情報理論及演習

2003 年 *7* 月 *7* 日

担当： 池口 徹

埼玉大学 大学院 理工学研究科 情報数理科学専攻 助教授

Email : tohru@ics.saitama-u.ac.jp

URL : http://www.nls.ics.saitama-u.ac.jp/~tohru

今日の講義の内容は?

インターネットの仕組み (続き)

- E-Mail はどのように配達されるか
- インターネットでのビデオ，オーディオの配信
  - ストリーミング
- WWW の仕組み
  1. ウエブブラウザ
  2. 検索エンジン
  3. セキュリティ
  4. クッキー

Ch.32 How E-mail Works

- インターネットの普及以前から
- 主な送受信のプロトコル
  - 送信：Simple Mail Transfer Protocol
  - 受信：Post Office Protocol
- アスキーテキスト情報だけでなく，ドキュメントファイル，グラフィクス，音声，ビデオなどの情報も添付可能
  - 送信時にアスキーテキストに符号化
  - 受信時に復号化
  - 規格
    - Multipurpose Internet Mail Extensions
    - uuenode
    - BINHEX

E-mail を送信する

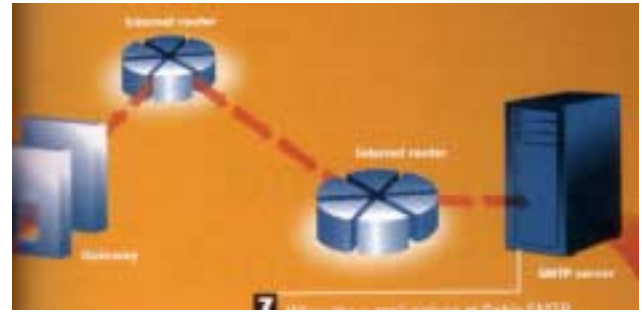
- Jane → Bob
- クライアント (Jane の PC) から SMTP サーバへ接続要求.
- SMTP サーバへデータ送信
- SMTP サーバから Domain Name Server へ
- DNS は，メッセージ送信の経路を決定

E-mail を送信する

- Jane → Bob
- クライアント (Jane の PC) から
  SMTP サーバへ接続要求.
- SMTP サーバへデータ送信
- SMTP サーバから Domain Name Server へ
- DNS は，メッセージ送信の経路を決定
- インターネット上の (いくつかの) ルータを経由.

E-mail を送信する

- Jane → Bob
- クライアント (Jane の PC) から SMTP サーバへ接続要求.
- SMTP サーバへデータ送信
- SMTP サーバから Domain Name Server へ
- DNS は，メッセージ送信の経路を決定
- インターネット上の (いくつかの) ルータを経由.
- Bob 側の SMTP サーバから POP サーバへ.



E-mail を送信する

- Jane → Bob
- クライアント (Jane の PC) から
  SMTP サーバへ接続要求.
- SMTP サーバへデータ送信
- SMTP サーバから Domain Name Server へ
- DNS は，メッセージ送信の経路を決定
- インターネット上の (いくつかの) ルータを経由.
- Bob 側の SMTP サーバから POP サーバへ.
- Bob から POP サーバへ要求

Ch.33 How Internet Video and Audio Work

- 大規模なデータ (音楽，映像) をインターネットを通じて配信する
- 配信方法
  - 全データをダウンロードした後，再生する
  - ダウンロードをしながら順次再生 ⇒ ストリーミング
- プロトコル ⇒ User Database Protocol
  1. TCP/IP におけるトランスポート層のプロトコル
  2. 処理が簡易，高速
  3. 確実性は低い，再送要求無し

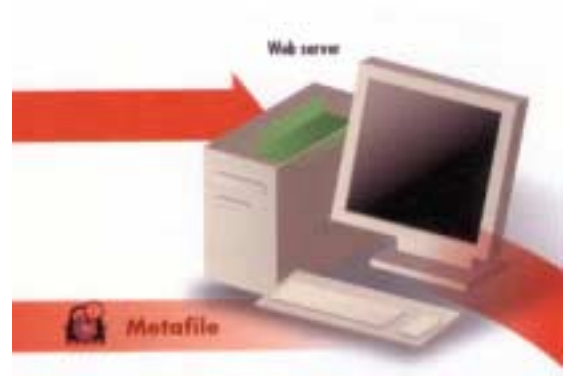
cf Transmission Control Protocol/Internet Protocol
UNIX ワークステーションおよびインターネットにおける標準プロトコル

