情報処理技法(リテラシ)1

第4回
メールの読み書き(2), インターネット

人間科学科コミュニケーション専攻
白銀 純子

第4回の内容

- メールの読み書き(続き)
- インターネット

前回の復習問題の解答

- 拡張子とは何か、次のキーワードを使って答えなさい。
  - キーワード: ファイル名, 種類

解答例:
拡張子とは、ファイル名の一部である。ファイル名の「.」以降の部分の文字で、
拡張子がどのようなものであるかによって、ファイルの種類を表す。

電子メール～一般的注意～

メールアドレスは正確に(p. 75)

- 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. 76)

- 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

メールの安全性[秘匿性](p. 76)

- 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(他人に読まれない程度)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)

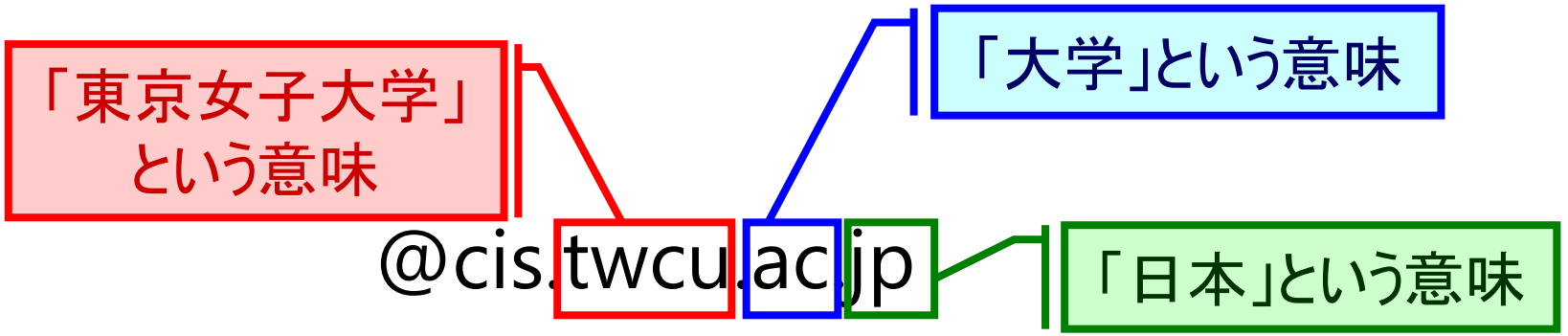
- 大学のメールアドレス: 自分が東京女子大学の学生であることを証明できるもの
  - プロバイダや携帯電話、フリーメールのアドレスは、東京女子大学の学生でなくても持つことができる
  - 特に携帯電話やフリーメールのアドレスは…
    - 簡単に変えることができる →
      メールを送っても届かないかも、と思われることがある
    - 携帯メールでは、文字制限があることもある →
      メールを送るときに、文字数を気にする必要がある

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. 77)

- ねずみ講:「楽して儲ける」という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. 77)

- 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. 77)

- 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こと
- 自宅のコンピュータはウィルス対策をしっかりとする!

スパムメール[1](p. 78)

- 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. 78)

- 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
      →メールの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
   - メールの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、と思われてしまうので、きちんと身につけよう

添付ファイルの名前(p. 80)

- コンピュータ上での日本語の扱い方は様々な種類あり
  - 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. 80)

