管理番号＃１３－０７

平成１７年度

研究開発成果報告書

ユビキタスコンピューティング環境を実現する基盤ネットワークプロトコルの研究開発

委託先：　㈱横須賀テレコムリサーチパーク

平成１８年４月

情報通信研究機構

平成17年度　研究開発成果報告書

（一般型）

「ユビキタスコンピューティング環境を実現する基盤ネットワークプロトコルの研究開発」

目　次

1 研究開発課題の背景

20 世紀後半より，情報通信技術・IT（Information Technology）の急速な進展と広範な普及によって，我々の社会は大きく変革し，いわゆる情報社会へと突入した．我が国も情報通信技術に関しては世界を牽引した数少ない国の一つして自負するに十分であり，多くの研究開発がなされてきた．現在も次世代携帯電話を始めとして，世界に貢献する成果を輩出している．

1.1 ユビキタスコンピューティング

1990 年代からの情報通信網基盤の爆発的発展は，ネットワークの大容量化と接続機器（コンピュータ）の高性能化によって，より高度なユーザサービスを実現してきた．それと同時に，近年の我が国では，これとは異なる情報通信網の急速な発展も起きている．それは，従来は情報処理能力や通信能力を持たなかった，身の回りに存在する無数の小さな「モノ」に対して，計算力と通信力を与える方向への爆発的な拡大である．こうした身の回りのあらゆるものをインテリジェント化することで，高いユーザサービスを実現する情報通信のパラダイムは，ユビキタスコンピューティング （Ubiquitous Computing）や「どこでもコンピュータ環境」と呼ばれている．このパラダイムは，1980年代後半に日米で同時に提唱され，その後ポストPC時代の情報通信技術のパラダイムとして，専門家の間で広く受け入れられている．

このユビキタスコンピューティングこそが今後の日本型の IT 技術開発のパラダイムとして有望なものであり，本研究開発課題はこのパラダイムの実現に対して正面から取り組むものである．

1.2 我が国の産業構造との関係

情報通信分野は極めて広範で深いため，単一の国や会社，組織ですべてをカバーすることは，もはや不可能である．世界全体でみた情報通信分野は，様々な国の様々な組織がそれぞれに得意な部分を分担し，世界規模で協調と競争をしながら発展していくのが健全な姿である．

現在，すでにインターネットやPCの分野の技術的主導権は米国が握っている．実際，パーソナルコンピューティング分野は，心臓部である CPU や OS といった根幹技術を"Wintel"という造語が示すように，米国の特定ベンダーの独占状態にあり，我が国の研究開発は壊滅状態である．しかし，情報通信分野で十分に大規模な収益が見込める分野は，インターネットや PC の分野だけではない．特に，ポスト PC 時代の主力産業と考えられる情報家電，ネットワーク機能をもった電子機器に目を向ければ，ITRON（Industrial TRON: The Real-time Operating system Nucleus）を始めとして，我が国の独自技術が世界的に強い競争力を維持し続けている．我が国の産業構造からみて得意な部分とは，小さく緻密な機器を生産するところにある．こういった視点からも，効率的な研究開発投資を考えると，むしろ，我が国が最も得意な分野を更に発展させることを目指すべきである．こうした技術は今だ世界の先端を走っており，この点を活かした新しい産業を創造し，世界をリードする分野を積極的に開拓すれば，当該分野の世界的イニシ

アチブを獲得することも可能である.

1.3 緻密でクリーンなIT技術開発への要求

21 世紀を迎え，光ファイバー網を使ったインターネット等が目指している，より速く・より大容量・より広帯域を追求する情報通信技術の重要性は高いものの，現在それに加えて更に，次のようなより緻密でクリーンな情報通信技術への要求も高まっている．第一に，豊富な容量・帯域・速度をもった IT 基盤上のデジタル情報の流れを，人間や社会の意志に基づいて確実に制御できること．権利がある人にだけに情報のアクセスを許可し，権利の無い人の不正な盗聴を防ぐこと，また，不正な情報複製ができないようにするといったことが，確実に行えることが重要である．従って，これには，広い意味での，暗号技術や認証技術などが含まれる．第二に，省電力をはじめとして，資源を浪費せず，環境への悪影響を最小限にとどめる，クリーンな情報通信技術．こうした考え方は，カームコンピューティング（Calm Computing）とも言われる．

1.4 セキュアコンピューティング

2001 年は，我が国でもサイバーテロが行なわれた．また，Nimda，CodeRed，Circum といったインターネットを介して大規模に感染するコンピュータウィルスやワームも発生した．既に米国では我が国以上にサイバーテロが行なわれ，情報社会を脅かしている．今後もこうした危険性は確実に拡大するだろう．現在の情報通信インフラで解決することが最も要求されている課題は，こうした攻撃に強い，セキュアな情報通信基盤である．しかもそれが，一般素人でも簡単に扱うことができなければならない．インターネットの当初の設計方針には，インターネットを通じて通信する者同士が信頼できないようなこと，また，これほどまでに素人ユーザの割合が多くなることは，想定されていなかった．現在これに対して抜本的対策を施さない限り，かつての公害問題のように，将来の情報社会に禍根を残すことになりかねない．

2 研究開発の全体計画

2－1 研究開発課題の概要

本申請によるプロジェクトの研究開発課題は、我々の身の回りの、あらゆるものにマイクロコンピュータと通信機能を組み込み、それらが互いに情報を交換しながら協調動作を行い、人間生活をより高度にサポートする、ユビキタスコンピューティング環境を構築するための、次世代通信の基盤プロトコルおよびそのシステムの確立である。

1. ユビキタスコンピューティング環境が目指す最終目標

ユビキタスコンピューティング環境とは、身の回りのあらゆるものにマイクロコンピュータと通信機能を組み込み、それらが互いに情報を交換しながら協調動作を行い、人間生活をより高度にサポートする環境のことである。今まで、こうした環境を使った IT の多様な「夢」が語られており、その「夢」を実現することが本研究プロジェクトの最終目標である。

例えば、家庭では、家に設置された温度センサーが常に外気温と室内温度を監視しており、居住者が部屋の温度を下げようとした時、もしも外気温が室温より低ければ窓を開ける。しかし、部屋でピアノを弾き、外部に騒音が漏れたら、窓を閉めて自動的に空調が入る。また、自家用車で帰宅するときに、自動車のナビゲーションシステムから、到着時刻に合わせて自宅の風呂の湯を沸かすこともできる。

こうした環境を実現するためには、膨大なコンピュータを身の回りのあらゆるものに埋め込み、人間自身も常にコンピュータを携帯し、それらが互いにネットワークで接続され、情報交換しながら協調処理を行うメカニズムが必要とされる。我々は、この埋め込まれたり、携帯されたりするコンピュータを「インテリジェントオブジェクト」とよび、これらを接続する通信メカニズムのことを「ユビキタスネットワーキング」と呼ぶ。

本研究では生活空間を構成する大量のインテリジェントオブジェクトからなるネットワークを想定している。このネットワークと他の既存のネットワークとの違いは、まずネットワークにつながるノードの数が桁違いに多いことである。一人当たり数十から数百のプロセッサがある高密度のユビキタスコンピューティング環境のなかから、通信すべき適切なコンピュータを指定するためにはどうすればよいか。更にそれが何百、何千もの人が活動するビルや都市、最終的には世界までつながった時に、このユビキタスネットワーキングがどのように展開されるべきか、といったことが重要な課題となっている。従って、本研究における中心課題は、この「ユビキタスネットワーキング」の根幹となる基本方式を明らかにし、更にそれを動作させるシステムを構築することである。

これらの多くのインテリジェントオブジェクトを協調させるためには、調停動作の実現がポイントである。例えば、一億個のコンピュータがネットワークにつながった場合、全部のデータを手に入れそれに基づいて中央で方針を決定するという、中央集権的な手法で全部の動作を最適化することはもはや不可能ではないかと考えている。そのためには何らかの分散的な最適化方

式を考案する必要がある。

生活の場におけるインテリジェントオブジェクトは個々のエンドユーザの都合でネットワークに突然追加されたり、はずされたり、次の日には別の箇所につながったり、ということが起こる。そのような「アドホック(ad hoc)」性をもったネットワークを実現しなければならない。その際に一般の人でも扱え、面倒なオペレーションが不要な「エフォートレス(effortless)」な性質を持つ必要がある。ユビキタスコンピューティング環境において、無数のコンピュータをちりばめた時に重要なことは、その上で、これらのコンピュータ群が 24 時間 365 日正常動作するように運用できることである。そのためには、ユビキタスコンピューティング環境を構成するシステムと社会との親和性、運用技術に対する研究も重要となる。

2.技術課題の概要

本研究では、このユビキタスコンピューティング環境の基盤技術となる通信プロトコル(ユビキタスネットワーキングプロトコル)や、それを用いた通信網基盤の構築技術の研究開発を行う。そのために以下の研究開発項目を実施する。

(a) リアルタイム通信プロトコル
(b) セキュアネットワーキング、セキュアコンピューティング
(c) コンパクト性
(d) エフォートレスオペレーション、エフォートレスマネジメント
(e) ユーザとの親和性
(f) 省リソース
(g) 既存通信網との親和性
(h) 高度な協調・調停動作による人間生活の支援機能の実現

(1)リアルタイム通信プロトコル

ユビキタスコンピューティング環境を実現するための基本プロトコルには、人間の振る舞いや生活・社会を構成するあらゆる事象に追従して応答できるための、(ソフト)リアルタイム性が必要である。特に、身の回りのインテリジェントな機器(アクチュエーター)を制御する部分には、より強いリアルタイム性が要求される。

(2)セキュアネットワーキング、セキュアコンピューティング

先に述べたユビキタスコンピューティング環境による夢、例えば、未来の ITS(Intelligent Transportation System)のイメージとして、自動車のナビゲーションシステムから、到着時刻に合わせて自宅の風呂の湯を沸かすといったシナリオが描かれてきた。実際に、このシナリオを実現するためには、悪意ある他者が自宅の風呂を操作することを防げなければならない。更に近年は、サイバーアタックやクラッキング、サイバーテロを想定した対策も求められている。ユビキタスコンピューティング環境を、ネットワーク経由のアタックから守るためには、セキュアな通信プロト

コル、セキュアな通信システムの開発が不可欠である。ネットワーク基盤の遍在化（ユビキタス化）が急速に進んでいる現在、セキュリティーを向上させる技術開発は急務である。

（3）コンパクト性

ユビキタスコンピューティング環境では、非常に膨大な数の小さな機器にコンピュータや通信機能が埋め込まれる。従って、各ノードが小さくコンパクトであること重要である。計算機能や通信機能の遍在性（ユビキタス性）を高めるためには、各ノードがコンパクト化できることが不可欠であり、本研究課題における目標としては、SOC （System-On-Chip）上で実現できる程度にまで最適化を図る。

（4）エフォートレス（Effortless）

ユビキタスコンピューティングのためのネットワークプロトコルを実現する上で重要なことは、コンピュータに詳しくない一般利用者でさえも、自身が所有する機器の安全性、蓄積情報や通信の秘匿性等を手軽に確保できることである。現在でも多くのセキュアプロトコルがあるが、そのほとんどが、認証や暗号のための鍵の管理や認証局（CA 局）からの証明書の取得といった、専門知識を要する運用作業を伴うため、普通の人が手軽に使えるものになっていない。そこで、本研究課題では、耐タンパ性を有するハードウェアを利用することによって、より手軽で簡便なセキュア通信プロトコルを開発する。このプロトコルによって、簡単に使えるパッケージ化された強固で安定した汎用セキュリティー基盤が実現され、コンピュータに詳しくない普通の人でも、セキュアな通信基盤の恩恵に浴することができる。

（5）ユーザとの親和性

ユビキタスコンピューティングは、人間の身の回りに計算機能や通信機能を埋め込むことで、人間生活をサポートする。そこで、重要な観点の一つは、どのように人間をサポートしていくかということである。ユビキタスコンピューティング環境においてこうした人間との境界部分、つまりヒューマンインタフェースをつかさどる分野は、強化現実環境（Augmented Reality）とか、複合現実環境（Mixed Reality）といった分野となる。本研究でも人間にとって、より自然でかつ利便性の高いサポートの手法の研究開発を進める。

（6）省リソース

ユビキタスコンピューティング環境では、ノード数が従来の分散環境やインターネット環境にもまして膨大な数になることから、一つのノードが使う電力量など、消費する各種リソースが小さくなるような Calm Computing 技術を確立する。従来の情報通信技術は、性能や利便性を最大化するための研究開発に重きがおかれており、省資源を最大化するといった基準に則った研究開発は比重が低かった。本研究課題で実現するプロトコルやシステムでは、こうした省電力・省資源を実現する。

(7)既存通信網との親和性

現在、IP による世界的ネットワークが構築されている。その他にも既存の通信網には、携帯電話網、通常の加入電話網をはじめとして、多様なものが存在する。これらは、性能、サービス、保守の容易性といった点で利害得失があり、これらが単一のプロトコルに統合されるとは考えづらい。ユビキタスコンピューティング環境を構成する通信プロトコルに関しても同様に、様々な利害得失をもった多様なプロトコルが混在する環境を前提とし、互いに補完的な関係になることが理想的である。

そこで、本研究開発課題では、こうした既存の多様なプロトコルとの相互接続によって、柔軟な情報交換や制御を行うメカニズムを確立する。具体的には、現在の IPv4・IPv6 に基づくインターネット、携帯電話網上に構築されている情報通信網基盤と、ユビキタスネットワーキングプロトコルとを相互接続する、ゲートウェイ技術を確立する。それは単に、ネットワーク層やトランスポート層によるゲートウェイだけではなく、セッション層やアプリケーション層にいたる、ほぼ全ての層において接続する必要があり、そのための統合的なゲートウェイ技術を構築する。

(8)高度な協調・調停動作による人間生活の支援機能の実現

ユビキタスコンピューティング環境では、単に多くのノードがあるだけでなく、それらが「協調」「調停」動作をすることで、人間生活を高度に支援する。例えば、部屋の温度が上ったら、窓を自動的に開け、もしも部屋の中でピアノをひきはじめ騒音が発生したら、窓を自動的に閉めて空調を入れるといった動作である。こうした協調・調停作業が、あちこちに埋め込まれた膨大な数のコンピュータの間で実施できなければならない。そのための通信システム、交換情報形式、超機能分散型ソフトウェアのためのプログラミングシステムなどの研究開発を行う。

3. 研究実施計画の基本方針(概要)

ここでは、1.、2.で示した本研究の目標と課題を達成する実施計画の方針の概要を示す。

(1)システム単位のサブプロジェクト構成

本研究開発課題における技術的ボトルネックは、いかに大量の小さいノードを、特定の目的に沿って協調動作させるかという、システム統合技術にあると考えている。そこで、要素技術毎に細分化したサブテーマわけをした場合、最後に統合化して相互接続環境を構築するのが困難になるため、次の通り「機器」による切り分けを中心としたサブテーマわけを行う。

- セキュアハードウェア
- 通信システム
- ユーザ側のエンドノードシステム(モバイル端末／情報家電／PDA 等)
- サーバ側のエンドノードシステム(認証サーバ／アプリケーションサーバ等)
- システム統合技術
- 超機能分散システム指向の開発環境

(2)システム工学的検証の重視

ユビキタスコンピューティング環境は、単に情報通信のメカニズムだけを研究開発するだけでは成功しない。ユビキタスコンピューティング環境は、人間・社会生活に無数に埋め込まれ、社会活動や生活を支援するものであるため、技術的に優れていても、例えば騒音や発熱の程度によっては人間生活にはなじまない。公共の場に設置するものは、多少の悪戯や荒い扱いにも耐えなければならない。膨大な数のノードが現実社会の中で容易にかつ安全に運用できるのか、無数に埋め込まれたインテリジェントオブジェクトのメンテナンスは可能なのか、ユビキタスコンピューティング環境のセキュリティーは厳密に運用できるのか、といった諸問題がある。

そこで、本研究開発課題では、こうした社会や生活と、ユビキタスコンピューティング環境の間の親和性を重視し、本研究開発成果を実用に耐えるシステムとして完成させるために、システム工学的見地からその検証を行う。検証項目としては、①システムの信頼性の検証、②運用評価、③ユーザビリティ、④スケールファクターのシミュレーション、⑤環境アセスメントを計画している。

4. 研究実施計画の詳細(システム部分)

システム面の研究のサブテーマは、「3. (1)システム単位のサブプロジェクト構成」の部分で述べたとおり、機器種類毎に切り分けを中心とする。サブテーマとしては、以下を計画している。

【サブテーマ1】
セキュアコンピューティングの基盤となるセキュアハードウェア
【サブテーマ2】
基盤通信システムの研究開発
【サブテーマ3】
ユーザノードシステムの研究開発
【サブテーマ4】
サーバノードシステムの研究開発
【サブテーマ5】
ユビキタスコンピューティング環境を構成するシステム統合技術の研究開発
【サブテーマ6】
超機能分散システム指向の開発環境の研究開発

【サブテーマ1】セキュアコンピューティングの基盤となるセキュアハードウェア

通信のセキュリティーは一般的にはソフトウェアだけで確保することはできない。何らかのハードウェアによる情報保護が不可欠である。従来型の情報システムでは、機材が設置されてい

る建物や部屋に対する入退館管理等による物理的な保護が前提であった。ユビキタスコンピューティング環境では、公共の場に露出して設置されたものも対象であり、ユーザが常に携帯し頻繁に紛失や盗難が起きるものまで含まれる。しかも、前述したようにセキュリティを確保するために、ユーザが暗号・認証の仕組みを理解することが必須であってはならない。

そこで、本研究では、LSI 自体に不正アクセスが加えられないように加工を施した、いわゆる「耐タンパ性（Tamper Resistance）」を有するハードウェアを、ユビキタスコンピューティング向けチップとして新規に開発し、それをユビキタスコンピューティング環境のセキュアシステムの基盤パーツとする。本研究では、ユビキタスコンピューティング環境を構成する耐タンパーチップとして、以下の 2 種類を研究開発する。

コンタクトレスチップ

ユビキタスコンピューティング環境と、ISO14443 規格に基づくコンタクトレス通信上で、ユビキタスネットワークプロトコルをサポートする。

デュアルチップ

ユビキタスコンピューティング環境と通信する、ISO14443 上のコンタクトレス通信チャンネルと、機器組み込み用のセキュアな内部チャンネルの 2 つを有する、デュアル型の耐タンパーチップである。

従来から、IC カードなどに用いられている LSI チップも似た性質を持っているが、それらと比べた場合においても以下の新規性をもたせる。

- 分散環境ノードとして動作
- 公開鍵暗号技術を基盤とした暗号／認証系のサポート（PKI にも対応）
- 高度な省電力機能

【サブテーマ2】基盤通信システムの研究開発

(2-1) 基盤プロトコル概要

基盤通信システムのサブテーマでは、ユビキタスコンピューティング環境を構成する通信システム全般を扱い、本研究の核であるユビキタスネットワークプロトコルの研究、そのプロトコルスタックの開発、ルータをはじめとした各種ネットワーキング装置を含む。ユビキタスコンピューティングシステムにおいては、その目的に最適化したネットワークアーキテクチャを導入する。今回の研究対象となるユビキタスネットワークのアーキテクチャと機能は以下の特徴をもつ。

(2-2) データリンク層

データリンク層は既存の方式を用いる。例えば、2.5GHz および 5GHz 帯の無線 LAN、Bluetooth、ISO 14443、PHS、第 3 世代の移動体通信ネットワークなどである。これらの方式としては、端末と端末が直接通信するアドホックモードの通信形態と、基地局およびバックボーンネ

ットワークを介した通信形態の双方を開発する。

(2-3) ネットワーク層

ネットワーク層はユビキタスネットワークに適した新しい方式を考案して実現する。通信形態は、ユニキャストとマルチキャストをサポートし、それぞれ帯域保証や優先制御を行うリアルタイム通信と、ベストエフォート通信を扱う。帯域保証等を行うリアルタイム通信の場合は、そのためのシグナリングを提供する。

ここでは、Layer 2 ARP(Address Resolution Protocol)が必要である。ユビキタスネットワーキングでは、IP で使用される ARP とは異なり、実世界上の位置や社会的なセマンティックスなどに基づいたノード指定に対応する(デバイス・ノードルックアップ機能)。

ネットワーク構成やノード間の帯域などのルーティング情報を交換するルーティングプロトコルを実現する。このプロトコルは、ユニキャストのためのプロトコルと、マルチキャストのためのプロトコルの双方、またダイナミックな変化に追従できる柔軟性が必要となる。

更に、ネットワークにおける輻輳や障害等を通知するための OAM (Operation Administration and Maintenance)情報交換プロトコルを備える。このプロトコルは、ネットワーク経路上の故障に加え、リアルタイム通信のための輻輳の検知やマルチキャストにおける障害情報の転送などを、統合的にサポートする。

(2-4) トランスポート層

トランスポート層のプロトコルとしては、コネクション型とコネクションレス型のプロトコルを用意する必要がある。双方のプロトコルとも、遅延変動や誤り率などのサービス品質に関して、アプリケーションが要求する品質を最小限の機能で実現するサービス品質機能を有する。コネクション型のプロトコルはユニキャストを対象とし、コネクションレス型のプロトコルはユニキャストとマルチキャストの双方を対象とする。また、通信相手の指定については、アドレスを指定する方式のほかに、要求条件を指定する方式についてもサポートする。確認応答を有し、信頼性の高い通信を可能とするマルチキャスト用のプロトコルも用意する。

(2-5) セッション層

セキュリティーや認証のための機能を提供する。相互認証と同時に鍵交換を行い、セッション中は暗号通信が行なわれるセキュアセッション機能、またロールバック機能を備えたトランザクションセッション機能、リアルタイム応答が要求される場合のライトウェイトセッション機能を備える。

(2-6) アプリケーション層

アプリケーション層は、各種応用に対応するプロトコルを用意する。その他に、通信のサポートのために各種応用から共通に使用されるプロトコルを用意する必要がある。1 つは、サービス

ルックアップ機能で、サービス名からそれを提供するノードの物理アドレスを検索するなど、各種のネットワーク構成情報の検索プロトコルを構築する（サービスルックアッププロトコル）。また、ネットワーク機器の状態監視や構成変更などを遠隔で行うネットワーク管理用プロトコルも備える。

【サブテーマ3】ユーザノードシステムの研究開発

ユビキタスコンピューティング環境を構成するノードの中で、ユーザと直接接することが想定される機器類の研究開発である。これをここではユーザノードと呼ぶが、想定されるユーザノードには、ユーザが携帯する移動ノードと、生活環境に設置される固定ノードがある。双方とも、「(2)基盤通信システムの研究開発」のサブテーマで開発された、ユビキタスネットワーキングプロトコルを搭載する。移動か固定かに応じて、利用可能な計算・通信資源や、物理通信路の環境、物理的な大きさ、それに基づくユーザインタフェース等が異なるために、それぞれ固有の実現技術が必要とされる。本サブテーマでは、こうした条件に適合した様々なユーザノードの構成方法・機構を中心に研究開発を進める。

(3-1) 移動ノード

移動ノードや、常にユーザが携帯してユーザとユビキタスコンピューティング環境との間のインタフェースの役割を担う端末である。具体的には、PDA（Personal Digital Assistant）、携帯電話スマートカードなどが想定される。固定ノードと比べた場合、移動ノードに関する研究課題として以下がある。

- 物理通信路は基本的に無線通信であり、ユーザの移動を考慮すると通信品質は安定しない、
- 紛失・盗難が起こる可能性が高いため、それに備えたセキュリティーメカニズムを備えること、
- 物理サイズが小さいため、それに適した洗練されたユーザインタフェース、
- 計算資源も限られているため、コンパクト性が求められる。
- バッテリー量の制約も大きいため、徹底した省電力機構。

移動ノードでは、こうした条件をクリアした中で、ユビキタスネットワーキングプロトコルの実現技術を確立する。ここでは、カスタム LSI を作成することを念頭に置く。

(3-2) 固定ノード

固定ノードは、ユビキタスコンピューティング環境に設置され、人間の振る舞いや、環境の変化に応じて柔軟かつ緻密に動作するインテリジェントオブジェクトである。具体的には、住宅内にある電子機器類、オフィスにあるコピー機やファックス、シュレッターといった機器、また公共の場に設置された券売機、自動販売機、チケットゲートといった機器を想定している。移動ノードと比べた場合の固定ノードに関する研究開発項目の特徴は、以下の通りである。

- 物理的認証をうけない不特定多数によって利用されることが前提となり、そのための認証機能、セキュリティー機能が必要とされる。
- 特に公共の場に置かれた機器は、ネットワーク的にも公共的なセグメント上に置かれることになり、その場合にセキュア通信の確保
- ユーザノードであると同時に、サーバ的な機能の提供も求められる。
- 回線や電源の状況は良い環境にある。

固定ノードでは、こうした特質を前提とした、ユビキタスネットワーキングプロトコルの実現技術を確立する。

【サブテーマ4】サーバノードシステムの研究開発

サーバノードは、ユビキタスネットワーキングプロトコルを実現し、特にユーザノードを対象としてネットワークサービスと機能を提供するノードである。具体的には、①セキュアセッションのための認証局、登録局、②分散トランザクションを支えるトランザクションサーバ、③サービスルックアップやデバイスルックアップのためのネットワーク環境サーバ、④ネットワーク管理のための管理サーバ、⑤各アプリケーションに依存したアプリケーションサーバなどが想定される。

従来の電子商取引分野の研究開発の経験により、サーバの運用者側の不正行為も問題とされており、サーバ側も耐タンパー性を持ったハードウェア構成が必要である。かえって移動型のユーザノードのように小型機器の方が、対タンパー性を実現することが容易であり、サーバノードの場合は、大きなノードにおいての耐タンパーハードウェアの実現技術が課題である。

また、ユビキタスコンピューティング環境においては、サーバにおいても、セキュア性を保ちながら、リアルタイム性を実現できるに十分な高応答性能を実現する必要がある。そこで、本研究開発課題では、サーバをセキュアに性能向上させるための、セキュアクラスタリング、暗号・認証処理機能を持ったデータキャッシュ・プロセスマイグレーションのメカニズムを確立する。特に、動的な情報更新が可能な高応答性を達成できるディレクトリサーバを実現する。

【サブテーマ5】ユビキタスコンピューティング環境を構成するシステム統合技術の研究開発

ユビキタスコンピューティング環境は、様々なプロトコルを用いる様々な膨大な機器がヘテロジニアスに結合したシステムであり、それを統合し協調動作させるための技術を確立する。その統合技術を要素技術に分割すると、以下の項目が挙げられる。①通信環境を意識する必要のない確実なコネクティビティおよびサービスの実現、②ネットワーク運用状況、サービス実行状況に応じた、最適なリソース配分によるコンパクトネットワーク／サービス実行環境の構築、③通信環境に最適化したサービス実行メカニズム、④ネットワークへのノードの簡単な装着／脱着と移動時のサービス継続の開発。

上記の課題を実現するときに、本研究開発課題で開発するプロトコルと既存のIPや電話網を使った通信プロトコルの相互運用をスムーズに行うため、次の基本技術の開発を目指す。①アドレスを陽に指定しないアドレス解決およびルーティングメカニズム、②プロトコル変換メカニズ

ム、③複数の異なるネットワークをまたがったときの品質制御メカニズム、④端末と連携したサービス実行メカニズム。

【サブテーマ6】超機能分散システム指向の開発環境の研究開発

ユビキタスコンピューティング環境を構築する上での技術的な課題として、システム開発効率がある。ユビキタスコンピューティング環境は、他の分散環境と比べると、膨大なノード数に特徴がある。現在の計算機科学では、ここまで分散化された多数のノードを協調動作させるソフトウェアを効率よく開発する手法が存在しない。しかも、各ノードはリアルタイムプログラミングとセキュリティーという、単独でも困難なプログラミングを施さなければならない。従って、ユビキタスコンピューティング環境のソフトウェアの開発環境は重要であり、本研究の成否を左右する大きな課題である。

現在計画している開発環境研究は、以下の 3 段階で進める。

- ユビキタスコンピューティング標準開発環境
- ユビキタスネットワーキングプロトコルを扱うミドルウェア
- ユビキタスコンピューティング環境における情報処理モデルの確立

(6-1) ユビキタスコンピューティング標準開発環境

ユビキタスコンピューティング環境は膨大な数のノード数になる。まずハードウェアやオペレーティングシステムといった基盤ソフトウェア部分に対する標準化が必要である。膨大なノード数をまちまちの開発環境で構築しては、ソフトウェアの再利用性の観点から効率よくプロジェクトを運営できない。そこで、まず本プロジェクトの標準ハードウェア、標準基盤ソフトウェアの仕様を決め、その上でのユビキタスコンピューティング環境やユビキタスネットワーキングプロトコルのソフトウェアの再利用性、移植性の高い環境を構築する。

(6-2) ユビキタスネットワーキングプロトコルを扱うミドルウェア

ユビキタスネットワーキングのアプリケーション層のプログラミングを支援するためのミドルウェアを構築する。現在は、こうした分散環境のプログラミングに適したオブジェクト指向言語である Java を用い、このクラスライブラリとしてミドルウェアを構築する。また、ユビキタスコンピューティングに適したコンパクトでセキュアな Java VM（Java Virtual Machine）の実現も行う。

(6-3) ユビキタスコンピューティング環境における情報処理モデルの確立

ユビキタスコンピューティング環境を実現する上で最も重要な分散協調動作を実現するソフトウェアの構築手法を研究する部分である。このテーマにおいても、次の2つのサブテーマを計画している。

- 現実世界の記述方式
- 超機能分散環境に適したプログラミングモデル（協調動作の記述）

ア. 現実世界の記述方式

ユビキタスコンピューティング環境では、現実世界にコンテクストを取得し、協調動作の結果として、何らかの作用を現実世界にフィードバックする。こうした処理をコンピュータが扱うためには、現実世界をデジタル情報で表現し、それをノード間で交換できるための標準形式を構築する必要がある。しかもユビキタスコンピューティングが扱う事象は、単にオフィス空間といったものだけでなく、人間社会生活のあらゆる場面に及ぶため、まさに、現実世界あのあらゆる事象の標準デジタル表現形式を研究開発する。

