

情報処理技法(リテラシ)I

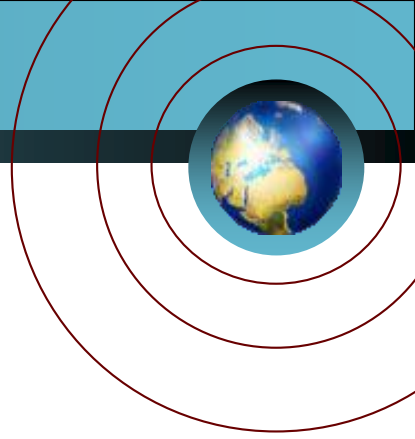
第5回 電子メール(2), WWW(1)



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

- 電子メールの読み書き(続き)
- メール利用の注意事項
- WWW



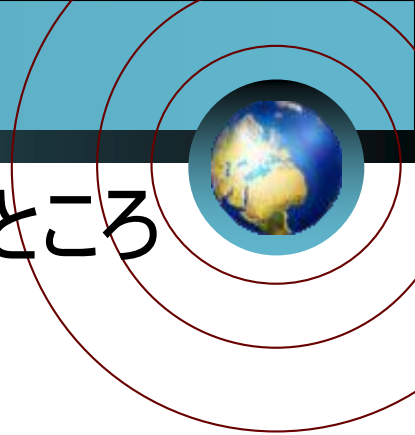
前回の復習問題の解答(問題2)



- 自宅のPCのセキュリティについて、下記の中から適切なものをすべて選択しなさい。
 - a. ネットワークにPCを接続しただけでウィルスに感染することはない。
 - b. ウィルスに感染すると、自分のPCが官公庁のコンピュータに攻撃をすることがある。
 - c. ウィルス対策ソフトに対してかかるお金は、PCへの導入時のみ必要である。
 - d. スマートフォンがウィルスに感染することがある。
 - e. パスワードが他人に知られなければ、不正アクセスを受けることはない。
 - f. Webページにアクセスしただけでウィルスに感染することはない。

解答: b, d

「迷惑メール」ボックス[1](p. 76)



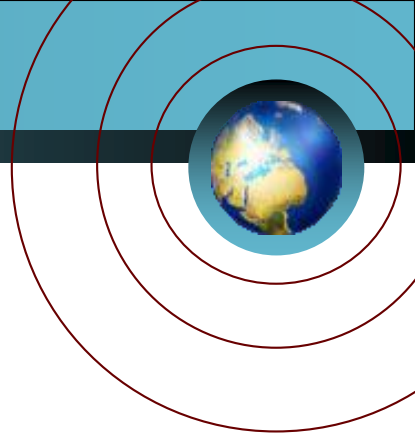
- 東女Gmailが「迷惑メール」と判断したメールが保存されているところ
 - 東女Gmailの迷惑メール判断機能は非常に強力
 - ほとんどの迷惑メールを自動的に判断可能
 - 迷惑メールと判断されたメールは、自動的に「迷惑メール」に保存

but...

非常に強力すぎて、逆に、必要なメールを迷惑メールと判断することもしばしば

- 授業の先生からの授業に関するメール
- 友達からのメール
- etc.

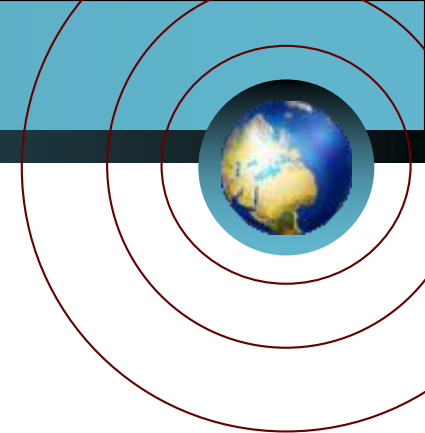
「迷惑メール」ボックス[2](p. 76)



- 「迷惑メール」に入れられたメールは、30日後に自動的に削除
 - 削除されたら、もう2度とメールは戻ってこない

最低限、1ヶ月に1～2度程度は迷惑メールボックスをチェックして、大切なメールを救おう!

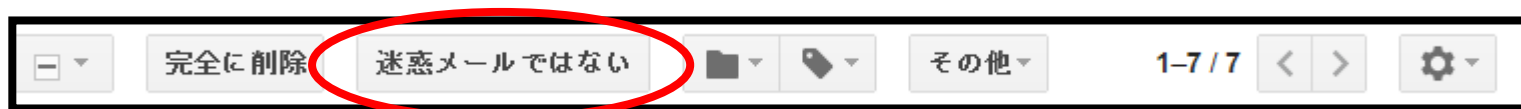
「迷惑メール」ボックス[3](p. 76)



- 迷惑メールボックスからメールを救うには...
 - 「開く」→「迷惑メール」とたどって、必要なメールを探す

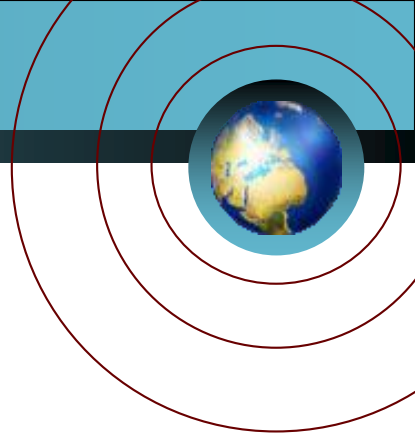


- 必要なメールの左側にチェックをする
- 「迷惑メールではない」ボタンを押す



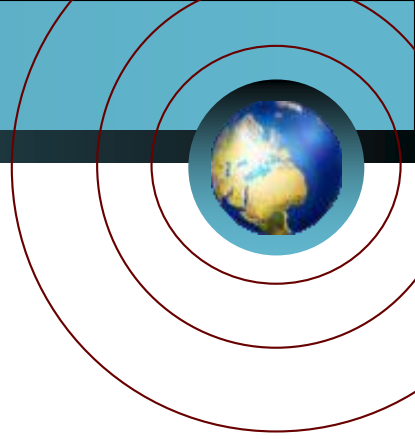
やってみよう!

- 演習4.2.8(p. 72)
- 演習4.2.9(p. 75)
- 演習4.2.10(p. 75)
- 演習4.2.11(p. 75)

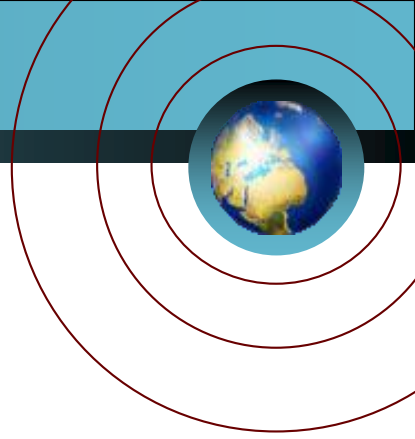


メールの終了(p. 66)

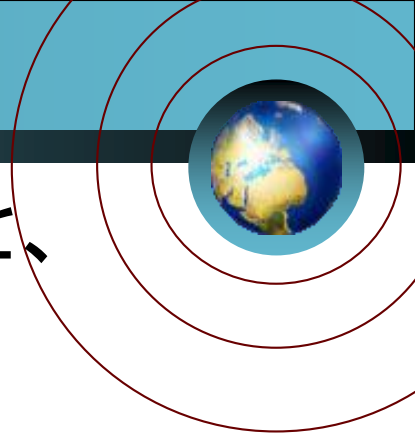
- 画面右上のメールアドレス→「ログアウト」



電子メール～一般的注意～



メールアドレスは正確に(p. 76)



- メールを送りたい相手のメールアドレスを、1文字でも間違えると、相手のところには届かない

間違えたメールアドレスが

➤ 存在しないメールアドレスの場合:

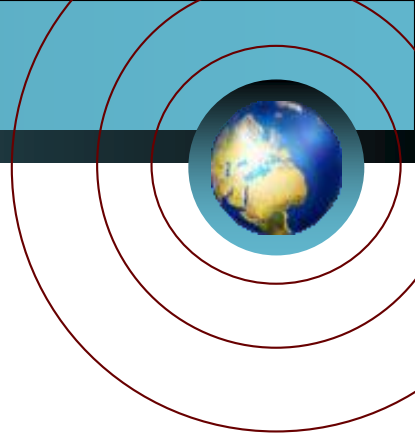
➡ 「Mail Delivery System」(MAILER-DAEMONなど)という人からメールが来る(宛先不明で届かなかったという意味)

➤ 存在するメールアドレスの場合:

➡ そのメールアドレスの持ち主(全く知らないかもしれない人)に自分が書いたメールが届く

メールアドレスは間違いないように
よく確認すること!

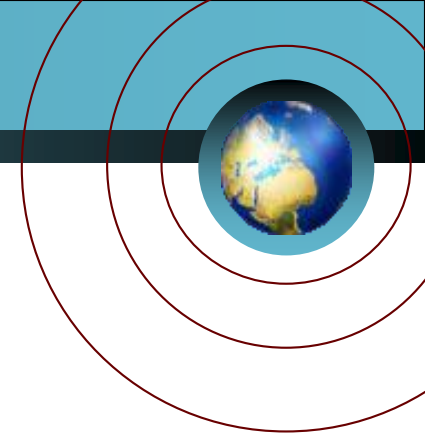
メール配送の信頼性(p. 77)



- メールはすぐ届かないことも
 - メールが通る経路が混雑
 - メールを送る・受け取るコンピュータの故障

非常に重要なメールが届かなかったかもしれない場合は、相手に確認してみることを

メールの安全性[秘匿性](p. 77)



- メールは、自分のコンピュータから相手のコンピュータに直接届くわけではない

- いくつかのコンピュータを経由して届く

どこの誰が管理しているかわからないコンピュータも...

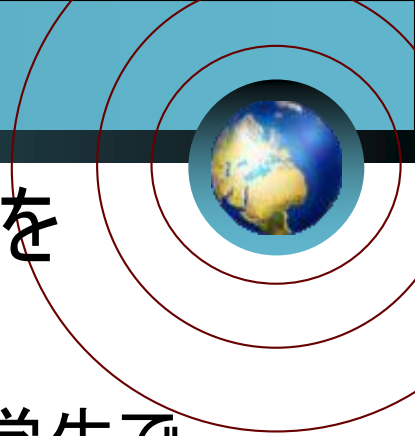
- 一般的に、メールの秘匿性(他人に読めない程度)は
はがき程度

➡ メールの内容が途中で読まれる可能性も...

メールに重要な情報は書かない!

- 住所や電話番号
- クレジットカードの番号
- etc.

大学のメールアドレスの利用[1](p. 77)

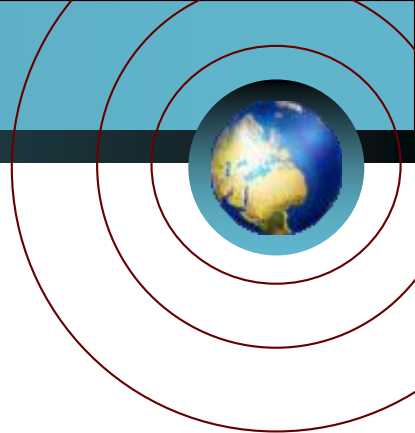


- 大学のメールアドレス: 自分が東京女子大学の学生であることを証明できるもの
 - プロバイダや携帯電話、フリーメールのアドレスは、東京女子大学の学生でなくても持つことができる
 - 特に携帯電話やフリーメールのアドレスは...
 - 簡単に変えることができる →
メールを送っても届かないかも、と思われることがある
 - 携帯メールでは、文字制限があることもある →
メールを送るときに、文字数を気にする必要がある

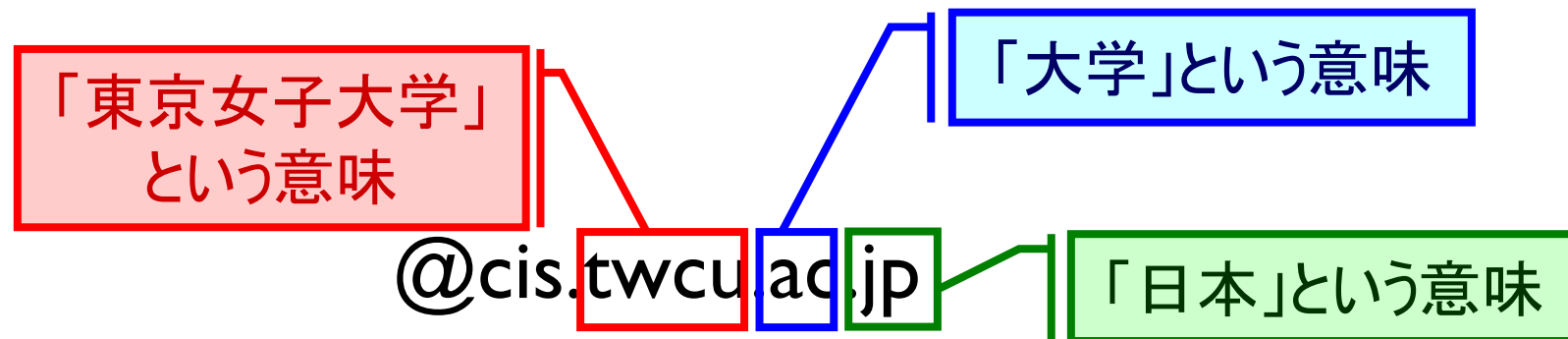
メールアドレスの信頼性が低い

➡ メールアドレスの持ち主の信頼にもかかわる

大学のメールアドレスの利用[2](p. 77)



- メールアドレスを見ると、大学のものかそうでないかはすぐわかる



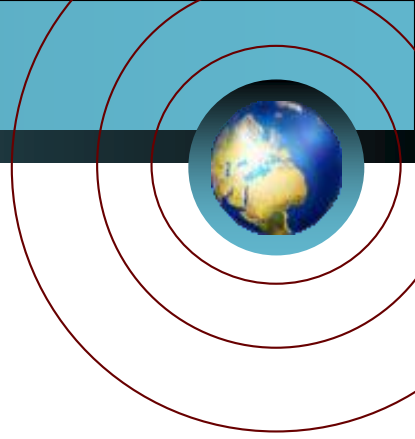
特に就職活動など、学生として活動をするときには...

