

# 2009 年度 1 学期 情報試験について

理一 36 組シケ対の福田です。試験の前日とかいうちょー今更なアップでスンマセン。まー今年の外クラにゃパクられんから良しとしますかね。別にパクられても困らんけど。今度学校で会ったら俺の首を締め上げて構いませんですます。

というわけで今回のテストについてですが、既に HP にあげている 2006 年度のシケプリを元に、必修項目に関して[このページ](#)にあってシケプリで抜けていると思われる箇所を加筆したものを掲載しとこうかなと思います。

題して、『**シケプリ補足シケプリ(笑)**』。

補足内容の所にシケプリと教科書の該当箇所を明示してありますので、手元に情報の教科書やシケプリのプリントを置いてこのシケプリ補足シケプリ(笑)を読むことをお勧めします。決して手抜きではありません。

特に言及がない章・項目については、2006 年度シケプリの該当箇所をご覧ください。

## 《注意事項》

- 1: 試験範囲と想定している範囲は**美馬の授業とは無関係に**上述のページに基づいています。共通試験問題のみの出題なので、常識的にはこの範囲からしか出ないはず。
- 2: **必修科目についての漏れのみ載せています**。理系文系を問わず、**選択問題範囲の中でシケプリに入っていない内容については全く言及していません**。(シケプリに載ってる項目の中で、必修ではなく選択問題範囲になっているものについては以下で示しています。) みなさんが理系・文系問題のどちらを取るかわからない為こうしました。すみません。

## 2.2.2 数の表現—記号と解釈の規則体系

(教科書 P.19~,シケプリ P.6 の「◆日本語文字コード」の次)

ここでは、記号の規則体系の違いが処理体系にどう影響するのかを見るために、数の表現について取り上げる。

(例) アラビア数字とローマ数字等との比較

現在ではアラビア数字“0”で表現される、“無”を表す記号は以前にも存在。

インド人の功績 ①数字の“0”の発見

②“位取り表記法”による算術演算の発見

例えば  $1963+41$  を筆算で行う場合、位を縦に揃えて書き下の位から順に加算を行っていく。同様の操作を下記の対応表に則ってローマ数字で行おうとすると、特殊な場合を除くと非常に不便であることに気付くだろう。これはローマ数字に 0 に対応する記号がないためである。

アラビア数字とローマ数字の対応表

1	2	3	4	5	6	7	8	9	10	20	30
I	II	III	IV	V	VI	VII	VIII	IX	X	XX	XXX

11	40	50	60	90	100	110	400	500	600	900	1000	1100
XI	XL	L	LX	XC	C	CX	CD	D	DC	CM	M	MC

アラビア数字の利点…0～9の10種類の記号のどれか1つが必ず各桁に対応している。即ち、同じ記号でも場所によってその意味が異なる点において、ローマ数字より有用。

→ “0”の発見により、人間の思考様式ひいては経済や文化にまで影響。ただし、2030→1203000のようにアラビア数字表記法は改ざんされやすい。一方でローマ数字表記法や漢数字表記法は改ざんされにくく、この点でアラビア数字より有益。

	利点	不利益点
アラビア数字	算術が容易	改ざんされやすい
ローマ数字	改ざん防止に優れる	算術が困難

この例のように、同一対象を表現する上で複数の方法が考えられる場合、それらの情報表現間のトレードオフ（ある側面を優先すると別の側面に問題が生じてしまう関係）を考慮しなければならない。

コンピュータでは0と1という2種類の記号のみを用いて数字を表現するビット列が使われている。これは2進法でもって表され、一般にnビットで $2^n - 1$ までの数値を表現できる。

《この項目はおしまい》

★シケプリ P.7～9にある、2.3.2 量子化 から 2.3.4 周期関数への分解 の件くだけは理系選択問題の試験範囲です。（範囲表のWEB ページ参照）

## 2.4.1 デジタル符号化の事例

(教科書 P.27～,シケプリ P.9 の最下部から)

### ●2進符号 …10進数を2進数に変換したもの

※例 (順に 10進数→2進数表現とし、) 1→0001, 2→0010, 3→0011, 10→1010, …

ハミング距離…ある2つの2進符号において、対応する桁の0と1が異なる個数

2進数符号における数値の差とハミング距離は、10進数で考えた場合と異なり一致しない。

※例 1と2…2進数で0001と0010なのでハミング距離は2

7と8…2進数で0111と1000なのでハミング距離は4 など。

## 3.2.2 プロトコルの (b)アプリケーションとプロトコル

(教科書 P.46～,シケプリ P.12 の最下部から。図は教科書 P.27 の上図参照。)

以下では、プロトコルの例として WWW を参照するときを例にとる。一般に、

クライアント…情報を請求する側

サーバ…要求に応じて適切な情報を送り出す側

であり、今回の場合は前者がウェブブラウザ、後者がウェブサーバである。両者間の通信は、HTTP という規約で規定されている (逆に言えば、HTTP に則って通信できるならこれら以外のアプリケーションでもよい。)