イ. 超機能分散システムのプログラミング技法

従来は、ネットワーク接続された複数のノード間における分散処理は、オブジェクトベースでモデル化したソフトウェア開発が主流になっている。しかしユビキタスコンピューティング環境のようにノード数が膨大である場合、扱うオブジェクト数も膨大になるため、その間の協調動作をノードオブジェクトレベルの peer-to-peer の協調関係をベースとした動作でプログラミングしては、抽象度が低すぎるということが問題となっている。従って、本研究では、ユビキタスコンピューティング環境全体に対して「計算場（Computing Field）」と呼ばれる仮想的なプログラミング抽象を提供し、各ノードとこの計算場の間の協調動作によってプログラミングする。

5. 研究実施計画の詳細（システム工学的検証）

ユビキタスコンピューティング環境と人間社会・生活の間の親和性を重視し、本研究開発成果を実用に耐えるシステムとして完成させるために、システム工学的見地から、以下の検証を行う。

【サブテーマ7】ユビキタスネットワーキングシステムのシステム工学的検証

(7-1) 信頼性の検証

本研究開発課題で構築されたシステム（以下、本システム）を、実際のユビキタスコンピューティング環境と同様の設置状況において運用し、そのシステム信頼性を検証する。ユビキタスコンピューティング環境は、生活のあらゆる面を支援するタイプのシステムであるため、誤作動などは致命的であり、この点に関する検証を行う。

(7-2) 運用評価

実際に本システムに想定される技術レベルの人員が、実験的に作られた本システムの環境を、一定期間オペレーションすることによって、①統合的視点によるセキュリティー強度の検証、②運用やメンテナンスの容易性を評価する。

(7-3) ユーザビリティ評価

本システムが利用者に提供するサービスのユーザインフェース手法について検証、評価する。特に、情報通信に関する技術に明るくない一般ユーザに対するユーザビリティ、また、身体障害者や子供、老人を含めたあらゆる人に対して使えるシステムになっているかという、ユニバーサルデザインの視点による評価を重要視する。

(7-4) スケールファクターのシミュレーション

本研究開発プロジェクトはあくまでも研究段階のものであるため、本研究成果が実際に世の中に大規模に普及した場合、どのような問題が起こっていくかを、本研究における実験のサンプルデータを使ったシミュレーションによって検証する。

(7-5) 環境アセスメント

本システムを生活環境に埋め込んだ場合の、放熱、騒音、電磁波などの影響を計測し、人体や他の機器、環境に対する影響を調査する。その結果をシステムの省資源部分にフィードバックしていく。

2－2 研究開発目標

2－2－1 最終目標(平成18年3月末)

■全体を包括する最終目標(概要)

(1) 人間の振る舞いや生活・社会を構成する事象に追従して応答するのに十分なリアルタイム性を持つ。この観点からソフトリアルタイム性で十分であるものの、正常に通信処理が行なわれた場合には、PAN、LAN環境では1ms以内、WAN経由では0.1s以内の誤差を目標とする。

(2) 公開鍵暗号とPKIをベースとした暗号、認証のメカニズムを有し、社会のインフラを支えるユビキタス環境にふさわしい安全性と信頼性を実現できること。

(3) 情報家電やインターネットアプライアンスといった比較的乏しい計算機環境の上でも効率よく動作するように、実行性能がよくかつ規模が小さいシステムになっていること。基盤プロトコル全体で、200～300KB程度の規模を狙う。

(4) システムを管理するための労力が小さいこと。具体的には、ユビキタスコンピューティング環境を構成する機器が設置されたら、たとえ停電等が起きても、無設定で復旧し、基本的に機器が故障するまで、メンテナンスする必要がない。

(5) 非専門家でも扱える簡便さを有すること。例えば、暗号・認証機構を知らない人でも、セキュアネットワーキングサービスを利用できること。

(6) 省リソース対応した回路技術を確立する。特に、省電力機能による電磁ノイズ発生の問題等を解決する。

（7） IP 網、デジタル方式の携帯電話網、PHS 網、固定加入電話網、ADSL 網といった、既存通信網との間のインターオペラビリティ―機能を有すること。

（8） ユビキタスコンピューティング環境における典型的な協調・調停動作を複数実現することに成功し、その処理コードを分散透明な高い抽象度で記述できること。

■サブテーマ別の最終目標（詳細）

ア．基盤通信システムの研究開発

（1） ユビキタスネットワーキングプロトコルのセッション層部分までの基本プロトコルの仕様を開発し、その正当性、有効性を検証する。

（2） 上記のプロトコルを実現し、評価を行う。

（3） ユビキタスネットワーキングの物理層・データリンク層を担う、以下のプロトコル・ネットワークシステムの上で動作させるためのスタブ部分の仕様を開発すること。

(3-1) Bluetooth

(3-2) ISO 14443

(3-3) IEEE 802.11

(3-4) ISO 7816

(3-5) 無線系電話プロトコル

（4） 既存のインターネット網である IPv4、IPv6 網との間で相互運用と情報交換を可能にするゲートウェイ技術およびシステムを開発する。

（5） 基本機能として、認証機能、暗号機能を有すること。

（6） 認証・暗号に用いる鍵は、本研究のサブテーマ「カ．」で開発したセキュアハードウェアに格納する。

（7） ソフトウェア規模は、200KB～300KB のバイナリサイズを想定する。

イ．ユビキタスコンピューティング環境を構成するシステム統合技術の研究開発

（1） IP 通信網や電話網などの既存の通信網との相互接続性を検証する。

ウ．超機能分散システム指向の開発環境の研究開発（ハードウェア部分）

（1） ユビキタスコンピューティング環境の構築に用いる標準開発プラットフォームとしてのハードウェアを開発する。

（2） その上で、サブテーマ「**エ．**」で開発した標準 OS が動作する。

（3） サブテーマ「**カ．**」で開発したデュアル型のセキュアチップを搭載している。

（4） サブテーマ「**ア．**（3）」で挙げた各種 LAN、PAN のプロトコルを搭載可能である。

（5） 音声 CODEC を備える。

（6） グラフィックチップを備える。

（7） CPU 性能として、300MHz 以上の動作周波数を持つこと、また主記憶として 32MB

以上を格納すること。ハードディスクを搭載可能な回路インタフェースを備える。

エ. 超機能分散システム指向の開発環境の研究開発（ソフトウェア部分）

（1） 本研究サブテーマ「**ア.**」で開発するユビキタスネットワーキングプロトコルを標準機能で組み込み、それを本研究全体の標準プラットフォームとして利用する、標準リアルタイム OS を開発する。

(1-1) マルチタスク機能と、豊富なタスク間通信・同期機能を提供することができる。

(1-2) 省電力機能を有する。

(1-3) 本研究のサブテーマ「**カ.**」で開発したセキュアチップとの通信機能を有する。

（2） 本研究サブテーマ「**ア.**」で開発するユビキタスネットワーキングプロトコルに対して高抽象度のプログラミングインタフェースを提供するためのミドルウェアを開発する。

(2-1) オブジェクト指向言語 Java のクラスライブラリとして構成されている。

(2-2) ユビキタスコンピューティングに適する、軽くソフトウェア規模の小さい Java Virtual Machine を開発する。

（3） 現実世界記述標準形式に関する研究開発

(3-1) ユビキタスコンピューティング環境が取り扱う実世界の各種環境情報の標準デジタル表現形式を策定する。

(3-2) ユビキタスコンピューティング環境が扱うあらゆるパラメータの表現を目指すため、その規模を例えると、「理科年表」のようなものになると考えている。

(3-3) 開発された標準記述形式は、ユビキタスネットワーキングプロトコルのプレゼンテーション層標準の一部として、全機器において使う。

(3-4) 表現の枠組みとしては、文字列形式である XML（eXtensible Markup Language）とバイナリ形式である TAD（TRON Application Databus）形式を構築する。特に後者は表現情報を効率よく表現できるための圧縮表現形式として、計算機資源が乏しいノードで利用する。

（4） 超機能分散プログラミングモデルに関する研究開発

(4-1) ユビキタスコンピューティング環境中に存在する莫大なノードの協調動作を高い抽象度でプログラミングできるプログラミングモデルおよび、そのプログラミング環境の開発を行う。

(4-2) ノード数は、数十から数万までを取り扱うことができ、ノードの分散性、動作の並列性をエンカプスレーションすることができる。

(4-3) あるユビキタスコンピューティング環境で動作していたソフトウェアをそのまま同じ機能をもった、他のユビキタスコンピューティング環境上でも稼動する移植性を有する。

オ. ユビキタスネットワーキングシステムのシステム工学的検証

(1) 本研究開発課題で構築したユビキタスコンピューティング環境の、一年程度の試験を行い、その期間の運用に耐えること。

(2) 現実社会における仕組みの中で運用しても、十分なセキュリティー強度、運用の容易性が達成できること。

(3) 情報通信分野の素人である一般ユーザでも十分本システムを使いこなし、ユビキタスコンピューティング環境の機能の恩恵を受けられること。

(4) ユーザインタフェース部分には、ユニバーサルデザインが施されていること。

(5) 本研究開発課題で作成した実験レベルのシステムの運用データに基づき、それを都市レベルに拡大して普及させた場合の各種スケールファクターが確かめられること。

(6) 本システムを社会・生活の場に持ち込んでも、ユーザに不快感を与えたり、社会活動に悪影響を与えたりしないこと。

■主に再委託する予定のサブテーマ

以下、中心部分を再委託する予定のサブテーマの最終目標について記す。

カ. セキュアコンピューティングの基盤となるセキュアハードウェア

(1) コンタクトレス(無線)チャンネルのみを有するコンタクトレスチップと、コンタクトレス(無線)チャンネルとコンタクト(有線)チャンネルの双方を有するデュアルチップを開発する。

(2) コンタクトレス通信チャンネルの物理層・データリンク層のプロトコルは、ISO14443 Type-C 規格を満たす。

(3) コンタクト通信チャンネルの物理層・データリンク層のプロトコルは、ISO 7816 規格を満たす。

(4) 本課題で開発したユビキタスネットワーキングプロトコルで通信する機能を備える。

(5) PKI を使った公開鍵暗号技術に基いた暗号機能・認証機能を備える。

(6) 共通鍵暗号技術に基いた、実行効率のよい暗号機能・認証機能を備える。

(7) 耐タンパー性を有しており、悪意あるユーザからの不正操作から格納情報が守られる。

(8) ユビキタスコンピューティング環境を構成するノードに組み込むことで、そのノードの通信の安全性を向上できる。

(9) CPU には 16bit 以上のワード幅を持ち、RAM: 10KB、ROM: 64KB、EEPROM: 64KB 以上を有する。

キ. ユーザノードシステムの研究開発

(1) ユーザノードとは、ユビキタスコンピューティング環境の中で、利用者が直接接するユーザインタフェースをもった機器である。移動ノード、固定ノードとして、それぞれ複数種類のインテグレーションされたユーザノードを開発する。

(2) ユーザノードは、最終的にはサブテーマ「**ウ.** 」で開発した標準ハードウェアを用い、サブテーマ「**エ.** 」で開発した標準 OS、ミドルウェアなどを利用して開発する。

(3) サブテーマ「**ア.** 」で開発したユビキタスネットワーキングプロトコルを実現する。

ク. サーバノードシステムの研究開発

(1) サーバノードとは、ユビキタスコンピューティング環境を裏で支える基盤サーバ群を含む。

(2)サーバノードは、以下の機能を提供する。

- CA 局や鍵配布サーバを含む PKI(公開鍵インフラストラクチャ)機能
- 電子マネーや電子チケットの決済機能
- 価値情報の発行機能
- デジタルコンテンツの発行機能

(3) サーバノードも悪意ある攻撃から守るためにハードウェアに一定の耐タンパー性を持たせる。

2−2−2 中間目標(平成16年3月末)

■全体を包括する中間目標

(1) 公開鍵暗号とPKIをベースとした暗号、認証のメカニズムを有し、社会のインフラを支えるユビキタス環境にふさわしい安全性と信頼性を実現できること。

(2) 情報家電やインターネットアプライアンスといった比較的乏しい計算機環境の上でも効率よく動作するように、実行性能がよくかつ規模が小さいシステムになっていること。基盤プロトコル全体で、200〜300KB 程度のソフトウェア規模を狙う。

(3) 非専門家でも扱える簡便さを有すること。

(4) システムを管理するための労力が小さいこと。

■サブテーマ別の中間目標（詳細）

ア．基盤通信システムの研究開発

（1） ユビキタスネットワーキングプロトコルのセッション層部分までの基本プロトコルの仕様を開発する。

（2） 最終目標の記載欄で挙げた物理層・データリンク層プロトコルのうち、以下の3種類に関しては、そのスタブ部分の仕様開発を完了している。

(2-1) Bluetooth

(2-2) ISO 14443

(2-3) 無線系電話プロトコル

（3） 基本機能として、認証機能、暗号機能を有すること。

（4） ソフトウェア規模は、200KB～300KB のバイナリサイズを想定する。

イ．ユビキタスコンピューティング環境を構成するシステム統合技術の研究開発

（1） 相互接続性の検証が一部完了していること。

ウ．超機能分散システム指向の開発環境の研究開発（ハードウェア部分）

（1） ユビキタスコンピューティング環境の構築に用いる標準開発プラットフォームとしてのハードウェアを開発する。

（2） その上で、サブテーマ「**エ．**」で開発した標準 OS が動作する。

（3） サブテーマ「**オ．**」で開発したデュアル型のセキュアチップを搭載している。

（4） サブテーマ「**ア．**（3）」で挙げた各種 LAN、PAN のプロトコルを搭載可能である。

（5） 音声 CODEC を備える。

（6） グラフィックチップを備える。

（7） CPU 性能として、300MHz 以上の動作周波数を持つこと、また主記憶として 32MB 以上を格納すること。ハードディスクを搭載可能な I/F を備える。

エ．超機能分散システム指向の開発環境の研究開発（ソフトウェア部分）

（1） 本研究サブテーマ「**ア．**」で開発するユビキタスネットワーキングプロトコルを標準機能で組み込み、それを本研究全体の標準プラットフォームとして利用する、標準リアルタイム OS を開発する。

(1-1) マルチタスク機能と、豊富なタスク間通信・同期機能を提供することができる。

(1-2) 省電力機能を有する。

(1-3) 本研究のサブテーマ「**カ．**」で開発したセキュアチップとの通信機能を有する。

(2) 本研究サブテーマ「**ア.** 」で開発するユビキタスネットワーキングプロトコルに対して高抽象度のプログラミングインタフェースを提供するためのミドルウェアを開発する。

(2-1) オブジェクト指向言語 Java のクラスライブラリとして開発する。

(2-2) ユビキタスコンピューティングに適する、軽くソフトウェア規模の小さい Java Virtual Machine を開発する。

(3) 現実世界記述標準形式に関する研究開発

(3-1) 内容的には、最終目標で記載したとおり。中間目標の時点では、標準形式の策定が完了している。それを実際のユビキタスコンピューティング環境に組み込んで実現するのは、これ以後の年度に行うものとする。

(4) 超機能分散プログラミングモデルに関する研究開発

(4-1) ユビキタスコンピューティング環境中に存在する莫大なノードの協調動作を高い抽象度でプログラミングできるプログラミングモデルおよび、そのプログラミング環境の開発を行う。中間目標の時点で、その基本モデルは確立する。その実現や検証はそれ以後の年度に行うものとする。

■主に再委託する予定のサブテーマ

以下、中心部分を再委託する予定のサブテーマの中間目標について記す。

オ. セキュアコンピューティングの基盤となるセキュアハードウェア

(1) 最終目標に挙げた中で、コンタクトレス(無線)チャンネルのみを有するコンタクトレスチップの開発が完了している。

(2) コンタクトレス通信チャンネルの物理層・データリンク層のプロトコルは、ISO14443 Type-C 方式である。

(3) この時点で開発された版のユビキタスネットワーキングプロトコルで通信する能力を有する。

(4) 共通鍵暗号技術に基づいた、実行効率のよい暗号機能・認証機能を有すること。

(5) 耐タンパー性を有しており、悪意あるユーザからの不正操作から格納情報が守られること。

(6) CPU には 16bit のワード幅を持ち、RAM: 10KB、ROM: 32KB、EEPROM: 32KB 以上を有する。

カ. ユーザノードシステムの研究開発

(1) ユーザノードとは、ユビキタスコンピューティング環境の中で、利用者が直接接す

るユーザインタフェースをもった機器である。移動ノード、固定ノードとして、それぞれ1種類以上のインテグレーションされたユーザノードを開発する。

（2） ユーザノードは、最終的にはサブテーマ「**ウ.** 」で開発した標準ハードウェアを用い、サブテーマ「**エ.** 」で開発した標準 OS、ミドルウェアなどを利用して開発する。

（3） サブテーマ「**ア.** 」で開発したユビキタスネットワーキングプロトコルを備える。

キ. サーバノードシステムの研究開発

（1） サーバノードとは、ユビキタスコンピューティング環境を裏で支える基盤サーバ群を含む。

（2）中間目標の時点では、CA 局や鍵配布サーバを含む PKI（公開鍵インフラストラクチャ）機能の開発が完了している。

２－３ 研究開発の年度別計画

金額は非公表

研究開発項目	13 年度	14 年度	15 年度	16 年度	17 年度	計	備考
①セキュアハードウェア 1-1. 全体アーキテクチャ	→						
1-2. コンタクトレス・耐タンパーチップ		→	→	－	－		一部再委託（日立製作所、等）
1-3. デュアル・耐タンパーチップ		－	－	→	→		一部再委託（三菱電機、等）
②基盤通信システム 2-1. 基盤プロトコル全体アーキテクチャ設計・検証					→		一部再委託（KDDI 研究所，富士通、等）
2-2. 基盤プロトコル（データリンク層 IF）	－	→	→	→	→		
2-3. 基盤プロトコル（ネットワーク層）	－	→	→	－	－		
2-4. 基盤プロトコル（トランスポート層）	－	→	－	－	－		
2-5. 基盤プロトコル（セッション層～アプリケーション層）	→	→	→	→	－		一部再委託（東芝、NTT データ、等）
③ユーザノード 3-1. 移動ノードシステム	－	→	→	→	→		一部再委託（日本電気、等）
3-2. 固定ノードシステム	－	－	→	→	→		一部再委託（東芝、等）
3-3. 強化現実型ヒューマンインタフェース	→	→	→	→	－		

研究開発項目	13 年度	14 年度	15 年度	16 年度	17 年度	計	備考
④サーバノード							
4-1. 暗号認証通信基盤用サーバ	－	→	→	→	→		
4-2. セキュア分散化サーバ	－	→	→	－	－		一部再委託(三菱電機、等)
4-3. コマース処理用サーバノード	→	→	→	→	→		
4-4. デジタルエンティティ発行ノード	－	－	→	→	→		一部再委託(NTT データ、等)
⑤システム統合化							
5-1. ユーザノード・サーバノード統合技術	－	→	→	→	→		
5-2. 対電話網ゲートウェイ研究開発	－	－	→	－	－		一部再委託(富士通、等)
5-3. 対 IP 網ゲートウェイ研究開発	－	－	－	→	→		一部再委託(富士通、等)
⑥超機能分散システム指向開発環境							
6-1. 標準開発ハードウェア研究	→	→	→	→	－		
6-2. 標準開発基本ソフトウェア研究	→	→	→	→	→		
6-3. 標準開発ミドルウェア研究	→	→	→	→	→		
6-4. 現実世界記述標準形式		→	→	→	→		
6-5. 超機能分散プログラミングモデル		→	→	→	→		

研究開発項目	13 年度	14 年度	15 年度	16 年度	17 年度	計	備考
⑦システム工学的検証	－	→	→	→	→		
間接経費	→	→	→	→	→		
合　　計							

注)1　経費は研究開発項目毎に消費税を含めた額で計上。また、間接経費は直接経費の30％を上限として計上(消費税を含む。)。

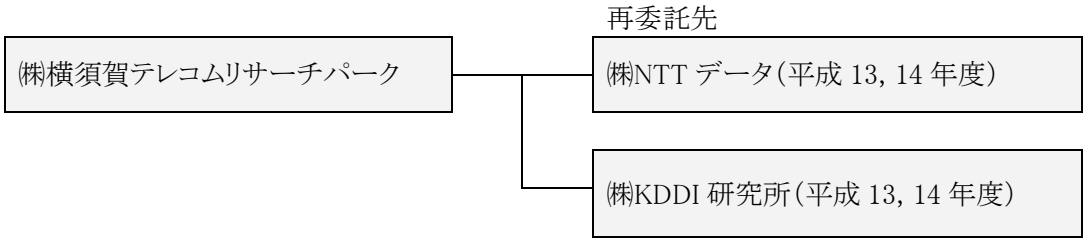
2　備考欄に再委託先機関名を記載

3　年度の欄は研究開発期間の当初年度から記載。

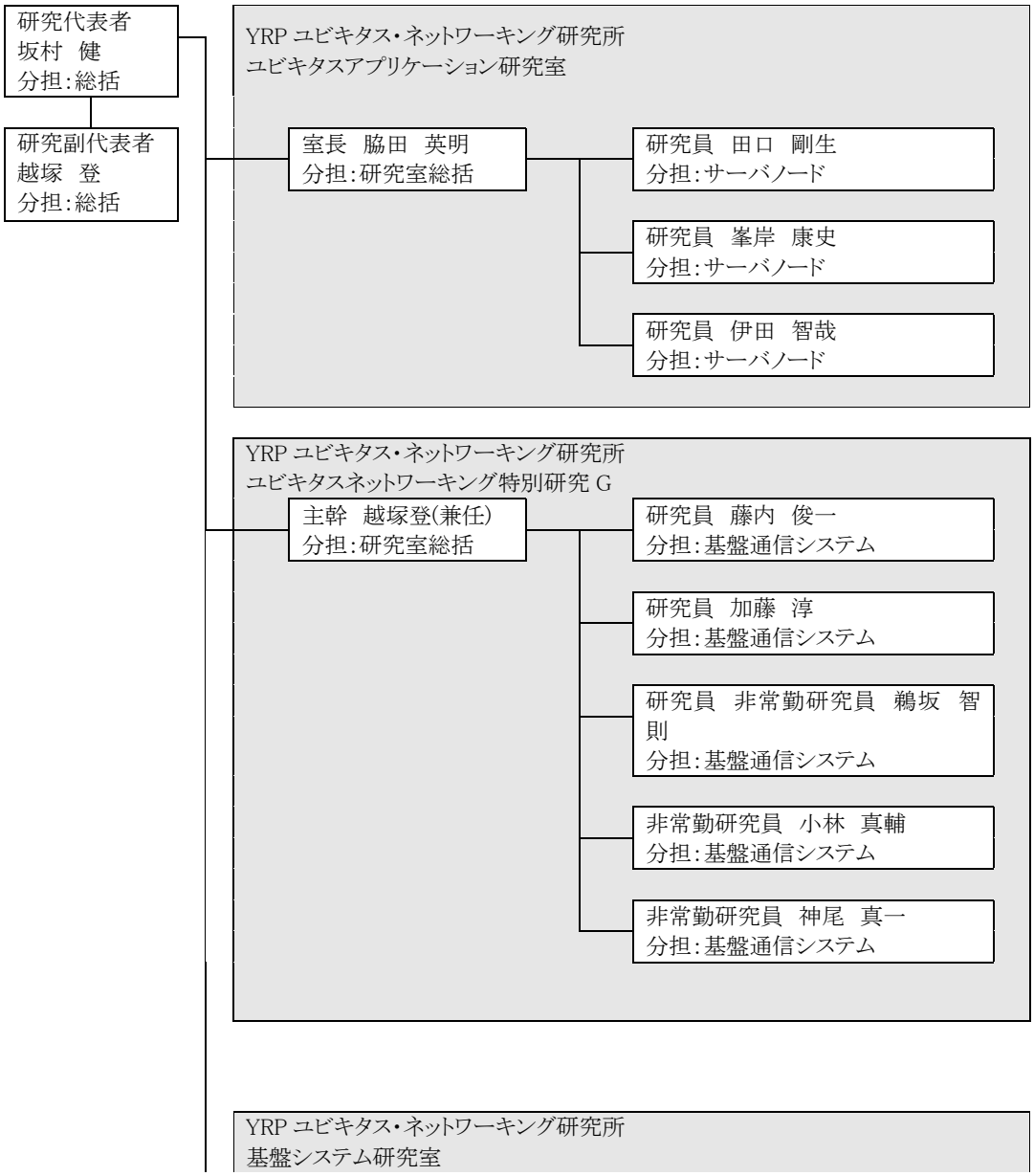
3 研究開発体制

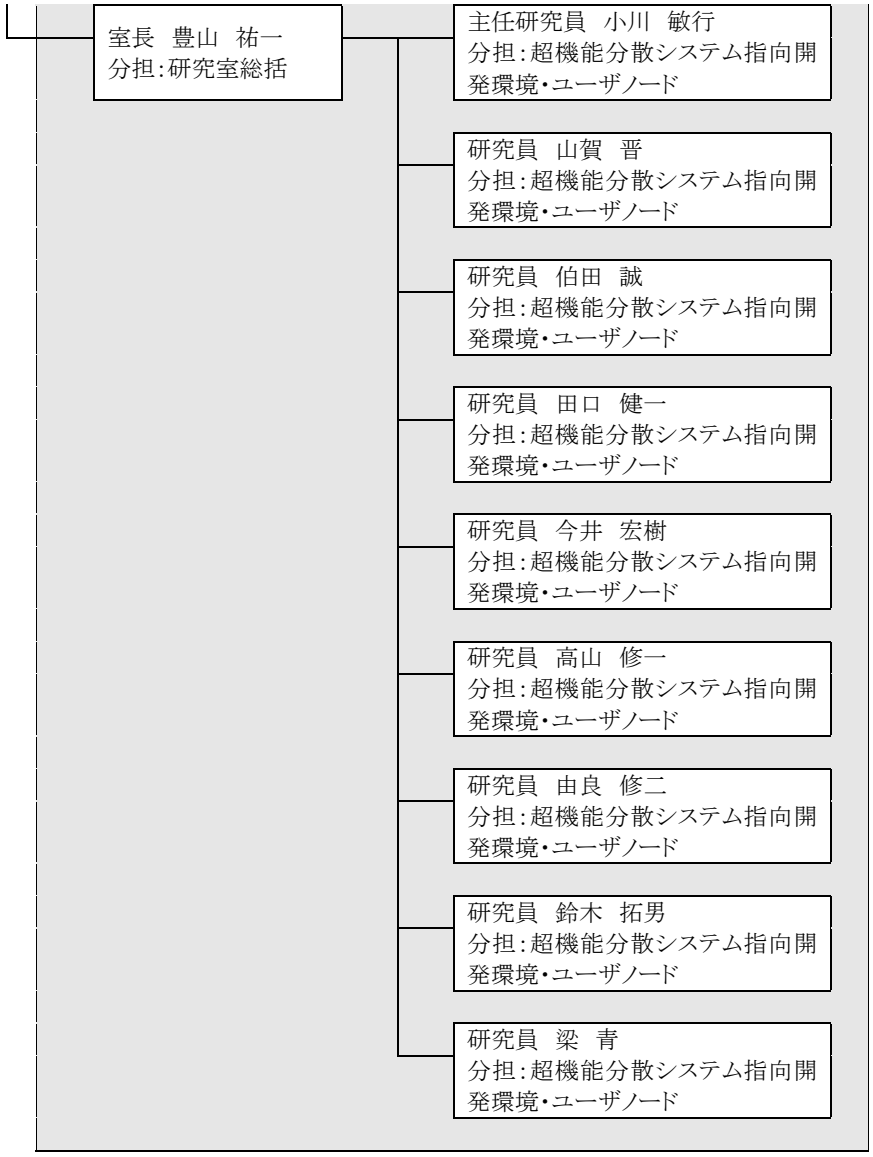
3－1 研究開発実施体制

3-1-1 プロジェクト全体の研究開発体制（含、再委託先）



3-1-2 ㈱横須賀テレコムリサーチパークの研究開発体制




室長　豊山　祐一
分担:研究室総括
主任研究員　小川　敏行
分担:超機能分散システム指向開発環境・ユーザノード
研究員　山賀　晋
分担:超機能分散システム指向開発環境・ユーザノード
研究員　伯田　誠
分担:超機能分散システム指向開発環境・ユーザノード
研究員　田口　健一
分担:超機能分散システム指向開発環境・ユーザノード
研究員　今井　宏樹
分担:超機能分散システム指向開発環境・ユーザノード
研究員　高山　修一
分担:超機能分散システム指向開発環境・ユーザノード
研究員　由良　修二
分担:超機能分散システム指向開発環境・ユーザノード
研究員　鈴木　拓男
分担:超機能分散システム指向開発環境・ユーザノード
研究員　梁　青
分担:超機能分散システム指向開発環境・ユーザノード

4 研究開発実施状況

4－1 基盤通信システムの研究開発

4－1－1 研究開発内容

本研究開発における課題は、我々の身の回りのあらゆるものにマイクロコンピュータと通信機能を組み込み、それらが互いに情報を交換しながら協調動作を行い、人間生活をより高度にサポートする、ユビキタスコンピューティング環境を構築するための、次世代通信の基盤プロトコルおよびそのシステムを確立することである。

上記の基盤プロトコルとそれを利用したシステムを確立するために、以下のとおり研究開発の最終目標を設定した。

（1） ユビキタスネットワーキングプロトコルのセッション層部分までの基本プロトコルの仕様を開発し、その正当性・有効性を検証する。

（2） 上記のプロトコルを実現し、評価を行う。

（3） ユビキタスネットワーキングの物理層・データリンク層を担う、Bluetooth やISO 14443, IEEE 802.11, ISO 7816, 無線系電話プロトコルプロトコル等の中からネットワークシステムの上で動作させるためのスタブ部分の仕様を開発すること。

