2011 年夏学期情報共通問題

共通問題 1

1-1

以下の各小問に解答せよ。まず、与えられている例文に含まれる誤りの箇所を簡潔に指摘せよ。次に、用語から二つ以上用いて、主題に関して説明する文章を作成せよ。説明の文章の量は 50～150 字を目安とする。

(1)

（主題）インターネットを通じて電子メールが届く仕組み

（例文）送信者が電子メールを書く時に用いたコンピュータと受信者がメールを読む時に用いたコンピュータが、~~通信ケーブルで直接に~~"インターネットを介して"に結ばれている必要がある。

（用語）DNS、パケット、ルータ

解答①：メールの内容を送信側のマシンで 1 つ 1 つのデータ量が少ない複数のパケット分割してから、インターネットに向けて送信する。その情報は幾つものルーターを介してやがて受信側のマシンに届く。受信側は送られてきたパケットを順番通りに並べ替えてメールの内容を読み取る。

解答②：主に文字で構成されるメールの内容を符号化したデータを、送信側は DNS サーバーに問い合わせて名前解決をしてドメイン名に対応する送信先の IP アドレスを入手してから、インターネットに送信する。このパケットは複数のルーターを介して受信側に送られ、受信側はパケットを順番通りに並べ替えてメールの内容を得る。

コメント：通常は①を、がっつり書きたい人は②を参考に。

(2)

（主題）公開鍵暗号方式

（例文）公開鍵暗号方式でメッセージを送る際は、~~送信者と~~受信者が~~お互いに~~に鍵を公開し、公開された鍵を用いて暗号化と~~復号~~を行う。

（用語）公開鍵、共通鍵、秘密鍵、平文

解答：公開鍵暗号方式では受信側が秘密鍵から生成した公開鍵を、送信側が受け取って平文を暗号化する。暗号文を受信側が受け取ったら、秘密鍵を用いて暗号文から復号して平文を得る。公開鍵から秘密鍵を生成することは事実上不可能なので途中の通信を傍受されても、第三者が平文を得ることはできない。

コメント：公開暗号鍵は（共通鍵暗号とは違い）途中の通信を傍受されても平文を第 3 者が得ることはできないという点は、おそらく書かないと点が来ない。平文とは暗号化する前の文のこと。

(3)

（主題）インターネットと通信の所要時間

（例文）自宅のインターネット設備を整えた記念に 1 メガバイトのファイルをインターネットからダウンロードした際には α 秒かかつた。従つて今後 10 メガバイトのファイルをダウンロードする際には αX10 秒より長くかかることはないと結論づけられる~~る~~"無い"。

（用語）サーバ、DNS、パケット、ルータ

解答：インターネットではパケットがどのルーターを通って送信側から受信側に到着するかという経路制御をすることができないため、基本的に送るたびに経路は違う。よって例文の状況で 10MB のデータをダウンロードした時に α×10 秒以上かかることは十分にありえる。

コメント：DNS、サーバーを入れるのはちょっとむずかしい（あまりこの 2 つの用語は主題とあまり関係がない）。

(4)

（主題）ドメイン名と地域や組織

（例文）インターネット上で使われるホスト名やドメイン名とは、完全に仮想的な名前であり、接続者の国、地域、所属組織などとの対応関係は~~一切ない~~"ある程度ある"。

（用語）IP アドレス、DNS、ドメイン名

解答：ドメイン名は IP アドレスと 1 対 1 で対応するもので、数字の羅列である IP アドレスよりも人間が覚えやすくするために付けられている。ドメイン名は階層構造をなしており、この階層に従って区切ったある一定の範囲を各 DNS サーバーが担当しており、DNS サーバーの処理を分散させている。

コメント：地域の話では「.tv（ツバルの国別コード）」は世界中の企業で使われていますし、所属組織の話では個人でも「.com（企業）」を取得することが出来るので、完全にあるというのは減点の可能性があります。ドメイン名とホスト名は細かい定義の違いがありますが、同じものと思って構いません。後半はちょっと難しい内容。

