研　究　報　告　書

２００８年度

財団法人ハイパーネットワーク社会研究所

巻頭言

雲の彼方へ

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

子供時代に，「雲の中はどうなっているのだろうか，雲の上と下はどう違うのだろうか，雲の彼方には何があるのだろうか」など，小さな心は想像に膨れたものである。クラウドコンピューティングという概念が，２００６年にGoogle CEOのエリック・シュミット氏により提唱された。グリッドコンピューティング，ユーティリティコンピューティング，ＳａａＳ(Software as a Service)等の単なる言い換えであるなど，さまざまな定義が自らの主張を喧伝するためになされている感さえする。しかし，インターネットを従来，雲形(cloud)で表し，実体を隠すようにした発想は，むしろ急速に進展する仮想世界を想起させ，妙を得ている気もする。１９９０年代にサン・マイクロシステムズ社の標語「The network is a Computer」が，同社の技術者でもあったシュミット氏の頭のなかにあり，Web2.0のあちら側にあるネットワーク基盤をサービス環境として捨象化したものであるとしたら，「古い革袋に新たな酒を注いだ奥深い概念」なのかも知れない。

大学卒業後，大学の計算機センターでシステムの運用管理と利用者サービスに関わっていた者として，当時のＴＳＳ(Time Sharing System)は，高価なメインフレームを多くの利用者が自分のコンピュータであるかのごとく占有して使用できることに驚いた。その後の計算環境の進展は，「メインフレームからパソコン」へ，「集中から分散」へ，「システム中心から利用者中心」へ，「所有から利用」へ，「見えるものから見えないもの」へと移ってきた。これらのパラダイムシフトのなかで，情報セキュリティの確保，グローバル資源の共有化と融通，ITのグリーン化の必要性が新たに大きな問題を投げかけている。「自律・分散・協調」と「善意」を元に発展してきたインターネットでは，これを使って力任せに大きな蜘蛛の巣が張れる者が隆盛を極めている。インターネットの商用化とともに，悪意を排除したり，新たな垣根を設けたり，バラバラにしたものを再び集中させる急速な動きは，ネット社会が人間社会の歴史をたどっているようで興味深い。

クラウドコンピューティングの本質は何なのか？利用者を場所や機器から解放し，どこからでも継ぎ目なく（シームレスに）ＩＴ資源を利用できるということならば，ユビキタスの概念の域を出ない。情報化投資を抑制するために，ＩＴ資源を所有せず，システム管理負担を増やさず，安全性と利便性を両立するためにサービスを借りるのであれば，オープンソースと仮想化技術導入のデータセンターとどう違うのか。客のサービス量や負荷変動に応じてＩＴ資源をクラウド内部で融通し合う拡張性ゆえ，自前より安価に高度なサービスが受けられるという。しかし，利用が集中した際に回避をするには，提供側はピーク負荷に即応できるＩＴ資源を集中配置するか，グリッドコンピューティングのように高度な負荷分散処理をするしかない。データストレージに預けるので情報流出は防止できると言われるが，保管場所（国）の制約を現行法は求めていないのか，セキュリティポリシは合意できるのか。経験上，２４時間３６５日の安定運用は容易でない。サービスの突然停止時に，誰がその修復に駆けつけられるのか。業務・機器・ソフトを標準化・共通仕様化して集約すれば投資収益率は上がり，運用コストは下がる。しかし，利用者側の

リスク分散や自己防衛が図られなければ，群れが環境変化や病気で全滅するように，大きな危険に曝されないのか。自らの手で触り(hands-on)，反応を確かめ，よりよいものに進化させたいと考えている者には，その制御権や自律性をクラウドに剥奪されては，利用技術は停滞しないのか。

本研究所に，「ネットワーク基盤のハイパーな社会」の研究所だと思って問合せがある。クラウドコンピューティングは，地球（リアル）と雲の彼方（ヴァーチャル）を継ぎ目なくつなぎ，ハイパー社会を創造する概念なのか，一過性のセンセーショナルな新語なのか，バラ色雲となるのか暗雲となるのか，周囲の動きはあまりにも慌ただしいが，定着にはまだ時間が必要な気がする。

こうしたさらなる仮想化の進展，環境を重視したＩＴ化の推進の新潮流も念頭に置いて，本報告書にまとめられた２００８年度の研究所の活動を振り返ってみる。ハイパーネットワーク２００９ワークショップは，「今、問われる情報モラルとガバナンス － 地域で取り組む『情報公害（ネットいじめ、人権侵害、犯罪誘発・・・）』」というテーマで実施した。別府のホテルに高校生から７０代のネット利用者まで１００名近い参加者が集い，国内およびインターネット先進国韓国からの著名なスピーカが講演し，参加者を交えてネットワーク社会で現実になった「情報公害」「地域での問題解決の取組み」等について活発な議論がなされた。「携帯中毒とも思える現象」「プロフへの無防備な書込み」など高校生の赤裸々な告白やそれでいて意外な健全性に聴衆は驚かされた。この様子はネット上のニュースでも取り上げられ大きな反響を呼んだ。これらの実態は，子どもは大人と同じ権利をもたないが，現実社会への対応の育成には大人並の権利や自由を「道具」として試行錯誤しながら行使する必要があるという「権利の道具理論」を想起させられた。

情報セキュリティに関しては，普及啓発活動やセキュリティ対策推進の枠組みづくりを継続した活動が実を結び，２００９年度に「おおいたネットあんしんセンター」の開設につながった。情報モラル啓発セミナーについては，２００８年度は，前年度に続き，全国５箇所（神戸，津，札幌，鶴岡，宮崎）で実施した。２００９年度も中小企業庁公募事業として採択され継続される。

地域情報化については，「大分県における自治体ＥＡ調査研究」の委託研究および「次期豊の国ハイパーネットワーク機器構成調査・検討」の公募事業を実施し，県内の情報インフラについてハード，ソフト両面からのあり方を提案した。また，防災や危機管理に関しては，総務省九州通信局の「九州広域での危機管理体制確立のための情報通信プラットフォーム構築に関する調査研究」に参画し，実証実験および周知啓発イベントを実施し，ネットワーク利用による県域を越えた連携と縦割組織に横串を入れることの重要性を今更ながら痛感した。デジタルデバイドに関しては，総務省の「衛星ブロードバンド基盤整備に係る標準化モデル構築」に加わり，衛星がブロードバンドゼロ地域解消への最後の切り札として活用されるための残された課題に取り組んだ。オープンソースソフトウエア（ＯＳＳ）については，大分県ＯＳＳ研究会活動を通じて，ＯＳＳの普及啓発と地域ＩＴ企業への普及促進活動を継続している。２００９年度に県のＩＴ推進課が情報政策課に衣替えをするので，ＯＳＳ活動も地域全体への新たな展開が期待できる。

２００９年度は，ハイパーネットワーク２００９別府湾会議に加え，これまでの活動の延長として，ブロードバンドゼロ地域を解消するための方策の具現，住民主体の情報ネットワークのあり方や利活用の検討，ＯＳＳ活用による人材育成と産業振興，ネットワーク社会に顕在化してきた諸問題の解決の仕組みづくりなどインターネットガバナンスの調査研究や地域情報化の推進を通じて，環境を重視したハイパーネットワーク社会の構築による真に豊かな人間社会の実現を目指して努力を続けたい。変化の激しい社会にあって，「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，今後も持続できるように皆様方のご支援・ご協力が引き続き必要である。

【目　　次】

サイバーセキュリティ調査　エストニア事例研究

ハイパーネットワーク社会研究所
副所長　会津　泉
iza@anr.org

はじめに　サイバー攻撃への国家の関与

サイバー空間における紛争は、リアル世界における対立、紛争を反映して発生するということはほぼ自明といえるだろう。これまでにも、国際社会における実際の戦争や紛争、あるいは緊張関係の高まりによって、愛国的ハッカーたちが相手国のサイバー空間を攻撃し、報復合戦が繰り返されるといった事態はしばしば観察されてきた。それらのいくつかの事例をあげると、以下のようになる。

・旧ユーゴスラビア連邦解体に伴う地域紛争（セルビア、クロアチア、ボスニアなど）
・コソボ紛争に伴う、NATOのユーゴスラビア爆撃
・アラブとイスラエルの対立
・靖国神社参拝や教科書問題などによる日中韓の対立
・インドネシアとマレーシアとの紛争
・インドとパキスタンとの対立

2001年、米国への同時多発テロ事件のあと、安全保障の専門家からは「アルカイダなどのテロ集団がサイバーテロを行う可能性が高まった」、「電子真珠湾攻撃が発生する可能性がある」などとする警告が続いた。しかし、実際には爆弾などによる物理的なテロ事件は各地で多発したが、サイバーテロとしてとくに顕著なものは起きないまま数年が経過した。

このため、2006年頃にはとくに米国の安全保障の専門家などの間では、イラク戦争など地上戦へのIT技術の応用に関心が集中する一方、「サイバーテロが起きる可能性はきわめて低い」というのが大勢となっていた。

しかし、最近、こうした見方は再び変わりつつある。国家機関なども関与した本格的なサイバー攻撃の可能性、脅威が現実的に存在するという見方が増大している。

この変化を引き起こした要因としては、とくに最近は以下のイベントがあげられるだろう。

1) 2007年頃から頻発する欧米各国政府機関システムへの不正侵入
2) 2007年4月から5月に発生したエストニアに対する大規模なサイバー攻撃
3) 2008年6月に発生したリトアニア政府サイトへのサイバー攻撃（ウェブ書き換え）
4) 2008年8月に発生したジョージア政府サイトへのサイバー攻撃

この他、一般のメディアでも繰り返し報道された、中国人民解放軍による欧米政府各国や軍機関、さらに一般企業のシステムへの不正侵入、機密情報漏洩などの事件が、「情報戦争」として警戒されるようになったことも、大きな要因となったと考えられる。[1]

同時に、各国ともインターネットや携帯電話などを経由して、社会的にオープンに利用される情報通信システム・サービスが広く浸透し、それらの「重要情報インフラ」上に構築されている「サイバ

[1] http://www.yomiuri.co.jp/net/feature/20070927nt09.htm

一空間」がもつ社会的機能、政治的重要性、安全保障上の依存度が、従来よりはるかに高まってきたことも、サイバー攻撃を脅威として受け止める立場の増加を推進する大きな要因となっているといえるだろう。

2008年11月、エストニアをはじめバルト三国などの欧州諸国を訪問したが、国による強弱の差はあれ、国家組織が関与するサイバー攻撃の脅威に対する警戒感は全体として上昇していたことは明らかであった。同時に、国家・政府および国際社会として、そうした脅威をどのように抑止できるか、決定的な事態となるのをどう回避するかといった政策上の問題意識も育っていることがうかがわれた。

また、12月には米国ワシントンを訪問して安全保障および情報セキュリティの専門家らに面談・取材したが、彼らの多くも、数年前とは異なり、サイバーテロないしサイバー戦争の脅威を現実のものとして認めるべきだという立場に立っていた。2009年1月に就任したオバマ大統領による米国新政権も、サイバーセキュリティについての政策的な取り組みを強化するだろうという期待を受けていた。

これらのサイバー攻撃に、ロシアなどの国家機関あるいは軍事機関が直接関与していたとの明確な実証は、少なくとも現時点までにはなされておらず、関与はないとする立場と、程度の差はあれなんらかの形での関与があったという両者の立場が並立している。

ただし、上述のように、各国政府や関係者の間に、そうした事態への警戒感が強まっていること事態は否定できない事実であり、政策的な影響は明確に存在し、深化しているといえる。

わが国も、北方領土問題では、ロシアと直接の「紛争」ないし政治課題を抱えている。その帰結のいかんによっては、なんらかの形でのサイバー攻撃が発生してもまったく不思議ではない。

かりに技術的な意味では、攻撃のレベルが低ければ、さしたる影響を受けずにすませることも、現状では十分可能であろう。しかし、技術の進化はしばしば非連続的に起き、予想外の事態が発生することもありえないわけではない。その意味では、ロシアや中国を中心に発生してきた「サイバー攻撃」から読むとるべき教訓は、けっして小さいものではないと思われる。

エストニアへのサイバー攻撃

エストニアへのサイバー攻撃　調査テーマの設定

2007年4月から5月にかけて発生したエストニアへの大規模なサイバー攻撃は、一国の情報資源全体を対象としたという範囲の広さと、断続的ではあるが数週間にわたって継続したという期間の長さにおいて、前例のない突出したものだったといえる。

同時に、この攻撃を実行した主体が実際に誰なのか、自然発生的なものなのか、それとも組織的なものなのかという点でも、ロシアの政府機関による組織的関与の可能性が疑われ、もしそれが事実であるとすれば、一国の公的機関がサイバー攻撃を本格的に実行した史上初の事件となり、国際社会でも注目された。

かりに政府機関が実行に関与していたとなれば、国際社会においてそのような行為にどう対処すべきか、それは「軍事」ないし「戦争」行為に属すものとみなすべきか、対抗措置はどのようにとるべきか、などなど、政治的、法的、外交的、軍事的な数々の疑問や課題が浮上することになる。

こうした問題は、もちろん理論上の問題としてはこれまでも専門家の間で議論されてこなかったわ

けではない。しかし、「可能性の問題」として議論することと、実際に発生した問題について議論することでは、質的にまったく次元が異なるといえる。

この点について、エストニアなどバルト三国への訪問の前にヒアリングした内外のCERTなどの関係者の間では、

「ロシア政府であれ、軍などの組織であれば、実際にエストニアへのサイバー攻撃に関与したという確実な証拠はどこにも存在していない。たしかな根拠もなくロシア政府が関与したというような発言、憶測は慎むべきだ」とする意見が大勢を占めていた。

「サイバー攻撃の技術的レベルは低く、たいした被害は出なかった。ロシアの圧力を訴えたいエストニア政府やNATOなどの過剰反応だ」

といった見方もあった。[2]

また、ロシア政府は繰り返し、以下のようにその関与を全面的に否定していた。

「エストニアを攻撃したDDoS攻撃の元となるIPアドレスは世界中に存在していたことがわかっている。なぜロシアだけを疑うのか。言いがかりに過ぎない」、と。

たしかに、BOTなどを巧妙に使えば、世界中のサイトからDDoS攻撃を仕掛けることは十分可能である。IPアドレスを偽装するなどの手法を使い、攻撃の大元を隠蔽することも難しいことではない。したがって、技術的な意味で攻撃源を特定することはほとんど不可能といってよい。

こうしたことから、本調査においては、エストニアへのサイバー攻撃に果たしてロシア政府機関が何らかの形で関与していたのかについて、確たる実証を得ることは当初より想定しなかった。

しかし、たとえ実証を得ることは無理だとしても、実際に攻撃を受けたエストニア側の当事者が、現時点でどのように総括しているのか、それを政策的にどうフォローしているのか、今後にどのような備えをとろうとしているのか、といった点を中心に調査・整理することによって、間接的にではあれ、事態の一端が浮かびあがり、かつわが国における同種の課題に対する対応を検討する上での貴重な参考になるものと想定された。

同様に、エストニアへの攻撃が欧米諸国の政策にどのような影響があったのかという点も、重要な課題と思われる。

エストニアの地理・歴史・政治的背景

エストニアへのサイバー攻撃について理解するためには、エストニアの置かれた地理的、歴史的および政治的な背景となる事実を知っておくことはきわめて重要である。

エストニアは、ヨーロッパ北部、バルト海の北端に位置し、面積は4万5千平方キロと九州よりやや広いぐらいで、人口134万人の独立国家である。東はロシアに、南はラトビアに直接接し、北はバルト海をはさんでフィンランドに、西はおなじくスウェーデンに向き合っている。

民族構成としては、フィン・ウゴル系のエストニア人が65%、ロシア人が28%で、残りはベラルーシ人、フィン人、その他である。

エストニアはラトビア、リトアニアとともに「バルト三国」と呼ばれるが、この3国は言語・文化的には相互に独立しており、明確な政治的同盟関係にあるわけではない。ただし、ソ連からの独立時には連携して行動し、以来友好関係にある。

---

[2] http://blog.wired.com/defense/2007/06/substancefree_c.html

歴史的には、10世紀までに独立した言語をもつエストニア民族が形成されたが、中世からはドイツ騎士団、デンマーク、ポーランド、スウェーデン、ロシアなどの周辺する諸国に繰り返し侵略された複雑な歴史をもっている。

1917年のロシア革命を契機に、エストニアは近代国家として独立を宣言し、ソ連をはじめ、国際社会によって承認された。しかし、第二次世界大戦の進展に伴い、ナチス・ドイツによるポーランド侵攻を受けて、スターリン率いるソ連によって、1940年6月にラトビア、リトアニアとともにソ連軍に侵入され、8月にはソ連に強制的に併合された。

ソ連は、その後抵抗するエストニア人らを大量に処刑するとともに、シベリアの収容所にも多数追放し、多くはそこで死亡している。

米国をはじめ西側諸国などの国際社会はソ連の併合を承認しなかったが、第二次大戦終了後、ソ連はエストニアを再併合し、リトアニア、ラトビアなどとともに15の共和国の一つとした。抵抗する人々はシベリアなどの強制連行される一方で、ロシア人、ベラルーシ人などの多数がエストニアに移住し、支配的地位に就いていった。

1980年代後半、ソ連に改革の波が訪れたことに伴いバルト三国には民主化、独立の気運が高まり、1989年に3国の首都であるタリン、リガ、ビリニュスを結ぶ「人間の鎖」運動に100万人が参加、翌年にはバルト三国首脳が集り、事実上の独立回復を宣言した。ソ連のゴルバチョフ大統領はこれを承認しなかったが、ソ連邦崩壊に伴い、91年9月にはソ連も独立を承認し、国連にも加盟するなど、独立国としての地位を確立し、2004年には北大西洋条約機構（NATO）および欧州連合（EU）への加盟を実現し、現在に至っている。

エストニア略史

年　月	
1219年	デンマーク人が進出し、タリン市を築く。
1346年	ドイツ騎士団が進出し、領有。
1629年	スウェーデン領となる。
1721年	北方戦争の結果ロシア領となる。
1918年	独立を宣言。
1920年	ソ連と平和条約を締結。
1940年	ソ連に編入。
1990年5月	独立回復宣言。
1991年 9月6日	ソ連国家評議会がバルト三共和国の国家独立に関する決定を採択。
2004年3月	NATO加盟
2004年5月	EU加盟

出典：外務省ホームページ　http://www.mofa.go.jp/Mofaj/area/estonia/data.html

独立に伴って、それまで支配的地位にあったロシア人の多くは本国に帰還したが、エストニアに残って定住したロシア系住民も多く、現在も人口の約4分の１を占めている。

彼らの多くはソ連時代に労働力として移住させられた人々で、現在はエストニア人中心の新体制のなかで「二流市民」として扱われ、経済的にも貧しい層が多く、不満は蓄積していた。

政府は1940年以降にエストニアに移住してきた人々はすべて、エストニア語と歴史についての試験に合格しなければ市民権を与えないと決定した。その結果、ロシア系少数住民は、政治的な意見を表

明することさえ困難な立場に置かれることになったのである。

かつての支配層であるロシア系住民に対するエストニア人側の反感の強さは想像に難くないが、残されたロシア系住民の側にも怒りの根拠はあった。

本調査でも、「エストニアは一方的に被害者としての立場を宣伝しているが、実際にはエストニア政府を含めて、ロシア系住民への社会的差別はひどいものがあり、むしろそこに問題の原因がある。サイバー攻撃云々というのは的違いだ」との意見を聞いた。

もちろん、サイバー攻撃は、それ自体が原因であるような問題ではないという意味では、この意見は一面の真実を写しているということは否定できなくはない。しかし、「国内紛争」としてそうした対立が起きているということと、国境を超えて、オンラインで政府機関やその他の社会的なインフラに対してサイバー攻撃が起きることとは、質的に異なる面があることもまた事実である。

本稿は、エストニアとロシアのいずれが正しいのか、どちらを支持するのか、といった政治的な意見の表明ないし分析を意図するものではない。どのような立場であれ、互いに対立する勢力が衝突する際に、「サイバー」の要素が無視できないものとなりつつあるということを、情報社会の特徴としてとらえ、その帰結、対応法を検討しようというのが基本的な趣旨である。

電子化の高度の普及：もう一つの背景

エストニアへのサイバー攻撃をめぐる背景として重要なもう一つの要素は、エストニアが1991年の独立以来の新たな国づくりのなかでIT利用を積極的に推進し、インターネットの普及をはじめ、全国民への電子IDカード配布、電子政府サービス、オンラインバンキングなどのICT利用が高度に発達普及しており、現在ではヨーロッパおよび世界でもっとも電子化が進んだ国の一つとなっているという事実である。

議会の選挙にもすでにオンライン投票が導入されている。通常の、紙による投票と並立している。国民議会の採決でも、議事堂には議員一人ひとりの席に電子投票用のボタンが用意され、日常的に利用されているという。

国連機関であるUNDESAによる「2008年国連グローバル電子政府準備化調査」では、エストニアは192カ国中13位と上位に位置している。

この調査は、各国政府の電子政府サービスの提供・利用状況について、ウェブ上のサービス機能、アクセス手段の普及状況、識字・教育など人的資源の状況の３分野を複合評価したもので、国によるICT活用全般を評価する指標と考えることができる。

2008年のランキングでは、エストニアは日本よりやや下だが、この表には出ていないドイツ（22位）やシンガポール（23位）をも上回っている。

E-Government Readiness Index 2008

順位	国名	2008年 指数
1	Sweden	0.9157
2	Denmark	0.9134
3	Norway	0.8921
4	United States	0.8644
5	Netherlands	0.8631
6	Republic of Korea	0.8317
7	Canada	0.8172
8	Australia	0.8108
9	France	0.8038
10	United Kingdom	0.7872
11	Japan	0.7703
12	Switzerland	0.7626
13	**Estonia**	**0.7600**
14	Luxembourg	0.7512
15	Finland	0.7488
16	Austria	0.7428
17	Israel	0.7393
18	New Zealand	0.7392
19	Ireland	0.7296
20	Spain	0.7228

（出典『UN E-Government Survey 2008』）[3]

アクセスに限っていえば、世界銀行の2006年発表の調査データによれば、電話普及率は、固定回線で人口比40.4%、携帯が123.6%である。インターネットの普及率は人口の56.6%で、2000年の28.6%からほぼ倍増した。パソコンは100人あたり48.3台、テレビの世帯普及率は93%に達している。[4]

学校、公共機関でのインターネット接続率は100%、所得税のオンライン申告率82%という数字を達成している。

IT産業も発達を続けている。スカイプの本社はエストニアにある。無線LANも浸透し、主なカフェやショッピングモールなどでは無料の無線アクセスが当たり前にように使える。

こうして、エストニアは、国民生活全般におけるITやインターネットへの社会的な依存度はきわめて高く、政府も通信ネットワークを重要インフラに位置づけていた。またサイバー攻撃が発生する可能性も想定されていたという。しかし、実際に起きたサイバー攻撃は、そうした想定を上回るものだった。この点については、政府による想定が楽観的過ぎたとの指摘は妥当であろう。ただし、それも「結果論」ということは免れない。

[3] unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf

[4] http://devdata.worldbank.org/ict/est_ict.pdf

エストニアへのサイバー攻撃の経緯

ソ連兵士の銅像移転が契機に

2007年4月に始まったエストニアに対するサイバー攻撃の直接の端緒は、第二次大戦の終結を記念し、犠牲となったソ連赤軍兵士を顕彰する銅像を、エストニア政府が首都タリンの中心部から町はずれに移動しようとしたことにあった。

ただし、この銅像の移転は、エストニア政府が一方的に行ったというよりも、以下に述べるような流れを受けてのことであった。

もともとこのソ連兵士の銅像は、エストニアの首都タリン中心部のトゥニスマギ公園に1947年に設置された。ソ連支配時代に、ナチス・ドイツへの戦勝を祝して建てたものである。ただし、エストニアがソ連から独立した後最近までは、ロシア系住民の間でも、主に高齢者が訪れるところで、一般にはさほど注目されるものではなかったという。

ところが、近年になって、旧ソ連の復活を願う勢力によってロシア系住民の間にパンフレットが配布され、ソ連の戦勝記念日である5月9日に、あるいは結婚式や子供の幼稚園入園といった人生の節目のときに、この銅像の前で歴史を振り返る会合や儀式が行われるようになり、この銅像を象徴とする政治運動が組織されるようになったという。背後になんらかの勢力による政治的な意図が読み取れるという。

彼らにとっては、ソ連軍はナチスからエストニアを解放してくれた象徴である。一方、エストニア人にとっては、ソ連軍こそはソ連による長年の支配の源泉であり、ソ連兵士の銅像は忌まわしい記憶の象徴である。したがって、愛国的なエストニア人の間にロシア系住民のこうした政治的な動きへの反発が高まり、5月9日には双方のグループが銅像の前に集って小競り合いを繰り返すといったことが、ここ数年続くようになった。警察は兵士の像の周囲に掲げられたエストニア国旗を撤去するなど、双方の対立の緩和に努めたという。

タリン郊外に移設されたソ連兵士の銅像と、それが置かれている戦没兵士の墓地

首都タリンの市内中心部にあったこの銅像は、その下にソ連軍兵士の12名の遺体が埋葬された墓でもあった。そこで政府は、兵士の鎮魂を静かに祈れるようにするためには、銅像を含めて郊外の戦没兵士の墓地に移動させることが必要だとして、2006年に移転を決定して発表した。この発表に対しては、ロシア政府や議会が反発し、ファシズム復活をたくらむものだといった非難声明が発表され、緊張が高まる事態となった。

こうしたなか、2007年4月26日夜、約1000人のロシア系の住民が銅像周辺に集まり、道路の自動車に放火し、周囲の商店のウィンドウを割り、商品を略奪するなどの暴動となった。これによりロシア系住民一人が死亡、40名ほどの負傷者と約300名の逮捕者が出た。独立後のエストニアでロシア系住民による物理的な暴動は初めてのことだった。

この暴動を受けて、政府は当初5月に予定していた銅像の移設を、市民の安全を守るためにと、急遽前倒しで実施した。

物理的な暴動は4月28日に終息したが、サイバー攻撃はその後も断続的に発生した。

なお、暴動から一年後の2008年5月のソ連戦勝記念日に、移転されたソ連兵士の銅像の前に再びロシア系住民たちが集るものと注目されたが、予期に反してそうした動きはほとんど見られなかったという。CERT関係者によれば、これはまさに前年までのロシア系住民の動きは明らかに人為的に呼びかけられて起きたことを示すもので、今年はそうした組織的働きかけが何らかの理由で行われなかったため、数年前までと同様の静穏な状況に戻ったという。

筆者も同兵士の記念像のある場所を訪れたが、いくらかの献花は見受けられたものの、訪問者はだれも見られず、静謐そのものの状況であった。

サイバー攻撃の経緯

上記のCERTによる文書によれば、エストニアの政府をはじめとするさまざまなウェブサイトに対するサイバー攻撃は4月27日夜22時半頃から始まり、5月18日まで断続的に続いた。[5]

一連の政治的な動きのなかで、4月中旬には「5月9日のソ連の戦勝記念日にサイバー攻撃を仕掛ける」との予告ないし呼びかけがなされており、CERTなどの関係者はある程度は予期していたという。しかし、4月末に、銅像移転とほぼ同時に攻撃が起きるとは予想しておらず、5月9日がターゲットと考えていたようである。攻撃の規模も、予想よりは大きなものであったという。ただし、終了時期は予想より早かった。CERTなどでは、半年から一年続く可能性まで予期していた。

4月27日に開始された最初の攻撃では、大統領府、首相府、内務省、外務省、経済省、議会、警察、主要政党などのウェブサイトが攻撃された。これらの攻撃はDOS攻撃とウェブサイトのコンテンツの不正書き換えが主であった。

電話回線用のシステムが攻撃され、救急車や警察の緊急通報システムがダウンしたという噂もあったが、それは真実ではないようだ。

エストニアでは法律によって政府機関の職員のメールアドレスは一般に公開されることが義務付けられており、そうしたアドレス宛に「お前の家族に危害を加える」というような脅迫メールも送ら

---

[5] 一部には、4月26日夜から攻撃が開始されたという記述もある。

れてきた。

ウェブの書き換えの例としては、攻撃の初日、4月27日主要政党のサイトに「銅像移転が中止された」といった偽のニュース情報が掲載されたり、ヒトラーの写真が掲載されるといったものがあった。

時間の経過とともに攻撃のターゲットは拡大ないし変更され、財務省、環境省、農業省など上記以外の政府機関のサイトや新聞社のニュースサイトが攻撃を受け、さらに30日には主要インターネット・サービスプロバイダー（ISP）にも攻撃が加えられた。

これらの攻撃は、エストニア政府のオンライン・サービスや主要メディアの機能を停止させることで市民の信頼を損なうことが主な目的だったとみられる。

フィンランドに本社のあるF-Secure社は、4月28日にエストニア政府の主なサイトへのアクセスを試み、以下のようなデータを取得し、ネット上で即時公表した。ただし、この時点で、政府機関のサイトがすべてアクセス不可能でとなったわけではない。

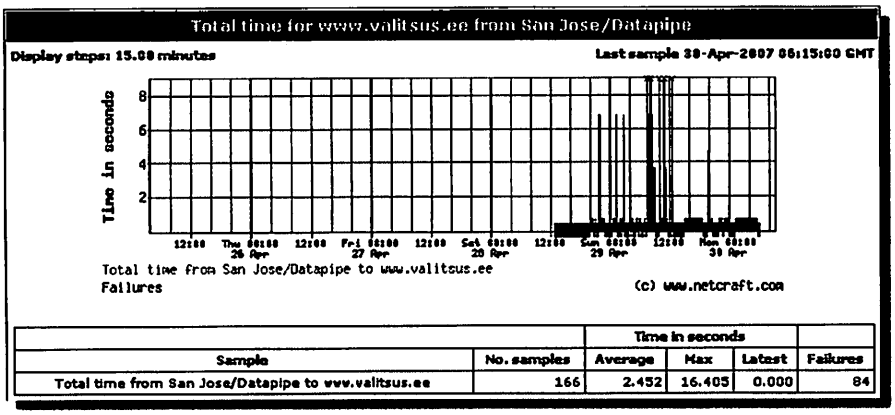
エストニア政府サイトの接続状況　2007年4月28日

Here's the status as we saw it on Saturday at 15:00 GMT:

www.peaminister.ee (Website of the prime minister): unreachable
www.reform.ee (Party of the prime minister): reachable
www.agri.ee (Ministry of Agriculture): reachable
www.kul.ee (Ministry of Culture): reachable
www.mod.gov.ee (Ministry of Defence): reachable
www.mkm.ee (Ministry of Economic Affairs and Communications): unreachable
www.fin.ee (Ministry of Finance): reachable
www.sisemin.gov.ee (Ministry of Internal Affairs): unreachable
www.just.ee (Ministry of Justice): reachable
www.sm.ee (Ministry of Social Affairs): reachable
www.envir.ee (Ministry of the Environment): reachable
www.vm.ee (Ministry of Foreign Affairs): unreachable
www.pol.ee (Estonian Police): reachable
www.valitsus.ee (Estonian Government): unreachable
www.riigikogu.ee (Estonian Parliament): unreachable

以下のグラフは、同じくF-Secure社が公表したもので、4月30日時点におけるエストニア政府全体の公式ポータルサイト"Vabariigi Valitsus"　www.valitsus.ee　の接続状況を示したもので、赤い部分が接続不可能と観測されたものである。

エストニア政府公式ポータルの接続状況　2007年4月30日



		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from San Jose/Datapipe to www.valitsus.ee	166	2.452	16.405	0.000	84

エストニアCERTによる「Overview of the Cyber attacks 'against Estonia」と題する文書では、27日から29日までの最初の３日間を「フェーズ１」、4月30日から5月18日までを「フェーズ2」として、2段階に分けられると分析している。

フェーズ１は、ソ連兵士の銅像移設に対する「感情的な反応」とされ、攻撃の大半はエストニア政府のウェブサーバーと民間の新聞社などのニュースポータルに対する比較的単純なDOS攻撃であった。この間、ニュースポータルの多くがアクセス不能となった。その他、ウェブの内容の書き換え（ディフェースメント）が行われたサイトもいくつか存在していた。

一方、フェーズ2は「メイン攻撃」とされ、攻撃に使われた手法がより高度で、大規模なBOTネットによる組織的に連携した攻撃が行われたという。そのなかでもっとも危険度が高かったのが、重要な国家情報インフラに対する分散DOS攻撃（DDoSアタック）だったとされる。これらのDDoS攻撃のうちのいくつかは一時的には効果をあげた。たとえば、エストニアの二大銀行のインターネット・サイトが大量かつ執拗なDDoS攻撃にさらされ、うち一行はほぼ二日間、それぞれ数時間にわたってオンライン・サービスが利用できない状態が続いた。

また、インターネット・サービスプロバイダー（ISP）の主要ルータに対する攻撃も行われ、短時間ではあったが、政府のインターネットを利用したコミュニケーションに障害を発生させた。さらに、政府サイトへの大規模なDDoS攻撃も組織され、いくつかは一時的に機能が停止させられた。エストニアのccTLDのDNSサーバーも攻撃を受けたが、防御ができており、たいした障害は発生しなかったという。

これらの攻撃はいわゆるBOTを使って巧妙に仕掛けられたものも多く、発生源の特定は不可能に近かった。攻撃の大半がエストニア国外からのものであったこともあり、インターネットの国際回線とのゲートウェイでトラフィックを制限することで、国内のトラフィックの確保が実現された。しかし、その後には国内のコンピューターにも多数のBOTが仕掛けられ、攻撃が行われたという。ただし、上記CERT文書によれば、主要なデータベース、サービスその他の機能が大きな障害に見舞われたことはなかったとされる。

攻撃の手口は、主として以下の3つの方式だったという。まず、もっとも単純なスクリプト・キディを使う方法で、ロシア語のチャットルームで4月27日の銅像移転に対する抗議の一環として呼びかけられ、個々人に対してエストニアのウェブサイトに Ping 攻撃を仕掛けるものだった。同じ手法は一週間後にもチャットルームに登場し、5月9日のソ連の戦勝記念日を前に広く用いられ、ロシア

やエストニア領内のロシア系愛国主義的ユーザーに、「エストニア政府に反対なら、君もインターネットで彼らを懲らしめることができる」といったメッセージが数多く飛び交ったという。

次に使われたのがボットネットで、インターネット上にゾンビを仕掛け、その侵入を受けた何十万台ものコンピューターが指定されたアドレスへの大量アクセスによるDOS攻撃を自動的に繰り返し行う、分散DOS攻撃である。

3つ目の手口は、特定のウェブサイトに不正侵入し、そのコンテンツを書き換えてしまうものだ。これにはSQLインジェクションが多用され、成功したものだ。ただし、重要なホストのデータに対して不正侵入、改ざん、盗み出しを行って成功したものはなかったという。

このほか、スパムも大量に発生した。

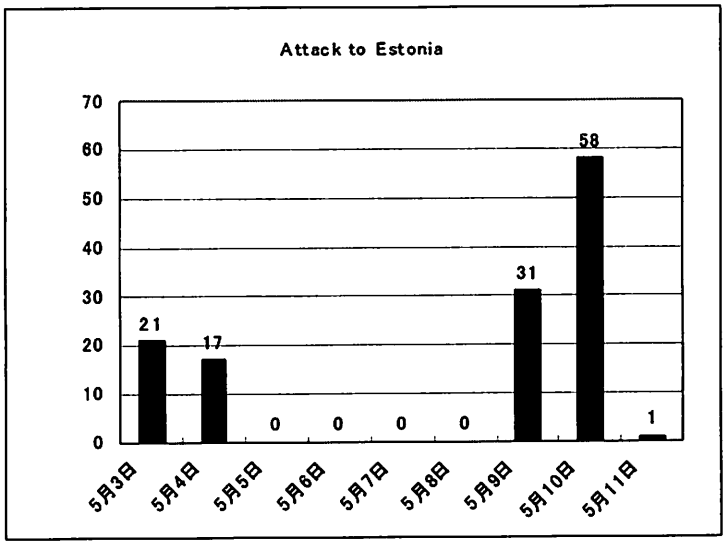
彼らの攻撃は、いわゆるブルートフォース攻撃と称されるものが主で、自分たちの主張を誇示し、かつエストニア側のサイトの信用を失墜させ、面倒と不快感を与える狙いのものだったと、エストニア側の関係者は受け止めている。これらの攻撃は、とくにロシア語によるフォーラム、チャットルームなどで、繰り返し教唆され、扇動されて発生したという。手動での攻撃については、攻撃対象となるサイトのアドレスが公表されていった。

またボットネットによる攻撃でも、次々に異なる対象が選択され、背後に巧妙な組織的動きが存在していたものと推定されている。

物理的な暴動は4月28日でほぼ沈静化したが、オンラインでの攻撃は5月に入ってからも断続的に発生し、エスカレートしていった。この事実も、サイバー攻撃が単なる自然発生的なものでなく、背後に組織的な動きがあったことを示唆するとエストニアの関係者は指摘する。

エストニアへのサイバー攻撃は、前述のように、5月9日のソ連の第二次大戦戦勝記念日に集中することが予測されていた。事実、5月9日から10日にかけて攻撃はピークに達したが、関係者の予測に反して、その後攻撃は一気に減少し、5月18日を最後に収束した。

エストニアへのDoS攻撃の回数

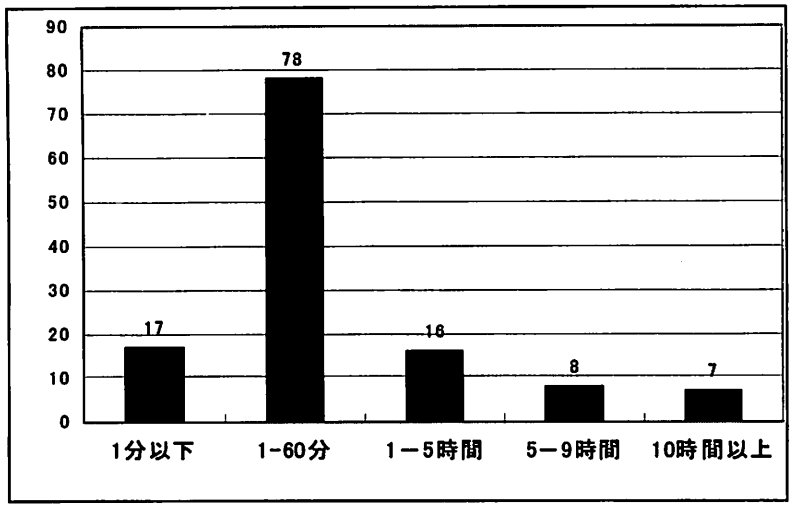


(出典：Jose Nazario " Estonian DDoS Attacks - A summary to date" [6]

[6] http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

この間の攻撃の持続時間は、短いものは1分以下だったが、多くは1時間近く持続し、10時間以上のものも7回、5時間以上が8回と、執拗な攻撃も多かった。

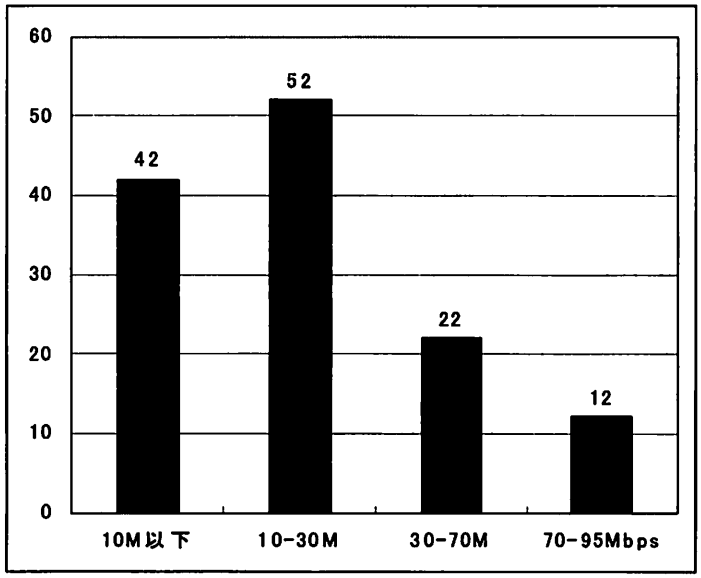
エストニアへのDoS攻撃の持続時間



（出典：前掲）

攻撃の帯域は、最大で総計100Mbps以上に達し、そうした攻撃が10時間以上持続したということから、この攻撃が一定の組織力と意図をもって実施されたことが伺える。

エストニアへのDoS攻撃の帯域合計



（出典：前掲）

政府、CERTなどの対応

これらの一連の攻撃に対して、政府および情報セキュリティの関係者は以下のような対応をとった。4月30日、まずとられたのは、ロシアからの直接攻撃を抑止するために、「.ru」ドメインからのトラフィックをすべて遮断する措置だった。すると翌日からはISPに対する攻撃が集中的に行われた。同じ30日の午前11時に、政府の危機管理委員会、エストニアCERT、エストニアTLD、ISP、電話会社、銀行、司法当局、サイバー警察、インテリジェンスおよびカウンターインテリジェンス機関などの関係者が集まって非公式の緊急会合を開き、対策を検討したという。ただし、決定された事項は限られており、上下の階層型組織ではなく、緩やかに横に連絡をとりあう、ネットワーク型のものとすること、連絡はリアルタイムで、互いの危機管理計画を知らせあう、といった原則が確認されたようだ。また、ゾーンディフェンスの採用、国境でのコントロール、国際的なセキュリティのコミュニティに注意を喚起し、協力を呼びかけること、エストニア国内のハッカーたちを大人しくさせることなども確認され、内務省に報告をしたという。

また、オンライン・バンキングサービスなどへの波状攻撃が予測され、対策が練られた。5月2日から5日かけて、予測通り、銀行への攻撃が集中してきたのに対応して、特定のIPアドレス群からのトラフィックの遮断、バンキングサイトのインターネットからの完全切り離しなどの対抗措置がとられた。これには、世界中のISPが協力したという。

なお、アーレライド氏によれば、国際回線がすべて遮断されたという事実はなく、各国のISPなどに、通常以上の異常なトラフィックがエストニアに向けられていることを発見した場合には、エストニアのCERTに問い合わせることなく、そのトラフィックを制限するように依頼したという。

5月2日には、二回目の会合がもたれ、それまでの誤りの修正などが行われた。首相府からも指示があり、ライフラインやニュースの確保などを優先することが確認された。

攻撃の主体について

エストニアという国家の主要な情報資源に一斉攻撃が加えられたことの意味は大きい。少なくとも特定の国の情報資源にこれだけ大規模なサイバー攻撃が数週間にわたって持続したことは、前例のないことである。

前述したように、そこにロシア政府およびその関連する機関などの関与があったかどうかについては、確かな証拠が存在しているわけではない。現地訪問の前に、JPCERTなど日本のインターネットの関係者に話を聞いた段階では、「ロシアなどの政府組織が公式に関与した証拠はない。明確な根拠がないのに政治的な結論を出すのはかえって危険だ」というのが有力な意見だった。IGFやISSEなどの国際会議の席上でも、欧州のCERT関係者などからは、同様の意見の表明が大半だった。

しかし、今回訪問して取材した、エストニアの政府、議会、軍、NATOのサイバーディフェンスセンター、CERT、銀行その他の関係者は、いずれも
「物理的な直接の証拠はないが、ロシアからだったことは間違いなく、手口や規模からみて相当の能力がなければ不可能で、政府や軍などの機関の関与がなかったとは考えられない」という意見だった。

エストニア政府も、公式にはロシアの政府機関の関与があったとは主張していない。また、それを示唆するような発言や文書の公表も行っていない。しかし、だからといって、彼らがそう考えていないということではない。繰り返しになるが、今回面談した関係者は、いずれもロシア政府の関与を当然のこととして存在していたと述べていた。

前述のCERT文書では、攻撃の主体については以下のように記述されている。

「どのような人間、グループないし組織が攻撃の背後に存在したかは明確ではない。インターネットの匿名性は特定の攻撃主体を特定することを困難としている。これまでに唯一、自ら攻撃を認めた主体として知られているのは、『ナーシ（Nashi)』という親クレムリン派ロシア人の青年集団のコミッサール（軍事・イデオロギー担当組織）である。しかし、最初のフェーズは、単純なハッカーたちによる政治的なイベントに対する主に感情的・自然発生的な反応だったといえるが、第二フェーズには、高度の技術をもったサイバー攻撃の専門家たちが関与していたと結論づけることが可能である。キャンペーンの間中、多くの攻撃が巧妙に連携されたもので、それらは通常膨大な資源を必要とするものである。

この点についてCERTの責任者であるヒラー・アーレライド氏は、今回の取材のなかで以下のように述べている。

「ロシア政府が関与したことを証明するような証拠が発見されることはほとんどありえない。今回の攻撃はまさにそうした証拠が発見できないように巧妙に仕掛けられたからだ。ただし、攻撃のあと、ロシア政府の高官が、

『われわれはこの戦争に勝利した。別に法律に違反したわけではない、そうした法律は存在していないからだ。』と述べていた。

今回起きたことの全体を、サイバーだけでなく様々な異なるイベントを通してその本質をとらえようとすれば、単に草の根の運動だと決め付けることは非常に難しい。

攻撃は、多少弱めに、まさに組織的に行われたとは見えないように巧妙に組織されていたのだ。きわめて周到な計画、調整なしには不可能なものだ。背後に組織的な動きがあったことは明らかといえる。

そうした証拠の一例は、ロシア語で書かれた様々なエストニアを攻撃しようという呼びかけである。異なる対象に対して、スラングを使ったり、それぞれもっとも効果的な言葉遣いで、巧みに人心をつかんでいた。

銅像の歴史的背景などについても、巧みにメッセージを流した。「結婚式のときは、そこで写真を撮ろう」とか「幼稚園の子供たちとそこに行こう」など、四年がかりで仕掛けていったものだ。

それも昨年、2007年には何万人もの人々が銅像のところに行った。今年はまったく静かで、組織的な動きはなにもなかった。なぜか。そう呼びかけた組織がいなかったからだ。」

アーレライド氏は、こうしてロシア政府の組織的な関与の可能性はほぼ100%示唆する発言を行っていた。このほか、議会関係者、経済開発省、民間銀行の人間も、いずれも同様の意見であった。

アーレライド氏も述べているように、これまでのところ、ロシアの国家組織が直接関与した証拠は、発見されていない。

唯一の例外といえるのが、上述文書に出てくる、サイバー攻撃を行ったことを自ら認めたロシア系住民による親ロシア集団「ナーシ」の存在である。そのナーシの攻撃の、少なくとも一部は、ロシアからではなく、旧ソ連領のモルドバ共和国の領内からだったことが、エストニアで確認されていることも注目に値する。これについては、後にモルドバを訪問したときにもモルドバ政府側の認識として指摘された。

また、エストニア国内でロシア系住民一名が、サイバー攻撃を実行したとして逮捕・起訴されている。この逮捕が、「エストニア内部からの攻撃だ」との誤解を生んだが、実際には大半の攻撃はエストニア国外からのものだったという。

なお、攻撃が起きている最中に、エストニアの司法機関がロシア政府に対して公式に、サイバー攻撃の発生源を特定するために協力するよう要請したが、ロシア側からは回答すらなかったという。エストニア側では、ロシアは政府がその気になれば、犯罪集団などに対してきわめて厳しい取締りを実施することは十分可能であり、国内のインターネットも巧妙に情報操作を行って、反ロシア的言論はほとんど存在できないのであり、エストニアへの攻撃を本気で抑制しようとすれば、できないわけはない、とする。それを容認したことは、少なくとも攻撃に加担した責任は免れないというのである。

もっとも、エストニア側もすべてのロシアの関連組織が反エストニアで一致しているわけではなく、ロシア側にも正常な対応をするところはみている。反対に、西側の機関であるFBIやインターポールに対しても、エストニア側の不満は強く、申し入れをしてから6カ月以上たっても協力行動をとらなく、書類をたくさん書かされ、それも内務省経由などで正式のルートをとらなければならず、インターネット経由で瞬時に犯罪者がグローバルに動きまわる時代にまったく対応できていないと批判していた。

なお、ロシアのCERTは、資金こそ政府から得ているようにみえるが、その機能は独立しており、特定の省庁の支配にないことが評価されていた。

以下が、前述のアボカスー国防大臣が2007年秋に米国を訪問した際、国際戦略問題研究所（CSIS）で行った講演のうち、攻撃主体、ロシア政府の関与の可能性にかかわる部分のハイライトである。

「これらの攻撃を突出したものとしたのは、その規模の大きさだけではなく、きわめて巧妙に連携が図られていたことだ。政治的なイベントに伴って自然発生的に起きたものとは明らかに違っている。タリンにあるソ連時代の遺物の移転にまつわる出来事だけではなく、モスクワのエストニア大使館へのデモや妨害とも関連していたのだ。

これらの攻撃は非常に正確な時間的な枠組みと、組織的なコンピューターのグループによって実行され、いわゆるボットネットないしロボットネットワークで、世界中から多数のコンピューターをハイジャックし、マルウェアによってゾンビ化し、世界のどのターゲットでも攻撃するのに利用できるようにした明らかな違法集団である。」

「(昨年4月から5月にかけて起きたサイバーアタックは)、その組織のされ方、コーディネーションと規模の次元では、明らかに政治的な動機に基づくものといって差し支えないと思う。それは、エストニアのような小国にとっては、明確に国家安全保障にかかわる次元に達したものだった。