（4） 既存のインターネット網であるIP 網との間で相互運用と情報交換を可能にするゲートウェイ技術およびシステムを開発する。

（5） 基本機能として、認証機能・暗号機能を有すること。

（6） 認証・暗号機能の実現には、セキュアハードウェアを十分に活用する。

そして、これらの最終目標を実現するため、具体的に下記方式およびプロトコルの研究開発を行った。

1. ソフトウェア無線方式によるユビキタス型近接通信方式（L1／2）
   一つのハードウェアで複数の無線通信プロトコルに対応する近接無線通信装置の研究開発
2. ユビキタス・ネットワークプロトコル(UNP)（L1／2）
   ユビキタス情報提供・制御用プロトコルであるユビキタスネットワーキングプロトコル（UNP）の研究開発
3. ユビキタス・シームレス通信プロトコル（L3）
   モバイル IP において、移動先の予測が不要でかつ高速化方式に対応しない既存のルータが混在する環境でも動作する、高速なハンドオーバ方式の開発
4. ユビキタス価値転送プロトコル（eTP）（L4／5）
   eTP の実装手法としてCPU の性能に応じて8 ビット版、16 ビットCPU 版、32 ビット CPU 版とそれぞれシリーズ化を考慮し、共通する操作に関して共通のコマンド及びメッセージフォーマットの提案およびハードウェアでの実装をしたチップを利用しての実証実験

5. セキュア・ユビキタスVPN（L4／5）
セキュリティがあまり考慮されていない組み込み環境でのネットワーク通信に、PKIを利用したVPN機能を、その方面の知識が乏しい組み込みプログラマでも手軽に利用できるように提供するための機能設計および、実装例の提供

これらの方式やプロトコルを当研究所をはじめとした様々な実験フィールドで稼動させて、本研究開発の目標に照らしてその成果を実証的に検証した。本節では、各方式およびプロトコルの技術内容およびその成果について記載する。

4－1－2 ソフトウェア無線方式によるユビキタス型近接通信方式（L1／2）

（1）研究内容

ユビキタスコンピューティング社会では、非接触で情報のやり取りが可能である近接無線通信デバイス(RFID)を環境に配置してモノや場所を認識し、コンテクストアウェアネスを実現することが期待されている。この際、通信に適した周波数やプロトコルはアプリケーションに依存して様々で、プロトコルの違いをリーダライタ側で吸収し、様々なRFIDを統一的に扱うリーダライタの技術開発が必須である。そこで、ユビキタス社会を構成する様々なコンピュータと通信を行う近接無線通信技術を確立することを目的として研究開発をおこなった。

（2）本通信方式の特徴

我々は、一つのハードウェアで複数の無線通信プロトコルに対応する近接無線通信装置を目標に研究開発を実施した。本近接無線通信装置に求められる条件として、下記の点を最も重視した。

- ユーザが意識することなく複数のプロトコルが混在した環境下で通信が行える
- モバイル型ユーザ端末への適用を目指し小型・低電力化を志向した方式である
- 新規プロトコルをソフトウェアの変更のみで対応できる

様々な無線通信プロトコルにソフトウェアの変更のみで対応できる技術に、ソフトウェア無線技術がある。しかし、一般的なソフトウェア無線技術は、プロトコル処理に高性能なプロセッサが必要となり、小型・低消費電力化に適さない。

そこで平成16年度、携帯端末に搭載するための小型・低消費電力に志向したソフトウェア無線技術として、物理層、データリンク層の機能をFPGA等の論理回路上のハードウェアブロックで構成し、ソフトウェアでスケーリング、選択するソフトウェア無線技術を開発した。その評価のためISO18000-4の近接無線通信規格のデータリンク層プロトコルをFPGA上に実装した近接無線通信装置を試作した。

（3）成果

これまでに開発したアーキテクチャを用いて、ソフトウェアの変更のみであらゆるプロトコルに対応できる近接無線通信装置を開発した。本装置上に表1に示す一般的な3周波数5プロトコルを実装し、ソフトウェアの変更のみで複数のプロトコルに対応できることを実証した。

表 1 複数プロトコル対応の実証に使用したプロトコル

13.56MHz 帯域	ISO15693 準拠 RFID
	eTRON カード (ISO18092)
950MHz 帯域	ISO18000-6 準拠 RFID
2.45GHz 帯域	日立製作所製 ミューチップ
	日立超 LSI 製 ミューチップ RW (ISO18000-4 準拠)

図 1 ソフトウェア無線方式による複数プロトコルに対応したリーダライタ

4－1－3 ユビキタス・ネットワークプロトコル(UNP)(L1／2)

(1)研究内容

ユビキタスコンピューティング環境においては、情報家電機器の他にセンサーやアクチュエータ等の超小型のコンピュータが多数存在し、少量のデータが飛び交うことになる。このような環境では、セキュリティを確保しつつリアルタイム性を損なわずに効率的な通信を行うプロトコルが必要となる。そこで、ユビキタス情報提供・制御用プロトコルであるユビキタスネットワーキングプロトコル(UNP)の研究開発を行った。

(2)プロトコルの特徴

ユビキタスコンピューティング環境では多数のノードが存在するネットワーキングが前提となるが、同時にこの環境ではローカリティすなわちその場その場の状況やニーズにあったサービスをリアルタイムに提供することが必要となる。そこで、本プロトコルが前提とするネットワークアーキテクチャは、2階層の構造とした。具体的には、下の階層では255台の機器を収容する基本ネットワークを構成し、これを1ドメインと定義した。この基本ネットワークの上の階層でこれらを束ねるネットワークを構成し、ここでは255ドメインを収容できるようにした。この構成によって、最大で約64000台の機器を収容しつつ、ローカリティに配慮したリアルタイム通信が実現可能となった。

以下、UNPプロトコルの各階層について説明する。

データリンク層には既存のトークンパッシング方式を改良したプロトコルを開発して実装した。通信形態は、ユニキャストとマルチキャスト(ブロードキャストを含む)をサポートした。ネットワーク

上の論理アドレスについては、機器同士が協調してアドレスを管理できるアルゴリズムを開発することによって、特別な設定なしに機器をネットワークに接続するだけで動的に論理アドレスが決定できるようにした。また機器が削除された場合でも、論理的に近くにいる機器がタイムアウトすることによって削除されたことを検知するアルゴリズムを開発した。また、本レイヤをLSI化することでシステム全体の処理速度の向上が図れリアルタイム性を確保することに寄与した。

データリンク層の上の階層では、セキュリティや認証のための機能を提供した。相互認証と同時に鍵交換を行い、セッション中は暗号通信が行なわれるセキュアセッション機能、リアルタイム応答が要求される場合のライトウェイトセッション機能を備えた。また、階層構造をもつネットワーク構成においてセキュリティの強度を上げるために、各ドメイン単位で異なる鍵を使用するなどの配慮も行った。

セキュリティ層の上の階層では、大きなデータを送受信する際に必要となるパケットの分割・組み立ての機能を提供した。またパケット毎に肯定応答や否定応答の返送を指示できる機能も提供した。これらの機能によって、アプリケーションに応じて柔軟なトラフィック制御が行えるプロトコルとなった。

(3)成果

4－3－4節に示すようなコイン型の開発環境ボードやUNPネットワークと既存のIPネットワークとの相互接続のためのUNPゲートウェイ装置やUNPネットワーク内で上記のボード類の多段接続をおこなうためのUNPルータ装置を開発し、いくつかのシステムを構築してUNPの有用性を検証したが、いずれのシステムでも問題なく動作しており、UNPが実用に耐え得る技術であることを実証した。

4－1－4 ユビキタスシームレス通信プロトコル(L3)

(1)研究内容

モバイルIPでは端末は移動の度にホームエージェント(あるいは通信相手)に気付アドレスの変更を登録する必要があり、この処理に時間がかかるためその間通信が途切れるという問題があった。これを解決するための方式として、従来検討されている方式と異なり、移動先の予測が不要で、かつ高速化方式に対応しない既存のルータが混在する環境でも動作する、以下の要素からなる高速なハンドオーバ方式を開発した。

(2)プロトコルの特徴

(1) ハンドオーバ処理のうち網の移動検出の処理時間を短縮するため、移動端末(MN)が常にレイヤ2のリンク状態を監視し切断・再確立を検出、ハンドオーバの契機とする。通常のネットワーク環境でも動作するようネットワーク側にはリンク状態検出等の機能を要求しない。

(2) ハンドオーバ前のネットワークのルータ(PAR)とハンドオーバ後のルータ(NAR)の間で双方向トンネルを設けることで、移動先でのMNが存在する網の特定のIPアドレス

（気付けアドレス:CoA）の取得、ホームエージェント(HA)（および通信相手(CN) ）への移動登録処理の間にも PAR 経由での通信を可能とする。ここで、予め移動先が不明でもよいようMNからのハンドオーバ要求を契機としてNARからPARにトンネルを設定する。

(3) MN がリンク確立時に、通常のルータが必ず反応するルータ要請(RtSol: Router Solicitation)に独自オプションとしてこのハンドオーバ要求を追加する。このオプションを解さない通常ルータは提案方式のオプションを含まないルータ通知(RtAdv: Router Advertisement)を返送するため、MN はすぐにルータが対応するか否かを判別できる。

(4) トンネリングに必要な機能の一部を MN や HA が持ち、PAR や NAR が通常のルータの場合、トンネルの終端処理をMNやHAが代替する。これにより通常のルータが混在する環境でも利用可能とする。

(5) 通信の信頼性を向上させるため、アクセスネットワークのルータ(AR)や HA、MN にオプションとしてパケットのバッファリング機能を持たせる。

(3)成果

同方式を FreeBSD 上の KAME および T-Kernel 上の KASAGO という2つの IPv6 モバイル IP プロトコルソフトウェアを改造して実装し、評価を行った。その評価結果を下表に示す。

表 2 有線 LAN 上でのハンドオーバ時間

		平均値(秒)	分散	最大値(秒)	最小値(秒)
提案方式	対応ルータ間	1.9	0.001	1.9	1.8
	ホーム→対応ルータ	1.9	0.002	2.0	1.9
	対応ルータ→ホーム	2.0	0.003	2.0	1.9
	対応ルータ→通常ルータ	2.0	0.003	2.0	1.9
	通常ルータ→通常ルータ	2.0	0.003	2.1	1.9
従来方式	ルータ間	5.8	2.2	8.1	4.2

＃対応ルータとは、Fast-handover Mobile IP(FMIP)を解するルータ

＃ハンドオーバ時間には、手動での LAN ケーブル時間を含まれる

上記の結果より、手動での LAN ケーブル繋ぎ変え時間 1.5 秒を除くと，実質上 400 ミリ秒程度で切り替わっているといえる。従って提案方式では通常のモバイル IP と比較してハンドオーバ時間が約 1/3 に減少しており、提案方式の優位性が実証できた。また，FMIP を解さない通常のルータに対しても高速なハンドオーバが実現できていることが確認できた。

4－1－5 ユビキタス価値転送プロトコル（eTP）（L4／5）

(1)研究内容

本研究では eTP の実装手法として CPU の性能に応じて 8 ビット版、16 ビット CPU 版、32 ビット CPU 版とそれぞれシリーズ化を考慮し、共通する操作に関して共通のコマンド及びメッセージフォーマットを提案し、さらにハードウェアでの実装をしたチップを利用しての実証実験を

行なった。これによりプロトコル仕様の正当性、有効性を確認した。

(2)プロトコルの特徴

eTP (entity Transfer Protocol)は、eTRON アーキテクチャで価値情報を転送するノード間の通信規約である。(eTRON (entity TRON)は、東京大学坂村健教授が推進するトロンプロジェクトが目指す、超機能分散システムにおいて、価値情報の格納媒体となるコンピュータシステム(例えば IC カード等)のアーキテクチャをいう。eTP の交換対象 はネットワークで交換される価値情報(例:チケット、クーポンなど)である。これらの価値情報を 計算実体 (eTRON Contents Holders) と呼ばれるものの間で通信交換を行なう。)

eTP の特徴を以下に述べる。

eTP を行なう 計算実体 は 従来の IC チップのように、コンピュータの周辺機器として、リーダライタを通して操作されるものではなく、分散環境におけるノードとして設計されている。ネットワーク上のサービス提供モジュールとチップ、チップとカードが対等に peer-to-peer で通信する。リーダライタ装置は、LAN との通信物理層を橋渡しするゲートウェイ(ブリッジ)となる。従って eTP の認証の対象は、例えばリーダライタではなく、ネットワークとリーダライタを経由して、チップと情報交換をするネットワーク上の計算実体 である。eTP では 認証相手を eTRON ID と呼ぶ ID 番号で特定し、それをもとにアクセス制御が行なえる。

(3)成果

(i) 認証、暗号通信

eTP では、認証、暗号メカニズムを提供し、これにより安全な通信環境を構築し、価値情報の交換を行なうことができる。 貧弱なハードウェアの上では、共通鍵暗号をベースとし、そうでない場合には PKI を利用した認証を行なう。

別に 4-6 節 で述べる「セキュアコンピューティングの基盤となるセキュアハードウェアの研究開発」での 16 ビットの CPU を利用したセキュアハードウェア実装例では、この PKI 認証、暗号通信機能を実装しており、この実装チップを活用した実証実験も行なった。

(ii) 資源が乏しいハードウェアでの利用

eTP を実装するライブラリを複数構築した。情報家電、インターネットアプライアンスといったハードウェア資源が少ない組み込みボードでも利用できるような小型ライブラリを作成して、実際の組み込み装置実験環境での動作を確認している。

(iii) 既存通信網に eTP のパケットを流す事ができる。

既存通信網のパケットに eTP のパケットを流す事で、既存通信インフラを利用することができる。実際に IP 網に eTP を流しての価値情報交換実験を行なった。

4－1－6 セキュアユビキタスVPN（L4／5）

（1）研究内容

現在、セキュリティがあまり考慮されていない組み込み環境でのネットワーク通信に、PKI を利用した VPN 機能を、その方面の知識が乏しい組み込みプログラマでも手軽に利用できるように提供するための機能を設計し、実装例を提供し、その有効性を確かめた。

（2）本研究の特徴

(i) セキュアハードウェアによる VPN 用共通鍵のダイナミック生成

PKI 認証を利用できる物理的な耐タンパー性をそなえる セキュアハードウェア IC カード（4-6 参照）が広まれば、そこに VPN で利用するための鍵の情報を入れたいという要求が当然でてくるが、我々は耐タンパーカードとはいえ、共有鍵そのものをいれるのでは危険が大きいと判断した。

そこで共有鍵をオンデマンドで要求に応じて発生するための VPN 用の公開鍵／秘密鍵の情報を入れておき、必要に応じ DH（Diffie-Hellman）鍵交換アルゴリズムを使い共有暗号鍵をダイナミックに生成するというのが我々のアプローチである。これにより共有鍵を事前配布をする必要がなくなった。

(ii) 複数のユーザドメインでの異なる鍵の利用

VPN の利用はユーザ情報の秘匿が目的であり、このための PKI の認証体系はチップ、ソフトウェアを作った主体ではなく、あくまでもユーザが属する団体／機関が管理するべきである。我々のアーキテクチャでは、ユーザが属するVPN管理団体／機関（VPNドメインと呼ぶ）を複数サポートする事ができる。

(iii) VPN 鍵生成メカニズムと利用ポリシーの分離

VPN の鍵の生成メカニズムの提供と、実際にセッションで暗号の利用ポリシーは分離されている。あくまでもメカニズムを提供することで上位のアプリケーションでの利用に自由度を持たせている。

(iv) 簡潔な API

簡潔な API を提供することで、暗号、認証機構を詳しくしらない組み込みプログラマでもセキュアなネットワーキングサービスを利用することができる。

（3）成果

上記「簡潔なAPI」に関しては、組み込み機器での利用例を学会で発表済みである。別に説明する セキュアハードウェア（4-6節参照）を利用する事で、実際に応用ソフトウェアに VPN 機能を提供して、各種実験でその有効性を確かめた。IP 網での uID 解決サーバーへの通信の保護、アプリケーションデータの交換の際の秘匿がこれで行なわれた。

4－1－7 まとめ

本研究開発課題で開発した方式やプロトコルを使用することによって、我々の身の回りのあらゆるものにマイクロコンピュータと通信機能を組み込み、それらが互いに情報を交換しながら協調動作を行い、人間生活をより高度にサポートする、ユビキタスコンピューティング環境を構築することが可能であり、現実社会への展開が可能であることを実証した。以下に、4－1－1節で述べた本研究開発課題における最終目標の観点から見た各方式およびプロトコルの成果を示す。

1. ソフトウェア無線方式によるユビキタス型近接通信方式(L1／2)

ソフトウェアの変更のみであらゆるプロトコルに対応できる近接無線通信装置を開発した。本装置上に3周波数5プロトコルを実装し、ソフトウェアの変更のみで複数のプロトコルに対応できることを実証した。

2. ユビキタス・ネットワークプロトコル(UNP)(L1／2)

4－3－4節に示すようなコイン型の開発環境ボードや UNP ネットワークと既存のIPネットワークとの相互接続のためのUNPゲートウェイ装置やUNPネットワーク内で上記のボード類の多段接続をおこなうためのUNPルータ装置を開発し、いくつかのシステムを構築してUNPの有用性を検証したが、いずれのシステムでも問題なく動作しており、UNPが実用に耐え得る技術であることを実証した。

3. ユビキタス・シームレス通信プロトコル(L3)

本方式では通常のモバイルIPと比較してハンドオーバ時間が約1/3に減少しており、本方式の優位性が実証できた。また, FMIP を解さない通常のルータに対しても高速なハンドオーバが実現できていることが確認できた。

4. ユビキタス価値転送プロトコル(eTP)(L4／5)

(i) 認証、暗号通信

別に 4-6 節 で述べる「セキュアコンピューティングの基盤となるセキュアハードウェアの研究開発」での 16 ビットの CPU を利用したセキュアハードウェア実装例では、この PKI 認証、暗号通信機能を実装しており、この実装チップを活用した実証実験も行なった。

(ii) 資源が乏しいハードウェアでの利用

eTP を実装するライブラリを複数構築した。ハードウェア資源が少ない組み込みボードでも利用できるような小型ライブラリを作成して、実際の組み込み装置実験環境での動作を確認している。

(iii) 既存通信網に eTP のパケットを流す事ができる。

実際に IP 網に eTP を流しての価値情報交換実験を行なった。

5. セキュア・ユビキタスVPN（L4／5）

4－6節で述べるセキュアハードウェアを利用する事で、実際に応用ソフトウェアに VPN 機能を提供して、各種実験でその有効性を確かめた。IP網でのuID 解決サーバーへの通信の保護、アプリケーションデータの交換の際の秘匿がこれで行なわれた。

以上のように、最終目標に掲げた項目の達成に加え、UNPは当研究所の所内システムの一部で実運用中であり、セキュア・ユビキタスVPNはuIDセンターとの通信に使われていることを鑑み、本研究開発課題の定量的評価としては120％の成果を上げることができた。

4－2 ユビキタスコンピューティング環境を構成するシステム統合技術の研究開発

4－2－1 研究開発内容

（1）研究の背景と目的

ユビキタスコンピューティングを実現するには、あらゆるネットワーク同士が相互に接続できることが求められる。つまり、ユビキタスネットワーキングプロトコル（UNP）や既存通信網が相互にやりとりできなければならない。IP 網や携帯電話網などの既存の通信網との橋渡しを実現するゲートウェイ技術が必要である。

ユビキタスコンピューティング環境にとって重要と考える要素技術と、既存の通信網との接続方式について検討・開発を進めること。これら通信網間の相互接続性をフィールド試験などにより検証することを本研究の目的としている。

（2）研究開発の概要

ここでは研究開発の概要を説明するにとどめ、4－2－2～4－2－5節で各々の技術要素について詳細を述べる。

UNP－IP間GW技術とは、制御ネットワーク（UNP網）で流れるセンサー値や制御値などのデータを情報ネットワーク（IP網）にあるサーバノード機器が透過的にアクセスするためのゲートウェイ技術である。ゲートウェイが相互にプロトコルを変換する機能を提供する。

UNP－ユビキタス型近接通信間GW技術とは、ユビキタス型近接通信を実装した無線アクティブノードとUNPベースの制御ネットワーク間を透過的にアクセスするためのゲートウェイ技術である。ゲートウェイが相互にプロトコル変換する機能を提供する。

IP－PIAFS間GW技術とは、PIAFSによるデータ通信をサポートする機器と情報ネットワーク（IP網）を相互に接続するためのゲートウェイ技術である。ユーザノードの１つであるUC-Phone がPIAFS経由でIP網に接続する際に本GW技術を適用した。

統合型分散バイオメトリクスシステム技術とは、バイオメトリクス認証システムでPKIベースの認

証暗号通信を可能にするための技術である。バイオメトリクス認証に使う生体情報（基準テンプレート）を暗号化してやりとりすることにより、システムの安全性を高められるようにした。

4－2－2 UNP－IP間GW技術

（1）本研究開発の意義

ユビキタスネットワーキングプロトコル：UNP とは、ユビキタスコンピューティング環境において、身のまわりの至るところに組込まれた無数の機器を制御するネットワークプロトコルである。また、UNP は、セキュアでリアルタイム性を有し、主に数バイトのデータ送受信を行うネットワーク技術である。その為、UNP は、情報ネットワークの基盤技術であるインターネットプロトコル：IP を補完する役割を担う。以上の理由から、UNP と IP をブリッジする専用のハードウェアを開発した。

（2）システム構成

図 2 に、UNP-IP 間 GW 技術に関するシステム構成を示す。UNP と IP をブリッジすることで、それぞれのネットワークに対して、透過的にアクセスすることが可能である。

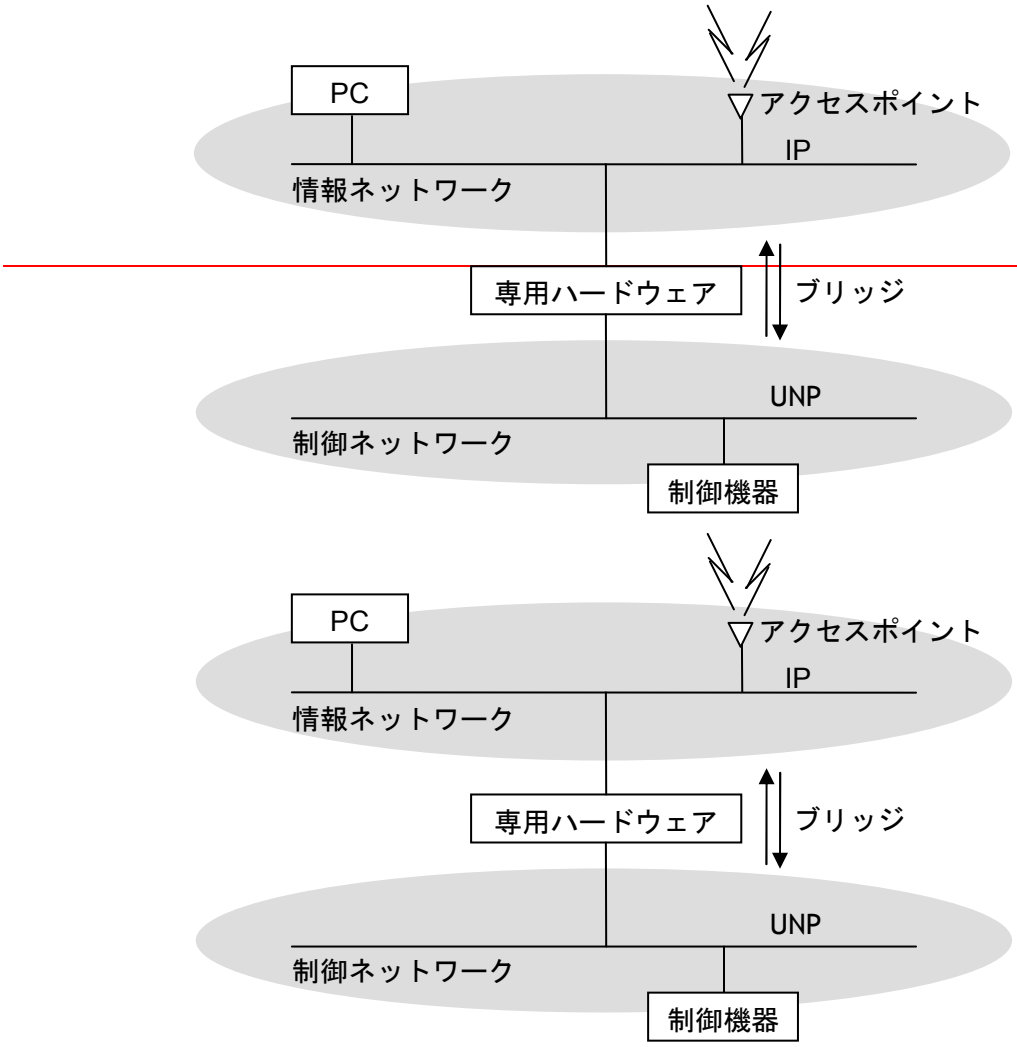


図 2 システム構成

(3)成果

図 3 に、UNP と IP をブリッジする専用ハードウェア:UNP ゲートウェイを示す。今回、UNP ゲートウェイを用いた多くの実証実験を行うことで、UNP-IP 間 GW 技術が実用に耐え得る技術であることを確認した。

図 3 UNP ゲートウェイ

4－2－3 UNP－ユビキタス型近接通信間GW技術

(1)本研究開発の意義

UNP を利用した機器制御システムと、ユビキタス型近接通信方式を利用した環境情報測定システムを組み合わせることにより、リアルタイム性の高いユビキタスコンピューティング環境を構築できる。しかし、2つのシステムを単純に重ね合わせたシステムの場合、サーバがシステムのボトルネックになる。

UNP-ユビキタス型近接通信 GW 技術を開発すれば、システム構築時にサーバが不必要になり、フォールトトレラント性能、スケーラビリティ、リアルタイム性の高いシステムを構築できる。

(2)システム構成

本研究開発の目的は、UNP とユビキタス型近接通信方式間の相互接続を確認することである。目的を達成するため、UNP-ユビキタス型近接通信 GW のハードウェアを試作開発した。試作したハードウェアの写真を図 4 に示す。

次に、試作したハードウェアを利用して、UNP とユビキタス型近接通信によるユビキタスコンピューティング環境の評価システムを構築した。評価システムの概要を図 5 に示す。

以下に評価システムの動作を示す。

環境情報(評価システムでは温度)を測定したセンサは、ユビキタス型近接通信方式を利用して環境情報を UNP-ユビキタス型近接通信 GW に送信する。環境情報を受信した UNP-ユビキタス型近接通信 GW は、UNP を利用して環境情報を環境制御機器及び環境情報表示機器へ送信する。環境情報を受信した環境制御機器は、受信した環境情報によって環境を制御する。評価システムでは、扇風機を制御して温度調整をおこなった。環境情報を受信した環境情報表示機器は、受信した環境情報を人間にわかるように表示する。評価システムでは、温度分布を3次元グラフ表示した。

(3)評価

構築した評価システムは 1 週間連続動作させ、完全動作を確認した。

評価システムの動作とともに、UNP とユビキタス型近接通信方式間の相互接続が確認できた。

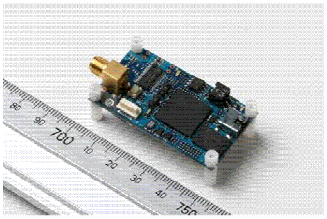


図 4 試作したGWハードウェア

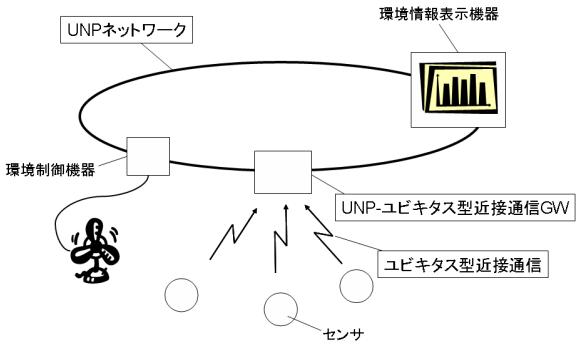


図 5 評価システム

4－2－4 IP－PIAFS間GW技術

(1)背景と目的

UC-Phone は、ユビキタスコミュニケータ(UC)の1形態として開発したPHS電話型ユーザノードである。PHSによる音声通話機能とPIAFS(PHS Internet Access Forum Standard)によるデータ通信機能を実装している。また、ユビキタスコンピューティング環境とのインタフェース装置としてRFIDリーダライタを搭載しているのが UC-Phone の特徴である。

一方、サーバノード群(ucode 解決サーバや情報サービスサーバ)はIP網で動作する形態をとっている。このため、IPとPIAFSの通信網をブリッジする機構として、ゲートウェイアーキテクチャを適用した。UC-Phone ゲートウェイには、主要機能としてIP－PIAFS間のプロトコル変換機能をもたせている。上位のアプリケーションプロトコルにはHTTPを使用している。

UC-Phone とサーバノードの連携機能を実現するにあたり、IP－PIAFS間GW技術について相互接続性を検証することを本研究開発の目的とする。

(2)システム構成

UC-Phone、UC-Phone ゲートウェイ、サーバノード群(ucode 解決サーバ,情報サービスサー

バ)を連携させたネットワーク型ユビキタス情報配信アーキテクチャの構成を図 6 に示す。

まず、ユーザノード端末(UC-Phone)が読み取った ucode をゲートウェイあてに送信する。ゲートウェイが下位プロトコルを変換する。ゲートウェイは、サーバノード群とやり取りし、ucodeに対応した情報サービスサーバのありかを同定して URL を取得する(ucode 解決)。取得した URL からコンテンツをダウンロードする。ゲートウェイは、取得したコンテンツデータをPIAFSプロトコルによって UC-Phone に返却する。

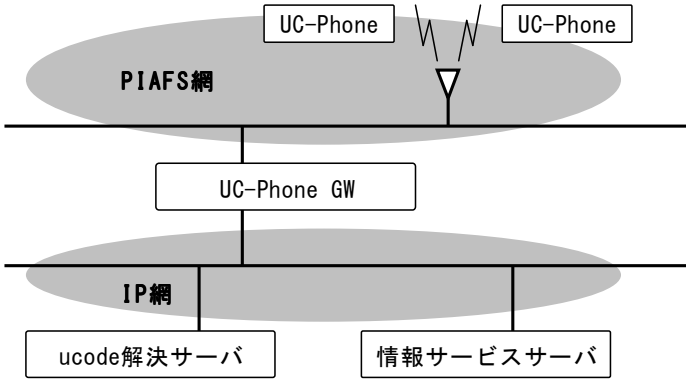


図 6 システム構成

(3)成果

本GW技術を適用することにより、サーバノード群と UC-Phone 端末を連携させたシステムが構築可能となった。各種実証実験やデモンストレーションにより、GW技術の有用性を確認した。

