平成１６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**

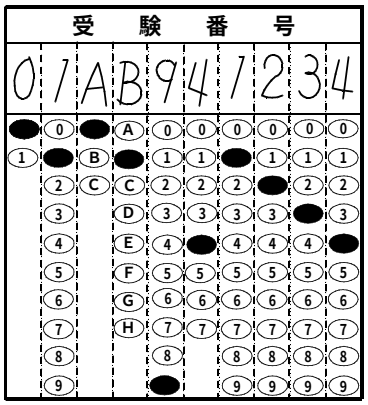
3　試験種別と試験科目別の問題(解答)数及び試験問題ページ

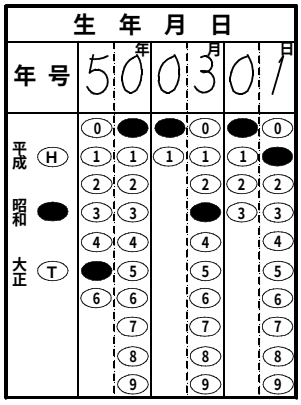
試　験　種　別	試　験　科　目	問　題　(　解　答　)　数					試験問題
		第１問	第２問	第３問	第４問	第５問	ペ　ー　ジ
伝送交換主任技術者	法　規	7	7	7	7	7	1～13
	伝送交換設備及び設備管理	8	8	8	8	8	14～27
線路主任技術者	法　規	7	7	7	7	7	1～13
	線路設備及び設備管理	8	8	8	8	8	28～41

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。

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、信頼性設計技術における冗長構成設計法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)

(ⅰ)　信頼性工学では、故障は永久的機能の停止を意味し、故障したアイテムは自然に復旧することはなく、保全活動によってのみ元の機能に復旧するものと考えられている。アイテムの信頼性を向上させる手法に冗長構成設計法がある。冗長構成設計法は、システム構成に工夫を加えて、システムに冗長性を付与することにより信頼性を向上させるための設計手法である。

ハードウェアによる冗長構成方法は、常用冗長と［　(ア)　］とに大別することができる。

常用冗長は、要求機能を遂行するため、すべての構成要素が規定の機能を同時に果たすよう構成された冗長であり、並列冗長、［　(イ)　］などがある。

［　(ア)　］は、要求機能を遂行するために構成要素の一部が動作し、その間、構成要素の残りの部分は必要となるまで動作しないように構成された冗長である。必要となるまで動作しないような構成要素には、その待機状態が、作動状態になくて、システムにも機能的に接続されていない待機形式である［　(ウ)　］などがある。

(ⅱ)　信頼性設計には、信頼度の予測、保全性への配慮、標準化への配慮、システムの安全性への配慮などが考慮されるが、これらの評価には信頼性試験や［　(エ)　］といわれる設計管理手法が用いられる。

<(ア)～(エ)の解答群>

①　ＣＭ(Condition Monitoring)	②　情報冗長	③　冷予備
④　ＤＲ(Design Review)	⑤　時間冗長	⑥　温予備
⑦　ＰＭ(Preventive Maintenance)	⑧　多数決冗長	⑨　熱予備
⑩　ＳＱＣ(Statistical Quality Control)	⑪　ソフトウェア冗長	⑫　待機冗長

(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は、 [(オ)] が正しい。

<(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等の直後にも、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、運用段階の保全性作業管理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） 保守支援管理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 保守作業方法の管理としては、保守作業マニュアルの整備や、保全作業方式及び保全周期の設定などがある。保全コストの適正化を図るため、当該設備の運用期間中においては、各機器ごとに、設計時点であらかじめ定めた作業方式及び保全周期を順守する必要がある。

② 作業管理としては、機器ごとの保全作業における、作業体制、人員、作業時間などを計画することなどが挙げられる。その際、機器のアベイラビリティや事故時の影響などの点から、重要機器を分類して作業管理することが望ましい。

③ 予備品管理においては、その数量の適正化が重要であり、また、緊急復旧作業時に使えるよう、日常の点検や試験、さらには寿命管理が必要である。

④ データ管理としては、単に保全作業結果を履歴として残すのみならず、問題点などを評価、洗い出し、次期作業に反映させることが重要である。

⑤ 保全作業は、設備の性能や信頼性を維持するために必要であるが、これら作業結果を基に設備の性能などの劣化評価や改善計画を立案することも、保守支援管理として重要である。

