

### 前回のおさらい

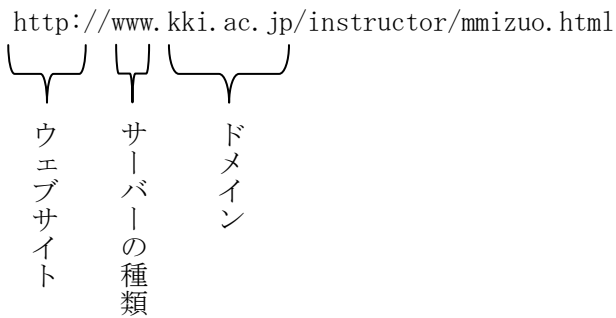
- PowerPoint によるスライドショー製作の流れ  
スライドマスター

## 情報理論

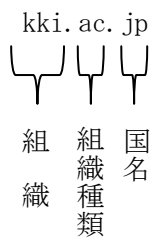
### インターネット通信の仕組み

#### URL とドメイン

- URL ⇒ウェブサイトなどの(俗に言うところの)アドレスのこと



- ドメイン ⇒URL の中心的部分 →その組織の名称・属性を表現している。



#### IP アドレス

コンピューターに数字の番地を割り当てたもの。携帯電話の場合は電話番号そのものが番地の役割を担っている。

例 192.168.230.258

- 管理組織 →NIC(ニック)によって世界規模で管理
- IP アドレス検索 →IP アドレス検索用のホームページなどでも検索可

#### 問題

SONY のホームページのドメインと IP アドレスを調べなさい。

## 問題

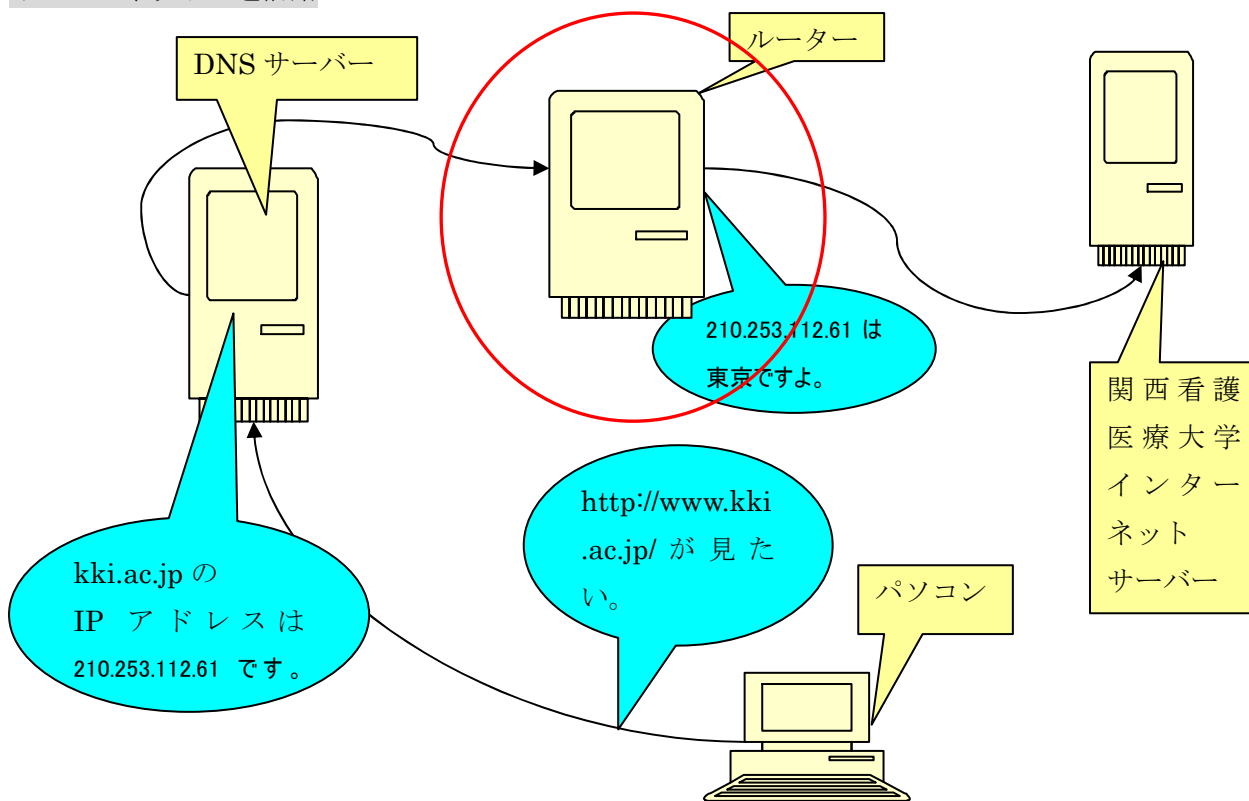
自分の使用しているパソコンの IP アドレスを調べなさい。

解答(本大学の場合)

- ① スタートメニューのコントロールパネルをクリック
- ② ネットワークとインターネット接続をクリック
- ③ ネットワーク接続をクリック
- ④ ローカルエリア接続のアイコンの上で右クリックして状態を選択
- ⑤ サポートのタグをクリック

注意 自宅のパソコンの場合は③がローカルエリア接続(=LAN)ではなく契約している**プロバイダー**の接続(例えば無線接続)になる。

## インターネットの通信路



## ネチケット

○インターネット上での**エチケット**のこと

○インターネット上の信号は**全て記録が残る**。

## 情報の量

### 情報量の単位

○bit(ビット) ㊦bits(ビッツ)

2つの状態(電圧のONとOFF)の識別が出来る。

=1個の記憶素子が扱う情報の量

= $2^1$ (10進法で)

2bits=2個の記憶素子=4つの状態{00, 01, 10, 11}= $2^2$

3bits=3個の記憶素子=8つの状態{000, 001, 010, 011, 100, 101, 110, 111}= $2^3$

