インターネット応用特論
１０．ＲＴＰ、時間同期、クロック同期、利用者認証、課金、ＲＡＤＩＵＳ

太田昌孝

mohta@necom830.hpcl.titech.ac.jp

ftp://ftp.hpcl.titech.ac.jp/appli10j.ppt

ネットワーク

- 物流網
  - 郵便、宅配便、コンビニ
- 情報通信網
  - 出版網（書籍、新聞、レコード（CD）、映画）
  - 金融網
  - 電話網
  - 放送網
  - インターネット

出版網

- 同じ情報を大量に配布
- 情報流通は遅くていい
- 著作権法による保護
- いまのインターネットの好餌
  - 壊滅寸前

金融網

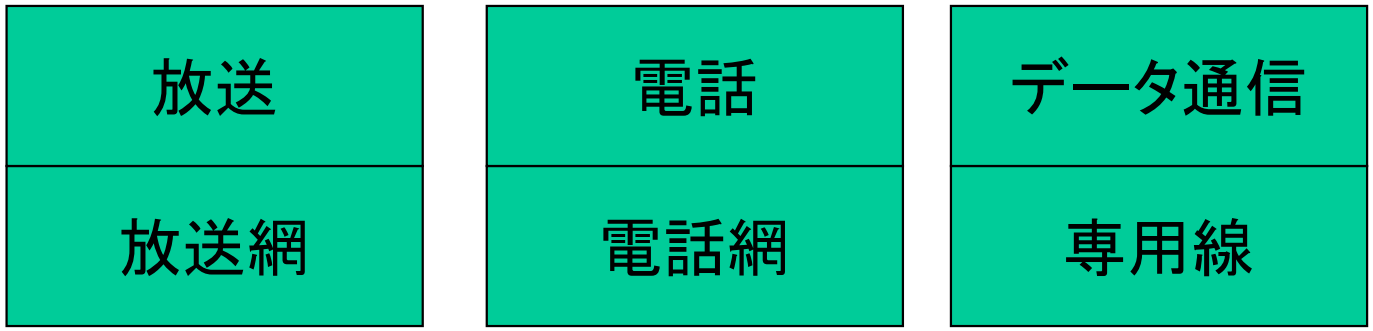
- お金のやりとりを管理
- 物流網でもあるが、今や、情報通信網としての面がはるかに大きい
- セキュリティー！！！

電話網

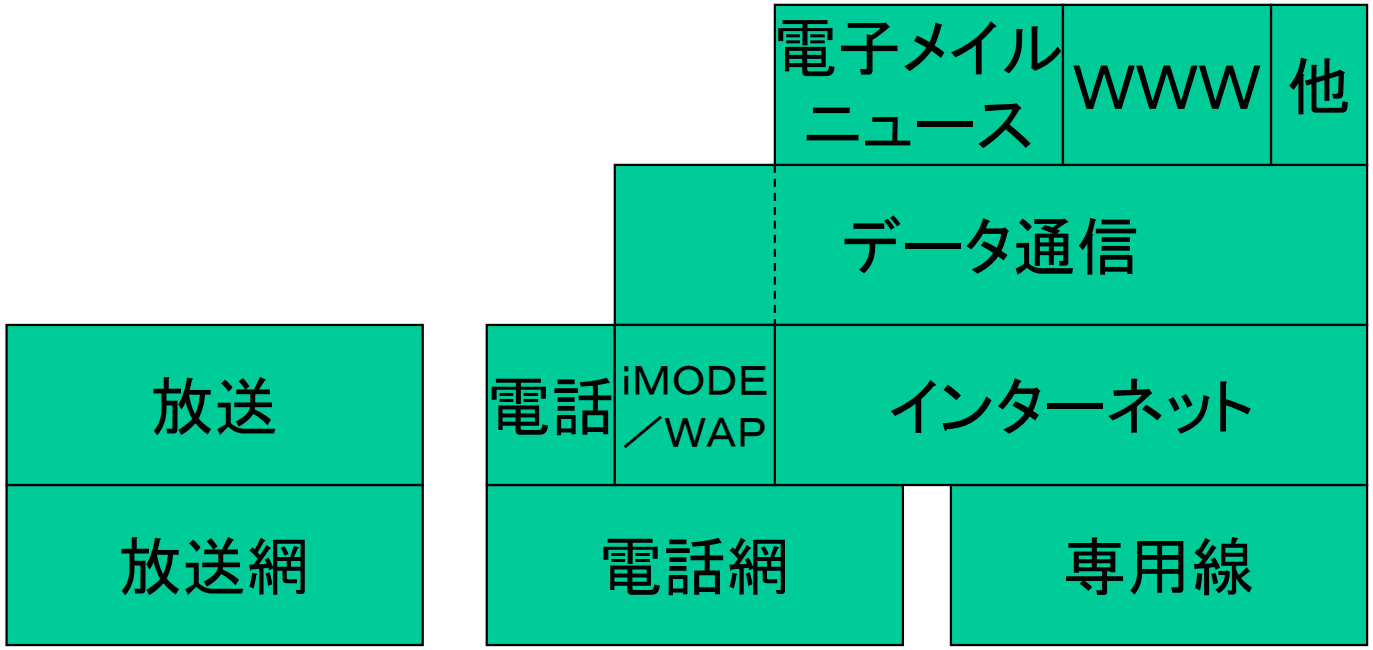
- 音声を実時間で伝送する網
  - 音声伝送の帯域を確保
  - 音声伝送の遅延を最小化（保証）
- 専用線事業も
  - あくまで音声伝送事業が主
- 遅くて高い
- 電電公社として保護、電気通信事業法で開放

放送網

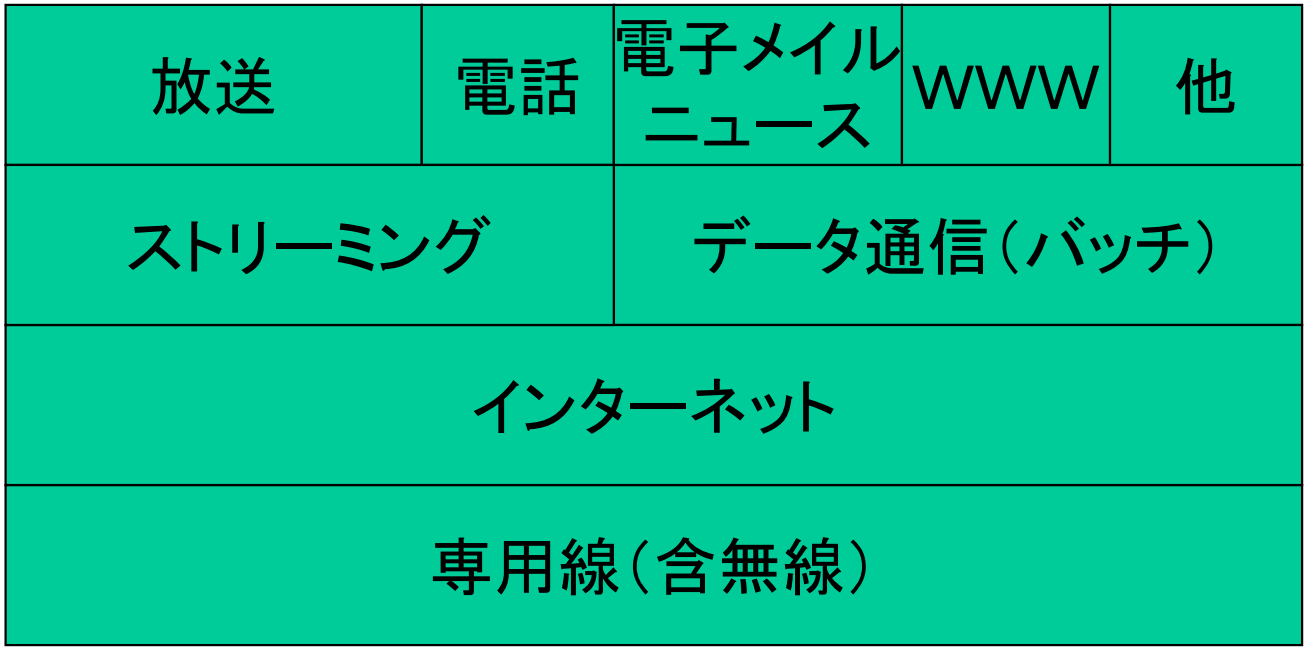
- 音声、画像を実時間で多数に伝送する網
  - 伝送帯域を確保
  - 遅延を最小化
- 電波による広域一対多通信
  - ブロードキャスト／マルチキャスト
- 放送法による保護



