

問1 Ethernetフレームで、同一LAN上の転送先を識別するために最初に配置されるフィールドはどれか。

- ア．宛先MACアドレス
- イ．送信元IPアドレス
- ウ．TCPポート番号
- エ．FCS

正答：ア

4肢解説

ア：正しい。Ethernetフレーム先頭部には宛先MACアドレスがあり、受信対象の識別に用いられる。

イ：IPアドレスはネットワーク層のIPヘッダに含まれ、Ethernetフレームの先頭フィールドではない。

ウ：TCPポート番号はトランスポート層のTCPヘッダに含まれる。

エ：FCSは誤り検出用でフレーム末尾に配置される。

総合解説：Ethernetでは宛先MACアドレスと送信元MACアドレスを使ってデータリンク層の配送を行う。IPアドレスやTCP/UDPポート番号とは階層が異なる。

問2 Ethernet IIフレームのEtherTypeフィールドの主な役割はどれか。

- ア．フレームの送信時刻を記録する
- イ．上位層で運ばれているプロトコルを識別する
- ウ．送信元MACアドレスを暗号化する
- エ．スイッチのポート番号を指定する

正答：イ

4肢解説

ア：EtherTypeは時刻情報を保持するフィールドではない。

イ：正しい。EtherTypeはペイロードに格納されたIPv4やIPv6などのプロトコルを識別するために用いられる。

ウ：EtherTypeに暗号化機能はない。

エ：物理ポート番号を指定するためのフィールドではない。

総合解説：EtherTypeはフレーム内の上位プロトコルを識別する。代表例としてIPv4、ARP、IPv6などがある。

問3 EthernetフレームのFCSの目的として最も適切なものはどれか。

ア．宛先IPアドレスを決定する

イ．フレームを暗号化する

ウ．伝送中に生じたビット誤りを検出する

エ．再送回数を記録する

正答：ウ

4肢解説

ア：IPアドレスの決定はネットワーク層の処理であり、FCSの役割ではない。

イ：FCSは暗号化や秘匿化を行わない。

ウ：正しい。FCSはCRCに基づいて受信フレームの誤り検出に用いられる。

エ：Ethernet FCSは再送回数を保持するフィールドではない。

総合解説：FCSは誤りを訂正するのではなく、受信側がフレーム破損を検出するために利用する。

問4 L2スイッチがMACアドレステーブルを学習するとき、通常どの情報を利用するか。

ア．受信フレームの宛先MACアドレスだけ

イ．受信フレームの宛先IPアドレスだけ

ウ．TCPの送信元ポート番号

エ．受信フレームの送信元MACアドレスと受信ポート

正答：エ

4肢解説

ア：宛先MACアドレスは転送先決定に使うが、学習の基本は送信元MACアドレスである。

イ：通常のL2学習はIPアドレスではなくMACアドレスを基にする。

ウ：TCPポート番号はL2スイッチのMAC学習には用いない。

エ：正しい。スイッチは受信フレームの送信元MACアドレスを、そのフレームが到着したポートと対応付けて学習する。

総合解説：MACアドレステーブルは、送信元MACアドレスの観測によって動的に形成され、既知ユニキャスト転送の判断に使われる。

問5 L2スイッチが受信したユニキャストフレームの宛先MACアドレスをMACアドレステーブルで見つけられなかった。通常の動作として最も適切なものはどれか。

ア．受信ポート以外の同一VLAN内ポートへフラッディングする

イ．必ずフレームを破棄する

ウ．デフォルトゲートウェイへだけ送る

エ．全VLANの全ポートへ送る

正答：ア

4肢解説

ア：正しい。未知ユニキャストは通常、同一VLAN内で受信ポートを除く該当ポートへフラッディングされる。

イ：未知宛先だからといって通常ただちに破棄するわけではない。

ウ：L2スイッチは未知MACをIPデフォルトゲートウェイへ限定転送しない。

エ：VLANによるブロードキャストドメイン分離を越えて無条件に送ることはない。

総合解説：未知ユニキャスト、ブロードキャストなどはVLAN内でフラッディングされる。宛先が学習されると既知ユニキャストとして限定転送できる。

問6 EthernetのブロードキャストMACアドレスはどれか。

ア．00:00:00:00:00:00

イ．FF:FF:FF:FF:FF:FF

ウ．01:00:5E:00:00:01

エ．FE:80:00:00:00:00

正答：イ

4肢解説

ア：全ビット0はブロードキャストMACアドレスではない。

イ：正しい。全ビットが1のMACアドレスはEthernetブロードキャストアドレスである。

ウ：IPv4マルチキャストで使われるMACアドレス範囲の一例であり、ブロードキャストではない。

エ：IPv6リンクローカルのプレフィックス表記に似ており、EthernetブロードキャストMACではない。

総合解説：Ethernetブロードキャストは同一ブロードキャストドメイン内の全端末に届けるために使用される。

問7 スイッチと端末がポイントツーポイントで全二重Ethernet接続されている。このリンクに関する説明として適切なものはどれか。

- ア．送信と受信は必ず交互に行う
- イ．同一リンク上で衝突が頻発することを前提とする
- ウ．送受信を同時に行え、通常CSMA/CDによる衝突検出は不要である
- エ．トークンを取得した端末だけが送信できる

正答：ウ

4肢解説

- ア：全二重では同時送受信が可能である。
- イ：全二重ポイントツーポイント接続では衝突は前提としない。
- ウ：正しい。全二重のポイントツーポイントリンクでは衝突ドメインを共有せず、CSMA/CDを必要としない。
- エ：Ethernet全二重通信はトークンパッシング方式ではない。

総合解説：CSMA/CDは共有媒体の半二重Ethernetで衝突を扱う仕組みであり、現代のスイッチ型全二重Ethernetでは通常利用しない。

問8 ストアアンドフォワード方式のスイッチングの特徴として最も適切なものはどれか。

- ア．宛先MACアドレスを読む前に転送を開始する
- イ．必ずL3ルーティングを行ってから転送する
- ウ．受信フレームのFCSを確認できない
- エ．フレーム全体を受信してFCSなどを確認してから転送できる

正答：エ

4肢解説

- ア：宛先を判定できないため通常のフレーム転送として成立しない。
- イ：L2ストアアンドフォワードは必ずL3処理を行う方式ではない。
- ウ：全体受信するためFCS確認が可能である。
- エ：正しい。フレーム全体を受信してから転送するため、FCSを使った誤り確認が可能である。

総合解説：ストアアンドフォワードは誤りフレームの転送抑止に有利だが、フレーム全体を待つ分だけカットスルーより遅延が大きくなり得る。

問9 カットスルー方式のスイッチがストアアンドフォワード方式より低遅延になりやすい主な理由はどれか。

ア．フレーム全体の受信完了を待たず、宛先情報を得た段階で転送を開始できるため

イ．FCSを必ず修正してから送るため

ウ．IPルーティング計算を省略するからだけ

エ．送信速度を物理的に2倍へ変更するため

正答：ア

4肢解説

ア：正しい。フレームを全て蓄積する前に転送開始できるため、転送遅延を小さくしやすい。

イ：FCSの誤り訂正を行う仕組みではない。

ウ：L2転送方式の違いであり、主因は全フレーム受信を待たない点である。

エ：リンク速度そのものを倍にする方式ではない。

総合解説：カットスルーは低遅延が利点だが、フレーム末尾のFCSを受信する前に転送を始めるため、破損フレームを転送する可能性がある。

問10 端末を別のスイッチポートへ移動した後も古いIMACアドレス学習情報が長時間残ると、通信に影響する可能性がある。動的MACエントリのエージングの目的として適切なものはどれか。

ア．全てのフレームを暗号化する

イ．一定時間使われない古い対応付けを削除し、トポロジ変化へ追従しやすくする

ウ．IPアドレスを自動配布する

エ．STPのルートブリッジを固定する

正答：イ

4肢解説

ア：エージングは暗号化機能ではない。

イ：正しい。動的エントリを期限切れにすることで、端末移動などによる古い学習情報を解消できる。

ウ：IPアドレス配布はDHCPなどの役割である。

エ：MACエージングはSTPのルート選出を制御しない。

総合解説：スイッチの動的MAC学習は環境変化に応じて更新される。エージングは不要になった古いエントリを除去する仕組みである。

問11 冗長化のためL2スイッチ間を複数経路で接続したところ、STPなどのループ防止機能が動作していなかった。ブロードキャストフレームについて最も起こりやすい現象はどれか。
ア．各フレームが1周すると自動的にTTL=0で破棄される
イ．ループがあってもブロードキャストは必ず1台だけに届く
ウ．フレームがループし続けて複製され、ブロードキャストストームを起こす
エ．L2ループはDNSサーバだけに影響する
正答：ウ

4肢解説

ア：Ethernetフレーム自体にIP TTLのようなフィールドはない。
イ：ブロードキャストは同一VLAN内へフラディングされ、ループがあると増殖し得る。
ウ：正しい。EthernetフレームにはIPのTTLのようなL2ループを自動終息させるホップ数機構がないため、ループで増殖し得る。
エ：ネットワーク全体の帯域やスイッチCPU、MAC学習を不安定化させる可能性がある。
総合解説：L2冗長経路にはSTP/RSTPなどで論理的なループを抑止する必要がある。ループはブロードキャストストームやMACフラッピングを引き起こす。

問12 同一のMACアドレス値が異なるVLANに存在する可能性を考慮したL2スイッチの転送学習として、設計上最も妥当な考え方はどれか。
ア．全VLANを常に一つのブロードキャストドメインとして扱う
イ．MACアドレスが同じなら必ず同じ物理ポートへ転送する
ウ．VLAN情報はL3ルータだけが使い、L2スイッチは参照しない
エ．MACアドレスだけでなくVLANの文脈も含めて転送先を管理する
正答：エ

4肢解説

ア：VLANによる論理分離の目的に反する。
イ：異なるVLANでは同じMAC値でも別の転送文脈として扱える。
ウ：VLANタグやVLAN所属はL2ブリッジングそのものに関係する。
エ：正しい。VLANは独立したブリッジドメインを形成するため、転送判断ではVLAN文脈を区別する必要がある。
総合解説：VLAN対応ブリッジでは、フレーム転送データベースをVLANなどのブリッジング文脈に関連付けて扱う。

問13 VLANを利用する主な目的として最も適切なものはどれか。

ア．物理配線に依存せず、L2のブロードキャストドメインを論理的に分割する

イ．IPアドレスを暗号化する

ウ．全端末を必ず同じサブネットに統合する

エ．ルータを不要にして全VLAN間通信を自動許可する

正答：ア

4肢解説

ア：正しい。VLANは同一の物理スイッチ群上でも論理的にブロードキャストドメインを分離できる。

イ：VLANは暗号化機能ではない。

ウ：VLANはむしろ論理的な分離に用いる。

エ：異なるVLAN間通信には通常L3機能が必要である。

総合解説：VLANはセグメント分離、ブロードキャスト範囲の制御、組織単位の論理構成などに利用される。

問14 IEEE 802.1QタグをEthernetフレームへ付加する主な目的はどれか。

ア．送信元IPアドレスを圧縮する

イ．フレームが属するVLANなどの情報を識別できるようにする

ウ．TCPの再送制御を行う

エ．光信号の波長を指定する

正答：イ

4肢解説

ア：802.1QタグはIPアドレス圧縮を行わない。

イ：正しい。802.1QタグにはVLAN識別子などが含まれ、複数VLANのフレームを同一リンクで扱える。

ウ：TCP再送はトランスポート層の機能である。

エ：VLANタグは物理層の波長制御情報ではない。

総合解説：802.1QタグはブリッジドネットワークでVLAN識別を行うための代表的な仕組みである。

問15 L2スイッチを冗長接続したネットワークでSTPを利用する主な目的はどれか。

ア．全リンクで必ず同時に同じフレームを転送する

イ．IPアドレスを自動設定する

ウ．物理的な冗長性を残しつつ、論理的なループを防止する

エ．BGPのAS_PATHを短縮する

正答：ウ

4肢解説

ア：それではL2ループが発生しやすくなる。

イ：IPアドレス設定はSTPの役割ではない。

ウ：正しい。STPは一部リンクを転送に使わない状態にしてループのない論理トポロジを作る。

エ：STPはL2のループ防止技術でありBGP属性を操作しない。

総合解説：STPはブロードキャストストームやMACアドレス学習の不安定化を防ぐため、冗長L2トポロジからループのない転送木を形成する。

問16 STPで複数スイッチのブリッジ優先度が同じ場合、ルートブリッジの選出で次に比較される情報はどれか。

ア．IPアドレスのTTL

イ．TCPポート番号

ウ．DNSサーバの優先順位

エ．MACアドレスを含むブリッジIDの残りの部分

正答：エ

4肢解説

ア：STPのルート選出にIP TTLは使わない。

イ：TCPポート番号はL2ブリッジ選出と無関係である。

ウ：DNS設定はSTPルート選出に影響しない。

エ：正しい。ルートブリッジは最小のブリッジIDで決まり、優先度が同じならMACアドレス部分などで差がつく。

総合解説：STPではブリッジIDを比較してルートブリッジを決定する。設計では意図したスイッチをルートにするため優先度を調整する。

問17 非ルートブリッジ上で、ルートブリッジへ到達する最小コストの経路として選ばれるポートは何か。

- ア．ルートポート
- イ．指定ポート
- ウ．ミラーポート
- エ．ループバックポート

正答：ア

4肢解説

ア：正しい。各非ルートブリッジでは、ルートへの最良経路となるポートがルートポートになる。

イ：指定ポートは各セグメントでルートへの最良経路を提供する側のポートであり、非ルートブリッジ自身の最良ルート向けポートという定義ではない。

ウ：パケットキャプチャなどに使う管理上のポートでSTP役割ではない。

エ：STPの標準的なポート役割ではない。

総合解説：STPはルートブリッジ、ルートポート、指定ポートなどを決定し、冗長経路の一部を非転送状態にする。

問18 RSTPが従来のSTPに比べて改善している点として最も適切なものはどれか。

- ア．IPv6アドレスを自動生成する
- イ．トポロジ変更時の収束を高速化する仕組みを備える
- ウ．ルータ間でAS_PATHを交換する
- エ．暗号鍵を自動配布する

