平成２０年度　第１回
電気通信主任技術者試験問題

午前の部
法規・設備及び設備管理

注　意　事　項

1　試験開始時刻　　**１０時００分**

2　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**

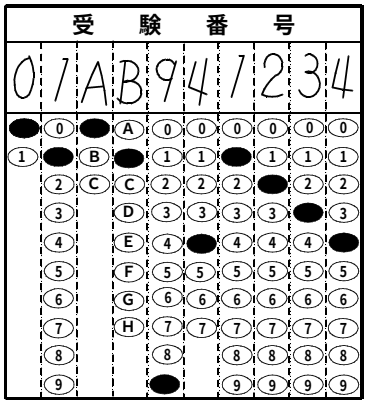
3　試験種別と試験科目別の問題(解答)数及び試験問題ページ

試　験　種　別	試　験　科　目	問　題　(　解　答　)　数					試験問題
		第1問	第2問	第3問	第4問	第5問	ペ　ー　ジ
伝送交換主任技術者	法　規	7	6	7	7	6	1～12
	伝送交換設備及び設備管理	8	8	8	8	8	13～26
線路主任技術者	法　規	7	6	7	7	6	1～12
	線路設備及び設備管理	8	8	8	8	8	27～37

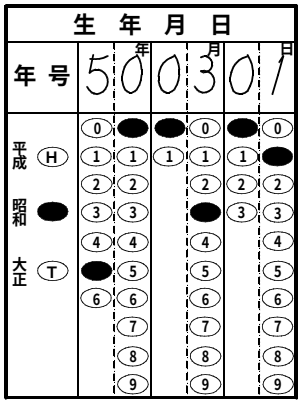
4　受験番号等の記入とマークの仕方

(1) **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。**
(2) **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。**
(3) **生年月日の欄は、年号をマークし、生年月日に１けたの数字がある場合、十の位のけたの「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



5　答案作成上の注意

(1) **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。
(2) **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。**
① **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。
② **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。
③ **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。**
(3) **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。
(4) **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。)
① 伝送交換主任技術者は、　　**『伝 送 交 換』**
② 線路主任技術者は、　　**『線　　路』**

6　合格点及び問題に対する配点

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

7　登録商標などに関する事項

(1) 試験問題に記載されている会社名又は製品名などは、それぞれ、各社の商標または登録商標です。
(2) 試験問題では、® 及び ™ を明記していません。
(3) 試験問題の文中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、ＩＰ系におけるインタラクティブ通信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)

ＶｏＩＰなどＩＰ系におけるインタラクティブ通信のためのプロトコルは、［(ア)］系プロトコル、［(イ)］系プロトコル、ＭＧ制御系プロトコルなどに分類される。

［(ア)］系プロトコルは、発信側からの要求に応じた着信先の指定機能、チャネル(通信回線)の設定・切断機能、エンド・ツー・エンドで［(イ)］系プロトコルが動作する環境や条件を調整するなどの機能を有しており、ＩＳＤＮユーザ・網インタフェース信号方式をベースにした［(ウ)］、ＨＴＴＰのメッセージフォーマットなどをベースにしたＳＩＰがある。

ＳＩＰにおける［(エ)］は、ＳＩＰユーザエージェントとＳＩＰユーザエージェントの間にあって、端末の代理としてセッションを制御する。

<(ア)～(エ)の解答群>

①　ＡＴＭ	②　ＢＩＣＣ	③　Ｈ.２６４	④　Ｈ.３２３
⑤　ゲートキーパ	⑥　ＳＮＭＰ	⑦　Ｗｅｂサーバ	⑧　呼番号
⑨　プロキシサーバ	⑩　高度ＩＮ	⑪　パケット通信	⑫　呼制御
⑬　デジタル交換機	⑭　情報転送	⑮　呼情報	⑯　保守運用

(2) 次の文章は、ＩＰ網におけるルーチングプロトコル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)

(i) ＲＩＰ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>

① ＲＩＰは、異なる自律システム間を接続させるために用いられるプロトコルである。

② ＲＩＰにおけるホップ数は、あて先ネットワークへ到達するまでに経由するルータの数であり、ホップ数の最大値は１６であることから、１７台を超える数のルータを経由させることができず、大規模なネットワークはサポートできない。

