2年次演習

第11回
セキュリティ

人間科学科コミュニケーション専攻
白銀 純子

第11回の内容

- セキュリティのおはなし

セキュリティのおはなし

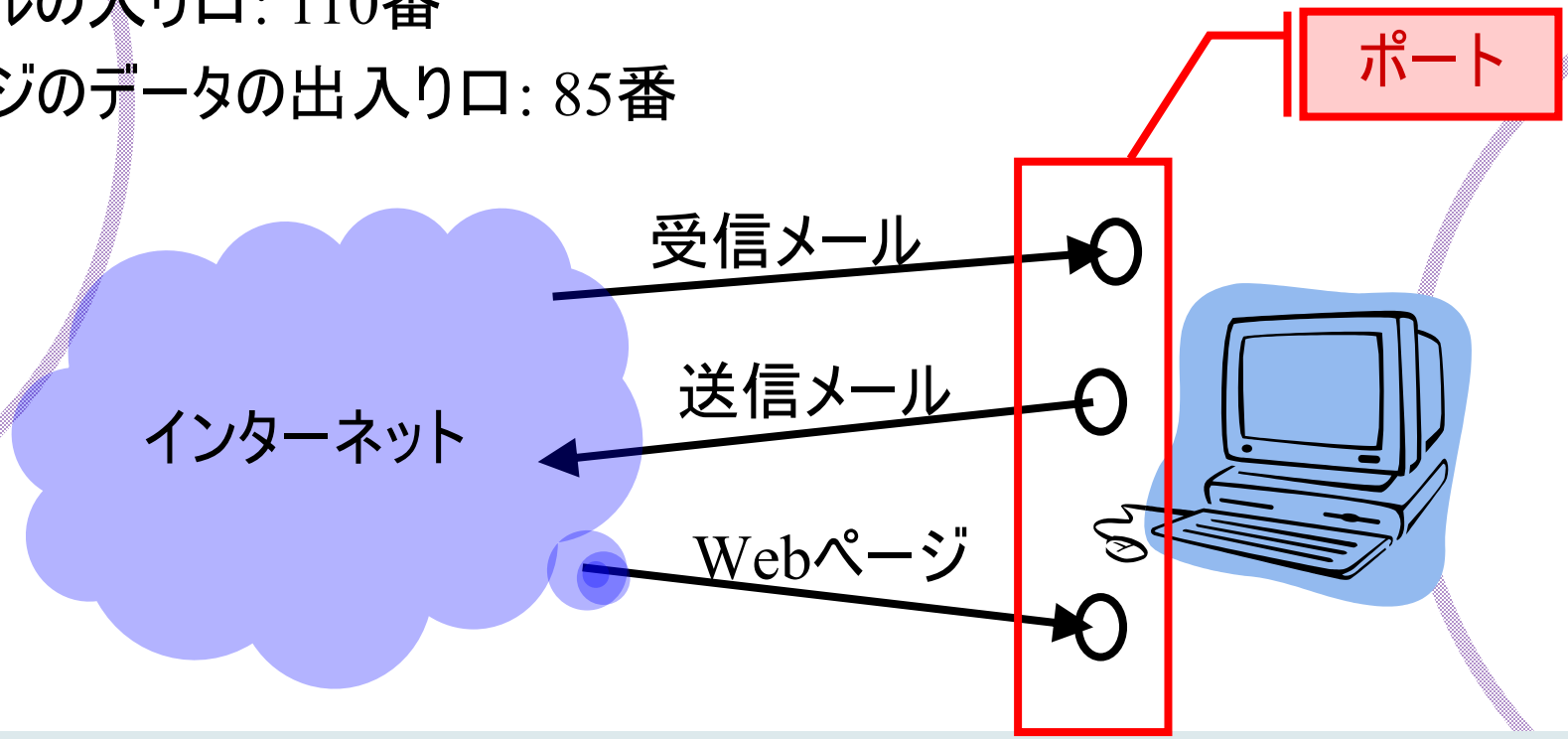
ユーザビリティとセキュリティ

- ユーザビリティとセキュリティは常に対立関係
  - Ex. パスワード
    - ない方がいちいちログインしなくてめんどくさくない
    - なければ、第三者に悪さをされる可能性がある
  - Ex. 情報の持ち歩き
    - USBメモリに入れて自宅に持ち帰れば自宅でも作業ができる
    - 自宅に持ち帰ると紛失の可能性があるので、仕事場からの持ち出しは禁止する