（ⅱ） 運用段階における予防保全技術について述べた次のＡ～Ｃの文章は、［（ク）］。

Ａ 故障発生を少なくし、さらに定期検査期間の短縮や設備更新などによる寿命延長を図るには、運用段階における予防保全技術の適用が重要である。

Ｂ 予防保全技術の一つである経年劣化診断技術は、停止中診断技術と運転中診断技術に分けることができる。停止中診断は状態監視保全であり、運転中診断は時間計画保全のことである。

Ｃ 故障発生を防ぐための保全作業をより経済的に行うためには、保全性作業管理プログラムの見直しを行うことが重要であり、その手法の一つにＲＣＭ(Reliability Centered Maintenance)といわれる方法がある。

<(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２　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、ＩＰパケットなどの伝送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)

(ⅰ)　ＳＤＨはＩＴＵ－Ｔ標準として、ＳＯＮＥＴは米国標準として、それぞれ規定された伝送技術である。ＳＯＮＥＴの基本速度は５１.８４〔Mbit/s〕としているのに対し、ＳＤＨは、［(ア)］〔Mbit/s〕を基本速度としている相違はあるものの、両方式に大きな差異はなく、実際のルータやスイッチのインタフェースカードでは、両方式ともサポートしている例が多い。

(ⅱ)　ＳＤＨ／ＳＯＮＥＴのインタフェースでＩＰパケットを伝送するための方式はＰＯＳといわれる。ＰＯＳは、ＩＰパケットをＡＴＭセルを使って伝送する方式と比較して、［(イ)］という特徴がある。

(ⅲ)　ＳＤＨ／ＳＯＮＥＴなどの伝送信号を複数束ねて、１心の光ファイバを用いて伝送する技術としてＷＤＭがある。ＷＤＭでは、多重化する各伝送信号ごとに異なる波長の光信号を用い、それらを多重化することで大容量化を実現している。より大容量の伝送を可能とするため、波長相互の周波数間隔を狭くし、１心の光ファイバに数十波以上の信号を多重化する方式は、［(ウ)］といわれる。

(ⅳ)　ＷＤＭの各波長に対して、ＰＯＳと比較してより効率的にＩＰパケットの伝送を行うこと、より多くの種類の信号を柔軟に収容可能とすることなどを目的として、ＩＴＵ－Ｔでは、［(エ)］といわれる次世代の光伝送網に関する勧告化が進められている。

<(ア)～(エ)の解答群>

①　２.０４８	②　８.１９２	③　５４.０	④　１５５.５２
⑤　ＯＣ－１	⑥　ＣＷＤＭ	⑦　ＦＤＭ	⑧　ＯＸＣ
⑨　ＴＤＭ	⑩　ＯＴＮ	⑪　ＤＷＤＭ	⑫　ＰＯＷ

⑬　ペイロードの割合が少ない　　⑭　オーバーヘッドの割合が少ない

⑮　伝送路上での符号誤りによる影響が少ない

⑯　より長距離伝送が可能である

(2) 次の文章は、インターネットのプロトコルとして用いられているＩＰｖ４の問題点と活用方法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) インターネットの急速な発展によりＩＰｖ４の問題点が指摘されている。その問題点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 ＩＰｖ４のＩＰアドレスは６４ビットで構成されているため、インターネット規模の拡大、利用範囲の拡大などによりＩＰアドレス空間が限界に達しようとしている。

② ＩＰｖ４では、ネットワークのトポロジー、地理的な情報などが考慮されないまま、申請順にアドレスの割当てが行われたため、ネットワーク全体に無秩序にアドレスが分散する結果となった。このため、バックボーンのルータは、莫大な数の経路エントリーを保持する必要があり、ルータへの負荷が大きくなっている。

③ ＩＰｖ４においては、ユーザの認証、データの機密性・完全性などのセキュリティに対する機能が標準ではサポートされていない。

④ データリンク層においては、一般に、エラーチェックが行われているため、ＩＰｖ４におけるヘッダ・チェックサムフィールドの機能の重要性は、パケット長フィールドの機能と比較して低い。

(ⅱ) ＩＰｖ４におけるＩＰアドレスの活用方法について述べた次のＡ～Ｃの文章は、［（カ）］。

Ａ ＩＰアドレスにおいて、ホスト部のアドレスビットの一部を仮想的にネットワーク部として使用することにより、複数のアドレスブロックとしてネットワークを構成する方法は、サブドメインといわれる。

Ｂ プライベートネットワークにあるホストが、プライベートＩＰアドレスをグローバルＩＰアドレスに変換し、一つのグローバルＩＰアドレスで多数の外部のホストと同時に通信が可能となるネットワークアドレス変換機能は、ＮＡＰＴといわれる。

