問1 『Web会議を快適に利用できるネットワークにしたい』という業務要求を、設計・受入れで検証しやすい要件へ具体化する方法として最も適切なものはどれか。
ア．同時会議数、必要帯域、許容遅延・ジッタ・損失率などを数値で定義する
イ．『高速であること』だけを要件書に記載する
ウ．利用者の感想だけで性能を決める
エ．使用するルータの製品名だけを先に固定する
正答：ア
4肢解説
ア：正しい。抽象的な業務要求を、帯域、遅延、ジッタ、損失率、同時利用数など測定可能な指標へ落とし込むと、設計と受入れの基準にできる。
イ：評価基準が曖昧で、設計の妥当性や受入れ結果を客観的に判定しにくい。
ウ：利用者評価は参考になるが、ネットワーク要件としては測定可能な指標も必要である。
エ：製品指定は実装条件であり、まず業務要求から必要性能・品質を定義すべきである。
総合解説：要件定義では、業務上の期待を可用性、性能、セキュリティ、拡張性、運用性などの非機能要件に変換し、測定可能な受入れ基準へ具体化する。

問2 ネットワークサービスにおけるSLAの説明として最も適切なものはどれか。
ア．ルータ同士が経路情報を交換するためのプロトコルである
イ．サービス提供者と利用者の間で、可用性や障害対応時間などのサービス水準を合意する
ウ．IPアドレスを自動配布する仕組みである
エ．暗号鍵の長さだけを規定する技術標準である
正答：イ
4肢解説
ア：SLAは契約・サービス管理上の合意であり、ルーティングプロトコルではない。
イ：正しい。SLAは、提供するサービスの品質水準や測定方法、責任範囲などを合意するために用いられる。
ウ：IPアドレス配布はDHCPなどの役割である。
エ：SLAは暗号アルゴリズム仕様ではなく、サービス水準の合意である。
総合解説：SLAでは可用性、応答時間、復旧時間、サポート時間帯、測定方法、除外条件などを具体的に定めることが重要である。

問3 災害対策要件で『業務停止後4時間以内にサービスを再開する』と定めた。この4時間は主にどの指標に該当するか。
ア．RPO
イ．MTBF
ウ．RTO
エ．TTL
正答：ウ
4肢解説
ア：RPOはどの時点までのデータを復旧する必要があるかという目標復旧時点を表す。
イ：MTBFは平均故障間隔であり、災害後の復旧目標時間ではない。
ウ：正しい。RTOは障害・災害発生後、どの程度の時間で業務やサービスを復旧させるかという目標時間である。
エ：TTLはIPパケットやDNSキャッシュなどの寿命に関する値である。
総合解説：BCP・DR設計ではRTOとRPOを区別し、必要な冗長化、バックアップ、回線切替え、復旧手順を決める。

問4 24時間365日提供するサービスについて、年間可用性99.9%を要求する。1年を365日とし、計画停止を含めず単純計算した場合、許容される年間停止時間に最も近いものはどれか。
ア．約52分
イ．約87時間36分
ウ．約36時間30分
エ．約8時間46分
正答：エ
4肢解説
ア：これは概ね99.99%可用性の年間停止時間に近い。
イ：これは1%停止に相当し、可用性99%程度である。
ウ：99.9%の単純計算値ではない。
エ：正しい。年間時間は8,760時間で、停止可能割合0.1%なので8,760×0.001=8.76時間、約8時間46分である。
総合解説：可用性要求は『9の数』だけでなく、測定対象、計画停止の扱い、測定単位、サービス時間帯を明確にする必要がある。

問5 既設データセンターのラック電源容量を増設できず、新ネットワーク機器の追加消費電力を2kW以内に抑える必要がある。この条件の位置付けとして最も適切なものはどれか。
ア．設計上の制約条件
イ．業務機能要件だけに分類する
ウ．ルーティングプロトコルのメトリック
エ．SLAの可用性指標そのもの
正答：ア
4肢解説
ア：正しい。電源容量のように設計案が従う必要のある外部条件は制約条件として整理する。
イ：電源上限は利用者が行う業務機能ではなく、実装・設備上の制約である。
ウ：経路選択値ではない。
エ：可用性とは別の設備制約である。
総合解説：要件定義では、業務要求だけでなく予算、既存設備、法令、移行期限、電源・スペース、利用可能回線などの制約を明示する。

問6 月間可用性99.95%をSLAに定める。後の解釈差を減らすために、併せて定義すべき事項として最も適切なものはどれか。
ア．担当者の氏名だけ
イ．停止の開始・終了判定、測定点、計画停止の扱い、集計期間
ウ．機器の筐体色
エ．全端末の壁紙設定
正答：イ
4肢解説
ア：担当者情報だけでは可用性の算定条件を定義できない。
イ：正しい。数値だけでは可用性の算定方法が一意にならないため、測定条件や除外条件を合意する必要がある。
ウ：サービス水準の測定とは無関係である。
エ：SLA可用性の測定条件とは関係しない。
総合解説：SLAは指標値に加えて、対象範囲、測定点、測定方法、報告方法、免責・除外条件などを定義して初めて実務で機能する。

問7 業務システムでRPOを5分以内とする必要がある。毎日深夜に1回だけバックアップする方式について、最も適切な評価はどれか。
ア．1日1回でも必ずRPO 5分を満たす
イ．RPOは復旧所要時間なのでバックアップ頻度は無関係である
ウ．通常はRPO 5分を満たせないため、より高頻度な複製やログ転送などを検討する
エ．RPOはネットワーク帯域の上限を表す
正答：ウ
4肢解説
ア：バックアップ間隔がRPOより大幅に長い。
イ：復旧所要時間はRTOであり、RPOは復旧可能なデータ時点に関係する。
ウ：正しい。1日1回のバックアップでは最大約24時間分のデータを失う可能性があり、5分以内のRPOには不十分である。
エ：帯域指標ではない。
総合解説：厳しいRPOには同期・非同期レプリケーション、継続的ログ転送、短周期スナップショットなどが候補になるが、回線・コスト・整合性も評価する。

問8 店舗ネットワークは営業時間8:00〜22:00の可用性を最重要とし、深夜2:00〜4:00には計画保守を認める。SLA設計として最も適切なものはどれか。
ア．24時間全て同一条件とだけ記載し、計画保守の扱いは決めない
イ．営業時間の定義を削除する
ウ．障害時間を利用者ごとに任意に数える
エ．サービス時間帯と計画保守時間を明確に分け、可用性算定への扱いを合意する
正答：エ
4肢解説
ア：実際の運用とSLA判定の間で解釈差が生じる。
イ：業務要件を反映できなくなる。
ウ：客観的なSLA評価ができない。
エ：正しい。業務影響の大きい時間帯と保守可能時間を区別し、SLA算定条件を明文化するべきである。
総合解説：SLAは業務の重要時間帯に合わせる。サービス提供時間、計画保守、障害判定、部分障害の扱いまで定義すると実効性が高い。

問9 海外拠点ネットワークで『通信経路は必ず二重化』『運用要員は増員しない』『月額回線費は現状以下』という要求が同時に提示された。設計者の対応として最も適切なものはどれか。
ア．各要求の優先度と根拠を確認し、実現性・コスト・運用負荷のトレードオフを示して合意形成する
イ．全要求を検討せず満たせると約束する
ウ．最も安価な案だけを提示して他の要求を無視する
エ．技術担当者だけで業務優先度を決める
正答：ア
4肢解説
ア：正しい。相互に競合し得る要件は、優先順位や受容可能なリスクを明確にし、代替案を比較して合意する必要がある。
イ：実現性評価を欠き、後工程で品質・コスト問題を招く。
ウ：冗長性や運用性などの重要要求を満たさない可能性がある。
エ：業務影響や経営判断を含むため、関係者との合意が必要である。
総合解説：要件定義は要求を列挙するだけでなく、競合条件、優先順位、制約、受容リスクを整理し、実現可能な設計基準へ落とし込む工程である。

問10 回線は二重化しているが、両回線が同一キャリアの同一収容局・同一管路に依存している。大規模断線時の可用性要求を高めたい場合の改善として最も適切なものはどれか。
ア．同じ物理経路の回線をさらに1本追加するだけ
イ．キャリア、収容局、物理経路などの共通障害点を減らすよう冗長経路を分離する
ウ．SLA値だけを99.999%へ書き換える
エ．端末のDNSキャッシュ時間だけを延ばす
正答：イ
4肢解説
ア：共通障害点が残るため、大規模断線への耐性向上は限定的である。
イ：正しい。論理的に2回線あっても物理経路や事業者設備を共有すれば共通原因障害で同時断となり得る。
ウ：実装の冗長性を改善せず数値だけ変更しても可用性は向上しない。
エ：物理回線断への対策にはならない。
総合解説：高可用性設計では機器台数だけでなく、電源、回線、収容局、経路、建物、運用手順などの共通障害点を洗い出すことが重要である。

問11 ルータのWANインタフェースについて、一定期間の送受信バイト数から平均帯域利用率を算出したい。代表的に利用できる情報はどれか。
ア．DNSのMXレコード
イ．TLSサーバ証明書
ウ．SNMPで取得するインタフェースのオクテットカウンタ
エ．ARPの静的設定数だけ
正答：ウ
4肢解説
ア：メール配送先を示す情報であり、インタフェース利用率は分からない。
イ：通信相手の認証などに使うもので、リンク利用量のカウンタではない。
ウ：正しい。インタフェースの送受信オクテットカウンタを一定間隔で取得し、差分と時間から平均ビットレートを算出できる。
エ：インタフェースの転送量を表さない。
総合解説：現状分析ではSNMP等でインタフェース利用率、エラー、廃棄、CPU、メモリなどを時系列で取得し、ピーク・傾向を確認する。

問12 『どの送信元・宛先、どのプロトコルの通信がWAN帯域を多く消費しているか』を把握するために有効な情報はどれか。
ア．NTPのstratumだけ
イ．VLAN名だけ
ウ．DHCPリース期間だけ
エ．IPFIXなどのフローレコード
正答：エ
4肢解説
ア：時刻同期階層であり、通信量の内訳は分からない。
イ：論理セグメントの名称だけでは通信相手やバイト量を把握できない。
ウ：アドレス貸出期間であり、トラフィック量の内訳ではない。
エ：正しい。フローレコードには送受信アドレス、ポート、プロトコル、バイト数などを含められ、通信内訳の把握に適している。
総合解説：SNMPはインタフェース全体の量を見るのに有効で、IPFIX/NetFlow系は誰が何とどれだけ通信しているかを分析するのに有効である。

問13 ネットワーク性能の現状分析でベースラインを取得する主な目的はどれか。
ア．通常時の利用率・遅延・損失などの基準値を把握し、将来の異常や増加傾向と比較できるようにする
イ．全ての通信を永久に暗号化解除して保存する
ウ．ルータの設定を毎日初期化する
エ．DNS名をIPアドレスへ固定変換する
正答：ア
4肢解説
ア：正しい。平常時の基準を持つことで、異常検出や容量計画、設計変更前後の比較がしやすくなる。
イ：ベースライン取得の目的ではなく、プライバシー・セキュリティ上も問題がある。
ウ：基準値取得とは無関係である。
エ：名前解決設定の変更が主目的ではない。
総合解説：ベースラインは曜日・時間帯・月末処理など業務周期を含めて取得し、単発の測定だけで判断しないことが重要である。

