平成１８年度　第２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**

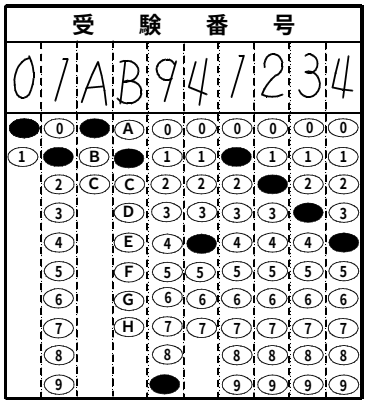
3　試験種別と試験科目別の問題(解答)数及び試験問題ページ

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	6	7	7	7	6	1～13
	伝送交換設備及び設備管理	8	8	8	8	8	14～26
線路主任技術者	法　規	6	7	7	7	6	1～13
	線路設備及び設備管理	8	8	8	8	8	27～38

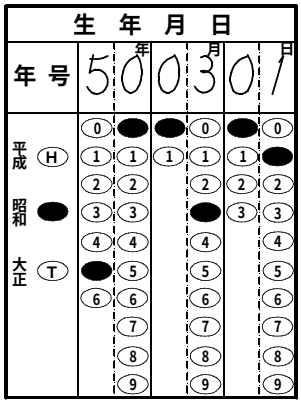
4　受験番号等の記入とマークの仕方

(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、ＳＤＨ／ＳＯＮＥＴ伝送路を用いてＩＰパケットを伝送する技術であるＰＯＳ方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、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)

ＳＤＨ／ＳＯＮＥＴ伝送路を用いて、ＩＰパケットを伝送する方法の一つに、ＰＯＳ(Ｐａｃｋｅｔ over ＳＤＨ／ＳＯＮＥＴ)方式がある。ＰＯＳ方式は、ＩＰパケットをＨＤＬＣ準拠のＰＰＰ(Point to Point Protocol)フレームで［(ア)］し、［(ア)］されたＩＰパケットを、ＳＤＨ／ＳＯＮＥＴフレームのペイロードに収容して伝送する方式である。

ＰＯＳ方式では、ＩＰ over ＡＴＭのような、セル単位に［(イ)］を付加することなく、ＳＤＨ／ＳＯＮＥＴフレームを用いるため、ＩＰパケットを効率的に伝送することができる。また、セルへの組立て・分解処理を行わないため、ネットワークでの伝送遅延が小さいという特徴もある。

ＰＯＳ方式で使用するＰＰＰフレームの［(イ)］には、フレームの［(ウ)］を記述するフィールドが設定されているが、ＰＯＳ方式では、ポイント・ツー・ポイント通信への適用を想定しているため、このフィールドは［(エ)］としている。

一方、このフィールドを拡張し、フレームの［(ウ)］を入れることによりマルチポイント・ツー・マルチポイント通信を可能とする方式も実用化されている。

<(ア)～(エ)の解答群>

①　ＳＯＨ	②　分　割	③　正規化	④　連続値
⑤　ヘッダ	⑥　トレイラ	⑦　ＭＡＣアドレス	⑧　プロトコル
⑨　固定値	⑩　多重化	⑪　カプセル化	⑫　プリアンブル
⑬　ランダム値	⑭　制御情報	⑮　あて先アドレス	⑯　不定値

(２) 次の文章は、信頼度と故障率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) 故障率の基本パターン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 故障率減少型(ＤＦＲ)は、システムの初期運用時によくみられる。また、保全作業やシステムの改造などの直後にも、一時的に表れる場合がある。

② 故障率一定型(ＣＦＲ)の時期の持続時間は、システムの有用(有効)寿命の長さに反比例する。

③ 故障率一定型(ＣＦＲ)の時期は、故障の発生が偶発的である。予防保全としての定期交換が有効である。

④ 故障率増加型(ＩＦＲ)は、システムの耐用寿命が来る時期によくみられる。ＩＦＲ期における信頼性改善方法として、エージング試験などが有効であり、この時期のＭＴＢＦ(修理系)又はＭＴＴＦ(非修理系)は故障率の逆数となる。

