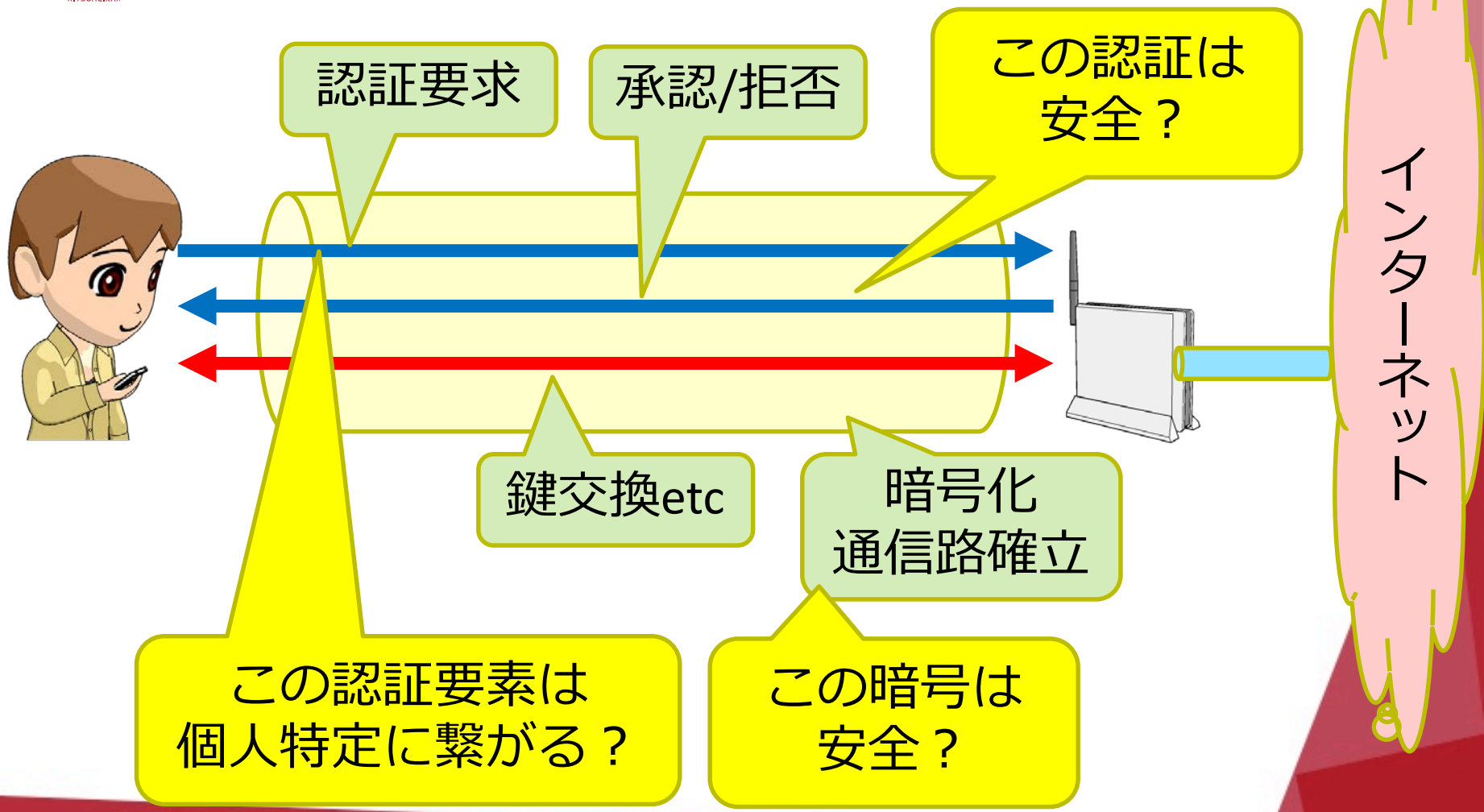
資料1－7

RITSUMEIKAN

# 公衆無線LANセキュリティの状況整理

立命館大学情報理工学部
上原哲太郎

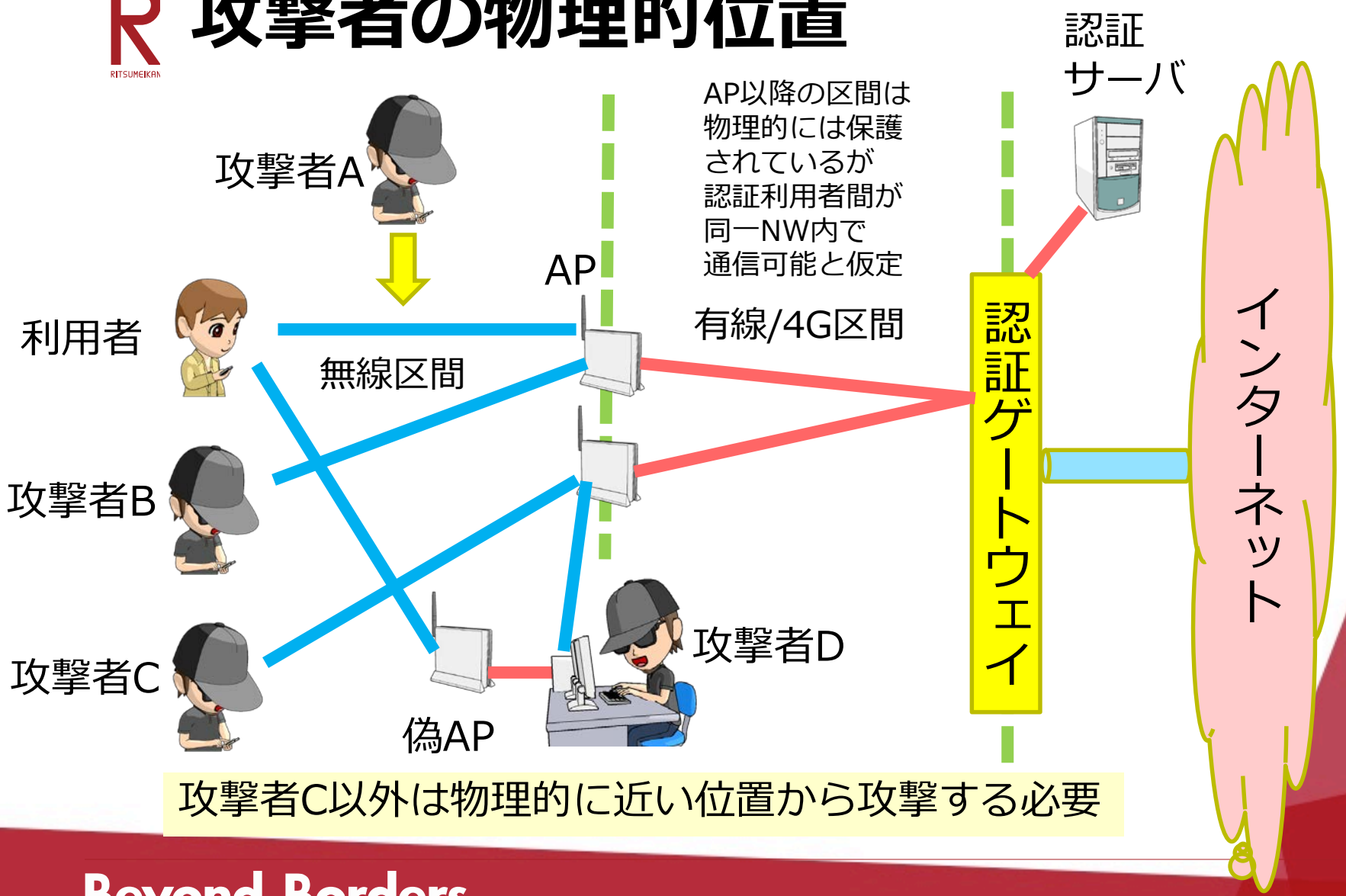
# 暗号・認証・追跡可能性


認証要求
承認/拒否
この認証は
安全？
インターネット
鍵交換etc
暗号化
通信路確立
この認証要素は
個人特定に繋がる？
この暗号は
安全？

# 公衆無線LANの主な利用者認証

- 無認証
  - MACアドレスのみ記録/それもなし
- 無登録でWeb上にクリック後利用可
  - メールアドレス等を登録させる場合もあり
- Web認証
  - 事業者のIDとパスワード(PW)を入力
  - 他の認証との連携（SNSなど）
  - Web-API認証（アプリ用など）
- 802.1X/WPA-Enterpriseによる認証
  - EAP-PEAP等のパスワード認証
  - EAP-AKA等のSIM認証
- スマホアプリによる認証も
  実質は上記いずれかが多い

