東京大学教養学部前期課程必修科目「情報」試験対策冊子

情報シケプリ

（文系特化版）

ver.1.50

= INDEX =

文系の、文系による、文系のための、情報のシケプリ。

＊ はじめに

※ 一般的なこと

1. 試験について
   - 大問は４問あるが、前半２題は必須問題・後半２題は選択問題でうち一題を解答すればよい。一応、文系向けと理系向けとに区分されている。
   - 前半２題は次頁以降に掲載される「学習項目」の赤字（必修学習項目）から出題され、後半２題は同緑字（A）の問題らしい…。
   - 共通問題のみの場合、試験時間は６０分・結局３題。
   - 個別試験が課される場合、試験時間は 90 分・大問数は３題の共通問題＋個別問題。

2. 参考書／教科書について
   - 「情報」(東京大学出版)
   - 情報処理 Navigator 第３版 ５７０円＋税
   - その他（http://lecture.ecc.u-tokyo.ac.jp/~chiraki/Books.html）

3. 重要リンク集
   - 情報の共通 Web ページ（試験範囲や各教官の Web ページにアクセス可）
     http://www.edu.c.u-tokyo.ac.jp/edu/information.html
   - はいぱーワークブック
     http://hwb.ecc.u-tokyo.ac.jp/current/

※ 諸注意

⑴ 解説は教科書・授業スライド・他年度他クラスシケプリを融合して作成。これだけ読めば、授業内容の把握は可能。
⑵ 原則的には、次に上げる範囲表に従って編集。
⑶ ただし、利用者にいかなる不利益が生じたとしても、編者は一切責任を負いません。
⑷ 理系問題対策としては、2012.s1.28 のシケプリがおすすめ。
⑸ 過去問分析を行い、項目横に**青字の太字**で年度記載しています（2006-2012）。過去問演習の際にご活用ください。ただし、理系分野については対応していません。
⑹ それに伴う注意としては、2006/2007/2010 年にそれぞれ試験範囲の変更が行われています。過去問の年度によっては試験範囲が異なっているので、注意してください。
⑺ 編集・カスタマイズ自由。編集時の諸注意、詳しくは巻末に掲載。

＊ 学習項目

（参照 URL：http://www.edu.c.u-tokyo.ac.jp/edu/requisites2010.htm）

学習項目表のうち、必須項目と要望項目 A のみを掲載。試験（共通問題）では 1,2 は必須項目から、3A は要望項目 A（文系向け）から出題される模様。なお、B（理系向け）は省略。

［ 必須学習項目　赤字と太字で示す / 要望学習項目 A　緑字と下線で示す / 要望学習項目 B　青字と下線で示す（略）］

第 1 章 情報の学び方

1.1 **情報の性質ととらえ方** … 1

1.2 **情報の多面性** … 2

1.3 情報活動の諸要素 … 3

表現と伝達, **モデル化**, **問題解決**

1.4 計算の機構 … 6

コンピュータ, **２進数モデル**

1.5 情報システムと社会 … 7

情報システム, **ユーザインタフェース**, **社会**

第２章 情報の表現 ― 記号・符号化

2.1 情報の表現 … 11

“表現”のさまざまな側面, **情報の表現とモデル**, **情報の表現とは**

2.2 記号と表現 … 16

図記号（ピクトグラム）― 記号と意味, **数の表現 ― 記号と解釈の規則体系**

2.3 アナログとディジタル … 22

アナログ表現とディジタル表現, **量子化**,

2.4 ディジタル符号化 … 27

ディジタル符号化の事例((a)２進符号のみ),

第３章 情報の伝達と通信

3.1 情報の伝達と情報量 … 37

情報の伝達, **情報の大きさ**,

3.2 情報通信 … 46

実際の通信, **プロトコル((b)アプリケーションとプロトコルまで)**

通信の秘密と相手の認証((a)共通/公開鍵暗号のみ)

3.4 インターネット … 55

ネットワークの集合体と通信,

第４章 データの扱い

4.1 データモデル … 71

データとデータモデル

4.3 代表的なデータモデルと演算 … 79

第1章　情報の学び方

▼ INDEX と教科書該当箇所

- 授業で具体的に扱っていない
- 試験でもメインで出題されないらしい
- 他の章と内容重複も多い

以上のことを理由に、省略させて頂きます。適宜、教科書を読んでおくようにしてください。

第2章　情報の表現～記号・符号

▼ INDEX と教科書該当箇所

2.1 情報の表現

- “表現”の様々な側面

＜情報を表現する言語の違い＞

➢ **自然言語**	人間が日常的に使用している言語
➢ **人工言語**	プログラミング言語のように人工的に作られた言語

＜情報の説明の仕方の違い＞

➢ **手続き的表現**	時間をおった手順を説明 （例：道案内で「二つめの信号を右に曲がって三軒目」）
➢ **宣言的表現**	対象間の関係や対象の属性を脱明 （例：道案内で「三越デパートの隣」）

＜情報の表現のされ方の違い＞

➢ **記号表現**	与えられた記号の集合と解釈するための規則体系 （例：数学の記号，数式，方程式，始理式）
➢ **パターン表現**	構成要素間の時空間パターン（例：地図）
➢ ディジタル／アナログによる表現の違い	
➢ 情報量からみる側面	

＜言語の３つの側面＞

➢ **構文論（Syntax）**	表記 if…then…else…fi のような構造
➢ **意味論（semantics）**	書いたものがどのように解釈されるか？ 「a=b」…等しい？代入？
➢ **語用論（pragmatics）**	主体や行動まで考えたもの

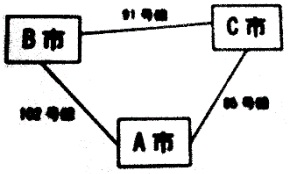
- 情報の表現とモデル

➢ **モデル**	単純化，抽象化された事物，事象，概念 例：（ジェット旅客機設計）実際の旅客機をテストする前に，小型模型（モデル）を用いた風洞実験を行う.
➢ **モデル化**	実際の事物、事象に対応したモデルを構築する過程

＜モデルの表現形式の例＞

① **表（table)**
- こみいった事柄を整理できる
- 歴史年表／貸借対照表／成績表など
- 計算機上の表計算ソフトの利用も一般的

② **図**
- 何らかの目的で描いた 2 次元図形
- 人間の思考・推論を支援／拡張する
- 設計図／地図など
- 広義には絵画／スケッチなども含める



③ **グラフ**
- **ノード（node）とエッジ（edge）**から構成される
- **ラベル付きグラフ（labeled graph）**：ラベル付きのエッジで構成されるグラフ
- **有向エッジ（directed edge）**または**弧（arc）**：方向を持つエッジ
- 道路ネットワーク／組織図／pert 図／意味ネットワークなど様々な領域で幅広く用いられるグラフ表現の例

※ 上図でいうと、市が「ノード」、道が「エッジ」、各道に名前をつけて「ラベル付きグラフ」

- 情報の表現とは － 情報表現で考慮すべきこと
  - ➢ 情報表現の受け手側：情報表現を適切に理解・解釈しなければならない
  - ➢ 情報表現のデザイン側：目的に応じて適切な表現手段を選択しなければならない
  - ➢ 情報は解釈・処理されるものである
    - ✧ 特に人間が扱う情報―解釈
    - ✧ 特に機械が扱う情報―処理

＜解釈・デザインをする際の考慮すべき点＞

✓ **表現の対象**に関して：表現の対象となる事物／事象を明確にする必要がある
※ 表現の対象：物理的実体．抽象的アイディア，思考の方法．思考の結果など

✓ **表現の目的**に関して：表現されている／する目的を理解する
※ 表現の目的：他者への伝達，依頼，自身のアイディアの整理，効率的な問題解決など

✓ **表現の方法**に関して：表現に関わるコストや目的に照らして、よりよい方法を選択する必要がある

2.2 記号と表現

＜記号表現＞

- 記号表現：事物／事象、心的概念を抽象化したもの
- 記号表現の実際の形式：図記号（ピクトグラム）.数の表現など
- 記号が表す２側面
  - i. 意味されるもの（シニフィエ）…（例）サービスエリア
  - ii. 意味するもの（シニフィアン）…（例）図記号

※ 記号論

「あるものが別のあるものを表すという規定に含まれる２つのあるものの間の相互依存関係。この２つの項を『記号表現（シニフィアン)』と『記号内容（シニフィエ)』と呼ぶことにする」（池上嘉彦「記号論への招族」岩波新書 1984）

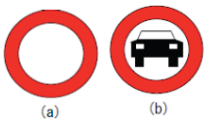
※ 「シニフィエ」「シニフィアン」は、教科書には出てきていない。したがって暗記不要。（ソースは編者の受講していた授業のスライド）

- **図記号（ピクトグラム）- 記号と意味**

＜図記号の修辞法＞

- 提喩に相当する表現方法
  - ある事物を表現するのに、それと意味的包含関係にある事物を代わりに用いる比喩
    Ex.）ナイフ、フォークの図でサービスエリアを表現する
- 隠喩に相当する表現方法
  - GUI（→P.35）におけるゴミ箱アイコンは「ゴミを捨てる」という行為の隠喩

＜交通標識の図表現＞

日本	欧州
	
(a) 車両通行禁止の標識（日本） (b) 禁煙の標識（日本） 禁止や否定を表すために用いられる図記号（日本）	(a) すべての車両通行禁止（欧州） (b) 二輪車以外の車両通行禁止（欧州）

＜サービスエリアの図記号＞

- 抽象化された図形によるデザイン
  → 瞬時に表示内容を認識できる

- 記号表現とパターン表現の混在
  → パターン表現は常に具体的／直接的であればいいわけではない
  （具体的なのが求められるなら、写真載せろって話になる…。）

＜記号の恣意性＞

- 記号表現と命題の対応付けは恣意的
  - ○×による表現が常に肯定、否定（禁止）に対応づけられるわけではない
- 情報表現のデザイナーは受け手側の解釈の枠組みに注意を払う必要がある

＜記号（言語）の恣意性＞

「ある言葉が指すものは、世界にある実物ではない。その言葉が世界から勝手に切り取ったものである（**分節**）。言葉が何を指すかは社会的・文化的に決まっているだけである。自然自身の中にそれを必然とする根拠があるわけではない。こういう特徴をソシュールは**言語の『恣意性』**と呼んだ。」（橋爪大三郎「はじめての構造主義」講談社現代新書、1988）

＜文字の符号化＞（2010.2）

【日本語文字コード】

- ✧ 文字と計算機上の符号（数値）を対応づけるための枠組み
- ✧ 現在、JIS・Shift・JIS・EUC-JP などの異なった日本語文字コードが混在している
- ✧ 解釈の枠組みが異なれば記号の意味が異なってしまう例
  - プログラムが想定するコード体系と異なると，「文字化け」が起こる
- ✧ コード体系の**標準化・統一化**には困難も多い
  - 歴史的経緯、利害関係、処理の都合、拡張性、文字セットの違い

【文字の符号化の問題】

- ✧ 歴史的性質：過去に符号化された文字は読めるべし
- ✧ 転送・記録の効率：短い符号化→速く転送・沢山記録
- ✧ 文字の量：ヨーロッパ語は数十文字・漢字は数千以上
- ✧ 複数の標準：メーカーごと、地域ごとに決定
- ✧ 細かな、しかし文化的には無視できない違い：見た目の類似性、異体字、方言ごとに異なる文字
- ✧ 国際化：狭いコミュニティだけの使用→世界中のコンピュータが通信をする時代、多言語の同時使用

- **数の表現 － 記号と解釈の規則体系**

＜数の表現の歴史＞

- ➢ インドでの発見
  - ✧ 数字のゼロ
  - ✧ 位取り表記法による算術演算
- ➢ アラビア数字表記法
  - ✧ 0 から 9 の 10 種類の記号を用いる
  - ✧ 各記号が各桁に対応している
- ➢ ローマ数字表記法
  - ✧ Ⅰ、Ⅱ、Ⅲ、X、C などの記号を用いる

＜位取りに基づいた計算＞

- ➢ アラビア数字での 1963+41 の計算
  - 表記上の各桁を計算していけばよい
- ➢ ローマ数字でのMCMLXIII+XLIの計算
  - 位取りに基づいた計算をすることが出来ない

```
  1963
+   41
------
  2004
```

```
  MCMLXIII
+     XLI
----------
```

