公衆無線インターネットサービスのセキュリティモデル

岡部　寿男
（京都大学学術情報メディアセンター）

背景：
公衆無線インターネットアクセスサービスの現状

- IEEE802.11b/g 無線LANの急速な普及
  - ノート型PCのほとんどに標準装備
  - セキュリティの甘さで社会問題化
- 公衆無線インターネットアクセス
  - 無線LAN技術を利用した公衆インターネットサービス
    - いわゆる『ホットスポット』
    - メディアが注目
  - 米国では
    - Mobile Starの倒産
  - 日本では
    - 有料サービスの苦戦
      - MIS社の廃業
      - BBモバイル…無料試験サービス
      - NTT系サービスの乱立

HOTSPOT (NTTcom)
Mzone (NTT DoCoMo)
無線LAN倶楽部(NTT-BP)
ネオモバイル(NTT-ME)
フレッツ・スポット（NTT西・東）
Mフレッツ（NTT東）

公衆無線インターネットアクセスサービスのビジネスモデルの困難

- カバーエリアの問題
  - 公共スペース（駅・空港・ホテル）では事業者が競合
    - IEEE802.11b/gのチャネル数の制限
  - 喫茶店などでは一つの事業者のみ
    - その事業者と契約しているユーザだけが利用可能
  - 都心部中心、郊外・地方都市ではわずか
    （例）**無線スポット検索サイト** http://dokoyo.jp による最寄り駅検索
    - 大手町（東京）…81件、淀屋橋（大阪）…26件
    - 和歌山（和歌山）…5件、園田（兵庫）…1件、豊岡（兵庫）…0件
- 料金体系の問題
  - 割高感
    （例）HOTSPOT（NTTcom）
    - 月額固定 1,600円、1日利用500円
  - 事業者により携帯電話並みに使えるようにするには莫大な資本投下が必要

シーズ指向はPHSでも失敗

みあこネット (MIAKO.net)

Mobile Internet Access in KyotO

主旨に賛同した基地局オーナー、会員などによる
「街中公衆無線インターネットサービス」実験プロジェクト

- 主旨:
  自らの手で自分達の都市に公衆無線インターネットの仕組みを作り上げ情報自由都市にしよう！
  みあこネットを普及させることで多くの人を街に引き込み、街を活性化させていきたい
- 実行主体:NPO法人日本サスティナブル・コミュニティ・センター(SCCJ)
- 協力団体・企業　:京都大学、(財)京都高度技術研究所など
- 規格　:IEEE802.11b　2.4GHz
- アクセスポイント数　:19都道府県に300局(2003年11月
- アカウント登録者数　:延べ約7000人
- 実験期間　:2002年5月～2005年3月末

ビジネスモデルを継続的に模索中…

みあこネットのとりくみ

通信事業者ビジネスモデル

「客間の亭主」モデル
（グリーンレンタルの感覚）

来客への「おもてなし」に、客間・生け花・お茶などがあるように、会議室にプロジェクタ、プリンタ付のホワイトボード、観葉植物などがあるように、
「公衆無線インターネット」が、今後はオフィスの必需品。家庭の必需品。

→ユビキタスネットワーク環境の実現モデル

無料のサービスは可能か？

- 実は、インフラはすでにある
  - ほとんどのオフィス・商店・家庭がブロードバンド化
    - ADSL (1～10Mbps) ⇒光ファイバ (100Mbps～1Gbps)
- 第三者への提供の可能性
  - 帯域はほとんど空いている
  - 無線で提供すれば手間はかからない
- 問題はセキュリティ
  - 見ず知らずの人にネットワークを貸すことのリスク
    - 内部ネットワークからの隔離（セキュリティポリシー）
    - 外部への不正アクセス等

公衆無線インターネットアクセスにおけるセキュリティ

- 利用者にとって
  - 盗聴・改竄、MIM (man-in-the-middle)攻撃の防止
  - なりすましの防止
    - 不当な嫌疑をかけられないこと
- 基地局設置者にとって
  - 有料サービスの場合、課金できること
    - ただ乗りの防止、重複利用の制限
  - 利用者を特定できること
    - プロバイダ責任制限法上の**発信者特定責任**
      - クラッキング、ウイルス散布、SPAMメール大量送信
      - 掲示板書き込み、コンテンツ配信
    - 発信者を特定できないと設置者が民事上の責任

公衆無線インターネットアクセスサービスのセキュリティモデル

- セキュリティモデルの分類
  - 従来のサービス
    - 事業者型（有料サービス）
    - 自営型（無料サービス可能だがセキュアでない）
  - 我々の提案
    - 自律分散型（無料サービス可能かつ安全）
- インターネットアクセスサービスにおける**発信者特定**とは？
  - インターネット：IPパケットによる通信

⇒通信相手に届いたIPパケットの送信元アドレス(source IP address)からそのパケットの真の発信者を特定できること

  - 通常のインターネットアクセスサービスでは
    - 通信事業者は、有線をたどることで利用者を特定できる
  - 公衆無線インターネットアクセスサービスでは
    - **認証手順**を経て利用を許可することで利用者を特定

無線「LAN」の認証・暗号技術と公衆無線サービスでの問題

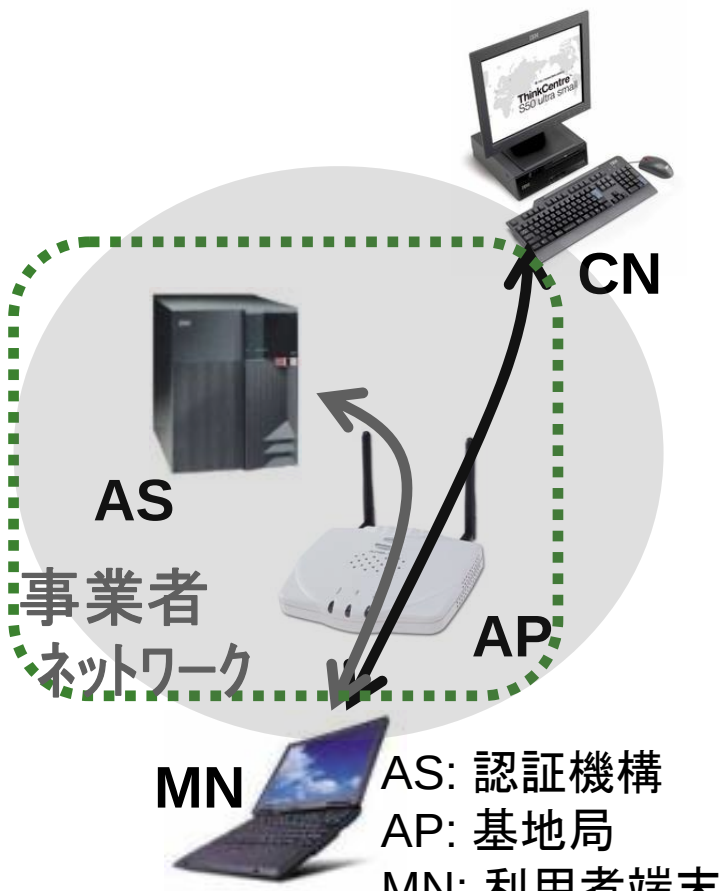
- MACフィルタリング(認証)
  - 容易に偽装可能
- WEP (暗号化)
  - 共有鍵の事前配布
  - 全利用者で同じ鍵を使用
- WPA (認証・暗号化)
  - IEEE802.1x
    - アカウント＋パスワードまたはPKIによる認証
  - 利用者グループごとに異なる鍵

