2025 年 7 月 9 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　情報セキュリティ専攻　博士前期課程
2026 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、2,000 字以上 3,000 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) 次の行列の固有値を求めよ。

$$\begin{pmatrix} 2 & 1 & -3 \\ -2 & -1 & 2 \\ 1 & 1 & -2 \end{pmatrix}$$

(問 2) $n \times n$ 行列 A に対し、行列 A の固有値の和と、行列 A の対角成分の和が等しいことを証明せよ。

(問 3) ある正の整数 m に対し $A^m = O$ となる $n \times n$ 行列 A に対し、行列 A の固有値の和を、計算の過程を示し求めよ。

Ⅱ 情報数学B

奇素数 p について、1 とは異なる複素数 ω が $\omega^p = 1$ を満たすとする。以下の問いに答えよ。

(問 1) $i = 1, 2, \ldots, p-1$ について、ω^i は多項式 $f(X) = 1 + X + X^2 + \cdots + X^{p-1} = \sum_{j=0}^{p-1} X^j$ の根であること、すなわち、$f(\omega^i) = 0$ を示せ。

(問 2) ω^i たちの積は 1 に等しいこと、すなわち、

$$\prod_{i=1}^{p-1} \omega^i = 1$$

を示せ。

(問 3) $1 - \omega^i$ たちの積は p に等しいこと、すなわち、

$$\prod_{i=1}^{p-1} (1 - \omega^i) = p$$

を示せ。

(問 4) 以下の値を計算せよ。

$$\prod_{i=1}^{p-1} \frac{p\omega^{i(p-1)}}{1 - \omega^i}$$

Ⅲネットワーク

ネットワークのセキュリティプロトコルと応用に関して次の問いに答えよ。

(問 1) インターネットで広く使われているセキュリティプロトコル SSL/TLS は、次の 4 つのプロトコルから構成される。それぞれの役割を数行で説明せよ。なお、TLS のバージョンは 1.2 以上とする。

(ア) HandShake プロトコル

(イ) ChangeCipherSpec プロトコル

(ウ) Record プロトコル

(エ) Alert プロトコル

(問 2) セキュリティプロトコル IPsec について以下の問いに答えよ。

(ア) IPsec には、二つの方式（トランスポートモードとトンネルモード）がある。それぞれの方式について、数行で説明せよ。図を使って説明しても良い。

① トランスポートモード

② トンネルモード

(イ) IPsec の OSI 階層における特徴について、SSL/TLS と比較しながら説明せよ。

(問 3) VPN について以下の問いに答えよ。

(ア) VPN の役割について数行で説明せよ。

(イ) IPsec VPN について数行で説明せよ。

(ウ) SSL-VPN について数行で説明せよ。

(エ) MPLS と MPLS を用いた VPN について数行で説明せよ。

(問 4) 昨今、企業や病院などを標的としたランサムウェア攻撃が社会問題となっており、その被害状況や原因についての報告書が公表されている。ランサムウェア攻撃の感染経路となる脆弱性にはどのようなものがあると報告されているか、また、そのセキュリティ対策の在り方について、自身の考えを述べよ。

Ⅳ 情報システム

(問 1) 逆ポーランド記法（後置記法）ではスタックベースで計算するモデルであり、通常の演算記法（中置記法）の（A－B)×C は逆ポーランド記法で AB－C× となる。

(1) 下記の逆ポーランド記法を通常の演算記法で示せ。
AB-CDE÷＋×

(2) 下記の通常の演算記法を逆ポーランド記法で示せ。
A+B*(C-D)/E

(3) スタックマシンは逆ポーランド記法をベースした計算モデルである。命令セットやメモリアクセスなどの違いを中心に現在の CPU アーキテクチャとして比較して、利点と欠点をそれぞれ 3 行程度で述べよ。

(問 2) CPU のキャッシュに関する問題に答えよ。

(1) キャッシュのアクセスタイムが 5 ナノ秒、メインメモリのアクセスタイムが 0.1 マイクロ秒、キャッシュのヒットレートが 90%とした時の平均アクセスタイムは何ナノ秒になるか。

(2) キャッシュとメインメモリの差が小さい時と大きい時でヒット率の影響が大きいのはどちらか。その理由も含めて数行程度で説明せよ。

(3) キャッシュの特性が活用するためにはプログラムの参照局所性を使っている。参照局所性の二つの特徴を各 3 行程度で説明せよ。プログラムコードのサンプルを示してもよい。

Ｖソフトウェア

アジャイル開発およびDevOpsについて、下記の問に答えよ。

(問1) アジャイル開発の特徴と期待される効果について、下記の4つの観点で、ウォーターフォールと比較しつつ、4つの観点ごとにそれぞれ数行で説明せよ。

(1) ステークホルダの関わり方
(2) 属人性
(3) ドキュメント(文書化)
(4) 要求の柔軟性

(問2) アジャイル開発が適するシステム、適さないシステムをそれぞれ挙げ、その理由を数行で説明せよ。

(問3) DevOpsの特徴について数行で説明せよ。

(問4) CI/CDとは何かについて、数行で述べよ。また、それらがアジャイル開発やDevOpsに果たす役割について、数行で述べよ。

(問5) アジャイル開発やDevOpsにおいて、セキュリティ品質を確保する際に注意すべき点について考察し、数行で述べよ。

小論文

情報処理推進機構（IPA）が 2025 年 1 月に公表した「情報セキュリティ 10 大脅威 2025」では、「内部不正による情報漏えい等」が第 4 位になっている。

内部不正による情報漏えいについて、実際に発生した事案を 1 つ以上取り上げなさい。その際、自分自身が経験したり、見聞きしたりしたことを含めても構わない。また、このような内部不正による情報漏えいが発生する原因について、人間の心理的な側面や、法的・制度的な側面から述べなさい。そのうえで、内部不正による情報漏えいの問題について、どのようにしたら解決することができるか、自分なりの解決策を提案しなさい。解決策については、人間の心理的な側面に着目した解決策や、法的・制度的な側面に着目した解決策を提案すること。

文字数は、全体で 2,000 文字以上、3,000 文字以内とする。