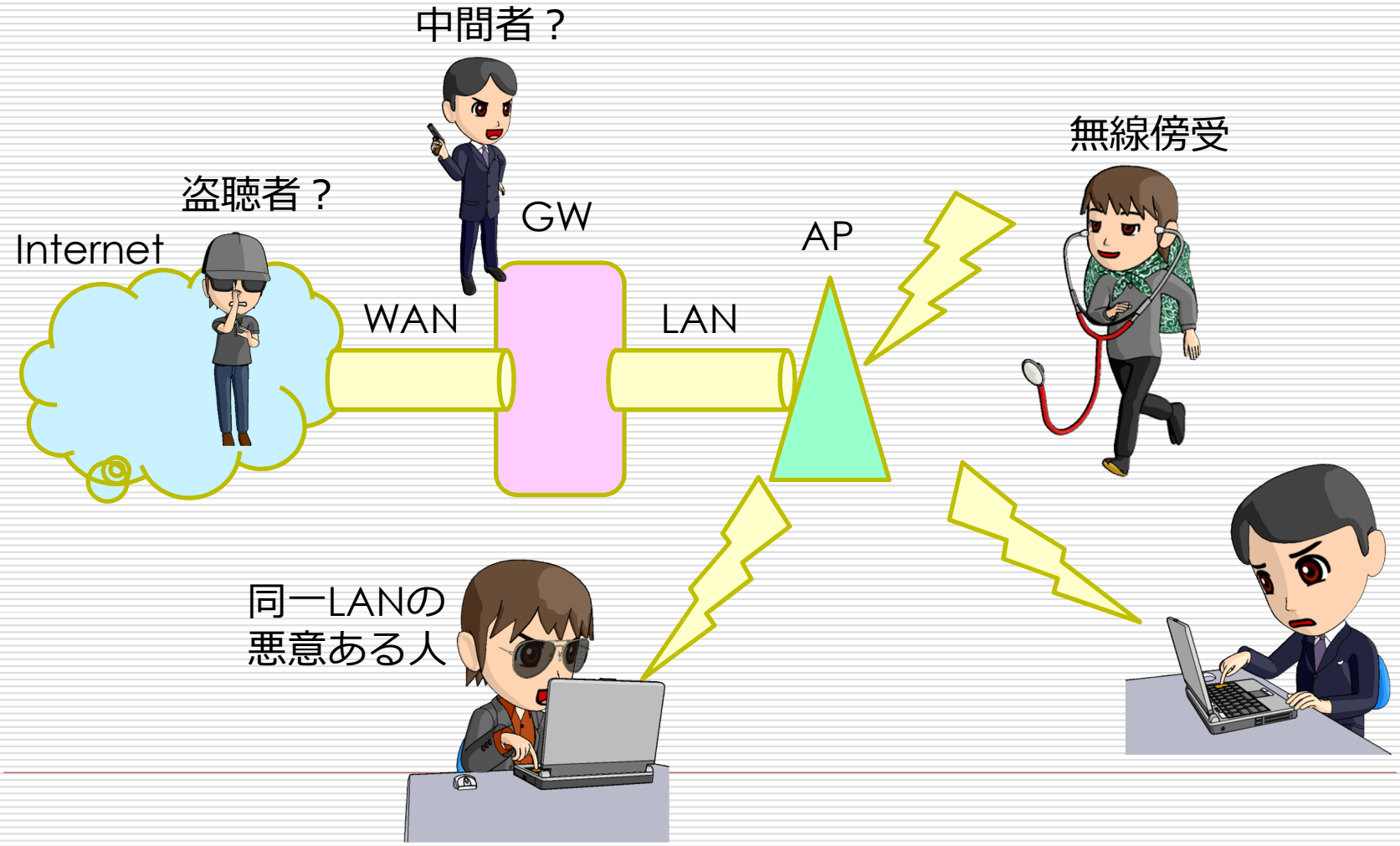
Wi-Fiを巡る【社会的】問題

立命館大学
情報理工学部
上原哲太郎

Wi-Fiは「セキュリティ」が良く話題になるが…どこの話？



問題の整理が多次元

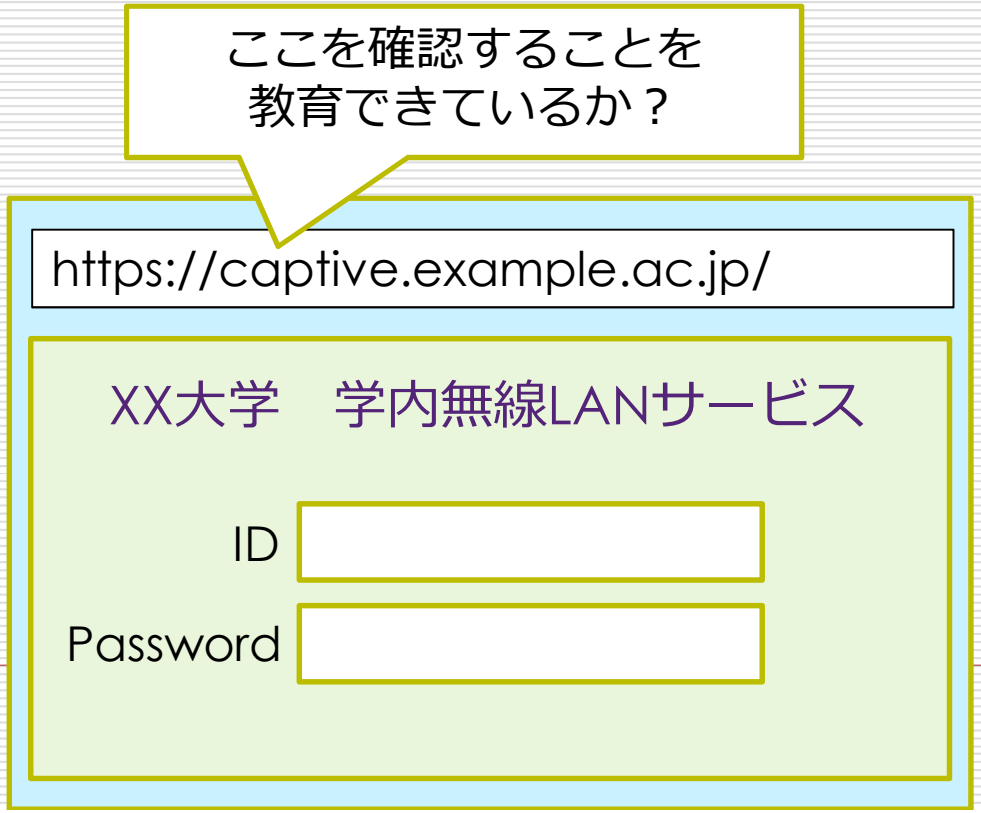
- 組織内無線LAN vs 公衆無線LAN
  - LAN区間に攻撃者がいる可能性の差
- 無線区間 vs 有線LAN以遠
  - 攻撃される場所
  - APの認証・暗号化かGWでの認証か、など
- AP設置者 vs 端末利用者
  - 社会的責任か自衛か
- セキュリティ vs プライバシー
  - 認証突破、盗聴、認証要素窃取…
  - ESSID漏洩、MACアドレス追跡…
  - 認証ログと匿名性（特にROAMING時）

組織内WiFiのセキュリティ

- タダ乗り＆内部LANへの攻撃を防ぎたい
- 認証
  - MACアドレス→詐称が容易／MACランダム化問題
  - 他にID/PW, 電子証明書, ICカード, SIM認証など
- 暗号化
  - WEP→完全に解読ができる
    - Passiveな場合は数十万パケットを要する
      Activeな場合は数万
  - WPA-PSK→パスフレーズが共用なので漏洩に注意
    4way-handshake時のキャプチャデータから
    PSKが総当たりで検索可能
    - TKIP→一部インジェクションが可能
    - CCMP(AES)→PSKが漏れなければ安全
  - WPA-Enterprise→ユーザごとの認証を実現
    - 認証も多彩（ID/PW, 証明書, SIM…）
    - 多数の仕様があるため設定が複雑でサポートコストが大きい