Ｃ アドレスを割り当てる場合、連続する複数のクラスＣアドレスを一つの組織等に割り当て、これらを集約し、一つのネットワークと表現する技術は、ＣＩＤＲといわれる。

<(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、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の機能、特徴について述べた次の文章は、 [　(キ)　] が正しい。

<(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結んでアドレスとして表記される。

② 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。

③ ＩＰｖ６のヘッダには、送信元ＩＰアドレス及びあて先ＩＰアドレスのフィールドがあり、それぞれ８バイトが割り当てられている。

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) ＩＰｖ４からＩＰｖ６への移行技術について述べた次の文章のうち、<u>誤っているもの</u>は、[　(ク)　] である。

<(ク)の解答群>

① ＩＰｖ４からＩＰｖ６への移行技術の一つに、ゲートウエイによりＩＰｖ４とＩＰｖ６を交換する方法がある。

② ＩＰｖ６パケットの前にＩＰｖ４ヘッダを付けてカプセル化し、トンネリングする技術によりＩＰｖ６ネットワークを通過させることができる。

③ ＩＰｖ４／ＩＰｖ６デュアルスタック網では、ホストやルータは、ＩＰｖ４とＩＰｖ６のいずれのプロトコルにも対応している必要がある。

④ 移行の最終段階においてインターネットを使用するに当たっては、既存のネットワークで利用されているＩＰアドレス、ネームサーバ(ＤＮＳ)、アプリケーションなどがＩＰｖ６対応となっている必要がある。

問３　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、無線ＬＡＮ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)

オフィスや家庭におけるパーソナルコンピュータの普及に伴い、配線の不要な無線ＬＡＮの導入が進んでいる。この無線ＬＡＮの主な標準化規格には、ＩＥＥＥ８０２.１１ａ規格、ＩＥＥＥ８０２.１１ｂ規格などがある。

ＩＥＥＥ８０２.１１ｂ規格における無線ＬＡＮの使用周波数としては、ＩＳＭバンドといわれる［(ア)］GHz帯が用いられており、アクセス制御方式としては、［(イ)］方式が採用されている。また、ＩＥＥＥ８０２.１１ｂ規格の変調方式には、［(ウ)］変調方式が用いられ、最大伝送速度［(エ)］〔Mbit/s〕を実現している。ただし、［(ア)］GHz帯は、医療用機器や電子レンジなども使用可能な周波数帯であるため、電波干渉の問題が生ずる可能性がある。

一方、ＩＥＥＥ８０２.１１ａ規格では、変調方式としてＯＦＤＭ(直交周波数分割多重)方式を採用することなどにより、最大伝送速度は、５４〔Mbit/s〕を実現している。

<(ア)～(エ)の解答群>

①　１.９	②　２.４	③　５.２	④　１１
⑤　２６	⑥　３６	⑦　４８	⑧　ＦＨＳＳ
⑨　ＣＣＫ	⑩　ＨＤＬＣ	⑪　ＣＳＭＡ／ＣＡ	⑫　ＦＤＭＡ
⑬　ＴＤＭＡ	⑭　デルタ	⑮　ＣＳＭＡ／ＣＤ	⑯　周波数

(２)　次の文章は、ディジタル加入者線交換機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)　集線段における集線方式について述べた次の文章のうち、<u>誤っているもの</u>は、［(オ)］である。

<(オ)の解答群>

①　集線方式には、空間分割集線方式、時分割集線方式、周波数分割集線方式がある。

②　集線段で用いられるメモリスイッチなどは、汎用性のあるＬＳＩ技術の適用分野であり、電磁部品に比較して小型、軽量化が図れる。

③　加入者線の使用率が一般的に低いので、集線段ではその使用率に応じた比率でトラヒックの集線を行い、分配段に対し一定の使用率で入力させる。

④　集線段では、トラヒック集線機能のほか、電話機からのアナログ信号を加入者回路でディジタル信号に変換した後、分配段で使用するハイウェイの多重度まで多重化していく機能も有している。

⑤　多重化の段階では、加入者線の使用率の向上は図れない。

(ⅱ) 分配段における通話路の構成について述べた次の文章は、［　(カ)　］が正しい。

<(カ)の解答群>

① 時間スイッチは、ゲート回路及びその制御メモリから構成され、タイムスロットの入替えを行うことができる。

② 空間スイッチは、通話メモリといわれる回路を格子上に配置することで、ディジタル信号のハイウェイ間の乗換えを実現している。

③ 時間スイッチでは、同一速度で処理できる素子を使用する場合、８ビットに符号化された音声信号を各ビットごとに並列処理するより、直列処理を行う方が等価的にスイッチの容量を大きくすることができる。

