

問 1 正解  完璧  直前チェック

ネットワーク機器のイーサネットポートがもつ機能である Automatic MDI/MDI-X の説明として、適切なものはどれか。

- ア 接続先ポートの受信不可状態を自動判別して、それを基に自装置からの送信を止める機能
- イ 接続先ポートの全二重・半二重を自動判別して、それを基に自装置の全二重・半二重を変更する機能
- ウ 接続先ポートの速度を自動判別して、それを基に自装置のポートの速度を変更する機能
- エ 接続先ポートのピン割当てを自動判別して、ストレートケーブル又はクロスケーブルのいずれでも接続できる機能

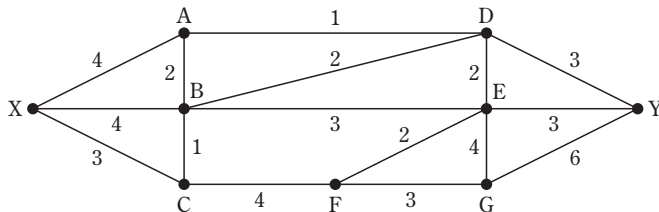
問 2 正解  完璧  直前チェック

高速無線通信で使われている多重化方式であり、データ信号を複数のサブキャリアに分割し、各サブキャリアが互いに干渉しないように配置する方式はどれか。

- ア CCK      イ CDM      ウ OFDM      エ TDM

問 3 正解  完璧  直前チェック

図のネットワークで、数字は二つの地点間で同時に使用できる論理回線の多重度を示している。X地点からY地点までには同時に最大幾つの論理回線を使用することができるか。



- ア 8      イ 9      ウ 10      エ 11

問 1 エ

**解説** Automatic MDI/MDI-Xとは、スイッチングハブや、ハブがもつ機能で、通信ポートがMDIかMDI-Xかを自動的に判別し接続する機能である。よってエが正解。具体的には、PC (MDI) とスイッチングハブ (MDI-X) をLANケーブルで接続する場合は、LANケーブルの種類はストレートケーブルを使用する必要がある。このとき、クロスケーブルを使用しても、接続の間違いをスイッチングハブに実装されている、Automatic MDI/MDI-Xによって通信可能となる。

問 2 ウ

**解説**  
**CCK** (Complementary Code Keying：相補符号変調)：コンプリメンタリコード (相補符号) を用いてDQPSK (差動4層位相変調) 信号を拡散する方式である。  
**CDM** (Code Division Multiplex：符号分割多重化)：拡散符号を各情報に割り当てて、スペクトル拡散変調する方式である。  
**OFDM** (Orthogonal Frequency Division Multiplexing：直交周波数分割多重)：データを直交したサブキャリアに乗せることで、密に並べても互いに干渉しない多重方式である。よってウが正解。  
**TDM** (Time Division Multiplex：時分割多重化)：時分割した固定スロットをそれぞれの情報に割り当てる方式である。

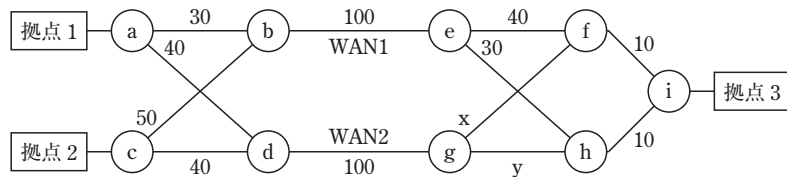
問 3 ウ

**解説** 多重度の最大値とは、各経路の最小回線数を求めればよい。よって次表よりウが正解。

論理	回線数
X-(A, B, C)	4 + 4 + 3 = 11
(A, B, C)-(D, E, F)	1 + 2 + 3 + 4 = 10
(A, B, F)-(D, E, G)	1 + 2 + 3 + 2 + 3 = 11
(D, E, G)-Y	3 + 3 + 6 = 12

問 4 正解  完璧  直前チェック

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コストを占めず。



	x	y
ア	20	20
イ	30	30
ウ	40	40
エ	50	50

問 5 正解  完璧  直前チェック

ネットワークのQoSを実現するために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放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 フレームの種類や宛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

