Ver.2.0

情報学基礎

アウトライン

2013/07/18
Misawa

第１章
情報倫理
作成者に利用に関する権利がある
パスワード、ウイルス、アプリケーションの更新
　踏み台･･･感染に気づかず、意識しなくても
　　周りへの脅威になる
　クラッキング･･･パスワードが盗まれること
→署名機能を利用

著作権
著作権　　←自動的
特許権、商標権　←登録必要

知的創作活動の結果である著作物の権利を保証
　原著作物･････元
　二次著作物･･･元を編集
　編集著作物･･･元を部品として新しく作成

無断でできること･･････著作物を使用する
できないこと(コピー)･･･利用する
　他人の文章を無断で利用しない

・著作権････死後50年有効、譲渡可能
・著作者人格権････同一性保持性
　（勝手に変えられない）
・公表権　（勝手に公表されない）
・著作隣接権　←伝達する人に与えられる

情報セキュリティ
脆弱性orセキュリティホール ････弱点
脅威････攻撃
　例：盗聴、情報漏洩、改ざん、なりすまし、
　　不正アクセス、コンピュータウイルス
暗号化されているか？踏み台にされないか？

情報セキュリティ
情報のCIA････機密性、完全性、可用性
　機密性･･･第三者が利用できない
　完全性･･･完全に維持
　可用性･･･要求があれば、使用できる。

現在では、
真証性(自分がしたのか)、責任追求性(トラブルの元をたどれる)、否認防止、信頼性(いつでも)

アクセス権、認証、署名
・ログ････処理の記憶
・アクセス権････情報の利用、操作できる権利

アクセス権の有無で正当、不当なユーザをcheck
認証
ユーザIDとパスワードによる認証
・デジタル署名････本物で変更されてない証明
　セキュリティ
・マルウェア････悪意のあるソフトウェア
　コンピュータウイルスとか
　アンチウィルスソフト入れる、感染して踏み台注意
　推察しやすいパスワードを避ける

暗号化技術
・暗号････第三者に理解できない
　伝達、蓄積時に用いる。機密性が保たれる。
・平文････誰でも読める

暗号文
・暗号化････平文→暗号文の変換
・復号････戻す
・暗号化アルゴリズム････暗号化の手順。
　暗号鍵を用いる。
　例：シーザー暗号

解読
・暗号強度････解読の難しさ。高いほど良い。
・共通鍵暗号････暗号化と復号化で同じ鍵を用いる。
　鍵は秘密にする。鍵配送問題
　代表:DES

・公開鍵暗号････暗号化と復号化で異なる鍵を用いる。
　公開鍵の一方を公開し、他方を秘密にする。　（公開鍵、秘密鍵）
　例）AからにBに公開鍵暗号で情報を送る時、
　Aは『Bの公開鍵』で暗号化し送る。
　受け取ったBは『Bの秘密鍵』で復号化する。

第２章
コンピュータ
・デスクトップ型、ラップトップ型(ノートPC)
　応答性能、グラフィック性能が重要。
・サーバ
　大規模な計算。信頼性が重要。
・スーパーコンピュータ
・組込み
　決まった処理しかしない。コストが安い。
　消費電力の削減が重要。
・スマホ、タブレット
　PCと組込みの中間。ネットワーク機能、
　ユーザインターフェースが重要。

デジタル論理回路

1.0のみを用いる。　AND素子、NAND素子
8ビット=1バイト
　　AND　→入力が両方1なら出力1。
　　　　それ以外なら0。
　　NAND→ANDの逆
CMOS素子から発展

コンピュータの3要素

-中央処理装置（CPU）
　　レジスタ（演算を一時保存）、データパス（演算器）、入出力装置からなる。データパスはALU（算術理論装置）とレジスタからなる。
-メモリ
　　主記憶のDRAM（RAM）と小容量のキャッシュ
　　→記憶の階層
　　フラッシュメモリは不揮発ROM
-入出力装置

プログラム

例）演算命令　ADD R1,R2,R3
　　ADD　オプコード・・・・操作を指定
　　R1R2R3　オペランド・・・操作対象を指定
　　意味　R1←R2+R3　Rはレジスタ

　　分岐命令（繰り返し）もある
　　プログラム格納型という。

二進数

負の数
　　符号付き整数（+ -）←負数の足し算は不可能
　　補数表現　←負数の足し算OK
小数
　　浮動小数点　←循環小数による丸め誤差あり
　　実際にはIEEEが使われてる。

　☆補数表現、浮動小数点は扱えるように！

文字
　　文字コード　ASCII（アスキー）コード...7bit
　　ひらがな、カタカナ、漢字は...16bit
　　JISコード、シフトJISコード、Unicode