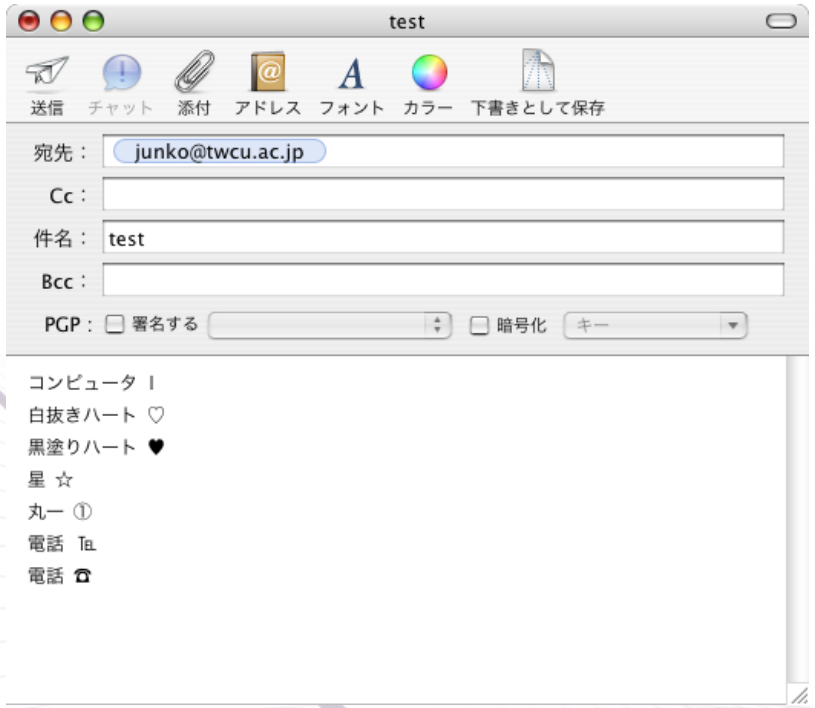
- いくつかの文字は、メールを書いたコンピュータでは正しく表示されても、メールを受け取ったコンピュータでは正しく表示されない
  - ○つき数字
  - ローマ数字(アルファベットのIやV, Xのような数字)
  - ハートマーク
  - 電話マーク
  - 株式会社マーク
  - 音符マーク(「♫」や「♬」), etc.

「機種依存文字」と呼ぶ

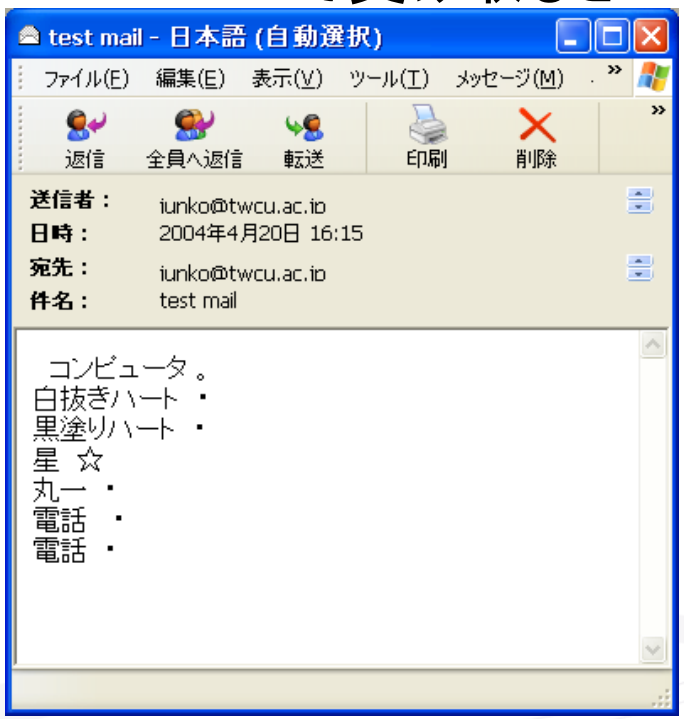
- 絵文字は、携帯電話の機種やキャリアが違うと、違う絵文字になる

機種依存文字や絵文字[2](p. 80)

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. 80)

- 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. 81)

- メールアドレスも個人情報の1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. 81)

- 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. 81)

- 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!

個人情報の管理(p. 82)

- 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. 82)

- 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すると、刑法の「名誉毀損罪」にあたることも

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

インターネットって?[3](p. 48)

- 現実世界の道路
  - 通るもの: 人, 自転車, バイク, 車
    →共通のルールとそれぞれに特有のルールあり
    - 共通のルール: 赤信号で止まる, etc.
    - 人のルール: 歩道を通る, etc.
    - 自転車のルール: 二人乗りをしない, etc.
    - バイクのルール: ヘルメットをかぶる, etc.
    - 車のルール: 車道を通る, etc.