かってのネットワーク



現在のネットワーク



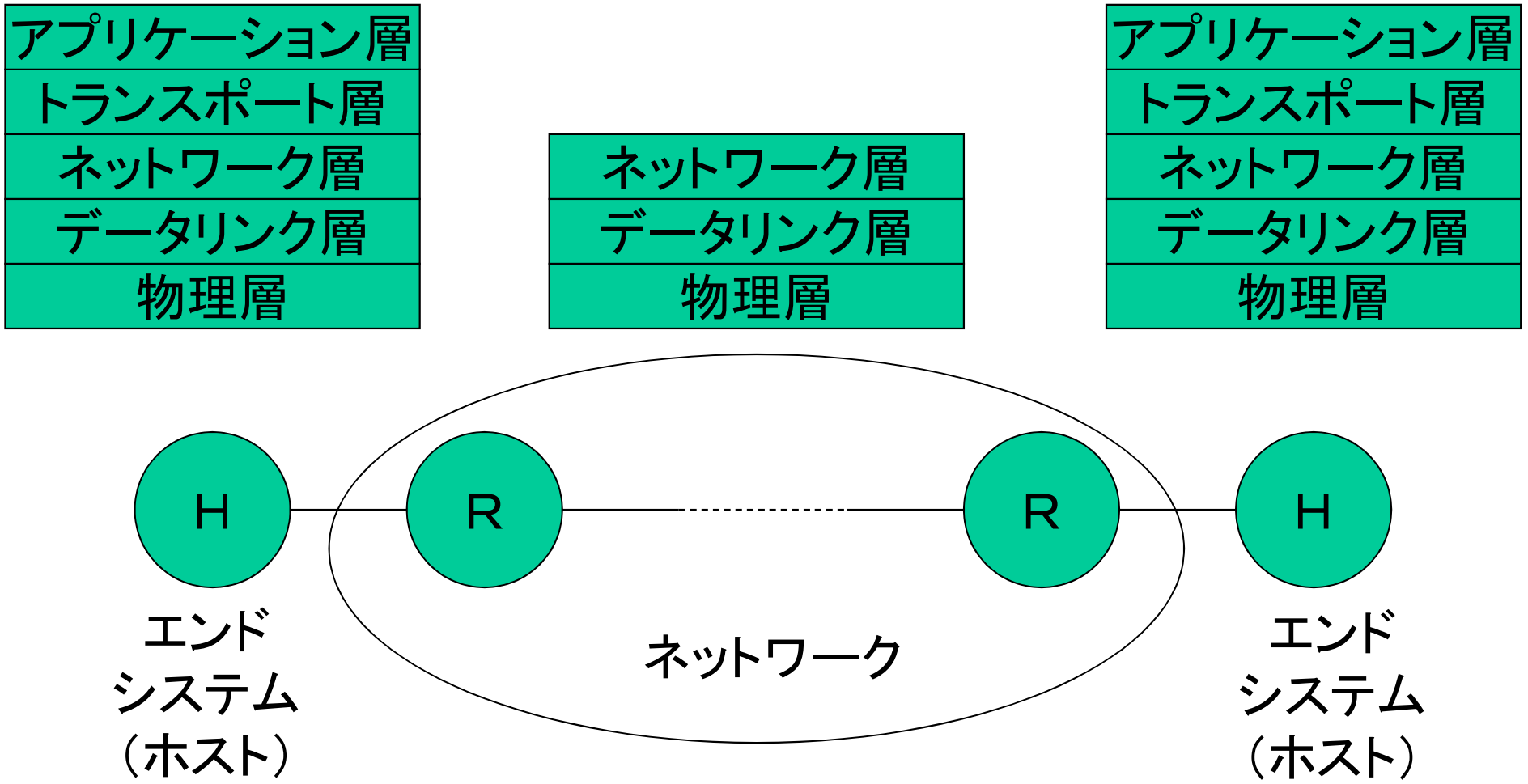
今後のネットワーク

ストリームメディアを インターネットにのせるには？

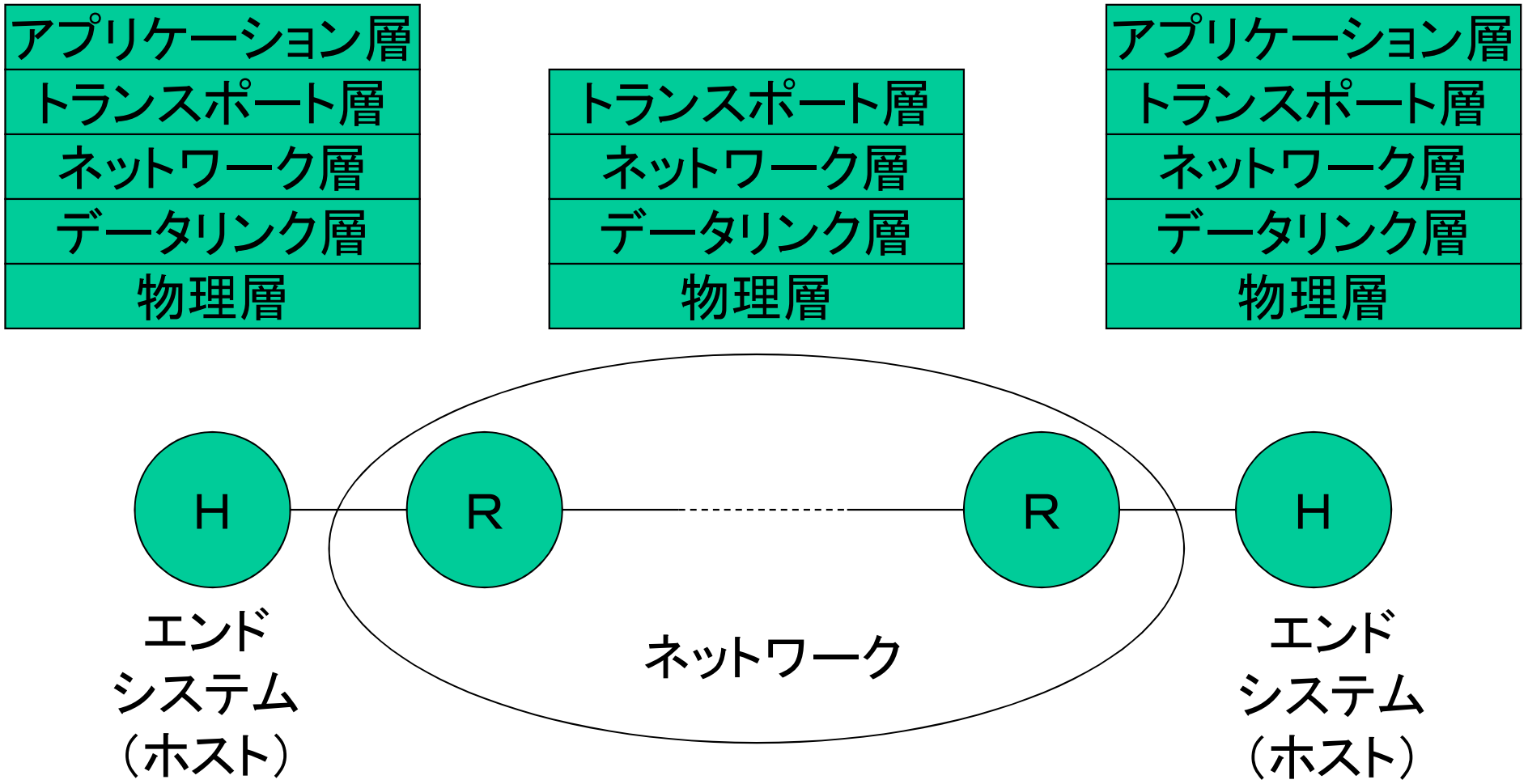
- QoS保証があればより快適
  - インフラの話
- 両端でのクロック同期
  - クロック速度があわないとバッファが溢れる／枯渇する
  - 時刻があわないと多地点からのメディアの合成ができない

