無線LAN(Wi-Fi)の仕組みとセキュリティについて知ろう

九州大学 情報基盤研究開発センター
笠原 義晃

自己紹介

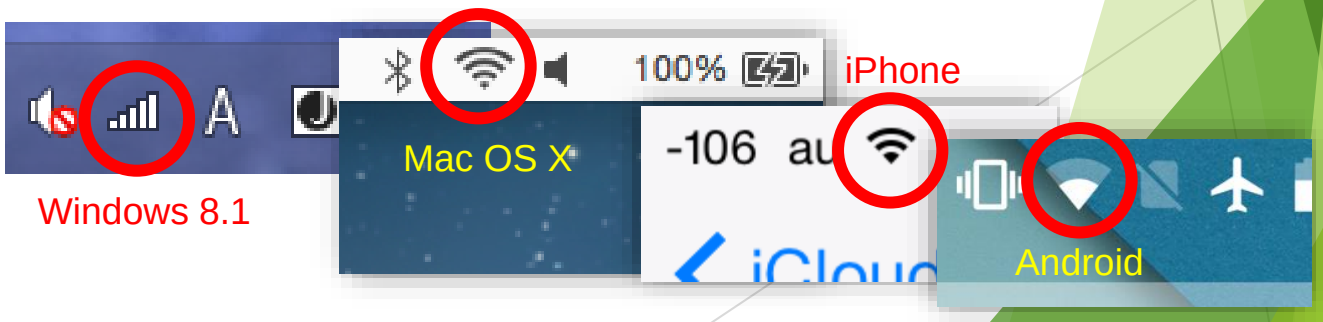
- 九州大学 情報基盤研究開発センター 助教
- インターネット上の基盤サービスの運用管理に従事
  - 電子メール
  - Webサーバ
  - DNSサーバ
  - プライベートクラウド
  - 等々…
- インターネット運用管理、情報セキュリティの研究

本日の内容

- インターネットを利用する際の端末からの「最初の一歩」となる無線通信について
  - 仕組み
  - 危険性
  - 利用時の留意点

無線LAN（Wi-Fi）について

- 皆さんが使っているパソコンやスマホをネットワークに接続している仕組みの一つ
- スマートフォンや携帯の「3G」「4G」「LTE」「Xi」などとは別の仕組み
- ほとんどのスマートフォンは両方使える
  - 「ガラケー」では使えないことが多い
- 扇型のマークで表現されることが多い



Wi-Fi って？

- IEEE802.11規格（後述）に基づいた無線LAN機器
- 実は「Wi-Fi Alliance」の登録商標
- この団体が認定した機器には「Wi-Fi Certified」のロゴが付けられる
  - 他の Wi-Fi 機器と問題なくつながるかどうかの試験を通過している証拠
- 現在ほぼ「無線LAN」と同義で使われている

無線LAN（Wi-Fi）のメリット

- 家庭で利用する場合（家にネットがある前提）
  - ケーブルを引き回さなくていい！
  - 家族みんなで使えて機器が増えても追加の出費がない
  - パソコン、スマートフォン、タブレット、ゲーム機、プリンターなどなど、Wi-Fi の普及で対応する機械が増えている
- 携帯電話網の通信量制限を気にしなくていい
- Wi-Fi でしかできないことがある
  - iPhone のアップデートやサイズの大きなアプリのダウンロード、iCloud へのバックアップなど
- 海外など携帯網が使えない場合にはWi-Fiを使いたい
  - 携帯のローミングは高額

たくさん規格がある

名称	周波数	通信速度
802.11b	2.4GHz	11Mbps
802.11a	5GHz	54Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4/5GHz	65~600Mbps
802.11ac	5GHz	290M~6.9Gbps

- IEEE （アイトリプルイー）802.11 - 無線LAN標準規格
  - The Institute of Electrical and Electronics Engineers, Inc.
- 同じ規格を使っていないと通信できない
  - 複数の規格に対応している機器も多い

無線LANが使う周波数帯

- 2.4GHz 帯 （ISM バンド） (ISM: Industry-Science-Medical)
  - 小出力なら免許・許可なしで利用できる周波数帯
  - 電子レンジの使う周波数とかぶっている
- 5GHz 帯
  - 日本では一部気象レーダー等とかぶっている
    - 屋外での利用が一部制限されている
- 周波数が低い方が透過力が強く遠くまで飛ぶ
  - 2.4GHz より 5GHz の方が壁などで止まりやすい
- 2.4GHz はより「汚れている」
  - 無線LAN以外にも使っている機器が多いため