セキュリティ事案

ネットワークでのデータのやり取り

- 「IPアドレス」と「ポート」を使ってデータをやりとり
  - IPアドレス: インターネット上でのコンピュータの住所
  - ポート: コンピュータへのデータの出入り口の番号
    - 電子メールの出口: 25番
    - 電子メールの入り口: 110番
    - Webページのデータの出入り口: 85番
    - etc.



不正アクセス

- あるコンピュータが、所有者の意図しない操作をされること
  - データが盗まれる
  - システムが破壊される
  - etc.
- 不正アクセスは、開いているポートを使って行われる
  - 攻撃対象のコンピュータの、開いているポートの有無を調査(ポートスキャン)
  - 開いているポートが見つかったら、そこを突破口にして対象のコンピュータに攻撃

不正アクセスを防止するには?

- 不要なポートを閉じておく
  - どのポートが必要で、どのポートが不要かの判断が難しい
- ファイアウォールを導入
  - ファイアウォール: コンピュータに出入りするデータを監視して、許可されているデータのみ通すためのソフトウェアや機器
    - 許可されていないものは廃棄
  - 個人のPC用のファイアウォールソフトもたくさんあり、簡単に導入可能
    - Windowsに付属
    - 各種ウィルスソフトにも付属
    - etc.

ユーザビリティとの対立点
- 開けていないポートでの通信ができない
  - ✓ 時々、特殊なポートで通信するものがある

マルウェア

- マルウェア: 悪意を持って不正な動作をさせるようなソフトウェアの総称
  - コンピュータウィルス
  - スパイウェア
  - etc.

コンピュータウィルス

- コンピュータを病気のような症状にするための一種のソフトウェア
  - データなどを破壊する
  - 自動的に自分自身のコピーをたくさん作り出す
  - コンピュータの利用者に特定の動作をさせない
    - 特定のページ(特にウィルスソフトのメーカーのページなど)へのアクセス
    - etc.
  - etc.

ウィルスの主な感染方法(1)

- メールの添付ファイルから感染
  - メールに添付された画像や文書などのふりをしたウィルス
  - 添付ファイルを開くことで感染
  - メールソフトのアドレス帳などを利用して、自分自身のコピーを勝手に他人に送りつけるものが多い
- Webページにアクセスすることで感染
  - 公開されているWebページのシステムに感染し、Webページを勝手に書き換え
  - 書き換えられたWebページにアクセスすると、アクセスしたコンピュータが感染
  - 電子メールで自分自身のコピーもあちこちに送信

ウィルスの主な感染方法(2)

- ネットワークに接続することで感染
  - 自宅などのネットワークの環境によっては、PCの電源を入れただけで感染
  - ネットワークに接続して稼動しているコンピュータを探し、そのコンピュータに自分自身のコピーを送りつけるタイプ
  - コンピュータが感染すると、コピーを送りつけるだけではない被害も
    - ある特定のコンピュータに攻撃する
    - 感染したコンピュータの不安定化(自動的に再起動を繰り返す、など)

ウィルスの主な感染方法(3)

- マクロから感染(マクロウィルス)
  - マクロ: ある一連の作業を自動的に行えるようにするための仕組み
  - Microsoft Word, Excel, PowerPointなどのOfficeソフトでマクロが利用できることが多い
  - OSを問わず感染するものもあり
    - 通常のウィルスは、OSが違うと感染しないものが多い
    - Ex. Microsoft Wordのファイルについているマクロウィルスは、WindowsでもMacでも感染する可能性