問14 WAN利用率は通常30%だが、毎日数分だけ100%近くになる。平均値だけでは混雑を見落とす可能性があるため、追加で確認する指標として有効なものはどれか。
ア．機器の製造年月だけ
イ．95パーセンタイル値やピーク時間帯の分布
ウ．DNSのSOAシリアル番号だけ
エ．端末の画面解像度の平均
正答：イ
4肢解説
ア：トラフィック混雑の定量評価にはならない。
イ：正しい。平均値だけでなく高い側の分布やパーセンタイルを見ると、短時間の混雑や継続的なピークを把握しやすい。
ウ：帯域利用状況とは無関係である。
エ：ネットワーク混雑の指標ではない。
総合解説：容量分析では平均値、最大値、パーセンタイル、継続時間、時間帯別傾向を組み合わせて判断する。

問15 あるインタフェースで帯域利用率は40%程度だが、入力エラーが継続的に増加している。最も適切な初動はどれか。
ア．帯域利用率が低いので問題なしと判断する
イ．DNSキャッシュを削除するだけ
ウ．物理媒体、光レベル、ケーブル、NIC/ポートなどの物理層・リンク層異常を確認する
エ．BGPのAS番号を変更する
正答：ウ
4肢解説
ア：エラーカウンタ増加は品質問題の兆候であり、利用率だけで正常とは言えない。
イ：物理受信エラーの原因解消にはならない。
ウ：正しい。帯域余裕があるのに入力エラーが増える場合、物理媒体やポート品質などを確認すべきである。
エ：入力エラーの一次原因とは考えにくい。
総合解説：トラフィック分析では利用率だけでなくCRC/FCS系エラー、discard、再送、損失など品質指標も併せて確認する。

問16 出力インタフェースで物理エラーはないが、出力キューのdiscardがピーク時間帯だけ増加する。最も考えやすい原因はどれか。
ア．必ずDNS障害である
イ．必ず光ファイバ断線である
ウ．DHCPのリース時間が長すぎる
エ．瞬間的または継続的に送信能力を超えるトラフィックが入り、キューがあふれている
正答：エ
4肢解説
ア：キュー廃棄の直接原因とは限らない。
イ：物理断なら通常はリンクダウン等の別の兆候が出る。
ウ：出力キュー廃棄と直接関係しない。
エ：正しい。物理エラーがなく出力キュー廃棄が増える場合、輻輳やバーストによるバッファ枯渇を疑う。
総合解説：平均利用率が低くてもマイクロバーストでキューがあふれることがあるため、短い粒度の監視やキュー統計が重要である。

問17 拠点間回線で帯域利用率は50%未満だが、業務アプリの応答が遅い。ping等の測定でRTTとパケット損失率を確認する理由として最も適切なものはどれか。
ア．帯域使用率以外の遅延・損失要因を切り分けるため
イ．RTTを測れば必ずアプリケーション処理時間も完全に分かる
ウ．pingだけで全てのQoS設定を自動修正できる
エ．損失率はTCP性能と無関係だから
正答：ア
4肢解説
ア：正しい。アプリ性能は帯域だけでなくRTT、損失、再送、サーバ処理時間などにも影響される。
イ：RTTはネットワーク往復時間の一部指標であり、サーバ処理時間を完全には分離できない。
ウ：測定は診断情報であり、自動的に全設定が修正されるわけではない。
エ：パケット損失はTCP再送や輻輳制御を通じて性能へ大きく影響し得る。
総合解説：現状分析では帯域、RTT、ジッタ、損失、再送、アプリ応答時間を層別に測り、ボトルネックを切り分ける。

問18 片方向だけに設置したパケットキャプチャ装置でTCP通信を分析したところ、ACKがほとんど観測できない。経路設計上まず考慮すべきことはどれか。
ア．TCPではACKを使用しないため正常である
イ．往路と復路が異なる非対称経路になっていないか確認する
ウ．全てのTCP通信は必ず同一物理経路を双方向に通る
エ．DNS TTLが短いとACKが消える
正答：イ
4肢解説
ア：TCPはACKを利用して信頼性制御を行う。
イ：正しい。非対称ルーティングでは、片方向の観測点だけでは通信の全体像を取得できない場合がある。
ウ：IPルーティングでは往路と復路が異なることがある。
エ：直接の関係はない。
総合解説：パケット分析では観測点の位置と経路対称性を確認し、必要に応じて複数地点でキャプチャする。

問19 5分平均のSNMP利用率は30%なのに、スイッチの出力キューdropが断続的に発生し、短時間だけアプリの遅延が急増する。最も適切な分析方法はどれか。
ア．5分平均が30%なので輻輳は絶対にないと判断する
イ．DNSサーバを増設するだけ
ウ．より短い時間粒度のテレメトリやキュー統計を確認し、瞬間的なマイクロバーストを調べる
エ．全端末のIPアドレスを変更する
正答：ウ
4肢解説
ア：短時間のバーストは平均値に現れにくい。
イ：症状の根拠からは出力キュー輻輳の確認が先である。
ウ：正しい。長い平均化間隔では短時間の帯域飽和が平均化され、見えなくなることがある。
エ：マイクロバースト分析にはならない。
総合解説：高速ネットワークではミリ秒〜秒単位のバーストがキューをあふれさせる場合があり、監視粒度を要件に合わせる必要がある。

問20 本社LAN内ではサーバへのRTTが2ms、WAN出口直後では10ms、拠点側では80msで、拠点側アクセス回線の利用率がピーク時95%に達している。最初に改善候補として優先すべき箇所はどれか。
ア．本社LAN全体を無条件に全面更改する
イ．DNSドメイン名を変更する
ウ．サーバの時刻同期方式だけを変更する
エ．拠点側アクセス回線とそのキュー・帯域設計
正答：エ
4肢解説
ア：本社LAN内のRTTは小さく、提示データから優先度は低い。
イ：遅延増大区間と直接関係しない。
ウ：提示されたネットワーク遅延の主因とは考えにくい。
エ：正しい。RTT増大と高利用率が拠点側アクセス区間で顕著なので、そこがボトルネック候補として強い。
総合解説：現状分析では複数地点の利用率・RTT・損失・キュー統計を相関させ、どの区間で品質が悪化しているかを特定する。

問21 回線容量を現在のピークトラフィックと完全に同じ値で設計せず、一定の余裕を持たせる主な理由はどれか。
ア．トラフィック変動、成長、障害時迂回などでピークが増える可能性に備えるため
イ．利用率が高いほど必ず遅延がゼロになるため
ウ．回線容量を余らせるとIPアドレス数が増えるため
エ．DNS応答を暗号化するため
正答：ア
4肢解説
ア：正しい。容量に余裕を持たせることで、短期変動や成長、冗長経路切替え時の負荷増加に対応しやすい。
イ：高利用率では待ち行列や廃棄が増え、遅延が悪化することがある。
ウ：回線帯域とアドレス数は別の要件である。
エ：容量余裕とは無関係である。
総合解説：容量設計では通常時だけでなく成長率、バースト、障害時の経路集約、将来サービス追加を考慮する。

問22 トラフィック増加に対し、同一役割の装置や処理ノードを追加して負荷を分散する拡張方式はどれか。
ア．スケールアップ
イ．スケールアウト
ウ．フェイルクローズ
エ．フラグメンテーション
正答：イ
4肢解説
ア：スケールアップは単一装置のCPU・メモリ・インタフェース能力などを強化する方式である。
イ：正しい。スケールアウトはノード数を増やして処理能力や容量を拡張する方式である。
ウ：障害時のアクセス制御動作に関する考え方で、容量拡張方式ではない。
エ：パケット分割の仕組みであり、システム容量拡張方式ではない。
総合解説：拡張性要件では、どの単位で増設できるか、増設時に停止が必要か、制御プレーンやライセンス上限がないかも確認する。

問23 リアルタイム音声の品質要件として、単純な平均帯域だけでなく特に確認すべき指標の組合せはどれか。
ア．ディスク容量、CPU型番、ラック色
イ．DNSゾーン数、MX優先度、SOAシリアル
ウ．遅延、ジッタ、パケット損失率
エ．MACアドレス文字数、VLAN名長、SSID文字数
正答：ウ
4肢解説
ア：音声ネットワーク品質を直接表す指標ではない。
イ：メール・名前解決管理の情報であり、音声品質指標ではない。
ウ：正しい。音声は到着時刻の変動や損失に敏感なので、帯域だけでは品質を十分に評価できない。
エ：性能指標ではない。
総合解説：アプリケーション特性に応じて、スループット、遅延、ジッタ、損失、同時接続数、ppsなど適切な性能指標を選ぶ。

問24 1拠点で1セッション当たり上下各2Mbit/sを必要とするWeb会議を最大40セッション同時利用する。上り回線について、プロトコルオーバーヘッドや余裕を考慮しない最低必要帯域はどれか。
ア．20Mbit/s（同時利用数を十分反映しない）
イ．40Mbit/s（2Mbit/s×40の半分として計算）
ウ．160Mbit/s（上下2方向を上り帯域へ合算）
エ．80Mbit/s（上り2Mbit/s×40セッションで計算）
正答：エ
4肢解説
ア：1セッション当たりや同時数の扱いが不足している。
イ：2Mbit/s×40の半分であり計算が合わない。
ウ：上下方向を合算して上りだけに必要とした値であり、設問は上り回線を問うている。
エ：正しい。上りは2Mbit/s×40セッション=80Mbit/s必要となる。
総合解説：実設計ではさらにIP/UDP/RTP等のオーバーヘッド、制御通信、バースト、他アプリ、余裕率を考慮する。

問25 2本のWAN回線に通常時それぞれ300Mbit/sずつトラフィックを分散している。片系障害時にも全トラフィックを残存回線へ収容したい。最低限必要な各回線容量はどれか。
ア．600Mbit/s（通常時合計300+300を1本で収容）
イ．300Mbit/s（通常時の1回線分だけを収容）
ウ．150Mbit/s（通常時1回線分にも不足）
エ．900Mbit/s（最低限値に追加余裕を見込む）
正答：ア
4肢解説
ア：正しい。通常時の合計トラフィック600Mbit/sを1本で収容できる必要がある。
イ：片系障害時にはもう一方の300Mbit/sも流入するため不足する。
ウ：通常時の1回線負荷にも不足する。
エ：余裕を見込む場合はあり得るが、設問の最低限値では600Mbit/sである。
総合解説：冗長設計では通常時だけでなくN-1障害時の集中負荷を基準に容量を確認する。

問26 現在のピークトラフィックが500Mbit/sで、年20%ずつ増えると仮定する。2年後のピーク値に最も近いものはどれか。
ア．600Mbit/s
イ．720Mbit/s
ウ．700Mbit/s
エ．1,000Mbit/s
正答：イ
4肢解説
ア：1年分の20%増加しか反映していない。
イ：正しい。複利的に500×1.2×1.2=720Mbit/sとなる。
ウ：毎年100Mbit/sを単純加算した値で、20%複利ではない。
エ：2年間で倍増する前提にはなっていない。
総合解説：容量計画では線形成長か複利成長か、業務イベント、拠点増加、サービス導入予定を踏まえて予測する。

