1. 情報の伝達と通信

情報量　　（確率pで起こる事象の情報量）＝log2(1/p)と定義する。（単位はビット）

そうすると（１）「情報ＡとＢを同時に受け取った時の情報量と、それぞれの情報量の和が等しい」（２）「レアな情報は情報量が大きい」、という２つの性質が満たされて便利。

基礎知識

* プロトコル

通信のための手順の取り決めのことで、通信の当事者たちが共有する必要がある。www(world wide web)においてはHTTP（hypertext transfer protocol）というプロトコルが使われている。

* クライアントとサーバ

通信において、情報を要求する側をクライアント、情報を与える側をサーバと呼ぶ。

* webブラウザ

webサイトを閲覧するためのソフトウェア。Internet ExplorerやNetscapeなど

* 回線交換とパケット交換

教科書P５２を参照すること。

インターネット

いくつかの機器が繋がったものが**ネットワーク**であり、ネットワークが**ルータ**を介して接続した集合体が**インターネット**である。日常的にはwebサイトを見るのがインターネットだと思われがちだが、それはwww(world wide web)であり、インターネットの機能の一部に過ぎない。インターネット内の通信はTCP/IPというプロトコルに基づく。このTCP/IPは階層的構造をしていて、右下表のように分かれている。

実際の通信手順は以下のようになる。

|  |  |  |
| --- | --- | --- |
|  | プロトコル | 役割 |
| アプリケーション層 | HTTP | アプリケーション間の通信 |
| トランスポート層 | TCP | １対１の通信路の確保 |
| 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ーフェース層 | (イーサネット) | ネットワーク内通信 |

1. HTTPがメッセージを作る。
2. TCPが送信先に接続を依頼すると共に、

メッセージのデータを分割する。

1. IPが２で分割したデータを送信先が

属するネットワークまで運ぶ。

1. ネットワーク内で、送信先までデータが運ばれる。

階層プロトコルでは、プロトコル間に順位があり、表で上にあるものが上位プロトコルである。通信手順で上位から下位にデータが渡されるとき、元のデータに制御のためのデータが付加される。元のデータの先頭に付くものは**ヘッダ**、末尾に付くものは**トレーラ**と呼ばれる。

暗号

暗号において、もとのデータを白文といい、暗号化したデータを暗号文という。

暗号化と復元は、計算手順と鍵を用いて行う。鍵には二種類ある。

１つめの**共通鍵暗号**は、暗号化と復元に同じ鍵を使うものである。この鍵を使うときは、いかにして相手と鍵を共有し、他者に知られないようにするかが重要である。

２つめは**公開鍵暗号**で、暗号化と復元に使う鍵が別である。暗号化用の鍵と復元用の鍵の組を自分用に作っておき、片方を公開し（これが**公開鍵**）他方を秘密にしておく（これが**秘密鍵**）。暗号化用の鍵を公開すれば、自分宛のメッセージを自分だけが読めるようにできる。また、復元用の鍵を公開し、一方向ハッシュ関数（←テスト範囲外）と組み合わせることによって、メッセージの発信者が自分であることを証明するのにも使える。