正答：イ

4肢解説

ア：RSTPはIPv6アドレス生成機能ではない。

イ：正しい。RSTPはポート役割や状態遷移の見直しなどで従来STPより高速な収束を実現する。

ウ：それはBGPの役割である。

エ：RSTPは暗号鍵管理を行わない。

総合解説：RSTPはSTP互換性を考慮しつつ、障害時やトポロジ変更時のL2収束時間短縮を目的としている。

問19 複数の物理Ethernetリンクを一つの論理リンクとして扱うリンクアグリゲーションの利点として適切なものはどれか。

ア．各物理リンクの伝送速度そのものを必ず倍増させる

イ．IPルーティングを不要にする

ウ．帯域の集約とリンク障害時の冗長性を得られる

エ．ブロードキャストを全て暗号化する

正答：ウ

4肢解説

ア：個々の物理リンク速度自体を変更するわけではない。

イ：LAGはL2リンクの束ねでありL3ルーティングの必要性を消すものではない。

ウ：正しい。複数リンクを論理的に束ねることで、負荷分散と一部リンク障害時の継続性を高められる。

エ：暗号化機能ではない。

総合解説：リンクアグリゲーションでは複数の物理リンクを一つの論理ポートとして扱い、可用性と総スループット向上を狙う。

問20 LACPの主な役割はどれか。

ア．DNSゾーン転送を行う

イ．IPv4アドレスをNAT変換する

ウ．OSPFのLSAを中継する

エ．リンクアグリゲーションを構成する相手やリンク状態をプロトコルで確認し、論理リンク形成を支援する

正答：エ

4肢解説

ア：LACPはDNSプロトコルではない。

イ：アドレス変換機能ではない。

ウ：LACPはルーティングプロトコルではない。

エ：正しい。LACPはリンク集約のメンバー選定や相手確認に使われる制御プロトコルである。

総合解説：LACPを使うと両端でリンクアグリゲーションの整合性を確認しやすくなり、誤配線や状態変化への追従に役立つ。

問21 4本の1GbpsリンクでLAGを構成している。単一のTCPフローが必ず4Gbpsまで利用できるとは限らない主な理由はどれか。

ア．多くの実装ではフローの順序を保つため、ハッシュ等で一つのフローを特定メンバーリンクへ割り当てるため

イ．LAGでは常に1本しか有効化できないため

ウ．Ethernetには全二重通信が存在しないため

エ．LACPがTCPをUDPへ変換するため

正答：ア

4肢解説

ア：正しい。フロー単位の割当てでは複数フロー全体では帯域集約できても、単一フローは1本の物理リンク速度に制約されやすい。

イ：複数メンバーを同時利用できる。

ウ：Ethernetは全二重通信をサポートする。

エ：LACPはトランスポートプロトコルを変換しない。

総合解説：リンクアグリゲーションの総帯域は複数フローで活用しやすいが、負荷分散方式によって単一フローの上限は各物理リンク速度に依存する。

問22 二台のスイッチ間を4本のケーブルで接続し、4本を同一LAGとして正常に構成した。STPから見た扱いとして最も適切な考え方はどれか。

ア．4本すべてを独立リンクとして必ずブロックする

イ．複数物理リンクを一つの論理リンクとして扱い、各物理リンクを独立した並列L2経路として扱わない

ウ．STPを完全に無効化しなければLAGは動作しない

エ．LAGを構成するとVLANは使用できなくなる

正答：イ

4肢解説

ア：LAGとして束ねた場合の扱いとして不適切である。

イ：正しい。正しく構成されたLAGは論理リンクとして扱われ、STPとの組合せで冗長性とループ防止を両立しやすい。

ウ：LAGとSTPは併用できる。

エ：LAG上でVLANを運ぶ構成は一般的である。

総合解説：LAGは物理リンクを論理的に束ね、STPはL2ループを防止する。両者を適切に組み合わせることで冗長性を確保できる。

問23 1回のシンボルで4種類の状態を表し、1シンボル当たり2ビットを伝送する方式が2,000 baudで動作している。理論上のビットレートは幾らか。
ア．1,000 bit/s (2,000 baudを2で割る)
イ．2,000 bit/s (1シンボル=1ビットとして扱う)
ウ．4,000 bit/s (2,000 baud × 2ビットで計算)
エ．8,000 bit/s (1シンボル=4ビットとして扱う)

正答：ウ

4肢解説

ア：baudを2で割っており、1シンボル2ビットという条件と合わない。

イ：1シンボル1ビットの場合の値である。

ウ：正しい。1シンボル当たり2ビットなので、2,000シンボル/秒 × 2ビット=4,000 bit/sである。

エ：1シンボル4ビットとして計算した値である。

総合解説：baudは1秒当たりのシンボル数、bit/sは1秒当たりのビット数を表す。多値変調では両者が一致しない場合がある。

問24 二つの装置が同時に双方向へデータを送受信できる通信方式はどれか。

ア．半二重通信

イ．単方向通信

ウ．ブロードキャスト通信

エ．全二重通信

正答：エ

4肢解説

ア：双方向通信は可能だが、一般に同時送受信は行わない。

イ：一方向にだけ情報を送る方式である。

ウ：宛先形態の分類であり、同時双方向性を表す用語ではない。

エ：正しい。全二重通信では両方向の通信を同時に行える。

総合解説：全二重は同時双方向、半二重は双方向だが同時ではない、単方向は一方向だけの通信である。

問25 長距離・高速伝送で光ファイバを用いる利点として最も適切なものはどれか。
ア．電磁誘導ノイズの影響を受けにくく、長距離伝送に適した方式を選択できる
イ．導体なので落雷電流を必ず直接伝える
ウ．全ての光ファイバは同じ距離・波長でのみ使用できる
エ．FCSが不要になるため誤り検出を行えない

正答：ア

4肢解説

ア：正しい。光信号を用いるため電磁ノイズに強く、用途に応じて長距離高速伝送が可能である。
イ：光ファイバ自体は光を伝送媒体とし、銅線と同じ電氣的導通を前提としない。
ウ：シングルモード/マルチモードや光学仕様により特性は異なる。
エ：媒体が光であってもEthernetフレームの誤り検出機構は存在する。
総合解説：光ファイバは電磁ノイズ耐性や長距離伝送に優れるが、光源・受光器、波長、ファイバ種別、コネクタなどの整合が必要である。

問26 一般に、より長距離の高速光伝送に適する光ファイバとして最も適切なものはどれか。
ア．マルチモードファイバだけが長距離に適する
イ．シングルモードファイバ
ウ．同軸ケーブル
エ．UTPだけ

正答：イ

4肢解説

ア：マルチモードは一般に構内など比較的短距離用途で使われることが多い。
イ：正しい。シングルモードはモード分散が小さく、長距離・高速伝送に適している。
ウ：光ファイバではなく電気信号を伝える銅系媒体である。
エ：ツイストペア銅線であり、長距離光伝送用ではない。
総合解説：シングルモードとマルチモードではコア径や伝搬モードが異なり、到達距離・光源・コストなどの設計条件が変わる。

問27 UTP/STPケーブルで導線を対にして撚る主な理由として適切なものはどれか。

ア．IPアドレスを自動設定する

イ．光の全反射を起こす

ウ．外来ノイズや対間の電磁的な影響を低減しやすくする

エ．STPのルートブリッジを選ぶ

正答：ウ

4肢解説

ア：ケーブル構造はIPアドレス設定を行わない。

イ：これは光ファイバの伝搬原理に関係する。

ウ：正しい。対線を撚ることで誘導ノイズの影響を相殺しやすくし、クロストークなどを抑える。

エ：物理ケーブルの撚りとSTP制御は無関係である。

総合解説：ツイストペアは撚りによって電磁誘導の影響を抑える。STPケーブルではさらにシールドによるノイズ対策を行う。

問28 電力比を $10\log_{10}(P2/P1)$ dBで表す。受信電力が送信電力の1/100になった場合の値はどれか。

ア．-10 dB（電力比1/10に相当）

イ．+20 dB（電力が100倍になった場合に相当）

ウ．-40 dB（電力比1/10,000に相当）

エ．-20 dB（ $10\log_{10}(1/100)$ で計算）

正答：エ

4肢解説

ア：電力比1/10の場合の値である。

イ：符号が逆で、受信電力が100倍になった場合に相当する。

ウ：1/10000程度の電力比に相当する。

エ：正しい。 $10\log_{10}(1/100)=10\times(-2)=-20$ dBである。

総合解説：デシベルは比を対数で表す。電力比では $10\log_{10}$ を使い、1/10で-10 dB、1/100で-20 dBとなる。

問29 8b/10b符号化では8ビットのデータを10ビットの符号に変換する。ユーザデータ800 Mbit/sを符号化後に送るために、少なくとも必要な線路上のビットレートはどれか。

- ア．1,000 Mbit/s
- イ．640 Mbit/s
- ウ．800 Mbit/s
- エ．1,600 Mbit/s

正答：ア

4肢解説

ア：正しい。800×10/8=1,000 Mbit/sである。

イ：符号化でデータ量が減る計算になっており逆である。

ウ：符号化オーバーヘッドを考慮していない。

エ：2倍する必要はなく、10/8倍でよい。

総合解説：伝送路符号化では同期や直流成分制御などのため冗長ビットを加えることがあり、実効データ率と線路速度が異なる。

問30 工場棟間を数km接続し、高速通信が必要で周囲の電磁ノイズも大きい。媒体選定として最も妥当な考え方はどれか。

- ア．一般的な短距離用UTPを距離制限を無視してそのまま延長する
- イ．必要距離と速度を満たす光ファイバ方式を選び、光学仕様と冗長性を確認する
- ウ．ノイズが大きいほど無線だけを無条件に選ぶ
- エ．媒体特性を考えず最も安いケーブルだけで決める

正答：イ

4肢解説

ア：規格上の到達距離を超えると品質を保証できない。

イ：正しい。長距離・高速・高ノイズ環境では光ファイバが有力で、トランシーバや波長、損失予算も含めて設計する。

ウ：無線も干渉や伝搬条件の評価が必要であり、無条件に最適とはいえない。

エ：距離・帯域・環境条件を満たさなければ通信品質を確保できない。

総合解説：媒体選定では帯域、距離、電磁環境、施工性、費用、保守性を総合評価する。光は長距離・ノイズ耐性に優れる一方、光損失や部品整合の設計が必要である。

問31 IPv4アドレスの長さは何ビットか。
ア．16ビット（IPv4の半分の長さのみなす）
イ．64ビット（IPv6の一般的なサブネット境界長と混同する）
ウ．32ビット（4オクテット×8ビットで構成）
エ．128ビット（IPv6アドレス全体の長さ）

正答：ウ

4肢解説

ア：IPv4アドレス長ではない。
イ：IPv4アドレス長ではない。
ウ：正しい。IPv4アドレスは32ビットで表される。
エ：128ビットはIPv6アドレスの長さである。

総合解説：IPv4は32ビット、IPv6は128ビットのアドレス空間を持つ。

問32 IPv6のアドレス空間に関する説明として適切なものはどれか。
ア．32ビット（IPv4と同じ長さのみなす）
イ．48ビット（一般的なEthernet MACアドレス長と混同する）
ウ．64ビット（IPv6のインタフェースID部分だけを全体のみなす）
エ．128ビット（IPv6アドレス全体の長さ）

正答：エ

4肢解説

ア：32ビットはIPv4アドレスの長さであり、IPv6ではない。
イ：48ビットは一般的なEthernet MACアドレス長として知られる値で、IPv6アドレス全体の長さではない。
ウ：IPv6では64ビット単位が使われる場面はあるが、アドレス全体は64ビットではない。
エ：正しい。IPv6アドレスは128ビットで構成され、IPv4より大幅に広いアドレス空間を持つ。

総合解説：IPv6は128ビットのアドレス空間を持つ。通常は16進数をコロンで区切って表記し、IPv4の32ビットより大幅に拡張されている。

問33 IPv4ヘッダのTTLフィールドの主な目的はどれか。

ア．パケットがルーティンググループなどで無期限に転送され続けることを防ぐ

イ．TCPのウィンドウサイズを決める

ウ．送信元MACアドレスを保存する

エ．DNSキャッシュの有効期限だけを決める

正答：ア

4肢解説

ア：正しい。ルータで転送されるたびにTTLが減少し、0になると破棄される。

イ：TTLはTCPフロー制御とは無関係である。

ウ：MACアドレスはEthernetヘッダで扱う。

エ：DNSのTTLとは同名だが、IPv4ヘッダTTLとは別の概念である。

総合解説：IPv4 TTLとIPv6 Hop Limitは、ルーティンググループによる無限転送を防ぐ役割を持つ。

問34 IPv6ヘッダのHop Limitフィールドに最も近いIPv4のフィールドはどれか。

ア．Header Checksum

イ．TTL

ウ．Identification

エ．Protocol

正答：イ

4肢解説

ア：IPv6基本ヘッダにはIPv4と同じヘッダチェックサムはない。

イ：正しい。IPv6のHop Limitは、各転送ノードで減算される点でIPv4のTTLに相当する。

ウ：IPv4のフラグメント識別に使うフィールドであり、Hop Limit相当ではない。

エ：上位プロトコル識別に使うフィールドで、Hop Limitとは役割が異なる。

総合解説：IPv6ではTTLに相当する概念をHop Limitとして明示し、転送ホップ数の上限を管理する。

問35 IPv6基本ヘッダに関する説明として適切なものはどれか。
ア．IPv6ではFCSもTCPチェックサムも全て禁止される
イ．IPv6基本ヘッダはIPv4より必ず長さが可変である
ウ．IPv4ヘッダにあるHeader Checksumに相当するフィールドは基本ヘッダに存在しない
エ．IPv6では送信元・宛先アドレスを持たない

正答：ウ

4肢解説

ア：下位・上位層の誤り検出機構まで禁止されるわけではない。
イ：IPv6基本ヘッダは固定長で、追加情報は拡張ヘッダを用いる。
ウ：正しい。IPv6ではルータ処理簡素化などのため、IPv4のヘッダチェックサムは基本ヘッダから除かれている。
エ：IPv6基本ヘッダには128ビットの送信元・宛先アドレスがある。
総合解説：IPv6基本ヘッダは固定長で簡素化され、追加機能は拡張ヘッダへ分離されている。

問36 IPv6のフラグメンテーションに関する説明として最も適切なものはどれか。
ア．全てのIPv6ルータがIPv4と同様に途中で自由にフラグメントする
イ．IPv6ではフラグメンテーションという概念自体が存在しない
ウ．IPv6ではMTUを考慮する必要がない
エ．中継ルータは通常パケットをフラグメントせず、必要な場合は送信元がFragmentヘッダを用いる

正答：エ

4肢解説

ア：IPv6では中継ルータによるフラグメントを行わない。
イ：送信元がFragment拡張ヘッダを用いてフラグメントできる。
ウ：経路MTUは依然として重要である。
エ：正しい。IPv6では途中のルータによるフラグメントを行わず、送信元側が必要に応じて処理する。
総合解説：IPv6ではPath MTU Discoveryなどを用い、途中のルータではなく送信元がパケットサイズを調整する設計になっている。

問37 IPv6リンクローカルユニキャストアドレスのプレフィックスとして適切なものはどれか。

ア . FE80::/10
イ . FF00::/8
ウ . 2001:DB8::/32
エ . 127.0.0.0/8

正答：ア

4肢解説

ア：正しい。IPv6リンクローカルユニキャストはFE80::/10の範囲に属する。

イ：IPv6マルチキャストアドレスの範囲である。

ウ：文書・例示用に予約されたプレフィックスである。

エ：IPv4のループバック用範囲でありIPv6ではない。

総合解説：リンクローカルアドレスは同一リンク内の通信やNeighbor Discoveryなどで利用され、ルータ越しに通常転送されない。

問38 IPv6で、IPv4のブロードキャストに相当する用途を実現したい場合の考え方として適切なものはどれか。

ア . IPv6は全通信を必ずブロードキャストで行う
イ . IPv6にはIPv4のようなブロードキャストアドレスはなく、必要な用途にはマルチキャストなどを使う
ウ . IPv6ではマルチキャストが禁止されている
エ . IPv6ではユニキャストアドレスが存在しない

