第 4 回大学情報入試全国模擬試験#005B

# 情報

試験時間 45 分

- 試験開始の合図があるまで、本冊子を開いてはいけません。
- 出題内容は、以下の通りです。

| 問題 | 選択方法 | 分野 |
|---|---|---|
| 第 1 問 | 必答 | 共通 |
| 第 2 問 | 必答 | 情報の科学 |
| 第 3 問 | 必答 | 社会と情報 |

- 試験中に問題冊子・解答用紙の印刷不鮮明、落丁・乱丁・汚れに気がついた場合は、手を挙げて監督者に知らせてください。
- 問題冊子の余白などは、適宜、計算などに利用して構いません。
- 試験終了後、問題冊子は持ち帰ってください。

2016 年 2 月 27 日
情報入試研究会
情報処理学会 情報入試 WG

（このページのこの下は白紙。計算に用いてよい。）

## 第 1 問　（必答問題）

下の問い（問 1 ～ 問 6）に答えよ。

**問 1**　公開鍵暗号方式を使った電子署名に関する文章として、不適切なもの 1 つを次の解答群の選択肢から選べ。

解答群

**ア** 暗号化されていても、電子署名がされていないことがある。

**イ** コンピュータに保存されたいかなるファイルに対しても、電子署名をすることができる。

**ウ** 電子署名された文書を読むためには、暗号を復号する必要がある。

**エ** 電子署名をされた文書の署名を確認するには、そのためのソフトウェアが必要になる。

**オ** 文書全体に対して電子署名をする代わりに、文書のハッシュ値に対して電子署名をすることがある。

**問 2**　「インタフェース」の説明として最も適切なものを、次の解答群の選択肢から選べ。

解答群

**ア** コンピュータと周辺機器を接続する部分のこと。

**イ** 電子商取引で使われるセキュリティ技術のこと。

**ウ** 人間の顔に基づいてユーザ認証を行う技術のこと。

**エ** ネットワーク上のユーザ同士をつなぐ仕組みのこと。

**オ** 複数の LAN を統合した、中規模のネットワークのこと。

**問 3**　ディジタルカメラで撮影した画像と油絵を比較したときの、ディジタルカメラで撮影した画像が持つ利点を書き出した。利点として適切なものを次の解答群の選択肢からすべて選べ。

解答群

**ア** 時間がたっても色が劣化しない。
**イ** いくらでも拡大して細かいところを見ることができる。
**ウ** コピーすることが容易である。
**エ** 隠れて写っていない箇所も必要なら見ることができる。

**問 4**　情報機器やネットワークサービスを利用する際に存在する (1)〜(5) のような危険性に対して、それに対する態度としてもっとも関連が強いものを、それぞれ下の解答群の選択肢から選べ。ただし、各選択肢は 1 度しか使用してはいけない。

(1) 暗号通信でない通信は他人に内容を知られる危険性がある。
(2) 自分が撮影した写真のインターネットへの公開は、他人の肖像件等を侵す危険性がある。
(3) 自分が撮影した写真のインターネットへの公開は、自分の所在情報を晒してしまう危険性がある。
(4) 不用意にアプリケーションを導入すると自分の住所録などを盗まれる危険性がある。
(5) 広告などのメッセージが多数送られて来て重要なメッセージが紛れる危険性がある。

解答群

**ア** 位置情報が使用される内容・範囲に注意を払う。
**イ** ソフトウェアがどのような情報アクセス権限を要求してくるかに注意を払う。
**ウ** 自分が公開する情報と他人のプライバシーの関わりに注意を払う。
**エ** メールアドレスを用途に応じて使い分ける。
**オ** ブラウザのアドレス入力欄の鍵マークや URL スキームに注意を払う。

**問 5**　親方は、弟子 2 人を連れて自宅から仕事場へ車で出かけ、仕事場で製品製作を行い、弟子とともに車で自宅に戻ってくる。自宅と仕事場の間の車での移動には片道 1 時間かかる。製品製作は、規格化された工程に従って単独作業で行われる。1 人が同時に 2 個以上の製品製作を手がけることはない。その日はそれぞれの工程時間が 2 時間、3 時間、4 時間、5 時間である合計 4 個の製品製作を行うことになっていた。これらの製品製作を行う順序や誰が担当するかについては何の制約もない。車の乗り降り、仕事場での準備や片付け、作業の切り替えなどに時間がかからないものとして、次の文中の［（1）］と［（2）］に入る数値を、下の解答群の選択肢から選べ。

