令和６年度 春期 午前Ⅱ問題の解答・解説

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

問１：正解ウ

BGP-4 は，AS（Autonomous System：自律システム）間を接続するダイナミックルーティングプロトコルであり，経路ベクトル型が採用されている。AS とは，同一の管理ポリシによって管理されるネットワーク群であり，2 オクテット又は 4 オクテットの AS 番号によって識別される。よって，正解は選択肢**ウ**となる。

ア：OSPF のエリアに当てはまる記述である。Router-LSA は，OSPF が使用する LSA（Link-State Advertisement）の一種である。Router-LSA は，同一エリア内のルータに伝播する。

イ：OSPF では，Neighbor の確立には Hello プロトコルが用いられる。Neighbor を確立した後も，相互に死活監視するために定期的に Hello パケットを交換する（その間隔はネットワークタイプによって異なっている。ブロードキャスト・マルチアクセスネットワークでは 10 秒間隔である）。

Neighbor が確立された後に Adjacency（隣接関係）が確立されるが，ネットワークタイプによって Adjacency を確立する方法が異なっている。point-to-point ネットワークでは，Neighbor を確立したルータ間で Adjacency を確立する。マルチアクセスネットワークでは，全てのルータ間でフルメッシュに Adjacency を確立しない。同一エリアで同一サブネットワーク内の，ルータと DR（Designate Router：代表ルータ）との間，及び，ルータと BDR（Backup Designate Router）との間でのみ，Adjacency を確立する。したがって，マルチアクセスネットワークでは，Adjacency の確立に先立ち，DR，BDR を選出する必要がある。Neighbor を確立する際の Hello プロトコルの交換を通して，DR と BDR がサブネットワークごとに定まる仕組みになっている。

Adjacency を確立するルータ間では，LSDB（Link State Database）の同期を取る必要がある。そのため，Adjacency の確立に際し，まず Database Description パケットを用いて LSDB の情報を交換する。次いで，自分がもっていない LSA を相手に要求することで LSDB を同期させる。

Adjacency を確立したら，ネットワークの構成が変更された場合，ただちに LSA を交換して LSDB の同期を維持する。なお，ネットワークの構成が変更されなくても，30 分間隔で LSA を交換する。

エ：BGP-4 は，リンクステート型ではなく，経路ベクトル型が採用されている。リンクステート型を採用しているダイナミックルーティングプロトコルには，OSPF などがある。

問２：正解ア

CS-ACELP（G.729）は，1 秒間の音声信号を 8k ビットに符号化する。したがって，20 ミリ秒間の音声信号は，

0.02［秒］× 8k［ビット／秒］= 160［ビット］= 20［バイト］

となる。よって，正解は選択肢**ア**である

問３：正解イ

呼損率表から必要回線数を求めるには，まず，呼量を計算する。

$$\text{呼量［アーラン］} = \frac{\text{呼数} \times \text{平均保留時間}}{\text{単位時間}}$$

その後，呼損率表から，計算した呼量を満たす回線数を求める。

呼数は，問題文に「1 時間当たりの平均通話回数が 60」と記述されているので，60［回］である。さらにこの記述から，単位時間は 1 時間であることが分かる。

平均保留時間は，問題文に記述されているとおり，120 秒である。

したがって，呼量は次式より求まる。

$$\text{呼量［アーラン］} = \frac{60［回］ \times 120［秒］}{3600［秒］}$$

$$= 2［アーラン］$$

呼損率表を見ると，呼損率 0.1 のとき 2［アーラン］を満たす回線数は，呼損率 0.1 のとき呼量が 2.045［アーラン］になる 4 回線である。

よって，正解は選択肢**イ**となる。

問４：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
可変長サブネットマスクへの対応可否	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。

