平成２０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**

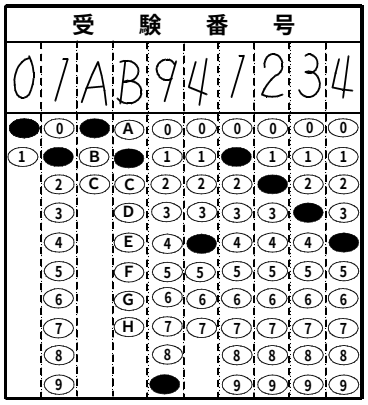
3　試験種別と試験科目別の問題(解答)数及び試験問題ページ

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	7	7	7	7	6	1～11
	伝送交換設備及び設備管理	8	8	8	8	8	12～24
線路主任技術者	法　規	7	7	7	7	6	1～11
	線路設備及び設備管理	8	8	8	8	8	25～35

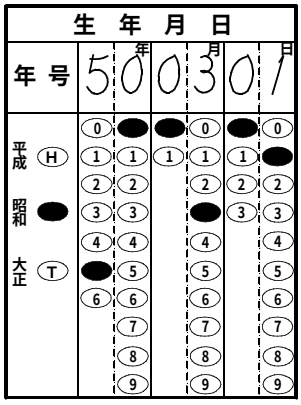
4　受験番号等の記入とマークの仕方

(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、コンピュータシステムなどの高信頼化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。

(２点×４＝８点)

コンピュータシステムにおいて、システムの構成要素にフォールトが発生した場合、要求される信頼性の水準を維持し、あるいは、回復させる必要があるときは、冗長構成を採ることが一般的である。

冗長構成は、静的冗長と動的冗長に分けることができる。静的冗長は、［(ア)］ともいわれ、固定的な冗長構成を用いることにより、フォールトによる誤りを認識させず、フォールトの影響を無くす方式である。ハードウエアによる［(イ)］方式は静的冗長の例である。

一方、動的冗長は、フォールトによる誤りを認識した後に、その回復処理を行い、誤りから回復する方式である。誤りを検出した時点の処理を何度か繰り返す方法は、［(ウ)］といわれている。

システムに与えられた役割によっては、万一、その機能が停止したときの状態を常に安全側に保障する必要がある。これは［(エ)］といわれ、信号システムなどがその例である。

<(ア)～(エ)の解答群>

①　誤り特性	②　垂直分散処理	③　縮　退
④　再構成	⑤　フェールソフト	⑥　時間冗長
⑦　多数決冗長	⑧　ロールバック	⑨　リトライ
⑩　待機冗長	⑪　フォールトマスキング	⑫　リスタート
⑬　フェールセーフ	⑭　ソフトウエア冗長	⑮　フールプルーフ

(2) 次の文章は、アクセス方式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)

(i) ＬＡＮのアクセス制御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 トークンパッシング方式では、フレームのヘッダ内のアクセス制御部に優先度を示す情報を設定することにより、特定の端末に、他の端末と比較してより高い優先権を与えることができる。

② 物理トポロジーの違いにより、信号の流れが異なることから、トークンパッシング方式には、リング型トポロジーで使用するトークンパッシングリング方式とバス型トポロジーで使用するトークンパッシングバス方式がある。

③ ＣＳＭＡ／ＣＤ方式には、フレームを送信しようとする端末が、他の端末からのフレームとの衝突を避けるため、フレームの送信に先立ってキャリアの有無を調べ、伝送媒体が空いているか否かを確認するキャリアセンス機能がある。

④ ＣＳＭＡ／ＣＤ方式には、送信中の端末が常にフレームの衝突を監視し、フレームの衝突を検出すると送信を中止し、ある時間をおいて再送信を試みる衝突検出機能がある。

⑤ ＣＳＭＡ／ＣＤ方式においては、一般に、最大、８回の再送信を試みてもフレームの衝突が発生するときは、送信エラーとして処理される。

(ii) 無線ＬＡＮのアクセス方式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 無線ＬＡＮのアクセス方式には、ランダムアクセス方式と多重アクセス方式があり、ランダムアクセス方式の一つに、ＦＤＭＡ方式がある。

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、ＴＤＭＡ方式と同様、時間軸でのバースト同期処理及び時間軸でのオーバラップを防止するためのガードタイムの設定が必要である。