4－2－5 統合型分散バイオメトリクスシステム技術

(1)背景

バイオメトリクスに基づく認証は人間個人の身体に固有な指紋、声紋、虹彩パターンなどをもとに、個人を特定して、それをもとに各種のアクセス制限を行なうもので、暗号を使った認証と相補的な関係にある。暗号技術を知らない人でも、バイオメトリクス認証の原理はわかりやすく、利用しやすい。しかし、認証に使う基準データの保管方法で様々なバリーエーションがあり、安全性やシステム運営の容易さが異なる。

バイオメトリクス認証においては、個人のバイオメトリクス特徴を抽出してあらかじめ保持しておき(基準テンプレート)、それを認証の都度、認証を求める者から読みだす値と比較するアルゴリズムを実行して、正当性を判断する。

これまでは基準テンプレートを遠隔のサーバに格納し、それを認証の必要な場所に設置した読取り装置の CPU、あるいは遠方のサーバにおいて合致検出アルゴリズムを実行して、認証するという形態が一般的であった。

この場合、遠方サーバで合致アルゴリズムを実行すると、読取り装置からその都度読みだすバイオメトリクスデータをネットワークに送信する必要がある。また、認証が必要な場所に設置し

た読取り装置の CPU で行なう場合には、遠方サーバから基準テンプレートを送信しなければならない。このため、ネットワーク通信を暗号化するなどの保護が必要となる。さらに、個人のプライバシー情報保護に対する意識が高まり、このような基準テンプレートを自分の身近にない装置に格納することには、ユーザの抵抗感が強まる。

(2)本研究の特徴と成果

本研究では、バイオメトリクス認証システム内部でネットワーク通信を利用する場合には、4－6節で研究したセキュア IC チップを使った VPN (4-1-6 参照)を利用することで通信経路の保護を可能にした。これにより、既存のバイオメトリクス認証システムで、PKI を使った認証暗号通信を容易にした。

また、セキュア IC チップを使いバイオメトリクス機能をどのように実装するかについて検討した。既存のPKIを使った暗号認証なども含めた、チップのための認証(場合によれば 既存のバイオメトリクス認証とパスワード認証などの複数の組合せが考えられる)について手順を柔軟に記述する方法を考え、それにもとづきセキュア IC チップに各種のバイオメトリクス認証をシステマチックに取り込むことを目標とした。

第1段階として、セキュア IC チップに 個人のバイオメトリクス認証基準テンプレートを保管することにより、ごく短時間の利用の間のみ外部に取り出すことで、外部にバイオメトリクス認証用データを長期保存することに対する抵抗感をなくして利用を促進できるようなシステムアーキテクチャを考案し、静脈認証システムを実装し、有効性を検証した。

ただし、短時間とはいえ外部に基準テンプレートを出すことは望ましくない。第2段階として、セキュア IC チップ内部で合致検証アルゴリズムを実行して、テンプレートデータを外部に出す必要のないチップのアーキテクチャ指針検討を行なった。

4－2－6 まとめ

(1)研究成果

本研究では、以下の技術テーマについて動作するシステムを構築し、その検証を進めてきた。

- UNP－IP間GW技術
- UNP－ユビキタス型近接通信間GW技術
- IP－PIAFS間GW技術
- 統合型分散バイオメトリクスシステム技術

いずれの技術についても、試作／実装／検証を重ねることで、基本動作と実装アーキテクチャに問題がないことを確認した。当初、本研究の目標としていた相互接続性については十分に検証できたと言える。

また、これらGW技術は研究開発するだけでなく、各方面に展開してユビキタスコンピューティング環境の一部として活用をはじめている。システム統合技術としての安定度が高まったことから、実証実験や応用システムへの適用事例が増えている。次節では、こうした本研究成果の

展開状況を述べる。

(2)研究成果の展開状況

UNP－IP間GW技術(4－2－2)については、さまざまな実証実験に適用して、システムのブラッシュアップを図ってきた。また、本技術は実証実験の段階を超えた技術展開を進めている。セキュリティ管理システム(4－5)の一部として投入し、実運用システムとしての実績をあげることに成功した。

UNP－ユビキタス型近接通信間GW技術については、基本動作の検証を終えたことで、今後は無線アクティブノードを使ったシステムで本GW技術の適用事例が増加していくと思われる。

IP－PIAFS間GW技術については、UC-Phone ゲートウェイとしての機能を絞込み、ノートパソコン上のソフトウェアとPHSデータ通信カードでGW機能を実現させることに成功した。これにより、小規模なユビキタス情報配信アーキテクチャシステムの構築が可能となり、一般の利用者に普及させやすい体制を整えることができた。

統合型分散バイオメトリクスシステム技術については、認証に使う生体情報を安全に扱う方式を検討し、実装したものを動作させて有効性を確認した。また、より安全性を向上させる方式の検討も進めた。本研究で得られた知見をベースにして、機能を拡張したセキュア IC チップの設計や実装を進める動きが今後も活発化すると考えられる。

4－3　超機能分散システム指向の開発環境（ハードウェア）の研究開発

4-3-1　研究開発内容

近年の我が国では、従来は情報処理能力や通信能力を持たなかった、身の回りに存在する無数の小さな「モノ」に対して、計算力と通信力を与える方向が急速に拡大している。こうした身の回りのあらゆるものをインテリジェント化することで、高いユーザサービスを実現する情報通信のパラダイムは、ユビキタスコンピューティング （Ubiquitous Computing）や「どこでもコンピュータ環境」と呼ばれている。

こうした、ユビキタスコンピューティング環境を構築する上での技術的な課題として、システム開発効率がある。ユビキタスコンピューティング環境は、他の分散環境と比べると、膨大なノード数に特徴がある。現在の計算機科学では、ここまで分散化された多数のノードを協調動作させるソフトウェアを効率よく開発する手法が存在しない。しかも、各ノードはリアルタイムプログラミングとセキュリティーという、単独でも困難なプログラミングを施さなければならない。従って、ユビキタスコンピューティング環境のソフトウェアの開発環境は大変重要となってくる。

膨大なノード数をまちまちの開発環境で構築しては、ソフトウェアの再利用性の観点から効率よくプロジェクトを運営できない。

そこで、まず標準ハードウェア、標準基盤ソフトウェア(リアルタイムオペレーティングシステム)の仕様を決め、その上でのユビキタスコンピューティング環境やユビキタスネットワーキングプロトコルのソフトウェアの再利用性、移植性の高い環境の構築を行う。

本研究を行うにあたって、下記の事項を目標とした。

（1）　ユビキタスコンピューティング環境の構築として用いる標準開発プラットフォームとしてのハードウェアを開発する

（2）　4-4 で開発した標準基盤ソフトウェア(リアルタイムオペレーティングシステム)が動作する。

（3）　4-6 で開発したセキュアチップを搭載する。

（4）　Bluetooth,ISO 14443,IEEE 802.11,ISO 7816,無線系電話プロトコルなど各種 LAN、PAN のプロトコルが搭載可能である。

（5）　音声 CODEC を備える。

（6）　グラフィックチップを備える。

ハイエンドクラスのユビキタス環境向けの開発環境の研究を行い、本開発環境を使用した IC カードと連携したセキュリティシステム(鍵システム、ゲート)、IC カードと連携した電子実体流通システム(発券機、自動販売機)などの試作を行い、その実用性を検証した。

また、本開発環境をベースとしたユーザノードの研究、開発を行った。ユビキタスコンピューティングに関連する各種デモンストレーションの開発に応用することで、その有用性を確認した。具体的には、RFID タグと組み合わせてグラフィックユーザインタフェースにモノの情報を有機的に表示するシステムや、電子的な価値情報を転々させるシステムを試作完成させ、評価した。

さらに、最も小型で、安価なユビキタス環境向けの計算機ノードアーキテクチャの研究も行っ

た。通信インタフェースを含んだ、全システムをワンチップに実装し、500 円玉サイズのコイン型開発環境ボードシステムとして、仕様作成および開発が完了した（図 7）。セキュアチップを接続するインタフェースおよび各種通信機能を搭載したシステムとなっている。

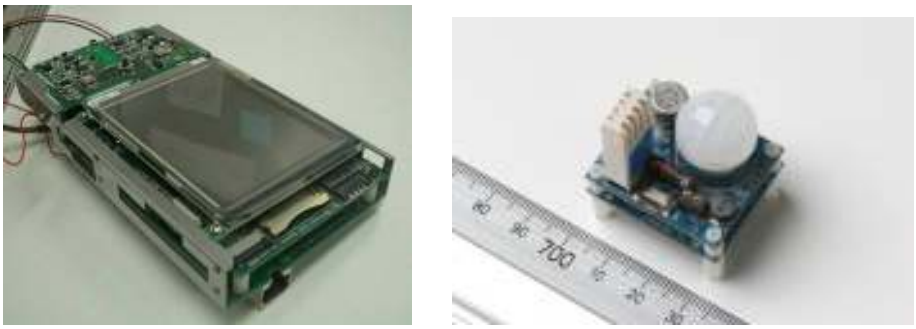


図 7 開発環境ボード（左）、コイン型開発環境ボード（右）

4-3-2 標準開発環境ボード

携帯型ノードを想定した、実験開発用ボードを開発した。CPU として SH3 を用い、各種実験開発が行えるように、ユビキタス環境に必要な多くのインタフェース(USB,PCMCIA,シリアル,ISO/IEC7816,ISO/14443,液晶モニタ,音声 CODEC,指紋認証用のセンサーなど)を備えている。ネットワーク類は市販の PCMCIA カードが多くあるため、あえてオンボード化せずに PCMCIA を用いる方針とした。

この実験開発用ボードを用いて試作したセキュリティードアシステムについて報告する。

入退出ドアに開発した制御機器を取り付け、所定の位置に設置した制御機器に接続した IC カード R/W(リーダライタ)に IC カードをかざすとドアの開錠を行うようになっている。この制御機器は LAN に接続されており、かざされた IC カードの認証情報をサーバに送り、サーバ側でドアの開錠権限があるかチェックし、権限がある場合はドアの開錠を行う。このシステムは、4-4 で開発した標準基盤ソフトウェアを用いて制御を行っている。

上記の実験開発用ボードをベースにした RFID インタフェース付の情報端末の研究、開発も行った。

ここでは、この情報端末を使用した医薬品チェックシステムについて説明する。

本実験システムでは、医薬品の容器にチップが埋め込まれ、薬品の種類や製造時刻が記録されている状況を想定している。各人は携帯している情報端末を医薬品に近づけることにより、薬品の種類や用法、使用期限などを知ることができる。また、複数の薬品を使用しようとする場合に、薬の飲み合わせをチェックすることにより、薬品による事故を防ぐ事ができる。

以下に本実験システムの動作を説明する。

1）医薬品の選択

情報端末上で本実験システムのソフトを起動後、チェックしたい医薬品に情報端末をかざ

す。

2)医薬品の説明表示

情報端末のディスプレイ上にかざした医薬品の説明が表示される。この時、かざした医薬品の使用期限が切れていた場合は、その旨も通知される。

3)飲み合わせのチェック

引き続き、他の医薬品を情報端末にかざすと、その医薬品の説明を表示すると同時に、先にチェックした医薬品との飲み合わせ情報が表示される。一緒に服用しても安全な医薬品はその旨が表示される。一緒に服用すると危険な医薬品は警告画面が表示される。

情報端末外観

薬品の説明表示画面

飲み合わせが危険な
医薬品の表示画面

以上のようにユビキタスネットワーキング環境構築に用いる開発環境の仕様を策定し、実験開発用ボードを開発して、様々な応用システムを開発することで、その開発環境の実用性を検証した。開発したシステムには 4-4 で開発した標準基盤ソフトウェアを用いており、4-6 で開発したセキュアチップを搭載している。これらの開発環境ではBluetooth、各種LANなどのプロトコルが搭載可能である。また、実験開発用ボードを応用した情報端末の実験・デモシステムを開発した。

開発環境を用いて様々な応用システムを試作することで、有用性を確認できた。

4-3-3 小型開発環境ボード

据え置き型ノードを想定した、実験開発用ボードである。CPU として M32R を用い、各種の実験開発が行えるように、多くのインタフェース(シリアル,PCMCIA,ISO/IEC7816,10base-T,人口網膜カメラなど)を備えている(図 8)。

このボードを使用してセキュリティーゲートの入場開閉、セキュリティードアの開錠施錠を行い、

さらに入室入場の様子のカメラ画像を表示端末に転送するシステムを開発した。この実験開発用ボードはシステム中のカメラ画像の転送を行う部分に使用されている。

図 8 実験開発ボード

さらにこのボードを使用して IC カード発券機システムを開発した(図 9)。下記にその概要を示す。

構成

IC カード発券機本体
カード発券機制御部
GUI(グラフィカルユーザインタフェース)部
IC カード R/W

機能

ユーザが入力した個人情報(大人/子供、日本語/英語など)およびユーザが入金した金額情報を IC カードに書き込み発券する。また、ユーザがカードの金額を精算する際、カードの回収および残金情報に相当する金額をユーザに返済する。

図 9 カード発券機

発券機の制御に使用しているボード上では、4-4 で開発した標準基盤ソフトウェアを用いている。

このように開発した開発環境を用いて様々な応用システムを試作し、その有用性を評価し、適用可能なことが分かった。開発した応用システムは本研究所の研究に活用された。

4－3－4 コイン型開発環境ボード

(1)本研究開発の意義

4－1－3章ではユビキタス情報提供・制御用プロトコルであるユビキタスネットワーキングプロトコル(UNP)の研究開発を行った。ここでは、UNPの有用性を検証するために、それぞれ異なる機能を持ったコイン型の開発環境ボードを開発した。

(2)システム構成

図 10 から図 11 にかけて、UNPの有用性確認のために開発した開発環境ボードの一部を示す。センサーボードは、5種類のセンサーを1枚のコイン大のボード上に搭載した。調光ボードは、白熱球の調光を動的に制御するために開発した。赤外線ボードは、エアコンやTVなどの既存の家電機器をUNPネットワークから制御するために開発した。基地局ボードは、4－2－3章で述べたように、UNPとユビキタス型近接通信網とのゲートウェイ機能を実装した。

図 10 センサーボード(左)、調光ボード(右)

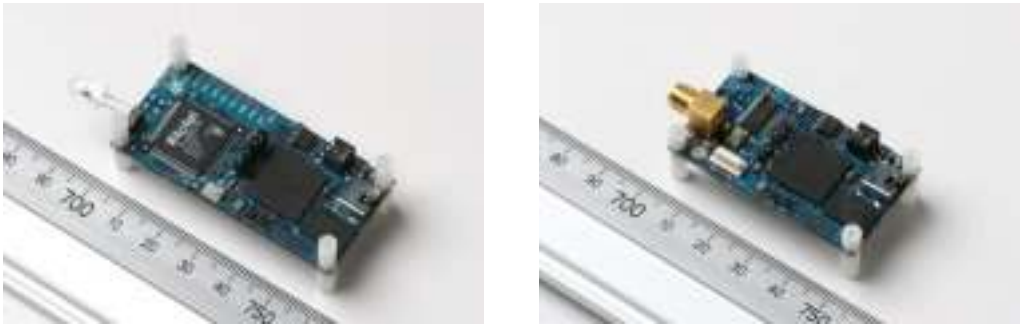


図 11 赤外線ボード(左)、基地局ボード(右)

(3)成果

上記以外にも、UNPネットワークと既存のIPネットワークとの相互接続のためのUNPゲートウェイ装置やUNPネットワーク内で上記のボード類の多段接続をおこなうためのUNPルータ装

置を開発した。これらの開発環境ボードを用いていくつかのシステムを構築して評価UNPの有用性を検証したが、いずれのシステムでも問題なく動作し、UNPが実用に耐え得る技術であることを確認した。

4－4　超機能分散システム指向の開発環境（ソフトウェア）の研究開発

本章では本研究のソフトウェアに関する成果に関して説明する.

4－4－1　研究開発内容

ユビキタスコンピューティング環境では，身の回りのあるゆるものに計算力と通信力を与えてインテリジェントオブジェクト化，ネットワーク化することで高いユーザサービス機能の実現を目指している.

本研究では，以下のような，ユビキタスコンピューティング環境を実現する上で必要となる一連のソフトウェアや開発環境，流通機構をトータルに設計・開発することにより，ユビキタスコンピューティング環境の効率的な実現に向けた研究を実施してきた.

（1）ユビキタス型組込リアルタイムカーネル

マルチタスク機能と豊富なタスク間同期・通信機能を持ち，同時に高いリアルタイム性と省資源を実現するユビキタス型組込リアルタイムカーネルに関する研究を行った.

豊富な機能はアプリケーションの生産性を向上させ，インテリジェントオブジェクトの開発効率を向上させる. 高いリアルタイム性は利用者に対するストレスの無い応答性を提供するだけでなく，制御機器や他のノードに対する高速なリアルタイム性も実現する. また，ユビキタスコンピューティング環境では接続ノード数が膨大になることから省資源，省電力も重要な研究課題となる. そこで，カーネルの実行サイズを小さくすることによる省資源の実現も研究研究対象とした.

（A）ユビキタス型組込リアルタイム拡張カーネル

本研究によって開発したユビキタス型組込リアルタイムカーネルはコア部分であり，小さな組込機器には本カーネルを単体で適用することもできるが，より複雑な機器を開発する場合には別途多様なミドルウェアを自由に追加できるように設計しておく必要がある.

そこで，ミドルウェアの中でも共通的に利用される機能についてユビキタス型組込リアルタイム拡張カーネルとして開発を行い，ミドルウェアのインタフェースに関する研究を実施した.

（B）Java 言語実行環境

Java 言語は"Write Once, Run Anywhere"という目標が示すとおり，プラットフォームへの依存性が低い開発言語である. 本カーネル用のミドルウェアとして Java 言語実行環境を実装することで，他の環境で開発した Java のプログラムとユビキタス型組込リアルタイムカーネルのプログラムを連携させて，アプリケーションの開発効率向上させる研究を実施した.

(C)ユビキタスソフトウェア流通システム

ユビキタス型組込リアルタイム拡張カーネルや各種ミドルウェア，ドライバを安全に流通させるための仕組みに関する研究を実施した．本システムはソフトウェアの再利用性の向上により，ユビキタスコンピューティング環境構築の開発コストの低減と開発期間の短縮を目指す．

(D)ユビキタスミドルウェア群

ユビキタスコンピューティング環境に対応したアプリケーションの開発に必要となるユビキタスネットワーキングプロトコル用の API に関する研究・開発を実施した．

(E)GUIベースの開発環境の開発

インテリジェントオブジェクトの生産性を向上させるためにGUIでの開発ツールを用意した．

パソコン用のソフトウェア開発に比べて難しいとされる組込機器用の開発環境をGUIに対応させることで，開発を開始しやすい環境を作り出し開発者の裾野を広げるという目的もある．

(F)uTAD/Contents

ユビキタスコンピューティング環境で必要とされるコンテクストアウェアネスを実現するための標準データ表現形式となる uTAD/Contents に関する研究を実施した．

uTAD/Contents には，物体の識別情報から分類，性質といったメタ情報，センサの検出状態などの純粋な意味での情報まで含まれている．しかも，常に新しい製品やアプリケーション，サービスが現れるという点を考慮して，非常に単純な基本構造をベースとしながら，必要に応じて拡張できる形式としての実現を目指して研究を実施した．

ユビキタスコンピューティング環境の効率的実現のために必要となるソフトウェアとして，以上のような課題について研究を行った．以下その成果について説明する．

4－4－2 ユビキタス型組込リアルタイムカーネル

ユビキタスコンピューティング環境に配置されるインテリジェントオブジェクトのコアとして利用するためのユビキタス型組込リアルタイムカーネルを開発した．

本カーネルの特徴は以下の通りである．

(A)高いリアルタイム性

ハードウェアにも依存するが基本機能はマイクロ秒オーダーで動作する．

ユーザに対する高い応答性を持つアプリケーションを開発可能にするだけでなく，機器制御用のアプリケーションに対しても十分なリアルタイム性を持つカーネルとして実装した．

(B)豊富な機能

複数のアプリケーションを独立して動作させるためのマルチタスク機能を有するだけでなく，

複数のタスクを連携して複雑な動作を実現するためのタスク間同期・通信機能も豊富に用意した.

これらの機能を利用することでアプリケーションを機能単位に分割して実装することも可能である. 複雑なアプリケーションであっても独立した機能単位に分割して実装することで効率的に開発できるようになる. また, 機能単位毎に独立性の高いモジュールとして存在することになるので高いメンテナンス性を維持することができる.

(C)省資源

本研究で開発したユビキタス型組込リアルタイムカーネルは豊富なタスク間同期・通信機能を持ちながら高いリアルタイム性と省資源性を兼ね合わせている. 実際, 本カーネルは ROM, RAM それぞれ 100KB あれば十分に実用的に動作させることが可能である.

少ないメモリで動作することはメモリに供給される電力を減少させられるという意味でもあり, モバイル機器をそれだけ長時間駆動させられるという意味でもある. モバイル機器の駆動時間の延長はどこでも使えるユビキタス環境の提供に必須の技術であり, しかもユビキタスコンピューティング環境を構成するインテリジェントオブジェクトの数は, 従来のネットワークによるノード数とは比較にならない程膨大である. このため, たとえ1つ1つの機器の電力消費量の削減がわずかであったとしても, 何万個, 何億個と集まれば全体としては膨大な量の電力を節約できることになる.

本カーネルは単に省電力のインタフェースを持つだけでなく, 標準状態において無駄が無く, 組込む機器に適応させることでより省電力にしていける仕組みを実装してある. 全てのインテリジェントオブジェクトの基盤となるカーネルであるためには本カーネルのような設計が必須である.

(D)拡張性

本カーネルは標準状態でも組込機器用のリアルタイムカーネルとして十分に利用可能であるが, 次節で説明するユビキタス型組込リアルタイム拡張カーネルと組合わせることでより複雑な機能が必要となる機器に対応することも可能となる.

ユビキタス型組込リアルタイムカーネルとユビキタス型組込リアルタイム拡張カーネルを合わせて設計・開発することにより, 個別に開発したのでは実現し得ない高い互換性を持つソフトウェアグループを構築することができた.

また, 本カーネルはチューニングによって更に小さな機器にも対応できることを確認している. この研究成果を活かし, 今後はより小型の機器にも対応できるユビキタス型組込リアルタイムカーネルを開発し, 一般に公開していく予定である.

(E)移植性

標準となるカーネルの仕様をハードウェアの標準仕様を含めてトータルに設計することで, 組込機器開発におけるプラットフォームとしての有用性を確認した. 実際, 本研究の成果である仕

様書とソースコードは共に一般に公開しており，既に多くの CPU に対応できることを実証している．

カーネルのリファレンスソースコードを公開することで他の OS にありがちな詳細な動作の違いが発生しないようにも配慮している．これにより，上位アプリケーションの開発効率を高め，更に異なる CPU 間であってもドライバやミドルウェアを容易に流通できる環境を用意した．

以上のような特徴を持つカーネルを設計・開発・公開することで，本カーネルは既に次世代の組込カーネルとして広く認知されてきている．実際，市販製品への採用も進んでおり，現在時点でも多くの製品への適応や検討が進行中である．

本ユビキタス型組込リアルタイムカーネルに関する研究成果は，この先も継続して非常に多くの成果を出していくものと期待される．

4－4－3 ユビキタス型組込リアルタイム拡張カーネル

「ユビキタス型組込リアルタイム拡張カーネル」とは，「ユビキタス型組込リアルタイムカーネル」に対し，より高度な OS 機能を実現するための拡張プログラムである．代表的機能として，MMU（Memory Manegement Unit）による論理多重空間やメモリ保護，プロセス間同期通信，ファイルシステムなどを備える．

（1）概要

「ユビキタス型組込リアルタイム拡張カーネル」は，「ユビキタス型組込リアルタイムカーネル」の上位レイヤに存在し，アプリーションプログラムなどに対し OS 機能を提供する（図 12）．

図 12 ユビキタス型組込リアルタイムカーネルアーキテクチャにおけるソフトウェア構成

以下に機能概要を説明する.

メモリ管理

MMU によるメモリ管理を行う.これによりメモリ保護付きの論理アドレス空間上にて,プロセスアプリケーションの動作が可能である. また論理アドレス空間には, ローカルメモリ空間, 共有メモリ空間, システムメモリ空間の 3 種類があり, それぞれの空間に対して, 指定したメモリブロックサイズの割当て / 解放等を行う機能を提供する.

プロセス/タスク管理

シングルユーザ/マルチプロセスのシステムを提供する. プロセス自体は, OS が管理するプログラム単位であり,「プロセス = 複数タスク + メモリ管理 + リソース管理」を意味する. また処理はタスク単位であり, 複数タスクが存在する場合は, 優先度順および時分割のスケジューリングによって平行実行となる.

プロセス/タスク間の同期・通信機能

プロセス間の同期・通信機能として「プロセス間メッセージ・グローバル名機能」,タスク間の同期・通信機能として「セマフォ・ミューテックス・イベントフラグ・ランデブポート・メッセージバッファ・メールボックス」を提供する.

グローバル名管理

プロセス間で共有するデータ(例えばオブジェクト ID)を任意の名前で参照する機能を提供する.

標準入出力管理

ファイル入出力の基本機能を提供する. なお現在, 対応可能なファイルシステムは以下の通りである.

- 標準ファイルシステム
  - T-Kernel 標準ファイルシステム
- 拡張ファイルシステム
  - FAT ファイルシステム (FAT12, FAT16, FAT32)
  - CD-ROM ファイルシステム (ISO 9660 Level 1)

イベント管理

イベント管理は, 各デバイスからの通知を統一的に管理する機能である. イベント管理の対象となるデバイスは, 主としてキーボード , ポインティングデバイスなどだが, ucode (ユビキタスコード:128 bit 長のコード体系)などのデータを取り扱うことも可能である.

共有ライブラリ機能

複数プロセスが，モジュール共有するための管理機能である．本機能により，プログラムモジュールの動的リンクが可能となる．結果としてモジュールの共有化が可能となり，メモリの使用効率が向上する．

その他

その他の機能として，下記機能を提供する．

デバイス管理	：	各種デバイスを操作するための機能．
時間管理	：	時間・日時に関する管理機能．
システム管理	：	システムプログラムのロード，アンロード機能．

(2)今後の展開

「ユビキタス型組込リアルタイム拡張カーネル」は，カーネルコアのリアルタイム性と拡張機能を持ち合わせており，現代の高度・肥大化した組み込みアプリケーションに対し，非常に有用性の高い OS となっている．

現状においては，すでにユビキタス・コミュニケータなどにも移植されており，工業製品への適用検討も始まっている．また「ユビキタス型組込リアルタイムカーネル」同様，オープンソースとして広く一般に公開する予定である．

4－4－4 Java言語実行環境

Java は，Sun Microsystems Inc.社が 1995 年に開発したオブジェクト指向開発言語，及びその実行環境である．本研究では，「ユビキタス型組込リアルタイムカーネル」，「ユビキタス型組込リアルタイム拡張カーネル」，「ユビキタスミドルウェア群」等の機能を利用して Java 実行環境の実装を行った．本 Java 実行環境の特徴を以下に示す．

(1)採用した Java 実行環境のアーキテクチャ

Java 実行環境のアーキテクチャでは，Java 2 Enterprise Edition(J2EE)，Java 2 Standard Edition(J2SE)，Java 2 Micro Edition(J2ME)の 3 つ【エディション】が定義されている．さらに J2ME では，Connected Device Configuration(CDC)，Connected Limited Device Configuration (CLDC)の 2 つの【コンフィグレーション】が定義され，そのコンフィグレーションの上に，複数の【プロファイル】が定義されている．

本研究では，比較的リッチな組込み向け Java 実行環境として，次のような構成を採用した．

【エディション】

Java 2 Micro Edition(J2ME)

【コンフィグレーション】

Connected Device Configuration (CDC) [JSR-36]

【プロファイル】

Foundation Profile (FP) [JSR-46]

Personal Basis Profile (PBP) [JSR-129]

(2)スレッドモデル

本 Java 実行環境では，ネイティブスレッド方式と呼ばれるスレッドモデルを採用している．これは，Java のスレッドが，ホスト OS(「ユビキタス型組込リアルタイムカーネル」に相当)のネイティブタスクと，1 対 1 で対応するものである．つまり，Java スレッドを 8 つ生成すると，ホスト OS のネイティブタスクが 8 つ生成されることになる．

なお，ネイティブスレッド方式の他に，グリーンスレッド方式と呼ばれるスレッドモデルが存在する．これは，Java 実行環境が，ホスト OS の 1 ネイティブタスク上で動作するものである．つまり，複数の Java スレッドを生成しても，使用するホスト OS のネイティブタスクは 1 つである．

ネイティブスレッド方式を採用した理由は，比較的リソースに余裕があることを想定したことと，後述するネイティブコードとの連携を行う上で，グリーンスレッド方式では不都合な点が多いためである．

(3)ネイティブコードとの連携

本 Java 実行環境上で動作する Java アプリケーションは，Java Native Interface(JNI)を利用して，ネイティブコードとの連係を行うことが可能である．

例えば，GUI アプリケーション，ソケットベースの通信アプリケーションは Java で作成し，デバイスドライバやリアルタイム制御が必要な部分は「ユビキタス型組込リアルタイムカーネル」ベースのネイティブコードで作成する．双方は，この JNI 機能を利用して連携動作させることが可能である．

(4)本 Java 実行環境を利用した組込み向け Java アプリケーションの開発

Java で作成する部分は，PC の Java 実行環境(J2SE)で動作確認できるため，ハードウェア，デバイスドライバの完成を待たずに，先行して開発することが可能である．

また，Java はターゲットに依存しないので，他の CPU を搭載したプラットフォーム上で動作させる場合も，基本的にそのまま(コンパイル不要)で動作する．このように開発の工数，費用削減に大きく貢献すると思われる．

以上のような特徴を持つ Java 実行環境を開発・公開することで，組込み分野におけるアプリケーション開発の効率化，機器のジャンルを越えた Java アプリケーションの再利用等，今後ますます多機能化・高機能化する家電製品の設計・開発が，容易にかつ加速されるものと期待する．

4－4－5 ユビキタスソフトウェア流通システム

(1)はじめに

本研究では，安全にソフトウェア資産を再利用し，テスト期間の短縮を図りながら信頼性の高い組み込みソフトウェアを開発するための，ソフトウェア流通プラットフォームの構築を研究開発テーマとした．