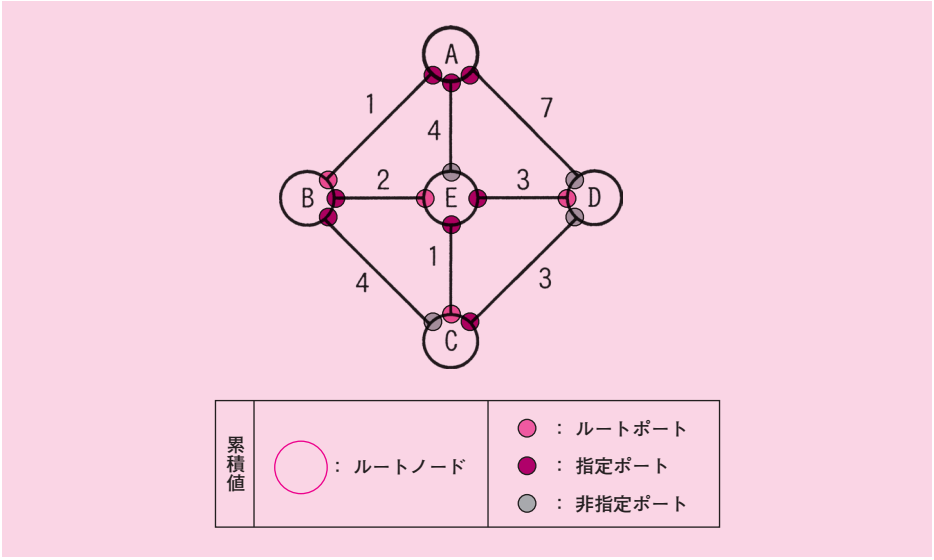
イ：**正解**。OSPF に当てはまる特徴である。ルータは，自分のリンク状態及び受信したリンク状態の情報を管理するデータベースをもつ。この情報に基づき，ルータはルーティングテーブルを生成する。

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 5：正解エ

5 個のノード A ～ E から構成される図のネットワークにおいて，A をルートノードとするスパニングツリーを構築したとき，ポート状態は次の図のようになる。



図：ネットワークのポート状態

本問が問うている「隣接するノード」とは，ノード間のリンクがブロッキングポートにより遮断されていないものを指している。選択肢ア～エの中でこれに該当するものは，選択肢**エ**の「D と E」である。よって，これが正解となる。

なお，スパニングツリーを構築する手順や各ポートの状態について，詳しくは付録 PDF の第 6 章「6.2.6 スイッチの冗長化」の「●スパニングツリーを構成する手順」を参照していただきたい。

問 6：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，詳しくは付録 PDF 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 7：正解エ

マルチキャストアドレスブロックは，クラス D に相当する。すなわち，アドレスの上位 4 ビットが「1110」であり，通常表記で 224.0.0.0 ～ 239.255.255.255 の範囲内のものである。したがって，先頭の 4 ビットを除いた残りの 28 ビットが，実質上，マルチキャストグループを識別するために用いられている。

よって，正解は選択肢**エ**となる。

ア：127.0.0.1 はループバックアドレス用として予約された IP ユニキャストアドレスである。

イ：192.168.1.255 は，ネットワーク「192/168/1.0/24」の全ホストを宛先とするブロードキャストアドレスである。このように，あるネットワークの全ホストを宛先とするブロードキャストアドレスを，ディレクテッドブロードキャストアドレスと呼ぶ。

ウ：IP マルチキャストアドレスの上位 4 ビットが「1111」のアドレスは，マルチキャストアドレスではなく，クラス E のアドレスに相当する。RFC1112 は，クラス E のアドレスを「future addressing modes」のために予約すると規定している。

問８：正解エ

ア：CHAP（Challenge Handshake Authentication Protocol）は，PPP のユーザ認証方式の一つであり，チャレンジレスポンス方式を採用している。

イ：PAP（Password Authentication Protocol）は，PPP のユーザ認証方式の一つであり，ID とパスワードを平文で送信する。

ウ：PPTP（Point to Point Tunneling Protocol）は，データリンク層のパケットである PPP パケットを，GRE でカプセル化し，さらに IP でカプセル化するプロトコルである。

エ：**正解**。RADIUS（Remote Access Dial In User Service）は，認証（Authentication），認可（Authorization），アカウンティング（Accounting）の三つの機能を提供するプロトコルである。RAIDUIS は，リモートアクセス環境において，認証情報やアカウンティング情報をやり取りするために用いられる。

問９：正解ア

TCP 通信のデータ転送フェーズでデータを送信する際，ホストが送信するパケットのシーケンス番号は，次式を満たす。

シーケンス番号　＝
　自ホストが直前に送信したパケットのシーケンス番号　＋
　自ホストが直前に送信したパケットのペイロード（TCP セグメント）のバイト数

この式は，正常にやり取りが行われている限り，パケットを連続転送するか否かに関わらず，常に満たされる。

よって，正解は選択肢**ア**となる。

イ：シーケンス番号と受信確認番号はランダム値から開始される。この値は，コネクション確立フェーズで決定される。

ウ，エ：返信パケットに格納された受信確認番号には，「相手ホストが『次に受信すべきシーケンス番号』として識別しているもの」が格納されている。それゆえ，自ホストは，返信された受信確認番号と，次に自分が送信するシーケンス番号が同じであることを確認すれば，正常に通信が行われていることを確認することができる。