やむをえない理由がない限り、
大学のメールアドレスを使おう!

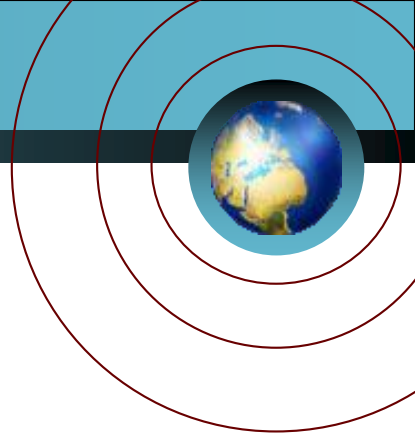
メールアドレスの使い分けをしよう!

- 大学のメールアドレス: 学生としての活動をするとき(あまり親しくない人とやり取りするとき)
- プロバイダや携帯電話、フリーメール: 友達などの親しい人とメールのやり取りをするとき

電子メール～妙なメール～



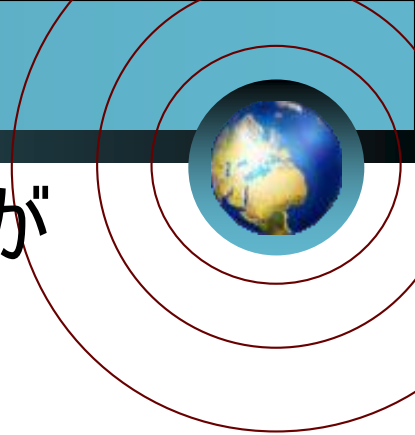
ねずみ講(p. 78)



- ねずみ講:「楽しんで儲ける」というたい文句の勧誘メール
 - 加入者をねずみ算式に拡大させて利益を出すしくみ
 - 「無限連鎖講の防止に関する法律」で禁止
 - 加入することも勧誘することも違法

おいしい話にだまされないように!
情報の真偽・信憑性・適法かどうかなどは自分で考えて
責任を持って判断すること!

ウィルスメール[1](p. 78)



- コンピュータにも、人間の病気のような状態があり、コンピュータが病気になると...

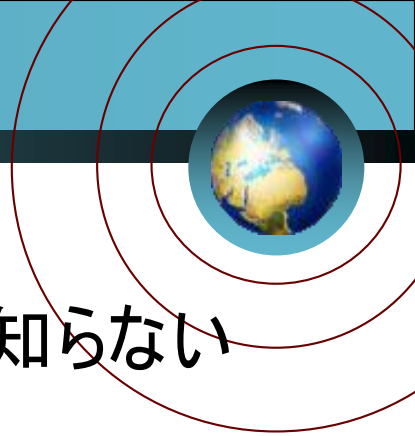
- 保存していたデータを破壊される
- コンピュータそのものが壊れる

コンピュータウィルスのためにこのような状態に

→ コンピュータウィルス:
メールから感染することが圧倒的に多い

メールにくっついてくる絵や写真、音声、文書などのファイルのふりをして
ウィルスがやってくる(添付ファイルから感染する)

ウィルスメール[2](p. 78)



- 自分のコンピュータがメールからウィルスに感染すると...
 - ウィルスは、友人や知り合いのメールアドレスに、自動的に(持ち主の知らないうちに)同じウィルスを送りつける



友人や知り合いのコンピュータもウィルスに感染

知らない間に自分が加害者になってしまう!

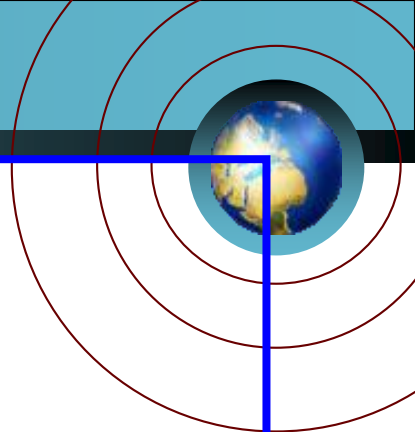
ウィルスに感染しないためには...

➤ 添付ファイルをむやみに開かない!

※送り主から聞いていない添付ファイルは、送ったかどうかを送り主に確認してみる

➤ 自宅のコンピュータはウィルス対策をしっかりとる!

スパムメール[1](p. 79)

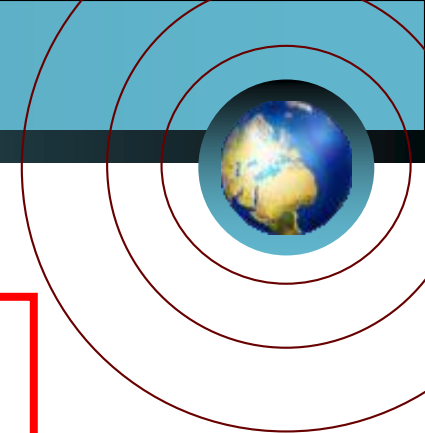


- 機械的に送られている大量のメール
 - サーバやネットワークに不具合を起こさせるということが目的
- 様々な勧誘のメールや脅迫のメール
 - 例えば...
 - 少しの労力で大もうけしましょう!
← 違法行為の場合もあり
 - あなたは借りたお金をまだ返していません。期日までに返さない場合は、大学や実家に担当者を...

送る人は、送るメールアドレスが存在するかどうか知らずに手当たり次第送っている

こういった迷惑なメールのことを「スパムメール」と呼ぶ

スパムメール[2](p. 79)



- 特に勧誘・脅迫メールの場合: 返事をしてしまったら...



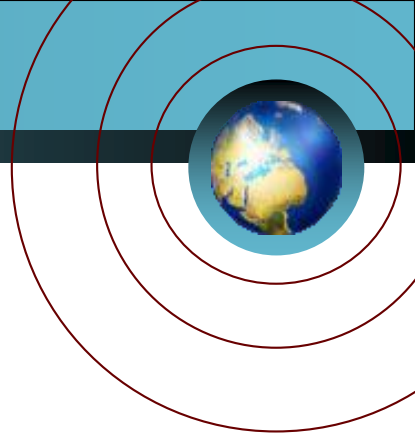
メールアドレスが存在することを、勧誘・脅迫メールを送った人に知られてしまい、さらに標的にされてしまう!

勧誘・脅迫メールを送る人は、メールアドレスが存在するかどうか知らずにメールを送り、返事が返ってくるのを待っている

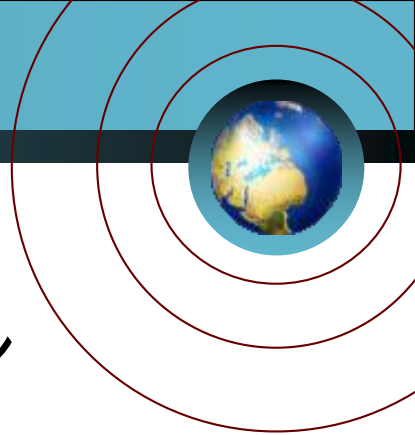
勧誘・脅迫メールには
絶対に返事をしないこと!

※「このメールが不要な人は、xxx@yyyに連絡を」という言葉があっても、連絡をすると、勧誘・脅迫がひどくなる(言葉が守られないことが多い)

電子メール～マナー～



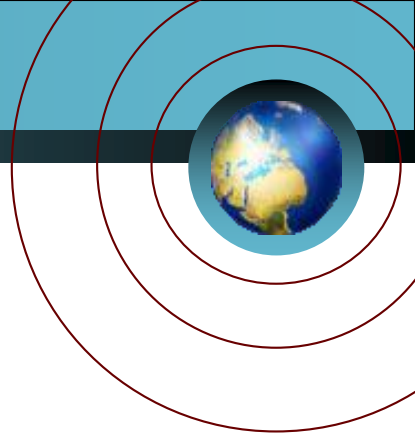
名乗って文章をきちんと書く[1](p. 79)



- 学生さんからのよくあるメール
 - その1: 何かの提出物のメールで、本文なし・添付ファイルのみのメール
 - その2: 「XXについて教えてください」という用件のみのメール

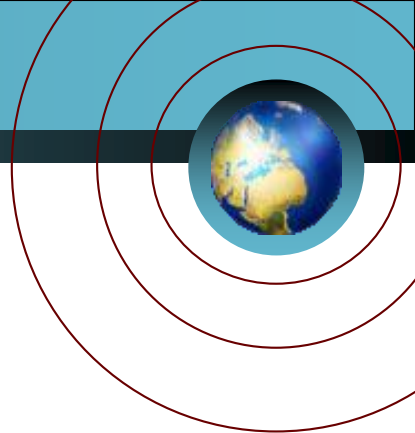
何がいけないか???

名乗って文章をきちんと書く[2](p. 79)



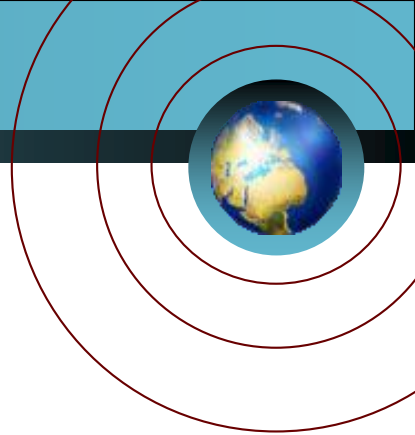
- いけないことその1: 誰が送ったメールかわからない
 - 携帯電話のメールの場合...
 - やりとりする相手は、親しい人の場合が多い
 - アドレス帳に名前やメールアドレスが登録されている
 - メールを送り主は誰かわかるように携帯電話が表示してくれる
 - コンピュータのメールの場合...
 - メールソフトには、メールアドレスのみしか表示されないことも多い
 - メールアドレスから、送り主の名前を調べる必要
 - 面倒 & 結局送り主の名前がわからないことも
 - 迷惑メールが多い世界なので、送り主がわからないメールは、気持ち悪い

名乗って文章をきちんと書く[3](p. 79)



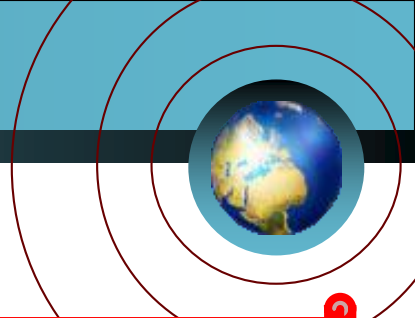
- いけないことその2: 本文をきちんと書いていない
(特に提出物のメールの場合), 用件だけ書いている
 - 携帯メールの場合...
 - メールを読む画面が小さいので、文字数は少ないほうが良いのでOK
 - 現実の世界で誰かと話をする場合...
 - 親しい友人であれば、会ってすぐ話し始めることも
 - あまり親しくない友人の場合、必ず「こんにちは」などの何らかの挨拶をしてから、話し始めるのが常識
- 挨拶をして話し始めるのがマナー
- コンピュータのメールの世界でも同じ

名乗って文章をきちんと書く[4](p. 79)



- いけないことその3: 本文をきちんと書いていない
(特に提出物のメールの場合)
 - 相手に何かを手渡しする場合...
 - 必ず、「これ、お願いします」など何か少し言って手渡すのが常識
→ **何も言わずに、ものだけ差し出すのは失礼**
コンピュータのメールも同じ(本文なしで添付ファイルだけ、というメールは相手にとって失礼)

名乗って文章をきちんと書く[5](p. 79)



■ 失礼なメールを書かないために...