問27 同じ1Gbit/sのトラフィックでも、64バイト程度の小さいパケットが大量に流れると装置負荷が高くなる場合がある。設計時に追加確認すべき性能指標はどれか。
ア．DNSのTTL上限
イ．SSID数だけ
ウ．packet per second（pps）処理能力
エ．ラックの高さだけ
正答：ウ
4肢解説
ア：パケット転送処理能力とは異なる。
イ：有線ルータの小パケット転送能力を表さない。
ウ：正しい。小さいパケットでは同じビットレートでもパケット数が増えるため、装置のpps性能がボトルネックになることがある。
エ：装置性能指標ではない。
総合解説：ネットワーク機器はbpsだけでなくpps、セッション数、ルート数、ACLエントリ数、暗号化性能など複数の上限を確認する。

問28 アクセススイッチ48ポートが各1Gbit/sで接続され、上位リンクが合計10Gbit/sである。この構成を評価する際に最も重要な考え方はどれか。
ア．48ポートなので上位リンクも必ず48Gbit/sでなければ設計違反である
イ．上位10Gbit/sなら端末数に関係なく絶対に輻輳しない
ウ．VLAN数だけ見れば十分である
エ．全端末が同時に最大送信する前提では48Gbit/sとなるため、業務トラフィック特性と許容するオーバーサブスクリプションを確認する
正答：エ
4肢解説
ア：利用特性によってオーバーサブスクリプションを許容する設計は一般的にあり得る。
イ：同時トラフィックが10Gbit/sを超えれば輻輳し得る。
ウ：帯域容量の評価にはならない。
エ：正しい。アクセス帯域総和と上位帯域の比率だけでなく、同時利用率やピーク特性を踏まえて許容性を判断する。
総合解説：アクセス層では端末数、同時利用率、トラフィック方向、バックアップなどの集中イベントを考慮して上位リンク容量を決める。

問29 回線利用率が平常時70%からピーク時98%へ上昇すると、パケット損失がなくても遅延が大きく悪化することがある。設計上の説明として最も適切なものはどれか。
ア．高利用率では到着トラフィックの揺らぎにより待ち行列が伸びやすく、キューイング遅延が急増するため
イ．利用率が100%に近づくほど必ず伝搬遅延がゼロになるため
ウ．IPアドレス数が自動的に減るため
エ．DNS応答が必ずTCPからUDPへ変わるため
正答：ア
4肢解説
ア：正しい。回線が飽和に近づくほどトラフィック変動を吸収する余裕が小さくなり、待ち行列時間が増えやすい。
イ：伝搬遅延は距離や媒体に依存し、高利用率でゼロにはならない。
ウ：アドレス数とキューイング遅延は別問題である。
エ：高利用率による遅延の一般原理ではない。
総合解説：性能要件では平均利用率だけでなく、ピーク時に遅延・ジッタが許容範囲に収まるよう十分なヘッドルームを確保する。

問30 ファイアウォール更改で、帯域性能は10Gbit/sと十分だが、3年後には同時セッション数が現行の4倍になる見込みである。設計判断として最も適切なものはどれか。
ア．10Gbit/sなら他の性能上限は確認不要である
イ．帯域だけでなく最大同時セッション数、新規セッション毎秒、ルール数などの上限も将来予測と照合する
ウ．端末の画面解像度を下げれば必ず解決する
エ．ルール数は性能や拡張性と無関係である
正答：イ
4肢解説
ア：セッション数やCPSなど別の上限がボトルネックになり得る。
イ：正しい。装置性能には複数の独立した上限があり、帯域だけ満たしても別資源が先に枯渇する可能性がある。
ウ：セッション上限の設計とは直接関係しない。
エ：製品によってはルール数や処理条件が性能・容量へ影響する。
総合解説：拡張性要件は帯域、pps、セッション、VPN数、ルート数、MAC/VLAN数、AP収容数、ログ量など対象装置に応じた指標で確認する。

問31 企業LANのアクセス層・ディストリビューション層・コア層の役割分担として最も適切なものはどれか。
ア．全ての層で同じ端末収容だけを行う
イ．コア層に全利用者端末を直接接続することだけを目的とする
ウ．アクセス層で端末を収容し、上位層で経路集約やポリシー適用、コア層で高速・高可用な中継を行う
エ．アクセス層だけで外部BGPを必ず運用する
正答：ウ
4肢解説
ア：階層化の利点である役割分離が失われる。
イ：通常の階層設計の役割分担とは異なる。
ウ：正しい。階層化により役割を分離し、障害範囲・拡張性・運用性を管理しやすくする。
エ：端末収容層の一般的な役割ではない。
総合解説：階層型設計は大規模LANで障害ドメイン、経路集約、ポリシー境界を明確化し、変更影響を抑えるのに有効である。

問32 同一VLANを多数のフロアへ広域に延伸した場合に増えやすい設計リスクはどれか。
ア．IPルーティングが必ず不要になり全障害が減る
イ．MACアドレスが不要になる
ウ．全ての通信が暗号化される
エ．L2障害やブロードキャストの影響範囲が広がる
正答：エ
4肢解説
ア：L2延伸は別の障害リスクを増やす場合がある。
イ：EthernetではL2転送にMACアドレスを利用する。
ウ：VLAN延伸自体に暗号化機能はない。
エ：正しい。同一L2セグメントを広く延伸すると、ループやブロードキャストストームなどの影響範囲が大きくなる。
総合解説：設計では必要以上にL2ドメインを広げず、L3境界を適切に設けて障害・ブロードキャスト範囲を制御する。

問33 端末のデフォルトゲートウェイ障害に備え、複数ルータで仮想IPアドレスを共有する代表的な仕組みはどれか。
ア．VRRP
イ．ARPだけ
ウ．DNSSEC
エ．SMTP
正答：ア
4肢解説
ア：正しい。VRRPは複数ルータで仮想ルータを構成し、デフォルトゲートウェイの冗長化に利用できる。
イ：ARPはIPアドレスとMACアドレスの解決に使うが、ゲートウェイ冗長プロトコルではない。
ウ：DNSデータの真正性検証に関する仕組みである。
エ：メール配送プロトコルである。
総合解説：デフォルトゲートウェイ冗長化では、仮想IP、優先度、障害検知、切替え時間、上位経路との整合を設計する。

問34 大規模キャンパスLANで、アクセススイッチから上位をL3接続とし、VLANをアクセススイッチ間で延伸しない設計の利点として最も適切なものはどれか。
ア．全端末が同一ブロードキャストドメインになる
イ．L2ループやSTP障害の影響範囲を狭くし、経路制御で冗長化しやすくなる
ウ．ルーティングテーブルが完全に不要になる
エ．VLAN IDを無制限に増やせることだけが利点である
正答：イ
4肢解説
ア：むしろL2ドメインを分割する設計である。
イ：正しい。L3境界をアクセス側へ寄せるとL2ドメインを局所化でき、ECMP等を利用しやすい。
ウ：L3接続なので経路制御が必要である。
エ：主な利点は障害ドメイン縮小や経路冗長性である。
総合解説：L2/L3境界の位置は、端末移動要件、冗長化方式、障害範囲、運用スキルを考慮して決める。

問35 データセンターで東西トラフィックが多く、サーバ間のホップ数を揃えながら水平拡張したい。適したトポロジとして最も代表的なものはどれか。
ア．全サーバを1台のハブに接続するだけの構成
イ．直列にスイッチを数十台連結するデイジーチェーン
ウ．スパイン・リーフ型トポロジ
エ．全サーバをWANルータへ直接収容する
正答：ウ
4肢解説
ア：可用性・拡張性の面で大規模データセンターには不向きである。
イ：ホップ数や障害影響が増えやすい。
ウ：正しい。リーフ間通信をスパイン経由で一定ホップにし、スパイン・リーフの追加で拡張しやすい。
エ：データセンターLANの一般的な東西トラフィック設計ではない。
総合解説：スパイン・リーフではL3 ECMPなどと組み合わせ、複数経路を活用しながら予測可能な遅延と拡張性を確保する。

問36 同一コストのL3経路が複数存在するとき、帯域活用と冗長性を高めるため複数経路へフローを分散する考え方はどれか。
ア．STPのルートポート固定
イ．DNSラウンドロビンだけ
ウ．NTP stratum
エ．ECMP
正答：エ
4肢解説
ア：STPはL2ループ防止の仕組みであり、L3等コスト経路分散とは異なる。
イ：名前解決での分散であり、ルーティングのECMPとは異なる。
ウ：時刻同期階層の概念である。
エ：正しい。ECMPは等コスト複数経路を利用し、経路冗長性と帯域利用効率を高める。
総合解説：ECMPでは通常フロー単位のハッシュなどを用いて順序逆転を抑えながら複数経路へ分散する。

問37 2台のスイッチ間で複数の物理リンクを同時利用しつつ、STPによって個々の並列リンクが不要にブロックされるのを避けたい。代表的な設計はどれか。
ア．複数物理リンクをリンクアグリゲーションで1論理リンクとして扱う
イ．各物理リンクを別々の同一L2経路として無制御で使う
ウ．全リンクのSTPを無効化する
エ．全リンクを異なるDNSゾーンへ登録する
正答：ア
4肢解説
ア：正しい。リンクアグリゲーションにより複数物理リンクを論理的に束ね、帯域増加とリンク冗長化を図れる。
イ：L2ループを発生させる危険がある。
ウ：ループ防止機能を失い危険である。
エ：L2転送設計とは無関係である。
総合解説：L2冗長化ではSTP、リンクアグリゲーション、装置冗長化の相互作用と障害時の収束を考慮する。

問38 アクセススイッチから上位へ10Gbit/sリンクを2本使用し、通常時は合計12Gbit/sのピークトラフィックを分散している。1本障害時にも全通信を収容したい場合、現状構成の評価として適切なものはどれか。
ア．2本の合計が20Gbit/sなので障害時も必ず20Gbit/s使える
イ．1本では10Gbit/sしかないため、障害時12Gbit/sを収容できず要件を満たさない
ウ．STPがあれば物理帯域不足は自動解消する
エ．VLAN数を増やせば12Gbit/sを10Gbit/sへ圧縮できる
正答：イ
4肢解説
ア：1本障害時は残存帯域10Gbit/sである。
イ：正しい。通常時に2本で足りても、N-1時の残存帯域がピークトラフィックより小さい。
ウ：STPは帯域容量を増やさない。
エ：VLAN分割では物理帯域不足は解消しない。
総合解説：冗長設計は正常時の合計容量ではなく、障害時に残る帯域でサービス要件を満たせるかを確認する。

問39 仮想マシン移動のため2棟間で同一VLANを延伸したいという要求がある。一方、棟間障害を相互に波及させたくない。設計者の対応として最も適切なものはどれか。
ア．要求を確認せず全VLANを両棟へ延伸する
イ．VM移動要件を無視して必ずL3分離だけを採用する
ウ．L2延伸が本当に必要な通信要件を確認し、可能ならL3境界を維持する方式や移動方式を比較する
エ．STPを完全に無効化すれば安全に延伸できる
正答：ウ
4肢解説
ア：不要なL2障害範囲を広げる可能性がある。
イ：業務・システム要件を無視した設計になる。
ウ：正しい。L2延伸には利便性がある一方、障害ドメイン拡大やループ影響などのリスクがあるため代替案を比較すべきである。
エ：ループ防止を失い危険である。
総合解説：L2延伸は必要最小限とし、障害ドメイン、MACテーブル規模、STP、BUMトラフィック、冗長化方式を総合評価する。