③ ルーチングループを発生させないようにするため、ルーチング情報を受信したインタフェースには、受信した情報を送らないようにする機能が具備されており、この機能はポイズンリバースといわれる。

④ 故障などの発生していないネットワークの運用状態におけるルーチング情報の更新は、一般に、３０秒ごとに行われる。

⑤ ＲＩＰversion2(ＲＩＰｖ２)では、マルチキャストによるルーチング情報の更新が可能となったが、ネットワークへの負荷軽減の観点から、ＲＦＣでは、ブロードキャストが推奨されている。

(ii) ＯＳＰＦ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>

① ＯＳＰＦは、リンクステート型のルーチングプロトコルであり、エリア内のすべてのルータがネットワーク全体の接続状態情報を持っている。

② ＯＳＰＦでは、あて先ネットワークまでの経路を選択するための基準(メトリック)として、コストを用いている。コストは、経路構築に要した支出額に比例した値であり、通常、ネットワークの管理者が設定する。

③ ＯＳＰＦにおけるネットワークの監視にはＨｅｌｌｏパケットを、ルーチング情報の送受信には、ＬＳＵ(Link State Update)パケットが用いられる。

④ ＬＳＵパケットで運ばれるルーチング情報には、サブネットマスクが含まれており、可変長サブネットマスクに対応している。

⑤ ＯＳＰＦでは、ネットワークを複数のエリアに分割し、エリアごとにネットワーク情報をまとめて取り扱うことができる。

(3) 次の文章は、信頼性設計及び保全性設計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)

(i) 信頼性設計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>

① 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、信頼性設計技術が用いられている。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、構造の簡素化、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、誤操作防止に効果のある人間工学的施策の導入などがある。

② 劣化故障の予測には、システムや装置を構成する部品の特性値の経時変化から劣化故障を予測する方法が用いられている。具体的な手法としては、最悪値設計法、モンテカルロ法、パラメータ設計法などがある。

③ ＦＭＥＡ(Failure Mode and Effects Analysis)は、システムや装置の故障原因として考えられる特定部品の劣化度やソフトウェアのバグなどが全体に及ぼす影響を予測し、システムに顕在化している弱点を摘出する手法である。

④ ＦＴＡ(Fault Tree Analysis)は、あらかじめ対象システムにとって望ましくないすべての事象を規定し、その事象の解決策を洗い出してツリー(Tree)状に展開する。ＦＴＡは複雑なシステムの修理方法や潜在的な不具合事象の解析に適している。

(ii) 保全性設計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>

① 保全性設計で用いられる保全性特性値には、保全度、修復率、ＭＴＴＲ、ＭＤＴ(Mean Down Time)などがある。

② 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。緊急保全は、予防保全を行う対象となるシステムや装置の故障時に行う保全であり、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。

③ 保全方式における予防保全は、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。予知保全では、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、異常の兆候がある場合に修理などを行う。

④ 保全方式における予防保全のうち、時間計画保全には、システムや装置の休止状態又は待機状態において故障の兆候や性能低下などを定期的な機能試験などで確認して状態が異常の場合に処置を行う方式と、使用状態を常時又は定期的に特定のイベントごとに監視し、異常を早期に発見し処置する方式がある。

問２　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、動画像情報の圧縮技術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)

動画像情報の圧縮技術には、元の画像の時間的相関関係を利用した圧縮処理と空間的相関関係を利用した圧縮処理がある。このうち、空間的相関関係を利用した圧縮処理は、動画を構成する各画面の中で、隣接する画素間の関係を基に情報圧縮を図るものであり、一定の画素数で構成される正方形の領域に対して［(ア)］といわれる処理を施す方式が広く採用されている。

動画像情報の圧縮符号化の際には、時間的相関関係及び空間的相関関係を利用した圧縮処理とともに、情報の出現確率の偏りを利用した［(イ)］符号化を用いて更なる圧縮を図っている。