③ 多重アクセス方式の一つであるＡＬＯＨＡ方式は、通信チャネルの使用状況に無関係に各端末がランダムにアクセスする方式である。

④ 符号拡散を利用したＣＤＭＡ方式は、スペクトル拡散方式ともいわれ、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。

⑤ ＳＤＭＡ方式は、無線ゾーン内において、基地局のアンテナの指向性を利用して同一の周波数、タイムスロットで通信を行うユーザを空間領域で分割して多元接続する方式である。

(3) 次の文章は、ＩＰｖ６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) ＩＰｖ６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 ＩＰアドレス空間として１２８ビットが割り当てられ、この１２８ビットを１６ビットずつに区分し、区分された一つ一つを１０進数で表記したものをカンマでつないで、アドレスとして表記される。

② ＩＰｖ６のヘッダには、送信元ＩＰアドレス及びあて先ＩＰアドレスを合わせて１２８バイトのフィールドが割り当てられている。

③ ＩＰｖ６のヘッダは、４０バイトの固定長の基本ヘッダと必要により付加される拡張ヘッダにより構成される。

④ 基本ヘッダには、トラヒッククラス、フローラベル、ペイロード長、ホップ制限、認証ヘッダ、暗号ペイロードヘッダなどのフィールドがある。

(ii) ＩＰｖ６の特徴、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、 [(ク)] である。

<(ク)の解答群>

① セキュリティ機能として、通信内容の暗号化、通信相手の認証などがあり、暗号化には、共通鍵暗号アルゴリズムなどが利用される。

② ＩＰヘッダの誤りチェックを行うためのヘッダチェックサムフィールドとして、１６ビット長が規定されている。

③ 基本ヘッダと拡張ヘッダの機能分離により、ヘッダの簡素化と拡張性が確保されている。

④ フローラベルフィールドの追加により、ルータにおけるフロー検出処理が、ＩＰｖ４と比較して簡便になっている。

問２　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、波長多重伝送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。　　(２点×４＝８点)

ＩＰブロードバンドサービスの基幹系ネットワークでは、ストリーミングなど、動画情報の伝送によるトラヒックの増加が顕在化し、伝送路の大容量化及び超高速化が重要になってきている。伝送路の大容量化の方法の一つに、一心の光ファイバに複数の異なる波長の光信号を多重化して伝送するＷＤＭ伝送方式がある。

ＷＤＭ伝送方式では、たとえば、光の伝搬速度を3×10^{8}〔m／s〕、使用する波長帯域を１.５〔μm〕から１.６〔μm〕までの０.１〔μm〕としたとき、その伝送帯域幅は、周波数に換算すると［　(ア)　］〔THz〕となり、波長を１００〔GHz〕間隔に配置すると、［　(イ)　］波長の多重化が可能となる。

また、ＷＤＭ伝送方式では、光ファイバの送受端に、光デバイスとしてアイソレーションが高く、［　(ウ)　］が少ない特性を有する［　(エ)　］が用いられる。

<(ア)～(エ)の解答群>

①　０.１２５	②　１.２５	③　１２.５	④　１２５
⑤　１,２５０	⑥　２,０００	⑦　光共振器	⑧　位相変動
⑨　ＭＣ	⑩　光カー効果	⑪　挿入損失	⑫　変・復調器
⑬　自然放出光雑音		⑭　光合・分波器	

(２)　次の文章は、通信用予備電源装置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)　交流同期発電装置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　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、火花が発生しやすいが、スリップリング(滑動環)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。

②　回転界磁形同期発電機では、電機子巻線が固定されており、これは固定巻線といわれる。また、回転する界磁巻線は界磁子といわれる。

③　交流発電機の回転速度は発電機の極数、電源の周波数により決定され、これらと回転速度(同期速度)との関係は、一般に、次式で表される。

$$Ns〔rpm〕=\frac{120P}{f}$$　　Ns：同期速度、ｆ：周波数〔Hz〕、Ｐ：極数

④　回転界磁形同期発電機は、電機子巻線が固定され、界磁部分が回転する構造であり、スリップリング(滑動環)が必要である。

⑤　交流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、整流器を搭載し、固定界磁を用いた交流励磁機と組み合わせて、無接触での励磁電流供給を行う方式である。

