

平31 高等学校情報 (5枚のうち1)

(解答はすべて、解答用紙に記入すること)

I 次の各説明文に該当するものをそれぞれア～エから1つ選んで、その符号を書きなさい。

1 2018年12月からはじまる新たな衛星放送の視聴に対応した、4Kディスプレイの解像度。

ア 1024 × 768 イ 1920 × 1080 ウ 3840 × 2160 エ 7680 × 4320

2 HTMLなどの色指定で利用される16進数のカラーコードで、「#FFFF00」で表現される色。

ア 青 イ 黄 ウ 黒 エ 緑

3 電子メールにおいて、テキストだけでなく、音声や画像なども扱えるようにした規格。

ア HTML イ IMAP ウ MIME エ SMTP

4 マルチメディアに関するデータのうち、可逆圧縮のファイル形式。

ア JPEG イ MP3 ウ MPEG エ PNG

5 日本では1964年の東京オリンピックをきっかけに公共施設に導入され、何らかの情報や注意を文字でなく図で表現することで、言語に制約されずに直感的に伝達できるように表現した絵文字や図記号。

ア アイコン イ ピクトグラム ウ ヒストグラム エ ユニバーサルデザイン

6 ある言葉に対する同義語や広義語など、言葉どうしの意味や関係を定義づけたもの。

ア エンコード イ カテゴリ ウ シソーラス エ データベース

7 アイデアや意見を小さなカードに記し、それらをまとめる過程で新たな関係性を見つけ出して問題解決をはかる方法。

ア KJ法 イ NM法 ウ マッピング法 エ プレインストーミング

8 交通事故の減少や交通渋滞の軽減など、交通問題の解決に取り組むためのシステム。

ア HEMS イ ITS ウ POS エ RSS

9 インターネット上の取引所で他者や法定通貨と交換できたり、物品やサービスの対価に使用可能な財産的価値。

ア 仮想通貨 イ クレジットカード ウ 電子マネー エ プリペイドカード

10 日本政府が第5期科学技術基本計画で提唱した、仮想空間と現実空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会をめざす、科学技術政策の一連の取組。

ア Industry 4.0 イ IoT 2.0 ウ Science 2.0 エ Society 5.0

II 次の各問いに答えなさい。

1 11ビットのデータのそれぞれのビットに、先頭から順に b_0, b_1, \dots, b_{10} と名前をつける。これに、チェック符号としての4ビット h_0, h_1, h_2, h_3 を、次の①～④のルールで付加する。

① h_0 は、 $b_4, b_5, b_6, b_7, b_8, b_9, b_{10}$ に対する偶数パリティ

② h_1 は、 $b_1, b_2, b_3, b_7, b_8, b_9, b_{10}$ に対する偶数パリティ

③ h_2 は、 $b_0, b_2, b_3, b_5, b_6, b_9, b_{10}$ に対する偶数パリティ

④ h_3 は、 $b_0, b_1, b_3, b_4, b_6, b_8, b_{10}$ に対する偶数パリティ

(1) 11ビットのデータが10000100110のとき、 $h_0 \sim h_3$ をそれぞれ書きなさい。

(2) 通信結果をチェックすると、上の①と③のルールにあてはまっていないことがわかり、 $b_0 \sim b_{10}$ の11ビットのうち、どこか1ビットに誤りが発生していることが判明した。誤りが発生したビットの名前を書きなさい。

2 ある携帯電話会社のパケット通信サービスでは、1パケットあたり税込で0.2円である。この条件で、260KBのデータを受信する場合、パケット通信料金を計算しなさい。なお、1パケット = 128Bで、各パケットには24Bのヘッダ部分が存在するものとする。また、1KB = 1024Bとする。

3 4ビットの2進数 $(1110)_2 - (1010)_2$ を、補数を利用して計算しなさい。なお、答えは4ビットで書き、計算過程も示すこと。

平31 高等学校情報 (5枚のうち2)

(解答はすべて、解答用紙に記入すること)

