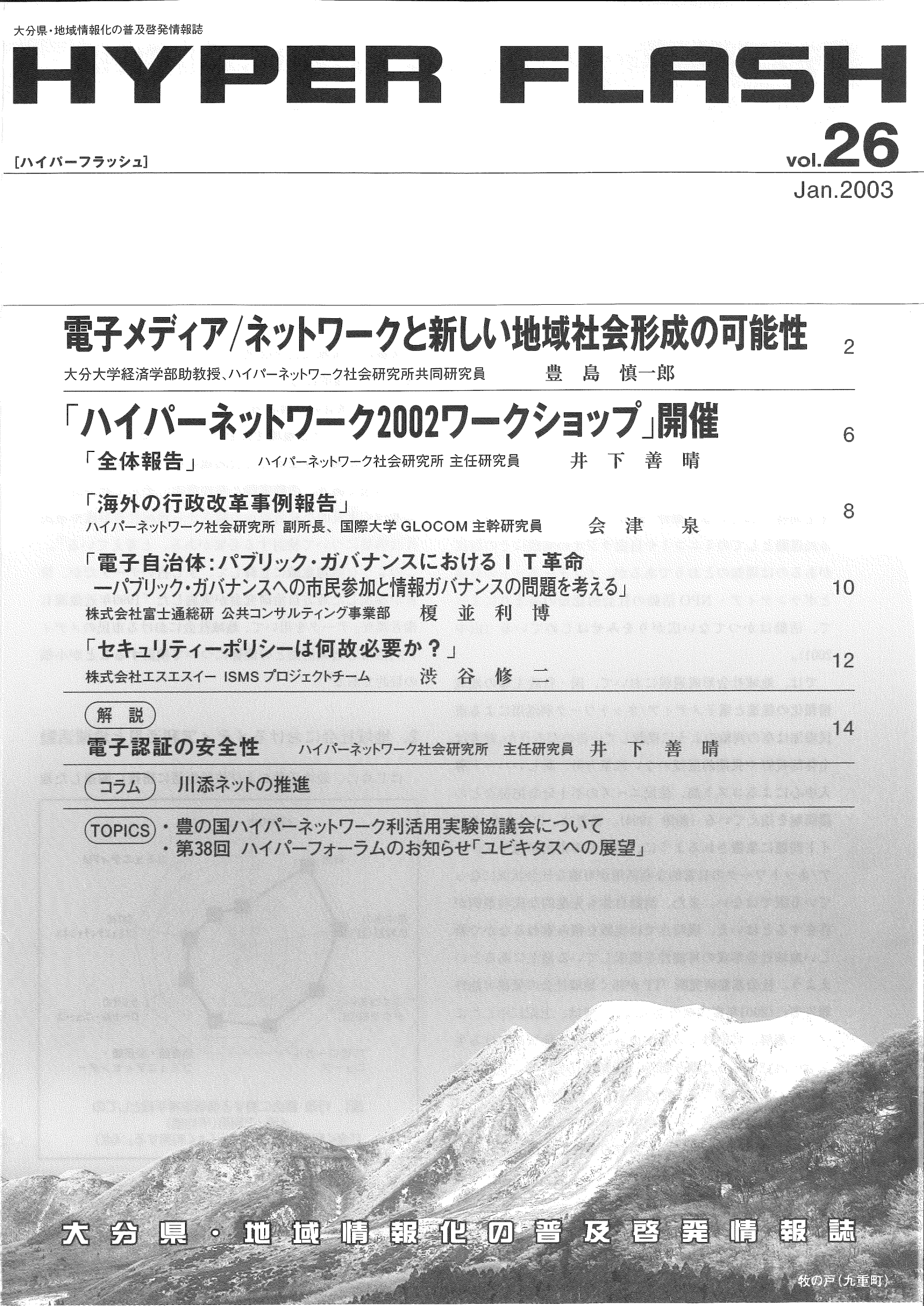
大分県・地域情報化の普及啓発情報誌

HYPER FLASH

[ハイパーフラッシュ]

vol.26

Jan.2003



牧の戸（九重町）

電子メディア/ネットワークと新しい地域社会形成の可能性

大分大学経済学部助教授
ハイパーネットワーク社会研究所　共同研究員　豊　島　慎一郎

1. はじめに

現在、地方自治体は、政府主導による情報化推進政策と呼応して、地域活性化や地域問題の解決、コミュニティ形成などを目的として情報通信基盤の整備・充実を急速に進めている。その一方で、地域社会の危機や崩壊が叫ばれているなか、情報ボランティアや情報化支援NPO、シニアネット、パブリック・アクセスといった「電子メディア/ネットワークを利活用した市民活動」が新しいタイプの地域社会形成（まち（むら）づくり）の実践としてその展開の可能性を期待されている（細野 2000)[1)]。こうした取り組みは、市民運動としてのミニコミや自由ラジオの実践にその源流があるのは周知のとおりであるが、インターネットの登場とボランティア・NPO活動の社会的認知の高まりによって、活動はかつてない広がりをみせはじめている（山中 2001)。

では、地域社会形成過程において、国・行政主導の地域情報化の推進と電子メディア/ネットワーク利活用による市民参加は車の両輪のように機能しているのだろうか。前者は、全体的視野や長期的展望のない政策方針、新しいハード導入中心によるコスト高、住民ニーズの不十分な把握などの諸問題を抱えている（船津 1994)。後者は、デジタル・デバイド問題に象徴されるように、すべての市民が電子メディア/ネットワークの日常的な利活用が可能な社会状況になっている訳ではない。また、活動自体も先進的な成功事例が存在するとはいえ、現時点では実践を積み重ねるなかで新しい地域社会形成の可能性を模索している途上にあるといえよう。社会基盤研究所『ITが拓く地域社会の発展可能性報告書』（2001年度内閣府委嘱調査）では、上記に示したような課題解決に向けての基本提言として「地域における生活者の視点に立った取り組みの必要性」、「地域ニーズの内容に応じた効果的なIT化の推進」、「地域社会に主体的に参加する意識の尊重」、「地域コミュニティの重視と新しいコミュニティへの対応」、「生活者の多様な生活スタイルへの対応」、「産官学民のパートナーシップの推進」、「人材の育成」、「誰でもが情報へのアクセシビリティを高められる環境の確保」をあげている。これらの提言はいわば現実の裏返しであり、「上からの情報化」と「下からの情報化」との架橋は、地域社会形成過程において十分に展開されていないことを端的にあらわしている。

ここで、筆者の立場を明らかにしておきたい。電子メディア/ネットワークと地域社会を繋ぐのは、身の丈レベルで他者や社会に関わりながら社会問題の解決を志すひとりひとりの市民であり、活動実践と参加意志、そして社会的連帯に基づく実質的な社会参加の観点から地域社会形成や市民社会構築について検討する必要がある、と考えている[2)]。このような問題意識に立脚して、少し古いデータだが、筆者が参加した地方自治研究会が実施した「1999年近畿圏有権者調査」データを用いて、地域社会における市民のメディア利活用と地域活動との関係について検討することが小稿の目的である[3)]。

