

高等学校 情報

(解答はすべて、解答用紙に記入すること)

1 次の(1)～(11)の問いに答えよ。

(1) 10進数200を2進数および16進数で記せ。

(2) 10進数の分数 $\frac{11}{32}$ を16進数の小数で記せ。

(3) 次の10進数の小数のうち、2進数で表すと無限小数になるものはどれか。すべて選び記号で答えよ。

ア 0.8 イ 0.5 ウ 0.375 エ 0.125 オ 0.05

(4) 32ビットで表現できるビットパターンの個数は24ビットで表現できる個数の何倍か答えよ。

(5) 負数を2の補数で表す8ビットの数値がある。この値を10進数で表現すると-100である。この値を符号なしの数値として解釈すると、10進数ではいくらか答えよ。

(6) 16進数2AB5を4倍して16進数で記せ。

(7) TCP/IP階層モデルにおいて、TCPが属する層はどれか。適切なものを選び記号で答えよ。

ア アプリケーション層 イ インターネット層
ウ トランスポート層 エ リンク層
オ データリンク層

(8) TCP/IPネットワークにおいて、ネットワークの疎通確認に使われるものはどれか。適切なものを選び記号で答えよ。

ア fps イ DHCP ウ DNS エ ping オ FTTH

(9) 次の①～④の特徴をすべてもつ画像フォーマットはどれか。適切なものを選び記号で答えよ。

- ① 静止画像を対象としている。
- ② RGBの24ビットデータを輝度信号と色信号にわけて記録するので、写真などの自然色画像に適している。
- ③ 人間の視覚は高周波になるほど鈍感で、低周波では敏感であることを利用し、低周波部分ほど細かく量子化する。
- ④ 非可逆圧縮によりファイル容量を小さくできる。

ア GIF イ BMP ウ JPEG エ MPEG

(10) ある画像を 1200dpi のスキャナで入力し、画素数を変えずに 300dpi のプリンタで出力した。このときの入力画像と印刷結果の画像の大きさに関して面積比を答えよ。

(11) 通信速度が 192 [kbps] のネットワークを用いてダウンロードしながら再生する場合、符号化速度が 256 [kbps] の音声データ 2.4 [Mバイト] を途切れることなく再生するためには、再生開始前のデータのバッファリング時間として最低何秒間が必要か。

ただし、1 [kbps] = 1000 [bps]、1 [Mバイト] = 1000 [kバイト] とし、通信は常時理論値で行われるものとする。(途中の式も書くこと)

2 次の(1)～(5)の問いに答えよ。

(1) 次のア～エのうち、購入したソフトウェアの取扱いに関する記述として著作権法(平成26年6月改正)に照らして、最も適切なものを一つ選び記号で答えよ。

ア 複製をとることは、一切認められていない。

イ 個人が所有しているなど特定のコンピュータであれば、ソフトウェアをより効果的に利用するなどの目的で、改良を加えることは認められている。

ウ 営利を目的としない学校などの教育機関においては、ソフトウェアの複製は無制限に認められている。

エ 他者にソフトウェアを売った後、このソフトウェアの作成者の許可が無くても、自分のもっているコンピュータにインストール済みのこのソフトウェアを使い続けることは認められている。

(2) 次のア～エのうち、著作権法(平成26年6月改正)に違反しない行為の記述として最も適切なものを一つ選び記号で答えよ。ただし、いずれの行為も著作権者の許可を得ていないものとする。

ア 営利を目的としない個人のWebページに、新聞の記事を転載する。

イ 厚生労働白書の調査統計データをそのまま引用するとともに、図表化したものを社内刊行物に記載する。

ウ 雑誌の記事をコピーし、社内掲示板に掲示し内容を社員に周知する。

エ 自社製品のパンフレットのために使用している風景写真を、社外における他製品に関するプレゼンテーション資料として用いる。

(3) 学校その他の教育機関における著作物の複製に関する記述のうち、著作権法(平成26年6月改正)に違反しない行為の記述として最も適切なものを一つ選び記号で答えよ。