**解説** 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－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－拠点3**

拠点1－拠点3の条件から、xおよびyは30以上になるため選択肢アは該当しない、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-iもしくは、c-d-g-y-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の経路が、190のコストであるため、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

**解説** 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。よってアが正解。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、状況などにより、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 6 正解  完璧  直前チェック

IPv4でのARPを利用したGratuitous ARPの説明として、適切なものはどれか。

- ア ターゲットIPアドレスフィールドに自端末が使用するIPアドレスを入れて、MACアドレスを問い合わせる。
- イ ターゲットIPアドレスフィールドに通信したい相手のIPアドレスを入れて、MACアドレスを問い合わせる。
- ウ ターゲットMACアドレスフィールドに自端末が使用するMACアドレスを入れて、IPアドレスを問い合わせる。
- エ ターゲットMACアドレスフィールドに通信したい相手のMACアドレスを入れて、IPアドレスを問い合わせる。

問 7 正解  完璧  直前チェック

図はIPv4におけるIPsecのデータ形式を示している。ESPトンネルモードの電文中で、暗号化されているのはどの部分か。

新IP ヘッダ	ESP ヘッダ	オリジナル IPヘッダ	TCP ヘッダ	データ	ESP トレーラ	ESP 認証データ
------------	------------	----------------	------------	-----	-------------	--------------

- ア ESPヘッダからESPトレーラまで
- イ TCPヘッダからESP認証データまで
- ウ オリジナルIPヘッダからESPトレーラまで
- エ 新IPヘッダからESP認証データまで

問 8 正解  完璧  直前チェック

クラスDのIPアドレスを使用するのはどの場合か。

- ア 端末数が250台程度までの比較的小規模なホストアドレスを割り振る。
- イ 端末数が65,000台程度の中規模なホストアドレスを割り振る。
- ウ プライベートアドレスを割り振る。
- エ マルチキャストアドレスを割り振る。

問6 ア

**解説** Gratuitous ARPは、ARP(Address Resolution Protocol)の一つで、同一ネットワーク上に、自身に設定するIPアドレスの重複検出や、同一セグメントの機器に対するARPキャッシュの更新を行うプロトコルである。よってアが正解。

イ：ターゲットIPアドレスフィールドに通信したいIPアドレスではなく、自端末のIPアドレスを入れる。よって誤りである。

ウ、エ：ARPは、IPアドレスからMACアドレスを問い合わせるので、MACアドレスフィールドから、IPアドレスを問い合わせるのは誤りである。

問7 ウ

**解説** ESPトンネルモードは、ネットワーク間でオリジナルパケット(オリジナルIPヘッダからデータまで)を暗号化して送信する際に使用される。

データの暗号化では、暗号化されるデータが暗号アルゴリズムのビット長の倍数となる必要があるため、オリジナルパケットにパディングデータ(ESPトレーラ)を加えて、調整してから暗号化処理を行う。そのため、暗号化されているのはオリジナルIPヘッダからESPトレーラまでである。よってウが正解。

問8 エ

**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。よってエが正解。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)による通信方法である。

ア：クラスAは、254台( $2^8-2$ )のホストアドレスをもつ。

イ：クラスBは、65,534台( $2^{16}-2$ )のホストアドレスをもつ。

ウ：プライベートアドレスは、クラスA、B、Cすべてで利用できる。

問 9 正解  完璧  直前チェック

MPLSの説明として、適切なものはどれか。

- ア IPプロトコルに暗号化や認証などのセキュリティ機能を付加するための規格である。
- イ L2FとPPTPを統合して改良したデータリンク層のトンネリングプロトコルである。
- ウ PPPデータフレームをIPパケットでカプセル化して、インターネットを通過させるためのトンネリングプロトコルである。
- エ ラベルと呼ばれる識別子を挿入することによって、IPアドレスに依存しないルーティングを実現する、ラベルスイッチング方式を用いたパケット転送技術である。

問 10 正解  完璧  直前チェック

インターネットプロトコルのTCPとUDP両方のヘッダに存在するものはどれか。

- ア 宛先IPアドレス           イ 宛先MACアドレス
- ウ 生存時間(TTL)           エ 送信元ポート番号

問 11 正解  完璧  直前チェック

IPv4アドレスが192.168.10.0/24～192.168.58.0/24のネットワークを対象に経路を集約するとき、集約した経路のネットワークアドレスのビット数が最も多くなるものはどれか。