問40 コアスイッチを2台に冗長化したが、両方が同じ電源系統と同じラック内PDUだけに接続されている。設計上の問題として最も適切なものはどれか。
ア．2台あるので単一障害点は存在し得ない
イ．L3スイッチなら電源障害の影響を受けない
ウ．VLANを増やせば電源冗長になる
エ．装置は二重化されていても電源系統が単一障害点となっている
正答：エ
4肢解説
ア：共通電源障害で同時停止する可能性がある。
イ：装置は電源を必要とする。
ウ：論理設定では物理電源障害を解消できない。
エ：正しい。冗長設計では装置だけでなく電源、配線、ラック、経路などの依存関係も分離する必要がある。
総合解説：高可用LANではシャーシ、電源、PDU、UPS、配線、上位経路、管理系を含めたエンドツーエンドの冗長性を評価する。

問41 インターネット経由で拠点間IP通信の機密性・完全性・送信元認証を確保する代表的な技術はどれか。
ア．IPsec
イ．ARP
ウ．STP
エ．SNMP
正答：ア
4肢解説
ア：正しい。IPsecはIPパケットに対して暗号化、完全性保護、認証などのセキュリティサービスを提供する。
イ：IPv4アドレスとMACアドレスの対応解決に用いる。
ウ：L2ループ防止のためのプロトコルである。
エ：ネットワーク管理・監視に用いるプロトコル群である。
総合解説：拠点間VPNではIPsecのトンネルモードを利用する構成が一般的で、暗号方式、認証、鍵更新、経路設計も検討する。

問42 IPsec VPNでIKEv2が主に担う役割はどれか。
ア．EthernetのMACアドレス学習
イ．対向装置の認証と暗号パラメータ・鍵情報を含むSAの確立・維持
ウ．DNS名前解決
エ．HTTPキャッシュ制御
正答：イ
4肢解説
ア：L2スイッチの機能である。
イ：正しい。IKEv2はIPsecで利用するSecurity Associationを動的に確立・管理する。
ウ：DNSの役割である。
エ：HTTPの機能である。
総合解説：IKEv2は認証、鍵交換、暗号スイート交渉、CHILD_SA確立などを行い、手作業の鍵管理を減らす。

問43 通信事業者の閉域IP網とインターネットVPNを比較した説明として最も適切なものはどれか。
ア．閉域網では暗号化やアクセス制御を一切検討する必要がない
イ．インターネットVPNは必ず閉域網より遅延が小さい
ウ．閉域網は事業者管理網内で顧客通信を分離し、インターネットVPNは公衆インターネット上で暗号トンネルを構成する方式が代表的である
エ．両者は完全に同じサービスで名称だけが違う
正答：ウ
4肢解説
ア：閉域であっても機密性・認証要件に応じ追加対策が必要な場合がある。
イ：経路や混雑に依存し、一律には言えない。
ウ：正しい。両者はアクセス経路、分離方式、品質保証、暗号化要件、コストなどが異なる。
エ：ネットワーク基盤や品質特性が異なる。
総合解説：WAN選定では可用性、遅延、帯域、SLA、暗号化、拠点数、コスト、開通速度、インターネット出口設計を比較する。

問44 複数拠点間で動的ルーティング用のマルチキャスト通信をトンネル化しつつ、インターネット上では暗号化したい。代表的な構成として適切なものはどれか。
ア．GREだけで強力な暗号化を提供する
イ．IPsecを使うとルーティングは一切できない
ウ．DNSでマルチキャストを暗号化する
エ．GREで必要なトラフィックをカプセル化し、そのGRE通信をIPsecで保護する
正答：エ
4肢解説
ア：GRE自体は暗号化機能を提供しない。
イ：構成方式により動的ルーティングも可能である。
ウ：DNSにはその機能はない。
エ：正しい。GREは多様な上位プロトコルをトンネル化でき、IPsecと組み合わせて暗号化する構成がある。
総合解説：GRE over IPsecではカプセル化オーバーヘッド、MTU、断片化、経路制御、トンネル障害検知を考慮する。

問45 IPsec/GRE等のトンネル導入後、一部の大きなパケットだけ通信できなくなった。設計時にまず確認すべき項目として最も適切なものはどれか。
ア．カプセル化で実効MTUが小さくなり、断片化やPMTUDに問題がないか
イ．DNSのMX優先度
ウ．NTPのstratum
エ．VLAN名の文字数
正答：ア
4肢解説
ア：正しい。トンネルヘッダ分だけ外側パケットが大きくなり、経路MTUを超えると通信障害の原因になり得る。
イ：メール配送先選択であり、トンネルMTUとは無関係である。
ウ：時刻同期階層であり、大きなパケット問題の原因ではない。
エ：MTUには影響しない。
総合解説：VPN設計では暗号化性能だけでなく、追加ヘッダ、MTU/MSS、フラグメント、PMTUDを確認する。

問46 重要拠点で回線を2本契約しているが、両方とも同じ通信事業者・同じアクセス設備を利用している。可用性をさらに高める改善策として最も適切なものはどれか。
ア．同じアクセス回線を論理的に別VLANへ分けるだけ
イ．異なる事業者や物理経路を利用し、共通障害点を減らす
ウ．2本とも同じCPEの同じ電源へ接続する
エ．DNS TTLを長くする
正答：イ
4肢解説
ア：物理回線障害に対する冗長性は増えない。
イ：正しい。回線本数だけでなく事業者、収容局、管路、引込経路の分離が重要である。
ウ：新たな単一障害点を残す。
エ：回線物理障害の対策ではない。
総合解説：WAN冗長化ではアクセス回線、キャリア、CPE、電源、建物引込、ルーティングまで共通障害点を評価する。

問47 通信事業者のMPLS L3VPNで、複数顧客が同じ事業者網を共有しながら顧客ごとに経路情報を分離する仕組みとして代表的なものはどれか。
ア．全顧客を同一グローバルルーティングテーブルだけで管理する
イ．顧客ごとにEthernet FCSの計算方式を変える
ウ．VRFを用いて顧客ごとのルーティングテーブルを分離する
エ．DNSのゾーンを分けるだけ
正答：ウ
4肢解説
ア：顧客経路分離ができない。
イ：経路分離とは無関係である。
ウ：正しい。MPLS L3VPNではPEルータ上でVRFを用いて顧客経路を分離する。
エ：IPルーティング分離にはならない。
総合解説：VRFとMPLS/BGPを組み合わせ、同一事業者バックボーン上で複数顧客のL3VPNを分離する。

問48 インターネットVPNで平常時800Mbit/s、障害時最大1.4Gbit/sの暗号化トラフィックが1台へ集中する。障害時も処理したい場合、装置のIPsec暗号化スループット要件として最低限どれが適切か。
ア．800Mbit/s以上（平常時最大だけを基準にする）
イ．600Mbit/s以上（平常時負荷にも届かない）
ウ．1.0Gbit/s以上（障害時最大1.4Gbit/sに届かない）
エ．1.4Gbit/s以上（障害時最大値を基準にする）
正答：エ
4肢解説
ア：平常時は満たすが障害時1.4Gbit/sを処理できない。
イ：平常時の負荷にも不足する。
ウ：障害時最大値に達しない。
エ：正しい。障害時最大値を1台で処理する必要があるため、少なくとも1.4Gbit/s以上が必要である。
総合解説：VPN装置は通常転送性能と暗号化時性能が異なる場合があるため、暗号方式やパケットサイズ条件を含めて確認する。

問49 全国200拠点を短期間で接続したい。各拠点には安価なインターネット回線が既にあり、業務は暗号化必須だが数十msの遅延変動は許容できる。第一候補として合理的な方式はどれか。
ア．既存インターネット回線を活用したIPsec VPNを評価する
イ．必ず全拠点へ新規専用線だけを敷設する
ウ．暗号化要件を無視して平文通信にする
エ．LAN内VLANだけで全国拠点を接続する
正答：ア
4肢解説
ア：正しい。既設回線の活用、暗号化要件、短期展開、ある程度の遅延変動許容という条件から有力候補になる。
イ：要件上必須とは言えず、コスト・開通期間が大きくなる可能性がある。
ウ：明示された要件を満たさない。
エ：WAN接続手段にならない。
総合解説：WAN方式は要件に応じて閉域網、インターネットVPN、SD-WAN、専用線等を比較し、複数方式の併用も検討する。

問50 ルータの物理インタフェースはUPのままだが、通信事業者網の先で障害が発生しインターネットへ到達できない。このときバックアップ回線へ確実に切り替えたい。設計として最も適切なものはどれか。
ア．物理ポートのUP/DOWNだけを唯一の障害判定にする
イ．リンク状態だけでなく遠隔到達性を監視し、その結果を経路制御へ連動させる
ウ．DNSキャッシュを増やせば必ず回線切替えできる
エ．バックアップ回線を常にshutdownして監視しない
正答：イ
4肢解説
ア：上流障害ではリンクUPのまま通信不能になり得る。
イ：正しい。物理リンクUPだけでは上流障害を検出できないため、IP SLA的な到達性監視や動的ルーティング等を組み合わせる。
ウ：経路切替えの検出手段ではない。
エ：障害時に利用可能か確認できず、切替えも遅れる。
総合解説：WAN冗長では障害の検出点、検出時間、経路収束、セッション影響、戻し条件まで設計する必要がある。

問51 IPアドレスを連続したブロックで拠点へ割り当てる設計上の利点として最も適切なものはどれか。
ア．各端末のMACアドレスが不要になる
イ．全通信が自動的に暗号化される
ウ．上位ルータで複数サブネットを1つの要約経路に集約しやすくなる
エ．DNSサーバが不要になる
正答：ウ
4肢解説
ア：IPアドレス集約とMACアドレスの有無は無関係である。
イ：CIDRに暗号化機能はない。
ウ：正しい。連続アドレス割当てにより経路集約がしやすくなり、ルーティングテーブルや経路変動の影響を抑えられる。
エ：名前解決の要否とは別である。
総合解説：アドレス計画は現在の端末数だけでなく、経路集約、拡張余地、拠点追加、アドレス重複回避を考慮する。

問52 部門ごとに必要ホスト数が異なるため、同じ固定サイズではなく必要数に応じて異なるプレフィックス長のサブネットを割り当てる設計はどれか。
ア．NATだけ
イ．STP
ウ．SMTP
エ．VLSM
正答：エ
4肢解説
ア：NATはアドレス変換であり、サブネットサイズを可変に割り当てる考え方ではない。
イ：L2ループ防止プロトコルである。
ウ：メール配送プロトコルである。
エ：正しい。VLSMは可変長サブネットマスクを用いて、用途に応じたサイズのサブネットを割り当てる。
総合解説：VLSMを使うとアドレス空間を効率利用できるが、将来増加分を見込んだ余裕と集約可能性を考慮する。