QoSの例

- 電話
  - 帯域64Kbps、遅延0．1秒以下
- CD再生
  - 帯域1．5Mbps、遅延1秒以下
- テレビ放送
  - 帯域6Mbps、遅延1秒以下



ベストエフォートインターネット



QoS保証付きインターネット

遅延とジッタ

- ジッタ＝（最大遅延）－（最小遅延）
- スムーズな再生にはジッタ分＊２のバッファが必用
  - 最小遅延の直後に最大遅延でデータが到着しても再生するものがなくならない
  - 最大遅延の直後に最小遅延でデータが到着してもためておける
- ただし、送受信の速度の同期が必要

バッファとクロックのずれ

- クロックのずれはスムーズな再生を妨害
  - 送信側のクロックが受信側より遅いと
    - 受信側のバッファはいずれ空に
  - 送信側のクロックが受信側より速いと
    - 受信側のバッファはいずれあふれる

再生速度の同期のため

- 全ネットワーク機器に同一のクロックを供給する
  - イーサネットでは無理
  - IEEE．１３９４？
  - 全端末がGPSを受信？
- クロックはばらばらでも、速度を同期できないか？

再生速度の同期

- クロックのずれはそのままで
  - 再生速度を調節する
  - 送受クロックの相対誤差以上
- バッファをジッタの２倍以上用意して、再生速度を調整
  - バッファが半分以下なら再生速度を遅めに
  - バッファが半分以上なら再生速度を速めに
- 水晶発信機の精度なら音でも気にならず

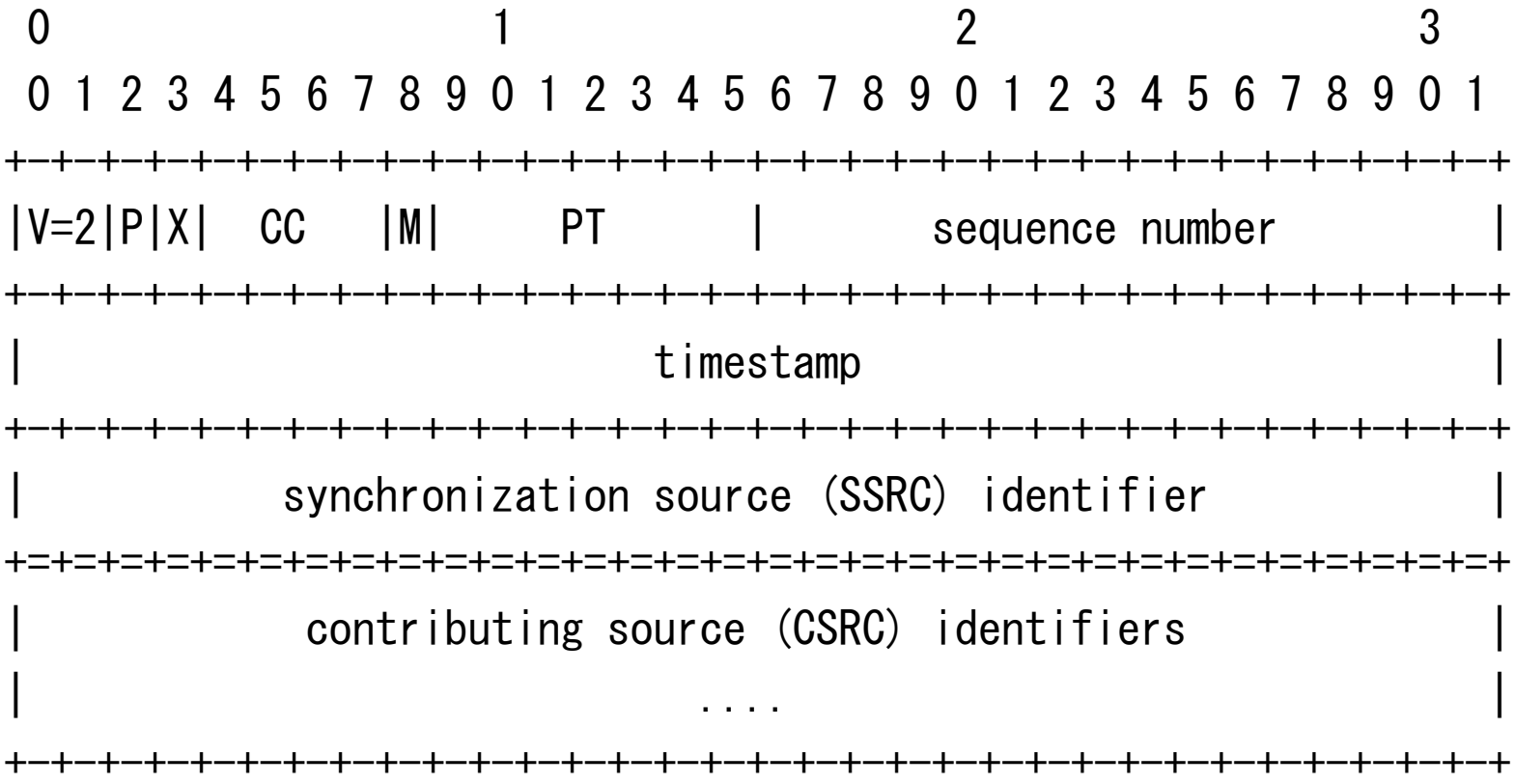
ジッタによる遅延

- 実遅延＝（ネットワーク最低遅延）＋（バッファ遅延）
- バッファ遅延＝２＊（ジッタ）

RTP （Real―Time Transport Protocol）（RFC1889）

- ホスト間の同期のためのトランスポート／アプリケーション層のプロトコル
  - ネットワーク中の遅延やジッターが減るわけではない
  - ペイロードタイプ（PT）によるメディアの識別
  - シーケンス番号による順序の回復
  - タイムスタンプによるクロック同期
- 各種のメディアに対応（RFC1890他）

RTPのヘッダー（１）


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|V=2|P|X| CC |M| PT | sequence number |
| timestamp |
| synchronization source (SSRC) identifier |
| contributing source (CSRC) identifiers |
| .... |

RTPのヘッダー（2）

- v
  - バージョン（2）
- p
  - パディング
- x
  - 拡張ヘッダあり
- CC （CSRC Count）
  - CSRCの数

RTPのヘッダー（３）

- M
  - マーカー
- PT
  - ペイロードタイプ
  - エンコーディング方式などを指定
- sequence　number
  - パケットごとの通し番号
  - 初期値はランダム