動画像情報の圧縮符号化技術の標準化は、多くの機関で実施されており、その一例として、［(ウ)］のワーキンググループから勧告された［(エ)］がある。［(エ)］は、一般に、デジタル放送やＣＡＴＶなどの放送分野で用いられている。

<(ア)～(エ)の解答群>

①　ＭＰＥＧ－１	②　ＩＴＵ－Ｔ	③　ＭＲ	④　ＤＣＴ
⑤　ＭＰＥＧ－２	⑥　ＩＴＵ－Ｒ	⑦　スプライト	⑧　差　分
⑨　ＪＰＥＧ	⑩　ＩＳＯ／ＩＥＣ	⑪　可変長	⑫　誤り訂正
⑬　Ｈ.２６１	⑭　ＩＥＴＦ	⑮　動き補償	⑯　固定長

(2) 次の文章は、ＵＰＳなどに用いられるインバータの種類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)

(i) 自励式インバータ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>

① インバータは、直流電力を交流電力に変換する機能を有する。インバータには他励式インバータと自励式インバータとがあり、一般に、自励式インバータが広く使用されている。

② 電圧型インバータの出力電圧波形は、く形波パルスとなり、出力電流波形が正弦波に近い波形となる。また、電流型インバータの出力電流波形は、く形波パルスとなり、出力電圧波形が正弦波に近い波形となる。

③ 電圧型インバータは、交流電圧を出力し、入力側には直流電圧を平滑化するため、平滑コンデンサが使用される。

④ 電圧型インバータは、電流型インバータと比較して電源インピーダンスが大きく、過電圧保護が難しい半面、負荷短絡時の過電流保護が比較的容易である。

⑤ 電流型インバータは、交流電流を出力し、入力側には直流電流を平滑化するため、直流リアクトルが使用される。

(ii) インバータの電圧制御方式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>

① インバータの出力電圧を制御する方式には、直流電圧を制御する方式、インバータの半導体の導通時間を変えてパルス幅を制御する方式及び出力側に定電圧制御装置を設ける方式があり、ほとんどのＵＰＳは、定電圧制御装置を設ける方式である。

② インバータの出力電圧を制御するため、直流チョッパ装置を設ける方法では、インバータの位相制御により高調波電圧が発生する。この高調波電圧含有量は出力電圧に比例する。

③ ＰＷＭ制御方式は、得ようとする出力交流電圧の半サイクルの間に複数個のパルスを発生させ、それらのパルス電圧のパルス幅を制御することによりその合計値を正弦波に近づける方式である。

④ 多重インバータ方式は、複数台のく形波インバータを並列に配置し、各々から出力される異なった振幅の出力を同位相で合成することにより、正弦波に近い出力波形を得る方式である。

⑤ インバータで作られる出力電圧波形は、一般に、く形波である。このため、インバータの出力側には、リアクトルとコンデンサの組合せで構成される三巻線変成器が用いられる。

(３) 次の問いの [　　] 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)

移動通信システムに用いられる多元接続方式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>

① 移動通信に用いられるＵＨＦ帯は、ユーザのトラヒック需要に対し、十分な周波数帯域を有するため、一般に、ユーザが用いる周波数チャネルをあらかじめ固定し、そのユーザで占有させるプリアサイン接続方式が用いられている。

② 周波数スペクトル軸上に独立にチャネルを配置するＦＤＭＡ方式には、デュープレクス通信を行うための方式として、ＦＤＤ方式及びＴＤＤ方式があり、ＦＤＤ方式においては、時間軸での多元接続同期処理が不要である特徴を有する。

③ アナログ自動車電話及びアナログ携帯電話において採用されているＴＤＭＡ方式は、各移動局と基地局間の距離差などによるバースト信号の時間軸上でのオーバラップを防止するためのガードタイムが必要である。

④ 符号拡散を利用したＣＤＭＡ方式では、無線チャネルは同一の無線周波数において全ユーザが同一の符号(コード)を用いて変調される。

(４) 次の問いの [　　] 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)

