問題

問 1

正解 □ 完璧 □ 直前CHECK □

100Mビット／秒のLANを使用し，1件のレコード長が1,000バイトの電文を1,000件連続して伝送するとき，伝送時間は何秒か．ここで，LANの伝送効率は50％とする．

ア　0.02　　イ　0.08　　ウ　0.16　　エ　1.6

問 2

正解 □ 完璧 □ 直前CHECK □

CSMA/CD方式のブリッジで接続された二つのセグメント間で，ブロードキャストフレームの中継と，衝突発生時にできる不完全フレームの中継について，適切な組合せはどれか．

	ブロードキャストフレームの中継	衝突発生時にできる 不完全フレームの中継
ア	中継する	中継する
イ	中継する	中継しない
ウ	中継しない	中継する
エ	中継しない	中継しない

問 3

正解 □ 完璧 □ 直前CHECK □

CSMA方式のLAN制御に関する記述として，適切なものはどれか．

ア　キャリア信号を検出し，データの送信を制御する．
イ　送信権をもつメッセージ（トークン）を得た端末がデータを送信する．
ウ　データ送信中に衝突が起こった場合は，直ちに再送を行う．
エ　伝送路が使用中でもデータの送信はできる．

問1　ウ

全体のデータ長は，1,000バイト×1,000件＝1Mバイト＝8Mビットとなる．

伝送速度が100Mビット／秒のLANを使用するので，8M÷100M＝0.08〔秒〕となる．ただし伝送効率が50％なので，伝送速は半分となり，伝送時間も倍となる．したがって，0.08×2＝0.16秒となる．

問2　イ

ブリッジとは，電気的な信号をフレーム情報に戻してから中継処理を行う装置である．OSI参照モデルのデータ層にあたる．衝突フレームや破損フレームは破棄し，正常なフレームのみを中継送信する．

ブロードキャストフレームは，ブリッジのすべてのポートに転送される．

問3　ア

CSMA（Carrier Sense Multiple Access）は「搬送波感知多重アクセス」と訳される．ユーザがパケットを送出する際，LAN上のキャリア信号を検出することにより回線の空き状況を調べてから送出を実行する方式である．

イ：**トークンパッシング**に関する説明である．

ウ：衝突が発生した場合，CSMA方式では送信を中断し，一定時間が経過した後，改めてLAN上のキャリア信号検出を行う．

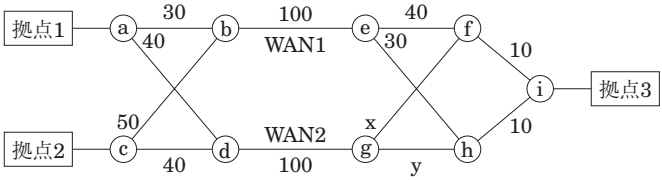
エ：伝送路にキャリア信号が検出された場合，送信を中断し，一定時間が経過した後，改めてLAN上のキャリア信号検出を行う．

問題

問 4

正解 完璧 直前CHECK

図は，OSPFを使用するルータa～iのネットワーク構成を示す．拠点1と拠点3の間の通信はWAN1を．拠点2と拠点3の間の通信はWAN2を通過するようにしたい．xとyに設定するコストとして適切な組合せはどれか．ここで，図中の数字はOSPFコストを示す．



	x	y
ア	20	20
イ	30	30
ウ	40	40
エ	50	50

問 5

正解 完璧 直前CHECK

ネットワークのQoSで使用されるトラフィック制御方式に関する説明のうち，適切なものはどれか．

ア　通信を開始する前にネットワークに対して帯域などのリソースを要求し，確保の状況に応じて通信を制御することを，アドミッション制御という．

イ　入力されたトラフィックが規定された最大速度を超過しないか監視し，超過分のパケットを破棄するか優先度を下げる制御を，シェーピングという．

ウ　パケットの送出間隔を調整することによって，規定された最大速度を超過しないようにトラフィックを平準化する制御を，ポリシングという．

エ　フレームの種類やあて先に応じて優先度を変えて中継することを，ベストエフォートという．

問4　イ

OSPF（Open Shortest Path First）は，TCP/IPにおける**経路選択**（ルーティング）**プロトコル**の一つである．一般的に，ルータに設定することで複数のルーティング情報を自動的に更新する．OSPFは，最小のコストとなるよう経路を選択する．