1-2

以下の空欄にもっともよくあてはまる言葉を、それぞれの選択肢から選び、記号で答えよ。

（ア）とはウェブサーバとウェブブラウザ間の通信を規定する規約である。このような規約を定めることによって、ウェブブラウザ以外の（イ）あってもウェブサーバと通信をして（ウ）することができる。チケット予約システムなどでは、ウェブサーバの背後にチケット予約に関する具体的な処理を行う（エ）や公演情報などを記録 した（オ）が存在する。

（ア）の選択肢 (a)HTML (b)HTTP (c)SMTP (d)URL

（イ）の選択肢 (a)CUI (b)LAN (c)プログラム (d)電子メールソフト

（ウ）の選択肢 (a)メールの受信　(b)決済を完了 (c)モデル化 (d)文書を収集

（エ）の選択肢 (a)インターネット (b)プログラム (c)階層構造 (d)組み合わせ回路

（オ）の選択肢 (a)DNS (b)アルゴリズム (c)デ ータベース (d)集合モデル

（ア）b （イ）c （ウ）d （エ）b （オ）c

（ア）HTTP の P は protocol＝規約

（イ）、（ウ）電子メールソフト＆メールの受信 としたくなるが WEB とは通常 WEB ページのことのみを指して、メールのやりとりをするのはウェブサーバーではなく、メールサーバーである。また（ア）の答えである HTTP はメールの送受信用のものではない（メールは SMTP 等）。よって前の文脈から答えは決まる。

（エ）処理を行うのはプログラム

（オ）情報を記録＝データベース

共通問題 2

4 つ の政党の得票数が配列 votes によって与えられているとする。これらの政党に 8 つの議席を割り当てるときの各党の議席数を配列 seats に求める以下の手順について答えよ.

```
c ← 8
while c > O do
        「i に votes 中 の最大値の添え字を代入する」
        seats_i ← seats_i + 1
        votes_i ← votes_i × seats_i ÷ (seats_i + 1)
        c ← c-1  ★
done
```

ただし手順開始前の配列 seats と 配列 votes は 以下のようであったとする。

配列 seats

添字	要素値
1	0
2	0
3	0
4	0

配列 votes

1	102000
2	81000
3	30000
4	20000

(1)

「i に votes 中の最大値の添え字を代入する」一連の手順を、上の記法にならって書け。ただし、 votes 中の最大値の添え字(i とする)とは、i と異なる votes の全ての添え字 j に対して $votes_i \geqq votes_j$ となっているようなものである。ここでは,$votes_i = vote_j$ の場合はないと仮定してよい。また,条件付き処理は

```
if 条件
then 条件が成立した場合に行なう処理
{ else 条件が成立しない場合に行なう処理 }
endif
```

のように書くものとする（{ }の部分はなくてもよい。）

解答：

```
j=1
i=1
while j<=4 do
        if vote_i   < vote_j
                then i=j
        end if
        j ← j+1
done
```

コメント：j はただ 1～4 まで変化するだけのカウンタで、i は始めは 1 で最終的に一番大きい配列 votes の中で一番大きいものの添字が入ります。$vote_i$ と $vote_j$ を比較して、$vote_i$ のほうが大きければそのまま、$vote_j$ の方が大きければ i に j を代入します。

（2）

★の処理を終えた時点での c が 7、4、0 の時の配列 votes の中身をそれぞれ書け。

（3）

各党の議席数を求める手順全体が終了した時点での配列 seats の中身を書け。

解説：とりあえず★が終わった時の c の値が 7 から 0 までの時の各配列の状態をすべて書きます。

		start	c=7	6	5	4	3	2	1	0
votes	1	102000	**51000**	51000	**34000**	34000	**25500**	25500	25500	**20400**
	2	81000	81000	**40500**	45000	**27000**	27000	27000	**20250**	20250
	3	30000	30000	30000	30000	30000	30000	**15000**	15000	15000
	4	20000	20000	20000	20000	20000	20000	20000	20000	20000
seats	1	0	**1**	1	**2**	2	**3**	3	3	**4**
	2	0	0	**1**	1	**2**	2	2	**3**	3
	3	0	0	0	0	0	0	**1**	1	1
	4	0	0	0	0	0	0	0	0	0

解答：

(2)

	c=7	C=4	c=0
1	51000	34000	20400
2	81000	27000	20250
3	30000	30000	15000
4	20000	20000	20000

