問 1 正解 完璧 直前チェック

DNSの資源レコード（リソースレコード，RR）に関する記述のうち，適切なものはどれか。

ア　CNAMEレコードは，他のDNSサーバのキャッシュ領域に情報を残す許可時間や，ゾーン情報の更新をチェックする間隔などを指定するレコードである。
イ　MXレコードは，電子メールの送り先となるサーバのIPアドレスを指定するレコードである。
ウ　NSレコードは，そのゾーン自身や下位ドメインに関するDNSサーバのホスト名を指定するレコードである。
エ　PTRレコードは，名前に対応するIPアドレスを指定するレコードである。

問 2 正解 完璧 直前チェック

ZigBeeの特徴はどれか。

ア　2.4 GHz帯を使用する無線通信方式であり，一つのマスタと最大七つのスレーブから成るスター型ネットワークを構成する。
イ　5.8 GHz帯を使用する近距離の無線通信方式であり，有料道路の料金所のETCなどで利用されている。
ウ　下位層にIEEE 802.15.4を使用する低消費電力の無線通信方式であり，センサネットワークやスマートメータなどへの応用が進められている。
エ　広い周波数帯にデータを拡散することで高速な伝送を行う無線通信方式であり，近距離での映像や音楽配信に利用されている。

問1 ウ

解説 **DNS**（Domain Name System）で利用されるデータを，リソースレコード（RR）と呼ぶ。主なリソースレコードの役割は下表のとおりである。

レコード名	説　明
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。
NSレコード （Name Serverレコード）	ドメインの委任を行うときに指定するレコード。例えばxxx.co.jpというドメインを立ち上げたときにco.jpから各種レコードを参照するため，co.jp側にてxxx.co.jpのNSレコードを設定する必要がある。
PTRレコード （逆引きレコード）	IPアドレスからドメイン名を問い合わせるためのレコード。
SOAレコード （Start Of Authorityレコード）	DNSで指定するゾーン（xxx.co.jp）の基本的な設定を行うレコード。シリアル，リフレッシュなどを指定する。
Aレコード （正引きレコード）	ドメイン名からIPアドレスを問い合わせるためのレコード。
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。

ア：SOAレコードの説明である。
イ：MXレコードは，IPアドレスではなくホスト名を指定するレコードである。
エ：Aレコードの説明である。

問2 ウ

解説 **ZigBee**は，ワイヤレスセンサネットワークに利用する，低コスト，低消費電力の無線通信規格である。
ア：**Bluetooth**の説明である。
イ：**DSRC**（Dedicated Short Range Communications：別名スポット通信）の説明である。
エ：**UWB**（Ultra Wide Band）の説明である。

問 3

正解 □ 完璧 □ 直前チェック □

OSI基本参照モデルのトランスポート層の機能として，適切なものはどれか。

ア　経路選択機能や中継機能をもち，透過的なデータ転送を行う。
イ　情報をフレーム化し，伝送誤りを検出するためのビット列を付加する。
ウ　伝送をつかさどる各種通信網の品質の差を補完し，透過的なデータ転送を行う。
エ　ルータにおいてパケット中継処理を行う。

問 4

正解 □ 完璧 □ 直前チェック □

IPv4ネットワークにおけるOSPFの仕様に当てはまるものはどれか。

ア　経路選択に距離ベクトルアルゴリズムを用いる。
イ　異なる自律システム（ルーティングドメイン）間でのルーティング情報交換プロトコルである。
ウ　サブネットマスク情報を伝達する機能があり，可変長サブネットに対応している。
エ　到達可能なネットワークは最大ホップ数15という制限がある。

問 5

正解 □ 完璧 □ 直前チェック □

平均ビット誤り率が1×10^{-5}の回路を用いて，200,000バイトのデータを100バイトずつの電文に分けて送信する。送信電文のうち，誤りが発生する電文の個数は平均して幾つか。

ア　2　　イ　4　　ウ　8　　エ　16

問3　ウ

解説 **OSI基本参照モデル**は，7階層となっており，トランスポート層は4層目の機能である。下表の**PDU**（Protocol Data Unit）は，各層で扱うデータの単位である。例えば，ネットワーク層であれば，「通信量は10パケット」と呼ぶ。