＜情報表現間のトレードオフ＞

- アラビア数字表記
  - 筆算や位取りの観点からは優れている
- ローマ数字表記，漢数字表記
  - 表記された数字改ざん防止に優れている
    - アラビア数字表記「2030」は「1203000」のように改ざんされやすい
    - 漢数字表記「弐千参拾」は改ざんされにくい
- 情報表現のデザイナーは情報表現間のトレードオフを考慮する必要がある

＜コンピュータでの数の表現＞

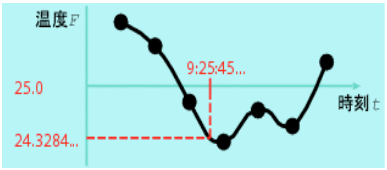
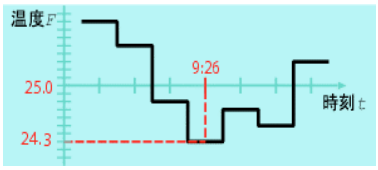
- 「0」と「1」の２種類の記号を用いたビット列で表現される
- 表現できる数値はコンピュータに依る
  - 表現できる正の整数
    - 16 ビットのシステム：0～65535（$=2^{16}-1$）までを表現できる
    - 32 ビットのシステム：0～4294967295（$=2^{32}-1$）を表現できる

＜正整数の表現：２進数＞

- コンピュータで最も良く使われている表現
- 基数を２とする（単純で信頼できる）→各桁は０と１だけになる
- 位取り記法を使う（計算に便利だから）→n 桁目は 2^n 倍された数を表わす

2.3 アナログとディジタル

- アナログとディジタル表現

アナログ表現	ディジタル表現
• ある情報を連続量（アナログ量）として表すこと • 無限の精度を必要とするため，データの複製は元のデータの近似にしかならない	• ある情報を離散的に表すこと（ディジタル量） – ある情報に対して一定の間隔の尺度を導入し、その尺度の値に近似して表現する • 複製時にデータが劣化しにくい • 情報コンテンツの著作権保護への問題をもたらす
• 気温のアナログ表現 	• 気温のディジタル表現 

※ アナログ量をディジタル量に変換する際には、情報を離散化する間隔を選択し，表現する必要がある

- 離散化する２つの軸→量子化，標本化
  - 量子化：測定値をある間隔ごとに表現する。
  - 標本化：一定時間間隔ごとの計測。

- **量子化**
  - 連続量の情報を有限個の段階の**離散量**として表現すること
    - 段階を多くすれば，より詳細な情報となる
  - 情報の用途によって間隔の詳細度を決める
    - コンピュータディスプレイ装霞
      - 赤（R）縁（G）青（B）を混色した RGB 形式を用いている
      - 各々256 種類の具なる色で表現
      - 256x256x256=16,777,216 色を表示できる
    - 音楽 CD
      - 音の振幅を 65536（2の 16 乗）個の段階に分割している
      - 65536 段階は 16 ビットで符号化できる

- **標本化**
  - 情報をある間隔（頻度）ごとに抽出すること

    例：温度を「１時間ごと」に測る

    例：部屋の温度を「10cm ごと」に測る

    例：音圧を「0.0000227 秒ごと」に測る
  - 標本空間
    - 対象の情報が定義される時間や領域
      - ある音楽が鳴っている時間
      - ある絵画全体の領域

- **標本化定理**（学習項目外）（2006･2009）

  （文系履修範囲ではないが、参考までに…。他年度他クラスシケプリほぼ引用。箇条書き化）
  - 周期：振動などのように同じ動作、状況が繰返し起きるとき、その動作一つに掛かる時間

    $$周期 = \frac{1}{1秒辺りの振動数}$$
  - この１秒あたりの振動数のことが「周波数」であり、上の式より

    周期×周波数＝１

    という関係が成立
  - 周期を T、周波数を w とすると

    $w = 1/T$

- 「間隔１／２W で対象となる情報を標本化すれば、元のアナログ関数 F を完全に復元できることが保証される」（教科書）というのは要するに、１周期内で２個点をサンプリングすれば、どうしてそうなるかはわからないけど、サンプリングした点だけを記録しても、もとの波が復元可能であるということ。
- **ナイキスト周波数**：復元できる上限の周波数であり、これはつまり、時間間隔 t で点があったとしたら、波を復元するには１周期内に２個あればいいので、周期は２ t となります。よってw＝１／T より

  ナイキスト周波数 = 1/2t

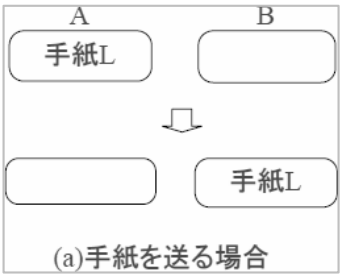
2.4 ディジタル符号化

- ディジタル符号の事例
  - **２進符号**：10 進数を２進数に変換したもの
    - 表記：10 進数なら$(1)_{10}$、２進数なら$(1)_2$など。（基数を下付き添字で表す）
  - **ハミング距離**：２つの符号間で対応する桁の記号が異なる個数
    - （0000）と（0001）では、一箇所異なるのでハミング距離は１
    - （0011）と（0100）では、三箇所異なるのでハミング距離は３
    - ２進符号では数値の差とハミング距離が一致しない

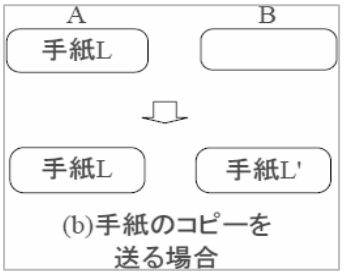
第3章　情報の伝達と通信

▼ INDEX と教科書該当箇所

3.1 情報の伝達と情報量



(a)手紙を送る場合



(b)手紙のコピーを送る場合

- **情報の伝達**：受取側の状態の変化が本質
  - 様々な伝え方で同じ「情報」（メッセージ）が伝わる
  - 「手紙」を送る／「手紙のコピー」を送る、の２つ比べる…。前者も伝達だが後者も然り。つまり受け取り側の状態変化こそ本質的なものだ！手紙の物理的な移動は本質でない
  - 電子メールを送る

- **情報の大きさ：”情報を受け取った効果”を測る**

＜“情報を受け取った効果”の直感的な説明＞

I. 情報を受け取った場合
  - ✧ 自分に影響がある、未知の事実を知った
  - ✧ なんらかの判断の材料にできる事実を知った

II. 情報を受け取ったと言い難い場合
  - ✧ 関心のない手紙を受け取った（迷惑メール etc.）

※ 情報を受け取る効果は、受け取る人の「状態」と関係がある

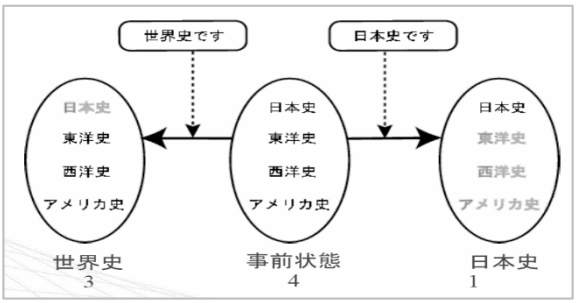
※ メッセージの効果を「**情報量**」として表現したい

＜例：試験に関する情報の価値＞

【前提】：日本史・東洋史・西洋史・アメリカ史のどれか一つが出題
　　事前にはどれが出題されるかわからない

【メッセージ】
　　「今回は日本史から出題する」
　　「今回は世界史から出題する」

どちらも、試験勉強をすべき範囲が狭まるという



意味では同じものであるし、文字数も同じ。だが、「日本史」と限定されたほうが、「世界史」と限定されたよりも勉強すべき範囲が狭められる。つまり、この場合「日本史」と言及したメッセージ方が、「情報量」大。(図も参照)

＜場合の数に着目したとき、情報量をどうやって決めようか…＞

1. 候補

案	定義	問題点
① 差	事前の場合の数ー事後の場合の数	100→97 と 4→1 が同価値？
② 商	事前の場合の数÷事後の場合の数	情報量の加法性(後述)満たさず…
③ 商の対数	log (事前の場合の数/事後の場合の数)	

2. **情報量の加法性**（先程の例を借用する）（2008.2）

i. 情報を一度に受け取った場合（A）
- メッセージＡ：「アメリカ史を出題する」（場合の数：4→1）

ii. 分割して受け取った場合（B+C）
- メッセージＢ：「世界史を出題する」（場合の数：4→3）
- メッセージＣ：「東洋史と西洋史は出題しない」（場合の数：3→1）

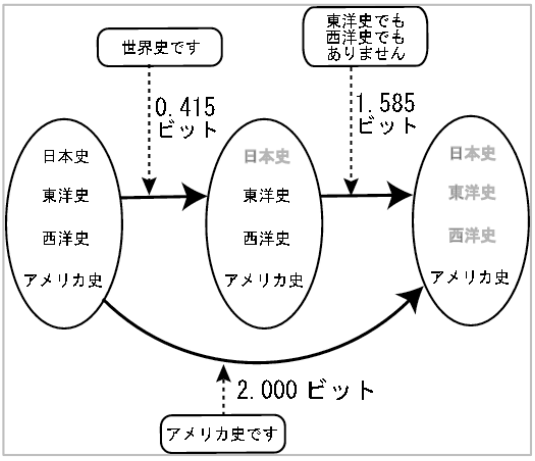
⇒ 情報量（A)＝情報量（B)＋情報量（C）としたい

＜場合の数に基づいた情報量の定義＞

【定義】：$\log_2$（事前の場合の数/事後の場合の数）

【単位】：ビット（bit）

【性質】
- 場合の数が大きく減る程数が大きい
- 底が２なので二者択一（場合の数が２から１になる場合）に 1.0
- 情報量の加法性を満たす



【確認】
- 先程の例で確認すると右図。
- イメージわかない人は適当に数字を当てはめてみて、納得してください。

Ex.) 「100 個の箱があり、当たりは一つ。選べ」のゲームで、さらに「実は、手前のｘ個の箱のどれかが当たりだよ」という情報をくれるおじさんがいたとする。
- x=100 なんのヒントにもなってないし、このおじさん死んでほしい。情報量あるわけない！情報量＝０であるべき！で【定義】に代入すると、$\log_2(100/100)=\log_2 1=0$。よし。
- x=50 半分には絞れている。$\log_2(100/50)=1$。情報量１となる（「情報量」の最大値が絶対的に固定されているわけではない。つまりパーセント表示だと一応100%がマックスってことだけど、「情報量」は事前の場合の数によって変わり

うる）

- x=1 いやマジおじさんサンキュー、ゲームとしては何も楽しめなかったけど…。今までの中で最も情報量が多くなるべし！$\log_2(100/1)=\log_2 100$。まあ6よりはでかいよね。

限定されればそれだけ情報量が増えるという構図になっている！

ちなみに情報量の加法性も、まあ変数使うのはかっこいいけどわかりにくいのでさっきのおっさんゲームでいうと

A) 「手前の 97 個の中に当たりがある」「あああ、しかもこの 97 個中一番奥の３個の中に当たりあるわ」

B) 「あそこにある３つの中に当たりあるよ」

この二つが同じ情報量であるべし。

A) $\log_2(100/97)+\log 2(97/3)=\log_2(100/3)$

B) $\log_2(100/3)$

＜確率に基づいた情報量の定義＞

> 先程の定義を log(確率の逆数) とみなせば式変形をしているだけであることが一目瞭然。というよりも説明過程であの定義を定めたまでのことであって、こちらだけを頭に入れておけばいいのかな…。ともかく、理解さえできればそれでいいのではないでしょうか

【定義】：$-\log_2$（確率）（2008.2）

【単位】：ビット（bit）

【性質】：確率が低いことを伝えるメッセージほど大きい

- 確率 1.0 ー情報量 0
- 確率 0.5 ー情報量 1.0
- 確率 0.25 ー情報量 2.0
- 確率 0→情報量無限大

【場合の数に基づく定義の一般化】：

全てが等確率で起こる時は、場合の数の定義と同じ

「犬が人間を噛んだ」は珍しくないからニュースにならないが、「人間が犬を噛んだ」は珍しいからニュースになる。つまり、珍しい（確率低い）ほど情報量も多くなるということ。その例を教科書では紹介している。