拠点1ー拠点3

a－b－e－h－i（30＋100＋30＋10＝170）が最小コストとなる．拠点1－拠点3はWAN1（b－e間）を通る必要があるため，拠点1－WAN2－拠点3の経路のコストは，WAN1経路の170よりも大きい180以上に設定する必要がある．したがって，xおよびyは30以上となる．

拠点2ー拠点3

拠点1－拠点3の条件から，xおよびyは30以上となるため，選択肢イ，ウ，エをそれぞれ代入して解答を求める．したがって，拠点2－拠点3の経路がc－d－g－(x)－f－i，もしくはc－d－g－(y)－h－iとなる，WAN2を通る経路を選択する．

イ：拠点2－拠点3の経路は180となり，正しいコストである．

ウ，エ：c－b－e－h－iの経路のコストが190であるため，xおよびyに40以上を設定するとWAN2を経由しないケースが出る．したがって誤りである．

問5　ア

アドミッション制御は，**QoS保証**の枠組み（IntServ/RSVP，DiffServ）に基づいて，通信を開始する前にネットワークに対してリソース確保要求を行い，リソースの確保状況に応じて通信を制御する．例としては，音声通話や映像配信などの遅延が問題となるアプリケーションや，緊急通話のような高負荷状況のネットワークでも通話可能であるアプリケーションに用いる．

イ：**ポリシング**の説明である．

ウ：**シェーピング**の説明である．

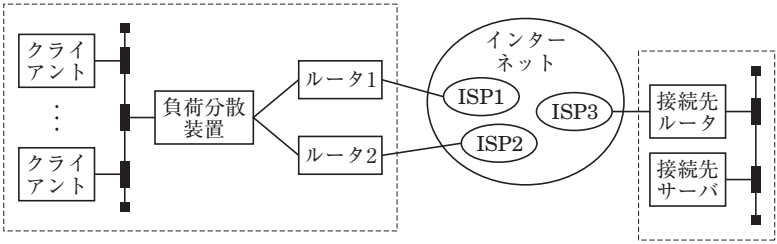
エ：**ベストエフォート**とは，状況等によってネットワークのパフォーマンスは上下するが，それぞれの状況に応じて最善の努力を行い，サービスを提供することを意味する．

問題

問 6

正解 □ 完璧 □ 直前CHECK □

図のようなルータ1とルータ2及び負荷分散装置を使ったマルチホーミングが可能な構成において，クライアントから接続先サーバあてのパケットに対する負荷分散装置の処理として，適切なものはどれか.



ア　あて先IPアドレスはそのままで，あて先MACアドレスを接続先サーバのMACアドレスに置き換える.

イ　あて先IPアドレスはそのままで，あて先MACアドレスをルータ1又はルータ2のMACアドレスに置き換える.

ウ　あて先MACアドレスはそのままで，あて先IPアドレスを接続先ルータのIPアドレスに置き換える.

エ　あて先MACアドレスはそのままで，あて先IPアドレスをルータ1又はルータ2のIPアドレスに置き換える.

問 7

正解 □ 完璧 □ 直前CHECK □

TCP/IPネットワークで使用されるARPの説明として，適切なものはどれか.

ア　IPアドレスからMACアドレスを得るためのプロトコル

イ　IPアドレスからホスト名（ドメイン名）を得るためのプロトコル

ウ　MACアドレスからIPアドレスを得るためのプロトコル

エ　ホスト名（ドメイン名）からIPアドレスを得るためのプロトコル

問 8

正解 □ 完璧 □ 直前CHECK □

DHCPを用いるネットワーク構成で，リレーエージェントが必要になるのは，ネットワークにどの機器が用いられている場合か.

