問 1 正解 完璧 直前チェック

IPv6が利用できるネットワークに接続したPCにおいて，二つのIPv6アドレスが割り当てられていた。

(1) 2001:db8::b083:ba94:60c7:7c36
(2) fe80::200:c0ff:fea8:2

このうち，(2)はリンクローカルユニキャストアドレスである。この説明として適切なものはどれか。

ア 下位のビットにこのPCのIPv4アドレスを埋め込み，IPv6アドレスとIPv4アドレスを関連付けて管理を安易にするアドレスである。
イ グローバルユニキャストアドレスが取得できなかったときだけに有効なアドレスである。
ウ このアドレスを使った場合，パケットはネットワークには送信されず，自分自身のPC内で動作しているプログラムとだけ通信できる。
エ このアドレスをもつネットワークインタフェースからルータを介さずに直接接続できる相手との通信にだけ使用できるアドレスである。

問 2 正解 完璧 直前チェック

通信技術の一つであるPLCの説明として，適切なものはどれか。

ア 音声データをIPネットワークで伝送する技術
イ 電力線を通信回線として利用する技術
ウ 無線LANの標準規格であるIEEE 802.11シリーズの総称
エ 無線通信における暗号化技術

問 3 正解 完璧 直前チェック

180台の電話機のトラフィックを調べたところ，電話機1台当たりの呼の発生頻度（発着呼の合計）は3分に1回，平均回線保留時間は80秒であった。このときの呼量は何アーランか。

ア 4　　イ 12　　ウ 45　　エ 80

問1 エ

解説 **リンクローカルユニキャストアドレス**は，同一リンク（ネットワーク）上でのみ有効なアドレスである。IPv6は，PCをスイッチングハブなどのネットワーク機器に接続した際に，同一リンク上ではネットワークの設定を行わなくても通信が可能である。これは，IPv6の規定によって定義されているためである。ほかのリンクとの通信を行う場合は，PCにネットワークの追加設定が必要となる。

問2 イ

解説 **PLC**（Power Line Communication）：電力線通信は，電力線を利用してネットワーク通信を行う技術である。用途例は，家庭内でネットワーク接続する際に，既存の電力線を利用した接続を行うことである。電力線は，どの家庭でも配線されているためLAN配線を行うよりも導入が容易である。

ア：**VoIP**（Voice over IP）の説明である。
ウ：**IEEE802.11**は，IEEE802.11a，IEEE802.11bなど複数の規格がある。
エ：WEP，WPA，WPA2など無線通信の暗号化技術は複数ある。

問3 エ

解説 **アーラン**は通信回線の単位で，1回線を1時間継続的に占有して利用するときの呼量を指す。アーランの計算は，電話機1台当たりの利用時間を求め，全体の台数を掛ければよい。

60分÷3分＝20回（1時間当たり）
20回×80秒＝1,600秒（1台当たり）
1,600秒×180台÷3,600秒＝80〔アーラン〕

問 4

正解 完璧 直前チェック

IPv4のマルチキャストに関する記述のうち，適切なものはどれか。

ア　全てのマルチキャストアドレスは，アドレスごとにあらかじめ用途が固定的に決められている。
イ　マルチキャストアドレスには，クラスDのアドレスが使用される。
ウ　マルチキャストパケットは，TTL値に関係なくIPマルチキャスト対応ルータによって中継される。
エ　マルチキャストパケットは，ネットワーク上の全てのホストによって受信され，IPより上位の層で，必要なデータか否かが判断される。

問 5

正解 完璧 直前チェック

スパニングツリープロトコルに関する記述のうち，適切なものはどれか。

ア　OSI基本参照モデルにおけるネットワーク層のプロトコルである。
イ　ブリッジ間に複数経路がある場合，同時にフレーム転送することを可能にするプロトコルである。
ウ　ブロードキャストフレームを，ブリッジ間で転送しない利点がある。
エ　ルートブリッジの決定には，ブリッジの優先順位とMACアドレスが使用される。