正答：イ

4肢解説

ア：IPv6にはブロードキャストアドレスが定義されていない。

イ：正しい。IPv6はブロードキャストアドレスを定義せず、マルチキャストやエニーキャストを利用する。

ウ：IPv6ではマルチキャストを広く利用する。

エ：IPv6にもユニキャストアドレスが存在する。

総合解説：IPv6はブロードキャストを廃し、Neighbor Discoveryなどでもマルチキャストを活用する。

問39 IPv6アドレス 2001:0db8:0000:0000:0000:0000:0001 の省略表記として適切なものはどれか。

ア . 2001:db8:0:0:0:0:1:0

イ . 2001.db8.0.0.0.0.1

ウ . 2001:db8::1

エ . 2001:db8::00001

正答：ウ

4肢解説

ア：IPv6の通常表記は128ビットを8個の16ビット区切りで表すため、この表記は区切りが9個となり不適切である。

イ：IPv6の通常表記はコロン区切りであり、ドット区切りだけで表すこの形式は不適切である。

ウ：正しい。各16ビット区切りの先頭ゼロを省略でき、連続する0の区切りは一度だけ::で圧縮できる。

エ：1区切りは最大4桁の16進数であり、00001は5桁なので不適切である。

総合解説：IPv6表記では各16ビットの先頭ゼロを省略でき、連続するゼロの列を::で一度だけ圧縮できる。

問40 IPv4とIPv6の基本ヘッダを比較した説明として適切なものはどれか。

ア . IPv6はIPv4よりアドレス長を短くした

イ . IPv6は全てのルータでヘッダチェックサムを再計算する

ウ . IPv6は必ずTCPだけを運ぶ

エ . IPv6では基本ヘッダを簡素化し、オプション相当の情報の多くを拡張ヘッダとして扱う

正答：エ

4肢解説

ア：IPv6は32ビットから128ビットへ拡張している。

イ：IPv6基本ヘッダにはIPv4のHeader Checksumがない。

ウ：Next HeaderによりTCP以外の上位プロトコルや拡張ヘッダも扱える。

エ：正しい。IPv6は基本ヘッダを固定長・簡素化し、追加情報を拡張ヘッダへ分離している。

総合解説：IPv6はアドレス空間拡張に加え、基本ヘッダの簡素化や拡張ヘッダ方式を採用している。

問41 192.0.2.0/25 と 192.0.2.128/25 の二つの連続したネットワークを、追加のアドレスを含めずに一つのCIDRプレフィックスへ集約するとどれか。
ア . 192.0.2.0/24 (192.0.2.0 ~ 192.0.2.255を包含)
イ . 192.0.2.0/26 (192.0.2.0 ~ 192.0.2.63だけを包含)
ウ . 192.0.0.0/16 (192.0.0.0 ~ 192.0.255.255を包含)
エ . 192.0.2.128/24 (/24境界に整列しない表記)

正答：ア

4肢解説

ア：正しい。二つの/25は同一/24を前半・後半に二分したもので、192.0.2.0/24へ正確に集約できる。

イ：/26は範囲が狭く、二つの/25を包含できない。

ウ：包含はするが多数の追加アドレスを含み、設問の条件に合わない。

エ：/24のネットワークアドレスは第4オクテット0境界であり、この表記は正規な集約ネットワークを示さない。

総合解説：CIDRでは連続し、共通する上位ビットを持つプレフィックスをまとめることでルーティングテーブルを縮小できる。

問42 IPv4サービスを維持しながらIPv6対応を段階的に進め、同一ホストが必要に応じてIPv4とIPv6の両方を利用できるようにする方式として最も適切なものはどれか。

ア . VLANトランキン

イ . デュアルスタック

ウ . リンクアグリゲーション

エ . STP

正答：イ

4肢解説

ア：L2で複数VLANを運ぶ仕組みであり、IPv4/IPv6共存方式ではない。

イ：正しい。デュアルスタックはノードにIPv4とIPv6の双方を実装し、相手や経路に応じて使い分ける方式である。

ウ：複数物理リンクを論理的に束ねる仕組みである。

エ：L2ループを防止するプロトコルである。

総合解説：IPv4からIPv6への移行ではデュアルスタック、トンネリング、変換方式などを要件に応じて組み合わせる。

問43 IPv4ネットワーク 192.0.2.0/26 のホスト部は何ビットか。

- ア．4ビット（ /28とした場合のホスト部）
- イ．26ビット（プレフィックス長をホスト部とみなす）
- ウ．6ビット（32-26で求める）
- エ．32ビット（IPv4アドレス全体をホスト部とみなす）

正答：ウ

4肢解説

ア： /28の場合のホスト部ビット数である。

イ：プレフィックス長そのものをホスト部と取り違えている。

ウ：正しい。IPv4は32ビットなので、32-26=6ビットがホスト部である。

エ：アドレス全体のビット数であり、ホスト部だけの長さではない。

総合解説：IPv4のCIDR表記では/の後ろがネットワークプレフィックス長を示し、残りがホスト部になる。

問44 IPv4の /27サブネット一つに含まれる総アドレス数は幾つか。

- ア．16個（ホスト部4ビット相当）
- イ．30個（ /27で予約2個を除いた通常ホスト数）
- ウ．64個（ホスト部6ビット相当）
- エ．32個（ホスト部5ビットなので2^5）

正答：エ

4肢解説

ア： /28の総アドレス数である。

イ：ネットワークアドレスとブロードキャストアドレスを除いた従来の利用可能ホスト数であり、総アドレス数ではない。

ウ： /26の総アドレス数である。

エ：正しい。ホスト部は5ビットなので、2^5=32個のアドレスを含む。

総合解説：サブネットの総アドレス数は2^(32-プレフィックス長)で求める。利用可能ホスト数を問う場合は用途や予約アドレスの条件に注意する。

問45 RFC 1918で定義されるIPv4プライベートアドレス範囲に含まれるものはどれか。

ア．172.16.0.0/12（172.16.0.0～172.31.255.255の範囲）

イ．100.64.0.0/10（共有アドレス空間として予約された範囲）

ウ．169.254.0.0/16（IPv4リンクローカルの範囲）

エ．224.0.0.0/4（IPv4マルチキャストの範囲）

正答：ア

4肢解説

ア：正しい。RFC 1918では10.0.0.0/8、172.16.0.0/12、192.168.0.0/16をプライベート用途に定めている。

イ：共有アドレス空間として別用途に予約された範囲で、RFC 1918のプライベート範囲ではない。

ウ：リンクローカル用途の範囲である。

エ：IPv4マルチキャスト用の範囲である。

総合解説：RFC 1918のプライベートアドレスはグローバルインターネットで通常経路広告されず、組織内部での利用を想定する。

問46 IPv4アドレス 192.168.10.77/26 が属するネットワークアドレスはどれか。

ア．192.168.10.0（第4オクテット0～63の/26境界）

イ．192.168.10.64（第4オクテット64～127の/26境界）

ウ．192.168.10.77（与えられたホストアドレスそのもの）

エ．192.168.10.128（第4オクテット128～191の/26境界）

正答：イ

4肢解説

ア：0～63の/26サブネットのネットワークアドレスである。

イ：正しい。/26は第4オクテットを64刻みで分割し、77は64～127の範囲に属する。

ウ：これはホストアドレスでありネットワークアドレスではない。

エ：128～191の次の/26サブネットのネットワークアドレスである。

総合解説：/26のブロックサイズは64であり、ネットワーク境界は0、64、128、192となる。

問47 192.0.2.10/28 と同一サブネットに属するIPv4アドレスはどれか。
ア．192.0.2.16 (次の/28ブロックの先頭)
イ．192.0.2.31 (次の/28ブロック末尾側)
ウ．192.0.2.14 (192.0.2.0～15の範囲内)
エ．192.0.2.33 (192.0.2.32/28の範囲内)
正答：ウ
4肢解説
ア：次の/28サブネットのネットワークアドレスである。
イ：192.0.2.16/28のブロードキャスト側に属する。
ウ：正しい。/28は16アドレス単位で、192.0.2.0～15が同一サブネットである。
エ：192.0.2.32/28に属する。
総合解説：/28では第4オクテットを16刻みで区切る。アドレス10は0～15の範囲に属する。

問48 NATの基本的な動作として最も適切なものはどれか。
ア．EthernetのFCSを再計算するだけ
イ．DNS名をIPアドレスへ変換する
ウ．OSPFのルートブリッジを選ぶ
エ．IPパケットのアドレス情報を境界装置で変換する
正答：エ
4肢解説
ア：NATの本質はIPアドレス変換であり、FCS処理だけではない。
イ：それはDNS名前解決の役割である。
ウ：OSPFにルートブリッジという概念はなく、NATとも無関係である。
エ：正しい。NATは内部・外部のアドレス空間間でIPアドレスを変換する仕組みである。
総合解説：NATはアドレス変換を行うため、IPや上位層のチェックサム等に影響する場合があります、アプリケーションによっては透過性の課題も生じる。

問49 複数の内部端末が一つのグローバルIPv4アドレスを共有して外部通信する際、送信元ポート番号なども変換してセッションを識別する方式はどれか。

ア．NAPT
イ．単純な1対1 NATだけ
ウ．ARP
エ．STP

正答：ア

4肢解説
ア：正しい。NAPTはIPアドレスだけでなくTCP/UDPポート番号なども利用して複数通信を多重化する。
イ：1対1 NATでは一つの外部アドレスを多数端末でポート多重化する説明にならない。
ウ：ARPはIPv4アドレスに対応するリンク層アドレスを解決する。
エ：STPはL2ループを防止する。

総合解説：NAPTは一般にPATとも呼ばれ、一つまたは少数の外部アドレスへ多数の内部通信を対応付けるために使われる。

問50 内部Webサーバを外部から常に同じグローバルIPv4アドレスで到達可能にしたい。設計として最も適切なものはどれか。

ア．送信のたびに外部アドレスをランダムに変更し、対応を公開しない
イ．固定的なアドレスまたはポート対応を設定し、外部から内部サーバへ転送する
ウ．NAT装置で全ての受信通信を無条件に破棄する
エ．内部サーバのMACアドレスだけをDNSへ登録する

正答：イ

4肢解説
ア：外部利用者が安定して到達できない。
イ：正しい。公開サーバでは外部から予測可能な固定対応が必要になる。
ウ：外部公開という要件を満たさない。
エ：通常のインターネットDNSは到達用IPアドレスを扱い、MACアドレスだけではルーティングできない。

総合解説：外部公開には静的NATやポートフォワーディングなどで固定対応を設け、同時にファイアウォール等で必要な通信だけを許可する。

問51 ルータに 10.0.0.0/8 と 10.1.0.0/16 の経路があり、宛先10.1.2.3のパケットを受信した。その他の条件が同じなら、どちらの経路が優先されるか。

ア．10.0.0.0/8

イ．両方に複製して送信する

ウ．10.1.0.0/16

エ．宛先アドレスに一致する経路はない

正答：ウ

4肢解説

ア：一致はするが/16より具体性が低い。

イ：通常の最長一致による単一経路選択の説明ではない。

ウ：正しい。両方に一致するが、より長いプレフィックスである/16が最長一致により優先される。

エ：10.1.2.3は両方のプレフィックスに含まれる。

総合解説：IP転送では一般に、宛先に一致する複数プレフィックスのうち最も長いプレフィックスを優先する。

問52 多数の内部IPv4端末をNAPT経由でインターネット接続している。高頻度の外向きセッションが増えたときに、設計上確認すべき事項として最も適切なものはどれか。

ア．STPのルートブリッジMACだけを確認する

イ．全端末のEthernet FCS値を固定する

ウ．IPv4のTTLを常に255へ設定すれば変換容量が増える

エ．変換テーブル容量や利用可能な外部アドレス・ポート資源、タイムアウトを確認する

正答：エ

4肢解説

ア：NAPTのセッション容量とは直接関係しない。

イ：FCSを固定することはできず、NAPT容量問題の解決にもならない。

ウ：TTLとNAPTの変換テーブル容量は別問題である。

エ：正しい。NAPTでは同時セッション増加に伴い変換エントリやポート資源が制約になり得る。

総合解説：大規模NAPTではアドレス・ポートの多重化資源、状態テーブル、タイムアウト、ログ量などが性能・可用性設計上の重要点になる。

問53 IPv4ホストが同一LAN上の宛先IPv4アドレスに対応するEthernet MACアドレスを知るために用いる代表的なプロトコルはどれか。

- ア．ARP
- イ．DNS
- ウ．BGP
- エ．SNMP

正答：ア

4肢解説

ア：正しい。ARPはネットワーク層のIPv4アドレスからリンク層アドレスを解決するために使われる。

イ：DNSは主に名前とIPアドレスなどの資源レコードを対応付ける。

ウ：BGPはAS間で経路情報を交換するルーティングプロトコルである。

エ：SNMPはネットワーク機器の監視・管理に使われる。

総合解説：Ethernet上のIPv4通信では、同一リンク上の次ホップヘッフレームを送るため、ARPで対応するMACアドレスを取得する。

問54 pingコマンドが到達性確認に利用する代表的なICMPメッセージの組合せはどれか。

- ア．Router Advertisement と Router Solicitation
- イ．Echo Request と Echo Reply
- ウ．OPEN と KEEPALIVE
- エ．SYN と ACK

正答：イ

4肢解説

ア：これらはIPv6 Neighbor Discoveryでルータ探索に用いられる。

イ：正しい。pingは通常ICMP Echo Requestを送信し、相手からのEcho Replyを確認する。

ウ：BGPのメッセージ種別である。

エ：TCP接続確立で使われるフラグでありICMPメッセージではない。

総合解説：ICMPはIPのエラー通知や診断に用いられ、Echo Request/Replyは疎通確認の代表例である。

問55 ARPで一度得たIPv4アドレスとMACアドレスの対応を一定時間キャッシュする主な利点はどれか。

ア．IPパケットを暗号化できる

イ．BGP経路を自動集約できる

ウ．同じ宛先への通信ごとにARP要求を繰り返す必要を減らせる

エ．TCPの輻輳制御を無効化できる

正答：ウ

4肢解説

ア：ARPキャッシュは暗号化機能ではない。

イ：ARPはAS間経路制御を行わない。

ウ：正しい。キャッシュによりブロードキャストARP要求の頻度を下げられる。

エ：ARPキャッシュとTCP輻輳制御は無関係である。

総合解説：ARPキャッシュは効率向上に有効だが、古い対応が残ると端末移動や変更時に一時的な通信不整合が起こることもある。

問56 IPv4でTTLが0になったパケットをルータが破棄したことを送信元へ知らせる際に利用される代表的なICMPメッセージはどれか。

ア．Echo Reply

イ．Redirectだけ

ウ．Neighbor Advertisement

エ．Time Exceeded

正答：エ

4肢解説

ア：Echo Requestへの応答でありTTL超過通知ではない。

イ：経路変更を示唆するメッセージで、TTL超過通知とは役割が異なる。

ウ：IPv6 NDPのメッセージでありICMPv4 TTL超過通知ではない。

エ：正しい。TTLが尽きた場合、ルータはICMP Time Exceededを返すことがあり、traceroute系ツールでも利用される。

総合解説：TTL/Hop Limitを段階的に変えてTime Exceeded応答を観測することで、経路上のルータを推定する手法がtracerouteの基本である。

