平成１３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

株式会社横須賀テレコムリサーチパーク
ユビキタスネットワーキング研究所
（研究代表者：坂村　健）

# 目次

参考資料，参考文献

（添付資料）

1　研究発表，講演，文献等一覧　（←研究開発実績報告書を参考に記載）

# 第一章
# 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．

# 第二章
# 研究開発分野の現状

身の回りのあらゆるものにコンピュータをうめこみ,それらが互いに協調動作することによって高い機能とサービスを提供する情報通信環境は，Ubiquitous Computing という言葉で代表され，1980 年代～1990 年代にかけて，日米で提唱された.

米国では Xerox 社 Palo Alto Research Center (PARC) の Mark Weiser 博士が，自らの研究グループによるユビキタスコンピューティングの研究を発表した，1991 年 9 月の Scientific American 誌の論文"The Computer for the 21st Century"が，最初にユビキタスコンピューティングのコンセプトを提案したもので,これは特にユーザインタフェースの研究者に対して大きな影響を与えた．というのも,当時のユーザインタフェースの研究は,コンピュータグラフィックスを活用した GUI の研究や,マルチメディアを使ったインタフェース研究が主流であり,どちらもデスクトップのコンピュータと相対して対話するものであった．ところが Weiser 博士は，非デスクトップのユーザインタフェースの重要性を説き，むしろそちらの方が，通常の人間生活の中で接する頻度の大きいインタフェースであることを述べた．まだ当時は，新しい技術が開発されたというよりは，当時の技術を利用してユビキタスコンピューティングが目指す姿をとりあえず構築し,そのユーザインタフェース上の有効性を検証するものであった．日本では，本研究課題の研究代表者である坂村健が，1989 年に超機能分散システム (HFDS: Highly Functionally Distributed System)としてこのユビキタスコンピューティングのコンセプトを提唱した．PARC の研究よりも，より分散システム技術に比重が置かれている点が特徴である.

## 2.1 Xerox PARC の UbiComp [1991～]

Xerox Palo Alto Research Center (PARC) では，Mark Weiser 博士を中心としたグループによって，Ubiquitous Computing (UbiComp) の研究が行われていた．UbiComp は，人間の生活のいたるところで,人間の目には触れないコンピュータを利用する環境の構築を目指している．UbiComp は，以下の様なシナリオの実現を目指していた.

- オフィスビルの従業員は，常にアクティブバッヂを身につける.
- 正当なアクティブバッヂを身に着けている時しか開かない自動ドア.
- 名前で挨拶してくれる部屋.
- どこに居ても居場所にかかってくる電話.

- 従業員がどこにいるか把握している受付.

このシナリオを実現することに焦点が置かれており,それを実現する上で必要な通信プロトコルや，リアルタイム性，セキュリティー，運用や利用の容易性，更にはコンパクトな実現方法などには，ほとんど取り組まれていない.あくまでも技術的な課題を抽出するためのフィージビリティー研究に近い.

## 2.2 RANK Xerox EuroPARC

RANK Xerox EuroPARC でも，Pierre Wellner 博士を中心とした研究グループが,早い時期からユビキタスコンピューティング研究に取り組んできた.代表的な研究は DigitalDesk といわれるもので，実物の机をコンピュータのモニタのように使ってコンピュータと対話する技術である.従来の GUI がデスクトップを模擬してコンピュータの画面を構築していたケースと逆に,本物のデスクトップをコンピュータとの対話の場に使うものである.これはユビキタスコンピューティング

環境の一部として使うことはできるものの,ユビキタスコンピューティング研究の中でも,ユーザインタフェース部分に限定されたミクロレベルの研究である.

## 2.3 MIT Media Lab.

MIT Media Lab.では，TTT（Thing That Think）という研究プロジェクトがあり,ユビキタスコンピューティング環境への研究に取り組んでいる.代表的な研究として，コンピュータを埋め込んだインテリジェントなおもちゃであるとか，洋服を「着る」感覚で常に携帯する「Wearable Computer」の研究がある. TTT の上位コンセプトとして「Tangible Bit（触れるビット)」というものがあり，コンピュータやネットワーク上の仮想的なデジタル情報に対して,実世界のモノを通してアクセスするというコンセプトを実現するために,身の回りのものにコンピュータを埋め込んでいるのであって,我々がユビキタスコンピューティングで目指している目標と方向性が異なっている.

## 2.4 MIT AI Lab.

MIT AI Lab.では，SmartRoom という研究が行なわれている. 部屋の中にコンピュータを埋め込み,部屋が知的に振舞うようにすること

が目的である．ここは，人工知能の研究所であることから，研究の力点も，いかに部屋を「知的」に振舞わせるかという部分に重点がおかれており，あくまでも人工知能研究の一貫として取り組まれている．

## 2.5 IBM Pervasive Computing Project

IBM の Pervasive Computing Project では，ポスト PC 時代に向けた IBM 社の戦略の一環として進められているプロジェクトである．従来，大型計算機や PC を商品としてきた IBM 社が，情報家電といた非 PC 製品を商品化するために必要な技術開発をしており，本研究開発課題のような，基盤技術を扱うものではない．

## 2.6 US NIST Pervasive Computing Project

米国の NIST にも Pervasive Computing を扱うプロジェクトがある．ここの特徴は，現在ネットワーク型言語として広く使われている Java 言語の処理系をコンパクトかつ軽量化することや，Java にかわるよりコンパクトで実行効率の良いネットワーク言語の開発，またその上のミドルウェアなど，やはり製品改良に近いレベルの研究が行なわれており，本研究開発課題のような基盤性を有する研究ではない．

## 2.7 SONY CSL

国内では，SONY Computer Science Laboratory (CSL)の Interaction Laboratory の暦本氏らによって，"Augmented Interaction"の研究がなされている．ここの研究も研究室レベルの小規模なものであること，また，あくまでも情報環境との Interaction を研究しており，我々のように，基盤プロトコルに関する研究開発を行っているわけではない．

## 2.8 UCB／Endeavour ［1999～2002］

カリフォルニア大学バークレー校(UCB)の電気電子および計算機科学科では，Randy H. Katz 教授を中心とした多数のグループによって，コンピュータが内蔵された多種多様な情報機器(大型コンピュータから，家電製品，さらには超小型センサーまで）を相互接続することにより，あらゆる種類の情報を収集し，さらにその情報を即時に引き出したり，情報に従って最適な対応を自動的に行ったりできるような次世代コンピュータネットワークを構築するのに必要となる要素技術の研究・開発が進められている．これにより，例えば家に取り付けら

れた情報収集機器により,その家の住人の生活パターンを自動的に認識し，その収集された情報に従って各機器が動作する Smart House 等が実現できる．このために,

- 超小型センサー
- クラスターベースの大規模計算処理及びメッセージ処理システム
- スケーラブル，メインテナンスフリーのストレージサーバーシステム
- ネットワーク上で，スケーラブルかつ安全にサービスを実行できる環境
- 異種の通信デバイス間で広域通信やモビリティを提供するプラットフォーム
- 超小型デバイスのための OS
- 広域データ蓄積システム
- 適応型データフローシステムの開発
- 広域ネットワーク上でデバイス間の通信を動的に制御（帯域管理，複数コネクション間の同期確保，動的な接続の切断・再接続，等）するための機構
- セキュリティツール

の研究が行われている．基本的には，各サブプロジェクトが独自に研究を進めているため,プロジェクト終了後に新しいコンピュータネットワークシステムが完成するというものではない．また，研究の内容については，新規のコンピュータネットワークを作るというよりは，現在のインターネットに導入できるような技術として検討している面がある．これらの点において，新規にユビキタスネットワークを研究開発することを目的とする本研究課題のアプローチとは異なっている．

## 2.9 MIT／Oxygen ［2000～2005］

遍在する自己組織化するコンピュータ網を実現するために MIT の LCS と AI Lab が共同で DARPA の資金により進めている統括プロジェクトで，LCS の所長 Victor Zue と副所長 Anant Agarwal および AI 研の所長 Rodney Brooks が中心となってすすめている．この目的を実現するために必要となる個々の技術要素，例えば，知識の格納及びアクセス，網構成の自動化，網構成要素間の強調，音声認識，画像認識，変更可能なソフトウェア，N21 と呼ばれる分散型ネットワーク，セン

サー等が接続される E21 と呼ばれるデバイス，H21 と呼ばれるユーザ用のハンドヘルドデバイス，等 30 ものサブプロジェクトにおいて研究が進められている．既にいくつかの E21，H21 の試作が発表されている．但し，ネットワークに関しては Endeavour と同様に従来のインターネットをベースとしており，本研究課題のアプローチとは異なっている．

## 2.10 CMU／Aura ［2000～］

CMU は，計算機学科の学部長 Raj Reddy を中心に，ユーザの注目が最も重視すべき資源であるというコンセプトの元に，ユーザに気を散らせない，高信頼なモバイルネットワークとその上のサービスを提供するための研究を Aura と呼ぶ統括プロジェクトの元で進めている．タスク指向型コンピューティング，省電力コンピューティング，ウエアラブルコンピューティング，音声認識，分散協調，等を課題に 9 つのサブプロジェクトで研究が進められている．基本的に Endeavour と同様に既存のネットワークの上を考慮した QOS 制御やルーティングなどを研究しており，本研究課題のアプローチとは異なる．また，リアルタイム OS の研究もマルチメディア通信を提供するためのもので，本研究の小型かつセキュアなリアルタイム OS の研究とは方向が異なる．

## 2.11 ワシントン大学／Portlano ［2000～］

ワシントン大学は，XEROX PARC と共同で，ユーザに，計算機の存在を意識させない分散サービス提供環境を実現するために必要となる，多様なユーザインタフェースの統合技術，自律的にデータを分散格納しそれに対するアクセスを提供するロバストなデータ指向のネットワーク技術，およびその網の上で多様な分散サービスを提供するためのソフトウェア技術の研究を進めている．具体的には，大型ユビキタス表示装置，新しい位置センサー，モジュール式のセンサー，安価な ID システム，センサーの統合技術，プロトタイププラットフォームの試作及び，試作プロトタイプの大規模実証実験等 15 のサブプロジェクトにより進められている．主に，ネットワーク上でのデバイスの開発と分散処理技術に重点があり，本研究課題で提案するような，セキュアかつリアルタイムな通信とそのために必要となる OS やプロトコルの開発は研究の対象外となっている．

# 第三章
# 研究開発の全体計画

# 3.1 研究開発課題の概要

本研究開発課題は，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を確立することである．

## 3.1.1 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.

### 3.1.2 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.

1. リアルタイム通信プロトコル
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
3. コンパクト性
4. 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
5. ユーザとの親和性
6. 省リソース
7. 既存通信網との親和性
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

#### (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偏在性（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・省資源に取り組む.

### （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，IP 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．

## 3.1.3 研究実施計画の基本方針（概要）

ここでは，2.1，2.2 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あ困難になるため，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．

1. セキュアハードウェア
2. 通信システム
3. 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）
4. 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）
5. システム統合技術
6. 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．

## 3.1.4 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，「2.3 （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ーを確保するために,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**「耐タンパー性（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.

**【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,ルーター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．現時点では，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ものを想定しているが，これは研究の進捗・進展や，他の技術動向

に応じて変化する部分もある.

### (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検討する.

### (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.

### (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,**【サブテーマ２】基盤通信システムの研究開発**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．

### (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が必要である．
- 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.

1. ユビキタスコンピューティング標準開発環境
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
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

**(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.

**(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．

1. 現実世界の記述方式
2. 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．

### 3.1.5　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．

# 3.2 研究開発目標

## 3-2-1 最終目標

### ■全体を包括する最終目標（概要）

（１） 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つ.

（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.

（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ー機能を有すること.

（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，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，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を十分に活用する.

（７） ソフトウェア規模は，十分小さい規模を想定する.

**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の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）」**で挙げた各種ネットワークプロトコルを搭載する.

（５） 音声 CODEC を備える.

（６） グラフィックチップを備える.

**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.

（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たこと．

（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ないこと．

**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．

**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．

## 3-2-2 中間目標

**■全体を包括する最終目標**

（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．

**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物理層・データリンク層プロトコルのうち，いくつかに関しては，そのスタブ部分の仕様開発を完了する．

（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，十分小さい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の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．

**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．

（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．

**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） 最終目標の挙げた中で，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．

**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．

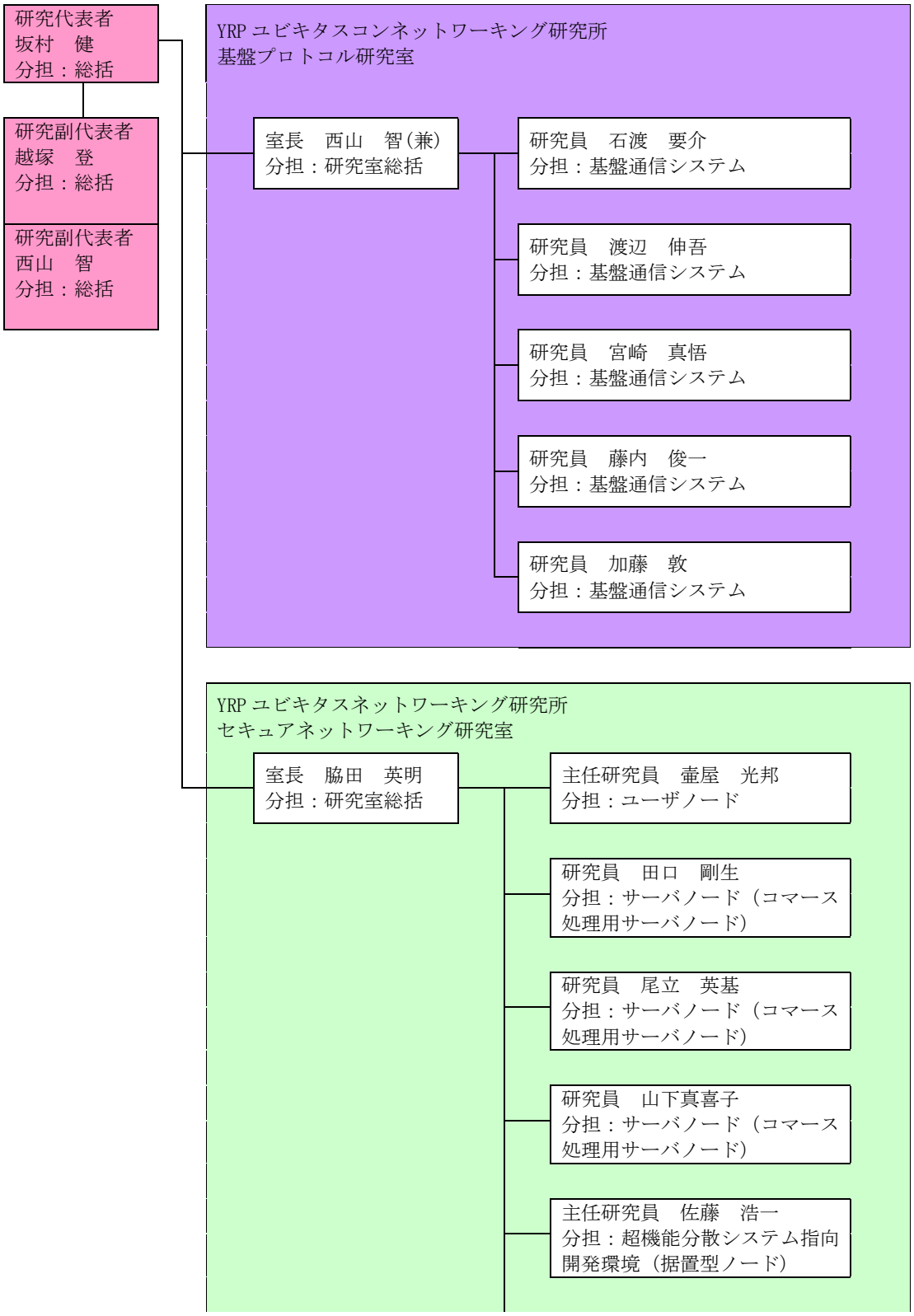
（３） サブテーマ「**ア.**」で開発したユビキタスネットワーキングプロトコルを備える．

**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.

# 3-3 研究開発体制


研究代表者
坂村　健
分担：総括
研究副代表者
越塚　登
分担：総括
研究副代表者
西山　智
分担：総括
YRP ユビキタスコンネットワーキング研究所
基盤プロトコル研究室
室長　西山　智(兼)
分担：研究室総括
研究員　石渡　要介
分担：基盤通信システム
研究員　渡辺　伸吾
分担：基盤通信システム
研究員　宮崎　真悟
分担：基盤通信システム
研究員　藤内　俊一
分担：基盤通信システム
研究員　加藤　敦
分担：基盤通信システム
YRP ユビキタスネットワーキング研究所
セキュアネットワーキング研究室
室長　脇田　英明
分担：研究室総括
主任研究員　壷屋　光邦
分担：ユーザノード
研究員　田口　剛生
分担：サーバノード（コマース処理用サーバノード）
研究員　尾立　英基
分担：サーバノード（コマース処理用サーバノード）
研究員　山下真喜子
分担：サーバノード（コマース処理用サーバノード）
主任研究員　佐藤　浩一
分担：超機能分散システム指向開発環境（据置型ノード）

研究員　小俣　三郎
分担：超機能分散システム指向
開発環境（据置型ノード）

# 第四章
# 研究開発の概要
## （平成 13 年度）

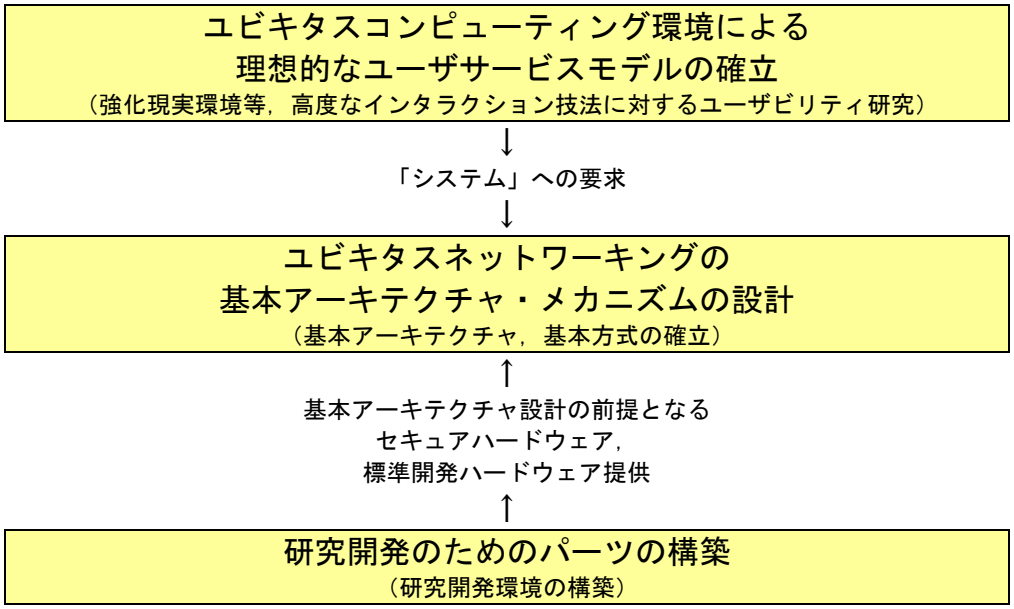
# 4.1 研究開発実施計画

## 4.1.1 研究開発の計画内容

平成 13 年度は平成 14 年の 1 ～3 月の 3 ヶ月間で次の三つの柱に基づき研究を遂行する.

1. 各サブテーマにおける基本アーキテクチャ，基本方式の確立
2. 強化現実環境等，高度なインタラクション技法に対するユーザビリティ研究
3. 研究開発環境の構築

今年の計画のポイントは，基本アーキテクチャや基本方式という，次年度以降に大きく影響与える基盤部分の基礎的検討を行うことと，その検討にために必要な材料を得るための実験や次年度以降の開発に必要な道具となるパーツの設計･試作を行う点である(下図参照).




### 1）基本アーキテクチャ，基本方式の確立

本年度は，サブテーマの中でも，本研究開発課題の核となる以下のものの基本アーキテクチャやメカニズムに関して,それを確立する上で必要な各要素技術，関連技術の調査検討を行った上で，基礎的なプロトコルやその実現アルゴリズムの検討と初期バージョンを設計する.

本年度基本方式の検討に取り組むサブテーマとその取り組みの内容は以下の通りである.

1. 基盤通信プロトコル
2. ユーザノード（移動ノード）
3. ユーザノード（固定ノード）
4. サーバノード（特に，PKI に関連する部分）
5. 統合技術のための，既存網とユビキタスネットワーキング網との間のゲートウェイ方式

**２）強化現実環境等，高度なインタラクション技法に対するユーザビリティ研究**

ユビキタスネットワーキング研究の基本アーキテクチャや設計方針を決める上で重要な判断材料となる，アプリケーション側の要求を明確にし，それを検証する必要がある．そこで，本年度，まずは，ある意味で，その実現方式ではなく，ユビキタスコンピューティング環境の理想的なユーザサービスがどのようなものかを明らかにする．これが明らかになることによって，基本アーキテクチャを策定する側からも，目指すべき要求が明らかになり，それを効率よく実現するための方式を設計することができる．

本年度は，そのようなユーザサービスモデルの中でも，特に，ユーザインタフェース部分の研究を行なう．つまり，身の回りに埋めこまれて，互いに協調動作を行なうユビキタスコンピューティング環境は，人間の活動をどのように支援するべきなのかといった手法を研究する．具体的には，ユーザ情報，人間活動や社会の活動のセマンティックスの検出方法，それによってユーザに対する情報やサービスをどういったメディアやインタフェースを通じて提供すると効果的かといったユーザビリティ研究を中心に扱う．

**３）研究開発環境の構築**

本年度は，研究開始の初年度であることから，まずこの３ヶ月の間で，全５ヵ年計画の研究開発の基盤となる研究開発環境を構築する．研究開発環境の構築は，以下の二つの事項がある．

**本研究プロジェクトの共通のパーツの設計・試作**：次年度以降に，上記の①の研究によって確立した基盤システムの構築が開始されるが，その構築のためのベースとなる共通開発のためのハードウェアを今年度は設計を完了し，試作を開始する．その中には，【サブテーマ１】に含まれる，セキュアハードウェアとして，コンタクトレス型のセキュアチップである．もう一つが，【サブテーマ６】の「(6-1) ユビキ

タスコンピューティング標準開発環境」の中で，最も下位レイヤ部分である基盤ハードウェアの標準である．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，移動・固定のユーザノードを構築する際の標準ハードウェアとする予定である．これを確立することによって，次年度以降，当社または再委託先で研究開発したソフトウェアの再利用性が高まり，多大な研究開発力を結集した時の効率的なシステム開発が実施できるようになる．

**研究設備の導入・稼動**：本年度は，本研究開発の初年度であるため，研究開発機関を通じて利用する恒久的な研究開発設備の設計と導入を行う．具体的には研究開発環境となるサーバやワークステーションの導入，通信回線の敷設などを行なう．

## 4.2 研究開発の実施内容

本年度実施した委託業務の内容には，大きくわけて３つの柱がある．

1. 基本アーキテクチャ，基本方式の確立のための調査，基礎検討
2. 強化現実環境等，高度なインタラクション技法に対するユーザビリティ研究
3. 研究開発環境の研究開発

以下，それぞれの柱について委託業務の実施内容について述べる．

### 4.2.1 基本アーキテクチャ，基本方式の確立のための調査，基礎検討

本年度は，まず，本研究開発課題の核となる基本アーキテクチャやメカニズを確立する上で必要な各要素技術，関連技術の調査検討，更に，基礎的なプロトコルやその実現アルゴリズムの検討，初期バージョンの設計を行なった．その内容は，以下の通りである．

#### １)ユビキタスコンピューティング／ユビキタスネットワーキング技術全般の調査

このユビキタスコンピューティング／ユビキタスネットワーキング技術全般の研究調査として，当該分野の学会誌や国際会議の論文などの文献調査を行った．

#### ２）基本アーキテクチャ策定に必要な基礎情報の調査

次年度以降におけるユビキタスネットワーキングの基本アーキテ

クチャの策定に必要な以下の基礎情報の収集を行なった.

**実世界コンテクストの記述形式に関する調査**:ユビキタスネットワーキングやユビキタスコンピューティングでは,実世界のコンテクストをコンピュータやネットワーク上で有効に扱う点に特徴がある.そこで,ユビキタス環境のソフトなインフラの一つとして,実世界コンテクストの情報記述形式や情報交換形式が不可欠である.これは,言い換えれば,実世界全体をデジタル情報記述することであり,広い範囲と膨大な量に及ぶ.そこで,今年度は,特に重要な我々人間自身にかかわる①個人属性情報,ユビキタス環境の応用として実用化に最も近い分野の一つである②交通システム,この二つの領域に絞り,情報記述の前段階としての,これらの属性自体が有する内容を調査した.

**決済プラットフォームインタフェースの調査**:ユビキタス環境の重要な応用の一つは経済活動である.現在我々の社会は資本主義社会であり,日常のあらゆる活動に経済活動が伴う.「もの」を購入する,使用料を支払うなど,経済活動を抜きに実用的なユビキタス応用を確立することはできない.経済活動をコンピュータ上で処理するのが,決済システムであり,従来は金融機関や電子マネーシステム上で実現されてきた.そこで,我々は,これらの決済システムをユビキタス環境と接続する手法を確立するために,既存の決済システムのネットワークインタフェースや通信プロトコルの調査を行なった.

### ３)ユビキタスネットワーキングプロトコルアーキテクチャ確立のためのアルゴリズム・プロトコルの開発と初期バージョンの設計

**アドホックネットワークの研究**:ユビキタスネットワーキングプロトコルでの物理層～ネットワーク層部分における経路確立方式として,アドホックネットワーキングが注目されている.本年度,我々はユビキタスネットワーキングへの適用を考慮した上で,アドホックネットワーキング方式上で,新しい名前解決方式とその効率化手法を開発し,その効率を定量的に評価した.

**超軽量型価値情報通信基盤の基本アーキテクチャの研究**:ユビキタスネットワーキングのトランスポート層～セッション層において,価値情報を交換するための通信プロトコルと,それを実現する情報通信基盤の初期バージョンを設計・試作した.このプロトコルは,ユビキタ

ス環境で頻繁に用いられる IC カードといった超小型の計算ノードでも利用可能なように,実行負荷が小さくコンパクトな点に特徴がある.また,耐タンパー性をもったハードウェアを用いることで,複製攻撃を防ぐことが可能である.

### 4.2.2 強化現実環境等，高度なインタラクション技法に対するユーザビリティ研究

ユビキタス環境では,いつでもどこでも通信・計算環境にアクセスできることが重要である.そういった環境とユーザとのインタラクションは,現在最も一般的なデスクトップ型のＧＵＩではなく,コンピュータの存在を意識することなく，自然に対話するための強化現実（Augmented Reality）といった高度なユーザインタフェースが有効である．こういった観点に基づき，本年度，我々は次の新しいインタラクション手法を使った実験システムを試作した.

1. IC カードを使ったユビキタス環境との多目的型対話システム
2. 遠隔操作と遠隔ステレオ映像を用いたテレプレゼンスシステム
3. IC カードを使った実世界ブックマークシステム

これらのインタラクション技術は,東京大学総合研究博物館のデジタルミュージアムⅢに設置し,数千人規模のユーザによって利用された.

### 4.2.3 研究開発環境の研究開発

次年度以降のユビキタスネットワーキング研究に必要な基盤プラットフォームを設計・試作を行なった．構築した基盤プラットフォームは，以下の通りである.

1. ユビキタスネットワークノードのための基本ボード（携帯型）
2. ユビキタスネットワークノードのための基本ボード（据置型）

#### 1）ユビキタスネットワークノードのための基本ボード（携帯型）

携帯型ノードを想定した,実験開発用ボードである.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/IEC 7816，ISO/IEC 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．こうした機能を有するハードウェアが，バッテリーで駆動する.

### 2) ユビキタスネットワークノードのための基本ボード（据置型）

据置型ノードを想定した,実験開発用ボードである.CPU とした M32 を用い,各種の実験開発が行なえるように,多くのインタフェース(シリアル, PCMCIA, ISO/IEC 7816, 10base-T, 人工網膜カメラなど）を備えている.

# 第五章
# 研究開発実施状況
## （平成 13 年度）

# 5.1 世界における研究動向

## １）はじめに

本節では，ユビキタスネットワークに関連する各研究機関の研究プロジェクトの調査報告を行う．具体的には，米国を中心としたユビキタス関連のプロジェクトのうち，活発に活動している以下の５つのプロジェクトの現状を調査した．

- Endeavour プロジェクト (University of California, Berkeley)
- TinyOS プロジェクト (University of California Berkeley)
- The NewArch プロジェクト ( University of Southern California Information Sciences Institute 他)
- Chord プロジェクト (Massachusetts Institute of Technology)
- Bio-networking プロジェクト( University of California, Irvine)

Endeavour プロジェクトの目的は,コンピュータが内蔵された多種多様な情報機器（大型コンピュータから，家電製品，さらには超小型センサーまで）を相互接続することにより，あらゆる種類の情報を収集し，さらのその情報を即時に引き出したり，情報に従って最適な対応を自動的に行ったりできるような次世代コンピュータネットワークを構築するのに必要となる要素技術を研究・開発することである．

TinyOS プロジェクトの目的は，超小型デバイスのためのシステムサービスとネットワークサポートを提供する OS を開発し，ネットワークに接続されたセンサープラットフォーム（ハードウェアとソフトウェアを含む）上で，超低電力・低コストのセンサーネットワークの展開を可能とすることである．

NewArc プロジェクトの目的は，インターネット技術の発展に向けた新しいアーキテクチャを定義し，そのプロトタイピングを行うことにある．具体的には，既存のインターネットアーキテクチャの上ではなく，将来のインターネットにおける要求条件を検討し，長期的な視点に立った研究を目指している．特に QoS 関連の話題が中心となる．

Chord プロジェクトの目的は，peer-to-peer の通信方式によりスケーラブルで頑健な分散システムを構築することである.Chord は完全に分散化された対称的なシステムであり，log(N)のオーダのメッセージ数でデータを探索することが可能な検索メカニズムを核技術として研究を進めている．

Bio-networking プロジェクトの目的は,将来の人間やコンピュータ,家電や自動車などの多種多様なデバイスや装置がノードとして接続されるユニバーサルネットワーク上に存在するあらゆるサービスを有機的につなぐ適応型サービスを提供するために，生物界のコンセプトやメカニズムをモデルとした，Bio-networking アーキテクチャおよび,その実現手法を提案することである．以降，各プロジェクトの調査結果を順次報告する．

## ２）The Endeavour Project at University of California, Berkeley

### 2-1) プロジェクトの概要

プロジェクト名：　Endeavour

実施機関：　カリフォルニア大学バークレー校 EECS 学部（Department of Electrical Engineering and Computer Sciences, University of California, Berkeley)

スポンサー：　DARPA (The Defense of Advanced Research Projects Agency)，および，本プロジェクトに参加している企業からの寄付

期間：　1999 年 6 月 1 日から 3 年間

参加教授：　Randy H. Katz 教授（本プロジェクトの責任者，ネットワークが専門）を筆頭に，OS，人工知能，データベース，コンピュータアーキテクチャ，ユーザインタフェース，小型デバイス，セキュリティ等を専門とする教授陣　（約 15 名の教授が関与している.）

参加企業：　SUN，HP，インテル，ゼロックス，ジーメンス，ノキア，ノーテル，マイクロソフト，等

ホームページ：　http://endeavour.cs.berkeley.edu/

### 2-2) プロジェクトの目的

Endeavour プロジェクトの目的は,コンピュータが内蔵された多種多様な情報機器（大型コンピュータから，家電製品，さらには超小型センサーまで）を相互接続することにより，あらゆる種類の情報を収集し，さらのその情報を即時に引き出したり，情報に従って最適な対応

を自動的に行ったりできるような次世代コンピュータネットワークを構築するのに必要となる要素技術を研究・開発することである.

このようなことを実現するには，各機器のシームレスなネットワーク接続，情報収集・交換能力の向上，高速な意思決定機構と学習能力，ユーザの好みに合致したサービスの提供，概念的なサービスの構成，大規模システムのデザイン・構築・管理手法，セキュリティおよびプライバシーの確保，といった多くの項目を実現する必要があり，これらを実現するための研究が行われている.

### 2-3) プロジェクトの構成

本プロジェクトの研究の進め方としては，ある特定のシステムを構築することが目的とするのではなく，2-2)で述べられているような新しいコンピュータネットワークと必要となる要素技術を研究・開発していくことが目的となっている. したがって, Endeavour プロジェクトには，複数のサブプロジェクトが存在し，各教授がそのサブプロジェクトの指揮を執って研究が進められている. それぞれのサブプロジェクトは，基本的には独立して研究を進めており，すべてのサブプロジェクトが集まればシステムが構築できるというものではない. また，Endeavour プロジェクト開始前から行われていた研究も, サブプロジェクトとして存在している. サブプロジェクトとしては，以下のようなものがある.

- Smart Dust
  - 超小型電子機器システム（MEMS: Micro-Electro-Mechanical System)を使用したセンサー, アクチュエータ, コミュニケータの開発
- Millennium
  - クラスターベースの大規模計算処理，および，メッセージ処理システムの構築
- IStore
  - ネットワークを利用したスケーラブルでメインテナンスをほとんど必要としないストレージサーバーシステムの構築
- Ninja
  - ネットワーク上で，スケーラブルかつ安全にサービスを実行できる環境を提供するための仕組み提供
- ICEBERG

- 異なった種類の通信デバイス間で広域の通信環境やモビリティを提供するためのプラットフォームの提供

- Tiny OS, Ad Hoc Wireless Networking
  - 超小型デバイスのためのシステムサービスとネットワークサポートを提供する OS の作成
- OceanStore
  - 不安定なサーバーを含むインフラ上においても一貫性を保ち，利用しやすいサービスを提供可能で，かつ，数十億人のユーザが利用可能な広域データ蓄積システム
- Telegraph
  - どこからでもデータへのアクセス，データの解析，その他の処理を行えるような適応型データフローシステムの開発
- Data Recharging
  - 利用状況とユーザの選択により，広域ネットワーク上でデバイス間の通信を動的に制御（帯域管理，複数コネクション間の同期確保，動的な接続の切断・再接続，等）するための機構の開発
- Athena/APG
  - セキュリティプロトコルの自動検証ツール，自動セキュリティプロトコル生成ツール（APG: Automatic secure Protocol Generation)，等，セキュリティツールの開発

### 2-4) まとめ

Endeavour プロジェクトでは,複数のサブプロジェクトが相互に関連しながら，将来のコンピュータネットワークで必要となると考えられるハードウェア（通信デバイス，dust motes，スケーラブルクラスター，…）とソフトウェア（OS，分散ファイルシステム，スケーラブルプロセッシング，広域データ管理システム，セキュリティ機構，….）が研究・開発されている．基本的には，各サブプロジェクトが独自に研究を進めているため，プロジェクト終了後に新しいコンピュータネットワークシステムが完成するというものではない．しかし，研究の内容については，新規のコンピュータネットワークを作るというよりは，現在のインターネットに導入できるような技術として検討している面があり，インターネットの将来像を考える上でも参考になると考えられる．

Endeavour プロジェクトは，1999 年 6 月からの 3 ヵ年プロジェクト

で，2002 年で終了することになる．そこで，この後継プロジェクトとして，CITRIS (The Center for Information Technology Research in the Interest of Society)プロジェクトが開始された．これは，カリフォルニア州が中心となっており，研究に関しては，カリフォルニア大学のバークレー校，デービス校，マーセッド校，サンタクルーズ校と，Endeavour プロジェクトに参加していた企業が参加する．プロジェクトの目的は，エネルギー問題，交通問題，地震等の災害に対する安全確保，教育，健康管理，環境問題，等の社会的な問題に対応できるようなネットワークのインフラストラクチャーを形成しようというもので，Endeavour プロジェクトで行われた研究の成果も，このプロジェクトの基礎となっている．

## 参考文献


4. J. Kahn, R. H. Katz and K. Pister, "MOBICOM Challenges: Mobile Networking for 'Smart Dust'," ACM MOBICOM Conference, Seattle, WA, August 1999.
5. B. Raman, H. J. Wang, J. S. Shih, A. D. Joseph and R. H. Katz, "The Iceberg Project: Defining the IP and Telecom Intersection," IT Professional, Nov/Dec 1999.
6. R. Gummadi and R. H. Katz, "The Data Management Problem in Post-PC Devices and a Solution," SIGOPS EW2000: 9th ACM SIGOPS European Workshop, "Beyond the PC: New Challenges for the Operating System," Kolding, Denmark, September 2000.
7. X. Hong, "Personal Activity Coordinator: A Coordination layer for Independent Services," UC Berkeley, master's report, December 1999.
8. J. Hong and J. Landay, "A Context/Communications Information Agent," Workshop on Situated Interaction in Ubiquitous Computing, CHI 2000 Conference, The Hague, The Netherlands, April 2000.
9. J. M. Kahn, R. H. Katz and K. Pister, "Emerging Challenges: Mobile Networking for Smart Dust," Journal of Communication and Networks, Vol. 2, No. 3, September 2000.
10. S. Agarwal, R. H. Katz, S. Krishanmurthy and S. Dao, "Impact of Group Movement on Energy Consumption in Ad-Hoc Wireless Networks," Infocomm 2001.

11. D. Song, A Perrig and D. Wagner, "Search on Encrypted Data," Prof. IEEE Symp. Security and Privacy, May 2000.

## ３）TinyOS: An operating system for Networked Sensors

### 3-1) プロジェクトの概要

実施機関： カリフォルニア大学バークレー校 EECS 学部 (Department of Electrical Engineering and Computer Sciences, University of California, Berkeley)
スポンサー： the Defense Advanced Research Projects Agency, the National Science Foundation
参加教授： David Culler 教授
参加企業： Intel Corporation , Ericsson , Philips , Sun Microsystems, IBM, Nortel Networks, Compaq
ホームページ：
http://tinyos.millennium.berkeley.edu/index.html

### 3-2) TinyOS の目的

（１）目的

TinyOS とは，超小型デバイスのためのシステムサービスとネットワークサポートを提供する OS である．

TinyOS の目的は，ネットワークに接続されたセンサープラットフォーム（ハードウェアとソフトウェアを含む）上で，超低電力・低コストのセンサーネットワークの展開を可能とすることである．

（２）背景

わずか 1 立方 mm の容積内での計算が可能かを検討する．低電力無線通信技術とマイクロ電気機械センサー変換器における利点がこれを可能とする．その際，検出と通信と計算を 1 個のアーキテクチャに結合する方法，ソフトウェアに要求される条件，与えられた設計を評価する方法などが問題となる．

（３）特徴

TinyOS は，物理的なサイズが小さく消費電力が低いプラットフォー

ム上での動作を前提としている．そのため，そのプラットフォームは，物理的な並行処理と制御の階層が制限されており，デバイスに直結のインタフェースを採用している．

また，同時集中処理を行うので，フロースルーであり，コマンド応答を待たない．すなわち，複数の入出力を同時に取り扱わなければならない．

設計や用法も様々で，アプリケーションに特有な普遍性はなく，デバイスに極めて多様性がある．それにより，効率的なモジュラリティーとハードウェア／ソフトウェア境界を超えての移動が可能になっている．

管理されていない不安定なプラットフォームにおいてもロバストな処理を行い，狭帯域のインタフェースとなる．また，効率的なモジュラリティーを提供する．

### 3-3) Mote

（１）「Mote」ハードウェア

現在の「Mote」の初期プラットフォームである．「Mote」とは，センサーとアクチュエータの機能に計算・通信機能を組み込んだ超小型デバイス上で動作させることを目標として開発されている OS である．以下に示すような，既製の構成要素から成り立っている．

- 4MHz，8bit MCU (ATMEL)……512 バイト RAM，8KB ROM
- 900MHz 無線(RF モノリシック)……10～100 フィート範囲
- 温度センサー
- 光センサー
- LED 出力
- シリアルポート

（２）第二世代「Mote」

現在進行中の第二世代 Mote のハードウェアキットは，2 ボードサンドイッチである．すなわち，無線通信用メイン CPU ボードと第 2 センサーボードからなる．また，拡張とカスタマイズが可能となっている．

現在の（実験用に設計された）センサーは，以下に示す項目を測定できる．

- 加速度
- 磁界
- 温度

- 圧力
- 湿気
- 光
- RF 信号強度

RF 伝送強度と感受強度を制御することができる.

また,「実験用に設計された」Mote では, 以下のセンサーが追加設計される.

- 2 軸加速度計と 2 軸磁気計
- 湿気・温度・圧力センサー
- 伝送強度センサーと制御

（3）非専用入出力制御装置

無線を用いてビット単位での通信をする. この際, ソフトウェアは 100μs 毎にビットを送らなければならない. バッファリングは無いので, デッドラインを過ぎたデータはロストする.

### 3-4) TinyOS ソフトウェア

（1）ソフトウェア要求条件

TinyOS のソフトウェアに対して, 以下のような要求条件を満足させる必要がある.

- 小さな物理的サイズ
- 効率のよい資源利用
- 高度なモジュール化

（2）ソフトウェア概要

TinyOS のソフトウェアは, アプリケーションプログラマからのハードウェアの詳細を抽象化するモデルに基づいた装置を提供する. また, 複数のアプリケーションを並行して実行できる.

提供されるサービスは, 以下の通りである.

- RF メッセージプロトコル
- 周期的なタイマイベント
- UART データ転送に対する非同期アクセス
- 静的不揮発性記憶のための機構

アプリケーションに特有で必要な機能を持たせるために, システム装置の交換を可能とする. また, 4KB の ROM と 256B の RAM の中に 1 個のアプリケーションを収める.

### 3-5) TinyOS の構成

（１）内部

TinyOS の内部には構成要素のスケジュラーとグラフがあり，2 段階スケジューリングモデル（スレッドおよびイベント）が強く推奨されている．

TinyOS 構成モデルは，以下の項目から成り立っている．

- フレーム（記憶）
- タスク（計算）
- コマンド，ハンドラー（イベントインタフェース）

推奨される記憶装置モデルでは，構成要素毎にフレームがあり，スタックを共有しているが，ヒープは持たない．

非常に細いマルチスレッディングが行われている．レイヤリングにより，構成要素が低位の構成要素に対してコマンドを発行したり，イベントが高位のイベントかまたは低位のコマンドに信号を送る．

（２）構成要素

図 1 に，TinyOS の構成要素を示す．

（http://tinyos.millennium.berkeley.edu/presentations/TinyOSTalk.ppt よりの抜粋）

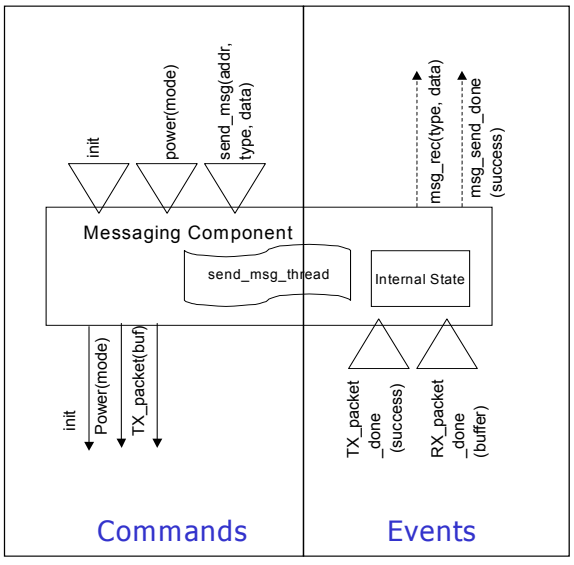



図 1　TinyOS の構成要素図

図 2 に，1 個のアプリケーションに対する構成を示す．

（http://tinyos.millennium.berkeley.edu/presentations/TinyOSTalk.ppt よりの抜粋）

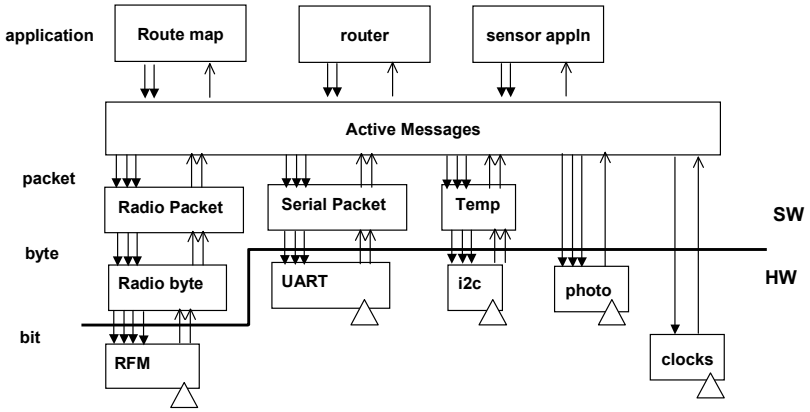



図２　１個のアプリケーションに対する構成

（３）イベントベースプログラミングモデル

TinyOS は状態機械プログラミングモデルであり，システムは状態機械で構成されている．各状態機械は，1 個の TinyOS「構成要素」である．

命令とイベントハンドラーは，モジュールをある状態から別の状態へと，速やかかつ低オーバーヘッドで遷移させる．多くの独立なモジュールが，単一の実行状況を効率的に共有することができる．このことは，大規模なシステムに対する設計パラダイムである．「タスク」は計算作業の遂行に用いられる．

（４）ハードウェア・ソフトウェア境界の容易な移動

TinyOS の構成要素は，ソフトウェア内にハードウェアの抽象をモデル化することにより，ソフトウェア構成要素のハードウェアへの移動を可能にしている．

### ４）The NewArch Project: Future-Generation Internet Architecture

#### 4-1）プロジェクトの概要

プロジェクト名： NewArch
実施機関： 南カリフォルニア大学 情報科学研究所 (UCS/ISI: University of Southern California Information Sciences Institute), マサチューセッツ工科大学 計算機科学研究所 (MIT/LCS: Massachusetts Institute of Technology Laboratory for Computer Science), 国際計算機科学研究所インターネット研究センター (ICSI CIR: International Computer Science Institute, Center for Internet Research)
スポンサー： DARPA (The Defense of Advanced Research Projects Agency)
主な担当者： Robert Braden (ISI), Noel Chiappa (コンサルタント), David Clark (MIT), Mark Handley (ICSI), Scott Shenker (ICSI), John Wroclawski (MIT)
ホームページ： http://www.isi.edu/newarch

### 4-2) プロジェクトの目的

インターネットの技術的なデザインは1970年代に作成されたネットワークアーキテクチャに基づくものであり，その後のさまざまな要求条件を解決するために追加された機能により，当初のアーキテクチャからかけ離れつつある．このプロジェクトの目的は，インターネット技術の発展に向けた新しいアーキテクチャを定義し，プロトタイピングを行うことにある．インターネットに関する多くの研究開発は既存のインターネットアーキテクチャの上に構築されているが，このプロジェクトは将来のインターネットにおける要求条件を検討し，長期的な視点に立った研究を目指している．

### 4-3) 研究内容

このプロジェクトは 2000 年に始まったと思われるが，フレームワーク作りをしている最中であり，まだ実際のプロトコルの設計や実装には至っていないようである．このプロジェクトで議論されているインターネットのアーキテクチャや，将来のインターネットのための要求条件は以下のようなものである．

- モビリティ

これからのインターネットは動的なモビリティを柔軟でかつ効率的にサポートすべきである．ここにはすべての装置がモビリティを持つようなユビキタス・モビリティも含まれる．

- ポリシーベースの自動設定
  DHCP（Dynamic Host Configuration Protocol)に代表される現在の自動設定機能では，セキュリティやポリシーに関する機能が十分ではない．これからのインターネットは，ホストやルータに対してポリシーや管理上の制約に基づいた自動設定機能を提供すべきである．
- 頻繁に変動する網資源への対応
  回線交換型のバックボーンやノードが移動することにより接続方法が切り替わるなど，網資源が短時間に変動する形態に対応すべきである．
- 通信容量の割当機能
  インターネットは，ユーザやアプリケーションに対して通信容量を割り当てる機能をそのユーザやネットワーク管理者に提供する必要がある．現在のインターネットは輻輳が起こることによって，結果的に帯域の割当が行われている．一般的には，輻輳しているときにはすべてのユーザがレートを下げるような「公平性」的なものが目標となってきたが，必ずしも正しいモデルではないだろう．商用サービスでは料金に応じて通信容量を割り当てるという要求があるし，行政的な目的では災害対応のように優先度の高さに応じて帯域を割り当てる必要性もある．管理者がネットワークに対して網資源を要求したり，ネットワークがユーザに対して要求帯域が確保可能かどうかを通知する機能があるべきである．
- 極端に大きい伝搬遅延
  この要求は，特に NASA の惑星探査計画にインターネット技術を使うための惑星間インターネットで提起されたものである．これまでに議論されてきた広帯域・高遅延ネットワークの延長ではあるが，遅延そのものと，遅延帯域積の相互作用がネットワークアーキテクチャを複雑化していることを反映したものと言える．

商用プロバイダがインターネットのアーキテクチャにまで責任を持っているとは考えていないので，このプロジェクトの組織に関しては，

これまでのように政府の資金で行う研究が中立的な役割を担う．このプロジェクトは，二つのフェーズで進める．最初のフェーズは，ネットワークアーキテクチャに関する有識者が要求条件に優先度付けをして項目にまとめる．第 2 フェーズでは，シミュレーション，プロトタイプの開発および試験などを適切に組み合わせることによって，設計したアーキテクチャの検証実験を行う．この二つのフェーズは部分的に重なりながら，また交互に繰り返しながら進められ，アーキテクチャに関する抽象的な考えを，実験を通して確実なものとする．基本的なアーキテクチャの設計は 6～10 人の小さなグループで行うのが理想的である．もしこのフェーズで有望な案が出てきたら，特定のプロトコルやアルゴリズムを設計・開発するためにもっと多くの人数からなる組織を構成する．これが具体的な成果を出せば，DARPA や NSF や業界の資金協力を得て，アーキテクチャの草案作りを継続して進めていくことも可能になるであろう．アーキテクチャの草案が完成すれば，もっと大きな研究機関が参加することにも役立つし，ワークショップを組織してアーキテクチャの議論を行うことを促進することも可能である．この作業は IRTF (Internet Research Task Force)の研究グループが引き受けることも可能であろう．このプロジェクトでは，ネットワークアーキテクチャの設計方針，要求条件や目的を作ることなどが大きな成果になると期待されるが，これまでの経験からトップダウンのプロトコル設計だけでは限界がある．このプロジェクトは実験的な実装やシミュレーションを組み合わせ，アーキテクチャに沿ったプロトタイププロトコルの構築や試験といった活動を重視する．新しいアーキテクチャは，既存の OS のカーネル部分に実装されてきたアプリケーション層より下のプロトコル郡を変更することになるかもしれない．このため，プロトタイプの開発や試験は，一部の研究環境，テストベッド，インターネット上でトンネル化するなどの方式をとることになるであろう．しかし，このような試験方式では計ることのできない項目もあり，特に(1)スケーラビリティ，(2)異種環境，(3)高い性能，(4)経済またはビジネスモデルとの相互作用などはシミュレーションや議論の中で実証していくしかない．

### ５）The Chord Project at MIT

#### 5-1）プロジェクトの概要

プロジェクト名： Chord
実施機関： マサチューセッツ工科大学LCS学部PDOS研究グループ (Massachusetts Institute of Technology, Laboratory for Computer Science, Parallel & Distributed Operation Systems)
スポンサー： DARPA (The Defense of Advanced Research Projects Agency), SPAWAR (The Space and Naval Warfare Systems Center)
期間： 不明(2001 年 5 月にホームページ公開開始)
参加教授： Frans Kaashoek 教授（コンピュータサイエンス，電気工学専門)
参加企業： LCS の Oxygen プロジェクト，NTT
ホームページ： http://www.pdos.lcs.mit.edu/chord/

### 5-2) プロジェクトの目的

Chord プロジェクトの目的は，peer-to-peer の通信方式によりスケーラブルで頑健な分散システムを構築することである．この研究における核となる技術は，Chord 分散ハッシュ検索プリミティブである．Chord は完全に分散化された対称的なシステムであり，log(N)のオーダのメッセージ数でデータを探索することが可能である(N はシステムのノード数を表す)．Chord の検索メカニズムは，頻繁なノードエラーやシステムへの新規ノードの参入に対し，証明可能な頑健性を持つ．

Chord を利用する方向性として，CFS (Cooperative File System)ストレージシステムの基盤技術となることが挙げられる．CFS では誰でも自分のファイルシステムへの開示，更新が許可されており，他人には read-only として提供するファイルシステムである．CFS は極端に込み合った場合でも高いパフォーマンスを達成するため，非常に広範囲でデータサービスの負荷分散を行う必要がある．さらに全てのデータのコピーを作成し，システムへのノードの離脱や再参加の時にそのコピーを利用して信頼性を維持する必要がある．これらの解決に Chord は有効なソリューションとなる．

### 5-3) 研究内容

Chord プロジェクトの中心的技術は peer-to-peer 通信を利用した分散ハッシュ検索プリミティブ(ミドルウェア)であり，個々のノードにマッピングされた Key により情報検索を行うプロトコルを提供する．

また，システムへのノードの参加，離脱(failure を含む)をサポートする．応用先として，分散型検索システムや協調ファイルシステム等が考えられている．

**■システムモデル**

従来の peer-to-peer システムの中心的機能のほとんどは効率的なデータ配置である． Chord は頻繁にノードの出入りのある動的な peer-to-peer システムにおける検索のための柔軟なプロトコルである．Chord プロトコルは，ノードに対応した Key をアプリケーションに提供する．以下が Chord のシステムモデルである．

- ロードバランス
  平均的なキーの分散による分散ハッシュ関数
- 分散化
  完全に対等なノード群(階層構造でない)
- スケーラビリティ
  大規模システムに向けた検索コストの削減
- availability（強靭さ）
  ノードの参加・離脱等の不安定な状態における動作に信頼性がある
- 柔軟な名前付け
  階層構造を持たない自由なネーミングが可能

**■コア技術**

分散ハッシュ技術と呼ばれるものであり，以下の 3 つの問題を解決することを目標とする．

- どのようにキーの位置を見つけるか
- どのように新しいノードがシステムに参加するのか
- どのようにノードが failure した場合にシステムが復帰するのか

consistent ハッシングを用い，ほぼ同数のキーを全てのノードが受け取るように高効率の負荷分散が可能であることや，N 番目のノードが動いたときに，全体のほんの 1/N のオーダのキーの移動で済むことが達成できる．このように，最小のメンテナンスで負荷分散が可能となる．

(ア)ルーティング情報の分散化

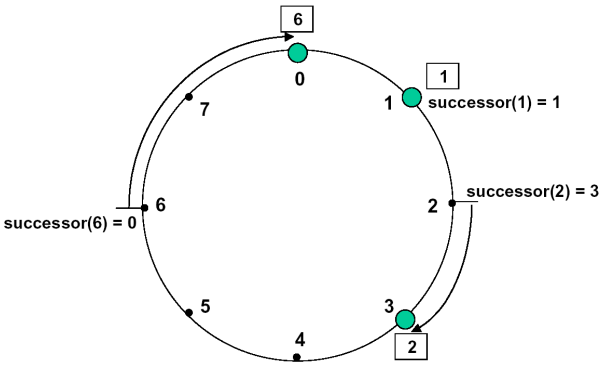



図 3　m=3 の時の identifier circle の例

仮想的な空間である identifier circle を用いて Chord ネットワークの各ノードに Key を配置し，ルーティング情報(finger table)を作成する．以下にその方法を示す．

(1)ノードと Key に対してそれぞれ m-bit の ID を割り当てる．ID はノードの場合は IP，Key の場合はその Key のハッシュ値とする．(m は同じ ID が生成される確率がほとんどない程度に十分な大きさとする)
(2)ノードおよび Key のハッシュ値に対して mod 2^m を算出し，identifier circle 上にそれぞれ配置する．(図 3)．
(3)Key をノード上に配置する．具体的にはその Key から時計回りに数えて最初に出会うノードに配置する．図 3 の場合，Key1 はノード 1 へ，Key2 はノード 3 へ，Key6 はノード 0 へそれぞれ配置する．なお，各ノードは時計回りに次のノードに関する情報(IP アドレス等)を知っているとする．
(4)各ノードで finger table(ルーティング(検索)テーブル)を作成する (図 4 (b))．
実際の検索方法は，図 4 (b)の場合，例えばノード 3 が identifier1 を検索したいとする．ノード 3 の finger table を見ると，1 は [7,3) に含まれる．次に succ.(successor)の欄が 0 であることから，ノード 0 に問い合わせればよいことが分かる．同様に，ノード 0 の finger table には identifier1 に対する successor はノード 1 であり，さらにノード 1 において identifier1 の succcessor はノード 1 自身であるため検

索が完了する.