2. 地域社会におけるメディア利活用と地域活動

はじめに、地域活動および住民生活に密接に関連した地

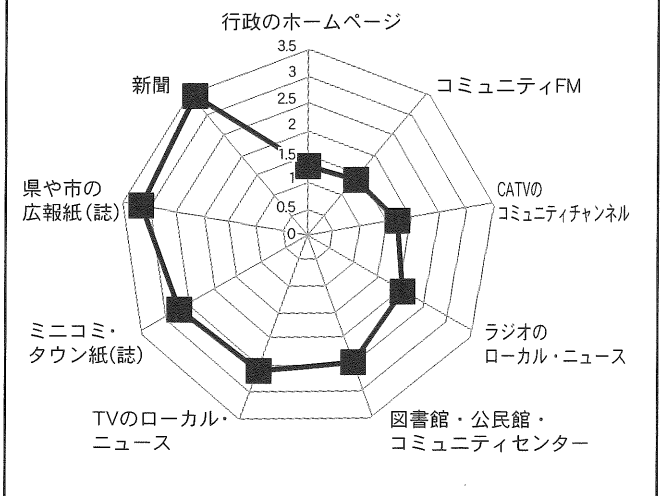


図1　行政・議会に関する情報取得手段としてのメディア利用（平均値）
（「全く利用しない」:1点～「よく利用する」:4点）

域情報のひとつである「市町村行政や議会の動向に関する情報」を知る手段として、人びとはどのようなメディアをどの程度利活用しているのかをみてみよう。

図1は、人びとの行政・議会情報の取得行動についてメディア別に利活用頻度の平均を示したものである。相対的に数値が高い傾向にあったメディアは、新聞、市町村の広報誌、ミニコミ誌といった「紙媒体」=「オールドメディア」である。つづいて、TV・ラジオといったマス・メディアと図書館や公民館、コミュニティセンターといったスペース・メディアが情報源として比較的利活用されている。そして、ほとんど利活用されなかったメディアは、ケーブルテレビ（CATV）、コミュニティFM、インターネットという、かつて「ニューメディア」とよばれ、地域情報化政策において重要な役割を担うことを期待された電子メディア/ネットワークであった。このことから、新しい電子メディア/ネットワークが地域のコミュニケーション回路として十分に機能していないことがみてとれる。これと共通する傾向は、現在、筆者が分析作業中の「大分市市民福祉意識調査」（2002年10月実施）の結果においても確認されている[4]。福祉保健関連の行政サービス情報の取得手段として、市報（約35%）、新聞（約23%）、TV・ラジオ（約18%）の順で利活用率が高い一方、インターネットは1.3%という非常に低い利活用率が示された。

つぎに、地域情報に関するメディア利活用と地域活動への参加および意識との関連を検討する[5]。表1に示されているように、地域活動参加行動と地域社会形成への参加意識について地域情報に関するメディア利活用との間に正の関連（一方の値が大きくなれば、他方の値も大きくなるという関係）がみられる[6]。これは、地域活動への参加経験が多い人であればあるほど、また、まち（むら）づくりに対する参加意識が高い人であればあるほど、地域情報の取得手段としてメディアを利活用する頻度が高い傾向にあることを意味する。この点から、地域情報取得行動は、地域社会形成への実質的参加と関係していることが確認された。

表1 地域情報に関するメディア利活用と地域活動・参加意識との関係

	相関係数	有意確率
地域活動参加行動	0.28	0.00
地域社会形成への参加意識	0.26	0.00

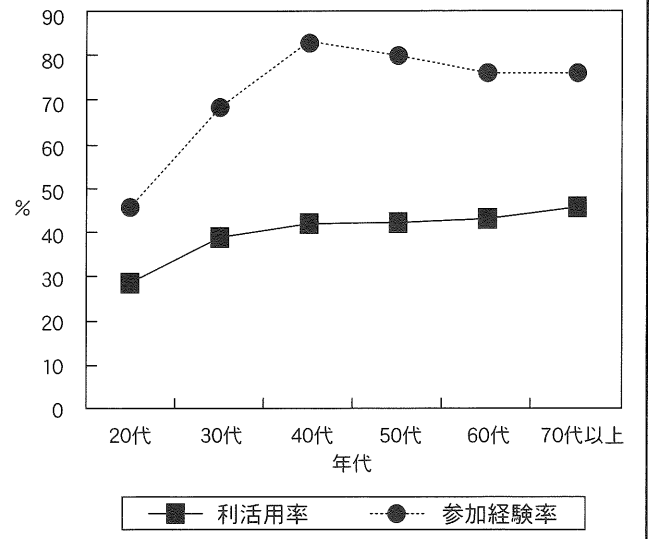


図2 地域情報に関するメディア利活用と地域活動参加

最後に、年代別に地域情報に関するメディア利活用と地域活動参加をみてみると、20代の利活用率と参加経験率の低さが顕著にあらわれている（図2）。この傾向は、若年層の地域政治への無関心や地域活動に対する消極的傾向といった「地域離れ」現象に関する従来の知見と符号する。

3. おわりに

以上、ごく簡単ではあったが、地域社会における電子メディア/ネットワークの利活用と地域活動の関係を検討した。その結果、オールドメディア利活用中心の地域情報取得行動、地域情報に関するメディア利活用と地域活動参加との関連、そして若年層の地域情報取得行動および地域活動参加への消極性が明らかとなった。とくに、1番目の知見は、地域情

報取得行動は依然として行政と既存のメディアの影響下にあり、市民によるアクセスと参加が比較的可能な新しい電子メディア/ネットワークは、地域社会形成過程においてその「力」を十分に発揮できていないことを示唆している。この点をより明確に示すためには、市民が地域情報を生みだす主体としてメディアをいかに利活用しているのか、あるいは利活用していないのかを実証的に捉える必要があるだろう。

地域社会が直面する諸問題の解決に向けて、市民間、ないしは行政との協働を可能にし、かつ人びとの思いや志を実現させる市民力を醸成する「地域のコミュニケーション・ツール」として電子メディア/ネットワークを生かすのは、地域社会形成に主体的に参加する市民である。このような視点に基づいて、ひとりひとりが日常生活のなかで従来の市民とメディア、市民と行政との関係を問い直しながら、新しい地域社会形成の可能性について考えることが最も重要である、と筆者は考えている。

【注】

1) ハイパーネットワーク社会研究所の取り組みを例にあげると、ハイパーネットワーク2001別府湾会議（2001年11月開催）の分科会「ネットを活用した市民活動」、ハイパーネットワーク2002ワークショップ(2002年12月開催)の分科会「地域コミュニティの未来とIT活用」では、市民や行政関係者、研究者の間で情報ネットワークを基盤とした市民社会構築の可能性について活発に議論された。前者の内容については、拙稿（2002）を参照されたい。

2) 社会参加と市民社会構築に関する筆者の基本的な考え方については、拙稿（2000）を参照されたい。

3) 1999年地方自治研究会有権者調査は、近畿圏の満20歳以上の男女有権者から確率比例抽出法によって5,400人を調査対象者として郵送法で実施された。有効回答者数は1,533人（有効回収率は28.4%）であった。なお、この調査は、1998年に文部省（現 文部科学省）科学研究費の補助を受けている（基盤研究(A)(1)「地域社会における政治構造と政治文化の総合研究：近畿圏を中心として」(1998～2001年度) 研究代表者：青木康容 佛教大学教授)。

4) 調査結果については、2003年5月に調査報告書として公開される予定になっている。

5) 使用した指標は、以下のように作成した。

地域活動参加：「地区の公園や公民館などの住民管理」、「地域の運動会・お祭りの準備や世話」、「自然保護・農林業支援の市民活動」、「審議会委員などの自治体の計画づくり」、「行政が呼びかけたお年寄りの介護や給食サービスの手伝い」、「再開発や施設整備についての住民同士の話し合いや作業」、「障害者の手助けや手話・点訳などの団体やサークル活動」、「行政のおこなうごみ減量やリサイクルの取り組み」という8項目について、参加経験があれば1点、参加経験がなければ0点を与えて、全項目を単純加算したものである。

地域社会形成への参加意識：「まち（むら）づくりについての会合には、すすんで出席して積極的に発言したい」という意識について尋ねた項目（「全く思わない」1点～「そう思う」5点）を使用した。

地域情報に関するメディア利活用：「図書館・公民館・コミュニティセンター」、「TVのローカル・ニュース」、「ラジオのローカル・ニュース」、「新聞」、「ミニコミ紙（誌）やタウン紙（誌）」、「県や市の広報紙(誌)」、「ケーブルテレビの地域(コミュニティ)チャンネル」、「コミュニティFM」、「インターネットの行政のホームページ」という9項目それぞれについて、単純平均を算出して作成した（「全く利用しない」1点～「よく利用する」4点)。

6) 相関係数（Pearsonの積率相関係数）は、2つの事象（変数）間の関連を双方向的に捉えて、関連の強さを測定する指標である。この相関係数は、1.0から－1.0の値をとり、絶対値が大きいほど強い関連をあらわす。

【文献】

藤本昌代、2001、「地域情報化と地域アイデンティティ」地方自治研究会『地域社会の政治構造と政治文化の総合研究』1998-2001年度科学研究費補助金研究成果報告書、佛教大学、94-104。

船津衛、1994、『地域情報と地域メディア』恒星社厚生閣。

細野助博、2000、『スマートコミュニティ』中央大学出版部。

豊島慎一郎、2000、「新しい市民像 社会的活動」高坂健次編『日本の階層システム第6巻 階層社会から新しい市民社会へ』東京大学出版会、143-159。

豊島慎一郎、2002、「参加する市民が繋ぐ〈電子ネットワーク〉と〈地域社会〉」『ハイパーネットワーク2001別府湾会議報告書』ハイパーネットワーク社会研究所、130-137。