3.2 情報通信

- **プロトコル**：通信の際の決め事（2010.3A・2011.1-2）
  - 通信の意図を理解するための決めごと
    Ex.）電話「もしもし」・トランシーバ「（自分の発言の終わりに）どうぞ」
  - コンピュータ同士の通信：人間より厳密
    - WWW(HTTP) 電子メール（SMTP）
      我々が PC で **WWW**（World Wide Web）閲覧（ネットサーフィン）などするとき、Web ページを見るためのソフトウェ

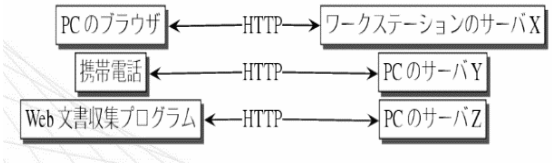
クライアント	情報を要求する側
サーバ	情報を提供する側

ア、それがウェブブラウザ。Web サーバに情報を要求する**クライアント**の一つ。このブラウザが**サーバ**に情報を要求したり、あるいは提供してもらったりするときにも当然規則がある。そういうものを一般に**プロトコル**と呼ぶ。特に WWW（ネット）を見るとき（正確に言えば WWW において Web 情報を要求し提供を受けるとき）、そのプロトコルは **HTTP**(hypertext transfer protocol)と呼ばれる。（ちなみに具体的に Web ページの情報をもらうとき、そのページの規格というのは、通信プロトコルとは別に HTML として標準化されている）。通信の種類ごとにプロトコルも異なる。Email のプロトコル（ブラウザで表示する Gmail とかだとイメージがわきにくいが、PC のメール用ソフト（Outlook, Thunderbird など）を用いてメールの送受信を行う場合を想定してほしい）は **SMTP** と呼ばれる。

	クライアント	**プロトコル**
WWW	ウェブブラウザ etc	**HTTP**
Email	メールソフト etc	**SMTP**

- プロトコルを正しく使えば機器によらず通信可能

  先ほどの話で言えば、HTTP というルールさえ守れば、どんなソフトでも通信できるということ。だれでも知識さえ身につけば、自分に都合の良い WWW 閲覧ソフトやメールソフトだって作れるし、Web 文書収集プログラムによる情報収集も可能である。



- 通信の秘密と相手の認証：**暗号**（2010.2）

平文	元のデータ。第三者に読まれたくないもの。（ex.明日のランチは…）
暗号文	変換後のデータ。盗聴されても平文を容易には取り出せない（ex.繍図激鴛悼挨…）
暗号化	平文から暗号文を作成すること
復号	暗号文から平文を取り出すこと
鍵	暗号化や復号の際に用いられるデータ

（補足）

暗号化は、**計算手順**と**鍵**を用いて行われる。「50 音を 3 つずつ移動させる。（「あ」→「え」、「そ」→「つ」）」という簡易なもので言うのならば、「移動させる」というのは計算手順で「3」というのが鍵ということである。実際には手順を知っていても鍵を知らなければ復号できないような暗号化手順を用いる。

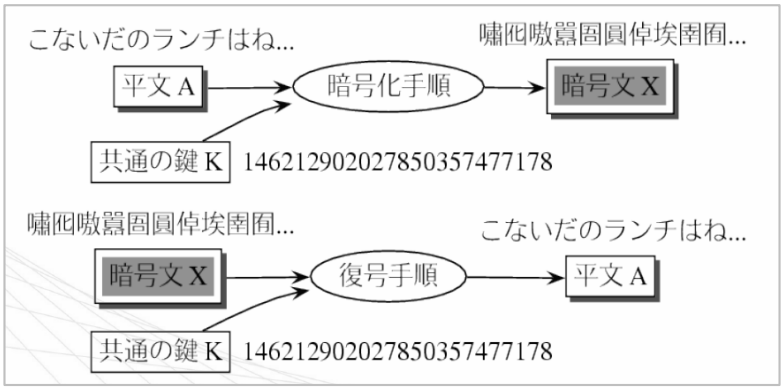
(A) **共通鍵暗号**：一つの鍵で暗号化と復号化が両方できるモデル

※　鍵を秘密に保つ必要性

Ex1）会社の PC と自宅の PC とにそれぞれ鍵があり、会社の PC から送信した暗号化さ

れたデータを自宅の PC で復号して平文として読める、というイメージ

Ex2）図



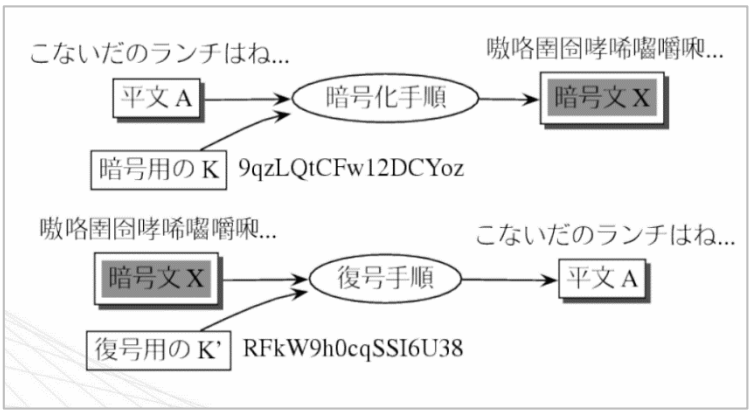
Ex3）DES, AES

(B) 公開鍵暗号（2007・2012.1）

- 暗号文を作るときに用いる鍵と復号するときに用いる鍵が別
  （＝公開鍵で復号は不可）
- 双方の鍵は異なり、片方からもう片方を推測することも難しい
- 自分用の鍵の組みを作り、片方を公開し（**公開鍵**）、もう一方を自分しか知らない状態（**秘密鍵**）にする

Ex1）課長が部下たちに自分の公開鍵（暗号化用）を教えておく。部下たちが文書をそれで暗号化して課長に送信すると、課長は自分だけが知っている秘密鍵（復号用）を用いることで部下の作成した資料を読める、というイメージ。

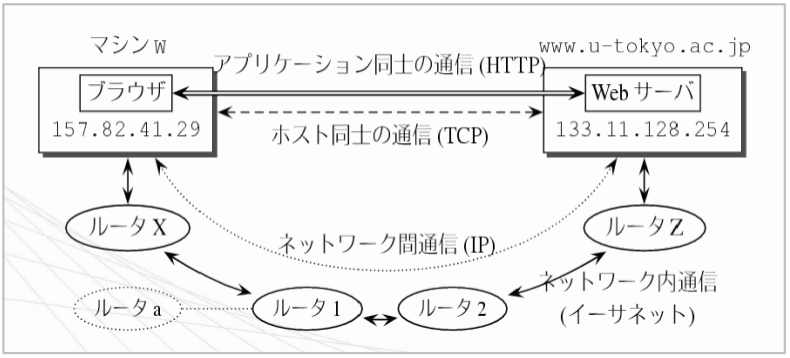
Ex2）右図



3.4 インターネット

- ネットワークの集合体と通信
  - **ネットワークの集合体**：
    インターネットは小規模なネットワークが互いに接続した集合体である。
  - **ルータ**：ネットワーク間の通信を中継
  - 様々なプロトコル：現在インターネットでは TCP/IP と呼ばれるプロトコルが使用されている。これを用いれば OS 問わず接続可。この相互接続性がインターネットの発展に寄与。

【簡単な解説】
ルータを通じて、ブラウザ・Web サーバ間の情報のやり取りが行われている。



【具体的な解説】（教科書に同じ）
1. ブラウザが URL から IP アドレス（133.11.128.254 など）を調べる（**DNS** を用いる）
（IP アドレスについてはこれ以上知る必要なし）
2. ブラウザが、宛先の IP アドレスのウェブサーバに対して、HTTP のメッセージを送る
＜実際の処理＞
⑴ 送信マシン W、メッセージをパケット（細かく知らなくていい）に分割。パケットごとに IP アドレスに送信
⑵ 各パケットは、まず同一ネットワークのルータ X に届けられる。ルータ X は宛先の IP アドレス向けの適切なルータ Y を選び、そこに転送。順に適切なルータに転送され、最終的には宛先マシンまで届けられる。
⑶ 受信したマシンは、パケットをもともとの順番通りに並べ、もとの HTTP メッセージを取りだし、Web サーバに渡す。
3. Web サーバがブラウザにメッセージを返す（同様なので省略）

- TCP … データのパケット分割・合成を担当
- IP … 分割されたパケットを宛先に届ける、また、そのために適切なルートを選ぶ

TCP/IPモデル	主なプロトコル	主な役割
アプリケーション層	**HTTP**,SMTP	アプリケーション間の通信
トランスポート層	**TCP**,UDP	信頼性のある1:1の通信
インターネット層	**IP**	ネットワーク間通信
ネットワークインタフェース層	（イーサネット）	ネットワーク内通信

3.4.7（参考）
- **IP アドレス**は数値でわかりにくい！→「**ホスト名**」使用されること多し。
- IP アドレスとホスト名の関連付けを行うのが **DNS**
- いっぱいあって集中管理は限界→一定範囲ごとに別々に管理する DNS…分散管理
- 反復問い合わせ
  Ex.) www.u-tokyo.ac.jp の場合、
  - ルートサーバに jp を管理するサーバ聞く
  - jp 管理するサーバに ac.jp 管理するサーバ聞く
  - 最後に u-tokyo.ac.jp 聞く
    ※　同じ問い合わせ結果は保存、再利用することも。

第4章　データの扱い

▼ INDEX と教科書該当箇所

4.1 データモデル … 71
　　データとデータモデル
4.3 代表的なデータモデルと演算 … 79
　　ネットワークモデル(「ウェブ」まで)，階層モデル(「住所の階層性」まで)，

- **データのデータモデル**

コンピュータで情報を扱うための表現！

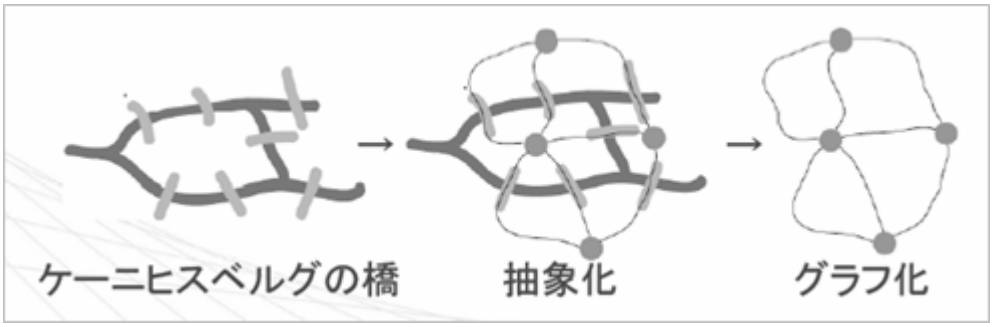
➢ データ	コンピュータの処理対象。符号化された情報
➢ データモデル	データを体系的に扱うためのモデル

- **代表的なデータモデルと演算**
  - ➢ **ネットワークモデル**…「つながり方」を表すモデル（2012）

Ex.）グラフ…〇を線で結んだもの。

→ グラフ使用例：”ケーニヒスベルグの橋”の抽象化

「とりあえず、２度同じ橋を渡りたくない！さてそれは可能か」

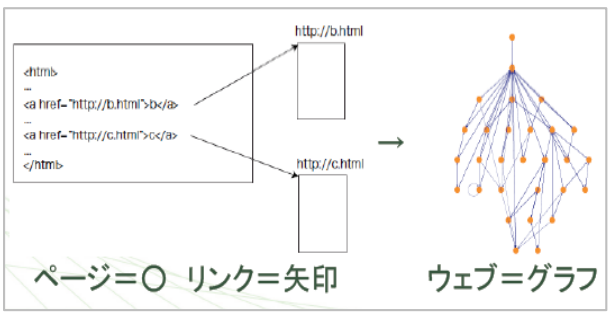


＜用語＞

陸地「ノード」、道「エッジ」、順にたどれるエッジの列「路」、重複なくたどる路「オイラー路」

ウェブ

- ✧ ウェブページそれぞれを〇と考えると、リンクは〇から〇を指す矢印（有向エッジ）と見られる。
- ✧ 〇が矢印で結ばれたものもグラフという
- ✧ 「重要ページからのリンクは重要」という規則の方程式を作って解くことで、ページごとの重要度を決定（Google 等の検索エンジンもこれを