WPA-PSK＋Web認証？

- 公衆無線LANでよく使われる方式
- 組織内LANでは大学などに多い



偽Captive Portal問題

統合認証で
ID/PWが共通化されてると
漏洩の被害が深刻に

WPA-PSK+Web認証のその他の問題

- 認証後はMACアドレスを利用して
  セッション管理をするが…
  MACアドレスは固定値で詐称が容易
- 利用者は普通「ログアウト」してくれない
  事実上タイムアウトを使うしかない
- よって認証済みセッションの
  MACアドレスを横取りして
  セッション乗っ取りが可能

ある程度リスクを許容して使うもの
建物への出入り管理がある等の前提

WPA-Enterpriseの認証

- 「寄せ集め規格」なので大変種類が多い
- EAP-TLS
  - サーバクライアント双方向に電子証明書で認証
  - 中間者攻撃に強い
- EAP-TTLS
  - サーバ側は電子証明書で認証
    クライアントはID/PW
    （オプションで電子証明書）
  - ID/PWのみ利用時は電子証明書の確認を
    厳密にしないと中間者攻撃の危険
- PEAP/MS-CHAPv2 (単にPEAPとも)
  - サーバ側は電子証明書で認証
    クライアントはID/PW　ほぼMS独自仕様
  - MS-CHAPv2に脆弱性が見つかったが…
    - PPTPでは危険だがPEAPではそれほどでもない

公衆無線LANの種別

- キャリア等が行う有料サービス
  - 課金があるので利用者認証必須
  - ただし従量課金でない場合が多い
- 他のサービスに付帯する有料サービス
  - ホテルでの有料サービスなど
- 他のサービスに付帯する無料サービス
  - ホテルでの無料WiFi、喫茶店
    ショッピングモール、コンビニ…
- 自治体等が行う無料サービス

公衆無線LAN提供時の考慮点

- 利用者認証のありかた
  - 課金のため／無料でも使いすぎ防止のため
  - 利用状況を利活用したい（vsプライバシー）
  - プロバイダ責任制限法への対応のため
  - 警察等からの照会への対応のため
- 提供者視点から見た不正利用防止
- 利用者保護としてのセキュリティ
- プライバシー

全てに「通信の秘密」がかかってくることに注意！

公衆無線LANの利用者認証

- Web認証
  - 対応機種が多い・サポートコストが低い
  - 偽AP/CPやセッション横取りに弱い
- WPA-Enterprise
  - ID/PW(EAP-TTLS, PEAP)が大勢
  - SIM認証(EAP-SIM)がスマホで流行
- 一部でアプリケーションによる認証
  - 実態はさまざま（Web, WPA-Enterprise…）

公衆無線LANのアカウント管理

- 独自アカウント
  - ID/PW
  - SIM認証
- ローミング（特に有料サービス）
- SNS等の外部認証（特に無料サービス）
- メールなどを用いた一時アカウント付与
- アカウント管理なし
  - 認証なし／チケット制など

携帯キャリアに広がるEAP-SIM認証

- 3大キャリアがそれぞれEAP-SIMに対応
  - NTTドコモ: 0001docomo
    KDDI: au Wi-Fi2
    Softbank: 0002softbank
- セキュリティ上も強固
- 認証が高速になりWi-Fiオフロードがシームレスに
  - 将来のLTE over WiFiへ
- これに将来IEEE 802.11aiが加われば…

参考： IEEE802.11ai

- 旧名WI-FILS (Fast Initial Link Setup)
- 従来はレイヤ下層から順にリンクを確立
  - Wi-Fiにおけるリンク確立
    (Assoc Req→4way handshake…)
  - DHCPで自己IP取得、経路確立
    DNSサーバを取得　ARPでIPとMACを紐づけ
  - DNSでサーバのIP取得…
  - ここまでで数十往復のパケットが行きかう！
- これをまとめて行えば数往復で済む
  接続が劇的に高速化

