平成26年度 秋期 午前Ⅱ問題の解答・解説

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

問 1：正解エ

● IPv6 のアドレス

IPv6 ノードは，1 個のネットワークインタフェースに，複数の IPv6 アドレスをもつことができる。

その一つに，リンクローカルアドレスがある。これは，使用できる範囲が一つのリンクに限定されるアドレスである。ここでいう「リンク」とは，ネットワークインタフェースからルータを介さずに直接接続できる範囲を指しており，IPv4 のサブネットワークと同じものである。IPv6 ノードは，リンクローカルのユニキャストアドレスを必ずもつ。

他には，グローバルアドレスがある。これは，同一リンク内のルータからグローバルアドレスのプレフィックスをルータ広告メッセージで通知されたときだけ，付与される。

リンクローカルアドレスは，近隣探索など，IPv6 ネットワークの制御用メッセージのやり取りで，主に使用される。先ほど触れたルータ広告メッセージは，近隣探索の一つである。

グローバルアドレスは，アプリケーションのデータのやり取りなど，通常のデータ通信で使用される。

IPv6 のアドレスについて，詳しくは《基礎編》第 3 章「3.9.2　アドレス空間の拡張」を参照していただきたい。

●解の導出

本問は，リンクローカルユニキャストアドレスについて問うている。これは，選択肢エに記述されているとおり，「このアドレスをもつネットワークインタフェースからルータを介さずに直接接続できる相手との通信にだけ使用できるアドレス」である。よって，これが正解となる。

問 2：正解イ

PLC（Power Line Communication：電力線通信）とは，電力線を通信回線として利用する技術である。

よって，正解は選択肢**イ**となる。

●参考

電力線で送電される交流電圧の周波数は，関東で 50Hz，関西で 60Hz である。これに対し，PLC は，交流電圧よりも高い周波数帯域を使用してデータを通信する。その周波数帯域には，低速用（10 ～ 450KHz）と高速用（2 ～ 30MHz）の 2 種類がある。一般的に言うと，屋内

では高速用，屋外（ネットワークインフラ）では低速用が使用されるなど，利用目的に応じた使い分けがなされている。

PLC が注目を集めている理由は，経済性と導入容易性である。

既存の屋外電力線と屋内配線を使用するため，通信用の工事が不要となり，経済的である。部屋や廊下の各所に設置されたコンセントにプラグを挿せば使えるので，電化製品のような手軽さで情報端末を利用でき，家庭内に LAN を簡単に構築できる。無線 LAN では壁が電波障壁となり得る点を考慮するなら，PLC を利用した LAN は無線 LAN よりも導入が容易であると言える。

とはいえ，屋内で利用する場合は，通信速度の不安定さに留意しておく必要があるだろう。既設の屋内配線の電力線は，そもそも高周波の重畳を想定したものではないため，様々な電化製品を同時に使用すると，ノイズの影響により実効通信速度が得られない可能性がある。

問 3：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 4：正解イ

マルチキャストアドレスブロックは，アドレスの上位 4 ビットが「1110」，すなわち，通常表記で 224.0.0.0 ～ 239.255.255.255 の範囲内のものである。これは，クラス D のアドレスに相当する。よって，正解は選択肢**イ**となる。

ア：マルチキャストアドレスブロックには，アドホックブロックが割り当てられている。
　　これは，あらかじめ用途を固定するのが適さないアプリケーション用のマルチキャ

スト通信に使用される。

ウ：マルチキャストパケットも，ユニキャストパケットと同様に，TTL の値が 0 になったら廃棄される。

エ：マルチキャスト通信は，送信元と宛先が 1 対多となる形態の通信である。その宛先は，ネットワーク上の全てのホストが対象となることもあれば，そうではないこともある。

マルチキャストパケットを受信したホストは，宛先 IP アドレスに指定されたマルチキャストアドレスに基づき，自ホストがこのパケットを受け取る対象に含まれているか否かを判断する。この判断はインターネット層（IP）で行われる。

受け取る対象であれば，IP パケットのペイロードを上位層に渡す。そうでなければ，IP パケットを廃棄する。

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

ア：**正解**。AAAA レコードは，ホスト名に対応する IPv6 アドレスを登録するレコードである。

イ：CNAME 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）を登録するレコードである。

ウ：MX レコードは，ドメイン名に対応するメールサーバのホスト名を登録するレコードである。

エ：SOA レコードは，ゾーン全体に関する情報を登録するレコードである。例えば，ドメイン管理者のメールアドレス，リフレッシュ間隔（ゾーン転送の時間間隔），ネガティブキャッシュ有効時間などを登録する。