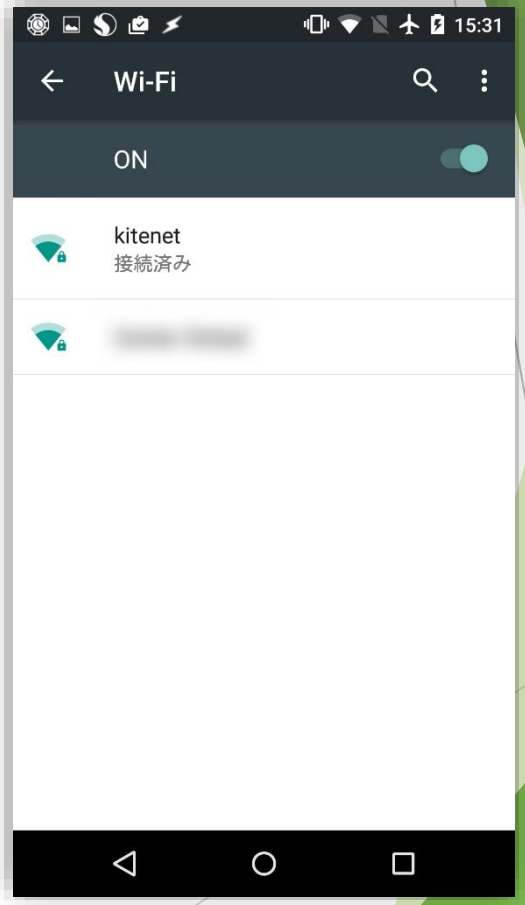
無線LAN

SSIDとチャンネル

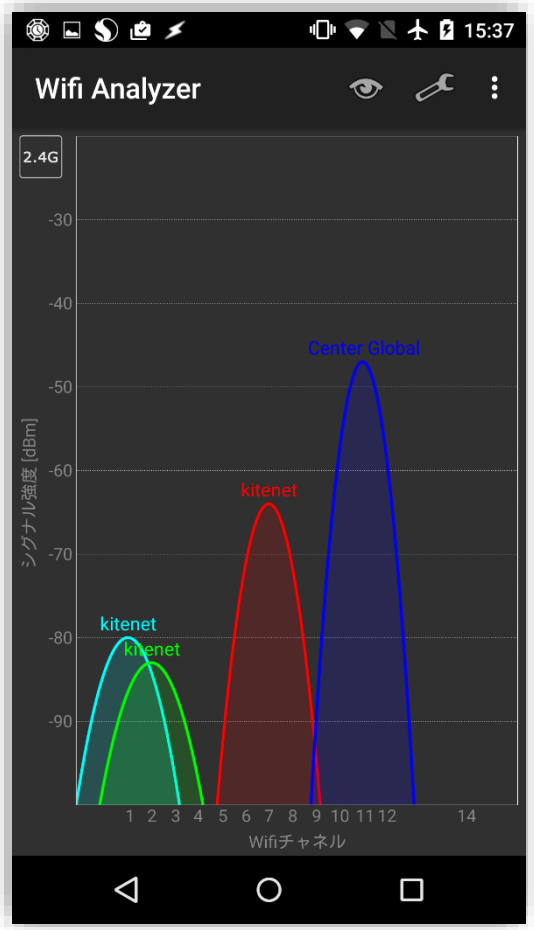
- チャンネルとSSIDで接続先が決まる
  - 基地局のチャンネルは通常固定
    - テレビのように番号がついている
      - 1ch, 2ch, 3ch…
  - 子機は自動でスキャンして基地局を探す
  - SSIDはネットワークの名前
    - 同じチャンネルでもSSIDが違えば違うネットワーク
    - (SSID: Service Set Identifier)

SSIDの見える様子

-101 au
15:25
設定
Wi-Fi
Wi-Fi
kitenet
ネットワークを選択...
eduroam
その他...
接続を確認
接続したことのあるネットワークに自動的に接続します。接続したことのあるネットワークが見つからない場合は、手動でネットワークを選択する必要があります。


15:31
Wi-Fi
ON
kitenet
接続済み

チャンネル



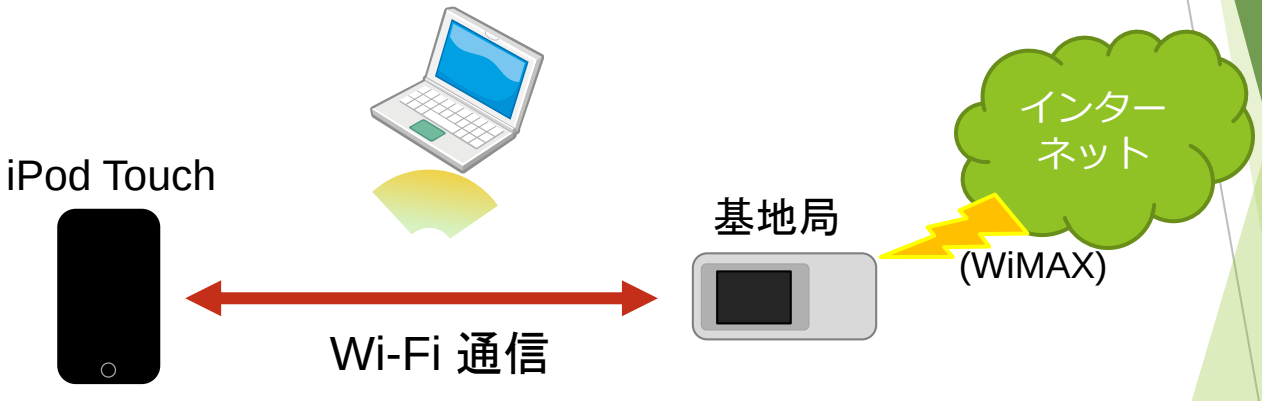
- 2.4GHz帯は13チャンネル
- 上下2ch分強重なっている
  - 干渉させたくないなら3~4つしか取れない
- 5GHz帯はもともと重ならないようにチャンネル割当（詳細略）
  - 最大19チャンネル