仕事場で弟子 2 人だけで製品製作にあたる場合、自宅を出てから仕事場で 4 個の製品製作を終えて自宅に戻ってくるまでの最短時間は［（1）］時間である。

仕事場で親方も弟子 2 人も製品製作にあたる場合、自宅を出てから仕事場で 4 個の製品製作を終えて自宅に戻ってくるまでの最短時間は最短で［（2）］時間である。

解答群

| | | | | |
|---|---|---|---|---|
| **ア** 7 | **イ** 8 | **ウ** 9 | **エ** 10 | **オ** 11 |
| **カ** 12 | **キ** 13 | **ク** 14 | **ケ** 15 | **コ** 16 |

**問 6**　図 1 のように、正方形の枠に収まる大きい直角二等辺三角形 1 つと小さい直角二等辺三角形 2 つの計 3 つのパネルを組み合わせて信号を作る。(大きい直角二等辺三角形のパネルの等辺の長さは枠の正方形の辺の長さと等しく、小さい直角二等辺三角形のパネルの底辺の長さは枠の正方形の辺の長さと等しい。) 信号が遠くからも見えるように、枠は塔の壁に固定されている。3 つのパネル全てを重ならないように枠にはめて信号を作る。信号を作る 3 つのパネルの表面と裏面には、遠くから識別できる 7 種類のパターン (P1～P7 と呼ぶ) のいずれかが描かれており、パネルに描かれるパターンは表裏で異なる場合がある。3 つのパネルを枠のどの位置にどちらを表にしてはめるかにより、異なる信号を作ることができる。

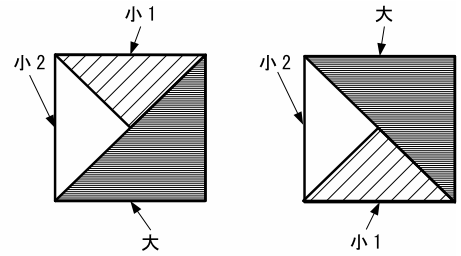


図 1　直角二等辺三角形のパネルによる信号の例 (2 種類の異なる信号)

信号のパネルのパターンは遠くからも見分けられるが、同じパターンのパネルが隣接している場合は、その境界は遠くからは見分けられないものとする。例えば、図 2 に示す 2 つの信号は、区別できないので同一の信号とみなす。

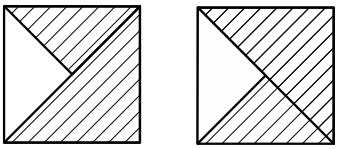

図 2　見分けられないパネルの組合せの例

3 つのパネルの表裏へのパターンの割り当てによって，作ることのできる信号の種類の数を例示した次のページの表を作成した。パターンの割り当てと信号の種類の数の組合せが間違っているものをすべて選べ。

| | 大 | | 小 1 | | 小 2 | | 信号の |
|---|---|---|---|---|---|---|---|
| | 表 | 裏 | 表 | 裏 | 表 | 裏 | 種類の数 |
| **ア** | P1 | P1 | P2 | P2 | P3 | P3 | 16 |
| **イ** | P1 | P1 | P2 | P2 | P2 | P2 | 4 |
| **ウ** | P1 | P1 | P1 | P1 | P2 | P2 | 8 |
| **エ** | P1 | P4 | P3 | P5 | P6 | P7 | 64 |
| **オ** | P1 | P1 | P3 | P5 | P3 | P7 | 28 |

## 第 2 問　（必答問題）

図 3 のような動き方だけができるロボットが、ます目に区切られた長方形の盤の中にいる。ロボットは回転することや、ます目の領域からはみ出して動くことはできない。最初、このロボットをどこかのます目に置くものとして、他のます目に到達するまでに、何ステップ動く必要があるかを調べる方法を考える。

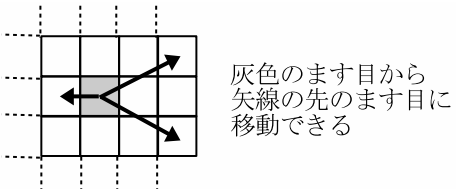


図 3　ロボットの動き方

この処理を示すために、図 4 のような 4×4 のます目に区切られた盤を用いて説明する。

- 図 4 の (a) のように、ロボットを最初に置くます目に「0」を記入する。
- 図 4 の (b) 以降のように、前の手順で数「i」を記入したます目から、ロボットが 1 ステップで動けるます目にまだ何も記入されていないなら数「i+1」を記入する。
- すべてのます目に数が記入されるか、または、それ以上新たなます目に数を記入できないならば、終りにする。