(2)本研究開発の目標

T－Dist(DistはDistribution＜流通＞の略)を開発する．T－Distとは，サブテーマ(ウ)で開発した，標準開発プラットフォームハードウェア，及び，サブテーマ(エ)の(1)で開発した標準リアルタイム OS 上で動作するソフトウェアの流通を強力かつ安全にサポートするプラットフォームであり，本プラットフォームを利用することにより，組み込みシステムにおけるソフトウェアの再利用性を高め，開発コストの低減と開発期間の短縮を目指す．

(3)本研究開発の成果

ソフトウェアの不正利用を防止しながらソフトウェアの流通促進を図るT－Distシステムを構築し，目標を達成した．

T－Distは，ソフトウェアが不正利用されないようにソフトウェアを暗号化し，更に改ざん防止の電子署名を付与して配信する．ソフトウェア利用者は，利用ライセンスを格納したセキュアな耐タンパチップを保持する．流通ソフトウェアを利用するためには，この利用ライセンスが必要で，このライセンスを利用してソフトウェアの暗号を復号してソフトウェアを実行する．最終的に，ソフトウェアを利用者に対して安全に配送し，許可された利用者だけが実行可能となる．これにより，あるユビキタスコンピューティング環境で動作していたソフトウェアをそのまま同じ機能をもった，他のユビキタスコンピューティング環境上でも安全かつ簡単に稼動させることが可能となる．

(4)成果補足説明

T－Distの実装を完了した．また，実用の組み込みソフトウェアを使った機能検証実験を実施し，機能評価，性能評価を実施した．

実装を行った全体システム構成概要およびモジュール構成を図 13・図 14 に示す．

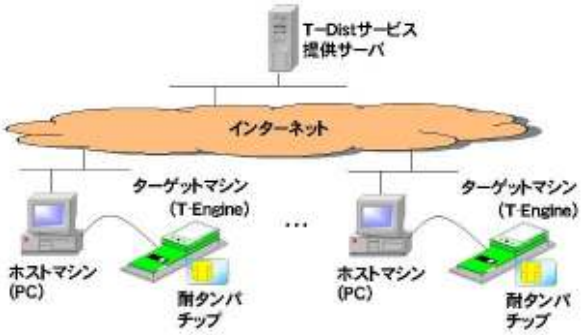


図 13 全体システム構成概要

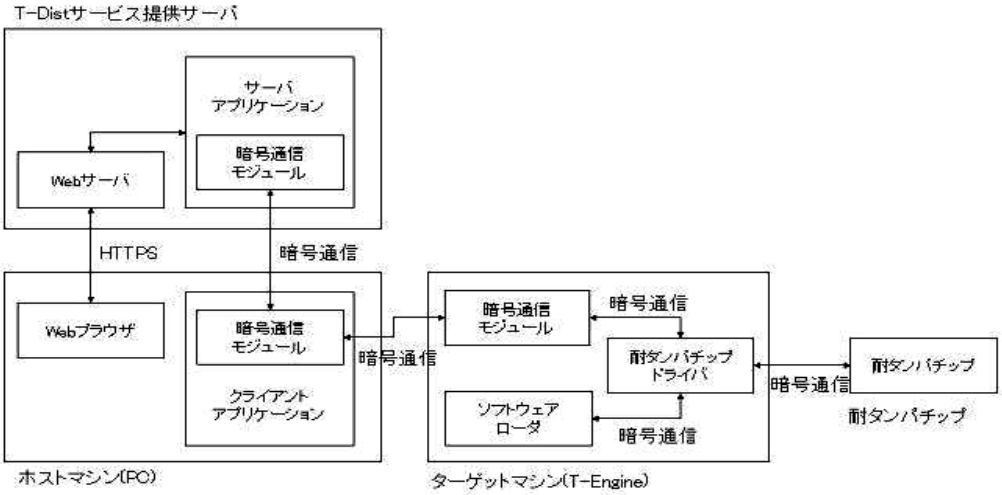


図 14 モジュール構成

本実装では，T－Distサービス提供サーバ，ホストマシン，ターゲットマシン，および耐タンパチップにおける，暗号化ソフトウェア生成機能，ソフトウェアライセンス生成・発行機能，ソフトウェア登録・削除・検索機能，ソフトウェアライセンス一覧表示機能，ソフトウェアライセンスダウンロード要求機能，耐タンパチップ初期化機能，ソフトウェアフォーマットチェック機能，ソフトウェアライセンスチェック機能，ソフトウェア実行機能の実装を行った．これにより，ソフトウェアの不正利用を防止しながら，ソフトウェアを安全に配布することが可能となり，セキュアにソフトウェアの実行を管理することが可能となった．

4－4－6ユビキタスミドルウェア群

(1)概要

ユビキタスネットワーキングプロトコルに対して，抽象度の高いプログラミングを実現する API: Application Program Interface を開発した．

(2)ユビキタスネットワーキングプロトコル用 API

ユビキタスネットワーキングプロトコルとは，ユビキタスコンピューティング環境において，身の

まわりの至るところに組込まれた無数の機器を制御するネットワークプロトコルである．ユビキタスコンピューティング環境において，機器が組込まれている場所，すなわち位置情報は非常に重要な要素となる．また，無数の機器を協調的に動作させるソフトウェアを考えた場合，データ送信時の宛先情報として，それぞれの機器に付与されたネットワーク ID を指定し，ネットワーキングするのは現実的ではない．以上の背景から，機器の位置情報と，照明・空調という機器の機能的な情報で構成される宛先情報で，ネットワーキングすることを可能にするユビキタスネットワーキングプロトコル用 API を開発した．ユビキタスコンピューティング環境下におけるソフトウェアにおいて，本 API を用いることで，『部屋 A の照明すべて』や『フロア B の機器すべて』など，抽象度の高いプログラミングが可能となった．

(3)API 一覧

表 3 ユビキタスネットワーキングプロトコル用APIー覧

機能		名称
初期化・終了	初期化	unl_unp_apiINITUNP
	起動	unl_unp_apiSTARTUNP
	一時停止	unl_unp_apiSTOPUNP
情報参照	状態の参照	unl_unp_apiGETSTATUS
	属性情報の参照	unl_unp_apiGETSPEC
	ネットワーク ID の参照	unl_unp_apiGETDIDNID
通信処理	データの送信	unl_unp_apiSEND
	受信するデータの登録	unl_unp_apiACCEPT
	登録したデータのクリア	unl_unp_apiClrACCEPT
	データの受信	unl_unp_apiRECV
	ARP 要求	unl_unp_apiARP
	RARP 要求	unl_unp_apiRARP
	PING 要求	unl_unp_apiPING

4－4－7 GUIベース開発環境

近年，ターゲットとなる組込み機器ハードウェアの性能向上に伴い，組込み機器用ソフトウェアの開発規模は，PC 用ソフトウェアのそれに近づく規模に増大している．さらに，ビジネスの観点から開発期間の短縮を要求され，生産性向上がますます重要となっている．そのため，組込み機器向け GUI ベース開発環境の整備が必要とされてきている．

本研究開発では，4-4-4節の研究テーマと連携して，オープンソースの GUI ベース Java 開発環境である NetBeans を，ユビキタス型組込リアルタイムカーネル上の Java 言語実行環境と連携させるプラグイン機能を開発した(図 15)．本プラグインは以下の機能・特長を持つ．

(1) コンソール経由での NetBeans・ターゲットボード間のデータ入出力．NetBeans 上で開発した Java アプリケーションをその場で転送・実行できる．

(2) Java 言語実行環境が利用可能な API を検証する機能．Java 言語実行環境で利用できない API(PC またはサーバ機器用 Java 実行環境でないと使えない API)を使用したアプリケーションをターゲットボード上で動かすと発生する，実行時エラーを未然に防ぐことができる．

(3) Java 言語実行環境用のプロジェクトテンプレート自動生成機能．アプリケーション

の構築環境を自動生成してくれるため，環境設定の作業工数削減につながる．

（4） エディタによるアプリケーション作成時に Java 言語実行環境で利用可能な API を補完する機能．プログラミングにおける作業効率が向上する．

Java 言語実行環境用プラグインの導入により，Java 言語実行環境用 Java アプリケーションのコーディング，コンパイル，ターゲットボードへの転送，ターゲット上での実行およびデバッグ，これらの作業を同一の GUI ベース開発環境で，しかも効率よく行なえるようになった．これにより，組込み機器用ソフトウェア開発の生産性向上に役立つことを確認した．

なお，本成果は，T-Engine フォーラムを通じて，2006 年夏をめどに一般公開される予定である．

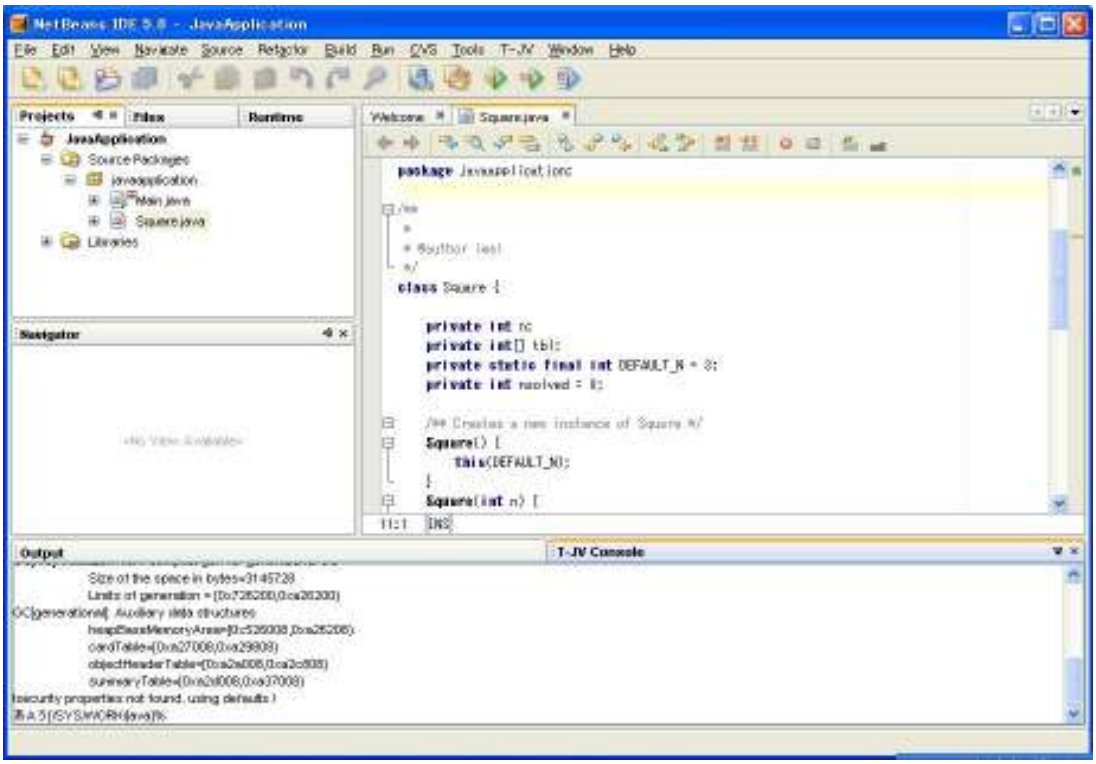


図 15 Java言語実行環境用プラグイン実行例

4－4－8 uTAD／Contents

(1)はじめに

uTAD/Contents は，ユビキタスコンピューティング環境が取り扱う実世界環境のさまざまな情報を記述するための標準データ形式である．記述の基本となる core クラスを基底クラスとし，それを各種アプリケーションごとに拡張することで，さまざまなモノの情報を記述することが出来る．

図 16 uTAD/Contents を利用した情報交換

(2)uTAD/Contents 概要

uTAD/Contents は，さまざまなモノに関する情報を記述するための，RDF（Resource Description Framework)をベースとして設計されたデータ形式である．ここで言うモノとは，具体的な一つ一つの商品や物体だけでなく，サービスに関する情報や，物のクラスに共通のメタ情報，あるいはセンサーからの情報など，情報として区別する必要があるもの全般を含むものとする．モノの情報はアプリケーションやデータベース毎にそれぞれ適した形式で格納されるが，情報交換のための形式として uTAD/Contents を利用することで，アプリケーション間での情報交換が容易となる．(図 16)

uTAD/Contents では，モノに関しての情報を，リソース(主語)とプロパティ(述語)，そしてプロパティの値(オブジェクト，目的語)の三項関係で記述する．また，さまざまなモノを記述するために，モノのクラスを定義する．モノの名称や，包含関係，単位付きの値の記述方法など，基本的なプロパティや記述方式は uTAD core クラスで定義し，この uTAD core クラスから，さまざまなアプリケーションで必要なクラスを派生させ，記述に必要なプロパティを拡張することが出来る．

(3)実証的評価

uTAD/Contents は RDF をベースとしているため，RDF/XML による表記が可能である．XML 形式では既存の XML 形式の記述と親和性が良く，既存形式と uTAD/Contents 形式の相互変換も行うことが出来る．また，RDF は単純な 3 項関係が基本となっているため，uTAD/Contents のシリアライズ処理は容易であり，そのため，バイナリ形式である TAD 形式との相互変換も容易である．

4－4－9 まとめ

本研究ではカーネルなどの基本的なソフトウェアを設計・開発するだけでなく，抽象度の高いプログラミングを可能とするユビキタスネットワーキングプロトコル用 API や GUI ベースの開発環境，コンテクストアウェアネスを実現するための標準データ形式の設計・開発を行った．

ユビキタスコンピューティング環境を実現するソフトウェアに関して，このように広範な研究を

実施することで，基礎的な研究の成果を上位のアプリケーションの開発にまで適用して評価することができ，研究成果の有用性を確認することができた．

各研究項目においては，それぞれ以下のような研究の成果を出している．

(A)ユビキタス型組込リアルタイムカーネル

マルチタスク機能，豊富なタスク間同期・通信機能，高いリアルタイム性，省資源，省電力を実現するユビキタス型組込リアルタイムカーネルを実現し，既に一般に公開している．

本カーネルは，単体で動作する超小型の組込機器から比較的大規模な機器まで幅広い分野での応用事例が報告されており，このことは本カーネルがユビキタスコンピューティング環境を実現している業界において，既に一定の地位を築いていることを示している．

(B)ユビキタス型組込リアルタイム拡張カーネル

ユビキタス型組込リアルタイムカーネルのリアルタイム性を損うことなく機能拡張を可能にするプログラムである．代表的機能として，MMU によるメモリ保護，マルチプロセスにあるアプリケーション管理，ファイルシステム，プログラムの動的なロード，アンロード機能などがある．

(C) Java 言語実行環境

Java のプログラムはプラットフォームが違っても基本的に同一のバイナリでの実行が可能であり，他の環境で開発した Java アプリケーションをユビキタス型組込リアルタイムカーネルで動作させることが可能となる．また，JNI を通して Java アプリケーションからユビキタス型組込リアルタイムカーネルの他のプログラムとの連携が可能となっている．

以上の特長を生かすことで，組込機器に対して GUI やソケット通信をベースとするような上位のアプリケーションを容易に構築できる環境を提供できるようになった．

(D)ユビキタスソフトウェア流通システム

ソフトウェアを暗号化，改ざん防止の電子署名を付与したうえで配信し，利用ライセンスを格納した耐タンパチップによって正当な権利保有者のみが利用できる仕組みを開発した．これによりセキュアにソフトウェアの実行を管理できる仕組みを構築できた．

(E)ユビキタスミドルウェア群

ユビキタスネットワーキングプロトコルを開発し，ユビキタス型組込リアルタイムカーネルで動作する API として実装した．本 API を用いることでユビキタス型組込リアルタイムカーネルで動作するアプリケーションからユビキタスコンピューティング環境に対する抽象度の高いプログラミングが可能となった．

(F)GUIベースの開発環境

本研究の対象である標準開発プラットホームとオープンソースの GUI ベース Java 開発環境で

ある NetBeans を連携させることで，Java によるプログラム開発をシームレスに行えるようにした．これにより Java による組込機器用プログラム開発の生産性を更に向上させることに成功した．

(G)uTAD/Contents

そのクラスから派生させることで様々なモノの情報を記述するための規定クラスとして uTAD core クラスを開発した．情報交換のための形式としてuTAD/Contentsを利用することで，異なるアプリケーション間での情報交換を容易に実現できるようにした．

本研究によって開発した基本ソフトウェアと開発環境，流通システムはユビキタスコンピューティング環境の効率的実現に必要不可欠なツールとなり，実際の組込機器への適用が進んでいる．本研究の成果を活用した製品の開発が進められているだけでなく，既に開発作業を終えて一般市場に投入されている製品も存在している．このことは，本研究の成果，ひいては本研究そのものが実社会にとって真に有用であったことを示している．今後，本研究の成果を利用した機器が広まることで，ユビキタスコンピューティング環境が世界に先駆けて日本で実用化されることが期待される．

4－5 ユビキタスネットワーキングシステムの検証

4－5－1 研究開発内容

本研究テーマにて研究開発した多様なユビキタスコンピューティング技術を駆使し、構築したユビキタス応用システムを数年期間で実運用し、実証的な評価を実施した。各応用システムを構築する上での設計指針は下記のとおりである。

[1] 1 年以上の長期運用に耐え得るシステムであること
[2] 実社会で運用しても実用的なセキュリティ強度と運用容易性を達成できること
[3] 情報通信分野の素人でも容易かつ自在に利活用できること
[4] ユーザインターフェース部分にユニバーサル・デザインが施されていること

本設計指針に基づき、具体的に下記システムの構築および実証的評価を実施した。

■ユビキタスデジタルミュージアム

ユビキタスコンピューティング技術を、博物館展示や屋外の観光ガイドなどに応用し、展示・運営・管理などの機能強化を支援するシステム

■ユビキタススマートオフィス

セキュリティカードを駆使して、利用者の権限に応じて会議室の様々な設備機器を厳重に制御管理する状況認識型の設備機器管理システム

■セキュリティ管理システム

耐タンパ性セキュリティデバイスにて利用者権限や適用されたセキュリティポリシに応じて電子錠の堅牢制御を行う状況認識型の入退室管理システム

■食品トレーサビリティシステム

食品を対象とし、生産・加工・流通・販売の全過程のシステムを有機的に結合し、当該食品情報の遡及・追跡を透過的に提供する統合的な食品情報基盤システム

これら 4 種類のユビキタスネットワーキングシステムを、本研究所を始めとした様々な実験フィールドで 1 年以上長期稼動させ、本研究開発課題の目標を兼ねた上記設計項目を実証的に検証した。このうち、ユビキタスデジタルミュージアムと食品トレーサビリティシステムでは、当該システムを基盤として現実社会での実証実験を展開した。具体的に、ユビキタスデジタルミュージアムでは島根県津和野市の観光ガイドシステムでの実験、食品トレーサビリティシステムは京急ストアや三越といった実店舗での販売実験に成功した。本節では、各応用システムの技術概要およびその実証的評価を記載する。

4－5－2 ユビキタスデジタルミュージアム

(1)骨子

ユビキタスデジタルミュージアムは、ユビキタスコンピューティング技術を、博物館展示や屋外の観光ガイドなどに応用し、展示・運営・管理などの機能強化を目指すものである。利用者の個人プロファイルを利用することで、利用者ごとの展示解説の最適化や、展示評価に利用できる利用者の閲覧履歴追跡などが可能となる。

(2)システム概要

本システムは、(a) 個人プロファイルを記録する耐タンパ性ハードウェア、(b) 展示解説コンテンツを表示するためのキオスク端末や携帯端末、(c) 展示解説コンテンツを格納・配信する情報サーバから構成される(図 17)。

ユビキタスデジタルミュージアムでは、利用者はまず「展示解説に利用する言語」「説明は子供向けか一般向けか専門家向けか」「表示に用いる文字の大きさ」「興味分野」などの、個人プロファイルの登録を行う。個人プロファイルは個人的な情報が含まれるため、第三者から読み取られないように、耐タンパ性ハードウェアに記録する。本システムでは、耐タンパ性ハードウェアとして eTRON カード、あるいは携帯端末であるユビキタスコミュニケータを利用している。

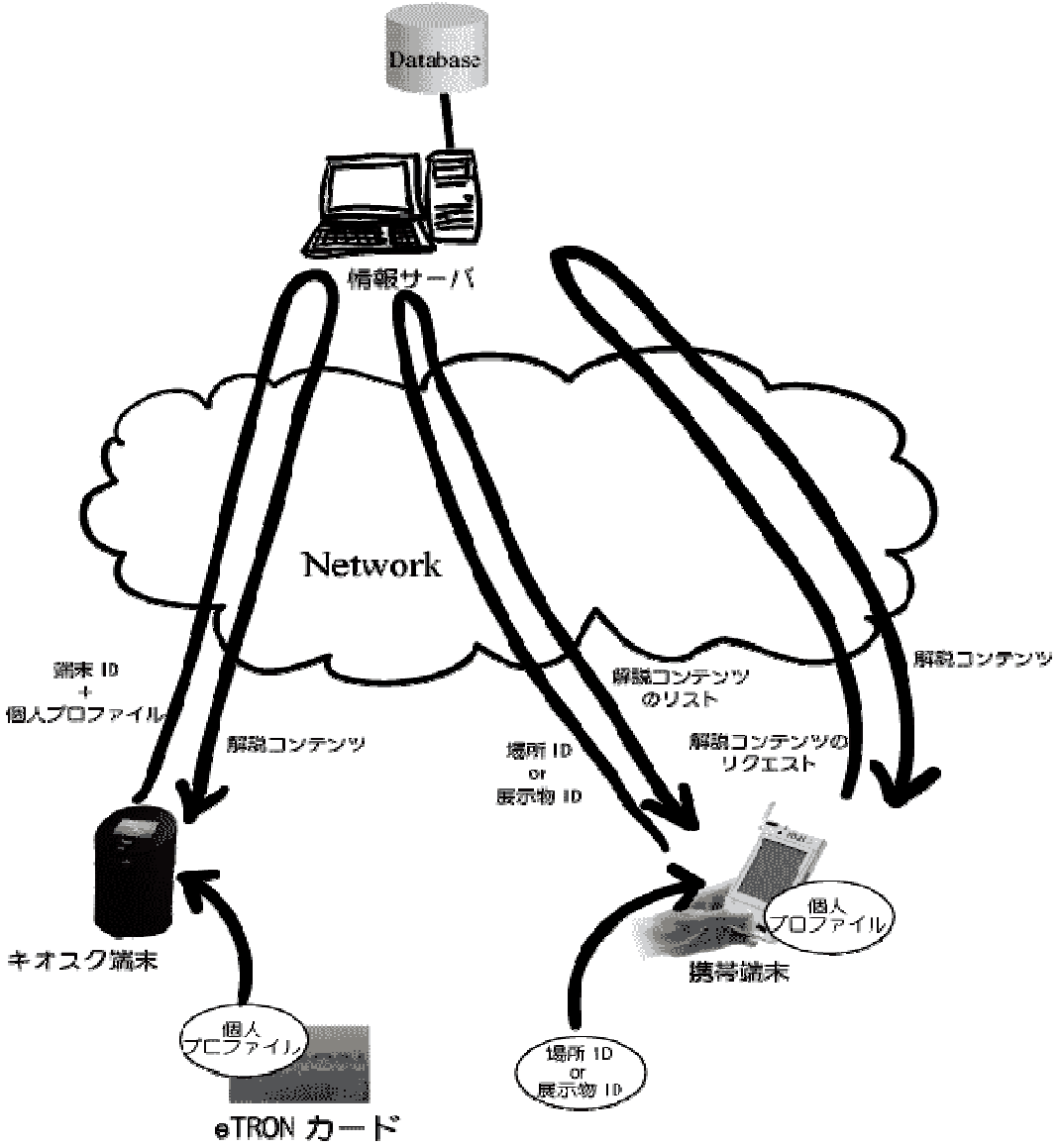


図 17 システム構成

キオスク端末で解説を表示する場合は、キオスク端末に個人プロファイルを読み取らせる。個人プロファイルは、キオスク端末 ID とともに情報サーバに送信され、個人プロファイルに適合する解説コンテンツが送り返される。このとき、閲覧履歴追跡のためのデータベースの更新などの処理も可能である。

また、携帯端末を利用する場合は、展示物や場所などに割り当てられた ID を携帯端末で読み込み、携帯端末が ID に対応する解説コンテンツを情報サーバから取得する。この場合、個人プロファイルは送信せずに、情報サーバから、様々なプロファイルに対応する解説コンテンツのリスト情報だけを受け取り、その中から個人プロファイルに合致したコンテンツを選択して、その後、解説コンテンツ本体を受信するという手法を取ることも可能である。

(3)実証的検証

本システムは、島根県津和野市での観光ガイドシステム実証実験などで運用された。情報通信分野の素人である一般ユーザに実際に利用してもらい、本システムが素人でも十分に使いこなすことが出来ることを実証した。

4－5－3 ユビキタススマートオフィス

(1)骨子

ユビキタススマートオフィスとして、使用者の権限に応じて各会議席より照明、プロジェクタ、ブラインドなどの設備機器を制御する会議室制御システムを構築した。本システムを長期稼動させ、オフィス空間に適用するユビキタスネットワーキングシステムを実証的に評価した。

(2)システム概要

図 18 に、会議室制御システムのシステム構成を示す。各会議席の会議卓内には、タッチパネルより設備機器を制御する制御端末が設置される。各会議卓には、セキュリティカードリーダが設置される。使用者は、権限情報が格納された耐タンパ性セキュリティカードを、セキュリティカードリーダにかざすことで、操作可能な設備機器のみを制御することができる。また、ユニバーサル・デザインに配慮し、音声により設備機器を制御する制御端末も設置される。

(3)実証的評価

本システムを本研究所内に設置し、所内基幹制御システムとして実運用することで、オフィスでのユビキタスネットワーキングシステムを検証した(図 19)。その結果、情報処理分野の素人である一般ユーザでも、本システムを容易に使いこなし、ユビキタスコンピューティングの恩恵を受けられることを確認した。また、約 4 年間の実運用を通し、長期間の運用にも耐え得る情報システムであることを実証した。

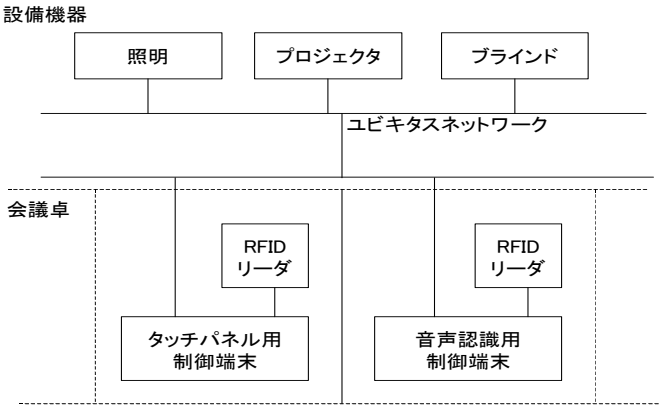


図 18 システム構成


図 19 会議室制御システム（左）、会議卓内の制御端末（右）

4－5－4 セキュリティ管理システム

（1）骨子

本委託テーマで研究開発したユビキタスコンピューティング要素技術を駆使し、本研究所全域の入退室を管理するセキュリティ管理システムを構築した。本システムでは、本研究所の全所員に耐タンパ性を有するセキュリティ管理デバイスを所持させ、本デバイスを用いた入退室管理の数年に至る実運用と実証的評価を実施した。

（2）システム概要

本システムは下記特徴を有するユビキタスネットワーキングシステムである（図 20）。

（1） 所員証を担うセキュリティカードにて所員を特定し、各扉ごとに当該所員の入退室可否を権限管理基幹サーバにて照合および入退室状態を記録管理するセキュリティ管理システム。

（2） 扉制御機器として画面を有する T-Engine や制御装置用 nT-Engine といった各設置環境に最適な組込み制御機器およびこれらを統制する権限管理基幹サーバで構成。

（3） 各扉での制御核となる機器（T-Engine／nT-Engine）上で動作する、セキュリティカード読取装置制御、扉制御、タッチパネル制御、LED 制御、通信制御を担う制御ソフトウェアを搭載。

（4） 本管理制御サーバ扉開閉の時限的制御機能や災害発生時の避難支援機能といった、ユビキタスコンピューティング環境における高度な状況認識型セキュリティ管理機能を具備。

（5） 多様なセキュリティポリシに応じて機器制御や入退室権限を制御管理可能な権限管理基幹サーバの管理者用制御機能を具備。

（3）実証的評価

全所員にセキュリティカードを配布し、本研究所の入退室基幹制御システムとして約 4 年の実運用を実施し、十分にその実用に耐え得る情報システムであることを実証した。情報通信技術者ではない所員、初めて本システムに触れる所員でも十分に本システム機能を利活用可能で、その恩恵を受けられるユニバーサル・デザイン性を具備する情報システムであることを実証

した。

図 20 セキュリティカード(所員証)を用いたセキュリティ管理システム

4－5－5 実証実験での評価

(1)骨子

農林水産省の総合食料対策補助事業に T-Engine フォーラムが主体となり応募、3 年間に渡り採択された実証事業の中で、本研究開発課題で構築したシステムを基盤とした、主に食品トレーサビリティシステム(図 21)に関する実証実験を展開した。

(2)システム概要

(a) 青果・精肉・水産・加工品といった食品を対象として、生産・加工・流通・販売の全段階のシステムを有機的に結合し、各段階で発生する様々な情報を記録し、事故発生時や消費者からの要求時に、その情報を遡及・追跡できる機能を有する。

(b) 図 22 に当該システムとの関連を明確にするシステム構成を示す。

(c) 図 23・図 24 にトレーサビリティ・データを開示するための各手法を示す。

(3)実績

(a) H15 年度実証実験では、1 ヶ月に渡り京急ストア(3 店舗)にて約 3 万個のキャベツと大根に電子タグを貼り付けての販売実験に成功。

(b) H16 年度実証実験では、約 1 ヶ月の間に三越(1 店舗)と京急ストア(1 店舗)それぞれの店舗にて青果物・精肉・加工品・日配品の販売実験に成功。

(c) H17 年度実証実験では、約 1 ヶ月半の間に三越(1 店舗)、コープさっぽろ(2 店舗)とサミット(1 店舗)それぞれの店舗にてお弁当(加工品)・青果物・精肉・鮮魚(養殖)の販売実験に成功。