RTPのヘッダー（４）

- time　stamp
  - ペイロードごとに間隔は異なる
  - 初期値はランダム
- SSRC　（Synchronization　Source）
  - 同期のソースのID（IPアドレスではない）
  - SSRCが同じタイムスタンプは比較可能
- CSRC　（Contributing　Source）
  - コンテンツのソース（話者）のID

RTPとエンドツーエンド原理

- RTPはアプリケーションゲートウェイを仮定
  - トランスレータ
    - メディアを変換
  - ミキサー
    - 複数の音声（？）を混合、会議では当然？
  - エンドツーエンド原理は重要視されない
    - IPアドレスでなく、SSRCでソースを識別
- クロック同期はエンドツーエンド
  - ネットワークにグローバルクロックは不要

時刻の同期

- 絶対時刻に意味なし
  - 相対性原理
    - ２地点間で情報が伝わるのにかかる時間の以下の時刻のずれは観測不能（あっても困らない）
- NTPという時刻合わせのプロトコルはある
- RTPでも可能
  - 各CSRCがSSRCの送る時刻に同期

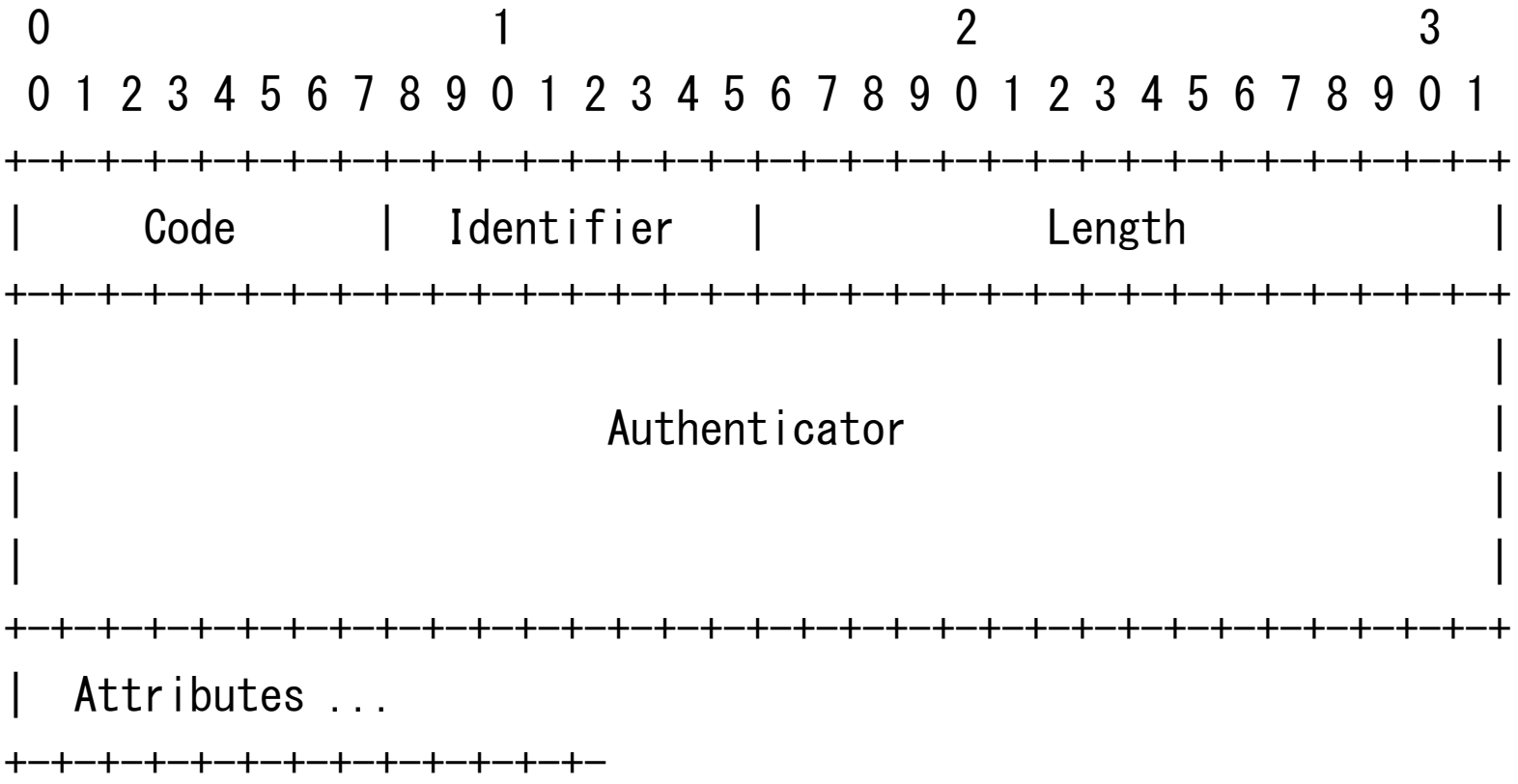
AAA （Authentication、 Authorization、 Accounting）

- 利用者の
  - 認証
    - 身元確認
  - 利用許可
    - 適切な権利付与
  - 課金
    - 利用に応じた課金

RADIUS （Remote Authentication Dial In User Service、 RFC2138、 RFC2139）

- 本来ダイアルアップISPのプロトコル
- UDPベース
- ダイアルアップの受け口がクライアント
- RADIUSサーバでクライアントを集中管理
  - サーバクライアント間にも認証あり
    - クライアントからサーバに送るパスワードは秘匿
- AAA（Authentication、Authorization、Accounting（RFC2139））を行う

RADIUSのパケット形式

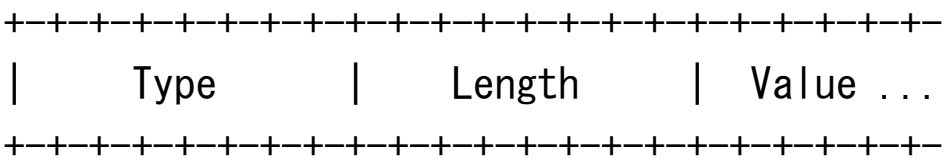


RADIUSのパケット形式

- Code
  - 1　Access-Request
  - 2　Access-Accept
  - 3　Access-Reject
  - 4　Accounting-Request
  - 5　Accounting-Response
  - 11　Access-Challenge
  - 12　Status-Server (experimental)
  - 13　Status-Client (experimental)
  - 255　Reserved

RADIUSのパケット形式

- Identifier
  - リクエストとリプライをマッチ
- Length
- Authenticator
  - 16バイトの認証情報
- Attributes



Attributesの例

- 1 User-Name
- 2 User-Password
- 3 CHAP-Password
- 4 NAS-IP-Address
- 5 NAS-Port