問 6

正解 完璧 直前チェック

DNSサーバにおいて，IPv6のアドレス情報を登録するレコードはどれか。

ア　AAAAレコード　　イ　CNAMEレコード
ウ　MXレコード　　エ　SOAレコード

春 秋

問4　イ

解説　**クラスDのIPアドレス**は，マルチキャストアドレスを割り振るために使用する。マルチキャストとは，単一のパケットで複数のノードに同一データを送信するパケット通信技術（同報通信）による通信方法のことである。

ア：アドレスごとに固定の用途は決められていない。
ウ：マルチキャストパケットは，TTL（Time To Live：存続時間）が0になるまでマルチキャスト対応ルータによって中継される。TTLが大きい値であれば広範囲に中継されることになる。
エ：全てのコンピュータに受信されるのは，ブロードキャストである。

問5　エ

解説　**スパニングツリー**は，データリンク層（OSIレイヤ2）で利用するもので，スイッチングハブネットワークループの検出や，迂回ルートの自動切換えを行うプロトコルである。STPとも呼ばれる。インテリジェントスイッチングハブには，ほぼ実装されている。

通常スイッチングハブをループ状にLANケーブルで接続すると，ブロードキャストストームが発生するので通信できない。STPは，ループ内の一つのポートを自動的に停止してループを防ぐ機能をもつ。

ア：**スパニングツリー**は，データリンク層のプロトコルである。
イ：複数経路を，一つの経路に制御するプロトコルである。
ウ：**ブロードキャストフレーム**は，ブリッジ間で転送される。ループさせないためのプロトコルである。
エ：**ルートブリッジ**の決定には，プライオリティ値による優先順位が採用される。同一プライオリティ値の場合では，MACアドレスを利用して決定する。**ルートブリッジ**とは，スパニングツリーを設定した際に，経路情報の元を管理するスイッチングハブの名称である。

問6　ア

解説

AAAAレコード：IPv6のアドレス情報を登録するレコードである。IPv4の場合は，Aレコードであり，正引きレコードとも呼ぶ。ドメイン名からIPアドレスを問い合わせるためのレコードである。

CNAMEレコード：Canonical Nameレコード。ホスト名に別名を付けるレコードである。

MXレコード：Mail Exchangerレコード。電子メールの送信に利用される。DNS上で電子メールの配送先ホスト名を指定する際に利用する。

SOAレコード：Start Of Authorityレコード。DNSで指定するゾーン（xxx.co.jpなど）の基本的設定を行うレコードである。シリアル番号，リフレッシュなどを指定する。

問 7

正解 □ 完璧 □ 直前チェック □

ルーティングプロトコルであるBGP-4の説明として，適切なものはどれか。

ア　自律システム間で，経路情報に付加されたパス属性を使用し，ポリシに基づいて経路を選択するパスベクタ方式のプロトコルである。

イ　全てのノードが同一のリンク状態データベースを用い，コストが最小となる経路を最適経路とするプロトコルである。

ウ　到達可能な宛先アドレスまでのホップ数が最小となる経路を，最適経路とするプロトコルである。

エ　パケットが転送される経路のノードを，送信元ノードが明示的に指定するプロトコルである。

問 8

正解 □ 完璧 □ 直前チェック □

DNSでのホスト名とIPアドレスの対応付けに関する記述のうち，適切なものはどれか。

ア　一つのホスト名に複数のIPアドレスを対応させることはできるが，複数のホスト名に同一のIPアドレスを対応させることはできない。

イ　一つのホスト名に複数のIPアドレスを対応させることも，複数のホスト名に同一のIPアドレスを対応させることもできる。

ウ　複数のホスト名に同一のIPアドレスを対応させることはできるが，一つのホスト名に複数のIPアドレスを対応させることはできない。

エ　ホスト名とIPアドレスの対応は全て1対1である。

問 9

正解 □ 完璧 □ 直前チェック □

IPv4におけるARPのMACアドレス解決機能をIPv6で実現するプロトコルはどれか。

ア　DHCPv6　　イ　ICMPv6　　ウ　IGMPv2　　エ　RIPng

問7　ア

解説　**BGP-4**は，組織間の経路情報をやり取りする経路制御プロトコルである。対象となる組織を自立システム（AS：Autonomous System）と呼ぶ。主にプロバイダ間の経路制御に用いられる。