(ⅱ) 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、［（カ）］である。

<(カ)の解答群>

① ディーゼル機関は、ガソリン機関のような電気点火装置や気化器が不要なため、比較的故障率が低い利点を持っている。また、ガスタービンと比較して燃料消費量は少ない。

② ガソリン機関は、一般に、吸入行程で燃焼室内にガソリンと空気の混合気を吸入し、圧縮行程の後、点火プラグで点火、燃焼、膨張させてピストンを往復させる内燃機関である。

③ ガスタービンは、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、車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、硫化物質の濃度が低い。

④ ガスタービンは、ディーゼル機関と比較して、運転に必要な空気量が多く、一般に、４～６倍を必要とするため、吸排気対策を十分考慮する必要がある。また、エンジンの回転が高速であることから、機関冷却のための冷却水が多量に必要である。

(３) 次の文章は、デジタル電話交換機の加入者回路に具備されているＢＯＲＳＣＨＴ機能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) ＢＯＲＳＣＨＴ機能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 ＢＯＲＳＣＨＴ機能のＢは、通話に必要な電流を加入者線に供給する機能である。

② ＢＯＲＳＣＨＴ機能のＯは、加入者ケーブルの心線を伝搬して交換機に侵入する外来電圧から交換機を保護するための機能であり、交換機の部品の耐圧を超える雷サージを減圧したり、耐電流値を超える一定時間以上の一定電流を遮断する機能である。

③ ＢＯＲＳＣＨＴ機能のＳは、アナログ－デジタル変換を行う符号化・復号機能であり、その機能は４線側の通話路にある。

④ ＢＯＲＳＣＨＴ機能のＨは、通話路が４線構成であることから、加入者線の２線と通話路の４線を相互に変換する機能である。

(ⅱ) 加入者回路の制御方法などについて述べた次のA～Cの文章は、 (ク) 。

A　加入者回路には、加入者線の監視結果の収集、加入者回路内のポイント制御のための制御回路が設けられている。この制御回路とプロセッサ間でやりとりされる監視信号及び制御信号は、ループの断続で行われる。

B　呼出信号送出機能には、発呼検出、ダイヤルパルス受信、通話中監視、終話検出などがある。

C　加入者回路の試験では、加入者線試験台から加入者回路に割り込むことにより、加入者線側の試験及び通話路系側の試験が可能である。

<(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

問3　次の問いに答えよ。　(小計２０点)

(1) 次の文章は、地上マイクロ波通信におけるフェージング及びフェージング対策など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)

地上マイクロ波通信において電波の伝搬する空間では、空気の密度分布の変化、反射体の形状変化、降雨・降雪などの影響を受け、電波伝搬状態が変化するフェージング現象が発生する。

フェージングには、電波伝搬上において、電波の反射あるいは屈折などが発生し、受信側では、経路長の異なる２波以上の電波を受信することにより発生する (ア) フェージング、電波伝搬上における雨や雪による電波の減衰などにより発生する (イ) フェージングなどがある。

フェージング対策には、ダイバーシチによる方法と自動等化器を使用する方法がある。

ダイバーシチによる方法には、マイクロ波の伝搬は、空間により伝搬変動が異なることを利用して受信アンテナを二つ以上互いに異なった場所に設け、受信信号を選択あるいは合成する (ウ) ダイバーシチ、二つ以上の異なる周波数の電波を同時に伝搬させる周波数ダイバーシチなどがある。

また、自動等化器を使用する方法には、一般に、トランスバーサル・フィルタを用いた (エ) 領域自動等化器を利用したものがある。

<(ア)～(エ)の解答群>

① ＩＦ帯　② Ｋ　形　③ スペース　④ シンチレーション形
⑤ 回折性　⑥ 吸収性　⑦ ルート　⑧ ベースバンド帯
⑨ 距　離　⑩ 角　度　⑪ 遅　延　⑫ マルチパス
⑬ 時　間　⑭ 位　相　⑮ 偏　波　⑯ ダクト性

(2) 次の文章は、生産管理用語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。なお、文章の内容は、ＪＩＳ　Ｚ　８１４１を基にしている。　(3点×2＝6点)