無線LANと暗号化

- 電波なので届けば誰でも受信可
  - 携帯電話も無線だが、暗号化の仕組みがあり無線区間の盗聴の心配はまずない
  - 無線LANは条件によって簡単に盗聴可能
- パスワードも何もなしでつながる無線LANは基本的に盗聴し放題
  - 暗号化対応かどうかは基地局の設定次第
  - 子機（みなさんのスマホなど）は基地局の設定に従うしか無い
- パスワード保護でもそのパスワードが相手に知られていると盗聴可能な場合がある

デモ

- 実際にWi-Fiの通信をパソコンで覗いてみます
  - パソコン: MacBook Air
  - 使用ソフト: 無料で手に入る Wireshark



- 持参した基地局の都合により簡単なセキュリティ（WEP）がかかっている通信を盗聴
  - 鍵はわかっていると仮定

無線LANのセキュリティ

- WEP: Wired Equivalent Privacy
  - 事前に設定した共有キーで接続・暗号化
  - 暗号キーの保護が弱く危険性が高い
- WPA: Wi-Fi Protected Access
  - WEP に代わるべく作られた
  - 古い機械でも使えるように設計された規格
- WPA2: Wi-Fi Protected Access 2
  - 現状で一番強い規格
  - 強い（処理が複雑な）暗号を使っているので古い機械では使えないことがある

無線LANの安全性

強い

弱い

WPA2

WPA(Wi-Fi Protected Access)

保護なしも同然

WEP(Wired Equivalent Privacy)

保護なし

WPA/WPA2

- WPA/WPA2 は複数の認証・暗号方式が使える
- 家庭用基地局では PSK が一般的
  - Pre Shared Key （事前共有鍵）
    - Personal という表記の場合もある
  - 接続しようとするとパスワードだけを聞かれる
- 九州大学では Enterprise という方式を利用
  - 接続しようとすると個別のユーザ名とパスワードを聞かれる
  - 共通の鍵を使わないので他人の盗聴は困難
  - 別途認証サーバなど必要で会社向け

自宅に基地局を置く場合の留意点

- 他人のただ乗り
  - 違法行為に利用されて犯人扱いされる危険性
- 他人からの盗聴
  - 自分の情報が盗まれるかもしれない
  - 家族にも被害が及ぶかもしれない

- これらを防ぐためにセキュリティ機能を有効にする

自宅に基地局がある人は

- セキュリティを WPA2-PSK に設定する
  - 対応していない古い基地局は買い換えたほうがいいかも
  - 子機が対応していない場合は WPA-PSK もやむなし
    - 基地局で両対応にできる場合もある
  - WEP やパスワードなしでは使わない
- パスワードの長さは長いほうがいい
  - SSIDから類推できないようにする
  - WPA/WPA2-PSK では 8～63 文字で設定可能
- SSIDは無理に変えなくてもいい
  - 最近の製品は機器ごとにランダムな文字列が入っているため

よその基地局を使う場合

- 無料の公共無線LAN
  - てんちかWi-Fi、Fukuoka City Wi-Fi
  - コンビニ系
  - カフェ等
- 有料・契約が必要な無線LAN
  - 携帯キャリアの提供する無線LANなど
- ホテルなど顧客のみ利用できる無線LAN
  - チェックインすると接続方法を教えてくれる等