移動通信システムに用いられる音声符号化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>

① 移動通信システムにおける音声符号化技術は、限られた周波数を有効に利用するための必要な技術であり、高ビットレートでの符号化が要求される。

② 音声符号化の方法には、音声波形そのものを忠実に再現することを目的に信号の冗長度を圧縮する波形符号化法、音声生成モデルのパラメータを符号化する分析合成法などがある。

③ 移動通信環境下での伝搬条件における音声符号化方式には、無線伝送路での符号誤り及び受信入力レベルの変動に対しても音声品質が大きく劣化しない技術が要求される。

④ ＣＥＬＰ方式は、ＡＰＣ方式と比較して、圧縮率を高くすることができ、無線伝送路の有効利用が図れることから、一般に、移動通信システムの標準方式として選定されている。

問３　次の問いに答えよ。　(小計２０点)

(１)　次の文章は、公衆電話網及びＩＳＤＮ網の加入者線区間における選択信号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)

電話機と交換機間における選択信号の伝送方式には、ＤＰ信号方式とＰＢ信号方式がある。

ＤＰ信号方式は、加入者線ループを選択数字に従った［　(ア)　］のパルスとなるよう断続させて数字情報を伝達する方式であり、ＰＢ信号方式と比較して、その伝達速度が遅い。

ＰＢ信号方式は、低群及び高群のそれぞれ［　(イ)　］つの周波数の中からそれぞれ１周波数ずつを組み合わせて、選択信号の数字やその他の符号を構成する方式である。ＰＢ信号は、［　(ウ)　］であるため、選択信号として使用する以外に、通話中のエンド・ツー・エンド信号としても使用可能である。

ＩＳＤＮ基本インタフェースでは、Ｄチャネルといわれる信号チャネルを通じて選択信号が伝送されており、各々の選択数字は［　(エ)　］で表される。

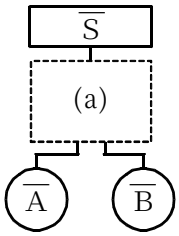
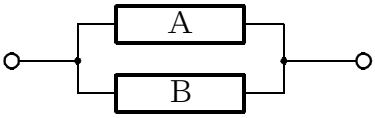
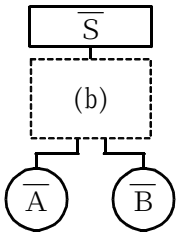
<(ア)～(エ)の解答群>

①　２	②　３	③　４	④　８
⑤　振　幅	⑥　幅	⑦　回　数	⑧　可聴信号
⑨　ＢＣＨ符号		⑩　ＬＡＰＤ	
⑪　４ビットのコード		⑫　８ビットのコード	
⑬　共通線信号方式		⑭　アウトチャネル信号	
⑮　ＭＦ信号方式と同一周波数			

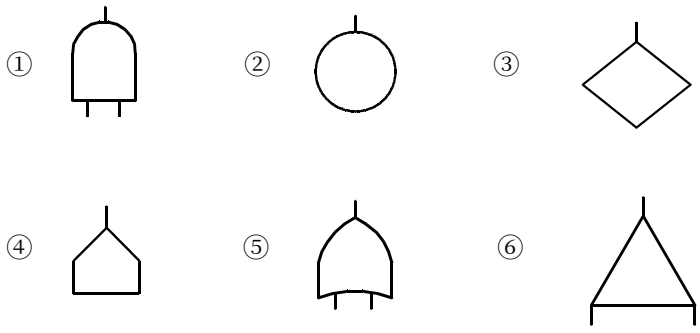
(2) 次の文章は、信頼性ブロック図などについて述べたものである。［　　］内の(オ)、(カ)に適したものを、下記の解答群から選び、その番号を記せ。　　(3点×2＝6点)

図は、システムの信頼性ブロック図とＦＴ図の対応を示したものである。図中の(ａ)は［（オ）］、(ｂ)は［（カ）］である。ただし、それぞれのシステムが正常の事象はＳで表し、構成要素Ａ(又は構成要素Ｂ)が正常の事象はＡ(又はＢ)で表し、さらに、システムが故障の事象は$\overline{S}$で表し、構成要素Ａ(又は構成要素Ｂ)が故障の事象は$\overline{A}$(又は$\overline{B}$)で表している。