ア　スイッチングハブ　　イ　ブリッジ

ウ　リピータ　　エ　ルータ

問6　イ

問題の**負荷分散装置**は，クライアントから接続先サーバへの経路を二つにすることで，伝送路の負荷を軽減することを目的としている．

クライアントから送信されるパケットでは，あて先IPアドレスが接続先サーバとなっている．また，あて先MACアドレスは負荷分散装置となっている．負荷分散装置ではこのあて先MACアドレスを書き換える．負荷分散装置は伝送路の負荷状況を確認して，ルータ1あるいはルータ2のMACアドレスに書き換える処理を行う．

問7　ア

ARP（Address Resolution Protocol）：TCP/IPネットワークにおいて，IPアドレスからイーサネットの物理アドレス（MACアドレス）を求めるために使用するプロトコルである．逆に，MACアドレスからIPアドレスを求めるためにはRARP（Reverse ARP）を利用する．

ア：ARPの説明である．
イ：DNS（Domain Name System）の説明である．
ウ：RARPの説明である．
エ：DNSの逆引きの説明である．

問8　エ

DHCP（Dynamic Host Configuration Protocol）とは，各クライアントがDHCP サーバからIPアドレスを割り当ててもらうためのプロトコルである．

クライアントは起動時に自分のIP アドレスを取得するために，DHCP DISCOVERというブロードキャストパケットを送信する．このパケットに対してDHCP サーバが応答して，IPアドレスが割り当てられる．しかしクライアントが属する自ネットワーク内にDHCPサーバがなく，隣接するネットワークにDHCPサーバがある場合は，DHCP DISCOVERを隣接するネットワークのDHCPサーバに代理問い合わせる機能が必要になる．この機能が**リレーエージェント**である．

ブロードキャストパケットを通過させるスイチッングハブやブリッジ，リピータではこの機能は必要ない．ブロードキャストパケットを通過させないルータでは必要となる．

問題

問 9

正解 □ 完璧 □ 直前CHECK □

DNSに関する記述のうち，適切なものはどれか．

ア　インターネット上のDNSサーバは階層化されており，ある名前に対して情報がない場合は，上位のDNSサーバに問い合わせる．

イ　セカンダリサーバは，大規模なネットワークシステムにおいてプライマリサーバの負荷を軽減するために用いられ，プライマリサーバとは異なる内容のデータベースを保持している．

ウ　ネームリゾルバは，クライアントからの要求に応答し，データベースを使用してドメイン名，ホスト名に対応するIPアドレスを返すプログラムである．

エ　リソースレコードには，ドメイン，ホスト，ネームサーバなどに関する情報が保持されており，DNSサーバの構築時に登録され，更新することができない．

問 10

正解 □ 完璧 □ 直前CHECK □

HTTPのGETメソッドとPOSTメソッドに関する記述のうち，適切なものはどれか．

ア　GETの実装は必須であるが，POSTはオプションである．

イ　GETはサーバへの送信，POSTはサーバからの応答である．

ウ　POSTの応答はキャッシュされるが，GETはキャッシュされない．

エ　POSTはサーバのCGIを起動できるが，GETは起動できない．

問 11

正解 □ 完璧 □ 直前CHECK □

電源オフ時にIPアドレスを保持することができない装置が，電源オン時に自装置のMACアドレスから自装置に割り当てられているIPアドレスを知るために用いるデータリンク層のプロトコルで，ブロードキャストを利用するものはどれか．

ア　ARP　　イ　DHCP　　ウ　DNS　　エ　RARP

問9　ア

DNS（Domain Name System）はTCP/IPネットワークで用いられるネームサービスの仕組みのことである．対応表を用いて，ドメイン名やホスト名とIPアドレスを互いに変換する機能を持つ．対応表を一つのDNSサーバに格納することは不可能であるので，DNSサーバは木構造を持った分散型のデータベースとなっている．

イ：**セカンダリサーバ**の内容は**プライマリサーバ**の機能を代行するものであるから，その内容は一致したものである．

ウ：**ネームリゾルバ**は，ドメイン名やホスト名とIPアドレスの対応をクライアントからサーバに問い合わせるクライアント側の機能である．

エ：**リソースレコード**はDNSが利用するデータのことである．主なリソースレコードには，電子メールの送信に利用される**MXレコード**，ドメイン名からIPアドレスを問い合わせるための**Aレコード**，ホスト名に別名を付ける**CNAMEレコード**などがある．

問10　ア

GETメソッド：HTMLページを呼び出すとき，ブラウザがサーバにファイルを要求するために使用するメソッド．サーバはGETメソッドとHEADメソッドを必ずサポートしなければならない．