OSI基本参照モデル	PDU	機　器	機　能
第7層　アプリケーション層	メッセージ	ゲートウェイなど	プログラムが扱うデータの単位。例えば電子メールなど。
第6層　プレゼンテーション層			データの表現を管理する。
第5層　セション層			データの交換を管理する。
第4層　トランスポート層	セグメント		TCP，UDPなど通信制御を管理する。
第3層　ネットワーク層	パケット	ルータ，L3スイッチ	通信経路（ルーティング）を管理する。
第2層　データリンク層	フレーム	ブリッジ，L2スイッチ	同一サブネットでの通信を管理する。
第1層　物理層	ビット	リピータ，ハブ	電気的な通信を管理する。

問4　ウ

解説 **OSPF**（Open Shortest Path First）：TCP/IPにおける経路選択（ルーティング）プロトコルの一つ。一般的にルータに設定し，複数のルーティング情報を自動的に更新する。隣接するルータの状態やサブネットマスクを参照して，隣接ルータとやり取りする情報量を少なくしている。

ア：OSPFは，経路選択に**リンクステート型**を用いている。
イ：**BGP**（Border Gateway Protocol）の説明である。
エ：**RIP**（Routing Information Protocol）の説明である。

問5　エ

解説 平均ビット誤り率が1×10^{-5}であるから，誤りの発生するビット数は次のとおりである。

$1 \times 10^{-5} \times 200{,}000 \times 8 = 16$〔ビット〕　（×8は，バイトをビットに変更するため）

全体で16ビットの誤りが発生するため，平均して16電文に誤りが発生する。

問 6 正解 完璧 直前チェック

HDLC手順で用いられるフレーム中のフラグシーケンスの役割として，適切なものはどれか。

ア　受信確認を待たずに複数フレームの送信を可能にする。
イ　フレームの開始と終了を示す。
ウ　フレームの転送順序を制御する。
エ　フレームの伝送誤りを検出する。

問 7 正解 完璧 直前チェック

IPv4におけるICMPのメッセージに関する説明として，適切なものはどれか。

ア　送信元が設定したソースルーティングが失敗した場合は，Echo Replyを返す。
イ　転送されてきたデータグラムを受信したルータが，そのネットワークの最適なルータを送信元に通知して経路の変更を要請するには，Redirectを使用する。
ウ　フラグメントの再組立て中にタイムアウトが発生した場合は，データグラムを破棄してParameter Problemを返す。
エ　ルータでメッセージを転送する際に，受信側のバッファがあふれた場合はTime Exceededを送り，送信ホストに送信を抑制することを促す。

問 8 正解 完璧 直前チェック

マルチキャストグループへの参加や離脱をホストが通知したり，マルチキャストグループに参加しているホストの有無をルータがチェックしたりするときに使用するプロトコルはどれか。

ア　ARP　　イ　IGMP　　ウ　LDAP　　エ　RIP

問6　イ

解説 **HDLC**（High-level Data Link Control）は，OSI基本参照モデルのデータリンク層通信のプロトコルである。データ通信はフレーム単位で行われ，任意のビットパターンを伝送できるビット透過性をもっている。フレームの通信は同期方式で，フラグシーケンス（0111 1110のビット列）によって行われ，フレームの誤り制御は，CRC（Cyclic Redundancy Check）方式となる。

ア，ウ：HDLCの制御部が制御する。

エ：誤り検出は，CRC方式となる。

問7　イ

解説 **ICMP**（Internet Control Message Protocol）とは，IPのエラーメッセージ・制御メッセージを転送するネットワーク層のプロトコルである。

ア：ソースルーティングが失敗したときは，**Destination Unreachable**メッセージを返す。Echo Replyは，Pingでの応答メッセージである。

イ：経路変更要請のメッセージは**Redirect**が適切である。

ウ：**Parameter Problem**は，ICMPのヘッダが解釈できない異常状態になったときのメッセージである。

エ：**Time Exceeded**は，許容可能なルータ数を超えたときに発生する。

問8　イ

解説

ARP（Address Resolution Protocol）：IPアドレスからイーサネットアドレス（MACアドレス）を得るプロトコルである。

IGMP（Internet Group Management Protocol）：マルチキャストにおいて，ホストのグループ制御に利用されるプロトコルである。

LDAP（Lightweight Directory Access Protocol）：ディレクトリサービス（ファイルやプリンタなどネットワーク上の資源の位置や名前などを検索するサービス）の一つで，インターネット向けに簡素化されたもの。