4bits=...

○byte(バイト) ㊦bytes(バイトズ)

本来は(半角英)文字1文字を記憶するためのデジタル情報の量

=8bits

=8個の記憶素子が扱う情報の量

= $2^8$ (10進法で)=256(10進法で)

=256の状態の識別が出来る。

注意 歴史的な理由から、bitは通信速度に関する量で用いられることが多い。他方 byteは記憶装置の記憶量に関する量で用いられることが多い。

### 記法

2B=2bytes

2b=2bits

### 問題

1300Bは何b

### 解答

$1300 \times 8b = 10400b$

### 補助単位

(物理の知識)

k(キロ)  $\times 1,000$

M(メガ)  $\times 1,000,000$

G(ギガ)  $\times 1,000,000,000$

### 問題

10kmは何m  $10,000m$

200Mgは何g  $200,000,000g$

200Mgは何kg  $200,000kg$

40MBは何b  $40,000,000B=320,000,000b$

#### 問題

記憶容量 1.4MB のフロッピーディスクに 160kB の Word 文書ファイルは何個保存できるか？

#### 解答

$1.4MB/160kB=1.4 \times 1,000kB/160kB=8.75$

したがって最大でも 8 個まで

注意 フロッピーディスクの(一般の記憶装置も)外側の部分はデータの管理用に使われている。したがって実際には丸ごと 1.4MB は使用できない。

#### ネットワーク伝送方式

1つのファイルを1塊にして伝送することは有り得ない。

→分割して伝送

→**伝送渋滞緩和&伝送エラー低減**

○分割フレーム ⇒1つのファイルの分割の方法とその基本単位のこと

パケット単位(パケット交換式、不定長) →携帯電話などで利用

セル単位(ATM 交換式、固定長) →光通信などで利用

#### 回線速度

回線(光, ADSL など)の速さは1秒間に**最大**どの位の情報量が流れるかによって表現する。

例  $64kbps=64kb/s=64k \text{ bits per second}=1 \text{ 秒間に } 64kb \text{ の信号が流れる。}$