(i) 設備管理及び工事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 価値管理とは、設備の計画、設計、製作、調達から運用、保全をへて廃却・再利用に至るまで、設備を効率的に活用するための管理のことである。

② 劣化とは、設備が次のいずれかの状態になる変化のことである。

ⓐ 規定の機能を失う。

ⓑ 規定の性能を満たせなくなる。

ⓒ 設備による産出物や作用が規定の品質レベルに達しなくなる。

③ ライフサイクルとは、設備を導入し、使用を開始してから、廃棄又は更新するまでの期間のことである。

④ 陳腐化とは、技術の進歩によって、所有している設備の技術レベル又は経済的価値が相対的に低下していく変化のことである。

⑤ オーバーホールとは、設備の点検及び性能回復を目的として、設備又は生産ラインを長期間にわたって休止して行う大規模な工事のことである。

(ii) 保全及び保全活動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 予防保全とは、故障に至る前に寿命を推定して、故障を未然に防止する方式の保全のことである。

② 改良保全とは、故障が起こりにくい設備への改善又は性能向上を目的とした保全活動のことである。

③ 定期点検とは、主として設備劣化防止のために、始業時又は終業時若しくはロット切換時などに実施される設備の日常的な点検作業の総称のことである。

④ 点検とは、設備の劣化防止とその状況を調べる機能を担う方策の総称である。

⑤ 設備診断とは、設備の性能、劣化状態などを、設備の運転中に定量的に把握し、その結果を基にして、設備の信頼性、安全性、寿命の予測を行う活動のことである。

(3) 次の文章は、ＩＰ電話網における通話品質の評価方法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) 主観的評価方法及び客観的評価方法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 主観的評価方法の一つであるオピニオン評価法は、被験者が、耳で聞いた試験音声の品質に対し、非常に良い、良い、まあ良い、悪い及び非常に悪いの５段階に評価する方法である。
② オピニオン評価法では、評価点は被験者によってばらつくので、多数のデータを集めて統計的な処理を行う。集めたデータを統計的に処理した値を平均オピニオン評点(ＭＯＳ値)という。
③ 客観的評価方法では、１種類のテスト用音声を基準音声として準備する。その基準音声が評価対象システムを通過した後の劣化した音声信号と基準音声との間で、比較演算処理を行い、その結果をＭＯＳ値と対応したスコアとして出力する。
④ 客観的評価方法には、ＰＳＱＭ、ＰＥＳＱなどがある。このうち、ＰＳＱＭは、コーデックの音声品質評価のために開発された評価方法である。
⑤ ＰＥＳＱは、ＰＳＱＭの弱点を補強した評価方法であり、ＩＰ電話特有のパケットゆらぎやパケット損失の影響を評価結果に反映できるようになっている。

(ⅱ) 総合音声伝送品質を表すＲ値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 Ｒ値による評価では、ＰＳＱＭやＰＥＳＱと同様に、伝送遅延による音声品質の劣化について考慮されていない。
② Ｒ値は、Ｅモデルという音声品質評価のための計算モデルに、音声品質に関係する回線の雑音や音量、エコーをはじめとする五つのパラメータを代入して求める。
③ Ｒ値は、エンド・ツー・エンドの音声品質を１～１００までの数値で示したもので、数値の小さい方が高品質であることを意味している。
④ Ｒ値は、主観的評価であるＭＯＳ値と相関があることから、ＭＯＳ値に換算することができる。
⑤ Ｒ値による品質評価は、日本国内におけるＩＰ電話の品質クラス分類に採用されており、「０５０」で始まるＩＰ電話専用の電話番号を使用するには、Ｒ値が８０より小さな値でなければならない。

問４　次の問いに答えよ。　(小計２０点)

(１)　次の文章は、ライフサイクルにおける信頼度と故障率の概要など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)

システムのライフサイクルにおける故障率のパターンは、故障率減少型(ＤＦＲ)、故障率一定型(ＣＦＲ)及び故障率増加型(ＩＦＲ)に分類される。

ＤＦＲの期間は、システムの中に潜在していた設計ミス、製造工程での欠陥などの弱点がシステムの初期運用時に発生する故障率のパターンを示す時期であり、運用時間の経過とともに、故障率は減少傾向を示す。また、この故障率のパターンは、初期運用時のほかに、保全作業やシステムの［(ア)］の直後にも一時的に現れるパターンである。