コンピュータ歴史

　　1940~ENIAC　真空管用いた←配線必要
　　1980~パーソナルコンピュータ
　　ムーアの法則　←電力の問題、周波数が上がらない
　　マルチコアの時代へ

第3章

ソフトウェア

　　ハードウェアに何させるのか決めるもの
　　ハードと比べて変更、拡張しやすい。

プログラム

指示内容を書き下したもの
同じ処理でも、方法によって処理速度が異なる。
具体的な解法をアルゴリズムという。

・アルゴリズム
　　同じ問題でも色々。実効速度が速いのがよいアルゴリズム。
　　計算量をO（　）　　オーダーと表す。
　　O（1）は定数。O（logn）は効率がいい。

・プログラミング言語
機械語・・・・2進数　←CPUにとって分かりやすい。
アセンブリ言語・・・・ADDとか　←人に分かりやすい。
　　これらは低水準言語（ハードに近い）
　　→面倒、分かりにくい。

高水準言語
FORTRAN、Lisp、Java、（Smalltalk、Haskell）
人にとって分かりやすい。大規模化しやすい。

CPUには理解出来ないので、翻訳、通訳する。
（プログラミング言語処理系）
　　翻訳・・・・コンパイラ方式　←翻訳済み
　　通訳・・・・インタプリタ方式　←同時通訳

　　ライブラリ、ソフトウェアフレームワーク
　　、、、よく使う機能や間違いを指摘する

第4章

ソフトウェアの階層

・オペレーティングシステム（OS）
　　他のソフトウェアの環境づくり的な働き　（土台）
・ミドルウェア
　　特定の分野に特化した土台
・アプリケーション
　　ユーザーの望む処理を直接行う。
　　OSに処理を依頼する。
　　インターネットに接続するアプリケーションはwebサーバというソフトウェアと通信する。

アプリケーションの種類

　　文書処理、作図と画像処理
　　表計算とデータ処理、数式処理と数値解析
　　ネットワークアプリケーション（サーバとクライアント）
　　マルチメディアアプリケーションとオーサリングツール（動画や音楽）

ソフトウェア開発

プログラミング‥‥プログラムつくること。

ウォーターフォールモデル

1、要求定義‥‥なに作りたいのか要求仕様書作る。
2、分析・設定‥‥どう作るのか
3、プログラミング
4、テスト‥‥確認
5、運用・保守

第５章

1980~インターネット接続業者（ISP）が登場

電話の歴史

回線を直接電気的に繋ぐ（回線交換）
↓
グラフにして（標本化）データを減らし、
一本の回線で済むようにした。

インターネット

定義：インターネットはTCP/IPというプロトコルを使用してデータ通信を行うネットワーク

多くのISPの集合。
「ネットワークのネットワーク」という。
自立システム（AS）
‥‥同一の運営方針で管理されてるISP系

インターネット
内部のルータが互いに接続。末端がホスト。

情報をパケットに分割し、送信元（ホスト）と宛先（終点）を示すIPアドレスをそれぞれのパケットに付加して送る。
ルータでは次にどのルータに転送するか判断する。
回線はなく、すべてパケット転送で共有される。
（パケット交換）
パケット交換では、通信品質の保証は困難。
通信の数は増やせる。

プロトコル

通信における決まり事。　パケットのフォーマット、送受信の手順、受信時の動作を定義。

プロトコルの階層化が必要。
OSI参照モデル‥‥ISOが定義した7階層のプロトコル階層

インターネットは5階層構造。下から
1、物理層‥‥電圧等を指定
2、データリンク層‥‥機器間の通信手順
3、ネットワーク層‥‥ルータ間の通信手順
4、トランスポート層‥‥エンドホストでの通信手順
5、アプリケーション層‥‥アプリケーション毎の通信手順

アプリケーション層からデータ（ペイロード）が下に降りる度に各階層で、先頭に情報（ヘッダ）を付加する。
（多重化）
PDU‥‥ヘッダとペイロード合わせたもの。

受信先でPDUを適切にヘッダを取りながら上の層に渡す。（逆多重化）

プロトコルの階層化の利点は
機能詳細の隠蔽‥‥下の層を気にせず作れる
モジュール性の高さ‥‥変更してもプロトコル階層全体に影響ない

データリンク層プロトコル　←第2層

通信媒体で接続されたホスト間の通信手順を規定する階層。
通信媒体は有線と無線がある。
代表：イーサネット（Ethernet）
通信（伝達）速度を上げてきた。
データリンク層アドレス（MACアドレス）で特定のホストを識別する。

