

情報処理技法(リテラシ)I

第5回 インターネット(2), WWW(1)

人間科学科コミュニケーション専攻
白銀 純子



第5回の内容

- インターネット(続き)

- WWW



前回の復習問題の解答

○以下の文章の(ア)～(ウ)に入る適切な言葉を答えなさい。

- メールを送信するとき、(ア)というコンピュータにより、メールが相手先に届けられる。メールを受信するとき、利用者が使っているコンピュータは、(イ)というコンピュータにアクセスして、その利用者のメールを受け取る。また、東女Gmailは、特定のメールソフトを必要とせず、Webブラウザで世界中どこからでも読み書きができる(ウ)という形態のメールシステムである。

解答:

(ア) SMTPサーバ (イ) POPサーバ (ウ) Webメール



インターネット



インターネットって? [1] (p. 47)

- **コンピュータネットワーク**: コンピュータ同士で通信を行うことができるようにした仕組み
- **インターネット**: 世界中のコンピュータを接続する通信網
(コンピュータネットワークの一種であり、最も有名なもの)
 - インターネットは、コンピュータ同士の通信内容の通り道



インターネットって?[2](p. 47)

○インターネット上で様々なサービスを提供するコンピュータが存在

- Webページを公開するためのコンピュータ
- 電子メールの配送を行うためのコンピュータ

インターネットを通じて、サービスを提供する
コンピュータを利用できる

サービスの利用: サービスを提供しているコンピュータから自分の
コンピュータにデータをもらってきたり送ったりすること

インターネット: データの通り道



利用できるサービス[2](p. 48)

- インターネット: データが通るための通り道を提供しているだけのもの
- 各サービスのためのルールは各サービスによって決定
 - 「インターネット」という道路を通るための共通のルールだけ守れば、様々なデータをやりとり可能
 - プロトコルを独自で定義して、新しいサービスを作ることも可能



インターネットを利用するには(p. 48)

- 必要な機器を用意する
- インターネット接続のためのサービスを提供している会社(プロバイダ, ISP)と契約する
 - 東京女子大学: 大学自体がIJというプロバイダと契約
 - 個人が作業しなくても、情報処理教室でインターネットを利用可能
 - 設定すれば、自分のノートPCを大学内でインターネットに接続可能
- 自宅: プロバイダと契約して料金を支払う必要



セキュリティ対策の必要性



現実的な解決方法は?-最低限の義務-(I)(p. 52)

○ウィルス対策ソフトを利用

- ウィルスからの防御・ウィルスの駆除・不正アクセスの防止の機能

- ただし、状態のアップデートが必要

 - ウィルスは毎日のように新しいものが出現するので、アップデートをしなければ、古いウィルスには対応できても新しいものに対応できなくなる

 - 店でPCを購入後、一定期間を過ぎると、ウィルス対策ソフトのアップデートの権利が切れるので、権利の更新が必要になる

- 初期設定にしておけば、状態のアップデートは自動

ウィルス対策ソフトの導入とアップデートの権利の購入は
必ずすること!



現実的な解決方法は?-最低限の義務-(2)(p. 52)

○ソフトウェアのアップデート

- ソフトウェアには利用上の不具合やセキュリティ上の問題になる不具合(セキュリティホール)が存在

- セキュリティホール: ウィルスや不正アクセスの侵入口になりえる

- 様々な不具合は、見つければ、解消するための追加ソフトウェアが提供

ソフトウェアのアップデートを必ず行うこと!

- WindowsやMac OSなどのオペレーティングソフト(基本ソフト)
 - ✓ 自動でアップデートを行うように設定可能
- その他のアプリケーション
 - ✓ アップデートの通知機能がついているものが多いので、通知されたアップデート



インターネット上のサービス



クライアント/サーバ(I)(p. 53)

- インターネット上でのサービスの基本形態: クライアント/サーバシステム

- クライアント (Client)

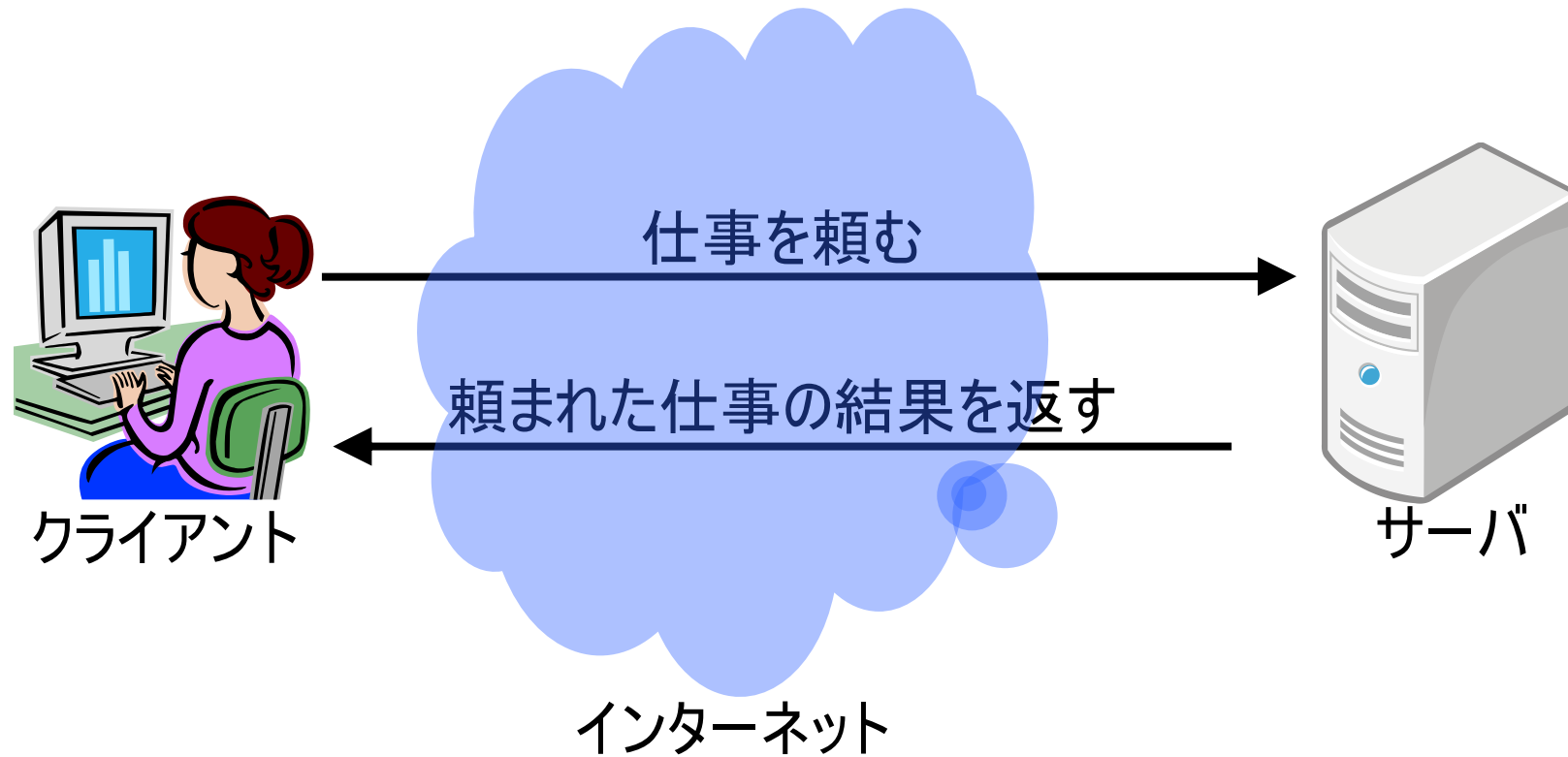
- サーバに要請をして、様々な処理をしてもらうコンピュータ(or ソフトウェア)
- Ex. Webページを見せてもらう, 届いているメールを見せてもらう, 商品の注文処理をしてもらう, etc.

