

試 験 種 別	試 験 科 目
第 2 種 伝 送 交 換 主 任 技 術 者	伝 送 交 換 設 備 及 び 設 備 管 理

問 1 次の問いに答えよ。

(小計 20 点)

- (1) 次の文章は、デジタル電話交換機の通話路スイッチについて述べたものである。 内の(ア)～(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、 内の同じ記号は、同じ解答を示す。 (2点×4 = 8点)

デジタル電話交換機は、電話機からのアナログ信号をデジタル信号に変換し、一つのハイウェイ上に時分割多重化し、時分割多重化したままで交換処理を行っている。

通話路スイッチは、一般に、 (ア) スイッチと (イ) スイッチとで構成されている。

(ア) スイッチは、音声情報のビット列群単位の書き込み、記録、読み出しのできるメモリ素子を用いてハイウェイ上の (ウ) の入替えを行っている。

また、 (イ) スイッチは、同一時間位置の信号を入れ替えるスイッチであり、 (エ) を格子状に設けることにより、ハイウェイ相互間の信号の入替えを行っている。

<(ア)～(エ)の解答群>

セル	加入者線	フレーム	時 間
ゲート回路	中継線	タイムスロット	リード
空 間	バッファ	キャッシュメモリ	制御メモリ
通話メモリ	伸張回路	カウンタ回路	

- (2) 次の文章は、自立電源方式などについて述べたものである。 内の(オ)、(カ)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。 (3点×2 = 6点)

- () 自立電源方式として、エンジン発電装置と組み合わせて使用される太陽光発電方式について述べた次の文章のうち、誤っているものは、 (オ) である。

<(オ)の解答群>

日照時は、太陽電池の出力により蓄電池を充電しつつ負荷に電力を供給し、太陽光の得られない時間には蓄電池から電力が供給される。

晴天が継続して、蓄電池が過充電となるのを防ぐための過充電防止回路を設ける場合がある。

併設されたエンジン発電装置の発電機は、一般に、直流発電機が用いられ、出力電圧を任意に設定できることから、整流装置、直流電圧変換装置を必要としない。

使用する太陽電池の容量を決めるには、日射量の状況と内燃機関の燃料補給費用などを考慮し、個々に検討を加えて決定する必要がある。

太陽電池の起電力が蓄電池の電圧以下になった場合、蓄電池から太陽電池に電流が逆流することを防ぐための逆流防止ダイオードを設ける場合がある。

() エンジン発電装置について述べた次の A ~ C の文章は、。

- A エンジン発電装置は、商用電源停止の場合の予備エネルギー源として用いられている。また、1次エネルギー源としても用いられる場合がある。
- B ディーゼル機関は、発電効率が高く、燃料が廉価で経済的であるが、回転数の変化が比較的大きく、運転時の騒音や振動が大きいため、通信用電源のエンジン発電装置の動力源としては用いられない。
- C ガスタービンは、冷却水なしで運転可能な利点を有している。

<(カ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

(3) 次の文章は、通信網の網構成の種類と特徴について述べたものである。内の(キ)、(ク)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。(3点×2=6点)

() 網構成の特徴について述べた次の A ~ C の文章は、。

- A 星状網は、中継ノードを設置することにより、ノード間のリンク数が少ない網構成であるが、中継ノード若しくはリンクが故障になった場合、う回できない。
- B 網状網は、星状網に比較して、ノード間のリンクを多く必要とするが、ノード間のトラヒックが非常に少ない場合にはコスト的に有利な網構成である。
- C 環状網は、網状網に比較して網の拡張が容易であるが、大規模な網では、一般に、中継呼量、伝送遅延時間が大きくなる。

<(キ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

() 網構成について述べた次の文章のうち、誤っているものは、である。

<(ク)の解答群>

実際の公衆電話網では、星状網と網状網を組み合わせた複合網になっていることが多い。

星状網は網状網に比べ、中継ノードやリンクの故障時の影響が大きく、網の信頼性は低い。

コンピュータ通信におけるLANなどの小規模網では、バス型といわれる網構成も用いられる。

環状網では、中央同期装置により、網全体の同期や監視・制御を行う方式もある。

網状網では、1リンクが故障になった場合、それぞれのノードに中継機能が無くても通信には影響を与えない。

- (1) 次の文章は、ATMスイッチの種類について述べたものである。□内の、(ア)~(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、□内の同じ記号は、同じ解答を示す。(2点×4=8点)