⑤ 故障率増加型(ＩＦＲ)の時期における信頼度は、故障率と同様、時間の経過とともに増加する。

(ⅱ) 信頼度と故障率の関係などについて述べた次のＡ～Ｃの文章は、 [(カ)] 。

Ａ 偶発故障期での信頼度は、時間の指数分布に従い、故障率も、時間の指数分布となる。

Ｂ 故障率関数は、故障確率密度関数を信頼度関数で除した値となる。

Ｃ 不信頼度関数と信頼度関数の和は、どの時間においても、常に“１”となる。

<(カ)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

(3) 次の文章は、ＩＰ電話網における品質劣化要因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) 伝送遅延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>

① ０５０番号を提供するＩＰ電話網での伝送遅延の変動は、０ＡＢ～Ｊ番号を提供する固定電話網と比較して小さい。

② 送信側ゲートウェイでは、音声信号のディジタル化やパケット化などの処理を行う。パケット化による遅延は、一つのパケットに収容する音声データを小さくし、音声パケットの送出間隔を短くすれば小さくすることができる。

③ 送信側ゲートウェイでは、音声信号をパケット化し、一定の送出間隔で送出する。受信側ゲートウェイでは、これら音声パケットの到着時間間隔にずれが発生することがあり、これはジッタといわれる。ジッタは、そのすべてが、送信側ゲートウェイ及び受信側ゲートウェイ内の処理で発生している。

④ ジッタによる音声品質劣化への影響を抑えるため、受信側ゲートウェイでは、ゆらぎ吸収バッファ(ジッタバッファ)を実装している。バッファメモリを大きくすることにより、ジッタ及び遅延の影響を小さくすることができる。

(ii) 音声パケットの損失及びエコー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 ＩＰ網の経路上で音声パケットの損失があると、受信側ではその部分の音声を再生できず、音声が途切れる場合がある。音声パケットの損失は、受信側ゲートウェイでも発生する。

② ＩＰ網の経路上で音声パケットの損失が起こる原因の一つに、網のふくそうにより、ルータが過負荷になるために起こるバッファオーバフローがある。音声パケットが、ＵＤＰで送信されている場合、音声パケットの損失が発生すると、パケットの再送が行われる。

③ ＩＰ網では、音声パケットの送信元からあて先までの経路が変化することで、先に送信した音声パケットが後から受信されるという順序逆転が生ずることがある。受信側ゲートウェイのゆらぎ吸収バッファ(ジッタバッファ)は、この順序逆転を元に戻す機能は有していない。

④ エコーには、４線式回線と２線式回線の変換回路(ハイブリッド回路)で発生するエコーがある。このエコーによる音声品質の劣化を抑えるため、受信側ゲートウェイでは、エコーキャンセラーといわれるエコー除去機能が搭載されているものがある。

問２　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、アクセス制御方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、下記の解答群から選び、その番号を記せ。　　(２点×４＝８点)

バス型の物理トポロジーを有し、接続される複数の端末が伝送媒体を共有するＬＡＮなどの通信形態においては、それぞれの通信が相互に影響を与えないよう制御を行うことが求められる。

イーサネットに代表される、複数の端末が共有の伝送媒体を使用して送受信する多重アクセス伝送方式では、複数の端末が同時に送信を開始した場合、信号の［(ア)］が発生する。

イーサネットのアクセス制御では、フレームを送信する端末が、送信前に、他の端末が送信していないかどうかをキャリアの検知により確認する［(イ)］方式が用いられている。

無線ＬＡＮのアクセス制御では、端末によって電波の届く範囲が異なり、お互いにすべての無線信号を受信できないため、自立的に送信制御する［(ウ)］方式が用いられている。

一方、ＩＳＤＮのユーザ・網インタフェースでは、複数の端末がＤチャネルを共用する共通チャネル形信号方式が用いられており、複数の端末が同時にＤチャネルにアクセスした場合でも常に情報の正確な伝送を保証するため、［(エ)］方式によるＤチャネルアクセス制御手順が規定されている。