- サーバ (Server)

- クライアントからの要請を受けて、様々な処理をするコンピュータ(or ソフトウェア)
- Ex. Webサーバ, メールサーバ, 受注発注システム, etc.



クライアント/サーバ(2)(p. 53)



Webサービスの利点(p. 54)

- Webサービス: WWWの仕組みを利用したサービス

- いつでもどこからでも利用可能

- クライアントコンピュータがインターネットに接続されていれば、いつでも利用可能

- Ex. 自分のPCにOfficeソフトが入ってなくても、PCをネットワークに接続すると、WebサービスのOfficeソフトを利用可能

- 様々なコンピュータ環境から利用可能

- Ex. MacでもWindowsでも、まったく同じソフトを利用可能
(例えばMicrosoft Officeだと、MacとWindowsでいろいろ違う)



Webサービスの注意点[1](p. 55)

○知らないうちに公開されているデータ

○Webサービスでは、ネットワーク上にデータを保存
= 常に、データが第三者に漏えいする危険性

○Webサービスの提供元は、データを十分に保護してくれるわけではない

- データの公開範囲などをきちんと確認して、設定すること
 - ✓ 自分で何も設定しなければ、初期設定の状態で、世界中に公開という設定になっていることも
- Webサービスで保存しておいて良いデータかどうかをよく考えること
 - ✓ Webサービスの提供元は、保存されているデータを分析



Webサービスの注意点[2](p. 56)

○保存しているデータの安全性

- Webサービスのサービスを利用して作成したデータは、Webサービスの提供元のサーバに保存
 - サーバ側でトラブルが発生すること
 - データが失われても、補償をしてくれないことも

重要なデータについては、自分でバックアップを取っておくこと

○サービスの永続性

- Webサービスの提供元の事情により、突然サービスを終了されてしまうことも
- 無料だったものが有料になることも

代替手段を考えておくことも重要



ドメイン



ドメイン[1](p. 56)

- 現実世界: 手紙を送るときには住所、電話するときには電話番号が必要
- インターネット: 情報のやり取りをするには「住所」が必要
 - データの受け取り先の「住所」
 - データの送り主の「住所」



ドメイン[2](p. 56)

○インターネットでの住所は?

=IPアドレス

インターネット上でコンピュータを
識別する住所

=「192.168.200.1」のように、「.」で区切られた3桁の
数を4つ並べたもの(それぞれの数は、0～255までの数)

コンピュータにとっては、数値のほうがわかりやすいので、数値で表す



ドメイン[3](p. 56)

○IPアドレス

- インターネット上の住所を数値で表したものの
人間にとっては、数値の住所はわかりにくい!

ex. 電子メールアドレス

「**利用者の名前@メール配送コンピュータの住所**」の形になっている
→コンピュータは電子メールアドレスを
「**利用者の名前@192.168.200.1**」のように考えている

➡ **ドメイン名**



ドメイン[4](p. 57)

- **ドメイン**: 数値ではなく、アルファベットを使ってコンピュータが所属する組織の住所を表したもの

東京女子大学のドメイン: `twcu.ac.jp`

「.」で地域を区切る

現実世界の住所

東京都 杉並区 善福寺 2丁目6番

一番左が一番大きな地域

インターネットでの住所

`twcu.ac.jp`

一番右が一番大きな地域

- jp: 日本
- ac: 大学
- twcu: 東京女子大学



ドメイン[5](p. 57)

- ドメイン名で、その組織が何かがある程度わかる
 - ドメイン名は、地域を国、研究機関や政府、企業などで区切ることも多い
 - 国: 「jp(日本)」, 「uk(イギリス)」, 「cn(中国)」, etc.
 - 組織: 「ac(研究教育機関)」, 「go(政府)」, 「co(企業)」, etc.
- ➡ twcu.ac.jp: 「ac」と「jp」があるので「日本の研究教育機関」
- ➡ mext.go.jp(文科省): 「go」と「jp」があるので「日本の政府組織」



コンピュータとIPアドレス(p. 57)

○IPアドレスとの対応: コンピュータの住所

○ドメイン名: インターネットの世界での組織の住所

○コンピュータ: 組織に所属する一員

○データのやり取りは、コンピュータ同士

ドメイン名を使ったコンピュータの住所の表記: **コンピュータ名.ドメイン名**

➤ コンピュータ名: それぞれの組織でつけるコンピュータの名前

コンピュータの住所の例

➤ **www**.twcu.ac.jp

➤ **mail**.cis.twcu.ac.jp

➤ **ftp**.lab.twcu.ac.jp

組織がつけた
コンピュータ名

ドメイン名



第1回課題

○<http://www.cis.twcu.ac.jp/~junko/LiteracyI/Report/IstRep.html>



Webページ閲覧の仕組み



WWW(p. 85)

- 「World Wide Web」の略

- 「世界中に張り巡らされたくもの巣」という意味
 - 様々な情報を公開・閲覧するための仕組み

- インターネットを使うサービスの1つ

- CERN(ヨーロッパ高エネルギー物理研究所)で、研究者がデータなどをお互いに検索するために開発

- 「ブラウザ(browser)」というソフトウェアを使って情報を閲覧

- Webページ:文章や図が入ってブラウザの中に表示される内容



Webブラウザとは?(p. 85)

- Webページを見るためのソフトウェア
- 単に「ブラウザ」とも(種類はたくさんある)

- Internet Explorer

- Mozilla Firefox

- Safari

情報処理教室で利用するWebブラウザ

- Google Chrome

- etc.



