2018年7月4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
2019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　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) n を自然数とする。

$$\lim_{x\to\infty}\frac{x^n}{2^x}=0$$

であることを証明せよ。

(問2) n を2以上の整数とし、

$$f(x) = x\log x$$

とする。n 次導関数 $f^{(n)}(x)$ を求めよ。

(問3)

$$\int_{-\infty}^{\infty}\frac{1}{1+x^2}dx$$

を求めよ。

II 情報数学B

iを虚数単位とし、$\zeta = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$とする。多項式$A(X) = X + X^4$について、$\alpha = A(\zeta)$および$\beta = A(\zeta^2)$とする。

(問1) $\alpha + \beta$と$\alpha \cdot \beta$を求めよ。

(問2) αを小数点以下、第2位まで計算せよ。

III ネットワーク

(問 1) コンピュータネットワークにおいて、ルータは IP パケットを転送したり破棄したりしながら、複数のネットワークを中継する機能を担う。ルータについて、以下の質問に答えなさい。

① OSI 参照モデルのどの層で機能するか
② パケットの転送経路選択の際に何を用いてフィルタリングを行うか
③ ブロードキャストされてきた IP パケットをどのように扱うか

(問 2) スタティックルーティングとダイナミックルーティングについて、経路情報の管理方法の違いを簡潔に述べよ。

(問 3) ルーティングプロトコルにおける、リンクステート型とディスタンスベクタ型の違いを 3 つ取り上げて説明せよ。

(問 4) あるホストの IP アドレスが、172.16.199.56/19 であるとした時、以下について各々算出方法を示しながら求めよ。

① このホストが属しているネットワークのネットワークアドレス
② このホストが属しているネットワークのブロードキャストアドレス
③ このネットワークで利用可能な IP アドレスの総数

(問 5) 192.168.13.0/24 のネットワークに、少なくとも ア) 90 アドレス、イ) 50 アドレス、ウ) 10 アドレスを利用可能な 3 つのサブネットを作成したい。各々のネットワークアドレスとサブネットマスクについて、算出方法を示しながら求めよ。

Ⅳ 情報システム

次の問に各数行以内で答えなさい。図表を加えて回答しても良い。

(問 1) 現代の多くのコンピュータの基本的なアーキテクチャである、プログラム内蔵方式 (Stored Program Architecture) とは、どのような方式であるか説明しなさい。

(問 2) プログラム内蔵方式の長所と短所をそれぞれ説明しなさい。

(問 3) 現代のコンピュータは、階層的なメモリの構造を取っている。数段のメモリの各階層を示し、なぜそのような階層になっているかを説明しなさい。

(問 4) 問 3 で回答した各層のメモリにはどのようなデバイスが使われているか、メモリの種名と特徴を説明しなさい。

Vソフトウェア

(問 1)

ビットごとの排他的論理和(XOR)を用いた暗号文作成ソフトがある。平文を入力したところ、暗号文は下記の通りとなった。

平文

x57	x50	x41

⊕

鍵

?	?	?

↓

暗号文

x0	x15	x11

このとき、鍵となる3バイトを16進表記で記述せよ。

(問 2)

次ページのJavaプログラムは、4ビットのデータを入力とし、ハミング符号を実現するプログラムである。各ビットはint(整数)型、ビット列はint型の配列として表現している。

(1) プログラム中の(ア)～(エ)に入る整数を書け。

(2) プログラム中の(オ)(カ)に式を書いて、プログラムを完成させよ。

Javaにおいて乗算は*、排他的論理和は^で記述するが、×や⊕を用いて書いてもよい。

(3) (1 1 0 1)を次ページのプログラムで符号化した結果を書け。

(4) ある符号化されたデータ(0 0 1 0 1 1 0)がある。これを次ページのプログラムで検査した結果と、もし誤りである場合は、本来の正しいデータを記述せよ。

```
//ハミング符号のプログラム

public class HammingCode {
    static int[][] g = {{1,0,0,0,1,1,0},  //生成行列G
                        {0,1,0,0,0,1,1},    //2次元配列は、g[行の添字][列の添字]で指定
                        {0,0,1,0,1,0,1},  //例えば、gの2行目3列目はg[1][2]で値は0
                        {0,0,0,1,1,1,1}};  //(添字は0から開始)
    static int[][] h = {{1,0,1,1,1,0,0},  //検査行列H
                        {1,1,0,1,0,1,0},
                        {0,1,1,1,0,0,1}};

    static int[] encode(int[] in) {  //符号を生成
        int[] out = new int[7]; //符号化データ格納用配列
        for (int i=0;i<(ア);i++) {
            out[i]=0;
            for(int j=0;j<(イ);j++) {
                out[i]= (オ);
                    }
            }
            return out;

    }

    static int[] check(int[] data) { //符号の誤り検査
            int[] out = new int[3]; //検査結果格納用配列
            for(int i=0;i<(ウ);i++) {
                    out[i]=0;
                    for(int j=0;j<(エ);j++) {
                            out[i]=カ;
                    }

            }
            return out;

    }
}
```

小論文

近年、フェイクニュースがソーシャル・ネットワーキング・サービス（SNS）等の上で流布されるようになっている。フェイクニュースによって一般大衆の誘導や世論操作が行われるようになり、各国の政府機関や企業にとっての脅威ともなってきた。

このようなフェイクニュースには、どのような対策を取ることが有効か。フェイクニュースに関する自分自身の経験や見聞にも即しながら、2,000 字以上 3,000 字以内で小論文を作成せよ。