主に使われている認証方法

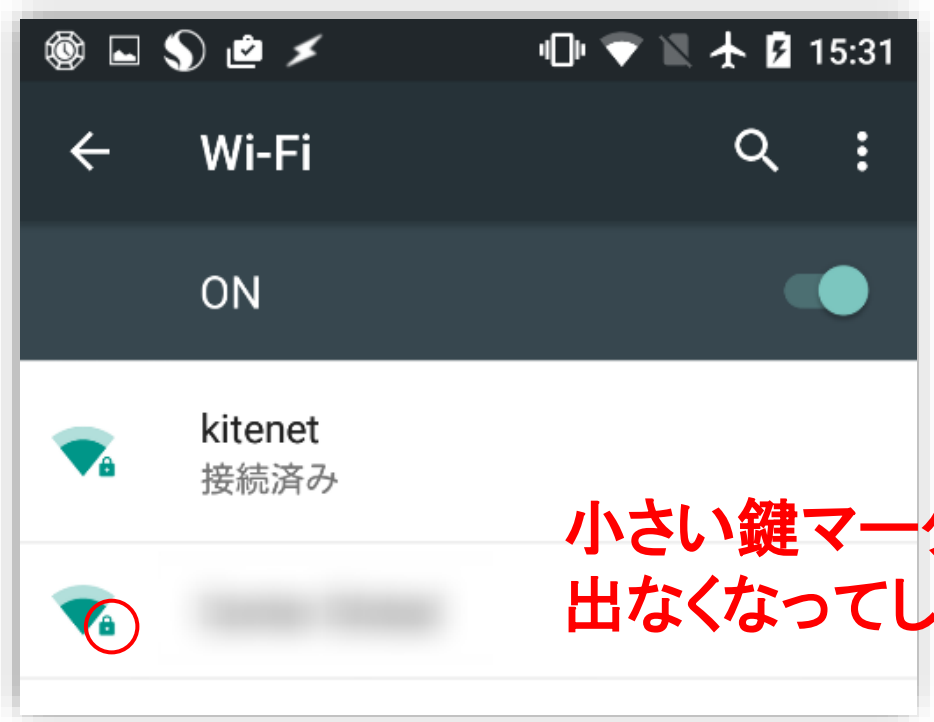
- なにも認証なし
  - SSIDさえわかればつながる
  - 利便性重視、まずつながることが重要という場合
- 無線LAN認証なし＋ウェブ認証
  - 無線にはつながるが、インターネットにはつながらない
  - ウェブ画面で必要な情報を入力すると外に出られるようになる
    - ここで料金を支払ったりする場合もある
- WEP/PSK（＋ウェブ認証）
  - SSIDに加えてパスワードが必要
  - さらにウェブ画面での操作が必要な場合もある
- より強固な方式
  - Enterprise 型（事前にユーザ名・パスワードを登録）
  - 携帯の契約情報を利用するもの

基地局の設定を確認する

- 今からつなぐ基地局がどんな相手かわからないことには使っていいか判断できない、が…
- 最近の端末では情報出ない方向に行っているみたいでちょっと困る☹

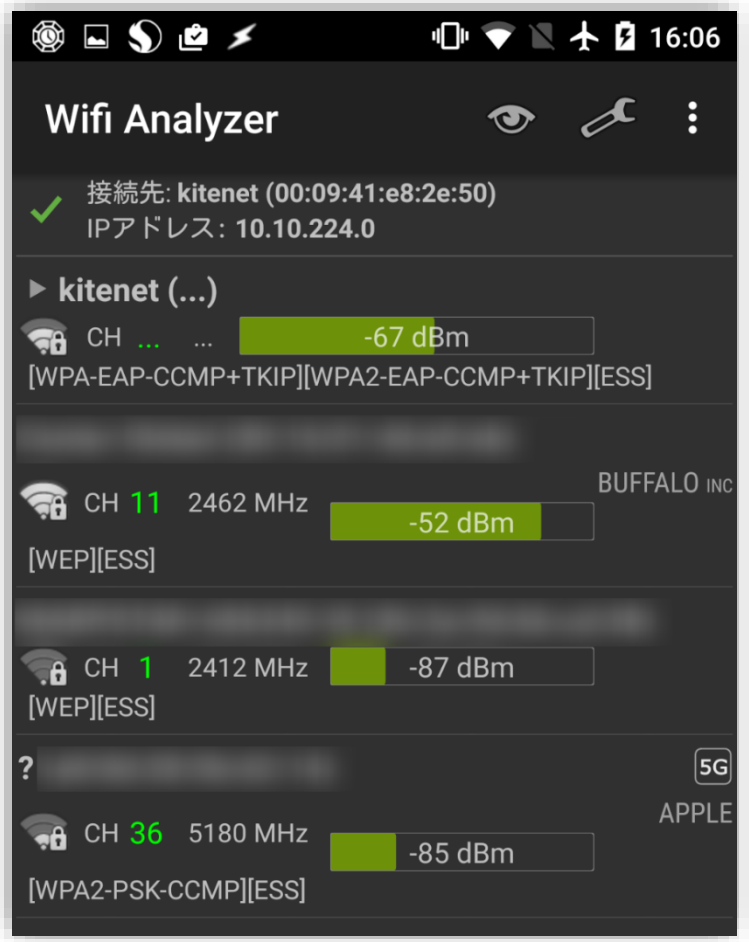
Androidでの確認例

Android 5 (Lollipop)