図 4 の (h) は、4×4 のます目で左端の上から 2 ます目にロボットを置いて最後まで処理をおこなった結果である。

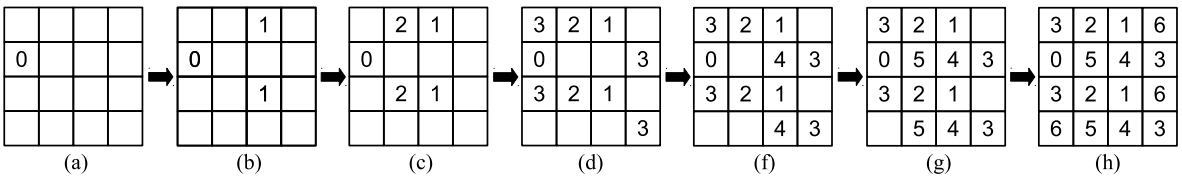


図 4　4×4 のます目への記入

次に、図 5 のような 4×6 のます目について、左上隅にロボットを置いて同じように最後まで処理することを考える。

**問 1**　図 5 の「X」のます目に入る整数を、次のページの解答群 1 の選択肢から選べ。

**問 2**　図 5 で「7」が記入されるます目の個数を、下の解答群 1 の選択肢から選べ。

**問 3**　図 5 のます目に記入される最も大きい数を、下の解答群 1 の選択肢から選べ。

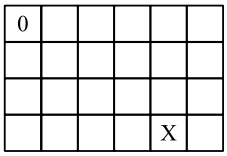


図 5　4×6 のます目への記入

解答群 1

**ア** 1　　**イ** 2　　**ウ** 3　　**エ** 4　　**オ** 5　　**カ** 6
**キ** 7　　**ク** 8　　**ケ** 9　　**コ** 10　　**サ** 11

**問 4**　上の処理が必ず止まり無限に続くことはない理由を 20 文字以内で述べよ。

**問 5**　次の文は、「すべてのます目に対して、数が記入されたら、その数がロボットがそこへ到達するのに必要な最も少ないステップ数である」ということの説明である。 (1) ～ (6) に入る最も適切なものを、下の解答群 2 の選択肢から選べ。

「条件 P: 記入されている数より (1) ステップ数で到達できる」を満たすます目が存在すると仮定する。条件 P を満たすます目で、ステップ数が最少のます目 Y を選び、Y に記入されている数を i、Y までのステップ数を k とする (仮定から i (2) k) 。最初のます目から Y に至る最短経路のます目を $M_0, M_1, \cdots, M_k(= Y)$ と名づける。Y は条件 P を満たすます目でステップ数（k）が最も (3) ものなので、$M_{k-1}$ には (4) が記入されている。$M_{k-1}$ から Y には (5) ステップで到達できることから、Y には i が記入されており、これが (6) と等しいはずである。これは i (2) k に矛盾する。従って、記入されている数よりも少ないステップで到達できるます目は存在しない。

解答群 2

**ア** 多い　　**イ** 等しい　　**ウ** 少ない　　**エ** ＜　　**オ** ＞
**カ** i　　**キ** k　　**ク** k+1　　**ケ** k−1　　**コ** 1

## 第 3 問　（必答問題）

情報セキュリティに関する次の文章を読み、下の問い（問 1〜問 8）に答えよ。

近年、情報セキュリティを脅かすような事象が頻発している。情報セキュリティを高めるための方法としては、技術的方法以外にもさまざまなものがある。また、いくら技術的に頑丈なシステムを構築しても、ユーザのセキュリティ意識が低いと、そこが穴となってセキュリティ事故につながることが多々ある。

