第2日目 補足講演及び討論

秋山：では，これから12時までの2時間の間，昨日頂戴した3つの貴重な講演のかみ合わせのための補足講演と，それから私どもの方からも議論ということで，是非2時間を有効に過ごしたいと考えております．司会はこの会の仕掛け人の早田さんに仕切っていただくことになっていますので，よろしくお願いします．

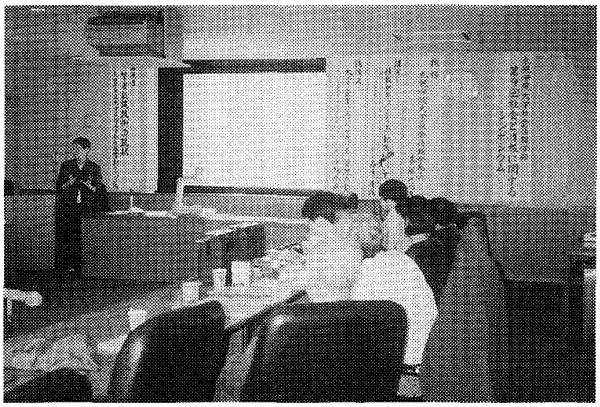
司会(早田)：それではプログラムにありますように，まず最初に補足講演から始めさせていただきたいと思います．各先生方から15分前後の講演を，昨日言い残したことがもしかあれば，それについて話していただきたいと思います．あと昨日の討論のときの文脈において何か付加すべきことがあれば，出していただきたいと思います．順番は昨日と同じということで，森田先生からお願いします．

〈情報セキュリティに関する標準化活動状況〉

森田：おはようございます．昨日は後半の話はちょっと駆け足でしたので，この時間をお借りして説明させていただきます．

1995年の『タイム』という雑誌に，結構ここでいわれているようなインターネットキャッシュに類似した話が載っていました．これに関連したことについて少し紹介しようと思います．

私もよくするのですが，別のサイトからインターネットを介して電子メールを送ることがあります．会社で名乗っているアドレスにうまくすり替えて出すということがごく簡単にできることで，ただサイトのログを全部見るとどういう順番かということがわかるのですが，それを消すことが自由にできるということがあって，うまくすると天国というところにいる神様からメッセージがきているというようなことができたりします．例えば，今ではビル・クリントンやビル・ゲイツから気軽にいろいろなサービスの話やメッセージがきていたりしているそうです．



もっと問題となるものとしては，西海岸のお話だったらしいのですけれども，スパゲティー屋さんみたいなところに，こういうメッセージを見たということを，あなたが当たったからおいでとか，何とか旅行が当たったからおいでとかのようなメッセージに変えられて送られ，それを真に受けて行ってしまったらそんな話は全然なくて，お食事して終わりだったというような話があります．こういうメッセージの信頼性というのが，我々が実際にもらっているメッセージのアドレスとかを見ただけでは問題があると言われています．特に昨日大分お話しましたが，プライバシーの問題でたとえばお金に一種の秘匿性を与えようということも非常に重要なのですが，それに合わせて，お金というと日本銀行の権威がついている1万円札とか千円札とか500円札とかあるわけですけれども，結局インターネットキャッシュとしてのお金の流通は，結局つくってみたものの，電子マネーといいながら電子署名をどんどん付けて，私は

基本的に日本銀行の権威の上でその上で認められた私の権威で，私は一応1万円札を持っているのですけれども，そのうちあなたに100円あげるという電子署名を付けて単に渡しているだけのことです．中身がわかってしまうと非常にたわいのないことを行っています．

これと対応してもうひとつ重要なことがあります．それはプライバシーという観点です．お金を千円，2千円というふうに使うのですが，はっきり言って森田という名前が知れるか知れないかということはそれほど重要ではないじゃないかという議論があります．たとえば私が八百屋さんに毎朝買い物に行くとします．そこでいつもメロンを買っていく．そのときにメロンを買っていく森田さんという名前よりは，あの顔とあの表情とこっちににこにこしてやってくると，必ずメロンを買ってくれる，そういう情報の方が重要なわけでです．そもそも本名とか仮名とかいうのは重要な意味があるのかという議論が今すごく起こっています．

そうはいっても，はじめて会ったときから電子的な，即ちインターネットの社会でしかコミュニケーションがもともとなかった人というのが結構いるわけです．オフ会とよくいわれるのですけれども，あまりに親しくなってしまったので会わなければしょうがないという状況もあるのですが，そういうのは特殊なケースというふうに考えて，やはり離れていて顔が見えない状態でもある程度誰が誰なのかというのをチェックする方法は必要だと思います．今現実としてプライバシーがどの程度必要か，その最底限の枠組みをどうするかというのが今すごく重要になっています．

そういう意味で昨日インフラとして電子署名における本人確認を行う形式として2通りあり，自分の名刺にお墨付きをつけるというケースと，名刺をもらったあとで後付けでどこか権威機関を訪ねてこれは正しかったということをチェックするケースです．この2つのケースが非常に重要です．このような枠組みをつくろうと思って現在いろいろな研究を行っています．

標準化組織では，情報セキュリティ全体の枠組みをどうするについては20年くらい前からいっていましたが，いわゆる情報処理の分野では，JTC1という組織で行っています．これは，ISOとIAIECという国際電機連合のJTC（ジョイントテクニカルコミッティ）で，情報処理に関する情報セキュリティについて検討しています．アメリカでいえばANSIに相当するような形の組織をつくっていて，アメリカが非公式で事務局を担当し，ニューヨークに事務局があります．JTC1はISOとは区別した情報処理の分野という形で活動しています．

JTC1の下にはいろんなテクニカルコミッティが出てきて，有名なところではMPEG3という規格をつくったSC29があります．そこでは我々の情報セキュリティよりもかなり先行した形で参照レイアモデルをつくっていて，その関連でセキュリティの枠組みをつくったチームがいろいろあります．その中でセキュリティだけを専門に扱うのがSC27です．国内では，全部ではないですが，ほとんどのJTC1に関係する部分は工技院が窓口になっていますが，実際に委託を受けてやっているのは情報処理学会や情報規格調査会などが日本の窓口になっています．