上記方式に対し，以下の定理が証明されている.
各ノードは logN のオーダの他のノードの情報を扱えばよい.
検索は logN のオーダのメッセージ数で完了する.
参加と離脱時には log^2N のオーダのメッセージ数で完了する.

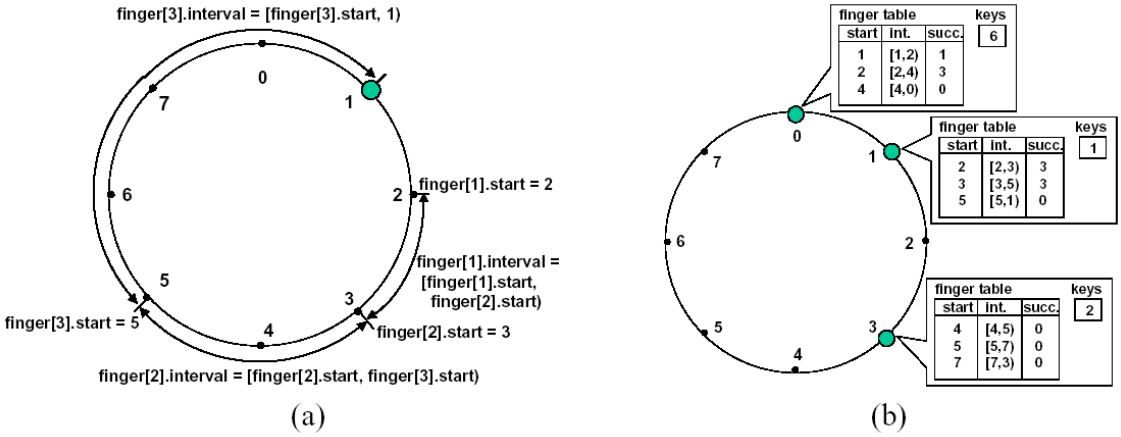



図 4 m=3 の時の finger table の例

(イ)ノードの参加と離脱時の finger table の更新
前提として，新規に参入したノード n は，identifier circle 上の predecessor ノード n′との通信方法(アドレスなど)を何らかの手段で入手できるとする.
ノード参加時の更新手順を以下に示す.

(1)新規ノードnは,ノードn’に問い合わせながら自身のfinger tableを作成する．最適解として，新規に参入したノードは近隣のノードから finger table のコピーを貰って自分の finger table を作成するために参照すると，finger table が短時間で生成可能である.
(2)既存のノードの finger table を書き換える.
(3)新規ノードにに対応する Key を新規ノードに移動する.
ノードの離脱時は，あるノードを参照できない場合に次に参照するノードを示したsuccessor-listをあらかじめ用意しておくことで容易に更新できる.

■他の技術との比較

(1)DNS (Domain Name Server) [1]

ホスト名を IP アドレスにマッピングするサービスである．Chord でもほぼ同じことができるが，Chord の場合は分散環境であるため，専用のサーバが必要ないという点で異なる．また，DNS では名前の構造が決まっているが，Chord の場合は決まっていない．さらに DNS のタスクは名前解決だけであるが，Chord は特定のマシンに関連しないデータオブジェクトの検索にも用いることが可能である．

(2)Freenet peer-to-peer storage system （以下，Freenet）[2][3]

Freenet は Chord と似ており，分散的かつ対称的であり，ホストの参加，離脱に対して自動的に対応できる．しかし，Freenet はドキュメントと明示的なサーバの対応付けに対する信頼性がなく，キャッシュされたコピーを検索する方式としている．Freenet は匿名を許可しているが，存在するドキュメントの検索の保証や検索コストの下限値を提供することができない．一方，Chord は匿名を許可しないが，検索時間は有限であり，成功，失敗にかかわらず必ず検索結果を提示する．

(3)Ohaha System [4]

Ohaha はドキュメントをノードにマッピングする際に，Chord の consistent ハッシュのようなアルゴリズムを採用している．また，Freenet と同じの要求ルーティング方式を採用している．その結果，Freeneto と同じ欠点を持っている．内蔵メモリによりオフラインでデータを保持するマシンにマッピングするツリーを利用する．

(4)Globe system [5]

移動するオブジェクトの位置にオブジェクト ID をマッピングする広範囲の位置サービスを提供する．インターネットを地理的，トポロジ，管理上の領域の階層にアレンジし，DNS に良く似た静的な world-wide な検索ツリーを構築する．オブジェクトに関する情報はツリーの葉に蓄積し，ポインタのキャッシュにより検索のショートカットを提供する．Globe system はハッシュのような技術で複数の物理的な基幹サーバ間でオブジェクトの振り分けを行うことにより，論理的な root において高負荷な処理が起こるため，スケーラビリティがない．Chord のハッシュ機能は階層化することなしに十分によいスケーラビリティを達成している．ただし，Chord は Globe system のようなネットワークの

位置情報は扱うことができない.

(5)Plaxton が開発した分散データ位置プロトコル (in OceanStore) [6][7]

おそらく最も Chord プロトコルに近いと思われる.Chord よりも強い保障機能を持つ.Chord のようにクエリが対数ホップ数内で目標に到達することを保障し，キー配置のバランスもよい結果となる．Plaxton プロトコルでは，キーが蓄積されたノードよりもネットワーク的に遠くへは，決してクエリが届かない．Chord の利点は，実質的に複雑でないこと，およびノードの参加と離脱が起こった場合の扱いがうまいことである.

(6)Pastry (PAST を利用した位置アルゴリズム) [8]

これも Chord と似ているが，Pastry はプレフィックスベースのルーティングプロトコルであり，また他の細かい点で Chord と異なる.

(7)CAN [9]

キーを値にマッピングする分散ハッシュテーブルを実装するために d 次元のデカルト座標空間を利用している(d はいくつかの固定値を取る)．検索コストは dN^(1/d)のオーダである．Chord との差異は，CAN のノードが扱う情報が，ネットワークサイズ N に依存しないことであるが,検索コストが logN よりも速く増加する点が Chord に劣る.また，Chord は部分的に間違ったルーティング情報に対する場合においても，頑強である.

(8)Grid [10]

Chord のルーティングプロセスは，Grid 位置システムの 1 次元版として見られるかもしれない．Grid はクエリのルーティングは，実世界の地理的位置情報に依存している．Chord は Grid に似たアルゴリズムでルーティングを実行しているが，ノードを 1 次元空間にマッピングしている点で異なる.

**参考文献**

12. MOCKAPETRIS, P., AND DUNLAP, K. J. Development of the Domain Name System. In *Proc. ACM SIGCOMM* (Stanford, CA, 1988), pp. 123-133.

13. CLARKE, I. A distributed decentralised information storage and retrieval system. Master's thesis, University of Edinburgh, 1999.
14. CLARKE, I., SANDBERG, O., WILEY, B., AND HONG, T.W. Freenet: A distributed anonymous information storage and retrieval system. In *Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability* (Berkeley, California, June 2000).
15. http://freenet.sourceforge.net.
16. Ohaha, Smart decentralized peer-to-peer sharing.
17. http://www.ohaha.com/design.html.
18. BAKKER, A., AMADE, E., BALLINTIJN, G., KUZ, I., VERKAIK, P., VAN DER WIJK, I., VAN STEEN, M., AND TANENBAUM., A.The Globe distribution network. In *Proc. 2000 USENIX Annual Conf. (FREENIX Track)* (San Diego, CA, June 2000), pp. 141-152.
19. KUBIATOWICZ, J., BINDEL, D., CHEN, Y., CZERWINSKI, S., EATON, P., GEELS, D., GUMMADI, R., RHEA, S., WEATHERSPOON, H., WEIMER, W.,WELLS, C., AND ZHAO, B.OceanStore: An architecture for global-scale persistent storage. In *Proceeedings of the Ninth international Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2000)* (Boston, MA, November 2000), pp. 190-201.
20. PLAXTON, C., RAJARAMAN, R., AND RICHA, A. Accessing nearby copies of replicated objects in a distributed environment. In *Proceedings of the ACM SPAA* (Newport, Rhode Island, June 1997), pp. 311-320.
21. DRUSCHEL, P., AND ROWSTRON, A. Past: Persistent and anonymous storage in a peer-to-peer networking environment. In *Proceedings of the 8th IEEE Workshop on Hot Topics in Operating Systems (HotOS 2001)* (Elmau/Oberbayern, Germany, May 2001), pp. 65-70.
22. RATNASAMY, S., FRANCIS, P., HANDLEY, M., KARP, R., AND SHENKER, S. A scalable content-addressable network. In *Proc. ACM SIGCOMM* (San Diego, CA, August 2001).
23. LI, J., JANNOTTI, J., DE COUTO, D., KARGER, D., AND MORRIS, R. A scalable location service for geographic ad hoc routing. In

*Proceedings of the 6th ACM International Conference on Mobile Computing and Networking* (Boston, Massachusetts, August 2000), pp. 120-130.

## ６）Bio-Networking Architecture プロジェクト

### 6-1) プロジェクトの概要

プロジェクト名：Bio-Networking Architecture プロジェクト
実施機関：　カリフォルニア大学アーバイン校，ICS 学部 Network Research Group
(University of California, Irvine, Department of Information and Computer Science
スポンサー：　DARPA
担当教授：　須田　達也　教授　（学生や研究員１２名）
ホームページ：　http://netresearch.ics.uci.edu/bionet

### 6-2) プロジェクトの目的

同プロジェクトの目的は，将来の人間やコンピュータ，家電や自動車などの多種多様なデバイスや装置がノードとして接続されるユニバーサルネットワーク上に存在するあらゆるサービスを有機的につなぐ適応型サービスを提供するために，生物界のコンセプトやメカニズムをモデルとした，Bio-networking アーキテクチャおよび，その実現手法を提案することである．将来のユニバーサルネットワークの要求条件として，１）スケーラビリティがあること，２）多様で動的に変更されるな条件に適応的であること，３）セキュアであること，があげられているが，蜂や蟻等の大規模な生物界のシステムでは，上記要求条件を解決するのに適した特徴を有している．このため，これらに着目し，Bio-networking アーキテクチャを提案することとした．

### 6-3) 基本概念

Bio-networking アーキテクチャは，ユニバーサルネットワーク上で適応型サービスを実現するために，生物学的な進化メカニズムを適用したアーキテクチャである．

Bio-networking では，集中的な管理機構を排除した完全分散型のアプローチに基づき，ユーザや多種多様なデバイス，サービス要素など

を含むネットワーク上の構成要素を，自律的で，生物的な動作を行うサイバーエンティティ(CE)として抽象化して扱う．CE は，何百万ものユーザに作成されて大量に存在し，simple behavior を有し，自身の behavioral policy に基づいて自律的に行動する．CE の設計を以下に記す．

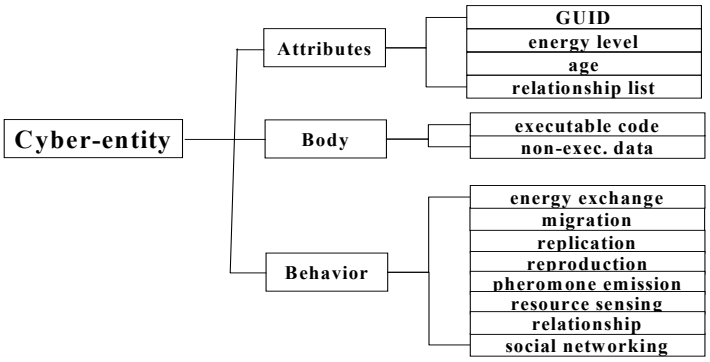



図 5　Cyber-Entity の構成

CE の構成を図 5 に示す．CE は属性情報，ボディ，動作の３つを主な構成要素とする．属性情報は，CE 自身に関する情報で，ボディは CE が提供するサービスを実際に実装したプログラムがあり，動作は CE の自律的な動作を定義・制御する．

特徴的な動作には，以下の２つがある．

24. energy exchange： CE は生存のためにエネルギーを必要とし，自分自身のエネルギーを管理する．CE は，他の CE に対してサービスを提供することによってエネルギーを獲得する．一方，リソースを利用する際の対価としてエネルギーを支払う．つまり，エネルギーは人間社会における金銭のような役割を果たす．
25. relationship の形成： CE は，関連するサービスを提供する他の CE に対して relationship を形成する．この relationship 形成方法は重要なテーマである．
26. CE には，進化と適用のモデルがある．CE はエネルギーがなくなれば死ぬため，良い CE は残り，悪い CE は自然淘汰されて死ぬこととなる．

### 6-4) サービスコンセプト

同プロジェクトでは，成果の適用例として，以下の３つのサービスコンセプトを想定している．

#### 例 1：サービスのパーソナライズ

個人の嗜好や行動パターンに基づいて，サービスをパーソナライズする．例えば，ヘアサロンに関する情報を検索しているユーザ（を表す CE）が環境に対してサービス要求を出すと，ヘアサロンに関する Web ページをサービスとして提供する CE が応答する．サービスを提供する各 CE は，ユーザを表す CE とインタラクションすることで，そのユーザの関心や好みのヘアサロンなどの情報を取得する．この結果，ユーザの好みにマッチする度合が高いページ（CE）から順番にユーザの検索結果表示画面に表示する．

また，ヘアサロンの予約サービスを提供する CE が，ユーザのヘアサロンの予約頻度や行動パターンに基づいて次のヘアサロン予約の時期を予測し，その時期が近付くとユーザの周囲にサービスの複製を生成する．また，利用してくれたユーザとの間にリレーションシップを形成し，利用の頻度に応じてリレーションシップを強めることで，優先的にサービスを提供するようになる．

#### 例 2：動的なコミュニティの発生

個人の興味や嗜好，現在の位置，サービスのタイプ，利用傾向などの基準に基づいて CE の集団（コミュニティ）が自然発生・消滅する．コミュニティにおいてCEがインタラクションすることで新たなサービスを創発する．

例えば，ユーザが利用したサービス（CE）がユーザの携帯端末を移動手段とすることによって，ヘアサロンに関心を持っている客が多いレストランには，ヘアサロンに関する情報・サービスを提供する CE が集まりコミュニティが発生する．そして，コミュニティにおいて CE がインタラクションすることで，ヘアサロンに関心を持つユーザ向けの情報提供サービスなどが創発される．

このレストランに，ファッションへの関心が高い客が入ってくると，そのユーザが利用したファッション情報を提供する CE や，ファッションショーの優待チケットのCEがコミュニティに新たに加わるようになる．レストランの客が，ヘアサロンの情報とファッションの情報を組み合わせて利用するようになると，例えばヘアサロンを予約したユー

ザにはもれなくファッションショーの割引チケットをプレゼントするなどという新しいサービスが生まれる.

**例 3：スモールデバイスの自己組織化**

センサのようなスモールデバイスが自己組織化することで，強調して高度な情報処理サービスを提供する.

例えば，地理的に広範囲な場所にランダムに配置された複数のセンサ（センサを制御する CE）が，それぞれ自分の周囲の環境（他のセンサの出す情報や稼動状況など）をセンシングする．そして，センシングによって得られた情報を元に，自身の機能，センシングの頻度，場所（センサが移動可能な場合）などを調節することで，役割分担を行う.

### 6-5) プロジェクト構成

Bio-networking プロジェクトは，指導教授の須田達也教授の下，１名のポスドク，４名の博士課程，５名の学部学生，２名の研究員の合計１２名で研究を遂行している．同プロジェクトは，Bio-networking を実現するための重要な要素となる以下のサブプロジェクトに分かれ，取り組まれている．また，幾つかの研究課題については，NTT と共同で実施しており，実装や評価を NTT が担当しているものもある.

- Peer to Peer Discovery in Bio Net
  - キーワードと relationship に基づく CE の発見手法に関する研究.
- Platform Design
  - Bio-networking の実効環境であるプラットフォームの設計に関する研究
- Service Composition
  - 複数のサービスを統合して composite service として提供するための研究

また，将来の課題として以下が予定されている.

### 6-6) 関連するプロジェクト

Bio-networking に密接に関連する研究として，NTT みらいねっと研究所において，Bio-networking の基本コンセプトをベースとした Jack-In-the-Net(Ja-net)システムに関する研究が進められている[2].

Ja-net は，Bio-networking が進化の対象が CE(の動作)であり，その結果としての集団の創発を扱っているのに対し，これに加えて複数の CE 間のインタラクションを進化の対象とし，その結果として生じるサービスの創発も可能としている点が異なる．須田教授は NTT の研究員でもあるため，同システムにも密接に関与している．Ja-net 研究に関するホームページがないため，研究の進捗度合いやプロジェクトといして成立しているかは不明であるが，既発表の論文から推察すると，コンセプトの提示と研究要件の抽出を行い，いくつかの研究に着手しているところであると考える．

## 参考文献

27. M. Wang and T. Suda, "The Bio-Networking Architecture: A Biologically Inspired Approach to the Design of Scalable, Adaptive, and Survivable/Available Network Applications," Proceedings of the 1st IEEE Symposium on Applications and the Internet (SAINT), 2001.
28. T. Suda, T. Itao, T. Nakamura and M. Matsuo, "Adaptive Networking Architecture for Service Emergence," the Trans. Inst. Electronics Commun. Engineers of Japan (IECEJ), Invited Paper, Vol.J84-B, No.3, pp.310-320, 2001. (in Japanese)

# 5.2 セキュアコンピューティングの基盤となるハードウェアの研究開発

## 5.2.1 平成 13 年度の成果概要

ユビキタスコンピューティング環境および，ユビキタスネットワーキング環境の発展を背景として，社会のあらゆる場面をコンピュータ化することで，社会を効率化しようとしている．

近年，インターネットでは，いわゆる「クラッカー」等の悪意ある輩により，また悪意ある人物によって流通させられた各種ウィルスやワームが蔓延している．インターネットに接続された各種コンピュータは，日常的に不正アクセスが試みられ，コンピュータ自体，またそのコンピュータから操作できる機器に対して，ネットワークを介して不正操作がおこなわれている．

ユビキタスコンピューティング環境，ユビキタスネットワーキング環境においては，あらゆる場面がコンピュータ化される．こうした環境で，現在のインターネットのような不正利用が行われた場合，我々の生活を根底から脅かされることになる．従って，ユビキタス環境において，セキュリティーを確保することは重要な課題である．

一方，ユビキタス環境では，政治，経済，文化といったあらゆる分野をデジタル情報で表現し，コンピュータやコンピュータネットワークの上に実現しようともしている．社会が機能するための重要な仕組みの一つに価値情報の流通がある．例えば，現代社会における最も重要な価値情報は「貨幣」であり，その他にも各種証書，証券，チケットなどがある．これらが実効性を持つためには，オーソライズされた者以外が偽造できないこと，流通時に改変されないことが保証されなければならない．例えば，貨幣は，各人が勝手に作りだしたり，改変して金額を増やしてはいけない．ところが，デジタル情報は，本来，情報品質を劣化させることなく完璧に内容を複製・変更できるため，こうした価値情報を改変させないことは，根本的に難しい．

デジタル情報に対する操作を制限したり，ネットワーク経由での各種不正を防ぐことは，ソフトウェアだけでは不十分であり，ハードウェアによる支援が不可欠である．現在は，耐タンパー性をもったハードウェアを使うことで，こうした支援を行うことができる．

そこで本研究開発プロジェクトでは，ユビキタスコンピューティング環境に埋め込むためのセキュリティーチップとして，SDCC（Secure

Data Carrier Chip）の研究開発に取り組んでいる．SDCC は有線の通信チャンネルを持つ接触型のチップと，無線の通信チャンネルを持つ非接触型のチップがある．本年度はまず，現状の技術で実現可能な，接触型の SDCC を構築した．SDCC の基本アーキテクチャとしては，トロンプロジェクトで基礎研究がすすめられた，eTRON（Entity TRON）の方式を採用し，その仕様を満たす接触型の SDCC を開発した．

### 5.2.2 セキュア・データ・キャリア・チップ(SDCC: Secure Data Carrier Chip)の研究

#### １）はじめに

コンピュータ化された社会で用いるデジタル化された価値情報を安全に格納し，デジタル情報インフラ上で流通させるために，耐タンパーハードウェアを核技術とした，セキュアな広域分散システムアーキテクチャとして eTRON（Entity TRON)が提案されている[1)]．

耐タンパー性をもったハードウェアはカード状に実装されたものが多く，IC カードやスマートカードと呼ばれ，銀行のキャッシュカード，クレジットカード，公共交通システムのパスといった，貨幣に関連する情報を格納するデバイスとして広く使われている．IC カードやスマートカードを使ったセキュアシステムは，応用を限定した専用システムとして構築され，アーキテクチャやシステム構成はクローズなものが多く，またそれによって信頼性を確保している．

ところが，近年インターネットのようなオープンでかつ，信頼性は低くとも高い普及力をもった情報インフラの普及に伴い，オープン環境でも価値情報を安全に流通させたいという要求が高まっている．そこで，eTRON は，オープンな情報インフラ上で安全な価値情報流通を実現することを目標とする．そのため，eTRON の枠組みは必然的に分散システム全体を包含することになる．そこで用いられる耐タンパーデバイスも，分散システムの一部として位置付けた設計がなされている．

#### ２）eTRON アーキテクチャ

eTRON（Entity TRON）は，インターネット等のオープンな通信基盤上で，耐タンパー性を有するハードウェアを利用し，価値情報を安全に流通させるための広域分散システムアーキテクチャ（図 5.2.2-1）である．

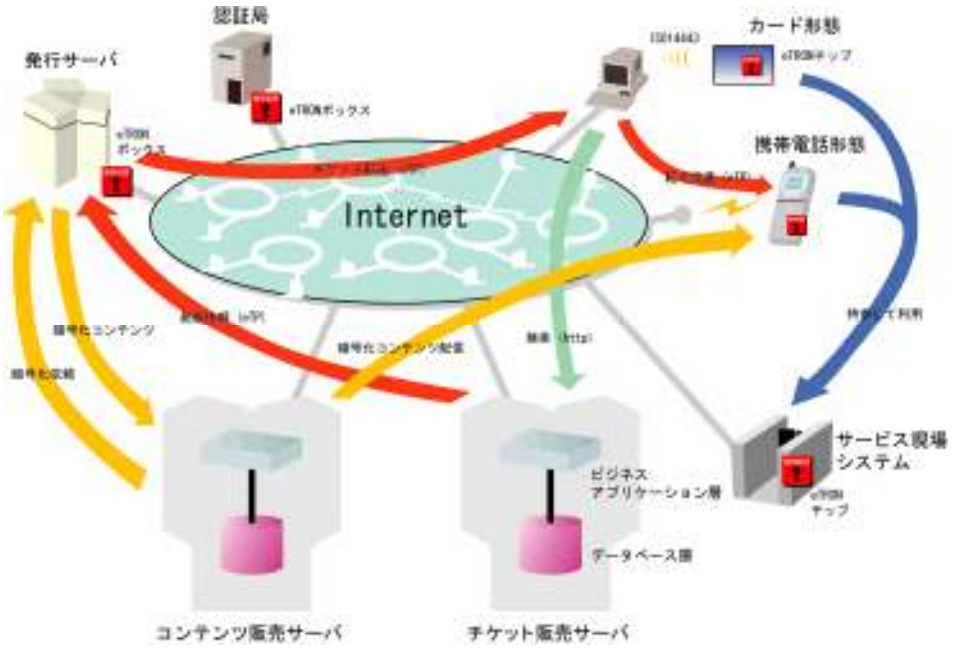



図 5.2.2-1：eTRON アーキテクチャ

eTRON アーキテクチャには次の特徴がある.

**◆多目的**

eTRON は，特定アプリケーション用のアーキテクチャではなく，価値情報を交換する汎用的なアーキテクチャである．この上で，複数のアプリケーションを同時に扱うことができる.

**◆分散アーキテクチャ**

eTRON では価値情報は，サーバに集約する方式ではなく，各ユーザが分散して保持する**分散型アーキテクチャ**を採用した.

**◆Peer-to-Peer**

価値情報を格納するエンドノードが Peer-to-peer で通信する．これにより，エンドノード間の通信経路途中での，暗号や署名のデコードが不要になるため，エンドノード間の通信基盤は単なる通信路を提供するだけになる．これによって，オープンな通信路上での価値情報の安全な流通が可能にある.

**◆耐タンパーハードウェアの利用**

各エンドユーザが持つ価値情報の格納デバイスには，耐タンパー性

を有するハードウェアを用いる．携帯端末やカードに組込むための **eTRON チップ**,据え置き型の大容量ストレージとしての **eTRON ボックス** がある．

**◆価値情報の転々流通機能**

eTRON では，eTRON チップ／eTRON ボックスに格納された価値情報をユーザ間でやり取りする際には，サーバを介さずに当事者間で行うこと，つまり価値情報の**転々流通**，を可能にする．

**◆単一価値情報の分散分割格納機能**

各ユーザが所有する耐タンパーデバイスに格納できない大きなサイズの情報を扱うために，eTRON では，単一価値情報を，複数のノードに分散して格納し，互いにリンクで接続することができる．各ユーザが所有する耐タンパーデバイスに格納できないような，大きい情報を扱う時に有用である．

**◆PKI（Public Key Infrastructure）**

eTRON はノードが公開鍵暗号系の認証や暗号を扱うための **PKI（公開鍵暗号基盤）** を含んでいる．

**３）SDCC の概要**

**SDCC** は，上記の eTRON アーキテクチャに基づき，本研究所のユビキタスネットワーキング環境実現を実現するエンドノードを構成する重要な要素で，耐タンパー性を持ったハードウェアである．ユーザが Valuable Entity を格納するために用いる．**SDCC** は，カード型に実装したり（**SDCC カード**），また携帯電話のようなモバイル端末や，家電製品などに組み込んで，それらの機器が安全に Valuable Entity を扱えるように用いる．

**◆分散環境ノードしての SDCC**

**SDCC** は既存のスマートカードとは異なり，コンピュータの周辺機器ではなく，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バや他の **SDCC** と，コンピュータネットワークを介して peer-to-peer で通信する．**SDCC** インタフェース装置（**リーダライタ**等）は，さほど信頼性が高くない，単なるゲートウェイで十分である．

**◆eTRON ID で特定する相互認証方式**

SDCC は eTRON 仕様に基づいたチップであり，eTRON システム全体の中で唯一の識別子（**eTRON ID**）を持つ．チップを物理的に識別するだけでなく，チップへの通信の経路制御にも利用される．SDCC と通信セッションを構築する際には，相互認証がなされ，相互に確実に相手の eTRON ID が把握される．IP などの通信でも相互に IP アドレスを把握し，それに基づいたアクセス制御などが行われる．しかし，IP アドレスはパケットの改変などにより簡単に Address Spoofing が行えることに脆弱性がある．SDCC では PKI を用いて eTRON ID の正当性を認証するため，高い信頼性がある．

**◆eTRON ID に基づいたアクセス制御リスト方式による統合的な資源保護機構**

SDCC は，相互認証によって通信相手の eTRON ID を高い信頼性で特定できる．そこで，SDCC がチップ持つ資源を保護するために，この eTRON ID に基づいたアクセス制御リストを提供する．SDCC では，セッションを張った相手の eTRON ID に応じて，資源に対して，**発行者（ISSUER）**，**所有者（OWNER）**，**それ以外（OTHERS）**という属性が決まる．さらに，アクセス制御リストによって，発行者・所有者・それ以外が発行可能な命令を制限することができる．

価値情報の格納庫に対する操作権限として重要な性質は，価値情報の発行者と所有者が相互に信頼しないことである．つまり，情報の発行者だけができる操作，情報の所有者だけができる操作といったものをこの資源保護機能によって実現しなければならない．SDCC では，上記の資源保護機構によって，以下のような情報管理が可能になる．

- 情報の所有者は変更できずに情報の発行者だけが変更できる情報（例：電子チケットの座席番号）
- 情報の所有者に見せない情報（例：電子チケット変更の鍵）
- 情報の所有者だけが完全に制御できる情報（例：所有者の個人情報）
- 誰でも読める情報（例：鉄道定期券の区間情報）

SDCC では，アクセス制御リストの中で，所有者，発行者，その他のサービスクライアントを統一的に扱い，それぞれのもつ権限に応じて，アクセス制御リストを変更する API を発行することによって，アクセス権限の制限や解放，委譲といった制御を柔軟に行うことを可能にし

ている．

**◆転々流通のためのチップ間通信**

eTRON アーキテクチャでは，サーバーを介さず，価値情報を格納した eTRON ノード間で直接情報を交換することができる（**転々流通**）．SDCC は，チップ間で直接価値情報を安全に交換するために，SDCC 間で直接ピア・ツー・ピア通信できる機能をもっている．

**◆ロールバック可能なトランザクション機構**

SDCC への価値情報の移動は，安全に行う必要がある．SDCC では，特に価値情報の作成・削除に関しては，処理の原始性を保証するトランザクション機構を提供している．トランザクション処理中にアボート命令が発行された場合，またコミット命令がタイムアウトした場合は，トランザクション処理は**ロールバック**（roll-back）される．ネットワーク上にトランザクションコーディネータを置ける場合は，**二層コミットプロトコル**（Two-Phase Commit Protocol）も対応できる．

**◆リンク機能を持った記憶構造**

現在，耐タンパー性をもったチップは，まだ利用可能な資源が乏しいため，想定するアプリケーションの全ての価値情報を SDCC に格納できない場合もある．そこで，SDCC ではコンテンツを複数の **eTRON コンテンツホールダ**，例えば，SDCC とネットワーク上の eTRON ボックスの間で分散して保持し相互の間にリンクを設定することが可能である．

**４）SDCC の実装**

我々は上記の特徴を持った SDCC を用途に応じていくつか構築しようとしている．これらは互いに外部インタフェースレベルで互換性を持つように設計されている．

まず，我々は平成 13 年度には，16bit のマイクロコントローラを使った非接触型の SDCC を開発した．SDCC はカードとして実装され，接触通信の ISO/IEC 7816 インタフェースを有する．これは，まだ大量の計算機資源を持たないため，一部の eTRON 仕様の特徴を備えていない，マイクロ eTRON であると位置付けている．現在，上記の特徴を完全に備えた，次世代の SDCC の開発を進める予定である．

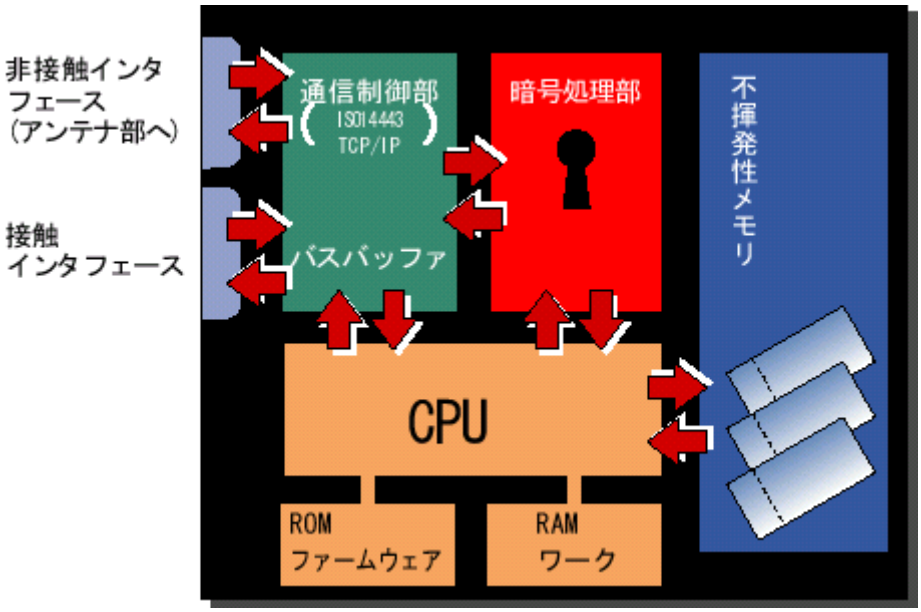



図 5.2.2-2：SDCC の構成


図 5.2.2-3：SDCC カード（１）


図 5.2.2-4：SDCC カード（２）

## 参考文献

29. Ken Sakamura and Noboru Koshizuka: ″The eTRON Wide-Area Distributed-System Architecture for E-Commerce″, IEEE Micro, Vol. 21, no. 6, Dec., 2001, pp. 7～13.

# 5.3 基盤通信システムの研究開発

## 5.3.1 平成 13 年度の成果概要

本サブテーマのミッションは，ユビキタスコンピューティング環境を構築するベースとなる，基盤通信システムの研究開発を行うことである．ユビキタスコンピューティングのプロトコルは，すべての層に及ぶが，今年度は，全体の中で，以下のプロトコルの構築に取り組んだ．

**１）ネットワーク層**

ユビキタスコンピューティング環境でしばしば用いられるネットワーク層のプロトコルクラスに，アドホックネットワークプロトコルがある．アドホックネットワークとは，複数の自律的な計算・通信ノードを集合させたときに，これらのノード間の通信経路を自動的に構成するメカニズムである．本年度は，ユビキタス環境に適したアドホックネットワーキングプロトコルに関する研究を行った．（⇒**「5.3.2 アドホックネットワーキングの研究」**）

**２）セッション層**

ユビキタスコンピューティング環境上で安全な通信路を構成するセッションプロトコルとして，価値情報転送プロトコル（VITP: Valuable Informatiaon Transfer Protocol）の研究を行った．（⇒**「5.3.3 価値情報転送プロトコルの研究開発」**）

**３）プレゼンテーション層**

ユビキタスコンピューティング環境では，インターネットを構成する IP のように，位置や物理的な環境を完全に仮想化するだけでなく，実世界と密に連携する通信を行うことを目指している．従って，コンピュータネットワーク上で，現実の物理的，社会的状況（コンテクスト）が交換できることは，きわめて重要性が高い．これは，従来型のネットワークシステムのリファレンスモデルに基づくと，プレゼンテーション（表現）層に相当する部分である．そこで，本年は，ユビキタスコンピューティング環境にとって重要なプレゼンテーション層構築のための研究開発として，人間の属性の表現に取り組んだ（⇒**「5.3.5 ユビキタスネットワーキング環境における個人属性情報」**）．また，ユビキタスコンピューティング環境の重要な応用として，交通機関があ

るが，この交通機関にユビキタスコンピューティング環境を適用するために必要な属性表現に関する研究を行った（⇒「5.3.4 ユビキタスネットワーキング環境における交通チケットコンテンツ方式」）．

## 5.3.2 アドホックネットワーキングの研究

### １）概要

将来的なユビキタスネットワークでは，ユビキタス空間に多数存在するユビキタス・ノードを設定なしに接続する手段が必要となる．これらのノード間がすべて直接接続できない場合，間接的に通信を行う必要があり，そのためにはアドホックネットワークと呼ばれる技術が重要となる．具体的には，①アドホックネットワークを実現するためのルーティング技術，②アドホックネットワークにおける名前解決方式，および③アドホックネットワークにおけるサービス発見方式が重要であると考えられる．本章では，これらアドホックネットワークに重要となる技術についての研究を報告する．

①アドホックルーティング技術については，現在の研究で主流となりつつあるルーティングプロトコル AODV (Adhoc On-demand Distance Vector)について，シミュレーションを行い，ユビキタス環境への適用性を検証する．次に，②名前解決方式に関しては，アドホックネットワーク用に，自律分散により名前解決を実現する方式を考案し，その性能をシミュレーションにより確認した．最後に③アドホックネットワークにおけるサービス発見方式については，AODV 的な発想に基づくマルチホップサービス発見方式を考案し，その性能をシミュレーションにより確認した．

### ２）アドホック用オンデマンド型距離ベクトルルーティングプロトコルの評価

#### 2-1）概説

アドホックネットワークにおける主なルーティングプロトコルは図に示すように，通常の固定網のようにあらかじめルーティングテーブルを作成しておく事前作成型と通信が必要になった段階で経路を生成するオンデマンド型に別れる．事前作成型はさらに通常の IP ルーティングのように距離ベクトル型とリンク状態型に分類される．事前作成型とオンデマンド型の各方式にはそれぞれ長所と短所があり，ノードの移動が遅く，通信相手の数が多いときには事前作成型が，逆にノードの移動が速く，通信相手の数が少ないときにはオンデマンド型が有

利であるといわれている．ユビキタスネットワークにおいて特に考慮すべき点は，

- 接続ノード数が多くなった場合にも効率的にルーティングできること．
- サイズやコストの面から記憶容量が制限される可能性がある．

ことである．アドホックネットワークに関する研究報告のほとんどは 20 から 50 ノード程度の規模であるが，ユビキタスネットワークに適用する場合には 100 ノードを越える規模のネットワークも考慮の対象とする必要がある．また，事前作成型の場合には，通信の有無にかかわらずネットワークの規模に応じてルーティングテーブルのサイズも大きくなることと，ルーティングテーブルを維持管理するための制御メッセージがネットワークに対する負荷となることが問題となる．一方オンデマンド型の場合には通信開始要求があってからルートを探索するため，実際に通信が開始する時間が事前作成型より多くかかるが，通信に必要な経路情報のみを保持するため，スケーラビリティの面から事前作成型よりも有利と考えられる．IETF (Internet Engineering Task Force)においても MANET (Mobile Adhoc NETwork) ワーキンググループの中で種々のルーティングプロトコルが提案されている（**図 5.3.2-1** の＊のついたもの）．特にオンデマンド型の AODV (Adhoc On-demand Distance Vector)は研究論文も多い．

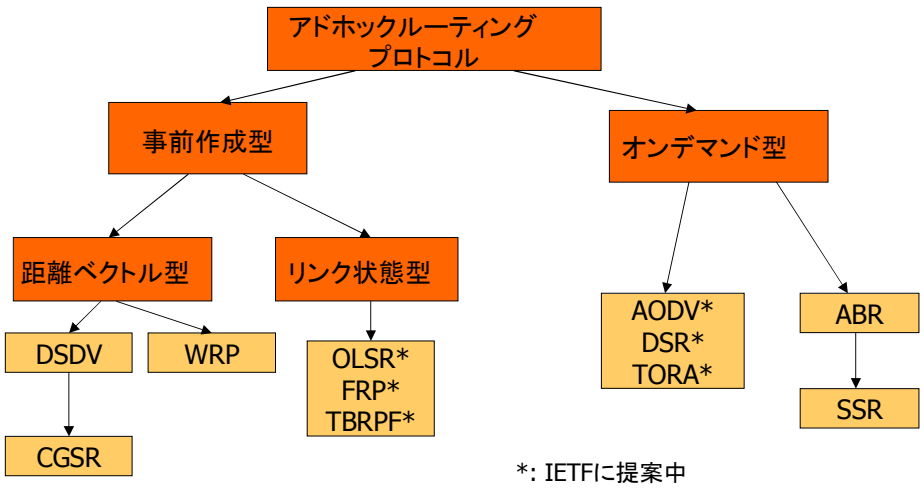



図 5.3.2-1：アドホックネットワークにおけるルーティングプロトコル

そこでここでは，オンデマンド型のアドホックルーティングプロト

コルとして AODV を取り上げ，ユビキタスネットワークを想定した多数ノード環境におけるプロトコルの性能を計算機シミュレーションにより評価を行う．シミュレーション結果をもとにユビキタスネットワークにおいて必要となる機能について考察する．

### 2-2) シミュレーション概要

#### ■AODV プロトコルの概要

AODV では，送信ノードにおいて通信の要求が発生した時点で，宛先までの経路（パス）を形成する．この処理をパス発見(Path Discovery)とよび，**図 5.3.2-2** に示すように送信ノード(S)がルート要求(Route Request または RREQ)メッセージに宛先ノード(D)の IP アドレスを格納してブロードキャストする．この RREQ を受信した隣接ノードはそれが自分宛ではない場合には同様にして再ブロードキャストする．このとき，RREQ を受信したノードは送信ノードと直接通信可能なことがわかったため，宛先ノードとは逆の送信ノードへパス（逆方向パス）を形成する．このようにして RREQ はアドホックネットワーク内のノードを経由し，逆方向パスを形成しながら宛先ノードまで到着する．

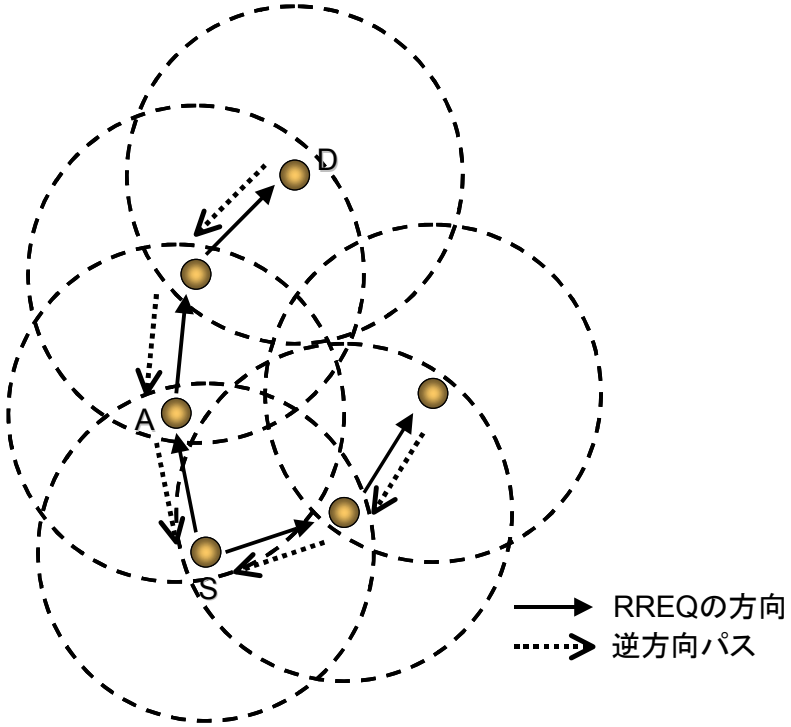



図 5.2.2-2：：逆方向パス設定

RREQ が宛先ノードに到達した時点で，送信ノード(S)から宛先ノード(D)までの逆方向パスが完成する．宛先ノードは RREQ が自分宛である

と判断すると，ルート応答(Route Reply または RREP)メッセージに送信ノードの IP アドレスを入れて，送信ノードへの逆方向パスからネクストホップ，すなわち RREQ を送信した隣接ノードにユニキャストで送信する．RREP を受信したノードは，この時点で**図 5.3.2-3** に示すように宛先ノードへのパス（順方向パス）が形成される．このようにして RREP が送信ノードに到達した時点で送信ノードから宛先ノードまでの双方向パスが形成される．これにより送信ノードは，宛先ノードに対してデータを送信することが可能となる．RREQ はブロードキャストを繰り返してネットワーク内で配送されていくが，宛先 D に到達しない可能性がある．各ノードは逆方向パスに対する有効期間(REV_ROUTE_LIFE)を持ち，この期間内に RREP を受信しなかった場合には逆方向パスが削除される．