ア 生徒がWebサイトから「コンピュータのできるまで」の図を印刷して持ってきたので、複製して授業で配り、利用した。

イ 授業参観で参観者に授業で使用する教科書の複製を配り、利用した。

ウ 授業で使用する著作物を校内LANサーバに蓄積した。

エ 教科研究会で授業実践を発表し、授業で利用した市販の問題集の複製を配り、利用した。

(4) 次のア～ウはマルウェアに関する説明である。説明ア～ウとマルウェアの分類の適切な組合せを解答群より選び、A～Fの記号で答えよ。

ア 感染したコンピュータが、外部からの指令によって、様々な妨害行為や破壊行為等を行う。

イ コンピュータに設けられた通信経路のうち、正規の経路や手段を経ずにシステムへ侵入するために設けられる接続経路である。

ウ 利用者によるパソコンの使用状況や利用者に関する情報を収集する。

解答群

| | ア | イ | ウ |
|---|--------|--------|--------|
| A | スパイウェア | バックドア | ボット |
| B | スパイウェア | ボット | バックドア |
| C | バックドア | スパイウェア | ボット |
| D | バックドア | ボット | スパイウェア |
| E | ボット | スパイウェア | バックドア |
| F | ボット | バックドア | スパイウェア |

(5) デジタル署名などに用いるハッシュ関数の特徴として、誤っているものを1つ選び記号で答えよ。

ア メッセージダイジェストの長さはメッセージの長さによって異なる。

イ メッセージが一文字でも変われば、メッセージダイジェストも異なる。

ウ メッセージダイジェストからメッセージを復元することは困難である。

エ 同じメッセージダイジェストを出力する異なる二つのメッセージを求めることは、事実上不可能である。

3 高等学校学習指導要領（平成21年3月告示）に示されている内容について、下の（1）～（3）の問いに答えよ。

（1）次の文は、共通教科情報の科目「情報の科学」2 内容（1）イ 情報通信ネットワークの仕組み について示したものです。文中の にあてはまる言葉を書きなさい。

情報通信ネットワークの構成要素、 の役割、情報通信の仕組み及び情報セキュリティを確保するための方法を理解させる。

（2）次の文は、共通教科情報の科目「社会と情報」2 内容（3）イ 情報セキュリティの確保 について示したものです。文中の にあてはまる言葉を書きなさい。

個人認証と暗号化などの技術的対策や の策定など、情報セキュリティを高めるための様々な方法を理解させる。

（3）共通教科情報の科目「社会と情報」2 内容（1）ウ 情報の表現と伝達について は、「情報を分かりやすく表現し効率的に伝達するために、情報機器や素材を適切に選択し利用する方法を習得させる。」とある。3 内容の取扱い では、ウについては、実習を中心に扱うとある。この場合どのような評価活動を取り入れることとされているか、簡潔に述べよ。

4 データベースに関する次の(1)～(5)の問いに答えよ。

あるカルチャーセンターでは受講生や講座の管理は、従来次のレコードで管理されている。これをデータベース化する。

| | | | | |
|--------|-------|-------|-----|------|
| 受講生コード | 受講生名前 | 講座コード | 講座名 | 担当講師 |
|--------|-------|-------|-----|------|

(1) データベース化にあたって従来のレコードの項目のみを正規化する場合、正規化されたデータベースのテーブルのレコードとして、最も適切な分け方はどれか、ア～エの記号で選び答えよ。
 なお、データベース化に関する条件は以下のa～dのとおりである。

- a 受講生コードと講座コードが、レコードを検索するためのキーとなる。
- b 受講生コードから講座が参照できなければならない。
- c 1つの講座の担当講師は1名である。
- d 受講生は複数の講座を受講することが可能である。

ア

| | | |
|--------|-------|------|
| 受講生コード | 受講生名前 | |
| 講座コード | 講座名 | 担当講師 |

イ

| | | |
|--------|-------|-------|
| 受講生コード | 受講生名前 | 講座コード |
| 講座名 | 担当講師 | |

ウ

| | | | |
|--------|-------|-----|------|
| 受講生コード | 受講生名前 | | |
| 受講生コード | 講座コード | 講座名 | 担当講師 |

