平成29年度 秋期 午前Ⅱ問題の解答・解説

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

問 1：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活かし，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。前述の特性を活かし，近距離での映像配信といった応用が検討されている。

問 2：正解エ

呼量［アーラン］は，次の式から求めることができる。

呼量＝平均回線保留時間［秒］× 1 台当たりの呼の発生頻度［件／秒］／台数

問題本文より，平均回線保留時間は「80 秒」，電話機 1 台当たりの呼の発生頻は「3 分」（180 秒），電話機の台数は「180」なので，これらを代入すると，

呼量＝ 80［秒］× 180［件／秒］／ 180 台
　　＝ 80［アーラン］

となる。よって，正解は選択肢**エ**となる。

問 3：正解イ

RIP-2 と OSPF の特徴を比較すると，次のようになる。

表：RIP-2 と OSPF の特徴

特徴	RIP-2	OSPF
可変長サブネットへの対応可否	可	可
経路制御の方式	距離ベクトル方式	リンク状態方式
経路情報交換の通信形態	マルチキャスト	マルチキャスト
経路情報交換の更新間隔	30 秒	ネットワーク構成が変化したときに更新する。変化しなかった場合でも，30 分ごとに更新する

ア：RIP-2，OSPF の双方に当てはまる特徴である。

イ：**正解**。OSPF に当てはまる特徴である。ルータは，自分のリンク状態及び受信したリンク状態の情報を管理するデータベースをもつ。この情報に基づき，ルータはルーティングテーブルを生成する。

ウ：RIP-2，OSPF の双方に当てはまる特徴である。

エ：RIP-2 に当てはまる特徴である。

問 4：正解ウ

IEEE802.1Q で規定された VLAN の ID（VLAN Identifier）のビット長は 12 ビットである。よって，正解は選択肢**ウ**となる。

問 5：正解エ

スパニングツリー機能は，複数のブリッジ（又はスイッチ）からなるネットワークを冗長化する機能である。スパニングツリー機能による冗長化を実現するため，ブリッジ間でやり取りされるプロトコルが，スパニングツリープロトコルである。

ネットワークの物理的な構成がループ状のネットワークトポロジであるとき，ブリッジ間には経路が複数存在している。スパニングツリー機能は，ブリッジ ID，パスコスト，ポート ID に基づいて一部のポートをブロックすることにより，ツリー状のネットワークトポロジを論理的に構成する。このツリーのことを，スパニングツリーという。

物理的な構成がループ状であっても，論理的な構成はツリー状なので，複数ある経路のうち一つだけがアクティブの状態になっている。障害が発生して通信が途絶えると，障害の発生箇所を迂回するようなスパニングツリーが新たに構成され，通信が再開される。

スパニングツリーのルートに位置するブリッジは，ルートブリッジと呼ばれる。ルートブリッジは，ブリッジ ID の値が最小のものが選ばれる。ブリッジ ID は 8 バイトの長さをもち，上位 2 バイトはブリッジの優先順位，下位 6 バイトはブリッジの MAC アドレスである。よって，正解は選択肢**エ**となる。

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は，エンドシステム間（送信元ホストと宛先ホスト間）の通信を行うプロトコルであり，エンドシステム間の経路選択と中継を担っている。
一方，スパニングツリープロトコルは，ブリッジからなるネットワークを冗長化するために使用される。したがって，エンドシステム間の経路の中にある一つのセグメント（サブネットワーク）を対象としているに過ぎない。よって，「ネットワーク層のプロトコル」という記述は誤りである。
正しくは，「データリンク層のプロトコル」である。

イ：前述のとおり，論理的な構成はツリー状になっている。複数の経路が存在している場合でも，そのうちの一つの経路だけがアクティブの状態になっている。よって，「複数経路がある場合，同時にフレーム転送する」という記述は誤りである。