<(ア)～(エ)の解答群>

①　拡　散	②　衝　突	③　同期はずれ
④　ＡＣＫ	⑤　パリティチェック	⑥　エコーチェック
⑦　ポーリング	⑧　トークン	⑨　パッシング
⑩　フレームチェック	⑪　ＴＤＭＡ	⑫　ＣＳＭＡ／ＣＤ
⑬　ＣＳＭＡ／ＣＡ	⑭　ＣＤＭＡ	⑮　ＦＤＭＡ

(２)　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、［(オ)］である。　　(３点)

<(オ)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方式は、ＳＣＰＣ(Single Channel Per Carrier)により構成でき、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。

(3) 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、 (カ) である。 (3点)

<(カ)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、伝送路での符号誤り、周囲雑音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求められる。

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。

(4) 次の文章は、ＵＰＳ(無停電電源装置)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) ＵＰＳの構成、機能など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>

① ＵＰＳは、整流装置、蓄電池、インバータ、蓄電池の接続のためのスイッチ、商用電源との切替を行う切替スイッチなどから構成されている。

② ＵＰＳで広く使用されている電圧形インバータから出力される電圧波形は方形波であり、これを正弦波に変換するため、ＰＦＭ(Pulse Frequency Modulation)制御が用いられている。

③ ＵＰＳの故障時など、負荷への電力供給の途絶を防止するため、商用電源への切替方式として無瞬断バイパス切替方式がある。

④ ＵＰＳと商用電源との相互切替時に用いられる同期制御は、切替時における瞬断や電圧変動を許容値内に抑えるため、インバータの出力と商用電源との同期運転を行い、同一周波数、同一位相での切替を行う機能である。

(ⅱ) ＵＰＳの蓄電池接続方式である「直流スイッチ方式」と「フロート方式」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>

① 直流スイッチ方式は、半導体スイッチを介して蓄電池がＵＰＳの直流母線に接続され、一般に、整流器は、インバータと蓄電池に対して常時、並列に給電する。

② 直流スイッチ方式では、停電発生時に発生するインバータ出力の瞬断を小さくするため、一般に、半導体スイッチにサイリスタスイッチのような動作速度の速いスイッチが用いられている。サイリスタスイッチは、停電が発生すると即時にオンの状態となり、停電の回復と同時に自動的にオフの状態になる。

③ フロート方式は、一般に、サイリスタ整流器を用い、整流器とインバータを接続する母線に蓄電池が直接接続される。サイリスタ整流器は、常時、均等充電電圧で運転され、必要に応じて浮動充電電圧で運転される。

④ フロート方式は、停電時に直流電圧の急変が少なく、かつ、停電が回復したときにも直流電圧の過渡変動が少なく安定しているという特徴を有している。

問３ 次の問いに答えよ。 (小計２０点)

(１) 次の文章は、ＡＴＭネットワークにおけるトラヒック制御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ネットワークにおけるトラヒック制御には、コネクション受付制御、 (ア) 、優先制御などがある。

(ア) は、ネットワークの入り口でユーザからのトラヒックが、申告値を満足しているか否かを監視する機能である。 (ア) には、 (イ) から、一定量のトラヒックを送出する (ウ) 方式や、一定周期ごとに到着したセル数をカウントするクレジットウィンドウ方式などがある。

一方、設備の故障などにより、ＡＴＭネットワークのふくそうが発生した場合の対処方法としては、ネットワークが、ＡＴＭセルのヘッダのふくそう表示ビットを用いて (エ) にふくそうの有無を通知するＦＥＣＮ(Forward Explicit Congestion Notification)や、コネクション受付制御機能により、新しいコネクションの受付の中止など、各種のトラヒック制御機能を組み合わせてふくそうの制御が行われる。

<(ア)～(エ)の解答群>

① リーキーバケット	② フロー制御	③ 発側ユーザ
④ リソース監視制御	⑤ ＣＬＰ	⑥ 着側ユーザ
⑦ フィードバック制御	⑧ ＯＡＭ	⑨ 網管理局
⑩ 使用量パラメータ制御	⑪ 網内装置	⑫ 送信バッファ
⑬ スライディングウィンドウ	⑭ シェーピングコントロール	
⑮ 網パラメータ制御	⑯ ピークセルレート	

