14－H001

次世代情報通信環境における
ヒューマンインタフェース技術に関する
調査研究報告書

－安心・安全なユビキタス社会へ向けて－

平成15年3月

財団法人　日本情報処理開発協会

KEIRIN

この事業は、競輪の補助金を受けて実施したものです。

ま え が き

現在、高速通信網を基盤とする次世代インターネットによる情報ネットワークが構築され、その上で電子商取引などの社会・経済の様々な活動やコミュニティ活動が展開され、さらに拡大しようとしています。また、様々なセンサーやデバイスの研究開発に伴い、ウェアラブルコンピュータや認識システムが実用化されようとしています。これは、現在が「いつでも、どこでもネットワークにつながり、コンピューティングしうる」ユビキタス情報環境の上に成り立つ社会へ向かっていく入口にあることを示しています。そのような高度情報化社会にあっては、ヒューマンインタフェースの重要性がますます高まっていきます。

そこで、当協会では「次世代情報通信環境におけるヒューマンインタフェース技術に関する調査研究」を実施することとし、昨年度は電子商取引分野を取り上げ、そこで要請されるヒューマンインタフェース利用上の課題、関連技術の技術課題を明確にし、今後の研究開発の方向性・実現上の課題について検討いたしました。

本調査研究の2年目に当る平成14年度は、ユビキタス情報社会において安心・安全を実現する機能がプラットフォーム（情報通信基盤）や各種機器（携帯機器、自動車、情報家電、組み込み機器を含む）に備わっていなければ、生活・産業や電子政府・電子自治体など社会システム全般が脆弱となることに鑑み、ユビキタス情報社会における安心・安全を実現するセキュリティ確保やプライバシー保護に関する技術、および、新産業の創造に結びつく新しいシステムモデルについて検討しました。安心・安全を実現した将来においては、個人が使いやすいヒューマンインタフェースが実現するものと期待されます。

実施に当っては、「ヒューマンインタフェース技術調査委員会」（委員長 竹林洋一　静岡大学情報学部情報科学科教授）および「ユビキタス情報社会のシステムモデル分科会」（主査　竹林洋一 前掲）、「ユビキタス・セキュリティ分科会」（主査　加藤和彦 筑波大学電子・情報工学系助教授）を設置して、調査研究の基本方針、個別テーマの審議・検討を行うとともに、文献調査等を行いました。

本報告書は、平成14年度の調査研究成果を取りまとめたもので、2編から構成され、Ⅰ編は本編であり調査研究成果の概要及び詳細を、また、Ⅱ編は資料編でIPv6の動向、企業各社のユビキタス関連ビジネスの取組み、内外における関連研究開発プロジェクトの情報等を、まとめています。

本書が広く各界の方々に活用されることを念願する次第です。

最後に、本調査研究の実施にあたり、ご指導ご協力をいただいた委員各位ならびに関係各位に深甚なる謝意を表します。

平成15年3月

財団法人　日本情報処理開発協会

委員会および協力者名簿

（敬称略、50 音順）

「ヒューマンインタフェース技術調査委員会」

委員長　竹林　洋一　静岡大学情報学部情報科学科教授

幹　事　間瀬　健二　名古屋大学情報連携基盤センター情報基盤システムデザイン部門教授

〃　加藤　和彦　筑波大学電子・情報工学系助教授

委　員　合原英次郎　松下電器産業（株）東京支社渉外グループ IT・セキュリティチーム副参事

〃　石橋　泰博（株）東芝　ディジタルメディアネットワーク社コアテクノロジーセンター
ホームブロードバンドシステム開発部グループ長

〃　岡田　誠　（株）富士通研究所 IT コア研究所サービスマネジメント研究部主任研究員

〃　椎尾　一郎　玉川大学工学部電子工学科教授

〃　杉山　岳弘　静岡大学情報学部情報社会学科助教授

〃　高木　浩光　独立行政法人産業技術総合研究所グリッド研究センター
セキュアプログラミングチーム研究チーム長

〃　高橋　成文（株）NTT データ技術開発本部セキュアユビキタスグループグループリーダ

〃　福本　雅朗（株）NTT ドコモ　マルチメディア研究所メディア制御研究室主任研究員

〃　星澤　裕二　（株）シマンテック　Symantec Security Response マネージャ

〃　若井　裕久　シャープ（株）技術戦略企画室企画グループ副参事

「ユビキタス情報社会のシステムモデル分科会」

主　査　竹林　洋一　静岡大学情報学部情報科学科教授

副主査　間瀬　健二　名古屋大学情報連携基盤センター情報基盤システムデザイン部門 教授

委　員　椎尾　一郎　玉川大学工学部電子工学科教授

〃　　杉山　岳弘　静岡大学情報学部情報社会学科助教授

〃　　福本　雅朗（株）NTT ドコモ　マルチメディア研究所メディア制御研究室主任研究員

「ユビキタス・セキュリティ分科会」

主　査　加藤　和彦　筑波大学電子・情報工学系助教授

委　員　合原英次郎　松下電器産業（株）東京支社渉外グループ IT・セキュリティチーム副参事

〃　　岡田　誠　（株）富士通研究所 IT コア研究所サービスマネジメント研究部主任研究員

〃　　石橋　泰博（株）東芝　ディジタルメディアネットワーク社コアテクノロジーセンター
ホームブロードバンドシステム開発部グループ長

〃　　高木　浩光　独立行政法人産業技術総合研究所グリッド研究センター
セキュアプログラミングチーム研究チーム長

〃　　高橋　成文（株）NTT データ技術開発本部セキュアユビキタスグループグループリーダ

〃　　星澤　裕二（株）シマンテック　Symantec Security Response マネージャ

〃　　若井　裕久　シャープ（株）技術戦略企画室企画グループ副参事

協　力　者：

江崎　　浩　　東京大学大学院情報理工学系研究科助教授

岡田　仁志　国立情報学研究所人間・社会情報研究系情報制度論研究部門助教授

小田切博之　セイコーインスツルメンツ（株）e ソリューション・ビジネスユニット
WD 部 WD 技術推進グループ課長

菊池　浩明　東海大学電子情報学部情報メディア学科助教授

田中　　厚　（株）日立製作所システム開発研究所第 5 部部長

玉田　　樹　（株）野村総合研究所理事

オブザーバ：

和泉　　章　経済産業省商務情報政策局情報政策課課長補佐

牧　由美子　経済産業省商務情報政策局情報政策課技術３係

湯沢　広吉　経済産業省商務情報政策局情報通信機器課情報家電企画調整官

重松　孝明　電子商取引推進協議会主席研究員

荒川　一彦　電子商取引推進協議会主席研究員

事　務　局：

茂呂　知明　（財）日本情報処理開発協会技術企画部技術課専任調査役

金剛寺英雄　（財）日本情報処理開発協会技術企画部技術課課長

石本　恵　　（財）日本情報処理開発協会技術企画部次長

１４－Ｈ００１

平成１４年度

「次世代情報通信環境におけるヒューマンインタフェース技術に関する調査研究報告書」

目　次

Ⅰ．本編

1．調査研究の概要

（1）背景と目的

現在、インターネットなど高度な情報ネットワークが構築され、また、各種情報端末やセンサーが開発・提供されており、ユビキタス情報社会へ向って進展している。ユビキタス情報社会においては、人間と情報環境そのものとのインタフェースが特に重要になる。

このような状況に鑑み、ヒューマンインタフェースに要請される利用上の課題を把握し、その課題を解決するヒューマンインタフェース関連技術について、現状と動向を調査した上で技術課題を明確化し、さらに、今後の研究開発の方向性・実現上の課題を明らかにし、ヒューマンインタフェース技術の研究開発のための提言を取りまとめる目的で「次世代情報通信環境におけるヒューマンインタフェース技術に関する調査研究」を平成 13 年度及び 14 年度の 2 年間実施した。

（2）調査研究の実施

調査研究の実施にあたっては、「ヒューマンインタフェース技術委員会」を設置して調査研究を行うとともに、外部講師からヒアリングを行った。

平成 13 年度は、①ユビキタス情報環境の実現に貢献する現状のヒューマンインタフェース技術と動向、②ユーザの観点からのヒューマンインタフェースに関する利用上の課題と期待感、③今後のユビキタス情報環境実現のための主要な技術課題、④ユビキタス社会における望ましいヒューマンインタフェース等を考察するとともに、ユビキタス情報環境におけるヒューマンインタフェースを実現するための方策を取りまとめた。上記②のために、電子商取引（EC）の利用者を対象にアンケート調査を実施した。

平成 14 年度は、「ヒューマンインタフェース技術委員会」（委員長　竹林洋一静岡大学情報学部情報科学科教授）の下、ユビキタス情報社会における安心・安全なヒューマンインタフェースの実現という観点から、①ユビキタス情報社会で想定される光と影、②セキュリティ／プライバシー保全技術の現状、③セキュリティ／プライバシー保護に関する制度、④ユビキタス情報環境におけるセキュリティ／プライバシーの脅威等を考察するとともに、ユビキタス情報社会におけるセキュリティ／プライバシー保全技術・システムを開発するための提言を取りまとめた。また、本調査研究の成果発表のために「ユビキタス情報社会における安心・安全なヒューマンインタフェースに関するワークショップ」（平成 15 年 3 月 14 日）を開催した。

「ユビキタス情報社会における安心・安全なヒューマンインタフェースに関するワークショップ－ユビキタス情報社会におけるセキュリティ・プライバシー確保を目指して－」

開催日：平成 15 年 3 月 14 日

開催会場：機械振興会館（東京都港区）

プログラム：

招待講演「ユビキタスネットワークと市場創造」
玉田　樹（株）野村総合研究所理事

講演１：ユビキタス・コンピューティングの展望
間瀬健二　名古屋大学情報連携基盤センター教授
講演２：ユビキタス情報社会におけるセキュリティ・プライバシー
加藤和彦　筑波大学電子・情報系助教授
講演３：ユビキタス情報社会における安心・安全なヒューマンインタフェース実現へ向けて
竹林洋一　静岡大学情報学部情報科学科教授
パネルディスカッション
「ユビキタス情報社会の安心・安全をいかに確保するか？」
コーディネータ：竹林洋一（静岡大学）
パネリスト：玉田 樹（野村総合研究所）、間瀬健二（名古屋大学）、加藤和彦（筑波大学）、高木浩光（産業技術総合研究所）

（３）報告書の概要

調査研究の成果である本報告書の構成は、以下のとおりである。

Ⅰ．本編

１．調査研究の概要

２．ユビキタス情報環境におけるヒューマンインタフェースとは

ユビキタス情報環境におけるヒューマンインタフェースについて、「安心・安全・快適」の観点からその意義と重要性を説明。

３．ユビキタス情報社会の展望

ユビキタス情報社会では人々の暮らしは格段に便利になり、産業界にとっても新しい技術分野と市場が生まれ活性化される。その一方で、生活のあらゆる状況をコンピュータネットワークから把握できてしまう情報化社会には、さまざまな問題が浮上してくると考えられる。そこで、ユビキタス情報社会の光と影の側面を考察。

４．セキュリティ／プライバシー保全技術の現状

暗号技術の現状を解説し、ユビキタス環境におけるセキュリティとプライバシーについて、従来型 IT システムとの比較から分析し、ネットワーク、デバイス、情報家電の各面から検討。

５．セキュリティ・プライバシー保護に関する制度

ネットワーク社会におけるセキュリティ・プライバシー保護について、制度面から解説。

６．ユビキタス情報環境におけるセキュリティ／プライバシーの脅威

ユビキタス情報システムのためのシステムモデルを示してユビキタス情報社会におけるセキュリティとプライバシー問題を分析し、また、個人が撮影された映像や音声が他人に閲覧される脅威について検討。

7．セキュリティ／プライバシー保全技術・システムの開発のために（提言）

セキュリティ・プライバシー保全技術の開発、および、ユビキタス特区の実証実験プロジェクトへ向けて提言。

Ⅱ．資料編

IPv6に関する内外の状況、各社のユビキタスコンピューティング関連ビジネスの取組み、Ubicomp2002から見たユビキタス情報環境関連研究の動向を紹介。

また、内外のユビキタス情報環境およびセキュリティ関連プロジェクト一覧を掲載。

2．ユビキタス情報環境におけるヒューマンインタフェースとは

携帯電話や PDA などのモバイル機器の高機能化とネットワーク環境のブロードバンド化が進み、個人が気軽にネットワークサービスを利用できる情報環境が実現しつつある。最先端の情報通信技術が仕事や生活の様々な場面に浸透し、行政、金融、教育、出版、放送、輸送、観光、娯楽、スポーツから戦争に至るまで、産業や社会基盤をも変革する存在となった。情報のデジタル化と有線/無線ネットワークの拡張は今後も続き、2005 年ごろの次世代情報通信環境は、「いつでもどこからでも」ネットワークにアクセスできる「ユビキタス・ネットワーク環境」と捉えることができる。「ネットワークありきの環境」の下で、新しい技術、製品、サービス、産業が生まれるであろう。2010 年以降には、「人間のいる環境自体にいたるところ埋め込まれたセンサおよびコンピュータが、個々の人間の状況・情報を感知し、ネットワークを介して適切な情報を検索・収集して提供する環境」すなわち、「ユビキタス情報環境」が実現していくことが予想される。サイバー/リアル・ワールドが共生するユビキタス情報環境の上に成り立つユビキタス情報社会においては、産業・経済・社会インフラ等が一変し、新たな社会問題も生まれる可能性がある。多様な個人が情報通信技術の恩恵を受けて、安心・安全・快適な生活を送るためには、ユビキタス情報環境におけるヒューマンインタフェースがますます重要となることは間違いない。

ヒューマンインタフェースは「人間社会のためにコンピューティング・パワーを活用する」という懐の深い研究分野であり、「操作性（usable)」と「有用性（useful)」の二つの方向性を追求している。前者は人間支援のための大切な研究アイテムであるが、既存製品の操作性改良だけでは新しい市場や文化を創造できない。後者は人間に役立つ新しい機能・環境・サービスを創造する成長分野である。様々な入出力デバイス、知的情報処理、情報通信インフラの利用を視野に入れており、ユビキタスコンピューティング(Ubiquitous Computing) の主要学会でも、ヒューマンインタフェース研究者が中心的役割を果たしている。

ユビキタスコンピューティングのコンセプトを提唱した故Mark Weiserは、オペレーティング・システムとヒューマンインタフェース（ユーザインタフェース）を専門としていた。同じゼロックス社のパロアルト研究所のAlan Kayに感化され、人間社会の望ましい姿を展望し、パーソナルコンピュータに続くコンピュータのパラダイムとして、多様なコンピュータや入出力デバイスが遍在し、その存在を意識しない形で生活空間に溶け込むユビキタス情報環境（世界）のビジョンを描いたわけである。

パソコンや携帯電話で現在主流のGUI（Graphical User Interface）は、WIMP（Window、Icon、Menu、Pointing Device）と「See & Point」型の操作が基本となっている。パソコン、携帯電話、インターネットが普及し、ブロードバンド化とワイヤレス化が進み、ネットワーク上の情報は飛躍的に増大し、GUIでは欲しい情報に思い通りにアクセスできないというGUIの限界が明らかとなってきた。ユビキタス情報環境下では、さらにセンサ情報が指数関数的に増大し、情報洪水の問題が深刻化することは間違いない。このため、ユーザの意図や情報の内容を理解して「Ask & tell型」で対話できるPUI(Perceptual User Interface)

や様々なセンサ情報から状況を理解するマルチモーダル情報マイニングの研究が重要視されてきた。

本調査研究では、「次世代情報環境におけるヒューマンインタフェース技術」について、安心・安全なユビキタス情報社会の実現と産業貢献に的を絞って検討してきた。特に、現実社会を注視するという立場から現行の技術的課題を掌握し、2010年の本格的ユビキタス環境に向けて、次世代のヒューマンインタフェースの研究開発に関する提言を行うこととした。

昨平成13年度の調査研究において、電子商取引（EC）におけるユーザ・アンケート調査の結果からも、また、ユビキタス情報環境とのヒューマンインタフェースを実現するための技術調査においても、使いやすいインタフェースとともに、安全・安心な生活や産業を支えるものとして「セキュリティやプライバシー」が重要課題と指摘された。

携帯電話、PDA、デジカメ等の多様なモバイル機器の高機能化と普及は進んでおり、それと同時に、有線・無線の通信インフラの高速化とサービス拡大が進んでいる。パーソナルな情報はますます増え、個人情報の交換・流通が増え、個人にとっては利便性が増し、また、産業にとってもビジネス展開の上で重要となっている。さらにユビキタス情報社会へ向けて、センサ・各種デバイスが微細になり各所に埋め込まれ、それら「全てのモノ」に個別のIDが付与され、各種センサ情報や位置情報が付与され、コミュニケーション機能とインテリジェント機能が充実した情報環境が実現すると、個人情報の交換・流通は激増する。マルチモーダル情報のマイニング技術の高度化で個人の様々な活動もトレース可能となる。

そのようなユビキタス情報社会では、多様な個人の多様な要求に応える新しいビジネスモデルの開発や産業の創生も期待される。しかし、プライバシーに関わる自己情報をコントロールし、安心・安全を保全する機能が情報通信インフラや各種ユビキタス機器（携帯機器、自動車、情報家電、組み込み機器を含む）に備わっていなければ、社会システム全般が脆弱となる。来るべきユビキタス情報環境で発現するセキュリティやプライバシーの諸問題を技術的かつ法的な側面から洞察することも必要となる。

本調査研究においては、ユビキタス情報環境におけるヒューマンインタフェースを「人間支援のためのコンピューティングパワーの活用」という観点で捉え、様々な分野の専門家で「光と影」を議論した。ユビキタス情報社会におけるプライバシー保全に関する多面的な問題点の整理と具体的提言は世界でも先駆けたものであり、「安心・安全・心地良い」ヒューマンインタフェースの実現についての知見が得られている。

３．ユビキタス情報社会の展望

コンピュータが究極的に小型になり安価になる近未来には、これに単機能の仕事をさせたり、使い捨てに近い形で利用することが可能になるであろう。その時代には、身の回りの全ての物、日用品、環境、衣類などに、コンピュータが認識できるIDタグや、ネットワーク接続されたコンピュータとセンサが組み込まれる、ユビキタスコンピューティングが今後のコンピュータ利用の主流になると考えられている。このようなユビキタス情報社会では、人々の暮らしは格段に便利になり、産業界にとっても、新しい技術分野と市場が生まれ活性化されであろう。その一方で、生活のあらゆる状況をコンピュータネットワークから把握できてしまう情報化社会には、さまざまな問題が浮上してくると考えられる。

そこで本章では、ユビキタス情報社会を展望する目的で、その光と影の側面を考察する。以下では、人々の生活シーンを、仕事場、外出先、家庭の３つに分類して、それぞれの場面でのユビキタスコンピューティングアプリケーションの可能性と、想定しうる問題点を未来予想のシナリオ形式で展開する。なお、シナリオからはそれぞれのテーマが読み取りにくいと考えたので、傍注の形式で論点を示した。

３．１　ユビキタス情報社会の光

３．１．１　オフィスにおけるシーン

人手で管理していた宅配便も数年前までには、電子的に現在地を登録していくシステムが完備し、預かり番号さえわかっていればWWWでトレースできるようになった。しかし、人的ミスにより、バーコードの読みとりもれなどにより、紛失やトレース不能の事故はなかなか減らなかった。

位置特定による物流管理

いまは、伝票につけたIDタグを無線でスキャンすることで、店舗受付、輸送、拠点での作業、宅配のすべての行程でスキャンゲートを通過するようになっており、品物が追跡から漏れることはなくなった。さらに、最近では、店舗受付も簡略化され、データの投入ミスも激減した。住所に固有のIDをつけるシステムが普及し、親しい知人の場合にはあらかじめ相手のIDをもったタグを受け取り、それを貼り付けるだけでよくなったのである。

物流は安全、安心が競争力となった。とくに、安全の保証となる宅配保険は、包みの中のタグ付きの物品にだけかけられるようになった。コンビニで預けた内容物をスキャンしたスナップショット受領書をもらっているので、預かり証拠となる。一般の商品もどういう生産ルートを通ってきたか、タグをよみとってIDサーバで検索すれば一目瞭然になっている。生産から流通ルートまではっきりしているので責任をとる部署がはっきりしていて、もし問題があれば追跡できる。結果として、安心して商品や食品を入手できるようになった。

流通経路IDによる保証

再活性化の自動化

引っ越し業者も流通の一部であるが、不活性処理のおかげで少々やっかいである。一時期、購入した物品はタグの不活性化をすることが奨励されたので、これをまとめて運ぶ際にはあらためてタグを貼らなければならない。タグとモノの対応付けはその場限りなので人手では大変である。幸いトラックに乗せるコンベアに自動カメラがついたので、荷積みのときの物品一覧ができるようになった。また、その一覧データを使って家財保険事業が成功した。

入社屋証タグを使った音声秘書

社屋に入る人はすべてタグつきのバッジをつけてもらう。見覚えがあるあの人は株主総会にいた個人出資者だが、急に名前が思い出せない。耳栓イヤホンにふれておけば、「やあ、いらっしゃい」と挨拶しているうちに、相手のタグを読みとって、耳元で「Y さんです」とささやいてくれる。「株主の Y さんでしたね。さあ、こちらへ、確か動線設計の経験がおありとか」とスムーズに会談に入れた。

行動パターン解析によるワークフロー改善

社員のワークフローにも効果がある。個人 ID トラッカーを使うと、社内での個人の動線が明らかになってくる。会社規模でのワークフローの最適設計が可能になった。年間を通じての動線管理データから、繁忙期を抽出して、作業量を平準化できるようになったのだ。データ解析の時には個人が特定されないようになっている。よく監督している上司なら、パターンをみれば大体、どれが誰かわかってしまうが、問題とはならない。

コールドスポットの設置

社内には、タグ不活性ルームができた。いわゆるコールドスポット（あるいはほっとスポット）だ。行動パターンデータは統計的な意志決定と安全のためにのみ利用可能で、個人の業績を査定することは禁止されたのだが、まだ気味が悪いという人は多い。しかし、このような行動が記録されない、ほっとする場所に集まっているうちに、新しいアイデアがどんどんでるようになってきた。

会議調整エージェント

突然の会議の招集などは、個人のエージェント同士がネゴシエーションするので、いま、だれがどこにいるかをいちいち人が知る必要はない。

状況認証付き伝言エージェント

そういえば、今日は忙しくて昼ご飯を食べ損なった。だれでもいいからあと 30 分のうちに、あの鮨屋の近くを通る社員がいたら、寿司でも買ってきてもらおう。相手を決めずに場所に対して社員にメールを送っておいた。だれか買ってきてくれるだろう。場所 ID と個人 ID を関係づける仕組みとメールがうまく働いている。

ユビキタスセンサ病院

病院はユビキタス特区に指定されて、すべてのモノに ID タグがつけられ、院内のあらゆる場所に ID リーダが設置されている。ビデオカメラやタッチセンサ、マイクロホンが主要な診察室、手術室、廊下、病室、看護師室に設置されている。トイレなどは壁床圧センサのパタ

ーン解析で異常検出ができるようになってから、事故が早期に発見できるようになった。

医師と看護師はウエアラブルシステムを装着し、音声と映像、行動パターン、生理データを記録している。ビデオは特定の処置のみが記録されるようになっているし、医者と患者のプライバシーは最大限に配慮され、これらの記録は自由にON/OFFできる。しかし、このデータが医療の向上に役に立つことが実証されるにつれ、協力的な医師・看護師と患者が増えてきた。記録したデータは、日々の医療・看護日誌として自動的に記録され、過酷な一日のしめくくりは15分のサマリーのチェックで終わるようになった。今日はたくさんの急患があってすっかり忘れていたが、サマリーチェックで思い出すこともある。この数日の勤務記録と当日の体調と、点滴液を用意したときの状況のデータを集めて、ヒアリハット対策室に送っておいた。これで体調の悪いときは宿直からはずしてくれるかもしれない。

電子医療日記システム

体調が悪いときに、ちょっとヒヤッとしたこともある。患者Bさんの点滴液を患者Aさんに投与するところだったのだ。幸い点滴器のリーダが、カルテIDとベッドIDと患者さんにつけた腕輪ＩＤと看護師IDを全部読とっていて、看護計画との照合を行っていて、点滴液の間違いを警告してくれたのだ。

医薬品ID完全管理システム

製薬会社Xの納入した点滴液が一箱全部、違うIDとラベルが付いてきた大事件があったことを思い出した。あのときは、点滴器のリーダは完全にだまされてしまったが、チューブについていた成分センサが点滴液との不致を教えてくれて間一髪だった。病院の緊急アラームに点滴液のタグをつけて、病院中に知らせてやったので、あの会社の薬剤が一瞬にして使用不可になって、事故にはならなかった。

薬剤センサシステムと病院集中管理システム

研究者のR氏の一日は秘書S氏とのミーティングから始まる。昨日の電子秘書エージェントによる推薦や外部との自律応対パターンをチェックして、その応対アルゴリズムをチェックし、その後で、その日一日の計画を確認して電子秘書エージェントにそのスケジュールを知らせるのである。電子秘書エージェントは、昨日のR氏の記録を、タグとのインタラクションをベースに、何があったかを記録している。それぞれのイベントに意味づけをし、状況説明ができるところとできないところを一つずつ提示する。複数のプロジェクトを持っているR氏の行動によると、そろそろプロジェクトXのことを忘れているかもしれない。状況から、そろそろ催促メールを出す必要がありそうだ。

賢い電子秘書システム

電子秘書エージェントが新しい会議の約束をもっていた。R氏のスケジュール表に書き込む。N社との製品Yのプロジェクトの打ち合わせである。スケジュール表には、製品Yの試作品のIDをいれておいた。こうすれば、当日、会議に向かう時間に、試作品を手に持ってい

状況依存リマインダー

なければアラームがなるのである。ついでに、手帳、財布、PDA の ID も入れておいてあげよう。ここ 2、3 度忘れて、届けたことがあるから。

記憶想起型在庫管理システム

今日は物品検査の日だ。以前は研究室中をスタッフ全員で捜し物をしたこともあって、検査に 1 週間も 2 週間もかけたものだ。秘書の S 氏でも、物品のおよその場所と、使っている写真と、名称がわかっているので探し出すことに苦はない。棚には ID リーダが埋め込まれているから、自動的に一覧表ができあがる。空間に放置してあるものは、それを運んだ人とのインタラクション記録からおよその位置が割り出せる。それでもわからなければ、その人に聞きに行くと、教えてくれる。使った人もどこへおいたのか忘れてしまうが、その人のビデオ想起システムにより、記憶をスキャンしてもらうとわかる。

実体験ヘルプマニュアル

S 氏は頼まれた原稿をコピーするためにコピー室に向かった。古い e-paper をセットして古い原稿 ID と文字を一緒に不活性化するが、紙固有の ID は消えない。原稿ファイルをドラッグ＆ドロップしたが、なにやらエラーメッセージがでてうまく使えない。コピー機のメッセージボードには、同じエラーメッセージ前後のユーザ ID がでている。どうやら R 氏のようである。本人にどう解決したのか聞いてみよう。

パーソナル道ナビ

R 氏は今日は幕張の新製品展示会に出かけた。新しい機械を探しに行ったようだ。出張にウェアラブルヘッドセットは欠かせない。道ナビが行き先を教えてくれる。あちこちの電光掲示板や LED がマーカーになっていて場所を教えてくれる。会場に着くと、展示会プラグインチップを預かった。これで会場のマップとローカルサービスが受けられる。

活動レポート自動作成

ここでのサービスは、訪問記録を自動的にとって、出張レポートを作ってくれることだ。また、自分の行動や映像記録は皆で利用できるが匿名になるようになっている。興味をもって見た製品や、業者との質問回答がビデオと書き起こした文章で整理される。会場で会った O 氏とのちょっとしたプライベートな会話はプライバシーモードの記録に残っているだろう。O 氏は何を見たのかな？ちょっとメールで検索先を教えてもらおう。

3．1．2　パブリック＆モバイルにおけるシーン

行動予定参照による携行品決定

外出時の支度の方法も以前とは大きく変わった。ホームサーバからユーザの一日の行動予定（何処へ行くか、移動手段は何か、屋内か屋外か、など）を参照し、その場所の気象データと付き合わせることで、傘の有無や快適な服装が選択される。この時代、忘れ物は存在しない。外出時に必要なモノがその存在場所を「自己申告」してくれる。全てのモノを携行しないとドアが開かないようにすることもできる。

詳細な位置把握とナビゲーション/途切れない通信環境

知らない街への出張も苦にならない。歩道の敷石に埋め込まれたチップと靴底のアンテナが通信するので、自分の位置を見失うことは無い。郊外でも、街灯や電線がホットスポットを兼ねた位置検出システムを形成しているので、位置情報やネット接続が途切れることは無い。目的場所への道順や地図は手元の小型ディスプレイに表示されることが多いが、メガネやコンタクトレンズに仕込まれたウェアラブル・ディスプレイを使う人や、耳に装着したイヤホンによる音声ガイドの他、背中や腰に振動で伝えるバイブレーションガイドもある。最近では、靴底に仕込まれたマイクロアクチュエータで歩く方向を自動調節してくれるものも出始め、考え事をしながらでも目的地につけると評判になっている。

全車ネットによる総合交通コントロール

車による外出もずいぶん楽になった。数年前までは名物だった交通渋滞もまず見掛けない。全ての車と信号器がネットワーク化されているので、全ての車の行き先を考慮して、最も効率の良いルートと信号のタイミングがリアルタイムに設定され、各車のナビゲーション機器に通知される。最近は自動運転が流行りだ。一部の車マニア以外にとっては「移動手段」でしか無いので、寝ているうちに目的地に着いてくれる方が有りがたい。自動運転の導入時に問題になった事故時の責任についても、「人間操縦モード(最終責任は人間が持つが操作可能)」と「自動操縦モード（最終責任はシステム側（作成及運用）が持つが、人間は最低限の操作しかできない)」の２者択一によって解決された。もちろん、全ての人やモノに識別タグが付いた結果、自動運転による事故が起こらなくなったからこそできたと言える。

任意視点画像取得/人物やモノの追跡/混雑状況把握

一昔前は、観光地など限られた場所にしかなかったWebカメラは、今では全ての街路灯や建物にくまなく設置されるようになった。当初は観光目的の他、商店街等で防犯目的での設置が進んだが、「どの場所でも見られる」ことの便利さが認知されるにつれ、急速に広がっていった。今では一部のプライベートな空間を除けば、人々は自由に画像を見ることができる。マルチカメラを用いた任意視点合成技術によって、好きな角度から街を眺めることも可能になった。

また、画像データの他にも、街中に設置されたタグセンサによって、人物やモノに付けられたID情報も参照できるので、「誰がどこにいるか」がわかる。特定の人の動きをトレースすることも可能であり、特に小さな子供を持つ親には安心なようだ。実際、誘拐事件や窃盗事件（＝モノの位置もトレース可能）はほとんど見られなくなった。待ち合わせの時もイライラすることは無い。カメラとIDセンサで目的の人物を見つけ出し、PDAやゴーグルの中に表示することで、雑踏の中でも確実に目的の人物を探し当てることができる。最近では、人が集まっているところ（＝人気のある場所やイベント）をリアルタイムで探し出し、行動目的（スケジュールデータの付き合わせでわかる）や

そのコミュニティにおける持ち物の指向を示してくれる「トレンド・ファインダー」が話題を集めている。

部品レベルのセンサ設置による早期異常把握

タグやセンサの貼り付けは個々の製品から部品レベルにまで及びはじめている。自動車・建物の構造部材・発電所や工業プラントなどの重要部品には、個々にセンサが取りつけられており、耐用年数経過や異常時には自ら申告するようになった。これによって、定期点検を行って異常を発見するという機器メンテナンスの常識は大きく変わることとなった。無駄な検査と不用意の機器停止が大きく減った結果、機器の稼働率増加による生産性の向上がもたらされたのは良く知られているところである。身近な例では、ペンキ塗り立てのベンチが教えてくれるので、誤って座ってしまう悲劇が見られなくなったのがあげられるだろう。

センサタグによる鮮度管理/万引き検出/指紋センサ付き紙幣

買い物のスタイルも大きく変わった。IDタグによる商品管理は以前から行われていたが、最近ではタグチップ自身がセンサと通信機能を持つようになっている。流通段階での温度管理（温度センサ内蔵チップ）はもちろん、ガスセンサによる食品の鮮度把握まで行われるようになっている。熟れ具合いを検出して食べ頃を教えてくれるメロンや、冷蔵庫に解凍具合いを指示する冷凍マグロなどが良い例である。品質の劣化した食品を食べてしまうことによる事故はほとんど見られなくなった。最近では、毒素センサ組み込みによる「絶対当たらない生ガキ」が人気を集めている。タグの効能は商店側にとっても多い。特にチップがセンサと通信機能を持ったことで、万引き対策も大きく変わった。レジを通らずに店を出ようとしたことをチップが検出し、通報が行われる。一時期、電磁波遮蔽バッグによるタグ隠しが行われたこともあったが、遮蔽検出機能付き新型タグ（通信が途絶したことを親機が検出する）が開発されたことで、現時点では店側の勝ちと言えそうである。また、お札や手形に指紋センサつきチップが搭載されたことで、「貨幣」の持つ意味が大きく変わりつつある。紙幣はそれ自身の有効性だけでなく、それを渡す人間の認証も行うのである。マネーロンダリングが事実上不可能になった為に、暗黒社会の縮小というオマケもついた。

状況把握によるモノ自身の動作制御

一方、モノの側から見れば、環境側との通信によって、自身が置かれている状況を知ることができる。その結果、動作モードを環境に応じてモノ自身がコントロールすることが可能になる。公衆環境ではマナーモードになり、所有者が車両運転中はドライブモードになる携帯電話は最も簡単な例である。この他にも、免許を携帯していないとエンジンのかからない車、禁煙場所では火のつかないタバコ、未成年だと蓋の空かない酒瓶などが広がりつつある。最近では、イタズラ防止の目的で、公共物に向けては噴射できないペイントスプレー等も出始

めている。

チップの別の利用方法もある。個々のチップの処理能力は非常に小さいが、数が膨大なので、全体としての処理能力はスーパーコンピュータを遥かに凌駕する。これを利用して、複雑な解析問題をチップに分担させる試みも行われている。ゲノムや蛋白質の構造解析の他、SETI（地球外知的生命探査）への応用など分野も広い。さらに、種々のセンサを持ったチップが地球全体に広がっている為、気象や大気の状態等が地球規模で観測可能である。加えて、チップ網の膨大な計算能力を利用した「地球規模の地球シミュレータ」との結合によって、ほぼ 100%の確率で天気予報が行えるようになっている。将来は、チップに装備されたアクチュエータを用いることで、気象や海流の制御、果ては惑星改造までが考えられているとのことだ。

グリッドコンピューティング/地球サイズの地球シミュレータ

3．1．3　家庭におけるシーン

高齢化社会が進行し、高齢者だけの家族や独居老人が増えてきた。昔のように大家族で暮らし、家族が支えあうライフスタイルも一つの理想であるが、それぞれ世代の家族が、生活のしやすさ、住み慣れた場所の快適さを享受して核家族で暮らす社会はしばらく変わりそうにない。近年の交通／通信事情と、生活のあらゆる場所に入り込んだユビキタスコンピューティング環境が、核家族にも、大家族の安全性とつながり感を提供しつつある。たとえば、住む人々の状況に気付いてくれるコンテクストアウェア機能が装備された住宅が一般的になっている。たとえ一人暮らしをしていても、親しい家族の役割を果たすハイテク住宅が見守ってくれて、必要ならば遠隔地の家族に知らせてくれる。この機能により、火事や災害、病気、犯罪などの緊急事態はもちろん、薬の間違いや忘れ物などにも対応してくれる。

高齢化社会とテクノロジー

たとえば今の家は、人の位置や状態を様々なセンサで検出してくれている。オフィスとはちがって、くつろぎの空間であるので、位置検出のためにアクティブバッジのように身に付けるデバイスを利用するのでは、はなはだそぐわない。そこで、天井や壁などに取り付けたカメラ、赤外センサ、マイクロフォン、振動センサ、加重センサなどが使われている。もちろん、スリッパや服、食器や家具、日用雑貨など家庭の中のあらゆる物に内蔵されているRFIDタグも利用される。その人の発話が聞こえれば、話者特定も可能である。服、スリッパ、話し声などから家族の誰であるかを特定した後は、カメラや人体センサが追跡して、家のどこに誰がいるか把握する。家の中のどこに誰がいるかが分かれば、その人の置かれた状況も分かってくる。周囲に誰か居るのか、一人なのか、曜日や時刻はいつなのか、その日のスケジュールはどうなっているのか、食卓についているのか、台所にいるのか、

コンテクストアウェアな家

周囲の温度はどうなのか、などの情報から、食事をしている、くつろいでいる、家事をしている、寝ているなどの状況を判断することができる。家にコンピュータやセンサ、ネットワークが組み込まれ、このような状況が安価にわかるようになった結果、これを利用した様々なコンテクストアウェアなアプリケーションが可能になった。

防犯

そんなアプリケーションの一つが、賢い防犯システムである。家宅侵入や窃盗などの犯罪を防ぐための機能は、コンテクストアウェアな家により容易に実現できるようになった。家の中にはカメラ、マイクロフォン、赤外線、電磁波、RFID タグや各種人体センサが設置されていて、家族の状況をコンピュータが把握しているので、侵入者の把握や、これを家族と区別する機能などは簡単に実装できる。

数年前までのホームセキュリティシステムは、泥棒も家族も区別が出来なかった。だから、自分で仕掛けたセンサに自分や家族がひっかかって、警備員に無駄な手間をかけて、警備会社からの請求額がふくらむこともしばしばあった。逆にセキュリティシステムを稼働させるのを忘れて外出する失敗も多かった。人の識別と位置が分かる家ならば、そのような心配は全くない。常時家が見張っていてくれるのだから、以前よりずっと安全である。ドアや窓の状態、家具の位置、物の位置まですべて検出可能なので、泥棒がどこから侵入して、どの家具を動かし、どこの戸棚の扉をあけていて何を盗もうとしているのか、インターネット上から生中継で把握することさえ可能だ。

コンテクストアウェアな家とネットワークが普及した結果、ホームセキュリティシステム自体のコストも劇的に下がった。数年前なら家に泥棒センサを取り付けるのはお金持ちぐらいのものだったが、現在では、簡単なセンサをネットワークに接続する安価なユニットがいくらでも売られているので、一人暮らしの若者でも、留守宅の異常を携帯電話に通知したり、留守宅を携帯電話から監視したりする仕掛けを利用している。

安全

台所、風呂、階段などで、火傷をしたり、溺れたり、転倒／転落する家庭内の事故は少なくない。だが、コンテクストアウェアな家では、一人暮らしの老人や、大人の目の届かないところにすぐに行ってしまった幼児や児童が、このような事故に遭い、手遅れになる心配はほとんど無い。どこに誰がいて、どう言う状況にあるかが分かり、通報などの必要な処置を手配してくれるからだ。家が常に家族の健康と安全に気を使っていてくれると言える。

家の中には危険物も多い。視力や判断力の弱った病人や老人が、間違った薬を飲むかもしれない。幼児が洗面所の扉を開けて、薬や消毒液や洗剤を飲むかもしれない。家が人と薬瓶の識別が出来れば、生活パターンからあり得ない投薬を警告することもできるし、大人が近くに居ない状況で、幼児が一人で危険物が入っている戸棚をあける動作

も警告できるだろう。

家の中で物をなくして困ることが最近めっきり減った。昔なら、テレビのリモコンや眼鏡を置き忘れて見つからないことが多かった。いまでも置き忘れることは変わらないが、家がその状況を覚えてくれているので、最後にリモコンを使った場所、眼鏡をかけた場所を指摘してくれる。ほとんどのなくし物はこれで見つけられる。　記憶の補助

面倒な作業の最中に中断が入るというのは厄介である。でもその作業の進行状況も家が見ていてくれれば助けになる。たとえば、ケーキを焼こうとボウルに粉や砂糖を入れている最中に、電話がかかってきて中断したとする。ボウルの前に戻ってきて、そこでベーキングパウダを入れたのかどうか、記憶がないことに気付きあわてることがあるかもしれない。だが、台所のカメラや、ボウルや調味料瓶のセンサが、状況を記録しておいてくれれば、自分がやっていたことを思い出す手がかりを与えてくれる。

人の行動を見ていてくれて、記録してくれる家ならば、人の記憶の手助けもしてくれることになる。人は高齢になると物忘れがひどくなる傾向にあるので、コンテクストアウェアネスは高齢化社会の家に必須の機能になっている。

人の位置や状況を知ることで、家の中のちょっとしたコミュニケーションを簡単に実現できる。例えばお母さんが台所で家事をしている最中に、子供に向かって「宿題はやったのか」って話しかけるとする。家はその発話を認識して、家の中の子供の居る場所を探して、そこに音声で伝達する。こんなスタートレックのドラマに出てくるような賢いインターフォンが実現できる。　家族のコミュニケーション

家族のコミュニケーションは、遠隔地で別居している家族の間で特に重要になる。遠隔地の独居老人が危険な状態になった場合に緊急に通報してくれる機能は先に述べた。それだけではなく、離れた家族のつながり感をアンビエント（環境に溶け込んだ）な表示や、タンジブル（物の手応えのある）な操作で実現するカジュアルなコミュニケーションツールが出現した。日用品にネットワーク接続されたコンピュータが組み込まれた結果、このようなツールが安価に実現できるようになったからだ。　つながり感通信

例えば遠隔地で暮らす家族の、電気ポット、ドアや窓やクローゼットの開閉、照明の点灯などの状況がネットワーク経由で得られるので、この状況を、暖炉の上の液晶表示の写真立て、電気スタンドの明るさ、造花の装飾の変化、床や壁を振動させることで発生する疑似生活音などにより、アンビエントに表示する装置が使われている。装飾の変化や、ドアの開閉音のような生活音から、遠隔地に暮らす家族の存在を身近に感じたり、異常を感じることができるのである。

子供や孫と離れて暮らす老人は、生活の一部を孫と共有したいと考

えている。もし孫と同居していれば、子供が居間のテーブルや棚に置いた、お気に入りの玩具や、学校で書いた絵や作品などを見ることができる。それをきっかけに話をすることも出来る。センサやカメラがいたるところにあり、ネットワーク接続されているなら、それを遠隔地で実現することができる。とはいえ、居間の様子のカメラ映像がそのまま伝わるのは、プライバシーの侵害になる。そこで、引き出しやおもちゃ箱や棚などの閉ざされた部分を撮影して、遠隔地に伝える家具が販売されている。機能は昔の Web カメラと同様であるが、物を入れるだけで伝達されるので直感的で使いやすい。表示も対になった家具の収納部分に実物大で表示されることが多いので、小さい子供にも内容を理解しやすい。一人暮らしの世帯にメリットが多いので、おばあちゃんなどが買って、孫の家に置くことが多いが、孫の方も誕生日プレゼントのリクエストをそれとなく入れたりして、ちゃっかり利用しているようである。

家族の思い出

つながり感通信のために、子供がおもちゃ箱を閉じるたびに写真を撮って、遠隔地のおばあちゃんの家に伝える装置がある。これで撮られた写真からは、子供のおもちゃの変遷も分かり、貴重な成長記録にもなる。台所の調理を記録してくれるカメラにより、日々の料理メニューの記録をつくることも出来るし、家庭料理のレシピを記録することも出来る。通常は人の位置検出にしか使っていない天井などのカメラも、パーティ、来客、家族の記念日などのイベントの時には、記念撮影のカメラとして使うこともできる。小説のレトリックに「家族の歴史を見守ってきた家」というような表現があるが、コンテクストアウェアな家はまさに文字どおり家族の思い出を記録してくれる家でもある。