山中速人、2001、「市民力としての情報メディア—市民的活動と情報技術—」立木茂雄編著『ボランティアと市民社会〔増補版〕—公共性は市民が紡ぎだす—』晃洋書房、175-193。

コラム

川添ネットの推進

川添ネット提唱者　椎　原　　功

私の住んでいる川添地区は大分市の東部にあり人口は大分市の約1.6%、7300人で大分市のベッドタウンとして発展しています。ここでも高齢化が進んでおり各種文化活動が活発に行われてはいるものの、新しい社会への対応やいろいろな課題を地区民が話し合う場がないという悩みがあります。

私は昨年あるインターネットグループの会員になり、勉強会に参加しました。そこでは連絡やデータ交換に電子メールが活用されており、これがコミュニケーションの有効な手段であることを実感しました。

この勉強会は(財)ハイパーネットワーク社会研究所の支援で行われているものですが、そのほかにも時代の最先端の情報を入手することが可能です。昨年12月に研究所が主催したワークショップの「地域コミュニティーの未来とＩＴ活用分科会」では国内外からのNPO活動家とも親しく交流し、地方にいてはなかなか聞くことの出来ない時代の流れを肌で感ずることができました。

私はここで得た成果は、わが川添地区の発展に必ずや生かすことが出来ると確信し、地元の公民館長や自治会役員に会議の状況を説明したところ快諾が得られたので「川添ネット企画書」をまとめ推進することになりました。

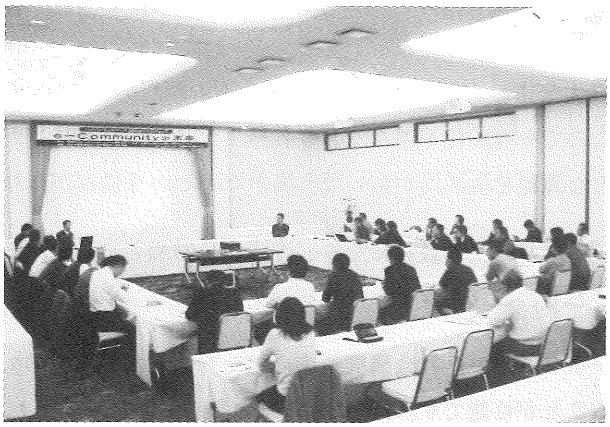
まず住民の意識調査を行い地区の全家庭2,300世帯にパソコン勉強会のアンケート調査を行ったところ約80名の受講生、講師希望者（コアボランティア）が集まり、第１回川添ネット連絡会で今後の進め方等を打ち合わせた結果、本年１月より川添公民館研修室で勉強会がスタートすることになりました。講師陣は校長、高等学校教師、情報システムメーカーの部長等顔ぶれも多彩であり、これなら成功させられるという確信をもちました。

川添ネットは「地域に立脚した市民のハイパーネットワーク社会実現」の具体例として情報を発信し、国内外の地域と交流しながら良き先例となれるよう推進して行きたいと考えています．インターネット社会は私たちにとって未経験の分野であり、この意味で(財)ハイパーネットワーク社会研究所と密接に連携して進めてゆきたいと考えております。

「川添ネット」説明会の様子（2003年１月19日川添公民館ホールにて）

ハイパーネットワーク2002ワークショップ開催全体報告

ハイパーネットワーク社会研究所　主任研究員 井　下　善　晴



ハイパーネットワーク2002ワークショップが2002年12月5日（木）から2日間に渡って、国東町のいこいの村国東にて開催された。前回のワークショップは2001年3月に「ファーストマイル・ブロードバンド」と題し、福岡市百道のソフトリサーチパークで開催されたが、それから約2年、“ブロードバンド”という言葉も当たり前になり、ネットワークと私たちの関わり方も大きな変化を遂げた。このようなネットワークともはや無縁ではいられない社会をe-Communityということができるならば、その未来を考えることは重要である。そこで今回は「e-Communityの未来」と題し、あらためて“ハイパーネットワーク社会”の現状と未来を見つめ直す場としてのワークショップが開催され、あらゆる方面から多くの人が国東町に集まった。

ここで、今回参加された方には議論の再確認と新たな問題提起のきっかけとして、参加できなかった方にはワークショップの様子や議論の中身をお伝えするために簡単に報告をまとめる。

セッション1「海外の行政改革事例」

セッション1では最初に韓国ソウル特別市の市政改革団（市政改革を推進している部署）の申相詰（Shin Shang Chur）氏よりOPENシステム（注1）について報告された。

OPENシステムとは“許認可処理オンライン公開システム”のことであり、行政の許認可処理の状況をリアルタイムに情報公開するシステムである。開発の背景としては日本の電子自治体と大体同じであるが1つだけ違うのが「公務員の腐敗防止」が第1の目的として明記されていることである。日本ではなかなかこういうことは公言できない。驚くべきことにOPENシステムの開発はわずか10週間の期間と4200万円の予算で実現できたということである。日本ではまず不可能と思える開発コストだが、見習うべきことは多いだろう。システムの機能や運営状況について実際の画面を例に詳しい説明が“日本語で”行われた。

次にフランスのNPOであるVECAMで代表を務めるバレリー・プジョー氏（Velerie Peugeot）よりVECAMでの自身の活動や考え方についての報告があった。

VECAMでは多様な国際的活動を行っているが、特に地方自治体のIT施策や地域ネットワークコミュニティ形成への取り組みに積極的である。フランスの自治体は人口6000万人に対し3万6000もあるということで、それだけでも日本とは大きな文化、制度の違いがあることが容易に想像できる。フランスの行政はICT（注2）普及に積極的に取り組んでいるようであり、一応の成功を収めているようである。ただフランスでは地方民主主義が重要視されており、いかにこの地方民主主義にICTが貢献できるかが今の課題ということであった。また自治体の電子化については日本と同様に行政組織改革や情報格差などが課題として取り上げられているとの報告があった。

セッション2「自治体の情報化推進・CIO」

e-Communityを考える上で、地域や住民に最も身近な地方自治体の情報化（電子自治体）の推進状況が実際に自治体で情報化推進にたずさわっておられる長崎県庁の島村秀世氏（総務部参事監）と大阪府羽曳野市の戸谷壽夫氏（秘書室理事）より報告された。

まず島村氏より長崎県の情報化についての指針がいくつか紹介された。行政の効率化は個々の業務で考えるのではなく組織全体で考えなければ効果が出ないということや、効率化のためのコストをいかに抑えるかについて長崎県の独自の基本思想を策定されているようであった。地場企業の育成やフリーソフトの活用などについて大胆な施策を推進されているようであり、今後の長崎県の電子県庁化はおおいに注目される。

次に戸谷氏より羽曳野市がこれまで実施してきた行政の情報化に関する事例紹介と今後の課題について報告された。羽曳野市は証明書自動交付機の設置や住民サービスのため

（注1）
Online Procedures ENhancement for civil applications

（注2）
最近ではIT(Information Technology)をさらに拡げICT(Information Communication Technoloy)という言葉がよく使われるようになった。
プジョー氏も発表の中ではICTという言葉を使った。

のカード発行などで先進的な取り組みを既に実践しているが、今後は市民の視点に立った一層の利便性向上を目指し、官民一体のサービス実現に努力されていることが報告された。また“自治体バーチャル合併”という新しい考え方も提示された。セキュリティ確保など課題も多いようであるが、羽曳野市の“市民の視点に立った”しっかりとしたポリシーが感じ取れた。

セッション3「情報ガバナンス・ＩＳＭ」

セッション3ではそれまでのセッションでの事例報告を受け、ではこれから何が必要なのか、という観点での報告がなされた。

まずは著書「自治体のＩＴ革命」で有名な富士通総研（株）の榎並利博氏より自治体と市民の関係をパブリック・ガバナンスという新しい言葉で表現しながらこれからの自治体のあるべき方向性や行政への市民参加のあり方について提言がなされた。さらに行政だけではなく立法（議会）や司法のＩＴ化や市民参加についても言及があり、幅広い分野を視野に入れた興味深い話であった。