ウ：スパニングツリープロトコルで一部のポートがブロックされている点を除けば，イーサネットフレームを伝送する通常のネットワークであることに変わりはない。したがって，「ブロードキャストフレームを，ブリッジ間で転送しない」という記述は誤りである。

問 6：正解ア

DNS サーバには，その DNS サーバが管轄するドメインにおけるメール交換ホストを登録することができる。その登録には MX レコードを用い，その書式は次のようになっている。次の網掛け部分にパラメータ値を指定する。

ドメイン名　IN　MX　プリファレンス値　メール交換ホストのホスト名

先頭のフィールドには，メールアドレスのドメイン名を指定する。

よって，正解は選択肢**ア**となる。

イ：MX レコードを複数登録し，メール交換ホストの冗長化を図ることができる。そのように登録する場合，それぞれのプリファレンス値を異なる値にする。その中で，最小のプリファレンス値をもつ MX レコードが，最も高い優先度をもつ。

ウ：メール交換ホストの指定には，IP アドレスではなくホスト名を用いる。

エ：メール交換ホストを指定する際，ホスト名の別名を用いることはできない。

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：正解エ

ア：IPv6 は，IPv4 とは異なり，IP ヘッダ長は固定である。したがって，ルータでの中継処理の高速化が図られている。

イ：IPv6 アドレスは，通常，16 進数で表記する。ただし，射影アドレスなど，IPv4 アドレスを含んだアドレスを表記する際は，その IPv4 アドレス部分を 10 進数で表記することができる。

ウ：射影アドレス（IPv4-mapped IPv6 address）は，IPv4 アドレスしかもたないホストが，IPv6 ネットワーク上で使用する IPv6 アドレスである。

射影アドレスは，上位 96 ビットを「0:0:0:0:0:ffff」，下位 32 ビットを当該ノードの IPv4 アドレスに設定したアドレスから構成される。

エ：**正解**。IPv6 は，ルータ要請／ルータ広告パケットのやり取りを通して，ホストのグローバルアドレスを自動設定することができる。これをステートレスアドレス設定という。

IPv6 について，詳しくは《基礎編》の第 3 章「3.9　IPv6」を参照されたい。

問 9：正解エ

迷惑メールの送信を防止するため，ISP は，「自 ISP から他 ISP に転送されるメールは，自 ISP が指定したメールサーバを経由するものを除き，全てブロックする」という規制を設けている。これを OP25B（Outbound Port 25 Blocking）という。

この OP25B を実現するため，ISP とインターネットとの境界に位置するルータで，自 ISP 拠点から出ていく，宛先ポート番号が 25/TCP の通信（SMTP）をフィルタリングしている。

この規制対象となるホストは，ISP から IP アドレスの動的な割当てを受ける利用者のものである。それらの利用者は，主に個人や小規模な組織である。

自 ISP の利用者が，OP25B を実施している他 ISP 拠点からメールを送信する場合，その OP25B による規制を受けることなく，自 ISP のメールサーバに接続する必要がある。そのため，他 ISP 拠点からメールを送信するときは，宛先ポート番号として，通常の 25/TCP ではなく，587/TCP を用いる。このポートをサブミッションポートという。

このように，迷惑メールを防止するため，メールクライアントからのメール送信に用いるポート番号は，通常のメール送信（メールクライアントとメールサーバ間，及び，メールサーバと他のメールサーバ間の通信）に用いるポート番号と異なるものを使用することがある。

よって，正解は選択肢**エ**となる。

ア：拡張機能の一覧の応答を求めるコマンドは，HELO コマンドではなく，EHLO コマンドである。

イ：RCPT コマンドに指定する宛先メールアドレスの数は一つである。したがって，宛先のメールアドレスが複数ある場合，メールアドレスごとに RCPT コマンドを一つずつ用いる。