「公衆」無線インターネットには適用できない

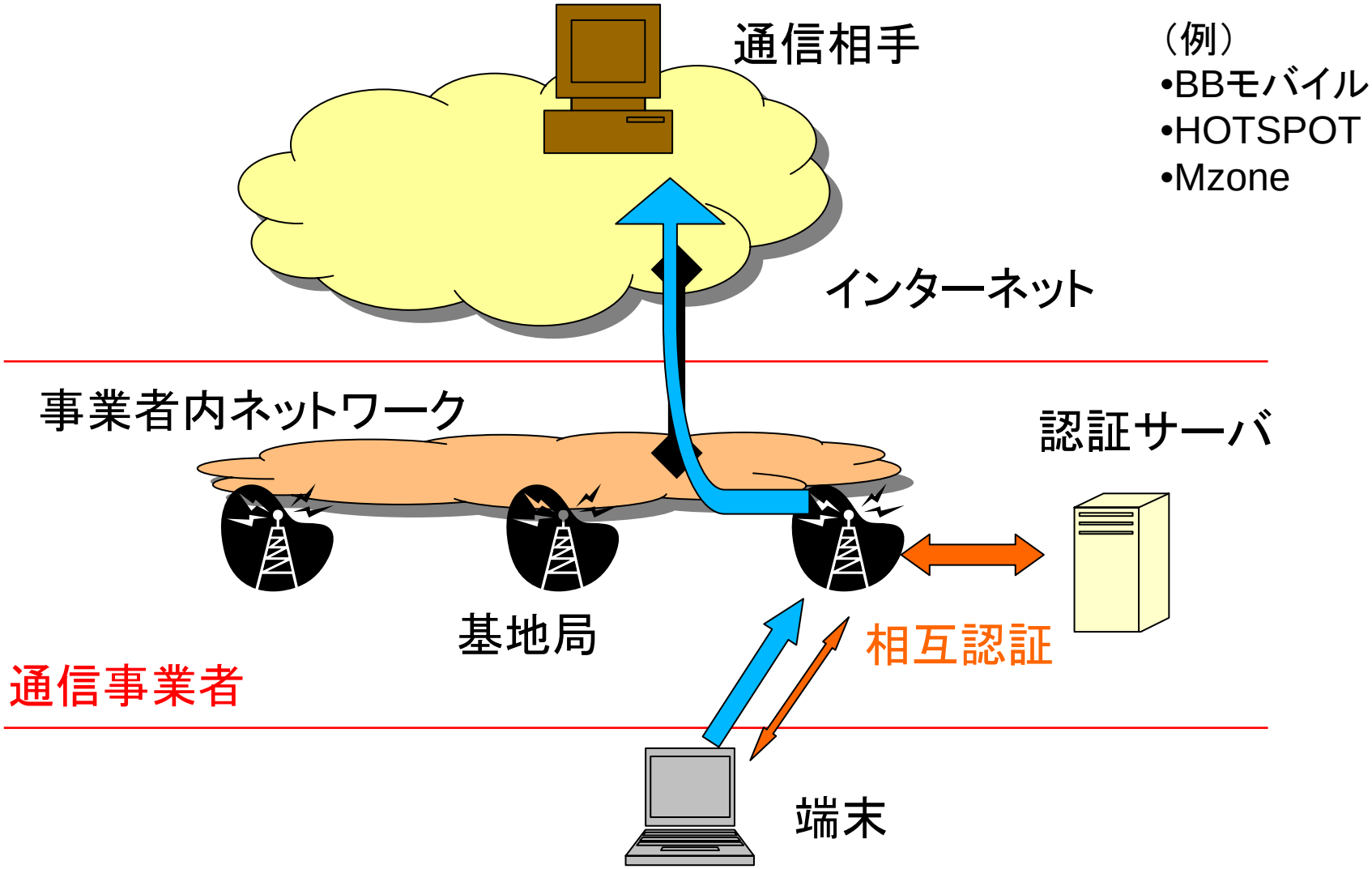
無線区間
（無線基地局ー利用者端末）
のみの暗号化

事業者型公衆無線インターネット

- 特徴
  - 事業者による集中管理
    - アクセス線、無線基地局の所有
    - アカウント管理 (認証機構提供)
  - 利用者が事業者を信用するモデル
- 問題点
  - 当該事業者と利用者の間で契約関係が必要
    - 事前のアカウント取得が必要
    - 有効期限付きの場合も