- ア 192.168.0.0/16           イ 192.168.0.0/17
- ウ 192.168.0.0/18           エ 192.168.0.0/19

問9 工

解説

MPLS (Multi Protocol Label Switching)：主にWANで使用されるL3スイッチングである。

ルーティング情報にラベルを付けることでルーティングを高速化する。よってエが正解。

ア：IPsecに関する記述である。

イ：L2TP (Layer 2 Tunneling Protocol)に関する記述である。

ウ：PPTP (Point to Point Tunneling Protocol)に関する記述である。

問10 工

解説

TCP (Transmission Control Protocol)：通信相手との準備 (SYN, ACK) を用いて通信する方式である。

UDP (User Datagram Protocol)：通信相手との特別な準備をせず通信する方式である。

ア、ウ：宛先IPアドレス、生存時間 (TTL) は、IPヘッダに含まれるため、TCP、UDPのどちらのヘッダにも含まれない。

イ：MACアドレスはデータリンク層の、イーサネットフレームに含まれるため、TCP、UDPのどちらのヘッダにも含まれない。

エ：TCP、UDP両方のヘッダに含まれる。よって正しい。

問11 ウ

解説 設問内のサブネットがすべて包括されている範囲の中で最小のものが回答となる。サブネットは、/24といった、/で示された後の数字部分。ホスト部は、サブネット部分以外の部分である。

	ネットワーク	サブネット	ホスト部
①	192.168.10.0/24	11000000.10101000	00000000
②	192.168.58.0/24	11000000.10101000	00000000
ア	192.168.0.0/16	11000000.10101000	00000000.00000000
イ	192.168.0.0/17	11000000.10101000.0	00000000.00000000
ウ	192.168.0.0/18	11000000.10101000.00	00000000.00000000
エ	192.168.0.0/19	11000000.10101000.000	00000000.00000000

①、②は、左から18ビットまでが同一である。すべてを包括するには18ビット以内で、ア、イ、ウとなり、その中でもホスト部の桁数が最小のウが正解となる。

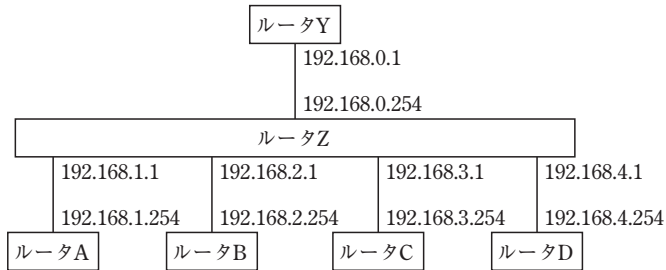
問 12 正解  完璧  直前チェック

TCPヘッダ中のウィンドウサイズの説明として、適切なものはどれか。

- ア 受信エラー時の再送に備えて送信側が保持しているデータのサイズを受信側に知らせるために使用される。
- イ 受信側からの確認応答を待たずに、データを続けて送信できるかどうかの判断に使用される。
- ウ 送信側と受信側の最適なバッファサイズを接続開始時のハンドシェイクで決定するために使用される。
- エ 複数セグメントから成るデータの送信時、後続するセグメント数を受信側に知らせるために使用される。

問 13 正解  完璧  直前チェック

図のようなルータ6台から成るネットワークにおいて、宛先IPアドレス10.100.100.1のIPパケットをルータYから受け取ったルータZは、どのルータに転送するか。ここで、ルータZは次に示すルーティングテーブルを用い、最長一致法(longest-match algorithm)によってルーティングするものとする。



[ルータZのルーティングテーブル]

宛先アドレス	サブネットマスク	ネクストホップ
10.0.0.0	255.0.0.0	192.168.1.254
10.64.0.0	255.224.0.0	192.168.2.254
10.96.0.0	255.252.0.0	192.168.3.254
10.128.0.0	255.128.0.0	192.168.4.254
0.0.0.0	0.0.0.0	192.168.0.1