利用）

- **階層モデル（木構造）**（2007.2）

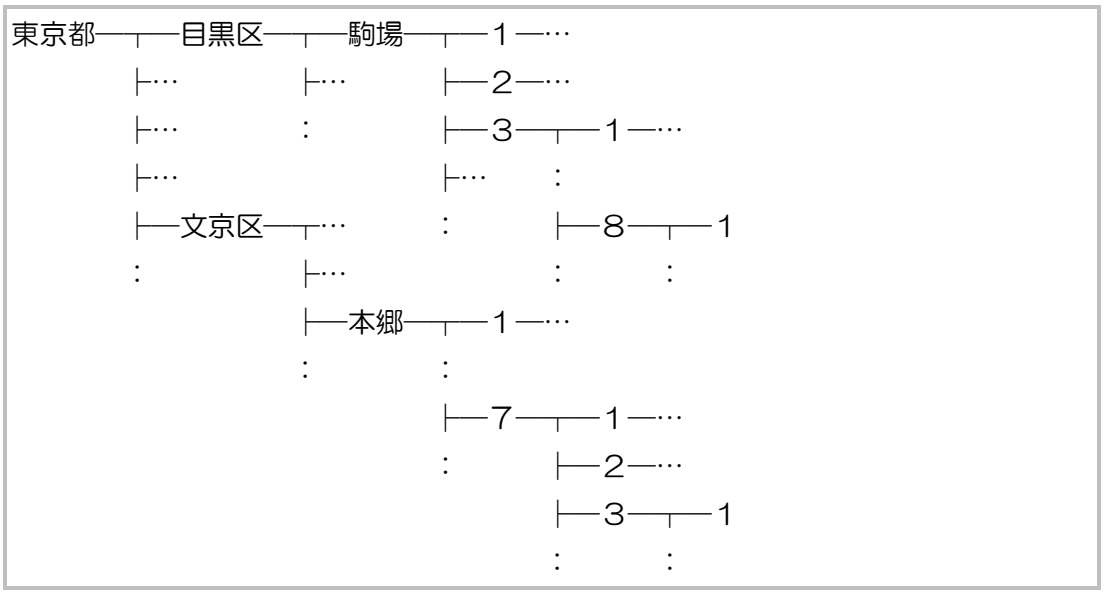
…「ひとつ上位の要素に対して、ひとつ以上の要素が回に存在し、ある要素はより上位の要素を用いて一位に特定できる性質を持つモデル。」（他年度他クラスシケプリより）

→ 枝分かれ構造 / 有向グラフの特殊なものと見ることも可

✧ **コンピュータのファイルシステム**（2007.2）

1. 仕分け可（サブフォルダ利用）
2. 混合防止
3. 重複なき処理可
4. サブフォルダ以下の内容をそのサブフォルダで代表可。
   例）階層構造下、サブフォルダ移動→サブフォルダ以下のものも移動

✧ **住所の階層性（コンピュータのドメイン名でも…）**



※ ドメイン名も階層構造になっている

u-tokyo.ac.jp … jp（日本）→ac（大学等）→u-tokyo（東京大学）→…

第5章　計算の方法

▼ INDEX と教科書該当箇所

5.1 計算とその記述方法 … 97
　　計算の方法，計算の記述，

- **計算とその記述方法**
  - 計算…モデル化されたデータに対する操作
- **計算の方法**

＊ 計算例：計数（counting）

「ある集合 A の要素数を求める」

＊n は答え

(1) **取り出し型**：指折り数える

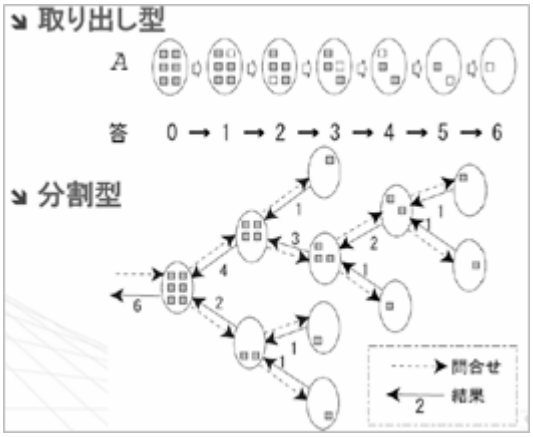
＜用意される処理＞

(a) 空かどうかを判断する

(b) 要素を１つ取り出す（集合要素数は 1 減る）

＜計算＞

- n を 0(ゼロ)にする
- A が空でない間(a)、以下の処理繰り返す
  - 要素を 1 つ取り出す(b)
  - n を１増やす



(2) **分割型**：できない仕事は下請けに任せる

＜用意される処理＞

(a) 「空」or「要素１つだけである」を判定

(b) 空でない２つの集合に分割する

＜計算＞

- A が空なら n=0，要素数が１なら n=1 (a)
- どちらでもないとき以下の処理(b)
  - A を B と C とに分割（B,C も空集合でない）
  - n=B の要素数+C の要素数

- **計算の記述**

[例題]
今年の八十八夜（立春から数えて 88 日目；87 日後）は何月何日か．ただし今年の立春は 2 月 4 日であり、今年は平年である．

［考え方］

- ２月４日の 87 日後は”２月をはみ出す”→ ２月の残り日数（28 － 4=24 日）を引く（87 － 24=63 日）
- ３月 63 日は３月を越す → 31 日を引く（63 － 31=32 日）
- ４月 32 日は４月を越す → 30 日を引く（32-30=3 日）
- ５月２日は５月に収まる → 最終的な答えは５月２日

- **変数（variable）**
  - 値（例：残り日数）を覚えておく”もの”
  - つまり、[考え方]で言うところの　87→63→32→2 の個々の数字。
  - 変数の値は「代入」（assignment）により変化させることができる
  - 代入（assignment）：変数に値を設定する操作
    - 表記方法：「変数名」←「式」

※ 数学の用語とは概念も違うから注意！

	計算記述	数学
英語（変数/代入）	variable/assignment	parameter/substitution
変数の意味	値を覚えておくもの	値と結合するもの
代入の意味	変数に値を設定する操作	置き換え

- **逐次処理**…書かれた順序通り処理することが必要。抜かしたり２つのことを同時にやったりは禁止。
- **条件付き処理**…条件によって実施すべき操作が異なる処理

＜表記方法＞

```
If 条件
 then「条件が成立した場合に行う処理」
 else 「条件が成立しない場合に行う処理」
endif
```

※ Else 以降がない場合は省略可。

［例題の解法手順］

右図参照…。

右に凹ませて書くのは、「まとまり構造」を一見して見られるよう工夫したもの。（これを 字下げ indentation と呼ぶ）

＜問題点・改良点＞

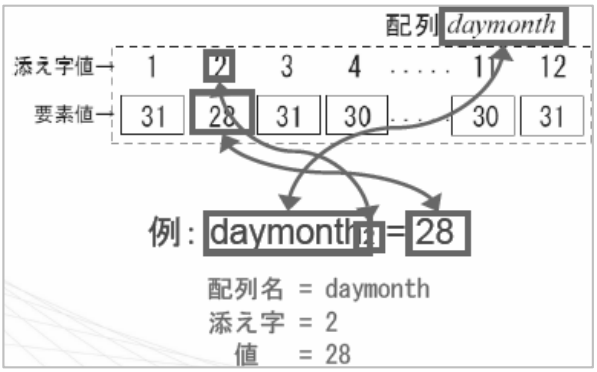
- 「６月以降の処理」…実際６月以降の処理が必要になった時に正しい答え求まる保証なし。
- 簡素化希望
- 「m（n 月の日数)」という表現が何度も出現しているところに着目。
  Ex.) 28（2 月の日数）

- **反復処理**

＜表記方法＞ while 条件 do 「処理」 done
＜現代語訳＞ 条件が成立している限り「処理」を繰り返し実行しろ。

- **配列**
  - 要素の集合から「添え字」を使って値を取り出し、変数として扱うことができる
  - 要素全体をまとめて扱うことができる。

Ex.）[例題の解法手順]で「m（n 月の日数）」という形が頻出。これを $daymonth_m$ と書けるものとする。$daymonth_2$=28 であり、以下 $daymonth_3$～$daymanth_{12}$ も同様に設定してあるものとす。



[例題]の解法手順 － 改良版

＜残り日数＞ ← 4＋87
m ← 2
while 「残り日数」＞ $daymonth_m$ do
　「残り日数」←「残り日数」 － $daymonth_m$
　m ← m＋1
done

『「残り日数」と月の日数の比較を繰り返し行う』手順を**反復処理**と**配列**とを使うことですっきりと記述することができた。

第6章　問題の解き方

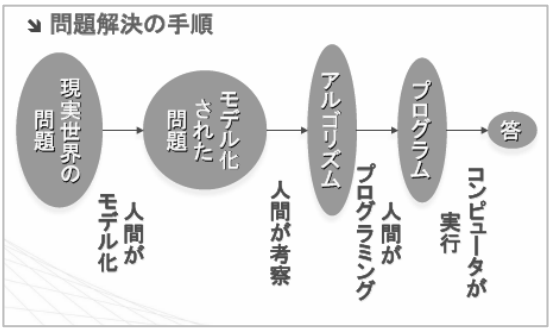
▼ INDEX と教科書該当箇所

6.1 アルゴリズム … 121
　　アルゴリズムの役割，アルゴリズムの実例（2分法まで），
　　計算量

● アルゴリズムの役割

＜問題解決手順＞

(1) 問題モデル化
(2) 問題を解く計算手順を考える
(3) 手順通り計算するプログラム作る
⇒ アルゴリズム…この場合の「計算手順」



＜アルゴリズムの重要性＞

- 性能に大きな違いが出る
  - 同じ問題を解くにも、複数のアルゴリズム存在。
  - アルゴリズムによって計算時間が大きく変わる。影響も大きい。
- 類型化されている
  - 全く違う問題を解くアルゴリズムが同じものになることアリ。
  - 性能に関する考察・プログラミングを共通化可。

＜コンピュータより古いアルゴリズム＞

必ずしもアルゴリズムはコンピュータによって実行されるものとは限らない。
Ex.)ユークリッドの互除法・ドント方式（比例代表選挙）など

● アルゴリズムの実例：平方根の問題

（具体例を知るのみならず、同問題でも複数のアルゴリズムが存在し、計算時間も変わることを知ってほしいらしい）

[注意など]

$\sqrt{x}$ を求める / 小数の計算は有限の精度で行わせる ⇒ 近似値しか求められない

[問題]

- ある正の実数 x が与えられた時に、2 乗すると x に近くなる正の実数 y を精度 δ(ﾃﾞﾙﾀ)で求める
- つまり $|\sqrt{x}-y|<\delta$ となるような y を 1 つ求める。

＜アルゴリズム１＞ 反復法

【アルゴリズム】	【現代語訳】
y ← 0	とりあえず y は 0 に設定しとくぜ。
while $(y+\delta)^2 < x$ **do**	★ $(y+\delta)^2<x$ が成り立つ**限り、以下を行い、これを繰り返せ。**
y ← y + δ	「今回の y に δ を加えたのを次回の y として、もう一度★からやれ。」
done	$(y+\delta)^2<x$ が成り立たなくなったら**終われ。**
return y	終わった時点の y が答えだから、**吐き出せ。**

解説的な例

・ x = 90，δ = 1 （90 の平方根の近似値を整数の範囲で求める）

アルゴリズム「y = 0, 1, 2, 3, …を順に検討してゆき、$(y+\delta)^2$ が 90 より大きくなったらその一つ前が答え」

・ x = 2，δ = 0.0001

回数	0	1	2	···	14140	14141	14142
候補 (y)	0.0000	0.0001	0.0002	···	1.4140	1.4141	1.4142
$(y+\delta)^2$	0.00000	0.00000	0.00000	···	1.99968	1.99996	2.00024