今その中でWG1・2・3の3つありまして，WG1はトラステッドサードパーティと言って，CA，つまり証明書の権威付けをしてチェックをするための機関となっています．あとタイムスタンピングが最近流行のテーマで，社会的な枠組みをつくろうという流れでやっています．WG2は，電子署名や暗号アルゴリズムをどういう枠組みでつくったらいいかというのを決めています．ほとんどは学会と表裏一体の活動を行っています．WG3は

あとで紹介しようと思っているのですが，コモンクライテリア，これも一種の枠組みづくりなのですが，いわゆるセキュリティというものを社会の一種のインフラ的な意味で捉え，たとえばソフトウェアに関しても，安全性の強度のレベルはあるかというようなことを議論しています．たとえばFAXレベルでアタックはこのくらいだったら，このレベル以上の機能を備えているものが安全度C3レベルとかですね．ウインドウズ95でしたら，コモンクライテリアのレベルですとDで，Dというのはセキュリティをまったくケアしていないということです．しかし，ウインドウズNTになるとたしかA1のレベルで，かなりケアしていることになります．このようなクラス分けは，いわゆるDODという国防総省のオレンジブックが源流になっているのですが，その後民生品においても重要になってきているので，よく使われるようになっています．

2年くらい前にアメリカの委員会で報告したとき，その内容をあとで送ってくれとか，コピーとらせてくれないかとか，あとでFAX送ってくれとか，色々と要求がありました．いろいろ難しい内容があるので慎重に対応したいと言ったのですが，そうしたら向こうもセキュリティの担当者で，FAXのレベルは何とかレベルだから，君は安心していいからどうか送ってくれということでした．既に欧米ではこういうセキュリティ基準に照らした行動が普通に行われているのです．

現在のSC27の規格は，電子署名とか相手確認とか鍵配送とかいうメカニズム的な規格を即国際標準にしたということで，現状では全部アルゴリズムしかできていません．後追いで今JISをつくっていますが，今年中にISOになっていてJISにないというものはほとんどなくなります．今回お話したようなことは全部いずれJISにもなります．

先のWG2で少し特徴的なことは，暗号登録制の問題があります．現在，イギリスのナショナルコンピュータセンターという政府系の組織で暗号を登録するというような話になっております．昨日お話しました中で，20件中4件も日本の登録があるので日本のアクティビティが高いがごとく言ってしまったのですが，暗号登録と暗号が標準に採用されているというのが一般には同じに聞こえてしまうようで，この面をコマーシャル的にうまく利用して，どうも各社がどんどん暗号登録しているからのようです．暗号登録制の目的は単に通信という共通の土台をつくるためのオブジェクトアイデンティファイアの暗号版をつくったというだけなのですが，話がどんどん権威付けの方にいってしまっているので，日本の活動が少々問題視されています．

登録制にする意味として叫ばれていた話は，一つでは安全性を保障できないじゃないかという不安への対応のためでした．それから世代交代も当然激しいということが2つ目の理由です．しかし，1996年にCOCOMからワッセナ条約というちょっと方針転換が起こって，いわゆる共産主義，危険な国家に対するブロックづくりとしてのCOCOMだったのですが，それがもっと限定されてというよりは，ロシアや中国もちゃんと仲間に入れていわゆるテロ国家を封じ込めるための対応に関するものです．暗号は1種の武器ですから，それがテロ国家に流れては困るというので，特に先進国中心に方針転換が行われて，そのあとOECDで一応権威付けされて，日本でも去年くらいから徐々にいろんな法制化が進んでいるような状況にあると思います．実際に運用までは至っていない状況ですが，ワッセナ条約との関連で暗号登録制を見た場合，登録制に関してかなり批判がありまして，我々は信頼性のある社会的責務を負った標準化活動にしていることをアピールしているわけですが，今後は自分たちがいいというものをちゃんと標準としてつくってみんなで使っ

てもらおうと，そのぐらいの気構えでやりましょうということで1996年に方針転換になりました．

標準で採用されているアルゴリズムはいっぱいあるんですが，結果的に権威付けされているのはアメリカの規格とNTTのESIGNチャットで，この2つだけが今国際標準の本当の規格として認められているものです．それ以外に松本・高島・今井方式ですが，これなんかはまだアルゴリズムとして入っているだけですが，それでも驚くべきことに，日本の委員会が提案したんじゃないです．韓国の方からこれが良いんじゃないかと．他の日本の方式もそれなりに評価されています．暗号登録制のもとで実際には，今20個あります．国際的知名度という面では10番目や11番目がそれなりに有名でしたが，そのあと日本電気が2つ，日立が3つ目を入れたりと，このような登録活動については批判的な見方もあります．

安全性について昨日ちょっとご質問があったのでその話をいたします．昨日のようなあやふやな話を普通我々いってしまうのですが，それでは困るというのが結構ありまして，TC68という金融関係をやっている委員会で勧告というのをだしております．それによると共通鍵暗号，我々のFEALやDESというよく聞く暗号，に対して推奨される最短鍵長はどのくらいあればよいかということです．鍵探索はものすごくコンピューティングパワーを必要としますが，LSIの技術等の進歩によって，ものすごい驚異になっていますので，共通鍵暗号については少なくとも80ビット以上の鍵を採用するべきであると言われています．斜線の部分だけは本当に勧告になったところです．公開鍵暗号に関しては楕円曲線暗号が160ビット以上で，その他は普通RSA暗号とかDSLという方式で，それは1,000ビット以上が基準となっています．デジタル署名については勧告がなかったのですが，実は電子署名ともいいますが，公開鍵暗号と電子署名は区別がないと思われてしまったようで，それでこれににについては勧告を出さなかったと担当の方が話していました．そんなこんなで現状は安全性についてそれなりのケアをしているという状況です．

最後にセキュリティの評価基準についてですが，一応系譜を出しますとNATOの諸国が主に活動をしてきています．コモンクライテリアを去年までかなりの時間をかけて，ヨーロッパ標準とアメリカのオレンジブックのセキュリティ評価基準とさらにカナダの3つを合わせてつくっておりました．それを今度はISO版にしようというので，リファレンシャルクライテリアという似たような名前なのですが，そういうものをこれまで作業としてやっていました．ともかくISOIC 15408として，今年の6月8日成立しました．ISOのページを見るとcongratulationと書いてあります．ISOの9000とか14000シリーズというのがありまして，これは欧米主導のもので，9000は日本でいうとQCサークルなどががんばっていたようですが，そういうクオリティーを上げるためのクオリティーコントロールですね．その辺のシリーズ化がされていたということです．

