

注 意 事 項

- 試験開始時刻 10時00分
- 試験科目別終了時刻

試験科目	科目数	終了時刻
「法規」のみ	1科目	11時20分
「伝送交換設備(又は線路設備)及び設備管理」のみ	1科目	11時40分
「法規」及び「伝送交換設備(又は線路設備)及び設備管理」	2科目	13時00分

- 試験種別と試験科目別の問題(解答)数及び試験問題ページ

試験種別	試験科目	問題(解答)数					試験問題ページ
		問1	問2	問3	問4	問5	
伝送交換主任技術者	法規	6	6	6	6	6	1~14
	伝送交換設備及び設備管理	8	8	8	8	8	15~29
線路主任技術者	法規	6	6	6	6	6	1~14
	線路設備及び設備管理	8	8	8	8	8	30~44

- 受験番号等の記入とマークの仕方

- マークシート(解答用紙)にあなたの受験番号、生年月日及び氏名をそれぞれ該当枠に記入してください。
- 受験番号及び生年月日に該当する箇所を、それぞれマークしてください。
- 生年月日の欄は、年号をマークし、生年月日に1桁の数字がある場合、十の位の桁の「0」もマークしてください。

【記入例】 受験番号 01AB941234

生年月日 昭和50年3月1日

受 験 番 号									
0	1	A	B	9	4	1	2	3	4
●	○	●	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○

生 年 月 日									
年	号	5	0	3	0	1			
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○

- 答案作成上の注意

- マークシート(解答用紙)は1枚で、2科目の解答ができます。
「法規」は赤色(左欄)、「伝送交換設備(又は線路設備)及び設備管理」(「設備及び設備管理」と略記)は緑色(右欄)です。
- 解答は試験科目の解答欄の正解として選んだ番号マーク枠を、黒の鉛筆(HB又はB)で濃く塗りつぶしてください。
ボールペン、万年筆などでマークした場合は、採点されませんので、使用しないでください。
一つの問いに対する解答は一つだけです。二つ以上マークした場合、その問いについては採点されません。
マークを訂正する場合は、プラスチック消しゴムで完全に消してください。
- 免除の科目がある場合は、その科目欄は記入しないでください。
- 受験種別欄は、あなたが受験申請した試験種別を で囲んでください。(試験種別は次のように略記されています。)
伝送交換主任技術者は、 『伝 送 交 換』
線路主任技術者は、 『線 路』
- 試験問題についての特記事項は、裏表紙に表記してあります。

- 合格点及び問題に対する配点

- 各科目の満点は100点で、合格点は60点以上です。
- 各問題の配点は、設問文の末尾に記載してあります。

マークシート(解答用紙)は、絶対に折り曲げたり、汚したりしないでください。

次ページ以降は試験問題です。試験開始の合図があるまで、開かないでください。

受験番号 (控え)									
--------------	--	--	--	--	--	--	--	--	--

(今後の問い合わせなどに必要になります。)

試験種別	試験科目
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、電話の番号計画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。(2点×4=8点)

公衆電気通信網において、電気通信番号は、端末設備の識別、任意の端末への接続などに用いられており、端末などへの電気通信番号の付与規則は、一般に、番号計画といわれる。また、通話先の端末などに付与されている電気通信番号は、一般に、電話番号といわれ、数字を組み合わせた番号である。

国際公衆電気通信番号計画はITU-T勧告E.164で規定されており、国際電話番号は、一般に、□(ア)、国内宛先コード及び加入者番号から構成される最大□(イ)桁の番号である。

日本国内の番号計画は総務省により定められている。固定電話の電話番号は、一般に、先頭の数字が□(ウ)といわれる0から始まり、市外局番、市内局番及び加入者番号で構成されている。また、A及びBを0以外の番号としたとき、一般に、0A0で始まる電話番号は携帯電話、PHSなどに用いられており、0AB0で始まる電話番号は、一部地域の市外局番として使用されているほか、通信事業者が提供する□(エ)サービスに用いられている。

<(ア)～(エ)の解答群>			
1 1	1 5	外線発信番号	国内プレフィックス
1 2	IP電話	事業者識別番号	サービスコード
1 3	緊急通報	エリアコード	国際プレフィックス
1 4	国番号	高度な電話	PBXダイヤルイン

- (2) 次の文章は、映像信号の圧縮符号化技術などについて述べたものである。 内の(オ)、(カ)に最も適したものを、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)