アルゴリズムの速度

- 繰り返しの回数で比べる
  - プログラムの実行時間の、非常に大雑把な近似
  - 実際のコンピュータの性能と無関係に検討可
  - 異なる種類の計算の速度差も無視してしまう
- 反復法の場合
  - 繰り返しの回数は約 $\sqrt{x}/\delta$ 回
  - 精度一桁増やすと回数も 10 倍増える

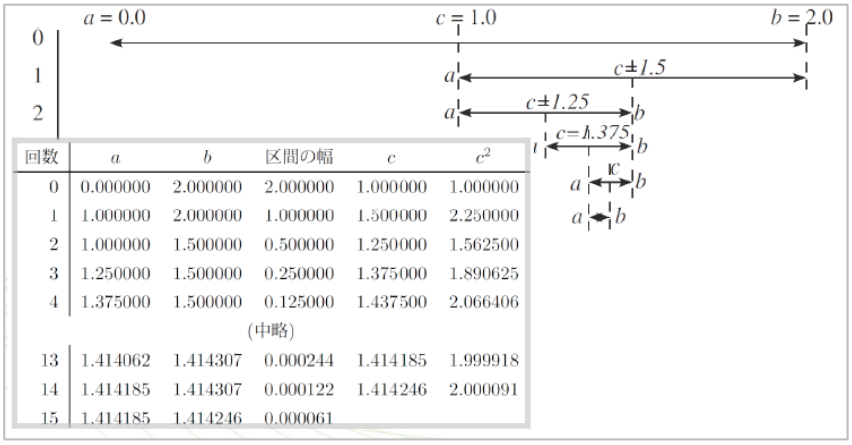
下から探る（今回）と時間かかりそう。上から解を求める、範囲を狭めるやり方は ないのか…。

＜アルゴリズム２＞ 二分法 (但し $x > 1$)

【アルゴリズム】	【現代語訳】
a ← 0	とりあえず、a は 0 と設定し、
b ← x	b は x と設定しておくぞ。
while b – a > δ **do**	★ b – a > δ が成り立つ限り、以下を行い、これを繰り返せ
c ← $\frac{a+b}{2}$	「まず、c を (a+b)/2 と設定するぞ。んで…
if $c^2 > x$	☆ $c^2 > x$ が成り立ったら、
then b ← c	今回の c を次回の b に設定しよう
else a ← c	成り立ってなかったら、
endif	今回の c を次回の a に設定しよう
done	☆ココまで。（★に戻るぞ）」
return a	b － a > δ が成り立たなくなったら、終われ。
	終わった時点の a が答えだから、吐き出せ。

解説的な例

- x = 2，δ = 0.0001



回数	a	b	区間の幅	c	c^2
0	0.000000	2.000000	2.000000	1.000000	1.000000
1	1.000000	2.000000	1.000000	1.500000	2.250000
2	1.000000	1.500000	0.500000	1.250000	1.562500
3	1.250000	1.500000	0.250000	1.375000	1.890625
4	1.375000	1.500000	0.125000	1.437500	2.066406
			(中略)		
13	1.414062	1.414307	0.000244	1.414185	1.999918
14	1.414185	1.414307	0.000122	1.414246	2.000091
15	1.414185	1.414246	0.000061		

※ ぼくたちも近似値探しで、しばしばやってきたやり方

351 の平方根を超えない最大の整数、何やったかな。
20 の２乗は 400、デカすぎ
10 の２乗は 100、小さすぎ
15 の２乗は 225、まだ小さい
18 の２乗は 324、まだ小さい
19 の２乗は 361、いやちょいとデカイな
とりあえず 18 かな。
出だしが違うからちょっと意味もずれるけど、
ニュアンスはこんな感じなので、
参考にしたければ参考にしてください。

アルゴリズムの速度

- 反復法の場合：約 $\sqrt{x}/\delta$ 回
- 二分法
  - 一回繰り返すごとに区間の幅が 1/2 に。
  - N 回繰り返したあとの区間幅は、$x/2^n$
  - これが δ 以下になるのに要する回数であるから、約 $\log_2 \frac{x}{\delta}$ 回

    （ $\delta = x/2^n \Leftrightarrow 2^n = x/\delta \Leftrightarrow n = \log_2 \frac{x}{\delta}$ ）
- 比較：x = 2 , δ = 0.0000000001（小数点以下１０桁まで求めるとき）
  - 反復法：約 141 億回
  - 二分法：３５回

- **計算量の考え方**
  - 重要：計算時間の見積もり
  - アルゴリズムにより計算時間も違う

    Ex.1)明日の天気予報の計算に３日かかっては意味ない

    Ex.2)100 年後に計算が完了する、は解けないに等しい

- **計算量**
  - 対象：アルゴリズムの計算時間（コンピュータ性能の違いやプログラムの作り方無視）
  - 「問題の大きさ」に対する関係の大まかな見積もり

- **計算量の使い方**
  - アルゴリズム同士の比較：プログラム作る前に良いアルゴリズム選べる
  - プログラムの計算時間を予想：
    - 悪いアルゴリズムが現実的な時間では終わらないな、てことがわかる
    - 小さい問題の計算時間 → 大きい問題の時間を類推・予測

- **計算量の見積もり**
  - 問題の大きさを変数で表し、：Ex.)n 個のデータを処理する
  - 計算の回数を式で表す：Ex.)3n+8 回, $5\log_2(n+1)$回
  - 詳細な式ではなく「オーダー」を使う
    - 例：O(n)回、O(log n)回
      - ※ ポイント：定数を無視 / 各変数について一番変化の大きい項だけを残す
      - ※ 理由：低数倍の差はコンピュータの性能の違いやプログラムの作り方ですぐに変わる

- **計算量の例**：平方根の計算
  - 反復法アルゴリズム：O($\frac{\sqrt{x}}{\delta}$)
  - 二分法アルゴリズム：O(log($\frac{x}{\delta}$))

【追記】
・計算量は？と聞かれたら、 3n+8 など
・計算量のオーダーは？と聞かれたら、 n などと答える
※だから O(n) という表記をいつ使うのかはナゾ…。

- **計算量の違いによる実行時間の差**

n	一	十	百	千	万	十万	百万	千万
$\log n$	—	1ns	2ns	3ns	4ns	5ns	6ns	7ns
n	1ns	10ns	100ns	1μs	10μs	100μs	1ms	10ms
n^2	1ns	100ns	10μs	1ms	0.1s	10s	16 分	27 時間
n^3	1ns	1μs	1ms	1s	16 分	11 日	31 年	3 千年
2^n	2ns	1μs	40 兆年					

  - 1 回の計算に 1 ナノ秒かかる場合の計算時間
  - 差が大きい → 定数倍の差は無視して大丈夫！
  - （数倍速くするよりも、計算量の違うアルゴリズムを使うほうが良い場合も多い）

第５章・第６章は近年頻出！かつ重要！（2011.2・2012.2）

第7章　コンピュータの仕組み

▼ INDEX と教科書該当箇所

7.1 計算の実現機構 … 153
　　コンピュータの基本構成,

- コンピュータの扱う情報：プログラム ＆ データ

➢ **プログラム**	コンピュータの実行する計算処理手順に関わる情報
➢ **データ**	コンピュータが処理する対象の情報

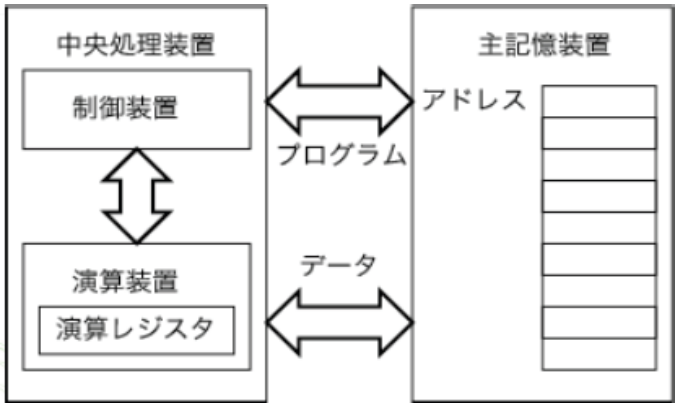
- 計算の実現機構
  - ➢ **プログラム内蔵方式**（フォン・ノイマン型コンピュータ）
    - ✧ メモリ上にデータとプログラムを保持
    - ✧ 万能チューリングマシンと同様の仕組みで計算進行
  - ➢ コンピュータ：機械語プログラムを解釈し、実行。

- コンピュータの基本構成
  - ➢ **中央処理装置（CPU）**：制御装置・演算装置を組み合わせたもの

✧ **制御装置**	主記憶装置と演算装置の制御
✧ **演算装置**	データに対する演算処理
✧ **演算レジスタ**	データ保持装置。CPU 計算の対象データはここに。 演算結果データも一度ここに。

※　アキュムレータ（AC；accumulator ）
…演算レジスタが一個しかない、初期のコンピュータ。
［＊ 編者注：教科書の英語は誤植 ］

  - ➢ **主記憶装置（メインメモリ）**
    - ✧ 情報（データ）の格納と選択的な読み書き
    - ✧ アドレスによってデータの位置を特定。（アドレス…数値で表す）



第8章　情報システムの役割

▼ INDEX と教科書該当箇所

8.2 情報システムの仕組み(クライアント・サー バまで，防火壁(ファイアウォール)以降 ）… 193

- **情報システムとは**
  - 今回見るのは広義（狭義省略）
    情報処理機器（コンピュータ）+情報伝達ネットワーク
    ⇒多様なサービスや機能を提供する
  - 実体が見えにくい…。

- **情報システムの仕組み**
  - ソフトウェア（コンピュータ内の話）：機能、作成の際のむずかしさ
  - ハードウェア（割と物理的な話）　　：構成、ネットワークの向こうに何があるか

  ※　チケット予約システムの例で確認

- **チケット予約システム概観**：利用者、空き状況見て予約（情報の入力）

＜実際のシステム＞

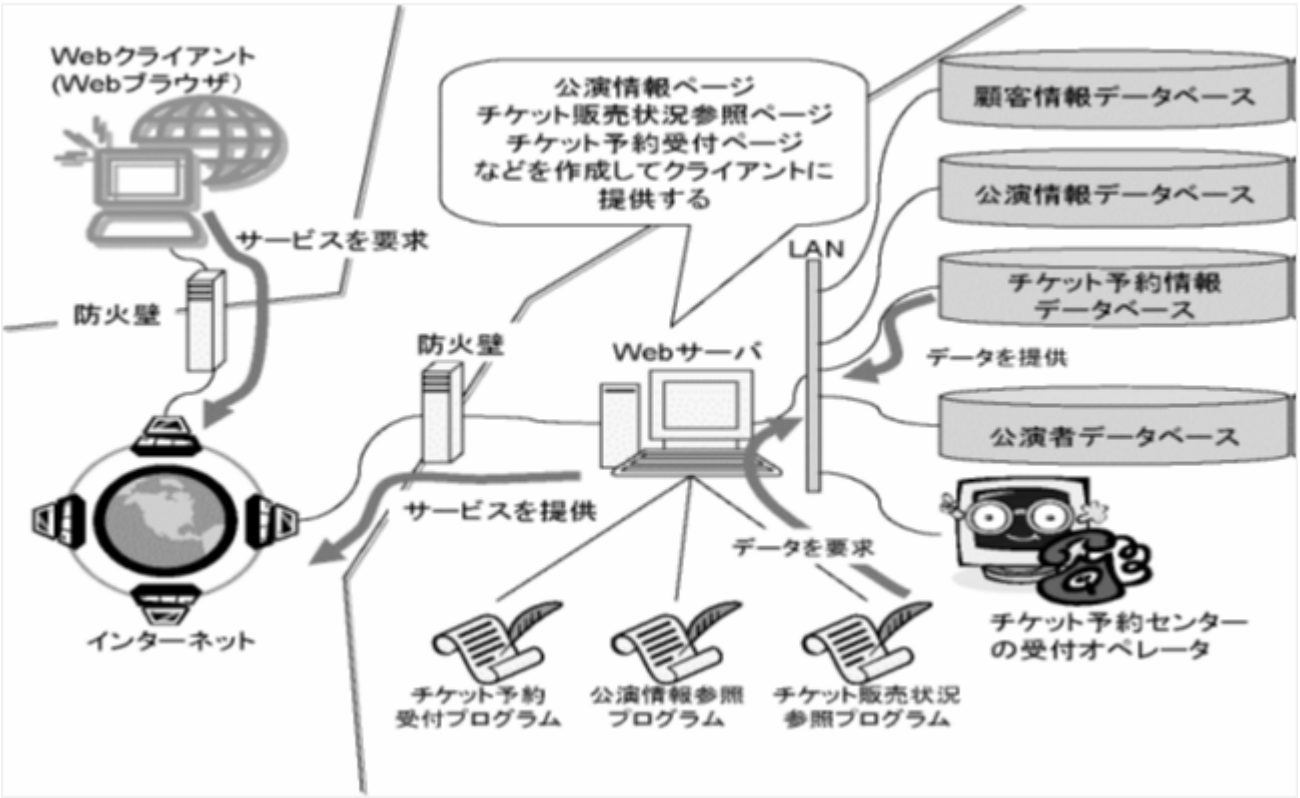
① ソフトウェア、多岐にわたって活躍。
　Ex.)公演情報管理・提供、チケット予約決済、会員情報管理

