



3年次演習

第9回
セキュリティのおはなし(1)

人間科学科コミュニケーション専攻
白銀 純子

Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

今回の内容

- セキュリティ
 - 企業・組織の観点から
 - ユーザの観点から



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

ユーザビリティとセキュリティのトレードオフ

■ トレードオフ: 一方を取ればもう一方を取れないという関係

ユーザビリティとセキュリティ

ユーザIDとパスワード

- ない方が使いやすい
- × なければ、どこに誰に東京女子大学のシステムを使われるかわからない

インターネットショッピング

- 店に行かなくても買い物ができるので便利(買い物をしやすい)
- × 個人情報(特にクレジットカード)の保護の面で不安

どこで折り合いをつけるかは非常に難しい問題

ただし、現在は多少利便性を犠牲にしてもセキュリティを上げておく必要

Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.



セキュリティ関係の事件簿

- 日本年金機構の個人情報流出(2015)
- ベネッセコーポレーションの個人情報流出(2014)
- DDos攻撃でPlaystation Networkがダウン(2014)
- LINEアカウントの乗っ取り(2014~)
- インターネットバンキングでの不正送金
- 企業・官公庁のWebサイト改ざん
- 無線LANの不正使用



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

事件一覧

■ 個人情報漏洩事件・事故一覧:
<http://www.security-next.com/category/cat191/cat25>

■ サイバーセキュリティ事件簿:
http://www.mbsd.jp/casebook_index.html

Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.



企業・組織の観点から



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

ポートを使った攻撃(1)

- ネットワークでのコンピュータは、アパート or マンションのようなもの
 - IPアドレス(ネットワークでのコンピュータの住所)は、アパート or マンションの住所のイメージ
- ネットワークでやりとりされるデータは、アパート or マンションの各部屋からやりとりされるもの
 - データに関して、どこに送るか・どこから送られるかの部屋番号が必要

部屋番号 = ポート



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

ポートを使った攻撃(3)

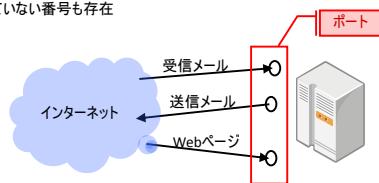
- ポートを使うには、ポートを開いておく(部屋のドアを開いておく)必要
 - ポートは、アパート or マンションの玄関のドアのようなイメージ
- ポートを開いておくことで、攻撃のターゲットに
 - 攻撃対象のコンピュータの、開いているポートの有無を調査(ポートスキャン)
 - 開いているポートが見つかったら、そこを突破口にして対象のコンピュータに攻撃



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

ポートを使った攻撃(2)

- ポート: コンピュータへデータが出入りする部屋番号
 - 1つのコンピュータに多くのポートが存在
 - 原則として、通信の種類によってどの番号を使うかは決定済み
 - メール受信・メール送信・Webページアクセスなど
 - 使われていない番号も存在



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.



ポートを使った攻撃を防止するには?(2)

- 不要なポートを閉じる: ファイアウォールを導入する
 - **ファイアウォール:** コンピュータに入り出すデータを監視して、許可されているデータのみ通す(フィルタリング)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
 - ちなみに...個人のPC用のファイアウォールソフト(パーソナルファイアウォール)もたくさんあり、簡単に導入可能
 - Windows XP Service Pack 2以降に付属
 - ウィルスソフトを開発・提供している会社で、ウィルスソフトと一緒にして提供しているもの
 - etc.
 - Windowsのものよりも高機能なので、こちらを導入することがおすすめ



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

IPアドレスの偽装(1)

- プロキシサーバー: 不正アクセスから内部のコンピュータを守るための仕組み
 - 外部から直接アクセスできるコンピュータを少数に限定する
 - このコンピュータを「プロキシサーバ」と呼ぶ
 - 外部からのアクセスは、必ずプロキシサーバを通して行う
 - 不正アクセスで攻撃されるのは、プロキシサーバだけになる
 - 内部の重要なコンピュータは壊されない

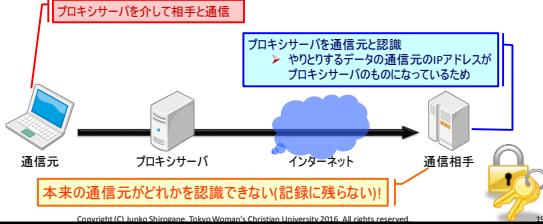


Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.



IPアドレスの偽装(2)

- 本来はプロキシサーバは不正アクセスを防止するためのものだけど...
 - プロキシサーバを使った通信は、相手先から本来の通信相手を隠す
 - 相手先で通信相手として記録されるIPアドレスが、プロキシサーバのIPアドレスになる



Copyright (C) Junko Shiragane, Tokyo Woman's Christian University 2016. All rights reserved.