イ：**OSPF**（Open Shortest Path First）に関する説明である。

ウ：**RIP**（Routing Information Protocol）に関する説明である。

エ：**ソースルーティング**に関する説明である。

問8　イ

解説　**DNS**（Domain Name System）のホスト名は，厳密にはFQDN（Fully Qualified Domain Name）で記述される。これは，TLD（トップレベルドメイン）までのドメイン名が記述されたホスト名である。基本的に，FQDNとIPアドレスは1対1であるが，バーチャルホストを利用すると，一つのホストと複数のFQDNに対応付けられる。またDNSラウンドロビンを用いると，一つのFQDNを複数のIPアドレスに対応付けることができる。なお，DNSラウンドロビンは負荷分散で用いる技術である。

問9　イ

解説　IPv4の**ARP**（Address Resolution Protocol）は，IPアドレスからMACアドレスを解決するプロトコルである。

DHCPv6（Dynamic Host Configuration Protocol for IPv6）：コンピュータがネットワーク接続する際に，必要な情報を自動的に割り当てるプロトコルのIPv6版である。IPv4では，DHCPとなる。

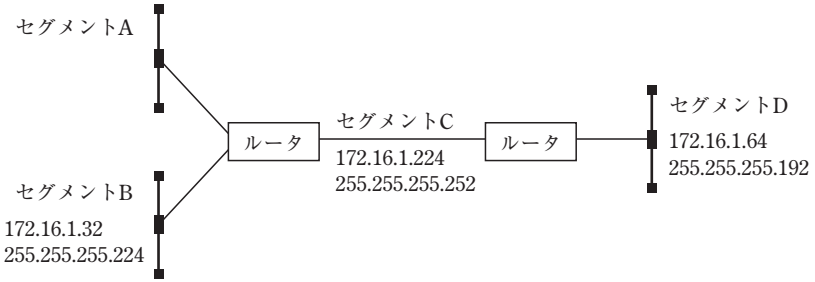
ICMPv6（Internet Control Message Protocol for IPv6）：隣接探査に使用される。IPv4のARPと同等のプロトコルである。

IGMPv2（Internet Group Management Protocol version 2）：マルチキャストを利用する際に利用されるプロトコルである。

RIPng（RIP Next Generation）：IPv6で利用される，ルーティングプロトコルである。IPv4では，RIP（Routing Information Protocol）となる。

問 10 正解 完璧 直前チェック

可変長サブネットマスクを利用できるルータを用いた図のネットワークにおいて，全てのセグメント間で通信可能としたい。セグメントAに割り当てるサブネットワークアドレスとして，適切なものはどれか。ここで，図中の各セグメントの数値は，上段がネットワークアドレス，下段がサブネットマスクを表す。



	ネットワークアドレス	サブネットマスク
ア	172.16.1.0	255.255.255.128
イ	172.16.1.128	255.255.255.128
ウ	172.16.1.128	255.255.255.192
エ	172.16.1.192	255.255.255.192

問 11 正解 完璧 直前チェック

RIP（Routing Information Protocol）における，宛先に到達可能な最大ホップ数は幾らか。

ア 15　　イ 31　　ウ 63　　エ 127

問 12 正解 完璧 直前チェック

RSVPの説明として，適切なものはどれか。

ア QoSを実現するために，IPパケットに優先度情報を付加することによって，インターネットを流れるトラフィックを制御する。
イ オーディオ情報・ビジュアル情報などの連続した情報の発生源を遠隔制御する。
ウ シーケンス番号とタイムスタンプを付加することによって，リアルタイム情報を伝送するパケット間の時間差を保証する。
エ ネットワーク資源の予約を行い，ノード間でのマルチメディア情報などのリアルタイム通信を実現する。

問10 ウ

解説 設問の条件は，「全てのセグメント間で通信可能としたい」とあるため，セグメントA～Dは重複しないネットワークアドレスとする必要がある。サブネットマスクによるIPアドレスの範囲から割り当て可能なネットワークアドレスを求める。