② システム構成
　✧ 利用者：いろいろな端末からアクセス
　✧ サービス提供者側：複数のコンピュータ
　　Ex.)WEB サーバ（利用者から要求受付)、要求処理プログラム、情報管理データベース

＜チケット予約システムの機能＞

① 情報照会：ジャンル・地域・販売スケジュール
② 公演詳細情報提供：
　個々の公演の情報（内容・出演者・会場・チケット情報（値段・座席)・手続き情報・主催協賛）
③ 予約機能：公園指定・チケット受け渡し型方法・予約確定・決済
④ 付随機能：誤入力処理・キャンセル処理（公演キャンセル・予約キャンセル）

- **チケット予約システムの仕組み**
  （次ページ図）(2009.3)

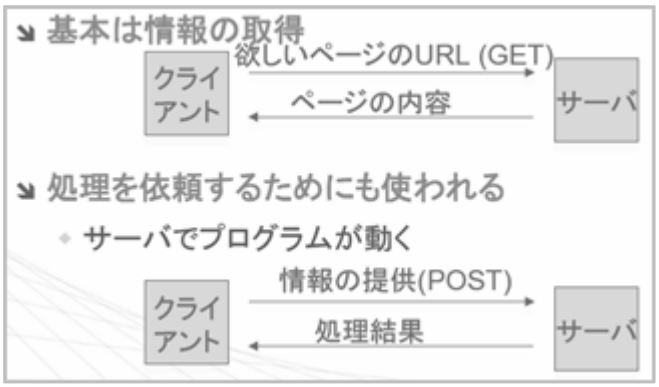


- **クライアント・サーバ型**（2010.3）
  （ネットワーク上の分散システムの構成）

➢ クライアント	サービスを要求
➢ サーバ	サービスを提供

- **通信規約 HTTP（Hypertexts Transfer Protocol）**

① WWW クライアントとサーバの間の通信に関する約束事（protocol）



② 通信要求のコマンド例（上図参照）

- ✧ GET：クライアントがサーバに情報資源をくれるように要求
  （Web ページ・ダウンロードみたいな）
- ✧ POST：クライアントがサーバに情報を与えるために出す要求
  （チケット予約・アップロード・掲示板投稿みたいな）

- **防火壁（ファイアウォール）**

① 不正アクセス排除目的で装備

② データベースサーバへのアクセス制御

（利用者直接アクセス不可・ブラウザ利用時のみ許可）

- **システム開発上の考慮点（2010.3）**

1. 利用者の使いやすさ：見た目・手間・ミス防止（利用者不快だと使わなくなる）
2. データの機密保護：個人情報!!!

   → 暗号化（情報漏洩×）、個人認証（なりすまし×）、プライバシー・ポリシー（外部流出×）
3. 処理の一貫性

   → 途中で故障 / 予約だけされて決済いかんとか、決済だけ行くとかあっちゃダメよね。
4. 並行処理：同時多数利用者アクセス!!!

   → 重複予約防止 / 最新予約状況表示
5. 悪意を持った攻撃への対処

   - 「不正な大量アクセス→サーバ・ダウン」
   - 対策

     i. トラフィック量などのデータ監視による攻撃検出

     ii. 特定された攻撃サイトからのアクセス拒否

     iii. ログデータの収集と分析

第9章　ユーザーインタフェース～人にやさしいデザイン

▼ INDEX と教科書該当箇所

9.2 インタフェースの定義とモデル … 213
　　インタフェースの定義と機能,　インタフェースの二重接面性,
9.3 インタフェースのデザインと評価 … 217
　　技術的側面からみたインタフェースデザイン ― インタフェースの種類と構成要素,

- **インタフェースの定義**：２つの異なる存在の境界面
  ①　水と油のように異なる物質間
  ②　コンピュータの複数のハードウェア間やソフトウェア間

＜この章で扱うインタフェース＞
　コンピュータなど人工物とユーザ（人間）との間
　＝「ユーザインタフェース」「ヒューマンインタフェース」と呼ばれる

- **インタフェースの機能**

ユーザはインタフェースを通して人工物を操作。
→ 人工物が機能を最大限に発揮するためには、使いやすいインタフェース必要
　Ex.）ドライバ…人間は握りを通してドライバを操作。最大限ドライバの機能を発揮するためには、使いやすい握り必要

＜コンピュータのインタフェースの特徴＞
（ドライバであれば、人間の道具への働きかけがそのまま対象であるネジへの働きかけとなるわけだが、コンピュータはそうもいかん…。エンターキーを押した力で何かが起こるわけではない）

道具	ドライバ	コンピュータ
インタフェース	握り	キーボード・マウス・ウインドウシステム・・・
道具への働きかけ	回す	キーを押す、マウスを動かす、・・・
対象への働きかけ	ネジを締める・緩める	メールを送る・変換を確定する・ウインドウを閉じる・入力を取り消す・・・

道具への働きかけと対象への働きかけが、１対１に対応しているかどうか

- **インタフェースの二重接面性**

① 第一接面（操作インタフェース）

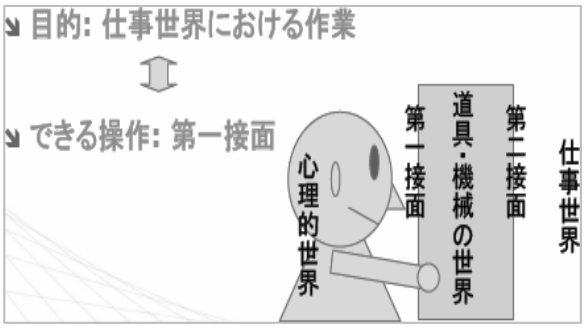
- ユーザ（心理的世界）と人工物（道具・機械の世界）の間
- 直接的

② 第二接面（制御インタフェース）

- 人工物と物理的タスク（仕事世界）の間
- 間接的

※ ユーザの目的は物理的なタスクの実
but 操作可能なのは第一接面

※ コンピュータなど、高度人望筒には二重接面性が存在する



＜二重接面性と汎用性＞

- 道具・物理世界から仕事世界への対応づけは多様（多様なソフトウェアによる）

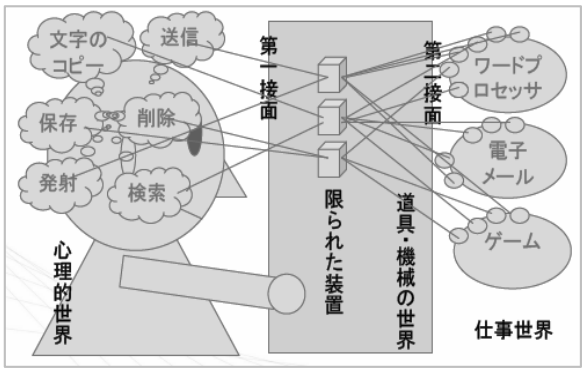
Ex.）ワープロによる文書作成・データベースソフトによるデータ管理•数値計算プログラムによる建物の構造計算

- 心理的世界から道具•物理世界への対応づけは限定的

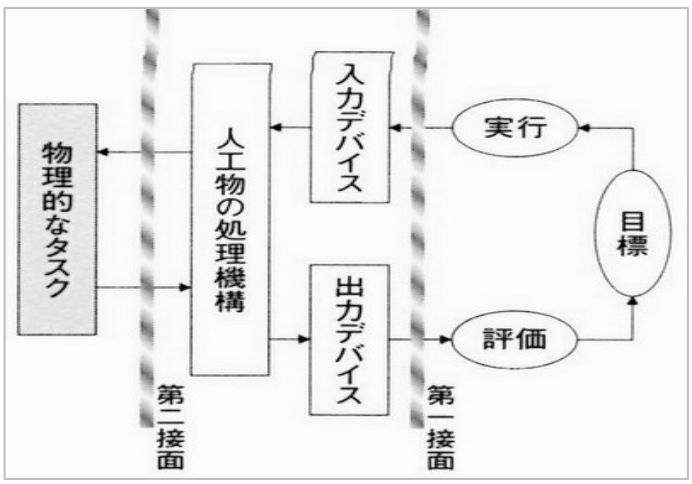
Ex.）キーボード、ポインティング・デバイス、GUI（Graphical User Interface）

- 逆向きの対応づけも同様
  - ✧ コンピュータやソフトウェアの状態や実行結果も多様
  - ✧ But ユーザに提供される出力は限られる…

Ex.）エラーメッセージ



- **技術的側面から見たインタフェースデザイン － インタフェースの種類と構成要素**



＜入力デバイス＞（2011.3）

- キーボード
- ポインティング・デバイス
  - ２次元的な位置情報を入力するデバイス
    （メニュー選択・アイコン操作 に最適）
  - **直接入力型デバイス**：ライトペン、タッチスクリーン[＊ 編者注：今時はタッチパネルと言うと思うが、ここは教科書の記載を尊重]
  - **間接入力型デバイス**：：デジタイザ、マウス、トラックボール、ジョイスティック
- その他：マイク、OCR 機器、バーコードリーダ

※ 用語解説

【 デジタイザ 】

位置を検出するセンサーを内蔵したボードと、位置を指定するペン（スタイラスペン）またはマウス型の装置で構成され、CAD(キャド)などに用いられる。

【 CAD 】

コンピュータを使って製品や建築物の設計・製図を行うためのシステム、およびソフトウェア。

【 ジョイスティック 】

ゲームコントローラの一。通常、前後左右に動かして位置や方向を指定するスティック（棒）と各種ボタンを備える。

（出典：コトバンク）

【 OCR 】

光学文字認識のこと。画像データ上にある文字と思われる部分を解析し、コンピュータ上で扱える文字(テキスト)データに変換すること。パソコンではスキャナーやデジタルカメラによって画像データ化された印刷物を「テキスト化」するのに利用されることが多い。パソコン用の市販ソフトウェアも数多く販売されており、Word ファイルや PDF ファイルを出力可能な製品もある。パソコン用のスキャナー(イメージスキャナー)の多くに、OCR ソフトが付属する。アルファベットや数字など、画数が少ないラテン系の活字に関してはかなり確実な認識を行うが、画数が多く偏(へん)と旁(つくり)など複数のパーツが 1 文字をなすことのある漢字等や、手書き文字の認識については改善の余地がある。OCR は、郵便物の郵便番号をスキャンして自動振り分け、および確定申告・労災申請といった政府機関への申請用紙、金融機関の振り込み用紙等の機械処理にも利用されている。（出典：知恵蔵 2013）

＜出力デバイス＞（2007.3・2010.2・2011.3）

- ディスプレイ、プリンタ、スピーカなど
- **GUI** (Graphical User Interface)
  - 情報の表示にウィンドウやアイコンなどのグラフィカルなオブジェクトを多用
  - ポインティング・デバイスでオブジェクトをそうさすることで基本操作の多くを実現

- **CUI** (Character User Interface)
  - ✧ 情報の表示を文字によって行う
  - ✧ すべての操作をキーボードで行う

	GUI	CUI
操作情報の提示	絵や画像も用いて視覚的に情報を表示する.	キーボードから命令を文字で入力, 文字列で結果を出力する.
特徴	直感的で, わかりやすい.	慣れれば, 作業は迅速.
構成要素と操作	ウィンドウ(window), アイコン(icon), メニュー(menu), マウス(mouse)などを用いた直接操作.	プロンプトに続いて, 文字列による命令を与える.

