平成27年度 秋期 午前Ⅱ問題の解答・解説

□問 1	ウ	□問 11	ア	□問 21	イ
□問 2	ウ	□問 12	エ	□問 22	ウ
□問 3	ウ	□問 13	イ	□問 23	ウ
□問 4	ウ	□問 14	イ	□問 24	ウ
□問 5	エ	□問 15	イ	□問 25	ウ
□問 6	イ	□問 16	ウ		
□問 7	イ	□問 17	イ		
□問 8	イ	□問 18	イ		
□問 9	エ	□問 19	イ		
□問 10	ア	□問 20	イ		

問 1：正解ウ

ア：CNAME（Canonical NAME）レコードは，外部に公開するホスト名（別名）に対応するサーバ名（正式名）を指定するレコードである。

イ：MX（Mail eXchange）レコードは，ドメイン宛ての電子メールの送り先となるメールサーバのホスト名を指定するレコードである。

ウ：**正解**。NS（Name Server）レコードは，ゾーン自身や下位ドメインに対する権威をもつ DNS サーバ（プライマリ DNS サーバ，セカンダリ DNS サーバ）を指定するレコードである。

エ：PTR（PoinTeR）レコードは，IP アドレスに対応するホスト名を指定するレコードである。

問 2：正解ウ

ZigBee（IEEE802.15.4）とは，短距離無線通信の規格である。使用周波数帯域は（日本国内では）2.4GHz 帯の ISM バンドである。伝送速度は低く通信距離も短いが，安価で省電力であるという長所をもつ。ZigBee 端末は転送機能を有し，直接電波の届かない端末間でも通信できる。ZigBee 端末は多数の端末と通信でき，大規模なメッシュ状のトポロジを形成できる。安価で省電力であるという特性を生かし，ビル内のセンサネットワークなど低速通信に用いられている。よって，正解は選択肢**ウ**となる。

ア：Bluetooth（IEEE802.15.1）について記述したものである。使用周波数帯域は 2.4GHz 帯の ISM バンド，通信距離は数 m ～数十 m 程度，Bluetooth 3.0 の最大伝送速度は 24Mbps である。近距離での携帯端末同士の通信に用いられている。

イ：路車間・車車間通信の規格である DSRC（Dedicated Short Range Communications）について記述したものである。使用周波数帯域は 5.8GHz 帯の ISM バンド，通信距離は数 m ～数十 m 程度である。車両有料道路における ETC を用いた料金徴収，VICS（道路交通情報通信システム）対応のカーナビゲーション搭載車両への情報配信などに用いられている。

エ：UWB（Ultra Wide Band）について記述したものである。数百 MHz ～ 1GHz 超の広い周波数帯にデータを拡散することで高速な伝送を実現する。ノイズに強い，位置検出の精度が高いなどの長所をもつが，通信距離が長くなると伝送速度が落ちるという短所もある。前述の特性を生かし，近距離での映像配信といった応用が検討されている。

問 3：正解ウ

OSI 基本参照モデルのトランスポート層は，通信品質を確保するためのエラー訂正や再送制御の機能を備え，エンドシステム間で信頼性の高いデータ転送を行う。

ア：経路選択機能や中継機能をもつのはネットワーク層である。

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」という記述に最も当てはまるのは，データリンク層である。

データリンク層は，各通信網の MTU（Max Transfer Unit：最大転送長）に合わせて「情報をフレーム化」する。ネットワーク層，トランスポート層も「情報をパケット化」しているが，各種通信網を流れるフレームのサイズは，データリンク層の MTU を超えることがない。MTU を超えるとフレームを分割して転送するので，不要な分割を回避するため（不要なヘッダ付加を回避するため），上位層プロトコルの中には，MTU に合わせてパケット化するものがある（例：TCP/IP）。データリンク層は，フレームサイズを最終的に決定する役割を果たしていることを考慮に入れるなら，「情報をフレーム化（する）」という記述に最も当てはまるのは，データリンク層であると言えよう。

データリンク層の多くのプロトコルは，伝送誤りを検出するためのビット列を，フレームの末尾に付加している。これをトレーラという（例：イーサネットフレームの FCS）。ネットワーク層の IP，トランスポート層の TCP，UDP も，伝送誤りを検出するためのビット列をフィールドにもっている。とはいえ，そのようなビット列を「付加する」という表現は，フィールドにもつ上位層よりも，それをトレーラとしてもつデータリンク層によりいっそう当てはまると言えよう。