次にエス・エス・イー（株）の渋谷修二氏より「セキュリティ・ポリシーは何故必要か？」と題し、セキュリティ・ポリシーの必要性を逆説的に訴える報告がなされた。最近では個人情報保護などセキュリティに関する話題もマスコミで数多く報道されるようになってきた。現在の情報化社会で見落とされがちな情報ガバナンス（注3）の確立に不可欠なセキュリティ・ポリシーについて短い時間ではあったが、実例の紹介を交えながらの説明があった。セキュリティ・ポリシーの考え方や策定自体は難しいものでなく、極論すれば「当たり前」のことをきちんとやる、というだけのことであるが、実際の世の中では当たり前のことが実はなかなかできていないということが、あらためてセキュリティ・ポリシーに取り組むことの重要性を感じさせるものであった。

セッション4「e-Communityを支える技術」

セッション3の終了後、交流会を挟んでセッション4が行われた。セッションの前半はアソシエント・テクノロジー（株）のスティーブン・ヴェルテマ（Steven Veltema）氏から「ワールド・バーチャル・フォーラム（World Virtual Forum）」の紹介が行われた。ワールド・バーチャル・フォーラムは8カ国語翻訳機能を備えたWeb上での電子会議システムで、2003年3月に京都で開催される「第3回世界水フォーラム（注4）」で使用される予定である。実演を交えたプレゼンテーションで大変分かり易いものであった。今後、このようなバーチャル会議システムが普及していけばネットワーク（インターネット）が時間と地域の制約を克服してきたように、「言語の壁」も近い将来に取り除かれる可能性も大きいと思われる。

セッションの後半はソリトン・システムズの中村雄彦氏と嶋田政貴氏によるセキュリティに関するプレゼンテーションが行われた。両氏は普段、主に企業のセキュリティを守る仕事をされている関係で、攻撃する側の手口も熟知されている。今回はハッカーなどがどのような手段でネットワークに侵入してくるのか、デモを交えて報告があった。遠隔地にある、本来は操作できないはずのwebサーバをカンタンに操作してしまう、というデモには夜のセッションだったにも関わらず、大勢の参加者が熱心に見入っていた。

このあと、いこいの村に宿泊した参加者は夜なべ談義で夜遅くまで自由な議論で盛り上がった。

セッション5（分科会）「e-Communityガバナンスの形成」

2日めの午前は3つのグループに別れてそれぞれのテーマで分科会を行った。テーマは「セキュリティ・ポリシー作成の実際（コーディネーターは渋谷氏）」、「地域コミュニティの未来とＩＴ活用（同、豊島氏（大分大学）、武本氏（ハイパー研））」、「パブリックガバナンス（同、榎並氏）」であった。

セッション6「まとめ」

各分科会の報告の後、午後からはe-Communityに何を期待しているのか、何が問題なのかについて全員参加で議論を行った。それぞれが地域でコミュニティの活性化、ＩＴの活用に積極的に取り組んでいる様子が報告されると共に、このワークショップを主催したハイパーネットワーク社会研究所に対する期待や要望も数多く発言された。

地方ではインフラ整備さえまだ不充分であることや、情報格差の問題も取り上げられた。ファーストマイル問題と人材育成の重要性があらためて認識されたようである。

（注3）
ガバナンス（governance）：直訳すると統治。外部から監視する仕組みや、どのように運営するかといった意味合いも含まれる場合も多い。

（注4）
The 3rd World Water Forum: http://www.worldwaterforum.org/jpn

海外の行政改革事例報告（セッション1より）

ハイパーネットワーク社会研究所副所長、国際大学GLOCOM主幹研究員 会津　泉

セッション1のコーディネータ会津（筆者）

セッション1　まとめ

このセッションでは、海外から二人のスピーカーを招き、韓国とフランスの地域に根ざした事例を紹介してもらうことで、日本との比較対照を試みた。

まず韓国ソウル特別市の申相喆（Shin Shang Chul）氏から、ソウル市の電子自治体について報告を受けた。ご承知のように韓国は1997年の経済危機の最中からインターネットの爆発的普及が始まり、2000年以降はADSLおよびケーブルモデムによるブロードバンドの驚異的な普及へとつながり、現在では国民の約7割、1000万世帯がブロードバンドを利用する、「世界一のブロードバンド国家」である。

その韓国で、市民を対象に行政がどのような電子サービスを提供しているのか、日本で実態を知る機会は少ない。今回ソウル市を招くことができたきっかけは、OECD（経済開発協力機構）が刊行した『Citizens as Partners』（パートナーとしての市民）という本にOPENという自治体ネットの事例報告が紹介されていたおかげだった。

ネットで検索したところ、このOPENについての日本語の翻訳資料が見つかった。自治体国際化協会が出した「韓国自治体のIT施策」という報告書で、以下のURLから無料でダウンロードできる。

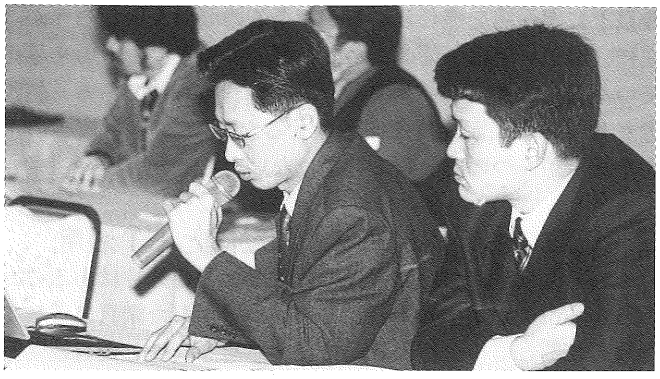
（www.clair.nippon-net.ne.jp/HTML_J/FORUM/C_REPORT/CRNUM.HTM）

この報告書は、自治体国際化協会ソウル事務所に出向した静岡県職員の澤井亨さんという方が独自にまとめたもので、OPENをはじめ電子納税制度などを含む韓国自治体の電子業務の全般を、中央政府と各自治体の事例報告を含めて包括的に紹介した力作だ。今回発表いただいた申相喆さんも澤井さんに紹介していただいた。

申さんのプレゼンは、まずソウル市が電子自治体にどう取り組んでいるかをわかりやすく、イメージ風に描いたビデオから始まった。日本語のナレーションがついている本格的なものだ。その後、OPENの内容を説明されたが、彼の所属は「市政改革団」で、OPENの目的は「公務員の腐敗防止」が第一だというところが、強いインパクトを与えた。

このシステムは金泳三政権で首相を務め、その後ソウル市長となった高建（コ・ゴン）氏が積極推進し、その後市長は昨年6月の選挙で交代したが、基本方向は変わっていない。高氏は盧武鉉新大統領によって首相に指名される予定だ。ソウル市のホームページには、現在も「腐敗防止」として、「市政の透明性を高め、腐敗が予防できる一歩進んだ腐敗防止対策として、民願処理オンライン公開システムを開発・運営している。この制度は、市民生活と密接に関連がある業務の処理過程をインターネットを通じて市民に公開することにより市民の知る権利を満たし、不正を事前に予防して行政の透明性に寄与している」と日本語で記されている。

この「民願システム」は、インターネット経由で、たとえば労働組合設立申告、水道の名義変更・料金納付証明、婦女保護所の収容証明、河川の占用許可延長、土地利用計画確認書、土地台帳など様々な種類の申請ができる。特徴的なのは、市民が申請した案件がどう処理されているかを追跡できることで、それも自分の行った申請に加えて第三者が申請したものまで公開されるという、徹底した透明性が追求されている。ただし、プライバシーへの配慮から、すべての申請が公開されているわけではなく、



セッション 1 講師
リー・ヤンソン氏（韓国ソウル特別市市政改革団団長）：右
シン・サンチュル氏（同チーム長）：左

セッション 1 講師
バレリー・プジョー氏（フランス VECAM 代表）

あくまで問題の少ないものが選ばれているという。

なお、開発のスピードも特記すべきで、わずか10週間だったという。申さんによると、「細かい検討を徒に重ねるより、とにかく動かして、必要な改良は稼動させた後で行う」という考え方で進めたという。このあたりにいまの韓国人の気質がよく現れているように思える。