エ

| | | |
|--------|-------|------|
| 受講生コード | 受講生名前 | |
| 講座コード | 講座名 | 担当講師 |
| 受講生コード | 講座コード | |

(2) 関係データベースを構築するに当たり、データの正規化を行う目的について簡潔に述べよ。

(3) 複数の利用者が同一データベースに同時にアクセスする処理のうち、データの整合性を保つための対策が不要な処理はどれか。一つ選び記号で答えよ。

- ア オンラインショッピングの申し込み処理
- イ 図書館の検索処理
- ウ 銀行口座の振込処理
- エ ホテルの宿泊予約処理

(4) 関係データベースの操作について、次のような操作を行う関係演算の名称について適切なものをそれぞれ一つ選び記号で答えよ。

- ① 表から条件に合致する特定の列を取り出し新しい表を作る演算操作
- ② 表から条件に合致する特定の行を取り出し新しい表を作る演算操作

- ア 結合 イ 射影 ウ 選択 エ 差

(5) データベースの障害回復に用いられ、データベースの更新に関する情報が格納されているファイルの名前を答えよ。

- 5 ある会社Xではインターネットを利用して商取引を行う。このときの暗号技術に関する次の(1)～(4)の問いに答えよ。

(1) 会社Xは顧客n人と取引をする。ネットワーク上で使用される共通鍵暗号方式と公開鍵暗号方式について次の表の(ア)、(イ)にあてはまる数を答えよ。

α 方式、 β 方式は、共通鍵暗号方式か公開鍵暗号方式を示す。

| | α 方式 | β 方式 |
|----------------------|-------------|------------|
| 暗号化と復号に用いる鍵 | 同じ鍵 | 違う鍵 |
| 代表的な方式 | DES等 | RSA等 |
| 会社が秘密に管理しなければならない鍵の数 | (ア) 個 | (イ) 個 |

(2) 会社XではSSLを利用して通信販売を行う。SSLの手順の説明は以下のとおりである。会社側は認証局を利用して、公開鍵と秘密鍵を入手している。(ウ)～(オ)にはいる鍵の名称の正しい組み合わせを解答群より選び、A～Eの記号で答えよ。

SSLの手順

- ① 会社Xはアクセスしてきた顧客に認証局のサーバ証明書と会社Xの(ウ)を送付する。
- ② 顧客は(エ)を作成する。
- ③ 顧客は(ウ)を利用して(エ)を暗号化し、会社Xへ送付する。
- ④ 会社Xは(オ)を利用して(エ)を復号する。
- ⑤ 顧客と会社Xは(エ)を利用して取引を行う。

解答群

| | (ウ) | (エ) | (オ) |
|---|-----|-----|-----|
| A | 公開鍵 | 秘密鍵 | 共通鍵 |
| B | 共通鍵 | 公開鍵 | 秘密鍵 |
| C | 公開鍵 | 共通鍵 | 秘密鍵 |
| D | 秘密鍵 | 公開鍵 | 共通鍵 |
| E | 秘密鍵 | 共通鍵 | 公開鍵 |

- (3) SSLでは会社Xのサーバ証明書を送付する。サーバ証明書の利用手順は以下のとおりである。
(カ)～(ク)にはいる鍵の名称の正しい組み合わせを解答群より選び、A～Eの記号で答えよ。

- ① 会社Xはアクセスしてきた顧客に、認証局からの会社Xのサーバ証明書を送信する。証明書にはX社の(カ)と、認証局の(キ)で証明書のハッシュ値を暗号化した電子署名が記載されている。
- ② 電子署名は認証局の(ク)で復号され、ハッシュ値の検証が行われる。

解答群

| | (カ) | (キ) | (ク) |
|---|-----|-----|-----|
| A | 公開鍵 | 秘密鍵 | 秘密鍵 |
| B | 秘密鍵 | 公開鍵 | 秘密鍵 |
| C | 公開鍵 | 公開鍵 | 秘密鍵 |
| D | 秘密鍵 | 秘密鍵 | 公開鍵 |
| E | 公開鍵 | 秘密鍵 | 公開鍵 |

