無線LANとシームレス モバイルインターネット

太田　昌孝
東京工業大学情報理工学研究科
モバイルインターネットサービス（株）
mohta@necom830.hpcl.titech.ac.jp

無線（LAN）ネットワーク (ホットスポットサービス)

≠

モバイルインターネット

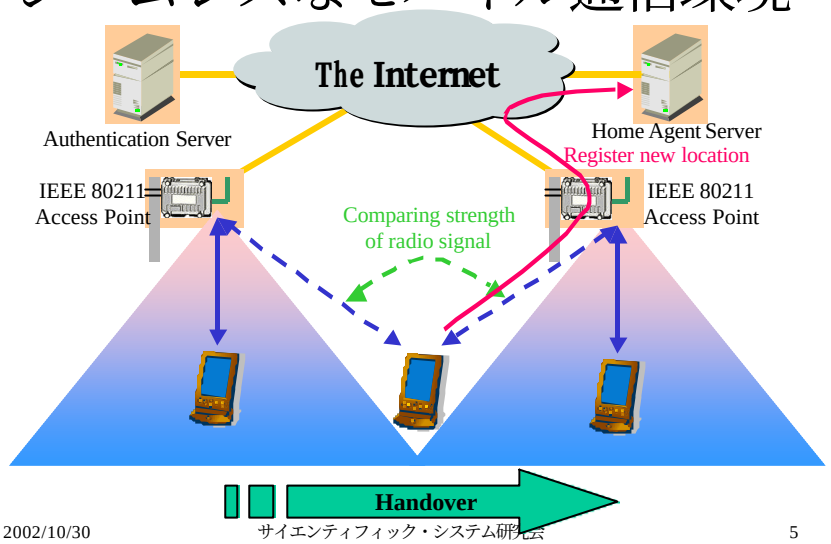
MIS（Mobile Internet Services, Inc.）とは？

- 2001年４月設立の移動体第一種電気通信事業者
- ２００２年4月より商用ブロードバンドモバイルインターネットサービスを提供中
- http://www.miserv.net

MISの モバイルインターネットサービス

- GENUINE（純正）と命名
  - 純正モバイルインターネット接続性を提供
    - 安くて速い
    - 時速１００Kmでも問題なくハンドオーバー
- エリア？
  - 東京で２５０局、京都で１５０局程度
- 端末？
  - 最近はPDA、デジカメにも対応

シームレスなモバイル通信環境

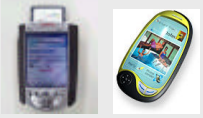


ビジネス展開イメージ

Phase1

User Interface

PDA to support wireless LAN



Mobile phones, Camera, Mp3 etc

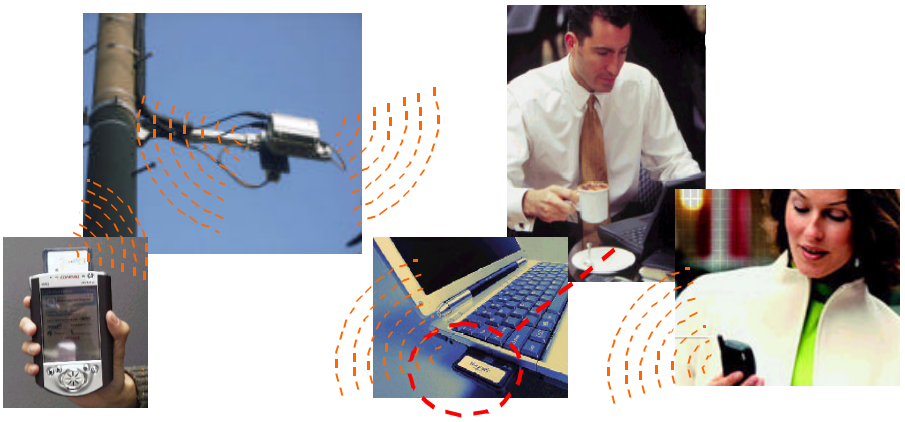
Service area

Hot spots including cafes, restaurants, airports, hotel lobbies etc.

Stop-off points, for example,at intersections, railroad stations and vending machines.

To support users in transit as possible.

サービスのイメージ



Users can access the service with their current handy devices.

次世代の情報通信インフラ

- 完全にインターネット化
  - 単なるプライベートIP網は無関係
- 完全に光化
  - 光ファイバーは極めて高速（10Tbps≫）
- しかし、人や車は光ファイバーにつながったままは移動できない
  - 携帯インターネット環境では電波利用は必須

「モバイル」「インターネット」とは？

- モバイル
  - 携帯性、いつでもどこでも
- インターネット
  - 世界最大規模の公衆ＩＰ網
  - 単なるIP網ではない

モバイルとは

- いつでもどこでもネットにつながっていること
  - エリアの広さが重要
  - 移動のたびの再接続の操作は不要
- いまどき、固定は光ファイバー

無線（LAN）ネットワーク

≠

モバイルインターネット

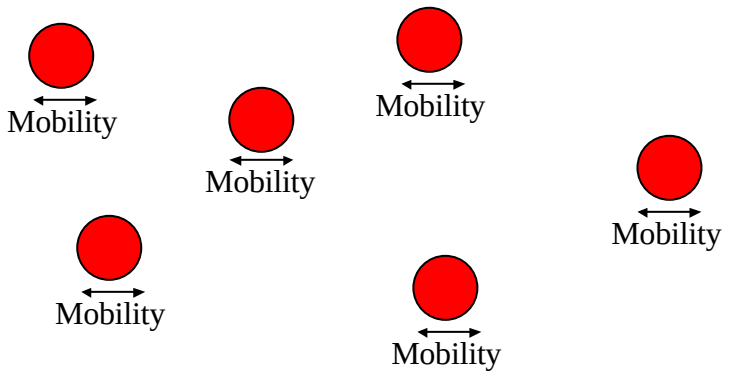
モバイルじゃないもの (1)
ホットスポット

- 無線！＝モバイル
  - 無線だけでは、同一基地局内での移動のみ
  - インフラモードでもせいぜい数十基地局程度
- ホットスポットは公衆電話程度のもの
  - 広域移動できない
  - 使うたびにログインが必要
    - ダイアルアップサービスでしかない