問53 一般的なIPv6 LANセグメントのプレフィックス長として標準的に用いられるものはどれか。
ア．/64
イ．/8
ウ．/24
エ．/128を全LANで共有する
正答：ア
4肢解説
ア：正しい。IPv6の多くのLANでは64ビットのインタフェース識別子を前提とする/64サブネットが標準的である。
イ：一般的なIPv6 LANサブネットとしては大きすぎ、IPv4的なクラス概念でもない。
ウ：IPv4 LANでよく見る長さだが、IPv6 LANの標準的なサブネット長ではない。
エ：/128は単一アドレスを表すため、複数端末LANの共有サブネットには使えない。
総合解説：IPv6ではアドレス空間が広いため、過度な節約より階層性・集約性・運用性を重視した設計が基本となる。

問54 企業買収後、両社とも10.0.0.0/8内の同じサブネットを多数利用していることが分かった。統合ネットワーク設計で最も注意すべき問題はどれか。
ア．プライベートアドレス同士なら自動的に重複を解決する
イ．アドレス重複により相互接続時の経路識別ができず、NATや再アドレス設計が必要になる可能性がある
ウ．RFC1918アドレスは企業内で1社しか使えない
エ．DNSを使えばIP重複は常に無関係になる
正答：イ
4肢解説
ア：そのような仕組みはない。
イ：正しい。同一アドレス空間が両側に存在すると通常のルーティングでは宛先を一意に区別できない。
ウ：多くの組織が独立して同じ範囲を使えるため、統合時に重複し得る。
エ：最終的なIP転送では宛先アドレスを一意に扱う必要がある。
総合解説：将来のM&A、クラウド接続、取引先VPNを考えると、過度に広いRFC1918空間の乱用を避け、用途別に計画的に割り当てることが重要である。

問55 192.168.8.0/24、192.168.9.0/24、192.168.10.0/24、192.168.11.0/24の4ネットワークを、余分な/24を含めず1本に集約する最小のCIDRはどれか。
ア．192.168.8.0/24（8の1ネットワークだけを包含）
イ．192.168.8.0/23（8〜9の2ネットワークを包含）
ウ．192.168.8.0/22（8〜11の4ネットワークを包含）
エ．192.168.0.0/20（0〜15を包含して余分な範囲を含む）
正答：ウ
4肢解説
ア：1つ目のサブネットしか含まない。
イ：8と9の2個の/24しか含まない。
ウ：正しい。第三オクテット8〜11の4個の連続/24は、4アドレスブロック境界である8から始まる/22に集約できる。
エ：4ネットワークを含むが、余分な範囲を多数含み『余分な/24を含めない最小』ではない。
総合解説：経路集約では対象ネットワークが2のべき乗個で連続し、集約プレフィックスの境界に整列しているか確認する。

問56 小規模支店は本社WANへ1本だけ接続し、支店外宛て通信は全て本社へ送る。支店ルータの経路設計として簡潔で適切なものはどれか。
ア．インターネット全経路を必ず支店へ配布する
イ．全宛先を同一LAN内としてARPする
ウ．DNSのAレコードだけで経路制御する
エ．支店LANの直結経路に加え、本社側をネクストホップとするデフォルトルートを設定する
正答：エ
4肢解説
ア：必要以上に経路数と運用負荷が増える。
イ：異なるIPネットワークへはルータ経由で転送する。
ウ：DNSはIPルーティングテーブルを置き換えない。
エ：正しい。外部への出口が1方向だけなら、個別経路を大量に持つよりデフォルトルートが適している。
総合解説：スタブ拠点ではデフォルトルートを活用し、上位側では支店プレフィックスを集約するなど階層的な経路設計が有効である。

問57 OSPFネットワークを適切に複数エリアへ分割する主な設計上の利点はどれか。
ア．LSDBやSPF計算、トポロジ変化の影響範囲を階層化して抑えやすくする
イ．全ルータが必ず同じLSDBを全ASで保持するようにする
ウ．BGPのAS番号を不要にする
エ．EthernetのMAC学習を停止する
正答：ア
4肢解説
ア：正しい。エリア分割によりリンク状態情報の範囲を制御し、大規模ネットワークの拡張性を高める。
イ：エリア分割はむしろ詳細トポロジ情報の範囲を分ける。
ウ：OSPFエリアとBGP AS番号は別概念である。
エ：OSPFエリア設計とは無関係である。
総合解説：OSPF設計ではバックボーンエリア0、ABR配置、要約、エリアサイズ、障害収束を考慮する。

問58 IPv6で組織内部の限定用途に使用し、グローバルインターネットでの経路広告を前提としないアドレスとして利用できるものはどれか。
ア．IPv4の169.254.0.0/16をそのままIPv6として使う
イ．Unique Local IPv6 Unicast Address（ULA）
ウ．全てのIPv6グローバルユニキャストを内部専用とみなす
エ．EthernetのMACアドレスをIPv6アドレスとして直接経路広告する
正答：イ
4肢解説
ア：IPv4リンクローカル範囲でありIPv6 ULAではない。
イ：正しい。ULAは組織内など限定範囲で利用するIPv6ユニキャストアドレスとして定義されている。
ウ：グローバルユニキャストはインターネットで経路制御され得る。
エ：アドレス体系が異なる。
総合解説：IPv6設計ではGUA、ULA、リンクローカルなどの役割を理解し、NAT依存ではなく階層的なプレフィックス設計を行う。

問59 自社ASが2社のISPへマルチホームし、通常はISP-Aを主要出口、ISP-Bをバックアップとして使いたい。設計として最も適切な考え方はどれか。
ア．BGPは常に物理帯域が大きい回線を自動選択するので設定不要
イ．両ISPへ同じ設定を行えば必ず完全な主従になる
ウ．BGP属性や受信・広告ポリシーを使い、送信方向と受信方向の経路選好を意図通り制御する
エ．DNS TTLだけで全IPトラフィックの出口を制御する
正答：ウ
4肢解説
ア：BGPの経路選択は帯域を直接基準に自動選択するものではない。
イ：同一条件なら期待する主従制御にならない場合がある。
ウ：正しい。マルチホームではLocal Preference等の内部ポリシーと、広告方法やAS_PATH等を組み合わせて経路選好を設計する。
エ：DNSは送信元ネットワークのBGP出口選択を直接制御しない。
総合解説：BGPマルチホームでは送信方向と受信方向で制御方法が異なり、障害時収束や経路フィルタも含めて設計する。

問60 上位ルータへ10.10.0.0/16の要約経路だけを広告しているが、配下の10.10.50.0/24が障害で到達不能になった。上位からの通信が要約経路に従って流入し続ける場合のリスクはどれか。
ア．経路集約を使うと全障害が自動的に上位へ通知される
イ．要約経路がある限り配下全サブネットは必ず到達可能である
ウ．DNSが自動で別サブネットへ転送する
エ．詳細経路が消えても要約経路が残ると、到達不能宛て通信が要約元へ送られブラックホール化する可能性がある
正答：エ
4肢解説
ア：要約により詳細障害が隠れる場合がある。
イ：実際の詳細経路やリンク障害に依存する。
ウ：IPルーティングのブラックホールをDNSが自動解決するわけではない。
エ：正しい。集約は経路数を減らす一方、詳細な到達性変化を隠すため、要約生成条件やdiscard route等を適切に設計する必要がある。
総合解説：経路集約はスケーラビリティを高めるが、要約の有効条件、障害時挙動、ループ・ブラックホール防止を確認する。

問61 同じ送信条件を単純化して比較した場合、2.4GHz帯と5GHz帯のWi-Fi設計について一般に適切な説明はどれか。
ア．2.4GHz帯は比較的到達しやすい一方、利用機器や干渉源が多く混雑しやすい
イ．5GHz帯は壁の影響を一切受けない
ウ．2.4GHz帯ではチャネル設計が不要である
エ．周波数帯が違っても伝搬・干渉特性は完全に同じである
正答：ア
4肢解説
ア：正しい。2.4GHz帯は伝搬上有利な場面がある一方、利用可能チャネルや他機器との干渉を考慮する必要がある。
イ：高い周波数でも壁・床などによる減衰は発生する。
ウ：隣接・同一チャネル干渉を避けるためチャネル設計が重要である。
エ：周波数や利用可能チャネル、規制条件により特性が異なる。
総合解説：無線LAN設計では到達距離だけでなく、干渉、利用可能チャネル数、端末対応、必要容量を考慮して周波数帯を使い分ける。

問62 Wi-Fiで20MHzより広いチャネル幅を利用する場合の一般的なトレードオフとして最も適切なものはどれか。
ア．チャネル幅を広げるほど必ずAP台数を無制限に増やせる
イ．1通信で高い速度を得やすい一方、利用できる独立チャネル数が減り、密集環境では干渉設計が難しくなる
ウ．広いチャネル幅では電波干渉が物理的に発生しない
エ．チャネル幅は無線速度や容量に影響しない
正答：イ
4肢解説
ア：利用可能な周波数資源が減るため高密度配置では逆に不利になる場合がある。
イ：正しい。広帯域化はピーク速度向上に有効だが、周波数資源を多く消費する。
ウ：隣接・同一チャネルの競合は引き続き考慮が必要である。
エ：利用可能帯域幅はPHYレートやチャネル再利用に影響する。
総合解説：高密度環境では最大チャネル幅より、セルごとのチャネル再利用と同時利用容量を優先することがある。

問63 無線LANの受信品質評価で、受信信号強度だけでなくSNRを確認する理由として最も適切なものはどれか。
ア．SNRはIPアドレス数を表すため
イ．SNRが低いほど必ず高い変調方式を使えるため
ウ．信号が強くても雑音が同程度に強ければ通信品質が悪化するため
エ．RSSIがあれば雑音レベルは常にゼロとみなせるため
正答：ウ
4肢解説
ア：SNRは無線信号品質の指標でありアドレス数とは無関係である。
イ：一般に高い変調方式にはより良好なSNRが必要である。
ウ：正しい。SNRは信号と雑音の差を示し、復調可能性や実効速度を判断する重要な指標となる。
エ：RSSIだけでは雑音環境を把握できない。
総合解説：サイトサーベイではRSSI、SNR、チャネル利用率、干渉源、再送率などを組み合わせて評価する。

問64 隣接するAPが同じチャネルを使用しており、互いの電波が十分強く届いている。この状態の主な問題として最も適切なものはどれか。
ア．同じチャネルなら必ず互いを無視して同時送信できる
イ．IPアドレスが自動的に重複する
ウ．TLS証明書が無効になる
エ．同一チャネル上で送信機会を共有するため、競合が増えて実効容量が低下する
正答：エ
4肢解説
ア：同一チャネルでは媒体アクセスを共有するため競合が発生する。
イ：チャネル一致とIPアドレス重複は別問題である。
ウ：無線チャネルとは無関係である。
エ：正しい。同一チャネルの端末・APは同じ無線媒体を共有し、CSMA/CAによる競合が増える。
総合解説：AP配置では同一チャネル再利用距離を確保し、隣接チャネル干渉も避けながらセル容量を設計する。