④ 時間スイッチは、これに入出力されるハイウェイの多重度がｎの場合、内部ふくそうのない、完全群の格子として機能し、２ｎ×２ｎの空間スイッチとして表すことができる。

⑤ Ｔ－Ｓ－Ｔ構成は、Ｓ－Ｔ－Ｓ構成と比較して、多重化されるチャネル数が増大するにつれ、選択できる経路数が多くなるため、その結果としてネットワークの使用効率を高めることができる。

(3) 次の文章は、通信用電源設備の受電方式について述べたものである。［　　］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)

受電装置について述べた次の文章は、［　(キ)　］が正しい。

<(キ)の解答群>

① 受電装置に具備される主な機能は、一般に、変電、整流、分配、保安である。

② 受電装置に具備される保安機能には、遮断器、ヒューズなどが用いられている。保安機能の一つである遮断器は、平常時には電流の開閉により負荷設備の運転・停止に使用されるが、異常時や事故時には過電流を迅速、確実に遮断して他への波及を防止する役割を持っている。

③ 受電装置の具体的機能には、内部故障時における外部への事故波及防止機能、特に電力の入力系統が一重系の場合での内部故障に対するバックアップ機能、設備の運転管理に必要な各種の計測機能などがある。外部からの事故波及防止は商用電源側の責任において行われている。

④ 一般に、受電装置には使用電力量の計量を行う電力計が設置されており、これを電力会社との財産責任区分の分界点としている。

⑤ わが国の商用電源の配電電圧は、交流では、６００〔V〕以下の低圧、７０００〔V〕以下の高圧、７０００〔V〕を超える特別高圧のほか、直流では、４８〔V〕が標準となっている。

（４） 次の文章は、通信用電源設備の予備電源方式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）

予備電源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 予備電源設備には、エンジン発電装置と鉛蓄電池の組合せが広く用いられている。この方式では、平常時、商用電力を受電し鉛蓄電池に対して維持充電するための電力が供給されており、停電時はエンジン発電装置から鉛蓄電池及び負荷に電力を供給する。

② ガスタービンの燃料消費量及び運転に必要となる空気量は、ディーゼル機関と比較して少ない。また、ガスタービンの出力は、吸気温度が高くなると上昇する特徴がある。

③ ディーゼル機関の水冷方式には、一般に、ラジエータ冷却方式と水槽循環冷却方式がある。水槽循環冷却方式において、水槽容量が不足する場合には、クーリングタワーによる冷却方式を併用している。

④ 長時間にわたる電力故障には、一般に、Ⓐ自然災害等による商用電源の停電とⒷ設備センタ等の電力設備の故障との二つの形態が考えられ、これらに備えた災害対策用予備電源方式が使用される場合がある。この場合、Ⓐの対策用には発電装置を車両に搭載した移動発電機を配備し、Ⓑの対策用には、これに加え電力変換装置を実装した可般形電源装置が配備される。

⑤ 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当て、車軸を回転させるため、ディーゼル機関のように往復運動を回転運動に変える機構を必要としない。また、騒音の主なものは回転音であり、その周波数も高いため、騒音対策は比較的容易である。

問４　次の問いに答えよ。　(小計２０点)

(１)　次の文章は、アベイラビ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)

修理可能なシステムでは、信頼性と同時に保全性を考慮しなければならない。アベイラビリティは、システムの信頼度と保全度を総合したシステムの広義の信頼性を表す尺度であり、その考え方によっていくつかの定義がある。アベイラビリティは、時間の関数であり、システムあるいは装置がある規定の条件下で使用されたとき、与えられた時点において満足に動作する確率は、［(ア)］アベイラビリティといわれる。また、ある時間間隔でのアベイラビリティを示す平均アベイラビリティでは、特に長時間使用でのアベイラビリティを問題にすることが多く、［(イ)］アベイラビリティや［(ウ)］アベイラビリティという尺度で表される。［(イ)］アベイラビリティは、ＭＵＴとＭＤＴから算出される尺度である。一方、［(ウ)］アベイラビリティは、ＭＴＢＦと［(エ)］によって求められる。［(ウ)］アベイラビリティは、ＭＴＢＦを大きくしても１００％に近づくが、ＭＴＢＦが小さくても［(エ)］を小さくすることで１００％に近づけることができるので、耐久性と保全性の経済的なバランスのとれたシステムが構築できる。