問 10：正解エ

選択肢のうち，TCP と UDP 両方のヘッダに存在するものは，送信元ポート番号である。よって，正解は選択肢**エ**となる。

ア：宛先 IP アドレスは，IP ヘッダに存在する。
イ：宛先 MAC アドレスは，MAC ヘッダに存在する。
ウ：生存時間（TTL）は，IP ヘッダに存在する。

TCP ヘッダ，UDP ヘッダについて，詳しくは本書の第 3 章「3.3.2　TCP ヘッダ」，「3.3.3 UDP ヘッダ」を参照していただきたい。

問 11：正解ウ

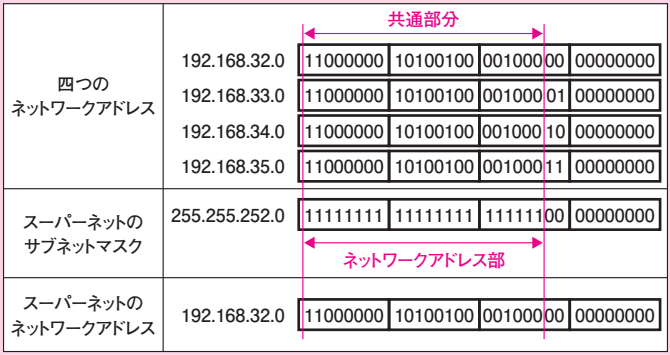
IPv4 ネットワークで使用される IP アドレス a は，ネットワークアドレス部とホストアドレス部の二つから構成されている。サブネットマスク m は，ネットワークアドレス部のビットが「1」に，ホストアドレス部のビットが「0」になっているので，次式からネットワークアドレスとホストアドレスをそれぞれ求めることができる。

ネットワークアドレス　＝　a & m
ホストアドレス　　＝　a & ~m

よって，ホストアドレスを求める式は選択肢**ウ**となり，これが正解となる。

問 12：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 13：正解イ

ホストの IP アドレスとして使用できるものは，クラス A ～ C に属するものとなる。ただし，下記の条件を満たすものを除く。

- ホストに割り当てることができない，特別な用途に予約されている。例えば，ループバックアドレス（127.0.0.0 ～ 127.255.255.255）などである。
- ホスト部が，ネットワークアドレス（全ビットが 0）であるか，又は，ブロードキャストアドレス（全ビットが 1）である。

ア：127.16.10.255/8 は，クラス A（0.0.0.0 ～ 127.255.255.255）に属するが，ループバックアドレス用に予約されたアドレスブロックにも属している。したがって，ホストの IP アドレスとして使用できない。

イ：**正解**。172.16.10.255/16 は，クラス B（128.0.0.0 ～ 191.255.255.255）に属する。これは，RFC1918 によりプライベート IP アドレス用に予約されていたアドレスブロックに属するが，ホストに割り当てることができる。ホスト部は下位 16 ビットであり，ネットワークアドレスでもなく，ブロードキャストアドレスでもない。したがって，ホストの IP アドレスとして使用できる。

ウ：192.168.255.255/24 は，クラス C（192.0.0.0 ～ 221.255.255.255）に属する。これは，RFC1918 によりプライベート IP アドレス用に予約されていたアドレスブロックに属するが，ホストに割り当てることができる。ホスト部は下位 8 ビットであり，全ビットが 1 となるため，ブロードキャストアドレスである。したがって，ホストの IP アドレスとして使用できない。

エ：224.168.10.255/8 は，クラス D（224.0.0.0 ～ 239.255.255.255）に属する。これは，マルチキャストアドレスに使用される。したがって，ホストの IP アドレスとして使用できない。

問 14：正解イ

IPv6 に対応した RIP は RIPng であり，IPv6 に対応した OSPF は OSPFv3（バージョン 3）である。よって，正解は選択肢**イ**となる。

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：正解ア

Web コンテンツを提供する際，CDN（Content Delivery Network）を利用することで，コンテンツの配信サーバを各地に分散配置することができる。その結果，ある拠点の配信サーバが DDoS 攻撃を受けて配信サービスを提供できなくなっても，別の拠点の配信サーバで配信サービスを継続することができ，DDoS 攻撃の影響を軽減することができる。