- ア ルータA      イ ルータB      ウ ルータC      エ ルータD

問 12 イ

**解説** TCPでは、送信側が確認応答を待たずに送信できるデータの大きさをウィンドウサイズという。受信側が送信側に受信可能なデータサイズを通知するようになっている。

受信側が送信側にウィンドウサイズを通知することで、受信側がデータを取りこぼさない大きさのデータサイズでデータを送信し、データの再送を発生させない、効率のよい通信を行う。よってイが正解。

問 13 ア

**解説** ルーティングの最長一致法とは、宛先IPアドレスに対して一致するビット数が最も長いルートを採用する方式である。

本問の宛先IPアドレス、10.100.100.1が、表の宛先アドレスの範囲内かつ、最も長いルートを採用する。宛先アドレスと、サブネットマスクから、IPアドレスの範囲を計算する方法は、2進数に変換し、ANDを取ることで求めることができる。

宛先アドレス	サブネットマスク	IPアドレスの範囲
10.0.0.0 00001010.0.0.0	255.0.0.0 11111111.0.0.0	10.0.0.0 ~ 10.255.255.255 <u>00001010</u> .00000000.00000000.00000000 ~ <u>00001010</u> .11111111.11111111.11111111
10.64.0.0 00001010.01000000.0.0	225.224.0.0 11111111.11110000.0.0	10.64.0.0 ~ 10.95.0.0 <u>00001010.010</u> 00000.00000000.00000000 ~ <u>00001010.0101</u> 1111.11111111.11111111
10.96.0.0 00001010.01100000.0.0	255.252.0.0 11111111.11111100.0.0	10.96.0.0 ~ 10.99.0.0 <u>00001010.011000</u> 00.00000000.00000000 ~ <u>00001010.011000</u> 11.11111111.11111111
10.128.0.0 00001010.10000000.0.0	255.128.0.0 11111111.10000000.0.0	10.128.0.0 ~ 10.255.0.0 <u>00001010.10000000</u> .00000000.00000000 ~ <u>00001010.1</u> 11111111.11111111.11111111

0.0.0.0は、デフォルトゲートウェイを意味し、すべてのルーティングテーブルに当てはまらなかったときのネクストホップが指定される。

10.100.100.1は、宛先アドレス10.0.0.0の範囲であるため、ネクストホップは、192.168.1.254となり、ルータAとなる。よってアが正解。

問 14 正解  完璧  直前チェック

WebDAVの特徴はどれか。

- ア HTTP上のSOAPによってソフトウェア同士が通信して、ネットワーク上に分散したアプリケーションを連携させることができる。
- イ HTTPを拡張したプロトコルを使って、サーバ上のファイルの参照や作成、削除及びバージョン管理が行える。
- ウ WebアプリケーションからIMAPサーバにアクセスして、ブラウザから添付ファイルを含む電子メールの操作ができる。
- エ ブラウザで“ftp://”から始まるURLを指定して、ソフトウェアなどの大容量ファイルのダウンロードができる。

問 15 正解  完璧  直前チェック

チャットアプリケーションのようなWebブラウザとWebサーバ間でのリアルタイム性の高い双方向通信に利用されているWebSocketプロトコルの特徴はどれか。

- ア WebブラウザとWebサーバ間で双方向通信を行うためのデータ形式はXMLを使って定義されている。
- イ WebブラウザとWebサーバ間でリアルタイム性の高い通信を実現するためにRTPを使用する。
- ウ WebブラウザとWebサーバとの非同期通信にはXMLHttpRequestオブジェクトを利用する。
- エ Webブラウザは最初にHTTPを使ってWebサーバにハンドシェイクの要求を送る。

問 14 イ

解説

**WebDAV** (Web Distributed Authoring and Versioning) : Webコンテンツの編集や管理を目的としたHTTPを拡張し、クライアント(Webブラウザ)からWebサーバ上のファイルやフォルダを管理できるようにした仕様。よってイが正解。HTTP 1.1を拡張した仕様で、IETFによってRFC2518として定義されている。HTTPの拡張仕様であるため、SSLによる暗号化はHTTPS上でWebDAVを利用するだけでよい。