1. 名前と所属(学科や専攻)をきちんと名乗る

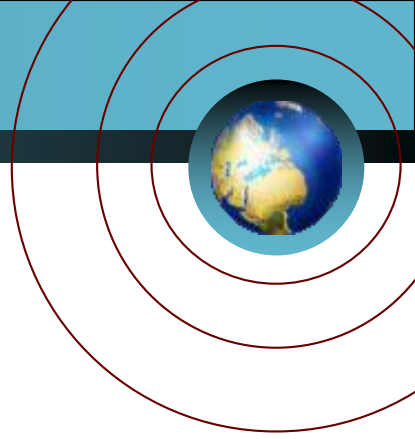
- メール本文の最初で名乗る
- 「こんにちは」などの挨拶文はあってもなくても良い(名乗ることが挨拶の代わり)
- 例: 本文の最初で「XX学科YY専攻ZZ年の東京子です。」

2. 本文をきちんと書く

- 質問等の用件は、わかりやすく丁寧に書く
- 提出物の場合には、「～を提出します。よろしくお願いします。」程度の文章を本文の最初で必ず書く

こういうことがきちんとできないと、社会人になったときに、まわりの人にマナーを知らない人、と思われるので、きちんと身につけよう

添付ファイルの名前(p. 81)

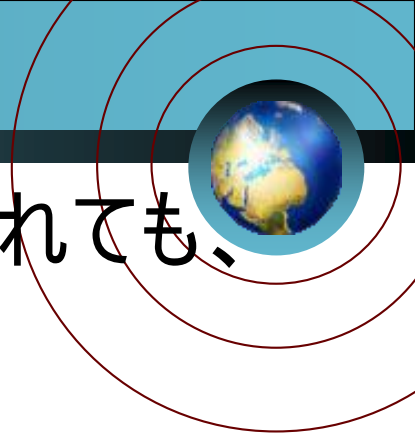


- コンピュータ上での日本語の扱いは様々な種類あり
 - Mac OSで作成した日本語ファイル名はWindowsでは使えない
(ファイルの名前がおかしくなってしまう)
 - Windowsで作成した日本語ファイル名はMac OSでは使えない
(ファイルの名前がおかしくなってしまう)

添付ファイルの名前に濁点・半濁点を
使わない!
(濁点や半濁点がついたファイル名はトラブルの元)

※できれば、半角英数8文字以内が望ましい

機種依存文字や絵文字[1](p. 81)



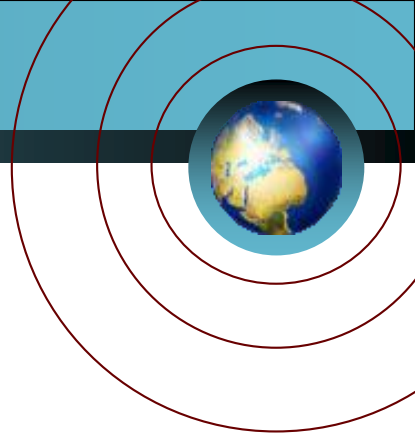
- いくつかの文字は、メールを書いたコンピュータでは正しく表示されても、メールを受け取ったコンピュータでは正しく表示されない

- ○つき数字
- ローマ数字(アルファベットのIやV, Xのような数字)
- ハートマーク
- 電話マーク
- 株式会社マーク
- 音符マーク(「♪」や「♫」), etc.

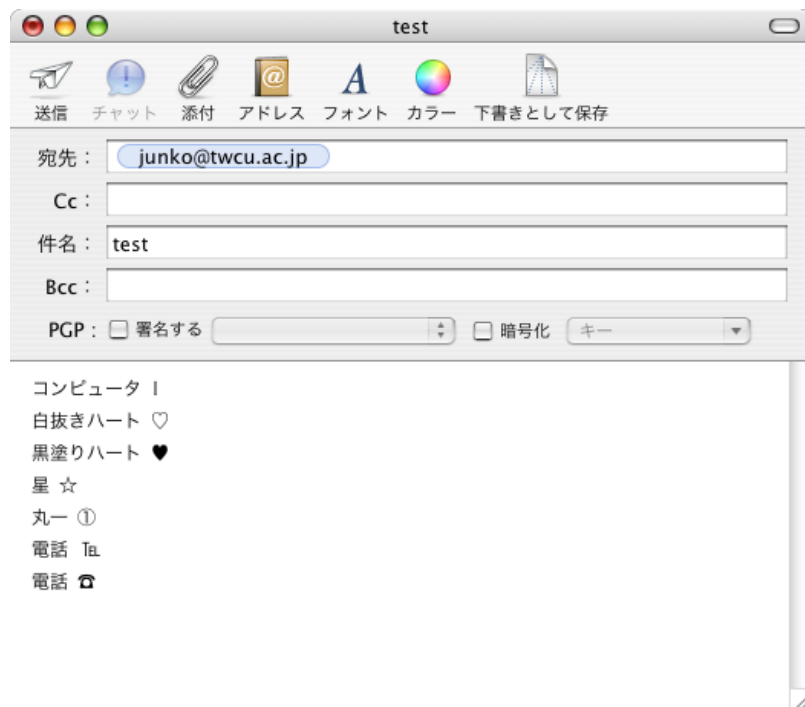
「機種依存文字」と呼ぶ

- 絵文字は、携帯電話の機種やキャリアが違くと、違う絵文字になる

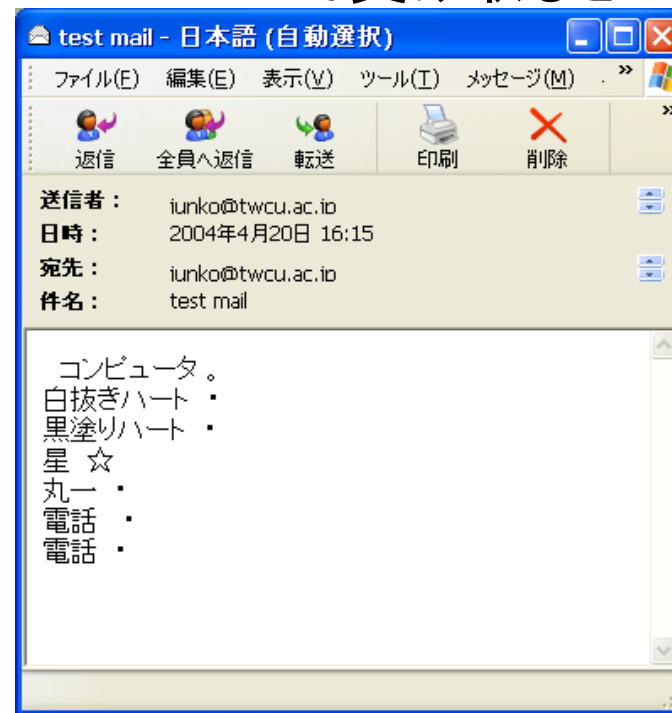
機種依存文字や絵文字[2](p. 81)



Macで送信したメール



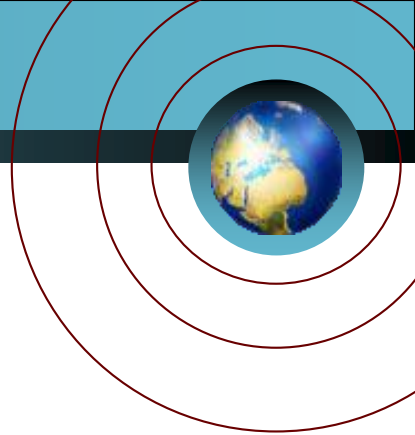
Windowsで受け取ると...



➡ メールを受け取る人は、どういうコンピュータを使っているかわからない!

特にコンピュータでのメールでは
機種依存文字や絵文字は使わないこと!

表現に注意(p. 81)



- メールを読む人は、書いた人の顔を見ながら読むわけではない

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

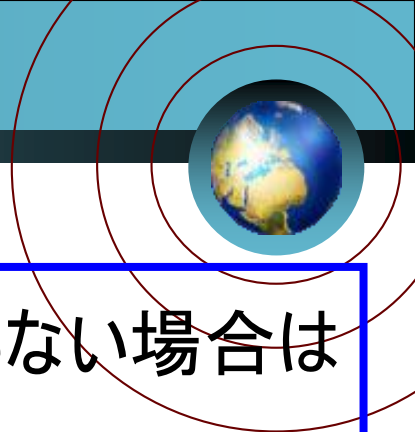
電子メール:

- 電子メールを読む人は、文字だけしか見えない

➡ メールに書いた内容が、自分が全く意図しない意味で解釈されることも

メールの文章の表現には十分注意

Bccの使いどころ(p. 82)

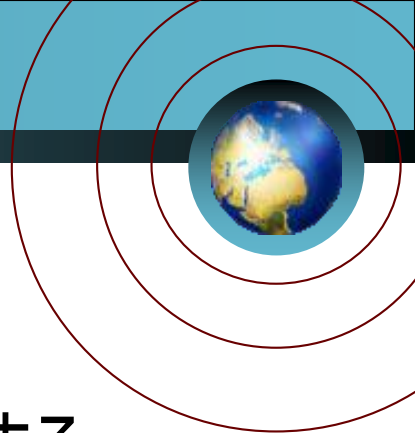


- メールアドレスも個人情報のひとつとみなされることも多い
 - 複数の相手に同じメールを送る場合、その相手同士がお互いを知らない場合は注意が必要

To: やCc: の欄に相手のメールアドレスを並べて書いてしまうと、他人の個人情報を勝手に他の人に知らせてしまうことにも...

お互いに知らない相手にメールを送るときはBcc: を使おう

Subject[件名](p. 82)



- Subject(件名): メールにつけるタイトル
 - メールの内容を簡潔に表すもの
 - メールを受け取った人は、Subject(件名)を見てメールの**内容**を判断する
緊急性があるか、後回しにしてもいいか、etc.

適切なSubject(件名)をつけることは、メールの重要なマナー

Subject(件名)は具体的かつ簡潔に
(必ずつけること!)

Ex.

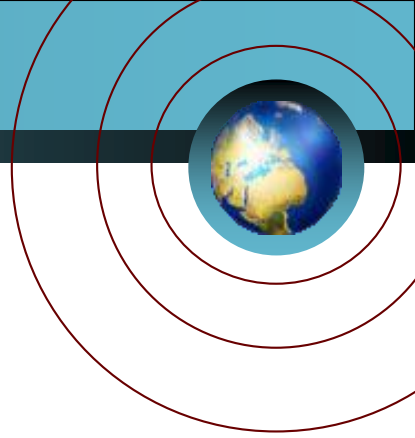
~~「質問」~~

~~「こんにちは、東京子です」~~

「ブラウザで画像が表示されません」

「Excelの授業に関する質問」

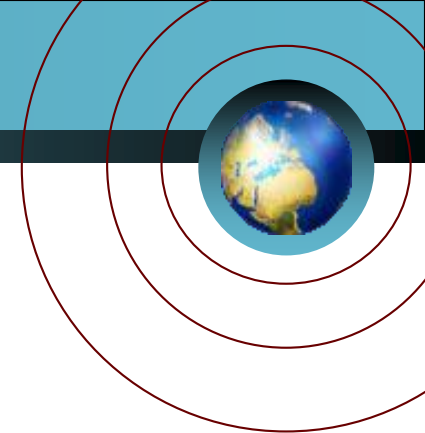
添付ファイルの大きさ(p. 82)



- ファイルにはそれぞれサイズあり
 - 絵のファイルやPowerPointファイルなどはかなり大きくなることもあり
 - サイズの大きなファイルを送ると、相手に迷惑がかかることも
 - 1つのファイルでもサイズの大きなものを送る場合
 - 1つ1つのファイルは小さくても、複数送る場合

添付ファイルのサイズには要注意!
送信前に確認すること!