ウ：**正解**。選択肢に，「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」と記述されているとおり，経路上の各種通信網の品質の差をトランスポート層の機能で補完することができる。それゆえ，エンドシステム内のアプリケーションの見地に立つと，トランスポート層の働きにより，あたかも高品質な経路があるかのように見える。問題文は，そのことを「透過的」（経路上の各種通信網には品質の差が存在しているが，それが存在していないかのように見える）と表現している。

エ：「パケット中継処理を行う」とあるので，中継機能をもつのはネットワーク層である。

問 4：正解ウ

OSPF（Open Shortest Path Fast）は，リンクステート型のダイナミックルーティングプロトコルである。OSPF の主な特徴は，

① 自律システム内で使用する
② ネットワークを複数のエリアに分割できる。その場合，一つのエリアをバックボーンエリアとし，残り全てのエリアをバックボーンエリアに接続する形態をとる
③ 最小のパスコストで到達できる経路を選択する
④ 可変長サブネットマスクに対応する

などがある。

ア：OSPF の経路選択はリンクステート型である。距離ベクタ型のアルゴリズムを用いるルーティングプロトコルの例として，RIP がある。
イ：①にあるとおり，OSPF は自律システム内で使用されるルーティングプロトコルである。異なる自律システム間で使用されるルーティングプロトコルの例として，BGP がある。
ウ：**正解**。④にあるとおり，可変長サブネットに対応している。
エ：OSPF は，到達可能なネットワークのホップ数に関する制限がない。到達可能なネットワークのホップ数が最大 15 であるルーティングプロトコルは，RIP である。

問 5：正解エ

平均ビット誤り率が 1×10^{-5} の回線で，200,000 バイトのデータを送信するときに発生するビット誤りの数は，

$$1 \times 10^{-5} \times 200{,}000 \times 8 = 16$$

である。つまり，これだけの数のビット誤りが電文の中にランダムに入り込むことになる。平均ビット誤り率の値は 1×10^{-5} と極めて小さいため，一つの電文に発生するビット誤りの数をたかだか 1 個と仮定してよい。したがって，16 個の電文に誤りが発生することになる。

よって，正解は選択肢**エ**である。

問 6：正解イ

HDLC（High-level Data Link Control）は，OSI 基本参照モデルのデータリンク層に位置するプロトコルであり，ビット単位でのデータ転送が可能である。

HDLC のフレームフォーマットを次の図に示す。

名称	内容
F（フラグシーケンス）	フレームの開始と終了
A（アドレスフィールド）	送信元，宛先のアドレス
C（制御フィールド）	フレームの種類，フレームの番号
I（情報フィールド）	転送するデータ
FCS（Frame Check Sequence）	CRC を用いた誤り検出

したがって，フラグシーケンスの役割は，選択肢イにあるとおり，「フレームの開始と終了を示す」となる。よって，正解は選択肢**イ**である。

問 7：正解イ

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，宛先到達不能メッセージ（Destination unreachable Message：ICMP メッセージタイプ 3）のソースルート失敗（Source Route Failed：コード 5）を返す。

イ：**正解**。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，リダイレクトメッセージ（Redirect Message：ICMP メッセージタイプ 5）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，フラグメントの再組立て中に時間が超過したことを示すメッセージ（Fragment Reassembly Time Exceeded：ICMP メッセージタイプ 11）を返す。

エ：ルータでメッセージを転送する際，受信側のバッファがあふれた場合は，送信元抑制メッセージ（Source Quench Message：ICMP メッセージタイプ 4）を返す。送信元ホストは，送信元抑制メッセージを受け取ると送信レートを落とす。やがて，ホストは送信レートを徐々に上げていくが，送信元抑制メッセージを再び受け取る

と送信レートを落とす。これが何度か繰り返されるうちに，送信元ホストの送信レートと，ルータや宛先ホストがバッファを処理できる速度とが平衡状態に至り，フロー制御が成し遂げられる。

問 8：正解イ

IGMP（Internet Group Management Protocol）は，IP ネットワークでマルチキャスト通信を行うために，ルータとホストが使用するプロトコルである。ホストは，マルチキャストグループへの参加や離脱を通知するために，IGMP メッセージを送信する。ルータは，マルチキャストグループに参加しているホストの存否を定期的に（デフォルトで 60 秒間隔）でチェックするために使用する。よって，正解は選択肢**イ**となる。