ユビキタス情報ディスプレイ

家の中の日用品に、コンピュータ、ネットワーク、ディスプレイ、アクチュエータが組み込まれることで、日常必要なインターネット上の情報を、このようなどこにでもある日用品に表示して利用できるようになった。たとえば、インターネットトースターは、その日の予報天気や、株価の値を焦げ目で表示してくれる。数年前まで居間に置かれた温度計や晴雨計は、現在の温度、湿度、気圧などを表示するだけであった。今日の温度計はインターネットから予想最高／最低気温を取り寄せて表示してくれる。晴雨計もインターネットから正確な予報天気を取り寄せて表示してくれる。

このように必要な情報を常時表示してくれる単機能な日用品ディスプレイにより、忙しい朝の時間がすこしは楽になった。テレビの天気予報に自分の地域の情報が現れるのを待つ必要も無い。予想気温がクローゼットに表示されれば着ていく服を選ぶ参考になるし、降水確率が傘立てに表示されれば傘を持っていく判断がその場で出来る。目覚まし時計には、天気予報を表示する機能だけでなく、雪や大雨の悪天

候の場合、道路や電車バスの遅延があった場合、これらの情報をインターネットから取り寄せて、いつもより早めに目覚ましを鳴らす機能も組み込まれている。

家の中の人や物の状況が分かることで、エアコンや AV 機器のリモコンもいろいろと変わった。部屋に居る人の位置、人数、好みにより温度や風量／風向を変えるエアコンが可能になった。また、音楽 CD をスピーカーに置くだけで（あらかじめ音楽サーバに蓄積された音楽データが）再生できたり、その CD を左右や上下にうごかすことでボリュームや選曲を行うなどのリモコンが現れた。従来の機器をコントロールする機器／機能指向のリモコンから、空気や音楽などのサービスを直接コントロールする実世界／コンテンツ指向のリモコンにシフトしつつある。

実世界指向リモコン

3．2　ユビキタス情報社会の影

3．2．1　オフィスにおけるシーン

購入したものまで、流通経路と同じく場所を管理されるのはあまり気持ちのいいものではない。外の道から、家の中の財産の値踏みをしている輩がいないとも限らない。そこで、ID の読み取りが不可能になる、不活性化処理が流行しだしたが、こんどはそれを逆手にとった、保険金詐欺が現れた。受け取ってから不活性化をしてそのモノが紛失したと訴える手口である。商品の価格に比例して、保険の額も上がるので、詐欺師にはうまい商売である。

不活性化処理の悪用

ユビキタス社会は信用社会でもある。お互いに誰がいつどこで何をしているのか、誰が何を持っているのかを比較的楽に知ることができる。信用社会のアウトローは信用情報を闇社会に流してお金を儲ける。再活性化処理を行う引っ越し担当者は、その家の財産を全部リストとして簡単に入手できる。荷積みをしている最中から、オークションに登録する大胆な悪者も現れた。こういう輩を取り締まる方法はないものか。

信用の不法利用

病院がユビキタス環境になって集中管理されるようになったのはミスを減らすのには貢献したが、人間の尊厳はどこへいってしまったのか。病室はまるでロボットの体の中に閉じこめられているようだ。また、人間の独創的な判断もシステムはエラーとして解釈する。手術などの極限状態において医師の直感に基づく診断が、システムに受け入れられないと何もできなくなってしまうことになりかねない。

人間の尊厳無視と独創性の排除

3．2．2　パブリック＆モバイルシーン

ユビキタスの導入当初は大変だった。なにせ人の居場所やスケジュールは勿論、所持品や購入品、果ては食べたものや会った人まで全て

秘密の暴露による人間関係の破綻

わかってしまうのだ。これでは秘密や隠しごとなんて絶対にできない。「効率が良いクリーンな社会を造る」という建前論はわかりやすいし、実際に全てのヒト・モノ・カネの流れが全てネットワークを通じて参照可能になった結果、情報を制限することで利益を得ていた前時代的な商売が駆逐され、社会効率が大幅に向上したのは理解できる。でも個人的なつきあいは別だ。秘密の無い人間なんていないのだから。実際に導入当初には人間関係がほとんど破綻状態になった。システムを作った技術者連中はこんなことまで考えが及ばなかったんだろうけど、離婚率が98%になった年もあったっけ。私自身も職場・友人から家族に至るまで、全部ご破算になったクチだ。最近は一見落ち着いて来て、はた目には「クリーンな社会」が実現されたようにも見えるが、それは表面だけのこと。みんなあの手この手で逃げてるだけのことだ。

タグの不活化/ネットフリー物の氾濫

たとえば商品は、買ってきたらすぐに「不活化ボックス」に入れてタグを殺してしまうので、それ以後のトレースができなくなる。忘れ物管理なんかの便利機能が使いたければ、後付けのパーソナルタグをつければ他人からトレースされずに自分だけ使えるし、そもそもタグなんて無くても困らない。もっとも「私がこの商品を買った」こと自体は把握されてしまうので、特に気にする人は「足のつかない」旧札を使っている。最近は旧札人気でプレミアがつくようになったのが困ったものだ。モノ自体も、ユビキタス以前の「ネットフリー」なものが人気で、政府の駆逐策にもかかわらず、古道具屋やリサイクルショップは繁盛している。スケジュールなんかも会社で規定されている分はともかく、個人の分はネットに繋がないのが一般的だ。繋ぐ場合でも、「他からは読めない」ことを売りにしている業者や、政府にも解けないので使用が禁止されている強力な暗号が使える草の根ネットのサーバに置く人が多い。

広告メッセージ氾濫と重いフィルタ

街を歩けば広告の嵐だ。一歩進むたびに周囲から広告メッセージやSPAMが飛び込んでくるので、小さなウェアラブル・サーバなんかすぐにパンクしてしまう。かといってネットアクセスを閉じてしまったら、メールはもちろん、交通機関に乗ることもできなくなるし、だいいち信号が変わってくれないので道も渡れない。結局、強力なCPUを使ってフィルタリングするしか方法が無い。電池は持たないし重く熱いので、困り者だ。まだ昔の携帯電話の方が軽かったんじゃないか？SPAMの氾濫は重いOSと強力なCPUを売りたいメーカーとトラフィックを増やしたい通信業者の陰謀だという話がネットに載っていたけど…。

情報統制を嫌った草の根ネット化

車だって同じだ。今の全車ナビシステムは全体としての効率が優先されるので、個々の車にとっては最短ルート（時間や距離）では無いことがあるのが嫌なところだ。ネットの掲示板では、VIP向けに信号制御する裏オプションが高値で取引されている。位置情報検出装置の

設置は法律で義務づけられているので、外すのは違法だが、ナビの示す道を通らなくても違反にはならない。情報操作を嫌がる人達は、自分達で未加工の交通情報を収集して、草の根ナビシステムを造っているようだ。

情報集中による権力の発生

この時代、情報を持っているところが一番強い。基幹サーバにヒトやモノの情報が集中しているので、これにアクセスしないと何もできない。昔はOSやアプリを握ることが支配の条件であったが、今は違う。如何に大きなサーバを持つかで勝負が決まる。ユビキタスの黎明期から、サーバ（情報）の主導権争いは熾烈を極めたが、離合集散を繰り返して世界的に3つのグループに再編された。グループを跨がった情報参照は基本的にできない（ゲートウェイサービスもあるが、料金が高額なので、利用者は少ない）。まるで冷戦時代に逆戻りだ。もちろん、情報を握ることは国家にとっても支配の条件なので、当初は国家レベルで基幹サーバを運営し、法律をちらつかせて囲い込みが行なわれたが、いち早く国際的な巨大サーバ群を稼働させ、多様なサービスを提供した企業にはかなわなかった。今や少数の全体主義国家だけが、自前のサーバを運営し、自国民に使用を義務づけている（噂ではチップの不活化が禁止されていたり、身体へのチップ埋め込みが強制されているようだ）。しかしそのサービスレベルはお粗末なものであり、完全に世界から取り残されている。同じような例は、情報によるコントロールを目的とする宗教や民族団体にも見られるようだ。一方、特定の国家や企業のサーバに依存することを嫌がった人達が、草の根サーバを立ち上げることも多くなった。権力を求めないこれらのサーバ群が相互接続されることで、インターネットが始まった時のように、国家や民族を越えた新しい形態のコミュニティが拡がりつつある。

クラックによる情報漏洩

しかし一方で、毎日のように基幹サーバへのクラックと、情報漏洩が問題になっている。新聞の最終ページは告知記事で埋め尽くされており、人々は毎日、自分のデータが漏れていないかを確かめないと安心できない。一旦情報が漏れると大変だ。世界中の闇集団に寄ってたかって身ぐるみはがされるか、おもしろ半分のDDoSの嵐で生活すらできなくなる。持ち物を全部捨て、住所や時には名前や国民番号も替えて一からやりなおすしか無い。先日はついに国民番号サーバ（新旧番号のリンクが唯一保存されている）がクラックされて、大騒ぎになった。結構な人がネットが全く届かない公海上の漂流船舶集団に逃れたと聞いている。

3．2．3　家庭におけるシーン

プライバシー問題

家の天井にカメラを取り付けることは、最初のうちは抵抗があった。セキュリティや利便性の為に取り付けるにしても、居間や廊下などの

パブリックなスペースに限ることも多かったようである。しかしそれでは風呂で老人が倒れても、洗面所で幼児が洗剤を飲んでも家が知ることができない。カメラ映像はすべてコンピュータ処理され、画像データとしては残らないことが保証されてようやく普及したようである。そのために、業界団体が基準を設けて、生データが間違いなく廃棄されていることを証明するステッカーを貼付けている。カメラを内蔵した光学式マウスが受け入れられているのだから、同じような問題かもしれない。

話者特定や音声認識の為に常時稼働しているマイクロフォンも、不快な存在かもしれない。そこでカメラと同様に、音声システムにおいても音声データや認識結果がすぐに廃棄されることが重要とされ、それを認定するステッカーが貼られている。

とはいえ、遠隔の家族とコミュニケーションする場合や、家族の記念写真を撮影するアプリケーションでは、生の映像／音声データを保存することになる。メーカーもこのような製品が市場から拒否されないように気を使っていて、生映像を撮影するカメラは、引き出しや箱の中のような閉じられた空間に設置されるとか、生音声を録音するマイクロフォンは、ボタンを押している時しか機能しないなどのデザインが重視されている。

また、現在どのような情報が取得されているかをユーザに公開することで、プライバシーに関する不安に応えようとする製品もある。たとえばプライバシーミラーは、カメラとディスプレイからなる電子的な鏡であるが、自分に関してどのような情報を家が取得しているかを同時に表示してくれる。

家庭内情報の漏えい

家庭内の状況情報が外部からアクセスされるとしたら重大事件である。プライバシー的に問題であるばかりではなく、生活パターンが漏れたり、状況情報が改ざんされたりしたら、防犯機能も正しく働かなくなり、犯罪にも巻き込まれかねない。そこまで深刻な事態にならなくとも、家の中の商品の一覧、家族の趣味などの情報は、マーケティング情報として価値が高いので、狙われることも多い。そこで、家庭からインターネットに接続するゲートウェイサーバには強力なファイアウォール機能が求められる。

4．セキュリティ／プライバシー保全技術の現状

4．1　暗号技術の現状

本節では、ユビキタス環境でのプライバシーを保護する暗号技術の最新の現状について述べる。

情報通信におけるこれまでの暗号技術は、送信者と受信者の間に不正な第三者がおり、メッセージの暗号化や送受信者の認証などにより、それらの脅威から送信者と受信者を守ることに焦点が置かれていた。ところが、P2Pをはじめとする従来の枠組みでは説明の出来ないネットワーク環境やユビキタスデバイスなどの新しいプライバシーの要請が生じてきている。暗号技術も、古典的な送信者と受信者の信頼を仮定したモデルではなく、送信者と受信者が互いに信頼できない、あるいは、受信者に対して送信者が分からないようなより強いモデルの上での安全性にその主流が移行してきている。

1978年の公開鍵暗号の発明を発端とした現代暗号理論は、インターネットの時代の到来と共に多くが実用化に至っている．最近の研究の主流は、量子暗号などの新しい暗号技術の開発と従来の暗号技術の安全性の理論的な証明である。プライバシーを守るための研究は、これらの要素技術に付随して発展してきている。暗号プロトコルも、こういった新しい研究のひとつである。

暗号プロトコルとは、暗号要素技術を道具としてネットワーク上での作業を安全に、公平に、確実にするための研究である。プロトコルと言うからには，通信のための手順であり、互いに信頼できないプレーヤーがこの手順を守っている限り，不正がないことを互いに検証できる。例えば、代表的な暗号プロトコルである電子選挙の例で考えよう。投票者は集計者を信頼できず、投票内容を知られたくないが、正しい集計結果は知りたい。集計者は投票者が信頼できず、正しい投票権を持っている投票者が本物の投票用紙で投票しているか確認したい。この二種類の要請を満たすために、1）公開鍵暗号技術、2）一方向性関数、3）秘密分散法、4）ロ知識証明などを用いて、安全なプロトコルを構成することが、暗号プロトコル技術の目的である。

通信路を秘匿して第三者から守るのはもはや当たり前で、暗号プロトコルが目指しているのは、不正直な送信者や受信者の内部からの不正から守ることである。そして、残念ながら我々は本質的にこの不正直さから逃れることは出来ない。多少乱暴を覚悟して言い切ってしまうと、暗号プロトコルとは、内部不正を防止して、個々のプライバシーを守る技術である。

ここでは、プライバシー保全技術の例として、内部告発を安全に行うリング署名と匿名通信路について紹介する。

４．１．１　リング署名

2002年度の米国Time誌の今年の顔（persons of the year）は、3名の女性が選ばれた。ワールドコム，エンロンといった内部不正によって経営破綻した大手企業において、自己の不利益を省みず、不正経理などを告発をした、いわゆるホイッスルブローワー（whistle blowers = 警笛を吹く人たち）である。奇しくも、日本においてもホイッスルブローワー達が大活躍した年であった。電力会社の運営記録改竄や牛肉偽造などの記憶が生々しい。幸いにして、これらホイッスルブローワーに対する印象は悪くない。企業経営を正しく補正する潜在力として期待されているほどである。

しかしながら、実際には内部告発者には苦悩がつきない。告発による経営側による差別、経営の悪化による自己の不利益。これらのリスクがあるにも関わらず、虚偽の告発でないことを保証するためには、やはり社内の者であることを証明する必要がある。プライバシーは守って欲しいが，社員であることは信じて欲しい。この相反する要請を満たすにはどうしたらよいだろうか。

リング署名は、2001年のASIACRYPTでRivest、Shamir、Taumanらによって提案された暗号プロトコルである。“How to leak a secret”（秘密を漏らす方法）という挑発的な論文名をつけている。このプロトコルは次の二つを目的としている。

－メッセージの完全性（メッセージが署名されてから改竄されていないことの確認)、
－署名者の匿名性（署名者が列挙されたものの中の誰かであるかわからない）

リング署名は、署名者が他のユーザの公開鍵と自分の秘密鍵を用いて連鎖的に計算するデジタル署名である。乱数から初めて、他の候補者の公開鍵を用いて署名の連鎖を作り、最後に自分の秘密鍵を用いて、署名連鎖と最初の乱数の逆関数を求めて、リングを「つなぐ」。この署名の連鎖と署名候補者の公開鍵の列がリング署名となる。検証者は、リング署名から、少なくともその候補者の中の一人がリングを「つない」でいることを確認するが、誰が真の署名者かはわからない。署名の連鎖がどこから始まっているかわからないことが匿名性の保証である。戦国時代に，誰が発起人かわからないように傘状に連判を行った「唐傘連判」こそがリング署名の原理であるとも言える。

以下に，公開鍵（トラップドア付き一方向性関数）を用いて抽象化した、3ユーザ（A、B、C）のリング署名の具体例を次に示す。検証者Vは任意の第三者である。

1. 署名者Bは、乱数Rを選び、$c_C = R$とする。
2. Bは乱数s_Cを選び、候補者Cの公開鍵E_Cを用いて、$c_A = E_C(R, s_C)$を求める。
3. Bは同様に、$c_B = E_A(c_A, s_A)$を求める。
4. Bは、最後に、自分の秘密鍵E_B^{-1}を用いて、$s_B = E_B^{-1}(c_B, R)$を求めて、リングを閉じる。リング署名は、$s_A, s_B, s_C, c_A, c_B, c_C$である。
5. 検証者Vは，リング署名から、$c_B = E_A(c_A, s_A)$を満たすことを順に検証する。

4．1．2　課題

2001 年の Rivest らの発表を元に、次のような拡張や一般化の改良が行われている。

- ハッシュ関数と一方向性関数を用いた一般化と効率化（阿部，大久保ら，2002 ASIACRYPT）
- しきい値リング署名（n 人中の k 人以上が協力して行う署名）(Bresson, Stern and Szydlo, 2002 Crypto，桑門，田中，2002 ISEC，菊池，多田，2002 CSS)
- 匿名性破棄（Camenish and Lysyanskaya，2002，中西，2003 SCIS）

リング署名に限らず、暗号プロトコル一般に広く言える課題はその効率である。プライバシーを保証するためには、通常のプロトコルに対して必ず何らかの対価を納める必要がある。理論的な興味だけで構築されたプロトコルの中には、これらのコストが膨大で非現実的なものも少なくない。

- ラウンドコスト（プレーヤー間で行わなくてはならない通信の回数）
- 通信コスト（一回の通信で消費する帯域の大きさ）
- 計算コスト（各プレーヤーが実行しなくてはならない計算量および暗号化にかかる処理）

これらのコストは、署名候補者の数 n の関数で与えられる。基本リング署名のコストは，通信と計算のコストとも $O(n)$、ラウンド数は 1 である。

4．1．3　匿名通信路

匿名通信路（anonymous channel, anonymous communication）は、メッセージの送信者や受信者、あるいは両者をわからなくする技術である。ステガノグラフィが秘密通信の存在を隠し，送受信者の 2 者は特定されていたのと対照的に、匿名通信路では通信があることは明示的であり、多くの送信者と受信者の中で誰が本物であるか同定できなくすることを目的としている。電子現金や電子選挙などのセキュアプロトコルを構成する際に必須な要素技術の一つである。

明示的にされていないだけで、我々の身の回りの通信路のいくつかは既に匿名である。例えば、クライアントの情報を直接サーバに与えないと言う意味で、Web におけるプロキシーサーバ（proxy server）も一つの匿名通信路である。Web サーバは送信者、ブラウザは受信者なので、この場合は受信者の匿名性を守っていることになる。一方、郵便というメディアは、無人の郵便ポストがいたる所に用意されているという意味で送信者の匿名性がある。発信者不明の怪文書や細菌兵器を封印した郵便の配布に、この匿名性が悪用されていることがわかるだろう。もっと身近な例では、誰が見ているか同定しきれないと言う意味では、新聞、雑誌、テレビなどの既存のマスメディアは（受信者）匿名通信路といえよう。

匿名通信路を構成するには、いくつかのモデルがある。

1. 匿名中継者 - 単一の中継者による代理の通信。送信者の匿名性、受信者の匿名性の両方がある。
2. 確率的中継者 - 複数の中継者間で確率的に経路制御する通信。送信者の匿名性を保証する。
3. 多重暗号（MIX-NET） - 複数の中継者のそれぞれについて経路と中継先を暗号化する通信。
4. 公開掲示板 - 誰もがアクセスできるメディアを媒体にした真の受信者に通信。
5. 秘密分散 - メッセージを複数の中継者に分散し、それらの協調によりメッセージを復元する通信。送信者の匿名性を対象とする。

匿名中継者は、最もシンプルな匿名通信路である。使い捨ての仮名を用意し，真の送信者の代理でメールを転送する匿名リメーラーはこのモデルである。送信者の匿名性を保証している。一方、前述の Web プロキシサーバは受信者の匿名性を守る匿名中継者である。更に、クッキーやスクリプト言語の処理を追加したよりセキュリティに特化したシステムもある。これら匿名中継者の欠点は，匿名性が単一の中継者への信頼にかかってしまう点である。中継者の通信履歴が漏洩すれば、匿名性は容易に失われてしまう。そこで、中継者を複数用意し、受信者までの経路を確率的に決定する確率的中継者も提案されている。

Mix-net は最も強い強い匿名性を保証しており、匿名通信路の代表的なモデルになっている。

1. Aは、Bに至るまでの経路を自分で決める。これを、$C_{i1}, C_{i2}, \ldots, C_{im}$とする。
2. Aは、メッセージmをBの公開鍵で暗号化し、それを更に、m番目の中継者C_{im}の公開鍵で、

$$X_{im} = E_{im}\left(B \,\|\, E_B(m)\right)$$

と暗号化する。ここで、$\|$は文の連結、$E_B(\ )$はBの公開鍵による暗号化を表す。同様の処理を他の中継者についても繰り返し、最後に

$$X = E_{i1}\left(C_{i2} \,\|\, X_{i2}\right)$$

を得る。これを、最初の中継者C_{i1}へ送る。
3. C_{i1}は自分の秘密鍵で復号化して，次の中継者C_{i2}とメッセージX_{i2}を取り出し、その中継者に送信する。他の中継者も同様の処理を繰り返し、最終的な受信者Bへ$E_B(m)$が届く。
4. Bは復号化してmを得る。

経路は送信者によって動的に決められていて、各中継者は、自分の手前の中継者と次の中継者までしかわからないので、中継者の結託に対しても耐性がある。

4．1．4　まとめ

暗号プロトコルの背景とその要求条件を示し、内部告発を安全に行うリング署名の構成例と匿名通信路について述べた。安全性と同様に、プライバシーを守るためには通信量や計算量などの多くのコストをかけなくてはならない。他の代表的な暗号プロトコルの例には、億万長者問題（財産を秘密のままで比較する）、電子オークション（入札値を秘匿したまま落札値を計算する）、匿名通信（送信者の秘匿性して中継者の正当性を保証する）などがある。

個人情報の漏洩や度重なる内部不正行為を防止することが、電子政府や住民基本台帳ネットワークの運用に伴い最重要課題になってきている。官だけではなく，決算業務報告の証明、すなわち、アカウンタビリティ（説明責任）の重要性が企業でも認識されてきている。それらのために，コンプライアンスプログラムやシステム監査が効果があることは知られている。しかし、法制度だけではなく、技術的な観点からも、アカウンタビリティの実現を試みていくべきであろう。

４．２　ユビキタス環境におけるセキュリティ／プライバシー

４．２．１　ユビキタス情報システムにおける安全性

ユビキタス情報システムは、ITシステムが作る、いわゆるサイバーワールドと、人間・モノ・社会・自然環境等が作るリアルワールドとが共生し、相互的な関わり合いを持ちながら形成する新しい情報システムである（図 4.2-1 参照）。これまでの情報社会で主流として使われていたITシステムでは、ITシステムが提供するサービスを受けるために、人間がコンピュータに「向かう」必要があった。ユビキタス情報システムにおいては、情報機器はリアルワールドに溶け込み、その存在を人間に意識させない、もしくは、必要なときにすぐそばにある。このような情報機器を、ユビキタスデバイスと総称する。

ユビキタスデバイスは内部に、センサ、ID、プロセッサ、メモリ、ネットワークインタフェースを含みうる。センサはリアルワールドの状況を情報化して、情報処理可能な表現形式に変換する。IDはユビキタスデバイスを一意に識別するための識別子である。プロセッサとメモリがユビキタスデバイス内の情報処理を行う。ネットワークインタフェースは、ユビキタスデバイスと IT システムと間の情報交換や、ユビキタスデバイス同士の通信に用いられる。ネットワークインタフェースはしばしば、無線通信機能をもつ。このような

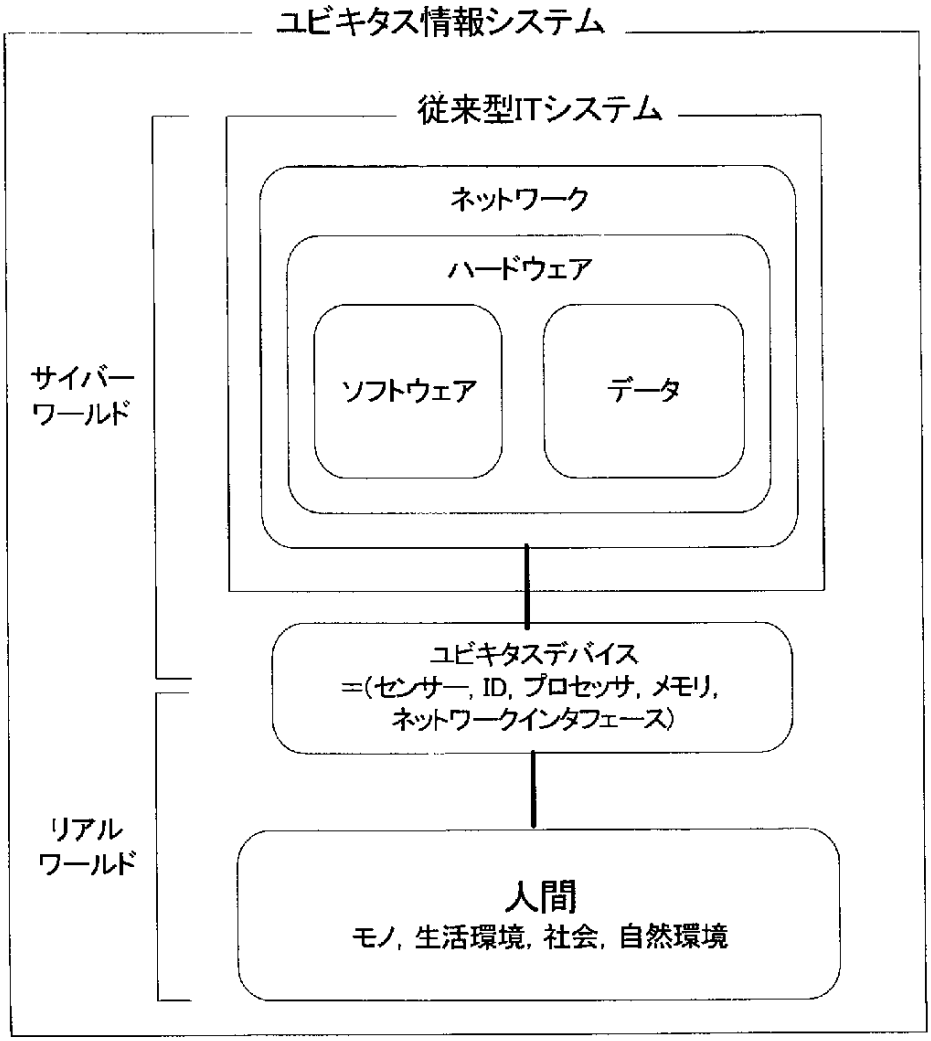


図 4.2-1　従来型 IT システムとユビキタス情報システム

機能を持つユビキタスデバイスが、デバイス技術の目覚ましい技術革新により、小型化・軽量化し、大量に、安価に入手可能となりつつある。

すでに生活に広く溶け込むに至ったユビキタスデバイスの一例が、ソニーの非接触型 IC カード FeliCa を利用した、JR 東日本の Suica である。2001 年 11 月 18 日の導入開始以来、2002 年 10 月 22 日に累計 500 万枚を突破しており〔1〕、国内の非接触型 IC カードのトップシェアを誇る。FeliCa は内部に 8 ビット RISC CPU、2～32Kbytes 実メモリ、212～848 Kbps の無線データ通信機能、ハードウェア DES 暗号処理系を有し、アンテナより受信した電磁波により動作電力を得る。典型的なトランザクション処理を 0.1 秒程度で終了する〔2〕。多数の一般市民の財布や定期入れの中に、クレジットカードのように薄く、軽いカードとしてこのような機能が「溶け込ん」でおり、情報処理機器であることをほとんど意識することなく、日常的に使用されている。

本章の主題は、このように現実のものとなりつつあるユビキタス情報システムの「安全性」、特に人間たるユーザの視点に立った「安全性」を検討することである。従来型 IT システムの安全性は、これまで長年に渡って、コンピュータセキュリティの技術として、研究開発が行われてきた。そこでの主題は、コンピュータシステムとネットワークシステムの内部に存在するソフトウェアやデータを、外敵からいかにして保護するかであった。一般にコンピュータセキュリティでは、機密性（confidentiality）、一貫性（integrity）、利用可能性（availability）の三概念が重要とされてきた*。機密性とは、情報資産（assets）にアクセス可能な者は、読み出し権限を与えられた者のみに限られていることである。一貫性とは、情報資産を更新可能な者は、更新権限を与えられた者のみに限られていることである。利用可能性とは、読み出し権限もしくは更新権限を持った者が、情報資産に対してアクセス可能で、与えられた権限を行使できる（すなわち、読み出しもしくは更新操作を行える）ことである。

セキュリティ上の脅威としては、図 4.2-2 に示すような、四つの脅威がある。(a) 妨害（interruption）とは、情報資産が破壊されたり、アクセス不能、利用不能とされることで、利用可能性を不能にする。(b) 傍受（interception）とは、情報資産へのアクセス権限をもたない者が、情報資産へアクセスを行ってしまうことを意味する。(c) 改変（modification）は、権限を持たない者が、情報資源の内容にアクセスすると共に書き換えることである。(d) 偽造（fabrication）は、権限を持たない者が、偽情報を送り込むことである．IT システムにおけるユーザ間、プロセス間、ネットワークを介したサイト間等で、これらの脅威があり得る。

従来型 IT システムにおいては、情報資産が、IT システムの内部で管理された、いわば閉じた情報資産であった。それに対して、ユビキタス情報システムにおいては、IT システムの外部にあり、ユビキタスデバイスを通じて IT システムと接続された、人間・モノ・社会・自然環境までもが情報資産となり、セキュリティを考慮されるべき対象となる。

---

* 第四の概念として、認証性（Authenticity）を加える場合もある。この概念は、コンピュータシステムが正当なユーザであることを確認できることを意味する。

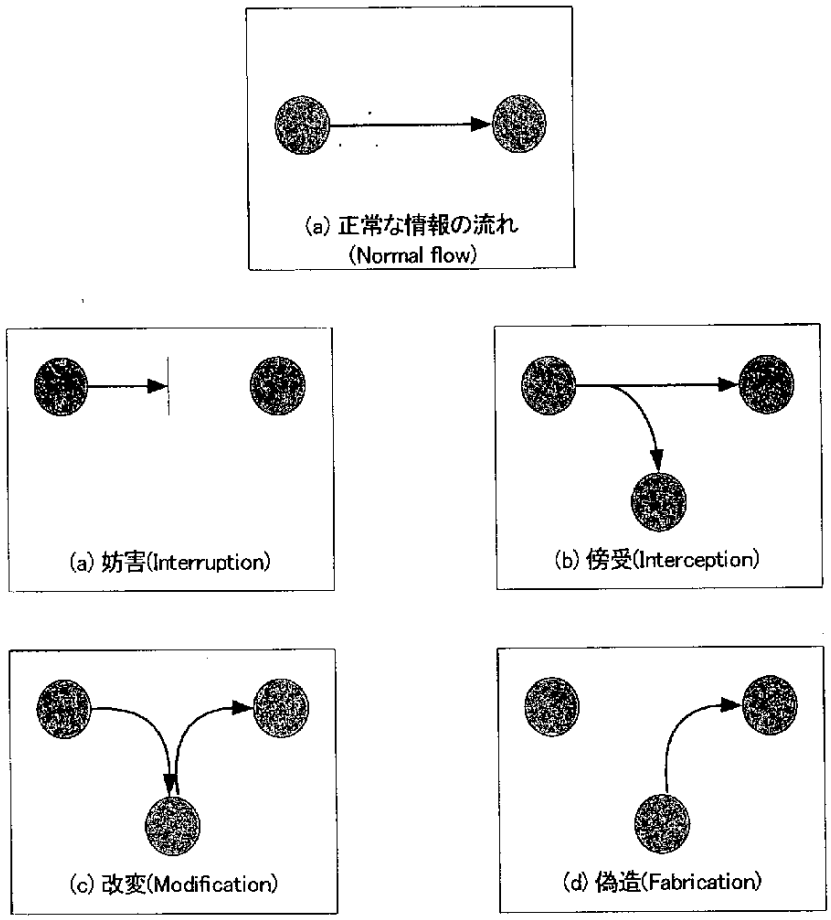


図 4.2-2　セキュリティ上の脅威
(W. Stallings, Operating Systems, 4th Ed., Prentice-Hall, 2001 より)

1990 年代中盤以降、インターネットや携帯電話に代表されるネットワーク・インフラの普及と整備は、情報の発信・収集・交換を行うコストを大幅に引き下げた。そしてさらに近年は、無線ネットワークや非接触型通信機能を有するユビキタスデバイスの普及により、極めて安価かつ容易に、人間世界の情報をコンピュータシステムの世界に取り込むことが可能になりつつある。このような技術革新の中で、情報の発信・収集・交換を容易にする技術を開発するのみならず、中心に存在すべき人間の意思、意図に反しないようにそれらをコントロールする技術や方法論を確立していくことが肝要である。人間は、他の構成要素と異なり、それ自身のさまざまな権利が保障されており、また、さまざまな感情や社会習慣も持ち合わせている。ユビキタス情報社会が発展するにつれて、人間に対するさまざまな安全性に関する問題が露見してくるものと思われる。以下では、現時点で露見している、あるいは、予見しうる、人間中心型ユビキタス情報システムの「安全性」に関する問題を、情報工学的な観点から検討する。

4．2．2　ユビキタス情報システムにおけるセキュリティ／プライバシー

従来の IT システムが形成するサイバーワールドは、情報資産はすべてコンピュータシステムの管理化にあるという意味で「閉じた」世界であり、セキュリティは、閉じた世界

の中で情報資産を外敵から守ることを主題としていた†。それに対して、ユビキタス情報システムが扱うリアルワールドは、コンピュータシステムの外にある「開いた」世界であり、ユビキタスデバイスが、閉じた世界と開いた世界の接点に位置し、両者の架け橋としての役割を果たす（図 4.2-1 参照）。ユビキタスデバイスをネットワークの一部と考えれば、人間と IT システムの間に、図 4.2-2 に示した四つの脅威があることを類推できる。あるいは、人間とユビキタスデバイスの間、および、ユビキタスデバイスと IT システムのネットワークとの間に図 4.2-2 に示した四つの脅威があることを類推できる。

人間中心型のユビキタス情報システムにおいては、従来の IT システムのセキュリティとして重要と考えられていた三つの主要概念—機密性(confidentiality)、一貫性(integrity)、利用可能性(availability)—に加え、識別性(identification)の概念が重要であると考えられる。識別性とは、他とそれとを区別し、存在を正しく認識できることである。ユビキタス情報システムは、サイバーワールドとリアルワールドがスーパーインポーズ(superimpose)された、一種のハイブリッドシステムであり、両世界の間での対応関係を制御することが重要である。しかも、人間は「自己に関係する情報をコントロールする権利」(情報プライバシー権)を有していると考えられている。この権利は、現代憲法論において、日本国憲法第 13 条が保証する生命・自由・幸福追求権に基づいたプライバシー権の定義となっている‡。

ユビキタス情報システムにおいては、コンピュータシステム側が識別性の制御を行えるようになっていると同時に、人間たるユーザ側も識別性の制御を行えるようになっているべきである。コンピュータシステムがネットワーク接続された IT 社会では、セキュリティのコントロールが重要な課題となったが、ユビキタス情報社会では、セキュリティに加えて、プライバシーのコントロールが重要な課題となる。

本章の続く節は、来るユビキタス情報社会において起こりうる問題を洗い出すために、既にある程度の利用経験がある二つの分野において、セキュリティおよびプライバシー問題の実際を解説する。4.3 節では、インターネットの Web システム上におけるクッキー、SSL、P3P 等の利点・問題点、携帯電話固有 ID に関する問題、常時接続時代における IP アドレス問題について論じる。続く 4.4 節では、ユビキタスデバイスの典型の一つである IC カードにおける、セキュリティおよびプライバシー技術の現状を概観し、問題点を整理・分析する。4.5 節では、情報家電のネットワーク化のときに、CPU パワーが弱くても、簡便性もあり、しかも高いレベルのセキュリティ／プライバシー保護機能をどのように表現するかを検討する。

---

† 認証性（Authenticity）が、コンピュータシステムの外部にある人間を、システムの正しい「ユーザ」として閉じた世界に接続することを表す概念。

‡ プライバシーの権利は、1964 年の「宴のあと」事件の一審判決で「私生活をみだりに公開されない法的保証ないし権利」と定義された。その後、情報社会の進展に伴い、「自己に関する情報をコントロールする権利」（情報プライバシー権）と捉えられて、自由権的側面のみならず、プライバシーの保護を公権力に対して積極的に請求していくという側面が重視されるようになってきている。（芦部信喜著、憲法、第 3 版、岩波書店、pp. 117-118 より引用）

【参考文献】
〔1〕 http://www.jreast.co.jp/press/2002_2/20021013.pdf
〔2〕 松尾隆司，非接触型 IC カード技術「FeliCa」の概要，インタフェース，2003 年 3 月号，pp. 66-75.
〔3〕 芦部信喜，憲法，第 3 版，岩波書店，2002 年.
〔4〕 Frank Stajano, Security for Ubiquitous Computing, John Wiley & Sons, 2002.
〔5〕 William Stallings, Operating Systems, Fourth Ed., 2001.

