

第1問 (40点)

以下の文章中にある空欄（ア）～（ク）にあてはまる用語や数値を選択肢（a）～（t）から選べ。ただし、同じ記号の空欄には同じ選択肢が入るものとする。また、同じ選択肢が異なる記号の空欄に入ることはないものとする。

長さや質量、温度、時間などのように連続的に変化する量を、時計の針の位置のように連続した量で表現することを という。一方、連続的に変化する量を、一定の間隔で区切った数値や段階的な数値で表現することを という。

画像は、連続的に変化する明るさや色の濃淡が平面上に分布した 情報である。画像の 化は次の手順で行われる。まず、画像を画素（ピクセル）に区切り、代表となる色を数値として取り出す。これを 化という。次に、各画素の数値を何段階かに分けた数値に変換する。これを 化という。最後に、 化された数値を2進法に変換する。これを 化という。

2進法4桁では 通りの情報を表すことができる。10進法の を2進法4桁で表すと1101となり、10進法の6を2進法4桁で表すと となる。

選 択 肢

- | | | | | |
|----------|----------|----------|----------|----------|
| (a) デジタル | (b) アナログ | (c) 符号 | (d) 暗号 | (e) 量子 |
| (f) 可視 | (g) 標本 | (h) 標準 | (i) 2 | (j) 4 |
| (k) 8 | (l) 9 | (m) 11 | (n) 13 | (o) 15 |
| (p) 16 | (q) 0100 | (r) 0111 | (s) 0110 | (t) 1100 |

第2問 (100点)

表1は、ある店舗の3月3日から3月12日までの10日間の気象情報(天気と最高気温)、来客数および売上高のデータである。このとき、以下の問いに答えよ。

表1 ある店舗の売上データ

No.	日付	天気	最高気温(℃)	来客数(人)	売上高(千円)
1	3月3日	晴れ	10	5	900
2	3月4日	雨	8	4	300
3	3月5日	晴れ	15	9	2,000
4	3月6日	雨	6	8	600
5	3月7日	曇り	9	10	950
6	3月8日	晴れ	12	9	1,800
7	3月9日	晴れ	10	12	2,500
8	3月10日	曇り	8	8	800
9	3月11日	晴れ	12	10	1,800
10	3月12日	雨	5	15	-

問1 一般に、(ア) 量的データ、(イ) 質的データおよび(ウ) 欠損データとは何かそれぞれ説明せよ。さらに、表1の先頭行にある項目「天気」、「最高気温(℃)」、「来客数(人)」、「売上高(千円)」を(ア) 量的データ と(イ) 質的データ に分類せよ。

問2 表2は、天気ごとに表1のNo. 1からNo. 9までの売上高の合計、平均値、標準偏差をまとめたものである。このとき、空欄(エ)～(カ)に入る数値を答えよ。なお、表1のNo. 10の売上高が欠損データのため、表2ではNo. 10は除外されていることに注意すること。

表2 ある店舗の売上データの天気ごとの集計結果

天気	合計(千円)	平均値(千円)	標準偏差
晴れ	9,000	(オ)	517.7
曇り	(エ)	875	75.0
雨	900	(カ)	150.0

問3 一般に、標準偏差とは何を表す指標か説明せよ。さらに、表2から天気ごとの売上高の平均値と標準偏差から読み取れることを述べよ。

問4 1月1日から3月31日までの売上データから、天気が晴れのときの来客数と売上高との相関係数を求めたところ0.90であった。この相関係数が意味することを述べよ。また、表1のNo. 1, 3, 6, 7, 9の来客数と売上高の値から、それらの相関を視覚的にとらえることができるグラフ（散布図）を作成せよ。

第3問 (80点)

学校のコンピュータクラブで、CPU（中央処理装置）、主記憶装置（メモリ）、入力装置および出力装置で構成される小型コンピュータを作製した。作製した小型コンピュータを使って、クラブメンバ20 人分の売店のカードのポイント数の合計を計算することにした。小型コンピュータ上でプログラムを作成する前に、クラブメンバで計算方法について議論した。