IPアドレスの偽装(2)

- 不正アクセスの攻撃者はプロキシサーバで自分のIPアドレスを偽装(プロキシサーバを「踏み台」にする、と呼ぶ)

- 被害にあったコンピュータの通信の履歴(アクセスログ)にはプロキシサーバのIPアドレスが記録
- 攻撃者本人のコンピュータのIPアドレスは記録なし

- 攻撃されると、攻撃者を特定して対処する必要
 - IPアドレスをもとに攻撃者を特定
 - IPアドレスが偽装されていると、偽装されたプロキシサーバからさらにたどる必要
 - 複数のプロキシサーバを踏み台にしている場合も

攻撃者の特定がしにくくなる



Copyright (C) Junko Shiragane, Tokyo Woman's Christian University 2016. All rights reserved.

個人情報の流出



Copyright (C) Junko Shiragane, Tokyo Woman's Christian University 2016. All rights reserved.

なぜ流出事件が多い??

- 個人情報はお金になるから!

- まともな企業でも個人情報は欲しい
 - ダイレクトメールや勧誘などの営業のために...



- 興味本位や個人的欲求

- 仕事で会う人の個人情報を見てみたかった!
- 気になる人の家に訪ねたい!
- etc.



Copyright (C) Junko Shiragane, Tokyo Woman's Christian University 2016. All rights reserved.

どうやって流出するか??(1)

- 個人情報を扱っているコンピュータへの不正アクセス

- IDとパスワードの利用
 - 簡単なパスワードを設定していたためにパスワードを解析された
 - 他人にパスワードを教えてしまった
 - etc.
- コンピュータ利用上のミス
 - 世界中に公開している場所に個人情報を置いてしまった
 - セキュリティホールを埋めるパッチを適用していなかった
 - セキュリティホール・ウィルスや不正アクセスをされやすい、ソフトウェアの不具合
 - パッチ: セキュリティホールやその他不具合を修正するための差分ソフトウェア
 - etc.
- ワイルスを介した乗っ取りやセキュリティホールをついた攻撃
- etc.



Copyright (C) Junko Shiragane, Tokyo Woman's Christian University 2016. All rights reserved.

どうやって流出するか??(2)

- 個人情報へのアクセスが許可された人が持ち出し

- 故意に持ち出し
 - 売ってお金儲けが目的、など
- 管理不行き届き
 - 個人情報の入ったノートPCを電車内などに置き忘れた、など

- 古いPCや携帯電話、スマホなどの機器類の処分

- 保存されていたデータの消し忘れ
- データを消しても、データ復元ソフトで読み取り
 - データをゴミ箱に入れ、ゴミ箱から消去しても、データ復元ソフトで復元できるものも多い



Copyright (C) Junko Shiragane, Tokyo Woman's Christian University 2016. All rights reserved.

日本年金機構での個人情報流出～前提知識～

- 個人情報の取り扱い: 個人情報は断片にされて別々のコンピュータで管理
 - 住所や氏名、電話番号、年金番号など、バラバラにして管理
 - 1つ1つのデータを見ただけでは、個人の特定は不可
- ファイルにパスワードをかければ、各情報を集めて保存してもOKというルール
 - 個人と連絡を取りたいときなど



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

日本年金機構での個人情報流出～経緯～(1)

■ 職員が各情報を集めてファイルに保存した作業をした

- 大半のファイルにパスワードがかけられていなかった

■ ファイルを保存したコンピュータをネットワークに接続したまま、メールを読んだ

- 件名はまともそうなメール

- 添付ファイルも開封

→ ウィルスつきの添付ファイルで、職員のPCがウィルスに感染

- 数人の職員が同様にメールの添付ファイルを開封してPCがウィルスに感染

- ウィルスはいくつかの違う種類のものだったが、ほとんどが新しいもの



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

日本年金機構での個人情報流出～経緯～(2)

- ネットワークを通じて他のPCにもウィルスが広まった
 - ネットワークは接続したまま
 - ウィルス対策ソフトは更新
- ウィルスを介してファイルを保存したコンピュータにアクセスされた



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

DoS攻撃



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

DoS(Denial of Service)攻撃って?

- コンピュータに大量の負荷をかけて、コンピュータを動作不能にする攻撃
 - スパムメールを一斉に大量に送りつける(メール爆弾、メールボム)
 - DoS攻撃ではないが、あけおめメールとか災害時の一斉安否確認なども同様の結果に
 - Webページへの一斉の大量アクセス
 - etc.

コンピュータの処理能力の限界を超える攻撃

- 複数のコンピュータから一斉に攻撃することをDDoS攻撃

- DDos: Distributed Deinal of Service



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

DoS攻撃の理由と影響

■ なぜDoS攻撃をするのか?

- 愉快犯
 - おもしろそうなソフトがあったから使ってみた、とか...
- 自分の技術力の自慢
- 攻撃先に対するうらみ, etc.