問65 オフィス全域でSSIDは見えるが、昼休みに接続端末が集中すると通信が著しく遅くなる。追加設計で最も重視すべき観点はどれか。
ア．カバレッジだけでなく、AP当たりの同時端末数・通信量・チャネル利用率による容量
イ．SSIDが見えるので無線設計は完了している
ウ．APの送信出力を全台最大にすれば必ず改善する
エ．端末のDNS名を短くすれば容量が増える
正答：ア
4肢解説
ア：正しい。電波が届くことと、必要な同時通信容量を満たすことは別の設計問題である。
イ：利用者密度が高い環境では容量不足が起こり得る。
ウ：セルが広がり同一チャネル競合やローミング問題を悪化させる場合がある。
エ：無線媒体の容量にはほぼ影響しない。
総合解説：高密度Wi-Fiでは端末密度とトラフィック需要からAP・チャネル数を設計し、単なる電波到達確認で終えない。

問66 多数の端末が小さなデータを頻繁に送受信する高密度Wi-Fi環境で、802.11axのOFDMAが有効な理由として最も適切なものはどれか。
ア．全端末へ常にチャネル全幅を独占させるため
イ．チャネルを複数のリソース単位に分け、複数端末を効率よく同時に収容できるため
ウ．有線EthernetのVLANを自動削除するため
エ．DNS応答を圧縮する技術だから
正答：イ
4肢解説
ア：OFDMAの狙いとは逆である。
イ：正しい。OFDMAは周波数資源を細分化して端末へ割り当て、高密度環境での効率向上を狙う。
ウ：無線PHY/MAC効率化とVLAN削除は無関係である。
エ：OFDMAは無線アクセス技術である。
総合解説：802.11axはOFDMAなどを利用して、多数端末が存在する環境でのスペクトル利用効率向上を図る。

問67 5GHz帯でDFS対象チャネルを利用する無線LANを設計する際に考慮すべき事項として最も適切なものはどれか。
ア．DFSチャネルでは電波法上の制約が一切ない
イ．DFSを使えば必ず干渉がゼロになる
ウ．レーダ波を検出した場合にチャネル変更等が必要となり、通信へ影響する可能性を考慮する
エ．DFSはDNSのフェイルオーバ方式である
正答：ウ
4肢解説
ア：周波数共用のための条件がある。
イ：他のWi-Fiや環境要因による干渉は残り得る。
ウ：正しい。DFS対象帯域ではレーダ等との共用条件があり、検出時のチャネル移動が発生し得る。
エ：無線周波数の動的選択に関する仕組みである。
総合解説：チャネル設計では利用可能チャネル数だけでなく、DFSイベント時の切替え、端末対応、重要通信への影響も評価する。

問68 隣接AP間のセル重なりを適切に保ちつつ、端末が遠方APへ張り付き続ける問題を減らしたい。設計として最も適切な考え方はどれか。
ア．全APを常に最大出力に固定する
イ．セルが全く重ならないようにする
ウ．SSIDごとに異なるIPバージョンを使えば解決する
エ．APの送信出力と配置を調整し、必要以上にセルを広げず適切な重なりを確保する
正答：エ
4肢解説
ア：高密度環境ではセル過大・干渉増加につながる場合がある。
イ：ローミング時の通信継続が難しくなる。
ウ：無線セル設計の問題とは別である。
エ：正しい。出力を過大にすると端末が遠いAPを受信し続け、同一チャネル干渉やローミング遅延を招くことがある。
総合解説：送信出力はカバレッジ、干渉、端末送信能力、ローミング境界を考慮して調整する。

問69 通信が遅いという理由だけで同じチャネルのAPを狭い範囲へ大量追加したところ、さらに性能が悪化した。最も考えやすい理由はどれか。
ア．同一チャネルの競合と管理フレーム等の無線オーバーヘッドが増え、1セル当たりの利用可能時間が減った
イ．AP数が増えると必ず周波数帯域そのものが増える
ウ．Wi-FiではAP同士の干渉は発生しない
エ．DNSレコード数が増えたため
正答：ア
4肢解説
ア：正しい。AP数を増やしてもチャネル再利用設計が不適切なら、同一チャネル競合が増えて容量が低下する。
イ：同一周波数資源を共有するAPでは容量が単純加算されない。
ウ：同一・隣接チャネルで干渉や競合が発生する。
エ：無線媒体性能の主因ではない。
総合解説：高密度設計ではAP台数よりチャネル再利用、セルサイズ、送信出力、端末密度、管理オーバーヘッドを総合評価する。

問70 同一APに高速端末と低速な旧規格端末が混在し、旧端末が大量通信すると全体性能が低下した。理由として最も適切なものはどれか。
ア．低速端末は周波数を一切使用しないため
イ．低速端末は同じデータ量を送るのに長いエアタイムを消費し、他端末の送信機会を減らすため
ウ．高速端末のIPアドレスが消えるため
エ．APの有線ポートが必ず10Mbit/sへ固定されるため
正答：イ
4肢解説
ア：実際にはより長時間媒体を使用することがある。
イ：正しい。無線LANでは共有媒体のエアタイムが重要で、低PHYレート端末が多くの時間を占有すると全体容量が低下する。
ウ：アドレス管理とは無関係である。
エ：そのような自動動作はない。
総合解説：無線容量設計では接続端末数だけでなく、PHYレート分布、再送率、エアタイム使用率、旧規格端末の影響を確認する。

問71 802.1X認証で、端末、アクセス装置、認証サーバの役割名の組合せとして適切なものはどれか。
ア．Client、Router、DNS Rootだけ
イ．Sender、Receiver、NTP Server
ウ．Supplicant、Authenticator、Authentication Server
エ．Publisher、Broker、Subscriber
正答：ウ
4肢解説
ア：802.1Xの標準的な役割名ではない。
イ：802.1X認証の構成要素ではない。
ウ：正しい。端末がSupplicant、APやスイッチがAuthenticator、RADIUS等の認証基盤がAuthentication Serverとして動作する。
エ：MQTTのpublish/subscribeで使われる役割である。
総合解説：企業無線LANではAPが802.1X Authenticatorとなり、RADIUSサーバを認証サーバとして利用する構成が一般的である。

問72 企業無線LANでEAP-TLSを利用する主な特徴として最も適切なものはどれか。
ア．全端末が同じ共有パスワードだけを使う
イ．認証サーバを使わずMACアドレスだけを暗号鍵にする
ウ．認証後も通信を暗号化しないことが必須である
エ．クライアント証明書とサーバ証明書を利用した強固な相互認証を構成できる
正答：エ
4肢解説
ア：これはPSK型の考え方に近く、EAP-TLSの特徴ではない。
イ：EAP-TLSの証明書認証とは異なる。
ウ：無線LANの暗号化と組み合わせて利用する。
エ：正しい。EAP-TLSはTLSと証明書を用いて端末・利用者側と認証サーバ側の相互認証を実現できる。
総合解説：EAP-TLSは強い認証を提供する一方、証明書配布・更新・失効などPKI運用が重要になる。

問73 多数の社員が利用する企業無線LANで、退職者だけのアクセス権を個別に無効化し、利用者単位で認証ログを残したい。一般に適した方式はどれか。
ア．802.1X/EAPを用いるEnterprise認証
イ．全社員で同じPSKを永久共有する
ウ．SSIDを非表示にするだけ
エ．MACアドレスを公開Webページへ掲載する
正答：ア
4肢解説
ア：正しい。個別IDや証明書を利用するEnterprise認証は、利用者・端末単位の失効や監査に適している。
イ：一人の退職時に個別無効化しにくく、共有鍵漏えい時の影響も大きい。
ウ：SSID非表示は強固な利用者認証の代替にならない。
エ：認証強化にならず、セキュリティ上不適切である。
総合解説：企業無線では認証の粒度、鍵管理、監査、端末管理を考慮してPSKと802.1X系を使い分ける。

問74 無線APが802.1XのEAPメッセージを認証基盤へ中継し、認証結果や属性情報を受け取る構成で一般的に利用されるプロトコルはどれか。
ア．OSPF
イ．RADIUS
ウ．ARP
エ．FTP
正答：イ
4肢解説
ア：ルーティングプロトコルである。
イ：正しい。802.1X Enterprise環境ではAP/コントローラがRADIUSクライアントとなり、認証サーバとAAA情報を交換する構成が一般的である。
ウ：IPv4アドレス解決プロトコルである。
エ：ファイル転送プロトコルである。
総合解説：RADIUS属性を利用してVLANやACL等を認証結果に応じて動的適用する設計も可能である。

問75 802.1X/EAP-TLS環境で、クライアントが認証サーバ証明書を適切に検証しない場合のリスクとして最も適切なものはどれか。
ア．無線電波の周波数が自動的に変わる
イ．IPv6アドレスが必ず重複する
ウ．偽の認証サーバへ接続してしまい、中間者攻撃などを許す可能性がある
エ．APのPoE給電が停止する
正答：ウ
4肢解説
ア：証明書検証とは無関係である。
イ：直接関係しない。
ウ：正しい。信頼するCAやサーバ名を検証しないと、攻撃者のサーバを正規と誤認する恐れがある。
エ：認証サーバ証明書とは無関係である。
総合解説：無線認証ではクライアント側のサーバ証明書検証設定と証明書ライフサイクル管理が重要である。

問76 音声端末がAP間を移動する際の認証・鍵確立時間を短縮し、通話断を抑えたい。IEEE 802.11の高速BSS遷移機能として代表的なものはどれか。
ア．802.11ax OFDMA
イ．802.1Q VLAN tagging
ウ．NTP
エ．802.11r Fast BSS Transition
正答：エ
4肢解説
ア：高密度環境の無線効率向上に関する機能で、主目的はローミング認証短縮ではない。
イ：有線ブリッジのVLAN識別であり高速BSS遷移の機能ではない。
ウ：時刻同期プロトコルである。
エ：正しい。802.11rはAP間ローミング時の認証・鍵管理を高速化し、リアルタイム通信への影響を減らす。
総合解説：ローミング性能は802.11rだけでなく、認証方式、コントローラ設計、セル重なり、端末実装にも依存する。

問77 端末がより適切なAP候補を見つけやすくし、無線LAN側からBSS遷移候補を提示したい。関連する機能として適切な組合せはどれか。
ア．802.11kの無線資源情報と802.11vのBSS Transition Management
イ．802.3のAuto-NegotiationとSTP
ウ．SMTPとIMAP
エ．BGPとMPLS
正答：ア
4肢解説
ア：正しい。802.11kの測定・近隣情報や802.11vの管理機能はローミング判断を支援できる。
イ：有線Ethernet機能でありWi-Fiローミング支援ではない。
ウ：メール通信プロトコルである。
エ：WANルーティング・ラベル転送技術である。
総合解説：最終的なローミング判断は端末実装に依存する場合があるため、802.11k/vは支援機能として設計・検証する。

問78 同じSSIDを利用しながら、社員・委託先・管理端末で接続先VLANを分けたい。適切な設計として代表的なものはどれか。
ア．全利用者を必ず同じVLANへ入れる
イ．802.1X認証結果とRADIUS属性に基づきVLANを動的に割り当てる
ウ．SSID名の文字数だけでVLANを決める
エ．DNSキャッシュの有無でVLANを変更する
正答：イ
4肢解説
ア：要求である利用者区分ごとの分離を満たさない。
イ：正しい。認証属性に応じて利用者・端末ごとにネットワークセグメントを分離できる。
ウ：認証された属性に基づく制御ではない。
エ：認証ポリシーとは無関係である。
総合解説：認証連動制御ではVLANだけでなくACL、ロール、セキュリティポリシーを動的適用する構成もある。