Streaming Audio

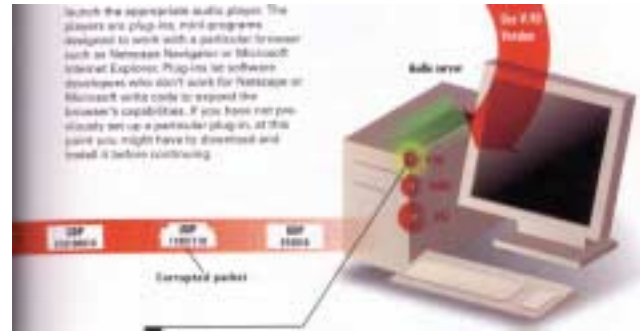
◀ ユーザからの要求

Streaming Audio

- ユーザからの要求
- ブラウザからウエブサーバへ要求

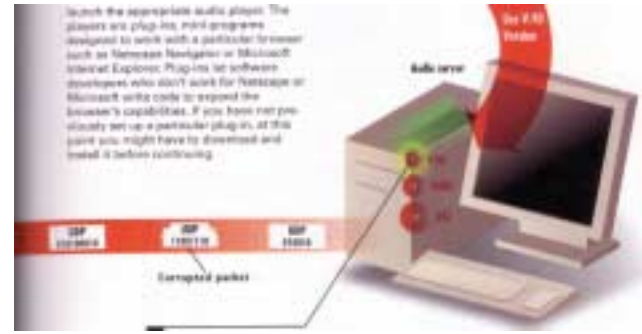


Streaming Audio

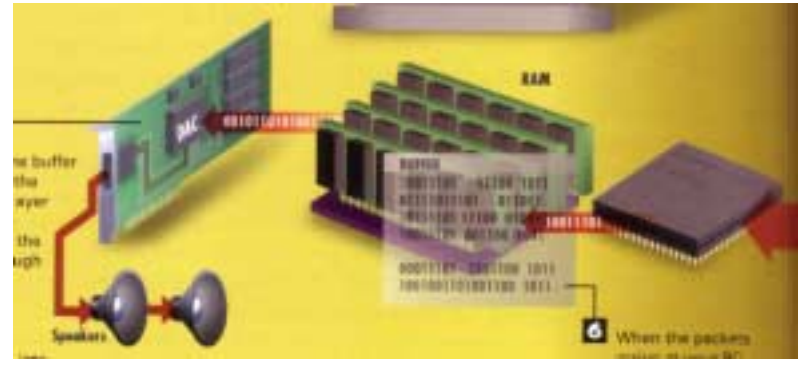


- ユーザからの要求
- ブラウザからウエブサーバへ要求
- ウエブサーバから，
  オーディオファイルの存在位置を返信
- オーディオプレイヤが起動し，オーディオサーバへ接続
- ユーザのネット接続環境に応じて
  オーディオファイルを選択し，
  UDP により PC へ送信

Streaming Audio

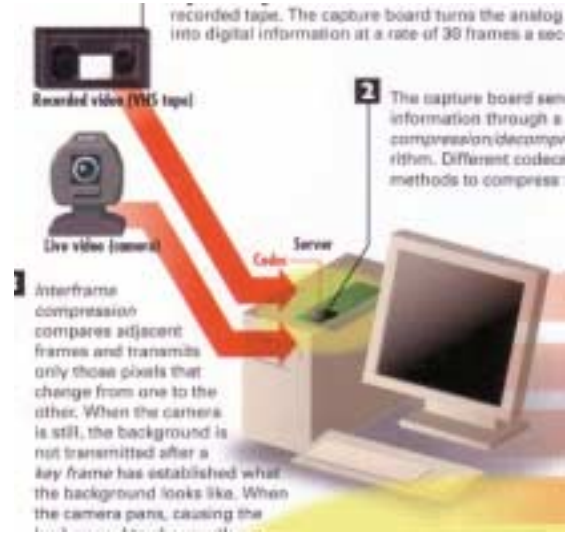


- ユーザからの要求
- ブラウザからウエブサーバへ要求
- ウエブサーバから，
  オーディオファイルの存在位置を返信
- オーディオプレイヤが起動し，オーディオサーバへ接続
- ユーザのネット接続環境に応じて
  オーディオファイルを選択し，
  UDP により PC へ送信
- バッファに格納
- オーディオプレイヤが再生開始