問57 IPv6 ノードが同一リンク上の近隣ノードのリンク層アドレスを解決する際に用いるNDPメッセージとして適切なものはどれか。

ア . Neighbor Solicitation
イ . ARP Request
ウ . BGP UPDATE
エ . DHCPACK

正答：ア

4肢解説

ア：正しい。Neighbor Solicitationは近隣探索やアドレス解決、到達性確認などに用いられる。

イ：ARPはIPv4で利用され、IPv6ではNeighbor Discoveryが役割を担う。

ウ：BGP経路広告メッセージであり近隣のMAC解決には使わない。

エ：DHCPの応答でありNDPのアドレス解決メッセージではない。

総合解説：IPv6ではARPを使わず、ICMPv6ベースのNeighbor DiscoveryでNeighbor Solicitation/ Advertisementなどを利用する。

問58 IPv6ホストがリンク上のルータ情報やプレフィックス情報などを得るために関係するNDPメッセージの組合せはどれか。

ア . ARP Request と ARP Reply
イ . Router Solicitation と Router Advertisement
ウ . OSPF Hello と DBD
エ . TCP SYN と FIN

正答：イ

4肢解説

ア：IPv4のリンク層アドレス解決に使う。

イ：正しい。ホストはRSを送り、ルータはRAでルータ存在やプレフィックス等の情報を通知できる。

ウ：ルータ間OSPF隣接関係で用いるメッセージで、ホスト向けNDPではない。

エ：TCP接続制御フラグである。

総合解説：NDPのRouter DiscoveryはIPv6ホストがデフォルトルータやオンリンクプレフィックス等を学ぶ重要な仕組みである。

問59 攻撃者が偽のARP応答を送り、端末のARPキャッシュに誤ったMACアドレス対応を登録させようとしている。この攻撃で悪用されるARPの性質として最も適切なものはどれか。

- ア．ARPが必ずTLSで暗号化されること
- イ．ARPがAS_PATHを検証すること
- ウ．ARPの対応情報に強い認証機構が標準で組み込まれていないこと
- エ．ARPがIPv6専用であること

正答：ウ

4肢解説

ア：ARPはTLSで保護されるプロトコルではない。

イ：AS_PATHはBGP属性でありARPには存在しない。

ウ：正しい。ARPは同一リンク内での単純なアドレス解決を目的としており、応答の真正性を強く認証する設計ではない。

エ：ARPは主にIPv4で用いられる。

総合解説：ARPスプーフィング対策には、スイッチの検査機能、静的対応、セグメント分離など環境に応じたL2セキュリティ対策を検討する。

問60 IPv4からIPv6へ移行したネットワークで『IPv6でもARPブロードキャストを使ってMACアドレスを解決する』という説明が誤りである主な理由はどれか。

- ア．IPv6にはMACアドレスを使うリンクが存在しないため
- イ．IPv6では同一リンク通信が禁止されているため
- ウ．IPv6は必ずMPLSラベルだけで転送するため
- エ．IPv6ではARPではなくICMPv6ベースのNeighbor Discoveryを使い、マルチキャストを活用するため

正答：エ

4肢解説

ア：IPv6もEthernet上ではMACアドレスを利用する。

イ：同一リンク上でIPv6通信できる。

ウ：IPv6がMPLS必須ということはない。

エ：正しい。IPv6の近隣探索はNDPが担い、IPv4 ARPブロードキャストとは異なる仕組みである。

総合解説：IPv6 Neighbor Discoveryはアドレス解決に加え、ルータ探索、到達性確認、リダイレクトなど複数の役割を担う。

問61 OSPFの説明として最も適切なものはどれか。
ア．単一AS内部で利用されるリンクステート型IGPである
イ．AS間専用のバスベクトル型EGPである
ウ．L2ループ防止専用プロトコルである
エ．名前解決専用プロトコルである

正答：ア

4肢解説

ア：正しい。OSPFはAS内部の経路制御に用いるリンクステート型のInterior Gateway Protocolである。
イ：AS間で代表的に使われるバスベクトル型プロトコルはBGPである。
ウ：L2ループ防止はSTP/RSTPの役割である。
エ：名前解決はDNSの役割である。

総合解説：OSPFはリンク状態情報を共有し、各ルータがLSDBを基に最短経路木を計算する。

問62 OSPFルータが最短経路を計算するときに基礎となる情報はどれか。

ア．ARPキャッシュだけ
イ．リンクステートデータベース（LSDB）
ウ．DNSキャッシュだけ
エ．MACアドレステーブルだけ

正答：イ

4肢解説

ア：ARPキャッシュは同一リンクのIPv4-MAC対応情報で、OSPF全体のトポロジを表さない。
イ：正しい。OSPFルータはLSAから構成したLSDBを基にSPF計算を行う。
ウ：DNSキャッシュは名前解決結果でありルーティングトポロジではない。
エ：L2スイッチング用の情報でありOSPFの経路計算基盤ではない。

総合解説：同一エリアのOSPFルータは整合したリンク状態情報を持ち、その情報から最短経路を計算する。

問63 マルチエリアOSPFでバックボーンエリアとして扱われるエリアはどれか。

- ア．Area 255だけ
- イ．VLAN 1
- ウ．Area 0
- エ．AS 0

正答：ウ

4肢解説

ア：Area 255がバックボーンとして固定されるわけではない。

イ：VLAN IDとOSPFエリア番号は別概念である。

ウ：正しい。OSPFのバックボーンエリアはArea 0である。

エ：BGPのAS番号とOSPFエリアは別概念である。

総合解説：マルチエリア構成ではArea 0を中心にエリア間接続を設計し、LSA伝播範囲や経路計算負荷を抑える。

問64 OSPFで同一宛先への二つの候補経路があり、一方の累積コストが10、他方が20である。その他条件が同じ場合に選ばれる経路はどれか。

- ア．累積コスト20の経路
- イ．必ず両方を同じ割合で使う
- ウ．MACアドレスが小さい側だけで決める
- エ．累積コスト10の経路

正答：エ

4肢解説

ア：OSPFでは一般により小さい累積コストが優先される。

イ：コストが異なる経路は等コストではない。

ウ：OSPFの経路メトリック選択はMACアドレス大小だけで決まらない。

エ：正しい。OSPFは最小コスト経路を優先する。

総合解説：OSPFはリンクごとのコストを積算し、SPF計算で宛先までの最小コスト経路を求める。

- 問65 OSPF Helloパケットの主な役割はどれか。
- ア．近隣ルータの発見と隣接関係維持に必要な情報交換を行う
 - イ．経路全体を圧縮してDNSへ登録する
 - ウ．EthernetのFCSを計算する
 - エ．TCPコネクションを確立する

正答：ア

4肢解説

ア：正しい。Helloはネイバー検出や生存確認、各種パラメータ確認に用いられる。

イ：HelloはDNS登録を行わない。

ウ：FCSはEthernetフレーム処理でありOSPF Helloの役割ではない。

エ：OSPFはTCP上で動作するプロトコルではない。

総合解説：OSPFではまずHello交換により近隣を認識し、条件が整えば隣接関係を形成してLSDB同期へ進む。

問66 ブロードキャスト型ネットワークでOSPFがDR/BDRを選出する主な目的はどれか。

- ア．全ルータのIPアドレスをNAT変換する
- イ．全ルータ間で完全な隣接関係を張ることによる情報交換量を抑える
- ウ．STPのブロッキングポートを決める
- エ．BGPのAS番号を割り当てる

正答：イ

4肢解説

ア：DR/BDRはNAT機能ではない。

イ：正しい。DR/BDRを介した隣接関係により、マルチアクセスネットワークでの隣接関係数とLSA交換を効率化する。

ウ：L2 STPのポート役割とは別である。

エ：AS番号割当てはDR/BDRの役割ではない。

総合解説：OSPFのブロードキャスト/マルチアクセスネットワークではDRとBDRを選び、隣接関係の増大を抑制する。

問67 OSPFでリンク状態の変更が起きたとき、LSAをフラッディングする目的はどれか。

ア．全ホストへDHCPアドレスを配布する

イ．Ethernetフレームを無限に複製する

ウ．対象範囲のルータヘトボロジ変更情報を伝え、LSDBを整合させる

エ．TCPセッションを暗号化する

正答：ウ

4肢解説

ア：OSPFはDHCPサーバではない。

イ：制御されたルーティング情報配布でありL2ループとは異なる。

ウ：正しい。LSAフラッディングによりルータ間でリンク状態情報を共有する。

エ：OSPF LSAはTCP暗号化機能ではない。

総合解説：リンク状態型ルーティングではトボロジ情報の同期が重要で、変化をLSAとして伝播させ再計算する。

問68 リンクステート型のOSPFと距離ベクトル型ルーティングの一般的な違いとして適切なものはどれか。

ア．OSPFはMACアドレスだけを隣接ルータへ広告する

イ．OSPFは必ず経路全体をBGPのAS_PATH形式で広告する

ウ．OSPFはルーティングテーブルを持たない

エ．OSPFはリンク状態情報からトボロジを把握し、自ら最短経路木を計算する

正答：エ

4肢解説

ア：経路計算のためリンク状態情報を扱う。

イ：AS_PATHはBGP属性である。

ウ：OSPF計算結果はルーティングテーブルへ反映される。

エ：正しい。リンクステート型ではLSDBを構築しSPFアルゴリズムで経路を計算する。

総合解説：リンクステート型はトボロジ認識とSPF計算を特徴とし、距離ベクトル型とは情報共有と計算方式が異なる。

問69 大規模OSPFネットワークを複数エリアに分割する主な設計上の利点はどれか。

ア．LSAの影響範囲やSPF計算対象を抑え、ルーティング処理のスケーラビリティを高められる

イ．全ルータでLSDBを必ず無限に大きくする

ウ．異なるエリア間通信を禁止する

エ．OSPFをL2スイッチングへ変換する

正答：ア

4肢解説

ア：正しい。エリア分割によりトポロジ変化の影響を局所化し、LSDB規模や計算負荷を抑えやすい。

イ：エリア分割は負荷抑制を狙う。

ウ：ABRなどを介してエリア間ルーティングを行える。

エ：エリア分割してもOSPFはL3ルーティングプロトコルである。

総合解説：大規模OSPFではエリア設計、要約、ABR配置などにより収束性と運用性のバランスを取る。

問70 OSPFネットワークで主要リンクが断になった。一般的な再収束の流れとして最も適切なものはどれか。

ア．全ルータがARPキャッシュだけを削除して終了する

イ．変化を検出し、リンク状態情報を更新・伝播し、SPF再計算後に新経路を反映する

ウ．BGP AS番号を変更しない限り経路は変わらない

エ．STPルートブリッジを再選出すれば必ずL3経路も決まる

正答：イ

4肢解説

ア：ARPだけではルーティングトポロジの再計算にならない。

イ：正しい。リンク状態型IGPでは障害情報を共有し、各ルータが新しい最短経路を再計算する。

ウ：OSPF内部障害の再収束にAS番号変更は不要である。

エ：STPとOSPFは異なる層の制御である。

総合解説：OSPFの収束は障害検出、LSA更新・フラディング、LSDB反映、SPF計算、RIB/FIB更新という流れで理解するとよい。

問71 BGP-4の主な役割として最も適切なものはどれか。

ア．同一LAN内のMACアドレスを学習する

イ．IPv4アドレスからMACアドレスを解決する

ウ．異なる自律システム（AS）間で到達可能性情報を交換する

エ．L2ループを防止する

正答：ウ

4肢解説

ア：これはL2スイッチの役割である。

イ：これはARPの役割である。

ウ：正しい。BGPはインターネットを含むAS間ルーティングで中心的に用いられる。

エ：これはSTP/RSTPの役割である。

総合解説：BGPはAS間の経路交換とポリシー制御を行うバスペクトル型のルーティングプロトコルである。

問72 BGPが隣接ルータとのセッションに利用するトランスポートプロトコルと代表的なポート番号の組合せはどれか。

ア．UDP 53

イ．TCP 80

ウ．UDP 161

エ．TCP 179

正答：エ

4肢解説

ア：DNSで代表的に使われる組合せである。

イ：HTTPで代表的に使われるポートである。

ウ：SNMPで代表的に使われるポートである。

エ：正しい。BGPはTCPを利用し、標準の宛先ポート番号179で接続を受け付ける。

総合解説：BGPはTCPの信頼性を利用して経路情報を交換するため、独自の再送機構で全メッセージを運ぶ設計ではない。

問73 BGPのAS_PATH属性の重要な役割として最も適切なものはどれか。
ア．経路が通過したASの列を保持し、ASレベルのループ検出や経路選択に利用する
イ．Ethernetの送信元MACアドレスを保持する
ウ．TCPのウィンドウサイズを指定する
エ．IPv6のリンクローカルアドレスを生成する

正答：ア

4肢解説

ア：正しい。AS_PATHには経由AS情報が含まれ、自AS番号を含む経路を拒否することでループ防止に寄与する。
イ：AS_PATHはBGP経路属性でありMACアドレスを保持しない。
ウ：TCPフロー制御の値ではない。
エ：IPv6アドレス生成機能ではない。
総合解説：AS_PATHはBGPの代表的なパス属性で、経路のAS通過履歴を表す。

問74 AS 65001のルータとAS 65002のルータの間でBGPセッションを確立する場合、この関係は一般に何と呼ばれるか。
ア．iBGP
イ．eBGP
ウ．OSPF
エ．LACP

正答：イ

4肢解説

ア：iBGPは同一AS内のBGPルータ間で用いられる。
イ：正しい。異なるAS間のBGPセッションはExternal BGP、すなわちeBGPである。
ウ：OSPFは別のIGPでありBGPセッション種別ではない。
エ：LACPはリンクアグリゲーション制御プロトコルである。
総合解説：同一AS内のBGPはiBGP、異なるAS間はeBGPと呼ぶ。両者は経路伝播ルールにも違いがある。

問75 BGPのNEXT_HOP属性が示すものとして最も適切なものはどれか。

ア．ASの組織名

イ．EthernetフレームのFCS値

ウ．その経路の宛先へ向かうために利用すべき次ホップのIPアドレス

エ．DNS問い合わせ回数

正答：ウ

4肢解説

ア：組織名を示す属性ではない。

イ：L2誤り検出値ではない。

ウ：正しい。NEXT_HOPはBGP経路の転送先となる次ホップ情報を示す。

エ：DNS統計情報ではない。

総合解説：BGP経路を実際にFIBへ載せるにはNEXT_HOPへの到達性も重要で、IGPとの連携が必要になることがある。

問76 一つのASが複数の外部回線を持つ。AS内部で『外向き通信は原則として回線Aを優先する』というポリシーをBGPで表現する際に有効な属性はどれか。

ア．FCS

イ．ARP opcode

ウ．VLAN ID

エ．LOCAL_PREF

正答：エ

4肢解説

ア：Ethernetの誤り検出値で経路ポリシーには使わない。

イ：ARP要求/応答種別でありBGPポリシー属性ではない。

ウ：L2セグメント識別子でありBGP出口選択属性ではない。

エ：正しい。LOCAL_PREFはAS内部で出口経路の優先度を表すために利用され、一般に大きい値が優先される。

総合解説：LOCAL_PREFはiBGPでAS内部に伝えられ、複数出口からどこを優先するかという運用ポリシーに使われる。

問77 隣接ASに対し、自ASへの複数の入口のうちどの入口を相対的に選好してほしいかを示すために用いられるBGP属性はどれか。
ア．MULTI_EXIT_DISC (MED)
イ．AS_PATH
ウ．ORIGINATOR_ID
エ．EtherType
正答：ア
4肢解説
ア：正しい。MEDは複数の相互接続点がある場合に、隣接ASへ入口選好のヒントを与えるために使われる。
イ：通過AS列を示し、MEDとは目的が異なる。
ウ：ルートリフレクタ環境でループ防止などに用いられる属性である。
エ：Ethernetの上位プロトコル識別値である。
総合解説：MEDは隣接ASへの比較情報として用いられるが、受け手のポリシーによって扱いは決まるため強制力のある指示ではない。