直列システムと並列システムの信頼性ブロック図とＦＴ図の対応

	信頼性ブロック図	Ｆ　Ｔ　図
直列システム		
並列システム		

<(オ)、(カ)の解答群>



(3) 次の文章は、日程管理に用いられるアローダイヤグラムなど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)

(i) 日程管理などに用いられるアローダイヤグラムについて述べた次の文章は、［(キ)］。

A　アローダイヤグラムは、各作業を矢線で表し、作業の従属関係にしたがって矢線を相互に結び、アローダイヤグラムの出発点を0日として、日程管理などに活用される。

B　アローダイヤグラムにおける日程の計算には、その作業を最も早く始めることができる最早開始日程、その作業を最も早く終了する最早終了日程、その作業を遅くとも終了しておかなければならない最遅終了日程、その作業を遅くとも始めなければならない最遅開始日程がある。

C　アローダイヤグラムにおいて、クリティカルパスとは、作業の出発点から作業の最終点に至るまでの最短経路で、日程管理上の重点となる作業の連なりをいう。

<(キ)の解答群>
① Aのみ正しい　② Bのみ正しい　③ Cのみ正しい
④ A、Bが正しい　⑤ A、Cが正しい　⑥ B、Cが正しい
⑦ A、B、Cいずれも正しい　⑧ A、B、Cいずれも正しくない

(ii) 表は、あるプロジェクトが作業を実施するに当たり、その作業名と所要期間及び各作業の前に完了していなければならない先行作業を示したものである。このプロジェクトの着手から終了までの最短期間は、［(ク)］日である。

作業名	A	B	C	D	E	F	G
所要期間〔日〕	3	3	4	9	3	4	2
先行作業	なし	A	なし	なし	B及びC	B及びC	D，E及びF

<(ク)の解答群>
① 9　② 10　③ 11　④ 12　⑤ 28

問４　次の問いに答えよ。　(小計２０点)

(１)　次の文章は、情報通信ネットワークの安全・信頼性対策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)

情報通信ネットワーク安全・信頼性基準(郵政省告示第７３号、総務省告示第１４４号)は、情報通信システムにおける安全・信頼性対策全般にわたり、基本的、かつ、総括的な指針を示すものである。本基準は、全部で１１９項目２４３対策からなっており、設備及び設備を構成する環境の基準である［(ア)］と、設計、施工、保全及び運用などの基準である管理基準とに区分されている。

情報通信ネットワーク安全・信頼性基準における管理基準は、５５項目８７対策から構成されており、ネットワークの設計管理、施工管理、保全・運用管理のほか、設備の更改・移転管理、［(イ)］管理、環境管理など広い範囲に及んでいる。これら基準項目のうち、ネットワークの設計管理、施工管理及び保全・運用管理に関する項目は１９項目あり、それらの項目は下表のとおりである。

ネットワーク設計管理	［(ウ)］の明確化 設計指針の明確化等 設計工程の明確化等 相互接続への対応 品質・機能検査の充実化
ネットワーク施工管理	［(ウ)］の明確化 作業工程の明確化等 相互接続への対応 委託工事管理 検収試験管理
ネットワーク保全・運用管理	［(ウ)］の明確化 基準の設定 作業の手順化 監視、保守及び制御 相互接続への対応 委託保守管理 保守試験管理 情報の収集 ［(エ)］対策

<(ア)～(エ)の解答群>

① 停　電	② 体　制	③ 一般基準	④ トラヒック
⑤ 地　震	⑥ 予備品	⑦ 設備等基準	⑧ 責任の範囲
⑨ 火　災	⑩ 作業分担	⑪ 技術基準	⑫ 電気通信事業法
⑬ 品　質	⑭ ふくそう	⑮ 連絡体系	⑯ 情報セキュリティ

(２)　次の文章は、修理系の装置Ａの信頼性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、下記の解答群から選び、その番号を記せ。　　(３点×２＝６点)