HTTP は要求と応答で構成される単純なプロトコルで、代表的には以下の通信がある。

- (1)クライアントからサーバに目的文書の URL を送信する。
- (2)サーバがその文書を返す

要求に対する様々な事態に備えた応答が HTTP には定義されている。

ちなみにウェブのための HTTP、電子メール送信には SMTP のように、応用目的に応じて色んなプロトコルが作られている。

《この項目はおしまい》

★シケプリ P.14 にある、3.3 情報ネットワークの枠組み の件は 2009/07/25 現在、必修学習項目に入っておりません。

★シケプリ P.15 にある、「◆プロトコル」の項目は理系選択問題の試験範囲です。

★シケプリ P.17 にある「◆集合モデル」は 2009/07/25 現在、必修学習項目に入っておりません。

★シケプリ P.19 にある「◆関係モデル」は 2009/07/25 現在、必修学習項目に入っておりません。

★シケプリ P.24～25 にある「◆プログラム言語処理系」は 2009/07/25 現在、必修学習項目に入っておりません。

★シケプリ P.32～35 の上段にある、「◆機械語レベルのプログラム例」の項目は理系選択問題の試験範囲です。

★シケプリ P.36～38 にある、「◆n 入力 1 出力の論理関数（教科書では 7.2.1 真理値表と論理関数に該当）」の項目は理系選択問題の試験範囲です。また、教科書 P.159～160 にある証明は試験範囲外です。

★シケプリ P.39～41 の上段にある、「◆MIL 表記法」の項目は理系選択問題の試験範囲です。

★シケプリ P.41 の下段～42 にある、「【加算器】」の項目は 2009/07/25 現在、必修学習項目に入っておりません。

★シケプリ P.43 の上段にある、「【見えにくい情報システム】」の項目は 2009/07/25 現在、必修学習項目に入っておりません。

★シケプリ P.46 の中段にある、「【こんな経験ないですか】（教科書 P.211～213 の 9.1 世の中、かくも使いにくい物ばかり？ に該当）」の項目は 2009/07/25 現在、必修学習項目に入っておりません。

★シケプリ P.46 の下段～48 にある、「【インターフェースの定義と技能】」と「【インターフェースの二重接面性】」の項目は文系選択問題の試験範囲です。ただし、以下でインターフェース絡みのシケプリには未掲載の項目を補足しますし、以下の項目に出てくる言葉の中に、教科書 P.211～218 上段にある範囲外の項目で説明されているものもあるので、この範囲のシケプリと教科書は一読したほうがいいです。

### **9.3.2 技術的側面からみたインターフェースデザイン – インターフェースの種類と構成要素**

（教科 P.218～、シケプリ P.48 のあと）

【の前に！インターフェースとは…】

原義は二者の「界面」「接面」を意味する言葉。つまり、2つの異なる存在（今回はコンピュータを含む人工物とそのユーザとの間）の境界面のこと。券売機のコイン投入口等。

(a)入力デバイス…実行の淵を越える際に相対するシステム。キーボード、マウス等  
ポインティングデバイス

└直接入力型デバイス（タッチスクリーンなど）…表示画面上で直接位置を指定する

└間接入力型デバイス（マウスなど）…机上で間接的な操作をする

└絶対的な座標値を入力するもの（デジタイザなど）

└相対的な移動量を入力するもの（マウスなど）

└方向のみを入力するもの（ジョイスティックなど）

(b)出力デバイス…評価の淵を超える際に相対するシステム。ディスプレイ、スピーカ等。

**GUI**…ユーザに対する情報表示にグラフィックなオブジェクトを多用し、ポインティングデバイスを用いて操作すること。GUIの基本技術はA.Kayが提唱しワークステーションAltoを開発、その後Macのインターフェースとして採用されWindowsなどの同様なGUIが開発された。

初心者ユーザにも使いやすいようにデスクトップメタファ（※1）を採用。直接操作（※2）という考え方が背後にある。

別名WINPシステム。←ウインドウ・アイコン・メニュー・ポインティングデバイス の頭文字。

これを実現するシステムが（マルチ）ウインドウ・システム。

※1 **デスクトップメタファ**…机上に書類を広げる感覚で操作できるように、即ち机上の書類や文房具との類推によりコンピュータ内での目的の操作を達成できるように現実世界を模したインターフェース。早い話、現在のWindowsやMacのデスクトップみたいな感じ。

※2 **直接操作**…ユーザと環境との間に確立された自然な関係を人工物の設計に取り込み、その装置や表示を見れば、どのように実行可能かが即座にわかるようになること。ギブソンのアフォーダンスの概念をノーマンが拡張して提案した。

**CUI**…GUIの対置概念。ユーザに対する情報表示に文字を用い、すべての操作をキーボードで行うインターフェース。

《この項目はおしまい》

★シケプリ P.49～50 の中下段にある、「◆技術と社会」、「◆情報技術による技術上の変化（教科書 P.233～の 10.2.1 技術上の変化）に該当」、の項目は文系選択問題の試験範囲です。