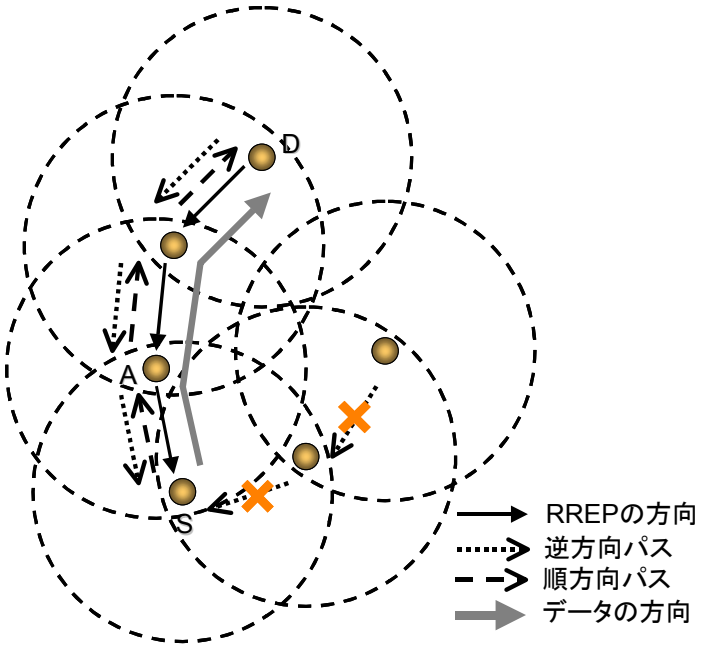



図 5.2.2-3：順方向パス設定

AODV では，中継ノードがすでに宛先ノードへのパスを知っている場合には，受信した RREQ に対して，即座に RREP を応答することが可能である．これは制御メッセージ数の削減およびパス確立の時間の短縮を図ることを目的とした処理である．また，送信ノードは複数の RREP を受信することもあるが，その際には宛先までのホップ数（RREP に格納されている）の小さい方を選択する．たとえば，**図 5.3.2-4** においてノード B とノード E の間にすでにパスが確立されている状況でノー

ドAがノードE宛のRREQを送信した場合には,ノードBにおいてRREPがノードA宛に送信される．これによりノードA-E間にA-B-C-D-Eというパスが確立する．RREQはフラッディングされるため，ノードFおよびEにも転送される．ノードEもノードAに対してRREPを送信するが，ノードAはノードEまでのホップ数を比較して，ノードE間でのパスをA-F-Eに変更する．

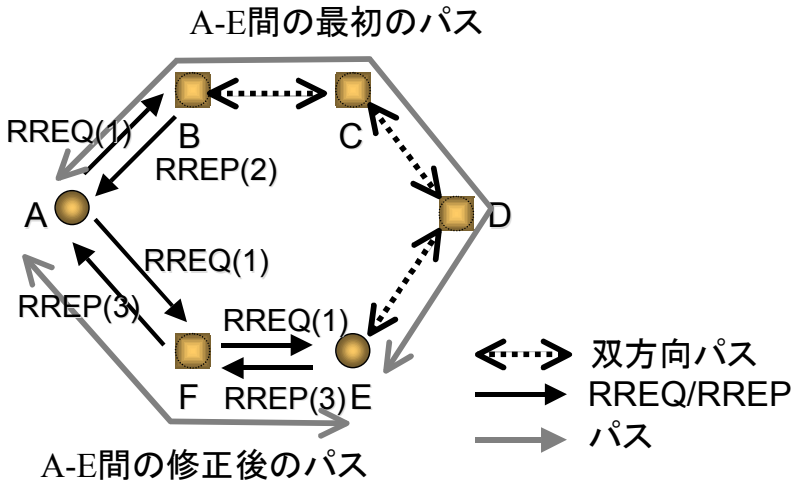



図 5.3.2-4: 最小ホップ数のパス選択

また，送信ノードがRREQを送信して一定期間(RREP_WAIT_TIME)内にRREPが到着しなかった場合にはRREQを再送する.AODVでは,RREQの到達範囲(TTL)を段階的に広げることにより，パス確立時のフラッディングによる通信帯域の負荷を軽減する手法をとっている（リングサーチと呼ばれる）．最初に送信されるRREQのTTLは初期値(TTL_START)に設定され，このホップ数内に宛先ノードがいる場合には，最も効率良くフラッディングを抑制することが可能となる．この時点でRREPによる応答がなかった場合にはTTLを一定増分(TTL_INCREMENT)だけ増加させてRREQを再送する．TTLが閾値(TTL_THRESHOLD)に達しても応答がない場合には,TTLをその最大値(NET_DIAMETER)に設定して再送する．ここから一定回数(RREQ_RETRIES)再試行してもパスが生成されなかった場合には，宛先ノードへの到達が不可であることを上位層に通知し，パケットを廃棄する．一般に送信ノードと受信ノードが必ずしも近くに位置するとは限らないと考えられ，アドホックネットワークにおいてこのようなリングサーチによるパス発見が有効であるかは立証されていない．また，AODVではNET_DIAMETERを越えるノードとは通信ができないた

め，このパラメータは最も重要な要素の一つである．

一度生成されたパスは，ユーザデータが流れている間はアクティブ状態であるとしてルーティングテーブルに継続して登録され，一定期間(ACTIVE_ROUTE_TIMEOUT)データが流れなくなると，ルーティングテーブルからは参照されなくなるがノード内には保持しておく．この時点から一定期間(DELETE_PERIOD)内に再度データが到着した場合には，パス発見の処理をせずにルーティングテーブルに再登録する．逆に，この期間内に利用されなかった場合にはそのパスを完全に削除する．また，パスを形成するノードの移動により，パケットの転送が途中で失敗した場合には，転送に失敗したノードが送信元ノードに向かってルートエラー(Route Error または RERR)メッセージを送信元ノード宛にユニキャストで転送する．送信元ノードが RERR メッセージを受信した場合には，再度パス発見を行う．

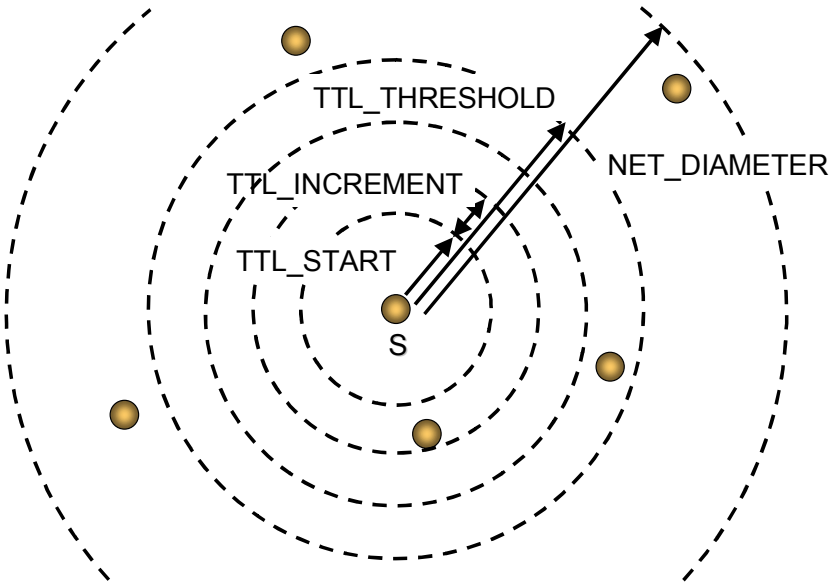



**図 5.3.2-5**：リングサーチと RREQ の再送

上記が AODV における基本的なパス形成とデータ転送の原理であるが，このほか RREQ のループを防ぐためのブロードキャスト ID，逆方向パスを維持・管理するための送信元シーケンス番号，順方向パスを維持・管理するための宛先シーケンス番号などが定義されている．

アドホックネットワークにおけるルーティングアルゴリズムは AODV に限らず，ルーティングテーブルまたはパス形成をするためのメッセージをネットワークの一部または全体にブロードキャストを繰り返す

フラッディングを基本とする．一般にフラッディングは通信資源を多く消費する処理であることから，相互のパス形成やユーザデータの転送への負荷が問題となる．本シミュレーションではこの点に着目し，パス形成の成功率やユーザデータのスループット，遅延時間に関する評価を行う．

**■ノード数と空間モデル**

- 室内モデル
  会議室のような室内を模擬するモデルで，一辺が 20ｍの正方形の領域内にノードが配置され移動する．ノード数は 5 ノード，10 ノード，20 ノードの 3 通りについて評価を行う．
- 屋外モデル
  屋外を模擬するモデルで，一辺が 1Km の正方形の領域内にノードが配置され移動する．ノード数は 50 ノード，100 ノード，200 ノード，300 ノードの 4 通りについて評価を行う．

**■移動モデル**

ノードの移動モデルはいくつか提案があるが，よく利用されているのがランダムウェイポイントモデルである．このモデルでは，各々のノードは規定の領域内でランダムに目標点の座標を定め，規定の最大速度以下のランダムな速度で，目標点まで等速直線的に移動する．目標点に到達した時点で，規定の静止時間だけ静止したのち，次の目標点を定めて移動する．この他のモデルとしてランダム方向モデルも提案されており，目標点の座標のかわりに領域の横軸を基準とした角度を 0～359° の範囲でランダムに選択する．ノードが領域の境界まで移動し一定時間静止した後，0～180° の範囲で次に移動する角度を選択し移動を開始する．

実際の移動形態が規定しにくいことから，移動モデルについての妥当性を検討することは困難であるが，アドホックネットワークに関する多くの研究においてランダムウェイポイントモデルが利用されていることから，本シミュレーションにおいても本モデルを採用する．また，移動速度の最大値に関して，室内モデルについては低速(5Km/h，歩行速度)，屋外モデルについては中速(20Km/h，自転車)および高速(60Km/h，自動車)について評価を行う．

**■通信モデル**

本シミュレーションで利用する通信モデルを以下に示す.

30. イーサネットフレームのペイロードサイズを 512Byte 固定とする.
31. トラヒックモデルは固定長のパケットを一定間隔で送信する CBR (Constant Bit Rate)とする.
32. 1 コネクションの通信速度は 64Kbps, 384Kbps, 1.5Mbps とする. また, ベアラ速度は 2Mbps とする.
33. 1 つのコネクションが転送を開始・終了するまでの時間は 1 秒および 10 秒の 2 通り評価する. 前者はトランザクション的な利用, 後者はストリーミングなど連続通信を模擬するモデルを想定する.
34. 通信頻度（同時に通信を行っているノードの割合）は, 全ノードのうち任意の 1 秒間に同時に通信しているノードの数が 10%, 30%および 50%となる 3 通りの場合を試行する.

**■評価項目**

本シミュレーションでは, 以下に示すデータを取得する.

35. 制御パケット数：一つのパスを確立するのに送受信された RREQ および RREP の数の平均値
36. データパケット数:ひとつのセッションを流れるユーザデータパケットの総数
37. スループット:一つのセッションにおいて受信側が受信するデータ量(バイト)を受信側での転送開始から終了までの時間で割った値.
38. 転送時間:任意のパケットについて受信側での受信時刻から送信側での送信時刻を引いた値の平均値. 送受信間の遅延時間を表す.
39. 誤り率:ひとつのセッションについて受信ノードで受信したパケットの総数を,そのセッションを介して送信ノードから送信したパケットの総数で割った値. ただし, パスが確立したセッションのみを対象とする.

**■その他**

一回のシミュレーション時間を 30 秒とし, 一つのパラメータセットにつき, 異なるノード配置で 4 回試行した結果の平均値を算出する.

シミュレーションソフトウェアとして ns-2.1b8[1]を用い, CMU による AODV 用の拡張ソフトウェア[2]を利用することとする. AODV プロトコルのバージョンはドラフトのバージョンは第 8 版[3]を利用する.

### 2-3) 結果と考察

■室内モデルについて

室内モデルにおいては，各ノードが他のすべてのノードと 1 ホップで到達可能となっている．通信頻度が 10%の場合，64Kbps から 1.5Mbps に渡ってほぼ通信速度と同等のスループットが得られていることがわかる．また，**図 5.3.2-8** からパス成功率についてもすべて 90%を超えていることがわかる．ただし，誤り率については**図 5.3.2-9** から 384Kbps 以上の通信速度になると大きくなり，とくに通信速度が 1.5Mbps で通信頻度が 30%以上の状況では誤り率が 80%を超えてしまう．上記の結果より，室内において無線 LAN を用いて AODV を利用した場合には，ノード数は 10 ノード程度，通信速度は 384kbps 程度が限界と思われる．

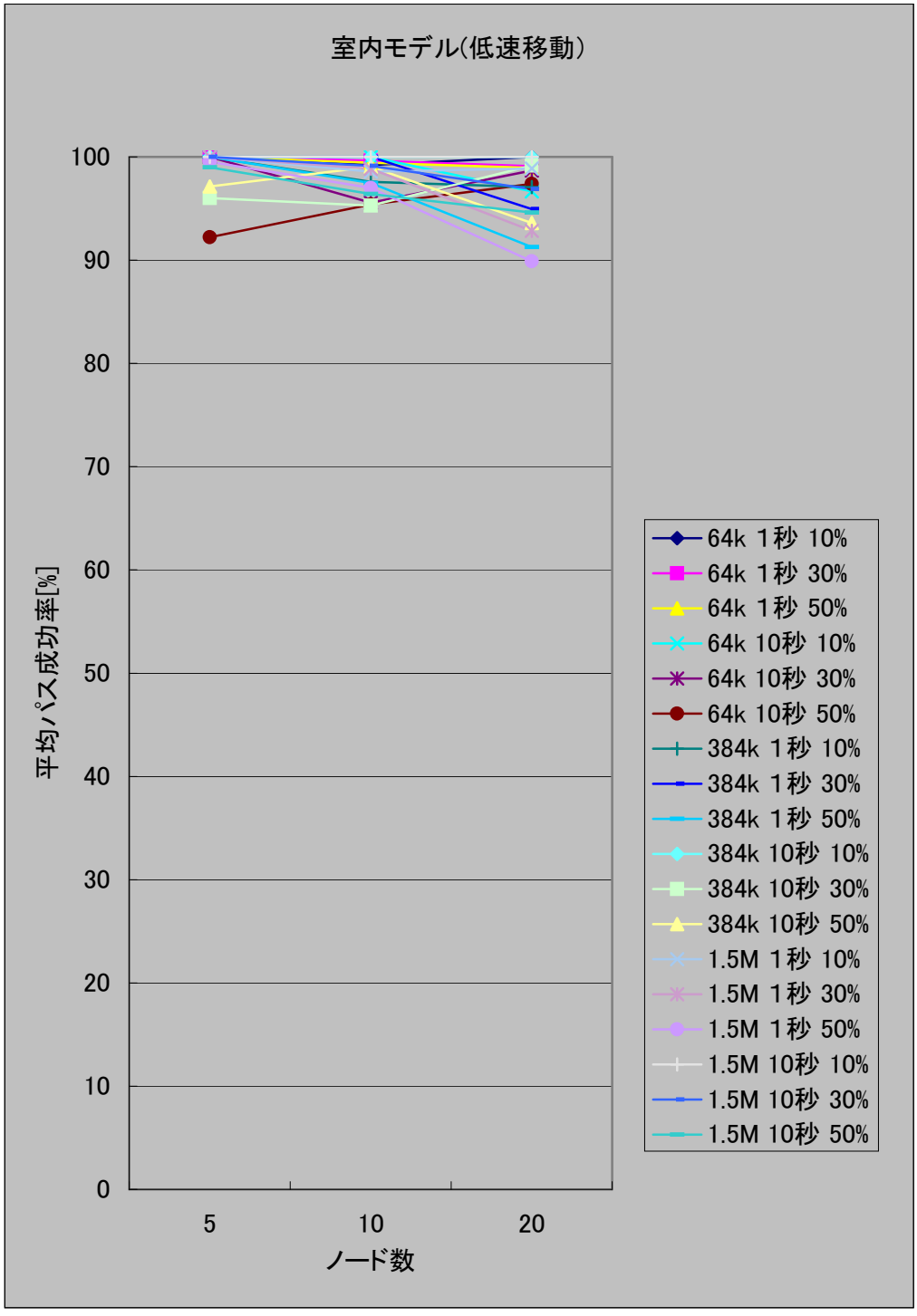



図 5.3.2-6：平均パス成功率（室内モデル）

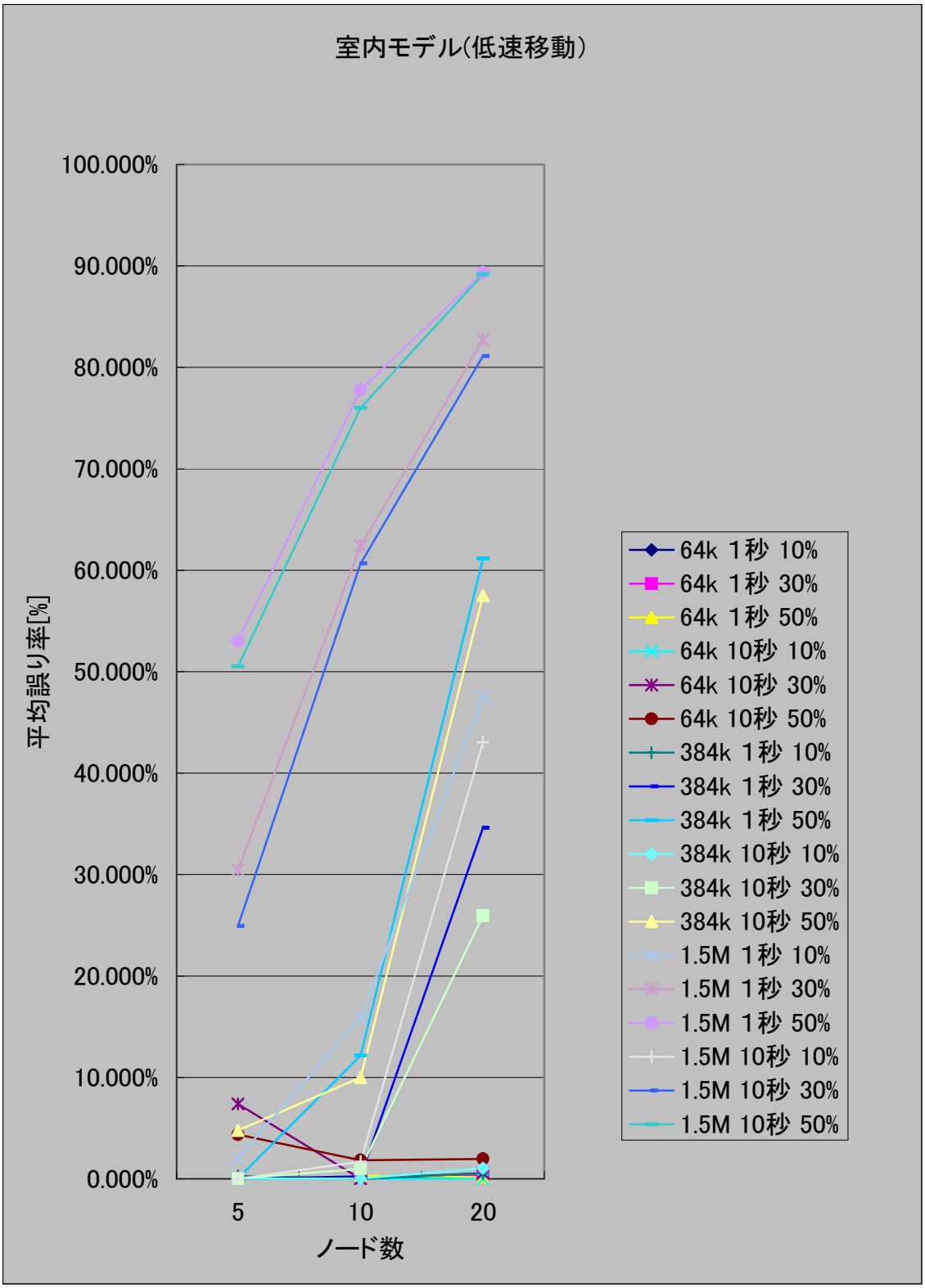



図 5.3.2-7：平均誤り率（室内モデル）

■屋外モデルについて

中速移動屋外モデルについては，**図 5.3.2-8** から 50 ノードの場合でも，通信速度が 1.5Mbps に対して最大スループットが 260Kbps 程度となり，十分なスループットが得られていないことがわかる．300 ノードにおいて 1.5Mbps，1 秒転送，通信頻度 50%の場合のスループットが，200 ノードで同条件の場合よりも高くなっているのは，300 ノードの場合ではパスが確立しても 1～2 パケットしか受信されていないために，連続して到着した数パケットによるスループットの計算値が高くなっているためである．実際にこのケースでのパス成功率は図 6 より 17%と著しく低い．また誤り率に関しては，300 ノードの場合 64Kbps で 40～50%，1.5Mbps では 98%にも達する．従って屋外モデルでは，ノード数は 100 程度，通信速度は 64Kbps 程度が限界と思われる．

**図 5.3.2-10** および**図 5.3.2-11** から，中速移動と高速移動の平均 RREP 数に 2 つのグループが見られる．上のグループは通信時間が 10 秒のケースで，下のグループは通信時間が 1 秒のケースである．この傾向は室内モデルでは見られない．これはノード数が多い屋外モデルではパスの成功率が低いため，RREQ の再送が頻発し，かつ RPEP が送信元ノードに到達する確率が低くなるために起こるものと思われる．通信時間が 1 秒で，かつ通信時間中にパスの確立が成功しない場合には，1 秒後にパス確立の処理を終了するのに対して，通信時間が 10 秒のケースでは最大再試行回数に達する可能性が高い．RREP に関して 200 ノードの場合よりも 300 ノードの場合のほうが少なくなっているのは，RREQ が宛先ノードに到達する確率が少なくなっていることが考えられる．

また，中速移動と高速移動のケースではあまり差が見られなかったが，中速移動では最大速度が 20km/h=5.6m/s，高速移動では最大速度が 60km/h=16.7m/s となり，通信時間が 1 秒の場合には，通信中に中速移動，高速移動についてそれぞれ最大 5.6m および 16.7m，通信時間が 10 秒の場合でそれぞれ最大 56m および 167m 移動する．無線 LAN の通信可能範囲の半径が 250m であることから，通信中に現在の通信範囲から外れる可能性はあまり高くない．したがって，無線 LAN において自転車で移動する程度の速度と自動車のそれではあまり通信特性の差がないといえる．

これらの評価結果から，ノード数が 100 を超えるような状況においては，パスの確立やスループットの面から見て AODV は効率的なルーティングを行うことは難しいと考えられる．他の多くのオンデマンド型

のアドホックルーティング方式もフラッディングを基本としているため，同様な傾向があるものと思われる．ユビキタスネットワークにおけるルーティング方式を設計する場合においては，フラッディングを極力抑制するなど，通信リソースの効率的な利用を考慮する必要がある．

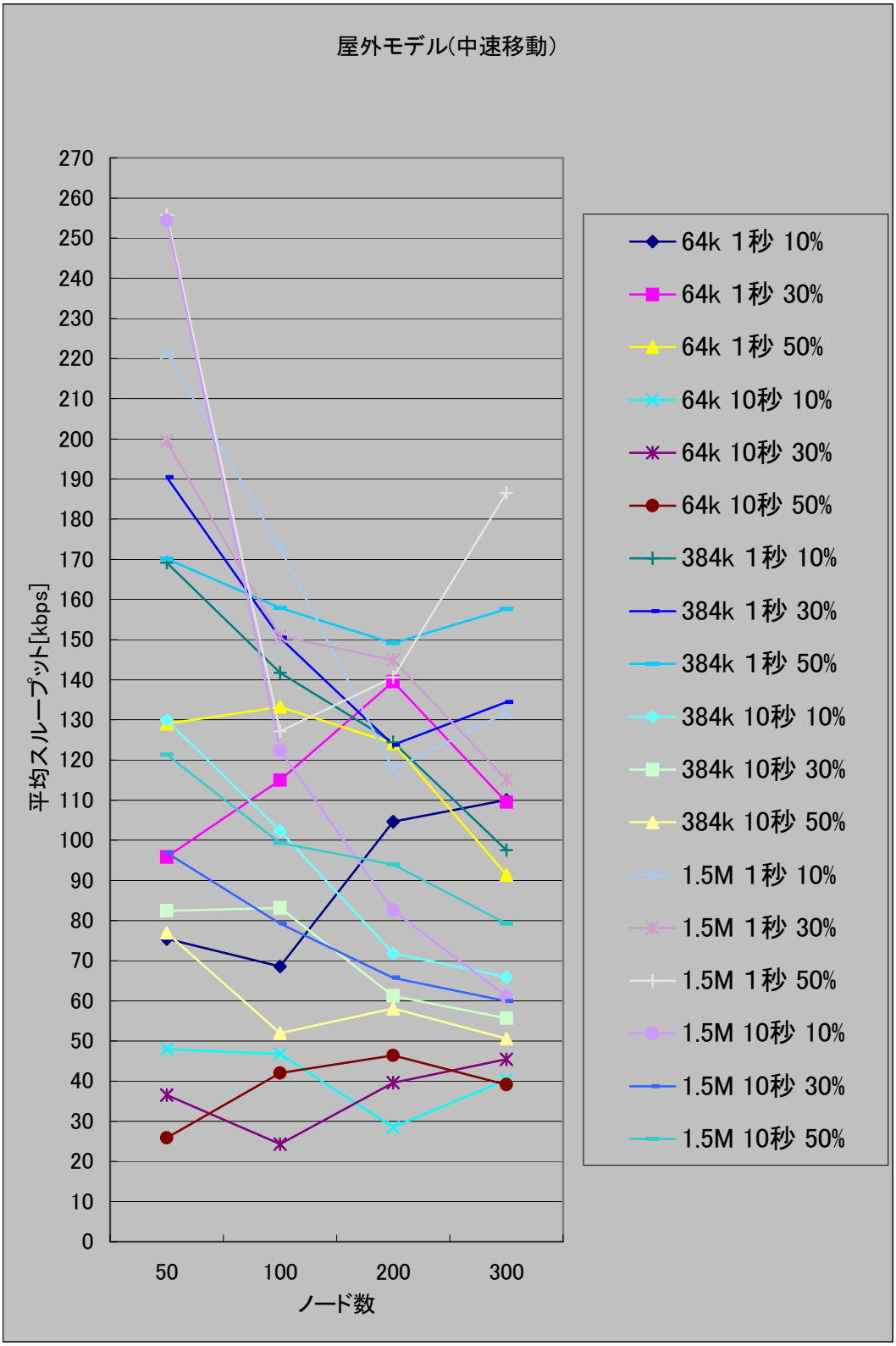



図 5.3.2-12：平均スループット（屋外モデル，中速移動）

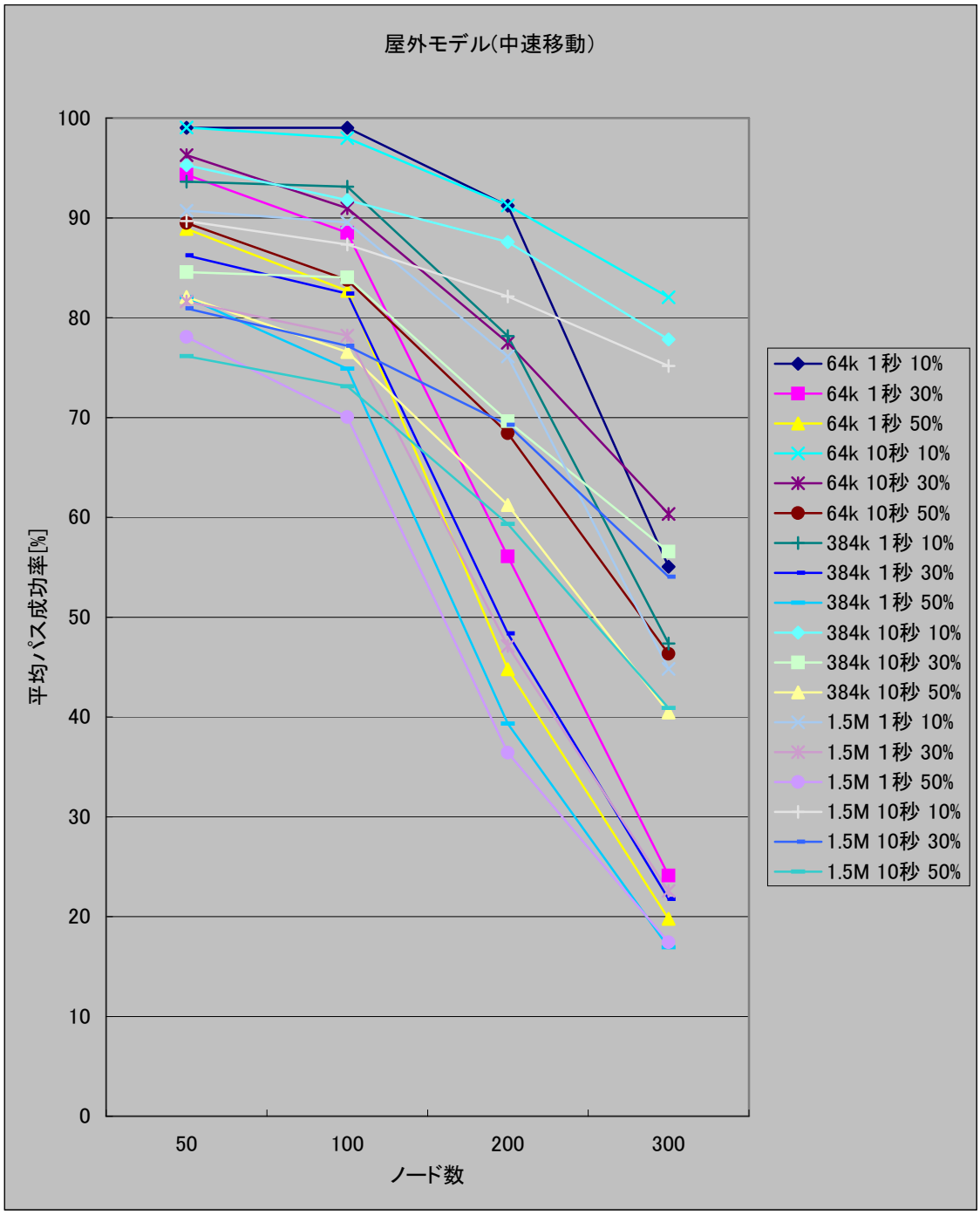



図 5.3.2-13：平均パス成功率（屋外モデル，中速移動）

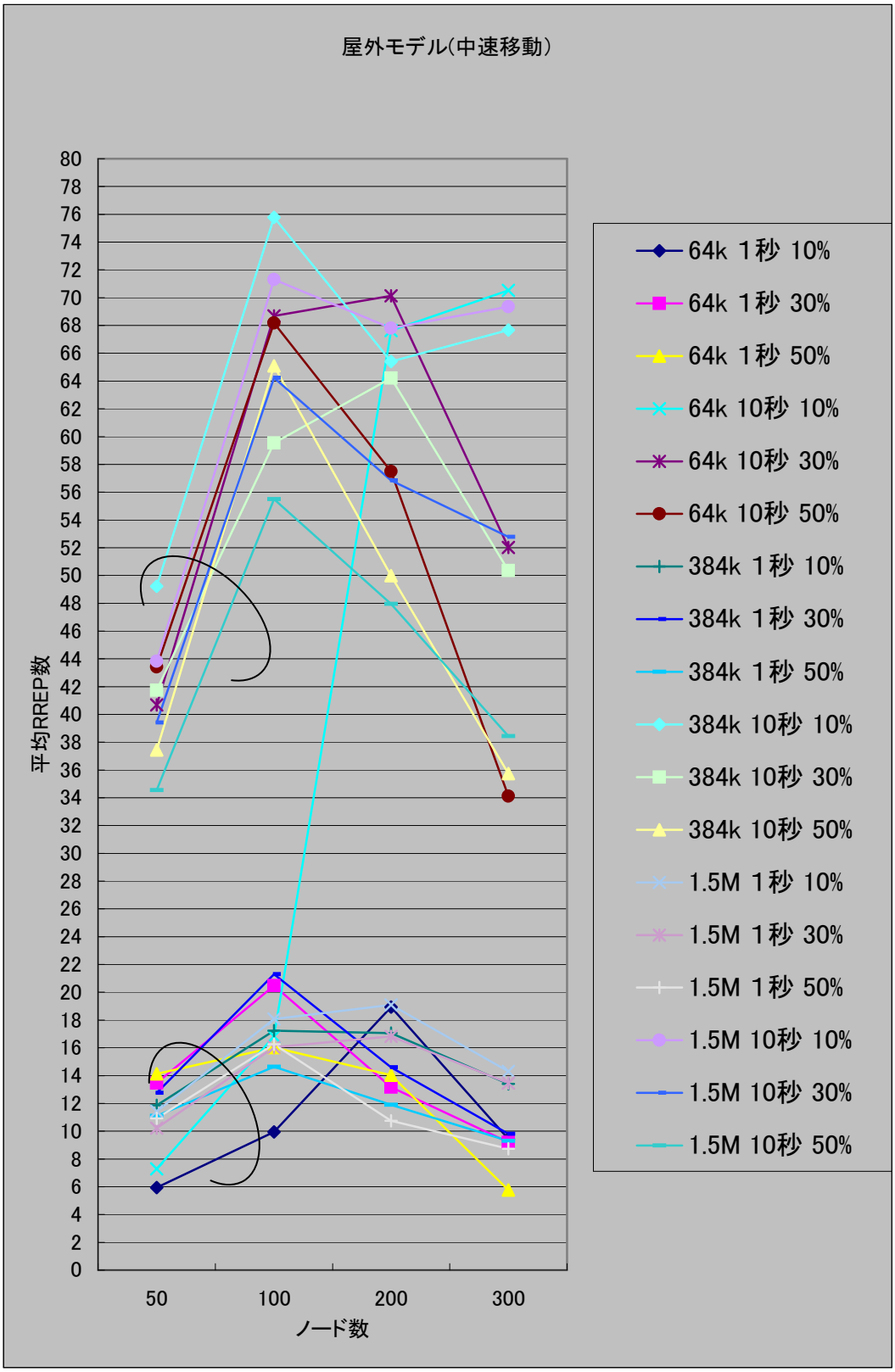



図 5.3.2-14：平均 RREP 数（屋外モデル，中速移動）

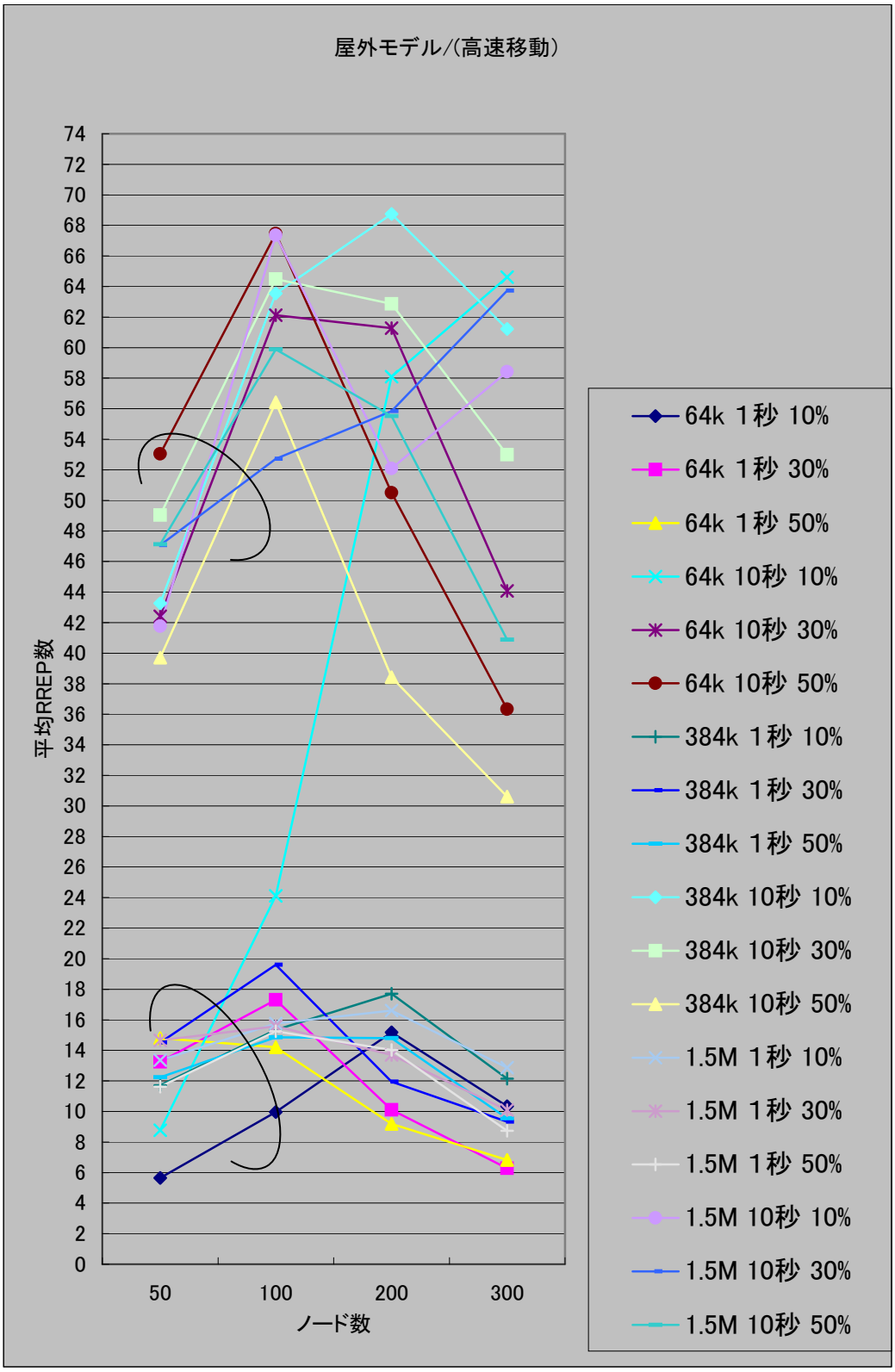



図 5.3.2-15：平均 RREP 数（屋外モデル，高速移動）

## ３）アドホックネットワーク用名前解決プロトコルの提案

### 3-1）概要

アドホックネットワークでは，固定のネットワークとは異なり，各端末が互いに中継を行うことで通信が行われる．そこで各移動体端末は中継機能を行うために，経路情報を知る必要がある．アドホックネットワークに適した経路制御については，AODV（Ad hoc On-Demand Distance Vector）を始めとしていくつかの方式が提案されている．

通常の端末に対してアドホックネットワークでの通信を提供するには，経路制御だけでは不十分であると考えられる．すなわちユーザがアドホックネットワークを利用して通信を行う際には，固定ネットワークと同様にIPアドレスではなくホスト名により通信相手を指定すると考えられる．つまりアドホックネットワークにおいても，固定ネットワークと同様に名前解決の手段が提供されていなければならない．

しかし，一時的に作られるアドホックネットワークでは，そのネットワーク内に必ずしも DNS サーバなどの名前解決を行うサーバが存在するとは限らない．さらに，仮に DNS サーバが存在しても，各移動体がネットワークへ出入りする度にその移動体の情報をサーバへ反映させる必要があり現実的ではないと考えられる．そこで，アドホックネットワークに適した名前解決の手法を提案する．

提案手法では，AODV を用いたアドホックネットワーク上に，名前解決要求パケットのブロードキャストを繰り返すフラッディングを用い，応答をユニキャストで行う手法を用いて名前解決を行う．この手法はパケットの構成や手順がAODVの経路確立と同様な形態を取っていることから，名前解決と同時に通信相手の移動体への経路確立も行える．そのため，通信の開始まで必要な経路確立や名前解決を効率よく行い，通信開始までの遅延時間を減らすことが出来るという特徴を有している．提案する手法の詳細手順と，実装と実験による測定結果について述べる．

### 3-2）AODV における名前解決手法

**■提案手法概要**

アドホックネットワークにおいて DNS を利用した名前解決は問題があり，アドホックネットワークに適した方法ではないことを述べた．そこで，アドホックネットワークに適した名前解決手法を提案する．概要を以下に示す．

- AODV により経路制御を行うアドホックネットワークでの利用を想定する.
- 名前解決はDNSのように特定のサーバに問い合わせるのではなく，問い合わせをブロードキャストし各ノードが自分の情報，あるいは保持している情報で応答を行う.
- 名前解決には，要求パケット IREQ (Information Request)を，応答パケットには IREP (Information Reply)の二種類を使用する.
- 名前解決を要求するノードは,IREP パケットをブロードキャストし，受け取ったノードは AODV の RREQ パケットと同様な方法でブロードキャストを繰り返すフラッディングを行いネットワークに存在するノード全体に問い合わせを行う.
- 問い合わせへの応答は，IREP パケットを用いる. 応答は名前解決を要求したノードへユニキャストで送る.
- 名前解決を AODV と同様な手順でフラッディングをするため，名前解決の手順と同時に目的のノードまでの経路を確立することができるようにする.

**■基本的な名前解決手順**

名前解決は,**図 5.3.2-16** の構造をもつ IREQ パケットを用いて行う. IREQ パケットは通信相手先ホスト名を Information フィールドへ格納してブロードキャストにより名前解決の問い合わせをおこなう. 名前解決の問い合わせに用いる IREQ パケットは,AODV の経路問い合わせに用いる RREQ パケットに Type, SubType, Length, Information というフィールドを付加し，これらのフィールドを名前解決に使用している. 提案方式では Type, SubType フィールドには名前解決を要求する定数を設定し,Information フィールドには目的とするホスト名を設定しブロードキャストを行なうが，Type，SubType フィールドに異なる定数を設定することで，名前解決以外の利用も可能になっている. また，IREQ パケットの送信時点では宛先ノードの IP アドレスはわかっていないため，RREQ パケットに存在する Destination IP Address と Destination Sequence Number の値は含まれていない.

IREQ パケットを受け取ったノードは，Broadcast ID と Source IP Address から過去に受信したものか否かを判断し,重複するものであればそのパケットは破棄する. それ以外では，IREQ パケットの発信元への経路(逆方向経路)を設定する. 次に Hop Count を 1 増やし，IP ヘッ

ダの TTL を 1 だけ減らし(TTL が 0 になるものは破棄される),再度ブロードキャストを行う．また，問い合わせがあった内容が自ノード宛てか，情報を保持しているか調べ，該当する場合であればユニキャストにより問い合わせ元へ応答を行う．

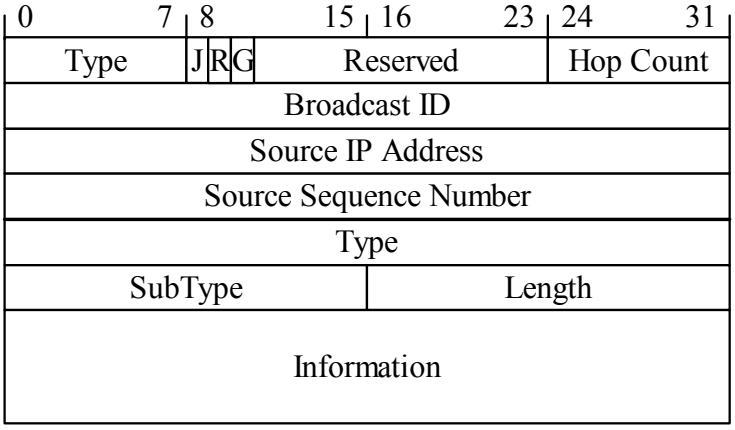



図 5.3.2-16：名前解決に用いる IREQ パケットの構造

問い合わせに対して応答をする際には**図 5.3.2-17** の構造を持つ IREP(Information Reply) パケットを使用する．IREP パケットは AODV で使用する RREP パケットにいくつかのフィールドを追加する形で構成されている．拡張されたフィールドで Type, SubType は IP アドレスが格納されている事を示す定数を使用し,Information フィールドに応答内容の IP アドレスを設定する．Broadcast ID フィールドは，どの名前解決の問い合わせに対応するものかを識別するための識別子として使用するフィールドで，応答を受け取る側で識別する際に必要となる．つまり IREP により応答を行う際には IREQ パケットに存在する Broadcast ID の値をそのまま代入することでパケットを組み立てて応答を行い，要求と応答の対応づけをする．

IREP は，IREQ による問い合わせ時に設定された逆方向経路を使用してユニキャストで送信される．IREP を受け取ったノードは，まず IREP パケットの発信元ノードへの経路(順方向経路)を設定する．次に IREP が，自ノードが行った問い合わせか否かを調べ，自ノード受け取るべきパケットではない場合には IREP の宛先(IREQ により問い合わせたノード)への中継を行う．このとき既に IREQ パケットにより逆方向経路が設定されているので経路が確立されているので経路探索は不要となる．

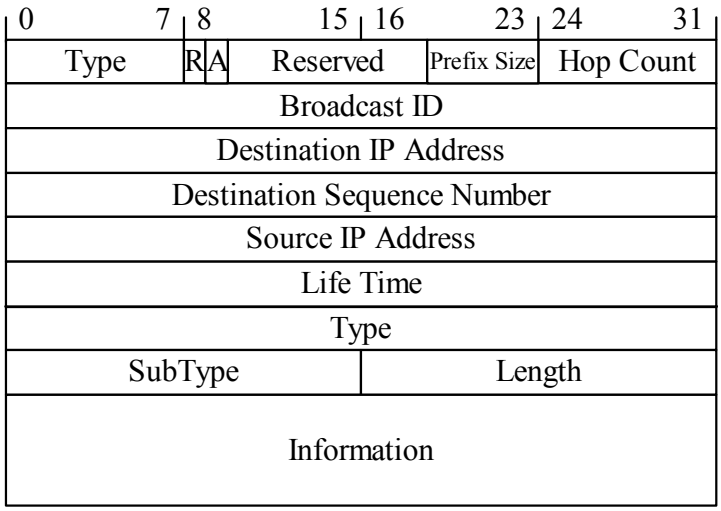



図 5.3.2-17：名前解決に用いる IREP パケットの構造

このようにして，AODV の経路確立と同様の手順で，名前解決要求をアドホックネットワーク内にフラッディングし，特定のサーバに依存すること無くアドホックネットワークに適した名前解決を行うことができる．

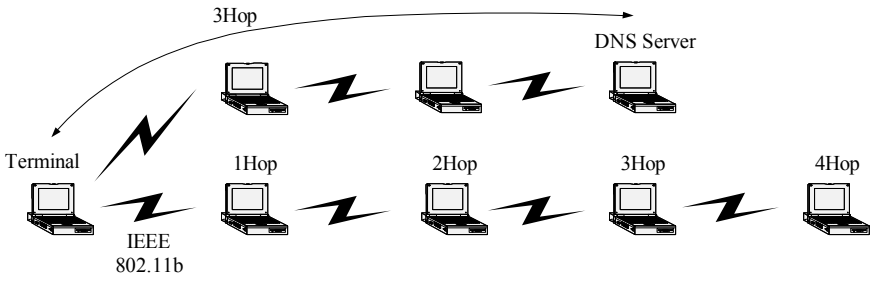



図 5.3.2-18：ネットワークトポロジ

### 3-3) 実証評価

提案手法を実証するために AODV と名前解決方式を FreeBSD 3.5.1-RELEASE + PAO 上に実装し，通信実験を行った．隣接ノードのみと通信できる状態で直線的に 5 ノードを配置した**図 5.3.2-18** のトポロジを持つネットワークを無線 LAN で構成し，末端のノードから各ノードへの ping の応答時間を測定した．比較のために 3 ホップ先に DNS サーバを設置し，名前解決に DNS を用いた通信を行なった場合の測定結果を**図 5.3.2-19** に示し，提案手法による名前解決を行なった場合の測定結果を**図 5.3.2-20** に示す．

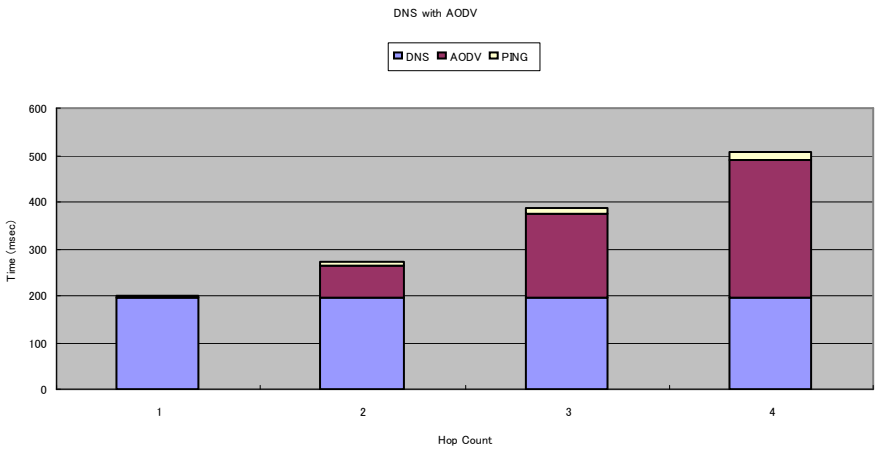



図 5.3.2-19： DNS を用いた場合の測定結果

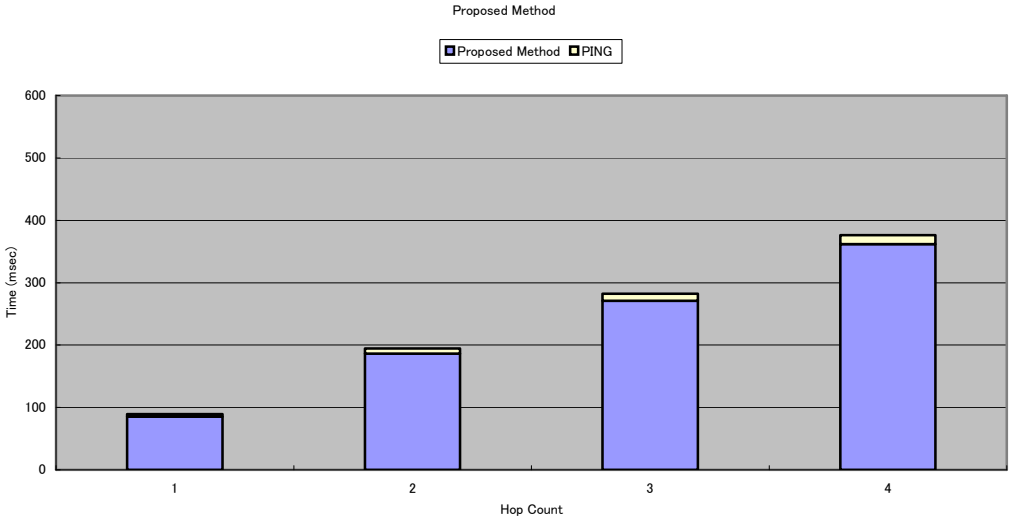



図 5.3.2-20： 提案手法による名前解決を行った場合の測定結果

DNS サーバを用いた場合には，通信の開始までに，DNS サーバまでの経路設定,DNS での名前解決および通信相手までの経路設定の三度のパケットの往復を要する．DNS サーバが遠い場合には，たとえ通信の相手先が隣接のノードの場合であっても遠方のサーバへの経路を設定する必要がありオーバヘッドが大きくなる．一方，提案手法では特定のサーバに依存することのなく行えるだけではなく，通信相手先のノードの名前解決と経路設定を一度のパケットの往復だけで行うことができ，効率の良い通信が可能となる提案手法の有効性を示すことができた．

### 3-4) まとめ

アドホックネットワークにおける名前解決の方法として DNS を使用する問題点を指摘し，それを克服する名前解決の手法を提案した．提案手法では既存の DNS のように特定のサーバに依存するのではなく，名前解決の要求をブロードキャストを繰り返すフラッディングという手法で行い，各ノードが保持する情報に応答を行う構成になっている．

そして，名前解決に使用するパケットを，経路制御プロトコル AODV を拡張した構成を取ることで，名前解決と同時に AODV の経路確立もおこなう事ができる．これにより，効率の良い名前解決を行うことが可能となっている．つまり，通信の開始までのオーバヘッドを少なくすることができ，データ送出までの遅延時間を小さくすることができる．

AODV による経路制御方式と提案手法の名前解決方式を FreeBSD 上に実装した．DNS サーバを利用した場合との比較測定実験を行い，提案手法では DNS と比較し小さい遅延時間で通信を開始でき，本方式の有効性を実証した．

### ４）アプリケーションレベルにおけるマルチホップサービス発見方式の提案

#### 4-1）はじめに

いつでも，どこでもネットワークを利用した情報交換を可能とするモバイルネットワークの形態として，携帯電話端末，PDA(Personal Digital Assistance)及びラップトップ PC などの可動性ある各ノードがルータとしての機能を持つことで一時的なネットワークを形成するアドホックネットワークが注目されている．このように一時的に形成するネットワークでは，ネットワーク上に提供されているサービスを利用するために通信を開始する以前に，ユーザは，ユーザのアプリケーションが指定するサービスの IP(Internet Protocol)アドレスやポート番号，及び設定パラメータなどの構成情報を何らかの方法で取得し設定を行う必要がある．そのため，アプリケーションが指定するサービスの発見要求を行い，その要求を満たすサービスの構成情報の自動取得を可能とするサービス発見方式は，サービスの迅速な利用開始を可能とすると共に，ネットワーク上のサービスが提供する全ての資源を有効利用することを可能とする．

従来のサービス発見方式として SLP(Service Location Protocol)[11]，Salutation[12]，Jini[13]等がある．これらは，基本的に構成情報を提供するセンタサーバを設けることで構成情報の取得を可能とする．しかしながら，アドホックネットワークでは，ネット

ワークを構成するたびにセンタサーバを設けその管理を行うことは，ユーザにとって大変煩わしい手間となってしまう．そのため，センタサーバを設けずに構成情報の取得を行うことを可能とするサービス発見方式が求められている[14]． それらの方式は，補足としてセンタサーバを用いずに，ブロードキャストを活用し，サービスを提供するノード（以下，サーバと呼ぶ）がユニキャストで構成情報を含むメッセージを応答する方式を提案している．近年，ノード数の増加に伴いサービス発見のためにブロードキャストするメッセージ数が増大し輻輳の原因となってしまう問題を回避するため，ユニキャストで応答したメッセージを中継するノードがメッセージ内の構成情報を蓄積し，あらたにサービス発見を要求するメッセージを受信した場合は蓄積している情報を元に応答することで対処する方式が提案されている．しかしながら，応答したノードの蓄積にない構成情報が示すサーバを発見することができなくなってしまう問題があった．

そこで，上記の課題を解決する一環として，上記の方式にサービス発見の要求を行ったノードが取得した全ての構成情報をその構成情報の提供元のノードに向かって配布する拡張を図ったアドホックネットワークにおけるサービス発見方式を提案する．

### 4-2) 従来のサービス発見方式とその課題

#### ■サービス発見方式を用いるシナリオ例

カンファレンス会場において発表者がプレゼンテーション資料を聴講者に提供するシナリオ例を示す．カンファレンス会場に到着した聴講者のノードは，先ず特定の IP アドレス帯の中からランダムに IP アドレスを決定しアドホックネットワークに参加する[15]．次にこのノードは，サーバの有無の情報及びサーバがある場合はその構成情報を保持していないため，自動的かつ迅速なサーバの発見とその構成情報の取得を可能とするサービス発見方式を活用する．

一般にサービス発見方式では，発見を要求するサーバを特定するための情報，例えば SLP の場合は IANA(Internet Assigned Number Authority)で規定される“ftp”等の文字列となるサービス種別及び必要に応じて属性等を指定してサービス発見要求を行う(**図 5.3.2-21①**)．この要求に対し，センタサーバもしくはサーバは指定されたサービス種別に一致するサーバの構成情報を応答する(**図 5.3.2-22②**)．これより，聴講者のアプリケーション（FTP クライアント）は，取得した構成情報を元にサーバ（FTP サーバ）にアクセスして各発表者のプレゼンテ

ーション資料の取得を行うことが可能となる.