ア：ARP（Address Resolution Protocol）は，IP アドレスから MAC アドレスを取得するために用いるプロトコルである。

ウ：LDAP（Lightweight Directory Access Protocol）は，ITU-T 勧告である X.500 を簡略化して RFC2251 で規定された，ディレクトリサービスを実現するプロトコルである。ディレクトリサービスとは，資源とその属性を登録し検索できるようにしたシステムである。

エ：RIP（Routing Information Protocol）は，距離ベクタ型のダイナミックルーティングプロトコルである。

問 9：正解エ

ア：IPv6 では TOS フィールドが廃止された。通信の優先制御を実現するため，TOS フィールドに代わって，新たにトラフィッククラスが規格化された。とはいえ，選択肢に記述された「特定のクラスのパケットに対する資源予約」を行えるわけではない。

イ：IPv6 は，アドレス空間が 128 ビットに拡張された。

ウ：IPv6 ではチェックサムフィールドが廃止されており，ルータがチェックサムを計算する負荷が軽減されている。

エ：**正解**。IPv6 では「次ヘッダ」が規格化され，IPv6 の機能拡張を行うことができる。次ヘッダの一つに IPsec のセキュリティプロトコル（AH, ESP）があるので，パケットの暗号化，メッセージ認証（改ざんの検出），送信元ノードの認証など，IP レベルのセキュリティ機能を実現することができる。

問 10：正解ア

ア：**正解**。RSVP（Resource reSerVation Protocol）について適切に説明している。
イ：VLAN（Virtual LAN）に当てはまる記述である。
ウ：マルチリンク PPP に当てはまる記述である。
エ：RADIUS（Remote Authentication Dial In User Service）に当てはまる記述である。

問 11：正解ア

選択肢のうち，トランスポート層に UDP を使用するプロトコルは，選択肢**ア**の DHCP である。それ以外の選択肢にあるプロトコルは，いずれも TCP を使用する。

問 12：正解エ

VRRP（Virtual Router Redundancy Protocol）とは，ルータを冗長化させるためのプロトコルである。VRRP を利用すれば，同一サブネット内に存在する複数台のルータをグループ化し，1 台の仮想ルータが存在しているかのように見せかけることができる。

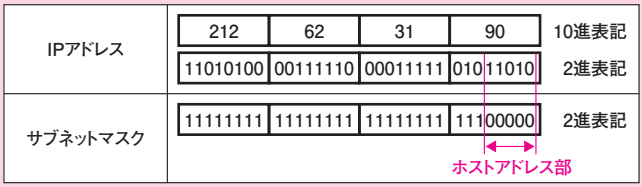
VRRP を使用する際，この仮想ルータがもつ IP アドレス（仮想 IP アドレス）をクライアントのデフォルトゲートウェイとして設定する。仮想ルータのグループを構成する実ルータのうち 1 台以上が稼働していれば，デフォルトゲートウェイとなるルータが存在しているので，ルータの障害の影響を回避することができる。

よって，正解は選択肢**エ**である。

ア：RARP（Reverse Address Resolution Protocol）とは，外部記憶装置をもたない装置が，RARP サーバから自装置の IP アドレスを取得するために用いるプロトコルである。
イ：RSTP（Rapid Spanning Tree Protocol）とは，同一ブロードキャストドメイン内のスイッチ間でやり取りし，スパニングツリーアルゴリズムに基づき，一部のスイッチの特定ポートを論理的にブロックする機能をもつプロトコルである。同じくスパニングツリーアルゴリズムを用いる STP を改良し，障害発生時の切替え時間を短くしたプロトコルであり，IEEE802.1D-2004 規格（旧 IEEE802.1w 規格）で標準化されている。
ウ：RTSP（Real Time Streaming Protocol）とは，リアルタイムにストリーミングを実現するためのプロトコルである。ストリーム配信を行うサーバに際し，クライアントが再生，停止，記録などの操作をリクエストする仕組みを備えている。