ATMスイッチは、その構成から、□(ア)型スイッチと□(イ)型スイッチとに大別される。

□(ア)型スイッチは、入力信号をバッファメモリに高速多重化し、時分割的に出力ポートにセルを出力する。

□(イ)型スイッチは、あて先ごとに異なる経路(インターコネクション)を通してスイッチングされることから、□(ア)型と比較してメモリアクセス速度による制限が少なく、高速・□(ウ)のスイッチ構成に適している。このスイッチ構成の一例として、□(エ)スイッチがある。

<(ア)~(エ)の解答群>

周波数分割	空間分割	ナイキスト
機能分割	広帯域	ハミング
高スループット	高周波	CRC
高蓄積度	バニヤン(Banyan)	マルチキャスト
共通リソース	リーキーパケット	

- (2) 次の文章は、TCP/IPプロトコルについて述べたものである。□内の(オ)~(ク)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。(3点×4=12点)

() TCP/IPプロトコルとOSI基本参照モデルとの階層の対比について述べた次のA~Cの文章は、□(オ)。

A TCP/IPプロトコルのアプリケーション層は、OSI基本参照モデルのネットワーク層に対応している。

B TCP/IPプロトコルのトランスポート層は、OSI基本参照モデルのトランスポート層に対応している。

C TCP/IPプロトコルのインターネット層(ネットワーク層)は、OSI基本参照モデルのセッション層に対応している。

<(オ)の解答群>

Aのみ正しい	Bのみ正しい	Cのみ正しい
A、Bが正しい	A、Cが正しい	B、Cが正しい
A、B、Cいずれも正しい	A、B、Cいずれも正しくない	

() TCP/IPプロトコルのインターネット層(ネットワーク層)のIPについて述べた次のA～Cの文章は、(カ)。

- A IPプロトコルは、コネクション型サービスを提供する。
- B IPでは、インターネットで各ホストを指定するために、IPアドレスが使用される。
- C 送信側でトランスポート層から渡されたデータは、IPパケットといわれる単位にパケット化される。

<(カ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

() TCP/IPプロトコルのトランスポート層について述べた次のA～Cの文章は、(キ)。

- A トランスポート層のプロトコルには、TCP、UDP、SMTPがある。
- B TCPでは、順序制御やフロー制御を行っていない。
- C TCPではコネクション型サービスを提供し、UDPではコネクションレス型サービスを提供している。

<(キ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

() TCP/IPプロトコルのアプリケーション層について述べた次のA～Cの文章は、(ク)。

- A ICMP、IGMPは、アプリケーション層に属さないプロトコルである。
- B HTTPは、電子メールの配送を行うプロトコルである。
- C FTPは、ネットワーク管理用のプロトコルである。

<(ク)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

- (1) 次の文章は、通信サービスの品質管理の概要について述べたものである。[]内の(ア)~(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、[]の同じ記号は、同じ解答を示す。(2点×4=8点)

通信サービスにおける品質管理は、利用者の満足度の維持・向上を図ることが目的であり、ネットワーク要素及びこれらの集まりで構成されるネットワークに対して、エンド・ツー・エンドの接続品質、伝送品質、[(ア)]などの目標値を満足するように管理される。エンド・ツー・エンドの品質管理は、ネットワーク設備全体の品質を維持するために行われ、設備区間ごとなどに、個々の品質を管理し、品質劣化の発生箇所や原因を特定して、必要な改善のアクションを実施する。具体的には図に示すような品質管理のサイクルを回すことにより、ネットワークの品質を常に監視し、[(イ)]、測定データの[(ウ)]、評価などを行い、品質劣化の検出と劣化設備及び劣化原因の特定、[(エ)]などを行う。