当然のことながら草の根レベルでは欧米なんかより全然日本の方が進んでいたのですが，それをロジカルに指針にまとめ上げて，こういうふうにやるのが全体の効率向上にもなるし，プロダクトの発展にもなるんだということになりました．彼ら欧米の流れに結局負けてしまって，ISO 9000の認定を受けるためにまた認定機関がどうのこうのと非常に悲しい思いをしたということがちょっと前にありました．第2波として表れたのは，日本は全然マインドは低かったので影響はそんなにひどくはなかったのですが，環境基準ですね．14000シリーズといわれているのがそれです．エヴァリュエーションクライテリアとい

うのは欧米の基準にそろえるという意味で15408からスタートするのですが，エヴァリュエーションクライテリアの認定機関はどうなっているのだということですね．セキュリティ評価基準もまたこういう枠組みの第3波としてきたのじゃないかなと，通産省なども緊張していたかもしれません．欧米に比べてこういう考え方の枠組みづくりというのは日本では遅れていますね．ところで，セキュリティ評価基準っていうのはシステムのためのもので，ここは認定に使われただけであって全体の枠組みをつくりましょうとそれだけのもので，そんなにこれ自身がテクニカルにすごいとかそういうものではないということをちょっと補足しておきます．時間が少々過ぎてしまいましたので，話はこのくらいで終りにします．

司会：どうもありがとうございました．それでは質問，コメント等ございましたらお願いします．ございませんか．それでは引き続き中野先生の補足講演に移ります．

司会：それでは次に中野先生に補足講演をお願いします．

中野：昨日はネットワーク管理について詳しくお話をしたのですが，こちらが社会情報学部ということもありまして，本日はまず，我々の学術情報総合センター（学情）における教育と研究について述べることに致します．

このセンターには，専任教員が全部で12名，4つの部門に3名ずつの先生がいます．ほぼ2年半前にセンターが立ち上がりましたが，それから1年くらいかなりしっかりいろいろなことをやりました．何しろその頃はスタッフは8人しかいなくて，更に実際にネットワークとかコンピューターで動ける人間は4人しかいませんでしたので．研究と教育というのは大学の先生の責務です．つまり授業を通して教えなければいけないというのがひとつ，それから自分の研究をちゃんとしましょうねというのがひとつです．これは誰もが認めることだと思います．ところが我々12名は，研究と教育だけではなく基盤支援もしなさいというように実は言われ続けてきたわけです．基盤支援の仕事を皆が1/3づつ受け持つかといいますと，先生方によって得手不得手が違いますから必ずしもそうではなくて，特にネットワークやコンピューターが得意な方は基盤支援が1/2であったりしますので，当初はそういう感じでやっておりました．ところがセンターが動き出すと幸いなことに非常に評判が良くて，本学の学生は8,000人なんですけれども，当初このうち2,500人程が毎日センターを使用しました．ゼミや研究室に入っていない学生以外はほとんどが，気楽にくつろげる場所としてセンターを利用してもらっています．7月に入ると試験が始まりますので，学内で唯一クーラーがきいている場所ということで，入館する学生数は5,000人とか6,000人のカウントがあるといいます．ただし，入館する度にゲートでカウントされ，二度三度入りますと重複されてカウントされることになりますから，実質はもう少し少なくなると思いますが，それにしてもよく利用されているといえます．ただ，基盤支援もネットワークもまだ全機能の1/2も使われていません．例えば情報コンセントについては，センターの中に4,500くらい埋められてあるのですが，残念なことに学生がコンピューターを持ってきて自由に使えるという環境にまだありません．

そういうことで，まだ100%を使い切っていないのですけれども，外から見る限りでは非常にうまくいっているように見える．それでは次は何をしなさいということなのですけれども，教員12名で独立大学院をつくりなさいという話が既にあります．元々我々12名が来たときは，基盤支援と並行して我々独自の研究をしなさいというように言われていた．

すなわち，教員の数を8名から12名にするときの条件として，大学院をつくりなさいと言われていたのですが，ついつい基盤支援が前へ走ってしまったので徐々に遅れてきたわけです．今年度に入って学長から，「新しい研究分野を創成してほしい」という内容のことを言われています．現学長は理学部出身の方なのですが，各学部の各分野で「情報」というキーワードを入れることによって何か新しい学問ができないかというように言われているのです．他の学部，例えば工学部だとか生活科学部，医学部など理系の学部は基本的に大学院の重点化構想に乗っかろうとしています．文系でも，この流れの中でどうしようかということが議論されています．各学部には縦割りの理念があるようです．理学部というのは自然界におけるものの本質を探るという理念，法学部には法学部の理念，医学部は医学部でまた固有の理念があるわけです．これらの理念を大学院重点化という形で実現してゆきたい．それでは我々が考えているのは何かといいますと，実はそういうような縦割りの理念ではなくて，それぞれを横断するような，「情報」というキーワードを基に応用分野を開拓する．逆に，各学部に所属している先生方のなかで，情報のいいところを使って新しいことをしたいという意欲的な方がおられれば，我々と協同して何かできないかと願っております．ですから，これまでの学部にはない新しい理念を指向し，それに基づいて独立大学院をつくりたいということで，実は5月に文部省の方に挨拶に行ってきた次第です．理念の大まかなところは文案も大体でき上がっているような段階で，まだ公式には出ていないのですが，大体こんな感じで進めております．コアになるのが12名で，各人各様の研究分野を担当するということになるでしょう．私はネットワークのセキュリティをやれといわれていますが，実は本当の専門はアルゴリズムでして，いまですと分散計算とか並列計算，元々はグラフ理論とかそういうところから始めていますので，この辺のところをこれからもしっかりとやれたらなと考えています．12名のなかには女性の先生が2名おられまして，いずれも出身は心理学です．また，インドから来られた方が1名おられまして，この方はGISの研究をされております．この他に図書館情報学のプロの方もおられる．それぞれの人が独自に研究分野をもっていて，またそれぞれがそれを使った基盤支援，私の場合ですと，セキュリティを含めたネットワーク支援をしています．これを更にもう少し他の学部の先生方と連携するような方向に発展させる．連携の仕方については模索中なのですが，例えばひとつには単位互換というのが考えられます．学部間の単位互換ということが考えられますし，それから他学部の先生方に兼担という形で入ってもらうという方法もあります．それからもうひとつは，いくつかのプロジェクトを立ち上げて，そのプロジェクトに入って頂くというそんな形もいいかなという気がしています．このような形態の大学院をもっているところでは，大体こういうプロジェクトを立ち上げて募集するという形をとっているようです．我々のところでは，一応総合情報学ということで検討しております．ただし，総合とはいいましても，社会科学，人文科学，自然科学のコンピューターや情報に関係したあらゆる人達と協同するということはとても無理ですが，例えば商学部や経済学部の先生と連携しながら，広い意味での電子商取引について共同研究を行うといったことなら可能かもしれません．社会科学の先生方から見ると，電子商取引というものはどうイメージされるのか．また，我々情報系の人間からすると，そのイメージされているものの実現は技術的に可能か，ということが議論の中心になるところです．それから逆に，商学部や経済学部の先生方が知らない世界があります．例えば先程森田さんが言