ウ：差出人のメールアドレスは，MAIL コマンドに指定する。DATA コマンドに指定するのは，送信するメッセージである。

問 10：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 11：正解ウ

ア：TCP は，輻輳を回避するためにウィンドウサイズを小さくする機能をもっている。

イ：フォワード誤り訂正方式（FEC：Forward Error Correction）とは，送信側がメッセージに誤り訂正用の情報を付与する方式である。受信側で誤りを訂正できるので，送信側にデータの再送を要求しない。携帯電話での通話や宇宙探査機からのデータ送信など，ノイズの影響を受けやすく，再送に不向きな通信で用いられている。

ウ：**正解**。ウィンドウによるフロー制御について適切に記述している。この方式は，TCP のフロー制御に採用されている。

エ：データグラム方式とは，送信ホストと受信ホスト間にコネクションを確立せずにパケットを送受信する方式である。IP や UDP はデータグラム方式を採用している。データグラム方式はコネクション方式とは異なり，パケットの順序管理，パケット廃棄に伴う再送要求，ウィンドウを用いたフロー制御や輻輳制御（スロースタートや輻輳回避）などを行わない。したがって，コネクション確立フェーズ，確認応答処理，再送処理，スロースタートといった，コネクション管理に特化したやり取りが発生しない。さらに，コネクション方式よりもヘッダが簡略化されている分，そのサイズが小さいので，1 パケットに占めるデータの割合は大きくなる傾向がある。したがって，コネクション方式に比べ，確認応答処理や再送処理に伴う遅延が発生せず，単位時間当たりに通信できるデータ量が多くなる。それゆえ，DNS など，概して要求／応答の 1 往復で事足りるプロトコルで，使用頻度が高い通信に用いられる。また，音声通信など，多少のパケット廃棄は許容できるので再送処理は不要だが大幅な遅延が問題視される通信に用いられる。なお，パケット廃棄の検知及び対応は，必要ならば上位層で行う。例えば，IP であれば TCP が，UDP であれば DNS が行う。

選択肢の文中に「経路選択のオーバヘッドを小さくしている」とあるが，経路選択はルータが行っているため，データグラム方式であろうとコネクション方式であろうとこのような働きはしない。

問 12：正解イ

特定サブネット内でのブロードキャストアドレスは，ホスト部をすべて 1 にセットした値である。192.168.10.192/28 のサブネットの場合，下位 4 ビットがホスト部になる。このネットワークアドレスの第 4 オクテットを 2 進数で表記してみると，11000000 となるので，下位 4 ビットをすべて 1 にセットした値は 11001111 になる。これを 10 進数で表記すると 207 になるので，ブロードキャストアドレスは 192.168.10.207 である。よって，正解は選択肢**イ**である。

問 13：正解ア

OpenFlow は，SDN（Software-Defined Networking）で利用されるプロトコルである。

OpenFlow では，従来のスイッチ機能を，経路制御などの管理機能を実行するフローコントローラと，データ転送を行うフロースイッチに分離している。フロースイッチは，パケットの経路制御の動作を定義したフローテーブルをもっている。フローコントローラは，フロースイッチに対し，フローテーブルに特定の動作を登録したり更新したりするコマンドを送信し，フロースイッチに入るパケットの経路制御を管理することができる。

よって，正解は選択肢**ア**となる。

イ：SNMP（Simple Network Management Protocol）に関する説明である。SNMP は，ネットワーク管理に用いるプロトコルである。

ウ：IPFIX（Internet Protocol Flow Information Export) に関する説明である。IPFIX は，IP ネットワークのトラフィック分析に用いるプロトコルである。

エ：STP（Spanning Tree Protocol）に関する説明である。STP は，レイヤ 2 の冗長化に用いるプロトコルである。

問 14：正解ウ

FTP（File Transfer Protocol）は，クライアントと FTP サーバ間でファイル転送を行うプロトコルである。その通信に際し，制御用コネクションとデータ転送用コネクションの二つのコネクションを用いる。