ウィルスに感染しないために

- ウィルスソフトを導入・更新し、ソフトウェアのアップデートをこまめにする
  - ウィルスソフト
    - ウィルスは毎日新しく出てくるので、ソフトを導入しただけでは、新しいウィルスは防げない
    - ウィルスソフトを無料で更新するための権利は、通常90日～半年程度しかない
    - 更新権利が切れると、更新権利(1年分～3年分程度)を購入する必要がある
  - アップデート
    - ソフトウェアは人間が作るものなので、完璧ではない
    - 不具合や、ウィルスが侵入して来やすい穴(セキュリティホール)がたくさんある
    - 不具合やセキュリティホールは、見つかると修正したり埋めるためのソフトウェア(パッチ)が出る

ユーザビリティとの対立点
- ウィルスソフトが常に動いている(常駐している)ので、PCの動作が重くなることがある
- アップデートの作業中にPCが重くなる
  - ✓ アップデートをすると自動的に再起動されることも…

スパイウェア

- コンピュータの利用者に関する情報を集めて、スパイウェアの製作者に送るソフトウェア
  - 利用者の個人情報やインターネットでの行動などの情報を収集
  - 他のソフトウェアにくっついてインストールされることが多い
    - ソフトウェアのインストール時の使用許諾条件に、スパイウェアが何をするかが書かれていることが多い
    - 使用許諾条件にOKしてしまうと、法律上、スパイウェアの活動を認めたことになる
  - トラブルが発生することも多い
    - 個人情報の流出
    - コンピュータの不安定化(スパイウェアがずっと動作し続けるため)

スパイウェアを防止するには?

- スパイウェアのインストールを許可しない
  - ソフトウェアの中には、スパイウェアをインストールしないように指定できるものも
    - ソフトウェアのインストール時に、「標準インストール」などのおまかせモードではなく、「カスタムインストール」などの自分で項目を選択するモードでインストール
- ソフトウェアのアップデートをする
- ウィルスソフトの導入と更新をする
  - ウィルスソフトはスパイウェアにも対応

ユーザビリティとの対立点(ウィルスと同様)

- ウィルスソフトが常に動いている(常駐している)ので、PCの動作が重くなることがある
- アップデートの作業中にPCが重くなる
  - ✓ アップデートをすると自動的に再起動されることも…

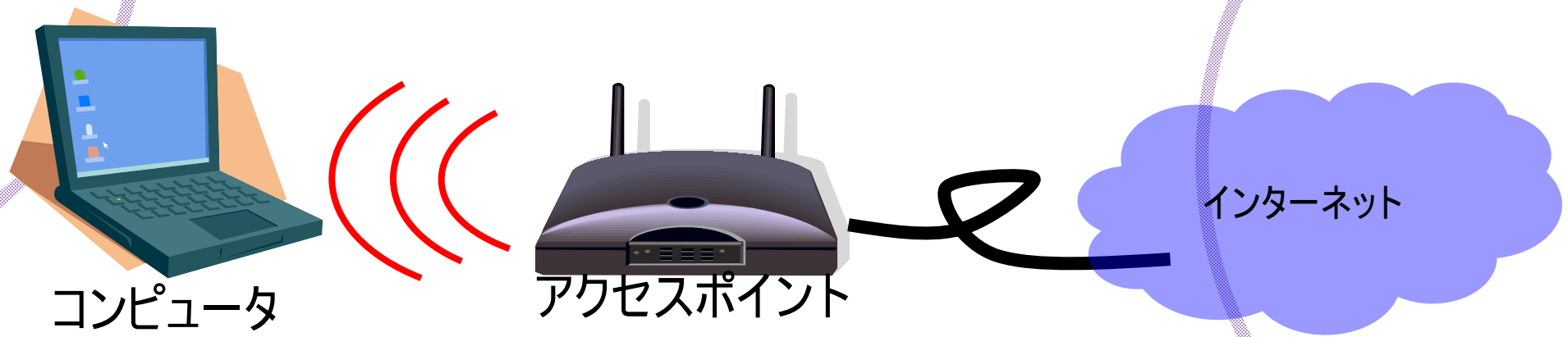
お役立ちサイト

- 各種セキュリティに関する情報や対策方法
  - 情報処理推進機構・セキュリティセンター: http://www.ipa.go.jp/security/
  - JPCERT CC: http://www.jpcert.or.jp/

無線LANのセキュリティ対策

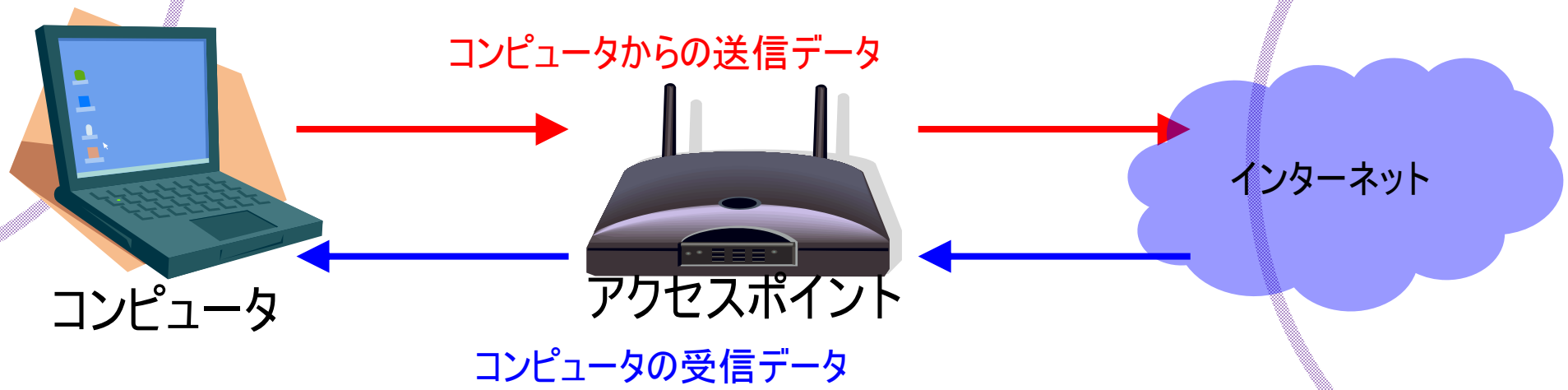
無線ネットワークの仕組み(1)

- アクセスポイントを利用して無線で接続
  - アクセスポイント: コンピュータを無線でネットワークに接続させるための電波を出すための機器
  - コンピュータが電波をキャッチしてネットワークに接続



無線ネットワークの仕組み(2)

- コンピュータからの送信データ: アクセスポイントを通って目的地へ
  - コンピュータ→アクセスポイント→目的地へ
- コンピュータの受信データ: アクセスポイントを通ってコンピュータ内へ
  - データ送信元→アクセスポイント→コンピュータへ



無線LANの怖いところ

- 無線LAN: データのやりとりは電波を利用
  - 人間の目に見えない・においなし・触った感触もなし
    = 誰がどのように使っているか人間の感覚で感知不可能
    = 知らない人に電波を使われて、いたずらされる可能性

- 有線LAN: データのやり取りはケーブルを利用
  - データをやりとり自体は感知できなくても、やりとりを仲介するケーブルを見る・触るは可能
    = 少なくとも、誰が使っているかも感知可能
    = 知らない人に使われて、いたずらされる可能性は低

無線LANは、有線LANとは別のセキュリティ対策が必要

無線LANの不正アクセス

- 無線LANが利用された事件も多数
  - フィッシング詐欺(2015)
  - ウィルス送信(2014)
  - パスワード改ざん(2012)
  - 他人になりすまして嫌がらせメールを送信(2011)
  - etc.

一般家庭の無線LANを勝手に利用し、犯人が逮捕された事件

自宅の無線LANは…
- セキュリティの設定をきちんとしてから利用する

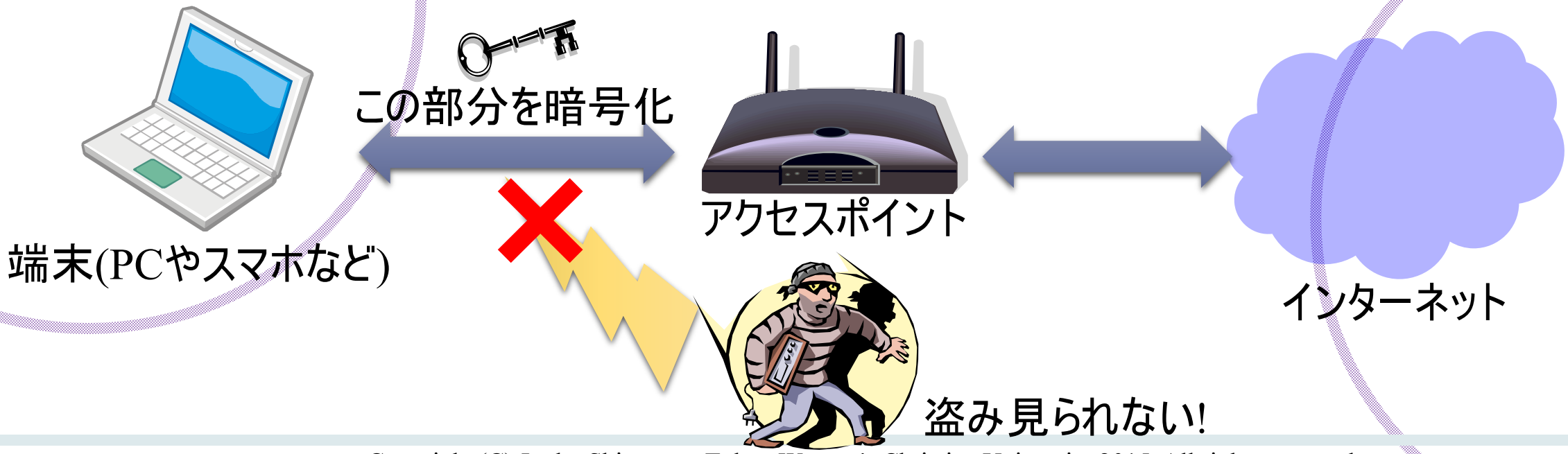
セキュリティの設定がされていない他人の無線LANは…
- 利用しない(勝手に利用すると、不正アクセス禁止法に引っかかる可能性も)

無線LANのセキュリティ対策は?

- WEPキーの設定
- WPA/WPA2キーの設定
- MACアドレス登録
- ANY接続禁止
- 電波の範囲制限

WEPキーの設定(1)

- WEPキー: 無線LANでやりとりされるデータを暗号化するためのキーワード
  - コンピュータ～アクセスポイント間の通信を傍受されても、内容を見られる可能性が低
    - WEPキーを設定しておかないと、コンピュータ～アクセスポイント間の通信を傍受されて個人情報などを盗まれる可能性
  - 無線LANに接続するためのパスワードのようなもの



WEPキーの設定(2)

- WEPキーを使うには?
  - アクセスポイントとコンピュータの双方に設定
    - アクセスポイント側の設定: その無線LANでどういうWEPキーを使うかという設定
      (どういうパスワードを設定するか、の設定)
    - コンピュータ側の設定: アクセスポイント側で設定されているWEPキーの設定
      (無線LANへログインするようなイメージ)
- WEPキーを設定すると…
  - アクセスポイントはコンピュータに設定されているWEPキーをチェック
    - 正しいWEPキーが設定されていれば、接続を許可
    - 正しいWEPキーが設定されていなければ、接続を不許可

WPA/WPA2キー

- WEPキーの欠点を克服するために提供された暗号化の仕組み
  - WEPの欠点: キーを解読されやすい
    - キーの文字数が少ないなどのため
- WPAが先に提供
- WPA2はWPAよりも強力な暗号化の仕組み
- 設定に関してはWEPキーと同じ