RIP（Routing Information Protocol）：パケットが到達する経路の最小ルートを選択するダイナミックルーティングプロトコルである。ルータを1台経由するごとに1ホップだけカウントアップする。最大数は15ホップ。16ホップ目でパケットは破棄される。RIPはホップ数のみをカウントしているため，経路中の回線速度（コスト）や遅延，均一化は考慮されない。

問 9 正解 完璧 直前チェック

IPv6においてIPv4から仕様変更された内容の説明として，適切なものはどれか。

ア　IPヘッダのTOSフィールドを使用し，特定のクラスのパケットに対する資源予約ができるようになった。
イ　IPヘッダのアドレス空間が，32ビットから64ビットに拡張されている。
ウ　IPヘッダのチェックサムフィールドを追加し，誤り検出機能を強化している。
エ　IPレベルのセキュリティ機能（IPsec）である認証と改ざん検出機能のサポートが必須となり，パケットを暗号化したり送信元を認証したりすることができる。

問 10 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　IPネットワークにおいて，ホスト間通信の伝送帯域を管理するためのプロトコルである。
イ　LANシステムにおいて，物理的なケーブルやノードの接続形態に依存せず，ノードを任意に論理的なグループに分ける技術である。
ウ　PPPによるデータリンクを複数束ねることができるように拡張したプロトコルである。
エ　リモートアクセスを利用する利用者の認証を行うためのプロトコルである。

問 11 正解 完璧 直前チェック

UDPを使用するプロトコルはどれか。

ア　DHCP　　イ　FTP　　ウ　HTTP　　エ　SMTP

問9　エ

解説

ア：**IPv4**の**TOS**（Type Of Service）**フィールド**は，転送優先順位を指定する。IPv6にはTOSフィールドはないが，**Traffic Class フィールド**が同じ機能を果たしている。
イ：**IPv6**では，IPヘッダのアドレス空間が32ビットから128ビットに拡張された。
ウ：IPv4の**Header Checksum フィールド**はIPv6にはない。
エ：**IPsec**機能を標準実装することで，認証と改ざん検出，暗号化機能が利用可能となる。

問10　ア

解説　**RSVP**（Resource reSerVation Protocol）は，ネットワークの帯域制御用のプロトコルである。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。
イ：**VLAN**（Virtual LAN）の説明である。
ウ：**MP**（Multilink Protocol）の説明である。
エ：**PPP**（Point to Point Protocol）の説明である。

問11　ア

解説

DHCP（Dynamic Host Configuration Protocol）：IPアドレスなど各種設定の自動割当てを行うプロトコルである。ほかに設定できる項目として，デフォルトゲートウェイ，サブネットマスク，DNSサーバなどがある。一般的にダイヤルアップ，ADSL，ISDNなどプロバイダと接続する際に利用される。**UDP**を利用した通信である。
FTP（File Transfer Protocol）：TCP/IPネットワークでファイルの転送時に使われるプロトコルであり，IETFによってRFC 959で定義されている。**TCP**を利用した通信となる。
HTTP（Hypertext Transfer Protocol）：インターネットにおいて，WWWサーバとクライアントの間でHTML文書を送受信するためのプロトコル。TCPを利用した通信である。
SMTP（Simple Mail Transfer Protocol）：電子メールの送受信用プロトコル。サーバ対サーバ間のメール転送に利用される。TCPを利用した通信である。

問 12 正解 □ 完璧 □ 直前チェック □

IPネットワークにおいて，クライアントの設定を変えることなくデフォルトゲートウェイの障害を回避するために用いられるプロトコルはどれか。

ア RARP　　イ RSTP　　ウ RTSP　　エ VRRP

問 13 正解 □ 完璧 □ 直前チェック □

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

解説

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である。**ARP**の逆の機能となる。

RSTP（Rapid Spanning Tree Protocol）：ネットワークの冗長化方式の**STP**（Spanning Tree Protocol）よりも高速に冗長化が切り替わる方式となる。STPの冗長化切り替えは約30秒となるが，RSTPは約1秒で切り替わるのが特徴である。