Webページ(p. 85)

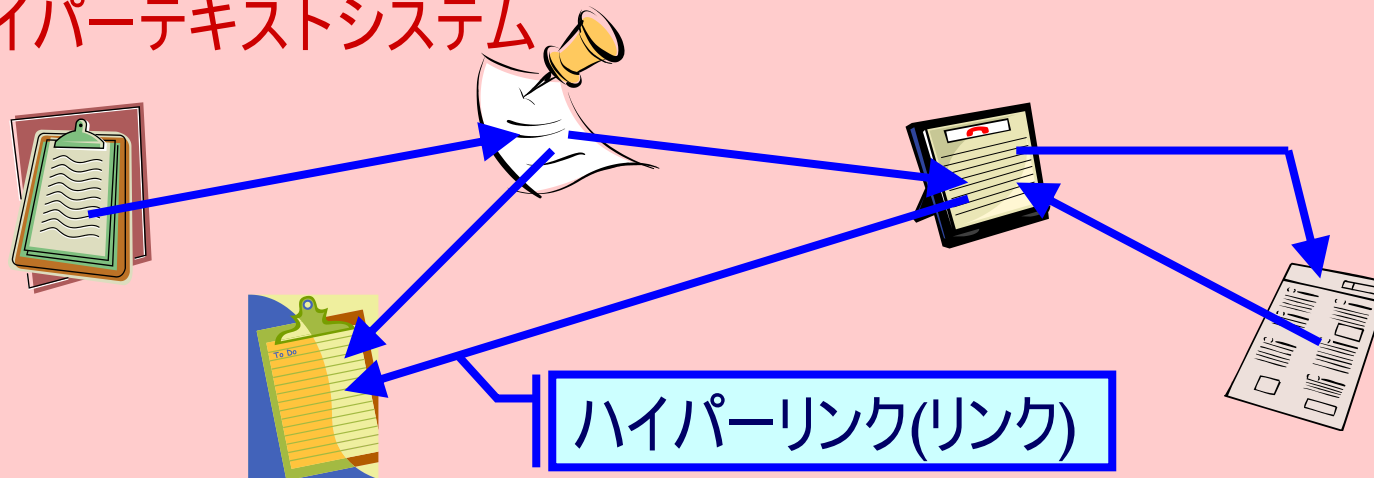
○ハイパーテキスト形式の情報表現方法

- 情報は通常、何ページかに渡り、その最初のページを「トップページ」

ハイパーリンク

文書中に、他の文書の位置情報を埋め込むことで、複数の文書をつなぎ合わせる仕組み

ハイパーテキストシステム



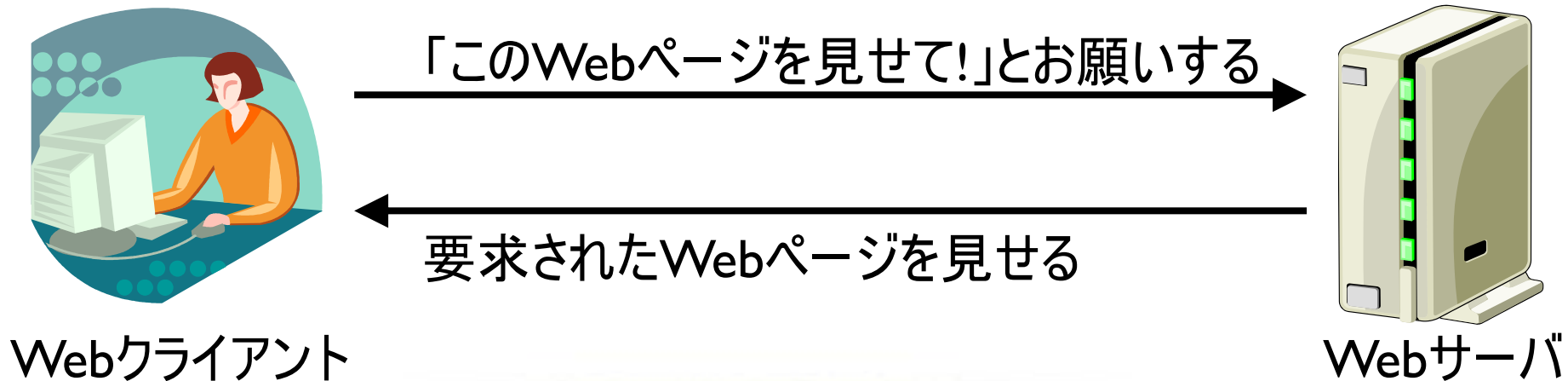
リンクって?(p. 85)

- ハイパーリンクの略
- クリックすることで別のページを見ることが可能
 - 通常、リンクは別のページへの「**URL**」を指し示しており、リンクをクリックすることで、そのページが表示される
 - URL(Uniform Resource Locator)**: Webページが置いてある場所についての情報(ページの住所)
- リンクをたどることで様々なページを見ることが可能
 - リンクがクモの巣のように張り巡らされている



WebサーバとWebクライアント(p. 85)

- **Webサーバ**: Webページが置かれている(公開されている)コンピュータ
 - それぞれの組織のどこかに置かれているコンピュータ
- **Webクライアント**: 公開されているWebページを見るコンピュータ(又は、Webページを見るソフトウェア)
 - 普段人間が使っているコンピュータ



URLって? [1] (p. 86)

- Webページのありかを示す情報

- URLの形式:

プロトコル名 : // **Webサーバ** / **Webページの内容**

- **プロトコル名**: WebサーバとWebクライアントでどういうルールで通信をするかというプロトコル
- **Webサーバ**: Webページの内容を置いているコンピュータの住所と名前
- **Webページの内容**: Webページの内容が書き込まれたファイルが、Webサーバのどこに置かれているか



URLって?[2](p. 86)

○例えば...