われた匿名の世界，これはコンピューターの世界では割と一般的になっています．社会に出ると私は大阪市立大学の中野なのですけれども，家に帰ると吹田市山田東の中野というように二面性をもっています．これからの社会というのは，従来の職場としての人間と家庭としての人間に加え，三番目の顔として，おそらくボランティアとしての顔が出てくるだろうと想像しています．ところが現実のネットワーク社会はそうではなくて，自分の大学の名前のアカウントですべてメールを出してしまっている．家庭の中の中野ではなくて，大阪市大の中野として普通の友達と話をしている．私の場合は自宅にドメインがありますので，割とそういう切替ができるのですけれども，一般の方はそういうことをしません．普通はどうするかといいますと，社会，すなわち企業や大学の中での電子メールアドレスと，ニフティのような商用プロバイダへの個人アカウントの二つをもつということをします．後者では，割と匿名性が一般的な世界なのですね．このように，ネットワーク社会と現実の社会とは違うので，その辺はこれからどうなっていくか．これは広い意味で社会科学なのですけれども，電子商取引という形でプロジェクト化した場合どうなるかという話がまずあります．それからいま一つは，今回のテーマのセキュリティとも絡んでくるのですけれども，法学部の先生方と共にセキュリティだとか知的所有権だとかプライバシーだとか，そういうものをこれからやっていけないかなと考えております．要するに短期的な研究をするのではなくて，5年，10年を見込んだ研究がプロジェクトという形で可能かどうかということを各学部の先生と相談し合う．また本学は8学部もっていますので，これら8学部の学生，あるいは他大学の学生，社会人や留学生でも結構なのですけれども，このようなテーマに関心を持っている学生をうまく取り込んではどうか．たまたま入ったのは文系だけれども，もう少し理系的な側から情報について勉強したいという場合があるでしょうし，逆に，たまたま理系に入ってしまったけれども，もう少し人間や社会のことについて勉強したいと感じている人達を見つけて彼らを積極的に取り込む．一応，大学院のことを考えていますので，2年ないし5年入ってもらって，各分野のノウハウ的なもの，例えば我々の場合でいうと，コンピューターサイエンスではどういう流れの中でどういうことをやっていて，というようなことを理解して卒業してもらうわけです．おそらくこういうような体制は各大学必要だろうと思います．我々のところのように12名程度がいいかどうかはわかりませんが，各大学がそういうような形で動くときに我々のような組織が必要とされるように思いいます．そうするとそういう人達を我々が新たにつくり出して送り込む．そういう人達をつくり出すような大学院をつくりたいなと思っています．

この学部が抱いているイメージと多少異なるかもしれないのですが，我々がいまどういうことを考えているかということをお話させて頂きました．以上です．

司会：どうもありがとうございました．それではただいまのご講演に対しまして，何か質問やコメント等ございましたらお願いします．

秋山：社会情報学部の秋山です．たいへん参考になる興味深いお話を伺ったのですが，独立大学院については，20年くらい前に北海道大学に環境科学研究科というのがつくられております．当時は核になる組織が12名ではなくてもう少し多かったかもしれませんが，協力講座という形で，理学部，工学部，医学部の各講座から入ってかなり大きなものにしておりました．先生のところでは，そのような協力講座ということをお考えになっていらっしゃるのでしょうか？

中野：大学院をつくるためには，いわゆるマ

ル合の先生が必要なのですね．私が文部省になぜ行ったかといいますと，本当のところマル合の先生が何人いるかということを尋きに行ったわけです．12名のうち2名は助手ですからノーカウントです．各学部とも同じように重点化の問題を抱えておられて人を出せないという状態なのです．とりあえず12人で何ができるかということを模索しながら，でもやっぱり人が足りないということになれば，先生がいまおっしゃった形でやっていく．プロジェクトとしていま，商学部・経済学部に対しては電子商取引という話で，法学部にはセキュリティということで打診していきたいと考えていますが，これらについては割とみんな認めて頂けるかなと想像しております．そういうなかでやっていこうかなというように思っています．12名のうち心理学出身の先生もおられますので，文学部とは，社会心理に関係したグループウェア的なことを少し検討してみたいと思っています．他の大学でも同じような試みがあるのですが，ほとんどがプロジェクト形式をとっており，なかには一風変わった名前のものまであります．ですからある意味で，今後何十年も続くようなコースなどつくれないと開き直る．ただひとつ問題となるのは，私などあと10年くらいは別に構わないのですけれども，定年まであと20年とか30年という先生を貼りつけたときに，プロジェクトが終わったらどうするのだろうということがあります．現在，大学では任期制の問題が取りざたされていますよね．その辺の含みで何かできないかなと考えているところです．5年経ってからどこか職を探してよというのはちょっとまずいので，その辺りのコンセンサスを取る必要があります．

秋山：プロジェクトというのは非常によい方法だと思うのですが，ただ，いま任期制というお話があって，2003年のデッドラインがございますね．ですから，文部省の認可の際には任期制という条件の下で認めるということになるのではないかと思われますが，その点は如何でしょうか．