- () 映像信号の圧縮符号化技術について述べた次の文章のうち、正しいものは、 (オ) である。

<(オ)の解答群>

映像信号の圧縮符号化では、映像信号の情報をできるだけ少ないデジタルの情報に置き換えており、圧縮符号化の手順は、一般に、量子化、予測符号化、符号割当て、変換符号化の順で行われる。

量子化では、入力された信号値を離散的な代表値で近似するため、量子化雑音が生ずる。量子化のステップの幅を大きくすれば、一般に、量子化雑音を小さくすることができる。

映像は、一般に、時間的に連続する静止画像のフレームを並べたものとみなすことができる。このため、予測符号化として用いられるフレーム間符号化では、一般に、ある画素の予測誤差を求めるために他のフレームの画素を利用している。

符号割当てには、一般に、可変長符号が用いられ、発生頻度の高い信号値には長い符号を割り当て、発生頻度の低い信号値には短い符号を割り当てることにより、情報量を削減している。

- () 映像信号の圧縮符号化の国際標準規格など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>

I T U - T 勧告 H . 2 6 1 は、テレビ会議、テレビ電話などの通信を対象とした規格であり、走査線やフレーム数が異なるテレビジョンの信号形式 (N T S C 、 P A L など) に依存しないよう、いったん共通の形式に変換した後に符号化する手順を採用している。

M P E G - 1 は、コンパクトディスクなどの蓄積メディアを対象とした 1 . 5 [M b i t / s] 程度の伝送速度の動画像符号化方式であり、プログレッシブ信号及びインタレース信号に対応している。

M P E G - 2 は、地上デジタルテレビ放送、DVDなどで利用されており、H D T V 相当の解像度の映像信号などの圧縮符号化に対応している。

M P E G - 4 A V C / H . 2 6 4 は、ワンセグ放送、スマートフォンなどで利用されており、圧縮符号化効率は、一般に、M P E G - 2 の 2 倍以上とされている。

- (3) 次の文章は、IP網におけるルーティング技術について述べたものである。□内の(キ)、(ク)に最も適したものを、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)

- () ルーティングテーブルの生成について述べた次の文章のうち、正しいものは、□(キ)である。

<(キ)の解答群>

スタティックルーティングでは、ルーティングテーブルを隣接するルータ間で交換する。そのため、ネットワークの故障などによりネクストホップにパケットが到達できない場合には、ルーティングプロトコルを用いて迂回経路を設定することができる。

ダイナミックルーティングでは、ルータ間で交換した経路情報をもとにしてルーティングテーブルを生成する。そのため、ネットワークトポロジに変化があった場合には、自動的にルーティングテーブルを更新することができる。

ディスタンスベクタ方式では、隣接するルータの経路情報とルータ自身が保有する経路情報をもとにして、最短の物理的な経路長や帯域幅を考慮して目的地まで到達できるような経路を計算し、ルーティングテーブルを生成する。

リンクステート方式では、一般に、すべてのルータが常に同一のデータベースを保持しており、各ルータが個々に最短パスツリーを作りルーティングテーブルを生成する。リンクステート方式は、経路情報に変更があると、ディスタンスベクタ方式と比較して、処理が複雑であるため経路が収束するまでの時間が長くなることが多く、経路がループになってしまうこともある。

- () ルーティングプロトコルの種類について述べた次の文章のうち、誤っているものは、□(ク)である。

<(ク)の解答群>

自律システム(AS)は、一般に、統一されたポリシーで運用されるネットワークの集まりとされており、IGPは、AS内部のルーティングで用いられるプロトコルである。

RIPは、IGPとして用いられるディスタンスベクタ型のルーティングプロトコルである。RIPにはRIPv1及びRIPv2の規格があり、RIPv2では認証機能などが追加されている。

OSPFは、IGPとして用いられるパスベクトル型のルーティングプロトコルである。OSPFでは、メトリックとしてリンクの優先度を表すコストといわれる値を用いている。

BGPは、EGPとして用いられるルーティングプロトコルであるが、ASの内部における外部経路情報の交換などでも用いられる。BGPでは、パス属性を利用して最適な経路を選択する。

- (1) 次の文章は、インターネットにおけるIPv4及びIPv6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)

