研　究　報　告　書

２００６年度

財団法人ハイパーネットワーク社会研究所

目　次

巻頭言

実空間と仮想空間のはざまで

ハイパーネットワーク社会研究所
所長　宇津宮　孝一
utsumiya@csis.oita-u.ac.jp

２００６年度は，Tim O'Reilly の論文（www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html）が契機となってＷｅｂ２.０が急速に広まった年であった。この正確な定義は，まだよくわからない。しかし，Ｗｅｂをプラットホームとして，利用者が自由にコンテンツを作成・編集し，そのコンテンツが蓄積・関連づけ(tagging)され，「集合知」として広く共有されるという概念は，次世代 Web の大きな胎動が感じられ，大変興味深い。過去に，古典的人工知能の問題点が，「実世界の状態を一度記号化してコンピュータ内に取り込み，情報の世界ですべて処理しよう」という点にあったと言われることを考えると，実空間のさまざまな情報が，「Wiki」，「ブログ」，「SNS(Social Networking Service)」，「RSS(RDF Site Summary)」などの技術や仕組みにより，コンピュータのネットワークがつくる仮想空間上で広がっていくＷｅｂ２.０が拓く世界は，大きな可能性を秘めているものと期待されている。私自身も，センサネットワークの研究を始めているが，モノの情報など実空間の状況を自動収集する手段の発達は，情報社会の有り様を根本的に変えるものと考えている。一方で，人類の情報をすべて検索できるようにするとか，大勢の意見は案外正しいとか，素性を明らかにした者の閉じた世界の交遊関係は安全だというような議論には，共鳴しつつも，疑問を感じている人も少なくない。実空間で棲息してきた人間の一人として，本当に「人類の知識や知恵」をすべて集めて独占できるのか，「情報や知識」の信憑性は実体験に裏打ちされた「情報鑑識眼」がなくてどのように確認すればよいのか，「面識」もなく「対面」での「実経験」がないのに安心して交友関係に身を任せられるのかといった素朴な心配は尽きない。しかしながら，茂木健一郎氏が「フューチャリスト宣言（ちくま新書）」の梅田望夫氏との対談で語っているように，「できることは何でもやる」という Google の精神は，「黒船襲来」としてわが国の関係者に大きな衝撃を与えたことはまぎれもない事実である。

私は，最近，大学の基盤情報システムの更新に関わった。華やかな仮想空間の対極の実空間で，現実に情報ライフライン化したネットワークを切り替えることの大変さを身をもって体験した。ＩＰアドレスの振替えや設定・切替え，スイッチ類の設定と切替え，回線の切替え，ＤＮＳ(Domain Name System)の設定と切替えは，人海戦術そのものであり，間違えると大混乱が起こる（事実起こった)。メールサーバの切替えでは，「これまで使えた機能が使えない」，「メールが届かなくなった」，「何日か遅れて届いた」などさまざまな事案が発生した。問合せや苦情の電話（メールの唯一の代替え機器）が鳴りやまず，顔が見えない匿名社会では，「謝罪せよ」，「重要書類が遅れた責任は誰がとるのか」，「メールの送受信を保証せよ」など，１００％の完全性・安全性を求める利用者の会話は，エスカレートの一途をたどる。元々がベストエフォートのインターネットでは，利便性が高い分だけ，リスクも大きいのは当たり前であると考えながら，これまでインフラ周りの研究や技術開発に携わってきた者の一人として，「実空間と仮想空間のはざま」で悩む。認証にしても，現実空間でも「本人が本人であることを確認する」ことは，それほど容易ではない。仮想空間での識別と認証の困難さは，なおさ

らのことである。このようにユビキタス情報社会において，実空間と仮想空間の間に横たわる障壁をどのように解決していけばよいのか大きな問題である。佐々木俊尚氏は，「ネット vs.リアルの衝突」（文藝春秋）で，『新たな技術やネットワークによって，コミュニティや統治の仕組みが再編され，あらたな基盤を持った社会が生まれるのか，それともリアル社会が解体された結果，社会の基盤は失われ，秩序は崩壊していくのか。』について別の書物で論じていきたいと書いておられる。実空間と仮想空間の融合は本当に進もうとしているのであろうか。どちらにしても，われわれ人類は，実空間と仮想空間のなかで生き抜いていかなければならない世界に入ってきたことには，間違いはない。

こうした潮流も念頭に置いて，本報告書にまとめられた２００６年度の研究所の活動を振り返ってみる。これらの活動は，インターネットガバナンスと情報セキュリティ，地域情報化とデジタルデバイド，ＯＳＳ(Open Source Software)の実証実験，「ハイパーネットワーク２００６ワークショップ」を通じてのネットワーク社会の動向および国内外の情報化の進展に関わる調査・研究などである。

ワークショップでは，「ネット社会論 2006 徹底検証 Web2.0、OSS、NGN、IPv6・・・」というテーマで実施した。話題を多面的・多層的に取り扱うことによって，情報通信基盤からネットの新たな利用者参加型方式までの本質的な問題点のいわゆる「見える化」が図られた。インターネットガバナンスでは，アテネで開催された IGF 第１回会合に会津副所長が参加した。全体セッションのなかでは，本研究所の重要テーマでもあるセキュリティとデバイドが取り上げられており，解決困難な問題であることが窺える。情報セキュリティに関しては，本研究所の長年の普及啓発活動が評価され，経済産業省商務情報政策局長表彰を受けた。また，情報モラル啓発セミナーについては，２００６年度は福島・愛媛・名古屋で実施するとともに，その成果として具体的事例に基づく「情報モラル実践ガイド」を新たに発行した。

豊の国ハイパーネットワークを中心とする地域情報化およびデジタルデバイドについては，国のブロードバンドゼロ地域解消計画もあり，引き続き連携・支援活動を継続している。また，４年目に入ったマイクロソフト社のＵＰ社会貢献プログラムは，障がい者のＩＴ活用による自立支援やＩＴ就労を促進する取組みが確実に拡大している。研究所は，「Open School Platform」プロジェクトでの実績が認められたのか，独立行政法人情報処理推進機構（ＩＰＡ）のオープンソースソフトウエア（ＯＳＳ）活用事業を受託し，大分県庁での導入実証実験が実施されている。この事業の推進を通じて，地域でのソフトウエア供給にもＯＳＳは有効ではないかと考え，２００６年７月にＯＳＳ研究会の設置に参画し，ＯＳＳの普及啓発と新たな適用分野開拓に努めている。

一方，ネットワーク社会の新たな課題への取組みとしては，防災情報ポータル研究会を立ち上げ，情報ライフライン化が進展することが予想されるなかで，地域の安全・安心を確保するための今後の方策に関して，地域横断的な観点から論議を深め，問題点の洗い出しを行った。

こうした２００６年度の実績を踏まえて，２００７年度は，情報モラルや情報セキュリティ，防災や医療など住民主体の情報ネットワークの在り方，ネットワーク社会のガバナンスなどの調査研究や地域情報化の推進を通じて，デジタルデバイドのない安心・安全なハイパーネットワーク社会の実現を目指して努力を続けたい。また，ハイパーネットワーク２００７別府湾会議は，本研究所のルーツでもあるので，次代を見通した意義のある集まりにしたいと考えているので，ぜひご支援をいただきたい。

最後に，本研究所が，わが国では唯一と言っても過言ではない「地域に根差し，世界を見据えた情報社会科学研究所」として，さらに飛躍できるよう，皆様方のご支援・ご協力を引き続きお願いする次第である。

サイバーセキュリティのグローバルガバナンス

ハイパーネットワーク社会研究所副所長
会津泉

サイバーセキュリティに関連する国際協力の枠組みの現状と課題に関する考察

1. はじめに

1.1 変化する「インフラと責任」の範囲

情報社会の構築が急ピッチで進展するなかで、社会全体の情報通信サービスへの依存度は、従来とは比較にならないほど高まっている。エンドユーザーが直接目にするサービスとしてのインターネットや携帯電話サービスだけではなく、あらゆる産業、あらゆる企業活動、あらゆる非営利活動、あらゆる一般生活の諸活動に、さまざまな形で組み込まれている。今後さらに、ブロードバンド、携帯電話、無線 ID などによる新手のサービスが拡大・普及することで、いわゆるユビキタスネット社会の形成が進むことは必至といえる。

こうしたなかで、情報社会全般の諸活動について、だれがどのような責任を担い、どこまでを管理するのか、しないのか、とりわけ何らかの問題・事故・障害が起きたときにだれがどう対処するのか、といったことが、従来と同様のルールと実装でいいのか、新たなルールと運用・実装が必要なのか、といったことが問われている。

こうしたなかで、情報通信事業の関係者に対して社会基盤（インフラストラクチャー）の担い手として求められる責任は、今後ますます高まることは必至であり、かつその質も大きく変化すると考えられる。それには以下のような要因が関係するといえる。

IP 技術基本にシフト

まず、通信技術そのものがインターネットプロトコル（IP）技術を基本とするサービスへと全面的なシフトが進んでいく。これに伴い、「情報通信インフラ」の意味や範囲も大きく変化すると考えられる。従来、情報通信インフラに求められる機能としては、まずは社会の「ライフライン」として、水道・ガス・電気などと同様に、市民の生活に不可欠なコミュニケーションのチャネルという側面があった。同様に、企業、行政などの組織活動を支える上でコミュニケーションの必要性はきわめて高いことはいうまでもない。

しかし、近年のインターネットの発展・普及は、従来は他の手段で行われてきた様々な社会的活動をネットワーク上に移行させた。郵便や FAX による通信は電子メールに置き換えられ、株の売買、銀行取引などの金融サービスをはじめ、「電子商取引」と広く括られる各種商品、サービスの購買な

どがそれらにあたる。従来重要視されてきた「対面」での活動が、「オンライン」ないし「電子的」な活動へと主役の座を譲る場面が増大している。

ここで、従来の「電気通信サービス」の主たる任務は基本的な通信サービスの提供、すなわち物理的な信号の伝送であったといえるが、現在の「情報通信サービス」は、物理的な伝送に加えて、その上での各種の「情報処理」が加わり、少なくとも利用者側からみた場合には、両者は不可分一体のものとして受け取られている。

同時に、従来、通信事業者が垂直統合的にサービスを提供していたのとは異なって、現在提供されているサービスの多くは、物理的な基幹回線、その上のインターネット接続、サーバーを介したアプリケーションサービス、さらに支払・決済処理、商品配送など、提供者側は機能別に分化しつつ、全体としては複合的なサービス形態が普遍化している。

障害の影響範囲の拡大

これらのサービスの構成要素のうちどれか一つにでも故障が起きると、利用者には全体が機能していないのと同等の障害として受け取られることになる。もちろん、基幹回線に障害が起きた場合は、ある特定の販売サービスだけに起きる障害と比較して、その社会的な影響の範囲や深刻度がはるかに大きくなることは言うまでもない。しかし、最近の東京証券取引所におけるシステム障害の事例にみられるように、たとえ上位レイヤーの情報システムのアプリケーションにおける障害であっても、その影響度の大きさは経済価値に換算すれば無視できないものがあるケースも増大している。

この意味で、従来の「物理的インフラ」に求められる社会的責任に加えて、仮に「論理的インフラ」ともいえる、こうした情報システムにおけるアプリケーションやサービスに求められる社会的責任の大きさは、今後の情報社会における情報通信インフラ事業の責任のあり方を考える上で、重要な要素となるだろう。

ユビキタス化の進展

一方、携帯電話の普及は、ライフスタイルを大幅に変えてしまった。携帯をもつことで、事前に正確な時間や場所を定めないで人と待ち合せることはごく当たり前になってきた。出発時間間際に列車や飛行機の切符を購入することも可能となった。こうした「時間のソフト化」も、通信インフラのサービス形態の変化がもたらしたものといえる。現在普及が急速に拡大している、スイカ、エディ、おさいふ携帯など、IC チップによるサービスをはじめとするモバイル・小型機器によるアプリケーションは、今後さらに技術革新が進むことで、より普及し、サービスのユビキタス化は大幅に進展するであろう。

それに伴って、プライバシーの侵害など、新しい質の問題が発生する可能性も高くなる。ユビキタス、すなわち「だれでもどこでもいつでも」とは、プラスの意味での可能性を表すばかりではなく、個人情報保護、セキュリティの確保などを含めて、社会的責務を果たすという意味での責任の所在を求める表現ともなりつつあるととらえるべきである。責任もまた、ユビキタスに広がるのだ。

これらの社会的責務をもったインフラそのものの拡大は、そのガバナンスのあり方の変質を求め、それは情報通信市場そのもののあり方と、さらに情報通信を利用したサービス市場の形成・展開のあり方にも、直接・間接の影響を及ぼすものと考えられる。

1.2 セキュリティ意識の高まり

こうした状況を受けて、通信ネットワークおよび情報システム全般を総合した「サイバーセキュリティ」に関する意識は高まりつつある。各国政府はサイバーセキュリティに関する各種の戦略・施策を策定し、個人情報保護をはじめとした法制度の確立や司法体制の充実などに力を入れている。2005年11月にチュニジアで開催された世界情報社会サミット(WSIS)でも、セキュリティについての重要性と国際協力の必要性について合意されている。我が国でも内閣府情報セキュリティセンターが設立され、基本計画が策定されるなど、取り組みが加速している。

しかし、社会全般におけるサイバーセキュリティの重要性についての認識は、一部関係者の間では高まっているが、経営者をはじめ一般の企業の担当者のレベルまで、十分に浸透しているとは言い難い。企業の取り組みをいっそう推進するための有効な方策が求められている。

また、最近はとくにフィッシュングなど、経済的な実利を狙ったより組織的、悪質なセキュリティ事犯が大幅に増加している。これらの手口は技術的にも高度化し、対応する側も、当然より高度の技術的、組織的取組みが求められている。

同様に、経済的なセキュリティ侵犯は、国際的な犯罪ネットワークとの結びつきが深まっている。従来のような一国単位での対応では、彼らの国境を超えた連携に追いつかない。それだけ、国際的な対応が求められるようになってきた。しかし、国際的な協力の枠組みについては、必要とされるレベルに達しているとはいえず、様々な課題がある。

本稿は、上記の問題意識に基づきつつ、国際社会における情報セキュリティへの取組みについて、国際機関による取組み動向を中心に現状を調査し、比較分析を行い、課題の抽出を試みたものである。[1]

2. なぜ国際協力の枠組なのか

サイバーセキュリティについてよく言われることは、システムのセキュリティの強度はその全体のなかのもっとも弱い部分の強度で規定される、ということである。

インターネットによって、国境を超えて世界中のコンピューターとネットワークがオープンに相互接続されるようになった今日、外部からの侵入を効果的に防ぐためには、自らのシステムのみを強化しても不十分である。

多く場合、脅威の発生源は、自国の法制度・司法能力が及ばない海外に存在している。攻撃を受けた場合にも、即時の対応が難しい。政策や法制度の相違は、迅速な対応にとって大きな桎梏となる。

ここに、サイバーセキュリティに関する国際的な協力の枠組みの重要性が存在する。

しかし、国際協力の枠組は、その重要性については関係者のほぼすべてが強調する一方で、実際に十分な国際協力の組織や枠組みが機能しているかというと、実はそうではない。それには様々な要因

---

[1] 本稿は、筆者が責任者を務め、多摩大学情報社会学研究所が日本電信電話会社から受託した調査研究プロジェクトの一テーマ、「グローバルガバナンス論：国際協力の枠組みについて」の結果をベースに、加筆修正したものである。

が存在するものと思われるが、いずれにしても、スパムやフィッシングをはじめ、DDOS 攻撃など、インターネットなどを媒介として増大する一方の国際的なサイバーセキュリティへの脅威に対して、これに対処する側の国際的な動きは、残念ながら必要なレベルに達しているとは思われないのである。

本調査は、こうした問題意識に基づいて、現在存在しているサイバーセキュリティに関する主な国際協力の枠組みについて、その現状を、主な性格・対象分野、機能、特徴、構成主体、組織体制、課題などについて調査・分析し、あるべき方向性について考察・実践するための素材を提供しようというものである。

実際に現存している国際協力の枠組みは、歴史も浅く、範囲も限定されており、法制度、政治的正統性、社会的受容度などのいずれの点からみても、十分に確立されたものとなっているとはいえない。

2.1 本調査の方法

調査対象

本調査では、サイバーセキュリティにかかわる国際組織、ないし協力の枠組として、以下の組織を主な対象として取り上げた。

IGF　EU・ENISA　OECD　APEC　ITU
ICANN　IETF　FIRST

また、関連して、欧米諸国の政府についても、情報セキュリティ政策にを対象として調査を行った。

調査日程

本調査は、以下の日程で進められた。

時期	項　目	内　容
2006 年 9 月	実施準備	調査対象の整理 文献調査・訪問準備
10 月	欧州出張 10 月 3－16 日	EU(ブラッセル)　ITU(ジュネーブ) ISSE2006 会議(ローマ)　OECD(パリ)
11 月	米国・欧州出張 10 月 23－11 月 6 日	Economics of Security Workshop （ワシントン DC) 関係者へのインタビュー(ワシントン DC、ニューヨーク) インターネットガバナンス・フォーラム （アテネ) European Network and Information Security Agency (ENISA) （ヘラクリオン）
12 月	訪問まとめ 文献調査 訪問準備	
2007 年 1 月	米国訪問	関係者へのインタビュー(ワシントン DC)
	訪問まとめ 文献調査	資料・論点の整理 報告書執筆(①グローバルガバナンス論)

調査対象者

本調査では、以下の専門家に面会し、面談を行った。

月日	場所	氏　名	所属・役職	組　織
10月 4日	ブラッセル	Michael Niebel	Head of Unit, DG Info Soc & Media	EU
9日	ジュネーブ	Yoshio Utsumi Robert Shaw George Sebek	Secretary General Deputy Head, Stratety and Policy Unit Counseller, TSB	ITU
10日	ローマ	Andrea Pilloti Andreas Mitrakas	Executive Director Leagal Advisor	ENISA
11日		Dionisio Zumerle	Technical Officer	ETSI
12日		Serge Lebel	Infosec Advisory Team	Secretariat General for National Defence (SGND), France
		Charles Brookson	FIEE FRSA AFRIN	Department of Trade and Industry, United Kigdom
13日	パリ	John.Dryden Andrew Wyckoff Anne Carblanc Sam Partridge	Deputy Directo, Science, Technology and Industry Directorate Head of ICPC, STID Principal Administrator, ISPCP, STID	OECD

月日	場所	氏　名	所属・役職	組　織
10月 23日	ワシントンDC	Steve Crocker	CEO	Shinkuro
		Matt Larson	Director, DNS Research	VeriSign
24日		Sam Weiler	Senior Scientist, Network Security Division	SPARTA
25日		Jean-Paul Enrad	Director, Industry Forums	Alliance for Telecommunications Industry Solutions (ATIS)
		Liz Gasster	General Counsel	Cyber Security Industry Alliance
		Michael Nelson	Director, Internet Technology and Strategy	IBM
26日		Rich Hovey	Public Safety Homeland Security Bureau	FCC
		James Dempsey	Policy Director	Center for Technology and Democracy (CDT)
27日 ～ 11月 2日	アテネ	Bruno Lanvin	Regional Coordinator, Europe and Central Asia, Global Information and Communication Technology Dept.	World Bank
		Stefaan Verhulst	Chief of Research	Markle Foundation
		ENISA、EU、ICANNなど多数の関係者	インターネットガバナンス・フォーラム	
6日	ヘラクリオン	Andrea Pilloti Panagiotis Trimintzios	Executive Director Expert, Industry and International Institutions	ENISA

3 調査結果の概要

3.1 各国際機関・枠組みの特性と課題

本調査は、サイバーセキュリティにかかわる主な国際協力機関・協力枠組みについて、その概要、活動状況などを調査し、その特性と課題を抽出したものである。

調査対象とした機関は、その属性によって、以下のように４つに大別できる。

属　性	機関名
国際連合の関連組織	IGTF　ITU
地域的な国家間国際組織	EU・ENISA　OECD　APEC
民間主体の国際管理・標準化組織	ICANN　IETF　FIRST
民間主体の地域標準化組織	ETSI　ATIS

以下に、各機関の主な特性と課題を一覧にして記す。

IGF（インターネットガバナンス・フォーラム）

特性

設置主体：国際連合　5年時限で設置

使命：「インターネットガバナンス」に関するマルチステークホルダーの対話の推進

特徴：拘束力をもつ決定は行わない

参加組織：各国政府・産業界・市民社会　オープン参加

アテネ会合：推定約100カ国、計1400名が参加

政府代表：85カ国・320名　国際機関：28機関・70名

民間（産業界・市民社会）：440組織・770名、メディア：35組織40名

焦点：開発途上国のインターネットガバナンス政策

サイバーセキュリティも主要テーマとして認識

課題

・「対話」から実際に具体的な成果をあげられるか

・途上国からの実質参加を増やすことができるか

・インターネットの資源問題（ICANNを中心に）の解決策実現に寄与できるか

・資金を確保できるか

・5年間の時限で設置、その後継続されるか

・MSH方式が実を結ぶか、あるいは政府側が、政府の立場をより強める方向で主張するか

・国連事務総長の交代の影響を受けないか

（WSISもIGFも、コフィ・アナン前国連事務総長の強い個人的コミットがあった）

EU（欧州連合）

特性
主体：欧州27カ国による地域超国家国際機構
特徴：経済中心の国際組織だが、欧州指令を通して加盟国の政策に一定の拘束力をもつ
（外交、国防、司法については各国の主権尊重）
地域機構としては、実績も厚く、組織も定着
「情報社会」政策を推進、情報セキュリティも重視、ENISAを設立
課題
・加盟国間の経済・技術・制度・文化的格差大きく、統一的施策の実装は困難
・経済分野限定、他分野（外交、国防、司法）は国家主権の壁が厚い
・政策の調整・ガイダンスが中心で、技術・運用面の取組みは弱い
・オペレーションレベルでの活動は行っていない

ENISA（欧州ネットワーク情報セキュリティ庁）

特性
設置主体：EU
活動分野；経済分野中心、意識啓発、CERT形成支援などが中心
組織構成：理事会には政府以外のステークホルダーも参加、MSH型運営
特徴：EUの「外局」機能、EUの政策企画立案機能への補完的役割増大へ

課題
・「経済活動」に限定され、司法当局などとの密接な連携は困難
・「国家主権」を重視する一部加盟国からは、ENISAの活動への抵抗が強い.
・加盟国間の経済・技術・制度的な格差が大きく、統一的な施策の実装は困難
・ブラッセルのEU情報社会メディア総局との役割分担が必ずしも明確でない
・国際協力の推進をうたっているが、実質的には担当者2名で、人員・予算が弱体
・技術分野も「フォロー」に止まり、政策的な関与は難しい

OECD（経済開発協力機構）

特性
主体：30カ国政府による国際経済協力機関　先進国中心
組織構成：国際条約による政府間組織、産業界、専門家などもオブザーバー参加
焦点：情報技術政策に注力、セキュリティガイドライン、スパム防止などで国際的なイニシアティブを発揮し、影響力は強い
特徴：拘束力のないフォーラムとして、ガイドラインなどの「ソフトロー」を重視

課題

・国際政府機関であるが、法的拘束力をもたないフォーラムで、実効性の担保がない
・先進国の利害に限定されがちで、途上国を含めたグローバルな影響力は不十分
・先進国中心の「金持ちクラブ」だとして、途上国側からの反発が強い
・セキュリティに関する「上流」の技術標準化活動には直接関与ができない
　フォローに止まり、課題の先取り、調整が難しい
・セキュリティに特化した活動に十分な資源をさけない
　事務局の人員にも限界

APEC（アジア太平洋経済協力）

特性

主体：アジア太平洋21カ国政府・地域による地域経済協力機構
　　米国、中国、日本、ロシア、カナダ、オーストラリアなどの主要国を網羅
特徴：情報交換中心の緩やかなフォーラム　参加国の政治体制はきわめて多様

課題

・　経済面の緩やかな協力が中心で、拘束力のある決定・活動は行われない
・　加盟国間の政治体制、経済水準などのギャップが大きく、効果的施策の実装は困難
・　情報交換、政策調整・ガイダンスが中心で、技術的な取組みもあるが弱い
・　オペレーションレベルでの活動は行っていない
・　技術標準化分野に関して直接の関与はない

ITU（国際電気通信連合）

特性

主体：国際連合傘下の国際専門機関　190カ国加盟
組織構成：政府間組織が基本　民間企業もオブザーバー参加
目的：通信技術標準化、電波周波数割当調整、途上国への通信普及など
特徴：国際機関のなかではもっとも長い歴史・伝統をもつ

課題

・電気通信主体で、コンピューター、インターネット分野の蓄積、認知が弱い
・技術標準中心の専門機関で、政策取組み体制は弱い
・オペレーションレベルでの取組みはない
・官僚的な意思決定機構のため、小回りが利かない
・先進国から途上国まで加盟国間のギャップが大きく、効果的な施策は実施困難

ICANN

特性

主体：技術分野中心の国際非営利組織　米国政府の契約で存在を担保

組織構成：インターネットの技術コミュニティ・企業が中心、政府・市民は助言組織

目的：ドメイン名とIPアドレスの管理割当中心、インターネットの安定運用

特徴：1998年設立、数次の組織改革を経るが、組織的には不安定な状況が続く

ルートサーバーのオペレーションには間接関与

課題

・草の根的な発展の歴史を背景に、政治的正統性、認知度が弱い

・米国政府が最終的な決定権をもち、政治的正統性・中立性に問題

・技術者中心のコミュニティの性格が強く、政策的な取組み体制は弱い

・組織構成が複雑で、決定が遅く、不透明との批判も強い

・政府政策担当者、一般利用者（パブリック）が意思決定に有効に参加できていない

・DNSのオペレーションでは、運用者への強制力をもたず、責任も薄い

・グローバルな組織を標榜するが、実態は先進国中心で途上国からの参加は弱い

IETF

特性

主体：関心と実力があれば、だれでも個人で参加可能　ボランティア性が強い

特徴：議論も情報も、すべてオープンな原理と実装を重視

インターネットの文化を体現

課題

・標準化の速度が遅い

・セキュリティの取組みも遅い

・定められた手順通りに作業が進まない

・WG間のコンフリクトが解消されない

・知的所有権（IPR）がブロックになることも多い

・統治機能としてのIESGの権限が不足

・事務局を支える恒常的な体制が不安定

・（とくに外部から）特定の人々による支配との批判が根強く存在

FIRST

特性

主体：CERT、CSIRTのグローバルな民間連合体　ただし政府組織も多数参加

目的：セキュリティの障害関連情報の共有

課題

FIRST およびその構成体である CERT/CSIRT が直面している課題としては、以下があげられる。

・制度的法的位置づけが確立していない
・運営資金・財政の基盤が安定していないところもある
・活動対象・範囲が曖昧で公的政策領域と企業・民間活動が明確に分かれていない
・国際協調体制は欧米中心で、途上国、とくにアフリカは大きく立ち遅れている

サイバー犯罪条約（Convention on Cybercrime）

特性

主体：欧州評議会

参加組織：欧州各国＋日本、米国、カナダ、南アフリカ、モンテネグロが署名
批准国 18、署名国（未批准国）25

目的：著作権、オンライン詐欺、児童ポルノ、違法アクセス、違法傍受などのセキュリティ侵犯に対し、司法協力枠組についての国際基準を定め、対応国内法の整備推進

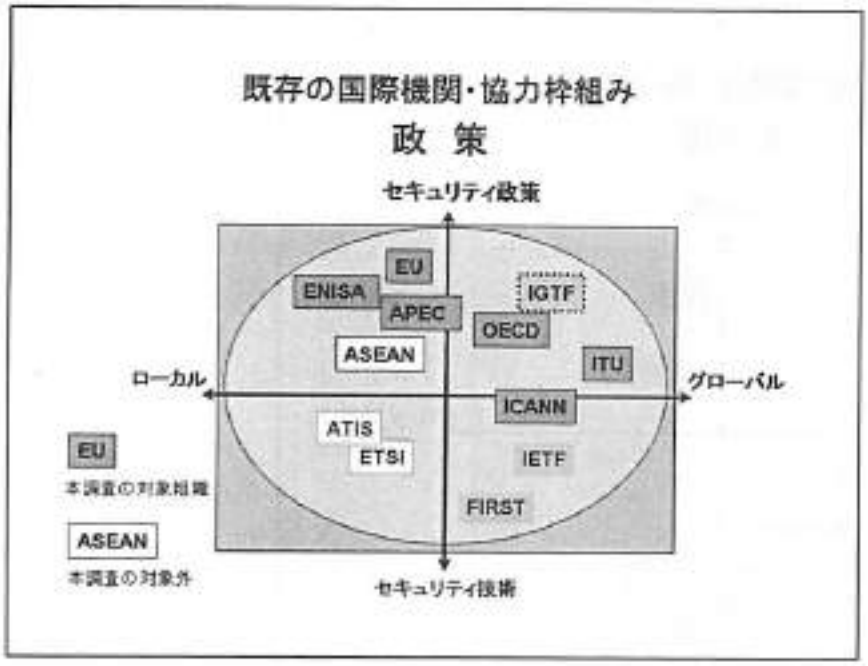
課題

・批准・署名国とも、まだきわめて少数
・人権・プライバシー侵害のおそれが強いと批准反対も
・途上国も含めて真にグローバルな実効力もつには、相当の時間がかかる

3.2 国際機関・協力枠組みのマッピング分析

これらの国際機関・協力枠組みを、その主たる任務の分野別にまとめ、カバーしている地理的範囲を座標軸として、マッピングによる分析を試みた。

政策推進

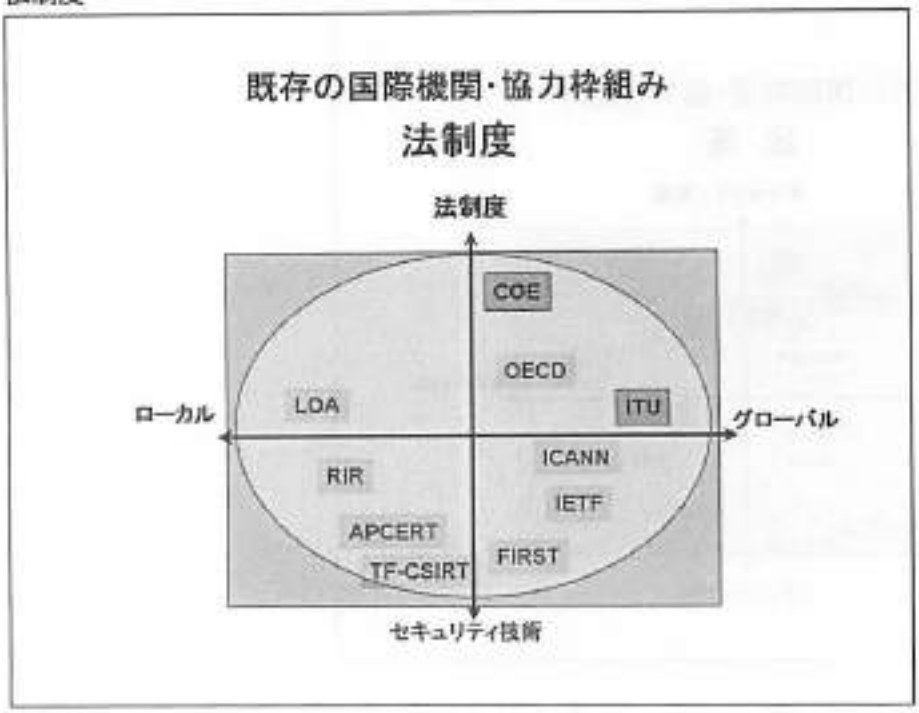


マッピングの最初は、サイバーセキュリティの政策に関連する活動を行っている機関をとりあげた。これらは ITU、OECD、EU、APEC、ENISA、ICANN などで、本調査では直接調査はしなかったが、ASEAN も政策の形成、推進に関与している。アジアと欧州諸国の連絡機関である ASEM も広範な政策課題で定期会合を開いているが、サイバーセキュリティに関しては、2005 年にソウルでワークショップを開いただけで、重点を置いた取組みはみられない。

グローバルなカバーという点では、ITU が、発展途上国にも広く加盟国をもち、もっとも広範な影響力をもっているといえる。ただし、ITU は技術標準および途上国への通信普及が主な使命とされ、サイバーセキュリティに関する実際の政策形成への影響力は相対的には限定されている。OECD は、加盟国こそ 30 と少ないが、先進国をほぼ網羅しており、その影響力という点では、相対的には高い。ただし、国際条約などの拘束力をもった決定は行わないため、その影響はいわゆる「ソフトロー」にとどまる。

EU は、「超国家」としての政策をもち、加盟国の国内政策に対しても、EU 指令などにより一定の法的措置を義務付けられる力をもっており、その影響力はかなり高い。しかし、基本は経済分野に限定され、国家主権に直接かかわる司法、外交、国防分野での各国の政策への影響力は最小限に制限されている。サイバーセキュリティは、これらの分野との関連も密接にある分野であるため、この点は、EU にも一定の制約となっている。

法制度



サイバーセキュリティに関する国際的な法的枠組みとしては、欧州評議会（Council of Europe: COE）が中心になって制定されたサイバー犯罪条約（Convention on Cybercrime）が唯一存在している。同条約は、地域を問わず、批准手続きを行えば加盟できる国際条約である。

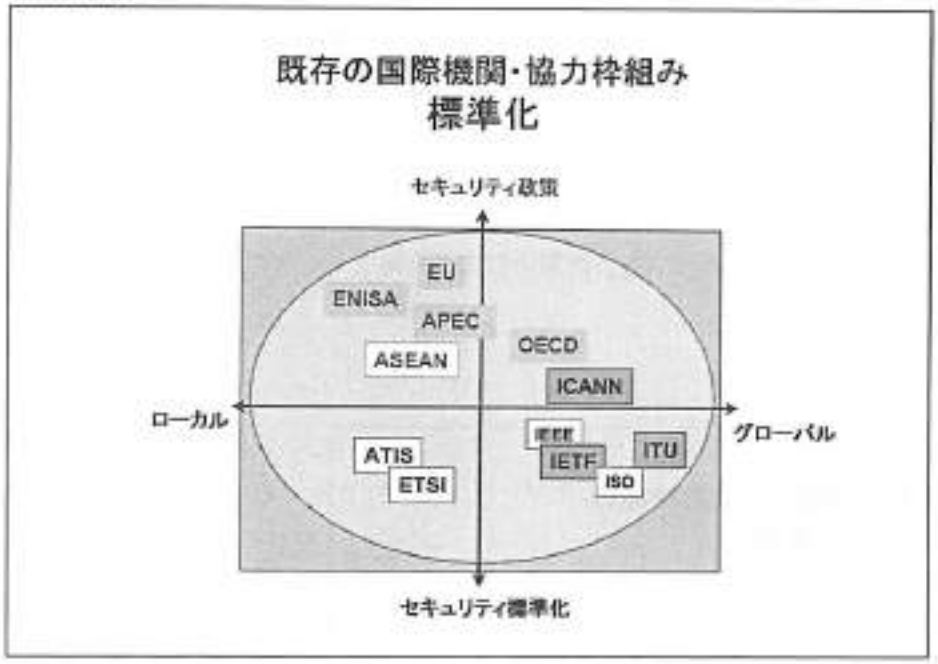
同条約は 2001 年 11 月に欧州評議会が採択し、2004 年 7 月に 3 カ国以上が批准して発効した。2006 年 9 月に米国政府が欧州以外の国として初めて批准を行い、現在、批准国は 18 カ国、署名国で未批准国が 25 カ国を数えている。[2]

日本は、2004 年に国会で承認して形式上は発効しているが、国内法整備のための刑法改正が「共謀罪」の扱いをめぐって難航しているため、正式な批准はまだ行われていない。日弁連や市民団体の間には、人権・プライバシー侵害のおそれが強いして批准反対の意見が強く、かりに批准するとしても条約で認められている最大限の「留保」をすることが要請されている。

いずれにしても、批准国はまだ 20 カ国にも達してなく、途上国も含めて真にグローバルな実効力をもつまでには、今後相当の時間がかかるものとみられる。

[2] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=2&DF=1/30/2007&CL=ENG

技術標準化



通信技術における標準化においては、ITU が伝統的には大きな役割を果たしてきた。ただし、1980 年代から 90 年代前半にかけて、ITU はインターネットが当初の学術研究のためのネットワークから、広く一般・商用に利用されるグローバルなネットワークへと成長を遂げるプロセスを認知するのに遅れをとった。電話中心の通信の世界の専門機関としての ITU は、コンピューターが中心となるインターネットの世界のもつ新たなパラダイムをタイムリーに認識できなかったのである。

なお、本調査の対象とはしなかったが、国際標準機構（ISO）も 80 年代にコンピューターネットワークの標準として OSI を提唱したが、実用性を欠いたことが大きく影響し、インターネットに主役の座を譲る結果となったものである。ITU も ISO も、公的プロセスを重視したいわゆる「デジュール標準」での標準化を推進してきたのに対して、IETF は、ラフコンセンサスによる「デファクト標準」を重視し、結果として急速かつ広範な普及を実現した。

インターネット技術は、IETF が中心に標準化を進めてきた。ただし、IETF も、セキュリティについては実社会のニーズに対して必ずしもタイムリー、的確に対応できたとは言いがたい。

また、これまでは技術標準化というと、社会政策的な側面はほとんど意識されず、「純粋に」技術的な作業と受け取られていた。しかし、コンピューターとインターネットが社会活動全般のインフラとなり、その上で金融、商取引から政治、経済活動まで広範な営みが行われるようになった現在、そうした技術が、どのような新機能を提供するのかは、結果として大きな社会的影響をもつようになったことは否定できない。なかでも、セキュリティにかかわる要件は、大きな社会的インパクトをもつ。犯罪（防止）、ID 管理とプライバシー、トレーサビリティと人権などは、技術がもつ社会性が顕著に現れる分野である。

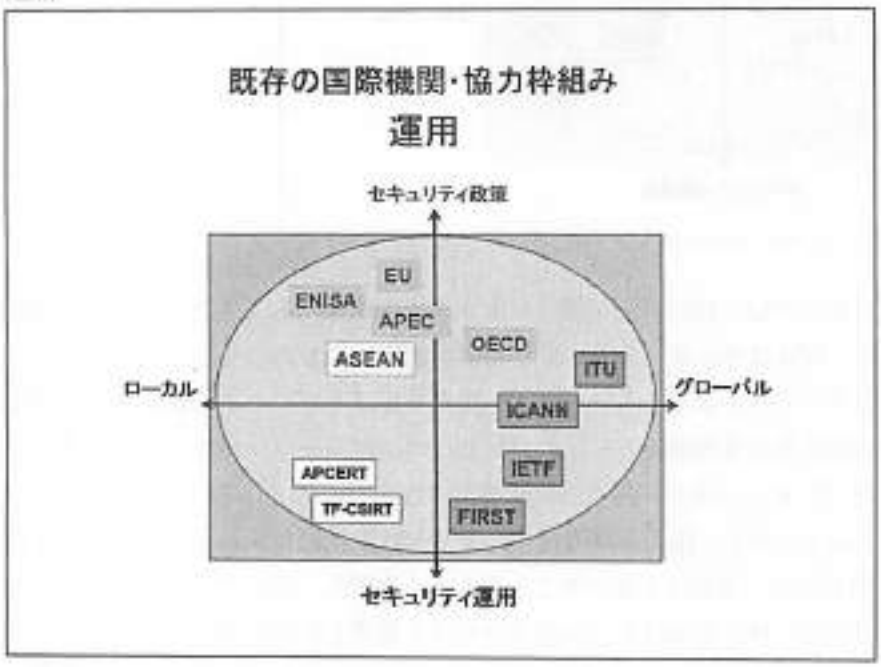
ということは、標準化のプロセスにおいても、本来ならそうした社会性の観点からの検証作業が必要となると考えられる。しかし、現実には、ITU-T における NGN のセキュリティの標準化作業においても、IETF における DNSSEC の検討においても、あるいは ICANN における新 TLD の導入検討プロセスにおいても、社会政策的な論点は、ほとんど考慮されていないか、不十分であることは否定で

きない。

OECDのセキュリティガイドラインを策定した事務局のメンバーは、NGNにおいてID管理が米国政府から提唱されていることをほとんど知らなかった。また、仮に知ったとしても、OECDEのもつ基本的な任務外であるために、実際に議論に関与することは難しい。しかも、おそらくこれは、きわめて多岐にわたる事項のごく一部だろうから、政策担当者が実際に個々の問題に深く関与することは、現実的にはきわめて困難である。

その意味で、国際的な標準化の策定プロセスと、政策の立案・実施プロセスのそれとの間には、大きなギャップが存在しているといえる。

運用



運用面からサイバーセキュリティに取り組んでいる国際組織は少なく、関係者も限られている。CERT、CSIRTの連合体としてインシデント情報の共有を行っているFIRSTがもっとも顕著といえるが、普及・浸透度は十分とはいえない。情報技術関連の政策担当者や企業の間でも、FIRSTの一般的な認知度は、おそらく相当低いと思われる。

実際のオペレーションでは、米国のCERT/ccおよびUSCERT、イギリスのNISCC、日本のJPCERT/ccおよび内閣情報セキュリティセンター（NISC）、それにカナダやオーストラリアのCERTなどを加えた個別組織同士の連絡体制が中心に機能し、FIRSTは、その「外枠」を提供しているとみるべきだろう。また、FIRSTは民間組織でありつつ、政府機関も個別には加盟しており、情報の共有などの面で、法的根拠、正統性については明確ではない。

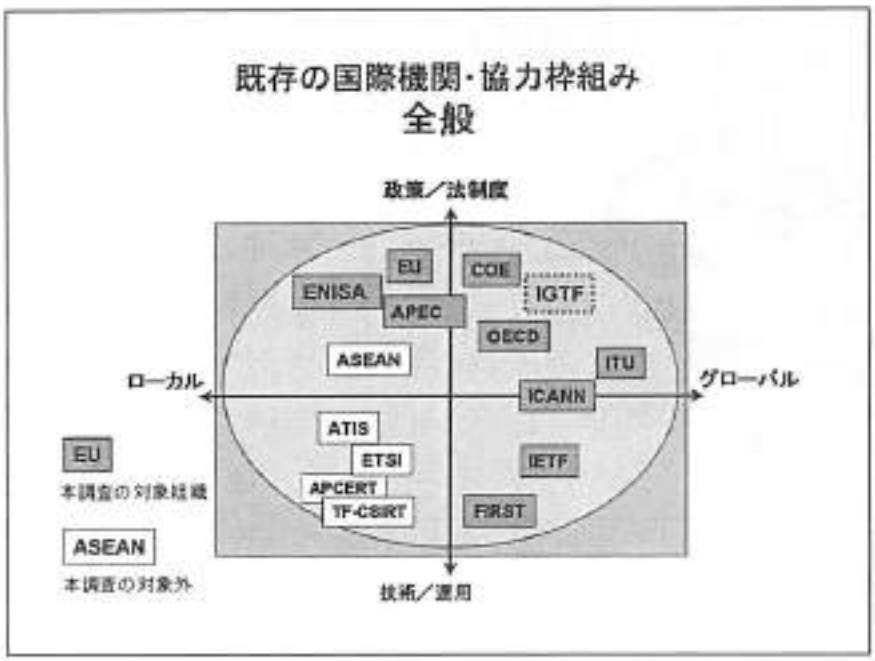
ICANNも、DNSルートサーバーの運用の責任の一端をもっているが、実際のルートサーバーの運用主体との間に、明確な契約関係は存在せず、自発的な協力に止まっているため、法的・政治的な責任体制の面で疑問も出されている。gTLD運用者との間には契約関係があるが、国別のccTLD運用者との契約は、一部に過ぎない。

このほか、本図には入れてないが、業界セクター別のISACも存在し、緩やかな連携はあるが、大

半が国内的な活動が中心で、国際的な協力活動として確立されているとはいえない。

また、インターネットのオペレーター同士の連絡組織としては、NANOG、SANOG、APOPS などの地域別組織があるが、いずれも個人中心のボランタリーな集まりで、恒常的な組織とはいえない。

全般の取組み状況



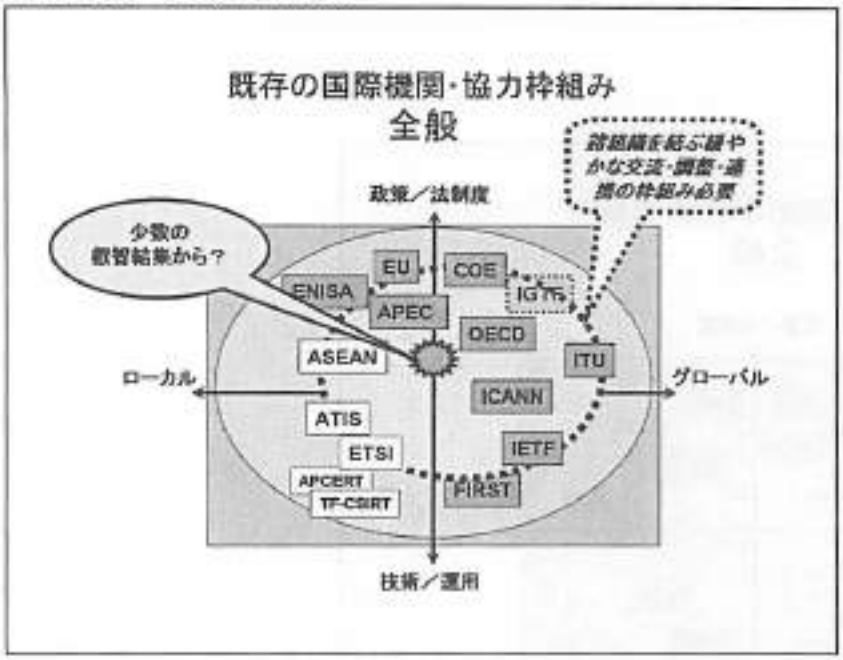
こうして、政策、法制度、技術標準、技術運用の各分野での既存の国際機関および国際協力の枠組みについて概観してきたが、いずれの分野においても、増大するセキュリティの脅威への対応に求められる活動や機能を鑑みたときに、十分な体制が存在していないことは明らかである。

また、グローバルな体制という点では、各分野の国際機関・枠組み自体がいずれも、参加する国や組織主体の数、分布において、十分とはいえない実態がある。とくに技術系の要素が強い組織においては、途上国側の参加・実質的な関与が明らかに不足している。もちろん、経済水準と情報ネットワークの普及・利用とは、相対的に比例すると考えられるから、ある程度はそうしたアンバランスもやむをえないといえよう。ただし、ことセキュリティに関しては、途上国側をベースとしたウィルス、フィッシング、DOS 攻撃など、多くの障害事例が多発していることも事実であり、必ずしも経済水準に見合った体制が十分とはいえないことは留意する必要があるだろう。システム全体のセキュリティ水準はもっとも弱い環の強度で既定されるという一般則を考えれば、途上国であるからということで、国際協力の枠組みに入らなくても仕方がないという考えはとるべきではない。

同時に、サイバーセキュリティは、異なる専門分野・組織を横断する形で、相互に連関する要素が大きく、異なる分野同士の組織による相互連絡・コーディネーションは重要であるが、この点でも、既存の機関・枠組みはほとんど機能していないといえる。

3.3 あるべき国際協力の枠組みについての考察

今後のあるべき協力の枠組み



以上の分析に基づいて、今後のあるべき国際協力の枠組みについて若干の考察を試みた。

大きな戦略としては、一気にグローバルな協力枠組みを全体として統合的に実現することには無理があり、現実性をもたない。そうではなく、政策、法制度、技術標準化、運用などの各分野のそれぞれにおいて、地域内なカバレージを高め、その集積のもとにグローバルな体制を構築していくことが重要であるといえる。たとえば運用面では、CERT、FISRT を通して一定の連携があるが、アフリカはカバーされていないし、政府や民間企業などの関与にもバラつきが大きく、十分な体制とはなっていない。また、インターネットでいえば、通信事業者、ISP など、レイヤー単位での連携は比較的存在しているが、レイヤーを超えた連携となると、公的な形になったものはほとんど存在していない。同様のことは、ITU や ISO などにおいてもあてはまり、通信事業者・ベンダー中心の通信プロトコルのセキュリティ標準化と、情報システムベンダー、ユーザー企業が中心の企業システムのセキュリティ標準化との連携は薄い。産業システム、インフラ分野の連携も、同様にして、業種毎では多少存在しているが、地域的にも国境を超えたものはまだほとんど実体はない。

同時に、分野を横断してのグローバルな連絡・調整の仕組みも、必要といえる。これについては、現在はそうした枠組みはまったく存在していないといえる。

ただし、現在そうした枠組みが存在していないということは、相応の理由があってのことであり、それらが容易に克服されると考えるのは難しいのというのも現実である。

そこで、国際協力のあるべき姿そのものについて、当事者を中心として広範な主体によって検討を重ね、方向性について合意を見出す努力をすることが必要かつ有効と思われる。

この点、世界情報社会サミット（WSIS）から派生したインターネットガバナンス・フォーラム（IGF）

は、理論的にはそうした場になる可能性をもっている。ただし、実際には政治的な立場を強くもって参加している主体が多く、セキュリティに関する認識の違いも大きく、生産的な議論ができる可能性はまだまだ低いといわざるをえない。

むしろ、当初は、国際協力の枠組みについて、どのような方向、工程で、何を進めていけばいいかの検討を、グローバルに、しかし少数の専門家を集めて叡智を結集することから始めることが望ましいのではないかと考えられる。

1990年代の前半、インターネットが急速にその存在を拡大していったときに、アスペン研究所が中心になって「国際通信ラウンドテーブル」や、「インターネット政策プロジェクト」など、欧米、アジアの政策担当者、有識者などを25名程度集めて、「賢人会議」が行われていた。これは非公式な集まりとはいえ、その後のICANNの形成やそれをめぐる政策議論の土台を作る上で相当の役割を果たしていたのである。

情報セキュリティに関しても、同様にして、参加者について当初は慎重に人選を行って少数精鋭を集め、グローバルに、どのようなステップを踏めばあるべき国際協力の枠組作りが可能かを非公式に、しかし真剣に検討する試みが必要かつ有効と考えられる。

これらの点については、具体化に向けて今後引き続き検討することが必要と考えるものである。

4. 欧米主要政府のサイバーセキュリティ政策の動向

以下に欧米の主要政府のサイバーセキュリティ政策の動向についての調査結果を記す。

4.1 全般の傾向　サイバーセキュリティ政策の強化

全般的な傾向として、調査の対象とした各国政府のサイバーセキュリティに関する政策的な取組みは、明らかに強化されている。これは予算、産業政策、法制度および企業ガバナンスのいずれの面でも共通する傾向だった。

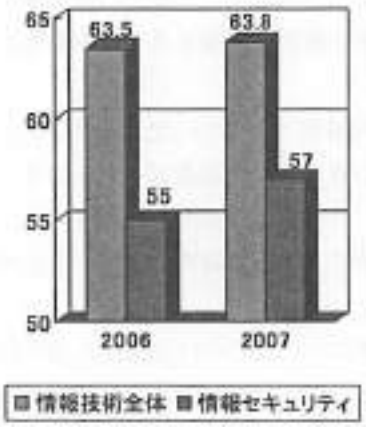
サイバーセキュリティにかかわる予算は、大きく政府内部の情報システムのセキュリティ対策と社会全般に対する政策推進の二種類に分けられるが、とくに後者はほぼすべての政府で増額されている。

そもそも、「サイバーセキュリティ政策」の範囲や基準が各国で共通になっているわけではない。また、予算についての情報が公開されているとは限らない。米国政府は情報公開が進んでいて、相当詳細な情報が入手できた。韓国も、調査に協力してくれた韓国政府のインターネット情報安全振興院（KISA）のおかげでかなり詳しいデータが入手できた。一方、ドイツ、イギリス、フランスなどは非公式で入手できたものも含めて情報が限定されていた。イタリアはほとんど予算が入手できなかった。従って、サイバーセキュリティに関する政府予算の絶対額は、国により相当異なる。

図1は、アメリカ政府の情報技術全体についての予算額と、そのうちのサイバーセキュリティの予算額を示したものである。総額で57億ドル（約7000億円）となっている。うち、政府内部の情報システムに関する予算がおよそ50億ドル強とされ、いわゆる政策予算は20億ドル（2400億円）とみられる。

情報技術全体は伸びていないが、セキュリティだけは4%近い伸びであることがわかる。

図　アメリカ政府の情報技術全体の予算とサイバーセキュリティ予算



一方、日本政府は、平成18年度のサイバーセキュリティに関連予算として、総額319億円と発表している。ただし、これには、通常のシステム管理のセキュリティ施策予算など、単独で抽出するのが困難な額は含まれていない。単純に比較すれば、米国の10分の1程度の額といえるだろう。

因みに、日本政府のIT関連予算の総額は、1兆3115億円と発表されている。これは「高度情報通信ネットワーク社会の形成に関する予算」である。

韓国は、2006年度のサイバーセキュリティに関する政府予算が、総額7千920万米ドル、約100億円ほどである。日本の3分の1、米国の30分の1となる。

産業政策では、米国、イギリス、ドイツは「基本的には民間に任せる」との立場を明らかにしたが、実態を調べると、これらの国でも技術分野の研究開発を中心に、なんらかの形の産業支援策を講じていた。2006年にイギリスで国民IDカードの実施が決定されたが、これも広い意味での産業政策といえる。

米国では、連邦政府の全省庁にサイバーセキュリティ対策が義務付けられ、政府共通IDカードや国防分野の調達も含めて、政府調達市場全体を通してサイバーセキュリティ産業への実質的な支援策が実施されているといえる。ドイツはサイバーセキュリティ産業の海外進出を積極支援している。

フランスでは、政府がサイバーセキュリティに関する産業政策の推進を提唱し、技術開発分野で「地域クラスター」プロジェクトなどの動きがある。

韓国、シンガポールの政府も、技術開発、企業支援などの産業政策を積極的に推進しているとみられる。

なお、有識者からは、政府に対して研究分野の長期戦略プロジェクトの支援、人材育成支援などの施策を求める意見が出された。国際的な標準化への取組みの推進を求める意見もあがっている。

4.2 官民のパートナーシップの推進

サイバーセキュリティ政策においては、官民のパートナーシップが推進されていることも特徴的であった。ヨーロッパのイギリス、ドイツ、フランスなどでとくにその傾向が強い。米国も、業界団体などとの緩やかな連携が進められている。韓国、シンガポールでは政府主導の動きが強く、民間部門はこれに追随する傾向がある。

官民連携の典型な取組み事例としては、コンピューター障害・事故に対する対応組織、CERT・CSIRTがあげられる。

民間の自主基準が事実上の規制として影響力をもつ動きもある。たとえばクレジットカード業界によるPCI（Payment Card Industry）標準などである。金融機関に対する国際的な規制、バーゼルIIも、サイバーセキュリティに関するリスク管理を求めることから、今後影響力が強まるとみられる。ただし、その影響範囲については、金融機関に留まるとの見方と、融資対象となる広範な企業群に拡大するとの見方に分かれた。

また、欧米の多国籍企業や広く国際展開する日本企業からは、現在は国・地域・業種によって様々に異なる法制度、規制、標準が並存し、それらに個別対応することに多大なコストがかかるため、各国政府・国際機関に、国際的な協調、制度の統合やハーモナイゼーションの推進を求める意見が強く出された。