RADIUSの拡張

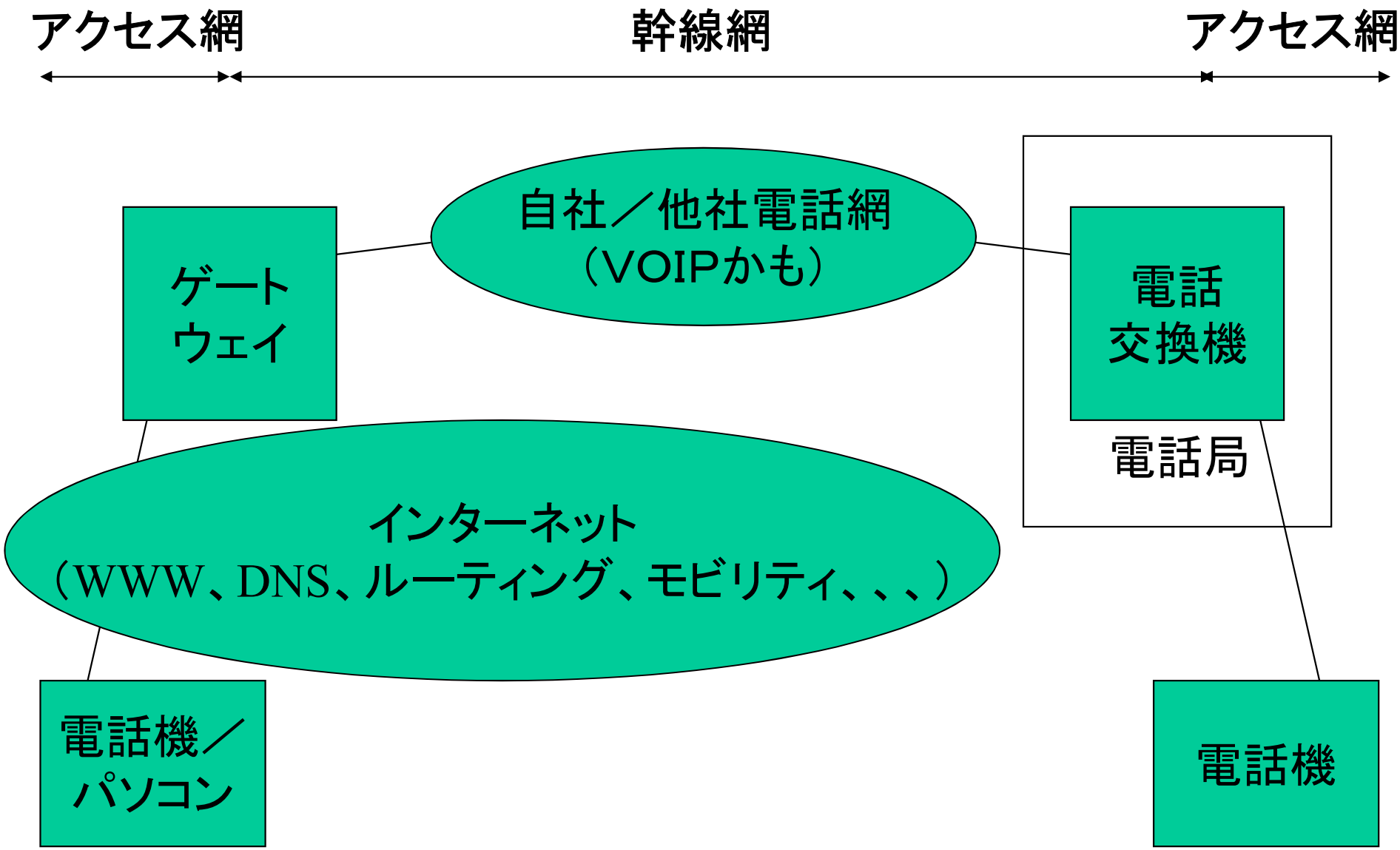
- RADIUSメッセージはTLV（Type　Length　Value）形式のオブジェクトからなる
  - 拡張は容易
    - Typeは、特定のサーバ、クライアントで一致すればよい
- インターネット電話への拡張
  - インターネットから電話網をアクセス
- 無線インターネットへの拡張

インターネット時代の電話サービス（ビジネス？）モデル

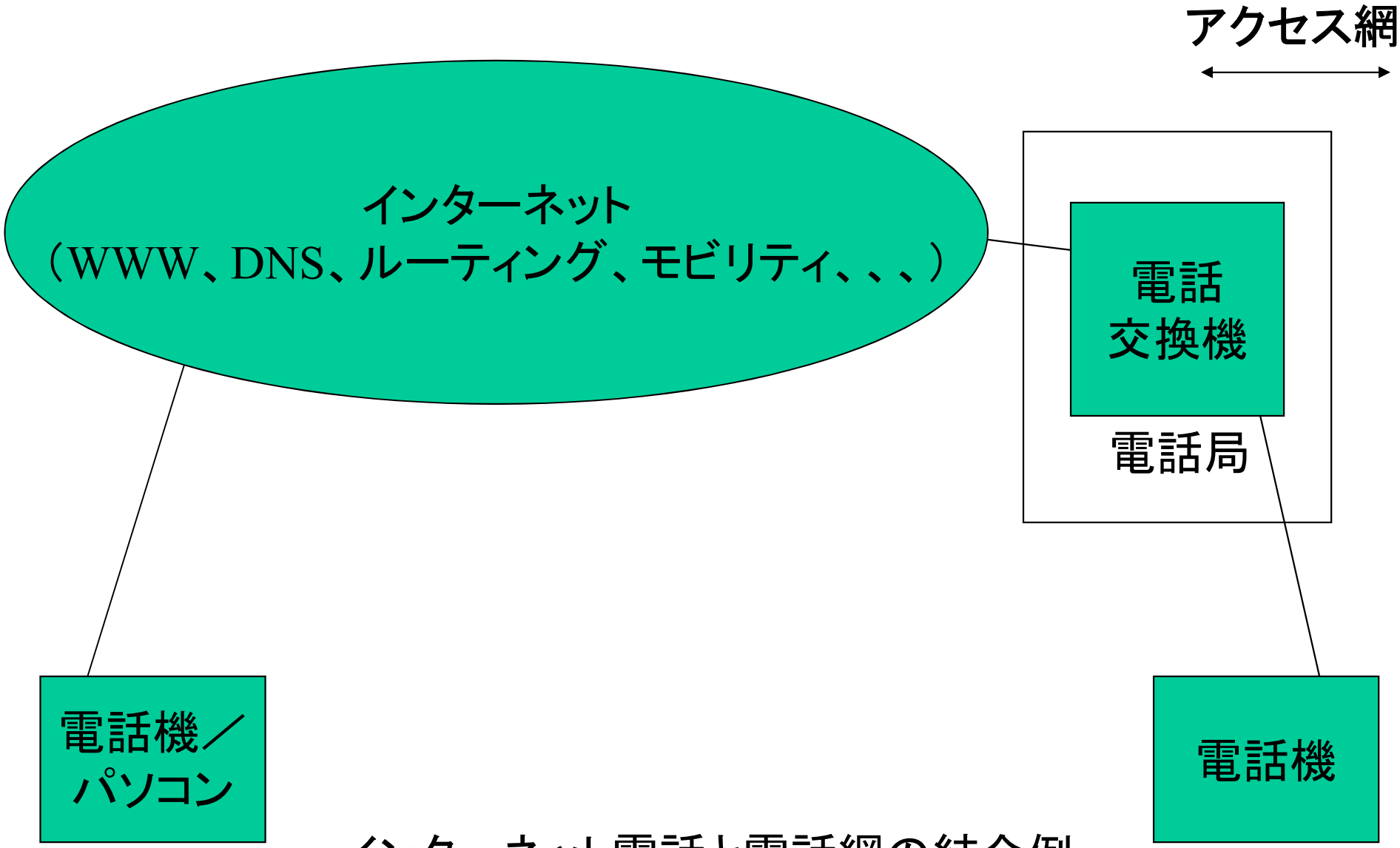
- インターネット内では
  - ピアツーピアで通話
  - ネットワークは何もしない、ネット事業者も不在
    - 規制やビジネスの余地なし
    - 端末は売れる
- インターネットと電話網とのゲートウェイ
  - 当面（電話網存命中）は事業として成立
- 電話網事業は存続できない

インターネット＜ー＞電話網の中継サービス

- 中継ゲートウェイを適当に配置
  - 各市内におけば、もっとも安い
  - 東京、大阪、米国程度でも十分かも
- インターネット内は無料（ISP料金のみ）
- 電話網内は従量制課金