問 7：正解ア

ア：**正解**。BGP-4 はパスベクタ方式のプロトコルである。

イ：リンク状態データベースを用い，コストが最小となる経路を選択する方式をリンクステート（リンク状態）方式と呼ぶ。これを採用しているプロトコルの一つに OSPF がある。ただし，同一のリンク状態データベースをもつのは，同一エリア内のルータである。

ウ：ホップ数が最小となる経路を最適経路として選択する方式を距離ベクタ方式と呼ぶ。これを採用しているプロトコルの一つに RIP がある。

エ：転送経路を送信元ノードが明示的に指定する方式をソースルーティング方式と呼ぶ。

問 8：正解イ

DNS でのホスト名と IP アドレスの対応付けは，選択肢イに記述されているとおり，多対多である。よって，正解は選択肢**イ**である。

ホスト名と IP アドレスの対応付けは A レコードに登録する。一つのホスト名に複数の IP アドレスを対応させたい場合，及び，複数のホスト名に一つの IP アドレスを対応させたい場合は，それぞれ次の図に示すように指定する。なお，一つのホスト名に複数の IP アドレスを対応させた場合，名前解決時にラウンドロビンされる。

〔一つのホスト名に複数の IP アドレスを対応させる例〕

hostA	IN	A	192.0.2.1
hostA	IN	A	192.0.2.2
hostA	IN	A	192.0.2.3

名前解決時にラウンドロビンされる

〔複数のホスト名に一つの IP アドレスを対応させる例〕

hostB	IN	A	192.0.2.4
hostC	IN	A	192.0.2.4
hostD	IN	A	192.0.2.4

図：A レコードの登録例

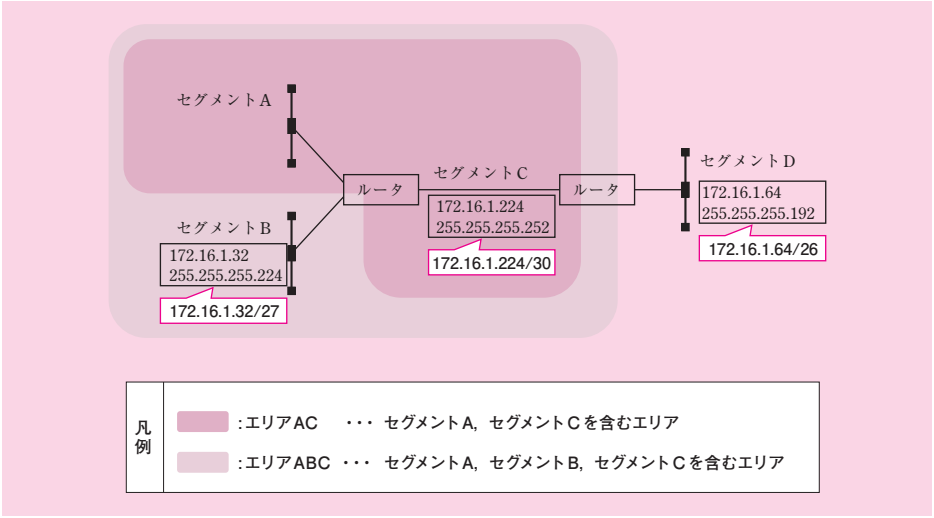
問 9：正解イ

IPv4 では，ARP を用いてリンク層のアドレス解決と重複アドレスの検出を実現していた。IPv6 では ARP が廃止され，代わりに ICMPv6（Internet Control Message Protocol version 6）に規定された近隣探索の仕組みを用いて，これらを実現する。よって，正解は選択肢**イ**となる。

IPv6 の近隣探索について，詳しくは《基礎編》の第 3 章「3.9.3　近隣探索とアドレス自動設定機能」を参照していただきたい。

問 10：正解ウ

問題の図を，次の図「ネットワーク構成」に示す。



図：ネットワーク構成

まず，最も大きいアドレス空間をもつセグメント D に着目し，ネットワーク全体をセグメント D とエリア ABC に分けて考える。ここで，エリア ABC とは，セグメント A，セグメント B，セグメント C を含むエリアを指す。

セグメント D のネットワークアドレスは「172.16.1.64/26」である。エリア ABC のアドレス空間はセグメント D と重複しないので，これに割り当てることのできるアドレス空間は，「172.16.1.0/26」「172.16.1.128/26」「172.16.1.192/26」となる。