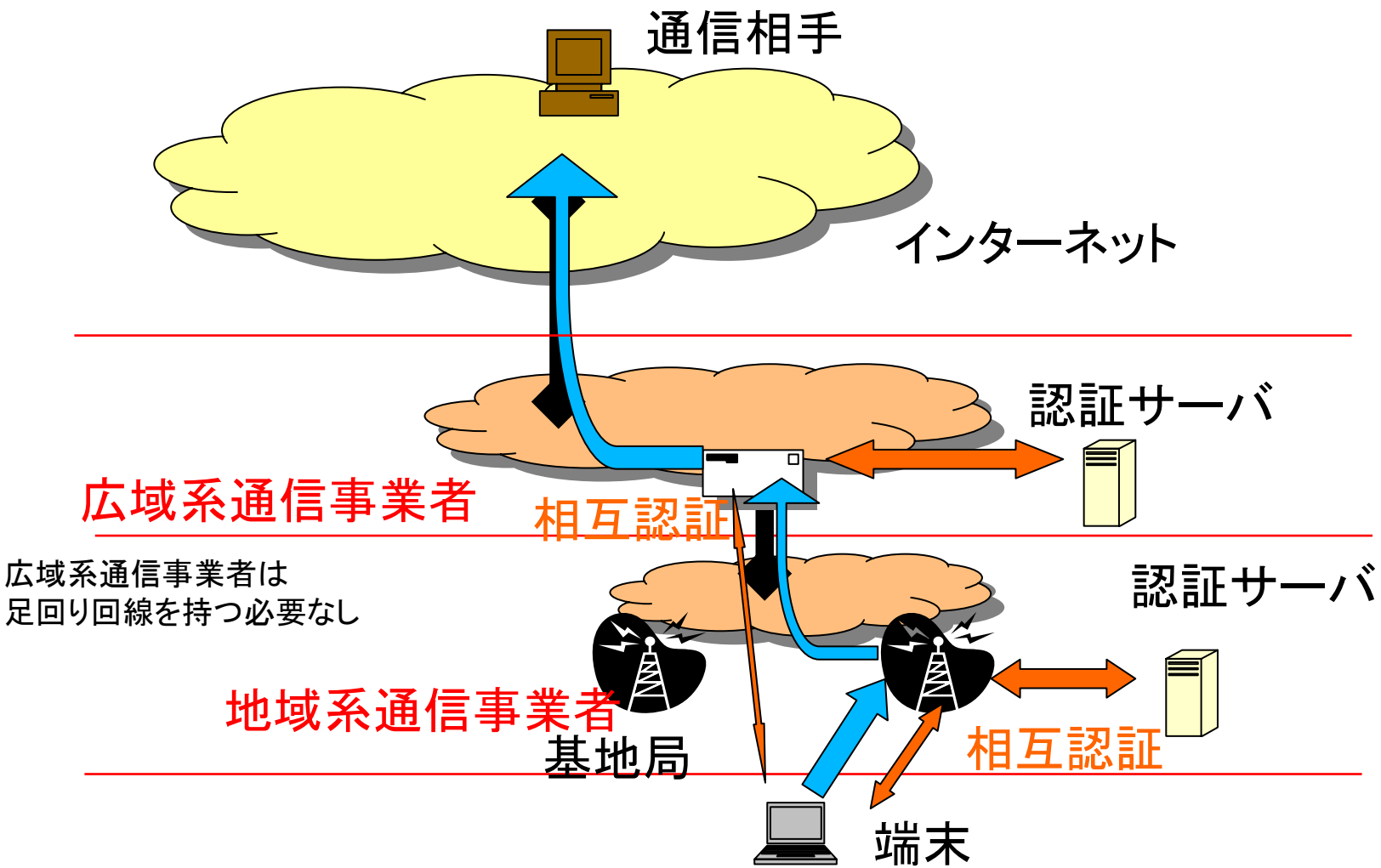


事業者型(1)　単一事業者による運営



事業者内ネットワークをサービスエリア全域で構築する必要あり

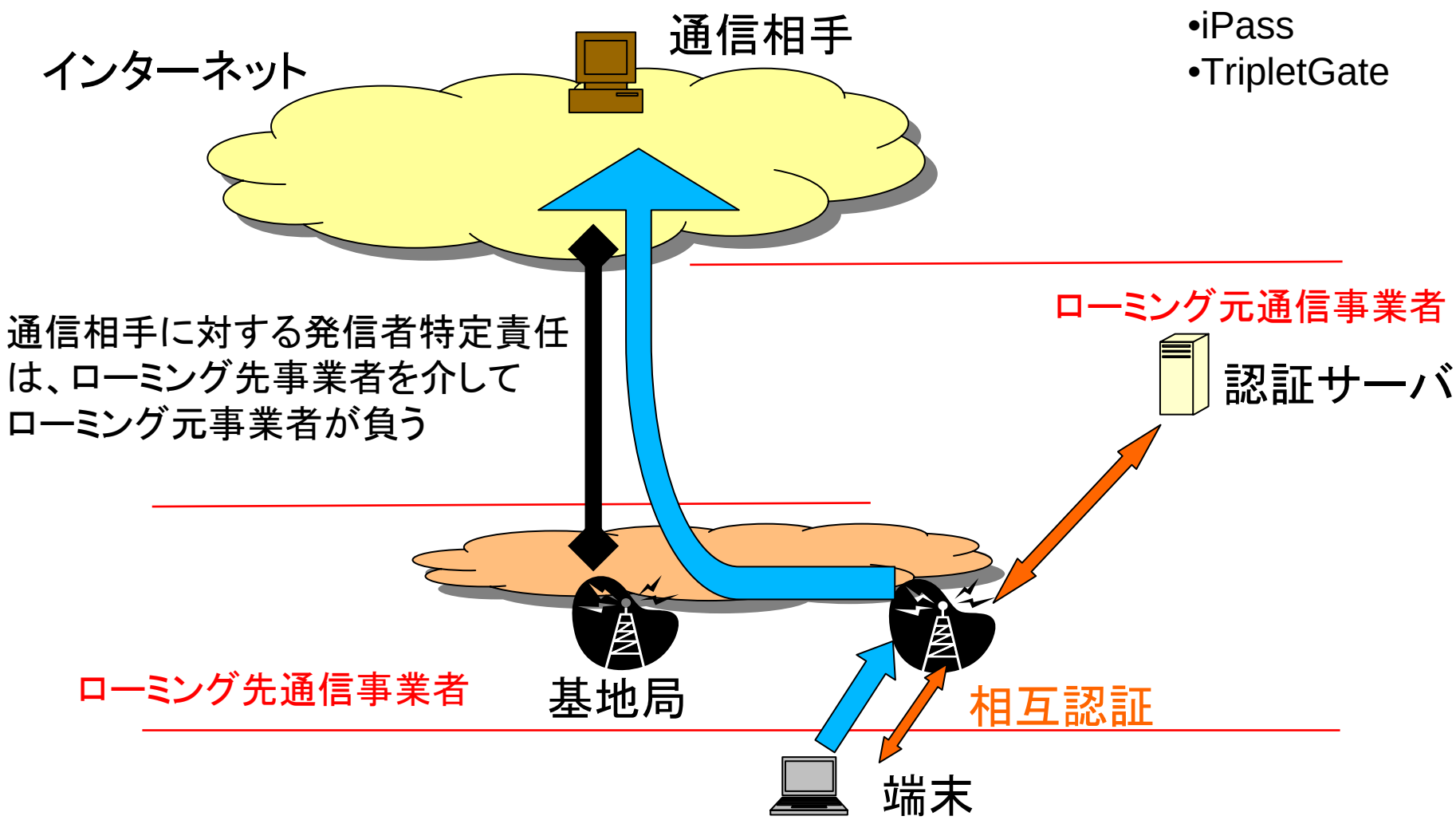
事業者型(2)　NTT フレッツ・スポット



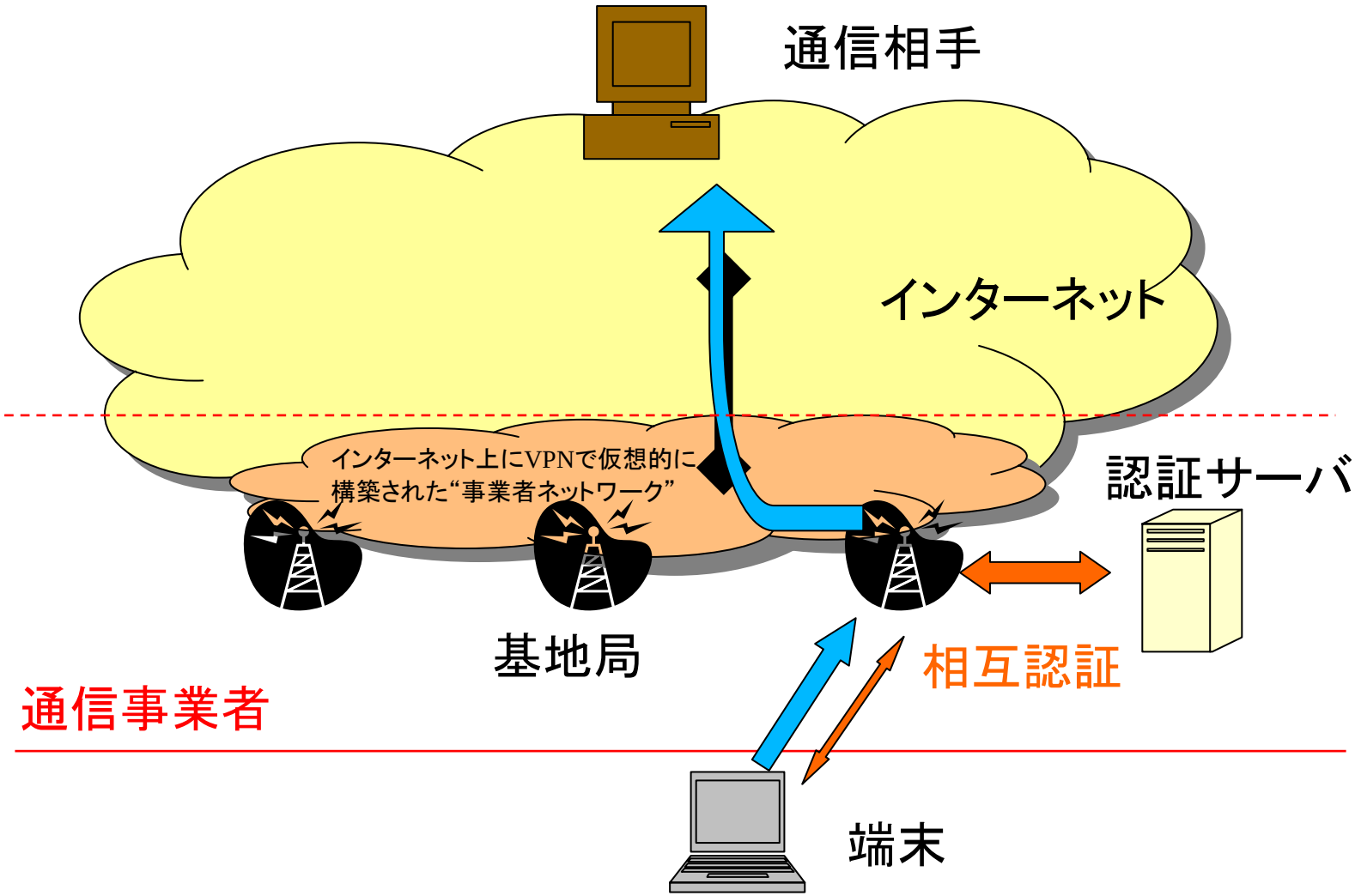
通信相手に対する発信者特定責任は、広域系通信事業者が負う

事業者間ローミング

（例）
•iPass
•TripletGate