(3)

seats	
1	4
2	3
3	1
4	0

コメント：ドント式である。ということが見抜けないと辛い。見抜けなかった場合でも 1 つずつ丁寧に順をおってどうにかしよう。

共通問題 3

以下の問題 A および B のうちいずれか一方を選択し、答えよ。

問題 A

以下の中問 A-1、A-2 に答えよ。

A-1

ユーザインタフェースについて書かれた次の文章を読み、[ア]～[キ]に適切な言葉を埋めなさい。また[ク]については、適切な文を下の選択肢から一つだけ選び、その番号を答えなさい。

CUI(Character User hterface)は,キーボードを用いて入力を行い、文字によって出力を行うタイプのユーザインタフェースである。情報基盤センターのコンピュータ端末(iMac)で、ターミナルを用いて CUI による作業を行う場合、

g123456$ ←ターミナル

などという形で表示されている[ア]に続いて、ユーザが[イ]を入力することになる。CUI と対比されるユーザインターフェイスとして[ウ]がある。これは、ユーザへの情報の表示に、ウィンドウ、[エ]、メニューなどのグラフィックなオブジェクトを多用し、マウスなどの[オ]を用いてそれらのオブジェクトをユーザが操作することで、ファイル操作な どの基本操作の多くを実現しているユーザインタフェースである。ウインドウ、[エ]、メニュー、[オ]の頭文字をとって WIMP システムと呼ぶこともある。具体的な入力デバイスとして、表示画面を直接指で触って入力する[カ]の利用が最近増えている。また、[ウ]の背景にある考え方が、「その装置あるいは表示を見れば、どのように実行可能かが即座に分かるようになる」という[キ]である。さらに、[ウ]の画面において、キーボード操作に慣れているユーザーにも、慣れていないユーザーにも操作効率の良いインターフェースとするための留意点として[ク]が挙げられる。

[ク]の選択肢

(a) キーボードから入力させる項目数を最少にして，できる限り項目の一覧からマウスで選択させるようにすること

(b) 使用頻度の高い操作は，マウスをダブルクリックして実行できるようにすること

(c) できる限り多くの操作に対して，マウスとキーボードの両方のインタフェースを用意すること

(d) 入力情報の形式にとらわれずに，必須項目など重要なものは 1 か所に集めて配置し，入力漏れがないようにすること

解答：

[ア]プロンプト [イ]コマンド　[ウ]GUI　[エ]アイコン　[オ]ポインティングデバイス（ポインター）

[カ]タッチスクリーン（タッチパネル）　[キ]アフォーダンス　[ク](c)

コメント：[エ]、[オ] 後ろの WIMP システムというのがヒントになります。よって I:アイコン、P:ポインティングデバイスとなります。[ク]は A なユーザー、B のユーザー両方にとあるので、答えは両方のインターフェイスに対応することです。って教科書丸暗記していないと解けないだろこれ。さすが A 問題。

A-2

最近、ソニーの関連会社が運営するネットワークサービスに関して、複数の情報流出が問題となった、以下は，2011 年 5 月 3 日付の日本経済新聞からの引用である。

「ソニーまた情報流出か 別の米子会社、カード１万件超 」

ソニーのインターネット配信サービスで米ゲーム子会社から個人情報流出の恐れが出ている問題で、別の米子会社もハッカー攻撃を受け、全世界で 1 万 2700 件余りのクレジットカード情報が引き出された可能性のあることが 2 日、新たにわかった。ソニーが米国時間 2 日午後（日本時間 3 日未明）に発表する。

攻撃を受けたのは、米国カリフォルニア州にあるゲーム配信子会社ソニー・オンライン・エンタテインメント。関係者によると、米国時間 1 日午後にシステムの異常を発見。世界で 1 万 2700 件余りのカード情報が流出した可能性があることがわかった。ソニーは 4 月に判明した 7700 万件の個人情報流出の恐れについて調査しているさなかに、別の米子会社でもハッカーの攻撃を防げなかった可能性がある。

今回判明した 1 万 2700 件のうち約 4300 件が日本国内のカード情報という。流出した恐れのあるカード情報は 2007 年のもので多くが失効しているとみられるが一部は有効期限内のカード情報もあるもようだ。