ＣＦＲの期間は、デバギングにより取り除き得なかった構成部品の故障率が重なり合って、故障率は、ほぼ一定の値をとる。このパターンにおいては、可能な限り故障率が低いこと、かつ、持続時間が長いことが望ましい。この持続時間は、一般に、［(イ)］といわれる。

ＩＦＲの期間は、故障率が上昇傾向を示す時期であり、信頼度の分布は、一般に、［(ウ)］分布を示す。また、システムの保全が可能であれば、故障が予測される部品を取り替えるなどの予防保全、故障した部品を取り替える［(エ)］などの措置を行い、故障率を一定値以下に保つことによって［(イ)］の延伸を図ることも可能となる。

<(ア)～(エ)の解答群>

①　点　検	②　正　規	③　対数正規	④　事後保全
⑤　検　査	⑥　指　数	⑦　ポアソン	⑧　平均故障寿命
⑨　改　造	⑩　保全時間	⑪　定期保全	⑫　状態監視保全
⑬　診　断	⑭　耐用寿命	⑮　修復時間	⑯　時間計画保全

(2) 次の文章は、ある部品の信頼性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、すべての部品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を自然対数の底とすると、$e^{-0.10}=0.90$、$e^{-0.08}=0.92$、$e^{-0.04}=0.96$とし、答えは、小数点以下を切り捨てるものとする。
(3点×2＝6点)

(i) 部品Aの総動作時間を4,000〔時間〕、動作不能時間を200〔時間〕、保全時間を100〔時間〕、故障件数を5回とするとき部品AのMTBFは、［(オ)］〔時間〕である。

(ii) 部品B及びCのMTBFをそれぞれ2,000〔時間〕及び2,500〔時間〕としたとき、部品B及びCをそれぞれ一つ用いた並列冗長システムの200〔時間〕における信頼度は、［(カ)］〔%〕である。

<(オ)、(カ)の解答群>
① 92　② 95　③ 98　④ 99
⑤ 760　⑥ 800　⑦ 840　⑧ 860

(3) 次の文章は、あるシステム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、それぞれの装置は、偶発故障期間にあるものとする。(3点×2＝6点)

(i) 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98.0〔%〕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>
① 1.00　② 1.96　③ 4.08　④ 10.00　⑤ 10.20

(ii) 信頼度70〔%〕である装置Bが複数台並列に接続されているとき、システム全体の信頼度を99〔%〕以上とするためには、装置Bを最低［(ク)］台構成とする必要がある。ただし、必要に応じ$\log_{10}0.3=-0.523$、$\log_{10}0.7=-0.155$の値を用いること。

<(ク)の解答群>
① 4　② 5　③ 6　④ 7　⑤ 8

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、デジタル署名など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)

デジタル署名は、電子化された文書などの電子情報の内容と署名の正当性を公開の検証手段によって保証するものであり、［(ア)］方式とハッシュ関数を組み合わせて作られている。

一般的に用いられているＲＳＡによるデジタル署名は、次の手順により行われる。なお、受信者はあらかじめ［(イ)］を入手しているものとする。

ⓐ　送信者は送信するデータを作成する。

ⓑ　作成したデータを基に、ハッシュ関数を使ってハッシュ値を生成する。

ⓒ　［(ウ)］を使ってハッシュ値を暗号化する。暗号化されたハッシュ値がデジタル署名となる。

ⓓ　ⓐで作成したデータにデジタル署名を添付して送信する。

ⓔ　受信者は、受信したデータを基に、送信者が使ったものと同じハッシュ関数を使ってハッシュ値を算出する。

ⓕ　送信者が送ってきたデジタル署名を、［(イ)］で復号する。

ⓖ　ⓔで算出したハッシュ値とⓕで復号したハッシュ値を比較する。

ハッシュ値が一致すれば、伝送路上でデータが改ざんされていないこと及び送信者が署名者本人であることを確認できる。

デジタル署名は、電子商取引、電子政府、電子メールなどで利用されているが、電子商取引、電子政府の利用においては、電子文書の完全性の確保が重要な課題となっており、完全性を確保する技術として、デジタル署名と［(エ)］を併用する方法がある。デジタル署名により「だれが、何を」を行ったのかを証明し、［(エ)］により「いつ」行ったのかを証明することができることから、電子文書の完全性の確保が可能になる。