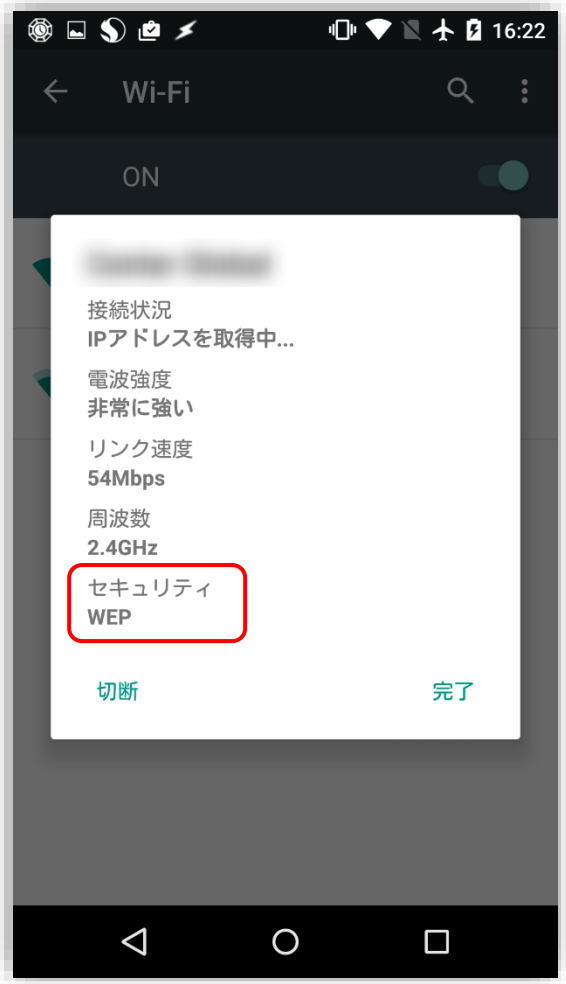
小さい鍵マーク以外
出なくなってしまった…

Wi-Fi Analyzer (Android アプリ)



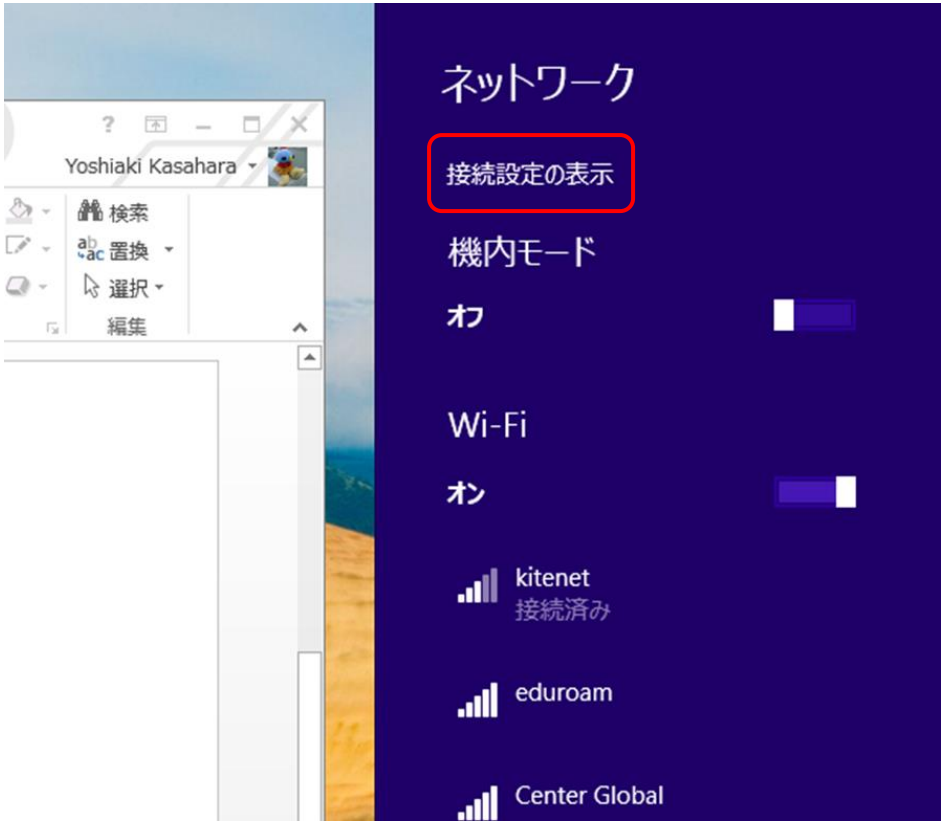
http://wifinalyzer.mobi

接続後なら表示できる


16:22
Wi-Fi
ON
接続状況
IPアドレスを取得中...
電波強度
非常に強い
リンク速度
54Mbps
周波数
2.4GHz
セキュリティ
WEP
切断
完了

16:23
Wi-Fi
ON
kitenet
接続状況
接続済み
電波強度
強
リンク速度
48Mbps
周波数
2.4GHz
セキュリティ
802.1x EAP
切断
完了

Windows 8.1
（なにもわからない…）



Windows 8.1 も接続後ならわかる

Mac OS X は結構詳しくわかる

- option キーを押しながら扇アイコンをクリック
- 接続している無線基地局の詳細情報が表示される

- option キーを押したままマウスポインタを SSID の上に移動すると接続していなくても詳細が見える

気にする人は…

- 以下のSSIDは強い仕組みなので比較的安全
  - 0001docomo
  - au_Wi-Fi2
  - 0002Softbank
- ただし docomo 以外は携帯の契約がある端末しか使えないらしい