注意 **回線速度とはその回線の理論上の最高速度である**。現実にはこの速度は有り得ない。

#### 回線効率(回線利用率)

回線効率 =  $\frac{\text{実際の転送速度}}{\text{回線速度}} \times 100(\%)$

#### 問題

回線速度 128kbps の回線に実際には 6.4kbps の速さで情報を送信することができた。このときの回線効率は幾らか？

#### 解答

$6.4kbps/128kbps \times 100\% = 0.05 \times 100 = 5\%$

注意 自分の家のパソコンの回線効率は自分が契約しているプロバイダーのホームページを調べなさい。

#### 問題

回線速度 128kbps 回線効率 10%の回線を 8 秒間使用した場合何 B のファイルが転送できるか？

## 解答

実際の転送速度＝回線効率/100×回線速度

$$=0.1 \times 128\text{kbps}$$

$$=12.8\text{kbps}$$

$$=1.6\text{kBps}$$

$$=1600\text{Bps}$$

したがって  $1600\text{Bps} \times 8\text{s} = 12800\text{B}$

## 情報セキュリティ

◎セキュリティ＝防犯

◎看護師・保健師の扱う情報データ →患者さんのデータ

→情報セキュリティ&個人情報保護法は忘れない！

◎情報セキュリティ ⇒当事者以外の者が情報データに接近できない。そして情報の紛失が無い。

◎個人情報保護法 ⇒当事者が業務遂行以外の目的に情報を扱わない。そして第三者に情報を漏洩しない。

◎情報セキュリティ技術 ⇒認証技術+暗号技術

◎認証 ⇒誰がいつどの情報データにアクセスできるか及びアクセスしたかを管理・記録すること

利用者認証 →アカウント(ログイン ID+パスワード), 指紋認証, 網膜認証など

端末認証 →IP アドレスなど

相手認証 →コールバック, デジタル署名など

本物認証 ⇒本物のデータか偽造コピーかを識別する技術 →電子透かしなど

◎情報セキュリティの脅威

災害(自然災害、人災) →??