「そこで、たしかに、これらの攻撃の背後には、不満や怒りに満ちたシビリアンとは異なる主体や、より組織的な仕組みが存在していた。現時点では、特定の主体がこうした一連のイベントを組織したと非難するためにわれわれが使える確かな証拠はどこにも一切存在していない。そうした事実の一部は必然的なものである。というのは、まさにサイバースペースの本質でもある匿名性に関係しているからだ。また、これらがまさに隠密裏に実行されたからでもあって、われわれが言えること

といえば、せいぜい少なくとも部分的にはわれわれの巨大な隣人の外交代表によってコーディネートされ、資金提供されて起きた他のイベント群との相互関係のなかで見るべきことだ。[7]

今回の調査では、エストニアに続いて、バルト三国として同じ旧ソ連圏のリトアニア、ラトビアを訪問したが、リトアニアでは、2007年7月に、やはり政府組織のウェブサイトの大半が一時的に改ざんされ、旧ソ連の「赤旗」が一斉に表示される事態が起きたていた。また、今回は訪問しなかったが、8月にグルジアでロシアとの武力紛争が起きた際には、ロシア軍の本格的な地上攻撃が始まる数時間前に、グルジア政府のウェブサイトが一斉攻撃され、アクセスが不能となった事件が起きている。

これら一連のイベントを総合すると、ロシア政府のいずれかの組織が関与する形で攻撃が起きたと見ても、さほど不自然とはいえないだろう。

ボットネットなどによる自動化された攻撃もあったが、同時に、人間の手による攻撃も多数存在したという。ロシア語による掲示板、フォーラムなどにはエストニアへのサイバー攻撃を扇動、指示するメッセージが多数掲示され、それに従った攻撃が多く発生した。

つまり、こうした攻撃のほぼすべてがロシア語を話す人々によるもので、民族主義的な背景が強くみられたという。

もちろん、一般のロシア人が攻撃に参加したとするのと、ロシアの政府組織が公的に関与したとするのでは、まったく次元が異なることはいうまでもない。少なくとも、後者の見方を明示的に証明するような事実、証拠となる材料は、現在までどこにも存在していない。ロシア政府の関与を主張する見方をする人々も、そのような証拠を提示しているわけではない。

ただし、彼らは「そもそも攻撃元が判明するような攻撃方法を、ロシア政府組織が採用するわけがない。彼らは巧妙に、そうした証拠を残さないような攻撃を行ったのだから、証拠がないからといって、彼らの関与を否定することにはならない」と主張する。

一方、ロシア政府の関与を否定する側は、「どこにもそうした（技術的な）証明材料がないのだから、政府組織の関与を主張することは誤りである」と述べる。

多くの戦争において、開戦時にどちらの側が先に戦闘を開始したのかをめぐって、確たる証拠がなく、非難の応酬がなされることがよくあるが、サイバー攻撃においても、その主体を判定することは容易ではない。

この点について、スウェーデンのインターネットの関係者で、今回のサイバー攻撃時にエストニアへの支援活動に直接かかわったパトリック・ファルストロームは、当方の質問に答えて、以下のように述べている。

「どこが攻撃の主体だったかについては、コメントしない。技術的な観点からいえば、攻撃がロシアから起きたということはできない。わかっていることは、いくつかのブログ上に、「銅像が移設されたことにロシア系の少数住民が反対しているのだから、[エストニア] 政府のサーバーに過負荷をかけよう」などといった投稿があったことだ。非常に大勢の人々が、オープンな議論のなかでそれに同意し（グーグルで検索すればだれでもわかる）、何をどうすればいいかの指示に従うことにした。余談だが、それでわれわれも攻撃が来ることがわかったのだ。

この『ランダム』な攻撃は、国際的なサミットなどへの攻撃と似ているものだが、エストニア国内を起源とするものについていえば、警察がブログに投稿した一人を逮捕し、エストニアの朝のテ

---

[7] http://www.csis.org/component/option,com_csis_events/task,view/id,1440/

レビ番組でインタビューを放送したことでなくなった。その後は、攻撃はエストニア国外のみから来るようになった。

なので、攻撃そのものは非常にランダムだったといえるが、もちろんその背後の『アイディア』がある政治的な勢力によって植えつけられたものかどうかは疑問として残る。

これについてもコメントはしない。」

攻撃後のCERTやその他の技術コミュニティの対応としては、ファルストロームは以下のように回答した。

「西側社会での企業と同様に、より強力なフィルタリングの仕組みが導入された。それらのフィルターの前に、より大きな帯域が確保され、これらの負荷が過大になるリスクが軽減されたことだ。」

攻撃の主体について、特定することを避けるという慎重な態度は、多くのCERTやインターネットの技術系の人間たちに共通するものである。

そのなかで、イスラエルのCERTの創設者の一人で、現在は、英国を中心とするアフィリアスのセキュリティ責任者を務めるガディ・エブロンは、攻撃当時エストニアに滞在し、エストニアCERTを支援するなどの活動にもかかわり、その後、国際会議などでこの問題について活発な発言を繰り返している。

エブロンは、ジョージタウン大学の論文誌への寄稿記事のなかで、以下のように述べている。

("*BATTLING BOTNETS AND ONLINE MOBS*", Gadi EVRON, Journal of Science & Technology Winter/Spring 2008 ")

「[エストニアへの] 攻撃が発生する以前から、数多くの痕跡が、大規模な作戦がオンラインで計画されていることを示していた。ロシア語のインターネットの討論フォーラムで、オンライン攻撃の準備が話し合われていた。攻撃予定と目されていた日の三日前に、攻撃がロシア政府によるものかどうかにかかわりなく、エストニアはヨーロッパのメディアが注目することでEUがクレミリンに圧力をかけることを期待して、攻撃の到来を予測するニュースを流そうと計画した。しかし、当時EU議長だったドイツのメルケル首相とロシアのプーチン首相との会談が予定されているところから、EU諸国のプレッシャーのためにエストニア政府は声明の発表を見送った経緯がある。

＜略＞

ロシア政府が公式に攻撃を認めていたかどうかは不明だが、ロシア人に責任があることは間違いない。ロシア語のウェブサイト、オンラインフォーラム、ブログなどには、銅像の移転とそれに続くサイバー攻撃についての会話が多数飛び交っていた。エストニアの攻撃目標と、どう攻撃するかのマニュアルを掲載するロシア語サイトもいくつかあった。

サイバー攻撃の起源やそれに同調した者をトレースすることは技術的には不十分で信頼できないが、それはインターネットの設計がそもそもオープンなものであり、広い地域や国に対して割り当てられるIPアドレスからは、コンピューターや攻撃の起源となった正確な場所を特定することは難しい。また、コンピューターを乗っ取ることも容易であるため、だれでも実際の攻撃源を秘匿しながら、プロキシーによって攻撃を実行することが可能となる。

しかし、攻撃の正確な起源が不明であるとしても、多くの証拠が、きわめて巧妙に組織された攻撃であったことを示唆している。サイバー攻撃がほぼ同時に開始されたこと、ロシア語で新しい攻

撃目標や方法についての指示が次々にブログに登場したことなどの詳細からは、サイバー攻撃がエストニア側の防衛に応じて対応していったことがわかる。

攻撃者たちはエストニアのIP空間に外部からボットネットを仕掛け、次に、そうして侵入されたコンピューターのネットワークに中央コントロールによる「トロイの木馬」ソフトが働きかけてボットネットに仕立てていった。

外部のアタックに対する防御が成功した後は、こうしたエストニア内部のボットネットが作動した。＜略＞

ロシア政府が関与したかどうかは確認できない。ただし、そうした疑いを高めたのは、ロシア政府が最初の攻撃から三週間にわたって、エストニアへの「サイバー暴動」を停止することに失敗したこと、ないしは積極的に協力しようとしなかったことである。」

（下線部は筆者）

後述するが、バルト三国に続いてルーマニアとウクライナにはさまれた小国であるモルドバを訪問したが、政府の情報セキュリティ担当責任者は、「われわれはロシアと良好な関係を保っている限り、サイバーテロの心配はない」と言いつつ、実際には、状況によって自国のウェブサイトが攻撃されることへの懸念を深めていた。親ロシア系の若者集団が、モルドバ領内だが、ロシア系住民によって「独立」が宣言されて事実上「無法地帯」となっているトランスニステリアからエストニアにサイバー攻撃をしていた事実に着目し、警戒を隠さなかった。

バルト三国のうち、リトアニアの政府関係者もエストニアへのサイバー攻撃について、「サイバー戦争」と呼び、自国への同種の攻撃の脅威についての対策を進めている。

2008年8月に発生した、グルジアでのロシア軍とグルジア軍との紛争の前後に、グルジア政府サイトなどに対して、やはりロシア側からサイバー攻撃が発生したという報道がなされている。今回、直接グルジアを訪問したわけではなく、詳細な情報を直接得たわけではないので、性急な結論を出すことは控えるが、今回訪問して会った多くの関係者が、グルジアの事例は、エストニアよりさらに深刻なものとみる人も多く、そこでは地上戦闘とサイバー攻撃との連携がみられるとしていることは興味深い。

以上、エストニアへのサイバー攻撃とそれに対する政策・対策・評価について考察してきたが、結論としては、ある部分を切り取ってその是非をミクロ的に論じるよりも、サイバーセキュリティが、一国と社会全体にかかわる安全保障の重要な一環になりつつあることを踏まえた、総合的な観点での研究と実践が求められるようになったということを示唆する重要な事例だととらえることが、より生産的であると思われる。

保健師による子育て支援のためのネットワークの構築と実用化に関する検討

日本文理大学工学部情報メディア学科
教授　赤星　哲也
akahoshi@nbu.ac.jp

1．はじめに

我々は「保健師による子育て支援のためのネットワーク構築と実用化に関する検討」(科学研究費補助金萌芽研究　課題番号 18659694　平成 18～20 年度　赤星琴美*1 ・ 赤星哲也)において、「子育て支援携帯ネット」システムの試作を行った。本稿ではこの試作システムについて報告する。

2．先行研究

本研究に先立って、赤星ら*2 は、育児中の母親への効果的な育児支援には、個々人の状況に応じたサービスの提供が重要であるとの観点から、保健師から母親宛に携帯電話メールを用いて個別の情報を配信すると同時に、母親側からは随時、携帯電話向け Web サイトを通してタイムリーな情報を得ることができる「子育て支援携帯ネット」システムを試験運用し、携帯電話という身近なコミュニケーション手段を用いた個別的な子育て情報サービスの提供が、ICT 利活用による新しい形での育児支援手段として有効であることを確認した。

3．「子育て支援携帯ネット」システムの概要

先行研究において試験運用したシステムは、保健師側の作業の多くを手作業に依存していた。そこで、我々は保健師側の作業の省力化を目的に、手作業の多くを自動化、もしくは、半自動化したシステムを試作することにした。

試作システムは「携帯電話メール自動配信システム」、「携帯電話向け Web サイトシステム」の２つの独立したシステムから構成されている。

（1）携帯電話メール自動配信システム

ユーザー情報（育児中の母子に関する情報）を収めたデータベースから、各ユーザーの予防接種状況を取得し、その接種状況を手がかりに、次回の予防接種通知情報を各ユーザーの携帯電話宛に、週１回、携帯電話メールとして自動配信する。

本システムはクライアント／サーバシステムの構成を取っており、サーバ側の機能としては、①ユーザーを登録する、②ユーザー情報を更新するの２つが、クライアント側（保健師が使用する Windows マシン）の機能としては、③ユーザー（子育て中の母親）からのメールを受信してデータベースを更新する、④ユーザー毎に個別メールを作成・編集・配信するの２つの作業が、それぞれ実装されている。本システムの開発・運用環境は次の通りである。

サーバ側

OS：FreeBSD6.1　　Web サーバ：Appache1.3.39　　メールサーバ：POP3、SMTP
CGI スクリプト：Python2.4.3

クライアント側

OS：WindowsXP　GUIアプリケーション開発：Python2.5.1

データベース：SQLite3　GUIツールキット：Tk(Tkinter)

（2）携帯電話向けWebサイトシステム

保健師による週単位・月単位での情報更新作業を容易にするため、情報更新のしやすさを考慮して、Wikiクローン「PukiWiki」を用いて作成・運用している。

週単位での更新情報としては「どげかえ子育て」コーナー、「感染症発生動向」コーナー、「すこやか情報」コーナーを、月単位での更新情報としてはメール配信月の集団健康診査、個別健康診査、育児相談、電話相談、イベント情報を提供している。また、常設コンテンツとして、予防接種の必要性、接種を受ける順序、ワクチンの種類と特徴、副反応の有無、接種前後の注意事項、各予防接種の特徴等からなる「予防接種豆辞典」を用意している。

4．今後の展望

本システムは、場所・時間の制約を受けずにタイムリーな情報を入手できること、ユーザー個別の情報を提供できること、特に、予防接種に関する情報がタイムリーに携帯電話メール経由で届くことにより予防接種への勧奨効果が期待できること、などの利点をもつ。但し、今回試作したシステムはクライアント／サーバシステム方式を採用しており、これをそのまま実用化・製品化するには障害が多いため、今後はASP事業等への展開を円滑に行うことが可能なWebアプリケーションシステム方式等へのシステム設計の見直し・詳細化等の作業を行い、本システムの実用化・製品化につなげたいと考えている。

*1　大分県立看護科学大学広域看護学講座地域看護学　講師

*2　「携帯電話を利用した『子育て支援携帯ネット』の作成と運用―予防接種に関する情報を中心にして―」（赤星琴美・甲斐倫明・桜井礼子・草間朋子，　保健師ジャーナル，　61巻8号，　2005年8月，　pp.736-742）

ウェブアクセシビリティに関する一考察

大分県立芸術文化短期大学
教授　凍田　和美
korida@oita-pjc.ac.jp

1．はじめに

インターネットの急激な普及に伴い、インターネット利用者は増え続けている。総務省の平成20年度年末情報通信白書[1]によれば、平成19年度のインターネットの利用者数は8,811万人であり、人口普及率は69.0%と推計されている。

こうした中、インターネット上には企業のものから個人のものまで数多くのウェブページがある。無料でウェブサーバを提供してくれるプロバイダの増加や、簡単にウェブページを作成できるウェブオーサリングツールが増えたことから、HTMLの詳しい知識がなくてもウェブページが作りやすくなったため、ウェブページを閲覧するだけではなく、自らウェブページを作成・運営する人が多くなった。しかし、これらのウェブページの中には、「デザインだけにこだわりすぎていて、どこにリンクがあるのかわかりにくい」「ページを開くといきなり音楽が流れてきた」など、閲覧する側に不便さを感じさせるものもある。こうした不便さをなくすための指標として「ウェブアクセシビリティ」がある。ウェブページを作成するには、ウェブを利用する全ての人が年齢や利用環境、視覚・聴覚障害などの身体的制約に関係なくコンテンツにアクセスでき、情報を得ることできることを意味するアクセシビリティが重要である。

大企業のウェブページには、アクセシビリティを考慮しているページが多いが、中小企業や個人のウェブページはアクセシビリティを考慮しているページは少ない。これは、アクセシビリティの知識を持っている人が少なく、ただ好きなようにデザインしているためだと考える。

本研究では、①わかりやすいウェブアクセシビリティガイドラインの作成、それを用いた②県内のいくつかの市や学校のウェブページのアクセシビリティチェックを基本方針として、ウェブアクセシビリティについて考察する。

2．ウェブアクセシビリティガイドラインの作成

Accessibility（アクセシビリティ）は、「アクセスのし易さ」という意味の英語である。Web Accessibility（ウェブアクセシビリティ：ウェブサイトへのアクセスのし易さ」は、ウェブを利用する全ての人が年齢や利用環境、視覚や聴覚障害などの身体的制約などに関係なく、ウェブで提供されている情報に問題なくアクセスできることを意味する。

ウェブアクセシビリティ入門サイト[2]によると、これまでの具体的なウェブアクセシビリティ運動の流れは、1999年5月にW3C（※1）のWAI（※2）が「Web Contents Accessibility Guideline 1.0」[3]を勧告として発表したところから始まり、日本では、2004年6月に「JIS X 8341-3 高齢者・障害者等配慮設計指針ー情報通信における機器，ソフトウェア及びサービスー第3部：ウェブコンテンツ」が制定され、現在、W3CのWAIが1999年5月に勧告となった1.0を大幅にグレードアップ修正した「Web Content Accessibility Guidelines 2.0」の最終ドラフトを発行し、W3C勧告となるのを待っている状態であるという。

(※1)World Wide Web Consortium…各種技術の標準化を推進するために設立された非営利団体

(※2)Web Accessibility Initiative…World Wide Webにアクセスする人々のためにウェブアクセシビリティ向上を目的とする団体

インターネットの普及により多くの高齢者や障害者がウェブを利用するようになった。しかし、利用者の身体条件などによって思うように欲しい情報を取得できない問題が起きている。例えば、全盲や弱視の視覚障害者は、音声読み上げソフトや、情報を点字に変換して表示する点字ディスプレイなどを利用している。音声読み上げソフトとは、テキストデータを日本語で

読み上げるものである。ウェブの中では、大事な情報が画像で表現されるケースが多いが、音声読み上げソフトではテキストデータしか読み上げられないため、画像で表現された部分は何が書かれているか判別できず、読み飛ばされてしまう。よって、音声読み上げソフトを使ってウェブを利用している視覚障害者は、画像で表現された重要な情報を知ることができない。また、ウェブアクセシビリティは、高齢者や障害者のためにだけ必要なのではない。携帯電話など、パソコン以外からのウェブサイトの利用が拡大しつつあり、画像の容量が大きくて表示できないなど、重要な情報を得ることができない状況は一般的にも起きる。

高齢者や障害者、“非パソコン”端末からの利用者は、ウェブサイトを閲覧する際に多くの問題が発生する。そのような問題を解決するためにも、ウェブサイトを作成する際にアクセシビリティを考慮することは必要不可欠である。アクセシビリティを十分確保したウェブページでは、音声読み上げソフトや、非パソコンからのアクセスに対しても、必要な情報を提供することができる。例えば、どんなに画像をたくさん使ったサイトでも、画像が表わしている情報をテキストで説明した「代替テキスト」が提供されていれば、画像が表示されなくても情報を理解することができる。

誰もが不自由なく閲覧することができるウェブページを作成するには、気をつけなければならない事が数多くあり、これらをまとめているものがアクセシビリティガイドラインである。これはアクセシビリティの高いウェブページの作成時に参考になる重要なものである。現在、様々なウェブページの基準となっているアクセシビリティガイドラインは、W3C の「Web Contents Accessibility Guideline 1.0」である。このガイドラインには大きく分けて 14 の項目がある。この 14 項目の中にもいくつかのチェックポイントがあるため、合計すると全部で 61 のチェックポイントがある。その 61 のチェックポイントをそれぞれ 1 から 3 までの優先度で分けた表も「Web Contents Accessibility Guideline 1.0」に掲載されている。

ガイドラインの１４項目

（１） 聞くための内容や見るための内容には、同等の役割を果たす代わりのものを提供する。
（２） 色だけに依存しない。
（３） 正しくタグ付けし、適切にスタイルシートを使う。
（４） 自然言語の取り扱い方に関する情報を明確に示す。
（５） うまく変換されるテーブルを作る。
（６） 新しい技術を利用したページは、うまく変換されるようにしておく。
（７） 時間とともに変化する内容については、ユーザーが制御できるようにする。
（８） ページ中に組み込まれたもののユーザーインターフェイスは、それ自体がアクセシブルなものにする。
（９） 装置に依存しないように設計する。
（１０） 暫定的な解決策をとる。
（１１） W3C のテクノロジーとガイドラインを使用する。
（１２） 前後関係や位置を表す情報を提供する。
（１３） はっきりとわかるナビゲーションのための仕組を提供する。
（１４） 文書は明瞭で簡潔なものにする。

アクセシビリティの優れたウェブページを作成するには、このガイドラインを参考にするとよい。しかし、このガイドラインには専門用語や難しい表現が多く使われているため、インターネットの知識が少ない人にとっては内容を理解するのは難しい。我々は、インターネットの知識が少ない人にも容易に理解できるガイドラインを作成することにした。

W3C の「Web Contents Accessibility Guideline 1.0」や、ガイドラインを日本語でわかりやすくまとめているユーディット[4]のウェブページを参考にして、実際にガイドラインを作成した。わかりやすくするために“専門用語の解説”“なぜそうしなくてはいけないのかの説明”

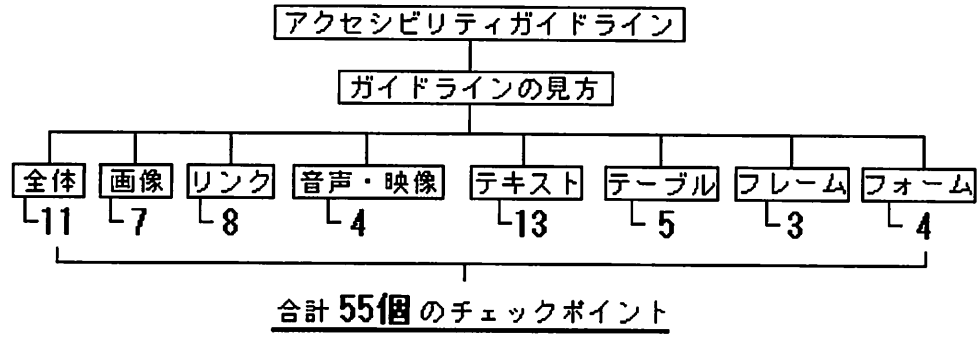


図１　作成したガイドラインの構成

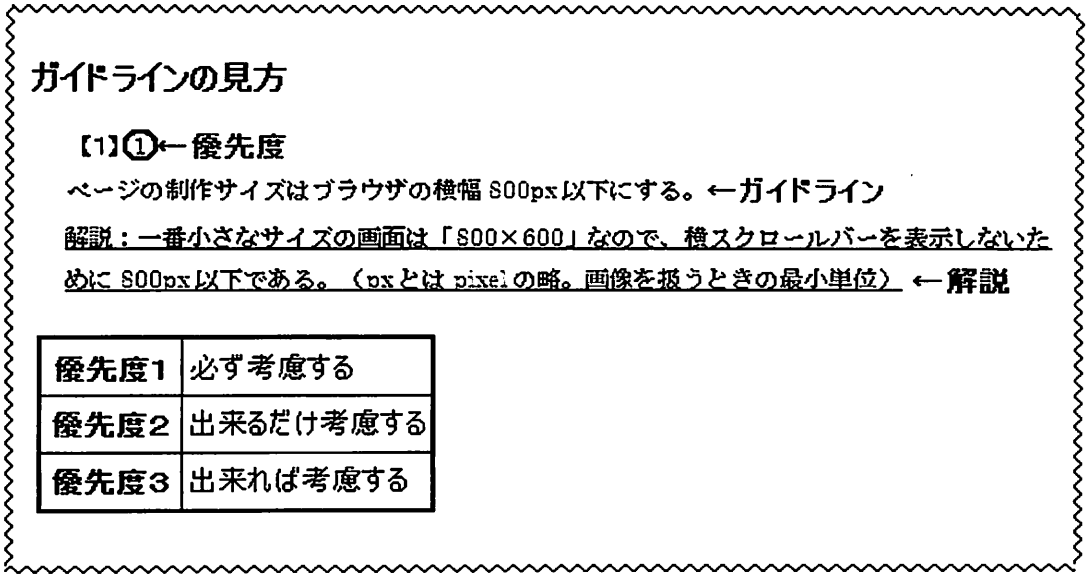


図２　作成したガイドラインの一部

“実際のページの画像を入れる”などを工夫した。ガイドラインを大まかに「全体」「画像」「リンク」「音声・映像」「テキスト」「テーブル」「フレーム」「フォーム」の 8 項目に分け、その項目ごとにチェックポイントを作成した。チェックポイントの数は、「Web Contents Accessibility Guideline 1.0」にのっている 61 個を参考に、類似している項目を削減・結合させ、最終的に全体 11、画像 7、リンク 8、音声・映像 4、テキスト 13、テーブル 5、フレーム 3、フォーム 4 の、全 55 個にした（図１）。さらに、解説部分や優先度がわかりやすいよう、一番上に図２のようにガイドラインの見方を作成した。

各項目中で優先度が高いチェックポイントから順に並べ、解説や画像を追加した。例えば、「画像」項目の中には７つのチェックポイントがあるが、その１番目と２番目は「画像には ALT 属性をつける。また、ワンポイント的な画像の ALT にはスペースを入れる。」「リンクの画像やイメージマップにも、リンク先の内容を明確に示す ALT 属性をつける。」となっている。これは優先度１で絶対に守って欲しい項目である。よって、ALT 属性が何のことかわからない人にも理解できるように、画像を入れて説明した（図３）。

３．市のホームページのアクセシビリティチェック

作成したガイドラインを使って、県内の市のウェブページのアクセシビリティチェックを行った。市のウェブページは、多くの市民が閲覧する可能性が高く、アクセシビリティ面も考慮

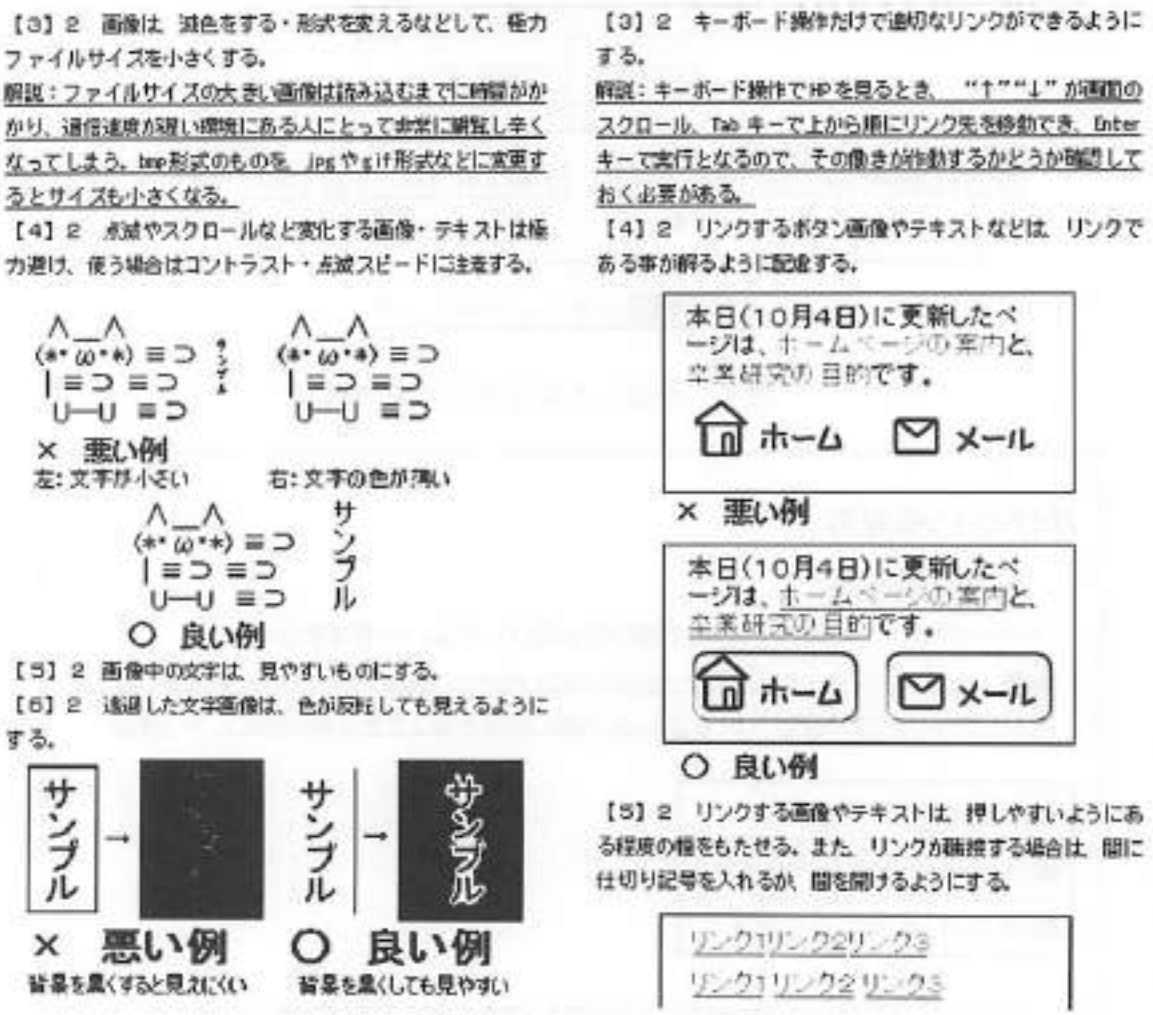


図3 作成したガイドラインの一部

されていると予想した。そこで、どのくらいアクセシビリティが考慮されているのかをガイドラインを見ながらチェックした。チェック方法はガイドラインの全55項目を1つずつチェックし、出来ている場合は○、出来ている箇所と出来ていない箇所がある場合は△、全然出来ていない場合は×という、3段階評価で行った。(紙面の都合により、ここではA市とB市のウェブページについて示す。)

チェックの結果、どちらのウェブページにも×がついている項目はあるが、A市はB市よりも○が多いので、アクセシビリティ面をより考慮していると考える。しかし、どちらのウェブページにも守れていない箇所があり、完璧ではない(図5a・5b参照)。

表2a・2bにあるように、A市の△と×の9個の中には、優先度が1のものが2つ・優先度2のものが6つ・優先度3のものが1つあり、B市では20個の中に優先度1のものが4つ・優先度2のものが14つ・優先度3のものが2つあった。A市に比べ、B市のウェブページの方が良くない項目も多い、優先度の高い項目があまり守られておらず、B市のウェブページはアクセシビリティが低い。それぞれのウェブページのトップページをアクセシビリティチェックサイトの「HAREL」[5]でチェックしたところ、A市が78点、B市が66点となり、B市は得点が低くなっている。

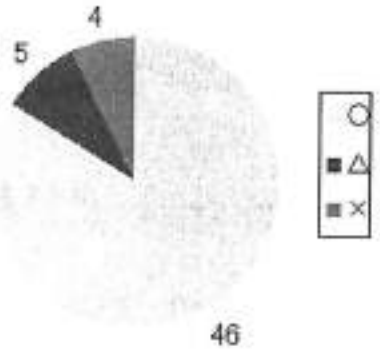


図4a　A市のHPチェック結果

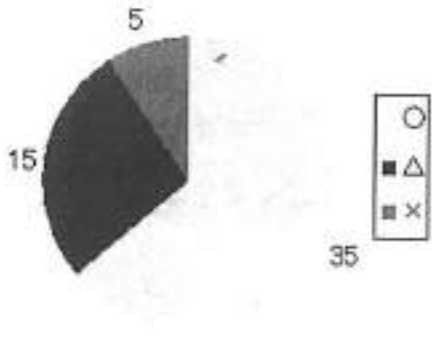


図4b　B市のHPチェック結果

表1a　A市のウェブページの△・×の項目

評価	優先度	項目と番号	内容
×	1	画　像[1]	画像にはALT属性をつける。
△	1	テキスト[4]	見出し要素を正しく付け、順番を守る。
△	2	全　体[4]	背景色・文字色等は、見やすくする。
△	2	全　体[5]	ページレイアウトのためのテーブル利用は避ける。
△	2	画　像[5]	画像中の文字は、見やすいものにする。
×	2	テーブル[3]	行や列の見出し項目には<TH>を使って指定する。
×	2	リンク[7]	ナビゲーションがある場合は読み飛ばせるようにする。
×	2	テキスト[5]	一単語内にスペースや強制改行を入れないようにする。
△	3	画　像[7]	重要な画像には解説を入れるか解説ページをつくる。

表1b　B市のウェブページの△・×の項目

評価	優先度	項目と番号	内容
△	1	画　像[1]	画像にはALT属性をつける。
△	1	画　像[2]	リンク画像やイメージマップにも、ALT属性をつける。
△	1	テキスト[3]	丸付き数字等の機種依存文字は使わないようにする。
×	1	テキスト[4]	見出し要素を正しく付け、順番を守る。
△	2	全　体[4]	背景色・文字色等は、見やすくする。
×	2	全　体[5]	ページレイアウトのためのテーブル利用は避ける。
△	2	全　体[6]	文字の制御にはスタイルシートを使うようにする。
△	2	リンク[2]	サイト内の基本操作は同じ位置・形状にする。
△	2	リンク[4]	リンクする画像やテキストなどは、わかりやすくする。
×	2	リンク[7]	ナビゲーションがある場合は読み飛ばせるようにする。
△	2	映　像[2]	重要な情報は聴覚的な方法と視覚的な方法で知らせる。
△	2	テキスト[5]	一単語内にスペースや強制改行を入れないようにする。
△	2	テキスト[8]	リストは正確に構造を記述し見栄えのために用いない。
△	2	テキスト[9]	リストの番号表示は読み上げられないので注意する。
△	2	テーブル[2]	表の始まりには「表題」を付けるようにする。
×	2	テーブル[3]	行や列の見出し項目には<TH>を使って指定する。
△	2	テーブル[5]	テーブルは適切に読み上げられるようにする。
△	2	フォーム[1]	フォームにはデフォルト値を持たせるか説明を付ける
△	3	フォーム[4]	フォームによる入力は代替手段を用意する。
×	3	全　体[11]	ページレイアウトや文章表現は出来るだけ統一させる。

4．小学校ホームページのアクセシビリティチェック

大分市小学校のウェブページのアクセシビリティをチェックした。

（1） 目的：大分市内の小学校のウェブページを対象にアクセシビリティがどの程度考慮できているのかを調査する。

（2） 対象：大分市の小学校 20 校

（3） 方法：ガイドラインの一部 20 項目をチェックし、出来ているものには○、出来ていないものには×と分けた。出来ているところと出来ていないところがあった場合は、出来ていないとみなす。また、使っていない場合は未とする。

（4） 設問項目：ガイドラインの項目の中から優先度が高いものや、この項目はクリアして貰いたいと考えるもの、また、閲覧した際にすぐ判断が出来るものなどを合計した 20 項目にした。

①ページの制作サイズはブラウザの横幅 800px 以下にする。
②HEAD に付ける<TITLE>は内容が解りやすい適切なタイトルにする。
③ページのレイアウトのためにテーブルを利用するのは極力避ける。
④フォントサイズ・色・表示位置等の制御にはできるだけスタイルシートを使うようにする。
⑤サイト全体の構成を示すために、サイトマップや目次を提供する。
⑥画像には ALT 属性をつける。また、ワンポイント的な画像の ALT にはスペースを入れる。
⑦リンクの画像やイメージマップにも、リンク先の内容を明確に示す ALT 属性をつける。
⑧画像中の文字は、見やすいものにする。
⑨リンクの下線はむやみに消さないようにする。
⑩リンクするボタン画像やテキストなどは、リンクである事が解るように配慮する。
⑪リンクする画像やテキストは、押しやすいようにある程度の幅を持たせる。また、リンクが隣接する場合は、間に仕切り記号を入れるか、間を開けるようにする。
⑫最初にナビゲーションがある場合は、読み飛ばせるように本文に直接飛べるリンクをつける。
⑬丸付き数字等の機種依存文字は使わないようにする。
⑭点滅やスクロールしたりするテキストの使用は極力避ける。
⑮リストの番号表示等は音声では読み上げられないので注意する。
⑯ＰＤＦでの情報提供は極力避ける。
⑰表の始まりには「表題」を付けるようにする。
⑱行や列の見出し項目には<TH>を使って指定する。 ※（<td>タグを使用しない）。
⑲全ての FRAME 要素に、フレームの内容を的確に示し、フレームの識別が可能なタイトルを付ける。
⑳フレームのスクロールバーを非表示にしないようにする。

（5）結果：

表２にあるように、ガイドラインの項目の全てが出来ている小学校はなかったが、10 以上の項目が出来ている小学校は 20 校中 11 校あった。項目ごとに見てみると、出来ていない数が最も多かったのは⑤の「サイトマップや目次を提供する」であった。これは、多くの人が観覧する小学校のウェブページでは作成してもらいたい項目であり、我々もできている小学校が多いと予想していただけに、出来ている小学校が１つもないことに驚いた。また、⑥の「画像に ALT 属性を付ける」という項目も、図５を見てわかるようにほとんどの小学校では守られていなかった。守られていない小学校の中には、ところどころに ALT 属性をつけているものの、ウェブページの全ての画像につけていない小学校が多々あったため、ALT 属性を全く知らないわけではないようである。これは、ALT 属性のことは知っているものの、その重要性を知らないためと考える。また、項目⑲「全てのフレーム要素にタイトルをつける」と⑳「フレームのスクロ

ールバーを非表示にしない」に関してはフレームを使っているウェブページ自体は少なかったが、フレームを使っていても、気をつけなければいけない部分ができていなかった。

最も出来ていた項目は⑪と⑮である。⑪の「リンクする画像やテキストは、押しやすいようにある程度の幅を持たせる」の項目では、文字リンクの場合、原則文字が2文字以上でないといけない。ウェブページの中にはリンクの文字が2文字のところがあったが、文字のサイズが大きく押しやすくなっていたため問題なかった。⑮はリストを使っているところがあると考えていたが、今回チェックした20校の中に番号のあるリストを使用しているウェブページはなかった。

5．考　察

アクセシビリティガイドラインはアクセシビリティを理解してない人や、アクセシビリティを知らない人、アクセシビリティは知っているけど、どうすればいいのかわからない人でも、比較的簡単にアクセシビリティに触れることができる。こうすればアクセシビリティが高くなる、ということを書いており、どうすればいいのかすぐにわかる。しかし、ガイドラインだけを見ながらの作成では足りない部分もあるため、アクセシビリティチェックができるウェブページも合わせて利用すると良い。また、有料ではあるがかなり精密にチェックをしてくれるソフトも販売されているので購入するとよい。

ガイドラインはあくまでアクセシビリティを考慮するための参考資料であるため、ウェブページの作成自体を支援できるものにはならないが、これを読んでアクセシビリティとはどういったものがあるのかを知ることができる。そして、作成したウェブページのアクセシビリティチェックに利用してもらいたい。

市や学校のアクセシビリティチェックの結果では、我々が予想していたよりもできていない項目が多かった。これらを改善するためには、アクセシビリティとはどんなものであり、どれくらい重要であるかを知る必要がある。小学校のウェブページは、大企業のウェブページに比べれば利用者も少なく見る人も限られているため、ウェブページにこだわる必要はないと考えるかもしれないが、ウェブページを所持している以上は、常にそのページを見てくれる人のことを考えて、見やすく使いやすいウェブページの作成をしてもらいたい。そのためには、自分なりにアクセシビリティの重要性を学ぶ必要がある。

また、アクセシビリティの重要性を知っていても改善しなければ何もかわらない。チェックをするだけで満足せず、実際にウェブページの修正をすべきである。

我々はアクセシビリティのみに着目していたが、アクセシビリティのよいウェブページを作成してもそのウェブページを見てくれる人がいなければ意味はない。ウェブページを多くの人に見てもらえるように努力する必要がある。

表2　小学校ごとの出来ている部分と出来ていない部分の数

	○の数	×の数		○の数	×の数
小学校A	12	6	小学校K	6	12
小学校B	7	11	小学校L	11	7
小学校C	9	9	小学校M	9	9
小学校D	12	6	小学校N	11	7
小学校E	12	7	小学校O	9	9
小学校F	12	6	小学校P	12	4
小学校G	11	7	小学校Q	9	9
小学校H	11	7	小学校R	10	10
小学校I	12	6	小学校S	9	9
小学校J	9	11	小学校T	8	10

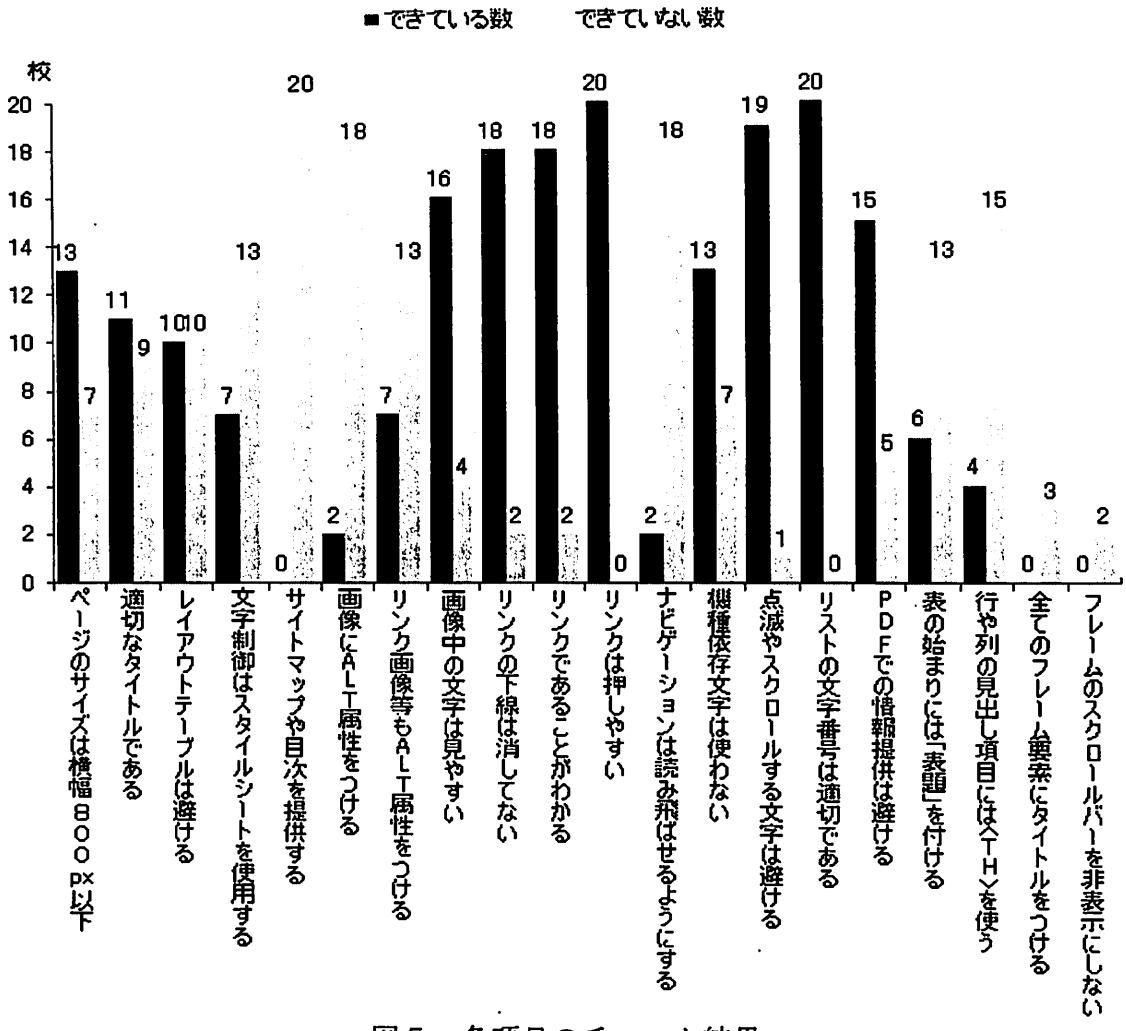


図5　各項目のチェック結果

6．おわりに

本研究の次の基本方針に基づき研究を行った。

（1）　わかりやすいウェブアクセシビリティガイドラインを作成した。インターネットの知識がない人でもガイドラインを理解できるように画像や説明など追加した。

（2）　いくつかの市や学校のウェブページをチェックした。アクセシビリティが完璧に出来ているウェブページは少なかった。

ウェブページは様々な人が見るものであり、大切な情報源である。ウェブページの作成者は、どのような環境でも見やすく、知りたい情報が簡単に得られるウェブページを作成すべきである。本研究で作成したアクセシビリティガイドラインを参考に、小学校のホームページ作成を行ったが、これについては、別途報告する予定である。

参考資料

【1】総務省ホームページ　http://www.soumu.go.jp/
【2】ウェブアクセシビリティとは？ウェブアクセシビリティ入門サイト
http://www.webaccessibility.jp/
【3】ウェブコンテンツ・アクセシビリティ・ガイドライン 1.0
http://www.zspc.com/documents/wcag10/
【4】株式会社ユーディット　http://www.udit.jp/
【5】HAREL　http://harel.nttdata.co.jp/index

相関行列主成分分析ブロードバンド普及モデルに基づく情報政策評価

鳥取大学大学教育総合センター　研究開発部
准教授　永松　利文
tnagamatsu@uec.tottori-u.ac.jp

1. 先行研究のレヴューと概要

日本国内におけるブロードバンドの普及は、主として供給及び市場均衡要因によって進んできた。しかしながら、近年のブロードバンド普及においては、消費者すなわち需要要因もこれに大きく関係していると推測できる。またブロードバンドの技術的要因が市場経済に適応することで、その普及は、供給や市場均衡要因よりも需要要因に規定されていくのではないかとも考えられる。本研究は、このような問題意識をもとに、マクロデータを解析し現象の検証を試みる。なお、本稿は平成20年7月に刊行された拙稿『開発技術学会誌』第14巻に基礎を置いている[1]。

これまでブロードバンド普及分析に関する研究としては ITU（国際電気通信連合）や田尻信行をはじめいくつかの事例があるが、その普及要因としては、おおむね供給、需要、規制を大項目としている[2]。なかでも ITU はこれを細分化し、競争状況、技術革新、アプリケーション、競争をうながす規制、マーケティング、料金、通信速度、技術利用度合い、都市部の人口、ベンチマークの10項目を挙げている[3]。

『開発技術学会誌』第14巻では、回帰分析によって目的変数をブロードバンド契約者数とし、以下に示す説明変数を与え、普及式を構築した。その特徴はブロードバンドの需要要因が補完財であるアプリケーション・コンテンツと仮定しその検証を試みた。ただし、先行研究を踏まえ、その代替変数としてインターネットドメイン数を充てたが、この変数の起用には、課題を残したままであり、正確な弾力性を測るには他の変数が望ましいだろう。なおこのデータは JPRS 社[4]に依頼し2007年6月末のデータを収集したものである。

表 1.1 は回帰分析に要したパラメータである。なお弾力値により解析したので、自然対数を採用した。

表 1.1　変数一覧

変数名	主区分	変数の内容　　（＋又は－）予想される符号
BBS		目的変数 ブロードバンド加入者を人口（千人）で除した値（2005 年）
L	供給	説明変数（基本設備）（＋） 固定電話加入者数を人口（千人）で除した値（2005 年）
D	供給	説明変数（人口集中度）（＋） 人口密度（1ｋ㎡当たり人口数）（2005 年）
Iw	供給	説明変数（産業規模）（＋） 情報通信専業者数（2002 年）を人口（千人）で除した値
Pc	需要	説明変数（利用環境）（＋） パソコン保有台数（2004 年）を人口（千人）で除した値
U	需要	説明変数（利用能力）（＋） 高等教育経験者数（大学及び大学院経験者割合）（2000 年）を人口（千人）で除した値
Id	需要	説明変数（補完財）（＋） インターネットドメイン数（2007 年 6 月末に調査を実施）を人口（千人）で除した値
Ch	市場均衡	説明変数（設備型競争）（－） HHI 指数を BBS 各サービス契約者数から算出（2006 年）[5]
PC	市場均衡	説明変数（＋？－？） CATV 月額料金（2007 年）各地域で最も加入者の多い CATV 事業者の最速サービス（CATV 視聴とセットした場合の最安価料金体系を適用）を対象。これを一人当たり都道府県民所得月額（2003 年）で除した値
PD	市場均衡	説明変数（＋？－？） DSL フレッツ ADSL47Mbps タイプ月額料金（2007 年）。これを一人当たり都道府県民所得月額（2003 年）で除した値
PF	市場均衡	説明変数（＋？－？） FTTH 月額料金（NTT 東日本管轄地域は B フレッツファミリータイプ、NTT 西日本管轄地域はフレッツ光・プレミアムファミリータイプ*「フレッツあっと割引適用」）（2006 年）。これを一人当たり都道府県民所得月額（2003 年）で除した値

（出所）総務省による各種統計調査、学校教育基本調査報告書、各事業者公表値、社団法人日本ネットワークインフォメーションセンター、Japan Registry 社、Office E-Guild 社、社団法人日本ケーブルテレビ連盟等を参考に情報を収集した。また、DSL1M 換算料金は、NTT 東西の提供する最速サービス（47M）　当該地域における 100kbps 換算の料金である。なお、前述したように、都道府県別のインターネットドメイン数は、Japan Registry 社と協同し独自のデータ収集を実施した。

2. 回帰分析の結果のレヴュー

推定結果は以下の表の通りとなった。

表 2.1　結果(1)

BBS1		
定数項	0.435	
L	0.300**	(0.128)
D	0.029	(0.019)
Iw	0.073	(0.047)
Pc	0.434***	(0.119)
U	0.221**	(0.092)
Id	0.098**	(0.043)
Ch	-0.210**	(0.079)
PC	0.048	(0.053)
PD	-0.202	(0.258)
PF	0.128	(0.294)
R^2	0.946	
AdjustedR^2	0.931	
N	47	

(　)は標準誤差

***1%水準で有意　**5%水準で有意

(　)内の数値は t 値。

$$= 0.435 + 0.300 \ln(L) + 0.029 \ln(D) + 0.073 \ln(Iw)$$
$$(0.328) \quad (2.335) \quad (1.495) \quad (1.548)$$
$$- 0.210 \ln(Ch) + 0.434 \ln \ln(Pc) + 0.221 \ln(U)$$
$$(-2.659) \quad (3.644) \quad (2.409)$$
$$+ 0.098 \ln(Id) + 0.048 \ln(PC) - 0.202 \ln(PD)$$
$$(2.251) \quad (0.901) \quad (-0.785)$$
$$+ 0.128 \ln(PF)$$
$$(-0.785)$$