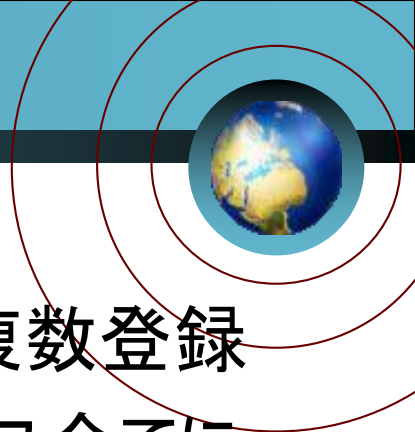
個人情報管理(p. 83)



- コンピュータネットワークには情報漏えいの危険はつきもの
 - メールの署名などに個人情報を書いておくと...
 - メールを受け取る側としては便利
 - メールを送る側は、個人情報がどこの誰に知られてもおかしくない状態

自宅の住所や電話番号は
メールの署名には書かないようにしよう

メーリングリスト(p. 83)



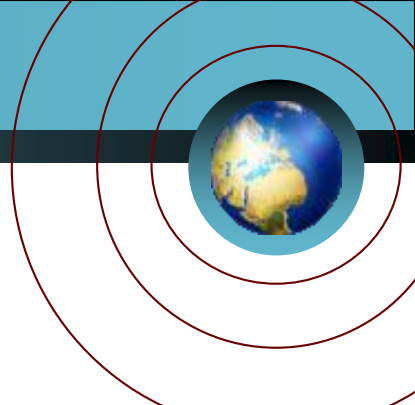
■ 仕組み

- あるメールアドレス(メーリングリストアドレス)に、別のメールアドレスを複数登録
- メーリングリストアドレスにメールを送ると、登録されているメールアドレス全てに同じメールが送信メールの「宛先」の欄に、メーリングリストアドレスを入力する

■ 注意

- メーリングリスト宛で届いたメールにそのまま返信すると、メーリングリストに返信される(登録されている人全員に返信メールが送られる)
 - 個人宛に返信すべきか、メーリングリスト宛に返信すべきかをきちんと考えること
 - 個人情報の漏洩にもなることがあり、プライバシーの侵害になることも
 - メーリングリストでの議論を、メンバの許可なく公開することは不可
 - 個人宛の誹謗中傷をしてしまったりと、刑法の「名誉毀損罪」にあたることも

課題のお知らせ

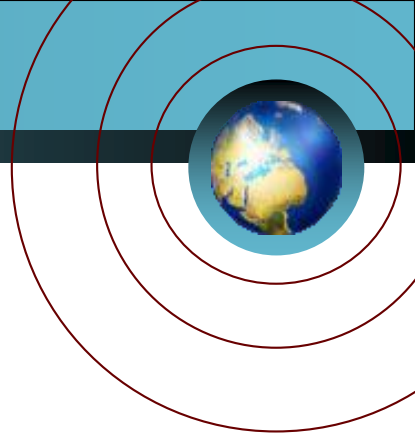


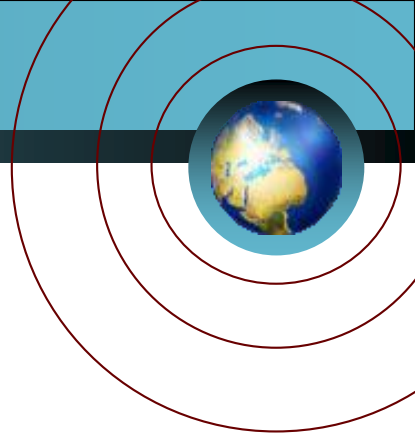
- 課題内容と×切:

<http://www.cis.twcu.ac.jp/~junko/Literacy/>

- 課題提出用と連絡用のメールアドレスが違うので、間違えないように注意すること
 - 課題提出用のメールアドレスで、質問などは受け付けない
 - 連絡用のメールアドレスで、課題提出は受け付けない
 - 課題提出・質問とも、大学のメールアドレスから送られたメールでなければ受け付けない

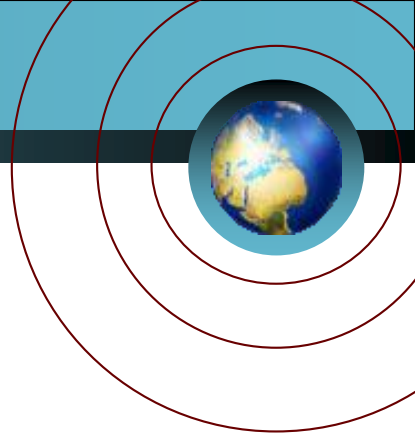
Webページ閲覧の仕組み



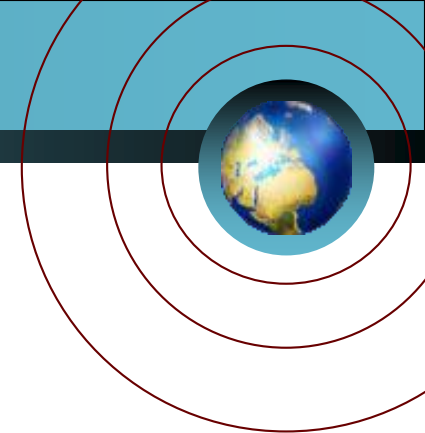


- 「World Wide Web」の略
 - 「世界中に張り巡らされたくもの巣」という意味
 - 様々な情報を公開・閲覧するための仕組み
- インターネットを使うサービスの1つ
 - CERN(ヨーロッパ高エネルギー物理研究所)で、研究者がデータなどをお互いに検索するために開発
- 「ブラウザ(browser)」というソフトウェアを使って情報を閲覧
 - Webページ:文章や図が入ってブラウザの中に表示される内容

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.

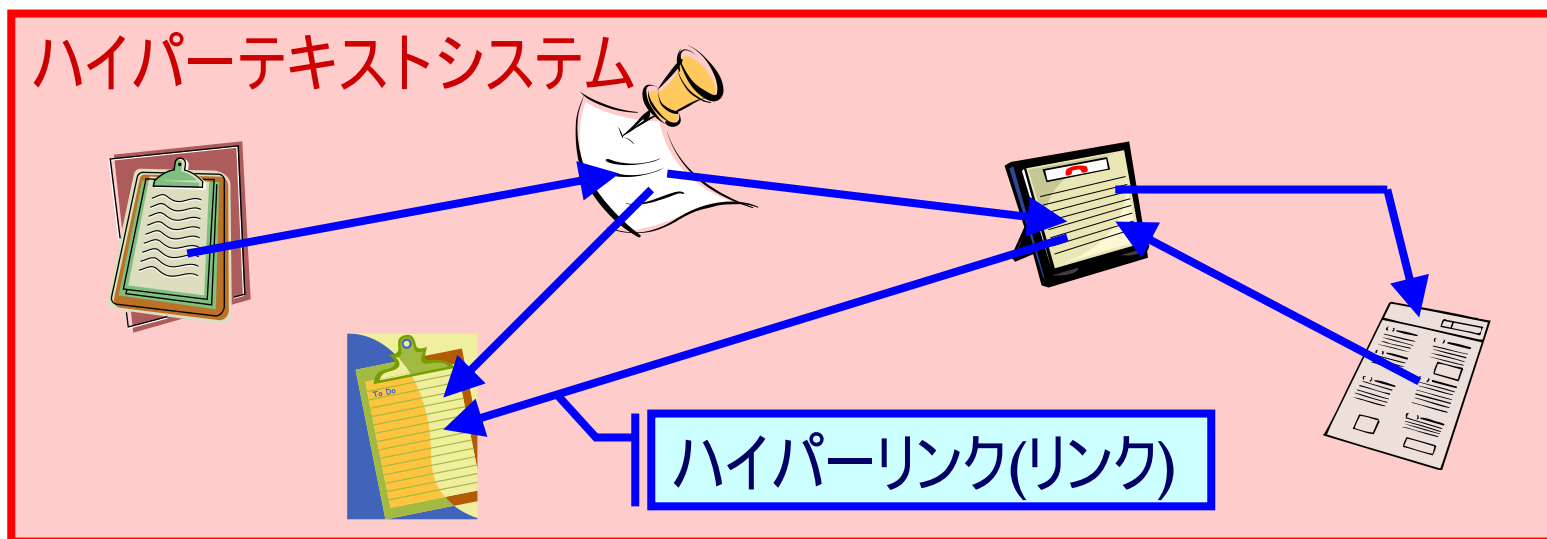


■ ハイパーテキスト形式の情報表現方法

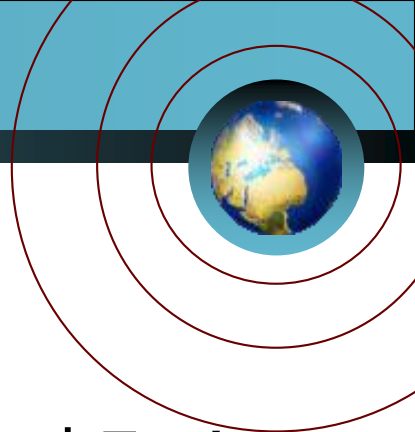
- 情報は通常、何ページかに渡り、その最初のページを「トップページ」

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

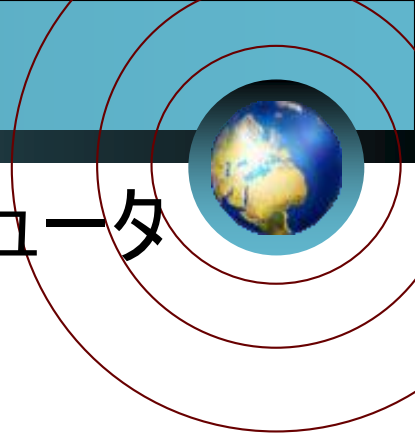


リンクって?(p. 85)

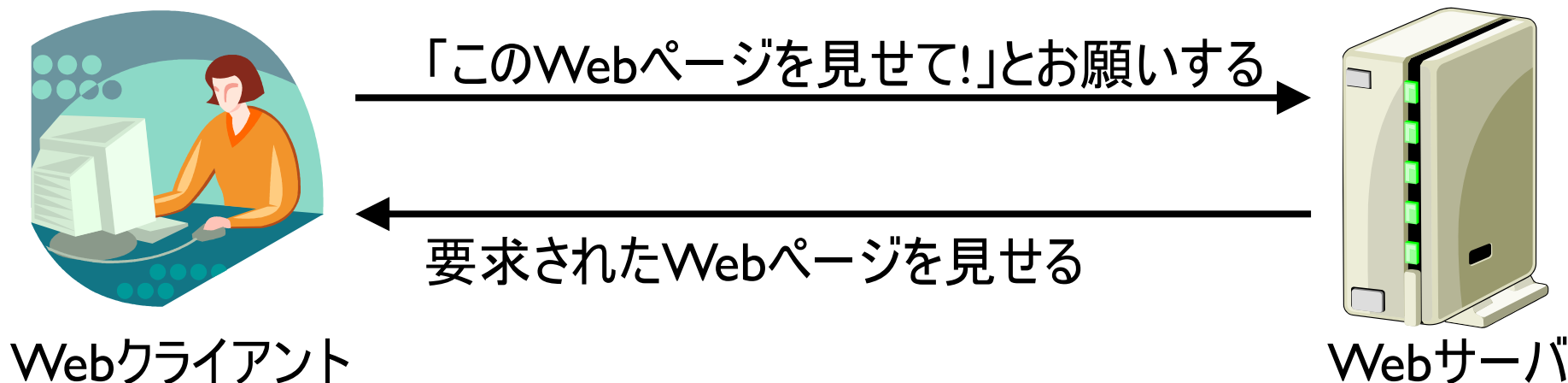


- ハイパーリンクの略
- クリックすることで別のページを見ることが可能
 - 通常、リンクは別のページへの「**URL**」を指し示しており、リンクをクリックすることで、そのページが表示される
 - **URL(Uniform Resource Locator)**: Webページが置いてある場所についての情報(ページの住所)
- リンクをたどることで様々なページを見ることが可能
 - リンクがクモの巣のように張り巡らされている

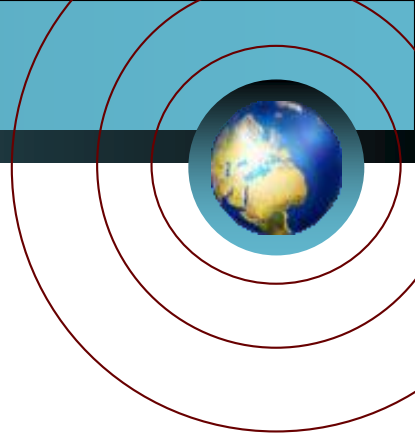
WebサーバとWebクライアント(p. 85)



- **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)