問78 多数のBGP経路に同じポリシーを適用するため、経路へ論理的なタグを付けて分類したい。最も適した仕組みはどれか。
ア．ARPキャッシュ
イ．BGP Community
ウ．STPポートコスト
エ．TCP MSS
正答：イ
4肢解説
ア：L2アドレス解決結果の一時保存である。
イ：正しい。Community属性を用いると経路をグループ化し、広告制御や優先度設定などのポリシーを適用しやすい。
ウ：L2ループ防止の経路計算値でBGP経路タグではない。
エ：TCPセグメントサイズに関する値でBGPポリシータグではない。
総合解説：BGP Communityは多数経路に共通の意味付けを行い、ポリシールーティングの運用を簡素化する。

問79 一つのAS内でiBGPルータ数が増え、全ルータ間フルメッシュのセッション数が運用負荷になっている。代表的な改善策はどれか。

- ア．全BGPルータをL2ハブへ置き換える
- イ．全経路をARPだけで配布する
- ウ．ルートリフレクタを導入してiBGP経路配布を階層化する
- エ．TCP 179を閉じたままBGPを継続する

正答：ウ

4肢解説

ア：ルーティング機能とポリシー制御を失い、解決にならない。

イ：ARPはAS内の経路配布プロトコルではない。

ウ：正しい。ルートリフレクタはiBGPフルメッシュ要件を緩和し、セッション数を削減する代表的な仕組みである。

エ：BGPセッションを確立できなくなる。

総合解説：大規模iBGPではルートリフレクタやコンフェデレーションなどによりフルメッシュのスケーラビリティ問題を軽減する。

問80 顧客ASから本来受け取るべきでない大量のインターネット経路が誤広告され、自ASがそれを外部へ再広告するリスクを下げたい。最も適切な対策方針はどれか。

- ア．全BGP経路を無条件に受信・再広告する
- イ．Ethernet FCSを無効化する
- ウ．VLAN IDを毎秒変更する
- エ．受信・送信経路フィルタとプレフィックス上限などを設定し、許可する経路を明示的に制御する

正答：エ

4肢解説

ア：誤広告や経路リークの影響を拡大する。

イ：BGP経路リーク対策と無関係である。

ウ：BGPポリシー問題の解決にならない。

エ：正しい。BGPでは隣接先ごとのポリシーで受け入れ・広告可能なプレフィックスを制限することが重要である。

総合解説：BGP運用ではプレフィックスフィルタ、AS_PATHフィルタ、max-prefix、RPKI等を組み合わせて誤広告やハイジャックのリスクを抑える。

問81 IPルータが宛先に一致する複数の経路を持つ場合、通常の転送で最も優先されるのはどれか。

- ア．最も長いプレフィックス長で一致する経路
- イ．最も短いプレフィックス長の経路
- ウ．MACアドレスが最小のルータの経路
- エ．登録時刻が最も古い経路

正答：ア

4肢解説

ア：正しい。宛先アドレスに対して最も具体的な経路、すなわち最長プレフィックス一致が優先される。

イ：より広い集約経路より具体的な経路が優先される。

ウ：L3の通常の経路選択はMACアドレス大小で決まらない。

エ：一般的なIP転送の最長一致原則とは無関係である。

総合解説：経路選択では、まず宛先へのプレフィックス一致を評価し、最も具体的な経路を選ぶ。デフォルトルート/0は最も具体性が低い。

問82 VRF（Virtual Routing and Forwarding）の主な目的として最も適切なものはどれか。

- ア．Ethernetの物理速度を自動的に倍増する
- イ．同一ルータ上で複数の独立したルーティング/フォワーディングテーブルを保持する
- ウ．全VLANを一つへ統合する
- エ．TCPの暗号化を行う

正答：イ

4肢解説

ア：VRFはL3の経路分離機能であり物理速度を変更しない。

イ：正しい。VRFにより顧客や用途ごとに経路空間を分離できる。

ウ：VRFは論理分離に利用される。

エ：VRF自体は暗号化機能ではない。

総合解説：VRFは同一装置上でルーティングテーブルを分離し、重複アドレス空間を扱うVPNなどに利用される。

問83 MPLSの転送に関する説明として最も適切なものはどれか。

ア．必ず宛先MACアドレスだけでAS間経路を決める

イ．DNS名をラベルとして直接利用する

ウ．パケットをFECへ分類し、付与されたラベルを用いてLSR間で転送できる

エ．TCPポート番号をEthernet FCSへ書き換える

正答：ウ

4肢解説

ア：MPLSはラベルを用いた転送であり、AS間経路をMACだけで決めるものではない。

イ：MPLSラベルはDNS名ではない。

ウ：正しい。MPLSではFECに対応するラベルを用いてラベルスイッチングを行う。

エ：そのような処理はMPLSの基本動作ではない。

総合解説：MPLSでは入口でパケットをFECへ分類し、ラベルプッシュ、スワップ、ポップなどを行って転送する。

問84 同一宛先に対して同じコストの複数経路を持ち、複数の次ホップヘトラフィックを分散する方式は一般に何と呼ばれるか。

ア．NAT

イ．ARP

ウ．STP

エ．ECMP

正答：エ

4肢解説

ア：アドレス変換技術であり等コスト経路分散ではない。

イ：IPv4アドレスからリンク層アドレスを解決するプロトコルである。

ウ：L2ループ防止プロトコルでありL3の等コスト経路分散ではない。

エ：正しい。Equal-Cost Multi-Pathは等コストの複数経路を利用する方式である。

総合解説：ECMPでは通常、フロー順序を保つためハッシュ等で次ホップを選択する実装が多い。

問85 顧客Aと顧客Bがともに内部で10.0.0.0/8を使っている。1台のPEルータで両顧客を分離して扱うために有効な仕組みはどれか。
ア．顧客ごとに別VRFへ収容する
イ．両顧客を必ず同一VRFへ入れる
ウ．MACアドレスを全てFF:FF:FF:FF:FF:FFへ変更する
エ．TTLを0に固定する

正答：ア

4肢解説

ア：正しい。VRFごとに独立したルーティングテーブルを持つため、同じIPv4プレフィックスでも別コンテキストとして扱える。
イ：同一経路空間では重複プレフィックスの区別ができなくなる。
ウ：ブロードキャスト化するだけでL3アドレス重複を解決しない。
エ：パケットが転送されなくなる。

総合解説：VRFは顧客ごとに経路空間を分離し、MPLS L3VPNなどで重複アドレスを扱う基礎となる。

問86 BGP/MPLS IP VPNで、異なるVRFに存在する同一IPv4プレフィックスをVPN-IPv4経路として一意に区別するために用いるものはどれか。

ア．Route Target (RT) だけ
イ．Route Distinguisher (RD)
ウ．EtherType
エ．OSPF Router ID

正答：イ

4肢解説

ア：RTは主にVPN経路のインポート/エクスポートポリシーに用いられ、経路一意性を付与するRDとは役割が異なる。
イ：正しい。RDをIPv4プレフィックスへ付加することで、重複する顧客アドレスをBGP上で一意に扱える。
ウ：Ethernet上位プロトコル識別値である。
エ：OSPFルータ識別子でありVPN-IPv4経路一意化の仕組みではない。

総合解説：RDはVPN-IPv4アドレスを一意化する識別子で、RTはどのVRFが経路を取り込むかというポリシーに使う。

問87 BGP/MPLS IP VPNで、あるVPN経路をどのVRFへインポートするかを制御するために代表的に利用されるものはどれか。

- ア . Route Distinguisher (RD)
- イ . IPv4 TTL
- ウ . Route Target (RT)
- エ . Ethernet FCS

正答：ウ

4肢解説

ア：RDは重複プレフィックスを一意化するための識別子で、主目的はインポート制御ではない。

イ：転送寿命を制御する値でVPNメンバーシップ制御には使わない。

ウ：正しい。RTはBGP拡張コミュニティとしてVPN経路のインポート/エクスポートポリシーに利用される。

エ：フレーム誤り検出値である。

総合解説：RDとRTは混同しやすい。RDは一意性、RTはVPN経路の所属・配布ポリシーを表す。

問88 MPLS中継LSRが受信したラベル付きパケットについて、入力ラベルを対応する出力ラベルへ置き換えて転送する操作はどれか。

- ア . ラベルプッシュ
- イ . ラベルポップ
- ウ . ARPリブライ
- エ . ラベルスワップ

正答：エ

4肢解説

ア：新しいラベルをスタックへ追加する操作である。

イ：最上位ラベルを取り除く操作である。

ウ：IPv4アドレス解決の応答でMPLSラベル操作ではない。

エ：正しい。中継LSRはLFIB等に従い入力ラベルを出力ラベルへ交換して転送できる。

総合解説：MPLSの代表的なラベル操作はpush、swap、popであり、入口・中継・出口で役割が異なる。

問89 MPLSバックボーンを使うBGP/MPLS L3VPNで、入口PEから出口PEへ顧客パケットを運ぶ際に二つのラベルを使う設計の説明として最も適切なものはどれか。
ア．外側ラベルで出口PEまでのトランスポートを示し、内側ラベルで出口側のVPN/転送文脈を識別する
イ．二つともEthernet VLAN IDとして使う
ウ．外側ラベルはDNS名、内側ラベルはTCPポート番号を表す
エ．二つのラベルは必ず同じ値でなければならない

正答：ア

4肢解説

ア：正しい。典型的なL3VPNでは外側のトランスポートラベルと内側のVPNラベルをスタックして転送する。

イ：MPLSラベルは802.1Q VLAN IDとは別の識別子である。

ウ：そのような意味付けではない。

エ：異なる役割を持つため同値である必要はない。

総合解説：MPLS VPNではラベルスタックにより、バックボーン内のトランスポートと顧客VPN識別を分離できる。

問90 サービスプロバイダが複数顧客のL3VPNを提供している。制御プレーンと転送プレーンの対応として最も妥当なものはどれか。

ア．CEが全顧客のVRFを必ず集中管理し、PEはL2ハブとしてのみ動作する

イ．PEはVRFで顧客経路を分離し、BGPでVPN経路を配布し、MPLSラベルでバックボーン転送を行う

ウ．MPLSを使うとルーティング情報は一切不要になる

エ．VRFを使うと顧客間の経路は自動的に全共有される

正答：イ

4肢解説

ア：一般的なRFC 4364型L3VPNの役割分担と異なる。

イ：正しい。BGP/MPLS L3VPNではVRF、MP-BGP系のVPN経路配布、MPLSラベル転送を組み合わせる。

ウ：ラベル転送にもFECや経路、ラベル配布などの制御情報が必要である。

エ：RT等のポリシーにより共有範囲を制御でき、分離が基本である。

総合解説：BGP/MPLS L3VPNは、VRFで顧客のルーティング空間を分離し、BGPでVPN経路を交換し、MPLSラベルでコアを効率的に転送する。

問91 TCPがアプリケーションに提供するサービスとして最も適切なものはどれか。

- ア．信頼性のある順序付きバイトストリーム
- イ．メッセージ境界を保持する信頼性なしのデータグラム
- ウ．各パケットを必ず同一経路で転送するネットワークサービス
- エ．ブロードキャストによる1対多配信

正答：ア

4肢解説

ア：正しい。TCPは損失検出・再送・シーケンス制御などにより、信頼性のある順序付きバイトストリームを提供する。

イ：これはUDPの性質に近く、TCPはアプリケーションのメッセージ境界を保持しない。

ウ：経路選択はIP層の機能であり、TCPが同一経路を保証するものではない。

エ：TCPは基本的にユニキャストのコネクション指向通信である。

総合解説：TCPはコネクション指向で、アプリケーションには順序付きのバイト列としてデータを渡す。

問92 TCPで通常の接続確立時に交換される制御フラグの順序として適切なものはどれか。

- ア．ACK → SYN → FIN
- イ．SYN → SYN+ACK → ACK
- ウ．SYN → FIN → ACK
- エ．RST → SYN+ACK → ACK

正答：イ

4肢解説

ア：通常の接続確立手順ではない。FINは接続終了時に用いられる。

イ：正しい。クライアントがSYNを送り、サーバがSYN+ACKで応答し、クライアントがACKを返すことで接続を確立する。

ウ：接続確立途中にFINを使う手順ではない。

エ：RSTは接続のリセットに用いられるため、通常の接続確立手順ではない。

総合解説：TCPの3ウェイハンドシェイクでは、双方の初期シーケンス番号を確認しながら接続状態を確立する。

問93 TCP接続確立で、クライアントがシーケンス番号1000のSYNを送信した。サーバがこのSYNを正常に受信したとき、通常返すACK番号はどれか。
ア．ACK=1000（SYNが番号を消費しない考える）
イ．ACK=999（受信済み番号の直前を返す考える）
ウ．ACK=1001（SYNが1番号を消費する考える）
エ．ACK=2000（初期番号を2倍して返す考える）

正答：ウ

4肢解説

ア：SYN自身がシーケンス番号を1つ消費することを反映していない。
イ：受信済みSYNより前の番号であり、次に期待する番号ではない。
ウ：正しい。SYNはシーケンス番号空間を1つ消費するため、次に期待する番号は1001となる。
エ：送信元の初期シーケンス番号とは無関係な値である。

総合解説：SYNとFINはデータ長が0でもシーケンス番号空間を1つ消費する。ACK番号は次に受信したいシーケンス番号を示す。

問94 TCPヘッダの送信元ポート番号と宛先ポート番号の主な役割はどれか。

ア．ルータが最短経路を計算する
イ．Ethernetの宛先NICを識別する
ウ．DNS名をIPアドレスへ変換する
エ．同一ホスト上の複数アプリケーション通信を識別・多重化する

正答：エ

4肢解説

ア：経路計算はIPルーティングの機能であり、TCPポート番号の役割ではない。
イ：データリンク層ではMACアドレスが用いられる。
ウ：名前解決はDNSの機能である。
エ：正しい。ポート番号はホスト内の通信端点を識別し、複数のTCP通信を多重化するために使われる。