## 10.3.2 フライバシーとセキュリティ

(教科書 P.243～, シケプリ P.52 の最下部から)

コンピュータは、以前には全く不可能であった個人に関する多くの詳細な情報を電子媒体の形で収集・記憶することを可能とした。

この情報収集の規模の拡大は、ネットワーク技術の発展にもよって情報交換の規模をも拡大させ、個人情報や一度コンピュータ上に記録されれば別の媒体への転送は容易である。これが以下の議論を生み出した。

**プライバシーの議論**…記録された個人情報は、売買や無償配布、盗難されることなく保護されなければならない。

**セキュリティの議論**…個人情報や帰郷・国家の機密情報の安全を如何に確保するか。

### (a) プライバシー

個人情報を欲しがるとはそれがよりよい判断に役立つと考えるが、誤った使い方をされると個人に被害が及ぶ危険性がある。これを防ぐ為にプライバシーの議論がある。また、すべての個人の行動が記録・公開されると自由が侵食される。よって、プライバシーの保護は民主主義を支える自由のために必要である。

### (b) 個人情報保護法 (2003年5月公布、2005年4月施行)

└官民を通じた基本法 ※官＝公的部門 (国の行政機関・地方公共団体・独立行政法人)

└民間事業者に対する個人情報の取り扱いのルール

├ (1)利用・取得に関するルール (2)適正・安全な管理に関するルール

├ (3)第三者提供に関するルール (4)開示などに応じるルール

└個人情報取扱業者に対する個人データの開示・訂正・利用停止の要求の権利の保障

※(1)～(4)についての詳細は教科書 P.245 の表参照。

目的：個人情報の有用性に配慮しつつ個人の権利利益を保護する。

→各企業・公的部門におけるプライバシー概念が浸透。

個人情報の流出・漏洩は、企業では「会社の命取り」

公的部門では「国民の信頼の失墜」という意識が高まる。

(世界では・・・) OECD 加盟国の多くが個人情報保護に関する法律を有する。

… “プライバシー保護と個人データの国際流通についてのガイドライン” (OECD 理事会勧告)

### (c) セキュリティ

└①機密性(Confidentiality)：認可されたもののみ情報アクセスを許すこと

└②完全性(Integrity)：情報が正確で完全であること

└③使用可能性(Availability)：必要時に必要な情報資源にアクセス可能なこと

①の侵害→情報漏洩 ②の侵害→改ざん ③の侵害→使用妨害

情報セキュリティ…情報システムにおける安全性の確保

- 対策：(1)問題発生を防ぐ対策 (2)問題発生時を想定した対策  
(3)問題発生時の対策 (4)問題の再発防止の対策

### ●機密性の管理に関して

不正アクセス防止法（1999年8月公布、2000年2月施行）

目的：不正アクセスの禁止とこれに対する罰則・再発防止のための措置等を定めることで、高度情報通信社会の健全な発展に寄与する

- ・不正アクセス（他人のアカウントや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）
- ・その助長行為（他人のアカウントやパスワードの第三者への提供）

を禁止。

- ・アクセス管理者＝情報システムの管理者による不正アクセス行為の防御措置実施の努力
- ・以上の措置に対する都道府県公安委員会による援助
- ・違反者に対する罰則

を制定。

### (d)セキュリティ確保の技術的枠組み

#### 個人認証技術

…情報システムの管理者が、アクセス者を利用権者（システム利用が許諾された者）であるかを識別する技術。不正アクセス防止法での定義は“識別符号”。

（例）ID、パスワード、生態固有特徴による認証（指紋、声紋など）、バイオメトリクス

#### 暗号化技術

…元のデータを解読不可なデータに変換する技術。元のデータに戻すのは復号。

（例）ネット通販での、クレジットカード番号の自動暗号化送信

#### 公開鍵暗号方式と PKI

前者…3.2.3（教科書 P.48、シケプリ P.13）を参照。これを社会全体で成立させるには、各人に固有の正しい公開鍵を配布する機関が必要。

後者…前者を利用したセキュリティインフラストラクチャのこと。上述の機関もこの1つ。

認証局…各人に固有の正しい公開鍵を配布し、各人の身分証明書を保管・発行し他人の要求に応じてその証明書（＝公開鍵）を提供する機関。

#### 電子署名

※詳しくは 3.2.3-(b) を参照（必修範囲外）。

…特定の文書の発行人を保証するために用いる。購入・契約時のなりすましを防ぎ、本人確認を可能にする。電子署名・電子決裁は紙の決裁文書の回覧・押印より迅速。

《この項目はおしまい》

★シケプリ P.53～最後にある、「【情報技術論】」の項目は文系選択問題の試験範囲です。

シケプリ補足シケプリ(笑)はこれでおしまい。**お疲れしたー！**