2015年7月8日

情報セキュリティ大学院大学
情報セキュリティ研究科（博士前期課程）情報セキュリティ専攻
2016年度特待生選抜試験問題

1次選考（筆記試験）

10:00～11:30

(1)
- Ⅰ　情報数学A
- Ⅱ　情報数学B
- Ⅲ　通信ネットワーク
- Ⅳ　情報システム
- Ⅴ　ソフトウェア

(2)
- 小論文

【注意事項】

1. 指示があるまで、この問題冊子を開いてはならない。
2. この問題冊子の本文は全部で12ページある。落丁、乱丁があれば申し出ること。
3. (1)、(2)のいずれかを選択し、答案を作成せよ。ただし、技術系の研究テーマを希望する受験者は(1)を選択すること。
4. (1)を選択した受験者は、上記Ⅰ～Ⅴの5項目から2項目を選択し、解答すること。5項目中どの2項目を選択してもよい。
   (2)を選択した受験者は、与えられた課題について、2000字以上3000字以内の小論文を作成すること。
5. 解答用紙は計3枚（(1)用解答用紙2枚、(2)用解答用紙1枚）配布される。
   (1)を選択した受験者は、「筆記試験(1)用解答用紙」を、選択した項目ごとに1枚ずつ使用すること。必要があれば裏面を使用してよい。筆記試験(2)用解答用紙には何も記入しないこと。
   (2)を選択した受験者は、「筆記試験(2)用解答用紙」1枚のみを使用すること。筆記試験(1)用解答用紙には何も記入しないこと。
   同一受験者が(1)、(2)両方に解答した場合、いずれの解答用紙も無効となるので注意すること。
6. 解答用紙の指定欄に、選択した項目名（「ローマ数字＋科目名」※(1)を選択した受験者）、受験番号（全受験者）を必ず記入すること。解答用紙の回収前に、これらを記入したかを必ず確認すること。
7. 問題冊子、解答用紙、計算・下書き用紙は持ち帰ってはならない。

I情報数学A

(問1) $f(x)$ が $[a,b]$ で2階微分可能とする。

$$f(b) \;=\; f(a)+f'(a)(b-a)+\frac{f^{(2)}(c)}{2!}(b-a)^2$$

を満たす c (ただし $a<c<b$) が存在することを証明せよ。

(問2) 次の関数の0におけるテイラー展開 (マクローリン展開) を求めよ。

$e^x \sin x$

Ⅱ 情報数学B

正の整数nについて、対角成分がすべてnであり、その他の成分がすべて-1であるn次正方行列をAとする:

$$A = \begin{pmatrix} n & -1 & \cdots & -1 \\ -1 & n & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \cdots & -1 & n \end{pmatrix}.$$

Aのすべての固有値と固有ベクトルを求めよ。

III 通信ネットワーク

複数の通信端末がイーサネットや無線 LAN を共用している場合、フレーム送信の競合(以下、競合と略す)が行われ、送信フレームが衝突することがある。この衝突の確率を小さくするため、メディアアクセス制御 MAC(Media Access Control)が用いられる。この MAC に関連する以下の問 1 から問 3 に答えよ。
なお、通信端末間の時刻は同期しており、各競合において送信タイミングの値は 0、1、2、・・・と整数で与えられるものとする。

(問 1)MAC では、イーサネットか無線 LAN かを問わず、バイナリバックオフと呼ばれるアルゴリズムを用いてフレームの送信タイミングが選択されることが多い。このバイナリバックオフを用いた MAC の概要を説明せよ。

(問 2)イーサネットでは CSMA/CD(Carrier Sense Multiple Access/Collision Detection)というMACを用いている。CSMA/CD では、送信フレームの衝突が発生した場合、フレーム送信は行われず、次回の競合では全ての通信端末がバイナリバックオフで送信タイミングを選択する。いま、端末 A と端末 B の 2 通信端末がイーサネット上で同時に通信を開始したため、最初の競合で衝突が発生したものとする。2 回目の競合で初めていずれかの通信端末が送信できる確率は 1/2 である。3 回目の競合で初めていずれかの通信端末が送信できる確率を求めよ。