問 13：正解イ

ホストの IP アドレスが 212.62.31.90，サブネットマスクが 255.255.255.224 なので，ホストアドレス部は下位 5 ビットとなる。

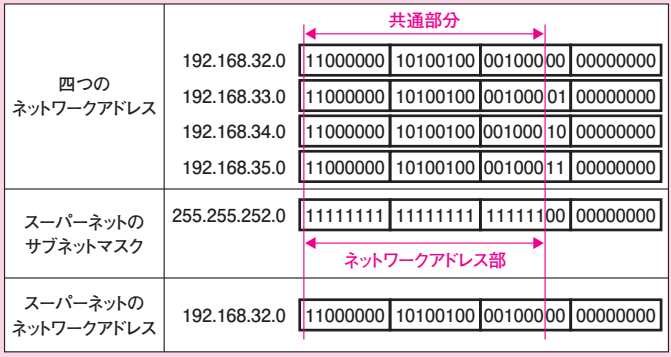


図：IP アドレスとサブネットマスクの対応

したがって，ホストアドレス部（下位 5 ビット）の値は，2 進表記で「11010」となり，10 進表記では「26」となる。よって，正解は選択肢**イ**である。

問 14：正解イ

問題文にある四つのネットワークのネットワークアドレスは，最上位ビットから上位 22 ビット目（第 3 オクテットの上位 6 ビット目）までが共通の値をもつ。



図：CIDR でスーパーネット化した場合の対応

CIDR を使ってスーパーネット化した場合，この共通部分がネットワークアドレス部となる。

したがって，サブネットマスクは 255.255.252.0 となり，ネットワークアドレスは 192.168.32.0 となる。よって，正解は選択肢**イ**である。

問 15：正解イ

ア：MOS 値とは，通話品質を評価する指標の一つである。R 値とは異なり人間の耳を用いるため，ユーザの体感品質をより反映した指標となり得る。複数の被験者が受話器越しに聞いた音声の品質を 5 段階で評価し，その平均を MOS 値とする。

イ：**正解**。R 値に当てはまる記述である。

ウ：ジッタ（揺らぎ）とは，音声パケットを受信する際，パケットごとに遅延時間が異なっていることをいう。パケットを受信する間隔がばらついているため，ノイズや音飛びなど，音声品質劣化の要因となる。

エ：パケット損失率とは，送信したパケット数のうち，パケット損失により受信できなかったパケット数の割合である。パケット損失は，音切れや音飛びなど，音声品質劣化の要因となる。

問 16：正解ウ

問題文に記述された手順を整理すると，次のようになる。

（準備）

送信者 A と送信者 B は，鍵を共有する（以下，この鍵を「共有鍵」と称する）

（メッセージの転送）

1. 送信者 A は，メッセージを作成する。以下，このメッセージを M1 と称する。
2. 送信者 A は共有鍵を用いて，メッセージからメッセージ認証符号を生成する。
3. 送信者 A は，メッセージとメッセージ認証符号を受信者 B に送信する。
4. 受信者 B は，メッセージとメッセージ認証符号を受信する。

本問は，このメッセージとメッセージ認証符号を用いて受信者 B が行えることを，選択肢の中から選ぶよう求めている。選択肢を一つずつ確かめていけば，解を導くことができる。

説明を分かりやすくするため，まず，正解である選択肢ウから解説する。

次の手順に従えば，受信者 B は，メッセージの改ざんがないことを判定することができる（前の手順に続いて付番する）。

5. 受信者 B は共有鍵を用いて，メッセージ認証符号を復号し，メッセージを復元する。以下，復元したメッセージを M2 と称する。
6. 受信者 B は，受信したメッセージ M1 と，復元したメッセージ M2 が一致するかどうかを確認する。一致していれば，M1 は改ざんされていない。

共有鍵が第三者に秘匿されているため，第三者はメッセージ認証符号を復号することができない。それゆえ，第三者は，メッセージ M1 を改ざんするとともに，その改ざんした内容と整合するようにメッセージ認証符号を変更することができない。

したがって，第三者がメッセージの改ざんをしても，手順 6 で検出されてしまう。

よって，正解は選択肢**ウ**となる。

これ以外の選択肢には次のような誤りがある。

ア：ハミング符号等の誤り訂正アルゴリズムを用いない限り，伝送誤りが生じたビットを訂正することはできない。なお，伝送誤りがあれば，前述の手順 6 において，受信したメッセージ M1 と復元したメッセージ M2 は一致しない。したがって，伝送誤りが生じたことを検出することまでは行える。