- (4) 問い(3)の手順で検証結果が正しかった場合、確認できることがらは何か。A～Dより2つ選び記号で答えよ。

- A サーバ証明書が改ざんされていないこと。
B サーバ証明書が会社Xと取引実績のある顧客のものであること。
C サーバ証明書が認証局の発行審査を受けた会社Xのものであること。
D サーバ証明書が盗み見されていないこと。

6 あるロボットに関する次の記述を読み、下の(1)、(2)の問いに答えよ。

ロボットは以下の命令を実行する機能をもつ。

命令A「歩く」前に1マス進む

命令B「走る」前に2マス進む

命令C「右」進行方向に向かって右に90度回転する

命令D (命令A、B、Cのうち2つを組み合わせて作る)

命令E すべての命令の終了 (最後に必ず1回のみ使用する)

【命令Dの説明】

命令Dは、2つの命令を組み合わせて作成する新しい命令である。この2つの命令は同じものでもよい。A「歩く」A「歩く」を組み合わせた場合、「前に2マス進む」という命令になる。

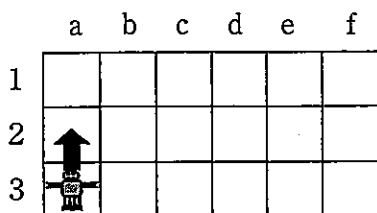
【命令使用時のルール】

すべての命令に関して同じ方向に進むときは、進むマスの多い命令を先に使用する。命令A「歩く」の後に命令B「走る」を使うことはできない。命令Dを作成するとき、また作成された命令Dの使用もこのルールに従う。

【例】

このロボットに命令A、B、C、Eを使い下の図のコースのa3のマスを出発させ、f1に到着させる。このとき、最少の命令数で到着させる命令順を示す。↑は最初の進行方向を示す。

コース

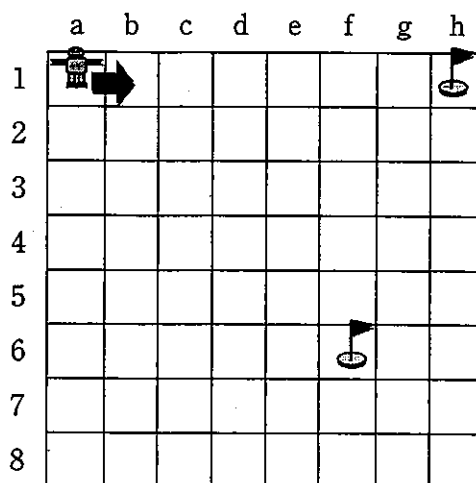


命令順

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | → | C | → | B | → | B | → | A | → | E | → | → | → |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

(1) このロボットを、命令A、B、C、Eのみを使い下の図を移動させる。a1のマスを開始し、2か所の旗（f6・h1）のマスを通りf8のマスに到着させる。このとき、①～③の問いに答えよ。

- ① 最少の命令数でのf8のマスに到着させる方法は何通りあるか答えよ。
- ② 旗のマスで必ず停止させる場合、最少の命令数でf8のマスに到着する方法は何通りあるか答えよ。
- ③ 旗のマスで必ず方向転換させる場合、最少の命令数の手順を命令A、B、C、Eの記号を用いて【例】の命令順にならって答えよ。



(2) ロボットに、命令Dを加え(1)のコースを最少の命令数で移動させる。このとき、次の①～③の問いに答えよ。

- ① 新しい命令Dは命令A、B、Cのうち、どの2つの命令を組み合わせたものか、命令順に答えよ。
- ② 命令Dを使って、最少の命令数でf8のマスに到着させる方法は何通りあるか答えよ。
- ③ 最少の命令数でf8のマスに到着させるとき、命令Dが連続して使用される手順を命令A～Eを用いて【例】の命令順にならって答えよ。