【 GUI 】

- 歴史
  - ✧ ライトペンやビットマップディスプレイの実用化（1960 年代）とともに構想される
  - ✧ アラン・ケイによるダイナブック構想（1968 年）と Alto の開発
  - ✧ マッキントッシュへの採用
  - ✧ Windows, X window system (UNIX 系)開発
- 特徴（2011.3）
  - ✧ **デスクトップメタファ**：机上に書類を広げる感覚での操作
  - ✧ **直接操作**の考え：**アフォーダンス**の概念拡張
    = その装置あるいは表示を見れば、どのように実行可能か即座にわかる
  - ✧ **WIMP システム**
    - ウィンドウ（W)、アイコン（I)、メニュー（M)、（マウス）ポインタ（P）を主な要素として構成
    - （マルチ）ウィンドウシステムによって実現

※ **アフォーダンスの概念**

外界の環境や事物が、生体の活動を供するべく持っている情報

Ex.）椅子の形状は、人が座るという情報を持っているとされる

【注意】（他年度他クラスシケプリより）（2008.3）

- マウスのほうが直感的操作可能（だからって常にマウスの方が優れているわけではない）
- キーボードのほうが精密で正確なものの作成可能

第10章　　情報技術と社会

▼ INDEX と教科書該当箇所

10.1　技術と社会

- 本章の目的
  - 現代社会において科学研究および技術開発の成果は、社会全体やその構成員の将来を左右するような形であらわれる。

    ＜ライフサイエンスと医療＞
    新しい治療法、生殖医療、再生医療の応用は、社会の構成員の一人一人の生や死と直結
    ＜情報技術＞
    技術の流通は、社会構成員一人一人のリスクや安全、セキュリティとプライバシーの問題と直結。

  - 科学技術に関係した（安全と安心に関わる）重大な社会的政治的問題が発生したとき、未来を選択する権利は、民主主義社会においては国民一人ひとりにある。
    →社会の構成員は、科学技術の研究成果について、その選択に必要な程度の基礎知識をもっておく必要がある。
  - 情報についても然り。
  - 民主主義社会において、「情報」に関する選択主体は私達、その選択に必要な程度の基礎知識はもっておく必要あり。＝情報を学ぶ意義。
  - 概略。およびその技術の人間や社会に対する意味。

- この章の目標：情報リテラシーの習得
  - 情報技術とどうつきあってゆくべきか？　―　答えはない
  - 情報技術が世の中にどのような影響を与えるか？
    - ✓ 良い・悪い影響両方ある
    - ✓ いくつかの事例

- ✓ 情報技術の特徴がどう関係するのか？
- ✓ どのような点が問題になるか（論点）

➢ 情報技術とどうつきあってゆくべきか？

10.2 情報技術による技術上の変化とその影響

年代	技術	影響
1960 年代 ～70 年代	商用・科学技術用コンピュータ	巨大データベース・大規模計算 ⇒権力の集中・個人のプライバシー問題化
1980 年代	マイクロコンピュータ ビジネスソフト・ゲーム	個人の道具としてのコンピュータ・ソフトウェア/ソフトウェアの所有権 *人工知能にも脚光
1990 年代～	インターネット・WWW	個人による情報発信が可能に プライバシー、情報の所有権

- **技術上の変化**（2009.3）

「500 年に一度の革命が今、世界で進行している。その名を **IT 革命**という。約 5 世紀前、グーテンベルクが発明した**活版印刷**はカトリック教会の独占物であった聖書を大衆に普及させ、宗教革命を勃発させた。**テレビ**は鉄のカーテンを突破して社会主義国家を崩壊させ、冷戦を終結に導いた。**情報メディア**はそれまで社会を支配していた権威をひっくり返してしまう破壊力を秘めている。そしていま、**インターネット**が日本でも IT 革命に火をつけた。」（AERA,2000,７月５日臨時増刊）

【解説】

Before　IT 技術	ホストコンピュータ管理による閉じられた世界 ➢ ホスト － 端末コンピュータ のネットワーク（村） ➢ 中央集権的管理可能 ➢ 閉鎖的 イメージ）組長のもとに組合員が集まる感じ。組長がホストで組合員が各端末コンピュータという関係図
インターネット（IT）技術	ネットワーク中心の開かれた世界 ➢ ネットワークとネットワークとの情報交換が自由に。 ➢ そのネットワークの境界の外に出ることも可能に ➢ 一つ一つのコンピュータが独自にネットワークとつながることが可能に ➢ 相対的に、中央集権的手法（ホスト対端末）を弱めることに。 イメージ）いろんな事務所があってどこもつながっているものだから、ある組織の組合員も好きに何処かにいける感じ。組長の影響が少し弱まる…。

- **技術変化の結果としてもたらされたもの**（2009.3）
  ① 場所の制約からの解放
  ② 時間の制約からの解放
  ③ 経路の制約からの解放
  ④ 輸送コストほぼゼロを実現

  Ex.） FAX 時代とメール時代とを比較すればわかる…。

※ コミュニケーション形態の変化

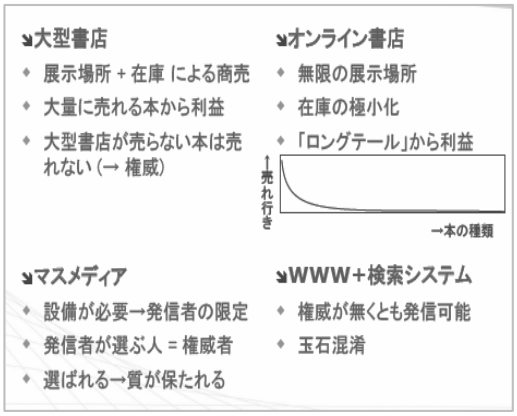
Before	➢ 場所・時間・経路に制約 ➢ （∴）国家や地域共同体のような地理的要素に依拠したコミュニケーションが中心
After	➢ 制約からの解放 ➢ （∴）上記のような地理的要素に依拠しないコミュニケーションが可能に。 ➢ （⇒）国家や地域共同体のような地理的要素に依拠した社会を相対化。

- **権威の崩壊**（以降の 10.2 は学習項目外）（2009.3）

例 1）流通機構の変化と規制
✧ 税務署も手の届かない巨大オークションの普及
- 流通経費がかからないために巨大店舗をもつものが優位を維持できない
- 従来の流通システムに対応した税システムが機能しなくなる可能性あり

例 2）系列会社優遇の壁の崩壊
✧ ウェブ上の部品取引による系列会社壁の崩壊
- 瞬時にして最安値の部品を仕入れることが可能
- 系列企業優遇の障壁が少なくなる可能性あり

例 3）情報流通．検閲機能の低下
✧ 検閲なしの情報の流通
- 出版社などのチェック機能なしに．すぐに電子出版が可能
- 個人のホームページを通じた情報の公開
- 情報は玉石混交
- ex．原爆の作り方が個人で入手できる．個人の意見が「事実」のように web 上に載せられるなど



例 4）文化や宗教への影響
✧ イスラム教徒でもアクセスできるアダルト画像
- 従来の検閲機能の機能不全．宗教への脅威

- **技術領域を超えた問題**

＜技術領域を超えた問題の例のまとめ＞

- 例 1＝税制や法への影響
- 例 2＝経済面の影響
- 例 3＝情報検閲の問題
- 例 4＝宗教や文化への影響

✧ 技術の普及によって、国境がない、法律が効かない、既存の権力が及ばない範囲での交流が可能になった。

✧ しかも、国家はネットなしで生きていけない。

✧ アナーキー（既存の秩序が及ばない）でかつ必要不可欠、破壊と創造の同居。

＜技術領域を超えた問題＞

➢ 技術領域を越えた問題の山積

➢ 既存の社会規範（法、倫理）によっては十分に制御しえず、新たな社会規範の形成が必要

- 法 の側面：有害情報の規制，著作権の保護，知財の分類
- 経済の側面：商取引の秩序と規制，流通機構の変化など
- 文化の側面：情報検閲の可否，デジタルデバイド

➢ サイバースペースの良い影響

✧ 情報技術を使った情報空間が公共的な議論を促進、

✧ 電子民主主義を促進。民主主義の発展に貢献する可能性

10.3 情報技術に固有な社会との軋轢

➢ 情報技術は、既存の社会規範（法、倫理）によっては十分に制御しえず、新たな社会規範の形成を必要とさせている。しかし、情報技術に限らなくても、新しい技術の開発は常に技術領域を越える問題を発生させ、新しい創造と破壊を作り出す

例：遺伝子組換え食品技術→食の安全についての新しい議論
再生医療や脳死移植技術→生命倫理についての議論
ナノテクノロジー→安全性にかかわる新たな議論

➢ では、情報技術に特徴的な社会との軋轢とは？（2012.3）

(1) 無形性と複製可能性（ジョンソン，2002）（2009.3）

✧ 無形性＝ソフトウェアやデジタルコンテンツが、従来の「モノ」概念とは異なる性質をもつこと

✧ 所有と権利に関わる法制度や倫理との間の軋轢

(2) グローバルな通信射程と匿名性

✧ ネット上の自由で規制のない議論空間、公共空間の構築として、電子民主主義の促進や情報技術によるガバナンスといった展望を開く

✧ 同時に、プライバシーやセキュリティといった側面での軋轢を生む

- **権利と所有概念への影響**

(a) 序論

- 情報技術は、市場に流通するものの「媒体」を変えつつある

  例：これまでの CD、ビデオテープ、現像された写真、本、コピーといった物質的な媒体で扱われてきたもの

→電子的に取り扱われることになる（電子媒体）

↓

- 保有あるいは所有といった概念も変容（2012.3）

  > 複写する行為、著作権の侵害に対する利用者の意識の希薄さ目の前のモノ（物質的媒体）のときは所有者がはっきりし、コピーをとることに対して対抗があったのに対し、電子媒体になったときにこのような抵抗が少なくなる

- このことが端的にあらわれるのが、著作権をめぐる議論。

(b) 著作権（一般）（2007.3・2009.3）

【著作権法第一条】
この法律は，著作物並びに実演，レコード，放送及び有線放送に関し著作者の権利及びこれに隣接する権利を定め，これらの文化的所産の公正に留意しつつ，著作者等の権利の保護を図り，もって文化の発展に寄与することを目的とする．

＜保護される著作物＞

1. 小説、脚本、論文、講演その他の言語の著作物
2. 音楽の著作物
3. 舞踏または無言劇の著作物
4. 絵画、版画、彫刻その他の美術の著作物
5. 建築の著作物
6. 地図又は学術的な性質を有する図面、図表、模型その他の図
7. 形の著作物
8. 映画の著作物
9. 写真の著作物
10. プログラムの著作物

- 本・映画・音楽等を作った人を複製から守る権利
  - ✧ 創作の労力に比べて複製は非常に簡単
  - ✧ 複製技術が登場して以来の概念
- 文化の発展が目的
  - ✧ 作者が安心して製作できるようにする
  - ✧ 誰もが安心して二次利用できるようにする
    - パロディも文化
  - ✧ 「物質」に依らないものなので，問題点も多い
    - 過ぎたる保護は発展を阻害

表 10.1 著作権法のなかのプログラムの定義

著作物として保護される	ソースプログラム オブジェクトプログラム オペレーティングシステム（OS） アプリケーションプログラム
著作物として保護されない	プログラム言語 規約 解法

(c) コンピュータプログラムの著作権

- プログラムの特異性
  - ✧ 小説のように人間が読むものではない
  - ✧ 配布メディアから複製をしないと動かない
  - ✧ 「情報」である → 創作の労力は大，複製は容易
  - ✧ デジタルコンテンツである→完全な複製が作成可能

- 1985 年の著作権法改正で「著作物」に
  - 保護されるのはプログラム
  - 「プログラム」の定義は図[表 10.1]参照（2010.2）
  - プログラミング言語・アルゴリズム（[表 10.1]でいう「プログラム言語・解法」）は対象外