Ⅲ 次の文章を読み、あとの問いに答えなさい。

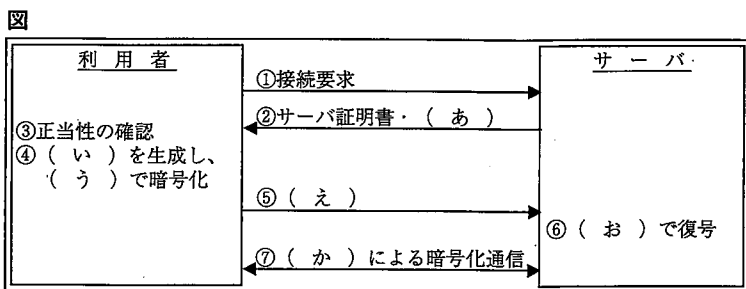
(a)情報セキュリティを脅かす事象が頻発する近年、(b)組織において情報資産を守るための方針や基準を定め、それが適切に機能しているかを確認しながら、改善策を検討・修正する対策を講じるとともに、研修等とおして情報機器の適切な活用方法を利用者に周知することが重要である。

まず、利用者を認証する技術の中でも ID と(c)パスワードによる方法は広く普及しているが、(d)あるシステムで利用するこれらの組合せを他のシステムでも使い回すことにより、情報漏洩の危険性を高めてしまう事象が増えている。利用者にはこのような使い回しを避けるとともに、サービス運営者には(e)複数の異なる認証方式を組み合わせる仕組みを導入することや、定期的なパスワード変更の運用方針を見直すことが求められる。

また、インターネットで情報をやり取りする際、第三者にその内容を読み取られる危険性が高い。このため、利用者は機密情報を入力する場合、(f)表示されている Web サイトの URL が「https」ではじまり、ブラウザで鍵マークが表示された暗号化通信がなされていることを十分に確認しなければならない。なお、(g)無線 LAN でも暗号化通信が用いられているが、最も安全性が高いと評価されてきた WPA2 の規格にも、2017 年に欠陥が見つかっている。このため、暗号化技術に加え、(h)アクセスポイントに登録された端末しか接続できない設定や SSID を表示しない設定を併用したり、関連機器のファームウェアを更新することなどが対策として必要である。

さらに、メールの添付ファイルを開かせたり、悪意ある Web サイトにアクセスさせることにより、ウイルスに感染させるといった OS 等の(i)プログラム上の不具合や設計ミスによる欠陥をねらった事象が増加している。なかでも、(j)端末内のファイルを開けないようにしたり、端末の操作ができないようにロックした上で、復旧を名目に金銭を要求する悪質な犯罪が、大きな被害をもたらしている。利用者自身が、メールの添付ファイルやアクセスする Web サイトに対して十分に確認するのはもちろんのこと、日頃からファイルのバックアップを取ることや、ウイルス対策ソフトの定義ファイルや OS 等の更新プログラムについて、たえず最新のものを適用できるように組織でも十分な環境づくりが求められる。

- 下線部(a)について、「情報セキュリティの3要素」として適切なものを次のア～オから3つ選んで、その符号を書きなさい。
ア 完全性 イ 可用性 ウ 保守性 エ 機密性 オ 信頼性
- 下線部(b)について、この名称を書きなさい。
- 下線部(c)について、10進数の数字とアルファベット小文字を使用して8桁でパスワードを作成する場合、同じ桁数で10進数の数字だけで作成した場合に比べ、最大で()の8乗倍の組合せを設定することができる。()に適切な数字を書きなさい。なお、パスワードを設定する際、各桁に同じ文字等を何度利用してもよいものとする。
- 下線部(d)について、この現状を悪用し、不正アクセスを試みる手法の名称として適切なものを次のア～エから1つ選んで、その符号を書きなさい。
ア ゼロデイ攻撃 イ パスワードリスト攻撃 ウ パスワード推測攻撃 エ ブルートフォース攻撃
- 下線部(e)について、指紋や虹彩などの生体情報を用いる認証方式の名称として適切なものを次のア～エから1つ選んで、その符号を書きなさい。
ア ケルベロス認証 イ ツーフアクタ認証 ウ バイオメトリクス認証 エ マトリックス認証
- 下線部(f)について、1995年に公表され、2014年に欠陥が発見された暗号化技術の名称として適切なものを次のア～エから1つ選んで、その符号を書きなさい。
ア HTML4 イ SSL3.0 ウ SHA-1 エ TLS1.0
- 下線部(g)について、この暗号化通信の手順をまとめた右の図の(あ)～(か)にあてはまるものを次のア～ウからそれぞれ1つずつ選んで、その符号を書きなさい。なお、同じものを何度利用してもよい。
ア 秘密鍵 イ 共通鍵 ウ 公開鍵
- 下線部(h)について、暗号化方式の名称として適切なものを次のア～エからすべて選んで、安全性の高い順にその符号を書きなさい。
ア AES イ RSA ウ TKIP エ WEP
- 下線部(i)について、この名称をカタカナで書きなさい。
- 下線部(j)について、この特徴を持つマルウェアの総称を書きなさい。
- コンピュータの技術でなく、なりすましや盗み見などの人的手段により、他人の ID やパスワードなどを収集する手法の総称を書きなさい。