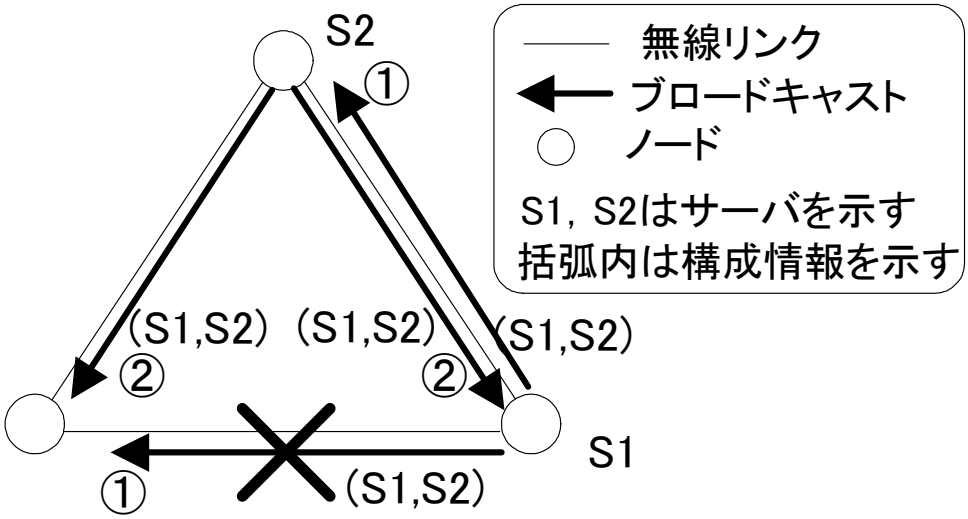



図 5.3.2-23: proactive 型のサービス発見方式

**■アドホックネットワークを対象とするサービス発見方式とその課題**

アドホックネットワークを対象とした従来のサービス発見方式は, アプリケーションの要求とは無関係にサービス発見を行う proactive 型のサービス発見方式とアプリケーションが要求とする時にサービス発見を行う reactive 型のサービス発見方式に分類することができる.

proactive 型の方式として, 1 ホップの 1 対 1 のリンクのみで構成するアドホックネットワークを対象とし, 各ノードが定期的に自身が持つ全ての構成情報を相互に交換するサービス発見方式が提案されている 63. この方式では, 自身が提供するサービスの構成情報のみをブロードキャストするのではなく, 自身が持つサービスの構成情報とこれまでに取得した他のノードが提供するサービスの構成情報の双方を含むメッセージのブロードキャストを行う. 定期的に双方の構成情報を含むメッセージをブロードキャストすることにより, メッセージが失われた場合でも (**図 5.3.2-23①**), 次回のブロードキャストもしくは他のノードのブロードキャストにより構成情報を取得することが可能となる (**図 5.3.2-23②**).

しかしながら, この方式は構成情報を全ノードと相互に定期的に交換するため, サービス発見に必要となるメッセージ数が増加し輻輳の原因となってしまう問題がある. また, この方式は 1 ホップのリンクで構成するアドホックネットワークのみ適用可能であり, より広域のエリアでの通信が可能となるマルチホップ・アドホックネットワーク

おける検討は行われていない.

reactive 型の方式として，マルチホップ・アドホックネットワークにおける経路制御方式である AODV (Ad Hoc On-Demand Distance-Vector)[3]の経路発見アルゴリズムを用いる方式が提案されている 65. この方式は,

アプリケーションが要求する時にサービス発見を要求するメッセージをブロードキャストし（**図 5.3.2-24**(a)①②③），指定されたサービス種別の構成情報を保持するノードがユニキャストで応答を行う（**図 5.3.2-24**(a)④⑤⑥）. また，ユニキャストでの応答を中継するノード（**図 5.3.2-24** (a),N1 及び N2）は構成情報を蓄積する. あらたに同一のサービス種別のサービス発見を要求するメッセージを蓄積を持つノード（**図 5.3.2-24** (a)N1）が受信した場合(**図 5.3.2-24** (b)①），他のノードにメッセージのブロードキャストを行わずにユニキャストで応答する**図 5.3.2-24** (b)②). このサーバ以外の蓄積を持つノードがブロードキャストを転送せずに応答することで，ブロードキャストするメッセージ数を削減することが可能となる.

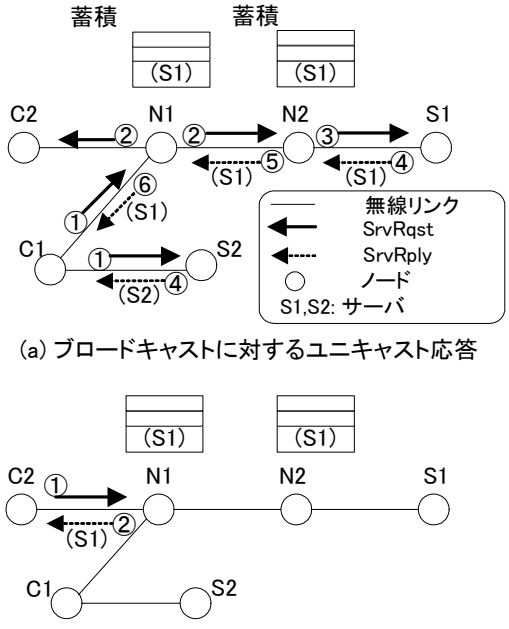
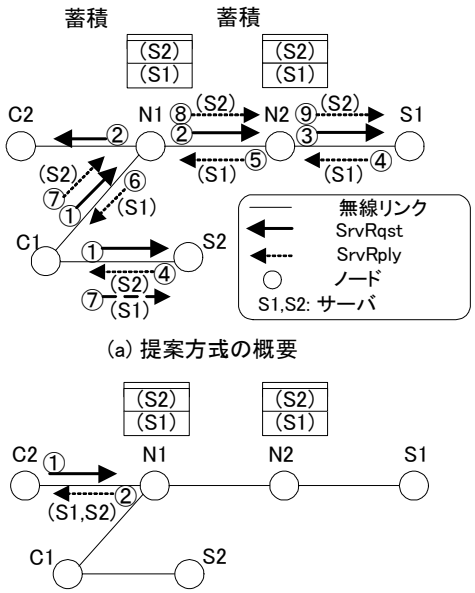



図 5.3.2-24: 従来のサービス発見方式の概要

しかしながら，この方式が用いる経路発見アルゴリズムは発見の要求時に指定する１つの IP アドレスに対して発見される経路が１つとなるのに対し，サービス発見では発見を指定する１つのサービス種別に

対して発見結果が複数のサーバとなる性質があることにこの方式は留意していない．そのため，アプリケーションが指定したサービス種別のサーバが他にもあるにもかかわらず，蓄積を元に応答したノードはブロードキャストを行わないため，応答したノードの蓄積にない構成情報のサーバ（**図 5.3.2-24 (b) S 2**）を発見することができなくなってしまう問題があった．これは上記で示したシナリオを例とすると，全ての発表者のプレゼンテーション資料が提供されているにもかかわらず，聴講者が取得することができないプレゼンテーション資料が生じてしまう原因となってしまう．




(a) 提案方式の概要

(b) N1からの応答によりC1は，S1とS2の双方を発見できる

図 5.3.2-25：提案方式の処理手順の概要

### 4-3) 提案方式

**■基本方針**

前節で示した課題に以下の(1)(2)の基本方針に従って対処し，アドホックネットワークにおけるサービス発見方式を提案する．

40. サービス発見に必要となるメッセージ数の削減を図るため，蓄積を用いる従来方式を拡張する．
41. IP ネットワークて提供されるサービスの発見を主な目的とするため，サービス発見に用いるメッセージは SLP で規定されるメッセージを拡張する．

(1)の基本方針に従い，サービス発見要求のメッセージのブロードキャスト（図 5.3.2-25(a)①②③）とユニキャスト応答（図 5.3.2-25(a)④⑤⑥）を行う reactive 型の手順に，サービス発見要求の結果得た構成情報を配布する手順（図 5.3.2-25 (a)⑦⑧⑨）をあらたに導入する．このあらたに導入する手順により，サービス発見要求を行ったノードが取得した全ての構成情報を蓄積を持つ他のノードに提供可能となる．そのため，蓄積を持つノードが，あらたにサービス発見要求を受信した場合（図 5.3.2-25 (b)①）でも，サーバの構成情報（図 5.3.2-25 (b)，S1 及び S1 の構成情報）を提供することが可能となる．

また，(2)の基本方針に従い，SLP から(1)の基本方針にもとづいた手順に必要となるメッセージを抽出し，マルチホップでメッセージを中継するために必要となる項目をメッセージ内にあらたに追加する．

| Header | |
|---|---|
| **サービス発見の要求元ノードのIPアドレス** | |
| length of <PRList> | <PRList> String |
| length of <service-type> | <service-type> String |
| length of <scope-list> | <scope-list> String |
| length of predicate string | ServiceRequest<predicate> |
| length of <SLP SPI> string | <SLP SPI> String |

(a)　拡張したSrvRqst

| Header | | |
|---|---|---|
| **サービス発見の要求元ノードのIPアドレス** | | |
| **サービス発見の要求に対し応答したノードのIPアドレス** | | |
| Error Code | | URL Entry count |
| <URL Entry 1> | ... | <URL Entry N> |

(b)　拡張したSrvRply

図 5.3.2-26：SLP のメッセージの拡張

**■メッセージの拡張**

アプリケーションが要求するサービスの発見要求を行うメッセージである Service Request(SrvRqst)[11]，SrvRqst により要求されたサービスに関する構成情報の応答を行うメッセージである Service Reply(SrvRply) [11]について以下の通り拡張する．

42. SrvRqst の拡張(図 5.3.2-26(a))

- サービス発見の要求元ノードの IP アドレスを記述する項目を SrvRqst にあらたに追加する．この項目は，サービス発見要求に対して応答を行うノードが SrvRply を送る次ホップのノードを決定するために導入する．

- SLP では，同一内容のサービス発見を再要求する場合は，SLP のメッセージヘッダに付加されるメッセージ識別子(XID)を同一の値を用いることに規定されている．これに対して，ここでは，同一内容のサービス発見の再要求時でも XID を 1 増加させることとする．これによりブロードキャストを受信したノードは，XID と SrvRqst 内の要求元ノードの IP アドレスの組が既に受信しているメッセージと同一か否かを判断することが可能となり，その組が同一の場合はメッセージを破棄することで，重複するメッセージを再びブロードキャストしてしまうことを防止することが可能となる．

43. SrvRply の拡張（図 5.3.2-26 (b)）

- サービス発見の要求元ノードの IP アドレスを記述する項目を SrvRply にあらたに追加する．この項目は，サービス発見の要求に応答したノードから受信した SrvRply を中継するノードが SrvRply を送る次ホップのノードを決定するために導入する．
- サービス発見の要求に対し応答したノードの IP アドレスを記述する項目を SrvRply にあらたに追加する．この項目は，サービス発見の要求元のノードが発見要求の結果得られた構成情報を，応答元のノードに向かってユニキャストするときに宛先の IP アドレスとして必要になるために導入する．

これらの SrvRqst 及び SrvRply は UDP を用いて送受信を行い，通常の IP ヘッダを付加した処理を行う．ブロードキャストした SrvRqst 転送するときは IP ヘッダ内に示される TTL(Time To Live)を 1 減らしてブロードキャストを行う．

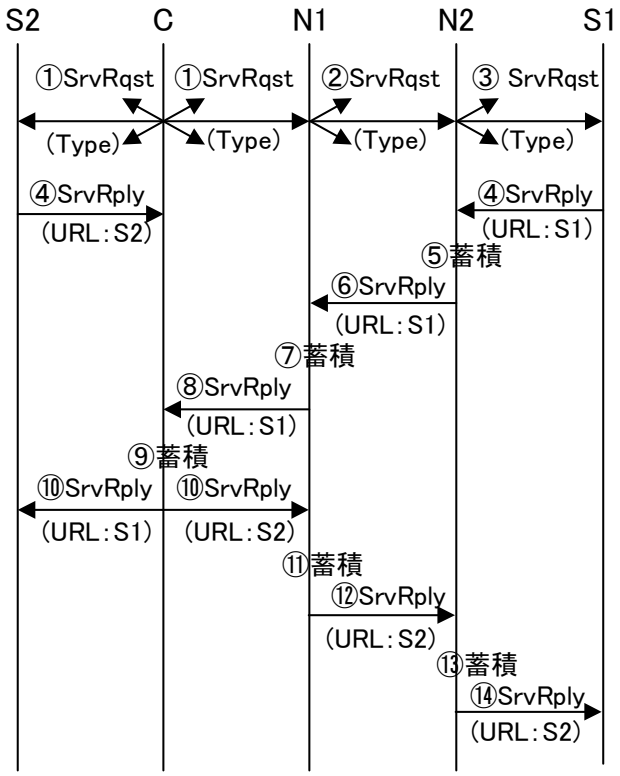



図 5.3.2-27：拡張したメッセージを用いた処理手順の例

**■拡張したメッセージを用いた処理手順の詳細**

拡張した SrvRqst および SrvRply を用いた処理手順を以下に示す．

アプリケーションが発見を要求するサービス種別（図 5.3.2-27：Type）を指定しサービス発見を要求する．

自身の蓄積の中に，サービス発見の要求があったサービス種別の URL(Uniform Resource Locator)等からなる構成情報があるか否かを調査する．構成情報が蓄積にある場合は，その構成情報をアプリケーションに提供する．構成情報が蓄積にない場合は，サービス種別を指定し，SrvRqst にあらたに拡張したサービス発見の要求元ノードの IP アドレスを記述する項目に自身の IP アドレスを記述したメッセージを作成しブロードキャストする（図 5.3.2-27①）．

SrvRqst メッセージを受信したノードは，SrvRqst のヘッダに含まれる XID と SrvRqst 内の要求元を表す IP アドレスの組が既に受信している SrvRqst の組と同一か否かを判断する．その組が既に受信している SrvRqst と同一の場合はメッセージを破棄し，組が同一でない場合は，SrvRqst 内に指定されるサービス種別の構成情報を蓄積しているか否かを確認する．蓄積していない場合は，TTL を 1 減らしてブロードキャ

ストする（図 5.3.2-27②③）．蓄積している場合もしくは自身がそのサービス種別のサービスを提供するノードである場合は，あらたに拡張した SrvRqst のサービス発見の要求元ノードの IP アドレスを記述する項目に SrvRqst 内に示される要求元ノードの IP アドレスを記述し，サービス発見の要求に対し応答したノードの IP アドレスを記述する項目に自身の IP アドレスを記述した SrvRply を作成する．経路情報を参照し，SrvRqst に記述されている要求元ノードへの経路となる次ホップのノードに対して SrvRply を送信する（図 5.3.2-27④）．

SrvRply を受信したノードは，メッセージに示される要求元のノードの IP アドレスが自身の IP アドレスと同一か否かを確認する．同一でない場合は，先ずメッセージ内の構成情報を構成情報内に示される有効期限の間蓄積する（図 5.3.2-27⑤⑦）．次に，経路情報を参照し，SrvRply に記述されている要求元ノードへの経路となる次ホップのノードに対して SrvRply を転送する（図 5.3.2-27⑥⑧）．また，同一の場合の手順は，5)となる．

SrvRply を受信したサービス発見の要求元ノードは，受信した SrvRply に含まれる構成情報をアプリケーションに提供すると共に構成情報を蓄積する（図 5.3.2-27⑨）．２つ以上の SrvRply を受信した場合は，得られた全ての構成情報を含み，要求元ノードの IP アドレスを記述する項目に先に受信した SrvRply の応答元 IP アドレスを記述した SrvRply を作成する．経路情報を参照し，先に受信した SrvRply 内に示される応答元ノードへの経路となる次ホップのノードに対して SrvRply を送信する（図 5.3.2-27⑩）．

5)でサービス発見の要求元ノードがユニキャストした SrvRply を転送する中継ノードは 4)と同様の処理を行う（図 5.3.2-27⑪～⑭）．

### 4-4）シミュレーション評価

#### ■評価方式と評価項目

サービス発見方式として，提案方式と次に示す方式を評価対象とする．

- 方式 A
  SLP においてセンタサーバを用いずにブロードキャストに対しサーバがユニキャスト応答する方式
- 方式 B
  ブロードキャストに対しサーバもしくは蓄積を持つノードがユニキャスト応答を行う従来方式方式[16]

方式Ａは，サービス発見に必要となるメッセージ数の削減を図る蓄積による効果を明らかにするために対象とする．方式Ｂは，２章で示した応答したノードの蓄積にない構成情報のサーバを発見することができなくなってしまう問題を解決する提案方式の効果を比較評価するために対象とする．

また,次の3項目についてシミュレーションによる性能評価を行う．

44. サービス発見率
    サービス発見要求の結果発見したサーバ数（取得した構成情報数）をアドホックネットワーク内のサーバ数で規格化した値の評価を行う．
45. メッセージ数
    サービス発見に用いられた，サービス発見要求メッセージである SrvRqst，及び応答メッセージである SrvRply それぞれのメッセージ数の評価を行う．
46. サービス発見に要する時間
    サービス発見要求を行ってから応答の SrvRply を受信するまでに要する時間の評価を行う．なお,複数の SrvRply を受信する場合は,最後の SrvRply を受信するまでに要する時間とする．

**■シミュレーション設定**

- シミュレーションモデル
  アドホックネットワークにおけるサービス発見方式を評価するシミュレーションプログラムを OPNET を用いて実装した．経路制御には，OPNET の無線 LAN モデル上に実装されている NIST により開発された AODV を活用した．サービス発見方式の処理部から渡させるサービス発見に用いるメッセージは，UDP 処理部において UDP ヘッダを付加した後 IP 処理部に送られ,送信バッファに経路が発見されるまで格納される．送信バッファには最大 64 パケットを格納し，最大格納数を超える場合は古いパケットから順に破棄する．また，無期限でパケットを格納するのを防ぐために,30 秒を経過しても経路が見つからない場合はその格納しているパケットを破棄する．無線 LAN モデルは，通信速度を 2 Mbps とし通信可能距離を 250 ｍとする．

- サービスの提供とサービス発見要求モデル
  サービスを提供するノードであるサーバは，あらかじめ全ノードの中からランダムに選出し，選出したノードに対してサービス種別をランダムに割り当てる． 選出したノードは，割り当てられたサービス種別のサービスを提供するノードとして，クライアントから SrvRqst を受信した場合，構成情報を含む SrvRply を応答する．また，サービス発見の要求を行うノードは，あらかじめ指定するノード数のノードを１秒ごとに全ノード中からランダムに選出する．選出したノードに対してサービス発見要求を行うサービス種別をランダムに割り当てる．
- 移動モデル
  クライアントの移動モデルは，ランダムウェイポイントモデル[17]とする．各ノードは長方形の領域内を，ランダムに選択した位置から移動先の位置をランダムに選択し，あらかじめ指定する速さの中からランダムに選択した速さで移動する．そして，移動先の位置に到着した場合，指定する停止時間停止した後，再び移動先をランダムに選択して移動を繰り返す．

**■評価結果**

47. サービス発見率の評価結果

時間が経過するに従い提案方式が方式Ａ及び方式Ｂに比べサービス発見率が大きくなる結果となった．方式Ａでは，SrvRqst もしくは SrvRply の転送中にパケットロスが生じる結果，発見することができなくなってしまうサーバが生じるためにサービス発見率が低下しているものと考えられる．方式Ｂでは，SrvRqst または SrvRply のパケットロス及び上記で示した課題があるためにサービス発見率が低下しているものと考えられる．

48. メッセージ数の評価結果

- サービス発見要求に用いるメッセージ数
  共に蓄積を用いるアプローチである提案方式と方式Ｂは，シミュレーション時間の経過と共にサービス発見要求のためブロードキャストするメッセージ数が方式Ａに比べ大幅に減少している．これは，サービス発見要求が行われた回数が時間の経過と共に増加するに従い構成情報を蓄積するノード数が増加することで，サービス発見要求のためブロードキャストしたメ

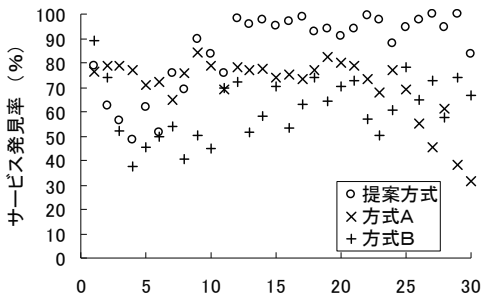
ッセージがサーバまでに到達する以前に蓄積しているノードが応答することでブロードキャストするメッセージ数を削減しているためである.

- 応答に用いるメッセージ数
  構成情報の蓄積を持つノード数が少ないと考えられるシミュレーション開始から10秒間は,提案方式が方式Bに比べメッセージ数が多くなるがシミュレーション時間の経過と共に同程度となっている.メッセージ数が多くなるのは,提案方式は方式Bに対してあらたに拡張したサービス発見要求の結果得た構成情報を配布する手順があるためである.

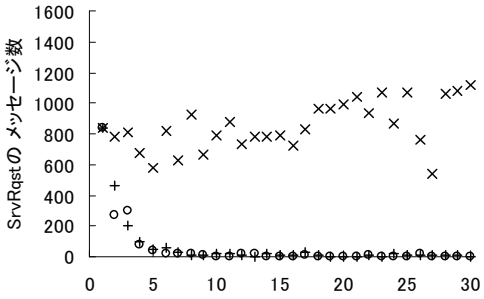
  シミュレーション時間の経過とともに,構成情報を蓄積するノード数が増加するにつれて,サーバのみならずその構成情報を蓄積する他のノードがサービス発見要求に対して応答可能となり,サービス発見要求元ノードと構成情報の提供元ノード間のホップ数が小さくなるため,その結果として応答メッセージ数が減少するものと考えられる.

49. サービス発見に要する時間

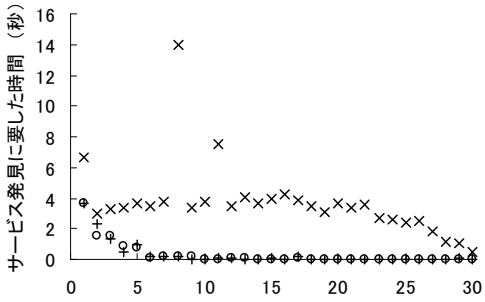
共に蓄積を用いるアプローチである提案方式と方式Bは，シミュレーション時間の経過と共にサービス発見に要する時間が方式Aに比べ大幅に減少している．これは，(2)で述べた通りサービス発見の要求元ノードと構成情報の提供元ノードのホップ数が蓄積を持つノード数が増加するに従い小さくなる効果によるものと考えられる.



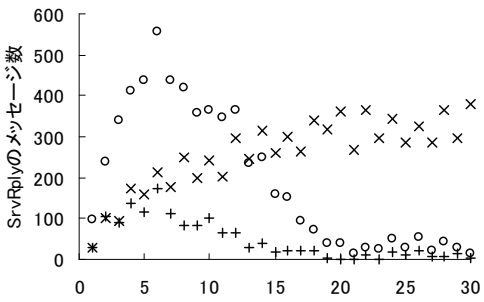

(a) サービス発見率の評価結果




(b) SrvRqst のメッセージ数の評価結果

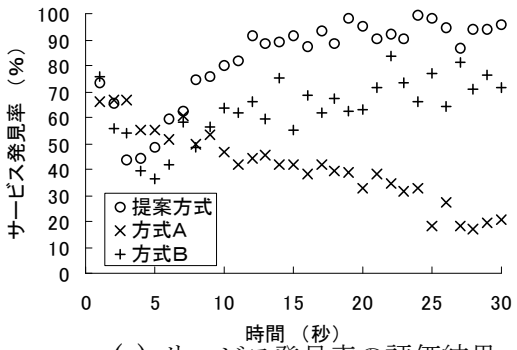



(d) サービス発見に要した時間の評価結果

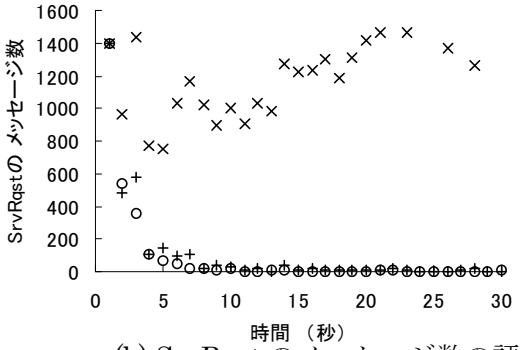



(c) SrvRply のメッセージ数の評価結果

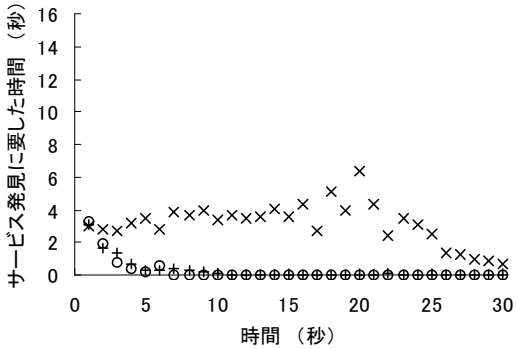
図 5.3.2-28：静止時の評価結果



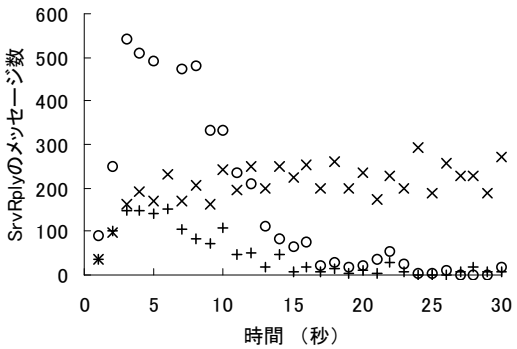

(a) サービス発見率の評価結果




(b) SrvRqst のメッセージ数の評価結果




(d) サービス発見に要した時間の評価結果




(c) SrvRply のメッセージ数の評価結果

図 5.3.2-29：評価条件 6 の評価結果

■考察

● 蓄積を用いる効果に関する考察

アドホックネットワークにおいて通信を行うノードの組が増加するに伴いパケットロスが増大することが報告されていることからも，メッセージ数が増大する評価結果となった方式Aはブロードキャストした SrvRqst がサーバに到達する以前に，もしくは，サーバからユニキャストされた SrvRply がサービス発見の要求元ノードに着信する以前に失われてしまう割合が大きくなることを意味する．これより，サービス発見要求を行ったノードが発見することができなくなってしまうサーバ数が増加するため，方式Aは制御メッセージ数が小さいくなる方式B及び提案方式に比べサービス発見率が低下しているものと考えられる．

また，ノードのみでネットワークを構成するアドホックネットワークは，ノードの移動性が大きくなるに伴ってネットワークの切断や結合が頻繁に発生する．このような環境においてサーバを発見する時間を多く要する場合，サーバと通信を行う時点では通信を行うことができなくなってしまうことが考えられる．従って，サーバと通信を行うための事前処理となるサーバの発見とその構成情報の取得を迅速に行うことが重要となる．これより，既に提供されているサーバの利用可能性の観点からは，方式 A に対しサービス発見に要する時間が短い評価結果となった方式 B 及び提案方式が有効といえる．

● 新たに導入した構成情報を配布する手順の効果に関する考察

サーバを発見できなくなってしまう問題を解決する提案方式以外の方法として，サービス種別に加え例えば属性等を指定してサービス発見要求を行うことで，同一のサービス種別のサーバが複数ある場合でも個々に発見することで対処する方式が考えられる．しかしながら，この方法は，サービス種別と属性の組が一致するサーバのみ応答し，サービス種別が同一でも属性が一致しないサーバは応答しないことから，応答メッセージを中継するノードはサービス種別と属性の組により指定された構成情報のみを蓄積することになる．そのため，属性は異なるが同一のサービス種別を指定したサービス発見要求をあらたに蓄積を持つノードが受信した場合，サービス種別と属性の組が蓄積している構成情報と異なるため，同じサービス種別に対するサービス発見要求であるにもかかわらず再びアドホックネットワーク全体にブロードキャストすることになってしまう．従って，このサービス発見要

求時にサービス種別に加え属性等を指定する方式は，蓄積によってブロードキャストするメッセージ数を削減する効果を得ることができないといえる．これより，サービス発見要求時にサービス種別のみを指定する提案方式は，サービス種別に加え例えば属性等を指定する方式と比べ蓄積によるメッセージ数を削減する効果を有効利用することができるといえる．

また，評価結果から提案方式は，アプリケーションが必要とするときにサービス発見を行うため定常的にサービス発見を行う方式 A に比べサービス発見に必要となるメッセージ数を大幅に削減し，また従来の蓄積を用いる方式に対しては同程度のメッセージ数でのサービス発見を可能としている．サービス発見率は，サービス発見の要求を行ったノードが取得した全ての構成情報をその構成情報の提供元のノードに向かって配布する手順をあらたに拡張したことによって従来の蓄積を用いる型の方式に比べ平均で 30 %程度向上することが明らかになった．

このように，従来の蓄積を用いる方式と比べ，サービス発見に必要となるメッセージ数を従来方式と同程度に抑制しつつ，平均で 30 %程度サービス発見率を向上させる提案方式は有効といえる．

### 4-5）おわりに

従来，アドホックネットワーク内の全ノードが定期的に相互の構成情報を交換する proactive 型のサービス発見方式やアプリケーションが必要なときにサービス発見を要求するメッセージをブロードキャストすることで構成情報の取得を行う reactive 型のサービス発見方式が提案されていた．しかしながら，proactive 型の方式はサービス発見に必要となるメッセージ数が増加し輻輳の原因となってしまう問題があった．また，サーバ以外のノードが構成情報を蓄積し，サービス発見の要求に対して応答を行うことでブロードキャストするメッセージ数の削減を図る reactive 型の方式は，応答するノードの蓄積にない構成情報のサーバを発見することができなくなってしまう問題があった．

提案方式では，reactive 型の方式にサービス発見の要求を行ったノードが取得した全ての構成情報をその構成情報の提供元のノードに向かって配布する拡張を図った．また，提案方式の有効性を検証するためサービス発見要求の結果発見されるサーバの割合であるサービス発見率，サービス発見に必要となるメッセージ数及びサービス発見に要する時間についてシミュレーション評価を行った．その結果，従来の

reactive 型の方式と比べ，サービス発見に必要となるメッセージ数を従来方式と同程度に抑制し，平均で 30 %程度サービス発見率を向上させる提案方式の有効性を明らかにした.

今後は，電力消費を考慮した上でのサービス発見方式や固定網と相互接続したアドホックネットワークにおけるサービス発見方式が課題である.

## 参考文献


50. Network Simulator (ns-2), http://www.isi.edu/nsnam/ns/
51. Wireless and Mobile Extensions to ns-2: CMU Monarch Project, http://www.monarch.cs.cmu.edu/cmu-ns.html
52. C. Perkins, et al.: "Ad hoc On-Demand Distance Vector (AODV) Routing", draft-ietf-manet-aodv-8, March 2001.
53. J. Macker and S. Corson (chairs): "Mobile Ad-hoc Networks (manet)", http://www.ietf.org/html.charters/manet-charter.html
54. David B. Johnson, David A. Maltz, Yih-Chun Hu and Jorjeta G. Jetcheva: "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet draft draft-ietf-manet-dsr-04.txt, November 2000.
55. C. Hedrick: "Routing Information Protocol," RFC1058, June 1988.
56. J. Moy: "OSPF Version 2," Internet standard STD0054, April 1998.
57. P.V. Mockapetris: "Domain names - concepts and facilities," Internet standard STD0013, November 1987.
58. P. Vixie, Ed., S. Thomson, Y. Rekhter and J. Bound: "Dynamic Updates in the Domain Name System (DNS UPDATE).," RFC2136, April 1997.
59. R. Droms: "Dynamic Host Configuration Protocol," RFC2131, March 1997.
60. E.Guttman, et al., "Service Location Protocol, Version2", IETF, RFC 2165, June 1999.
61. The Salutation Consortium Inc., Salutation Specification, 2.0b ed ., Oct. 1997.
62. Sun Microsystems Inc., Jini architectural Overview, 1999.

63. Michael Nidd,″ Service Discovery in DEAPspace″, IEEE Personal Commun., Aug. 2001.
64. C.E.Perkins, et al.,″IP Address Auto configuration for Ad Hoc Networks″, IETF Internet Draft(draft-perkins-manet-autoconf-01.txt), Nov.2001(work in progress).
65. Srinivasan Sesha, et al.,″Arguments for Cross-Layer Optimizations in Bluetooth Scatternets′, Symposium on Applications and the Internet (SAINT'01), Jan 2001.
66. Josh Broch,et al., ″A performance comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols″, Proc.IEEE/ACM Mobicom′98,1998.
67. C.Perkins, et al., ‟Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks″, IEEE Personal Communications, Feb. 2001.

## 5.3.3 価値情報転送プロトコルの研究開発

### １）設計目標と特徴

ユビキタスネットワーキングプロトコルスタックのセッション層の一つとして，**価値情報転送プロトコル**（VITP: Valuable Information Transfer Protocol）の研究を開始し，本年度はその基本的枠組みを定めた．VITP は以下の設計目標を持ったプロトコルである．

68. 安全に価値情報がユビキタスコンピューティング環境を構成するノード（Peer）間で流通することができる．
69. 価値情報の流通過程で，改竄を行うことができない．そのために，すべてのパケットには，MAC をつけることが可能である．
70. 様々な目的に用いる汎用性を有する．
71. 末端のノードが IC カードレベルの軽量ノードでも実装できる，実装規模が小さく，軽快なプロトコルであること．

### ２）VITP が前提とするネットワーク構造

VITP が実装されるネットワークは，基本的には，ユビキタスネットワークプロトコルスタックのL4の上で動作することが最終的な姿である．今年度は，まだL4以下が完備されていないことから，以下の性質を満たす下位層を前提として，研究開発を進めた．

72. システム設計を容易に行うために，下位層として，信頼性を有する双方向通信路が確立しているもの(例えば,TCP 等)を前提とする．
73. 下位層は,単一のプロトコルによるネットワークを必ずしも前提としない．つまり，通信するノード-to-ノードの通信が，異なる複数のネットワークを介することがありうる．
74. 単一のネットワークの中では,経路制御アドレスを付与したメッセージを与えたとき,そのネットワークが正常に動作している限りにおいて,そのアドレスのノードにメッセージが信頼性をもって送信されることが保証されるものとする．

ここでは，VITP を流通させるネットワークを **VITN**(Valuable Information Transfer Network)と呼ぶ．上記の前提とし，VITN を構成する要素は，以下の３種類から構成される．

75. **エンドノード**

VITP では,VITP に基づく通信を行う個体を,エンドノードと呼ぶ．

エンドノードには，16 Octet のユニークな ID（eTRON ID）が振られており，VITP 通信の通信相手の指定に使う．エンドノードは，サーバーとして動作するノードと，クライアントとして動作するノードの二種類に大別され，それぞれ以下の様に呼ぶ．

（ア） **価値情報レポジトリ（eR: entity Repository，サーバー側）**
価値情報レポジトリは，VITP の中で，サーバーとして動作する個体である．中に，価値情報を格納し，サービスクライアントからの要求に応じて，その内容を操作する．サーバーといっても，かならずしも，システム規模が大きいわけでない．代表的な実装としては，耐タンパー性を有する IC カードや，安全に価値情報を格納する耐タンパー性を有するマイクロコンピュータなどがある．

（イ） **サービスクライアント（SC: Service Client）**
サービスクライアントは，VITP の中で，クライアントして動作する個体である．VIR に格納されている情報を利用して実行するアプリケーションの動作する個体である．

※ エンドノードの中には，eR と SC の両方の動作を行うものもある．

76. **VITP ルータ**
異なるネットワークの間で VITP メッセージを交換するセッション層ゲートウェイノードのことを，VITP ルータと呼ぶ．

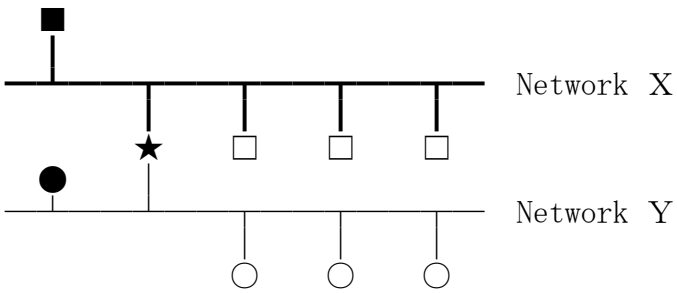
77. **アドレス解決サーバ（ARS: Address Resolution Server）**
eTRON Id とネットワーク層の経路制御アドレスの間の対応を保持するサーバ．

こうした一般的な VITP のネットワーク構造は，**図 5.3.3-1** のようになる．この図では，２つのネットワーク，X と Y が接続された構造となっている．論理的には，このネットワークがいくつ存在しても良いことになる．しかし今年度の研究では，この構造を以下のように制限する．

78. 経路制御が必要になるネットワークは，一つとする．これを主ネットワークと呼ぶ．

79. この主ネットワークを拡張する形で，対向通信，つまり２ノードから構成される小ネットワーク（ユビキタスＬＡＮを想定）が接続することがある．

従って，エンドノード間の通信では，最大，３種類のネットワークを経て VITP メッセージが交換されることになる．（小ネットワーク→主ネットワーク→小ネットワーク）




■： ARS over X
□： End Node over X
●： ARS over Y
○： End Node over Y
★： VITP Router between X and Y

図 5.3.3-1：VITP が前提とする一般的なネットワーク構成

**図 5.3.3-2** と**図 5.3.3-3** は，今回想定する典型的な例の構造である．**図 5.3.3-2** は，非接触型 IC カードを使った例えば，電子マネーによる決済を VITP で行う応用などを想定したネットワーク構造である．この例では，ベースとなるネットワーク基盤として IP 網を想定している．IP 網上に決済を行う，Service Clients が設置されている．IP 網には，非接触 IC カードのインタフェースを有する IP 網のノードが VITP ルータとして機能している．非接触 IC カードは，ISO 14443 によってこの VITP ルータと２ノードで独立したネットワークを構成する．IP 網の方は，多くのエンドノードによって構成されるため，アドレス解決サーバが必要となるが，14443 側の網の方は，対向で２者間のみの通信になるため，アドレス解決サーバは不要である．

一方，**図 5.3.3-3** は，高機能携帯電話やＰＤＡのような携帯側端末内に，セキュアチップを格納することで，この携帯電話端末の通信機能を使って，安全に電子商取引などを行う場合のネットワーク構成である．この例でも，主ネットワークを IP 網としている．末端のネットワークは，携帯型端末内のセキュアチップと携帯端末の通信を行う，

ISO 7816 ベースのネットワークがある.

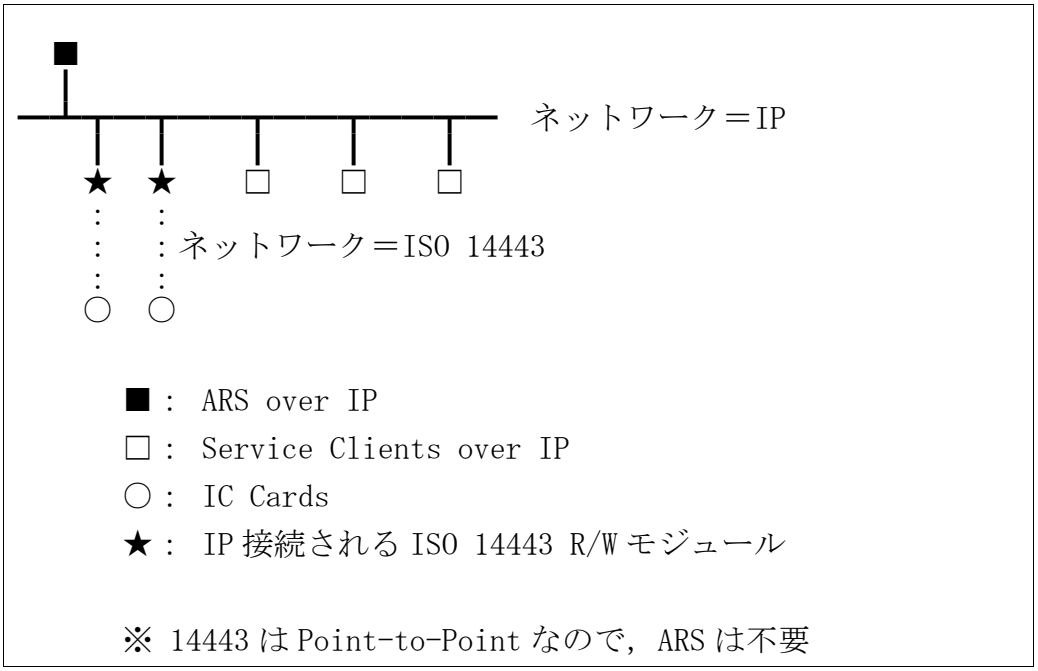



**図 5.3.3-2**：VITP が前提とする典型的なネットワーク構成例（１）

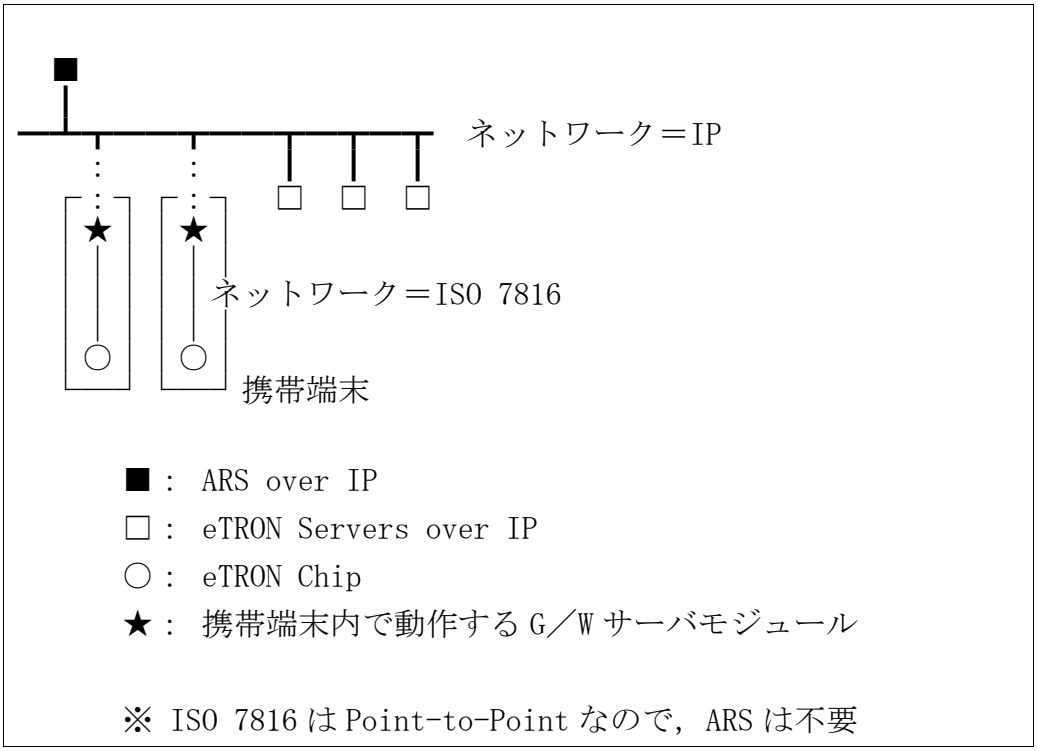



**図 5.3.3-3**：VITP が前提とする典型的なネットワーク構成例（２）

### ３）VITP による通信

#### 3-1）アドレス解決サーバへの eTRON アドレスの登録

アドレス解決サーバーは，eTRON ID とその ID を持つノードへの経路制御アドレス（例：IP アドレス）または，eTRON ID とその ID を持つノードへの経路を持つVITPルータノードの経路制御アドレスを管理するサーバである．VITP エンドノードから，eTRON ID をキーとしてそれが持つ経路制御アドレスを検索することができる．

VITP では，通信の相手を eTRON ID で指定する．その VITP のメッセージがきちんと相手のノードの到達するためには，その eTRON ID に対応した経路制御アドレスが取得できることが不可欠である．従って，網に VITP エンドノードが加わったときには，そのノードが持つ，eTRON ID と経路アドレスのペアを登録する必要がある．つまり，VITP エンドノードは，ネットワークに接続されると，以下のメカニズムで ARS に登録される．

**（例１）スマートカード形式の eTRON SCs の場合**

- タイミング：R／W ノードに載せられた時
- 動作概要：　R／W ノードが eTRON カードから eTRON ID を読み出し，R／W ノードが持つ IP 側の足のホストアドレスと eTRON ID のペアを ARS に登録する．

**（例２）サーバータイプの eTRON SCs または eTRON CHs の場合**

- タイミング：そのマシン上で，VITP サーバーが起動した時．
- 動作概要：　そのマシンが自分が持つ eTRON ID と IP アドレスのペアを ARS に登録する．

**（例３）携帯端末に差し込まれた eTRON チップの場合**

- タイミング：その携帯端末が VITP ハンドラが動作している状態で，オンラインになった時．
- 動作概要：　そのマシンに差し込まれた eTRON チップから ISO7816 経由で eTRON ID を読み出す．自分が持つ IP アドレスのペアを ARS に登録する．

逆にエンドノードがネットワークから切り離されるときは，ARS からその VITP エンドノードのアドレスエントリは削除される．

**（例）**

- タイミング：VITP エンドノードへの通信ができなくなる瞬間

- 動作概要： 自分が ARS に登録したエントリーを削除する.