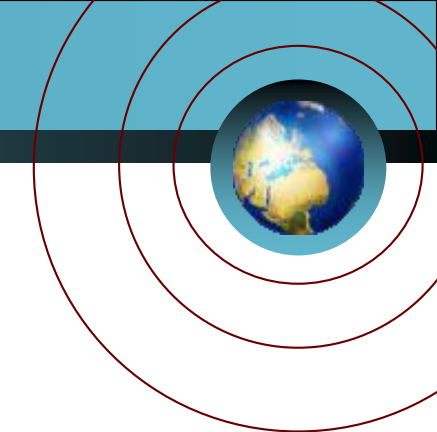
- Webページのありかを示す情報

- 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

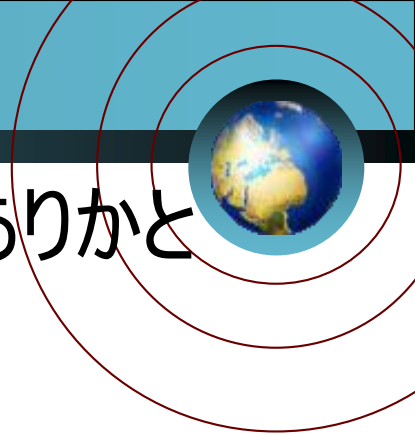
WebサーバとWebクライアントとの間で通信をするためのプロトコル

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

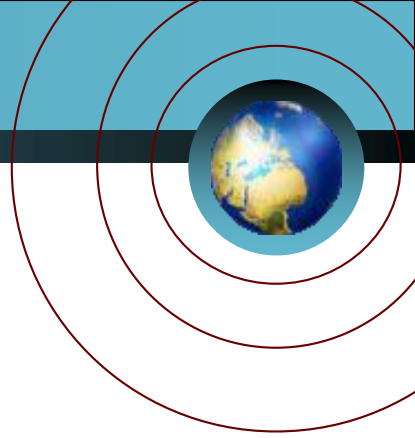
`http://www.cis.twcu.ac.jp/cis/index.html`

「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`

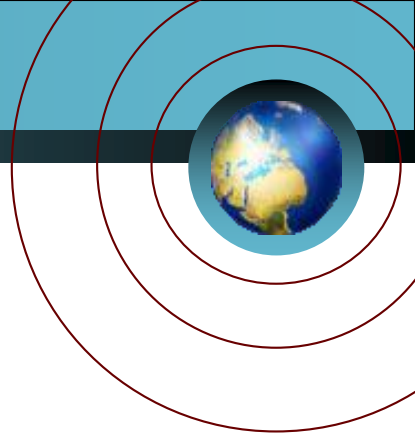
「東京女子大学のWebサーバの中の『~junko』というフォルダの中の『LiteracyI』というフォルダの中の『abc.html』というファイル」という意味

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

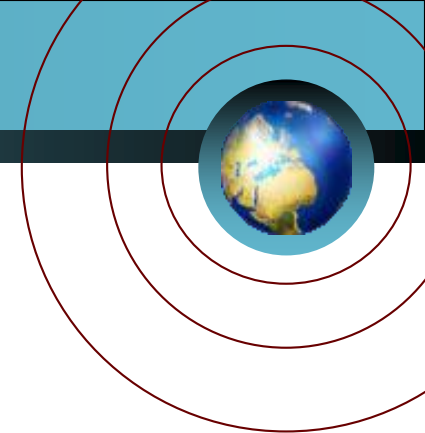
URLって?[5](p. 86)



- 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
 - **`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

同じURL(同じファイルを探す)

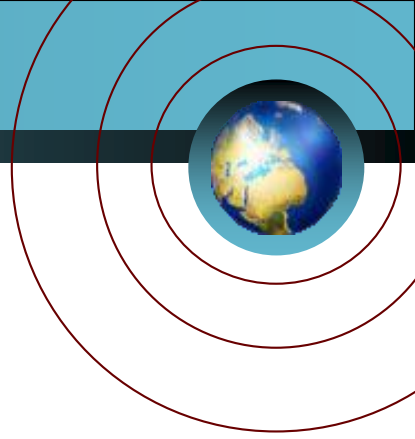
httpとhttps(p. 86)



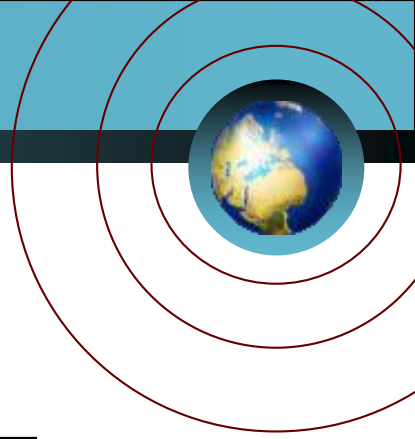
- どちらもWWWでのプロトコル
 - http: HyperText Transfer Protocol(**http**://～というURL)
 - https: HTTP over SSL/TSL(**https**://～というURL)
 - インターネット上でデータを暗号化して送る仕組み
 - インターネットショッピングでの個人情報の送信やWeb上での認証、電子メールなどで利用
 - 東女Gmailもhttps
- インターネットでのデータの送受信は...
 - httpだと: 経由したところで中に書かれてあるデータをそのまま見ることが可能
 - httpsだと: 経由したところで中を見られても、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

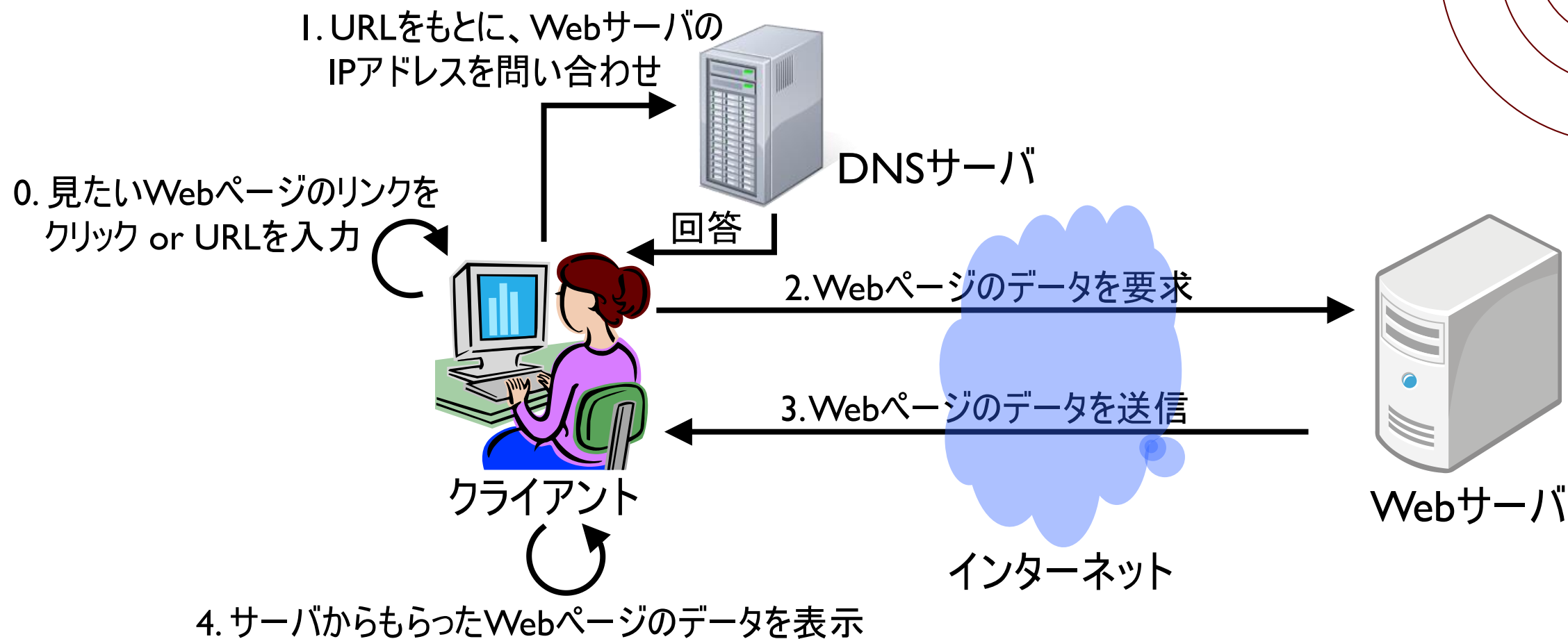
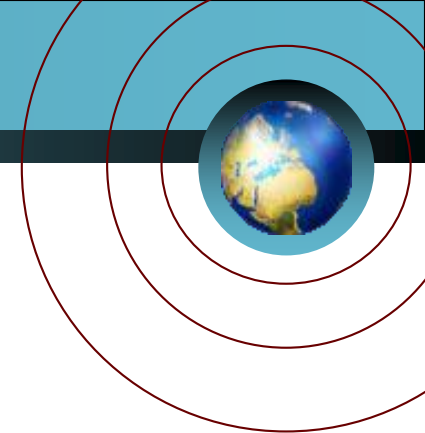


WWW上での情報のやりとり[1](p. 87)



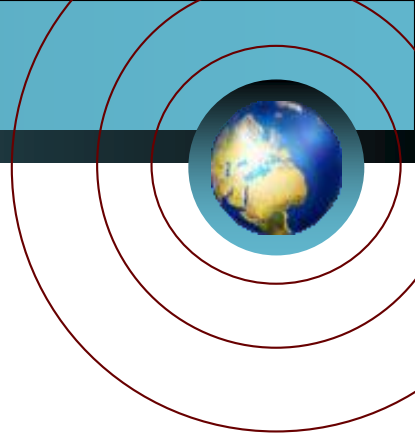
1. URLからWebサーバの住所(IPアドレス)が特定される
2. ブラウザが、そのWebサーバに必要なWebページを要求する
3. Webサーバは、要求されたWebページのデータをブラウザに送る
4. ブラウザは、Webサーバから送られてきたデータを画面に表示する

WWW上での情報のやりとり[I](p. 87)

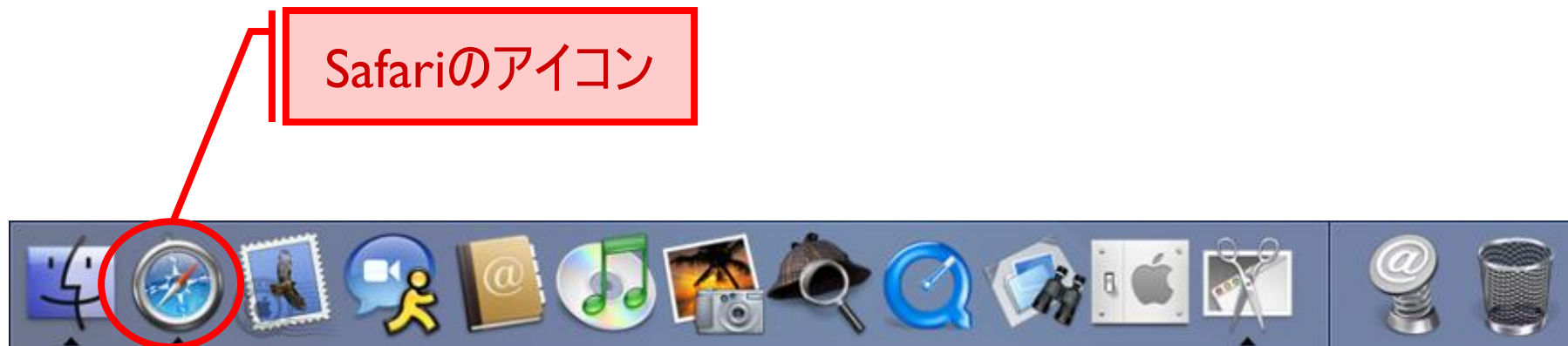


※DNSサーバ: IPアドレスと、コンピュータ名・ドメイン名の対応関係を管理するサーバ

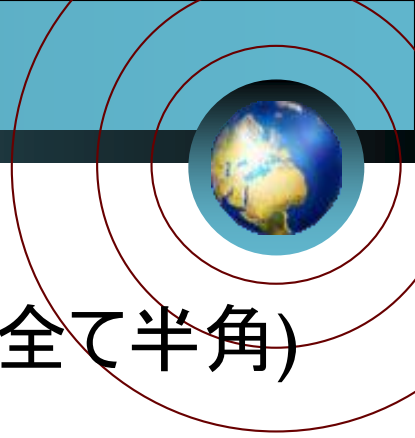
Webブラウザを利用するには?(p. 87)



- 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)