装置Ａの稼働実績データを分析したところ、平均故障率が２．５×１０$^{-4}$〔件／時間〕の結果が得られた。この装置Ａについて次の問いに答えよ。ただし、この装置Ａは偶発故障期間にあるものとする。また、指数関数の値は、ｅ$^{0.1}$＝１．１１、ｅ$^{0.5}$＝１．６５とし、ｅは、自然対数の底とする。なお、答えは、有効数字は２けたとする。

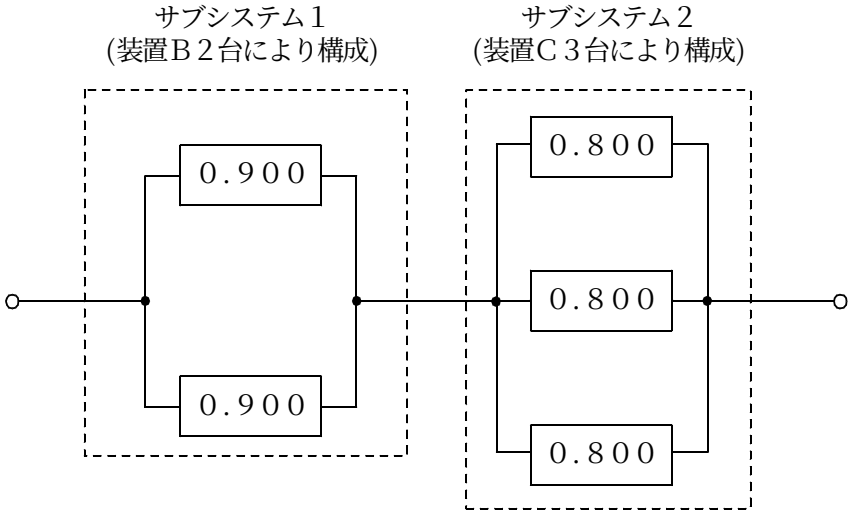
(ｉ)　装置ＡのＭＴＢＦは、［　(オ)　］〔時間〕である。

(ii)　装置Ａの動作開始後２,０００時間における信頼度は、［　(カ)　］である。

<(オ)、(カ)の解答群>

①　４．２×１０$^{-6}$	②　１．５×１０$^{-2}$	③　０．３９
④　０．５０	⑤　０．６１	⑥　１．６
⑦　４．０×１０^{3}	⑧　２．４×１０^{5}	

(３)　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(キ)、(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、四捨五入により小数第３位までとする。　　(３点×２＝６点)



(ｉ)　装置Ｂ２台からなる二重化されたサブシステム１(１／２冗長構成)の信頼度は、［　(キ)　］である。

(ii)　装置Ｂ２台からなる二重化されたサブシステム１(１／２冗長構成)と装置Ｃ３台からなるサブシステム２(２／３多数決冗長構成)を接続した全体のシステムの信頼度は、［　(ク)　］である。

<(キ)、(ク)の解答群>

①　０．８１０	②　０．８７９	③　０．８８７	④　０．９１０
⑤　０．９５０	⑥　０．９７２	⑦　０．９８２	⑧　０．９９０

問５　情報セキュリティに関する次の問いに答えよ。　(小計２０点)

（１）　次の文章は、ファイアウォール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）

ファイアウォールは、組織の内部ネットワークとインターネットの間で許可する通信と禁止する通信を管理するものであり、一般に、［（ア）］型とアプリケーションゲートウェイ型に大別される。このうち、［（ア）］型は、［（イ）］を用いた通信処理の一部として用いられており、高速に動作するが細部にわたる通信の検査など複雑な処理には適していない。［（イ）］は、インターネットで標準的に使われるプロトコルの総称のことであり、インターネットプロトコルスイートともいわれる。

ファイアウォールで実現可能な機能としては、一般に、［（ウ）］制御、通信にかかわるログの取得などがある。また、ファイアウォールの付加機能として、［（エ）］機能、ＮＡＴ機能、ＶＰＮ機能などを追加することがある。［（エ）］機能は、アプリケーションゲートウェイ型の一種であり、不適切なＷｅｂサイトの閲覧を制限する手法として用いられることが多い。