また，各エンドノード側で，一旦取得した，eTRON ID-経路制御アドレスのペア情報は，一定期間エンドノード内にキャッシュする実装もありうる（アドレス解決表：ART: Address Resolution Table). この場合，ARS への問い合わせを減らし，通信の応答性を向上させることができる.

### 3-2) VITP エンドノード間の VITP メッセージ送付の前提メカニズム

次に，この VITP ネットワークにおいて，VITP メッセージが送付される経路制御方式について述べる．まず，最初に同じ主ネットワーク上ある，エンドノード間の通信のメカニズムについて述べる.

通信主体である，各エンドノードは，**表 5.3.3-1** に示す情報を通信時に所有している.

| 項目 | 内容 |
|---|---|
| アドレス解決表(ART) | (eTRON ID, IP address) の集合 |
| アドレス解決サーバ(ARS)の経路制御アドレス | IP アドレス |
| デフォルト VITP ルータ(アドレス解決できなかった eTRON Id へのメッセージの転送先) の経路制御アドレス | IP アドレス |

**表 5.3.3-1**：VITP エンドノードが持つ情報

次に VITP が実装される下位ネットワーク層（ここでは IP 層）が提供する通信インタフェース例として，以下を想定する.

80. ipAddress で指定された経路制御アドレスを持つマシンに message を送る

```
err = sendmsg (IPADR ipAddress, UB *message);
```

81. eTRON ID（eid）のアドレス解決を行ない，ipAddress を得る

```
err = resolve(EID eid, IPADR *ipAddress);
```

この resolve()関数の動作は以下のとおりである．

- 始めにローカルなアドレス解決表をみて，eid のエントリーが登録されていれば，それを返す
- ARS サーバがあればそこから取得して返す(自分のアドレス解決表にそれを追加する)

82. デフォルトゲートウェイの ipAddress を取り出す

```
err = getDefaultGw(IPADR *default);
```

次に，下位層が ISO 14443 や ISO 7816 のような，対向通信用の L2 プロトコル上に VITP を実装する場合，その中間のスタブインタフェースが VITP に提供するサービスは，以下である．

メッセージ message を対向の相手に送る．

```
err = sendmsg (UB *message);
```

### 3-3) VITP エンドノードの VITP メッセージ送付動作

VITP による通信手順は以下の順序で行われる．

83. アドレス解決（表 5.3.3-4★１）
    （ア） アドレス解決表から destination eTRON ID を探す．
    （イ） もし見付からなかった場合，ARS に問い合わせる．
    （ウ） ARS で見付かった場合，その経路制御アドレスに自分のアドレス解決表にそのエントリーを加える．
84. デフォルト VITP ルータがある時は，それを取り出す．（表 5.3.3-4

★２）

85. 見付かった先（相手エンドノードまたはデフォルト VITP ルータ）に VITP メッセージを送付する．（表 5.3.3-4★３）

```
ERR sendVITPMessage(UB* message)
{
        EID     eid;
        IPADR   ipadr;
        ERR     err;
                :
        /* VITP パケットから eTRON ID フィールドを取り出す */
        eid = GET_EID(message);

        /* アドレス解決を試みる */
        err = resolve (eid, &ipadr);                    ★１

        /* 解決出来なかったら */
        if (err < 0) {
                /* デフォルトゲートウェイを取り出す */
                err = getDefaultGw(&ipadr); ★２
                if (err < 0) goto ERR;
        };

        /* デフォルト GW またはそのホストにメッセージを送る */
        err = sendmsg(ipadr, &message);                 ★３
        return err;

    ERR:
                :
}
```

図 5.3.3-4：VITP の送信手順のアルゴリズム

### 3-4) VITP ルータの経路制御動作

前述のとおり，一般的には，VITP のネットワークは，複数種類のネットワーク層のネットワークにまたがって構築される．その境界部分

を VITP ルータと呼ぶ．一般的な形としては以下の構造になる．

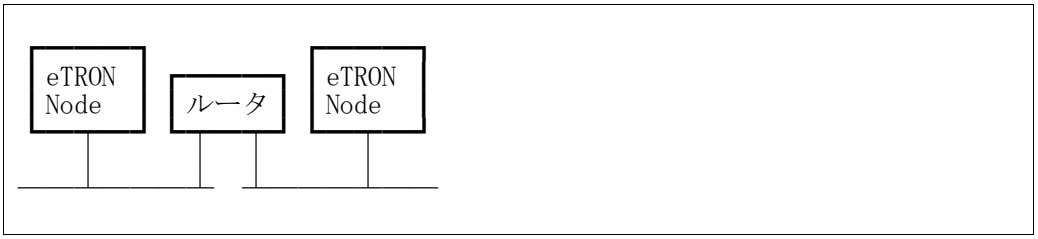



図 5.3.3-5

例えば，典型的な構成例として，IP 網に接続された ISO 14443 の非接触型カードベースの eTRN の場合は，以下のように位置付けられる．

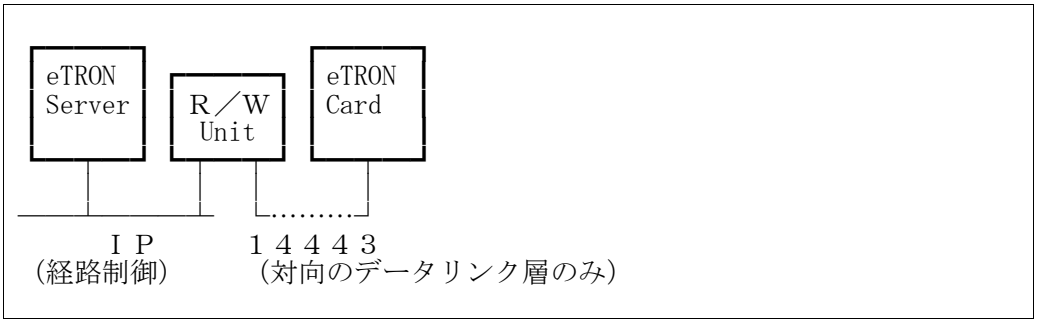



図 5.3.3-6

また，携帯型機器に内蔵された eTRON CHIP のような場合は，以下のように位置付けられる．

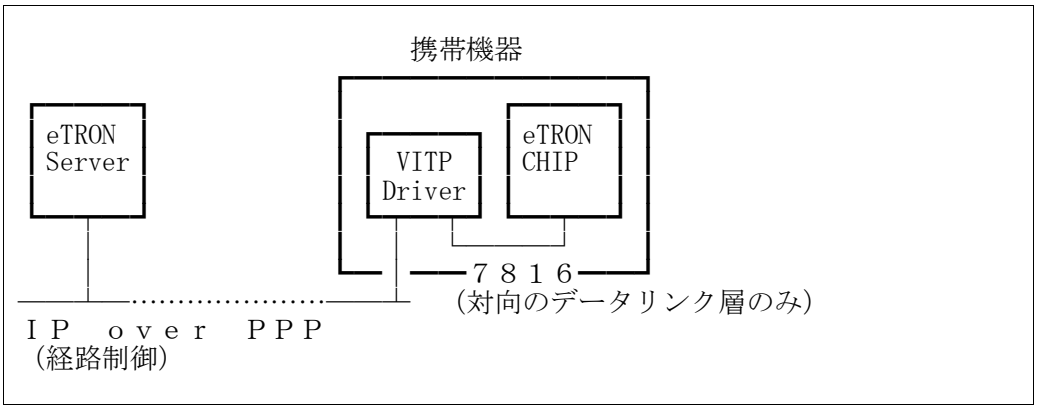



図 5.3.3-7

携帯型機器に内蔵された VITP 対応セキュアチップをもち，更に，14443 R/W 機能ももつと，以下のようになる．

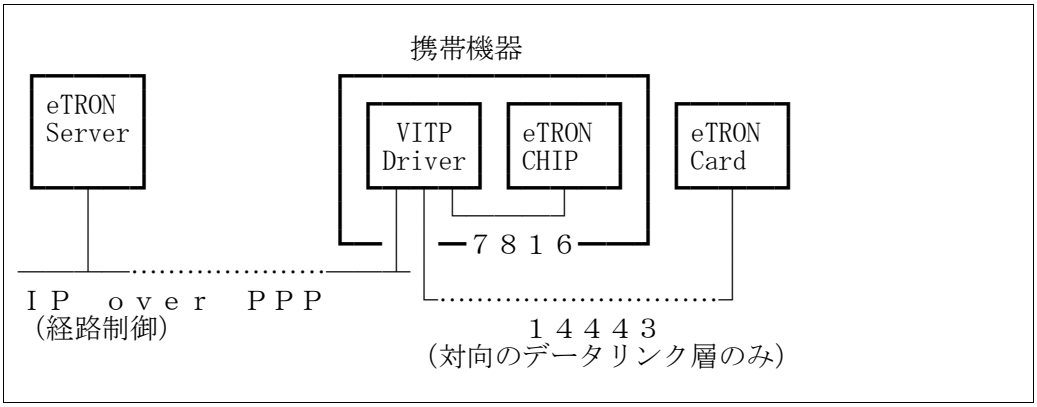



図 5.3.3-8

このアーキテクチャを考えると，携帯機器の内部での VITP ドライバも，カード型 eTRON のR／Wユニットも，単純に，異る複数のネットワーク層の上で VITP パケットをゲートウェイするルータ(ゲートウェイ)として実装すれば良いことがわかる．

※ これが eTRON がネットワーク対応チップであることの本質である．つまり，eTRON Chip をハンドルする部分は，通信の「鍵」などの秘密情報を持たずに，単純にアドレスをみてルーティングだけをすれば良いため，その部分のパーツを信頼しないですむのである．

この時，接続されたネットワーク層が，経路制御を伴うような網の場合，ARS(アドレス制御サーバ)のようなものが，そのネットワーク上に必要となる．ISO14443 や 7816 の様な対向通信の場合は，通信相手は一つなので，アドレス解決は，ナイーブに決まる．

次に，VITP ルータの動作を説明するために，VITP ルータが持つ情報について説明する．一言で言えば，ルータが持つ各ネットワークインタフェース毎に，VITP エンドノードが持つ情報と同じものを保持している．

**[経路制御があるネットワークへの I/F に対して持つ情報(例：IP)]**

- アドレス解決表(ARS のキャッシュ)
  (eTRON ID, IP address) のペアの集合
- アドレス解決サーバ(ARS) IP Address

- デフォルトゲートウェイ IP Address

※ アドレス解決できなかった eTRON Id へのメッセージの転送先

[経路制御がないようなネットワークへの I/F の場合(例：14443)]

- 対向の先の eTRON エンドノードの eTRON ID

これを前提に，VITP ルータの動作を以下の述べる．

- 基本的にルータが持っているすべてのネットワーク I/F について，VITP パケットが来るのを待っている．
- VITP Packet (P) を受け取る．
- P から destination node の eTRON Id を取り出す．
- どこに転送するかを決める
- まず対向 I/F (例えば，7816 や 14443)の先につながっている eTRON の ID と，destination が一致するか調べる．一致したら，それを転送先として確定する．
- 次に経路制御を伴う大きなネットワークへの I/F(例：IP)でアドレス解決を試みる．
- 解決できたら，それを転送先として確定する．
- 転送先が確定した場合はそこへ送る，確定しない場合はエラーになる．

### 3-5) VITP 暗号認証セッション

VITP は基本機能として，セッション開始時に相互認証，またセッション確立後に暗号通信を行うことができる．実際に，認証や暗号を行うためには，具体的なアルゴリズムが必要である．VITP は，認証や暗号の具体的アルゴリズムを定めるものではなく，それを適用するための共通の枠組みを提供する．

現在，VITP では，２種類の認証フレームワークを提供している．それは，２パス認証と３パス認証である．２パス認証は，２往復のメッセージ交換によって相互認証を行うためのパケット形式とその交換法式を定めるものである．また，３パス認証の場合は，ここを３往復によって行うための枠組みである．２パス認証の場合，以下の流れになる．

- １パス目：OPEN SESSION MESSAGE
- ２パス目：CONFIRM SESSION MESSAGE

３パス認証の場合は，PKI ベースの方式が前提とされており，以下の流れになる．

- １パス目：EXCHANGE CERTIFICATE MESSAGE
- ２パス目：OPEN SESSION MESSAGE
- ３パス目：CONFIRM SESSION MESSAGE

確立した認証セッションを終了するために，CLOSE SESSION MESSAGE を提供する．

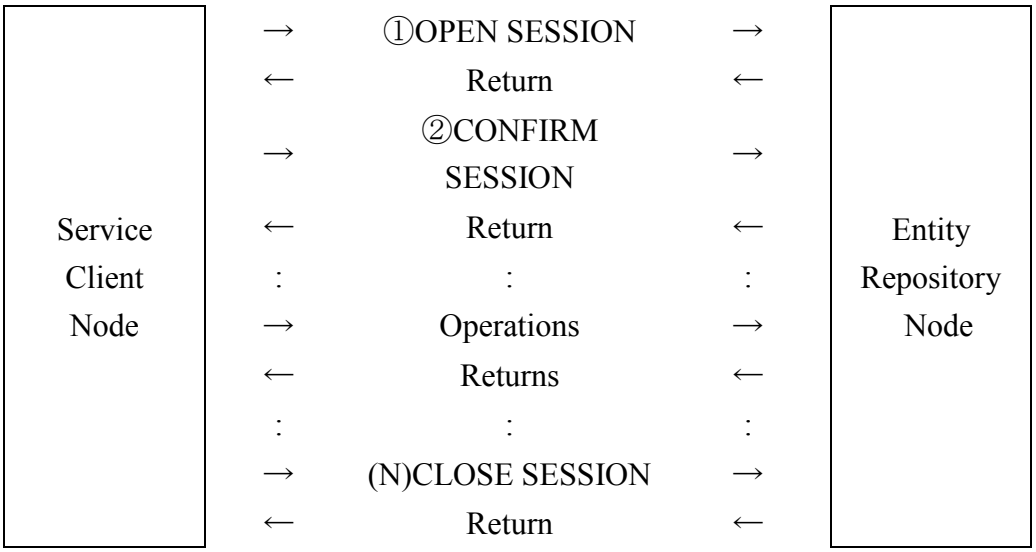



図 5.3.3-9：２パス認証によるセッション

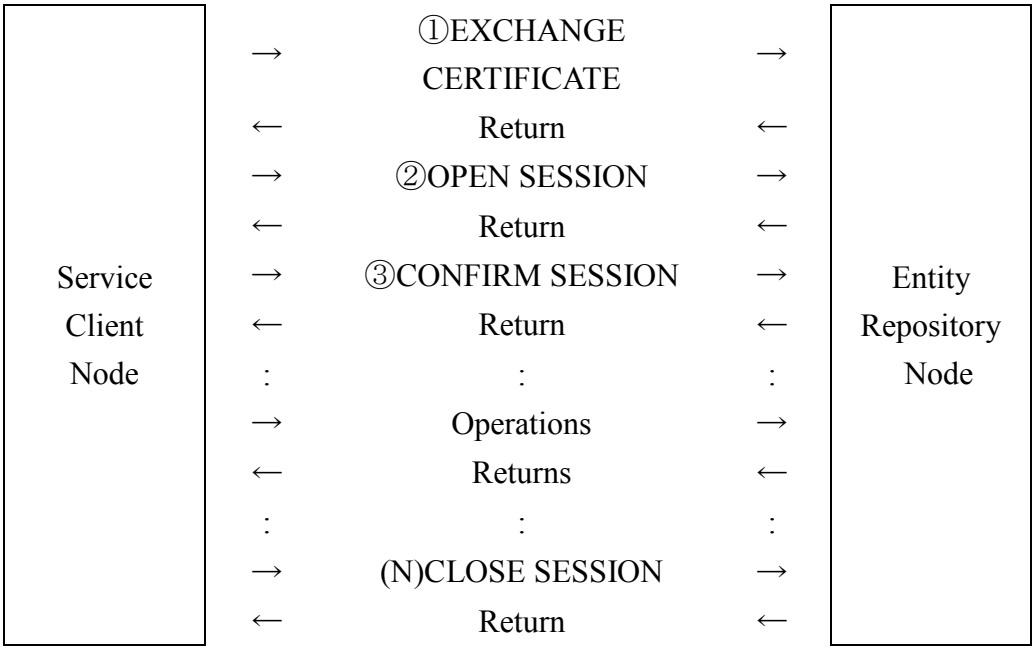



図 5.3.3-10：３パス認証によるセッション

この相互認証が PKI ベースの方式の場合は，VITN 上に証明書の破棄リスト（CRL）サーバが提供される．VITP は，この CRL サーバとの通信メッセージもサポートしている．

このセッション確立時には，通常認証を行うと同時に，秘密情報を安全に２ノード間で共有することができる．この秘密情報を使って，セッション確立後のセッション通信は，その秘密情報を鍵とした計算負荷の軽い秘密鍵暗号によりメッセージ本体を暗号化する．また，メッセージの中間攻撃や改竄を防ぐために付与される MAC も，その秘密情報を鍵とした HMAC などの方式をとることができる．

## 5.3.4 ユビキタスネットワーキング環境における交通チケットコンテンツ方式

### １）目的と概要

ユビキタスコンピューティング環境が整った社会生活においては，現在使用されている公共の交通機関（鉄道／バス／タクシー／航空／船舶）を，ユーザが事業者を意識することなく利用できることが望ましい．

上記を実現するため，交通チケットの分類／現状調査を通し，交通チケットをどのような概念でとらえるべきかを考察する．また，その概念に基づいて各交通機関のチケット内データの論理モデルを考察する．

### ２）交通チケットの位置付け

世間に流通している様々なチケットの中における交通チケットの位置付けを明確にするため，各種チケットの分類を行う（**表 5.3.4-1** 参照）．

交通チケットはその種類により，予約券型／ライセンス（定期券）型／金券型（プリペイドカード型，商品券型）のいずれかに属する．次項にて，現在使用されている交通チケットがどのように分類されるかを考察する．

### ３）交通チケットの現状

交通チケットの概念を抽象化するため，現在使用されている交通チケットの整理／分類を行う．

また，交通チケットを共通化するに当たり，現在のシステムとの互換性を図るため，現在使用されている交通チケット内データについて調査する．これに当たり，標準化された仕様がある場合，その標準に従い汎用性を持たせることが望ましいため，標準化動向についても調査を行う．

#### 3-1）現在使用されている交通チケットの整理・分類

現在使われている交通チケットを「**２）交通チケットの位置付け**」における分類とマッピングすると，下記のようになる．ただし，交通チケットとは，交通機関に乗車する時に使用するチケットを指し，その

引換券にあたるものは含めない（表 5.3.4-2 参照）.

| タイプ | | チケットの性質 | | 特定の資源の確保 | 順序性 | 譲渡性 | 匿名性 | 有効回数 | 例[1] |
|---|---|---|---|---|---|---|---|---|---|
| 引換券型 | | 取引対象を受け取る権利 | 物 | あり | なし | 要,否 | なし | 一回限り | 切手，不動産権利証 |
| 予約券型 | | | サービス（場所，時間） | | | 要 | あり | | コンサートチケット，**電車指定券，船舶指定券** |
| | | | | | | 要,否 | なし | | **航空券**，ホテル予約券，テニスコート予約券，レストラン予約券 |
| ライセンス（定期券）型 | | | サービス | なし | なし | 要 | あり | 無制限（有効期間あり） | 遊園地バス |
| | | | | | | 要,否 | なし | | ソフトライセンス，免許証，保険証券，**電車／バス定期券**，パスポート，ゴルフ会員券，違反切符 |
| 金券型 | プリペイド型 | | サービス，金 | | | 要 | あり | 回数・度数指定 | **電車／バス回数券**，テレホンカード，Ｕカード，ハイウェイカード，**イオカード，バスカード** |
| | 商品券型 | | 物，サービス，金 | | | 要 | あり | 一回限り | 商品券，ビール券，図書券，米券，印紙，切手，宿泊クーポン券，食事券，駐車サービス券，**電車乗車券，乗船券，タクシーチケット** |
| | | | | | | 要,否 | なし | | 手形，小切手 |
| 整理券型 | | 取引事実の証拠 | | なし | あり | 要 | あり | 一回限り | 購入整理券，レストラン順番待ち整理券，銀行窓口整理券，診療整理券 |
| 証明書型 | | | | | なし | 要,否 | | | 宝くじ，馬券，ナンバーズ，高速道路通行券，駐車券，預り証 |

*1　**太字**　：交通チケット

表 5.3.4-1：各種チケットの分類

| 交通機関 | 種類 | タイプ | 匿名／譲渡性 | 有効回数 | 割引 | 例 |
|---|---|---|---|---|---|---|
| 鉄道 | 定期／ストアードフェアカード融合型 | ライセンス（定期券）型+プリペイド型 | なし | なし | あり | Suica カード |
| | 定期乗車券 | ライセンス（定期券）型 | なし | なし | あり | 通勤，通学，その他 |
| | 周遊券<br>イベント乗車券<br>Q キップ・S キップ等 | | あり | なし | あり | |
| | ストアードフェアカード | プリペイド型 | あり | なし | なし | イオカード，パスネット，スルッと KANSAI 等 |
| | プリペイドカード | | あり | なし | なし | オレンジカード等 |
| | 回数乗車券 | | あり | あり | あり | 普通，均一，特殊 |
| | 普通乗車券 | 商品券型 | あり | １回 | なし | 片道，往復，連続 |
| | 特別急行券<br>急行券 | | あり | １回 | なし | |
| | 指定券 | 予約券型 | あり | １回 | なし | |
| バス | ストアードフェアカード | プリペイド型 | あり | なし | あり | |
| | 定期券 | ライセンス（定期券）型 | なし | なし | あり | 通勤，通学，その他 |
| | 回数券 | プリペイド型 | あり | あり | あり | |
| タクシー | タクシーチケット | 商品券型 | なし | １回 | なし | |
| | プリペイドカード | プリペイド型 | あり | なし | あり | |
| 船舶 | 乗船券 | 商品券型 | あり | １回 | なし | |
| | 指定券 | 予約券型 | あり | １回 | なし | |
| 飛行機 | 搭乗券 | 予約券型 | なし | １回 | なし | |

表 5.3.4-2：交通チケットの分類

### 3-2) 標準化の動向

#### ■ 複数事業者間で利用される交通チケット

**【標準化団体等】**

平成８年度から 11 年度にかけ，日本鉄道サイバネティクス協議会，汎用電子乗車券開発検討委員会，汎用電子乗車券技術研究組合(TRAMET)の三者が協力し合い，IC カードを使用した汎用電子乗車券システムの利用モデルを作成した．

- 汎用電子乗車券開発検討委員会
  次世代の乗車券として非接触式の IC カードを用いた「汎用電子乗車券」のコンセプトの検討を行った.
- 汎用電子乗車券技術研究組合(TRAMET)
  公共交通機関の汎用電子乗車券の普及・促進のため，現行磁気カードに寄せられる諸課題(自動改札の混雑，料金精算の複雑さ・繁雑さ，公共交通機関の共通利用範囲の拡大等)を解決し，多様化・高度化する情報化社会，キャッシュレス社会に適応できる次世代乗車券の基盤技術の確立を図った.

**【規格内容】**

汎用電子乗車券技術研究組合で規定された規格について調査を行った.

汎用電子乗車券技術研究組合では，ＳＦカードの実用化及びこれを非接触型定期券と併用化した場合の下記の内容ついて検討を行い，平成 12 年 3 月にカードの標準仕様を策定した.

a)定期券区間外で乗降する際の運賃精算の仕組み
b)バス，タクシー等の複数の交通機関における利用
c)駅構内での買い物における利用
d)クレジットカード，銀行カードなどのサービスカードとの共通化

規格には，電波方式や利用者の情報管理の方法，自動改札機などの内容も含まれるが，本調査では，IC カード内のチケットデータに関する部分のみを取り扱う．また，その中でもチケット内のデータ項目／データ構成に関してはここには記載せず，参考となるチケットの捉え方について，汎用電子乗車券技術研究組合の IC カード部会研究成果の要約を記載する.

・規定範囲

汎用電子乗車券技術研究組合で規定した内容は，**図 5.3.4-1** の範囲である.

| ストアードフェア | 普通乗車券 | | | 定期乗車券 | | 回数乗車券 | | 特殊乗車券 | | その他特殊券 | バリューカード情報 | クレジットカード情報 | 電子マネー情報 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 片道乗車券 | 往復乗車券 | 連続乗車券 | 通勤定期乗車券 | 通学定期乗車券 | 普通回数乗車券 | 均一回数乗車券 | 急行券 | 特別車両券等 | | | | |

網掛け部分が TRAMET で仕様を決めた部分

図 5.3.4-1：「規定範囲」

・汎用電子乗車券の考え方

切符や定期券の概念を徹底的に抽象化することにより，現行の定期券と切符を，「料金割引権（定期券）付きストアードフェアカード」という 1 つの概念（同じオブジェクトクラスからコピーし，生成された 2 つのインスタンスで定期券と切符のそれぞれを表現し，両者の違いは，ある特定のプロパティの違いだけ）で表現した．

これまで定期券，ストアードフェアカード，融合型（定期＋SF）と 3 種類の概念で捉えられていたものを，料金割引率とストアードフェアのプリペイド額が異なる料金割引権（定期券）付きストアードフェアカードと捉えることにより，1 つの概念にまとめたのである．これにより，これまでの 3 種類の概念は下記のように表された．

a)　融合型（定期＋SF）

料金割引権（定期券）付きストアードフェアカード

b)　定期券

料金割引権（定期券）付きストアードフェアカードだが，プリペイド残高が 0 円のカード

c)　ストアードフェア

割引率 0%の料金割引権付きストアードフェアカード

これは，定期券を切符の一種としてではなく，料金割引権の先払い購入であると捉えたことにより実現した．

・本来あるべき乗車券の流れ

現在の乗車券にて清算が必要になる原因は，乗車券が暫定的に目的地を定めての先払い方式で，実際には経路変更等は自由に行う事が可能

であることによる．乗車券の流れを下記のように整理することにより，清算処理をなくすことができる．

step1）乗った駅が判明するような入場証明を乗車駅で受け取る
step2）目的地で入場証明を提示する
step3）目的地の駅員が乗車料金を計算する
step4）もし定期券所有者であれば，定期区間を考慮し，乗車料金の計算を行う
step5）請求額に従い，料金を払う

**【導入事例】**

・都営地下鉄 12 号線，都営バスでの実証実験

汎用電子乗車券技術研究組合で行った実証実験の適用範囲は**表 5.3.4-3** の通りである．

a)定期券＋SF についてのみ規定する
b)回数券／中長距離乗車券／金融カードについては規定しない
c)乗車券の種類と規格の適用範囲は以下の通り

| 乗車券の種類 | 適用範囲 | 考え方 |
|---|---|---|
| 定期券 | ○ | 規定する |
| 近距離乗車券 | × | SF で置き換え可能と考える |
| ストアードフェア | ○ | 規定する |
| 回数券 | × | 規定しない |
| 中距離乗車券 | × | 規定しない |
| 金融カード（クレジットカード） | × | 規定しない |

表 5.3.4-3：「実験の適用範囲」

d)バス定期券は鉄道定期券の付属的位置づけとし，バス定期券単独での利用はないものとする
e)バスでの定期の利用は区間フリーの均一料金とする
f)バスでの SF の利用は，鉄道と同一の SF を使用するものとする

**■鉄道**

**【標準化団体等】**

鉄道に関する各種標準規格を定めているのは，日本鉄道サイバネティクス協議会（ＣＪＲＣ）である．

各鉄道事業者は日本鉄道サイバネティクス協議会に仕様を開示して

もらい，これに準拠したシステムを導入している．基本的に，鉄道業界に関してはここで決めた仕様に準拠していないコンテクストはないものと考えられる．ただし，この仕様は，民間企業が営利目的のシステム構築を計画した場合，それに関連する事業者・メーカーなどにのみ開示される．

**【規格内容】**

日本サイバネティクス協議会では，汎用電子乗車券技術研究組合にて規定した仕様を参考にしているため，ここでは特に内容について記述しない．

**【導入事例】**

- スルッとＫＡＮＳＡＩ
- Suica カードシステム

**■バス**

**【標準化団体等】**

- バス共通カード規格管理委員会
  東京・神奈川・埼玉・千葉の一都三県に路線を持つ主なバス事業者で共通して利用できるバスカードの規格を制定している．
- その他
  各地のバス会社にて，磁気や非接触 IC カード型のプリペイドカード導入している．これらのシステムのうち，鉄道と共通で使用可能なものはもちろん，将来鉄道と共通化することを念頭に置き，日本鉄道サイバネティクス協議会で規定した標準仕様に準拠しているものも存在する．

**【導入事例】**

- バス共通カードシステム：バス共通カード規格管理委員会で規定した仕様
- 非接触 IC カード乗車券・定期券システム（山梨交通）：日本サイバネティクス協議会仕様

**■タクシー**

**【標準化団体等】**

タクシーチケットは，各クレジットカード会社で発行されたものが，

当該クレジットカードの引き落とし口座からの引き落としに，また，企業向けに発行されたものが，当該企業の口座からの引き落としに対応しているといった状態であり，標準化のための機関等は存在しない．また，タクシー業界内では，事業者独自仕様のプリペイドカードシステムを導入している事業者や，クレジットカードによる支払いに対応している事業者も増えているが，これについても標準化のための機関等は存在しない．

ただし，日本鉄道サイバネティクス協議会で規定した汎用電子乗車券は，タクシーにも共通で使えるよう意識した設計となっている．

**■航空**

**【標準化団体等】**

航空業界における標準化団体は IATA（国際航空輸送協会）である．定期国際航空輸送の 95%以上を担う 200 社以上が IATA に加盟しており，その規格に準拠している．

**【規格内容】**

発券した航空会社や代理店に関わらず，全てのチケットの情報がどのチェックイン機でも読み取ることができるようにするため，チケット内の論理データのみでなく，チェックイン機などについても規定している．

最新の規格では，航空券をペーパーレス化し，搭乗カウンターで本人の確認を取るだけで，飛行機に乗ることができるようにする集中管理サービスを取り扱っている．

**【導入事例】**

現在一般的に使用されている，磁気テープのついたボーディングパス／搭乗券一体型のチケットに関しては，ほぼ全ての事業者が IATA の規格に準拠している．

E-Ticket サービスの導入事例は下記の通り．

- British Airways
- United Airlines, American Airlines, Northwest, Airlines
- JAL, ANA （日系のエアラインについては，一部路線）

**■船舶**

標準化のための機関等は存在しない．

### ４）現状のまとめ

**「汎用電子乗車券の考え方」**における，本来あるべき乗車券の流れの考え方を基に，回数券や中長距離乗車券も含めた交通チケットについて下記のように整理した．

**【基とした本来あるべき乗車券の流れ】**

step1）乗った駅が判明するような入場証明を乗車駅で受け取る
step2）目的地で入場証明を提示する
step3）目的地の駅員が乗車料金を計算する
step4）もし定期券所有者であれば，定期区間を考慮し，乗車料金の計算を行う
step5）請求額に従い，料金を払う
（引用：汎用電子乗車券技術研究組合　IC カード部会研究成果から）

step1，2，3 に関しては，現在鉄道，バス，タクシー，船舶の共通の考え方と言える．Step4 については，鉄道，バスの共通の考え方と言える．

汎用電子乗車券技術研究組合では，ストアードフェアと定期券についてのみ考察しているが，実際には，定期券を割引券として捉えている．したがって，「定期券（割引権）」→「乗車場所と下車場所以外の情報により，料金の計算に影響が与えれられるもの」と置き換えると，回数券，プレミアム付き乗車券，中長距離乗車券，指定券といった，様々なチケットについてもここで考えることができるようになる．

ここで，

a)乗車場所と下車場所の情報のみにより，乗車料金が決まる＝単純積み増し／引き落とし可

b)乗車場所と下車場所以外の情報が，料金に影響を与える＝単純積み増し／引き落とし不可

とし，現在使用されている交通チケットを，単純積み増し／引き落とし可能か不可能かによって分類した（**表 5.3.4-4**）．

| 単純積み増し／引き落とし | チケットの種類 | 交通機関 | 情報 |
|---|---|---|---|
| 可 | ストアードフェアカード | 鉄道／バス | 乗車地点と下車地点の情報から判断できる金額情報 |
| | プリペイドカード | 鉄道 | |
| | 普通乗車券 | 鉄道 | |
| | 特別急行券<br>急行券 | 鉄道 | |
| | タクシーチケット | タクシー | |
| | 乗船券 | 船舶 | |
| 不可 | 定期／ストアードフェアカード融合型 | 鉄道 | 期間情報<br>区間情報<br>個人情報 |
| | 定期券 | 鉄道／バス | |
| | 周遊券<br>イベント乗車券<br>Q キップ・S キップ等 | 鉄道 | 期間情報<br>区間情報 |
| | 回数券 | 鉄道／バス | 回数情報<br>区間情報 or 価格情報 |
| | 指定券 | 鉄道／船舶 | 区間情報<br>座席情報 |
| | 搭乗券 | 飛行機 | 日付情報<br>区間情報<br>座席情報<br>個人情報 |

表 5.3.4-4：交通チケットの整理

交通チケットを「料金割引権（定期券）付きストアードフェアカード」という１つの概念で表した汎用電子乗車券技術研究組合の考察とは反するが，「交通チケットの整理」の表と「本来あるべき乗車券の流れ」を併せると，単純積み増し／引き落とし不可な「料金割引権（定期券)」を，事前に用意する特別なチケットとして切り離すことにより，「本来あるべき乗車券の流れ」は交通チケットを用意することなく，汎用の電子マネーで代用できる．下記のように整理した．

従来の交通チケットを

a)マネー型（単純積み増し／引き落とし可）

b)チケット型（単純積み増し／引き落とし不可）

に大きく二分する．

### 4-1）マネー型

**【特徴】**

- 単純積み増し／単純引き落としが可能
- 割引なし

- 汎用で使用可能

**【乗車券の流れ（マネー型）】**

step1）乗車地点が判明するような入場証明を乗車地点で受け取る
step2）目的地で入場証明を提示する
step3）目的地の係員が乗車料金を計算する．
Step4）もしチケット型交通チケットの所有者であれば，その区間を考慮し，乗車料金の計算を行う．
Step5）請求額に従い，料金を払う（計算処理）

**【結果】**

- マネー型の交通チケットに関しては，乗車地点の情報を保持する必要がある．
- 料金計算機能は交通機関特有のものであるが，計算された金額を引き落とすだけの処理であるため，交通チケットとしてのストアードフェアを用意する必要はなく，汎用の電子マネーが使用可能である．

### 4-2）チケット型

**【特徴】**

- 単純積み増し／単純引き落としが不可能
- 事業者個別の情報が必要
- 交通チケットの種類により，必要となる情報が異なる

**【乗車券の流れ（チケット型）】**

step1）席情報，利用期間情報，利用区間情報，割引情報等を事前に受け取る（前精算処理）
step2）乗った駅が判明するような入場証明を乗車駅で受け取る
step3）目的地で入場証明，および①の情報を提示する
step4）利用区間外であれば，目的地の駅員が区間外の乗車料金を計算する．
step5）請求額に従い，料金を払う（再計算／後精算処理）

**【結果】**

- 交通チケットの種類によって必要とされるデータが異なるため，これらの交通チケットに関し，チケット内データの考察が

必要となる.

- アプリケーションにより，交通チケットをダウンロードする場合とサーバに置いておく場合があるが，サーバに交通チケットを置いておく場合，手元に送られてくるものは引換券にあたるため，交通チケットに含めない.

例)航空業界における E-Ticket

### ５）サービスモデル

ユビキタスコンピューティング環境において交通チケットを使用するシーンを考察し，サービス要件を明確にする．また，**「４）現状のまとめ」**と併せ，交通チケット内データの論理モデルを作成する.

#### 5-1）シーンの考察

**■デバイス非依存**

**【サービスイメージ】**

携帯電話，PDA，IC カードなど，利用者が使いたいデバイスにチケットを入れ，使用可能．また，２人分まとめて購入したチケットなどの譲渡も可能.

**【サービスの流れ】**

**図 5.3.4-2** 参照.

**【サービス要件】**

- 常に身近にインターネット接続が可能なデバイスがあること
- いつでもどこでもインターネットを通して電子チケットが購入できること
- 購入したチケットをどんなデバイスにも移せること
- 購入したチケットを譲渡できること

**【機能要件】**

身近にあるデバイスを利用した

- インターネットを通した各種交通機関のチケットの購入／ダウンロード機能
- インターネットを通した電子マネーのダウンロード機能
- 券売機（駅／バス車内など）における非接触でのチケット購入

機能（インターネット接続不要）
- 各種交通機関の改札における電子マネーの使用機能
- チケットのデバイス間移動機能
- チケットの譲渡機能

**■色々な交通機関に精算なしで乗車可能**

**【サービスイメージ】**

電子マネーと電子チケットを同一デバイスに入れ，電子マネーをストアードフェアとして使用することにより，指定席や定期券以外は，チケットの購入，精算，チャージの必要がなく，全ての改札を通過可能（定期券外への乗り越し，異なる事業者への乗り越しに関しても同様）.

**【サービスの流れ】**

図 5.3.4-3 参照.

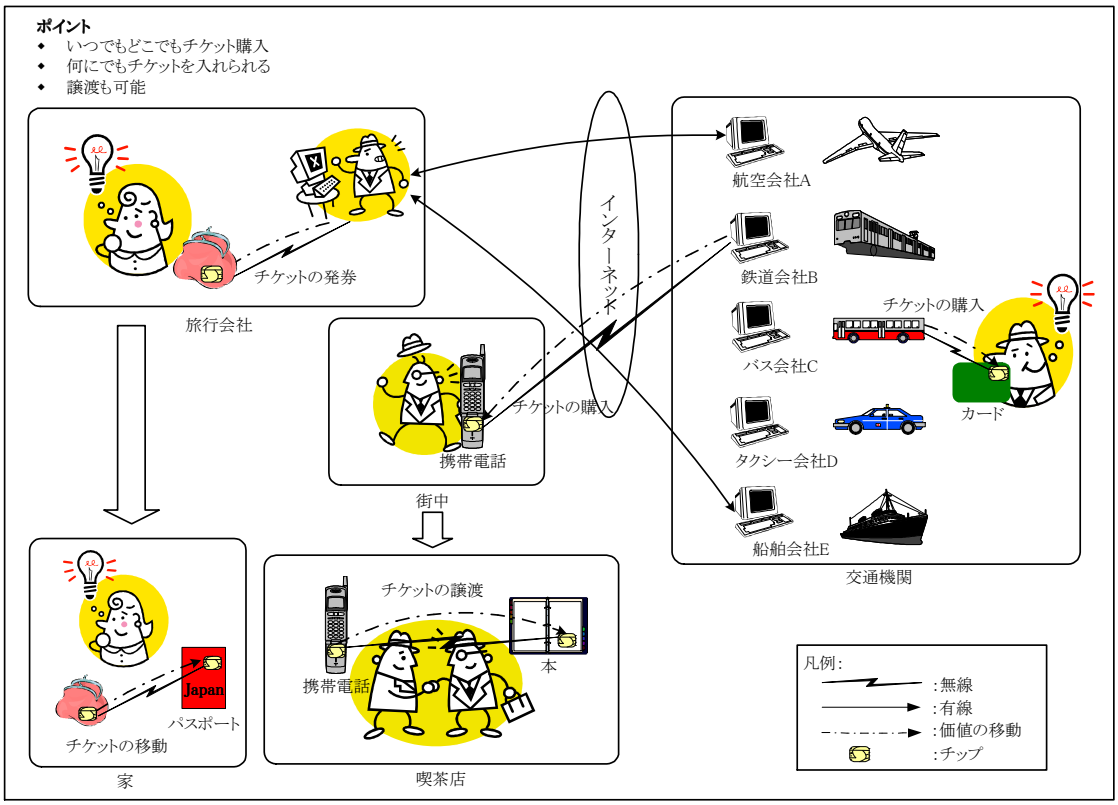



図 5.3.4-2：デバイス非依存

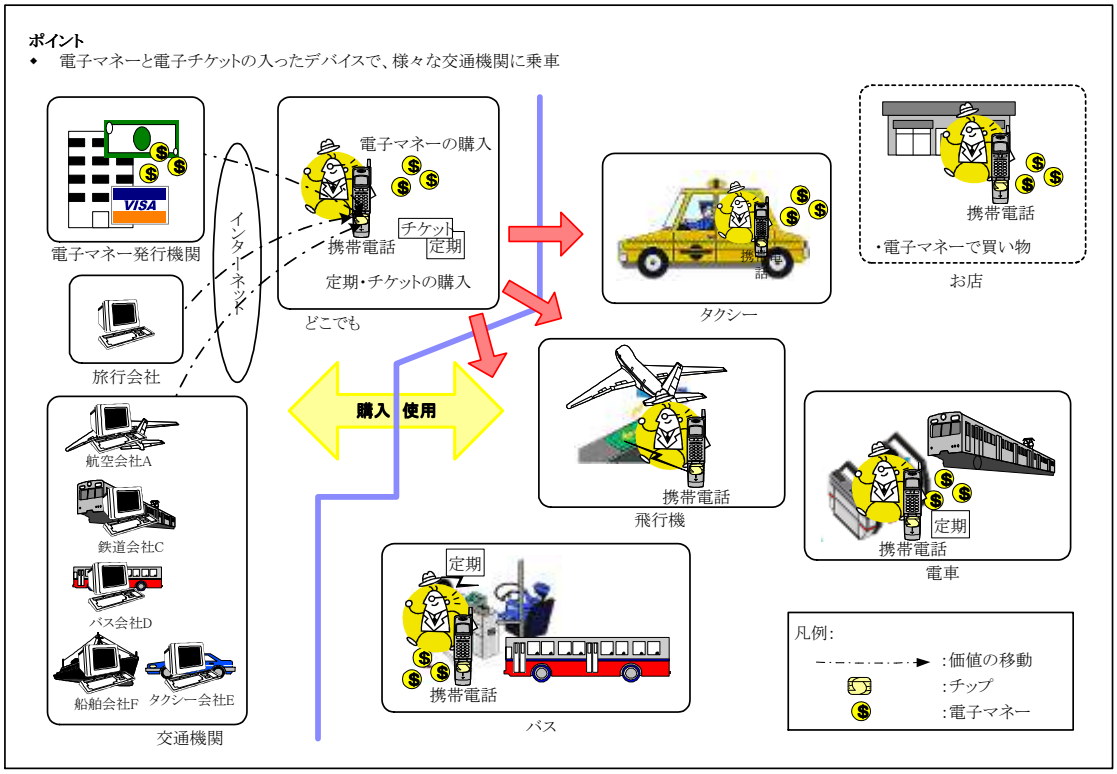



図 5.3.4-3：様々な交通機関に精算なしで乗車可能

**【サービス要件】**

- 電子マネーと電子チケットの併用により，精算することなく全交通機関に乗車できること

**【機能要件】**

- 各種交通機関の改札における電子マネーと電子チケットの使用機能
- 乗車場所書き込み機能
- 乗車場所読み取り／料金計算機能（定期券／その他チケットを併用時を含む）

### 5-2）交通チケットに関する要件

「5-1）シーンの考察」で挙げられた要件を整理すると，表 5.3.4-5 のようになる．

| チケットタイプ | | 属性 | 要件 | 例 |
|---|---|---|---|---|
| 電子マネー型／<br>電子チケット型共通 | | | • インターネットを通して購入／ダウンロード<br>• 券売機等にて非接触にて購入<br>• デバイス間移動<br>• 譲渡 | |
| 電子マネー型 | | 乗車場所情報<br>残高情報 | • 乗車場所書き込み／読み取り<br>• 乗車場所からの料金計算（事業者間乗り換えを含む）<br>• 電子チケットの情報を加味した料金計算 | |
| 電子チケット型 | 定期券型 | 個人情報<br>期間情報<br>区間情報 | • 期間切れ時の更新 | 定期券 |
| | 予約券型 | 個人情報<br>期間情報<br>区間情報 | • 譲渡不可能とする機能 | *1 航空券 |
| | | 期間情報<br>区間情報 | | 新幹線指定券 |
| | プリペイド型 | 事業者情報<br>残高情報<br>（期間情報）<br>（区間情報） | • 事業者ごとにプレミアム情報を管理<br>• 降車時に，当該事業者領域に残高がある場合は，そこを優先に使用する機能 | プレミアム回数券 |

*1 e-Ticket 対応の航空券は本研究テーマの対象外とする

表 5.3.4-5：「交通チケットへの要件」

### 5-3) 交通チケット内データ

**■コンセプト**

- 汎用電子マネー情報については，交通チケットとは別に用意された汎用電子マネーのフォルダを参照する．
- 個人属性情報は，電子チケット型の交通チケット購入時に必要となることがあるが，事業者ごとに同じ個人属性情報を保持するのは冗長であるため，交通チケットとは別に用意された個人属性情報のフォルダを参照する．
- 全交通チケットを，電子マネー型と電子チケット型に分類する．
- セキュリティや認証が万全なデバイス，ネットワークを使用する．

【電子マネー型】

- 汎用電子マネーを使用する
- 入場／出場のログを取る
- 基本的には，汎用電子乗車券技術研究組合で規定したカード内データフォーマットを踏襲する．

【電子チケット型】

- 事業者ごとにフィールドを用意する
- 定期券型のデータについては，基本的には，汎用電子乗車券技術研究組合で規定したカード内データフォーマットを踏襲する
- 予約券型，プリペイド型のデータについては，汎用電子乗車券技術研究組合で規定したカード内データフォーマットの定期券型を参考にし，追記した

■データ構成

図 5.3.4-4 参照.