総合解説：TCP接続は送信元・宛先のIPアドレスとポート番号などによって識別される。

問95 TCP受信側が広告する受信ウィンドウ（rwnd）の主な目的はどれか。

ア．受信側バッファを超えてデータが送られないよう送信量を制限する

イ．ネットワーク全体の輻輳だけを検出する

ウ．EthernetフレームのFCSを計算する

エ．IPパケットのTTLを増やす

正答：ア

4肢解説

ア：正しい。rwndは受信側が現在受け入れ可能なデータ量を送信側へ通知し、フロー制御を行う。

イ：輻輳制御には主にcwndなどが用いられ、rwndは受信側能力に基づくフロー制御である。

ウ：FCSはデータリンク層の誤り検出である。

エ：TTL/Hop LimitはIP層のフィールドであり、TCP受信ウィンドウとは関係しない。

総合解説：TCP送信側は受信側の処理能力とネットワーク輻輳の両方を考慮して送信量を調整する。

問96 TCPのMSS（Maximum Segment Size）の説明として適切なものはどれか。

ア．Ethernetフレーム全体の最大長そのもの

イ．1セグメントで送るTCPデータ部の最大サイズを示す値

ウ．受信側が広告するウィンドウサイズそのもの

エ．ルータが保持できる経路数の上限

正答：イ

4肢解説

ア：それはMTUやフレームサイズに関する説明であり、MSSとは異なる。

イ：正しい。MSSはTCPヘッダやIPヘッダを除いたTCPペイロードの最大サイズを表す。

ウ：受信ウィンドウはフロー制御の値であり、MSSとは役割が異なる。

エ：ルーティングテーブル容量とは無関係である。

総合解説：MSSは一般に経路上のMTUを踏まえて設定され、IPフラグメンテーションを避ける観点でも重要である。

問97 TCPのSACK (Selective Acknowledgment) を利用する主な利点はどれか。
ア．暗号鍵を交換できる
イ．IPアドレスを自動割当てできる
ウ．受信済みの不連続なデータ範囲を送信側へ知らせ、必要な部分を効率よく再送できる
エ．TCPをコネクションレスに変える

正答：ウ

4肢解説

ア：SACKは再送効率化のためのTCPオプションであり、暗号鍵交換機能ではない。
イ：アドレス自動割当てはDHCPなどの役割である。
ウ：正しい。SACKにより受信済みブロックを通知でき、複数損失時などに不要な再送を減らせる。
エ：SACKを使ってもTCPはコネクション指向のままである。
総合解説：累積ACKだけではどの後続データを受信済みか分かりにくい場合がある。SACKはその情報を補う。

問98 TCPの再送タイムアウト (RTO) を、観測した往復時間 (RTT) とは無関係に常に極端に短い固定値へ設定すると、どの問題が起こりやすいか。
ア．受信ウィンドウが必ず最大になる
イ．TCPヘッダが自動的に短くなる
ウ．IPアドレスが重複する
エ．正常な遅延でも損失と誤認して不要な再送が増える

正答：エ

4肢解説

ア：RTOと受信ウィンドウ最大化には直接の因果関係はない。
イ：RTO設定でTCPヘッダ長は変わらない。
ウ：アドレス重複はRTO設定とは無関係である。
エ：正しい。RTOが実際のRTTに対して短すぎると、ACK到着前にタイムアウトして不要な再送を起こしやすい。
総合解説：TCPはRTTを観測しながら再送タイマを調整する。早すぎる再送も遅すぎる再送も性能を悪化させる。

問99 TCPで能動クローズ側が一定時間TIME-WAIT状態を保持する理由として最も適切なものはどれか。

ア．遅延した旧セグメントの影響を抑え、最後のACKが失われた場合の再送にも対応するため

イ．DNSキャッシュのTTLを待つため

ウ．EthernetスイッチのMAC学習を完了させるため

エ．必ず暗号鍵を破棄するため

正答：ア

4肢解説

ア：正しい。TIME-WAITは古い接続の重複セグメントが新しい接続へ混入するのを防ぎ、FIN再送への応答も可能にする。

イ：DNS TTLとTCP TIME-WAITは別の仕組みである。

ウ：MACアドレス学習とは無関係である。

エ：TCP自体は暗号鍵管理を行わない。

総合解説：TIME-WAITはTCP接続の安全な終了に関わる状態で、単なる無駄な待ち時間ではない。

問100 TCPチェックサム計算でIPアドレスなどを含む疑似ヘッダを利用する主な目的はどれか。

ア．TCPデータを暗号化するため

イ．誤った通信端点へ配送されたセグメントなども検出しやすくするため

ウ．IPアドレスをNAT変換するため

エ．ルーティングプロトコルを選択するため

正答：イ

4肢解説

ア：チェックサムは誤り検出用であり、機密性を提供しない。

イ：正しい。疑似ヘッダには送信元・宛先IPアドレス等が含まれ、TCPセグメントと配送先情報を関連付けて誤り検出する。

ウ：NATの変換処理自体を行うものではない。

エ：経路選択とは無関係である。

総合解説：TCPチェックサムはヘッダとデータに加え、IP層の一部情報を疑似ヘッダとして含めて計算する。

問101 受信側が次にシーケンス番号5000から始まるデータを期待している。5000～5999の1000バイトが欠落したまま、その後の6000～6999を受信した場合、通常の累積ACKで返されるACK番号として最も適切なものはどれか。
ア．ACK=6000（後続ブロック先頭まで進める）
イ．ACK=7000（後続ブロック末尾まで進める）
ウ．ACK=5000（欠落先頭を次の期待番号として維持する）
エ．ACK=4999（最後に連続受信した番号を返す）

正答：ウ

4肢解説

ア：5000～5999が欠落しているため、次に期待する番号を6000へ進めることはできない。

イ：後続データを受信しても、欠落部分があるため累積ACKは7000まで進まない。

ウ：正しい。累積ACKは連続して受信できた範囲の次の番号を示すため、5000からの欠落が埋まるまでは5000を通知する。

エ：ACK番号は最後に受信した番号ではなく、次に期待する番号を示す。

総合解説：TCPの累積ACKでは、順序外で後続データを受信しても欠落箇所の先頭がACK番号として繰り返し通知される。SACK利用時は受信済み範囲も追加通知できる。

問102 TCP接続で一方がFINを送り、そのFINがACKされた後も、反対方向のデータ送信が継続できる理由として適切なものはどれか。

ア．FINは単なる受信ウィンドウ拡張要求だから

イ．TCPは常に片方向通信しかできないから

ウ．ACKを受信すると自動的に新しいTCP接続が作られるから

エ．TCPは双方向のバイトストリームを方向ごとに独立して終了できるため

正答：エ

4肢解説

ア：FINは送信終了を示す制御フラグであり、ウィンドウ拡張要求ではない。

イ：TCPは双方向通信をサポートする。

ウ：ACKで別接続が自動生成されるわけではない。

エ：正しい。FINは送信した側からのデータ送信終了を示し、反対方向のストリームまで直ちに終了させるものではない。

総合解説：TCPでは各方向の送信終了を独立して扱えるため、片方向だけを閉じたハーフクローズ状態が成立する。

問103 コネクション確立を伴わないUDPの通信モデルを説明したものとして、最も適切なものはどれか。

ア．コネクション確立を行わず、データグラム単位で送受信する

イ．3ウェイハンドシェイク後に信頼性のあるバイトストリームを提供する

ウ．全てのパケット損失を自動再送して必ず順序通り届ける

エ．経路情報を交換して最短経路を計算する

正答：ア

4肢解説

ア：正しい。UDPはコネクションレスで、アプリケーションのデータグラム境界を保持して送受信する。

イ：これはTCPの特徴である。

ウ：UDP自体は再送や順序保証を提供しない。

エ：これはルーティングプロトコルの役割である。

総合解説：UDPは低いプロトコルオーバーヘッドが特徴だが、信頼性や順序制御が必要ならアプリケーション側などで補う必要がある。

問104 UDPヘッダに含まれるフィールドの組合せとして適切なものはどれか。

ア．シーケンス番号、ACK番号、ウィンドウ、SYN

イ．送信元ポート、宛先ポート、長さ、チェックサム

ウ．送信元MAC、宛先MAC、EtherType、FCS

エ．TTL、Protocol、送信元IP、宛先IPだけ

正答：イ

4肢解説

ア：これらはTCPIに關係するフィールドである。

イ：正しい。UDP基本ヘッダはこれら4フィールドで構成される。

ウ：これらはEthernetフレームに關係する。

エ：これらはIPヘッダ側の情報であり、UDPヘッダの構成ではない。

総合解説：UDPはTCPより単純なヘッダを持ち、接続管理や再送制御のフィールドを持たない。

問105 アプリケーションがUDPソケットから2回に分けて100バイトと200バイトのデータグラムを送信した。受信側での扱いとして基本的に適切なものはどれか。

ア．必ず300バイトの連続バイトストリームとして結合される

イ．必ず1バイトずつ別パケットになる

ウ．それぞれ別個のUDPデータグラムとして境界が保たれる

エ．必ず送信順序通りに到着することが保証される

正答：ウ

4肢解説

ア：これはTCPのバイトストリームのな考え方に近く、UDPではない。

イ：送信単位を自動的に1バイトずつに分割する仕様ではない。

ウ：正しい。UDPはデータグラム指向で、送信単位のメッセージ境界を保持する。

エ：UDP自体には順序保証がない。

総合解説：UDPではアプリケーションはデータグラム単位で送受信する。ただし損失・重複・順序逆転への保証はない。

問106 多少のパケット損失よりも遅延増大を避けることを優先し、アプリケーション側で必要な補正を行えるリアルタイム音声通信について、トランスポートの選択として一般に適しやすいものはどれか。

ア．TCPの再送が完了するまで必ず再生を停止する方式だけを採用する

イ．ARPだけで音声データを転送する

ウ．OSPFをアプリケーションの音声転送プロトコルとして使う

エ．UDPを利用し、必要な損失対策や順序処理を上位で行う

正答：エ

4肢解説

ア：リアルタイム性を重視する用途では再送待ちが大きな遅延要因になる場合がある。

イ：ARPはアドレス解決用で、音声トランスポートではない。

ウ：OSPFはルーティングプロトコルである。

エ：正しい。リアルタイム通信では再送待ちによる遅延を避けるため、UDPを基盤にRTP等を利用する構成が一般的である。

総合解説：UDPはリアルタイム系や問い合わせ応答型など、アプリケーション自身が信頼性・遅延要件を制御したい用途で使われる。

問107 QUICの説明として最も適切なものはどれか。

ア．UDPを基盤に、暗号化された接続管理や複数ストリームなどを提供するトランスポートである

イ．EthernetのVLANタグを暗号化する規格である

ウ．TCPの上に必ずTCPを二重化して動作する

エ．DNSのゾーン転送だけに使われる専用プロトコルである

正答：ア

4肢解説

ア：正しい。QUICはUDP上に構築され、TLSを統合した安全な接続とストリーム多重化などを提供する。

イ：QUICはトランスポートプロトコルであり、VLANタグ暗号化規格ではない。

ウ：QUICは基本的にUDP上で動作する。

エ：QUICの用途はDNSゾーン転送に限定されない。

総合解説：QUICはユーザ空間で実装しやすく、暗号化、接続確立、ストリーム多重化、接続移行などを統合する。

問108 HTTP/3がQUICの複数ストリームを利用する利点として最も適切なものはどれか。

ア．全パケットが損失しても再送が不要になる

イ．あるストリームのパケット損失が、他の独立ストリームの配送まで必ず停止させることを避けやすい

ウ．IPルーティングが不要になる

エ．TLSによる暗号化を使えなくなる

正答：イ

4肢解説

ア：QUICにも信頼性を確保するための損失検出と再送がある。

イ：正しい。QUICではストリームごとに順序制御されるため、TCP上のHTTP/2で生じるトランスポート層のHOLブロッキングを軽減できる。

ウ：QUICもIPネットワーク上で通信する。

エ：QUICはTLS 1.3を利用して暗号化を統合している。

総合解説：QUICは接続内に複数ストリームを持ち、ストリーム間の独立性を高めることで一つの損失が全アプリケーションデータを止める影響を減らす。

問109 スマートフォンがWi-Fiからモバイル回線へ切り替わり、送信元IPアドレスとポート番号が変化した。QUICがTCPより接続を維持しやすい理由として適切なものはどれか。
ア．QUICはIPアドレスを一切使わないため
イ．QUICは全てのパケットをブロードキャストするため
ウ．Connection IDによって接続を識別でき、ネットワーク経路の変更に対応する仕組みを持つため
エ．QUICではルータが端末のセッション状態を必ず保存するため

正答：ウ

4肢解説

ア：実際にはQUICもUDP/IP上で通信する。

イ：ブロードキャストで接続を維持する仕組みではない。

ウ：正しい。QUICはConnection IDを用いて接続を識別し、IPアドレスやポートが変化する接続移行を支援する。

エ：接続維持をルータの必須状態保存に依存するものではない。

総合解説：QUICの接続識別はTCPの4タプルだけに固定されず、Connection IDを用いることで端末の経路変更に柔軟に対応できる。

問110 QUICについて『UDP上で動くので、ネットワーク輻輳を考慮せず無制限に送信してよい』という説明が誤りである理由として最も適切なものはどれか。

ア．UDPが常にTCPの輻輳ウィンドウを自動継承するため

イ．QUICは輻輳時にEthernetのVLAN IDを変更するため

ウ．QUICではパケット損失が物理的に発生しないため

エ．QUIC自身が損失検出と輻輳制御を実装し、ネットワーク状況に応じて送信量を調整するため

正答：エ

4肢解説

ア：UDPにはTCPのcwndを自動継承する仕組みはない。

イ：VLAN ID変更はQUIC輻輳制御の仕組みではない。

ウ：QUIC通信でもパケット損失は発生し得る。

エ：正しい。QUICはUDPを利用するが、信頼性や輻輳制御をQUIC層で実現する。

総合解説：QUICはUDP上に独自の信頼性・損失検出・輻輳制御を実装するため、UDP採用は『制御をしない』ことを意味しない。

問111 TCP送信側が同時に送信できる未確認データ量を決める際、受信側の処理能力とネットワーク輻輳の両方を考慮する考え方として適切なものはどれか。

- ア．受信ウィンドウ`rwnd`と輻輳ウィンドウ`cwnd`の小さい方を上限として考える
- イ．`rwnd`と`cwnd`の大きい方だけを必ず採用する
- ウ．常にEthernetのMTUだけで送信量を決める
- エ．DNSのTTLに応じて送信量を決める

正答：ア

4肢解説

ア：正しい。`rwnd`は受信側のフロー制御、`cwnd`はネットワーク輻輳制御の制約を表し、実効送信量は両者の制約を受ける。

イ：大きい方を採用すると、受信側能力または輻輳制御の制約を超える可能性がある。

ウ：MTUは1パケットの大きさに関係するが、未確認データ総量の制御とは異なる。

エ：DNS TTLはキャッシュ有効時間であり、TCP送信ウィンドウとは無関係である。

総合解説：フロー制御は受信側を過負荷から守り、輻輳制御はネットワーク全体の混雑を抑える。両者は目的が異なる。

問112 TCPのslow startで、損失などがなくACKが順調に返る場合の`cwnd`の増加傾向として最も適切なものはどれか。

- ア．常に一定値のまま変化しない
- イ．おおむねRTTごとに指数的に増加する
- ウ．おおむねRTTごとに半減する
- エ．DNS応答数に比例して増える

正答：イ

4肢解説

ア：slow startでは通信開始直後などに`cwnd`を拡大して利用可能帯域を探る。

イ：正しい。slow startではACKごとに`cwnd`が増え、結果として概ねRTT単位で倍増するような増え方になる。

ウ：損失時の減少動作とは異なる。

エ：DNSとは無関係である。

総合解説：slow startは小さい送信量から急速に増やし、ネットワーク容量を探索する仕組みである。

問113 DiffServでIPパケットに転送クラスを示すために利用される値として最も適切なものはどれか。

- ア．TCPのACK番号
- イ．EthernetのFCS
- ウ．DSCP
- エ．DNSのMX優先度

正答：ウ

4肢解説

ア：ACK番号はTCPの信頼性制御に用いる。

イ：FCSはフレーム誤り検出に用いる。

ウ：正しい。DSCPはIPv4/IPv6のDSフィールド内に設定され、各ノードで適用する転送動作の識別に利用される。

エ：メール配送先選択に関する値でありQoS分類ではない。

総合解説：DiffServではパケットをクラス分けし、DSCPに応じてPHBを適用することでスケーラブルなQoS制御を行う。

問114 TCPがslow start thresholdを超え、congestion avoidanceで動作しているときのcwndの増加特性として一般に最も適切なものはどれか。

