

2017年7月5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
2018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

\log を自然対数とする。

(問1) $x > 0$ のとき

$$\frac{x}{x+1} < \log(1+x)$$

であることを証明せよ。

(問2) $a_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n$ により定義される数列 $\{a_n\}$ が収束するか否かを示し、それを証明せよ。

II 情報数学 B

正の整数 q について、 0 以上 $q-1$ 以下の整数の集合を $\mathbb{Z}_q = \{0, 1, \dots, q-1\}$ と書く。 \mathbb{Z}_q から 2 つの整数 a と b を独立かつ一様ランダムに選んだとき、それら a と b の最大公約数 $\gcd(a, b)$ が q と互いに素である、すなわち、 $\gcd(\gcd(a, b), q) = 1$ となる確率を P_q とする。以下の問いに答えよ。

(問 1) P_{512} を求めよ。

(問 2) P_{259} , P_{341} , P_{512} を小さい順に並べよ。

III ネットワーク

図1、図2に示す誤り確率 p の2元対称通信路および消失確率 q の2元消失通信路について以下の問いに答えなさい。

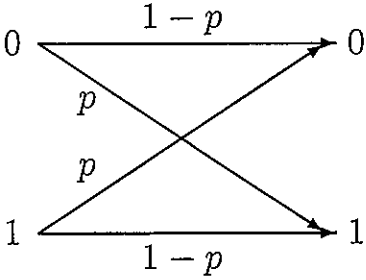


図1. 2元対称通信路

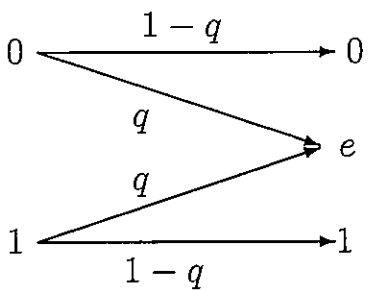


図2. 2元消失通信路

- (問1) 図1、図2に示す各通信路について通信路容量を p, q の式として与えよ。但し、 e は消失を表す。
- (問2) 図1、図2に示す各通信路について、 $p = 0.25, q = 0.1$ の時の通信路容量を計算せよ。但し、 $\log_2 3 = 1.6$ として良い。
- (問3) 図3に示すような2元対称通信路が n 段連なった通信路を考え、この通信路の通信路容量を C_n と書く。 $p \neq 0, 1$ ならば $\lim_{n \rightarrow \infty} C_n = 0$ となることを証明せよ。

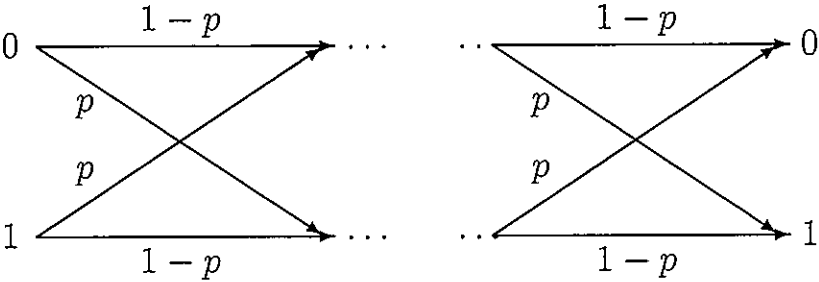


図3. n 段2元対称通信路

IV 情報システム

コンピュータの入出力機構に関する以下の質問に答えよ。

(問 1) デバイスドライバの説明として正しい記述を記号で選べ。

- (ア) 安全のため一般ユーザーがアクセスできないように仕組みられたデバイスの蓋や覆いを開けるための専用のドライバ
- (イ) CD-ROM や USB メモリから読み込まれて、インストールを自動実行するプログラム
- (ウ) プリンタやネットワークなどのデバイスとの通信を情報圧縮などによって高速化するプログラム
- (エ) オペレーティングシステム・カーネルの中にあってハードディスクや USB ポートなどの入出力デバイスの制御を受け持つプログラム

(問 2) 割り込み機構の果たす役割、目的として不適切な記述を (ア) ~ (オ) から 2 つ選べ。

- (ア) 計算の過程でオーバフローが生じたことを知らせる
- (イ) 低速な入出力デバイスの処理から CPU を解放して他の処理を実行させる
- (ウ) 使用できる範囲外のメモリを使用したときにエラーを警告する
- (エ) 緊急なイベントが発生すると、現処理を中断して実行する
- (オ) タイマーによって複数のプロセスの実行を切り替えるタイミングを作る