中野：ただ公立大学というのは少し事情が異なります．国から束縛されているわけではなくて，我々の大学の場合，大阪市の意向が非常に強い．また，いま国立大学の独立行政法人化の話が出ていますが，それでは市立はどうなるのか．このような状況のなかで，なるべくうまく人事の流動化を図るような形にもっていけないかどうか模索しているところです．若手のうちはものすごく研究ができる環境のなかにいて，ある程度年配になってくるとマネージメントというか研究指導というか，そういった方面で活躍できるように流動性をもたせた仕組みをつくることができればよいかな，というような気がします．

司会：ありがとうございました．はいどうぞ．

野川：札幌医大の野川です．横断的なプロジェクトを行うときに，まずひとつ問題となるのは，両方分かっている人間が一人いないと，うまく機能しないという面があります．例えば，工学部の人間が医学を勉強し，医学部の人間が工学の勉強をするというような場合，前半の2年くらいは他の分野の勉強で終わってしまうというケースが非常に多いと思います．その辺のことをどのように考えておられるのか伺いたいのですが．両方分かる人間っていらっしゃるのですか？

中野：私は工学部の電気系の出身ですから，電気から情報に変わったという立場で言いますと，基本的にはユーザ系の人が情報なり電気の方へ流れていった方がいいように感じています．ユーザ系でよくわかっている人が一人コアとなるような仕組みをつくっておくと割と便利な気がします．文系でも学部に一人くらいよくわかっておられる先生がいます．そういう人達をうまく使う手があります．それから，若手のなかでも，コンピューター大好き，インターネット大好きという先生がいらっしゃいます．こういった方々をうまくナ

ビゲートしていければよいかなと．逆に情報系の人はあまり前面に出るとよくないような気がします．なるべくユーザ系の先生を立てるような形でやっていく．我々の学術情報総合センターの次の所長をどうするかという話は既に始まっているのですが，文系を含め，学内で人脈が豊富な先生を候補として立てることでできればと考えています．

野川：確かにそのとおりで，僕がいた大学院では工学部系と医学部系でずいぶん事情が違っていました．僕は医学部出身で，一応工学部の人間に医学関係の研究をするための勉強をいろいろ教えてきたわけですけれども，僕は彼らが医学関係の知識を修得するよりもはるかに速いスピードでネットワーク管理の知識を修得して，数年いたら教室の管理者になっていました．２年で管理者になっていました．３年目にはとうとう普通の工学部のドクターコースの学生以上の管理をしていました．

中野：それは考えてみれば当然で，ユーザ系といったらおかしいかもしれませんが，要するに自分が何かやりたくてそこに入られた方が単なる道具としてコンピューターのネットワークを使うわけで，それは上達が速いと思います．その単なる道具に過ぎないコンピューターとかネットワークが好きで入った人が，「あなた明日から金融関係をやりなさい」とか「明日から解剖をやりなさい」と言われたって戸惑うだけです．たまたまその分野が好きだといいですけれど．そのあたりに関してはある程度仕方がないのかなと．逆に我々は，普遍性のあるもの，いかにそういう人たちにとって使いやすいものを提供するかということにもっと注意を向ける必要があるように思います．工学系の人が使いやすいというのと，それ以外の人，私はよく「普通の人」という言葉を使うのですけれども，普通の人が使いやすいというのには大きなギャップがあるのですね．ですからその辺の事情を我々が理解するという姿勢が必要だと感じます．例えば，普通の人たちに講義するとき，安心させるためによく「マウスのダブルクリックというのは50歳を過ぎたらやれません．安心して下さい」と言うようにしております．更に加えて，「あれはコンピューターをやっていた人の奢りであって，若い人がやってやれたから使っているわけで，いまどんどんユーザインターフェイスの主流はワンクリックの方向に動いています」と言うと割と安心するみたいです．似たようなことが他にも割とあります．こういった事情を理解できる人達をやはり情報系のなかでも育てないといけない．特に最近，障害者の人たちともおつき合いしていますので，特にそう感じますね．コンピューターネットワークをやっているとどうしても視野が狭くなるので，それを何とか広げる．そういう意味でもやはり応用の人達と一緒にするような研究が大切であると考えます．

野川：それで大学院として認められたら何博士になるのですか？

中野：それぞれだと思います．その他に学術博士というのがあります．本学では，生活科学部，昔の家政学部ですが，ここで学術博士が出ています．こういった方法もあるのでそれでもいいのかなという気がしています．ただ二つのコースをつくるので，そのうちひとつは工学博士となるかもしれません．最終的には文部省との交渉になるでしょう．

司会：話題は尽きないと思いますが，もう既に予定の時刻を超過してるようですので，中野先生の補足講演はこの辺で終わりにしたいと思います．どうもありがとうございました．引き続いて，吉村先生の補足講演に移ります。

吉村：昨日お話が足りなかった部分を補わせていただきます．フローとしてはこんなふうになります．このように各プロセスにおいて

いくつかの注目すべきことがありますので，この辺を少し要約しておきます．

前処理はどんなのがいいのか．特徴はどれが適切か．そして測度は何で測ったらいいか．判定法はどうか．

さて，どんな前処理が必要か？　良いか？ノイズ処理はノイズの入り方によって有効性が違います．これはたぶん実際にやる人でないとあまり興味ないでしょうけど，ぼかしとか平滑化，スムージングですね．閾値処理，細線化，輪郭線抽出，正規化，周辺部分領域の濃度除去，領域からの文字部分きりだし，こういうものが役に立ちます．

それからどの特徴量が有効か？　適切か？これはやはり簡単で早く抽出できるものがいいでしょう．勿論正答率をあげ，頑健性，汎用性のあるものがいいでしょう．物理的意味との対応も考えたいです．ストロークの形，接続関係も役に立ちます．パターンマッチングできそうなもの，方向とか円弧はよく使われます．領域分割をして領域の重ね合わせなども考えられます．輪郭，細線，イメージ全体いずれを使うかは対象次第です．こういう形で入っています．これはやはり実際にやってみて，これは使えるかな，使えないかな，どのくらいうまくいくかなということでやっていくのであって，こう列挙されても使えるかどうかわかりません．