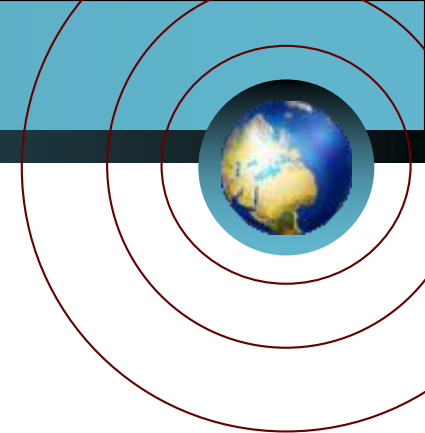


- **アドレスバー**: URLを入力する場所
 - URLを入力して「Enter」を押すと、そのページが表示(ただし、文字は全て半角)



※大文字小文字は区別される

Webページの指定方法(p. 88)



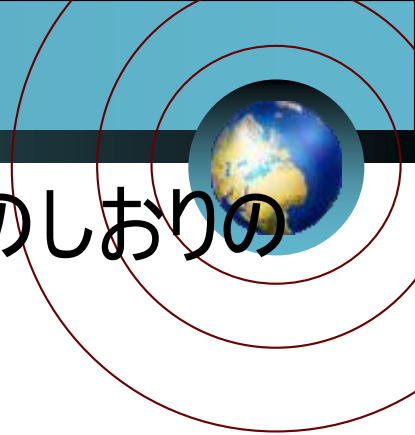
■ 新規表示の場合

- 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

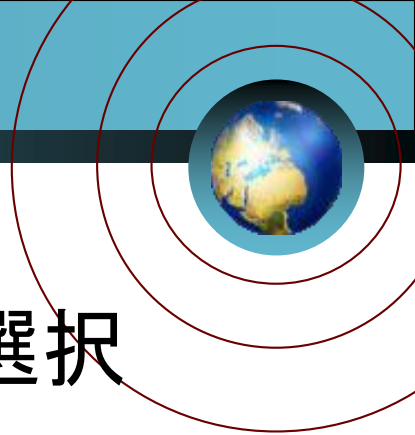
- ブックマークバー(アドレスバーの下)に登録してある場合: 登録してあるページの名前をクリックする
- ブックマークメニューに登録してある場合: メニューバーから「**ブックマーク**」→「**すべてのブックマークを表示**」と選択し、目的のブックマークをダブルクリックする

ブックマーク(p. 88)

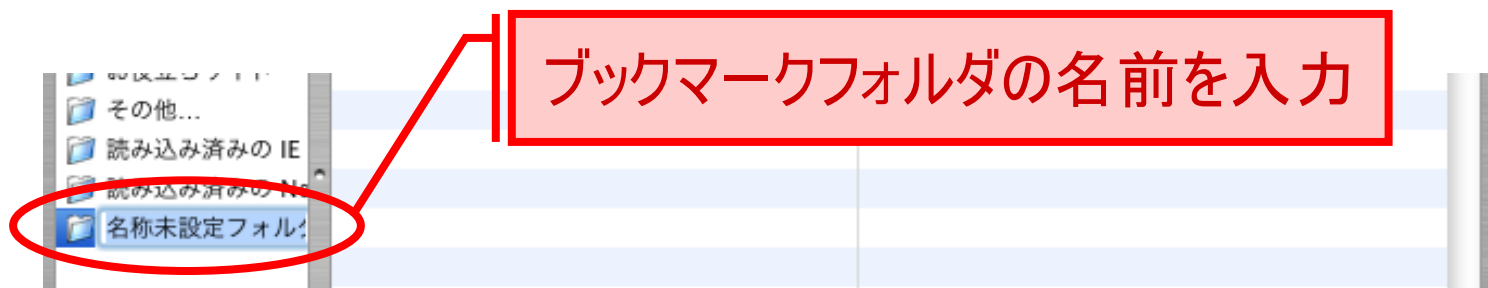


- よく利用するWebページを、簡単に表示させるための機能(本のしおりのようなもの)
- ブックマークをWebページの内容ごとに分類することも可能
 - 内容ごとに異なるフォルダを作成して分類

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
- 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

ブックマークの名前を入力後、
保存場所を指定してください。

東京女子大学-トップページ

ブックマークバー

キャンセル 追加

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

ブックマークを分類するフォルダを選択
(「ブックマークバー」を選択すると、
アドレスバーの下に追加される)

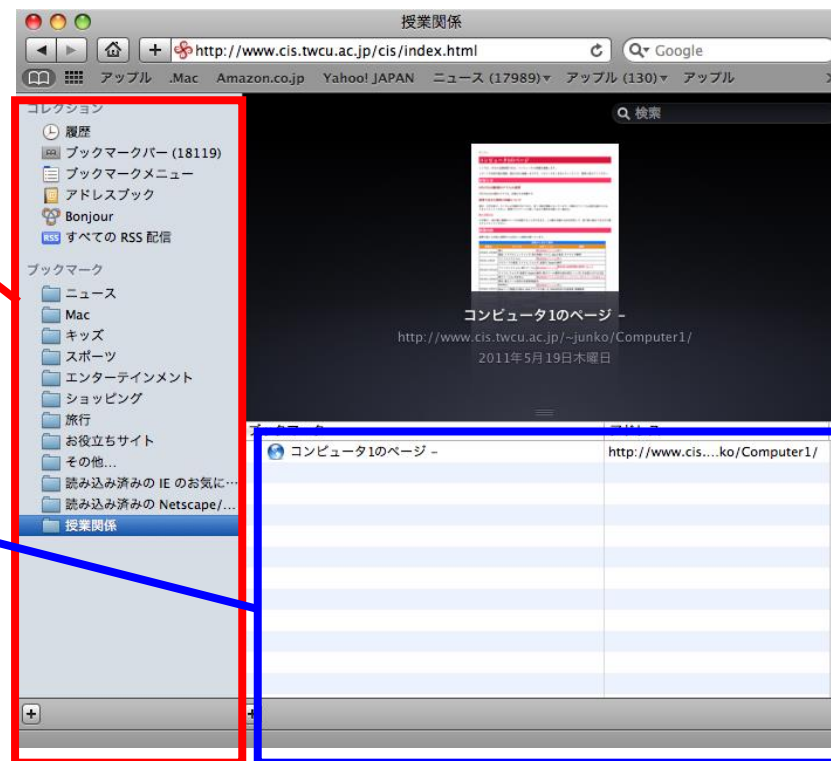
ブックマークから表示(p. 88)



- メニューバーの「ブックマーク」→「すべての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

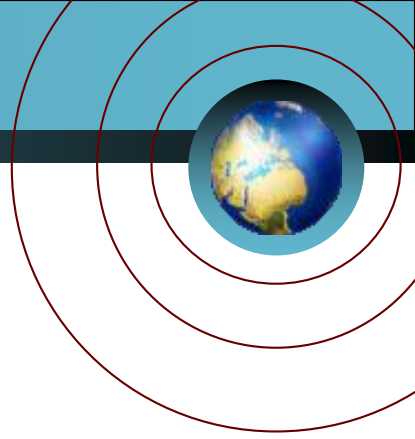
Webページが入っている
フォルダを選択

表示したいWebページの
名前をダブルクリック

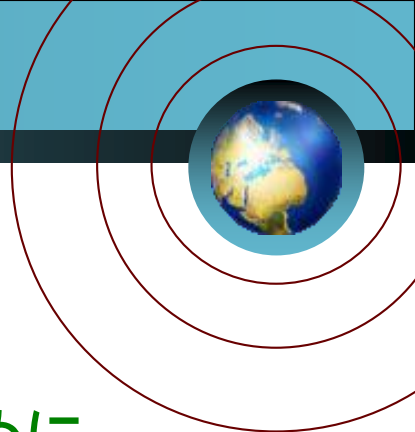


やってみよう!

- 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

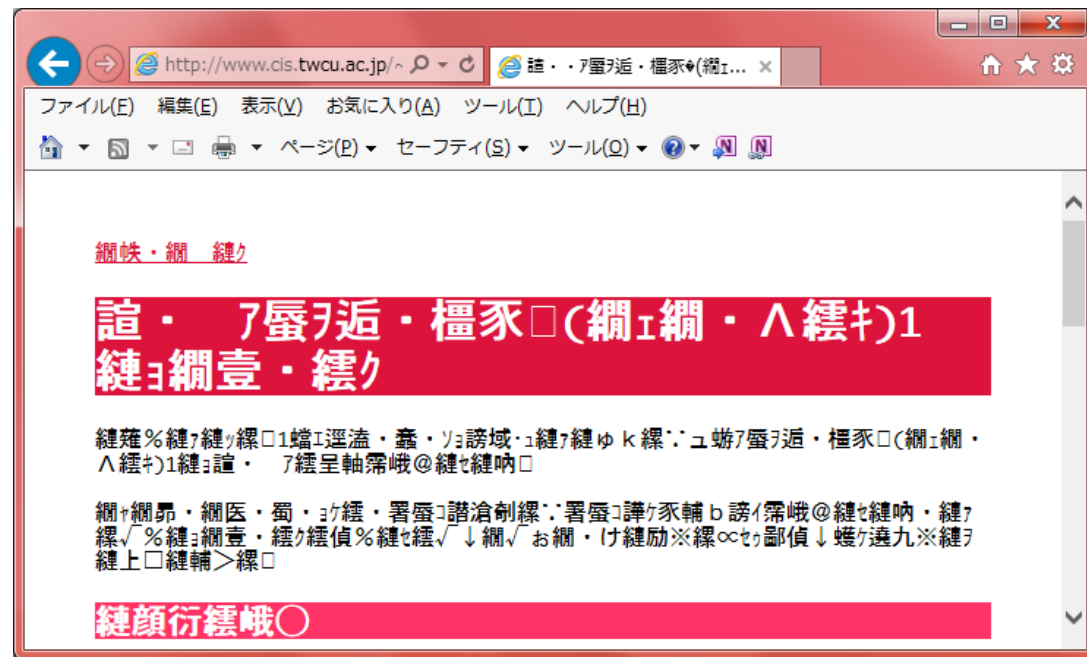


文字化け(p. 89)

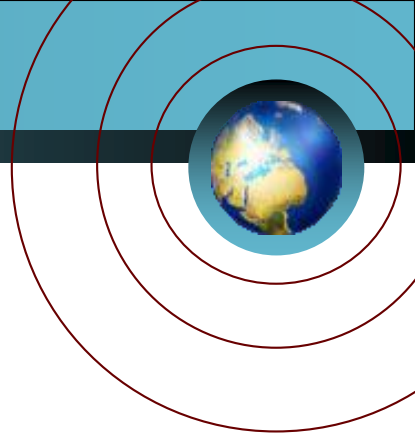


- **文字化け**: 日本語で表示されるはずのページが
意味不明の文字で表示される現象

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[I](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

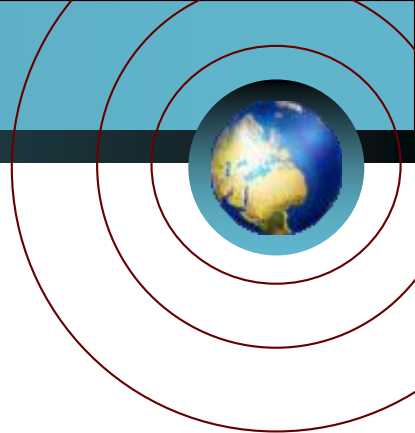
➡ 文字コード: 文字を表す0と1の組み合わせの規格

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文字組み合わせせて表現

➡ 最大65536文字の表現が可能

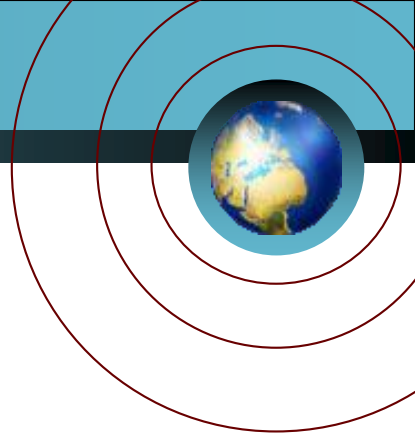
どの半角文字を組み合わせせて全角文字を表現するかで
いくつかの組合せ方(文字コード)あり