<(ア)～(エ)の解答群>

① 動　作	② 装　置	③ 瞬　間	④ ＭＡＤＴ
⑤ 長　期	⑥ 固　有	⑦ 正　規	⑧ ＭＴＴＭ
⑨ 偶　発	⑩ 使　命	⑪ 運　用	⑫ ＭＴＴＲ
⑬ 定　常	⑭ 通　常	⑮ 保　全	⑯ ＭＴＢＯ

(２)　次の文章は、直並列系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、答えは、四捨五入により小数第２位までとする。　　(３点×４＝１２点)

(ｉ)　図１の装置Ｘの信頼度は、 [　(オ)　] である。ただし、下図の数値は、各部品単体の信頼度である。

装置Ｘ

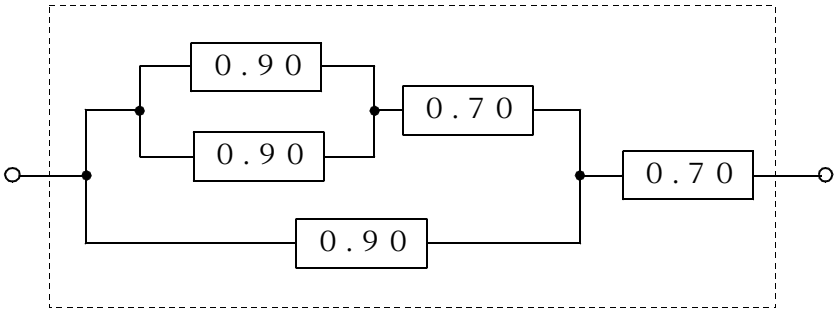


図１

(ii)　図２の装置Ｙの信頼度を、次の(ａ)、(ｂ)、(ｃ)の算出順序で求めるとすると、下記のとおりとなる。ただし、部品Ａ、Ｂ、Ｃ及びＤの信頼度は、すべて０.９０とする。

装置Ｙ

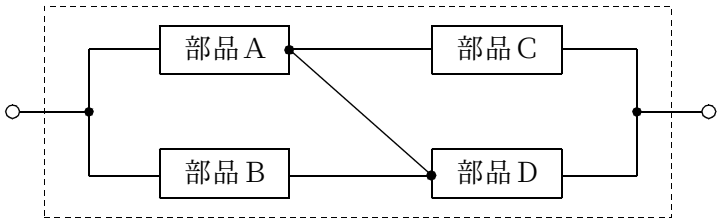


図２

(ａ)　部品Ａが故障しているという条件の下での装置Ｙの信頼度は、部品Ｂと部品Ｄが故障していない場合を計算すればよいので、 [　(カ)　] である。

(ｂ)　部品Ｂが故障しているという条件の下での装置Ｙの信頼度は、部品Ａが正常に動作しており、かつ、部品Ｃ、部品Ｄの少なくとも一つが正常で故障していない場合を計算すればよいので、 [　(キ)　] である。

(ｃ)　部品Ａと部品Ｂが共に故障していないという条件の下での装置Ｙの信頼度は、部品Ｃ、部品Ｄの少なくとも一つが正常で故障していない場合を計算すればよいので、 [　(ク)　] である。

以上(ａ)、(ｂ)及び(ｃ)の結果から、装置Ｙの信頼度は、０.９７となる。

<(オ)～(ク)の解答群>

①　０.０３	②　０.０４	③　０.０８	④　０.０９
⑤　０.２４	⑥　０.５５	⑦　０.６８	⑧　０.６９
⑨　０.７８	⑩　０.８０	⑪　０.８５	⑫　０.８８
⑬　０.８９	⑭　０.９６	⑮　０.９７	⑯　０.９９

問５　次の問いに答えよ。　　(小計２０点)

(１)　次の文章は、公開鍵(かぎ)暗号基盤(ＰＫＩ：Public Key Infrastructure)を用いた情報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)

ＰＫＩは、公開鍵暗号方式を用いてディジタル署名、相手認証、メッセージ認証、安全な鍵配送などの情報セキュリティサービスを行うための基盤となるものである。

［(ア)］が発行する公開鍵証明書を利用して、公開鍵が本当に本人のものであることを確認することができる。

メッセージの送付にあたり、送信者は、メッセージの［(イ)］を秘密鍵で暗号化してディジタル署名を生成し、メッセージに添付して送付する。受取側では、送信者の公開鍵を用いて、受信したディジタル署名を復号し、メッセージの［(イ)］が一致することを確認することにより、ディジタル署名者の正当性と［(ウ)］を確認できる。