4．3　ユビキタスネットワークのセキュリティ／プライバシー：Web を例として

4．3．1　cookie とはどのような仕組みか

インターネットの World Wide Web では、「cookie」と呼ばれる仕組みが、Web 利用者のプライバシーを脅かす場合があるとして、たびたび問題視されてきた。

cookie は、それ自体は非常に汎用的な仕組みで、直ちにプライバシー上の問題を引き起こすわけではない。昨今の多くの Web サイトに見られる、ユーザ名とパスワードを入力してログインする機能を持つ Web アプリケーションを構築するために、cookie は技術的に欠かせない仕組みであると言える。その場合には、cookie は一時的なチケットとして機能する。

例えば、病院で健康診断を受ける情景を思い浮かべてみよう。受付で氏名を名乗ると受付番号を記した札を発行される。これを持って、内科、眼科、放射線科をまわって担当医に札の番号を見せて診断を受ける。このときの患者を Web ブラウザとすれば、受付はログイン画面で、ログインしたときに受け取った札が cookie である。ブラウザ（患者）は、各 Web ページ（各担当医）にアクセスするごとに、cookie（札）に書かれた番号（受付番号）をサーバ（担当医）に渡すという動作をする。この受付番号は一時的なものであって、ログアウト（健康診断が終了）すれば破棄される。次の年に同じ病院で再び健康診断を受けたとしても、同じ受付番号が与えられるわけではない。

しかし、cookie は、サーバ側の指示によって、長期間保存させることも可能である。例えば 1 年間有効な cookie を発行すれば、ブラウザは 1 年間、そのサーバにアクセスするたびに、その値をサーバに送信することになる。この場合、cookie の値は、ユーザのコンピュータのハードディスクに保存される。この機能の活用方法としては、ユーザの好み（画面設定）を覚えさせておいたり、掲示板に書き込む際の氏名を覚えさせておくといったことを、簡単に実現する（サーバ側で記憶するのではなしに、ブラウザに覚えさせる）ことなどが挙げられる。

4．3．2　cookie のプライバシーへの影響

こうしたハードディスクに保存される cookie が、その使い方によってはプライバシーの問題を引き起こす。

例として、ログイン、ログアウト機能のあるネットショップを考えてみる。アカウントを持つユーザが、ログインした状態でショッピングを楽しむと、そのユーザがどんな品物を手に取ったか（どんな品物の紹介ページにアクセスしたか）の情報が、サーバ側に知ら

れることは、ユーザにも用意に予想されることであり、そうした情報を蓄積され得ることは、ユーザも了解していると考えられる。もし、自分が誰だか知られることなく、いろいろな品物を手にとってみたいのであれば、ログアウトした後に、商品のページを渡り歩けばよい。このように、ユーザは、自分が誰であるかを示しながらアクセスする必要のある場合と、匿名のまま気楽にアクセスしたい場合があり、これらは切り替えられるようになっていてしかるべきである。

しかし、そのネットショップが、数年間有効なcookieを発行し、そこにユーザに関連付けた番号を記入していたとするとどうだろうか。ログインした状態であっても、ログアウトした状態であっても、ブラウザはこの番号をcookieとしてサーバに送信する。サーバの管理者は、ログイン時のユーザ名とその番号とを付き合わせることによって、ログアウト後のアクセスについても、番号からユーザを特定することができる。その結果、ユーザが匿名のつもりでいても、サーバ側が誰がどの品物を手に取ったかを知っているという事態が起こり得る。

このことはさしたる問題ではないと感じる人も多いかもしれない。ユーザは、そのネットショップにアカウントを作った時点で、そこを信頼したのであり、どの品物を手に取ったかについて、そのショップに知られたところで、プライバシーが侵害されたとは感じない人も多いかもしれない。幸い、cookieは、その発行元のドメインのサーバに対してしか送信されないように設計されているため、別のサイトへこの番号が漏れることは起こらない。（もしそれが起きるのなら、それはブラウザかサーバにセキュリティホールがあるということになる。）

4．3．3　サイト横断型cookieがもたらし得るプライバシー侵害

ところが、cookieが設計された当初にはおそらく予想もされなかったと思われる使い方が、バナー広告業者によって行われるようになった。

バナー広告は、広告を画像ファイルとして作成し、HTMLのIMGタグによって様々なWebサイトに貼り付けることで成り立っている。一般に、広告画像はバナー広告業者のWebサーバに置かれている。HTMLのIMGタグは、そのHTMLの置かれているサーバと、IMGのリンク先のサーバが別であっても、同じ画面中に表示するという設計になっているため、このように、広告出稿先の任意のWebサイトに、広告業者のサーバ上にある画像を貼り付けることができる。

ユーザがある人気のあるWebサイトを訪れたとき、そこにバナー広告が貼り付けられていたとすると、バナー広告業者のサーバのアクセスログには、そのユーザのIPアドレスと、広告出稿先のWebサイトのアドレスが記録されることになる。ユーザにとって、人気のあるサイトを訪れたとき、IPアドレスがそのサイトに記録されることは了解の上であろう。しかし、バナー広告業者のサーバにも記録されることはどうだろうか。IPアドレスが記録されても、それが誰であるかが常に特定されるわけではないので、そのことは気にしない人も多いかもしれない。

それに対し、バナー広告業者がcookieを発行して、そこに数年間有効な固有番号(ID)を記憶させていたとしたらどうだろうか。ユーザは、広告業者にユーザ登録するわけでは

ないので、広告業者が勝手に発行したIDから、そのIDの持ち主が誰であるのかは直ちには特定されない。しかし、もし、広告業者が、広告出稿先のネットショップと結託したらどうなるか。ネットショップのアクセスログから、そのショップにアカウントを持つユーザと、広告業者が発行したIDとの対応表を作ることができてしまう。これによって、広告業者は、そのIDの持ち主が誰であるのかを知ることができる（結託したショップの登録ユーザについてのみであるが)。

こうして広告業者に誰であるかを知られてしまったユーザは、その動向を広告業者に逐一知られることになる。これは、広告業者が結託したネットショップでの行動を追跡されるだけではない。その広告業者が広告を出しているすべてのWebサイトにおけるアクセス行動が追跡されることになる。もし、ある業者が、インターネットにおいて非常に高いシェアでバナー広告を出すようになったとすると、どこのWebサイトに行ってもその行動が、その広告業者に知られてしまうという事態になりかねない。

こうした問題は現実に起きそうになった。2000年1月27日のZDNetニュースには、「プライバシー侵害と消費者団体から反発受けるDoubleClickのデータ照合」という報道(*1)があった。

現在もそうであるが、バナー広告業者のほとんどは、広告画像に対してcookieを発行して数年間にわたり有効なIDを付与している。これは、誰であるかはともかく、同一の閲覧者がどの広告を既に見たかを管理するために発行されており、同じ広告を出さないようにするなどといった、効率の良い広告表示のために使われている。そうした目的のためだけにIDが使用されているのなら、ユーザのプライバシーを侵害することにはならないのだが、報道によると、DoubleClick社は、他社が集積した購買情報データと照合することにより、個々の人が関心を持ちそうな広告を表示することを計画していたという。

この訴訟は、2002年5月に和解に至ったと報道された(*2)。和解条件では、DoubleClick社は、「個人データの開示に関するプライバシー方針を掲載すること」、「顧客企業との個人データの開示に関する契約条件を守るために適切な手続きを保持すること」、「表示内容と一致した方法でのみ個人データの収集、利用を行なうこと」、「広告配信機能『DART』に関連して収集したデータは3カ月で破棄すること」、「顧客の1社に代わって収集した個人データを顧客以外と共有しないこと」などを遵守することとされたという(*3)。

4．3．4　P3P技術による解決

プライバシー侵害を引き起こすようなcookieの使い方を、法律や訴訟によって防止することも確かに有効かもしれないが、それと平行して、できることならば、技術的手段によってそうした使われ方ができないようにすることが望ましい。そのひとつとして、W3C (World Wide Web Consortium) は、P3P (Platform for Privacy Preferences) という技術仕様を開発した。P3Pは、Internet Explorer 6に採用されたことにより、広くユーザに普及した。

P3P登場以前でも、ユーザは、ブラウザのセキュリティ設定で、cookie機能を無効にすることができた。しかし、cookieを無効にしてしまうと、正当な目的でcookieを必要としているネットショップへのログインもできなくなってしまうため、ユーザは設定を適宜変

更する必要に迫られ、設定によるプライバシー確保は現実的でなかった。

それに対し、P3P 技術が導入された Internet Explorer 6 では、メニューの「インターネットオプション」に新たに「プライバシー」の項目が用意され、6 段階でプライバシーレベルを選択できるようになった。この設定によって、cookie が送信されたりされなかったりが、機械的に選択されるようになる。

機械的な判断には、サイト側が cookie をどのような目的で使用するのかを宣言した記述と、cookie が「サードパーティ」のものであるかどうかが加味される。「サードパーティ」の cookie とは、cookie 発行元のサーバが、画面の URL のサーバと異なる場合の cookie のことを指すもので、つまり、バナー広告画像が発行する cookie などがそれに該当する。Internet Explorer の出荷時設定では、サードパーティの cookie で、かつ、使用目的が宣言されていないものは、発行を拒否するようになっており、一定のプライバシー対策はなされたと言えるだろう。

4．3．5　「スーパークッキー」問題

P3P による cookie の問題が解決されつつある一方で、Web ブラウザの別の新たな機能が同様のプライバシー問題を引き起こす可能性があると、2002 年 1 月に指摘された(*4)。

Windows Media Player には、アプリケーションが初めから利用者固有の ID が組み込まれており、Web ブラウザの HTML から JavaScript を用いることでその値にアクセスできてしまうのだという。これは、cookie を使わずとも、個人の動向追跡に利用できてしまう。この問題は「スーパークッキー」と呼んで批判され、Microsoft 社は、この機能を無効化できるよう、ユーザが設定で選べるように Intrenet Explorer を改善した。

この改善は、具体的には、「ツール」メニューの「オプション」を選び、「プレーヤー」タブのところにある、「インターネットサイトによるプレーヤーの個別識別を認める」のチェックを外す設定にすると、Windows を再起動するたびにこの ID がランダムに変化するようになったというものである。これは、cookie 技術に、ハードディスクに保存されない使い方があるように、ID が長期間保存されないようにすることで、プライバシー侵害の危険性を軽減するものである。一般に、一時的な ID の必要性を維持しつつプライバシー侵害の危険を避けるには、こうしたセッション限りの ID とすることが有効であると言える。

4．3．6　携帯電話のサブスクライバーID 問題

最近の携帯電話のほとんどには、インターネットの Web を閲覧するための、簡易 Web ブラウザ機能が搭載されているが、日本の一部の携帯電話事業者が採用しているブラウザには、プライバシー侵害をもたらす可能性を持つ機能が搭載されている。サブスクライバーID と呼ばれる契約者固有の番号を、Web サーバにアクセスするたびに送信しており、利用者はこれを止めることができないからである。

サブスクライバーID は、cookie のようにサーバ側が ID を発行するまでもなく、携帯電話を契約した時点ですべてのユーザに初めから割り当てられている番号であり、その点ではスーパークッキーと同様である。そして、スーパークッキーでは、サーバが ID を得るには ID を得るためのプログラムを Web ページ内に仕掛ける必要があった（ID を得る意

思がないと得られない）のに対し、携帯電話のサブスクライバーIDは、サーバ側の意思とは関係なく、常時サーバへ送出されるものである。そして送らない設定にすることもできない。

このIDがプライバシーの問題を引き起こすのではないかという点について、携帯電話事業者のサポートセンターに問い合わせると、「サブスクライバーIDからお客様を特定することはできません」という答えが返ってくるという(*5)。

しかし、それが本当ならば、諸外国でクッキーが問題にされることはなかったはずであり、実際には、これまでの節で述べたように、個人の追跡に利用できる可能性をもたらしているはずである。

4．3．7　常時接続による固定IPアドレスがもたらす問題

かつてインターネットが専門家だけのツールであったころは、自分のIPアドレス（勤務先の研究所や企業のアドレス）が相手に知られることは了解の上でソフトウェアを使っていた。その後、インターネットが一般消費者のツールとして普及し、その利用目的も、研究や業務だけでなく、個人的な消費行動にも使われるようになった。利用目的が変化したことにより、一部の利用については、匿名性が求められるようになっているだろう。

一般消費者にインターネットが普及する過程で、当初は、インターネットへの接続方法は、電話回線を通じたダイヤルアップ接続によるものであった。ダイヤルアップ接続では、IPアドレスが毎回変化するため、これは結果的にプライバシー確保の役割を担ってきたといえる。偶然にも、利用目的が匿名性を必要とするものとなったと同時に、接続方法が匿名化されていた。

ところが、ADSLや光回線などによる常時接続が普及するにつれて、この匿名化が崩れつつある。グローバルアドレスが半固定的に割り当てられることが多くなってきたからである。今後さらにIPv6が普及すれば、IPアドレスがそのまま個人の所有物に一対一対応するようになるかもしれない。ほとんどの消費者がそうした状況におかれるようになれば、IPアドレスはスーパークッキー代わりとして使われるようになる危険性がある。何らかの方法によって、IPアドレスから個人が特定されることのない（またはそれを個々のユーザが選択できる）ように対策する必要があると思われる。

【参考資料】

*1: ZDNet News:「プライバシー侵害」と消費者団体から反発受けるDoubleClickのデータ照合, 2000年1月27日, http://www.zdnet.co.jp/news/0001/28/doubleclick.html

*2: ZDNet News: DoubleClickのプライバシー侵害訴訟、裁判所が和解を承認, 2002年5月23日, http://www.zdnet.co.jp/news/0205/23/nebt_16.html

*3: INTERNET Watch: 個人情報の取り扱いを巡る調査で米DoubleClickが10州と和解, 2002年8月27日, http://www.watch.impress.co.jp/internet/www/article/2002/0827/dc.htm

*4: Internet Explorer SuperCookies bypass P3P and cookie controls, Richard M. Smith,2002年1月16日,

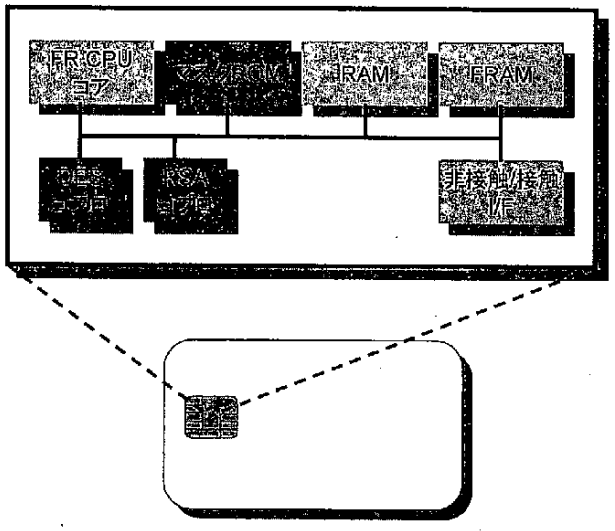
http://www.computerbytesman.com/privacy/supercookie.htm

*5: オープン化によるユビキタス普及・促進とプライバシー確保のジレンマ，日経ネット時評，高木浩光，2003 年 3 月 10 日，http://it.nikkei.co.jp/it/njh/njh.cfm?i=20030307s2000s2

4．4　ユビキタスデバイスのセキュリティ／プライバシー：IC カードを例として

IC カードは国内 IC カード市場としても 2001 年実績で 3500 万枚を超え、JR 東日本の Suica に代表される運輸交通分野など様々な分野で、ユーザである我々自身が広く実際に利用する段階に入りつつある。クレジットカードに代表される金融分野や形状は異なるが類似の機能を有する携帯電話の USIM カードなど、IC カードは、情報流通社会において確実な本人確認、権限の有無確認、情報（バリュー、個人情報）の格納などを行うためのキーデバイスとして、今後ますますその重要性が増すと予想される。IC カードはユビキタス情報環境における各種認証のキーデバイスとしての役割を果たすことになる。

IC カードは、CPU の有無などの機能面から、あるいは接触・非接触などのインターフェースの面から分類することができ、またその利用目的や利用要件によって様々なタイプがある。たとえば図 4.4-1 に示す FRAM§混載のマルチアプリケーション IC カードの例では、演算処理を行う CPU コアおよび DES コプロセッサ、RSA コプロセッサとマスク ROM、RAM、FRAM といったデータおよびプログラムの格納部から構成されているし、Suica などに用いられている交通カードの場合には、交通カードの特性からより単純な構成・メモリサイズが取られている。図 4.4-1 のように、IC カード自体が DES, RSA 等のコプロセッサなど高度な演算機能を有していれば、PKI などセキュリティに関してより上位の機能を持たせたデバイスとして用いることが可能になる。



チップ	MB94R211/R216
CPU	32bit(FR65Eコア)
最大動作周波数	13.56MHz
ROM	96/128KBマスクROM
RAM	4/8KB
FRAM	32/64KB
暗号回路	DES, RSA
ICカードI/F	非接触/接触 (T=0,1,CL)

図 4.4-1　IC カード構成例

§ FRAM: Ferroelectric Random Access Memory 強誘電体ランダムアクセスメモリ

ICカードはまた、耐タンパ装置の代表ともいえる。耐タンパ性とは、薬の瓶のキャップのように、物理的な破壊や非可逆的な操作を加えない限り、中身にアクセスできないような措置がとられていることを意味する。ICカードなどの耐タンパ装置の場合は、装置の内部のメモリなどの情報に、解体やクロックの低速化などの方法で物理的にアクセスしようとすると、データが破壊されたりロックされて使用不能になったするといった様々な安全策が取られている。また電力解析攻撃といった新たに発見された攻撃手法に対しても、内部格納情報の乱数化といった方法によってこれに対処している。

ICカードのソフトウェアアーキテクチャに関しては、従来の単機能カードから、1枚のカードで複数のサービスを実現するマルチアプリケーション化へと進みつつある。図4.4-2に示すJava Card[1]およびGlobal Platform[2]の組合せも、マルチアプリケーションICカードにおけるオープンスタンダードとして、世界のICカードベンダーで積極的に検討が進められているものである。Java Cardはマルチアプリケーション実行環境のひとつであり、Java言語によるAppletの開発や、カード発行後のAppletの追加・削除が可能である。またGlobalPlatform仕様はマルチアプリケーションICカードの管理機能を定義・標準化し、複数のアプリケーションプロバイダが互いにセキュリティを保ちつつ一枚のカードを共有することを可能にする。

GlobalPlatformに限らず、実際のICカードの運用においては、さらに、カード発行者、サービス提供者などのシステムに関わる様々な組織や運用者等のプレイヤーモデルについても考えておく必要がある。すなわち、「そのカードは誰が発行し、そのカードにインストールされるサービスは誰がどのように信認し、そのサービスを利用するにあたっては誰のどのような権限に基づいてアクセス権が付与されるか」といったICカードの発行からサービス利用に至るまでの情報の流れの管理運用が必要となる。このような管理運用やプレイヤーモデルについては、NICSSフレームワーク[3]においても議論が進められている。

ここで第一に重要なことは、プレイヤーモデルやプレイヤー間での情報交換におけるユーザのプライバシー管理の側面である。運用システムの構築にあたり、プレイヤー間の情

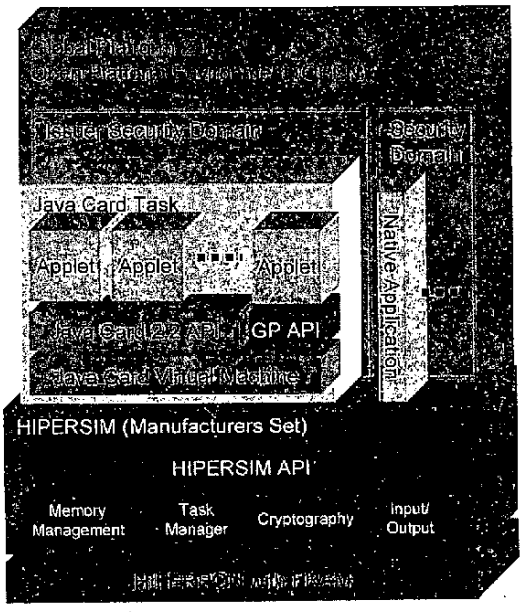


図4.4-2　マルチアプリケーションICカードのソフトウェアアーキテクチャ構成例

報管理モデルとしてプライバシ保護に関するモデル・理解・運用が十分でない場合、一般論としてのフレームワークには問題がなくても、ユーザのプライバシー情報がすべてサーバ側で管理されるようなモデルが用いられてしまう可能性を無視することはできない。

第二に重要なことは、ICカードのような耐タンパ装置を用いてユビキタス情報環境を利用するにあたっての個体認証の位置づけである。ユビキタス情報環境の利用において、必ずしも個体認証に相当するものが必要であるかどうかは議論の分かれるところである。たとえば、PKIは誰もが公開鍵と秘密鍵の対を持っている状態を作ることを目的にした社会インフラである。そしてPKIの認証は、暗号鍵とそれを所持する主体の固有名との対応を保証することに基づいている。つまり、暗号鍵と対応した名前空間の権威機関による厳密な管理が本質である。しかし、ユビキタス情報環境において、固有名が認証に必須のものであるかどうかは自明ではない。多くの場合には、「いまそこにいるその人」で十分なのである。自動改札を通過する人の固有名が誰かなどということは実用上必須の要件ではなく、どこで乗車した人かという属性が信頼できることだけが重要なのである。すなわち、PKIでも実際の応用システムで本当に重要なのは、個体認証ではなくて実は属性認証の方である。図 4.4-3 は、個体認証、属性認証、その上のサービス利用ポリシーの認証という3段階での管理機構を模式的に表したものである。サービスの提供においては、図 4.4-3 の二層目の証明書と三層目のポリシー証明書とによって適切なロールが割り付けられればそれでよいということができる。

別の言い方をすれば、個体認証は個人が持つ多数の属性を一つに統合するための中心としての役割を持っているものと考えることができる。初期のX.509標準に基づくPKIは、歴史的にはX.500ディレクトリシステムの一部として設計されたが、現在でも、ディレクトリに登録された多数の属性情報の一つとして個人認証のためのデジタル証明書があるというモデルが最も基本的で自然なものであると言える。プライバシー保護という視点に立てばまず図 4.4-3 の一層目と二層目を分離することが重要といえる。耐タンパデバイスが普及したユビキタス情報社会では、耐タンパデバイスの中に属性情報を入れて持ち歩き、必要に応じてそれを適切な相手のみに属性情報に応じた計算能力を示すことが可能である。

第三に重要なことは、複数の属性を統合するアイデンティティになるものとして耐タン

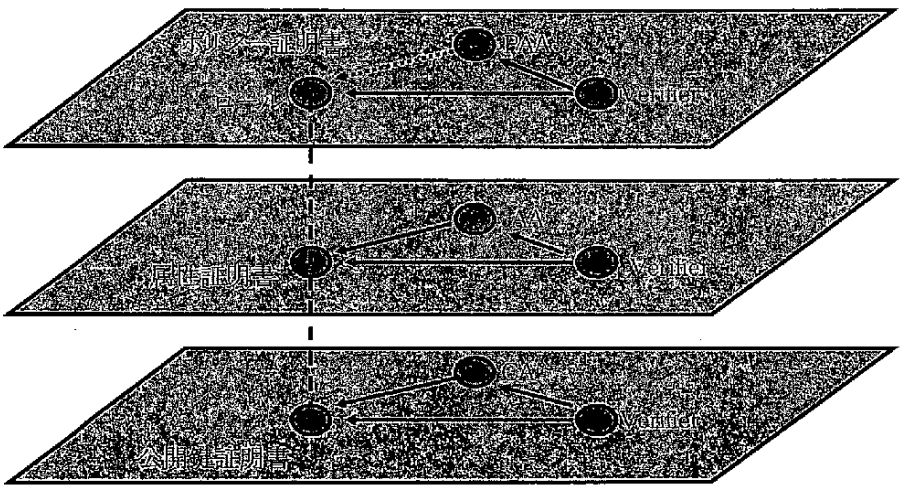


図 4.4-3　認証の S3A モデル[4]

パデバイスという物理的存在を不用意に用いれば、たとえこれが固有名の名前空間の管理とは分離されていても名寄せの問題が生じえるということである。したがって、ICカードを用いるフレームワークの運用においては、これを注意深く実施するか、図 4.4-3 の二層目の属性と三層目のポリシとの組合せによるロールの割付とがサービス毎に分離することが好ましいといえる。また役割割り当てのロジックは、プライバシーの流出を最小限にするという意味でもサーバ側ではなくユーザに近い IC カードの中で行うことが望ましい。実際、そのような運用は、プライバシー保護におけるオプトイン・オプトアウトといった考え方との整合性も高いと考えられる。

ICカードの利用は、ICカード自体の性能向上にマルチアプリケーション実運用の開始、USIM との連携による携帯電話との連携など、今後ますます身近なものになっていくと考えられる。また IC カード自体が持つセキュリティ能力やそこで用いられているアーキテクチャおよびフレームワークは、それ自体でプライバシー保護と本来的には矛盾しないものである。その意味からも、今後は IC カードの運用とプライバシー保護との整合性とがより重要になっていくと考えられる。

【参考文献】

〔1〕 Java Card, http://java.sun.com/products/javacard/
〔2〕 GlobalPlatform, http://www.globalplatform.org/
〔3〕 NICSS, http://www.nicss.gr.jp/
〔4〕 山崎重一郎、荒木啓二郎, "信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案",情報処理学会ジャーナル Vol.40 No.01, 2001, http://www.ipsj.or.jp/members/Journal/Jpn/4001/article032.html

4．5　情報家電ネットワークのセキュリティ／プライバシー

ブロードバンドネットワークの急激な普及により、ユビキタスネットワーク環境が真実味を帯びてきた。従来、パソコンだけがネットワークの利便性を享受してきたわけだが、ブロードバンドの普及によるユビキタスネットワーク環境が整うにつれ、パソコンではないテレビに代表される AV 機器やエアコン等白物家電（情報家電）をホームネットワークに接続し、新しい機能サービスを提供しようという動きが急速に進んでいる。特にこの新しい機能では、Peer to Peer 接続による直接通信を基本としている。

ネットワーク（インターネット）に接続するということは、パソコン同様ハッキング／クラッキングの危険性にさらされることにも繋がる。一般的に、このようなハッキング／クラッキング対策にはファイヤウォールや暗号化等のソフトウェア技術で対抗することになるのがだが、これらソフトウェア技術には多大な CPU パワーを必要としている。コスト的要求が厳しい情報家電はパソコンのように潤沢なパワーを有する CPU を使用できるわけではない。しかしながら、セキュリティやプライバシーの観点から考えると生活に密着している情報家電の方が、パソコンより高いレベルのセキュリティやプライバシー保護を要求されるのである。例えば、エアコンがネットワーク接続されたことを考えてみる。エアコンがネットワークに接続されると、会社から帰る時にネットワーク経由でスイッチ

を入れておき、帰り着いたころには暖かいまたは涼しい部屋になっている等の便利な機能を容易に想像することができる。しかし、もしこのエアコンがクラックされ、外部から自由に温度設定を変更できるようにされてしまう事態に陥ると、部屋の温度を極端に変えることが可能となる。結果、就寝中に温度を下げられてしまい、風邪を引かせてしまう等のPL 事故を引き起こしかねない。特に、乳児や幼児の場合はより深刻な事態になる可能性がある。情報家電では、潤沢な CPU パワーなしに、パソコンより高いレベルのセキュリティ／プラバシー保護機能を実現するという背反した問題を解決する必要に迫られている。

一方で、ネットワークに接続して提供される新しい機能やサービスは簡便性が必要とされる。一般的に、セキュリティレベルを上げようとすると手順が煩雑になるが、便利な機能やサービスを使うために複雑な手順を踏まねばならないようでは、便利なネットワーク機能の意味がなくなってしまう。情報家電はここでも、高いセキュリティと簡便性という背反する問題を解決しなければならない。

本節では、情報家電のネットワーク化のときに解決しなければならない、CPU パワーが弱くても、簡便性もあり、しかも高いレベルのセキュリティ／プラバシー保護機能をどのように実現するかを検討する。

４．５．１　ホームネットワークの構造の検討

ここでは、ホームネットワークの構造を工夫することにより、情報家電に適したセキュリティ／プライバシー保護を実現する方法を検討する。

一般的なホームネットワークは、ホームゲートウェイ（ルータ）を介してインターネットに接続される。このホームゲートウェイがホームネットワークを制御する。従来のホームゲートウェイは、ホームネットワークを一つのサブネットとして、インターネットに接続する。パソコンの延長線上として情報家電を考えると、このサブネットに情報家電を接続することになる。同じサブネットに接続されるということはネットワーク上パソコンと同様に扱われることを意味し、同様のセキュリティ機能を要求されてしまう。これは、限られた CPU パワーしか持たない情報家電では問題となってしまう。

そこで、ホームネットワークを３つの仮想的なサブネットに分類する。それぞれのサブネットに接続される機器は、その機器の特徴により接続されるサブネットを決定される。サブネットＡは、パソコンが接続されるサブネットで従来のホームネットワークがこれに当たる。サブネット B は情報家電用のサブネットで、自分自身で自分を守ることが困難なデバイス用のサブネットである。サブネット C はゲーム機用のサブネットで、ファイヤウォールがあると接続性が損なわれてしまうような機器で、クラックされても大きな事故に到らないようなデバイス用のサブネットである。

図 4.5-1 は、情報家電を接続するためホームネットワークの構造を示したものである。この図は、PDA を使ってユビキタス情報環境下にあるインターネット経由で家庭に接続し制御することを示している。

図 4.5-1 中にある経路①は、PDA から、サブネット A 上にあるパソコンにアクセスしていることを示している。このとき①はセキュリティ上の観点から暗号化（VPN）される。VPN は PDA とパソコンの間で直接接続されることを示している。このサブネットは、ホ

ームゲートウェイ上のファイヤウォールで守られているが、特定のポートを介してリモート機器（例では PDA）とサブネット A 上の機器（例ではパソコン）が直接通信することができる。

経路②は、PDA からサブネット B 上にあるエアコンをコントロールすることを示している。しかし、エアコンはセキュリティ機能を持たないので VPN は PDA とホームゲートウェイ間で接続され、ホームゲートウェイで VPN を終端する。サブネット B 上は平文の通信が行われる。ホームゲートウェイが暗号処理を肩代わりすることで、情報家電は暗号処理を行う必要がなくなる。このサブネットは、ホームゲートウェイで完全に守られており、ホームゲートウェイと認証しない通信を行うことが出来ない。

サブネット C はインターネットとトランスペアレントなサブネットとなっていて、経路③にはまったくファイヤウォールを適用しない。基本的にこのサブネットは不特定なポートを多用するゲーム機用のサブネットとなっている。

このようにサブネットを分類し、それぞれの機器の要求仕様に合ったサブネットに接続することで、ネットワークを構成する機器に応じたセキュリティレベルを提供することができる。特に情報家電用のサブネット（サブネット B）では、ホームゲートウェイがまとめて保護することにより、情報家電それぞれがセキュリティ機能を持つ必要がなくなり、セキュリティにかけるコストを軽減する。

4．5．2　Visible Internet を使うことによるセキュリティ／プライバシー保護の検討

現在のインターネットは、悪人を取り締まることが困難な（トレースができない）無法地帯ネットワークである。一方、ブロードバンドと無線技術が成熟してきたことにより、より多くのホームネットワークがインターネットに接続されるようになってきた。当然ながら、無法地帯ネットワークに接続するわけなので、セキュリティやプライバシー保護が必要とされる。セキュリティやプライバシー保護技術はもっぱら接続する側（ホームネットワーク側）で、ファイヤウォールや VPN と言ったセキュリティ機能を実装することになり、自分自身を守るために多大な費用をかけることになる。しかしながら、セキュリテ

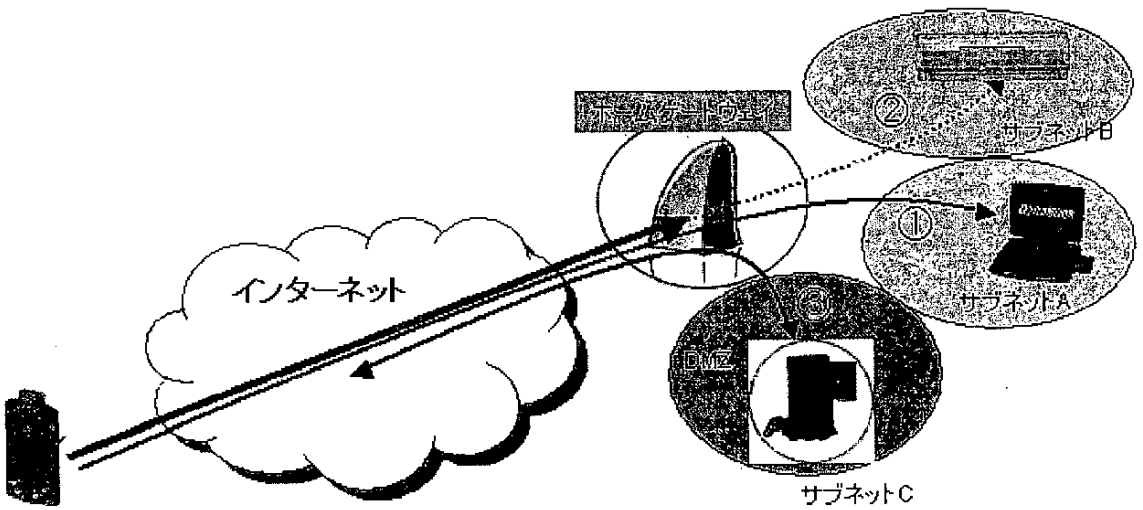


図 4.5-1　ホームネットワークの構造

ィ技術というのは完璧な物などなく、機能強化とクラッキングのイタチゴッコとなる。企業ネットワークならば、頻繁にセキュリティ機能をアップデートできるがホームユースの場合、機器は安価であることが要求されるため、機能的にも高いセキュリティ技術を実装できるわけでもなく、頻繁にアップデートすることもできない。Visible インターネットは、無法地帯ネットワーク接続に要求されているセキュリティ機能の実装を軽減することを目的としている。

図 4.5-2 は、Visible インターネットの構成である。

Visible インターネットでは、アクセスする際、オーソライズされたデバイスのみが参加できるよう、各接続ポイント（ISP）で認証を行う。これは現在の PPP のようにルータで終端されるようなものではなく、接続するデバイス自身を認証する。

ISP 側の機器には比較的多額なコストをかけられること、アップデートも容易であろうから、セキュリティのイタチゴッコにも対応できると考えられる。Visible インターネットでは不測の事態の場合、トレース可能な技術も提供する。トレーサブルにすることにより、犯罪の抑止力とする。

Visible インターネットにアクセスしているデバイスはオーソライズされたデバイスのみで、悪人は基本的に排除されている。よって極端なことを言えば、ファイヤウォールを適用する必要がない。

インターネット自身を Visible にすることで、それに接続されるデバイスに要求されるセキュリティ機能を軽減し、トータルのコストを軽減することが可能となる。

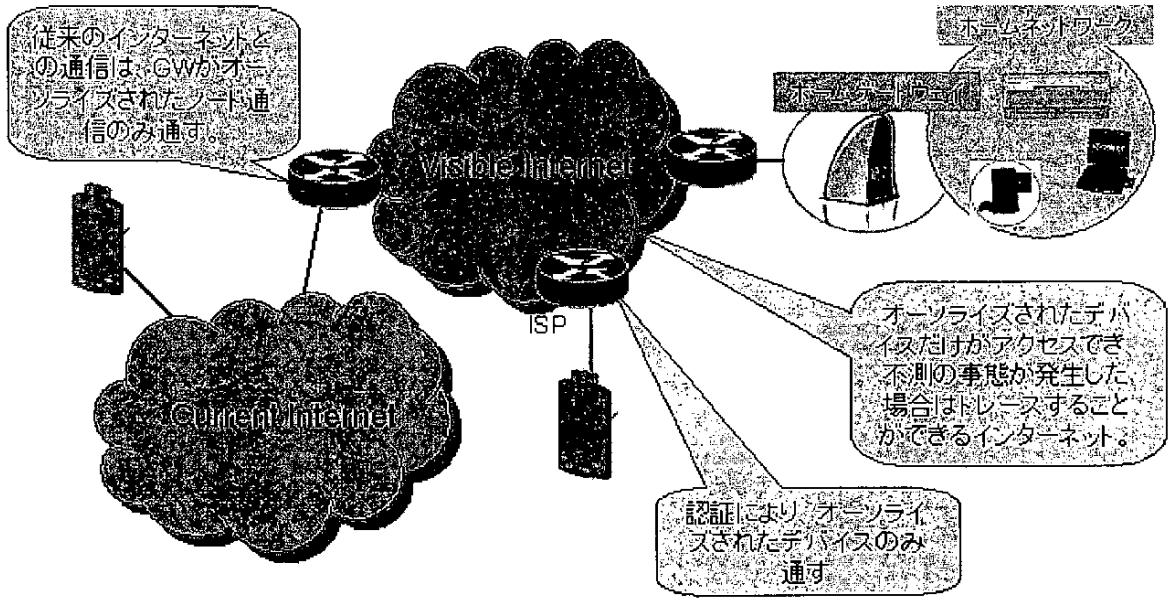


図 4.5-2　Visible Internet の構成図

５．セキュリティ／プライバシー保護に関する制度

５．１　ユビキタス情報社会におけるセキュリティ／プライバシー保護の重要性

インターネット環境の広がりにさらに拍車をかけるブロードバンド環境の浸透により、オンライン上を行き交う様々な情報フローは従来に比べて格段に加速されることとなった。つまり従来からの電子商取引を含めた物やサービスの売買といったオンライン上の経済活動、それに企業や個人間のデータ交換等に加えて個人間同士のデータ通信にいたるまで、あらゆる通信手段・媒体を通しての相互コミュニケーションが容易になってきた。

こういった行為が安全かつ安心に実現するためには、ハッカー・コンピュータウイルス対策等の在り方を含めて情報が漏洩したり改ざんされたりしないという、ネットワーク上の最も基本的なインフラであるセキュリティ･プライバシーが確保されなければならない。

このようなブロードバンド化による常時接続、IPv6の進展と情報家電を核にした本格的なユビキタス情報社会においてそのセキュリティ･プライバシー保護は、各セキュリティ評価基準の在り方及び暗号・認証問題についての対応を含めて、社会インフラの確保としての根本的な要求課題として急浮上してきている。

５．１．１　ネットワーク社会とセキュリティ／プライバシー保護

ネットワーク社会を考察する中で、インターネット上での匿名性は一見して端末操作者同志の間では保持されているように思われる。例えば電子掲示板の書き込み・ニックネームを使ったメールのやり取り等、通常の端末操作では個人と特定するのは困難である。

また、現状のシステム構築の主流となっているクライアントサーバシステムでは、クライアント権限は当然のことながら限定されている。一方サーバ（管理者）側においては、詳細なアクセスログ情報やクッキーによるブラウザ情報を含めて個人を特定でき個人をプロファイルできる情報が大量に蓄積されることになる。

つまり、一昔前のホストコンピュータとスレーブ端末のように極端ではないにせよ、ネット上においてはホスト・サーバ（管理者）側の権限は強大であり、そこに集積されるクライアント側の情報は様々な利用方法が考えられると同時に、この貴重な情報を如何に安全管理していくかというセキュリティ･プライバシー保護が喫緊の課題となる。

とくにユビキタス環境下におけるビッグブラザー（影の支配者）の存在は、もしそれが現実となれば、その懸念が最初に示された過去の場面よりも圧倒的に深刻な状況にあることは論を待たない。

５．１．２　ネットワーク社会に求められるセキュリティ／プライバシー要件

このようにネットワーク社会での流通情報の特徴を挙げると、一つにデジタルデータとしての特性（収集･保管・加工･抽出の容易さ）、二つ目に情報の保持の偏重性（サーバ側への偏り・クライアント側からの無意識提供情報の存在等）が該当する。

そしてこれらネット情報の保護要件としては、インターネット上のクライアント端末間

同士のプライバシー・匿名性の維持およびデジタルデータが故の大量・一括・瞬時漏洩の防止・安全管理、それに大量保有情報の収集・利用時における提供者（情報主体）への告知義務・同意取得・透明性の維持等に対する対策がポイントになってくる。

とくに、ユビキタス情報社会においては、IPv6 をはじめ、至る所にネット情報のフロー窓口が存在し、情報分類でも単純な個人属性情報だけでなく、信用・資産情報並びに個人のロケーション・位置情報さらにハイリーセンシティブな健康・医療情報がネットワーク上を流通する世の中となる事が、上記の要件をさらに厳格化させるニーズがでてくる所以である。

5．1．3　ネットワーク社会に求められるセキュリティ／プライバシー保護責任

まずプライバシー・セキュリティ保護の観点からのネット社会に求められる責任問題として、オンライン上のプライバシー・匿名性の維持責任がある。技術的な対応策は 4 章、7 章に譲るとして制度・インフラ観点からの内容としては、この壮大なインターネット上のクラインアント同士（ピア 2 ピア）の関係における最大の保護要件であり、この保護責任がどこに存するかが論点となるであろう。

一般的にはシステムインフラの情報セキュリティ保護を含めてサーバ（管理者）側ないしはどのようなシステム導入を選択するかを含めてプロバイダー側にあるといっていい。しかし、ネットワーク社会に生きる我々ネチズン（ネットワーク市民）にとっては、ネチケット（ネットワークエチケット）として個人情報も含めて自己情報コントロール権があると解釈されるケースがある。

つまり、最低限、自分の情報が外部に提供されると推定できる場合には、その範囲・レベル・頻度等につき、自己の可能な限りはこれをコントロールする意思と自己防衛手段を持たねばならない。

具体的には、ネチズンとして個人情報提供時の範囲・レベル判断やその提供によって得られるメリットとデメリットの判断（例：オンラインショッピング時の買い物カゴの使用・不使用等）を下す必要がいろいろな場面で発生してくる状況が挙げられる。また民間の自主規制の一環として、個人情報保護や消費者保護をアピールするマーク制度等（詳細後述）もこれらをサポートする有効なインフラの一つであろう。

5．2　セキュリティ／プライバシー保護制度の現状

まず関連する政府全体の現状取組としては、2001 年 1 月施行の「IT 基本法」があり、高度情報ネットワーク社会の形成に関する施策の推進とこれにあたっての基本理念・方針を定めている。これに基づき、日本における国家戦略としての「e-Japan 戦略」を具体化した施策の全容として「e-Japan 重点計画」策定があり、これの施策反映のため「e-Japan2002 プログラム」が公表されている。また法規制の現状としては遡って 1988 年に行政機関を対象とした個人情報保護法を制定しているほか、通産省（1997 年）を皮切りに、民間部門を対象とした各官庁毎の個人情報保護ガイドラインの策定が行われている。

また民間の自主規制の一環としては、この省庁ガイドラインをベースにした各業界団体毎の個人情報保護ガイドラインの策定が挙げられる。日本工業規格としては 1999 年

JISQ15001を制定してこれを基準としたプライバシーマーク制度の運用をJIPDEC((財)日本情報処理開発協会)が開始しているが、さらなるネットワーク化の進展に伴い、民間部門における個人情報保護を強化するため、現在審議中の個人情報保護法案を含めた法的

表5.2-1　セキュリティ関連法律／ガイドライン／政策一覧

区　分	名　称	担当組織	概　要	URL
法律	高度情報通信ネットワーク社会形成基本法（IT基本法）	高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）	2001年1月6日 施行	http://www.kantei.go.jp/jp/it/kihonhou/honbun.html
	電子署名及び認証業務に関する法律（電子署名法）	総務省 経済産業省 法務省	2001年4月1日 施行	http://www.meti.go.jp/policy/netsecurity/digitalsign.htm
ガイドライン／政策	情報通信ネットワーク安全・信頼性規準	総務省 郵政事業庁	2000年6月18日 ハッカー対策など追加 2001年2月21日 危機管理政策追加	http://www.radio-operators.net/telecom/nwanzen1.html
	セキュリティポリシーに関するガイドライン	内閣安全保障・危機管理室 情報セキュリティ対策推進室	2000年7月18日発表 2000年12月に各省庁毎のセキュリティポリシー策定の予定	http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
	重要インフラのサイバーテロ対策に係る特別行動計画	内閣安全保障・危機管理室 情報セキュリティ対策推進室	2000年12月15日発表	http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/1215actionplan.html
	e-Japan重点計画	高度情報通信ネットワーク社会推進戦略本部	2001年3月29日 発表	http://www.kantei.go.jp/jp/it/network/dai3/jyuten/index.html

出典元：IPAセキュリティセンター（IPA/ISEC）

表5.2-2　「e-Japan2002プログラム」で示されたセキュリティ関連の重点施策項目

重点施策項目	概要	担当省庁
信頼性の高い「電子政府」の構築	電子政府における情報セキュリティに関する支援、評価・監査、緊急対応を行う体制の検討	内閣官房
	セキュリティポリシーの継続的な評価・見直し手法の検討	内閣官房
	地方公共団体の情報セキュリティ支援	総務省
サイバーテロ対策の強化	情報共有のためのデータベースの構築・機能強化 人材育成 体制整備 国際連携	内閣官房、警察庁、防衛庁、金融庁、総務省、経済産業省、国土交通省
情報セキュリティの意識の向上	民間イニシアチブ連携のための枠組みの整備 人材育成プログラム支援	総務省、文部科学省、厚生労働省、経済産業省
民間部門における情報セキュリティ対策への支援	民間への情報提供・受入・指導助言機能の強化 相談受付業務の充実 ハイテク犯罪対策のための体制強化	警察庁、総務省、経済産業省
	普及啓発活動および情報セキュリティ対策促進のための支援	総務省、経済産業省
情報セキュリティに係る基盤技術の開発	基盤技術の開発および政府他部門・民間への公開	警察庁、防衛庁、総務省、文部科学省、経済産業省

出典元：IPAセキュリティセンター（IPA/ISEC）

な規制の導入、及びマネジメント／技術の両面にわたる個人情報保護対策の更なる強化が必須である。

次にセキュリティの保護に関しては、評価基準・規格の整備と言う観点から、マネジメント規格面ではISO／IEC17799をベースとした2002年JISX5080の制定、また情報技術を用いた製品評価面ではISO15408（JISX5070：2000年7月）の本格導入が行われている。また、法規制の面では、後述の刑法改正をふくめて、営業機密保護については不正競争防止法、それに不正アクセス禁止法がすでに施行されている。

5.2.1　現行セキュリティ／プライバシー制度の脆弱性

まず、プライバシー・個人情報保護の現行制度上の施策的脆弱性としては、民間分野を総括的に保護する法規制が現時点では全く行われていない事が最大のポイントである。

前述のように、行政機関の保有する個人情報については1988年に個人情報保護法が成立しているが、民間企業・事業者が保有する情報について規制する法律が無いことが、現状の日本における個人情報保護の後進性を際立たせる格好となっている。

またセキュリティ上の観点からも、現行の不正アクセス禁止法の適用要件は、オンラインネットワーク上での不正アクセスに限られている点（つまりスタンドアロンへの不正アクセスは対象外）、またその対象パソコン等にアクセス権が設定されていることが要件となっている点である。つまりネットワークに接続されていないアクセス制限の無いパソコン等から情報窃盗する場合は対象外となっている。

そしてウイルス対策一つをとっても、不正プログラムを作成する行為自身は罪にならずに、それによって何らかの実害が出て初めて不法行為で訴えられることになるのが現状である。

とくに1987年には刑法が改正され、電磁的記録不正作出罪、電子計算機損壊等による業務妨害罪が規定されたが、この改正によっても、データの不正取得及びコンピュータの不正使用の形態をとっている不正アクセス、発病前の段階のコンピュータウイルス投与行為・配布・転送については犯罪は成立しない。

5.2.2　セキュリティ／プライバシー保護に関する取組みの現状と問題点

はじめに民間分野をカバーする個人情報保護法の現状であるが、1999年の11月に政府の個人情報保護部会による「わが国における個人情報保護システムついての中間報告」が出されて、法制化の提言と共に個別法の検討また民間自主規制の推進について提案がなされた。

また2000年の5月には個人情報保護法制化専門委員会による「個人情報保護基本法制に関する大綱案」がまとめられ、これを内閣に提出して大綱として決定して、国会に上程したが未だ野党及びマスコミ等の反対によって成立はしていない。

現状としては2002年末に一旦廃案として、2003年の通常国会に下記内容の修正を行って成立を目指している。

表 5.2-3　個人情報保護法の比較

国　名	法律・ガイドラインの名称	対象及び範囲	収集規制	利用提供規制	適正管理	開示請求権	国外提供規制	罰則	損害賠償	監督機関
日本	個人情報保護基本法制に関する大綱[3]	公的および民間部門	○	○	○	○		○		主務省庁
	行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律	公的部門		○	○	○				総務庁（現総務省統計局）
	民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン	民間部門	○	○	○	○				通産省（現経済産業省）
	電気通信事業における個人情報保護に関するガイドライン	通信業界	○	○	○	○				郵政省（現総務省）
OECD	プライバシー保護と個人データの国際流通についてのガイドライン[4]	公的および私的部門	○	○	○	○	○			
EU	個人データ処理に係る個人情報保護及び当該データの自由な移動に関する欧州議会及び理事会の指令[5]	公的および私的部門	○	○	○	○	○	○		公共機関
米国、EU	セーフハーバー原則[6]	私的部門中心	○	○	○	○				
国際連合	個人データおよびファイルに関するガイドライン[7]	公的および私的部門	○	○	○	○	○	○	○	公平独立な機関
スウェーデン	データ法	公的及び民間部門	○	○	○		○	○	○	データ検査委員会
アメリカ	プライバシ法	公的部門	○	○	○			○	○	大統領府 行政管理予算庁
ドイツ	連邦データ保護法	公的及び民間部門		○	○		○	○		データ保護受託官
ノルウェー	個人データ保護法	公的及び民間部門	○		○			○		データ監視局
オーストリア	データ保護法	公的及び民間部門			○			○		データ保護委員会
オーストラリア	プライバシ法	公的及び民間部門			○			○	○	プライバシコミッショナー
ルクセンブルグ	電子計算機処理に係る個人データ利用規制法	公的及び民間部門	○		○			○		諮問委員会および主務大臣
フランス	データ処理、データファイル及び個人の諸自由に関する法律	公的及び民間部門	○	○	○		○	○		情報の処理と自由に関する国家委員会
イギリス	データ保護法	公的及び民間部門	○	○	○			○	○	データ保護登録官
カナダ	プライバシ法	公的部門			○			○		プライバシコミッショナー
韓国	公共機関における個人情報保護に関する法律	公的部門	○	○	○			○		個人情報保護審議委員会