コンピュータウイルス →ワクチンソフト, アンチウイルスソフトなどで対抗

スパイウェア →アンチウイルスソフトなどで対抗

ハッカー・クラッカー →不正侵入, 盗聴する者のこと

→ファイヤーウォール, 暗号などで対抗

◎一番大切なのは倫理(道徳)の問題。

## 暗号

万一情報が盗まれた場合のために！

### 暗号通信

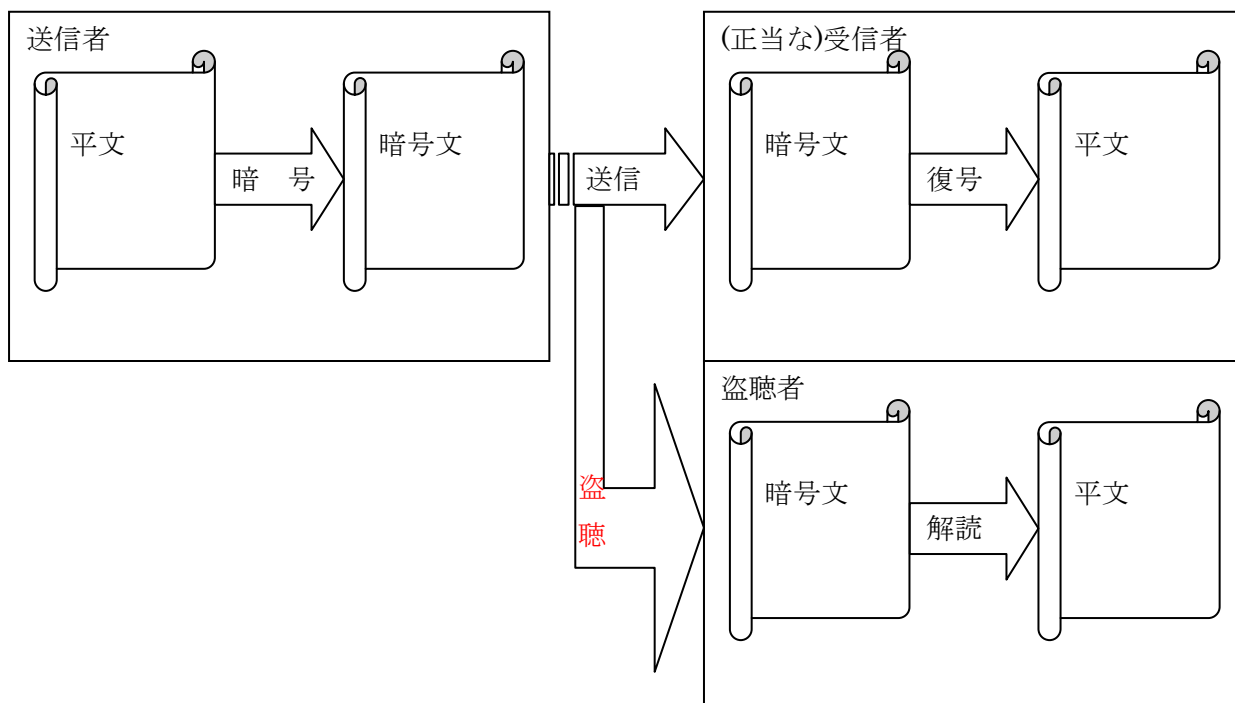
◎ ホームページの暗号規格 https など

◎ 電子メールの暗号規格 PGP など

メールは最も盗聴され易い

→ 暗号化していない電子メールで大切な情報を絶対に  
送信しない。

### 暗号化



### カエサル暗号

平文	暗号化鍵＝「2つ先の文字に変える」	暗号文
あ	→	う
い	→	え
う	→	お
え	→	か
お	→	き
か	→	く
き	→	け
・		・
・		・

例 あんごう→ういじお

#### 問題

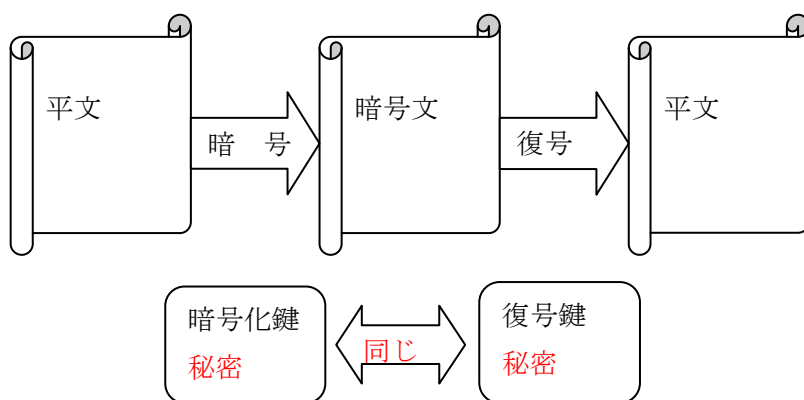
暗号化鍵＝「1 つ前の文字に変える」のカエサル暗号を使ったときの暗号文「おをげ」を復号して元の単語を見つけなさい。