RTSP（Real Time Streaming Protocol）：リアルタイムでデータをストリーミング配信するためのプロトコルである。

VRRP（Virtual Router Redundancy Protocol）：ルータやゲートウェイの多重化を行うためのプロトコル。デフォルトゲートウェイを冗長化することができるため，障害時にクライアントは，冗長化された片系でアクセスでき，設定を変えることなく通信を継続できる。

問13 イ

解説 サブネットマスクから，ホストアドレスを求める。設問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，下表となる。

サブネットマスク	255.	255.	255.	224
2進数表記	1111 1111.	1111 1111.	1111 1111.	**1110 0000**
ホストのIPアドレス	212.	62.	31.	90
2進数表記	1101 0100.	0011 1110.	0000 1111.	0101 **1010**

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ビットで示されるため，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 14

正解 □ 完璧 □ 直前チェック □

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のネットワーク番号とサブネットマスクの組合せとして，適切なものはどれか。

	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 □ 直前チェック □

IP電話の音声品質を表す指標のうち，ノイズ，エコー，遅延などから算出されるものはどれか。

ア　MOS値　　イ　R値　　ウ　ジッタ　　エ　パケット損失率

問14　イ

解説 **CIDR**（Classless Inter-Domain Routing）：サブネットマスクの上位から数えて1になっているビット数をクラスA，B，C，Dといい，各クラスをサブネットに分割して利用できる形にしたものである。

スーパーネット化とは，連続したネットワークをまとめて一つのネットワークで表すことである。ルータに設定する場合，ルーティングテーブルが少なくなるため負荷軽減などの目的で用いられる。

選択肢から，ネットワーク番号32および35とサブネットマスクの組合せを見ると，35の場合は32のネットワークを含まないことがわかる。そのため，選択肢ウ，エは誤りとなる。残りの選択肢ア，イでは，アはイだけを含むが，イは32から35全てのネットワークを含むため，適切な解答はイとなる。

	10進数	2進数
ア	32	**0010 0**000
	248	**1111 1**000
イ	32	**0010 0**000
	252	**1111 1**100
ウ	35	**0010 0**011
	248	**1111 1**000
エ	35	**0010 0**011
	252	**1111 1**100

問15　イ

解説 **IP電話**は，**VoIP**（Voice over IP）を用いてインターネットなどのIPネットワークを利用して音声を送る技術である。

MOS値：電話の音声品質を評価するための手法。人間の耳で主観的に確認し，5段階で評価する。

R値：電話の音声品質を評価する手法。ノイズ，エコー，遅延，音量などのデーを入力して計算を行い，客観的に評価する。

ジッタ：受信パケットのばらつきによって発生する音声のずれや揺らぎである。

パケット損失率：パケットがあて先に届かない場合や，破損して通信路の途中で失われること。

問 16

正解 □ 完璧 □ 直前チェック □

送信者Aが，受信者Bと共有している鍵を用いて，メッセージからメッセージ認証符号を生成し，そのメッセージ認証符号とメッセージを受信者Bに送信する。このとき，メッセージとメッセージ認証符号を用いて，受信者Bができることはどれか。

ア　通信路上でのメッセージの伝送誤りを訂正できる。
イ　通信路上でのメッセージの複製の有無を検知できる。
ウ　メッセージの改ざんがないことを判定できる。
エ　メッセージの盗聴の有無を検知できる。

問 17

正解 □ 完璧 □ 直前チェック □

無線LANにおけるWPA2の特徴はどれか。

ア　AHとESPの機能によって認証と暗号化を実現する。
イ　暗号化アルゴリズムにAESを採用したCCMP（Counter-mode with CBC-MAC Protocol）を使用する。
ウ　端末とアクセスポイントの間で通信を行う際に，TLS Handshake Protocolを使用して，互いが正当な相手かどうかを認証する。
エ　利用者が設定する秘密鍵と，製品で生成するIV（Initialization Vector）とを連結した数を基に，データをフレームごとにRC4で暗号化する。

問16　ウ

解説　**メッセージ認証符号**は，送信するメッセージをハッシュ関数によって，送信前と送信後のメッセージが同一であることを証明するための仕組みである。メッセージの改ざんを判定することができる。

ア：メッセージが変更されたかは確認できるが，途中で変更された内容を訂正することはできない。
イ：メッセージが複製されても検知することはできない。
エ：メッセージの盗聴を検知することはできない。