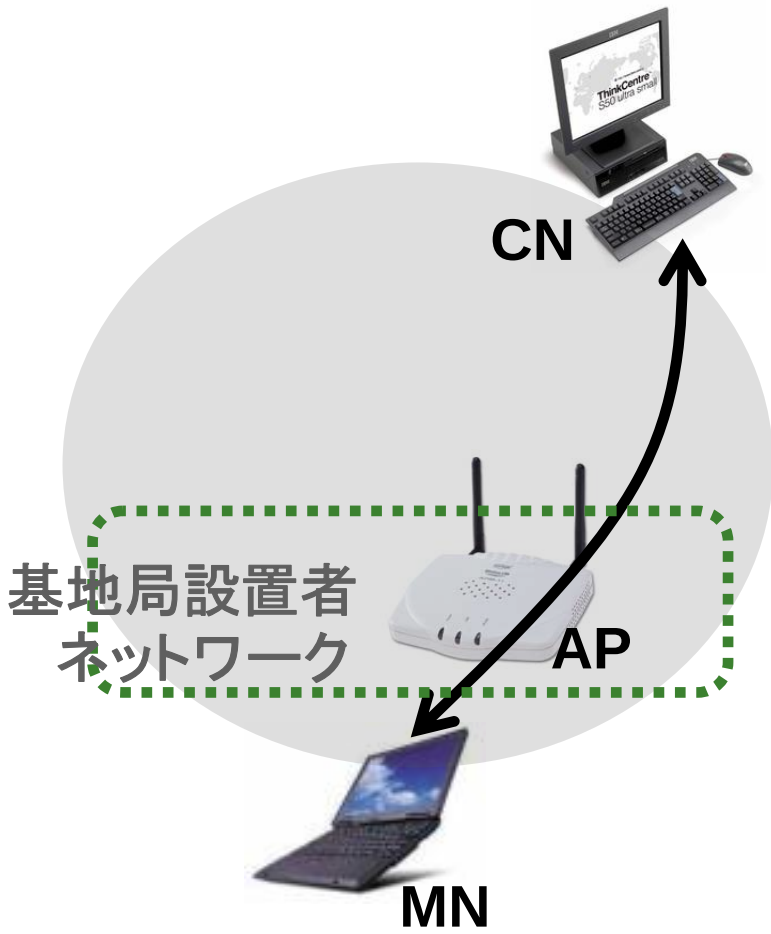
事業者型(4) MIAKO2(みあこネット)



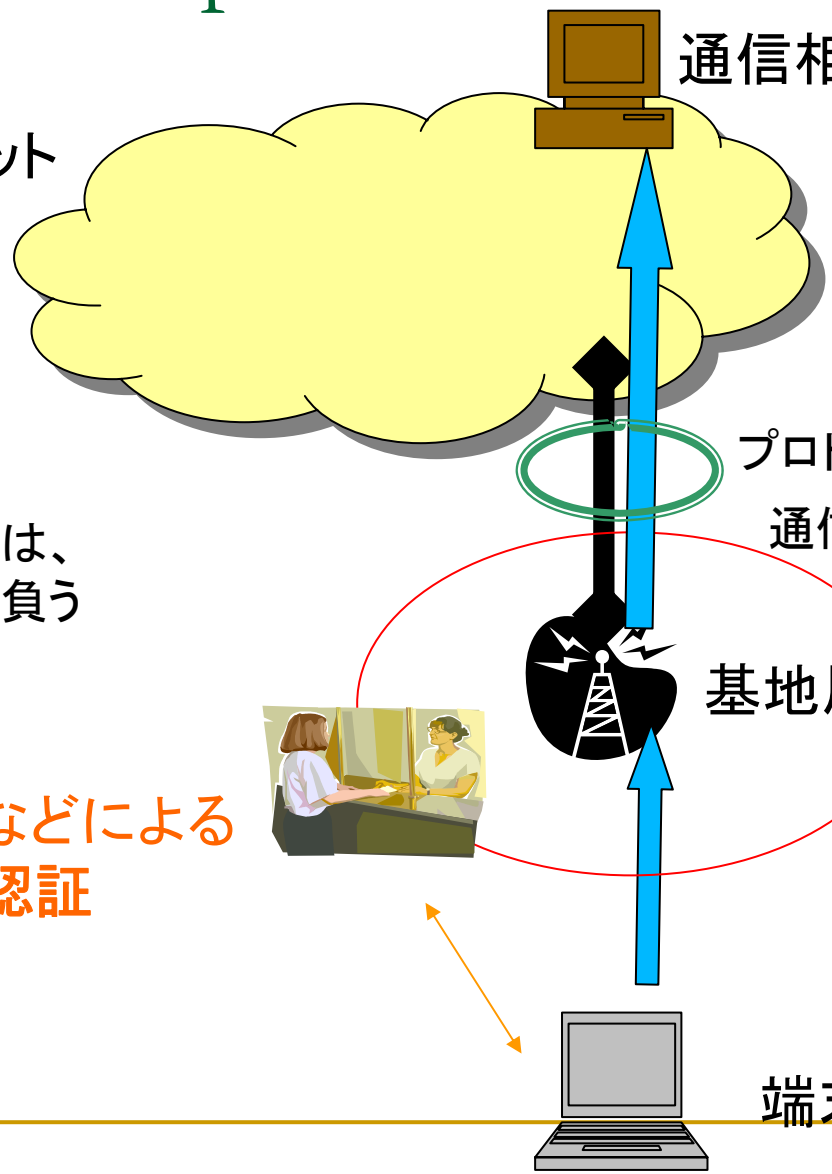
単一事業者による運営と論理的には同等

自営型公衆無線インターネット

- 特徴
  - １台～数台の基地局で独立に運用
    - 運用コストは低い
  - 個々のセキュリティポリシー
  - 草の根的な展開が容易
- 問題点
  - 発信者特定が可能なレベルのセキュリティの確保は困難
  - 基地局設置者が悪意をもった場合の問題