- 認証なしはなるべく避ける
  - それしか接続手段がない場合はやむを得ない
- PSKでもパスワードがわかれば盗聴可能
  - 公共無線LANの場合公開されている場合もあるため

無線LANは有線より弱いもの

- 現状、公共無線LANは他に自分で対策していない場合盗聴されてもしかたないと思うしかない
  - 利用規約にも「盗聴される恐れがあるので自己責任で利用してください」などと書いてある
- 通常大事な通信は別の方法で暗号化されている（はず）
  - インターネット自体も盗聴の可能性はあるから
- 後で少し紹介

「野良無線LAN」の危険性

- 鍵のかかっていない、公衆向けでない無線LANを見つけることがある
  - 鍵がかかっていないので、接続すると使えそうに思えるし、実際使えることも多い
- 誰が設置したかわからない、悪意があるかも？
  - 盗聴・偽サイトに誘導等の危険性
- 素性の分からない無線LANは利用しない

デモ２

- 正しい名前を入力しても偽ページに接続されてしまう様子
  - 簡単のためこのデモではパソコン自体に細工してます
- 無線LANで接続すると、基地局から接続先の探し方を教えられる
  - 嘘を教えられても気づかないかもしれない
- 素性のよくわからない基地局（SSID）には接続しない

サーバとの通信の暗号化

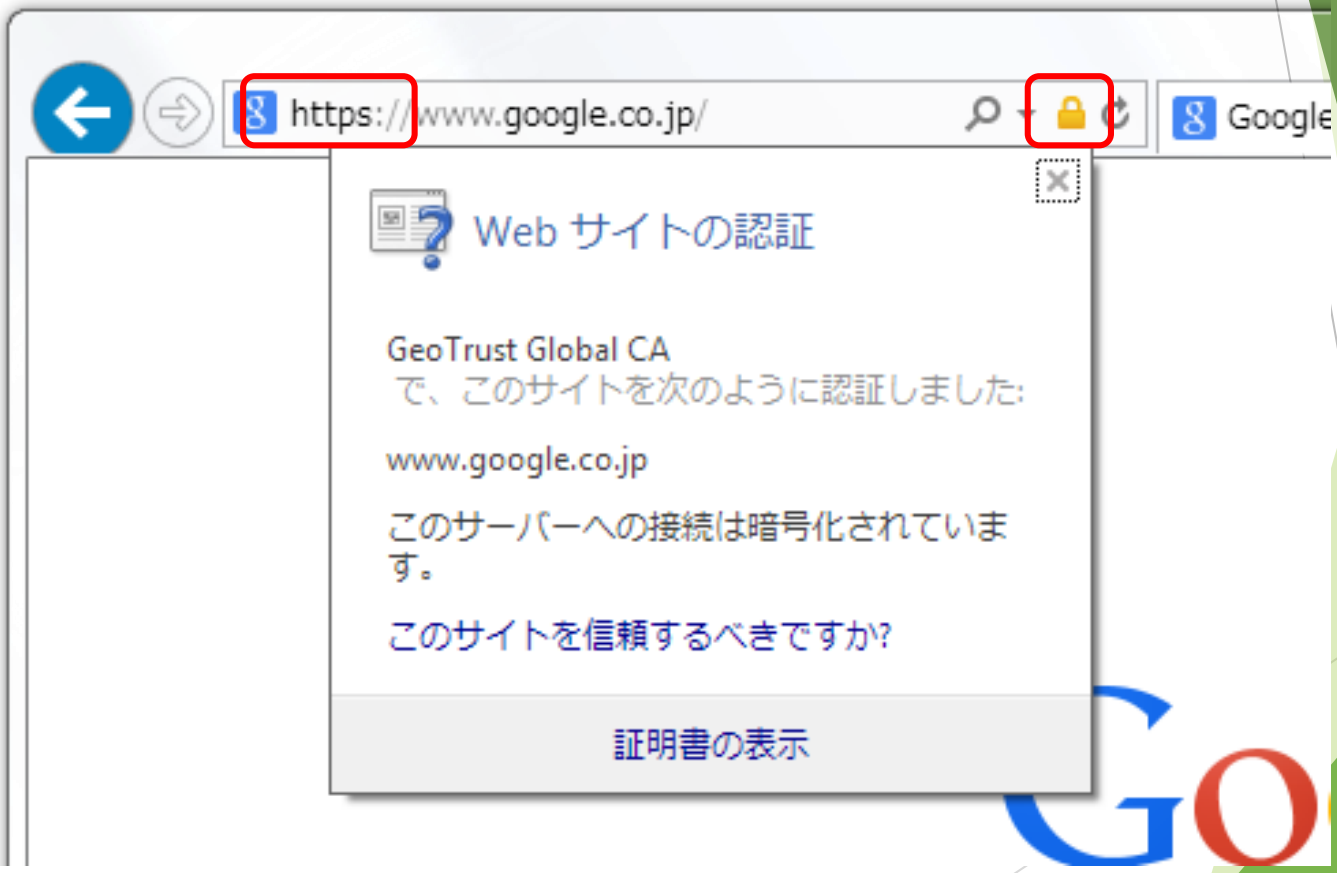
- インターネットは盗聴されている可能性がある
- 無線LANも盗聴されているかもしれない