問17　イ

解説

WPA2（Wi-Fi Protected Access 2）：AES（Advanced Encryption Standard）を採用した**CCMP**暗号化方式を採用している。無線の暗号化は，WEPがセキュリティ的に脆弱（ぜい）だということでWPAが作られ，さらに強力なWPA2が作られた。日々の技術進歩により，暗号が解読される速度が速くなっているため，より強力な暗号技術が必要となっている。

WPA（Wi-Fi Protected Access）：WEPで存在したセキュリティ面での脆弱点を補強し，強化したもの。

AES（Advanced Encryption Standard）：共通鍵暗号方式のブロック暗号であり，DESの後継規格となった米国政府標準暗号である。鍵長は128ビット，192ビット，256ビットの3種から選択できる。

ア：**IPsec**（Security Architecture for Internet Protocol）の説明である。
ウ：WPA2では，AESを利用するため，TLSを利用していない。
エ：**WEP**（Wired Equivalent Privacy）の説明である。

問 18 正解 完璧 直前チェック

プロキシサーバ又はリバースプロキシサーバを新たにDMZに導入するセキュリティ強化策のうち，導入によるセキュリティ上の効果が最も高いものはどれか。

ア　DMZ上の公開用Webサーバとしてリバースプロキシサーバを設置し，その参照先のWebサーバを，外部からアクセスできない別のDMZに移設することによって，外部のPCとの通信におけるインターネット上での盗聴を防ぐ。

イ　DMZ上の公開用Webサーバとしてリバースプロキシサーバを設置し，その参照先のWebサーバを，外部からアクセスできない別のDMZに移設することによって，外部から直接Webサーバのコンテンツが改ざんされることを防ぐ。

ウ　社内PCからインターネット上のWebサーバにアクセスするときの中継サーバとしてプロキシサーバをDMZに設置することによって，参照先のWebサーバと社内PC間の通信におけるインターネット上での盗聴を防ぐ。

エ　社内PCからインターネット上のWebサーバにアクセスするときの中継サーバとしてプロキシサーバをDMZに設置することによって，参照するコンテンツのインターネット上での改ざんを防ぐ。

問 19 正解 完璧 直前チェック

インターネットサービスプロバイダ（ISP）が，OP25Bを導入することで得られるセキュリティ上の効果はどれか。

ア　ISP管理下のネットワークからISP管理外のネットワークに対するICMPパケットによるDDoS攻撃を遮断できる。

イ　ISP管理下のネットワークからISP管理外のネットワークに向けて送信されるスパムメールを制限できる。

ウ　ISP管理下のネットワークに対するISP管理外のネットワークからのICMPパケットによるDDoS攻撃を遮断できる。

エ　ISP管理下のネットワークに向けてISP管理外のネットワークから送信されるスパムメールを制限できる。

問18　イ

解説

プロキシサーバ：内部ネットワークから外部ネットワークへのアクセスを中継するサーバである。

リバースプロキシサーバ：外部ネットワークから内部ネットワークへのアクセスを中継する。プロキシサーバと逆の役割となる。

DMZ（DeMilitarized Zone）：ファイアウォールによってネットワーク上に隔離された区画を作り，外部とのアクセスの中継となるサーバ（リバースプロキシサーバ）を配置する。

ア，ウ：外部や内部のPCの通信の盗聴は，プロキシサーバをどのように変更しても防ぐことができない。通信を暗号化するなどの盗聴対策が必要となる。

イ：公開用WebサーバをDMZに配置し，実データは外部からアクセスできない場所に配置することで外部からのWebデータ改ざんを防止することができる。

エ：DMZに配置したプロキシサーバには，インターネット上のコンテンツ改ざんを防ぐ機能はない。

問19　イ

解説　**OP25B**（Outbound Port 25 Blocking）は，内部ネットワークから外部ネットワークへのポート25番の通信（SMTP）を遮断する手法である。例えば，ISPがOP25Bを用いることで，会員がISPの外部ネットワークに存在するメールサーバを使用してスパムメールを送信しようとすることを防止することが可能となる。