自営型　FreeSpot　（無料サービス）

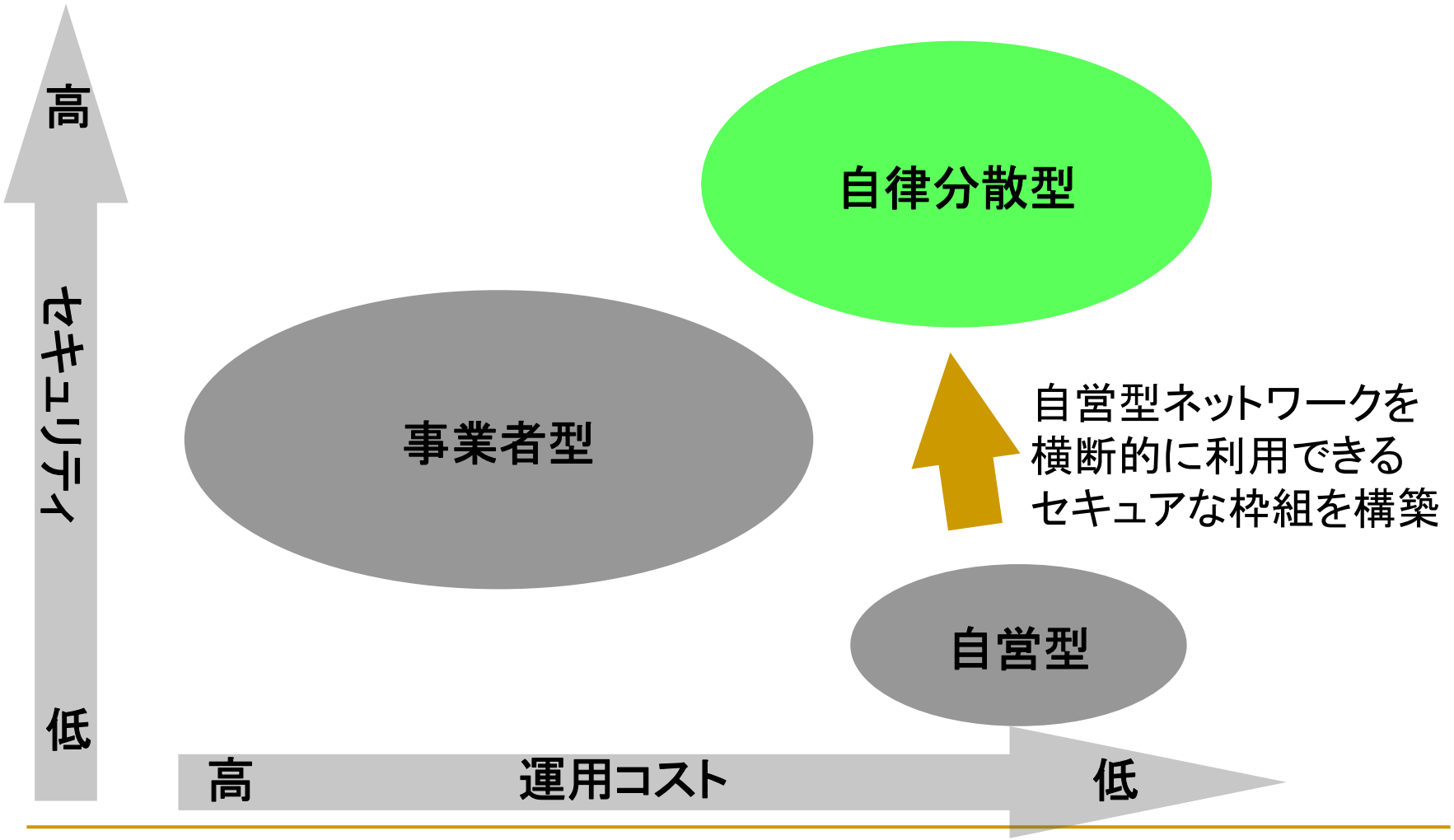


不正なパケットを受信した場合、基地局設置者と利用者とどちらが悪いと言えるか？

発信者特定責任は、
基地局設置者が負う

面談などによる
簡易認証

公衆無線インターネットの比較



自律分散型公衆無線インターネット

- 設計目標
  - 発信者特定に関して、通常の有線インターネットアクセスサービスと同程度のセキュリティ
    - 通信相手はIPアドレスをもとに責任を問える
  - 認証機構と基地局設置者を分離
    - 認証機構の運用者と基地局設置者は別
      - 両者の間の信頼関係を仮定しない
    - 基地局設置者が悪意を持っていても、利用者と認証機構運用者の間に信頼関係があれば不正が行えない