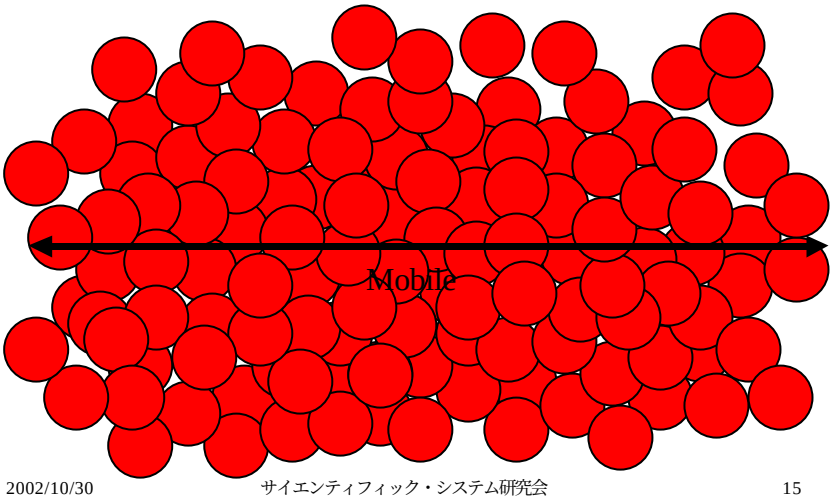
ホットスポットサービスとは？

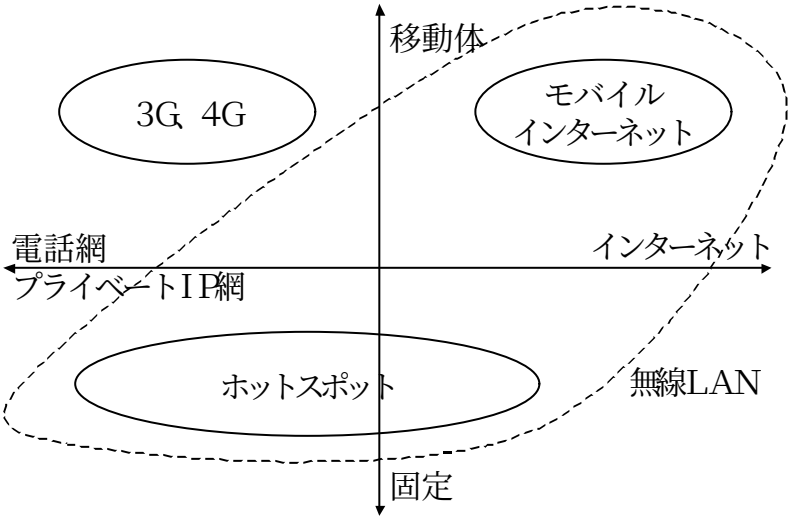
- そもそもはローミング事業者の無駄あがき
- ローミングはダイアルアップ時代の遺物
  - 常時接続環境の整備とともに消滅
- 電話網経由のダイアルアップは
  - 遅くて高くて低信頼性
  - ＡＤＳＬ網経由のダイアルアップも
    - 遅くて高くて低信頼性（RASがネック）
- ホットスポットもダイアルアップの一形態

ホットスポットサービス



モバイルインターネットサービス





ホットスポットサービスの将来は絶望的

- 基地局が増えてもモバイルへは移行不能
  - ダイアルアップサービスをいくらいじっても、常時接続環境への移行は不可能
  - 狭い地域内で事業者間ローミングは無意味
    - ローミングが成り立つのは従量制課金だから
      - 接続時間に応じた電話サービスには対応可能
      - インターネット常時接続には対応不可能
  - 802．1x等は重すぎ
    - 高速ハンドオーバーは不可能

モバイルじゃないもの (2) ノートパソコン

- 重い
- かさばる
- 歩きながら使えない
- 電源がもたない
  - 電源を有線接続するくらいなら、、、
- せめてＰＤＡなら
  - ウェブや電子メイルを使うなら我慢できる

インターネットとは？

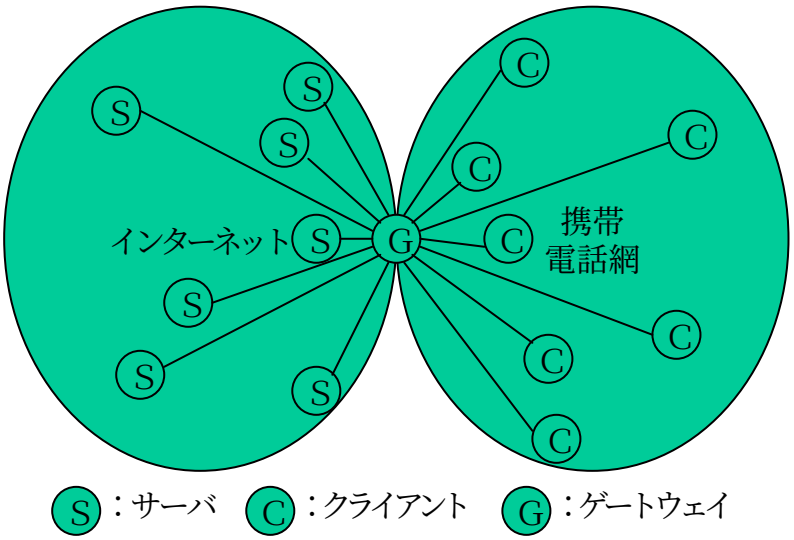
- 電子メイルのことではない
  - 数年前には大真面目で主張されていた
- ウェブのことでもない
  - 現在は勘違いしている人が多い
- インターネットはＩＰ（インターネットプロトコル）を用いて、インターネットの原理に基づいて相互接続された網である
  - IP網はかならずしもインターネットではないが

インターネットじゃないもの（1）電子メイル

- UUNET（JUNET）はインターネットではなかった
- パソコン通信もインターネットではなかった
- 電子メイルはインターネット上でも動くアプリケーションの一種
  - その他のネットワーク（電話網）上でも動く
- 昔の（海外）電子メイルは有料だった
  - 今でも携帯電話網上の電子メイルは有料

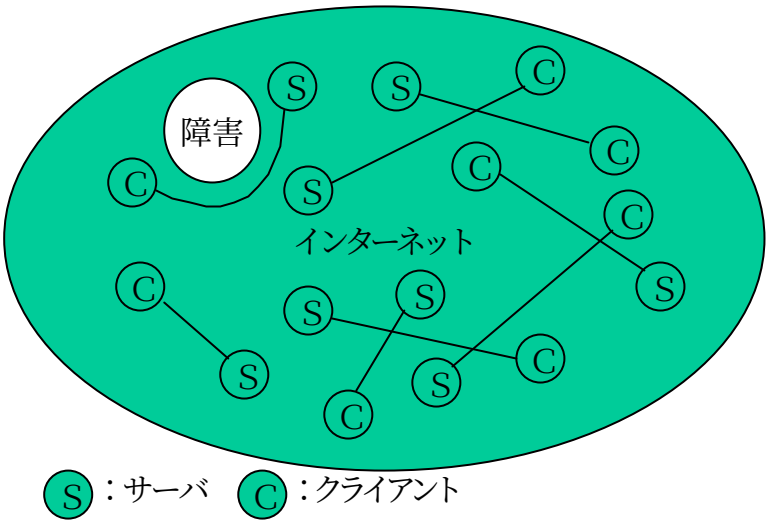
インターネットじゃないもの (2)
ウェブ

- ウェブはインターネットではない
  - マイクロソフトはそのへんを誤魔化しているが
- ウェブもインターネット上でも動くアプリケーションの一種
  - その他のネットワーク上でも動く
  - 携帯電話網からウェブを見るのは有料