	利用可能なIPアドレスの範囲
セグメントB	172.16.1.32 ～ 172.16.1.63
セグメントC	172.16.1.224 ～ 172.16.227
セグメントD	172.16.1.64 ～ 172.16.127

選択肢	利用可能なIPアドレスの範囲	重複
ア	172.16.1.0～172.16.1.127	セグメントB，Dと重複
イ	172.16.1.128 ～ 172.16.1.255	セグメントCと重複
ウ	172.16.1.128 ～ 172.16.1.191	割り当て可能
エ	172.16.1.192 ～ 172.16.1.255	セグメントCと重複

サブネットマスクからIPアドレスの範囲の求め方は以下のとおりである。

セグメントBの場合は，4オクテット目の224を，255から引いたものがIPアドレスの個数となる。利用できるIPアドレスの最大値は，ネットワークアドレスの4オクテット目32と，IPアドレスの個数31を足した63となる。

255 − 224 + 32 = 63

同様に，セグメントC，セグメントD，選択肢ア～エも求めればよい。

問11 ア

解説 RIP（Routing Information Protocol）は，ゲートウェイ間のホップ数によって経路を制御するプロトコルである。RIPでは，宛先にパケットが到達するまでに経由するルータの数が最大となっている（最大ホップ数15）。

問12 エ

解説 RSVP（Resource reSerVation Protocol）は，ネットワークの帯域制御用プロトコルである。テレビ会議や，リアルタイム動画配信では，動画や音声を途切れなくスムーズに表示する必要性がある。帯域制御がない状態では，大量のパケット送信がほかのPCから行われるとパケットの遅延や，再送が発生する。RSVPでは，通信相手までのネットワーク帯域を予約して，通信品質を確保するために利用される。

問 13 正解 完璧 直前チェック

クラスBのIPアドレスで，サブネットマスクが16進数のFFFFFF80である場合，利用可能なホスト数は最大幾つか。

ア 126　　イ 127　　ウ 254　　エ 255

問 14 正解 完璧 直前チェック

ネットワークの制御に関する記述のうち，適切なものはどれか。

ア TCPでは，ウィンドウサイズが固定で輻輳(ふくそう)回避ができないので，輻輳が起きると，データに対してタイムアウト処理が必要になる。
イ 誤り制御方式の一つであるフォワード誤り訂正方式は，受信側で誤りを検出し，送信側にデータの再送を要求する方式である。
ウ ウィンドウによるフロー制御では，応答確認があったブロック数だけウィンドウをずらすことによって，複数のデータをまとめて送ることができる。
エ データグラム方式では，両端を結ぶ仮想の通信路を確立し，以降は全てその経路を通すことによって，経路選択のオーバヘッドを小さくしている。

問 15 正解 完璧 直前チェック

インターネットの国際化ドメイン名（IDN：Internationalized Domain Name）の説明として，適切なものはどれか。

ア IDNでは，全角英数字を含むドメイン名（例：ＥＸＡＭＰＬＥ１.jp）と半角英数字によるドメイン名（例：EXAMPLE1.jp）は異なるドメイン名として扱われる。
イ IDNでは，通信する際に，漢字やアラビア文字などのドメイン名を，ASCII文字だけから成る文字列のドメイン名に一定の規則で変換する。
ウ IDNとは，“.com”や“.net”などの，どの国からも取得できるトップレベルドメイン名のことである。
エ IDNとは，“.jp”や“.uk”などの，国別トップレベルドメインを使ったドメイン名のことである。

問13 ア

解説 16進表示のホスト数を求める計算である。ホスト数を計算するには，サブネットマスクの最下位8ビット（16進で80の部分）を計算すればよい。

（80）16進＝（1000 0000）2進

0の部分がホスト部であり，ホストアドレスとして利用できない2を引くと答えが求められる。ホストアドレスとして利用できない二つのアドレスは，ネットワークアドレスと，ブロードキャストアドレスとなる。

選択肢は，10進数であるため，（1000 0000）2進を10進数に変換し，128とする。

128 − 2 = 126

問14 ウ

解説

ア：**ウィンドウサイズ**は固定ではなく可変長である。
イ：**フォワード誤り訂正**は，送信側で行う。
エ：**VC**（バーチャルサーキット）の説明である。