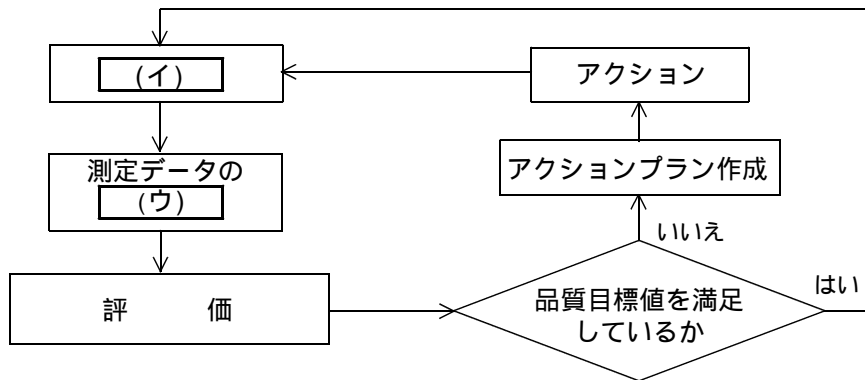


図 品質管理のサイクル

<(ア)~(エ)の解答群>

損失	回線断	品質の測定	復旧体制
分析	番号計画	顧客情報の把握	整理保存
加工修正	信頼性品質	アウトソーシング	
品質トレンドの予測		同期多重化	

(2) 次の文章は、ネットワーク運用業務の概要について述べたものである。 内の(オ)、(カ)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。(3点×2=6点)

() ネットワークオペレーションについて述べた次の文章は、 (オ) が正しい。

<(オ)の解答群>

局部的なふくそうを回避するための通信網トラヒック制御の措置として、う回路変更やう回選択範囲の拡大を行なう拡大的な措置は効果がない。

主要伝送路の信頼性確保のために予備の伝送路を備えている場合は、定期的に現用伝送路と予備伝送路で伝送路切替を行なわなければならない。

局部的なふくそうを回避するための通信網トラヒック制御の措置として、トラヒックの実時間変動に応じて中継経路の選択手順を変更する適応的な措置を行なうことがある。

通信網トラヒック制御の措置として、局部的なふくそうが発生した場合は、ネットワーク全体にその影響が及ぶことを防止するため、発信規制・出接続規制・う回規制などの措置を行なってはならない。

() ネットワークの故障時の措置などについて述べた次のA～Cの文章は、 (カ) 。

- A 故障が発生した場合は、迅速に故障診断、故障箇所の特定制を行い、故障状況を把握する。この時点で明確に通信設備の責任分界点と連絡体制を決め、修理の手配を行う。
- B ネットワークは、故障箇所の確定や故障の修復に意外と時間がかかるものもあるため、ネットワークの2ルート化などにより、修理作業着手以前に、いち早くバックアップ側に切り替えてサービス中断時間を極力短時間に抑える工夫が必要である。
- C ネットワークの運転、故障切り替えなどを行う場合、その操作に不注意に基づく人為的ミスが発生する危険性があるため、できるだけ自動化を図る等の工夫が必要である。

<(カ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

(3) 次の文章は、デジタル信号伝送で用いられる符号誤りの検出・訂正方法である A R Q (Automatic Repeat Request)方式と F E C (Forward Error Correction)方式について述べたものである。 内の(キ)、(ク)に適したものを、下記のそれぞれの解答群から選び、その番号を記せ。 (3点×2=6点)

() A R Q方式の特徴について述べた次のA～Cの文章は、 (キ) 。

- A 帰還通信路を必要とするため、片方向通信方式には不向きである。
- B 通信路での誤り率が高い場合、データの再送要求の回数が増える。
- C 符号の冗長度が F E C方式と比較して大きくなる。

<(キ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

() F E C方式の特徴について述べた次のA～Cの文章は、 (ク) 。

- A 片方向通信方式にも適用できる。
- B すべてのランダム誤り、バースト誤りに対して誤り訂正が可能であり、エラーフリー伝送が実現できる。
- C 送信側では、送出する符号構成が偶数か奇数かを表示して送信するため、受信側では1ビットの符号誤りの場合のみ訂正ができる。

<(ク)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

問4 次の問いに答えよ。

(小計20点)

(1) 次の文章は、伝送路符号形式について述べたものである。 内の(ア)～(エ)に最も適したものを、次ページの解答群から選び、その番号を記せ。ただし、 の同じ記号は、同じ解答を示す。 (2点×4=8点)