次に大きいアドレス空間をもつセグメント B に着目し，エリア ABC をセグメント B とエリア AC に分けて考える。ここで，エリア AC とは，セグメント A，セグメント C を含むエリアを指す。

セグメント B のネットワークアドレスは「172.16.1.32/27」である。エリア AC のアドレス空間はセグメント B と重複しないので，これに割り当てることのできるアドレス空間は，「172.16.1.0/27」「172.16.1.128/26」「172.16.1.192/26」となる。

ここまでの考察でおおよそ見通しが立ったので，選択肢に挙げられたアドレス空間の中から，セグメント A に割り当てることのできるものを導いてみよう。

選択肢アのアドレス空間は「172.16.1.0/25」である。これは，セグメント D のアドレス空間を含んでおり，エリア AC に割り当てることのできるアドレス空間とは異なっている。したがって，セグメント A に割り当てることができない。

選択肢イのアドレス空間は「172.16.1.128/25」である。これは，エリア AC に割り当てることができる。しかし，セグメント C のアドレス空間を含んでいるので，セグメント A に

割り当てることができない。

選択肢ウのアドレス空間は「172.16.1.128/26」である。これは，エリア AC に割り当てることができる。しかも，セグメント C のアドレス空間を含んでいない。したがって，セグメント A に割り当てることができる。

選択肢エのアドレス空間は「172.16.1.192/26」である。これは，エリア AC に割り当てることができる。しかし，セグメント C のアドレス空間を含んでいるので，セグメント A に割り当てることができない。

以上より，正解は選択肢**ウ**となる。

問 11：正解ア

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。距離ベクタ型とは，経由するルータのホップ数が最小の経路を選択する方式である。

RIP では，ホップ数が 15 を超える経路は，経路選択の対象から除外する仕組みになっている。言い換えるなら，宛先に到達可能なホップ数は，15 が最大になる。よって，正解は選択肢**ア**となる。

問 12：正解エ

ア：ToS フィールド（RFC791），または DiffServ（RFC2474）による優先制御を説明したものである。

イ：RSVP には，遠隔制御する機能はない。

ウ：RTP を説明したものである。

エ：**正解**。RSVP は，IP ネットワークにおいて，ホスト間通信の伝送帯域を予約する仕組みをもつプロトコルであり，ホスト間のリアルタイム通信を実現する。

問 13：正解ア

サブネットマスクが 16 進数の FFFFFF80 なので，ホストアドレス部は下位 7 ビットとなる。すなわち，ホストアドレス部のアドレス空間には，2^7（= 128）個のアドレスが存在する。

このうち，ホストアドレス部のビットがすべて 0 になるアドレスは，サブネットワーク自身のネットワークアドレスを表すため，ホストに割り当てることができない。

ホストアドレス部のビットがすべて 1 になるアドレスは，サブネットワーク内のブロード

キャストアドレスを表すため，ホストに割り当てることができない。

したがって，ホストに割り当てることができるのは，$2^7 - 2$（＝ 126）個のアドレスとなる。よって，正解は選択肢**ア**となる。

問 14：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 15：正解イ

国際化ドメイン名（IDN：Internationalized Domain Name）とは，ドメイン名に，漢字やアラビア文字をはじめとする ASCII 以外の文字を使えるようにする規格である。

IDN は，従来の ASCII 文字からなるドメイン名の名前解決と互換性を保っている。

クライアント側で IDN の名前解決を問い合わせるとき，一定の規則に従って，ASCII 文字だけからなる文字列のドメイン名に変換する。この結果，従来のドメイン名と同じ範疇の文字列になる。名前解決の問合せ先となる DNS サーバでは，その変換後の ASCII 文字だけからなるドメインで登録されている。