(2) 次の文章は、ディジタル加入者線交換機のＢＯＲＳＣＨＴ機能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) ＢＯＲＳＣＨＴ機能のうち、Ｓ機能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 一般に、発呼検出、ダイヤルパルス受信、終話検出のＳ機能は、直流監視回路により、A線、B線に流れる加入者回線のループ電流を監視することによって行われる。
② Ｓ機能には、着信端末の呼出信号送出中に、加入者回線のループを検出し、呼出信号送出を停止するリングトリップ機能がある。
③ Ｓ機能の一つであるハイアンドドライ機能とは、加入者回線の故障などにより、加入者回線が長時間にわたり、開放状態であるか否かを監視する機能である。
④ Ｓ機能には、加入者回線からの雷サージや混触による過電流の流入防止機能がある。

(ii) ＢＯＲＳＣＨＴ機能のうち、Ｈ機能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 Ｈ機能は、従来のアナログ交換機の場合は、ディジタル伝送路とのインタフェース点での機能であったが、通話路のディジタル化に伴い、集線段通話路へ実装されている。
② Ｈ機能は、ディジタル交換機の時分割形通話路に用いられる論理回路が、通常、一方向性であるため、上り下りの信号を分離し、上り下り各2線ずつ、計4線式の通話路とするための機能である。
③ Ｈ機能には、加入者回線のＡ線地気、Ｂ線電池の状態に、１６〔Hz〕の交流信号を重畳させ、電話機のベルを鳴らすための信号送出機能がある。
④ Ｈ機能には、給電制御回路により、通話に必要な電流を加入者線に供給する機能もある。

(３) 次の文章は、品質管理に用いられるＱＣ七つ道具(新ＱＣ七つ道具を含む。)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) 特性要因図について述べた次のＡ～Ｃの文章は、 [(キ)] 。

Ａ　計画を推進していく上で必要な作業要素を抽出する。これらをつなぎ合わせて作成し、計画の進捗管理などに用いられる。
Ｂ　中心線と上方及び下方の管理限界線で構成され、一般に、魚の骨といわれている。
Ｃ　原因と結果との関係を表し、現象、原因、対策などの内容を整理するために用いられる。

<(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) ＱＣ七つ道具(新ＱＣ七つ道具を含む。)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　連関図法は、問題(目的、目標などの事象)を着目点(手段)で幾度も枝分かれさせながらその全容を明らかにし、問題解決の手段・方策に到達していくために用いられる。
②　パレート図は、項目を横軸に、度数を縦軸に取るとともに度数の多い項目から順に並べ、かつ、累積相対頻度曲線を併記したもので、不良、欠点などを原因別、状態別、位置別などで層別した結果を示すために用いられる。
③　チェックシートは、データの分類項目別分布を調べるなど要因の系統的整理を行う場合に用いられ、効率よくデータを採るために有効なものである。
④　ヒストグラムは、データの存在する範囲を幾つかの区間に分け、各区間を底辺とし、その区間に属するデータの出現度数に比例する面積を持つ柱(長方形)を並べたもので、母集団の分布の形などを把握するためなどに用いられる。
⑤　散布図は、２変数を横軸と縦軸にとり、値を打点したもので、相関性など二つの変数の関係を把握するために用いられる。

問４　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、ネットワーク管理の基本機能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)

大規模化・複雑化したネットワークでは、ネットワークの故障は、ユーザに与える影響が大きく、また、効率よく安定して運用することが難しくなり、性能の最適化も重要な問題となっている。そのため、ユーザが簡単に、安心してネットワークを利用できるとともに、運用管理者が高い信頼性を保ちながら、容易にネットワークを運用管理することが必要となっている。

ＴＴＣ標準ＪＴ－Ｍ３０１０「通信管理ネットワークの原則」において、ネットワークの管理項目として、［　(ア)　］管理、［　(イ)　］管理、課金管理、障害管理、機密管理の五項目が規定されている。

［　(ア)　］管理では、ネットワーク内の資源の数や各々の属性、それらの関係などを一元的に把握、管理し、資源を初期状態・稼働状態・保守状態のいずれかの状態に設定したり、どの状態にあるかを把握することなどを行う。