インターネットに求められる技術的条件は多様化しているが、IPv4では、IPアドレスの枯渇、[(ア)] 及びモビリティの機能拡張が困難などの問題点があり、この解決策の一つとして、IETFにおいてIPv6の仕様が制定されている。

IPv6のアドレスは128(bit)で表現され、IPアドレスの表記方法は、128(bit)を[(イ)] ブロックに分け、各ブロックをコロンで区切り、それぞれを16進数で表示する方法が採られている。

IPv4ヘッダとIPv6ヘッダを比較すると、IPv4ヘッダには可変長のオプションフィールドが含まれるためヘッダ部分の長さは可変となるが、IPv6の基本ヘッダは全長[(ウ)] オクテットであり、必要に応じて機能ごとに拡張ヘッダを付加する構成が採られている。

また、IPv4では、機能拡張が困難であり、かつ、オプションであった[(ア)] 機能は、IPv6では基本機能の一つとして位置付けられている。

なお、インターネットにおけるIPv6の普及を推進するため、これまで使用されてきたIPv4環境にIPv6パケットによる通信の混在を可能とする方法の一つとして、IPv6パケットをIPv4パケットにカプセル化する[(エ)] といわれるトンネリング技術が用いられている。

<(ア)~(エ)の解答群>			
4	24	NAT	IPv4 over IPv6
8	32	セキュリティ	トランスレータ
16	40	DNS	IPv6 over IPv4
20	64	ホップリミット	プラグアンドプレイ

(2) 次の文章は、移動通信システムの概要について述べたものである。 内の(オ)、(カ)に最も適したものを、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)

() 移動通信システムの規格について述べた次の文章のうち、正しいものは、 (オ) である。

<(オ)の解答群>

P D C (Personal Digital Cellular)及びC D M A 2 0 0 0は、総称してI M T - 2 0 0 0といわれ、第2世代移動通信システムの規格とされている。

W - C D M A (Wideband CDMA)、c d m a O n e 及びP H Sは、総称して3 G (3rd Generation)といわれ、第3世代移動通信システムの規格とされている。

C D M A 2 0 0 0 から発展したデータ通信用規格である1 × E V - D O (Evolution Data Optimized/Only)、W - C D M A から発展したH S D P A (High Speed Downlink Packet Access)などは、一般に、第3.5世代移動通信システムの規格とされている。

L T E (Long Term Evolution)は、一般に、第3.9世代移動通信システムの規格とされており、サービス名称としては、W i - F i (Wireless Fidelity)を含めて、4 Gといわれる。

() I T U - R の3 G P Pで規格化されたW - C D M A方式を用いた携帯電話サービスのネットワーク構成及び機能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>

W - C D M Aのネットワークアーキテクチャは、一般に、コアネットワーク、無線アクセスネットワーク及びユーザ端末で構成される。

コアネットワークは、移動通信ネットワークの基幹部分であり、一般に、移動交換局、閉門移動交換局、パケットゲートウェイノード、ホームロケーションレジスタなどで構成される。

移動交換局は、電話の通話路及びデータ通信路の設定・開放・交換、ユーザ端末の移動管理などの機能を有している。

ホームロケーションレジスタは、一般に、当該設備を保有する事業者に参加するすべての加入者に関するサービス加入情報や認証情報、ユーザ端末に関する位置情報などを保持している。

無線アクセスネットワークは、一般に、無線ネットワーク制御装置、パケットアクセス制御ノード及び基地局で構成されており、無線ネットワーク制御装置は無線チャネルのユーザ端末への割当てや切替えを制御する機能を有している。

- (3) 次の文章は、予備電源方式の装置概要などについて述べたものである。 内の(キ)、(ク)に最も適したものを、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)

- () 予備電源方式に用いられている動力源について述べた次の文章のうち、誤っているものは、 (キ) である。

<(キ)の解答群>

ディーゼル機関は、ガソリン機関で必要とされる電気点火装置や気化器が不要という利点を持っており、ガスタービン機関と比較して、一般に、燃料消費量は少ない。

ガソリン機関は、一般に、ガソリンと空気の混合気を、吸入行程で燃焼室内に吸入し、圧縮行程の後、点火プラグで点火、燃焼及び膨張させることによりピストンを往復させる内燃機関である。

ガスタービン機関は、燃焼室内で燃料を燃焼させ、発生した高圧ガスを直接羽根車に噴き付け、出力軸を回転させる原動機であり、ディーゼル機関と比較して、排気ガス中に含まれる二酸化炭素、窒素酸化物及び硫化物質の濃度が低い。