ソニーは 26 日に米ゲーム子会社が運営するプレイステーション・ネットワーク（ＰＳＮ）のサーバーが攻撃を受けたと発表。会員 7700 万件の氏名や住所、生年月日、メールアドレス、暗号化後のパスワードなどが漏洩した可能性が高いとしていた。

(1)

この記事からわかるように、これらの情報流出には、(A) セキュリティの問題ならびに(B) プライバシーの問題で、それぞれに共通点がみられる．(A) と(B) の問題を合計 5 行(150 文字) 以内でまとめよ。

この問題では、問題が起きたことを想定した対策がなされていないために、再び情報漏洩という同じ過ちを繰り返してしまったことも問題である。また、サーバーに保管されている個人情報のデータが一部暗号化されずに保管というずさんな管理体制出会った子会社を放置していたソニー本社にも責任はある。

コメント：まず文章の情報が少なくて、ここから情報を引き出すのは難しいかな？ だがその分、本文に書いていることを 1 つ 1 つかみ砕けば答えが出るということかな？

(A)セキュリティー面での問題：セキュリティーには 4 つの対策があります（教科書 P244）。

(1)問題が発生しないようにするための対策

(2)問題が発生したときのことを想定した対策

(3)問題が発生したときの対策

(4)問題が再発しないようにする対策

(1)内容が広すぎるので触れないとして、今回は(2)、(4)で引っかかります。(2)については、本文最後の行からパスワードは暗号化されていたが、その他の個人情報は暗号化されていなかった事が分かります（ちょっと読みづらいと思うけど）。暗号化されていれば、流出しても平文を得られないので、被害は小さくなります。

一番大きいのは(4)についてで、別の子会社がハッキングを受けていたが、その時に適切な対処ができなくてまた問題が再発してしまったのが最大の問題です。

(B)プライバシーの問題：プライバシーについてのポイント 4 つ（P245）

(1)利用・取得に関するルール：勝手に個人情報を集めてはいけない

(2)適正・安全な管理に関するルール：漏洩しないように監視

(3)第 3 者への提供に関するルール：事前に許可を得た範囲でのみ可

(4)開示に応じるルール：個人からの請求に応じる義務

今回の問題は(2)です。ソニー本社はその子会社の個人情報の管理が適正かを監視する義務がありました。

(2)

このような情報流出が日本国内において発生した場合に、(1) で回答した問題に直接関連する法律ならびにその対象者の組を 2 つ以上挙げよ。さらに、それぞれの組ごとに、法律に抵触したり、法律で規定された義務を怠ったとされうる対象者の行為を 3 行(100 文字) 以内で説明せよ。

公的部門（国の行政機関、地方自治体、独立行政法人）は保持している国民の個人情報を流出した場合、それを防ぐ対

策を十分に撮っていなかったとして、行政機関個人情報保護法に反する。

民間の事業者は保持している国民の個人情報を流出した場合、それを防ぐ対策を十分に撮っていなかったとして、個人情報保護法に反する。

コメント：何を書いて欲しいのかという意図がよくわからない。ポイントは個人情報保護法の対象者は民間の事業者のみであって、行政機関については行政機関個人情報保護法によって規定されている。

問題 B

通常のサイコロは 6 面体であるが、世の中には 8、10、12、100 など様々な面数のサイコロが存在する。ここでは 1 から 8 までが記された面(それを面 1 から面 とする) を持つ 8 面体のサイコロを考えてみよう。

(1)サイコロを一回振ると面 1 から面 8 のどれかが上になる。まず、各面が等確率で上になる場合を考える。

(1a)面 1 から面 8 のどの面が上になるかについての平均情報量を求めよ。

(1b)サイコロを振った際に面 1 が上となる場合、面 2 が上となる場合、……、面 8 が上となる場合をそれぞれ表 1 のように符号化する．ここで"."は文字数に含める。なお"."は区切り文字としての役割を果たす。例えば I.II. の"."を省略して III と符号化すると II.I.を符号化したものと区別がつかない。

表 1								
面	1	2	3	4	5	6	7	8
符号	I.	II.	III.	IV.	V.	VI.	VII.	VIII.