インターネット電話と電話網の結合例



インターネット電話と電話網の結合例
ーここまでやる（全市内にゲートウェイを置く）ことも可能ー

インターネットと電話網の接続

- 電話網ー＞ゲートウェイー＞インターネット
  - インターネット側利用者が定額制で登録
- インターネットー＞ゲートウェイー＞電話網
  - 電話網部分は従量制課金
  - コーリングカード程度のセキュリティで十分
- 電話網ー＞インターネットー＞電話網
  - 普通の長距離電話業者とあまりかわらない

NOTASIPプロジェクト

- インターネット電話のプロジェクト
  - 郵政省（TAO）の補助金
- 何も発明しない、何も凝らない
  - URLによる端末の認識
  - RADIUSにより電話網との接続を管理
    - コーリングカード（PIN）セキュリティで十分
  - アナログ電話の使い心地をそのままに
  - 経路選択やモビリティは、インターネット任せ

無線インターネット

- 固定インターネットが大前提
  - 速くて安くて定額制の固定インターネットに速くて安い無線機を接続すると
    - 安くて定額制の無線インターネットが実現
  - 無線機の密度を十分高くすると
    - 速くて安くて定額制の無線インターネットが実現

無線インターネットの技術的課題

- 無線は不特定多数が使える
  - 認証
    - 誰もがいつでもどこでもインターネットをつかえるのはいいが
    - どこの誰なのか身元がわからないのは困る
      - 犯罪捜査
      - 課金
  - 暗号化
    - 本来はエンドツーエンド
    - 無線上でパスワードを入力するような場合に便利

ダイアルアップインターネットの一般的セキュリティ

- 接続は電話網等が提供、維持
  - そこそこにセキュア
    - 犯罪捜査等には電話網等のログが利用可能
- 電話網等の接続中は他者は割り込めない
  - 接続開始時にだけ認証すればよい
    - PPPの当初にパスワード等で認証
    - 以後、接続が切れるまで、そのまま

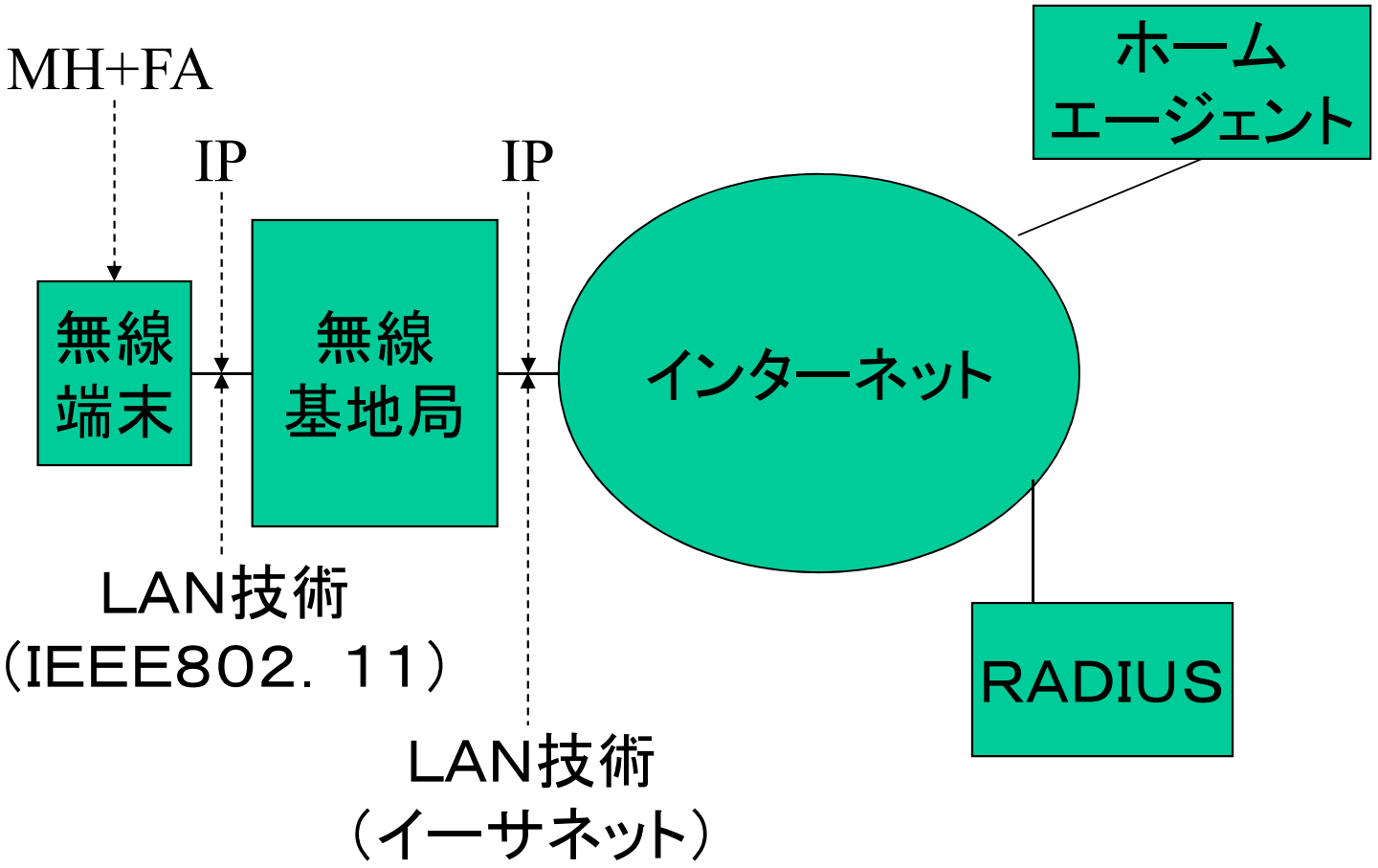
無線を利用したダイアルアップインターネットのセキュリティ

- 接続は無線が提供、維持
  - セキュリティ皆無
    - 犯罪捜査等には独自のログが必要
- 接続中に他者が割り込める
  - 接続開始時にだけ認証すると、、、
    - 利用者はIPアドレスとMACアドレスで特定？
      - 誰でも偽造可能
  - パケット単位の認証が必須
    - 接続開始時には、セッション鍵を交換