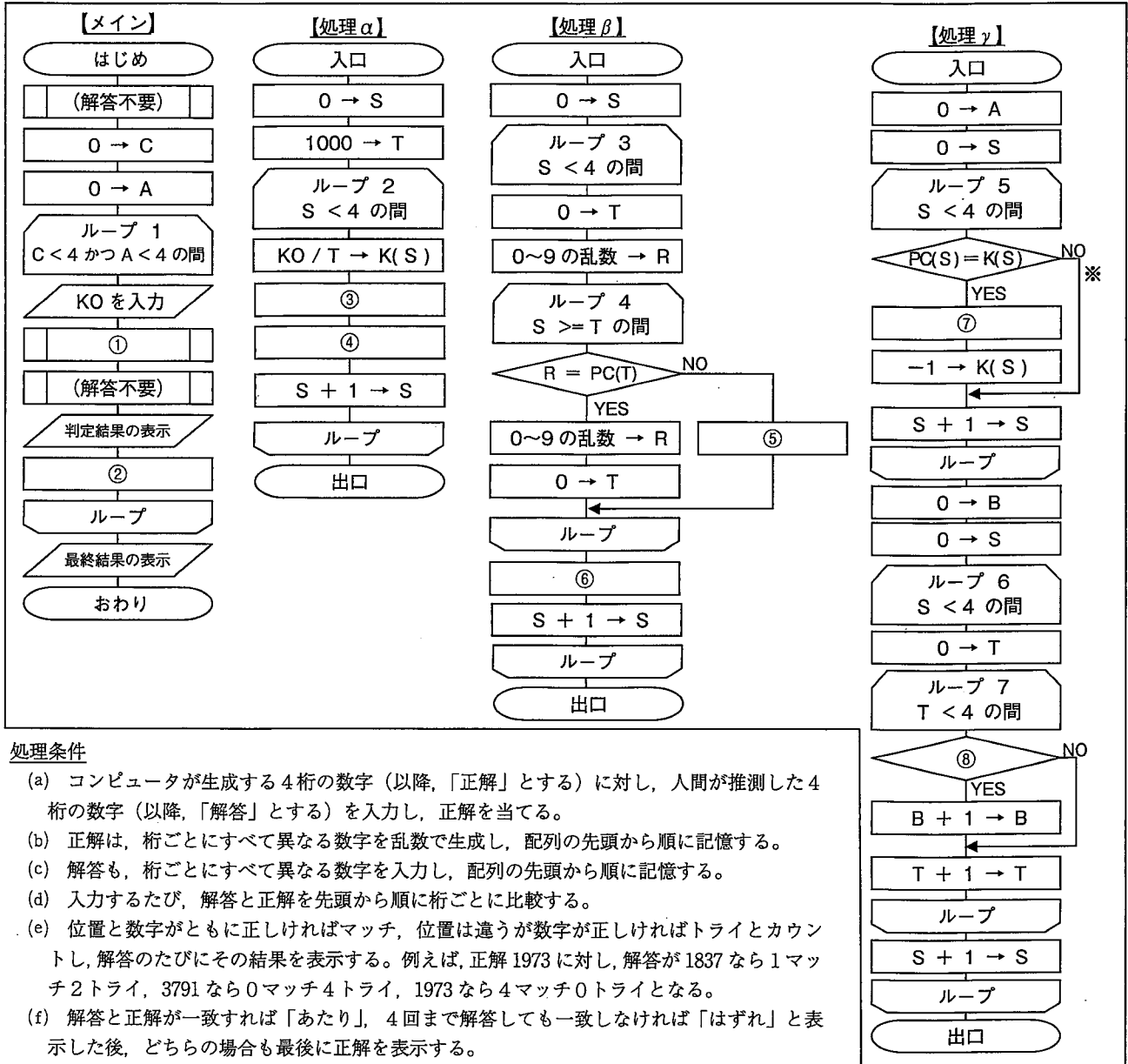


平31 高等学校情報 (5枚のうち3)