問 15 エ

**解説** **WebSocket**プロトコルは、RFC6455で勧告されている、WebブラウザとWebサーバ間でのリアルタイム性の高い双方向通信に利用されているプロトコルである。

通信の開設(openingハンドシェイク)には、HTTP Upgradeリクエストによって行われる。通信の終了(closingハンドシェイク)は、TCP closingのFin/ACKパケットによって行われる。よってエが正解。

ア : **SOAP** (Simple Object Access Protocol) の説明である。

イ : **RTP** (Real-time Transport Protocol) は、音声や動画などをリアルタイムで配信するためのデータストリームで利用される。

ウ : **XMLHttpRequest** は、JavaScriptのAPIおよびオブジェクトの一つである。Ajax (Asynchronous JavaScript XML) で用いられる。



問 16 正解  完璧  直前チェック

SAML (Security Assertion Markup Language) の説明として、最も適切なものはどれか。

- ア Webサービスに関する情報を広く公開し、それらが提供する機能などを検索可能にするための仕様
- イ 権限がない利用者による傍受、読取り、改ざんから電子メールを保護して送信するための仕様
- ウ デジタル署名に使われる鍵情報を効率よく管理するためのWebサービスの仕様
- エ 認証情報に加え、属性情報とアクセス制御情報を異なるドメインに伝達するためのWebサービスの仕様

問 17 正解  完璧  直前チェック

無線LANで使用される規格IEEE 802.1Xが定めているものはどれか。

- ア アクセスポイントがEAPを使用して、利用者を認証する仕組み
- イ アクセスポイントが認証局と連携し、パスワードをセッションごとに生成する仕組み
- ウ 無線LANに接続する機器のセキュリティ対策に関するWPSの仕様
- エ 無線LANの信号レベルで衝突を検知するCSMA/CD方式

問 18 正解  完璧  直前チェック

NTPを使った増幅型のDDoS攻撃に対して、NTPサーバが踏み台にされることを防止する対策として、適切なものはどれか。

- ア NTPサーバの設定変更によって、NTPサーバの状態確認機能(monlist)を無効にする。
- イ NTPサーバの設定変更によって、自ネットワーク外のNTPサーバへの時刻問合せができないようにする。
- ウ ファイアウォールの設定変更によって、NTPサーバが存在するネットワークのブロードキャストアドレス宛てのパケットを拒否する。
- エ ファイアウォールの設定変更によって、自ネットワーク外からの、NTP以外のUDPサービスへのアクセスを拒否する。

問 16 工

解説

SAML：標準化団体OASISによって策定された、IDやパスワードなどの認証情報を安全に交換するための仕様。SAMLを用いることで、一度の認証で複数のWebサイトやサービスの利用が可能となるシングルサインオン(SSO：Single Sign-On)を実現できる。WebサイトがSAMLに対応していれば、異なるドメインのサイトへ移動したときに、移動元のサイトと移動先のサイトがSAMLプロトコルで通信し、自動的に認証情報を引き継ぐことができる。よってエが正解。

ア：WSDL (Web Services Description Language) の説明である。

イ：S/MIME (Secure MIME) の説明である。

ウ：XKMS (XML Key Management Specification) の説明である。

問 17 ア

解説

IEEE802.1Xは、クライアントPCとアクセスポイント間での鍵交換(鍵更新を含む)や、認証のフレームワークを提供している。よってアが正解。鍵交換により共有された鍵を用いて、クライアントPCとアクセスポイント間でセッションごとに動的に異なる暗号化鍵を用いた暗号化通信が可能となる。また認証では、EAP-TLSやEAP-PEAPなどの認証方式が使用される。

問 18 ア

解説

NTP増幅型攻撃は、インターネットの時刻動機プロトコルであるNTP (Network Time Protocol) の弱点を利用して、不正なネットワークトラフィックを発生させ増幅することで攻撃する手法である。