制御用コネクションは，クライアントから FTP サーバへのコマンドの送信，及び，同コマンドに対する FTP サーバからクライアントへの応答に用いられる。主なコマンドには，クライアントから FTP サーバへのファイルのアップロード，FTP サーバからクライアント

へのファイルのダウンロード，FTP サーバ側のファイル一覧の取得，ユーザ認証（FTP サーバがクライアントを認証）などがある。

データ転送用コネクションは，コマンドの内容に応じた，クライアントと FTP サーバ間のデータ転送に用いられる。

制御用コネクションの確立は，クライアントから FTP サーバに対して行われる。

データ転送用コネクションの確立は，2 種類の方法がある。

一つ目は，FTP サーバからクライアントに向けて行われるもので，アクティブモードと呼ばれる。二つ目は，クライアントから FTP サーバに向けて行われるもので，パッシブモードと呼ばれる。

コネクション確立の方向に関する内容をまとめると，次の表のとおりとなる。

したがって，パッシブモードを用いる場合，どちらのコネクションの確立もクライアントから FTP サーバに対して行う。よって，正解は選択肢**ウ**となる。

表：コネクション確立の方向

種類	アクティブモード	パッシブモード
制御用コネクション	クライアントから FTP サーバ	クライアントから FTP サーバ
データ転送用コネクション	FTP サーバからクライアント	クライアントから FTP サーバ

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：正解エ

ウイルスを検知する手法には，パターンマッチング法，コンペア法，チェックサム法，ヒューリスティック法，ビヘイビア法などがある。

本問が問うているビヘイビア法とは，検査対象プログラムの挙動を観察し，ウイルスによく見られる行動を起こさせばウイルスとして検知する手法である。

コードの読込みを妨害するステルス型や，感染するたびにウイルス自身のコードを暗号化して変容させるミューテーション型にも対応できる。ただし，実際に動作したときの挙動を観察する必要があるので他の方法に比べて検知に時間がかかる。

よって，正解は選択肢**エ**となる。

ア：パターンマッチング法に当てはまる記述である。
イ：チェックサム法に当てはまる記述である。
ウ：コンペア法に当てはまる記述である。

●補足

どの選択肢にも登場しないヒューリスティック法について補足する。

ヒューリスティック法とは，ウイルスによく見られる行動がどのようなコード列に対応するかを事前に登録しておき，検査対象プログラム内にそのコード列が存在しているかを調べて，もし存在していればウイルスとして検知する手法である。

「ウイルスによく見られる行動」に着目する点では，ビヘイビア法と似ている。しかし，ヒューリスティック法は検査対象を動作させない点が，ビヘイビア法と異なっている。ヒューリスティック法はコード列を調べる手法なので，ステルス型やミューテーション型には対応できないとされる。

問 17：正解ア

サービス妨害攻撃を仕掛ける攻撃者は，大量の攻撃用パケットを送信する際，送信元 IP アドレスを詐称する。自分の IP アドレスを送信元アドレスに設定しない理由は，攻撃用パケットに対する応答パケットが自分自身に大量に返らないようにするためであり，さらには追跡を免れたるためでもある。

送信元アドレスに指定する詐称用の IP アドレスには，例えば，ダークネット（未使用の IP アドレス空間）のものが選ばれる。

さて，サービス攻撃の一種である SYN フラッド攻撃を仕掛けるため，次に示す攻撃用パケットを攻撃者が送信したとしよう。

送信元 IP アドレス	ダークネットの IP アドレス
宛先 IP アドレス	A
宛先ポート番号	80/tcp
パケットの内容	SYN パケット

このとき，標的となったホストからダークネットに対し，次に示す応答パケットが返信される。

送信元 IP アドレス	A
宛先 IP アドレス	攻撃用パケットの送信元に指定された，ダークネットの IP アドレス
送信元ポート番号	80/tcp
パケットの内容	SYN/ACK パケット