現在よく使われている文字コード

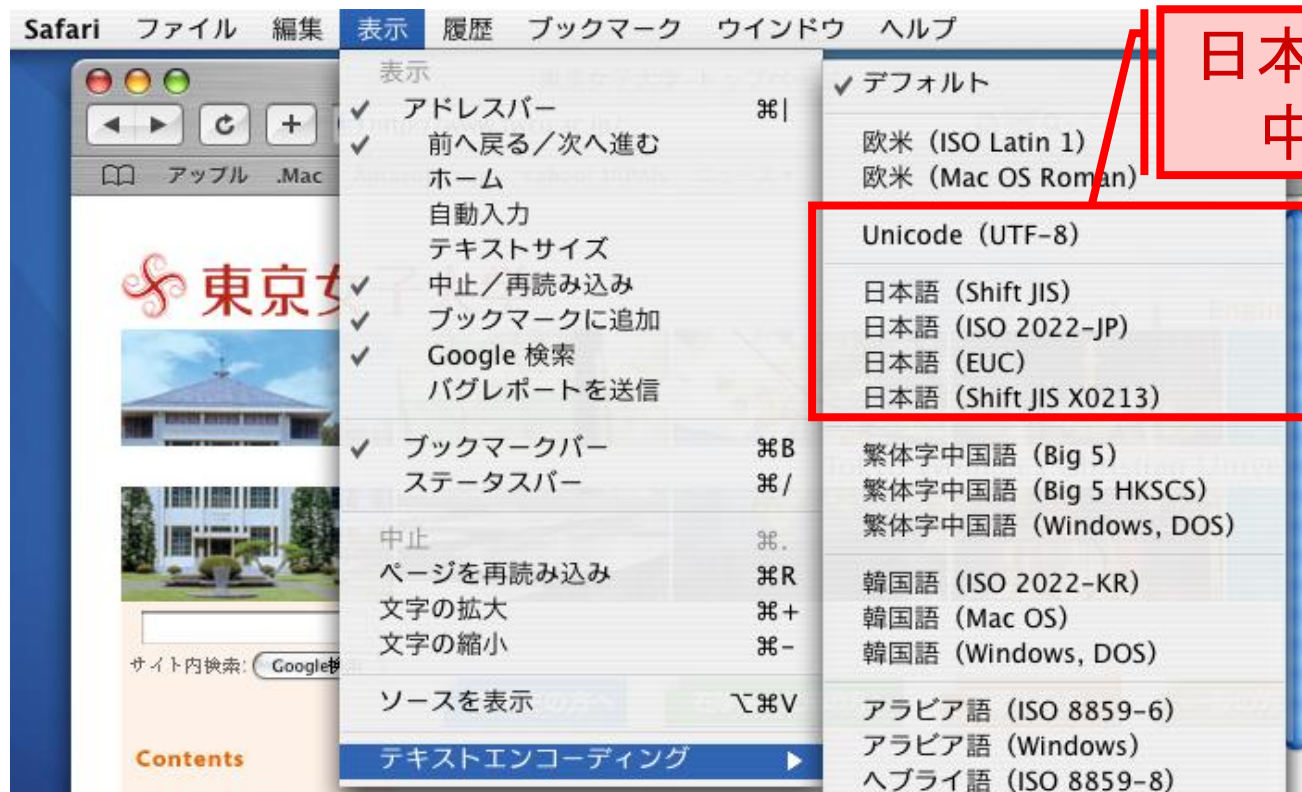
- JIS(電子メールで使われる文字コード)
- UTF-8(MacOSで使われる文字コード)
- Shift JIS(Windowsで使われる文字コード)

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

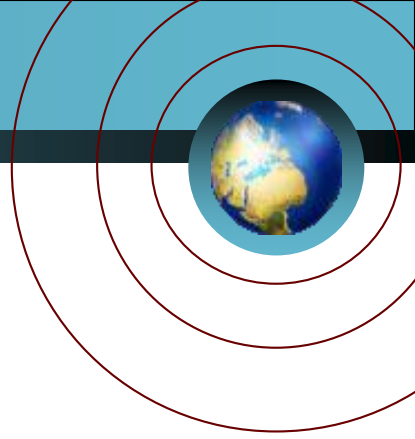
文字化けの直し方(p. 89)



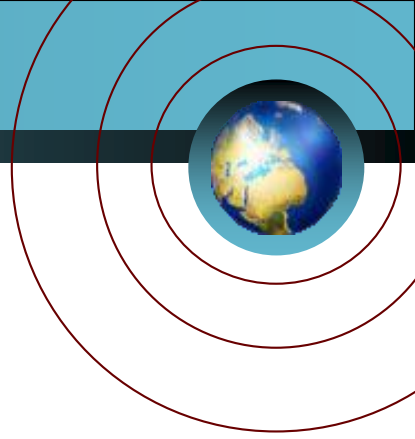
- メニューバーの「表示」→「テキストエンコーディング」→「文字コードの名前」をクリックする



Webページ利用の注意事項



全般的な注意事項(p. 90)



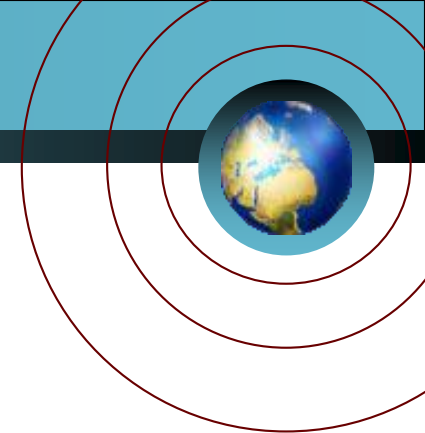
- 怪しいページを見ない
- 怪しいリンクをクリックしない
- 個人情報をもやみに入力しない

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～[I](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...?



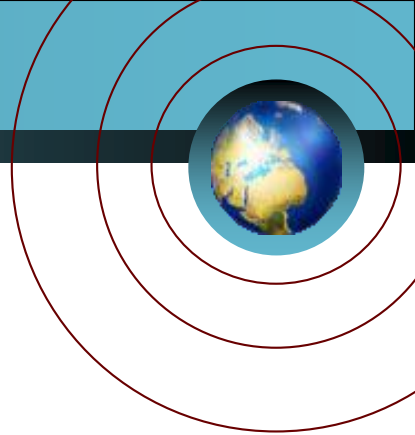
裁判に敗訴する



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)



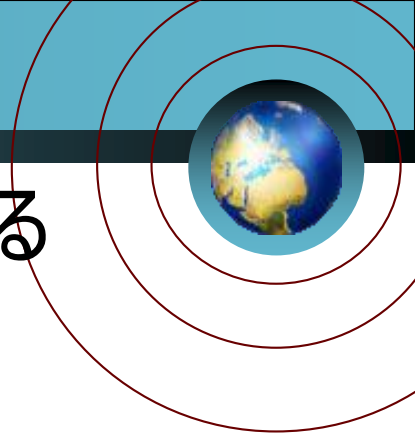
- 最近、裁判所を名乗った通知がメールで届くことも多い

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)

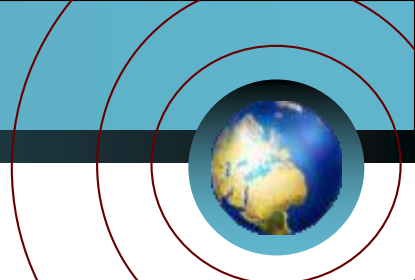


- もっともらしいURLを書いたメールを送信し、URLにアクセスさせる
 - URLは、銀行やクレジットカードの会社などを装っている
- 開いたページで個人情報を入力させる
 - 開いたページは、もっともらしく作ってある
 - ウィルスを使って本物のサイトにアクセスさせないケースもある
- 入力された情報を盗み取る
 - クレジットカードの番号やユーザ名、パスワード, etc.

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

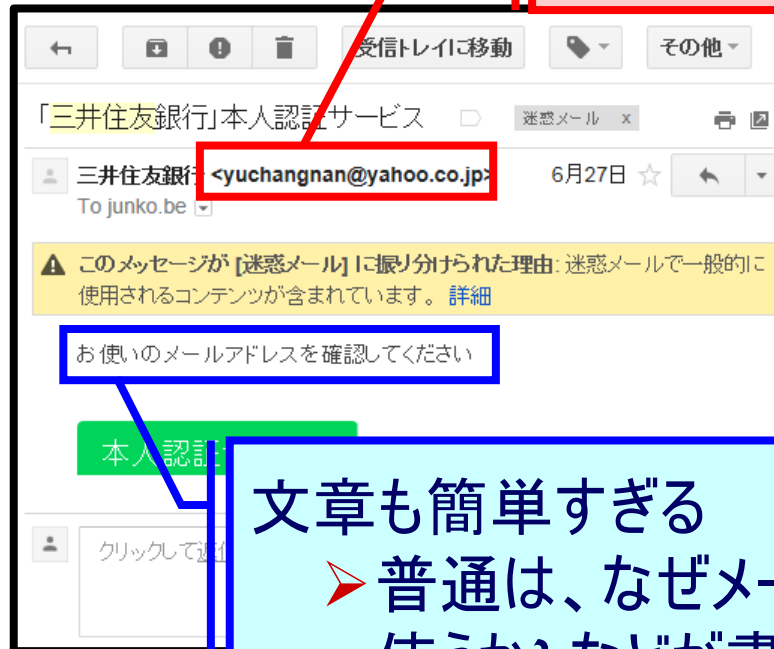
ありがちな被害～偽のサイト～[2](p. 91)



■ 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

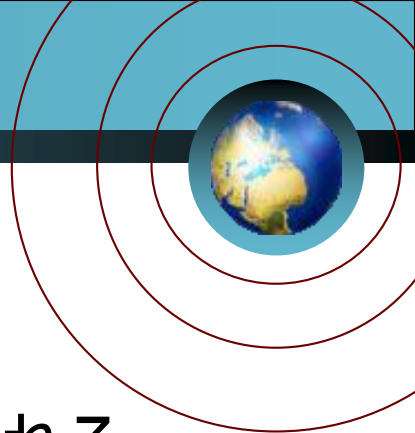
- メールアドレスはYahoo!のフリーメール
- まともな銀行が、フリーメールでメールを送ってくるはずがない



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

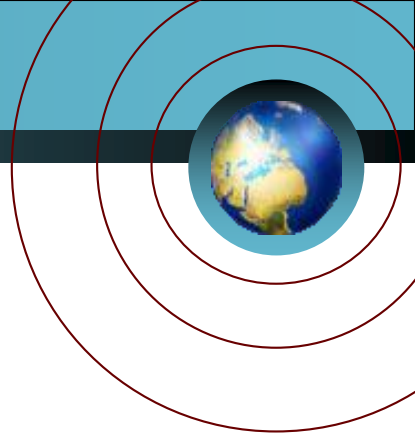
ありがちな被害～入力記録～(p. 91)



- **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

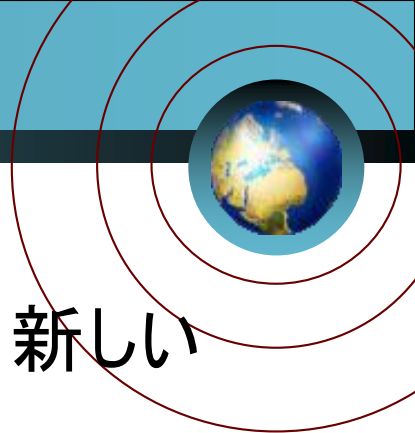
不特定多数の人が使うコンピュータで
個人情報を入力しないこと!

ありがちな被害～ウイルス[1]～(p. 91)



- ウイルスの感染経路
 - 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イルスも存在
 - 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イルスに感染する場合も

ありがちな被害～ウイルス[2]～(p. 91)



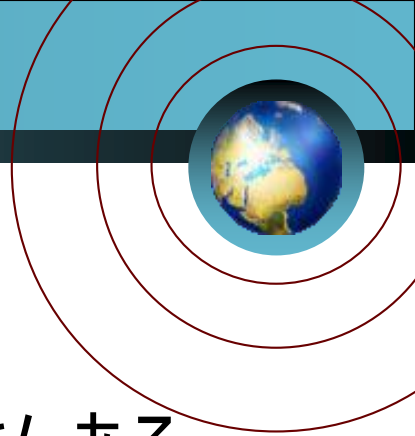
■ ウィルスソフト

- 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)



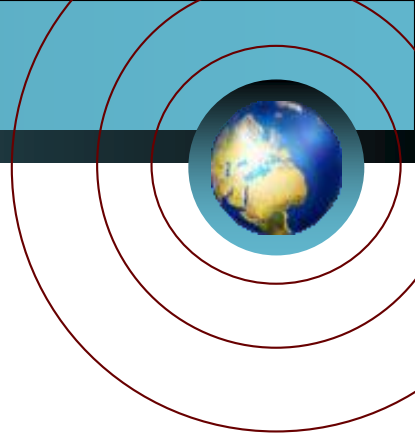
■ アップデート

- 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、見つかる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!

