

令和7年度
京都工芸繊維大学 大学院工芸科学研究科
博士前期課程（修士課程）推薦入学特別入試
情報工学専攻 小論文 課題

[注意]

1. この課題冊子は合図があるまで中を開かないでください。
2. 課題は3題あり、課題1は必須です。課題2と3はどちらか一方を選択してください。課題1と、課題2と3のどちらか一方の、計2題について小論文を作成してください。
3. 配布物は、この課題冊子1部、解答用紙2枚、および下書き用紙2枚です。解答する課題毎に別の解答用紙を用いてください。汚損等でやむを得ない場合を除き、解答用紙および下書き用紙の追加配布はしません。
4. 解答用紙裏面を使用する場合は、おもて面右下に「裏面使用」と断り書きして使用してください。
5. 机の上には受験票以外に、次のものを置いてもよろしい：黒鉛筆またはシャープペンシル（黒）、プラスチック製の消しゴム、鉛筆削り（電動式・大型のものは不可、カッターナイフは可）、計時機能のみの時計（秒針音のするもの・大型のものは不可）、予備も含めた感染防止用の無地のマスク、眼鏡・ハンカチ・目薬・ティッシュペーパー（袋又は箱から中身だけ取り出したもの）。これら以外のものについては監督者の了解を得た場合に限り、置くことができます。
6. 試験時間は、9：30～11：30の120分間です。中途退室は認めません。ただし、トイレなどやむを得ない場合は、一時退室を認めますので、挙手して知らせて下さい。試験終了後も退室の許可があるまで退室はできません。
7. 解答用紙2枚とも、上欄指定枠内に、課題番号（「科目」欄に記入すること）、志望専攻名、受験番号を忘れず記入してください。
8. 試験開始後、課題冊子印刷の不鮮明や落丁などに気づいたら申し出ること。この課題冊子はバラしても構いません。
9. 課題冊子と下書き用紙は持ち帰ってください。

[以上]

課題 1

問 1 C 言語で文字列の末尾にヌル文字の追加が必要であるが、ヌル文字が入っていない場合にどのような問題が生じるかを具体例と共に説明しなさい。また、空ポインタを表すオブジェクト形式マクロである NULL とヌル文字との違いを説明しなさい。なお、それぞれ 100 文字程度で解答しなさい。

問 2 C 言語における malloc() と free() の役割とそれらを使用する際に注意すべき点を 150 文字程度で説明しなさい。

問 3 下記の名称を全て利用して、100 文字程度で C 言語のソースプログラムから実行ファイルを生成する流れを記述せよ。また、この記述とは別に、オブジェクトモジュール、コンパイル及びリンクのそれぞれの役割を説明せよ。

名称：

オブジェクトモジュール、標準ライブラリ、コンパイル、リンク、実行ファイル、ソースプログラム

課題 2

- 問1 多くのプロセッサのマシン命令において、直接アドレス指定だけでなく、レジスタ間接アドレス指定、ベースインデックスアドレス指定など、多様なアドレッシングモードが用意されている。多様なアドレッシングモードを備えることの得失を論じなさい。
- 問2 プロセッサにおける負の整数の表現形式として、「符号－絶対値表現」、「1の補数表現」、「2の補数表現」が挙げられる。このうち、プロセッサで一般的に用いられている表現形式を示し、その形式が用いられる理由をできるだけ多く述べなさい。

課題3

問1

誤り率を p ($0 \leq p \leq 1$) とする 2 元対称通信路の通信路容量は、 $1 + p \log_2 p + (1-p) \log_2 (1-p)$ bit と与えられる。横軸を p 、縦軸を通信路容量とした概形を示せ。また、 $p = 0, 1/2, 1$ のそれぞれの場合の通信路容量の値を示すとともに、なぜその値となるか理由を説明せよ。

問2

インターネットを介して組織外の第三者と機密情報を安全にやりとりする方法について考える。

- (a) 「暗号化したパスワード付き ZIP ファイルを電子メールに添付して送った後、復号用のパスフレーズを別メールで送る」という方法のセキュリティ上の問題点について説明せよ。
- (b) (a) で述べた問題点の解決策を提案し、技術的なメリット・デメリットを説明せよ。

問3

将来、量子コンピュータが実用化されると、RSA 暗号や楕円曲線暗号など、現在用いられている多くの公開鍵暗号方式が危殆（きたい）化されると言われている。

- (a) その理由について説明せよ。
- (b) 現在用いられている公開鍵暗号の鍵サイズを大きくすることでは対応が難しい理由を説明せよ。
- (c) 量子コンピュータの実用化に備えて、どのような対策が考えられているか説明せよ。