http://www.cis.twcu.ac.jp/cis/index.html

http : HyperText Transfer Protocolの略

WebサーバとWebクライアントとの間で通信をするためのプロトコル

www.cis.twcu.ac.jp : Webサーバの名前と住所

(「www」がWebサーバの名前、「cis.twcu.ac.jp」が住所)

cis/index.html : Webページの内容が書き込まれているファイルの名前
(フォルダ名を含む)



URLって?[3](p. 86)

- 「Webサーバ名/」の後は、Webサーバ内でのファイル(文書)のありかとも名前を示す

`http://www.cis.twcu.ac.jp/cis/index.html`

「東京女子大学のWebサーバの中の『cis』というフォルダの中の『index.html』というファイル」という意味

`http://www.cis.twcu.ac.jp/~junko/LiteracyI/abc.html`

「東京女子大学のWebサーバの中の『~junko』というフォルダの中の『LiteracyI』というフォルダの中の『abc.html』というファイル」という意味



URLって?[4](p. 86)

- <http://www.cis.twcu.ac.jp/cis/index.html>

- 「http」という方式で
- 東京女子大学の「www」という名前のWebサーバと通信し、
- 「cis」というフォルダの中の「index.html」というファイルを見せてもらう

- <http://www.twcu.ac.jp/~junko/LiteracyI/index.html>

- 「http」という方式で
- 東京女子大学の「www」という名前のWebサーバと通信し、
- 「~junko」というフォルダの中の「LiteracyI」というフォルダの中の「index.html」というファイルを見せてもらう



URLって?[5](p. 86)

- URL: 通信する方式とWebサーバの住所、見せてもらう文書のファイル名を表したもの

- 「index.html」というファイル

- URLから省略できる

同じURL(同じファイルを探す)

- `http://www.twcu.ac.jp/index.html`

- `http://www.twcu.ac.jp/`

- URLの最後がファイル名ではない場合: コンピュータは自動的に「index.html」というファイルを探す



httpとhttps(p. 86)

○どちらもWWWでのプロトコル

- http: HyperText Transfer Protocol(**http**://～というURL)

- https: HTTP over SSL/TSL(**https**://～というURL)

 - 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

 - 東女Gmailもhttps

○インターネットでのデータの送受信は...

- httpだと: 経由したところで中に書かれてあるデータをそのまま見ることが可能

- httpsだと: 経由したところで中を見られても、暗号化されたデータが見えるだけ
(内容を解読できない)

個人情報の入力を求めるサイトでは、httpsを使うことが多い
= 自分の個人情報を入力するときには、確認すると良い

Webブラウザの使い方

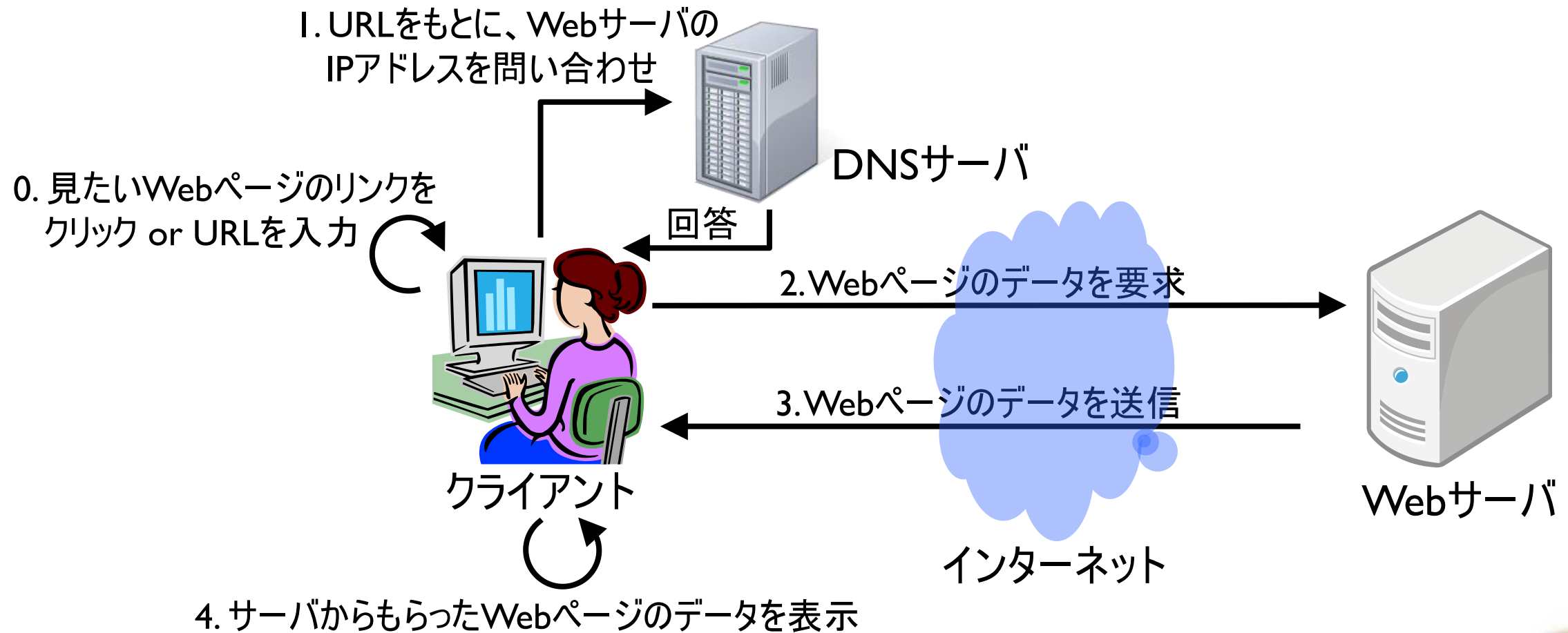


WWW上での情報のやりとり[1](p. 87)

1. URLからWebサーバの住所(IPアドレス)が特定される
2. ブラウザが、そのWebサーバに必要なWebページを要求する
3. Webサーバは、要求されたWebページのデータをブラウザに送る
4. ブラウザは、Webサーバから送られてきたデータを画面に表示する



WWW上での情報のやりとり[1](p. 87)



※DNSサーバ: IPアドレスと、コンピュータ名・ドメイン名の対応関係を管理するサーバ

Webブラウザを利用するには?(p. 87)

○情報処理教室ではSafariを利用

○ただし、Safariが調子が悪いときはFinder→「アプリケーション」の中の他のブラウザを使おう!