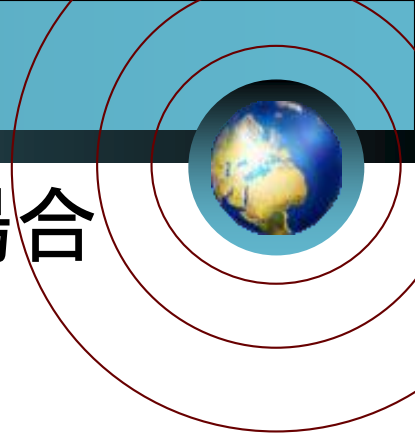
- Windows Update
- Office Update

ありがちな被害～ウィルス[4]～(p. 91)



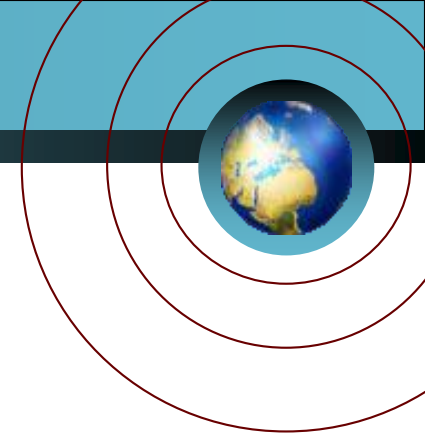
- Windows Update: Microsoft Windowsのための不具合やセキュリティホールを修正するソフトウェア
 - 「スタート」→「すべてのプログラム」→「Windows Update」とたどる
 - Windows UpdateのWebページが表示されるので、そのページの指示通りに操作をしていく
 - 「優先度の高い更新プログラム」の数が「0」になるまで、この作業を繰り返す
 - 1回この作業をしただけでは不十分なこともある

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

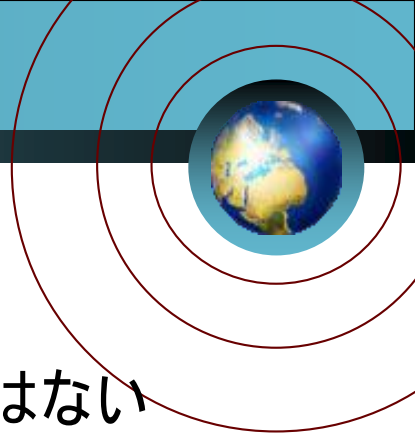
情報源と相談窓口(p. 92)



- 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[I](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?

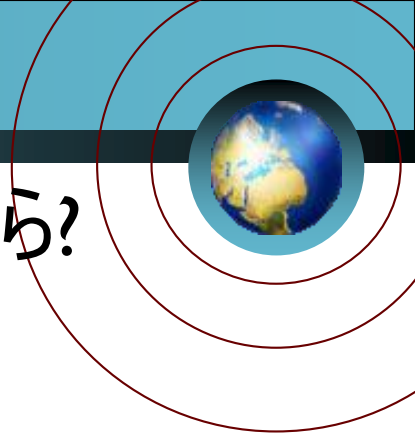
例えば...ショッピングをするページ

品物を売る気はなくて、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)



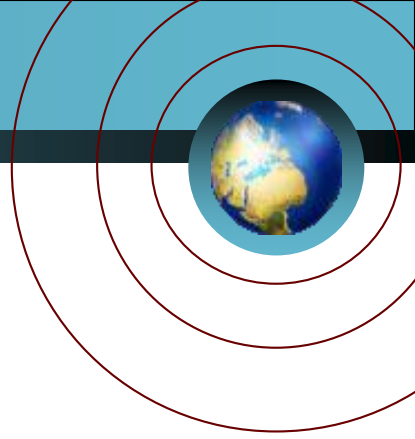
■ 個人情報が、それを集めることを目的とする人に渡ってしまったら?

- 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

個人情報を入力は慎重に!

- 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)

個人情報の入力[3](p. 93)

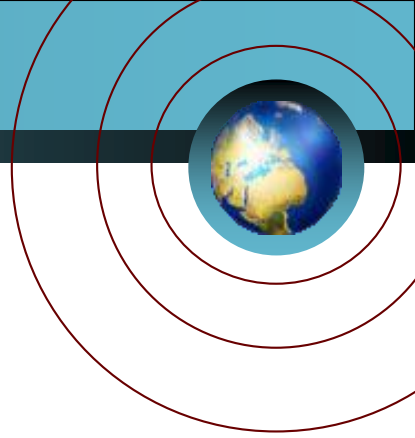


- 自分の個人情報: 入力していいかは自分の判断でOK
- 他人の個人情報: 扱う権利は自分にはない

例えば友達の詳細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)



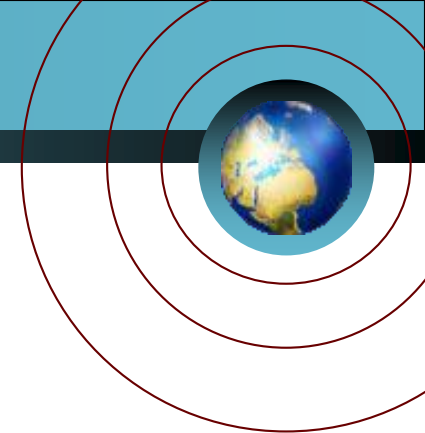
- Webページには様々な情報が掲載
- 様々な人が、様々な目的でWebページを作成
 - 情報の真偽を確認せずに掲載されているもの
 - 悪意を持って間違った情報を掲載しているもの
 - etc.

※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[I](p. 94)



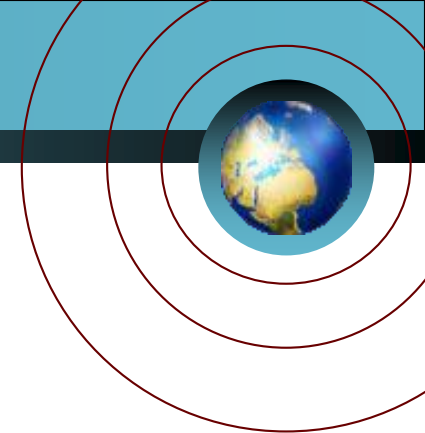
- コンピュータでは、様々な行為の履歴を記録
- 例えば...掲示板
 - 様々な話題について、Web上で自由に意見を交換する場

発言者:A 2015/05/1 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 2015/05/1 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 2015/05/1 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

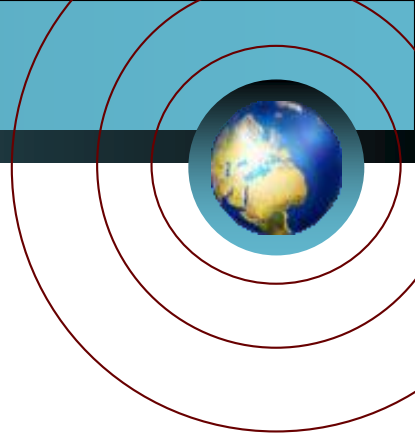
掲示板

- 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

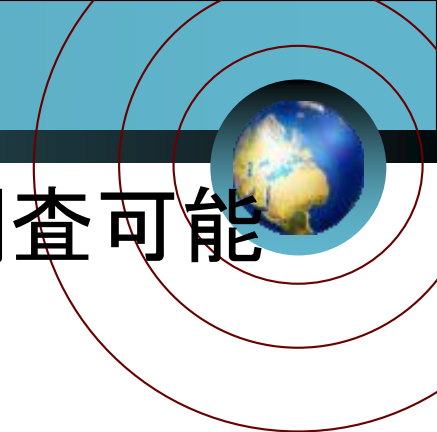
2016年5月1日 13:30:30
from 東京女子大学XX番のコンピュータ
発言内容

2016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

2016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

2016年5月1日 13:00:05～14:20:50

利用者:A(ログイン名)

2016年5月1日 15:05:15～15:40:20

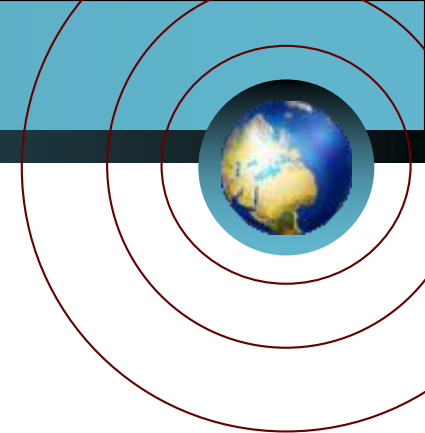
利用者:B(ログイン名)

2016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!



■ 最近、トラブルが急増

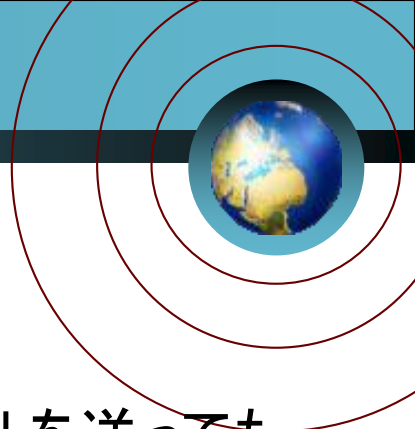
- 仲間内での雑談のつもりで書き込んだ発言
- 軽い気持ちで規則違反やありもしないことを発言
- etc.

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!

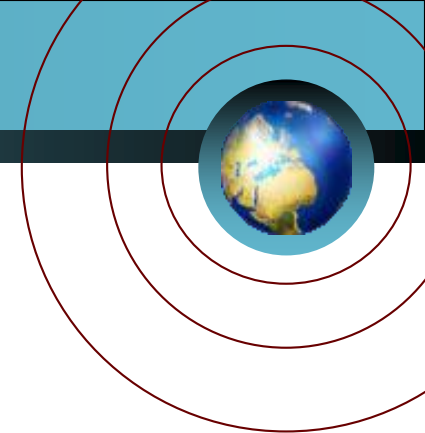
- 問題発言を探して発言者を特定し、公表するような人も...



■ 情報の信頼性の面も問題

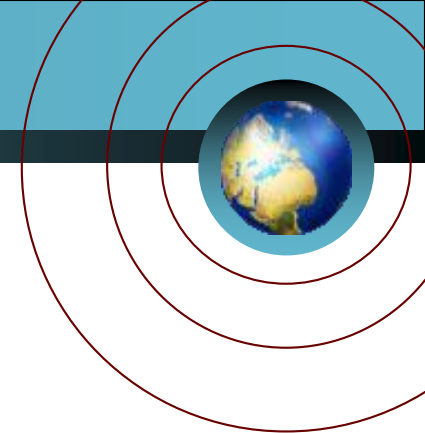
- 発言当時は正しくても、少し時間がたつと古くなることも
 - Ex. 東日本大震災で、救助を求めるTwitterのつぶやきがあり、その人にメールを送っても返事が来ない(すでに救助済みだった)
→ 救助を求める他の発言も、疑われる事態に
- 「拡散希望」という発言も、真実である保証はなし
- 悪質なWebサイトに誘導される場合も
 - ウィルスを仕掛けたサイトに誘導するなど

知らない人が書いているURLをむやみにクリックしない!



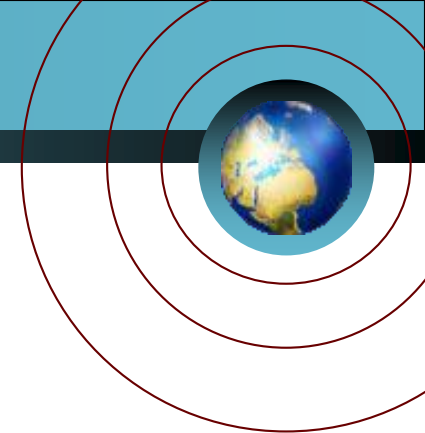
- Facebookは実名登録が原則で、個人情報公開
 - 反社会的なグループに登録される
 - スпамを送りつけられる
 - 「友達を探す」ことで、自分のアドレス帳を全世界に公開することになる
 - etc.

- 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!



- 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!



■ 個人情報情報の漏えいの危険

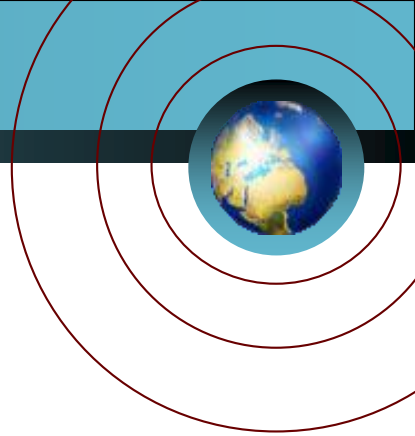
■ GPS付きのカメラで撮った写真やスマートフォンからの発言

- 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!

次週

- 5月19日(木) 1限は出張のため休講