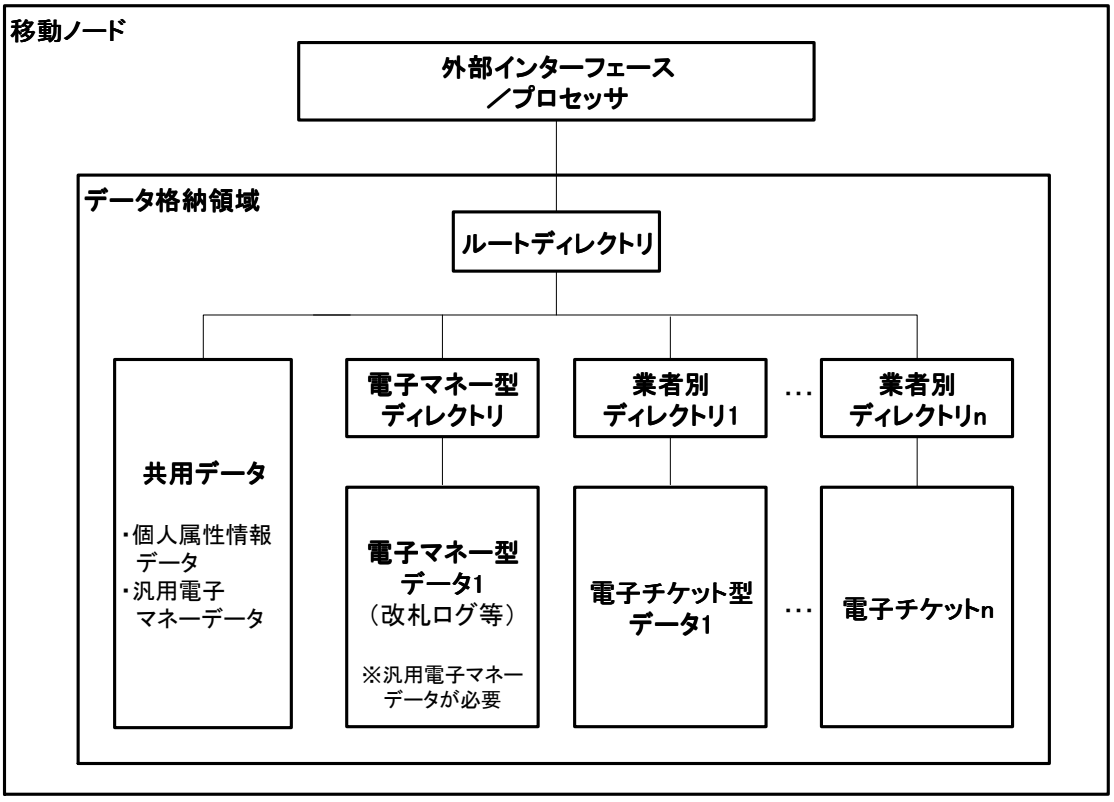



図 5.3.4-4 :「データ構成」

■論理データフォーマット

図 5.3.4-5 IC チップ内データフォーマット参照（別紙）

5-4）交通チケットを利用したサービス

これまでに考察した交通チケットをユビキタスコンピューティング環境で使用することにより，実現可能となるサービス例を２つ挙げる．

■指定席のサービス

【サービスイメージ】

予約席に座ると，座席に埋め込まれたチップとチケットが通信し，正しい人が座っていれば車掌の持つリストにその旨が通知される

【サービスの流れ】

図 5.3.4-6 参照

■行き先ルート検索

【サービスイメージ】

PDA などにチケットを差し込むなどし，行き先を指定すると，ルート検索が可能

【サービスの流れ】

図 5.3.4-7 参照

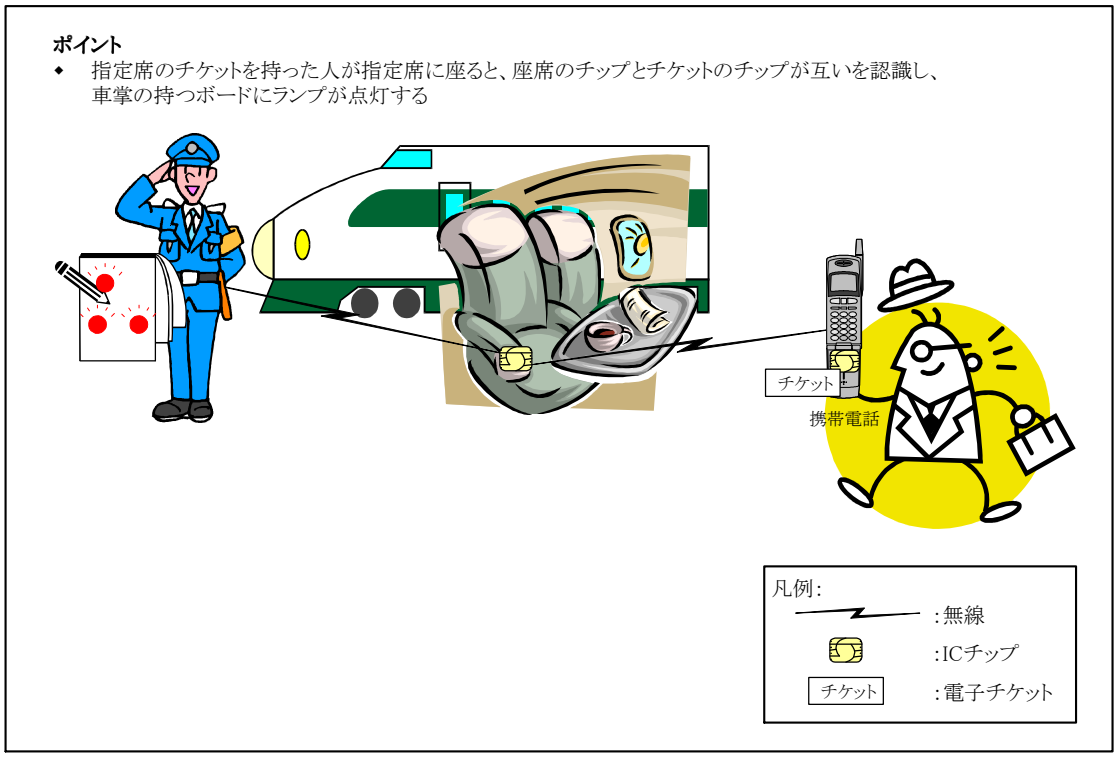



図 5.3.4-6：指定席のサービス

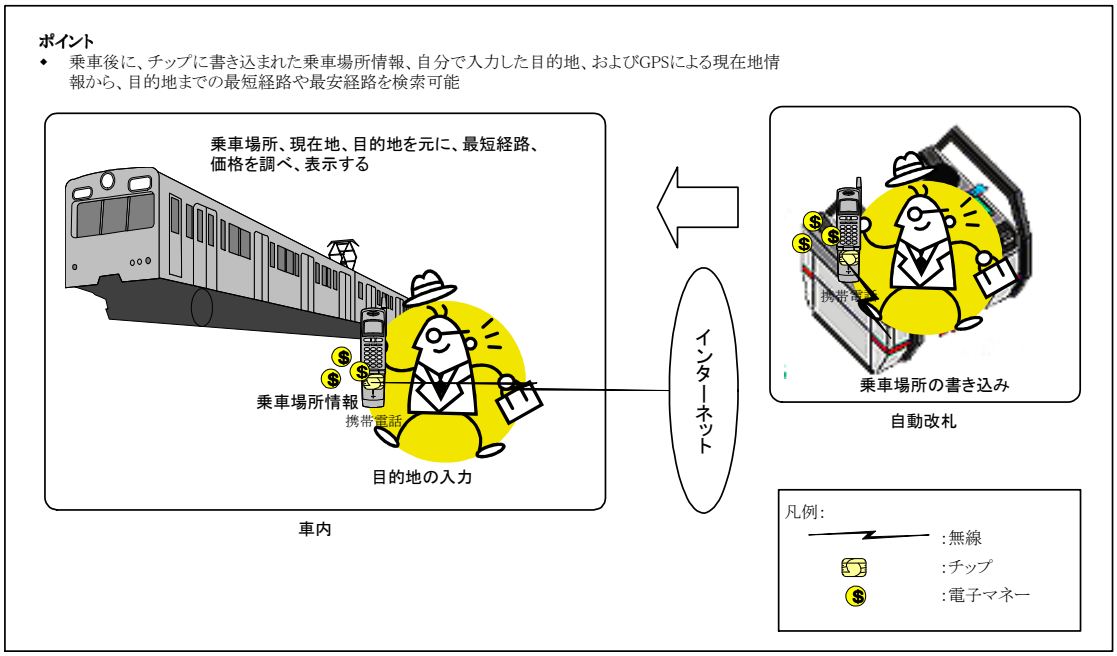



図 5.3.4-7：行き先ルート検索

## ６）課題

### 6-1）移行期における現行システムとの互換性

現在使用されている磁気カードのリーダは，IC カードと互換性がない．本研究課題では，考察した論理モデルを格納する媒体は問わないが，現行の磁気カードリーダ，IC カードリーダ等と互換性を取る必要がある

### 6-2）各事業者／標準化団体に規格を採用してもらう必要性

- 各事業者（交通機関，旅行会社等）に関する導入効果（販売促進効果／経費節減効果）の考察など，規格を採用してもらうためのビジネスモデルが必要となる
- 国内の各標準化団体に当該論理モデルを規格として採用し，全交通機関で共通して利用する必要がある

### 6-3）ハードや処理速度などの物理的制約

- 全交通チケットを１つの媒体に入れることにより，全体の容量が大きくなる．そのため，現在の媒体内に格納した上で，必要な処理速度が保てるかを検討する必要がある
- 各種情報種別間でのトランザクションが発生するため，現在のリーダ／ライタで充分な処理速度が出るかを検討する必要がある
- 定期券を２枚，プレミアムの付いたチケット型データを１枚所有した場合，340byte 程度となる

### 6-4）セキュリティ

- 交通チケットの偽造防止のための仕組みやデバイスが必要となる
- 譲渡時にチケットが偽物でないことを確認する方法が必要となる

### 6-5）論理モデル内

- 事業者別に情報を用意することにより，データに冗長性が出る
- 情報種別を規定したため，各情報種別間でトランザクションが発生する．トランザクション量を最低限に抑えるシーケンスが必要となる
- 駅コードなど，事業者間で使用する情報を統一しなければならない
- 交通チケットをダウンロードしないサービスに関し，交通チケ

ットを受け取る際に必要となる個人認証に，本論理モデルの個人属性情報を使用することが望ましい．実現方法の考察が必要である．

### 6-6) 考察範囲

今年度は，公共の交通機関に乗車してから下車するまでのサービスモデルについて考察したが，交通コンテクストには「個人の移動」や「交通機関の設備（空港やホームなど）の利用」なども含まれる．この部分では，位置情報を使用することにより，ユビキタスコンピューティング環境特有の様々なサービスが考えられるが，未考察である．

**例１）エスカレータ（場所は問わない）**

車椅子がエスカレータに近づくと，エスカレータが車椅子のチップから車椅子が近づいたことを判断し，一段の幅を広くする

**例２）車の運転**

左折のウィンカーを出すと，左後ろにバイクがいないか，曲がった先や横断歩道に歩行者がいないかをチップによってセンスし，通知してくれる

## 参考文献


### (1)　複数事業者間で利用される交通チケット

- 「プリペイドカード」
  http://www5a.biglobe.ne.jp/~hirok/prepaid/
- 「オクトパスカード　基本編」,「オクトパスカード　応用編」
  All About Japan
  http://allabout.co.jp/travel/travelhongkong/closeup/CU20011210A/index.htm
- 「不揃いなカード達」　上海事情
  http://www.mrisys.net/SHANGHAI/REVERSAL/2001/011012.html
- 「汎用電子乗車券技術研究組合　IC カード部会研究成果」
  TRAMET
- 「汎用電子乗車券とは」　国土交通省
  http://www.mlit.go.jp/sogoseisaku/ns/jireishuu/bus/iccasdshiryou_1.htm

- 「共通乗車カードシステムの導入」　国土交通省
  http://www.mlit.go.jp/sogoseisaku/ns/jireishuu/tetsudou/kyotuca.htm
- 「駅における IT」　鉄道総研月例発表会　輸送情報技術研究部（旅客システム）　研究室長　後藤 浩一
  http://www.rtri.or.jp/infoce/getsurei/2001/Getsu09/g143_3.pdf

(2)　鉄道

- 「IC カード乗車券規格を開示」　IC カードシステム利用促進協議会
  http://www.jicsap.com/
- 「鉄道・バス共通乗車システム「スルッと KANSAI」　国土交通省
  http://www.mlit.go.jp/sogoseisaku/ns/jireishuu/tetsudou/kyotuca.htm
- 「スルッと KANSAI」
  http://www.ya.sakura.ne.jp/~tokuden/info/surutto.html
- 「Suica」　JR 東日本
  http://www.jreast.co.jp/suica/
- 「次世代交通カード革命」　ＮＴＴ出版　編者：圓川　隆夫
-

(3)　バス

- 「バス共通カードシステムの導入」　国土交通省
  http://www.mlit.go.jp/sogoseisaku/ns/jireishuu/bus/kyoutsuu.htm
- 「バス＜共通＞カードのホームページ」
  http://www.kurumi.sakura.ne.jp/~buscard/
- 「バス IC カード乗車券・定期券システム」　NTT データ
  http://www.nttdata.co.jp/service/s0606106.html
- 「非接触 IC カード乗車券＜1＞」　国土交通省
  http://www.mlit.go.jp/sogoseisaku/ns/jireishuu/bus/iccard1_1.htm
- 「バスカードご利用ガイド」　道北バス
  http://www1.biz.biglobe.ne.jp/~dohoku/

### (4) 航空

- 「IATA（国際航空輸送協会）の目的」 ISO 中央事務局 http://www.net.intap.or.jp/INTAP/information/journal/no.50/materials50.htm
- 「 Resolution 722c Automatic Ticket/Boading Pass-Version2(ATB2)」 IATA
- 「Resolution 722d Off Premise Automatic Ticket/Boading Pass-Version2(OPATB2)」 IATA
- 「E-ticketing An interline solution」 IATA&SITA
- 「Interline Electronic Ticketing」 IATA&SITA
- 「IATA と米 IBM, 鉱区業界向けの e-ticket システムを共同開発」 ASCII24 http://ascii24.com/news/i/serv/article/1999/08/18/603946-000.html
- 「E チケット」 United Airlines http://www.unitedairlines.co.jp/site/united/e-chicket.htm

## 5.3.5 ユビキタスネットワーキング環境における個人属性情報

### 1) 目的と概要

ユビキタスコンピューティング環境が整った社会生活においては，数多くのコンピュータの間を，個人情報を含んだデータが無数に往来することが想定され，より効率的かつ安全に個人情報を取り扱う必要がある．

上記を実現するために，ユビキタスコンピューティング環境における最適な個人情報の表現形式と，各ノードでの個人情報の取り扱いについて述べるとともに，実現に向けた課題を抽出する．

### 2) 個人属性情報の現状分析

#### 2-1) 定義

本研究課題における個人情報の定義は，

- 「個人に関する情報であること」
- 「それによって個人を識別できるもの」（他の情報と照合し個人を識別できるものを含む）
- 「それを利用することによってサービスの享受を期待できるもの」

の三点を満たすものとする．

また，このようなユビキタスコンピューティング環境における個人情報を「個人属性情報」と呼び，一定の目的を達成するために体系的に構成された個人情報の集合物を「個人属性情報利用形態」とし，以下「利用形態」と呼ぶ．

#### 2-2) 個人属性情報の分類

実社会において使用されている個人属性情報の分類について以下**表 5.3.5-1「個人属性情報分類表」**に示す．

| 分類 | | 個人属性名 | 評価項目 | | | | | | | | | | 備考・説明等 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 識別性 | | 使いやすさ | | | | 唯一性 | 不変性 | 共用性 | 詐称困難性/公証可能性 | 提供受容性 | |
| | | | 単独での個人識別性 | 他情報との照合による識別性 | 呼称としての利用性 | 馴染み深さ | 件数・種類の少なさ，体系化 | 単純さ・短小さ | | | | | | |
| 個人識別情報 | 基本情報 | 氏名 | 高 | 高 | 高 | 高 | 中 | 中 | 中 | 中 | 高 | 高 | 中 | ユニークではない<br>国や地域により，複雑・長大な表現内容 |
| | | 住所 | 中 | 高 | 低 | 高 | 中 | 中 | 高 | 高 | 高 | 高 | 中 | |
| | | 生年月日，年齢 | 中 | 高 | 低 | 高 | 高 | 高 | 中 | 高 | 高 | 高 | 中 | |
| | | 性別 | 低 | 中 | 低 | 高 | 高 | 高 | 低 | 中 | 高 | 高 | 高 | |
| | | 連絡先電話番号 | 中 | 高 | 低 | 高 | 中 | 高 | 高 | 中 | 高 | 低 | 中 | ユニークだが，家族等と共用の場合あり |
| | | 家族構成 | 中 | 高 | 低 | 高 | 中 | 中 | 中 | 中 | 高 | 高 | 中 | |
| | 一定環境下での情報 | 役職・肩書き | 低 | 中 | 中 | 中 | 中 | 高 | 低 | 低 | 中 | 高 | 中 | |
| | | 組織内 ID | 高 | 高 | 中 | 低 | 高 | 高 | 高 | 中 | 低 | 低 | 高 | 社員番号／学籍番号など |
| | | 電子アドレス | 高 | 中 | 中 | 中 | 中 | 中 | 高 | 中 | 中 | 中 | 中 | メールアドレス，ip アドレス |
| | | エイリアス | 中 | 高 | 高 | 中 | 低 | 高 | 低 | 低 | 高 | 低 | 高 | ニックネーム，ペンネーム，ハンドルネーム |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | デジタル証明書 | 高 | 高 | 中 | 低 | 中 | 中 | 高 | 高 | 高 | 高 | 高 | |
| | | バイオメトリクス情報 | 高 | 高 | 低 | 低 | 中 | 中 | 高 | 高 | 中 | 高 | 中 | 指紋・声紋・虹彩・DNA 情報 |
| 特定サービス情報 | | 個人信用情報 | 低 | 低 | 低 | 中 | 低 | 低 | 低 | 低 | 中 | 中 | 低 | 金融・資産関連・預貯金残高 |
| | | 趣味・嗜好 | 低 | 低 | 低 | 中 | 低 | 低 | 低 | 低 | 中 | 中 | 低 | |
| | | 身体特性 | 中 | 中 | 低 | 中 | 低 | 低 | 中 | 高 | 中 | 中 | 低 | |
| | | 交友関係 | 中 | 中 | 低 | 中 | 低 | 低 | 中 | 中 | 中 | 中 | 低 | |
| | | 就学・就業先 | 中 | 中 | 低 | 中 | 低 | 中 | 中 | 中 | 中 | 中 | 低 | |
| | | 学歴・結婚暦 | 低 | 低 | 低 | 中 | 低 | 中 | 低 | 高 | 中 | 中 | 低 | |
| | | 性格診断／心理テスト | 中 | 中 | 低 | 低 | 低 | 低 | 中 | 中 | 中 | 中 | 低 | |
| | | 個人医療情報 | 高 | 高 | 低 | 低 | 低 | 低 | 高 | 高 | 低 | 中 | 低 | カルテ・病歴, 看護/検査記録/レセプト |
| | | 収集・利用・提供の基本禁止事項（許可・手続きを要する） | 低 | 低 | 低 | 低 | 低 | 低 | 低 | 低 | 低 | 中 | 低 | 人種, 民族, 門地, 本籍,<br>信教（宗教・思想・信条）<br>政治的見解, 労働組合への加盟,<br>保健医療及び性生活,<br>前科・犯暦 |
| | | 購買関連情報 | 中 | 中 | 低 | 低 | 低 | 低 | 低 | 高 | 低 | 低 | 中 | 時期・商品名・金額・決済方法・目的 |
| | | 行動履歴 | 中 | 中 | 低 | 低 | 低 | 低 | 低 | 高 | 低 | 低 | 低 | 素行調査データ, アクセスログ, cookie |
| | | 所在情報 | 中 | 中 | 低 | 低 | 高 | 中 | 高 | 低 | 中 | 中 | 低 | GPS 位置情報, 携帯電話の位置情報 |

表 5.3.5-1：個人属性情報分類表

| 利用形態 | | 構成要素 | 利用者側格納媒体 | 提供者側格納媒体 | アクセス権限 | | | 具体例 |
|---|---|---|---|---|---|---|---|---|
| | | | | | 閲覧 | 書込み | 書換え | |
| プライベート | 関係 | 家族構成，しきたり | ― | ― | ― | ― | ― | 暗黙のルール，決まりごと（体系だった利用なし） |
| 公共 | 証明 | 氏名，本籍，住所 | 紙<br>磁気カード<br>IC カード | 台帳（原本）<br>電子データ | 本人<br>公共機関 | 本人（申請）<br>公共機関 | 本人（申請）<br>公共機関 | 住民基本台帳，住民票，年金手帳 |
| | | 氏名，国籍，本籍 | 紙 | | | | | パスポート |
| | 免許 | 氏名，本籍，住所，免許内容，有効期限 | 紙 | | | | | 運転免許証 |
| | 賞罰 | 氏名，住所，性別，賞罰内容 | ― | | （本人）<br>公共機関 | 公共機関 | 公共機関 | 犯暦 |
| 民間 | 証明 | ID 番号，氏名，所属（参加）組織，有効期限等 | 紙<br>磁気カード<br>IC カード | 台帳<br>電子データ | 本人<br>民間企業 | 本人（申請）<br>民間企業 | 本人（申請）<br>民間企業 | 社員証，学生証，会員証 |
| | 資格 | 氏名，資格内容，付与年月日等 | 紙 | | | | | 実用英検， |
| | 決済 | クレジット番号，氏名，有効期限等 | 磁気カード<br>IC カード | | | | | クレジットカード |
| | 医療 | 氏名，住所，性別，生年月日，身体的特徴， | 紙 | | | | | カルテ |
| | アンケート | （氏名），回答日，回答 | 紙 | | 本人 | 本人 | ― | アンケート |
| | インセンティブ | （権利行使時）氏名，住所，電話番号 | 紙 | | 本人 | 本人 | ― | ポイントカード |
| | 購買履歴 | 個人識別情報，商品名，数量，購入日時 | ― | | 民間企業 | 民間企業 | ― | |

表 5.3.5-2：利用形態分類表

| 情報種別名 | | ファイル名 | データ項目 | アクセス権限保持者 | | | | | | | ユニーク性 | 説明・用途等 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | ファイル生成 | ファイル消去 | ファイル転送 | 照合 | 閲覧 | 書込み | 書換え | | |
| 共　用情報 | 個人識別情報 | PKI 情報 | デジタル証明書(ユビキタス ID 含む) | {CA＋利用者} | 利用者 | 利用者 | Free | Free | CA | × | ユビコン環境 | ユビキタスコンピューティング環境において PKI を用いて本人性を証明するための情報.<br>CA はユビキタスコンピューティング環境において認証業務の実施を認められた認証局でなくてはならない.<br>デジタル証明書内には，Subject エリアにユビキタスコンピューティング環境内で一意に定められた ID（ユビキタス ID）を格納する. |
| | | | 秘密鍵 | | | | × | × | CA | × | ユビコン環境 | |
| | | バイオメトリクス情報 | 指紋，虹彩等 | | | | Free | × | 利用者 | 利用者 | × | ID 型ユーザノードの正当な所持者を識別し，PKI を補完するためのバイオメトリクス情報.<br>詳細な種別（指紋，虹彩など），形式については要検討. |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 共用個人属性情報 | ホーム情報 | 所属ホームサーバ物理アドレス | {利用者＋ホームサーバ} | 利用者 | 利用者 | 利用者，ホームサーバ | 利用者，ホームサーバ | 利用者，ホームサーバ | 利用者，ホームサーバ | ユビコン環境 | |
| | | | サブホームサーバ物理アドレス 1～n | | | | | | | | ユビコン環境 | |
| | | | 連絡先電話番号 | | | | | | | | ○ | |
| | | | 電子メールアドレス | | | | | | | | ○ | |
| | | エイリアス | エイリアス | | | | | | | | × | |
| | | 個人基本属性 | 姓 | | | | | | | | × | |
| | | | 名 | | | | | | | | × | |
| | | | 住所 | | | | | | | | × | |
| | | | 性別 | | | | | | | | × | |
| | | | 生年月日 | | | | | | | | × | |
| | | 家族構成 | 父母ユビキタス ID1 | | | | | | | | × | |
| | | | 父母ユビキタス ID2 | | | | | | | | × | |
| | | | 子ユビキタス ID1～n | | | | | | | | × | |
| | | 身体情報 | 身長 | | | | 任意設定 | 任意設定 | 任意設定 | 任意設定 | × | 身体情報及び特定サービスの情報については，アクセス権限を各項目個別に任意設定できることとする．<br>所属ホームサーバのみではなく，訪問先や公共の休憩場 |
| | | | 体重 | | | | | | | | × | |
| | | | 血液型（ABO，Rho(D)） | | | | | | | | × | |
| | | | 視力（近眼／老眼） | | | | | | | | × | |
| | | | 喫煙フラグ | | | | | | | | × | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | … | | | | | | | | | 所，トイレ等でも情報をオープンにしてサービスを享受したいとするニーズに対応するものである． |
| | | 特定サービス情報 | 快適気温（夏） | | | | 任意設定 | 任意設定 | 任意設定 | 任意設定 | × | |
| | | | 快適気温（冬） | | | | | | | | × | |
| | | | 風呂の湯加減 | | | | | | | | × | |
| | | | 喫煙フラグ | | | | | | | | × | |
| | | | 食べ物の好み 1～n | | | | | | | | × | |
| | | | アレルギー1～n | | | | | | | | × | |
| | | | 既往症 1～n | | | | | | | | × | |
| | | | … | | | | | | | | | |
| 個別アプリケーション情報 | 住民基本台帳情報 | PKI 情報 | デジタル証明書等 | {CA＋利用者} | 利用者 | 利用者 | Free | Free | CA | × | ○ | 4ケタ |
| | | パスワード | パスワード | | | | × | × | CA | × | × | |
| | | 基本情報 | 氏名 | {利用者＋公共機関}※ | 利用者※ | 利用者※ | 利用者，公共機関※ | 利用者，公共機関※ | 利用者，公共機関※ | 利用者，公共機関※ | × | |
| | | | 住民票コード | | | | | | | | ○ | |
| | | | 生年月日 | | | | | | | | × | |
| | | | 性別 | | | | | | | | × | |
| | 公共アプリケーション情報 2 | 任意設定 | 任意設定 | {利用者＋公共機関} | 利用者 | 利用者 | 任意設定 | 任意設定 | 任意設定 | 任意設定 | - | 運転免許証，健康保険証，年金手帳等 |
| | ～ | | | | | | | | | | | |
| | 公共アプリケーション情報n | 任意設定 | 任意設定 | {利用者＋公共機関} | 利用者 | 利用者 | 任意設定 | 任意設定 | 任意設定 | 任意設定 | - | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 個別アプリケーション情報 | 民間アプリケーション情報 1 | 任意設定 | 任意設定 | {利用者＋公共機関} | 利用者 | 利用者 | 任意設定 | 任意設定 | 任意設定 | 任意設定 | － | クレジットカード情報，交通チケット情報， |
| | ～ | | | | | | | | | | | |
| | 民間アプリケーション情報n | 任意設定 | 任意設定 | {利用者＋公共機関} | 利用者 | 利用者 | 任意設定 | 任意設定 | 任意設定 | 任意設定 | － | |

表 5.3.5-3：ＩＤユーザノードのデータフォーマット

### 2-3) 個人属性情報の特徴

**■個人属性情報の二分化**

一般的な人間社会における個人属性情報を分類した結果，個人識別性が高い【個人識別情報】と，特定サービス享受を目的とした【特定サービス情報】とに二分されることが判明した.

**【個人識別情報】**

個人属性情報のうち，個人識別性が高い情報を個人識別情報として分類した.

そのうち，日常馴染み深く，比較的手軽に扱えるデータを基本情報，企業内やインターネット等といった一定環境下で個人を識別するデータを一定環境下での情報として分類した.

基本情報の具体的項目は，「氏名」「住所」「生年月日」「性別」（住民基本台帳の基本 4 情報），及び「連絡先電話番号」，「家族構成」（戸籍）を加えた 6 種類である.

これらは体系の単純さ・短小さなどから，組み合わせて照合し，個人を識別することに適している.

また，公的証明も可能なため一般的に広く認知・活用されている.

これらの情報は，結婚，養子縁組，死別，引越しなどにより変更が生じることによる不変性の欠如があり，またプライバシー侵害やストーカー犯罪の不安による提供への抵抗，センシティブさは他の情報と同質である.

こういった問題点もあるが，認知度・利便性から今後も継続して活用されていくと考えられる.

一方，企業等の組織や，インターネット等のバーチャルな社会といった，一定の環境のもとで活用される個人識別情報の利用も活発である.

これらの情報には，特定組織内や環境内において使用される「組織内 ID」，インターネット等での呼称として使用される「エイリアス」，生体情報を使用し識別性が高く詐称が難しい「バイオメトリクス情報」，秘密鍵やデジタル証明書等の「PKI に用いる各種情報」が含まれる.

**【特定サービス情報】**

特定サービスで活用される情報はサービス内容に特化した属性を持つため，共用性は低くなり，積極的にサービスを享受する意思の無い

場合は提供寛容性が低くなるといった，センシティブな傾向がより強い．

これらの情報は，活用されるサービスごとに細かな提供・活用の管理を行うべきであり，そのコントロールは情報の発生元である個人が全て行うことが理想である．

しかし，これらの情報は専門的かつ膨大であり，個人でコントロールできる個人属性情報種別には質／量的な限界があり，医療分野のカルテなど，所有者個人以外の専門家により情報コントロールされているのが現状である．

### 2-4) 個人属性情報取り扱いの課題

**■詐称対策**

氏名や住所といった基本的なデータは取り扱いが簡単である反面，一時的な成りすまし／改ざん等の詐称も容易である．公的機関の証明が可能であり，詐称を防ぐ方策となるが，手続きの煩雑さや迅速性の面で課題が多い．

また，公証手段のない個人属性情報に関しては，内容の真正性についての保証がさらに困難な状況である．

**■提供抵抗性への配慮**

個人属性情報の提供に関しては，昨今のプライバシー侵害問題，ストーカー等の犯罪行為の多発といった社会的な背景も考慮し，きめ細かい提供形態の実現などの配慮が必要である．

## 3) 個人属性情報利用形態の現状調査

### 3-1) 利用形態の分類

一定の目的を達成するために体系的に構成された個人情報の集合物である利用形態について，**表 5.2.5-2「利用形態分類表」**のとおり分類する．

### 3-2) 利用形態の特徴

**■利用形態の多様性と格納内容**

個人属性情報の利用形態は多様であり，それぞれの利用形態に応じて多くの形式が存在する．

利用者側と提供者側にて格納媒体が異なるが，概ね提供者側の格納内容に利用者側の内容を包含している．

格納項目は，「2）個人属性情報の現状分析」にて大きく分類した「個人識別情報」と「特定サービス情報」の双方が同一媒体に格納されることが多い．

**■アクセス権限**

各種利用形態は，名目上は提供者側と利用者側のみ閲覧，書き込みが可能だが，利用者側の格納媒体のほとんどが紙媒体あるいはカード等の券面に印刷・刻印された状態であり，利用時や運搬時に盗み見される危険性がある．

また，「個人識別情報」と「特定サービス情報」の双方が同一の媒体に記録され，１枚で一覧できる状態になっており，記載内容に応じたアクセス権限の設定は困難な状況である．

**■格納媒体の電子化**

格納媒体は，公共・民間分野を通じて紙ベースの印刷物を多用しているが，近年データベースや電子媒体（磁気カード，IC カード等）を利用した電子化が進んでおり利便性の向上が図られている．

### 3-3）利用形態の課題

**■格納媒体保有数と情報の冗長性**

格納媒体保有数の多さ，情報の冗長な格納などから，各サービスにおける個人属性情報の共用化が今後の課題となる．

**■アクセス権限**

情報漏洩，書き換え・改ざんなどによる不正への対応の甘さ，アクセスコントロールの不足などから，厳密なアクセス権限の設定・管理・運用による高いセキュリティの実現が今後の課題である．

### 3-4）標準化動向

**■プライベート分野**

プライベート分野においては，体系だった個人属性情報の利用形態は存在しなかったが，昨今の情報家電分野の進展により，規格の中で個人属性情報を利用することが想像される．情報家電分野の規格は乱立状態であったが，現在は各規格間の連携を検討する方向に傾いている．

ここでは情報家電分野の規格と応用の一例を示す．

**【情報家電規格例 ～ECHONET～】**

ECHONET は，省エネルギー，セキュリティの高度化，ホームヘルスケアの高度化等のために活用できるホームネットワークの基盤ソフトウェアおよびハードウェアの開発を目的に設立されたコンソーシアムである．（運営委員会：シャープ，東京電力，東芝，日立製作所，松下電器産業，三菱電機の 6 社）

2000 年 7 月には，ホームネットワークシステムの通信の標準規格「エコーネット規格書バージョン 1.0」を作成し，一般公開した．家電機器をデータとサービス(機能)といった「オブジェクト」とみなすオブジェクト指向技術により，アプリケーション，家電機器(ハード)の統合的な開発を容易に実現することを目指している．また，家庭内に敷設された電灯線を利用して通信するため，新たな通信線の敷設が不要，といった特徴をもっている．

この規格では，家電機器の状態を表す詳細なステータスの規定が行われているが，個人属性情報を示す内容については，人体検知状態を 8 段階の閾値で表現するのみにとどまり，人間生活のきめ細かいサービスには対応していない．

**【情報家電応用例 ～JEITA ハウス～】**

2002 年 1 月，社団法人電子情報技術産業協会（JEITA）は，経済産業省が進める「住宅分野の情報システム 共通基盤整備推進事業」の研究実績として東京都多摩ニュータウンに建設した「情報家電モデルハウス」を公開した．

「指紋認証鍵無し玄関ドア」「IT 書斎」「自動給水システム」「ポット安否確認システム」などのアプリケーションが用意され，各情報家電は場所や条件によって，光ファイバー，電灯線，IEEE802.11b，Bluetooth，IEEE1394（i-Link）などで相互に接続されている．

介護に関連して，脈拍と呼吸を測定し，異常時には家族に通報するなどといった，個人属性情報を活用したサービスも実現されている．

**■公共分野**

**【戸籍】**

・戸籍の概要

戸籍は，日本国民について，その身分関係を登録し，公証する公簿である． 戸籍は一つの夫婦とこれと氏を同じくする子を単位として作ら

れ，個人の出生から死亡に至るまでの身分上の重要な事項が記載される．

・戸籍に関する動向

戸籍法第 117 条の 2 により，市町村長は，戸籍事務の全部又は一部を電子情報処理組織によつて取り扱うことができる．各自治体による電子政府／電子自治体の進行とともに，提供者側のデータベース化，および電子申請による作業の効率化が進んでいる．

**【住民基本台帳】**

・住民基本台帳の概要

住民基本台帳は，市町村において，住民の居住関係の公証，選挙人名簿の登録その他の住民に関する事務の処理の基礎とするとともに住民の住所に関する届出等の簡素化を図り，住民に関する記録の適正な管理を図るため，住民に関する記録を正確かつ統一的に行うものである．

・住民基本台帳に関する動向

住民基本台帳法の改正により，2002 年 8 月より住民基本台帳ネットワークシステムが導入される．これは，各種行政の基礎であり居住関係を公証する住民基本台帳のネットワーク化を図り，４情報〔氏名・住所・性別・生年月日〕と住民票コード等により，地方公共団体共同のシステムとして，全国共通の本人確認ができる仕組みを構築するものである．

また，希望者には IC カードを配布し，利用者の利便性向上を目指している．

**【運転免許証】**

・運転免許証の概要

運転免許は，自動車及び原動機付自転車を運転しようとする者が，公安委員会によって与えられる免許である．運転の目的や免許対象等によって詳細が規定されている．

・運転免許証に関する動向

2001 年 6 月 13 日に成立した道路交通法の改正により，2004 年から，偽造防止と海外での使用を理由に，運転免許証の IC カード化が導入されることになった．

**■民間分野**

**【クレジットカード】**

・クレジットカードの概要
クレジット業界では，国際ブランドの下で発行されている汎用クレジットカードの磁気ストライプフォーマットは，JIS-Ⅰ型および JIS-Ⅱ型（ISO/IEC 7810 及び 7811 ベース）に準拠している．この統一規格に業界各社が準拠することにより，利用者は店舗において様々なカード会社のカードを利用して決済することが可能となっている．
・クレジットカードに関する動向
磁気ストライプカードはセキュリティ面で問題が指摘されており，IC カード化の取り組みが行われている．
金融に関する IC カードの規格は，世界統一規格であるＥＭＶに収斂する状況にある．ＥＭＶは欧州のクレジットカード会社 3 社（Europay, Master, VISA）が共同で策定した仕様で，欧米では金融機関におけるＩＣカードの事実上のデファクト・スタンダードになっている．日本でも，ＪＣＣＡ（日本クレジットカード協会）が中心となり，ＥＭＶに基づくクレジットＩＣカードの仕様標準化を進めている．

**【銀行キャッシュカード】**
・銀行キャッシュカードの概要
銀行業界におけるキャッシュカードに関しては，統一した磁気カードストライプの仕様のもと各行 ATM で他行のキャッシュカードによる現金の引き出し・残高照会等が可能となっている．採用されている仕様は，JIS-Ⅱ型（国内仕様）を採用する点がクレジットカードと異なる．
・銀行キャッシュカードに関する動向
銀行キャッシュカードについても，IC カード化の取り組みが進んでいる．
2001 年 3 月，全国銀行協会（以下，全銀協という）は，金融取引用 IC カード分野の国際的なデファクト・スタンダードである EMV 仕様に準拠した「全銀協 IC キャッシュカード標準仕様」を制定した．

**【医療カルテ】**
・電子医療カルテの標準化動向
標準化作業は，厚生省電子カルテ開発事業内のカルテ構造検討チームから派生した，電子カルテ研究会と MERIT9 研究会に分かれて進めている．
日本医療情報学会課題研究会「電子カルテ研究会」の成果物としては「Medical Markup Language （MML）Version2.3」があり，XML をベー

スとした記述仕様が公開され，実装可能な技術として成熟している．
「MERIT9 研究会」は，成果物として XML 形式の「MERIT-9 診療情報提供データ」を公開している．
双方とも，患者名，生年月日，性別，国籍，住所，婚姻状態といった基本的な個人属性情報（個人識別情報）のほか，既往症，病状経過といった医療分野特有の情報も含まれた仕様となっている．

**【デジタル証明書】**

・デジタル証明書の概要

PKI において公開鍵の証明に用いるデジタル証明書の規格については，通常 X.509（ISO/IEC9594-8）で定義されているものが用いられる．また，RFC2459 でも X.509 と同じ規格が定義されている．

### 3-5) 技術動向

**■IC カードの動向について**

個人属性情報を格納する適切なデバイスとして，IC カードが採用されるケースが増加している．

CPU と不揮発性メモリを備えた IC カードは，暗号ロジックを実装するなどセキュリティに優れ，数キロ~数十キロバイトの容量を活用したマルチアプリケーション対応など，従来使用されていた磁気ストライプカードに変わるデータ格納媒体として有望である．

接触型（ISO7816），非接触型（主に ISO14443）の物理・電気特性に関する標準化は既に制定済みである．

また，アプリケーション分野におけるコマンド／データ内容は，金融分野における EMV 仕様，国内公共分野における JICSAP 仕様など標準化が進んでいる．

価格は 1 枚 1000 円程度といわれ，普及の妨げとなっていたが，住民基本台帳カード，JR 東日本の suica に採用されるなど，大量生産による低価格化が期待される．

一方，処理速度，記憶容量，伝送速度には限界があるため，利用にあたっては携帯電話などの周辺機器による補助を得てサービスを実現することも考えられる．

**■PKI とバイオメトリクスによる個人認証**

ネットワーク社会における個人認証をより強固なものとするため，PKI とバイオメトリクスを組み合わせた認証方式が考えられる．

PKI は,あくまでも秘密鍵が本人によって使用されるという前提に基づいており，秘密鍵が他人に盗用された場合，成りすましの不正行為が容易に行われてしまう．こういった PKI の弱点を補う方法として，指紋や虹彩といったバイオメトリクス情報を組み合わせて利用する方法が考えられている．

### 4）現状のまとめ

個人属性情報は，個人識別のための「個人識別情報」と，特定サービス享受のための「特定サービス情報」に大別できる．

個人属性情報は漏洩，詐称（成りすまし・改ざん）といったセキュリティに関する対策を施すとともに，適切なアクセス権限の設定と情報保持者による権限コントロールを実現し，提供抵抗性に配慮した社会を実現することが肝要である．

また，IT 社会の進行によって，「電子 ID」，「エイリアス」，「バイオメトリクス情報」，「PKI 関連情報」などの情報が利用されており，今後も積極的に活用していくべきである．

利用形態では，共用すべき情報が複数の利用形態に冗長に格納され，効率的に利用されておらず，利用者側の利便性を著しく損ねている．また，個人属性情報へのアクセス権限設定は利用形態の提供者側に委ねられ，電子媒体では，利用者本人でもアクセス困難な場合もある．また，プライバシーへの配慮も必要である．こうした個人属性情報のアクセス権限管理は，可能な限り利用者個人に委ねられるべきである．利用形態の媒体，フォーマットの標準化は進められているが，利用状況に応じて多数の利用形態の中から選択する不便さは存在する．公共分野の媒体統一化（行政 IC カード）や，全ての分野においてマルチアプリケーション対応の媒体を利用したサービスの相乗りを進めていくべきである．

こうした状況から，セキュアなマルチアプリケーション対応の情報格納媒体として IC カードの利用が広がりを見せ，PKI とバイオメトリクスを融合させた個人認証システムの開発例も登場している．

### ５）ユビキタスコンピューティング環境におけるサービスモデルの考察

#### 5-1）サービスモデルの考察

**■プライベートにおけるサービスモデル**

**【サービスイメージ】**

家庭内の生活行動において，個人識別情報をもとにサービスを享受することができる．家庭内では比較的緩やかな個人属性情報へのアクセス制限のもと，多様なサービスを実現することが可能である．
個人識別により玄関ドアの鍵の施錠／開錠ができる，詳細な個人属性情報により快適な室温や食事が楽しめるなどのきめ細かいサービスが想定される．

**【サービスの流れ】**

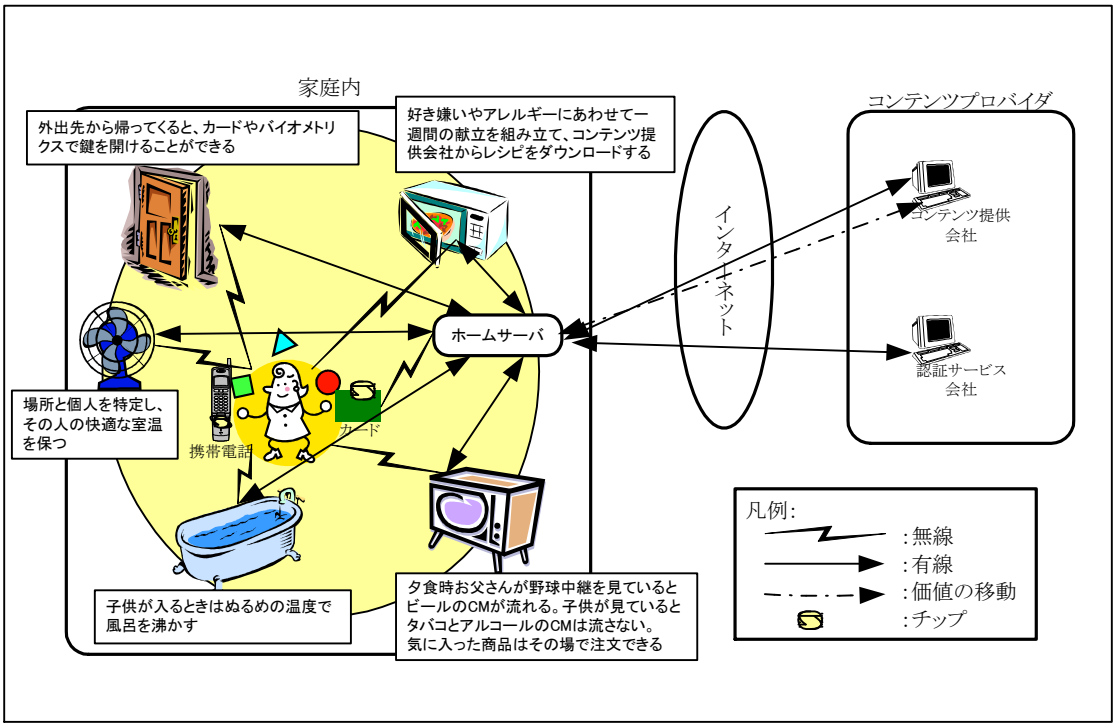



図 5.3.5-1：「プライベートにおけるサービスモデル図」

**【サービス要件】**

ID 型ユーザノードひとつで，家庭内の多様なサービスを簡単にすばやく受けることができる．

**【機能要件】**

- 個人識別情報による操作資格・動作モードを瞬時に判断する
- 詳細な個人属性情報により，きめ細かいサービスをタイムリーに提供する
  - 適切なアクセス権限行使

■公共・民間分野におけるサービスモデル

【サービスイメージ】

公共機関・民間サービスにおいては，高いセキュリティのもと，個人識別情報を活用したサービスや，電子マネー・電子チケットといった価値情報の権利行使によるサービスを享受することが可能である．様々な利用シーンが想定されるが，単一の格納媒体によって様々なサービスを受けることができる点はプライベートと変わらない．

【サービスの流れ】

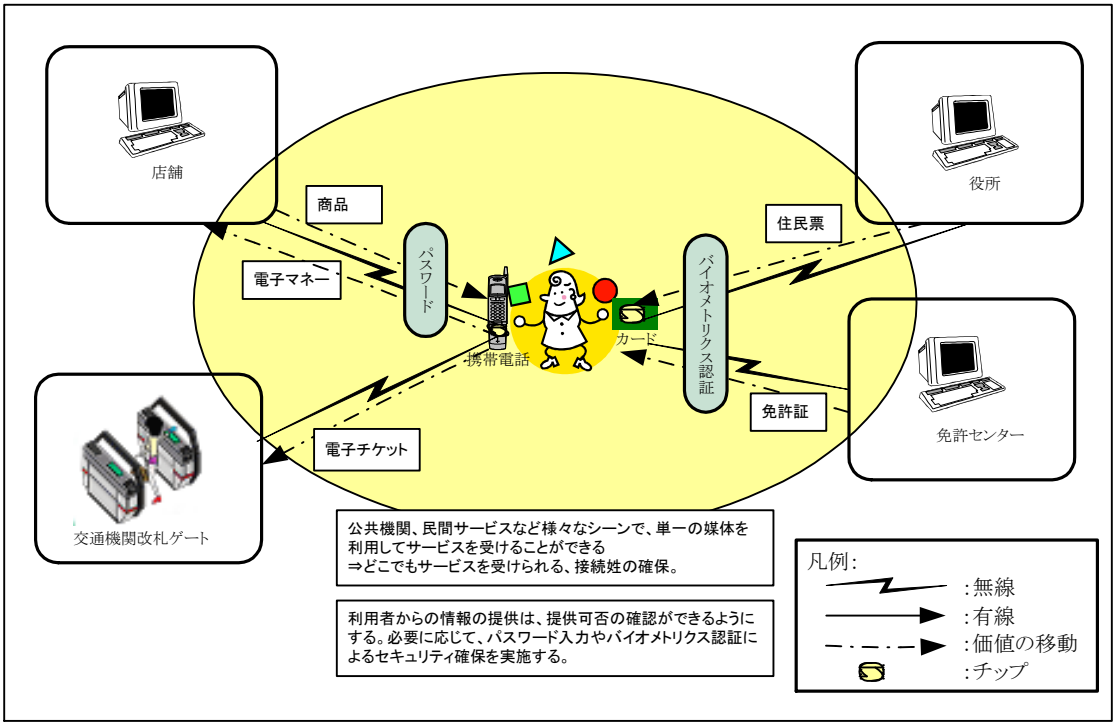



図 5.3.5-2：公共・民間におけるサービスモデル

【サービス要件】

- ID 型ユーザノードひとつで，公共・民間の多様なサービスを簡単にすばやく受けることができる
- セキュアな環境のもとで，利用者が安心して情報提供や権利行使を実施することができる
-

【機能要件】

- 個人識別情報による情報や価値の獲得，行使の資格を瞬時に判断する
- 移動先でも，個人属性情報を格納したノードが確実にネットワークに参加できるよう接続性を確保する
- 個人属性情報への不特定多数からのアクセスを考慮し，
- 厳密なアクセス権限の設定と高いセキュリティを実現する
- パスワードチェックやバイオメトリクス認証を行う．
- 価値情報の権利行使にあたっては，アトミックな操作による価値移動を実現する．
- 年配者や身体障害者への配慮から，操作端末等には音声認識・合成等による入出力インタフェースも備える．

### 5-2）サービス要件のまとめ

前項までに想定したユビキタスコンピューティング環境におけるサービスモデルから，サービス要件を以下に示す．

**【リアルタイム】**

- 人間生活に即した迅速なサービスの享受が可能なこと

**【セキュア】**

- 安全に個人属性情報を格納し，利用することができること
- 情報種別に応じたアクセス権限の設定・行使ができること

【エフォートレス】

- 年齢，性別，個人の性質（身体特徴の差異，身体的障害の有無）を問わず誰でも簡単にサービスが受けられること

【アドホック】

- 必要な時に必要なだけの情報を取り出せること
- 外出時や移動時の外部接続性を確保できること

## ６）個人属性情報表現形式の考察

### 6-1）個人属性情報表現形式の考察

**■考察の手順**

**【個人属性情報格納ノードの考察】**

個人属性情報を格納すべきノードについて分類し，考察対象を特定

する.

**【個人属性情報データフォーマットの考察】**

各章の考察から導き出された，必要条件を満たす個人属性情報データフォーマットを策定する.

**【格納ノード以外の役割の整理】**

個人属性情報データを格納するノード以外についても，その役割に応じた条件・機能等の考察をする.

**■個人属性情報格納ノードの考察**

ユビキタスコンピューティング環境においては，リアルタイム性確保，セキュリティ管理の観点から利用者側に個人属性情報を保持することが望ましい.

従って，個人属性情報を格納するノードとして，IC カード等の ID 型ユーザノードを選定し，そのデータフォーマットを考察する．また，ID 型ユーザノードに不足する位置／時間情報などの動的情報の格納や電源供給，操作性，容量の必要性から，携帯電話や PDA 等の操作端末型ユーザノードに関する考察も併せて行う.

また，その他のノードの役割について言及する.

**■ID 型ユーザノードに格納する個人属性情報データフォーマット**

ID 型ユーザノードは，ユビキタスコンピューティング環境において主に所有者の身分証明を行うためのノードである.