【事例】
- A 社はビデオゲーム X を開発し，その著作権を所有している．
- B 社は都内で経営する喫茶店にゲーム X の無断複製ビデオゲームを設置して，顧客に利用させた．
- A 社は著作権侵害を B 社に対し訴えることができるだろうか？

【答え】可能。
【理由】この場合，ビデオゲーム機に取り付けられた ROM に収納されているオブジェクトプログラムは，A 社の著作物（ソースプログラム）の複製物である．したがって，B が使用したビデオゲーム機のように，ROM のオブジェクトプログラムを他の ROM にコピーして製造した偽造ゲーム機は，A のソースプログラムの著作権を侵害する．

(d) デジタルコンテンツの著作権（2012.3）

- デジタルコンテンツ
  - 音楽・映像・画像・電子書籍・ソフトウェアのファイルなどを指す。
- アナログコンテンツ（CD・カセットなど）との違い（2009.3）
  - 完全な複製が作れる
  - 簡単に複製が作れる
  - （＋ネットワーク）低コストで広範囲に配布できる
  - 複製しないと利用できない場合もある
  - システム次第では，利用方法を強く制限することもできる
    （cf.ディジタル放送のコピー制御）
- ネットワークによる情報発信と著作権
  - 放送と性質が似ている
  - 放送との違い
    - 必要な設備が非常に安い
    - 許可いらず
    - 「送信」ではない（受信側がサーバに要求するとサーバが返答しているだけ）
    - 世界中に発信する場合も組織内で共有する場合も仕組みが同じ
  - 1997 年の著作権法改正で「送信可能化権」が「公衆送信権」の 1 つに
- デジタルコンテンツの著作権

＜電子媒体＞
＝ デジタルコンテンツ記憶媒体
⇒ 新しい流通形態をもたらす
- 個人への直接の供給と消費
- 多種多様なデバイスによる交換が可能
- 使用許諾の概念曖昧化
  （メモリ上の電子情報は市場や流通機構なしに直接個人の手にわたることが可能）

↓

Winny の例

＜Winny 開発者起訴問題＞（2012.3）

【Winny】：匿名ファイル交換システム

- 中央集権的なサーバが不要
- 端末どうしでファイルを交換
- 匿名：最初に公開した端末が分からない・実際にファイルが置かれている端末はファイルの内容が分からない

→ ファイル交換が完全に匿名化されていることが特徴

→ デジタルコンテンツの著作権の侵害を幇助する側面を持っている

【Winny の利用実態】
- 著作権のあるデジタルコンテンツ(音楽・映像)の交換
- サーバがないので規制が困難

2004 年 5 月、開発者が著作権侵害幇助(ﾎｳｼﾞｮ)の疑いで逮捕・起訴

【起訴した側の主張】

現行の法律から鑑みて、開発者の行動は著作権侵害を幇助するという意味で罪である

【開発者の支援者や技術者の主張】

技術の進歩とともに法律も進化しなくてはならず、現在の技術によって簡単に著作権法違反が発生してしまう現状のほうが問題である

＝ 技術進歩と共に法律も進歩すべき

⇒ 論争における論点の幅が大きい

- 現実の著作権侵害をどう解決すれば良いのか？
- 侵害目的でモノを作るのは犯罪に問えるか？
- モノを作る人間は，使われ方にまで責任を負うか？
- 匿名システムはプライバシー保護につながるが，それを一切禁じることにならないか？
- 良い流通システムが無いからファイル交換ソフトが使われたのではないか？

例【研究者倫理と情報倫理】：包丁による殺人事件が発生したら包丁作った人まで罪に問われますか？違うでしょ、使い方の問題でしょ！Winny だって同じですよ、作ったからというただそれだけで罰するのはおかしくないですか？

※これは、Winny 開発者起訴問題における、開発者の支援者や技術者の主張ではないので注意

【結果】（おまけ）2006 年 12 月 13 日、京都地　裁は、著作権法違反の幇助により罰金 150 万円の有罪判決を言い渡した。同日、検察、被告双方が判決を不服とし大阪高等裁判所に控訴。2009 年 10 月 8 日、大阪高裁は、一審判決を破棄し、無罪を言い渡した。2009 年 10 月 21 日、大阪高等検察庁は判決を不服として、最高裁判所に上告。2011 年(平成 23 年)12 月 19 日、最高裁判所第三小法廷、最高検察庁側の上告を棄却し、無罪確定（Wikipedia 参照）

※2003 年 11 月、利用者 2 名逮捕

（∵ゲームソフトや映画などを不特定多数の人間がダウンロード出来る状態にし、著作権を侵害）

- プライバシーとセキュリティ

⑷ プライバシー（2011.3）

- ✧ コンピュータ技術による情報収集の規模拡大
- ✧ 自分の行動もすべて記録される
- ✧ 自分の行動記録の公開が常態化すれば、行動の自由もなくなる！
- ✧ 民主主義を支える自由のためにプライバシー保護必要！

→ 個人情報保護法

⑸ **個人情報保護法**（2003.5 成立公布・2005.4 施行）（2007.3・2011.3）

- ➢ 個人情報の有用性に配慮しながら個人の権利を保護することが目的
- ➢ 構成 = 官民を通じた基本法 + 民間事業者に対する個人情報の取り扱いのルール

＜個人情報取り扱い事業者が守るべきルール＞

1. 利用・取得に関するルール，
   - 個人情報の利用目的をできる限り特定し，利用目的の達成に必要な範囲を超えて個人情報を取り扱うことを禁止
   - 偽りその他不正な手段によって個人情報を取得することを禁止
   - 本人から直接書面で個人情報を取得する場合には．あらかじめ本人に利用目的を命じする必要があり．間接的に取得した場合には．すみやかに利用目的を通知または公表する必要がある
2. 適正．安全な管理に関するルール
   - 顧客情報の漏洩などを防止するため，個人データを安全に管理し，従業者や委託先を監督する必要がある
   - 利用目的の達成に必要な範囲で，個人データを正確かつ最新の内容に保つ必要がある．
3. 第三者提供に関するルール
   - 個人データをあらかじめ本人の同意を取らないで第三者に提供することは原則禁止．
4. 開示等に応じるルール
   - 事業者が保有する個人データに関して，本人から求めがあった場合は．その開示・訂正・利用停止などを行なわなければならない

- 個人情報の取り扱いに関して苦情がよせられたときは．適切．迅速に処理しなくてはならない．

(c) セキュリティ（2011.3）

3 つの側面	説明	もし侵されれば…
機密性 Confidentiality	許可されたもののみ情報アクセス可 → 不正アクセス防止法	情報漏洩(ロウエイ)
完全性 Integrity	情報が正確かつ完全なこと	情報改竄(カイザン)
使用可能性 Availability	必要な時に必要な情報資源にアクセス可能	使用妨害

- **不正アクセス防止法**（2008.3・2011.3）
  - ✧ 不正アクセス禁止
    Ex.)他人のアカウントとパスワードの無断使用・セキュリティホール利用による侵入
  - ✧ 不正アクセスを助長する行為の禁止
    Ex.)他人のアカウントとパスワードを第三者に提供すること
  - ✧ 罰則・再発防止のための措置などを定める
  - ✧ アクセス管理者(情報システムの管理者)、不正アクセス防御措置を講じる努力義務
  - ✧ 防御措置に対する都道府県公安委員会による援助について定める

→ 高度情報通信社会の健全な発展に寄与

(d) セキュリティ確保の技術的枠組み

イ) **個人認証技術**

- 情報システム管理者がアクセスしてきた人間を、利用権者であるかどうかを識別する技術
- 不正アクセス防止法「識別符号」
  Ex.)アカウント ID とパスワード・生体固有な特徴による個人認証

ロ) **暗号化技術**：元のデータを解読できないデータに変換すること（第三章参照）

ハ) 公開鍵暗号方式と PKI (Public Key Infrastructure)

- **公開鍵暗号方式**
  - ✧ 送信者：受信者が公開している公開鍵を入手し，その鍵で暗号化を行った結果を送信
  - ✧ 受信者：送信者から送られてきたデータを自分の秘密鍵で復号し，元のデータに戻す
- PKI (Public Key Infrastructure)
  - ✧ 公開鍵暗号方式を利用したセキュリティインフラストラクチャーのこと
  - ✧ 各人に固有の正しい公開鍵を配布 + 各人の身分を証明する証明書を発行
  - ✧ ＝ 認証局：各人の証明書を保管、他人の要求に応じてその証明書（つまり公開鍵）提供

ニ) **電子署名**：特定の文書の発信人を保証。

→ 契約時の本人確認・組織内合議での押印回覧の代替迅速化

10.4　情報技術論

- **技術は中立か**

➢　技術本質主義	技術は社会の形態や要望にかかわらず独立に発展するという立場
➢　技術の社会構成主義	今ある技術は、多くの可能性のなかから社会の構成員によってそのつどそのつど選択された結果であるという立場

- 社会構成主義

  確立された判断基準や分類境界に対する懐疑的態度、現在当然視されている事柄がどのようにしてそうみなされるようになったのかを問い直すこと

- 技術に応用：技術の社会構成主義（SCOT）

  現在確立されている技術に対する懐疑的態度、現在当然視されている技術がどのように確立したのかを問い直すこと

＜情報技術の場合＞

✧　ハードウェアが選択淘汰され、基本ソフトウェアが選択淘汰され、情報技術やブラウザが選択淘汰され、現在の形になってきている。

✧　今もさまざまな情報技術や情報をめぐる制度が選択淘汰されつつある時代に生きている。

✧　我々の今の選択は、将来世代の情報技術に影響を与える。

✧　技術開発と同時に社会への影響を考え，選択を公に開くことが必要

- **情報リテラシー**

➢　一般にリテラシー：読み書き能力、職字率のこと

➢　**科学技術リテラシー**：
科学や技術を使う上での基本的な能力、科学・数学・技術に関係した知識・技術・物の見方。物事を論理的に考える能力も含まれている。

【情報リテラシー】（2007.3）

➢　ただ単にパソコンを操作できるという意味の情報機器操作能力ではない。

✧　情報を主体的に選択、収集、活用、編集、発信する能力をもつこと

✧　情報機器を使って論理的に考える能力

➢　マウスでクリックしたときに「裏で何が動いているのか」についてのおおまかな想像力がおよぶ程度の理解能力

➢　情報技術の日常生活への浸透度が高い

➢　日々の技術革新の速度が速い

✧　広範囲の人に情報における批判釣思考の育成が必要

- ✧ 情報における批判的思考＝自分の操作の裏で何が動いているのかについて、ある程度論理的に考えること

➢ 技術の便利さの進展が操作の裏側を知らずに行う操作を増やしている
- ✧ 情報技術の特徴（多対多の通信射程、匿名性、複製可能性）を押さえた上での批判的思考が必要

10.5 これからの世代の情報

- 情報技術の普及
  - ✧ よい側面とダークサイド双方が同居。社会の新陳代謝加速。
  - ✧ 面白いものにぶつかるチャンスもあるし、危ないものにぶつかるチャンスも多い。
  - ✧ 状況ごとに技術開発者、利用者、法律の専門家や倫理の専門家などの相互の議論が必要。

- 我々の今の選択は、将来世代の情報技術に影響を与える。
  - ✧ 文明時代の野蛮人になるのではなく、
  - ✧ 問題が発生するごとにそれらの議論に「参加」し、新しい社会規範の構築に参加できる情報リテラシーを身に付けること

参考文献（体裁は気にしないこと）

- 「情報」(東京大学出版)
- 情報の共通 Web ページ
  http://www.edu.c.u-tokyo.ac.jp/edu/information.html
- 開先生の情報ページ
  http://lecture.ecc.u-tokyo.ac.jp/~chiraki/Jyouhou2013.html
- 他年度他クラスのシケプリ
- その他

更新情報

[ver.1.00]クラス内公開。以降、ver.1.11/1.12/1.20 で微修正追記を重ねる。割愛。[ver.1.50]一般公開版。

情報シケプリ（文系特化版）
¥0000000000

2013 年 7 月 25 日　ver.1.00　さとうまさし
2013 年 7 月 30 日　ver.1.50　さとうまさし

編　者　上に記載
印刷所　略
製本所　略

なまえ：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿.