3年次演習

第10回
セキュリティのおはなし(2)

人間科学科コミュニケーション専攻
白銀 純子

今回の内容

- セキュリティ
  - 主に一般ユーザの観点から

マルウェア

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
  - リッチテキスト形式のメールにウィルスが仕込まれていることもあり
    - リッチテキスト形式: 色やフォントを変更して文章を飾ることができる形式のメール
  - 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も多数
- Webページにアクセスすることで感染
  - Webページにウィルスを仕込んでおく
  - ウィルスを仕込んだWebページにアクセスさせて、端末をウィルスに感染させる
    - ツイッターやメールなどに書かれていたURLをクリックさせるなど

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
- 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

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)

遠隔操作事件(2012年～2013年)

- 一般ユーザのPCが誰かに勝手に操作されて犯罪に使われた事件
  - 真犯人により、一般ユーザのPCがウィルスに感染
    - 多くはアプリケーションのダウンロード&インストール
  - 真犯人が、感染者のPCを使って犯罪予告を掲示板などに書き込み
    - 殺人, テロ, etc.
    - 感染者は、自分のPCから書き込みがされたことには気づかず
  - 感染者のPCから書き込みがされたことにより、感染者4名が逮捕
    - 警察は書き込みの記録(IPアドレスなど)の追跡により、書き込んだPCを特定
  - その後、犯行声明の発表やウィルスのソースコードを記録した媒体などにより真犯人が逮捕
    - ソースコード: 人間が書いたプログラム(PCが実行するのはソースコードを変換したもの)
    - 媒体を猫の首輪に取り付ける映像が監視カメラにより記録

ウィルスではないけれど…

- スマートフォンのアプリを使った遠隔操作も結構ある
  - 知り合い(特に彼氏・彼女など)が触って遠隔操作用アプリをインストール
  - スマホの持ち主の知らないうちに遠隔操作アプリが動いていて、GPS情報や写真、電話の通話履歴などを、アプリを仕込んだ人に送信

ストーカー!

無線LANのセキュリティ

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

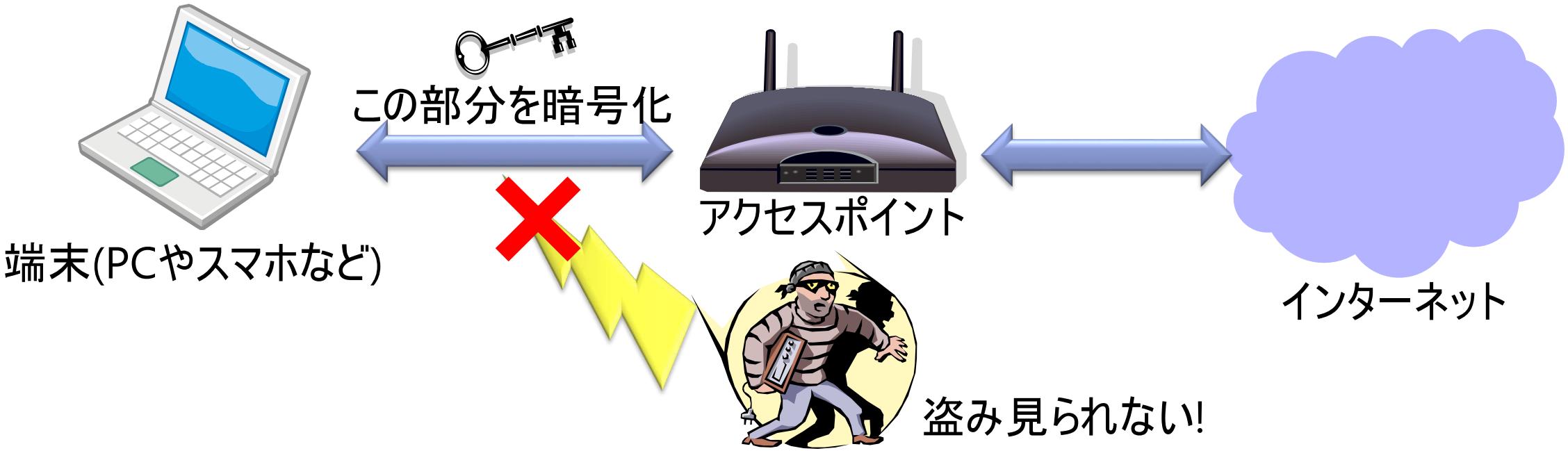
無線LANは、有線LANとは別のセキュリティ対策が必要

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

- 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



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

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
  - ネットワークカード: 端末に装備されている、ネットワークに接続するための部品
- 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

- 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
- 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
- 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)端末のみ,、その無線LANに接続が可能

電波の範囲制限

- 電波: 強弱(電波の届く範囲の広さ・狭さ)の設定が可能
- 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.
- 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の不正利用事件簿

- フィッシング詐欺(2015年)
  - 遠くの家の無線LANの電波を、電波法に違反した装置を使ってキャッチ
  - 雑誌の付録についていたソフトウェアを使って、WEPキーを解析
- ネットバンキングのIDやパスワードを狙ったウィルス送信(2014年)
- パスワードの改ざん(2012年)
- 他人になりすまして嫌がらせメールの送信(2011年)

その他利用時のセキュリティ

クッキー(Cookie)(1)

- Webサイトの管理者が、そこを訪問した利用者のコンピュータにデータを保存させる仕組み
  - 利用者に関する情報(名前・アカウント名など), 訪問した日時・訪問回数など
  - Webサイトを訪問したときにクッキーのデータもWebサイト側に送信
  - 以前訪問したことの有無・そのWebサイトで何をしたか(見たか)などにより、個人ごとに提示する情報が変化
  - Ex.: 訪問すると、ログインしていないのに「こんにちは、xxさん。おすすめの商品があります」と表示されるのはクッキーによるもの

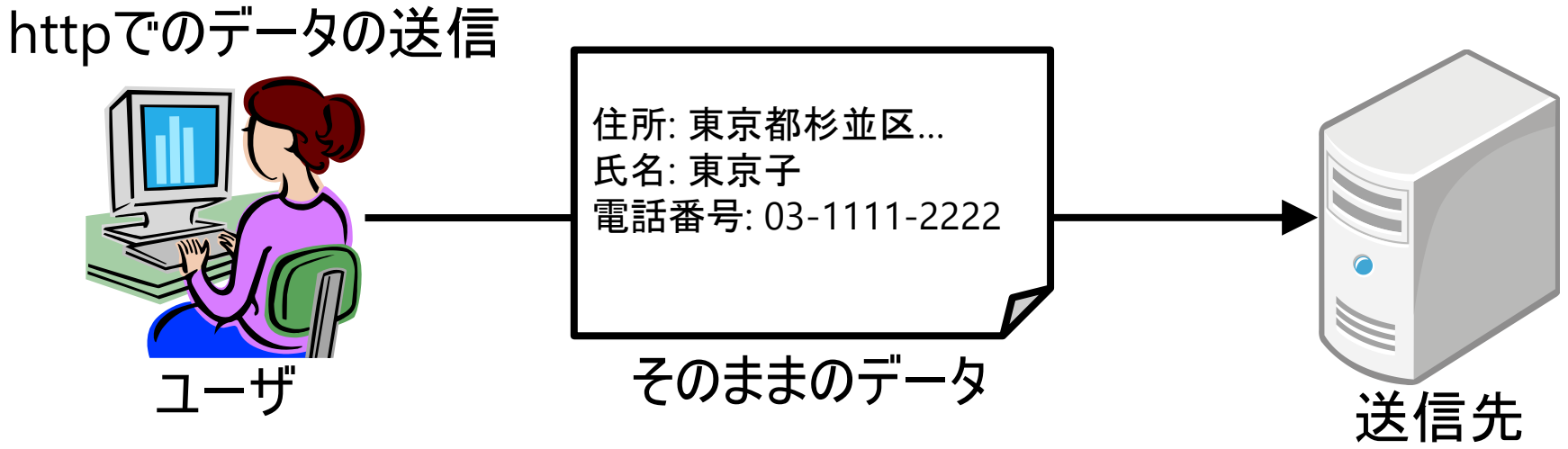
クッキー(Cookie)(2)