この仕組みにより，クライアントとサーバ間の通信，及び，サーバ側の名前解決の処理は，従来どおりとなる。

よって，正解は選択肢**イ**となる。

問 16：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 17：正解イ

ア：ディジタル証明書の規格は X.509 である。

イ：**正解**。ディジタル証明書に当てはまる記述である。

ウ：ディジタル証明書は，申請者の公開鍵に対して認証局が電子署名したものである。

エ：ルート認証局は，下位層の認証局の公開鍵に対してディジタル証明書を発行する。その際，ルート認証局の秘密鍵で電子署名する。

問 18：正解イ

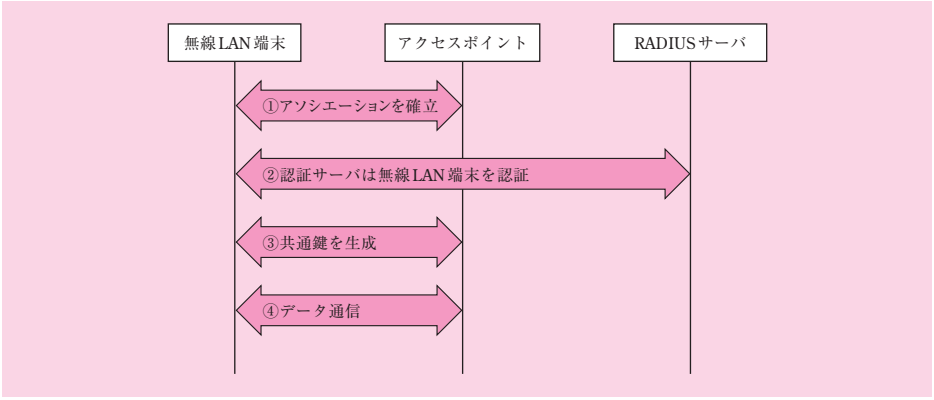
本問は，利用者認証とアクセス制御に IEEE802.1X と RADIUS を使用する場合の実装方法を問うている。まず，IEEE802.1X と RADIUS を使用したときの，認証とアクセス制御のシーケンスについて解説する。次いで，解を導こう。

●認証とアクセス制御のシーケンス

無線 LAN 環境で IEEE802.1X 認証を導入すると，認証に成功した端末だけが，アクセスポイントを経由したデータ通信を行えるようになる。

IEEE802.1X と RADIUS を使用したときの，認証とアクセス制御の一般的なシーケンスは，おおよそ次のとおりである。

① 無線 LAN 端末とアクセスポイントの間でアソシエーションが確立される。
② RADIUS サーバは無線 LAN 端末を認証する。アクセスポイントは，両者のやり取りを中継する。
③ 認証に成功すると，アクセスポイントは，無線 LAN 端末との間で共通鍵を生成する。
④ 無線 LAN 端末は，アクセスポイントを経由したデータ通信を行う。その際，③で生成した共通鍵で通信を暗号化する。



図：IEEE802.1X 認証の動作シーケンス

ここで，IEEE802.1X 認証の処理が行われているのは，項番②である。

なお，共通鍵を生成する処理である項番③は，本問で問われているわけではないが，参考までに掲載した。無線 LAN のセキュリティの規格である IEEE802.11i は，認証（項番②）と暗号化（項番③）を規定している。IEEE802.1X 認証を導入するときは暗号化も含めて IEEE802.11i に対応するのが一般的である。

IEEE802.1X 認証を利用しない場合（より正確に言うと，IEEE802.11i に対応しない場合），項番①でアソシエーションを確立したら，すぐに項番④で通信を行える状態になる。

●解の導出

項番②の処理を行うには，アクセスポイントが，IEEE802.1X 認証に対応した機能をもっていなければならない。この機能を実装した機器のことを，IEEE802.1X 規格の用語で「オーセンティケータ」と呼ぶ。オーセンティケータがもつべき機能には，項番②のやり取りを中継すること，認証が成功するまでは項番④の通信を許可しないこと，などがある。

更に，項番②の処理を行うには，無線 LAN 端末が，RADIUS クライアントの機能をもっていなければならない。

よって，正解は選択肢**イ**となる。

なお，IEEE802.1X について，詳しくは本書の第 4 章「4.4.3　IEEE802.1X」を参照していただきたい。

問 19：正解ウ

ア：ICANN（The Internet Corporation for Assigned Names and Numbers）の説明である。

イ：IETF（The Internet Engineering Task Force）の説明である。

ウ：**正解**。CSIRT（Computer Security Incident Response Team）の説明である。

エ：ハクティビストの説明である。

問 20：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を実際に動作させてその挙動を観察し，ウイルスによく見られる行動を起こ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，実際に動作させ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 21：正解ウ

ア，エ：DKIM，SPF は，いずれも送信ドメイン認証の仕組みである。

送信ドメイン認証とは，送信者メールアドレスに含まれるドメイン名の正当性を確認する仕組みであり，受信側サイトのメールサーバが，メールの受信時に実行する。

・DKIM

メールの送信時，送信側サイトのメールサーバは，メール全体（ヘッダと本文）に対する電子署名を作成し，メールヘッダに格納しておく。そして，メールの受信時，受信側サイトのメールサーバは，メールヘッダ中の送信者メールアドレスから送信ドメインを抽出し，同ドメインの DNS サーバから公開鍵を取得する。これを用い，付与された署名を復号することで認証を行う。