○Google Chrome

○Firefox

○etc.



Safariの利用(p. 87)

○アドレスバー: URLを入力する場所

○URLを入力して「Enter」を押すと、そのページが表示(ただし、文字は全て半角)



※大文字小文字は区別される



Webページの指定方法(p. 88)

○新規表示の場合

- Google検索を使う: アドレスバーに検索したいキーワードを入力してReturnキーを押す

- アドレスバー: ウィンドウ一番上の、URLを入力する欄

- アドレスバーに、目的のWebページのURLを入力する

○ブックマークに登録済みのページの場合

- ブックマークバー(アドレスバーの下)に登録してある場合:
登録してあるページの名前をクリックする

- ブックマークメニューに登録してある場合:
メニューバーから「ブックマーク」→「ブックマークを表示」と選択し、
目的のブックマークをダブルクリックする



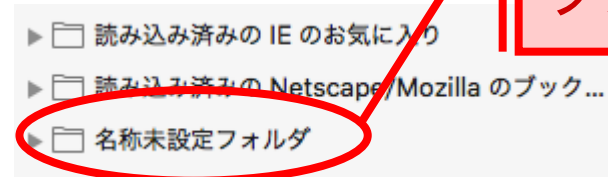
ブックマーク(p. 88)

- よく利用するWebページを、簡単に表示させるための機能(本のしおりのようなもの)
- ブックマークをWebページの内容ごとに分類することも可能
 - 内容ごとに異なるフォルダを作成して分類



ブックマークフォルダの追加(p. 88)

- ブックマークフォルダ: ブックマークを整理するための箱
- メニューバーの「ブックマーク」→「ブックマークフォルダの追加」を選択
- 「名称未設定フォルダ」というフォルダができるので、右クリック→「名前変更」でブックマークフォルダの名前を入力



ブックマークフォルダの名前を入力



ブックマークの追加(p. 88)

1. ブックマークに追加したいWebページを表示する
2. メニューバーの「ブックマーク」→「ブックマークに追加」を選択する
3. ブックマークの名前を入力し、それをどのフォルダに分類するかを選択して「追加」ボタンを押す

○ブックマークの名前: そのWebページが何のページかを示すもの

このページの追加先:

お気に入り

Center for Information Science

説明

キャンセル 追加

ブックマークを分類するフォルダを選択

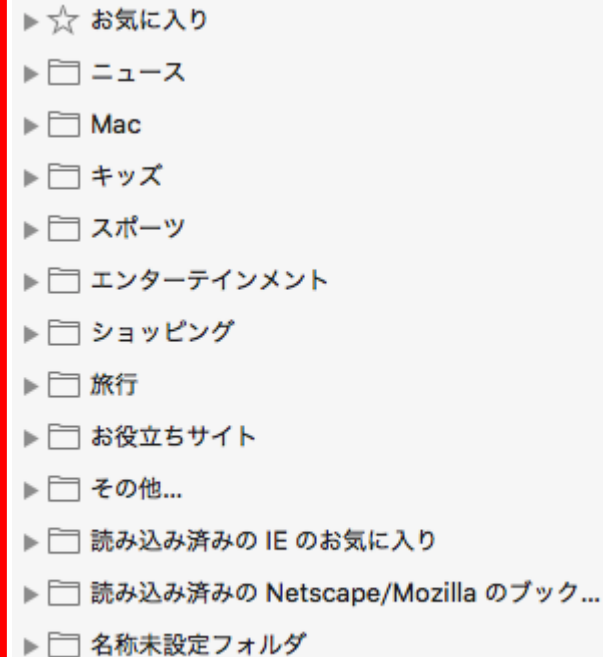
ブックマークの名前(そのWebページが何のWebページかを示すもの)を入力



ブックマークから表示(p. 88)

- メニューバーの「ブックマーク」→「ブックマークを表示」を選択
- 表示したいWebページが入っているフォルダを選択し、Webページの名前をダブルクリック

- Webページが入っているフォルダを選択
- 表示されたWebページのリストから、表示したいページをダブルクリック



- ▶ ☆ お気に入り
- ▶ フォルダ ニュース
- ▶ フォルダ Mac
- ▶ フォルダ キッズ
- ▶ フォルダ スポーツ
- ▶ フォルダ エンターテインメント
- ▶ フォルダ ショッピング
- ▶ フォルダ 旅行
- ▶ フォルダ お役立ちサイト
- ▶ フォルダ その他...
- ▶ フォルダ 読み込み済みの IE のお気に入り
- ▶ フォルダ 読み込み済みの Netscape/Mozilla のブック...
- ▶ フォルダ 名称未設定フォルダ



やってみよう!

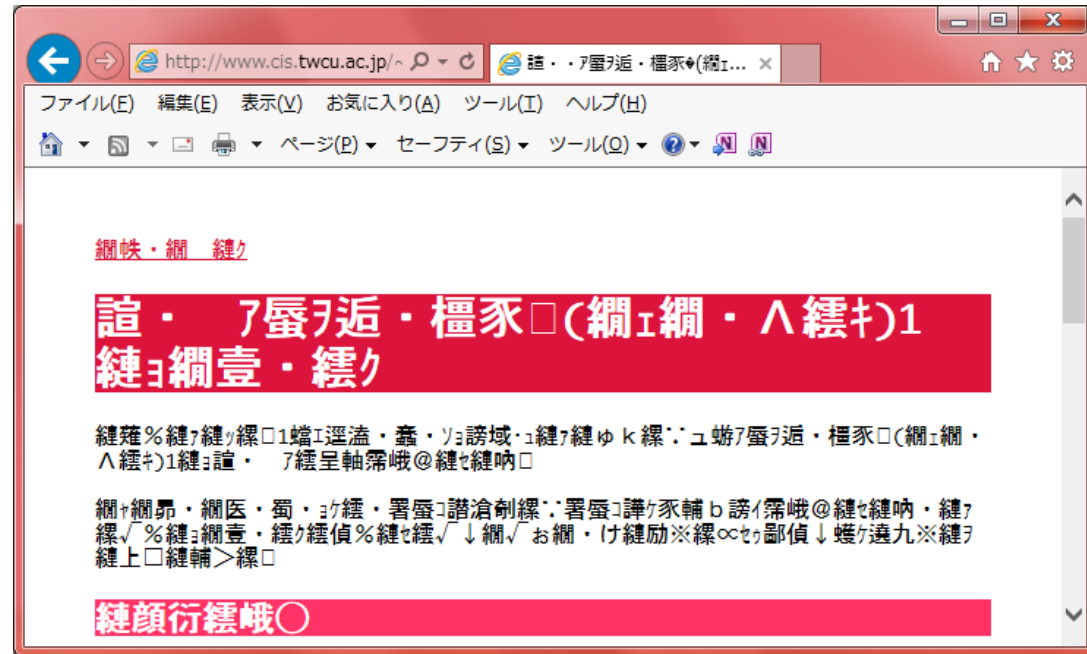
- 自分がよく使うWebページをいくつか、ブックマークに登録しよう
- 登録したブックマークから、好きなWebページを開いてみよう