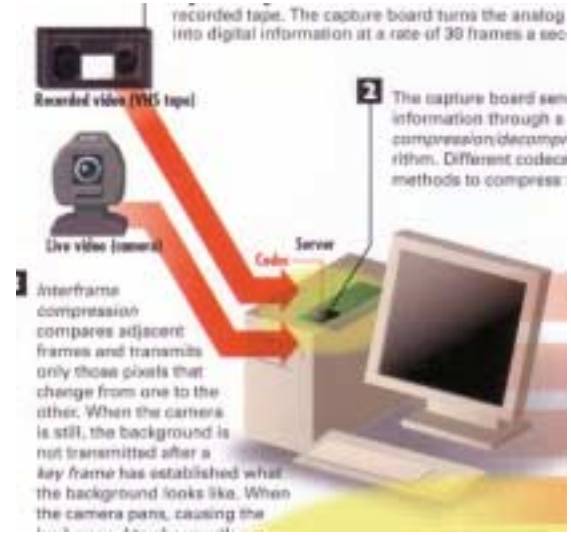
Streaming Video

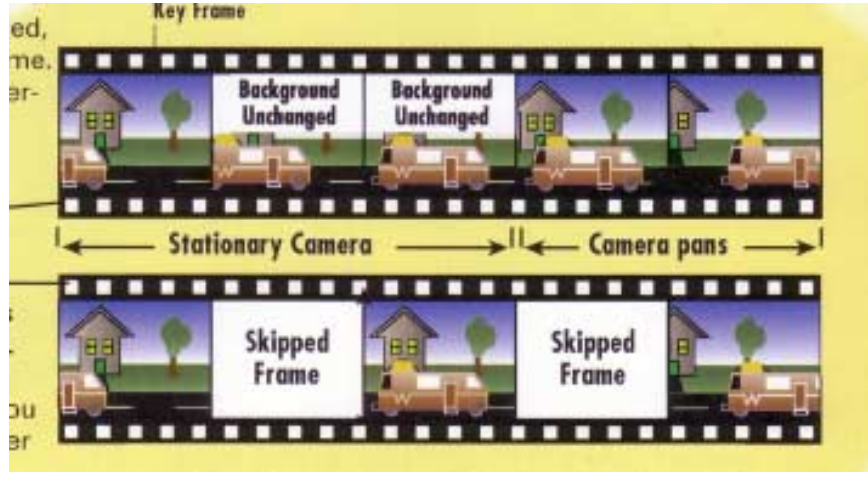
- VTR，Live Video (アナログ信号)
- 1 秒 30 フレーム
- データを圧縮



Streaming Video

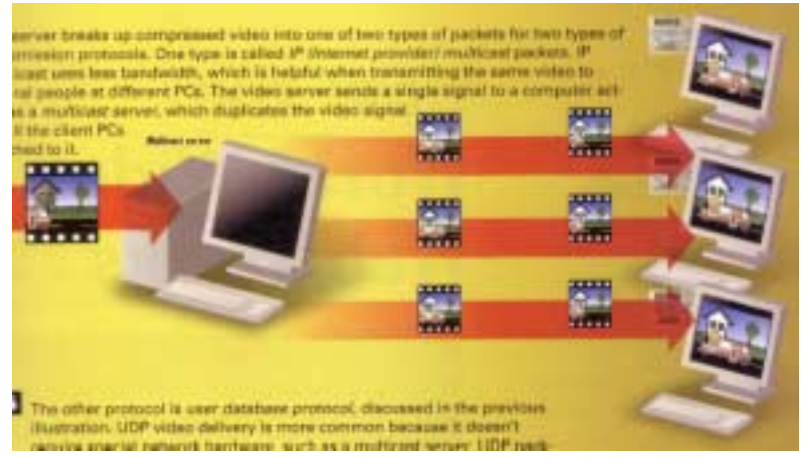
- VTR，Live Video (アナログ信号)
- 1 秒 30 フレーム
- データを圧縮
  - カメラ静止
  - カメラ移動
  - フレームのスキップ