出典元：IPA セキュリティセンター（IPA/ISEC）

①５つの「基本原則」の削除
②主務大臣の勧告・命令は、表現の自由等を「妨げてはならない」と明確に表現
③報道機関への情報提供者は、主務大臣の勧告・命令権が及ばないと明記
④義務規定の除外対象に「個人」を明記し、フリージャーナリストらを加える
⑤義務規定の除外対象に「著述を業として行う者」として作家を加える
※行政機関対象分...秘密にあたる個人情報を職権乱用により収集した場合や外部提供についての罰則を規定

この法案が成立すれば、現状では、実質野放し状態における「情報窃盗」そのものを罪として直罰可能な法規制が確立するという画期的な個人情報保護環境が生まれる。

次にセキュリティ関連の取組施策についてであるが、従来から大きく分けて下記のような内容がポイントになる項目である。

①ハッカー・コンピュータウイルス等不正アクセス対策のあり方
②暗号・認証問題についての対応
③電子計算機システム安全対策基準
④セキュリティ評価基準

まず①ハッカー・コンピュータウイルス等不正アクセス対策についての取組経過であるが、1995年7月の「コンピュータウイルス対策基準」の改訂実施がある。(以下通商産業省の「セキュリティ・プライバシー問題検討委員会報告書」資料より一部関連個所を抜粋)

(1)「コンピュータウイルス対策基準の見直し」

ネットワーク化の進展、クライアント／サーバ（以下 C／S）システム・アウトソーシングの普及等を考慮して、基準の適用範囲を 拡大することとし、基準の構成を以前の「ユーザー基準」「システム管理者基準」「ソフトウエア開発管理者基準」の３つの基準から「システムユーザー基準」「システム管理者基準」「ソフトウエア供給者基準」「ネットワーク事業者基準」「システムサービス事業者基準」の５つの基準とした。

表 5.2-4　コンピュータウイルスに関する法律の比較

国名	日本	米国	英国	イタリア	中国
法律の名称	刑法234条の2 「電子計算機損壊等業務妨害」	合衆国連邦法1030条 コンピュータと関係する詐欺及び関連行為	1990年 コンピュータ不正使用法	刑法典 615条 コンピュータシステムの損壊または中断を目的とするプログラムの配布	コンピュータ情報システム安全保護条例
ウイルスの投入		○			○
ウイルスの配布 転送 流布				○	○
ウイルスによる妨害行為	○	○	○	○	○
ウイルスによる破壊行為	○	○	○		○
罰則	5年以下の懲役 または 百万円以下の罰金	重罪かどうかによって、18編 「犯罪及び刑事手続」の定める罰金若しくは20年を超えない拘禁刑又はその併科、 または罰金若しくは20年を超えない拘禁刑又はその併科	5年以下の拘禁刑 もしくは無制限の罰金	2年以下の懲役 または2千万リラ以下の罰金	個人ごとに5千元以下の罰金、 部門ごとに15千元以下の罰金

出典元：IPA セキュリティセンター（IPA/ISEC）

さらに、C／S システム等においては非専門家であるエンドユーザコンピューティングが重要となるため、米国の NIST（National Institute of Standards and Technology）のガイドラインから、ユーザ管理として重要な対策項目として、「監査、監視」及び「ユーザ教育と啓蒙普及」の観点を取り込むこととした。

これらは従来からの「情報システム安全対策基準」・「システム監査基準」に加えて機密情報の保護・漏洩対策及び保持・検出機能による措置がまとめられている。

（2）不正アクセス被害届出制度等の創設

わが国では、コンピュータウイルス被害を対象とした届け出制度は実施に加えて、不正アクセス（ハッキング）について、IPA（情報処理振興事業協会）において以下の内容の不正アクセス届出制度を開始。

a.不正アクセス被害届出制度の概要（実施機関：IPA）

・被害届け出の対象：不正アクセスによる被害を受けた法人及び個人

・届け出の内容分析・公表：被害を受けたシステムの構成、ハッカーの侵入経路、被害状況、実施していたセキュリティ対策等の分析・公表。

b.不正アクセス対策基準の策定（1996 年 8 月）

コンピュータウイルスに対する予防、検知、事後対応等について、ユーザがとるべき対応策を取りまとめた基準に加えて、不正アクセスからの予防、事後対応等についての対応策をまとめた「不正アクセス対策基準」を策定。

c.不正アクセス禁止法（2000 年 2 月施行）

同法では不正アクセス行為（無権限使用・無権限アクセス・コンピュータ侵入等）を禁止してその違反に対しては罰則（一年以下の懲役または 50 万円以下の罰金）を

表 5.2-5　不正アクセスに関する法律の比較

名	法律の名国称	対象及び範囲	処罰の対象となる不正行為								罰則
			接続のみ	無権限アクセス	コンピュータ侵入	サービスの妨害	不正使用	サービスの窃盗	助長行為	個人情報の探査行為	
日本	不正アクセス行為の禁止等に関する法律	電気通信回線に接続している電子計算機の電気通信回線を通じて行われる不正アクセス行為(1、2条)		○	○				○		・不正アクセス行為に対しての罰則が一年以下の懲役または50万円以下の罰金 ・助長行為に対しては罰則 30 万円以下の罰金
米国	合衆国連邦法 1030条 コンピュータと関係する詐欺及び関連行為	・金融機関若しくは合衆国政府が排他的に利用するコンピュータ ・州際取引又は外国との取引若しくは通信において利用されるコンピュータ(1030 条(e)項(2)号)		○	○	○	○	○			重罪かどうかによって、18 編「犯罪及び刑事手続」の定める罰金若しくは 20 年を超えない拘禁刑又はその併科、または罰金若しくは20 年を超えない拘禁刑又はその併科
	カリフォルニア州刑法典 502 条 コンピュータ、コンピュータシステムおよびコンピュータデータに対する無権限アクセス	州の範囲内にあって合法的にそのコンピュータ、コンピュータシステム及びコンピュータデータを利用しているすべての金融機関、企業、政府機関、その他の者(502 条(a)項)		○	○	○	○	○	○		罪状の大きさにより、10,000 ドル以下の罰金、16 ヶ月、2 年もしくは 3 年の州刑務所での懲役、または 5,000 ドル以下の罰金、1 年以下の郡刑務所内拘禁
	ウェストバージニア州刑法典 61 条 コンピュータ犯罪及び盗用法	州内における違反者、侵害された保有者、アクセスがなされた開始地、仕向地、または、経由地 (§ 61-3C-18)		○	○	○	○	○	○	○	最も重いもので、10,000 ドル以下の罰金、もしくは、10 年以下の懲役場内拘禁
	サウス・カロライナ州刑法典 16 条コンピュータ犯罪法	州内における違反行為および違反行為を構成したコンピュータ、コンピュータシステム、コンピュータネットワーク、または、その構成部分の保有者もしくは賃借人 (§ 16-16-30)	○	○	○	○	○	○	○		重罪の有罪判決の場合、125,000 ドル以下の罰金もしくは 10 年以上の拘禁刑

出典元：IPA セキュリティセンター（IPA/ISEC）

設けている。

また他人の ID を無断提供する等の不正アクセス行為を助長する行為についても禁止して違反罰則（30 万円以下の罰金）を課している。

次に②暗号・認証問題についての対応であるが、具体的に以下の施策が講じられた。

（３）暗号・認証技術に関する情報提供・調査研究

a.暗号・認証技術等の動向調査、啓蒙普及

・IPA において暗号アルゴリズム等に関する情報提供事業の実施に向けて体制を整備。

・具体的な項目（案）：機能、性能、強度、コスト負担、特許権の行使に関する制約情報、国内外の基礎的な暗号技術動向、等

b.暗号アルゴリズム等の研究開発の推進

・わが国の暗号・認証技術のレベルアップを図る観点から、平成７年度より、IPA に事務局を設置し、民間企業、大学等による暗号アルゴリズム等の研究開発を開始。

c.CRYPTREC：暗号技術評価委員会設置

・電子政府における暗号に関する利用方針の策定のため、当時の通産省事業として我が国の暗号技術を集結し、専門的・技術的見地から、暗号技術評価を実施（IPA に委託）。総務庁、防衛庁及び郵政省（当時）とも連携。

対象としては、共通鍵暗号（ブロック、ストリーム）、公開鍵暗号、ハッシュ等として暗号アルゴリズムの、Security, Flexibility, Efficiency 等について、具体的評価基準を定める。特徴として公募形式により広く透明に（外国暗号受け付けも含む）。

また ISO／IEC への対応として標準化について合意後、具体的中身につき国際標準には、我が国の暗号も採用へ働きかけ、また将来の技術開発については暗号モジュールの評価も視野にいれて取組み。

５．３　セキュリティ／プライバシー保護対策の在り方とその推進動向

まずプライバシー保護の観点からは、国際的に見ても EU（欧州連合）では、加盟国から域外第三国への個人情報の移転を禁止する旨の内容を盛り込んだ「個人データ処理に係る個人の保護に関する理事会指令」が発効しており我が国が EU より個人情報保護レベルが低いと認定されると欧州との商取引ができなくなる可能性もある。

また最近の個人情報の漏洩事件やスパムメールの横行それに名簿屋と称する個人情報売買／斡旋業の台頭を見るに付け、早い機会にこれらの規制を図らねばならない。このため、個人情報保護に必要な強化策を速やかに個人情報保護法の成立を含めて実施しつつ我が国として、民間部門における個人情報保護の在り方についてのさらなる自主規制・制度化を推進することが肝要である。

次にセキュリティ保護の観点からは、住民基本台帳法の改正を受けたクローズド環境からオープン環境への情報環境の劇的変化の進展を受けて、従来とは全く別な視点でのセキュリティ保護対策が必要となってきたことを肝に銘じなければならない。

5.3.1　セキュリティ／プライバシー保護対策の検討に際して考慮すべき事項

（1）プライバシー保護対策

まず国内のニーズとしては、前述のように個人情報の漏洩、改ざん、悪用といった危険性が増大している現在、わが国では、国の公的機関を対象とした個人情報保護法を制定しているほか、民間部門を対象とした個人情報保護ガイドラインを策定しているが、ネットワーク化の進展に伴い、民間部門における個人情報保護を強化するため、法的な規制の導入を含め、個人情報保護対策のさらなる強化が必要との指摘が強まっている。

また、次に国際的な背景として、前述のEUにおいては、域外第三国が十分なレベルの個人情報保護措置を講じていない場合には、加盟国から域外第三国への個人情報の移転を禁止する旨の内容を盛り込んだ「個人データ処理に係る個人の保護に関する理事会指令」を発令しており、わが国がEUより個人情報保護レベルが低いと認定される可能性もある。このため、個人情報保護のために必要な強化策を速やかに実施しつつ、わが国として、民間部門における個人情報保護のあり方についての保護体制を早急に固めることが必要である。

（2）民間事業者による自主的措置の充実

法制による個人情報の保護措置以外に、個人情報を扱う民間事業者による自主的措置（自主規制）を充実することにより、保護体制をかなりのレベルでアップすることが可能であると考えられる。このため、適切な個人情報保護措置をとっている事業者等に対して何らかの形で社会的なインセンティブを付与するべく、具体的に以下のような施策を講じた。

a.民間事業者による業界別ガイドライン・社内規定等の策定

業種ごとの民間事業者による個人情報保護についての社内規定等（コンプライアンス・プログラム：C／P）の策定の参考となる、各業界の実状に応じた各事業者団体のガイドライン（G／L）つくりを推進し、最終的には、G／L雛形を踏まえて、個々の民間事業者が独自のC／Pを策定することとなった。

b.認証・マーク付与制度の創設

民間事業者が個人情報保護対策を強化するインセンティブを付与するとともに、いかなる民間事業者が適切な個人情報保護を行っているかを個人消費者等が認識できるようにすることを目的として、個人情報の適切な保護対策を講じている民間事業者を第三者的に認証し、マーク付与等により一般に周知徹底する制度を創設。（プライバシーマーク制度）

具体的には、個人情報保護に関する一定の条件を満たしたC／P及び所要の当該C／Pの実効担保体制を策定・整備した個々の民間事業者に対し、実施している保護措置等のレベルに応じて、認証やマーク付与を行う。

c.電子計算機システム安全対策基準

情報システムのユーザが講じるべきセキュリティ対策を具体的にガイドラインとして取りまとめたものとして、以前「電子計算機システム安全対策基準」が策定、公表されていた。しかし、以前の基準については、集中処理型のシステムを想定しており、クライアント／サーバ分散処理型のシステムの進展という新たな技術環境に対応でき

表 5.3-1 機密情報漏洩に対するガイドラインの比較

国名	日本			イギリス
ガイドラインの名称	通産省 現経済産業省） 情報システム安全対策基準	通産省 現経済産業省） コンピュータウイルス対策基準	通産省 現経済産業省） システム監査基準	BS7799 情報セキュリティ管理実施規定
資産目録	情報システムの資源の機密度を区別する機能を設けること	ソフトウェア管理、コンピュータ管理		全ての重要な情報とIT資産の目録は保守されなければならない
情報の分類	データ等は、機密度及び重要度に応じて区分を設け管理計画を策定すること	管理体制の明確化		分類された情報に対する保護は、事業ニーズと一致し、システムからの出力に適切な名称を受けなければならない
データ取扱手順	情報漏洩を防止する機能を設けること	セキュリティ機能の利用	識別コード及びパスワードの管理、入力管理、データ管理、出力管理	機密データを取り扱うための手順が設定されなければならない
データ交換	集中、分散処理の形態に応じた管理計画を策定すること		データの交換は、不正防止及び機密保護の対策を講じているか	データの紛失、修正または誤用を防止するために、組織間のデータ及びソフトウェアの交換を制御しなければならない
機密システムの分離		機密情報を格納しているファイルの厳重管理	建物及び室への入退の管理は、不正防止及び機密保護の対策を講じているか	機密性の高いシステムは、専用のコンピュータ環境が必要である
データの暗号化	ファイル、伝送情報等を暗号化する機能を設けること			機密性の高いデータについては、暗号化を検討しなければならない
メッセージの検証	アクセス権限を制御する機能、アクセスを監視する機能を設けること			機密データの送信を行うアプリケーションについては、メッセージ検証システムが検討されなければならない

出典元：IPA セキュリティセンター（IPA/ISEC）

るよう基準の見直しを実施、その改定基準は、阪神大震災の震度７レベルの地震にも対応できるよう、地震対策関連項目の見直し、強化を図った。

さらに、「システム監査基準」についても、情報技術の進展、震災対策等の観点から、やはり見直しの必要性が指摘されている。

（３）セキュリティ評価基準

情報システムのセキュリティのレベルを客観的に評価するセキュリティ評価は、ユーザが情報システムや情報機器のセキュリティのレベルを把握することを可能とするものであり、ネットワーク化の進展に伴うハッカーやコンピュータウイルスのリスクの増大に対応する上で不可欠である。

a.取組み経過

わが国においてまずは、平成８年１月に出された Common Criteria 1.0 版に基づく評価の試行を重ね、セキュリティ評価を行うための手法を定めた、ガイドラインの最終版を平成９年に策定。

（４）評価認証制度の立ち上げ

（セキュリティ評価）→情報技術を用いた製品のセキュリティ規格

a.ISO 国際評価規格（ISO15408）

セキュリティ評価とは、ハードウェア／ソフトウェアのセキュリティに関するの品質確認を行うもの。先進諸国においては、政府調達の観点から、民間の評価機関及び公的な認証機関による評価認証スキームが確立。NATO（北大西洋条約機構）諸国中心に、そのスキーム及び利用について相互に合意。また、ISO においても国際規格化（ISO15408）。

このスキームは、セキュアなシステム構築に有効であるのみならず、今後の国際的なインターオペラビリティの確保のための技術的要素となる可能性。また、我が国の製品の国際マーケットでの競争力にも影響を与える懸念ありとの指摘あり。そのため、電子政府の構築にあわせて、我が国においてスキーム運営を開始し、その成果を電子政府における利用方針として活用。

なお、2002年には情報技術の観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されているかを評価するためのセキュリティ基準（ISO/IEC15408）に基づいて評価または認証された製品等を、すべての行政関連機関の物品及び役務調達において、可能な限り利用する事との指導がなされ、既に実施がはじまっている。

（セキュリティ管理）→組織運営のセキュリティ規格

b.情報セキュリティの国際標準「BS7799」と国内標準「ISMS適合性評価制度」

国際標準化動向としては、情報セキュリティ管理・運用に関する実践規範、またはガイドラインとして「BS7799」と「GMITS(Guidelines for the Management for IT Security : ISO/IEC TR 13335)」が注目されている。この中で「BS7799」は、すでに規格に基づく認証制度が確立されており、欧米では情報セキュリティ管理の規格として広く認知されている。BS7799の規格は2部で構成されており、第1部は「情報セキュリティ・マネジメント・システム(ISMS)の実施基準」、第2部は「情報セキュリティ・マネジメント・システムの仕様(認証システムを含む)」について記載されている。

このうち第1部は、2000年、国際標準化機構ISOと国際電気標準会議IECより、ISO化(ISO/IEC17799)され、国際標準となった。第2部は2003年末を目指して、ISO化進行中である。

国内では、経済産業省が公表した情報セキュリティ管理に関する国際標準の導入に基づき、（財）日本情報処理開発協会（JIPDEC）が2002年4月から本格運用を始めた、情報セキュリティ管理に関する適合性評価制度「ISMS適合性評価制度」がある。

この制度は、2001年3月をもって廃止された「情報処理サービス業情報システム安全対策実施事業所認定制度(安対制度)」に代る民間ベースの第三者認証制度として位置付けられている。

5．3．2　セキュリティ／プライバシー保護対策の実施に向けた考え方

ハッカー・コンピュータウイルス対策を効果的に実施していくためには、法律上の対応を行っていくことも重要である。このため、情報システムの完全性を確保するため、不正アクセス行為やコンピュータウイルス投与行為に対する罰則規定の制定、セキュリティ確保のために民間事業者に対する行政法的対応について検討を行うことが必要と考えられる。

表 5.3-2　電子署名法の内容（日本）

	日本
法律の名称	電子署名及び認証業務に関する法律案
法律の目的	この法律は、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度、その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とする(第一条)。
法律の対象及び範囲	－
ディジタル署名の定義	「電子署名」とは、電磁的記録(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。)に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものを言う。 (1)当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること (2)当該情報について改変が行われていないかどうかを確認することができるものであること
ディジタル署名の法的効果 文書の法的位置づけ (文書の成立の真実性、本人の同一性、文書の非改竄性の推定)	電磁的記録であって情報を表すために作成されたもの(公務員が職務上作成したものを除く。)は、当該電磁的記録に記録された情報について本人による電子署名(これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。)が行われているときは、真正に成立したものと推定する(第三条)。
認証機関の法的位置づけ	特定認証業務の認定(第三章)
認証機関の法的責任及び義務	・認定認証事業者は、主務省令で定めるところにより、その認定に係る業務に関する帳簿書類を作成し、これを保存しなければならない(第十一条) ・認定認証事業者は、その認定に係る業務の利用者の真偽の確認に際して知り得た情報を認定に係る業務の用に供する目的以外に使用してはならない(第十二条)。
その他特色等	利用者が認定認証事業者等に不実の証明をさせる行為について、3年以下の懲役又は200万円以下の罰則規定を設けている(第四十一条)。

出典元：IPA セキュリティセンター（IPA/ISEC）

５．３．３　セキュリティ／プライバシー保護対策の推進方策

暗号・認証技術が不可欠な要素となるエレクトロニック・コマース（電子商取引）を確立するためには 、電子データ署名等の法的位置づけ等、電子取引に係る法的環境の整備を図ることが必要である。

これらについては、電子署名に関して電磁的記録の真正な成立の推定、特定認証業務に関する認定制度、その他の必要な事項を定めた「電子署名および認証業務に関する法律」（2001 年 4 月施行）や電子契約法（民法の電子商取引に関する特則）及びこれに関する解釈指針としての準則の策定等が挙げられる。

５．３．４　国際連携の推進方向

IT セキュリティ評価・認証制度に係る国際相互承認への参加について 2002 年 6 月経済産業省及び独立行政法人製品評価技術基盤機構は、ISO/IEC15408(JISX5070)に基づく IT セキュリティ評価・認証制度について、その認証結果を相互に承認する国際相互承認スキームである CCRA（Common Criteria Recognition Arrangement）への参加表明を行い、本格的な準備を開始した。

（１）目的・背景

安全性及び信頼性の高い電子政府を構築するため、e-Japan 重点計画においては、政府部内における情報セキュリティ対策の一つとして「各省庁の調達におけるセキュリティ水準の高い製品等の利用方針」（2001 年 3 月 29 日行政情報化推進各省庁連絡会議了承）を踏まえた IT 関連製品の政府調達の実施を行うとともに、そのための情報セキュリティに

関する評価・認証基盤の整備を行う。このため、経済産業省は、独立行政法人製品評価技術基盤機構に本事業の委託を行い、2001年4月にITセキュリティ評価・認証制度を発足させた。

CCRAに参加することにより、本制度により評価・認証されたIT関連製品は、参加国間において評価・認証結果が同等であると認められる。このため、政府は調達に当たって、再度の評価を要求して技術レベルを確認することなくIT関連製品を早期にかつ安価に世界の市場から調達することができるようになる。

また、日本のITベンダー等にとっては、国内で評価・認証されたIT関連製品が参加国内において再度の評価を受けることなく市場に提供できるため、国際的な市場競争力の確保の観点からも有効である。

その他、国際連携の関連では、民間の自主規制（マーク制度等）の例として、個人情報保護の分野において、日本国内のプライバシーマーク制度（JIPDEC運営）と米国のBBB online（商事改善協会）の運営するプライバシー・シール（マーク）・プログラムとの間で相互乗り入れが実現し、両マークの間で相互認証が可能となっている。

6．ユビキタス情報環境におけるセキュリティ／プライバシーの脅威

6．1　セキュリティ／プライバシーに対する新しい脅威

6．1．1　ユビキタス情報システム検討のための簡単なモデル

本節では、ユビキタス情報システムのための簡単なシステムモデルを示し、4 章で述べたユビキタス情報社会におけるセキュリティとプライバシー問題の分析を行う。

人間やモノと、IT システム空間との接点となるデバイスを総称してユビキタスデバイスと呼ぶ。ユビキタスデバイスは、センサー、ID、プロセッサ、メモリ、ネットワークインタフェースを持ちうる。IC カード、RFID タグはユビキタスデバイスの例である。ユビキタスデバイス以外の、従来型の情報機器を IT デバイスと呼ぶ。例えば、ノート PC、デスクトップ PC、サーバコンピュータ、メインフレーム等は IT デバイスである。ユビキタスデバイスを次の 3 つ組でモデリングする。

ユビキタスデバイス ::= (owner, ID, 属性)

第一項の owner は，ユビキタスデバイスの所有者を表す。人間社会には、人とモノの間に「所有する」という関係があるが、所有関係は owner の一形態で、あるユビキタスデバイスがある人によって所有されているとき、そのユビキタスデバイスから所有者への参照が owner として設定されることになる。第 2 項の ID は、ユビキタスデバイスを一意に識別するための識別子である。第 3 項の属性は、ユビキタスデバイスのさまざまな性質を表したもので，属性名と属性値のペアの集合である。

属性 ::= {(属性名 $_1$，属性値 $_1$)，(属性名 $_2$，属性値 $_2$)，…，(属性名 $_n$，属性値 $_n$)}

センサ機能をもつユビキタスデバイスの場合は、センサによって獲得したリアルワールドの情報を属性値として保持する。センスされる情報が、時間と共に変化する場合（GPS による位置情報，温度情報等）は、属性値が時間と共に変化することとなる（ストリーム型データとして保持すると考えてもよい)。

ユビキタスデバイスは、IT システムと接続され、コンピュータシステム側はユビキタスデバイス側の情報を保持する。この情報は、次の形態で保持されているものとする。

システム保持情報 ::= (ID, 属性)

ここで ID は、対応するユビキタスデバイスの識別子である。属性はユビキタスデバイスに関する情報を保持する。

以下では、この簡単なモデルを使って、ユビキタス情報システムに関係するデバイス、システムのモデリング例をあげ、セキュリティ・プライバシー問題について考えていく。

例 1（日立製作所のミューチップ）。日立製作所が開発したミューチップは、縦 0.4mm、横 0.4mm、厚さ 0.06mm の非接触型 IC チップで、紙に埋め込むことを想定して開発された。128 ビットの情報が向上出荷時に書き込まれる。このデバイスは下記のようにモデリングできる。

ミューチップ ::= (owner, 128 ビット ID, nil)

owner は、ミューチップが埋め込まれたモノである。埋め込まれたモノを所有する人間に間接的にリンクするとも考えられる。図 6.2-1 は、一人のユーザが、ミューチップが埋め込まれた二つのモノを所有している場合の例である。

ミューチップはわずか 128 ビットの識別子（read-only data）と外部への通信機能のみを有する最小のユビキタスデバイスの一種であると考えられる。一つのミューチップ単体は、識別子情報のみをもつに過ぎないが、owner（モノ）へのリンクが implicit に存在することと、IT システム側サーバにおいて属性情報を保持することにより、owner であるモノに関する情報および owner の owner である人間に関する情報が管理可能となる。また、属性情報を処理することにより、ある人間が所有するモノが何かを調べたり、ある人間が所有するモノの変遷を追尾することが可能である。あるいは、あるモノがどのような人間達によって所有されていったかという変遷を追尾することができる。このような属性情報管理や追尾操作は，人間の知らないところで行われる可能性があり、4.2 節で述べた「識別性」に関する脅威であり、「情報プライバシー権」が冒される可能性がある。

例 2（IC カード Suica）。JR 東関東の Suica は、ソニー製の FeliCa を使用した非接触型 IC カードで、定期券およびイオカード機能をもつ。FeliCa は内部に 8 ビット RISC CPU、2～32Kbytes 実メモリ、212～848 Kbps の無線データ通信機能、ハードウェア DES 暗号

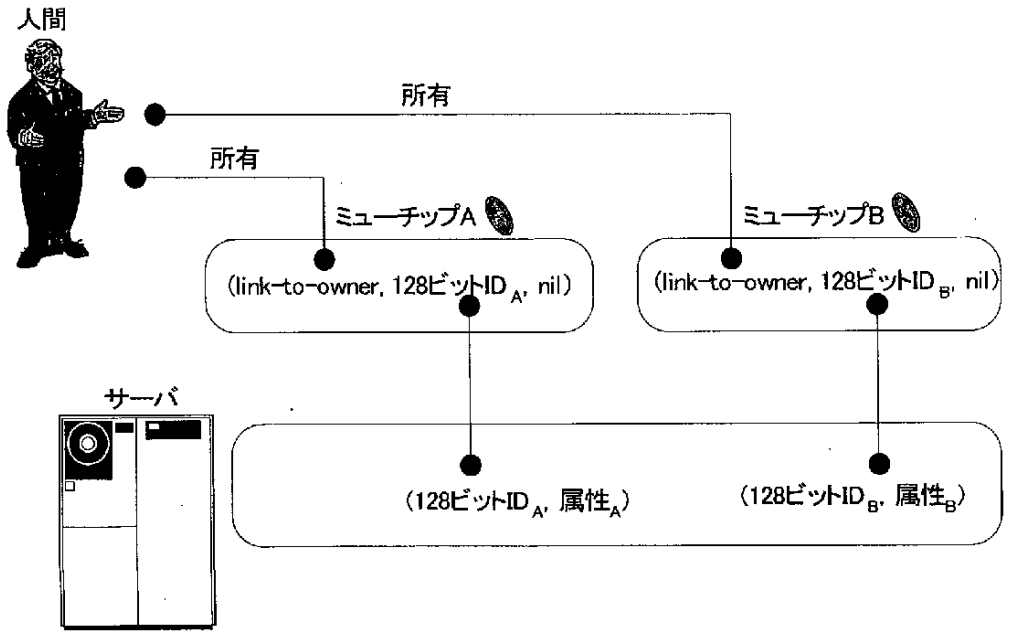


図 6.1-1　ミューチップ（日立製作所）

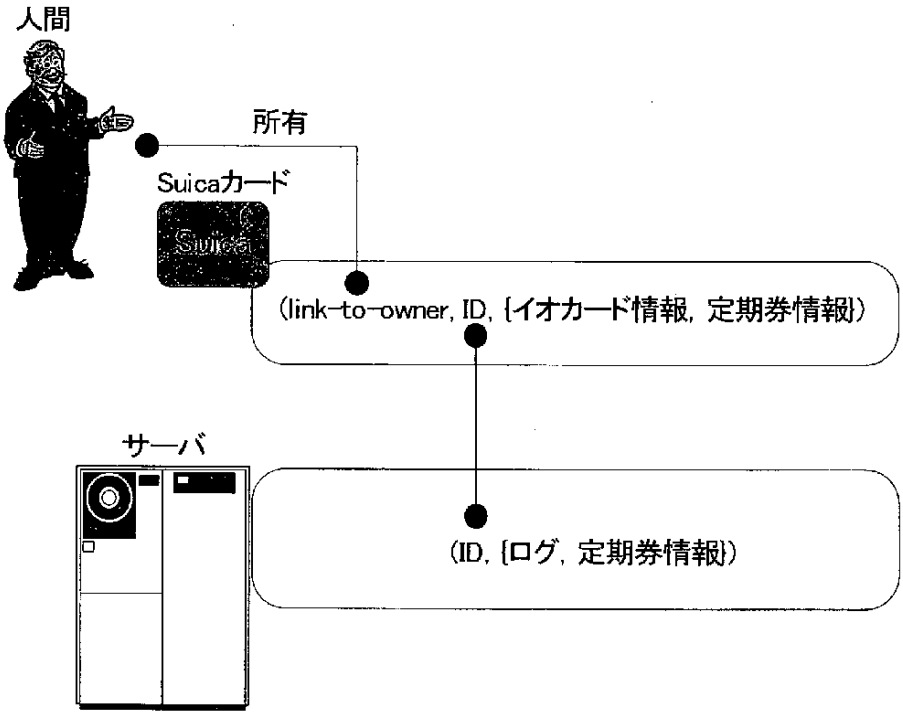


図 6.1-2　Suica（JR 東日本）

処理系を有し、アンテナより受信した電磁波により動作電力を得る。一般的なトランザクション処理を 0.1 秒程度で処理できる。

Suica カード ::= (owner, ID, {イオカード(プリペイドカード)情報，定期券情報})

Owner は、Suica カードの持ち主であり、属性としてイオカード情報（プリペイドカード情報）および定期券情報を持つ。図 6.1-2 はこれを図示したものである。

Suica カードは、バッテリー不要の無線 LAN 付き超小型 PC のようなもので、内部メモリを利用して、ユビキタスデバイス中に属性情報を保持することができる。また ID のマッチングを利用して、IT システム側のサーバに属性情報を保持することも可能である。この構造は、次で述べる、PC をクライアントとし、ネットワークを介してサーバと接続して使う場合と類似している。

例 3（クライアント PC）。IT デバイスであるクライアント PC も、このモデルを用いてモデリングすることができる。IP アドレスを有するクライアント PC は、下記のようにモデリングできる。

クライアント PC ::= (owner, IP アドレス，サイト属性)
サイト属性 ::= {ホスト名，ドメイン名}

システム側保持情報 ::= (IP アドレス，IP アドレス付随情報)

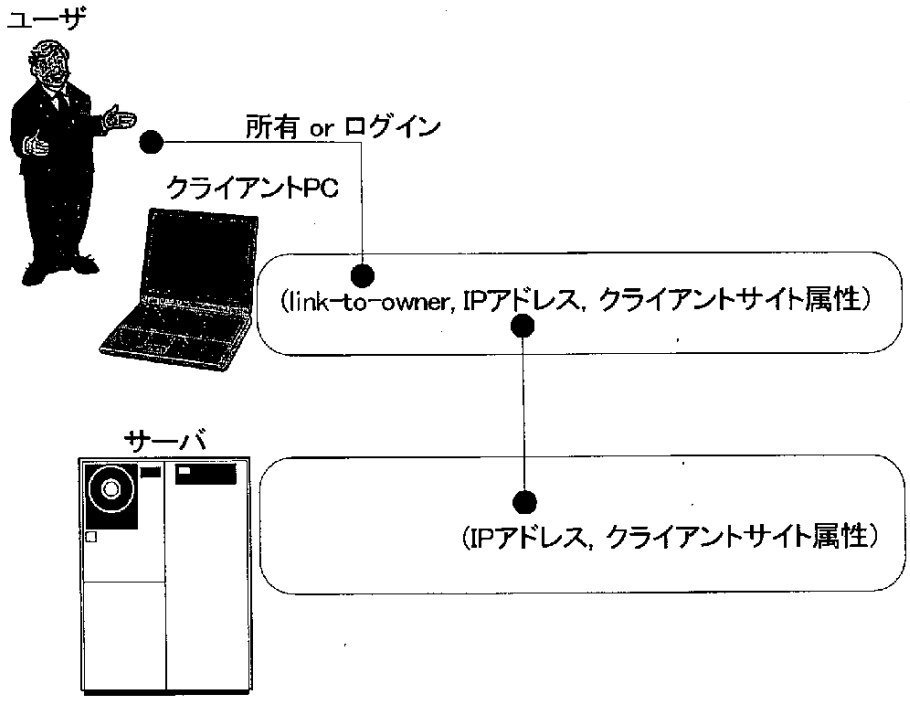


図 6.1-3　クライアント PC

図 6.1-3 はこれを図示したものである。

クライアント PC が固定の固有 IP アドレス（いわゆるグローバル IP アドレス）を持つ場合は、サーバはそれを用いてクライアント PC やそのユーザを識別し、それらに関する情報をクライアントサイト属性として保持することができる。

クライアント PC が固有の IP アドレスを持たず、DHCP プロトコルなどを用いて、動的な IP アドレスが割り当てられることがある。その場合、サーバから見たときのクライアント PC の識別子として IP アドレスを使用できない。この問題に対処することを一つの動機として、Web システムのサーバは，次に述べる「クッキー」を用いることがある。

例 4（Web システムにおけるクッキー）。クッキーとは，クライアント側に保持される永続的名前付き値のことである。保持される期間は下記のようである：

(a) 生成時にサーバ側指定した期限まで
(b) サーバが明に削除するまで
(c) クライアントが明に削除するまで

Web システムにおけるクッキーは、図 6.1-4 のようにモデリングできる。同図は、サーバ A によって発行されたクッキーA と、サーバ B によって発行されたクッキーB が、1 台のクライアント PC に保持されている状況を表している。

サーバ A とサーバ B が互いの情報の付き合わせを行える場合、もしクライアント ID_A= クライアント ID_B であれば、両サーバは「名寄せ」操作を容易に行え、あるユーザに関して互いの持っている情報を結合することができる（図 6.1-4 中の名寄せ 1）。クライアント

ID_A≠クライアントID_Bである場合でも、それぞれが保有するクライアント属性中に、ユーザ固有で同一の値があれば，それを用いて名寄せ操作が行える（図 6.1-4 中の名寄せ２）。実際、クッキーはしばしば、サーバがクライアントを一意に識別するためにも使用される。サーバが一意性を管理する値をクッキーとしてクライアントに書き込み、次回のクライアントからのアクセス時にそのクッキーの値を参照することにより、クライアントを識別する。これが、クッキーの値が他に漏洩すると、プライバシー情報が漏洩する危険性がある可能性の一例である。これ以外のクッキー漏洩の例としては、クライアント側にクッキーとして、サーバへのログイン名とパスワードが保持され、それらが他のサーバに漏れてしまう場合がある。

この状況は図 6.1-5 に示した二つのユビキタスデバイス A、B との OID リンクをサーバ A、B のそれぞれが保持する場合と類似している。この類似性は、現在、インターネット上のセキュリティ・プライバシーに関してしばしば議論となるクッキーに関する問題が、固有 ID をもつユビキタスデバイスの場合でも容易に起こり得ることを示唆している。

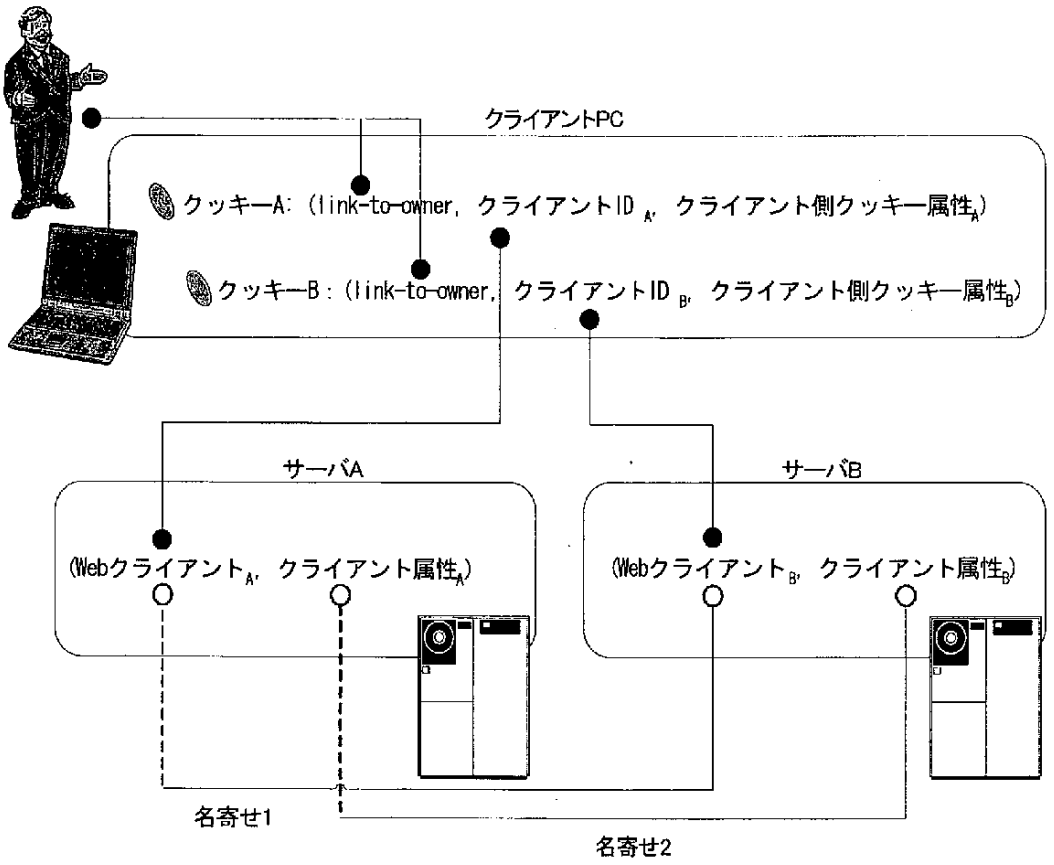


図 6.1-4　Web システムにおけるクッキー

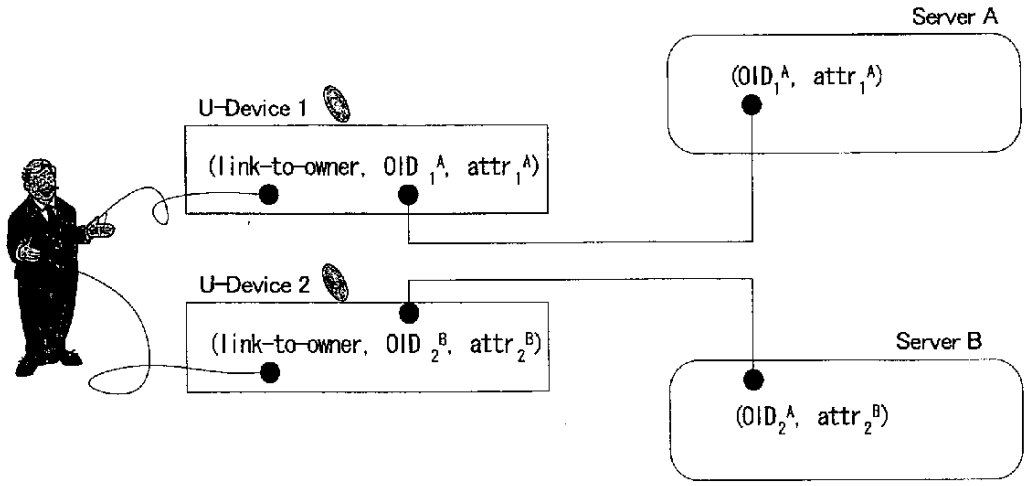


図 6.1-5　ユビキタスデバイス

例 5（住基カードシステム）。住民基本台帳ネットワークシステム（以下、住基システム）は図 6.1-6 のようにモデリングできる。住民票コードという識別子によって、住基カード－市町村サーバ－都道府県サーバ－指定情報処理期間サーバに格納された情報が推移的（transitive）にリンクされる。

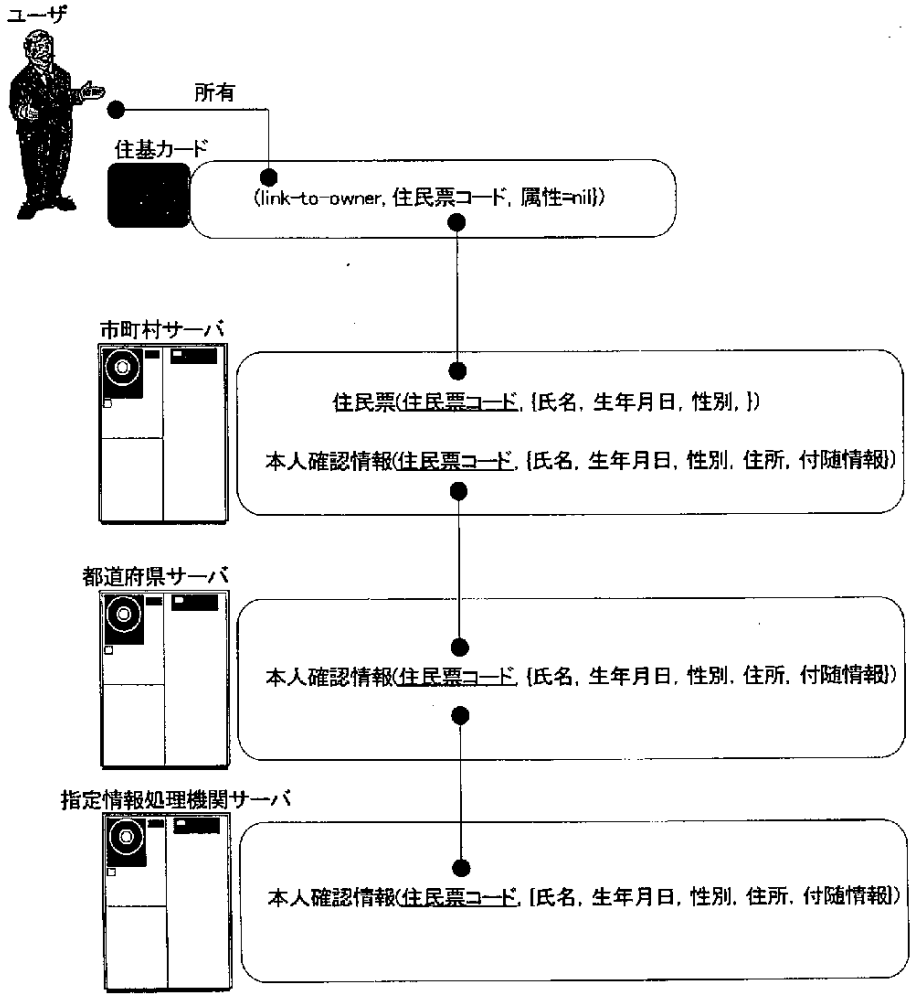


図 6.1-6　住民基本台帳ネットワークシステム

以上述べてきたことを以下にまとめる。

・ミューチップのようなRFIDタグは、単に識別子情報をもつだけに過ぎないが、これによって提供される識別性は、実世界における人間やモノをコンピュータシステム内の属性情報と結びつけるという重要な役割を果たす。
・ICカードは識別子情報に加え、それ自体が属性情報を持ちうる。例2（ICカード）と例3（PC）を見比べるとわかるように、規模やパワーは大きく異なるものの、ICカードとPCは、識別性と属性値に着目すると、よく似ている。
・ユビキタスデバイスやPCが、あるサーバにおいてローカルに一意の情報をもつ場合、サーバは、ユビキタスデバイスやPCおよびそれらの所有者に関する属性情報を保持することができる。PCが一意の情報を持たない場合も、クッキーを用いてそれに代用することができる。
・ユビキタスデバイスやPCが、グローバルに一意の識別子を持つ場合、もしくはそれらの属性値中に一意の値を持つ場合は、独立したサイト間にまたがって識別情報の付け合わせを行う、いわゆる「名寄せ」を容易に行えてしまう。これによって、ユーザの知らないところで、ユーザのプライバシー情報が漏洩したり、蓄積されていく可能性がある。
・住基システムにおいて既に行われているように、固有識別子を用いて複数のサーバを有機的に関連付けることができる。一つの識別子情報が漏洩すると芋づる式に、複数のサイトのさまざまな情報が漏洩する可能性がある。