プログラムを作成する際の前提条件（1）～（4）は次のとおりである。（1）入力となる数値データは、入力装置を使って主記憶装置に格納されているものとする。（2）主記憶装置に格納されているデータは、必要に応じてプログラム実行前に自由に追加・変更ができるものとする。（3）CPU は、2つの値に対する四則演算（加算・減算・乗算・除算）を1回で実行できるものとする。（4）四則演算の結果は、CPU 内のレジスタにすべて保存でき、常時読み出しできるものとする。このとき、以下の問いに答えよ。

問1 表3に示されたポイント数が、1 番目から 20 番目まで順に主記憶装置に格納されているとする。20 人分の合計を1 番目から順に1 つずつ足して計算するとき、CPU において実行される四則演算の総実行回数を答えよ。なお、その答えの導出過程も述べること。

表3 メンバのポイント数データ

メンバ	ポイント数	メンバ	ポイント数
1	40	11	90
2	40	12	76
3	76	13	76
4	65	14	65
5	76	15	65
6	76	16	55
7	90	17	76
8	76	18	40
9	76	19	55
10	65	20	55

問2 クラブメンバと四則演算の回数について議論したところ、あるメンバAが「表3の代わりに各ポイント数の出現回数の表を作成し、その表に基づいて数値データを主記憶装置に格納して利用すれば、四則演算の総実行回数を減らせるのではないか？」と提案した。このとき、メンバAの提案と考えられる四則演算の実行回数を減らす方法を説明せよ。なお、表3を見ていてメンバAが気づいた数値データの特徴、使用する四則演算とその実行回数および総実行回数について言及すること。

問3 メンバAが手作業で問1の表3から各ポイント数の出現回数を数えてから問2で提案した計算方法で合計を求めたところ、問1で計算した値と異なってしまった。2つの計算結果が異なった原因をメンバで調べたところ「計算に用いた出現回数に間違いがある」ことに気づき、正しい出現回数で計算し直すと同じ結果が得られた。表3のポイント数データから各ポイント数の出現回数の表を作成する際に、各ポイント数の出現回数を数えたり、正しいか否かを確認したりする作業に難があることが原因であることが分かった。そこで、各ポイント数の出現回数の表を作成する前に、表3のポイント数データに変更を加え、各ポイント数の出現回数を数えやすくかつ確認しやすい表現形式にしたい。どのような表現形式が適しているかをその理由とともに述べよ。

第4問 (80点)

次の文章について、以下の問いに答えよ。

情報セキュリティとは、情報の (ア) 機密性・(イ) 完全性・(ウ) 可用性の維持を指す。情報の機密性は、古くから軍事や政治の場面で常に求められている。この機密性を確保するための技術として暗号技術がある。もとの情報(平文)を暗号にすることを暗号化、暗号化された情報(暗号文)をもとの情報(平文)に戻すことを復号という。暗号化と復号で同じ鍵(共通鍵)を用いる暗号方式の1つである (エ) シーザー暗号は、各文字をアルファベット順で数文字分シフトして(ずらして)暗号文を作るものである。たとえば、“HAL”は“IBM”をアルファベット順で1文字前にずらした暗号文である。シーザー暗号では、アルファベット順でシフトする文字数が共通鍵となる。(カ) 共通鍵は送信者ごとに別々に必要となり、送信者と受信者がともに共通鍵を秘密に管理しなければならない。そこで、共通鍵を受け渡す過程での盗聴のリスクに加え管理が非常に煩雑になる。この問題を解決するために、暗号化のための鍵と復号のための鍵を別々にした公開鍵暗号が提案された。公開鍵暗号は、送信者は受信者が公開した鍵(公開鍵)で平文を暗号化し、受信者は自分が秘密にもつ鍵(秘密鍵)で復号する暗号方式である。また、公開鍵暗号の1つである RSA 暗号は、公開鍵と秘密鍵のどちらの鍵でも暗号化ができるという性質を有している。このため、受け取った電子文書がなりすましにより改ざんされたものであるか否かを確認する (ク) 電子認証に应用されている。