S：サーバ C：クライアント G：ゲートウェイ

携帯電話網からのインターネットの利用
サーバとクライアントが分離されゲートウェイ経由で通信



インターネット
サーバとクライアントが混在して最短経路で通信

インターネットじゃないもの (3) 電話

- 電話は電話網ではない
- 電話は電話網上でも動くアプリケーション
  - その他のネットワーク上でも動く
  - インターネット電話自体は無料
- もはや電話はインターネットの販促ツール
  - わざわざそれ自体をサポートする価値なし
  - 携帯電話はモバイルインターネットの販促ツール

インターネットじゃないもの（4）電話網

- 電話は電話網ではない
- 電話は電話網上でも動くアプリケーション
  - その他のネットワーク上でも動く
  - インターネット電話自体は無料
- もはや電話網は不要
  - 携帯電話網も同じ
  - 電話番号も不要
    - ＩＰアドレスが基本（内線番号もあってもいい）

インターネットじゃないもの（5）ダイアルアップ

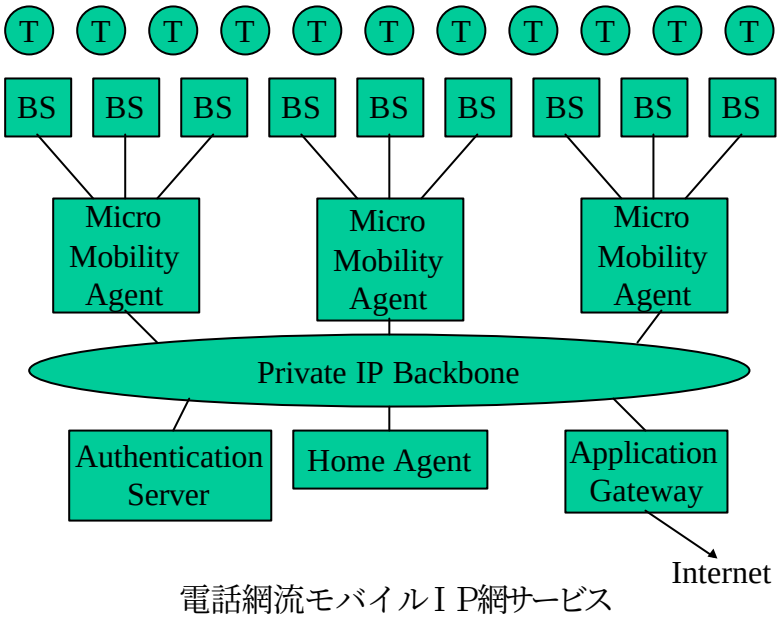
- インターネットじゃない網を前提に外から
  - インターネットを利用するのがダイアルアップ
    - 電話網経由のダイアルアップは常時接続でない
    - ＡＤＳＬ網経由のダイアルアップも常時接続でない
    - ホットスポットでのログインも常時接続でない
- （固定ＩＰアドレスによる）常時接続でないと
  - 情報発信できない
    - サーバが持てない、電話を着信できない

インターネットじゃないもの（6）プライベートIP網

- インターネットはIP技術により世界中の端末が直接接続された網
- 同じIP技術を利用しても
  - プライベートIP網はインターネットではない
    - 網構築コストは同じだが
    - 使い勝手は最悪（ネットワーク外部性がない）
    - インターネットとのゲートウェイは
      - 高い、遅い、耐障害性が低い
      - 携帯電話網とインターネット間のゲートウェイと同レベル

電話網流モバイル網

- プライベートIP網で全てを接続
  - インターネットにはゲートウェイで接続
- 一部でＱｏＳ保証
  - ただしエンドツーエンドな保証はない
- 網中の局所的サーバでマイクロモビリティーをサポート
- ２．5G、3G、4G等



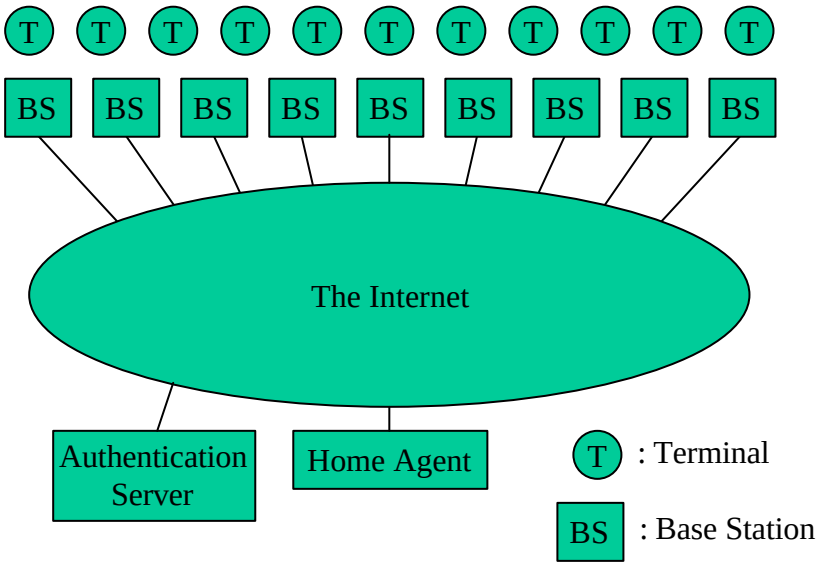
電話網流モバイルＩＰ網サービス

マイクロモビリティ？

- 電波による局所モビリティ
  - 電波
- ＩＰモビリティによる広域モビリティ
- マイクロモビリティによる中域モビリティ？
  - 遅延と広域制御トラフィックを減らす？
  - 不要
    - ＩＰモビリティは十分（1秒以下）速い
    - インターネットでは広域トラフィックは無料

インターネット流モバイル網
(ベストエフォートインターネットを活用)

- インターネットは全てを結合
  - プライベートIP網はムダ
    - 顧客がつなぎたい相手もインターネット内に存在
- 現在のインターネットはＱｏＳを保証しない
  - 経路の一部でのＱｏＳ保証は無意味
- インターネットでは電話（音声）すら無料
  - 制御パケット程度は無視できる