4.3 米国が先行する法制度整備

法制度の整備・実施においては、各国で共通の方向性が推進されているとは必ずしもいえないが、広範な展開がなされていることは事実である。ドイツや米国のように連邦政府と州政府で法制度が分立されているところもあり、個人情報保護法や企業の内部統制法などの施策をみても、法制度には各国の歴史的、社会的、文化的な背景の相違が明確に現れている。

アメリカでは、金融、医療などの特定業界を対象とした業法規制に加えて、SOX法によって企業活動全般への内部統制の観点からサイバーセキュリティ施策の実施を事実上義務付ける法律が施行され、企業に大きな影響を与えている。また連邦政府機関にサイバーセキュリティ施策の推進・報告を義務づけるFISMAは民間企業にも強い影響力をもっている。

SOX法に対しては、経営への負担が強すぎるとの指摘があったが、サイバーセキュリティ専門家の間にはセキュリティ施策の推進に効果的だと評価する意見が強かった。施行から間もないこともあって、コスト増加につながる解釈・運用上の曖昧さを解消してほしいとの意見も強かった。

ヨーロッパには直接SOX法に該当するような法的規制は、いまのところ存在していない。一方、EU指令により個人情報保護の法制化が進んでいる。また、2006年に固定・携帯電話会社、ISPなどの通信事業者に対してデータ保存を義務付けるEU指令が可決され、今後各国で法制度化が進むことになる。

韓国では、SOX法に該当する法律は存在していない。サイバーセキュリティ全般に関しては、通信事業者への対策を求める法律などが整備されている。シンガポールでもサイバーセキュリティに関する包括法は、現在は存在していない。ただし、「サイバーセキュリティマスタープラン」を策定しているところから、今後法制度も含めた整備が進む可能性は高い。

4.4 プライバシー保護、個人情報保護とセキュリティの一体化

従来は、「プライバシー保護」政策、すなわち個人の情報にかかわる権利を濫用から守ることを主たる目的とする政策と、サイバーセキュリティに関する政策とは別のものととらえる傾向が強かった。前者は人権意識に基づき、国家や企業から個人を保護する色彩が強いのに対して、後者はナショナルセキュリティなど、国家や社会の安全確保を重点として、個人の権利保護の優先順位は相対的には低いとみられてきた。

しかし、とくに最近になって、インターネット経由などで顧客データなど個人情報の大量漏洩事件が頻発し、直接・間接の被害額が巨大なものとなる傾向が強くなってきたため、個人情報保護の推進策はサイバーセキュリティ施策と密接な関係にあるとの認識が政府、専門家、企業担当者などの間に共通に形成され、その方向での施策も推進されていることが、本調査によっても明確に実証された。

米国では、連邦レベルの個人情報保護法が未成立で、個人情報保護のEU指令の実施を各国で推進しているヨーロッパとは状況が異なっている。しかし、州レベルの立法化の推進と連邦取引委員会（FTC）の規制強化によって、企業組織による個人情報保護策の推進はセキュリティ施策の一部として不可避となった。

ヨーロッパは、個人情報保護が先行してきたが、最近ではその一環として企業にサイバーセキュリティ施策を義務付ける傾向がみられる。アジアでは個人情報保護に関する政策的措置は遅れているが、韓国の国会で個人情報保護法案が審議中であるなど、今後は対応が進むとみられる。

4.5 企業のガバナンスの進展

企業のガバナンス面でのサイバーセキュリティへの取組みは、全般には従来の個別的、技術的対策を中心としたものから、より包括的、組織的な対応を重視する方向へと移行しつつある。本調査では、組織的対応と技術的対応に分けて調査したが、究極的には相互に関連が深いと考えるべきであろう。

・組織的対応

組織的対応の面では、様々なコンプライアンス（法律遵守）の要請の高まりに応じ、内部統制を強化し、社内組織を改変する動きがみられる。この点で、企業のサイバーセキュリティへの取組みを総合的なリスクマネジメントの一部として位置づける動きが注目される。その一環として、個人情報保護対策をサイバーセキュリティの一環として取組みを強化する企業も増加している。事故もしくは犯罪によって顧客データなどの個人情報が大量漏洩する事件が続発しており、事故を起こした企業には、損害賠償、訴訟対応などで多額の費用が発生することに加えて、事故が公表されることで社会的な信頼が大幅に低下し、株価の低落、顧客減少などにより事業継続が困難になるといったリスクが意識されるようになったためである。

こうしたガバナンス意識の高まりから、各種の国際標準・認証を採用する企業は増えている。ISMSについては、これまでは日本の事業者が世界的にも突出して認定を獲得してきたが、最近は欧米でもISO標準を採用する企業は増加している。なお、認定取得に伴うコストについて負担軽減策を求める意見も多かった。

サイバーセキュリティへの取組みは、各国によって状況が異なっている。米国におけるSOX法の実施は米国企業および米国に上場している外国企業に直接の影響を与えることに加えて、米国企業とサプライチェーンで結ばれている他国の企業にも間接的な影響をもたらしている。

米国、ヨーロッパとも、サイバーセキュリティ管理の国際標準であるBS7799、ISO17799、ISO27000シリーズを採用する企業が増加している。コストがかかる認証までは取得しないが、社内基準として実質的に採用する企業が多い。

モニタリング、外部監査は、業種による取組みの格差が大きく、全般にはようやく重要性が認識され始めた段階である。とくに外部監査には、コストが高く予算がとりにくいとの指摘もある。日本では、サイバーセキュリティ監査とともに、事業継続計画の採用についても欧米と比較して立ち遅れているが、企業の必要性への認識は増加している。

韓国やシンガポールでは、政府がサイバーセキュリティ施策の一環として企業のガバナンス対策に取り組む動きは、本調査ではほとんど見られなかった。ただし、多国籍企業や米国上場企業と取引のある企業では、SOX法の影響を受けて対応を進める動きはある。韓国ではISMS、BS7799の認定を受ける企業もあるが、通信や電力などのインフラ企業などに限られ、その他の分野の企業はまだ少ない。

・技術的対応

企業のサイバーセキュリティガバナンスに関する技術的対応策は、次の3種に分類できる。

1）内的脅威対策

2）外的脅威対策

3）法手続き上の対策

内的脅威とは、内部的な犯罪や不正行為を指し、外的脅威とは、外部からの侵入によるデータの盗用・漏洩・改ざん、システム破壊などである。法手続き上の対策とは、犯罪や訴訟に備えて、証拠能力のある電子データの保全、関連する電子的情報の抽出などの技術的対策である。

従来のサイバーセキュリティへの技術的対策・ツールは、外的脅威への対応が中心で、内的脅威は、社員のモラル、社員教育の問題として捉えられがちで、技術的な対策はあまりとられてこなかった。

しかし、最近米国のSOX法にみられるように内部統制の強化が義務付けられる傾向が強まってきたことから、社員の行動の監視機能、情報やデータの変更の検知・追跡機能、監査支援機能などが求められ、そのための製品が登場している。SOX法対応をうたった製品、全社的に情報・データを管理するECM（Enterprise Contents Management）、情報やデータの正当性を証明し、犯罪行為などの追跡を可能とするフォレンジックスなどの製品である。

外的脅威への対応製品は従来から多種存在しているが、最近は大容量のデータ媒体を事故や盗難によって消失しても安全を確保できる暗号化などの製品が注目されている。

法手続き上の対策は、狭義のサイバーセキュリティ技術には分類されないが、製品としては、ECMやフォレンジックス関連製品が該当する。

内的脅威対策は、技術自体が未成熟なためインハウス開発が中心で、ECMやフォレンジクスなどのツールが部分的に利用されている。SOX法対応製品については、評価がまだ定まっていない。

法手続き上の対策は、必要性についての認知度が低く、製品仕様の作成も困難な状況である。したがって、まず問題の存在自体を啓発する活動が必要と思われる。またガイドラインの作成／広報など、対応製品の開発を促す施策も望まれる。

ハイパーネットワーク2006ワークショップ

園田　和孝

◆ネット社会論2006：徹底検証Web 2.0、OSS、NGN、IPv6…

ハイパーネットワーク社会研究所が、「リゾート＆リサーチ」を合言葉に1993年の設立以来開催してきたワークショップを、別府湾が一望できる日出町の「ウェルサンピア大分日出」で、11月9日～10日に開催した。1990年の「日出会議」と同じ場所の開催ということもあり、懐かしむ方々も多くおられた。今回のワークショップでは、近年のインターネット利用形態が、ウェブの進化とともに変わってきたところにスポットをあて、"Web 2.0"の掘り下げから、それを支えるオープンソース・ソフトウェア（OSS）の意義と課題、情報社会の基礎となる生き方、モラル、コンテンツ制作、さらに未来技術としての次世代ネットワーク（NGN）からIPv6の社会的な課題まで多岐に渡るテーマを取り上げた。「技術論」だけではなく「社会論」として、また地域（ローカル）とグローバルな視野の双方をもちながら、広く、深く、次世代のネット社会への道筋を徹底検証するという趣旨だった。「リゾート＆リサーチ」の「リゾート」部分では、10日早朝には、日出町郷土史愛好会会員副会長の魚住修三氏、日本野鳥の会大分県支部事務局の幸徳行氏、岩尾建氏、岩尾淳子氏ら地元ガイドの方々のご協力を得て、「糸ヶ浜海岸のウォーキング」を行った。前日遅くまで議論（夜なべ談義）がなされたにもかかわらず、30数名もの参加者にお集まり頂いた。海辺の自然と新鮮な空気を満喫し、続く午前の会議には、瑞々しい感覚をもって臨むことができたと、大変好評だった。

延べ15時間、20名の発表者と70名の参加者、合計90名で行われた今回のワークショップについて、プログラム順に報告を行うこととする。

延べ14時間、30名の発表者と150名を超える参加者が、以下の問いを囲んで議論した。

「Ｗｅｂ進化論をどう読む？」

「OSSは地域を、行政を、社会をどう変えるか？」

「ビデオプレゼン」

「私たちが求めるネット社会とは？」

「NGNとIPｖ6で社会の何が変わるの？」

「見えてきたか、2006年のネット社会論」

会議の内容は以下に続くページで詳しく報告するが、全体像を掴んで頂くために、冒頭の部分を最初に紹介しておくこととする。

冒頭、当研究所の宇津宮孝一所長は、「1990年の日出会議の原点に立ち返り、同年に取り上げられたハイパーネットワークに関する議論が、現在の技術的なパラダイムへどのように繋がっているのかを、社会論的な立場から活発に議論し、大分という地から新たな展開がなされるよう」と呼びかけ、これに沿った形で徹底検証が行われた。

◆セッション1

コーディネーターの会津泉副所長と関口和一氏よりウェブ2.0の現状とメディアについて、軽快なトークで語って頂き、次に当研究所理事長の公文俊平氏より、現在進行しつつある産業と情報の新た

な局面から情報社会の進展のご紹介とウェブ 2.0 を語ることの重要性を語った。次に米 Socialtext 社 CTO（最高技術責任者）であるピーター・カミンスキー氏は、ネットづくりの最大の目的は、人々をつなげる事にあると説明をした。それから Wiki と Socialtext の相違点の紹介とデモを披瀝して利点について語った。次に 1976 年生まれでワークショップの発表者の中で最若手であるフォートラベル社代表取締役社長の津田全泰氏より、ネット旅行ベンチャー企業の 2003 年 10 月設立時より旅行メディアとして No.1 の閲覧者獲得にいたる今日までを語った。本セッションを締め括る最後のスピーカーとして、『グーグル Google 既存のビジネスを破壊する』の著者として知られる佐々木俊尚氏にロングテールやソーシャライズといった現象、データベース極大化と進んでいっている状況の説明と有用な情報をどう拾いあげるか、アキーテクチャの仕組みをどうするのかといった今後の問題提起もした。以上の発表を受けて、参加者と現在進行しつつあるネット社会の実情に基づいた上で、今後予想されるウェブの進化について活発な議論を行なった。

◆セッション 2

長崎県 CIO 島村秀世氏に、なぜ OSS なのか？OSS は何をもらすか？について語った。「OSS 導入以前の行政系システムのシェアは 99%以上を大手企業が握っており、地場企業はその下請けや運用での参入で、1%未満という状態であった。しかし OSS が普及し始めてくると大手と地場のシェアに変化が表れるようになったことから、OSS は地域産業が生き残ることが可能な道具となり得るという見方ができる」という意見を述べた。また行政側の変化として「OSS 化を進めシステムを独自開発することでコスト 81%減を達成し、OSS を導入して開発をやらざるを得ない状況ができてきた。しかし、PDCA を実践して改善し、失敗できる環境を用意し、失敗が減点につながらないようにすることも必要で、OSS 導入により地域は活性化する可能性があるが、地域内部の人が変わらなければ何も変化していかないこと」を強く唱えた。次に大分県システム全体最適化の取組みを大分県企画振興部 IT 推進課長の山戸康弘氏が語った。情報システムの課題について業者の独自ツールの利用や、業者のメンテナンス問題等の課題を挙げ、これらの問題を解決すべくシステム全体最適化に取組んでいると背景を説明した。取組み内容はサーバ統合、OSS 共通基盤決裁システム構築、統一ルール導入、実施体制整備の４つを柱に強力に推進していくことを語った。今後は分割発注方式にもチャレンジし、IT 推進課がシステムの開発・運用に全体的に関与していくとのことで大分県のシステム最適化へ更に期待がよせられる。ネットワーク応用通信研究所代表取締役の井上悟氏からは島根県における OSS への取組みについて語った。「Java の 10 倍の生産性を実現と噂される Ruby on Rails が出現し、Ruby on Rails 市場拡大へ取組んでいる。」と述べ、当日まだ発売開始したばかりの Ruby on Rails の開発環境である Rails Platform のデモンストレーションを行なった。デモからは生産性の高さが感じられ、今後の Rails Platform、Ruby on Rails の動向が注目される。津久見市秘書課の戸田尊道氏には OSS デスクトップのネットワークブート環境下での 2005 年度 IPA 実証実験について語った。津久見市が実証実験に求めたものは日常業務において実用的に利用可能である、コストやセキュリティ等の課題を解決できる、Windows 環境からの移行が容易であることの３点で、ワープロ、表計算ソフト等の一般事務処理について実証を行い、HTTP-FUSE KNOPPIX によるシンクライアント環境を構築した。運用後に実施したアンケート集計によると“今後も職場の特定業務に利用してみたいか？”“検証したアプリ（OpenOffice、Firefox、Nvu、QCAD）は既存と併用であれば業務に置き換え可能か？”に対する回答はいずれも半数以上と良好であった。逆に日本語変換への不満、データ受渡し、既存データ再利用等の解決すべき課題も見えてきたとの説明があった。

◆ビデオ

1日目のセッションが終了し、夕食を兼ねた交流会を行いお互いに親睦を深めた後、和やかな雰囲気の中でビデオプレゼンが始まった。このビデオプレゼンはハイパーネットワーク社会研究所が平成17年度の中小企業庁委託事業で制作したビデオ「情報モラルが会社を救う　～IT時代の社会的責任～」をワークショップに来て頂いた方々にも広く知ってもらおうと企画したものである。ビデオプレゼンを行うにあたって、ビデオの企画・制作を勤めた渡辺律子氏と映像の専門家である狩谷新氏に、ビデオの上映とともに狙いや苦労した点などを語った。

◆スペシャルセッション

「私たちが求めるネット社会とは？」をテーマに、LOHASプロデューサーの大和田氏とハイパー研の渡辺の進行で議論が行われた。はじめに、大和田順子氏から発表があった。大和田氏は、2002年に日本に初めてLOHASを紹介した方である。『LOHASとは、体の健康、心の健康に加え、社会・地球の健康を考えることであり、特に持続可能な社会をめざす:サステナビリティの概念が重要である。現在、個人のライフスタイルだけでなく、企業の価値観、経営方針などを考える際にも、LOHAS的な考えが求められるようになった。世の中を変えていくのは私たち一人ひとりであり、どうやって情報を収集し、判断し、行動していくかがロハスの考え方の基本でもある。持続可能な社会を実現するために、毎日の生活や仕事の中でどうしていかなければならないかを問題提議したい』。次に、NPO法人パワーウェーブ日出　理事長の小野町子氏から、『日出町は、7～8割が県外からの転勤者であるため、ITをツールとして地域の中でコミュニケーションが出来ればと考え、マイクロソフトの社会貢献プログラムUP事業として「日出町・子育て支援UPプログラム」を始めた。日出町、社会福祉協議会、パワーウェーブ日出、3団体の共同で地域の活性化事業として進めている。高齢者UPでは、50歳以上のコミュニティ活動として、生活に役立てるIT講座などを行ってきた。また、障害者UPでは、障害者小規模作業所による就労の推進に取り組み、地域の人たちと通所する人のコミュニケーションも活発になった。さらに、視覚障害者当事者による講座実施に1年掛けて取り組んだ。こうした取り組みにより、マッサージ以外の就労の道を推進していきたい。』などの発表があった。最後に、じんわり村の村長である木本直實氏が発表した。『現在、じんわり村、というネットショップで食べ物を販売している。村長が「すごい」と感動したものだけを売っている。農薬を使わずに育てた野菜や米、天然酵母のパン、自然の塩、素材にこだわったスイーツなど、体にもよく栄養もあり、環境にもよいものを選んでいる。2000年に神戸から杵築市へ転勤してきた際、大分の自然の大きさ、魚・農作物が美味しいことに驚いた。生産者の事情と消費者の事情、両方解かっている自分がパイプ役になりをそれぞれに伝えることができればと考え、「村長」という存在をキャラクタライジングし、信頼性をあげるために、HPで自分自身の情報を発信したり、ブログを書いたり、スカイプをしたりと、ネットを活用している。』会場からは、LOHASの考え方や、発表者の取り組み事例について、感想や意見が出され、リラックスした雰囲気であったが、真剣な議論が交わされたセッションになった。

◆セッション3

「未来技術の社会的課題：NGNとIPv6で何が変わるの？」をテーマに、3つの発表をもとに、インテック・ネットコア代表取締役荒野氏、ハイパー研の青木の進行で議論を行なった。荒野高志氏より「ＮＧＮとは」と題して、NGNの概要とNGNが構成すべき機能、及びインターフェイスの概要を話された。NGNの本質については多くの人達が定義されている。例えば、固定電話と携帯電話の融合である。インターネット、音声、映像のバンドルしたサービスである等がある。また、荒野高志氏独自の見解も述べた。次にNTT第三部門担当部長チーフプロデューサの影井氏から、セキュリティ面から捉え、

インターネット後では、やっと電話を追い越せる機能となった。次の世代に求めるものは何か、または提供できるものは何かと考えた場合、確実に、目指す相手に対して接続または接続拒否できる。通信内容や重要な内容を漏洩や破壊から守るなどが機能すれば、社会に役立つものになると思われる等のお話を受けて討議に入った。現在のネットワークにおける実態の保障、IPアドレスが本人の見えないところで管理されている不安の感はあるが、ある範囲のクローズされたネットワーク内での利用であれば、うまく使い分けたインターネットに利用になる等の意見が出た。次に、日本ンターネットプロバイダー協会副会長の立石氏から「地方ISPからみたNGN」と題して、今までアメリカで作られた物をベースに今後のＮＧＮ用アプリケーションを使う。果たして日本の土壌で育つのか。または、日本国中インターネットが使える地域が100%あるわけではなく、デジタルデバイドのことを考えるとＮＧＮのサービスを受けられなくなる人々が出てくる。どういう風にすれば、日本中の情報化に役に立つのか。地方の過疎の地域でNGNが役に立つのかどうか、現在のところ明確になっていない。また、大分のケーブルテレビの実情を踏まえた内容で川上氏30Mbpsの高速インターネットビジネスを展開している。地方では初めて新サービスであるケーブルモデムでの120Mbps実現を目指している。IPv6に推移していくと地方でのビジネスが広がってくると思われる。当時のＡＤＳＬのユーザである藤野氏からユーザの意見として、ポケットマネーで払える安価な料金でないと利用者にとってのサービスとしては厳しい等の意見があった。他方、今の電話トラフィックが増大し、電話網のメンテナンス費用にお金をかけるよりは、新しい仕組みに乗り換えた方が効率的な経営とサービスが提供できるとの意見もあった。大分県下では携帯電話不貫地域があり、ある町では、ブロードバンドがない地域がある。全ての地域に光ケーブル化する必要があるのか。高齢化率４０％もあり、電話に関心がない、インターネットなどコンピュータを意識しなくて、高齢者などを救済する仕組みがIPv6の利点を活かして実現できるのではないかと思うなどの意見が出た。

◆セッション4

二日間のまとめでもあるこのセッションでは、ハイパーネットワーク社会研究所の会津泉吹く所長より、コンピュータとネット社会について、グローバルな観点から、また、社会状況の変化とともに今までどう変わってきたのか振り返り「で、これからどうなるの?」という問題定義を行い、今後のユビキタス化するネットワーク社会では、新しいガバナンスが必要になり、またプライバシーとセキュリティ統合へ向けての話やインターネットガバナンスがWSISにおける、最も大きな対立点になるのではないかと述べた。ガバナンスには、第一にインターネット全体のガバナンス、第二に社会のガバナンス、そして第三にガバメントのガバナンスの三つがあり、それを踏まえた上で、なぜガバナンスがデジタルデバイドなどの著しい途上国で重要なのかという点について説明を行った。続いて、セキュリティ調査の話や、IPv6とNGNに関する標準化について多岐に渡る話をし、この種の議論には技術者の登場する機会が多く、偏ったものになることへの懸念と今後はもっと全体的に見ていく必要性があることを指摘し盛況のうちに無事終了する事ができた。

●報告感想

今回ワークショップを終え振り返ってみると、正直なところ「こうすればよかった」と思うところがある。それでも無事開催できたのは、このワークショップに携わっていただいた方ならびにご参加者の皆様のご協力の賜物であり「お蔭様で」という言葉を、私自身改めて身にしみて感じたところである。今、私達はデジタルという言葉とともに、急激な成長を迎えた。インターネット社会においてもウェブの進化とともに大きく変わろうとしている。今回のワークショップではその部分に焦点をあて論議し、少し先の未来も語り、徹底検証をしたわけだが、参加者の中からも様々な意見が出た。そ

の中で特に私が注目したのは、ウェブの使い方に疑問を投げかける異例的とも言える発言がいくつか上げられた事であった。これは非常に重要な声だとして、受け止める時期にきたのではないかと考えさせられた。同時に私自身アナログ部分的なものが多く残っている人間にとっては、とてもありがたいご意見でもあった。ウェブの進化によりユビキタスがもっと私達の身近になって来たのは事実である。それでもデジタルデバイドを考慮すると、ネットワークの部分では、まだまだ近づかなければならないと思っている。それでは世の中はどうだろうか？この 25 年で物は確かに豊富になったが、人間の心の豊かさは随分減ったように思える。同じような言葉を、講師の中で一番年長者である公文先生も語ったが、私と同じように感じ、豊かさに疑問を抱いているのは、私だけではないのだと強く感じた。それでは、これからのウェブとの付き合い方は？日本のウェブのあり方で、不思議なのは、どこまで使えるのかの議論が多く、どこまで利用し、どこを利用しないのかなどを決めていこうという動きを少なくとも、私はセキュリティやモラル意外に知らないし、あまり聞いた事がない。例えば、業務の効率化をうたい電子化するのがよいと思われがちだが、実際は紙ベースの方がベターだったりする。しかし現在、その発言自体がナンセンスにとられる傾向にある。今回、LOHAS 部分を取り入れた環境とネットワークの社会論でコラボレーションしたわけだが、その考え方はモラルにも、ガバナンスにも通じる部分があった。NGN や IPv6 の次世代のネットワークの世界を迎えようとしている私たちにとって、次世代の人達に『心地よい』本当に便利で、同時に豊かさを感じさせる選択をしていく準備の機会でもあったと考える。これからの社会論を論じていくうえで、人間のサポートツールとして、どこまでウェブを活用するのか例えば、どのシチュエーションで、どの範囲で、どのような対象を、どのような保護の仕方で、どのように活用していくのか「本当の豊かさ」を追求する為の IT 議論をこれからしていって欲しいと願った次第である。

ＩＴボランティアによる大分市地域情報化Ⅱ

大分県立芸術文化短期大学　　凍田　和美

はじめに

総務省の通信利用動向調査（平成１８年）によると、日本のインターネット人口は平成１７年の調査時点で 8,529 万人、人口普及率は 66.8%となっている（図１参照）。また、年代別のインターネット利用率をみると 6～12 歳は 65.9%、13～49 歳は 90%以上、50～59 歳は 75.3%、60 歳～64 歳は 55.2%がインターネットを利用しており、幅広い世代にインターネットが普及していることが分かる。特に、60 歳以上は平成１６年と比べて増加率が著しく高くなっている（図２参照）。

政府（高度情報通信ネットワーク社会推進戦略本部）は、平成１７年度までに世界最先端のＩＴ国家となることを目指して、平成１３年１月に「e-Japan 戦略」を策定した。さらに、ＩＴの利活用による「元気・安心・感動・便利」社会を目指すため、平成１５年７月に「e-Japan 戦略Ⅱ」を策定している。大分市が「大分市地域情報化計画」[1]を策定するなど、多くの市町村がＩＴを利活用するために情報化の計画を進めている。大分市中心部では、民間事業者等により早くからインターネットサービスが提供され、情報化に向けた基盤整備が進められた。今後は、ＩＴを利活用することにより、市民一人一人や市民団体・企業・行政などの地域の活動主体が、市民の生活を豊かにすることが求められる。平成１７、１８年度に、大分市地域情報化計画の一部である「インターネットを活用した市民活動支援」に、本学学生らがＩＴボランティアとして参加し、市内商店街の住民と共同で、商店街のホームページを作成した。

本研究では、ＩＴボランティアである本学学生と共に、大分市地域情報化計画に参画するなかで、地域情報化の課題となる要因や商店会の情報化の課題を明らかにする。また、住民が更新しやすいホームページについても考察する。

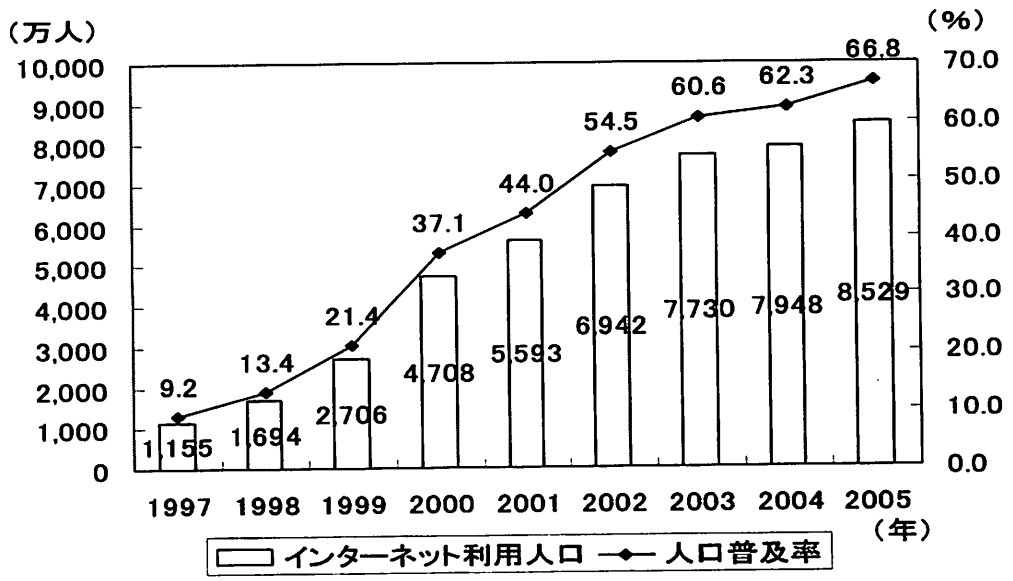


図１　インターネット利用者数・人口普及率[2]（総務省 18 年度版情報通信白書より）

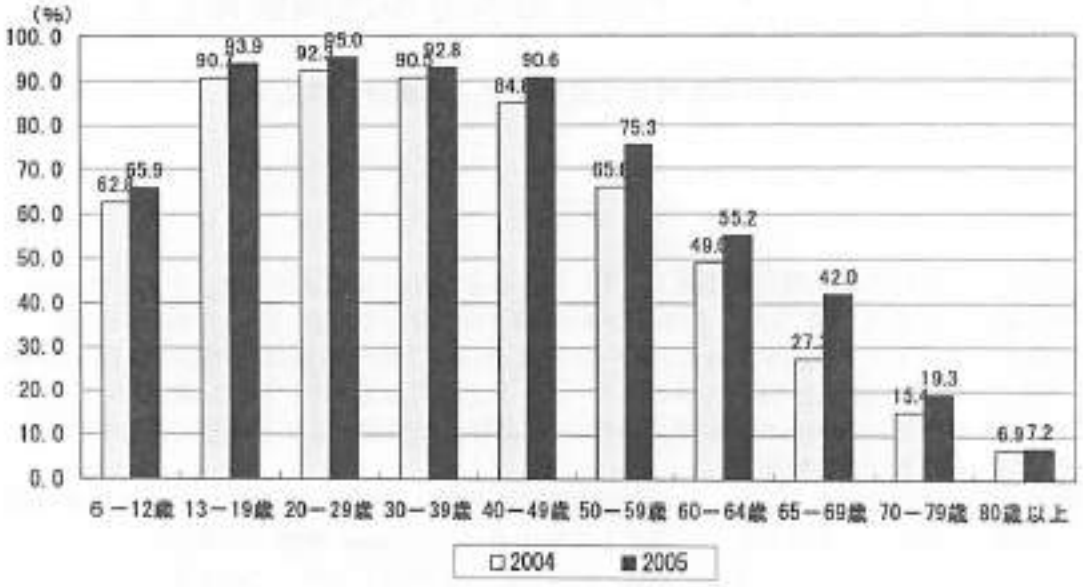


図２　年代別にみたインターネット利用率[3]

大分市の地域情報化

（１）大分市地域情報化計画の概要[1]

大分市地域情報化計画の趣旨は、市民や企業への情報のサービス内容や提供方法、市役所内部の情報化などについて方針と施策を明らかにし、情報化を実現することである。大分市地域情報化計画策定のために、①大分市民や大分市内企業の情報化の現状や要望を把握するためのアンケート調査、②大分市民や大分市内企業と協力・連携を深め、市民の声や民間企業のノウハウを取り入れながら進めていくための懇話会の開催（「大分市地域情報化懇話会」を設置、平成１５年４・８・11月の合計３回）、の２つを実施し多くの意見を大分市地域情報化計画に反映している。

計画実施期間は平成１６年度～平成２０年度、基本理念は<「つながる」「ひろがる」「創り出す」情報躍動都市ＯＩＴＡ>である。この理念に基づき施策の柱として「市民の情報化」「産業の情報化」「行政の情報化」「パートナーシップの創出」の４つの方向性を掲げている。

（２）情報化施策の４つの展開

大分市地域情報化計画は施策の４つの柱を基に、具体的な取り組みを策定している。「市民の情報化」は快適で豊かな市民生活の実現、「産業の情報化」は活力ある地域経済・産業の創造、「行政の情報化」は市民のための行政サービスの充実、「市民との協働」は市民とのパートナーシップの創出を目指している。

① 快適で豊かな市民生活の実現

施策の柱は、市民の情報リテラシーの向上を図る「ひとづくり」、市民生活の安全、利便、快適を支援する「まちづくり」である。

② 活力ある地域経済・産業の創造

施策の柱は、「ＩＴの活用による既存産業の活性化」「企業家支援」である。

③ 市民のための行政サービスの充実（電子自治体の構築）
施策の柱は、「行政サービスの向上」「業務の効率化」「庁内インフラの拡充」である。
④市民とのパートナーシップの創出
施策に、市民の市政参画、市民との協働、市民をささえる団体・人材育成支援などがあげられる。

（３）大分市情報化の状況[1]
大分市の地域情報化に関する取り組みは以下の通りである。
① 国の計画による整備
大分市は、昭和５９年にテクノポリス構想（旧通産省）の母都市と位置づけられて以来、ニューメディア・コミュニティ構想（旧通産省）、テレトピア構想（旧郵政省）、インテリジェント・シティー構想（旧建設省）、ハイビジョン・シティ構想（旧郵政省）等の指定を受け、高度情報通信技術の整備や各種システムの整備を進め、地域情報化の推進に取り組んでいる。
② 地域情報化に関わるシステムの稼動状況
テレトピア計画の推進等による在宅老人コミュニケーションシステム、市民図書館貸し出しシステム、大気汚染常時監視テレメーターシステム、公共施設案内・予約システム、大分市ホームページ、例規集検索システム、物品見積システム、議事録検索システムなどを構築し、市民サービスの向上を図っている。
③ＩＴ講習
平成１３年度に、e-Japan 戦略に基づいて、全ての国民の情報リテラシー向上のために学習機会を与えるＩＴ基礎技能講習会事業が全国で実施され、大分市でも多くの市民が受講した。講習はパソコンの基本操作やメール、インターネットの利用方法などを中心に行われ、その後も子供や親子、高齢者等を対象にした講習が公民館や情報学習センター等で行われている。

インターネットを活用した市民活動の支援

（１）ＩＴボランティア
市内大学の学生や市民からなるＩＴボランティアがホームページを作成することで、①市民がインターネットを積極的に利用した活発な活動を展開できる。また、②市民ポータルサイトの充実を図り、地域情報の発信とネットワーク化を推進できる。さらに、③住民の相互理解や産業の振興等、様々な市民活動を支援する。
ＩＴボランティアの役割は、①商店街のホームページ作成支援を行い、②商店街がホームページを自己管理できるように指導することである。大分市内の大学生や市民がＩＴボランティアとして、各団体の要望を聞き、それをホームページの企画や作成に反映させる。そして、インターネットにより全国に情報を発信し、その団体の活性化を図る。
平成１７年度は、日本文理大学の学生３名が佐賀関ツーリズム研究会、戸次本町街づくり推進協議会のホームページを、本学学生４名が西大分商店街と東大分商工振興会のホームページを作成した。平成１８年度は、本学学生３名が、富士見が丘商店会のホームページを、日本文理大学の３名が、ＮＰＯ法人岡原花咲かそう会のホームページを、大分大学の学生３名が大分県腎臓病協議会のホームページをそれぞれ作成支援する。本稿では、大分県立芸術文化短期大

学生が支援を行った西大分商店街、東大分商工振興会、富士見が丘商店会に対する活動について述べる。

（2）現地調査

平成１７年度は、西大分商店街と東大分商工振興会の現地で取材を行った。西大分商店街では、柞原八幡宮に行き、神社の様子を写真やビデオで撮影をした。浜の市（仲秋祭）にも参加し、祭りの様子を撮影した。また、現地の人に話を聞いたり、西大分駅周辺の景観を撮影したりした。東大分商工振興会では、萩原の夏祭りと朝市に参加し、それぞれの様子を撮影した。また、現地の人に話を聞くためにお店を一軒ずつ取材した。

平成１８年度は、富士見が丘商店会に行き、各店舗の人にＩＴボランティアの活動を伝えた。富士見が丘商店会の人は、直接の取材などが苦手な人が多いため、それぞれの店舗に手紙を送り、調査紙面を回収するとともにお店の人や店舗の外観を写真撮影した。

①西大分商店街

西大分駅周辺に１４店舗が存在している。上八幡には豊後一の宮である柞原八幡宮がある。宝物殿には国指定重要文化財や県指定重要文化財が所蔵されている。西大分駅近くにある柞原八幡宮仮宮では、志きし餅で有名な浜の市（仲秋祭）が毎年９月に行われる。浜の市の日は、民謡・神楽や花火などが催され、地元だけでなく多くの人々で賑わう。

② 東大分商工振興会

大分市萩原地区周辺に点在した２９店舗から成っている（平成 18 年 1 月 24 日現在）。飲食店・文具店・電気屋・印刷屋など幅広い分野のお店が振興会に参加している。元々は、まとまった商店街であったが道路拡張工事のための立ち退き後、店が散らばり現在の商工振興会が形成された。商工振興会の主催する行事に「夏祭り」と毎月第４日曜日に開催する「朝市」がある。12 月の朝市の餅つきには多くの人が訪れる。

③富士見が丘商店会

大分市富士見が丘団地の中にある。富士見が丘団地は広く、多くの市民が住んでいる。その中で富士見が丘商店会は、市民にとってなくてはならない存在である。商店会には、気さくな人が多く、温かい雰囲気を持った商店会である。富士見が丘商店会では、様々な行事を企画しており、住民の多くがそれに参加している。

（3）ホームページ作成

ホームページ作成には、ホームページ・ビルダーを使用した。掲載している写真は取材で撮影したものと商店街から借りた写真を使った。富士見が丘商店会では、代表者あいさつの音声を聞けるようにした。各ホームページの情報量と作成日数を表２に示す。

＜西大分商店街＞

ホームページには、柞原八幡宮，浜の市，志きし餅，お店紹介，写真，地図のメニューがある。トップページは、商店街の様子、浜の市の様子、柞原八幡宮の写真を使い、レトロをイメージして、フラッシュによる動画を作成した（図３）。

①「柞原八幡宮」と「浜の市」と「志きし餅」のページ

『郷土の歴史　生石風聞録』甲斐光：著の本を参考にそれぞれの歴史や由来を掲載した。

②「植木商事」のページ

店主の希望を聞き、ＦＡＸで注文出来るようにした。更新しやすいように注文書は画像にした。

③「地図」のページ

地図は、詳しいお店の位置が分かるように、Microsoft Word の図形描画の機能と Microsoft ペイントを使って作成した。

表1　現地調査

	西大分商店街	東大分商工振興会	富士見が丘商店会
調査日数	5日	8日	5日
内　　容	柞原八幡宮仮宮、かんたんサーカス、浜の市、神楽、出店、志きし餅、花火、試作ページ意見収集、道着の写真、駅周辺の景観の写真。	打ち合わせ、神社の写真、夏祭り取材、催し物、お店の取材、資料依頼、朝市取材、お店の取材、試作ページ意見収集。	朝市取材、店舗へあいさつ、店舗資料回収、各店舗の写真撮影、試作ページ閲覧、代表者の音声を録音。

表2　ホームページの情報量と作成日数の比較

	西大分商店街	東大分商工振興会	富士見が丘商店会
総ページ数	11ページ	25ページ	31ページ
写真の数	31枚	43枚	54枚
作成日数	3ヶ月程度	3ヶ月程度	3ヶ月程度

図3　西大分商店会のトップページ

④「写真」のページ

昔ながらの商店街の様子を出すために、西大分駅周辺を撮影した写真を掲載している。

＜東大分商工振興会＞

ホームページには、お店紹介，地図，朝市，夏祭りのメニューがある。商工振興会の人の意見を取り入れ、赤色を多く使用した。全てのページに統一感を出すために、同じデザインの画像をページの一番上につけた。フラッシュを用いた動画のイメージも「和風」にし、リ

図4　東大分商工振興会のトップページ

図5　富士見が丘商店会のトップページ

ンクボタンもあわせて作成した（図4参照）。

①「お店紹介」のページ

東大分商工振興会は２９店舗あるので、お店を「グルメ」「ライフ」「ショップ」「カルチャー・ホビー」の４つの分類に分け載せることにした。

②「朝市」「夏祭り」のページ

朝市と夏祭りは商工振興会が主催の大きな行事なので、掲載文や写真の選考に時間を要した。

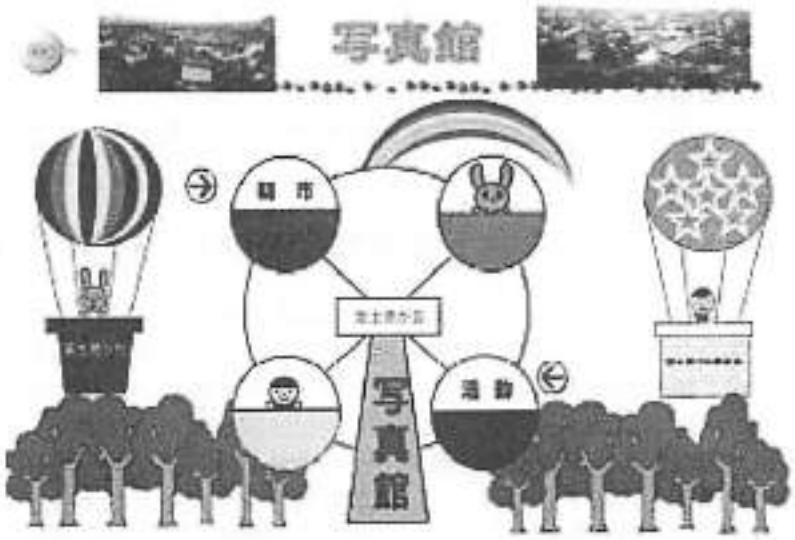


図６　「写真館」の「朝市」「夏祭り」のページ

③「地図」のページ
東大分商工振興会は店舗が荻原地区周辺に点在して、場所がわかりにくいため、詳しい地図が必要だった。小さな道が多く、複雑だったため
地図作成ソフトで作成することができなかった Microsoft Word と Microsoft ペイントを利用した。
＜富士見が丘商店会＞
各店舗の情報と、富士見が丘団地で行っている行事の情報を収集し、ホームページを作成した。トップページは、楽しい・賑やかなイメージになるように、気球・虹・風船・車・道路・マイクなどはウェブアートを利用した。気球は、両サイドに配置し飛んでいるように動きをつけた。背景は、イラストやボタンが見栄え良くするために白に設定した（図５参照）。
①「商店会マップ」のページ
　一つひとつのお店がわかりやすいようにイラストを取り込み、地図は、ペイントで描いた。お店の人のイラストをクリックすると、詳しい情報を見ることが出来る。
②「写真館」の《朝市》と《活動》のページ
　写真館のページは、朝市と活動にリンクできるように作成した（図６参照）。朝市のページは、売られている商品がわかりやすいように配置した。活動のページは、富士見が丘団地で行われている行事を掲載した。
③「会長あいさつ」のページ
　会長の写真を載せ、かつイラストを利用して親しみやすさを出すように心がけた。背景を取り入れた。
④「アクセス」のページ
　富士見が丘商店会の地図と、バスの時刻表を取り入れた。バスの時刻表は、大分交通バスのホームページへのリンクを付した。

考察

（1）大分市の地域情報化

ＩＴボランティアの活動を通して、学生も十分に地域情報化に参加できることが分かった。また、商店街（商工会）の人々がもつ以下の課題が明らかになった。

①情報化の効果が理解できていない

②ホームページ管理に必要なパソコンなどの情報機材やネットワークが揃っていない

③情報機材を扱える人がいない

商店街の事務所のパソコンで、試作ホームページを閲覧したが、商店街の人はパソコンの利用にまったく不慣れな人が多かった。情報を更新する場合も学生任せであり、商店街の人が地域情報化について消極的なようであった。アンケートを回収時の白紙の回答や写真の拒否があり、商店会の中にやる気が十分ではない人もいた。地域情報化を進めるためには、商店街の人たちが地域情報化に関する知識を深め、その効果を理解することが必要である。大分市も地域情報化計画を市民に十分説明して、意識を高めるべきだと考える。しかし、年度末に行った意識調査では、各商店街ともに、地域情報化に触れたことで各商店街の技術や知識が増えたように感じた。

（2）ＩＴボランティア

地域の取材とホームページ作成に時間がかかり、商店街の人たちが自分でホームページを管理できるように指導することは不十分であった。次のことが明らかになった。

① ホームページ作成の過程で教室では得られない意義を感じる勉強ができた

学生は授業でしかホームページを作成したことがなく、ホームページ作成のために必要な知識や経験が少なかった。そのため、ホームページ作成に予想以上に時間がかかったが、学生にとっては、教室では得られない意義を体験できる勉強ができた。

②地域社会に学生が参加し、地域の文化や生活に触れることができた。

授業では経験することのできない地域の方々との交流や、今まで知らなかった地域の行事やお店などを知ることができた。少人数で商店街のホームページを作成することは時間的に厳し面があった。人数が多ければ、作成するページの分担ができ作業がはかどったかと思う。

③商店街（商工会）の人々と予定合わせるのは難しい

学生の授業の日程と商店街の人の仕事の日程がなかなか合わず、実際に取材に行くまで時間がかかった。東大分商工振興会では、メールでやり取りをしたが、返信が届くまで日数がかかった。

（3）ホームページ作成

ホームページ作成途中に、他の学生、商店街の方、市役所の方に試作したホームページを見てもらいその結果による改善を行った。以下に改善した点を示す。

＜西大分商店街＞

①商店街の写真の追加：西大分商店街周辺の写真を入れたらどうかという意見があったので、西大分駅周辺の景観の写真を撮影しページを作成した。文字ばかりで見にくかったページには、写真を増やすことで読みやすくなるように工夫した。

②難しい漢字のふりがな付け：難しい漢字にふりがながほしいという意見があったので、子供や誰にでも読めるように漢字にふりがなをつけた。

③写真の明るさの強化：全体的に写真が暗く、商店街のイメージが暗かったので写真を明るくした。

＜東大分商工振興会＞
①動画に使用する写真の追加：東大分商工振興会の動画で使用している写真を増やした。
②お店の写真の追加：お店から要望のあったページしかお店の外観の写真を載せていなかったので、商工振興会の方と全てのお店を回り、全てのページにお店の外観の写真を載せた。
③朝市と祭りのページのデザイン変更：朝市と夏祭りのページは写真が並んでいるだけだという意見があったので、デザインを変更し、写真と文章を交互に表示した。また、全てのページを左揃えで作成していたので、中央揃えに変更した。
＜富士見が丘商店会＞
①トップページ：楽しい・賑やかなイメージで作りかえた。スクロールを不要にした。
②朝市ページ：デザインを変更し、商品を主に並べるようにした。そして、一つひとつの画像に、商品の名前を入力した。朝市の写真の大半が、無表情で写っている方の写真だったので、なるべく顔がはっきり写っていて、笑顔の写真を提供して頂いた。
③全体的に楽しさが出るように、ＢＧＭを取り込んだ。
④トップページで、ホームページの説明が出るように、声の挨拶を聞けるようにした。

（4）ウェブアクセシビリティ

高齢者や障害者など心身の機能に制約のある人もウェブ情報に利用できるウェブアクセシビリティに気を使った。「大分県ホームページ作成ガイドライン」[4]には、コンテンツを作成する際の技術的な基準が、①全体構成に関すること、②文字や色に関すること、③画像に関すること、④リンクに関すること、⑤その他、の５つに分類されて記されている。これを参考にして、商店街のホームページを作成に臨んだ。画面サイズは、左右スクロールを必要としないように 600～750 ピクセルに固定した。文字のサイズは、利用者側が自由に変更出来るように固定しなかった。読み上げソフト使用の際に画像の意味が分かるように、写真や図には alt 属性で図の意味を説明するテキストをつけた。利用者のブラウザの種類に関係なく動作するように、「Ｎｅｔｓｃａｐｅ」と「Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ」で閲覧を確認した。また、読み上げソフトを使用し、視覚障害者が使いやすいような検討を行った。使用したソフトは「ボイスサーフィン（体験版）」[5]である。読み上げソフトを使用した結果、①リンクが分かりにくい、②漢字の読み方が違う、の２つの問題が明らかになった。対応として、①リンクボタンにリンク先を alt 属性で「お店紹介」→「お店紹介へのリンク」に変更した、②単語ごとに空白を入れる、文章の分かりやすい位置で句読点をいれる、の２つにより改良した。

（5）ホームページの更新方法

商店街の人が各自でホームページの情報管理ができるように更新方法を検討した。

ページの編集には、①ホームページビルダーソフト、②Microsoft Word、③フリーソフト HTML エディタの３方法が考えられる。西大分商店街と東大分商工振興会では、ソフトを新たに購入する必要がなく、初心者でも使用しやすい Microsoft Word で更新する方法をとった。富士見が丘商店会は、事務所のパソコンにホームページ・ビルダーが入っていたので、これを使用することにした。画像・写真の変更方法では、画像・写真の拡大・縮小や画像・写真に文字を入れることが必要なので、Microsoft ペイントを使用することにした。ホームページの更新作業は、フリーソフトの FFFTP ソフトを使用することにした。

更新方法についての手順は、Microsoft Word を使用してプリントを作成し、そのプリントの内容は、実際にホームページ・ビルダーの画面を使用して、画像を挿入する例を挙げ、誰でも更新できるように図を多用した。ホームページの更新方法を各商店街の人に伝え、ア

ンケートを実施した。しかし、次年度になって、画像が欠落しているページやリンクができないページがあることが分かり、学生と共に前年度のホームページのアフターケアーを行った。今後は、更新など各商店街から質問などに、常に対応できる体制作りが必要だと感じた。

おわりに

地域の情報化は、その地域に住む全ての人が関心をもたなければ広がらない。本活動を進める過程で、地域の情報化を進めるには、①地域情報化計画を市民に十分に説明し、情報化の意義を地域住民が理解する、②情報機器利用率に不慣れな世代にＩＴ研修の場や講習会開催する、③学生や市民がＩＴボランティアとして参加する機会を増やし、市内商店街の住民と共同で、商店街のホームページを作成する、などの必要性が明らかになった。

一方、ＩＴボランティアとして、商店街のホームページ作成支援を行うことで、学生は、①住民の要望を集める難しさ、②要望を満たすホームページ作成の難しさ、③多くの人にとって、見やすいホームページ作成の困難さ、④高齢者や障害者など心身の機能に制約のある人に気を使ったホームページ作成の大切さ、⑤文字・静止画・動画・音声など、多様な情報の活用の大切さ、など、それまで、教室では得られない勉強ができた。

さらに、大分市の地域情報化計画に学生として参加することで、学生は、授業では経験することのできない地域の方々との交流や、今まで知らなかった地域の行事やお店などを知ることができた。お店の取材では、学生は、実際に商品を作る所、商品を作るための特別な機械などを見ることができた。また、参加したことのない行事に参加したことで、地域の行事の賑やかさを知り、昔から言い伝えられている話や代々受け継がれている山車に触れることができた。

今後の課題として、実際に視覚障害者に閲覧してもらいウェブアクセシビリティが十分かどうか確認する必要がある。また、商店街の人たちが容易に行えるホームページの更新方法の開発、商店街の人から質問などがある場合に、きちんと対応できる体制作りを早急に行うが必要である。

謝辞　学生が商店街のホームページを作成する機会を与えてくれた市役所の情報政策課の方々、ホームページ作成にご協力して頂いた商店街の方々に感謝いたします。また、ＩＴボランティアとして実際に大分市地域情報化に参加した、１７年度卒業研究生の佐藤麻代さん、清家美香さん、１８年度卒業研究生の河野愛さん、谷口理美さんに感謝します。

参考文献

［１］大分市：大分市地域情報化計画、情報化施策の展開、情報化を取り巻く状況
http://www.city.oita.oita.jp/
［２］社会実情データ図録：インターネット人口普及率推移と年齢別地域別利用率
http://www2.ttcn.ne.jp/~honkawa/6210
［３］総務省　http://www.soumu.go.jp/
［４］大分県ホームページ作成ガイドライン
http://www.pref.oita.jp/menu/guidelines/guidelines.html
［５］ボイスサーフィン
http://www.amedia.co.jp/product/vs3/

大分県内企業の情報化に関する調査

凍田　和美　　足立　若菜　　藤本　麻貴

大分県立芸術文化短期大学　情報コミュニケーション学科

研究の背景

コンピュータや通信技術が急速に進展し、ＩＴ（情報通信技術）が市民生活に浸透してきた。2006年度版情報通信白書によると、2005年のインターネットの世帯利用人口普及率は66.8%、インターネットの利用人口はおよそ8,529万人（対前年581万人増）と推定されている。一方、法人によるインターネットの利用状況については、2005年で97.6%の企業、85.7%の事業所がインターネットを導入済みとされている。ＩＴの浸透は企業間の関係を変容させるとともに、製品をユーザーに直接販売している企業にとっても、ＩＴを活用することにより販売力、営業力が強化される。国民生活のＩＴ化が進展する中で、消費者の新しいニーズを的確に捉え、迅速に対応していくためにも、企業にとってＩＴの活用は必要である。このような状況の中で、ＩＴ化を我が国の経済成長に結びつけるためには、大企業のみならず、企業数の９９%以上、雇用の約７０%を占める中小企業のＩＴ化が不可欠である。中小企業の健全な発展は経済面でも社会面でも重要である。しかし、統計的な観点からみると、一般的に中小企業は大企業に比べてＩＴ化が遅れている。図１と図２は、従業員別のＩＴ関連費用を示したものであるが、１企業あたりの費用（図１）が業種によって異なっている。しかし、１従業員あたりの費用（図２）でも、従業員数が大きいほうが大きくなっていることがわかる。規模（従業員数）が小さいと売上も少ないので、ＩＴの固定費的な費用が影響するからであると思うが、従業員数の少ないほうがＩＴ投資率は高くなっている。また、業種別にみると、当然であるが情報サービス業ではＩＴ投資率が高くなっている。従業員１人あたりのパソコンの装備率（図３）では、小売業では店舗現場が多くなるのが原因であると考えられる。従業員数が大きくなるにつれて減少しているが、一般的には従業員数が大きいほど、増大している。また、パソコンのＬＡＮ接続率（図４）では、１００人以上ではほとんどが接続しているのに、９９人以下では接続率が低くなっている。このように、企業規模によりＩＴ化の状況は大きく異なる。

本研究では、大分県内企業２５１社に対して企業の情報化とその取り組み状況の実態調査を行い、大分県内企業の情報化とその問題点を明らかにする。

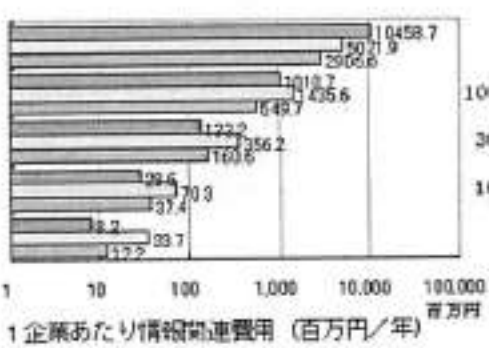
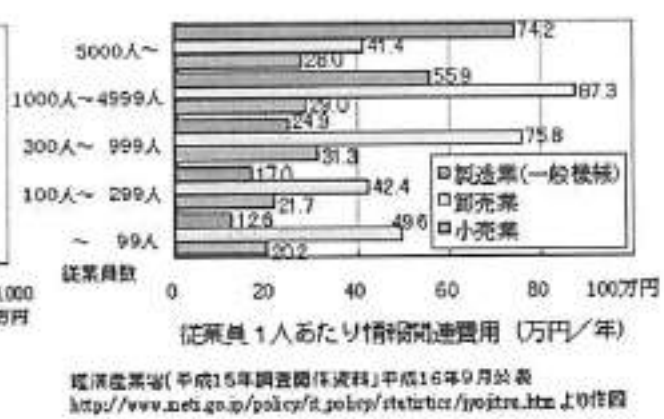
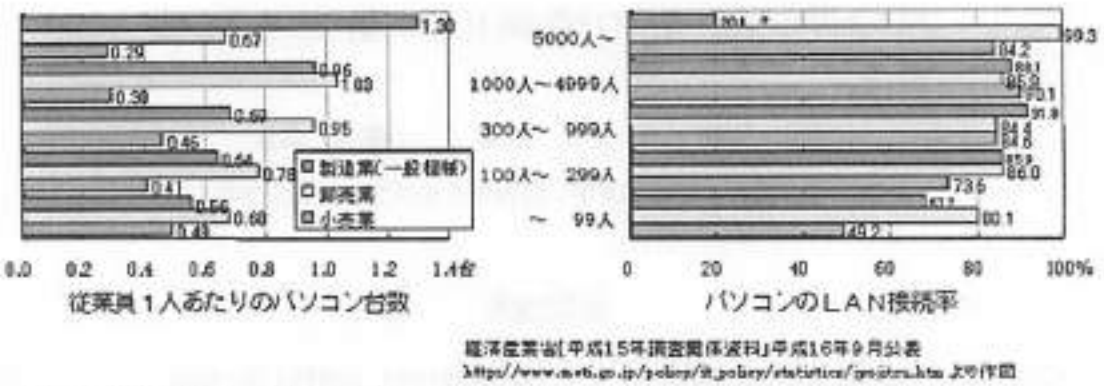