⇒発信者特定責任は、認証機構運用者が直接負う仕組み

- 不正利用があっても基地局設置者は責任を問われない

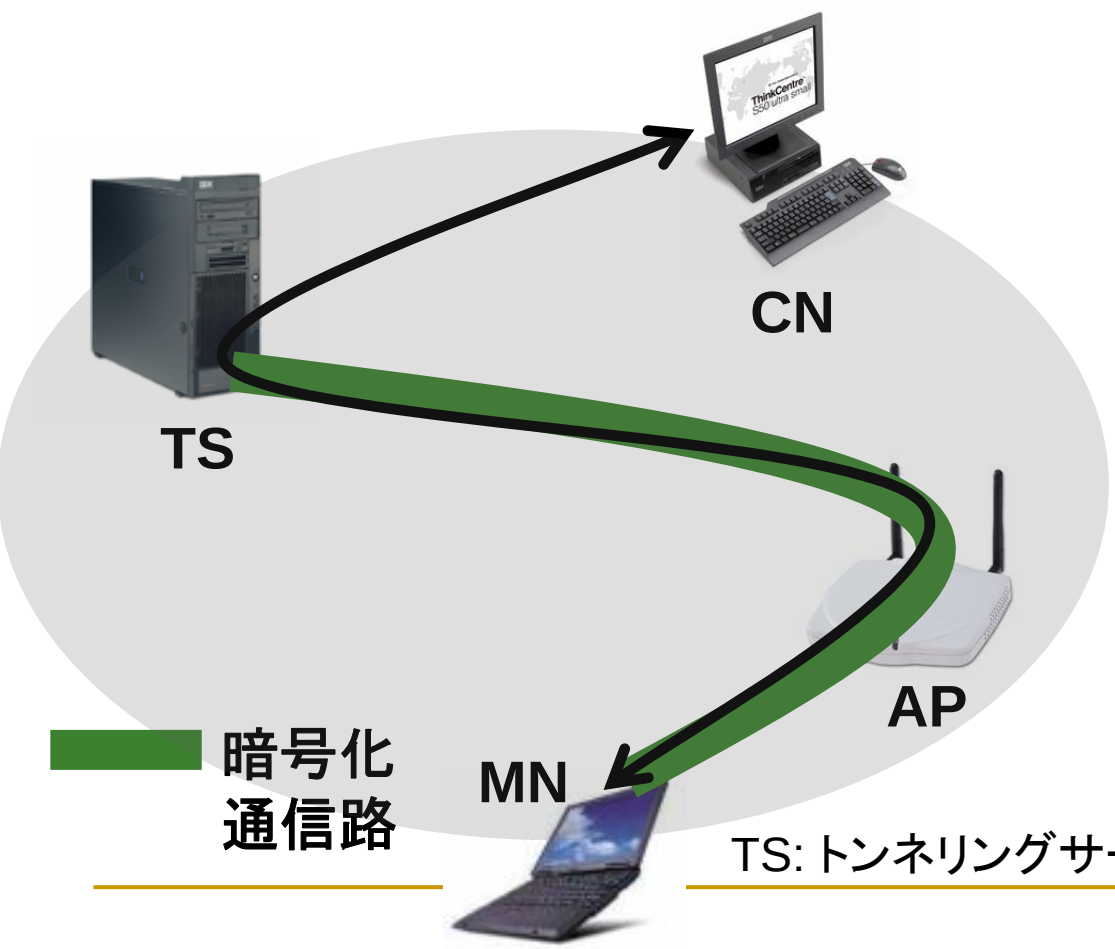
自律分散型公衆無線インターネット

- “自律”
  - 認証基盤と基地局設置者との間の信頼関係は仮定しない
- “分散”
  - 認証基盤と基地局はインターネット上に分散配置

- 運用コスト
  - 基地局設置者は認証に関して考慮しなくてよい
- セキュリティ
  - 有線インターネットと同程度に発信者特定が可能

提案方式(1) 基地局認証なしトンネリング方式

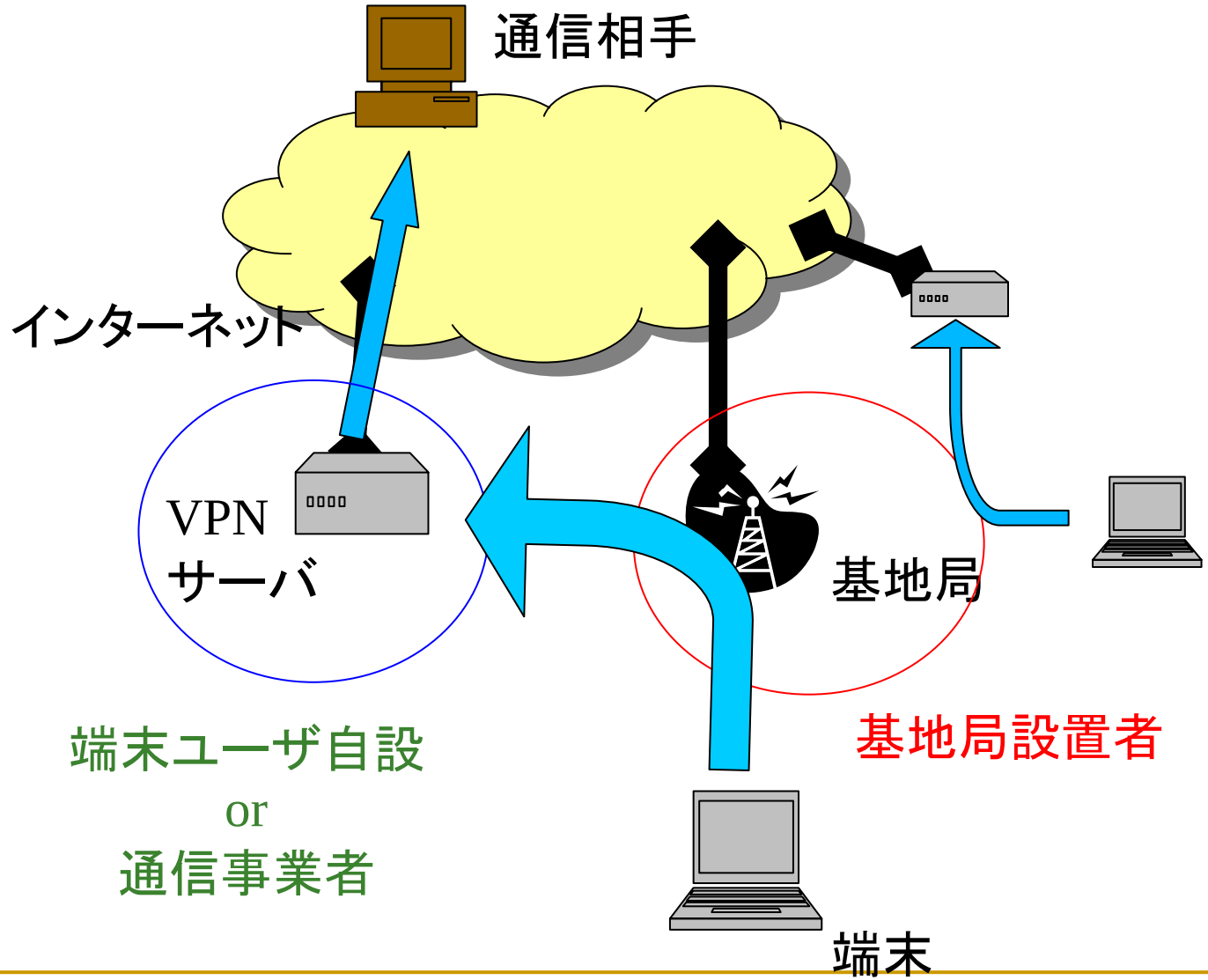
『みあこネット方式』



- 全通信はトンネリングサーバ経由
- TS-MN間はVPN
  - AP設置者による盗聴・改竄・なりすましはできない
- 基地局は、特定のVPNプロトコルによる通信のみを許すプロトコル制限
  - 認証されていない端末からインターネットへの直接のアクセスを禁止