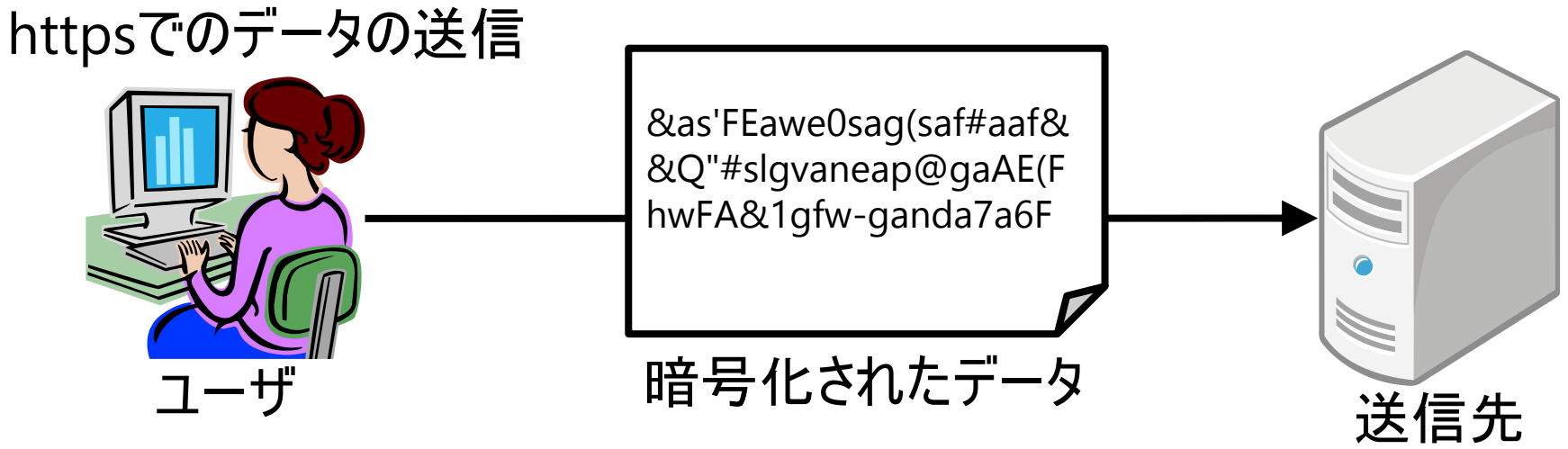
- 会員制のサイトなどで、クッキーをオフにしているとアクセスできないことも
- クッキーには重要な個人情報が保存されることも
  - 1つのPCを複数の人で共有して使う場合に、個人情報が盗まれることも
    - Webメールや会員サイトのパスワードなど

SSL

- Secure Socket Layerの略
- インターネット上でデータを暗号化して送る仕組み
  - インターネットショッピングでの個人情報の送信やWeb上での認証、電子メールなどで利用
  - Webの場合、URLが「https://」で始まっていれば、SSLでの通信
    - 「http://」の場合は、普通の暗号化しない通信

httpとhttps





無線LAN探検

- スマートフォンの無線LANの電波をキャッチするモードに
  - Android:「設定」→「WiFi」
- キャンパス内を歩いて、電波をキャッチ
  - キャッチした電波は、WEPやWPA/WPA2で保護されているか?を確認

やってみよう!

- Internet Explorerのセキュリティの設定を変更して、普通にアクセスするのとどう違うか比べてみよう!
  - セキュリティレベルの設定: 設定(歯車のアイコン)→「セキュリティ」タブで、「このゾーンのセキュリティのレベル」を「高」に変更
  - プライバシーの設定:設定(歯車のアイコン)→「プライバシー」タブで、「設定」を「すべてのCookieをブロック」に変更

※変更前の設定内容をメモしておくこと(演習終了後に直すこと)!