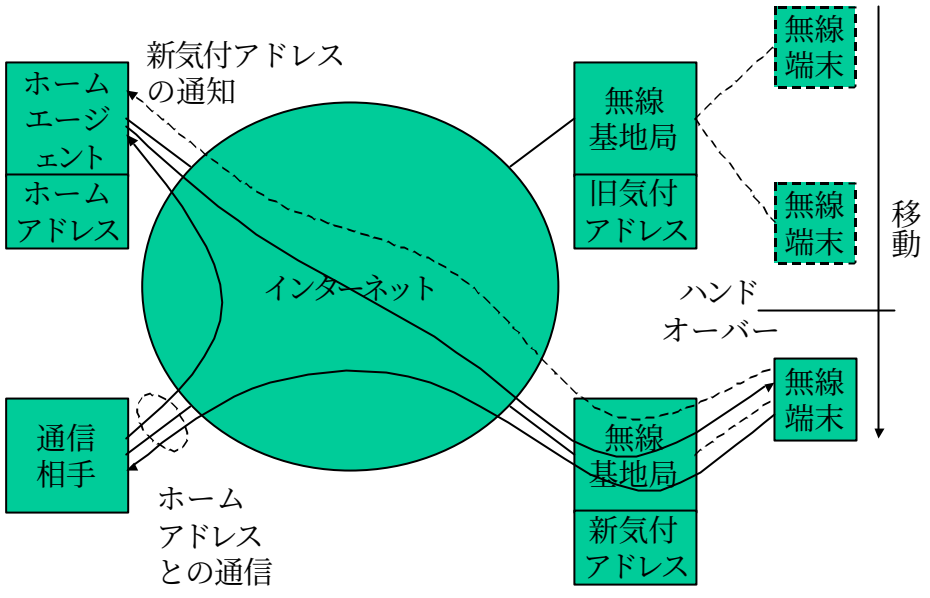
インターネット流モバイルＩＰ網サービス

モバイルインターネットサービスのために

- 高速低額常時接続定額の固定インターネットに接続した安価な無線機を密に配置
  - 高速低額常時接続定額の無線インターネット
- IP mobilityとの組み合わせで携帯インターネットに
- 無線区間のセキュリティには一工夫必要

IP Mobility (RFC2002)

- 端末が移動しても、同じＩＰアドレスを使い続けたい
  - ＴＣＰ接続なども維持
- ４つの要素
  - ホームエージェント： モバイルIPのサーバ
  - モバイルホスト： 移動端末
  - フォーリンエージェント： MISでは端末と同居
  - コレスポンデントホスト： 通信相手



モバイルＩＰ技術

商用ＩＳＰとIPモビリティの間をつなぐ技術

- 安価な無線技術
  - ＩEEE 802.11b
- 安価な有線技術
  - ＡＤＳＬ／ケーブル／イーサネットによるFTTH
- 軽い認証技術
  - WEPやIEEE802.1xは論外

ＩEEE802．11bと その他の無線LAN技術？

- ＩEEE802．11bは
  - 2．4GHzを利用し、一般的な都市環境で１００m程度の距離で１１Mbpsの通信が可能
  - モバイル利用に最適
- １１Mbｐｓより速いと距離が伸びない
  - より多数の基地局が必要で採算性が低下
- ５GHｚは直進性が強すぎて不適
  - モバイル環境では使えない

干渉？

- 無線ＬＡＮでは電波が干渉するので、同じ地点で数局しか運用できない？
  - 回線交換屋の与太話
- イーサネットでも、干渉は同じ
  - 同時の送信を抑えれば問題なし
    - ＣSMA／CD、ＣSMA／CA

無線サービスには認証は必須

- 誰でも無線リンクにはパケットを送れる
- 顧客から以外のパケットはインターネットに中継しないようにしないと
  - だれもお金を払わない
- 犯罪捜査のためにも利用者特定は必要
  - 誘拐犯からの匿名の連絡
  - 初期のプリペイドカード携帯の匿名利用
  - ＳＰＡＭのばらまき

2002/10/30 サイエンティフィック・システム研究会 39

認証（Authenticaion）技術

- ダイアルアップ感覚の認証は無意味
  - 電話網等が、電話番号等で相手を特定
  - 電話網等が、ログイン後の割り込みを防ぐ
- 無線ではログイン後も他人が割り込める
    - パケット単位の認証が必須
  - 端末による基地局の認証も必要
- ＩＥＥＥ 802.1x
  - 遅い、重い、そのままではセキュアでない

2002/10/30 サイエンティフィック・システム研究会 40

IEEE802.1xの歴史

- WLANのセキュリティ問題の存在は自明
  - IEEE802.11にはWEP (Wired Equivalent Privary)というセキュリティ機能あり
- WEPのセキュリティ問題が発表されたが
  - ベンダー側は無視
- airsnoutという自動攻撃ツールを公開
- やっとIEEE802.1x (IEEE802.11i)の開発が開発される

2002/10/30 サイエンティフィック・システム研究会 41

IEEE802.1xは「公衆」「モバイル」環境では使い物にならない

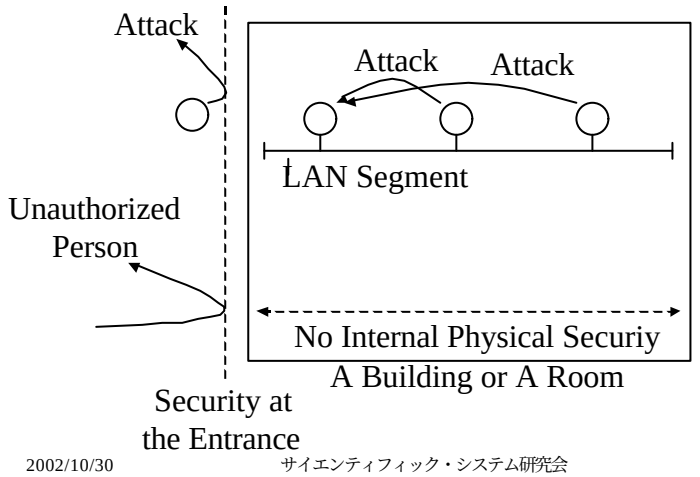
- IEEE802委員会は本来LAN規格の委員会
  - 最近こそWANでのイーサネット利用も考慮
- 802.1xはLAN環境が前提
  - 公衆による利用は考えてない
    - セキュリティモデルが脆弱
  - 高速移動のことは考えてない
    - 通信開始まで十回程度のパケット交換が必要

2002/10/30 サイエンティフィック・システム研究会 42

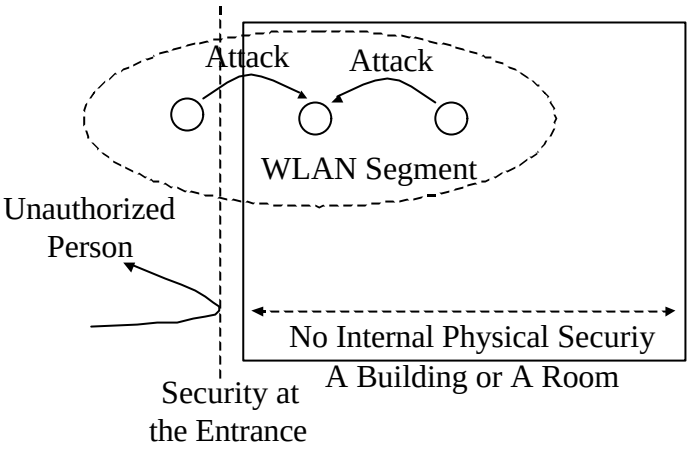
IEEE802．1xのセキュリティの目標

- Make WLAN secure as **private** LAN
  - 公衆サービスの場合は？
- “All authenticated end stations on the local access Bridge are protected from non-authenticated end stations”
  - Authenticated end stationsからの攻撃は？
  - Attacks from brides to end stationsは？