(問 3)無線 LAN では CSMA/CA(Carrier Sense Multiple Access/Collision Avoidance)という MAC を用いている。CSMA/CA では、フレームを送信できた通信端末は次回の競合ではバイナリバックオフで送信タイミングを選択し、フレームを送信できなかった通信端末は、自身の送信タイミングの値から送信できた通信端末の送信タイミングの値を差し引いた値を次回の送信タイミング(持越しタイミングと呼ぶ)に設定する。いま、端末 A と端末 B の 2 端末が無線 LAN 上で通信中で、ある競合で端末 B が送信し端末 A が送信できなかった。次の競合では、端末 A が送信し端末 B が送信できなかった。この時の端末 B の持越しタイミングが 2 であった場合、端末 A がさらに3回続けて送信できる確率を求めよ。なお, 両通信端末が同じタイミングを選択した場合は、前回の競合で送信できなかった通信端末が送信できるものとする。

Ⅳ情報システム

次の問いのすべてについて、それぞれ6行程度で答えよ

(問1) 引数の受け渡しのあるサブルーチンのコールとリターンの動作を、スタックを用いて説明せよ。

(問2) 応用例を用いて分散型システムと集中型システムを比較し、それぞれの利点と課題について述べよ。

(問3) コンピュータ上で仮想マシンを動作させる利点と課題を、一つ以上の例を使って説明せよ。

(問4) 少なくとも1年間にわたって停止することなく動作し、正しい計算処理を続けることが必要な情報システムを設計・開発するとき、どのような方法を取り入れるか、方法（複数も可）とその効果を述べよ。

Vソフトウェア

入力：n 個の数の列 $\langle a_1, a_2, \ldots, a_n \rangle$を、出力：$a'_1 \leq a'_2 \leq \ldots \leq a'_n$ であるような列$\langle a'_1, a'_2, \ldots, a'_n \rangle$に置換する問題をソーティング問題と呼ぶ。ソーティング問題を解くアルゴリズムはいくつかあるが、その中で挿入ソートは少数の要素を効率よくソートするアルゴリズムである。挿入ソートは、トランプ遊びで手札をソートするときに多くの人が使う。まず、左手を空にし、テーブルの上にカードを裏向きに置く。次に、テーブルからカードを 1 枚ずつとって、左手の正しい位置に挿入していく。挿入ソートのアルゴリズムを擬似コードで記述すると下記の通りになる。

		実行回数
INSERTION-SORT (A)		
1.	for $j = 2$ to $A.length$	n
2.	$key = A[j]$	(ウ)
3.	//$A[j]$をソート済みの列 $A[1..j-1]$に挿入する	
4.	$i = j - 1$	(エ)
5.	while $i>0$ かつ $A[i] > key$	$\sum_{j=2}^{n} t_j$
6.	$A[i+1] =$ (ア)	$\sum_{j=2}^{n} (t_j - 1)$
7.	$i = i - 1$	$\sum_{j=2}^{n} (t_j - 1)$
8.	(イ)	(オ)

$A.length$: 配列 A の長さ(要素数)

t_j: 第 5 行の while 文の判定が値 j に対して実行される回数

(問 1) 上記の擬似コードの空欄(ア) (イ) を埋め、アルゴリズムを完成させよ。

(問 2) 上記アルゴリズムの実行時間について考える。上記右欄(ウ)～(オ)に入る実行回数を答えよ。

(問 3) 挿入ソートは、入力列の並び方によって実行時間が変化する。

(1)入力列がどのような時に最良の実行時間となるか。またその実行時間を n のオーダーで表せ。

(2) 入力列がどのような時に最悪の実行時間となるか。またその実行時間を n のオーダーで表せ。

小論文

下記のＡさんとＢさんの会話を読み、情報セキュリティにおけるヒューマン・ファクター（人的要因）についてどのように考えるか。自分自身のこれまでの経験にも即しながら、2,000 字以上 3,000 字以内で小論文を作成せよ。

Ａ さん「最近、怪しい電子メールの添付ファイルをうっかり開いてマルウェア（コンピュータ・ウィルス）に感染したり、パスワードの設定を適切に行っていなかったりして、個人情報や企業情報などが漏洩(ろうえい)する事件が相次いでいるみたいだね。」

Ｂ さん「そういうことが起きないように、企業や組織のルールできちんと取扱いについて決めて、所属している人にそれを守らせるようにするべきだと思う。」

Ａ さん「だけど、ルールでいくら決めていたとしても、人間は機械じゃないんだからミスを完全になくすことはできないよ。誰かがミスするかもしれない、と考えておいた方が現実的なんじゃないかな。」

Ｂ さん「それじゃあ、ルールをきちんと守っている人が損をするような感じになるよ。ルールを守れなかった人にはきちんと制裁を受けさせるようにしないと、誰もルールを守らなくなって情報がどんどん漏洩する、ということになりかねないね。」