6．2　メディアによるセキュリティ／プライバシーの脅威

ユビキタス情報環境におけるセキュリティ／プライバシーを議論する際に、行動履歴などの文字化されたデータとしての個人情報が他人に知られることによる脅威の他に、個人が撮影された映像や音声が他人に閲覧される脅威についても注意が必要である。ここでは、これを「メディアによるセキュリティ／プライバシーの脅威（または、メディアによる脅威）」と呼ぶことにする。

すでに現在，街中に監視カメラがあふれている。注意深く観察すると、道路の交差点、ショッピングセンター、銀行ATMなど多くの場所にカメラがあり、ビデオデータを記録したり、あるいは監視員が常時異変の有無をチェックしていることに気がつく。これらは保安上のためという理由で特定の場所に限って撮影されたり、高セキュリティ区域ということで社会的に容認されている。ユビキタス情報環境を目指した研究開発においては、ユーザの利便性、とくにユーザインタフェースを改善するという目的で、カメラやマイクロフォンを使ったセンサーシステムや状況理解システムが多数研究されている。将来には、個人を特定したり、顔や声が本人の了承なしに記録される状況が生ずる可能性がゼロではない。また、ディジタルカメラの普及や携帯電話やPDAにディジタルカメラが装備されるようになり、近い将来、国民の半分以上が手軽に街中で写真を撮影できる環境になると思われる。

このような状況で、メディアの脅威について議論をしておく必要がある。ここでは、まず現状分析として、このようなカメラやマイクロフォンなど音声・映像センサーの実世界への導入状況と、研究開発分野における動向のうち主だった例を示す。次に、それらがどのような脅威をもたらすのかを考察する。

６．２．１　音声・映像センサーの実世界導入状況

（１）監視カメラ

前述したとおり，道路の交差点における混雑状況の監視、高速道路の道路状況、無人式速度取り締まり装置（オービス）、インテリジェントビルの監視、観光地ライブ、銀行 ATM の監視、コンビニエンスストアのレジ監視などの目的でカメラが多数設置されている。英国では、全国で約 1,000 万台の監視カメラが設置されていて、平均５分に１回撮影をしている。このカメラ設置については当初賛否両論あったと思われるが、現在は犯罪防止に役に立っていると住民に受け入れられているとのことである。オービスは速度違反車の運転手と車番の写真をとって行政処分の証拠としている。

（２）携帯カメラ

デジタルスチルカメラ、デジタルビデオカメラの小型化と廉価版の普及により、多くの人が所有し利用するようになっている。テーマパーク旅行や運動会などの「ハレの場所」でアマチュアカメラマンが並ぶ光景に我々は慣れてきている。さらに近年、携帯電話にカメラが装備され、町中にカメラがあふれ、気軽にディジタル写真がとれて、ネットワーク経由で簡単・気軽に送ることができるようになっている。

（３）研究開発動向

古くはヒューマンインタフェースの研究として人物像・顔画像の研究が 20 年以上前から行われている。撮影条件のよい環境では顔画像を使ったコンピュータの識別（同定）能力は 95%を超えるところまで来ている。ヒューマンインタフェース研究の立場では、ジェスチャを使うことによって非侵襲の手軽な非言語インタフェースが可能になるため、熱心に研究されてきた。視野の隠れ（オクルージョン）を避けるために、カメラ台数を増やし、分散協調型の視覚情報システムを構築する研究が進み、ユビキタス情報環境の研究のブームの中で、部屋中にカメラを設置して、人間の行動をとらえて、位置関係などから、家電製品の制御コマンドになるジェスチャやそぶりを認識する手法が多数開発されている。そのための実験環境も多くの研究機関で設置されている。ジョージア工科大学の Aware Home プロジェクトでは、家のなかに各種センサーを設置しているが、カメラも含まれている。

次に、シーンの伝送を目的として、多数カメラを用いる方法も研究されている。サッカースタジアム、アメリカンフットボール、スキージャンプなど、多視点の撮影映像を使って利用者が自由な視点での合成画像を楽しめるようにしようという目的で、多数カメラのパンチルト制御や画像処理による画像合成技術の開発が行われている。

さらに、ウェアラブル・コンピューティングの研究の流れの中で、コンピュータディスプ

レイを眼前に置くだけでなく、ビデオカメラを眼前に設置して自分の視野と同じ映像をコンピュータ処理する研究が行われている。これらは，記憶想起の補助として用いたり、自己の体験として記録したり、あるいは拡張現実（Augmented Reality, AR）のための対象物識別のために用いられたりする。拡張現実の際は出力は対象物のIDがあればよいので、本来は映像データを必要とはしないが、センサーとしては2次元CCDなどの画像センサーを利用している。

6．2．2　メディアによる脅威

上記のように、すでに町中にカメラが設置されつつある。また将来、便利さと安全・安心をうたい文句にさらに多くのカメラがオフィス、家、街に氾濫する可能性がある。なお、マイクロフォンについては固定で設置されているケースはほとんど見られない。しかし、携帯電話の普及により、至る所で音響環境を録音してネットワーク上に置くことなどは技術的には可能となっている。

このような状況で、セキュリティ／プライバシーの観点から注意すべきことは、撮影録音の宣言と許可、肖像権の侵害、公衆への過度の露出、盗撮・盗聴、行動履歴の翻訳と利用である。

（1）撮影録音の宣言と許可

カメラやマイクで撮影収録していることを宣言し一般市民の許可を得ることが必要である。そのデータを誰が閲覧し、どのように記録しているかなどの情報開示が欠かせない。これを怠ると後出の盗撮盗聴と同じ批判をうける。撮影録音するカメラやマイクが機能していることを明示するアーキテクチャが必要であるし、公衆の場所では、市民のコンセンサスが必要である。しかしながら、監視カメラなどは、犯罪者に対しては隠して許可なしで撮影できなければ意味がない（カメラを設置して監視していることを宣言することが犯罪防止に役立つという側面もある）。この背反する条件を、どのように折り合いをつけるか、コストとメリット・デメリットと個人情報の開示許容のバランスのなかで決定されるべきものである。

（2）肖像権の侵害

我々は、知らない人に撮影録音されることに、生理的な嫌悪感を抱くことがある。その原因は確定できないが、その場の表情や言動が記録されて後世に残り、第3者が見て批評する機会となったり、自分の制御を超えたところで使われることへの懸念が背後にあると考えられる。例えば、図6.2-1はATRメディア情報科学研究所が2002年10月に実施した実験の様子である。部屋の随所と参加者それぞれにカメラとマイクが設置・装着されている。

この実験では、室内に居る人はその映像と音声がすべて録画録音される（音声はウェアラブルシステムを着用しない場合，めったに録音されることはない）。この実験環境に入る人は撮影されることを事前に了解しているが，撮影したデータを使ってドキュメンタリーを作り、本人に提示すると、映像の被写体になっていることよりも、話している音声対話

図 6.2-1　ユビキタスセンサールーム
（写真提供：ATR メディア情報科学研究所）

の内容にセンシティブな反応を示す。元来記録しないものである発言が記録されて残ることになると、人々がどのような反応をもつか、さらに研究が必要である。技術によって、加工する前の生の声や映像が利用されるようになることは、ユビキタス情報環境における大きな利点をもたらすものであることは間違いないが、データの流通とは別の視点で、映像・音声メディアがもたらす特質としてシステムデザインの際にプライバシー上の注意が必要である。これまで日常的な場では記録されることのなかったものが記録されるようになると人々がどのような反応を示すか、まだわからないことが多い。

（３）公衆への過度の露出

インターネット社会を基盤とするユビキタス情報環境において、特殊なプライバシーの脅威と考えられるものとして、意味もなく個人の情報が公衆に過度に露出することがある。情報伝達モデルにおけるセキュリティ問題は、経路切断、詐称、経路変更、すり替え、盗聴などに類別されるが、インターネット社会においては、個人の写真や行動を世界中にばらまくことも容易である。たとえ正規の情報収集手順を経たとしても、この過度の露出によって、個人のプライベートな空間を作ることが困難になる可能性がある。

（４）盗撮・盗聴

前述したように情報伝達経路に、密かに別ルートを設定し、情報を故意に入手することをいう。電話などの情報システムと違い、ユビキタス情報環境では、空間も情報伝達経路であり、任意の場所にカメラやマイクを設置することで盗聴・盗撮の危険にさらされる。また、ユビキタスセンサーの出力を送信する回線に接続するケースもある。これらの個人情報であるデータは商品としての価値をつけて売買されることもあり、プライバシーの侵害にあたる。とくに映像の場合には、本人の氏名などが添えられない場合でも、知人や隣人にとっては識別できるキューを与えるため、問題となる。

（５）行動履歴の翻訳と利用

ユビキタス情報環境で得られるカメラ画像は今後高解像度で撮影できるようになり、画

像処理の技術によって、映像から個人を同定して追跡することが次第に現実味を帯びてきている。すなわちユビキタス情報環境のうえに、将来その技術が成熟すると、個人の誰が、いつ、どこで、何をしていたかの 4W1H 情報を取得できるようになる。個人名は別のデータとの関連を調べる必要があるが、違う場所における行動も関連づけらるようになる。映像データなども、一旦行動履歴情報に翻訳されると、セキュリティ／プライバシーの問題は本報告書で中心的に議論していることに帰着する。

7．セキュリティ／プライバシー保全技術・システムの開発のために（提言）

7．1　セキュリティ／プライバシー保全技術の開発へ向けて

今後のセキュリティ／プライバシー保全システムの開発に向けた提言を行うために、ユビキタス情報システムと従来型の IT システムとの相違を明らかにすることから記述を始める。従来型 IT システムは、図 7.1-1 に示すように、コンピュータネットワークの世界の中に、サイバーワールドともいうべき、仮想的な情報世界を作り、ユーザは IT システムの存在を意識して IT システムの操作を行う。つまり、IT システムの存在がユーザにとって明示的(explicit)である。それに対して、ユビキタス情報システムは、図 7.1-2 に示すように，IT システムは暗黙的（implicit）となり、直接には人間が意識する必要はなく、実社会のさまざまなモノに、IT システム内のソフトウェアオブジェクトが結合されて構成されている。この暗黙性は、しばしば、disappearing computing(見えなくなるコンピューティング)と称される。デジタルデバイドという言葉があるが、この言葉は、従来型 IT システムの明示的な操作をうまく行える者とそうでない者の間に生じうる格差を指したものであるが、コンピュータの存在が暗黙的となるユビキタス情報システムにおいては、存在し得ないはずである。

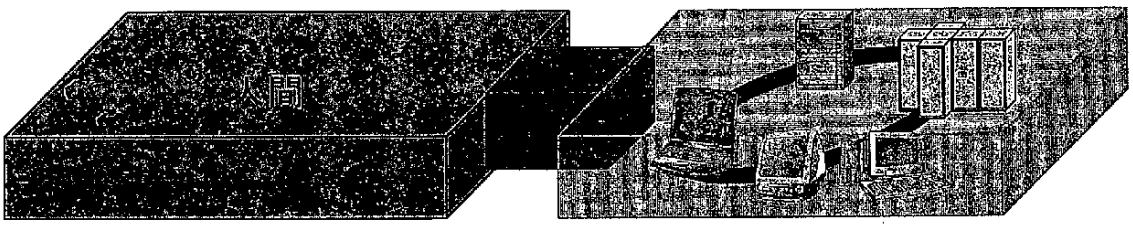


図 7.1-1　従来型 IT システム

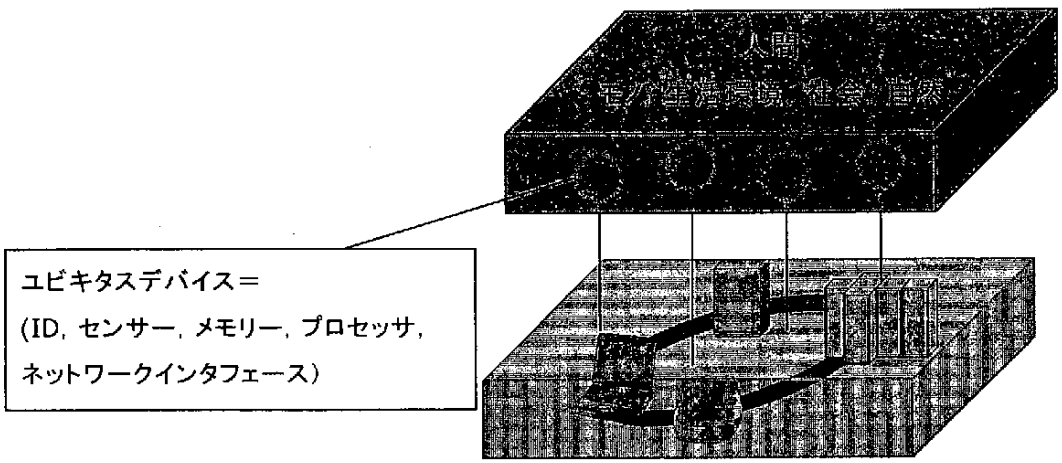


図 7.1-2　ユビキタス情報システム

このようなユビキタス情報システムにおいて、新たに問題となってくるのは、実世界に存在する、人間およびユビキタスデバイスと、IT システム内に存在するソフトウェアオブジェクトの間の結合関係である。4.2 節で説明した識別性の問題が、正に、この結合関係に関係している。人間とユビキタスデバイスの間の結合関係は、「所有関係」に代表されるように implicit な関係であり、ユビキタスデバイスとソフトウェアオブジェクトの間の結合関係も implicit である。implicit であることは、デジタルデバイドという概念をなくすことに端的に見られるように大きな利点であるが、反面、各個人の意識しないところで、各個人に関するさまざまな情報が IT システムにおいて、蓄積・追跡・処理・保存され得ることも意味する。このため、今後のユビキタス情報システムにおいては，これらの前述の二つの結合関係（すなわち、人間とユビキタスデバイスの結合関係、および、ユビキタスデバイスとソフトウェアオブジェクトの結合関係）をユーザがコントロールできるようにすることが必要である。

現状でのソフトウェアオブジェクトとユビキタスデバイスの関係を図 7.1-3 に示す。IT システム側のからユビキタスデバイス（もしくはその識別子）を直接に見ることができ、ソフトウェアオブジェクトがユビキタスデバイスに直接的に結合されている。この結合が自動的に保守・追跡され、両者間の相互交信が自動的に行われることによって、いわゆる disappearing computing が達成される。主導性(initiative)は IT システムおよびソフトウェアオブジェクト側にある。これは、ユビキタスデバイスは一般に計算処理能力は限られており、単に識別子を供給したり、僅かな情報量および情報処理力のみを保持しているためである。ユーザが自己情報をコントロールできるようにするためには、ユビキタスデバイス側に情報コントロールの主導性を持たせる必要がある。

一般に非力なユビキタスデバイスに、いかにして情報コントロールの主導性を持たせるか？　考えられる一つのアプローチは、図 7.1-4 に示すように、ユビキタスデバイスとソフトウェアオブジェクトの間に仮想的なデバイスを配置するようにし、この仮想デバイスに情報コントロールの機能を持たせることである。仮想デバイスは、図 7.1-4 のように一つ当たりが一つのユビキタスデバイスを管理してもよいし、あるいは、図 7.1-5 のように一つ当たりが複数のユビキタスデバイス（グループ）を管理してもよい。仮想デバイスは、ユーザの自己情報制御ポリシーに基づき、相手のソフトウェアオブジェクトを認識して、必要な識別情報や属性情報を提供する。識別情報をグローバルにユニークにするだけでなく、相手に応じて、時間に応じて、異なるようにしてもよい。属性情報も、フィルタリングをしたり、何らかの処理の後に送るようにすることも考えられる。このような機能を実現するためには、同機能を有する専用デバイスもしくはミドルウェアを作って、ネットワークおよび IT システムのいずれかのレイヤに配置すること、あるいは、ユビキタスデバイスに同機能を組み込むようにすること（今後のデバイス技術の発展がこれを可能にする可能性がある）等の方策が考えられる。

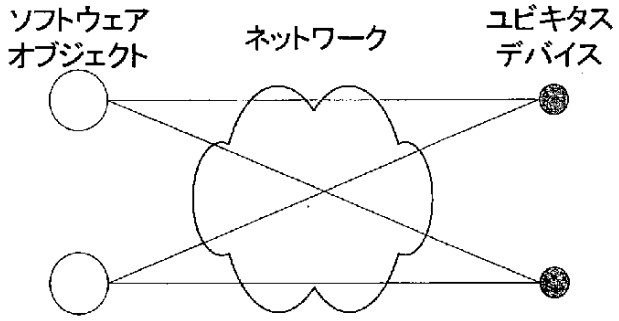


図 7.1-3　現状

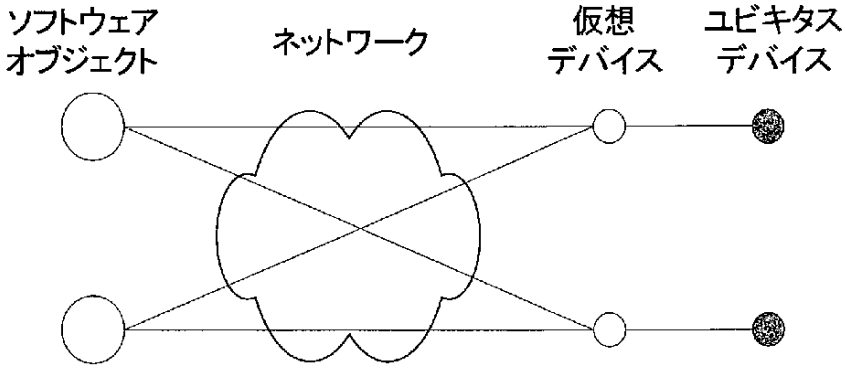


図 7.1-4　仮想デバイスを用いた間接アクセス

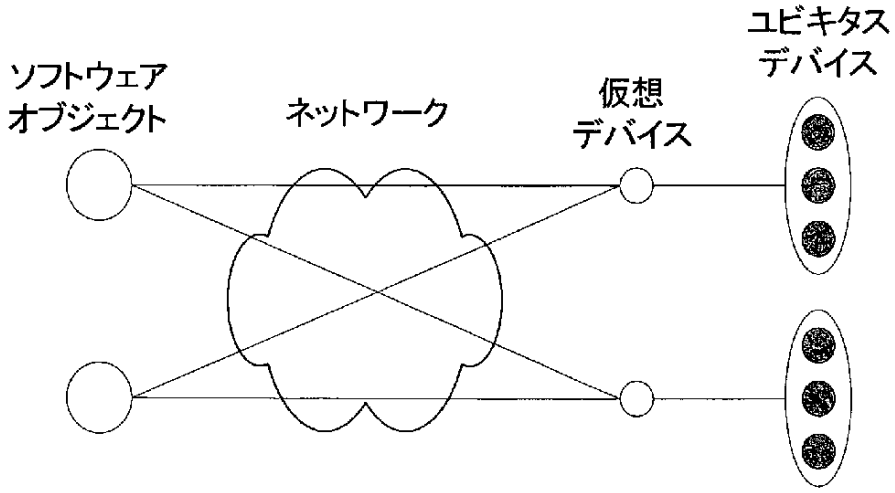


図 7.1-5　仮想デバイスを用いた間接アクセス（ユビキタスデバイスのグループ化）

7．2　ユビキタス特区の実証実験プロジェクトへ向けて

本報告では、ヒューマンインタフェース技術を「使いやすさ」の追求としてではなく、新産業の創出と安心・安全な社会の構築という視点で検討を進めてきた。ユビキタス情報社会が個々の人間の多様な生活をサポートし、多様な産業と活力ある社会を創造することが可能であるという「光」の側面について検討した。また、人間の日常生活の原点にある安心と安全を脅かすプライバシー侵害を生み出す恐れがあるという「影」の部分について、現状の問題点を詳しく調査するとともに、ユビキタス情報環境下で出現する問題点を重点的に調査した。世界的にもユビキタス情報環境下におけるプライバシー確保の問題が話題になり始めた段階であり、Ubicomp2002 のセキュリティワークショップとプライバシーワークショップでも課題の整理をしている段階である。その意味でも、本報告書 7.1 の提案は、非力なユビキタスデバイスが出回って生活に浸透した際の、新しいセキュリティ／プライバシー保全技術として、研究開発に着手すべきテーマである。

電子・情報・通信の研究開発は性能向上を追及し、計算・通信・記憶などのコストを低減させて発展してきた。20 世紀末の IT ブームは、材料・デバイスからメディア・サービス産業を牽引した。インターネットの整備と e ビジネス発展との相乗効果で、行政、金融、教育、医療などの仕事や社会の仕組みを変革したのである。その一方で、電子機器やオーディオ機器、パソコンは低価格競争を相変わらず繰り返し利益なき繁忙状態に陥ったままである。そのような状況下でユビキタスという言葉がにわかに脚光を浴びてきたが、本報告の各章節で論じてきたように、ユビキタス技術は広範な技術や産業と複雑に関わっており、市場原理で製品やサービス開発を行うだけでは本格的な産業創出は困難であり、安心・安全なユビキタス社会のデザインも難しい。

多数のセンサとコンピュータが広域かつ高密度で埋め込まれ、ネットワークで相互接続される「ユビキタス」の世界は各所で語られ始めた（本報告もその一つである）。しかし、ユビキタス世界の有効性（＝光）と問題点（＝影）の双方の課題については、様々な観点から議論されてはいるものの、想像の域を出ていない。インターネットやコンピュータの例を持ち出すまでもなく、新しい技術や製品・サービスの有効性や問題点は実際に使ってみないと明らかにはならない。

EU（欧州連合）の “Disappearing Computer”、米国の “Aware Home”、“Star Dust” や” Oxygen” プロジェクトなどの「ユビキタスプロジェクト」では、これらの課題を明らかにすべく、システムやサービスの実証実験が計画されてはいるが、いずれも特定のオフィスやテーマパーク内を対象にした限定的なものに過ぎない。

本来、「ユビキタス」はコンピュータを遍在させて、個々の人間において日常生活の全ての場面をカバーするものなので、家庭・仕事・都市・余暇等、生活の全ての状況を網羅しない限りは、潜在的な可能性や問題点、研究課題を明らかにすることはできない。ある特定区域の住民を対象にした本格的実証実験プロジェクトは、これまでに行われてきた CATV やインターネットの実証実験よりも効果は大きい。地域のプロジェクト参画者が利益を享受できるレベルでサービスを提供するには、通信インフラやエネルギーなどの社会

インフラ問題や予算的な問題はあるにせよ、技術的には生活空間全体のユビキタス化は可能なレベルに達しようとしている。世界各国でユビキタス関連の研究への投資が活発化しているが、実証実験は“Toy”レベルのものばかりである。各種社会インフラや行政や法律など制度的な問題が絡んで大規模な実証実験はなされていない。国が安心・安全なユビキタス社会の構築を先導し、知的社会基盤の構築、プライバシー保全技術開発と法律の整備を行うことは可能である。大規模な実証実験がなされれば、日本のお家芸であるハードとソフトの融合商品やサービス開発など関連する産業の伸張や地域の振興を推進し、ユビキタスコンピューティングで世界をリードできると考えられる。

例えば、ユビキタス情報社会を実現する場合、道路にくまなくセンサを埋め、ネットワークを整備しようとすれば、国土交通省、総務省、警察庁や自治体などの複数の役所から許認可を得る必要がある。また、プライベートな「持ち物」を含めて個々人の所有物全てにチップを埋め込み、街頭や家庭のセンサで常に行動を把握されるユビキタス世界の住人に対しても、全て許可を取って廻らなければならず、多大な労力を必要とする。しかし、この問題を避けて通っている限り、ユビキタスの本質と課題を明らかにすることはできない。この許認可の問題は「産・学」のサイドではどうすることもできない。これこそ「官」側に求められる役割なのではないだろうか。そこで我々は、上記のような「ユビキタスの大規模実証実験」を実施するための方策として、以下の「ユビキタス特区」の制定を提案する。

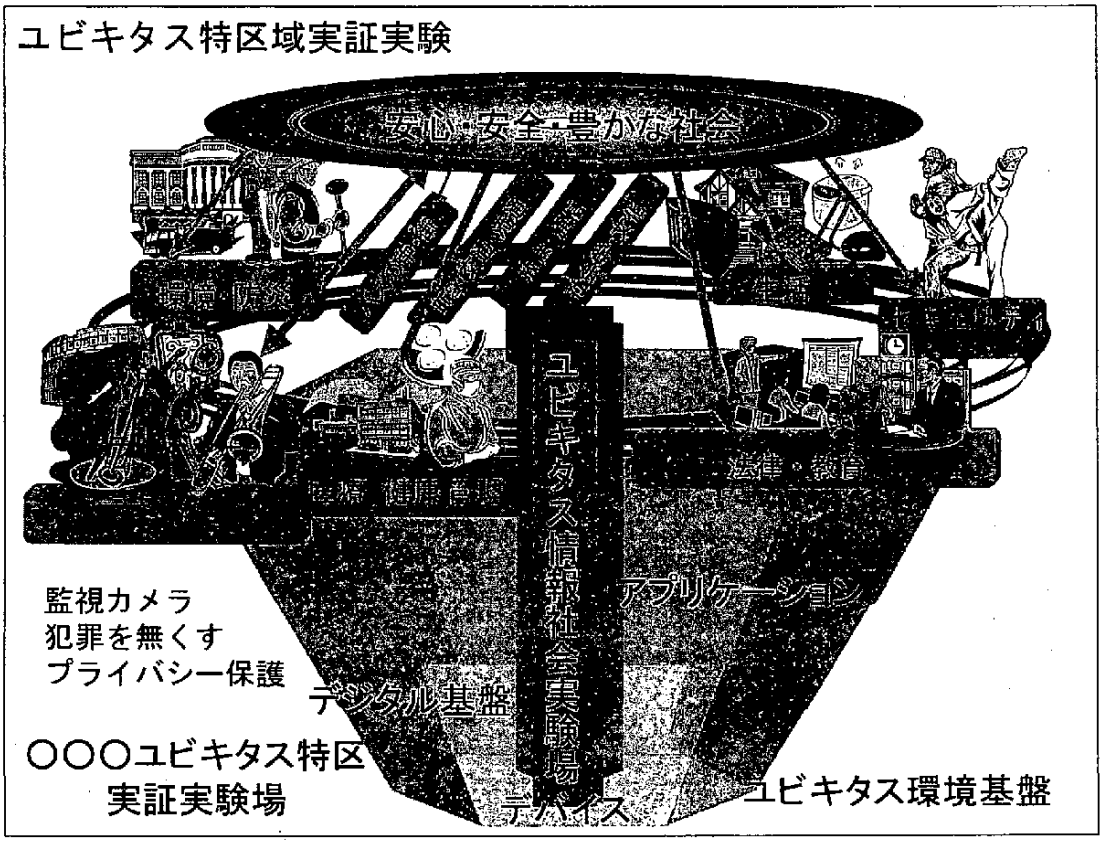


図 7.2-1　ユビキタス特区域実証実験の機能図

・名称：

ユビキタス特区（ユビキタスタウン）

・目的：

特定区域の住人と企業・官公庁などを対象に、日常生活の全ての場面を可能な限り「ユビキタス化」し、実際の生活活動を通じて、その産業やサービス創出と、安心・安全面の効用と問題点を洗い出すことで、将来のユビキタス情報社会実現の設計指針をつくる。

・概要：

家庭・仕事・ライフライン・交通・余暇を含めた生活全般を網羅するような特定区域（街路・モノ・ヒト）に様々なセンサを装着し、ネットワーク化と各種ユビキタス情報環境を整備する。そのような情報基盤上で特区内の住民や企業などを対象に、機器システムや知識コンテンツ開発を進め、教育、福祉、交通、娯楽、演劇、健康などのサービスを提供する。セキュリティ・プライバシー保全技術も研究テーマとして、社会学的な検討も進める。サービス開発や技術開発は、区域外の企業や大学も公募で参加できるようにする。

・産学の役割：

街路や家などの特区内のあらゆる場所に自由にセンサや機器システムを設置でき、システムを稼働できる。プライバシーポリシーは遵守するが、企業やシステムの運用データは、ユビキタス研究を加速するために原則公開とし、ユビキタス情報環境の効用や問題点を洗い出す。

・官公の役割：

産学サイドがシステムを動作可能にできるように、関係省庁との調整を図る。セキュリティ／プライバシーのポリシーを明確化し、住民や関係機関が実験を効果的かつ安心して推進できるような仕組みを作る。当該区域の住民についても、持ち物へのセンサの設置や、24時間の行動把握の合意を得る。また、ネットワークや電力・ガス・水道などの共通インフラ設備を整備する。

本ユビキタス特区の提案では許認可と関係機関との調整という困難な問題を官公側が担当することとした。官公サイドが、将来の「ユビキタス社会」を実現する上で必須の項目についての先行実験から、行政や法的な制度上のノウハウを得られることは間違いない。また、産学にとっては、面倒な許認可問題を考えることなく、安心安全と豊かさを追求し、情報通信技術やヒューマンインタフェース、プライバシーなどの基盤技術の研究と、ユビキタスの効用と問題点の洗い出しに注力できるというメリットがある。

ユビキタス特区となる地方/都市の自治体にとっても、制度上のノウハウ取得はもちろん、大規模なネットワーク整備が国の予算で行なわれるという魅力がある他、安心・安全な暮らしの実現、企業誘致、住民の参画意識の向上、教育や学習システムの整備、産業や知識の獲得、住民の意識向上と「先進都市」というイメージ向上の副産物もある。

本報告書ではヒューマンインタフェース技術とプライバシーという観点からユビキタスコンピューティング技術を様々な観点から調査し、来るべきユビキタス社会の光と影を検討することにより、ユビキタス環境下におけるプライバシー保全研究プロジェクトの具体的提案と、広範な分野と関わるユビキタス技術の実証実験の場としてユビキタス特区の提案を行った。ハードとソフトと人間とビジネスが関係するユビキタス技術では日本は世界的にもプレゼンスと競争力が高い。このチャンスを逃さずに本報告書で論じてきた研究開発を加速したい。

ユビキタス特区の提案は斬新なものであり、課題は多いと思われるが、本報告書の読者諸氏にご意見を伺いたいと思う。特に、産官学のそれぞれの立場から具体的な賛同意見や提案、補足やアドバイスをいただけたら幸いである。

Ⅱ．資料編

A．IPv6 に関する内外の状況

A．IPv6に関する内外の状況

1．背景

20世紀の情報通信基盤は、インターネットプロトコルIP（Internet Protocol）をそのコア技術として、信頼性のある産業・生活基盤としての役割を果たさなくてはならない。インターネット技術は、これまで、いわゆるコンテンツと呼ばれる情報を、人々に提供したり、人々の間で共有したりすることがその主な利用法であったといえる。ところが、半導体技術を核としたデジタル情報処理技術の発展は、コンピュータ以外のデジタル機器をも、インターネットに接続することを可能にし、実際に、これまでは、ネットワーキングされることがなかった機器までも、インターネットに接続されようとしている。その結果、これまでのいわゆるコンテンツ以外の情報が交換共有処理される機会と量が急速に増大するとともに、その質的な多様性も急拡大している。

インターネットは、地球上で最も複雑な自律的分散情報システムであり、常に新しい技術やサービスを導入しながら、現在も驚くべき速さで成長を続けている。インターネットは、これまで、TCP/IP技術を用いたオープンなグローバルネットワーク化（第1の波）、Web技術の導入による利用者の一般化（第2の波）、信頼性向上技術の向上によるビジネス化（第3の波）という、3つの大きな波を経験し、今、常時接続（ネイティブインターネット)を前提としたブロードバンド化とユビキタス化という第4の波を経験している。

これまでのインターネット成長と発展を支えてきたインターネットシステムを形作るプロトコル群（さまざまな機能を実現するために多数のプロトコルが定義され実装されている)は、IPをその核としており、TCP/IPプロトコルスウィートとも呼ばれている。TCP/IPプロトコルスウィートは、インターネットの発展とともに、次々に継続的に進化を遂げてきた。すなわち、インターネット自身の成長と発展は、インターネットの環境を変化させ、それに対応するために必要な新しい技術が、発明され導入・普及してきた。しかしながら、インターネットシステムおよびインターネット技術の進化の過程において、根幹にある思想は、一貫して変わっていない。それは、以下の4点であるといえる。

（1）End-to-End Principle（エンドエンドの原則）
（2）IP over Everything（データリンクに依存しないシステム）
（3）Everything over IP（IPを用いたデジタル通信の統合化）
（4）Connectivity is own Reward（接続性こそが本質）

インターネットの基本原理は、言うまでもなく、エンドエンドアーキテクチャ（End-to-End Architechture）である。エンドエンドアーキテクチャにより、ユーザ側が主役となって、地球規模の新しいサービスを迅速、自由にかつ低コストで実現することを可能にする。エンドエンドアーキテクチャを維持し、この第4の波を実現発展するために必須となる基盤技術の確立を推進なければならない。エンドエンドアーキテクチャモデルを維持しながら、コンピュータ以外のさまざまなデジタル機器が偏在し、これらが相互接続される環境を構築するための基盤技術が、IPv6（IPバージョン6）技術である。

今後、インターネットは、北米、欧州、アジアの工業的先進国のみではなく、アジア、

アフリカ、南米の発展途上国にも幅広く展開されるとともに、工業先進国ではさらに高密度で普及しなければならない。既に、携帯電話の加入者数は、我が国でも5千万を突破しており、中国においては1億以上の加入者数が存在している。もはや、携帯電話の利用法は、音声から電子メールを中心としたデータ通信へと変化している。すなわち、音声通信を第1の目的にした電波の利用法は、データ通信を第1の目的としたものへと進化する必要がある。この1つの動きが、無線LAN技術を用いた広域無線データ通信サービス（数メガから十メガビット毎秒の通信速度を提供可能）の展開である。また、家庭用電気機器ベンダーは、いわゆる白物家電やAV機器（Audio Visual機器）をインターネットに接続させ、それぞれが、グローバルなIPアドレスを持ち、インターネットへのアクセスおよびインターネットからのアクセスを実現しようと、研究開発を加速させている。例えば、冷蔵庫と食品流小売業とをインターネットを用いて有機的に結合させて、新しいビジネスモデルを構築展開しようとする動きもある。さらに、自動車をインターネットと相互接続し、車から入手可能なさまざまな情報（温度、湿度、位置など）をインターネットとやり取りするための技術開発やビジネスモデルの検討が進められている。

“End-to-End Architecture”に基づいた“Connectivity is own Reward”がインターネットの本質であることは上述の通りである。ところが、電話システムや広域無線サービス（2Gや3Gなど）では、「（通信）品質第一」で「鎖国管理貿易」がその設計方針のように見える。 これを、技術的にかつ美麗に表現すれば、「シームレスな（高品質）マルチメディアを先端的な差別化技術で実現」となる。これまで、常に、シームレスと（高品質な）マルチメディアが切り離されることなく、電話を基盤としたインフラは設計されてきた。しかしながら、インターネットは、継ぎ目が前提のシステムであり、ネットワークはメディアを意識せず、デジタル情報で、すべてのメディアを抽象化し統一的に処理する。この、「継ぎはぎだらけのネットワーク」、「メディアを意識しないStupidなネットワーク」という特徴が、インターネットが汎用性の高い情報インフラとして、継続的に利用可能な、根本的な理由である。

現在のインターネットで広く用いられているIPv4（IPバージョン4）技術は、1970年頃のインターネットシステムを仮定して設計されたものであり、コンピュータの数は、比較的少なく、技術知識の高い専門化（研究者）が利用者であり、さらに、コンピュータは移動しないものであると仮定されていた。21世紀のインターネットでは、このようなIPv4では解決できなかった問題を解決することは、もはや不可能であり、これらの課題を解決するIPv6の導入が必須となる。

IPv6技術の導入により、すべてのデジタル機器が、自律的にかつ容易にネットワーキングされ、トランスペアレントなエンドエンドでのデジタルコミュニケーションを行うことが可能となる。 このような、環境では、デジタル機器が、容易にネットワーキングされるだけではなく、"安全に"、これが実現されなければならない。ここでいう、「安全」とは、第3者からの敵対的な攻撃に適切に対応可能でなければならない という意味（Security & Privacy）と、さまざまなシステム障害の発生に対しても信頼性高く接続されなければならない（resiliency, robustness, dependable）という2つの意味を持つ。

以下、ここでは、ユビキタスネットワーク環境を支える基盤技術であるべきIPv6技術の概要と現状を概観し、その後、ユビキタス情報環境の具体的な展開の状況と方向性、最後

に、ユビキタスネットワークが解決すべき技術的かつ社会的な課題について、報告を行っている。

２．基盤技術としてのIPv6技術

２．１　IPv6技術の必要性

インターネットは、今後、欧米、アジアの工業的先進国のみではなく、アジア、アフリカ、南米の発展途上国にも幅広く展開されるとともに、工業先進国ではさらに高密度（ユビキタス化）で普及しなければならない。現在のインターネットで広く用いられているIPv4技術は、1970年頃のインターネットシステムを仮定して設計されたものであり、コンピュータの数は、比較的少なく、技術知識の高い専門化（研究者）が利用者であり、さらに、コンピュータは移動しないものであると仮定されていた。21世紀のインターネットでは、このようなIPv4では解決できなかった問題を解決することは、もはや不可能であり、これらの課題を解決する基盤技術として、IPv6の導入が必須となる。

1990年初頭、インターネットが急速に普及したために、特に、IPアドレスの不足と経路数の増加が、IETF（Internet Engineering Task Force）において、懸念されるようになった。そこで、この問題をどのようにして解決していくべきかという議論が開始された。1960年代以降、初めて、本格的に新しいプロトコルを議論設計することになったため、今後のインターネットに必要な以下の新しい要求条件を満足するようなプロトコルの設計を行うことになった。

（１）セキュリティ機能
（２）モビリティ機能
（３）プラグ・アンド・プレイ
（４）マルチキャスト

IPv6は、IETFにおいて技術検討が開始されたとき（1991年）には、IPng（IP next generation）と呼ばれ、1994年7月に基本的なプロトコル設計の方向性（SIPPを基本にする）が決定された。

IPv6の技術的な概要を、IPv4と比較しながら、以下に簡潔にまとめた。

（１）アドレス空間の拡大

IPv4のアドレス長は32ビットであるのに対して、IPv6はその4倍の128ビットのアドレス長を持つ。

32ビット＝4,294,967,286 (約43億)

128ビット＝　340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6が提供するアドレス空間は、IPv4のアドレス空間の2の96乗倍もの大きさとなる。

（２）アドレスアーキテクチャ

a.階層的なアドレス構造

b.アドレススコープの導入

c.アドレス種別の明確化

（３）マルチキャストの標準化

（４）パケット転送の高速化への対応

a. ヘッダフォーマットの簡素化

b.パケットのフラグメント(分割)の廃止

（５）リンク層とネットワーク層のアドレス解決

a.ARP(Address Resolution Protocol)機能をより一般化高機能化し、
NDP(Neighbor Discovery Protocol)機能とした。

b.不到達性の検知を能動的に行うものとした。

（６）セキュリティ機能

IPSecを、IPv6が実現すべき標準の機能とした。

以上が、IPv6技術の、非常に大まかな概要である。IPv6技術は、

（１）アドレス空間の拡大によるエンドエンドアーキテクチャモデルへの回帰と維持、

（２）集約可能な階層的アドレスアーキテクチャの導入による効率的なアドレス管理と経路数の増加を防止

（３）マルチキャスト/モビリティ/セキュリティという新たな機能への対応

（４）アドレス自動設定機能やネットワークレベルでのIPアドレスのリナンバリングなどプラグアンドプレイ機能の充実

が、その技術的な特徴として挙げられる。

２．２　IPv6研究開発の現状

２．２．１　オペレーティングシステム

通常のパソコンやワークステーションにおいて利用されている、汎用のオペレーティングシステムのIPv6対応は、2001年9月時点でほぼ完了しているといえるであろう。

（１）マイクロソフト

Windows2000およびWindowsXPでは、マイクロソフト社自身が提供するIPv6スタックが提供されている。さらに、組み込み用のOSとしても利用されているWindows CEのIPv6対応版のリリースも予定されている。さらに、WMT（Windows Multimedia Technolohies）技術のIPv6対応も完了している。また、IPv4とのIPv6の共存環境への対応のためにも、6to4技術（ダイヤルアップやxDSLなど GlobalなIPv4アドレスが利用可能な環境で適用）、ISATAP技術（イントラネット環境で適用）、TEREDO技術（NATを用いたプライベートIPv4アドレスが使用される環境で適用）を、実装提供している。

（２）サンマイクロシステム

Solaris8 から、既に、IPv6対応を行っている。

（３）アップルコンピュータ

MacOS-Xから、マッキントッシュのネットワークコードは、UNIXのネットワークスタックを参照利用している。

（４）BSD系UNIX

KAMEプロジェクトが提供するIPv6プロトコルスタックが採用されており、既に、正式配布パッケージでのIPv6への対応が完了している。

（５）LINUX

USAGIプロジェクトが、LINUXのIPv6プロトコルスタックの品質向上を推進している。

（６）その他

産業用システム(例えば携帯電話など)用の組み込みOSとして、日本国内で広く利用されているTRONのIPv6化も、ACCESS社によって行われた。さらに、ネットワーク機器用の組み込みOSとしては大きなシェアを持つVxWorks（WindRiver社）のIPv6化も既に完了している。

２．２．２　ルータ

ルータ市場の最大のシェアを持つシスコシステム（Cisco Systems）社を始めとして、バックボーンルータ市場で第2位のシェアを持つジュニパー（Juniper）社も、IPv6のサポートを既に行っている、さらに、国内のルータベンダーのほとんど（日立製作所、日本電気、富士通、ヤマハなど）も、既にIPv6機能を盛り込んだ製品を市場に投入している。

（１）バックボーン

既に、ほとんどのルータが、ハードウェア処理によるIPv6パケット転送処理が可能となっており、Wire-Speedでのスイッチングが可能である。バックボーンのルータで必要な経路制御プロトコルであるBGP、OSPFおよびRIPの開発も既にほぼ完了している。