図１　１企業あたり情報関連費用



経済産業省（平成15年調査開示資料）平成16年9月公表
http://www.meti.go.jp/policy/it_policy/statistics/joji16.htm より作図

図２　従業員数１人あたり情報関連費用



経済産業省「平成15年調査関係資料」平成16年9月公表
http://www.meti.go.jp/policy/it_policy/statistics/pointo.htm より作図

図3　従業員１人あたりのパソコン台数　　図4　パソコンのＬＡＮ接続率

大分県内企業の情報化の実態調査

（1）調査の背景・目的

本調査は、大分県内企業の情報化の進行状態と問題点を明らかにすることを目的に行った。

（2）調査方法

①調査期間　：２００６年９月１日～１０月１５日
②調査対象　：従業員数５０～３００人以下・資本金５０００～３億円以下の２５１事業所
③調査方法　：紙面による調査（アンケート）

（3）調査内容

全国調査との比較が可能なように、２００３年に中小企業庁から受託して行った三菱総合研究所の調査と同じ設問を使った。調査内容は、①事業所や従業員、②情報化への取り組み、③パソコン導入、④電子メールアドレスの導入、⑤ＩＴ能力向上の取り組み、⑥ＩＴ導入の効果、⑦インターネットの利用、⑧電子商取引の実施、⑨ＩＴ導入の問題点、⑩セキュリティの方針、⑪セキュリティの方針と内容、⑫個人情報漏洩の問題、⑬個人情報の保護

（4）調査の状況

２００６年９月１日に県内の、従業員数５０～３００人以下・資本金５０００～３億円以下の２５１事業所に紙面による調査票を郵送した。回収期限の１０月１５日までに、９２事業所の回答を回収した。

（5）調査結果

今回の調査結果を２００３年に三菱総合研究所が行った全国調査結果と比較して示す。

[事業所や従業員]

①事業所

事業所所在地は、大分市が全体の５１．１％（４７社）、別府市が５．４％（５社）、国東市・中津市が４．３％（４社）、豊後高田市・杵築市・宇佐市・日出町・日田市・由布市が３．３％（３社）、臼杵市・竹田市が２．２％（２社）、玖珠町・九重町・豊後大野市・佐伯市が１．１％（１社）、津久見市が０％（０社）という回答であった（図５参照）。

②業種

業種は、製造業（３０．２％）、サービス業・その他（１５．１％）、建設業（１１．６％）であった（図６）。

③［従業員数］では、少人数の中小企業は少なく、５０人以下の企業が約７％で、１００人以上の企業が約半数を占めている（図７）。

④［資本金］でみても、資本規模の小さな企業が少なく、約１０％となっている（図８）。

〔情報化への取り組み〕

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

情報化への取り組み状況で8割を超えるのは、パソコン導入９７．１％、インターネット導入９３．９％、電子メールが８４．９％となっている。社員に対するＩＴ教育・研究は４６．８％の企業で実施されている。

②大分県の状況

今回実施したアンケート調査によると、大分県内でもほぼ全部の企業がパソコンとインターネットの導入をしていることが分かった。全体的に比較してみると、全国の調査結果より若干大分県内の導入率の方が上回っているものが多い。全国の状況が平成１５年度のものであり３年間の情報化の浸透と大分の場合は中小企業の割合が低いことがその要因と考えられる（図９）。

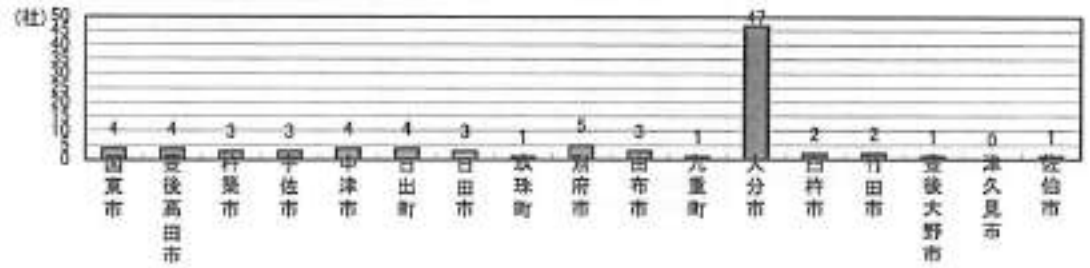


図５　所在地

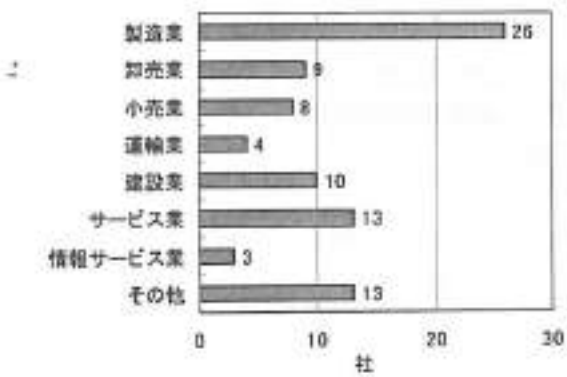


図６　業種

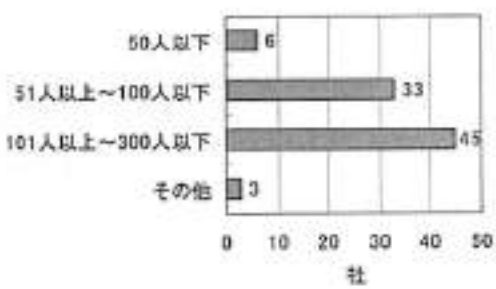


図７　従業員数

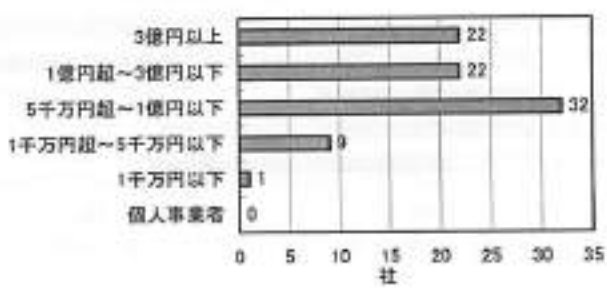


図８　資本金

〔パソコンの導入〕

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

パソコンの導入割合は、３企業に１社が１人１台という状況である。業種別にみると１人１台の割合が高い業種は、情報サービス業が８割を超えていて、次いでサービス業が約６割である。

②大分県の状況

県内中小企業での社員あたりの導入割合をみると、現状では２～３人に１台がもっとも高く、次いで１人に１台となっている（図１０）。業種別にみると、建設業、情報サービス業は１人に１台の割合が高い。サービス業は１人に１台というところはなく、２～３人に１台、４人以上に１台という割合が高い。全国的な状況と比較して、遅れていることが分かる（図１１）。

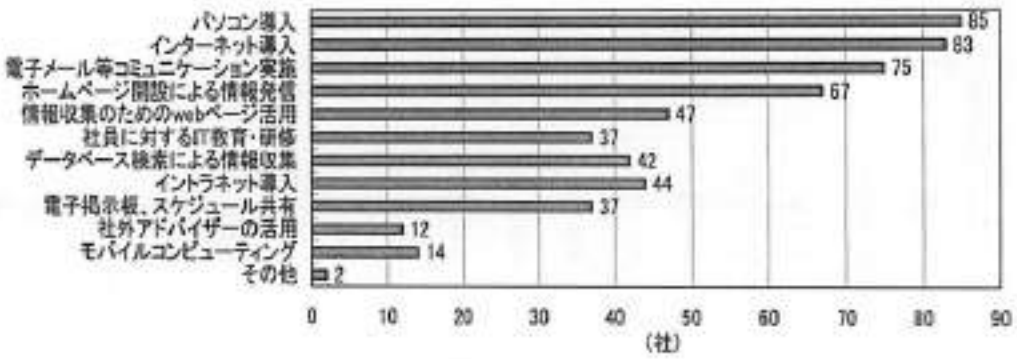


図９　情報化の取り組み

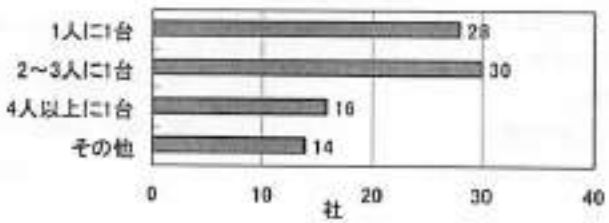


図１０　パソコン導入率

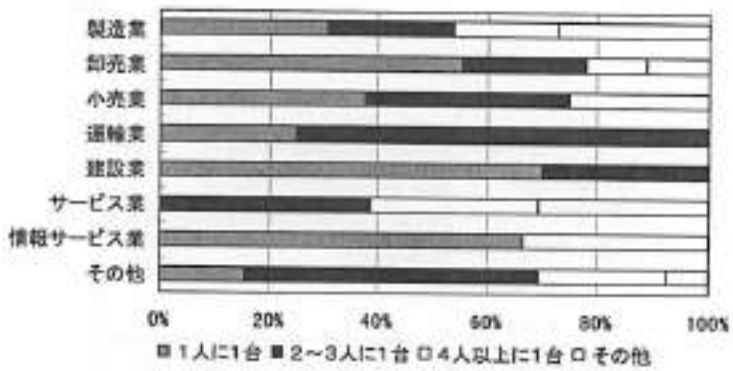


図１１　パソコン導入率

〔電子メールアドレスの導入〕

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

企業の電子メールの導入割合は、４人以上に１アドレスが４０．６％と最も多くなっている。業種別では、１人１アドレスが多いのは情報サービス業７２．２％、サービス業５１．１％、卸売業３８．２％である。

②大分県の状況

県内企業では、インターネットを利用している企業のうち、メールアドレスを付与している社員割合の平均は８５．９％である（図１２）。業種別に見ると、情報サービス業では全ての企業が１人に１アドレスとなっている。運輸業、サービス業は１人に１アドレスの割合は比較的低く、全国と比較してみるとサービス業は導入が遅れていることが分かる（図１３）。

〔ＩＴ能力向上の取り組み〕

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

企業に対するＩＴ教育・研修は、社外ＩＴ研修・講習会の参加支援が５７．３％と最も多くなっている。一方、ＩＴ能力の高い人材の採用は１５．１％である（図１４）。

②大分県の状況

業種別に見ると、運輸業、サービス業、情報サービス業ではＩＴ能力の高い人材の採用の割合が高い。全国と比較してみると、県内企業では社外ＩＴ研修・講習会の参加支援が十分に行われていないといえる（図１５，１６）。

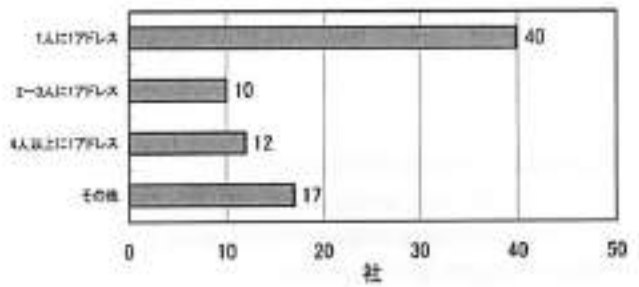


図１２　電子メール導入率

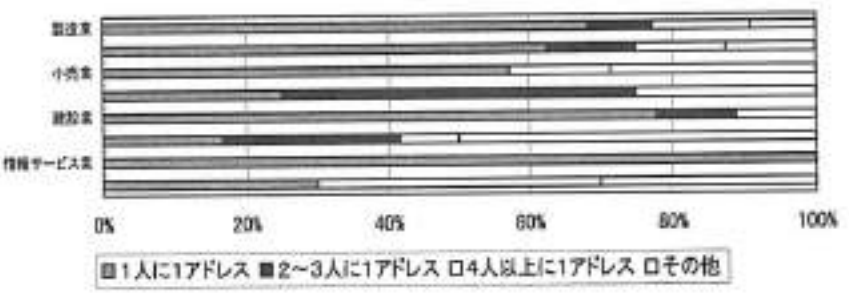


図１３　電子メール導入率

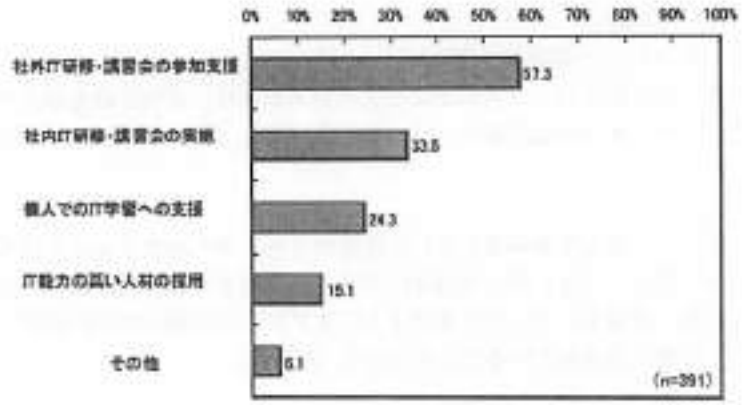


図１４　ＩＴ能力向上についての取り組み（２００３年に三菱総合研究所が行った全国調査より）

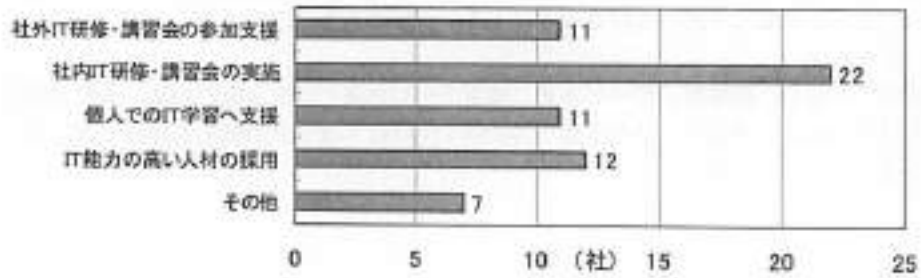


図１５　ＩＴ能力向上についての取り組み

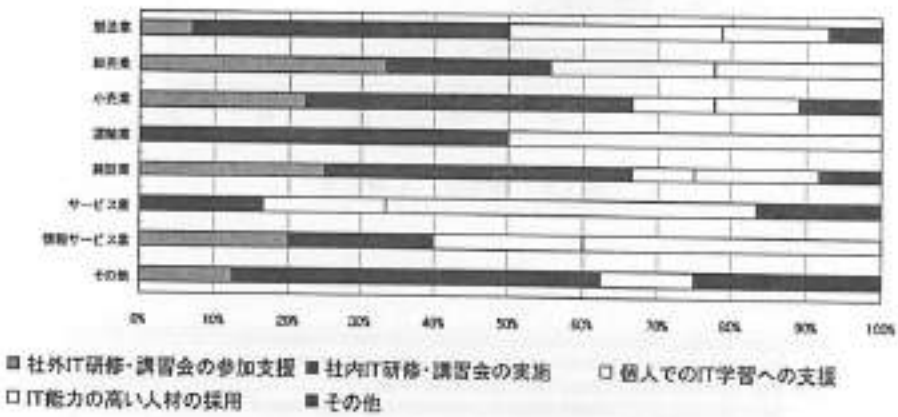


図１６　ＩＴ能力向上についての取り組み

［ＩＴ導入の効果］

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

ＩＴ導入効果の全体評価は、効果ありが７１．３％と比較的高いことが分かる。業種別にみると、効果ありの割合が高いのは、運輸業の８３．９％である。それに対して、効果ありが低いのは、サービス業の５９．４％、建設業の６６．４％である。

②大分県の状況

効果が出ている企業が約半数となっていて、効果が出ていないと答えた企業は０％であった。全国と比較してみると、全国の結果では効果が出ていない企業が２％あるので、県内企業の方が全国的な数値をやや上回っていると考えられる（図１７）。業種別に見ると、情報サービス業では全ての企業で効果がでている。他の業種も、ほとんど効果がでている、どちらかといえば効果がでているとなっている（図１８）。

〔インターネットの利用〕

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

インターネット利用年数は、１年未満が２．９％、３年未満が２６．９％である。
業種別にみると、卸売業と小売業は１年未満が多い。

②大分県の状況

県内企業では、利用年数が３年未満の企業が２％となっていて、全国的な数値より上回っていることが分かる。さらに、業種別ではあまり差が見られなかった（図１９）。

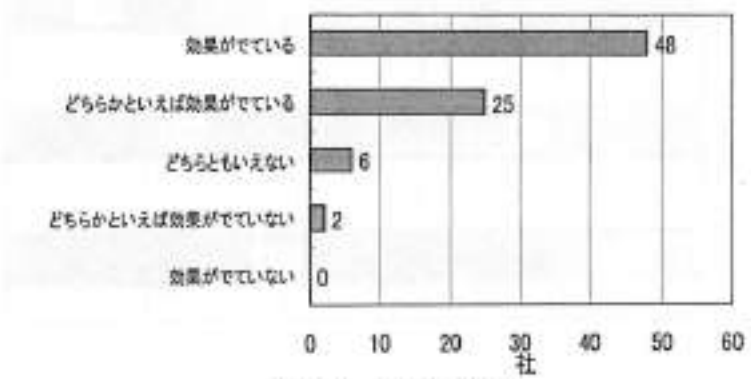


図１７　ＩＴ導入効果

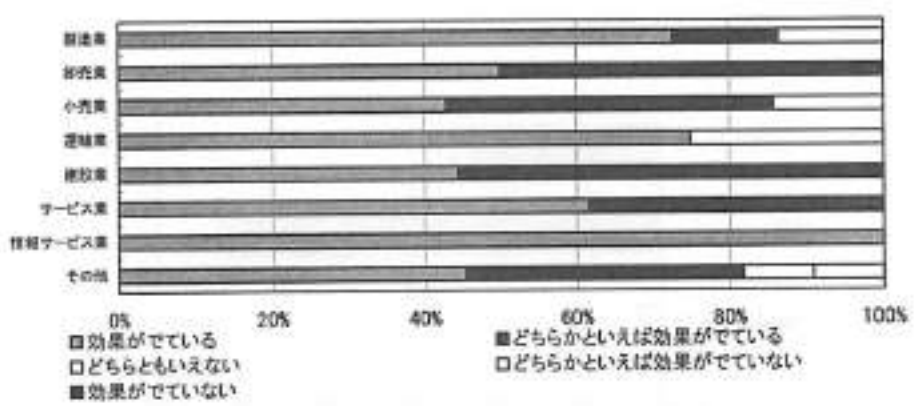


図１８　ＩＴ導入の効果

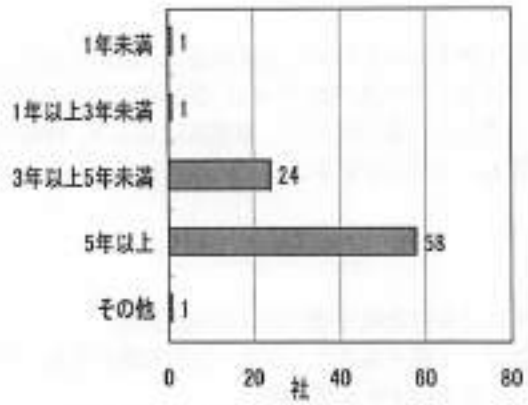


図１９　インターネット利用年数

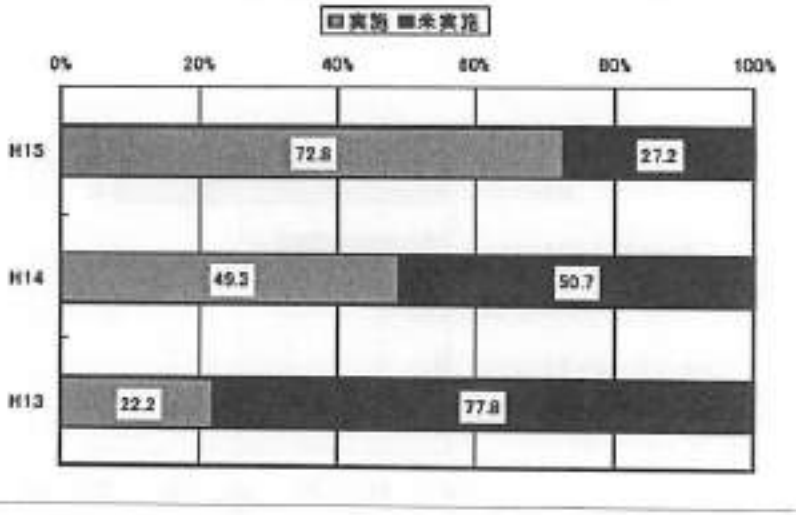


図２０　電子商取引実施率（２００３年に三菱総合研究所が行った全国調査）

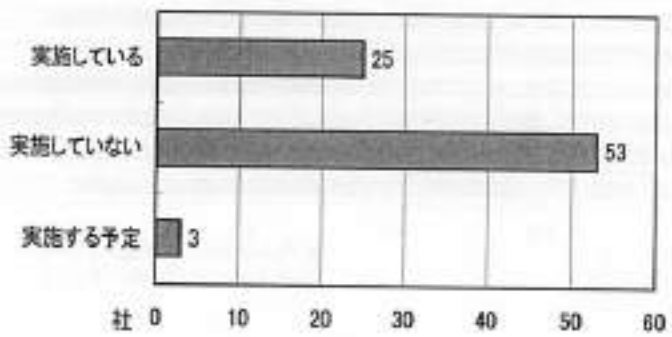


図２１　電子商取引実施率

〔電子商取引の実施〕

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

企業の電子商取引について、実施済みは７２．８％、未実施は２７．２％である（図２０）。

②大分県の状況

全国と比較して、県内企業は未実施の企業が約半数以上となっていて、実施済みの企業は３割にも満たなかった。さらに、未実施と答えた企業で今後実施予定のある企業は約３％であった（図２１）。

〔ＩＴ導入の問題点〕

①全国の状況（２００３年に三菱総合研究所が行った全国調査）

企業のＩＴ導入における問題点は、対応する人材不足が３６．５％、情報セキュリティ対策が３２．８％、ＩＴ投資に見合う効果がみえないが３０．７％となっている。

②大分県の状況

県内企業では、情報セキュリティ対策が４５．７％ともっとも高くなっている。業種別に見ると、運輸業では６０％が対応する専門の人材不足を問題点に挙げている。どの業種も情報セキュリティ対策を問題としている割合が比較的高い。情報サービス業では、ＩＴ関連投資の増大の割合が他の業種に比べ高くなっている。全国と比較してみると、県内企業でも全国の企業でも人材不足を問題としている割合が高いことが分かった（図２２，２３）。

〔セキュリティの方針と内容〕

①セキュリティの方針

県内企業では、決めているが全体の７２．３％、決めていないが２７．７％となっていて、多くの企業がセキュリティの方針を決めていることが分かった（図２４）。

②セキュリティの内容

社内方針・社内規定・ガイドライン等の遵守が全体の２３．４％（３９社）、法令等に遵守が２２．８％（３８社）、管理体制の確立が１８．６％（３１社）、安全対策の実施が１０．８％（１８社）、相談窓口の明確化が９．６％（１６社）、事故発生時の対策が８．４％（１４社）、方針の公開が６．６％（１１社）、その他が０％（０社）である（図２５）。

〔個人情報の漏洩問題〕

個人情報の漏洩は「ない」が全体の９９％（８１社）、「ある」が１％（１社）である（図２６）。

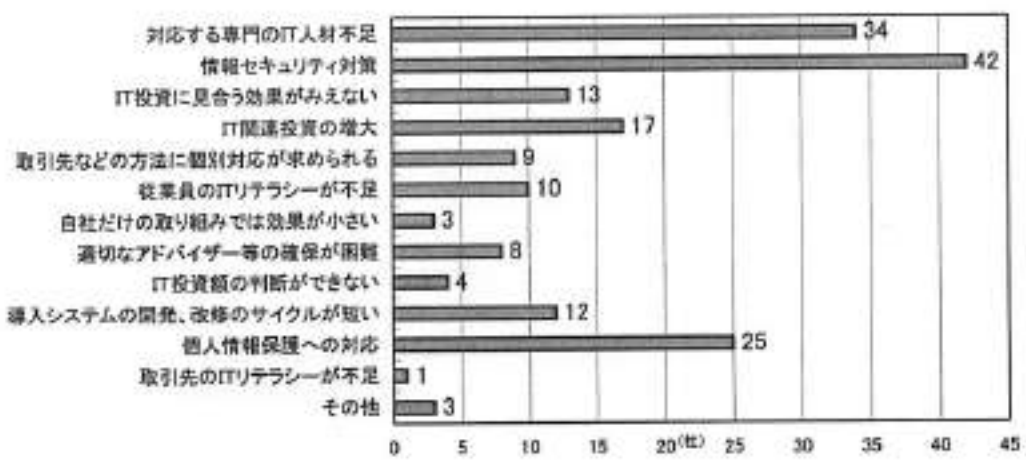


図２２　ＩＴ導入による問題点

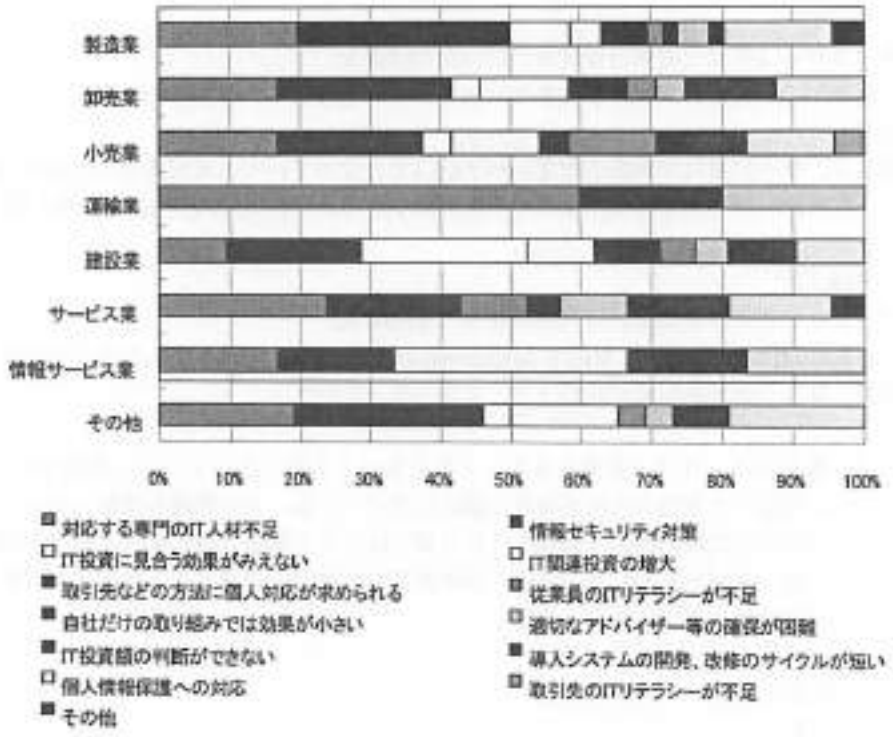


図２３　ＩＴ導入による問題点

図２４　セキュリティの方針

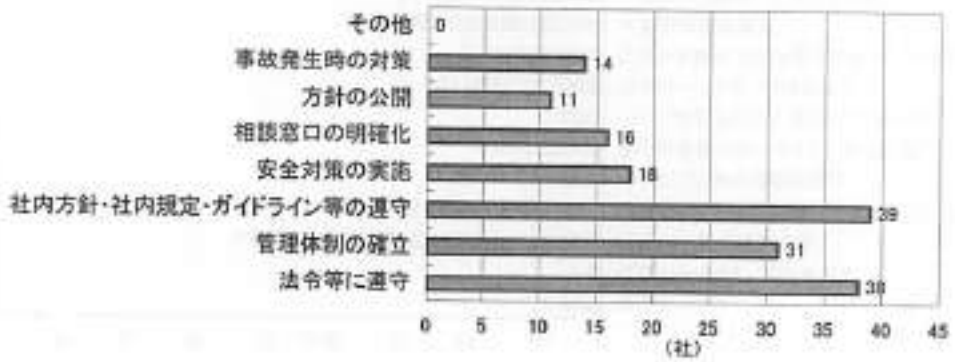


図２５　セキュリティの方針内容

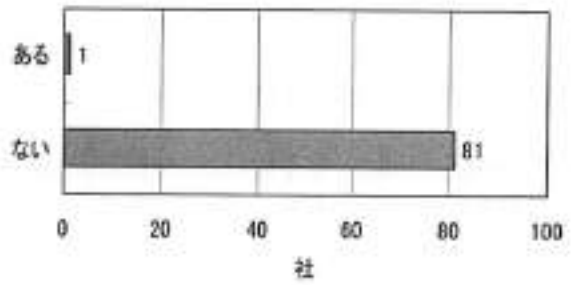


図２６　個人情報の漏洩問題

考　察

本調査により、県内企業の情報化の現状が明らかになった。

ＩＴインフラについては、ほとんどの企業で整備されつつあるが、多くの企業ではその利用が電子メールやインターネット、ホームページの公開などに止まっていて、電子商取引については、全国的な結果と比較すると、県内企業では取り組みが大幅に遅れていることが分かった。

ＩＴ化のレベルは多くの中小企業は基盤整備を終え、業務改善に取り組み始めた段階にある。企業はＩＴを利用した経営改善・改革が不可欠であることを認識してはいるが、その活用の方法が分からない、社内に適切な人材がいないということが問題になっている。インターネットを中心にした情報化が進展する中、ネットワーク、情報セキュリティなどのＩＴ技術を身につけた人材の需要は強く、県内のＩＴ企業をはじめ情報化を推進する中小企業に対して充分な人材を供給しきれていない。業種別に比較すると、情報サービス業は他の業種に比べＩＴ導入率が高い。しかし、情報サービス業だけでなく、今後はすべての産業が情報技術の恩恵に浴する必要がある。大企業や先端的なベンチャー企業に限らず、多くの平均的な中企業が自社のビジネスに応じて情報技術を経営にとりいれて、ＩＴ革命に対応していくことが重要な課題となっている。

また、中小企業がＩＴを導入する際に課題として挙げられるのがセキュリティの問題である。県内企業では、情報セキュリティ対策を問題としている割合がもっとも高いが、セキュリティ対策を行っている企業は３分の２となっていて、残りの企業は対策を行っていない。今日インターネットが、生活に深く結びついた重要な社会基盤のひとつになる一方で、通信内容の盗聴や他人へのなりすましや情報の改ざんといった不正が行われる危険性も十分に含んでいる。特に中小企業にとっては、緊急の課題であるインターネットを利用した電子商取引の実現のためには、ウェブ上のセキュリティを強化し、安心できるビジネス環境を築くことは、重要な課題である。これが行われずにＩＴ技術を利用することは、自社企業が被害を受けるだけでなく、利用者に対して加害者となり得る訳で、企業の社会的信頼を無くし、存続が危ぶまれることにもなる。今回、県内の２５１事業所に紙面による調査（アンケート）を郵送し、回収期限の１０月１５日までに、９２事業所の回答を回収した。回収率が約３７％であり、期待に比べるとやや低い値になった。今後は、自治体などによりさらに大規模な調査が行われるのを期待したい。

おわりに

本調査で明らかになった主なものを以下にまとめる。

①パソコン導入の割合状況は、大分県の場合、２～３人に１台がもっとも高く、全国的な状況から、

わずかに遅れている。
②電子メールアドレスの導入割合では、全国と比較するとサービス業は導入が遅れている。
③ＩＴ能力向上についての取り組みは、全国と比較すると、県内企業では社外ＩＴ研修・講習会の参加支援が十分に行われていない。
④ＩＴ導入の効果では、全国の状況の場合、ＩＴ導入効果の全体評価は、効果ありが約７０％と高いが、県内では、効果が出ている企業が約半数程度になっている。
⑤インターネット利用年数は、全国の状況では、インターネット利用年数が１年未満は２．９％、３年未満は２６．９％である。県内企業では、利用年数が３年未満の企業が２％となっていて、全国的な数値より上回っている。
⑥電子商取引の実施では、全国の状況は、実施済みは７２．８％、未実施は２７．２％である。県内企業は未実施の企業が約半数以上となっていて、実施済みの企業は３割にも満たない。
⑦ＩＴ導入における問題点では、県内でも全国でも人材不足を問題としている割合が高い。
⑧セキュリティの方針については、県内企業では、決めているが全体の７２．３％、決めていないが２７．７％となっていて、多くの企業がセキュリティの方針を決めている。
⑨セキュリティの方針内容では、社内方針・社内規定・ガイドライン等の遵守が全体の２３．４％、法令等に遵守が２２．８％、管理体制の確立が１８．６％である。
⑩個人情報の漏洩問題は、大分県の状況は、個人情報の漏洩は「ない」が全体の９９％で、「ある」が１％である。

このような情報化を進める上での課題に対応していくためには、次のような中小企業に対する行政の積極的な支援が必要となる。

①IT 推進のための情報提供

中小企業の IT 化を推進するために、施策情報の提供、技術情報の提供、ビジネス情報の提供を行う。

② IT 活用に対する意識向上と人材の育成

IT 化には、経営者が IT の効果と問題点を十分理解することが必要である。中小企業経営者に対し、業種・業態や進展段階に応じた、IT 活用の IT セミナーや実践的な研修を実施する。

③ ＩＴ化に関するアドバイスやコンサルティング

中小企業の IT 化推進には、専門的な知識や経営革新を踏まえた適切なアドバイスが必要である。IT 導入に対し、中小企業の実態を踏まえたアドバイスができる人材を育成する。また、行政機関がコンサルティング費用を一部負担するなどにより中小企業を支援する。

④ IT システム導入に対する支援

金融機関の IT 貸付等により、中小企業の IT システム導入に対する支援を行う。また、アフターサービスも含めた IT 導入支援サービスを行う。

本研究のような研究活動が地域の情報化に役立つことを期待する。

参考文献

〔1〕中小企業庁ホームページ　http://www.chusho.meti.go.jp/
〔2〕大分県内中小企業の情報支援サイト　コロンブス　http://www.columbus.or.jp/
〔3〕県民経済計算　http://www.esri.cao.go.jp/jp/sna/toukei.html
〔4〕就業構造基本調査　http://www.stat.go.jp/data/shugyou/

Development of National Information Security Index

Min, Kyungsik

Policy Development Division Director,Korea Information Security Agency, (Kyoungsik @kisa.or.kr)

Abstract

It is a very difficult task to measure the information security level, because the information security area continues to expand, making it difficult to define its concept, and also because it is difficult to select the information security index involving multi-dimensional factors, time series statistical data are lacking, and there is the problem of having to integrating different information security indices into a single index. Nonetheless, the most appropriate methodology of measuring the information security level metrically is to put it into an index. This makes it easy for policy makers or parties related to information security to determine the information security level goals from comprehensive perspectives and evaluate the outcome of implementing the policy.

This research aims to present a comprehensive information security index model aimed at calculating the index which can be used as the basic data for formulating and evaluating the information security policy, as well as to calculate the index.

As a result of calculating the index, the information security level, in the time series of 2002 to 2005, increased by 5.8% yearly. But, the information dysfunction level continued to decline except 2003 which experienced a massive Internet debacle on January 25. In particular, since the information security level is increasing, and the information dysfunction level is declining, it is deemed that the information security policy is effectively working.

Key word: information security, index

Ⅰ. Introduction

In the late 20th century, globalization and informationization have greatly influenced our economy, society, culture and environment, and are expected to continue to drive changes. [1] Advanced nations including the US, in particular, have continued to endeavor to structure the so-called knowledge-based economy by which people develop economy through the production, distribution and utilization of knowledge.

Meanwhile, Korea's IT paradigms are shifting from e-Korea focusing on informationization expansion to u-Korea emphasizing mobility and convenience. Also, numerous information-related international indices have proved that Korea's information level is ranked in the top category in the

[1] The term, information, was first used in the form of informationization society by Japanese researchers in the late 1960.

world. For instance, Korea is ranked first in the world in terms of the broadband Internet penetration rate per 100 people (OECD, 2005). Meanwhile, Korea's information society index was ranked in the 20th range up until 1999, in 2000 entered the 10th range, and grew fast to be ranked the third in 2005 after Sweden and the US (National Computerization Agency, White Paper on National Informationization, 2005).

However, despite this prominent information society index, worm viruses, spam mails, and Phishing or financial frauds are threatening the safety of our IT environment. Also, private information leakages, privacy infringement and other diverse information pathological phenomena, namely, dysfunctions, are spawning social problems. To ensure information security and cope with information dysfunctions in various social sectors, the government has formulated comprehensive information security measures and are pushing for them. [2]To effectively push for information security policies, the nation has first to establish a system of evaluating its information security levels according to the objective criteria. Such criteria make it possible to effectively analyze a nation's information security level and identify diverse information security phenomena from various perspectives. Also, such criteria measure and analyze information security levels, thereby allowing ex ante and ex post evaluation of policies, among others.

UN, OECD, ITU and other international organizations regularly announce information society indices for their respective member nations to utilize in establishing and evaluating information policies. Information society indices are utilized as important data for individual nations to evaluate their information policy performances and select future related projects. Meanwhile, as for the information security, there have not yet been internationally agreed-upon accurate criteria for measuring information security, making it impossible to measure information security levels objectively and compare them between nations. Currently, OECD (Communication Outlook) uses the number of security servers as an information security index, and IMD has since 2004 announced national rankings in terms of corporations' information security levels as an information security index. However, these indices are lacking in explaining the whole information security level.[3]

This research presents metrical index measurement models as a methodology of evaluating information security levels. Such indices are a very useful tool in determining policies by analyzing social phenomena, together with various statistical figures. Information security index-related research in Korea was conducted by Kim Jeong-deok (1998), Koh Il-seok (2002), Oh Jeong-hun (2004), Jung Gyeong-ho (2004), etc. These researches mostly focused only on how to analyze information security levels in what frameworks, but did not present models designed to measure metrical levels. Also, there are similar research achievements such as Shin Yeong-jin's research (2003) on comparing information security policies between nations, and Lee Jong-hwa's research (2005) on the government's role in ensuring information security. [4]

This research aims to present comprehensive index models for evaluating national information

---

[2] Information security is difficult to define in a word. This is because it is a combination of the concept of information and the concept of security. Also, threats to these security activities should be defined. Information security is defined as follows. It is to protect information assets from diverse dangers and threats, and maintain normal functions and status in terms of confidentiality, integrity, and availability, by enhancing the reliability of information systems or information, and ensure that users of information systems can use information systems safely. (Introduction to Information Security, 2000)

[3] Also, this Korean research team has since 2005 been working together with its Japanese counterpart to develop index models designed to measure and compare information security levels between nations.

[4] There are researches on the analysis of information security using economic logics and models, and other theories, such as Gordon and Loeb(2002), Cavusoglu, Mishra and Raghunathan(2002).

security levels in order to calculate indices which can be used in establishing and evaluating national information security policies, as well as to use statistics and calculate indices.

Ⅱ. Methodologies for Measurement of Information Security Levels

1. Concept of Information Security Index

It is very difficult to measure a nation's information security level, and there have not been desirable research achievements in this regard. The reason for such difficulty is because, with the area of information security continuing to expand, its concept is difficult to define, it is difficult to select information security indices encompassing multidimensional attributes, there is a lack of time series statistical data, and there is the problem of integrating different information security indices. Nonetheless, the most suitable methodology of measuring information security levels metrically is to express them in terms of indices. These indices make it easy for policy makers or information security stakeholders to determine information security level goals from comprehensive perspectives and evaluate the results of performance.

Normally, an index is a method to express a certain social phenomenon metrically or numerically. As such, it is produced in order to induce the representativeness of certain social phenomena, make comparison between nations, between regions or between organizations, induce policy significance, or provide raw data to follow-up research by creating indicators and conducting metrical analysis. Generally, the use of indices and indicators is mixed. Indicators are variables useful for measuring changes, and are considered a public statistical norm that provides a simple, inclusive and balanced judgment to conditions of and changes in systems.[5] Such indicators can be classified diversely according to their expression forms. Carley(1981) classified indicators into information indicators, predictive indicators, problem oriented indicators, and program evaluation indicators. [6]Also, by general usage, indicators are also categorized as social indicators, policy indicators, economic indicators, etc. Indicators, according to their expressed forms, are grouped into economic indicators and non-economic indicators, performance indicators and structure indicators, input indicators and output indicators, flow indicators and stock indicators, positive (plus) indicators and negative (minus) indicators, and objective

---

5 Land, Kenneth C., " Theories, Models and Indicators of Social Change" , *International Social Science Journal*, Vol.27 No.1, 1975, pp.7-8.

6 Carley, Michael, Social Measurement and Social Indicators, London: George Allen and Unwin, Ltd, 1981.

indicators and subjective indicators.[7]

Meanwhile, indices are an expression of such diverse indicators into a single value. Thus, information security indices can be used in determining the status of a nation's information security. This research, in an effort to distinguish it from detailed indicators in each sector, defines as an index a single value that determines the security level of the whole nation or each sector.

Indices should play double roles as policy data. First, they should play a descriptive role of fully reflecting the reality that they intend to measure. Second, they should play a normative or policy oriented role of what part of complicated multi-faceted reality they should measure to help make better policy decisions and implement them. Likewise, desirable indices should not only well reflect the target reality, but also have policy implications for leading to better policy decision making.

Types of indictors of which indices consist can be categorized according to their attributes. First, according to the degree of the possibility of metering indices, they are grouped into qualitative indicators and quantitative indicators. Also, they are categorized as static indicators and dynamic indicators according to their relations with time. In the past, quantitative indicators and static indicators prevailed, but recently, qualitative indicators and dynamic indicators are considered important. Likewise, indicators can vary widely according to purposes of developing indices or the definition of the concept of targets to be measured.

The information security index[8] is a figure to express the characteristics of a particular group's information security the most succinctly and clearly, and can be employed very usefully in determining information security policies together, with various statistical data. However, in fact the information security index has the following limitations due to problems surrounding its calculation methods and data collection. First, it is difficult to ensure the establishment of a unified concept of information security phenomena. Second, it is difficult to select appropriate components that represent information security phenomena. In particular, there is a lack of criteria for applying differentiated levels of importance to selected components, making it difficult to ensure an appropriate integration of such components for producing the index. Third, there is an absolute lack of statistical data, and the reliability of surveyed statistical data is problematic.

Also, requirements for developing ideal information security indices are as follows. First, the index

---

[7] ① Economic indicators: indicators expressed in terms of currencies, non-economic indicators: indicators not expressed in terms of currencies

② Performance indicators: indicators to measure performance results, structure indicators: indicators that influence the production of results

③ Input indicators: indicators to measure input factors of the system, output indicators: indicators that concern the output factors of the system

④ Flow indicators: indicators identified during a certain period of time, stock indicators: indicators at a certain point of time

⑤ Positive (+) indicators: indicators whose increase is seen as increasing certain status, negative (-) indicators: indicators whose increase is seen as lowering certain status

⑥ Objective indicators: indicators that measure various actual social conditions, subjective indicators: indicators that measure the status of individuals' personal experience

(NCA, Development and Research of Comprehensive National Information Index Models, 2004)

[8] This research refers to NISI as information security index.

should reflect the scope and purpose of information security. Likewise, it should involve diversity to be able to express the interest and phenomena of various information security-related parties (users, information security industry, general organizations, nations, etc.). Second, it should objectively and accurately reflect and measure the level of information security. Third, it should be equipped with timeliness to appropriately reflect changes in information security. In addition, it should consider systematic methods to be able to offer forecasts.

2. Methods of Measuring Information Security Index

The simplest method of calculating an information security index is a simple summing method; with an assumption that all components and indicators have an equal importance, it is to calculate an arithmetic mean of indices individually calculated regarding the components. Such representative indices are WEF(World Economic Forum)'s networked readiness index and Swiss IMD's national competitiveness index.[9] This method, from the viewpoint of integration of components, does not consider each component's contribution, and if basic indicators have an increasing number of measurement components, such related measurement components will have relatively low weighted value, thereby having problems.

This shortcoming can be resolved to a certain degree by using the factor analysis (FC) method that provides relative weighted value. The FC is a statistical method to explain the correlation between many variables by hidden shared factors. As such, the FC is to obtain a common variation from correlations between numerous variables, define the duplication of measured values, extract several basic hypothetical variants, namely, factors, and redefine the correlation between numerous variables by the correlation between several factors. However, due to its characteristics, the factor analysis method also gives a high weighted value to an array of highly correlated variables, and a low weighted value to low-correlation variables.[10] Likewise, since, of variables that influence information security, low-correlation variables have too low weighted value, such variables' influence upon the evaluation of national information security levels may be distorted.

Meanwhile, there is a method of assigning weighted value by letting experts in related areas assess the relative importance of components. This method is categorized into two groups. First, the delphi technique is to assign a different weighted value to each item and indicator according to the agreement among the group of experts. Second, the analytic hierarchy process (AHP) is to let individual experts assess the relative importance of each component and indicator, gather the results and assign weighted value.[11]

---

9 With regard to both quantitative and qualitative data, WEF uses mean and standard deviation and converts them into standard scores, assigns one-third weighted value to small components, and again one-third weighted value to large components, and comes up with the final indicator. The IMD assigns two-thirds weighted value to quantitative data and one-third weighted value to surveyed data, and the same weighed value to detailed indicators.

10 These feedbacks are found in researches related to national information indices, such as Kang Sin-won (1999) and Jie Gyeong-yong (1999).

11 ITU's Mobile/Internet index assigns 50% weighted value to the infrastructure, and 25% weighted value to types of usage and market structures, while EIU arbitrarily assigns weighted value to six categories in the e-business readiness index. Weighted value by component in the e-business readiness is 25% for connectivity and technology infrastructures, 20% for business environment, 20%

The delphi technique is to let a group of experts work together and share their respective views, thereby maximizing such advantages. As such, this methodology is to conduct logical, objective and systematic analysis, get feedbacks several times, and gather opinions of experts, thereby making it useful in ensuring more systematic and objective results.[12]

The greatest advantage of the AHP is to stratify complicated problems, segment it into major factors and detailed factors, compare these factors, and thus induce important points. The AHP can analyze and resolve the whole decision making process by process to boost the objectivity of decision making, as well as verify the consistency of weighted values resulting from the comparison and bolster the robustness of decision making. The advantage of this technique is to analyze, decompose and organize problems using an approach similar to humans' system of thinking, and to use models, systematically put relative importance or preference into a ratio scale, and thus produce results in the quantitative form.[13]

III. Models and Measurement Indicators of Information Security Index

1. Information Security Index

Kim Jeong-deok's (1998) and others' research results use the U.S. Department of Defense-formulated TCSEC (Trust Computer System Evaluation Criteria), and BS7799 and other information security class certifications of the U.K. Department of Commerce and Trade, as information security indices. These indices target government agencies or corporations, making them inappropriate as indicators for measuring national information security levels. Thus, this research attempts to present models of information security indicators that show Korea's information security levels accurately and easily and simultaneously and can be compared objectively with those of numerous nations.

Such models should include the assessment of information security infrastructures for individuals, corporations and others, and security activities including information security environments consisting of information security budgets and manpower, thereby comprehensively considering threats to information security levels and protective activities, and other information dysfunctions, and encompassing the measurement at the level of the nation's various components such as the government, individuals, and corporations. Shown in [Figure 1] is the framework of evaluating the national information security levels.

The selection of detailed indicators of which the national information security index consists involves the following process. First, to induce detailed indicators of which the information security index consists, existing references were surveyed, the domestic and overseas reality surrounding information

---

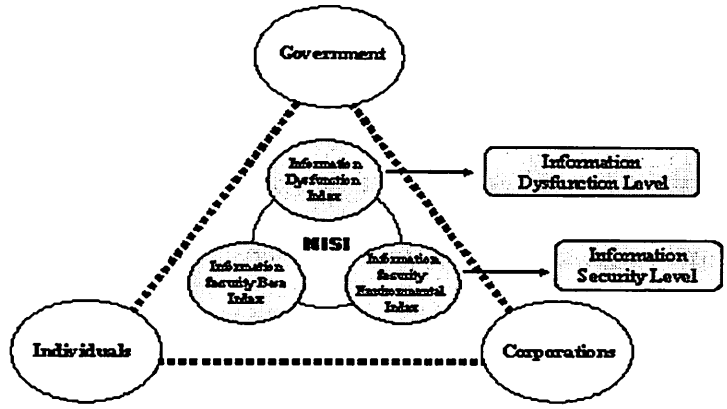
for acceptance level of consumers and corporations, 15% legal and policy environment, 15% for social and cultural infrastructures, and 5% for the supported e-service.

ITR evaluated corporations' information levels, and KIMI evaluated small and medium firms' information levels, by using Saaty(1980)'s AHP and assigning weighted value to components and indicators. These institutes survey experts to establish weighted value criteria in order to reflect changes in relative importance by area in conjunction with the fast IT development and mature informatization stage.

12 The term, delphi, was invented by philosopher Kaplan at US RAND research institute.

13 The AHP was first developed by Saaty(1980) in the early 1980. This method is widely used in diverse areas, and is employed mainly in determining the decision making priority in evaluating, selecting and forecasting indices.

security was analyzed, and thus all subsequently possible indicators were put together.[14] Thereafter, the results were reviewed by the research group and the group of experts, and detailed indicators deemed as the most representative were induced.[15]



[Figure 1] Framework of National Information Security Index

Review results led to the composition of detailed indicators which can be metered and are statistically significant. Second, in order to enable the comparison between nations in selecting indicator components, the analysis was limited to internationally verified obtainable statistical data (hard data). Components that could represent information security but whose comparable statistical data could not be obtained were in principle excluded from the selection of indicator components. In the event that particular factors were considered inevitable in evaluating the related nation's information security level, they were additionally included in the evaluation of that nation. However, when comparing nations, such evaluation indicators were excluded, creating the model to ensure an objective comparison between nations.[16]

Indicators to compare information security levels between nations should ensure relevance and reliability given their characteristics. The said relevance means that results of evaluation using the national information index presented herein should transparently and subjectively reflect the related nation's information security level, and thereby should befit the purpose of the national information security index. The said reliability means that indicator components of which the national information security index consists should always produce reasonable and same results whenever, wherever and by whomever they are measured, and they are publicly accredited indices that are universal factors that can be accepted by all related parties. Given that the existing information security indices are lacking in reliability due to their controversial representativeness and lack of reliability arising from statistical

---

14 To develop the indices, the research referred to NCA's national information security index-related data, and overseas data such as Information Society Technologies(2003), CSI/FBI(2003), and RAND(2003) in the informatization area.

15 This research was the project of KISA's policy development group conducted since 2004, and selected measurable indices after 15 experts in information security held meetings for review.

16 The reason why this research model determined some ten indicators is because, as seen in existing researches into information security indices, too many detailed indicator items make it difficult to gather appropriate related statistical data. Meanwhile, since a too small number of detailed indicator items weaken the explanatory power of indices, the index was made to consist of 10 representative indicators.

quality difference between nations, this intends to prevent the repetition of controversies regarding information security indices. [Table 1] shows the classification of the final information security index and its detailed indicators. Statistical data used for detailed indicators in [Table 1] were based on the survey of information security by Korea Information Security Agency and from the collection of information statistics by NCA. And, the penetration rate of security servers was based on OECD's Communication Outlook.

As for the characteristics of each index, the information security base index indicates the level of structuring systems and information security activities by individuals and corporations to protect information. The information security base index indicates the level of direct information security activities. The information security environmental index consists of the people's awareness level of information security, the level of securing specialized manpower for information security activities, and the positivity towards the research and development of information security. The information security environmental index indicates an indirect information security level. The information dysfunction index concerns results of vulnerability of information security due to lack of the infrastructure and environment. It indicates system attack levels, data attack levels, and spam mail receip levels. Likewise, the higher the information dysfunction index is, the lower information security activities are. Thus, the information dysfunction index is in a negative relation with information security levels.

[Table 1] Composition of Information Security Index and Its Indicators

Description	Division	Detailed indicators
Information security index	Information security infrastructure	Vaccine penetration rate
		Patch penetration rate
		PKI penetration rate
		Firewall penetration rate
		IDS penetration rate
		Security server penetration rate
	Information security environment	Information security-related budget ratio
		Information security manpower ratio
		People's security awareness ratio
Information dysfunction level	Information dysfunction	Hacking and virus report ratio
		Private information intrusion report ratio
		Spam mail receipt ratio

Researches into the development of information security indices produced many arguments regarding so called efforts towards information security, namely, functions and dysfunctions of information security. Jung Gyeong-ho (2004) defines trade-off effects between functions and dysfunctions and uses a methodology to measure the difference between the two.[17] It is not proper to consider dysfunction as the opposite concept of the information security function. This is because dysfunctions have the

17 $H = \ln\left\{\frac{TE}{N}\right\}$, here, TE indicates the function of information security, and N dysfunction.

following several aspects. They are the dysfunction created when functions of information security do not work, information damage sustained in the process of informationization apart from functions - like air and other public pollutions - and inevitable occurrences of incidents. Thus, this research measured information security levels in terms of functions and dysfunctions, and evaluated the validity of effects of information security policies through the movement of the two indices.

2. Analysis of Information Security by Indicator

1) Measurement of Information Security Base Levels

The information security infrastructure criteria measure the degree of efforts towards information security, such as vaccine penetration rate, patch penetration rate, and PKI penetration rate.[18] The PKI penetration indicator evaluates users' concern for security and their efforts to that end in conducting economic activities through Internet. The PKI penetration rate is calculated by dividing the number of issued public certifications by the total number of Internet users.[19]

To measure corporations' information security infrastructure levels, the firewall penetration rate, the IDS penetration rate, and the security server penetration rate are measured.[20] As of June 2004, firms that structured networks numbered 271,000, and the yearly firewall penetration rate included the estimation of that of those small-sized firms whose employees numbered up to five (Statistics on Informationization, 2005). In the case of small-sized firms with the number of employees at below 50, it was assumed that, in consideration of their economic operation, they satisfied the required information security level even through individuals' information security level even if no firewalls were used. The firewall penetration rate used the average firewall usage rate of firms with the number of employees at above 50, as a supplementary indicator. Also, the IDS penetration rate used the average usage rate for firms with the number of employees at above 300.

The number of serviced security servers is one of representative statistical data that IMD, WEF, OECD and other major international agencies use as an evaluation indicator in the information infrastructure area. However, these agencies refer to the research agency Netcraft's survey statistics on security servers, and since these figures are based only on the number of certifications issued by Verisign, they have limitations of lacking statistical objectivity. This research seeks to define a security server as the whole servers that provide a safe communication function between web servers and web browsers, and to survey servers operated by using web security solutions of Verisign and other security firms alike to use the results. Thus, based on the statistics of all Korean security servers including SSL security servers,[21] the research intends to define the average number of security servers per 100,000

---

18 Vaccine penetration rate [(the number of users of vaccine programs/the number of Internet users)*100], patch penetration rate[(the number of installed patches/ the number of Internet users)*100], PKI penetration [(the number of users of public certifications / the number of Internet users)*100]

19 In the case of PKI, it can be recognized as one of universal information security indicators in Korea, but since the use of PKI varies according to nations, other indicators should be considered.