それからどの測度，指標が有効か？　妥当か？　羅列になりますが，飯島先生が提案した複合類似度．マハラノビス距離，線形判別関数，2次判別関数．固有値と固有ベクトルに基づく次元縮小での最良パラメータの決定．私はこれらをいろいろ検討しました．

どんな判定法が有効か？　階層的判定と単純判定，判定不能の採用．各段階での閾値の決定方式は，最大値，平均値，中央値，いずれの定数倍にするか？　私の場合は参照資料から辞書を求めておく．閾値を決めるためのテスト資料を少し用意しておいて，それらと辞書との距離を求め，その距離の最大値あるいは平均値，中央値，いろいろやってみて最もいい方法でやっています．正答率の推定値をどうするか？　参照標本からの代表の選択法をどうするか？　これらのことについてもいろいろ検討しています．

正答率の推定をどうするか？　leave-one-out 法や交差検証法があります．正答率を上げるための標本の大きさをどうするか？　正答率を推定する場合に，もともとデータがあるのですからいろいろと工夫しています．

以上，まとめておいた方が良いかなと思ったものを追加させていただきました．

次にこの図を紹介させていただきます．この図は署名照合の例としていろいろな本に紹介されています．当時画像処理の神様ともいわれた Rosenfeld，ご存じないでしょうか．ユダヤ系のアメリカに住んでいる先生なんですけども大変有名です．その先生のところで，Nagel という人が署名照合の研究をしましたが，そのとき用いた周辺分布の図です．1977年 IEEE の論文誌に載っています．この周辺分布はその後ずっと現在に至るまでいろいろな本に載せられています．

さて個人性情報というのは文字認識にも役に立ちます．たとえば次のような実験をしてみました．

この実験では，普段文字認識実験で用いるような沢山のデータではなく，筆者認識用に集めた7人のデータや11人のデータを用いておこなったのですが，うまいこと工夫して，それぞれの人の自分専用，自分を含む汎用，自分を含まない汎用，それから他人専用の辞書を，それぞれつくります．これらを用いて文字認識をやります．そうすると自分専用でやる方がはるかに良い結果を得ます．自分専用を使うと99．数%の認識率が得られる．それに対して他人専用，誰かのものを使って，クセ字のある人の認識をすると80%くらいになるということなので，もし文字認識をす

る場合でも個人性情報を利用するという考えを持つならば，その文字を書いた人の専用の辞書を使うといいですよということです．以上，個人性情報は文字認識に貢献できるということをここでお伝えしておきます．

次に我々が何気なく書いている文字．この図は「愛」の縦書きと横書きです．縦書きと横書きの文字というのは違うんだということ，おわかりでしょうか．私は実験をするまで知らなかったのですが，縦書きで書いた文字，横書きで書いた文字というのは字の形が違うんですよ．もう驚きましたね．それで縦書きの方がこう，皆さん自分の文字を縦書きと横書きで比べたことがあるでしょうか．違うんです．横書きは横に書いていきますね．横にずれていきます．どんどん縦長になってしまうんです．横書きは下にどんどん書いていきます．もともと日本の文字は縦書き文字です．ですからシュテムというんですけれども，シュテムというのはだいたい横線にあります．愛知県の愛という場合にはそこのところがよくでている文字ではないのですが.「愛知県名古屋市千種区不老町」という文章を用いて，縦書きの文字と横書きの文字を横書き同士，縦書き同士，相手のものを使うということで筆者識別実験をやると，正答率のパーセンテージが変わります．参照資料およびその数をどのようにするかによっても変わってきますけれども，もし縦書き同士でやると1字種単位の平均が90%くらいです．

これは全ての字種を使うともちろん100%になるのですが，縦書き同士でやると90%もあるのに対して，横書きだけだと88%．それと相手の違う筆記方法に関してやりますと74パーセントというようにかなり落ちてしまいます．これは参照資料の数が多いともうちょっと上がりますけど．今判定しようとする文字がどちらの方向で書かれた文字かということがわかっていたらそういうものを使った方が良いですよということです．それを顕著に棒グラフで表すとこういうふうになります．これは白い方が筆記条件が同じ場合，黒い斜線の入っている方が筆記条件の違うものでそれぞれ認識させた場合です．かなり違うんだということですね．だいたい実験条件っていうのはいつも横書きでやる．こんなふうに縦書きとか横書きというものを知って筆者認識をするということはあまりありません．両方使ってみると意外に違うんだなということがわかりました．ですからこれもひとつ知っておく必要があるかなと思います．

さて残された時間はあと10分くらいですけれども，私はこれまでいろんな研究をやってきました．1982年に主成分分析で手書き文字の個性を調べようと思って，その主成分が本当にその文字の個性を把握しているんだろうか，それをどうやって調べようかと考えました．それは私の研究の中でもなかなかいい研究だったんじゃないかなと思っていますので，その紹介をさせていただきます．

最初に，特性値は前にも，このように定義されていることをお話ししました．これらの特性値を使ってたとえばこういう文字があります．これは7人の人にひらがなを書いてもらったものです(図7)．繰り返し書かれた文字をこういうふうに並べたときに，縦が同じ人間の文字ですが．この中からいくつか取り

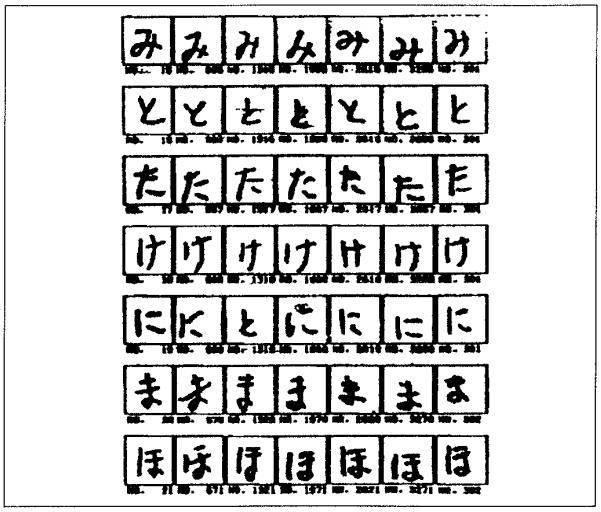


図7 7人の2値パターン

出してその人の個性を把握したいわけです．とにかく特徴量を約200個くらい取り出し，主成分分析をしました．それをたとえば多変量解析の表現，一般的に図表現というのはこんなふうに多角形で見るとか，あるいは折れ線グラフで見るとか，星の形にして見るとか，そこでどういうふうにとがっているかという形で，多変量の図表現をするのが一般的ではなかろうかと思います．いかがでしょうか社会系の先生方．あと顔の図をつくって，笑い顔になれば景気がいいだとかというこういうのになったら景気が悪いだとかというようにいろんな図表現を試みられております．