文字化け(p. 89)

- **文字化け**: 日本語で表示されるはずのページが
意味不明の文字で表示される現象

WebブラウザがWebページの「**文字コード**」を正しく理解できなかったために
起こる現象



文字コードのおはなし[1](p. 89)

○コンピュータは全てのことを0と1の羅列で解釈

たくさんのスイッチがあって、どのスイッチがONでどのスイッチがOFFになっているかの組み合わせ

➡ 文字コード: 文字を表す0と1の組み合わせの規格

半角文字:「ASCII」という名前の文字コード
(半角文字の文字コードは1種類なので普通は文字化けしない)

256文字しか表現できない=日本語には足りない

日本語はどうやって表現する?



文字コードのおはなし[2](p. 89)

○日本語(全角文字)は、半角文字を2文字組み合わせることで表現

➡ 最大65536文字の表現が可能

どの半角文字を組み合わせることで全角文字を表現するかで
いくつかの組合せ方(文字コード)あり

日本語の文字コード

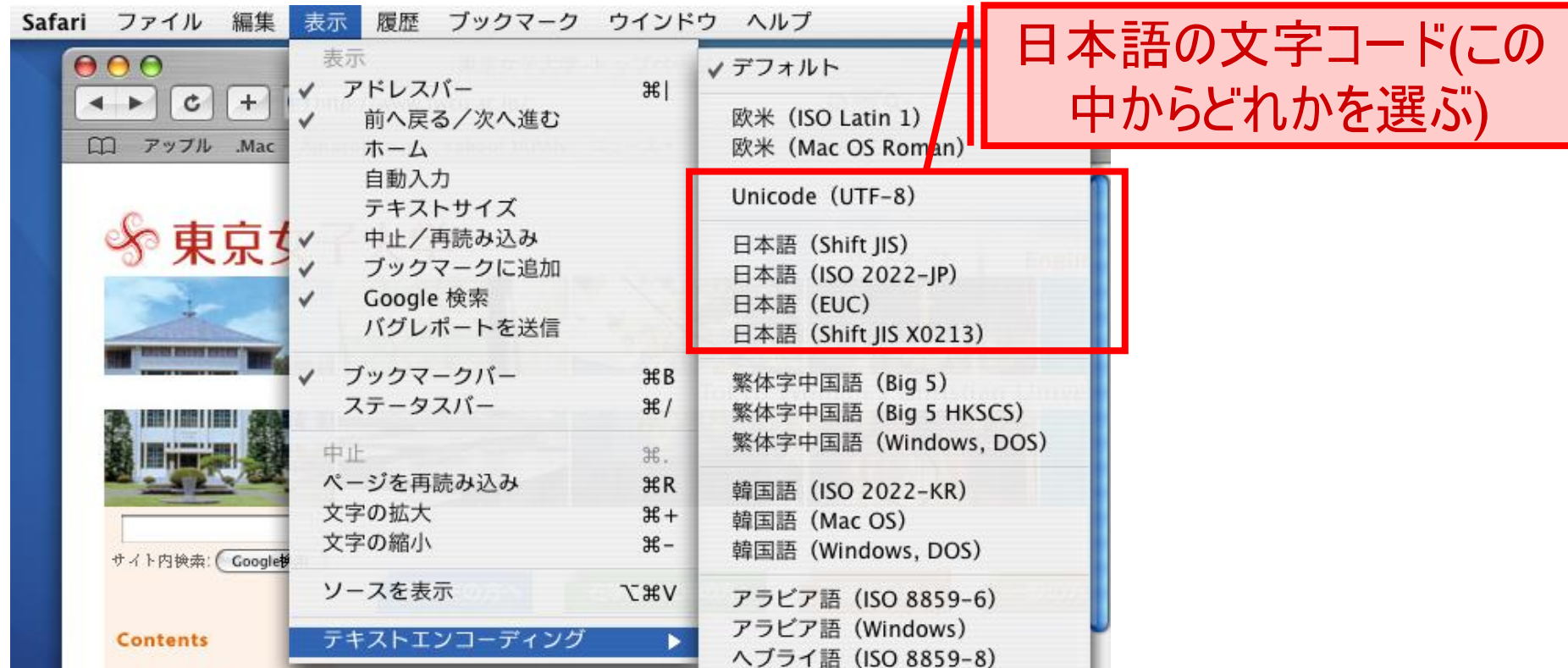
- UTF-8(MacOSで使われる文字コード)
- Shift JIS(Windowsで使われる文字コード)
- ISO-2022-JP
- EUC-JP

文字化け: Webページがどの文字コードで書かれているかをWebブラウザが
判断できないときに起こる現象



文字化けの直し方(p. 89)

- メニューバーの「表示」→「テキストエンコーディング」→「文字コードの名前」をクリックする



Webページ利用の注意事項



全般的な注意事項(p. 90)

- 怪しいページを見ない
- 怪しいリンクをクリックしない
- 個人情報をむやみに入力しない



ありがちな被害(p. 90)

- ページを見ただけで料金を請求された
- 無料と書かれていたのに料金を請求された
- 全く見ていないサイトの料金を請求された
- ネットオークションで詐欺にあった
- 届いたメールに書かれていたWebサイトにアクセスして口座番号や暗証番号を盗まれた
- インターネットカフェで、入力したキーの記録から情報を盗まれた
- ページを見ただけでウィルスに感染した
- 自分が公開したページを見てストーカーされた
- 掲示板で誹謗・中傷された
- etc.



ありがちな被害～架空請求～[1](p. 90)

- 心当たりのない請求は、原則として無視すること
- ただし、最近では、架空請求で裁判を起こされることも

裁判を起こされると、裁判所からの正式な通知(郵便)が届く

➤ 裁判所からの通知を無視すると...?