20 Firewall penetration rate [(the number of firms using firewalls / the number of firms)*100], IDS penetration rate [(the number of firms using IDS/the number of firms)*100], security server penetration rate [(the number of security servers sold in Korea / the population)*100,000]

21 Song Sang-hun(2004), Survey of Use of Passwords, KISA.

people in OECD nations as the target level and use Korea's relative level as an indicator. Likewise, the Korea's security server penetration rate was determined by calculating the number of its security servers sold per 100,000 people, and then when the OECD's average number of 15 was set at 100%, Korea's security server penetration rate was likewise converted into a corresponding rate.

2) Measurement of Information Security Environmental Levels[22]

The ratio of a nation's budget related to information security is crucial in enhancing its future information security level. This not only produces the effect of bolstering the information security level, led by the nation, but also creates ripple effects of triggering private investments and interest. The ratio of the government's budget related to information security is defined as the ratio of the nation's information security-related budget to its total information-related budget. Currently, the accurate information security budget size of the information budget is not available[23]. Thus, it is estimated from the White Paper on the Nation's Information Security. Here, the information security budget of the information budget was assumed at 10%, and it was converted into a corresponding figure.

Manpower specializing in information security, together with heavy investment in and spread of hardware and software aimed at ensuring information security, is human-ware aimed at utilizing, maintaining and developing these tools. The ratio of such experts was defined by the ratio of information security experts to the manpower engaged in the nation's information industry. According to the 2005 Korea's statistics on the information security industry, employees engaged in the information security industry numbered a total of 4,333. The ratio of the specialized information security personnel to the total manpower of the information industry is now very small at 0.3%. Here, the appropriate ratio of the specialized information security manpower to the total specialized information manpower is assumed at 1%, and then related figures are calculated.

The people's security awareness level can be a crucial measurement of the national information security level. To evaluate it, the research surveyed the people's necessity for and awareness of information security, and selected the ratio of the people who were aware of the necessity for information security, as a security awareness level indicator.[24]

3) Measurement of Information Security Dysfunction Levels [25]

---

22 A nation's information security-related budget ratio[(the nation's information security-related budget/the nation's information-related budget)*100], the ratio of specialized information security manpower[(information security manpower/specialized information manpower)*100], the people's security awareness level ratio [(5-point scale is needed, or the number of respondents saying "very much necessary" /the total number of respondents)*100]

23 This is so not only to Korea, but also to the US, Japan, and major European nations. This is because the budget for information security, given its nature, is not clearly disclosed in the information budget, or related agencies do not disclose it.

24 Available statistical data were surveyed for the first time in 2004.

25 The ratio of hacking and virus reports [(the number of reported hackings and viruses/ the total PC penetration number)*100], the ratio of private information intrusion reports [(the number of reported private information intrusions/ the number of Internet users)*100] the spam mail receipt ratio [(the number of spam mails received per account / the total number of e-mails received per account)*100]

Hackings and viruses are representative information dysfunctions, and have a negative relationship with the national information security level. The ratio of hacking and virus reports was defined as the ratio of the hacking and virus reports to the total PC penetration number, and was selected as an indicator.

Intrusions on private information are also a representative information dysfunction in this age of information. The ratio of private information intrusion reports was defined as the ratio of the number of private information intrusions to the total number of Internet users, and was selected as an indicator. Types of Korea's private information intrusions include 14 cases such as the collection of private information without the agreement of concerned users, damage, intrusion, and leakage by the collector of private information, and non-destruction of private information after it is collected or provided thereby fulfilling the purpose.

Spam mails indicate commercial advertising messages that are sent by e-mail, phone, fax and other electronic media for the purpose of business although the recipients do not want to receive them. Generally, spam mails are indiscriminately sprayed to an unspecified multitude of people without the agreement of the recipients, thereby consuming concerned users's much time and cost, and causing unnecessary consumption of telecom resources and an increase in traffic for information telecommunication service providers as well as other tangible and intangible damages.

IV. Measurement of National Information Security Levels

1. Tallying of Indices

The national information security level evaluation index is shown as follows.

Information security level index: H=T+E

Dysfunction index: N .....(1)

In the equation (1), H indicates information security level index, T information security base index, E information security environmental index, and N information dysfunction index. Information security base index and information security environmental index are function indices, and work positively for informationization levels.

The national information security index is a total indicator that integrates indices at every stage as shown in [Table 2]. This total indicator is classified as the first stage upper-category indices, namely, information security level index and information dysfunction index. Likewise, the upper-category indices are categorized as the second-stage middle-category indices, namely, information security base index, information security environmental index, information dysfunction, etc. This is again categorized as the third-stage low-category 12 detailed indicators such as the vaccine penetration rate, patch penetration rate, and PKI penetration rate. Thus, the third-stage category detailed indicators undergo the reflection of weighted value and adjustment factor, and are integrated into the second-stage indices. Again, the second-stage indices are calculated in terms of the first-stage indices, and the first-stage indices are calculated in terms of the national information security index as in the equation (1).

The information security level index (H), information security base index (T), information environmental index (E), and information dysfunction index (N) are calculated as follows.

$$H = w_{1}T + w_{2}E \quad \text{.....(2-1)}$$

s.t. $w_{1} + w_{2} = 1$,

$$T = w_{t11}\alpha_{11}t_{11} + w_{t12}\alpha_{12}t_{12} + w_{t13}\alpha_{13}t_{13} + w_{t14}\alpha_{14}t_{14} + w_{t15}\alpha_{15}t_{15} + w_{t16}\alpha_{16}t_{16} \quad \text{.....(2-2)}$$

s.t $w_{t1}+w_{t2}+w_{t3}+w_{t4}+w_{t5}+w_{t6}=1$,

$E=w_{e1}\beta_{11}e_{11}+w_{e12}\beta_{12}e_{12}+w_{e13}\beta_{13}e_{13}$ .....(2-3)

s.t. $w_{e11}+w_{e12}+w_{e13}=1$,

$N=w_{n11}\delta_{11}n_{11}+w_{n12}\delta_{12}n_{12}+w_{n13}\delta_{13}n_{13}$ .....(2-4)

s.t. $w_{n11}+w_{n12}+w_{n13}=1$,

In the equations, the weighted value of each index by stage has the same value, and the sum of all weighted values is 1. This research employed the delphi technique, one of methods that can use experts' experience and knowledge and calculate appropriate weighted value.

The adjustment factor is a factor designed to adjust the criteria of each index. For instance, it is a value designed to adjust the amount base's indices and the number of cases, and logarithm base's indices on the same criteria. There are normally two methods to establish such an adjustment factor. First, for the criteria such as the amount of cost and the number of cases to determine other indices' base, meetings of a group of experts are held, and an appropriate adjustment factor is selected through the agreement of the parties concerned. Second, an adjustment factor can be selected by simply using statistical techniques and empirically standardizing the base.

Since the scope of measured figures may differ according to the attributes of individual indices, the value of individual indices was made to be equal by the ratio scale so as to make the influence of individual indices upon the integrated index equal.

[Table 2] Integration of Indices at Each Stage

Description					
1st stage	2nd stage (middle category)		3rd stage (low category)		
Total index	Weighted value	Item	Weighted value	Adjustment factor	Item
Information security level (H)	W_{t1}	Information security base index (T)	W_{n11}	α_{11}	Vaccine penetration rate t11
			W_{n12}	α_{12}	Patch penetration rate t12
			W_{n13}	α_{13}	PKI penetration rate t13
			W_{n14}	α_{14}	Firewall penetration rate t14
			W_{n15}	α_{15}	IDS penetration rate t15
			W_{n16}	α_{16}	Security server penetration rate t16
	W_{e1}	Information security environmental index (E)	W_{n11}	β_{11}	The ratio of information security-related budget e11
			W_{n12}	β_{12}	The ratio of specialized information security manpower e12

			W n13	β13	The ratio of the people's security awareness level e13
Information dysfunction level (N)	W n 1	Information dysfunction index (N)	W n11	δ11	The ratio of [illegible] n11
			W n12	δ12	The ratio of private information intrusion reports n12
			W n13	δ13	The ratio of spam mail receipt n13

2. Calculation of Indices

The establishment of detailed indices' weighted value is outlined as follows. The information security base level has a total of six detailed components in three stages. Thus, the weighed value of the 3-stage detailed components is set at 0.167 each.

$$T = w_{t1}\alpha_{11}t11 + w_{t12}\alpha_{12}t12 + w_{t13}\alpha_{13}t13 + w_{t14}\alpha_{14}t14 + w_{t15}\alpha_{15}t15 + w_{t16}\alpha_{16}t16$$

$$= \sum_{j=1}^{6} w_{1j} \times \alpha_{1j} \times t_{1j} \quad \text{.....(3-1)}$$

w_{1j} = the weighted value of the index in the t sector

t_{1j} = the detailed indicator in the t sector

α_{1j} = the adjustment factor in the t sector

Based on the above basic equation, the information security base index is calculated as follows. Here, the adjustment factor is all 1.

$$T = \sum_{j=1}^{6} 0.167 \times t_{1j}$$

The information security environmental level has a total of three 3-stage detailed components. Thus, the weighted value of each of the 3-stage detailed items is set at 0.33 each.

$$E = w_{e11}\beta_{11}e11 + w_{e12}\beta_{12}e12 + w_{e13}\beta_{13}e13$$

$$= \sum_{j=1}^{3} w_{e1j} \times \beta_{1j} \times e_{1j} \quad \text{.....(3-2)}$$

w_{e1j} = the weighed value of the indicator in the e sector

e_{1j} = the detailed indicator in the e sector

β_{1j} = the adjustment factor in the e sector

Based on the above basic equation, the information security base index is calculated as follows. Here,

the adjustment factor is all 1.

$$B=\sum_{i=1}^{3}0.33\times e_{1i}$$

In the case of the information dysfunction level, the weighted value by detailed component is set at 0.33, the same as that of the information security environmental level. Here, the adjustment factor is set at 100 only for the
private information intrusion ratio.

$$N=\omega_{n11}\delta_{11}n1+\omega_{n12}\delta_{12}n2+\omega_{n13}\delta_{13}n3$$
$$=0.33\times n11+0.33\times 100\times n12+0.33\times n13$$

This process leads to the calculation of "2nd-stage index value = weighted value×adjustment factor×3-stage index's statistical value." The process of integrating the second stage into the first stage index considers only weighted value. Likewise, the sum of the weighted value of second-stage indices by each component that belong to the first-stage index components is 1. Since "Information security level index=information security base level+information security environmental level," the information security base level, and information security environmental level each consider the 0.5 weighted value.

$$H=\omega_{t1}T+\omega_{e1}B$$
$$=0.5\times T+0.5\times B$$

[Table 3] Calculation of Indices (2005)

1st-stage index	2nd-stage index	3rd-stage index		
Index value	Item	Weighted value	2005 data	Detailed item
57.12	Information security base 59.39	0.167	87.9	Vaccine penetration rate
		0.167	82	Patch penetration rate
		0.167	37.6	PKI penetration rate
		0.167	66.7	Firewall penetration rate
		0.167	38.4	IDS penetration rate
		0.167	43.0	Security server penetration rate
	Information security environmental 54.85	0.33	35	The ratio of information security-related budget
		0.33	34	The ratio of specialized information security manpower
		0.33	97.2	The people's security awareness level ratio
11.09	Information dysfunction 11.09	0.33	0.19	The ratio of hacking and virus reports
		0.33	0.056	The ratio of private information intrusion reports
		0.33	26.10	Spam mail receipt ratio

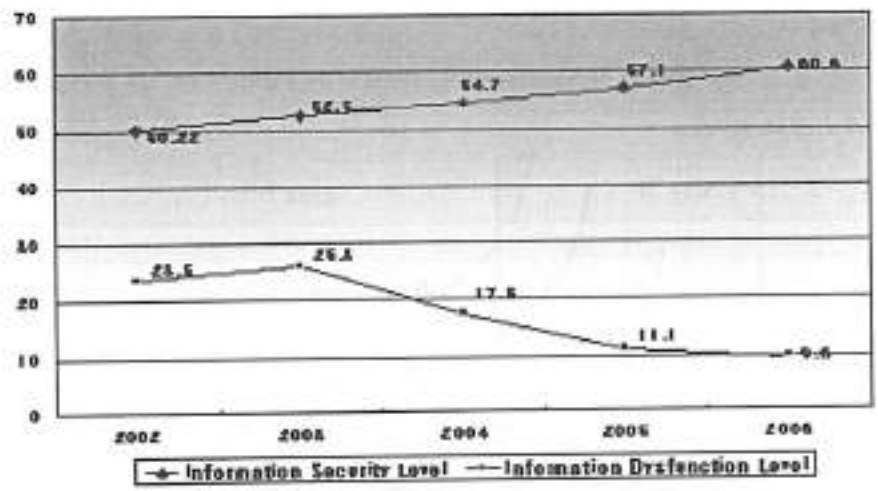
Using these index equations, the information security index was calculated from 2002 to 2005. [Table 3] shows the process of the calculation of the 2005 index. In 2005, the information security base level was calculated at 59.39, and the information security environmental level at 54.85; thus the 2005 information security level index came out as 57.1. The dysfunction level was calculated at 11.09.

3. Analysis and Utilization of Calculated Indices

This research calculated the national information security index for the period of 2002 to 2005 during which time series data could be secured. [Figure 2] shows the yearly index calculated for the period of 2002 to 2005. The calculation of the vaccine penetration rate and patch penetration rate was based on the 2004 survey results due to lack of related data.

The national information security level can be considered in terms of both information security level and information dysfunction level. The information security level increases by 5.8% yearly from 2002 to 2005, in terms of time series, while the information dysfunction level continues to fall except 2003 when it surged due to the January 25 massive Internet debacle. Given that the information security level is increasing and the information dysfunction level is declining, it is deemed that the nation's information security policy is effectively working.

[Figure 1] National Information Security Levels



Division	2002	2003	2004	2005	2006
SL	50.2	52.5	54.7	57.1	60.6
DL	23.5	25.8	17.5	11.1	9.0

Policy achievements in the information security level and dysfunction level can be summed up as four points as shown in [Table 4]. The table shows four areas of the policy level in consideration of the relationship between the information security level and dysfunction level.

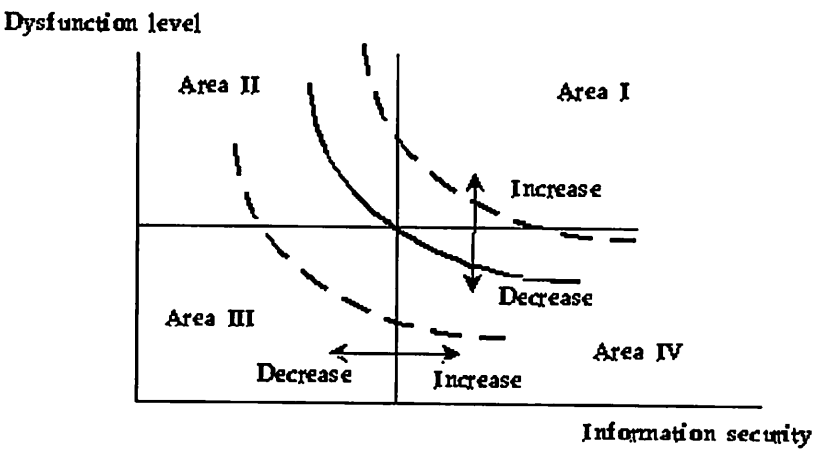
Based on these four areas, [Figure 3] presents the criteria for evaluating the effect of the policy. The information security policy curve A indicates a desirable policy direction, providing the criteria for assessing the significancy of the policy. Also, the information security policy curve can move to B and C according to results of policy execution; B produces the effect of investment for bolstering the information security level while it increases the dysfunction due to new hacking techniques, worm viruses, etc. Meanwhile, in fact the policy curve can hardly move to C, which indicates occasions when the investment in the information security is decreased and the dysfunction declines.

[Table 4] Information Security Policy Items

Policy area	Information security level	Dysfunction level
Area I	Increase	Increase
Area II	Increase	Decrease
Area III	Decrease	Decrease
Area IV	Decrease	Increase

Thus, in light of the results of calculating the information security index, the current information security policy level stands at area II, where the information security level increases and the dysfunction decreases, leading to an assessment that the information security policy is very effectively working. As such, the information security index can be used effectively as a tool of evaluating the information security level and policy achievements. However, this research could not sufficiently measure the information security level of the e-government, in particular, due to lack of data regarding the public sector.

[Figure 3] Assessment of Effects of the Policy



V Conclusion

This research sought to more accurately measure the national information security level, convert it into an index, and develop index models and indicator systems aimed at helping establish a rightful information security policy direction and push for efficient informationization efforts. Indices and statistics, which are numeric information of all social and natural phenomena, not only provide the basic data for knowing social phenomena correctly, but also are inevitably necessary for establishing and maintaining the nation's system framework, inducing the consensus of the society's members, and pursuing the subsequent consistent national strategy.

Since indices provide important basic data for determining practical goals and policy direction, they are useful in measuring the degree of information development according to the passage of time, and

helpful in determining strengths and weaknesses of a particular nation with regard to the related area. More diverse relationships of influence can be determined by using indices comprising multidimensional factors such as social and demographic features and purchasing power, instead of using single-dimensional indicators.

The desirable national information security index, based on the role of an index, should first faithfully reflect the structure and content of the information society. Second, the NISI components should be limited to the core and direct areas of information security, thereby enhancing its realistic persuasiveness. Third, in order to have policy implications, the NISI should have explanatory power regarding not only the resulting phenomena of information security but also information security factors and their process. To that end, detailed indicator components should have a close relevancy to information security factors, and should be able to measure the process of changes in these factors.

Indices have the limitation of having to express a large amount of information in terms of numbers. Likewise, indices are useful in simplifying comparison, but since they involve methodological assumptions to apply to all target nations for comparison, missing value and incorrect data, it is dangerous to simply draw a conclusion from the comparison of indices. Thus, the information security index herein for the period of 2002 to 2005 is just an example, and should not be accepted as an absolute value.

The limitations and future research tasks of this research can be outlined as follows. First, the representativeness of indicator components should be verified. In other word, the NISI needs to be accurately defined. In particular, to ensure an international comparison, components that can be commonly applied to all concerned nations should be secured. Second, statistical indicators to measure each indicator should be quantified. For the convenience's sake, this research used the most accessible statistical data, but to calculate more accurate indices, each indicator should be put into statistics in advance. Third, indicators should be developed that can more accurately measure private information security, a recent social concern, and policy achievements.

<References>

Kang Sin-won(1999). "A Study on the Weighted Value in Measuring the NISI: a case study of RCSS," Research on Information and Communication Policies 6(2):47-64

Kim Seong-tae(2004). Information Policy Theory. Seoul: Bobmunsa.

National Intelligence Service(2005). A White Paper on 2005 National Security Policy.

NIS(2006). A White Paper on 2006 National Secuirty Policy.

Shin Il-sun(2004). "A Study on Economics Significance of Information Security," Information Security Review, KISA.

Shin Yeong-jin(2003). 「A Comparative Study on International Information Security Policies. Doctoral dissertation, Sungkyunkwan University.

Lee Jong-hwa(2005). A Study on the Government's Role in Ensuring Information Security in the Cyber Space. Doctoral dissertation, Chung-Ang University.

Jie Gyeong-yong(1999). "An Analysis of NISI by Nation," Analysis of Electronic Communications Trends, 14(4):81-92

Ministry of Information and Communication(2004). Status of International Information Security Indices.

Jung Gyeong-ho, Koh Eung-ryeol, Kim Dong-ryeol, and Min Gyeong-sik(2004). Methods of Evaluating National Information Security Levels, and Development of the Index, Institute of Information Technology Advancement

KISDI(1997). A Study on the Methodology of Developing Information Policy Indicators.

NIDA(2005). 2005 Korea's Internet Statistics.

NCA(2001). Measurement of National Information Level and Development of Its Indicators.

NCS(2004). Informationization Statistics.

NCA(2004). A Study of the Development of Comprehensive National Information Index Models.

NCA(2005). Informatiozation Statistics.

NCA(2005). A White Paper on National Informationization.
Korea Internet Security Center(1998). A Study on Development and Metering of Information Indicator Components.
KISA (2002). Development of Information Index Components and Their Methodology.
KISA (2002). Statistical Survey of Korea's Information Security Industry.
KISA (2003). Statistical Survey of Korea's Information Security Industry.
KISA (2003). Status of and Response to Hackings and Viruses.
KISA (2003). Report on the Status of 2003 Information Security.
KISA (2004). Report on the Status of 2004 Information Security.
KISA (2004). A White Paper on 2003 Private Information Security.
KISA (2004). Development of NISI Model.
KISA (2005). Report on 2005 Information Security Status.
Camp, L. Jean & Lewis, Stephen (2004). Economics of Information Security, London: Kluwer Academic Publishers.
Carley, Michael (1981). Social Measurement and Social Indicators, London: George Allen and Unwin, Ltd.
Cavusoglu, H., Mishra, B.K. and Raghunathan, S.(2002). "Optimal Design of IT Security Architecture." Working Paper, University of Texas at Dallas.
CSI/FBI(2003). Computer Crime and Security Survey.
Gordon, L. and M. Loeb (2002). "The Economics of Information Security Investment." ACM Transactions on Information and System Security,5(4): pp.438-457.
Hanemann, W.M., J.B. Loomis and B. Kanninen(1991). "Statistical Efficiency of Double-bounded Dichotomous Choice Contingent Valuation." American Journal of Agricultural Economics, Vol. 73: pp. 1255 ~ 1263.
Information Society Technologies(2003). SIBIS-New eEurope Indicator Handbook.
Land, Kenneth C.(1975). "Theories, Models and Indicators of Social Change." International Social Science Journal, Vol.27 No.1: pp.7-8.
OECD (2005). "OECD Communication Outlook".
RAND Europe(2003). Benchmarking Security and Trust in Europe and the US.
Saaty, Thomas(1980). "Analytical Hierarchy Process: Planning, Priority Setting, Resource Allocation." McGrew-Hill.

インターネット選挙運動の分析

高選圭（韓国選挙研修院）

Ⅰ．はじめに

ITの発達は我々の生活領域だけではなく、政治世界においても大きな変化をもたらしている。特に、インターネットに代表される新しいメディアの登場とサイバー政治空間の形成は政党活動及び選挙運動にも大きな影響を与えている。インターネットというメディアが持っている双方向性、正確性、リアルタイム的な性格は政治コミュニケーションにも画期的な変化要因として作用している。インターネットは従来のメディアとは異なり誰でもオープンされているコミュニケーションネットワークであり、時間的、空間的制約がなく比較的安いコストで政治情報の発信・受信が可能である。このようなインターネットが選挙に導入されれば、政党情報、候補者情報の充実、投票参加の増加、有権者と候補者間の選挙情報の交換、お金がかからない選挙の実現で既存の選挙政治の問題点を解決できるだろう。

そもそも政治コミュニケーションは政治システムの中で有権者、政党・候補者、メディアがお互いに政治情報を伝送・受容する過程で政治過程においても最も重要な部分を成している。多様な政治コミュニケーション過程でメディアは、大量の政治情報を伝達すると同時に効率的な政治コミュニケーションの手段を提供する。特に政治過程の中で世論を形成し、それを政治システムに投入する役割を行うのでその影響は大きい。有権者は政治コミュニケーションのプロセスでメディアを通じて政治情報を入手し、政治的争点を認知するとともに自分の意見を発信する。選挙の際、メディアの政治コミュニケーション機能は有権者に有用な政治情報を伝達する機能、選挙過程、投票の基準、政治的争点の設定などの様々な機能を行う。こういう意味からみると、政治コミュニケーションにおいてメディアの役割は非常に大きい。また、そのメディアがラジオ、TV, インターネットのメディアのどちらかによってその影響は違ってくるのである。政治コミュニケーションにおいてラジオ、TV, インターネットの中でどのメディアの役割と影響が大きいかという問題は、技術的な要因と社会経済的な要因、政治的な環境によって違ってくる。

今、世界は情報化の急進展によってインターネットで一つに結ばれている。政治コミュニケーションの機能においてもインターネットはメイン手段になっていると思われる。しかし、インターネットのメディアが持っている効果を最大化するためには制度的、技術的対策が必要である。世界の各国はインターネットを政治に導入するため様々な試みを行っている。韓国の場合も例外ではない。韓国の場合、世界最先端のIT技術とインターネット利用者が存在している。IT先進国への進入と共に韓国政治にもITを活用した新しい試みが進行されてきた。政党の政治活動と選挙運動へのITの活用は、韓国政治の非効率性を解決する手段として認識され、インターネットを政治活動と選挙運動に活用するため公職選挙法の改正など様々な制度整備を行ってきた。

現在、韓国の場合、既にITを選挙運動に導入するため制度的整備が行われ選挙においてインターネットを利用した選挙運動はある程度自由に行われている。今後、政治過程におけるITの必要性は益々増加していくだろう。既に多くの人々は自分の意見をホームページ上に掲示して意見交換を行っている。このような状況を考えると、選挙運動にインターネットを活用することはIT時代の必然的な流れであるし、今後、インターネットは選挙運動における政治コミュニケーションの主な担い手となるだろう。

本研究では韓国の選挙において政治コミュニケーション・インターネット選挙運動の内容と、候補

者ホームページ（ＨＰ）の構築状況、有権者、政党・候補者間の政治コミュニケーション手段として活用されているインターネットメディアの利用状況、その特性を分析してみる。特に、インターネット選挙運動の内容と特徴を共同生産活動・動員活動に焦点を絞って分析したい。 最後には今後の政治コミュニケーションにおけるインターネットメディア及び選挙運動の新しい可能性について考えてみたい。

Ⅱ．インターネットメディアと選挙運動

国際化とともに急速に進展してきた情報化の波は政治過程にも多くの変化をもたらしている。1990年代半ば以後の情報化の進展は全世界中にインターネットの普及をもたらし、これによる政治全般における変化は予想を越えて展開されている。インターネットの普及とともに政治過程の変化に対する期待はインターネットメディアの機能と影響に関する研究を多様な形で進行させるきっかけにもなった。

インターネットメディアの機能と影響に関する研究は、情報通信技術（Information Communication Technologies: ICTs）の発達は新しい政治コミュニケーション手段を提供し、政治過程においての効率性と政治参加が促進されより効率的で民主的な政策決定が可能な変化仮説(change hypothesis)が主流の立場をとってきた。しかし、政治過程におけるインターネットの活用に関する研究がアメリカを中心として展開され、その実証研究の結果が紹介されることによって従来とは違う議論が関心を引いている。

即ちサイバー政治コミュニケーションの実証研究では、政治コミュニケーションは従来の実社会あるいはオフライン上の政治権力構造がそのまま反映されるかもしくはその権力構造がオフライン世界より強化される結果になるという正常化仮説(normalization hypothesis)を主張している。サイバー政治コミュニケーションでは、インターネットの接続性が最も核心的な要因となる。従って、インターネットへの接続に関する普遍性がとれていない状況でサイバー政治コミュニケーションは、オフライン上の社会的、経済的、政治的格差と亀裂を反映することによって既存の政治コミュニケーションの補充手段として認識されている。

ICTs を活用して政治過程の効率性を高める動きは政府、政党、議員ホームページの活用のように既存の政治コミュニケーションとは差別化された形で始まってきた。従来の有権者の意見反映を目的とする政治過程への投入過程は利益集約の効率性のみを強調してきたので、国民の利益表出過程における参加を低下させてきたが、ICTs を活用した政治コミュニケーションは。有権者の意見を政治過程に投入する方法において効率性と参加を高める手段として認識されてきた。

特に選挙過程にインターネットの活用は ICTs を利用した政治コミュニケーションの代表的な事例である。また選挙過程にインターネットの活用は政治過程に ICTs を導入して政治過程の効率性を高める最も重要な部分である。選挙過程にインターネットの活用はオフラインの選挙運動とは違って、大量の政治情報を多くの有権者に発信することが可能となる。更に政党・候補者と有権者が双方向的な政治コミュニケーションが可能である。

しかし ICTs を利用したインターネットの政治コミュニケーションの利点は利用コストが非常に安く、24 時間、場所に関係なく有権者は政治コミュニケーションすることが可能な側面である。このようなサイバー政治コミュニケーションの利点は、政治的弱者、周辺集団に有効な政治コミュニケーションの手段を提供すると言われている。即ち、少数政党とその候補者に低費用で効率性の高い選

挙運動の手段を提供する。しかし、多くの実証研究では変化仮説で議論されている内容とは違ってオフライン上でより多くの政治的財源と経験を持っている政党・候補者の利用度が高いと報告されている。

前述の正常化仮説の説得力にも関わらず、ICTs が政治過程の透明性、迅速性、正確性を保障することで高費用の選挙競争構造は変わると思われる。このようなサイバー政治コミュニケーションのプラス機能からみると、選挙過程での活用が増大すれば候補者間の公平性の確保と有権者間の連携の強化、それから効率的な政党・候補者の広報・運動の手段となる。

一方では実際にインターネットの政治コミュニケーションは、有権者と候補者間の直接的な相関関係はないが、より幅広い選挙運動の場を提供するのみで何よりも大事なことは情報技術を使う主体の態度・認識、情報技術、社会構造と文化等によってその影響と役割は異なってくると言われている。世界の各国における政党のオンライン化を分析したノリス(Norris, 2000)は、情報技術の差異がオンライン政党の活性化程度を左右すると指摘しながらも、オンライン政治過程の活性化と効率性に関する技術決定論的な立場と論議を乗り越える理論的分析枠組みを提示した。彼はサイバー政治コミュニケーションの活性化はサイバー空間の形成だけで可能となるものではなく、財源と主体の活用目標のような要因も大きく作用すると分析している。このような意味でサイバー政治コミュニケーションとオンライン政治参加の活性化は、技術的、経済的、社会的環境、サイバー政治空間の形成による政治システム稼動、それから主体の資源(resources)・動機 (motivation) という変数によって左右される。

実際に、アメリカの選挙過程におけるインターネットの影響を研究した多くの研究者によると、インターネットメディアは政治的討論と民主主義のあり方に大きな変化をもたらし、より多くの政治参加を誘導すると説明している。インターネットメディアはより多くの政治参加をもたらすとともに新しい政党・利益集団・選挙過程に参加する主体を活性化すると分析しているが、オンライン世論調査、オンライン選挙運動、インターネット投票などは政治権力をサイバー政治空間上で再分配するよりはそれを集中化する属性があることを明らかにしている。

Ⅲ. 韓国の国会議員選挙における候補者のホームページ構築状況

本稿では国会議員のホームページを 3 つの形態に分類する。まず、議員個人が独自的にサバーを契約し独立的にホームページを運営する個人型である。2 番目は、政党ホームページの所属議員欄に自分の情報を掲載する政党依存型である。3 番目はホームページを持っていない閉鎖型と分類する。個人型が一番積極的に政党や議員個人に関する政治情報を提供する。これに対して政党依存型は消極的な情報提供であろう。[1]

2004 年 4 月 15 日行われた国会議員選挙で立候補した全体候補者は 1，166 人である。その中で候補者個人のホームページを構築し、有権者へ何らかの形で選挙情報を提供している候補者は 932 人、80%を占めている。候補者個人のホームページを持っていない割合は 234 人で 20%をしめ、まだホームページを開設ない候補者の数も少なくない。しかし、候補者の個人ホームページを構築している候補者の中でも 2．7%は独立したサバーを利用した形ではなく政党ホームページの所属議員・候補者欄に自分の情報を掲載する政党依存型であった。

選挙における候補者ホームページ構築は国会議員としての経歴、ホームページに関する認識、メディア接近性等とも深く関連性があると思われる。また候補者ホームページは各候補者の社会経済的属

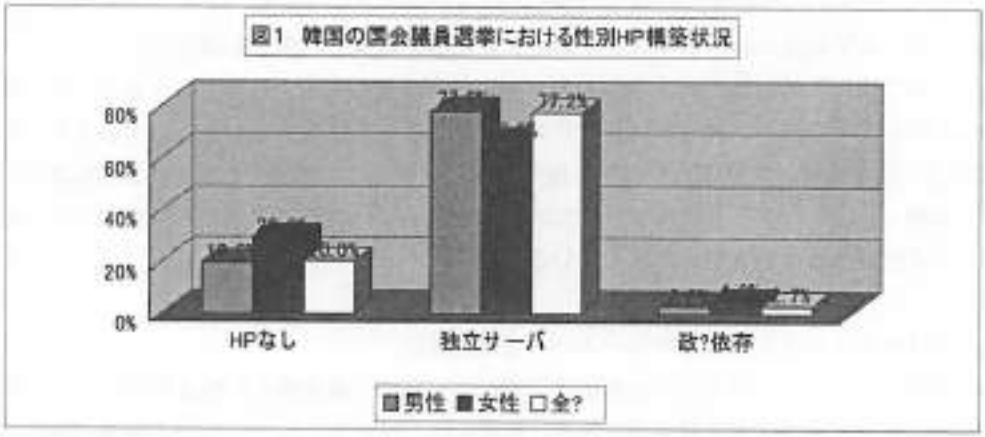
---

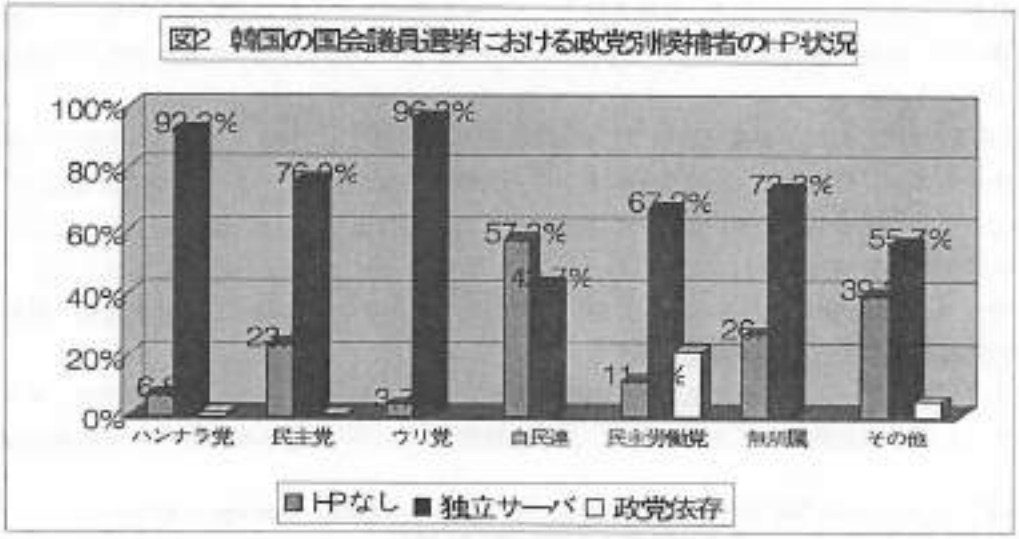
[1] Carlsin, Tom & Djupsund, Goran, "Old Wine In the New Bottle?: The 1999 Finnish Election Campaign on the Internet," *Harvard International Journal of Press / Politics*, Vol.6 No.1, Winter 2001, pp. 68-87.

性と関連性がある。

図1は、2004 年韓国の国会議員選挙における性別ホームページ構築状況である。男性の方が女性より候補者ホームページを持っている割合が高い。女性はホームページなし、政党依存型の割合が多いのが分かる。このような結果は、アメリカの分析結果と同じく正常化仮説を裏付ける結果となっている。しかし、図2で分かるように年齢による格差はないが、候補者個人ホームページを持ってない割合は年齢が増えることによって少しつつ増加している。2004 年 4 月の国会議員選挙で候補者ホームページ構築状況を年齢別にみると、特に候補者ホームページをもってない割合は、30 代 15. 1%、40 代 18. 8%、50 代 22. 1%、60 代以上は 23. 7%へ、年齢の増加によってその割合が増える。

図2は、各政党別候補者のホームページ構築状況を表しているグラフである。各政党別に見ると、ウリ党の候補者ホームページ構築比率が一番高い。その次がハンナラ党、民主労働党順で高い。自由民主連合（自民連）の候補者ホームページ構築比率は一番低い結果である。その次がその他政党、無所属、民主党の順で低い結果である。このような結果は既存巨大政党の候補者ホームページ構築の割合が高い。また、韓国政党の大半が人物中心の政党であるが、組織政党の性格が強い民主労働党の候補者ホームページ構築は高く、特に政党依存型の候補者ホームページが多いのが特徴である。民主労働党のこのような結果は政党の組織的な性格と関連性が深いと考えられる。





性別にホームページ構築状況をみると、男性と同じくウリ党の候補者ホームページ構築比率が一番高くてすべての候補者はホームページを持っている。その次がハンナラ党、民主労働党順で高い。同じく少数政党の自民連の候補者ホームページ構築比率は一番低い。従来の政治的資源が少なく、政治権力の周辺に存在している女性の場合でも巨大政党の候補者ホームページ構築の割合が高い。このような結果からでもインターネットを使った選挙運動でも実社会の社会経済的、政治的関係がそのまま反映されているような結果となっている。

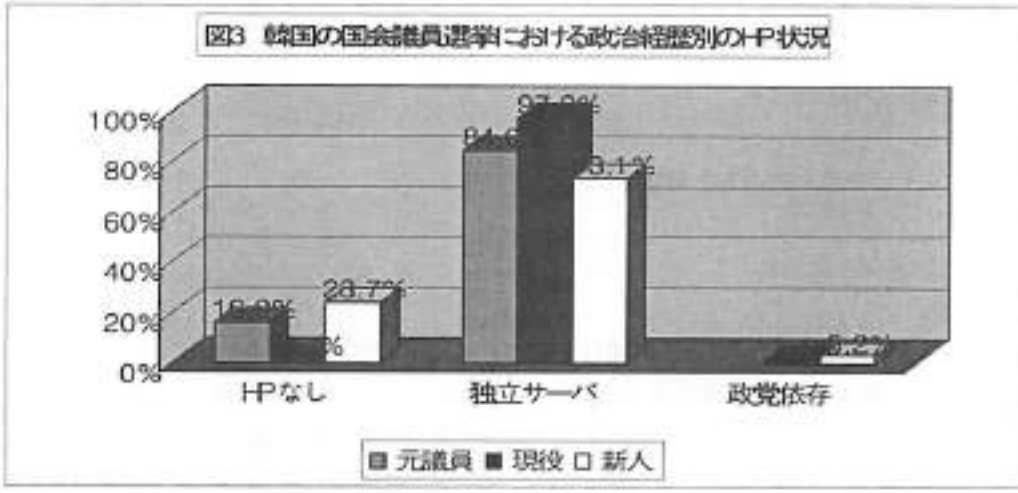


図3は、候補者ホームページ構築状況を候補者の政治的経歴に注目して調べた結果である。この結果をみても新人、元議員より現役議員の候補者ホームページ構築割合が高い。新人候補者ホームページは73．1%しか持っていない。この結果からでもより政治的資源を多く持っている前議員の候補者ホームページ構築率は高く現れている。

以上で2004年韓国の国会議員選挙における候補者ホームページ構築状況を国会議員としての経歴、各候補者の社会経済的属性と関連性から分析してみた。全体的な傾向としては、政党別にみると、ウリ党の候補者ホームページ構築比率が一番高く、その次がハンナラ党、民主労働党順である。このような結果は既存巨大政党ほど候補者ホームページ構築の割合が高いことをあらわしている。また、組織政党の性格が強い民主労働党の候補者ホームページ構築は高い理由は、政党の組織的な性格と関連性が深いことが明らかになった。更に候補者ホームページの構築パターンをみても少数政党・新党候補者ホームページは政党依存型がおおいのが分かる。

また、女性候補者のみをみてもこうのような結果は同じく現れている。女性候補者のホームページを政治的経歴からみても元議員・新人候補者は30%以上が自分のホームページを持っていない。女性候補者ホームページを政党別にみても、ウリ党の候補者ホームページ構築比率が一番高く、その次がハンナラ党、民主労働党順である。少数政党の自民連の候補者ホームページ構築比率は28．6%にすぎない。無所属の女性候補者ホームページ構築比率は46．2%で半分以上が持っていない。このような結果は、全体の傾向とあまり異ならないが、女性候補者のホームページ構築状況は政治的な資源の動員能力によってその格差が多いことが分かる。

以上の分析は情報化と候補者のホームページ構築は少数政党の候補者にも新しい機会を提供する

という従来の主張とは異なる現像が現れていることが明らかになった。インターネットの登場と新しい政治コミュニケーション手段は政治過程の効率性と参加の促進をもたらし、より民主的な政策決定・選挙競争の展開が可能となるという変化仮説がいわれてきたが実際はオフライン上の権力関係がそのまま反映され、更にそれが強化していく正常化仮説が現実化していることがこの分析結果から明らかになった。

これまでの分析結果は、インターネットという新しい政治コミュニケーション手段はコストが低く正確に更に多数の有権者へ候補者の情報を発信できる政治コミュニケーション手段にも関わらず、その活用においては異なる特徴があることが分かった。選挙過程でのインターネットの利用は内在的な標準化効果[2]をもたらすという議論とは反対の結果である。選挙過程では政党の規模と財源によって情報格差(digital divide)が拡大されていることが明らかである。

4. インターネット選挙運動の内容と特徴

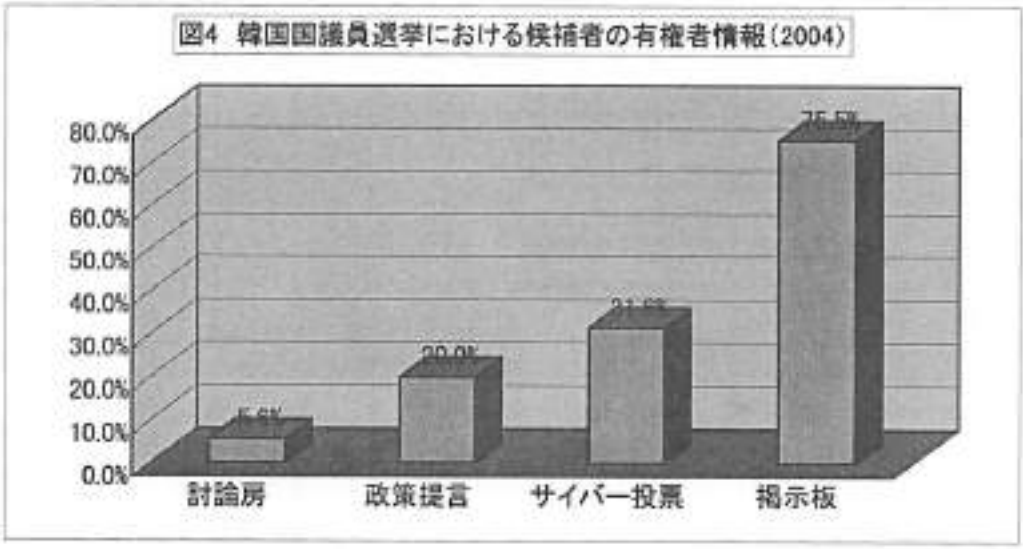
1）候補者 HP と共同生産活動

これまで 2004 年国会議員総選挙に立候補した候補者のホームページの構成とその内容を分析して全体的な傾向をみてきたが、韓国選挙では正常化仮説当てはまることが検証された。これからは、インターネットの特性は政党・候補者・有権者がネット上で共同参加の形で選挙運動は勿論政党・候補者の政策を共同参加の形で決めることが可能である。従って候補者のホームページで意見交換の場、複数の参加者による共同参加活動が行われているのか。また関連団体とのリンクの形で意見交換・情報交換が行われているのかという共同生産活動の有無を分析する。

次は、有権者の動員戦略の側面を分析する。候補者のホームページは多様な形で有権者を説得し、またその有権者が他の有権者を説得するいみで支持を動員する機能を果している。この動員戦略は候補者のホームページである特定の争点に対して賛成投票をさせると同時に争点に対する認知、アジェンダー設定の機能、投票交換の機能を通じて候補者の支持を最大化する。2004 年総選挙候補者のホームページがサイバー政治コミュニケーション手段として利用され、候補者の得票動員活動がおこなわれたかどうかを分析したい。

---

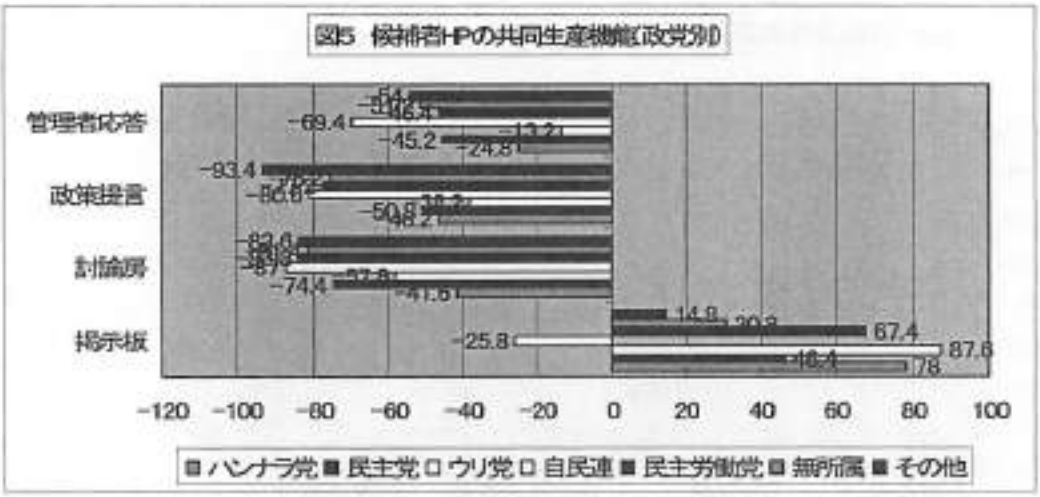
[2] Margolis, Michael, and David Resnick, and Joel D. Wolfe, ¡°party Competition on the Internet in the United States and Britain,¡±*Harvard International Journal of press/Politics*, Vol. 4, No. 4, 1999, pp. 25-47.



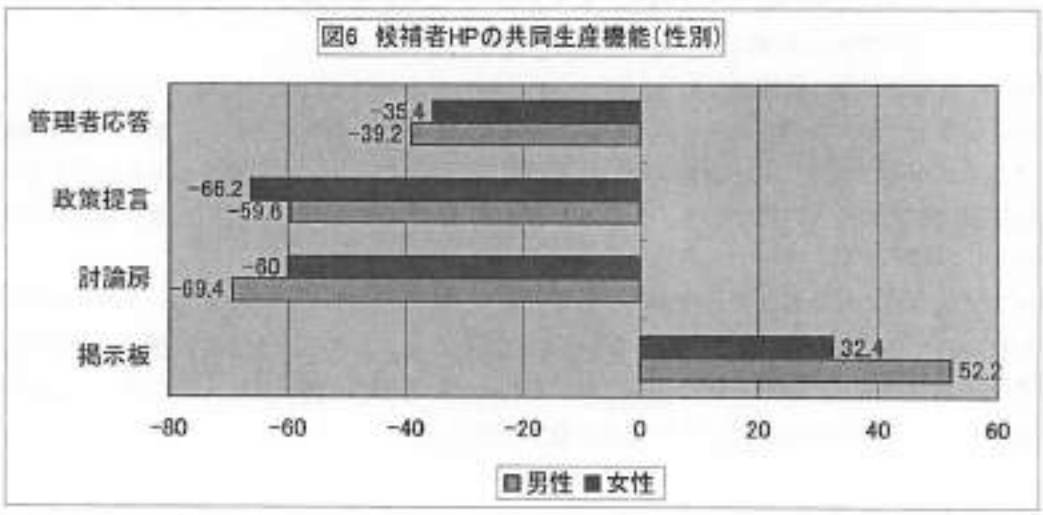
インターネットという新しい政治コミュニケーション手段は、時間的、空間的制約を越え 365 日何処からでも活用できる手段である。特に 1990 年代以後、韓国社会の急速な情報化の進展は国民生活に大きな影響をもたらした。韓国のインターネット利用人口は 2004 年に入り 3 千万人を突破している。超高速インターネット加入者 1,110 万、全国の 1, 430 万世帯の 70%以上へ普及した。地域からみても全国のほぼ 100%の町村に普及している。インフラの整備とインターネット利用者の増加によって政治過程にも大きな変化が起こっている。ネットワークの容量が高速化・大容量化することによってインターネットの環境は非常に良くなっている。

まず 2004 年総選挙の際、候補者のホームページ上で如何なる共同生産(coproduction)活動が行われているかを分析したい。候補者のホームページでは、全国の有権者が時間と空間を越え、選挙運動へ参加することが可能である。それは具体的に政策討論、政策提言、サイバー投票などを通じて候補者の政策を協働する形で生産可能である。このような機能は、インターネットという新しい政治コミュニケーションが持つ新しい属性である。

オンラインでは全ての政治参加者は政治的行為者であり、共同生産の担い手である。この共同生産が効率的に行われているのかは、まず複数の参加者が候補者のホームページ上で共同参加しているか。また候補者ホームページへの訪問者間の意見交換が行われているのか。他のサイトとのリンク機能がついて利用されているのかをみれば、その様子が分かるだろう。



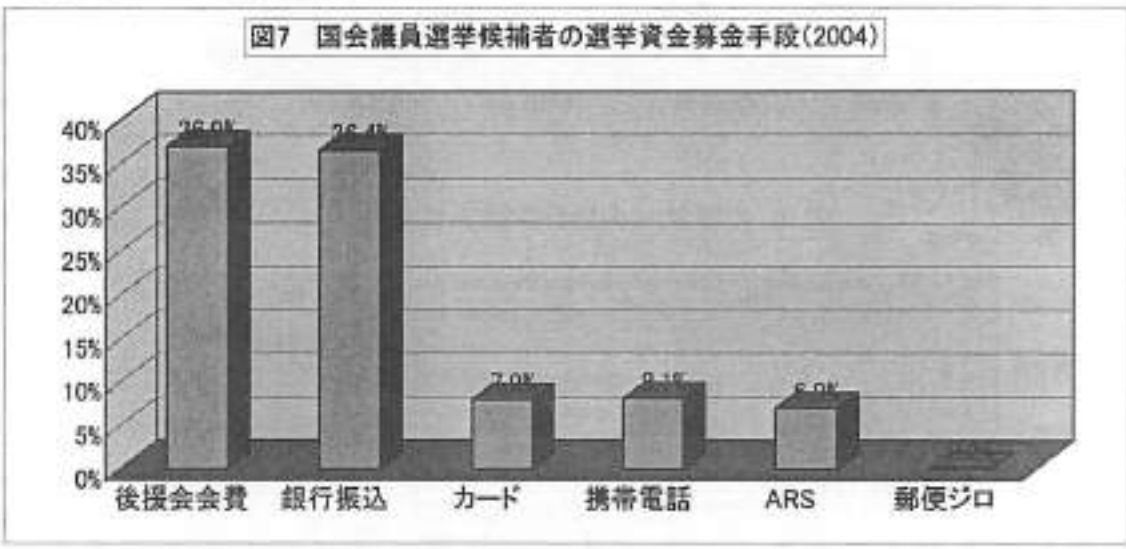
共同生産の活動の中で一番多く目に付くのは掲示板の討論で 75．5%の候補者が自分のホームページ上で掲示板を設置している。その次がサイバー投票で 31．6%である。このサイバー投票は選挙の争点となっている問題に対する賛成・反対投票を行いその結果で候補者の意見を決める。政策提言は 20%の候補者が共同生産の形で利用している。掲示板機能は従来と異なって有権者が自由に意見を述べるとそれに対して他の有権者もしくは候補者がその意見に対して返事を書くという形で利用されている。特にサイバー投票は 2004 年選挙の直前、大統領弾劾事件があり、それをめぐる賛成・反対の投票が多く行った影響である。

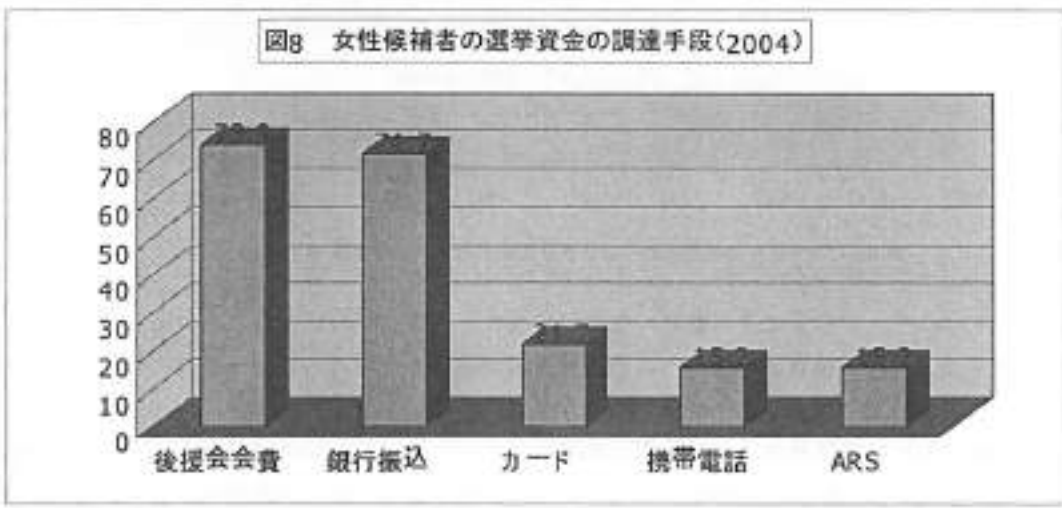


2）候補者 HP と動員活動

今まで政党と候補者ホームページは主に候補者の公約を一方的に有権者へ提供する機能のみをおこなってきた。また有権者は政党・候補者ホームページへ自分の意見を述べるレベルにとどまっていたが、今回の選挙ではサイバー政治コミュニケーションが活性化され、政党・候補者ホームページへ自分の意見を書くという消極的な方法から政策提言、政治資金後援、政策後援、サイバー投票への参加など多様な形で行われる。更に政治関連情報、資料提供、選挙運動関連の情報提供を通じても政治参加が行われる。このような結果は政党・候補者と有権者間の双方向的政治コミュニケーションが行