#### 解答

かんご

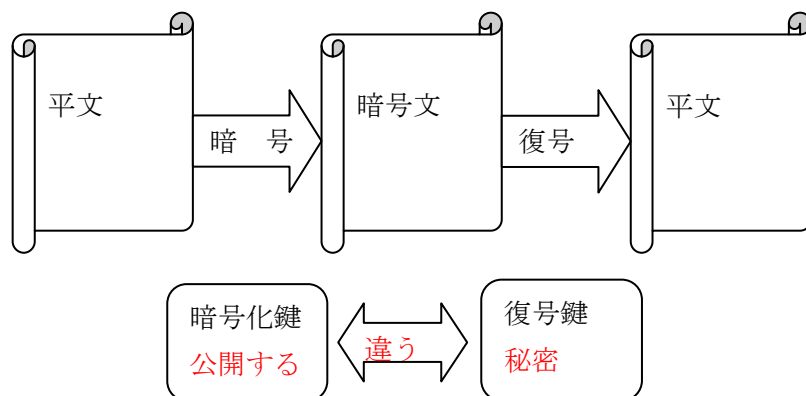
### 秘密鍵暗号

- ◎ 以前(コンピューター時代の初期に)使用されていた暗号
- ◎ カエサル暗号は秘密鍵暗号の最も簡単なもの



## 公開鍵暗号

### ◎ 現在の暗号



### ◎ 公開鍵暗号理論の優れた処

暗号化鍵と復号鍵が違う → 秘密の復号鍵は 1 人(受信者)だけ知っていれば良いので、バレナイ(受信者が喋らなければ)。

暗号化鍵から復号鍵を推測することが極めて困難 → 通常 70 桁以上の素数を 2 つ使って鍵を作成  
→ 暗号化鍵は公開しても OK

## 情報処理用語(補足)

これまでの講義で取り扱っていない重要用語

- ◎ **フォーマット** = (補助) 記憶装置をそのコンピューター(システム)で使用可能なように設定すること。具体的には、記憶領域の中に区切りを付けたりその区切りに番地(アドレス)を設定したりすること
- ◎ **オンライン処理** = 遠隔地のコンピューターとのインターネット回線によるデータアクセス+リアルタイム処理
- ◎ **レコードリンケージ** = (Excel とか Access などの) 複数の表データ中のデータを関連付けてあたかもより大きな複合表データのように扱うこと
- ◎ **情報リテラシー** = コンピューターの読み書きそろばんの技術 = Office や有名なアプリケーションソフトを使いこなすこと
- ◎ **ユビキタス** = 「どこにでも存在する」の意味 建物のいたるところに端末(入出力装置)が存在している様

## コンピューターのその他の知識①

### ファイルの圧縮・展開

コンピューターのファイルは一般に無駄な(あまり重要ではない)情報を多く含んでいる。

○ファイルの圧縮(凍結) ⇒無駄な(あまり重要ではない)情報を特殊な方法で整理してファイルの容量を小さくすること。圧縮(凍結)されたファイルそのものは一般には直接には動かない。

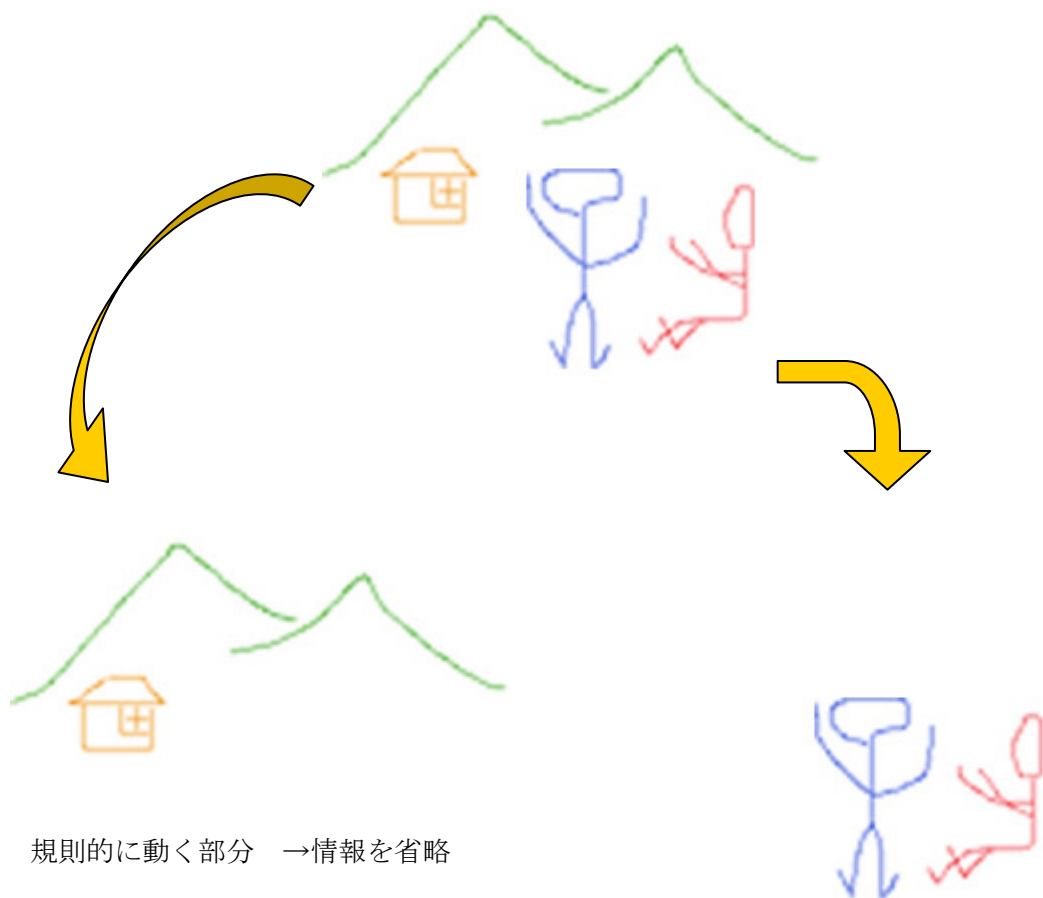
○ファイルの展開(解凍) ⇒圧縮(凍結)されたファイルをコンピューターで動かすことができる通常のファイルに戻すこと。