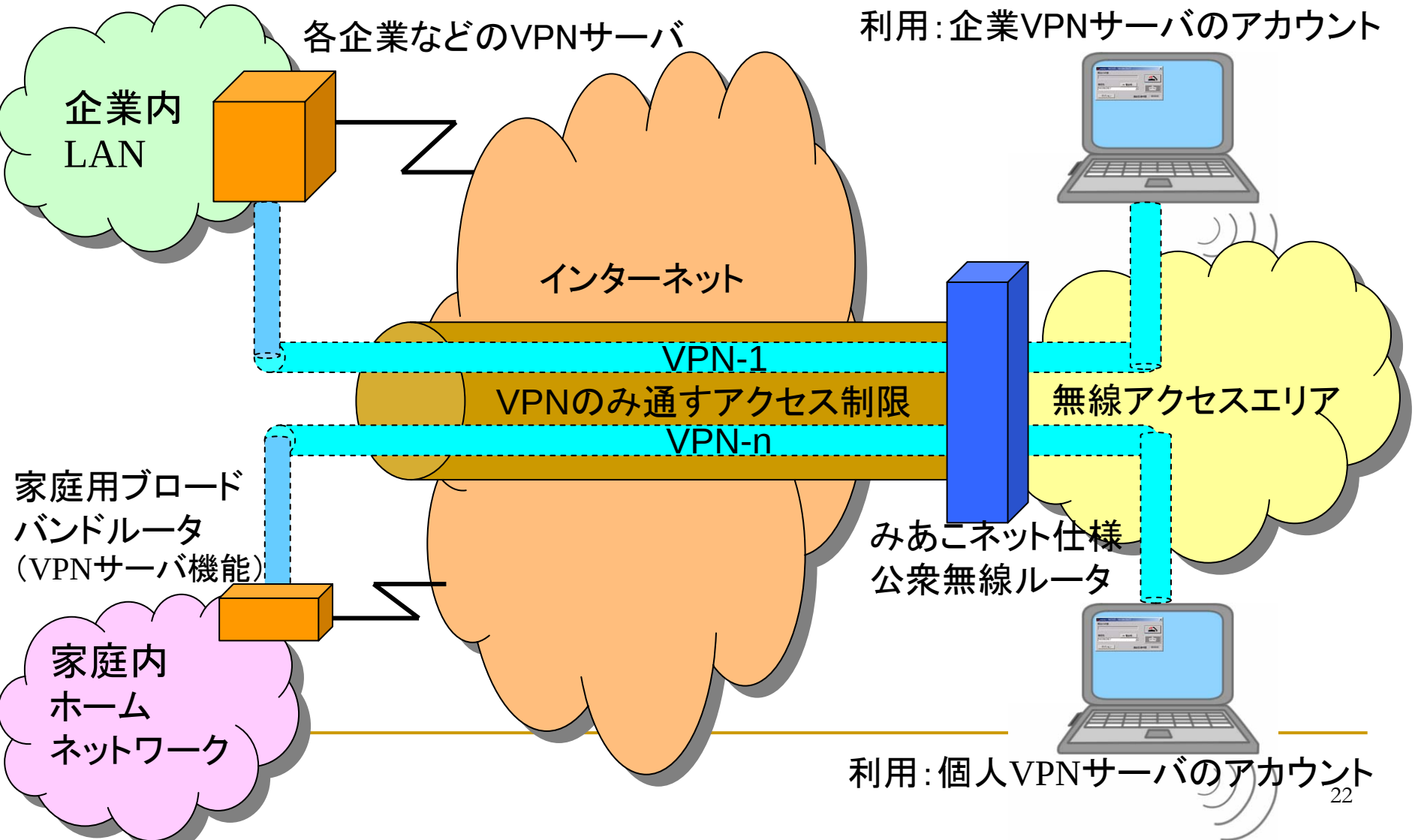
TS: トンネリングサーバ

自律分散型公衆無線インターネット『みあこネット方式』

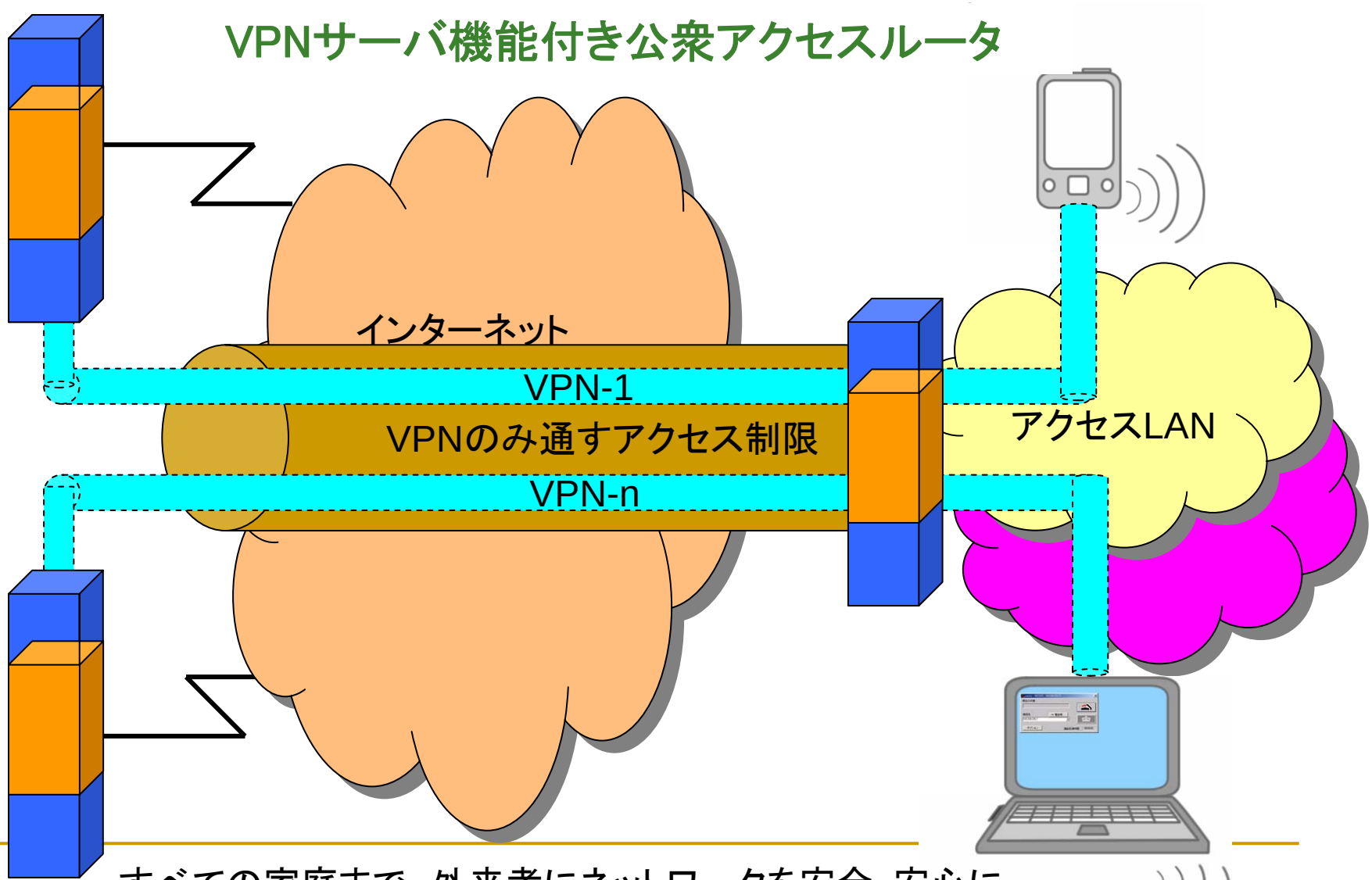


いつでもどこからでも「ホーム」環境へ安全に接続

ユビキタスネットワークインフラの実現　⇒みあこネット方式

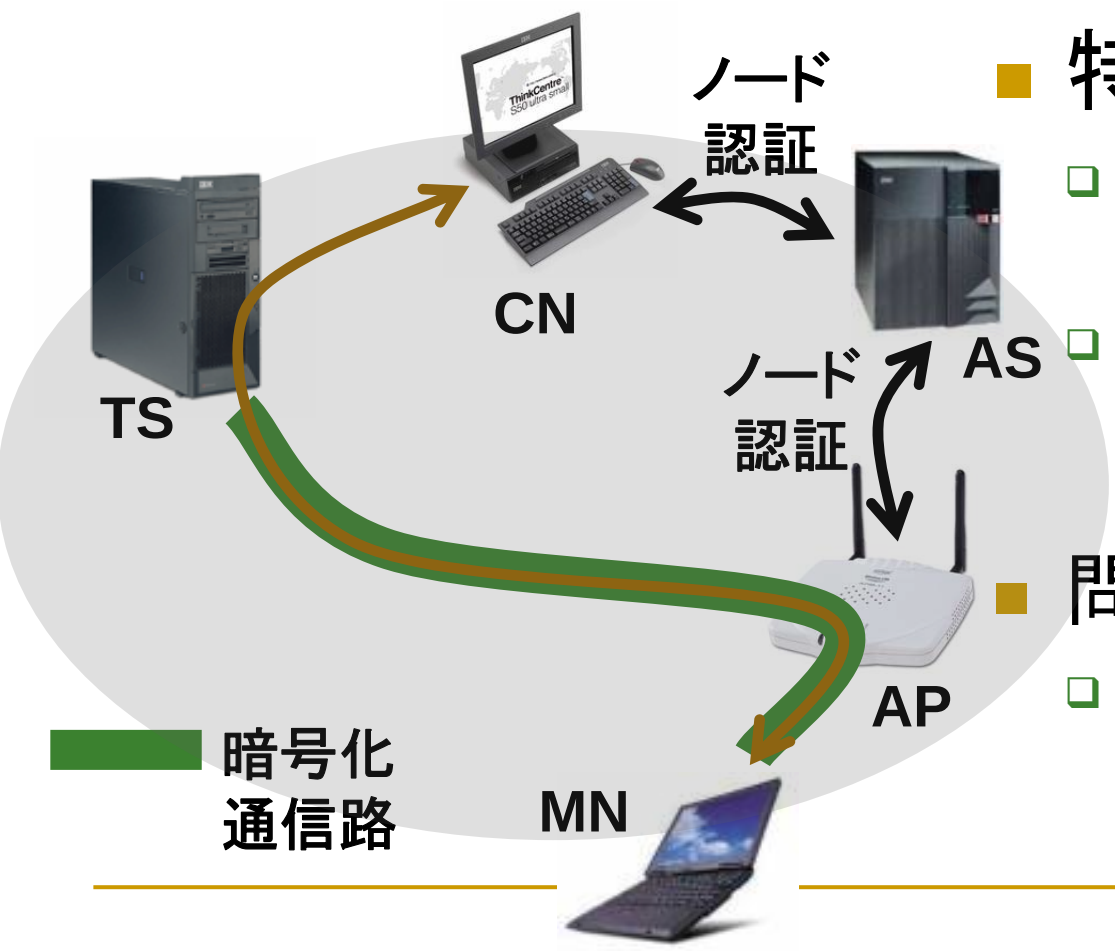


自律分散型公衆無線インターネットアクセスによるユビキタスネットワークインフラの実現



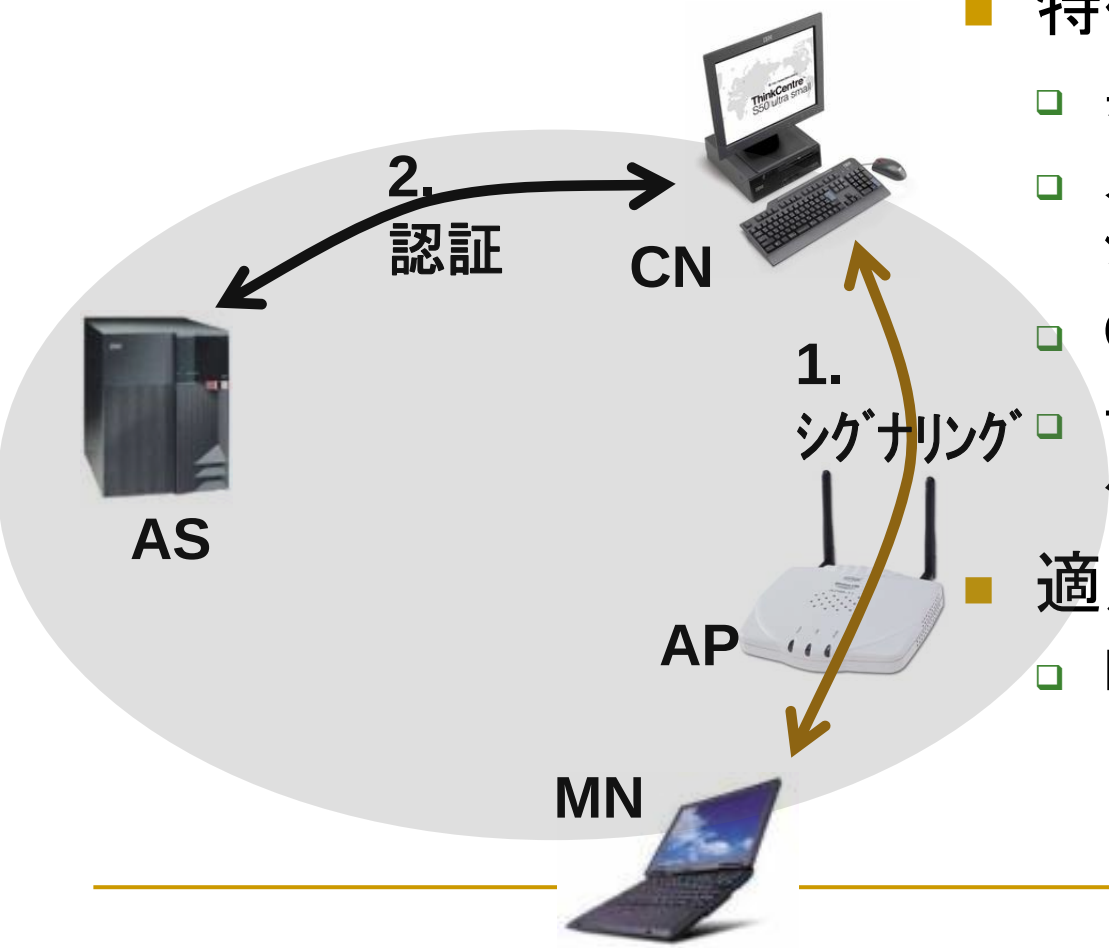
すべての家庭まで、外来者にネットワークを安全・安心に貸し借りできるユビキタスネットワーク環境

提案方式(2)
基地局認証ありトンネリング方式



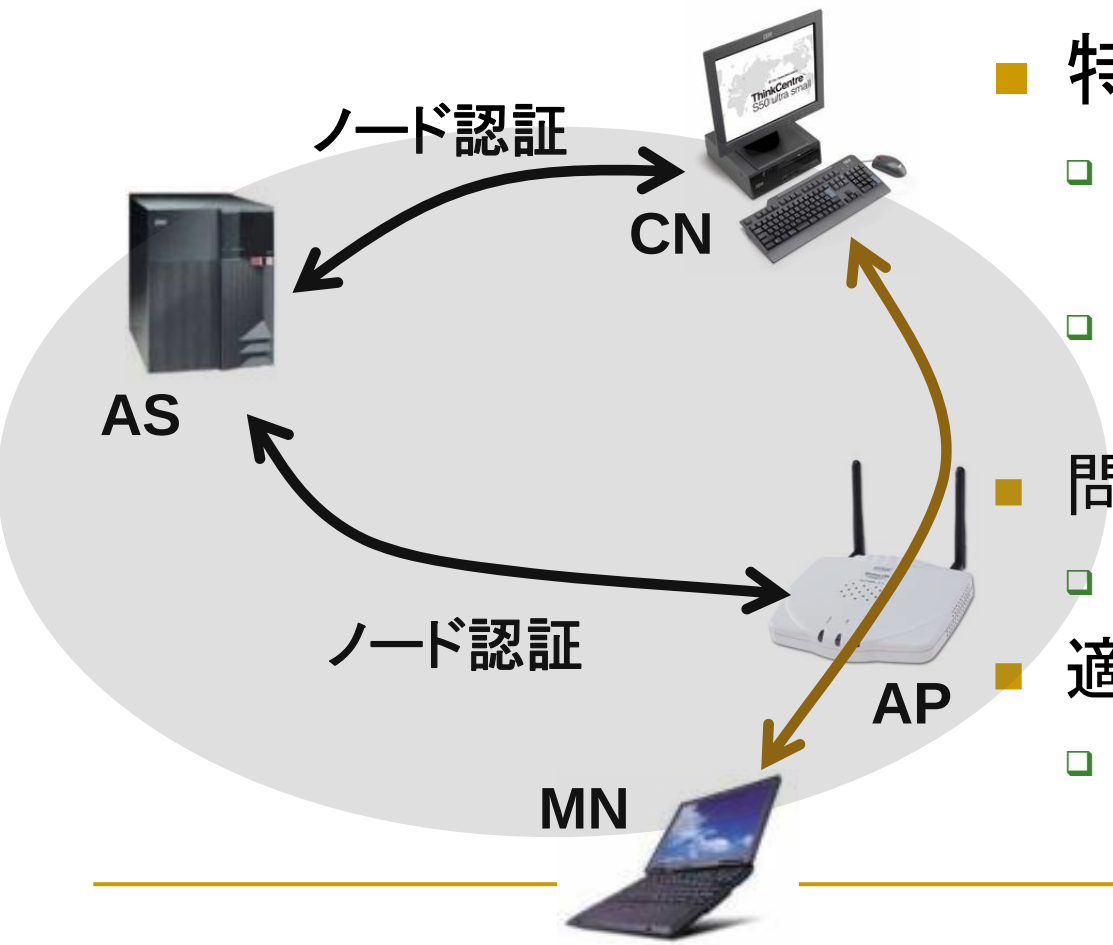
- 特徴
  - モバイルノードに対する認証機構に問い合わせ
  - AS-MN間の暗号化通信路上をCN-MNの暗号化通信が通過
- 問題点
  - 目的に対するAPの負荷
    - AS-MN間の認証

提案方式(3)
基地局認証なしダイレクト方式



- 特徴
  - 共通の認証機構を設置
  - ノード識別のための
    シグナリングをCN-MNで行う
  - CNはASに認証要求
  - データ通信は暗号化して