私の場合は文字から得た主成分ですから，文字的図形で表現できないだろうかと考えました．文字的図形というのは，たとえばひらがなの「か」を書くときにはこの図の1番から7番の点の場所がわかれば表現できます(図8)．この点の場所をどんな形で見つけるか．この見つけ方は少し複雑です．特徴点間の距離や傾きなどが利用できますが，もとの特性値（基本変数）にはストロークの始点，終点を決めるための情報が冗長に含まれています．文字的図形を書くための作図点の組は何組かあるのです．主成分はS個．何組かの作図点の中からグラフ理論のアイデアを用いてS個の主成分に寄与の大きいものを選びました．それを用いて文字的図形を書くのです．その文字的図形が先程お見せした，いっぱい書かれているあの形をしていれば，これはちゃんと個性を反映した主成分であるといえるわけです．

用いる作図用変数が具体的にきまれば，これを主成分からの推定値，観測値の平均値から求めます．それからそのストロークの作図．ストロークというのは書き始めから書き終わりまで湾曲がある場合と無い場合があります．作図をどうするか．2つの円弧で滑らかに接続させよう．ストロークの太さはどうしようか．それは0次のモーメントがありますから，それをストロークの長さの和で割れば太さを形式的にはこのように推定できます．結果としてこの作図法はうまくいったと思っています．

どういうふうになったか，その残された2～3分でちょっと結果をお見せします．先程の「か」，これは一番上のこの行は主成分から再構成したパターンです(図9)．これが書かれた2値パターンです．これは観測したときのまだ主成分に変換する前の平均値から構成したパターンです．これが，沢山の基本変数から高々6～7個の主成分を選んで再構成したパターンです．

また，これは上が2値パターンです．そして2番目が折れ線近似パターンです．3番目が観測値の平均値から再構成したパターンです．そしてこの赤いぽちのところが主成分だけから再構成したパターンです．もしそれを

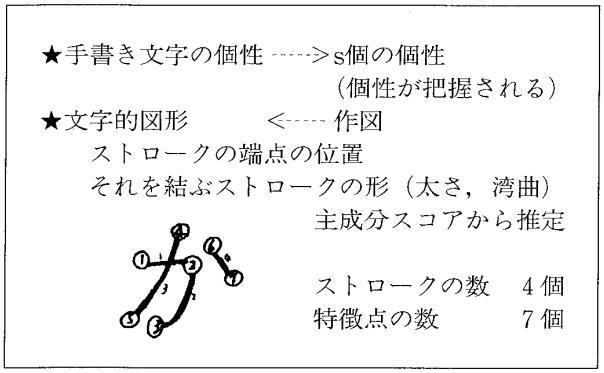


図8　文字的図形による表現

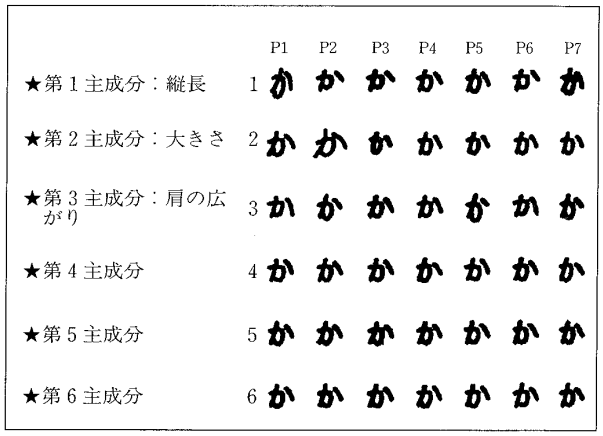


図9　主成分ごとに作図用変数を推定して再構成したパターン

主成分だけで多角形で見るとこんなパターンですね．それよりはるかにこの主成分は個性を反映しているという，そういうことがわかるような形ではないでしょうか．

これを紹介させていただいて，私の補足を終わらせていただきます．

司会：どうもありがとうございました．それでは質問・コメント等ございましたらお願いします．

山崎：札幌学院大学の山崎です．今の主成分分析を拝見して，たとえばペン習字ですとか，このポイントを守れば字の形がよくなるというような教育に応用できる気がしたのですけれども，そういう点についてはどのようにお考えですか．

吉村：これの応用ですか．目的は何にしましょうかね．というのはたぶんこれはいろいろとあるんですけれども，平均的なパターン，みんなが書いているような字を書かせたりとかそれによって変わってくると思います．個性的な文字というのは私は大切だと思っているんです．あまり曲げない方が良い．これは私個人の意見なので，どこをどうしたらあなたの字はこうなっていますよと見せるのには解析してあげるのはいいのだろうと思います．それをどういうふうに修正しかつ書かせるかということはまた教育のポリシーの問題ですね．何ともいえません．でも使えます．とにかく顔の再表現などにもこれは使えるのではないかと私は思っています．顔の場合には輪郭線をとっていきますね．こっからここまでは，ここととここの間とはじっことはじっこの間に上は何点とる，下は何点とる．これだけで主成分から再構成をすると口の形の個性を表現できます．目もそうです．最近目について同じようなことをやっている発表を聞いたもので，そうかこのごろまたこういうことも復活したんだなということで，一度どっかで言っておこうかなと思ったのです．