注意 ファイルを圧縮や展開するためのソフトウェアは、フリー(無料)のソフトウェアが沢山存在する。

○可逆圧縮 ⇒圧縮したファイルを展開によって元に戻すことができる通常の圧縮方法。一般の(任意の)ファイルに適用できる。圧縮の効果はそれほど期待できない。

○非可逆圧縮 ⇒重要性の低い情報を完全に取除いてファイルの容量を強引に小さくする特殊な圧縮方法。元のファイルを復元することは不可能。圧縮の効果は非常に大。圧縮されたファイルを専用のソフトウェアで直接動かすことができる。写真や映像のファイルなどに使用する。

例 DVD 映画の映像ファイル(. mpg)




規則的に動く部分 →情報を省略

不規則なアクションの部分  
→省略なし

### 課題

水尾のホームページにある7月03日ファイル圧縮・写真編集練習用ファイルは既に圧縮されたファイルです。これを一旦デスクトップに保存して、大学コンピューターに用意され

た圧縮・展開ソフトウェア  を用いて解凍しなさい。このとき解凍する前と解凍後でどの程度ファイルの容量が異なるか確認しなさい。

**ヒント** ファイルの容量の調べ方

ファイルのアイコンの上で右クリック →メニューの中のプロパティをクリック

### コンピューターのその他の知識②

#### 写真編集

将来自分の子どもの記録を残すために現代人に必要な知識

○画像処理 ⇒画像の大きさ・色合い・鮮明度などの処理など。

○画像への加筆の処理 ⇒画像に直接文字や線などを書き込む処理など。ペイント系ソフトとドロー系ソフトの2種類がある。

#### 課題

水尾のホームページにある7月03日ファイル圧縮・写真編集練習用ファイルの中の写真を用いて、Windows および Office に標準装備されている『Picture Manager』や『ペイント』のソフトウェアで写真の編集の仕方を練習しなさい。

注意 映像の編集も同様に家庭用コンピュータで可能。ただしソフトウェアの金額も作業の手間隙もずっと大。音楽の編集は簡単に可能。

#### 今後の予定についての連絡事項

○今期のレポート最終回(7月10日出題)

○7月10日(木)情報処理入門で定期試験対策資料(予想問題集)を配布

→定期試験では **60点分**はこの資料の問題の類似問題を出題

定期試験持込可 水尾作成の講義ノートを印刷したもの

定期試験対策資料

直筆ノート(あるいは水尾の講義ノートの上に直筆のメモ可)

電卓(携帯電話電卓機能使用不可)

○7月18日(金)に定期試験の日程・注意事項が掲示

→受講している講座の注意事項は全て確認しなさい。

→人体構造機能学は死ぬ気で試験準備をしなさい。

#### Wizの掲示板機能

① Wizにログイン

② **掲示板**を開く。

③ 水尾からの7月03日付掲示の指示に従ってその返答を1~2行程度で掲示板に書き込む。