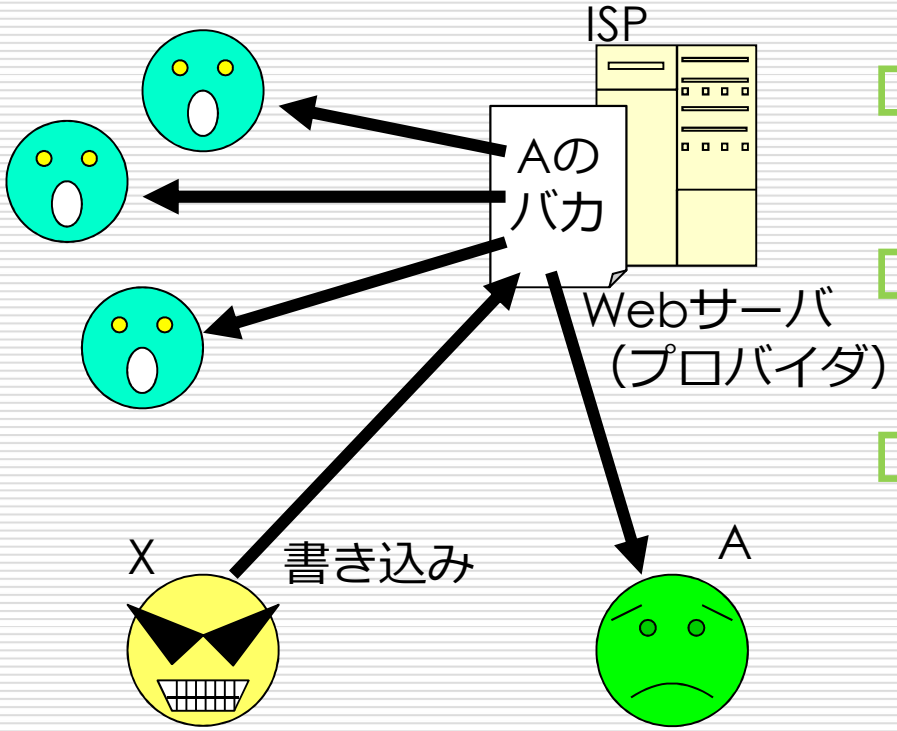
無料サービスにおける認証の必要

- プロバイダ責任法上の要請
  - 利用者による「権利侵害」があった際に「発信者情報」の開示手続きをとることで免責が受けられる
  - 逆に発信者情報を保持していないと手続きが取れないので免責が受けられない
- 警察からの発信者情報開示要請
  - 令状なしの場合（捜査関係事項照会）
  - 令状ありの場合（裁判所からの開示命令）

参考：プロバイダ責任制限法とは

特定電気通信役務提供者の損害賠償責任の制限及び
発信者情報の開示に関する法律

- 例えば、Webで誹謗中傷があった場合



- Aは書き込みを消してほしい
- Aは書き込みが誰か知りたい
- しかしISPは簡単に開示できない
  - Xは誰か＝通信の秘密
  - Xの書き込み
    ＝Xに所有権がある

違法なら警察や裁判所が出られるが判断が難しいとプロバイダは動けない
しかし権利侵害を放置するとプロバイダ自身が責任を問われる可能性がある

参考：
プロバイダ責任制限法の仕組み

- 権利侵害があると認めたとき・・・
  - 削除（発信の停止）の概要
    - 発信者に発信停止してよいか聞く（7日間の猶予）
      - 返事がなければ発信を停止してもよい
    - この手順で停止した場合、情報発信者に対して損害賠償請求を受けてもプロバイダは免責される
    - 停止しなくても権利侵害に関してプロバイダは免責される
  - 開示の概要
    - 発信者に開示してよいか聞く
    - 開示の同意が得られなければ裁判へ
    - 開示しなくてもプロバイダは免責

警察vs無料Wi-Fi 京都の場合

2015.9.20 11:00

文字の大きさ 小 中 大 印刷

【関西の議論】

「セキュリティー甘すぎやおまへんか」京都の無料ＷｉＦｉに警察の〝教育的指導〟　訪日客増「切り札」に暗雲？

ツイート おすすめ 541 G+1 23

（1/4ページ）【関西の議論】

ＪＲ京都駅の観光案内所でスマートフォンを操作する外国人観光客＝京都市下京区のＪＲ京都駅

京都市を訪れる外国人にとって長年、不満ナンバーワンといわれてきたのが、公衆無線ＬＡＮ「ＷｉＦｉ（ワイファイ）」の環境がもの足りないこと。京都市は市の中心部に無料ＷｉＦｉの整備を始めたのだが、この取り組みに思わぬところから「待った」がかかった。「犯罪に悪用されかねない」という京都府警だ。セキュリティーが弱いＷｉＦｉを通じて、サイバー攻撃や違法なダウンロード、麻薬取引に利用された場合、容疑者の特定が難しくなり、「追跡捜査はほぼ不可能な状態」となるからだという。京都市は、ＷｉＦｉ整備事業を観光客の〝不満解消〟の切り札と考えており、府警からの異例の注文にも当初、利便性を盾に推進の姿勢を見せていたが、徐々にトーンダウン。接続方法の見直しなどの対策を余儀なくされている。