ア，ウ：OP25Bはメール送信のブロックに利用されるため，ICMPによるDDoS攻撃は遮断できない。

エ：ISP管理外のネットワークから，ISP管理下のネットワーク内部に向けて送信されたスパムメールは，制限できない。

問 20 正解 □ 完璧 □ 直前チェック □

Webアプリケーションの脆弱性を悪用する攻撃手法のうち，Webページ上で入力した文字列がPerlのsystem関数やPHPのexec関数などに渡されることを利用し，不正にシェルスクリプトや実行形式のファイルを実行させるものは，どれに分類されるか。

ア　HTTPヘッダインジェクション
イ　OSコマンドインジェクション
ウ　クロスサイトリクエストフォージェリ
エ　セッションハイジャック

問 21 正解 □ 完璧 □ 直前チェック □

TLSに関する記述のうち，適切なものはどれか。

ア　TLSで使用するWebサーバのディジタル証明書にはIPアドレスの組込みが必須なので，WebサーバのIPアドレスを変更する場合は，ディジタル証明書を再度取得する必要がある。
イ　TLSで使用する個人認証用のディジタル証明書は，ICカードなどに格納できるので，格納場所を特定のPCに限定する必要はない。
ウ　TLSはWebサーバを経由した特定の利用者間の通信のために開発されたプロトコルであり，Webサーバ提供者への事前の利用者登録が不可欠である。
エ　日本国内では，TLSで使用する共通鍵の長さは，128ビット未満に制限されている。

問20　イ

解説

HTTPヘッダインジェクション：動的にHTTPヘッダが生成されるHTTP通信の機能を利用した攻撃手法。HTTPヘッダに改行コードを生成させることで不正な動作を実行させる。

OSコマンドインジェクション：サーバ内のOSコマンドを外部から実行させることで，サーバに不正な動作を実行させる攻撃手法。

クロスサイトリクエストフォージェリ：Webサイトに埋め込まれているスクリプトや命令が，利用者がそのWebサイトにアクセスすることによって自動的に実行させられてしまう攻撃手法。掲示板への書き込みやオンラインショップでの買い物などが，意図せずに行われてしまう。

セッションハイジャック：セッションIDを盗み出すことでセッションを乗っ取り，あたかもそのセッションの参加者であることを装う攻撃手法。セッションの参加者でなければ見ることのできない情報を盗み出すことができる。

問21　イ

解説　**TLS**（Transport Layer Security）とは，OSI基本参照モデル第4層のトランスポート層に基づいてディジタル証明書による認証を行う認証手順である。SSLを元に作られたプロトコルである。

ア：ディジタル証明書には，IPアドレスの組込みは必須ではない。
ウ：SSLを元に作られたプロトコルであり，不特定多数の利用者間の通信で利用される。
エ：共通鍵の長さは，256ビットを利用することができる。

問 22 正解 □ 完璧 □ 直前チェック □

パリティ専用の磁気ディスク装置をもち，ブロック単位のストライピングを行うRAIDの方式はどれか。

ア　RAID1　　イ　RAID3　　ウ　RAID4　　エ　RAID5

問 23 正解 □ 完璧 □ 直前チェック □

マルチプロセッサによる並列処理において，1プロセッサのときに対する性能向上比はアムダールの法則で説明することができる。性能向上比に関する記述のうち，適切なものはどれか。

〔アムダールの法則〕

$$性能向上比 = \frac{1}{(1 - 並列化可能部の割合) + \dfrac{並列化可能部の割合}{プロセッサ数}}$$

ア　プロセッサ数が一定の場合，性能向上比は並列化可能部の割合に比例する。
イ　プロセッサ数を増やした場合，性能向上比は並列化可能部の割合に反比例する。
ウ　並列化可能部の割合が0.5の場合は，プロセッサ数をいくら増やしても性能向上比が2を超えることはない。
エ　並列化可能部の割合が最低0.9以上であれば，性能向上比はプロセッサ数の半分以上の値となる。

問22　ウ

解説　**RAID**（Redundant Array of Independent Disks：ディスクアレイ構成方式）は，複数台のハードディスクを並列に接続し，全体を一つのディスク装置のように制御することで，高速かつ信頼性の高い外部記憶装置を実現するものである。