自由度調整済みR^2=0.931

ただし、多重共線性 (PC と PF) が確認されたので、以下を試みた。

表 2.2　結果(2)

BBS2		
定数項	0.634	
L	0.275**	(0.125)
D	0.022	(0.018)
Iw	0.088**	(0.039)
Pc	0.407***	(0.115)
U	0.208**	(0.086)
Id	0.092**	(0.042)
Ch	-0.173**	(0.066)
PC		
PD	-0.107	(0.135)
PF		
R^2	0.944	
AdjustedR^2	0.932	
N	47	

(　)は標準誤差

***1%水準で有意　**5%水準で有意

$$\ln(BBS2)= \ln(a_0)+b_1 \ln(L)+b_2 \ln(D)+b_3 \ln(Iw)+b_4 \ln(Ch)+ b_5 \ln(Pc) + b_6 \ln(U)+b_7 \ln(Id)+ b_8 \ln(PD)$$

$$=0.634+0.275 \ln(L)+ 0.022 \ln(D) +0.088 \ln(Iw)$$
$$(0.493) \quad (2.209) \quad (1.257) \quad (2.228)$$
$$-0.173 \ln(Ch) + 0.407 \ln(Pc)+ 0.208 \ln(U)$$
$$(-2.624) \quad (3.556) \quad (2.422)$$
$$+ 0.092 \ln(Id)-0.107 \ln(PD)$$
$$(2.181) \quad (-0.796)$$

自由度調整済みR^2=0.932

結果(2)のｔ値をみると、料金の影響力は小さいと推定できたので、料金にかかわるすべての説明変数を排除し、再度回帰を試みた。

表 2.3　結果(3)

BBS3		
定数項	0.110	
L	0.279**	(0.124)
D	0.026	(0.018)
Iw	0.093**	(0.039)
Pc	0.473***	(0.080)
U	0.190**	(0.083)
Id	0.105***	(0.038)
Ch	-0.164**	(0.065)
PC		
PD		
PF		
R^2	0.943	
AdjustedR^2	0.933	
N	47	

(　)は標準誤差

***1%水準で有意　**5%水準で有意

$$\ln(BBS3)=\ln(a_0)+b_1\ln(L)+b_2\ln(D)+b_3\ln(Iw)+b_4\ln(Ch)+b_5\ln(Pc)+b_6\ln(U)+b_7\ln(Id)$$

$$=0.110+0.279\ln(L)+0.025\ln(D)+0.092\ln(Iw)$$
$$(0.100)\quad(2.251)\quad(1.459)\quad(2.381)$$
$$-0.165\ln(Ch)+0.473\ln(Pc)+0.190\ln(U)+0.105\ln(Id)$$
$$(-2.544)\quad(5.933)\quad(2.304)\quad(2.730)$$

自由度調整済みR^2=0.933

結果(3)では料金を全て排除したが、R^2(0.933)は高い数値を示し、各説明変数の t 値も改善された。結果(3)が最も安定的であった。一連の分析から、拙稿のなかで以下のように結論づけた。

- 既存ネットワーク（固定電話）の充実度である L は 5%水準で有意。
- 人口集中度の指数である D は機能せず。
- 情報通信産業規模を示す Iw はほぼ 5%水準で有意。
- 設備型競争 Ch は、5%水準で有意。
- Pc は 1%水準で有意。
- 利用者の情報機器操作能力 U は 5%水準で有意
- Id は 5%及び 1%水準で有意。
- アプリケーション・コンテンツはブロードバンドの補完財となる。
- 料金の市場への影響力に翳りがみえる。

3. 相関行列主成分分析によるアプローチ

続いて相関行列主成分分析（以下、主成分分析という）を試みた。パラメータは回帰分析をもとに表 3.1 を採用した。

表 3.1 基礎データ

件数 47

	合 計	平 均	標準偏差(n)	標準偏差(n-1)
L	276.4791	5.882535	0.078288	0.079134
D	273.0652	5.809897	0.973632	0.984159
Iw	95.51776	2.032293	0.497048	0.502422
Pc	321.3254	6.836711	0.156141	0.157829
U	224.0157	4.766291	0.277681	0.280683
Id	64.20334	1.366028	0.436119	0.440834

表 3.2 は、表 3.1 パラメータ同士の相関行列を示す。

表 3.2 相関行列

	L	D	Iw	Pc	U	Id
L	1	0.1485	0.1243	0.0060	0.1341	0.3231
D	0.1485	1	0.7793	0.4378	0.8221	0.7335
Iw	0.1243	0.7793	1	0.5394	0.8355	0.7885
Pc	0.0060	0.4378	0.5394	1	0.6606	0.5272
U	0.1341	0.8221	0.8355	0.6606	1	0.7439
Id	0.3231	0.7335	0.7885	0.5272	0.7439	1

表 3.3 の主成分累積寄与率はいずれも 60%を超えている。

表 3.3 固有値

主成分 No.	λ	寄与率(%)	累積(%)
1	3.82	63.63	63.63
2	1.03	17.23	80.86

表 3.4 から導かれる固有ベクトルをグラフ化し、主成分の解釈を試みる。

表 3.4　固有ベクトル

	主成分 1	主成分 2
L	0.1201	-0.9295
D	0.4496	0.0099
Iw	0.4676	0.0647
Pc	0.3572	0.2989
U	0.4795	0.1054
Id	0.4552	-0.1767

図 3.1 の主成分は全てプラスを示しており、したがってこれは総合力を意味している。

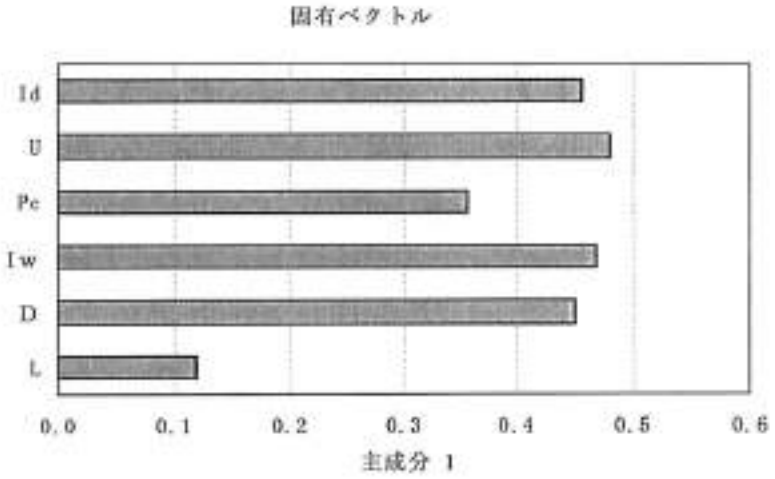


図 3.1　主成分 1 の固有ベクトル

つぎに図 3.2 に示す主成分 2 のベクトルをみると、各パラメータがプラスとマイナスに分かれている。マイナスを示すパラメータ L, Id の性質からこれを「インフラ型」とする。対してしてプラスは、人為的要素の色彩が強く、これを「ユーザー型」とする。

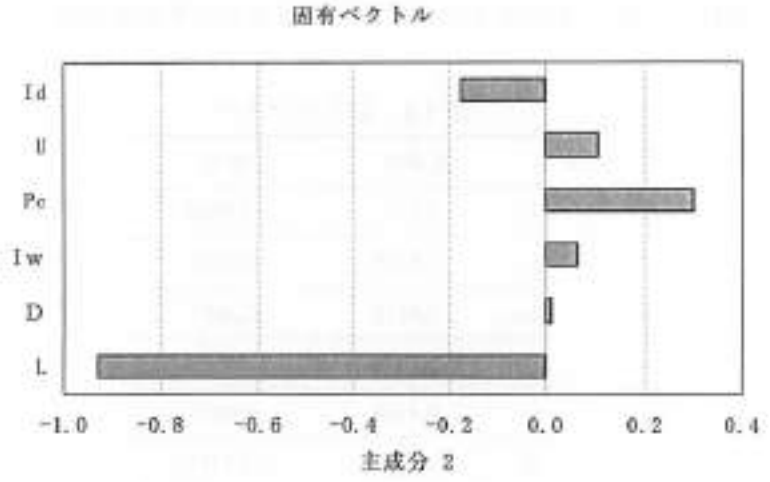


図 3.2　主成分 2 の固有ベクトル

図 3.3 は固有ベクトルを点グラフとして各パラメータを散布したものでる。これをみると、両主成分の関係性が分かる。全てのパラメータはブロードバンド普及にあたって総合的に影響を及ぼし、かつパラメータの特性によって、影響力の発揮が異なる。インフラとしての機能は L に大きく影響されている。これは、このデータ収集の時点(2005 年)においてはブロードバンド・アクセス回線として DSL が優勢であったと推定される。

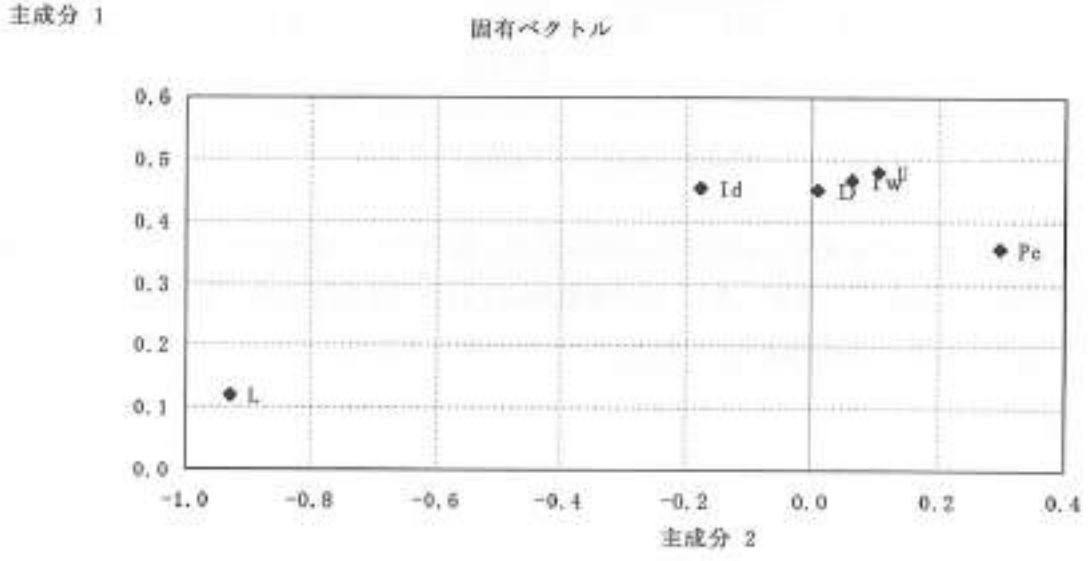


図 3.3　固有ベクトル散布

主成分 1

主成分得点

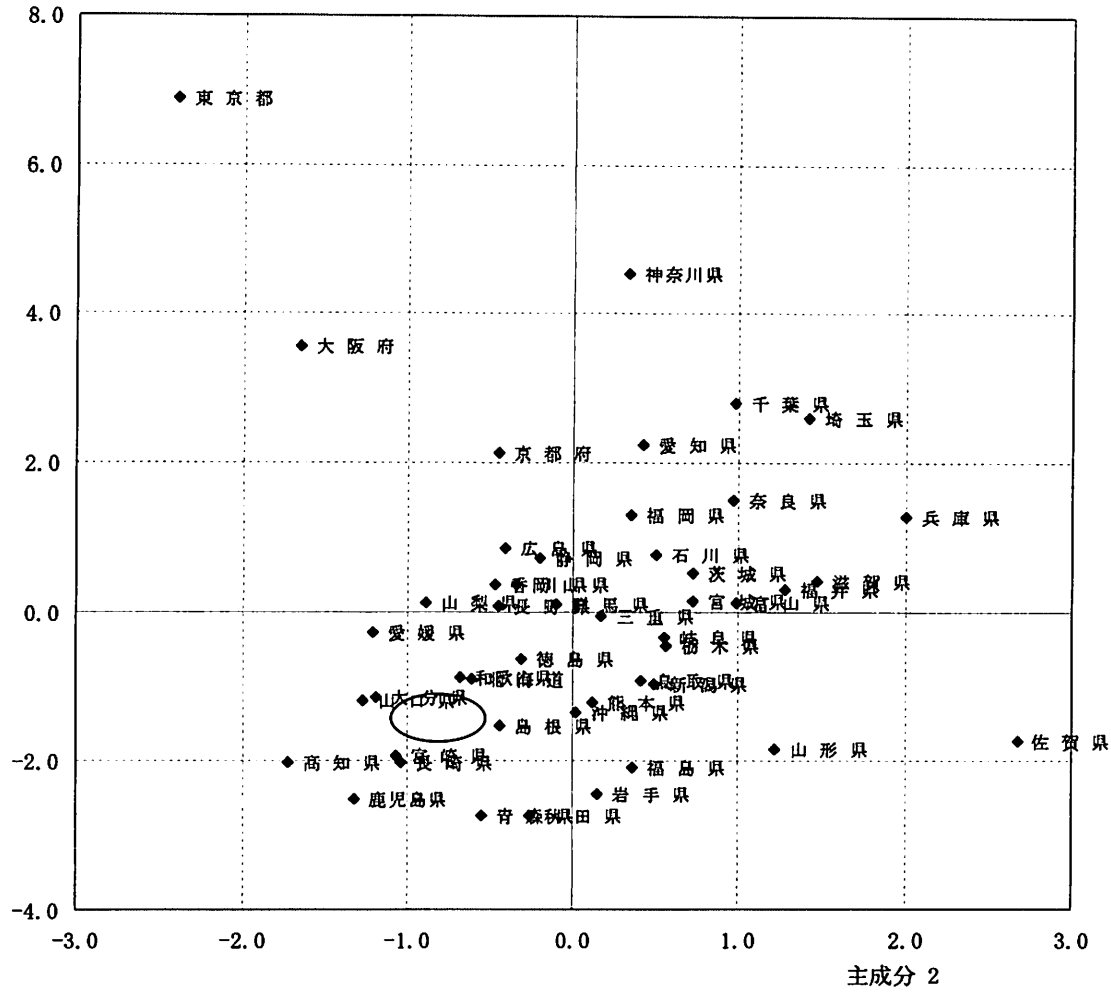


図 3.4　主成分得点表

4. 総　論

主成分分析は記述統計のなかでも非常に分かりやすい得点分布を作成できるので、これまでの結論として以下のことが推定できる。

図 3.4 をみると明らかなように、ブロードバンド普及について、大都市圏が進んでいることがわかる。それは主成分 1 の得点が示している。前述のように主成分 1 はブロードバンド普及の総合力であり、この得点が高いことはその普及が進んでいることを意味するからである。これを踏まえると、東京、神奈川、大阪、愛知、京都及び首都圏近郊、福岡、広島などでブロードバンドの普及力が総合的に高いといえる。

一方、大分県を省察すると、図 3.4 中の○を記したエリアに位置している。本分析から捉えると、大分県のブロードバンド普及の総合力は全国で中位に位置しており、かつ、普及に影響しているのは、インフラの整備が大きいと推定できる。そのひとつの要因として、ここ数年、自治体

が高速大容量ネットワークを政策的に整備してきた点を挙げていいだろう。本分析に基けば、大分県のブロードバンド普及を促進するには以下の方策が適当である。

・ユーザーの利用促進や高度な利用を牽引するための教育の実施

・情報ネットワークの倫理意識の高揚

・情報通信産業に関する雇用促進

いずれにしろ、大分県においては、主成分 2 で提起したところのソフト面（ユーザー型）の情報化対応を心がける必要がある。

註

[1] 拙稿「ブロードバンド普及要因の分析と推計に基づく政策インプリケーション」『開発技術』第 14 巻、1－22 ページ。開発技術学会、2008 年 6 月 26 日。

[2] Garcia-Murillo M. and Gabel D.、Kim, Jung-Hyun, Johannes M.Bauer, and Steven S. Wildman,などが主な先行研究である。

[3] International Telecommunication Union (ITU), *ITU Internet Report: Birth of Broadband,* ITU, 2003.

[4] Japan Registry 社。日本のドメイン名である"jp"ドメイン名の登録管理と、ドメインネームシステム(DNS)の運用を行っている。

[5] CATV,DSL,FTTH の各契約者数をブロードバンド契約者数合計（FWA を除く）で除した値を%（パーセント）表示し、その各自乗値を合計した。

参考文献

依田高典『ネットワーク・エコノミクス』日本評論社、2003 年。

鬼木甫「広帯域通信インフラ整備のエコノミクス」、増田祐司・須藤修『ネットワーク世紀の社会経済システム－情報経済と社会変化』富士通経営研修所、1996 年。

財団法人国際通信経済研究所『主要国・国際機関における情報通信の現状と動向』財団法人国際通信経済研究所、2003 年。

田尻信行「日本におけるブロードバンドの普及要因及び政策の役割等に
関する研究調査」『2006 年度電気通信普及財団研究報告書』電気通信普及財団、2006 年。90-96 ページ。

永松利文「ブロードバンド普及要因の分析と推計に基づく政策インプリケーション」『開発技術』第 14 巻、1－22 ページ。開発技術学会、2008 年 6 月 26 日。

林紘一郎「ネットワーク産業の競争と規制」林敏彦編著『講座・公的規制と産業電気通信』 NTT 出版, 1994 年。

Frances Cairncross, *The Death Of Distance. How the Communication Revolution Will Change Our Lives,* Harvard Business Press, 1998.

Garcia-Murillo M. and Gabel D., International Broadband Deployment: The Impact of Unbundling, Paper Presented at The 31st Research Conference on Communication Information and Internet Policy in Arlington, VA, United States, 2003.

International Telecommunication Union, *Internet Reports: Birth of Broadband,* September 2003.

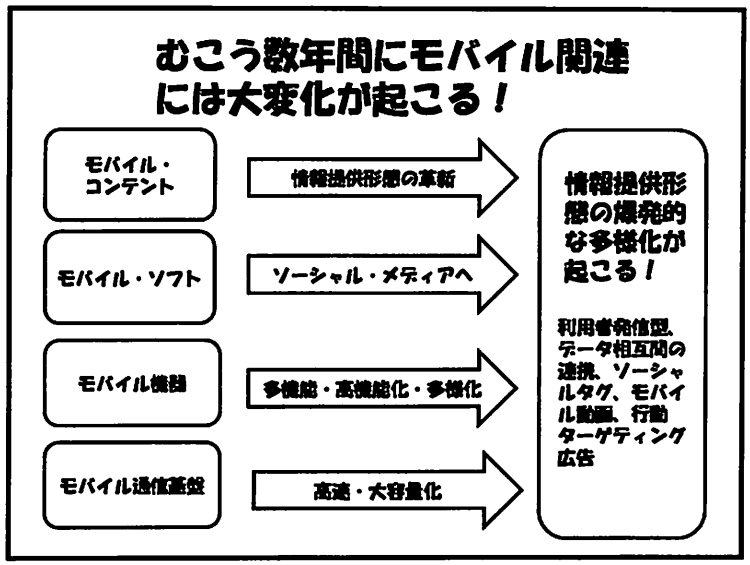
Schmalensee, R., *Product differenciation advantages of pioneering brands,* The American Economic Review, 1982.

大分市中心市街地におけるモバイルサービスの検討

ハイパーネットワーク社会研究所
共同研究員　藤野　幸嗣

ハイパーネットワーク社会研究所では大分商工会議所から中心市街地活性化計画の一環として、大分市の中心市街地において、モバイルを活用した活性化計画についての調査委託を受けました。このレポートはその調査報告の概要です。

１．モバイル基盤の高速化やケータイの多機能化が進んでいる。



豊富な地域情報を利用者が持っている端末に提供をすることが可能になりました。しかし、数年間でケータイの通信基盤は３．５世代から３．９世代、第４世代へと相当に早い段階で通信手順が変わっていき、端末にも大きな変化が起こる可能性があります。一方で２００９年の時点ではパケット通信料は月額５０００円程度であり、ケータイの主な利用層である若年層以外ではケータイによるデータ通信がそれほど普及をしている状況ではありません。また既存の無線ＬＡＮサービスの普及や次世代の無線ＬＡＮサービスなども出現しており、どのような通信サービスがこれから主流になるのか見通すこともできない状況となっています。

モバイル機器も、高機能、多機能化したケータイ、スマートフォンといわれる、よりパソコンに近い機能を持ったケータイ、PDA といわれる手軽に持ち運びができる情報機器の普及、パソコンもネットブックといわれる軽量化したノートパソコンなど、様々な機器が登場しており、利用頻度や用途に応じて利用者は賢く使い分けています。

モバイル機器における情報のやりとりの主流は、もともと電子メールによる利用者間のコミュニケーションとＷｅｂによる情報検索が主流でしたが、端末機器が高機能化したこと、Ｗｅｂ検索の急速な普及、ブログやＳＮＳなど利用者発信型サービスの登場などにより、コミュニケーション利用がメインとなっていて、さらにこうしたサービスを上手に使いこなして利用者相互間のコミュニケーションを促進するための活用法が主流になっており、ソーシャルつまり「社交」の目的で使われることが次第に多くなっている状況が顕著になっています。

こうした利用者同士の相互活用が主流になり、メールマガジンやＷｅｂを使った情報提供が利用者に訴求する効果は相対的に低くなっている傾向があります。また情報の量が多くなっており、いくら情報を出しても利用者が見てくれないという状況も起こっています。

こうした状況を打破するためには、新しいコミュニケーション活用シーンに合わせて、提供側も積極的に新しいコミュニケーションサービスを活用して、適切に情報を提供できるように努力

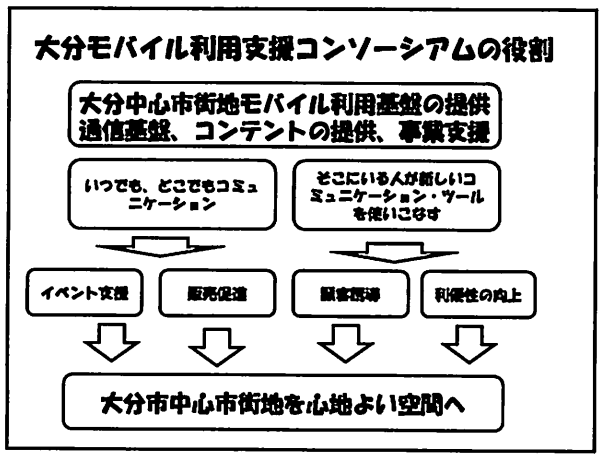
をしていかなければなりません。一方でこうした新しいコミュニケーションシーンにむけて適切な企業広告を提供するための技術や代理店サービスも登場しはじめています。

我が国のモバイル利用は、若者を中心にこれまでの一方的な情報提供とは異なる豊かなコミュニケーションをとろうとする世界が形成されようとしています。大分市の中心市街地活性化のためには、こうしたソーシャルなコミュニケーションを促進するための利用基盤の提供、適切なコンテントの提供、そうした事業を支援するためのスキーム作りが必要です。

まず中心市街地で事業を行っているセクターが新しいコミュニケーションツールを使いこなす、そうしたことを支援できるようにコンソーシアムを形成するなどの措置をとるが中心市街地活性化の前提として必要だと思われます。

2．大分市中心市街地の課題

大分市中心市街地の課題として、商業機能の衰退、高齢化（事業者・来訪者）、モータリゼーションへの対応（駐車場問題）、空店舗・空き地の増加などがあげられていましたが、さらに大分駅の高架に伴う交通体系の変化も加わりました。調査では「中心市街地」というものを単なるモノを買ったり消費をしたりする場ではなく、人々がそこで仕事や生活を行い、そして交流の場として街が本来の機能を活性化するための手段としてネットの活用を提案するものだと考えました。



それで単なる物販の支援や、クーポンの配布を行うことだけでは、確たる成果があがらないのではないものと予測をしています。

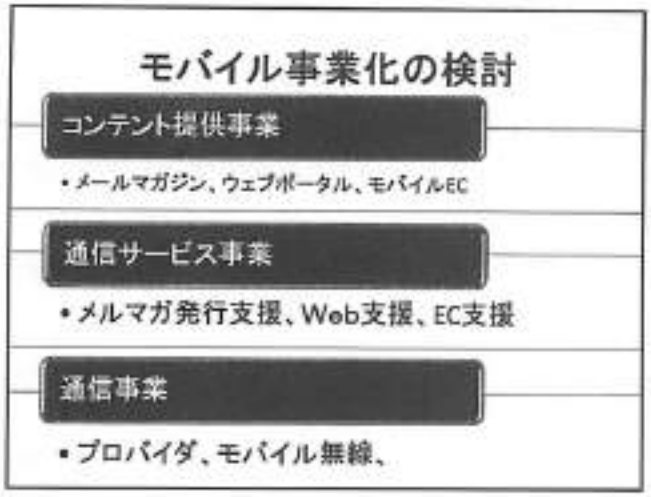
大分市の中心市街地がこれから長い目でみて、本当に発展していくためには、仕事の場としての機能と、買い物などの生活の場としての機能、そして何よりも本来の中心市街地の機能である、交流する場としての機能が、モバイルツールやネットをうまく活用することによってバランスよく、活性化できるかということが大切だと考えたからです。

この１０年間の間には、ブロードバンド（高速）よるインターネット利用と高機能・多機能な携帯電話、いわゆる「ケータイ」によるネットの利用が急速に進んできました。しかし２００９年の現時点では、ケータイによるブロードバンドの普及が始まったばかりで通信規格も定まっておらず、サービス事業の形態もそれほど確立されていない状況ですが、さらに、むこう数年でこのケータイによるネットの利用、つまりモバイル通信環境が劇的に変わることが予想されます。

そこで、情報通信環境の変化が中心市街地の活性化プランにこれからどのような影響をもたらすのかという検討を行いました。

3．モバイル事業の検討

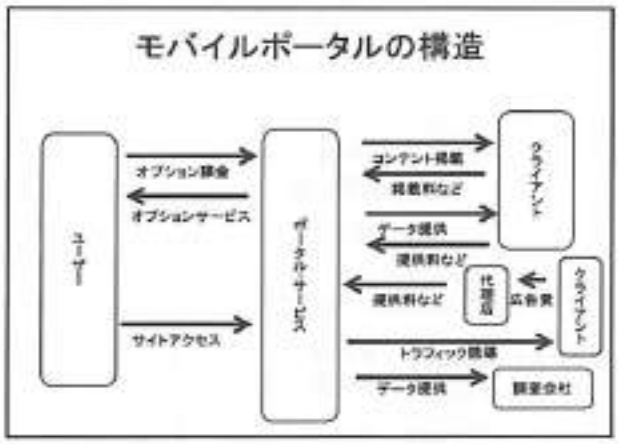
情報通信サービスの展開については、現時点での我が国のモバイル通信サービスは本格的普及期の手前という段階と見なさざるをえません、固定系の光ファイバー網やそれに先行したケーブルテレビ回線やＡＤＳＬ回線の普及がはじまる以前の段階という評価で、むこう数年でモバイル



サービスは飛躍的な高速化と高機能化がなされる可能性が高いこともあって、どういった技術が支配的になるのか見通すことが困難な状況です。また情報通信サービスについても既に個別のプロバイダが提供する状況ではなく、通信事業とサービスとが切り離されて提供されている現状を考慮すると、いまの時点で情報通信事業を中核とした地域の事業を展開することはリスクも高く、妥当性は薄いと観ざるをえないと言えます。

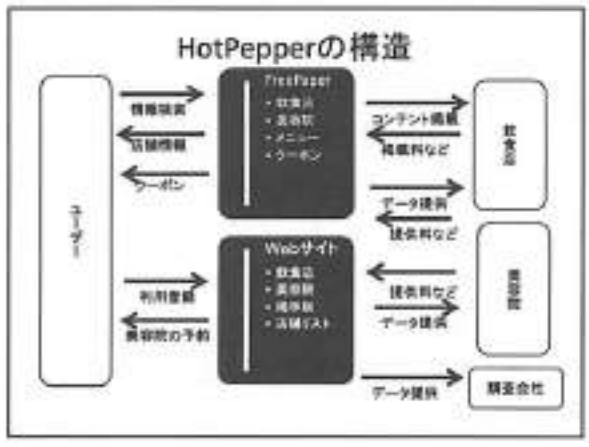
もちろん、利用者を十分に集める可能性があるなら（分岐点は数万人程度？）MVNO で展開をするという手法の可能性もまったくないわけではないですが、それだけの手間をかけて事業を開始する価値があるのかという点で疑問があります。通信事業の運営について、継続的な支援手段があるという前提ではじめて事業検討を行うのが妥当ではないかと思われます。

統合型地域ポータルサービスの展開



統合型のポータルＷｅｂサイトを、中心市街地の店舗を中心にして構築をして、利用者に情報の提供を行います。メールマガジンやジャンル別に分類された店舗紹介、クーポン券の配布や登録者へのメールマガジンの発行を行う方法、Ｗｅｂ１．０的なアプローチのサービスの展開です。

しかし、既にこうしたＷｅｂマーケティングの試みを個別にはじめている店舗もかなりあります。また「アイぶんぶんひろば」をはじめとして、「トスマップ」、モバイル特化型ポータルとして「ｉナビ大分」など地元メディアを中心として既にいくつかの地域ポータルの展開がなされています。こうした既にあるサービスをうまく活用するのが妥当ではないかと思われます。



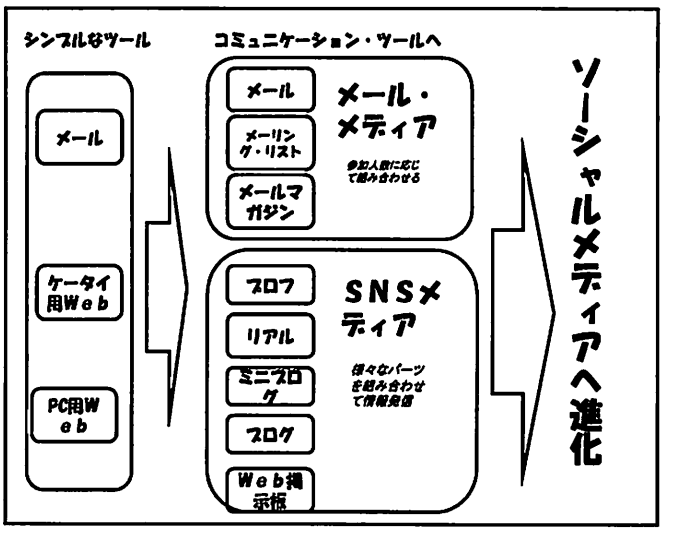
また全国的なサービスとして「ぐるなび」や「ホットペッパー」など飲食店のポータルサービスに既に登録をしている店舗も多く、新規に統合型ポータルサイトやメールマガジンを発行する余地も少ないのではないかと思われます。

４．モバイルサイトはソーシャルメディアへと変化する。

モバイル利用者は多機能ケータイやスマートフォン、パソコンなど異なった機器を使い始めており、情報の取得手段もＷｅｂからが主流になっていますが、利用方法は道具によって様々になっています。こうした急速なネットの進化によって、マーケティングの手法が変わってきておりＷｅｂとケータイの普及によって地域や年齢層、性別などターゲットを絞ったユーザーに対してダイレクトなコミュニケーションが取りやすくなっています。まず利用者側からウェブ上で見つけてもらえるようにする必要があります。モバイルについてはこれまでのキャリアの公式サイトやポータルサイトからのリンクから検索エンジンに容易に見つけてもらえるような情報の出し方の検討が必要です。

そして利用者から見つけてもらった後に良好な関係を築いていくための工夫も必要です。利用者が何を求めているのか細かく把握することも必要とされます。さらに利用者とのコミュニケーションの方法も利用者の環境にあわせて準備をしておく必要があります。少なくともメールマガジンをアクティブな利用者は敬遠しはじめているようです。ＲＳＳリーダー、PodCasting、動画によるプロモーションなのか、はたまたブログなのか、これまでのように幅広い層に向かって届けようとした一方通行のメッセージではもはや誰にも伝わない時代になろうとしています。

こうしたモバイルコンテントを取り巻く現状から、調査の結論としては早急なサービスを立ち上げるのではなく、それぞれの事業者に最適なマーケティングの手法をそれぞれのお店のスタッフにアドバイスするコンサルティングサービスが必要とされるように思われます。

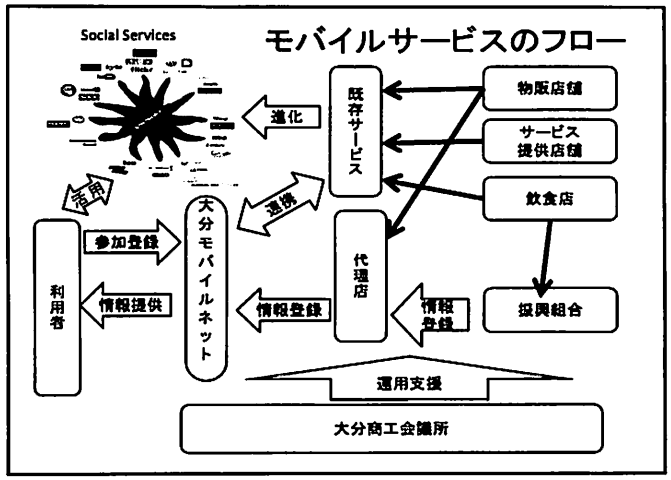


まずそれぞれの店舗＝クライアントがこうした新しいモバイル・ソーシャル・マーケティングの道具になれること、そしてそうしたツールが自分たちのビジネスにどう生かせるのか検討を行うことが必要だと思います。スタッフがブログを立ち上げる、ＳＮＳに参加する、Twitter でコメントを書いてみるなど、まず既存のソーシャルネットワーキングツールを使ってみることで、その可能性も見えてくるように思います。そうした実践を通して、各事業者がどのようにそうした新しいツールを使ってプロモーションやマーケティングを行えるのか検討をおこなわなければなりません。ブログにしても、数年前に出現したときは、よくわからないものでしたが、いまやホワイトハウスでもブログで情報を出す時代になっています。

利用者も情報が増えるにつれ次々と新しいサービスへと移っていきます、ソーシャル・マーケティングは人がいるところで行う必要があります。

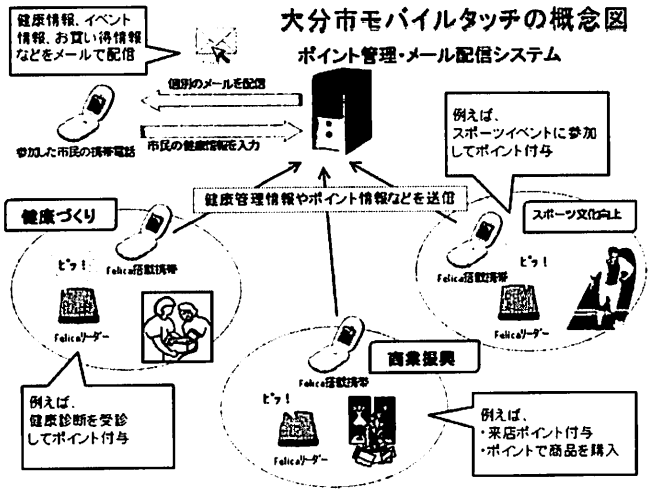
モバイルによるソーシャルネットワーキングサービスはこれから数年の間に急速に普及をする可能性が高いと思われます。２００９年の今の時点では、そうした動きをウォッチして、時代の波をうまく捕まえられるように、体制を整えておく段階だと思われます。

当面の準備として、専門家を招いたセミナーの開催や、ＵＳＡを中心にして急速に始まっている新しいソーシャルサービスを使いこなしておく必要があるように思われます。また地域でのまとまった事業については後追いで十分ではないかと思われます。今の段階ではモデル的な成功事例を見いだしていくことが重要だと思われます。



こうした潮流をみる限り、むこう数年の間にモバイルとネットを活用した新しいソーシャル・マーケットの時代が訪れることを見越して、中心市街地全体でそうしたあたらしい交流ツールを使いこなしていけるように準備をしておかなければならない時期だと思います。

導入の初期段階としては、普及がはじまったお財布ケータイを活用して、健康づくり活動やスポーツ振興などとからめて、店や商店街毎のメーリングリストや来店ポイントの運用が出来るサービスの検討が望ましいのではないかと思われます。



「私」中心の Web と OpenID, OAuth

近畿大学産業理工学部　情報学科
教授　山崎　重一郎

1．背景と概要

本報告書では，OpenID や OAuth に代表される個人中心型の web アイデンティティ技術とその応用についての解説を中心に報告する．社会情報基盤の一つとしての電子認証，認可の重要性は以前から指摘されてきた．電子認証や認可に関わるセキュリティ技術，電子署名法などの法整備，公的個人認証に代表される社会情報基盤の整備などについてもすでに多くの努力が行われてきた．そのような従来の電子認証認可基盤技術の典型として PKI や SAML を挙げることができる．

しかし，OpenID や OAuth などの個人中心型の Web 認証認可技術は，こういった従来の認証認可基盤技術とは対照的と言って良いほど直交する開発動機を持っている．これらの違いの本質を理解するためには，機能的視点だけではなく web の時代的な変遷とそれと同期する我々自身の「アイデンティティ」に対する意識の変化の視点から理解することがより自然である．

本報告書では，まず PKI，SAML，OpenID/OAuth の主な用途によってこれらの間の相違点を明確化した上で，web の進化に伴うアイデンティティの概念の変遷について解説する．次に個人中心型の Web 認証認可技術の実現方法という観点から，XRI，OpenID ，OAuth の技術的特長について解説を行い，仮名とペルソナに基づくプライバシ保護技術とその問題点について議論する．また，この議論の中でプライバシ保護を行いつつ個人の情報資産を AI 関連技術などを駆使した高度な web マーケティングに利用する方法について解説する．

2．PKI，SAML，OpenID/OAuth の主な用途

PKI，SAML，OpenID/OAuth のそれぞれの主な用途からその相違点を明らかにする．この三例は，後で述べる web 進化の三段階にそれぞれ対応する．

2.1. PKI の主な用途

PKI の主要な目的は，電子申請届出，電子決済，電子契約などにおける法的責任を担保できる信頼できる主体を構成することにあり，その主要な用途は，法的に効力を持つ電子署名である．PKI におけるアイデンティティは，国家や大企業などによる認証機関（CA）を信用の起点とする信用の連鎖の暗号的な構造体系と電子署名法による法的枠組みの中に個人の存在を埋め込むことによって実現される．（図１参照）

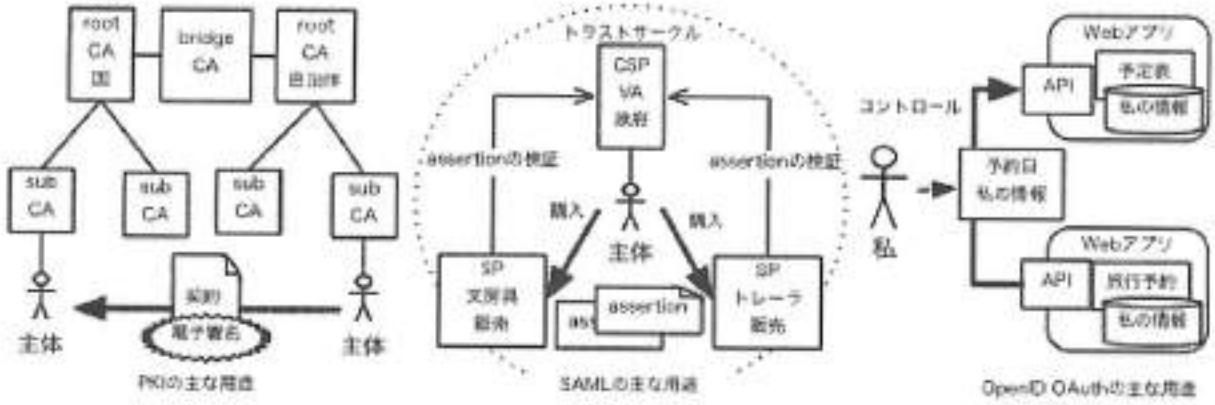


図 1　PKI、SAML、OpenID/OAuth の主な用途

2.2. SAML の主な用途

SAML の用途の典型例としては，米国連邦政府のシングルサインオン型の電子調達システムの基盤である e-authentication を挙げることができる．e-authentication は「消しゴムからトレーラーまで」をキャッチフレーズにする電子調達システムで，連邦政府の職員が「消しゴム３個とトレーラー５台の購入」というような操作を一度のログインのみで一括して実行できるシングルサインオンシステムである．この認証と認可のシステムは，連邦政府職員というアイデンティティと文房具会社や自動車会社との間にトラストサークルと呼ばれる認証と認可とポリシに関する相互承認関係が結ばれており，SAML によって標準化された XML 形式のアサーションによってそれらの正当性を web サービス間で自動的に検証できる仕組みを備えることによって実現されている．（図１参照）

2.3. OpenID, OAuth の主な用途

OPenID や OAuth などの個人中心型の Web 横断的な認証認可技術の主要な用途も SAML と同様にシングルサインオンであるが，両者はかなり様相が異なる．

OpenID, OAuth の主要な目的は，web 上に分散した自分の情報を自分でコントロールできるようにすることである．（図１参照）

図 2　OpenID OAuth による複数ガジェットへのシングルサインオンと連携の例

OpenID, OAuth が対象とするシングルサインオンの典型例として，Google 社が提供しているiGoogle ガジェットを使ったユーザのブラウザ上の複数のガジェット型 web アプリケーションへのシングルサインオンを挙げることができる．(図２参照) この環境でユーザがブラウザを起動すると，一つのブラウザ画面上に複数の小さなガジェット型の web アプリケーションが配置され，それらに対して一斉にログインが行われるという形でシングルサインオンが実施される．

この環境におけるガジェット間連携の典型的なシナリオとしては，航空会社のガジェットを使って航空機便を予約すると，その日時や便名や行き先などの情報が自動的に別のガジェットの個人予定表に登録されるという例を挙げることができる．

この連携はさらに，航空機便予約情報と社内の出張申請ガジェットへの連携や出張先ホテル近隣の飲食店の推薦ガジェットへの連携などへも発展させることができる

３．Web3.0 時代のアイデンティティ

2007 年 4 月にネット上で行われた”Define Web3.0 Contest” で勝者として選ばれた Robert O'Brien は，web の進化を次のような象徴的な言葉で表現している．

Web 1.0 = Centralized them
Web 2.0 = Distributed us
Web 3.0 = Decentralized me

web の３つの時代は，それぞれ次のように説明することができる．

3.1.Web 1.0=集権的な彼ら

“Web 1.0 = Centralized them.” とは，web コンテンツの生産者の中心がコンテンツ産業であったの時代を象徴している．この時代の web コンテンツはマスメディア，音楽産業，映画産業，ソフトウェア産業，ショッピングモールなどといったユーザから見た「彼ら」が生み出すものであった．注意すべきことは，この web1.0 のモデルが完全に過去のものではなく，現在も発展を続けているということである．例えば，音楽産業のネットストアは現在も発展を続けており，テレビ局のネット企業化なども今後の進展が期待できるものである．

3.2.Web 2.0 = まき散らされた私たち

“Web 2.0 = Distributed us.” とは，Web コンテンツの生産者の重心がコンテンツ産業側から「私たち」の側に移動した時代を象徴している．ブログ，SNS，動画や写真の投稿などに代表される web コンテンツ生産者のコンシューマ側へのシフトは CGM (Consumer Generated Media) という言葉でも表現される．また「私たち」が創造したコンテンツは個人のパソコンのハードディスクの中にではなく，多数の Web アプリケーションサーバ側に膨大な情報資産として蓄積されるようになった．web アプリケーションも Web API として公開されることによって，他の web アプリケーションから Mash-up や SaaS などとして機能レベルでの利用も可能になった．

しかし，現状では運営主体が異なる web アプリケーション間で蓄積された情報資産を適切に相互流通させることは困難であり，情報を統合的に利用できる事例はまだ限定的である．このような状況は，まさに「私たち」の情報が断片化され多数の web アプリケーションにまき散らされて

いることを意味している．また，Web2.0的なコミュニケーションは，これまでにない規模の強力なスケーラビリティを持っている．例えばSNSやTwitterのようなツールを利用すると，一人の人間が数100人の友人とリアルタイムに近い親密な関係を維持することも不可能ではない．しかし，このような大規模なコミュニケーションを適切にコントロールするための手段はまだ貧弱であると言わざるを得ない．「web2.0的アイデンティティ」には，このようなwebを媒体にした非常にスケールの大きい個人的なコミュニケーションの主体という意味も含んでいる．

3.3.Web 3.0=非集中的な私

"Web 3.0 = Decentralized me." という表現は，webの未来像を予測する言葉であるとともに，個人やweb企業の将来のwebに対する願望を象徴する言葉でもある．この表現の中の"Me"という言葉は，「私」がこの新しいwebのパラダイムの中心であることを象徴している．また，"Decentralized"という言葉は，これまでweb上にまき散らされていた情報資産の断片の統合化への期待が込められている．つまり，"Decentralized Me"とは，Web 2.0のトレンドの中で多数のWebアプリケーションの中に断片としてまき散らされてきた「私たち」の情報資産を，今度は「私」を中心にして統合的にコントロールできるようになることを意味している．また情報資産だけでなく，webを介したコミュニケーションにおいても，「私」の世界に踏み込む者を選択したり，放っておいてほしいときには，「私」へのアクセスを限定することができるように自分でコントロールしたいという願望をも表している．

web3.0に対するweb企業の期待という観点でも，複数形の「私たち」から単数の「私」へという精度の違いは重要である．各個人の人間関係や状況などを含む「私の断片」の情報を利用できれば，従来のポイントサービスなどによる顧客行動の把握などよりも遙かに生々しい情報を収集することが可能になり，これにAI技術を駆使することによってさらに効果的で高精度な商品の推薦などを行うことが期待できる。

4．web世代とアイデンティティ認証モデル

以上に述べたweb世代におけるアイデンティティの典型についての要点を整理し，それぞれの認証モデルとの対応を示す．ただし，以下の分類に登場する認証技術はそれぞれのweb世代における開発動機と基本的な設計思想に基づく典型としてのものであり，技術そのものの限界に基づくものではないことに注意が必要である．さらに，どの認証技術も現在も発展を続けており，それぞれの機能や関連技術との関連の視点でみると，それぞれが互いに同等の要求を実現する手段を備えていることに注意されたい．

4.1.web1.0的アイデンティティの認証モデル

web1.0的アイデンティティとは，典型的には企業や公的機関など「彼ら」のサービスの中に受動的に埋め込まれたエンドユーザとしての個人である．web1.0的アイデンティティの認証モデルとは，PKIやKerberosやLDAPなどに代表されるように，明確なアクセス管理のポリシを持ったサービスのドメインの構造的信頼関係の中に個人の存在を位置づけるものである．このような「固い」アイデンティティの実現は認証の基本であり，その重要性は現在も今後も変わらない．企業のイントラ，電子商取引，電子政府，電子決済，電子契約，音楽などのコンテンツ配信などを目的とするアイデンティティ管理には，明確な信用の構造の中に明確な形で個人が埋め込まれる

web1.0 的アイデンティティが適している.

4.2. web2.0 的アイデンティティの認証モデル

web2.0 的アイデンティティは，SNS や Twitter などによるコミュニケーション行い，写真や動画を web サイトで共有し，商品やホテルのサービスなどの口コミを登録する「私たち」である．web2.0 的アイデンティティの認証モデルは，一定のドメインに属している個人を対象に関連する web サービス相互の信頼の輪の中で認証や認可を行うものである．web2.0 的アイデンティティの認証認可システムの例として， Google Account Authentication や Flickr Authentication API や SAML2.0/Lierty Alliance などを挙げることができる.

web2.0 的アイデンティティの特長は，受動的な web1.0 的アイデンティティとは対照的に能動的に web 上で行動する主体であるという点である．このような能動的なユーザの行動は，web 企業のマーケティングに積極的に活用されるようになっている．web 企業は，個人の購買行動や検索履歴や口コミなどの情報を積極的に合法的な手段で収集し，商品のリコメンデーションや売れ筋商品の把握などに活用している．web 企業側から見た web2.0 的アイデンティティには，このような有用な個人情報の蓄積を行う上での識別キーとしての機能を持つ．SOA などによる web サービスの連携や Mash-Up による web アプリケーション機能の利用や SaaS 型のビジネスアプリケーションの認証基盤には，web1.0 的な国家を基点とする信頼構造に埋め込まれたアイデンティティに加えて，web2.0 的アイデンティティの認証モデルが必要となる.