よって，正解は選択肢**ア**となる。

これ以外の選択肢は，以下の説明にあるように，攻撃対象が配信サーバではないため，本問が問うている「CDN を利用することによって影響を軽減できる脅威」に該当しない。

イ：Man-in-the-Browser 攻撃は，ブラウザが中間者となる形態の中間者攻撃（Man-in-the-middle 攻撃）である。
中間者攻撃とは，クライアントとサーバ間の通信経路上に攻撃者が割り込み，攻撃者を経由して通信を行うように仕向けることで，両者間の通信の傍受や改ざんを行う攻撃である。攻撃者は，クライアントに対してはサーバになりすまし，サーバに対してはクライアントになりすますことで，両者間の通信を中継しつつ，傍受や改ざんを密かに実行する。
Man-in-the-Browser 攻撃は，攻撃者がブラウザを乗っ取ることで中間者攻撃を成立させ，当該ブラウザを用いた Web アクセス通信の傍受や改ざんを行う。

ウ：パスワードリスト攻撃は，あるユーザーがあるサイトのログインに使用している ID とパスワードの組を入手し，別のサイトのログインにそれを使用することで当該利用者になりすます攻撃である。

エ：リバースブルートフォース攻撃は，パスワードを固定した上で ID 文字列を総当たり的に試行して不正にログインする攻撃である。使用するパスワードには，ユーザーが安易に設定しがちなパスワードが用いられる。
これとよく似た名称をもつ攻撃が，昔からよく知られているブルートフォース攻撃である。ブルートフォース攻撃が ID を固定した上でパスワード文字列を総当たり的に試行するのに対し，本問で問われているリバースブルートフォース攻撃は，パスワードを固定した上で ID 文字列を総当たり的に試行する。
このように，ブルートフォース攻撃と比べたとき，固定するものと総当たり的に試行するものが逆になっているので，リバースブルートフォース攻撃と呼ばれている。

問 17：正解エ

UNICODE は，右から左に向かって文字列を表記するアラビア語等の言語に対応するため，RLO（Right-to-Left Override）制御文字「U+202E」を定義している。RLO 制御文字に続く文字列は，その表示順が左右逆になる。

これを悪用することで，OS やプログラムがファイル名を表示する際，その拡張子を偽装することができる。

例えば，「aaatxt.exe」というファイル名をもつファイルがあるとしよう。このファイルは，拡張子が「exe」であるから，Windows の実行ファイルである。この中の「txt.exe」という

部分だけ逆順に表示させるため，「txt.exe」の直前に RLO 制御文字を挿入すると，その表示は「aaaexe.txt」になる。この結果，拡張子が「txt」に見えるから，あたかもテキストファイルであるかのように偽装することができる。

しかし，表示が変わっただけであり，ファイル名は「aaatxt.exe」のままである。つまり，拡張子が「exe」であることに変わりはない。それゆえ，ダブルクリック等の操作により，OS はこのファイルを実行してしまう。

したがって，RLO を利用した手口の説明として適切なものは，選択肢エの「文字の表示順を変える制御文字を利用して，ファイル名の拡張子を偽装する」である。よって，正解は選択肢**エ**となる。

ア：“マルウェアに感染している”旨の広告を表示するように組み込まれたアドウェアの説明，又は，その種の広告を表示しているウェブサイトの説明である。

イ：ハニーポッドの説明である。

ウ：SNMP Trap メッセージの説明である。

問 18：正解イ

サイドチャネル攻撃とは，暗号化処理を行っている装置に対し，暗号化処理に要する処理時間や消費電力を測定するなどして，秘密情報を推定する攻撃である。

よって，正解は選択肢**イ**となる。

ア：キーロガーとは，キーボード入力を記録するソフトウェア又はハードウェアデバイスである。攻撃者によってキーロガーが仕掛けられていることを知らずに，住所氏名などの個人情報やパスワードなどの秘密情報を入力すると，攻撃者にその情報が漏えいしてしまう。

ウ：スミッシングとは，SMS（ショートメッセージサービス）を利用したフィッシング詐欺である。smishing（スミッシング）という名称は，SMS と phishing（フィッシング）から造られた。

SMS は携帯電話番号宛てに短いメッセージ（最大 670 文字）を送信するサービスである。メールを利用したフィッシングと同様，SMS の本文には，攻撃者が用意したサイトのリンクと共に，これをクリックさせようとする誘い文句が書かれている。