具体的デバイスは IC カード，SIM，UIM チップ，ウェアラブルコンピュータ等の，携帯性に優れたものが想定される.

また，価値情報を確実に移動する方法（アトミック操作）を備えた，PKI に対応したセキュアチップが望ましい.

以下に，ID 型ユーザノードに格納する個人属性情報データフォーマットを示す.

**【コンセプト】**

- 個人が携帯し，各種サービスを享受できるマルチアプリケーション対応ノードである
- 個人識別情報を共用情報エリアに，特定アプリケーションで利用する情報を個別アプリケーション情報エリアに格納する

- PKI を前提とし，デジタル証明書と秘密鍵を格納する．また，バイオメトリクス情報の格納エリアを設ける
- 共用情報は所持者の権限によって他の ID 型ユーザノードに転送することができる（ただし，複製はできない）
- 各情報については外出・訪問先での活用も考慮してユーザにてアクセス権限を柔軟に設定可能とする

**【内部構成】**

ID 型ユーザノード内の内部構成を以下に示す．

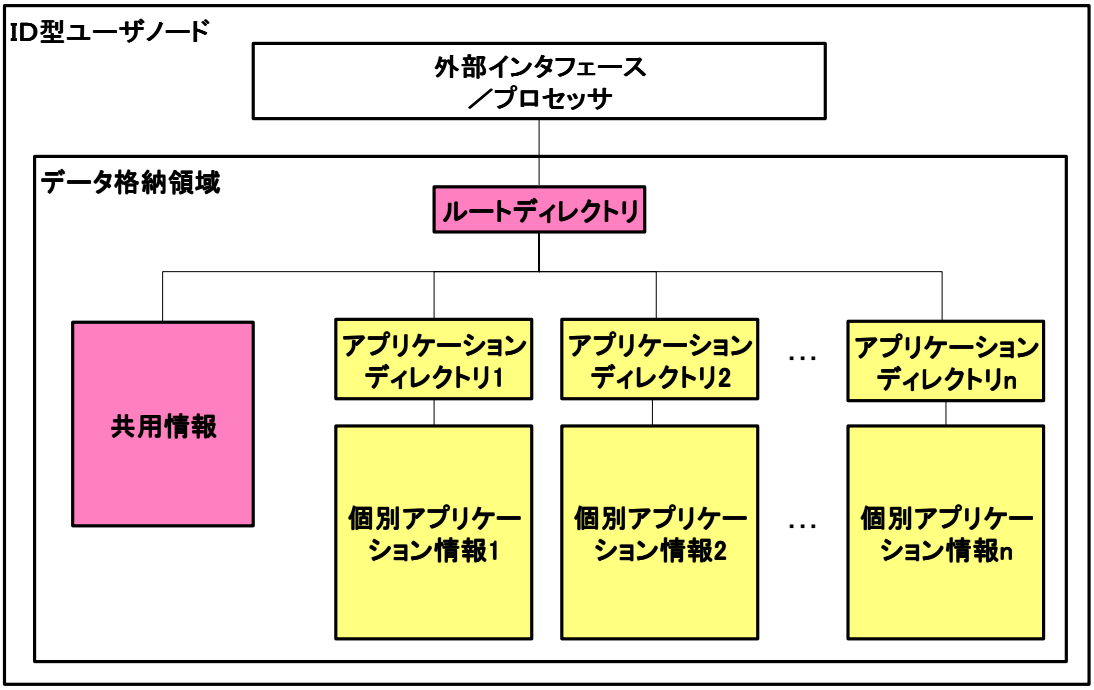



図 5.3.5-3：ID 型ユーザノードの内部構成

**【データフォーマット】**

ID 型ユーザノードに格納すべき個人属性情報論理データフォーマットを**表 5.3.5-3「ＩＤ型ユーザノードのデータフォーマット」**に示す．

**■操作端末型ユーザノードの役割**

操作端末型ユーザノードは，個人属性情報を格納した ID 型ユーザノードを補完するためのノードである．

具体的デバイスは携帯電話，PDA，手帳，鞄といった，ID 型ユーザノ

ードほどではなくとも，十分に携帯可能なもので，ID 型ユーザノードを装着して操作することが想定される．

操作端末型ユーザノードの具体的な役割について以下に示す．

【役割】

- ID 型ユーザノードと組合せて使用することを前提とする
- ID 型ユーザノードだけでは実現が困難な動的情報（位置情報，時間情報等）のリアルタイムモニタリング，多様なネットワークインタフェース，ヒューマンインタフェースの提供，電源供給等をサポートする
- ID 型ユーザノードの容量不足を補うため，トランザクションデータや一部の PKI 情報（CA のデジタル証明書等）をデータ格納領域に格納する
- 年齢や障害の有無に関係なくサービスを享受出来るよう，音声認識，点字ユニット等の入出力インタフェースを備える．

【内部構成】

操作端末型ユーザノードの内部構成を**図 5.3.5-4：「操作端末型ユーザノードの内部構成」**に示す．

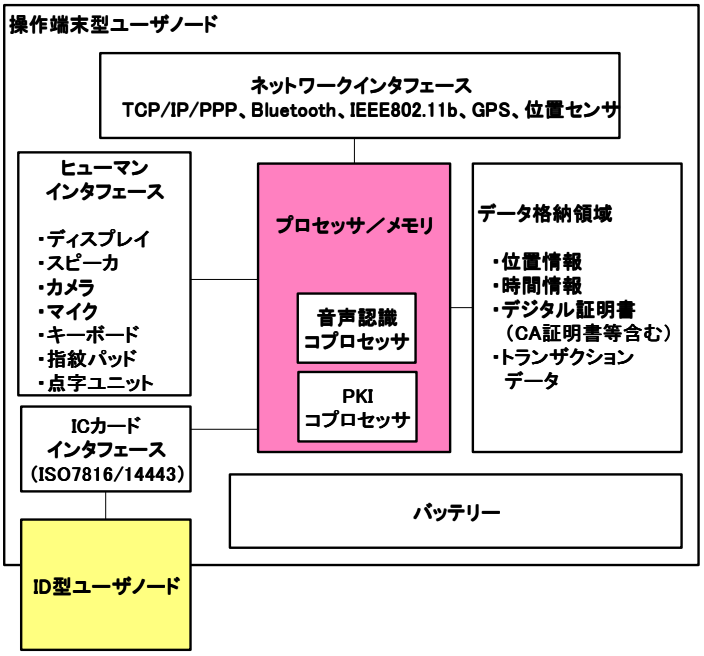



図 5.3.5-4：「操作端末型ユーザノードの内部構成」

■格納ノード以外の役割の整理

【ユーザノード（家庭設置型，及び民間・公共設置型）】

ID 型ユーザノードの個人属性情報をもとにサービスを提供する．公共・民間分野においては，PKI やバイオメトリクスによる個人認証を実施し，強固なセキュリティのもと確実な本人認証と適切なアクセス権限の行使を実施する．

【サーバノード（家庭設置型）】

ID 型ユーザノードの個人属性情報をもとに，家庭内部の固定型ユーザノードのサービスの仲介をしたり，外部ネットワークに接続することにより家庭外民間・公共設置型サーバノードのサービスを提供する．また，ID 型ユーザノードに格納する個人属性情報の初期設定情報，変更，削除等をサポートし，これらの設定情報を保管し紛失時のリカバリ等に役立てる．

【サーバノード（民間・公共設置型）】

ID 型ユーザノードの個人属性情報をもとにサービスを提供する．

ID 型ユーザノード内の個別アプリケーション情報の書込み，読み取りなどを行使するとともに，紛失時には再発行等のリカバリサービスも実施する．

6-2) 今後の取り組み

■移行期における現行制度，システムとの互換性の確保

住民票カード，交通カード（Suica）等といった IC カードタイプの ID 型ユーザノードの利用が進んでいるの分野に関しては，移行期の複数携帯等の措置が必要であり，いかに利便性を損なわず利用促進していくかがポイントとなる．

■サーバノード側の個人属性情報の管理，ライフサイクルの整理

利用者側への情報譲渡により，個人属性情報の管理，情報の生成・紛失時のリカバリ等といったライフサイクルの整理が必要となる．

個人属性情報は，基本的に利用者によるアクセス権限のコントロールを実現するが，個人での容易な運用を可能とする管理ツールの提供（家庭設置型サーバノードへの内蔵を想定）が必要である．また，公共・民間サービスにおいては，生成・リカバリサービスの提供も欠かせない．

■物理データフォーマットへのマッピング

【少容量化】

ID 型ユーザノードは，携帯性を追求するため，処理速度，伝送速度，記憶容量には限界がある．

従って，物理データフォーマットへのマッピングにおいては，小容量化に向けた取り組みが必要である．

短い鍵長でセキュリティ強度を保持できる認証方式（暗号アルゴリズム）の採用

【文字コード対応】

個人属性情報を表現するにあたっては，人名や住所などを表現するため，多様な文字情報を取り扱える文字コードをサポートする必要がある．

■認証システムの整理

家庭内，公共の場等での効率的かつ多段階の認証モデル／システムの構築が必要となる．

## 【参考文献】

### (1) 個人属性情報，及び利用形態に関する参考文献，Web サイト

86. 「企業システムのための PKI」 日立ソフトウェアエンジニアリング（株） 塚田孝則著（2001 年，日経ＢＰ社，ISBN4-8222-8117-5）
87. 「総務省」
http://www.soumu.go.jp/
88. 「総務省行政管理局」
http://www.soumu.go.jp/gyoukan/kanri/kanri_f.htm
89. 「HAVi.org」
http://www.havi.org/home.html
90. 「Jini」
http://wwwwswest2.sun.com/jini/
91. 「UPnP FORUM」
http://www.upnp.org/
92. 「LonWorks」

http://www.echelon.com/products/core/abtLonWorks.htm
93. 「エコーネットコンソーシアム」
http://www.echonet.gr.jp/
94. 報道記事：「白物家電などを統合できるホームネットワークの規格を公開」 MyCom PCWEB
http://pcweb.mycom.co.jp/news/2000/07/26/19.html
95. 「JEITA ハウス」
http://www.eclipse-jp.com/jeita/
96. 報道記事：「JEITA, ホームネットワークと情報家電を備えたモデルハウスを公開」 INTERNET Watch
http://www.watch.impress.co.jp/internet/www/article/2002/0128/it_house.htm
97. 「住民基本台帳ネットワークシステムの概要」 住民基本台帳ネットワークシステム全国センター
http://www.lasdec.nippon-net.ne.jp/rpo/juki-net_top.htm
98. 「社会情報システムレポート Vol.9」 株式会社 NTT データ
http://www.nttdata.co.jp/itinfo/publication/pdf/social09.pdf
99. 「社会情報システムレポート Vol.10」 株式会社 NTT データ
http://www.nttdata.co.jp/itinfo/publication/pdf/social10.pdf
100. 報道記事：「運転免許証を IC カード化 2004 年には交付開始」 Mainichi INTERACTIVE
http://www.mainichi.co.jp/digital/netfile/archive/200106/25-1.html
101. 「日本工業標準調査会（JISC）」
http://www.jisc.org/
102. 「日本クレジット協会（JCCA）」
http://www.jcca-office.gr.jp/
103. 「全国銀行協会（全銀協）」
http://www.zenginkyo.or.jp/
104. 報道発表：「全銀協 IC キャッシュカード標準仕様」の制定について」
http://www.zenginkyo.or.jp/news/index.html
105. 報道発表：マルチアプリケーション IC カード「XaicaTM -L シリーズ」 株式会社 NTT データ

http://www.nttdata.co.jp/release/2002/022000.html
106. MedXML コンソーシアム（「電子カルテ研究会」を母体として発足した MML 実装に向けたコンソーシアム）
http://www.medxml.net/
107. 「日本医療情報学会 MERIT-9 研究会」
http://merit-9.mi.hama-med.ac.jp/
108. 「IC カードシステム利用促進協議会（JICSAP）」
http://www.jicsap.com/index.html
109. 「EMV Co」.
http://www.emvco.com/
110. 「法庫」
http://www.houko.com/index.shtml

●

**(2)ユビキタスコンピューティング環境に関する参考文献，Web サイト**

111. 「手にとるようにユビキタスがわかる本」株式会社ＮＴＴデータ 荒川弘熙監修 日高昇治編著 2001 年，日経ＢＰ社，ISBN4-7612-5965-5）
112. 「野村総合研究所」
http://www.nri.co.jp/
113. 「ユビキタスネットワーク NRI の活動」
http://www.nri.co.jp/solution/ubiquitous/action.php
114. 「ユビキタスネットワークの進展シナリオ」 中村博之
http://www.nri.co.jp/report/chitekisisan/2001/pdf/cs20010311.pdf
115. 「ユビキタス環境を実現する携帯電話」 森本伊知郎
http://www.nri.co.jp/report/chitekisisan/2000/pdf/cs20000206.pdf
116. 報道記事：「「ユビキタス バリュー ネットワーク」と「FEEL」―ソニー・安藤氏が描いた未来図」 ZDNet JAPAN
http://www.zdnet.co.jp/news/0111/13/comdex_ando.html
117. 報道発表：「Bluetooth(TM)を利用したユビキタス・ヘッドセットの開発について」 株式会社 東芝
http://www.toshiba.co.jp/about/press/2002_01/pr_j0801.htm
118. 「HITACHI Ubiquitous World」 株式会社 日立
http://www.hitachi.co.jp/ubiquitous/

# 5.4 ユーザノードシステムの研究開発

## 5.4.1 平成 13 年度の成果概要

本サブテーマは，ユビキタスネットワーキング環境において，エンドユーザが直接接する機器類に関する研究開発である．ユーザノードには，ユーザが携帯する移動型ノードと，生活環境に設置される固定型ノードがある．今年度は，今後ユーザノードを研究開発する上での，まずは，ユビキタスコンピューティング環境による理想的なユーザサービスモデルを確立することを目的として，現状の技術で実現可能なユビキタスネットワーキング実験環境を構築し，ユーザビリティ研究を行った．

このユビキタスネットワーキング実験環境を構築するために，我々は，東京大学大学院情報学環と共同で，博物館の展示空間としてユビキタスコンピューティング環境を構築した．そのシステムを，2002 年 1 月～2 月にかけて東京大学総合研究博物館で開催された「デジタルミュージアム III 展」に導入し，全来館者の利用実験を実施した．

## 5.4.2 ハイパーギャラリー：ユビキタスコンピューティング環境が実現する複合現実型インタラクションの研究

### 1) はじめに

近年，ミュージアムにデジタル技術を導入し，ミュージアムの装置としての機能をより高度化することが期待されている．ミュージアムの役割には，文化的資産(コレクション)の収集，整理･蓄積，研究というと第一次機能と，それを使った教育普及活動である第二次機能(展示等)がある中でも，展示を含む第二次機能は，近年進展の著しいマルチメディア技術やインターネット技術等のデジタル技術によって，大きく変わる可能性を持っている．デジタル技術を用いた展示には，インターネット上で WWW 等のハイパーメディアシステムを使った展示手法や，VRML などの三次元仮想空間を用いた展示が一般的である．こうした仮想展示には，実展示にはない次の利点がある．まず，展示室という物理的な制約を受けずに自由で柔軟な展示が行えること，展示によってコレクションを傷めることがないこと，他の仮想展示のコンテンツをハイパーメディアの機能によって参照できることなどである．ところが，仮想展示では，実展示のような，コレクションの本物の迫力や，多様で大規模な入出力機器を用いたメディア表現ができないとい

った欠点がある.

そこで，我々は仮想展示空間と実展示空間を有機的に融合し，ユビキタスコンピューティング環境型の新しい展示空間，**ハイパーギャラリー(HyperGallery)**を構築している．ハイパーギャラリーでは，実展示空間と仮想展示空間が融合され，展示室においても情報量の豊富な教育的情報展示が可能になり，また「モノ」展示と情報展示の比率を来館者に応じて柔軟に変化させることも可能となる．更に，実展示用コンテンツと仮想展示用コンテンツの製作を一元化できるため，実展示と仮想展示の両方を常時提供するミュージアムにとっては，展示製作コストも低減できる.

ハイパーギャラリーによる展示の成否の鍵は，実空間内から仮想空間の情報を円滑に取り出す**AR(Augmented Reality)技術**，逆に仮想空間中に実空間情報を埋め込む **VR(Virtual Reality)技術**やハイパーメディア技術である.

### 2) ハイパーギャラリー

#### 2-1) 全体アーキテクチャ

ハイパーギャラリー(HyperGallery)における展示空間モデルは，**図 5.4.2-1** のような 3 重構造をとっている．それらは，実展示空間と 2 種類の仮想展示空間，それは WWW 展示空間とネットワーク型三次元共有仮想空間を使った仮想展示空間である．これらの間を相互に結合した点が，ハイパーギャラリーの展示空間構成手法の最大の特徴である．以下本節では，それぞれの展示空間の実現方法を概観した上で，両者を融合したハイパーギャラリーについて述べる.

**実展示空間**: ハイパーギャラリーでは，単にコンピュータネットワーク上の仮想展示だけではなく，実際の展示スペースにおける展示も扱う．本実験ではこの展示スペースとして，東京大学総合研究博物館一階の展示ホールを用いた．これらの展示スペースでは，ミュージアムコレクションの実物を見せ，それに関する情報展示として様々なデジタル技術を用いる.

**仮想展示空間**: ハイパーギャラリーの仮想展示空間は,WWW を使った二次元状の仮想展示空間(図 5.4.2-2 左)と，三次元仮想空間システム MMMUD[2, 3]を用いた仮想展示空間(図 5.4.2-2 右)から構成される．これらの展示空間によって提示されるコンテンツは，データベースによ

って一元的に管理され，それぞれの表現に適した形式に変換されて展示される．

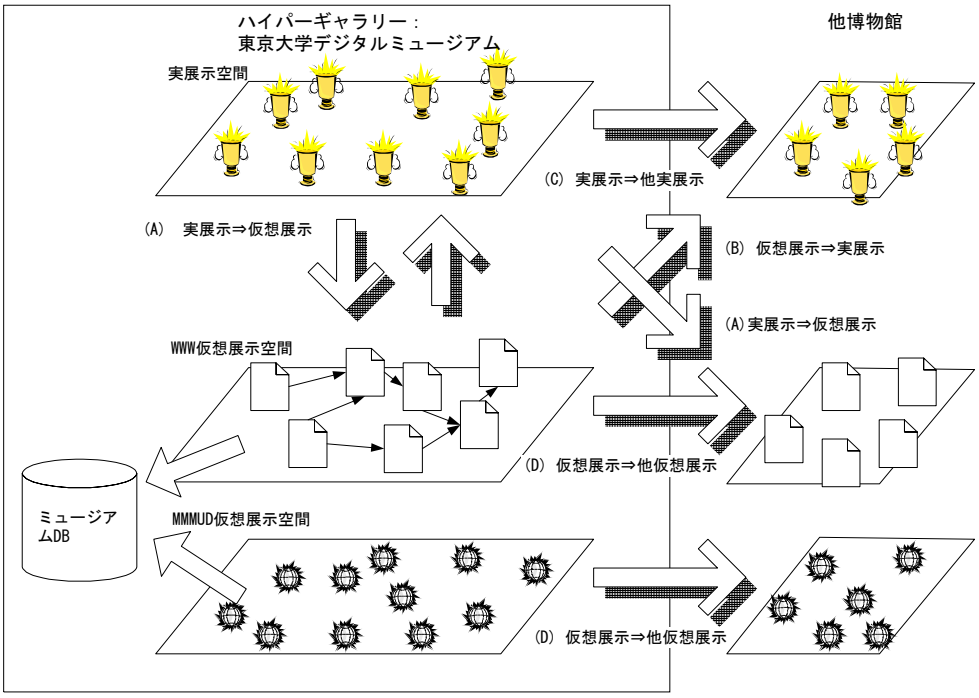



図 5.4.2-1:ハイパーギャラリー: デジタルミュージアムにおける基本展示空間モデル

### 2-2) 仮想展示空間と実展示空間のそれぞれの特性

仮想展示と実展示には，それぞれ利点と欠点がある．例えば，実展示には，ミュージアムコレクションの実物を見せることができるという利点がある．逆に欠点は，空間的な制約により，来館者に提示できる展示物の数や，それに付帯する情報提示が限定されることである．他方，仮想展示では，こうした空間制約がないため，膨大な情報を提供できること，端末とネットワークさえあればいつでもどこからでも観覧できることが利点である．しかし，あくまでもパーソナルコンピュータの画面を通して見られる情報しか閲覧できないという限界がある．


図 5.4.2-2:WWW による仮想展示画面(左)と MMMUD の画面例(右)

### 2-3) ハイパーギャラリー:仮想展示空間と実展示空間の融合

我々は，仮想展示と実展示の欠点を補い合い，より高度な複合化展示空間を構成するために，仮想展示空間と実展示空間を融合したユビキタスネットワーキング環境型の新しい展示空間を構築し，それをハイパーギャラリーと名づけた．この両者の融合とは，字義とおり，仮想展示空間と実展示空間が結合した空間を意味するが，その結合単位の粒度に応じてここでは 2 通りに分けて説明する．まず粗粒度の接合とは展示室を単位とした接合で，実展示空間の一つの壁の向こうに仮想展示空間が見えるようなものである．次に細粒度の接合とは，展示物を単位とした接合で，例えば，実展示空間の展示物の前で情報機器を通してその展示物に関する詳しい情報を仮想展示空間から取り出すような接合である．この場合，展示物が仮想空間への入り口としての役割を果たす．展示物は，自分に関する情報を，あたかも自分はこういうものだと語りかけてくるような錯覚を来館者に与えるヒューマンインタフェースが重要になる．

仮想展示空間と実展示空間の融合は，以下の 2 つに分類することができる．

A）実展示空間から仮想展示空間への参照
B）仮想展示空間から実展示空間への参照

同様のメカニズムによって以下の 2 つも実現できる．

C）実展示空間から別の実展示空間への参照
D）仮想展示空間から別の仮想展示空間への参照

従って，「実」と「仮想」の組み合わせの 4 通りの接合パターンがあ

る(図 5.4.2-1)．ここで，D)は，オープンな性質を持った仮想空間であれば容易に実現され，WWW も MMMUD もこの性質を満たすため，特に本稿では述べない．仮想展示と実展示を融合することによる具体的なメリットは，大別して以下の 3 点である．

第一に実展示空間でありながら場所の物理的制約を受けず，膨大な情報展示ができることである．

第二に，実展示空間において多くの情報を提示すると，パネルや展示物が高い密度で配置され，展示の種類によっては望ましくない．そこで，展示室から情報機器を通して仮想展示を覗き見できる仕組みを作ることによって，実展示空間を擬似的に拡大し，膨大な情報提示と展示空間の美観の維持を両立する．

第三点は，常に仮想展示と実展示の双方を構築するミュージアムにとっては，コンテンツを共有化できることにより，展示制作コストを軽減できることである．つまり，展示場でデジタル情報を使った展示を行う場合，展示場のためのデータのオーサリングと，仮想展示のためのデータのオーサリングとを2通りやっていては,コストがかかる．そこで，実展示空間と仮想展示空間を融合することで，これらのデータを共用でき，展示制作コストを軽減することができる．

### 3) 粗粒度の融合部の実現例

ハイパーギャラリーにおける実空間と仮想空間の粗粒度の融合とは,展示ギャラリー単位による接合を意味している．展示室の壁やパネルの向こうに仮想展示空間が見えたり，逆に仮想空間に中に，実展示空間の部屋が大きく映し出されているような接合の仕方をいう．本節では，東京大学デジタルミュージアムで実際に構築した，粗粒度の融合の実現例について紹介する．

### 3-1) 実展示⇒仮想展示(WWW, MMMUD)

実展示空間から仮想展示空間上の様々なデジタルコンテンツを活用するために，我々はいくつかのシステムを構築した．一つは，実展示と MMMUD 上の仮想展示がほぼ同一の縮尺になるように，仮想空間画面を壁面に投射する，実物大 MMMUD システムである．これにより，壁の向こう側に MMMUD の仮想ギャラリーが広がり，来館者はその向こうへ入っていけるようにしなっている．

実展示空間と WWW 展示空間を接合するために,我々が開発した Kiosk 型 WWW 端末を展示場に設置した.WWW 空間が実展示空間の中に自然に位

置付けられるため,WWW ドキュメントが展示物の解説パネルであるとみたてて展示を構成した.

### 3-2) 仮想展示(WWW, MMMUD)⇒実展示

WWW から実展示空間を参照するために,我々はテレオペレーションカメラシステムを構築した.展示場に遠隔操作が可能なカメラを設置し,そのライブ映像をネットワーク経由でプロジェクタ画面から見えるようにした.またそのカメラをトラックボールから制御できるようにすることで,遠隔地にある実展示空間を様々な角度から見ることを可能にした.

一方 MMMUD 空間と実空間を融合するシステムとして,我々はビデオアバターを利用した.ビデオアバターとは,MMMUD 空間内にビデオ映像を埋め込む技術である.単にビデオを仮想空間中に表示するだけでなく,複数方向から同時撮影したビデオ映像を用いると,MMMUD 上の観覧者の位置と視線の方向に応じて複数の方向からの映像を切り替えることができる.例えば仮想空間中に人物のビデオを登場させた場合,観覧者は,その人の前,右,後ろ等,複数の方向のビデオ画像を見ることができる.図 5.4.2-5 右は,ビデオアバターを使って,実展示空間にいる学芸員が仮想空間中の展示物を説明している画面例である.

### 3-3) 実展示⇒(遠隔)実展示

ハイパーギャラリーでは,離れた複数の展示場で同時に同じコンセプトの展示を行い,それらをデジタル映像回線で接続し,双方の様子を自由に参照できるシステムを構築した.我々はこれを,分散ミュージアムと呼んでいる.従来の実展示の空間は,当然ながら展示室に限定された閉じた空間であった.従って,様々なコレクションを扱う包括的な展示のためには,様々なミュージアム等からそれらを借り集めなければならなかった.これはコレクションの保存の立場から好ましくはなかった.そこで,我々の分散ミュージアムでは,上記の問題を解決するために,コレクションを所蔵する個々のミュージアムが独自に展示し,それらとの間をデジタル回線で接続することで包括的な実展示の実現を目指している.

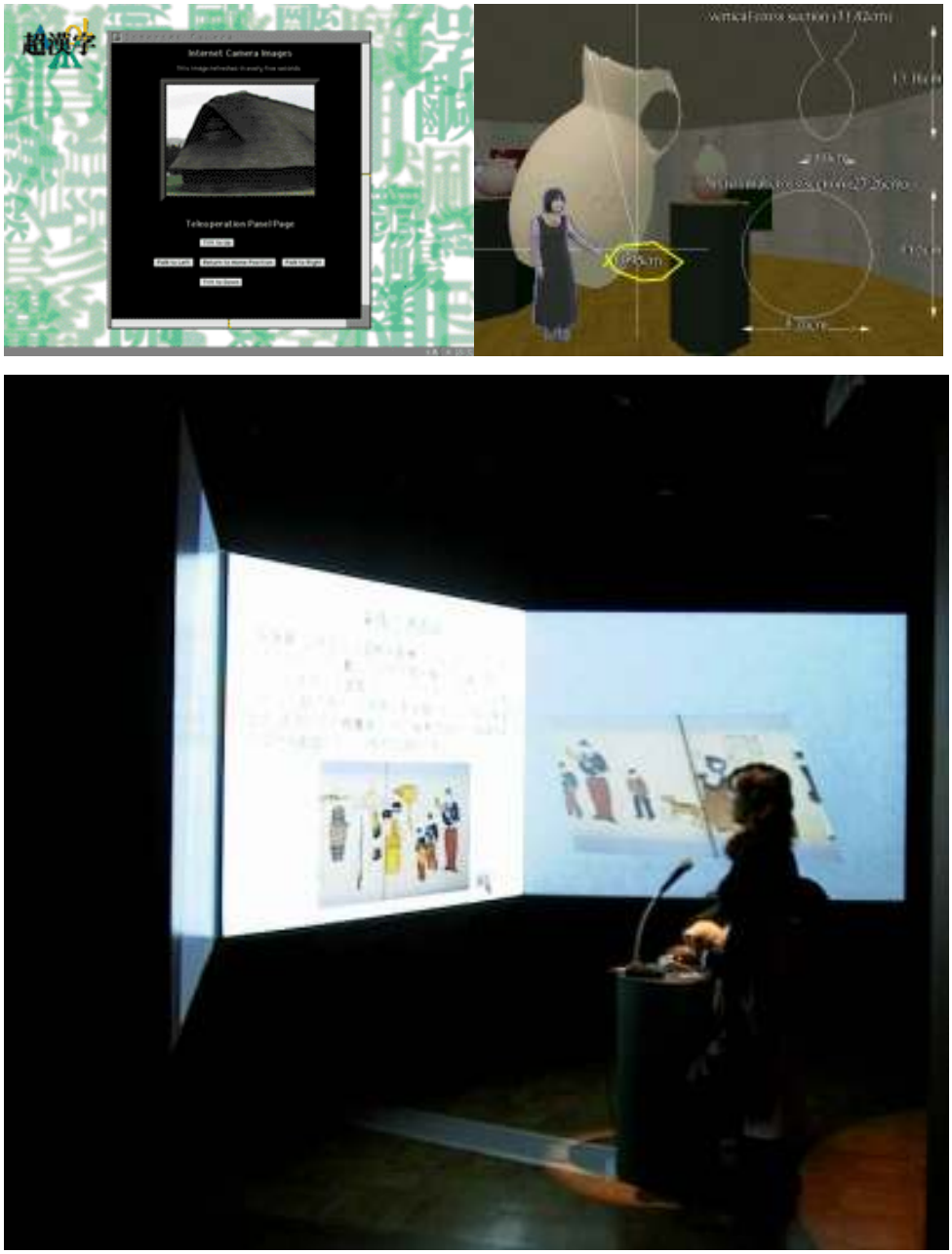



図 5.4.2-5:テレオペレーションインターネットカメラによる三内丸山遺跡復元展示（左上），MMMUD 仮想空間においてビデオアバターが展示物の説明をしている例（右上），三面大型スクリーンを使った MMMUD の展示例（下）

図 5.4.2-6：東大総合研究博物館内の複数の展示室を映像回線で接続（左：四天王像に，テレオペレーションカメラを設置，右：他の部屋の端末でカメラを操作しならが四天王像を立体視映像で巨大画面を使って詳細に見ることができる）

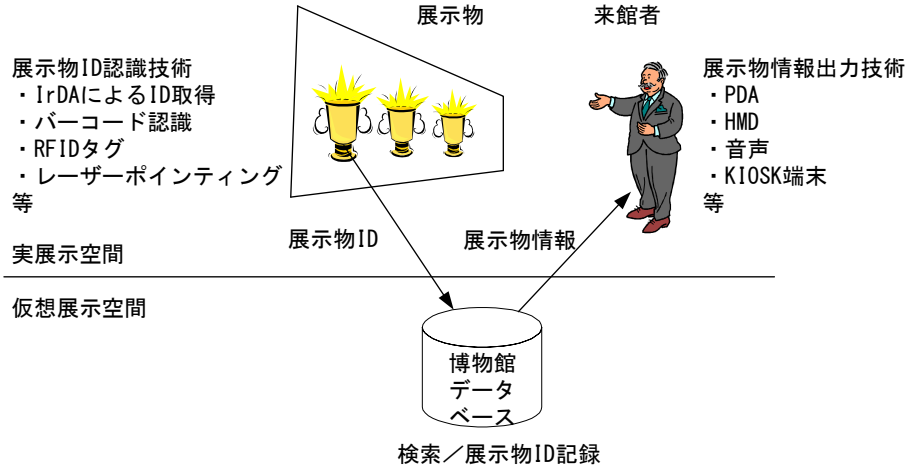



図 5.4.2-7：仮想展示情報を実展示空間から取り出す枠組み

図 5.4.2-8：PDMA（左），ミュージアム強化情報システム（右）

### 5.4.3 パーソナライズドミュージアム：ユビキタスコンピューティング環境が実現するユーザ適合型インタラクションの研究

#### １）はじめに

デジタルミュージアム III システムでは，展示空間をユビキタスコンピューティング環境として構築した．この展示空間の設計方針は，ユーザの情報や様々なコンテクスト情報を活用して，ダイナミックに展示内容を変化させることである．その際に，もっとも鍵になることが，ユーザ，つまり来館者の属性や Preference に応じて，その個人のマッチした展示を行うことであり，このコンセプトを我々はパーソナライズミュージアム（Personalized Museum）と呼んでいる．そのためには，来館者が自身の属性や preference を携帯し，展示空間にある機器に対して，必要なときに即時に提供できるメカニズムが不可欠である．そうした，来館者とユビキタスコンピューティング環境との間のインタラクションデバイスとして，非接触型の IC カードである，SDCC（Secure Data Carrier Chip）を利用した．非接触型ＩＣカードは次の性質をもつために，おそらく既存のデバイスの中で，この目的に最も適したものではないかと考えている．

- 非接触型ＩＣカードとのインタフェースが，簡易なＲ／Ｗ装置で実現でき，故障が少ない．（特に，接触型のＩＣや磁気カードと比べて）
- １Ｋバイト以下程度の少量の情報であれば，１秒以内の短時間で即座に通信することができる．
- 耐タンパー性を有するため，格納した情報の安全性や，カードの偽造可能性も少ない．
- 全来館者に配布するに十分安価である（１枚あたり，数百円）（特に携帯型端末と比べて）
- 個人情報のようなプライバシーにかかわる情報は，カード内部にだけに格納することによって，博物館側に個人情報が残存させずに，個人サービスが可能になる（単なるＩＤカードや，バーコードカードの場合，そういった情報は，サーバに格納する必要がある．この場合，その情報管理に対して，来館者がナーバスになるケースが多い．

デジタルミュージアム III で用いた SDCC には，ユーザの個人情報や Preference 情報を格納し，SDCC を展示端末等にかざすことによって，

個人情報をユビキタスコンピューティング環境に提供することができる．また，逆に展示端末等から情報を受け取る機能も有している．

### ２）デジタルミュージアム III システム

#### 2-1）デジタルミュージアム III の展示システムの全体構成

デジタルミュージアム III の展示システムは，主に，次の機器から構成されている．

- カード発券端末
- 個人情報設定端末
- 館内案内端末
- 情報提供ＫＩＯＳＫ端末
- ＷＥＢ情報提供システム（ＷＥＢサーバとデータベースサーバ）

これらの機器は，すべてネットワークで接続され，互いに協調して動作する．また，来館者はすべて eTRON 仕様の SDCC（Secure Data Carrier Chip）を所持し，デジタルミュージアム III 展示システムと来館者のコミュニケーションデバイスとして利用する．

#### 2-2）カード発券端末

**カード発券端末**は，ネットワーク接続されたパーソナルコンピュータと SDCC のリーダライタインタフェース，プリンタから構成される．カード発券端末は SDCC を初期化し，その中に必要なデータレコードを作製する．それと同時にインターネットサービスのために，バーチャル展示ＷＥＢのためのデータベースエントリーを作成し，そのエントリーを示す，アカウント名とアクセス用のパスワードを印刷する．展示場での運用時には，初期化された SDCC とプリンタが生成したインターネット上のＷＥＢアカウントを来館者に渡す．

### 2-3) 個人情報設定端末

**個人情報設定端末**は,カード発券端末によって初期化されたSDCCに,来館者の個人情報や展示に対する興味項目などを設定する．具体的には，以下の項目を設定した．

- 展示解説の表示言語
- 展示解説の表示文字の大きさ（２段階）
- 説明の難易度（大人向け，子供向け）
- 展示の興味分野
- 仮想展示空間上のニックネーム


写真 5.4.3-1：個人情報設定端末（左：端末外観，右：設定初期画面）

### 2-4) 館内案内端末

**館内案内端末**は，ディスプレイ上に表示された展示場の地図を使って，どこにどの展示があるかを表示して，来館者を適切に誘導するための端末である．この案内を行うときに，2-3）で行った個人情報設定の興味分野に応じて，*「あなたの興味のある展示はここ」*，というような案内を行った．また，展示を観覧した記録を利用して，*「あなたがまだ見てない展示はここ」*，という案内も行った．

写真 5.4.3-2: 館内案内端末外観


写真 5.4.3-3：館内案内端末画面例

### 2-5）情報提供ＫＩＳＯＫ端末

館内の展示物の解説や，展示物に関連する情報提供は，この**情報提供ＫＩＯＳＫ端末**（以下**ＫＩＯＳＫ端末**）が担っている．ＫＩＯＳＫ端末も，SDCC の R/W インタフェースユニットを備え，SDCC をかざすことをイベントして動作する．SDCC に設定された個人情報に応じて，表示コンテンツを切り替えるといった動作を行う．逆に，どのＫＩＯＳＫ端末の説明を見たかという閲覧記録を SDCC に保存する．ＫＩＯＳＫ端末は，ＷＥＢブラウザに SDCC インタフェース拡張を加えることで実装を行った．

また，この端末では，最初の個人設定端末で設定した個人情報の中でも，展示解説表示に関連する項目を on-the-fly で修正することができる．最初に個人設定端末で，説明の難易度や文字の大きさなどを設定したものの，実際の解説端末で解説を閲覧した状況によって，その場で修正することができるようになっている．

写真 5.4.3-3: 展示情報ＫＩＯＳＫ端末（実物展示の説明端末外観）

写真 5.4.3-4: 展示情報ＫＩＯＳＫ端末(プラズマディスプレイを用いた肖像画のデジタル展示の，Real-World Bookmark 専用端末群)

写真 5.4.3-5: 展示情報ＫＩＯＳＫ端末(プラズマディスプレイを用いた肖像画のデジタル展示の，Real-World Bookmark 専用端末，現在投影している肖像画画像に関する情報を SDCC に Bookmarking することができる)

### 2-6) ＷＥＢによる情報提供

デジタルミュージアム III では,館内の展示の解説と同等の情報を，ＷＥＢ上で情報提供を行った．この情報提供を実展示と連動させ，実展示に足を運ぶインセンティブを増大させるために，以下のような個人化情報サービスをなった.

デジタルミュージアム III の展示場では，ＷＥＢブラウザで，気に入ったページでブックマークをとるように，このＫＩＯＳＫ端末でも，気に入った情報があった場合には，そのページへのポインタを，SDCC

に記録することができる（RealWorld Bookmarking）．ここで，記録したブックマークを元にして，ＷＥＢサーバ上には，個人化されたホームページが自動生成される．退館後に，自宅や職場など，インターネットに接続された端末があれば，カード発券端末が発行したアカウント情報を使ってＷＥＢページにアクセスすることで，その個人化されたページを閲覧することができる．

# 5.5 サーバノードシステム

## 5.5.1 平成 13 年度の成果概要

本年度は，ユビキタスコンピューティング環境を実現するサーバ側システムの研究として，既存の決済型プラットフォームシステムとユビキタスネットワークの間の連携方式について研究を行った．特に，既存のネットワークと本開発課題で進めているユビキタスコンピューティング環境のためのユビキタスネットワークが共存する状態において，重要な技術テーマである．

## 5.5.2 決済プラットフォームとユビキタスネットワークとの連携方式

### 1) 目的と概要

ユビキタスネットワーク内で発生する決済と既存決済プラットフォームとの連携方式を検討することを目的とする．

上記を実現するため，既存決済サービスの調査と決済を円滑に行うための機能要件（以下，決済要件）を抽出する．さらに，決済要件を満たした既存決済プラットフォームとユビキタスネットワークとの連携モデルを設定し，課題を明確にする．

### 2) 既存決済サービスの分類

既存決済方式をリアル決済と電子決済というカテゴリに分類する．

※ 本節後ろに添付した**表 5.5.2-1 既存決済サービス一覧**参照

### 2-1) リアル決済の概要

リアルマネーは現実の実体に価値が与えられているため，転々流通が可能な反面，紛失した場合所有者は価値そのものを失う．

**■現金**

9 割が紙幣で，1 割が硬貨．日銀券（紙幣）は，日本銀行が発行し，硬貨は，補助貨幣として政府が発行する．

**【特徴】**

- 転々流通する
- 匿名の決済が可能である
- 回収，保管，運搬，計算などのコストが発生する

## 2-2) 電子決済の概要

### ■銀行振込み

受け手の預金口座に ATM や窓口から金を払い込む決済方式である.

**【特徴】**

- 相手の氏名と電話番号で決済を確認する
- 件数が多くなると受け取り側は照合が煩雑になる

### ■口座振替

事業者が，登録した口座から代金を引き落とす決済方式である.

**【特徴】**

- 公共料金やクレジットカード等の支払いで利用する
- あらかじめ口座振替先と引き落とし日を登録しておく

### ■クレジットカード

クレジットカード会社発行のカードを利用して後払いで商品やサービスの購入を行う決済方式である.

**【特徴】**

- 小銭や高額な紙幣を持つ必要が無い
- クレジットカード会社が手数料を受け取る
- 電子商取引における決済手段として利用可能である
- 他人の不正使用を防ぐことが困難である

### ■デビットカード

キャッシュカードを用い利用者の預金口座から即時に引き落とす決済方式である

**【特徴】**

- 小銭や高額な紙幣を持つ必要が無い
- 電子商取引における決済手段として利用可能である
- 暗証番号で認証する

### ■電子マネー

電子マネーには，現金と同じ価値を持つデータを IC カードなどに充填するオープンループ型，一度発行された電子マネーが再び発行体に還流するクローズドループ型，インターネットなどのネットワークを介して決済するネットワーク型がある.

**【特徴-オープンループ型】**

- 通常の現金と同じように転々流通することが可能である
- 匿名の決済が可能である
- マイクロペイメントにも対応できる
- 法律・社会的な整備が必要である

**【特徴-クローズドループ型の特徴】**

- 前払いした金額分だけ決済に利用できる
- 一度の決済にしか利用することはできない

### 3）ユビキタスコンピューティング環境で求められる決済要件

ユビキタスシーンを想定することから，ユビキタスコンピューティング環境で求められる決済要件を抽出する．

#### 3-1）シーンの想定

ユビキタスコンピューティング環境における決済機能を必要とする利用シーンを想定する．

なお，各シーンの【決済に関わる機能要件】において，「→・・・・」は，要件を一般化して表記したものである．

利用シーンの想定にあたってユビキタスコンピューティング環境の定義を確認する．

**【ユビキタスコンピューティング環境の定義】**

- 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んだ環境
- それらが互いに情報交換しながら協調動作する環境
- これらの仕組みにより人間生活を高度にサポートする環境

**■ホームユビキタスにおける自動発注**

**【サービスイメージ】**

米が残り少ないことを米びつが感知し，米屋に自動発注する．翌日米が配達されたのを確認して決済を済ませる．

**【サービス要件】**

- 住人が意識することなく米が常に補充されること
- 住人が意識することなく自動的に決済が行われること
- あらかじめ設定された限度額範囲内で決済をすること

- 注文情報が米屋のモニタに表示されること
- 米屋が米を配達すること
- 米屋が確実に代金を回収できること

【機能要件】

- 米の残量を感知するセンサ機能
- 店舗とノードに埋め込まれたチップが認証する機能

【決済に関わる機能要件】

- 米の受け取りと同時に代金を支払う機能
  →リアルタイム決済
- 利用者が設定した限度額範囲内で支払いが行われる機能
  →決済額設定機能
- 決済ルールの設定を簡単に行う機能
  →登録機能
- 米びつが決済を行う機能
  →デバイス非依存
- 利用者が意識せずに決済を行う機能
  →無意識
- 成りすましや送信否認を防止する機能
  →成りすまし・送信否認防止

■自動車の自動決済

【サービスイメージ】

東京都内を通行した業務トラックに対して通行税を徴収することを想定する．トラックが県境を通過した際，道路に埋め込まれたセンサが車種を特定して税金を徴収する．同様にスタンドにてガソリンを補充した際，車と自動車が自動的に決済を行う．

【サービス要件】

- ドライバが意識することなく通行税が徴収されること
- 都は，通過した車の車種に応じ，徴税額を把握できること
- 高速移動中でもトラックとゲートが決済を行える事
- 引き落とせない場合，トラックを特定できること
- トラックが即時に支払えない場合は，後日請求できること
- 徴税額がモニタに表示されること

- ガソリンスタンドで個人特定情報が取得されないこと

【機能要件】

- 道路がトラックの車種を特定する機能

【決済に関わる機能要件】

- 道路センサの読み取りと同時に税金を支払う機能
  →リアルタイム決済
- 支払いが不足していても事後に徴収できる機能
  →事後決済
- 高速移動中にも決済できる機能
  →リアルタイム決済
- 残金不足の場合に車の持ち主を特定できる機能
  →人を特定する決済
- トラック，道路，給油機が決済を行う機能
  →デバイス非依存
- 徴税額がモニタで確認できる機能
  →モニタリング機能
- 利用者が意識せずに決済を行う機能
  →無意識
- スタンドに個人情報が取得されない機能
  →匿名性
- 成りすましや送信否認を防止する機能
  →成りすまし防止・送信否認防止

■電子ブックの購入

【サービスイメージ】

音楽，画像，テキストが様々なノードで自由にやり取りされている．利用者 A は書籍「イタリアのレストラン」（全文価格 2000 円）をネットワーク上で見つける．A はローマのレストランについての記述（0.75 円）のみをダウンロードし購入する．同様に「大英辞典全 10 巻」50000 円もダウンロードしたが，手持ち資金が不足したため 2 ヶ月後の決済で支払う．

【サービス要件】

- 音楽，画像，テキストバリューが極小な単位で自由にやり取りされ，様々な機器を自在に移動すること

- 利用者がネットワークを通じて音楽・画像・テキストバリューを購入できること
- 電子マネーで決済を行えること
- 事後決済が行えること

【機能要件】

- 音楽，画像，テキストが，ハードを選ばずに移動できる機能
- 音楽，画像，テキストが，極小な単位でやり取りできる機能

【決済に関わる機能要件】

- コンテンツの受け取りと同時に支払う機能
  →リアルタイム決済
- コンテンツの受け取りの 2 ヶ月後に支払う機能
  →事後決済
- 1 円以下の支払いができる機能
  →マイクロペイメント
- 決済がネットワークを通じて行われる機能
  →ネットワーク流通性
- 小額決済にみあった低額な決済コストを実現する機能
  →コストが低額
- 事後決済にあたって利用者の支払い能力を判断する機能
  →与信
- 電子マネーの複製・改竄を防止する機能
  →複製・改竄防止

■通貨を意識しない決済

【サービスイメージ】

旅行者 A はアメリカで＄500 のバッグを購入する．その際，日本円でチャージを行った電子マネーで決済時の交換レートに応じて即時決済を行う．

【サービス要件】

- 利用者が円を電子マネーにチャージできること
- 利用者，店舗とも他通貨との取り扱いを意識しないで決済を行えること
- 利用者は現金通貨を両替しなくてもよいこと

- 店舗は代表的な通貨の支払いに応じること
- 店舗はリアルタイムな市場レートに応じて課金すること
- 利用者はレートと支払い金額をモニタリングできること

【機能要件】

- レジが IC カードに格納された通貨を認識する機能
- レジが為替レートをリアルタイムで入手する機能

【決済に関わる機能要件】

- 電子マネーを IC カードにチャージする機能
  →事前決済
- バッグの受け取りと同時に支払う機能
  →リアルタイム決済
- 通貨の変換レートを確認する機能
  →モニタリング機能
- 2 種類の通貨がネットワークを通じて変換される機能
  →ネットワーク流通性
- 電子マネーの複製・改竄を防止する機能
  →複製・改竄防止
- 日頃最も関与が深い通貨を扱う機能
  →既存決済との連携

■電子マネーによる買い物

【サービスイメージ】

母が電子マネーを,携帯電話に格納された IC チップにチャージする. 母はチャージした電子マネーの一部を子供の IC チップに移す. 母親から受け取った電子マネーを使って，子供が野菜を購入する.

【サービス要件】

- 電子マネーを扱うための登録ができること
- 電子マネーのチャージができること
- 電子マネーが母⇒子供⇒八百屋と流通すること
- 母は銀行から電子マネーを受け取ること事ができること
- 子供は銀行から電子マネーを受け取る事ができないこと
- 子供が野菜を購入できること

【機能要件】

- 店舗で購入する機能

【決済に関わる機能要件】

- モバイル機器に電子マネーをチャージする機能
  →事前決済
- 野菜の受け取りと同時に支払う機能
  →リアルタイム決済
- 1 円以下の支払いができる機能
  →決済額設定機能
- 電子マネーが転々流通する機能
  →転々流通
- ネットワークを経由する電子マネーに変換できる機能
  →ネットワーク流通性
- 子供でも決済できる機能
  →誰でも使える
- 電子マネーの複製・改竄を防止する機能
  →複製・改竄防止

### 3-2）決済に関わる要件

「3-1）シーンの想定」の 5 つのサービスシーンから抽出した【決済に関わる機能要件】を本節後ろに添付した表 5.5.2-2 ユビキタスコンピューティング環境において必要とされる決済要件に整理した.

### 4）決済方式の検討

表「既存決済サービス一覧」および表「ユビキタスコンピューティング環境において必要とされる決済要件」を分析・比較した結果，以下のことが結論として導き出される.

### 4-1）結論 1

ユビキタスコンピューティング環境を支える決済方式として,「転々流通性」「リアルタイム決済」「マイクロペイメント」を実現できるオープンループ型電子マネーを導入する必要がある.

ただし，オープンループ型電子マネーだけでは，ユビキタスコンピューティング環境において必要とされる決済要件を満たすには不十分である．その理由を次に示す.