問15 イ

解説 **国際化ドメイン名**（**IDN**：Internationalized Domain Name）は，アルファベット，数字，ハイフンに加え，そのラベルに漢字やひらがな，アラビア文字などのASCII以外の文字を使えるようにするものである。日本語ドメインのように，英語圏以外の国でドメインをよりわかりやすく利用するための仕組みである。

問 16 正解 □ 完璧 □ 直前チェック □

DNSSECの機能はどれか。

ア　DNSキャッシュサーバの設定によって再帰的な問合せの受付範囲が最大になるようにする。
イ　DNSサーバから受け取るリソースレコードに対するディジタル署名を利用して，リソースレコードの送信者の正当性とデータの完全性を検証する。
ウ　ISPなどのセカンダリDNSサーバを利用してDNSコンテンツサーバを二重化することによって名前解決の可用性を高める。
エ　共通鍵暗号技術とハッシュ関数を利用したセキュアな方法によって，DNS更新要求が許可されているエンドポイントを特定し認証する。

問 17 正解 □ 完璧 □ 直前チェック □

ディジタル証明書に関する記述のうち，適切なものはどれか。

ア　S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-T X.400で規定されている。
イ　ディジタル証明書は，SSL/TLSプロトコルにおいて通信データの暗号化のための鍵交換や通信相手の認証に利用されている。
ウ　認証局が発行するディジタル証明書は，申請者の秘密鍵に対して認証局がディジタル署名したものである。
エ　ルート認証局は，下位の認証局の公開鍵にルート認証局の公開鍵でディジタル署名したディジタル証明書を発行する。

問16　イ

解説　DNSSEC（DNS Security Extensions）は，DNSサーバから送られてくるIPアドレスとホスト名の対応情報の信頼性を証明するセキュリティ拡張機能である。応答を送信するDNSサーバが秘密鍵を使って応答に署名し，受信する側が公開鍵で検証する。秘密鍵で正しい署名を付けるので，署名の検証によって偽の応答を検知できる。そのためDNSキャッシュポイズニングを防ぐことができる。

問17　イ

解説　ディジタル証明書は，ITU-Tで公開鍵証明書の標準としてX.509が策定され，そのX.509v3をもとにインターネット利用を目的とした公開鍵証明書がIETFでRFCとして標準化された。ディジタル証明書には，シリアル番号，発行者名，有効期間，所有者名，所有者の公開鍵などの情報が含まれており，認証局の秘密鍵で電子署名が付与されている。

ア：S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-TのX.500ディレクトリシリーズのX.509で規定されている。
ウ：ディジタル証明書には，申請者の公開鍵に認証局の電子署名が付与されている。
エ：下位認証局の証明書は，ルート認証局の秘密鍵で電子署名されている。

問 18 正解 完璧 直前チェック

利用者認証情報を管理するサーバ1台と複数のアクセスポイントで構成された無線LAN環境がある。PCが無線LANに接続されるときの利用者認証とアクセス制御に，IEEE 802.1XとRADIUSを利用する場合の実装方法はどれか。

ア　PCにはIEEE 802.1Xのサプリカントを実装し，かつ，RADIUSクライアントの機能をもたせる。
イ　アクセスポイントにはIEEE 802.1Xのオーセンティケータを実装し，かつ，RADIUSクライアントの機能をもたせる。
ウ　アクセスポイントにはIEEE 802.1Xのサプリカントを実装し，かつ，RADIUSサーバの機能をもたせる。
エ　サーバにはIEEE 802.1Xのオーセンティケータを実装し，かつ，RADIUSサーバの機能をもたせる。

問 19 正解 完璧 直前チェック

CSIRTの説明として，適切なものはどれか。

ア　IPアドレスの割当て方針の決定，DNSルートサーバの運用監視，DNS管理に関する調整などを世界規模で行う組織である。
イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。
ウ　企業・組織内や政府機関に設置され，コンピュータセキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。
エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもった人や組織の総称である。