プライベート有線LANのセキュリティ

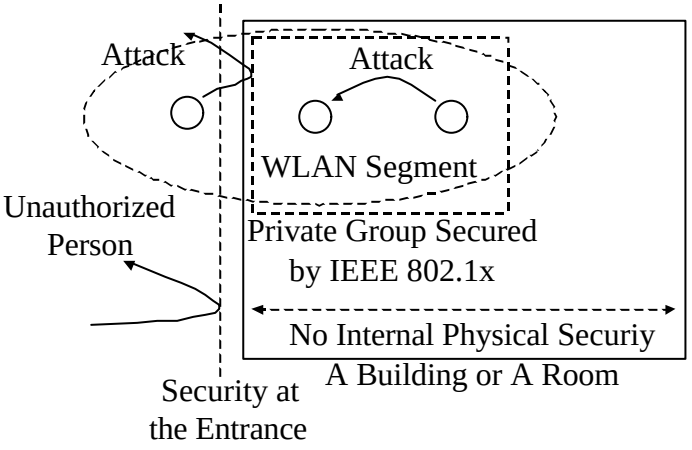


プライベート無線LANのセキュリティの欠如



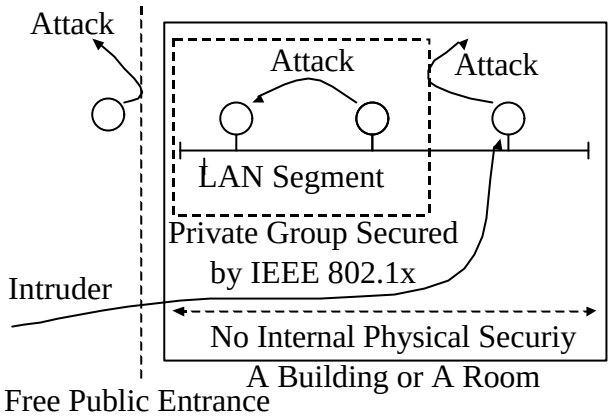
2002/10/30 サイエンティフィック・システム研究会 45

IEEE802．1xによるプライベート無線LANのセキュリティ？



2002/10/30 サイエンティフィック・システム研究会 46

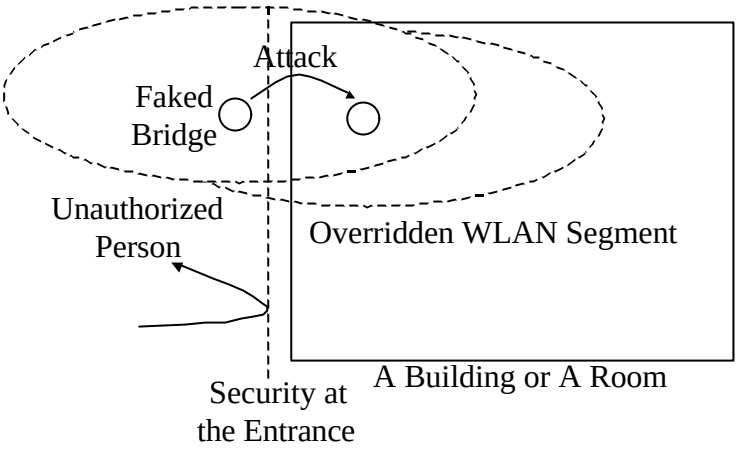
IEEE802.1xによる公衆エリアでのセキュリティ？



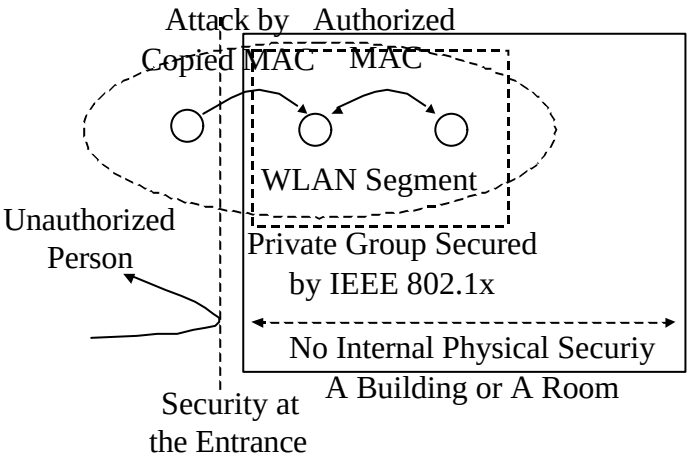
IEEE802.1xは そもそもセキュアではない

- 電話網によるダイアルアップの発想
- 電話網の場合
  - ダイアルした相手につながる
    - 偽基地局問題の心配はない
  - 相手との通信中に他者が割り込めない
    - 通信開始時だけ相手を認証すればよい
- 無線の場合
  - 近くにいる誰とでもいつでも通信可能

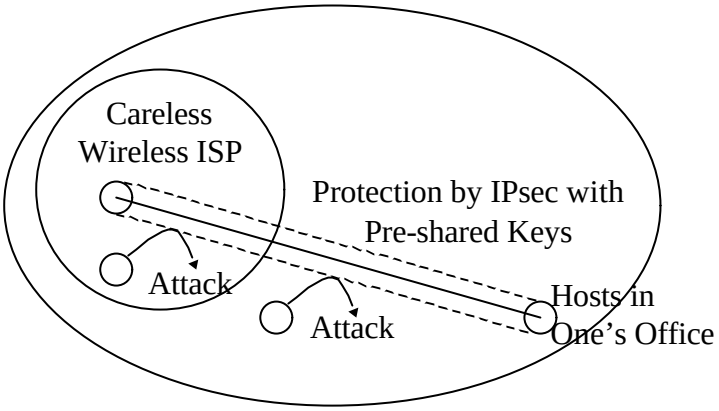
偽基地局によるセキュリティの欠如



ログイン時認証し、以後はそのMACアドレスと通信すると

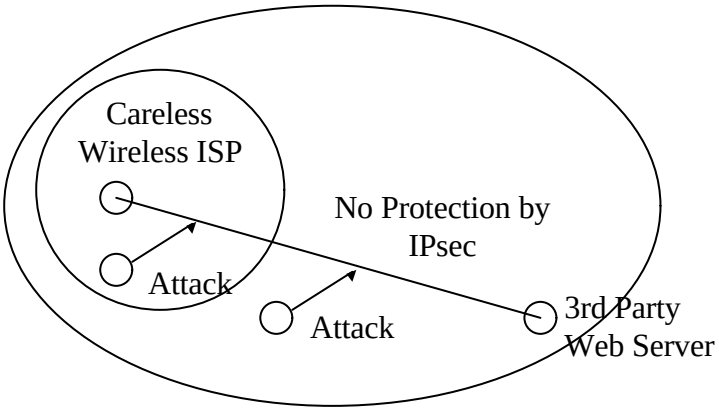


IPsec (VPN) による防衛？



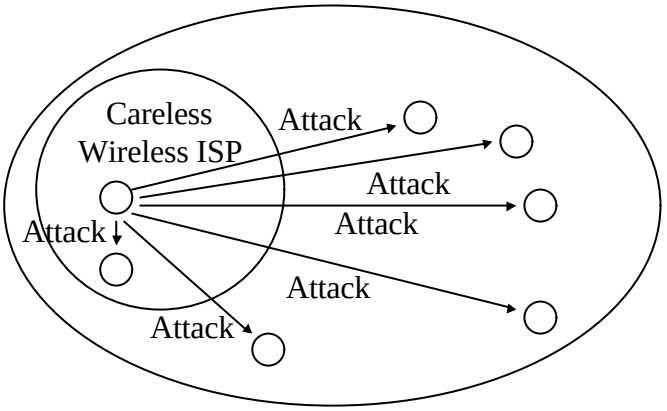
2002/10/30 サイエンティフィック・システム研究会 51

IPsec は公衆環境では役に立たない (1)