［　(イ)　］管理では、ネットワークの性能に関する統計情報の収集、記録、解析を行って性能低下の原因や稼働率の低い資源を指摘し、ネットワークの再調整に有効な情報をネットワーク管理者に提供する。また、ユーザに対しては、スループット、トラヒック、誤り率などの性能を測定・解析して［　(ウ)　］を確保することが可能となる。

機密管理では、資源に対する不正なアクセスから保護する手段を提供し、パスワードなどの認証、暗号化鍵の管理、ユーザごとの［　(エ)　］の登録や変更などを行う。

<(ア)～(エ)の解答群>

①　ＯＣ曲線	②　システム有効度	③　アクセス権限
④　構　成	⑤　ゲートウエイ	⑥　使用機器
⑦　履　歴	⑧　バージョン	⑨　ログファイル
⑩　レイヤ	⑪　サービスレベル	⑫　アクセスタイム
⑬　工　程	⑭　パフォーマンス	⑮　技術レベル

(2) 次の文章は、あるサービスエリアにおける専用回線の保全度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。ただし、表は1か月(30日)間に発生した20件の故障とその修理に要した時間を示したものであり、専用回線の故障は偶発故障期間にあるものとする。また、答えは、四捨五入により小数第2位までとする。　(3点×2＝6点)

(単位：分)

故障番号	1	2	3	4	5	6	7	8	9	10
修理時間	26	40	66	46	55	75	58	44	38	51

11	12	13	14	15	16	17	18	19	20	計
45	58	52	38	21	41	50	30	56	70	960

(i) このサービスエリアにおける専用回線の故障の発生から1時間における保全度は、［(オ)］である。

(ii) このサービスエリアにおける専用回線の平均修復率は、［(カ)］〔件／時間〕である。

<(オ)、(カ)の解答群>

① 0.15　② 0.67　③ 0.80　④ 0.85
⑤ 0.94　⑥ 1.25　⑦ 1.50　⑧ 3.00

(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、この装置は偶発故障期間にあるものとする。

また、指数関数の値は、$e^{-0.001}=0.999$、$e^{-0.01}=0.990$、$e^{-0.1}=0.905$、$e^{-1.0}=0.368$、$e^{-4.60}=0.010$とする。なお、eは自然対数の底である。

(3点×2＝6点)

(i) 装置の平均故障率が0.1〔%／時間〕のとき、その装置が100時間以内に故障する確率は、［(キ)］〔%〕である。ただし、答えは、四捨五入により小数第1位までとする。

<(キ)解答群>

① 9.5　② 10.0　③ 36.8　④ 90.5　⑤ 99.0

(ii) 装置が1,000時間稼動した時点での信頼度は、［(ク)］である。ただし、答えは、四捨五入により小数第3位までとする。

<(ク)の解答群>

① 0.368　② 0.632　③ 0.905
④ 0.990　⑤ 0.999

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、情報セキュリティの認証技術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)

認証については、現在数多くの認証技術が存在する。この中で普遍的に使用されているのが、ユーザＩＤとパスワードを用いる認証であり、一般に、［(ア)］認証ともいわれている認証技術である。この認証技術は、端末のオペレーティングシステムやネットワークへのログオン時などに、広く普及している。認証に用いられるパスワードは、一般に、認証時に同じパスワードを使用する固定パスワードと、毎回異なるパスワードを使用するワンタイムパスワードの二つに大別される。

固定パスワードによる認証は、実際には非常に多く利用されているが、［(イ)］、辞書攻撃などの脅威にさらされている。［(イ)］の脅威に対する対策としては、一般に、ＳＳＬ、ＩＰｓｅｃなどの暗号プロトコルを利用した上で、固定パスワードによる認証が行われることが多い。

一方、暗号プロトコルを利用せずに、［(イ)］の脅威に対する有効な対策の一つに、［(ウ)］方式を利用する方法がある。［(ウ)］方式を利用するワンタイムパスワードのシステムでは、ネットワーク上に毎回異なるパスワードを流すことにより、［(イ)］によるなりすましの脅威を回避している。