<(ア)～(エ)の解答群>

①　暗号化した共通鍵	②　受信者の秘密鍵	③　タイムスロット
④　暗号化した公開鍵	⑤　受信者の公開鍵	⑥　タイムスタンプ
⑦　暗号化した秘密鍵	⑧　送信者の秘密鍵	⑨　サイクルタイム
⑩　公開鍵暗号	⑪　送信者の公開鍵	⑫　オーバヘッドタイム
⑬　共通鍵暗号	⑭　送信者の共通鍵	⑮　ハイブリッド暗号

(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)

セキュリティプロトコル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 S／MIMEは、電子メールのセキュリティ機能を強化するプロトコルである。S／MIMEを用いた電子メールでは、送信者は、電子メールのメッセージを公開鍵で暗号化し、その鍵を送信相手の共通鍵を用いて暗号化している。

② SSHは、TCP／IPネットワーク上で強力な暗号化機能と認証機能によりセキュアなリモートログインを提供できるが、ファイル転送機能は有していない。

③ SSLは、OSI参照モデルのトランスポート層のプロトコルである。HTTPやSMTPなどは、SSLを用いた通信路上を透過的に利用することができる。

④ IPsecには、トンネルモード及びトランスポートモードの二つのモードがある。このうち、トランスポートモードは、送信するIPパケットのヘッダ部を含め暗号化して通信できる。

(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)

Webアプリケーションにおける脅威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 データベース(DB)と連携するWebアプリケーションの場合には、一般に、WebサーバをDMZ、DBサーバを内部ネットワークに配置し、ファイアウォールによりWebサーバとDBサーバ間は必要最小限の通信だけをできるように制限して、外部ネットワークからDBサーバに直接アクセスできないようにしている。

② データベースと連携したWebアプリケーションの多くは、ユーザからの入力情報を基にデータベースへの命令文を組み立てている。入力情報のチェックが適切でないと、悪意のあるユーザからの攻撃によってデータベースが不正に利用されることがある。この攻撃は、一般に、クロスサイトスクリプティングといわれる。

③ OSコマンドインジェクションは、攻撃者がURLのパラメータなどにOSのコマンドを挿入して実行させる攻撃であり、意図しないOSコマンドを実行させられて重要情報が盗まれたり、攻撃の踏み台に悪用される可能性がある。

④ セッションハイジャックが成立すると、攻撃者がユーザになりすまし、そのユーザ本人に許可されているすべての操作が不正に行われる可能性がある。

(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)

ファイアウォールの主な方式などについて述べた次のＡ～Ｃの文章は、［（キ）］。

Ａ　パケットフィルタリング方式は、一般に、ＩＰパケットのヘッダに記録されている送信元のＩＰアドレスやポート番号などの情報及びデータフィールドのデータの内容を基に、通信の許可又は不許可を判断している。

Ｂ　アプリケーションゲートウェイ方式は、ＩＤとパスワードを基にしてアクセスの許可又は不許可を設定することが可能である。認証の機能を有するＦＴＰ、ＳＳＨなどは、認証によって許可されたＩＰパケットだけを通過させることにより、アプリケーションレベルのセキュリティを確保できる。

Ｃ　ステートフルインスペクションといわれる機能を有するファイアウォールは、通過するＩＰパケットの状態を監視し、行きのＩＰパケットを許可した時点で、行きのＩＰパケットに対する戻りＩＰパケットのルールを動的に設定することにより、ＩＰパケットの通過を制限することができる。

<(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

(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)

ＪＩＳ Ｑ ２７００２「情報セキュリティマネジメントの実践のための規範」の事業継続管理における管理策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　組織全体を通じた事業継続のために、組織の事業継続に必要な情報セキュリティ要求事項を取り扱う、管理された手続きを策定し、維持することが望ましい。
②　業務プロセスの中断を引き起こし得る事象は、そのような中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに、特定することが望ましい。
③　重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の有用性及び完全性を確実にするために、計画を策定し、実施することが望ましい。
④　事業継続計画が最新で効果的なものであることを確実にするために、定めに従って試験・更新することが望ましい。