2002/10/30 サイエンティフィック・システム研究会 52

IPsecは公衆環境では役に立たない(2)



IEEE802.1xは、モバイル利用には致命的に遅い

- 認証だけで最低７回のパケット交換が必要
  - いわゆるホットスポット環境では他に
    - ＰＰＰｏＥによるセッション確立
    - ＩＰアドレスの割り当て
    - より複雑なセキュリティのための情報交換

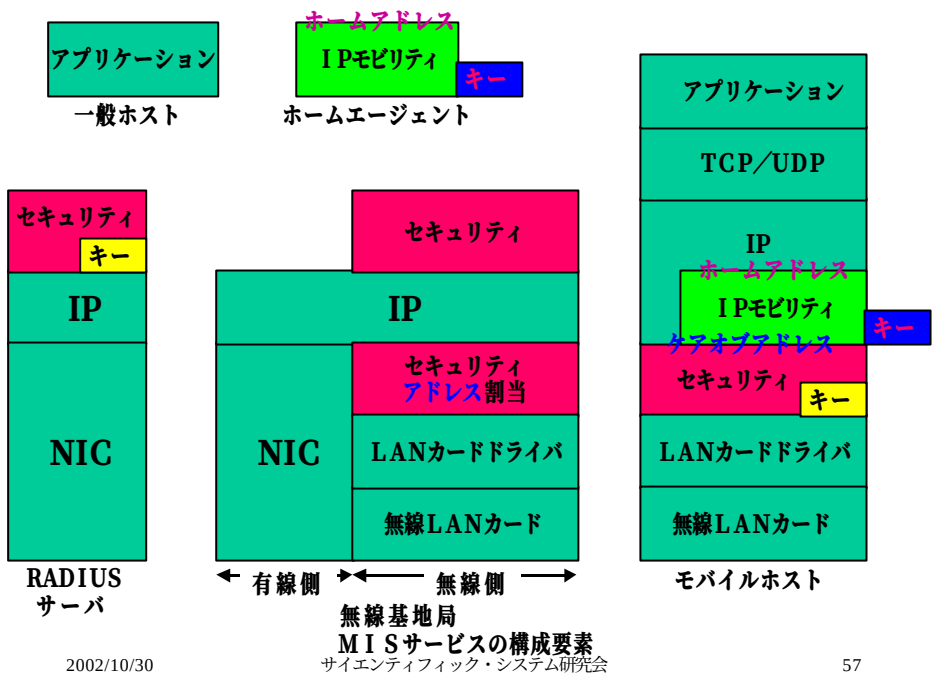
  等で、さらに数回のパケット交換が必要
- 途中でパケットが一回でも落ちると
  - タイムアウト待ち（数秒？）が発生

MISP (MIS Protocol)

- モバイルIPの商用化のために
  - 「まともな認証」を「高速」に行う
    - ログイン時等に秘密鍵を共有
    - 以後のパケットはMD５で相互に認証
    - すべての情報交換を１回（半）のパケット往復で
  - オプションでＡＥＳによる秘匿も提供

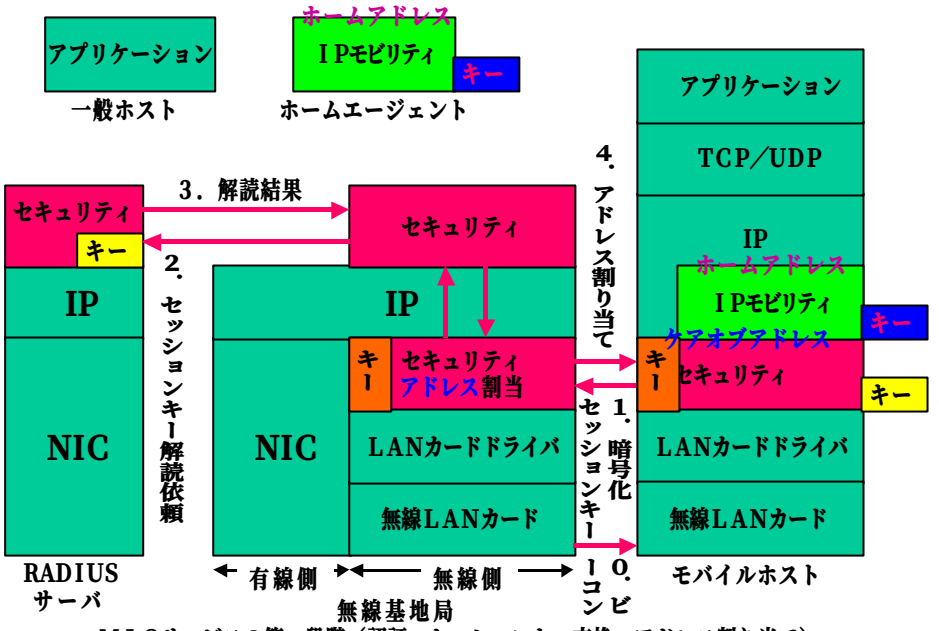
MISPの詳細

- 基地局は定期的にビーコンを送出
  - 自己の存在とその能力を広告
- 端末は最良の基地局に登録を試みる
- ＡＡＡサーバの介在により端末と基地局は互いを認証しセッション鍵を交換
- 基地局は端末に局所ＩＰアドレス（ケアオブアドレス）を割当てる