ガスタービン機関は、ディーゼル機関と比較して、運転に必要な空気量が多いため、一般に、吸排気対策を十分考慮する必要があり、機関冷却のための冷却水も多量に必要である。

- () 同期発電機について述べた次の文章のうち、正しいものは、 (ク) である。

<(ク)の解答群>

回転電機子形同期発電機は、電機子が回転する構造であり、一般に、アーク、火花などが生じやすいが、スリップリングが不要なため、小容量の低圧発電機に適用されることが多い。

回転界磁形同期発電機では、電機子巻線がケーシングに固定されており、これは界磁巻線といわれる。

同期発電機の界磁に励磁電流を供給する方式として、ブラシレス励磁方式がある。この方式は、整流器を回転子に搭載し、固定界磁を用いた交流励磁機と組み合わせ、励磁電流の供給を行っている。

同期発電機の効率は、同期発電機自体の損失に影響される。同期発電機の損失は、負荷電流により変動する負荷損と負荷電流に関係しない固定損に大別され、うず電流損やヒステリシス損は、負荷損に分類される。

同期発電機の定格運転時の回転速度 N_s (rpm) は、発電機の極数 P 及び発電する周波数 f (Hz) により決定され、これらの関係は、一般に、次式で表される。

$$N_s = \frac{120P}{f}$$

- (1) 次の文章は、IP電話網における音声伝送品質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、□内の同じ記号は、同じ解答を示す。(2点×4=8点)

IP電話網における音声伝送品質の劣化要因には、音声信号をデジタル化することにより発生する雑音、パケットを形成するために生ずるパケット化遅延、IP電話網での伝送遅延、パケットの到着間隔のずれによる□(ア)、ルータにおけるバッファのオーバーフローによるパケット損失などがある。

IP電話網では、これらの要因による音声伝送品質の劣化の低減を図るため、優先制御、□(イ)などを行い、伝送遅延時間の短縮を実現している。ルータによる優先制御は、ルータが受け取った音声パケットを、ほかのパケットよりも優先的に送信する機能である。また、□(イ)は、フレーム長が長いパケットを分割して、指定した長さ以下にする機能である。

IP電話網における音声伝送品質の評価方法の一つに、ITU-T勧告G.107で規定されている□(ウ)といわれる総合音声伝送品質で評価する方法がある。端末設備等相互間における通話の総合品質に関しては事業用電気通信設備規則の細目で定められており、0AB~Jの電気通信番号を用いるIP電話の総合品質の基準は、□(ウ)を80を超える値とし、端末設備等相互間の平均遅延の時間を□(エ)(ms)未満として、これらの値を算出できる確率が95(%)以上でなければならないとされている。

<(ア)~(エ)の解答群>			
50	150	200	400
MOS値	PSQM	エコー損失	帯域保証
圧縮	R値	符号誤り制御	フラグメント化
伸張	PESQ	遅延揺らぎ	データリンク制御

(2) 次の文章は、JIS Z 8101 - 2 : 1999 統計 - 用語と記号 - 第2部：統計的品質管理用語について述べたものである。 内の(オ)、(カ)に最も適したものを、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)

() 観測値・試験値に関する用語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>

測定結果とは、規定された測定方法の実施によって得られる特性の値のことをいう。

合意値とは、真の値の代用として、所与の目的に合った値のことをいう。

ばらつきとは、観測値・測定結果の期待値から真の値を引いた差のことをいい、かたよりは、観測値・測定結果の大きさがそろっていないことをいう。

真度とは、真の値からのかたよりの程度のことをいい、かたよりが小さい方が、より真度が良い又は高いという。

精確さとは、観測値・測定結果と真の値との一致の程度のこと、真度と精度を総合的に表したものをいう。

() サンプルング用語について述べた次の文章のうち、正しいものは、 (カ) である。

<(カ)の解答群>

サンプルサイズとは、母集団に含まれるサンプルング単位の数のことをいう。

抜き取り比とは、そのサンプルに含まれるサンプルング単位の数のことをいう。

ランダムサンプルとは、一つのサンプルング単位が取られ、測定され、次のサンプルング単位が取られる前に母集団に戻されるサンプルングのことをいう。

層別サンプルングとは、母集団中のサンプルング単位が、生産順のような何らかの順序で並んでいるとき、一定の間隔でサンプルング単位を取ること、をいう。

バルクマテリアルとは、個数では数えられないものの集まりのことをいう。

(3) 次の文章は、故障に対応するためのシステム設計技術及び保全方式について述べたものである。
□内の(キ)、(ク)に最も適したものを、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)