- 多くのサービスでサーバとの通信を暗号化可能
  - 盗聴されても内容がわからないようになる

- 接続先が本物のサーバかどうかわからない時は警告が出る

通信の暗号化

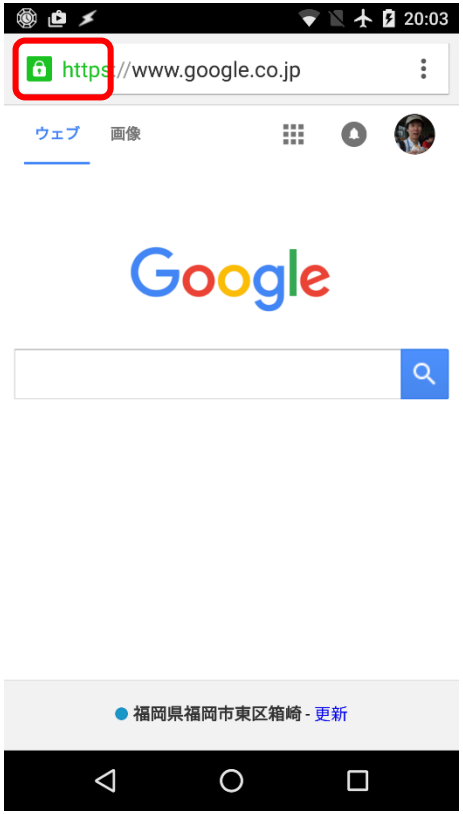
ウェブの暗号化（https）（Internet Explorer）



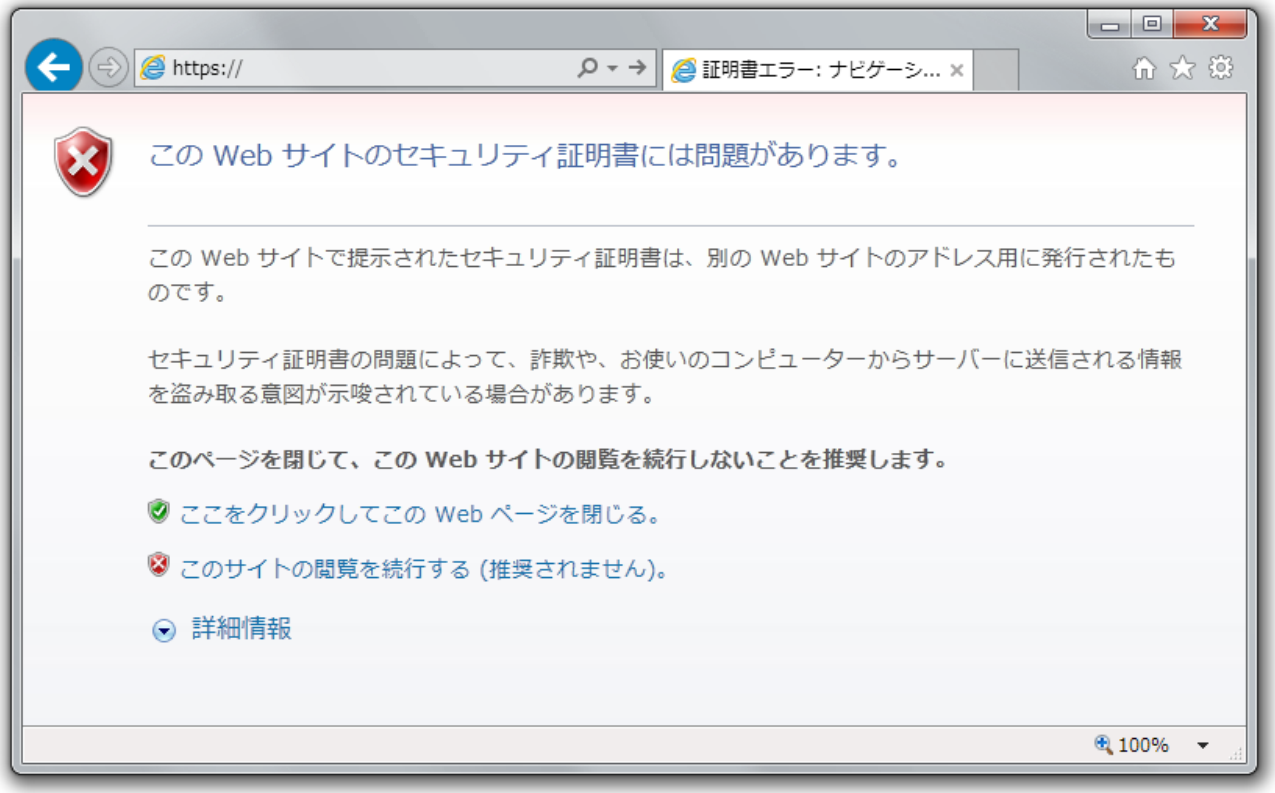
ウェブの暗号化（Google Chrome）

ウェブの暗号化（iPhone Safari）

ウェブの暗号化（Android Chrome）



偽サイトの警告画面（Internet Explorer）

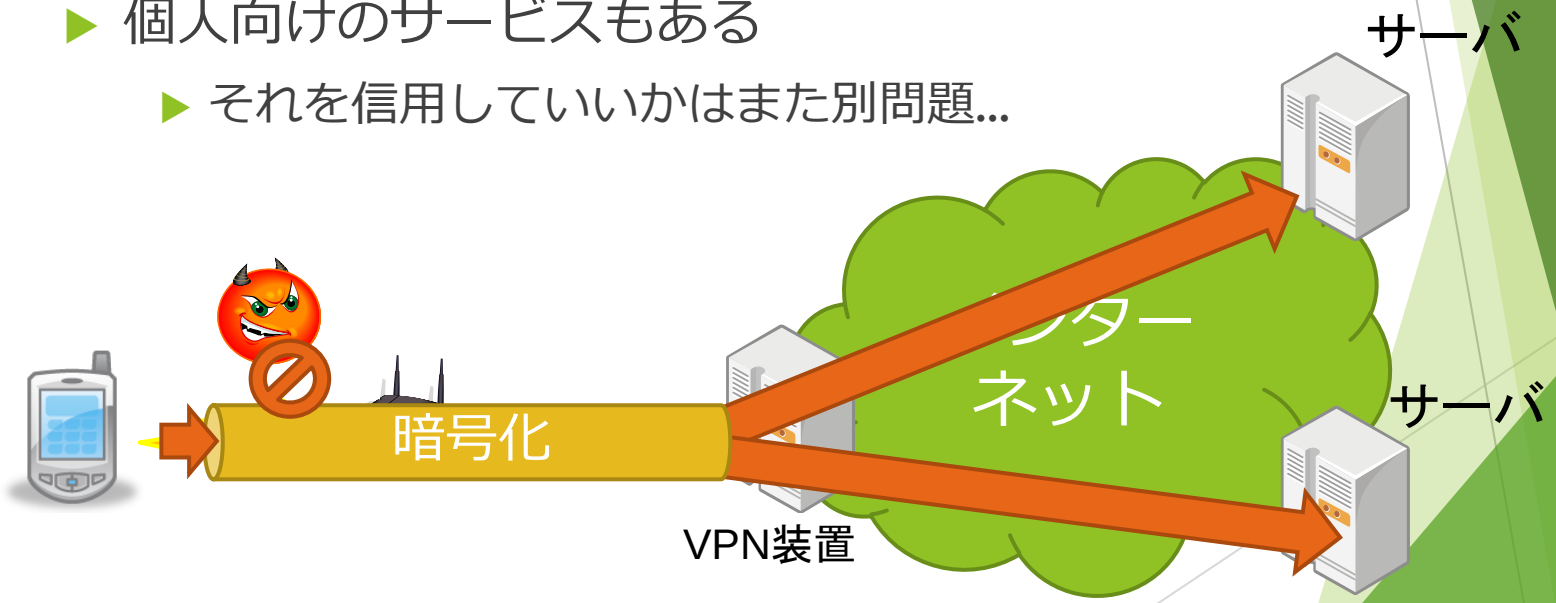


アプリは？

- 一見してわからない
  - 裏でウェブの通信をしている物が多い
    - ログイン処理などは https を利用している…はず
- 本当に暗号化しているかどうかは、通信をのぞいてみないとわからない
  - 正しく相手サーバを検証していないアプリも
    - 偽サーバに接続しても気づかないかもしれない

企業の人とかどうしてるの？

- VPN接続（Virtual Private Network）
  - 端末と、会社などにあるVPN接続装置の間で暗号通信する仕組み
    - 無線を盗聴できても暗号化されていて読み取れない
  - 個人向けのサービスもある
    - それを信用していいかはまた別問題…



まとめ

- 自宅の無線LANには鍵をかけよう
  - ただ乗りされたら面倒なことになるかも
  - 盗聴もできるだけ避けたい
- 公共の無線LANを使う時には「もしかしたら盗聴されるかも」とちらっと考えよう
  - 現実的に確率は高くないだろうが…
  - インターネットバンキングなどは家に帰ってから
  - 見慣れない警告画面には気をつける
- 無線LAN自体は便利な技術なので、上手に使いたい
- 今後サービス個別の暗号化も進んでいくでしょう