フランスのプジョーさんは、中央集権主義が強いフランスの自治体の ICT （情報通信技術）利用を推進する非営利組織、 VECAM の責任者である。プジョーさんは、パルトネという人口1万2千人という小さな自治体での ICT 取り組みが先駆者となったことを紹介しつつ、フランス全体で約3万6千ある自治体のうち独自ドメインをもつ自治体が4千、ウェブサイトがあるのは2千、一貫した ICT 政策が確立されているのはまだ5百と、フランスの自治体の情報化への取り組みが必ずしも順調ではないとまず報告した。

彼女がとくに強調したのは、ネットへの平等なアクセスで、女性、老人、農村、失業青年などの社会的に支援を必要とする人々へのプログラムの推進に取り組んできた。しかし、選挙で社会党が敗北した結果、大統領も首相も保守党が占め、こうした路線も変更を迫られている。

それでも、市民参加を基本とする地方民主主義の推進のために、情報化による情報公開の推進、透明性の向上が取り組まれ、非営利団体がこれに参加している。オープンソースソフトの開発・提供、とくに投票システムの開発が進められているという話は参加者の間から関心を呼んだ。

VECAM は、フランス国内のネット利用を推進するための NPO だが、ヨーロッパのコミュニティネットの会合を積極的に支え、さらにカナダ、オーストラリア、アルゼンチンなどグローバルなコミュニティネット運動の主要メンバーでもある。プジョーさんはその中心で、沖縄サミットの際につくられた、 G8によるデジタルデバイド解消のためのタスクフォースである、 DOT フォースにも参加した。

彼女の報告からは、フランスのコミュニティネットの運動は、「民主主義」「平等」といった価値観に強く支えられていることがよく伝わってきた。韓国も含め、地域での情報化の進展状況は、その社会の実態をよく反映すると参加者一同あらためて実感した。

「電子自治体：パブリック・ガバナンスにおけるIT革命
—パブリック・ガバナンスへの市民参加と情報ガバナンスの問題を考える」(セッション3より)

株式会社富士通総研 公共コンサルティング事業部 **榎 並 利 博**

1．はじめに


榎並利博さん、セッション3講演の様子

e－Japan戦略推進の下、今や各自治体は電子自治体の取組みに余念がない。2005年におけるＩＴ最先端国家を目指して、2003年度中に国家の電子行政情報基盤を構築しなければならないのである。それと同時にＩＴ講習会の実施など、国民の情報リテラシーを向上するという役割も自治体は果たしている。このようにＩＴの活用が行政効率を向上させ、ＩＴを基盤として生まれてくる新たなサービスやビジネスが社会経済を活性化させ、市民生活は今まで以上に豊かになっていくだろう。しかし、そのような効率性や経済的な観点だけで理解して良いのだろうか。市民の幸福感とは一体何なのか、市民の幸福感を増大させるためにＩＴを役立てることはできないのか。このような問題意識から行政・立法・司法というパブリック・ガバナンス、および情報のガバナンスについて考えてみたい。

2．市民の幸福とは

チューリヒ大学のフレイとシュツッツァーが、市民の幸福感と経済や行政制度との関係について研究した面白い論文[1]がある。二人は経済学者であるが、この論文の面白いところはスイスの26州において直接民主主義の度合い（すなわち、行政への参加のしやすさ）がすべて異なっていることを利用し、市民の幸福感と直接民主主義の度合いとに相関関係があることを統計学的に実証したところにある。

その結論として、「直接行政や政治へ参加できる制度や地方分権が整っている州ほど、市民はより多くの幸福感を感じている。」、「外国人であっても行政活動の結果からはスイス人と同じ恩恵を受けている。しかし、行政の意思決定プロセス自体からは排除されているため、直接民主主義の度合いがかなり高い州であっても、外国人は幸福感を得られていない。」ということが明らかにされたのである。

すなわち、ある程度成熟している社会においては「行政への参加」ということと「幸福感」というものが大きな相関関係を持つということが示されたのである。とすれば、ＩＴを活用して市民の行政参加度を上げていけば、市民が今以上に幸福感を感じることができるのではないだろうか。逆に、厳しい財政事情のなかで納税者の要求するものを与えていく従来のようなバラマキ行政はもう不可能である。納税者としての市民満足度を向上させるためには、「行政への市民参加」が一つの鍵となるのではないだろうか。

1 "HAPPINESS, ECONOMY AND INSTITUTIONS" (Bruno S. Frey and Alois Stutzer、University of Zurich,"The Economic Journal",2000年10月)

3．行政における市民参加の動向とＩＴ活用

それでは日本において市民の行政参加の必然性はあるのだろうか。市民が選出した首長と市民が選出した議員によって行政の統制と監視は行われ、市民の意思を反映した行政活動が実行される。この代議制民主主義の仕組みに歪みが生じているという事実がある。

2000年10月、長野県で大きな事件が起こった。40年間以上副知事が知事を務めるという異常な慣習を破り、県民の支持を受けて田中知事が誕生したのである。しかし、首長に対して公然と反旗を翻す行政幹部、首長に不信任を突き付けた議会、という具合に従来の構造を変えるために民主的な手続きで県民が選んだ知事を愚弄するガバナンス構造が暴露されたのである。住民投票も96年の巻町を皮切りにかつてないほどの勢いで広がっていった。首長や議会の意思と市民の意思の間に大きな乖離現象が起こっていたのである。吉野川可動堰問題は単に迷惑施設の問題ではないことを示す良い例だろう。空港建設問題など、公共事業の是非をめぐっての動きが活発になっている。

行政側としてもこのような市民の動きに対応して、市民を取りこむ努力をし始めた。北海道ニセコ町では、まちづくりの基本原則として「情報の共有」、「情報への権利」、「説明責任」、「参加原則」を掲げた「まちづくり基本条例」を制定した。「情報共有」と「住民参加」を柱として、行政と市民がともに責任をもって「自ら考え、自ら行動する」まちを目指している。また、最近ではアンケート調査やワークショップの開催など、パブリック・インボルブメントの手法を使って計画段階から市民を巻き込むというやり方も多くなってきた。従来型公共事業に対する市民の不信感や長期的な経済低迷による市民の重税感を行政側も無視できなくなっている。

このように、計画・執行・評価という行政活動の各段階においてＩＴを活用した市民参加手法を実践していくことは、市民が行政に参加する機会を増やし、市民の意思がより反映された行政活動を保証することになるとともに、市民の幸福感を増大させることにもつながっていくだろう。

4．立法および司法における市民参加の動向とＩＴ活用

同じようなことは、立法や司法の場においても言えるので

はないだろうか。先の住民投票の動向を見ても、住民の代表であるはずの議員の意思と住民の意思との間に大きな乖離が存在することが明らかだろう。地方分権一括法で議会権限が拡大しているにも関わらず、相変わらずの口利き議員ばかりでは本当の住民意思を行政に反映させることはできない。住民の失望は年々下がる投票率の動向にも如実に現れている。

このような立法機能を活性化させ、本来の代議制民主主義を復活させるためにもＩＴによる市民参加が有効だろう。米国ではインターネット選挙が草の根的に市民を選挙活動に巻きこむ有効な手法として評価されている。自分の考え方に最も近い候補者は誰なのかを探してくれるサイトや議員を鑑定するサイトは、市民の投票活動を活性化させるとともに、議員に対しても良い刺激を与える。将来的には市民の意思をインターネット投票で確認しながら政策立案をする、バーチャル議員として一般市民も議会に参加する、ということも夢ではない。

それでは司法はどうだろうか。司法においても、法曹界と市民の生活感覚との乖離現象が問題になっている。悪質な交通事故に対する軽過ぎる判決は世の中の議論を呼び起こし、異例のスピードで刑法改正が行われた。実際に司法の世界は非常に閉鎖的であり、ＩＴ活用も信じられないくらい低いレベルである。情報公開で努力している行政と比べればその差は一目瞭然である。このような現状を打破しようと、司法改革の動きも出てきている。司法制度改革審議会の意見書では国民が訴訟手続に参加する制度も提言され、裁判員制度への道が開かれた。

このように司法を国民へ広く開放していく手段としてもＩＴは有効だろう。東京弁護士会では「ＢＡＩ・ＳＡＮＳＩＮ」というサイトを立ち上げ、陪審員制度の実際を映像でシミュレーションし、利用者が陪審員になったという前提で評決に参加できる仕組みを提供している。また、現行の司法制度の不備を訴えるためにインターネットを活用したり、原告が医療過誤裁判で協力してくれる医師を募集する手段としてインターネットが利用されている実態もある。司法についても、ＩＴを活用して市民が参加し、市民に身近な司法、市民が自分の道具として使える司法へと変わっていかなくてはならない。