イーサネットはバス形式の接続でケーブル1本なので、同時に送信できない。
衝突を避けるための手順をCSMA/CD方式という。（他の人が話してたら話さない。遠慮）

イーサネットフレームフォーマット

ヘッダの付け方
・イーサネットフレームの前にプリアンブルがつく。（フレーム同期）
←受信ホストがフレームの位置を知るため。
・送信、受信ホストのMACアドレスも付く。

ネットワーク層プロトコル（IP）　←第3層

IPにより様々なデータリンク層プロトコルを用いるネットワークを接続。
IPv4‥‥主流。2の32乗　足りない。
IPv6‥‥普及していない。2の128乗

ネットワーク層アドレス（IPアドレス）

今は32bit
サブネット番号とホスト番号からなる。
インターネットからサブネットを識別。
サブネットからホストを識別。

パケット転送方式

ネットワーク層の通信方式は

仮想階層方式‥‥送信、受信ホスト間のルータで仮想回線を設定
データグラム方式　←インターネットはこっち

送信ホストがネットワーク層のヘッダに終点ホストのIPアドレスをかいて送信。
ルータは経路表から終点ホストを見つけ、指示されたルータにパケットを転送。
　　ヘッダのTTLは永遠の迷子を防ぐ。

トランスポート層プロトコル　←第4層

エンドホストでのアプリケーションの通信機能を提供する。

ソケットとポート番号

ソケット・・・・トランスポート層のアプリケーション層の接点
　　ソケットはIPアドレス（どのCPUか）と
　　ポート番号（どのアプリか）の対。

トランスポート層の通信方式

UDP・・・・コネクションレス通信。好きな時に話せる。信頼性はない。 radikoとか
TCP・・・・コネクション指向通信。信頼性保証。
　　メール、Webとか

シーケンス番号・・・・順序通り、欠落なし保証
チェックサム・・・・誤りなしの保証

　　正しく受信すると確認応答（ACK）パケットを返信（無かったら再送）。
　　→ストップアンドウェイトプロトコル
　　前者から高速化した
　　→スライディングウィンドウプロトコル

輻輳制御・・・・輻輳（混雑）が起きないようにウィンドウサイズを調整する
流量制御・・・・相手の受信能力に合わせて制御

第6章

ドメインネームシステム（DNS）

人間にとって分かりやすいコンピュータの名前（住所名）　←IPアドレス使わない
ドメイン（コンピュータの住所）を階層的に定義し、各階層がより下位の階層のドメインに権限を委譲する。
　　.com　米の商業組織
　　.edu　米の教育組織
　　.jp　　日本の組織
　co.jpは日本の商業組織、ac.jp日本の教育組織
　　慶応理工学部は　st.keio.ac.jp

探すには、jpドメインネームサーバに問い合わせ、次にac.jpを問い合わせと続く。（上に上に担当を探してく）

メール

メールシステム（プロトコル）は
配送 システムと受信システムの2つ。
　・配送システム
　　SMTP　自分のSMTPサーバが宛先ドメインのメールサーバを見つけるためは、DNSを用いる。
　・受信システム
　　POP（メールをダウンロード型）
　　IMAP（サーバ管理）

Web

HTTP（ハイパーテキストを取得するプロトコル）とTCP/IP、ハイパーテキスト、DNSを組み合わせたもの。
WebではURIの中のURLを用いる。
　　http:　スキーム
　　ホスト名、ポート番号、ユーザ情報を記述。
　　ホスト内での位置を示す、パス。