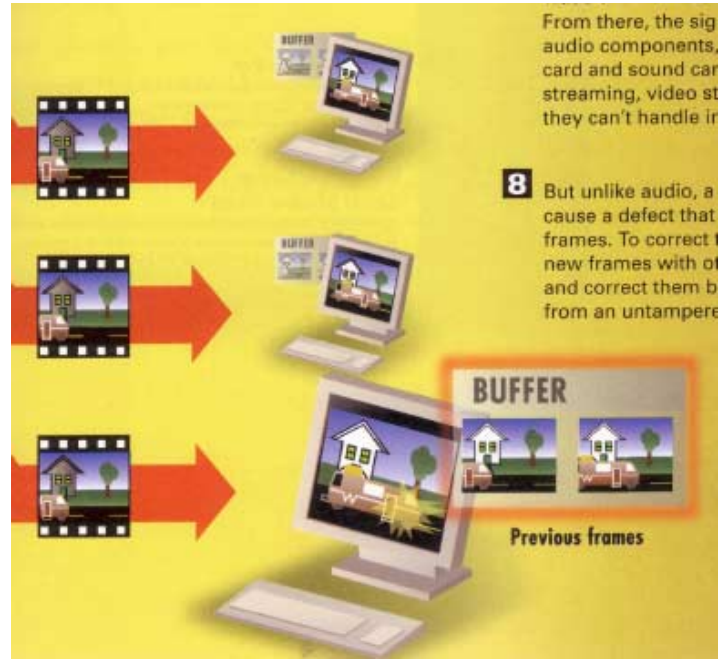
Streaming Video

- VTR，Live Video (アナログ信号)
- 1 秒 30 フレーム
- データを圧縮
  - カメラ静止
  - カメラ移動
  - フレームのスキップ
- 2 種類の伝送プロトコル
  - Internet Provider multicast
    クライアント PC にビデオ信号を多重化し配信
  - UDP



Streaming Video

- VTR，Live Video (アナログ信号)
- 1 秒 30 フレーム
- データを圧縮
  - カメラ静止
  - カメラ移動
  - フレームのスキップ
- 2 種類の伝送プロトコル
  - Internet Provider multicast
    クライアント PC にビデオ信号を多重化し配信
  - UDP



Ch.34 How the World Wide Web Works

- ウェブブラウザ
  1. Netscape Navigator
  2. Internet Explore
- Hyper Text Markup Language
- 検索エンジン
- セキュリティ
- クッキー

ウエブブラウザの仕組み

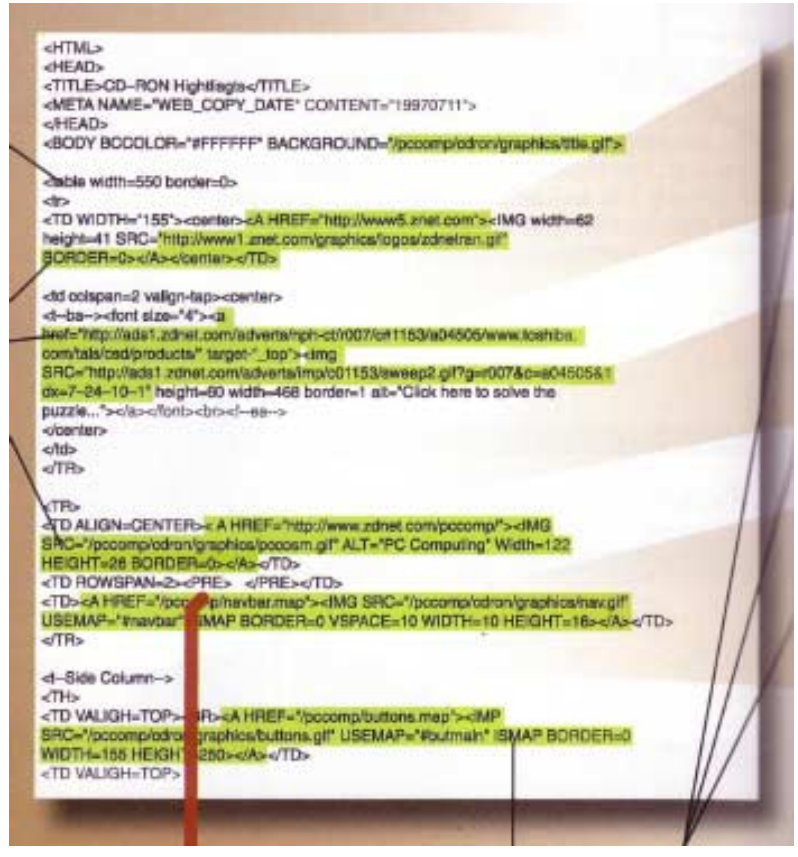
- ウエブサイトは,
  1. ファイル
  2. 文書
  3. グラフィック