サイコロを振った結果をこの符号化を用いて伝える場合の、平均符号長を求めよ。平均符号長とは、各場合を表す符号の文字数の、各場合の確率による期待値である。

(1c)A，B 二つの文字のみを使う符号を考える(A を 0 ，B を 1 と解釈すれば 2 進符号と同等であるが、0 と 1 は他の表記と紛らわしいためここでは A、B を用いる) 。(1b) の符号を、I を B、"."を AB、V を AAB と更に符号化することにする。それにより、サイコロを振った結果の各場合がどのように符号化されるか、表 2 の空いている部分を埋めよ。さらに平均符号長を求めよ。

表 2								
面	1	2	3	4	5	6	7	8
符号	BAB							

(1d)面 1 から面 8 が上となる場合のそれぞれを A、B 二つの文字のみ用いて直接符号化する方法を考える。平均符号長が(1b) よりも短い符号化を一つ(短いほど良い) 考案し、その平均符号長を平均情報量と比較せよ。

(2) ある歪んだ形のサイコロを考える．そのサイコロを振ると，面 1 から面 8 が，それぞれ 2^{-i} (1<=i<=7)、2^{-7}(i = 8) の確率で上になるとする．

(2a)面 1 から面 8 のどの面が上になるかについての平均情報量を求めよ。

(2b)(2a)で求めた平均情報量と(1a)で求めた平均情報量を比較し、それらの大小について議論せよ。

(2c)このサイコロに関しても、面 1 から面 8 が上となる場合のそれぞれを A、B 二つの文字のみ用いて符号化したい。そのような方法のなかで、できる限り平均符号長が短い符号化を一つ示せ。

(1a)

情報量は log_2(事前のパターン/事後のパターン)で求められるので、今回は log(8/1)=3

(1b)

1～8 までの各々の出る確率は全て 1/8 また 1～8 の符号長はそれぞれ 2、3、4、3、2、3、4、5 なので、平均情報長は 2*1/8+3*1/8+4*1/8+3*1/8+2*1/8+3*1/8+4*1/8+5*1/8=13/4=3.25

となる。

コメント：平均情報長(3.25)>平均情報量(3)よりこの符号化はちょっとだけ効率が悪い。

(1c)

面	1	2	3	4	5	6	7	8
符号	BAB	BBAB	BBBAB	BAABAB	AABAB	AABBAB	AABBBAB	AABBBBAB
符号長	3	4	5	6	5	6	7	8

平均符号長：3*1/8+4*1/8+5*1/8+6*1/8+5*1/8+6*1/8+7*1/8+8*1/8=11/2=5.5

(1d)

例

面	1	2	3	4	5	6	7	8
符号	AAA	AAB	ABA	ABB	BAA	BBA	BAB	BBB

平均符号長は

1*1/8+1*1/8+1*1/8+1*1/8+1*1/8+1*1/8+1*1/8+1*1/8=3

平均情報量＝平均情報長なので、この符号化の方式が一番符号長が短くなる方式の内の 1 つになる。

コメント：符号 2～8 はどれとどれを対応させても良い。

(2)(2a)

面	1	2	3	4	5	6	7	8
確率	1/2	1/4	1/8	1/16	1/32	1/64	1/128	1/128
情報量	1	2	3	4	5	6	7	7

平均情報量は

1*1/2+2*1/4+3*1/8+4*1/16+5*1/32+6*1/64+7*1/128+8*1/128=254/128

コメント：各々の面の出る確率が等しくないので、各面の出る情報量はそれぞれ違う。

(2b)

(1)の情報量＞(2)の情報量となる。つまり各々の事象の確率が等しい、つまりどれが来るのかがあたりを付けることもできない状態が最も情報量が高いということになる。

コメント：(1)>(2) を書くことが最低条件、あとは考察を書けばいいのかな？

(2c)

面	1	2	3	4	5	6	7	8
符号	B	AB	AAB	AAAB	AAAAB	AAAAAB	AAAAAAB	AAAAAAAB

平均符号長は

1*1/2+2*1/4+3*1/8+4*1/16+5*1/32+6*1/64+7*1/128+8*1/128=255/128

コメント：確率の大きいものにできる限り短い符号を割り当て、レアなものには長い符号を割り当てるのがポイント。

2012_s1_28 eri_A