MACアドレス登録

- MACアドレス: ネットワークカードごとに設定されている、世界中で一意(他のものと絶対に重ならない)の番号
  - アクセスポイントに設定
- MACアドレスを登録すると…
  - 無線LANに接続しようとしたとき、その無線ネットワークカードのMACアドレスをアクセスポイントがチェック
    - 登録されているカードであれば、接続を許可
    - 登録されていないカードであれば、接続を不許可

ANY接続禁止(1)

- SSIDの利用制限
- SSID: 無線LANを識別するための名前のようなもの
  - ESSIDとも
  - コンピュータは、SSIDを知らない無線LANへの接続は不可能
  - アクセスポイントとコンピュータの双方に設定
    - アクセスポイント側の設定: その無線LANにどういう名前をつけるかを設定
    - コンピュータ側の設定: アクセスポイント側で設定されているSSIDの設定
    - ただしコンピュータ側は、人間が設定するのではなく、コンピュータが自動的にSSIDを感知することも可能

ANY接続禁止(2)

- ANY接続禁止とは
  - コンピュータがSSIDを自動感知することを禁止アクセスポイントに設定

- ANY接続禁止の設定をすると…
  - コンピュータは、SSIDを自動感知が不可能
    = SSIDを知らないコンピュータがその無線LANに接続することは不可能
  - SSIDを知っている(設定されている)コンピュータのみその無線LANに接続が可能

※SSIDはログイン名のようなものなので、ANY接続禁止だけではセキュリティ対策としては不十分

電波の範囲制限(1)

- 電波: 強弱の設定が可能
  - 電波が強い: 電波が届く範囲が広い
  - 電波が弱い: 電波が届く範囲が狭い
- 電波を強くしておくと…
  - 自宅の外まで電波が届いて、外でキャッチされて使われる可能性
    - 自宅の前の道路
    - アパート or マンションの近所の部屋
    - etc.

電波の範囲制限(2)

- 無線LANの電波をキャッチされると…
  - 無線LANでの通信内容を読まれる
  - 自宅のLANに侵入していたずらされる
  - その自宅での利用者のふりをして、様々なところにいたずらされる
  - etc.

- 無線LANの電波の設定は…
  - できるだけ電波が届く範囲を狭く設定(アクセスポイントに設定)

次回

- 学内無線LAN探検
  - 身軽にしてきましょう!

次々回

- ユーザビリティとセキュリティの関係についてグループでディスカッション&発表

様々な事例で、どの程度で折り合いをつけるか?

- いろいろセキュリティ関係の事例を調べてみる
  - ✓ 企業や組織で実際に行われているセキュリティ対策
    - その対策は必要か? それはなぜか?
    - ユーザビリティは問題ないか? 問題があっても仕方ないか?
  - ✓ セキュリティに関する事件・事故
    - どんな対策が必要だったと思うか?
    - その対策を行うと、ユーザビリティはどうなるか?
  - ✓ Jacob Nielsenのユーザビリティの定義のどれを満たさなくなるか?
  - ✓ 自分が当事者になったとして、ユーザビリティ/セキュリティの度合いは適度だと思うか?
    - 適度であれば、なぜ適度だと思うか?
    - 適度でなければ、どちらをどのくらいに下げれば/上げれば良いか?
  - ✓ ユーザビリティ/セキュリティを落とさない解決策はあるか?

例えば…

- パスワード
  - ない方がいちいちログインしなくてめんどくさくない
  - なければ、第三者に悪さをされる可能性がある
- 情報の持ち歩き
  - USBメモリに入れて自宅に持ち帰れば自宅でも作業ができる
  - 自宅に持ち帰ると紛失の可能性があるので、仕事場からの持ち出しは禁止する
    - USB使用禁止の企業も多い

企業・組織のセキュリティ対策の事例や、
セキュリティ関係の事件・事故を調べてくること