よって，正解は選択肢**ア**となる。

問 18：正解エ

ディジタルフォレンジックスは，事故，不正行為，犯罪といったインシデントに関する証拠となり得るデータを，ありのままの状態で，確実に，収集（Collection），取得（Acquisition），保全（Preservation）することである。保全されたデータは，インシデントの解析，訴訟時の証拠提出などに用いられる。

よって，正解は選択肢**エ**となる。

ア：ステガノグラフィに関する説明である。ステガノグラフィとは，画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込むことである。

イ：ペネトレーションテストに関する説明である。ペネトレーションテストとは，システムを実際に攻撃して侵入を試みることで，コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法である。

ウ：ソーシャルエンジニアリングに関する説明である。ソーシャルエンジニアリングとは，ネットワーク管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手することである。

問 19：正解イ

DNSSEC とは，権威 DNS サーバが名前解決の回答をキャッシュサーバに返信する際，回答するリソースレコードに対してディジタル署名を付与する技術である。

受信側のキャッシュサーバは，ディジタル署名を用い，送信元ホストが正当な DNS サーバであるか（送信者認証），受信したリソースレコードが改ざんされていないか（メッセージ認証）を検証することができる。よって，正解は選択肢**イ**となる。

問 20：正解イ

問題文には，内部ネットワーク上の PC からインターネット上の Web サイトを参照するとき，次の条件に従うと記述されている。

- DMZ 上の VDI（Virtual Desktop Infrastructure）サーバにログインする。
- VDI サーバ上の Web ブラウザを利用する。

このとき，PC と VDI サーバ間は VDI の画面転送プロトコルだけを用いるならば，Web サイトとやり取りを行うのは，実質上，VDI サーバに限定される。

したがって，Web サイトからマルウェアが侵入したとしても，その侵入先は VDI サーバだけとなる。さらに，Web サイトへのデータ流出が行われたとしても，その流出元は VDI サーバだけとなる。

よって，正解は選択肢**イ**となる。

ア：PC と VDI サーバ間の通信に FTP を用いる場合，PC のデータが VDI サーバに転送される可能性がある。さらに，VDI サーバに保存されたデータが PC に転送される可能性がある。

この状況下で，Web サイトによって VDI サーバがマルウェアに感染するならば，そのマルウェアによって VDI サーバからデータが流出する可能性がある。したがって，結果的に，PC からデータが流出する可能性がある。

さらに，VDI サーバに保存されたマルウェアの実行ファイルが FTP で PC に転送されるならば，その後に PC がマルウェアに感染する可能性がある。

ウ，エ：問題文にあるとおり，VDI サーバにログインし，VDI サーバ上の Web ブラウザを利用する方式を採用している場合，PC と VDI サーバ間は VDI の画面転送プロトコルを用いる必要がある。

選択肢ウ，エを解く際，この画面転送プロトコルに加え，他のプロトコルも用いているものと仮定する。

選択肢ウにあるとおり，VDI サーバを HTTP プロキシとして利用しているとしよう。このとき，実質上，Web サイトと HTTP 通信をやり取りするのは PC となる。し

たがって，Web サイトによって PC がマルウェアに感染し，そのマルウェアによって PC からデータが流出する可能性がある。

選択肢エにあるとおり，VDI サーバが VDI の画面転送プロトコルのプロキシとなり，PC の画面を Web サイトに中継しているとしよう。このとき，PC の画面に表示された情報が Web サイトに漏えいする可能性がある。

問 21：正解ア

DNS amp 攻撃を理解するには，名前解決パケットの IP アドレス詐称の仕組み，及び，再帰的問合せの仕組みを理解する必要がある。これらの点について，まずは解説する。次いで，DNS amp 攻撃について解説する。最後に解を導こう。

●名前解決パケットの IP アドレス詐称の仕組み

DNS の名前解決は UDP パケットを用いており，問合せと応答の 1 往復（2 個のパケット）だけで完結する。したがって，名前解決の問合せパケットの送信元 IP アドレスを詐称すれば，応答パケットの返信先は，詐称したアドレスとなる。