問79 無線端末が建物間を移動すると接続先サブネットが変わり、IPアドレス変更によって長時間セッションが切断される。設計上まず検討すべきことはどれか。
ア．全APのSSIDを毎回変更する
イ．IPサブネット変更はTCPセッションに一切影響しないとみなす
ウ．端末移動範囲とIPサブネット境界を整理し、セッション継続が必要ならモビリティ機能やアプリ再接続方式を検討する
エ．DNSのMXレコードを変更する
正答：ウ
4肢解説
ア：ローミングとセッション継続を悪化させる。
イ：通常は送信元IPが変わると既存セッション維持が難しい。
ウ：正しい。無線ローミングとIPサブネット移動は別問題であり、L3境界を越えるとIPアドレスや経路が変わる可能性がある。
エ：メール配送設定であり無線モビリティの解決策ではない。
総合解説：ローミング設計では無線認証の切替え時間だけでなく、L2/L3境界、IPアドレス維持、セッション継続要件を確認する。

問80 全社Wi-Fiを802.1X化したところ、単一RADIUSサーバ障害で新規端末が全拠点接続不能になることが分かった。改善策として最も適切なものはどれか。
ア．SSIDを非表示にすればRADIUS障害を回避できる
イ．全端末の証明書を削除する
ウ．APを増設するだけ
エ．認証サーバを冗長化し、AP/コントローラ側に複数認証先とタイムアウト・切替え条件を設定する
正答：エ
4肢解説
ア：SSID非表示は認証サーバ可用性と無関係である。
イ：802.1X認証自体ができなくなる。
ウ：認証バックエンドの単一障害点は残る。
エ：正しい。認証基盤はネットワーク利用開始の重要依存先なので、サーバと経路の冗長化が必要である。
総合解説：Enterprise無線LANの可用性はAPだけでなくRADIUS、PKI、ディレクトリ、DNS/NTPなど認証依存サービスも含めて評価する。

問81 LPWA系通信をIoTで利用する代表的な目的として最も適切なものはどれか。
ア．低消費電力で比較的広域をカバーし、小容量データを長期間送信する端末を収容する
イ．常に数十Gbit/sの大容量映像を端末ごとに送る
ウ．有線Ethernetの代わりに必ず1m以内だけで通信する
エ．全端末を商用電源へ常時接続することが必須である
正答：ア
4肢解説
ア：正しい。LPWAは電池駆動センサなどで長距離・低消費電力・小容量通信を重視する用途に向く。
イ：LPWAの一般的な用途特性とは異なる。
ウ：広域性を重視する方式が多い。
エ：低消費電力・電池駆動を重視する用途がある。
総合解説：IoT無線方式は通信距離、データ量、電池寿命、移動性、免許帯/非免許帯、利用料金を比較して選定する。

問82 MQTTの基本的なメッセージングモデルとして最も適切なものはどれか。
ア．全端末が互いのMACアドレスだけを指定して直接配信する
イ．PublisherがBrokerへTopic付きで送信し、Subscriberが購読したTopicのメッセージを受け取る
ウ．ルータがBGPでTopicを広告する
エ．DNSサーバがセンサ値を必ず保存する
正答：イ
4肢解説
ア：MQTTのpublish/subscribeモデルではない。
イ：正しい。MQTTはBrokerを介するpublish/subscribeモデルを採用し、送信者と受信者を疎結合にできる。
ウ：BGPとMQTT Topicは無関係である。
エ：DNSはMQTT Brokerの代替ではない。
総合解説：MQTTは軽量なpublish/subscribe型で、多数IoT端末とバックエンド間の非同期メッセージ連携に利用される。

問83 制約の大きいIoT端末・ネットワーク向けに、HTTPに似たREST型の要求応答モデルを低オーバーヘッドで提供するプロトコルはどれか。
ア．BGP
イ．STP
ウ．CoAP
エ．VRRP
正答：ウ
4肢解説
ア：AS間ルーティングプロトコルである。
イ：L2ループ防止プロトコルである。
ウ：正しい。CoAPは制約ノード・M2M用途を想定し、REST型の通信モデルを小さなオーバーヘッドで提供する。
エ：デフォルトゲートウェイ冗長化プロトコルである。
総合解説：CoAPはURIやメディアタイプなどWebの概念を取り入れつつ、制約環境向けに軽量化されている。

問84 1分ごとに温度を送るセンサで、1件程度失われても次の値で補えるため通信量を最小化したい。MQTTのQoSとして最も適切な候補はどれか。
ア．QoS 2だけが必須
イ．QoS値は配送信頼性と無関係である
ウ．QoS 0は必ず全メッセージを重複配送する
エ．QoS 0（At most once）
正答：エ
4肢解説
ア：Exactly onceは高い信頼性が必要な用途向けで、追加オーバーヘッドがある。
イ：MQTT QoSは配送保証レベルを表す。
ウ：QoS 0はbest effortで、重複保証を行う方式ではない。
エ：正しい。QoS 0は再送による配送保証を行わずオーバーヘッドが最小で、多少の欠落を許容できるセンサ値に適する場合がある。
総合解説：MQTTではQoS 0/1/2で信頼性と通信オーバーヘッドのトレードオフを選択する。

問85 小さなIEEE 802.15.4フレーム上でIPv6を扱いやすくするため、ヘッダ圧縮やフラグメンテーション等を提供する技術はどれか。
ア．6LoWPAN
イ．MPLS
ウ．SMTP
エ．VRRP
正答：ア
4肢解説
ア：正しい。6LoWPANは制約のあるIEEE 802.15.4ネットワークでIPv6を利用するための適応層機能を提供する。
イ：ラベルスイッチング技術でありIEEE 802.15.4上のIPv6適応層ではない。
ウ：メール配送プロトコルである。
エ：ルータ冗長化プロトコルである。
総合解説：IPv6パケットは小さいリンクMTUに対して大きいため、6LoWPANでは圧縮や分割により制約ネットワークへ適応させる。

問86 非常に少量のセンサデータを低頻度で送り、低消費電力と広いカバレッジを重視し、高速移動や高データレートを必要としない。セルラーIoT方式として有力な候補はどれか。
ア．常にWi-Fi 7だけを使う
イ．NB-IoT
ウ．100GbE
エ．MPLS L3VPN
正答：イ
4肢解説
ア：要件は広域セルラーIoTであり、Wi-Fiだけが唯一の候補ではない。
イ：正しい。NB-IoTは低データレート、広域カバレッジ、低消費電力を重視する大量IoT端末用途に適する。
ウ：データセンター向け高速有線Ethernetであり電池駆動広域センサ用途ではない。
エ：WANの経路分離技術であり端末無線アクセス方式ではない。
総合解説：セルラーIoTではNB-IoT、LTE-M等を、移動性、データ量、遅延、消費電力、通信エリアに応じて選択する。

問87 工場の1,000台のセンサが毎秒生データを生成するが、クラウドへは異常時の要約だけ送ればよい。ゲートウェイで一次分析する利点として最も適切なものはどれか。
ア．全センサの電池を物理的に無限化できる
イ．IPアドレス設計が完全に不要になる
ウ．上位回線のトラフィックを削減し、異常判定の応答遅延も短縮できる
エ．クラウド障害が一切発生しなくなる
正答：ウ
4肢解説
ア：通信削減で電力低減は期待できても電池が無限になるわけではない。
イ：IoT端末・ゲートウェイ間のネットワーク設計は引き続き必要である。
ウ：正しい。エッジ処理により不要な生データのWAN転送を減らし、現場で低遅延に処理できる。
エ：エッジ処理はクラウド自体の障害をなくすものではない。
総合解説：エッジとクラウドの処理分担は帯域、遅延、可用性、データ保存、セキュリティ、運用更新を考慮して決める。

問88 数万台のIoT端末を安全に運用し、盗難端末1台だけを失効させたい。認証設計として最も適切なものはどれか。
ア．全端末で同一パスワードを製造時から永久共有する
イ．SSIDを非表示にすれば端末認証は不要である
ウ．IPアドレスを覚えていれば認証済みとみなす
エ．端末ごとに一意な認証情報を持たせ、個別にローテーション・失効できる仕組みにする
正答：エ
4肢解説
ア：1台から漏えいすると全端末が危険になり、個別失効も難しい。
イ：SSID非表示は端末認証の代替にならない。
ウ：IPアドレスは強い認証情報ではない。
エ：正しい。共通資格情報では1台の侵害が全端末へ波及するため、個別ID・鍵・証明書管理が望ましい。
総合解説：IoTでは製造・登録・運用・鍵更新・失効・廃棄までデバイスIDのライフサイクルを設計する。

問89 10,000台のセンサが1分に1回、200バイトのアプリケーションデータを送信する。プロトコルオーバーヘッドや再送を無視した平均データレートに最も近いものはどれか。
ア．約267kbit/s（10,000×200×8÷60で計算）
イ．約26.7kbit/s（正しい値の約1/10）
ウ．約2.67Mbit/s（正しい値の約10倍）
エ．約26.7Mbit/s（正しい値の約100倍）
正答：ア
4肢解説
ア：正しい。10,000×200=2,000,000バイト/分。8倍して16,000,000bit/分、60で割ると約266,667bit/sである。
イ：10倍小さい。
ウ：10倍大きい。
エ：100倍大きい。
総合解説：実際のIoT容量設計ではTCP/UDP、TLS/DTLS、MQTT/CoAP、無線再送、同時送信バーストを追加して見積もる。

問90 山間部のセンサゲートウェイは携帯回線が数時間途切れることがあるが、観測データを欠損させず回線復旧後に送信したい。最も適切な設計はどれか。
ア．通信断中のデータは全て即時破棄する
イ．ゲートウェイにローカルキューや永続ストレージを持たせ、送達確認に応じて再送するstore-and-forward方式を採用する
ウ．回線が切れない前提でRAMだけに無期限保持する
エ．DNS TTLを長くすれば通信断がなくなる
正答：イ
4肢解説
ア：データ欠損を許容しないという要件を満たさない。
イ：正しい。間欠接続を前提にローカル保持と再送を設計すれば、通信断中のデータを復旧後に送信できる。
ウ：電源断・再起動で消失する可能性があり、長時間断への耐性が不足する。
エ：無線回線断そのものを解消する方法ではない。
総合解説：IoTではネットワークが常時接続とは限らないため、バッファ容量、永続化、再送順序、重複排除、時刻情報を含めて設計する。

問91 クラウド環境におけるVPCの役割として最も適切なものはどれか。
ア．クラウド上に論理的に分離された仮想ネットワークを構成し、アドレス範囲やサブネット、経路などを設計する
イ．物理サーバのCPUクロックだけを制御する
ウ．DNSルートゾーンを独占的に管理する
エ．全テナントを同一L2ネットワークへ強制的に収容する
正答：ア
4肢解説
ア：正しい。VPCはクラウド上の仮想ネットワーク境界として、IPアドレス空間、サブネット、経路、接続方式などを設計する単位になる。
イ：VPCはネットワーク仮想化の概念でありCPUクロック制御が主目的ではない。
ウ：DNSのルート管理機能ではない。
エ：VPCはむしろ論理分離を実現するために用いられる。
総合解説：クラウドネットワーク設計では、VPCのCIDR、サブネット分割、経路、セキュリティ境界、オンプレミス接続を一体として考える。