- ア．毎RTT必ず2倍になる
- イ．ACKを受信するたび必ず0へ戻す
- ウ．常に受信ウィンドウと無関係に無限増加する
- エ．slow startより緩やかに、概ね線形に増加する

正答：エ

4肢解説

ア：これはslow startの増加傾向に近い。

イ：通常のcongestion avoidance動作ではない。

ウ：実際にはrwndや損失・輻輳状態などの制約を受ける。

エ：正しい。congestion avoidanceでは急激な指数増加を避け、より慎重に送信量を増加させる。

総合解説：TCPはslow startとcongestion avoidanceを使い分け、利用可能帯域を探しながら輻輳を抑制する。

問115 TCPで再送タイムアウトを待たずに欠落セグメントの再送を開始するfast retransmitの代表的な契機はどれか。

ア．同じACK番号の重複ACKを複数回受信する

イ．DNSキャッシュが期限切れになる

ウ．ARP Requestを1回受信する

エ．HTTPステータス200を受信する

正答：ア

4肢解説

ア：正しい。典型的には3個の重複ACKを受信すると、欠落が推定されfast retransmitを行う。

イ：DNS TTLとTCP再送制御は無関係である。

ウ：ARP受信はTCP fast retransmitの直接条件ではない。

エ：アプリケーション層の応答コードであり、TCPの損失検出条件ではない。

総合解説：重複ACKは後続セグメントが届いている一方で途中が欠落している可能性を示すため、タイムアウト前の再送判断に使える。

問116 ECN (Explicit Congestion Notification) の主な目的はどれか。

ア．IPアドレスを自動割当てる

イ．必ずパケットを廃棄しなくても、輻輳の兆候をエンドホストへ通知できるようにする

ウ．Ethernetの衝突を検出する

エ．TLS証明書を検証する

正答：イ

4肢解説

ア：これはDHCPの機能である。

イ：正しい。ECN対応ルータは輻輳時にマーキングでき、受信側から送信側へ輻輳を知らせて送信量調整を促せる。

ウ：CSMA/CDなどのデータリンク制御とは異なる。

エ：証明書検証とは無関係である。

総合解説：ECNは損失だけに依存せず輻輳を明示通知する仕組みで、対応するIP・TCPのフィールドを利用する。

問117 契約帯域を超えたトラフィックを即座に廃棄またはマーキングする制御と、バッファして送信タイミングを遅らせ平滑化する制御の組合せとして適切なものはどれか。

ア．前者がシェーピング、後者がポリシング

イ．両方ともDNSキャッシュ制御

ウ．前者がポリシング、後者がシェーピング

エ．両方ともTCPの3ウェイハンドシェイク

正答：ウ

4肢解説

ア：両者の説明が逆である。

イ：帯域制御とDNSキャッシュは無関係である。

ウ：正しい。ポリシングは超過トラフィックを廃棄・再マーキングしやすく、シェーピングは待ち行列で送信を平滑化する。

エ：接続確立手順とは異なる。

総合解説：QoS設計では、超過時に捨てるのか遅延させるのかを要件に応じて使い分ける必要がある。

問118 DiffServのEF PHBを優先的に適用する候補として最も適切なトラフィックはどれか。

ア．数日後に届いても問題ない大容量バックアップだけ

イ．ARPテーブルの静的設定ファイル

ウ．DNSゾーンファイルのコメント行

エ．遅延やジッタに敏感で、帯域を適切に制御したリアルタイム音声

正答：エ

4肢解説

ア：低遅延性の優先度が低く、EFを最優先で割り当てる必要性は低い。

イ：転送トラフィックの種類ではない。

ウ：ネットワーク上の優先転送対象そのものではない。

エ：正しい。EFは低損失・低遅延・低ジッタの転送を狙うPHBで、音声などのリアルタイム通信に利用されることがある。

総合解説：EFは優先制御だけでなく、過大なEFトラフィックが他通信を圧迫しないよう帯域制御と組み合わせることが重要である。

問119 TCP送信側のcwndが64KB、受信側が広告するrwndが24KBであり、他の制約を無視する。未確認データの送信上限として最も適切な値はどれか。
ア．24KB（min(cwnd,rwnd)で判断）
イ．64KB（cwndだけで判断）
ウ．88KB（cwnd+rwndで判断）
エ．40KB（cwnd-rwndで判断）

正答：ア

4肢解説

ア：正しい。実効的にはcwndとrwndの小さい方の制約を受けるため、24KBが上限となる。

イ：受信側が24KBしか受け入れられないため、cwndだけでは決められない。

ウ：cwndとrwndを加算するものではない。

エ：両者の差を使うものではない。

総合解説：TCPの送信量は、受信側フロー制御とネットワーク輻輳制御の両方を満たす必要がある。

問120 厳格優先キューイングで音声クラスを常に最優先し、帯域上限を設けなかった。音声トラフィックが急増した場合に起こり得る問題として最も適切なものはどれか。

ア．全てのIPアドレスが自動的に変更される

イ．低優先度キューが長時間送信機会を得られず、飢餓状態になる可能性がある

ウ．TCPチェックサムが無効化される

エ．DNSの権威サーバが必ず停止する

正答：イ

4肢解説

ア：キューイング制御はIPアドレス割当てを変更しない。

イ：正しい。厳格優先制御は高優先トラフィックが多すぎると他クラスを圧迫するため、ポリシング等との併用が重要である。

ウ：優先キューイングでTCPチェックサム機能が無効になるわけではない。

エ：直接の因果関係はない。

総合解説：QoSは優先度を付けるだけでは不十分で、各クラスの帯域設計、キュー長、廃棄方式、ポリシングなどを総合的に設計する必要がある。

問121 DNSの再帰問い合わせの説明として最も適切なものはどれか。
ア．DNSサーバは必ず次に問い合わせるべきサーバ情報だけを返す
イ．クライアントが必ずEthernetのMACアドレスを直接指定する
ウ．問い合わせを受けたDNSサーバが、最終的な回答またはエラーを得るまで必要な問い合わせ処理を引き受ける
エ．問い合わせのたびに必ずゾーン転送を行う

正答：ウ

4肢解説

ア：これは反復問い合わせで見られる動作に近い。

イ：DNS名前解決の方式とは無関係である。

ウ：正しい。再帰問い合わせでは、クライアントは問い合わせ先サーバに解決処理を委ねる。

エ：通常の名前解決でAXFRを行うわけではない。

総合解説：スタブリゾルバからキャッシュDNSサーバへの問い合わせは再帰型で行われることが多く、キャッシュDNSサーバは権威サーバなどへ反復的に問い合わせる。

問122 あるドメイン宛てメールを受け取るメールサーバを示すDNSリソースレコードはどれか。

ア．A

イ．AAAA

ウ．PTR

エ．MX

正答：エ

4肢解説

ア：Aレコードはホスト名に対応するIPv4アドレスを示す。

イ：AAAAレコードはホスト名に対応するIPv6アドレスを示す。

ウ：PTRレコードは主に逆引きで名前を参照するために用いられる。

エ：正しい。MXレコードはドメインのメール交換先を示し、優先度値とともにSMTP配送で利用される。

総合解説：DNSでは用途に応じてA、AAAA、MX、NS、CNAME、PTRなどのレコードを使い分ける。

問123 DHCPv4で新規クライアントがアドレスを取得する代表的なメッセージ順序として適切なものはどれか。

ア．DHCPDISCOVER → DHCPOFFER → DHCPREQUEST → DHCPACK
イ．DHCPACK → DHCPDISCOVER → DHCPOFFER → DHCPREQUEST
ウ．DHCPOFFER → DHCPDISCOVER → DHCPACK → DHCPREQUEST
エ．DHCPREQUEST → DHCPACK → DHCPDISCOVER → DHCPOFFER

正答：ア

4肢解説

ア：正しい。クライアントがサーバを探索し、提示された設定を要求し、サーバが承認する代表的なDORA手順である。

イ：ACKは要求が承認された後に返されるため順序が不適切である。

ウ：クライアントの探索より先にOFFERが始まる通常手順ではない。

エ：新規取得の代表的な順序ではない。

総合解説：DHCPではIPアドレスだけでなく、サブネットマスク、デフォルトゲートウェイ、DNSサーバ等も配布できる。

問124 DNSリソースレコードのTTLを短く設定することの一般的な効果として最も適切なものはどれか。

ア．DNSSECを自動的に無効化する
イ．変更がキャッシュに長期間残りにくくなる一方、権威DNSへの問い合わせが増えやすい
ウ．IPv4アドレスをIPv6へ自動変換する
エ．DHCPリース時間と必ず同一になる

正答：イ

4肢解説

ア：TTLの長短だけでDNSSECが無効になるわけではない。

イ：正しい。TTLが短いとキャッシュ更新が早くなるが、再問い合わせ頻度が増える。

ウ：TTLにはアドレス変換機能はない。

エ：DNS TTLとDHCPリース時間は独立した設定である。

総合解説：DNS変更時の反映速度と問い合わせ負荷はトレードオフになるため、運用要件に応じたTTL設計が必要である。

問125 自組織のexample.jpゾーンを管理し、そのゾーンの正式な回答を提供するDNSサーバの役割として最も適切なものはどれか。

- ア．キャッシュDNSサーバだけ
- イ．DHCPリレー
- ウ．権威DNSサーバ
- エ．NTPサーバ

正答：ウ

4肢解説

ア：キャッシュDNSは利用者の名前解決を代行・キャッシュする役割で、対象ゾーンの正式管理者とは限らない。

イ：DHCPメッセージを異なるセグメント間で中継する機能である。

ウ：正しい。権威DNSサーバは管理対象ゾーンのゾーンデータに基づき権威ある回答を返す。

エ：時刻同期を提供するサーバである。

総合解説：DNS運用では、権威DNSと再帰・キャッシュDNSを役割分離して設計することが多い。

問126 DHCPクライアントとDHCPサーバが異なるIPサブネットにあり、ルータがクライアントのブロードキャストをそのまま転送しない。一般的な解決方法はどれか。

- ア．全クライアントにBGPを設定する
- イ．DNSのMXレコードを変更する
- ウ．EthernetのFCSを無効化する
- エ．ルータなどにDHCPリレー機能を設定し、DHCPメッセージをサーバへ中継する

正答：エ

4肢解説

ア：DHCPメッセージ中継の解決策ではない。

イ：メール配送設定でありDHCPとは無関係である。

ウ：DHCPブロードキャスト到達性とは無関係である。

エ：正しい。DHCPリレーを利用すると、各サブネットにDHCPサーバを置かずに集中配置できる。

総合解説：DHCPリレーはクライアント側サブネット情報をサーバに伝え、適切なアドレスプール選択を可能にする。

問127 DHCPクライアントが有効なリースを保持し続けるための動作として最も適切なものはどれか。

ア．リース期限前にDHCPREQUESTなどを用いて更新を試みる

イ．リース取得後は期限に関係なく永久使用する

ウ．毎秒必ずDHCPDISCOVERからやり直す

エ．DNSのTTLが切れるまで更新してはいけない

正答：ア

4肢解説

ア：正しい。クライアントはリース期間中に更新を行い、期限切れ前に継続利用可能か確認する。

イ：DHCPの動的アドレスはリース期限の管理対象である。

ウ：通常は既存リースの更新処理を行う。

エ：DNS TTLとDHCPリース更新は独立している。

総合解説：DHCPのリース方式により、アドレスを一定期間貸し出し、更新・再割当てを管理できる。

問128 NTPのstratumに関する説明として最も適切なものはどれか。

ア．数値が大きいほど必ず時刻精度が高いことを保証する

イ．基準時計からの同期階層を表し、一般に数値が小さいほど基準に近い階層である

ウ．IPアドレスのネットワーク長を表す

エ．メール配送の優先順位を表す

正答：イ

4肢解説

ア：stratumは同期階層を示すもので、単純に精度保証値ではない。

イ：正しい。NTPでは基準時計に近いサーバほど低いstratum番号を持つ。

ウ：CIDRプレフィックス長とは別の概念である。

エ：MX優先度とは無関係である。

総合解説：NTPでは複数の時刻源を評価しながら時刻を同期する。stratumは同期元までの階層的距離を表す。

問129 存在しないホスト名へのDNS問い合わせが大量に繰り返されている。否定応答を一定時間キャッシュする主な利点はどれか。

- ア：存在しない名前を自動的に有効な名前へ変更できる
- イ：DHCPのアドレス枯渇を直接解消する
- ウ：同じ不存在名への問い合わせを毎回権威サーバへ送らず、負荷と応答遅延を抑えられる
- エ：全DNS応答を永久保存する

正答：ウ

4肢解説

ア：negative cachingは名前を生成・修正する機能ではない。

イ：DHCPアドレスプールとは無関係である。

ウ：正しい。NXDOMAINなどの否定応答も適切にキャッシュすることで、同じ無効問い合わせの繰返しを減らせる。

エ：否定応答にも有効期間があり永久保存する仕組みではない。

総合解説：否定応答キャッシュはDNSの効率と安定性に寄与するが、保持時間を適切に管理する必要がある。

問130 利用者はIPアドレスを直接指定すればWebサーバへ接続できるが、ホスト名では接続できない。同一端末から設定済みDNSサーバへの問い合わせもタイムアウトする。最初に疑うべき領域として最も適切なものはどれか。

- ア：WebサーバのHTTPコンテンツだけ
- イ：TCPのTIME-WAITだけ
- ウ：端末の画面解像度
- エ：DNSサーバへの到達性またはDNSサービスの障害

正答：エ

4肢解説

ア：IP直接指定で接続できるため、まずDNS側の問題を疑う方が合理的である。

イ：DNS問い合わせタイムアウトの直接原因として最優先ではない。

ウ：ネットワーク名前解決とは無関係である。

エ：正しい。IP直接通信ができる一方、DNS問い合わせ自体がタイムアウトするため、名前解決経路・DNSサービスの確認が優先される。

総合解説：障害切り分けでは、IP疎通、名前解決、対象サービスの順に層を分けて確認すると原因範囲を狭めやすい。

問131 HTTPの基本的な通信モデルとして最も適切なものはどれか。

ア．クライアントがリクエストを送り、サーバがレスポンスを返す

イ．サーバだけが一方的に全クライアントへブロードキャストする

ウ．ルータ同士が経路情報だけを交換する

エ．DNSサーバがDHCPリースを配布する

正答：ア

4肢解説

ア：正しい。HTTPは要求と応答の交換を基本とするアプリケーション層プロトコルである。

イ：HTTPの基本モデルではない。

ウ：これはルーティングプロトコルの役割である。

エ：DNSとDHCPの役割を混同している。

総合解説：HTTPではメソッド、ターゲット、ヘッダ、コンテンツなどを含むリクエストに対し、ステータスコード等を含むレスポンスが返る。

問132 HTTPで、対象リソースの取得を目的とし、仕様上safe methodに分類される代表的なメソッドはどれか。

ア．POST

イ．GET

ウ．DELETE

エ．PATCH

正答：イ

4肢解説

ア：POSTは処理の実行や状態変更を伴い得るためsafe methodではない。

イ：正しい。GETは対象リソースの表現を取得するための代表的なsafe methodである。

ウ：対象リソースの削除を意味し、safe methodではない。

エ：部分更新に使われ、safe methodではない。

総合解説：safe methodは、クライアントがサーバ状態の変更を要求する意味を持たないメソッドである。GETやHEADなどが該当する。

問133 HTTPSの説明として最も適切なものはどれか。
ア．HTTPをEthernetのFCSだけで暗号化する
イ．HTTPをDNSへ変換する方式である
ウ．HTTP通信をTLSで保護し、暗号化や相手認証などを提供する
エ．TCPのポート番号を使用しないHTTPである