(4)実証的評価

(a) 1 店舗に係わる生産・加工・流通・販売などの全てのサブシステムを当該システムにて連結し、そこに流通する食品のトレーサビリティの実現を現実社会制度の中で継続的に運用できた。

(b) 複数店舗、また複数事業主のシステムを、当該システムにてゆるやかに結合し、食品情報の相互流用を実現した。

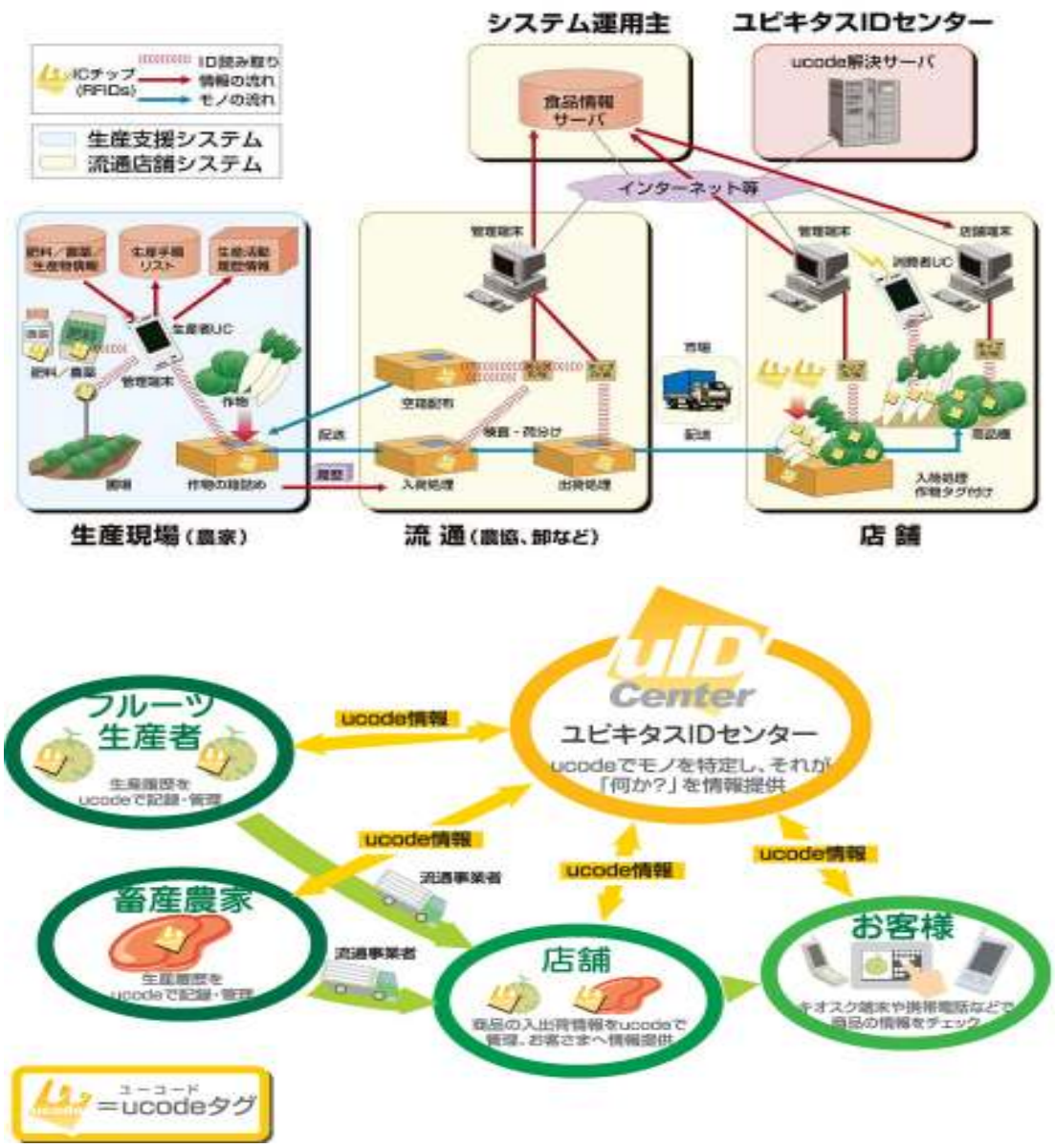


図 21 食品トレーサビリティシステム

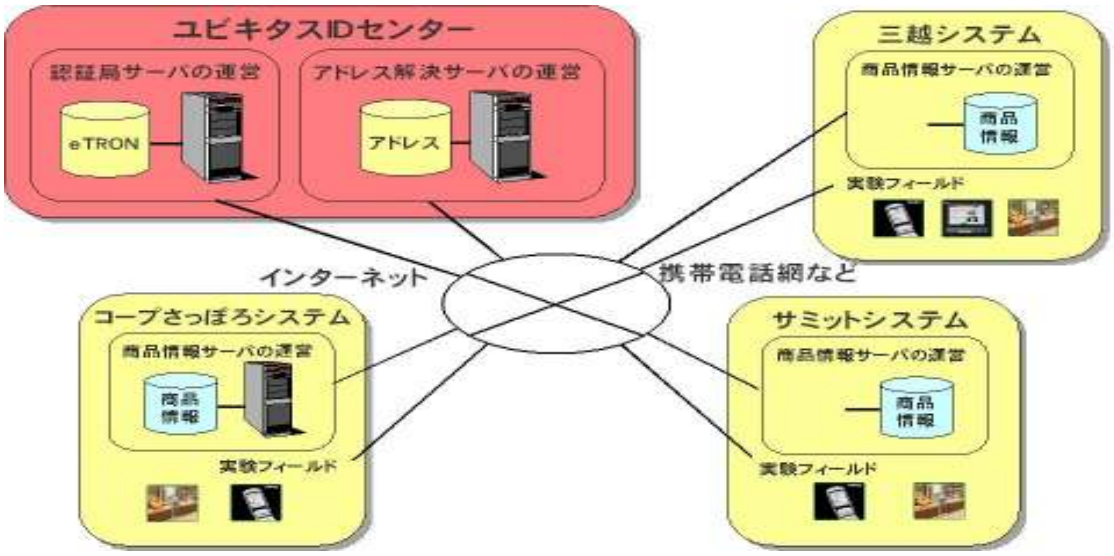


図 22 食品トレーサビリティのシステム構成

図 23 店舗端末での情報表示

図 24 UC／市販携帯電話／自宅PCでの情報表示

4－5－6 まとめ

本研究開発課題で構築したユビキタスネットワーキングシステムが所内運用や社会での実証実験を通じて、十分に実用に耐え得るレベルにあり、現実社会への展開が可能であることを実

証した。本評価は、以下に記すユビキタスネットワーキングシステムの各設計指針や実証的な検証観点からの個別評価を総合した結果である。

1） 1年以上の長期間に及ぶ所内実運用および具体的な実証実験を通して、当該システムが現実社会の中で、その実運用に十分耐え得ることを実証した。

2） ユビキタスミュージアムおよび食品トレーサビリティシステムの実証実験により、観光地や食品の生産現場・加工現場・流通現場・販売店舗といった現実社会における仕組みの中で継続的に運用しても、十分なセキュリティ強度および運用の容易性を確保できることを実証した。

3） 各情報通信分野の素人である一般ユーザや、当該システムの初心者でもその機能を容易かつ自在に利活用し、ユビキタスコンピューティング環境が提供する恩恵を十分に享受できることを実証した。

4） システムのユーザインターフェース部分には、文字、音声、画面推移といったシステム利用に折衝する人間の操作系にユニバーサル・デザインを施し、多様な利用者に柔軟に親和する情報システムであることを実証した。

5） ユビキタスミュージアムは観光ガイドシステムとして現実社会の観光地へ展開し、社会への適合性および実用性を実証的に検証した。また3年間に及ぶ食品トレーサビリティシステム実証実験において、初年度は1事業主（3店舗）、2年目は2事業主（2店舗）、3年目は3事業主（4店舗）と段階的に事業規模を拡大し、当該システムへの影響を検証した。この結果、当該システムの都市レベルへの普及拡大に際して、その実現性に何ら問題がないことを実証した。

6） 実証実験では、利用者やシステム運用主、関連組織への各種アンケート調査により、当該システムに情報システムとしての非社会性やユーザへの不快感を引き起こす要因が存在しないことを実証した。

これら最終目標に掲げた項目の達成に加え、観光ガイドシステムの適用エリア拡大や食品トレーサビリティシステムの汎用システム化および実証実験の拡大に鑑み、本研究開発課題の定量的評価として、120%の成果を上げることができた。

図 25 食品トレーサビリティシステム実証実験の様子

４－６　セキュアコンピューティングの基盤となるセキュアハードウェアの研究開発

４－６－１ 研究開発内容

セキュアハードウェアは、情報を安全に格納し、さらに以下に述べるように PKI ベースの認証、暗号通信機能をそなえることで、全体目標の「(2)公開鍵暗号と PKI をベースとした暗号，認証のメカニズムを有し，社会のインフラを支えるユビキタス環境にふさわしい安全性と信頼性を実現できること．」を実現する際の重要な技術要素となる。

セキュアハードウェアは能力の小さい組み込み機器に、計算量の多いPKI暗号などの機能を提供するための暗箱チップとしても使うことができ、全体目標の「(3) 情報家電やインターネットアプライアンスといった比較的乏しい計算機環境の上でも効率よく動作するように，実行性能がよくかつ規模が小さいシステムになっていること．」の実現に寄与する。

本研究プロジェクトでアーキテクチャを設計したセキュアハードウェアを、暗号、認証機構の知識の少ない組込みシステム開発者が敬遠して、使わないのでは全く意味がない。そこで簡単な API により利用できるセキュアハードウェアアクセスライブラリの提供、アプリケーションの開発環境の提供をもくろんだ。これにより全体目標の「(5) 非専門家でも扱える簡便さを有すること．例えば，暗号・認証機構を知らない人でも，セキュアネットワーキングサービスを利用できること．」を、暗号技術に疎い開発者を対象にして実現する。

セキュアハードウェアとの通信方式であるが、全体の目標にある「(7) IP 網，デジタル方式の携帯電話網，PHS 網，固定加入電話網，ADSL 網といった，既存通信網との間のインターオペラビリティー機能を有すること．」を実現するために、既存のネットワークで簡単に流せるような論理パケットを考案し、またハードウェアの物理インターフェイスは既存の工業標準に準ずるものとして、既存のリーダ、ライターを利用できるようにする。

以上を最終目的として、最初に掲げた具体的な研究の目標は以下の通りである。

(a) コンタクトレス(無線)チャンネルのみを有するコンタクトレスチップと，コンタクトレス(無線)チャンネルとコンタクト(有線)チャンネルの双方を有するデュアルチップを開発する．

(b) コンタクトレス通信チャンネルの物理層・データリンク層のプロトコルは，ISO14443 Type-C 規格を満たす．

(注意:研究開始当時 ISO に 14443 Type-C として提案された規格案は結局採択されなかったが、業界では今でも Type-C という通称でこの案にそった実装のことを呼んでいる。この案にそった「type-C」対応のリーダーライター装置が現在市場で商業的に入手できる。)

(c) コンタクト通信チャンネルの物理層・データリンク層のプロトコルは，ISO 7816 規格を満たす．

(d) 本課題で開発したユビキタスネットワーキングプロトコルで通信する機能を備える．

(e) PKI を使った公開鍵暗号技術に基いた暗号機能・認証機能を備える．

(f) 共通鍵暗号技術に基いた，実行効率のよい暗号機能・認証機能を備える．

(g) 耐タンパー性を有しており，悪意あるユーザからの不正操作から格納情報が守られる．

(h) ユビキタスコンピューティング環境を構成するノードに組み込むことで、そのノードの通信の安全性を向上できる．

以上の目標を達成するために本研究ではセキュアハードウェアのコアとなる IC チップ、カードのアーキテクチャ設計と、そこで使われる PKI 技術の開発をおこなった。IC チップ、カードについては、8ビットCPUコア、16ビットCPUコアを対象にアーキテクチャを設計し、それに準拠した実装の検討をおこなった。PKI 技術開発については、コンパクトな PKI 用の証明書を提案し、その利用に必要な認証局の試験実装を行い、チップシミュレータをつかい多数のユーザによる利用に耐えるスケーラビリティがあることを確認した。

4－6－2　8 ビット型 セキュアチップ

(1)研究内容

第一段階として、研究アプローチの妥当性をしらべるために、まず8ビット CPU コアを利用して実装できる規模の共通鍵を利用した認証を行うカードアーキテクチャの設計を行った。(この理由は、研究開発当時は 16ビット CPU コアを利用した IC カードは出始めてまもなく、まだ実績も少なく、PKI をフルに実装するには時間がかかることが予想されたからである。)

8ビットCPUコアを利用してできるICカードは、ハードウェア資源が非常に乏しいという制限をもつ。メモリ量、CPU 速度の制限から以下のような機能制限がある。

- PKI ではなく、共通鍵を使った認証のみをサポートする。
- プログラムをいれるメモリも少なく、通信プロトコルも簡素なものにせざるを得ない。また物理インターフェイスも複数もつことが困難だったため、非接触インターフェイスのみを考慮した。

なお、アーキテクチャの特徴と、命令の概要は次の16ビットデュアル I/F セキュアチップのところで説明する。

(2) 成果

結果として、共通鍵利用の認証を行い、非接触のリーダ、ライターを通じて遠方と通信ができて、ユーザのデータを安全に格納することができる IC カードのアーキテクチャを作成した。

共通鍵を利用する制限から、このチップアーキテクチャは安全性ならびに鍵の配送の問題をを深く追求するよりは、非専門家でもあつかえる簡便さを有するセキュリティシステムをつくるためのテストベッドとして広く利用された。このアーキテクチャに準拠したチップを利用して各種の実証実験を行なうことで、これにつづく16ビット CPU コアを利用する IC カードのアーキテクチャ設計、各種応用設計の基礎を確認することができた。

しかし、テストベッド以外の応用にも、この8ビット CPU コアを対象としたチップアーキテクチャ

は現在でも有用である。8ビット CPU コアを利用した IC カードはコストを低くおさえることができる。共通鍵認証の限界を理解した開発者がアプリケーションを設計すれば、低コストのセキュリティ応用に使うことができる。

4－6－3 16 ビット型 デュアル I/F セキュアチップ

(1)研究内容

PKI 技術を本格的に利用するには、8ビットCPUコアでは実用にならず、16ビットコアを使い、さらに多倍長指数計算を高速に行えるコプロセッサを持つことが必須である。そこでPKI利用のための16ビットCPUコアを利用するアイシーカード、チップのアーキテクチャを設計した。

16ビットCPUコアを使うICカード、チップでのハードウェアリソースは、当然のことながら8ビットCPUコアの場合にくらべれば多い。しかしRAMはせいぜい8KB程度しかない。このようなハードウェアを想定して、16ビット CPU コアを利用する場合のセキュアハードウェアのアーキテクチャ設計を行った。取り入れた主要な機能は以下の通りである。

- PKI を使った認証、暗号通信の実現（8ビット CPU コアのときの共通鍵認証もサポート。）
- 内部にユーザが情報を格納する部分を8ビットCPUコアの場合にくらべて大量に持つ。（ファイルと呼ぶ。）
- 「4-2-5 統合型分散バイオメトリクスシステム技術」で述べるテンプレートデータはこの「ファイル」に格納することで実証実験をおこなった。
- 暗号通信路を介して価値情報を安全に交換するためのトランザクション機能付きファイル交換機能。
- 認証した相手の ID をもとにしたアクセス制御機能。
- 外部との物理インターフェイスは、非接触、接触両方をサポートできるような切り替え機構。
- (この外部インターフェイスを通じて交換するパケットは 4-1-5 のユビキタス価値転送プロトコルである。既存のネットワーク経由で簡単に流すことができるように設計された。)
- VPN 機能（これは8ビットCPUコアでは容量制限で入らない。）
- 「4-1-6 セキュアユビキタスVPN」で述べる VPN機能に使える、PKI用鍵データ、ならびに共通鍵計算機能。
- なお 16 ビット CPU コアを対象とするアーキテクチャ仕様は巨大なものとなり、設計の問題点ならびに仕様の整合性をしらべるためにチップシミュレータをつくり動作の妥当性を検証した。アーキテクチャ設計にもとづき、試験的にチップを実装する際には、動作を比較して検証する上でシミュレータは非常に有用であった。

(2)成果

上記の16ビットCPUコア対象のアーキテクチャを準拠とするチップは、VPN 機能を使いアプリケーションデータの安全な通信での利用、価値交換を使いチケットのような有価情報を購入、交換する実証実験での利用、ホームないしはオフィスオートメーションのための組み込み機器が PKI を利用した暗号通信をする際の補助プロセッサとしての利用、バイオメトリクスのテンプレートデータの保存利用などを経て、その有効性が実証された。

4－6－4 ユビキタス PKI

(1) 研究内容

前説までに述べたセキュアハードウェアでのPKI技術の利用には、鍵データを認証局の署名付き証明書形式で保持する必要がある。

一般に PKI 技術の枠組みで広く使われる X.509 の証明書形式は記述機能が豊富な一方、比較的データサイズが大きくなり、証明書の中を解釈して処理をするプログラムルーチンは複雑で大きくならざるを得ない。

ゆえに、X.509 の形式はハードウェア資源が豊富にある PC,サーバーには問題なく使えても、リソースが乏しい IC カードで、単に解釈なしに証明書を格納するのではなく、eTRON アーキテクチャにおけるノードとして、積極的に証明書の内容を解釈して処理を行う目的には記述機能が高い分、IC カードの処理の負担が大きすぎる。

そこで本研究では X.509 形式のような記述機能が高い証明書形式ではなく、ユビキタス環境のハードウェアリソースの乏しい機器でも PKI 処理が確実に行えるような比較的サイズが小さい固定形式の証明書を利用してPKI認証を行うアーキテクチャの設計、実装、検証を行った。

(i) 証明書の小型化と認証方式

IC カードに格納できて、かつ高速に出し入れできるように全体のサイズを小さくした固定形式の証明書を設計し、これを利用するPKI認証方式を設計した。そして、その方式を備えるチップを実装して、実際に認証通信をおこなうようにした。(上記 4-6-3 での16ビットCPUコアの試験実装ではこの証明書と認証方法が利用されている。)

この方式はサービスを提供する機関が単一である場合に有効である。すなわち証明書発行機関がひとつしかない場合である。

(ii) 将来の大規模な利用に対するシミュレーションによる性能評価

固定形式の小型証明書(第一版)は、X.509 にあるような階層化された証明局による証明書の真正度の連鎖した保証はできないものであった。すなわち、ひとつの証明局がアプリケーションが想定するすべてのセキュアハードウェアを管理しているという応用モデルを採択していた。

しかしながら、将来のユビキタス環境においては、膨大な数のハードウェアノードをひとつの証明局がすべてをみるということは、信頼性ならびに処理速度の点からありえない。やはり階層化された複数の証明局の管理が普通となろう。

そこで、5年後、10年後の将来をみすえて、階層化された証明局複数による管理を行なった

場合に、効率良く利用できる証明書形式を考案して、それを利用した認証アルゴリズムを設計し、シミュレーションによる性能評価をおこなった。

この新方式で、リソースの乏しいセキュアハードウェアでどう対応するかが重要である。可能な範囲の必要最小限の認証はセキュアハードウェアチップが行うが、未知の第三者の証明書の正当性は外部 CA の検証局に判断を委譲するという方針のもとに、次世代証明書フォーマットの設計をおこない、外部サーバーの実装、チップシミュレータによる動作検証をおこなった。

ひとつの認証局が100万個オーダの証明書の発行、管理を行う場合のスケーラビリティもシミュレーションにより考慮したが、実用的な応答速度が得られている。

(2) 成果

ユビキタスコンピューティング環境でのリソースが乏しいハードウェアでも迅速に処理のできる証明書形式を単一証明書発行機関しかない場合、階層構造に複数の証明書発行機関が相互に連係しあっている場合のそれぞれに提案し、それを使った認証方法を実際のチップに実装したり、シミュレーションを行うことで有効性を確認できた。

4－6－5 まとめ

セキュアコンピューティングの基盤となるセキュアハードウェアの研究開発

(1)研究内容

以上のような背景と方針で研究をすすめてきた。最終目標の達成度を確認してみよう。

目標(1)

コンタクトレス(無線)チャンネルのみを有するコンタクトレスチップと，コンタクトレス(無線)チャンネルとコンタクト(有線)チャンネルの双方を有するデュアルチップを開発する.

実績:両方の実装版を作成した。

目標(2)

コンタクトレス通信チャンネルの物理層・データリンク層のプロトコルは，ISO14443 Type-C 規格を満たす.

実績:8ビット CPU コア、16ビット CPU コアの実装はこれをみたしている。

目標(3)

コンタクト通信チャンネルの物理層・データリンク層のプロトコルは，ISO 7816 規格を満たす.

実績:16ビット CPU コアの実装はこれをみたしている。

初期の段階では ISO 7816 の物理層、データリンク層だけをみたしていたが、徐々に改善を行ない論理的に T=1 と呼ばれる層も最近の実装では満たしており、通信互換性が非常に高く、

読み書きできる PC に USB 経由でつながるリーダーライターも多数ある。たとえば Windows OS を利用する PC に容易に繋げることができる。

目標(4)

本課題で開発したユビキタスネットワーキングプロトコルで通信する機能を備える.

実績: この通りであり、各種実験の場で、IP 網を通じて価値情報の交換、チップ間の通信を行ってきた。

目標(5)

PKI を使った公開鍵暗号技術に基いた暗号機能・認証機能を備える.

実績: 16ビット CPU コアの実装でこれを満して、各種実験で利用してきた。

目標(6)

共通鍵暗号技術に基いた, 実行効率のよい暗号機能・認証機能を備える.

実績: 8ビット CPU コア、16ビット CPU コアの実装はこれを満して、各種実験で利用してきた。

目標(7)

耐タンパー性を有しており, 悪意あるユーザからの不正操作から格納情報が守られる.

実績: 8ビット CPU コア、16ビット CPU コアのベンダーと協力し、試験実装はベンダーの保証する範囲で物理的なタンパー性を備える。

(たとえば鍵の計算中の消費電力の変動から、鍵の値の範囲を狭めるような予測を行う攻撃に対しても、ダミーの計算を混ぜることで、推定を困難にするなどの工夫がなされている。)

目標(8)

ユビキタスコンピューティング環境を構成するノードに組み込むことで, そのノードの通信の安全性を向上できる.

実績: 実験でこの機能は実証されている。バイオメトリクス(4-2-5 参照)を利用した実験、UC 端末のでのセキュアユビキタス通信(4-1-6),VPN 通信(4ー1ー6)を利用した食品トレーサビリティ実証実験における個人プライバシー情報の送受信など、機器に組込んで通信の安全性を向上できることが実証されている。

結論:上記に述べたように外部の第三者の参加する各種実験での利用により目的の達成が確認され、機能有効性が確認されており、達成度は120%と考える。

4－7ユーザノードシステムの研究開発

4－7－1研究開発内容

身の回りのさまざまな物や場所に小型化したコンピュータが存在し、常に私たちをとりかこむ環境をユビキタスコンピューティング環境という。この環境は単にコンピュータが小型化して埋め込まれたものではなく、”いつでもどこでも誰にでも”必要な情報にアクセスし最適なサービスを提供する。 この環境において、直接利用者（ユーザ）が接し、サービスを提供するものをユーザノードと定義する。このユーザーノードは本研究で規定した標準プラットホームのアーキテクチャをベースにしたもので実現をおこなう。

標準プラットホームはユビキタスネットワーキングプロトコルを標準で組み込み、マルチタスク機能やタスク間通信・同期機能に加え、セキュリティ機能を有するのを特徴とする。この標準プラットホームを基本として本研究にて PDA 型ノードと電話型ノードの2種類の開発を完了した。

これらのノードが従来のコンピュータと大きく異なる点は、ユビキタスコンピューティング環境とコミュニケーションをとり、その時点で最適なサービスをリアルタイムに提供することにある。ここでいうコミュニケーションは以下の3つの概念としてとらえることができる。

人とのコミュニケーション

言葉という音声や表情・身振りといった映像をおくることで、相対する人に自分の意思疎通を行う。

モノとのコミュニケーション

モノにその内容を示すコンピュータ（タグ）を埋め込み、これから読み取った内容をキーにネットワークによってつながれたサーバを検索しモノの持つ情報を提示する。

場所とのコミュニケーション

家電などに組み込まれたコンピュータやさらには場所に埋め込まれたコンピュータとの通信をおこない、環境の情報を入手してそれをもとに道案内やガイドなどのサービスや家電の操作などを行う。

これらに対してユーザに負担を強いる事無くコミュニケーションを行うのがユーザノードの目的である。

それには外部から取り込まれる様々な情報を抽象化して統一的に扱い、効率よく情報を抽出して提示するシステムが求められる。この要件に対して、すべての物・場所にユニークな ID を割り振ることで識別を行う情報管理体系を整備し、ID をもとに情報を検索するシステム、情報やサービスを提供するユーザノードのソフトウエアの開発を行った。

また場所に対してIDを割り付ける場合、その場所において最適なサービスを提供するためには精密な位置を特定する必要がある。既存のものとしては人工衛星を用いた位置測定として

GPS システムが知られているが、野外でしか運用できないという制約があり、かつ誤差が大きく発生するため最適とはいえない。これに対して新たに屋内でも運用でき、充分な精度を持つ位置検出方式を開発した。

4－7－2 PDA 型ノード(UC)(ハードウェア)

ユビキタスコンピューティング環境において，人が直接利用するコミュニケーションツールは必要不可欠である。これを PDA 型ノードとして実現したものが、ユビキタス・コミュニケータ（以降 UC と略）である。具体的には，複数の通信手段を搭載した携帯情報端末であり，場所やモノに設置した IC タグ・赤外線・微弱無線・BuleTooth マーカーなどから ucode を取得する（図 26）。そしてその ucode を元に、ユーザに最適な情報をネットワークなどを通じ提供する.

図 26 ユビキタス・コミュニケータ

4.7.2.1 UC の主な機能

UC は，T-Engine アーキテクチャを採用し、OS としてユビキタス型組込リアルタイムカーネル（T-Kernel） を搭載している。また各種ネットワーク機能や、画像処理用の専用 ASIC、音声 CODEC などを実装しており、様々な用途への対応が可能である.

図 27 各部機能名称

UC の特徴的機能について以下に挙げる.

1) マルチバンド ucode タグリーダ機能

2.45GHz と 13.56MHz のマルチバンドリーダを内蔵する. これにより, 1 台の UC 端末で, μチップや eTRON カードなどと通信することが可能である.

2) 赤外線送受信機能

赤外線方式によるデータ送受信が可能である. これにより ucode の受信や, UC をリモコンとして使用することも可能である.

3) Bluetooth 機能

内蔵する Bluetooth により, 外部接続の RFID リーダーライターやヘッドセット, その他の周辺機器をワイヤレスに接続することが可能である.

4) 無線 LAN 機能

IEEE802.11b に対応する. これにより各無線アクセスポイントへの接続や UC 同士の通信が可能である.

5) カメラ機能

CMOS 30 万画素(前面)と CCD 200 万画素(背面), 2 種類のカメラを実装している. これにより 2 次元バーコードや電子透かしなどからの ucode 取得も可能である。

6)高速な画像処理

MPEG4 動画の再生, JPEG 画像の展開・拡縮・回転が可能である.