ア：正しい。NTPサーバの状態確認機能を利用して攻撃することが可能であるため、無効にすることで防御できる。

イ、エ：NTPは他のサーバへ時間を合わせにくいため、自ネットワーク外への時刻同期ができないと時刻を合わせることができない。

ウ：ブロードキャストパケットを利用した攻撃ではないため、効果はない。

問 19 正解  完璧  直前チェック

テンペスト技術の説明とその対策として、適切なものはどれか。

- ア ディスプレイなどから放射される電磁波を傍受し、表示内容などを盗み見る技術であり、その対策としては、電磁波を遮断する。
- イ データ通信の途中でパケットを横取りし、内容を改ざんする技術であり、その対策としては、デジタル署名を利用して改ざんを検知する。
- ウ マクロウイルスにおいて使われる技術であり、その対策としては、ウイルス対策ソフトを導入し、最新の定義ファイルを適用する。
- エ 無線LANの信号を傍受し、通信内容を解析する技術であり、その対策としては、通信パケットを暗号化する。

問 20 正解  完璧  直前チェック

社内ネットワークとインターネットの接続点に、ステートフルインスペクション機能をもっていない、静的なパケットフィルタリング型のファイアウォールを設置している。このネットワーク構成において、社内のPCからインターネット上のSMTPサーバに電子メールを送信できるようにするとき、ファイアウォールで通過許可とするTCPパケットのポート番号の組合せはどれか。

	送信元	宛先	送信元 ポート番号	宛先 ポート番号
ア	PC	SMTPサーバ	25	1024以上
	SMTPサーバ	PC	1024以上	25
イ	PC	SMTPサーバ	110	1024以上
	SMTPサーバ	PC	1024以上	110
ウ	PC	SMTPサーバ	1024以上	25
	SMTPサーバ	PC	25	1024以上
エ	PC	SMTPサーバ	1024以上	110
	SMTPサーバ	PC	110	1024以上

問 19 ア

**解説** テンペスト技術とは、電子機器やケーブルから漏えいする電磁波に関するセキュリティ上の対策のことである。具体的には、回路設計の段階で信号の漏えいを防ぎつつ、ケーブルなどを被覆して電磁波をシールドすることが基本的な対策である。また、パソコンなどが入った部屋全体をシールドするという手段もある。よってアが正解。

イ：データの改ざん対策の説明である。

ウ：ウイルス対策の説明である。

エ：無線LANの盗聴対策の説明である。

問 20 ウ

**解説** 社内のPCからSMTPサーバに送るパケットとその応答パケットの通過を遮断する。発信では送信元が社内のPCとなり、宛先はSMTPサーバとなる。このとき、送信元のポート番号はOSが付与する1024以上の任意の番号であり、宛先ポート番号はSMTPの25番となる。

応答では送信元がそのSMTPサーバとなり、宛先は社内のPCである。このとき、送信元のポート番号はSMTPの25番であり、宛先ポート番号は発信時にOSが付与した1024以上の任意の番号である。よってウが正解。



問 21 正解  完璧  直前チェック

無線LANのアクセスポイントがもつプライバシーパレータ機能(アクセスポイントアイソレーション)の説明はどれか。

- ア アクセスポイントの識別子を知っている利用者だけに機器の接続を許可する。
- イ 同じ無線LANのアクセスポイントに接続している機器同士の直接通信を禁止する。
- ウ 事前に登録されたMACアドレスをもつ機器だけに無線LANへの接続を許可する。
- エ 建物外への無線LAN電波の漏れを防ぐことによって第三者による盗聴を防止する。

問 22 正解  完璧  直前チェック

ユーザプログラムの実行中に割り込みが発生した場合のプロセッサの処理として、適切なものはどれか。

- ① プログラムレジスタ(プログラムカウンタ)などの退避
- ② ユーザモードから特権モードへの移行
- ③ 割り込み処理ルーチンの開始番地の決定
- ④ 割り込み処理ルーチンの実行

- ア ① → ③ → ④ → ②      イ ② → ① → ③ → ④  
ウ ② → ③ → ④ → ①      エ ③ → ④ → ① → ②

問21 イ

**解説**

プライバシーパレータ機能：無線LANのアクセスポイントに接続されたPC間の通信を禁止する機能である。

ア、ウ：プライバシーパレータ機能は、接続許可するものではない。

イ：正しい。

エ：電波遮断用のフィルムや、シールド材の使用の説明である。

問22 イ

**解説**

プログラムレジスタは、現在実行している命令の次に実行される予定の命令のアドレスを保持する。分岐命令では、このレジスタの値を更新することによって実行の順序を制御する。処理の順序は、ユーザモードから特権モードへの移行(②)、プログラムレジスタ(①)、割り込み処理ルーチンの開始番地の決定(③)、割り込み処理ルーチン(④)の実行となる。よってイが正解。