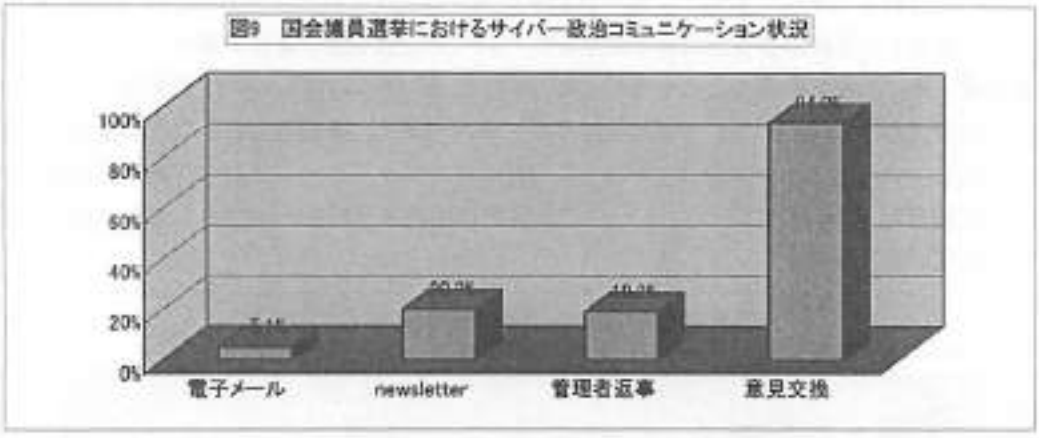
われていることを示している。
候補者ホームページ上で後援会加入と後援会の会費納付・寄付などは支持する有権者をネットワーク化し、その政治的資源を効率的に動員して選挙運動を展開する意味で非常に大事な機能である。
図7は2004年総選挙の全体候補者が自分の候補者ホームページ上で選挙資金の募集のため、設けている後援会会費・寄付金などの募金方法を分析した結果である。図8は同じく女性候補者ホームページを分析した結果である。全体の36．9%は候補者ホームページ上、選挙資金募金のため後援会の会費の納付と寄付金の銀行振込などを設けている。7．9%はクレジットカードで寄付金を払えるようにしている。また携帯電話の普及に伴って 8．1%の候補者は携帯電話料金の一部として寄付金を納付できるようにしている。

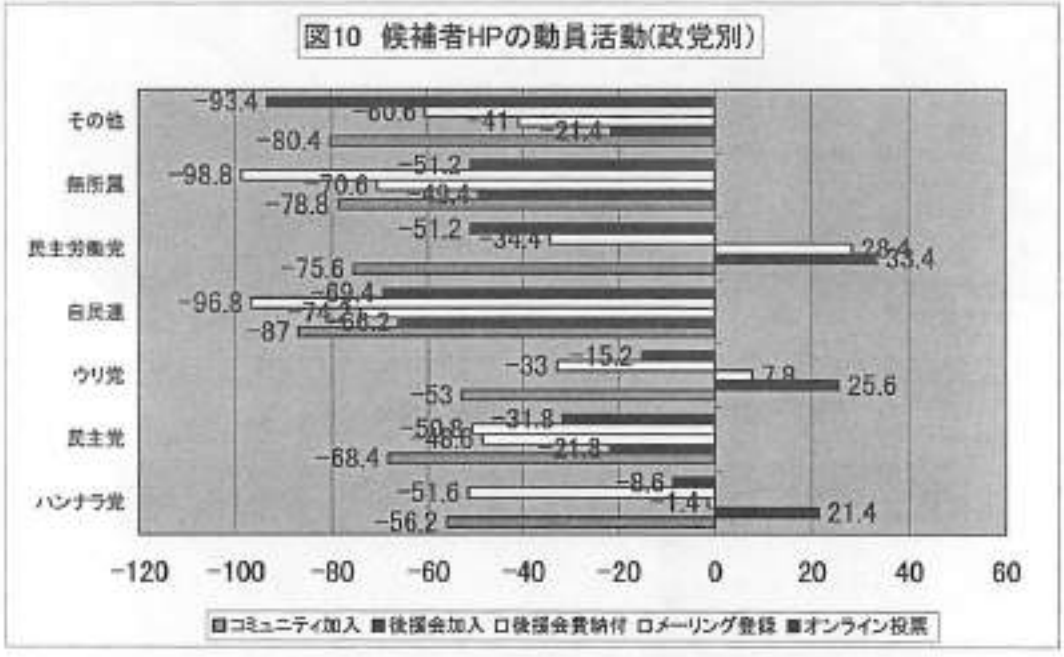




しかし女性候補者ホームページのみを分析してみると、全体の傾向とかなり異なる結果がある。70%以上の候補者ホームページが後援会の会費、それのための銀行振込番号を記載している。クレジットカード払いは21．7%である。携帯電話15．2%、ARS募金は15．2%である。このような結果は政治的資源が少ない女性候補者がより多くの選挙資金を集めるため、その通路を多様に確保している様子がうかがえる。特に民主労働党の女性候補者は可能な全ての選挙資金の募集手段を設定してい

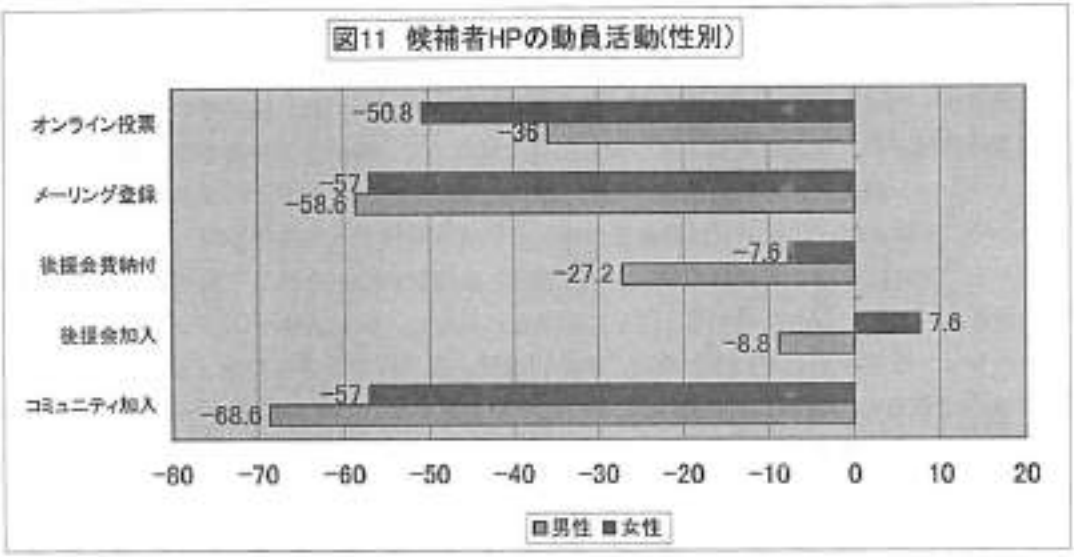
ることの影響が大きいと思われる。

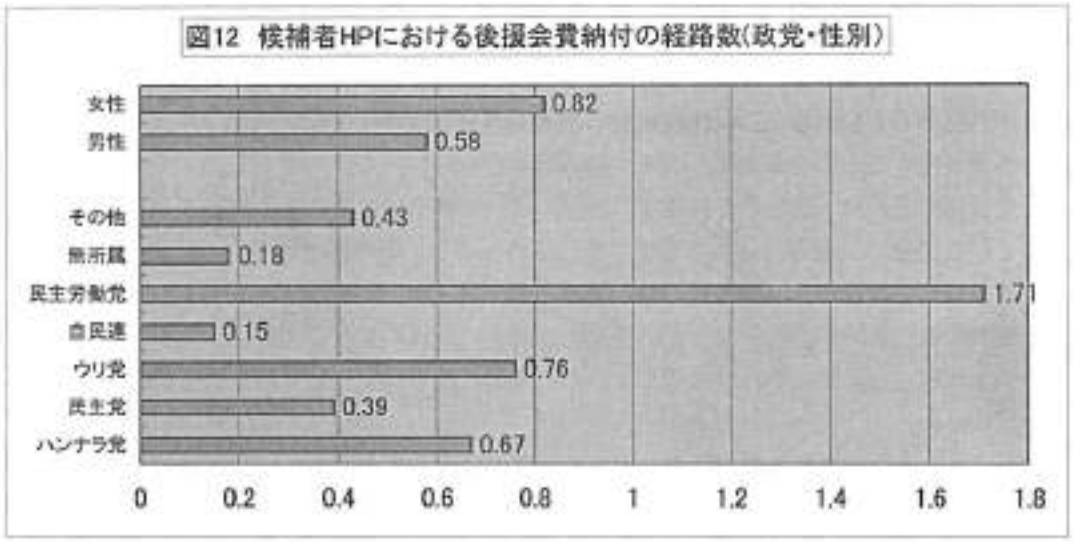




次は、候補者ホームページの中で得票動員のための候補者と有権者間の双方向政治コミュニケーション機能を分析する。特に候補者が有権者へ送る候補者情報媒体と有権者の質疑・提言に対する候補者の返事による双方向政治コミュニケーション機能を考えてみたい。

図9は2004年国会議員選挙における双方向政治コミュニケーションの状況と内容を分析した結果である。結果を見ると、94%の候補者ホームページでは掲示板での意見交換が行われている。この数字はかなり高い方である。掲示板が争点をめぐる意見交換の場になっていることを表している。





候補者ホームページ管理者への質問と要求事項に関する返事は2割程度である。また希望する有権者に対する候補者の情報をnewsletterの形で送る候補者ホームページも20%が存在している。女性候補者ホームページを分析した結果をみると、その割合が全体の傾向より高い。掲示板での意見交換の割合は全体傾向より低いが、候補者ホームページ管理者への質問と要求事項に関する返事は34%である。また希望する有権者に対する候補者の情報をnewsletterの形で送る候補者は21.7%である。電子メールで情報提供は39.1%で非常に高いことが分かる。このような結果は女性候補者のほうがより積極的に双方向政治コミュニケーションを行っていることがわかる。

図10から12までを見ると、候補者の動員活動においては政党・性別間の違いを分かる。まず、政党からみると、後援会加入、後援会費の納付において民主労働党の割合が一番高い。性別からみても、コミュニティ加入、後援会加入、後援会費納付、メーリング登録などで女性の方がより積極的である。図12の後援会費募金・納付の手段の確保からみても、男性より女性、韓国の巨大政党のウリ党、ハンナラ党より民主労働党の方が積極的で、数が多いのが分かる。このような結果は、従来の正常化仮説の主張とは違う現象であり、変化仮説を裏付ける結果である。またインターネットを選挙運動に導

入することによって生じた新しい現象である。また、このような分析結果は、候補者のHPが政治弱者である女性・弱小政党に非常に有用な選挙運動の手段として機能していることを明らかにした。

以上の候補者ホームページ上での共同生産活動と動員活動をみてみれば、候補者ホームページは単に候補者情報の提供という従来の制限された機能だけではなくて、候補者と有権者間の双方向的な政治コミュニケーション機能と選挙資金調達のため、様々な手段を設けて有権者の参加を呼びかけていることが分かる。候補者ホームページは候補者情報を有権者へ発信する大事な手段として認識していることが分かる。同時に有権者も自分の意見と政策提言、政治討論などを通じて候補者へ情報発信を行う際、候補者ホームページを活用する。従来の議論とは異なって候補者ホームページは双方向政治コミュニケーション機能を果している。特に、政治討論房、掲示板での意見交換、管理者への質疑・応答などの機能は双方向的な新しい政治コミュニケーション手段として候補者ホームページが機能していることを表す良い事例である。

V．インターネット選挙運動の新しい可能性

2004 年韓国の国会議員選挙における候補者ホームページ構築状況を国会議員としての経歴、各候補者の社会経済的属性から分析してみたが、全体的な傾向としては政党別にみると、既存巨大政党ほど候補者ホームページ構築の割合が高いことが明らかになった。逆に少数政党・新党候補者ホームページは政党依存型がおおい。また、女性候補者のホームページ構築状況は政治的な資源の動員能力によってその格差が多いことが分析結果、明らかになった。

このような韓国の結果は、情報化と候補者のホームページ構築は少数政党の候補者にも新しい機会を提供するという従来の主張とは異なる現像が現れていることが明らかである。インターネットの登場と新しい政治コミュニケーション手段は政治過程の効率性と参加の促進をもたらし、より民主的な政策決定・選挙競争の展開が可能となるという変化仮説がいわれてきたが実際はオフライン上の権力関係がそのまま反映され、更にそれが強化していく正常化仮説が現実化していることがこの分析結果から明らかになった。

しかし、インターネット選挙運動の活用と内容の側面では候補者ホームページは候補者情報を有権者へ発信する大事な手段として認識していることが明らかである。同時に有権者も自分の意見と政策提言、政治討論などを通じて候補者へ情報発信を行う際、候補者ホームページを活用していることが分かった。従来の議論とは異なって候補者ホームページは双方向政治コミュニケーション機能を果しているし、有用な政治コミュニケーション手段として利用されている。特に、政治討論房、掲示板での意見交換、管理者への質疑・応答などの機能は双方向的な新しい政治コミュニケーション手段として候補者ホームページが機能していることを表す良い事例である。

特に、選挙のお祭り(Festival)機能の活性化は従来の政治コミュニケーションでは考えられない新しい可能性を示唆している。有権者は政治・社会に対する不満を候補者ホームページへ接続し、そこでの参加を通じてその不満を発散・解消することが可能である。このような新しい政治コミュニケーション機能はインターネットが持つ大きな可能性であろう。

2004 年韓国の国会議員総選挙はインターネットを利用した選挙運動は、インターネットは双方向的な新しい政治コミュニケーション手段として有権者と候補者にも活用されていることが今回の分析で明らかになった。また、オフラインで不利な政治勢力である女性・小政党にも新しい政治資源動員の手段として機能していることが分かる。

社会情報基盤の課題

近畿大学　産業理工学部　情報学科

山崎重一郎

1. 本研究の背景と概要

2006 年は「Web2.0」というキーワードが大きくクローズアップされ注目を集めた年であった。そして、この年が本格的な情報化社会へのひとつの転換期であったと位置づけることが将来可能になるかもしれない。

Web2.0 というキーワードが象徴する社会の変化の背景にあるものは、普通の個人の日常生活レベルの感覚の変化である。例えば、何かちょっとした調べものをするときに、書籍や書類などではなくすぐにパソコンのデスクトップからインターネットのサーチエンジンで情報検索するということが日常化してきた。この何気ない日常行動の変化が次第に「サーチエンジンで検索できない情報は存在しないも同然」という感覚を社会の常識として定着させる可能性がある。さらに、ここでいう「情報」そのものの内容がめまぐるしい勢いで再定義が繰り返されている。たとえば自分が送った宅配便の現在の地図上の位置や図書館の書籍のスキャン画像やグループのメンバーのスケジュールまでもがブックマーク可能な情報になろうとしている。テレビや新聞よりも携帯やパソコンが身近になった多くの人々の日常の感覚の中で、商品やサービスが存在していること、人間が存在していること、人間の社会的行為の結果が存在していることなどの拠り所が現実世界から情報空間に重心が移動しようとしている。

本報告書では、まず「ファインダビリティ」という観点から、「情報」の存在が利用者の日常感覚の中でどのように再定義され変遷してきたのかということについて触れる。また、検索エンジンとともに重要性を増している RSS などによるライブ情報のプッシュ型の配信やタグ付けによる情報の組織化ついても情報のファインダビリティの視点から分析を行う。

また、この議論の中で検索連動広告のおける同義語の問題などを切り口に、利用者の認知モデルへの配慮の重要性についても言及する。さらに個人の認知のみでなく、Web 上でリアルタイムに変化する集団意識の形成やそこからコミュニティや友人関係などの人間関係を通じて情報を共同知として組織化する技術の研究の重要性についても触れる。

本報告書のもう一つの視点は「ディペンダビリティ」である。Web2.0 というキーワードが象徴するものの中には、もはや黎明期を終えごく普通の社会インフラの一部となったインターネットの姿が含まれる。インターネットの黎明期には、有志によるボランタリーな運営やベンチャーによる運営などが可能であったが、現在ではガス、水道、電気、電話などと同レベルの普通のライフラインのひとつとして安心して依存

できるような運用が強く要求されている。したがってそこの登場するプレーヤや技術もインターネットの黎明期とは大きく異なるものになろうとしている。Web2.0 のキーワードの下で認識されはじめたことは、この新しい社会情報基盤は、通信回線やネットワークのリーチャビリティを保証するというレイヤのみではなく、世界中の情報を記録する巨大なストレージや超強力な検索エンジンやその上でビジネスを展開したり情報の組織化を行ったりする情報処理のレイヤを含むということである。本報告書では、現在の Web2.0 的と言われている情報処理サービスのプレーヤが本当にディペンダブルなのかという観点で分析し、今後の日本の社会情報基盤の在り方について考察する。

最後に、本研究の主題である今後の社会情報基盤に求められる Web プライバシの問題について述べ、ひとつのモデルを提案する。この試論のポイントは社会情報基盤としての「人間の存在の情報化」である。人間の存在の情報化は、他の商品やサービスなどの情報化と異なり、安全性、利便性、コストに加えて人権に対するデリカシーを持った配慮と本人によるコントロールが常に失われないことが、技術に対してもシステムを運営する主体に対しても要求される。

我々は、そのような要件を満たす技術のひとつとして「仮名認証」の概念と SAML などの統合的な認証／認可のフレームワークに注目し、その具体像として「アイデンティティシェルタモデル」を提案する。そして、地域交通支援システムにおけるロケーションプライバシ保護という問題を題材にこのアイデンティティシェルタモデルを適用したシステムを構成し、ロケーションプライバシの問題に対してこのモデルが有効性を持つことを示す。

2. ファインダビリティ

Google Book Search を利用すると、ニューヨーク市立図書館などの公立図書館、ハーバード大学、スタンフォード大学、ミシガン大学、オックスフォード大学などの主要大学の図書館の蔵書の多くをパソコンのデスクトップから検索して閲覧することができる。このようなサービスが我々の日常の中でごく当然のものになったとき、わざわざ図書館に出かける機会は少なくなるだろう。

自分のパソコンのデスクトップや携帯の画面から世界中のどんな情報でも見つけることができるという感覚は、たとえそれが事実でなかったとしても私たちの日常の行動を変えてしまう力をもっている。

「ファインダビリティ」とは、ある手段を用いてその情報を見つけることができるということである。図書館の蔵書は、司書への問い合わせや書棚の分類コードや文献検索データベースによるファインダビリティを持っている。またインターネット上のドキュメントの多くはサーチエンジンを用いて検索できるというファインダビリティを持っている。整理されずに埋もれてしまい見つけることができない情報は存在しないのも同然である。

ファインダビリティは、情報検索のような手段のみを意味するのではない。我々は RSS やメールなどのプッシュ型の情報配信技術によっても情報の存在に気づくこと

ができる。しかし、重要なことはそういった技術が実際に我々の日常的な行動や感覚と結びついた結果として我々の世界観そのものに影響を与えているということである。したがって純粋に技術としての可能性の議論はあまり意味がない。

2.1. Web 上の情報の再定義

2.1.1. URI としての情報

現在の情報のファインダビリティの大部分を支配しているのは、Web 技術である。Web 技術の基本の一つである URL [RFC1808] は、Web 上のリソースの位置を識別するものである。URI [RFC2396, RFC3986] は URL の概念を拡張したものであり、URL と異なるところは、URI が必ずしもネットワーク上のリソースを意味するとは限らないことである。例えば名前空間の識別などにも URI が利用される。

```
URI = scheme ":" hier-part [ "?" query ] [ "#" fragment ]
hier-part     = "//" authority path-abempty
                                    / path-absolute
                                    / path-rootless
                                    / path-empty
```

図 1　RFC3986 の URI シンタックススキーマ

URI は、Web 上のリソースを表すものとして利用して定義されてきたが、その意味するところは Web 技術の進展とともに変化している。URI が指し示すリソースの最も基本は HTML などのファイル実体を持つリソースであった。ブログの記事へのリンクは記事データベースへのアクセス手段の識別を含むリンクになっている。さらに近年では Ajax のような技術が登場し、Google の Docs and Spreadsheet では、書きかけのドキュメントの全て状態に固有の URI が付与されておりブックマークすることができる。また宅配便の追跡機能におけるある時点における宅配便の地図上の位置や Web 上のスケジュール管理システムにおけるグループメンバーのスケジュール項目など非常に多様な情報に対して固有の URI を付与することが可能になってきている。

2.1.2. REST アーキテクチャスタイル

このように最近の先進的な Web 上のサービスにおける情報が極めて広範囲に URI で識別できるようになっているのは偶然ではない。REST (Representational State Transfer) とは、http プロトコルの設計者の一人として有名な Roy Fielding が、ウェブについて書いた博士論文で提案された Web システムのためのアーキテクチャスタイルすなわち設計原則である。

REST の設計原則

(1)ステートレスなクライアントサーバープロトコル

ひとつの HTTP メッセージがそのリクエストを理解するために必要な全てのコンテクストや状態の情報を含む。したがって、クライアントもサーバーも、セッションの状態を記憶しておく必要がない。

(2)すべてのリソースに適用できるメソッドセット

HTTP に定義されている４つのメソッド "GET"、"POST"、"PUT"、"DELETE" ですべてのリソースを操作する。

(3)URI の利用

REST に準拠したシステムでは、すべてのリソースが URI による一意的な 表現を持つ。

(4)アプリケーションの情報と状態遷移の両方を「ハイパーメディア」側で扱う

HTML または XML データの中に情報およびその他のリソースへのリンクを含める。こうすることにより、ある REST リソースから他の REST リソースを参照したい場合は単にリンクを辿るだけでよくする。

近年の Web システムのほとんどのものが REST のアーキテクチャスタイルの影響を受けている。その例を以下に示す。

* ブログシステムの大部分は REST ベースである。ほとんどのブログシステムでは、他のリソースへのリンクの一覧を含む XML ファイルを RSS 2.0、RSS 1.0、Atom などのフォーマットでダウンロードするようになっている。

* Amazon.com は REST 版と SOAP 版の API を公開しているが、REST バージョンがトラフィックの大部分を占めている。

* eBay は REST 型の API を提供している。

* Yahoo! は REST 型の API を提供している。

* Ruby on Rails では、MVC デザインパターンを使うことにより、RESTful アプリケーション設計を支援している。

2.2. ビジネスのファインダビリティ

「検索エンジンで見つからない商品やサービスは存在していないも同然」という日常感覚が一般化するとともに、検索連動広告の重要性は重くなっている。Google Adwords 広告は、広告主が Google のサイトから自分の広告文とキーワードを直接登録する。そして利用者がキーワードを検索したときに登録した広告文が検索結果の右側に表示されるという仕組みである。広告料金は、広告がクリックされたときだけ掲載料が課金される完全クリック保証型であり、発生する料金はオークションで決まるキーワード単価とクリック回数に基づいて算定される。

2.2.1. 広告の網をはるのに何語のキーワードが必要か？

検索連動広告は気軽に始められ、広告効果がなければ課金も少ないという点で広告主にメリットの多い広告方法のように見える。しかし、実際に広告効果を出すには多くの試行錯誤の努力が必要である。その最初が、利用者を自分の広告に誘導するため

にキーワードの網ををつくることである。では、一つの広告を有効に行うために一般的にどの程度の数のキーワードが必要だろうか？

Google社の担当者からのアドバイスによると平均して2000語から50000語であるという。これは想像を絶する数である。試みに自分が所属する企業の商品に関連するキーワードを連想してみると容易に了解されることだが、ひとつの商品について一般的な人が思いつくキーワードは200~300語程度がせいぜいである。この問題を解決するには、キーワードの自動的な生成などの言語処理システムのアシストが必要である。しかし、単純な同義語や類義語や関連語によるキーワードの拡張だけでは効果的なものにはならない。

2.2.2. 「オール電化」の広告ランクが低い？

キーワードの単価はオークションによって決定されるため、より多くの広告予算を持つ企業が有利なように見える。しかし、潤沢な広告費を持つ電力会社が推進する「オール電化」というキーワードのランクは低いままにとどまっている。しかし、その理由は明白である。単純にそんなキーワードで利用者は検索しないからである。利用者が「オール電化」住宅について知りたいのはどのようなときかという利用者の文脈を考えると、「リフォーム」→「オール電化」や「マンション経営」→「オール電化」や「火災保険」→「オール電化」というような流れが考えられるかもしれない。これらのキーワードは明らかに辞書的な類義語検索によるキーワードの自動拡張では生成することが困難であり、利用者の行動や文脈を理解しようとしなければ発想することもできない。

2.2.3. 検索連動広告のおける同義語の問題

辞書の上では「同義語」とされるキーワードが、実際の利用者にとっては同義語ではないこともある。例えば「USBメモリ」と「フラッシュメモリ」が同じものを指すと知らない利用者から見れば、この二つのキーワードは同義語ではない。したがって「USBメモリ」を購入しようとして検索を行っている利用者が「フラッシュメモリ」の購入ボタンをクリックすることはない。

Google Adwordsではひとつの広告に対して用意される広告文のパターンが50ほどにもなるのが普通である。なぜそれほどの数の広告文のパターンが必要かというと、利用者が検索に利用したキーワードを同じ語が現れる広告文を選択して表示するようにするのがその理由の一つである。利用者の行動や状態や興味など、実際の利用者の分析が検索連動広告効果の成功の鍵であると言って間違いないであろう。

将来的には、検索結果画面に表示される広告文だけでなく、実際に誘導した商品購入サイトのWebページそのものも、そこを訪問したそれぞれの利用者のコンテクストに基づいてキーワードなどを利用者に適応させる技術が登場すれば、商品購入のクリック率もさらに上がるかもしれない。

2.3. プッシュ型情報配信によるファインダビリティ

情報のファインダビリティにとって重要な技術は検索連動広告だけではない。RSSや電子メールのメールマガジンなどを利用したプッシュ型の情報配信も我々の日常に浸透した情報配信のシステムである。その中で、電子メールを利用した広告についてはスパムの蔓延によってすでに有効性は著しく低下している。メールマガジンの大きな問題は、配信停止のコントロール権が事実上本人にないということである。大手メーカが運営主体であっても、メールマガジンの配信停止の手続は非常に煩雑であり、一つのメールマガジンの配信を停止するために数時間を無駄にすることもまれではない。

これに対して RSS は純粋なプッシュ型ではなく、RSS リーダなどからのプル型のシステムであるため、配信の停止は完全に利用者が自分でコントロールできる。この利点が広く利用者に認識されるにしたがって、メールマガジンによる広告は RSS による広告配信に移行していくであろう。

2.3.1. サイトサマリかシンジケーションか

RSS には 2 系統の標準化があるが、この 2 つの標準はそのまま RSS の二面性を表している。一つは RDF をベースにしたサイトのメタ情報であるという定義であり、もう一つは Web システム上でライブな情報をシンジケーションするシステムであるという定義である。前者は、セマンティック Web の構想に基づいた Web 全体の壮大な意味論的体系の構築を目指しているのに対して、後者はライブで HTML よりもリッチな構造を持つ Web 情報の流通基盤を目指している

これら二つの側面は、今後の Web システムにとってどちらも重要な技術である。これまで相反する二つの側面を持ったシステムをどちらも「RSS」と呼んできたために混乱が生じたが、後者の標準として ATOM [RFC4287]が策定されたため、この混乱は納まっていくものと考えられる。

ファインダビリティの視点から見ても、サイトの内容を俯瞰するメタ情報の視点と様々なサイトに起きているライブな事象をリアルタイムに気づくことを可能にするシステムは共に重要である。

2.3.2. タギングとオントロジー

iPod で聴く音楽を管理するソフトである iTune や Web 上で写真のデータをみんなで分類できるようにした flickr や Google が提供する電子メールシステムの Gmail などでは、従来の階層構造を持つフォルダーを使った情報の分類の代わりにタギングやラベル付けという手法を用いている。

タギングは構造をもたないアドホックなキーワードを情報に付加するものである。タギングは体系を持たず、表記の揺れなどについてもあまり考慮しないため、冗長で統一性を持たない。しかし、画像や音楽などの情報への様々なイメージを想起させるキーワードのタギングはファインダビリティにとって重要な手がかりとなる重要なメ

タデータであり、実用上ではきわめて有効である。

オントロジーとは一つの世界観を矛盾無く階層的に体系化したものである。その思想においてタギングとは対極にあると言ってもよいであろう。オントロジーの最大の問題はその構築の困難さである。多数の利用者によってタギングを行うフォークソノミという手法があり成功しているが、同様のことを一定のオントロジーに基づいて実施することはほとんど不可能である。

2.4. 利用者の認知モデル

検索連動広告における同義語の問題でも触れたが、個々の利用者がどのように言葉や世界を認知しているのかという「利用者の認知モデル」をできる限り正確に理解し、それぞれの利用者に対応した表現を提示することが重要である。

2.4.1. 利用者とビジネスとのマッチング

本当の利用者の認知や意図を知ることは極めて難しい。しかしそれは検索エンジンのクエリに使われた言葉などの表象として観測することが可能になる。また一方で、ビジネスの側も自分の内容を何らかの表象として利用者に観測可能な情報としなければならない。

このようなマッチングを理解するための研究としては、人工知能における知識フレームによるアプローチ、ブルックスらの自律ロボットの制御に端を発するある状況の中において表象を用いずに行動から直接的に意味を導く行動主義的アプローチ、生物の自己保存や自己創発の原理に基づく人工意識や人工生命のアプローチなどがある。これらそれぞれの研究にそれぞれの優れたところと欠点がある。それぞれの技術を適材適所で利用するアプローチが必要であろう。

Web 上のメタデータを組織化するオントロジーやタクソノミーに基づくアプローチは、この中で人工知能的なアプローチに近い。Google Analytics などの行動履歴情報から利用者の意図や認知内容を推理するアプローチは行動主義に近いと言えるかもしれない。利用者を一つの生命体としての生存し続けるために合理的に環境に存在する情報を得ようとする人工生命や人工意識的なアプローチも今後重要性を増してくるのではないかと考える。

2.5. Web 上の集団意識の形成

インターネット上で利用者の集団が自ら情報内容を生成していくメディアのことを CGM (Consumer Generated Media) と呼ぶ。SNS をはじめとして現在 Web2.0 ビジネスで成功しているものはこの CGM を有効に利用していると言われている。「ブログから、話題を知る、きざしを見つける」ということを目的としている kizasi.jp も、このような CGM の実例の一つであろう。

非常に多くの人々が世界にあるニュースや出来事に対して何らかの反応を行った場合、そこにそれも一つのファインダビリティとみなすことが可能である。このような

多数の人々が表示した表象と実際の購入や移動などの行動を結びつけることは、一つの社会のトレンドを形成する集団意識の一部を表現しているといってよいであろう。集団意識にも個人の意識と同様に意図や合理的判断が含まれる。アドワーズのようなマーケティングツールが対象としている顧客像も典型的な利用者の意図や行動のシナリオであるとともにこのような集団意識にも近いものかもしれない。

2.5.1. 意識の階層

意識を自然科学的な研究対象とすることは、技術的に難しくまた倫理的にも抵抗があったため、本格的に研究が始まってからまだ日が浅い。動物に意識があるのは植物が光合成をするのと同様に生存に必要だったから進化の過程で発生したという生態学的アプローチも、意識や自由意志も一つの物理現象であるという物理学的アプローチもまだ万人が納得できるような理論を構成するには至っていない。

しかし、我々の意識がどのような性質を持つのかという研究は多くの蓄積を持っている。特に意識には階層があるということは多くの研究者が同意するものである。たとえば、サッカーをしているときにドリブルでゴールに接近できるときにはドリブルを行うことのみに意識を向けているが、敵に囲まれてドリブルを継続できなくなったときにパスを渡すべき味方を探すための上位の意識が働きはじめる。しかしこのときも並行して敵をかわしながらドリブルを続けることが可能なのは、無意識のレベルに落ちた意識が継続して存在しているからである。

ロボットの人工意識の研究を行っている喜多村は、意識を次のような5階層のものとして分析している。（1）生存の基礎反応があること、（2）持続した知覚と反応行動があること、（3）対象を空間と時間の中で捉えること、（4）概念として知覚できること、（5）自分自身の行動や思考を知覚できること。そして喜多村はこのような階層は、高等生物が下等生物を捕食するモデルに適用できるとしている。

2.5.2. 感情による情報処理

感情も意識と同様に自然科学の研究対象として扱われるには紆余曲折があったが、感情は生物の生存にとって必要な機能であり、生物の情報処理にとっても重要な役割をはたしている。恐怖心は危険を察知し逃走するために必要な身体のモードである。怒りも闘争に勝つために必要な身体のモードである。喜びも生命を維持するために重要な役割を果たしている。

感情は言語をもたない動物にも備わっている。生物にとって感情は言語よりも優先する情報である。動物の記憶は感情と結びついている。生物の記憶が生存を有利にするための情報だとすると、恐怖などの感情とのつながりがあって初めて記憶は生存にとって意味のあるものになるからである。いずれにしても、感情を持たない生物あるいはロボットは、自然界の中に投げ出されたときに生き残るための効率的な情報処理を行うことが難しいことは容易に想像でき、環境適応を必要とする情報システムには感情に相当するような何らかの機能を導入する必要があると考えられる。

我々は情報空間という新しい自然の中に投げ出され、新しい環境適応を迫られてい

る。そこで重要な情報は捕食者や食料などではなく、経済的に豊かになるための情報や犯罪やプライバシの危機などから身を守るための情報などであろう。

2.5.3. 「共感機」としてのWeb

蟻や蜂などの社会性生物は、自分たちの巣への進入者に対して群れ全体が集団的感情といえるような反応を示す。人間の感情も社会的な意味を持っており、集団意識と同様に集団が様々な感情を共有しそれが集団としての記憶となっていくという側面を持つ。

Kizasi.jp や SNS やソーシャルブックマークなどは、「集合知」として理解されることが多いが、共感のメディアとして側面にももっと注目すべきであろう。Web の中に相互にシンクロし現実の人間関係以上に共感を強めていくコミュニティが出現しはじめている。ATOM や SNS などのようなライブ情報のファインダビリティをコミュニティや人間関係の中で相互にシンクロさせる技術は、Web を共感機にする可能性をもっている。

粘菌は、独立した生物の集合体でありながら、頭部や尾部などの機能が分化しコロニー全体でひとつの生命体のようになっている。セカンドライフのような仮想世界を利用した Web システムは、共感機の中に自然に機能分化をもたらしさらに精緻で高度な集団意識を作り出すかもしれない。

2.6. 人間の存在（アイデンティティ）

2.6.1. 個人情報の必要性

個人情報保護法の施行時、個人情報は企業資産ではなく個人から預かった負債であるという認識が広まり、多くの企業で既存の個人情報を放棄し収集を止め個人情報の周辺から逃走するという行動がとられた。

しかし、Web2.0 企業と呼ばれる企業の多くは、無料のメール ID の提供サービスや Web サービスのカスタマイズなどを軸に、個人のあらゆるプロファイルや商品購入履歴や移動に関する情報や文書情報などを徹底的に収集しようとしている。

日本の個人情報保護法は、本来の主旨からいえば、個人情報を合法的に収集し活用するためのルールを定めた法律であったが、法の施行時に監督官庁が示したガイドラインは実施がきわめて困難なものやあいまいなものが多かったことが災いしたといえる。一方で、Mixi やはてななど個人情報保護法に臆さず、個人情報の合法的な収集と活用に知恵を絞った企業が Web2.0 における勝ち組になったともいえる。

検索連動広告においてもコミュニティ型のシステムにおいても、個人のプロファイルと行動履歴から導かれる利用者の認知モデルの推定とそれに対する利用者適応が非常に重要であることはすでに指摘した。そしてこのような個人情報を収集するためには、アイデンティティ管理の基盤が必須となる。

2.6.2. アイデンティティ管理の社会基盤

日本における個人のアイデンティティ管理というとすぐに思い起こされるのが住民基本台帳カードである。また、インターネットにおけるアイデンティティ管理では公的個人認証制度が存在する。これらは、現在も政府や自治体によって莫大な支出が維持されているが、利用率の低さは惨憺たるものであり、ニーズのないところに過剰な投資が続けられているという感は否めない。近い将来、財政的理由によって縮小されていくことは避けられないであろう。

アイデンティティ管理に対する反応は、国民性や歴史的要因によって大きく左右されるため、国際的な比較はあまり意味がないが、日本と同様に出だしが遅れていたアメリカでもID管理用のICカードの普及が始まった。

米国大統領指令HSPD-12は、９．１１テロ事件の後に発行された連邦政府職員および請負業者のための個人識別に関する制度設計ポリシーである。このICカードの標準は、徹底した情報公開の下で実施されているところが日本の住基カードとは大きく異なる点である。技術標準案の公開にともない、1900件ものパブリックコメントが集まったという。特にミドルウェアレベルでのテストベッドが公開されており、開発者が相互運用性をテストできるようになっているところがアイデンティティ管理の基盤として優れている。この大統領指令は計画通りに実施されており、2006年10月にICカードの発行が開始された。2009年までに2000万枚のカード発行が計画されている。

日本においても、住基カードや公的個人認証の失敗をきちんと失敗として反省的に分析したうえで、日本の社会情報基盤のための個人認証基盤の構築にむけた次のステップのビジョンを検討する必要があるだろう。

2.6.3. 人間のファインダビリティ

Google八分やMixi八分ということばがある。これは違法行為や迷惑行為を含むサイトや人をシステムの対象から除外することである。政府や自治体のような機関が法に基づいてこのような除外を実施するだけでなく、コミュニティが自治的機能としてこのような除外を行うことは合理的だといえる。

しかし、たとえば、もし検索エンジンサービスの主体に対して批判を行った者の情報をそのサービスのインデックスから外すというような行為が行われたとすると、それは人間の存在を抹殺するのに近い損害を与える可能性がある。

ファインダビリティと結びついた人間のアイデンティティに関する新たな法制度などのルールが必要となるかもしれない。

2.6.4. SNSにおけるアイデンティティとプライバシの問題

人はどのようなことに傷つくのかという感覚には大きな個人差がある。自分を批判されるよりも、自分の家族や自分が所属する企業や学校の批判を辛く感じる人もいる。出身地や宗教や信条や嗜好に対する批判に傷つく人もいる。このような感覚は、国民

性や世代や性別や文化などによっても違いがあり、共通の基準を見つけることは困難である。そしてこれがプライバシの問題を難しくしている原因の一つである。

SNS は、欧州の基準ではプライバシ情報の中でもハイセンシティブなものに分類される人間関係の露出を前提にしたシステムである。ひとりの人間にも様々な社会的な顔があり、そのそれぞれに異なった人間関係が存在している。家族の中での自分と教師としての自分と友人との間での自分は少しずつ違ったプライバシ的特性を持っている。そして、このような特性の違いが情報共有にも難しい問題を生じさせる。

たとえば、地震などの災害が発生したときに、家族や親戚や同僚や友人の安否を確認したいという動機で SNS を利用することは可能だろうかというと、それは困難である。通常時の友人との間の趣味の話などの情報は、家族や親戚などに公開するのが適さないものもあるだろう。

2.6.5. 人間関係で構成される情報空間

しかし、SNS の成功は、それまで社会学や複雑系システム学などの分野で検討されてきたさまざまな理論やモデルがシステム的に厳密に調査可能になり、さらにそれを活かしたシステムやサービスを提供可能にした。

伝染病や山火事や液体の浸透などを記述する方程式が、実際に流行の伝播やマーケティングなどに適用できるのか。スモールワールドネットワークの理論や相転移の理論などが社会現象を実際に説明できるのかなど興味深いテーマが実際に情報システムとして検証可能になっている。

SNS は、このような人間関係で構成される情報空間の最も原始的なものであり、今後より高度なシステムに発展していくであろう。そのとき、利用者が希望することが自由に簡単にできることとプライバシの問題の両立させることが重要な課題になる。

3. ディペンダビリティ

ここまで社会の情報化が我々の日常感覚にまで浸透し、情報の存在のありかたが情報空間の側に重心が移動してきたことについて説明してきた。しかし、本当に現在の社会情報基盤はそれに依存しても大丈夫なのだろうか？

確かにメールも文書管理も帳簿も Google を無料で使うことで実行できる。営業活動も人間が歩き回らなくとも、検索連動広告をうまく活用することで実行できる。無料のサービスなのでコストの観点からは圧倒的に有利でしかもサービスの質は高い。したがって同様のサービスを有料で行っている企業は太刀打ちできずに急速に淘汰が進むと考えられる。そのような無料で無保証のサービスを本当に社会情報基盤とみなしてよいのだろうか？

3.1. 「情報がずっと存在している」ための適切なプレーヤ

「世界政府というものがあったとして、それはどのようなサービスを提供すべきだろうか？」ということを Google は考えていると「web 進化論」の梅田望夫は書いて

いる。実際に、それを裏付けるように情報の存在とファインダビリティが同義になろうとしているこの世界の基盤を支えているのは Google の計算機システム群である。しかし、図書館や博物館のように現在の情報の存在を支える基盤が 100 年後にも利用可能でなければ社会情報基盤とは言い難いであろう。そういう意味で、やはりこのようなサービスは本物の政府機関が担うべき仕事であると考えざるをえない。

3.2. 黎明期を終えた社会情報基盤への投資

Google が示した Web2.0 とは、結局、社会情報基盤のプレーヤは圧倒的な力を持ったものが勝つというシンプルな原理である。超強力な計算能力、超巨大な記憶領域、超巨大な情報資産と最優秀な頭脳集団の存在が Google の立場を揺るぎないものにしている。

黎明期を終えたインターネットを中心にする社会情報基盤の主たるプレーヤーは NTT などの通信インフラを運営できる圧倒的な力を持つ大企業である。すでに地域プロバイダなどの役割は終わっている。中規模のプロバイダでさえ今後生き残ることは難しいだろう。

日本政府の社会情報基盤への投資のロジックは「200X 年までにすべての行政手続を電子化する」といった官僚主導型で明確な目的を欠いた情報化のための情報化が目に付く。しかし、無駄を黙認している余裕はすでになく社会情報基盤への徹底的に効率的な投資が必要になっていると考える。

4. Web プライバシとアイデンティティシェルタモデルの提案

4.1. 「仮名」(Pseudo Identity) 概念によるアイデンティティの保護

4.1.1. 我々の仮名の定義

我々は、「仮名」という用語を専門用語として導入し、特に「匿名」の概念と区別して用いる。我々の「仮名」は、現実の本人の属性と権限の正確な射影につけられた名前であり、名前以外には虚偽の情報を含まないものとする。そして、その内容の正確さは、信頼できる第三者によって保証される。仮名は、投票、決済、通報、取引などの行為を行う権限と責務を持つことができる。また、与信を受けることもできる。我々が提案する仮名は、EU の PRIME プロジェクトにおける pseudo identity の概念と類似しているが、仮名認証の手段を含めてより明確に定義するものである。

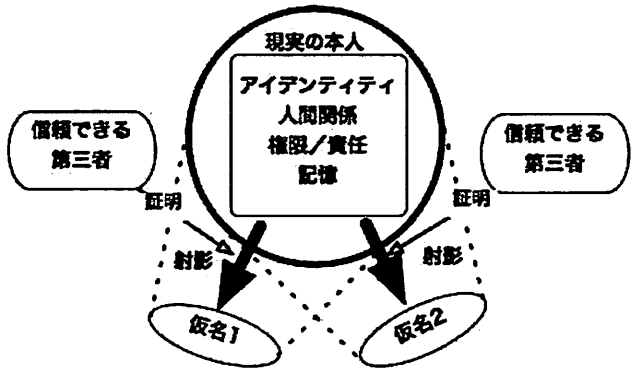


図 2 本人と仮名の関係

4.1.2. 仮名認証と仮名認証書

我々の仮名認証は、通常の PKI やその上の属性認証基盤などを利用する。

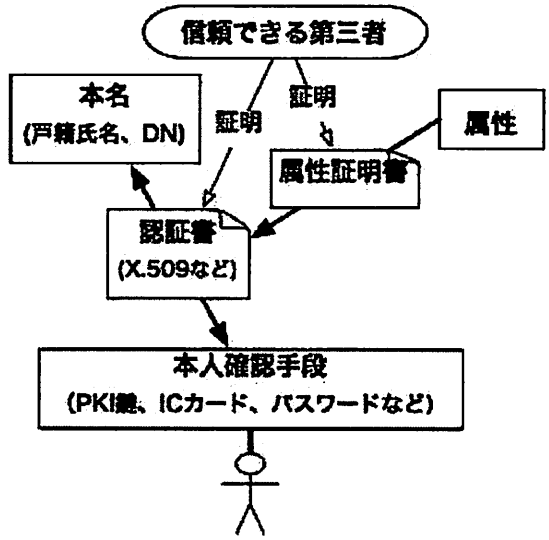


図 3 通常の認証書と属性証明書

したがって、仮名認証書は、X.509 などの通常の認証書と同様の構造で仮名と暗号鍵などの本人確認手段とを信頼できる第三者の署名によって結合させたものである。しかし、仮名ごとにポリシがことなるため、仮名認証書に対する属性証明書は当該仮名に限定された属性のみに定義可能となる。

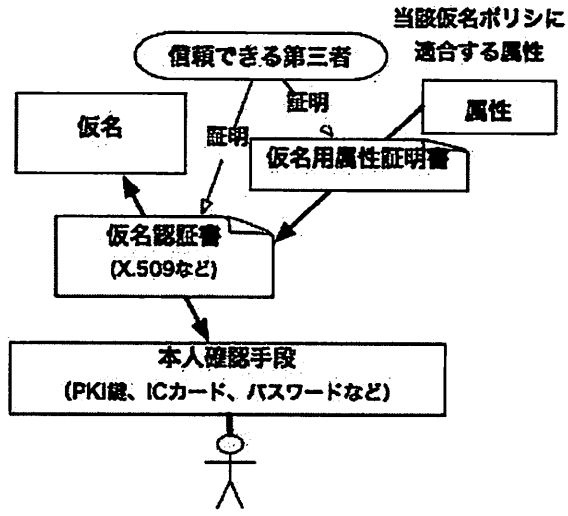


図 4　仮名認証書と仮名のための属性証明書

4.1.3. SAML の基本モデルと仮名認証

SAML は、web サービスにおけるシングルサインオンを実現するための認証と認可のフレームワークである。

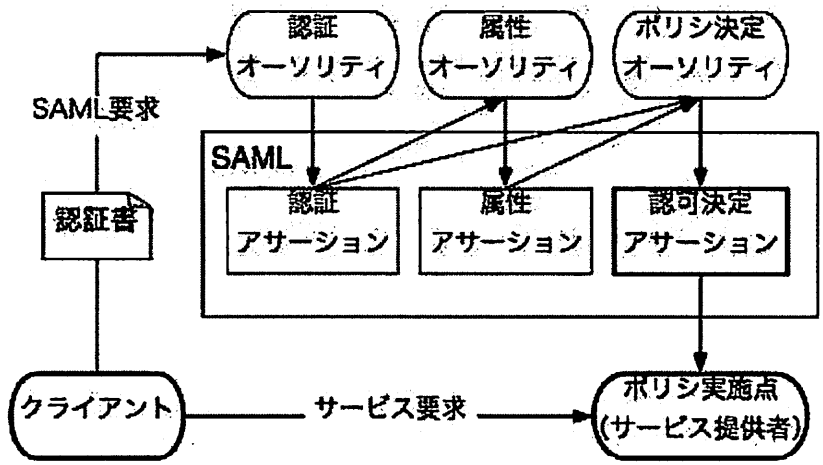


図 5　SAML モデルの認証と認可

SAML の基本モデルに基づいてサービスを要求する主体は、自分の認証書を SAML オーソリティに提示する。そしてその結果発行される SAML アサーションをサービス提供者が受け取ることで認可の判断が行われる。我々は、この SAML のモデルにおいてサービス提供者が必要とするものが認可決定アサーションのみであり、認証書や属性証明書などの個人情報に関わるものを要求しないことに注目した。

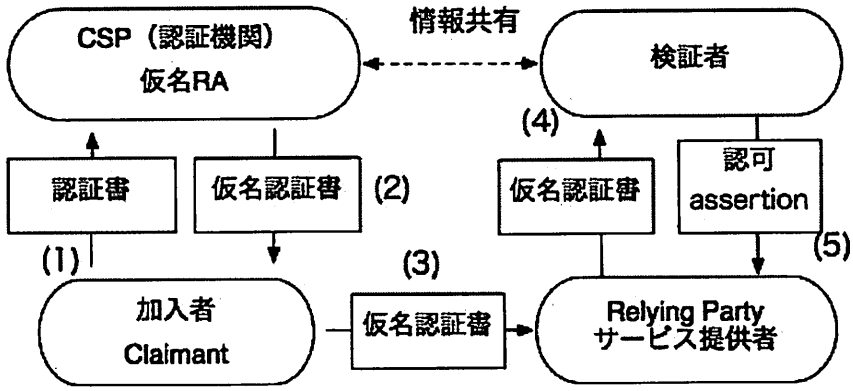


図 6 NIST SP 800-63 に基づく仮名認証

NIST SP 800 -63 は、ID 連携などを含む次世代認証基盤の抽象モデルとして認知されている。このモデルにおいて、実名の認証書を元に仮名認証書を発行する CSP サービスを仮定すると、これに基づいた認可のモデルを上記の SAML アサーションなどを参照モデルとして考えることができる。

4.1.4. アイデンティティシェルタ

アイデンティティシェルタは、我々が提案している仮名による個人の実名の保護と個人情報の統合管理を目的とした Agent システムである。

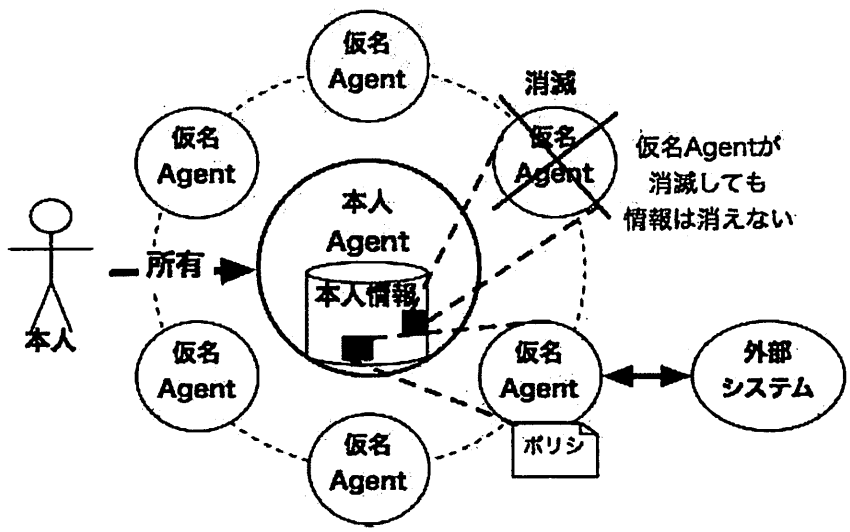


図 7 アイデンティティシェルタ

アイデンティティシェルタは、本人 Agent と複数の仮名 Agent 群から構成される。

(1) 本人 Agent

本人 Agent は、本人の属性、人間関係、記憶、行動履歴などのすべての本人情報を保存するシステムであり、本人のみがアクセスできる。

(2) 仮名 Agent

仮名 Agent は、本人の社会的立場、人間関係、行使権限などを代表するインタフェイスである。仮名 Agent は一定のポリシに基づいて生成され、このとき本人情報の一部を継承する。

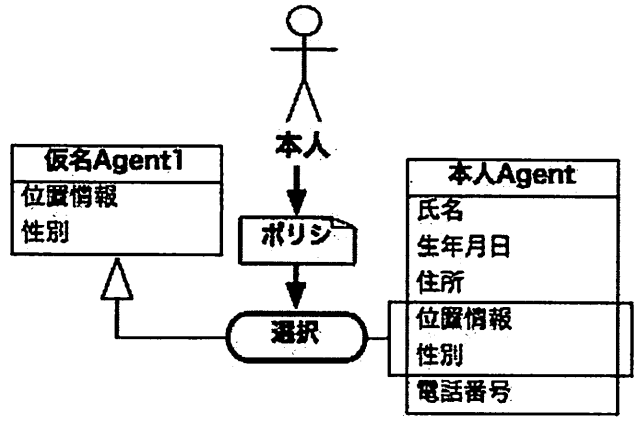


図 8 仮名エージェントの生成

仮名 Agent を介して外部システムとのコミュニケーションが実施される。仮名 Agent が消滅してもそれを介して蓄積された本人情報は消滅しない。

4.2. 地域交通支援システムへのアイデンティティシュエルタの適用

地方の人口減少と高齢化の進行による乗客減のためにバス路線が次々に廃止され地域住民の生活に深刻な影響を与えている。特に高齢者の徒歩移動可能範囲は 1 km 以内といわれており、バス路線の廃止は高齢者にとってより深刻な問題になっている。この問題に対して、福祉バスやコミュニティバスなども試みられているが、将来的に税収が増加する見込みのない現状で公的資金に頼った運営は限界が見えており実際に多くの試みが失敗している。

4.2.1. 地域の交通資源を有効活用する情報システム

しかしながら地域にはまだ工夫次第で利用可能になる交通資源が存在する。また、利用者の位置情報や行動情報を情報化し地域交通システムと有機的な連携を実現すればこういった地域の交通資源の活用効率は飛躍的に向上することが予想される。我々は、このようなことから地域のあらゆる交通資源と利用者を情報化によって結びつけ連携させることを目的とした徹底的に低コストの地域交通支援システムの構築を進めている。

4.2.2. ロケーションプライバシの問題

個人の現在の位置情報や行動予測情報を共有するシステムは、同時に個人の行動を監視し記録するものであり、監視社会の入り口となる危険性を含んでいる。このようなシステムがたとえ社会システムとして合理的であっても市民に受け入れられないこ

とがあることは住民基本台帳カードの例からも学ぶことができる。

また、現在の携帯電話を利用したナビゲーションシステムの多くで実施されているように、利用開示時に規約としてプライバシに関わる権利の放棄に合意したときのみサービスを受けることができるという選択式のプライバシの考え方も、地域交通のような交通弱者には生活に必須となるシステムへ適用することは適切ではなく、プライバシは常に確実に保護されるべきである。

4.2.3. 提案する地域交通支援システムの概要

提案する地域交通支援システムには、地域交通事業者向けのサービスと地域交通の利用者向けのサービスがある。

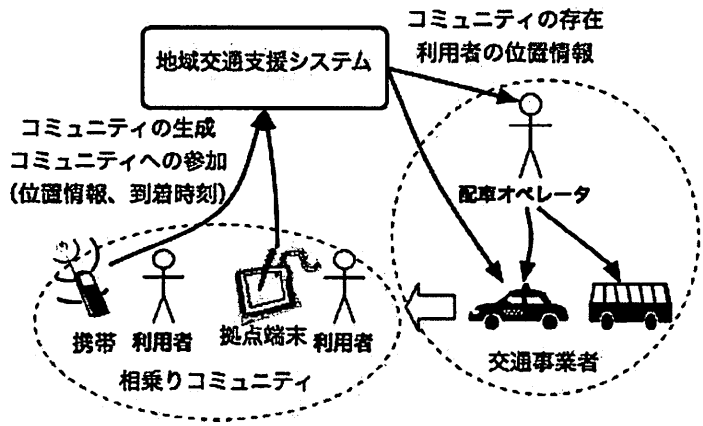


図 9　地域交通システムの概要

4.2.4. 交通事業者向けサービス

地域交通事業者向けのサービスとして、地域交通の配車オペレータや運転者が利用者の目的地と地理的な現在位置および到着希望時刻を知るためのシステムを提案した。

4.2.5. 利用者向けサービス

利用者向けのサービスとしては、地域交通の相乗り率を高めることを目的とした「あいのりコミュニティシステム」を提案した。これは同じ目的地に同じくらいの時刻に到着することを希望する人々がお互いの存在を知り仲間になることで相乗りをするコミュニティをリアルタイムで作るシステムである。