また、ネットワーク上に流すパスワードを毎回作成するために、［(エ)］といわれる物理的なデバイスを用いることがある。［(エ)］は、可搬性があり記憶要素としてのＰＩＮコードと組み合わせて使用されることがある。

<(ア)～(エ)の解答群>

①　バッファオーバフロー	②　ＤＤｏＳ	③　ＣＡを利用した電子
④　バイオメトリクス	⑤　ベーシック	⑥　フィルタリング
⑦　チャレンジレスポンス	⑧　モジュール	⑨　シングルサインオン
⑩　ネットワーク盗聴	⑪　メッセージ	⑫　ハードウェアトークン

(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)

公開鍵暗号方式及び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。
② 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、鍵の長さが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。
③ 共通鍵暗号方式は、主に、通信データの暗号化に用いられ、公開鍵暗号方式は、主に、認証と鍵配送に用いられる。公開鍵暗号方式の一つに、離散対数問題の困難性を利用したＲＳＡ暗号があり、広く利用されている。
④ 秘密に保持すべき鍵は、共通鍵暗号方式では通信相手ごとに必要であるのに対して、公開鍵暗号方式では、自分の秘密鍵のみである。

(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)

電子透かし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 静止画、動画、オーディオなどのディジタルコンテンツに、コンテンツとは別の情報を不可分に埋め込む処理及び読み出す処理を合わせたものは、電子透かしといわれる。
② 電子透かしに求められる性質は、電子透かし情報を埋め込んでも、ディジタルコンテンツの品質を落とさないことや、埋め込まれた情報が改ざん及び除去されないことである。
③ 画像に対する電子透かしの埋め込み方法には、画素領域への埋め込み方法と周波数領域への埋め込み方法などがある。一般に、周波数領域への埋め込み方法は、画素領域への埋め込み方法と比較して、埋め込みのための処理に時間がかかる短所がある。
④ 二次配布禁止のディジタルコンテンツ配信時に、電子透かし情報として「コンテンツ受信者のＩＤ」を埋め込むことにより、二次配布した不正受信者の特定は不可能であるものの不正コピーの抑止には利用できる。

(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)

ＶＰＮ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>

① ＶＰＮは、企業などの各拠点を相互接続するＬＡＮ間接続や、移動中や遠隔地のパーソナルコンピュータなどの端末からインターネット経由で企業のサーバなどにリモートアクセスする場合に用いられる。

② ＶＰＮに用いるＩＰｓｅｃには、送信するＩＰパケットのペイロード部分だけを認証・暗号化して通信するトンネルモードと、ＩＰパケットのヘッダ部まで含めてすべてを認証・暗号化するトランスポートモードがある。

③ ＶＰＮに用いるＬ２ＴＰは、レイヤ２で動作するトンネリングプロトコルであり、リモートアクセスＶＰＮだけでなく、ＬＡＮ間接続ＶＰＮにも適用可能である。

④ ＩＰｓｅｃは、ネットワーク層で用いられるため、ＩＰレイヤ以上で動作するプロトコルのセキュリティを保護できる。

(５) 次の文章は、広義のコンピュータウイルス(ワームなどの有害プログラムを含む。)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)

ネットワーク構築時におけるコンピュータウイルス対策について述べた次のＡ～Ｃの文章は、 [(ク)] 。

Ａ　Ｗｅｂページの閲覧は、コンピュータウイルス感染の原因となる可能性があるため、クライアントからのＷｅｂページの閲覧を制限するフィルタリング機能をメールサーバに設ける。

Ｂ　コンピュータウイルスに感染したメールの送受信が、コンピュータウイルスをまん延させる要因となるため、特定の差出人のメールを拒否したり、電子メールの本文や添付ファイルが、コンピュータウイルスに感染していないかチェックする機能などをゲートウエイに設ける方法がある。

Ｃ　ウイルス対策ソフトウェアは、その動作対象により、ネットワーク型やホスト型に分類できる。ホスト型の場合は、サーバ、クライアントなどすべての設備にこのソフトウェアを導入することにより、コンピュータウイルスの感染及び発病を完全に防止することができる。

<(ク)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