() 故障に対応するためのシステム設計技術について述べた次の文章のうち、正しいものは、
□(キ)である。

<(キ)の解答群>

故障発生を少なくして平均動作可能時間を長くするための信頼性設計技術には、使用部品数の低減、システムの直列化、先端技術を用いた新規開発品の積極的な採用、フォールトトレランスの導入などがある。

システムや装置を構成する部品の特性値の経時変化による故障には劣化故障があり、劣化故障を設計段階から予測するための具体的な手法として、モンテカルロ法などが用いられる。

FMEAは、システムや装置の故障原因として考えられる故障モードなどがシステム全体に及ぼす影響を予測し、システムに潜在する弱点を抽出するトップダウン的手法である。

FTAは、あらかじめ対象システムにとって望ましくない単一の事象を規定し、それを生起させうる原因事象を洗い出してツリー状に展開する手法である。FTAは、シンプルなシステムや顕在化した不具合事象を解析するのに適しているとされている。

() 保全方式について述べた次の文章のうち、誤っているものは、□(ク)である。

<(ク)の解答群>

保全方式は事後保全と予防保全に分類され、予防保全は予知保全(状態監視保全)と時間計画保全に分類することができる。

保全方式における事後保全は、一般に、緊急保全と通常事後保全に分類することができる。通常事後保全は予防保全の対象としないシステムや装置の故障時に行う保全として分類されている。

状態監視保全では、装置やシステムの動作状態の確認、劣化傾向の検出などの目的で、動作値及びその傾向を監視し、異常の兆候が見られる場合に修理などを行う。

時間計画保全は、あらかじめ計画した時間間隔によって行う保全方式で、一般に、予定の累積動作時間に達したときに部品交換などを行う定期保全と、予定の時間間隔で部品交換などを行う経時保全に分類することができる。

- (1) 次の文章は、アウトソーシングなど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、□内の同じ記号は、同じ解答を示す。(2点×4=8点)

組織が部品やユニットの製造などを外部の組織に委託することについて、狭い意味で□(ア)という言葉が用いられており、さらに、設計や人事、経理などの業務を外部の組織に委託することも含め、これらを総称して、一般に、アウトソーシングという言葉が用いられている。

J S Q C (日本品質管理学会)において、アウトソーシングとは、組織が□(イ)を効果的かつ効率的に活用する目的で業務の一部を外部に委託することとされている。アウトソーシングには委託側企業と受託側企業があり、受託側企業は、一般に、□(ウ)といわれる。なお、委託側企業が、アウトソースしたプロセスに対する管理を確実にしたとしても、すべての顧客要求事項及び法令・規制要求事項への適合に対する組織の責任が免除されるものではない。

また、J I S Z 8 1 4 1 : 生産管理用語において、アウトソーシングとは、企業の経営資源を中核業務に集中させ、□(エ)を高めるために、部門機能の一部又はすべてを外部の企業に委託する方法とされており、また、□(ア)とは、自社(発注者側)の指定する設計・仕様・納期によって、外部の企業に、部品加工又は組立を委託する方法とされている。

<(ア)~(エ)の解答群>			
調 達	クライアント	外 注	外製依存度
内 作	社外の製品	内部の環境	インソーシング
保全性	外部の資源	安全性	テレワーカー
常備品	アウトソーサ	業務移管	業務効率

(2) 次の文章は、信頼性に関する事項などについて述べたものである。 内の(オ)、(カ)に最も適したものを、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)

() 故障曲線の特徴などについて述べた次の文章のうち、正しいものは、 (オ) である。

<(オ)の解答群>

アイテムの使用期間中における故障率の時間的変化を示したものは、一般に、故障曲線又は障害曲線といわれ、アイテムの拡張性を評価するために有効である。

故障曲線の代表的なものにバスタブ曲線がある。バスタブ曲線は、修理系アイテムに限定した故障曲線として用いられる。

バスタブ曲線の初期故障期間における故障率低減のための方策の一つにエージングがある。これは、アイテムを使用開始前又は使用開始後の初期に動作させることにより欠点を検出・除去し、是正することである。