ファイアウォール・・・・送信元と宛先を見てパケットの通過の可否を判断する装置。
ネットワークセキュリティ
　　共通鍵暗号方式、公開鍵暗号方式とか

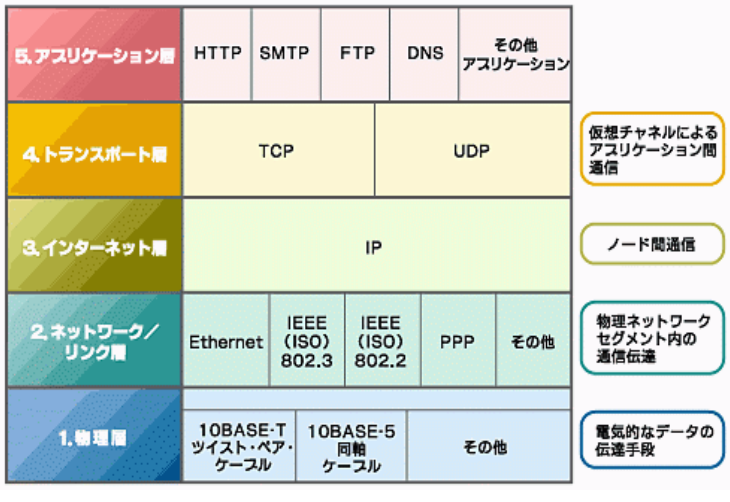
第７章

サイエンティフィックライティング

科学文書の書き方
概要、はじめに、終わりに、参考文献　の順

ワープロ

WYSIWYG式・・・・入力したまま表示できる。
　　エディタが内蔵。　wordとか
コンパイル式・・・・入力と最終的な表示が異なる。
　　好きなエディタを自分で選べる。
　　書式をあらかじめ指定し取り込めば、書式が統一される。
　　LaTeX（ラテフ）とか



[図１]インターネットの階層
加地眞也.“ルーターの仕組みを学ぼう(1)”. @IT. 2001-06-14.
http://www.atmarkit.co.jp/ait/articles/0106/14/news001.html, (参照 2013-9-30).
より引用

図の作成法

wordの描画ツールについて

ラスタ‥‥画素に分割して表現　←ガタガタ
拡張子：ポストスクリプト形式　.ps
ベクタ‥‥頂点の座標と接続だけで表現
←データ小さい、回転拡大に強い。
拡張子：拡張ポストスクリプト形式.esp
Illustrator形式　.ai

色と透明度

RGBモデル、、、赤、緑、青を256段調にして色指定
HSLモデル、、、色相、彩度、明度で色指定

マンセル色立体と同様にHSLモデルの方が直感的に欲しい色が手に入る。

透過性

透明度を百分率で調整。

2色の間の色はNewellの公式で求まる。
（どちらが上に重なるのか注意！）
カラー印刷はマゼンタ、シアン、イエロー

白黒印刷では異なる色でも、同じ明るさに変換されることがある。
（G成分が明るさに貢献、B成分の貢献は最も小さい）

図形

還元論‥‥「どれだけ複雑なイラストも、分解すれば単純な図形の集まり」
オートシェープの基本図形にあらかじめ図形が登録されている。

第９章

画像処理

GIMP、photoshopとか

カメラの仕組み

画像撮影素子は1-2cmの半導体素子。その表面上で光の強さが、数千x数千程度の画素という単位で表される。
デジタル画像はRGB3原色毎の画素値を1画素8bitにする。

データ量を削減するため、JPEG形式の圧縮をかける。
圧縮のない形式はbmp

濃度変換処理

・トーンカーブ‥‥出力画素値と入力画素値のグラフ
→ 一例、ガンマ変換

・ヒストグラム‥‥画素値の出現頻度
ヒストグラム均等化 → 明るさのバランスの自動補正

・空間フィルタリング処理
N×N画素の空間フィルタの積和演算子。
平滑化できる。
ラプラシアンフィルタ‥‥画像の鮮明化

・幾何学的変換処理　画像を歪ませる。
・物体抽出処理　切り抜き

第１０章

数式処理

Mathmatica、
（Reduca、Macsyma、Maple、Mupad）
数式を書ける。組み込み関数（expandとか）を書いて演算

数値計算

MATLAB、（無料ではscilab）
科学技術計算のための行列計算に基づく言語
ツールボックスから仕組み関数使う。低レベルなコードをかく必要はない。

第１１章

データ処理

定量的データ
比例尺度‥‥　×+=>　時間、長さ、質量、絶対温度(K)
間隔尺度‥‥　+=>　温度（摂氏、華氏）
定性的データ
順序尺度‥‥　=>　順位、アンケート
名義尺度‥‥　=　学籍番号、血液型

技術統計量

平均値（相加、相乗）
移動平均‥‥株価
加重平均‥‥重み付け
中央値　← 並び変えて、奇数個なら真ん中。
偶数個なら中央の2つの値の平均値。
最瀕値　← 最もよく出てくる値。

例）8,6,4,3,11,8,2,8
最頻値は8。
中央値は並び替えて　2,3,4,6,8,8,8,11
偶数個だから6と8の平均値7。

偏差、偏差平方和、分散(分母n)
不分散(分母n-1)、標準偏差は最後に解説。

グラフ

棒グラフ、折れ線グラフ、帯グラフ、円グラフ
散布図‥‥xy軸とってプロットしたもの。
誤差範囲をエラーバーで示す。

第１２章

ハードウェアインターフェース‥‥コネクタの形状、信号の特性、手順
ソフトウェアインターフェース‥‥ソフトウェア間のメッセージの渡し方

ヒューマンインターフェース
人とコンピュータが接する面

使いやすさ　←コンピュータの使いやすさは国際標準で「ある環境において、特定の利用者が、特定の目標を達成する際の効果、効率、満足度合い」と定義。
目標を達成する際の
　効果‥‥正確さ、完成度
　効率‥‥必要なリソース量
　満足の度合い‥‥快適さ、受容性
ターゲットを明示したときのみ有効