また、メッセージの暗号化・復号のための共通鍵の配送には［(エ)］などを使用して、安全な共通鍵の配送方法を実現している。

<(ア)～(エ)の解答群>

①　ＡＥＳ暗号	②　メッセージの完全性
③　ＤＥＳ暗号	④　オブジェクト識別子
⑤　ＲＳＡ暗号	⑥　不正アクセス防止機能
⑦　共通鍵の正当性	⑧　コンピュータウィルスの感染チェック
⑨　ハッシュ値	⑩　ＩＴＵ－Ｔセキュリティ ＷＧ
⑪　シリアル番号	⑫　ＩＥＴＦが設立した管理機関
⑬　バージョン番号	⑭　信頼できる第三者の認証機関
⑮　国際的に認知されたセキュリティフォーラム	

(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)

暗号方式について述べた次の文章は、 [(オ)] が正しい。

<(オ)の解答群>
① ＤＥＳは、公開鍵(かぎ)暗号方式の一つである。
② ＲＳＡは、素因数分解の計算の複雑さを利用した公開鍵暗号方式の一つである。
③ 共通鍵暗号方式は、公開鍵暗号方式と比較して、暗号化・復号処理に時間がかかる。
④ 共通鍵暗号方式の長所は、鍵の配送・管理が容易なことである。
⑤ ディジタル署名は、一般に、共通鍵暗号方式を利用して、ユーザ認証及びメッセージ認証を行う。

(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)

セキュアプロトコルであるＩＰsec、Ｓ／ＭＩＭＥ、ＴＬＳ(ＳＳＬ)について述べた次のＡ～Ｃの文章は、 [(カ)] 。

Ａ ＩＰsecは、ＩＰ層での暗号化と認証を行うための規格である。認証ヘッダを利用して、改ざん防止及びパケットの送信元確認が行われる。またパケットを暗号化することにより、通信路上での情報詐取を防ぐ。
Ｂ Ｓ／ＭＩＭＥは、Ｗｅｂブラウザ通信のセキュリティを確保するために開発されたプロトコルであり、インターネットを介した通信で、機密性、完全性及び認証の機能を有している。
Ｃ インターネット経由の電子メールのやり取りには、盗聴・改ざん・なりすましといったセキュリティの問題が付きまとう。ＴＬＳ(ＳＳＬ)は、これらの問題を暗号技術により解決する暗号電子メールの国際標準である。

<(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

(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)

ＩＤＳ(侵入検知システム)について述べた次のＡ～Ｃの文章は、 [(キ)] 。

Ａ　ＩＤＳは、不正侵入、情報の漏えいなどセキュリティ上の問題を分析、検知するために、ネットワークあるいは、コンピュータシステム上で起こった事象を監視・通知するシステムである。

Ｂ　ＩＤＳにより情報を取得する方法は、ネットワークモニタリングによる方法、アクセス制御による方法及びファイル情報の変化などを比較する方法の三つである。

Ｃ　ＩＤＳによる侵入検知のアルゴリズムは、不正検知(Misuse Detection)と異常検知(Anomaly Detection)の二つである。

<(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) 次の文章は、広義のコンピュータウィルス(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)

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 イントラネットに接続されているコンピュータのうち、１台でもセキュリティホールが存在すれば、被害が発生する可能性があるため、総合的なコンピュータウィルス対策が必要である。

② コンピュータウィルスに感染したメールの送受信が、コンピュータウィルスをまん延させる原因となるため、電子メールの本文や添付ファイルが、コンピュータウィルスに感染していないかチェックする機能や特定の差出人のメールを拒否するなどの機能をサーバなどに設ける。

③ イントラネット内のクライアント／サーバシステムでは、クライアント端末が起動されたときに、ファイルサーバのコンピュータウィルス対策ソフトウェアと当該クライアント端末のそれとを比較し、常に、クライアント端末を最新の状態に更新する仕組みを導入する。

④ Ｗｅｂページの閲覧は、コンピュータウィ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。

⑤ コンピュータウィルスが未知のもので駆除できないときや不審なファイルを発見したときは、感染防止などのために、該当するファイルの削除、拡張子の変更、隔離用フォルダへの移動などの処置を行う。