2019年7月10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
2020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

a, c_1, c_2, c_3 をいずれも実数とする。x, y, z を変数とする連立1次方程式

$$\begin{cases} x + 2y + z = c_1 \\ 2x + y + az = c_2 \\ x + ay + z = c_3 \end{cases} \tag{1}$$

について以下の問いに答えよ。

(問1) 連立1次方程式 (1) が一意に解を持つ条件を示し、その理由を説明せよ。

(問2) 連立1次方程式 (1) が複数の解を持つ条件を示せ。また複数の解を持つ (a, c_1, c_2, c_3) の例を1つ示し、その解を求めよ。

(問3) 連立1次方程式 (1) が解を持たない条件を示し、その理由を説明せよ。

II 情報数学B

正の整数 m の階乗 $m! = m \times (m-1) \times \cdots \times 2 \times 1$ の、任意の素数 p に関する指数を v とする。すなわち、p^v は $m!$ をわりきるが p^{v+1} は $m!$ をわりきらない。

$$v \leq (m-1)/(p-1)$$

であることを示せ。

III ネットワーク

(問 1) TCP および UDP プロトコルにおけるポートについて、以下の問いに答えよ。

(1) ポートの役割を説明せよ。

(2) Well-Known ポート番号について説明せよ。

(問 2) TCP によるデータ転送について、UDP と異なる特徴を３つあげて説明せよ。

(問 3) 商用で提供されるネットワークにおける SLA(Service Level Agreement)について、以下の問いに答えよ

(1) SLA の目的を説明せよ。

(2) SLA に含めるべき代表的な評価項目を３つあげて説明せよ。

(問 4) 垂直水平パリティ符号について、以下の問いに答えよ。

(1) 通信ネットワーク分野への応用について説明せよ。

(2) 長さ 4 の情報ビット 1101 に対する垂直水平パリティ符号を求めよ。

(問 5) IPv6 には IPv4 と比べた時に様々な利点があると言われている。IPv6 の利点を３つ取り上げて説明せよ。

Ⅳ 情報システム

インターネット上の Web システムの PC からの利用について、下記の質問に答えなさい。

(問1)　①-③の記述の空欄に最も適切な用語を選択しなさい。

① Web システムは、インターネットにつながる PC などのコンピュータ(以下、クライアント) が、＿＿＿＿＿＿を使って、サーバーが用意するコンテンツ情報を読み出すことを主たる目的としている。

a. HTTP　b. telnet プロトコル　c. イーサネット　d. HTML

② クライアントは、通信相手のサーバーを URL によって識別する。しかし、インターネットのネットワーク層のプロトコルでは IP アドレスによってホストを識別するので、URL から IP アドレスへの変換、すなわち名前解決のために＿＿＿＿＿＿を用いる。

a. HTTP　b. DNS　c.MAC アドレス　d. ARP (address resolution protocol)

③ Web サーバーが HTTP リクエストを受け取ると、そのサーバー上のリソースをクライアントに送信する。このリソースは、静的なファイルの場合もあるが、Web サーバーが＿＿＿＿＿＿を通じて各種の言語で作成されたプログラムを実行して動的にコンテンツを生成することもできる。

a. FTP　b. CGI　c. PHP　d. ルーター

(問2)　動的なコンテンツを生成する方法には、問 1-③のようにサーバー側で生成する方法の他に、クライアント側で生成する方法がある。このクライアント側での動的コンテンツ生成の方法の概略を説明しなさい。

(問3)　サーバーでの動的コンテンツ生成と、クライアントでの動的コンテンツ生成を比較し、2 点の相違点に着目して、特徴を論じなさい。

(問4)　クライアントが動的コンテンツを生成する方法を不用意に実装したのでは、Web サーバーが悪意を持っている場合にセキュリティ上の問題が生じることがある。それがどのような問題であるか 2 点示しなさい。