（２）アクセス

最もIPv6への対応が必要なルータおよびネットワーク機器であるが、IPv6への対応が最も遅れているカテゴリーといえる。 特に、ADSLやケーブルインターネット用のネットワーク側に設置する集線装置系の対応が遅れている。 また、BAS（Broadband Access Server）と呼ばれる、ADSL/ケーブル/FTTHなどのブロードバンドアクセスネットワークのための認証サーバのIPv6対応も行われなければならない。

（３）SOHOルータ

SOHOすなわちHome OfficeやSmall Office用のコンパクトなルータである。これまでは、アナログモデムやISDNルータが主流であったが、ブロードバンドの進展に伴い、ADSLやケーブルインターネット用のSOHOルータのIPv6対応が進んでいる。 家庭内やオフィス内では、IEEE802.11bなどの無線LAN技術を用いる場合も増えており、これらは、通常非常に単純なリンクレイヤ機能のみを持っており、IPv6への対応に関しては、何の問題もない。

２．２．３　サーバ

サーバノードとして、一般的に用いられるコンピュータ（BSD系UNIX、SUN Solaris、Linux、Windowsなど）は、上記の通り既に、IPv6への対応を終えている。したがって、基本的には、サーバ上で動作するさまざまなアプリケーションがIPv6への対応を行えば、IPv6化が進むという状況にある。

２．２．４　アプリケーション

IPv6が本格的に利用され普及するためには、いわゆるコンピュータのユーザ空間で動作するユーザアプリケーションが開発されなければならない。このようなアプリケーションの中には、ネットワーク管理ソフトウェアのようなネットワークの運用に関係するソフトウェアをはじめとして、Webブラウザ、メディアプレーヤ(e.g., RealVideoシステムやWMTなど)、あるいは、FTPやTelnet/SSHのような基本アプリケーションなど、いわゆるミドルウェア機能を実現するソフトウェアの開発と導入が進展しなければならない。このようなソフトウェアを開発するための、MIB（Management Information Base）の定義や、アプリケーションインターフェース（API）の規定は既にほぼ完了しており、Production Qualityでの導入と運用に向けた段階に入りつつある。 実際、たとえば、マイクロソフト社は、アプリケーションの開発ベンダーに対して、IPのバージョンに依存せずにアプリケーションを開発するために必要な開発環境の提供を、既に展開している。

２．３　IPv6の普及に向けた活動

IPv6技術の研究開発と普及、特に、Production Qualityレベルのネットワークの構築と運用に向けて、国内外において、さまざまな活動やプロジェクトが推進されている。

２．３．１　国際的活動

（１）6REN

IPv6 Research and Educational Network（http://www.6ren.net/）略。6RENは、米国エネルギー省（DoE; Department of Energy）の研究ネットワークであるESNET（Energy Science Network）の調整役を行っている、カリフォルニア大学（USC）Lawrence Berkeley国立研究所のBob Fink博士が中心となって推進している活動である。 Production Qualityのグローバルな研究教育ネットワーク（R&Eネットワーク）を構築運用するための、技術開発やネットワークの構築運用を推進することを目的としている。

（２）IPv6 Forum (http://www.ipv6forum.com/)

IPv6に関係する産業界、IETFコミュニティー、IPv6 R&Eネットワークコミュニティーから構成されるフォーラムで、IPv6の普及に向けた産業界やユーザコミュニティーの啓蒙活動を行うために設立された。IPv6フォーラムは、技術仕様の標準化活動は行わず、「v6サミット」とよぶコンファレンスの開催などを通じて、IPv6技術の現状と利点を啓蒙している。

２．３．２　欧州における活動

（１）GEANT (http://www.dante.net/geant/)

次世代インターネットに関する4年間のプロジェクト（2000年11月にスタート）。欧州の27カ国のNREN(National Research and Educational Network)を相互接続している。幹事/事務局はDANTE、資金源はEuropean Commissionの第5プログラム（Framework V Programme）である（TEN-155の後継）。

（２）6WINIT (http://www.cs.ucl.ac.uk/research/6winit/)

無線技術を用いたインターネットシステムの研究開発を推進するプロジェクトであり、欧州最初のIPv6-3G Mobile Internet Initiativeの運用を目指している。6WINITの目的は、有線のインターネットと無線のインターネット（広域セルラ技術と無線LAN技術の両方を考慮している）とを、有機的に相互接続してシームレスなIPv6インターネット環境を構築するための要素基盤技術の研究開発と運用ネットワークの構築と運用を行うことである。

（３）6NET / EURO6IX

欧州全体にまたがるIPv6バックボーンとして、欧州の情報通信キャリアが協力して構築したEURO6IXと、シスコ社を幹事として構築された6NETが存在する。

（４）IST FP6 (Framework Program 6)

現在、欧州は、第6次の科学技術研究開発プログラムFP6の検討を行っている。この中で、IPv6は重要な基盤技術と認識されている。

２．３．３　北米地区での活動

北米地区におけるR&Eネットワークおよび商用ネットワークのIPv6化は、残念ながら、必ずしも順調には進んでいないように見える。しかし、米国の産と学とが共同で運用するR&EネットワークであるAbelineがIPv6化を推進している。Abelineのバックボーンルータは、IPv6への対応を行う目的もあり、シスコ社のGSRからJuniper社のT640に総入れ替えが完了しようとしている。

さらに、北米、特に米国では、2001年9月11日のテロ以降、危機管理(Crisis Management)や公衆安全(Public Safty)に関する基盤の整備を推進するという動きがある。DARPA(国防総省先端科学技術研究機構）とDoD（国防総省）のネットワークで、IPv6機能を調達の

必須条件とすることが、2002年4月に正式にアナウンスされたこともあり、多くの政府機関のシステムの調達条件にIPv6機能が盛り込まれつつある。さらに、Public Safty Networkの構築は、すべて新しいネットワークを構築するのではなく、既に、存在しているネットワーク機器を上手に利用し、これらを、IP技術を用いて相互接続し、これまで、独立に動作していたシステムを統合化するという考え方が、一般化しつつある。シスコ社は、これを「Single Communication Grid」と呼んでいる。すなわち、これまで、独立に動作していた機器同士を有機的に相互接続して、ネットワーキングすることによって、効率的でシームレスなコミュニケーション環境を構築し、公衆安全（Public Safety）を確保するためのシステムの構築が推進されるわけである。これは、まさに、ユビキタスネットワーキング環境の構築に他ならない。このような環境では、IPv6とIPv4が混在し、良好に動作運用されなければならない。

２．３．４　アジア太平洋地区での活動

アジア太平洋地区における R&EネットワークであるAPAN（Asian Pacific Advanced Network、さらに、APANには、アジア各国を片方向の衛星リンクで相互接続したAI3（Asian Internet Interconnection Initiatives Project, http://www.ai3.net/）もIPv6化が完了している。

中国においては、MII(情報産業省)の研究所が中心となって推進している6TNETが北京に構築され、IPv6対応機器の中国国内のISPへの導入に向けた評価を展開している（日本の総務省が協力）。また、国家計画委員会は、日本の経済産業省と協力してIPv6テストベッドの構築と運用を計画している。

台湾でも、IPv6フォーラムの設立やIPv6 R&Eネットワーク（NBEN）の構築など、IPv6への対応が加速している。

２．３．５　国内活動

（１）IPv6普及・高度化推進協議会

平成12年10月に、総務省などの支援を得て設立された。協議会委員長は慶應義塾大学村井純教授。4つの分科会（WG; Working Group）が組織化され活動を展開している。

(a) IPv6アプリケーション開発WG、
(b) IPv6実験網構築WG、
(c) IPv6テクノロジーWG、
(d) 基本戦略WG

（２）IPv6ディプロイメント委員会（http://www.iajapan.org/ipv6/）

インターネット協会（http://www.iajapan.org/）では、IPv6に関する「普及啓発の活動」「情報交換の場の提供」を主な活動目的として、2001年4月に「IPv6ディプロイメント委員会」を設立した。委員会の開催を中心としてIPv6の技術や運用などに関するセミナー開催や研究会の開催、APNIC Policy Meetingへの参加、APRICOTへの参加などを行うこと

を予定している。

（３）総務省/通信放送機構JGN

JGN（Japan Gigabit Network, http://www.jgn.tao.go.jp/）は、平成11年度から運用を開始した、研究開発の促進を目的とした、全国規模の広域広帯域ネットワーク。レイヤ2サービスのみを提供してきたJGNにおいて、平成13年度に、IPv6のサービスを提供するためのネットワーク基盤を構築し、IPv6のサービス提供は開始された（平成14年4月）。 全国26箇所にIPv6ルータを配置しており、事実上世界最大のIPv6のR&Eネットワークとなっている。

２．３．６　インターネットエクスチェンジ

IPv6のサービスを行っているプロバイダ同士を効率的に相互接続するために必要となるIX（Internet eXchange）は、既に、10箇所で運用されている。

（１）北米：6箇所
6IIX（KDDI系の米国ISPのテレハウス）、6TAP（R&Eプロジェクト）、フロリダIX（ベルサウス社）、NY6IX、PAIX（MFN社）、S-IX（NTT）

（２）欧州：3箇所
AMS-IX（アムステルダム）、INXS（ミュンヘン）、UK6X（テレハウス社）

（３）アジア：1箇所
アジア地区においては、WIDEプロジェクトが運用するNSPIXP6（http://www.wide.ad.jp/nspixp6/）とNSPIXP2が唯一のIPv6-IXとなっている。

３．IPv6の展開とユビキタスネットワーク

従来のサーバクライアント型の情報提供サービス的なサービスだけではなく、IPv6は、いわゆるコンピュータ以外のデジタル機器が、インターネットと相互接続され、自律的に相互作用することが期待されている。以下、いくつか、具体的な研究開発活動の例を紹介する。 これらは、すべて、数年以内に、ビジネス展開が期待できる、ユビキタスネットワーキングの具体例と見ることができよう。

（１）情報家電機器

冷蔵庫、電子レンジなどの白物家電機器をはじめとして、AV（オーディオ ビジュアル）機器、さらにはゲーム機器など、身の回りのいわゆる電化製品が、IPv6のプロトコルスタックを実装し、インターネット接続することによって、新しいサービスを創造しようという方向性である。各機器の遠隔監視や遠隔操作など、後述する情報環境の構築整備と融合統合化されることになるであろう。

（２）移動通信

電車や自動車など、移動する車両がインターネットに相互接続する環境である。車両に乗車している人の活動を支援する目的も数多く検討されているが、「インターネット自動車」プロジェクトのように、自動車が、さまざまなデジタル情報を収集発信することで、乗車している人の活動支援以外の新しい価値を創造しようとしている。名古屋市のタクシーを用いた実証実験では、自動車の位置情報、速度情報、ワイパーの動作情報などを用いて、道路の混雑情報や降雨情報の把握などが低コストに実現可能であることを証明し、実証実験終了後も、タクシーの効率的運用に有効であることから、その運用が継続されている。

また、米国では、警察のパトカーにモバイルIP機能を拡張して実現したモバイルパトカーが実際に、運用されている。パトカーは、モバイルネットであり、小型のルータと、それに接続されたデジタル機器がサブネットを構成している。これらのデジタル機器は、パトカーの移動を意識するする必要はない。また、パトカーは、モバイルIP機能を用いて、外部からのアクセスを、適宜利用可能なデータリンク（CDMAやIEEE802.11b無線LANなど）を用いて実現することができる。

（３）情報環境

センサーノードをはじめとして、身の回りに、さまざまなデジタル機器を配備することによって、新しい情報空間を創造する方向性が模索されている。 単に、たくさんのデジタル機器を偏在させた、いわゆるユビキタスネットワーク環境ではなく、はっきりとした目的を達成するために必要なデジタル機器を配備するといった、現実的な検討が進められている。 たとえば、ビルシステムの空調・電源あるいはセキュリティシステムの制御は、インターネット技術（IPv6）を導入し、オープンシステム化することによって、大きなコストダウンを達成することが可能とされており、IPv6普及高度化協議会では、Building Automation分科会が設立された（2003年2月）。さらに、工場やプラントの制御である Factory Automation、あるいは、家庭環境の制御である Home Automation への展開が期待される。このような情報環境の構築には、最近急速に技術の標準化と研究開発が加速しているAuto-ID技術、RFID技術、あるいは、位置情報の自律的な検出技術などを、統合化した情報環境の研究開発が今後推進されるべきであろう。

当然ながら、ビル、工場、家庭の情報環境のネットワーク化は、これらの間のネットワーク化も推進することが可能であり、汎用性の高い自律的な情報環境の提供により、より低コストに種々のトータルSCM（Supplied Chain Management）などへの展開も期待される。

（４）自律的なクロスメディアコミュニケーション機器

エンドノードでの高度なデジタル処理、IPv6プロトコルを基盤としたPeer-to-Peer通信環境の提供は、人々が自由に、インターネット上に存在する知恵や情報を共有しながら、新しいコミュニケーションの形態を創造していくことになるであろう。既に、Instant Messaging Serviceでは、常時接続環境において非常に重要となる“Presence”と呼ばれる新しい概念を、リアルタイムコミュニケーションの世界に導入した。また、既に人々のコミュニケーションはシングルメディア（音やテキスト）に閉じることはなく、クロスメディ

アでのコミュニケーションへと移行している。

4．ユビキタスネットワーク環境とIPv6技術

4．1　技術課題

IPv6技術は、ユビキタスネットワークを実現する基盤技術と位置付けることが可能であり、上述の通り、IPv6技術そのものは、基本的な技術の国際標準化（by IETF）と要素技術の研究開発と製品化、さらに、既存アプリケーションのIPv6への対応など、基本的な対応は、ほぼ完了しているといえる状況である。今後は、既存のインターネットを構成しているコンピュータ以外のデジタル機器が展開する際に必要となる、新しい技術要素の研究開発を推進する必要がある。具体的には、以下のような技術課題が挙げられる。

（1）プライバシーとセキュリティ

個人情報のプライバシーの保護と、安全なシステムを構築運用するために必要な情報の収集と管理（たとえば個人認証やロギング）は、基本的には、相反するものである。この問題を、技術的に解決するための研究開発の緊急度と重要度は、ユビキタスネットワーク環境の登場とともに、急速に増加している。セキュリティ技術は、「鶏と卵問題」と「継続的な変更」が要求される技術分野である。また、プライバシーを保護しつつ、しかし、セキュリティーの実現に必要な技術を確立する重要度は極めて高い。たとえば、電子貨幣を用いた商取引のために研究開発された技術の適用と応用、ならびに、実証的環境での評価が重要となると考えられる。

さらに、グローバルなインターネットシステム（ユビキタスネットワークの環境では、質・量ともに複雑度と規模性が増大する）におけるセキュリティ機能実現のためのバックエンドシステムの構築は、地方自治体、国家の問題にとどまらず、国家間ならびにグローバル企業における問題として認識され、このためのグローバルスケールなインフラストラクチャ（たとえば、CAシステムなど）の構築と運用が行われなければならない。

さらに、危機管理体制を、国家、地方自治体、企業において確立し、これらが自律的に運用されつつ、かつ協調動作するようなシステム技術（Grid的な考え方）および体制の確立が行われなければならない。

（2）アクセスリンクおよびアクセスネットワーク

ユビキタスネットワークの環境において、各デジタル機器は、静止している場合もあれば、移動可能な機器である場合もある。また、これらの機器は、どのような環境で使用されるか、あらかじめ指定されない場合が、非常に多いと考えるべきである。したがって、これらのユビキタスなデジタル機器は、多様なデータリンクを自由に利用可能でなければならない。

ユビキタスネットワーク環境の構築には、既存のネットワーク環境のみならず、多様な無線および有線技術が融合され利用されなければならない。このような環境に向けた技術開発を推進し、安価で安全なユビキタスアクセス環境を、ユビキタス機器に対して提供することを可能としなければならない。

（3）識別子と名前空間

ユビキタスネットワーク環境においては、これまでの、情報通信システムやインターネットが収容サービスしていたノードの数をはるかに上回る、莫大な数のデジタル機器が接続される環境を想定しなければならない。エンドエンドアーキテクチャを基本とした、トランスペアレントなネットワーク環境は、今後、急速にその領域を拡大されることになる。しかし、常に、技術とコストのバランスで各デジタル機器の仕様は決められ、システム全体としては、自律的なアクティブな機器のだけではなく多数のパッシブなデジタル機器も存在し、ネットワーキングされなければならない。このような環境における、各デジタル機器をグローバルに識別可能とするための識別子のアーキテクチャ、その識別子と機器をヒトが識別可能な名前とマッピングするためのプロトコルとシステムアーキテクチャ、さらには、名前と識別子に関するプライバシーの問題を、われわれは解決しなければならない。

（4）ルーティング技術

ユビキタスネットワーク環境においては、これまでとは比較にならないくらいの多数のデジタル機器がネットワークに接続され、これらが、Place & Play 的に（かつ安全に）接続され、グローバルインターネットからの接続性（Accessabiliy）が提供されなければならない。移動するネットワーク、ネットワークのトポロジーの動的変化への対応が可能なルーティング技術の確立は、非常に重要な技術要素として認識されなければならない。

4．2　政策的社会的課題

ユビキタスネットワークの導入と利用の推進のためには、上述したような技術的課題の解決のみならず、このような技術の導入が、社会的にかつ政策的に推進すべきものであるいうことに関する社会的なコンセンサスの形成が極めて重要となる。ユビキタスネットワークの環境は、一部の業界における閉じたシステム環境ではなく、オープンで産業間ならびに企業間にまたがるような環境である。

したがって、各業界ならびに関係する業界間での連携、さらに、一般社会に対するコンセンサスの形成が非常に重要な課題となる。たとえば、米国においてはPublic Safey Sysemの構築は、個人のPrivacyよりも、ある面、優先して推進すべきであるとの社会コンセンサスが形成されているとみることも可能であろう。

5．まとめ

IPv6技術は、ユビキタスネットワーク環境が実現するリアルスペースとの融合および統合化へと大きく進展発展しようとしており、これまでの、いわゆるインターネットサービスでは想像することのできなかった情報環境を提供しようとしている。デジタル処理能力を持った機器やデバイスが、自律的に他の機器/デバイスとデジタル情報の交換共有を行うことで、まったく新しい情報環境を生み出そうとしている。このような環境を実現するためには、まだまだ、解決すべき技術課題が山積している。われわれは、これらの技術課題を順次解決し、豊かで安全な新しい情報の発展と構築に向かわなければならない。

Ⅱ．資料編

B. ユビキタスコンピューティング関連ビジネスの取組み

B.ユビキタスコンピューティング関連ビジネスの取組み

B．1　セキュアなユビキタスサービス実現に向けて　　（株）NTT データ

1．ユビキタスサービスの状況

コンピュータ技術、ネットワーク技術の高度化に伴い、「ユビキタス（ubiquitous=遍在する）サービス」が、様々な業界で提案されている。現在、この環境の変化をビジネスチャンスととらえ、各業界でもユビキタスに向けた取り組みを活発化している。図１は通信業界・コンピュータ業界・家電業界・自動車業界の取り組み概要をまとめたものであるが、それぞれの業界が自分の強みとなる製品・サービスを軸に適用領域を広げていこうという動きが見られる。

総務省が実施したユビキタスに関する調査研究会では、2010 年には、どこにいてもストレスなく、あらゆるサービスを自在に利用できるネットワークができるという将来イメージを示し、研究開発のトリガーとなる技術開発分野に対し、集中的にリソースを投下するという推進方策の下、3 つのプロジェクト設置（超小型チップネットワーキングプロジェクト、何でもマイ端末プロジェクト、どこでも NW プロジェクト）が提案されている。現在は、ユビキタスネットワーキングフォーラム（UNF）という任意団体の中で、研究開発の課題設定や標準化を引き続き検討しており、当社でも、運営委員会や技術部会に委員登録をするなどして積極的な活動をしている。

2．セキュアなユビキタスサービス実現に向けた技術開発

ユビキタスサービスに必要となる４つの遍在性として、ネットワークの遍在性、コンテンツ（情報）の遍在性、アプライアンスの遍在性、セキュリティの遍在性を設定し技術開発に取り組んでいる。ここでは、セキュリティの遍在性を実現する技術開発について説明する。

ユビキタスネットワークの世界では、パソコンや携帯電話、情報端末、情報家電、センサなど、あらゆる機器がネットワークにつながることが想定される。従って、ネットワークに接続される機器数は現在に比べ膨大となり、機器間トランザクションも膨大になると考えられる。これらのトランザクションに対して、正しく認証を行う必要があるが、現在のクライアント／サーバ型認証では、サーバへの負荷集中という問題発生が考えられる。また、パソコンに比べ CPU／メモリのスペックが劣る省リソース機器（情報家電やセンサなど）は、高度な認証機能の搭載が難しく、セキュリティを保てない可能性がある。そこで、これらの課題を解決するため、P2P（Peer-to-Peer）技術を利用した超分散認証プラットフォームを提案している。図２は、提案するプラットフォームを用いたサービスイメージを示したものである。このアーキテクチャでは、認証処理をユーザ側の Peer で管理するため、機器の登録・削除が容易で、ユーザの機器利用状況に合わせたセキュリティやスケーラビリティが実現可能である。

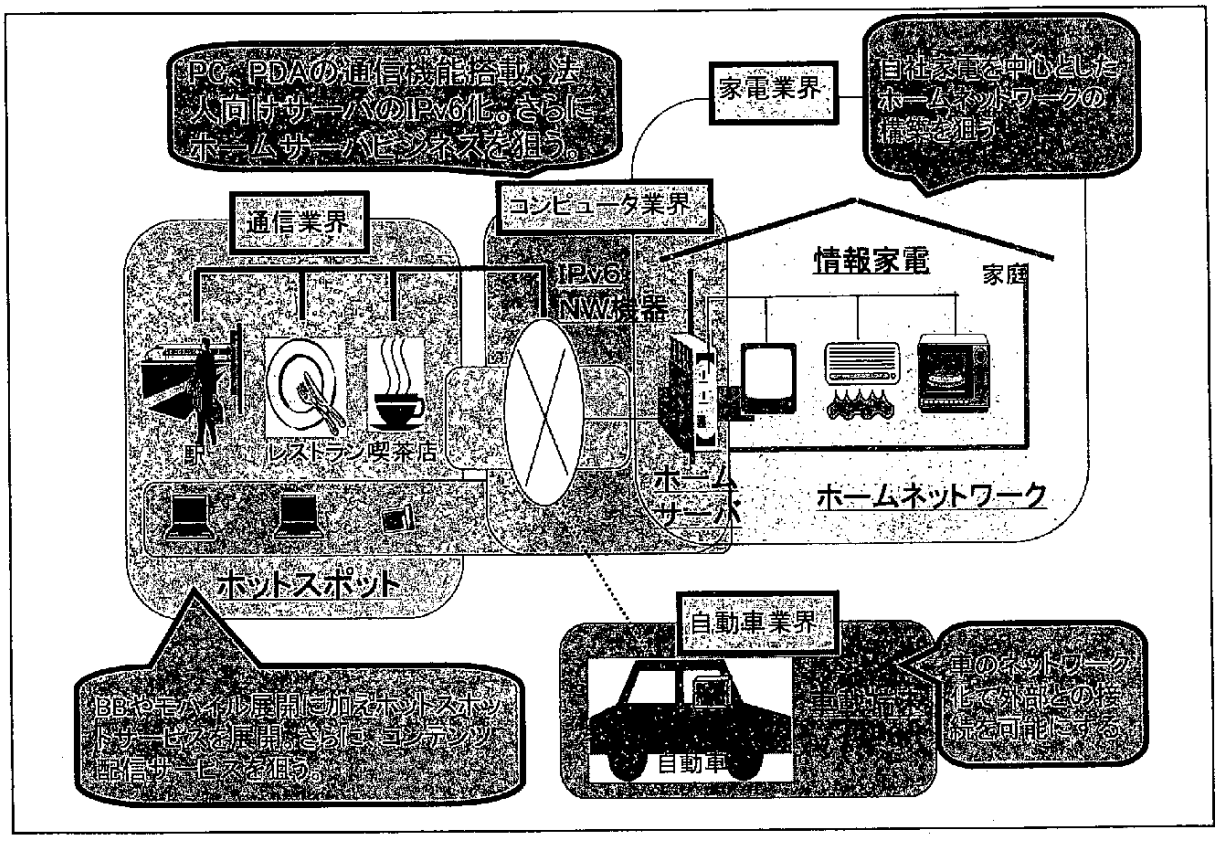


図 B. 1-1　ユビキタスに関する国内の動き（概要）

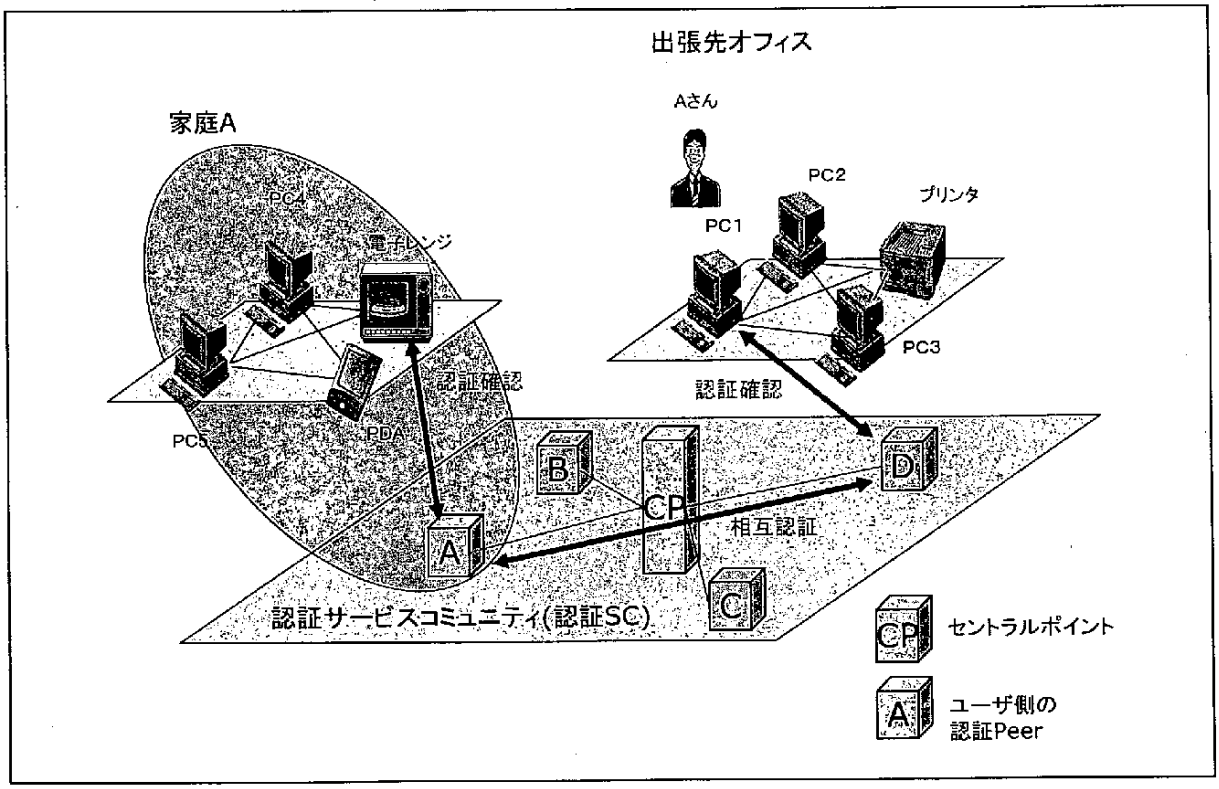


図 B. 1-2　超分散認証プラットフォームのサービスイメージ

B．2　シャープ（株）のユビキタスコンピューティング関連ビジネスの取組み

ユビキタスコンピューティング環境(以下、ユビキタス環境)を構成するシステムは、エンドユーザが占有的に使用する個人システムと、複数人或いは不特定多数ユーザが共用する公共システムに分類することができる。

個人システムは PDA、携帯電話、PC、そして各種情報家電から構成され、一般的にはホームネットワークや PAN(Personal Area Network)で接続されたシステムとなる。一方、公共システムを構成する機器は、オフィスにある共用の複写機やプリンターといった事務用機器の他、公共施設の待合室や街角に設置されるテレビや広告用ディスプレイ、そして環境情報などを取得するセンサーネットワークなどが挙げられる。オフィスでは各種事務用機器がイントラネットにつながっているが、現在存在する公共システムのほとんどは、機器単体、或いは閉じたネットワークで動作している。ユビキタス時代になるとすべての機器やシステムがインターネットにつながり、ネットワークを介して利用可能になると共に、個人システムと公共システムが無線通信等でつながって、個人が自由に公共システムを利用することができるようになる。

このような所謂ユビキタス環境では、ユーザが自分の PDA に入っているデータを街角に設置されたディスプレイに表示したり、コンビニエンスストアで目の前にある複写機(プリンター機能を併せ持つデジタル複合機)からプリントアウトするようなことが日常的に行われるようになる。現在でも出張中のビジネスマンなどにオフィス環境を提供するビジネス・コンビニエンスショップが存在するが、それに類する環境が、いつでも、どこでも構築できるようになる。

ところが、ここで浮き上がる課題の一つとして、公共システム/機器に転送されたデータのセキュリティが挙げられる。ユーザ所有のデータは一旦公共機器内のメモリやハードディスクに格納されるため、生のデータがいつまでもそのままの状態で残っていたのではセキュリティのみならずプライバシー上の問題も生じる。例えば、デジタル複合機のような公共機器に対する直接的な不正操作や、ネットワーク上のセキュリティ対策をかいくぐっての不正アクセスがあった場合、機器内に残っている機密データや個人情報が漏洩してしまう可能性がある（図 B.2-1)。ユーザが公共システムを安心・安全に利用できるようにするためには、この問題を解決しなければならない。

このような問題に対してシャープ[1,2]は、メモリやハードディスクを内蔵し、プリンタや FAX としても使用できるデジタル複合機に対して、複合機内のメモリに蓄積されたデータ

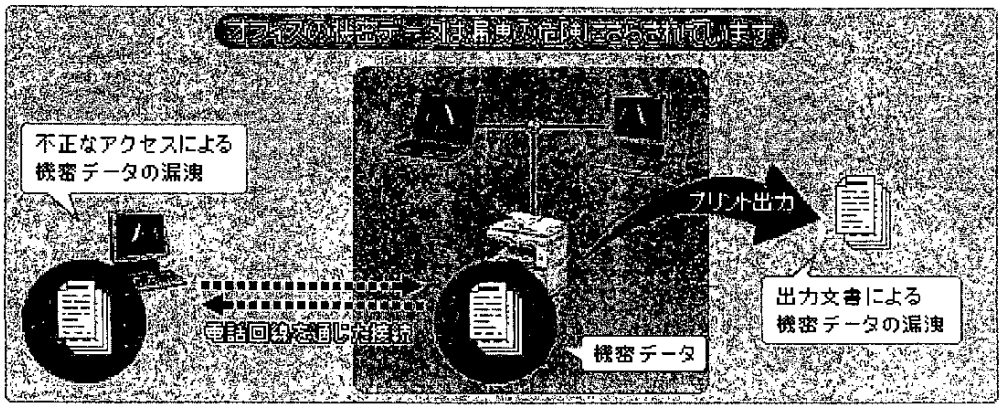


図 B.2-1　デジタル複合機におけるデータ漏洩の危険性

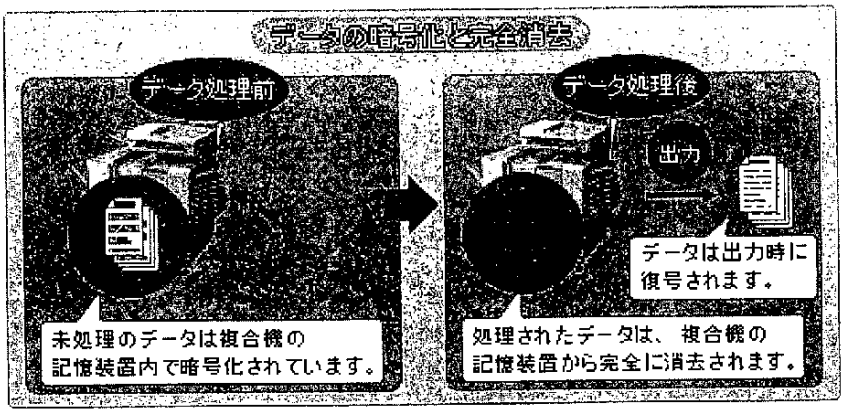


図 B.2-2　データの暗号化と完全消去

を暗号化するなどして保護すると共に、然るべきタイミングでデータ消去することを可能とするセキュリティキットを開発し発売している（図 B.2-2)。更に、ISO/IEC15408 情報技術セキュリティ評価基準[1]に基づいた認証を米国認証機関から受け、公的に一定以上のセキュリティ評価基準を満たしていることを保証する施策を取っている[2]。この取り組みは現在のところ複合機本体を対象にしたものとなっているが、今後、複合機に転送されるデータの暗号化や、複合機への不正アクセスの防止など、複合機がつながるネットワークの中での総合的なドキュメントセキュリティに拡張されることが予想される。また一方で、政府機関やオフィスユーザを中心に事務機器に対するセキュリティ対策へのニーズは強く、今後は更にその要求が強くなっていくものと思われる。

ユビキタス時代においては、公共システムを構成するすべての機器、或いはシステム全体が以上のようなセキュリティ施策を取っていることが必須条件となる。すなわち、機器やシステム全体が然るべきセキュリティ技術を装備し、更に公的な認証制度によりそれが保証されていなければならない。また、公共システムのエンドユーザのみならず、公共システムを設置し、それを利用したサービスをエンドユーザに提供する事業者も、このような施策が取られていることを必須と考えるようになるであろう。

【参考文献】

[1] http://www.sharp.co.jp/corporate/news/021206.html
[2] http://www.sharp.co.jp/print/document/security/security_1.htm
[3] http://www.ricoh.co.jp/imagio/iso15408/index.html

1 情報技術一般のセキュリティ評価基準の規格であり、各種情報関連機器やネットワーク機器、或いはそれらのソフトウェアも対象となっている。
2 シャープの他では、リコーがドイツの認証機関で複写機の ISO/IEC 15408 の認証を受けている[3]。リコーの複写機はパスワードによるデータ/アクセス管理を行っている

B．3　セイコーインスツルメンツ（株）のユビキタスコンピューティング関連ビジネスの取組み

1．はじめに

ユビキタスコンピューティング（UC）のユビキタス（Ubiquitous）とは、ラテン語で「偏在する」とか「いたるところに存在する」と言う意味である。この UC の概念は 1988 年に米ゼロックス社パロアルト研究所のマーク・ワイザーによって提唱された。同氏は 1993 年の論文で、UC を「computing access will be everywhere」と定義した。

セイコーグループの中核的なウオッチメーカーとして成長して来たセイコーインスツルメンツ（株）は、この UC の概念が実現した社会を標榜し、その実現に向けて努力して来たパイオニアであると自負している。何故ならば、ディジタルクオーツウオッチがまだランダムロジックで設計された 1 チップ IC や 4bit マイクロコンピュータ 1 チップで構成されていた当時 1984 年に、世界で初めてリストコンピュータ UC2000 を商品化した実績を持つ。リストコンピュータ UC2000 は、マルチチップで構成され、データ通信機能も備えた本格的なコンピュータであった。1998 年にはこの思想を進化させたウェアラブル PC“Ruputer”を製品化した。Ruputer はパソコンのパワーユーザに高く評価して頂いた。

ユビキタスコンピューティング社会には、現在の携帯電話や PDA、モバイル PC よりも更に小型の情報端末が必須になると考えている。その小型情報端末の特徴としては、オンデマンド機器では無く、ネットサイドから配信された情報の表示や蓄積、又は携帯情報端末自身が何らかの情報を収集してネットサイドに通知するタイプになるであろうと考えている。我々はこの様な小型情報端末を今までの実績をベースに、ユビキタスコンピューティング社会に提供して行きたい。合わせて、ハードウェアの提供ばかりでなく、価値ある情報を付加することで、革新的なソリューションを提供し、人と情報をつなぐネットワーク社会に貢献して行きたいと考えている。

以下、セイコーインスツルメンツ（株）が製品化して来たウェアラブル PC の歴史を振り返り、今後のユビキタスコンピューティング社会に必要な携帯情報端末を実現するための課題に触れると共に当社の取り組みの一端を簡単に紹介したい。

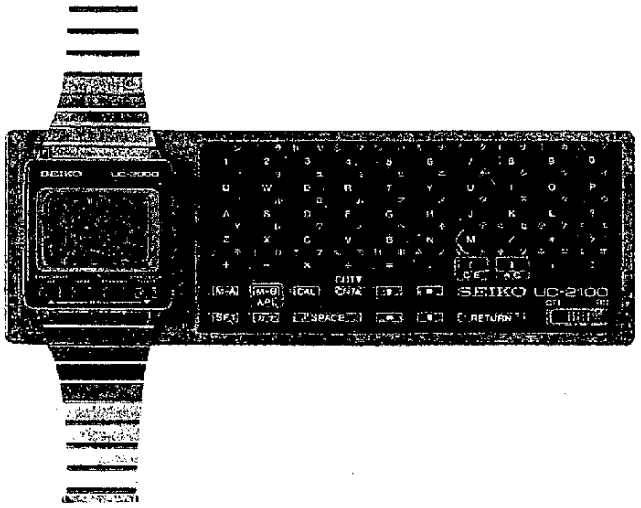
2．リストコンピュータ UC2000

1984年に商品化したUC2000は４つの品種から構成されるシステム商品であった。

- UC2000リスト部：リストコンピュータ本体
- UC2100キーボード部：携帯情報入力装置.
- UC2200コントローラ部：卓上情報演算入出力装置
- UC2300インターフェースアダプタ：PC－リスト間情報転送用インターフェース装置

特徴

- 無線転送によるデータ入出力方式
- フルドットマトリックスLCDによる表示
- アプリケーションプログラムの変更



図B.3-1　UC2000とUC2100

・5個のLSIを搭載した高密度実装
・インターフェース装置を介してホストコンピュータとデータ交換可能

以上の特徴は現在であれば全く当たり前の内容であるが、1984年当時、これらの機能を腕時計サイズで実現したのは画期的なことであった。

現在の携帯情報端末の課題でもある数少ないスイッチによる英単語の綴り入力等の不自由な操作性については、電磁結合無線通信を利用した携帯情報入力装置（UC2100）で解決していた。

3．ウェアラブルPC Ruputer

1998年に商品化したRuputerの外観を図B.3-2に示す。

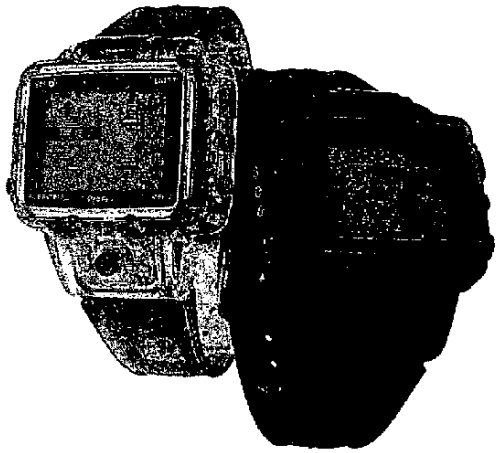


図 B.3-2　Ruputer Pro4

3．1　Ruputer の特徴

・最大4Mバイトの大容量フラッシュメモリを搭載
・完全なPCアーキテクチャーで、アプリケーションはパソコンを通じて追加、削除が可能
・IrCOMM対応で赤外線通信が可能
・既存のPC・PIMソフトとのデータリンクが可能
・アプリケーションプログラム開発環境を無償提供

以上の特徴を持ったRuputerはスタンドアローン型ウェアラブルPCとして、ハードウェアとしては完成されたと言える。

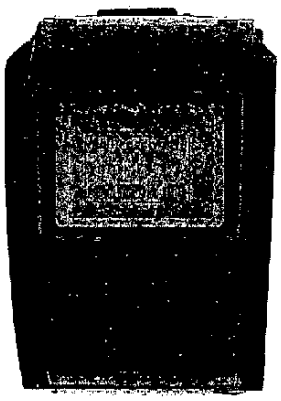
課題としては、下記のポイントが考えられる。

①更なる小型化薄型化の実現
②オンデマンドで無い通信への対応
③ローパワー化の促進

4．ユビキタスコンピューティング社会に求められる携帯情報端末

ユビキタスコンピューティングには必然的にネットワークへの接続機能が求められる。ユビキタス・インターネットと言う言葉もあり、家庭やオフイスだけでは無く、今後、飛躍的に設置数が増大するホットスポットへの接続機能は必須になる。接続技術としては、赤外線通信、Bluetooth,無線LAN、HomeRFなどのコードレス化が可能なものが必要不可欠になる。この中で低消費電力で高速な赤外線通信は、小型携帯情報機器にとって魅力的ではあるが、その限定的な指向性はオンデマンド通信向きである。接続を意識しないということでは、やはりRF（Radio Frequency）の利便性が高い。小型携帯情報機器用のRF技術としては、IEEE802.11ｂの無線LANに押されぎみで、当初の普及予測よりペースダウンしているが、低消費電力であることからBluetoothに期待感が強い。

Bluetoothを利用したウオッチの可能性の検証とマーケティングリサーチを目的として、セイコーインスツルメンツ（株）が試作したBluetoothウオッチを図B.3-3に示す。



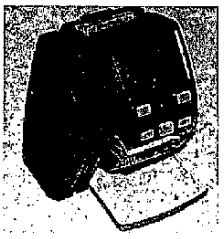


図 B.3-3-1　試作 Bluetooth ウオッチ

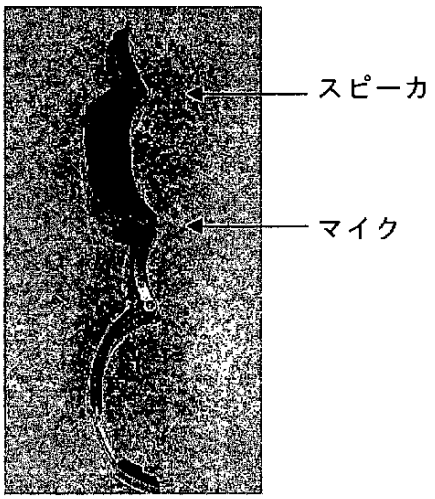


図 B.3-3-2　Bluetooth ウオッチバンド開いた状態

試作したBluetoothウオッチは、携帯電話やPC、AV機器、家電等とのネットワークを想定して下記の様な機能を搭載した。

・Bluetooth携帯電話とのリンク
・インターネットブラウザの搭載
・家電等のリモートコントロール機能

試作したBluetoothウオッチの大きな特徴として、マイク、スピーカを搭載し、音声コミュニケーションをサポートしたことが上げられる。これによりBluetooth搭載電話のハンドセットの機能を提供することが出来た。将来のIPv6/VoIP（voice over IP telephon）技術により、リスト型IP電話も可能となる。さらにウオッチ側から携帯電話をATコマンドで制御する仕組みを盛り込むことで、単なる通話機能だけで無く、電話着信時に相手先の電話番号の表示や電話番号の検索などの電話機側の機能をウオッチ側でも実現する事が出来た。また、大きな特徴として携帯電話と同じ通話スタイルを提供する目的で図B.3-3-2に示す様に通話する時には腕から外して、普通の電話機のように話せる方式を採用した。

試作したBluetoothウオッチは、ユビキタスコンピューティングが求める携帯情報端末の姿を具現化した一つだと思う。無線接続技術をもっとデータ伝送範囲の広い携帯電話接続やPHS接続に変更することも消費電力的な課題はあるが、技術的には容易である。これらの携帯情報端末のCPUパワーを増大させ、目的の機能を実現する為の専用ハードウェアを用意すれば、何でも出来ると言っても過言では無い。