無線インターネットの
セキュリティ

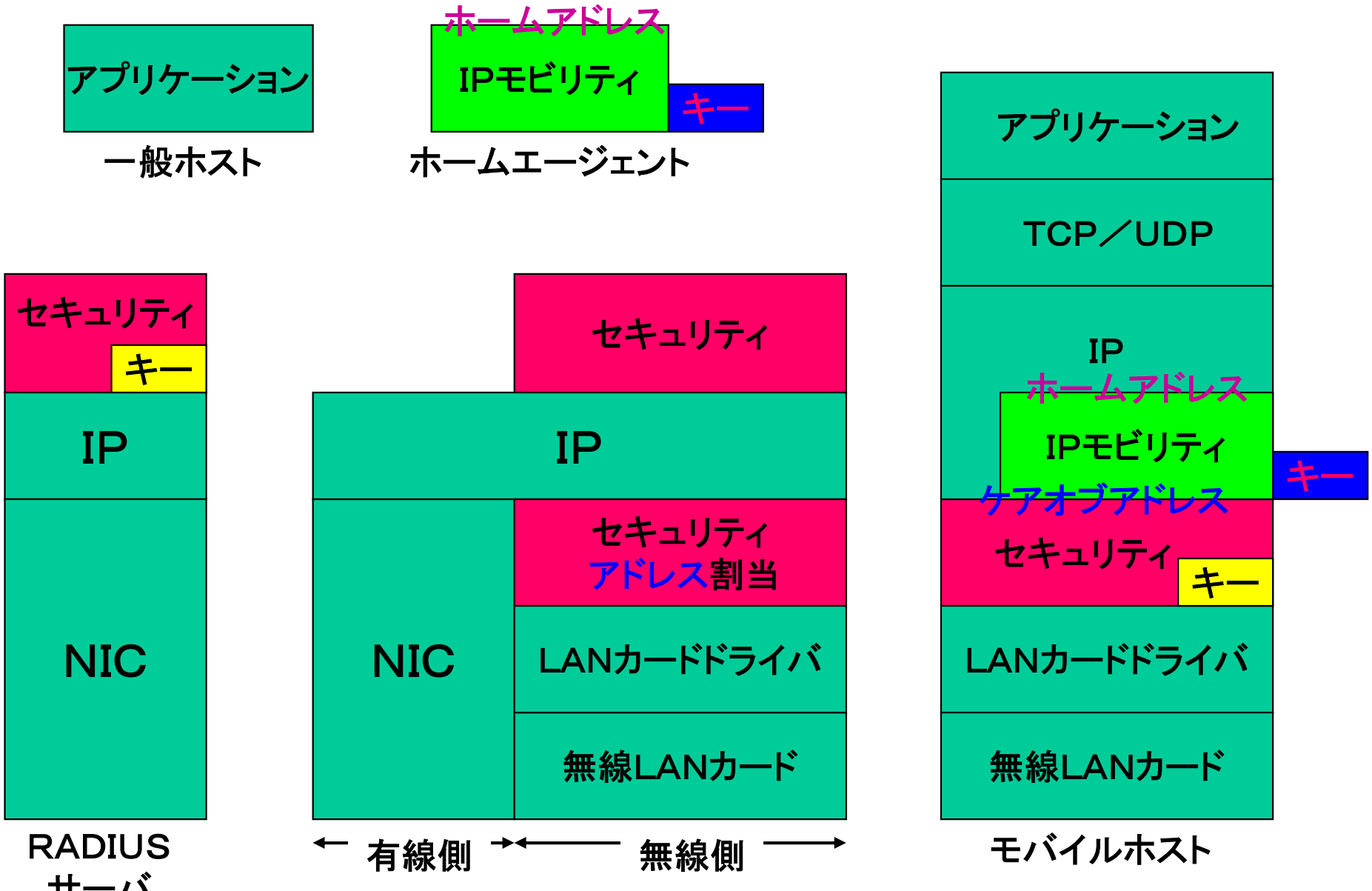
- RADIUSサーバでユーザごとの鍵を管理
- ユーザはセッション鍵を生成、自分の鍵で暗号化して無線基地局に送る
- 無線基地局はRADIUSサーバにセッション鍵の解読を依頼
- セッション鍵は認証と暗号化に利用可能

正しいモバイルインターネット



MISサービスの構成要素

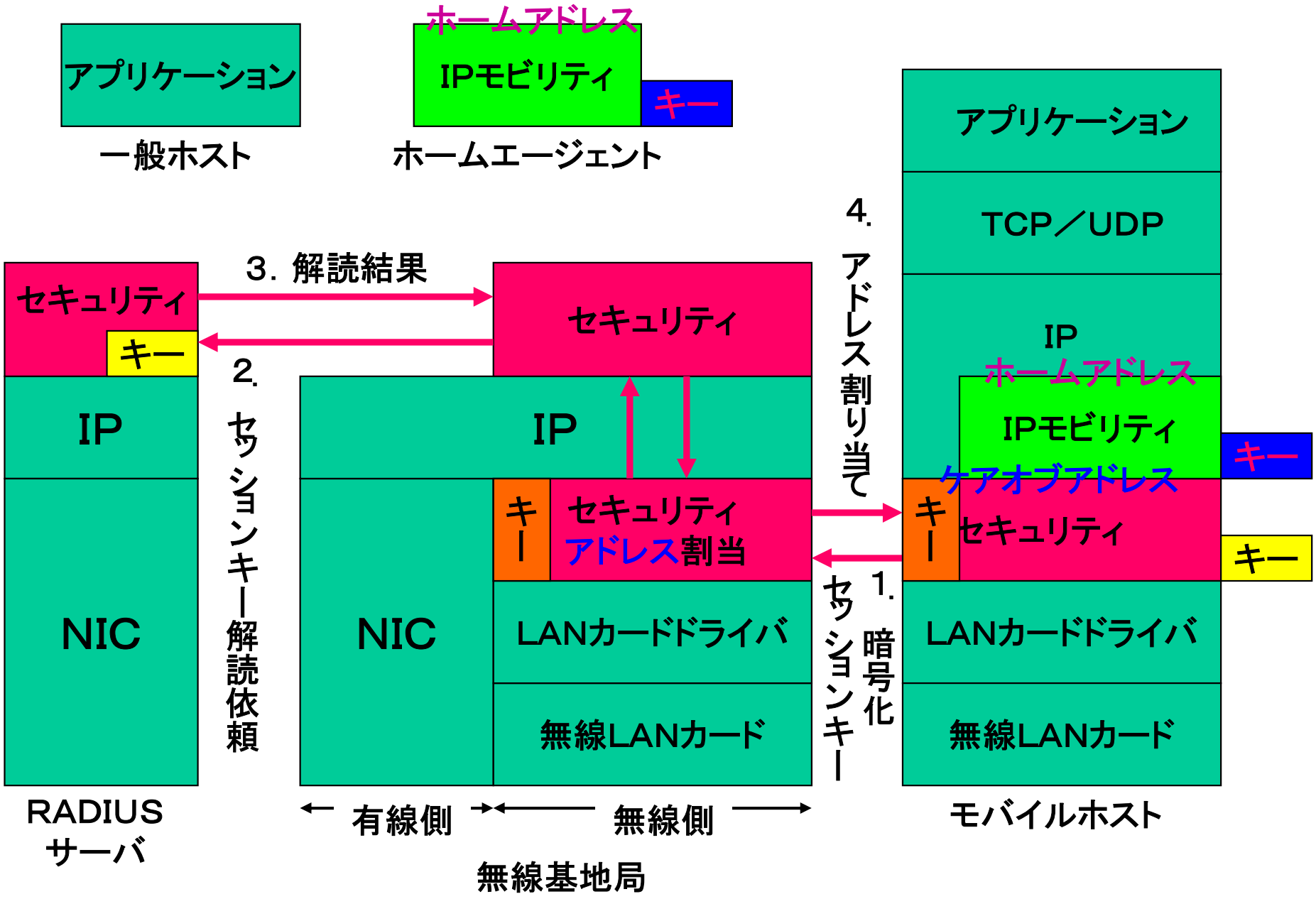
- モバイルホスト（無線端末）
  - 基地局エリア内、基地局間を移動する端末
- 無線基地局
  - 無線インターフェースをもったルータ
- RADIUSサーバ
  - 無線区間利用の鍵をユーザごとに管理
- ホームエージェント
  - ホームアドレス宛てパケットをモバイルホストに転送