7) クレードルによる機能拡張

平時使用しない機能については，拡張クレードルの接続により使用することが可能である．主な機能としては，USB，シリアル通信などがある．

4.7.2.2　UC 機能の応用

UC は各機能を利用することで，様々な用途への適応，システムへの組み込みが可能である．以下にその応用例を挙げる．なおこれら応用例は、各種実証実験等において実際に使用されている。

モノ・場所に関連した情報の提供

UC の持つ代表的なコミュニケーション機能（マルチバンド ucode タグリーダ・赤外線受信モジュールなど）を使用することにより，モノや場所に設置した ucode 情報を引き出すことが出来る．情報は音声・静止画再生だけでなく，動画再生なども可能であり，観光ガイドなどへの応用も期待できる．また外部の RFID リーダ（例えば杖型リーダ）と BlueTooth を連動させ，歩行者ナビゲーションなども行うことが可能である．

ucode タグを応用したユーザインタフェースの実現

カード型の ucode タグを UC にかざすことで，そのカード（ucode）に対応した言語に UC の再生モードを切り替えることが出来る．モードを切り替える方法は色々考えられるが，カードタグを利用することで直感的に，また容易に UC を操作することが出来る．

カメラ機能の応用

カメラ機能を利用することで 1・2 次元バーコードや電子透かしなどからも ucode を取得することも可能である．また UC の前面カメラと内蔵無線 LAN の組み合わせにより，VoIP（Voice over Internet Protocol）による電話機能も実現している．

4－7－3 UC ソフトウェア

ユビキタスコミュニケータ(UC)で動作するソフトウェアのアーキテクチャを図 28 に示す。

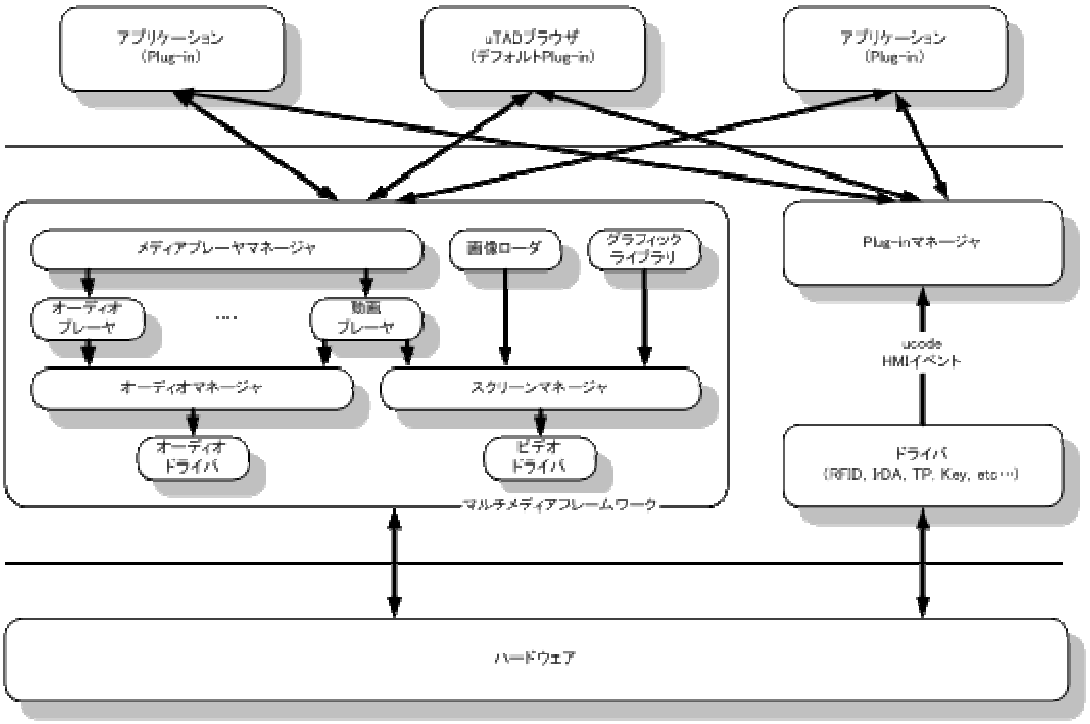


図 28　ＵＣソフトウェアアーキテクチャ

uTAD ブラウザ

UC に具備された各種デバイスで受信した ucode を元に，uTAD で記述されたコンテンツを取得／表示する機能を持つ．これを応用して ucode に括り付けられた情報をユーザに提供する様々なシステムに利用できる．また，ボタンやタッチパネルなどの HMI イベントにより，コンテンツのブラウジングや UC 本体の制御を行う機能も持つ．

Plug-in マネージャ

本アーキテクチャには，UC 上で動作するすべてのアプリケーションを Plug-in とし，それらを統括管理する Plug-in マネージャがある．UC ではこの Plug-in マネージャにより負荷が軽いマルチアプリケーションシステムを実現している．また Plug-in マネージャはシステム内で発生する HMI イベントや受信した ucode をアクティブな Plug-in に配送する機能も持つ．

マルチメディアフレームワーク

本アーキテクチャには，映像／音声などのメディアデータの種別毎に複数存在するプレーヤーミドルウェアをひとつの抽象化されたインタフェースを経由して制御可能にするマルチメディアフレームワークがある．その中核となるのがメディアプレーヤーマネージャであり，ここでシステム内にあるプレーヤーミドルウェアを統括管理することで，メディアデータのフォーマットに関わらず，再生／レコーディング等の制御を統一的なインタフェースで制御できる．そのためアプリケーションは各メディアプレーヤミドルウェアインタフェースを個別に定義する必要はない。

画像処理系

本フレームワークには複数アプリケーションに対し画像描画機能を提供するスクリーンマネージャがあり，アプリケーションはスクリーンマネージャを介して画像用メモリに対し画像を描画することができる．また複数枚のフレームバッファを使用した動画再生にも対応している．更には画像用メモリに対し線・点・文字などの低レベルオブジェクトの描画を行うための機能を持つライブラリや，JPEG などの各種静止画メディアデータを画像用メモリにロードするミドルウェアもある．

音声処理系

本フレームワークには複数アプリケーションのオーディオ出力のミキシングを行い、音声出力するためのオーディオマネージャがある．オーディオマネージャは仮想デバイスドライバをアプリケーションに提供し，そこへのオーディオ出力を内部でミキシングし実際のオーディオデバイスへ出力する．また複数オーディオデバイスの制御にも対応している．

UC ソフトウェアアーキテクチャに Plug-in マネージャとマルチメディアフレームワークを搭載することにより，UC をマルチアプリケーションシステムとして動作させることができるようになり，UC の利用シーンを広げることができた．

また，マルチメディアフレームワークを使用することでアプリケーションの開発効率や移植性，拡張性も向上することができた．

4－7－4 電話型ノード（UC-Phone）

（１）概要

UC-Phone とは、ひとり１台があたりまえになった携帯電話としての機能をベースにおきながら、ユビキタス環境とコミュニケーションする機能を搭載させたユーザノード端末である。本研究は、UC-Phone のハードウェアとソフトウェアとして実際に動作するものを試作し、実証試験を通して、ユーザノードとしての有用性の確認や問題点の抽出を目的とする。

（２）主要機能

■超小型 RFID リーダライタ

低消費電力、かつ、小型の RFID リーダライタを試作して UC-Phone に搭載している。研究開発の成果として、３種類の RFID リーダライタへの対応を完了した。13.56MHz タグ 1 種、2.45GHz タグ 2 種。これにより、実験環境（モノの材質や場所）に適したタグを選ぶことができた。

■レーザースキャナ

RFID の読み取りだけでなく、レーザースキャナによる印刷タグ（バーコード）の読み取り機能を搭載した。バーコードを使った既存システムと RFID システムの融合や、タグのコスト削減などを目的として、印刷タグを併用したシステムの構築は十分に想定でき

る。

■無線インタフェースに PHS

無線インタフェースには PHS を採用した。実験用の無線インフラを必要に応じて選ぶことができ、低コストでの実験環境構築を可能にした。移動体通信事業者の公衆接続サービスを使っての広域実験と構内 PHS 網による実験の両方に対応した。

（３）システム構成

図 29 に UC-Phone をユーザノードとした基本システム構成を示す。ゲートウェイアーキテクチャを採用し、以下の機能を UC-Phone ゲートウェイに持たせた。UC-Phone と UC-Phone ゲートウェイの組み合わせで、ユーザノードとしての機能を実現している。

- IP-PIAFS プロトコル変換機能
- サーバノードとの連携機能（ucode 解決）
- コンテンツ取得機能

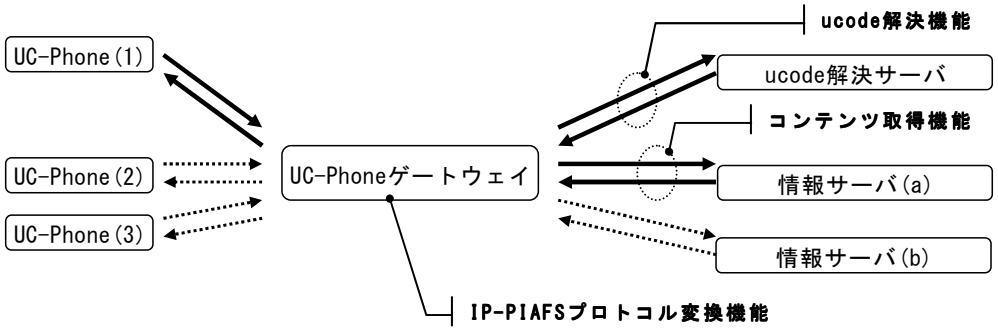


図 29 システム構成

4－7－5 AR型インタフェースのための屋内位置検出（電波方式）

AR 型インターフェースを実現するための屋内位置検出精度を達成するために、アクティブ方式の位置検出方式を開発した。アクティブ型位置検出方式では、AR型インターフェースを実現するに足る位置検出精度を得ることが一般に可能であるが、個々の対象物に位置取得のためのセンサまたは発信器を設置しなければならず、そのコストや電力供給が課題とされていた。それに対して本方式では、位置情報を取得する対象となる物へ位置センサを取りつけることなく位置や向きの情報を取得することを可能とし、物の位置を容易にコンピュータへ入力することを可能する方式を開発した。本方式のシステム構成を図 30 に示す。

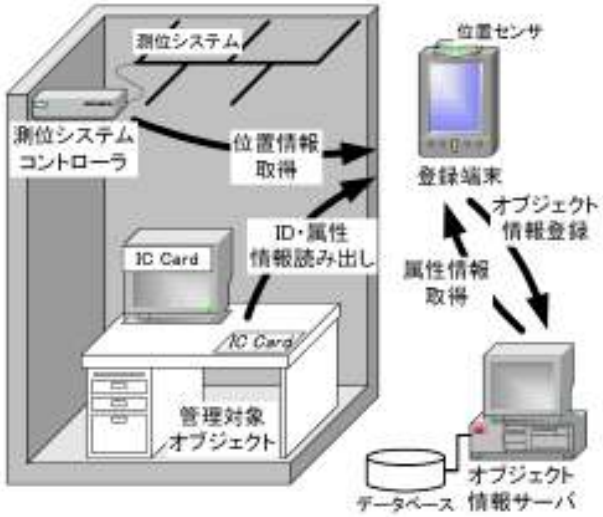


図 30 システム構成

本方式では、位置センサと比べて安価で薄く、電力を消費しない非接触電磁誘導方式の IC カードを管理対象オブジェクトの任意の場所に貼付する。IC カードにはオブジェクトの ID が格納されている。次に位置登録端末として、本章で記述したユーザーノードを用いる。同端末は、ユーザーノードの基本機能により、オブジェクトに貼り付けられたICカードを読み取り、その情報をネットワーク上のサーバに通信可能である。さらに本端末は、アクティブ型位置検出用センサを備えているものとする。位置検出の手順は以下のとおりである。

(a) ユーザは測定対象オブジェクトに貼付した IC カードへ端末を近づける。端末は IC カードとの通信を行い、オブジェクトの ID と、属性情報を読み出す。

(b) オブジェクトに隣接した端末に取りつけられている位置センサを利用し、測位システムから位置情報や大きさの取得を行なう。オブジェクトの位置情報の計測は、オブジェクトのあらかじめ定めた点の空間位置を測定することで行なうこととする。

(c) 端末を使用して得られた位置情報や属性情報などの全てのオブジェクト情報をオブジェクト情報サーバへ送る。

(d) オブジェクト情報サーバは、端末から送られてきたオブジェクト情報をデータベースへ登録する。

このように本方式では、コストと電力供給の課題を持つ位置センサをユーザーノードに搭載し、必要に応じて同ノードをユーザが持ち運ぶことで、その問題を解決した。また、非接触 IC カードの貼付位置も測定点ではないために、取り付け場所の制約も低く抑えることが可能となった。

オブジェクトの位置測定に用いる場所の違いによる測定誤差について測定・評価を行なった結果、位置測定に影響を与えない点を利用することで、1 から 2cm 程度の誤差で位置情報を取得でき、比較的小さい物(一辺が 10cm 程度)にも適用が可能であり、AR型インタフェースへの応用が可能であることがわかった。図 31 は、位置情報の取得結果を3Dグラフィックス化した

例である。

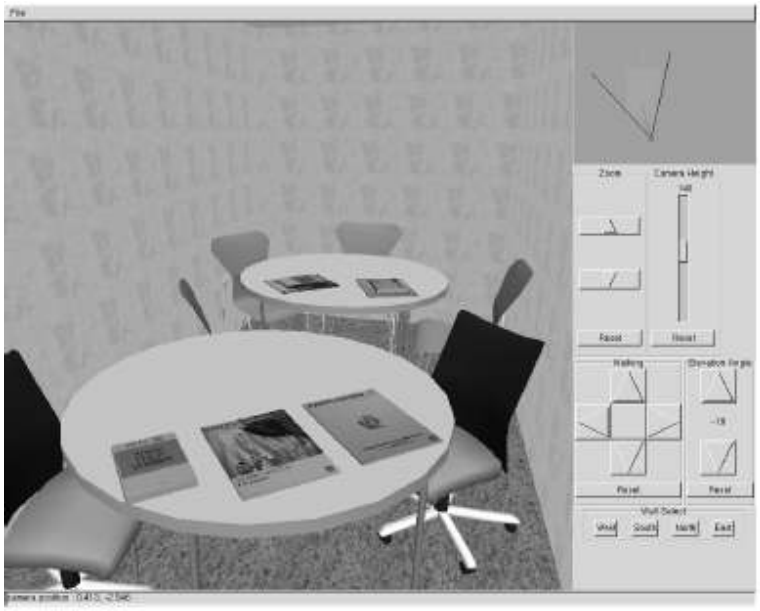


図 31 登録済みオブジェクトの3D表示例

4－7－6 AR 型インタフェースのための屋内位置検出（光学方式）

（1）はじめに

ここでは、複数台のビデオカメラ映像を利用して室内の人物の位置を検出する、光学方式での、AR 型インタフェースのための屋内位置検出手法に関して述べる。

（2）システム概要

本システムでの位置検出処理は、各人物の位置計算、各人間の識別、結果の送信という、大きく 3 つのステップからなる。

各人物の位置計算には、ビデオカメラ映像の画像処理を行うカメラノードを利用する。カメラノードで撮影された映像から、カメラノードから見て人物がどの角度にいるかを計算することが出来、カメラノードと人物の位置を通る直線が決まる。複数のカメラノードを利用してこのような直線が複数決まると、人物の位置はこれらの直線の交わる点として求めることが出来る。しかし、人物が複数いる場合には、位置が一意に決定できない場合も生ずる。本方式で位置計算をする限り、根本的にこの問題を解決することは難しいが、観測点（カメラノード）を増やすことである程度はこの問題に対処可能である。

人物の位置が確定すれば、次のステップは人物の識別処理である。本システムでは人物の色情報から個人識別を行うが、カメラ映像だけで人物の識別を行うのは困難である。そこで、被追跡者が個人識別のための何かしらのデバイスを所持している場合にはその識別情報を読みとり、以後その個人を保持しながら位置追跡を行い、個人の識別情報が得られない場合にも識別情報なしで追跡を行う。個人識別のためのデバイスは、識別カードや RFID といった安価なものでも構わない。本システムでは、各被追跡者に対して各センサーノードがローカルタグとい

う識別子を付けて、更にそのローカルタグの組み合わせを取り、その組み合わせを利用して被追跡者の識別を行う。こうすることにより、あるセンサーノードが間違ったローカルタグを付与した場合にも、それ以外のセンサーノードが正しいローカルタグを付与していれば間違いを訂正することができる。

個人識別のためのタグが求められたら、最後にクライアントノードへ、各被追跡者の識別情報及び位置情報を送信する。

(3)実証的評価

今回構築したパイロットシステムでは、残念ながら複数の人間の位置追跡ができなかった。これは、カメラ画像において複数の人物が重なってしまった場合、分離してそれぞれに対する観測角度を測ることが出来なかったことに起因する。しかし、人物の移動速度や前の位置などといった特徴値を利用すれば、さらに安定した識別を行うことができると考えられる。

4－8 サーバノードシステムの研究開発

4－8－1 研究開発内容

サーバノードシステムは、ユビキタス環境をバックエンドで支える、大量の計算資源と通信資源を有するインフラシステムである。セキュアハードウェアの研究開発と連携し、そこで研究開発されたセキュアチップのセキュア基盤のバックエンドとして動作するものを研究開発した。

また、ユビキタスコンピューティング環境下では、その特徴を生かした新たな応用分野が数多く存在することから、それらを裏で支える基盤サーバ群、ユビキタス情報配信サーバについて研究開発を行った。

各テーマの研究開発内容は以下の通りである。

(1)サーバノードとは、ユビキタスコンピューティング環境を裏で支える基盤サーバ群を含む。

基盤サーバに必要な機能として、色々な物や場所に付けられたIDを解決する機能の研究開発を実施した。本機能により、ユビキタスコンピューティング環境下での物や場所の情報の格納先を、全てのユーザがシームレスに取得することが可能となる。更に、物や場所の情報を格納・配信するユビキタス情報配信サーバ機能についても研究開発を実施した。

(2)サーバノードは、以下の機能を提供する。

- CA 局や鍵配布サーバを含むPKI(公開鍵インフラストラクチャ)機能
- 電子マネーや電子チケットの決済機能
- 価値情報の発行機能
- デジタルコンテンツの発行機能

ユビキタスネットワーキング環境下において重要なセキュリティ機能の研究開発を実施した。更に電子的価値情報を安全に記録、配信するコンテンツプロバイド機能の研究開発を実施した。

(3)サーバノードも悪意ある攻撃から守るためにハードウェアに一定の耐タンパー性を持たせる。

セキュアチップと連携した、セキュアプロトコルの研究開発およびサーバノードへの実装を行った。

4－8－2 ネットワーク型ユビキタス情報配信アーキテクチャ

(1)基盤アーキテクチャ

本研究開発では、現実世界のモノの個体識別情報に基いて情報配信を行うための基盤システムの仕組みを提案し、大量かつ多様な機器が接続された環境下において、状況に応じた適切な情報を配信できる基盤アーキテクチャの構築を行った(図 32)。本アーキテクチャでは、以下のノード群が連携することにより情報配信を行う。

- 個体識別用タグ:光学タグや無線タグなど、現実世界のモノとそれを個体識別するための情報を結びつける小型タグである。
- ユビキタス端末:ユビキタスネットワークに接続され、個体識別用タグを介して様々なチャネルから現実世界の環境情報を受信できるユーザ端末である。ユーザはユビキタス端末によりユビキタス基盤サーバ、情報配信サーバへアクセスすることで、それぞれの状況に応じた配信情報を取得できる。
- ユビキタス基盤サーバ:現実世界のモノの個体識別情報に基づいて、適切な情報配信サーバへの誘導を行うサーバである。個体識別情報と配信情報とのマッピングデータを管理するオープンなデータベースシステムである。
- 情報配信サーバ:現実世界のモノに関連した情報を配信するサーバである。

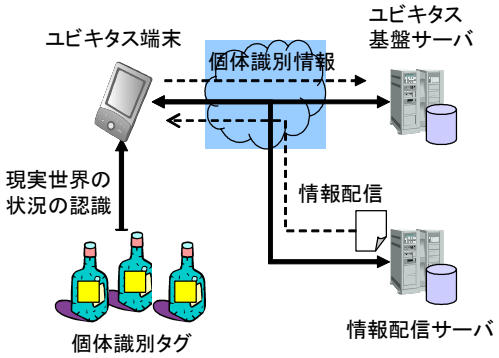


図 32 ユビキタス情報配信アーキテクチャ

(2)セキュリティ

現実世界の状況に基づいた情報配信では、人間の行動や嗜好分析などのプライバシーの問題、サイバー攻撃の現実世界への影響などの懸念から、セキュリティが大きな課題の 1 つであった。本アーキテクチャでは、利用権が格納された耐タンパチップを利用して各ノード間で暗号認証セションを構築することで、個体識別情報や配信される情報へのアクセスを制御できる仕組みを確立した。

(3)本アーキテクチャの成果

本研究開発の成果を以下に示す。

- 現実世界の情報をバーチャルなネットワークシステムに取り込み、実世界環境の状況に応じた情報配信を実現する仕組みを構築できた。
- 異なる応用間での連携やドメインをまたいだ情報配信の基盤を構築できた。
- 多様な機器やネットワークを介してシームレスかつセキュアに情報配信を行うための仕組みを構築できた。

4－8－3 ユビキタス情報配信サービスサーバ

(1)コンテンツプロバイド機能

電子マネーや電子チケットの決済機能、電子的価値情報の発行機能およびデジタルコンテンツの発行機能として、コンテンツプロバイドシステムを構築した。電子的価値情報の標準化を行い、セキュアチップと連動したユビキタスネットワーキング環境下での安全な価値情報のやり取りを実現した(図 33)。

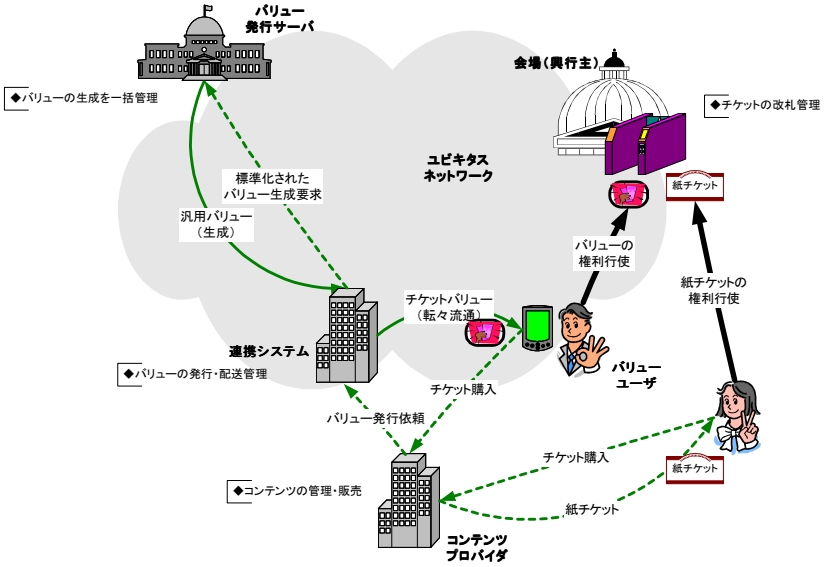


図 33 コンテンツプロバイド機能

(2)ユビキタス情報配信機能

ユビキタスコンピューティング環境を裏で支えるサーバ群として、ユビキタス情報配信システムを研究開発、実装した(図 34)。色々な物や場所の情報をいつでも、どこでも登録、参照可能な仕組みを確立し、多くのユビキタスアプリケーションで利用可能な基盤システムを構築できた。

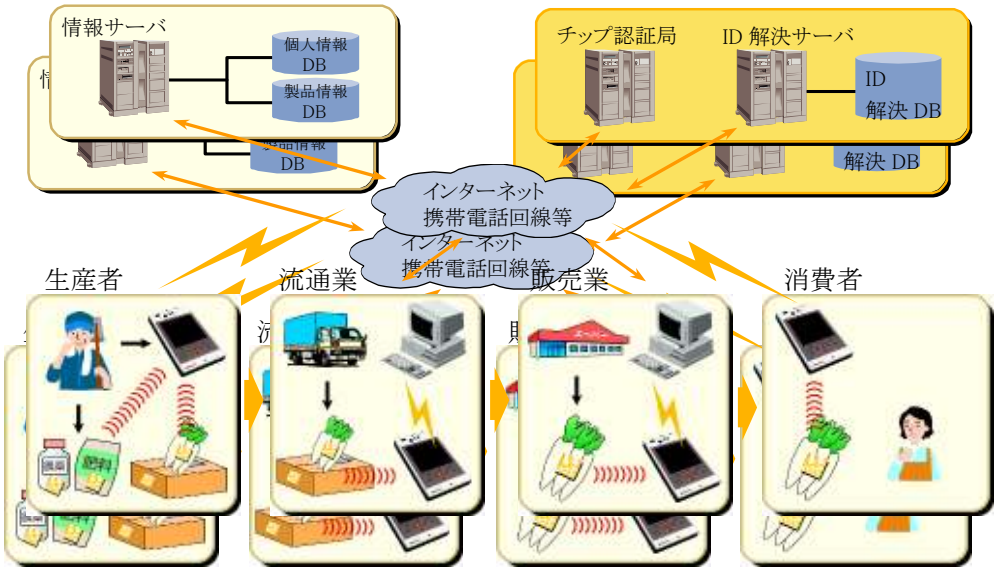


図 34　ユビキタス情報配信機能

4－8－4 ユビキタス情報配信用CA局

公開鍵暗号と PKI をベースとした暗号,認証のメカニズムを有し、社会のインフラを支えるユビキタス環境にふさわしい安全性と信頼性を実現するために、サーバノードシステムの一つとしてユビキタス情報配信用 CA 局を開発した(図 35)。この CA 局は、PKI で利用する公開鍵証明書を発行・管理する。また、失効した発行済証明書についても管理し、これらをもとにして証明書の有効・無効の問い合わせに対して検証結果を応答する証明書検証機能を提供する。この証明書検証機能を利用することで、情報家電やインターネットアプライアンスといった比較的乏しい計算機環境の上でも安全性と信頼性を享受できる。

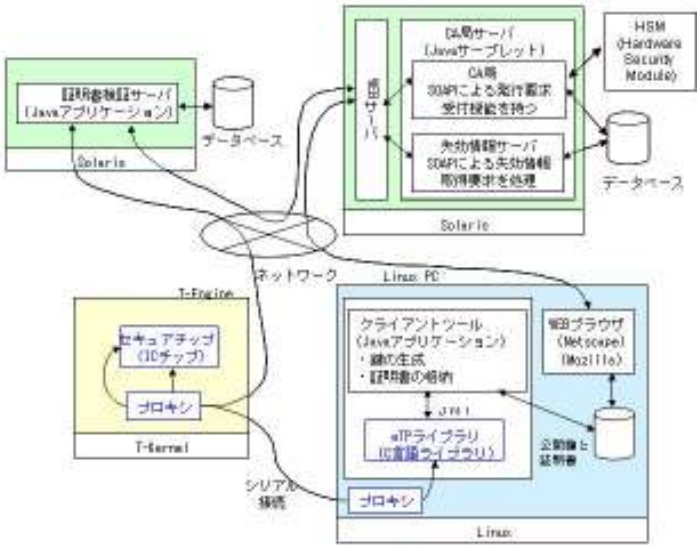


図 35　システム構成

CA 局における証明書の発行の際には、本研究のサブテーマ「カ．」で開発したセキュアハードウェアと連携し、安全の拠り所となる秘密情報の厳密な管理を非専門家でも簡便に行なえる。また、証明書検証機能には、処理の高速化を図るためのキャッシュ機構が組み込まれており、人間の振舞いや生活・社会を構成する事象に追従して応答するのに十分なリアルタイム性を持っている。更に、証明書への署名の際に必要となる CA 局の秘密鍵は、PKI における信頼の原点ともゆうべき最重要情報であるので、これを悪意ある攻撃から守るためにFIPS140-2 レベル3に適合した耐タンパ性を有するセキュリティ装置に格納した。これにより、不正アクセスを自動検出し、保管している秘密鍵の盗難を防ぐ。なお、ユビキタスコンピューティング環境中に存在する膨大なノードからの証明書検証要求に応えるため、証明書検証機能を複数サーバで分散処理可能とした。更に、CA 局の信頼モデルとしてツリーモデルを採用することで、証明書発行の分散処理によるスケーラビリティの確保、ならびに様々な運用形態への柔軟な対応を可能とすると共に、証明書検証における証明書経路構築を容易とし、証明書検証処理のスループットを確保した。

4－8－5 まとめ

サーバノード研究における各テーマの成果は以下の通りである。

(1)ユビキタスコンピューティング環境を裏で支える基盤サーバ群

全ての物や場所に ID(タグ)をつけ、現実世界をコンピュータが識別できるユビキタスコンピューティング環境を可能とする技術を確立した。更にそれらの技術を実装した基盤サーバ群を作成し数多くの実証実験および企業に提供した。

目標達成度は120％であった。

(2)CA 局や鍵配布サーバを含む PKI(公開鍵インフラストラクチャ)機能

情報家電やインターネットアプライアンスといった比較的乏しい計算機環境の上でも安全性と信頼性を確保したユビキタス情報配信用CA局を研究開発できた。分散処理手法を駆使して、ユビキタスネットワーキング環境におけるPKIの実現性に大きく寄与した。

目標達成度は100％であった。

(3)電子マネーや電子チケットの決済機能

ユビキタスネットワーキング環境で利用可能な電子マネー、電子チケットの方式を研究開発し、サーバノードに実装した。更に既存のインターネット上のサービスや紙媒体を用いたシステムから容易に移行できるような方式についても研究開発し、連携システムを構築した。

目標達成度は100％であった。

(4)価値情報、デジタルコンテンツの発行機能

電子的価値情報の標準化を行い、セキュアチップとの組み合わせにより、安全に発行する機

能を開発した。

目標達成度は100％であった。

(5)悪意ある攻撃から守るための耐タンパー性

利用権が格納された耐タンパチップを利用して各ノード間で暗号認証セションを構築することで、個体識別情報や配信される情報へのアクセスを制御できる仕組みを確立できた。

目標達成度は100％であった。

4－9 総括

4－1～4－8で報告したとおり、本研究開発における当初の最終目標の各項目については、達成することができた。更に、一部の項目に関する研究成果については、社外にリリースして、実用化されるものも出てきており、当初の目標以上の成果を達成しているということができる。例えば、セキュア・ユビキタス VPN、組込リアルタイムカーネル、組込リアルタイム拡張カーネル、Java 言語実行環境、セキュアハードウェアやその通信プロトコル、ユーザノードなどが挙げられる。更にこれらの成果は、様々な応用に適用した検証も経ることができた。従って、技術的研究成果としては、総括すれば、全体として当初の目標以上の成果をあげることができたといえる。今後、研究期間終了後は、この成果を実用化のために普及させることに全力を挙げたい。

5 参考資料・参考文献

5－1 研究発表・講演等一覧

5－1－1 平成17年度

研究論文（査読有）

1. 西山智，渡辺伸吾，山田満，越塚登，坂村健：「既存ルータ混在環境におけるモバイルIP高速ハンドオーバー方式」，情報処理学会論文誌,第47巻，第2号，pp. 279～290, 2006年2月.

収録論文（招待論文・基調論文）

1. Ken Sakamura: “T-Engine: The Open Platform for the Ubiquitous Computing Age”, in Proc. A-SSCC (IEEE Asian Solid-State Circuits Conference) 2005, pp. 3-6, 2005, *Keynote Paper*.
2. Ken Sakamura: “uID Architecture: an Open Foundation for Ubiquitous Computing”, in Proc. The Vision and Strategy of Ubiquitous Society, pp. 55-78, 2005, *Keynote Paper*.
3. Ken Sakamura and Noboru Koshizuka: “Ubiquitous Computing Technologies for Ubiquitous Learning”, in Proc. 3rd IEEE International Workshop on Wireless and Mobile Technologies in Education, Nov. 2005, Tokushima, pp. 11～18, *Keynote Paper*.
4. Noboru Koshizuka: “Ubiquitous ID Project”, the 8th International Conference on Advanced Communication Technologies (ICACT 2006), IEEE Communications Society, Feb. 2006, *Keynote Speech*.
5. Noboru Koshizuka: “Secure ID Tag and its Application”, in Proc. 11th German-Japanese Symposium “Security, Privacy and Safety in the Information Society”, 2005, Tokyo（招待論文・Extended Abstract）.
6. 坂村健：「情報化と建築・都市・環境」,日本建築学会 総合論文誌，第4号,情報化の視点からみた建築・都市のフロンティア, pp. 19～22, 2006年2月.（招待論文）
7. 越塚登，坂村健：「食の安全・安心を実現するためのユビキタスコンピューティング技術」，電子情報通信学会誌，Vol. 88, No. 5, 2005年5月，pp. 349～354.（招待論文）
8. 越塚登：「ユビキタス情報社会基盤のユニバーサルデザイン」，2006年電子情報通信学会総合大会・パネル討論「IT が拓く近未来の福祉情報システム」，2006年3月（招待論文）.
9. 越塚登：「ユビキタス ID 技術による食品情報基盤システム」，電気学会C部門大会・企画セッション，2005年9月7日（招待論文）.