セキュリティを確保するため、ID とパスワードで本人認証を行なうという方法は広く普及している。この方法の技術的な脆弱(ぜいじゃく)性としては、パスワードに使うことができる文字種や文字数の制限がある。パスワードを 4 文字とし 0 から 9 の数字だけが使える場合は、最大 [ (1) ] 通りの組み合わせしかできない。文字数を 6 文字としても、使える文字が 0 から 9 の数字である場合は，最大 [ (2) ] 通りの組み合わせしかない。文字数を 4 文字としても、0 から 9 の数字に加えてアルファベットの大文字 26 文字と記号 4 文字も使えるようすれば、最大 [ (3) ] 通りの組み合わせが可能になり、安全性が大幅に高まる。さらに、アルファベットも大文字に限定せず大文字と小文字を別個に識別したり、文字数を増やしたりすれば、いっそう安全性を高めることが可能になる。一方で、このようにしてパスワードの技術的な安全性を高めても、(a)ユーザの設定によっては、一気に脆弱性が高まる。従来、パスワードは、「定期的に変更する」「紙などにメモしない」「システム管理者から提供されたものは直ちに変更する」のが当たり前と言われていた。しかし、こうすることによって、(b)かえって脆弱性が高まってしまうという指摘もあり、パスワード管理の運用方針を変更する組織がでてきた。強固なパスワードを維持できていたとしても、ソーシャルエンジニアリングにより正規のユーザになりすましてシステムに侵入されるという危険性もあるので、継続的な対策が必要である。

パスワードだけでなく、バイオメトリック生体認証（生体認証）を併用するシステムも数多く存在する。(c)バイオメトリック生体認証（生体認証）を使用することには危険性も存在するが、併用することでセキュリティを高めることができる。

Web ベースのシステムで、ID やパスワードを入力しなければならないようなページは SSL/TLS でデータの送受信を行うべきである。しかし、(d)SSL/TLS で通信していれば安全かといえば、必ずしもそうではない。使用するコンピュータには、ウィルス対策ソフトを入れるなど、(e)マルウェアによる攻撃への対策を講じなければならない。このように、組織においてセキュリティを高めるためには、各部署がばらばらの基準で場当たり的に行なうことがあってはならず、(f)組織の情報資産を守るための方針や基準

を明文化しておく必要がある。また、(g)明文化するだけでなく、それを実行するとともに、それがきちんと機能しているか確認し、必要があれば改善策を検討し、方針や基準を修正するというサイクルを常に循環させなければならない。

**問 1**　文章中の (1) ～ (3) に入る数を、次の解答群の選択肢から選べ。

解答群

| | | | |
|---|---|---|---|
| **ア** 1,000 | **イ** 2,560 | **ウ** 10,000 | **エ** 25,600 |
| **オ** 100,000 | **カ** 256,000 | **キ** 1,000,000 | **ク** 2,560,000 |

**問 2**　下線部 (a) の原因として考えられる理由を、20 文字以内で答えよ。

**問 3**　下線部 (b) の原因として考えられる理由を、20 文字以内で答えよ。

**問 4**　下線部 (c) の理由として、最も適切なものを次の解答群の選択肢から選べ。

解答群

**ア** 簡単に偽装できるから。
**イ** 人体に悪影響があるから。
**ウ** 認証システムの信頼性が低いから。
**エ** 認証情報が漏洩してもその情報を変更できないから。
**オ** 認証システムの導入には莫大なコストがかかるから。

**問 5**　下線部 (d) の理由として考えられる事例として、適切なものを次の解答群の選択肢からすべて選べ。

解答群

**ア** ID とパスワードが盗まれてなりすまされる。
**イ** キーロガーなどで入力内容を盗まれる。
**ウ** 公開鍵を使って通信内容を解読される。
**エ** 通信内容が平文でやり取りされている。
**オ** 偽のサイトへアクセスさせられている。

**問 6**　下線部 (e) への対策として、適切なものを次の解答群の選択肢からすべて選べ。

解答群

**ア** スクリーンセーバーを設定する。
**イ** セキュリティパッチを適用する。
**ウ** OS のバージョンアップを行わない。
**エ** ユーザに対するセキュリティ教育を行う。
**オ** ユーザによるアプリケーションのインストールを認めない。

**問 7**　下線部 (f) を表す用語として最も適切なものを、次の解答群の選択肢から選べ。

解答群

**ア** 情報セキュリティエッセンシャル
**イ** 情報セキュリティガード
**ウ** 情報セキュリティコード
**エ** 情報セキュリティプロシージャ
**オ** 情報セキュリティポリシー

**問 8**　下線部 (g) を表すサイクルの名称として最も適切なものを、次の解答群の選択肢から選べ。

解答群

**ア** BIOS　　**イ** DHCP　　**ウ** MECE　　**エ** PDCA　　**オ** SWOT

**（これで、第 4 回大学情報入試全国模擬試験 B は終り。）**

（このページのこの下は白紙。計算に用いてよい。）

第 4 回大学情報入試全国模擬試験#005B


情報入試研究会

（共催）情報処理学会 情報処理教育委員会

http://jnsg.jp/


@jnsgsec