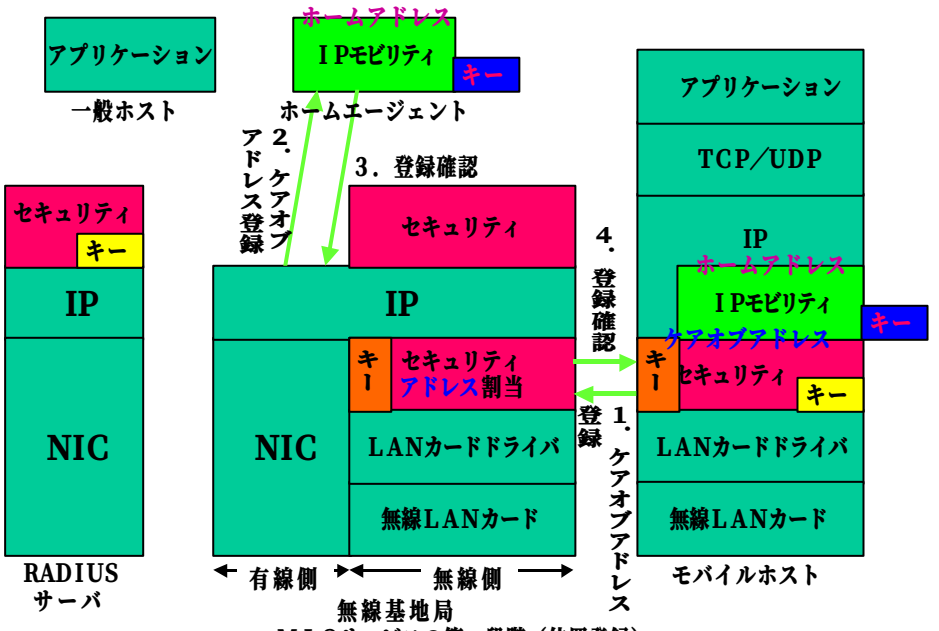


MISサービスの認証、セッションキー交換、アドレス割り当て

- モバイルホストはセッションキーを生成
- ユーザごとのキーで暗号化して無線基地局に転送
- 無線基地局はＲＡDIUSサーバに解読依頼
- 無線基地局とモバイルホストはセッションキーを共有
- 無線基地局はケアオブアドレスを割り当て



MISサービスの第一段階（認証、セッションキー交換、アドレス割り当て）

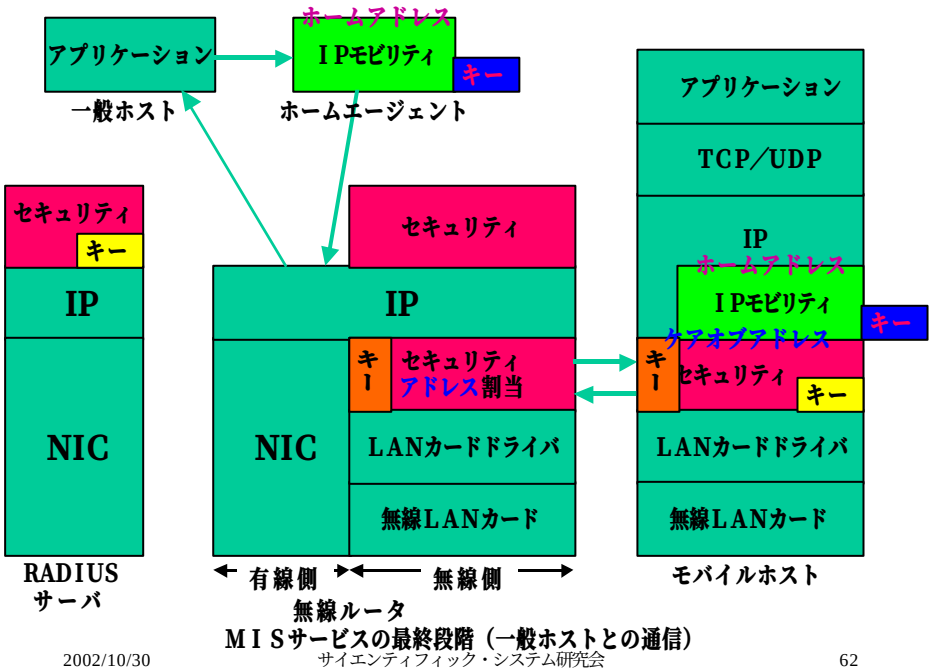


MISサービスの第二段階（位置登録）

パケット単位の通行許可

- 暗号技術による端末認証後、どのパケットをインターネットへ通すか？
  - MACアドレス見るだけではセキュリティ皆無
    - MACとＩＰアドレスは誰でもコピーできる
  - パケット単位での暗号技術による認証は必須
    - パケット単位での暗号化も望ましい
    - ＭＩＳＰはMD５とAESを利用
    - 基地局と端末はセッションキーを共有

2002/10/30 サイエンティフィック・システム研究会 61



2002/10/30 サイエンティフィック・システム研究会 62

高速ハンドオーバー

- 無線により基地局内の移動が可能に
- 基地局間の移動が
  - ハンドオーバー
- ハンドオーバーには時間がかかる
  - 新たな基地局を探すための遅れ
  - 新たな基地局との相互認証のための遅れ
  - モバイルIPの位置登録のための遅れ
- 高速ハンドオーバーのため遅れを最小化

ハンドオーバーが遅いと

- 高速移動できない
  - 新たな基地局とのハンドオーバー完了前にその基地局と通信できなくなる
- 通信が途絶する
  - ウェブ閲覧やメイル受信なら問題ない
    - TCPによる再送
  - VoIPでは音声が途切れる
    - 再送したのでは、遅れが大きくなりすぎる

ハンドオーバーの遅れ

- 新たな基地局を探すための遅れ
  - 無線ＬＡＮでは１～十数秒
- 新たな基地局との相互認証のための遅れ
  - インターネットでは０．１～１秒程度
    - ＩＥＥＥ８０２．１x等を使うとさらに遅れる
- モバイルＩＰの位置登録のための遅れ
  - インターネットでは０．１～１秒程度

2002/10/30 サイエンティフィック・システム研究会 65

IETFの高速ハンドオーバーへの対応

- 基地局が連携して認証を引継ぎ
  - 新たな基地局との相互認証の遅れを減らす？
- 基地局と端末が連携して
  - モバイルＩＰの位置登録の遅れを減らす？
- あらたな基地局を探す時間が減らないとほとんど意味がない
  - 携帯電話事業者とホットスポット事業者の机上の空論

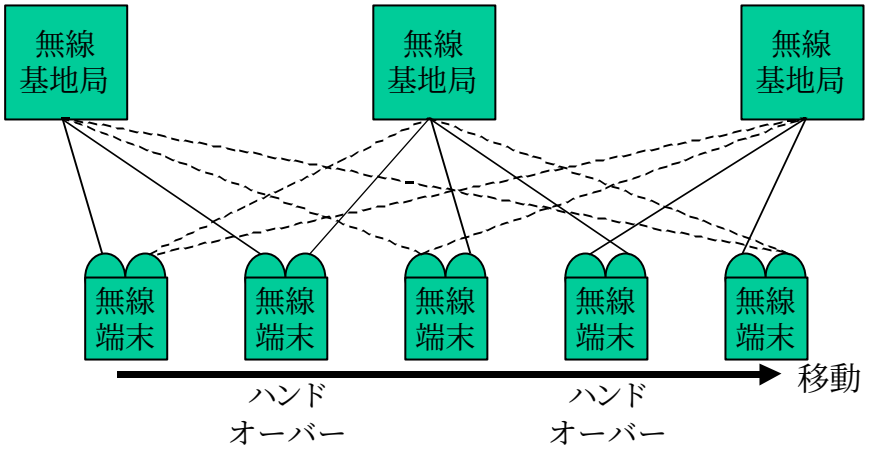
2002/10/30 サイエンティフィック・システム研究会 66

ＭＩＳの高速ハンドオーバーへの対応

- 基地局を探す部分を高速化
  - 無線LAN独自のモビリティ機構（インフラストラクチャモード）は、移動への対応が遅い
  - アドホックモードも遅い
  - モバイルIPのみを擬似アドホックモードで利用
- １秒程度でのハンドオーバーが可能に
- ＭＩＳPの認証も高速
- １００Km／Hの車でハンドオーバーを確認