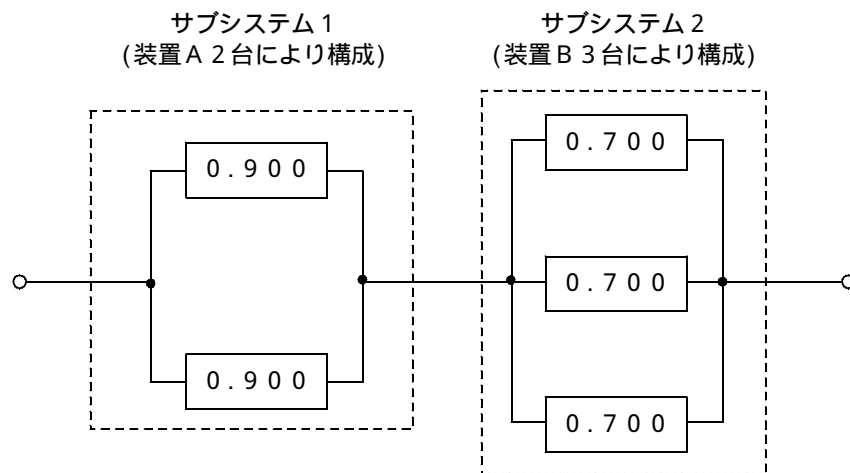
パルス伝送で用いられる伝送路符号形式の一つに、2進論理値“1”に対して正極性符号(+1)と負極性符号(-1)とを交互に対応させ、2進論理値“0”に対して零レベル符号(0)を対応させた符号として、 (ア) がある。

(ア) は、A M I符号ともいわれ、 (イ) 符号であるにもかかわらず伝送する情報は2値符号と同等であり、直流成分が小さく伝送上有利な点もあるが、2進論理値“0”が連続すると (ウ) が消失し、ビット同期の確立が不安定になるため、実際の伝送路符号としてこのままの形式で使用されることは少ない。このため、零連続を抑圧する機能を持たせた符号形式として (エ) 、C M I符号などが多く用いられている。

<(ア)～(エ)の解答群>

1 値	3 値	4 値
高周波成分	バイポーラ符号	N R Z 符号
ハミング符号	ユニポーラ符号	D M I 符号
符号ひずみ	直流成分	B 8 Z S 符号
タイミング成分	低周波成分	

- (2) 次の文章は、あるシステムの信頼度について述べたものである。□内の(オ)～(ク)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、下図は信頼度に関する概念図であり、図中の□内の数字はそれぞれの構成装置の信頼度を示している。なお、答えは、四捨五入により小第3位までとする。 (3点×4 = 12点)



- () 装置 A 2 台からなるサブシステム 1 (1 / 2 冗長構成)の信頼度は、□(オ)である。
 () 装置 B 3 台からなるサブシステム 2 (1 / 3 冗長構成)の信頼度は、□(カ)である。
 () 装置 B 3 台からなるサブシステム 2 が、多数決 (2 out of 3) 系システム (2 / 3 冗長構成) となっているときのサブシステム 2 の信頼度は、□(キ)である。
 () 二重化されたサブシステム 1 と多数決 (2 out of 3) 系構成のサブシステム 2 を接続した全体のシステムの信頼度は、□(ク)である。

<(オ)～(ク)の解答群>

0.278	0.340	0.343	0.635
0.776	0.784	0.788	0.810
0.885	0.900	0.910	0.963
0.970	0.973	0.990	0.999

- (1) 次の文章は、Webによる電子商取引におけるセキュリティについて述べたものである。
 内の(ア)~(エ)に最も適したものを、下記の解答群から選び、その番号を記せ。ただし、 内の同じ記号は、同じ解答を示す。(2点×4=8点)

クライアント端末からWebサーバへのアクセスは、通常HTTPといわれるプロトコルに従って行われる。一般に、クライアント端末とWebサーバとの間でやり取りされるデータは、暗号化されていないため、データが途中で第三者に盗聴され、悪用される危険性がある。

Webによる電子商取引などにおいては、金銭が絡むため、例えば、SSL(Secure Socket Layer)を利用し、データの暗号化や認証を行い、これらの危険性を回避することが多い。

具体的には、

- ① クライアント端末からSSL通信が要求される。
- ② Webサーバが自分の公開鍵^{かぎ}をクライアント端末に送信する。
- ③ クライアント端末から (ア) をWebサーバに送信する。

という順序の処理を行った後、データのやりとりを行う。また、SSLではハッシュ関数を用いたメッセージダイジェストの作成を行うことにより、 (イ) を防止することができる。

上記②の手順にあわせWebサーバは通常 (ウ) をクライアント端末に送信する。クライアント端末で (ウ) を検証することで、 (エ) を確認することができる。

<(ア)~(エ)の解答群>	
共通鍵暗号方式で暗号化した秘密鍵	データの改ざん
共通鍵暗号方式で暗号化した公開鍵	アクセス権詐取
公開鍵暗号方式で暗号化した共通鍵	クライアント端末のなりすまし
不正侵入	CAの発行する共通鍵
CAの発行する公開鍵	RAの発行する秘密鍵
CAの発行するデジタル証明書	クライアント端末の真正性
データの盗聴がされていないこと	Webサーバの真正性