この何でも出来る方向は、スリムノートパソコンやモバイルパソコンに任せ、操作スイッチの数が限定される小型携帯情報機器は、機能を明確にしたアプライアンスに特化して行くべきだと考えている。アプライアンスの例としては、ホットスポットから配信される情報を見るビュアーや、いつも身に着ける事が可能なことから生体情報センサを備えたものが有望であると思う。

５．アプライアンス例

５．１　脈拍計

日常生活の中で連続的に脈拍が計測可能になるとその効用と利用範囲は広い。例えば心疾患者のモニター等は重要な用途である。従来から日常生活下での心拍数（心筋を緊張させる電気信号）を電極で検出して測定していた。心拍信号によって心筋が緊張して心臓がポンプとして作動した結果である脈拍数は、活動中の連続計測が出来なかった。これを世界で初めて実現したのがSEIKO PULSE GRAPHである。

図B.3-4に運動中の心拍信号（心電波形）と脈拍（脈拍波形）の一例を示す。安静状態であれば、胸部電極で検出した心電波形から求めた心拍数と指尖部で光学的に検出した脈拍波形（脈波波形をある閾値で矩形派変換した変換波形）から求めた脈拍数とは一致する。しかし運動中では、運動による加速度で血流が乱れることにより図5の例に示す様に心電波形から求めた心拍数と脈波波形から求めた脈拍数が120拍と98拍と異なって来る。胸部電極で求めた心電信号は、運動中でも筋電位が雑音になる事も無く安定に測定可能である。

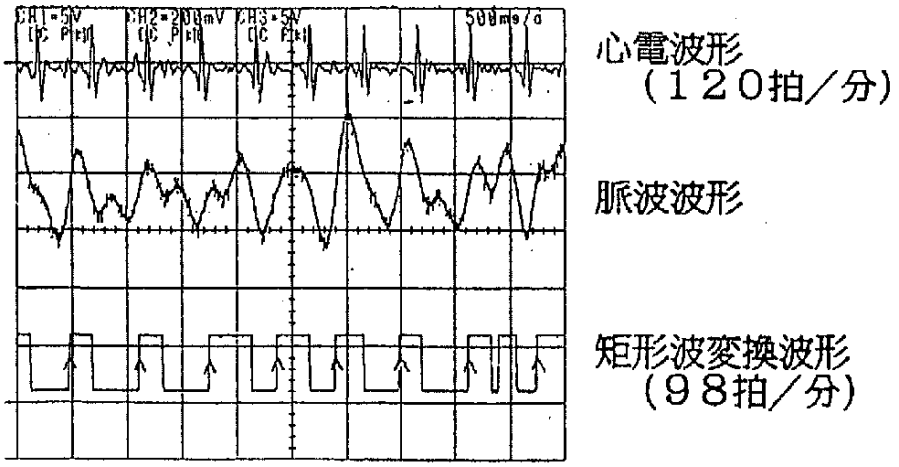


図 B.3-4　運動中の心電波形と脈波

ただ心電信号を得る為には胸部電極が必須になる。

SEIKO PULSE GRAPHでは、手首周辺から得た脈波波形から脈拍数を求めるために脈波波形の周波数分析をFFT（Fast Fourier Transform）処理によって行い、運動による体動周波数と脈拍周波数を切り分けて脈拍周波数から脈拍数を求めている。この方法は周波数分析にFFTを使用しているために、非定常周期の運動には対応出来ない課題があるが、ユビキタスコンピューティングのアプライアンスの一つとして有望だと思われる。

５．２　体動モニター

「こころの病」では身体活動パターンに異常が見られることが知られている。事実、米国精神医学会による「精神疾患の診断統計マニュアル(DSM-Ⅳ)」においても実に30種の精神疾患の診断基準に身体活動の異常に関する記述が含まれている。このような異常を定量的、経時的に評価するため、加速度センサーを用いた研究が行われている。日内の活動パターンと心の関係は、まだ研究が始まったばかりであるが、その因果関係が明らかになればこれもアプライアンスの一つとして利用できる。

６．セイコーインスツルメンツ株式会社の取り組み

当社のeソリューションビジネスユニット（eSBU）は「革新的なソリューション（製品とサービス）を提供し人と情報をつなぐネットワーク社会に貢献する。」を事業ミッションに活動している。

６．１　ネットインフラ/プラットフォーム

・時刻配信/認証サービス(Chronotrust)
・無線データ通信端末（PHSカードなど）

6．2ネット端末/アプライアンス

・携帯情報通信端末
・ウェアラブル情報通信端末
・特定用途向け注文入力端末・決済端末
・ハードディスクセキュリティモジュール(SecureDiskProtection)

6．3　ネットサービス

・外食産業向け店舗総合システム・サービス
・クレジット/デビットカード決済サービス(CREPiCO)
・携帯電話コンテンツ・サービス

7．まとめ

本格的なユビキタスコンピューティング社会の到来が目前に迫って来ている。われわれセイコーインスツルメンツ（株）は、ウオッチの開発製造技術で培った携帯情報端末をベースに特色ある端末開発を行うと伴に、単なる端末開発製造の枠に留まる事なく、需要者が最高のサービスを享受できるソリューションを提供して行きたい。そして来るべきユビキタスコンピューティング社会に貢献して行きたいと考えている。

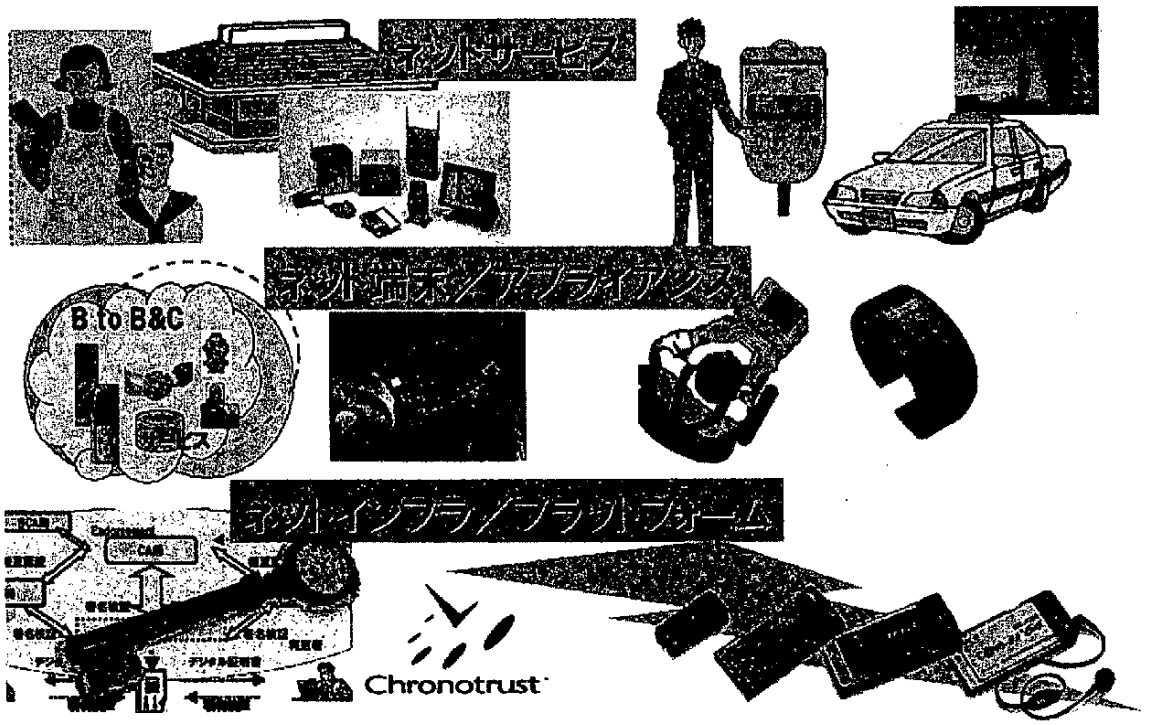


図 B. 3-5　SII e ソリューション･ビジネスユニットの製品とサービス

B．４　（株）東芝ディジタルメディアネットワークカンパニーのユビキタスコンピューティング関連ビジネスの取組み

１．ユビキタスコンピューティングの骨子

ユビキタスコンピューティングの骨子は以下の６点である。

1）オフィス/ホーム/パブリックエリアにおけるモバイルデバイスのユビキタスネットワーク環境を展開する。
2）IP ネットワークでは、IEEE802.11 を中心として、無線ネットワーク化を推進する。
3）パーソナルエリアでは、Bluetooth を中心として、無線化ネットワーク化を推進する。
4）ユビキタス環境の整備を推進するため、パブリックエリアにおけるインターネットアクセスサービスを推進する
5）ホームネットワークを推進するため、ホームサーバを中心に家電をネットワーク化を推進する
6）モバイル化を推進するため、それぞれのエリアをシームレスに接続するネットワーク化を推進する

２．デバイスのユビキタスネットワーク化推進

モバイルコンピューティングを推進するため、ノート PC のすべてのシリーズに無線 LAN 内蔵モデルを準備。

Pocket PC（PDA）にも無線ＬＡＮ内蔵モデルを準備。部門サーバには、無線 LAN アクセスポイント機能をオプションで準備し、ネットワークの無線 LAN 化を推進する。

３．Bluetooth によるパーソナルエリアネットワークの無線化

ヘッドセットや、マウス、キーボード等パーソナルエリアに存在し、従来ケーブルで接続されていたデバイスを、Bluetooth によって無線化を推進する。無線化することにより新しいスタイルを想像する。

４．パブリックエリアにおけるインターネットアクセスサービス

モバイルデバイスの無線ネットワーク化を進めるとともに、その無線ネットワーク化されたモバイルを生かすためパブリックエリアにおけるインターネットアクセスサービスを推進する。

パブリックエリアのインターネットアクセスサービスを展開する際のブレイクスルーは導入コストと考えている。サービスのコストを抑えると共に、導入コストを低くすることにより、個人経営のようなカフェでもサービスを展開できることがポイントと考える。

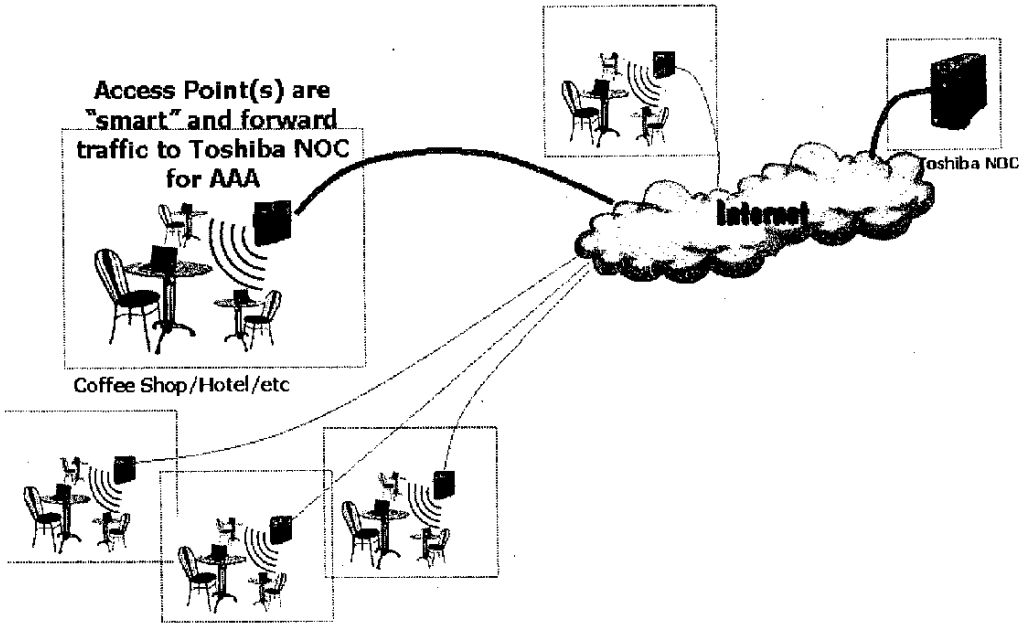


図 B.4-1　パブリックインターネットアクセスサービスの構造

導入コストを低く抑えるため、独自の機能を持つルータアクセスポイントを開発。1 アクセスポイントの導入コストを$200 にすることを可能にした。

東芝アメリカインフォメーションシステムズのインターネットアクセスサービス形態の構成図を図 B.4-1 に示す。

5．情報家電のネットワーク化

冷蔵庫や洗濯機といった白物家電、ディジタル TV や DVD プレーヤと言ったディジタルＡＶ機のネットワーク化を進める。そのネットワークを、ホームサーバがゲートウェイとしてホームネットワークをまとめる。

ネットワーク化することにより、機能の融合を図り新しいライフスタイルを想像する。特に、無線技術を積極的に進め、家庭内においても、モバイル、ポータブル環境を構築する。

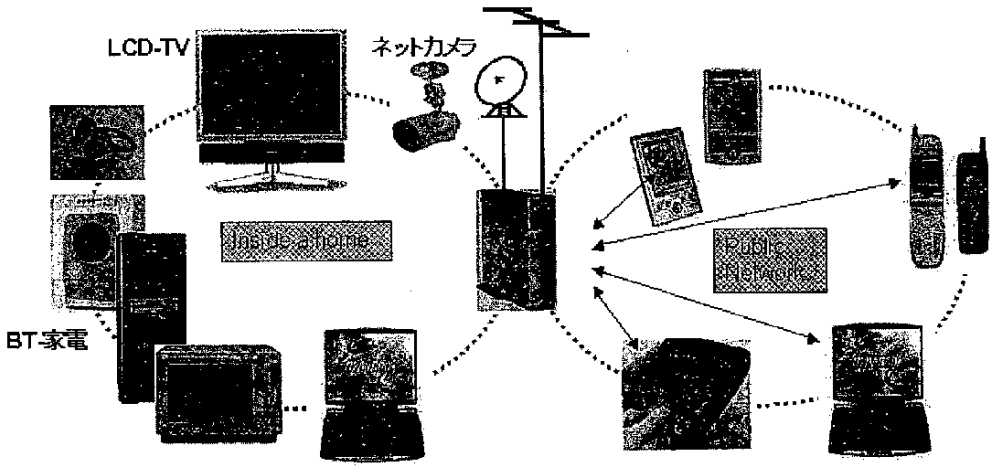


図 B.4-2　ホームネットワーク構成

B．5　富士通（株）のユビキタスコンピューティング関連の取組み

富士通（株）は、ICカード・RFID、無線LAN、携帯電話などユビキタスコンピューティングに関連する様々なソリューション提供と研究開発を実施している。本項ではその中で特に富士通研究所が九州大学および富士通プライムソフトテクノロジ（PST）とともに実施[1]している研究開発および実証実験について紹介する。

この研究開発および実証実験は、異なるセキュリティポリシーで運用されるP2Pネットワークが接続されたとき、それぞれのP2Pネットワークにおいて守られるべき安全性・整合性・信頼性が損なわれないようにするための方式およびシステム基盤の構築、標準化推進を目的としている。背景には、ユビキタス情報環境においてパソコンだけでなく携帯電話・PDA・情報家電などすべての情報機器がP2Pモデルを利用しながら情報交換を行なうネットワークシステムになる可能性があるにもかかわらず、現在のP2Pモデルでは、P2Pネットワークとしてのサービスの規定方法、信頼性・安全性に関する運用管理方法、異なる運用管理に基づくP2P間の通信規約や安全性の保障に関して具体的で合意のとれた方法論や規約が存在せず、その結果として、最終的なサービスの管理制御という重要な問題に対する解決方法が与えられていないことにある。富士通・九州大学・PSTは共同で、P2Pネットワークのセキュリティを検討する土台としてのネットワークアーキテクチャモデル、2Pネットワークという非集中型の分散ネットワークの中にポリシーによって規定されるP2P信用ドメインの構築を目指すプラットフォームの実装、そして実証実験を実施している。

P2Pネットワーク・アーキテクチャの検討においては、九州大学で開発したマルチエージェントシステムKODAMAのアーキテクチャをベースとし、KODAMAで導入したエージェント・コミュニティの概念をポリシに基づくP2P論理ネットワークの構成として応用している。KODAMAにおけるエージェントは、非循環な有向グラフ構造で構成されたエージェント・コミュニティに所属し、エージェントの名前付けはコミュニティを形成する階層構造によって与えられている。またエージェント・コミュニティの概念をポリシーに基づくP2P論理ネットワークに応用するためには、エージェント・コミュニティのそれぞれに対しポリシーを割り付けるというアプローチを取っている。このようなアプローチを採用することで階層的なコミュニティに属するエージェント群というKODAMAのアーキテクチャを、階層化されたポリシに属するピア群と対応させることができた。またKODAMAにおいてエージェント間のメッセージ通信に用いられていた名前付けの関係を、異なるポリシーに属するピア間の関係として対応させることが可能となった。このことは、KODAMAにおけるエージェント間のメッセージ通信経路の表現によって、異なるポリシに属するピアの関係を表現するというアプローチをとることが可能であることを意味している。このような通信経路の表現とポリシネットワークとの表現の対応関係は、異なるポリシーに属するピア間のメッセージ通信における制約条件として利用することができる。またこの対応関係はポリシ関係経路が与えられたときのセキュリティ条件のチェックとして利用することができる。さらに、KODAMAにおけるブロードキャストとパターンマッチとを用いた相手エージェント名とその経路の探索は、ポリシー空間におけるP2Pネットワーク間可能範囲の探索として利用することが可能となる。

プラットフォームについては、広域分散型の認証基盤として、個体認証、属性認証、ポリシー定義をそれぞれ異なる分離された権威機関が行なうモデル を用い、耐タンパデバイス内に保管した属性証明に係わる情報と口コミ型に他のユーザに渡されていくコミュニティ定義のポリシーとの照合によってコミュニティ内のロールが割り当てられる Virtual Private Community（VPC）プラットフォームを実装した。このプラットフォームは耐タンパデバイスとしてのICカードのJava Card上にロール割り当て機構を持ち、試験に用いているPDA側のコア部分実装も50 KB以下として携帯電話への適用を意識し、かつ複数端末上での分散協調が可能なアーキテクチャを用いることでさらに非力なデバイスとの連携動作も可能なものとしている。VPCプラットフォームのモデルではロール割り当ての操作がすべてユーザ側の耐タンパデバイス上で行われるために、プライバシー保護との整合性も高い。

2002年3月には、VPCプラットフォームを用いた実証実験をPST社が名古屋栄町で実施した。実験は、300m×100m規模の地下ショッピング街にIEEE 802.11bの無線LANを敷設し、PDA数十台を貸し出しながら、実際に一般モニタを募り、約2週間にわたって実施した。実験では地下街10ヶ所に設置した無線LANアクセスポイントからアクセスポイント近辺の店舗情報がポリシとセットとなったコンテンツを配信すると同時に、ユーザ間での口コミ型のコンテンツ交換を行った。配信されるサービスポリシをユーザ側の属性情報によって判定することで、ユーザ毎に属性に応じたアプリケーションが起動されると同時にプライバシー保護にも留意した実験を行うことができた[2]。また2003年3月からは名古屋大須商店街において、携帯電話とRFビーコンによるトリガーとを組み合わせた実験を実施している。ただしこの実験では異なるポリシー間のメッセージ配信を主眼として開発を実施したため、RF ビーコン部と個体認証との区別についての留意が弱くなってしまっている。プライバシー保護にも留意し、これまでの実験結果を踏まえた総合実験は2003年下期に実施する予定である。

図 B. 5-1　名古屋大須商店街

【参考文献】

〔1〕2002年3月プレスリリース，『広域ホットスポットエリアを対象とするP2Pコミュニティサービスの実験』，http://pr.fujitsu.com/jp/news/2002/03/27-1.html

〔2〕Iwao etal., "Virtual Private Community System[3]", Sixth International Workshop CIA-2002, http://www.dfki.de/~klusch/cia2002.html

[3] CIA System Innovation Award 2002を受賞

B．6　松下電器産業（株）のユビキタスコンピューティング関連ビジネスの取組み

1．ユビキタス・ネット家電のコンセプト

（1）ネット家電インターネットが新しい価値を提供

a．ネット家電時代の幕開け

まず最初にネット家電の動向、ユビキタスとの関わりについて概観すると、90年代に爆発的に発展したインターネットにアクセスする人数は、2000年以降の需要予測の示す通り2000万人を超えて急激に増加している。最近では「iモード」の普及により、ノンPCでのネット活用も急速に見えてきて、2003年には国民二人に一人はネット端末を持つ時代が来る。

2005年には、私たちは、いつでも・どこでも・簡単・便利にインターネットに接続できるユビキタスネットワーク社会つまり蓄積型情報ネットワーク社会の到来を想像することができる。

この時代を第2期インターネット時代またはネットCE（ネット・コンシューマエレクトロニクス＝家電）の時代と当社では位置付ける。2005年までは、ネットCEとそれを支えるキーデバイスを松下の重要な技術戦略として全力で取り組む。

そして、パソコンに携帯電話、TVなどのノンPCを加えたネットCEのビッグバンが、私たちの暮らし・文化のみならず、世の中を激変させる様になると考える。

また、環境・エネルギーなどの環境共生技術もわが社の製造業の将来を支える基盤である。

（2）ブロードバンド、ユビキタス、常時接続環境

a．ユビキタス、ブロードバンドの特徴

それでは、最初にネット家電の動向、ユビキタスとの関わりについて概観してみたい。

- 「ブロードバンド」は広帯域と言う意味であるが、ネットワークが高速化するのに伴い、テレビ放送並みの映像がインターネットを通じてオンデマンドで利用できたり、より高精細な映像や3D映像が利用できるようになる。これにより、相手の表情をリアルに読み取れるネット対面サービスや、3D映像によるeコマース、インターネット放送などが一般化していくことになる。
- 「常時接続、ピア・ツー・ピア」においては、PCからモバイルやネット電話、テレビ、白物、カーナビなど、すべての機器がインターネットへ常につながっている状態となる。これにより、常時情報サービス、常時コミュニケーションが可能となり、人と人、人と情報、人と企業などがより密接に結ばれる。人と人とのコミュニケーションに至っては、話をしていなくてもつながっているだけで価値があるような現象が出てくる。

b.ユビキタス・ネット家電時代へ

家電機器のデジタル化はマルチメディア家電と称された 1999 年にデジタル携帯電話がインターネットに接続されることによってネット家電と呼ばれるようになった。電話やFAX もすべてインターネット接続機能がついてきた。デジタル TV もインターネット接続機能がやがてついてくる。

AV 機器および携帯端末のインターネットを介した動画を扱うようになり、これがブロードバンドネット家電の登場である。

さらに、ワイヤレスの普及と共にネット家電がワイヤレスでネットワーク化されるようになると、モバイル機器やネット家電を介して、「いつでも、どこでも、誰とでも」、簡単に、そして便利なサービスが利用できます。これがユビキタス・ネット家電の誕生である。当社は「我々がユビキタスネットワーク社会の入り口に立つのは、2005 年から 2006 年あたり」と考えている。

こういったブロードバンドインフラを背景に、それぞれの場面（コンテンツ・パブリックインフラ・ホーム空間等）でサービス選択やアクセスも選択も含めて、ニーズや状況に応じたユビキタスな情報環境が実現する。これが当社が目指すトータルネット家電アーキテクチャのベースとなるものである。

c.新ネット家電サービスの創造

ネット家電時代のサービスは、個々のネット家電端末がインターネットを介して享受するものである。つまり、情報がインターネットを介して端末に届けられる。

ユビキタスネット家電の時代になれば、個々の端末の機能は別な端末から操作可能になる。つまり、情報とその情報を扱う端末の機能が一緒にインターネットを介して送られるようになる。

これにより、ユビキタスネット時代のサービスの形態は、①ピアツーピアのカスタマイズ②ユビキタスコンテンツサービスという２つの価値の提供が中心となってくる。

2.松下電器のユビキタスネット家電

（1）AV 機器のネットワーク化

a．AVC ネット家電システム

AVC ネット家電のシステム概念については、ネットワークタウ（仮称：メインヒューマンインターフェース）を通して、デジタル放送への対応は勿論、ブロードバンド化されたインターネット通信網との接続により、TV 番組を見ながら TV 向けのサイトの閲覧や、介護や教育など、生活に関する様々なサービスが受けられるようになる。

そして AVC サーバ（仮称）は大容量ハードディスクマルチフォーマットな DVD-RAM ディスク、マルチ入力インターフェース機能等を持つホームサーバで、テレビ放送は勿論、デジカメ画像やムービー映像など、くらしに関わる様々な AVC データを記録・保存する。

また、プラズマディスプレイ、デジタル TV、など様々な機器へ最適なフォーマットで出力したり、色々な機器から同時にアクセスしそれぞれが違うコンテンツを楽しむことなどもできる。

b. PCに続いて、DTV（デジタル・テレビ）がサーバになる

近い将来、家の中にある情報機器や家電製品を相互接続して、より便利に使えるようになる時が来る。

その際、いろいろな機器の中心にあってネットワークの要となるコンピュータあるいはコンピュータ的な機器をホームサーバと言うことができる。

これまで家庭のネットワーク化はPCによる通信だけでしたが、デジタルテレビにより放送と通信が融合する拡張されたネットワークが家庭に導入されることとなった。

従って、ホームサーバは従来のPCサーバに加えて、デジタルTVがその拡張性を活かして活用されるようになる。

つまり、すべてのIPネット家電は、将来、サーバ型になる可能性を持っていると考えられる。従って、HGW（ホームゲートウェイ）、くらしステーション、電話などもサーバ型機器になっていくであろう。

c. モバイル端末もサーバになる

エリクソンの調査によると、モバイル機器の総数が2003年にはコンシューマPC台数を追い抜き、モバイルウェブユーザが2005年には10億人を越えると予測している。
記憶機能を持ったネット家電はサーバ型に進化し、モバイル端末もサーバ型に進化するであろう。

松下電器が目指すネット家電アーキテクチャによれば、家の中の4ドメインは家の外のモバイルあるいはカーのサーバ間で、自在なネットワーキングが可能となる。

（2）白物家電のネットワーク化

a. 白物ネット家電システム

白物ネット家電のシステム概念であるが、ECHONETの特小無線を用いて、情報コントローラとネット家電機器群が連携する。

くらしネットワークでは、家庭内の白物家電をネットワークでつなぎ、便利で快適しかも安心できるくらしづくりをサポートする。エアコンや洗濯機の制御および電子レンジのレシピのダウンロードなど行うことができる。

また、くらしネットワークとインターネット網の接続により、外部からの家電機器の自動保守点検や環境共存型のエネルギー管理など様々なサービスの提供が可能となる。

b. ホームネットワークの基本モデル

松下電器の目指すネット家電アーキテクチャの家庭内部分、すなわちホームネットワークについては、先ほど示したゲートウェイステーションがこのHGWに対応する。また、エコーネットはこの図ではくらし環境で活用されるサービスとなる。

ホームネットワークの基本モデルは図に示すように、ゲートウェイ、IPネット家電、ネット家電の3段で構成される。そして、ゲートウェイとIPネット家電の間はインターネット・プロトコル（IP）で一本化し、IPネット家電と各ドメインに含まれるネット家電との間は、ドメイン毎の標準プロトコルを用いるというものである。

（3）セキュアな技術基盤

a. セキュアなネット家電の時代

いわゆるデジタル家電からネット家電への移行に際しては、デジタル信号処理・ヒューマンインタフェースを中心にソフト開発量の加速的な増加が、また次世代のセキュアな家電のレベルでは本格的なネットワーク機能の増加が見込まれる。

b．パッケージ系著作権管理技術体系

デジタル記録が本格化して以来著作権保護が重要な課題となっている。松下電器はDVDで本格的なコピーコントロールのための暗号化技術を開発し、実用化した。またオーディオ、ビデオ信号には更に高度な電子透かし技術が採用されつつあり、本格的なコンテンツ保護技術が整いつつある。

著作権保護のためにはこれらの技術はコンテンツ事業者と協調してトータルな著作権管理技術として体系的に活用されなければならない。松下電器は他社とも協力して業界内で率先して著作権保護技術の確立に取り組んでいる。

c. ネット家電機器の機能

家電機器のデジタル化が進み、ネット家電へ進化するにつれて、機器の機能は増大し始める。そして、機能の爆発とも言うべき状態に遭遇することになる。

アナログの家電機器がデジタルネットワーク家電になると機能は１桁ほど増加し、リモコン操作の限界を招く。この段階では操作支援が必要になる。

そして、デジタルネットワーク家電が相互に連携し始めるようになると、機能はさらに１桁ほど増大し、情報論的アプローチによるインタフェースの限界を招くことが予想できる。この段階では知的支援が必要になる。

またネットワークに関係する操作支援と知的支援を確立するには、ネットワーク・ヒューマンウェアというような概念を明確にしなければならない。

d.「トータルネット家電アーキテクチャ」

以上述べてきたように、当社が考える「ユビキタス・家電のコンセプト」は、著作権管理の仕組みを持つ様々なコンテンツ（テキスト情報・映像・音楽等）を、各分野（行政・医療・交通・金融・流通等）のサービス選択（提供サーバ）を通じて、放送網・有線通信網・移動通信網等のアクセス手段によりインターネット&ブロードバンドのパブリックインフラ空間経由で、一般消費者が享受できる環境である。

それからホームネットワークインフラ経由でホームゲートウェイを通じて、ホーム空間に入ったコンテンツは、有線・無線の宅内ネットによりIP家電（STB／PC／電話・FAX／くらし情報コントローラ／モバイル機器等）から蓄積メディア&機器間ネットワークでネット家電に接続されてオンデマンドに有効利用されることとなる。そしてこれらが当社が目指す「トータルネット家電アーキテクチャ」となっている。

Ⅱ．資料編

C．ユビキタス情報環境
および
セキュリティ関連プロジェクト

C．1　ユビキタス情報環境関連研究の動向

UBICOMP2002 参加報告（竹林洋一静岡大学教授）

1．　概　要

スウェーデンのゲテボルグ（Göteborg）で 2002 年 9 月 29 日から 3 日間にわたり開催された UBICOMP2002（International Symposium on Ubiquitous Computing）に参加した。2001 年 10 月に米国アトランタで開催された UBICOMP2001 に続いて 2 回目の UBICOMP であり、前身の HUC99(International Symposium on Handheld and Ubiquitous Computing)から数えて 4 回目にあたる。報告者は UBICOMP2001 と 2002 のプログラム委員を務めているが、2001 年は米国の航空機テロ事件のため参加できなかったので、今回の参加は初めてであった。UBICOMP2002 は、初日のワークショップと本会議という構成であり、米国、欧州、日本から約 500 人（昨年の 2 倍強、日本から 20 人参加）の研究者が参加した。発表件数はフルペーパ 15 編（採択率 12/135）、ショートペーパ 14 編（14/50）で、研究の広さと水準という意味でもユビキタスコンピューティングに関する世界最高峰の国際学会となった。

1 日目は日曜日であったが、ワークショップ開催された。本会議の論文発表よりも萌芽的な研究が多く異分野研究者が参加し、下記の 9 つのテーマについて九つの小さな部屋に分かれて熱心な討論が行われた。

1) Collaboration with Interactive Walls and Tables
2) User centered Evaluations for Ubiquitous Computing Systems: Best Known Methods
3) Supporting Spontaneous Interaction in Ubiquitous Computing Settings
4) Emotions in the World
5) UbiCog '02: First International Workshop on Ubiquitous Computing for Cognitive Aids
6) Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing
7) Security in Ubiquitous Computing
8) Concepts and Models for Ubiquitous Computing
9) Design and Evaluation of Notification Interfaces for Ubiquitous Computing

上記のワークショップには、Emotion（感情）、プライバシー、セキュリティ、自由な（Spontaneous）インタラクション、インタラクティブな壁とテーブルなどが含まれており、Ubiquitous Computing の研究が多様性に富む発展途上の研究分野であることが分かる。

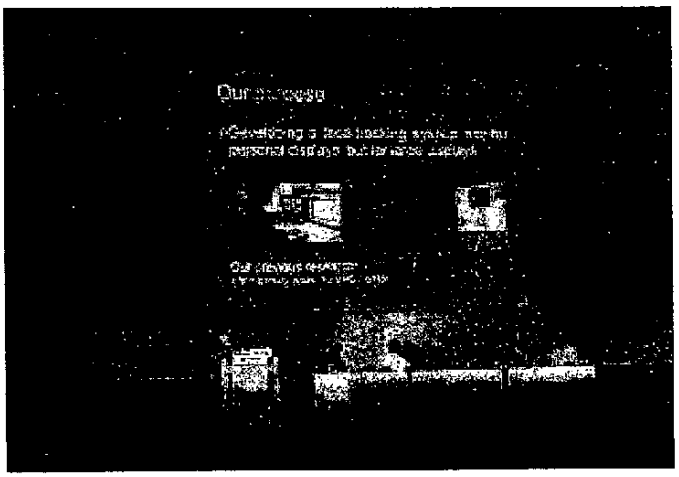
講演発表は、北欧の映画祭に使用する映画が上映される会場で、でシングルトラック（パラレルセッションなし）で行われた。因みに下記のようなセッション名が付けられていた。

1) Mobile and Context-Aware Systems
2) User Studies and Design
3) Perceptual Interfaces and Responsive Environments
4) Sharing and Accessing Information – Public and Private
5) Location, Location, Location
6) Sensors and Applications

このセッション名からもわかるように、モバイル,アウェアネス,PUI (Perceptual User Interface)、位置情報処理、センサなどヒューマンインタフェースや実世界指向インタフェースの応用に関係する発表が多い。

採択された論文は分野が多岐にわたるため、プログラム委員の専門外の論文を査読する場合があり、厳しい競争を経て採択された素晴らしい論文に混じって、時々首を傾げたくなるような論文の発表も散見された。研究の「価値」の判断基準が難しい。採択された論文はケンブリッジ大、ランカスタ大、ワシントン大/インテル研究所、ETH Zurich、MIT に集中しており、日本からのは角氏（ATR)、中西氏（電通大）の論文は内容が充実していて好評であった。

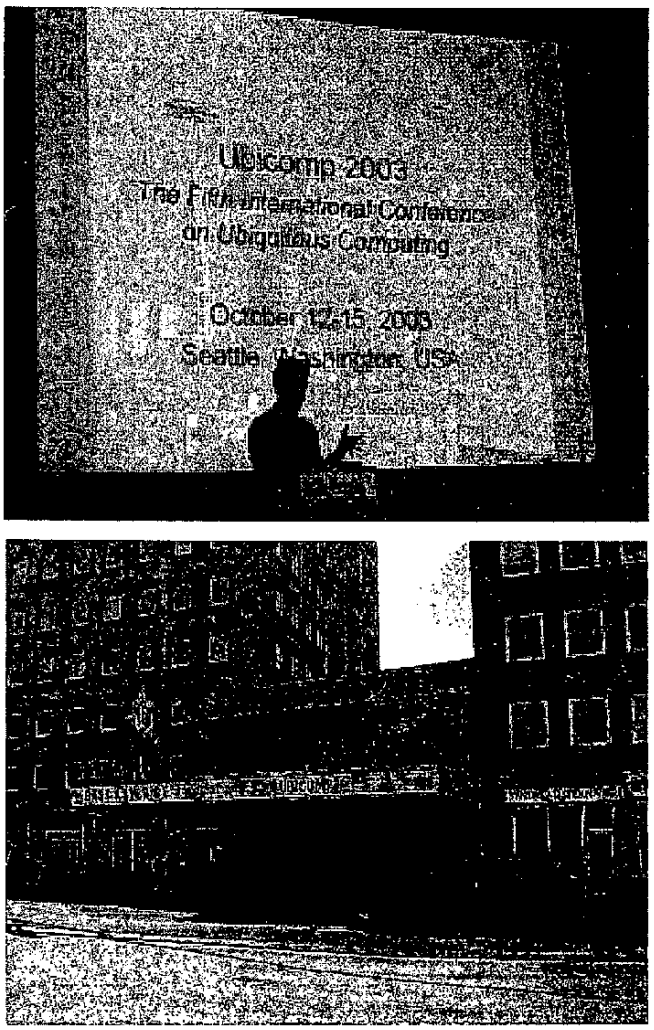
EU 横断の Ubicuitous Computing 関連の大型プロジェクトである The Disappearing Computer のデモ展示があり、進行中の様々なプロジェクトの担当者と意見交換できて有益なインタラクションの場となっていた。その他、ユビキタス・コンピューティングの研究の歴史を懐かしい映像で振り返る企画は、会場となった 1980 年代のオリベッティのコンセプトデモを初め随所で拍手喝采が起こるなど、印象的であった。次回は米ワシントン大とインテル研究所がホストとなり、米シアトルにて 2003 年の 10 月 12 日から開催される。



中西氏の発表

会議開催中に Ubicomp 運営に関するタウンミーティングが開かれ、プログラム委員の福本氏（ドコモ）と角氏（ATR）と報告者が参加し,Ubicomp の発展にはアジアの協力が必要との意見が出たので、筆者が 2004 年度は日本で開催することを提案し基本的に了承された。UBICOMP2004 の日本開催は、閉塞状態に陥っている日本の情報通信産業を活性化する起爆剤になる可能性がある。日本のお家芸の情報家電や機器デバイスのハードウェア技術とソフト・サービス・コンテンツ技術を融合すれば、新しいユビキタスコンピューティングの研究と産業の発展・成長も可能である。

UBICOMP2002 に先立って 8 月末に、チューリッヒで開催された Pervasive2002 (http://www.pervasive2002.org/) は、IBM 主催のシンポジウムを発展させ、IBM と ETH Zurich（スイス連邦工科大学チューリッヒ校）が共済したものである。参加者は約 120 名と小規模であったが,論文の採択率は約 1/8 と激戦だったとのことである。Pervasive Computing は IBM チューリッヒ研究所が標榜してきた次世代情報環境のコンセプトであり、IBM 事業領域との関連から"Pervasive"は、情報技術やインフラをコアにしているのに対して、Xerox 社の Weiser が提唱した Ubiquitous Computing はヒューマンインタフェースの色彩が強い。このため"UBICOMP"は、ACM の SIGCHI や Wearable 関連の研究



会場となった Draken Theater

者が多く、ヒューマンインタフェースやCSCW(Computer Supported Cooperative Work)など、人間や機器デバイス・インタフェースに重きを置いているのが特徴である。このため、プログラム委員の構成も Pervasive2002 は現実世界寄りのシステム研究者が多く、Ubicomp2002 は要素技術やヒューマンインタフェースに関わる研究者の比率が高い。上記のワークショップには、Emotion(感情)、プライバシー、セキュリティ、自由な(Spontaneous) インタラクション、インタラクティブな壁とテーブルなどが含まれており、Ubiquitous Computing の研究が多様性に富む発展途上の研究分野であることが分かる。

2．ワークショップ参加報告

9つのワークショップの中でプライバシーとセキュリティ関連の二つのワークショップについて次に述べる。

2.1 Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing

2．1．1 概要

報告者が参加した掲題のプライバシーワークショップは UC Berkley の John Canny 教授ら二人の博士課程の学生が精力的に活動し、議論の進行を仕切っていた。11月に米国ニューオリンズで開催される CSCW2002 でもプライバシー関連のワークショップを提案しているとのこと。ユビキタス情報社会におけるプライバシー研究の成長を睨んでおり、若手研究者が活躍するチャンスも多い。学生のうちの一人は日立 μ チッ プソリューションのコンサルティングをした経験もあり、ビジネスを含めてアプリケーションを検討しているとのこと。CSCW 研究がバックグラウンドのようであり、社会学的な視点から議論を展開していた。

参加者は多彩で経済学者の発表もあった。共通の問題意識として、サー ビス関連企業が個人情報を必要以上に収集しており、インターネットの世界で個人情報の漏洩や悪用に関する危険性が潜んでいる。今後発展するユビキタス情報環境では、ユーザの ID や位置情報など様々な場面で多様な個人情報が行き来するので、プライバシー保護の重要性は格段に高まる。

2．1．2 各部ごとの内容と感想

(1) Privacy - The User Experience

"Privacy Invasions in Ubiquitous Computing"

Marc Langheinrich

Swiss Federal Institute of Technology, ETH Zurich

・EU の Disappearing Computer Initiative プロジェクトの Privacy 研究のキーマンの講演。NEC の研究所に在籍経験があり、日本語が達者。Privacy はプロジェク

トの全てと関係していると力説。
・プライバシーの影響と侵害について包括的に講演.
・空間を超える侵害、組織を超える侵害、時間を超える侵害、うっかりした侵害、フォーマルな分類ではないが、参考にはなる.

(2) Economics and Privacy

"On the Benefit of Behavioral Privacy Experiments in Commercial Ubiquitous Computing Environments"
Jens Grossklags
University of California, Berkeley
・経済学もプライバシーと関係するということが興味深い。

"Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments"
Alessandro Acquisti
University of California, Berkeley
・ユビキタス情報環境下のプライバシー管理・公開は経済へも影響することは確実。

(3) Legal Principles and Privacy

"The Benefits of the Legal Analytic Perspective For Designers of Context-aware Technologies"
Annie Jacobs
Georgia Institute of Technology
・ユビキタスコンピューティングシステムを設計する際に、ヒューマンインタフェースの研究で盛んになっているアウェアネス技術の観点から、法的、道徳的側面を検討していた。

"Adopting Fair Information Practices to Low Cost RFID Systems"
Simson Garfinkel
MIT　LCS
・MIT の博士課程の学生。報告者が MIT メディア研究所に在籍していた 1985 年当時の政治学科の学部学生。明晰なハッカーで学内新聞に何度も投稿記事を書いていた。似たような顔の人間がいて驚いた．ベンチャーを失敗したらしい.
・法的にどのような規制が必要かという議論．技術的に何ができるかの説明が不足していたが、低価格の RFID タグの重要性は増すことは間違いない.

(4) Privacy-enhancing Technologies

"Some Techniques for Privacy in Ubicomp and Context-Aware Applications"
John Canny
University of California, Berkeley
・UCB の教授の発表。プライバシー保護するための技術の紹介.

・圧縮技術を用いたプライバシー対策、メタデータの利用など.

"Privacy Authentication - Persistent Non-identification in Ubiquitous Environments"
Stephan Engberg, Morten Borup Harning
Open Business Innovation
・相手を同定しないで認証する方法と匿名を使い認証をしながら、複数のサービスの間で個人を関連付ける技術。
・tracable, identifiable を区別することが重要

Privacy in Digitally Named World with RFID Tags"
Sozo INOUE, Shinichi KONOMI, Hiroto YASUURA
九州大学
・PFID タグを物品 ID に使う際のプライバシーの保護策について九州大学井上氏の講演
・構想レベルであり、インプリメントされていないが反響は大きかった

2．2 Security in Ubiquitous Computing

2．2．1 概要

プライバシーのワークショップと並行してセキュリティのワークショップが開催されていた。SAP が主導権を握っているようだったので報告者はプライバシーのワークショップに参加したが、セキュリティ・ワークショップの方が技術的に内容が充実していたようである。ユビキタス・コンピューティングにおいては従来のセキュリティ技術では対応不十分なものが多く、これらの課題や技術的な取り組みを共有し、議論することを目的としてワークショップが開かれた。
Workshop Homepage: http://www.teco.edu/~philip/ubicomp2002ws/index.htm

2．2．2 セッション構成とワークショップの議論の成果について

(1) セッション構成

第 I 部 Trust in UbiComp Environments (Moderator: Refik Molva)

- Dynamic Trust Models for Ubiquitous Computing (Colin English, PaddyNixon): presentation | paper
- On Trust for Ubiquitous Computing (Narender Shankar, William Arbaugh): paper
- Secure Ubiquitous Computing based on Entity Recognition (Jean-Marc Seigneur): presentation | paper

第Ⅱ部　User-centric Security (Moderator: Philip Robinson)

- Integrating Privacy Enhancing Services in Ubiquitous Computing Environments (Moamo Wu, Adrian Friday): presentation | paper
- Authentication in Ubiquitous Computing (Laurent Bussard, Yves Roudier): presentation | paper
- Identity Management (Michael Kreutzer): presentation | paper | demo

第Ⅲ部　Security and Context -Awareness (Moderator: Joachim Posegga)

- Enabling Secure Ad-hoc Communication using Context-Aware Security Services (Narendar Shankar, Dirk Bilfanz): paper
- Context Aware and Yet Another Service AYA (Hiromitso Kato): presentation | paper
- Protecting People Location Information (Urs Hengartner, Peter Steenkiste): presentation | paper

第Ⅳ部　Augmenting Security-Minded Worlds (Moderator: Refik Molva)

- Secure Media Consumption in a Ubicomp World (Stephanie Wald): presentation | paper
- "Threats, Risk Assessment and Policy Management in UbiComp" (Philip Robinson): presentation
- {Thanks to Håkan Kvarnström et al, "A Protection Scheme For Security Policies In Ubiquitous Environments Using One-Way Functions" in absentism}: paper

第Ⅴ部　Closing Discussion and Summary: presentation

(2)　上記のセッション構成についてワークショップでの議論の成果のまとめ

What is different in Ubicomp?