4.3. web3.0 的アイデンティティの認証モデル

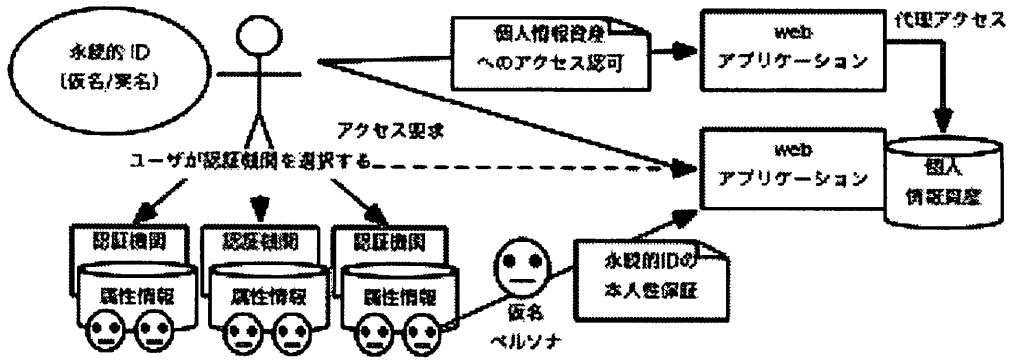


図 3 Web3.0 的アイデンティティの認証モデル

OpenID や OAuth のシングルサインオンには必ずしも SAML のような大規模な信用インフラを背景にしたアイデンティティは必要ない．例えば，自分の航空機便予約情報にアクセスしようとしている「私」が，カレンダの所有者である「私」でもあるということは，信頼できる第三者を介さなくても web 横断的に証明することが可能である．しかし認証認可システムとしての機能的な視点で見ると，OpenID や OAuth などの web 横断的な認証技術と SAML などのシングルサインオン技術は，使用するトークンの種類や内容においてもプロトコルにおいても類似点が多く，抽象化すれば基本的に認証認可の抽象モデル標準である NIST SP800-63 と同等の構造になる.

国家や企業への帰属よりも「私」というアイデンティティを第一義的な存在として中心に据え

る認証モデルを web3.0 的アイデンティティの認証モデルと呼ぶことにする．web3.0 的アイデンティティの認証モデルの特長を以下に示す．(図３参照)
この web3.0 的アイデンティティの認証モデルの大きな特長は，ID 管理の主体が認証機関とは独立していることである．このような，認証機関から独立した ID を「永続的 ID」と呼ぶことにする．

従来の認証システムでは，利用者の ID の名前空間は認証機関が定義していた．
web3.0 的アイデンティティは，同一の永続的 ID に対して，自分が利用するアプリケーションサービスに応じて適切な認証機関を選択することできる．例えば，他人のブログ記事へのコメントの書き込みを承認してもらうための認証機関と地域の介護情報共有サービスにログインのための認証機関では個人が認証機関に対して開示しなければならない個人情報の質も異なる．web3.0 的アイデンティティは，このような認証機関の選択を本人の意志の下で選択することができる．

このモデルにおいて，利用者が web アプリケーションサービスに対して提示するのは，自分の永続的 ID である．また，認証機関が web アプリケーションに対して本人確認後に証明するのは，利用者が提示している永続的 ID が確かに本人のものであるということである．この永続的 ID は，必ずしも実名である必要はなく，後で定義する「仮名」であってもよい．また，プライバシ保護のために複数の永続的 ID を必要に応じて使い分けてもよい．

しかし，web3.0 的アイデンティティも，他者に対して自分の権限の主張や証明を行おうとすると何らかの信頼の構造への依存が必要になる．
したがって，web3.0 的アイデンティティは，web1.0 的アイデンティティや web2.0 的アイデンティティとも無縁ではなく，むしろ相補的に結びつくことによって機能する．実際にリトアニア政府は２００９年１月より同国の国民 ID カードを OpenID に対応させ，国営の OpenID プロバイダサービスを開始しようとしているが，このような動向も web3.0 的認証モデルを補強するものであり矛盾するものではない．

５．永続的 ID とペルソナ

5.1. 個人や組織の時間的変化と永続アドレッシング問題

個人も組織も時と共に常に変化している．個人であれば，誕生，成長，死までの過程の中で，入学，卒業，就職，出向，転職，退職のような変遷を経験する．組織も新人，昇進，退職のような人事的な変化や改組による組織構造の変化や名称変更などを繰り返す．

永続アドレッシング問題とは，組織や個人の実体へのアクセス手段が時の経過とともに変わってしまったときにも，その組織や個人へのアクセスの一貫性が失われないようにしたいということである．
(図４参照)

5.2. XRI と i-name

XRI (Extensible Resource Identifiers) は，この永続アドレッシング問題の解決を目的とする ID 管理システムのための標準である．XRI は，DNS における IP アドレスとドメイン名の対応関係に似た二層構造を持ち，アイデンティティの実体とその名前をそれぞれ i-number と i-name という２種類の ID の対応関係として管理する．
XRI のシンタックスは次のようなものである．

xri://authority/path?query#fragment

ただし，'xri://' は省略することができる．

=names という構文は個人，@names という構文は組織，+names という構文は一般概念を表す．

5.2.1. i-number

i-number は，実世界での時間的変化に依存せずに個人や組織などに永続的に割り当てられる ID である．IP アドレスのように機械可読性を優先した構造を持つ．
一つの i-number は，常に同一のリソースを表し，決して再割り当ては行われない．

=!49B2.862C.E5FE　(個人の i-number)
@!1000.9554.fabd　(組織の i-number)

5.2.2i-name

i-name は，人間へのわかりやすさを優先した ID である．DNS のドメイン名のように長期にわたって個人や組織などに割り当てられるが，別の所有者に再割り当てを行うことも可能である．
i-name には所属やアクセス手段などの情報を付加することもできる．

=ichiro　(個人の i-name)
@kindai　(組織の i-name)

永続アドレッシング問題は，図 4 に示すように，主体自身には i-number を不変な ID として与え，時間の経過によって変化する ID を i-name として同一の i-number に再割り当てを行うことによって解決することができる．

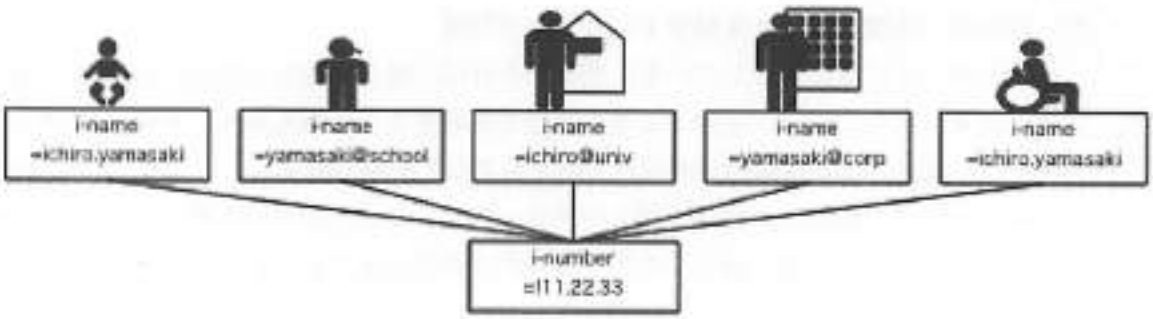


図 4　i-number への i-name の再割り当てによる永続アドレッシング問題の解決

また，i-name は，プライバシ保護の目的のために後に述べる「仮名」として利用することも可能である．

5.3. i-name の名前解決と XRDS による認証サービスの発見

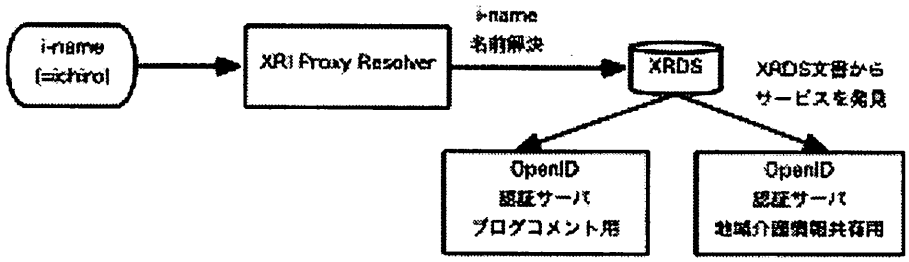


図 5　i-name の名前解決と XRDS による認証サービスの発見

i-name などの ID から認証サービスを発見するためのプロトコルが YADIS である．(図５参照) i-name の名前解決システムは，XRI プロキシリゾルバと XRDS 文書を格納する web サーバから構成される．i-name を与えられた XRI プロキシリゾルバは，まずその i-name の管理情報を格納している XRDS 文書を格納している web サーバを探し，そこから XRDS 文書を得る．XRDS 文書の内容には，その i-name を認証するために使用する認証サービスに関する情報が優先度付きで記載されている．この情報を参照することによって，OpenID 認証サーバが選択され認証が行われる．

このような抽象化は新しいものではなく，URN (Uniform Resource Name) や他の永続性識別子アーキテクチャも同じ効果を有している．World Wide Web の URI [RFC2396]の設計方針も，その一例であり，URI は，リソースの位置やアクセス手段を示す URL (Uniform Resource Locator) と永続的なリソースの名前を示す URN (Uniform Resource Name)[RFC2141]という二層構造として設計されていた．

5.4. 仮名と匿名

本稿における仮名と匿名の概念の違いを整理する．仮名(pseudonym)は，個人情報の開示を必要最低限にとどめるようコントロールするために使用される個人の識別名である．仮名は，EU の PRIME プロジェクトをはじめとするプライバシアーキテクチャの研究プロジェクトの中で中心的役割を果たす重要な概念である．(図６参照)

仮名を必要とする用途の典型例として，オンラインショップでワインを購入するときに自分の本名を明かさずに年齢が２０才以上であることを証明したいという事態を挙げることができる．

仮名は，実際に本人が持つ属性の部分集合を持ちその中に虚偽の情報は含まれない．一般に属性の正当性は信頼できる第三者を介して証明できる．例えば，ある仮名を使っている人の年齢が２０才以上であることを自治体が証明するというケースが想定できる．これに対して匿名は，本人の属性との関連が切り離された名前である．一般に，匿名から本人の属性にアクセスしたり属性の正当性の証明を行ったりすることはできない．

図 6　アイデンティティに対する仮名と匿名

web3.0 的アイデンティティの認証モデルの主要な特長は，個人の所属や認証機関から独立した永続的な ID を持つことである．web3.0 的アイデンティティの ID は，認証機関から与えられるのではなく，認証システムとは独立の外部の名前管理システムを使って定義される．この ID は，個人の卒業，退職，結婚，国籍変更などのような所属関係の変更や認証機関側の故障，停止やサービス廃止などのサービスの変更にかかわらずに一貫して存在する永続性を持つので，これを永続的 ID と呼ぶことにする．この認証モデルにおける OpenID プロバイダなどの認証機関の主な機能は，web アプリケーションに対してユーザの永続的 ID が正当なものであることを証明することである．ユーザは一つの永続的 ID を複数の認証機関を選択的に使って利用することができる．

永続的な ID は「私」の本名にあたる唯一の識別子を意味しないことに注意が必要である．むしろ複数の永続的 ID を用途によって使い分けることによって不必要な個人情報の暴露や他者からのコンタクトを防ぐことができる．「仮名（かめい）」とは，本人の「社会的な顔」を代表する名前のことである．仮名は匿名とは異なる概念であり，仮名を利用するためには認証機関による本人確認を必要とする．

仮名によって代表される「私」人格の内容にあたる属性情報は，認証機関によって管理される．この仮名によって代表される人格のことをペルソナと呼ぶ．ペルソナが持つ個人属性は本人が持つ情報の正しい部分集合であり，虚偽の情報は含まない．ペルソナは，ユーザの選択に基づいて必要に応じて認証機関から web アプリケーションに渡される．

web アプリケーション内に蓄積されている予定表，写真，利用履歴などの個人の情報資産を，本人のコントロールの下に他の web アプリケーションから利用できる．このとき，認可の主体も情報資産の所有者も「私」であるため，情報の流通は「私」の許可のみでコントロールされ，web アプリケーション間のトラストサークルへの所属などの信用構造は必要とされない．

6．OpenID

OpenID は，ユーザ中心型の認証モデルによる Web 横断的なユーザ認証システムである．

6.1.OpenID の主な主体

OpenID の基本モデルに登場する主な主体には次のものである．

- OP（OpenID provider）：認証機関
- RP（Relying Party）：web アプリケーション

・ UA (User Agent)：ユーザが使用する web ブラウザ

6.2. OpenID に使用する ID

OpenID では，次の 3 種類の ID を利用する

・ Claimed Identifier：ユーザの永続的 ID
・ User-Supplied Identifier：ユーザが RP に提示する ID
・ OP-Local Identifier：ユーザが OP で使用する ID

6.3. OpenID によるユーザ認証の流れ

OpenID による RP へのログインの典型的な流れを図 7 に示す.

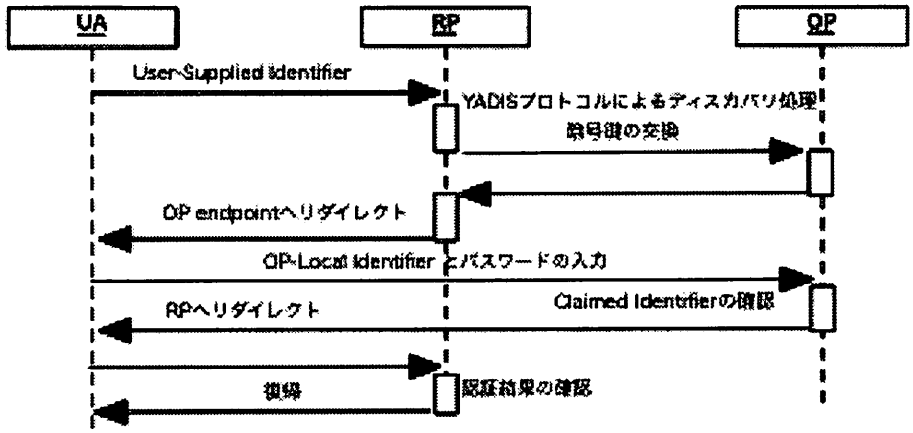


図 7　OpenID によるユーザ認証の流れ

（1）User-Supplied Identifier の入力

ユーザはブラウザから RP に対して User-Supplied Identifier を入力する．ここで入れることが可能な User-Supplied Identifier には，Claimed Identifier（ユーザの永続的な ID）もしくは，OP Identifier（OP を発見するための URL やドメイン名）が指定できる.

（2）YADIS プロトコルに基づく OP の Discovery 処理

RP は，ユーザから入力された User-Supplied Identifier を元に YADIS プロトコルを遂行し，OP のログイン処理を行う URL（OP Endpoint）を発見する.

（3）RP と OP の間の暗号鍵の交換

OP エンドポイントを発見すると，RP と OP の間でそれ以降の通信の暗号化と完全性保証のために Diffie-Hellman 法で暗号鍵を交換する.

この一連のプロトコルの結果として，ユーザはブラウザを介して OP のログイン画面にリダイレクトされる.

（4）OP でユーザ ID とパスワードを入力

ユーザは OP のログイン画面で自分の OP におけるユーザ ID（OP Local Identifier）とパスワ

ードを入力しOPはそれを検証する.

（5） OPにおけるClaimed Identifierの確認

OPにおけるパスワードの検証が成功した後に，アクセスしようとしているRPに対して提示する自分のID（Claimed Identifier）を確認する．このClaimed Identifierは，同じRPに対しての自己同一性を証明したい場合にはその後も同じものが継続して利用され，RP側もこのIDを記録し，同一のユーザであることを確認するために利用する.

（6）RPへリダイレクト

OPにおけるユーザの確認が完了すると，ユーザはOPによって再びユーザのブラウザ経由でRPにリダイレクトされ，一連の認証処理が完了する.

OpenIDには，いくつかの拡張機能があり，現在も改良が進められている．その一つは，OPが管理するユーザの属性情報をRPに開示するためのプロトコルで,SregやAXという仕様が存在する．また，OPの認証手段などのポリシ情報をRPとの間で交換するPAPEという仕様も存在する.

7．OAuth

webアプリケーションに蓄積された個人の情報資産を他のwebアプリケーションから利用できるようにする簡単な方法は，その情報資産にアクセスするためのユーザID やパスワードを当該webアプリケーションに預託してしまうことである.

しかし，そのようなパスワードや秘密鍵の預託は一般的に許されるものではなく現実的な方法ではない.

ユーザのパスワードを外部のwebアプリケーションに漏らすことなく，情報資産の所有者本人の承認に基づいてwebアプリケーション間で安全に流通可能にする技術がOAuthである.

OAuthによる情報資産へのアクセスの流れを図８に示す.

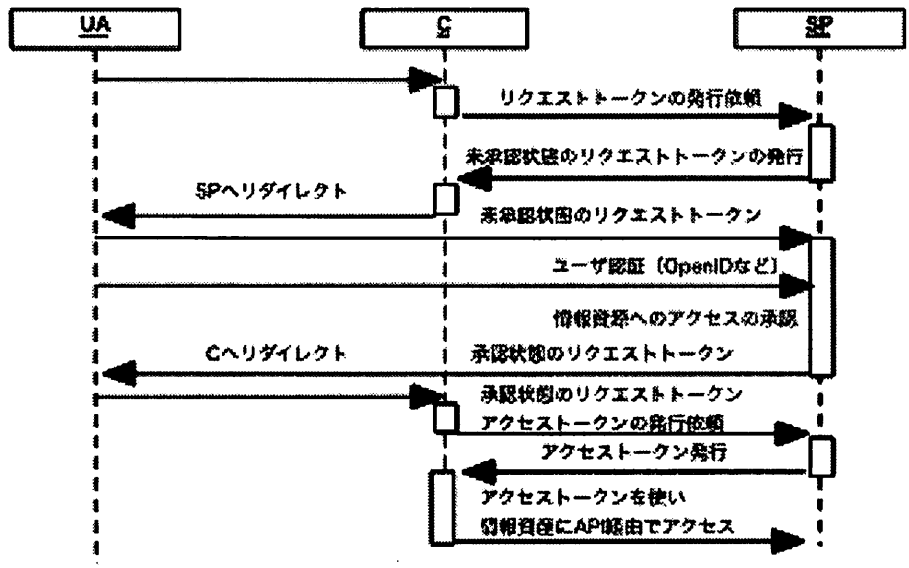


図 8　OAuthによる情報資産へのアクセスの流れ

2008年6月30日にGoogleがGoogle Data API でOAuthのサポートを開始した．OAuthは，認可に関する仕様であり，認証の方法については特に規程しないが，OpenIDは，OAuthの中の認証手段の一つになることができる．

7.1. OAuthの主な主体

OAuthに登場する主要な主体は次の２つである．

・SP（サービスプロバイダ）
・C（コンシューマ）

SPは，個人の情報資産を管理するWeb サービスであり，Cはその情報資産を利用しようとするwebアプリケーションである．OAuthでは，この両者の間には信頼関係が確立していることを事前条件としており，両者の間の暗号鍵交換などの作業はこの事前条件の段階で実施される．

7.2. Authに使用するトークン

OAuthでは，次の二つのトークンを利用する．

・リクエストトークン
・アクセストークン

リクエストトークンは，C がユーザから情報資産へのアクセス許可を得るために使用するデータである．リクエストトークンには，未承認状態と承認状態の二つの状態があり，ユーザが承認を与えることで未承認状態から承認状態に推移する．
アクセストークンとは，実際にSPのAPIを活性化して情報資産にアクセスするために使用されるトークンであり，C は承認状態のリクエストトークンを元にアクセストークンを得ることができる．この交換は一度きりであり，同じリクエストトークンで複数のアクセストークンを得ることはできない．

7.3. OAuthによる情報資産への認可の流れ

（1）リクエストトークン発行依頼

CがSPの情報資産にアクセスする必要が生じたときに，CはSPに対してその情報資産のリクエストトークン発行を依頼する．

（2）未承認状態のリクエストトークン発行

SPは未承認状態のリクエストトークンを発行しCに返送する．

（3）ユーザをSPにリダイレクトする

Cは情報資産の所有者の承認を得るためにユーザをSPにリダイレクトする．

（4）ユーザ認証とアクセスの承認

SP とユーザの間で認証が行われる．この認証手段は，OAuth の仕様の範囲外である．認証が成功すると，次にリクエストトークンの対象となる情報資産へのアクセスの承認をユーザに問い合わせる．

（5）リクエストトークンを承認状態にする

ユーザ認証とユーザによる承認が成功すると，SP はリクエストトークンを承認状態にして C にリダイレクトで返送する．

（6）リクエストトークンとアクセストークンの交換

C は SP に対して承認状態のリクエストトークンとアクセストークンとの交換を依頼しアクセストークンを獲得する．

（7）アクセストークンを使って情報資産にアクセス

C はアクセストークンを用いて SP の API 経由で情報資産にアクセスする．

8．ペルソナ

8.1. ペルソナとは

ペルソナとは，仮名によって名付けられ「私」の属性や関連情報のサブセットを保持する web 上の主体であり，典型的にはその人の社会的な顔を表す．ペルソナが持つ属性はすべて「私」が持つ正しい属性であり，虚偽の情報を含まないものとする．ただし，属性正しさについての明確な保証が必要であれば，それは外部の何からの信用システムや評価システムを利用して証明される．ペルソナは「私の断片」と言ってよいものであり，逆に多数の分散したペルソナをつなぎ合わせた全体の極限値が「私」であるということもできる．

ペルソナは単なるシンボルではなく，生きて生活している「私」の投影である．例えば，ペルソナの現在の緯度経度の位置情報があれば，それは現実の「私」が実際にそこにいる位置を表している．ペルソナの生活圏の気温が 35 度を超えていれば，「私」も暑さを感じていると推定できる．また，同じ情報が一日に繰り返し通知されると疎ましく思うといった具合にである．

ペルソナは，web アプリケーションサービスに対しては一貫性を持った一人の利用者である．そして，そのサイトに蓄積されている情報資産の所有者である．

また，web アプリケーションを介して情報資産へアクセスやそれを許可する主体でもあり，web アプリケーションを利用したコミュニケーションやインタラクションの主体でもある．すでに述べたように，ペルソナは，ユーザの同一性を証明するための永続的な ID を持つ．OpenID では，この永続的な ID が Claimed Identifier である．

8.2. プライバシ保護と個人情報の有効活用

個人が web アプリケーションを利用するときにペルソナを利用する主な理由は自分のプライバシを守るためであるが，一方で個人情報の開示や利用が本人にとってメリットを産む場合もある．その典型的な例は，本や商品の推薦などのリコメンデーションや検索などのサービスの個人へのアダプテーションである．つまり個人情報の保護と適切な有効利用のバランスが重要な要件であり，ペルソナはその両方にかかわる．

ペルソナにつけられる名称は仮名であり，実名とは切り離すことができる．もちろん実名を使わなければならない状況では，実名を含む仮名を使い分けることになる．OpenID プロバイダによっては，プライバシ上の配慮のために OP-Local Identifier と Claimed Identifier との対応づけを実質的に不可能にしているものがある．また mixi OpenID の OP では，Claimed Identifier の名前の構造を利用して，SNS における「X さんの友人の Y さん」という意味を持った ID や「Z というコミュニティの Y さん」という意味を持った ID を生成可能にしている．この mixi の例などを考えると，一人の人間が持ち得るペルソナの数は友人の数のオーダーに増える可能性があることがわかる．

8.3. ペルソナと AI 技術

ペルソナは単なるシンボルではなく生きて生活している．ペルソナは，現実の「私」が持つ属性のサブセットを持って私と共に行動している．例えば，ペルソナの現在の位置情報があればそれは現実の「私」が実際にそこにいる位置を表している，ペルソナの生活圏の地域で気温が 35 度を超えていれば，ペルソナも暑さを感じていると推定できる．もしその状態のペルソナに冷たいスイーツを推薦すると反応してくれる可能性が高い．

8.3.1. ペルソナによる協調フィルタリング

図 9　ペルソナによる協調フィルタリング

協調フィルタリングは，「この商品を買っている人はこの商品も買っています」というタイプの推薦を行うシステムである．
このようなシステムを構築するためには，商品ごとのユーザの購買状況の表を作成し，商品の組み合わせごとに商品間の距離を計算すればよい．(図 7 参照)
また，この表を縦に見れば，ペルソナの購買行動に関する類似度を表すものと見なすことができる．したがって，商品間の距離を求めるのと同様の方法でペルソナ間の距離を計算することによって購買行動が近いペルソナを求めることができ，さらに類似したペルソナの間で，一方のペルソナに未購買の商品があれば，その商品は推薦の候補としてよいであろう．

協調フィルタリングは，多数のユーザの集団的な行動からの推定を行う技術だが，ペルソナを利用すれば，さらにその個人特有の位置情報，人間関係，環境などの要因を複合的に組み合わることや，個人の行動の文脈を組み合わせることによって高精度の推薦が可能になる．このような推薦の高精度化においてAI技術への期待は大きい．

8.4. ペルソナを利用したコミュニケーションの効率化

100人の友人と24時間いつもつながりを持つことができるということは楽しいだけではない．人間だけではなく，広告や推薦システムから届くメッセージもいくら高精度で質の高いものであったとしても遮断したい場合がある．

ペルソナによる「断片化した私」に対する「私」の側の願望の一つは，私のこうした状況におけるコミュニケーションの効率化である．つまり，私の世界に誰が入って来られるのか，そこで何ができるのかを私がコントロールできるということであり，私を放っておいてほしいときには，そうしてもらえるということである．

現在のOpenIDやOAuthの技術だけではこの願いを実現することはできないが，「私」を数100のオーダーで断片化して制御することができるようなインフラが整ってくれば，このような意図に合致した技術への展望が開ける可能性がある．

8.5. 現実の私とペルソナの関係

ペルソナの属性は，現実の「私」の属性の変化に伴って変化する．現実の「私」が権限を失っているような行為をペルソナが実行できないように認可権限を管理することは，ペルソナシステムの基本となる．私が転職や退職などをすれば，ペルソナの関連した属性も連動して変化しなければならない．

8.6. ペルソナの使い分けによるコミュニケーションの効率化

100人の友人と24時間いつもつながりを持つことができるということは楽しいだけではない．また人間だけではなく，広告や推薦システムから届くメッセージもいくら高精度で質の高いものであったとしても遮断したい場合がある．ペルソナによる「断片化した私」に対する「私」の側の願望の一つは，私のこうした状況におけるコミュニケーションの効率化である．つまり，私の世界に誰が入って来られるのか，そこで何ができるのかを私がコントロールできるということであり，私を放っておいてほしいときには，そうしてもらえるということである．

現在のOpenIDやOAuthの技術だけではこの願いを実現することはできないが，「私」を数100のオーダーで断片化して制御することができるようなインフラが整ってくれば，このような意図に合致した技術への展望が開ける可能性がある．

9．ペルソナ利用の課題

これまでペルソナを「断片化した私」と表現してきた．

これはペルソナが私という実体の影であるかのような印象を与えるであろう．

しかしWebの世界においては，このペルソナの方こそが権限を持ったり行為の主体になったりする実像である．またWeb上での投票権や信用や評判や購入ポイントの小勇や会員ランクなどのステータスもペルソナに対して付与されるものである．

つまり現実世界の「私」の方がペルソナという「Web 上の身体」を介せずには何も行うことができない影のようなものであるということもできるかもしれない.

ペルソナの中には不要になったら捨てたり消去したりできるものではなく，切実な意味で「私」の一部であると考えるべきものがある.

そういう貴重なペルソナに関しては安易な利用を制限し，人権の観点からデリケートに扱われるべきものであるということへのルール化と社会的なコンセンサスの確立を進めるべきであろう.

また，現実の「私」はいつも健康で活動的でいるわけではない.

そのような「私」の健康状態や活動状態は何らかの形でペルソナにも影響が出てくることになるであろう.

そして，最終的に現実の「私」が生涯を終えた場合，すべての私のペルソナの状態を不活性化すべきである.

もちろん，死者のペルソナが持つ情報資産は生前と同じくデリカシを持って扱われるべきである.

１０．結び

本稿を執筆しながら頭の中にあったイメージは，ジョン・レノンの「イマジン」であった．国境もなく宗教もない世界の中に生きるアイデンティティという概念は，ジョン・レノンの時代には想像上のものでしか無かった.

しかしそれがいまでは，イデオロギーの類ではなく，web から航空券の予約情報の自分の web カレンダへの自動登録といったのような平凡な日常の一部として実現されようとしているということに感慨を持つ.

１１．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 ubiqui- 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.

TCPコネクション確立の偽装とその計数によるscan攻撃検知システム

大分大学学術情報拠点情報基盤センター　吉田　和幸
大分大学大学院工学研究科　大塚　賢治

サーバの使用状況や動作しているサービスの調査を行うscan攻撃が後を絶たない。scan攻撃の場合，宛先のアドレスをランダムに設定しコネクション要求を送るため、応答がないことが多い。このため、存在しないIPアドレスに対してコネクション要求を行なう回数を数えることでscan攻撃を検知することができる．しかしながら，検知したIPアドレスを単純にファイアウォールなどで止めた場合，TCP half open攻撃のように送信元のIPアドレスを偽装する可能性が高い攻撃に対して，問題が起こる可能性がある．そこで，TCPコネクション要求に対して送信元アドレスが偽装されていないか確認するとともに、コネクションが確立したか否かでscan攻撃を検知するシステムを試作した．本稿では、攻撃検知の方法と送信元の確認の効果について述べる

キーワード　IDS，ネットワークセキュリティ

Scan Attack Detection System using the Counting of TCP Connection Request with Pseudo SYN-ACK Reply

Kenji OTSUKA[†]　**Kazuyuki YOSHIDA**[††]

[†]Department of Computer Science and Intelligent Systems, Oita University

[††]Center for Academic Information and Library Services, Oita University

There are a lot of scan attacks which look for state of the server or check on service. Scan attacker send TCP connection request to random destination address, so there are seldom answer for them. For this reason, we can detect scan attack by count the number of failed connection request. However if we refuse detected IP address with firewall etc, a problem may occur for attacks like TCP half open attack with fake source IP address. We implement the system which detected scan attacks that we confirm source IP address is not camouflaged for TCP connection demand, and connection successfully or not establishes. In this paper, we describe this attack detection technique and its effect.

Keyword IDS, network security

1. はじめに

セキュリティホールの残っているホストや，特定のサービスを行っているホストを探すscan攻撃が後を絶たない．scan攻撃によるホストの発見後，ホストへの攻撃が行われ，そのためサービスを行えない，不正アクセスが行われるなどの問題が発生することが考えられる．不正アクセスによる侵入を許した場合，他のホストへの攻撃の踏み台，spamメールの中継，フィッシング詐欺などに利用され，他のユーザやネットワークに被害を及ぼすことが考えられる．

この結果を受け，単位時間当たりのコネクション要求回数から攻撃者を判断するシステムを作成し，運用を行った[5]．しかし，コネクション要求回数から攻撃者を判断する場合，攻撃者を決定する基準は，HTTPなどのコネクション確立と切断を繰り返す動作をするプロトコルでは大きめに設定するなど，プロトコルごとに設定する必要がある．また，大量にコネクション要求を送ってくる攻撃の一種であるhalf open攻撃では送信元のIPアドレスを偽装している可能性もあり，検知したIPアドレスをファイアウォールでフィルタする等，対処した際に問題が出る可能性がある．

scan攻撃では非常に多くの宛先に向かってコネク

ション要求のパケットを送信してくるため TCP コネクションが確立できないものが多くなる．この特徴を利用し，TCP コネクションが確立するか否かにより scan 攻撃を判断するシステムを試作した．また，送信元 IP アドレスが偽装されている場合を考え，コネクション要求に対する内部からの応答がない場合，システムが TCP 接続確立の手順通り応答を偽装しそれに対する攻撃者の反応により存在を確認する機能を実装した．

2. 関連研究等

フリーソフトの IDS(Intrusion Detection System)である snort[2]では、プリプロセッサにより scan 攻撃の検知を行っている．ステルススキャンと呼ばれる，ホストのログに残らない scan 攻撃の検知が可能である．しかし，scan 攻撃の判断基準が「単位時間当たりのパケットの送信回数のみ」であるため，Web クローラやプロキシを使用している場合，アクセス回数が閾値を超えてしまい誤検知が増えてしまうことや，攻撃者がパケットの送信時間間隔を大きくすることで容易に回避を行えるという短所がある．

また，Bro IDS[3]は，コネクションの状態を監視し，送信したパケットに対する応答がないものまたは拒否を行なったものを計数する．その計数値が閾値を超えた場合に scan 攻撃だと判断する．このため snort に比べて誤検知は少ない．しかし TCP half open 攻撃，smurf 攻撃等の送信元 IP アドレスを偽装する攻撃に対して偽装された送信元を攻撃者と誤検知する可能性がある．Bro IDS は IDP(Intrusion Detection and Prevention system)の機能も持っているおり，設定によりアクセスを禁止することもできる．

3. scan 攻撃検知システム

3.1. システムの概要

本システムは外部ネットワークから scan 攻撃を行なうホストの検知とそのホストの存在の確認を行なうものである．内部ネットワークが外部と送受信するパケットすべてをミラーリングし，本システムの入力とする（図１）．対象とする scan 攻撃は TCP を用いたものとする[4].

一般ユーザがインターネットへアクセスする場合，外部へ公開されている HTTP サーバやメールサーバなどへのアクセスを行なうため，コネクション確立が失敗することや，短期間に大量のコネクション要求を送信してくることは少ない．

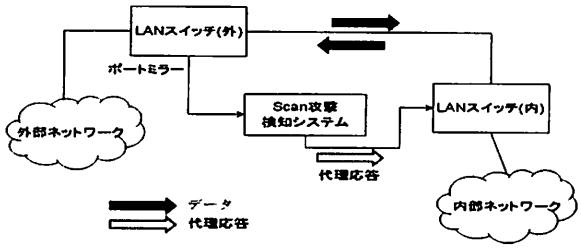


図１　scan 攻撃検知システム

しかし，scan 攻撃を行なってくる攻撃者は内部ネットワークのホストの使用状況やサービスの稼動状態などの情報を収集するため，パケットを非常に多くの宛先に向かって送信し，それに対する応答により内部ネットワークの情報を収集しようとする．このため，コネクション要求を用いた scan 攻撃であれば，パケットの送信数に対して，コネクション確立ができる数は少なくなり，FINScan などコネクション確立を行なわず調査する scan 攻撃であれば，未解決のコネクション数が増加する．また，短期間で情報を得ようとするため短期間に大量のパケットを送信してくることもある．

これらの特徴より，コネクション確立が成功したか否かあるいは，短時間に大量のコネクション要求パケットを送信してくるかで scan 攻撃を検知する．

3.2. 送信元ホストの確認

本システムは，ホストが存在しない，または，使用していないポートへ TCP フラグオプションの SYN フラグを１としたパケットを送信してきたホストに対し，SYN/ACK フラグを１としたパケットを送信する機能を持つ．代理応答により，送信元ホストから応答となる ACK フラグが１となっているパケットが返信されれば，送信元が存在していると確認を行なうことができる．また，返信がなければ送信元は IP アドレスが偽装されていると判断できる[6].

3.3. scan 攻撃の検出

3.3.1設定情報

本システムでは，設定と情報を保持するためにリストを使用する．外部から来たパケット送信元ホストのIP アドレスなどの情報を保持する送信者リストと，scan 攻撃を行なっていると判断された攻撃者の情報を保持する攻撃者リスト，特定のポート番号を除外する除外リストである．

送信者リスト，攻撃者リストはシステムの起動後，動的に作成され，除外リストはシステム起動前に静的に作成される．

以下簡単に説明を行う．

- 送信者リスト

送信元IPアドレスごとに1秒間のコネクション要求回数，未解決コネクション数を保持する．また，送信元 IP アドレスのコネクションごとに送信元ポート番号，宛先 IP アドレス・ポート番号，シーケンス番号，コネクションの状態，パケット受信時刻，を保持する．

コネクション確立後，FIN フラグまたは RST フラグを使用してコネクションを切断した場合，リストから削除される．しかし，コネクション確立なしで送信してきたパケット数と代理応答を行なった回数の合計，または単位時間当たりのコネクション要求回数が閾値を越えた場合，攻撃者リストへと登録され，送信者リストから削除される．

- 攻撃者リスト

攻撃者と判断されたホストを登録する．登録する情報は送信元 IP アドレスのみである．

- 除外リスト

外部からのコネクションをファイアウォールで止めているなど検査を行なわないでよいポート番号を登録する．

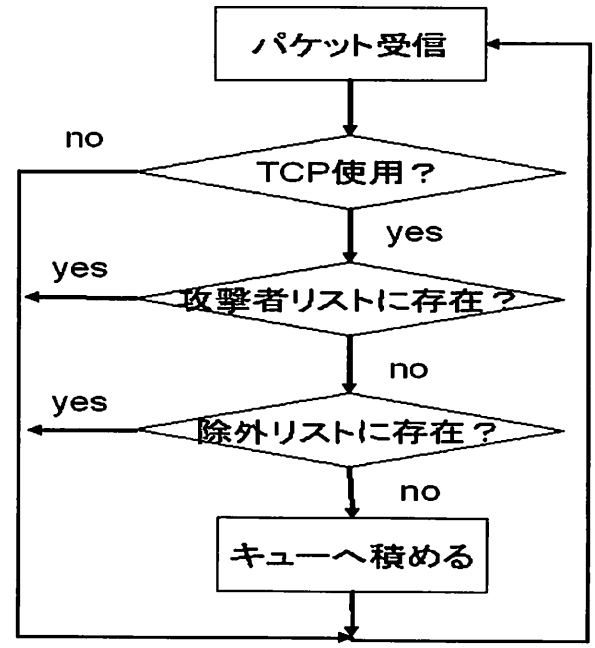


図２　受信時のパケット解析

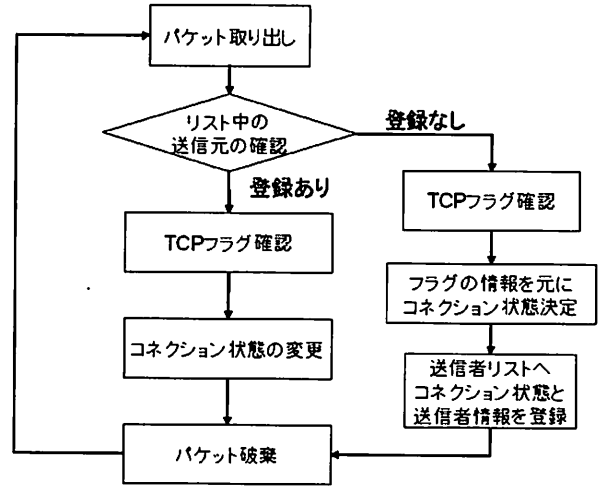


図３　キューからのパケット取り出し

3.3.2検出方法

外部ネットワークから受信したパケットについて，(1)ＴＣＰを使用しているか，(2)攻撃者リストに存在せず，除外リストにも存在しないものを抽出し，キューへと積める．それ以外はパケットを破棄する(図２)．

次に，キューからパケットをひとつ取り出し，そのパケットの解析を行う(図３)．

送信者リストに登録のない状態で SYN フラグが１のパケットを送信された場合，送信者リストに登録される．それ以外であれば未解決コネクション数を増加した後，登録する．

表1　パケットによる状態変化

TCPフラグオプション	コネクション状態				
	登録なし	接続確認	接続確立	終了	未解決
SYN	接続確認				
FIN	未解決	未解決	終了		
RST	未解決	未解決	終了		
ACK	未解決	接続確立			

＊斜線部は状態が変化しないことを示す

送信者リストに登録されていれば，送信者リストに保持しているコネクション状態とパケットの TCP フラグオプションを元に，コネクション状態を変更する(表 1)．表 1 では上の行に存在する TCP フラグオプションの優先度が高く設定されている．そのため，SYN/ACK パケットのように複数のフラグオプションが 1 となり送信されてきた場合，優先度の高い方のフラグオプションと同じ扱いを受ける．

コネクション要求を送信してきたが内部ネットワークにホストが存在しないなど応答がない場合，システムが代理応答を行う．その代理応答に対して確認応答がある場合，攻撃者が存在するものとして未解決コネクション数を加算する．応答がない場合，攻撃者の IP アドレスが偽装されているとして未解決コネクション数を変化させない．

最後にシステムは一定時間ごとに送信者リストに保持されている情報の走査を行う．この際に，未解決コネクション数または 1 秒間のコネクション要求回数が閾値を超えているかの確認を行なう．閾値を超えていなければリストに保持してある送信元ＩＰアドレスの情報の表示を行なう．どちらかが超えている場合，攻撃者リストに情報を登録し，送信者リストから情報を削除する(図４)．

3.5 運用環境

システムの使用しているPCのOSとハードウェア性能およびLANスイッチは以下のとおりである．

OS ： Linux 2.4.20-8

CPU ： Intel(R) Xeon(TM) CPU 3.06GHz

メモリ ： 2Gbyte

スイッチ ： DELL PowerConnect 3324

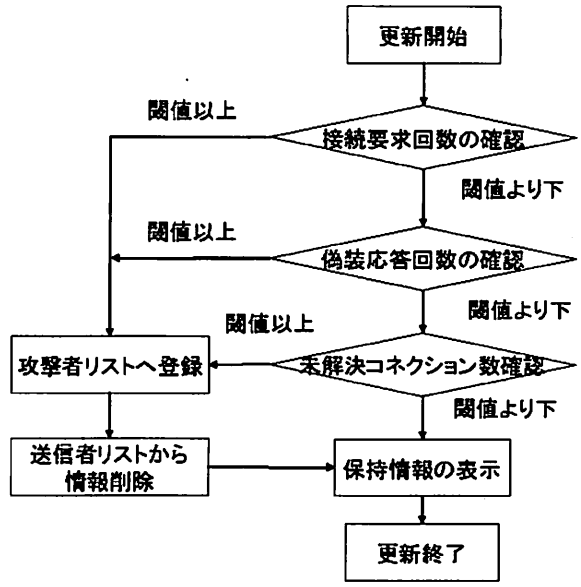


図４　更新処理

また，除外リストとして以下のポート番号を除外している．

80,135～139,445,443

これらのポートは Netbios など，LAN 内部などで使用するものなので，LAN 外部からのすべてのアクセスをファイアウォールなどで除外することができる．また，HTTP サーバ以外への 80・443 ポートへのアクセスを禁止することで容易に禁止できるため除外した．

4. 運用結果

4.1. ログの収集

本システムが動作している PC で同時にパケットキャプチャツールである tcpdump を用いて TCP が使用されているパケットのみを収集した．

収集を行なった期間は 2009 年 2 月 7 日 23 時 20 分から 2009 年 2 月 8 日 9 時 20 分の 10 時間である．

4.2. 攻撃者の決定について

今回は試験的にシステムを作成したため，未解決コネクション数が 5 回を超えたもの，または 1 秒間のコネクション要求回数が 30 回を超えたものを攻撃者として判断する．

表2　攻撃者検知数

検知数	569件
送信元の存在確認	408件
送信元の存在未確認	161件

4.3. 本システムによる攻撃検知の検証

システムを１０時間運用した結果，検知した攻撃者数を表2に示す．表2中の攻撃者のうち，代理応答に対し，応答を返したため送信元の存在が確認できたものが「送信元の存在確認」の件数である．また，コネクションを張らずにパケットを送信してきり，代理応答に対してRSTパケットを送信したりするものを「送信元の存在未確認」の件数としている．

まず，この結果について見ていく．本システムのログの一部を図5に示す．state：EXISTとなっているものが攻撃者から代理応答に対する応答があったものであり，state:ABSENTとなっているものは応答がなかったものとなる．

次に，「存在未確認」となっている攻撃者の検証を行なう．これに該当する送信元には，コネクションを確立せずにパケットを送信してきた，または，代理応答に対してRSTパケットを送信してきた，のどちらかである．検証を行なった結果，71件がコネクションを確立せずにパケットを送信している送信元であり，残りの90件が代理応答に対してRSTパケットを送信している送信元であった．

コネクションを確立せずにパケットを送る送信元に対して代理応答を行なうにしても，本来がRSTパケットを送信するか，何も送信しないため，送信元の確認がうまく行なえない．また，代理応答に対してRSTパケットを送信してくる送信元では送信元IPアドレスが偽装されていて，本来送信していないIPアドレスに題して代理応答をしている可能性がある．

RSTパケットを送信する送信元は主にDNSへのアクセス，メールサーバへのアクセス，または，短期間で集中的にパケットを送信してくるといったものがあった．特に，DSNへのアクセスはSYN/ACKパケットの後にRSTパケットを送信する送信元だけであった(図6)．

最後に，代理応答を行なったアドレスに対し，同一ネットワークではない複数のアドレスから複数回のアクセスがされていることがわかった(図7)．図7に示したものは一部を抜粋したものであるが，実際には各送信元から10数回づつのアクセスを受けている．これは，ボットネットなどを使ったDDoS(Distributed DoS)攻撃の可能性もある．

5. まとめと今後の課題

コネクション確立の有無によりscan攻撃を判断するシステムを試作し，コネクション要求を未使用のアドレスまたはポートに対し送信してきた場合，代理応答を行なう機能を実装した．

実験の結果，scan攻撃の検知は行なえていることがわかった．また，代理応答を利用することで，検知までのアクセス回数を減らすことができるのではないかと考えられる．

今後の課題として，代理応答をより確実に行い攻撃者の判断を正確にすることで送信元IPアドレスを攻撃者と判断できるまでの数を減らす．コネクションの確立を行なわないでパケットを送信してくるscan攻撃に対する対処や，代理応答に対するRSTフラグが1のパケットを送信された際の対処についてといったことが挙げられる．現状，コネクションを確立せずにパケットを送信してくる送信元の確認は行なえていない．また，RSTパケットを送信してくる送信元はRSTScanを行なっているとして判断している．しかし，IPアドレスが偽装されていて，RSTパケットを送信している可能性もあるため，scan攻撃か正規のRSTパケットなのか判断する必要がある．

```
attack_sip:58.63.148.144
        sp:3932->dip:133.37.  .30 dp:54060 state:EXIST Sun Feb  8 06:29:56 2009
        sp:3713->dip:133.37.  .30 dp:54060 state:EXIST Sun Feb  8 06:27:11 2009
        sp:3532->dip:133.37.  .30 dp:54060 state:EXIST Sun Feb  8 06:24:48 2009
        sp:3397->dip:133.37.  .30 dp:54060 state:ABSENT Sun Feb  8 06:23:06 2009
        sp:4349->dip:133.37.  .30 dp:54060 state:EXIST Sun Feb  8 05:40:44 2009
        sp:4196->dip:133.37.  .30 dp:54060 state:EXIST Sun Feb  8 05:38:26 2009
        sp:4013->dip:133.37.  .30 dp:54060 state:EXIST Sun Feb  8 05:36:15 2009
        sp:3874->dip:133.37.  .30 dp:54060 state:ABSENT Sun Feb  8 05:34:34 2009
        sp:3699->dip:133.37.  .30 dp:54060 state:ABSENT Sun Feb  8 05:31:38 2009
```

図5　システムログ

```
attack_sip:66.238.93.161
        sp:2287->dip:133.37.  .133 dp:53 state:RSTSCAN Sun Feb  8 00:33:31 2009
        sp:2282->dip:133.37.  .133 dp:53 state:RSTSCAN Sun Feb  8 00:33:31 2009
        sp:2272->dip:133.37.  .133 dp:53 state:RSTSCAN Sun Feb  8 00:33:31 2009
        sp:2544->dip:133.37.  .133 dp:53 state:RSTSCAN Sat Feb  7 23:55:10 2009
        sp:2537->dip:133.37.  .133 dp:53 state:RSTSCAN Sat Feb  7 23:55:10 2009
        sp:2525->dip:133.37.  .133 dp:53 state:RSTSCAN Sat Feb  7 23:55:10 2009
```

図6　DNSへのアクセス

```
attack_sip:77.202.182.253
        sp:3632->dip:133.37.   .83 dp:15729 state:EXIST Sun Feb  8 09:10:28 2009
        sp:2307->dip:133.37.   .83 dp:15729 state:ABSENT Sun Feb  8 08:29:25 2009
attack_sip:80.34.139.78
        sp:17158->dip:133.37.  .83 dp:15729 state:EXIST Sun Feb  8 08:43:14 2009
        sp:16276->dip:133.37.  .83 dp:15729 state:ABSENT Sun Feb  8 08:19:30 2009
attack_sip:81.0.148.21
        sp:1504->dip:133.37.   .83 dp:15729 state:EXIST Sun Feb  8 04:10:59 2009
        sp:4393->dip:133.37.   .83 dp:15729 state:ABSENT Sun Feb  8 04:00:42 2009
attack_sip:81.32.109.85
        sp:4693->dip:133.37.   .83 dp:15729 state:EXIST Sun Feb  8 08:29:01 2009
        sp:3824->dip:133.37.   .83 dp:15729 state:EXIST Sun Feb  8 08:08:23 2009
attack_sip:81.43.98.228
        sp:18814->dip:133.37.  .83 dp:15729 state:EXIST Sun Feb  8 04:22:00 2009
        sp:15099->dip:133.37.  .83 dp:15729 state:EXIST Sun Feb  8 03:50:30 2009
attack_sip:81.92.178.47
        sp:46715->dip:133.37.  .83 dp:15729 state:EXIST Sun Feb  8 08:22:14 2009
        sp:40874->dip:133.37.  .83 dp:15729 state:ABSENT Sun Feb  8 07:13:10 2009
attack_sip:83.40.73.195
        sp:1406->dip:133.37.   .83 dp:15729 state:EXIST Sun Feb  8 03:16:33 2009
        sp:3736->dip:133.37.   .83 dp:15729 state:EXIST Sun Feb  8 02:31:40 2009
```

図7　代理応答したアドレスへのアクセス

最後に，代理応答を行なうことでボットネットなどからの攻撃を集めている可能性がある．そのため，代理応答を利用することで，さらに少ない回数での攻撃者の判断ができるのではと考えられる．

謝辞

本研究の一部は，大分大学と大分シーイーシー株式会社との共同研究による。

参考文献

[1] 大塚賢治，兒玉清幸，吉田和幸，“偽装応答によるscan攻撃抑制システムについて”，マルチメディア，分散，協調とモバイル(DICOMO2008)シンポジウムpp.182-118, 2008.7

[2] Snort：http://www.snort.org

[3] Bro：http://www.bro-ids.org

[4] J.Postel, “Transmission Control Protocol”, RFC 793, 1981.9

[5] 衣笠雄気，大塚賢治，兒玉清幸，吉田和幸，“アクセス制御を用いたscan攻撃抑制システムについて”，電気関係学会九州支部連合大会(第61回連合大会)講演論文集 11-2P-13,2008.9

[6] 兒玉清幸，大塚賢治，南浩一，吉田和幸，“偽装応答を用いたscan攻撃抑制システムの提案”, FIT2007(第6回情報科学技術フォーラム)講演論文集 pp.71-73, 2007.7

[7] 大塚，兒玉，衣笠，吉田：TCPコネクション確立の偽装とその計数によるscan攻撃検知について，情報処理学会研究報告(インターネットと運用技術(IOT)研究会)，2007-IOT-4，pp.203-208, 2009.3

Study on Information Security Strategy for Ubiquitous Society

Min, kyoungsik (KISA)
Kyoungsik@kisa.or.kr

It is necessary for the government to anticipate threats and challenges that come with the promises of a ubiquitous information environment. Four different policy areas are distinguished for information security efforts including infrastructure, services, users and the environment, to comprehensively and effectively meet challenges to the security of the ubiquitous society. According to policy areas, four information security strategies are suggested which are securing information infrastructure, implementing trusted IT service, guaranteeing user privacy, and forming clean information use environment.