(問 3) コンピュータに接続される入出力デバイスとして、マウスと USB メモリの 2 つについて、入出力動作が始まるタイミングと、データ伝送の速度の観点から比較して論じなさい。

(問 4) 入出力機器の動作は、CPU やメモリの動作と比べると低速である。この速度の調整 (入出力制御) をビジーウェイトで行う場合と割り込みで行う場合の利害得失を論じなさい。

(問 5) 以下の 4 つの文は、複数のプロセスを並行して実行するシングルコアのプロセッサの割り込みハンドラが、入出力デバイスからのデータを受け取る処理を記述している。下線と (A) ~ (C) の記号で示す空欄に適切な用語を下の①~⑫の選択肢から選んで挿入しなさい。同じ記号の下線部には、同じ用語が入る。

- 入出力デバイスに外部からデータが届くと、デバイスから、 (A) が発生する。
- プロセッサは、割り込み可能な状態で (A) を受け取ると、次の命令の実行を延期して、割り込みハンドラを実行させる。そのために、現在の

(B)、プロセッサ状態語 (PSW)、および使用中の汎用レジスタをスタックに退避し、割り込みハンドラの先頭に分岐する。

- 割り込みハンドラは、入出力デバイスに届いたデータを読み出し、ユーザープログラムの受け取りバッファに移す。入出力の完了を待っているプロセスを(C)に遷移させる。
- 割り込みハンドラの処理が終了すると、退避した汎用レジスタ、プロセッサ状態語、(B)を復帰させ、割り込まれたプログラムの実行に戻る。

選択肢：

- ① 割り込み禁止信号、② 割り込み信号、③ リセット信号、④ データ受付信号
⑤ プログラムカウンタ (命令ポインタ)、⑥ 入出力命令、⑦ 実行中の命令、⑧ エラーコード、⑨ 停止状態から実行完了状態、⑩ 停止状態から実行状態、⑪ 待ち状態から停止状態、⑫ 待ち状態から実行可能状態

Vソフトウェア

ソフトウェア設計時に再利用される設計仕様であるデザインパターンの1つとして、Singletonパターンがある。Singletonパターンは、オブジェクト指向プログラムにおけるあるクラスのインスタンスがただ1つであることを保証するために用いられる。Singletonパターンを用いたJavaプログラムコードの例[コードA][コードB]を下記に示す。なお、Singletonを適用したCounterSingletonは外部の複数のクラスから呼び出されることを前提としている。

[コードA]

```
(ア) class CounterSingleton ( //Singletonパターンを適用したクラス
    (イ) Counter instance;
    (ウ) getInstance () {
        return (エ) ;
    }
}

public class Counter (
    int n;
    Counter () ( //初期化処理
        n=0;
    )
    public void count () {
        n++;
    }
}
```

[コードB]

```
Singleton service = (オ) . (カ) ;
(キ) . (ク) ;
```

(問1)

[コードA]の(ア)～(ウ)の中に入る修飾子を下記(a)～(c)から選び、記入せよ。□の中には複数の修飾子が入る場合もある、また、同じ修飾子を何度使ってもよい。

- (a) private (非公開)
- (b) public (公開)
- (c) static (静的)

(問 2)

[コード A] の (エ) に入るコードを記入せよ。

(問 3)

[コード B] は、複数の人がサービスにアクセスするたびに、カウントを 1 増やすために CounterSingleton クラスを呼び出している。空欄 (オ) ~ (ク) に入るコードを下記選択肢から選んで記入せよ。同じ選択肢を何度使ってもよい。

- (d) CounterSingleton
- (e) service
- (f) getInstance()
- (g) count()

(問 4)

1 つのカウンタを複数の人またはサービスから使いたい場合、Singleton パターンを使わないと、どのようなデメリットが起きることが予想されるか。簡潔に記述せよ。

小論文

ソーシャルネットワーキングサービス（SNS）が広く使われるようになってきているが、さまざまな手口で SNS のアカウントを乗っ取られて不正にアクセスされ、勝手にメッセージを送信されたりする被害が相次いでいる。

このようなアカウント乗っ取りによる不正アクセスを防止する方策について、自分自身の経験や身近な事例にも即しながら、2,000 字以上 3,000 字以内で小論文を作成せよ。