5．パブリック・ガバナンスにおけるＩＴ活用

ＩＴを使って市民が行政に参加する、立法や司法へ参加するという時代が徐々に迫ってきている。このとき現在の間接民主主義と市民が直接参加する直接民主主義との関係をどのように考え、行政・立法・司法というパブリック・ガバナンス（三権分立）はどのように統制されるべきなのだろうか。

ロバート．Ａ．ダールによれば、「代表制デモクラシー（間接民主制）には『闇の側面』すなわち『エリートによる取引（バーゲニング）』が存在する。そして、市民たちはそのことを知っており『代表制のコストの一部として容認』している」という重要な指摘をしている。ここで私たちが考えなくてはならないことは、現代社会はダールの指摘する間接民主制における「闇の側面」を容認できない時代に入っているということである。ＩＴを活用した市民参加は、現在の間接的なパブリック・ガバナンス構造へ直接民主主義的な要素を注入し、過去から連綿と続く「闇の側面」を排除し、社会的閉塞感を打破して活気ある社会を創造していくことができるのではないかと考えられる。

さらに、新しいサービスやビジネスを生み出し、社会がＩＴを活用してより発展していくためには個人情報の利用は避けられない。しかし現状では、法的な規制の無いままあやふやな個人情報が流通している一方、国民の統一番号制度は国家による個人情報統制につながるという問題も懸念されている。このジレンマを解決するためには、個人情報という資産を市民参加のもとに管理していく手法が有効ではないだろうか。

個人情報およびその利用については地方政府と市民参加による個人情報管理委員会によって管理する。市民は自分の情報の利用範囲を自分の意思で決定でき、行政機関は法令および本人の申請に基づく情報のみを利用することができる。民間企業も法令および本人の申請に基づく情報のみを利用できる一方で、不当な個人情報利用については法的に処罰される。情報のガバナンスとは、行政だけが考える問題ではなく、市民個人個人が参加して統制する問題でもある。

6．おわりに

新しい技術というものは、常に人々に恐怖感を与える。新しい技術は今までの常識を覆し、慣習を破り、仕組みを変えてしまう。今までに遭遇したことのないリスクにも晒されることになる。もちろん、それに対して背を向けるという選択肢もあるだろう。だが、リスクを負わなければ、新しいものを創造することはできない。リスクを並べ立てて現状維持を図ることは誰にでもできる簡単なことである。重要なことはリスクを負って新しいことに挑戦する勇気を持つことである。一人一人が勇気を持てば、日本全体を覆う社会的閉塞感を打破し、活気ある社会を再生していくことができるのではないだろうか。

「セキュリティポリシーは何故必要か？」（セッション3より）

株式会社エスエスイーＩＳＭＳプロジェクトチーム 渋　谷　修　二

渋谷修二さん、セッション3講演の様子

「セキュリティポリシー」という言葉は、いつ頃から頻繁に使われるようになったでしょうか。実はこの数年のことで、それまではほとんど耳にしませんでした。私の経験では、ネットワークにファイアーウォールが導入されはじめて、その設定内容をポリシーと言ったのが初めてでした。

では何故それまでポリシーを必要としなかったのでしょうか。ここ数年の社会変革にネットワークとパソコンの普及をあげることに、誰も異論は無いと思いますが、セキュリティポリシーはこのことに深く関係しています。実はＯＥＣＤ（経済開発協力機構）から、今年の８月に「情報セキュリティガイドライン」の改訂版が発表されましたが、まさにパソコンとインターネットの普及が旧来の大型コンピュータを中心としたガイドラインでは時代にそぐわなくなった為でした。英和対訳資料がＩＰＡ（情報処理振興事業協会）の研究成果として次のＵＲＬに発表されていますので、是非ご一読下さい。（http:/www.meti.go.jp/policy/netsecurity/OECD020917set.htm）情報の形態は電子情報に限らないので、情報セキュリティに関するポリシーは何も今に始まったことでは無いのは事実です。又電子情報については、コンピュータの歴史を東京オリンピック以降に限っても、40年近くも歴史を持っていた訳です。その間にセキュリティポリシーが表立って騒がれなかったのは、コンピュータを扱う、又は扱える人は極一部に限られていたからです。この状況が、インターネットとブロードバンドの普及、パソコンの価格、性能の向上と普及によって、情報が大きな脅威に曝されている状況が、ふと気付いたらそこにあったと言えます。そしてコンピュータ／ネットワークの専門家だけで無く、一般個人もセキュリティに責任を果たさなければならない時代になったのです。

先にファイアーウォールのポリシーの話をしましたが、ネットワークの脅威に対して、今では当たり前のようにファイアーウォールの導入が盛んに行われました。サーバのセキュリティホールが騒がれ、パッチをマメに当てる様にもなりました。Ｗｅｂ上のデータのやり取りに暗号を一般的に使用する様にもなりました。これらを通してセキュリティレベルは大変向上しました。ところがセキュリティ事故（漏洩や改ざん）は減ったようには感じません。

セキュリティ事故を見てみると、どうも高度なハッカーが難攻不落のファイアーウォールを破って重要情報を盗み出した、なんていうのは少なくとも新聞の社会面の記事には出ていません。つまりアルバイト従業員がＭＯにコピーして持ち出したり、盗まれたパソコンに重要情報が入っていたりで、お金を掛けたネットワーク対策が役に立っていないのです。言い換えるとセキュリティを技術的な側面でしか評価していなかった為に起きたことで、組織のＩＴ部門の方々の怠慢では全くありません。セキュリティはもっと人間臭い、泥臭いもので、人々の行いを管理することが最も大事です。組織の全部門が一丸となって取り組むべきテーマなのです。

つまりここでいうセキュリティポリシーは、その組織で働く人々の「情報取り扱い規約」だと言えます。ファイアーウォールのポリシー（設定情報）は設定ミスやバグが無ければ100%思惑通りに機能しますが、セキュリティポリシーを実行するのは人間ですから、これを機能させるのが大変なのはいうまでもありません。これは交通ルールに似ているところがあります。交通ルールの古さはコンピュータ利用ルールの比では無いにも関わらず、事故は一向に減りません。これも運用するのが人間であることと、速さ、便利さを求めることの折り合いで成り立っているようです。セキュリティ事故を防ぐ為、ネットワークスピードを１０Kbpsに制限するといわれたら、あなたは納得しますか？

ポリシーとは、組織がセキュリティに対する管理がちゃん

とできている証であるといえます。セキュリティの管理手法については、英国のＢＳ７７９９（ＩＳＯ／ＩＥＣ１７７９９としてＩＳＯ化されています。参考ＵＲＬ：http:/www.bsi-j.co.jp/）が有名で、日本でもＩＳＭＳという制度（ＪＩＰＤＥＣ日本情報処理開発協会、参考ＵＲＬ：http:/www.jipdec.jp/）があります。何れも認証制度がありますが、取得の有無は別にして、セキュリティポリシーを作ろうとお考えの方は、これら規格に従った管理の仕組みを作ることに他なりません。

それでは何故セキュリティーポリシーが必要かという本題に触れたいと思いますが、先に極端な例として、高価なネットワーク対策が役に立っていないという、とんでもない意見を述べましたが、この意見の真意は、本来ファイアーウォールはその組織のセキュリティーポリシーに従って導入すべきものなのです。ではセキュリティポリシーも無いのに何故入れたのでしょう？メーカが必要だと言ったからですか？隣の人が入れたからですか？さらにいえばファイアーウォール製品もピンからキリまであるのに、何故その製品を選んだのですか？

セキュリティポリシーを作成する手順には、まず守るべき情報資産を洗い出します。次にその資産の「何」を守るか決めます。これを資産価値の決定といいます。実は情報には「機密性」、「完全性」、「可用性」の３面があります。つまり１つの資産に対して、「機密性」を守ることと「可用性」を維持することは、相反することなのです。簡単な例で言えば、ファイアーウォールを導入することは「機密性（Confidentiality）」を高めますが、「可用性（Availability）」を制限することになります。