(1) 拠点端末

本研究の前提条件として、地域住民の生活拠点である病院の受付、薬局、郵便局、銀行、学校などに住民が利用可能な端末を設置するものとする。

(2) GPS 機能付き携帯電話

本研究の前提条件として、GPS による位置情報を通知する機能を備えた携帯電話からも「あいのりコミュニティシステム」を利用できるものとする。

4.2.6. 地域交通事業者支援システム

地域交通事業者支援システムは、地域交通のオペレータや運転者が利用するものである。

図 10　交通事業者向けシステムの画面

このシステムは次のような機能を持つ。

(1) あいのりコミュニティの一覧

ここには現在アクティブなコミュニティの一覧が表示される。

コミュニティ名は、目的地→移動目的、到着希望時間となっており、一目でそのコミュニティの目的地がわかるようになっている。

また、フォントの大きさは現在のコミュニティ参加者数を表す。

さらに、コミュニティに車いすを必要とするメンバーが存在することや同乗者を女性に限定するなどの条件がある場合にはコミュニティ名に記号が付加されて表示される。

(2) 地域交通車両の現在位置

地域交通車両の地理的な現在位置が表示される。

(3) コミュニティ参加者の地理的な現在位置:

コミュニティごとに現時点での地理的な位置が表示され、配車のコントロールに利用される。

4.2.7. あいのりコミュニティシステム

利用者が地域交通を利用するために使用するシステムであり、あいのりコミュニティに参加するためのものである。

(1) あいのりコミュニティの一覧

利用者の行き先や到着希望時刻が既存のコミュニティにマッチした場合、そのコミュニティ名を選択することで自分も参加することができる。

参加すると、交通事業者に利用者の現在位置がコミュニティメンバとして通知される。

(2) 新規のあいのりコミュニティの作成

既存のあいのりコミュニティと行き先や希望時刻が一致しなかった場合、自分で新しいコミュニティを作ることができる。このとき、目的地、移動目的、到着希望時刻、同乗者の制限などを指定することができる。

(3) 同乗者への条件の指定

デマンド交通は降車の場所から自宅の場所が同乗者にわかるという問題がある。

特に女性が帰宅する場合などに同乗者を女性だけに限定したコミュニティを作れる機能は必要である。

図 11　地域交通利用者支援システム

4.2.8. 利用者によるプライバシ設定

利用者は本人認証を行ったうえで自分のプライバシ要件を設定することができる。また、コミュニティに参加しようとしたときに、そのコミュニティのポリシと設定済みの自分のプライバシポリシとがミスマッチのときにも再度設定が促される。

図 12 利用者によるプライバシ設定

(1) 個人情報の開示ポリシ

情報開示する対象、開示する情報とその範囲などを指定できる。

(2) アクセス記録請求

自分の個人情報に誰がいつアクセスしたかという記録を請求することができる。

(3) 仮名の自動更新の設定

地域交通を利用するための仮名を更新する条件として、一定時間ごとと一定距離の移動ごとに自動的に仮名を更新する指定ができる。コミュニティに参加しているときに仮名を更新する場合、一度予約をキャンセルした後に別人格として再度参加することになる。

4.2.9. ロケーションプライバシの関連研究

ロケーションプライバシの目的は、意図しない第三者に自分の位置情報が知られてしまうことを防止することである。ロケーションプライバシの研究としては、ロケーションプライバシアーキテクチャに関する研究と位置情報や行動履歴の匿名化の手法に関する研究がある。前者としては、IETP GeoPriv WG における成果や M. Langheinrich のユビキタスシステムプライバシの6原則の研究を挙げることができる。

後者の研究としては、中西らによる人口密度に応じた位置情報粒度の変更による匿名性の保持の研究や貴戸らによる移動軌跡の追跡可能性の評価指標とダミー情報の挿

入による匿名性の研究などを挙げることができる。

4.2.10. IETF の Geopriv

IETF の Geopriv WG は、位置情報を扱うサービスの一般的アーキテクチャ標準を RFC3693 などで提案しようとしている。

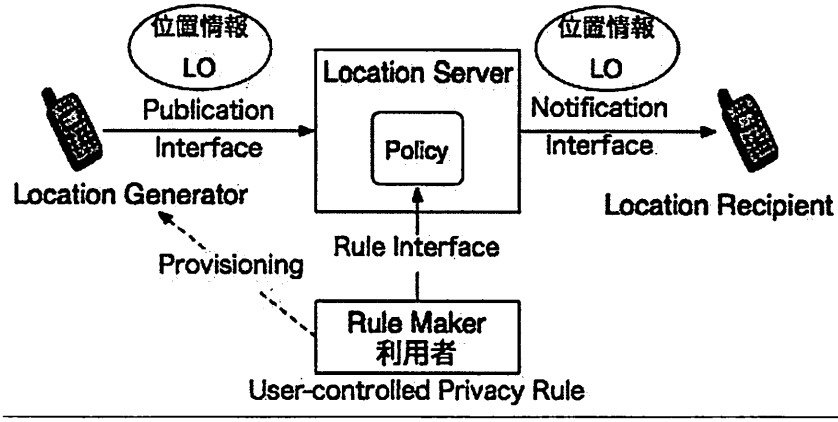


図 13 IETF Geopriv モデル

Geopriv WG のアーキテクチャは、ルールに基づいた LO (Location Object) の流通に関するセキュリティを定義している。LG (Location Generator)で発生した LO が LS(Location Server) を経由して最終的に LR (Location Recipient) に到達するという基本モデルに基づいている。

Geopriv には多くの原則があるが、特に利用者中心のルール作成と運用や合理的理由が無い限り LO とアイデンティティはリンクされるべきでないとしている。

4.2.11. Mark Langheinrich のユビキタスプライバシの 6 原則

Mark Langheinrich は、ユビキタスプライバシの 6 原則として、通知の原則、同意の原則、匿名と仮名の原則、局所化の原則、セキュリティの原則、請求権の原則を挙げている。

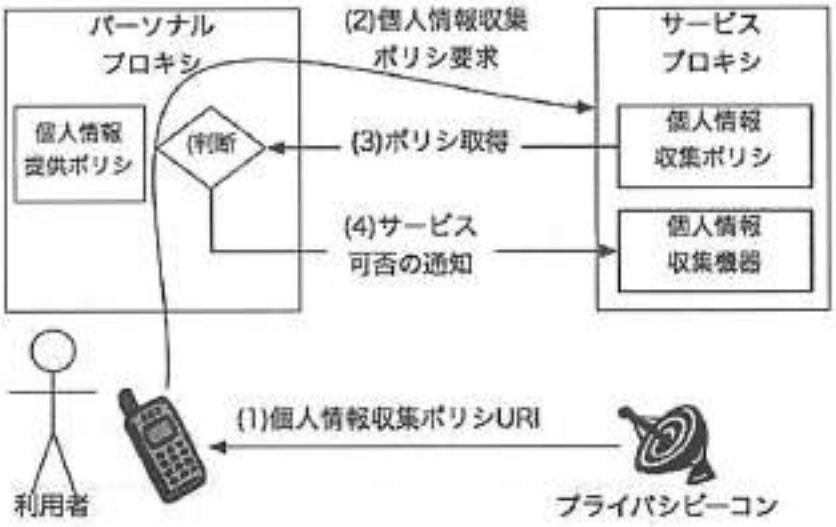


図 14 PawS の基本モデル

また、この原則にそったシステムである PawS の提案を行っている。

4.2.12. プレースエージェントモデル

プレースエージェントモデルは、Agent 間で情報の共有と流通を行うためのフレームワークである。

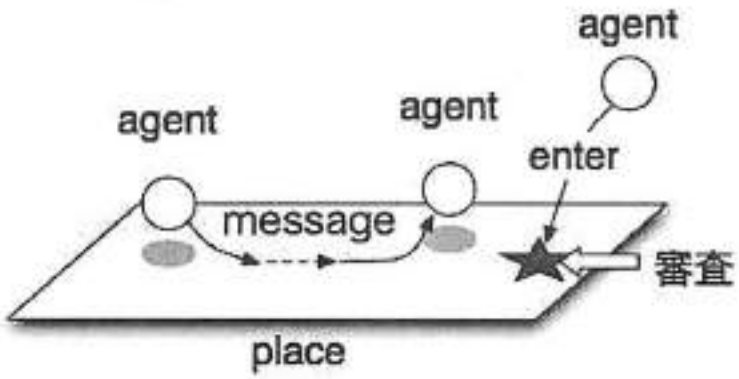


図 15 プレースエージェントモデル

プレースとは、Agent どうしがコミュニケーションを行う場である。プレースには、Agent がプレースに入る (enter)ときにプレースによる資格審査を受けるというセキュリティモデルを設定することができる。また、Agent は直接的にプレース内の他の Agent とコミュニケーションを行うのではなく、プレースに対してメッセージを送りそれを他の Agent が受け取るというモデルを利用することで、Agent 郡の動作の同期や協調動作を制御することができる。

4.2.13. プレースエージェントモデルによる地域交通支援システムの構成

我々は、プレースエージェントモデルを利用して、地域交通支援システムを構成した。

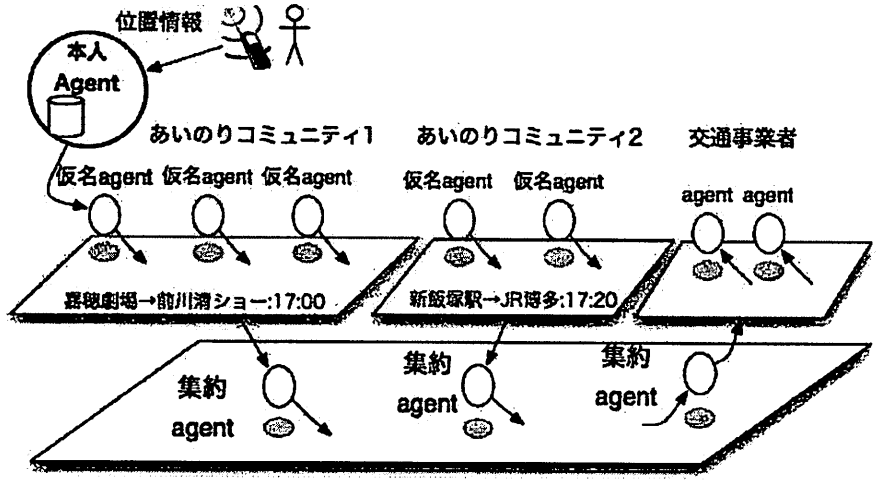


図 16 プレースエージェントモデルによる地域交通支援システムの構成

情報を共有する Agent の範囲をひとつのプレースとすることで、個人情報の開示範囲を明確に定義できるからである。このため、それぞれのあいのりコミュニティ、交通事業者のコミュニティを一つのプレースとした。また、これらのプレースの情報を集約し相互に連絡するために集約 Agent という中継用 Agent とそれらが相互にコミュニケーションを行う集約プレースからなる２階層プレースの構造を考えた。

4.2.14. 評価

提案した地域交通のためのプライバシフレームワークを Geopriv(RFC3603)のロケーションプライバシモデルとの整合性の観点と、Langheinrich のユビキタスプライバシの６原則との整合性の観点から評価を行う。

(1) 地域交通支援システムの GeoPriv モデルによる位置情報の流通

GeoPriv のモデルは、次のような対応によって我々の提案モデルに対応づけることができる。

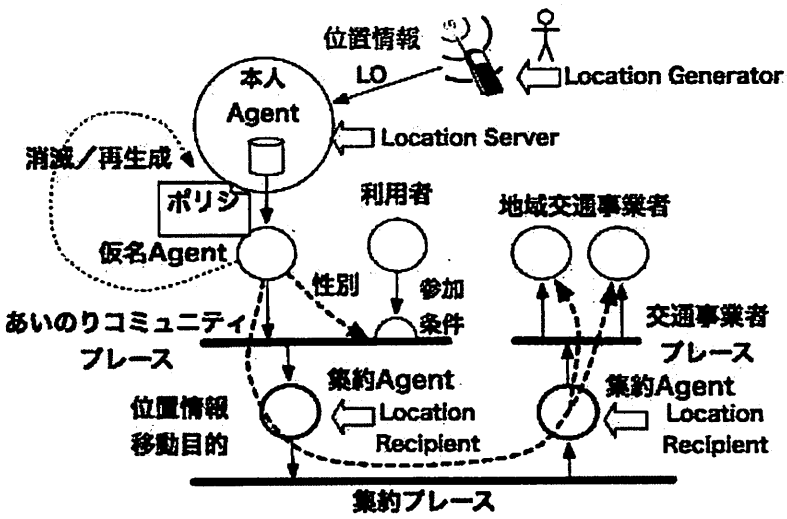


図 17　地域交通支援システムの GeoPriv モデルによる位置情報の流通

(2) Langheinrich のユビキタスプライバシの６原則との整合性

提案したフレームワークはユビキタスプライバシの６原則と次のように整合する。

・通知の原則：

プレースに入るときに、プレースのポリシ（性別情報の開示など）を通知し仮名 Agent が合意したときのみコミュニティに参加する。

・同意の原則：

プライバシ設定画面で明示的な選択を実施する。

・匿名と仮名の原則：

仮名 Agent の時間経過で再生成する。

・局所化の原則：

利用者が実際に地域交通車両に乗車すると仮名 Agent を消去する。

仮名 Agent を移動距離で再生成する。

・セキュリティの原則：

集約 Agent と集約プレースは信頼できる組織が安全に管理する。

・請求権の原則：

集約 Agent はプレースが消滅するまでアクセス履歴を管理し請求に応える。

以上のように、すべての原則を自然に充足できることがわかった。

5. まとめ

本報告書では、ファインダビリティとディペンダビリティの観点から近年の社会情報基盤のトレンドを分析し、社会情報基盤の今後の在り方について提言を行った。そ

してこの視点に基づく Web プライバシの問題に対する一つの解決案としてアイデンティティシェルタモデルを提案しさらに地域交通におけるロケーションプライバシの問題に適用することを試みた。

文　献

[1] Marit Hansen, Henry Krasemann: Privacy and Identity Management for Europe, PRIME White Paper, http://www.prime-project.eu.org/, July 2005.

[2] OASIS: Security Assertion Markup Language V2.0, http://www.aosis-open.org/communities/¥#documents, as of 9/1/2005.

[3] William E. Burr,Donna F. Dodson ,W. Timothy Polk: NIST SP800-63. Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, June 2004.

[4] D. Mulligan J. Cuellar, J. Morris. Request for comments: 3693 GeoPriv requirements. http://www.ietf.org/rfc/rfc3693.txt.

[5] JMarc Langheinrich. Privacy by design ? principles of privacy-aware ubiquitous systems. In G.D. Abowd, B. Brumitt, and S. Shafer, editors, Ubicomp 2001 Proceedings, Vol. 2201 of Lecture Notes in Computer Science, pp. 273?291. Springer, 2001.

[6] Marc Langheinrich. A privacy awareness system for ubiquity- tous computing environments. In Ubicomp 2002 Proceedings, Vol. 2498 of Lecture Notes in Computer Science, pp. 237?245. Springer-Verlag, 2002.

[7] Roy Fielding, Architectural Styles and the Design of Network-based Software Architectures0, http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

[8] Roy Fielding: Architectural Styles and the Design of Network-based Software http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm.

情報社会におけるプライバシーの位相と Sara Baase の視角

永松利文

1. はじめに

Sara Baase は、情報通信技術の有用性が脚光をあびるなかで、人間社会とのかかわりの中で生じる負の関係について哲学、社会、経済など社会科学（Social Sciences）からの視角を多用し、分析を行っている[1]。

本稿においては、情報社会におけるプライバシー（Privacy）に焦点を当てる。情報通信技術の発展によって情報、とくに個人情報の電子化によりプライバシーの危機が高まっている。本稿は、プライバシーの源流を辿りながら、現代社会における文化、政治、経済、自然等々の諸領域に普遍化しつつある情報通信技術によってそれがどのような影響を受けているかについて Sara Baase の理論を基軸としながら検証を行なう。

まず、プライバシーの概念を探る。プライバシーは、人間としての「個」の尊重であり人権として個の人間に属する権利ともいえる。

> 人間は、他の人々と共存し生活しなければならない。そのなかで人間は、要望、思考、欲、希望、充足について公の審判を受け、尊厳を失っている。人間は、大衆に埋没している・・・。そのような存在は、人とはいえない[2]。

Edward J.Bloustein は、プライバシーを人間の尊厳（human dignity）と規定し、最大級の賛辞を与え、プライバシーの保証は、人間の存在意義とほぼ同等の価値であるという。そのため、プライバシーの喪失した人間社会を否定するのである。この考え方は今日におけるプライバシー概念の根底をなすものである。

しかしながら、一方で過度のプライバシー尊重を疑問視する捉え方も存在する。たとえば、プリペイド式携帯電話の匿名性は犯罪を助長することを追い風にその加入時に ID の提示が法制度として義務付けられている。

ID がプライバシーであることは疑う余地はない。同サービスの加入を希望する善良なる市民は、個人情報というプライバシーをその取次店及びキャリアー（この場合、携帯電話事業者）に対して、その効用との「トレード・オフのギフト」として献上しなければならないのである。

---

[1] Sara Baase, *A Gift of Fire: Social, Legal, and Ethical Issues in Computing*, First Edition, Pearson Education, Inc., 1997.

[2] Edward J.Bloustein, "Privacy as an Aspect of Human Dignity," in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology,* Cambridge University Press, 1984, pp.156-203, quote on p.188.

ビジネス上のトレード・オフは、事務手数料やプリペイドカードを購入することで成立している。そのためこの取引行為のなかで価値を有する個人情報を無償で提供することは、紛れもなく顧客からの「プライバシーのギフト」の献上である。

善良なる市民がギフトとして提供したプライバシーが意図的又はアクシデント的に流出し、(市民が) 被害を蒙る事件・事故は多発している。このような場合、事業者は一応責任の一端を認めるが、利用者によるプライバシーとしての個人情報の献上の正当性を否定しない。

事業者はそのような場合管理方法を見直すであるとか、取り扱う社員の教育の徹底など、方法論に終始するのみである。おそらく彼らは危機管理マニュアル等の指示に従っているだけなのであろう。犯罪的行為などの負の側面のリスクが減退することの代償として、大多数の善良な市民のプライバシーが危機に晒されるリスクが増大することを容認していいのであろうか。

もっともわれわれ及び事業者は法治社会に生きているため、それが法制度としての義務であれば、従うしかないという現実がある。もはや、プライバシーは社会システムの中に組み込まれている。

本稿では Sara Baase 他の理論を参照しながら、プライバシーの本質及び理念と情報通信技術革新にみる現実的諸相との矛盾や問題点など示唆し、情報社会におけるパラドックスの一面を明らかにする。

2.プライバシーと「権利」認識に関する諸説

プライバシーが権利であるかについての論争は、19 世紀末に Samuel Warren and Louis Brandeis によって起こった[3]。それまで、プライバシーという概念は存在していたが、プライバシーは独立した権利として認識されていなかった。

Samuel Warren and Louis Brandeis の主張の骨子は、イエロージャーナリズムの台頭に関係している。イエロージャーナリズムと知る権利の拡大によって大衆の関心は、文化や政治経済以上に社会及び私生活に向けられた。それは、Warren and Brandeis の個人的体験として、つぎのように記されている。

> ・・・was gossip columnists writing about extravagant parties in Warren's home and particularly newspaper coverage of his daughter's wedding. The background of the article is described in a biography of Brandeis and summarized in the critical response to the Warren and Brandeis article by William L.Prosser[4].

---

[3] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, 1890, v.4, p.193.

[4] Ferdinand David Schoeman, "Privacy," in Schoeman, *Philosophical Dimensions of Privacy: An Anthology*, pp.104-55.

（Warren の家での豪奢なパーティーに関してのゴシップ・コラムニストの記述や彼の娘の結婚式をある新聞が掲載した。この背景は、Brandeis の伝記に記されており、William L.Prosser による Warren と Brandeis の著作への批判的反応としてまとめられた）

Warren and Louis Brandeis のプライバシー権とは、純粋に個人のパーソナリティーの侵害とその保護を求めるもので、肖像権等のような財産権に基づくものではないと捉えられている。この点は、情報社会におけるプライバシーと著作権の関係にも通じるものがあるが、本稿ではプライバシーに限定した議論を行なうので、ここまでは踏み込まない。ただし、この問題は情報社会における法制度や倫理上重要な課題であるので、別の機会で詳しく論じたい。

Warren and Louis Brandeis はプライバシーをあくまでも、個人に内在する権利だと捉え、プライバシーは、人間の心情に根ざすものであり、したがってそれを侵すことは経済的なダメージを与えるものではないと考える。また Warren and Louis Brandeis によると、プライバシーの侵害は、個人の名誉の侵害（名誉毀損）とも区分される。

個人の名誉が毀損されることは、社会やその個人を構成要員とするコミュニティーの存在を前提としている。つまり、名誉毀損とは個人の社会的地位や社会的評価という、いわば個人的属性が侵害されるものであるから、プライバシーの侵害とは異なるというのである。

Warren and Louis Brandeis は、プライバシーを個人に内在する権利として主張するが、これと相反する捉え方もある。それは、Judith J. Thomson の主張である。管見によると Thomson は、プライバシーを「単独の権利」と捉えていない。Thomson は、「本」の例を挙げ、プライバシーと財産権について以下のように捉えている。

Thomson は、ある人(A)が雑誌を購入した場合、当然その雑誌を読むことによって得られる情報を含む効用は購入した A に帰属すると考える（著作権はこれと区分されることはいうまでもない）。この場合、第三者が A の所有する雑誌を閲覧する場合、原則として A の許諾を得なければならない。しかし、許諾を得ずに第三者が A の所有する雑誌を閲覧する場合、その行為は A の財産権を侵害することになるが、必ずしもプライバシー権侵害に該当しないという。

Thomson によると、この場合プライバシー権侵害に該当するケースは、雑誌の「情報の内容」に依拠するという。すなわち、A の所有する雑誌が “Newsweek”である場合、第三者の無許諾閲覧は A の財産権を侵害するが、プライバシーを侵害することはないであろう。しかし、A の所有する雑誌が”Playboy”である場合、第三者による無許諾閲覧は、財産権の侵害にプラスしてプライバシーの侵害を起こす可能性が高いという。

Thomson はその主張の正当性のために、この他「身体を支配する権利」「暴力を受けない権利」等々示唆に満ちたケースを援用しており興味深いのだが、紙面の都合上紹介でき

ないので他の機会において述べる。

Thomsonのプライバシー権の特徴は、それが単独で機能しない点である。Thomsonは、プライバシーに含まれる各々の権利は、独立している権利であったり、また他の権利に含まれると述べている。この主張にもとづきThomsonは、プライバシー権の侵害の事実確認技術（heuristic device）は、その行為がプライバシーを侵害したかどうかを追及するのではなく、他の権利が侵害されたかどうかを追及すべきであると述べている[5]。

3.プライバシーとしての情報の価値

情報は価値を有する。これは、情報が経済的価値をともなうという現代的現象のみならず、個人が当該情報を秘匿したい場合のように個人の価値観にもとづく場合もある[6]。Richard Posnerは、このように述べ、財産権及び所有権の視点から情報の価値を分析している。Posnerの論文を要約すると、彼は情報の公共性を主張している。

しかしながら、矛盾するように映るが、以下のように情報は私的財産権及び所有権を包含する場合も認めなければ、真の情報の公共性は保たれないという。たとえば、当該情報の生産にコストを要する場合、またその獲得にあたってコストが伴う場合である（この場合、コストとは創造的な情報を生産したり、獲得するためのコストであるので、情報技術の発展により限界費用がゼロになるような情報はPosnerの概念に含まれないとすべきである）。

このような場合、当該情報に対する私的財産権及び所有権が否定されれば、それに対する経済的支出を行なったものは利益を得る事ができない。社会にとっては、むしろ創造的かつ経済的価値を伴うこのような情報こそ貴重で重要である。しかしながら、その私的財産権や所有権が認められないとすると、このような情報は稀少となり、結果的にそれは社会的損失となるという[7]。これらは、主に資本主義経済下における企業の法人としての経済活動に資する見識であろう。

一方、個人に関してはどうであろうか。Posnerは個人に関する情報については私的財産権及び所有権の存在を認めている。個人に関する情報は、当該個人が創造あるいは入手する場合、限界費用はほぼゼロに等しい。個人に関する情報をプライバシーとして保護すべきことが社会の賛同を得るような場合、当該個人情報に公共性を与える必要はないし、また公共性から隔絶する手段を講じるための社会的コストも実質的に発生しない。Posnerによるとこのような個人に関する情報は、私的財産権及び所有権を有するのである。

Posnerが財産権としてのプライバシー領域に挙げる事項は以下の通りである。

---

[5] Judith J. Thomson, "The Right to Privacy," in Schoeman, *Philosophical Dimensions of Privacy: An Anthology,* pp.272-89.
[6] Richard Posner, "An Economic Theory of Privacy," in Schoeman, *Philosophical Dimensions of Privacy: An Anthology,* pp.333-345.
[7] *Ibid*,Posner.

○会話やコミュニションは保護を要する（通信の秘密等として具現化）
○信用に関する個人情報に財産権は認められない（犯罪歴など）

Posnerは、英米の法制度の理念である"common law"を源流としているといわれているが、現実の法制度は米国でもこの理念と相反している部分も多いので、Posnerのプライバシーと財産権に対する批判は多い。

4. 情報通信技術革新とプライバシー

これまで、プライバシーの財産権及び所有権との関わりについて先行研究のレビューを中心に述べた。また、既に述べたようにプライバシーとは、必ずしも情報通信技術の利用に特定される概念ではない。

日常生活のなかで、プライバシーはいたるところで「危機」にさらされている。集合住宅における無施錠の郵便受け、毎○曜日に出すゴミ袋、街中で我々を撮る監視カメラ等々である。しかしながら、情報通信技術の普及は、プライバシー侵害の危険性を増幅した。インターネットとコンピュータの融合は多くの種類の個人に関する情報を瞬時に集積し、また短時間でそれは分析され、蓄積される。さらに、その再利用や第三者への流通も容易に可能である。

情報通信技術が今日のように普及する以前においても、個人に関する情報の蓄積は確かに存在したが、それらへアクセスするには膨大な作業が必要であり、容易ではなかったので、個人情報管理に関する危機管理意識は低かった。Harris Pollの調査によると、プライバシーに危機を感じている層は、1978年には64%であったが、1994年には82%となっている。

そのため、各種データベースのような電子情報集積が普及するまで、個人の犯罪歴、一般的な履歴、健康に関するプライバシーが、一般的に流通する範囲は限定されてきたといっていい。すなわち、それらプライバシーに関する情報が流通するのは人口に膾炙するコミュニティーに限られていたが、情報通信技術によってその流通する空間が無限に拡大するに至ったのである。

このような状況のなかで、Posnerの主張するようにプライバシーとくに当該個人に関する情報の財産権及び所有権の存在に対する侵害の危険性が高まってきているとみることができよう。

5.個人情報をコントロールできるのは誰か

本項では、プライバシーのなかの個人に関する情報に言及する。

個人情報のコントロール権は、少なくとも禁治産者等でなく一定の条件を満たしていれば、当該個人に帰属するし、またそれは基本的な権利でもある。しかしながら古今東西、自分自身の情報を当該個人だけがコントロールできた試しはない。例えば、情報通信技術の普

及する以前のコミュニティーにおいても個人のプライバシー（個人に関する情報）の流出は様々なかたちで発生している。たとえば当該個人のプライバシーに関する噂を第三者が広める行為について、その第三者は当該個人の許諾を得ることはない。

情報通信技術の普及以前において、人間はより小さなコミュニティーで活動していたとするならば、むしろ個人に関する情報を含むプライバシーを相互に共有することによって社会活動及び経済活動は成立していたともいえるのである。すなわち、AとBが商取引を行なう場合、そのコミュニティーが小規模であれば、相互の個人情報（信用情報など）は互いに知っているかもしれないし、或いは知らなくとも善意の第三者を通じて入手することができるからである。

一方、情報通信技術が普及すると商取引に及ぶ場合、その取引はサイバー空間上で行われるので、もはや前述のような牧歌的商取引は望むすべもない。このような状況における取引には開始当初から個人情報を含むプライバシーに関する信用情報はないので、一般的に商取引を行なう場合、それを入手しなければならない。

もし、A（購入側）、B（販売側）で相互に面識がない場合、この商取引には相互にリスクがともなう。簡単な理解のために、Bを善意の販売者とする場合、Bはリスク・ヘッジのためAに対してプライバシーの放棄を要求する。

しかし、もしAがこの要求をプライバシーの侵害として拒絶した場合、この商取引は成立しない。冒頭で述べたように、プリペイド式携帯電話の購入者は、善意の携帯電話会社からのプライバシー放棄の要求を受諾しなければ、プロペイド式携帯電話の効用を得ることができない状況と同様である。

情報社会に生きるわれわれは、ほとんど全ての社会生活上の便益とプライバシーをトレード・オフしながら生活している。情報通信技術がもたらしてくれる最高に快適な生活様式は、プライバシーをコントロールする当該個人の権利を自ら放棄させるほど甘美なものなのである。この放棄する行為は強制されたものではなく、当該個人のボランティア的行為（たとえ法制度の定めがあっても）なので、これはプライバシー侵害にあたらないように、よく仕組まれた社会システムである。

6.まとめ

情報社会の便益は人間を幸福にしたかどうかは、多様な角度からの議論が必要であろう。しかしながら、人間の有する基本的な権利や自由について概念的に考察すると多くの矛盾が発生しているのではないか。情報通信技術の発達は人々をして、とくに革新的な人々の先導により、その技術的恩恵からもたらされる便益を優先させた。

人間の有する権利の本質を欠く科学技術崇拝は、人間の基本的権利の概念崩壊の矛盾を秘匿させたい公権力に誘導されているのではないかとさえ思う瞬間がある。

単独で存在していれば、安全で有益である小規模な記録システムが自動化、相互に接続され、個人の自由が少しずつ侵害されていくことが真の危機である[8]。

情報通信技術の便益は、個人情報とのトレード・オフに値するとの考え方も根強いのも事実であり、個人の行動履歴や嗜好に応じたサービスの提供を期待している。そのためサービス提供者は、データマイニングにより、顧客の行動履歴などの個人情報を用いることになり、個人情報を含むプライバシー保護に対するスキームの再構築が迫られている。

近年、公的機関、企業や教育機関等の個人情報漏洩が頻繁に起こっている。これが単なる技術上の問題であればその対策は創意工夫により完璧ではないが比較的可能である。しかしながら、事件の多くは人為的な問題である。つまり、現実的に個人情報を保護できる保証はない。たとえ、企業内等において情報管理の徹底や情報モラル教育を徹底しても人間が関与する限り、個人情報等の流出を減少させる可能性はあるが防ぐことはできない。刑罰を強化しても犯罪が無くなることはないのと同様である。

教育機関及び企業等においてはこの人為的問題を防止することを目的に、××リテラシーのような各種研修・教育が行なわれている。とくに教育機関において、これに関する教育は活発化しており、児童、生徒、学生は情報社会におけるモラルと法治国家における市民として遵守すべき行動規範を学ぶ。また、企業等においてもコンプライアンス（法令順守）や法人としての社会責任を果たすため、規定の整備や社員教育に多大な努力を払っている。これらの努力及び人々に対する教育研修は、啓蒙としての価値はあるが、それ以上の効果を期待できないだろうし、期待をしてはいけない。

人々は情報社会の便益は人間の本質的権利を侵害していることを認識する必要しなければならない。データマイニングは消費者にとって有益なサービスだが、プライバシー侵害の「可能性(危険性)」もある点を個人が了承した上で個人の責任の上で利用すべきである。プライバシーの権利を根底から考察すると、この場合、もしプライバシーに関する何らかの権利が侵害された場合、個人の責任に帰すことも追求する必要があるだろう。

プライバシーをトレードの対象としてよりも権利として重視する場合、消費者保護論者の主張と合致する。極端な消費者保護を唱える Mary Gardiner Jones は、情報社会で個人情報（プライバシーの一種とする）が使用される際に、たとえ個人が許諾を与えてもその使用は正当化されないという。

多忙な消費者は、その（個人情報を使用する目的など）目的について、（正確な）理解することを期待できない。その使用法について自分との関わりかたを正しく理解できない[9]。

---

[8] U.S. Privacy Protection Study Commission, 1977.
[9] Dan Freeman, "Prvacy Profile: Mary Gardiner Jones," *Privacy and American Business*, 1:4, 1994, pp.15-17.

Jonesの消費者保護論は、企業ビジネスと個人の対峙的関係を機軸に、企業ビジネスの相対的優位性を前提とする個人に対する保護の主張である。個人情報の企業による様々な利用が、個人にとっての利益になると当該個人が認識しているケースもあるが、これは企業により創りだされた神話であるとJonesは主張している（例えば、学校の同窓会名簿作成時の勧誘等）。

本稿においては、このような消費者保護の立場はとらない。情報通信技術の便益を享受する上で、自身のプライバシーや各種権利の保護や行使を行なうためには、市民の知的な能力の向上が達成されなければならない。

それは単なる情報リテラシーやモラルのような「ノウハウ」を身につける技術ではなく、プライバシーを放棄することへの同意と便益とのトレード・オフを倫理や権利等の文脈から考察するチカラである。

参考文献

Anthes, Gary H., "Consortium Paves Way for 'Data Superhighway," *Computerworld,* vol. 27, no. 39, September 27, 1993.

Baase,Sara, *A Gift of Fire: Social, Legal, and Ethical Issues in Computing, First Edition,* Pearson Education, Inc., 1997.

Cowhey, Peter F. and Aronson, Jonathan David, *When Countries Talk: International Trade in telecommunication Services,* Ballinger, 1988.

Freeman, Dan, "Prvacy Profile: Mary Gardiner Jones," *Privacy and American Business* , 1:4, 1994.

Bloustein, J. Edward, "Privacy as an Aspect of Human Dignity," in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

Kahin, Brian, and Keller, James, *Public Access to the Internet,* The MIT Press, 1995.

Lessig,Lawrence, *Code and Other Laws of Cyberspace,* Basic Books, 1999.

Levinson, Paul, *Digital Mcluhan-a guide to the information millennium,* Routledge, 1999.

Posner, Richard, "An Economic Theory of Privacy," in Schoeman, *Philosophical Dimensions of Privacy: An Anthology,* Cambridge University Press, 1984.

Rushkoff, Douglas, *Cyberia: Life in the Trenches of Hyperspace,* Harper San Francisco, 1994.

Schoeman, David, Ferdinand, "Privacy," in Schoeman, *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

Thomson, J. Judith, "The Right to Privacy," in Schoeman, *Philosophical Dimensions of Privacy: An Anthology,* Cambridge University Press, 1984.

Warren, D. Samuel, and Brandeis, D. Louis, "The Right to Privacy," *Harvard Law Review*,v.4, 1890.

今井賢一『情報ネットワーク社会』岩波書店、1984 年.

内田貢「電子商取引と法(2)」『NBL601』NBL、1996 年.

公文俊平『情報文明論』NTT 出版、1994 年,

野口悠紀夫『情報の経済理論』東洋経済新報社、1974 年.

渡辺昭夫・土屋實男「国際機構」、渡辺昭夫・土屋實男編、『グローバル・ガヴァナンス』東京大学出版会、2001 年.

豊の国 IX のトラフィック動向

吉田和幸[1,2]、石丸忠教[1]

1 ハイパーネットワーク社会研究所
2 大分大学

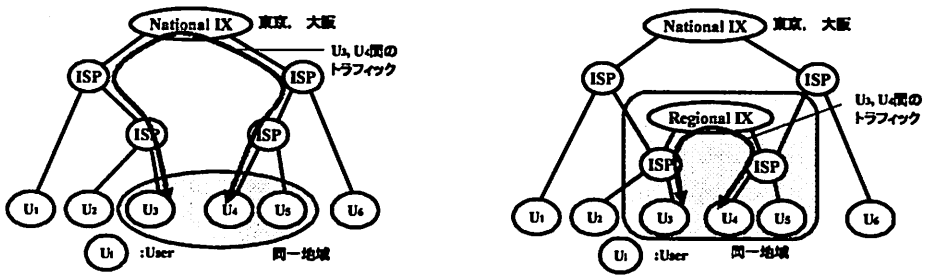
1．はじめに

インターネットはプロバイダやインターネット関連団体のネットワークを相互に接続することで成り立っている。これらはインターネット相互接続点（IX：internet exchange）で繋がっている。現在、国内では東京や大阪にある NSPIXP や JPIX といった National IX を通じて繋がっていることが多い。このため図 1 (a)に示すように、たとえ同一地域内の通信であっても、異なる ISP に加入しているならば東京や大阪経由の通信になってしまう。

このような状況を改善するために、図 1 (b)に示すように地域内のトラフィックをローカルに交換できる地域 IX（Regional IX）の考え方が登場した。

大分における地域 IX として豊の国 IX[1]があり、現在大分大学、地元 ISP である OEC-Net（以下 OEC）、OCT-Net（以下 OCT）、リングサーバ、実験用サーバが接続されている。そして、これらを通して県内の企業、官公庁、大学、研究機関などが接続されている。

本稿では豊の国 IX のトラフィック動向について述べる。



(a)従来のインターネット接続　　(b)地域 IX による地域 ISP の相互接続

図 1．インターネット接続の形態

2．豊の国ＩＸの現在の状況

大分における地域 IX として豊の国 IX が稼動を始めたのが 2003 年 3 月である。2003 年末から 2004 年にかけての実証実験を経て、構築から 3 年、運用に入ってからは 2 年経過している。豊の国 IX の特徴である①ダークファイバの使用、②レイヤ 2 スイッチの使用、③BGP4 によるルーティング、は変わっておらず現在も安定して運用されている。通信を行う具体的な組織としても 2004 年度と大き

[1] 2004 年度研究報告書「大分地域 IX のネットワーク構成とトラフィック分析」「豊の国 IX 研究会の動向と実証実験」を参照のこと

くは変わっていないが、旧大分医科大学は大分大学と統合されたことにより、通信は豊の国 IX を通らず大分大学内に閉じている。また、2006 年 12 月には大分県オープンソースソフトウェア研究会[2]の手により、リングサーバ[3]が構築され、現在豊の国 IX 内で試験運用中である。これら現在の構成を図 2 に示す。

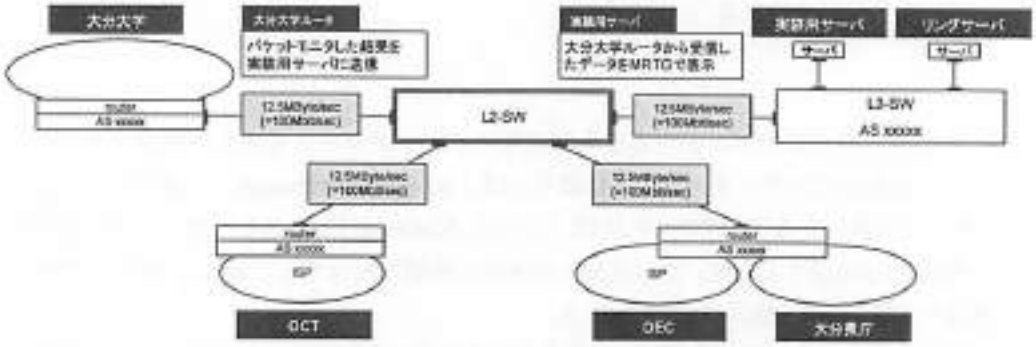


図 2．豊の国 IX の構成イメージ

3．トラフィックの推移

トラフィックの推移は豊の国 IX 内の L2-SW に仕掛けた MRTG[4]によって判断する。団体毎に L2-SW への接続ポートが異なっているため、それぞれの団体が豊の国 IX へどのようにアクセスしているのかが判断できる。なお、本稿では bit/sec ではなく Byte/sec[5]を基本単位として用いている。今後特に断りの無い場合、基本単位として Byte/sec を用いる事に留意頂きたい。

まず、図 3～4 に 2004 年 5 月時点に取得した年間トラフィックを示す。

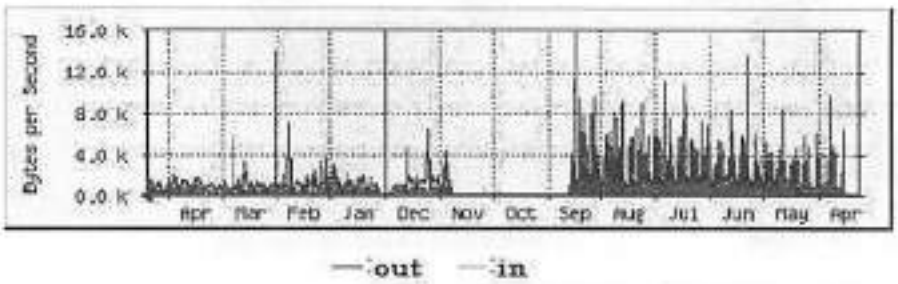


図 3．豊の国 IX ⇔ 大分大学の年間トラフィック（2004 年 5 月時点）

[2] http://www.hyper.or.jp/oita-oss/
[3] HTTP アクセス：http://ring.ix.oita-u.ac.jp/　FTP アクセス：ftp://ring.ix.oita-u.ac.jp/
[4] http://www.mrtg.jp/doc/
[5] 一般的な速度として用いられる bit/sec とするには値を 8 倍にする

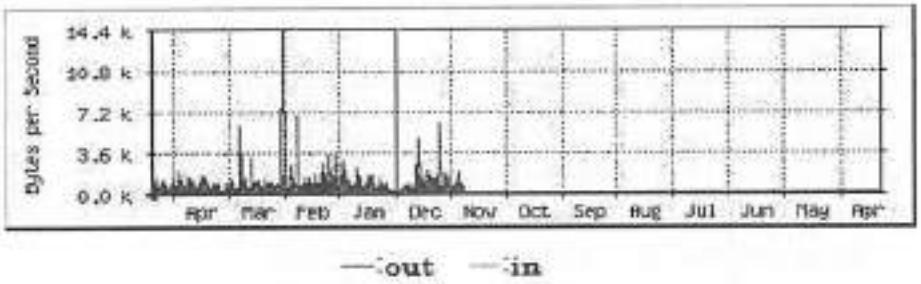


図4．豊の国 IX ⇔ OEC の年間トラフィック（2004 年 5 月時点）

図5～8に 2007 年 4 月時点に取得した年間トラフィックを示す。なお、2004 年 10 月に OCT が、2006 年 12 月にリングサーバがそれぞれ接続されたため、これらのトラフィックも掲載する。

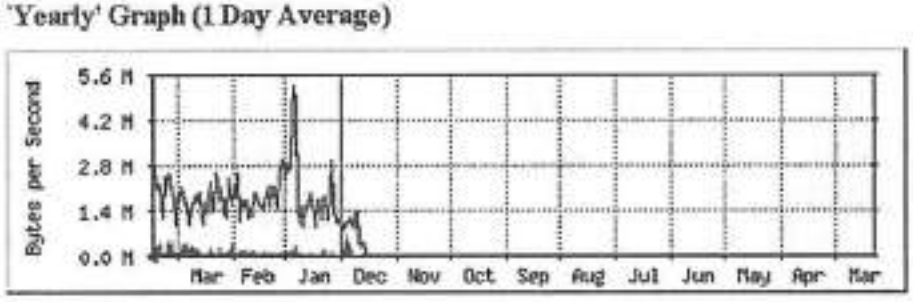


図5．豊の国 IX ⇔ 大分大学の年間トラフィック（2007 年 4 月時点）

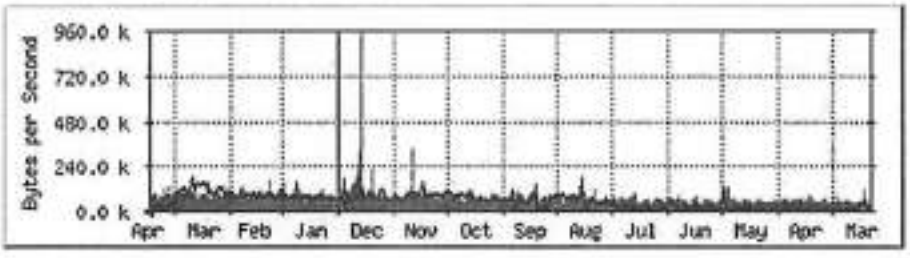
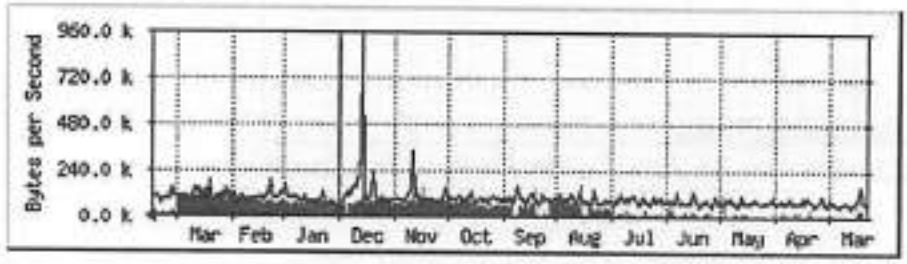


図6．豊の国 IX ⇔ OEC の年間トラフィック（2007 年 4 月時点）

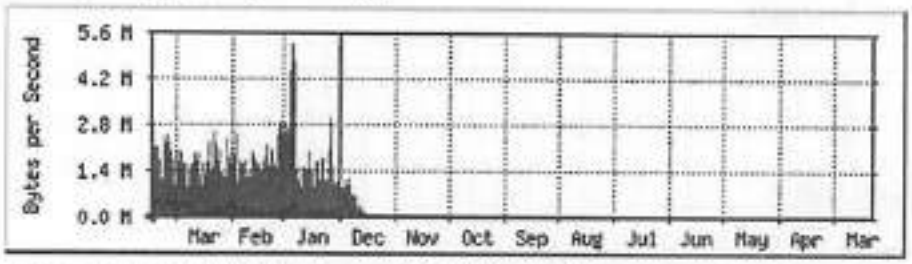
'Yearly' Graph (1 Day Average)



Max oct>iz 180.3kB/s (1.4%) Average oct>iz 55.6kB/s (0.4%) Current oct>iz 22.6kB/s (0.2%)
Max iz>oct 953.8kB/s (7.6%) Average iz>oct 96.0kB/s (0.8%) Current iz>oct 89.3kB/s (0.7%)

図7．豊の国 IX ⇔ OCT の年間トラフィック（2007 年 4 月時点）

'Yearly' Graph (1 Day Average)



Max In: 5298.0kB/s (42.4%) Average In: 1658.6kB/s (13.3%) Current In: 2082.5kB/s (16.7%)
Max Out: 646.5kB/s (5.2%) Average Out: 175.5kB/s (1.4%) Current Out: 220.7kB/s (1.8%)

図8．豊の国 IX ⇔ リングサーバの年間トラフィック（2007 年 4 月時点）

4．トラフィックの分析

新旧のグラフを比較するにあたり、OCT とリングサーバの追加接続を考慮する必要があるが、稼動当初のトラフィック（豊の国 IX ⇔ 大分大学、豊の国 IX ⇔ OEC）は共に 1kByte/sec 程度であり、現在のトラフィック（豊の国 IX ⇔ 大分大学、豊の国 IX ⇔ OEC）と比較すると 100 倍以上の差となっている。これは稼動当初、地域 IX として情報の流通はほとんど無かったということであり、新旧のトラフィックを比較することはあまり意味が無いということになる。

次に現在のグラフ同士を比較すると、面白いことに図5と図8，図6と図7が相似している。図5の大分大学は主な通信相手が他大学であり、遠隔授業などを行っている。この場合、豊の国 IX 経由ではなく豊の国ハイパーネット(大学間接続 VLAN)や SINET を経由して通信することになる。ところが、リングサーバを立ち上げたことで大分大学外から豊の国 IX へのアクセスが急増したと考えられる。なお、図5の大分大学は豊の国 IX 稼動時から継続して計測を行っている。トラフィックが無いように見えるのは前述のリングサーバが 2006 年から稼動することにより、稼動前のトラフィックがグラフの底辺で推移してしまったためだと考えられる。

図6と図7のグラフを比較すると基本的にトラフィックは OEC から OCT に流れている。つまり、OCT 配下のユーザが OEC（配下にあるコンテンツ）からダウンロードしているものと考えられる。OEC も OCT も地域 ISP であるが、OEC のメインユーザは法人や官公庁であり、OCT のメインユーザは一般家庭であると考えられる。このため、普段の利用において両 ISP 間の通信が発生する主な理

由は家庭から企業や官公庁のホームページを閲覧する場合が多いのではないかと考えられる。また、地域 ISP の取り組み[6]として、加入者に対して無償でマカフィー製ウイルスチェックプログラムの提供を行うサービスを実施している。このサーバが OEC 配下で管理されているため、トラフィックに影響を与えていると考えられる。

5．おわりに

豊の国 IX 稼動時に比べるとそのトラフィック量は 100 倍～300 倍以上にも増大している。これらトラフィック増には豊の国 IX を使用したプロジェクトが大きく影響している。リングサーバを設置するプロジェクトしかり、ウイルスチェックプログラムを無償提供するプロジェクトしかりである。前者のプロジェクトは豊の国 IX が存在したから出てきたプロジェクトであるし、後者のプロジェクトは豊の国IXを意識したものではなかったが結果的に豊の国IXが有効に活用されている良い例となっている。

地震が相次いだ今年度は、防災という観点からもネットワーク断を抑制する地域 IX（豊の国 IX）の存在感が高まっていくものと考えられる。今後も豊の国 IX 有効活用のため、より多くの団体・プロジェクトに参加してもらうよう努力していきたい。

[6] 2003 年度研究報告書「日本発!!地域 ISP 会員向けウイルスプログラムの無償提供」を参照のこと

ミレニアム開発目標（MDGs）にみるICTの役割と日本の国際協力

九州大学大学院 比較社会文化研究院 助教
大杉 卓三

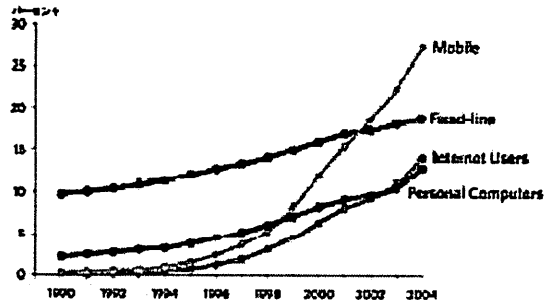
近年ではICTが開発援助における重要な分野として認識されるに至っている。本稿では国際開発目標の重要な枠組みである「ミレニアム開発目標（Millennium Development Goals：MDGs）」へのICTの影響について、ICTは開発援助においてどのように位置づけられ、国際的な取り組みがなされ、またその成果が期待されているのか、さらに日本はどのようにICT分野での貢献の枠組みを構築しているのかについて述べる。ICTの開発援助といった場合、多くの要素を含み分野横断的な内容となる。簡単に分類すると、ICTのインフラ整備、ICT産業育成のようにICT自体を目的とするものから、ICT教育や人材育成、制度整備といったICTを利用する社会環境の整備を目的としたもの、また医療保健や教育、電子政府などのようにICTを他分野に応用することを目的としたもの、と3つに区分される。ICTは開発援助のツールとしては比較的新しいものではあるが、社会や経済を大きく改善する可能性を持つと認識されるに至っている。

ミレニアム開発目標とは、国連が2000年にニューヨークで開催した国連ミレニアムサミットにおいて、参加した189の加盟国の代表が採択した国連ミレニアム宣言にもとづく開発目標である。21世紀の国際社会の目標として、平和と安全、開発と貧困、環境、人権とグッドガバナンス、アフリカの特別なニーズなどを課題として掲げており、国連の21世紀の役割に関する明確な方向性を示している。またミレニアム開発目標は、国連ミレニアム宣言と1990年代に開催された主要な国際会議やサミットで採択された国際開発目標を統合し、一つの共通の枠組みとしてまとめられたものである。アフリカ諸国の状況に適合させていることから、アジアなどの途上国の優先項目と必ずしも合致しない部分もあり、そのまま適用するよりも各国の状況にあわせた対応が必要であることは否めないが、各国の大事な指標のひとつとなっていることは間違いない。また、国際機関や二国間援助、NGOなどがパートナーシップを取り組んでいる課題としても重要な位置づけとなっている。

次に開発におけるICTによる開発援助をとりまく近年の状況を概観する。2000年に九州・沖縄サミットにて「グローバルな情報社会に関する沖縄憲章」が採択された。また同時に「ITが提供する機会の活用」「デジタルデバイド解消」のために「ドットフォース(Digital Opportunity Taskforce)」という作業部会が設置された。2000年という年は日本ではIT革命という言葉が流行した時期であり、開発途上国へのICTの導入の促進が開発活動の活性化につながるとの認識が共通認識となった時期でもある。同じく2000年に国連ミレニアムサミットが開かれミレニアム開発目標が発表された。2001年のジェノヴァ・サミットにおいてはドットフォースによるジェノヴァ行動計画が示され、2002年にはジェノヴァ行動計画の実施状況報告書が提示された。

2003年には国連による初めてのICT関連のサミットとして世界情報社会サミット(World Summit on the Information Society :WSIS)の第1フェーズがジュネーブで開催された。ここでは基本宣言の共通ビジョンとして「1.持続可能な開発と生活の質の向上を可能とする情報社会の構築」「2.ICTによる生産性を向上させ、経済成長の原動力となり雇用を創出するなどいっそうの発展のための新しい機会を提供」「3.デジタル・デバイドの解消」が掲げられた。また情報インフラ整備、人材開発、メディアの重要性などの「情報社会の鍵となる11原則」も基本宣言に含まれる。また世界の村々をネットワークに接続し公共アクセスポイントを設置、すべての大学、専門学校、中高校をネットワークに

接続するなどの「2015 年までの達成を目指した 10 の ICT の目標」の行動計画も示された。世界情報社会サミットは第 2 フェーズが 2005 年にチュニスで開かれた。ここでは第 1 フェーズで採択された基本宣言・行動計画がチュニス・コミットメントおよびチュニス・アジェンダとして確認され、これらを具体化するための要な資金支援メカニズムやインターネットガバナンス、また今後の実施とフォローアップについて具体的な検討がなされた。コミットメントでは「我々は、情報へのアクセスと知識の共有及び創造が、経済、社会、文化的発展の強化に大きく貢献するものであり、すべての国におけるミレニアム開発目標をはじめとする国際的に合意された開発目標の達成を助けることを認識する」とされ、コミットメントのなかのミレニアム開発目標と関連する部分においてはデジタル・デバイドの克服が強調されている。



図表 1　世界の携帯電話、固定電話、インターネットユーザー、パソコンの普及率
出所：国連開発計画（UNDP）The Millennium Development Goals Report 2006

ミレニアム開発目標の内容をみると、2015 年までに達成すべき 8 つの目標（ゴール）と 18 のターゲットを設定されている。またターゲットには合計で 48 の指標が設定されている。

目標 1.　極度の貧困と飢餓の撲滅	
	ターゲット 1 ：2015 年までに 1 日 1 ドル未満で生活する人口を半減させる。
	ターゲット 2:　2015 年までに飢餓に苦しむ人口の割合を半減さえる。
目標 2.　普遍的初等教育の達成	
	ターゲット 3:　2015 年までに全ての子供が男女の区別なく初等教育の全課程を修了できるようにする。
目標 3.　ジェンダーの平等の推進と助成の地位向上	
	ターゲット 4：初等・中等教育における男女格差の解消を 2005 年までには達成し、2015 年までに全ての教育レベルにおける男女格差を解消する。
目標 4.　幼児死亡率の削減	
	ターゲット 5:　2015 年までに 5 歳未満児の死亡率を 3 分の 2 減少させる。
目標 5.　妊産婦の健康の改善	
	ターゲット 6:　2015 年までに妊産婦の死亡率を 4 分の 3 減少させる。
目標 6.　HIV/AIDS、マラリア、その他の疾病の蔓延防止	
	ターゲット 7:　HIV／エイズの蔓延を 2015 年までに阻止し、その後減少させる。