# 攻撃者の物理的位置




攻撃者C以外は物理的に近い位置から攻撃する必要

# 攻撃者の位置と脅威

- 攻撃者A：無認証で無線区間から攻撃
- 攻撃者B：無線APに接続・認証した上で攻撃
- 攻撃者C：認証後に同一L3ネットワーク内から攻撃
- 攻撃者D：偽APによるなりすまし・中間者攻撃

| 攻撃 | 認証情報の窃取 | 盗聴 | なりすまし改ざん | 備考 |
|---|---|---|---|---|
| 攻撃者A | △ | ○ | ○ | 無線部分の暗号化形式に依存 |
| 攻撃者B | ○ | ○ | ○ | APで分離すれば攻撃困難に |
| 攻撃者C | ○ | ○ | ○ | 同一NW内での通信禁止で攻撃困難に |
| 攻撃者D | ○ | ○ | ○ | Web認証だと様々な攻撃が容易 |

どの場合でも盗聴可能性はあるがL2/L3以下
かつ多くは物理的に近傍にいないと攻撃できない

# 考慮すべき脅威（1）

- 無認証での無線区間からの攻撃(A)
  - MACアドレス窃用でのなりすまし
  - WEP鍵の窃取・盗聴
  - WPA-PSK鍵の窃取・盗聴
- 無認証での中間者攻撃(D)
  - パケット挿入
  - 盗聴
  - 中間者攻撃での認証情報窃取

# 考慮すべき脅威（2）

- PSK使用での無線接続後または認証後の無線区間からの攻撃(B)
  - 無線区間での盗聴
  - ARP毒入れでの中間者攻撃・盗聴
- PSK使用での無線接続後または認証後の有線区間からの攻撃(C)
  - ARP毒入れでの中間者攻撃・盗聴

# 中間者攻撃やフィッシングによるクレデンシャル窃用の容易さ

- Web認証は偽の認証画面による ID/PWの窃用に弱い
- EAP-PEAP等も認証サーバ証明書を確認しないとPW窃用の危険
- しかし利用者に徹底させるのが困難
  - 本来はアプリ等でやるべきだが 今度は偽アプリ問題との戦いになる
  - SIM認証等への移行

# 公衆無線LANのセキュリティ上考慮するべきこと

- 他の利用者が信用出来なければL3以下での盗聴や中間者攻撃の可能性は残る
  →TLSやVPN等の暗号化・認証を必要に応じ併用
  認証時の「サーバ認証」の徹底
- 「同一LAN内の端末を信用しない」設定が必須
  - PCのファイルやプリンタの共有設定
  - PCのパーソナルファイアウォールの設定
  - モバイル機器はどうするべきか？
- これらをどう認知させていくか
- 事業者は端末間通信を遮断すべきか否か

# 認証と個人追跡性がより課題

- 認証はなりすまし容易か？
- クレデンシャルの窃用の危険は？
- 認証IDの「個人特定度」(LoA)
- 認証や通信のログはどうするか
  - 保存内容と期間の問題
  - 通信ログについてはNAT問題も

- 犯罪捜査等では追跡性が特に課題

# ID/クレデンシャルと本人特定

| ID/クレデンシャル | 特徴 |
|---|---|
| MACアドレス | アドレスから端末の特定が難しい<br>詐称が容易<br>近傍から窃用される可能性がある |
| メールアドレス | 本人特定が難しい場合あり<br>到達性確認しないと詐称される |
| IDとパスワード | 発行時の本人確認に依存 |
| SIM | 音声契約があれば本人特定は精度高い<br>海外SIM、MVNOのデータ専用SIMは<br>本人特定困難な場合も |
| SNS等との認証連携 | 認証連携先の本人確認に依存 |
| その他 | 海外ではクレジットカード番号や<br>パスポート番号の例もあるが<br>詐称確認コストがかかる |

# コストとのトレードオフ

- 既存システム更新のコスト
- 利用者サポートコスト
  - 「使用法」「利用規約」を読ませる機会は？
- ID発行コスト
  - 本人確認した上での発行は高コスト
  - 認証連携を広げる方が楽
- インシデント対応コスト

- 公衆無線LANのビジネス構造の中では理想の姿に近づける最大の障害？