裁判に敗訴する



法的に支払い義務が生じてしまう!
(架空請求なのに)

裁判所からの正式な通知は無視しない!
国民生活センターとか弁護士とかに相談すること!



ありがちな被害～架空請求～[2](p. 91)

○最近、裁判所を名乗った通知がメールで届くことも多い

but...

- 裁判所からの通知は必ず郵便!
- メールで届くことはなし!

メールであれば無視してOK



ありがちな被害～偽のサイト～[1](p. 91)

- もっともらしいURLを書いたメールを送信し、URLにアクセスさせる
 - URLは、銀行やクレジットカードの会社などを装っている
- 開いたページで個人情報を入力させる
 - 開いたページは、もっともらしく作ってある
 - ウィルスを使って本物のサイトにアクセスさせないケースもある
- 入力された情報を盗み取る
 - クレジットカードの番号やユーザ名、パスワード, etc.

本当に信頼できるページかどうか、よく確認すること

- まともな銀行や会社がメールで個人情報を問い合わせることはない

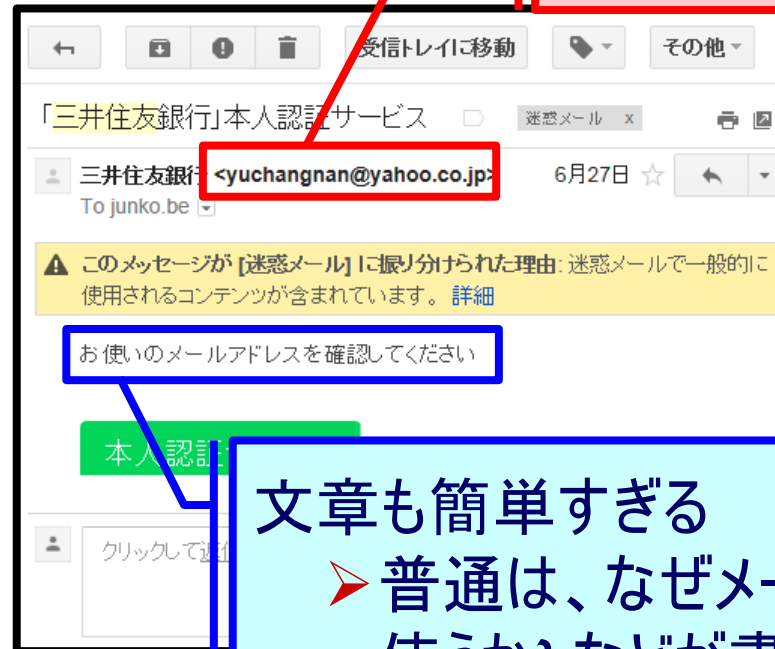


ありがちな被害～偽のサイト～[2](p. 91)

○実際のフィッシング詐欺の例

ドメインから考えて、銀行のメールアドレスではない

- メールアドレスはYahoo!のフリーメール
- まともな銀行が、フリーメールでメールを送ってくるはずがない



文章も簡単すぎる

- 普通は、なぜメールアドレスの確認が必要か? 何のためにこの情報を使うか? などが書かれてあるはず
- 問い合わせ窓口もあるはず

ありがちな被害～入力の記録～(p. 91)

- **キーロガー**: キーボードで入力したキーの記録をとるソフトウェア
 - インターネットカフェのPCなどで動いていることもある
 - とられた記録を見ると、クレジットカードの番号やパスワードなどを盗まれる

不特定多数の人が使うコンピュータで
個人情報を入力しないこと!



ありがちな被害～ウィルス[1]～(p. 91)

○ウィルスの感染経路

- メール

- Web

 - リンクをクリックしてページにアクセスしただけで感染するウィルスも存在

- コンピュータのセキュリティホール

- USBメモリやCD・DVDなどの記憶媒体

- 自宅などのネットワークの環境によっては、PCの電源を入れたただけでウィルスに感染する場合も



ありがちな被害～ウィルス[2]～(p. 91)

○ウィルスソフト

- ウィルスは毎日新しいものが出てくるので、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新しいウィルスに対応させるための権利(更新権利)は、通常60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)を購入する必要がある

ウィルスソフトの導入と更新を必ずすること!

- 必ず導入し、こまめに更新すること
- 更新の権利は必ず購入すること



ありがちな被害～ウィルス[3]～(p. 91)

○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、見つかりとそれを修正したり埋めたりするためのソフトウェア(パッチ)が出る

アップデートはこまめに行うこと!

- Windows Update
- Office Update



ありがちな被害～ウィルス[4]～(p. 91)

- Windows Update: Microsoft Windowsのための不具合やセキュリティホールを修正するソフトウェア
 - 「スタート」→「すべてのプログラム」→「Windows Update」とたどる
 - Windows UpdateのWebページが表示されるので、そのページの指示通りに操作をしていく
 - 「優先度の高い更新プログラム」の数が「0」になるまで、この作業を繰り返す
 - 1回この作業をしただけでは不十分なこともある



ありがちな被害～誹謗・中傷～(p. 92)

○掲示板やメーリングリスト等で自分のことを誹謗・中傷された場合

○原因を冷静に考えてみる

- 不当なまたは誤解されるような書き込みをしていないか
- 必要以上の個人情報を書き込んでいないか, etc.

あれば、その内容を削除・修正したり、誤解を解くように努力する

○プロバイダや掲示板管理者に連絡し、誹謗・中傷の内容を削除し、 そういう行為を厳重注意するよう要請する

○加害者が学内の関係者の場合は、人権相談委員に相談するのも良い

○悪質な場合には、警察に相談することも考える



情報源と相談窓口(p. 92)

○犯罪や被害に関する情報

- 国民生活センター

- 警察庁

- インターネットホットライン連絡協議会

- プロバイダ

 - NTT DoCoMo, au

○困ったときの相談的窓口

- 全国の消費生活センター

- 警視庁ハイテク犯罪総合センター

※URLは教科書参照



個人情報を入力[1](p. 93)

○個人情報の入力を求めるページは多い

自分の使っているコンピュータから相手のコンピュータに直接情報が届くわけではない

➡ 途中で個人情報が盗まれたりしない?

入力された個人情報を扱う人は誰だかわからない

➡ 情報を受け取る人は信頼できる?

例えば...ショッピングをするページ

品物売る気はなくて、個人情報を集めることが目的のページも

○掲示板などは、基本的には全世界から見える

○個人情報を書き込むと、世界中から見えてしまう



個人情報を入力[2](p. 93)

○ 個人情報が、それを集めることを目的とする人に渡ってしまったら?