POSTメソッド：メッセージの書き込みやデータの更新・追加など，ブラウザからサーバにデータを送付する際に使用するメソッド．

イ：サーバへのデータの送信はPOSTで行う．

ウ：GETの応答は，次に同じリクエストが発生する可能性があるので，キャッシュされる．

エ：GETがURLの一部になることを応用すると，サーバのCGIに直接データを送信して起動することができる．

問11　エ

ARP（Address Resolution Protocol）：IPアドレスからMACアドレスを取得するプロトコル．

DHCP（Dynamic Host Configuration Protocol）：IPアドレスやサブネットマスクなど，TCP/IP接続に必要な設定を動的に行うプロトコル．

DNS（Domain Name System）：機器名とIPアドレスの変換を相互に行うシステム．

RARP（Reverse Address Resolution Protocol）：MACアドレスからIPアドレスを取得するプロトコル．

問題

問 12

正解 □ 完璧 □ 直前CHECK □

HTTPを使って，Webサーバのコンテンツのアップロードや更新を可能にするプロトコルはどれか.

ア　CSS　　イ　MIME　　ウ　SSL　　エ　WebDAV

問 13

正解 □ 完璧 □ 直前CHECK □

ネットワークに接続されているホストのIPアドレスが212.62.31.90で，サブネットマスクが255.255.255.224のとき，ホストアドレスはどれか.

ア　10　　イ　26　　ウ　90　　エ　212

問12　エ

CSS（Cascading Style Sheets）：HTMLやXMLはファイルの論理構造を記述するものであるが，CSSはその見栄えを記述し，指示するものである．論理構造とCSSの記述を対応させておけば，CSSを変更することで複数のHTMLファイルやXMLファイルの表示を変更することができる．

MIME（Multipurpose Internet Mail Extension）：テキスト以外のデータ（画像，音声，バイナリデータなど）を電子メールで送信するための規格．

SSL（Secure Socket Layer）：インターネット上で情報を暗号化して送受信するためのプロトコルで，データの盗聴や改ざん，なりすましを防ぐことができる．公開鍵暗号方式やディジタル証明書など，いくつかのセキュリティ技術を組み合わせて実現している．

WebDAV（Web-based Distributed Authoring and Versioning）：Webサーバ上のファイルやフォルダを，HTTPを介して管理するための仕様．サーバ上のファイルやフォルダの一覧を表示したり，複製・更新・削除などが可能となる．

問13　イ

サブネットマスクから，ホストアドレスを求める．問題文からサブネットマスクとホストのIPアドレスを2進数表記すると，下の表のようになる．

サブネットマスク	255. 255. 255. 224
（2進数表記）	11111111. 11111111. 11111111. 11100000
ホストのIPアドレス	212. 62. 31. 90
（2進数表記）	11010100. 00111110. 00011111. 01011010

サブネットマスクの2進数表記では，下位5ビットが0となっている．ホストアドレスはこの下位5ビットで示されるところであるから，これをホストのIPアドレスの2進数表記から読み取ると「11010」となる．これを10進数に変換すると，11010＝26となる．

問題

問 14

正解 □ 完璧 □ 直前CHECK □

サブネットマスクが，255.255.255.0である四つのネットワーク192.168.32.0，192.168.33.0，192.168.34.0，192.168.35.0を，CIDRを使ってスーパーネット化したとき，ネットワーク番号とサブネットマスクの適切な組合せはどれか．

	ネットワーク番号	サブネットマスク
ア	192.168.32.0	255.255.248.0
イ	192.168.32.0	255.255.252.0
ウ	192.168.35.0	255.255.248.0
エ	192.168.35.0	255.255.252.0

問 15

正解 □ 完璧 □ 直前CHECK □

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，応答確認の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，以降はすべ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14　イ

CIDR（Classless Inter-Domain Routing）：IPアドレスの割当に当たって，ホストアドレスのフィールドをさらに分割して使用する仕組み．

スーパーネット化：ネットワークを管理する単位を大きくすること．つまり，複数のネットワークを統合して一つのネットワークと見なし，管理することである．ネットワークの数が減ることで管理の効率化が図れる．

ネットワーク番号：IPアドレスのうち，ネットワークアドレスを示す部分．

各ネットワークのIPアドレスに共通している部分を除くと，「32，33，34，35」となる．これらについての16進表現とそのサブネットマスクがどうなるかを考えればよい．