Key-Words: Security, Privacy, Ubiquitous

1 Background

Thanks to a remarkable progress of informatization and the increasing convergence between IT and the rest of the industry, Korean society is fast moving towards a ubiquitous information society; a transition expected to bring about dramatic changes touching all aspects of the lives of Korean people. Next-generation network infrastructure like BcN and USN paves the way toward a ubiquitously-networked society in which the physical world and virtual spaces are seamlessly integrated, triggering profound social and lifestyle changes. The accelerating convergence between IT and the rest of the industry offers multiple new economic opportunities, by spawning new generations of services like u-Health, and is opening up a new avenue of possibilities to strengthen national competitiveness.

Meanwhile, a u-society must contend with technological and cultural disparities in society, that sudden social changes, triggered by this process, are likely to widen, and the negative side effects of informatization, such as increasing threats to the privacy of information users. New cyber attacks of the types of bot-nets and Pharming can produce especially disastrous consequences in an information environment integrating wireless and fixed-line networks. RFID, LBS, smartcards and other ubiquitous technologies make it dramatically easier to collect, transmit and assemble personal information of users. Illegal spamming, online suicide communities or websites devoted to bomb-making and other reprehensible activities proliferate, inciting behaviors harmful to personal welfare of users and social order.

It is, therefore, necessary for the government to anticipate threats and challenges that come with the promises of a ubiquitous information environment, through appropriate response strategies, so that the benefits of u-IT may be safely enjoyed by all. In this paper, information security strategies for ubiquitous society are suggested to ensure the safety of IT-enabled services provided in a ubiquitous network environment, such as online financial transactions and medical and educational services, protect the privacy of information users and formulate clean information use environment.

2 Information Security Environment Forecast

2.1 From Information Society to Ubiquitous Society

The integration of IT in our lives and society, thus far consisting of use of communication tools linking people(P to P), is now evolving into a new, ubiquitous mode whereby people communicate with machines(P to M), and communication occurs also between things(T to T).

In this next stage of informatization in which people and things become integrated elements of an environment where information is ubiquitously present, IT has a much more direct and far-reaching impact on all aspects of life in our society.

The government has been assisting the transition of the Korean information landscape into a ubiquitous environment through its u-IT839 Strategy, providing support toward the growth of DMB, tele-matics and home networking technologies and the convergence between different IT services.

To be in keeping with the latest technological developments in IT fields, the U.S. and Japan and also the EU region have been massively investing in R&D in next-generation technologies and u-network infrastructure. In the U.S. efforts to take IT to the next level are coupled with initiatives for innovative applications by integrating IT with cutting-edge technological fields like NT and BT. Through the use of network, Japan successfully upgraded not just IT itself, but communications devices, consumer electronics, industrial equipment and peripheral technologies; in other words, its traditional areas of strength. The EU, interested in a human-centered computing approach, is looking to develop a variety of intelligent services.

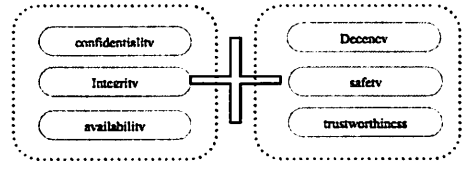
2.2 Characteristics of a Ubiquitous Society

Convergence between technologies, industries and services increases. New hybrid services, created from the convergence between telecommunications (internet) and broadcasting or other industries, are being introduced. DMB, a technology delivering broadcast content over mobile communications network, enables real-time TV viewing in a mobile environment. Next-generation consumer electronics and home appliances like D-TV sets, DVD players, internet refrigerators and intelligent service robots are expected soon to become industry-leading products. Integration of IT in the automotive industry (for example, cars shipped with built-in DMB devices), providing new ways to upgrade car models and differentiate product lineups, is helping to boost the sector's competitiveness.

New types of social interaction in cyberspace and lifestyle revolution are triggering personalization. A ubiquitous society offers personalized services, adapted to individual taste and interests. This will have a major consequence on the way the internet is used and how users interact with others online, giving rise to, among others, new types of virtual communities. Open communities like 'blog' are expected to sharply grow in numbers, becoming something that deserves to be called a one-person media market. With the progress of ubiquitous networking, one-person media is likely to evolve into new types of communities like 'locative media'.

Homes will no longer be simple places of residence and resting, but will be transformed into multi-function digitalized living spaces where knowledge is created, and information shared.

2.3 Characteristics of Information Security in a Ubiquitous Society



<Information Security Properties in the Ubiquitous age>

In a ubiquitous society, information security efforts, formerly concerned with the safety of systems and networks, now extend to that of devices. The current list of priorities in information security, consisting of confidentiality, integrity and availability, will be expanded with new goals such as trustworthiness, decency and privacy.

Information security, in a u-society, is no longer a static process, but becomes a 'conformable' process, whereby services are appropriately modified, based on contextual information captured through sensor technologies.

Information security for ubiquitous society enhances the public acceptance and adoption of new IT service by raising the level of users' trust in u-services and confidentiality of transaction information.

Information security anticipates and prevents new types of cyber attacks including hacking and viruses and cybercrime targeting the ubiquitous information environment. It prevents service disruptions for new converged-type, internet-based IT services such as IPTV and VoIP(Voice on IP) by thwarting cyber attacks launched via wireless and fixed-line networks. It fights cybercrime making use of the latest technologies and blocking indecent or harmful information. And it provides social and legal infrastructure necessary for controlling side effects of ubiquitous networking, including information

security-related laws to regulate the handling and use of location information and medical information.

Four different policy areas are distinguished for information security efforts, including infrastructure, services, users and the environment, to comprehensively and effectively meet challenges to the security of the ubiquitous society.

3 Information Security Strategy

Hierarchy of u-Society	Core Strategic Objectives
environment	guaranteed privacy
services	trusted IT services
users	guaranteed privacy
infrastructure	secure info. infrastructure

< Core Strategic Objectives for u-Society>

Four different policy areas are distinguished for information security efforts including infrastructure, services, users and the environment, to comprehensively and effectively meet challenges to the security of the ubiquitous society. According to policy areas, four information security strategies are suggested which are securing information infrastructure, implementing trusted IT service, guaranteeing user privacy, and forming clean information use environment.

3.1 Securing Information Infrastructure

Policy Areas	Detailed Objectives
network	Establishing management system to safeguard network infrastructure
software	Strengthening security and reliability of software applications
security capacity	Enhancing capacity to prevent cyber intrusion incidents

<Detailed Objectives for Securing Information Infrastructure >

A comprehensive security management system for BcN should be built. A strategy should be developed to effectively counter threats to personal data, posed by next-generation worms and viruses targeting mobile handsets and PDAs, and other intelligent, portable devices, magnified by the increased use of devices of this type. Cyber attack prevention and response technologies should be developed to strengthen the national response system. Security guidelines and security check methodologies to enhance security at the level of individual subscriber networks should be developed. Solutions to ensure the security of networks with different security levels and owned by different operators, interconnected within BcN should be devised.

A comprehensive security management system for USN and IPv6 should be developed. A network management system to guarantee secure transport of sensor-captured data should be created. Light-weight security chips for use with sensor nodes to effectively block attempts of illegal interception, forging or altering of information stored within sensor nodes are needed. Security standards for USN devices and develop a security test system should be established so that the reliable performance of security modules inside USN devices can be ensured from the design stage on. Security of the IPv6 environment and process of migration toward it is required. A security system for mixed IPv4/IPv6 networks to facilitate secure transition and to promote the secure operation of IPv6 networks is important.

Security and reliability of u-Society software Applications should be enhanced. An information security framework to block and respond to intrusion attempts targeting national software infrastructure to minimize disruptions of critical public services, making embedded security features mandatory and providing other security standards is required. A certification system for the security of open and embedded software products should be upgraded.

Capacity to thwart cyber intrusion attempts should be enhanced. An information tracking system allowing to trace the path of information, in reverse, back to the initiator of an intrusion attempt, should be reinforced. The focus of security efforts for networks and systems from monitoring-based protection to prevention should be shifted by investing more in detection tools for identifying and eliminating vulnerabilities before they may be exploited by intruders. Infrastructure for digital forensic investigations should be implemented, including standard procedures for collection, analysis and use of digital evidence and authenticating digital evidence.

The framework for information security governance should be built. An information security governance framework and guidelines for developing a governance structure to help companies protect their IT investments through systemic, organization-wide efforts is required. Information security architecture linked to EA/ITA and develop a reference model should be designed.

3.2 Implementing Trusted IT Services

Policy Areas	Detailed Objectives
users	Creation of a new authentication system adapted to next-generation u-services
contents	Integrated wireless-fixed-line content security system
platforms	Reliability of u-devices
services	Reliability of u-service use environment

<Detailed Objectives for Implementing Trusted IT Services >

Electronic authentication frameworks targeting different levels of threats should be developed. A framework for user authentication processes geared toward providers of critical, applied ubiquitous services that include a classification of authentication services according to the type of IT services for which they are used, recommended procedures and methods.

A Digital ID management system giving greater control to users over the level of privacy and security concerning their personal data should be implemented. ID management techniques should be developed which allow users to specify, in accordance with the privacy policy of service providers, whether personal information they provided to them, may be shared with third-party organizations and, if yes, under what conditions.

Protection of copyrighted digital content should be reinforced. A system to protect content distributed through converged telecom-broadcasting media and mobile networks, from unauthorized access and use (creation of a system integrating mobile DRM, CAS and CP technologies) should be developed. A content protection environment should be created in which DRM, CAS and CP technologies, independently developed for specific domains distributing content, such as wireless and fixed-line internet domains and servers transmitting digital broadcasting content or serving digital home can be used, without interruption, across diverse networks constituting the nexus of ubiquitous information services.

The reliability and interoperability of u-Devices should be improved. Device authentication models adapted to different ubiquitous service environments by analyzing authentication scenarios, varying according to service characteristics should be developed. Certificate lifecycle-based device authentication management models for different authentication environments and related guidelines should be designed. Mobile TPM and middleware technologies for security and reliability services should be developed, to enhance the dependability of converged/hybrid service devices that are becoming increasingly open, smart and multimedia-centered.

An information security management system for protection of personal privacy to minimize theft and misuse of personal data and other social losses caused by their unauthorized access and use should be created. International cooperation efforts to build public trust for information security services through international standardization of ISMS and mutual recognition agreements should be engaged. A methodology for assessment of impact on information security for use during the development of new converged and hybrid IT services like VoIP and WiBro should be developed to minimize social losses caused by intrusion incidents targeting these services.

3.3 Guaranteeing User Privacy

Policy Areas	Detailed Objectives
infrastructure	Building u-service privacy architecture
environment	Creation of social context and legal framework supportive of u-privacy
extended personal information(1)	Protection of video images
extended personal information(2)	Protection of biometrics, location and RFID data

<Detailed Objectives for Guaranteeing User Privacy >

Privacy protection architecture should be developed. Systemic and concrete approach to the development of privacy protection technologies should be

developed, to design solutions that are optimally adapted to the ubiquitous computing environment.

Social and cultural context supportive of privacy should be established. Training requirements for privacy officers of businesses with online presence and develop privacy rules adapted to individual business sectors should be reinforced. Certification marks to companies having privacy management systems meeting required standards and having completed privacy enhancement education can be issued. Special efforts to educate less information-savvy segments of the community about privacy risks and teach them how to minimize their vulnerability to identity theft should be given. International cooperation in privacy enhancement should be enlarged. A legal and regulatory framework for privacy protection should be established.

Protection of Location Privacy should be reinforced. Technical standards for personal location information security and enforcement of privacy rules should be developed. The technical standards can allow location-based services to automatically reflect user-defined settings so as to give users greater control over the information shared, and make the services more convenient for them. Legislation for protecting location privacy should be made. This legislation should make mandatory the location information security obtained by government organizations, through the bus information system or highway cameras, and employee location information from companies' internal network, and establishment of location privacy procedures.

Biometrics information privacy standards should be developed and public awareness about related privacy risks should be raised. A certification program to guarantee the integrity of biometrics information and technologies for secure transmission and storage can be effective. A central information system achieving optimal integration of individual medical information systems and enabling the efficient management of them, and common standards for medical information security should be developed.

A security system for CCTV-captured video data should be created. Rules to regulate the installation and operation of CCTVs to curb the privacy risks associated with the use of these surveillance units are required. Public awareness about potential privacy risks caused by the installation and operation of CCTV should be raised.

A privacy protection system for RFID services should be in place. Users' right to refuse tracking and tracing so that they can escape RFID-based monitoring whenever they choose should be ensured.

3.4 Forming Clean Information Use Environment

Policy Areas	Detailed Objectives
digital contents	Designing response system eradicating indecent or illegal contents
Information users	Educating users for safe and healthy use of information
Information use environment	Nurturing u-clean culture

<Detailed Objectives for Forming Clean Information Use Environment >

A response system to eradicate indecent or illegal contents in ubiquitous networks should be designed. Regulatory mechanism to control the circulation of objectionable information content threatening the decency of the ubiquitous information environment should be established. Cybercrime, cyber violence, cyber stalking and harmful content should be clearly re-defined to develop a precise classification system for internet and network-related offenses adapted to the new, ubiquitous information environment. The regulation and oversight of internet content to defend the decency of the internet should be strengthened when the introduction of converged telecom-broadcasting services and other hybrid services are triggering rapid changes in the nature of content distributed across cyberspace. International cooperation in blocking offensive and harmful content such as obscene materials or gambling-related information which can have disruptive consequences for society should be upgraded. Spam through a joint international response system should be lessened by strengthening cooperation and exchange with anti-spam organizations of the U.S. and E.U. countries and international organizations involved in anti-spam efforts.

Educating users for safe and healthy use of information should be reinforced. Measures to fight new types of media addiction in the ubiquitously

networked environment should be prepared. Prevention programs and internet hotlines for those suffering from media addiction should be operated, factors influencing excessive media dependence and identified, and related programs to ensure their effectiveness clearly monitored. The image of a model u-society citizen should be created and information ethics promoted. Internet ethics required for the well-functioning of the u-society in the public by educating general users and opinion leaders through various media should instilled.

The u-clean culture should be nurtured. Information security awareness to prevent information theft-related privacy infringement and losses should be raised. Education strategies to introduce youth, parents, teachers and online service providers should be devised. Inciting businesses to invest more in information security and take an active part in the fight against cyber attacks, and increase the supply of privacy manpower through a human resource development program in the area of personal information security, is needed. Education and prevention efforts against personal rights violations in the u-society should be launched and institutional and legal frameworks for defending basic human rights within cyberspace should be built. Programs to fill the digital divide should be launched, to ensure equal access to the benefits of the u-society by extending opportunities for informatization to all segments of the population.

5 Conclusion and Future Work

In this paper, strategy framework to manage information security in the ubiquitous age was suggested. Four core strategic objectives were identified to protect infrastructures, services, users, and environment in the future. Activities to perform the objectives were introduced.

This study would help information security policy makers and manager define strategic directions for information security in preparation for the ubiquitous age, and design countermeasures to emerging cyber threats.

As future work, development of metrics to measure the level of nation's security countermeasure against threats in the ubiquitous age will be considered. The metrics will be developed by considering core strategic objectives suggested in this paper and diverse security options including political, technical, and legal ones.

References:

[1]Ministry of Information and Communication, *information security strategy for the ubiquitous age*, 2006. 12.

地方における事業継続性の取り組み

ハイパーネットワーク社会研究所
事務局長　青木　栄二
blue@hyper.or.jp

１．はじめに

九州地方においては、例年 2～3 個の台風が接近し、そのうち 1 個が上陸している。たとえば大分県では、過去 30 年間、台風によって暴風雨の影響を受けた回数は約 60 回となっている。平均すると毎年 2 回という勘定だ。また梅雨時期における集中豪雨の影響で、土砂崩れや河川氾濫などの被害は、近年増加傾向にある。九州地方を中心に降り始めからの総雨量が 1,000mm を超えるような大雨が、毎年のように発生しているからである。

こうした自然災害をはじめ火事や停電などの事故、内部の不祥事や疫病などの緊急事態が発生した場合を想定して、重要な業務が中断しないように、また中断を余儀なくされた際でも迅速に復帰できるような事業継続性計画（BCP）が必要とされている。最低限の機能から順次回復して、業務の中断を最小限に抑えるといったことを、導入段階から、運用、改善、チェックにいたるまで、全体的に考えるための事業継続性管理（BCM）も重要となる。

九州地方では、これらの課題に対して各県が個 別に対策を講じている状況であり、台風被害などの広域的な防災については、県間連携の必要性が 問われ出してきている。昨今の ICT の進歩から、情報ネットワークが効果的な県間コミュニケーションに寄与できるのではないかと考えられるからである。そこで今回は、地方における ICT を利活用した事業継続性の取り組みを紹介する。具体的には、防疫のための対策システムおよびそれを情報共有アプリケーションとして、県間連携を行った実証実験である。また実験結果を通して、広域的な ICT プラットフォームの有効性を考察する。

２．家畜防疫マップシステム

大分県では、平成 16 年に鳥インフルエンザが発生した。その際の教訓を踏まえて、大分県家畜衛生飼料室では、家畜防疫マップシステムを地場企業の日建コンサルタントとともに開発した。それは、発生から制限区域の設定、清浄化宣言までの作業を、より迅速・効率的に行うためのシステムである。

利便性の高いものにするための開発ポイントは、 まず県庁内の各部署が持っているさまざまなデータ（地図や画像、航空写真や衛星写真など）を収集できたことである。おかげで基盤となるオルソ画像と地図データのプラットフォームを構築することができた。つぎに県内すべての畜産業者の協力である。農場の詳細なデータ(位置情報や画像 など)をシステムへインプットしている。これで緯度経度情報が明確となり、発生地点を中心とした制限区域設定、搬出時のチェックポイント等を瞬時に特定でき、どこまで範囲に入っているのか、 微妙な場所の農場をすべて判断できるのだ。それが意味するのは、発生から終息までの時間の短縮と伝染の防止、風評などの二次的な被害の抑制である。農場主の経済的メリットは大きい。いつどこからもたらされるか判然としない自然災害に近い家畜伝染病の対策は、時間との勝負である。農業産出額が高い県にとっては影響も大きい。

幸いなことに平成16年以降大分県では発生していないが、他の県では図1に示すように平成17年は 茨城県、埼玉県、平成18年は宮崎県、岡山県というように、いつどこで発生するか予測がつかない状況となっている。

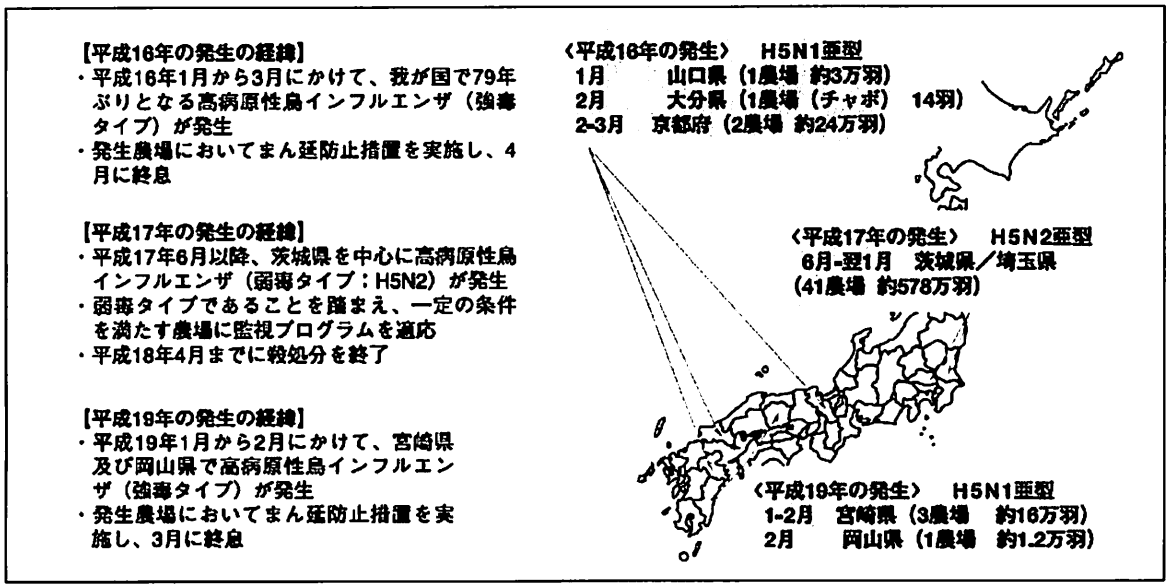
これは日本に限らず、世界の発生状況を見てみると大変なことになっているのが分かる。図2には 鳥だけでなく、ヒトへの感染データも示す。まさに予断を許さない現実である。昨今の新型インフ ルエンザにおけるパンデミックと同様に、事業継続性の観点からも重要な課題である。

大分県で開発した家畜防疫マップシステムは、オルソ画像／ラスター地図／ベクター地図／ポイントデータのレイヤ構成で、各種データをフォルダ管理している。実際に利用できる機能としては、 以下のものがある。

・発生ポイントの設定機能
・発生ポイントの緯度経度表示機能
・「移動制限区域」「搬出制限区域」同時設定機能
・指定半径による同心円内施設の自動抽出および集計機能、手動追加および削除機能
・指定半径制限区域にかかる大字界や大字内施設の抽出および集計機能、手動追加および削除機能
・複数発生ポイントとその複数移動制限区域および搬出制限区域の設定機能
・家畜保健衛生所毎のデータ抽出および集計機能
・消毒ポイント等のポイント設置機能
・抽出データの CSV 外部出力機能
・マップデータの BMP 型式出力機能
・農家台帳機能、各施設情報帳票表示および出力機能
・カーナビゲーション連携機能
・簡易作図機能
・ヘルプ機能

現在は図3に示すように、大分県本庁舎にある家畜衛生飼料室と県内4箇所にある各家畜保健衛生所をネットワーク化して、家畜防疫マップシステムによる情報共有とテレビ会議システムによる対面での意見交換を行っている。

図1 日本の鳥インフルエンザの発生状況（H16年~H19年）



出典：大分県農林水産部家畜衛生飼料室

3．危機管理体制構築のための広域連携

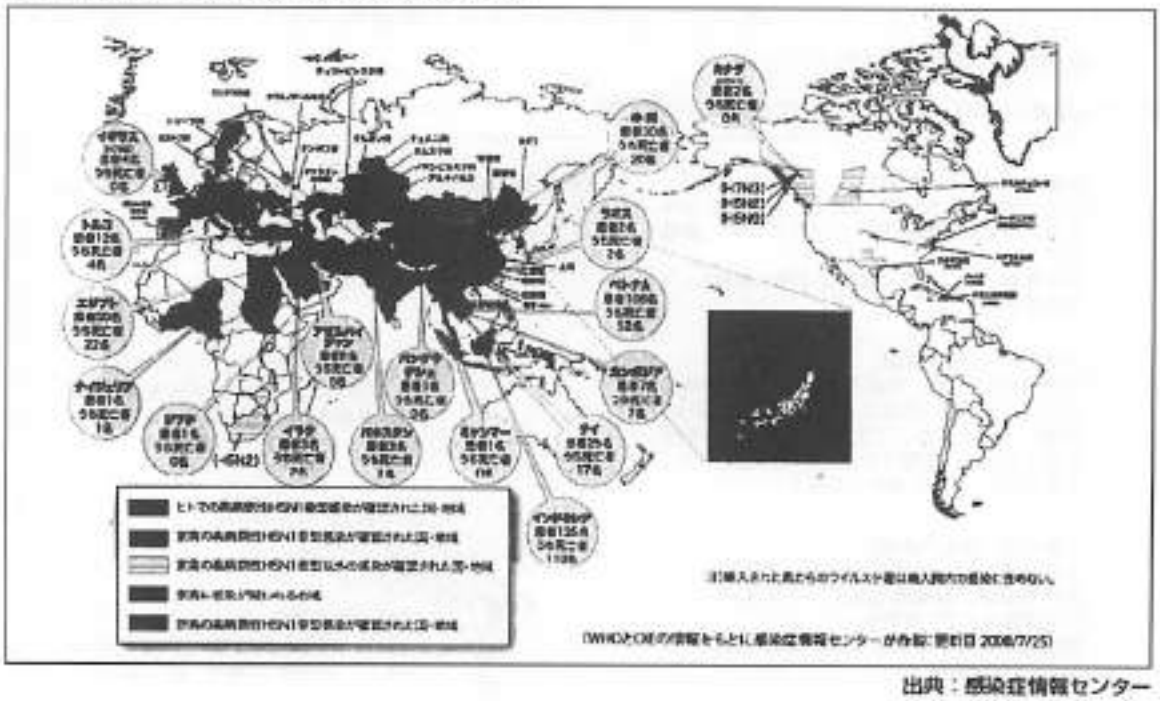
大分県では、家畜伝染病のためにこうした危機管理体制を構築しているが、他の県ではどういった状況にあるのだろうか？たとえば隣の宮崎県では地鶏や牛が有名にもかかわらず、まだ対策システムは導入されていない。仮に発生したとしても 平成 16 年当時の大分県と同じく、電話や FAX、地図を頼りに時間をかけて確認、対応していくことになる。しかし県内だけで納まればいいが、制限区域が県境を超えるケースも想定される。もし県境において伝染病が発生したらどうなるのだろうか？

こうした課題に対して、広域連携のための実証実験を行った。まず大分および宮崎の県庁内にテレビ会議システムを設置し、庁内 LAN／県域ネットワーク／JGN2plus を相互接続した。情報共有のためのアプリケーションとして、家畜防疫マップシステムを活用し、地図情報を共有しながら直接対話、情報交換できる仮想のプラットフォームを構築した。連携における防疫対策情報の質や量、システムの操作性、プラットフォームの有用性等の検証を行った。イメージを図 4 に示す。

実験結果としては、既存のインフラを相互接続することで安定的な県庁間ネットワーク環境を整えることができた。また対策情報の共有においても正確かつ迅速であり、システムの使い勝手も容易であった。これにより隣県で家畜伝染病が発生しても、情報共有できるプラットフォームがあれば被害を最小限にする対応が可能だと、十分に検証することができた。

この実験を通して見えてきたものは何か？明日、どこかで家畜伝染病が発生したらどうするのか？ 他の県については同様の対策システムがなく、県間ネットワークもないため、従前通りの対策方法しかない。しかし ICT は急速に進歩しており、多くの技術的な課題を克服してきている。問題は、いつ来るとも知れない災害対策のためにどれだけの準備をするのか、といった費用対効果である。

図2　世界の鳥インフルエンザの発生状況（H20年7月）



出典：感染症情報センター

事業継続性に照らした詳細な分析と試算が必要だが、科学的なデータによる根拠やコストというより、むしろ規則からの制約や新たなものに対する 枠組み作りなどのほうが難しいのかもしれない。

一方で民間サービスではどうだろうか？たとえばCATVでは、九州内の各社が物理的にネットワークを繋いでしまおう、という動きがある。すでにいくつかの県では、県内のCATV同士が相互接続されて、地上デジタル放送用共同ヘッドエンドの利用がなされている。アナログからデジタルへの転換という大きなコンテンツが動いたことによるものだ。では九州内の各CATVが接続するのは なぜだろう？それは新しいコンテンツをサービスしようという広域的な情報流通活動であり、新規 ビジネスの創出でもある。

それから考えてみると、自然災害や家畜伝染病といった凄まじいコンテンツに対しては、関係省庁や報道機関だけに任せるのではなく、公共サービスとして、自治体が情報共有、情報発信していくべきではないだろうか。被害を受けるのは地域住民であり、災害はそのほとんどが広域的である。 ICTは現場の自治体連携を容易にしてくれるものであり、コストについても大きな変革をもたらしている。グーグルマップやスカイプ、ユーチューブなどを参照すればよく分かる。このインターネット時代、だれもが情報共有できる時代だ。自治体ごとによる対策はもちろんのこと、自治体同士の連携がまさに求められている。地域における事業継続性とは、今後、隣りの地域との連携ではないだろうか。各自治体においては、真剣な検討がなされ、対策も講じられているのだが、なぜか境で切れてしまうのだ。広域といった視点が、ボー ダレスと言われる今の時代だからこそ重要となってきている。

図3 大分県防疫情報会議

出典：九州広域ICTプラットフォーム調査検討会

4．地方における事業継続性

食とエネルギー、二つのテーマは今後ますます重要なものとなってくるだろう。九州にとっての農業生産は大きな比重であり、大分にとっても一村一品に代表されるように事業の継続性を考えるうえで、家畜伝染病は非常に深刻な問題である。県内総生産は約4兆5千億円、そのうち農業産出額は約1.5千億円である。九州内の他県も同様に決して少なくない数字であり、対

策の是非はいうまでもない。家畜伝染病や自然災害への対策システムが、九州全県においてネットワーク化されるとすれば、大きな安心感を広域的に得ることができる。 とともに農業産出額の大きい九州にとって、全体的な食の安全性を保障する ICT プラットフォームとして、アピールすることができるだろう。また 全域的な意識啓発にも有効だ。つぎからつぎへと 発覚する食の偽装問題、モラル啓発にも九州全域で取り組むことにより、よりいっそうの事業継続性へつながるものと考えられる。さらには中国や韓国での鳥インフルエンザや BSE への恐怖に対して、九州物産の食の安全というコンテンツを売ることが可能になるのではないだろうか。こうした事業継続性計画を立てることのメリットは大きい。あとは自治体同士が事業継続性管理を明確にシステムとして持つことである。行政・生産者・消費 者が結びつくこと、それを支える産（システム開発）・官（公共サービス）・学（客観的研究）が それぞれの役割を持って、地域住民と相互理解することは、リスクコミュニケーションというかたちで管理システムへ反映されるものと考えられる。

5．おわりに

日本の食のレベルは高い、安全性のレベルも高い。各地方が競争する中で、県といった単位ではなく、九州を例にまとまった地理的な範囲における事業継続性への取り組みは、売れる商品である。それは ICT を利活用することで、十分に達成できるものである。

アンドロイドやアイフォンなどのモバイルデバイスの登場、つぎつぎに創出されるソーシャルメディアのコミュニティサービス、その基盤となるクラウド（未来情報インフラ）等、ICT の台頭により、「いつでも、どこでも、だれでも」というユビキタス時代の到来が、自然災害や伝染病に対しても有効に対応できる時代になってきたのだと考えるものである。インターネットが自律・分散・協調によって進化・発展して、事業継続性に寄与してきたように、地域においてもこれまでのヒト・モノ・つながりを基盤として、情報・コミュ ニケーション・技術を利活用することで、事業継続性をより確かなものにしていくことができるのではないだろうか。

図4 実証実験のイメージ

出典：九州広域ICTプラットフォーム調査検討会

地域のセキュリティを考える～ネットあんしんセンター開設へ向けて～

ハイパーネットワーク社会研究所
事務局長　青木　栄二
blue@hyper.or.jp

1．はじめに

2007年度研究報告書においては、「セキュリティUP活動からインターネット安全運動へ」と題して、2003年度からの情報セキュリティ活動の経緯をレポートした。

そこではこれまで取り組んできたさまざまな普及啓発活動や緊急対策情報の配信、活動の有効性を検証するためのアンケート実施や今後に向けての地域スキーム構築のモデル化などを紹介した。具体的には、約4,000名がセミナーを受講し、約30本のセキュリティ情報の配信をメールにてマスターと呼ばれる約100名の講師役の方々へ行い、約800名に対してアンケートを実施したというものである。また大分に続く地域モデルとして、松山との連携を試みた。

「地域のセキュリティは地域で守る」という意識調査のために、アンケートにおいてセキュリティ向上のためのボランティア活動に参加したいか、という質問項目を設けたところ、賛成割合が平均で24%もあったことは注目に値する。情報セキュリティの向上には、いかに地道で継続的な活動が重要かということを、十二分に考察することができた。さらに今後の展望として、地域にはある一定の単位でセキュリティセンターが必要とされてくるのではないか、と結んでいる。

2．2008年度の活動経緯

2003年度から始まったマイクロソフトのUPプログラムは、当初の予定どおり5年間で終了した。そのプログラムのセキュリティ対策として、2005年度より実施してきたセキュリティUP活動も同様に終了した。しかしセキュリティ対策の重要性は年々増してきていることもあり、その延長線上として、新たにインターネット安全運動という名称で活動を継続、地域のセキュリティ向上のあり方について模索した。一方では情報セキュリティ対策推進協議会（SPREAD）との協働や、日本ネットワークセキュリティ協会（JNSA）、マルチメディア振興センター（e-ネットキャラバン事務局）、情報処理推進機構（IPA）、日本情報処理開発協会（JIPDEC）などが企画実施する普及啓発活動への協力も行った。

（1）第4回セキュリティUP会議～新マスター講習会およびセキュリティセミナー～
＜日時＞　2008年6月30日（月）10：00－15：00
＜場所＞　日出町保健福祉センター（研修室）http://www.hiji-syakyo.jp/map/akusesu.html
　　大分県速見郡日出町大字藤原２２７７－１（TEL:0977-72-0323）
＜主催＞　大分UPプログラム（事務局：ハイパーネットワーク社会研究所）
＜プログラム＞
10：00－12：00　①新マスター講習会
「セキュリティUP活動の概要説明」ハイパーネットワーク社会研究所(事務局)
「新マスターのためのセキュリティ講座」NPOシニアネット大分 矢野豪志氏

12：00－13：00　②ランチミーティング（質疑応答や意見交換など）
13：00－14：45　③セキュリティセミナー
「セキュリティ最新動向～被害にあわないために～」
株式会社ラック サイバーリスク総合研究所 主管研究員 村上晃氏
「最近の脅威とマカフィーのアプローチ」
マカフィー株式会社　マネージャー　馬場敏文氏
14：45－15：00　④まとめ

（2）第5回セキュリティUP会議（共催：ハイパーネットワーク社会研究会）
＜日時＞　2008年10月3日（金）15：00－17：00
＜場所＞　第2ソフィアプラザビル2F　ソフィアホール　会議室A
＜主催＞　大分UPプログラム（事務局：ハイパーネットワーク社会研究所）
＜プログラム＞
15：00－15：45　①セキュリティUP活動報告
「5年間のセキュリティUP活動を振り返って」ハイパー研（菊池主任研究員）
「セキュリティUP活動通じての感想」NPOシニアネット大分 矢野豪志氏
「今後のセキュリティ活動について」ハイパー研（菊池主任研究員）
15：45－16：55　②勉強会
「社内教育を徹底する効果的な進め方」
有限会社関西レディースコーポレーション　長尾 裕子氏
16：55－17：00　③まとめ

当研究所においては、インターネット安全運動のためにこれまでのセキュリティUP活動の資産を生かすべく、上記のように説明会や講習会、勉強会を開催した。活動体制としてのスーパーマスターやマスターといったピラミッド構造を、フラットなセキュリティボランティア構造へと移行するための説明、また今後どういった方向性を持って活動していくべきかを議論した。並行して、セキュリティボランティアのレベルアップのために、各種の勉強会を開催した。ゆるやかなつながりを形成していけるようなコミュニティの創造である。

全国的には、インターネット安全教室やe-ネットキャラバン、IPAセキュリティセミナー、セキュリティ&プログラミングキャンプキャラバンなどが各地で開催されている。ここ大分においても当研究所が積極的にローカルホストを努めてきた。また県内では、大分県警、教育庁、市町村、PTAからの依頼により、子どもや保護者に対しての情報モラルや情報セキュリティの普及啓発活動を実施してきた。

しかしこうした動きは単発的であって、部局間の連携・協調性や継続性に欠けるところがあり、本当に実効性があるのか、検証も非常に難しい状況である。一方ではインターネット社会の進展、技術の進歩はすさまじく、問題や被害は増えているのである。たとえば、県警や消費生活センターへの相談件数は、ネット系のものが急増しているのだ。

地域にはある一定の単位でセキュリティセンターが必要になってくると、ここ数年考え続けてきたものが、ようやく現実味を帯びてきた。そこで当研究所では、大分県情報政策課の協力を得て、「ネットあんしんセンター」開設のための企画検討をはじめたのである。

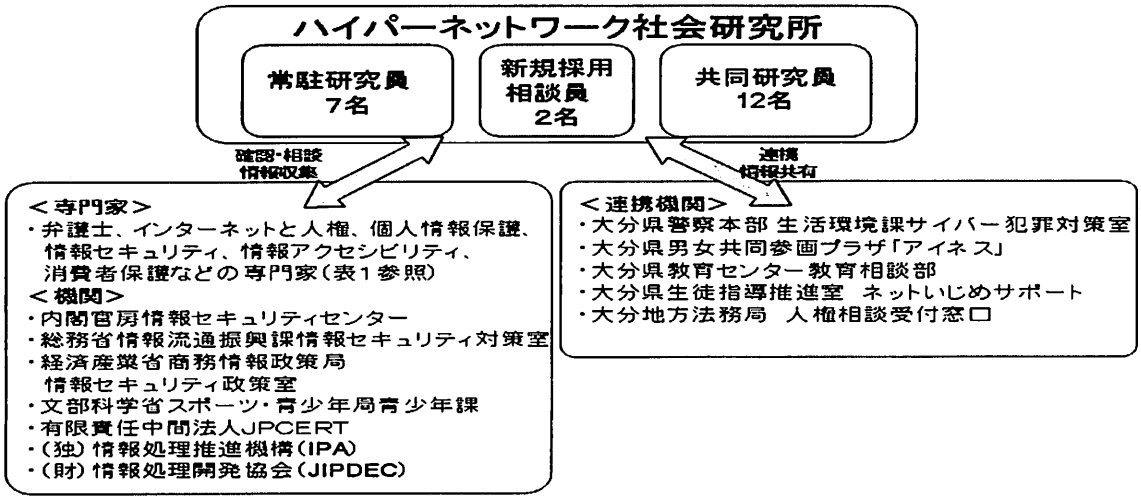
3．ネットあんしんセンターの活動概要案

（1）相談窓口の設置

相談窓口はハイパー研内にカウンターを設置し、パソコン等持参による相談についても柔軟に対応できる場所や環境を整備する。相談受付はメールや電話を基本とするが、メールや電話での対応が困難な場合、相談者が来訪を希望する場合については、センターにおいて応対する。

・メール対応：随時（基本的には当日回答、時間や内容によっては後日回答）
・電 話 対 応：月曜～金曜　10 時～17 時
・窓 口 対 応：月曜～金曜　10 時～17 時

体制としては、以下に示すように、今回、新規に雇用する相談員 2 名以外にも、当研究所の研究員が相談に応対する。また状況や要望によっては（緊急性がある場合など）、時間外にも相談に応じるものである。



業務内容としては、パソコンや携帯電話を使ったインターネットの利用時に発生する情報モラルや情報セキュリティに関する相談、たとえばコンピュータウイルスの被害、個人情報の漏洩、ワンクリック詐欺、架空請求、オークション詐欺、掲示板の書き込みなど誹謗中傷・名誉毀損、ネットいじめ、出会い系サイトの利用によるトラブル、などである。相談内容を把握し、問題の対策（予防や事後処理）についてアドバイスを行う。また状況に応じて一時切り分け、ケースによっては連携機関への紹介を行うものである。

＜連携機関＞

・大分県警察本部 生活環境課　サイバー犯罪対策室
・大分県消費生活・男女共同参画プラザ「アイネス」
・大分県教育センター教育相談部
・大分県生徒指導推進室　ネットいじめサポート
・大分地方法務局　人権相談受付窓口
・その他

対象としては、県内の中小企業や NPO、情報モラルや情報セキュリティの対策が不十分な IT 利用者である。これまで情報モラルや情報セキュリティの普及啓発活動を県内で実施する際には、以下の団体とも協働を行ってきた。今回の相談窓口の設置においても各機関と連携して、業務を進める予定である。

＜その他の関連機関＞

・大分県産業創造機構
・大分県情報サービス産業協会
・大分県商工会議所連合会
・大分県商工会連合会
・大分県中小企業団体中央会
・18 市町村

（2）講習会の開催

①市町村出張講座

企業や個人の情報モラルや情報セキュリティの意識向上を図るには、IT を利用する際に身に付けるべき各種対策について学習する必要がある。また県下にまんべんなく普及啓発することが大事であり、大分県内 18 市町村に出向くことで参加を容易にすべく出張講座を実施する。

なお、各市町村の商工会議所、商工会、学校、PTA などから、別途に講座開催の相談があった場合は、効果測定をしつつ出張講座とは別に対応を検討し、できる限り多くの要望に応えるべく効果的な普及啓発活動を実施する。

・日程：市町村との調整による（土日および夜間帯は応相談）2 時間程度。
・対象：対象市町村の中小企業の経営者・管理者・情報セキュリティ実務担当者、商工会議所／商工会の担当者、自営業者、NPO 担当者、市町村職員・教育関係者、PTA、市町村住民など。
・講師：当研究所の相談員や研究員など。
・内容：情報モラルや情報セキュリティの対策の必要性と、具体的な対策方法について初心者が分かるように事例をあげて解説する。ウイルス対策、個人情報保護、ワンクリック詐欺、ネット通販におけるセキュリティ、業務上のデータ管理、ネット上の誹謗中傷などの問題や対策などの講義を行う。
・資料：講座の内容を復習できるように、資料を配布する。
・形式：初心者が分かりやすく学ぶことができるように、ビデオ上映やクイズ学習などを取り入れる。またネット上にある情報セキュリティ対策コンテンツを有効に活用する。さらに参加者が受講後に自己学習するために、また社内で研修会を開催できるように、参考となるビデオやパンフレットなどの教材を配布する。

②大分 IT あんしんフォーラム

情報モラルや情報セキュリティについて、政府はどのような対策を考えているのか。またその取り組みの現状と今後の課題について、日本の政策を検討している部署の専門家を招き、大分市にてフォーラムを開催する。

・日程：情報化月間などの平日午後、半日程度を予定。
・場所：大分市
・対象：大分県内の中小企業の経営者・管理者・実務セキュリティ担当者、商工会議所／商工会の担当者、自営業者、NPO 担当者、市町村職員・教育関係者、PTA、大分県民など。
・内容：政府が考える情報セキュリティ政策についての講演。またネットあんしんセンターの取り組みを事例に、地域の情報セキュリティ対策の今後について専門家を交えて

議論する。

・講師候補：内閣官房情報セキュリティセンター、JPCERT、IPA などから講師選定。

（3）セキュリティ情報の配信

情報セキュリティの脅威は日々変化しており、常日頃から情報モラルや情報セキュリティに関する情報の配信が望まれるところである。しかしながら、通常配信されている情報は、専門家や技術者向けのものがほとんどであり、一般の利用者にとって理解できないものが多い。誰にでもわかりやすく伝えるために、カタカナ用語や専門用語の解説、イラストを使った解説、文字の大きさや表現方法などの工夫を行う。

こうした情報アクセシビリティに関する作業は、これまでも当研究所において、高齢者や障がいを持った方、子どもやネット初心者などを対象として、各種講座やパンフレット、テキスト作成などで行ってきたものである。

①配信内容

・情報モラルに関する基本知識として、メールのマナーや掲示板などへの書き込みで気をつけること、ネット上の誹謗中傷や名誉毀損に繋がるようなトラブルなどの問題と対策情報。
・情報セキュリティ対策の基本知識として、コンピュータウイルス対策やウィンドウズのアップデートの方法など、最新の情報セキュリティ動向、事象問題に関する解説などの情報。
・緊急情報として、マイクロソフトや IPA、SPREAD などから発表される緊急情報。緊急に実施すべきウィンドウズのアップデートやウイルス対策など。
・相談窓口に数多く寄せられる内容についての対策情報。寄せられた内容を体系化、分類・分析する。

②配信方法

・基本的にはメール配信とするが、ポータルサイトなども活用する。
・利用者ニーズに合わせるべく、携帯端末などのモバイル形態も活用する。
・新たに出てくるサービスツール（SNS、Twitter など）も活用する。
・初心者へも確実に情報が伝わるように工夫する。（地域の広報誌や回覧板など）

③配信対象

現在、情報セキュリティに関する緊急情報を、シニアネット大分など NPO に所属するパソコン講師へ向けてメール配信している。今回ネットあんしんセンターから配信する情報は、できるだけ多くの人に伝えるために、地域で核となりうる商工会議所や NPO などの各団体にも配信して、さらにそれぞれの会員や関係者に情報が広がるスキームをつくる。

・大分県内 18 市町村
・大分県商工会議所連合会
・大分県商工会連合会
・大分県内 14 市商工会議所
・大分県内 4 町村商工会
・大分県 PTA 連合会
・大分県教育委員会および教育センター
・メディア（テレビ、地域 CATV、ラジオ、新聞など）

4．まとめ

2009年度には、この地域でのセキュリティセンターが現実のものとなるように関係各所へ働きかけを進めていきたいと考えている。しかしながら他の先進諸国と比較しても、IT投資やセキュリティ投資の低い、日本の一地方で構想を実現するのはなかなか難しい状況である。そこで重要なのが、地域のセキュリティは地域で守るといったセキュリティボランティアの育成である。それと連携機関との情報共有は、企業や個人が情報化を進めていくうえで、大きな手助けとなるだろう。

セキュリティセンターが単なる相談窓口としてだけ機能するのではなく、バックオフィス的な情報の流通と人の交流、円滑なるコラボレーションのために存在できるようになることを望むものである。情報環境は今後も楽観視できない未来社会において、少しでもその環境を重視したインターネット社会を築くべく、地域に立脚して、試行錯誤でも価値ある努力、活動を続けていくものである。

ハイパーネットワーク2009ワークショップ報告

今、問われる情報モラルとガバナンス

―地域で取り組む『情報公害（ネットいじめ、人権侵害、犯罪誘発・・・）』―

ハイパーネットワーク社会研究所
研究企画部長　渡辺　律子
watanabe@hyper.or.jp

2009年2月19-20日に、別府杉乃井ホテルにて、「ハイパーネットワーク2009ワークショップ」を開催した（主催：ハイパーネットワーク社会研究所）。今回は、「今、問われる情報モラルとガバナンス－地域で取り組む『情報公害（ネットいじめ、人権侵害、犯罪誘発・・）』をテーマに、子どもたちのケータイ利用の実態、国や企業の取り組みと課題、そして地域が取り組むべきことは何かを考える場として企画した。会議では高校生から70歳代のネットユーザまで98名が集い、2日間に渡り熱心に意見が交わされた。またその様子は地元の新聞やネット上のニュース記事等に掲載され、特に高校生の発表内容はかなり話題を呼んだが、それだけ大人が子どもの実態を良く知らないことを表しているとも言える。このハイパーフラッシュ44号ではワークショップの全体概要と講演内容に関連した記事を掲載し、ワークショップ特集号として報告する。

はじめに、セッション1では子どもの実態と問題、国や企業での取り組み状況と課題を確認した（コーディネータ：ハイパー研　渡辺律子、凜田和美）。

千葉大学　藤川先生

大分県下の高校生

千葉大学の藤川大祐氏は、「ケータイの子どもへの悪影響は、1.生活習慣（利用時間、友人関係）、2.被害・加害（詐欺や性犯罪など悪意ある大人からの被害や子ども同士の中傷など）がある。特に最近はプロフ（プロフィールサイト）の利用などから深刻な被害に繋がっている」と説明した。また「学校へ持込禁止にしても問題が主に学校外で起きているため解決にならない。家庭に責任を押し付けても親がしつけを出来ない中で限界がある」と話し、「事業者が抜本的な青少年対策をすべき」と指摘した。そして「フェールセーフ（利用者に誤操作があっても安全が確保される仕組み）や、利用者の年齢に応じて利用できる範囲が自動的に変わる『標準未成年プラン』といったしくみが必要なのではないか。行政は事業者に対してルールづくりをして欲しい」と問題提起した。続いて、大分県内の5名の高校生（男子1名、女子4名）が『ケータイ』の利用状況について、質問に答える形で発表した。4人