次に情報資産のリスクを決定しますが、これをリスクアセスメントと言います。ＩＳＯ１４０００等の環境評価をご存じの方であれば、同様だと思って間違いありません。情報に対するリスクを何故評価するかと言うと、その対策として何が有効か、何が優先されるべき対策かを知る為です。ネットワークに繋がったサーバがあり、インターネットから侵入され、サーバが被害を受けるリスクを感じたら、対策の１つとしてファイアーウォールがあげられます。ここで１つのポリシーが生まれます。「インターネットの接続点において、外部からの侵入を防ぐ、ファイアーウォールを設置しなければならない。ファイアーウォールはパケットフィルタ機能を持ち、非武装セグメントを構成する為、内部ネットワークと外部ネットワークの２台で構成され、云々」。ここで注意すべきは、ポリシーレベルでは、なるべく普遍的な記述に止めて、下位レベルの手順書の中で、より機器を特定するような記述にしたほうが、ポリシーのメンテナンスがし易いと言えます。

もうひとつ大事なことは、ポリシーを作成すること自体がファイアーウォールを入れることと等しい、セキュリティ対策になることです。つまりこの組織において、将来どのようにネットワークの構成が変わってもファイアーウォールが必ず導入される、セキュリティレベルの維持が保証されます。と同時にポリシーは常に見直さなければならないことも読み取れたでしょう。つい数年前までファイアーウォール無しで平気でネットワークに繋いでいたのですから、この先いつまでファイアーウォール（と呼ばれる機器）があるかわかりません。事実ネットワーク構成に機能は別として、ルータという機器が見当たらなくなりました。これは昔からネットワークに携わっていた人間には信じ難い事象です。

非常に簡単ではありましたが、セキュリティポリシーの必要性と生成プロセスを述べてきました。ある人にとっては、セキュリティポリシーはＡ４、１枚に差し障りのない、宣言文があるだけと思った方もいるでしょう。もちろんその類いの文章も実は大変大事で、そこには組織のトップ（自治体であれば、首長）のコミットメントが述べられていなければなりません。本文の例に交通のことを書きましたが、最後に「ネットワークハイウェイを高速で飛ばしたいなら、是非セキュリティポリシーを！」といったところでしょうか。

電子認証の安全性

ハイパーネットワーク社会研究所 主任研究員 井 下 善 晴

1．公開鍵を使った電子認証

電子政府や電子自治体では電子認証のために「公開鍵方式」が採用されます。今回はこの方式による認証の安全性について考えてみることにします。

公開鍵方式を使用した認証の方法そのものについては紙面の都合もあるので割愛します。また、公開鍵方式を実現する技術にもいくつかありますが、ここでは古典的とも言える素因数分解を基礎としたRSA方式を前提に説明を行います。とは言ってもRSA方式は現在でも数多くのシステムで標準的に使われている方式です。

2．ＲＳＡ方式による暗号化と素因数分解

RSA方式の暗号解読が困難な理由は「大きな数の素因数分解は極めて難しい」という所にあります。実際の暗号化はもう少し複雑（興味のある方のために次頁に簡単な説明を載せておきます）ですが、素因数分解を解くことは結果的に暗号を解読することと同じですから、ここでは素因数分解について解説します。素因数分解とは学校で習いますが復習すると、「与えられた数を素数の積に分解する」ということで、例えば21は３×７というように分解できます。この程度の桁数なら電卓も必要ありません。では、7387の素因数分解はどうでしょう。電卓があっても難しいですね。

素因数分解の方法は色々な研究が行われ、楕円曲線を利用したもの、疑似素数を推定して見つけ出す方法、ふるい方などいくつかありますが、どれも劇的に短時間で解読できる、とは言えません。ここでは説明を簡単にするため、一番基本的な総当たり法を例に説明します。先ほどの21を素数に分解するには２、３、４・・・という数字で21を順に割り算していけば、３で割り切れて商は7なので３×７が答と分かります。これが総当たり法です。7837もこの方法で83まで行った時に83×89だと分かります。RSA暗号もこのように計算していけば必ず答を見つけ出すことができます。

そこで暗号の桁数が問題になってくるのですが、現在のRSA方式では1024ビットが標準的です。1024ビットは２の1024乗ですから10進数に直すと300桁以上の数字です。（参考までに256ビットで表現できる数を10進数で書いてみると11,267,210,267,647,966,460,912,964,486,932,558,653,966,460,912,964,486,267,210,267,647,966,460,964,486のような数ですが、桁数は77桁にすぎません）

3．素因数分解の困難さ

ではこれから実際に計算する前に計算回数を少しでも減らすための工夫をしてみます。

(1) まず総当たり法はその数の平方根以下の数まで割り算を行えば良いのです。21の場合、$\sqrt{21}$は4.58ですから５以上で割る必要はありません。（７で割れますが7という答は既に３で割った時に出ています。５以上での割り算はそれまでの計算を繰り返すことになり無意味です）‥①

(2) ４、６、８などの偶数も計算の必要はありません。これらの数で割れるかどうかは最初の２で既に答が出ているからです。……②

(3) どのくらいで答に辿り着けるかというと最初に見つかるかも知れないし、最後の数でやっと見つかるかも知れません。そこでやや乱暴ですが、半分までいった時に答に当たると仮定します。……③

これらを前提に、キー長256（2の256乗）の数字を素因数分解するのにかかる時間を計算してみます。

まず、①の前提から２の256乗の平方根を求めると約３×10の38乗になります(④)。さらに②と③から（④×1/2×1/2）と計算すると計算回数は約８×10の37乗(⑤)までに減りました。これを書いている時点で、出荷されている最高速のコンピュータ（注1）はNECの地球シミュレータ用スーパーコンピュータ（注2）で１秒間に40兆回計算できるというものです。ここではそれを使ってみます。すると⑤を40兆で割れば秒数が2126764793255865396646091秒と出てきます。これを3600秒×24時間×365日で割ると年数に換算できます。だいたい67439269192537588年となります。地球、いや宇宙の生命をはるかに超えてしまいます。（総当たり方は最も効率が悪いので、実際には他の効率の良い方法で数十年とか数百年といった“短期間”で解読できるようです）

4．コンピューター処理能力との関係

ここで次のような疑問が出てきます。何年かすればコンピュータの性能は飛躍的に高くなり、もっと短時間で解読できるようになるのではないか？。そこで、現在研究が進んでいるグリッドコンピューティング（注3）などの開発が進み、処理能力が今の100万倍になったとします。すると先ほど算出した解読時間は100万分の１、つまり67439269192年（674億年）となり少し危なくなりました。その場合はキー長を2048あるいは4096と増やしてやれば良いのです。（桁数が増えると解読時間は指数関数的に増大します）

コンピュータの世界ではこのようにキー長を長くすることはたやすいことです。コンピュータの性能がいくら上がっても追いつけないのです。（実は512ビットの暗号をある研究チームが292台のワークステーションと独自のアルゴリズムで半年ほどで解読しています。それでも1024ビットや2048ビットの解読は全く不可能と言われています（注4））

5．安全性に対する考え方

結論として現在の素因数分解を基礎にした暗号化方式は「完璧ではないが充分に安全である」と言えます。

・その一つめの理由はこれまで説明した物理的、数学的困難さです。

・二つめの理由はこれだけの計算を行うためにコンピュータを長時間使用すると、どう少なく見積もっても億単位の費用が必要になります。先の地球シミュレータは年間の電気代だけで10億円と言われています。（しかも誰にも気づかれずに実行する必要があります）

・三つめの理由は人間の特性というか理性です。誰も偽の１万円札を作るのに１万円以上の費用をかけることはしません。暗号の解読を試みるということはこれに等しい行為なのです。（もちろん、数学的な研究や暗号化技術の高度化のための研究等の場合は別ですが）

最後に、もし素因数分解を効率的に行う方法を発見できればその人は間違いなくノーベル賞の候補になります。この数百年の間、誰も発見できていないのですから。

（参考）ＲＳＡ方式暗号化の実際

【オイラーの定理】

基本となるオイラーの定理はどうしても説明しておく必要があります。

まず、n が次のように素因数分解されるとします。

$n = p \times q$

この時、オイラー関数 $\phi(n)$ は次のように計算されます。

$\phi(n) = (p-1)(q-1)$ （$\phi(n)$はn以下にnと互いに素である（注5）数字がいくつあるかを表しています）

nと互いに素である自然数 M に対して、

$1 = M$ の $\phi(n)$ 乗 $(\mathrm{mod}\ n)$ （注6）

が成り立ちます。これをオイラーの定理といいます。

【RSA 暗号のアルゴリズム】

以下、この定理を基礎とした鍵の生成、暗号化、復号化の方法について説明します。実際に $n = 21 (= 3 \times 7)$ を例にした計算式を併記します。