正答：ウ

4肢解説

ア：FCSは誤り検出用であり暗号化機能ではない。
イ：DNSは名前解決プロトコルでありHTTPSとは異なる。
ウ：正しい。HTTPSではHTTPをTLS上で利用し、通信内容の機密性・完全性やサーバ認証などを実現する。
エ：HTTPSでも通常はTCPまたはQUIC等のトランスポート上でポートを用いる。
総合解説：TLSはHTTP以外のアプリケーションにも利用可能で、暗号化と認証を提供する汎用のセキュリティプロトコルである。

問134 ブラウザが以前取得した表現を再検証するGETリクエストで、ETagをIf-None-Matchに設定して送信した。サーバ上の表現が変更されていなかった場合、代表的なレスポンスはどれか。
ア．201 Created
イ．404 Not Found
ウ．505 HTTP Version Not Supported
エ．304 Not Modified

正答：エ

4肢解説

ア：新しいリソースが作成された場合などに用いる。
イ：対象リソースが見つからない場合の応答であり、変更なしを示さない。
ウ：HTTPバージョンをサポートしない場合の応答である。
エ：正しい。表現が変更されていない場合、304を返してキャッシュ済み表現を再利用させることができる。
総合解説：ETagなどのバリデータを用了条件付きリクエストは、コンテンツ本体の再転送を減らしキャッシュを効率化する。

問135 機密性の高いレスポンスについて、共有キャッシュへの保存を避けたい。HTTPのキャッシュ制御を利用する際の考え方として最も適切なものはどれか。

- ア．Cache-Controlなどの指示を用いて保存可否や再利用条件を明示する
- イ．DNSのTTLだけを0にすればHTTPキャッシュも必ず無効になる
- ウ．TCPのMSSを小さくすれば保存されなくなる
- エ．EthernetのVLAN IDを変更すれば保存されなくなる

正答：ア

4肢解説

ア：正しい。HTTPのキャッシュ指示を利用して、キャッシュ可能性や再検証条件などを制御する。

イ：DNSキャッシュとHTTPキャッシュは別の仕組みである。

ウ：MSSはTCPセグメントサイズに関する値で、HTTPキャッシュ可否を決めない。

エ：VLANとHTTPキャッシュ制御は無関係である。

総合解説：HTTPキャッシュではCache-Controlやバリデータを使い、保存・再利用・再検証のポリシーを明確にする。

問136 HTTP/2が一つの接続上で複数のHTTP要求・応答を効率よく扱う仕組みとして最も適切なものはどれか。

- ア．要求ごとに必ず別のIPアドレスを割り当てる
- イ．複数のストリームをフレーム単位で多重化する
- ウ．全レスポンスをDNSゾーン転送で配信する
- エ．Ethernetフレームを必ずブロードキャストする

正答：イ

4肢解説

ア：ストリーム多重化にIPアドレス追加は不要である。

イ：正しい。HTTP/2では一つのTCP接続上で複数ストリームを多重化して並行処理できる。

ウ：DNSゾーン転送とは無関係である。

エ：HTTP/2の多重化方式ではない。

総合解説：HTTP/2はアプリケーション層でストリームを多重化するが、基盤が単一TCP接続であるためTCP層の損失は接続内データ全体へ影響し得る。

問137 HTTP/3のトランスポート基盤として適切なものはどれか。

- ア．OSPF
- イ．ARP
- ウ．QUIC
- エ．STP

正答：ウ

4肢解説

ア：OSPFはルーティングプロトコルである。

イ：ARPはIPv4アドレスとリンク層アドレスの解決に用いる。

ウ：正しい。HTTP/3はQUIC上でHTTPセマンティクスを利用する。

エ：STPはブリッジネットワークのループ防止に用いる。

総合解説：HTTP/3はQUICのストリーム多重化や接続確立機構を利用し、HTTP/2 over TCPとは異なる特性を持つ。

問138 社内クライアントの代理として外部Webサイトへアクセスし、アクセス制御やキャッシュを行う装置は一般に何と呼ばれるか。

- ア．リバースプロキシ
- イ．DHCPリレー
- ウ．NTPピア
- エ．フォワードプロキシ

正答：エ

4肢解説

ア：リバースプロキシは主にサーバ側の前段に置かれ、外部クライアントからの要求をバックエンドへ中継する。

イ：DHCPメッセージを中継する機能である。

ウ：時刻同期の相手であり、Webアクセス代理ではない。

エ：正しい。フォワードプロキシはクライアント側の代理として外部サーバへアクセスする。

総合解説：プロキシは配置位置と代理対象で役割が異なる。フォワードプロキシはクライアント代理、リバースプロキシはサーバ側の代理として使われる。

問139 HTTPSクライアントがサーバ証明書を受信した。中間者攻撃を防ぐ観点から、証明書チェーンの検証に加えて重要な確認はどれか。
ア．接続しようとしているサービスのDNS名と証明書に示された識別子が適切に一致すること
イ．証明書のファイルサイズが常に1KB未満であること
ウ．サーバのEthernet MACアドレスが証明書に必ず記載されていること
エ．HTTPレスポンスが必ず200であること

正答：ア

4肢解説

ア：正しい。信頼できるCAの署名だけでなく、接続対象のサービス名と証明書の識別子を照合する必要がある。
イ：ファイルサイズはサービス識別の正当性を保証しない。
ウ：通常のWeb PKIのサーバ名検証はMACアドレス一致を前提としない。
エ：HTTPステータスコードは証明書の名前検証を代替しない。
総合解説：TLSのサーバ認証では、信頼チェーン、有効性、サービス識別子の一致などを適切に検証する必要がある。

問140 クライアントがフォワードプロキシ経由でHTTPSサーバへ接続し、プロキシに宛先へのTCPトンネル確立を依頼したい。HTTPで代表的に利用されるメソッドはどれか。
ア．TRACE
イ．CONNECT
ウ．DELETE
エ．OPTIONS

正答：イ

4肢解説

ア：TRACEは要求経路の診断用途に関係し、一般的なHTTPSトンネル確立メソッドではない。
イ：正しい。CONNECTは指定した宛先へのトンネル確立を要求するために利用され、HTTPSのプロキシ通過で代表的に使われる。
ウ：リソース削除を要求するメソッドである。
エ：対象リソースやサーバの通信オプションを問い合わせるメソッドで、トンネル確立そのものではない。
総合解説：CONNECT成功後、プロキシは通常バイト列を中継し、TLSハンドシェイクはクライアントと宛先サーバ間で行われる構成がある。

問141 SMTPの主な用途として最も適切なものはどれか。

ア．IPアドレスを自動配布する

イ．時刻を同期する

ウ．電子メールを送信・中継する

エ．Ethernetのループを防止する

正答：ウ

4肢解説

ア：これはDHCPの役割である。

イ：これはNTPの役割である。

ウ：正しい。SMTPはメールクライアントからサーバへの送信やメールサーバ間の配送・中継に用いられる。

エ：これはSTPなどの役割である。

総合解説：メールシステムではSMTPが送信・配送に使われ、利用者がメールボックスを参照する際にはIMAPやPOP3などが使われる。

問142 FTPの特徴として適切なものはどれか。

ア．制御情報もデータも必ず単一UDPデータグラムだけで送る

イ．DNSのゾーン転送を利用してファイルを送る

ウ．Ethernetフレームだけでアプリケーション認証を行う

エ．制御用の接続とファイル転送等のデータ用接続を分けて扱う

正答：エ

4肢解説

ア：FTPはTCPを利用し、制御接続とデータ接続を扱う。

イ：FTPはDNSゾーン転送をデータ転送機構として使わない。

ウ：FTPのアプリケーション動作とは異なる。

エ：正しい。FTPはコマンドを交換する制御接続と、実データを転送するデータ接続を分離する。

総合解説：FTPは歴史的に制御とデータで別接続を利用するため、NATやファイアウォール設計でその特性を考慮する必要がある。

問143 IP電話やビデオ会議の開始・変更・終了を制御するシグナリングプロトコルとして、SIPが担当する機能はどれか。

ア．音声・映像などのセッションを確立、変更、終了するためのシグナリング

イ．音声サンプルそのものを必ず転送する

ウ．IPルータ間で最短経路を計算する

エ．DNSゾーンファイルを同期する

正答：ア

4肢解説

ア：正しい。SIPはマルチメディアセッションの開始・変更・終了などを制御するシグナリングプロトコルである。

イ：実際のメディア転送にはRTPなどが使われることが多く、SIPの主目的はシグナリングである。

ウ：これはOSPFなどのルーティングプロトコルの役割である。

エ：DNSゾーン転送とは異なる。

総合解説：SIPは呼制御や登録などを担当し、実際の音声・映像メディアはRTP等の別プロトコルで転送する構成が一般的である。

問144 SMTPセッションで、送信者を指定した後に受信者を指定し、続いてメール内容の送信へ移る代表的なコマンド順序として適切なものはどれか。

ア．DATA → MAIL FROM → RCPT TO

イ．MAIL FROM → RCPT TO → DATA

ウ．RCPT TO → QUIT → MAIL FROM

エ．GET → POST → CONNECT

正答：イ

4肢解説

ア：エンベロープ情報を指定する前にDATAへ進む順序ではない。

イ：正しい。SMTPではMAIL FROMでエンベロープ送信者、RCPT TOで受信者を指定し、DATAでメッセージ内容送信へ移る。

ウ：QUITはセッション終了コマンドであり、この位置では不適切である。

エ：これらはHTTPメソッドでありSMTPコマンドではない。

総合解説：SMTPではメッセージヘッダ上のFrom/Toと、配送に用いるSMTPエンベロープのMAIL FROM/RCPT TOを区別することが重要である。

問145 送信側メールサーバがuser@example.jp宛てメールを配送するとき、example.jpの受信メールサーバ候補をDNSから調べる際に主に参照するレコードはどれか。

ア．PTRレコードだけ
イ．TXTレコードだけ
ウ．MXレコード
エ．SOAレコードだけ

正答：ウ

4肢解説

ア：PTRは主に逆引きに用いられ、受信メールサーバ指定の中心ではない。

イ：TXTは様々な情報格納に使えるが、SMTPの受信サーバ選択を直接表す標準レコードはMXである。

ウ：正しい。SMTP配送では宛先ドメインのMXレコードを参照してメール交換先を決定する。

エ：SOAはゾーン管理情報を示し、メール交換先の直接指定ではない。

総合解説：MXレコードには優先度があり、送信側は利用可能なメール交換先を選択して配送を試みる。

問146 複数端末から同じメールボックスを利用し、サーバ上のフォルダや既読状態などを同期しながら管理したい。一般に適するプロトコルはどれか。

ア．POP3だけ
イ．ARP
ウ．OSPF
エ．IMAP

正答：エ

4肢解説

ア：POP3は主にメールを取得する比較的単純なモデルで、サーバ上の高度なメールボックス管理はIMAPの方が適する。

イ：アドレス解決用プロトコルでありメールボックス管理には使わない。

ウ：ルーティングプロトコルでありメール参照には使わない。

エ：正しい。IMAPはサーバ上のメールボックスやフォルダ、メッセージ状態を操作する機能を持ち、複数端末利用に適している。

総合解説：SMTPはメール送信・配送、IMAPやPOP3は利用者によるメール取得・管理という役割分担になる。

問147 FTPでクライアントがNATやファイアウォール内にあり、サーバからクライアントへの新規データ接続を受けにくい。一般にパッシブモードが扱いやすい理由はどれか。
ア．データ接続もクライアント側からサーバ側へ開始できるため
イ．FTPがUDPへ自動変換されるため
ウ．制御接続が不要になるため
エ．サーバのIPアドレスがDNSから削除されるため

正答：ア
4肢解説
ア：正しい。パッシブモードではサーバが待受け情報を提示し、クライアントがデータ接続を開始する。
イ：パッシブモードでもFTPはTCPを利用する。
ウ：制御接続は引き続き利用する。
エ：パッシブモードの理由とは無関係である。
総合解説：FTPアクティブ/パッシブの違いはデータ接続をどちら側から開始するかに関係し、NAT・FW通過性に影響する。

問148 SIPで新しいセッションの確立を開始するために用いられる代表的なメソッドはどれか。
ア．BYE
イ．INVITE
ウ．REGISTER
エ．ACKだけ
正答：イ
4肢解説
ア：BYEは確立済みセッションの終了に用いられる。
イ：正しい。INVITEはSIPセッション確立を開始する代表的な要求である。
ウ：REGISTERはユーザエージェントの現在位置を登録するために用いられる。
エ：ACKはINVITEに対する最終応答の確認などに用いられ、通常セッション開始要求そのものではない。
総合解説：SIPではINVITE、ACK、BYE、REGISTER、OPTIONSなどのメソッドを目的に応じて使い分ける。

問149 IP電話で呼の開始・終了操作は正常に行えるが、通話中に双方の音声だけが全く届かない。最初に重点確認すべき通信として最も適切なものはどれか。
ア．SIPのINVITEが一度も届いていないことだけ
イ．DNSのMXレコードだけ
ウ．RTPなどのメディア通信の経路・ポート・NAT/ファイアウォール状態
エ．FTPのパッシブモード設定だけ

正答：ウ

4肢解説

ア：呼の開始・終了が正常なら、SIPが全く届いていない可能性は低い。
イ：メール配送用レコードであり音声メディア障害の主因ではない。
ウ：正しい。SIPシグナリングが成立していても、RTPメディア経路が別途遮断されれば呼制御だけ成功して音声が届かないことがある。
エ：FTP設定はVoIPメディア転送と直接関係しない。
総合解説：VoIPではシグナリングとメディアが別フローになるため、障害時はSIPとRTPを分離して確認することが重要である。

問150 RTPパケットのシーケンス番号とタイムスタンプを利用する主な目的として最も適切なものはどれか。

ア．IPアドレスを自動配布する
イ．TLS証明書の署名を検証する
ウ．OSPFの最短経路を計算する
エ．パケット損失や順序を把握し、メディア再生タイミングの復元に役立てる

正答：エ

4肢解説

ア：これはDHCPの役割である。
イ：RTPのシーケンス番号・タイムスタンプの用途ではない。
ウ：ルーティング計算とは無関係である。
エ：正しい。シーケンス番号は損失・順序検出、タイムスタンプはサンプリング時刻に基づく再生タイミング等に利用される。
総合解説：RTPはリアルタイムメディア向けにシーケンス番号やタイムスタンプを提供するが、配送保証そのものは提供しない。