高校入学と同時に、１人は中学時代にケータイを購入している。「ケータイは１日中手放せない。なくなったら挙動不審になる」と答える生徒もいる一方、中学校から利用している生徒は「高校２年生になって利用時間が減ってきた」とも話した。女子は主にブログやプロフなどを利用して、日々の出来事など友達と情報交換している様子だった。「リアル（今、どこにいて何をしているかなどをその都度発信するサービス）」が流行しており、「友達の中にはリアルに友達の悪口を書く人もいた。悪口などの書き込みからクラスでもトラブルになった」という声もあった。一方、ケータイ小説の作品を書いて投稿したり、イラストを書いてネット上の仲間とやり取りしたりなど、ツールをうまく活用して自分の世界を広げている生徒もいた。「大人に言いたいことは？」という質問に「高校生に対してケータイのルールなど言っても無駄。反抗しない素直な時期に教育すべき」といった意見も出された。


モバイルコンテンツ審査・運用監視機構　岸原　孝昌氏

このほか、株式会社ディー・エヌ・エーの田中陽子氏から、モバゲータウンの健全性強化の取り組みについて、またモバイルコンテンツ審査・運用監視機構の岸原孝昌氏から、EMA の成り立ちや取り組みなどについての発表があった。

討論では、高校の教師から「以前はＰＴＡからケータイを学校に持ち込ませないでほしいと要望があったが、今はケータイの指導をしてほしいに変わった。入学説明会で気をつけることなど説明している」「生徒は授業よりも携帯に関心を持っている。どうやって指導するか頭を悩ませている」など現場の悩みが出された。これに対して全国高等学校 PTA 連合会高橋ＰＴＡ会長は「利用の仕方を大人がきちんと伝えていくべき。フィルタリングの言葉が一人歩きして、具体的に仕組みを理解せず、親が安心してしまう。子どもと親を一緒にならべてリテラシー教育をしていけばよい」と話した。また事業者に対して指摘があったことについて、KDDI 株式会社の辻中氏から「責任の重い事業だと実感している。フィルタリングを利用者がカスタマイズ出来るように進めている。また啓蒙活動（ルールマナー教育）を行っている。今回のワークショップでの貴重な意見などを反映していきたい」と述べた。他に参加者から「大人のリテラシー向上が必須」「ユーザー同士で学びながら使ううちに賢くなる仕組みを作って欲しい」「進化するテクノロジーに対して、適切なモラルが必要」などの意見が出された。


全国高等学校ＰＴＡ連合会
高橋正夫会長


ＩＴジャーナリスト
佐々木 俊尚氏

セッション２では、子供だけでなく社会全体が同じ問題を抱えていること、状況も刻々と変わっていることなどを取り上げ、それぞれの立場で出来ること、出来ないことも確認する場とした（コーディネータ：ハイパー研　会津泉、藤野幸嗣）。

IT ジャーナリストの佐々木俊尚氏は、「今後は動画などその空間をデジタライズ化してとらえていくことが IT 分野で日本がトップになれることではないか。ただしプライバシーと産業振興のバランスをどう考えるかが課題」と話した （4,5 ページ参照）。

続いてヤフー株式会社の別所直哉氏は、違法・有害情報対策の前提（可能なこと、可能でないこと）を「1.発信者を制限できない、2.何が書かれるかわからない、3.国外サーバからの発信も多く、誰が書いたか簡単に突き止められない、4.コミュニケーション手段の悪用を防ぐには悪人を捕まえるしかない」とし、その上で進めている取り組みについて説明した。また「違法・有害情報への対応を行ってきたが判断者はいったい誰なのか。社会的に許されないこと、有害ということを一企業が判断してしまっていいのか、表現の自由に影響しないか、など躊躇している」と心境を語った。

一方、ネット上の誹謗中傷問題が多いと言われる韓国の状況について、韓国ITジャーナリストの趙章恩（チョウ　チャンウン）氏は「韓国はPCの利用が中心。携帯からのネット利用ができるようになったのは最近である」「ネット上の誹謗中傷での自殺が多い。実名制度があるが、自分の意見を言うことに自信がある人が多い。有害情報対策、青少年保護に対する委員会も多いが、政府の経済対策を批判しただけで警察に拘束される状況もあり、行き過ぎた規制が課題」と説明した。

韓国ITジャーナリスト
チョウ　チャンウン氏

2日目のセッション3は、問題解決のために地域で取り組むべきことは何かを考える場とした（コーディネータ：ハイパー研会津泉、渡辺律子）。

交流会の様子

大分県教育庁生徒指導推進室主幹の佐藤晃洋氏から「県下の高校半数がまだ持ち込み禁止としていることもあり教育委員会としても原則持込禁止としている。ただ実際は学校におけるモラル教育、保護者との協力体制の構築が重要。特に実感できる情報モラル教育、コミュニケーション能力の育成が課題。問題が起きた後の対応について、ネットいじめ等相談窓口の設置やスクールカウンセラーの配置のほか、他の関係団体と連携していきたい」と発表した。大分地域若者サポートステーション臨床心理士の江口敦子氏（スクールカウンセラー）は「ここ数年、ブログに悪口を書かれたことでのトラブル相談が増えてきた。ネットでは書き込んだ相手が誰かわかりづらいため、人が信用できなくなる子どももいる。中には小学生のときのトラブルが中学生までひきずって、登校拒否になってしまった子もいる。傷ついた子どもの心のケアが難しいことが問題」と深刻な状況を話した。次に具体的に保護者の立場でできることについて、ネット教育アナリストの尾花紀子氏は、自身の子どものプロフを紹介しながら「実際に使わせながら親がサポータを務めるべき。子どもに携帯を持たせて、親が自分の時間を確保しようとしているのは親のわがまま。大人が責任回避することはやめて、家庭、学校、地域の連携が必要。IT環境誕生前に育った大人たちにできることがある（経験や知識からくる判断力の育成）」とした。ネットスター株式会社の高橋大洋氏は、フィルタリング提供側が目指している姿勢を説明したあと「フィルタリングだけでは解決できないことがあるため、保護者のリテラシー向上の取り組みに力を入れている。事業者側がもっと真剣にこの問題に取り

組むべき」と話した。

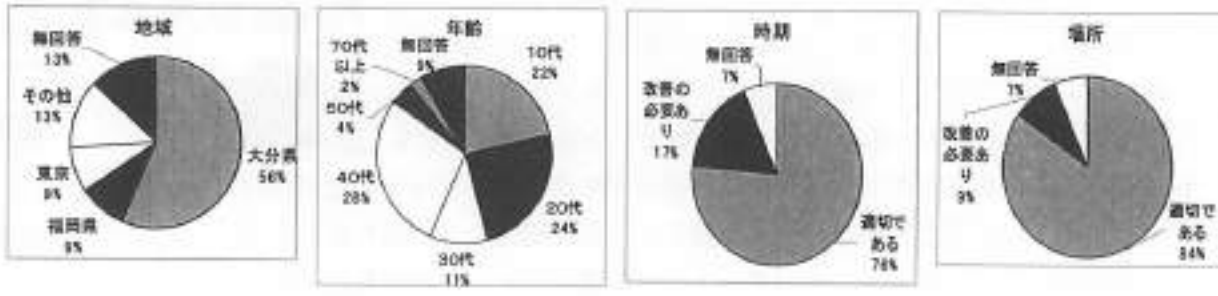
最後の討論では「学校、保護者、どっちが悪いという議論ではなく、現実的な仕組みはないか」「企業努力をさらに期待する。事業者が未成年の利用状況を把握して学校・保護者に問いかけるのはどうか」という意見が出された一方、「日本は心配しすぎ。韓国は学校の授業でITを使うので先生がITを使いこなし情報モラルは身に着けている。もっと子どもを信頼してはどうか」という指摘もあった。セッションのまとめとしてコーディネータの会津が「ワークショップ全体は地域からスタートして、また地域に戻りそして新しいことが始まる。自分の地域に戻って始めるためのいろんなヒントをいただいたと思う」と話し、ハイパー研の公文理事長は「前向きに使ってみるというやり方もある。学校とPTAがケータイを積極的に活用していくこともいいのではないか」と話した。最後にハイパー研の宇津宮所長より、「情報のライフラインになっているインターネットの利用には見えないものを想像する力が求められている。子どもを信頼してやらせてみることが大事。また地域で起きている問題は世界の問題ととらえ、さらにこれからも取り組みをすすめましょう」という閉会の挨拶があった。

2日間に渡るプログラムでは、各セッションから交流会、夜なべ討論会の中で、学校関係者、保護者、事業者、学生などさまざまな立場から意見や課題が出された。問題を絞り込んで掘り下げることは難しかったが、違う立場の考え方や取り組みについてお互いに情報交換でき、貴重な機会になったのではないかと思われる。このワークショップがそれぞれの今後の取り組みを進めるきっかけの一つになればと願うとともに、大分でも取り組みをさらに一歩進めたいと考える。

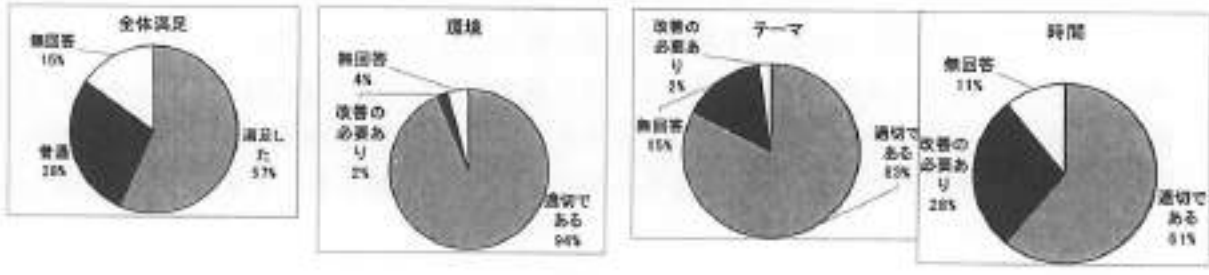
※ハイパーネットワーク2009ワークショップのプログラムなど詳細はこちらをご覧下さい。
http://www.hyper.or.jp/staticpages/index.php/ws2009/

【参考】ワークショップについてのアンケート結果
当日参加者98名（一般参加者58名、講師21名、ハイパー研スタッフ19名）、
アンケート回収数：46名

（1）参加者についての情報



（2）会議全体について



（3）セッション１についての意見・感想（抜粋）

- 高校生がよく発言していてよかった。モバゲーや携帯など、身近なテーマなので興味がわいた。
- 私、自身が短大生ですが、高校生の方々の話を聞いて驚きました。“リアル”というサイトの存在を知らないし、まずネットを利用しなかったからです。ここ数年で大きく使い方が変わったのだと思った。私は家のことを考えるとケータイを使えませんでした。だから今の学生の考え方に問題があると思った。自分で払っていないのが当然のような発言が驚きました。
- 中学生などが携帯を持つのは問題かなと思いました。書き込みの制限はむずかしいと感じました。
- 専門用語について分からないことが何度かあった。
- 世代によって利用するサービスの違いがわかって、これからの参考になった。
- ４つの立場からの発表を通して、中学生の関心が高いモバゲーの方針を知ることができました。今後も今、子どもたちが関わるサービスの会社に来て話しをしてもらいたいと思います。
- 様々な立場の方が一同に会して議論する場は無いと思いますので、非常に参考になりました。

（4）セッション２についての意見・感想（抜粋）

- 韓国みたいに、もう少し厳しくなるといいと思いました。
- ネット上での事件や犯罪についてよく分かりました。でも、少し内容が難しかったです。
- フィリタリングをつけていても１８歳をすぎて、いきなり外したとき、子どもは逆に無防備な状態になって危険だと思う。どのようなことが危険なのか実際に経験することが大事だと思う。
- 当初から健全への取り組みをしていたということですが、もし、問題発生がありその対策として新たに行ったものがあるのでしたら「問題の例をあげその対応としてこの対策をはじめた」とすると、さらにすばらしい活動をしてると伝えられるのではと思いました。
- 夫々の視点からの問題点が見え、利用者への教育（提案）の必要性を感じた。
- チョウ先生による韓国の事例が興味深かった。できれば、日本の事業者の感想をききたかった。
- 専門的なお話しが多くて少し難しかったです。
- Ｙ！のところで・・・有害情報の一例のところで、自殺を誘引する情報では、書き込む人はどんな思いなのか、学をひけらかしたいのか、自己満の為なのかな・・・とても気になりました。
- 問題の本質的なところが変わっていないのがよくわかりました。
- 議論をするのはいいが、何らかのはっきりした方向性（一方向でなくてもよい）が結論づけられていないのは、残念。
- 弊社側の反省としましては、もう少し発表する内容（特定のサービスのみ）を絞り込んだ上で企業姿勢も含めたガバナンスのお話をした方が良かったのかもしれません。全社的な話題ですと、若干つまらない話だったのではないでしょうか？

（5）夜なべ自由討論についての意見・感想（抜粋）

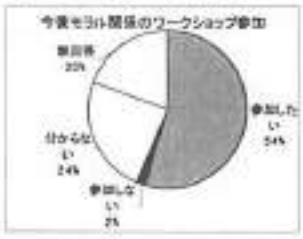
- 時間がもう少しあっても良かった。

・　話しをしやすい雰囲気で、参加者の考えを理解することができた。
・　人数が多すぎる。座談会のようにすべき。

（6）セッション3についての意見・感想（抜粋）

・　こどもを守ろう！の考えは構わないのですが、まずは親が子どもと対等もしくは上の立場になることから始めるべきだと思います。「パソコンは子どもの方が詳しいから・・・」と親が引いているから子どもがつけ上がるんです。（若干見下したり）
・　地域から何が出来るか、保護者が参加できるようなアクションプランの提案をもっと聞きたかった。
・　教育現場から大変関心がある３人の発表でした。発言をすることはできませんでしたが、見方・考え方を見直し、月曜から自分の研究に反映させていきたいと思います。
・　尾花さんの生の現場の声参考になりました。自分が親になる頃はどんな子どもたちを育てていくのだろうと不安になりました・・・
・　子どもをもっと信用するという考えには賛同します。いろんな考えがあってよかったです。
・　現在、発生している事例等のお話しが参考になりました。
・　フィルタリングは、「めんどう」という印象が強い。怖い世界も知っておかないと知らないことが一番怖いのではないだろうか、思った。
・　芦屋町では「脱ケータイ」を行っていますが、個人的には教育の情報化を進めていく必要性を感じています。社会的に情報モラル（いじめなど）が大きく取り上げられていますが、これから先の情報社会で生き抜くためにはモラルを基盤とする必要はありますが、情報活用能力こそが大切だと感じています。芦屋町では「ケータイ」についての考えを深め、それ以上に情報教育に力を入れていくつもりです。目標は、ケータイを含め情報を有効に活用できる生徒を育てることです。
・　相変わらず、技術屋さんの視点で話が展開してますね。教育関係者を低く見ていただいていると感じています。ネット利用の一番の問題を抱える子どもを置き去りにしたまま話が展開していて残念。佐藤さん尾花さんの話はとても有益でした。
・　率直な意見がでたことはよかったと思います。

（7）今後の参加について



（9）その他（抜粋）

・　すごくおもしろい話でした。勉強になり、このＷＳに参加出来よかったです。
・　同じ方が何度も発言していて、他の参加者の意見を聞けなかったり、自分が発言出来なかったのは淋しいですね。
・　危機感を持っていない人にモラルやリスクを話してもなかなか伝わらないので、もっと体験

できる場があればいいと思います。ＰＴＡで親全員にケータイを出させて、一斉にＷｅｂ検索してみるとか・・・。大学生も保護者も一般的には何の知識もない人が多すぎるので・・・。

- 情報化していく社会に後ろ向きでいたらマズイと本気で思いました。
- 教員がもっと参加しやすい形で行われると良いと思います。子どもたちと接する学校こそが情報を必要としていると思います。＊教育はどうしても教育関係でかたまりやすいので様々な方のお話を聞くことは大変勉強になりました。
- 今後も自分たちができることは、様々な人を巻きこんで、取り組んでいきます。
- この度は、このような会を設けていただきましてありがとうございました。とても有意義な１泊２日であったと感じております。今後とも何卒よろしくお願い申し上げます。
- さまざまな立場の人が一堂に会して議論することは、大変貴重だと思います。今回も、この点がとてもよかったと思います。特に、携帯電話をしっかり使っている高校生が来てくれたことは、大変よかったです。他方、講師やゲストの間で意見を交わすことが主なのか、一般の方々に適切に情報を提供することが主なのかが曖昧で、ややりづらかったと感じました。子どもと携帯電話・インターネットの問題については各所で頻繁に議論しており、今回のゲストの方々ともよくご一緒させていただいているので、たとえば「大分県での施策を決める」「携帯電話会社の人に提言する」というように話し合いのゴールがはっきりしているとよかったと思います。せっかくの温泉でしたが、大浴場が遠すぎて、夜のうちには行く気力がなく、結局朝になってようやく行けました。
- 技術的に閉じない難しいテーマと運営に挑戦するという、意欲的な試みを実現させたことに敬意を表します。また、そのような場に呼んでいただきありがとうございました。次回以降のさらなるチャレンジにも大いに期待しています。

大分県内の小・中・高校生のネット利用に関するアンケート調査結果

ハイパーネットワーク社会研究所
研究企画部長　渡辺　律子
watanabe@hyper.or.jp

1．背景

近年、子どもたちが携帯電話やパソコンを使ってインターネットを利用する際のトラブルがメディアなどでも頻繁にとりあげられるようになった。掲示板への誹謗中傷の書き込み、チェーンメールをはじめとする嫌がらせのメールや脅迫メール、プロフなどを通じての性的トラブル、架空請求などの経済的トラブルなど、問題は多岐にわたる。また携帯電話の利用が低年齢化したことから、こうした問題が小学生・中学生の間でも起き、2007年から2008年にかけては「学校裏サイト」「ネットいじめ」といったキーワードでニュースや新聞などに取り上げられた。そうした中、文部科学省は全国調査として行った「青少年が利用する学校非公式サイトに関する調査」結果において、2008年3月時点で学校非公式サイトが合計38,260個あると報告した。

大分県内においても、2002年ごろから、携帯電話を利用した掲示板への誹謗中傷などの書き込みからいじめが拡大し、登校拒否や裁判に持ち込むなどの問題まで発展しているケースもある。しかし実質、学校裏サイトなどの問題がどのくらい起きているのか、その実態はつかめていない。

そこで、今回、大分県内の子どものネット利用の実態について把握し、今後の普及啓発活動などに役立てるためにアンケート調査を実施した。

2．アンケート調査の実施

1.　調査期間・対象

今回のアンケートは、大分県教育庁生徒指導推進室にご協力いただき、各教育委員会を通じて配布・回収を行った。調査は2008年10月から11月の間で実施した。対象は大分県下の小学校5年生、中学校2年生、高等学校2年生、また中学校2年生の保護者、中学校・高等学校の教職員とした。

大分県内に広くアンケートを実施するため、できるだけ全ての市町村に1校は実施できるよう学校を選出した。調査対象の内訳を表1、表2に示す。

表1　アンケート調査回収数

校種	配布数	回収数	有効回収率
小学校5年生	2,427	2,383	98%
中学校2年生	3,374	3,198	95%
高等学校2年生	4,338	3,283	76%
中学校2年生の保護者	3,374	2,408	71%
小学校教員	879	777	88%
中学校教員	704	608	86%

表２　アンケート調査学校一覧

	小　学　校				中　学　校			
	学校名	5年生	教職員	計	学校名	2年生	教職員	計
中津市	南部小	22	12	34	緑ヶ丘中	206	39	245
	北部小	74	22	96	三光中	76	16	92
	大幡小	102	32	134				
豊後高田市	高田小	57	25	82	高田中	125	30	155
					真玉中	33	14	47
宇佐市	四日市北小	76	29	105	宇佐西部中	125	26	151
	安心院小	32	13	45				
杵築市	杵築小	92	31	123	杵築中	119	29	148
別府市	朝日小	103	38	141	朝日中	189	33	222
	鶴見小	85	29	114	山の手中	110	21	131
国東市	国東小	55	24	79	国東中	89	20	109
	安岐小	55	23	78				
姫島村	姫島小	25	12	37	姫島中	25	14	39
日出町	豊岡小	72	24	96	大神中	48	13	61
	日出小	51	22	73				
大分市	長浜小	31	17	48	碩田中	112	22	134
	豊府小	150	49	199	南大分中	290	47	337
	明野西小	137	40	177	城東中	257	48	305
	戸次小	110	32	142	大東中	320	39	359
	上戸次小	7	8	15	坂ノ市中	117	25	142
	判田小	174	53	227	判田中	162	34	196
	佐賀関小	26	13	39				
臼杵市	市浜小	80	27	107	臼杵西中	132	25	157
津久見市	津久見小	73	27	100	津久見第一中	127	25	152
由布市	挾間小	74	24	98	庄内中	67	22	89
	西庄内小	23	12	35				
	由布院小	64	26	90				
佐伯市	佐伯小	56	21	77	鶴谷中	196	36	232
	鶴岡小	114	35	149	直川中	29	12	41
豊後大野市	三重第一小	64	25	89	三重中	177	42	219
	緒方小	40	17	57				
竹田市	南部小	36	17	53	緑ヶ丘中	30	12	42
日田市	咸宜小	85	30	115	北部中	105	22	127
	光岡小	87	35	122	大山中	40	17	57
玖珠町	塚脇小	79	23	102	玖珠中	68	21	89
九重町	飯田小	16	12	28				
		2,427	879	3,306		3,374	704	4,078

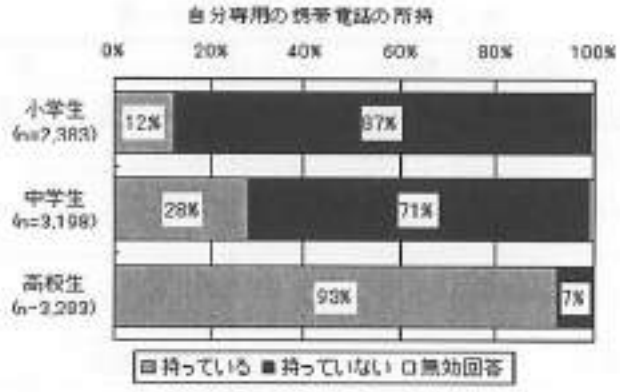


図１　自分専用の携帯電話の所持

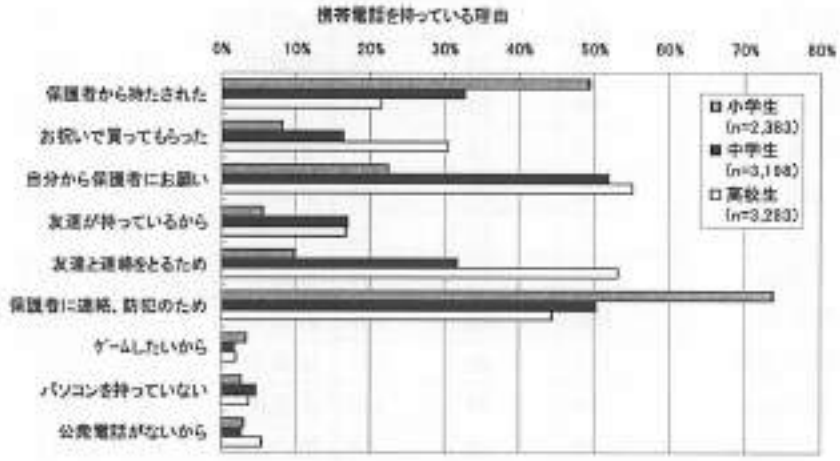


図２　携帯電話を持っている理由

2.　アンケート内容

主に以下のような内容についてたずねた。

○携帯電話の所持とその理由

○携帯電話での通話、インターネット利用、メール利用の状況

○メールのやりとりについて

○ネットサービスの利用経験

○トラブルの有無

○利用時に気をつけていること、ルールの有無

3.　アンケート結果

ここではアンケート結果のいくつかを示す。

携帯電話の所持について、「自分専用の携帯電話を持っている」と答えたのは、全体に対して小学生 12%、中学生 28%、高校生 93%であった（図１参照）。

携帯電話を持っている理由について、小学生は「保護者から持たされた」「保護者に連絡を取るため、防犯のため」が最も多い。中学生は「保護者に連絡、防犯のため」が「友達と連絡をとるため」「自分から保護者にお願いした」という回答も増える。高校生は「友達と連絡をとるため」「自分から保護者にお願いした」が最も多い（図２参照）。

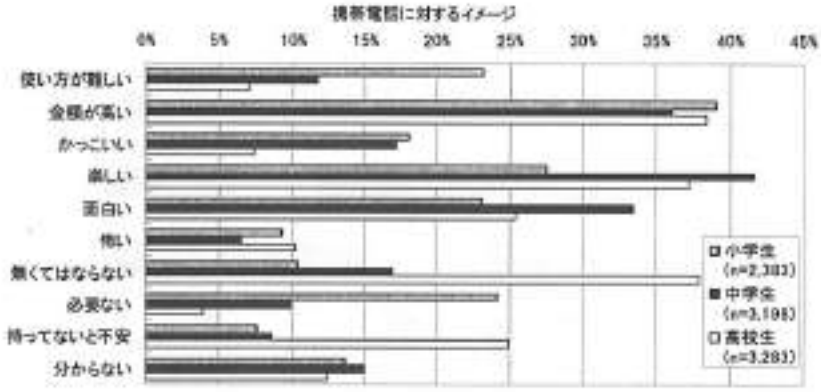


図３　携帯電話に対するイメージ

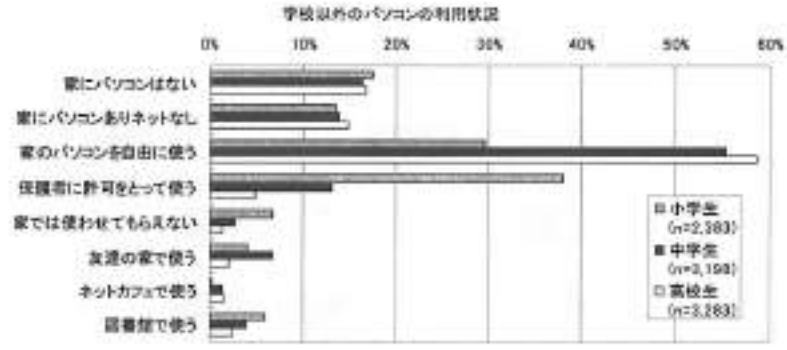


図４　学校以外のパソコンの利用状況

携帯を持っていない子どもはその理由について、小学生は「欲しいとは思わない、必要ない」が約 45%と最も多い。一方で中学生は「欲しいが保護者が反対する」という理由が 50%を超えて最も多く、続いて「必要時に借りる」「お金がかかるから」といった理由が多かった。

携帯に対するイメージは、全体に対して小学生、中学生、高校生ともに多かったのは「金額が高い」である。中学生は「楽しい、面白い」といった回答が最も多く、「怖い」ということ答えが他の校種に比べて最も少ない。高校生になると 35%程度が「無くてはならない」と感じ、25%弱が「持っていないと不安」と答えている。学年（年齢）により携帯電話に対するイメージが異なる（図３参照）。

学校以外でパソコンを利用する状況については、小学生は「自宅のパソコンを保護者に許可を取って使う」が最も多く約 35%である。中学生、高校生になると 50%～60%の割合で自由に使っている（図４参照）。

携帯電話を所持する児童・生徒のうち、携帯電話での通話利用は、「週 1,2 回」「週 3,4 回」が最も多く、「通話しない」がどの校種も 10%弱あった。

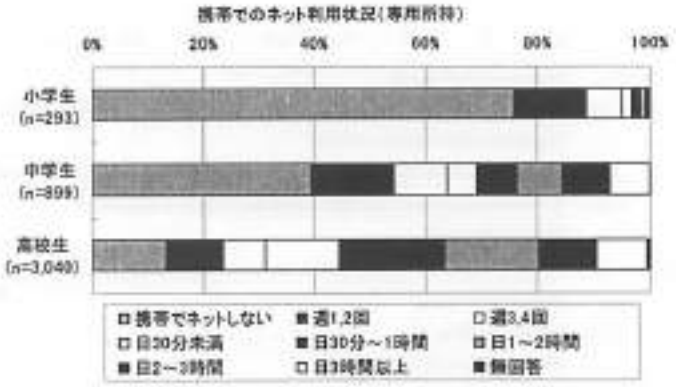


図5　携帯でのネット利用状況（専用所持）

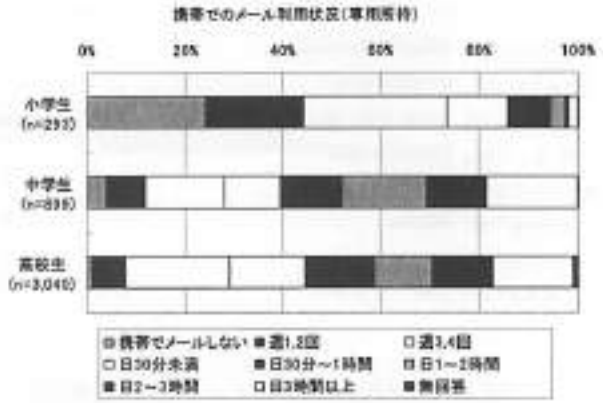


図6　携帯でのメール利用状況（専用所持）

また、「携帯でネットを利用しない」は、小学生 70%に対して、中学生 40%、高校生 10%である。携帯電話を所持する中学生の 60%以上、また高校生の 70%以上が、毎日 30 分以上から 3 時間以上、ネットを利用している（図5参照）。

携帯電話を所持する児童・生徒のうち、携帯電話でのメール利用は、小学生は「週 3,4 回」が多い。中学生、高校生は、「週 3,4 回」から「日 3 時間以上」まで幅広いが「日に 1 時間以上」という答えが 50%程度いることがわかる（図6参照）。

パソコンや携帯電話の利用時に、知らない人からメールが届いたことがあるかについて、小学生は全体の約 10%、中学生は 20%、高校生は 50%が「ある」と答えた。

知らない人からのメールが届いた人のうち、「どのように対応したか」、については、「無視した、削除した」が全体的に多い。続いて「とりあえず開いてみた」が 30%ある。「相手とメールのやり取りした」という回答は中学生、高校生に 10%見られた。さらに、相手に電話したという回答も少ないがあった（図7参照）。

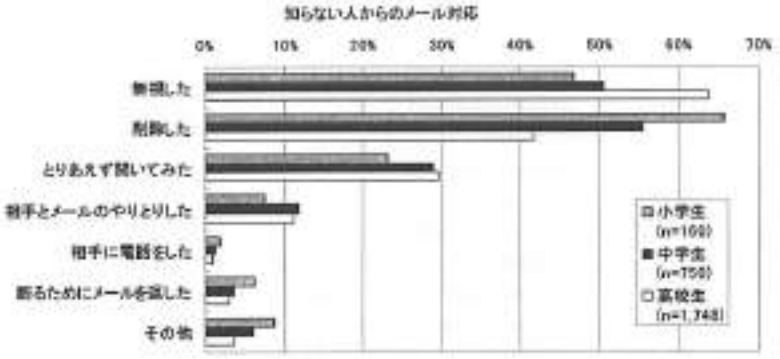


図7　知らない人からのメール対応

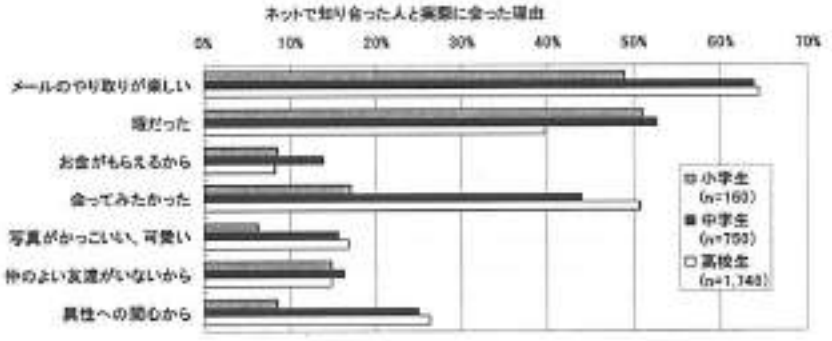


図8　ネットで知り合った人と実際に会った理由

また、「携帯やパソコンで知り合った相手と実際に会ったか、については「あったことがない」「無回答」が最も多い。「前にあったことがある」「今も会っている」という回答は小学生 160 人のうち、47 人、中学生 750 人のうち 116 人、高校生 1748 人のうち 365 人であった。

ネットで知り合った人と実際に会った理由は、「メールのやりとりが楽しい」が小学生 50%、中学生、高校生は 65%であった。次に「暇だったから」が小学生・中学生が 50%、高校生は 40%である。また、「会ってみたかった」は高校生、中学生が 45%から 50%あり、「異性への関心から」も 25%程度ある。回答数は少ないが小学生の 4 人、中学生の 6 人、高校生の 30 人が「お金がもらえるから」と答えた。このほか、「仲のよい友達がいないから」と答えたのはどの校種も 15%いた（図 8 参照）。

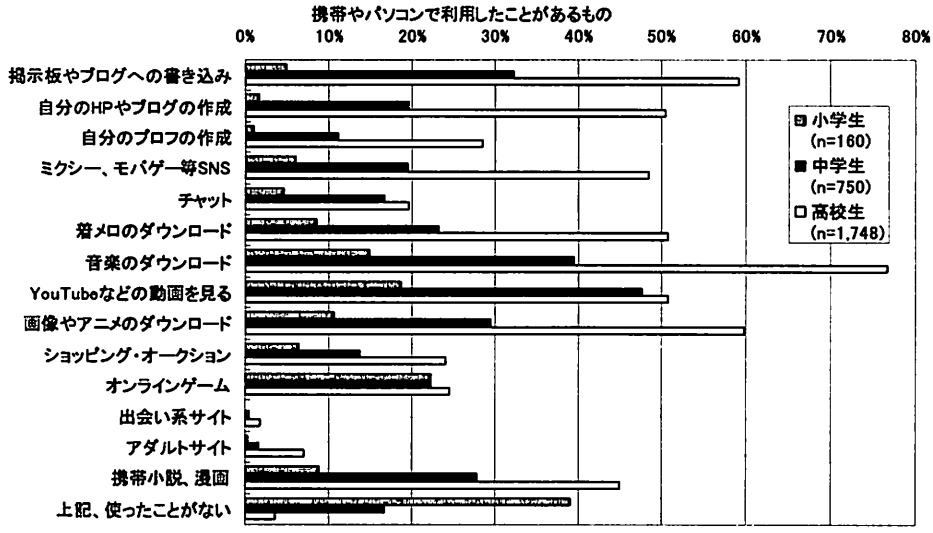


図９　携帯やパソコンで利用したことがあるもの

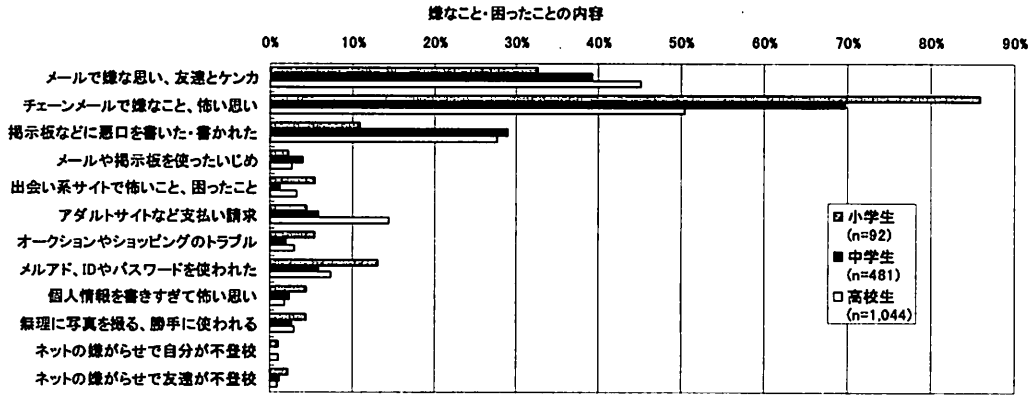


図１０　嫌なこと・困ったことの内容

携帯やパソコンで利用したことがあるものとして、小学生は「オンラインゲーム」が 20%で最も多い。中学生になると、「YouTube などの動画を見る」が最も多く 45%、続いて「音楽のダウンロード」約 40%である。「掲示板やブログへの書き込み」「画像やアニメのダウンロード」30%近くになる。高校生は「音楽のダウンロード」は約 75%が利用し、「掲示板やブログへの書き込み」、「自分の HP やブログの作成」などの情報発信も 50%となる。ほかに、「ミクシーやモバゲーなどの SNS の利用」、「携帯小説、漫画」などの利用も増えてくる（図９参照)。

携帯やパソコンを利用していて、「嫌なこと・困ったことがあるか」については「ある」と答えたのは小学生 4%、中学生 15%、高校生 32%だった。

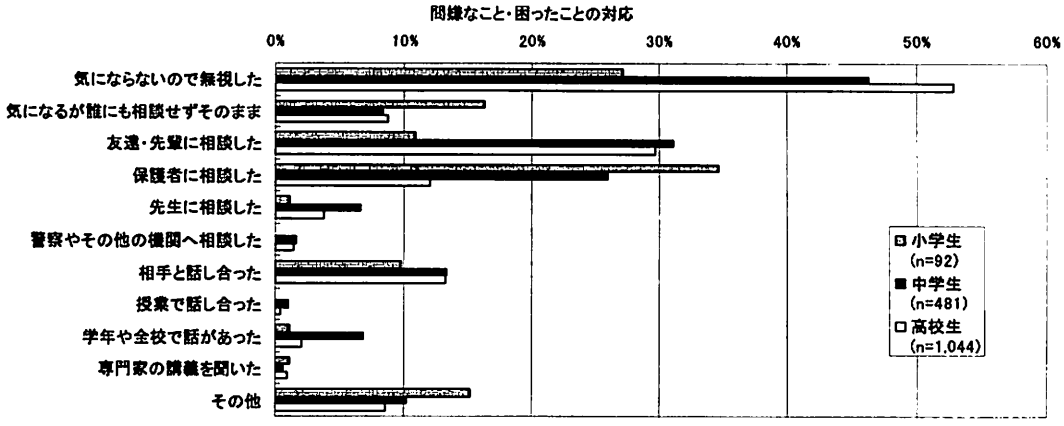


図１１　嫌なこと・困ったことの対応

嫌なこと、困ったことの内容は、小学生で最も多いのは「チェーンメールで嫌なこと、怖い思い」が 85%、中学生 70%、高校生 50%と最も多い。次に「メールで嫌な思い、友達とケンカ」の経験が高校生 45%、中学生約 40%、小学生 35%である。

掲示板などに悪口を書いた、書かれたといった経験を持つのは、中学生、高校生とも 30%弱、小学生が 10%である。また「アダルトサイトなど支払い請求」は高校生の 15%が経験があった。小学生の約 15%は「メルアド、ID やパスワードを使われた」というトラブルがある。ほか、「メールや掲示板を使ったいじめ」は、小学生 92 人のうち 2 人、中学生 481 人のうち 19 人、高校生 1044 人のうち 27 人が経験があった。数は少ないが「ネットの嫌がらせが理由で登校拒否になった」の答えもある（図１０参照)。

また「嫌なこと、困ったことの対応」については、「気にならないので無視した」高校生、中学生には多く 50%前後。小学生は保護者に相談したが最も多く 35%程度である。中学生、高校生になると、友達・先輩に相談したが最も多い。「先生に相談した」は 10%に満たない。また「相手と話し合った」はどの校種でも 10%見られた。このほか、授業、学校で話し合ったり、専門家の話を聞いたりはわずかであった（図１１参照)。

「これらの問題が解決したか」について小学生 40%、中学生 50%、高校生 60%が解決したと答え、小学生 15%、中学生約 10%、高校生の約 7%が解決していないと答えた。

また、文部科学省が行った学校非公式サイトについての質問をしたところ、「見たことがあるか」、については、全体のうち中学生 20%弱、高校生 30%が見たことがあると答えた。

見たことがある生徒のうち、学校非公式サイトを知った理由は、「友達や先輩に聞いて」が最も多い。小学生は、「きょうだいから」や「検索して」が多い。中学生、高校生になると、ブログを見てそうした掲示板を知ることも多い。

これらのサイトへの書き込み経験については、小学生、中学生は 80%が「ある」と答え、高校生は半々であった。

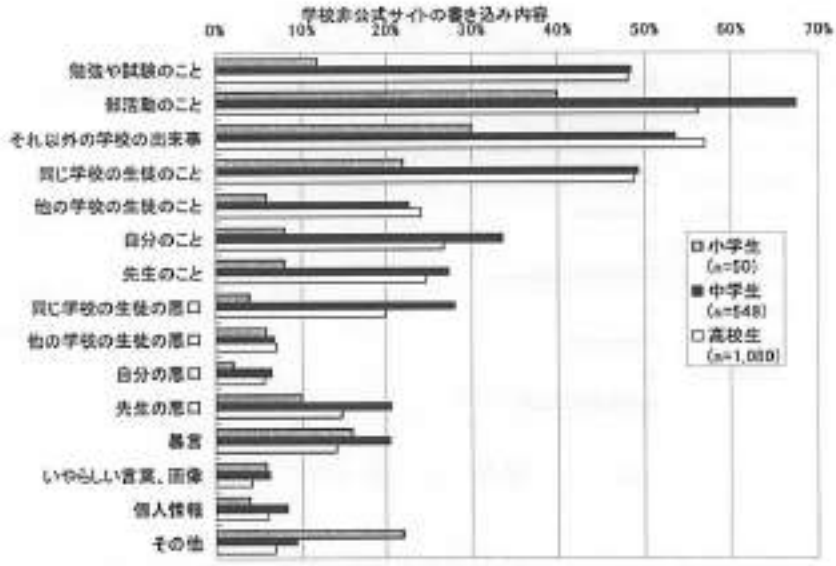


図１２　学校非公式サイトの書き込み内容

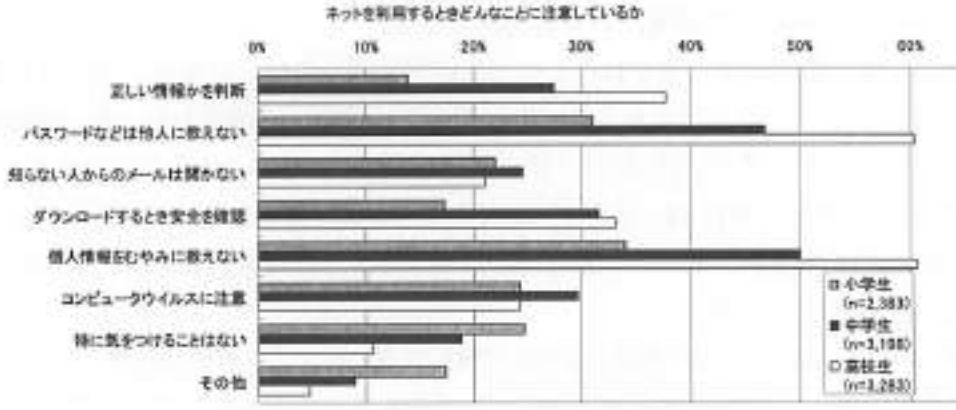


図１３　ネットを利用するときどんなことに注意しているか

学校非公式サイトに書き込まれた内容は、中学生高校生ともに最も多いのは「勉強や試験のこと」「部活のこと」「それ以外の学校の出来事」である。また、「同じ学校の生徒のこと」「自分や先生のこと」なども多い。そのうち、「同じ学校の生徒の悪口を見たのは」、中学生 20%～30%、高校生は 20%である。「先生の悪口」「自分の悪口」を見たという回答もある（図１２参照）。

ネットを利用するときにどんなことに注意しているか、中学生、高校生は「パスワードなどは人に教えない」、「個人情報をむやみに教えない」が最も多い。一方、小学生の 25%は「特に気をつけることはない」と答えた（図１３参照）。

気をつけることを誰に教えてもらったか、については、小学生・中学校では保護者が最も多い。また、「教えてもらったことがない」はどの校種も 25%から 30%程度あった。高校になると学校の先生や友達・先輩といった回答も 10~15%ある。

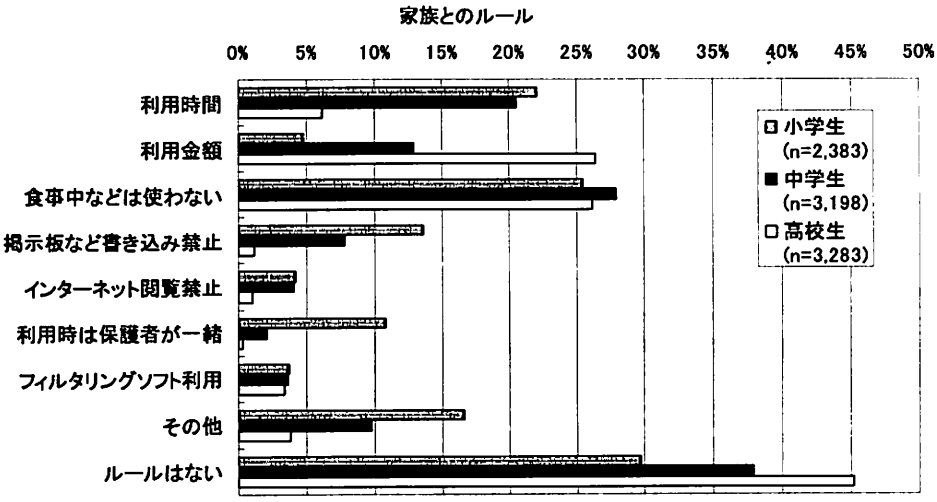


図１４　家族とのルール

家族とのルールは、「ルールはない」が小学生 30%、中学生 37%、高校生 45%と最も多い。ルールがある場合は「食事中などは使わない」がどの校種も多いが、それと同じくらい高校生は「利用金額」についてが多い。小学生、中学生は「利用時間」について 20%ほどがルールがあると答えたが、高校生は 5%程度であった（図１４参照)。

4.　今後の課題

今回の集計は校種・学年による比較など単純な集計に留まった。今後は次のような点についてクロス集計など行い解析をしたいと考える。

・全国調査との比較
・男女差
・地域差
・専用の携帯電話を持つ生徒と持たない生徒の違い

また、教職員や保護者に対して実施したアンケートを集計し、

・保護者・教職員の意識
・子どもと保護者の経験や意識の差
・学校での情報モラル教育の現状

などについて、解析結果を出したいと考える。

さらに、今回は集計のしやすさを考えてマークシート記入方式を選んだため、具体的な活用について調査できなかった。今後はヒヤリングなどの手法を用いて、子どもたちが実際にどのようなサイトをどのように利用しているかなどについて調査したいと考える。

Web2.0からソーシャルメディアとスマートフォンへ

ハイパーネットワーク社会研究所
主任研究員　菊池　達哉
kikuchi@hyper.or.jp

数年前、Tim O'Reilly が Web2.0 を提唱したことにより Web の世界は久々に活気づいた。技術的には、それまで不遇の扱いを受けていた Javascript が再び脚光を浴び、それを利用することでインタラクティブなユーザインタフェースの実現(Ajax: Asynchronous JavaScript+ XML)が可能になり、Web がより使いやすいものとなった。このユーザインタフェースを利用した代表例は Google 社の Google Map である。Google Map が実現したユーザインタフェースは、これまでの Web の規定概念を打ち破るものだった。

この結果、Web 利用者だけでなく Web 開発者も Web2.0 に期待を抱くことになり、さまざまな Web2.0 と言われる Web サービスが登場し、中にはそれでビジネスを立ち上げる者まで現れた。まさに、Web2.0 がネットの未来を担うような勢いであった。

しかし、時間の経過とともに Web2.0 も技術的な側面だけを言えば、衰退というよりは、むしろ一般化されていった。そのため、Ajax などの技術だけでは差別化を図るのが難しくなり、淘汰の波に煽られて、消えてなくなる Web サービスやニーズのあるものは巨大企業の買収されることになった。

一方、2008 年はスマートフォンの分野に大きな変化があった。それは、iPhone の登場である。iPhone は Apple 社から 2008 年 7 月に日本ではじめて発売された。iPhone は、電話機能やネット機能はもちろん、GPS を搭載し、多種多様なアプリケーションを必要に応じて使うことができ、また、それ自身の OS もバージョンアップすることも可能で、タッチスクリーンのユーザインタフェースを採用した新世代のスマートフォンである。この新しいスマートフォンの登場は、新しい Web の活用を予感させるのに十分であった。

私は、この iPhone を地域で活用できないかと考え、総務省の平成 21 年度戦略的情報通信研究開発推進制度(SCOPE)に、「地域住民の“信頼”と“人間関係”を基盤にした地域防災 SNS に関する研究開発」という課題名で大分県立芸術文化短期大学の凍田教授とともに共同提案した。これは、GPS やマップなどを駆使できる iPhone のポテンシャルと比較的にクローズドで親密度の高い SNS を組み合わせることで、平常時の地域のコミュニケーションと災害時の地域の助け合いを支援する防災 SNS システム構築の提案である。この共同提案は、21 年 4 月に採択されることになった。iPhone をはじめとするスマートフォンは、この防災 SNS で上手く活用できると考えているが、もう少し緩やかなコミュニケーション、つまり肩肘を張らないコミュニケーションで潜在能力を発揮するのではないかとも思っていた。

しかし、それは 2009 年 2 月に開催されたハイパーネットワーク 2009 ワークショップのときに疑問は解決した。この疑問を解いたのは、Twitter だった。Twitter とは、140 文字以内の文章を”つぶやく(書く)”マイクロブログのことである。Twitter は各ユーザー間でフォロワーという関係を構築することで、相手のつぶやきを参照したり、必要があれば返信などができる Web サービスのことである。この Twitter は、2 年前の 2007 年に登場して、一部(主に Geek と言われる人達)の間で一時的には活発化したのだが、次第に下火になっていった。