イ：ディジタル放送のコンテンツのようなコピーガードの仕組みを備えたデータ（及び，専用の再生装置）を用いれば，コピーワンス（1 回だけ複製可能）やダビング 10 等の高度な複製制御を実現できる。問題文にはその種の技術を使用している旨の記述がないので，複製の有無を検知することはできない。

エ：メッセージは暗号化されていないので，盗聴を防ぐことができないし，盗聴の有無を検知することもできない。

問 17：正解イ

ア：IPsec に当てはまる記述である。

イ：**正解**。WPA2 に当てはまる記述である。

ウ：SSL に当てはまる記述である。

エ：WEP に当てはまる記述である。

問 18：正解イ

リバースプロキシサーバは，コンテンツ改ざんを防ぐ効果がある。

その効果を得るには，選択肢イに記述された方法でサーバを設置する必要がある。

サーバ	設置方法（選択肢イの引用）
リバースプロキシサーバ	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（する）
Web サーバ	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

選択肢イには，リバースプロキシサーバの設置方法が簡潔に記されているので，補足しておこう。要するに，「DMZ 上にリバースプロキシサーバを設置する。そして，公開 Web サーバのホスト名とリバースプロキシサーバの IP アドレスを対応付けて DNS サーバに登録し，外部に公開する」ということである。

この結果，外部のクライアントが公開 Web サーバにアクセスするとき，実際には，外部クライアントはリバースプロキシサーバに接続する。そして，リバースプロキシサーバはそのアクセスを公開 Web サーバに中継する。外部クライアントからは，公開 Web サーバに直接アクセスできなくなる。

悪意あるクライアントが公開 Web サーバのコンテンツ改ざんを試みても，実際に接続しているのはリバースプロキシサーバである。サーバの脆弱性をつく攻撃を受けたとしても，リバースプロキシサーバ自体にはコンテンツがないので，改ざんのしようがない。

ただし，リバースプロキシサーバから公開 Web サーバに中継する通信の内容に脆弱性があるならば，公開 Web サーバへの攻撃（OS コマンドインジェクション等）は可能であるため，コンテンツ改ざんのリスクを完全になくすことはできない。

したがって，プロキシサーバ導入の効果は，選択肢**イ**が述べるとおり，「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」となる。よって，これが正解となる。

ア，ウ：インターネット上での盗聴を防ぐには，インターネットを経由する区間の通信を，暗号化機能を備えたプロトコル（SSL 等）を用いてトンネリングしなければならない。

選択肢アにあるとおり，サーバ側のサイトにリバースプロキシサーバを設置した場合，クライアントに代わってリバースプロキシサーバが公開 Web サーバにアクセスする。選択肢ウにあるとおり，クライアント側のサイトにプロキシサーバ（フォワードプロキシサーバ）を設置した場合，クライアントに代わってプロキシサーバがインターネット上の Web サーバにアクセスする。つまり，どちらの場合も，ただ TCP コネクションの接続元が変わるだけに過ぎない。したがって，これだけでは，盗聴を防ぐことはできない。

エ：解説に入る前に，選択肢にある「改ざんを防ぐ」という言い回しについて補足する。厳密に言うと，今のネットワーク技術で実現されていることは，「改ざんが行われたことを検出する」ことである。その技術は改ざん行為を抑制することにつながる

ので，そのことを指して「改ざんを防ぐ」と慣用的に言い表すことがある。その点を踏まえ，この解説では，「改ざんを防ぐ」という記述を，「改ざんが行われたことを検出する」と読み替えることにする。

インターネット上で改ざんが行われたことを検出するには，インターネットを経由する区間の通信を，改ざん検出機能を備えたプロトコル（SSL 等）を用いてトンネリングしなければならない。

選択肢エにあるとおり，クライアント側のサイトにプロキシサーバを設置した場合，クライアントに代わってプロキシサーバがインターネット上の Web サーバにアクセスする。つまり，ただ TCP コネクションの接続元が変わるだけに過ぎない。したがって，これだけでは，改ざんが行われたことを検出することはできない。

問 19：正解イ

OP25B（Outbound Port 25 Blocking）とは，ISP が，個人利用者に対し，メールを送信するときには ISP 指定のメールサーバを経由するよう規制を加える仕組みである。動的 IP アドレスを払い出した利用者からの送信が，規制の対象となる。