バスタブ曲線の摩耗故障期間は、アイテムの老朽化による故障が多く発生する期間である。そのため、この期間においては予防保全によるアイテムの取替えが効果的である。

バスタブ曲線の偶発故障期間は、故障率がほぼ一定とみなせる期間であり、アイテムの通常の使用期間に相当する。この期間の長さは、一般に、故障寿命といわれる。

() 信頼性の評価指標などについて述べた次の文章のうち、正しいものは、 (カ) である。

<(カ)の解答群>

アイテムの信頼度 $R(t)$ は時間 t の関数であり、 $R(0) = 0$ 、 $R(\infty) = 1$ となる性質を持っている。

修理系のアイテムにおいて、修復時間の期待値は、MTBFといわれる。

アイテムがダウン状態にある期間の期待値は、MDTといわれる。

修理系のアイテムにおいて、最初の故障が発生するまでの動作時間の期待値は、MTTFといわれる。

(3) 次の文章は、ある装置の信頼性について述べたものである。 内の(キ)、(ク)に最も適したものを、下記のそれぞれの解答群から選び、その番号を記せ。ただし、装置は偶発故障期間にあるものとする。 (3点×2=6点)

() 装置Aの故障率が0.2 [%/時間]であるとき、固有アベイラビリティが98 [%]であるためには、MTTRは、 (キ) [時間]でなければならない。ただし、答えは四捨五入により小数第2位までとする。

<(キ)の解答群>		
0.10	10.20	19.60
490.00	510.20	

() 装置Aの故障率が0.2 [%/時間]、装置B及びCのMTBFがそれぞれ800 [時間]及び400 [時間]であるとき、装置A、B及びCがそれぞれ1台ずつ直列に接続されたシステムのMTBFは (ク) [時間]である。ただし、答えは四捨五入により整数値とする。

<(ク)の解答群>				
5	42	174	567	600

- (1) 次の文章は、ポートスキャン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。(2点×4=8点)

攻撃者がインターネット経由でサーバに攻撃を行う際、攻撃対象に対して事前調査を行うことがある。この調査には、ICMPプロトコルを使用した□(ア)を用いて対象のサーバの稼動状態を確認する方法、ポートスキャンにより攻撃対象のサーバがどのようなサービスを外部に公開しているかなどを確認する方法がある。

ポートスキャンは、サーバとの通信が□(イ)層プロトコルであるTCPやUDPを用いて行われていることを利用しており、各ポートに対して開いているかどうかを連続で調べていくことにより、対象サーバが提供しているサービスを特定することができる。

ポートスキャンにはさまざまな手法がある。このうち、□(ウ)スキャンは標的ポートに対して完全なスリーウェイハンドシェイクを行うため、サービスの特定精度は高いが対象サーバのログに残る可能性は高い。一方、□(エ)スキャンはスリーウェイハンドシェイクの途中でRSTを返信することでコネクション確立を行わないため、対象サーバのログに残りにくい。

ポートスキャンにより提供サービスが攻撃者に知られてしまうと、サーバの脆弱性^{ぜい}に対して攻撃を仕掛けられるおそれがあるため、不要なサービスは停止し、ポートを閉じるなどの対策を講じておくことが望ましい。

<(ア)~(エ)の解答群>

ネットワーク	オンライン	pingコマンド
アプリケーション	データリンク	configコマンド
スパニングツリー	TCP接続	ネットワークインタフェース
TCP SYN	HTTP	トランスポート
TCP FIN	トンネリング技術	

- (2) 次の問いの 内の(オ)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。
(3点)

情報システム的设计及び運用においてセキュリティ上配慮すべき事項など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>

セキュリティインシデント発生時やシステム障害発生時などにはネットワーク機器やホストのログが重要な情報源となる。ログの収集、分析、監査などを行うことによって、セキュリティインシデントの早期発見や防止に役立てることができる。

セキュリティインシデントに対応することは、ソーシャルエンジニアリングといわれる。適切なソーシャルエンジニアリングを行うためにはセキュリティポリシーをベースとして、実際のルールやフローを明確にしておく必要がある。

アクセス制御における基本原則は、任命された業務を遂行するために必要な権限のみを与えることとされている。

アクセス制御には、大別して、ファイアウォールなどを用いてネットワークの境界で行う方法とホストのOSやアプリケーションで行う方法がある。アクセス制御の結果は、一般に、ログとして記録される。