  を提供
- 文書内に埋め込まれたハイパーリンクを辿って，他のサイト，文書への移動が可能
- Universal Resouce Locator
  インターネット上のリソースの所在の表現法
  http://www.tus.ac.jp/ → サイトのアドレス
  

ウエブブラウザの仕組み

- ブラウザから，アドレスを送信
- 最も近い Domain Name Server へ
  - 接続対象 URL を IP アドレスに変換する
  - IP アドレス
    IP プロトコルで用いる 32 bit のアドレス情報
    例:133.31.180.210
- DNS からルータを経由して WWW サーバへ，ブラウザの接続要求を送信
- ウエブサーバから，ブラウザへ HTML 形式のドキュメントを送信
- HTML 形式のドキュメントに従い，ブラウザが内容を表示

HTML



◀ ブラウザを用いて，HTML 形式のドキュメントのソースを閲覧可能
Netscape: 表示 → ページのソース

検索エンジンの仕組み

- 検索エンジンサイト (Yahoo, google, etc) が，ハイパーテキストのリンクを辿り，情報を収集する
- 収集情報後，情報の一覧を作成するソフトウエアへ
  - Universal Resource Locator
    情報の存在するアドレス
  - 情報そのもの
- 情報をデータベースへ
  - タイトル
  - 単語，頻度
  - 作成日時
  - サイズ

暗号

- 暗号化 → 通信内容が解読できないように，ある規則に従い，内容を他の記号に置き換えること
- 復号化 → 暗号化されたデータを元に戻すこと
- 暗号化の方式
  - 共通鍵 (秘密鍵) 暗号方式
    DES, IDEA, FEAL, MISTY
    1. 秘密鍵 → 公開しない
    2. 暗号化・復号化に秘密鍵を用いる
    3. アルゴリズムが単純 → 処理が高速
    4. 鍵の安全管理が困難
  - 公開鍵暗号方式 (Diffie and Hellman, 1976)
    RSA, EIGamal, 楕円曲線
    1. 公開鍵 → 公開する
    2. 秘密鍵 → 公開しない
    3. 暗号化には公開鍵，復号化には秘密鍵
    4. 処理が複雑

RSA

- MIT の Rivest, Shamir, Adelman, 1977
  - ある数を法 (mod) とする世界
    $12 = 2 \pmod{10}, 3 = 10 \pmod{7},$
  - (大きい) 素数の積を求めるのは簡単だが，ある整数を素因数分解するのは非常に困難
- アルゴリズム
  1. (十分大きい) 素数 p, q，素数の積 $n = pq$
  2. 暗号化 (e,n) $M^e \equiv C \pmod{n}$
  3. 復号化 (d,n) $C^d \equiv M \pmod{n}$
  4. $ed \equiv 1 \pmod{(p-1)(q-1)}$
- 例
  $p = 2, q = 7$ とすると，$n = pq = 14$