●再帰的問合せの仕組み

名前解決を行う際，クライアントは，自ホストに登録された DNS サーバに対し，問合せのパケットを送信する。これを再帰的問合せと呼ぶ。再帰的問合せを受けた DNS サーバ（登録された DNS サーバ）は，クライアントからの問合せに対する回答を保持していない場合，その回答が得られるまで，他の DNS サーバに問合せを行う。これを反復的問合せという。反復的問合せを受けた DNS サーバは，名前解決の情報が登録されているサーバである。これをコンテンツサーバと呼ぶ。再帰的問合せを受けた DNS サーバは，反復的問合せで得られた回答を，一定期間キャッシュする。それゆえ，これをキャッシュサーバと呼ぶ。

● DNS amp 攻撃の仕組み

DNS amp 攻撃は，次の三つの段階からなる。手順 1，2 が準備段階であり，手順 3 が攻撃である。

1. 攻撃者は，自分が管理する DNS サーバの TXT レコードに，大容量の文字列情報を登録する。
2. 攻撃者は，インターネット上のキャッシュサーバ（インターネット側から再帰的問合せを実行できるサーバ）に対し，「手順 1 で用意した DNS サーバの TXT レコード」を問

い合わせる。当該キャッシュサーバは，手順 1 の DNS サーバから TXT レコードを取得し，攻撃者にこれを回答する。それと同時に，当該キャッシュサーバは，この TXT レコードをキャッシュする。

これを，多数のキャッシュサーバにおいて実施する。

3. 攻撃者は，ボットを仕込んだホストを多数用意する。ボットに対し，手順 2 のキャッシュサーバ宛てに「手順 1 の DNS サーバの TXT レコード」を問い合わせるよう，指示を出す。その際，問合せパケットの送信元 IP アドレスを詐称し，これを攻撃対象のホストの IP アドレスに書き換えておく。この結果，TXT レコードの応答パケット（大容量の文字列情報を含むパケット）は，攻撃対象のホストに返信される。

これを多数のキャッシュサーバにおいて，一斉に実施する。この結果，攻撃を受けたホストは大容量のパケットを同時に多数受信するため，サービス不能に陥る。

●解の導出

本問は，DNS amp 攻撃の踏み台にされることを防止する対策を問うている。ここで，「踏み台にされる」サーバとは，前述の手順 2，3 に登場したキャッシュサーバである。

DNS amp 攻撃が成立するには，インターネット側からキャッシュサーバにアクセスできなければならない。したがって，対策として，インターネット側からキャシュサーバに問合せできないようにすることが有効な手段となる。よって，正解は選択肢**ア**となる。

参考までに，選択肢アにある「キャッシュサーバとコンテンツサーバに分離」という記述について補足しよう。キャッシュサーバは，コンテンツサーバの役割を担っていても構わない。しかし，コンテンツサーバを兼任してしまうと，インターネットからの問合せを受け付ける必要がある。そこで，キャッシュサーバがコンテンツサーバの役割を兼任しないようにし，インターネット側からキャッシュサーバにそもそもアクセスできないようにするとよい。

問 22：正解ウ

MLC（Multi-Level Cell）フラッシュメモリは，一つのメモリセルに 2 ビット以上のデータを記憶することができるメモリ素子である。

よって，正解は選択肢**ウ**となる。

ア：DRAM（Dynamic RAM）に関する説明である。DRAM は，コンデンサに蓄えた電荷を利用してデータを記憶する半導体メモリ素子である。

イ：抵抗変化型メモリ（ReRAM：Resistive RAM）に関する説明である。ReRAM は，ある種の電界効果トランジスタに電圧を加えたときに電気抵抗が大きく変化する現