インターネットって?[4](p. 48)

- インターネット
  - 通るもの: データ(Webページのデータ, メールのデータ)
    →共通のルールとそれぞれに特有のルールあり
    - 共通のルール: データがインターネットを通るためのルール, etc
    - 特有のルール: データを送るときの手順のルール, etc.

プロトコル通信規約)

特有のルールは、それぞれのサービスごと(Webページのためのプロトコル, 電子メールのためのプロトコル, etc.)

利用できるサービス[1](p. 48)

- インターネットで利用できるサービス
  - 電子メール
    - コンピュータネットワーク上でメッセージのやり取りのための仕組み
  - WWW
    - Webページという形で情報を公開したり情報を閲覧するための仕組み
    - 「インターネット = WWW」や「インターネット = Webページを見るためのもの」という認識は間違い

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IIJ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

セキュリティ上の脅威(p. 49)

- コンピュータの利用に当たっては様々な脅威が存在
  - コンピュータウィルス
  - 不正アクセス
  - etc.

コンピュータウィルス(p. 49)

- コンピュータにも、人間の病気のような状態になることも

  コンピュータウィルス

- 自分のコンピュータがウィルスに感染すると…
  - コンピュータ内のデータの削除や感染
  - 官公庁や企業のコンピュータへの一斉攻撃に使われる
    - ウィルスに感染した他のコンピュータと一緒になって一斉攻撃
  - 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させる

      知らない間に自分が加害者になってしまう!

ウィルスの感染経路(1)(p. 49)

- Webページへのアクセス
  - アクセス先のWebページがウィルスに感染していると、アクセスしたコンピュータも感染
- メールの添付ファイルやリッチテキスト形式のメール
  - リッチテキスト形式: 本文の文字に色をつけたりフォントを設定したりして飾り付けをしたメール
  - 添付ファイルや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と、開くだけで感染
- USBメモリなどの記憶媒体
  - ウィルスに感染した記憶媒体をコンピュータに取り付けると、コンピュータも感染

ウィルスの感染経路(2)(p. 50)

- ネットワークの利用
  - 家庭内・企業内の内部ネットワークのコンピュータがウィルスに感染していると、ネットワークに接続しただけで感染
- オフィスソフトのマクロ
  - マクロ: オフィスソフトでの一連の手順をまとめて簡略化するための機能
  - ウィルスが仕込まれたマクロがついているオフィスファイルを開くと感染
- アプリケーションのインストール
  - ダウンロードしてきたアプリケーション(スマートフォンやタブレットPCのアプリを含む)にウィルスが仕込まれていると、インストールで感染

不正アクセス(p. 51)

- 不正アクセス: 権限を持たない人が不正にコンピュータを利用すること
  - ネットワークを通じてコンピュータに侵入し、悪さ

- 侵入方法
  - 何らかの手段で入手した利用者のIDとパスワードを利用
  - ソフトウェアの不具合を利用

不正アクセスによってなされる悪事(p. 51)

- データの閲覧・改ざん・収集
  - 侵入したコンピュータに保存されているデータの閲覧・改ざん・収集
  - 個人情報の流出のもと
- 他のコンピュータへの攻撃
  - 他のコンピュータと時期をあわせて一斉に官公庁や企業のコンピュータに攻撃
  - 官公庁や企業のコンピュータに不具合を起こさせたり、壊すことが目的
- ウィルス感染
  - 侵入したコンピュータにウィルスを置いていき、感染
  - 他のコンピュータへの一斉攻撃の足がかり

セキュリティ対策をしなくてすむ場合は?(p. 51)

- ネットワークに一切接続しない(家庭・企業の内部ネットワークを含む)
  - Webページの閲覧をしない
  - 電子メールの読み書きをしない
  - 他のコンピュータと一切通信をしない
- USBメモリ等の外部記憶媒体を利用しない
- Officeソフトのマクロを利用しない
- アプリケーションをインストールしない

現在のコンピュータの状況では不可能!