問18　イ

解説 **RADIUS**（Remote Authentication Dial In User Service）は，アクセスサーバと認証サーバ間でやり取りする認証プロトコルである。クライアントが認証を求める際に，認証を必要とするサーバ（アクセスサーバ）と認証機能を分離し，利用者の一元管理，アクセスログの記録が可能となる。無線LANだけでなく，有線LANでも利用できる。

IEEE 802.1Xでは，認証のためのデータのやり取りを，PCとアクセスポイントで行う。また，アクセスポイントとRADIUSサーバの間ではRADIUSプロトコルによって中継する。サプリカントとは，IEEE 802.1X通信を可能とするためのPC用のソフトウェアである。

ア：PCでは認証自体を行わないため，RADIUSクライアントの機能をもたせない。
イ：正しい。アクセスポイントではRADIUSクライアントの機能をもたせ，認証を行う。
ウ：アクセスポイントにはサプリカントを実装しない。
エ：オーセンティケータは，認証を中継するアクセスポイントにもたせる。

問19　ウ

解説 **CSIRT**（Computer Security Incident Response Team：コンピュータ・セキュリティ・インシデント・レスポンス・チーム）は，セキュリティに関する様々な事象について活動を行う組織の総称である。企業の場合では，CSIRTを立ち上げることで，事象（インシデント）の問合せ窓口の設置やセキュリティ教育，技術情報の提供などを実施することでセキュリティ対応を継続的に高度に対応していくことが可能となる。

問 20 正解 完璧 直前チェック

ウイルス検知手法の一つであるビヘイビア法を説明したものはどれか。

ア　ウイルスの特徴的なコード列が検査対象プログラム内に存在するかどうかを調べて，もし存在していればウイルスとして検知する。
イ　各ファイルに，チェックサム値などウイルスではないことを保証する情報を付加しておき，もし保証する情報が検査対象ファイルに付加されていないか無効ならば，ウイルスとして検知する。
ウ　検査対象ファイルのハッシュ値と，安全な場所に保管してあるその対象の原本のハッシュ値を比較して，もし異なっていればウイルスとして検知する。
エ　検査対象プログラムを動作させてその挙動を観察し，もしウイルスによく見られる行動を起こせばウイルスとして検知する。

問 21 正解 完璧 直前チェック

利用者が別の機能によって認証された後，一定時間に限ってメールの送信を許可する仕組みはどれか。

ア　DKIM　　イ　OP25B　　ウ　POP before SMTP　　エ　SPF

問 22 正解 完璧 直前チェック

メモリインタリーブの説明として，適切なものはどれか。

ア　主記憶と外部記憶を一元的にアドレス付けし，主記憶の物理容量を超えるメモリ空間を提供する。
イ　主記憶と磁気ディスク装置との間にバッファメモリを置いて，双方のアクセス速度の差を補う。
ウ　主記憶と入出力装置との間でCPUとは独立にデータ転送を行う。
エ　主記憶の連続したアドレスを複数のブロックに分けて，並列的にアクセスすることでアクセスを高速化する。

問20　エ

解説　ウイルス検知手段の**ビヘイビア法**は，検査対象のプログラムの挙動を監視し，ウイルスとしての動作（ビヘイビア）を検出する手法である。
ア：ウイルス定義ファイルを用いた**パターンマッチング方式**である。
イ：**チェックサム法**の説明である。
ウ：**コンペア法**の説明である。

問21　ウ

解説
DKIM（Domain Keys Identified Mail）：送信元メールサーバがメールに付加したディジタル署名を受信側がチェックすることで送信元の正当性を確認する。
OP25B（Outbound Port 25 Blocking）：SMTPが利用するポート番号25の通信を拒否する。
POP before SMTP：利用者がメールサーバからメールをクライアントに取り込むときに認証した情報を元に，一定時間メール送信の許可を行うプロトコルである。
POP（Post Office Protocol）：クライアントが電子メールデータをサーバから取り込むためのプロトコルである。
SMTP（Simple Mail Transfer Protocol）：電子メールをサーバ間で送受信するためのプロトコルである。
SPF（Sender Policy Framework）：差出人のメールアドレスが他のドメインになりすましていないかどうかを検出する，電子メールにおける送信ドメイン認証の仕組みである。