	ターゲット 8: マラリア及びその他の主要な疾病の発生を 2015 年までに阻止し、その後発生率を下げる。
目標 7. 環境の持続可能性の確保	
	ターゲット 9: 持続可能な開発の原則を各国の政策や戦略に反映させ、環境資源の喪失を阻止し回復を図る。
	ターゲット 10: 2015 年までに安全な飲料水と基礎的な衛生施設を継続的に利用できない人々の割合を半減する。
	ターゲット 11:2020 年までに、少なくとも 1 億人のスラム居住者の生活を大幅に改善
目標 8. 開発のためのグローバル・パートナーシップの推進	
	ターゲット 12: 開放的でルールに基づき予測可能でかつ差別的でない貿易及び金融システムの構築。
	ターゲット 13: 後発開発途上国の特別なニーズに対応する。
	ターゲット 14: 内陸開発途上国及び小島嶼開発途上国の特別なニーズに対応する。
	ターゲット 15: 債務を長期的に持続可能なものとするために、国内及び国際的措置を通じて開発途上国の債務問題に包括的に対応する。
	ターゲット 16: 開発途上国と協力し、適切で生産的な仕事を若者に提供するための戦略を策定・実施。
	ターゲット 17: 製薬会社と協力して開発途上国において人々が安価で必要不可欠な医薬品を入手できるようにする。
	ターゲット 18: 民間部門と協力し、特に情報・通信における新技術による利益が得られるようにする。 指標 47. 人口 100 人当たりの電話回線及び携帯電話加入者数 指標 48. 人口 100 人当たりの使用パソコン台数及びインターネット利用者数

図表 2 ミレニアム開発目標が掲げる 8 つの目標と 18 のターゲット
出所：外務省「ミレニアム開発目標 2015 年に向けた日本のイニシアティブ」

ミレニアム開発目標において ICT に関連するのは「目標 8. 開発のためのグローバル・パートナーシップの推進」の、「ターゲット 18：民間部門と協力し、特に情報・通信における新技術による利益が得られるようにする」にある指標 47、48 の 2 つでのみある。しかし ICT はインフラ整備やハードウェアの普及という意味にとどまらず、有効なツールとして経済社会のあらゆる面での利活用が期待できる。そこで ITU の開発部門(Development Sector)である ITU-D の『World Telecommunication Report 2006』では ICT のミレニアム開発目標への影響を、組織または国家の 2 つのレベルに区分して指標を策定し測定を試みようとしている。

MDG 目標	インプット	アウトプット	結果（インパクト）
1	ICT による農産物価格情報の提供	農家の農作物価格情報へのアクセス	農業従事者の増収
2	ネットワークによる教員養成大学	ICT による低コストでの教員トレーニング	ICT トレーニングを受けた教師の増加
3	ICT トレーニングを提供するコミュニ	ICT によるトレーニングをうけ	女性が従事できる仕事の

	ティセンター	た女性	数と種類の増加
4	遠隔医療ネットワークに接続した地方病院	ウェブによる相談	乳幼児死亡率の減少
5	地方病院へのオンラインでの情報提供	診断の質向上	妊産婦死亡率の減少
6	HIV/AIDS 情報を提供するコールセンター	潜在的な患者へのアドバイス	新たに HIV/AID に感染する人数の減少
7	環境問題についての e-グループネットワーク	情報、問題の交換	環境意識の高まり
8	大学での ICT トレーニング	IT を学んだ学生の増加	若年失業率の減少

図表 3　組織レベルでの指標

出所：ITU　World Telecommunication Report 2006

MDG 目標	インプット	アウトプット	結果（インパクト）
1	ICT アクセスの普及	収入の増加	年収の増加
2	ICT トレーニングを受けた教員と ICT に支援された現職教員の増加	ICT を使用できる教員数の増加	ICT に支援された教育をうけた学生の増加
3	女性の訓練に向けられた ICT の取り組み	ICT トレーニングを受けた女性と取り組みの増加	女性ステータスの変化と ICT を使った雇用
4	インターネットに接続した地方病院の増加	看護師への ICT により支援されたアドバイス	ICT にサポートされた病院における乳幼児死亡率の減少
5	ICT に支援された訓練の増加とヘルススタッフへの相談	ICT を使った診断と専門家の増加	ICT による訓練をうけたスタッフによる妊産婦死亡率の減少
6	電話かインターネットによる相談にアクセスする機会の提供	電話かインターネットによるアドバイスをうけた人々	HIV/AIDS ケースの減少と電話やオンラインでのアドバイスをもとめた患者への治療の改善
7	ICT による持続的発展についてのナショナルレポートの提供	ICT による情報交換とネットワーキング	環境の濫用を抑制するより効果的アクション
8	グローバルな専門家のネットワーク	ベストプラクティスの共有	より円滑な MDGs の達成

図表 4　国家レベルでの指標

出所：ITU　World Telecommunication Report 2006

次に日本における ICT による開発援助について述べる。日本は多額の政府開発援助（Official Development Assistance:ODA）や国連の分担金を負担しており、世界でも最大規模のドナーカントリーとしてミレニアム開発目標の達成に取り組み、ミレニアム開発目標を開発途上国に対する重要な

目標と設定している。日本では2001年のe-Japan戦略の策定し推進したことにより通信インフラ整備や技術開発が進み、現在ではその整ったインフラの利活用に取り組む段階である。国際協力機構（Japan International Cooperation Agency: JICA）によると現在の日本のITに関する国際的な優位性は次の4つと認識されている。「世界的にみて安価で高速なインターネット環境」「モバイル技術、光通信技術、デバイス技術、情報家電」「ソフトウェア、情報セキュリティ、ヒューマンインターフェイスの技術研究」「アニメーションなどのコンテンツ制作技術」。これらの優位を活かした開発途上国への支援としては、デジタル・デバイドの解消とデジタル・オポチュニティの解消が現在の課題となっている。ICTに関する具体的な取り組みの分類は2000年の九州・沖縄サミットにおいて発表された「国際的な情報格差問題に対する我が国の包括的協力策」に示された4つの柱である。4つの柱はその後5つと変化しており、「1.IT政策における能力の向上」「2.IT人材の育成」「3.通信基盤の整備」「4.各分野へのIT活用による効率・効果の向上」「5.IT活用による援助における効率・効果の向上」でありそれぞれに中間目標が設定されている。

開発戦略目標	中間目標
1.IT政策策定能力の向上	1-1　電気通信政策の確立
	1-2　IT産業育成政策の確立
	1-3　国内格差の解消政策の確立
	1-4　利用者保護
2.IT人材の育成	2-1　技術者・講師の育成
	2-2　政策担当者の育成
3.通信基盤の整備	3-1　通信基盤の整備
	3-2　インターネット接続業者(ISP)への支援
	3-3　利用拠点の整備
4.各分野へのIT活用による効率・効果の向上	4-1　電子政府の整備による効率・効果の向上
	4-2　各分野のIT活用(保険、医療、教育分野等)
5.IT活用による援助における効率・効果の向上	5-1　既存知識の普及・移転
	5-2　経験知識の共有・創造
	5-3　事業実施業務へのIT利用

図表5　情報通信技術　開発課題体系全体図
出所：JICA「課題別指針情報通信技術」

2003年の新ODA大綱では「発展途上国の自助努力支援」「人間の安全保障」「公平性の確保」「日本の経験と知見の活用」「国際社会における強調と連携」を基本方針とし、4つの重点課題「貧困削減」「持続的成長」「地球的規模の問題への取り組み」「平和の構築」を掲げている。ICTは重点課題である「持続的成長」に含まれている。また「国際社会は、ICTを利用可能な人や地域とそうでない人や地域との間にある情報格差（デジタル・デバイド）の問題に対処するとともに、ICTを用いて開発途上国における貧困削減や持続的成長、人々の政治参加や政府の情報公開の促進等といった参加型の開発に貢献する」とされ、ミレニアム開発目標の「目標8：開発のためのグローバルなパートナーシッ

プの推進」と関連して、ICTの開発援助は「機材等のハード面やそれを使いこなす人材育成といったソフト面への協力にとどまらず、遠隔教育や統計・観測など様々な分野においても活用」するとしている。

日本はICTの先進国であるが、ミレニアム開発目標の達成やODAにおいてのICTの役割について考えることは少ないように思われる。まさにODA基本方針である「日本の経験と知見の活用」が開発協力には求められており、我々が日本の国内各地域で日々積み重ねているICTに関連する幅広い取り組みは、蓄積された経験と知見として求められているのである。

参考文献、資料：

infoDev(2003) "ICT for Development, Contribution to the Millennium Development Goals"
ITU(2006) "World Telecommunication Report2006"
The World Bank(2006) "2006 Information and Communication for Development Global Trends and Policies"
UNDP(2005) "Regional Human Development Report ,Promoting ICT for Human Development in Asia"
UNDP(2006) "The Millennium Development Goals Report 2006"
独立行政法人国際協力機構「課題別指針 情報通信技術 平成17年4月改訂版」

オープンソースソフトウエアの応用研究

(財)ハイパーネットワーク社会研究所 研究企画部長 江原 裕幸

1 はじめに

オープンソースソフトウエア(以下 OSS)と呼ばれる種類のソフトウエアを有効に利用し、迅速に安価に、高機能なシステムを作り上げることで、インターネット上の企業が急成長を遂げている。また、経済産業省の「情報システムに係る相互運用性フレームワーク案」に見られるように、特定の商品を前提とした調達を止め、オープンな標準に基づく調達を行なうことが望ましいなど、国の方針としてもプロプライテリアなソフトウエアからの脱却を図る機運にある。

その様な状況の中、当研究所においても、数年前から OSS の可能性に注目し、OSS の普及啓発に努めてきた。本研究報告では、当研究所における OSS の取り組みについて、これまでの経緯と、これからの可能性について説明したい。

2 調査、啓発活動

2003 年の 5 月の「Linux World Expo/ Tokyo 2003」をはじめとして、各種 OSS 関係のセミナーに出席し、OSS の現状の調査を行ない、第 40 回ハイパーフォーラム「オープンソース最前線」(2003 年 8 月 11 日開催) という形で、その調査成果を現すことができた。このフォーラムでは、当時インターネット上でその発言が物議を醸し出し非常に注目されていた経済産業省 商務情報局情報処理振興課 課長補佐 久米 孝 氏をはじめとし、OSDL ラボディレクタの高澤氏、Windows サーバ互換ソフトの samba の小田切氏など、非常に著名でありかつ OSS の将来について確固としたビジョンを持った方々を講師に招くことができ、大変好評を得た。

しかし、フォーラム終了後は、OSS に関する機運を高めることが出来ず、地道な調査活動を継続していった。

3 公募事業に関する活動

3-1 はじめての応募

OSS の安価で高機能なソフトウエアのメリットを大分でも享受可能であることを示すためには、実際に OSS を用いた導入事例を作ることが重要であると考えた。また、それに呼応するように OSS 普及促進のための導入実証実験が国を中心として公募されはじめていた。

そこで、Linux の一種である KNOPPIX の技術を持つ大分県産業科学技術センターの後藤氏、KNOPPIX の学校への展開を模索していたアルファシステムズの千葉氏と組み、学校関係の実証実験公募 (2005 年 6 月) に応募した。

提案書作成段階から参加学校の先生や参加企業でキックオフミーティングを行うなど、非常に協力的な関係が築け、提案内容も新規性、実現可能性を考慮した非常に完成度の高いものにすることができたが、残念ながら結果は不採択となった。今、振返ってみると、教育委員会など学校を監督する団体の参加が薄かったこと、公募元の要望を確かめるための努力が足りなかったなど、公募に対するノウハウが未熟であったと思われる。

3-2 はじめての採択

前回の応募の失敗を反省し、2005 年度の IPA(情報処理推進機構)の「オープンソースソフトウェア活用基盤整備事業」に挑戦した。これは、自治体の職員 PC を OSS に置き換えることができるか、という実証実験である。

実証実験に参加いただく自治体がなかなか見つからず応募が危ぶまれたが、締切の二週間前に津久見市が協力を申し出てくれて、津久見市、当研究所、大分県産業科学技術センター、(株)アルファシステムズ、(株)大分県自治体共同アウトソーシングセンターの体制で望んだ。公募元の IPA を訪ね公募目的の確認を行い、大分県庁 I T推進課をはじめとした関係部署の協力の承認をもらったうえで提案書を準備、応募した

結果として採択され 2005 年 10 月～2006 年 5 月まで導入実証を行い、大分における OSS 活用の貴重な一事例を作ることができた。

OSS による端末 PC の設置風景

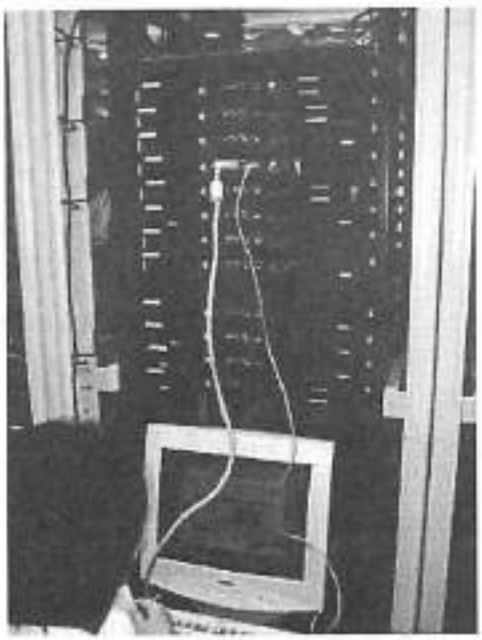
詳細については、昨年度の当研究所の研究報告書ならびに、以下で公開されている成果報告書を参照いただきたい。

http://www.ipa.go.jp/software/open/2005/stc/report/tsukumi.html

3-3 公募事業のその後

(財)コンピュータ教育開発センター「平成 18 年度教育情報化促進基盤整備事業（E スクエア・エボリューション)」(2006 年 8 月～2007 年 3 月)、2006 年度の IPA の公募(大分県庁において OSS を用いた自治体基盤システムの構築、導入実証 2006 年 10 月～2007 年 6 月)に採択され、大分での OSS 利活用事例を順調に増やしている。

OSS による授業風景



OSS 自治体基盤システムサーバ設置風景

4 その他の OSS 普及活動

2006 年 7 月には、大分県オープンソースソフトウエア研究会を大分県商工労働部工業振興課の協力のもと設立し、産官学連携による OSS の普及活動団体を立ち上げた。二ヶ月に一度のセミナーの開催、Ring Server の構築、北東アジア OSS 推進フォーラムでの展示、Open Source Conference 2007 Spring/Tokyo での展示、発表など、これまでとは異なり、大分での OSS 普及活動自体を広く全国に広報する活動を行っている。

研究会風景

また、公募事業の取り組みの結果、第 50 回ハイパーフォーラムにおいて「オープンソースソフトウエアの可能性」と言うタイトルで二年半ぶりに OSS 関連のフォーラムを開催することができた。

4 まとめと今後

全くのゼロからのスタートであった OSS に関する取り組みであったが、OSS 関係者との幸運な出会い、大分県下の自治体・企業・大学の皆さまの協力のおかげで、三つの公募事業を実施し、大分県 OSS 研究会を設立するなど、まさに花開こうとしている。

今後は、これまでの取り組みをより発展させていくとともに、OSS 関連ビジネスを大分で実施できるよう挑戦を続けていく。

日田玖珠広域圏における芯線民間開放への取組み

首藤　隆士

1．はじめに

大分県下の自治体向けに情報化支援及びコンサルティングを地域情報化の活動主体として行ってきた。大分県における豊の国ハイパーネットワークの構築も一段落をしたが、現在は構築されたネットワークを今後の地域発展に役立てて行きたいと検討する自治体に対し、支援業務を行ってきた。また、多くの市町村合併がおこなわれたが、合併した自治体にとっての一体感を出すための取り組みに対する支援業務も合わせて行ってきた。

助成金の活用が必要な事業においては、自治体が意図していることをヒアリングし、国の政策や助成事業の動きと比較しながら、交付金や補助金を活用する分野や可能性について検討し、助言するなど、準備段階からの支援に取組んでいる。

例えば総務省の地理的デジタル・ディバイドの解消を目指した地域情報基盤の整備促進を図る助成事業「地域情報通信基盤整備推進交付金」、「地域イントラネット基盤施設整備事業」、「地域公共ネットワークの民間開放」や、農水省の地域のケーブルテレビ・情報基盤の整備や良好な農村景観の再生・保全に向けた改修等を行う「元気な地域づくり交付金」[1]などから、地域の特性や自治体の要望、取り組みにあった助成事業を検討した。

各市町村の状況は様々であり、情報化の実施内容も市町村によってずいぶん異なるものとなってきているが、その実施内容の多くは市町村単独での事業は困難な状況にあるといえる。

地域間の連携、または自治体間の連携が、システムやインフラだけではなく、自治体発注事業を受注するための共同運営などの事務運営においても、従来の枠や考えにとらわれず、県及び近隣自治体と連携してより効率的な仕組みの創出が必要とされている。

2．目的

大分県内の学術・研究機関、教育機関は、県人口の3分の1を占める県庁所在地大分市に集中しているが、日田玖珠地域については、学術・研究機関等の数も少なく、これらの機関・施設のサービスの向上、技術の高度化等が求められている。

大分県内の学術・研究機関、教育機関等と日田玖珠地域の行政機関、学校、公民館等を光ファイバによる伝送路で結び、動画や音声などの大容量の情報を高速かつ双方向、リアルタイムで処理した情報通信ネットワークを構築して、教育、防災に密着したサービスを広域的に提供し、同地域の振興を図ることを目的としている。

また今回は、自治体や公共団体間の拠点接続のみをターゲットとしたものではなく、構築する双方向通信網(光ファイバー)の一部を、2007年(予定)から日田市は地域のケーブルテレビ会社に、九重町は町を主体としてケーブルテレビ事業を行い(予定)、ブロードバンドに関しては町全体が未整備地域でもあるため、高速インターネットアクセス事業者(予定)へ開放を行い、

---

1 *「元気な地域づくり交付金」は2007年度から林野庁・水産庁の交付金と統合し、農山漁村活性化プロジェクト支援交付金に変わった。*

玖珠町も高速インターネットアクセス事業者（予定)に開放し、住民サービスの向上を図るための新しい試みでもある。

3．背景と概要

日田玖珠広域圏と呼ばれる日田市、九重町及び玖珠町は、大分県の西部に位置し、地形的に山間地を多く抱えている。管内中心部を高速自動車道が貫通しているものの、周辺部の交通事情は決して良いとは言えない。日田市は平成17年3月22日に1市2町3村が合併し、新生日田市として動き出した。しかしながら、旧日田市については光ケーブルが未整備であり、日田市、九重町及び玖珠町はいずれも非常に広大な行政面積を有しており、一部の地域でケーブルテレビやADSLサービスが提供されているのみで、九重町、玖珠町の多くの地域では高速の情報通信インフラが提供されていない。情報化が世界的かつ急速に進展している中にあって、すべての住民がその恩恵を享受するためには、地域の情報通信インフラの構築は急務であると言える。そこで日田市役所、九重町役場及び玖珠町役場内に情報発信の拠点となる“地域情報センター”を設置し、公共施設、学校、民間施設等を100Mbpsの光ファイバで結ぶネットワークを構築する。これにより、動画や音声などの大容量の情報を高速かつ双方向、リアルタイムでの処理が可能となり、生活に密着したサービスを広域的に提供し、同地域の振興を図る。

また、日田市、九重町及び玖珠町は日田市内で三隈川となる同じ一級河川の流域に位置し、台風などの災害時には、リアルタイムでの河川状況や、雨量及び河川水位等の県の防災関係情報を迅速に共有する必要があり、県を含む日田玖珠広域圏の構成団体である日田市、九重町、玖珠町で連携し、本事業を活用しての防災への取組みを行う。

4．光芯線の民間への開放

2003年12月より開始された地上デジタル放送への対応、ケーブルテレビ事業者による電話サービスやインターネット接続サービスも盛んに行われてきている現状をふまえ、次のステップとなる民間への芯線開放について、ブロードバンド未整備地域の世帯数などを考慮しながら、開放用芯線数と開放拠点を検討した。

民間開放用芯線の運用には、次のような様々な形態があり、日田玖珠広域連携の事業ではあるが、日田市、九重町、玖珠町それぞれの地域によって最良の選択となるように今後も検討を重ねる必要がある。

FTTHでインターネット接続サービスとケーブルテレビサービスの双方を提供する場合

（1） 自治体が電気通信事業者及びCATV事業者として自らサービスを提供

（2） 自治体が整備した設備を民間事業者にIRU契約により提供し、当該事業者がサービスを提供

（3） 自治体が整備した設備を民間電気通信事業者及び民間CATV事業者にIRU契約により芯線単位で提供し、それぞれの事業者がサービスを提供

（4） 自治体が整備した設備を民間電気通信事業者に卸電気通信役務により波長単位で提供（帯域貸し）し、放送サービスについては自治体が CATV 事業者となり、自らサービスを提供

FTTH でインターネット接続サービスのみを提供する場合

（1） 自治体が電気通信事業者として自らサービスを提供

（2） 自治体が整備した設備を民間電気通信事業者に IRU 契約により提供し、当該事業者が　サービスを提供

（3） 自治体が整備した設備を民間電気通信事業者に IRU 契約により提供し、その役務提供を受けて自治体がサービスを提供

※ 地域情報通信基盤整備推進交付金 情報通信基盤整備事例集より抜粋［総務省 情報通信政策局］

5．事業の特徴

多種多様な情報がインターネット等を通じて流通しているなか、顕著化している情報と放送の格差を是正するため、また新しい地域発展が生まれるために必要とされる新しい情報ネットワーク構築を目指している。

ICT の活用は、費用や時間などに大きな変化をもたらすことが可能だが、高所得の追求や費用削減、時間の短縮ばかりに捉われた社会ではなく、地域文化や地域の交流なども支援するとともに、日常生活の向上に対する不安や障害を取り除きながら豊かな生活に役立つことを目指し、情報化を進めることが大切である。

自治体の情報化への取り組み次第では、近隣の自治体間でも情報格差が生じて市民生活等へ影響がでることが懸念されているなか、広域連携というかたちで、ICT をうまく活用し、産業の振興や防犯防災、福祉の増進、教育・文化の振興、新たな交流等を支援し、地域の隅々まで必要な情報が行き渡り、誰もが容易に情報を利活用できる環境の整備を推進する。

6．スケジュール

2005 年 11 月　地域情報化構想を取りまとめを開始
2006 年 3 月　2006 年度地域イントラネット基盤施設整備事業個別調書を提出
2006 年 5 月　2006 年度地域イントラネット基盤施設整備事業交付申請書を提出
2006 年 6 月　交付決定
2006 年 7 月　実施設計業者決定
2006 年 9 月　施工業者決定
2007 年 3 月　事業完了、実績報告書提出

7．日田市第２次情報化基本計画[2]策定の支援

日田市においては、日田市第２次情報化基本計画策定に向けて、開催している検討委員会の委員として参画し、下部組織であるワーキングにもオブザーバーとして出席、意見を述べるなどの活動も事業と並行し行ってきた。検討委員会は日田市第２次情報化基本計画のあり方を話し合う場として、外部有識者も参加し、活発な議論が行われた。

委員会のなかでは、未だ携帯電話の不感地域やテレビ放送の難視聴地域が多く存在している、ブロードバンド環境に関しても整備されていない地域が多く存在するなど、情報通信に関するインフラ整備の遅れによる市街地と周辺地域の情報格差拡大が、問題の一つとして取り上げられていたが、今回の民間開放への取り組みが問題解決の礎となることを期待している。

本計画は合併による行政区域の大幅な拡大、少子高齢化や過疎化等、第１次日田市情報化基本計画策定後の著しい社会情勢の変化に対応するとともに、近年のインターネットを中心とした急速な情報化の進展を踏まえた、情報化施策の指針となるものであり、この検討委員会へ参画した経験を他でも活かせるよう努力を続けていきたい。

第１回ワーキング開催　2006-06-xx
第１回委員会開催　2006-07-18
第２回ワーキング開催　2006-10-05
第２回委員会開催　2006-10-17
第３回委員会開催　2006-12-20
第４回ワーキング開催　2006-02-28

8．住民向けサービスの向上

国が e-Japan 戦略や u-Japan 戦略を推進した結果、情報基盤の整備からそれを活用したアプリケーションに重点が移されつつある。この事業も行政事務の効率化を目指したものではなく、基本路線は住民へのサービス向上であり、事業によって日田玖珠地域における各種行政機関等の機能を補完する下記のようなサービスの提供が可能となる。

（１）　おおいた教育ハイパーセンターネット
　　小･中･高等学校における、インターネット活用教育に必要な高速なインターネット回線を確保し、またインターネットコンテンツのフィルタリングを行う。

（２）　大分県総合防災情報システム
　　大分県防災センターが発信する防災ヘリコプター、交通監視カメラなどで撮影した災害状況等の映像情報を元に、住民への迅速な避難対策の指示を行う。

（３）　大分県生涯学習システム

---

[2]市政の最上位計画である第５次日田市総合計画がめざす「便利で快適なまちづくり」の「情報通信基盤整備」を実現させ、国の高度情報通信ネットワーク社会形成基本法（ＩＴ基本法）や e-Japan 戦略、e-Japan 戦略Ⅱ、IT 新改革戦略、u-Japan 政策、大分県の「大分県地域情報化計画」等との整合性を考慮し、これからの日田市の情報化施策に関する基本的な考え方、方向性を示すものである。

大分県生涯教育センター、大分県教育センター、大分県芸術文化短期大学、大分県立図書館等から発信する生涯教育公開講座等の映像コンテンツや生涯学習情報、蔵書検索等を市町村役場や公民館等で閲覧する。

（4） 施設情報提供システム

施設情報（施設紹介、活動内容、イベント情報等）の提供を行う。

（5） 電子申請等受付システム

ICカードとICカードリーダを用い、県や市町村への各種申請、届出を行う。

（6） 行政情報提供システム

行政情報を住民に対してわかりやすく情報公開し、住民サービスの向上を図る。
地域の福祉情報及びイベント開催、不審者情報のお知らせなど、行政情報の提供を行う。
またＷｅｂカメラによる地域の情報発信もおこなう事ができる。

（7） 図書館システム

日田市の図書館の蔵書情報及び予約状況等を、インターネットを利用して提供する。

（8） 防災情報提供システム

日田玖珠地域の防災情報を提供する総合ポータルサイトを作成し、日田市、九重町及び玖珠町の各所に設置したWebカメラからの映像情報や、日田玖珠地域の公共機関、交通機関及び県からの防災に関する各種情報を提供する。災害の危険がある時は住民及び遠隔地に住む日田玖珠地域ゆかりの人々に対して防災情報をいち早く提供する手段とする。

９．終わりに

豊の国ハイパーネットワークの構築及び地域イントラネット整備事業コンサルティングを通じて培った情報化支援業務のノウハウを県外自治体でも適応すべく、事業紹介を通して今後の共同事業化に取組んでいきたいと考えている。

地域情報ネットワークを構築することによって、どのようなアプリケーションやコンテンツを提供をしていき、どのようなまちづくりをしていくか？

技術動向やトレンドをを踏まえて、構築する地域情報ネットワークとはどのような技術、技法を採用したものであるべきか？

構築に際して活用する予算としての交付金や補助金を活用する分野や可能性は？、構築方法としての民間活力の活用は？、運営方法としての運営会社の形態は？

普及促進策として、地域の先進的な情報化の取組みに関する上記のようなナレッジを集約し、普及促進のためのセミナーや研究会等の開催および各種地域情報化推進に関する活動の支援を行っていく。

また、地方自治体の情報システムの改革支援や、地方自治体内外の地域における多数の情報システムをオープンに連携させるための基盤構築を推進するとともに、地方公共団体で共通利用が可能な公共のアプリケーションの整備等の促進を図る。

地域からの情報発信や、電子自治体の地域住民の Quolity Of Life（生活の質）を向上させるようなITライフ実現を目指し、今後も活動の場を広げていきたい。

地域情報化における支援活動内容

◆平成12年度　自治体向け情報化支援及びコンサルティング	
	＜豊の国ハイパーネットワーク事業関係＞
2000年4月～2001年3月	豊の国ハイパーネットワーク構想策定業務
2000年9月～2001年3月	県南ルート　事業開始支援
	設計業者に対して、ネットワーク構築に向けたすり合わせ、現地説明会を実施
2000年10月～2001年2月	県南ルート　直川村支援
	直川村の基本設計を請負い、関係各所と調整の上、基本設計書を作成
2000年11月～2001年8月	大野竹田ルート　事業説明事業開始支援
	大野竹田地区の市町村に対し、事業内容の説明会を実施し、郵政省に対しての予算申請書作成を支援。 設計業者に対して、構築に向けたすり合わせ、現地説明会また、事業費低減のために機器統合実現への調整作業を実施。
2001年2月～2001年9月	大野竹田ルート　千歳村支援
	千歳村の基本設計を請負い、関係各所と調整の上、基本設計書を作成
2001年2月～2001年9月	大野竹田ルート　竹田市支援
	竹田市の基本設計を請負い、関係各所と調整の上、基本設計書を作成
2001年3月～2002年9月	別杵国東ルート　事業説明支援
	別杵国東地区の市町村に対し、事業内容の説明会を実施し、総務省に対しての予算申請書作成を支援
	＜ISP協議会＞
2000年10月～（継続中）	地域ISP協議会設置に向けた活動
	豊の国ハイパーネットワークが民間開放された際、活用先として期待されている地域ISPに対して、その活動支援等を目的とした地域ISP協議会を設立に向けた動きを実施。 地域ISP間ではCATV各社を含めて、地方アクセスポイントやバックボーンの共有に向けた活動を支援も実施し、新設されるデータセンタの利用密度を上げるための活動。 2001年12月に開催する会議にて大分県ISP協議会を設立。
◆平成13年度　自治体向け情報化支援及びコンサルティング	
	＜テレビ会議＞
2001年4月～2001年10月	テレビ会議システム　検証
	豊の国ハイパーネットワーク上で稼動させるアプリケーションとして複数形式のテレビ会議システムの検証を実施。 山口、北九州に出向き調査検証し、メーカー約１０社のシステムの調査

	検討を行った。
	＜無線関係＞
2001年4月～2001年7月	県庁と大分商業高校との無線実験
	県庁と大分商業高校間を無線LANで結び、都市部における無線LANの接続試験を通し、有効性を検証
2001年6月～2001年9月	国見町と姫島村との無線接続検証
	国見町と姫島村間、海上約4キロをはさんで、VLAN対応無線LAN機器の性能試験を実施
	＜IT講習＞
2001年2月～2002年3月	豊の国IT塾サポート事業
	国のIT講習事業に基づき実施された、県下2万人を対象とした豊の国IT塾を実施するに際して、そのサポート事業を実施。
	豊の国IT塾講師向け講習会の実施、豊の国IT塾講習用テキストの作成配布、豊の国IT塾実施主体（市町村など）に対し支援を行う。
2001年6月～2001年9月	竹田市庁内LAN構築支援
	竹田市役所における新庁内LANシステム構築及びパソコン等導入を支援。
◆平成14年度　自治体向け情報化支援及びコンサルティング	
	＜豊の国ハイパーネットワーク事業関係（市町村単独事業分）＞
2001年12月～2003年3月	中津下毛地区　地域イントラネット事業支援
	中津下毛情報通信技術研究協議会への参加、先進地視察先のコーディネイト等を実施
	2002年3月、中津下毛地区の5市町村で中津下毛地域広域市町村圏事務組合が窓口となって広域的に地域イントラネット事業に取り組む。その事業計画の取りまとめ及び総務省への申請業務、地域イントラネット事業の基本設計を行う。
2001年12月～2003年3月	津久見市　地域イントラネット事業及び情報化事業計画策定支援
	津久見市にて構想中の情報化事業の実施に向けて、先進地視察のコーディネイト等を実施し、その後の現地調査及び基本計画作成を行う。 津久見市で地域イントラネット事業に取り組み、事業計画の取りまとめを実施。
	＜豊の国ハイパーネットワーク事業関係（県関係事業分）＞
2001年3月～2002年3月	別杵国東ルート　事業説明事業開始支援
	別杵国東地区の市町村に対し、事業内容の説明会を実施し、総務省に対しての予算申請書作成を支援。
2001年3月～2002年3月	日田玖珠ルート　事業説明事業開始支援
	別杵国東地区の市町村に対し、事業内容の説明会を実施、総務省に対しての予算申請書作成を支援。
2002年2月～2003年3月	別杵国東ルート　国東町支援

	国東町の基本設計を請負い、関係各所と調整、基本設計書を作成。 設計業者決定後、第三者的立場として国東町と設計業者との打ち合わせの場に参加し、実施設計書作成の監理を行う。
2002年2月～2003年3月	別杵国東ルート　姫島村支援
	姫島村の基本設計を請負い、関係各所と調整の上、基本設計書を提出。 設計業者決定後、第三者的立場として姫島村と設計業者との打ち合わせに参加し、実施設計書作成の監理を行う。
2002年2月～2003年3月	日田玖珠ルート　中津江村支援
	中津江村の基本設計を請負い、関係各所と調整の上、基本設計書を提出。 設計業者決定後、第三者的立場として中津江村と設計業者との打ち合わせに参加し、実施設計書作成を支援。
	＜テレビ会議＞
2002年1月～2003年3月	テレビ会議システム　検証
	2003 年度から児童相談所でカンファレンス用として使用することを目的に、複数形式のテレビ会議システムの検証を実施。
	＜電子自治体＞
2002年4月～（継続中）	電子自治体に関するメーリングリストの運営
	臼杵市、竹田市、大分県庁関係機関及び中央の有識者と共に、ハイパー研主催で電子自治体に関するメーリングリストを立ち上げ、ネットワーク上で議論を交換
◆平成15年度　自治体向け情報化支援及びコンサルティング	
2003年4月～2003年9月	宇佐両院地区［宇佐市、院内町、安心院町］
	2002年度補正地域イントラネット事業
	事業申請書作成、基本設計書作成、実施設計業者に対する監理を行う。
2003年4月～2003年9月	西高地区［真玉町、香々地町］
	2002年度補正地域イントラネット事業（大分県との共同事業）
	事業申請書作成、基本設計書作成、実施設計業者に対する監理を行う。
2003年4月～2004年3月	津久見市
	2002年度補正地域イントラネット事業（大分県との共同事業）継続
	2003年度当初住民向けインターネット事業（ADSLを用いた情報化）
	業申請書作成、基本設計書作成、実施設計業者に対する監理を行う。 総務省及びNTT西日本に対する事業申請業務の代行
2003年4月～2003年11月	中津下毛地区［中津市、三光村、本耶馬渓町、耶馬渓町、山国町］
	2002年度当初地域イントラネット事業
	実施設計業者に対する監理業務、実績報告書を作成
2003年4月～2004年3月	竹田直入地区［竹田市、荻町、久住町、直入町］
	2003度当初地域イントラネット事業
	事業申請書作成、基本設計書作成、実施設計業者に対する監理を行う。
2003年4月～2004年3月	県外自治体向け情報化支援及びコンサルティング

	大分県内における豊の国ハイパーネットワークの構築を通じて培った情報化支援業務のノウハウを県外自治体でも適応すべく、事業紹介を通し、今後の共同事業化を目指した活動を行う。
◆平成16年度　自治体向け情報化支援及びコンサルティング	
	＜合併情報化＞
2004年4月～2005年3月	豊後大野市　新市合併に伴う情報化支援
	基幹系システム統合の支援
	情報系システム統合の支援
	VoIP導入の支援
◆平成17年度　自治体向け情報化支援及びコンサルティング	
2005年10月～2006年3月	中津市　新情報ネットワーク検討委員会運営業務
	中津市　新情報ネットワーク基本設計書作成
	中津市新情報ネットワーク構築に向け、そのあり方を話し合う場として外部有識者も参加し、開催している検討委員会（外部有識者も参加）の事務局として取りまとめ、コーディネートを行う。 検討委員会の成果物として、基本設計書を作成。
2005年12月～2006年3月	日田玖珠地区［日田市、九重町、玖珠町］
	2006年度地域イントラネット事業（大分県との共同事業）
	地域イントラネット事業実施に向けて、個別調書及び交付申請書を作成。 日田市においては平成18年度の情報化構想策定に向けた支援も行う。
2005年4月～2006年3月	津久見市　情報化支援業務
	津久見市で構築した市民ADSL事業の構築支援をきっかけに、2003年より継続して情報化支援業務として、各種の指導、助言を行う。
	この支援業務を通して、当研究所がIPAより受託した「自治体におけるオープンソースソフトウェア活用に向けての導入実証」の実証自治体となって頂く。
◆平成18年度　自治体向け情報化支援及びコンサルティング	
2006年4月～2006年9月	日田玖珠地区［日田市、九重町、玖珠町］
	2006年度地域イントラネット事業（大分県との共同事業）
	総務省への交付申請書作成、基本設計書、実施設計入札仕様書を作成し、実施設計業者決定後は日田市、九重町とそれぞれの実施設計業者との打ち合わせに参加し、実施設計の監理を行う。
2006年4月～2006年6月	宇佐市　IP電話網構築事業実施設計及び監理業務
	豊の国ハイパーネットワーク上に新設されるＩＰ電話用の専用ＶＬＡＮ上にて運用されるIP電話網の実施設計書、入札仕様書を背う作成。
2006年5月～2006年8月	宇佐市　防災無線統合における基礎調査委託業務
	宇佐市が作成した宇佐、院内、安心院の防災無線統合仕様書の技術内容について調査、およびチェックを実施し、指導を行う。
2007年1月～2007年3月	日田玖珠地区［日田市、九重町、玖珠町］

	2006年度地域イントラネット事業（大分県との共同事業）
	施工完了後に玖珠町の実績報告書を作成し、総務省への対応を代行する。
2007年1月～2007年3月	由布市　情報化基礎調査報告書作成
	新市合併後の情報化基本計画策定に向けた情報化基礎調査報告書を作成。

企業に向けた情報モラル啓発活動について

渡辺律子

1．はじめに

近年、企業活動におけるＩＴの利用は欠かせないものとなっている。「平成１７年通信利用動向調査（総務省）」の結果によると、企業におけるインターネット普及率は、従業員が 300 名以上の企業で 99.1%、従業員が 5 人以上の事業所で 85.7%を占める。またホームページの開設率は、従業員が 300 人以上の企業で、90%～99.1%、従業員が 300 人以下の企業で 83.1%である（図１参照）。

このように、ＩＴは企業においても活動基盤の一つである一方、情報の不適切な取り扱いによって生じる問題も増えつづけており、社会的にも大きな課題となっている。

本研究では、情報社会において、企業がＩＴを活用する際に、やりとりする相手の人権へ配慮し、かつ社会的責任を果たすために必要な考え方や行動である「情報モラル」の普及啓発活動について報告する。

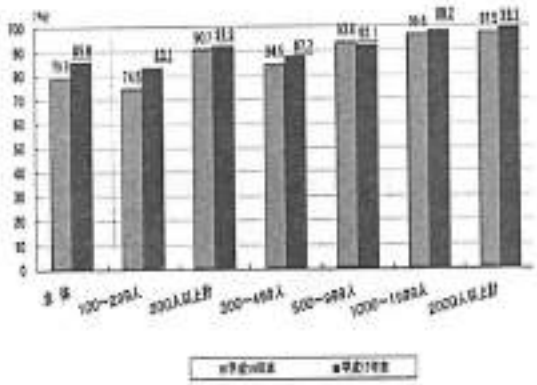


図１　ホームページの開設率（企業）
出典：総務省平成１７年「通信利用動向調査」

2．情報モラル啓発活動の必要性

日々、情報化が進む一方、それに関連する問題も深刻化している。「平成 18 年度のサイバー犯罪の検挙および相談状況について（警察庁）」によると、平成 18 年中のサイバー犯罪（情報技術を利用する犯罪）の検挙件数は 4,425 件で前年(3,161 件)より 40.0%増加している。

企業においても、顧客情報の漏えい、誹謗中傷、名誉毀損などの深刻な被害に遭遇する事例が急増している。インターネットなどＩＴを活用する企業は、常に適切な対応・対策が社会的責任として求められ、そうした対策が不十分な場合は、多大な損害をこうむるだけでなく、最悪の場合は企業の信頼を失い存在自体が危うくなることもありうる。

そのため、情報社会において、企業が積極的に社会的責任を果たし法令違反や人権侵害とならないように行動すべきための、企業の情報モラルの確立が重要であり、これについて普及啓発する必要がある。本研究所では、企業へ向けた情報モラル普及啓発活動を平成 15 年から中小企業庁の委託事業として実施している。

3．普及啓発内容の検討

企業に向けた情報モラルの普及啓発活動として、何を、どのように伝えれば、より効果のある普及啓発が実現できるかについて、主に以下の項目を検討している。

（1）誰に伝えるか

組織の情報モラルを確立するためには、組織のトップが率先して取り組む必要がある。また、より多くの人に伝えるために、情報分野や研修の担当者など、取り組みのリーダーとなりうる存在に伝え、そこから社内全体に広げていくことを期待する。そこで、「情報モラル啓発事業」では、次のような人を対象に、普及啓発を行っている。

・企業の経営者、管理者、実務担当者、企業でインターネットを活用する人
・企業における個人情報保護やセキュリティの取り組みなどの初心者。

特に、中小企業においては、情報に関係した部門などが設置されていない、専門とする担当者がいない、セキュリティ対策などにかける費用が限られていること、などの問題をかかえるケースが多いため、より積極的に働きかける必要があると考える。

（2）何を伝えるか

伝える内容の基本方針は以下のとおりである。

・企業が情報社会で信頼を得る活動を行うために、組織として求められる「情報の適切な取り扱い（情報モラル）」を伝える。
・「今ある問題は何か」、「解決のために何をすべきか」、「どうやって徹底するか」という内容を伝える。

具体的には、次のような要素を内容に盛り込むことで、より分かりやすく伝えることが重要と考える。

○伝えるべき情報モラルとは
○情報社会で起きている問題
○問題がおきる要因とその問題の影響
○情報社会・ＩＴの特徴と社会への影響力
○問題を解決するための対応・対策
・組織としての対策、マネジメントシステム
・技術的な対策
・情報社会に関係した法や規制

なお、伝える内容の基本方針、および伝えたい要素などから、セミナーなどの構成を考える際には、これまでに以下のような切り口によって、検討を進めてきた。

側面1	側面2	側面3
・概論・基本的な心構え ・情報社会における問題点 ・解決のために何をすべきか ・どう実装するか	・組織的対応 ・人的対応 ・法的対応 ・技術的対応	・個人情報保護 ・情報セキュリティ ・電子商取引

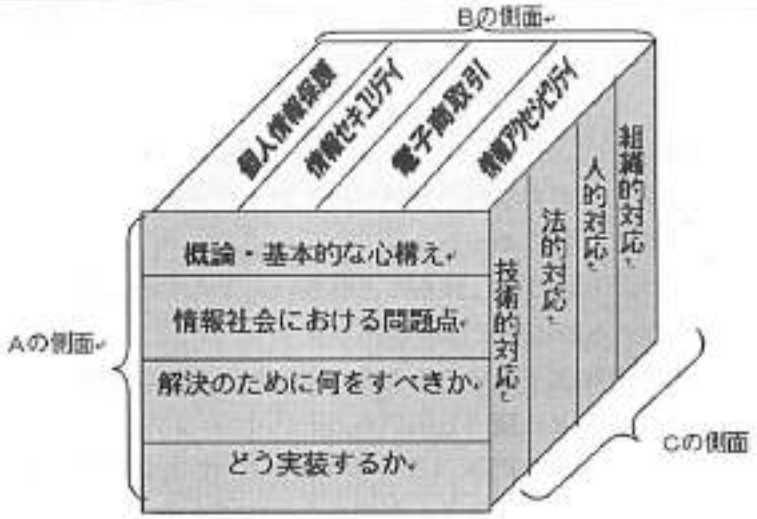


図3　情報モラル普及啓発内容を検討する切り口

（3）どうやって伝えるか

普及啓発の方法を考える際には、伝える内容によって、普及の形式や用いる教材などを検討し、使い分ける必要がある。

＜形式＞

セミナーや講演会などの集合教育と、社内での研修などの分散教育などがある。

①集合型教育：大きな会場などで講演会やセミナー、研究会、ワークショップなどを開催し、講師による講演や、パネラーによるディスカッションなどで、内容を伝える。その際、ビデオなどを利用する場合もある。

②分散型教育：各会社の研修担当者などが、教材を利用して、社内で研修を実施する方法。パンフレットやテキスト、ビデオなどを利用する。

③個別教育：分散型教育の一つになるが、パンフレットなどを使って、社員など一人ひとりが個別に学習を進める形式。近年では、e-learning システムを使って、セキュリティ対策などの学習を個別にする会社も増えてきている。

集合型教育では、よりダイレクトに著名な講師や実体験を持つ講師の話を聞くことができるため、普及啓発教育、特に入門教育などで多く見られる。普段聞くことが出来ないような話や、専門家の立場からの話など聞けることで、参加者の意識啓発が可能となる。デメリットとしては、直接、会場に足を運ぶために、地理的な問題で参加者が限られるということがある。

分散型教育では、各会社・団体の研修などの担当者が、適当な教材を使って、社員に研修を行うも

のである。社内の必要な対象者全員に実施することが可能となり、また会社の状況、対象者のレベルにあわせて、グループ分けし、それにあった内容を考えることができる。そのため、入門教育よりも少し深い内容まで学習することが可能となる。そうした担当者をおいていない場合は、準備に時間がかかるため、状況によっては、外部から専門家を招くなどで対応する場合も多い。

個別教育は、社員一人ひとりが個別に、自分の好きな時間を使って、学習を進めることが可能となる。デメリットとしては、ネットワークを利用して、学習をやりとりするため、システムの機能により、進捗度は把握できても、本当の理解度などについては、把握しづらいところがある。

分散教育・個別教育は、セミナーのように人数を限定しないため、より多くの普及啓発が可能となる。

＜媒体、伝える方法・教材＞

近年は、多方面で普及啓発のための無料の教材が出ており、企業向けの研修などでも利用される場合が多い。例として、以下のようなものがある。

◎ パンフレット：入門教育用として作られることが多い。セミナー会場で配られた後、さらに復習したり、学習を深めたりする際に利用できる。

◎ビデオ映像：伝えたい内容を映像で表現するもの。より現実的に感じることが可能となる。ドラマや解説、ドキュメンタリーなどの演出方法がある。

◎パンフレットのダイジェスト版、要約版（リーフレット）：小さくて持ち歩けるものや見開きの 1 枚から 2 枚程度のタイプで気軽に見ることができるものがある。

◎漫画：初心者にも分かりやすくするために、ストーリーを考え、漫画化したもの。

◎テキスト、書籍：自己学習や担当者が勉強するための教材。より深く学習するもの。

◎チェックシート：社内の取り組みがどの程度達成しているかについて確認するためのチェックシート。テキストなどと併用して使用することも考えられる。

◎広告・掲示物作成

・標語・川柳コンテストなどを行い、優秀な作品を発表するなど。

・ポスター、カレンダーなどの作成し、関係した内容の言葉や文章を掲載し、日ごろ目に着く場所に置くことによって、意識の向上を図る。

◎テレビＣＭ・ラジオ CM：耳や目に印象がのこる音や映像を利用する。

◎テーマ曲の制作：いつでも口ずさめるような歌詞やメロディーのテーマ曲を制作する。

情報モラル普及啓発事業としては、これまでに、セミナーの開催、パンフレットの作成、ビデオの作成により、それぞれの特徴をいかして啓発活動を進めている。

上記内容について検討しながら、平成 15 年度より、セミナーの開催やパンフレットの制作を進めてきた。

４．セミナーの開催

平成 18 年度は、福島、松山、名古屋をセミナー開催地とした。開催地の選定は、人権啓発関係のセミナー開催が少ない東北で 1 箇所、大都市で 1 箇所、その他、地方で 1 箇所、というような条件で候補地をあげ、さらに、協力団体の有無（協力の度合い）、広報活動のしやすさ（人口、企業（事業所）の数、交通の便）などを考慮して決定した。

セミナーの内容・講師の決定については、本報告書の「伝える内容」の検討に加え、基本からより実践に向けた内容が求められていること、参加者により身近なこととして実感してもらうために、日

ごろの業務に関係した話、理論ではなく実体験に基づく話、などのから検討した。その結果として、「ビデオプレゼンテーション＋講演」という形式で、「個人情報保護」「情報セキュリティ」「電子商取引」の方向から企業における情報モラル確立の重要性を伝えることとした。

新たな企画として加えたビデオプレゼンでは、昨年度制作したビデオを上映し、ハイパー研の研究員が企画のポイントや社内教育への効果的な活用法などについて解説した。

また、できるだけ実践に役立つ内容を伝えたいと考え、株式会社ジャパネットたかたや京都府宇治市の実体験をもとにした講演など、社内での取り組みを効果的にすすめるための具体的なヒントとなるような構成にした。

≪Ｈ１８年度情報モラル啓発セミナーの概要≫ テーマ：『情報社会で企業が問われる社会的責任』 個人情報保護、情報ｾｷｭﾘﾃｨ対策の効果的な取り組み（福島・松山） 個人情報保護・情報ｾｷｭﾘﾃｨ・電子商取引を考える（名古屋） 対　象：企業の経営者・管理者・実務担当者、 参加料：無料	＜松山会場＞事前受付　240 名、実参加者 169 名 期日：2006 年 10 月 23 日(月)13:20～17:00 会場：松山全日空ホテル（愛媛県松山市） 「ビデオプレゼン『今、企業に求められる情報モラルとは？』」 ハイパー研：青木、杉井、渡辺 「実体験から語る個人情報保護の取り組み」 関西情報・産業活性化センター　木村修二氏 「企業の信頼確保のためのセキュリティ対策」 独立行政法人情報処理推進機構　加賀谷伸一郎氏
＜福島会場＞事前受付　235 名、実参加者 191 名 期日：2006 年 9 月 15 日(金)13:20～17:00 会場：コラッセふくしま（福島県福島市） 「ビデオプレゼン『今、企業に求められる情報モラルとは？』」 ハイパー研：会津、杉井、渡辺 「『わかる』から『できる』へ －実体験から語る個人情報保護の取り組み」 株式会社ジャパネットたかた　吉田周一氏 「企業の信頼確保のためのセキュリティ対策」 独立行政法人情報処理推進機構　加賀谷伸一郎氏	＜名古屋会場＞事前受付　286 名、実参加者 174 名 期日：2006 年 12 月 15 日(金)13:20～17:00 会場：名古屋国際会議場（愛知県名古屋市） 「ビデオプレゼン『今、企業に求められる情報モラルとは？』」 ハイパー研：会津、杉井、渡辺 「個人情報保護に対する企業の実践的な取り組み」 ネットワンシステムズ株式会社　山崎文明氏 「安心・安全なネットビジネスをめざして」 有限責任中間法人ＥＣネットワーク　沢田登志子

5．パンフレットの作成

①『情報社会に問われる企業の社会的責任』（H16 年度作成、H17、H18 年度増刷）

平成 16 年度にパンフレット『情報社会に問われる企業の社会的責任』を作成した。これは、「企業がインターネットを活用して情報を扱う上での問題とは何か」「それらの問題に対して、社会的責任を果たすために企業はどのような取り組みをすべきか」について、入門教育用としてまとめたものである。それぞれのテーマ（個人情報保護、情報セキュリティ、電子商取引など）の中で、情報モラルに関連した「問題と対応」をとりあげている。

②『人権に配慮した個人情報の取り扱い方－企業に求められる情報モラル実践ガイド』（H18 年度作成）

18 年度に制作したパンフレットは、16 年度に作成したものよりもテーマを絞り、より具体的に取り組みをしめすことを目指し、内容の基本方針を以下のように定めた。

・情報モラル確立の取り組みのうち「個人情報の取り扱い」に限定する。
・「何が問題なのか（誰が、どう困るのか）」を伝える。
・具体的に「何をしなければならないか」という実践事例をとりあげる。
・情報漏えいが生活を脅かすことを書く。
・なぜ、個人情報の取り扱いが人権、社会の公正と関わってくるのか。
・事実の羅列や事件のインパクトだけではなく、なぜ問題なのか、どういう意味を持っているかなどの本質的なことを伝える。
・「誰がどう困るのか」「どういう人権上の問題があるのか」など、できるだけ人権啓発に繋がるような形にする努力をしてみる。
・また、なるべく起きやすそうな問題を取り上げる。

こうした方針から、以下の構成で内容を組み立てた。

○個人情報の取り扱いと人権への配慮（２Ｐ）
○情報モラル取り組み事例（ジャパネットたかたの取り組み事例）（４Ｐ）
○個人情報取り扱い方のポイント　業務の場面に沿って（８Ｐ）
・取得、利用、委託、保管、維持、廃棄・運搬、問合せ、事故

6．ビデオの制作

H17年度に情報モラル普及啓発のためのビデオを制作した。伝えたいことを映像でわかりやすくまとめ、ビデオテープ・CD などに収め、配布するとともに、インターネット上に掲載し、企業関係者のみならず個人ユーザからも参照することを目的とした。

映像化することのメリットとしては、パンフレットで表現できないところが映像で表現することでわかりやすくなる部分もある半面、そのイメージが具体的すぎる場合は、それだけで充分と思われがちなところがあるので注意が必要と考えた。

また、セミナー内容やパンフレットなどとの関連性については、特に、セミナーやパンフレットと合わせて活用するものではなく、ビデオだけ見て、単独で利用できるものとした。利用者は、中小企業の経営者を基本とし、情報モラル・ＩＴに関して初心者層を想定した。

制作に向けては、内容の企画、脚本の制作、ビデオ制作（撮影・編集）の３段階にわけ、それぞれこちらで取り入れたい内容を伝えて、業者を選定した。実際に、脚本コンペを行う前に、ビデオに盛り込みたい要素を検討し（○ページの要素）専門家に脚本化してもらった。

7．活動の成果

（1）セミナー

今回、福島、松山、名古屋で開催したセミナーの参加者は、ある程度、セキュリティや情報モラルの対策に取り組んでいるが、まだ充分に対策できていない現状があるとおもわれる（アンケート結果：「職場にセキュリティ対策や個人情報を保護する委員会などがあるか」の問いに、「ある」が福島７８％、松山６６％、名古屋７０％、「ポリシーを策定しているか」の問いに、「既に策定」が福島７４％、松山６０％、名古屋６８％、これに対し、社員教育をよく行っているのは、福島３６％、松山４２％、名古屋３６％にとどまっているなど）。

こうした参加者に対して、「対策の必要性を感じましたか？」という問いについては、どの会場においても、「対策の必要性を強く感じた」という答えが、７０％を超える結果となった。

図４　対策の必要性を感じましたか（参加者アンケートより）

このほか、『「ビデオ上映+パネラー」という形式はこれまであまり見かけなかったので良かった』『ビデオの企画意図についての話が興味深かった』『実例による講演で分かりやすい。すぐに実践できる。応用できる事例が多い』『モラルは一回で身につくものではないので、こういったセミナーを頑張って続けて欲しい。』などの感想があった。