---公開鍵・秘密鍵の生成----------

まず n を２つの素数 p、q の積となるようにします。

$n = p \times q$ ・・・$21 = 3 \times 7$

n でのオイラー関数の値は

$\phi(n) = (p-1)(q-1)$ ・・・$\phi(21) = (3-1)(7-1) = 12$

となります。

次に、$\gcd(n,e) = 1$ となるように、適当に公開鍵 e を定めます。この公開鍵から次の式を満たす d を計算し、これを秘密鍵(d)とします。何でもよいのですが、ここでは

$e = 5$ としてみます。

$1 = e \times d \ (\mathrm{mod}\ \phi(n))$ ・・・$1 = 5 \times d \ (\mathrm{mod}\ 12)$

を満足する d を例えば $d = 17$ とします。

公開鍵 e は送信者に送り、秘密鍵 d は秘密に保持します。

公開鍵 e,n ・・・ 5、21

秘密鍵 d,n ・・・ 17、21

---暗号化----------

次に、送信者が受信者の公開鍵 e および n から、暗号文を生成するには、送信したい平文を P としたときその暗号文 C を次の式により定めます。（平文(P)を仮に11とします）

C＝P の e 乗(mod n)

・・・C＝11の5乗(mod 21) ＝161051 (mod 21)＝2

暗号文(C)は 2 となりました。

この暗号文(C)を受信者に送信します。

---復号化----------

受信者は、送られてきた暗号文 C を次の式により復号します。

P'＝ C の d 乗(mod n)

・・・P'＝2の17乗(mod 21)＝131072(mod 21) ＝11

これで最初の平分 P は 11 と復号されました。鍵を知っていれば実に簡単です。

【RSA の安全性】

RSA の暗号化・復号化は以上の通りですが、公開鍵 e および n から、秘密鍵 d を生成することができれば、暗号文を解読することができます。e と d の関係は次の式を満たすように選ばれています。

$1 = e \times d \ (\mathrm{mod}\ \phi(n))$

これから、$\phi(n)$ が分かれば、公開鍵の e と n から秘密鍵 d が求められることになります。しかし、$\phi(n) = (p-1)(q-1)$ ですから、これを計算するためには、どうしても n を

$n = p \times q$

と素因数分解し、p、q を求める必要があるのです。

（注）

RSA 方式の暗号を解くのに素因数分解以外の方法がない、とは証明されていません。ただし、それ以外の方法はまだ見つかっていません。

（注1）http:/www.top500.org 参照

（注2）地球シミュレータ

地球シミュレータとは、コンピューター上に“仮想地球”を作り出し、地球規模の気候変動や地層/地殻変動メカニズムなどをシミュレーションで解明するためのベクトル型並列スーパーコンピューターのこと。

（注3）グリッドコンピューティング

遠隔地に存在するコンピュータをインターネット等を介して接続し、CPU や記憶装置などの資源をそれらのコンピュータ同士で共有して、処理を行うコンピューティング技術。複数のコンピュータが持つ処理能力を統合することで高速な計算が可能となる。

（注4）量子コンピュータ

量子コンピュータは、現在のコンピュータのような0と1のデジタルを処理するものではなく、0と1の重ね合わせの状態（例えば、0が何%、1が何%といったような）を処理するもので、今までのコンピュータとは全く異なる概念で処理を行う。量子コンピュータは理論上、素因数分解を極めて高速に計算できるとされている。ただし実用化はもう少し先になりそうである。

（注5）互いに素

最大公約数が1となる数字のペア。gcd (a,b)=1 と表す。

（注6）a(mod n)

a を n で割った余りを示す。5(mod 3) は2。

豊の国ハイパーネットワーク利活用実験協議会について

豊の国ハイパーネットワークが整備されることにより、県内の拠点間でギガビット級の高速通信が可能となります。また、豊の国ハイパーネットワークと地域ケーブルテレビ網が接続されることにより、各家庭までの高速通信の環境が実現されます。

これらの高速通信網を活用して、より住民に密着したサービス提供のあり方を検証するとともに、高度情報通信ネットワーク社会の実現のための社会的･技術的な課題について実証･研究することを目的として、豊の国ハイパーネットワーク利活用実験協議会が2002年10月10日に設立されました。

会員は大分県、豊の国ハイパーネットワーク運営協議会からの代表として佐伯市と三重町、大分県 ISP 協議会、大分地上デジタル放送推進協議会、大分県ケーブルテレビ協議会、大分県情報サービス産業協会、(財) ハイパーネットワーク社会研究所、(財) 大分県産業創造機構、学識経験者として２名、からなっています。

事業の内容としては、豊の国ハイパーネットワークを利用して実験を行おうとする会員から提出される実験計画案を、社会的、技術的観点から検討し、協議会として実験計画を策定します。その後、策定した実験計画を豊の国ハイパーネットワーク運営協議会に提出します。

実験分野としては、インターネット関係、放送関係、ケーブルテレビ関係、 ASP 関係、産業関係が見込まれています。

（ハイパー研 主任研究員 福田）

第38回 ハイパーフォーラムのお知らせ

テーマ：**「ユビキタスへの展望」　～いい社会・いい大分の実現～**
日　程：2003 年 2 月 18 日（火） 13:30 ～ 16:20
場　所：大分第 2 ソフィアプラザビル2階ソフィアホール（大分市東春日町 51-6）
定　員：130 名
参加料：無料
主　催：大分県，財団法人ハイパーネットワーク社会研究所

最近「ユビキタス」という言葉がよく使われるようになってきました。ユビキタスとは1990年代に米ゼロックス社のマーク・ワイザーによって提唱された「ユビキタス・コンピューティング」から来ている言葉で、「どこにいてもコンピュータがある」世界の実現をめざす概念です。この新しいコンピュータとネットワークに関する考え方は、21世紀のライフスタイルやビジネス、さらには社会まで変える可能性を秘めています。決して遠い未来の話ではなく、インターネット・携帯電話の普及、情報家電とすぐそこまで来ています。

大分県でも豊の国ハイパーネットワークの構築が進んでおり、公共機関等へのコンピュータの設置も増えています。今後は基本構想の実現に向け、学校教育、生涯学習、福祉・医療・産業等いろいろな分野での活用を予定しています。

そこで、今後どのような世界になって行くのか、近い未来を想像しながら、すべての県民がＩＴの恩恵を受けられる「いい社会・いい大分」を考えていく場として「ユビキタス」をキーワードにフォーラムを開催します。どうか奮ってご参加ください。

【スケジュール】

13：30　開会・挨拶　　大分県企画文化部ＩＴ推進課、(財)ハイパーネットワーク社会研究所
13：45　基調講演　**「ユビキタスコンピューティングの現状と課題」**
株式会社ＮＴＴデータ 技術開発本部 副本部長 山本 修一郎
質疑・応答
14：45　休憩
14：50　個別講演　**「情報家電プラットフォームを活用したエリア・ポータルビジネスについて」**
松下電器産業株式会社 システム営業本部 事業開発部 峯岸 稔冶
質疑・応答
「ビジネスにおけるモバイルインターネットソリューションについて」
富士通株式会社 ソリューションビジネス事業本部 ＣＲＭソリューション事業部
質疑・応答　　モバイル・ビジネス部 部長 関根 和彦
16：20　閉会

※詳細は、財団法人ハイパーネットワーク社会研究所　URL は http://www.hyper.or.jp/ をご覧下さい。
※どなたでもご自由に参加が可能ですが、念のため事前の参加登録をお願いしています。
参加登録は「所属、氏名、住所、電子メール、電話番号」を Fax 又は E-mail でお知らせ下さい。
Fax 097-537-8820　　Email ： post @hyper.or.jp
※定員（130名）に達し次第、申込みを締め切らせていただきますのであらかじめご了承下さい。
※駐車場に限りがありますのであらかじめご了承下さい（近くに有料駐車場もございます）。

（担当　ハイパー研 主任研究員　植木、林）

発行：大分県　www.pref.oita.jp
編集：財団法人ハイパーネットワーク社会研究所
www.hyper.or.jp　post @hyper.or.jp　Tel.097-537-8180
〒 870-0037　大分市東春日町 51-6　大分第 2 ソフィアプラザビル 4F