問1 (ア) 機密性、(イ) 完全性および(ウ) 可用性をそれぞれ説明せよ。

問2 (エ) シーザー暗号について、“HIRO”をアルファベット順で3文字後ろにずらした暗号文を答えよ。

問3 (オ)について、同じ人同士で送受信する際は同一の共通鍵を使うことにした場合、機密性を確保しつつ4人の間で相互に送受信するには6個の共通鍵が必要である。 n を2以上の整数とすると、 n 人の間では何個の共通鍵が必要か答えよ。なお、その答えの導出過程も述べること。

問4 図1は、(ク) 電子認証のしくみを示している。図1の認証局(CA)とは公開鍵を管理し正しい送信者であることを保証する機関である。また、要約文とはプログラムにより平文の特徴的な部分を生成した文である。そこで、図1の①～⑥にあてはまる適切な語句を選択肢(a)～(j)から選べ。なお、同じ番号には同じ選択肢が対応するものとする。さらに、同じ選択肢が異なる番号に対応することもないものとする。

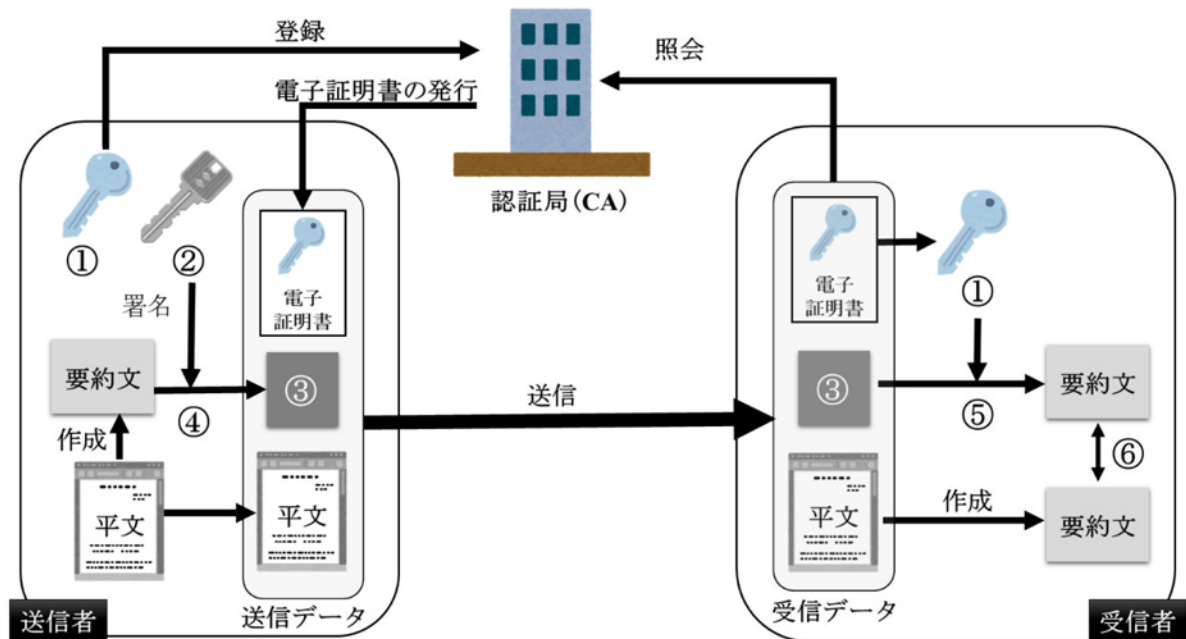


図1 電子認証のしくみ

選 択 肢

- | | | | |
|----------------------|----------|-------------|-------------|
| (a) 暗号化 | (b) 復号 | (c) 送信者の公開鍵 | (d) 受信者の公開鍵 |
| (e) 電子署名
(デジタル署名) | (f) 電子文書 | (g) 送信者の秘密鍵 | (h) 受信者の秘密鍵 |
| (i) 比較 | (j) 複写 | | |