http://www.sankei.com/west/news/150920/wst1509200010-n1.html

産経新聞
関西版
2015/9/20

KYOTO Wi-Fi事案の経緯

- 当初、利用者登録式で展開
  - メールによる認証
- 利用者が伸び悩んだため認証を事実上廃止
  - 利用規約を表示→クリック→MACアドレス記録
- これに京都府警がクレーム
  - 不正利用時に本人追跡ができない
- 現在は基本的にSNS認証に
  - ただし閉鎖空間は認証なし

落としどころはどこか？

- 警察が気にしているのは…
  音声携帯電話/スマホとのバランスの悪さ
  - データSIMやWiFiは本人確認義務がない
- 結局何らかの方法で対象が特定したい
  - 監視カメラ等も含む
- よってAPの設置されている空間が問題
  - 京都の場合はバス停だったので…
- APが他の手段で特定が難しければ
  SNSやキャリアメール等を欲しがる

提供者から見た不正利用防止

- フィルタリング？
  - DoS防止のための帯域制御
  - 特定ポートのフィルタリング
  - Webフィルタリング
  - P2P使用禁止
- 認証による抑止／認証記録の保存
- いずれも「通信の秘密」との関係
  - 正当業務行為
  - 利用者の同意

提供者から見たプライバシー問題

- Webフィルタリングの是非
  - いわゆる違法有害コンテンツフィルタ
  - 匿名掲示板への書き込み禁止
- 利用記録の保存問題
  - 特にMACアドレス記録の問題

あるコンビニのWi-Fi利用規約

当社は、利用者様が本サービスをご利用になる際に、以下の情報（「履歴情報および特性情報」）を取得し、管理し、利用します。

- 本サービスのご利用日時。
- 本サービスのご利用方法。
- 本サービスにより閲覧されたホームページ（XXのWifiサービスにおいて用意された専用サイト内のページ）。
- 本サービスのご利用環境（本サービスをご利用された店舗、OS種別およびバージョン、ブラウザ種別、利用モバイル機種、cookieおよびJavascriptがONであること）。
- 本サービスご利用時の利用者様のIPアドレス。
- 端末の個体識別情報（MACアドレス）。
- 利用者様の登録情報。
- その他、利用者様が本サービスをご利用される過程で当社が知り得た利用者様に関する個人情報。（以下略）

RITSUMEIKAN

あるコンビニの利用規約（続）

当社は、履歴情報および特性情報を以下の目的でのみ利用します。なお、当社が提携先に履歴情報および特性情報を提供する場合は、個人を特定できない統計データに加工したうえで提供するものとします。

- 本サービスの利用者数を調査するため。
- 利用店舗に応じた本サービスを利用者様に提供するため。
- 利用者様に対する本サービスの提供と本サービスの品質向上のため。
- 当社や提携先の商品やサービスの品質向上、新規開発のため。
- 当社や提携先のマーケティングに利用するため。
- 利用者様のお問い合わせに基づき、利用者様の本サービスのご利用状況を確認するため。

RITSUMEIKAN

MACアドレスランダム化（Ephemeral MAC Address）

- iOS 8以降、APへのProbe時のMACアドレスがランダム化される
  - ただし接続時は本来のMACアドレス
- Windows 10でMACアドレスランダム化が実装される
  - デフォルトはオフ　一部NICでは使用不能
  - 同一SSIDには同一MACアドレスという実装
    - さらに毎日変更するオプションもあり
- IEEEでも802.1委員会で議論？

端末利用者の社会的責任？

- 「悪いことはしない」は当然
- 「適切に自衛する」も必要
  - PCのマルウェア対策
  - 不用意に共有フォルダ等を開かない
  - スマホはJB/root化しない
- 「ただしい電波利用」
  - 特に技適問題
  - 他にテザリング時の干渉問題