(解答はすべて、解答用紙に記入すること)

IV 生徒のAさんは、情報の授業で習った内容をもとに数当てゲームを作成することにした。次の流れ図と処理条件をもとに、あとの問いに答えなさい。なお、流れ図内で割り算の計算結果は、すべて小数点以下を切り捨てる。

流れ図1



処理条件

- コンピュータが生成する4桁の数字(以降、「正解」とする)に対し、人間が推測した4桁の数字(以降、「解答」とする)を入力し、正解を当てる。
- 正解は、桁ごとにすべて異なる数字を乱数で生成し、配列の先頭から順に記憶する。
- 解答も、桁ごとにすべて異なる数字を入力し、配列の先頭から順に記憶する。
- 入力するたび、解答と正解を先頭から順に桁ごとに比較する。
- 位置と数字がともに正しければマッチ、位置は違うが数字が正しければトライとカウントし、解答のたびにその結果を表示する。例えば、正解1973に対し、解答が1837なら1マッチ2トライ、3791なら0マッチ4トライ、1973なら4マッチ0トライとなる。
- 解答と正解が一致すれば「あたり」、4回まで解答しても一致しなければ「はずれ」と表示した後、どちらの場合も最後に正解を表示する。

1 流れ図1の①～⑧に適切なものを次のア～タからそれぞれ1つ選んで、その符号を書きなさい。

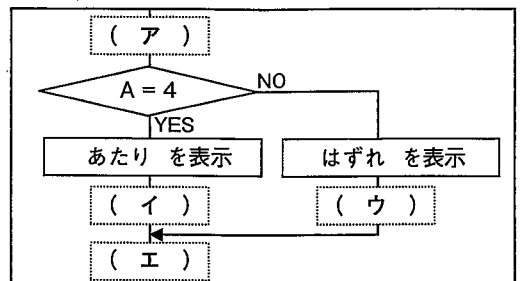
- | | | | |
|----------------------------------|-------------------------|----------------------------|-------------------------|
| ア $KO - T * K(S) \rightarrow KO$ | イ $PC(T) = K(S)$ | ウ $T * 10 \rightarrow T$ | エ $R \rightarrow PC(S)$ |
| オ $S + 1 \rightarrow S$ | カ $R \rightarrow PC(T)$ | キ $A + 1 \rightarrow A$ | ク 処理α |
| ケ $KO - T * S \rightarrow KO$ | コ $C + 1 \rightarrow C$ | サ $A + K(S) \rightarrow A$ | シ 処理β |
| ス $T / 10 \rightarrow T$ | セ $PC(T) = K(T)$ | ソ $T + 1 \rightarrow T$ | タ 処理γ |