・SPF

ドメイン所有者は，DNS サーバの SPF レコード又は TXT レコードに，同サイトのメールサーバの IP アドレスを登録しておく（SPF が規定する書式に則って記述する）。メールの受信時，受信側サイトのメールサーバは，エンベロープ From から送信ドメインを抽出し，当該ドメインの権威サーバに問い合わせて，同レコードを確認することで認証を行う。

イ：OP25B（Outbound Port25 Blocking）とは，ISP が，個人利用者に対し，ISP 指定のメールサーバを使用してメールを送信するように規制する仕組みである。

ウ：**正解**。POP before SMTP とは，SMTP サーバが，認証に成功した端末から，一定時間に限ってメールの送信を許可する仕組みである。

利用者は，SMTP の送信に先立って POP の受信を行う。POP はパスワード認証の

仕組みを備えているが，この POP 受信はその認証を行うことを目的としている。認証に成功したとき，一定時間だけ，SMTP サーバは，利用者端末の IP アドレスを送信元とする STMP の送信を受け付ける。

問 22：正解エ

メモリインタリーブは，主記憶の連続したメモリ領域を複数の領域（バンク）に分けておき，連続したメモリ領域を同時にアクセスできるようにした高速化方式である。

ア：仮想記憶の説明である。
イ：キャッシュメモリの説明である。
ウ：DMA（Direct Memory Access）の説明である。

問 23：正解エ

端末における電文の送信開始から受信完了までの所要時間は，次の三つの時間の合計となる。

①送信時間：端末からホストコンピュータへ電文を送信する時間
②処理時間：ホストコンピュータでトランザクションを処理する時間
③受信時間：端末がホストコンピュータから電文を受信する時間

問題本文に示された，伝送処理やトランザクション処理に関わるパラメータは，次のとおりである。このパラメータに基づき，前記の時間を一つずつ求め，最後に合計する。

表：伝送処理やトランザクション処理のパラメータ

パラメータ	値
送信電文長	400 バイト
受信電文長	600 バイト
回線速度	1×10^6bps
伝送効率	0.8
トランザクションの処理時間	40×10^{-3} 秒
無視できる時間	ホストコンピュータでの処理待ち時間 伝送制御のための処理時間

①送信時間

送信時間は，次の式で求まる。

$$送信時間 = \frac{送信電文長}{回線速度 \times 伝送効率}$$

パラメータを代入し，送信時間を算出する。

$$送信時間 = \frac{400 \times 8[ビット]}{1 \times 10^{6}[bps] \times 0.8}$$
$$= 4 \times 10^{-3}[秒]$$

②処理時間

問題本文に示されているとおり，40×10^{-3} 秒である。

③受信時間

受信時間は，次の式で求まる。

$$受信時間 = \frac{受信電文長}{回線速度 \times 伝送効率}$$

パラメータを代入し，受信時間を算出する。

$$受信時間 = \frac{600 \times 8[ビット]}{1 \times 10^{6}[bps] \times 0.8}$$
$$= 6 \times 10^{-3}[秒]$$

●解の導出

端末における電文の送信開始から受信完了までの所要時間は，前記①～③の時間の合計である。したがって，

$$所要時間 = 4 \times 10^{-3} + 40 \times 10^{-3} + 6 \times 10^{-3}[秒]$$
$$= 50 \times 10^{-3}[秒]$$

となる。よって，正解は選択肢**エ**となる。

問 24：正解ア

エラー埋込み法では，埋め込まれたエラー数とその発見数の比は，潜在エラー数とその発見数の比に等しいと仮定する。これを式で表したのが次式である。

$$\frac{\text{埋め込まれたエラーの発見数}}{\text{埋め込まれたエラー数}} = \frac{\text{潜在エラーの発見数}}{\text{潜在エラー数}}$$

埋め込まれたエラーの発見数を m，発見された総エラー数を n とおくと，潜在エラーの発見数は，n − m となる。

埋め込まれたエラー数を S，潜在エラー数を T とおき，この式に代入すると次式を得る。

$$\frac{m}{S} = \frac{n - m}{T}$$

よって，正解は選択肢**ア**となる。

問 25：正解ウ

リバースエンジニアリングとは，プログラムの実行ファイルからソースコードを生成し，コードの仕様や構造を明らかにする技術である。よって，正解は選択肢**ウ**となる。

ア：ソースコードの自動生成技術の説明である。
イ：リファクタリングの説明である。