(問5)　問 4 で上げた 2 点の問題を防ぐにはどのような方法が考えられるかをそれぞれ示しなさい。

Vソフトウェア

逆ポーランド記法について下記の(問 1)(問 2)に答えよ。

(問 1)

逆ポーランド記法は、計算する 2 つの数値の直後に演算子を書く記法である。

以下の式を逆ポーランド記法で書け。(数値の区切りには|を使うこと)

((2+3)*4-(2*4))/3=

(問 2)

逆ポーランド記法の式を数値/演算子ずつ読みとって計算するアルゴリズムを、下記の(ア)に(a)～(f)の選択肢から順に並べることで完成させよ。同じ選択肢を何度使ってもよい。

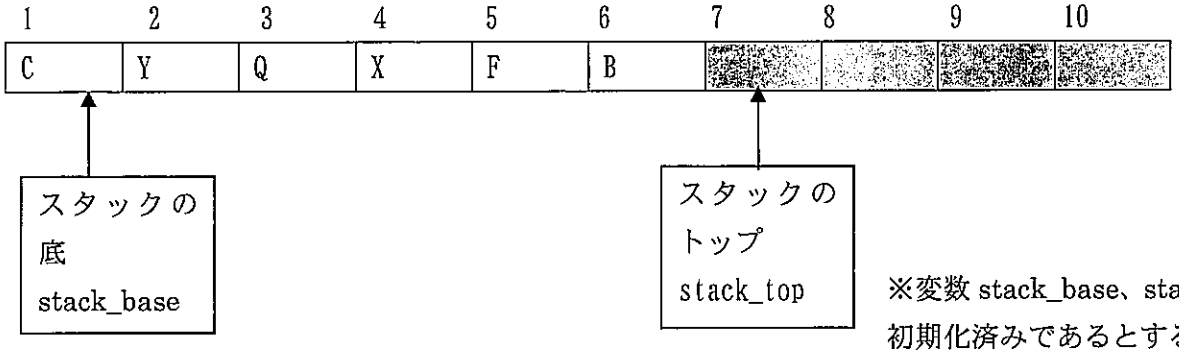
```
while true
  式から c に 1 つ読みこむ
  if c= ' ='
      then 計算結果を出力して終了
      else
           (ア)

end
```

選択肢

(a) スタックに数値をプッシュ (b) スタックから数値をポップ (c) スタックに演算子をプッシュ (d) スタックから演算子をポップ (e) スタックに途中の演算結果(数値)をプッシュ (f) 2 つの数値を演算子で計算

スタックについて、下記(問 3) (問 4)に答えよ。

(長さ length[A]=10 の配列 A の例)



※変数 stack_base、stack_top は初期化済みであるとする

(問 3) 下記 (イ) に入るべきコードを書け。

プッシュのアルゴリズム

```
PUSH(A[], x)                    //A:配列 x:プッシュする要素
1 i = stack_top    //i に stack_top を代入
2 A[i] = x         //配列 A の i 番目の要素に x を代入
3 stack_top = stack_top +1 //stack_top の値を 1 つ増やす
```

ポップのアルゴリズム

```
POP(A)
1 if  [        (イ)        ]
2     then error(‘スタックは空’) //「スタックが空である」というエラーを出力
3     else stack_top = stack_top -1 //stack_top の値を 1 つ減らす
4  return A[stack_top]              //取り出す値を A の stack_top 番目からとり返す
```

(問 4) ポップの場合と同様に、プッシュにもエラー処理が必要である。該当する行番号を書き、挿入する処理を書け。

小論文

AI（人工知能）技術や関連技術の発展によってAIの実用化が進み、私たちの生活のさまざまな領域で利用されるようになってきた。しかし同時に、プロファイリングやプライバシー侵害、軍事利用の恐れ、人間による作業がAIに置き換わることによる職業喪失の恐れなど、AI 利用に関するさまざまな問題点も指摘されるようになった。今後、AI と人間・社会が共生していくには、どのような社会的な対応を取るべきと考えられるか。AIやAI関連技術に関する身近な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。