問22　エ

解説　**メモリインタリーブ**とは，メインメモリをバンクと呼ばれるブロック単位に分割し，それぞれ独自に並列してアクセスできるようにする方式をいう。分割したメモリには順番が付与され，複数の連続したアドレスにアクセスする場合にアクセス時間を短縮することができる。
ア：**仮想記憶**の説明である。
イ：**ディスクキャッシュメモリ**の説明である。
ウ：**DMA**（Direct Memory Access）の説明である。

問 23 正解 完璧 直前チェック

端末から400バイトの電文を送信し，ホストコンピュータが600バイトの電文を返信するトランザクション処理システムがある。回線速度を1×10^6ビット/秒，回線の伝送効率を80%，ホストコンピュータのトランザクション当たりの処理時間を40ミリ秒とする。ホストコンピュータでの処理待ち時間，伝送制御のための処理時間などは無視できるとした場合，端末における電文の送信開始から受信完了までの時間は何ミリ秒か。ここで，1バイトは8ビットであるものとする。

ア 10　　イ 44　　ウ 46　　エ 50

問 24 正解 完璧 直前チェック

エラー埋込み法において，埋め込まれたエラー数をS，埋め込まれたエラーのうち発見されたエラー数をm，埋め込まれたエラーを含まないテスト開始前の潜在エラー数をT，発見された総エラー数をnとしたとき，S，T，m，nの関係を表す式はどれか。

ア $\frac{m}{S} = \frac{n-m}{T}$　　イ $\frac{m}{S} = \frac{T}{n-m}$

ウ $\frac{m}{S} = \frac{n}{T}$　　エ $\frac{m}{S} = \frac{T}{n}$

問 25 正解 完璧 直前チェック

ソフトウェアのリバースエンジニアリングの説明はどれか。

ア 開発支援ツールなどを用いて，設計情報からソースコードを自動生成する。
イ 外部から見たときの振る舞いを変えずに，ソフトウェアの内部構造を変える。
ウ 既存のソフトウェアを解析し，その仕様や構造を明らかにする。
エ 既存のソフトウェアを分析し理解した上で，ソフトウェア全体を新しく構築し直す。

問23　エ

解説 初めに端末からホストコンピュータに送信された電文400バイト＝3,200ビットの送信時間を求める。

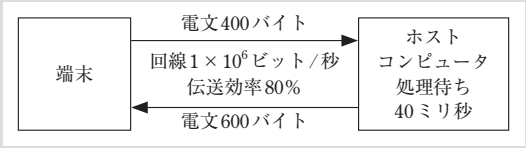
$3{,}200 / (1 \times 10^6 \times 0.8) = 0.004$秒＝4ミリ秒

次にホストコンピュータから端末に返信された600バイト＝4,800ビットの送信時間を求める。

$4{,}800 / (1 \times 10^6 \times 0.8) = 0.006$秒＝6ミリ秒

したがって解答は，4ミリ秒，6ミリ秒と，ホストコンピュータの処理待ち時間40ミリ秒を合計したものとなる。

4 + 6 + 40 = 50ミリ秒



問24　ア

解説 **エラー埋込み法**において，埋め込まれたエラー数と，そのなかから発見されたエラー数の比率および潜在エラー数とそのなかから発見されたエラー数の比率は，等しいものと考える。

埋め込まれたエラー数とそのなかから発見されたエラー数の比率は，問題より次のように表記できる。

$\frac{m}{S}$

潜在的なエラー数とそのなかから発見されたエラー数の比率も，同様に次のように表記できる。

$\frac{n-m}{T}$

これらが等しいことから，解答は次のとおりとなる。

$\frac{m}{S} = \frac{n-m}{T}$

問25　ウ

解説 **リバースエンジニアリング**は，既存のプログラムを解析し，その仕組みや仕様，目的，構成部品，要素技術などを明らかにすることである。解析結果は，ソフトウェアの修正や再開発の支援，他社製品の分析・調査に利用される。

また，リバースエンジニアリングには著作権の侵害になる可能性があるため，実施する際は注意が必要である。