<(ア)～(エ)の解答群>

①　帯　域	②　テキスト	③　グラフィック	④　ＴＣＰ／ＩＰ
⑤　優　先	⑥　アクセス	⑦　リンクステート	⑧　リモートバッチ
⑨　蓄　積	⑩　マクロ	⑪　コンテンツフィルタリング	
⑫　メールフィルタリング		⑬　パケットフィルタリング	

(２)　次の問いの［　　］内の(オ)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)

共通鍵暗号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>
① 共通鍵暗号方式の一つであるＡＥＳ暗号は、ＤＥＳ暗号の後継のブロック暗号である。ＡＥＳ暗号は、鍵の長さとして１２８ビット、１９２ビット及び２５６ビットが利用可能であることから、ＤＥＳ暗号と比較して、強固な安全性を持っている。
② 共通鍵暗号を用いる場合、安全性評価が行われた方式を選択して、一連のデータをやり取りするセッションごとに暗号鍵を変更するなどの安全性対策が必要である。
③ 共通鍵暗号方式は、公開鍵暗号方式と比較して、暗号化／復号化の処理速度が速いことから、データ量の多い情報や映像情報の秘匿に適している。
④ 共通鍵の安全な管理を実現する手段として、データを暗号化するためのデータ暗号化鍵と鍵自体を暗号化する鍵暗号化鍵との２種類の鍵を使用する方法がある。このうち、データ暗号化鍵は、事前に送信者と受信者間で安全な手段で共有しておく必要がある鍵である。

(３)　次の問いの［　　］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)

デジタル署名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>
① Ｓ／ＭＩＭＥなどで用いられるＣＭＳは、共通鍵暗号を用いたＡＳＮ.１形式のデジタル署名フォーマットである。
② デジタル署名は、データの発信者特定による否認防止、改ざん検出や認証などに利用されている。
③ デジタル署名は、一般に、公開鍵暗号を用いる場合が多いが、不特定多数に対してデジタル署名を提供する場合には共通鍵暗号を用いることが多い。
④ ＤＳＡデジタル署名は、素因数分解問題の困難性を利用したもので、ハッシュアルゴリズムには、ＳＨＡ－１が用いられている。
⑤ ＲＳＡデジタル署名は、離散対数問題の困難性を利用したもので、暗号と署名の機能を同時に実現できる。

(４) 次の問いの [　　] 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)

ＩＳＯ／ＩＥＣ ＴＲ１３３３５(ＧＭＩＴＳ:ＩＴセキュリティに対するガイドライン)に基づくリスク分析アプローチ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>
① ベースラインアプローチは、個々の情報資産の分析作業に多くの時間、労力、専門知識などを必要とするが、適切な管理策の選択ができる手法である。
② 詳細リスク分析は、基本的なリスクを想定した上で、既存の基準やガイドラインから管理策を選択する手法である。
③ 非形式的アプローチは、体系的、構造化されたリスク分析手法ではないため、詳細リスク分析と比較して、時間、労力などをあまり必要としないが、リスク分析の結果を正当化することが必要となる手法である。
④ 組合わせアプローチは、一般に、詳細リスク分析と非形式的アプローチを組み合わせることにより、リスク分析を実施する重要な部分を厳密に押さえながら全体についても基本的な管理策を適用できる手法である。

(５) 次の問いの [　　] 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)

ファイル共有ソフトウェアＷｉｎｎｙなど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>
① Ｗｉｎｎｙは、ピア・ツー・ピア(Ｐ２Ｐ)型のファイル共有ソフトウェアであり、ファイルの情報は利用者間をバケツリレー式に転送される。
② Ｗｉｎｎｙでファイルをダウンロードすると、そのファイルは他の利用者に向けて自動的に公開される。
③ Ｗｉｎｎｙの特徴の一つは、違法なデータがやり取りされていても監視や規制を行うことが事実上不可能で一元管理が困難なことである。
④ Ｗｉｎｎｙを利用しているパーソナルコンピュータには、Ｗｅｂページの閲覧、メールの添付ファイル実行などでコンピュータウイルスが感染することはなく、Ｐ２Ｐファイル共有ソフトウェアの共有フォルダ経由でコンピュータウイルスが感染する。