■ DoS攻撃されるとどうなるか?

- 提供していたサービスをユーザーが利用できなくなる
 - ゲームであれば遊べなくなる
 - メールのやり取りができなくなる, etc.

ものによっては深刻な影響も...

- 銀行や株式のシステムが攻撃されると、経済に影響
- 電車や飛行機のシステムが攻撃されると、人命に影響



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

Webページの改ざん



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

Webページの改ざんって??

■ Webページが、本来の内容とは違うものに変更されてしまうこと

- 不正アクセスの一種
- 見た目に変わりなくとも、何か仕込まれていることも...

改ざんの目的

- 愉快犯
- 自己主張: 自分の主義主張を世に知らせたい
- 攻撃先へのうらみ: 改ざんすることによって信頼のできない官公庁や企業であることを知らせたい
- ウィルスのばらまき: アクセスしてきたコンピュータをウィルスに感染させたい
 - ▷ DDoS攻撃に参加させるためとか



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

どうやって改ざんする?



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

- Webページの管理用IDとパスワードの入手
- 設定ミスがないかを調査
- セキュリティホールの利用
- ウィルスを送りつけ

セキュリティ関連の事件を防ぐには?



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

結局のところ...

セキュリティ関係の事件の主な原因

- IDやパスワードの流出
- 設定・利用上のミス
- ソフトウェア(OS, ウィルス対策ソフト, その他ソフトウェア)のアップデートの怠り
- ユーザの故意・過失
- セキュリティホール
- ウィルス

利用者(人間)側の問題

(アップデートの怠りなどがないければ)コンピュータ側の原因

- コンピュータでの対策は当然ながら、人間側の意識改善が一番必要!
- 企業・組織でのセキュリティのあり方(セキュリティポリシー)を策定する
- ユーザに対する教育をきちんと行って意識を向上させる



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

日本年金機構での個人情報流出での分類(1)

職員が各情報を集めてファイルに保存した作業をした

- 大半のファイルにパスワードがかけられていなかった

ファイルを保存したコンピュータをネットワークに接続したまま、メールを読んだ

- 件名はまともそうなメール

コンピュータ側の問題
➢ ウィルス対策ソフトは使っていたようなので

- 添付ファイルも開封

➢ ウィルスつきの添付ファイルで、職員のPCがウィルスに感染

■ 数人の職員が同様にメールの添付ファイルを開封してPCがウィルスに感染

■ ウィルスはいくつかの違う種類のものだったが、ほとんどが新しいもの

個人の問題

- ファイルにパスワードをかけなかったのはルール違反
- 添付ファイルをむやみに開かないのはセキュリティの基本
- ✓ ただし、組織の教育体制の不備である可能性も



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

日本年金機構での個人情報流出での分類(2)

■ ネットワークを通じて他のPCにもウィルスが広まった

■ ネットワークは接続したまま

■ ウィルス対策ソフトは更新

■ ウィルスを介してファイルを保存したコンピュータにアクセスされた

(おそらく)組織の考え方(体質)の問題
➢ 接続したまま良いという判断は組織の上部や全体でしているはず



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

ユーザの観点から



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

マルウェア



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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

■ コンピュータウイルス

■ スパイウェア

■ etc.

Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

コンピュータウイルス

■ 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.



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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ます

▪ 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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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働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(マクロウイルス)
 - 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
 - 通常のウイルスは、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イルスは、WindowsでもMacでも感染する可能性



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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
- ブラウザ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)



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

無線LANのセキュリティ



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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・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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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.



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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イルス送信(2014年)
- パスワードの改ざん(2012年)
- 他人になりますて嫌がらせメールの送信(2011年)



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

その他利用時のセキュリティ



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

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

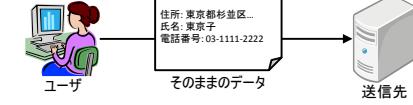
- インターネットショッピングでの個人情報の送信やWeb上での認証、電子メールなどで利用
- Webの場合、URLが「<https://>」で始まっていれば、SSLでの通信
 - 「<http://>」の場合は、普通の暗号化しない通信



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

httpとhttps

httpでのデータの送信



httpsでのデータの送信



Copyright (C) Junko Shirasane, Tokyo Woman's Christian University 2016. All rights reserved.

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



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

やってみよう!

■ニュースに出てきた企業や組織のセキュリティ関連の事件をいくつか探して、原因を分類してみよう

1. 企業・組織の考え方(体質・セキュリティポリシー)の問題?

2. 働いている個人の問題(教育の問題)?

3. コンピュータ側の問題(1.と2.はきちんと行っていたのでどうしようもなかった)?

■さらに、対処によってユーザビリティの問題が起こりそうかも考えてみよう



※自分はどう分類できると思ったか?でOK

Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.

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)!



Copyright (C) Junko Shirane, Tokyo Woman's Christian University 2016. All rights reserved.