたし，今もそう思っています．タイプIIのエラーをではどうするかという問題なんですが，アラン・ドロンの『太陽がいっぱい』で，署名を偽造して，そして多額のお金をせしめましたね．あれは取られ損ですね．署名を盗まれたことが問題ですね．ですからやはり，真似されない署名をつくることが先決です．やっぱり当人が被害を受けるのだから，これが大前提です．その次に，やはりもし見つかったときは，ものすごい罰を受けるんだと，すごい罰則が待っているんだということを使う人間にひやひやさせるようなことをすべきであると思います．それ以外はないと思います．ですから，署名をクリエイトしてくださいということです．

司会：どうもありがとうございました．

それでは残り時間が2～3分ということですので，最後に本学部の初代学部長で，日本社会情報学会会長の田中一先生から一言総括をお願いします．

田中：昨日もちょっと申し上げたことなんですが，一言だけ付け加えてご指名の責任を果たしたいと思います．

今回のシンポジウムもいろいろな興味あるお話を伺いました．お話を聞かれる皆さんはいずれもセキュリティ，あるいはそれに関連する技術的な話のように受け取られたと思いますし，また実際そういう面が強い話かと思います．しかしながら，お話の内容は決してそういうふうな視点だけからとらえるべきではなくて，もっと広い見地からも見ることができるのではないかという点について，感想を一つだけ申し上げておきたいと思います．

昨日も少し申し上げたところなんですけれども，別の観点から，すなわち社会的な観点からこれを見たときにどう見えるか．その考え方をたどる道筋がいろいろあろうかと思います．現在社会をつくっている人間も次第にこの地上に誕生し，生物から進化してきたものでありますので，その進化の中でどのように問題が現れて，それが人間社会に至るまでどう発展したかということをたどるのも一つの考える道筋ではないかと，私は思っております．そういう意味で，まず我々人間を生物として見ますと，この生物としての個体を支えていくものに免疫系があるということを昨日申し上げました．もちろん，その自己というものの誕生は，決して免疫系から出たものではありません．しかしながら，一旦自己が誕生しましたときに，それを支えていくものとして，支える必須の条件として，自分と自分以外のものを区別して，そしてその区別に基づいて異物を排除して個体を維持していく面が生じたと思います．この免疫系に類するものは，聞いてみますと，ミミズあたりの段階から次第に始まったようなんです．だからずいぶん長い歴史があるように思いますけれども，人間に至ってその免疫系は一層発達したというふうに聞いております．人間は意識的な存在として社会を形成しております．そうすると，自己を支えるものが社会的に存在する人間にも新しい形で現れてくるというふうに当然考えられるべきではないかと思います．社会的存在としての人間を他と区別する，そういうものが新しい形をとって現れざるを得なくなるのではないかという気がいたします．

全く話は別で，昨日も懇親会のときに申し上げていたのですが，コンピューターウイルスというのは，それが出現するまで，こういうものがあり得るということはほとんど誰も想像しなかったと思うんです．フォン＝ノイマンは自己増殖なるものを研究いたしましたけれども，そのときは自己増殖という生物現象には，最小限度どの程度の情報が必要であるかということを知りたい，そういうことから出発したということを聞いております．ノイマンの本を読んでみましても，コンピュー

ターウイルスの可能性というのは全く出てこなかったです．フォン＝ノイマンは極めて知的に優れた人ですけれども，人間的面ではいささか欠陥がある人だということです．ですから，たぶんコンピューターウイルスという可能性を知っていたら，とても面白がって書いたんじゃないかと思うのですが，一言も載っていませんでした．ですから，あれは全くの予想外のことだったと思います．そういう予想外のことがいろいろとこの情報的な人間社会で起こってきます．そこにおける社会的存在としての人間が他と区別される，その区別というものが，安全性という形で表れてくる．あるいは暗号という形で現れる，というふうに私には思えます．ですから，安全性とか暗号というのは何か受け身のもの，いろいろな問題が起こってきて，それに対する受け身のものとして考えられたようにみえますけれども，実は普通の生物の個体から社会的存在としての人間に至る進化の過程で，現れざるを得なかった自己を自己とする非常に積極的な内容，そういう意味で社会的でかつ積極的な内容をもったものだというふうにみることができるのではないか．したがって，ここにも，今後の私たちの学部の名称である社会情報学が大きな役割を演ずることができるのではないかなというふうなことを感じましたので，それを最後に一言申し上げておきたいと思います．

司会：田中先生，どうもありがとうございました．これをもちまして総括討論を終了いたします．それでは総合司会の秋山さん，お願いします．

秋山：研究委員長という立場で最後のまとめをしなければならないかなという気もしていたのですが，先程田中先生がまとめてくださいましたので，その必要はなくなりました．

私は地質学・古生物学が専門で，進化論だとか生命の起源の問題に強い関心をもっております．その話に関連して情報という観点から言いますと，遺伝子のイントロン・エクソンの問題で，エクソンの部分には遺伝情報がくみこまれて，種としての統一性を保っていますが，イントロンの部分では個体によってみんな違っています．イントロンは遺伝情報として役割を果たしていない．この問題は進化上でどのような意味を持っているのか非常に大きな課題であろうと思います．ところが，下等な生物ではそうではなく，DNA の情報すべてが生物の機能の発現に役に立っています．シアノバクテリア（藍藻）は，35 億年の歴史をもっていて，大変興味深い生物です．この生物は紫外線によるダメージに対して非常に強いんです．私どもはやられるとだめなんですけれども，彼らは修復機能をもっております．このことは，シアノバクテリアの出現当初の地球大気には酸素がなくオゾン層が形成されておらず，したがって地球表面には強い紫外線が降り注いでいたためと考えられます．そのことと関連させて考えると，生命の起源，進化の過程等と関わって，情報の問題は非常に面白いなと私自身思っております．

実は昨日まで弘前で学会がありまして，1日早く帰ってきました．友人に「情報とセキュリティ」の問題でシンポジウムがあるんだと言ったところ，「地質学専攻の君が参加しても，理解できないだろう」といわれました．確かにそのとおりだと思って参りましたけれども，昨日からのお話をうかがい，今日の討論をうかがって，大変いろんな点で勉強することができたと思います．全くの素人ですが，良い勉強になりました．本当にありがとうございました．社会情報学を専門とする私どもの仲間も，すべての人たちが，このシンポジウムでいろいろな情報を得ることができたと思います．

このシンポジウムの内容は，学部の紀要『社会情報』に掲載することになっていますので，先生方のご協力をいただきたいと思います．

２日間にわたりましてありがとうございました．ずいぶん勉強をさせていただきました．感謝の意味を含めて拍手で終わりたいと思います．