    ダイレクトにやりとり
- 適用例
  - HIP (Host Identity Protocol)

提案方式(4)
基地局認証ありダイレクト方式



- 特徴
  - モバイルノードに対する認証機構に問い合わせ
  - データ通信は暗号化してダイレクトにやりとり
- 問題点
  - 基地局の負荷が高い
- 適用例
  - MIPv6 + IPsec AH

提案方式の比較

サービスの要求要件によって推奨される方式は異なる

- トンネリング方式（みあこ3）
  - CN側がIPアドレスに基き発信者特定
  - 認証に関わりたくない→基地局認証なし
  - 未認証パケットを一切出したくない → 基地局認証あり
- ダイレクト方式（みあこ4）
  - IPアドレスに代わる発信者特定
    - 新技術（HIP, IPsec AH , MIP6 etc.)の導入が前提
    - CN側の対応が必須
  - 認証についての立場で、基地局認証の有無
- トンネリング方式とダイレクト方式の併用
  - 最初はトンネリング方式で接続し、CNが対応していればダイレクト方式に切り替える

まとめ

- 公衆無線インターネットアクセスのセキュリティモデル
  - 現状と課題
- 自律分散型公衆無線インターネットアクセス『みあこネット方式』の提案
  - すべての家庭に至るまでのユビキタスネットワーク環境の実現を、通信事業者主導でなく草の根的に行うモデルの提案