ところが、ワークショップの会議中に参加者がTwitterを用いて”つぶやいた”のである。実世界(リアル)で会議が進行している時に、Twitter(仮想)上でワークショップの参加者が自由に意見を言っているのである。私は、参加者の意見やコメントがTwitterという別の世界で同時に並行して発言されていることに驚きを感じた。ワークショップの後、有識者からのヒアリングやWebなどを調査し、Twitterと同様なWebサービスが多く存在することや、これらのWebサービスを総称して「ソーシャルメディア」と呼ばれていることがわかってきた。ソーシャルメディアとは、コミュニケーションを行うメディアであるが、既存のWebサービスと比較して情報を取捨選択することが可能であり、ユーザー間をゆるやかに結びつけるのが特徴である。しかし、「ソーシャルメディア」という言葉は、まだ一般化された定義ではないことに注意が必要であるが、このTwitterをはじめとするソーシャルメディアに新たな可能性を感じた。さらに、iPhoneに代表されるスマートフォンを組み合わせることで、特定の場所の旬な情報をリアルタイムにその場所にいる不特定多数の人に伝える手段になりえると考えている。これは、既存のWebやメール、検索エンジンなどでは困難なことである。

このような流れの中で、私は、TwitterをはじめとするソーシャルメディアとiPhoneに代表される新世代のスマートフォンをうまく組み合わせることで、地域の活性化、特に地域の商店街を支援できるのではないかと考えている。例えば、「今、この場所で、何ができるか？」という買い手のニーズと「今、この付近で、○○をしています」という売り手のニーズをスマートフォンとソーシャルメディアでうまくマッチングできれば、地域での販売促進につながるのではと考えている。今後、ソーシャルメディアとスマートフォンを用いた地域活用の研究をより深く行うことで、地域の活性化につなげていきたいと考えている。

大分県オープンソースソフトウェア研究会における取組みと活動報告

ハイパーネットワーク社会研究所　　大分シーイーシー株式会社
主任研究員　中川　俊哉　　ｸﾞﾙｰﾌﾟﾏﾈｰｼﾞｬ　江原　裕幸
nakagawa@hyper.or.jp　　hi-ehara@cec-ltd.co.jp

1．はじめに

これまで大分県オープンソースソフトウェア研究会（以下、OSS研究会）はハイパーネットワーク社会研究所を事務局として、2006年7月27日設立から約2年半オープンソースソフトウェア(OSS) の普及啓発に努めてきました。2007年度までは公募事業の推進を中心とした活動でしたが、活動の中心をセミナー開催や地域間連携、サーバを購入したOSS利活用調査へとシフトいたしました。

その間、大分県では、OSP基本パッケージを利用した図書館インターネット閲覧システムの導入が行われ、学校教育現場でのOSS継続の取り組みが行われています。

本報告書では、2008年度にOSS研究会が実施した活動について報告します。

2．２００８年度の活動内容（セミナー開催等）

2008年度は、7つのセミナー開催を行いました。その概要は以下のとおりで、主催3回、共催3回、併催1回を行いました。

(1)．第11回大分県オープンソースソフトウェア研究会【主催】

◆日時：2008/07/31(木) 14:00~17:00

◆会場：大分第2ソフィアプラザビル（ソフィアホールA）

◆概要：OSSベースのSIビジネス~IT化サービス

- 「明朗会計で中小企業のローコストIT化を強力に応援する！
  ~OSS活用が生んだ脱人月の新サービス"ギョイゾー！"~」
- 「ギョイゾー！」を利用してみて
- 「ひろしまオープンソフトウエアコンソーシアム」での発表について

図1．講演の様子1
(株)スターロジック
羽生 章洋 氏（代表取締役社長）

図2．研究会の様子

図3．講演の様子2
大分シーイーシー(株)，大分県OSS研究会
江原 裕幸(グループマネージャー，副会長)

(2)．第12回大分県オープンソースソフトウェア研究会【主催】

◆日時：2008/10/31(金)13:30~17:00

◆会場：大分第2ソフィアプラザビル（ソフィアホールA）

◆概要：「仮想化技術と OSS」セミナー
オープンソースカンファレンス２００９大分キックオフ

図 4. 講演の様子
日本仮想化技術(株),(株)ぴぎねっと
宮原 徹 氏（代表取締役社長兼ＣＥＯ）

図 5. 研究会の様子 1

図 6. 研究会の様子 2
大分県 OSS 研究会
宇津宮孝一（大分県 OSS 研究会会長）

(3). JaSST'08Kyushu（ソフトウェアテストシンポジウム）【共催】
◆日時：2008/11/07(金)10:00～17:00
◆会場：大分県消費生活・男女共同参画プラザ（アイネス）
◆概要：概要：NPO 法人 ソフトウェアテスト技術振興協会（ASTER)、JaSST' 08Kyushu 実行委員会との共催により、現場で役立つ、テスト設計・テスト技法を体験する。

図 7. 基調講演の様子

図 8. チュートリアルの様子

図 9. 発表の様子

(4). LL 温泉 2008 大分（湯布院）【共催】
◆日時：2008/11/07(金)10:00～17:00
◆会場：日本文理大学湯布院研修所
◆概要：日本文理大学と協力して、Lightweight Language（軽量言語）の Perl、PHP、Python、Ruby などの 4 大 LL のチュートリアルを合宿形式で開催

図 10. チュートリアルの様子

図 11. 夕食の様子

図 12. 会場からの湯布院の風景

(5). セキュリティ＆プログラミングキャンプ・キャラバン 2008 大分【共催】
◆日時：2009/02/21(土)10:00～16:00
◆会場：日本文理大学（25 号館 7 階 プレゼンテーションルーム）

◆概要：若年層の情報セキュリティおよびプログラミングについての興味を深めることと優れたセキュリティ＆プログラミング人材の発掘と育成、また、正しい情報セキュリティの理解と意識の向上を図ってもらうこと目的として開催

図13．ポスター

セキュリティ＆プログラミングキャンプ・キャラバン 2008 大分

図14．キャラバン会場の様子

（講師：左から）

・園田 道夫 氏　サイバー大学

・吉岡 弘隆 氏　ミラクルリナックス(株)

・国分 裕 氏　三井物産セキュアディレクション(株)

・宮本 久仁男 氏（株）NTT データ

図15．講師陣との質問の様子

(6)．第13回大分県オープンソースソフトウェア研究会【主催】

◆日時：2009/02/21(土)10:00～16:00

◆会場：日本文理大学（25号館　7階　プレゼンテーションルーム）

◆概要：OSSにおける勉強会の意義

「技術を高めるために勉強会を開催したいけどどうすればいいの?」

「なぜ、大分では勉強会が開催されていないの?」

「そもそも、勉強会ってなによ?」

図16．講演の様子
ミラクル・リナックス(株)
吉岡 弘隆 氏

図17．研究会の様子

図18．パネルディスカッションの様子
サイバー大学 准教授　園田 道夫 氏
日本アイ・ビー・エム　花田 智洋 氏
ミラクル・リナックス(株) 吉岡 弘隆 氏

(7)．オープンソースカンファレンス2009大分【併催】

（2日目：第14回大分県オープンソースソフトウェア研究会（OSC2009大分併催））

◆日時：2009/03/13(金)13:00～17:30、14(土)10:00～16:00

◆会場：大分第２ソフィアプラザビル（ソフィアホール）

◆概要：オープンソースに関する最新情報の提供、セミナーを１２本、研究会併催で地方とOSSについてパネルディスカッションを実施。

図19．カンファレンスの様子

図20．展示ブースの様子1

図21．展示ブース（日本文理大学）

図22．パネルディスカッションの様子

図23．展示ブースの様子2

図24．展示ブース（OSS研究会）

上記の様に本年度も多くのセミナーを開催でき、OSSの普及啓発に役立てたのではないかと考えます。

３．２００８年度の活動内容（その他）

(1).OSS研究会サーバ利活用

セミナー以外の活動として、OSS研究会で購入したサーバを会員企業へ貸し出しを行いました。２社へ３台を貸し出し、OSSの利活用（実験）に取り組んでいただきました。なお、この利活用の実績をOSS研究会で報告してもらい、会員間で有効利用できることを目的としています。

（貸し出し概要1）

◆貸出期間：2008年10月20日～2009年6月30日

◆サーバ数：２台

◆実施内容：仮想環境Xenの構築、その上で動作する仮想環境の構築を実証の目的とした。実証内容をレポートにて報告すると共に、他会員への仮想環境提供を実現する。

（貸し出し概要2）

◆貸出期間：2008年11月17日～2009年6月30日

◆サーバ数：１台

◆実施内容：自作開発したソフトや利用しているアプリケーションの制限により新しいＯＳバージョンへの移行ができない(高コストになる)場合があり、新しいハードウエア(サーバマシン)で古いＯＳを動かせれば、大きなコストを負担しなくて済むというメリットがある。そのため、新らしいハードウエアに対応できなくなった古いＯＳを仮想環境にて再利用できるか実証する。

(2). 対外的な活動

OSS 研究会では、昨年度に引き続き、外部セミナーへの参加・発表を行い、県外の様々な方からの意見の収集に努め、大分の活動の広報を行ってきました。

- 2008 年 5 月　「2007 年度自治体等実証実験成果報告会」
- 2008 年 5 月　「ひろしまオープンソースソフトウェアコンソーシアム」
- 2008 年 8 月　「NetCommons ユーザカンファレンス 2008」
- 2008 年 9 月　「オープンソースカンファレンス 2008 Shimane」
- 2008 年 12 月　「オープンソースカンファレンス 2008 Fukuoka」

4. 今後の取り組み

これまで、セミナー開催などの普及啓発に取り組んできました。今後は、以下について取り組み、OSS の発展に貢献していきたいと考えています。

- OSS 研究会でアンケートを実施し、これまでの取り組みの見直しを行う
- OSS でビジネスへと繋がる取り組みにシフトする
- 勉強会の実施を検討

大分県における自治体ＥＡ調査研究

ハイパーネットワーク社会研究所
主任研究員　工藤　賢　　事務局長　青木　栄二　　主任研究員　中川　俊哉
kudo@hyper.or.jp　　blue@hyper.or.jp　　nakagawa@hyper.or.jp

１．大分県における自治体 EA 調査研究の経緯

現在、情報システムの最適化計画はコスト削減が主目的となっているが、今後は業務やシステム全体の最適化及び住民満足度の向上も必要となる。
先進自治体では自治体ＥＡ（Enterprise　Architecture）という手法により最適化を図り、業務見直しをシステム構築と伴わせて導入している。

大分県においても行政システム、情報システムの効率性の向上とコスト削減を図るため、業務システムの構造化検討（現状分析、課題の洗い出し）や目的達成のための業務、システムの刷新について調査・研究を行った。

ここでは、その報告および考察を述べていくものである。

２．自治体ＥＡ業務・システム構造化に関する調査

どういった取り組みを行うことで自治体 EA を実現しようとしているのか調査するため、全国的な先進地事例を調査した。

福岡県では「ふくおか共通基盤」を利用することにより、コスト削減・住民サービス向上・地元企業の振興に繋げようと取り組んでいる。さらに福岡県電子自治体共通化標準技術では①縦割りのシステム開発による弊害、②システムが複雑となり、大手ベンダーへの依存が強まったことによる弊害、③人的な能力に依存した情報戦略立案、といった課題を解決するために構築し、他の自治体も技術的な標準として利用してアプリケーションを作成すれば、相互にシステムの利用が可能となるような形態を目指している。

岐阜県では県、市町村、(財) 岐阜県市町村行政情報センター、地元企業が協働で岐阜県標準システムのモデル化に取り組み、共同利用効果を一層高めたサービスを提供することとしている。このモデル化では、自治体、民間、NPO 等が連携することで、情報資源の有効活用による効率化が期待される。個別の取り組みでは実現できなかった新たな住民サービスの情報化を目指している。

北九州市では業務および業務システム間の連携を主眼に置き、組織体制・業務手順の見直しを含め、全体最適化の視点から、行政組織およびその情報システムの“あるべき姿”を目指している。情報システム再編の面では、増設・改修を繰り返すことで複雑化し、コストの透明性が保てない現行のホストコンピュータを核とした情報システムを廃止または極小化していき、オープン系の情報システムへ再構築する計画である。さらに、オープン系の技術で構築された分散システムも対象として統合することで、さらなる効率化を目指している。

3．自治体共通プラットフォームに関する調査

地方公共団体の情報システムにおいて「システムの標準化」により、システム同士を連携させ、業務処理の連携、データ共有を可能にすることを目指している。

総務省が推進している地域情報プラットフォーム構想については図１に示すとおりである。

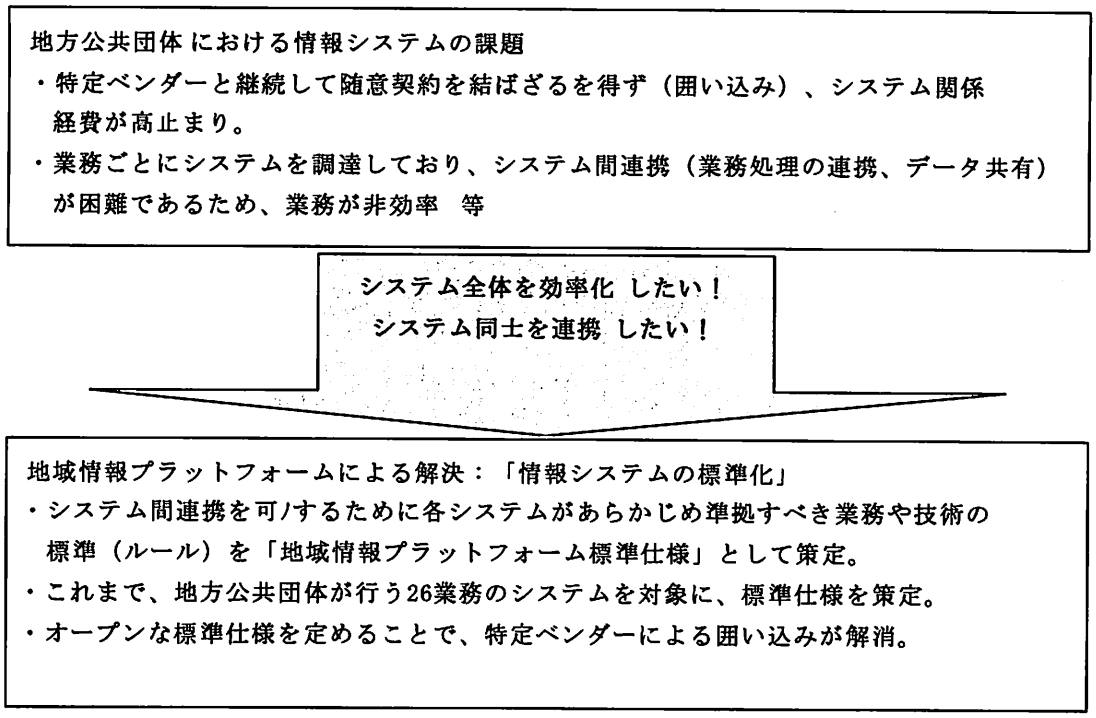


図１　総務省が推進している地域情報プラットフォーム構想
引用：総務省 地域情報プラットフォーム構想概要

4．第１回アンケート、第２回アンケート、ヒアリング調査

第１回のアンケートでは、各市町村における共通プラットフォームに関する意向を把握し、システム構造化を検討（現状分析、課題の洗い出し）することを目的に調査を行った。どの市町村でも共同利用でコスト削減をしたいという考えは一致しているが、各市町村のシステムリプレース時期が異なっているため、足並みをそろえて同時期に共同利用を開始することは非常に困難であると思われる。

第２回のアンケートでは共同利用についてさらに詳細を調査した。システム共同利用する業務については、利用頻度や業務効率の面を照らし合わせて自治体間で協議を行い、カスタマイズを極力行わない方針で取り組んでいく場合には運用している業務の見直しも含めて業務フローや処理方式を十分に検討することが必要である。

ヒアリング調査で、ワンストップサービスがなかなか進まないのは、費用対効果が期待できないことや、様々な業務スキルをもった人材育成の難しさが要因としてあることがわかった。

５．研修会

自治体共通プラットフォームや自治体 EA・共同化について先進自治体の取り組みや国の動向、大分県における共同化の現状について広報した。また、各自治体におけるシステム部門の問題点・課題を共有し、各自治体の担当者同士が意見交換を行った。

第１回
日　時：平成 21 年 1 月 15 日（木）13:00～17:30
場　所：大分県別府市田の湯町 13-13　つるみ荘　カトレアの間

第２回
日　時：平成 21 年 1 月 16 日（金）9:30～12:00
場　所：同　上

６．メリット・デメリット

システム共同利用化にどんなメリットがあるのか。これまでは共同アウトソーシングという言葉のみ先行していたが、ここへきて、地方行政の情報システムマネージメントのあり方が問われ出してきているため、厳しい財政状況とも相まって、明確にメリットが打ち出されるようになってきた。実際に共同利用化への期待度は高く、かりに共同アウトソーシングセンターなるものができれば業務システムの課題解決のため、人材の派遣もしていきたいという声がヒヤリング調査において、いくつかの市町村から聞くことができた。

・単純にコスト削減の可能性がある
・各自治体における担当者間の情報共有ができる
・情報共有により課題解決が容易になる
・情報システム関連の人材育成につながる

ではメリットに対してデメリットはどんなことが考えられるのか。共同利用が進まない一番の大きな原因は、このデメリットを過大に危惧することで、メリットが見えなくなることだ。業務上、どうしても目の前の課題解決が先行することも問題を難しくしている。

・システムに合わせての業務変更や体制変更の可能性がある
・職員研修へ多大な労力がかかる
・既存の条例や規則との整合性や改正問題がある
・リプレースの時期と移行にかかる諸問題の整理の必要性がある
・システムを入れ替える場合の職員意識をどう考えるか部局間の壁がある

これらのメリットとデメリットを見た場合、綿密な業務システムの構造化検討を実施して、現状分析や課題の洗い出しを行えば、ほとんど解決できるのではないかと考えられる。問題は各自治体に専門家がおらず、担当者も 2～3 年で交代するなかで、余計なコンサルティングコストをかけずにできるかということである。

さらに共同化利用にあたっては、各市町村自身の自律と併せて、市町村間の連携が必要とされる。それぞれの自治体は、人口も違えば、地理的状況や産業構造も違う。こうした違和感のなかで、どのようにして動的な平衡をとっていくのか。現場担当者レベルの横連携も必要だが、首長

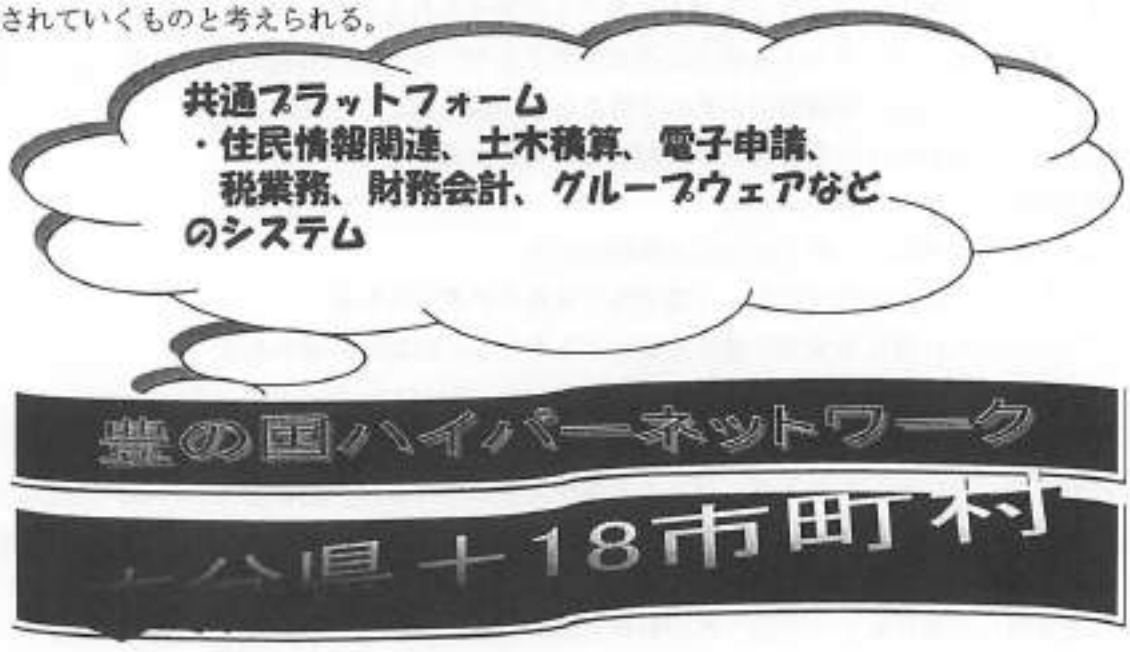
レベルの会合でも議論をしていくことはできないものか。単に一自治体のトップダウンだけではなく、首長同士の意見交換と横連携ができれば効率的な共同利用化の可能性が広がるのではないだろうか。

そのためには、前述のメリットとデメリットを市町村ごとに明確化、見える化したうえで、全体的な大分県としてのロードマップを提示することが、電子自治体推進の大きな役目ではないだろうか。ひいてはそれが一般ユーザ（大分県民）の利益につながるのではないかと考えるものである。

7．今後の展開

今回の調査研究で実施した研修会には、全市町村に参加いただき、そうした情報共有の場・意見交換の場というものが大変評価された。県内の事例を聞くことができる機会やベンダーも同席して質問に答えてもらう機会が非常に重要であることが分かった。大分県では、「電子自治体推進協議会」がその役を担ってきたので、今後もそうした場の企画検討が望まれるところである。またその協議会において、地域全体を将来予想も含めてデザインしていけるようなロードマップを作成することで、確固とした共通プラットフォームの構築が期待できるものと考える。

具体的には、一度にすべての1県18市町村がシステム変更して共同利用化することなど不可能なので、上記のようにできるところからやっていく。行政の業務の都合ではなく、一般ユーザ（大分県民）の視点に立ったサービスを、県と市町村が一緒になって検討していくべきではないだろうか。コスト削減と効率性が図れないサービスが取り残されて売れなくなるように、売れないサービスではなく、利活用されていくものが望まれる。大分県にはすでに「豊の国ハイパーネットワーク」なるセキュアで効率的な行政ネットワークが県内くまなく張り巡らされているので、この上で、共同アウトソーシングを活性化させることで、理想的な共通プラットフォームがモデル化されていくものと考えられる。



九州広域での危機管理体制確立のための
情報通信（ＩＣＴ）プラットフォーム構築に関する調査検討

ハイパーネットワーク社会研究所
主任研究員　菅 智広
suga@hyper.or.jp

・はじめに

この報告は、平成 20 年 7 月総務省九州総合通信局の「九州広域ＩＣＴプラットフォーム調査検討会」開催にあたり、「九州広域での危機管理体制確立のための情報通信プラットフォーム構築に関する調査検討」に関する請負として、財団法人ハイパーネットワーク社会研究所が、(1)調査検討会（作業部会）の準備・運営、(2)実証実験の実施、(3)周知啓発イベントの開催、(4)報告書のとりまとめ等　に関する事務局運営をおこなったものである。

・危機管理体制確立のために

九州地方では従来から台風や集中豪雨、それによる土砂災害や河川災害などの自然災害が数多く発生しており、その度に多くの被害を受けてきた。時に人命をも奪う危機事象への予測とその対策は、地域住民の安全・安心な生活を確保するためにも必要不可欠である。これら自然災害の他、感染症や家畜伝染病については発生する場所や時期の予想が難しく、ここ数年の間には東九州地域で牛口蹄疫や鳥インフルエンザなどの家畜伝染病が発生し、生産者をはじめ監督機関・流通販売事業者・消費者・地域住民に大きな影響を与えている。

このような家畜伝染病等をはじめとした広域的なエリアに影響を及ぼす危機管理情報に対して、地域の枠を越えた体制の整備が求められており、被害の縮小や地域住民の安心・安全な生活を確保するため、情報通信技術を活用した「九州広域での危機管理体制確立のための情報通信（ＩＣＴ）プラットフォーム構築に関する調査検討」がおこなわれることとなった。

・調査検討会の体制

本調査研究における調査検討会の名称は「九州広域ＩＣＴプラットフォーム調査検討会」（以下「調査検討会」）とされ、調査検討における実証実験等を円滑・効率的にすすめるため、調査検討会の決定に基づき「九州広域ＩＣＴプラットフォーム調査検討会作業部会」（以下「作業部会」）の設置がおこなわれた。

調査検討会は、学識経験者、各県の情報政策担当、ＩＣＴ関係団体、九州情報通信連携推

進協議会のメンバー15名から構成され、九州広域での危機管理体制の確立に資する情報通信プラットフォーム構築に向け、県域を越えた広範な危機管理情報の入手・伝達が可能となるネットワークやアプリケーションに関する調査検討を行うものとし、その結果を調査検討会の成果として取りまとめることを目的とする。この目的達成に向け、課題等抽出のための実証実験実施の他、九州広域ＩＣＴプラットフォーム構築に向け「広域ネットワークシステムの要件に関する技術的検討」「広域アプリケーションサービスに関する検討」「広域ＩＣＴプラットフォーム管理運営体制に関する検討」に対する課題検討及び、調査検討の成果を広く周知するための周知啓発イベントを開催する。

作業部会は、大学の獣医学関係者、県の情報通信分野及び防疫（畜産）分野の関係者、並びに九州情報通信連携推進協議会関係者から構成され、防疫情報の広域共有化のための実証実験など必要な作業を行うことを目的とする。

また、調査検討会の事務局を総務省九州総合通信局に置き、事務局運営は財団法人ハイパーネットワーク社会研究所が担当した。

・実証実験の検討

家畜伝染病は、発生した場所やその感染能力の大きさなどによっては県域を越えた対策が必要であるが、現時点では国、県、市町村などを中心とした垂直的連携を基準としたものが多く、隣県などへの影響を考慮した水平的対策を想定しているケースは少ないと思われる。また、実際に家畜伝染病の発生する現場は、都市部や住宅地から離れた山間部等に多いため、情報通信基盤の整備が遅れている地域である事が想定される。これらの地域で家畜伝染病等が発生した場合、迅速な情報収集や情報伝達ができずに、一刻も早い処置が必要とされる初期対応が遅れることとなりかねない。

これらの課題や調査検討会にて検討された実証実験概要を核にし、作業部会では対象フィールドの選定や実験実施スケジュール、実験進行イメージ（シナリオ）、ネットワーク構成などより詳細な部分を決定した。検討事項をより精査した結果、実証実験については、行政機関を越えた危機情報の水平展開を検討するものと、情報通信基盤が未整備な発生現場からの迅速かつ効率的な情報伝達手法を検討するものに分け、「複数の県における危機管理情報の広域共有化実験」（以下「実証実験１」）と「地理的条件不利地域における危機管理情報の伝送実験」（以下「実証実験２」）としてそれぞれ実証実験がおこなわれた。

・実証実験１

ここでは、家畜伝染病が大分県及び宮崎県の県境付近で発生したと想定。行政機関を跨る危機管理情報の広域共有化実験として、両県間の公共ネットワーク相互接続や共通アプリケーションソフト（※家畜防疫マップシステム）を活用することにより仮想のプラットフォームを構築し、各行政機関の間で必要とされる迅速な情報共有の姿について、次の課題２点について実証実験がおこなわれた。

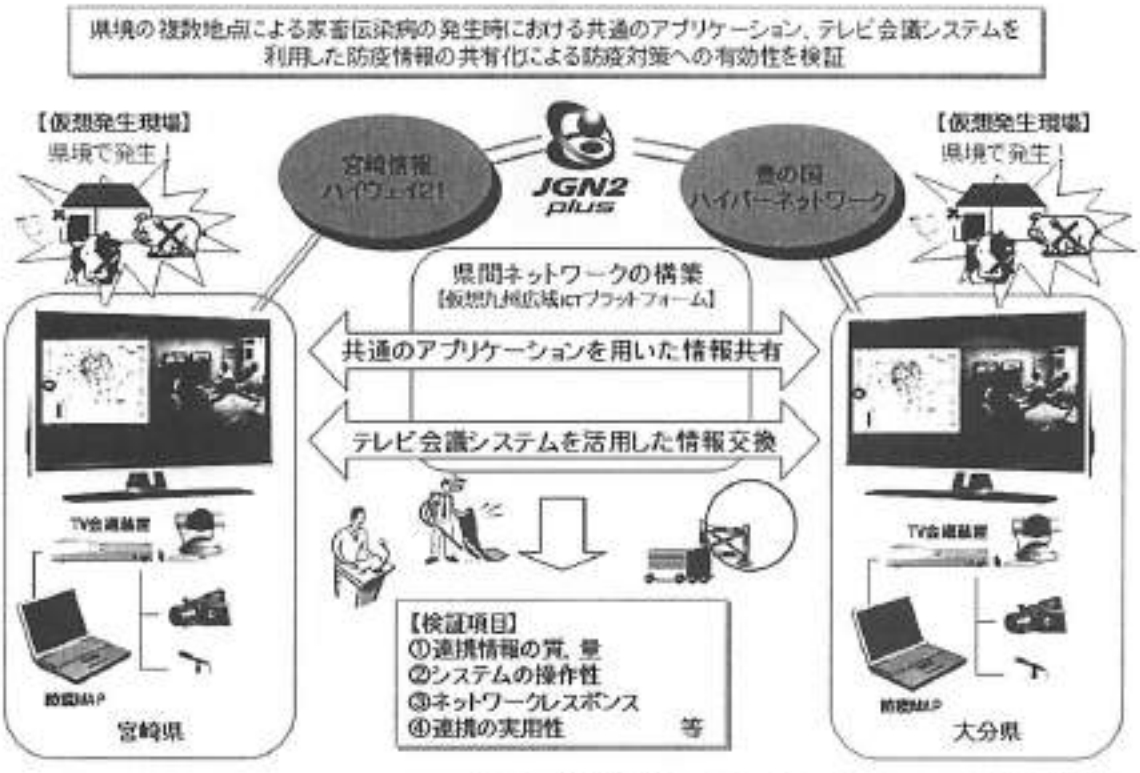
◎ネットワークプラットフォームの検証

ＪＧＮ２Plus や両県の情報ハイウェイ、庁舎ＬＡＮを相互接続したネットワーク基盤に、ＴＶ会議システムを設置し、その有効性有用性を検証。

◎アプリケーションプラットフォームの検証

家畜防疫マップシステムをアプリケーションプラットフォームとして、地理情報の共有できる環境を構築し、その有効性有用性を検証。

九州広域ICTプラットフォーム調査研究　実証実験1　全体構成図



出展：九州広域ＩＣＴプラットフォーム調査検討会

実験結果として、既存のネットワークを相互接続した県庁間ネットワーク環境にて、ハイビジョン画質ＴＶ会議システムによる安定的なコミュニケーションが確認できた。また、情報共有できるプラットフォームがあれば位置情報や画像データを相互に交換でき、迅速かつ的確な対応が可能である事を実証された。

個別に整備されたネットワークを相互に接続する事はそれほど難しい事ではないが、アプ

リケーション部分においては、例えば共通のＧＩＳプラットフォームのようなものがないと困難であったと思われる。

大分県側

宮崎県側

※家畜防疫マップシステム
（株式会社日建コンサルタント開発）
平成１６年２月、大分県内で鳥インフルエンザが発生した経験をもとに、防疫作業時の多くの課題を解決すべくシステム開発を行い、平成１８年度に大分県が導入したもの。県の担当職員および県下の家畜保健衛生所担当職員の意見や要望を取り入れた「現場仕様のGIS（地理情報システム）」である。

・実証実験２

情報通信基盤が未整備な（ブロードバンドや携帯電話も使えない）地理的条件不利地域で発生した危機管理情報に対して、いかに迅速かつ効率的に現場から情報伝達をおこなうかを実験課題として、以下の2つの実証実験がおこなわれた。

◎テンポラリー（臨時的）ネットワーク検証

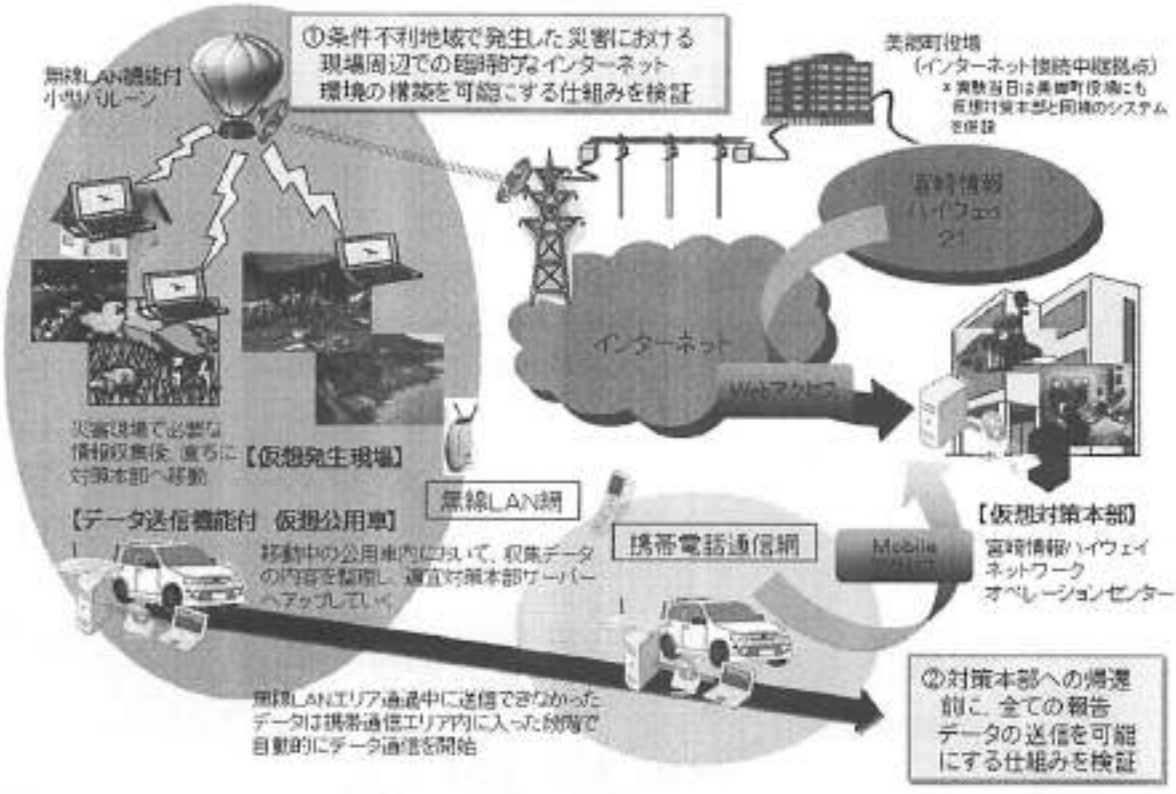
発生現場が起伏の激しい山間部であると想定し、無線LAN通信を小型バルーン上（空中）で中継させたテンポラリー（臨時的）なネットワークインフラを構築し、SkypePhone による音声コミュニケーションの確立、現場写真を添付したメールの送信、Skype ビデオ会議システムによる動画映像送信、地図情報システム（GIS）での情報共有を検証。

◎断続的ネットワーク環境での検証

一刻も早い本部等への現状報告が求められる状況であるにもかかわらず、現場からの帰路（移動中）についても通信状況が不安定（断続的）であると想定し、その車中から本部へのデータ伝送を可能とするＤＴＮ技術の有効性を検証。

場所については、中山間部であるとともにネットワーク設備や実験設備提供の他、役場職員の多大な協力を得る事ができた宮崎県東臼杵郡美郷町（西郷区）でおこなわれた。

九州広域ICTプラットフォーム調査研究　実証実験2　全体構成図



出展：九州広域ＩＣＴプラットフォーム調査検討会

実験結果として、エンドtoエンドのスループットは約2.5Mbpsあり、音声、ＴＶ会議、地図情報ともに情報共有の確認ができた。また、断続的ネットワークにおいても、再送信する事無く確実にデータ伝送をおこなうことが確認できた。つまり、仮想災害発生現場から対策本部への、迅速かつ効率的な情報伝達手段となりうることが検証された。

バルーン打ち上げ中

ビデオ会議システム（現場から本部へ）

※ ＤＴＮ（Delay Tolerant Network：遅延容認型ネットワーク）は、(独)情報通信研究機構九州リサーチセンターで研究開発中の技術で、断続的（常に繋がっていない）な通信ネットワーク環境下においてもデータ伝送を保障し、通信手段を確立するための技術。

・周知啓発イベント

危機管理情報の広域共有化を目指したＩＣＴプラットフォームの実現に向けた取り組みを広く周知啓発するため「九州広域ＩＣＴプラットフォームシンポジウム in 大分」が開催された。本調査検討会にて実施した実証実験の報告とそのデモンストレーションを交えながら、危機管理情報の共有化のための最新の技術動向や、その実現に向けた課題と解決策について、危機管理情報の専門家、有識者及び九州のＩＣＴ関係者に出演していただいた。

パネルディスカッションでは、宮崎県美郷町及び、宮崎大学医学部、ＮＩＣＴ北陸リサーチセンターの計３箇所と会場を接続し遠隔出演していただいた。

プレゼンテーション

会場の様子

【開催概要】

（１）名　　称　『九州広域ＩＣＴプラットフォームシンポジウム in 大分』
（２）開催日時　平成２１年２月２４日（火）１３：３０～１７：００
（３）会　　場　大分県消費生活・男女共同参画プラザ「アイネス」大会議室
（大分県大分市東春日町１－１）
（４）主　　催　総務省九州総合通信局
九州広域ＩＣＴプラットフォーム調査検討会
次世代高度ネットワーク九州地区推進協議会
（５）後　　援　九州情報通信連携推進協議会（ＫＩＡＩ）
大分県
独立行政法人情報通信研究機構大手町ネットワーク統括研究センター
社団法人九州テレコム振興センター
総務省北陸総合通信局
ＪＧＮ２Ｐｌｕｓ北陸地区推進協議会
九州インターネットプロジェクト

【プログラム】

（1）開会挨拶　　〔敬称略〕

主催者代表　武井 俊幸　総務省九州総合通信局長

来賓挨拶　平野 昭　大分県 副知事

（2）プログラム１：基調講演

「危機管理対応情報共有技術による減災対策」

鈴木 猛康　山梨大学大学院教授

（特定非営利活動法人防災推進機構 理事長）

（3）プログラム２：プレゼンテーション

「危機管理情報の広域共有化に向けた実証実験の取り組み」

コーディネーター

西野 浩明　大分大学工学部准教授（調査検討会座長代理）

プレゼンテーター

小林 信喜　九州総合通信局情報通信連携推進課 課長

長友 信裕　宮崎地域インターネット協議会 副会長

（調査検討会作業部会長）

広岡 淳二　九州情報通信連携推進協議会 事務局長

（4）プログラム３：パネルディスカッション

「九州広域ＩＣＴプラットフォームによる安心・安全な地域社会の形成に向けて」

コーディネーター

尾家 祐二　九州工業大学大学院教授（調査検討会座長）

パネリスト

池ノ上 克　宮崎大学医学部長・産婦人科教授【遠隔出演】

堀井 洋一郎　宮崎大学農学部獣医学科教授

宮川 明大　石川県七尾市企画政策部情報政策課【遠隔出演】

山崎 正幸　九州経済連合会情報通信委員会企画部会長

山戸 康弘　大分県企画振興部ＩＴ推進課 課長

（5）閉会挨拶

尾家 祐二　九州広域ＩＣＴプラットフォーム調査検討会 座長

パネルディスカッション

会場後方より

・**今後の課題**

正確で信頼性、安全性のある危機管理に対応する「広域ＩＣＴプラットフォーム」の実現に必要な要件である、基盤となる九州広域接続のネットワーク、ネットワーク上で展開される多様な広域アプリケーション、さらにそのＩＣＴプラットフォームの管理運営についての検討がおこなわれた。

１．広域ネットワークシステム

（１）相互接続におけるバックボーンネットワーク

①接続手法の検討

それぞれのネットワークで特徴や特性が異なっていること、バックボーンネットワーク上では多様なアプリケーションの利用が想定されることなどから接続手法の十分な検討が必要。具体的な接続形態としては、広帯域を確保した同一のＶＬＡＮ構成とし、セキュリティの観点からアプリケーションの種類に応じてＶＬＡＮタグを区別することが考えられる。併せて、フレキシブルな相互接続のためにアドレスやルーティング等を一元管理していく仕組みづくりの検討も必要になってくると考えられる。

②接続技術の検討

危機管理情報はいつ発生するか予測できないものである上に、緊急性を要するため、異種ネットワークが混在する広域接続配下のネットワークにおいては、広域ネットワークシステムへ常時接続可能なネットワーク環境を事前に構築しておくことが重要。そのための接続技術として、ＶＰＮ、オーバーレイネットワークといった「仮想化」技術や危機管理情報を広域プラットフォーム上で優先的に伝送させるＱｏＳ技術などの実装が考えられる。

（２）条件不利地域における情報伝達保障技術

バルーンを活用した無線ネットワーク環境の構築やＤＴＮ技術を活用した移動体からのシームレスな情報伝達手段の確立等については一定の有用性が検証できた。しかし、現場地域のロケーションやネットワーク環境は多種多様であり、各地域の実情を細かく分析したうえで、様々な通信技術を組み合わせながらその地域に最適なネットワーク接続環境を設計する必要がある。

２．広域アプリケーションサービス

（１）広域アプリケーションの活用と基盤技術

①活用形態としては、共通・統一のシステムに基づく広域アプリケーションの共有化が望ましいと考えられるが、導入コストやセキュリティ対策等の面から、現実的には既存利用しているアプリケーションの広域化検討が考えられる。

②広域アプリケーション構築には、これまで以上に基盤技術とインターフェイスの標準化・統一化の推進が求められる。また、この分野における論議はあまり活発では無いため、今後も必要な情報収集と調査をおこなっていくべきと考える

（２）広域アプリケーションのサービスモデル

①危機管理情報において広域アプリケーションサービスが果たす最大の役割は、危機管理体制マニュアルに基づく諸活動のために必要な情報収集と提供の支援である。そのため、

操作性、汎用性、拡張性への配慮とともに、当該自治体間で業務連携して実施展開できる機能が求められる。

②防疫分野、防災分野、地域医療分野といった危機管理のみならず、教育研究分野、自治体業務分野等を含めてアプリケーションを階層化した仕組みの上で検討していくことが現実的。そのためにも、各自治体を超えた広い産学官体制など九州全体で進めていく事も重要。

3．広域ＩＣＴプラットフォーム管理運営体制

①直接の利用者となる自治体の理解と協力とともに、産学官による連携した新たな取り組みが必要。

②プラットフォームの現状の物理的管理運営にとどまらず、機能的にも進化し続けることを想定した管理運営体制が望まれる。それぞれの専門性を生かした各アプリケーションごとの部会や、プラットフォームの利活用や各種実験を推進する企画推進ワーキンググループ、調査研究や各種開発を支援する技術開発ワーキンググループを設ける事が適当である。

③実サービスへの課題として、管理運営維持コスト、費用対効果の詳細な検討と、各地域や団体におけるコンセンサスの醸成が求められる。

今後、九州全域における広域ネットワークの構築・運営は課題が多いものの、継続していく必要がある。一方で、ネットワーク構築のシミュレーションや実証実験の積み重ねは重要であり、ネットワーク管理者や産学官が一体となった取り組みが求められる。

美郷町の青空に打ち上げられたバルーン

・調査検討行程〔参考〕

時　期	項　　目
平成２０年 ７月２４日	「第１回調査検討会」 開催（場所：総務省九州総合通信局） ・調査検討会の設置（開催要項の承認、座長の選任等） ・調査検討会の進め方 ・具体的な検討内容、スケジュール等の確認 ・実証実験の概要検討（実験項目、ネットワーク構成、実施体制、実施時期等）
９月１０日	「第１回作業部会」開催（場所：大分県庁内会議室） ・調査検討の概要について ・作業部会の進め方について ・実証実験の実施及びスケジュール等について
１１月４日	「第２回作業部会」開催（場所：宮崎県庁内会議室） ・実証実験の実施に向けた調整
１１月１３日	「実証実験１」実施（場所：大分県庁 及び 宮崎県庁）
１２月５日	「実証実験２」実施（場所：宮崎県東臼杵郡美郷町西郷区）
１２月１２日	「第２回調査検討会」開催（場所：福岡市博多区朝日ビル内会議室） ・実証実験結果の報告 ・九州広域ＩＣＴプラットフォーム実現に向けた検討 ・周知啓発イベント企画（案）の確認
平成２１年 ２月２日	「第３回作業部会」開催（場所：大分市ソフィアホール会議室） ・報告書案（実証実験結果報告）の説明及び確認 ・周知啓発イベント（シンポジウム）について
２月２４日	「九州広域ＩＣＴプラットフォームシンポジウム in 大分」開催 （場所：大分市アイネス大会議室）
３月１２日	「第３回調査検討会」開催（場所：熊本市ＫＫＲホテル熊本） ・シンポジウムの報告 ・調査検討報告書（案）の検討
３月２７日	「調査検討報告書」納品

巻末資料

■ ハイパーネットワーク２００９ワークショップ in 別府

■ 情報モラル啓発セミナー

■ 情報誌「ハイパーフラッシュ」

■ 普及啓発セミナー「ハイパーフォーラム」

■ ハイパーネットワーク社会研究会

■ 研究所スタッフ活動履歴

■ スタッフ一覧

■ 役員一覧

■ 賛助会員一覧

■ハイパーネットワーク２００９ワークショップ in 別府
「今、問われる情報モラルとガバナンス　ー地域で取り組む『情報公害（ネットいじめ、人権侵害、犯罪誘発・・・)』」実施報告

Ⅰ．内容

テーマ：「今、問われる情報モラルとガバナンス
ー地域で取り組む『情報公害（ネットいじめ、人権侵害、犯罪誘発・・・)』」

日　時：2009年2月19日（木）13：00～2月20日（金）12：00

場　所：杉乃井ホテル（大分県別府市）

主　催：財団法人ハイパーネットワーク社会研究所

定　員：当日実参加者98名（内訳：一般参加者58名、講師21名、スタッフ19名）

協　賛：東芝ソリューション株式会社　ネットワンシステムズ株式会社　富士通株式会社

後　援：大分県教育委員会、社団法人 全国高等学校PTA連合会、
特定非営利活動法人 ＩＴコーディネーター協会、独立行政法人 情報処理推進機構、
社団法人 日本インターネットプロバイダー協会、
特定非営利活動法人 日本ネットワークセキュリティ協会、
財団法人 日本情報処理開発協会、ＮＨＫ大分放送局、大分合同新聞社

Ⅱ．プログラム

◆2月19日（木）

○オープニング 13:00～

公文 俊平（ハイパーネットワーク社会研究所理事長）

○セッション1　13：15～16：00

『今、ネット社会で起きている問題（前半）～子どもの世界で起きている問題をどうする？！』

【発表】

藤川 大祐（千葉大学教育学部）

大分県内の高校生

田中 陽子（株式会社ディー・エヌ・エー）

岸原 孝昌（一般社団法人モバイルコンテンツ審査・運用監視機構）

【討論】

・コーディネータ

渡辺 律子（ハイパーネットワーク社会研究所）

凍田 和美（ハイパーネットワーク社会研究所）

・コメンテータ

辻中 伸生（KDDI株式会社）

高橋 正夫（社団法人全国高等学校PTA連合会・大分県高等学校PTA連合会）

渡辺 武経（社団法人日本インターネットプロバイダー協会（JAIPA））

○セッション2　16：00～18：00

『今、ネット社会で起きている問題（後半）～利用者・事業者を含む新しいガバナンスとは』

【発表】

渡辺 律子（ハイパーネットワーク社会研究所）

木付 吉弘（大分県警察本部サイバー犯罪対策）

佐々木 俊尚（ITジャーナリスト）

別所 直哉（ヤフー株式会社）

趙 章恩（チョウ チャンウン）（韓国ITジャーナリスト）

【討論】

・コーディネータ

会津 泉（ハイパーネットワーク社会研究所）

杉井 鏡生（ハイパーネットワーク社会研究所）

・コメンテータ

立石 聡明（社団法人日本インターネットプロバイダー協会（JAIPA））

藤野 幸嗣（ハイパーネットワーク社会研究所）

○チェックイン＋棚湯タイム　18：00～19：00

○交流会（夕食）19：00～21：00

○夜なべ自由討論　21：00～23：00

『モラル＆セキュリティ～韓日比較』

【発表】

閔 庚植（ミン キョンシック）（韓国情報保護振興院（KISA））

【コーディネータ】

立石 聡明（社団法人日本インターネットプロバイダー協会（JAIPA））

◆2月20日（金）

○セッション3　9：30～11：30

『信頼のネット社会実現のために～地域からアクションプランを考える』

【発表】

佐藤 晃洋（大分県教育庁生徒指導推進室）

尾花 紀子（ネット教育アナリスト）

高橋 大洋（ネットスター株式会社）

【討論】

・コーディネータ

会津 泉（ハイパーネットワーク社会研究所）

渡辺 律子（ハイパーネットワーク社会研究所）

○まとめ　11：30～12：00

会津 泉（ハイパーネットワーク社会研究所副所長）

○閉会挨拶

宇津宮 孝一（ハイパーネットワーク社会研究所所長）

■－中小企業庁委託事業「企業向け人権啓発活動支援事業（情報モラル啓発事業）」－
平成２０年度情報モラル啓発セミナー(兵庫・三重・北海道・山形・宮崎)実施報告

本事業では、企業の経営者や企業人が情報モラルの重要性を認識し、企業が積極的に社会的責任を果たすためになすべきこと、行動すべきことを普及・啓発した。

【兵庫会場 実施概要】

Ⅰ．内容

テーマ：企業に求められる情報モラルと人権への配慮
－個人情報保護･情報セキュリティ対策の効果的な進め方－

日 時：平成20年6月18日（水） 13時10分～17時00分

場 所：神戸商工会議所会館（神商ホール） 神戸市中央区港島中町 6-1

対 象：中小企業の経営者・管理者、実務担当者、企業でインターネットを活用する人等

定 員：事前申込み229名、当日参加者202名

主 催：中小企業庁、近畿経済産業局、(財)ハイパーネットワーク社会研究所

後 援：兵庫県、神戸市、(社)関西経済連合会、(財)ひょうご産業活性化センター、
(財)兵庫県人権啓発協会、兵庫県商工会議所連合会、兵庫県商工会連合会、
兵庫県中小企業団体中央会、兵庫県中小企業家同友会、(独)情報処理推進機構、
(社)日本青年会議所、(特非)日本ネットワークセキュリティ協会、
(社)日本情報処理開発協会、（特非）IT コーディネータ協会