現実的な解決方法は?-最低限の義務-(1)(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、見つかれば、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!

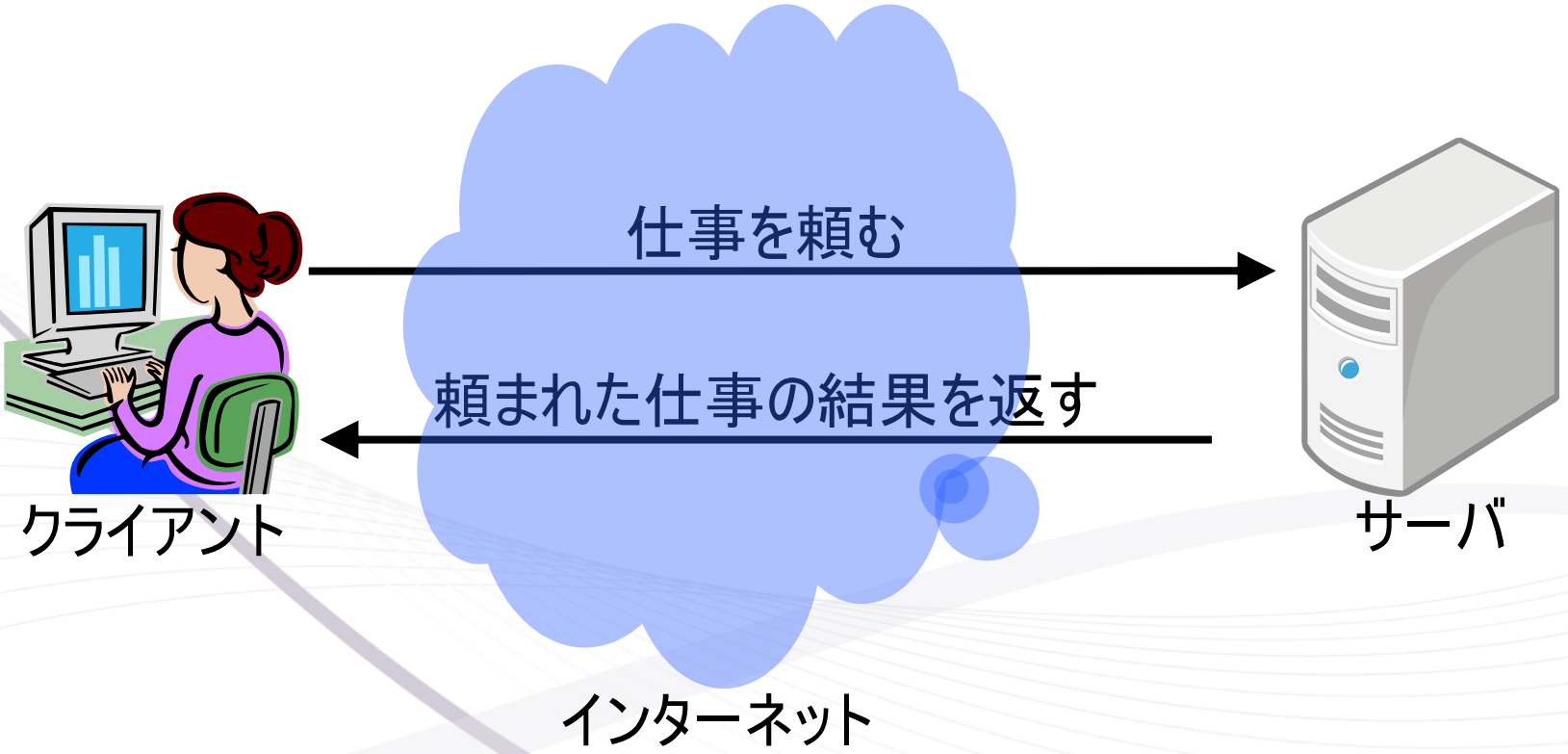
- WindowsやMac OSなどのオペレーティングソフト(基本ソフト)
  - ✓ 自動でアップデートを行うように設定可能
- その他のアプリケーション
  - ✓ アップデートの通知機能がついているものが多いので、通知されたアップデート