Trust

- Lack of a priori trust
- Old model based on verification of credentials (authentication)　and delegation not suitable
- Identity does not imply privilege or right
- Need for
- Methods to gain trust based on observation and reputation
- Dynamic evaluation of trust
- Multidimensional trust representation in a continous space
- Implementation in byzantine (malicious) environments

- New authentication mechanisms (entity recognition?)

Privacy

- Ubicomp ⇒ Pervasive disclosure of user information
- Strong requirement: location hiding
- Adaptive privacy management
- User-based privacy management vs Privacy infrastructure
- Research direction: Privacy enforcement built into Ubicomp
- Should new trust models ease the solution to privacy problems?
- Context-Awareness
- What do we mean by context?
- How can Context-Awareness enhance security?
- How to assure context authentication?
- Can Context-Awareness make security user-friendly?
- Can Context-Awareness help with the lack of explicit interaction?
- Can Context-Awareness enable new Trust Models?

Security vs. HCI

- How does Security affect the user-friendliness of Ubicomp?
- Can security be achieved without explicit interaction?

Directions for Security Research in Ubicomp

- New models for trust and security mechanisms
- Verification with partial information
- Security protocols based on context information
- User-controlled Privacy management
- Context authentication
- Content-protection

C. 2 ユビキタス・セキュリティ関連プロジェクト

	プロジェクト名	研究機関	コメント	関連サイト・URL
■海外 ユビキタスコンピューティング				
1	Nomad	Microvision	高解像度で、日光の下でも読み取り可能な携帯型シースルーディスプレイ。	http://www.mvis.com/
2	Shape	CID Stockholm, Sweden、MRL Nottingham, UK	博物館や体験型の科学教育施設など、学習環境の場で有効なユビキタスコンピューティングの研究。	http://www.shape-dc.org/
3	iButton	Maxim Integrated Products	ユビキタス環境下で様々な状況、用途に利用できるiButtonの研究。小型のボタンにチップが仕込んであり、様々なアプリケーションへの適用が可能。	http://www.ibutton.com/index.html
4	WearNET	Wearable Computing Laboratory	センサのウェアラブルプラットフォームを実装し、人や環境に設置した複数のセンサデータから人のさまざまな状況を理解する。	http://www.wearable.ethz.ch/
5	Project Aura	Carnegie Mellon University	着用可能な機器や携帯型機器などのコンピュータインフラを用いた、ユーザがどこにいても情報サービスを享受できるためのシステムの構築。	http://www-2.cs.cmu.edu/~aura/
6	PlantCare	Carnegie Mellon University	ユビキタス環境における、センサネットワークとモバイルロボットを使って、室内用植物に水を供給し、管理するシステム。センサを利用して、プラントの水分状況を把握し、必要に応じてモバイルロボットがプラントまで移動し、水遣りを行う。	http://seattleweb.intel-research.net/projects/plantcare/
7	GVU Center	Georgia Institute of Technology	オフィスでの共同作業を支援するためのContext-Awareなコンピューティングの研究。	http://www.cc.gatech.edu/gvu/
8	Palo Alto Laboratory	Fuji-Xerox	ユビキタス環境下での共有コンピュータに対するパーソナライズの実験と評価。	http://www.fxpal.xerox.com/
9	The UbiCampus Project	Institute of System Engineering	大学構内にユビキタスコンピュータを導入することによる高度な学習環境の構築と、必要なアプリケーション及びミドルウェアの研究。	http://www.sra.uni-hannover.de/index_eng.htm
10	Aware Home	Future Computing Environments	住居環境内に様々なコンピュータ技術を取り入れることにより、家庭での生活サポートを行う「Digital Family Portrait」などの研究。	http://www.cc.gatech.edu/fce/
11	Gaia project	UCD	インタラクティブシステムのためのOSやミドルウェアの設計と実装。	http://devius.cs.uiuc.edu/gaia/

	プロジェクト名	研究機関	コメント	関連サイト・URL
12	Rememberer	Hewlett Packard Labs	博物館で、ユーザが鑑賞している展示物に関する説明をPDAや小型ノートPC上に表示し、そこで得た経験を帰宅してからWebページ上で他者に公開できるシステム。	http://www.hpl.hp.com/
13	CoolTown	Hewlett-Packard Labs	車や建物など、全てのものにIPアドレスを振り、それぞれがwebサーバとして動作することで、E-mailやチャットなどのサービスを利用できる環境の構築。	http://www.cooltown.hp.com/
14	Xamax	Roger Clarke	ユビキタス環境における、人の位置や追跡技術の、適切な適用方法、性質や特性、危険性についての研究開発。	http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html
15	Bernt Schiele	EHT Zurich	作業の状況把握にセンサを使用して、必要なアクションを細分化し、ユーザの行動を詳しく検知するシステム。	http://www.vision.ethz.ch/publ/
16	The Interactive Workspaces Project	Stanford University	ユビキタス環境において共同作業を行うための、データベース、ネットワーク、コミュニケーション環境の構築。インタラクティブなワークスペース(iRoom)の開発。	http://graphics.stanford.edu/projects/iwork/
17	The Smart-Its Project	Lancaster University	ユビキタス環境下で有効な、自己認識型のセンサデバイスSmart-Itsの開発。	http://www.smart-its.org/
18	Atelier	University of Oulu Finland	グループ学習促進環境の構築による、創造的な学習環境を実現するためのユビキタスコンピューティングの研究。	http://atelier.k3.mah.se/home/
19	Computer and Information Science	University of Oregon	生活の中で人々を支援するウェアラブルコンピュータ技術の研究や、携帯電話やPDA・ウェアラブルコンピュータなどによって、形成されるコミュニケーションの研究。	http://www.cs.uoregon.edu/
20	Load Sensing Lab	Lancaster University	オブジェクトの重さ、位置、動きなどのコンテキスト情報を取得する、ロードセンシング技術に関する研究。	http://www.comp.lancs.ac.uk/~albrecht/load/
21	ForSe FIElds	University Of Limerick	Z-TilesとSOSを用いた、パフォーマンスミュージシャンの動作によるオーディオシグナルコントロールや、太極拳のセンシングなどの研究。	http://www.csis.ul.ie/
22	Mobile and Wearable Computing Group	University of Bristol	サイバージャケットとツーリストガイドの開発と、それらを用いた人の位置、動きをセンシングする研究。	http://www.cs.bris.ac.uk/
23	Oxygen	MIT	特別な知識を必要とすることなく、いつでもどこでもニーズに応じた情報通信サービスを利用することによるユビキタス協調コミュニケーション環境の構築。	http://oxygen.lcs.mit.edu/

	プロジェクト名	研究機関	コメント	関連サイト・URL
24	Auto-ID Center	MIT	ユビキタス環境において、あらゆるものがネットワークに接続する将来を想定し、あらゆるものにIDを振ることを目的とした研究開発。	http://www.autoidcenter.org/main.asp
25	Smart Dust	University of California	チリくらいの大きさの小さなチップ上に通信、センサ、電源モジュールを搭載させ、環境にばら撒く事で情報収集を行う環境を構築。	http://www-bsac.eecs.berkeley.edu/~pister/
26	Department of Computer Science	University of California	モバイル環境を利用して、位置情報に基づいた大学キャンパス内でのインタラクション活性化の研究。	http://www-cse.ucsd.edu/
27	Endeavour	University of Carifornia	多様なIT機器を用いた、大規模で自己組織化可能かつ適用性のある情報処理環境の構築。	http://endeavour.cs.berkeley.edu/
28	Portolano	University of Washington	インビジブルコンピューティング：目に見えず、コンピュータを意識しないコンピューティング環境実現のための研究開発。	http://portolano.cs.washington.edu/
29	The Labscape Project	University of Washington	人々のコミュニケーションと連携を支援するための言語、ツールの研究開発。	http://labscape.cs.washington.edu/

■海外　セキュリティ・プライバシー関連

1	Helen Lowe	University of Strathclyde Scotland	信頼できる暗号化技術の提案と、相互作用を行っているユビキタスコンピュータの信頼関係を保持することに注目したセキュリティモデルに関する研究。	http://www.cs.strath.ac.uk/
2	Narendar Shankar	Univ of Maryland Maryland	ユビキタス環境における、信頼性のある接続環境を構築するための、ベクトル微積分学に基づいたアプローチに関する研究。	http://www.cs.umd.edu/~narendar/
3	Adrian Friday	Lancaster University Lancaster	個人向けサービスを増強するためのプライバシー保護や、個人のプライバシーにおける必要条件を満たしながら、個別化されたサービスおよび統計データを収集。	http://www.comp.lancs.ac.uk/~adrian/
4	Yves ROUDIER	Institut Eur	一般的なネットワークセキュリティのアプローチが、ユビキタスコンピューティングにおける認証を保障するのに十分でないかを明らかにし、新しい認証方式の提案。	http://www.eurecom.fr/~roudier/
5	Hans Hedbom	Chalmers University of Technology Sweden	侵入検知システムでのセキュリティーポリシーや、ファイアウォール中のフィルタリングのポリシーなどのセキュリティ・メカニズム、製品中のセキュリティポリシーの改善。	http://www.cs.kau.se/~hansh/
6	Dirk Balfanz	Palo Alto Research Center	ユビキタスミーティング時に受け取った機密事項のドキュメントを共有する場合の、セキュリティマネージメントに関する研究。	http://www.parc.xerox.com/

	プロジェクト名	研究機関	コメント	関連サイト・URL
7	Hakan Kvarnstrom	Chalmers University	セキュリティ保護や、IDSにおける発見方法、ファイヤウォールのフィルタリング。	http://www.chalmers.se/
8	Information Security Group	MIT	暗号化、認証の手段についての研究とユーザ環境の構築。暗号のアルゴリズム、プロトコル設計、暗号化理論、安全な情報システムの応用工学に関する研究。	http://theory.lcs.mit.edu/~cis/
9	MIT Wearable Computing Project	MIT	MIThril、I Sensed、Wearable Phased Array Microphone 、 Stochasticks 、 DyPERS 、 FaceName、WearSATなど複数のWearable Computingに関する研究。	http://www.media.mit.edu/wearables/
10	Knowledge engineering	VTT Electronic	価値あるユビキタスコンピューティングのための多目的プラットフォームの実装。	http://www.vtt.fi/ele/indexe.htm
11	Group for User Interface Research	University of California, Berkeley	ユビキタス環境におけるプライバシーを管理するツールや、プライバシー固有の複雑さを、単純な概念モデルに変形する研究など。	http://guir.berkeley.edu/
12	A Privacy Awareness System	ETH Zurich	お互いにプライバシーを尊重することを支援するシステムや個人情報を管理するためのインタフェースの構築。	http://www.inf.ethz.ch/vs/
13	CCG	Georgia Tech	コンテクスチュアリーアウェア、ウェアラブルコンピューティングシステム分野の研究。	http://www.cc.gatech.edu/ccg/
14	Xamax	Roger Clarke	人の位置検出・監視におけるプライバシーについての研究。	http://www.xamax.com.au/

■海外　音声・音楽関連

1	The Sob project	University of Verona	Disappearing Computer の為の、物理的なオブジェクトに一致する音モデルの開発。	http://www.soundobject.org/
2	Music , Mind and Machine	MIT Media Laboratory	音楽の創作・送信・体験の方法を変える、未来のオーディオ技術やインタラクティブアプリケーションの研究・開発。	http://sound.media.mit.edu/
3	Hyperinstruments	MIT Media Laboratory	演奏やジェスチャーのための新技術の開発や、パフォーマンスアートとして音楽を強め、音楽が日常生活の「対位法」として変形する方式の開発。	http://www.media.mit.edu/hyperins/index.html
4	SmartKom	DFKI	音声、ジェスチャー、顔表情を入出力に利用したマルチモーダル対話システム。	http://www.dfki.de/pas/
5	The Speech Interface Group	MIT Media Laboratory	音声技術とポータブルデバイスを用いた、人のコミュニケーションサポートや、より使いやすいデジタルオーディオのデータタイプ開	http://www.media.mit.edu/speech/
6	DARPA	Univercity of Washington	インタラクティブ情報アクセスのための、強健な認識と対話トラッキング。	http://ssli.ee.washington.edu/

	プロジェクト名	研究機関	コメント	関連サイト・URL
■海外 ITS・ナビゲーション				
1	FCD、XFCD	Fela ドイツ	自動車自体がGSM電話で速度と位置情報を情報処理センターに送ることによる渋滞情報の生成。XFCDによる天候や路面の凍結情報などの情報の利用。	http://www.fhi.fela.de/
2	TEGARON	ドイツ・テレコム、ダイムラークライスラー	情報分野、安全/救難補助分野、およびナビゲーション分野を中心に、個人が日常的に行う移動の効率と快適性を向上させるテレマティックス・サービスの開発と実装。	http://www.t-traffic.de/
3	Visionaute	Mediamobile	所要時間を基準とする高品質交通情報サービス。RDS/TMCに加えて Wapや各種Web標準規格が使用され、フランス全土の98%以上で利用可能。	http://www.visionaute.com/visionaute.html
■海外 情報家電				
1	X10	X-10.org	欧米で10年以上昔から一般家庭で広く当り前に使われている電力線通信方式。電気のON／OFFや照明の明るさ調整を、簡易にリモートコントロールする事が可能。	http://www.x10.org/
2	HAVi	HAVi, Inc	コンシューマ・エレクトロニクスとコンピューティング・デバイスを相互に接するホームネットワーキング規格。	http://www.havi.org/
■日本 ユビキタスコンピューティング(大学)				
1	廣瀬 通孝 研究室	東京大学	約1350個のRFIDタグ、無線LAN、ネットワークカメラなどのシステムを用いた有機的なユビキタス環境下における、人間の行動の3次元的なリアルタイム計測。	http://www.cyber.rcast.u-tokyo.ac.jp/index-j.html
2	坂村健 研究室	東京大学	人々の身の回りの機器にOSを組み込み、それらを協調動作させることによって人々の生活を支援する「どこでもコンピュータ環境」の構築のためのTRONプロジェクト。	http://tron.um.u-tokyo.ac.jp/
3	青山 友紀 研究室	東京大学	ユビキタス環境下におけるサービス呼び出しのためのネーミング技術とサービス合成技術の研究。アプリケーションプラットフォーム「Stone」など。	http://www.mlab.t.u-tokyo.ac.jp/
4	松山 隆司 研究室	京都大学	様々なセンサから人間の意図や行動、環境の理解を行い、その結果に基づいて人間とのインタラクションを実現するシステムを構築。	http://vision.kuee.kyoto-u.ac.jp/index-jp.html

	プロジェクト名	研究機関	コメント	関連サイト・URL
5	西尾 章治郎 研究室	大阪大学	入出力制御のためのルールエンジンを搭載したユビキタスチップの開発。あらゆるものに埋め込むためのユビキタスコンピュータの要件を抽出し、必要機能のみに絞る事で小型化を実現。	http://www-nishio.ise.eng.osaka-u.ac.jp/
6	岸野 文郎 研究室	大阪大学	マルチメディア技術を用いて情報化された環境において人間の五感に反応する人間中心のインタフェースの研究。	http://www-human.ist.osaka-u.ac.jp/
7	田中二郎 研究室	筑波大学	モバイル/ユビキタスコンピューティングのための表示技術や、情報の公開度をグラフとして扱うインタフェースなどの研究。	http://www.iplab.is.tsukuba.ac.jp/~iplab/jiro-j.html
8	椎尾 一郎 研究室	玉川大学	人とコンピュータとの新しいインタラクションについての教育・研究。RFIDを利用したユーザ位置検出システム「ID Carpet」など。	http://siio.ele.eng.tamagawa.ac.jp/
9	中西泰人 研究室	電気通信大学	EnhancedWall 、Context Aware Messaginge Service、EnhancedMirrorなど、モバイルシステム、実世界指向インタフェースなどの研究。	http://naka1.hako.is.uec.ac.jp/
10	佐藤 洋一 研究室	電気通信大学	机上で手を用いてコンピュータを操作するシステム(EnhancedDesk Project)の開発による、人間の作業支援を目的とした研究。	http://www.hci.iis.u-tokyo.ac.jp/
11	安浦 寛人 研究室	九州大学	RFIDタグによる、オブジェクトと個人の関係についてのプライバシーを管理する研究。	http://www.slrc.kyushu-u.ac.jp/
12	竹林 洋一 研究室	静岡大学	ユビキタスミーティングを利用したマルチモーダル知識獲得や、センサデータを利用したコミュニティ支援、動作理解、感情理解などの研究。	http://www.takebay.net/
13	北澤 茂良 研究室	静岡大学	音声コーパス、マルチメディアコーパスによる収録素材からの重要場面抽出、韻律情報を含んだマルチモーダル対話コーパスの検討。	http://minny.cs.inf.shizuoka.ac.jp/
14	杉山 岳弘 研究室	静岡大学	知識映像コンテンツの蓄積、次世代学習環境システムの構築と情報教育教材作成。	http://vivid.ia.inf.shizuoka.ac.jp/
15	水野 忠則 研究室	静岡大学	モバイルコンピューティングを利用した情報共有やセキュリティ認証、無線通信における複数回線共有方式、アドホックネットワークトにおける電波制御などの研究。	http://www.mizulab.net/
16	長嶋 洋一 研究室	静岡文化芸術大学	センサを使用した新しいコンピュータミュージックの研究及びインタラクティブなメディアアートの作成。	http://1106.suac.net/

	プロジェクト名	研究機関	コメント	関連サイト・URL
17	徳田 英幸　研究室	慶応義塾大学	オペレーティングシステムによる資源予約機構やモニタリング機構、モバイルホストの認証機構を構築することによる、セキュアな実行環境の実現。	http://www.ht.sfc.keio.ac.jp/
18	安西 祐一郎 研究室	慶応義塾大学	移動するユーザへのサービス提供方法として、ユーザの移動を追随しながらネットワーク上を移動するモバイルエージェントフレームワーク FollowingSpaceに関する研究や、3次元位置検出システムを用いたユーザとサービスの動的な位置関係に基づくLookUp機構の構築。	http://www.ayu.ics.keio.ac.jp/
19	塚田 浩二、安村 通晃 研究室	慶応義塾大学	モバイル環境において、ベルトに方位センサ、GPSと複数のアクチュエータを装着し、方位情報を伴う触覚情報提示の実現。	http://mobiquitous.com/~tsuka/active-belt.html
20	高西　淳夫 研究室	早稲田大学	人間の知覚・認識・運動機能の研究に基づいた、人間と協調し、作業を支援するヒューマノイド・ロボットの研究。	http://www.takanishi.mech.waseda.ac.jp/
21	木戸出 正継 研究室	奈良先端科学技術大学院大学	ウェアラブル機器を用いた日常記憶支援のための支援モデルの研究。ロボットによる人間の情報活動支援のための研究。対話インタフェース、画像理解に関する研究。	http://ai-www.aist-nara.ac.jp/

■日本　ユビキタスコンピューティング(企業・研究機関)

1	増井 俊之・暦本 純一・綾塚 祐二	SONY CSL	実世界指向ユーザインタフェースの研究、情報視覚化、情報検索、予測インタフェース、テキスト入力システム。手や指の動作に敏感なセンサアーキテクチャ「SmartSkin」、「ちょっとした会話」を支援する「ChatScape」。	http://www.csl.sony.co.jp/
2	富士通研究所	富士通	Semantic Webを利用した、ユビキタス環境下で有効なグループウェアの開発など。	http://www.labs.fujitsu.com/
3	サイバーアシスト研究センター	産業技術総合研究所	1つのボタンで様々な用途に利用できる「マイボタン」の開発による人間中心の情報サポートシステムの研究。	http://www.carc.aist.go.jp/carc/
4	知能システム研究部門	産業技術総合研究所	ユーザやその周囲の状況を察知し、ユーザ本位の動作をしてくれる気の利いた着用型アシスタントの開発。	http://unit.aist.go.jp/is/index_j.html
5	マルチメディア研究所	NTTDoCoMo	携帯及びウェアラブル端末向けの新しいヒューマンインタフェースの研究。	http://www.lab.nttdocomo.co.jp/

	プロジェクト名	研究機関	コメント	関連サイト・URL
6	知識メディアラボラトリ・マルチメディアラボラトリ	東芝 研究開発センター	映像・ナレッジ・Bluetooth技術を融合し、マルチモーダル・ナレッジ（MPEG4映像、音声、テキスト）を、ユビキタス環境でオンデマンドでBluetooth機器に配信するシステムMKIDS、ユビキタスヘッドセットの開発。	http://www.toshiba.co.jp/tech/
7	個人向けナビゲーション	日立製作所 デザイン本部	ユビキタス環境における個人向けナビゲーションサービスのインタフェースの開発。	http://www.hitachi.co.jp/Div/dc
8	Cubium	日立製作所　中央研究所	ネットインフラ、ビジネス管理、アプリケーションに体系化したサービス商品メニューを豊富に取り揃えたネットソリューションの提供。	http://www.hitachi.co.jp/cubium/index.html
9	情報技術総合研究所	三菱電機	ディスプレイのある方向に視線を向けるだけで自然に映像が見える、ウェアラブルディスプレイSCOPO等の開発。	http://www.mitsubishielectric.co.jp/corporate/randd/

■日本 コミュニケーション

1	ユビキタス・ミーティング	東芝ITソリューション、ソフトスペース、オンソリ社	各々のPCの前に座り、ホワイトボード、PPTを共有しながら情報交換が行えるインターネット会議システムの開発。	http://www.toshiba-it.co.jp/ http://www.softspace.co.jp
2	やおよろずプロジェクト	日立、慶應大、東京工科大、東京大、メディア教育開発センター	社会的倫理と適合的なネットワークに関する研究、ライフスタイルデザインに関する研究、ユビキタス情報基盤の相互運用技術に関する研究。	http://www.8mg.jp/
3	ITメディア研究所	富士ゼロックス	普段の日常的なコミュニケーションにおける振る舞いをコミュニティの中で伝えるための環境を構築し、お互いのコンテキストの共有を行なうための研究。	http://www.fujixerox.co.jp/company/iml/
4	Knowledge-Drive	富士ゼロックス	インターネットの利用による、遠隔地の拠点同士のリアルタイムな双方向コミュニケーションと、保存されたコンテンツの知的資源としての活用を支援するサービス。	http://www.ubiquitous-media.com/
5	角　康之・間瀬 健二	ATRメディア情報科学研究所・ATR知能ロボティクス研究所	自律性のある人工物と人間との多様なインタラクションがもたらす協調的な活動に着目して、実世界コンピューティングが可能で、操作性がよいメディア技術を研究。「コミックダイアリ」、「エージェントサロン」など。	http://www.mis.atr.co.jp/index-j.html
6	メディア教育開発センター	文部科学省 大学共同利用機関	コンピュータや視聴覚メディア機器等と人間との双方的コミュニケーションや、メディア学習環境における様々なインタフェースについて、生理学、心理学、情報環境学、認知科学、教育工学等の手法を用いて多角的に評価・研究。	http://www.nime.ac.jp/index_ie.html

	プロジェクト名	研究機関	コメント	関連サイト・URL
7	高品質ライブ遠隔講義システム	沖電気カスタマアドテック	ブロードバンドでの映像配信・コミュニケーションを可能とする「OKI MediaServer」を映像配信エンジンとし、遠隔講義・講演に必要なさまざまな機能を提供。	http://www.oca.co.jp/
8	UCL	SBFコンサルティング	ユビキタスコミュニケーションを実現する各種アプリケーション、それを支えるソフトウェア、ハードウェアインフラ、R&D段階情報、ビジネスノウハウの集積。	http://www.sbfweb.com/japanese/ucl.html
9	ライフコミュニケーショングループ	NTT環境エネルギー研究所	人間関係の維持・構築を目的とした新たなメディアコミュニケーションスタイルの提案と、その効果の検証・分析。	http://kankyo.lelab.ecl.ntt.co.jp/
10	TOCSR	NTT-ME	企業等の遠隔地間の会議を支援するサービス。企業別に用意されたウェブ会議サイト上で、精細な図面やアプリケーション、プレゼンテーション資料の共有。	http://www.ntt-me.co.jp/index_f.html
11	ユビキタスインタフェース研究部	NTTマイクロシステムインテグレーション研究所	RealとVirtualを簡単にコネクトする「ミラーインタフェース」、指輪型音声受信ユニット「ボイスユビーク」、手軽でウェアラブルな血流測定マイクロ血流センサなど。	http://www.sctlg.ecl.ntt.co.jp/ntt_en/
12	SOBAプロジェクト	NTTコムウェア、京大、東京工大、早稲田大	インターネット上に「コミュニケーションの場」を、仮想的かつ動的な共有空間として作り出せる、従来なかった全く新しい概念に基づくフレームワーク。	http://www.soba-project.org/jp/

■日本　介護・福祉（大学）

1	福島 智 研究室	東京大学	障害者・高齢者のための先端科学技術の応用方法を探り、未来のバリアフリー社会空間の構築を目指す、科学技術と障害者・高齢者との関係に関する文理横断の研究。	http://satellite01.bfs.rcast.u-tokyo.ac.jp/project/
2	山本 義春 研究室	東京大学	生体リズム障害・睡眠障害、心臓疾患と関連した自律神経活動、運動不足に起因する生活習慣病の危険度など、院内検査のみからでは得られない情報を取得。	http://www.p.u-tokyo.ac.jp/~yamamoto/
3	濱本研究室 研究室	東海大学	生体を通過してきたエックス線や超音波から人間の体の情報を抽出し、可視化(Visualization)する技術についての研究。	http://www.dm.u-tokai.ac.jp/
4	光石 衛　研究室	東京大学	遠隔医療のための手術室（テレ・マイクロ・サージェリー・システム）の開発研究。	http://www.nml.t.u-tokyo.ac.jp/
5	中村 仁彦 研究室	東京大学	医者を支援するための外科手術ロボティクスの研究。	http://www.ynl.t.u-tokyo.ac.jp/

	プロジェクト名	研究機関	コメント	関連サイト・URL
6	土肥 健純 研究室	東京大学	人間の生命の支援という立場から、情報・機械技術と臨床医学を融合し治療を支援する「コンピュータ外科 -Computer Aided Surgery」の研究。	http://www.atre.t.u-tokyo.ac.jp/
7	黒田 知宏 研究室	京都大学	手術ロボットの開発や、手術に関するあらゆる機器・情報を統合管理し、遠隔ロボット手術の進行を全般的に管理・支援するためのシステムの開発研究。	http://www.kuhp.kyoto-u.ac.jp/Official/medinfo/
8	伊福部 達 研究室	北海道大	感覚代行システムに関する福祉工学の研究。	http://welfare.es.hokudai.ac.jp/
9	米本 清 研究室	岩手県立大学	補聴器の選択や調整、音環境の変化に対応した使い方を体得する場を提供する仮想音場システムを開発。	http://www.anna.iwate-pu.ac.jp/~yonex/
10	長嶋 祐二 研究室	工学院大学	聴覚障害者のための手話日本語の相互翻訳システムの開発。	http://www.ns.kogakuin.ac.jp/
11	大倉 元宏 研究室	成蹊大学	安全性、快適性、効率性をパラメータとした人間－機械システムの設計・開発・評価。	http://cleo.is.seikei.ac.jp/
12	森 英雄 研究室	山梨大学	視覚障害者のための、「歩行ガイドロボット」実用化のための研究開発。	http://133.23.237.210/~forest/
13	井手 将文 研究室	徳島大学	重度肢体不自由者の機器操作特性についての研究（現在はコンピュータの入力装置の操作特性についての研究）。	http://www.eco.tokushima-u.ac.jp/w3/ide/
14	太田 裕治 研究室	お茶の水女子大学	頭部動作を利用した高齢者・障碍者入力インタフェース、全方向移動ロボット制御。	http://biomed.eng.ocha.ac.jp/
15	内川 嘉樹 研究室	名古屋大学	きびきびと動くロボットを実現するための認知主体と環境との間に存在する（身体を介した）相互作用ダイナミクス、身体性、そして立脚性を考慮した知能システムの構築。	http://www.cmplx.cse.nagoya-u.ac.jp/
16	岩田 彰 研究室	名古屋工業大学	心臓疾患診断支援エキスパートシステム。	http://mars.elcom.nitech.ac.jp/
17	葛岡 英明 研究室	筑波大学	教示者が作業者に対してインタラクティブな支援が行えるような、遠隔医療指示を支援するシステムの研究。	http://www.kuzuoka-lab.esys.tsukuba.ac.jp/
18	神谷 好承 研究室	金沢大学	人にやさしいロボット・機械の研究。福祉・介護機器の開発。人間の存在する屋内で移動ロボットを信頼性良く安価なシステムでナビゲーションする研究など。	http://as.ms.t.kanazawa-u.ac.jp/index-j.html
19	手嶋 教之 研究室	立命館大学	障害者及び高齢者に対する福祉工学の基礎的研究、及びそれに基づいた福祉機器の開発。高齢者や障害者に優しい機器」の開発に必要な要素技術の解明を目指す。	http://www.ritsumei.ac.jp/se/~tejima/index.html
20	安村 通晃 研究室	慶応大学	障害者向けインタフェース、ユニバーサルデザインに関する研究。	http://buri.sfc.keio.ac.jp/

	プロジェクト名	研究機関	コメント	関連サイト・URL
21	井須 尚紀 研究室	三重大学	AIにおいて、生体情報工学、自然言語処理、画像理解といった知的活動を実現するために、様々な場面で人間の生活を支援する知的なソフトウェアについての研究。	http://www.shiino.info.mie-u.ac.jp/index-sj.html

■日本 介護・福祉(企業・研究機関)

1	電子カルテソリューション	NEC Medical Square	最小のカスタマイズで運用が可能な「MegaOakシリーズ」、オーダリングシステムから各部門システムとの連携を可能とした「スーパー診療サポートソリューション」等。	http://www.sw.nec.co.jp/igovcom/medsq/
2	LifeMinder	東芝	ウェアラブルセンサで計測したユーザの生体情報や動作・姿勢などの行動の情報から生活状況を取得し、これに合わせた健康管理サービスを提供するシステムの開発。	http://www.toshiba.co.jp/mmlab/tech/h04.htm
3	セキュリティ委員会	日本画像医療システム工業会	Remote Serviceに関する規約の制定(国外調整含む)、日本における医療用セキュリティの枠組み策定DICOMセキュリティ規格の検討。	http://www.jira-net.or.jp/
4	保健医療福祉情報システム	保健医療福祉情報システム工業会	健医療福祉情報システムに関する技術の向上、品質および安全性の確保、標準化の推進を図る。RIMの開発・生涯健康データベース構築(EHR)など。	http://www.jahis.jp/
5	医療用セキュリティ委員会	MEDIS-DS	医療情報システムに関する基本的かつ総合的な調査、研究、開発、実験、医療従事者管理のための認証等のガイドライン策定。	http://www.medis.or.jp/
6	Medical Station	ビー・エム・エル 医療情報システム事業部	カルテ作成、患者の診療情報を統合管理し、データベースを院内の各部門で共有するシステム。	http://www.bml.co.jp/medical_station/toku_fr.html
7	すこやかねっとi	NEC Medical Square	利用者宅または施設に健康支援端末「すこやかめいとi」を設置し、各種機関やインターネットに設けたセンターシステムへ伝送し、健康データの保存・照会・分析を行う。	http://www.sw.nec.co.jp/igovcom/medsq/
8	医療システム	SBS情報システム	オーダエントリーシステム、看護支援システム、医療画像参照システム、病床管理システム、ベッドサイド端末など、病院における様々な支援。	http://www.sys.sbs-np.co.jp/
9	介護・福祉機器	テクノスジャパン	ベッドサイドに敷くマットセンサに既存のナースコールシステムを接続した離床報知器。一人でベッドを離れると心配な痴呆性老人の離床を確実に報知する。	http://www.technosj.co.jp/fukusi/intro.htm

	プロジェクト名	研究機関	コメント	関連サイト・URL
10	HAMMYOシリーズ	日本道路	歩行者誘導機能を相互補完して、身体障害者、高齢者などのハンディキャップをもつ方々が自立できる環境、安全・安心・快適で使いやすい歩行空間の提供。	http://www.nipponroad.co.jp/
11	ココセコム	SECOM	人や車両の位置を提供して、必要に応じて警察・消防への通報などを行う。	http://www.855756.com/
12	UCN21	Universal Community Network	加齢や様々な障害による身体的・認知的機能低下や欠損を、高度な技術基盤により支援することを目指し、誰もが自由に情報の受発信を行うための技術を開発。	http://www.ucn21.com/
13	医用工学研究室	労働福祉事業団	これまで工学系研究機関が触れなかったリハビリテーションにおける生活系・生活環境系の機器を含めたHumanな領域を対象とした研究。	http://www.sekisonh.rofuku.go.jp/iyou/rihab-e.htm
14	伊藤　英一	神奈川リハビリテーション病院	手や，足など身体の機能，運動障害の内容に応じたパソコンのキーボードなどの代替となる入力デバイスの開発。	http://www.sfc.keio.ac.jp/~e-ito/
15	畠山　卓朗	横浜市総合リハビリテーションセンター	障害者支援システムの研究開発。携帯機器の方向によって音声情報を提供する視覚障害者用音声歩行案内システムや、聴覚障害者用筆談通信機(ライトーク)など。	http://homepage2.nifty.com/htakuro/
16	リハビリテーション工学研究室	埼玉県総合リハビリテーションセンター	福祉機器の研究・開発、リハビリテーションに関する基礎的な工学からの研究・開発、補装具製作、歩行測定、住環境整備。	http://www.pref.saitama.jp/A04/BL01/rihasen/index.htm
17	中国総合通信局	総務省	スポーツ現場において安全確保が行き届き、又、より効果的にスポーツをするために、どのような無線システムの開発が必要であるかを総合的に検討。	http://www.cbt.go.jp/kenkyuu/kenkyuu01_03.html

■日本 ITS・ナビゲーション

1	アイ・アシストナビ	アルパイン	ルート探索やオートリルートなどはその実行の瞬間さえ分からないほどに所要時間を短縮。地図をスクロールさせた時の表示画面の遅れを解消。	http://www.alpine.co.jp/
2	G-BOOK	TOYOTA	ユーザごとにサーバが割り当てられ、車以外の様々な端末からも外部ネットワークと通信できる車載コンピュータの開発。	http://g-book.com/pc/service_menu/
3	カーウイングス	日産自動車	携帯電話と接続することで、さまざまな情報サービス、メール、ハンズフリーフォン、緊急時の有人サービス等が利用できるカーナビシステム。	http://www.nissan-carwings.com/

	プロジェクト名	研究機関	コメント	関連サイト・URL
4	インターナビ	HONDA	ドライバーにとって本当に必要な情報だけに絞り込み、それを高度なレベルで提供する通信型カーナビ。いつでもどこでもユーザ専用のデータへアクセスできる。	http://www.internavi.ne.jp/
5	Air Navi	Pioneer	地図データや電話番号などを、カーナビではなくインターネット上のサーバ側に持たせることで、従来のCDやDVDと異なり、常に最新の情報を提供。	http://www.air-navi.com/
6	CADIAS	ADDZEST	Windows CE for Automotiveを搭載した、車載型パソコン。カーナビ機能に加え、メールの送受信などパソコンとして利用可能。	http://www.addzest.com/cadias/
7	HITACHI ITS21	日立製作所	プローブカー、路側システム、通信システム、コンピュータシステムから、サービス事業まで含めたITSソリューションを提供。	http://www.hitachi.co.jp/Prod/siji/its/jpn/index_j.html
8	VICS	道路交通情報通信システムセンター	VICSセンターで編集、処理された渋滞や交通規制などの道路交通情報をリアルタイムに送信し、カーナビゲーションなどの車載機に、文字・図形で表示するシステム。	http://www.vics.or.jp/
9	GISサービス	PASCO	歩行者ITSシステムの技術開発、震災時のデジタル地図共有などの道路震災情報ネットワークシステム、診療検索予約システムや救援支援システムなど。	http://www.pasco.co.jp/index.html
10	MASAMUNE・Trial	国土交通省　東北地方整備局	情報通信ユビキタス環境（公共施設管理用光ファイバーとブロードバンド無線LANの連携）の実証実験。	http://www.sendai-it.jp/
11	列車インターネット実験	四国総合通信局	列車内で、通常のインターネット利用に加え、列車の現在地、電子ニュース、LIVE車窓風景(先頭車両に設置したIPカメラによるライブ映像)などを利用。	http://www.shikoku-bt.go.jp/
12	InternetITS	慶應大学、トヨタ自動車、デンソー、日本電気	次世代インターネット技術を基礎としたITSの共通基盤の構築による、ITSビジネスの創出・活性化、産学官にまたがるオープンな情報共有や意見交換。	http://www.internetits.org/
13	村井 純	慶應義塾大学	自動車がもつ情報をどのようにしてインターネット経由で取得できるようにするのかなど、インターネット情報システムから見た自動車の情報化。	http://www.sfc.wide.ad.jp/InternetCAR/

■日本　音声・音楽

1	VariPhrase	ローランド	Vari-OS、バリボイス、電子楽器、V-Guitarなどの音響関連の研究と製品開発。	http://www.roland.co.jp

	プロジェクト名	研究機関	コメント	関連サイト・URL
2	サイレント楽器、着メロ用LSI	ヤマハ	ブロードバンドVoIPルータ ネットボランチの開発や、ユビキタス環境を想定した携帯電話を利用した音楽評価サイトの運営。着メロ用音源LSI、電子楽器の開発。	http://www.yamaha.co.jp/
3	中村 哲・田中 英輝	ATR 音声言語コミュニケーション研究所	タスクや発話スタイルの影響を受けない頑健な音響・言語モデルの研究、ハンズフリー音声認識、マルチモーダル音声認識、機械翻訳システムと音声認識システムを高度に統合した、独話の同時通訳システムの開発。	http://www.slt.atr.co.jp/

■日本 セキュリティ・プライバシー関連

1	JIPDECプライバシーマーク	日本情報処理開発協会	適切なプライバシー保護とセキュリティー対策のための、国内における代表的なプライバシーマークの認定やリスクマネジメントに関する指針。	http://www.jipdec.or.jp/security/privacy/
2	河野 通宗	SONY CSL	ユーザインタフェースを活用したセキュリティモデルの研究。セキュリティとユーザビリティの両立を可能にするセキュリティモデルの構築。	http://www.csl.sony.co.jp/person/mkohno/index.html
3	MMCソリューションセンター	日立製作所	ユビキタス環境下で遍在するコンピュータにアクセスするための、利用者本人の認証情報を格納した耐タンパー性のあるデバイス「ユビキタスカード」の開発。	http://www.hitachisemiconductor.com/

■日本 教育関連

1	遠隔教育センター	東京都立科学技術大学	教師と学生が啓発しあう、双方向型のマルチメディア遠隔教育システムの研究。	http://www.dlc.tmit.ac.jp/
2	上林 彌彦 研究室	京都大学	データベース技術による教育支援に関する研究。講義中の様々な情報の損失を、データベース技術を用いて解決するシステム「VIEW Classroom」など。	http://www.db.soc.i.kyoto-u.ac.jp/

■日本 情報家電

1	情報家電の実証実験プロジェクト	国土交通省	ホームサーバを家電と相互接続する。各家電の操作や部屋の状況の確認。セキュリティ管理やコンテンツ配信の機能の分担や地域のコミュニケーションを容易にする。	http://www.mlit.go.jp/kisha/kisha01/07/071206_2_.html
2	みまもりネット	松下電工	家の中に設置した複数のセンサが住居人を感知。在室状況を携帯電話やパソコンなどにEメールで送る。また毎日の生活パターンから体調不良などを知ることができる。	http://www.mew.co.jp/mimamori/

	プロジェクト名	研究機関	コメント	関連サイト・URL
3	FEMINITY	東芝	家電をBlueToothで結び、ITホーム端末を用いてIT冷蔵庫の食材管理やITレンジにレシピの配信、更にドアセンサや位置情報サービスを提供する。	http://feminity.toshiba.co.jp/feminity/
4	エコーネット	エコーネットコンソーシアム	エアコン、冷蔵庫、照明、ガス漏れ検知、火災検知センサ類など、多くの機器のコントロールができる標準的なシステムの開発や	http://www.echonet.gr.jp/
5	Jini	セイコーエプソン、沖電気、東芝	情報機器や家電を簡単につなぐ次世代ネットワーク技術Jiniの開発。Javaの上に構築した分散オブジェクト技術で、プログラムも周辺機器も区別せずに扱える。	http://www.jini.org/
6	ALICE FORUM	住宅情報化推進協議会	豊かでゆとりある暮らしのために情報をどのように取り入れて行けば良いか、その実証的検討と最新技術の紹介により住宅の情報化を推進する。	http://www.alice-f.or.jp/
7	情報家電インターネットサービス	NHKエンジニアリングサービス	テレビやホームサーバ(蓄積機能を持つ放送受信機)がインターネットにつながると、どのような新しいサービスが可能になるかについての研究。	http://www.nhk.or.jp/strl/open2001/tenji/id43/index2.html
8	ep	ホームインターゲート株式会社	放送と通信融合の蓄積型双方向サービス「ep」でのデジタルテレビをはじめ、ネット 家電機器とインターネットサービスプロバイダとの接続のサポート事業。	http://www.home-intergate.com/
9	イージーインターネット協会	伊藤忠、ケンウッド、東芝、大日本印刷	簡単な操作でインターネットに接続できる非パソコン端末を「イージーインターネット端末」とし、インフラの構築やコンテンツ整備を行う。	http://www.eia.or.jp/
10	HIIハウス	松下電器	ネットワーク技術を用いた暮らしのコンセプトを具体的に提案。	http://matsushita.co.jp/
11	JEITA HOUSE	電子情報技術産業協会	東京・多摩ニュータウンの一戸建て住宅を借用し、最新のホームネットワークシステムと最新情報家電機器を組み込んだモデルハウスを建設し一般公開。	http://www.eclipse-jp.com/jeita/
12	美濃 導彦 研究室	京都大学	AMIDEN: ネットワークインタフェースを搭載したそれぞれのアプライアンスが自律的に動作して通信パスを構築し、複合的で柔軟なサービスを提供。	http://www.imel1.kuis.kyoto-u.ac.jp/index.html

注記

本報告書の中にある登録商標および商標は、該当企業･団体の登録商標であります。

次世代情報通信環境におけるヒューマンインタフェース技術
に関する調査研究報告書
－安心・安全なユビキタス社会へ向けて－

発　行　平成15年3月
発行所　財団法人　日本情報処理開発協会
東京都港区芝公園3丁目5番8号
機械振興会館B1
電話（03）3432-9390

14－H001