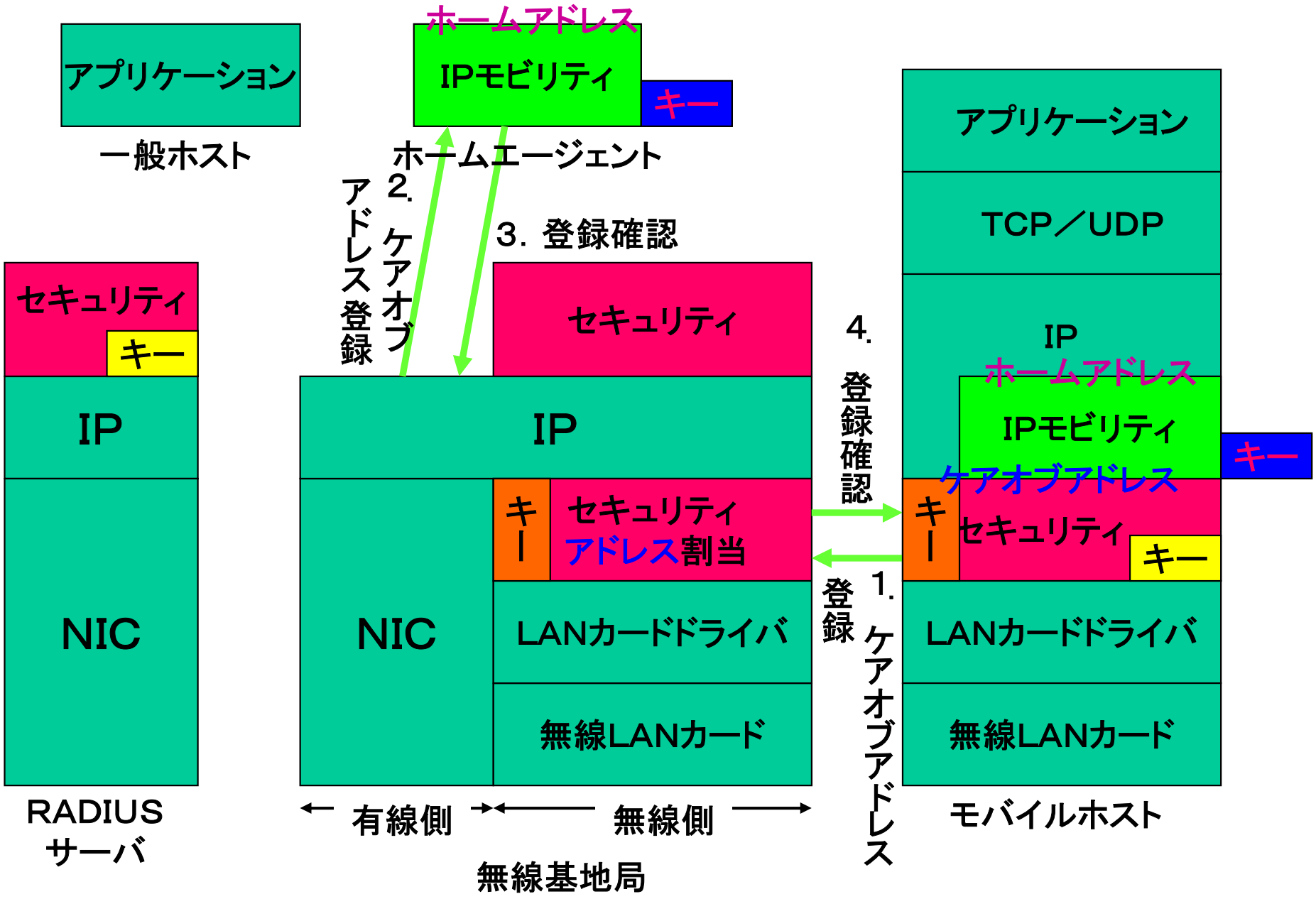
MISサービスの構成要素

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

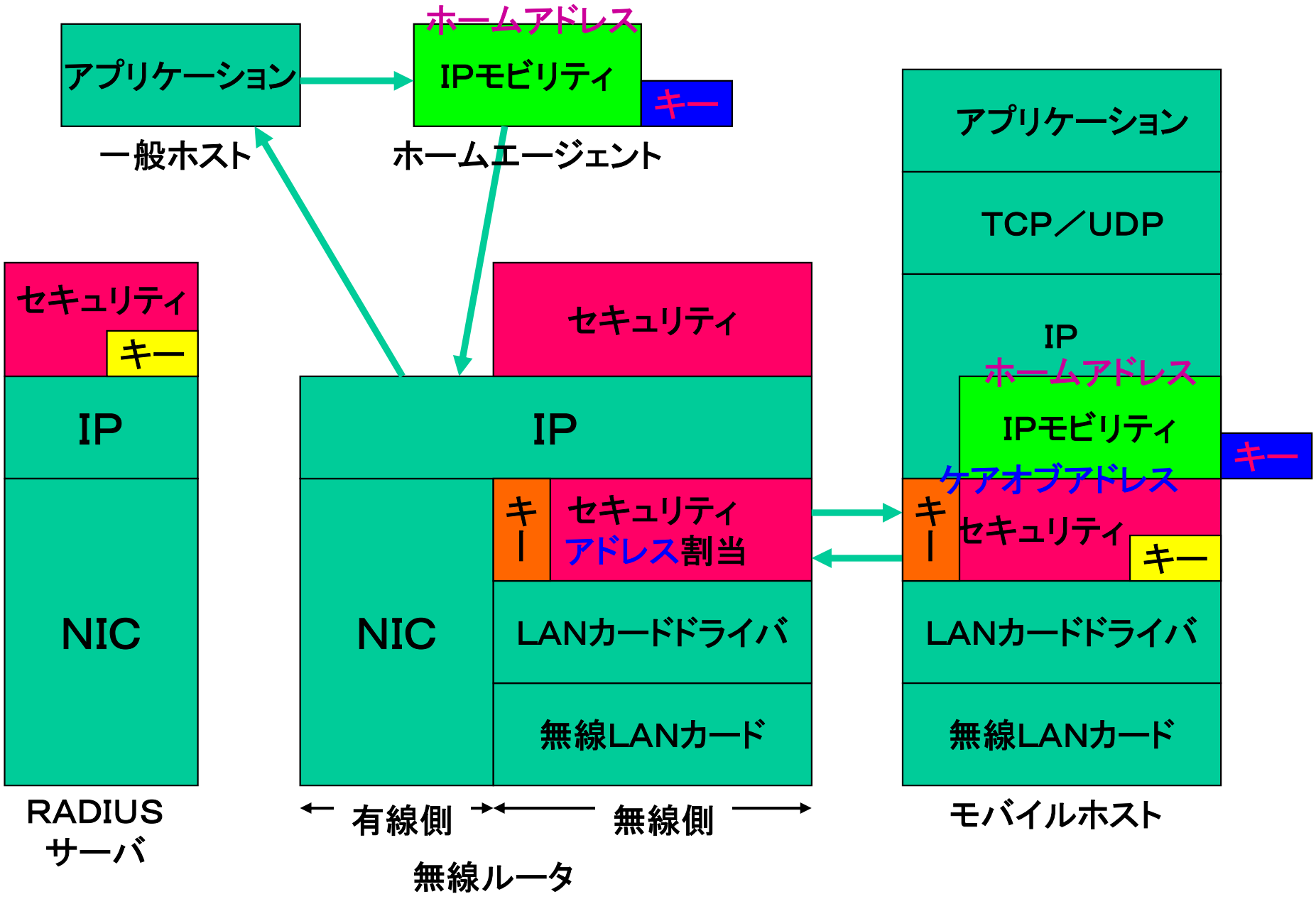
- モバイルホストはセッションキーを生成
- ユーザごとのキーで暗号化して無線基地局に転送
- 無線基地局はRADIUSサーバに解読依頼
- 無線基地局とモバイルホストはセッションキーを共有
- 無線基地局はケアオブアドレスを割り当て



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）



MISサービスの最終段階（一般ホストとの通信）

まとめ

- インターネット全体のクロック同期は不要
  - バッファで再生速度を調整
  - 時刻は、どこかに同期
- RADIUS（の拡張）は、いろいろな認証の役に立つ