具体的には，アウトバウンドの TCP/25 番ポートの通信（ISP から出ていく SMTP 通信）は，ISP 指定のメールサーバを送信元とするものだけに限定する。多くの迷惑メール（ウイルスメールを含む）は，動的 IP アドレスを払い出した利用者の端末から，ISP 指定のメールサーバを経由せずに送信されているので，この対策を実施することで，この種の迷惑メールを撲滅できる。

したがって，OP25B を導入することで，選択肢イにあるとおり，「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」。よって，正解は選択肢**イ**となる。

問 20：正解イ

OS コマンドインジェクションとは，アプリケーションが想定していない OS コマンドを攻撃者が意図的に実行させることで，OS を不正に操作する攻撃である。

Perl や PHP などのプログラム言語には，シェルを起動して OS コマンドを実行できる関数が存在する。Web アプリケーションのプログラムの中でそのような関数を不用意に使用しており，かつ，Web フォームにユーザが入力したパラメータをその関数の引数に渡すと，シェルが起動されてそのパラメータを OS コマンドとして実行してしまう。それゆえ，OS コマンドを効果的にパラメータに埋め込むことで，不正な操作が可能となる。

よって，正解は選択肢**イ**となる。

ア：HTTPヘッダインジェクションとは，HTTPパケットを偽造して不正なヘッダフィールドを HTTP ヘッダに埋め込み，これを受信したホストに不正な動作を行わせる攻撃である。
例えば，リダイレクトに使用する Location フィールドを偽造すれば，不正なサイトに誘導することができる。サーバからクライアントに Cookie を渡すときに使用する Set-Cookie フィールドを偽造すれば，不正な Cookie をクライアントに渡し，これをセッションハイジャック攻撃への足掛かりにすることができる。

ウ：クロスサイトリクエストフォージェリ（CSRF：Cross Site Request Forgery）とは，攻撃者の偽造したフォーム送信用のページ（以下，誘導ページと称する）を閲覧することを契機に，標的サイトに不正なフォーム送信を行う攻撃である。悪意あるスクリプトを誘導ページに仕組むことで，誘導ページを閲覧した時点で，自動的にフォーム送信を行わせることが可能となる。
攻撃者は，標的サイトの利用者が誘導ページを閲覧するように仕向ける（情報提供を装って，誘導ページへのリンクをクリックさせる，等）。かつ，攻撃者は，フォーム送信の受け手となる標的サイトのページとして，決済処理や退会処理など，利用者の意思確認を必要とする重要な処理を行うものを選ぶ。この攻撃によって，利用者の意図していない処理が，利用者に気づかれずに実行されてしまう。

エ：セッションハイジャックとは，セッションを用いた通信を第三者に乗っ取られる攻撃である。
Web アプリケーションで用いられる HTTP セッションは，セッション ID で識別される。Web サーバは，クライアントからの HTTP リクエストを受信すると，Cookie や URL に格納されたセッション ID に基づき，これに該当するセッションの処理を行う。したがって，セッション ID が漏えいしたり推測されたりすると，セッションハイジャック攻撃が成立してしまう。

問 21：正解イ

ア：Web サーバのディジタル証明書には，Web サーバのホスト名（FQDN）が記載されている。IP アドレスは記載されていないため，Web サーバの IP アドレスを変更しても，ディジタル証明書を再度取得する必要はない。

イ：**正解**。ディジタル証明書は IC カードなどに格納できる。

ウ：TLS は，サーバから要求したときだけ，クライアント認証を行う仕様になっている。

このクライアント認証にはディジタル証明書を用いるが，ごく一般的なインターネットの利用者は，自らを認証する用途でディジタル証明書を認証局から取得してはいない。それゆえ，インターネット上で不特定多数のクライアントからアクセスを受け付ける Web サーバは，TLS のクライアント認証を行わない。

したがって，選択肢にある「TLS は特定の利用者間の通信のために開発されたプロトコル」「Web サーバ提供者への事前の利用者登録が不可欠」という記述は誤りである。