問 23 正解  完璧  直前チェック

Webサーバ、アプリケーション (AP) サーバ及びDBサーバ各1台で構成される Web システムにおいて、次の3種類のタイムアウトを設定した。タイムアウトに設定する時間の長い順に並べたものはどれか。ここで、トランザクションはWebリクエスト内で処理を完了するものとする。

[タイムアウトの種類]

- ① APサーバのAPが、処理を開始してから終了するまで
- ② APサーバのAPにおいて、DBアクセスなどのトランザクションを開始してから終了するまで
- ③ Webサーバが、APサーバにリクエストを送信してから返信を受けるまで

ア ①, ③, ②      イ ②, ①, ③      ウ ③, ①, ②      エ ③, ②, ①

問 24 正解  完璧  直前チェック

システム開発で行うテストについて、テスト要求事項を定義するアクティビティと対応するテストの組合せのうち、適切なものはどれか。

	システム方式設計	ソフトウェア方式設計	ソフトウェア詳細設計
ア	運用テスト	システム結合テスト	ソフトウェア結合テスト
イ	運用テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
ウ	システム結合テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
エ	システム結合テスト	ソフトウェアユニットテスト	ソフトウェア結合テスト

問23 ウ

**解説** Webサーバ、アプリケーション (AP) サーバ、DBサーバで構成されるシステムでは、トランザクションの処理順序に合わせてタイムアウト時間を設定する必要がある。

処理の順序は、利用者からのリクエストとしては、Webサーバ→APサーバ→DBサーバ→APサーバ→Webサーバ→利用者となる。

そのため、Webサーバと、APサーバ間が最もタイムアウト時間が長くなる。次に、APサーバのAPが処理を開始してから終了するまでになる。APサーバはDBサーバからの返信を待つため、DBサーバよりタイムアウト時間を長くする必要がある。よってウが正解。

問24 ウ

**解説** システム開発では、次の工程が実行される。

システム方式設計→ソフトウェア方式テスト→ソフトウェア詳細設計→ソフトウェアユニットテスト→ソフトウェア結合テスト→システム結合テスト→運用テスト

システム方式設計：システム全体の方式設計を行う。

ソフトウェア方式テスト：システムを構成するソフトウェアの方式設計を行う。

ソフトウェア詳細設計：ソフトウェアをユニットに分け、各ユニットを詳細に設計する。

ソフトウェアユニットテスト：ソフトウェア詳細設計をもとに開発したユニットを、動作確認するテスト。

ソフトウェア結合テスト：それぞれのユニットを結合して、ソフトウェアを動作確認するテスト。

システム結合テスト：システム全体について、その目的や機能、応答時間や負荷を掛けたときの性能などが目標に達しているかどうかを確認するテスト。開発の最終確認となる。

運用テスト：システムの利用者や運用する担当者の主導で行われるテスト。利用部門が用意したデータを用いた承認テストなどがある。

問 25 正解 完璧 直前  
チェック

SOA (Service Oriented Architecture) の説明はどれか。

- ア Webサービスを利用するためのインターフェースやプロトコルを規定したものである。
- イ XMLを利用して、インターネット上に存在するWebサービスを検索できる仕組みである。
- ウ 業務機能を提供するサービスを組み合わせることによって、システムを構築する考え方である。
- エ サービス提供者と顧客との間でサービスの内容、範囲及び品質に対する要求水準を明確にして、あらかじめ合意を得ておくことである。

問25 ウ

## 解説

**SOA**：サービス指向アーキテクチャは、サービスの集まりとしてシステムを構築する方法である。サービスとは外部から標準化された手順で呼び出すことができるひとまとまりのソフトウェアの集合であり、各サービスがXMLで記述されたメッセージをSOAPでやり取りし、連携して動作する。

ア：**SOAP** (Simple Object Access Protocol) の説明である。

イ：**UDDI** (Universal Description, Discovery, and Integration) の説明である。

エ：**SLA** (Service Level Agreement) の説明である。