10. 越塚登:「ユビキタスID技術:ユビキタスIDセンターの活動とその技術」, 日本包装学会 第14回年次大会研究発表会予稿集, 2005年7月, pp. 54〜58(特別招待論文).

収録論文(一般)

1. 別所正博, 小林真輔, 越塚登, 坂村健:「状況情報の形式的記述の可能な位置モデルに基づくヒューマンナビゲーションのための経路生成手法」, 情報処理学会研究報告, 「モバイルコンピューティングとユビキタス通信」「ユビキタスコンピューティングシステム」, 2006-MBL-36 2006-UBI-10, pp. 97〜102, 2006年.
2. 加藤敦, 藤内俊一, 諸隈立志, 坂村健: 「UNP におけるネットワーク自動構築機能」, 情報処理学会研究報告, 2005-MBL-32 2005-UBI-7「モバイルコンピューティングとユビキタス通信」「ユビキタスコンピューティングシステム」, pp. 125〜132, 2005年.

著書等

1. 坂村健:「グローバルスタンダードと国家戦略」, 猪木武徳・北岡伸一・坂村健・松山巖 編集 日本の＜現代＞9, NTT出版, 2005年.
2. 坂村健, 越塚登:「ユビキタスが拓く食の安全」, 新山陽子編, 「解説:食品トレーサビリティ」, 昭和堂, 2005年, pp. 86〜99.(分担)

一般口頭発表

1. 越塚登:「ユビキタスIDで実現する食品とレーサビリティ」, 食品関連産業国際標準システム・食品トレーサビリティ協議会セミナー, 平成18年3月14日.
2. Noboru Koshizuka: “Ubiquitous ID Project”, ETRI, Daejeon, Korea, Feb. 20, 2006, Keynote Speech.
3. Noboru Koshizuka: “Ubiquitous ID Center”, ITU-T RFID Workshop, Feb. 2006, Geneva, Swiss.
4. Noboru Koshizuka: “Future Trend of Japanese RFID Technologies and Market”, ITU-T RFID Workshop, Feb. 2006, Geneva, Swiss.
5. 越塚登:「ユビキタスIDアーキテクチャ」, TRONSHOW 2006, 東京国際フォーラム, 2005年12月14〜16日.
6. 越塚登:「ユビキタスID技術が創る未来のICT基盤」, TRONSHOW 2006, 東京国際フォーラム, 2005年12月14〜16日.
7. 越塚登:「T-Kernel/T-Engine と ITRON の最新動向」, Embedded Technology 2005 チュートリアル, 2005年11月15日.
8. 越塚登:「Philosophy of NRFID Technologies and Application」, TSAG: Telecommunication Standard Advisory Group, ITU, Geneva, 2005年11月7日.

9. 越塚登:「基調講演:ユビキタスID技術の現状と展望―RFID やセンサネットワークによって自動認識されたコンテキストを使用した新しい情報サービス技術」, 第 51 回次世代センサセミナーシリーズ「認識」シリーズ No.1 -ID 認識-,次世代センサ協議会, 2005 年 11 月 2 日.
10. 越塚登:「Philosophy of NRFID Technologies and Application」, ASTAP(APT Standardization Program), オーストラリア・メルボルン, 2005 年 10 月 27 日.
11. 越塚登:「ユビキタス技術の最新動向」, 栃木県産業振興センター・ユビキタス技術者支援研修, 2005 年 9 月 28 日.
12. Noboru Koshizuka: "Secure ID Tag and its Application", in Proc. 11th German-Japanese Symposium "Security, Privacy and Safety in the Information Society", Sep. 14, 2005, Tokyo.
13. 越塚登:「ユビキタス ID 技術による食品情報基盤システム」、電気学会, 講演, 2005 年 9 月 7 日.
14. UID-AutoID Lab 合同シンポジウム, 2005 年 8 月 9 日.
15. Noboru Koshizuka: "Ubiquitous ID Technology and Pilot Projects", 2005 年第 2 回ユビキタス政府フォーラム, 韓国・光州市, 2005 年 7 月 7 日.
16. 越塚登:「ユビキタス ID 技術:ユビキタス ID センターの活動とその技術」、日本包装学会大会特別講演,2005 年 7 月 6 日.
17. 越塚登:「ユビキタス ID 技術の最新動向」, ESEC 組込みシステム開発技術展 2005, 東京ビッグサイト 2005 年 7 月 1 日.
18. 越塚登:「ユビキタス ID 技術の最新動向と具体的実用例」, ユビキタスネットワーキングフォーラム, 明治記念館, 2005 年 6 月 14 日.
19. Noboru Koshizuka: "Ubiquitous ID Technology and its Code Resolution Mechanism", 13th KRnet 2005: Korea Internet Conference, Seoul, Korea, June 29, 2005.
20. Noboru Koshizuka: "Active Tag Projects in YRP UNL", 2005 International RFID/Sensor Network Workshop, Seoul, Korea, June 10, 2005.

その他資料(一般記事)

1. 越塚登:「ユビキタスコンピューティング技術がつくる ICT の未来」, 地銀協月報, 2005 年 12 月号, pp. 2～8.
2. 越塚登:「ユビキタス ID センターとその活動」, ユビキタス社会の RFID タグ徹底解説, Electronic Journal 技術・ビジネス選書, 電子ジャーナル, 2005 年.
3. 越塚登:「農産物トレーサビリティ―ユビキタス ID 技術を使った実証実験事例」, 今月の農業, 第 49 巻, 第 8 号, 化学工業日報社, 2005 年 8 月, pp. 23～29.
4. 坂村健, 越塚登:「ユビキタスが拓く食の安全」, 新山陽子編, 「解説:食品トレーサビリティ」, 昭和堂, 2005 年, pp. 86～99.

5. 越塚登:「無線ICタグ普及の条件:標準プラットフォームを確立し、アクティブ型の実用化を後押し」, 日経 RFID テクノロジー, プロの眼, 2005 年 6 月号.

5－1－2 平成16年度

外国発表予稿等(査読有)

1. M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka, K. Sakamura: "TENeT: An Architecture for Distributed SmartCard", in Proceedings of the 2nd International Conference on Security in Pervasive Computing.
2. Lee Hoi Leong, Shinsuke Kobayashi, Noboru Koshizuka, Ken Sakamura: "CASIS: A Context-Aware Speech Interface System", in Proceedings of the International Conference of Intelligent User Interfaces (IUI 2005), ACM, Jan. 2005.
3. Shinsuke Kobayashi, et. al.: "T-Air: Low Power Wireless Sensor Network Platform for Ubiquitous Computing", in Proceedings of the 1st International Workshop on Networked Sensing Systems, June 2004.

収録論文(基調論文・招待論文)

1. 坂村健:「ユビキタス時代のシステム技術」, 映像情報メディア学会誌, Vol. 59, No. 1, pp. 27～32, 2004 年.(招待論文)
2. 越塚登:「ユビキタス ID センター」, 情報処理, 2004 年 6 月.(招待論文)
3. 越塚登, 坂村健:「ユビキタス ID 技術とその応用」, 電子情報通信学会誌, Vol. 87, No. 5, 2004 年 5 月, pp. 374～378.(招待論文)

収録論文(一般)

1. 小林真輔, 早川幹, 越塚登, 坂村健: 「T-Engine を用いた ISO18000-4 タグリーダライタのプロトタイプ設計」, 第 12 回 FPGA/PLD Design Conference ユーザープレゼンテーション論文集, pp. 79～84, 2005 年 1 月.
2. 小林真輔, 越塚登, 坂村健:「H. 263 デコーダを用いた『組込みソフトウェア開発プラットフォーム:T-Engine』の評価」, 情報処理学会 DA シンポジウム 2004, ポスターセッション, 2004 年 7 月.
3. 小林亜鈴, 上向俊晃, 井ノ上直己, 小池淳, 山田満, 坂村健:「統合PDA端末の開発(1)～端末実装」, 信学総大, 2005 年 3 月.
4. 松尾賢治, 橋本真幸, 小池淳, 山田満, 坂村健:「統合PDA端末の開発(2)～顔認証アプリケーションの実装と高速化」, 信学総大, 2005 年 3 月.
5. 服部元, 松本一則, 菅谷史昭, 小池淳, 山田満, 坂村健:「統合PDA端末の開発(3)～携帯端末のためのWebページ自動分割」, 信学総大, 2005 年 3 月.
6. 石川彰夫, 川田亮一, 小池淳, 山田満, 坂村健:「統合PDA端末の開発(4)～

3次元自由視点VoDシステムの実装」，信学総大, 2005 年 3 月.

7. 上向俊晃，小林亜鈴，井ノ上直己，小池淳，山田満，坂村健:「統合PDA端末の開発(5)～エラー耐性を強化した通信放送融合型データ配信システムの実装」，信学総大, 2005 年 3 月.
8. 加藤恒夫，河井恒，小池淳，山田満，坂村健:「統合PDA端末の開発(6)～分散型音声認証システムの実装」，信学総大, 2005 年 3 月.
9. 加藤 淳，藤内 俊一，諸隈 立志，坂村 健:「UNP:ユビキタス環境下における制御系ネットワークプロトコル」，情報処理学会ユビキタスコンピューティング研究会 第 7 回研究発表会, 2005 年 3 月.
10. 越塚登:「ユビキタス ID 技術とトレーサビリティ」，農業情報学会シンポジウム 2005 春 予稿集，農業情報学会, 2005 年, pp. 45～52.
11. 西山智，山田満，越塚登，坂村健，「ユビキタスサービスのためのエージェントプラットフォームの提案」，第 120 回情報処理学会 DPS 研究会(IPSJ SIG-DPS), 2004 年 11 月 4～5 日.
12. 渡辺伸吾，西山智，越塚登，坂村健:「既存ルータ混在環境におけるモバイル IP ハンドオーバ高速・高信頼化」，マルチメディア，分散，協調とモバイル(DICOMO2004)シンポジウム，情報処理学会, 2004 年 7 月.

学術解説等

1. 坂村健:「ユビキタス時代の半導体技術」，応用物理，第 73 巻，pp. 1155，2004 年.(招待論文)

著書等

1. 坂村健，竹村健一:「すべてのモノにコンピュータを，ユビキタス社会，始まる」，太陽企画出版, 2004 年.
2. 坂村健:「ユビキタス、TRONで出会う『どこでもコンピュータ』の時代へ」, NTT 出版, 2004 年.

一般口頭発表

1. 越塚登:「ユビキタスネットワークにおける GIS の活用」，GIS フォーラム，総務省、独立行政法人情報通信研究機構, 2005 年 2 月 16 日.
2. 越塚登:「ユビキタス ID センターにおける RFID への取り組み～実証実験を中心に～」，情報処理学会連続セミナー2004「IC タグ」, 2004 年 12 月 17 日.
3. 越塚登:「ユビキタス ID 技術」, TRONSHOW 2005, 12 月 9 日.
4. 越塚登:「トロン教育普及グループの活動」, TRONSHOW 2005, 12 月 8 日.
5. 徳田，越塚，下條，竹内，山田:「パネルセッション」，ユビキタスネットワークシンポジウム 2004, 11 月 30 日.
6. 越塚登:「基調講演:ユビキタスが拓く未来」，精密工学会 第 301 回講習会ユビ

キタスで変わる製造業:ヒット商品を産み出す組み込み OS, 11 月 16 日.
7. 越塚登:“Technologies and Activity of Ubiquitous ID Center”, SmartLabel Asia 2004, 11 月 11 日.
8. 越塚登:「T-Engine, ユビキタス ID 技術の最新動向」, 韓国 SYSKON(System Kernel Conference), 11 月 6 日, ソウル.
9. 越塚登:「ユビキタスが開く未来」, 栃木県ユビキタス講演会『ユビキタス・ネットワーク社会がやってくる』(10 月 8 日)
10. 越塚登:「ユビキタスと食:情報産業としての食品産業」, ユビキタス社会と地域振興:沖縄の可能性, 沖縄国際大学産業情報学部, 食のトレーサビリティシステムを広げる会(9 月 25 日)
11. 越塚登:「T-Engine とユビキタス ID 技術」, 第2回「ワイヤレス・センサー・ネットワーク社会に向けたナノメートル CMOS システムとその要素技術の研究」に関する先導的研究開発委員会, 日本学術振興会, 2004 年 9 月 7 日.
12. 越塚登:“Ubiquitous Network: An Introduction to the Activity of Ubiquitous ID Center”, 第三回日中韓情報通信大臣会合ビジネスフォーラム(7 月 27 日).
13. 越塚登:「ユビキタス ID 技術の最新動向―実用化に向けた具体的事例」, ESEC 2004, 2004 年 7 月 8 日.
14. 越塚登:「T-Engine, ユビキタス ID 技術の最新動向」, Networld+Interop 東京 2004, 2004 年 7 月 2 日.
15. 越塚登:「組込みリアルタイムプラットフォーム T-Engine・T-Kernel」, Networld+Interop 東京 2004, 2004 年 6 月 30 日.
16. 越塚登:「ユビキタス ID の最新動向―RFID を使ったユビキタスネットワークの実現にむけて」, 情報通信月間講演会(中国), 2004 年 6 月 25 日.

その他資料(一般記事)

1. 坂村健:「自律的移動支援プロジェクトから『ユビキタス国土』へ」, 都市政策 季刊 第 117 号, 2004 年 10 月号, pp. 20～30.
2. 坂村健:「ユビキタス・コンピューティング技術」, 建築雑誌, pp. 8～9, 2005 年.
3. 坂村健:「ユビキタス社会の現状・展望 ～ 産・官・学の進むべき方向 ～」, ESP (Economy Society Policy), January 2005, 特集:IT 化進展の検証・展望, pp. 42～45, 2004 年.
4. 坂村健:「ユビキタス社会における産業と物流」, 港湾, pp. 21～23, 2005 年.
5. 越塚登:NEC IT Square, UID レポート連載、第1回:ユビキタス ID センター (http://www.blwisdom.com/uid/)
6. 越塚登:NEC IT Square, UID レポート連載、第2回:組込み技術の先にあるユビキタス(http://www.blwisdom.com/uid/)
7. 越塚登:NEC IT Square, UID レポート連載、第3回:食品トレーサビリティ実証実

験(1)実験の狙いと方法(http://www.blwisdom.com/uid/)

8. 越塚登:NEC IT Square, UID レポート連載、第4回:食品トレーサビリティ実証実験(2)実験結果(http://www.blwisdom.com/uid/)
9. 越塚登:NEC IT Square, UID レポート連載、第5回:自律的移動支援プロジェクト(http://www.blwisdom.com/uid/)
10. 越塚登:NEC IT Square, UID レポート連載、第6回:ユビキタス ID 技術(1)ユビキタス ID アーキテクチャ(http://www.blwisdom.com/uid/)
11. 越塚登:NEC IT Square, UID レポート連載、第7回:ユビキタス ID 技術(2)ucode と ucode タグ、ユビキタスコミュニケーター(http://www.blwisdom.com/uid/)
12. 越塚登:NEC IT Square, UID レポート連載、第8回:ユビキタスセキュリティー(http://www.blwisdom.com/uid/)
13. 越塚登:NEC IT Square, UID レポート連載、第9回:TRONSHOW2005 誰でもできるユビキタス(1)(http://www.blwisdom.com/uid/)
14. 越塚登:NEC IT Square, UID レポート連載、第 10 回:TRONSHOW2005 誰でもできるユビキタス(2)(http://www.blwisdom.com/uid/)
15. 越塚登:NEC IT Square, UID レポート連載、第11回:ユビキタスとユニバーサル(http://www.blwisdom.com/uid/)
16. 越塚登:NEC IT Square, UID レポート連載、第12回:ユビキタスと循環型社会(http://www.blwisdom.com/uid/)
17. 越塚登:「ユビキタスが拓く食の安全:食品トレーサビリティを可能としたユビキタス技術は食を豊かにする」, CLINICIAN, Vol. 52, No. 536, pp. 40〜45.
18. D. E. カラー, H. マルダー:「世界を見守る賢いセンサー網」, 日経サイエンス, 第 34 巻, 第 9 号, pp. 66〜75.(翻訳監修)
19. 越塚登:「センサーネットワークには標準化が必要だ」, 日経サイエンス, 第34巻, 第 9 号, p. 73.
20. 越塚登, 峯岸康史:「ユビキタスIDセンターが描くICタグ普及のシナリオ」, 無線 IC タグ導入ガイド, 日経 BP, 2004.
21. 越塚登:「ユビキタス ID センターの技術と活動」, RFID の開発と応用Ⅱ, シーエムシー出版, 2004.
22. 越塚登:「文化と IT」, 異文化, 法政大学国際文化学部, 2004 年 5 月号, pp. 11〜15.
23. 越塚登:「ユビキタスID技術の詳細と適用事例」, Computer & Network, LAN, オーム社, 2004 年 5 月号.

5−1−3 平成15年度

研究論文(査読有)

1. Ken Sakamura and Noboru Koshizuka:“Technologies for Computing Everywhere

Environments”, Korea Information Processing Society Review, July, 2003, pp. 11～22.（招待論文）

収録論文（招待論文・基調論文）

1. Ken Sakamura: “T-Engine－The Open Development Platform fro Ubiquitous Computing”, サイバーアシストコンソーシアム第2回国際シンポジウム, pp. 1～15, 2003.（基調論文）
2. 坂村健,「ディジタルミュージアムからユビキタスミュージアムへ」, 人工知能学会誌 5 月号, Vol. 18, No. 3, pp. 259～266, 2003 年.（招待論文）
3. Ken Sakamura: “Ucode Architecture and RFID”, in Proc. 2004 RFID International Symposium (Korea), 2004 年, pp. 3～24.（基調論文）
4. 坂村健:「ユビキタス・コンピューティング社会にむけて」, シリコンシーベルトサミット 2004 福岡, 2004 年, pp. 3～10.（基調論文）
5. Ken Sakamura: “Ubiquitous Computing: Making It a Reality”, ITU TELECOM World2003, Geneva Palexpo, Geneva, Oct. 13, 2003, pp. 1～9.（招待論文）
6. 坂村健:「ユビキタスコンピューテング環境の実現にむけて」, Microwave Workshop and Exhibition (MWE 2003), 2003 年.（基調論文）
7. Shingo Watanabe, Satoshi Nishiyama, Noboru Koshizuka, Ken Sakamura: “Location Detection Method for Everyday Objects Using Contactless IC Cards”, Microwave Workshop and Exhibition (MWE 2003), Nov. 2003, pp. 245～250.（招待論文）
8. Katsunori SHINDO, Noboru Koshizuka, and Ken Sakamura: “Ubiquitous Digital Museum Using Contactless Smart Cards”, Microwave Workshop and Exhibition (MWE 2003), Nov. 2003, pp. 251～256.（招待論文）
9. Noboru Koshizuka and Ken Sakamura: “T-Engine Project: The Open Platform Project for Ubiquitous Computing”, in Proc. First International Conference on Ubiquitous Computing (ICUC 2003), pp. 185-190, 2003.（招待論文）
10. Ken Sakamura and Noboru Koshizuka: “T-Engine: The Open, Real-time Embedded-Systems Platform for Ubiquitous Computing”, in Proceedings of the 2003 Symposium on VLSI Circuits, June 2003.（基調論文）

収録論文（一般）

1. 李海量, 越塚登, 坂村健:「コンテキスト情報を利用して曖昧な音声入力の意味解決をする音声ユーザインタフェースシステム」, 第 66 回情報処理学会全国大会, 2004 年 3 月.
2. 松沢敬一, 新堂克徳, 越塚登, 坂村健:「管理者による視認型認証を支援する IC カードを用いた本人確認システム」, 第 66 回情報処理学会全国大会, 2004

年 3 月.

3. 別所正博, 鵜坂智則, 越塚登, 坂村健:「ユビキタス環境における緊急避難経路提示システムの提案」, 第 66 回情報処理学会全国大会, 2004 年 3 月.
4. 佐藤, 豊山, 田中, 越塚登, 坂村健:「組込みシステムのプラットフォームの標準化によるソフトウェア資産の再利用性向上の評価」, 第 66 回情報処理学会全国大会, 2004 年 3 月.
5. 渡辺伸吾, 西山智, 服部元, 小野智弘, 越塚登, 坂村健:「既存ルータ混在環境におけるモバイル IP ハンドオーバの高速・高信頼化の提案」, 第 66 回情報処理学会全国大会, 2004 年 3 月.
6. 宮崎真悟, 石川千秋, 鵜坂智則, 小俣三郎, 越塚登, 坂村健:「組込み機器に秘密共有機能を提供する SIM カード型セキュアチップの開発」, 第 66 回情報処理学会全国大会, 2004 年 3 月.
7. 西山智, 渡辺伸吾, 服部元, 小野智弘, 越塚登, 坂村健:「モバイル端末における応用の要求に応じた通信メディアの使い分け方式の提案」, 第 66 回情報処理学会全国大会, 2004 年 3 月.
8. 渡辺伸吾, 西山智, 服部元, 小野智弘, 越塚登, 坂村健:「ユビキタス環境のための非接触 IC カードを使用した位置検出方式の実装と評価」, FITS2003 第二回情報科学技術フォーラム研究報告, 2003 年 9 月.
9. 西山智, 渡辺伸吾, 服部元, 小野智弘, 越塚登, 坂村健:「屋内用センサネットワーク用ネットワークプロトコルの実装」, FITS2003 第二回情報科学技術フォーラム研究報告, 2003 年 9 月.
10. 渡辺伸吾, 西山智, 服部元, 小野智弘, 越塚登, 坂村健:「ユビキタス環境のための非接触IC カードを使用した位置検出方式」, 第一回ユビキタスコンピューティングシステム研究会, 情報処理学会, 2003.

学術解説等

1. 坂村健:「解説:特集『電脳都市』2」, 計測と制御1, 第 43 巻, 2004 年, pp. 52～58.（招待論文）

一般口頭発表

1. 坂村健, 越塚登:「ユビキタスコンピューティングの世界で, 何ができるのか？」ユビキタス ID セミナー, ユビキタス ID センター・日経BP社, 2003 年 4 月.
2. 坂村健:OA 学会, 中央学院大学, 2003 年 4 月.
3. 坂村健:RSA Conference2003 Japan, 東京国際フォーラム, 2003 年 6 月.
4. 坂村健:ACM 日本支部総会および特別講演会, 東京理科大学森戸記念館, 2003 年 7 月.
5. 坂村健:TRON プロジェクトの 20 年, 安田講堂, 2003 年 7 月.

6. 坂村健:建築学会(1400-1450), 中部大学, 2003 年 9 月.
7. 坂村健:Asian Enterprise Open Source Conference, 2003, Singapore, October, 2003.
8. 坂村健:データベース研究会, 日本科学未来館, 2003 年 11 月.
9. 坂村健:第一回アジアユビキタス会議基調講演, パークタワーホール, 2003 年 12 月.
10. 坂村健:TRONSHOW2004 基調講演, 東京国際フォーラム, 2003 年 12 月.
11. 坂村健:第 2 回武田シンポジウム, 東大武田ホール (6F), 2004 年 2 月.
12. 越塚登:「ユビキタス ID 技術」, 電子情報通信学会 QoS ワークショップチュートリアル, 2004 年 2 月.
13. 越塚登:「T-Engineとユビキタス ID」, 日本学術会議シリコン超集積化システム第 165 委員会, 2004 年 1 月.
14. 越塚登:「T-Engine とユビキタス ID」, 第 6 回 CEST 技術セミナー「TRON プロジェクトの最前線: T-Engine とユビキタス ID」, 組込みシステム開発技術研究会 (CEST), 豊橋商工会議所, 2003 年 10 月
15. 越塚登:「ユビキタスIDの最新動向」, 日経BP・RFIDユーザーフォーラムSpring 2004 “無線ICタグ実用化の幕開け”, 2004 年 3 月.
16. 越塚登:「ユビキタス ID 技術を用いた青果物トレーサビリティシステムの構築」, 食品トレーサビリティシステム普及推進セミナー, 2004 年 3 月.
17. 越塚登:「T-Engine とユビキタス ID プロジェクト-ユビキタス社会を目指して」, オープンソリューションパートナーズグループ (OSPG) 講演会, 2004 年 2 月.
18. 越塚, 他:「使ってみよう T-Engine」, TRONSHOW 2004, 2003 年 12 月.
19. 越塚, 他:「TRON ポータビリティーWG」, TRONSHOW 2004, 2003 年 12 月.
20. 越塚登:「T-Engine フォーラムの活動」, TRONSHOW 2004, 2003 年 12 月.
21. 越塚登:「T-Kernel のオープン化」, TRONSHOW 2004, 2003 年 12 月.
22. 越塚登:「ユビキタスコミュニケーター」, TRONSHOW 2004, 2003 年 12 月.
23. 越塚登:「ユビキタス ID 技術－次世代の情報技術基盤の確立に向けて－」,(社) 自動車技術会中部支部・技術講演会「21 世紀を担う情報・通信技術と自動車」, 名古屋, 2003 年 11 月.
24. 越塚登:「ユビキタスID技術とその応用事例」, まちと人のセキュリティーシンポジウム 2003, (社) 日本能率協会, 東京ビッグサイト, 2003 年 11 月.
25. 越塚登, 豊山祐一:「T-Engine とユビキタス ID 技術の最新動向－T-Engine Project－」, Embedded Technology 2002 組込み総合技術展特別講演, 2003 年 11 月.
26. 越塚, 他:「T-Engine セミナー」, Embedded Technology 2002 組込み総合技術展チュートリアル, 2003 年 11 月.
27. 越塚登:「ユビキタスコンピューティングの実現にむけて」, 日本フォーム印刷工

業連合会・技術セミナー, 2003 年 11 月.

28. 越塚登:「ユビキタスIDセンターの活動～ユビキタス環境の実現にむけて～」, 第 55 回テレコム技術情報セミナー, (財)テレコム先端技術研究支援センター, 2003 年 10 月.
29. 越塚登:「ユビキタスコンピューティングと物流システムーユビキタス ID 技術が創る未来ー」, ロジスティックスフォーラム関西 2003, 大阪, 2003 年 10 月.
30. 坂村健, 越塚登, 西山智:「ユビキタスコンピューティング環境を実現する基盤ネットワークプロトコルの研究開発」, 平成 15 年度通信・放送機構(TAO)研究発表会.
31. 越塚登:「トロンが実現するどこでもコンピュータの世界」, 滋賀県高度情報化推進会議, 2003 年 7 月.
32. 越塚登, 他:「ユビキタスコンピューティングの基礎技術『T-Engine』と『ユビキタス ID』の現状と展望」, 第 6 回組込みシステム 開発技術展 (ESEC: Embedded Systems Expo. & Conference in Tokyo 2003), 2003 年 7 月, 東京ビッグサイト.
33. 越塚登:「ユビキタス ID:技術的内容と方向性」, 日経コンピューター・セミナー, 「IC タグ」の全貌, 最新技術動向から応用まで, 日経BP社, 2003 年 5 月.

※ その他多数

その他資料(一般記事)

1. 坂村健:「環境とデザイン-05 情報環境から建築を考える」, 新建築 78, pp. 052～055, 2003.
2. 坂村健:「組み込みエンジニアへおくる最新情報, ユビキタス・コンピューティングにおける T-Engine の動向」, EPO (Electronics Product Digest), pp. 4～5, 2003.
3. 坂村健:「総特集 IT で医療が変わる:ユビキタス・コンピューティング実現のために」, 月刊 新医療, No.344, pp. 52～56, 2003.
4. 坂村健:「特集 ユビキタス・コンピューティングと物流システム」, ロジスティクスシステム, 12 (6), pp. 6～9, 2003.
5. 坂村健:「正論 開かれた土俵こそが相互繁栄の道 歴史的な MS とトロンの提携劇」, 産経新聞(10 月 3 日), p 13, 2003.
6. 越塚登:「ユビキタス ID センターとその活動」,「ユビキタス社会の RFID 徹底解説」, 電子ジャーナル, 2003 年.
7. 坂村健,「日本発ユビキタスの目標は, 監視社会ではなく究極の便利社会である」, 日本の論点 2004, pp. 412～417, 2003.
8. 越塚登:「ユビキタスコンピューティングとトロン」, 情報通信 i-Net, 第 7 号, 数研出版, 2003 年 6 月.
9. 坂村健,:「大事に育てたい未来技術ユビキタス, 社会的合意と環境整備を急げ,

産経新聞 (5 月 24 日), p. 12, 2003.

10. 坂村健,越塚登:「ユビキタス ID センターの取り組み」, 月刊バーコード, vol. 16, no. 5, 日本工業出版, 2003 年 4 月, pp. 15～20.

※ その他多数

5－1－4 平成14年度

外国発表予稿等(査読有)

1. Katsunori Shindo, Noboru Koshizuka, and Ken Sakamura: “Ubiquitous Information System for Digital Museum using Smart Cards”, in Proceedings of the SSGRR, Jan., 2003.
2. Katsunori Shindo, Noboru Koshizuka, and Ken Sakamura: “Large-scale Ubiquitous Information System for Digital Museum”, in Proceedings of the 21st IASTED, Feb., 2003.

収録論文(一般)

1. 太田陽基, 中尾康二, 田中俊昭, 西山智, 越塚登, 坂村健:「非接触 IC カードにおける X.509 証明書のコンパクト化に関する一考察」, 電子情報通信学会平成 15 年総合大会, A-7-29.
2. 西山智, 渡辺伸吾, 服部元, 小野智弘, 越塚登, 坂村健:「ユビキタスサービスのための屋内センサーネットワークの提案」,情報処理学会第 65 回全国大会, 3H-2, pp.3-247～248.
3. 渡辺伸吾, 西山智, 服部元, 小野智弘, 越塚登, 坂村健:「ユビキタス環境のための非接触 IC カードを使用した位置検出方式の提案」, 情報処理学会第 65 回全国大会, 3H-1, pp.3-245～246.

5－1－5 平成13年度

一般口頭発表

1. 坂村健,「ユビキタスネットワーキングを実現する基盤プロトコルの研究開発」, YRPユビキタスネットワーキング研究所開所式記念講演(2002 年 3 月 28 日).
   本研究所研究内容, 研究方針に関しての講演.