Ⅱ．プログラム

◆主催者挨拶 13：10～

◆ビデオプレゼンテーション 13：20～13：55
「実践・情報モラル～あなたの会社は大丈夫？～人権に配慮した個人情報保護の取り扱い」
講 師：財団法人ハイパーネットワーク社会研究所 杉井鏡生・渡辺律子

◆講演１ 13：55～14：55
「インターネット社会と人権」
講 師：株式会社インターネットプライバシー研究所 代表取締役 髙木 寛 氏

◆講演２ 15：10～16：10
「情報漏洩を防ぐ情報セキュリティ対策のあり方」
講 師：株式会社アークン 代表取締役 渡部 章 氏

◆パネル討論 16：15:～17：00
「いまなぜ情報モラルなのか」
講 師：高木寛、渡部章、杉井鏡生 モデレータ：青木栄二

【三重会場 実施概要】

Ⅰ．内容

テーマ：企業に求められる情報モラルと人権への配慮
－個人情報保護･情報セキュリティ対策の効果的な進め方－

日 時：平成20年7月17日（木） 13時10分～17時00分
場 所：三重県総合文化センター（小ホール）
対 象：中小企業の経営者・管理者、実務担当者、企業でインターネットを活用する人等
定 員：事前申込み151名、当日参加者121名
主 催：中小企業庁、中部経済産業局、(財)ハイパーネットワーク社会研究所
後 援：三重県、津市、(社)中部経済連合会、(財)三重県産業支援センター、
三重県商工会議所連合会、三重県商工会連合会、三重県中小企業団体中央会、
(社)三重県法人会連合会、三重県中小企業家同友会、
(社)三重県情報通信基盤整備協会、(独)情報処理推進機構、(社)日本青年会議所、
(特非)日本ネットワークセキュリティ協会、(社)日本情報処理開発協会、
(特非) ITコーディネータ協会

Ⅱ．プログラム

◆主催者挨拶 13：10～
◆ビデオプレゼンテーション 13：20～13：55
「実践・情報モラル～あなたの会社は大丈夫？～人権に配慮した個人情報保護の取り扱い」
講 師：財団法人ハイパーネットワーク社会研究所 杉井鏡生・渡辺律子
◆講演１ 13：55～14：55
「インターネット社会と人権」
講 師：関西大学 社会学部 教授 松井 修視氏
◆講演２ 15：10～16：10
「『わかる』から『できる』へ一個人情報保護の取組による企業価値の創出」
講 師：株式会社ジャパネットたかた 常務執行役員CPO 吉田 周一氏
◆パネル討論 16：15:～17：00
「いまなぜ情報モラルなのか」
講 師：松井修視、吉田周一、杉井鏡生 モデレータ：会津泉

【北海道会場 実施概要】

Ⅰ．内容

テーマ：企業に求められる情報モラルと人権への配慮
－個人情報保護･情報アクセシビリティ対策の効果的な進め方－
日 時：平成20年9月26日（金） 13時00分～17時00分
場 所：北海道経済センター（Aホール）
対 象：中小企業の経営者・管理者、実務担当者、企業でインターネットを活用する人等
定 員：事前申込み240名、当日参加者167名
主 催：中小企業庁、北海道経済産業局、(財)ハイパーネットワーク社会研究所
後 援：北海道、札幌市、北海道経済連合会、(財)北海道中小企業総合支援センター、
(財) さっぽろ産業振興財団、 (財) 北海道商工会議所連合会、札幌商工会議所
北海道商工会連合会、北海道中小企業団体中央会、北海道経営者協会、
(社) 北海道法人会連合会、北海道情報システム産業協会、

北海道中小企業家同友会、（社）北海道IT 推進協会、（独）情報処理推進機構、
（社）日本青年会議所、（特非）日本ネットワークセキュリティ協会、
（社）日本情報処理開発協会、(特非)ITコーディネータ協会

Ⅱ．プログラム

◆主催者挨拶 13：00～

◆ビデオプレゼンテーション 13：10～13：50

「実践・情報モラル～あなたの会社は大丈夫？～人権に配慮した個人情報保護の取り扱い」

講 師：財団法人ハイパーネットワーク社会研究所 杉井鏡生・渡辺律子

◆講演１ 13：50～14：50

「『わかる』から『できる』へ－個人情報保護の取組による企業価値の創出」

講 師：株式会社ジャパネットたかた 常務執行役員CPO 吉田 周一氏

◆講演２ 15：05～16：05

「IT 利活用における多様性への配慮－企業に求められる情報アクセシビリティとは」

講 師：株式会社ユーディット 代表取締役 関根 千佳氏

◆パネル討論 16：10～17：00

「いまなぜ情報モラルなのか」

講 師：吉田周一、関根千佳、杉井鏡生 モデレータ：会津泉

【山形会場 実施概要】

Ⅰ．内容

テーマ：企業に求められる情報モラルと人権への配慮
－個人情報保護対策と社内教育の効果的な進め方－

日 時：平成20年10月23日（木） 13時00分～17時00分

場 所：庄内産業振興センター（マリカ市民ホール）

対 象：中小企業の経営者・管理者、実務担当者、企業でインターネットを活用する人等

定 員：事前申込み263名、当日参加者236名

主 催：中小企業庁、東北経済産業局、(財)ハイパーネットワーク社会研究所

協 力：山形県、鶴岡市

後 援：（社）東北経済連合会、荘内日報社（独）情報処理推進機構、
（社）日本青年会議所、（特非）日本ネットワークセキュリティ協会、
（社）日本情報処理開発協会、(特非)ITコーディネータ協会

Ⅱ．プログラム

◆主催者挨拶 13：00～

◆ビデオプレゼンテーション 13：10～13：50

「実践・情報モラル～あなたの会社は大丈夫？～人権に配慮した個人情報保護の取り扱い」

講 師：財団法人ハイパーネットワーク社会研究所 会津泉・渡辺律子

◆講演１ 13：50～14：50

「情報漏洩事件の実体験から語る個人情報保護の効果的な取り組み～人権に配慮した情報セキュリティをめざして～」

講 師：財団法人関西情報・産業活性化センター 情報化推進グループ 部長 木村修二氏

◆講演２ 15：05～16：05

「社内教育を徹底する効果的な進め方」

講 師：有限会社関西レディースコーポレーション 代表取締役 長尾裕子氏

◆パネル討論 16：10～17：00

「いまなぜ情報モラルなのか」

講 師：木村修二、長尾裕子、公文俊平 モデレータ：会津泉

【宮崎会場 実施概要】

Ⅰ．内容

テーマ：企業に求められる情報モラルと人権への配慮
－個人情報保護・情報アクセシビリティの効果的な進め方－

日 時：平成21年2月6日（金） 13時00分～17時00分

場 所：宮崎観光ホテル（碧耀の間）

対 象：中小企業の経営者・管理者、実務担当者、企業でインターネットを活用する人等

定 員：事前申込み211名、当日参加者158名

主 催：中小企業庁、九州経済産業局、(財)ハイパーネットワーク社会研究所

後 援：宮崎県、宮崎市、（社）九州経済連合会、（財）宮崎県産業支援財団、
(社）宮崎県商工会議所連合会、宮崎商工会議所、宮崎県商工会連合会、
宮崎県中小企業団体中央会、宮崎県経営者協会、（社）宮崎県情報産業協会、
(社）宮崎県工業会、（社）宮崎県法人会連合会、宮崎県中小企業家同友会、
宮崎地域インターネット協議会、（独）情報処理推進機構、（社）日本青年会議所、
(特非）日本ネットワークセキュリティ協会、（社）日本情報処理開発協会、
(特非)ITコーディネータ協会

Ⅱ．プログラム

◆主催者挨拶 13：00～

◆ビデオプレゼンテーション 13：10～13：50

「実践・情報モラル～あなたの会社は大丈夫？～人権に配慮した個人情報保護の取り扱い」

講 師：財団法人ハイパーネットワーク社会研究所 杉井鏡生・渡辺律子

◆講演１ 13：50～14：50

「インターネット社会と人権」

講 師：株式会社インターネットプライバシー研究所 代表取締役 高木寛氏

◆講演２ 15：05～16：05

「IT 利活用における多様性への配慮－企業に求められる情報アクセシビリティとは」

講 師：株式会社ユーディット 代表取締役 関根千佳氏

◆パネル討論 16：10～17：00

「いまなぜ情報モラルなのか」

講 師：高木寛、関根千佳、杉井鏡生 モデレータ：会津泉

■情報誌「ハイパーフラッシュ」

情報施策関係者や地域づくりリーダー等を対象に、ITの最新動向、行政・地域情報化の先進的な事例、さらには大分県の情報化に関する現状、今後の展開等をテーマに発行した。

vol.42　紙面内容

○衛星によるブロードバンドの試み
　財団法人ハイパーネットワーク社会研究所　副所長
　衛星ブロードバンド普及推進協議会　事務局長　　会津　泉
○メディア表現をまなぶムービーカードワークショップ
　メディアアーティスト・早稲田大学　非常勤講師　　宮原　美佳
　メディアアーティスト・名古屋学芸大学　非常勤講師　杉本　達應
○香川・岡山交流事業：コミュニケーションツールとしてのデジタルビデオ製作体験
　ｅーとぴあ・かがわ(情報通信交流館)　釜野　陽介
○長崎のローカル局から発信！「環境リテラシー」
　株式会社テレビ長崎　編成業務部　増田　朋和
○チームＵ：ケータイ市民記者による佐賀総体・情報発信
　チームＵ　副会長　平田　義信
○フィフティプラス大分：輝く“人生第２幕の舞台”の活動をウェブで応援
　「団塊世代情報サイト５０＋大分（フィフティプラス大分)」　代表　渡辺　隆司
○ブロードバンドゼロ地域の解消に向けて～実証実験を終えて～
　財団法人ハイパーネットワーク社会研究所　主任研究員　菊池　達哉
○男女共同参画社会の促進に向けた在宅就業支援ＩＴ講座
　財団法人ハイパーネットワーク社会研究所　研究員　倉掛　崇
○報告
　第５７回ハイパーフォーラム
　「市民・企業・行政の協働による地域情報化～情報社会におけるエンパワメントの可能性を照射する～」
○トピックス
　インターネットによる差別表現の流布事案の対応について（その２）
○お知らせ
　情報コミュニティセンター案内

vol.43　紙面内容

○連載　海外の情報化動向「サイバーセキュリティ安全保障の重要な一部に」
　財団法人ハイパーネットワーク社会研究所　副所長　会津　泉
○地域ＳＮＳを活用した地域での世代間交流の活発化
　～西千葉あみっぴぃ(ＳＮＳ)の事例～
　特定非営利活動法人ＴＲＹＷＡＲＰ　代表理事　虎岩　雅明

○別府八湯町づくりの必需品：別府八湯メーリングリスト

別府八湯メーリングリスト世話人　菅　健一

○ITを利用した、地産地活の実現

デジタルバンク株式会社　常務取締役　木本　行圀

○トピックス

世界人権宣言６０周年

「すべての人と国が達成すべき権利と自由の基準・・・世界人権宣言の現代的意義」報告

○報告

第５８回ハイパーフォーラム

「グリーンＩＴを考える～企業と個人に求められる『環境への貢献』～」

○お知らせ

「ハイパーネットワーク 2009 ワークショップ in 別府」のご案内

vol. 44　紙面内容

○ハイパーネットワーク 2009 ワークショップ報告

「今、問われる情報モラルとガバナンス　－地域で取り組む『情報公害（ネットいじめ、人権侵害、犯罪誘発・・・)』

財団法人ハイパーネットワーク社会研究所　研究企画部長　渡辺　律子

○ストリートビューとプライバシーからLIFElogの問題まで

－今、ネットの世界で何が起きているか

ＩＴジャーナリスト　佐々木　俊尚

○第三者機関ＥＭＡの取り組みと法規制の動向

一般社団法人モバイルコンテンツ審査・運用監視機構　事務局　吉岡　良平

○連載　海外の情報化動向「モルドバにとってのネット社会　小国の生存とセキュリティ」財団法人ハイパーネットワーク社会研究所　副所長　会津　泉

○トピックス

「大分県人権尊重社会づくり推進条例」を制定しました

○報告

第５９回ハイパーフォーラム

「九州広域ＩＣＴプラットフォームシンポジウム in 大分　～危機管理情報の広域共有化に向けた取り組み～」

■普及啓発セミナー「ハイパーフォーラム」

情報施策関係者や地域づくりリーダー等を対象に、ITの最新動向、行政・地域情報化の先進的な事例、さらには大分県の情報化に関する現状、今後の展開等をテーマに開催した。

第５７回ハイパーフォーラム

主　催：大分県、財団法人ハイパーネットワーク社会研究所

テーマ：市民・企業・行政の協働による地域情報化
～情報社会におけるエンパワーメントの可能性を照射する～

概　要：大分では2003年度から、マイクロソフト社の社会貢献事業である、UP（Unlimited Potential）プログラムを、大分県の後援のもと、財団法人ハイパーネットワーク社会研究所が地域のコーディネーターとして、県内のさまざまな団体（NPO）と協働で実施してきた。UPプログラムとは、誰もが ICT（Information and Communication Technology：情報コミュニケーション技術）の恩恵を享受できる社会［デジタルインクルージョン］の実現に向けて、高齢者、障害者、子育て主婦など、これまでICTを活用する機会が少なかった方々に対し、研修を通じて、自己の可能性を広げ、力を発揮できるように支援する取り組みである。このUPプログラムも今年の6月で終了し、さらなる飛躍が期待されるところであるが、本フォーラムでは、大分UP関係者のみならず、同様な理念をもって活動されている県内外の方々も交え、とくに、福祉とICTを架橋する実践として、障害者のICT利活用による社会参加／就労に照準を合わせ、CSO（Civil Society Organization：市民社会組織）・企業・行政の協働によって達成されるべき福祉／情報社会の未来を展望し、誰もが包摂される（Social Inclusion）、共生社会はいかにして可能かを、会場の皆さまと一緒に考えた。

日　時：2008年8月5日（火）13:00～17:00

場　所：ソフィアホール　（大分市東春日町51-6 大分第2ソフィアプラザビル2階）

定　員：100名（事前申込み：99名、実参加者：107名）

［プログラム］

◆開会挨拶 13:00～13:10
　山戸　康弘　（大分県 企画振興部IT 推進課 課長）

◆講演1 13:10～13:40
「マイクロソフトが果たす社会貢献活動とは？」
　竹原　正篤　（マイクロソフト株式会社 社会貢献部 部長）

◆講演2 13:40～14:20
「佐賀県における協働化テストと「チャレンジドだれでもパソコン事業」」
　川島　宏一　（佐賀県 最高情報統括監 CIO）

◆ワークショップ 14:40～16:50

「誰もがICT の恩恵を享受できる社会の未来を考える」

討議者：松木　康司　(NPO法人障害者UP 大分プロジェクト 理事、全盲)

末廣　賢介　(NPO法人障害者UP 大分プロジェクト バーチャル工房事業担当)

西山　英樹　(社会福祉法人太陽の家 職業訓練課長)

山田　栄子　(NPO法人e-AT 利用促進協会 副理事長)

柴田　邦臣　(大妻女子大学社会情報学部 専任講師)

川島　宏一　(佐賀県 最高情報統括監 CIO)

永松　　悟　(大分県 福祉保健部障害福祉課 課長)

ファシリテーター：山戸　康弘　(大分県 企画振興部IT 推進課 課長)

倉掛　　崇　(財団法人ハイパーネットワーク社会研究所 研究員)

◆閉会挨拶 16:50～17:00

宇津宮　孝一　(財団法人 ハイパーネットワーク社会研究所 所長)

第５８回ハイパーフォーラム

主　催：大分県、財団法人ハイパーネットワーク社会研究所

テーマ:グリーンIT を考える

～企業と個人に求められる「環境への貢献」～

概　要：「グリーンIT」とは、IT技術における環境への取り組みのことで、世界的に大きな注目を集めています。2008年は「環境元年」そして「グリーンIT元年」とも呼ばれ、北海道洞爺湖サミットでも「グリーンIT」が話題になりました。2050年までに温暖化ガスを半減する長期目標は、困難な課題である反面、大きなビジネスチャンスを生むとも言われる。また、グリーンITという環境への貢献･配慮といった取り組みは、IT業界だけの問題ではなく、あらゆる企業や組織において、社会的責任の一つとして求められている。

今回のハイパーフォーラムでは、環境とITの関係について長年研究し、第一人者として知られる東京大学大学院工学系研究科の松野泰也准教授を基調講演にお迎えし、「ITのグリーン化(Green of IT)」および「ITによるグリーン化(Green by IT)」の2 つの視点について、お話ししていただいた。

また、日本AMD株式会社と日本電気株式会社から講師をお迎えし、実際に企業がグリーンITにどのように取り組んでいるのかについて、最新動向と最新技術事例をご講演いただいた。

日　時：2008年12月19日(金)13:00～16:35

場　所：ソフィアホール (大分市東春日町51-6 大分第2ソフィアプラザビル2階)

定　員：100名(事前申込み：88名、実参加者：61名)

[プログラム]

◆開会挨拶 13:00～13:05

宇津宮　孝一 (財団法人ハイパーネットワーク社会研究所 所長)

◆基調講演 13:05～14:25

「地球温暖化問題とグリーンIT ～ 取り組むための2 つの視点」

松野　泰也 氏(東京大学大学院工学系研究科マテリアル工学専攻 准教授)

◆質疑応答 14:25～14:30

◆講演1 14:40～15:25

「グリーンIT の最新動向と最新技術事例」

多田　和之 氏(日本AMD株式会社執行役員マーケティング ＆ ビジネス開発本部本部長 兼グリーンIT 推進室室長)

◆質疑応答 15:25～15:30

◆講演2 15:30～16:15

「グリーンITへの「途」」

野曽原　誉枝 氏 (日本電気株式会社 ITプラットフォーム販売推進本部REAL IT COOL 推進センター マネージャー)

◆質疑応答 16:15～16:30

◆閉会挨拶 16:30～16:35

青木　栄二 (財団法人ハイパーネットワーク社会研究所 事務局長)

第５９回ハイパーフォーラム

主　催：大分県、財団法人ハイパーネットワーク社会研究所

併　催：総務省九州総合通信局、九州広域ICTプラットフォーム調査検討会、次世代高度ネットワーク九州地区推進協議会

テーマ：九州広域ICTプラットフォームシンポジウムin大分
～危機管理情報の広域共有化に向けた取り組み～

概　要：「九州広域ＩＣＴプラットフォーム」の実現に向け、九州広域ＩＣＴプラットフォーム調査検討会において実施した実証実験のデモンストレーション等を交えながら、危機管理情報の共有化のための最新の技術動向や、広域ＩＣＴプラットフォームの実現に向けた制度的、技術的諸課題とその解決策について、危機管理情報の専門家及び有識者、九州のＩＣＴ関係者から広く意見をいただいた。

日　時：2009年2月24日(火)13:30～17:00

場　所：大分県消費生活・男女共同参画プラザ「アイネス」大会議室

定　員：100名(事前申込み：73名、実参加者：79名)

[プログラム]

◆開会挨拶 13:30～13:35

武井　俊幸 (総務省九州総合通信局長)

◆来賓挨拶 13:35～13:40

平野　昭 (大分県副知事)

◆基調講演 13:40～14:40

「危機管理対応情報共有技術による減災対策」

鈴木 猛康（山梨大学大学院教授）

◆プレゼンテーション 14:40～15:20

「危機管理情報の広域共有化に向けた実証実験の取り組み」

コーディネーター

西野　浩明（大分大学工学部准教授）

プレゼンテーター

小林　信喜（九州総合通信局情報通信連携推進課 課長）

長友　信裕（宮崎地域インターネット協議会 副会長）

広岡　淳二（九州情報通信連携推進協議会 事務局長）

◆パネルディスカッション 15:30～16:50

「九州広域ＩＣＴプラットフォームによる安心・安全な地域社会の形成に向けて」

コーディネーター

尾家 祐二（九州工業大学大学院教授）

パネリスト

池ノ上　克（宮崎大学医学部長・産婦人科教授）【遠隔出演】

堀井洋一郎（宮崎大学農学部獣医学科教授）

宮川　明大（石川県七尾市企画政策部情報政策課）【遠隔出演】

山崎　正幸（九州経済連合会情報通信委員会企画部会長）

山戸　康弘（大分県企画振興部IT 推進課 課長）

◆閉会挨拶 16:50～17:00

尾家　祐二（九州工業大学大学院教授）

■ハイパーネットワーク社会研究会

研究所の活動内容について、研究員、共同研究員及び賛助会員などがお互いの情報を共有する場として、「ハイパーネットワーク社会研究会」を開催した。

第３２回ハイパーネットワーク社会研究会

開催日時：平成20年8月8日（金） 16:00～17:15
開催テーマ：「おおいた街中モバイル調査」について
参加者：ハイパーネットワーク社会研究所 賛助会員、共同研究員、研究員、大学生（計１７名）
主催：財団法人ハイパーネットワーク社会研究所
講師：財団法人ハイパーネットワーク社会研究所共同研究員 藤野 幸嗣
会場：第２ソフィアプラザビル ソフィアホール会議室B

＜概 要＞

大分市の「中心市街地活性化事業」の一環で、普及しつつある情報端末（含、携帯電話・スマートフォン）を使って、生活者に大分市中心市街地域の商業情報や生活情報を提供して、活用を行うための事業の実現可能性に関する調査である。 携帯電話ではパケホーダイが始まり、各種の高機能なスマートフォンも発売されている。こうした端末を活用している生活者を対象に、地域のさまざまな情報を提供して、中心市街地の活性化に役立てようというものである。 携帯電話の技術動向や、各地のサービス動向から、大分市においてどのようなサービスが可能か本年度内にオープンなスタンスから検討を行う予定である。

＜内 容＞

まず、大分市中心市街地活性化基本計画の概要と大分市中心地区が抱えている問題点について話題に触れ、大分駅の高架化に伴う再開発が進んでいる状況と高齢化に伴い空き店舗が多くなっている現状を述べた。そこで、藤野氏は情報端末でのネットの活用を中心とした職、住、交流の場として中心市街地の活性化を図れないかと提案した。これは、10 年前から携帯を主とした情報端末の普及や利用が増えてきていることと、また低価格化も推し進められると予想されることからである。また、情報端末もさまざまな用途に応じた製品が販売され、どこでもインターネットという世界が近付いていると述べた。しかし、モバイル端末を利用した過去の同様な事例を紹介したが、Google などを含めて大成功したという事例は過去にはない。だが、地域密着型だとうまくいくかもしれないと藤野氏は推測している。今後の日程としては、技術調査や中間報告を経て実証実験の準備をする予定である。実証実験で実現の可能性が見えた場合、早くて2010 年には事業化したいと考えている。

第３３回ハイパーネットワーク社会研究会

開催日時：平成20年10月3日（金） 15:00～17:30
開催テーマ：第5 回セキュリティUP 会議

参加者：賛助会員、セキュリティ関係者、OISA 会員、研究員（計２１名）
主催：財団法人ハイパーネットワーク社会研究所
講師：NPO シニアネット大分 矢野豪志氏、関西レディースコーポレーション 長尾 裕子氏
　　財団法人ハイパーネットワーク社会研究所　菊池達哉
会場：第２ソフィアプラザビル ソフィアホール会議室B

＜概 要＞

今回の会議は二部構成で、第一部では、3 年間活動したセキュリティUP についての報告である。セキュリティUP 活動は2003 年度からマイクロソフト社の社会貢献事業であるUP(Unlimited Potential)プログラムを元に、2005 年度から地域の情報セキュリティの向上や普及啓発活動を行ってきた。このUP プログラムも今年の6 月で終了したことで、セキュリティUP 活動も節目をむかえることになった。この会議では3 年間の活動内容を報告し、関係者の感想や参加者の意見を聞きながら、今後のセキュリティ活動につながる会議にしたい。

第二部では、ハイパーネットワーク社会研究会と共催で、勉強会を開催する。今回の勉強では、社内教育に焦点を当てます。社内教育において、情報モラル・情報セキュリティ教育の進め方が分からない、効果が上がらないという声が少なくない。そこで、有限会社関西レディースコーポレーションの長尾氏をお招きし、「社内教育を徹底する効果的な進め方」と題して、社内教育が陥りやすい問題点を克服し、効果的に社内教育を進めるための方法について講演をして頂く。この講演は個人や組織でセキュリティ対策を進める方々にとって参考になる内容である。

＜内 容＞

第一部では、主任研究員の菊池が、セキュリティUP活動の成り立ちや活動内容、セキュリティUP活動も一つの区切りをむかえたことを報告した。その後、県警の方やスーパーマスターなど関係者の方に、セキュリティUP 活動の感想を述べて頂いた。また、NPO シニアネット大分 矢野豪志氏にスーパーマスターの代表者として、活動を振り返ってもらった。その際、「この活動が当初目標としていたことが達成できなかった」など悔いが残る結果となったことが残念という感想を頂いた。それを受けて、菊池が今後のセキュリティUP 活動は、地域住民の普通の会話にセキュリティの話が出てくるぐらいの普及活動が必要であると述べ、今後も活動を続けたいと締めくくった。

第二部では、関西レディースコーポレーション の長尾 裕子氏に「社内教育を徹底する効果的な進め方」の題目で講演して頂いた。講演では、人間としての基本的生活態度、「あいさつ」、「返事」が大事であること、また、組織としてどのように取り組みをすればよいのかなど、事例を踏まえて講演して頂いた。事例に基づいた内容のため、納得できる部分が多く、社内教育をはじめる際の良い材料となりうる内容であった。

第３４回ハイパーネットワーク社会研究会

開催日時：平成20年10月15日（水） 15:00～17:00
開催テーマ：「web2.0 から3Di（インターネット）の利用でエコ＆地域を活性化」
参加者：賛助会員、研究員（計１２名）

主催：財団法人ハイパーネットワーク社会研究所
講師：レゾナント・ソリューションズ株式会社 代表取締役CIO 首藤完治氏
会場：大分ＮＰＯプラザ 交流サロン

＜概 要＞

今回の研究会は、『エコと地域活性化』に焦点を当て、「web2.0 から3Di（インターネット）の利用でエコ＆地域を活性化」と題して行われました。企業活動におけるエコ（地球環境保護）活動の必要性、ネットショップ（ｗｅｂサイト）と連動させた販売・商品説明・イベント開催を行うことによる地域の活性化の取り組みについて、レゾナント・ソリューションズ株式会社の首藤 完治 氏をお招きし、講演していただきました。

＜内 容＞

海外での3Di３次元のインターネット利用において部分的な使い方が増えてきている現状および、エコ・ビジネススタイルで仮想空間を上手に活用できていれば距離・時間や人材・教育のデメリットをメリットに変える可能性についてのお話がありました。また3Di は地方での導入が難しい面もあるが、可能な部分は取り入れていかなければいけないとのご意見をいただきました。

意見交換・質疑応答では賛助会員の方からも「情報処理社会の中で環境を考えていく中で、我が社も仮想世界の利用を考えていかなければ」、「仮想空間を利用する場合に携帯との連携は今後どうなるのか」などといった活発な意見が出ました。

第３５回ハイパーネットワーク社会研究会

開催日時：平成20年12月2日（火） 14:30～17:00
開催テーマ：「公共ネットワークの目指すべき未来像」
参加者：30名（賛助会員様：13名、オブザーバ：10名、研究員：6名）
主催：財団法人ハイパーネットワーク社会研究所
講演者：アライドテレシス株式会社 ビジネスエンジニアリング事業部
事業部長 小田直之 氏
アラクサラネットワーク株式会社 営業本部マーケティング部
エキスパート 倉本雅之 氏
シスコシステムズ合同会社 ｴﾝﾀｰﾌﾟﾗｲｽﾞｼｽﾃﾑｴﾝｼﾞﾆｱﾘﾝｸﾞ
シニアマネージャ 原田新作 氏
会場：大分第2ソフィアビル2F「ソフィアホールB会議室」

＜概 要＞

ネットワーク機器メーカ3 社により、テーマに関連した事例や取組み、ソリューション等を紹介していただいた。具体的には、公共ネットワークにおける運用負担軽減、ネットワーク活用、グリーンIT、等について講演いただいた。その後、出席者の方々と意見交換を行った。

＜内 容＞

【講演-1】アライドテレシス株式会社

「アライドテレシスの公共ネットワークへの取り組み」

小田 氏より、アライドテレシス社の紹介にはじまり、製品ラインナップ、アメリカや国内の公共ネットワークの事例、スイッチ製品の省電力化の取り組みなどを講演いただいた。日本品質かつ低価格が同社の強みとのこと。省電力化の取組みについては、具体的なデータや内部構成部品について説明いただいた。

【講演-2】アラクサラネットワーク株式会社

「アラクサラの考える自治体情報ネットワークの未来像」

倉本 氏より、同社の自治体ネットワーク向けソリューションの概要を説明いただいた。続いて、「ネットワークパーティション」による設備投資の最適化、「FT（フォールト・トレラント）ネットワーク」などを分かりやすく講演いただいた。近いうち製品化される「ダイナミック省電力」機能は、オンライン電力削減、スケジュールに沿って消費電力調整により、更に省電力化を進めるとのこと。

【講演-3】シスコシステムズ合同会社

「公共ネットワークの目指すべき未来像 ～コネクテッド・コミュニティ～」

原田 氏より、同社のビジョン「人々の仕事・生活・遊び・教育の方法を変える」に基づき、「コネクテッド・コミュニティ」について提案があった。具体的には、リソースやサービスの「統合化」「仮想化」「自動化」、VRF 技術による自治体ネットワーク最後に、グローバルなテレプレゼンス（TV 会議）活用によるCO2 削減の提案、市町村合併に伴う固定系防災無線の事例紹介があった。

【質疑応答・意見交換】

大分県IT 推進課 清水 氏と椎原 氏より、大分県下の公共ネットワークの実情と、「豊の国ハイパーネット」の今後の計画について説明された。また、保守コスト低減のため、日本HP 社の「ライフタイム保証」を例に挙げ、講演いただいたメーカ3 社との意見交換が行われた。共通した課題として、保証サービスの継続性、後継機種との設定情報の互換性などが挙げられた。

第３６回ハイパーネットワーク社会研究会

開催日時：平成21年3月19日（木）13：00～15：00

開催テーマ：「地域情報セキュリティセンター（仮称）」の設立について

参加者：１４名（企業、大学、NPO、研究員）

主催：ハイパーネットワーク社会研究所

講師：マカフィー（木下所長代理、西村SE）

会場：ハイパーネットワーク社会研究所会議室

＜内 容＞

これまでハイパー研においては、2003 年度から情報モラルや情報セキュリティに関する調査研究、普及啓発活動を実施してきた。

しかしながら情報社会における問題は、増加するばかりでなかなか対策がおいつかず、県警や

消費生活センターへの問い合わせ件数も増加してきている。そうした状況を踏まえて、ハイパー研においては、「地域情報セキュリティセンター」の設立を検討してきた経緯がある。今回の研究会にでは、その有効性や有益性を高めるために、討論のための研究会を開催した。

はじめに、これまでの分野ごとの取り組みを報告した。NPO や県警、自治体、また学校やPTA との協働の実績について、さらには総務省や経産省、IPA やJNSA との関係について説明した。一方で部分的には他の地域の状況も把握しているが、具体的にどういう仕組みや技術を利用しているか、情報セキュリティの最新動向も併せて、マカフィー様を招いて講演会を行った。

大分県でのサービス状況と他の県との比較をしてもらった後に、現在のセキュリティ動向についての説明があった。いま、ウィルスは数秒に1 個発生して、パターンファイルに入れ切れなくなってきている。ウイルスチェックファイルだけでは守れなくなってきている。PC 権限の管理、パッチをあてる、ウィルス対策の重要性は大きい。またウィルスが復活の兆しがあり、USB での感染が増えてきている。インターネットから入って、横展開するというものだ。パケットを吐き出して、社内のネットワークを食いつぶしてしまう。これからのセキュリティはコンフリッカーから考える必要がある。セキュリティポリシーはあっても、それを強制するソリューションがなかったりする。

ウィルスの進化により、定義ファイルだけで守るのは、厳しい状況だ。亜種が大量に発生している。感染後、拡張子を隠したり、別のウィルスをダウンロードしたりというものだ。防御方法では、ポートを防ぐという方法もある。やはりポリシーを決めたらそれを強制する方法を考えなければいけない。ウィルス対策だけでなく、総合的なリスクマネジメントが必要になってきている。対策項目としては、ウィルス、パッチ、脆弱性マネジメント、ポリシー、デバイス制御、暗号化など。

討論として、地域セキュリティセンターについては、どういったことを考慮していくべきか。以下の内容について議論を行った。やはりさまざまな分野からの期待があるものと考えられた。

・情報モラルの考え方、パソコンを使う、ネットを使う人の心構え
・対18 市町村を対象にした普及啓発はもっと明確化する。誰に伝えるのか
・組織に属する人も対象とするのか、企業は対応しなくていいのでは？
　→企業へも市民へもサービスをすべき、市民が被害をうけないためにも
・これから習いたいという人達に向けての講習会、ぜひ、地域でやってほしい
・各市町村の受け皿をどこにするかが課題。商工会議所、商工会は大丈夫か？
・障害者の利用者、セキュリティ対策しているといってもしていない、ぜひフォローして欲しい
・とてもよい取り組みと思う。是非、進めてほしい。できれば市民向けに
・セキュリティだけでは参加しないかも。言葉だけ聞いても魅力がなく活用とセットでいければ・教育関係者への対応が重要。学校、先生は意識が低すぎる
・利用者に言っても限界があるので、ISP に責任を持たせてはどうか
・そういう意味で、OCT＋マカフィーの取り組みはすばらしい
・ウィルス対策については、MS が9 月から対応する予定
　→どこまで対応してくれるかどうかはわからない
・USB メモリのウイルス対策。どうしたらいいか
・セキュリティの本当の初心者がまだまだ多い。その層への普及啓発は継続して必要

・その上の層に、相談窓口があると有効
・相談窓口では、どういった内容を取り扱うのか？
　→誹謗中傷、ウィルス対策、架空請求などなど
　→ハイパー研が全体の窓口となり、あとは適宜ふさわしい窓口へつなぐ。クッション的存在
　今後、ハイパー研において来年度の取り組みとして、この研究会などの議論をもとに設立にあたって検討を進めていく予定である。4 月にはまた報告や相談の場が持てるものと考えている。これからも引き続きの協力をお願いして研究会を閉めた。

■研究所スタッフ活動履歴

☆会津泉（副所長）

【委員会活動】

ICANN（Internet Corporation for Assigned Names and Numbers）

AtLarge Advisory Committee アジア太平洋地域代表委員。

以下の会合に参加。

6月　パリ会議

11月　カイロ会議

2009年

3月　メキシコシティ会議

総務省

インターネット政策懇談会、通信プラットフォーム研究会、ICTビジョン懇談会基本戦略WG、IPv6によるインターネット高度利用化に関する研究会　各構成員

情報通信審議会インターネット基盤委員会　専門委員

経済産業省

インターネット上のサービスに関するイノベーション・競争環境の整備と利用者利益の確保について研究会　構成員

情報通信政策会議（ICPC）　アドバイザリー委員

5月　衛星ブロードバンド普及推進協議会設立、事務局長に就任。

9月－12月　衛星ブロードバンド実証実験実施（都留市、綾部市、庄原市、広島市）

【その他の会合・講演など】

4－6月　慶應義塾大学大学院メディアデザイン研究科非常勤講師

4月　総務省／ITU共催　気候温暖化とIT国際会議（京都）参加

7月　JAIPA沖縄ファーラム参加

情報モラルセミナー（三重）パネル司会ほか

iCommonsサミット（札幌）参加

9月　情報モラルセミナー（札幌）パネル司会ほか

10月　日経情報通信サミット　ネット中立性シンポジウム司会

情報モラルセミナー（鶴岡）パネル司会ほか

情報通信学会国際フォーラム　パネル司会ほか

11月　ICT未来フェスタ（徳島）講演

情報モラルセミナー（高松）パネル司会

情報セキュリティ調査（ベルギー、フィンランド、エストニア、リトアニア、ラトビア、モルドバ）

12月　衛星ブロードバンド普及シンポジウム（広島）

インターネットガバナンスフォーラム（ハイデラバード）

米国情報セキュリティ調査（ワシントンDC）

2009年

2月　情報モラルセミナー（宮崎）パネル司会ほか

ハイパーワークショップ（大分）

【執筆原稿】

「世界情報社会サミット（WSIS）とインターネットガバナンス」

『学びとコンピュータ ハンドブック』（東京電機大学出版局）所収

「シンガポールのインターネット　小国の生き残り作戦として」改定執筆

『シンガポールを知るための62章』（明石書房）所収

「多様化するインターネット、グローバルガバナンスへの挑戦　ＩＧＦ2008報告」

（日経デジタルコア「ネット時評」掲載

http://www.nikkeidigitalcore.jp/archives/2009/01/20081.html）

【主な研究調査プロジェクト】

衛星ブロードバンド基盤整備に係る標準化モデル構築業務（総務省委託）

情報セキュリティのガバナンスに関する調査研究（ＮＴＴ委託）

☆青木栄二（事務局長）

【委員】

2008.7.24　九州広域ICTプラットフォーム第1回調査検討会

2009.2.26　宇佐市情報化委員会

【講演】

2008.7.24　大分商工会議所平成20年度第1回IT化推進委員会（講話「迷惑メールの現状対策」）

2008.6.18　情報モラルセミナーin兵庫（パネルコーディネータ）

2008.8.28　第229回熊本知能システム技術研究会（RIST）フォーラム（パネリスト「KIAI」が目指すもの）

2008.9.30　九州テレコム振興センター運営委員会（発表「公益法人改革の現状」）

2008.10.9　九州・国際テクノフェアICTコンバージェンス2008＜ICTセミナー＞（パネリスト「地域情報化の取り組み」）

2008.10.30　日韓共同セミナー2008in京都ETRI-KCG（発表「ユビキタス社会における情報セキュリティ」）

2008.11.26　2008韓・日地域情報化セミナー（発表「地域情報化と情報資源管理」）

2009.2.28　インターネット安全教室in佐世保（司会）

☆渡辺律子（研究企画部長）

【委員】

・平成20年度のびゆく大分っ子育成サポート事業　ワーキング会議メンバー（大分県青少年育成県民会議）

・大分大学情報教育イノベータ実施プログラム委員（文部科学省委託、大分大学ＧＰ）

【学会発表】

2008.9.24　電気関係学会九州支部連合大会　大分大学（菊池研究員と発表）

2009.3.6　電子情報通信学会（熊本県）　「インターネットと倫理」にて発表
招待講演「企業に問われる情報モラル」

【講演】

○企業の情報モラル・情報セキュリティに関する講演（企業や自治体からの依頼）】

2008.6.7　愛媛県松山市、ITフェアにて　「企業に求められる情報モラル～人権に配慮した個人情報の保護～」　主催：IT推進協議会

2008.9.12　大分県佐伯市、「学校における情報モラル、情報セキュリティについての講演」（菊池研究員と対応）主催：佐伯教育事務所、　管内学校事務職員対象研修会

2008.10.10　長野県松本市「企業に求められる情報モラル～人権に配慮した個人情報の保護～」　主催：企業人権啓発推進連絡協議会

2009.2.28　長崎県佐世保市「インターネット安全教室」長崎県立大学シーボルト校（青木事務局長と対応）

○子どもたちのネット利用について－生徒、教員、保護者に向けた情報モラル講演

（1）生徒対象

「ネットを楽しく利用するための情報モラル」

「ネット社会で被害者・加害者にならないための情報モラル」

2008.5.2　大分県立津久見高等学校　全校生徒（459名）＋教職員、保護者、教育委員会

2008.7.14　大分市立碩田中学校　全校生徒対象＋教職員＋保護者（500名）

2008.10.17　大分舞鶴高等学校　全校生徒及び教職員（約1000名）

2008･10.29　豊後大野市立緒方中学校　全校生徒対象＋教職員＋保護者（200名）

2008.11.4　大分県立竹田高等学校　全校生徒＋教職員(581名)

2008.12.12　国東市立安岐中学校　全校生徒＋保護者＋教職員（450名）

2008.12.16　大分県立大分南高等学校　1・2学年生徒・教職員（550名）

2009.1.15　大分県立大分東高等学校　全校生徒・教職員（約500名）

2009.2.25　別府市立山の手中学校　全校生徒＋教職員＋保護者（約400名）

2009.3.12　由布市立湯布院中学校　1年生＋保護者（約130名）

（2）教職員対象「ネット社会と子どもたち　ー情報モラルと大人の役割ー」

2008.5.12　大分市生徒指導研究会総会（大分市金池会館)、大分市内小・中・高等専修学校校長、生徒指導担当教諭（130名）

2008.5.15　国東地区学校保健会「講演会」(国東地区学校保健会事務局)

2008.8.8　前期研修講座　情報モラル講座　別府市総合教育センター　約20名

2008.11.6　日田市生徒指導協議会（日田市教育委員会）　約20名

（3）保護者対象「ネット社会と子どもたち　ー情報モラルと大人の役割ー」

2008.4.18　大分市立稙田中学校　PTA役員及び会員（50名）

2008.6.21　中央地区PTA協議会指導者研修会　中央地区のPTA役員、教職員（約200名）

2008.6.27　国東地区学校保健会　国東地区養護教諭対象（約100名）

2008.8.9　大分地区高等学校PTA役員ならびに同地区学校関係者（約300名）

2008.9.5　6学年PTA研修「勉強会」（附属小学校ＰＴＡ）　約50名
2008.9.17　大分市立稙田東中学校　PTAならびに同地区学校関係者（約100名）
2008.10.30　中津市立耶馬溪中学校　PTAならびに教職員（約50名）
2008.11.12　南山田小学校　保護者・教職員（約40名）
2008.11.24　平成20年度高Ｐ連振興大会「子どもたちのインターネット利用について考える研究会九州大会」
2009.1.22　大分市立宗方小学校　PTA人権教育研修部　保護者（約30名）
2009.1.24　大分県立大分東高等学校　PTA研修会（約100名）

○その他の講演
2008.6.10　少年警察実務専科教養　（約30名）大分県警察本部生活安全部少年課
2009.1.27　平成20年度第2回青少年健全育成審議会（大分県青少年育成県民会議事務局

※上記講演は、学校からの個別の依頼、または大分県教育委員会生徒指導推進室、大分県私学振興・青少年課、および各学校のPTAや教職員等の依頼に対応する形で実施した。

【執筆原稿】
・大分市立稙田中学校ＰＴＡ広報誌　第117号～119号、情報モラルについてのコラム掲載

☆菊池達哉（主任研究員）

【学会発表】
2008.9.24　第61回連合大会にてハイパー研の取り組みについて発表

【講演】
2008.6.7　インターネット安全教室 in 松山
2008.6.28　シニア情報生活アドバイザ研修
2008.6.30　第4回 セキュリティUP会議
2008.7.23　教職員向けのセキュリティ講座(大分県立西高校)
2008.9.12　教職員向けのセキュリティ講座(佐伯教育委員会)
2008.10.3　第5回 セキュリティUP会議&ハイパーネットワーク社会研究会
2008.12.1　セキュリティ講座(パワーウェーブ日出)

【執筆原稿】
・ハイパーフラッシュNo42　ブロードバンドゼロ解消について執筆

■研究所スタッフ一覧（平成２１年３月現在）

所長	宇津宮孝一	大分大学工学部教授
副所長	会津　泉	
事務局長	青木　栄二	

研究企画部

部長	渡辺　律子	
主任研究員	菊池　達哉	
	中川　俊哉	
	菅　智広	
	工藤　賢	
	吉田　保博	
	下司　正和	
研究員	中川　譲	
アシスタント	植木　清美	

総務部

部長	森次　正浩	
主査	相原　幸	
アシスタント	得丸　好美	

共同研究員

赤星　哲也	日本文理大学工学部助教授
江原　裕幸	大分シーイーシー株式会社第一システム部 グループマネージャ
大杉　卓三	国立大学法人九州大学大学院比較社会文化学府・ 研究院助教
凍田　和美	大分県立芸術文化短期大学教授
杉井　鏡生	個人自営リサーチャー
永松　利文	国立大学法人鳥取大学大学教育総合センター 研究開発部准教授
西野　浩明	国立大学法人大分大学工学部准教授
藤野　幸嗣	梅林建設株式会社企画室次長
山崎重一郎	近畿大学産業理工学部教授
山戸　康弘	大分県企画振興部ＩＴ推進課長
吉田　和幸	国立大学法人大分大学学術情報拠点教授
Go Seon-Gyu	韓国中央選挙管理委員会選挙研修院教授
MIN Kyoung-Sik	韓国情報保護振興院チーム長

■役員一覧（平成２１年３月現在）

顧問	渡邊　文夫	東京海上日動火災保険株式会社名誉顧問
顧問	浜野　保樹	東京大学大学院新領域創成科学研究科教授
顧問	尾野　　徹	株式会社コアラ代表取締役社長
理事長	公文　俊平	多摩大学情報社会学研究所所長
専務理事	宇津宮孝一	大分大学工学部教授
理事	飯塚　久夫	ＮＥＣビッグローブ株式会社代表取締役執行役員社長
理事	井田　　敏	日本アビオニクス株式会社専務取締役
理事	大場善次郎	東京大学特任教授
理事	岡部　武尚	財団法人ニューメディア開発協会理事長
理事	津田　俊隆	株式会社富士通研究所常務取締役
理事	平野　　昭	大分県副知事
理事	藤原　　洋	株式会社インターネット総合研究所代表取締役所長
理事	山田　伸一	株式会社ＮＴＴデータ常務執行役員基盤システム事業本部長 兼技術開発本部長
監事	尾渡　秀成	大銀コンピュータサービス株式会社取締役総務本部長
監事	牧野　郡二	株式会社豊和銀行経営管理部長
評議員	荒木啓二郎	九州大学大学院システム情報科学研究院教授
評議員	石橋　幸一	ソフトバンクテレコム株式会社関西営業統括部 関西第２営業部部長
評議員	今井　賢一	スタンフォード日本センター理事
評議員	大橋　正和	中央大学総合政策学部教授
評議員	大輪　保夫	株式会社ＮＨＫエンタープライズ　ライツ・アーカイブス・ センター番組提供事業部シニア・エグゼクティブ・ プロデューサー
評議員	小田嶋　隆	クロスポイントコミュニケーションズ代表取締役
評議員	北矢　行男	多摩大学総合研究所所長
評議員	James Foster	マイクロソフト株式会社業務執行役員法務・政策企画統括本部 政策企画本部長
評議員	慈道　裕治	立命館大学政策科学部特命教授
評議員	長尾　利彦	アライドテレシス株式会社取締役副社長
評議員	堀川　　恵	安川情報システム株式会社経営企画室営業企画担当部長
評議員	松尾　　泰	株式会社エスシーシー代表取締役社長
評議員	村井　　純	慶應義塾大学環境情報学部教授
評議員	山崎　正幸	九州電力株式会社電子通信部長
評議員	渡部　国男	キヤノン株式会社常務取締役企画本部長
評議員	渡邉　俊治	新日鉄ソリューションズ株式会社技術本部ソフトウエア開発 センター所長

■賛助会員一覧（平成２１年３月現在）

アライドテレシス株式会社
アラクサラネットワークス株式会社
株式会社アルファシステムズ
梅林建設株式会社
株式会社オーイーシー
株式会社大分銀行
大分ケーブルテレコム株式会社
鬼塚電気工事株式会社
キヤノン株式会社
株式会社シーイーシー
シスコシステムズ合同会社
住友電気工業株式会社
ソフトバンクテレコム株式会社
株式会社ソリトンシステムズ
デジタルバンク株式会社
東京海上日動火災保険株式会社
日本ビジネスシステムズ株式会社
日本無線株式会社
ネットワンシステムズ株式会社
株式会社豊和銀行
マイクロソフト株式会社
マカフィー株式会社
ミカサ商事株式会社
株式会社リコー
（50 音順）

発 行

財団法人　ハイパーネットワーク社会研究所
〒870-0037　大分県大分市東春日町 51－6 大分第 2 ソフィアプラザビル 4F
TEL: 097-537-8180　FAX: 097-537-8820
E-MAIL: post@hyper.or.jp　URL: http://www.hyper.or.jp