- (2) 次の文章の 内の(オ)に適したものを、次ページの解答群から選び、その番号を記せ。(3点)

IDS(侵入検知システム)について述べた次のA~Cの文章は、 (オ) 。

- A ネットワーク型侵入検知システムは、ネットワーク上を流れるパケットのヘッダやデータの内容(ペイロード)を検査し、侵入、攻撃につながるものでないかを検知する。
- B ホスト型侵入検知システムは、ホスト上で出力される情報(ログデータ、コマンド履歴、ファイルの状態変化など)を用いて不正侵入を検知する。
- C ハイブリッド型侵入検知システムは、パケットのヘッダ情報より、発信元、あて先IPアドレス及びポート番号を用いて、アクセスを許可するかしないかを検査する。

<(オ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

- (3) 次の文章の、内の(カ)に適したものを、下記の解答群から選び、その番号を記せ。
(3点)

認証技術について述べた次の文章のうち、誤っているものは、 (カ) である。

<(カ)の解答群>

認証は、相手にその本人しか提示することができない何らかの情報を示させて、これを確認することによって行う。その際の情報は、その種類によって、

①知っていること、②持っているもの、③身体的特徴などによるものに分類することができる。

パスワードによる認証には、固定パスワードやワンタイムパスワードなどを用いる方式がある。ワンタイムパスワードは、固定パスワードに比較して盗聴に対する抑止力が小さい。

クライアントとサーバ間で認証を行う場合、クライアントからの接続を受け付けたアプリケーションのサーバは、認証サーバに対して、正しいクライアントか否かの認証要求を送る。

PPPの接続に使用されるCHAPやメールサーバへアクセスする際のプロトコルであるPOPでは、チャレンジ&レスポンス方式が用いられている。

- (4) 次の文章の 内の(キ)に適したものを、下記の解答群から選び、その番号を記せ。
(3点)

情報セキュリティについて述べた次のA～Cの文章は、 (キ) 。

- A 情報の漏えいを防止するために、IDとパスワードに関する情報は、原則として、本人の記憶と認証サーバの中にだけ存在するようにすべきである。
- B 人間の心理の弱点を突いた攻撃の手段に利用されないように、住所録、電話帳、組織図、ゴミなどの管理及び処理に注意し、情報が部外者の手に渡らないようにすべきである。
- C 企業等においては、IDやパスワードを取り扱う上で行ってはならないこと、会社情報や個人情報を扱う上で行ってはならないことなどを、文書として明確化し、関係者に周知することが重要である。

<(キ)の解答群>

- | | | |
|--------------|----------------|---------|
| Aのみ正しい | Bのみ正しい | Cのみ正しい |
| A、Bが正しい | A、Cが正しい | B、Cが正しい |
| A、B、Cいずれも正しい | A、B、Cいずれも正しくない | |

- (5) 次の文章は、コンピュータウイルス(狭義のコンピュータウイルスのほかワームなどの有害プログラム)対策について述べたものである。 内の(ク)に適したものを、下記の解答群から選び、その番号を記せ。 (3点)

次の文章は、 (ク) が正しい。

<(ク)の解答群>

コンピュータウイルス対策ソフトウェアを導入し、定期的にコンピュータをスキャンすることが肝要である。コンピュータウイルス対策ソフトウェアの導入後、一定の保証期間内は、コンピュータは安全である。

メールの添付ファイルにコンピュータウイルスが潜んでいる場合があるため、添付ファイルは開いて確認する必要がある。また、メーラー、ブラウザのセキュリティレベルを適切(中レベル以上)に設定することにより被害を防止することができる。

ワードプロセッサや表計算のソフトウェアのデータファイルを開くときに、マクロ機能の自動実行機能を無効にするなど、アプリケーションに搭載されているセキュリティ機能を活用することが必要である。

コンピュータウイルスに感染しておらず、安定して動作しているコンピュータであれば、OSやアプリケーションの製造元から発行される種々のセキュリティパッチを頻繁に施す必要はない。

コンピュータウイルスに感染した可能性がある場合は、まず、データのバックアップを行い、現状以上のデータの破壊、ファイルの損失を最低限に抑える。