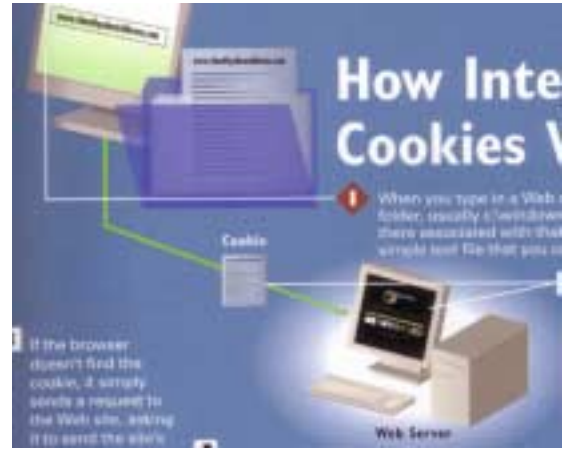
法を 14 とした巾乗

	巾乗数														
	1	2	3	4	5	6	7	8	9	10	11	12	13	···	25
1	1	1	1	1	1	1	1	1	1	1	1	1	1	···	1
2	2	4	8	2	4	8	2	4	8	2	4	8	2	···	2
3	3	9	13	11	5	1	3	9	13	11	5	1	3	···	3
4	4	2	8	4	2	8	4	2	6	4	2	8	4	···	4
5	5	11	13	9	3	1	5	11	13	9	3	1	5	···	5
6	6	8	6	8	6	8	6	8	6	8	6	8	6	···	6
7	7	7	7	7	7	7	7	7	7	7	7	7	7	···	7
8	8	8	8	8	8	8	8	8	8	8	8	8	8	···	8
9	9	11	1	9	11	1	9	11	1	9	11	1	9	···	9
10	10	2	6	4	12	8	10	2	6	4	12	8	10	···	10
11	11	9	1	11	9	1	11	9	1	11	9	1	11	···	11
12	12	4	6	2	10	8	12	4	6	2	10	8	12	···	12
13	13	1	13	1	13	1	13	1	13	1	13	1	13	···	13

- $p-1=1, q-1=6$
- $7=1\cdot(1\cdot 6)+1,\ 13=2\cdot(1\cdot 6)+1,\ 19=3\cdot(1\cdot 6)+1$
  $25=4\cdot(1\cdot 6)+1,\ 31=5\cdot(1\cdot 6)+1,\ 37=6\cdot(1\cdot 6)+1,\cdots$
- $25=5\cdot 5$ なので，$e=5, d=5$ とすれば良い．
- 平　文 $4,9,3,7,1,5,8,12 \Longrightarrow$ 暗号文 $2,11,5,7,1,3,8,10$
- 実際には p, q は 100 桁程度，従って n は 200 桁程度，
  n は公開されるが，p, q は秘密．復号化の巾乗数 d を推定するのは困難

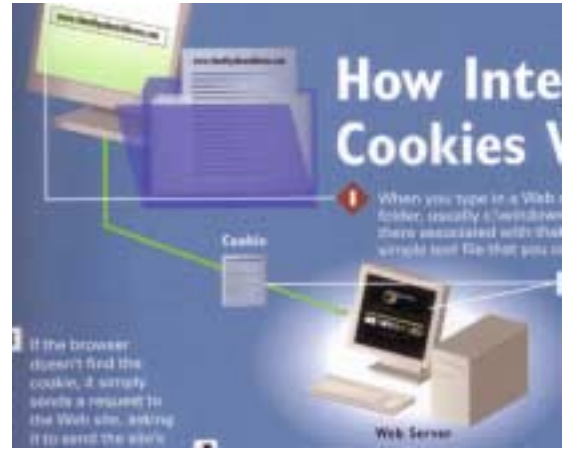
クッキー

- Web サーバにアクセス
  - 利用者識別目的
  - サーバからブラウザに送信 (URL, パス，有効期限)
  - ブラウザは保存
- 接続時発行 ID などの情報も保存



クッキー

- Web サーバにアクセス
  - 利用者識別目的
  - サーバからブラウザに送信
    (URL, パス，有効期限)
  - ブラウザは保存
- 接続時発行 ID などの情報も保存



来週

- 今週の演習問題の回答を配布
- 質問を受け付けます