2 流れ図2は、流れ図1の「最終結果の表示」の詳細を示したものである。「正解の数字を表示」の処理が入る場所を(ア)～(エ)から1つ選んで、その符号を書きなさい。

3 正解が8195で解答が2985の場合、(1)処理γの※を通る回数 (2)Bの値が1になったときのSの値をそれぞれ書きなさい。

4 流れ図1で、1ヶ所を書き換えれば、解答の機会を3回に変更できる。どこをどのように書き換えればよいか、書きなさい。

流れ図2

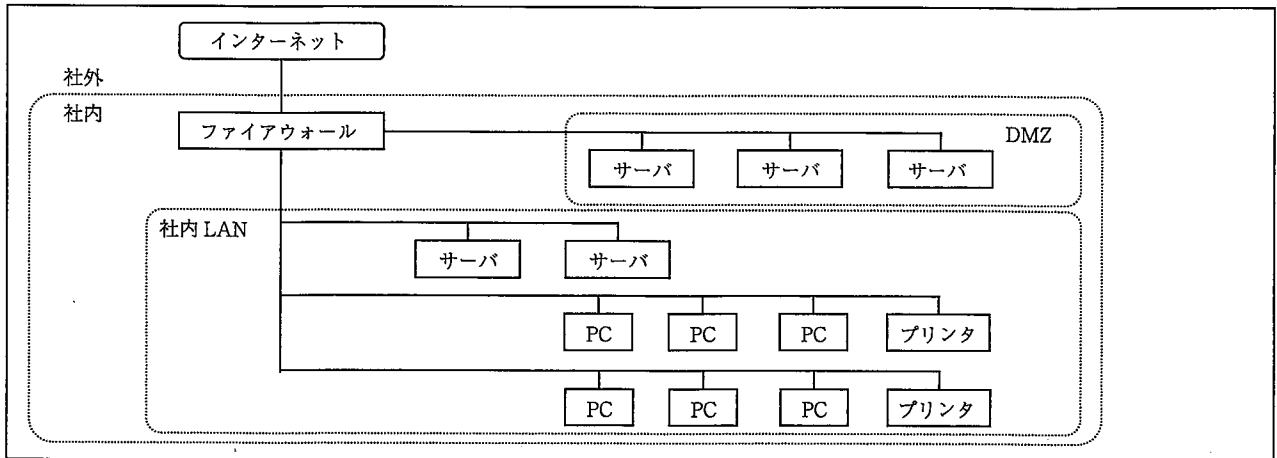


平31 高等学校情報 (5枚のうち4)

(解答はすべて、解答用紙に記入すること)

V 次の図および文をもとに、あとの問いに答えなさい。なお、サブネットワークのアドレスにすべてのビットが0または1の値は設定できるが、ホストアドレスには設定できないものとする。

図



ファイアウォールによって、インターネットからも社内 LAN からも隔離された場所を(a)DMZという。ここに設置したサーバは、ファイアウォールの機能により外部からの不正アクセスを防ぐことができる。

これまで、社内 LAN の PC 等には6つの課ごとに使用可能な範囲を決め、導入のたびに IP アドレスと 24 ビットのサブネットマスクを設定してきたが、台数の増加とともにシステム内の応答性能が低下する現象が生じている。そこで、サブネットの考え方で課ごとにネットワークを分割しつつ、1つのネットワークで接続できる台数を最大に設定できるよう構成変更を行うとともに、(b)ブロードキャストを他のネットワークへ通さない機器を社内 LAN に設置することにした。また、会議室では無線 LAN を使用することとし、そのために(c)PC等に IP アドレスなどの設定情報を自動的に割り当てられる機器を導入した。

- 下線部(a)について、この場所に設置するのが適切でないものを次のア～エから1つ選んで、その符号を書きなさい。
ア DNSサーバ イ NTPサーバ ウ ファイルサーバ エ プロキシサーバ
- 下線部(b)に該当しない機器を次のア～エから1つ選んで、その符号を書きなさい。
ア L3スイッチ イ ゲートウェイ ウ リピータ エ ルータ
- 下線部(c)を実現するためのサーバを次のア～エから1つ選んで、その符号を書きなさい。
ア DHCPサーバ イ IMAPサーバ ウ SMTPサーバ エ データベースサーバ
- 無線 LAN において、通信経路が一定時間以上継続して空いていることを確認し、その後にデータを送信するアクセス制御方式を次のア～エから1つ選んで、その符号を書きなさい。
ア CSMA/CA イ CSMA/CD ウ IEEE802.11 エ WPS
- DMZ に設置する公開用 Web サーバに、文字、画像、レイアウト情報などを一元的に保存・管理し、HTML 言語などの専門知識がない利用者でも Web による情報発信が容易にできるようにしたシステムを導入した。このシステムの略称を次のア～エから1つ選んで、その符号を書きなさい。
ア CMC イ CMS ウ CSS エ CVS
- 構成変更後のサブネットの最大数を次のア～エから1つ選んで、その符号を書きなさい。
ア 7 イ 8 ウ 9 エ 10
- 構成変更後のサブネットマスクに設定する値を次のア～エから1つ選んで、その符号を書きなさい。
ア 255.255.255.7 イ 255.255.255.128 ウ 255.255.255.224 エ 255.255.255.248
- 構成変更後に、1つのサブネットで使用できるホストアドレスの最大数を次のア～エから1つ選んで、その符号を書きなさい。
ア 30 イ 32 ウ 254 エ 256
- 構成変更後に、IP アドレス 192.168.1.130 と同一のサブネットに割り振ることができる IP アドレスを次のア～エからすべて選んで、その符号を書きなさい。
ア 192.168.1.120 イ 192.168.1.140 ウ 192.168.1.150 エ 192.168.1.160
- 構成変更後に、IP アドレス 192.168.1.130 が含まれるサブネットのブロードキャストアドレスを次のア～エから1つ選んで、その符号を書きなさい。
ア 192.168.1.128 イ 192.168.1.158 ウ 192.168.1.159 エ 192.168.1.254