アクセス先がどのようなサイトであり，そこで何をさせようと企図しているかは，攻撃者により様々である。

例えば，ネット通販や銀行など著名なサイトを偽装し，ID とパスワードを入力させることを企図しているかもしれない。他には，ウイルスに感染したと錯誤させるメッセージを送りつけてサイトに誘導し，ウイルス対策ソフトであるかのように詐称したマルウェアを携帯端末にダウンロードさせて感染させることによりこれを乗っ取り，個人情報や秘密情報を収集することを企図しているかもしれない。

エ：中間者攻撃（Man in the Middle 攻撃）とは，クライアントとサーバ間の通信経路上に攻撃者が割り込むことで，両者間の通信内容を傍受する攻撃である。攻撃者は，クライアントに対してはサーバになりすまし，サーバに対してはクライアントになりすますことで，両者間の通信を中継し，その通信内容を傍受することができる。

問 19：正解エ

なりすましメールの対策には様々なものがあるが，その一つが，送信ドメイン認証である。これは，メール送信者のドメインの真正性を検証する仕組みをもつ技術であり，これを用いてなりすましメールを検出することで，隔離や廃棄などの対策を講ずることができる。

送信ドメイン認証の代表的な方式として，SPF（Sender Policy Framework），DKIM（Domain Keys Identified Mail）の二種類がよく用いられている。両者を組み合わせた方式として，DMARC（Domain-based Message Authentication, Reporting & Conformance）がある。

選択肢エの SPF を実施するには，送信元ドメインの権威 DNS サーバの SPF レコードに，自ドメインがメール送信に使用するメールサーバの IP アドレスをあらかじめ登録しておく必要がある。これにより，自ドメインのメールサーバから，自ドメインのメールアドレスを送信元メールアドレスにもつメールを送信したとき，受信者が SPF レコードを取得してメールサーバの IP アドレスを確認することで，当該メールがなりすまされたものではないことを受信者に確認してもらうことができる。

よって，正解は選択肢**エ**となる。

送信ドメイン認証について，詳しくは本書の第 8 章「8.3.5 迷惑メール対策」の「●送信ドメインのなりすまし防止」を参照していただきたい。

ア：DMARC（Domain-based Message Authentication, Reporting & Conformance） は，送信ドメイン認証の SPF 方式と DKIM 方式を組み合わせ，かつ，DMRAC 独自の機能を追加した方式である。

DMARC 独自の機能の一つに，認証失敗時の処理方法をドメイン所有者が定義する，というものがある。その処理方法として，「何もしない」，「隔離」，「拒否」の 3 種類が標準化されている。しかし，「メールを送り返す」という処理方法は標準化さ

れておらず，不正確な記述であるため，誤った選択肢である。
DMARC は，認証結果のレポートをドメイン所有者に通知することができるので，送信元ドメインが不正な活動を把握し，必要な対策を講ずることができるようになる。

イ：IP25B（Inbound Port 25 Blocking）は，ISP が，自 ISP のメールサーバを宛先とし，自 ISP 以外の IP アドレスを送信元とする SMTP 通信（ポート番号 25/TCP）をブロックすることである。選択肢の記述は OP25B（Outbound Port 25 Blocking）を説明したものなので，誤りである。IP25B と OP25B を採用する ISP が増えることで迷惑メールの削減に貢献するが，IP25B がなりすましメール対策に直接効果があるとは言えない。

ウ：S/MIME（Secure MIME）は，メールにデジタル署名を付与する仕組みとして標準化された技術であり，デジタル署名が有する送信者認証（否認防止）を利用することでなりすましメールを検出することができる。
S/MIME はなりすましメール対策に有効な技術であるが，選択肢に記述された，デジタル署名の生成と検証に使用する鍵に関する説明が不正確であるため，誤った選択肢となる。正しい説明は，「自身の秘密鍵を使ってデジタル署名を生成」，「電子メール送信者の公開鍵を使ってデジタル署名を検証」となる。

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，インテグリティチェック法，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：インテグリティチェック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：正解ア

ア：**正解**。IPsec の通信モードをトンネルモードに指定すると，元の IP パケット全体をカプセル化することができる。さらに，IPsec プロトコルを ESP に指定すると，IPsec でカプセル化する際，暗号化することができる。