インターネット上のサービス

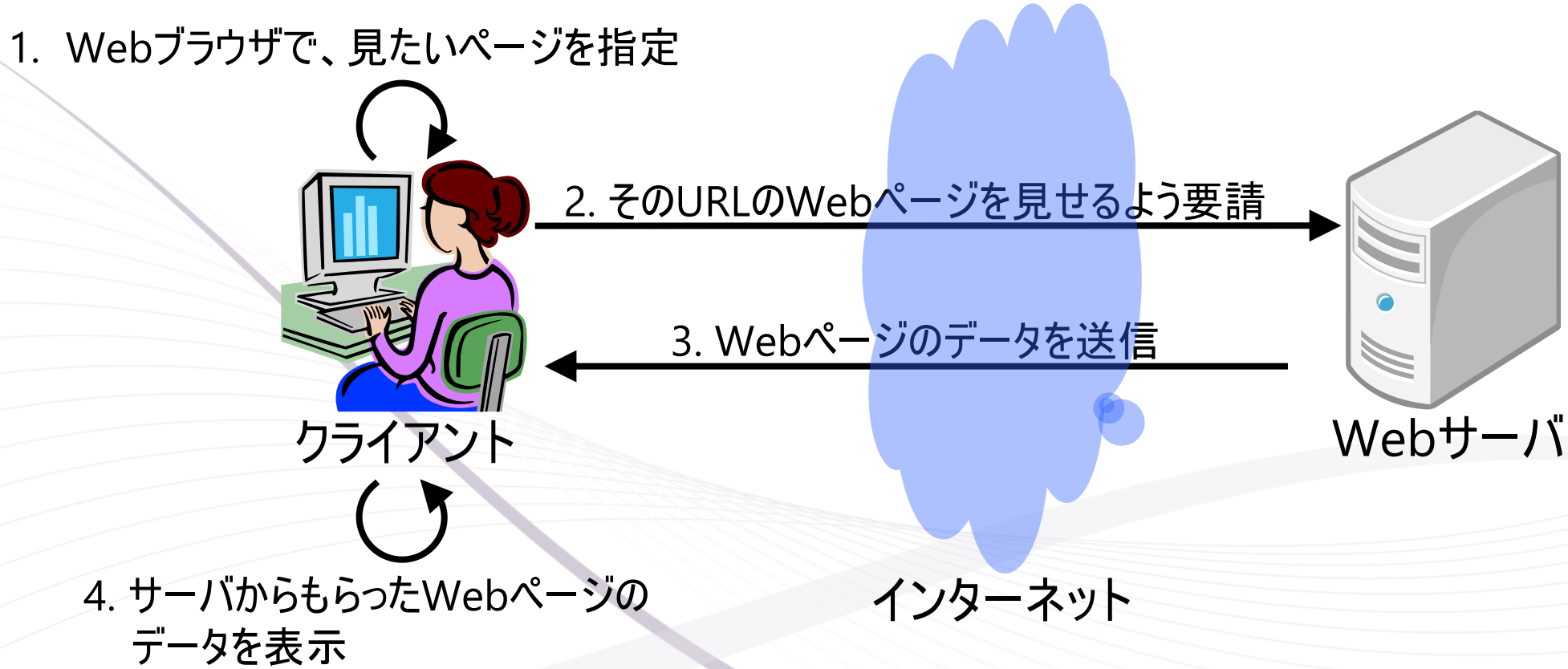
クライアント/サーバ(1)(p. 53)

- 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)



Ex. Webページ閲覧の仕組み(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ソフトが入っていなくても、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も
    - 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
    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