司会：それではもうおひと方くらいお願いします．

沖田：昨日の懇親会の席でもお話したのですけれども，先生の話を伺いますとどうも構造分析的立場からやってこられているような感じを受けるのですが．先程ちょっとテンプレートの話もあったのでお伺いしたいのですが，最近の脳研究によりますと，文字パターンなり，あるいは顔の認識なり非常に我々にとってファミリアな熟知した視覚イメージのパターン認識につきましては，先程のテンプレートマッチングですか，そうした全体的認識（holistic recognition）システムが部分依存的な認識系と対比したかたちで働いているようであります．たとえばトマトというひらがなで書くとなかなか認識しにくい．カタカナで書いた方が一瞬でわかります．そういうような全体像としてものを直感的にとらえる認識系が，筆跡鑑定というような時にも関わっているのではないでしょうか．だから世に言う筆跡鑑定家の域にまでコンピューター技術で追いかけていく場合に，もしコンピューターの方が追いつけない部分があったとしたら，人間らしい非常に筆跡鑑定家らしい，そういう全体的認識様式も取り入れてやっていく必要があるのではないかなという感想を受けるのですけれども．いかがでしょうか．

吉村：いくつかそこに問題点があるんじゃないかと思うんです．まず，私たちはトマトというのはいつもカタカナで見ています．私たちの頭の中にはどのようにトマトはイメージされているのでしょうか？　これはト・マ・ト．カタカナのイメージとして文字列が入っていますね．ですからひらがなよりはカタカナの方が良い．自分の頭の中にどういうテンプレートが用意されているかということで違ってくるのではないかと思います．それで私自身は構造情報で入ったのは，皆さんほとんどあのころは手書き文字が構造情報，活字はパターンマッチング．こういうふうに類別

していたのです．私もみんなと同じように，あるいは先輩たちのいろんなことが書かれているものを式に表現すると構造情報的になっていくということで入ったわけです．ところがそれらの特徴は取り出すのがとても大変なんです．安定した情報が取り出せないのです．それで時間もかかります．細線化してストロークの対応付けをするということはまた大変なことなんです．

最も安易なのはパターンマッチングです．今の顔情報だってたぶんパターンマッチングの方が楽でしょう．要素を取り出してあとはそこで濃淡情報のパターンマッチングをしていると思います．その方がずっと簡単なんです．簡単でなおかつ構造情報に比べてあまり見劣りしない結果が出るのではないかと思われます．ただ構造情報の良さは形を再現できることです．濃度情報ではできません．濃度情報の主成分での再現はちょっと思いつくことはできませんでした．とにかく構造情報は形を再現できる．これ以外ないと私は思っています．ですから目的が何であるかというときに，私たちが頭で考えているようなパターンマッチングが手書きに向かない，ということはなくて，それはそれなりにひとつの結果を与えます．ですから何ともいえません．これが変な結論で申し訳ありません．とにかく場合場合に応じて何を得たいのか，これによって考えていくしかないのではないかと思います．もちろんもっといい方法があったらいいのですが．それで昨日お話しした奥の細道の場合とか，この文書の中の文字はユニークだ，取り出して拡大していろいろと見ていこうなどと，場合によっていろいろな攻め方を考えるべきではないかと思います．答えにならなくてすみません．

司会：どうもありがとうございました．それではよろしいでしょうか．

中野：すいません，ひとつだけいいですか．大阪市立大の中野ですけれども，昨日聞き漏らしたものなんですけれども，今のお話の最後の部分の中でたとえば最近の私もそうなんですけれど，子どもたちというのは書き方を知らないですよね．筆順も知らないし，ここははねるというところもはねない．そういうのはこういう場合にはどういうふうになるのですか．

吉村：いわゆる子どもたちの書字教育ですね．書字教育というのは別のところでやりますよね．私は他のグループにも属していまして，ある時期，書字教育，要するにインターネットで文字板を使って文字を学習する．字の書き方を学習する．外国人が字を書く．こういうふうなプロジェクトに参加したことがあります．これはもう確実に採点方式にします．ここととここが合わなくてはだめよとか，あるいはこの書き順は絶対ここはこういうふうに書かなくてはだめよというふうに．チェックすべきところをきちっとおさえておく．それができなかったらだめ，ここができなかったらだめ．形の分離性と筆順のオーダーとそれからあとは，オンラインで示し合う．筆順を気にしないときには形だけ．いろいろな評価法を用意します．それで書字教育をします．形そのものはたくさんの人の文字を平均すると，平均パターンは平均的になかなかいい文字ができます．ですから平均文字から間違いを見ることでいいのではないかなと思います．

中野：最初のデータの場合には，要するにそういう間違いをした人のデータを入れないわけですね．

吉村：これはオンラインです．

中野：そういう意味で質問をしたのです．

吉村：オフラインです．オンラインの場合には入れてはいけません．

中野：たとえば〝か〟とか〝が〟とか間違う人はいないと思いますけれども，ちょっとした漢字ならだめになる．

吉村：それはもう筆順のオーダーで見るとあ

なただめ．そういう形で100点満点に対して5個の星を用意して，5つの星が全部ついたら100点満点．あとここがついたら筆順がだめだと．ここは書き方がだめと，ちょっとはねが足りないとか，はねが重要なところがあると書道の先生がいっていたので，ここも入れるとオンラインでは全部出ますから．そういうふうなことです．

中野：先生のデータの中にはそれを通った人のデータを使っているということですね．

吉村：もう一度お話しします．これはオフラインです．オフラインは通るもなにもない．できあがった形だけでやっているから．

中野：はねがあるなしも関係ない．

吉村：はい．私はこの文字がこういう形をしていなければならないと思ってはおりません．先程いったように署名というのは名前を表さなくてもいいのです．私のサインよと，これで登録しておけばいいのです．だからある人がひらがなの「か」というのを普通の人のように書かなければ，それはそれでその人の「か」なんです．いいですか．それでここでお話ししなかったのですが，2～3人だけのものを参照資料として使うときでも，安定した推定ができます．他の人間の文字データも取り込んで併合分散共分散行列をつくります．そして分散の推定をして平均だけが違うという形を取ります．他の字種も入れてしまいます．そしてそのたとえばその人の変な文字があったら，それは著しく違うところなのですが，いわゆる分散共分散行列の主成分の向きはみんなのものでまとめて使ってしまうわけです．数が少ないよりははるかにその方が推定能力があると私は思っております．これは長い間の実験結果から得たものです．だからそれで個人専用の文字認識の辞書を作るという考えがあったんです．私は書道屋ではないので，まったく無責任に本来その人の個性的な文字がよろしいという立場からそういう話をしました．

司会：先生，どうもありがとうございました．