■オープンループ型電子マネー単独方式の課題

オープンループ型電子マネー単独方式では大きく分けて　以下の 3 つの課題がある．

【決済タイミングの多様性の確保】

オープンループ型電子マネー単独方式を採用すると，リアルタイムな決済ができる．反面，事後決済が行えなくなり，利用者の利便性が低下する．

【決済方式と併せて検討する必要のある項目】

「デバイス非依存」「モニタリング機能」「登録機能」「誰でも使える」「無意識」などの要件を満たすためには，決済方式と併せて，デバイスの機能や電子マネー決済システムの構成を検討する必要がある．

【既存決済サービスからの移行】

オープンループ型電子マネーが普及し一般的な決済手段となるかどうかは，利用者に受け入れられるかどうかにかかっている．物理実体として存在する現金への信頼感や，事後の決済でサービスを享受できるクレジットカードなどの決済方式は広く受け入れられている．現在の状況から突然，新たな決済方式としてオープンループ型電子マネー単独方式に移行することは現実的でない．何らかの既存決済方式との連携が必要と言える．

4-1）結論 2

オープンループ型の電子マネー単独方式の課題から以下の結論が導き出される．

オープンループ型電子マネーと口座振替／クレジットカード／デビットカードとの連携方式を導入する．

これにより，オープンループ型の電子マネー単独方式の課題を解決することができる．

【決済タイミングの多様性の確保】

クレジットカードが与信機能を持つため事後決済を実現できる．

【決済方式と併せて検討する必要のある項目】

オープンループ型電子マネーと口座振替／クレジットカード／デビットカード連携を用いた決済システムの構成モデルを,**「５）連携方式」**の検討で具体的に検討する.

**【既存決済サービスからの移行】**

口座振替／クレジットカード／デビットカードは広く受け入れられており，こうした決済方式を活用することによって，スムーズにオープンループ型電子マネーが受け入れられる.

**５）連携方式の検討**

**「4-2）結論２」**にて,「結論 2：オープンループ型電子マネーと口座振替／クレジットカード／デビットカードとの連携方式を導入する」が導き出された．そこでここでは，口座振替／クレジットカード／デビットカードとオープンループ型電子マネー（仮称：UBI マネー）を連携させることによって，ユビキタスコンピューティング環境を支える決済を実現するモデルを検討する.

**5-1）連携の概要（全体イメージ）**

連携部分には UBI マネーWeb サーバ，決済サーバ，発行サーバを持つ UBI マネー発行システムを設置する．UBI マネー発行システムにて発行された UBI マネーは，各ノード（移動ノードや固定ノード）を転々流通しながら，ユビキタスネットワーク内での決済を担い，必要に応じて UBI マネー発行システムによりリアルマネーに変換される.

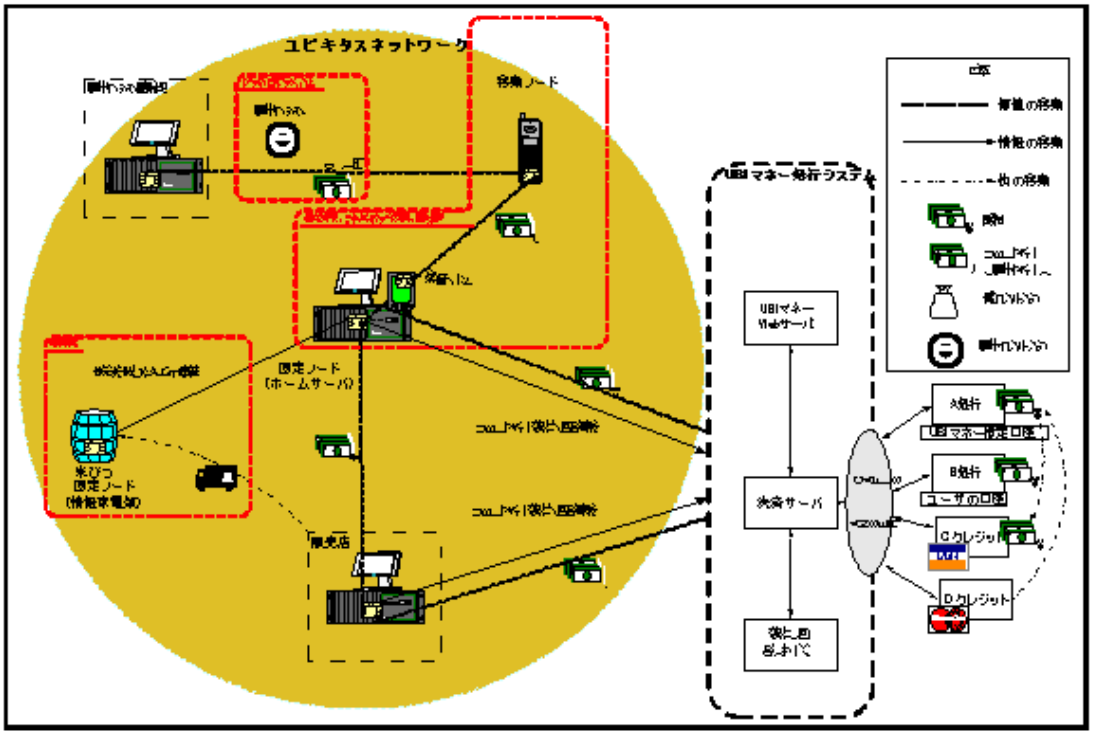



図 5.5.2-1：「連携方式概要図」

**■ユビキタスネットワーク上のノードの種類**

**【移動ノードと固定ノード】**

ユビキタスネットワーク上のノードには移動するものと固定されたものがある．ユーザに携帯される移動ノードと設置されることを想定した固定ノードに分類できる．

**【登録ノードと未登録ノード】**

ノードの登録機能を持つことによって，現在使われているモバイル機器・PC をユビキタスコンピューティング環境で利用できるため，利用者は新たな機器の購入をしないですむ．また，チャージ権限の有無を設定することによって，本来，高額な決済を行えなかった子供などにも，ユビキタスコンピューティング環境で決済を行えるようになる．

**【センサノード】**

センサノードは UBI マネーのやり取りを直接は行わないが，ユビキタスコンピューティング環境における決済を発生させる環境の変化（以下，環境情報とする）を感知する役割を担う．本機能により UBI マネーの集中管理が実現でき，分散格納によるリスクの拡散を防ぐ．

■UBI マネー発行システムのノードの種類

【UBI マネーWeb サーバ】

登録ノードに Web ページ（口座情報など他サーバとのやりとり）を表示する.

【UBI マネー決済サーバ】

銀行やクレジット会社との決済を行う.

【UBI マネー発行（回収サーバ)】

決済サーバより指定された登録ノードに UBI マネーの発行，回収を行う.

5-2) 連携方式の特徴

本連携モデルは以下の特徴を持つ.

■オープンループ型の電子マネーを実現する

オープンループ型電子マネーにより

- 転々流通を実現できる
- 即時決済を実現できる
- 匿名決済を実現できる
- マイクロペイメントを実現できる

■既存決済網の CAFIS・ANSER 等を活用する

- ユビキタスコンピューティング環境移行が現実的でスムーズとなる
- 利用者は使い慣れたクレジットカードやキャッシュカードを活用できる
- 移行の際の，投資コストが低額ですむ
- 払い戻し準備金に対する監査の手間が集約される

■ホームサーバを採用する

ホームサーバとして家庭内のさまざまな情報を扱い，機器と機器が協調するのを手助けする中心的な役目を担うサーバである.「(3)-2 決済に関わる要件」で抽出された決済要件のうち「無意識」,「誰でも使える」を実現する.

### 5-3) 決済要件に対する分析（本システムの考察）

「3-2) 決済に関わる要件」で整理されたユビキタスコンピューティング環境を支える決済要件項目を活用して UBI マネー発行システムを評価する．（参照：**表 5.2.2-3: ユビキタスコンピューティング環境において必要とされる決済要件**）

## 6) 課題

### 6-1) 運営/制度に関する課題

**■決済コスト**

本連携方式では UBI マネーのチャージ毎に，クレジットカード会社や各銀行への振込み手数料（コスト）が発生する．利便性を高めてもコストがかかればユーザに受け入れられない．

こうしたデメリットを解決するため，以下のような方式を採用し，ビジネススキームを確立する必要がある．

- 現金を数えるなどのコストがなくなる分，店舗が売り上げの一定比率分を UBI 会社に支払う
- 売り上げ増大が見込める分，店舗が売り上げの一定比率分を UBI 会社に支払う
- 回数による課金ではなく金額の割合に対する課金とする

**■オープンループ型電子マネーの法律の課題**

単純なプリペイドカードについては，プリペイドカード法が存在するが，電子マネーについては，“電子マネー法”が審議中であり，まだ施行はされていない．特に「オープンループ型電子マネー」に関しては，以下の法律が関係しており新たな法制度が必要になる．

- 出資法
- 銀行法
- 前払式証票規制法プリペイドカード法
- 紙幣類似証券取締法

**■オープンループ型電子マネーに関する運営主体の課題**

オープンループ型電子マネーは以下のような要件を備えた発行体により運営されなければならない．

- 偽造防止やネットワークの安全を保持する高い技術力があること

- 資産・管理のノウハウ運用能力があること
- 公的規制監督をうけていること

**■多通貨対応世界的な組織の必要性**

ユビキタスコンピューティング環境におけるオープンループ型電子マネーは，ユーザ利便性の観点から全世界でシームレスに利用できることが望ましい．しかし，利用当初から世界中で利用できる電子マネーを導入することは以下のような問題から事実上困難である．

- 電子マネーで取引を行う上での国際的合意や約束事（法律）が存在しておらず，消費者が利用を躊躇する
  （例） 署名に関する拘束力の共通化
- 基準レートをどのように設定するか整理されていない
- 限定した国・地域での利用を実験的に開始し，発生した問題点の解決，制度の整備を実現した上で，多地域，国家間の電子マネー導入を目指すのが現実的である．

### 6-2) 技術的な課題

**■セキュリティの確保**

セキュリティを確保するため，以下の技術的課題を解決する必要がある．

- ユーザノードの電子マネーを格納するマイクロチップの対タンパ性確保
- 電子マネーの偽造を防止する仕組みの構築
- 安全なネットワークと認証の仕組みの構築

## 7) 決済に関する現状調査

### 7-1) モバイル決済に関するトレンド

**■NTT ドコモの事例**

（株）NTT ドコモ，日本コカコーラ（株），伊藤忠商事（株）の３社が締結した合意に基づくサービスで，i モード携帯電話と新型情報端末自動販売機である Cmode 対応の自動販売機（愛称「シーモ」）を連動させることにより，情報発信サービス，コンテンツサービス，ポイントサービスを提供する会員制消費者サービス．

**■J－PHONE の事例**

2001 年 4 月，J-フォングループは，JCB，日本ヒューレット・パッカ

ードと，J-スカイ向けのモバイル決済システムを共同開発する．

■au の事例

icePAY Japan，KDDI ら 6 社は，ネットバンク決済連動型のモバイル(M)コマースのトータルサービス「icePAY」(Internet Certification Payment)を，2002 年春をめどに開始する予定である．

### 7-2) 電子マネーに関する動向

■Mondex

Mondex（モンデックス）は National Westminster 銀行（英）が 1990 年に開始した電子マネープロジェクトであり，IC カードを利用したオープンループ型の電子マネー方式を採用している．

このプロジェクトで流通する電子マネーは匿名性を保ったまま転々流通し，現金と同様即時決済が可能である．

バリューの移動は必ず「カード」間で実行され，「カード」から盗み出すことはできない．

日本では日立・JCB らと提携して利用拡大を図っている．

■Edy

Edy は，SONY の関連会社であるビットワレット株式会社が運営するプリペイド型電子マネーサービスの名称である．利用媒体はソニーの開発した IC カード技術『FeliCa』が使われている．

■PayPal

ネット上でのオンライン決済サービスで，個人を対象にしたクレジットカード支払いシステムである．利用者は全米で８００万人を越え，一日に約 800 万ドルの現金がペイパルを通じて支払われており，世界最大のインターネット上の支払いネットワークといえる．

### 7-3) 決済の標準化に関する動向

■Paycircle

米国およびヨーロッパの大手テクノロジー企業各社によるモバイル機器を使った決済方式の標準化を目指す団体である．設立メンバー企業となったのは，Hewlett-Packard ，Lucent Technologies，Oracle ，Sun Microsystems ， ドイツの Siemens の５社である．

### 7-4) 決済プラットフォームの現状

**■銀行振込の決済システム**

預金の移動による決済方法では，銀行を利用する者の間の債権 - 債務関係を銀行間の債権 - 債務関係に置き換えて決済することになる．

**■CAFIS**

クレジットカード会社，金融機関，流通企業，加盟店など幅広くを結ぶ共同利用型クレジットオンラインシステムである．

**■ANSER**

様々なネットワーク・各種ホストコンピュータを LAN で接続し，バンキングサービスの創造を支援するネットワークサービスである．

**■マルチペイメントネットワーク**

振込み業務を ATM，電話，パソコン等の各種チャネルを利用して支払いができ，収納企業に即時に消しこみ情報が通知されるサービスである．

| | | タイミング＊1 | 完了までの期間＊2 | 転々流通性 | 匿名性 | コスト 払い手 | コスト 受け手 | コスト 事業者 | 額・単位の制約 | 与信の必要性 | 利用者敷居 | インターネットの経由 | セキュリティーホール＊3 | モバイル機器からの利用 | 主なサービス元 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| リアル決済 | 現金 | 即 | 即 | 有 | 有 | ＊4 | 回収保管計算 | 発行 | 無 | 無 | 無 | 無 | 偽造 | 無 | 日本銀行 |
| | 小切手・手形 | 即 | ＊4 | 有 | 無 | ＊4 | 回収保管計算 | 発行 | 無 | ＊4 | 有 | 無 | 偽造<br>不渡り | 無 | 法人<br>個人 |
| | 各種金券 | 即 | ＊4 | 有 | 有 | ＊4 | 回収保管計算 | 発行 | 単位ごと | 無 | 無 | 無 | 偽造 | 無 | 図書券等 |
| 電子決済 | 銀行振込 | 即 | 即 | 無 | 無 | 100～400 円 | ＊4 | ＊4 | 無 | 無 | 無 | ネットバンク | 無 | ネットバンク | 銀行，郵便局，コンビニ |
| | 口座振替 | 後 | 1～2 月 | 無 | 無 | ＊4 | ＊4 | ＊4 | 無 | 有 | 無 | 無 | 無 | 無 | 公共料金業者<br>銀行 |
| | クレジットカード | 後 | 1～2 月 | 無 | 無 | ＊4 | 3%～7% | ＊4 | 限度額 | 有 | 与信 | 電子クレジット | 成りすまし，番号漏洩 | 有 | VISA<br>Master |
| | デビットカード | 即 | ＊4 | 無 | 無 | ＊4 | 1%～2% | ＊4 | 無 | 無 | 無 | インターデビット | 暗証番号漏洩 | 有 | 銀行 |
| | 代金引換 | 即 | ＊4 | 無 | 無 | ＊4 | ＊4 | ＊4 | ＊4 | 無 | 無 | 無 | 無 | 無 | ヤマト運輸<br>ｲｰｼｮｯﾋﾟﾝｸﾞ |
| | コンビニ決済 | 即 | ＊4 | 無 | 無 | ＊4 | 1% | ＊4 | ＊4 | 無 | 無 | NW 型 | 無 | 無 | ローソン<br>野村総研 |
| | 通信事業者代行決済 | 後 | 1 月 | 無 | 無 | ＊4 | ＊4 | ＊4 | ＊4 | 有 | 電話加入 | 無 | 無 | 無 | NTT<br>プロバイダー |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 電子マネー | オープンループ型 | 前 | 即 | 有 | 有 | ＊4 | ＊4 | ＊4 | マイクロペイメント可 | 無 | 無 | 有 | 偽造 | 有 | Mondex |
| | | クローズドループ型 | 前 | 即 | 無 | 有 | ＊4 | ＊4 | ＊4 | 上限有 | 無 | 無 | ＊4 | 偽造<br>改竄 | ＊4 | ネットーU<br>BItCash<br>Webmoney |
| | | ネットワーク型 | 前 | 即 | 有 | 無 | ＊4 | ＊4 | ＊4 | マイクロペイメント可 | 有 | 無 | 有 | ネットワーク漏洩 | ＊4 | Ecash<br>PAYPAL |

＊1 払い手が決済を済ませるタイミングのこと　前：事前決済　即＊リアルタイム決済　後：事後決済を示す
＊2 受け手が価値を受け取るまでの期間のこと
＊3 セキュリティーホールに関しては内部からの横領など想定しない
＊4 該当項目なし．もしくは様々でありどれとも言えない

表 5.5.2-1：既存決済サービス一覧

| 項目 | 要件 | 詳細要件 |
|---|---|---|
| タイミング | 事前決済 | 前払いする機能がある |
| | リアルタイム決済 | ・ 即時決済を行うことによってサービスを円滑にする<br>・ 与信機能のかわりとなる<br>・ 高速なデバイス間通信によって，高速移動中にも決済可能にする |
| | 事後決済 | 事後決済ができる |
| 範囲 | マイクロペイメント | 1 円以下の単位で決済をできる |
| | 決済額設定機能 | 設定した範囲内の決済ができる |
| 性質 | 転々流通性 | バリューが転々流通する |
| | ネットワーク流通性 | ネットワークを介した決済ができる |
| | 匿名性 | 匿名での決済が可能である |
| コスト | 低額　or　0 | 利用者負担が低額ですむ |
| ハード | デバイス非依存 | あらゆる家電やハードで決済が行える |
| | モニタリング機能 | 決済額やマネー残高などが表示される |
| 利用者 | 誰でも使える | 子供や障害者でも決済を行える |
| | 無意識 | 状況の変化を機器が判断して決済を行える |
| 認証・セキュリティ | 人を特定する決済 | 相手を特定しての決済が可能である |
| | 格納デバイスの対タンパ性 | チップが安全である |
| | ネットワークの安全性 | 安全なネットワークを通過する |
| | 成りすまし，送信否認，改竄，漏洩防止 | 成りすまし，送信否認，改竄，鍵やロジックの漏洩を防止する |
| 与信 | 与信 | 手持ち資金がない場合のクレジット機能がある |
| その他 | 既存決済との連携 | 既存の決済方式と円滑に連携する |
| | 登録機能 | 決済に必要な情報の登録や設定が簡単にできる |

表 5.5.2-2：ユビキタスコンピューティング環境において必要とされる決済要件

| 項目 | 要件 | 評価 | 評価内容 |
|---|---|---|---|
| タイミング | 事前決済 | ○ | UBI マネーのチャージが事前に行われている |
| | リアルタイム決済 | ○ | UBI マネーはサービスの授受と同時に決済 |
| | 事後決済 | ○ | クレジットカードと連携することによって実現 |
| 範囲 | マイクロペイメント | ○ | 円に替わりネットワーク流通可能な UBI マネーが，1 円以下の決済を実現する |
| | 決済額設定機能 | ○ | チャージ機能および未登録ノードを設定したことにより，ノードごとの決済額管理が容易 |
| 性質 | 転々流通性 | ○ | 価値実体である UBI マネーが転々流通する |
| | ネットワーク流通性 | ○ | 既存通貨を電子マネーに変える機能をもつ |
| | 匿名性 | ○ | UBI マネーを使用することにより匿名性を確保 |
| コスト | 低額　or　0 | × | チャージ時に手数料が発生する |
| ハード | デバイス非依存 | ○ | センサノードが直接 UBI マネーを保有することはないが，ホームサーバが管理することによって，家電などあらゆるノードが発する情報に対して円滑に決済サービスを提供する |
| | モニタリング機能 | ○ | デバイスにモニタリング機能を持たせることにより実現可能である |
| 利用者 | 誰でも使える | ○ | 権限委譲により子供でも未登録ノードを使うことができる |
| | 無意識 | ○ | ホームサーバや移動ノードに自動動作の条件を設定することによって無意識に行える |
| 認証・セキュティ | 人を特定する決済 | ○ | 移動ノードの個人識別情報により個人を特定して決済ができる |
| | 格納デバイスの対タンパ性 | — | |
| 与信 | 与信 | ○ | クレジット会社との連携により可能．UBI 決済システムが実現する |
| その他 | 既存決済との連携 | ○ | 銀行口座やクレジットカード等の既存の大規模な決済方式と連携している |
| | 登録機能 | ○ | アプリケーションの設計によって登録・設定を簡易にする（今回のシステム構成自体が登録・設定を複雑にすることはない） |

（＊○満たす　　×満たさない　　－本稿では調査外）

表 5.5.2-3：決済用件分析

# 参考文献

## (1) 決済サービス・プラットフォームに関する参考 Web サイト


- 株式会社 NTT データ
  http://nttdata.co.jp
- サービス・プロダクト
  http://www.nttdata.co.jp/service/index.html
- 株式会社ペイメント・ワン
  http://www.payment-one.com/service/b-2-01-01.shtml
- 電子マネーと経済秩序の変容可能性
  http://red.glocom.ac.jp/johoka/wp/EMONEY.html
- 日本銀行
  http://www.boj.or.jp/index.html
- 沖電気
  http://www.oki.com/jp/Home/JIS/New/OKI-News/2001/10/z0177.html


## (2) 決済に関する参考文献，Web サイト

### 2-1) 書籍


- 「手にとるようにユビキタスがわかる本」，株式会社ＮＴＴデータ，荒川弘熙監修，日高昇治編著（2001 年，日経ＢＰ社，ISBN4-7612-5965-5）．


### 2-2) Web サイト／Web ページ


- 電子商取引推進協議会
  http://www.ecom.or.jp/
- 日本デビット推進協議会
  http://www.debitcard.gr.jp/
- 日本マルチペイメントネットワーク推進協議会事務局
  http://www.jampa.gr.jp/
- 日本モンデックス推進協議会
  http://www.mondexjapan.com/index2.html
- ビット・ワレット株式会社
  http://www.bitwallet.co.jp/
- 株式会社 NTT ドコモ
  http://www.nttdocomo.co.jp/index.shtml

- 株式会社 KDDI
  http://www.au.kddi.com/
- J-フォン株式会社
  http://www.j-phone.com/h/index.html
- IcePAYjapan
  http://www.icepay.co.jp/
- PayPal
  http://www.paypal.com/cgi-bin/webscr?cmd=p/wel/index-outside

### (3) その他の参考文献


- 「ユビキタスネットワーク」, 野村総合研究所, 野村総合研究所広報部.
- 「ユビキタスネットワークと市場創造」, 野村総合研究所, 野村総合研究所広報部.
- 「手にとるようにユビキタスがわかる本」, 日高昇治, かんき出版.
- 「デジタルマネーのすべて」, 日経デジタルマネーシステム.
- 「最新欧州電子マネー事情」, ヨーロッパ電子マネー　リーディングエッヂ調査団.

# 5.6 システム統合技術

このサブテーマは，本研究プロジェクトが多くの個別の成果を生み出したあとで，それらを連携，結合させ，トータルなユビキタスコンピューティング環境を構築するための技術開発を目的としている．本年度は，まだ研究の立ち上げ段階であり，まだ本サブテーマの研究作業は継続的に進めており，まとまった成果として報告する部分は来年度以降になる．

# 5.7 超機能分散システム指向開発環境

## 5.7.1 平成 13 年度の成果概要

次年度以降のユビキタスネットワーキング研究に必要な基盤プラットフォームを設計・試作を行なった．構築した基盤プラットフォームは，以下の通りである．

119. U-Card (Ubiquitous Card)ユビキタスネットワークノードのための基本ボード（携帯型）

120. μU-Card(Micro Ubiquitous Card)ユビキタスネットワークノードのための基本ボード（据置型）

### 1) U-Card

携帯型ノードを想定した，実験開発用ボードである．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/IEC 7816, ISO/IEC 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．こうした機能を有するハードウェアが，バッテリーで駆動する．

### 2) μU-Card

据置型ノードを想定した，実験開発用ボードである．CPU とした M32 を用い，各種の実験開発が行なえるように，多くのインタフェース（シリアル，PCMCIA，ISO/IEC 7816，10base-T，人口網膜カメラなど）を備えている．

## 5.7.2 携帯型ノード開発システム（U-Card）の研究開発

### １）U-Card の位置付け

U-Card は，当研究所の研究開発における各種実験を行う際の標準開発プラットフォームである．様々な場所や状況において使用することを考慮し，バッテリ駆動が可能で携帯が容易にできる小型の開発装置とする．また，U-Card 単体でもユーザが各種操作を行えるようにディスプレイや各種入力装置を備える．

### ２）要求仕様の検討

U-Card に要求される仕様の検討を行った．以下にその要求仕様を示

す.

- CPU には高性能 32 ビット CPU を搭載し,種々のセキュリティ機能や通信機能を実現可能とする.
- ユーザインタフェースとして，カラーLCD とタッチパネルを搭載し GUI による操作を可能とする．また，複数のスイッチ入力も設ける.
- 周辺機器の拡張を可能とするため,カード I/F と USB ホスト I/F を設ける．カード I/F にはストレージカードを使用することにより外部記録装置として使用することができる．また，Ethernet 等の有線や Buletooth 等の無線のネットワーク I/F カードを使用する事により，これらの各種通信環境に対応することが可能である.
- セキュリティ機能については，SIM カード I/F を内蔵し SDCC チップを使用可能とする．また，非接触型 IC カードリーダライタおよび指紋認証ユニットを内蔵する.
- 音声の入出力 I/F を設ける.
- RTC（リアルタイムクロック）を内蔵する.
- ハードウェア全体は小型の筐体に内蔵し，各所への設置はもちろん携帯することも可能とする.
- 拡張スロットを設け，容易にハードウェアが拡張できるようにする.
- ソフトウェアは，組み込み機器で利用実績の高い ITRON 仕様をベースとしたリアルタイム OS を使用する
- ROM に 4M バイト以上のフラッシュメモリを搭載する．また RAM は 8M バイト以上とする.
- 電源は AC アダプタおよびバッテリの両方を使用可能する．バッテリ使用時にはパワーマネージメントが可能とする.

### ３）U-Card ハードウェアの仕様

前節で述べた要求しように基づき，U-Card のハードウェアの仕様を策定した．表 5.7.2-1 に U-Card ハードウェア仕様の概要を示す.

| 項目 | 内　容 |
|---|---|
| CPU | メイン: SH7727 (日立製作所 SH3-DSP)<br>サブ　: SH7290 (日立製作所 SH-Mobile) |
| 寸法 | 120mm × 75mm |
| RAM | 32MB SDRAM |
| ROM | 8MB Flash ROM |
| 内蔵機能 | TFT カラーLCD (QVGA サイズ)<br>タッチパネル<br>非接触型 IC カードリーダライタ<br>指紋認証ユニット<br>カメラモジュール<br>アプリケーションスイッチ<br>RTC（リアルタイムクロック） |
| 外部インタフェース | マイク入力/スピーカ出力 1ch<br>シリアルＩ／Ｆ　１ｃｈ<br>CF カード I/F１スロット<br>MMC カード I/F１スロット<br>SIM カード I/F１スロット<br>USB ホスト type A 1ch<br>USB デバイス 1ch<br>拡張バス I/F １スロット |
| 電源 | ＡＣアダプタおよびバッテリ駆動<br>電源制御ＣＰＵ (H8/3048F)搭載 |

表 5.2.7-1. U-Card ハードウェア仕様の概要

以下に U-Card ハードウェアの仕様の説明を記す.

**メイン CPU**：メイン CPU には, 日立製作所製 SH7727 を用いる. SH7727 は 32 ビット RISC マイコンであり,カラーLCD インタフェースを含む各種周辺機能内蔵している. 表 5.2.7-2 に SH7727 の仕様概略を示す.

| 項目 | 内容 |
|---|---|
| シリーズ | SH3-DSP |
| キャッシュメモリ | 16Kbyte |
| X/Y メモリ (DSP 用) | 16Kbyte |
| 内蔵周辺機能 | DMAC × 4ch<br>MMU<br>USB ファンクション ×1ch<br>32bit タイマ × 3ch |
| インタフェース | PCMCIA カード I/F<br>ADC 10bit × 8ch<br>DAC 8bit × 2ch<br>USB ホスト I/F × 1ch<br>カラーLCD I/F<br>シリアル I ／ F ×2ch<br>FIFO 付シリアル I/F× 2ch<br>調歩同期式シリアル I/F×2ch |

表 5.2.7-2. SH7727 の仕様概略

**サブ CPU**：サブ CPU には，日立製作所製 SH7290 を用いる．SH7290 は次世代携帯電話システム向けの 32 ビット RISC マイコンであり，ビデオ I/O インタフェースなどの携帯機器向けの周辺機能を有する．サブ CPU はこれらの周辺機能を用いてメイン CPU の機能を補佐する．表 5.2.7-3 に SH7290 の仕様概要を示す．

| 項目 | 内容 |
|---|---|
| シリーズ | SH-Mobile (SH3-DSP コア) |
| 内蔵ＲＡＭ | 128Kbyte |
| キャッシュメモリ | 32Kbyte |
| X/Y メモリ (DSP 用) | 16Kbyte |
| 内蔵周辺機能 | DMAC × 6ch<br>MMU<br>USB ファンクション × 1ch |
| インタフェース | ベースバンド LSI 接続用 I/F<br>NAND/AND 型フラッシュメモリ I/F<br>ビデオ I/O 直結 I/F<br>マルチメディアカード I/F<br>SIM カード I/F<br>キースキャン I/F<br>I2C バス I/F<br>シリアル I/F × 2ch<br>FIFO 付シリアル I/F × 2ch<br>調歩同期式シリアル I/F × 2ch |

表 5.2.7-3. SH7290 の仕様概要

**ユーザインタフェース**：QVGA (240×320 ピクセル) サイズのカラーTFT 液晶ディスプレイを搭載し，メイン CPU の LCD インタフェースにより制御する．また，この液晶ディスプレイにはタッチパネルの機能を持たせ，ユーザはタッチパネルにより入力を行う事ができる．入力スイッチとして，１つの十字型のカーソルスイッチと４つのアプリケーションスイッチを設ける．これらのスイッチはアプリケーションから自由に使用可能である．

**カメラモジュール**:11 万画素の CMOS センサカメラモジュールを内蔵する．このモジュールはサブ CPU により制御され，静止画および動画の撮影に使用する事ができる．

**SDCC 対応**：ボード上に SIM カードソケットを１つ設ける．また，非接触型 IC カードリーダライタを内蔵し，U-Card 単体で SDCC カードのリード/ライトを可能とする．

**カードインタフェース**：CF（コンパクトフラッシュ）カードと MMC（マルチメディアカード）のスロットを各々１つづつ設ける．

**ハードウェアの拡張性**:USB ホストおよび USB デバイスインタフェースを各々１つずつ設け，各種 USB デバイスの接続が可能である．また，ボード上に CPU バス信号を出した拡張ソケットを設ける．これにより必要に応じて拡張ボードを接続することができる．

**電源制御**：電源制御用マイコンとして H8/3048F を搭載する．電源制御マイコンはバッテリの管理やシステム全体の電源管理を行う．低消費電源モード時はこの電源制御マイコンのみを動作させ，メイン CPU およびサブ CPU は停止させることができる．また，この状態において電源制御マイコンはタッチパネルやスイッチの入力を監視し，必要に応じてメインおよびサブ CPU を起動することができる．

### ４）成果および課題

H13 年度は前項で述べた仕様に従い，U-Card のハードウェアの開発を行った．

このハードウェア上において，リアルタイム OS，ネットワークプロトコル，GUI 等のソフトウェアを動作させ，その確認を実施した．

写真 5.2.7-1 に U-Card の全体写真を示す．

今後は U-Card 上で動作するミドルウェアを充実させ，本研究所の各種実験に使用すると共に，標準開発プラットフォームとしての完成度を高めていく．

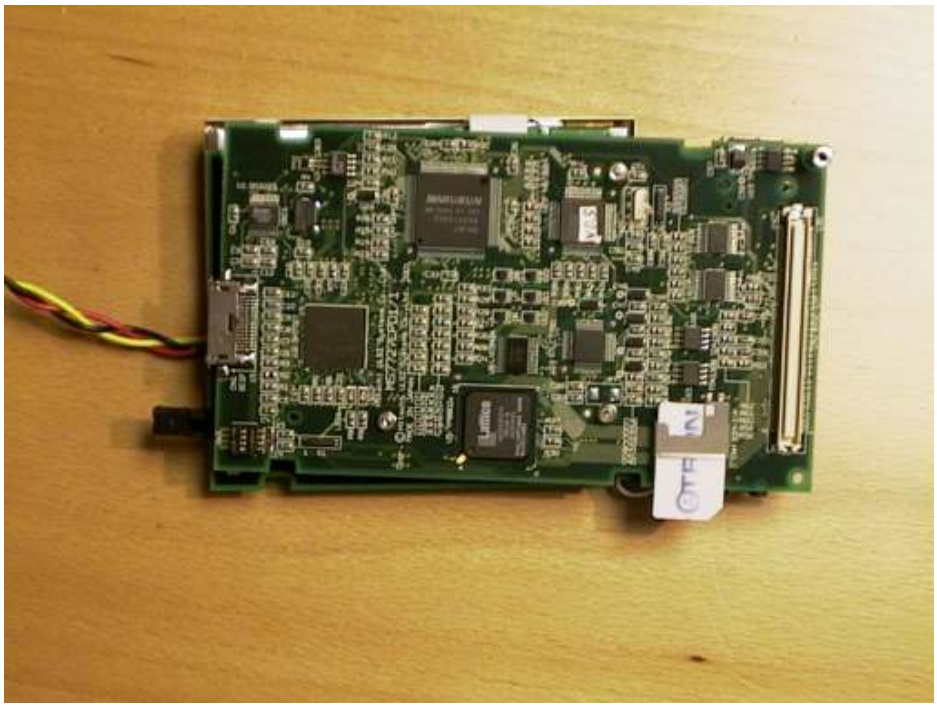


写真 5.2.7-1: U-Card（裏面）

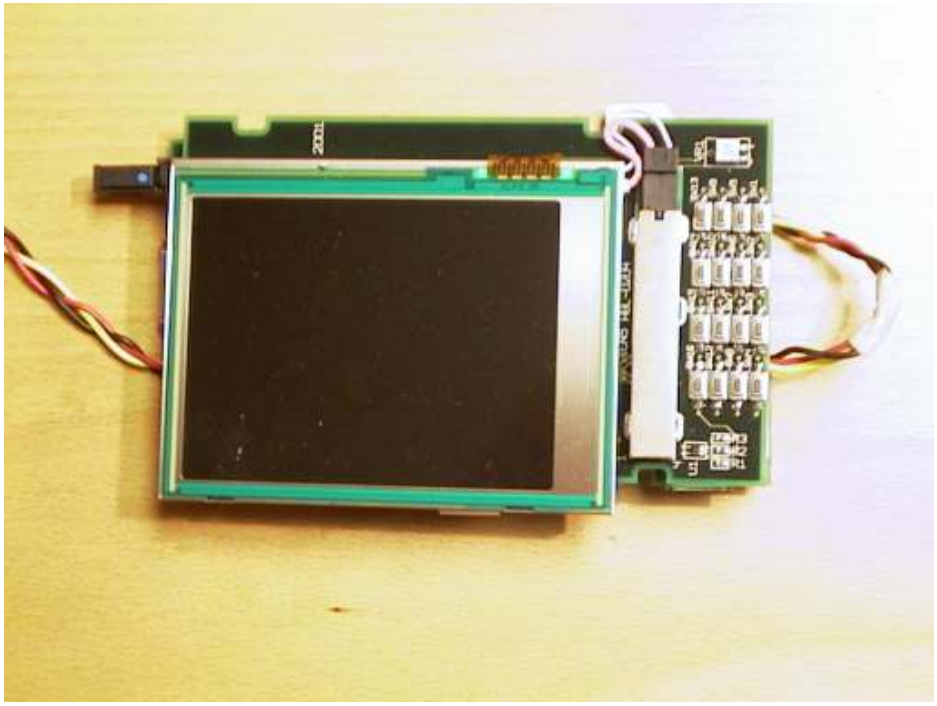


写真 5.2.7-2: U-Card（表面）

## 5.7.3 据置型ノード開発システム（μU-Card）の研究開発

### １）μU-Card の位置付け

本研究では，身の周りの様々な場所に配置されたコンピュータ同士がリアルタイムに情報をやりとりして協調動作するための，基盤プロトコルを開発する．そして，その有効性を検証するため，環境制御，環境把握を行うユニットを大量に環境に配置して実証実験を行う．例えば，部屋にいる人の位置や動作を検出したり，温度や湿度を多数のポイントで測定し，その結果をもとにドアの開閉をしたり，照明や空調を最適制御するといった実験を行う．

実験は様々な場面を想定して行うため，実験で使用するハードウエアは拡張性が良いことや，ミドルウエアやアプリケーションを効率良く開発でき，また設計資産を容易に流用できることが必要である．そのため本研究の目的に沿った仕様で標準化された開発プラットフォームが必要になる．またプラットフォームが標準化されていれば，研究成果の実用化および普及を促進する際のベース仕様とすることが可能となり，本研究の成果を具現化することに非常に効果がある．

μU-Card はこのような実証実験で使う標準開発プラットフォームである．様々な場所に配置するためコンパクトなサイズであること，様々な通信機能，センサ機能を実現できること，様々な機器が制御できること，セキュリティ機能が実現可能なことが要求される．

そして平成１３年度は，μU-Card の仕様研究および開発を行い，次年度以降の研究の基盤構築を行った．本章では平成１３年度の成果としてその内容を報告する．

### ２）μU-Card の仕様研究

まずμU-Card に要求される特徴を検討した．以下にそれを示す．

- 様々な場所に配置できるようにコンパクトなサイズであること．
- 様々な通信機能が実現できること．また研究場所の通信インフラと整合性があること．
- 様々なセンサ機能が実現できること．
- セキュリティ機能が実現できること．
- 様々な研究で使えるようにＣＰＵの処理性能が高いこと．
- 様々な研究で使えるように大容量のメモリを搭載していること．

- ソフトウエアの開発環境が統一できること.
- ソフトウエア基盤として ITRON が動作すること.
- 誤接続等による事故を防ぐ措置がとられていること.
- 電源等の取り回しが容易なこと.

これらの特徴を実現するために，標準開発プラットフォームへの要求仕様を検討した．以下にそれを示す.

### 2-1) μU-Card のシステム構成

μU-Card 標準開発プラットフォームは次の装置で構成される.

a）ＣＰＵボード　１式
b）通信・センサ機能拡張ボード　１式
c）電源等の付属品　１式

### 2-2）システム全体として満足する必要がある技術的要求要件

μU-Card 標準開発プラットフォームは長時間連続動作させて実験を行う場合がる．そのためハードウェアの信頼性・安定性・保守性がそれぞれ高いことを求める.

### 2-3）μU-Card 標準開発プラットフォームの要求要件

ここでは各機器に必要とされる要件の詳細について規定する.

#### （１）ＣＰＵボード

A) ２００ＭＨｚ以上の周波数で動作する３２ビットＣＰＵを搭載すること.
B) ２Ｍバイト以上のＲＡＭを搭載すること.
C) ４Ｍバイト以上のフラッシュメモリを搭載すること.
D) ３８．４ｋｂｐｓ以上のシリアルインタフェースを搭載すること．本シリアルインタフェースはデバッグ用コンソールポートとして使用する.
E) コンパクトフラッシュカードスロット（Ｔｙｐｅ２）を１スロット以上搭載すること.
F) マルチメディアカードスロットを１スロット以上搭載すること.
G) セキュリティチップインタフェースを搭載すること．物理仕様は ETSI TS102221，ISO 7816 仕様に準拠していること.

H) 拡張ボードを接続するソケットを搭載すること．誤接続防止のための措置がとられていること．
I) カレンダ機能を実現するクロックを搭載すること．バッテリバックアップされていること．
J) 電源として市販のＡＣアダプタ（５Ｖ）を接続して使用できること．ＤＣジャックはＥＩＡＪ電圧区分２を使用すること．ＤＣジャックの極性は外側マイナス，内側プラスとする．
K) リセットスイッチおよび電源スイッチを装備すること．
L) モード設定スイッチを装備し，CPU がポートを介して設定検出できること．
M) ＬＥＤを 2 個以上搭載し,CPU がポートを介して点灯/消灯できること．
N) ボードサイズは 85mm×60mm とする．

**（２）通信・センサ機能拡張ボード**

A) 有線あるいは無線通信を実現する機能を搭載すること．例えば次のような通信機能が考えられる．
- 有線通信
  - 100Base-TX イーサネット
  - 10Base-T イーサネット
  - 電力線モデム
  - ISDN
  - ADSL
- 無線通信
  - IEEE 802.11b 無線 LAN
  - Bluetooth
  - PHS
  - 赤外線通信

B) センサ機能を搭載すること．例えば次のようなセンサ機能が考えられる．
- 人あるいは物の位置検出機能
- 人あるいは物の動作検出機能
- 音声を認識するための情報入力機能
- 温度，湿度等の測定機能

C) 外部接続機器制御用のインタフェースを搭載すること．例えば次のようなインタフェースが考えられる．

- シリアルインタフェース
- ポートインタフェース
- USB インタフェース
- PWM(Plus width modulate)インタフェース

※研究場所で使用が想定される通信インフラは次の通りである．

- 10Base-T 及び 100Base-TX 仕様による有線 LAN ネットワーク
- IEEE 802.11b 仕様による無線 LAN ネットワーク
- PHS 内線を利用した PISFS による通信回線

※通信機能はコンパクトフラッシュカード（ＣＰＵボードに接続）で実現される場合もある．

### （３）電源等の付属品

A) ＣＰＵボードに電源供給するＡＣアダプタ．

B) ＣＰＵボードとデバッグコンソールを接続するシリアルケーブル．

## ３）μU-Card の開発

前節で述べた標準開発プラットフォームへの要求仕様を元に，具体的な実験用ハードウエアの仕様を策定し，その開発を行った．

### 3-1）実験用ハードウエア仕様

### （１）CPU ボード

CPU ボードの仕様を以下に示す．またブロック図を図 5.7.3-1 に示す．

- CPU: A 社製 32 ビット RISC マイコン
- 内部動作周波数:最大 216MHz
- 外部バス動作周波数:最大 54MHz
- 主な内蔵周辺機能
  - 割り込みコントローラ
  - マルチファンクションタイマー
  - シリアル I/O
  - メモリコントローラ

ブロックセレクトコントローラ
DMA コントローラ

- RAM:16M バイト
- フラッシュ ROM:4M バイト
- コンパクトフラッシュインタフェース
- マルチメディアカードインタフェース
- セキュリティチップインタフェース
- 非同期シリアルインタフェース:最大 115,200bps
- リアルタイムクロック:リチウム電池でバッテリバックアップ
- 拡張バスインタフェース
- 140 極コネクタ使用.
- 誤挿入防止のためにコネクタにハードウエア種別を示す突起を設け種別が一致した CPU ボードと拡張ボードの組み合わせのみで接続できるようにする.
- 拡張バスに出力する信号線は以下の通り.
  CPU バス(アドレス 23 本, データ 32 本, 制御線 7 本)
  バスクロック 1 本
  リセット信号 1 本
  割り込み信号 1 本
  入出力ポート 14 本
  デバッグインタフェース信号 6 本
  LED, スイッチ 4 本
  電源 8 本
  グランド 35 本
  未使用 8 本
- 電源　3.3V 単一電源.
- AC アダプタ(5V)からの電源を 3.3V に変換する基板モジュールを別途用意する. これにより, 電池等別電源への対応を可能とする.
- リセットスイッチ:CPU リセット端子に接続
- 電源スイッチ:CPU 割り込み端子に接続
- DIP スイッチ:CPU からはポートを介して設定検出
- LED 2 個:CPU からはポートを介して点灯/消灯
- ボードサイズ:85mm×60mm

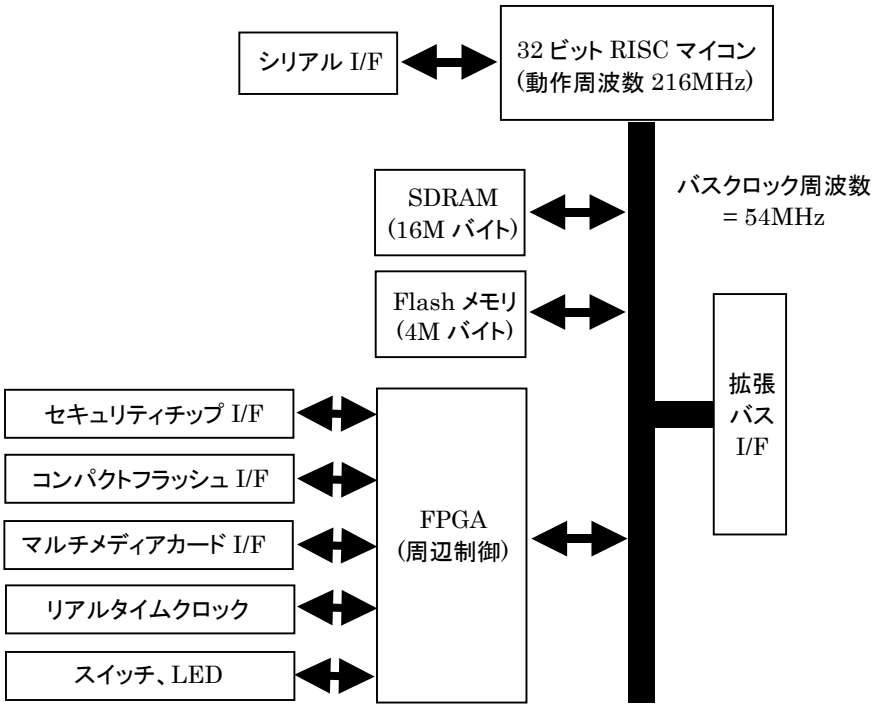



図 5.7.3-1: μU-Card CPU ボードブロック図

### （２）通信・センサ機能拡張ボード

- 通信機能
- 100Base-TX/10Base-T LAN インタフェースを搭載.
- UTP5 ケーブルの接続コネクタを実装.
- センサ機能
- CMOS イメージセンサ(画素数 160×144×RGB)を接続する
- インタフェースを搭載.
- 汎用制御/センサインタフェース
- 出力 8 ビット，入力 8 ビットの汎用ポートを搭載.
- 信号レベルは VLTTL(3.3 ボルト).

### （３）電源等の付属品

- AC アダプタ(5V)から CPU ボード用電源(3.3V)を生成する基板モジュール.
- デバッグ用コンソールに接続するためのシリアルケーブル.
- 専用筐体(実験で取り扱いが容易になるように準備).

## 3-2) 実験用ハードウエアの開発

平成１３年度の成果として，3-1) で述べた仕様の実験用ハードウエ

アを実際に開発した.基本機能の動作確認をはじめ,リアルタイム OS,ネットワークプロトコルソフトウエアを動作させて外部コンピュータと LAN 通信できること,また CMOS イメージセンサからの画像を取り出せることを確認している. 開発したボード写真を以下のとおり示す.


写真 5.7.3-1: CPU ボード(表面および裏面)

写真 5.7.3-2: 拡張ボード

## 5.8 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

このサブテーマは，本研究プロジェクトが多くの個別の成果を生み出したあとで，それらを連携，結合させ，トータルなユビキタスコンピューティング環境が構築可能かどうかを実際に検証することを目的としている．本年度は，まだ研究の立ち上げ段階であるため，まだ本サブテーマの研究作業は継続的に進めており，まとまった成果として報告する部分は来年度以降になる．

# 5.9 総括

平成 13 年度は，1 月 15 日より研究プロジェクトが開始し，当研究所の労力を多くを研究プロジェクトの始動のための諸準備に費やした．そうした環境化においても，当初の計画以上の多くの研究成果を生み出した．その内容の中心は，次年度以降，研究を本格化するために必要な基礎検討をや，研究開発環境の整備を進めた．今年度特に注力した研究項目を総括すると，次のようになる．

- **世界におけるユビキタスコンピューティング，ユビキタスネットワーキングの研究動向調査**
- **ユビキタス応用に向けた現実社会の計算機科学的モデル化**
  ユビキタスコンピューティングとは言い換えれば，現実世界の状況やコンテクストを計算機システムが認識し，それに応じて様々な動作をするメカニズムである．それが動作するためには，まず最初に，現実世界の状況やコンテクストがコンピュータ上で扱えるようにモデル化できなければ，それに応じた処理も行えない．そこで，本年度は，ユビキタス研究の最初にふさわしい，現実世界のいくつかの面に関してモデル化研究を行った．
- **ユビキタスコンピューティングの研究開発環境の研究開発**
  ユビキタスコンピューティング，ユビキタスネットワーキングは，90 年代における，パーソナルコンピューティング＋インターネットという計算機科学のスタイルと，大きく異なるものであり，その開発環境それ自体をも大きな研究分野を形成するものである．
- **ユビキタスコンピューティング環境の応用イメージの構築とニーズの明確化**
  既存の技術を用いて，tentative なユビキタス環境を構築して，運用することによって，今後我々が構築すべきユビキタス環境に求められるニーズや問題点を洗い出した
- ユビキタスプロトコルの基礎検討と実験
  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の核となる部分，特のルーティングやセキュアプロトコル部分に関しては，検討を開始し，一部試験的な実装やシミュレーションを実施した．

次年度以降は，本年度の成果を生かして，更にユビキタスコンピューティングのための基盤プロトコルの研究開発を推進していく所存である．

# 参考資料，参考文献

# （添付資料）
# １　研究発表，講演，文献等一覧

## 講演

121.　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.

## 報道

122.　日経新聞朝刊（3 月 28 日）
本研究所の設立について報道された.

※　本研究開発事業は，１月からの実施であるため，研究開発期間中の成果の公表する十分な期間がなかったため，本年度は記載すべき研究発表，講演等はあまりない.