RAID0：別名ストライピングという。2台以上のハードディスクを連結することによって，その合計容量をもつ仮想的な1台のハードディスクドライブとして使用できる。

RAID1：別名ミラーリングという。2台以上のハードディスクに同じデータを書き込むことによって，データの可用性を高める。

RAID2：エラー修復用のパリティ情報を，元データとともに複数ディスクに格納する。この方式は，他の方式よりも容量が増加することで利用効率が悪く，現在ではほとんど利用されていない。

RAID4：分割したデータと誤り訂正のためのパリティ情報を，パリティ専用HDDに書き込むことによって，データの可用性を高め，かつ，書込み動作を高速化する。

RAID5：分割したデータと誤り訂正のためのパリティ情報を3台以上のハードディスクに分散して書き込むことによって，データの可用性を高め，かつ，書込み動作を高速化する。

問23　ウ

解説　**アムダールの法則**は，プログラムやCPUのマルチコア化という並列化によって速度の向上が見込まれるが，逐次実行するしかない部分に，全体の実行時間が制約されることを提唱した理論である。

ア：プロセッサ数が1のとき，並列化可能部の割合が大きくなっても分母は1のままであるから，性能向上比は比例しない。

イ：プロセッサ数を極限まで増やすと，分母は「1－並列化可能部の割合」に収束する。ここで並列化可能部の割合を大きくすると分母が小さくなるので，性能向上比が大きくなる。したがって，並列化可能部の割合と性能向上比は比例関係となる。

　性能向上比が2になるためには，（並列化可能部／プロセッサ数）が0にならなければならない。割り算の計算上0になり得ないため，正しいということになる。

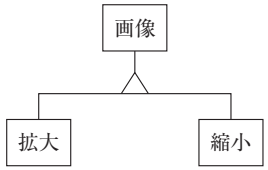
ウ：並列化可能部の割合が0.5のとき，プロセッサ数を極大まで大きくすると，分母は1－並列化可能部の割合＝0.5となる。したがって，性能向上比は2を超えることはない。

エ：並列化可能部の割合を1とすると，性能向上比はプロセッサ数と同じ値となる。並列化可能部の割合を0.9としてプロセッサ数を極大まで大きくすると，分母は0.1に収束する。このとき性能向上比は10となる。プロセッサ数が極大であるから，性能向上比はプロセッサ数の半分以下となる。

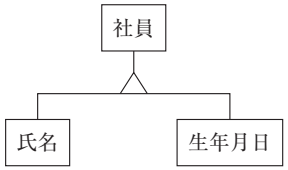
問 24 正解 完璧 直前チェック

オブジェクト間のis-a関係を表す図はどれか。

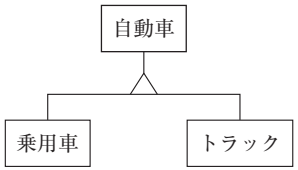
ア



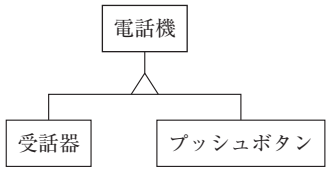
イ



ウ



エ



問 25 正解 完璧 直前チェック

SOA（Service Oriented Architecture）でサービスを設計する際の注意点のうち，適切なものはどれか。

ア　可用性を高めるために，ステートフルなインタフェースとする。
イ　業務からの独立性を確保するために，サービスの命名は役割を表すものとする。
ウ　業務の変化に対応しやすくするために，サービス間の関係は疎結合にする。
エ　セキュリティを高めるために，一度開発したサービスは再利用しない方がよい。

問24　ウ

解説 **is-a関係**とは，継承関係のことである。is-a関係にある場合，オブジェクトは上位のオブジェクトの一種といえる。選択肢ウの乗用車，トラックは自動車の一種である。ほかの選択肢は一種ではない。

問25　ウ

解説 SOA（サービス指向アーキテクチャ）には，設問では言及されていないが，「サービスは適切な粒度（オペレーションの数）を有すべき」「オペレーションは並行性を考慮して設計すべき」といった幾つもの原則がある。

ア：再利用を考慮して**ステートレス**なインターフェースとすべきである。業務の変化への対応を考慮して，**ステートフル**（状態と相互関係を重視する）インターフェースにはしない。

イ：サービスの命名はビジネス概念を表すものとする。サービス名には名詞，オペレーションには動詞がよいとされている。

エ：SOAにおいては，サービスを再利用することにより，効率や利便性を得ることができる。