スムーズなハンドオーバー

- ハンドオーバー時の通信中断は不可避？
- ＰＨＳ同様、端末が２波同時利用可なら
  - 旧基地局に接続したまま
    - 新基地局候補を探せる
    - 新基地局と相互認証し接続できる
  - 新旧基地局に接続したまま
    - モバイルＩＰの位置登録が可能
  - ハンドオーバーによるサービス中断は皆無



———：無線基地局との接続

-------：ハンドオーバー候補の探索

２台の送受信装置によるスムーズハンドオーバー

モバイルインターネット上のアプリケーション

- 既存のアプリは全てそのまま動作
  - もちろん無料のインターネット電話も
- ＭＩＳの取り組む事業ではない
  - 位置依存コンテンツ提供サービスだけは例外
- 位置依存コンテンツはMIＳの基地局に収納される
  - コンテンツ提供業者は利用基地局の数に応じて課金される

端末の例：ノートパソコン

- 電源が欲しい
- 歩きながら使えない
- ホットスポットで使うなら問題なし
- モバイル環境ではほとんど意味なし
- ウェブや電子メイルなら
  - ＰDAで十分

端末の例：インターネットデジカメ

- 携帯情報機器は常時ネット接続したい
- デジカメを携帯電話やＰＨＳでネット接続？
  - メモリー残量を気にせず撮影可能
  - 実時間で画像を公開できる
  - まともな解像度では莫大なパケット課金
  - ナローバンドでは、転送に莫大な時間
- ＭＩＳ（定額ブロードバンド）なら問題なし
  - オープンソースを元に三洋電機が開発

地域展開ー『コミュニティ・パートナー』

地域事業者と連携し、地域展開を推進。

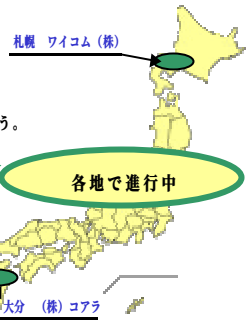
MIS

ＭＩＳAuｔｈ、HA、基地局ファーム、ドライバの情報を開示、指導。
基地局の稼動状況の監視、障害の検知、通知は、ＭＩＳが一括して行う。

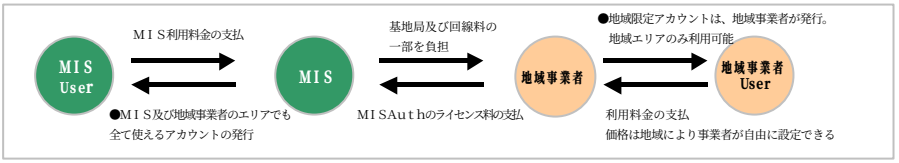
コミュニティ・パートナー

基地局の購入、設置工事、ＨAの設置。
基地局のメンテナンス、故障時の現場での対応。

地域事業者設置基地局にＭＩＳ Userがアクセスした場合、プロキシにて利用可能にする。



福岡ＩＭＳ　大分ネットピアッツア



【地域限定アカウントの顧客がＭＩＳアカウントに移行する場合】
■MISアカウントを地域事業者に卸売りし、地域事業者が顧客に再販。

2002/10/30　サイエンティフィック・システム研究会　73

IPv6実証実験

京都がモバイルブロードバンドシティに変貌中

TAO（通信・放送機構）委託研究開発事業として、京都のNPO、大学、民間企業、行政の協力のもと実証実験を開始。京都府一円に150ヶ所の基地局を設置、日本最大規模の実験に。

《京都府下》

宇治市内、舞鶴市内、福知山市内、宮津市内、綾部市内、綾野町内、峰山町内、精華町内、木津町内、・・・・・・・

《京都市内》

京都駅、京都タワービル、高台寺、円徳院、鴨川西岸、四条大橋、五条大橋、京都全日空ホテル、京都大学、龍谷大学、国立京都国際会館、国際日本文化研究センター、京都国際交流会館、京都リサーチパーク、京都市観光協会館観光情報センター、井筒八ツ橋本舗北座ビル、ぱるるプラザ京都、ホテル不二家、ホテル秀峰閣　他・・・・。

2002/10/30　サイエンティフィック・システム研究会　74

大学等への技術供与-『アカデミック・パートナー』

学内ネットワーク設備として、MIS方式の無線ネットワーク構築を希望される大学等へ技術供与。

名古屋大学

京都大学

和歌山大学

《今後の予定》

山口大学

イベント等への技術供与

●2002年7月 (横浜) 第54回 IETF国際会議へ協力予定。

●2002年1月 (富山) 日本ネットワーク・オペレーターズ・グループ (JANOG) 主催のJANOG9ミーティングに、機材・技術協力。

2002/10/30 サイエンティフィック・システム研究会 75

コンソーシアム

『モバイルブロードバンド協会』

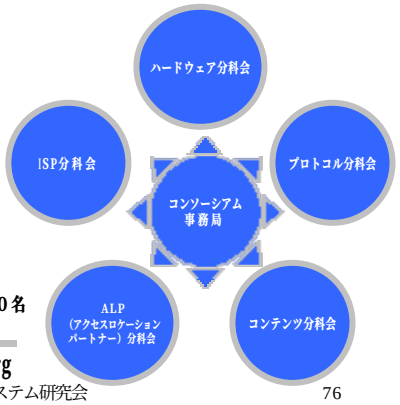
モバイルブロードバンドの円滑かつ効率的な研究開発・標準化活動を進める為に、関係者が一体となって、研究開発や標準化に関する情報交換を行うとともに、具体的な推進を図ります。

・2001年8月29日設立

・理事長 後藤 滋樹
（早稲田大学 理工学部 教授）

・会員数：88

- 法人56社（海外3社）、賛助会員2団体、個人30名
（2002年4月15日現在）



ご入会は随時受付中 http://www.mbassoc.org

2002/10/30 サイエンティフィック・システム研究会 76

結論

- ブロードバンドモバイルインターネットは
  - ＩＰモビリティ技術
  - ＩEEE 802．11b技術
  - ＭＩＳＰの高速認証技術
  - インターネット自体

  の組み合わせによって実現される
- スムーズハンドオーバーもＩPv6も簡単