255	1111 1111
32	0010 0000
33	0010 0001
34	0010 0010
35	0010 0011

上表より，32～35は下二桁が異なっていることがわかる．すなわち，下二桁をマスクしなければ各ネットワークの識別が可能となる．つまり該当箇所のマスクは「1111 1100＝252」となる．したがってサブネットマスクは「255.255.252.0」となる．

ネットワーク番号は四つのネットワークに共通となるIPアドレスの上位部分である．上表の32～35より，下二桁を00とすると「0010　0000」，すなわち「32」となる．したがって，「192.168.32.0」となる．

問15　ウ

フロー制御とは，データ転送での送信及び受信確認の制御である．現在のウィンドウ内にあるデータを相手方の確認応答無しに送信できるようにするために，ウィンドウをデータの送信方向にずらしながら送信する手法である．

ア：TCPでは，ネットワークの状況に応じて転送速度を制御する輻輳制御を行っている．輻輳制御では，タイムアウト処理ではなく転送速度の調節でネットワークの輻輳を回避する．

イ：**フォワード誤り訂正方式**は**自己訂正方式**とも呼ばれる方式である．誤りが軽微であれば，送信元に再送要求を行わずに自己訂正を行う．

エ：**データグラム方式**はコネクションレスの通信方式である．通信路の確立は行わない．

問題

問 16

正解 □ 完璧 □ 直前CHECK □

同一のLANに接続された複数のルータを，仮想的に1台のルータとして見えるようにして冗長構成を実現するプロトコルはどれか．

ア　ARP　　イ　OSPF　　ウ　RSTP　　エ　VRRP

問 17

正解 □ 完璧 □ 直前CHECK □

Webサーバを使ったシステムにおいて，インターネットから受け取ったリクエストをWebサーバに中継する仕組みはどれか．

ア　DMZ　　イ　フォワードプロキシ
ウ　プロキシARP　　エ　リバースプロキシ

問16　エ

ARP（Address Resolution Protocol）：イーサネット通信でのデータの送信において，あて先のIPアドレスからあて先のMACアドレスを問い合わせるプロトコル．

OSPF（Open Shortest Path First）：伝送速度などのコストを考慮に入れて経路選択を行い，ルーティング情報を更新する仕組み．

RSTP（Rapid Spanning-Tree Protocol）：伝送路がループ状態になっていると，伝送路上に送信されたデータがそのループを巡回し続けるループ障害が発生する．これを避けるためのプロトコルがSTP（Spanning-Tree Protocol）である．RSTPはこれを高速化したものである．

VRRP（Virtual Router Redundancy Protocol）：ルータを多重化するためのプロトコル．複数のルータを一つのグループとし，通常はそのうちの一つのマスタルータが通信を行う．マスタルータに障害が発生した場合は，残りのルータが通信を代替する．同じLANに接続されているルータを仮想的に1台のルータとして使うことで，ルータの障害をリカバリできるようにしたものである．

問17　エ

DMZ（DeMilitarized Zone）：外部ネットワークと内部ネットワークの間にある，ファイアウォールによって隔離された区域である．外部ネットワークからの不正アクセスを防止しながら，内部ネットワークを保護している．

フォワードプロキシ：内部ネットワークのクライアントから外部ネットワークのサーバへのアクセスを中継するプロキシ．

プロキシARP：ホストへのARP要求に対して，代理としてARP応答する機能である．

リバースプロキシ：外部ネットワークのクライアントから内部ネットワークのサーバへの要求を中継するプロキシ．

問題

問 18

正解 □ 完璧 □ 直前CHECK □

チャレンジレスポンス方式として，適切なものはどれか．

ア　SSLによって，クライアント側で固定パスワードを暗号化して送信する．
イ　トークンという装置が表示する毎回異なったデータをパスワードとして送信する．
ウ　任意長のデータを入力として固定長のハッシュ値を出力する．
エ　利用者が入力したパスワードと，サーバから送られたランダムなデータとをクライアント側で演算し，その結果を認証用データに用いる．

問 19

正解 □ 完璧 □ 直前CHECK □

企業のDMZ上で1台のDNSサーバをインターネット公開用と社内用で共用している．このDNSサーバが，DNSキャッシュポイズニングの被害を受けた結果，引き起こされ得る現象はどれか．