エ：日本国内では，TLS で使用する共通鍵の長さに制限は課せられていない。

問 22：正解ウ

ア：RAID1 は，ディスクをミラーリングする方式である。

イ：RAID3 は，パリティ専用の磁気ディスク装置をもち，データをビット単位でストライピングする方式である。

ウ：**正解**。RAID4 は，パリティ専用の磁気ディスク装置をもち，データをブロック単位でストライピングする方式である。

エ：RAID5 は，パリティ専用の磁気ディスクをもたない。データとパリティをともにブロック単位でストライピングする方式である。

問 23：正解ウ

問題文に示されたアムダールの法則は，次式のとおりである。

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

本問を解くには，各選択肢の記述に従ってパラメータをこの式に代入し，その真偽を確認すればよい。ここでは，正解である選択肢ウについてのみ解説する。

選択肢ウには，「並列可能部の割合が 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は 2 を超えることはない」とある。ここで，プロセッサ数について，選択肢ウに反して「正の有限の数である」との仮定を置き（プロセッサ数は分母にあるので 0 を除外），それ以外のパラメータは選択肢ウに合わせて，選択肢ウの正しさを背理法で導いてみよう。

まず，「並列可能部の割合」に 0.5 を，「性能向上比」に「2」をそれぞれ代入する。「性能向上比は 2 を超えない」とあるので，性能向上比は 2 以下である。すなわち，次式が成立する。

$$2 \geqq \frac{1}{(1-0.5)+\dfrac{0.5}{\text{プロセッサ数}}}$$

この式を解くと，

$$0 \geqq \frac{0.5}{\text{プロセッサ数}}$$

となる。

プロセッサ数が「正の有限の数である」と仮定するなら，この式は正しくない。したがって，「性能向上比」が 2 を超えず，かつ，「並列可能部の割合」が 0.5 であるならば，プロセッサ数に置いた仮定が誤っていることになる。定義上，プロセッサ数は負になり得ないので，考えられる値は正の∞となる。したがって，選択肢ウの正しさが証明された。

よって，正解は選択肢**ウ**である。

問 24：正解ウ

クラス A という集合がクラス B という集合の部分集合であるとき，クラス B はクラス A のスーパークラスとなり，クラス A はクラス B のサブクラスとなる。スーパークラスとサブクラスの関係のことを汎化関係という。これを is-a 関係ともいう。なぜなら，汎化関係にあるものを英語で「A is a B」と表現できるからだ。

ア：「拡大」「縮小」は，「画像」クラスがもつ操作である。

イ：「氏名」「生年月日」は，「社員」クラスがもつ属性である。

ウ：**正解**。「乗用車」「トラック」というクラスは，「自動車」というクラスの部分集合である。したがって，is-a 関係が成立している。

エ：「受話器」「プッシュボタン」というクラスは，「電話」クラスの属性である。もっとも，属性がクラスになっている場合，「受話器，プッシュボタンは，電話の構成要素（部品）である」と表現する方が自然である。クラス A がクラス B の構成要素であるとき，これを part-of 関係という。なぜなら，この関係にあるものを英語で「A is a part of B」と表現できるからだ。

なお，英語表現の「is-a」が汎化関係と厳密に符合しているわけではないため，「is-a」は方便であると割り切って理解しておこう（例えば，B が集合であり，A がその元であるとき，A is a B と言い表せる）。

問 25：正解ウ

SOA（Service-Oriented Architecture）とは，既存のアプリケーションを部品化し，その部品を組み合わせてビジネスプロセスを設計する手法である。

SOA では部品を「サービス」と呼んでいるが，この「サービス」の定義が SOA の特長であり，サービスをいかに設計するかが成否を左右すると言えよう。サービスを設計する際，サービスの粒度は，ビジネスプロセスのひとまとまりの処理（受注処理や在庫引当など，サービス内で処理が完結しているもの）にする。業務ルールが部分的に変化したときに，一部のサービスだけを入れ替えたり，サービス同士の順番や組合せを変更したりすることで対応できるようにするため，サービス間の独立性を高めておく。これを「疎結合」と呼ぶ。更に，開発言語やプラットフォームに依存せずに実行できるものにしておく。

よって，正解は選択肢**ウ**である。

ソフトウェア部品を組み合わせる技術として，SOA が登場する前から，CORBA や DCOM など分散オブジェクト技術が用いられていた。しかし，分散オブジェクト技術では部品の粒度がオブジェクトであり，プログラムから呼ぶ形態であった。したがって，ビジネスの視点から使いやすいものではなかった。更に，CORBA や DCOM などの技術基盤をシステム全体で共通化することが求められていた。2000 年代以降，HTTP や XML などのインターネット標準の技術を使った Web サービスが登場したことを背景に，2004 年頃から SOA の概念が提唱され，脚光を浴びるようになった。