- (3) 次の問いの 内の(カ)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。
(3点)

Web経路の攻撃について述べた次のA～Cの文章は、 (カ) 。

- A JavaScriptは、Webページに動きや対話性を付加することができるJava類似のプログラム言語であるが、JavaScriptを攻撃対象のWebページに埋め込み、そのページの閲覧者を不正サイトに誘導したり、データを盗用したりするために用いられる場合がある。
- B データベースと連携したWebサイトに対する攻撃手法の一つに、クロスサイトスクリプティングがある。クロスサイトスクリプティングは、データベースを操作する言語であるSQLを使って不正にデータベースを操作することを目的としている。
- C 攻撃者がURLのパラメータなどにOSのコマンドを挿入し、利用者が意図しないOSコマンドを実行させる攻撃は、一般に、OSコマンドインジェクションといわれ、重要情報が盗まれたり、攻撃の踏み台に悪用されるおそれがある。

<(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 | |

- (4) 次の問いの 内の(キ)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。
(3点)

P K I の構成要素などについて述べた次の文章のうち、正しいものは、 (キ) である。

<(キ)の解答群>

デジタル証明書申請者は、デジタル証明書及びこれに対応する公開鍵を安全に保持しておく必要がある。

デジタル証明書利用者は、認証局が保有するリポジトリから情報を入手して受け取った秘密鍵証明書が有効か否かを確認する。

認証局では、提出された公開鍵と申請者の情報に認証局の秘密鍵を用いて署名することによりデジタル証明書を作成する。

有効期間内のデジタル証明書であっても、秘密鍵の漏洩^{えい}やデジタル証明書申請者から失効の申し出などがあった場合には、認証局では当該のデジタル証明書を C R L (Certificate Revocation List) に加え、C R L は認証局において秘密に管理される。

- (5) 次の問いの 内の(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。
(3点)

デジタル署名又は M A C について述べた次の文章のうち、誤っているものは、 (ク) である。

<(ク)の解答群>

送信データへのデジタル署名は、悪意のある第三者による送信データの改ざんの有無と署名を行った送信者のなりすましを確認することができ、送信者が否認することの防止、改ざん検出、認証などに利用されている。

デジタル署名では、署名を行った送信者の公開鍵が漏洩しても、なりすましやメッセージの改ざんの危険は発生しない。

M A C (Message Authentication Code) は、送信者と受信者が鍵を共有するため、受信者が認証情報の改ざんを行うことが可能である。

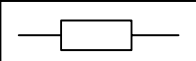

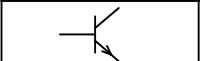

D S A デジタル署名は、E l G a m a l 署名の一種で、素因数分解問題を用いた公開鍵ペアを用いている。

試験問題についての特記事項

(1) 試験問題に記載されている製品名は、それぞれ各社の商標又は登録商標です。
なお、試験問題では、® 及び TM を明記していません。

(2) 問題文及び図中などで使用しているデータは、すべて架空のものであります。

(3) 試験問題、図中の抵抗器及びトランジスタの表記は、旧図記号を用いています。

新図記号	旧図記号	新図記号	旧図記号
			

(4) 論理回路の記号は、MIL記号を用いています。

(5) 試験問題では、常用漢字を使用することを基本としていますが、次の例に示す専門的用語などについては、常用漢字以外も用いています。

[例] ・迂回(うかい) ・筐体(きょうたい) ・輻輳(ふくそう) ・燃り(より) ・漏洩(ろうえい) など

(6) バイト(Byte)は、デジタル通信において情報の大きさを表すために使われる単位であり、一般に、2進数の8桁、8ビット(bit)です。

(7) 情報通信の分野では、8ビットを表すためにバイトではなくオクテットが使われますが、試験問題では、一般に、使われる頻度が高いバイトも用いています。

(8) 試験問題のうち、正誤を問う設問において、句読点の有無など日本語表記上若しくは日本語文法上の誤りだけで誤り文とするような出題はしてありません。

(9) 法令に表記されている「メガオーム」は、「メガオーム」と同じ単位です。

(10) 法規科目の試験問題において、個別の設問文中の「」表記は、出題対象条文の条文見出しを表しています。また、出題文の構成上、必ずしも該当条文どおりには表記しないで該当条文中の()表記箇所の省略や部分省略などを行っている部分がありますが、()表記の省略の有無などで正誤を問うような出題はしてありません。