ア　DNSサーバで設定された自社の公開WebサーバのFQDN情報が書き換えられ，外部からの参照者が，本来とは異なるWebサーバに誘導される．
イ　DNSサーバのメモリ上にワームが常駐し，DNS参照元に対して不正プログラムを送り込む．
ウ　社内の利用者が，インターネット上の特定のWebサーバを参照する場合に，本来とは異なるWebサーバに誘導される．
エ　電子メールの不正中継対策をした自社のメールサーバが，不正中継の踏み台にされる．

問 20

正解 □ 完璧 □ 直前CHECK □

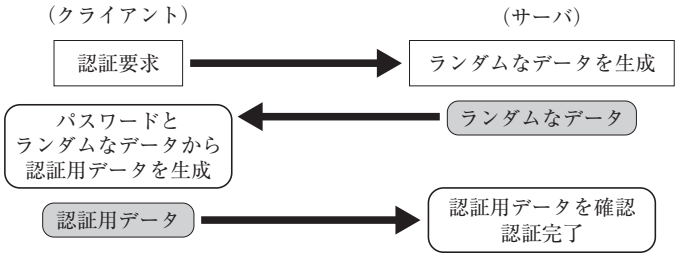
パケットフィルタリング型ファイアウォールのフィルタリングルールを用いて，本来必要なサービスに影響を及ぼすことなく防げるものはどれか．

ア　外部に公開していないサービスへのアクセス
イ　サーバで動作するソフトウェアのセキュリティの脆弱(ぜい)生を突く攻撃
ウ　電子メールに添付されたファイルのマクロウイルスの侵入
エ　電子メール爆弾などのDoS攻撃

問18　エ

ア：SSLで保護した**ベーシック認証**の説明である．
イ：**ワンタイムパスワード**の説明である．
ウ：**ハッシュ関数**の説明である．
エ：**チャレンジレスポンス方式**の説明である．

チャレンジレスポンスの図：



問19　ウ

DNSキャッシュポイズニングは，DNSサーバに偽ドメイン情報をキャッシュさせる攻撃手法である．DNSサーバに偽ドメイン情報がキャッシュされてしまうと，DNSサーバはクライアントに偽ドメインのアドレスを返してしまい，クライアントは偽装されたWebサーバに誘導されてしまう．

ア：**FQDN情報**とは，完全修飾ドメイン名（Fully Qualified Domain Name）と呼ばれる．これはDNSサーバにIPアドレスを問い合わせる際に問合せ側が使用する．したがってこれが書き換えられると，自社の公開サーバにアクセスできなくなる可能性がある．
エ：**踏み台攻撃**と呼ばれる手法である．

問20　ア

イ，ウ：**パケットフィルタリング**ではIPパケット内のデータをチェックしないため，ソフトウェアの脆弱性を突く攻撃を防止できない．同様に，電子メールに添付されたファイルをチェックしないため，**マクロウィルス**の侵入を許してしまう．
エ：電子メールによる**DoS攻撃**は，送信元のメールサーバからのパケットを通さないことで対応可能であるが，送信元から送られてくる正規のメールまで受け取れなくなってしまう．そのため，本来必要なサービスに影響を及ぼしてしまう．

問題

問 21

正解 完璧 直前CHECK

レイヤ2スイッチや無線LANアクセスポイントで接続を許可する仕組みはどれか.

ア　DHCP
イ　Webシングルサインオン
ウ　認証VLAN
エ　パーソナルファイアウォール

問 22

正解 完璧 直前CHECK

シリアルATAの説明として，適切なものはどれか.

ア　PCと周辺機器とを結ぶシリアルインタフェースであり，キーボード，マウス，スピーカ，プリンタ，CD-RWドライブなど多岐にわたる周辺機器を接続する
イ　PCと周辺機器とを結ぶシリアルインタフェースであり，磁気ディスク装置，DVDドライブなどの高速な周辺機器を接続する.
ウ　PCと通信機器とを結ぶシリアルインタフェースであり，ルータ又はモデムを接続する.
エ　PCとディジタルAV機器とを結ぶシリアルインタフェースであり，セットトップボックス，DVDプレーヤなどを接続する.