物理的側面‥‥入出力装置の物理的特性がマッチするか
認知的側面‥‥情報の形式や意味が認知的特性とマッチしているか

人とコンピュータの間のやりとり（インタラクション）
実行プロセス
（目標　→　行動の選択　→　入力装置）
→　処理装置
→（出力装置　→　状態の評価　→　目標確認）
評価プロセス

良いヒューマンインターフェースとは実行プロセスと評価プロセスにかかる負荷が少ないもの（直感的）

対話方式の変遷
・パッチ方式
・逐次対話方式‥‥時分割方式、ユーザ選んで数10msずつサービス提供
・直接操作方式

対話技法
・メニュー選択‥‥木構造メニュー
・空欄記入
・コマンド言語‥‥システム開発、アプリケーション開発
・直接操作‥‥WYSIWYG

入力機器
1.キーボード
　QWERTY配列、DVORAK配列、Alphabet配列
2.ポインティングデバイス
　タッチパネル、マウス
3.グラフィックユーザインターフェース（GUI）←画面直接操作、WYSIWYGできる。

アイコンは役割、機能を視覚的に伝える。
（視覚的メタファ）

ALTO　←マウスが使われた最初のCPU

未来
・実物指向インターフェース
・アバタ操作
・仮想現実　←仮想だけ
・拡張現実（AR）　←現実に仮想を重ねる

第13章
進化
メインフレーム→（ダウンサイジング）→パーソナルコンピュータ→クラウドコンピューティング
ワイヤレスアクセス（WiFi、LTE）

1.クライアント/サーバ型　←慶応の大型サーバ
2.P2P型　←個人PCで相手が分かる通信
3.クラウドコンピューティング　←どこにあるか分からない。

クラウドコンピューティング
SaaS‥‥サービスの利用
PaaS‥‥SaaSの提供者
IaaS‥‥CPU、サーバ等コンピュータのインフラを提供

データセンターの巨大化
　世界のエネルギーの1.5%消費

クラウドセントリック‥‥仮想クラウドを共有すべてを接続する。（ユビキタス）

フォトニックネットワーク技術
　将来、200THzが使用できる可能性
　光スイッチ　代表：MEMS、PLZT

ビッグデータとM2M
IPv6の普及ですべてにIPアドレスがつき、M2Mが可能になる。（スマートグリッド）
　→ビッグデータ

多くの無意味な情報をそのままストレージに溜め込むのは不可能で無駄。
　→必要なものだけにする。
　→必要なところに送る。

諸計算問題

テストに出てしまった、標準偏差、2の補数表現について解説する。
ある程度計算方法を身につけて下さい。

分散、標準偏差

最頻値、中央値については既習である。
ここでは、偏差、偏差平方和、分散(不分散)、
標準偏差(不偏標準偏差)を導出してみる。

例）2,4,6,8,10
　　総和は30なので、相加平均は6。

偏差

　　偏差はそれぞれの数について求める。
　　(10の偏差)＝10－(相加平均:6)= 4
　　同様に、
　　2→-4、4→-2、6→0、8→2
　　偏差を順に並べると　-4,-2,0,2,4

偏差平方和 S

　　S=$\sum_{i=1}^{n}(xi$*の偏差*$)^2$
　　偏差を2乗して全て足し合わせたモノ。
　　S=16+4+0+4+16=40

分散

　　分散は偏差平方和をnで割ったモノ。
　　不偏分散は　〃　　n-1　　〃　　。
　　この例では分散は　40÷5=8

標準偏差

　　分散の正の平方根を取ったモノ。
　　$\sqrt{8} = 2\sqrt{2} = 2.828\cdots$

　　不偏標準偏差は不分散の平方根。

～標準偏差～
偏差‥‥ ‥‥それぞれの相加平均との差
偏差平方和‥偏差の2乗の総和
分散‥‥‥‥‥偏差平方和をnで割った商
標準偏差‥‥‥分散の平方根

2の補数表現

二進数で、負数を足し合わせられるモノ。

例）『-6』 を補数表現したい。
　　①桁数を確認。
　　　ここでは4桁とする。
　　②正数6を二進数で表す。
　　　0110
　　③②の1を0に、0を1に変換
　　　1001
　　④③に1を足す。
　　　1010

1010 が2の補数表現での『-6』である。

確かめる　　0110
　　＋1010
　　0000　　OK!