- 名簿業者に売り渡される
 - ➡ 様々な業者に個人情報が売られる
 - ➡ 勧誘・ダイレクトメールなどが増える
- ひどい場合には、ストーカーの被害にも

個人情報の入力は慎重に!

- 入力しても大丈夫かどうかよく考える
- 入力が必要な場合には、必要最小限に
(必須項目以外は入力しない、など)



個人情報を入力[3](p. 93)

- 自分の個人情報: 入力していいかは自分の判断でOK
- 他人の個人情報: 扱う権利は自分にはない

例えば友達の個人情報を入力してしまったことで、
その友達が被害にあってしまったら?

他人の個人情報は絶対に
入力しない!



情報の信憑性(p. 93)

- Webページには様々な情報が掲載

- 様々な人が、様々な目的でWebページを作成

- 情報の真偽を確認せずに掲載されているもの
- 悪意を持って間違った情報を掲載しているもの
- etc.

※Webページを作成しているのは人間なので、大手企業などの信頼できそうなWebページの場合でも、間違い情報を掲載することも

内容を信じるかどうかは自分の責任

- 公的機関や信頼できる組織が公開しているページの内容を信頼する
- 複数のWebページを調べる(ただし、複数の Webページで同じ間違い情報を載せていることも)
- etc.



匿名性[1](p. 94)

- コンピュータでは、様々な行為の履歴を記録
- 例えば...掲示板
 - 様々な話題について、Web上で自由に意見を交換する場

発言者:A 2018/05/1 13:00:00
今度出たXXXのケーキってどう思います?
食べてみた人いませんか?

発言者:B 2018/05/1 13:05:30
とってもおいしかったですよ。おすすめです。

発言者:C 2018/05/1 13:10:10
うーん、私はあまりおすすめできないかも。
ちょっとパサパサしているような気が...



匿名性[2](p. 94)

○発言内容を見る人は、その発言をした人の顔は見えない

直接会ったり電話で会話するとき:

- 相手の顔の表情や声のトーンを見聞きできる

掲示板

- 掲示板を見る人は、文字だけしか見えない

➡ 発言をした内容が、自分が全く意図しない意味で解釈され、トラブルになることも

書き込む文章の表現には十分注意



匿名性[3](p. 94)

○何か問題のある発言をすると、必ずばれる!

問題のある発言をしてしまったとき:

- その掲示板などの管理者から東京女子大学に連絡
- 東京女子大学で、その発言をした人を特定

掲示板の管理者が持っている記録

問題のある
発言

2018年5月1日 13:30:30
from 東京女子大学XX番のコンピュータ
発言内容

2018年5月1日 13:35:55
from AプロバイダのYY番のコンピュータ
発言内容

管理者が
知らせてくるもの

2018年5月1日 13:50:20
from B会社のZZ番のコンピュータ
発言内容



匿名性[4](p. 95)

○誰が、いつからいつまで、どのコンピュータを利用していたかを調査可能

東京女子大学で持っている記録
XX番のコンピュータ

問題発言を
した人と特定

2018年5月1日 13:00:05～14:20:50
利用者:A(ログイン名)

2018年5月1日 15:05:15～15:40:20
利用者:B(ログイン名)

2018年5月1日 16:00:00～17:30:40
利用者:C(ログイン名)

※この記録は、何か問題があったときのみ調査され、通常は見られたりしない

インターネットに匿名性はなし!



Twitter・Facebook・LINE[1](p. 94)

○最近、トラブルが急増

- 仲間内での雑談のつもりで書き込んだ発言
- 軽い気持ちで規則違反やありもしないことを発言
- etc.

第3者に見られて問題に発展

- 発言者の所属機関(大学など)に通報されて、発言者が処分される
- TVや新聞などに通報されてニュースになる
- etc.

いつ、誰に見られているかわからない!

- 問題発言を探して発言者を特定し、公表するような人も...



Twitter・Facebook・LINE[2](p. 94)

○情報の信頼性の面も問題

○発言当時は正しくても、少し時間がたつと古くなることも

- Ex. 東日本大震災で、救助を求めるTwitterのつぶやきがあり、その人にメールを送っても返事が来ない(すでに救助済みだった)
→救助を求める他の発言も、疑われる事態に

○「拡散希望」という発言も、真実である保証はなし

○悪質なWebサイトに誘導される場合も

- ウィルスを仕掛けたサイトに誘導するなど

知らない人が書いているURLをむやみにクリックしない!



Twitter・Facebook・LINE[3](p. 94)

- Facebookは実名登録が原則で、個人情報公開
 - 反社会的なグループに登録される
 - スパムを送りつけられる
 - 「友達を探す」ことで、自分のアドレス帳を全世界に公開することになる
 - etc.

- 適切なプライバシーを設定する!
- アプリケーションの招待などを不用意にクリックしない!
- 知らない人を友達登録しない!



Twitter・Facebook・LINE[4](p. 94)

- LINEでは見ず知らずの人と連絡を取ってしまうことも
 - 実際に会うことでトラブルに巻き込まれる
 - 自宅に押しかけられたり、いたずら電話が来る
 - メッセージに従って会員登録して架空請求の被害にあう
 - etc.

- LINE IDを知らない人と交換しない!
- LINE IDをインターネットの世界で書かない!
- 知らない人から友達に追加されないようにLINEを設定する!



Twitter・Facebook・SNS[5](p. 94)

○個人情報の漏えいの危険

○GPS付きのカメラで撮った写真やスマートフォンからの発言

- 写真にGPSの情報が埋め込まれる(自宅で撮影したペットの写真など)
- 発言に、どこから発言したかのGPSの情報が付加される
(自宅から書き込めば、GPSでの自宅の位置情報が付加)

GPS情報をもとに、第3者に、自宅などの場所を知られてしまう

公開する写真を撮影するときや、スマートフォンから発言をするときは、
GPS機能をOFFにする!



結局のところ...

- Webに掲載した情報はどこの誰に見られるかわからない!
 - Twitter, Facebook, etc.
- 一度掲載した情報は、回収できない!
 - 自動的に世界中のWebサイトを回って情報を集めているソフトウェアも...
 - = 自分が掲載した情報の削除処理をしても、自分の権限の及ばないどこかに保存されている
- 悪人はいろいろな手口を考えて人をだまそうとする!

➤ 安易に情報を公開しない!
➤ 怪しいメッセージに反応しない!