象を利用してデータを記憶する半導体メモリ素子である。

エ：SRAM（Static RAM）に関する説明である。SRAM は，フリップフロップと呼ばれるメモリセルを用いてデータを記憶する半導体メモリ素子である。

問 23：正解ウ

問題文に示された，プリンタに対する印刷要求の到着数，プリンタの印刷時間（サービス時間），及びプリンタの台数（窓口数）の各条件を整理すると，次の表のようになる。

表：問題文の条件

条件		内容
到着数	平均到着数	1［回／分］（＝ 1/60［回／秒］）
	到着数の分布	ポアソン分布
サービス時間	平均サービス時間	15［秒］
	サービス時間の分布	指数分布
窓口数		1

到着数の分布がポアソン分布，サービス時間の分布が指数分布，窓口数が 1 なので，M/M/1 の待ち行列モデルに従う。

問題文に記されたプリンタの平均印刷時間は，印刷を要求してから終了するまでの時間であり，待ち時間を含んだものである。すなわち，これは待ち行列理論における平均応答時間に相当する。

M/M/1 の待ち行列モデルでは，平均応答時間は次式より求まる。ここで，平均応答時間を Tr，平均到着数を λ，平均サービス時間を Ts とする。

$$Tr = \frac{1}{1 - \lambda \times Ts} \times Ts$$

前述の表より，λ = 1/60［回／秒］, Ts = 15［秒］なので，これを代入して Tr を算出する。

$$Tr = \frac{1}{1 - \frac{15}{60}} \times 15$$

$$= \frac{15}{0.75} = 20$$

よって，正解は選択肢**ウ**となる。

問 24：正解ア

ISO/IEC25010 規格で標準化されているシステムとソフトウェアの製品品質は，次に示す 8 種類の品質特性からなる。

1. 機能適合性
2. 性能効率性
3. 互換性
4. 使用性
5. 信頼性
6. セキュリティ
7. 保守性
8. 移植性

同規格は，本問で問われている使用性を，次のように定義している。

> 明示された利用状況において，有効性，効率性及び満足性をもって明示された目標を達成するために，明示された利用者が製品・システムを利用することができる度合い

ア：**正解**。オンラインヘルプを充実させ，利用方法を理解しやすくすることは，使用性を向上させる施策である。

イ：外部インタフェースを見直し，連携できる他システムを増やすことは，互換性を向上させる施策である。

ウ：機能を追加し，業務においてシステムが利用できる範囲を拡大することは，（そのことが明示的及び暗黙的なニーズを満足させることに寄与するのであれば，）機能適合性を向上させる施策である。

エ：ファイルの複製を分散して配置し，障害によるシステム停止のリスクを減らすことは，信頼性を向上させる施策である。

この解説で取り上げた ISO/IEC25010 規格は，ISO/IEC9126 規格（ソフトウェア品質特性）の後継に当たる。システムやソフトウェアの品質について問われる場合，昔は ISO/IEC9126 規格から出題されていたが，今後は ISO/IEC25010 規格から出題されるものと考えられる。

ISO/IEC25010 規格の品質特性は，ISO/IEC9126 規格より品質特性が二つ多くなり（互換性，セキュリティ），品質特性を細分化した品質副特性を拡充するなど，全体的にブラッシュアッ

プされている。

したがって，今後は ISO/IEC25010 規格に基づいて，システムとソフトウェアの品質特性を学習しておくことをお勧めする。

問 25：正解エ

XP（eXtreme Programming）のプラクティスには様々なものがあるが，代表的なものの一つがペアプログラミングである。よって，正解は選択肢**エ**となる。

ペアプログラミングとは，その名のとおり，プログラミングを二人一組で行うことである。一人がプログラムを作成し，もう一人がそれを目視しながらフィードバックを適宜与える。二人は，この役割を定期的に交代する。

ペアプログラミングの実施により，問題解決の迅速化，コード品質の向上などの効果が得られると言われている。