イ：IKE はポート番号 500 を用いる。なお，「IKE は IPsec の鍵交換のためのプロトコルであ（る）」という記述は正しい。

ウ：HMAC-SHA1 は，暗号化のアルゴリズムではなく，メッセージ認証のアルゴリズムである。

エ：IPsec の通信に先立ち，メッセージ認証や暗号化のアルゴリズムを決定するのに用いられるプロトコルは，IKE である。

問 22：正解ア

PCI Express（Peripheral Component Interconnect Express）は，マザーボードのバスの通信規格であり，シリアル転送方式を採用している。このシリアル転送はレーン単位で独立して行われているが，１個のスロットは複数のレーンを有しているので，周辺機器は同時に複数のレーンを使用してデータを転送することができる。

PCI Express の転送レートは世代ごとに異なり，おおむね以下のとおりである。

表：PCI Express の 1 レーンあたりの転送レート

規格	片方向	双方向
PCI Express 3.0（Gen3）	1G バイト / 秒	2G バイト / 秒
PCI Express 4.0（Gen4）	2G バイト / 秒	4G バイト / 秒
PCI Express 5.0（Gen5）	4G バイト / 秒	8G バイト / 秒
PCI Express 6.0（Gen6）	8G バイト / 秒	16G バイト / 秒

注）シリアル転送の符号化（NRZ 128b/130b 等）を実施したビット列の転送速度

この表から分かるとおり，Gen3 以降は，世代が 1 つ上がるたびに転送レートが 2 倍になっている。よって，正解は選択肢**ア**となる。

イ：PCI Express は後方互換性がある。

ウ：規格上の最大レーン数は世代によって異なり，Gen3 は最大 32 レーン，Gen4 ～ Gen6 は最大 64 レーンである。

エ：シリアル転送の符号化方式は世代によって異なり，Gen3 ～ Gen5 は NRZ 128b/130b，Gen6 は PAM-4 224b/256b である。

問 23：正解ア

ジョブの多重度が 1 であり，到着順にジョブが実行される。したがって，あるジョブが実行されている場合，他のジョブは待たされることになる。待っているジョブが複数あるときは，到着順に処理される。

与えられた表に従ってジョブ A ～ C を処理するとき，ジョブ実行のシーケンスは次の図のようになる。

単位 秒

ジョブ	到着時刻	処理時間（単独実行時）
A	0	5
B	2	6
C	3	3

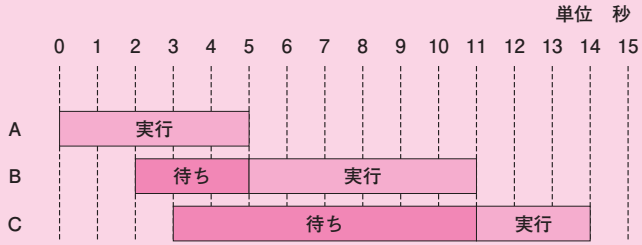


図　ジョブ実行のシーケンス

したがって，ジョブ C が到着する時刻は 3 であり，実行が終了する時刻は 14 である。ターンアラウンドタイムは，14 − 3 = 11 秒となる。よって，正解は選択肢**ア**となる。

問 24：正解ア

フールプルーフとは，ユーザの入力に対して確認のメッセージを出力したり，決められた順序で入力しなければ動作しないようにしたりして，不特定多数の人が操作しても誤動作が起こりにくいように設計することである。

問題文の〔方針〕には，「不特定多数の人が使用するプログラムには，……データチェックの機能を組み込む。（プログラムが処理できるデータの）前提条件を満たしていないデータが入力されたときは，エラーメッセージを表示して再入力を促す」と記述されている。

このような方針に基づく設計は，フールプルーフに該当する。よって，正解は選択肢**ア**となる。

イ：フェールセーフとは，システムの一部に故障や異常が発生したとき，データの消失，装置の損傷及びオペレータに対する危害を減じるよう，常に安全側にシステムを制御することである。

ウ：フェールソフトとは，装置の一部が故障しても，システムの全面的なサービス停止にならないようにすることである。

エ：フォールトトレランスとは，システムを運用中でも故障部分の修復を可能にしたり，システムのコンポーネントを冗長構成にしたりすることで，システムの信頼性を高めることである。

問 25：正解エ

バグトラッキングシステムとは，選択肢エに記述されているとおり，「発見されたバグの内容，バグが発生したソフトウェアのバージョンなどを記録し，その修正計画や修正履歴を管理する」システムである。

よって，正解は選択肢**エ**となる。

ア：デバッガに当てはまる説明である。

イ：テスティングフレームワークやテスト支援ツールに当てはまる説明である。

ウ：テスト工程で実施する品質管理に当てはまる説明である。