問 23

正解 完璧 直前CHECK

シンクライアントシステムの利点として，適切なものはどれか.

ア　アプリケーションが使用する主記憶のフラグメンテーションが起こりにくいので，応答性が向上する.
イ　サーバ側でアプリケーションやデータを管理するので，セキュリティが強化できる.
ウ　システムが利用するネットワーク資源が減るので，通信費を削減できる.
エ　データを保管する費用が減るので，サーバへの投資を削減できる.

問21　ウ

DHCP（Dynamic Host Configuration Protocol）：IPアドレスやサブネットマスクなど，TCP/IP接続に必要な設定を動的に行うプロトコル．

Webシングルサインオン：ユーザが認証サーバで一度認証操作を行えば，許可されたWebサーバで再度認証操作せずに接続可能となる．

認証VLAN：LANに，接続する際に，機器（レイヤ2スイッチや無線LANアクセスポイント）が認証サーバを用いてPCのユーザを認証し，そのユーザに対応するVLANにPCを接続する．

パーソナルファイアウォール：機器のネットワーク接続の通信を制御するアプリケーションであり，PCへの不正アクセスを防止する個人向けのファイアウォールである．

問22　イ

シリアルATA（SATA：Serial Advanced Technology Attachment）は，PCと周辺機器（CD-RW，DVDドライブ，HDD等）を接続するためのインタフェースである．

ア：キーボードやマウスは**USB**を利用して接続する．

ウ：PCと通信機器を接続するものはLAN接続である．

エ：**セットトップボックス**はCATVや衛星放送などの信号を一般のテレビで見ることができるように変換する装置である．

問23　イ

シンクライアントシステムとは，機能を限定的にすることでセキュリティやコストを効率的に管理することを目的としたクライアント端末と，アプリケーションやデータストレージといったリソースをネット経由でクライアント端末に提供するサーバにより構成されたシステムである．

ア：アプリケーションはサーバ側で稼働する．シンクライアントシステムによってクライアント側の負荷は軽減されるが，サーバ側でのフラグメンテーション発生が改善されることはない．

ウ：アプリケーションなどのリソースにアクセスするたびにネットワークを利用するので，通信費の削減には結びつかない．

エ：サーバ側で大規模なストレージを用意する必要がある．クライアント端末1台当たりのコストは下がるが，サーバ側への投資はより大きくなる可能性がある．

問題

問 24

正解 □ 完璧 □ 直前CHECK □

ブラックボックステストのテストデータの作成方法のうち，最も適切なものはどれか．

ア　稼働中のシステムから実データを無作為に抽出し，テストデータを作成する．
イ　機能仕様から同値クラスや限界値を識別し，テストデータを作成する．
ウ　業務で発生するデータの発生頻度を分析し，テストデータを作成する．
エ　プログラムの流れ図から，分岐条件に基づいたテストデータを作成する．

問 25

正解 □ 完璧 □ 直前CHECK □

開発した製品で利用している新規技術に関して特許の出願を行った．日本において特許権の取得が可能なものはどれか．

ア　学会で技術内容を発表した日から11か月目に出願した．
イ　顧客と守秘義務の確認を取った上で技術内容を説明した後，製品発表前に出願した．
ウ　製品に使用した暗号の生成式を出願した．
エ　製品を販売した後に出願した．

問24　イ

ブラックボックステストは，入力に対して仕様書通りの出力が得られるかどうかを確認することで，外部から見た機能の検証を行う．入力と出力だけに着目し，内部的な処理構造は問題としない．テストデータは，**限界値分析**や**同値クラス**を用いて作成する．

エ：ホワイトボックスにおけるテストデータ作成の説明である．

問25　イ

ア：特許法第29条1によると，「特許出願前に日本国内又は外国において公然知られた発明」は特許を受けることができない．出願前に学会で発表された発明は，この「公然知られた発明」に該当すると考えられる．

イ：守秘義務を伴って説明された発明は，「公然知られた発明」に該当しないので，特許を取得することができる．

ウ，エ：特許法第29条2によると，「特許出願前に日本国内又は外国において公然実施をされた発明」は特許を取得することができない．選択肢ウおよびエは，いずれも製品に使用しているので，これは「公然実施された発明」に該当すると考えられる．