（2）パンフレットの配布

このパンフレットを 18 年度末までに 23,500 部発行し、セミナー会場で配布するとともに、全国の都道府県や商工会議所などに配布している。また、約 200 社の企業や団体からは、社内研修などでの利用希望があり、まとめて送付している。

パンフレットを送付した企業・団体、６０社に対してアンケートを依頼し、３９団体からの回答を得た。

利用者は、建設業、製造業、情報通信業、金融業、卸売、小売業、教育関係、商工関係団体などで、幅広い業種で活用されていた。また、事業所の規模は、5 人未満の事業所から、300 人以上の企業までで、多いところでは、2 万人の社員を持つ会社での研修もあった。

また、今回、パンフレットを利用した団体において、セキュリティポリシーの策定についてたずねたところ、すでに策定しているところが６１％、また社員教育もよく行っている、少し行っているをあわせると、７９％である。そうした取り組みが全く無いところもあったが、パンフを利用する団体は、初心者から、社内においての情報モラルやセキュリティに対する意識が高い団体まで、幅広く利用されていることがわかった。

また、社員教育の研修会などでの利用が多く、社員や幹部に対して研修を行ったり、自己学習用として配布していた。

パンフの利用目的は、個人情報保護対策がもっとも多く、続いて、「情報モラル全般」「企業の社会的責任」についての利用が多い。

パンフレットについては、「とても参考になった　79%」と高い満足度が得られた。

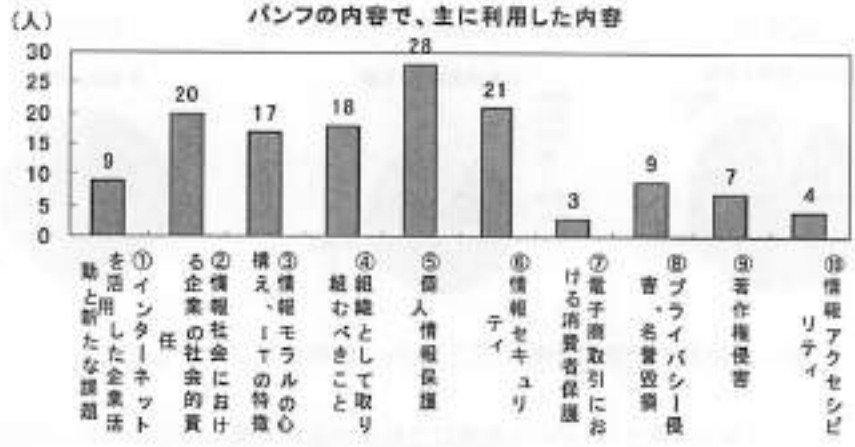


図5　パンフレットの内容の中で、主に利用した内容（複数回答可）。

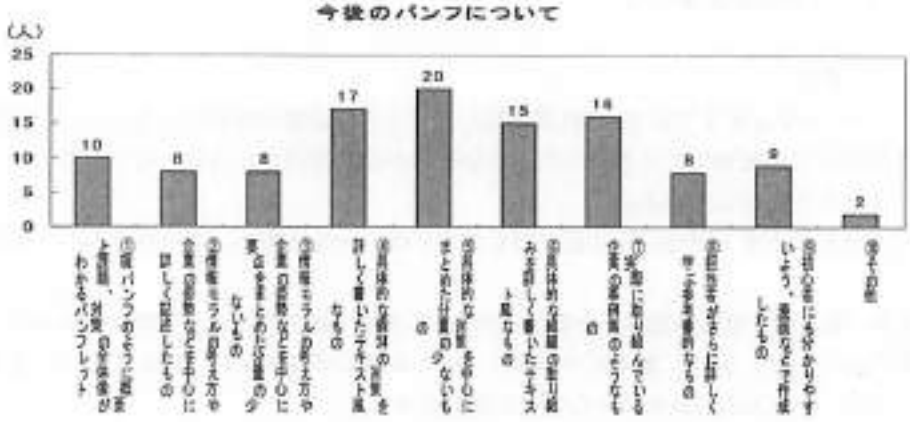


図6　今後のパンフについて取り上げてほしい内容

（3）ビデオ

17 年度に制作した情報モラル啓発ビデオが好評を得ており、18 年度は解説冊子を作成し映像をおさめたＣＤを付けて配布した。ビデオを見る際により理解を深めるよう、またビデオをまだ見ていない人に興味関心を持ってもらうよう、ドラマのポイントとなる場面に解説を加えて仕上げた。9 月に発行後、4ヶ月の間に社内研修などのために利用希望のあった企業・団体が約 100 社あった。

ビデオについては、現在もアンケートを実施中であり、次回の制作に役立てたいと考える。

セミナー会場のアンケートでは、ビデオに対して次のような感想があった。

「初心者にも受け入れやすいと思う。知り合いにも紹介したい。」「非常に分かりやすいビデオでした。」「わかりやすい事例を映像で知ることにより理解しやすかった。また、身近に起こりうる内容だったので、注意すべき点がわかりやすかった。」「零細企業をモデルにしたビデオであったのが良い。今は何ごとも企業間における温度差が大きく、小規模の企業でも情報モラルが必要であることを理解出来るのではと思われる。」「CD で資料をいただいたので、有難い。今後、いろんな場面で参考として使わせていただきます。」「知っている俳優が出ていて、見やすく、分かりやすかった。」

「・講演全体の入口としては適当な内容で分かりやすい。予算が許すのであれば、中級、上級等の作成をいただき、求める者に配布いただけると有り難い。」、半面「・内容が易しく、初心者の企業担当

者には良かったのではないかと思うが、私自身にはあまり役立たなかった。」といった声も少数ではあるがあった。

8．今後の課題

全国各地でのセミナーも 18 年度までに１０箇所の実施となった。毎回のアンケートから参加者企業においても、年々個人情報保護や情報セキュリティ対策が進められていることがうかがえる。しかし「セキュリティポリシーを既に策定」する企業がどの会場でも 60%～70%と増えてきたのに対し、社内教育については、「よく行っている」は 45%に満たないことから、現場でどのように徹底していくかが今後も課題になると思われる。

また、企業に対する情報モラルの普及啓発活動を進める中で、実際に取り組みはじめた企業が参考にできる情報や相談できる窓口の必要性を強く感じた。中小企業などで対策に費用をかけづらい場合、例えば、情報処理推進機構（IPA）の情報セキュリティ対策診断ツールなどの存在は貴重である。

今後の情報モラル普及啓発の在り方としては、以下のようなことも検討が必要と考える。

（1）セミナーと並行した研修講座の開催

・セミナーと並行して、50 人～100 人程度の研修講座を地元の団体と連携して開催する。

・少人数で、ワークショップのような形（議論する）も考えられる。

（2）リーダー研修、育成、資格

・現在は、会社の経営者に向けてセミナーを行っているが、地域情報化センターのようなところにいる中小企業診断士、会計士といったリーダー的な立場の人たちに、情報を提供するような研修会を行う。（人材育成事業、情報モラルリーダー育成事業など）

・そのリーダーが、それぞれの持ち場に帰り、さらに研修を実施していくなどにより、現場の経営者や実務担当者に広げていく。

・企業倫理アドバイザーといった資格のように、情報モラル資格を出してはどうか（中小企業庁が認定）。人材育成研修などを行い、修了証書を出して認定するなど。

（3）情報モラルの取り組み事例の評価

・社内で情報モラルの確立に取り組んだ実践事例集を作成する。

・実践が優秀なところには大賞などあげる。「情報モラル大賞」

・ネット上での商取引などの際にも、情報モラルに関する取り組みがなされているか評価する。

・集めた実践例を「実践事例集」としてまとめ、全国の商工関係団体に配布する。

（4）企業の情報モラルに関するポータルサイトの開設

・中小企業が情報セキュリティ・情報モラルに取り組んでいる具体的な事例を掲載する。

・漏洩事件など、どんな事件がおきているか、問題が起きたときにどこに相談したらよいかなどの情報を掲載。

・セキュリティ対策など、緊急で知らせなければならないことなど、ニュースとして掲載し、注意を呼びかける。

（5）情報モラル e-leaning

・社内などでの情報モラル教育のための e-leaning システムを作成する。

・システムの中に、情報モラルを学習するコンテンツ（教材）を作成する。
・講演の内容をオンデマンドでパワーポイントのスライドと講師の映像を並べて流すことにより、教材として使用する。

研究所としても、日々進展する情報社会において企業に求められる情報モラルを探究しながら、現場のニーズにも応えうる普及啓発活動を継続していきたい。

UPプログラム活動報告（FY07）

青木栄二

UP (Unlimited Potential) プログラムは、その言葉のとおり無限の可能性を秘めて、2003年度から始まった。5年計画のこの事業は4年目を迎えて、当初の目的である、ITを活用する機会が少なかった人たちに対してIT研修を行うことで、情報社会への参加を促し、その恩恵を享受してもらえたのではないかと考えている。これまでの経緯、および詳細な活動内容については、2005年度の当研究所研究報告書を参照していただくということで、今回の報告では、現状動向の把握と今後を展望していきたい。

このプログラムを主催するマイクロソフトは、地域において情報弱者への支援を行っている非営利団体と連携を図り、協働していくことで、地域社会の活性化に貢献しようとしている。当研究所では、従来から地域に立脚して実践的な研究活動を行っており、有志数名で始まったシニアネットなど、各種NPOの立上げやサポートに参画してきた。いまやシニアネットは約500名という会員を持つにいたっている。こうした取組みは、地域社会におけるさまざまな課題へのソリューションの提供という形で現れている。

マイクロソフトの事業年度は、7月から6月までとなっており、FY（Fiscal Year）という表記を用いる。FY07は、2006年7月1日から2007年6月30日までのことで、日本の年度とは違うため、今回は昨年7月から3月までの報告を行う。

◆ 現状動向

◇ 高齢者UP

NPOシニアネット大分と協働している高齢者UPプログラムでは、当初からの目的である、①生涯学習の場の提供、②ITの仕組みや使い方の支援、③生活に密着したITによる生きがい作りへの支援、をかなり達成してきたといえる。

FY07の成果目標と上半期の実績を以下に示す。

種別	項　目	目標(計画)	実　績	差　異
集合講座	研修会場の数	6	6	
	研修コース数	14	15	+1
	受講者数	140	150	+10
	育成した講師数	10	9	
	講師数	10	8	

まさにUPプログラムの主旨が効を奏したことにより、マイクロソフトからの支援をそれほど必要としないまでに自立運営が可能となってきた。シニアネットのなかでは、会員同士がITを通じてコミュニケーションを活発に図って、さまざまな同好会が立ち上がっている。これにより受講者やシニアネットへの入会者が増えて、それぞれの会員がインターネットを利用することのメリットを十分に感じている。

しかし、組織が大きくなることによるマネージメントの問題が持ち上がる。ボランティアの集まりという状態であればよかったものが、活動のひろがりにより役割分担など推進体制の人員を検討するといったことが必要となっている。また、高齢者という枠からみるとシニアネットは、まだその一部であり、受け入れ態勢や相談窓口なども考えていかなければいけない。さらには受講者を募集するためにいかなる広報手段をとっていくのか、そして受講者を満足させるための講師のスキルアップはどうすべきか、講座のコースはどういったものを望まれるか、そのテキストの作成をどうしていくかなど、新たな課題を抱えている。

問題解決にあたっては、以下の方策を実施しているところである。

- 組織内において、担当者選任、実施手順、事務手続きの明確化
- 受講者アンケートによるニーズの把握
- テキスト作成担当者による修正、追記作業の効率化
- 月1回の講師研修の実施
- ホームページの充実、市報やCATVなどメディアの活用、口コミでの紹介

◇ 障がい者UP

NPO障害者UP大分プロジェクトと協働している障がい者UPプログラムは、2005年から2006年にかけて大きく発展した。もともと大分県は、国際車椅子マラソン大会や太陽の家などの雇用など、障がい者に対する取組みが進んでいたため、今回のUPプログラムにおいても積極的な活動となった。

現在、障がい者の自立支援や就労機会獲得のためのIT研修を実施している。障害者施設は県内各所にあり、それら地域との連携、また講師養成のための人材育成が目的である。これからの団体の自立を見据えて、活動はUPプログラムだけにとどまらず、県・市・社会福祉協議会などへの事業の働きかけや民間助成金の申請に努めている。また2006年9月には、NPO会員の福祉情報技術の向上を目指してe-ATの技術研修を行うなど、より実用的な講座を重要としている。

シニアネットと同じく数名で立ち上がった同NPOも、今では100名に迫るほどの会員登録となっており、講師陣も充実してきた。障がい者に教えるということは、健常者に教えるのとは違う技術を要するので、一歩踏み込んだ積極性と責任感を持った人材育成がなされている。

FY07の成果目標と上半期の実績を以下に示す。

項目	年間目標	実績	備考
研修会場の数	19	14	74%
研修コース数	79	29	37%
受講者数	429	162	38%
育成した講師数	82	25	30%

2006年4月に施行された障害者自立支援法では、応益負担の考えに基づき、障がい者個人や施設の経済的な負担が増した。そのため、講座を中止した施設が3箇所あった。継続して受講を希望される場合でも、講座のレベルアップについていけなくなるケースが見られた。

こうした課題に対して有効な手立てを見出せないのが課題でもある。それは組織自体の未熟さであり、受講者にとっていかに魅力のあるテーマやテキストで講座をコーディネートできるかにかかっている。ただマイクロソフトから支援いただいた実用的なソフトウェアの寄贈により、新たな展開を下期では実践していく予定である。

大きな成果として挙げられるのが、7月2日に開催したフォーラムである。

第1回障害者UP大分プロジェクトフォーラムの報告

QOLの向上を目指して

～障害者と共にIT就労を考える～

◇開催　2006年7月2日(日)10:00－16:30

◇場所　大分県総合社会福祉会館

◇主催　特定非営利法人障害者UP大分プロジェクト

◇共催　財団法人ハイパーネットワーク社会研究所／特定非営利活動法人イーパーツ

◇後援　大分県／大分県社会福祉協議会／マイクロソフト株式会社

まず障害者UP大分プロジェクトの津田理事長より開会の挨拶が行われました。またフォーラムに先立って、リユースPCの贈呈式を行いました。これは東京でリユースPC寄贈プログラムを行っているNPOのイーパーツから贈られるものです。県内の3団体に対して、3台のPCが寄贈されました。

つづいて「IT活用で障がい者の自立支援を！」をテーマに、パネルディスカッションを行いました。ここでは障がい者の施設の方々に登壇していただき、障がい者が自立していくためには、いかにITを活用していくべきかなど、現場の取組について議論を交わしました。

(コーディネーター)NPO法人イーパーツ事務局長　会田和弘

(パネリスト)　地域生活支援センター三角ベース　佐藤恵文

社会福祉法人そよかぜ　小規模通所授産施設ひので　藤波志郎

入所授産施設千歳ハイツ・エイブル　首藤敏宣

身体障害者療護施設ハーモニーの森　釘宮定司

身体障害者小規模通所授産施設エバーグリーン　中西玲子

昼食や休憩時間には、各施設からの特産品やてづくりの品々の販売が行われました。ハイツ・エイブルや三角ベース、エバーグリーンからの出店で賑わっていました。

午後からは、「PC講習会で得るもの目指すもの」をテーマとして、第 1 部情報交換会を行いました。以下の方々から、それぞれのテーマに合わせて発表していただきました。

- *授産の向上に向けて「ひだまり工房のあゆみ」 小規模通所授産施設ひので 石橋伸之*
- *社会参加とは さいき未来21 渡辺捷三*
- *パソコンは身体の一部！ 視覚障害者PC講習会講師 松木康司*

つづいて(株)ユーディット「情報のユニバーサルデザイン研究所」の代表である関根千佳氏を招いて、記念講演を開催しました。同氏は各省庁や自治体のユニバーサルデザインに関する委員を多数務めており、第 1 人者と言えます。人間を幸福にできるIT技術とは？誰でもが社会へ参画できるユビキタス時代のユニバーサルデザインについて話をしていただきました。

それから「PC講習会で得るもの目指すもの」をテーマとして、第 2 部情報交換会を行いました。以下の方々から発表をしていただきました。

- *全てが工夫 さぽーとセンター風車 菊池祥江*
- *社会復帰に向かって 入所授産施設千歳ハイツ・エイブル 井野本喜子ほか 3 名*
- *聴覚障害者とともに学んで 聴覚障害者センターPC講習会講師 福盛洋子*

最後に、当研究所の宇津宮所長が閉会挨拶で締めくくりました。

積極的な活動がフォーラム開催へとつながり、大分県福祉協議会や大分市のボランティア協会からの助成を受けるにいたった。テレビなどメディアに取り上げられて、口コミよる勧誘が新規会員増に繋がっている。しかし、一方ではテキスト代など受講者負担の問題が指摘されている。ハードやソフトなどの使用機材の管理と効率化が求められており、テキストなども管理と有効活用が必要である。

◇ 子育て UP

NPO パワーウェーブ日出および津久見市福祉事務所と協働している子育て UP プログラムでは、核家族化に伴って孤立しがちな子育て中のお母さん方を対象に、交流や情報発信、就労に必要な知識や技能のスキルアップ、地域の活性化やコミュニティ活動への参加を促すことを目的として、活動している。

問題は IT 講習などに参加しているときの子供の世話である。これを地域の高齢者が見守り保育、母親クラブにて相互に面倒を見たりすることで解決している。地域の問題は地域で解決するといった根本的なことを実践することで、福祉や社会発展に寄与している。そこから出てくる積極的な人材が新たな活動の輪を広げるといった展開も見られる。

どちらの UP 活動についても共通して言えるのが、官民連携がうまく取れているということだ。NPO パワーウェーブ日出のほうは、日出町と積極的に共同ワークを行い、町の施策の一端を担っている。その取組みについては、新聞等のメディ

アからも数多く取り上げられている。

大分合同新聞（朝刊）　2006年（平成18年）11月5日

2006.11.5

日出町のNPO法人　IT技術習得で社会復帰へ　子育てママを支援

日出町の特定非営利活動法人（NPO法人）「パワーウエーブ日出」（小野町子理事長、約60人）は、「見合い托児」と名付けた相互支援の仕組みを使って子育て中の母親に情報技術（IT）を習得させ、社会復帰につなげる活動を続けている。

同法人に助成しているマイクロソフト社の担当者が1日、視察を訪問し「IT技術の習熟だけでなく、コミュニティーに密着した素晴らしい事例だ」と絶賛。小野理事長は「地域の共生や活性化に役立てたい」と意気込んでいる。

パワーウエーブ日出は昨年9月に発足。「社会貢献UPプログラム」を世界的に進めるマイクロソフト社やハイパーネットワーク社会研究所（大分市）の協力を受け、日出町と共同で独自のパソコン研修を開催。受講者が在宅就労やパソコン講師をできる程度のIT技術を習得している。

同NPOの最大の特長は、研修中の会員の子どもをほかの会員が面倒みる託児制度を取り入れていること。長女（3つ）と二女（1つ）を連れて来た日出町豊岡の主婦、[illegible]さん（31）は「知り合いの会員ばかりなので安心。お母さん同士の結び付きも深くなる」と歓迎している。

研修を経て在宅就労した主婦は4人。小野理事長は「今後は会員に在宅の仕事を回せるように、情報処理会社などへの営業を強めたい」と話している。

＝2006/11/5付 西日本新聞朝刊＝

津久見市福祉事務所では、市内いくつかの母親クラブ NPO やサークルなどと、需要に応じた講座内容を積極的に進めている。ワード、エクセルだけではなく、CAD など実務的なものから、ブログによる情報発信などさまざまである。

FY07 の成果目標と上半期の実績を以下に示す。

項目	年間目標	実績	備考
研修会場の数	3	2	
研修コース数	37	15	
受講者数	370	137	
育成した講師数	60	32	

課題として挙げられるのが、会場や設備の問題である。どこにでもパソコンやプロジェクター備え付けの会場があるわけではなく、都合よくあいているわけでもない。就労技能に向けたより高度な講座であれば、講師との日程調整が難しく、使用するソフトウェアが高価なものとなってしまう。テキストやマニュアルも揃えなければいけない。またせっかく高度な講座を受けても、就労や活躍の場がないため、レベルアップ講座へ臨まないケースも出てきている。

会場の確保に当たっては、市役所や町役場の協力により公的施設の予約配慮や利用しなくなった施設の再利用などで対応している。パソコンやプロジェクター、ソフトウェアについては、イーエルダーなどNPOのリユースパソコン寄贈プログラムやマイクロソフトのUPプログラムの支援を受けているが、十分ではないため、県内でもリユースパソコンの寄贈元を探している状況である。受講者のニーズに合わせて有効な講座を企画していかなければならないので、講師の人材育成やテキストの作成に力を入れている。

いくつかの課題はあるものの、受講者からは多くの感謝の声が挙がっており、メールやホームページ作成によるコミュニケーション、転入後の地域社会との関わり、子育て中の時間の使い方など、主婦の日常生活において役に立っていることが良く分かる。実際に就職後の業務に使えたり、就労の機会に恵まれたりしたこともあった。まさにUnlimited Potentialだといえる。

◇ セキュリティUP

大分におけるそれぞれのUPプログラムをコーディネートしていくうえで、最近の情報セキュリティ問題は日々その重要性を増してきている。そこで、初心者が情報セキュリティにどのように取り組むべきか、分かりやすく教えられるような講師の養成を目的として、当研究所が活動しているものである。

以下がFY07の目標と上期の実績である。

項目	年間目標	実績	備考
研修会場の数	10	2	
研修コース数	3	1	
受講者数	50	19	
育成した講師数	20	15	

年間の予定では、下期に重点を置いており、研修を実施していくものである。その牽引役となる講師を育てる講師（スーパーマスター）には、シニアネットの

中から情報セキュリティに詳しい5名の方々になってもらっている。2005年、スーパーマスター中心にセキュリティ関連情報を整理、講師用テキストを作成した。テキストの内容や情報は随時更新していくものである。

初心者に向けての情報セキュリティ講習にあたっては、マスターと呼ばれる30名の講師が、上記のテキストとイーパーツが作成しているセキュリティシートを利用して教えている。また普及啓発のための講習だけではなく、緊急セキュリティ情報やその対応についての情報伝達を行うようにしている。コンテンツリソースとしては、セキュリティ対策推進協議会の速報サイトを利用している。

情報セキュリティについては、根本的な意識改革が難しい。まず重要な入り口であるセキュリティの必要性をいかに啓発できるかにかかっている。そのため講師であるマスターの意識の持ち方、知識レベルの向上も大きな課題である。いかに安心と信頼のあるコミュニケーションを確立できるかが、セキュリティのサポートには重要なのである。

今後は大分県下あまねく情報セキュリティのレベル向上を行いたいと考えており、マスターの拡大や初心者のニーズ把握のためのアンケートの調査などを企画している。今年度の活動概要を以下に示す。

(1) 活動期間
- *2007年4月～6月*

(2) 体制
- *原案作成：ハイパー研事務局*
- *アドバイザー：情報セキュリティに関する専門家や有識者*
- *企画検討：sec-super@ML*
- *コンテンツ提供：イーパーツ会田氏、スーパーマスター、その他*
- *マスター支援：スーパーマスター（5名）＜シニアネット大分＞*
- *エンドユーザへの普及啓発および情報伝達：マスター（30名）sec-forum@ML ＜シニアネット大分＋障害者UP大分プロジェクト＋パワーウェーブ日出＞*

(3) 目的
- *大分県内の情報セキュリティレベルの向上とセキュリティリスクへの対策*
- *エンドユーザに対する普及啓発や情報伝達についての検証*

(4) 内容

① 情報セキュリティの普及啓発
- *エンドユーザへのパソコン教室などにおけるコンテンツを利用した学習*
  イーパーツ作成シートおよびスーパーマスター作成セキュリティテキスト
  http://www/spread-j/org/sheet/index.html
  http://www/eparts-jp/org/secure_method/index.html
- *コンテンツ利用に関するアドバイスとサポート*
- *インターネット安全教室の活用*

② 緊急セキュリティ情報の伝達
- *Sec-forum@MLへの警報および説明注釈の挿入（スーパーマスター）*
  セキュリティ対策推進協議会のセキュリティ速報
  http://www/spread-j/org/cgi-bin/index/snew.cgi
- *エンドユーザへの警報*
- *警報に関するサポート*

③ 以上の活動に関する検証
- *エンドユーザに対するセキュリティレベルの意識調査（アンケートなど）*

④ 講習会の開催
- *情報セキュリティに関わる人材育成および普及啓発のための講習会の開催*

◆ 今後の展望

◇ ポストUPプログラム

マイクロソフトのUPプログラムは、FY08（2007年7月～2008年6月）を持って終了する。そのため各UP活動は、ポストUPプログラムに備えて、いかに活動を維持していくかの方策を検討していかなければいけない。

シニアネット大分においては、かなり自立できているものの、活動の安定性を求めて財団法人ニューメディア開発協会が進める「シニア情報生活アドバイザー制度」の養成講座実施団体となっている。シニア情報生活アドバイザーとは、高齢者がパソコンやネットワークを利用して、より楽しく、活動的な生活を送れるようになるためのリーダーである。たんにパソコンやネットワークの使い方だけでなく、趣味や社会参加に役立てる方法を教えるものである。

地域のIT講習会のサポートやシニア向け講習会の開催、訪問サポートなどのボランティ活動により、高齢者間に人的なネットワークを広げていくことで、会員の募集につながるのではないだろうか。また、すでに実施している自治体主催の講座への講師の派遣など、自治体との連携事業を進めることも大事である。

ここまで成果を出してきたUPプログラムを、単純に終了するというだけではなく、マイクロソフトには社会貢献プログラムの中長期ビジョンを打ち出して欲しい。情報弱者にとって使っている製品メーカの支援は、大きな問題なのである。そうした次なるプログラムに対して、シニアネットは積極的な参画を果たしていきたいと考えている。

障害者UP大分プロジェクトは、現在のUPプログラムが基礎となってできたNPOであるため、依存度は大きい。今回のプログラムが終了することで、活動の幅が狭まることも十分に考えられるので、その危機感をどう乗り越えるかが焦点となっている。

これまで培ってきた知識とノウハウは、今後大きな力となりえるだろう。とくに相談や指導、そのコーディネートについては、かなりの専門性を持つことができている。2005年からスタートした障害者UPなので、5年間の事業という括りであれば、2009年までの支援を望むところであろうが、ポストUPプログラムを見出していくしか方法がない。

パワーウェーブ日出では、現行活動しているような行政機関との協働事業や委託事業が考えられる。また、ほかのNPOとの連携やマイクロソフトの新しい事業、各種助成金の申請などにも積極的にトライしていきたいところである。今回のプログラムにおいて、「社会の弱者に向けた貢献事業は生きがいへとつながる」といったビ

ジョンを掲げることで、事業運営ということを学ぶことができたのは大きい。

ただ実際の活動にあたっては、利用しているPCやOSの大多数が古く、これからVistaへ移行していくなかで、UPプログラムが終わっても、旧OSのサポート打ち切りについては、何らからの支援を望むものである。ハードソフトにとどまらず、社会弱者への情報化支援は、企業の社会貢献事業として継続されるべきであろう。

◇ これからのヒューマンデジタルデバイド対策にあたって

情報社会が急速に進む韓国では、UPプログラムは国単位で実施されており、受け皿となっているのが、韓国デジタル文化振興院（KADO）という政府機関である。

KADOでは、具体的に以下の3つの活動を行っている。

- 農業者、漁業者、低所得者、高齢者、障がい者を対象に、ITを活用した社会参加や自立支援を目指した研修や講師の養成
- デジタルデバイドに関する調査研究
- インターネット中毒に対するカウンセリングおよびカウンセラーの養成

IT国家を標榜する韓国としては、デジタルデバイドはかなり深刻な文化の問題だと捉えて、国を挙げての支援体制をとっている。

日本において、今後どういった情報弱者対策を実施していくのかは、非常に重要な問題である。韓国のように文化として捉えるのか、経済発展のキーワードとして考えるのか、社会福祉国家建設のための礎とするのか。さまざまな場面や未来予想図を想定するなかで検討、実施していくべきものなのだろう。

高齢者にとってのITは非常に有効であり、その関心の高さとニーズの多様性に応えるためには、高齢者みずからの目が必要である。ただ、積極的に活動されている講師などリーダー的な存在でも、その姿勢や能力には差があり、指導方法など難しい問題がある。ビジネスで行うものとボランティアで実施するものの違いは大きいのかもしれない。でも受講者の希望や悩みを把握して対応していくには、より近い関係が求められることもあるのだ。ということはシニアネット自体が単なるボランティアの集まりではなく、明確な役割を持った組織として、またその役割を果たすスタッフの集まりとして、より充実したものを目指していくべきだろう。

障がい者については、受益者負担を求めにくく、補助金がなければ活動の維持は難しい。直接的な援助以外の方法としては、NPO自体がほかに収益事業を有していれば、その利益部分を障がい者支援に回すといった、組織の中でのやりくりが可能となる。UPプログラムのように5年間のプログラムで活動自体が自立するといった構造になっていない。本来の意味のデバイド解消のための社会貢献とは半永久的な

ものではないだろうか。

地方における経済格差はそのまま情報格差を生む可能性をはらんでいる。さらに社会的な弱者にとっては、なんらかの支援がなければ自律的にこのデバイドを解消する目途は立たないだろう。

障害者自立支援法の施行から、就労への努力が望まれるところである。UP プログラムのおかげで、社会参加については少しずつ成果が見え出してきてはいるものの、就労はまだまだこれからであり、それこそ Unlimited Potential を信じて活動していくものである。

パワーウェーブ日出の活動から見えてきたのは、協働の重要性と、お互いに支えあっていこうという配慮である。子育て中のお母さん方などハンディを抱えた人たちが、社会に対していかにチャレンジしていけるか。活動における苦しさや喜びは、大きな成果を生み出していく。その過程において、受講者や活動している人たちの表情、目の輝きを見ることで分かってきたのは、年齢や環境の格差も乗り越えられるような人との出会いと結びつきが、社会の財産になるのではないかということである。

以前の就労環境と違い、幼稚園に入るまでの子育て期間である 5 年間のブランクでも情報化の世界では変化が激しく、まるでついていけなくなってしまう。UP プログラムのような機会提供は社会全体の底上げにつながるだろう。今後のデバイド解消にあたっての活動では、子育て UP で経験してきたような託児コスト、託児中のリスク回避のための保険など、経済的な対応策も求められる。

デジタルデバイドは、セキュリティの面でも情報弱者を生み出している。そのもっともたるものが初心者である。そのための普及啓発やセキュリティ講師の人材育成は必須となってきた。また、日々新たに生成される脅威に対する緊急情報の伝達も道路情報並みに必要となってくるのではないだろうか。

人材育成においては、教える側と教えられる側の信用できるコミュニケーションが、セキュリティにおいては特に大事な要素となる。地域社会における顔の見える安心感は、セキュリティのレベルアップに確かな役割を果たす。そうしたヒューマンネットワークを県単位ぐらいで運営できるような、情報セキュリティサポートセンターがあれば、情報社会の発展、地域社会の発展に寄与できるものと考える。

防災情報ポータル研究会

薬師寺俊生・石丸忠教・園田和孝

1．はじめに

「平成18年版防災白書」によると、北海道南西沖地震[1]、阪神・淡路大震災[2]が起こった平成5年、及び平成7年を除くと、土砂災害をはじめとした風水害、及び雪害による被害が大きな割合を占めている。

2006年度は、風水害を中心とした自然災害に対応するため、ITを活用した防災関係機関相互、及び住民と防災情報を共有する「防災情報ポータル」を研究する。

2．概要

昨年、主要な防災関係機関を中心として、財団法人ハイパーネットワーク社会研究所の自主研究として開催した「防災情報ネットワーク研究会」の実施内容を踏まえ、今年度の自主研究内容を検討した。その結果、更にテーマを絞り込み、風水害に伴う現場の防災関係機関の負荷軽減や住民への防災情報の提供機能を保有し、インターネットによるWeb参照および入力できる「防災情報ポータル」の研究検討テーマを実現化への高い優先度として認識し、下記の通り実施すべきと判断した。

《2006年度検討する内容》

○「防災情報ポータル」に必要とされる情報項目の定義。

○情報連携のための調整等に係る付帯作業検討。

○基本レイアウトの設計検討。

2－1．目指す方向性

・「防災情報ポータル」は、既存の防災関係機関のシステムを補完できるしくみ。

・防災関係機関が取扱う内部情報の収集と情報共有を可能とするしくみづくり。
（認証等により防災関係機関のみが入力及び情報の参照確認ができる）

・防災関係機関で精査された内容を住民へ提供するしくみ。

・災害発生により住民生活への影響を受けやすい道路情報、交通情報、河川の雨量情報など風水害関連を中心とした情報提供の検討。

2－3．研究会開催により想定される効果

・既に防災のホームページ関連を作成している市町村では、「防災情報ポータル」サイトと連携

---

1 平成5年（1993）7月12日、午後10時17分ころ海道の日本海側にある奥尻島の北西沖を震源とする地震が発生。地震発生のすぐあとから午後11時すぎまでに、北海道から東北、北陸、山陰の日本海側の海岸に津波がおしよせ、震源に近かった奥尻島では、地震直後、高さ20m以上もある津波が発生した。

2 平成7年（1995）年1月17日（火）午前5時46分発生、震央地名：淡路島、震源の深さ：16km 、規模：マグニチュード7.3。

する事により、更新作業負荷の軽減が図れる。
・今後、防災のホームページを構築する予定としている市町村では、「防災情報ポータル」リンクへ行う事により、住民に提供する防災関係情報システムの構築費用も軽減される。
・県と市町村の情報共有ツール(画像データ、テスキトデータ)として活用できる。
・他関係機関の既設の Web カメラや観光カメラの動画情報等を取り込む事で、既存設備の有効利用ができる。
・豊の国ハイパーネットワークと地域インフラの更なる有効活用ができる。
・防災関係者で精査した情報をタイムリーに住民に公開できる。
・情報の一元化により、住民から必要な情報を即アクセスできる。
・ポータルサイトを立ち上げることにより、住民の防災意識を向上させる。

3．開催期間

平成 18 年 10 月～平成 19 年 3 月

4．参加者

①大分県生活環境部防災危機管理課
②大分県生活環境部消防保安室
③大分県企画振興部 IT 推進課
④大分県警察本部警備部警備二課
⑤大分県警察本部交通部交通規制課
⑥大分県土木建築部　（担当課は、内容により随時出席）
⑦大分市消防局消防指令課
⑧臼杵市総務部総務課防災管財広報グループ
⑨株式会社アセンディア（ポータル技術支援）
⑩有限会社システム・エイド（GIS 技術、情報セキュリティ、ポータル技術支援）
⑪（財）ハイパーネットワーク社会研究所

（順序不同、敬称略）

5．内容

初回の研究会開催では、財団法人ハイパーネットワーク社会研究所 所長 宇津宮孝一より、防災情報ポータル研究会開催の挨拶をおこなった。続いて、趣旨説明と参加者全員の自己紹介が行われた。本研究会を開催するにあたり、検討素材として参考になる他県の防災ポータルサイト等を事前調査することから行った。その結果、検索用語の「防災ポータル」又は「防災ポータル情報」と入力して検索すると、常に上位にランキングされているポータルである。A県の防災ポータルサイトを参考にすることにした。

A県のポータルサイトの主な特徴として、

パソコンの画面を意識して、1画面（1024×768 の PC モニタ解像度）に収まるよう工夫されており、アイコン等でリンク先のイメージが分かりやすいようになっている。ポータルの動きとして、例えばリンク集をクリックするとA県だけでなく、他の防災関係機関が管理するページへのリンクも集約しており、まさにポータル（＝入り口）[3]となっている。リンク集の中でA県が提供しているシステム（例：道路情報提供システム）を見ると、GIS[4]を頻繁に使用しており、可視化を重視している。

リンク集の中にはライブカメラ映像もリンクしている。カメラの位置を地図と連動させて、見たい映像を容易に操作できるよう、利用者の視点で工夫されている。

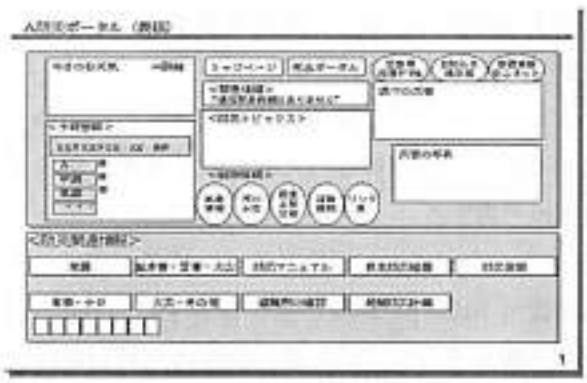
A県と同様にカメラの利用は、B市でも、災害時以外の平常時でも、交通渋滞などの利用として、住民からの Web アクセス利用が繁盛あった。

県レベルの比較として、A県と大分県を比較した。大分県の安全・安心ホームページの情報量は豊富であり、充実している。ただし、目的のページを探すのにA県のホームページより、やや階層が深いように思われる。

このコンテンツを階層が深くならないよう注意しながらできるだけ既存の情報にアクセスし易くすることが必要と感じた。

地図情報の利用は GIS メーカー、無料ツール各社の特徴もあり、GIS を活用した情報をポータルに取込むインターフェイス技術も含め検討する時期だと思われる。

〈A県防災ポータルサイト〉



（研究会　検討風景）

A県の GIS 情報推進化状況の説明を受け、「防災情報ポータル」の利用面のイメージ化を図るため、参加者によるブレーンストーミング[5]（以下、ブレスト）を実施した。

---

3 インターネットの入り口となる Web サイト。

4 地理情報システム（GIS：Geographic Information System）は、地理的位置を手がかりに、位置に関する情報を持ったデータ（空間データ）を総合的に管理・加工し、視覚的に表示し、高度な分析や迅速な判断を可能にする技術。

5 brainstorming / ブレスト　集団（小グループ）によるアイデア発想法の1つで、会議の参加メンバー各自が自由奔放にアイデアを出し合い、互いの発想の質さを利用して、連想を行うことによってさらに多数のアイデアを生み出そうという集団思考法・発想法のこと。省略して、「ブレスト」「BS」などともいう。

（ブレスト風景）

（討議資料）

その結果、「防災情報ポータル」の利用面としての検討案（抜粋）であるが、以下に記載する。

＜「防災情報ポータル」の利用面としての検討案（抜粋）＞

1. 災害弱者[6]を支援する人々に的確な情報を伝達する方法（“日頃の備え方”、“災害発生時の行動の方法”、“避難行動の手順”等）としての利用する。
2. 報道関係者への、災害情報の定期的な情報配信、及び県と市町村との共同記者会見方式等を組み合わせた現場の負荷軽減策の推進をする。
3. 防災関係者間の情報交換では未公開情報も含んでいるため、利用者のレベルに合わせた情報セキュリティの認証を考慮する。
4. 既存の防災システムにも災害状況に応じた有益な情報がある。映像関連などの入力された情報が可能となるように、既存システムとの情報連携を検討する。
5. 情報伝達の光ケーブルが断線していないという前提で、「防災情報ポータル」を考察している。そのため、災害地域が広域に、災害規模が大規模になった場合は、劣悪な環境下でも情報の伝達可能な防災無線との併用運用は考慮する。
6. B市では消防通信室から直接CATV会社、東京の共同通信、出版社等にも情報を提供している。また、情報の検索もマウスクリック回数4回以内で情報が探せるように工夫している。C市では、平成16年度までは放送局に専用線を導入していたが、平成16年度以降は、CATVへ災害発生時からリアルタイムでの情報連絡を伝達できるようになっている。大分県はCATV普及率も高く、CATVとの情報連携をする。
7. 平成19年4月以降に販売される携帯電話はどのメーカでもGPS機能を保有しており、発信場所の特定ができる。そのため、情報提供源の確認、救助、救援の位置確認に役立てる。
8. 将来、費用を投入し、開発されるであろう「防災情報ポータル」を陳腐化しないためにも、情報を発信、収集する双方向の機能を充実した運用を想定する。情報収集ではメール

---

6 災害が発生した場合、安全な場所への避難行動や避難場所での生活において大きな困難が生じ、まわりの人の手助けを必要とする人たち。例えば、移動が困難な人、車いす、補助器などの補装具を必要とする人、情報を入手したり、発信したりすることが困難な人、急激な状況の変化に対応が困難な人、薬や医療装置が常に必要な人、精神的に不安定になりやすい人等。

や掲示板など想定されるが、誹謗中傷や誤情報には充分配慮が必要である。情報提供者には、大分県警察本部の「まもメール」のように最初に基本情報の登録として氏名（及びニックネーム）、住所、電話番号などを登録条件として利用すること等が必要である。

9. ＦＡＸ利用は、緊急性を要する状況下で、手書きなどによる操作性が高い。また、受信側も物理的に目視できる人的手段のほうが、誰でも操作できるため、かえって効率的であり、情報が端末のディスク内に誤って埋没するおそれがない。

10. 今後、災害による迂回路や規制解除連絡などの映像や情報などが充実してくると、客観的に利用者が判断することができ、生活面での活用に効果がある。

第１回～4回までの前半部分の研究会では、現状の情報処理の流れを確認した。確認された内容をマインドマップツール JUDE/Think[7]というソフトウェアを活用して、サイトマップ的に構造ツリーを作成して整理した。更に、その構造ツリーを基に、ポータル作成用のイメージ及び概観を PowerPoint で作成した。

実際の Web イメージでポータルを共有認識するため、無償ツール” XOOPS”[8]を使い、暫定版の「防災情報ポータル」として作成し、意見交換を行った。

＜暫定版「防災情報ポータル」についての主な意見＞

シンプルなポータルで良い。ただし行政関係のホームページは文字量が多いため、図やロゴなどによる情報発信源の表示による効率的な表現が望ましい。

ライブカメラへのリンクについては一覧表ではなく、大分県の地図のように、地図上の場所の特定、地図上で特定された場所の災害映像状況とグラフなどの数値情報との連携など、一貫性がある形態が望ましい。

障がい者等への弱者支援対策としてアクセシビリティ[9]機能を取り入れるようにして、情報の周知徹底を可能とする。

ポータルにおけるリンクが広範、多岐に渡っているので緊急時に混乱しないように、緊急時には、周知したい大事な情報が、目立つように表示されるようにサイトマップを随時、切り替えできるような工夫も必要である。また、女性の意見を積極的に取り入れ、ボタンや表示される色では、ポータルサイトの選択ボタンを“押したくなるようなデザイン”に変更するなどポータルの表現をやさしくする。

---

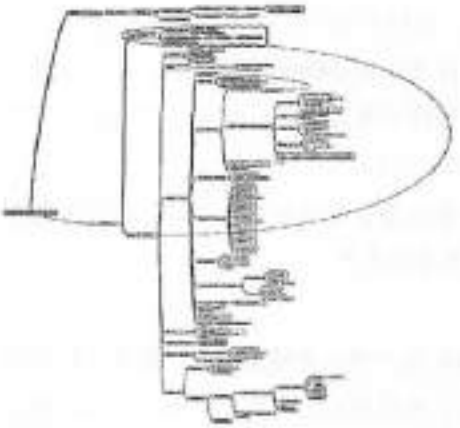
7 マインドマップは 1960 年代にトニー・ブザン氏が発案した独特のノート法。脳の記憶の仕組みに沿ったというその記法は、発想・思考支援ツールとして注目を浴びている。「JUDE/Think!」はマインドマップが描画できるツールとして開発された。

8 XOOPS はヤフーや CNET のようなポータルサイト(コミュニティサイト)を個人でも手軽に立ち上げることのできるソフト。XOOPS はオープンソースライセンスである GPL(GNU 一般公有使用許諾書)に基づいて開発されたソフトで、ソフトウェア部分では一切の費用がかからない。

9 高齢者や障害者などハンディを持つ人にとって、どの程度利用しやすいかという意味で使われることが多い。例えば、手や腕の障害のためにマウスを使えない場合、ソフトウェアはキーボードだけで利用可能である必要がある。弱視や老眼の人にとってはフォントサイズや配色は容易にカスタマイズ可能でなくては見にくい。視覚障害の人は読み上げソフトを使うので、それに適したレイアウトや記述方法が求められる。特に、Web ページについての「利用のしやすさ」を「Web アクセシビリティ」という。これについては「WCAG」(Web Content Accessibility Guidelines)という指針が W3C によって提唱されている。

（防災情報ポータル構造（案））　　（防災情報ポータル概観図(検討用)）

)



第５回以降開催の中盤における研究会では、これまで開催した研究会内容を振り返るとともに、昨年実施した「防災情報ネットワーク研究会」より顕在化した①被災地の避難地域から防災関係機関への情報発信。②平常時にも利用できるネットワークづくりと防災バックアップ。③GIS の必要性と既存システムとの情報連携の 3 点の課題を出発点として今回の研究会が実施されたことや新たな課題や、課題に対する対応案を再確認した。

（課題）

□他県における防災ポータルを参考にして・・・。

① 災害状況を伝えるためには写真等の画像による“災害現場の見える化”が最も適していることが分かった。ただし、対象物への写真だけでは場所の特定が難しいため、ある程度、位置を特定できる目標物と一緒に撮るような配慮が必要である。

② GPS 機能付き携帯電話のイメージが研究会参加者メンバーで理解できた。

③ 一般携帯電話の電波が届かない場所に対して、衛星携帯[10]、衛星電話[11]、衛星専用線[12]等の活用を検討している自治体所もあるが、運用コストが高価であるため、導入が進んでいない。

④ 画像などを公開する場合、どこまで公開情報として出せるのかを判断するのが難しい。例えば、防災カメラで人の顔が見えてしまう場合、肖像権の関係からマスキング対策が

10 世界中どこからでも繋がる携帯電話。通話だけでなくメールもできる。

11 衛星通信システムを利用した電話機であり、通信手段のない地域から通話やメール、ホームページ閲覧などを行うことが可能。衛星電話は海外通信インフラを経由するため、電話回線の混雑時などでも通話ができる。

12 定額制の衛星回線サービス（VSAT 端末やインマルサット専用線）がある。VSAT（ブイサット）［Very Small Aperture Terminal］の略で超小型地球局とも呼ばれ、その名の示すとおり双方向衛星通信のための小型の送受信設備。アンテナの直径は 60～120cm 程度である。VSAT 同士の通信の場合、親局（ハブ局）を経由して情報をやりとりするのが一般的ですが、最近ではハブレス（親局を経由しない）で通信できる VSAT も使われている。インマルサット衛星専用線には 128kbps と 64kbps の通信速度の異なる 2 種類のサービスがある。10 台のパソコンを接続して料金を気にしないウェブページ閲覧、メール、通話、FAX 等ができる。また、インマルサット衛星専用線から国際専用線に接続し、日本国内に設置されたサーバーへアクセスすることもできる。

必要。

⑤ 現場からインターネットを介して、防災ポータルの内部情報にアクセスすることは、情報の混乱など、発生後の影響リスクを考慮した場合、好ましくないと判断した。

（研究風景）

（他県の防災ポータルサイト）

次に既存のコンテンツと新たに作成する防災情報ポータルとのあり方について検討した。公開情報の前段階として、情報を整理する場面、公開すべき情報の精査や利用者の関心度や利用頻度などと照らし合わせながら分析し、「防災情報ポータル」の内容が利用者にとって有益な情報となっているかなど、情報を支える体制と役割を考えなければならないことの重要性を認識した。

特に災害地からの情報には、手書き等アナログ情報も含まれており、情報の整理、分析、精査、確定などには、多くの人的作業に関わる要員が必要である。また、災害規模に応じて、防災関係者以外の応援も考慮しなければならない。

「防災情報ポータル」を立ち上げる場合は、利用者に対してフレッシュな情報をいち早く伝達することであり、既存ポータルの見直しや、他ポータルとの融合などシステムの維持・管理するための保全チームが必要である。

開発・運用面においては、携帯電話との連携など、Web 技術、情報セキュリティ対策、データベース管理など IT 分野の専門知識を要するため、該当職員が行うよりも、IT 専門機関に外部委託することもコストや品質保持を考慮して想定することが必要である

情報セキュリティの観点から、大分県の認証基準がイントラの中でどのようになっているのか、内容の確認をした。ただし、どのような手段や方式の認証かは、情報システムにより異なるため、今回は、大きな方向性の確認にとどめた。

災害発生時にポータル利用者が具体的に欲しい情報の１つとして、道路情報がある。道路情報は道路に関する法律である「道路法」に基づき、高速自動車国道、一般国道、都道府県道、市町村道の四種類における路線の指定及び認定、管理方法、費用負担区分等が定められている。利用者からの立場を考えれば、どこか１箇所の Web で参照リンクが設定され、全ての道路情報が参照できれば良いと考えるが、現状では、一部の道路で若干の相互リンクがある。

将来、道路情報と地図情報の利用面を考えた場合、大分県の地図情報と地図上のアイコンを組み合わせ、クリックすると画像を表示することが利用者にとって分かりやすいとの指摘があった

ため、Google Earth を使用して実際に作成し、検証した。

（無償ソフト Google Earth を使用した写真のマッピング例）

新しい防災情報ポータルの内容を検討するに当り、既存のコンテンツの有効利用も含め、ハードウェアよりもコンテンツ内容を重視して考察することが研究会参加者で再確認した。

実際のポータル画面では、複数の階層が１つの画面に表示されることになる。

ライフライン・公共交通機関情報には、検討された表に記載されている以外にも、「ガス」、「水道」、「石油」、「船舶」、「飛行機」の情報がある。

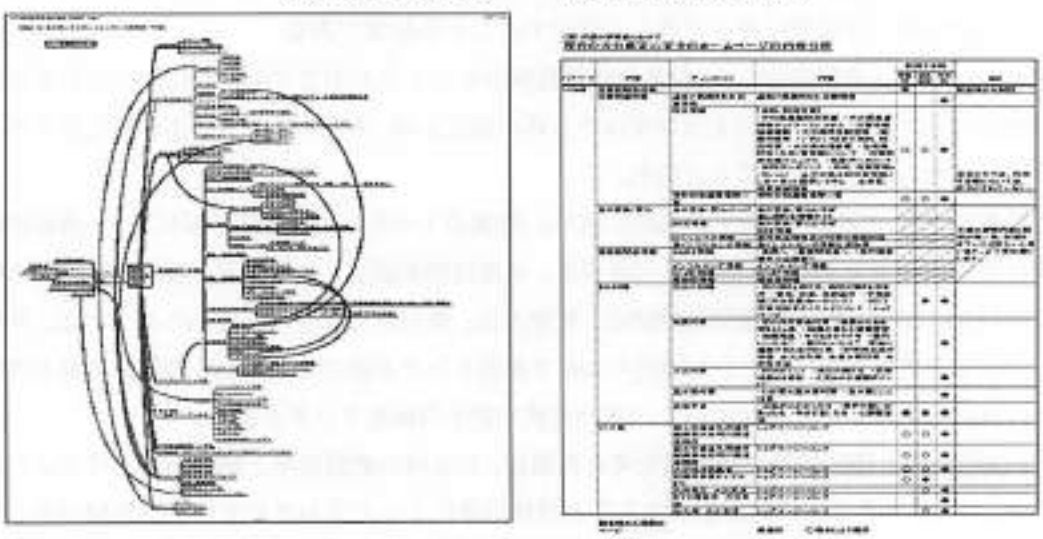
また、警察情報には「まもメール」という携帯電話を使用した、地域の安心・安全に関する情報を配信するサービスがある。

したがって、防犯という枠組みに含むか否かは別途協議する必要がある。

災害用伝言ダイヤル１７１通話は、利用者の立場から、他キャリア各社（NTT ドコモ／Au／ソフトバンク）へのリンクが必要である。

固定／携帯を含め、複数の選択肢があるため、家族間など連絡を取るグループ間でどのページの何の情報を参照して、どうやって避難するのかなど話し合っておく必要があるかもしれない。

（検討後の構造ツリー・構造化詳細等抜粋例）



昨年の「防災情報ネットワーク研究会」実施の資料であるが、阪神・淡路島大震災の事例を参考にして、被災後の被災証明、被災者証明[13]を住民が取得するしくみを紹介した。被災制度は各市町村別に個別制度の部分が多く、「防災情報ポータル」とリンクする場合は、居住区の市町村ポータルへ誘導する方法が良い。防災関連データ情報の階層としては、以下のような考察ポイント5点を抽出した。

①＜災害時協力団体&個人階層＞

現在のところ、防災ボランティア活動団体を想定されていないが、他県では、防災知識を保有し、住民の自助努力をサポートするボランティアの体制を確立する動きがあったため、項目を設定した。

②＜地図情報の階層＞

Google Earthなどの無料の地図ソフトを使用し、避難地域をマッピングさせた情報をレイヤー毎に重ね合わせ、利用者への利便性を図る。

③＜データベース階層＞

過去に発表された災害情報を蓄積する。普賢岳などのデータベース情報は、現在、内閣府で報告書を作成中であるが、大分県でも由布岳、鶴見岳があるため、参考になる。

④＜ライブカメラリンク集の階層＞

年々、ライブカメラ設置箇所は増加しており、昨年作成したライブカメラ集一覧表を更新した。ライブカメラ映像リンク階層では、地図情報とのリンクを考察した。例えば、マッピングした天気予報図とGoogle Earthを重ね合わせる工夫などを検討した。

⑤＜防災知識の階層＞

平常時、災害時、緊急時等のイベントに応じた防災マニュアルを整備することが必要である。また、利用者自身が必要事項（血液型、連絡先等）を印刷して情報を記入し、その紙を携帯しておく等。モバイルの階層ではQRコードなどを利用し、利便性を追及する。

研究会後半では、「防災情報ポータル」のコンテンツ項目を検討してきた。トップページの機能には、検索情報、障がい者の方々に配慮したバリアフリー機能、重要な項目の表示を随時表示、緊急投稿、My防災マニュアル等が分類されるようにした。

7．おわりに

住民のために最も早く防災情報を公開するにはどうしたら良いだろうか？という視点から、今年度の自主研究として「防災情報ポータル研究会」を発足した。

近年の情報公開という流れに対して、「住民が何を、どんな時に知りたいと思っているのか」

---

13 被災者証明書は発災当時、居住していた住宅の被災状況を示すもの、自己所有建物の登記、登記事項証明書取得、税、融資等一般的な目的に使用。また、被災証明書は、事業所（自己所有事業所）、賃貸住宅（貸し主）の被災状況、または、被災者でない（被災当時市外居住者）方の持ち家の被災状況を示すもので、税、融資、登記に使用。発行対象者は発災当時の持ち主で、発災当時の持ち主である事を証明する書類が必要となる。（出典：豊岡市 http://rescuenow.cocolog-nifty.com/typhoon23/2004/11/post_6.html）

「情報を提供する側として、どんな有益な情報を提供できるのか」というすりあわせをする中で、研究会参加メンバーの自由闊達な意見交換ができ、お互いの業務について理解できたことは今回の研究成果の一つではないだろうか。

防災対策の確立にはこれまで「公助」のみがクローズアップされてきた、今後は「自助」、「共助」を含めた適切な役割分担が重要である。特に「自助」、「共助」の面については適切な情報を提供することで住民の防災意識の向上が図れていくと思われる。

本研究会ではポータルを軸として様々な研究討論を行ってきた。住民が安全・安心のために情報を共有し、自らができることを実践することに意義があるのではないかと思う。

発行

財団法人　ハイパーネットワーク社会研究所

〒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

電話　097-537-8180　FAX 097-537-8820

E-mail：post@hyper.or.jp　HP：http：//www.hyper.or.jp/