問92 クラウドVPC内で、外部から直接到達させず、内部アプリケーションサーバだけを配置したい。最も適切な設計はどれか。
ア．必ずパブリックIPを付けてインターネットへ直接公開する
イ．インターネットへの直接受信経路を持たないプライベートサブネットに配置する
ウ．全サーバを同一ブロードキャストドメインへ配置する
エ．DNS名を削除すれば外部から到達できないとみなす
正答：イ
4肢解説
ア：外部公開不要という要件に反する。
イ：正しい。外部から直接公開しないサーバは、インターネット向けの直接受信経路を持たないサブネットへ配置するのが基本である。
ウ：クラウドVPCでは役割に応じたサブネット分割が重要である。
エ：DNS名がなくてもIP到達性があれば通信できる。
総合解説：サブネット設計では公開系、業務系、管理系などの役割を分け、経路とアクセス制御を組み合わせる。

問93 VPC内のサブネットから、別サブネット、VPN、インターネット出口などへの転送先を決めるために利用するものはどれか。
ア．TLS証明書だけ
イ．NTPのstratum
ウ．サブネットに関連付けられたルートテーブル
エ．HTTPのCookie
正答：ウ
4肢解説
ア：証明書は認証・暗号化に用いられ、IP転送先を決めない。
イ：時刻同期階層でありルーティングとは無関係である。
ウ：正しい。クラウド仮想ネットワークでも、宛先プレフィックスに応じた次の転送先をルートテーブルで定義する。
エ：アプリケーション状態管理でありIPルーティングには使わない。
総合解説：VPCの経路設計ではローカル経路、インターネット出口、NAT、VPN、専用接続、Peering等への経路を整理する。

問94 同一組織が別々に管理する二つのVPC間で、インターネットを経由せずプライベートIPで直接通信させたい。代表的な接続方式はどれか。
ア．DNSのMXレコード
イ．NTPピア
ウ．STP
エ．VPC Peering
正答：エ
4肢解説
ア：メール配送先を指定するものでVPC間接続ではない。
イ：時刻同期の相手を示すものでネットワーク相互接続ではない。
ウ：L2ループ防止プロトコルでありクラウドVPC間接続方式ではない。
エ：正しい。VPC Peeringは二つの仮想ネットワーク間をプライベートなIP接続で相互接続する代表的な方式である。
総合解説：Peeringでは両側のアドレス範囲、経路、アクセス制御、名前解決、非推移性など実装上の条件を確認する。

問95 VPC-AとVPC-B、VPC-BとVPC-Cだけを Peering接続した。代表的なVPC Peering実装を前提とすると、AからCへの通信について最も適切な考え方はどれか。
ア．A-BとB-CのPeeringだけではA-C通信を自動的に中継できないため、A-C接続やトランジット機能を別途設計する
イ．Bが存在すれば必ずA-Cも自動接続される
ウ．A-C通信にはDNS設定だけあればよい
エ．Peeringは必ずL2ブロードキャストを全VPCへ転送する
正答：ア
4肢解説
ア：正しい。多くのVPC Peeringは非推移であり、中間VPCを経由した自動中継を前提にできない。
イ：Peeringの非推移性を無視している。
ウ：IP経路・接続機能がなければ名前解決だけでは通信できない。
エ：一般的なVPC Peeringの動作ではない。
総合解説：VPC数が増える場合はフルメッシュPeeringの運用負荷を踏まえ、トランジット型のハブ構成を検討する。

問96 二つのVPCがともに10.10.0.0/16を使用している。相互接続時の主な問題はどれか。
ア．RFC1918同士なら自動的に区別される
イ．同じ宛先プレフィックスが両側に存在するため、通常のルーティングで一意に宛先を判断できない
ウ．CIDRが同じほど経路集約しやすく相互接続に有利である
エ．TLSを有効にすれば経路重複は解消する
正答：イ
4肢解説
ア：プライベートアドレスであっても重複はルーティング上の問題になる。
イ：正しい。アドレス重複はVPC PeeringやVPN接続で重大な制約となり、再アドレスやNAT等の対策が必要になる場合がある。
ウ：相互接続する独立ネットワーク間では重複が障害になる。
エ：暗号化は宛先経路の曖昧さを解消しない。
総合解説：クラウド導入初期から、将来のVPC追加、オンプレミス、M&A、他クラウド接続を考慮した重複しにくいアドレス計画が重要である。

問97 プライベートサブネットのサーバをインターネットから直接着信可能にはしたくないが、OS更新のため外向き通信は許可したい。代表的な設計はどれか。
ア．全サーバへ公開IPを付けて全ポートを開放する
イ．ルートを全て削除して通信不能にする
ウ．外向きNAT機能を経由させ、外部からの新規着信は直接受けない構成にする
エ．NTPだけ許可すればHTTP更新通信も自動通過する
正答：ウ
4肢解説
ア：直接着信を避ける要件に反する。
イ：OS更新の外向き通信もできなくなる。
ウ：正しい。送信元変換を用いた外向き出口により、プライベートアドレスのサーバから外部へ通信しつつ直接公開を避けられる。
エ：必要な宛先・プロトコルの経路とアクセス制御が必要である。
総合解説：NAT出口では可用性、帯域、同時セッション、送信元IP、ログ、障害時切替えを考慮する。

問98 本番環境と開発環境で管理者・変更手順・接続先が大きく異なり、誤操作の影響を相互に波及させたくない。設計として適切な考え方はどれか。
ア．本番と開発を同一サブネットにまとめ、全許可にする
イ．環境名だけ変えれば同等の分離になる
ウ．ルーティングを全許可すれば安全性が高まる
エ．必要に応じてVPCやアカウント等の管理境界を分け、接続は明示的な経路とポリシーで制御する
正答：エ
4肢解説
ア：障害・誤操作・権限の影響範囲が大きくなる。
イ：名称変更はネットワーク・権限分離にはならない。
ウ：不要な到達性を増やしリスクが高まる。
エ：正しい。論理的・管理的な境界を分けることで変更事故や権限誤設定の影響範囲を小さくできる。
総合解説：クラウド設計ではネットワーク境界と管理・権限境界を対応させ、必要最小限の接続だけを設ける。

問99 8個のVPCを全て相互に直接Peeringし、各VPC間に1本ずつ接続を作る。必要なPeering接続数は幾つか。
ア．28接続（8×7÷2で全ペアを数える）
イ．8接続（VPC数と同じ本数だけ作る）
ウ．16接続（各VPCに2本ずつとみなす）
エ．56接続（方向を区別して8×7で数える）
正答：ア
4肢解説
ア：正しい。n個を全組合せで直接接続する本数はn(n-1)/2なので、8×7/2=28本である。
イ：VPC数そのものであり、全組合せの接続数ではない。
ウ：全てのVPC間ペアを表していない。
エ：方向を区別して二重に数えた値である。
総合解説：VPC数が増えるとフルメッシュPeeringは$O(n^2)$で接続数が増えるため、ハブ型トランジット設計の検討価値が高まる。

問100 今後3年間でVPCが20個へ増え、オンプレミスと複数クラウドを相互接続する予定である。各VPCのCIDR設計として最も適切な方針はどれか。
ア．各VPC管理者が自由に10.0.0.0/16を使う
イ．全体アドレス計画を先に作り、重複を避けつつ環境・地域単位で集約可能な連続ブロックを割り当てる
ウ．VPCごとにランダムな重複CIDRを許可する
エ．経路集約を避けるため全サブネットを無関係な範囲へ分散する
正答：イ
4肢解説
ア：将来の相互接続で大規模な重複が発生する。
イ：正しい。将来接続を考えると、VPCごとの場当たり的なCIDR割当てではなく、全体で一意性と集約性を確保する必要がある。
ウ：経路設計が複雑化し、NAT依存が増える。
エ：経路表や運用を複雑にしやすい。
総合解説：ハイブリッド・マルチクラウドではIPAMを用い、オンプレミスとクラウド全体でアドレス一意性・拡張余地・経路集約を管理する。

問101 HTTPヘッダやURLパスの内容に応じてバックエンドを振り分けたい。最も適したロードバランシング方式はどれか。
ア．L2スイッチングだけ
イ．L3ルーティングだけ
ウ．L7ロードバランシング
エ．NTP
正答：ウ
4肢解説
ア：MACアドレスを基に転送するためHTTPパスによる振り分けはできない。
イ：IPアドレスを基に経路を決めるためHTTPヘッダ内容までは扱わない。
ウ：正しい。HTTPなどアプリケーション層の情報を見て振り分けるにはL7ロードバランサが適している。
エ：時刻同期プロトコルであり負荷分散機能ではない。
総合解説：L4 LBはIPアドレス・ポート等、L7 LBはHTTPヘッダ・URL・Cookie等を使った高度な振り分けが可能である。

問102 ロードバランサがバックエンドサーバへ定期的にヘルスチェックを行う主な目的はどれか。
ア．DNSゾーン転送を高速化するため
イ．暗号鍵を自動生成するため
ウ．サーバのIPアドレスを毎回変更するため
エ．正常に応答できないサーバへの新規振り分けを停止するため
正答：エ
4肢解説
ア：ヘルスチェックの主目的ではない。
イ：負荷分散の死活監視とは無関係である。
ウ：通常のヘルスチェック目的ではない。
エ：正しい。バックエンドの生存・サービス状態を確認し、異常サーバを振り分け対象から外す。
総合解説：ヘルスチェックは単なるTCP接続確認だけでなく、アプリケーション応答や依存先まで含めるかを要件に応じて設計する。

問103 CDNを利用する主な効果として最も適切なものはどれか。
ア．利用者に近い配信拠点からコンテンツを提供し、遅延やオリジンサーバ負荷を減らす
イ．全利用者を同一データセンターへ必ず直接接続させる
ウ．IPsec VPNを不要にすることだけが目的である
エ．DNSを完全に使用しなくなる
正答：ア
4肢解説
ア：正しい。CDNはエッジ配信拠点へコンテンツをキャッシュ・配信し、距離やオリジン負荷を低減する。
イ：CDNの分散配信とは逆である。
ウ：CDNの主目的ではない。
エ：CDNではDNSベースのリクエスト誘導なども利用される。
総合解説：CDNではキャッシュ、リクエストルーティング、オリジン保護、TLS終端などを組み合わせて配信性能を高める。

問104 Webアプリがセッション情報を各サーバのローカルメモリだけに保持している。LBで複数サーバへ分散するときに必要となる可能性が高い対策はどれか。
ア．全サーバのIPを同じ値にする
イ．同一利用者を同一バックエンドへ送るセッション維持、またはセッション情報を共有ストアへ移す
ウ．DNS TTLを無限にする
エ．HTTPをSMTPへ変更する
正答：イ
4肢解説
ア：IP重複となり正常な設計ではない。
イ：正しい。バックエンドをまたぐと状態が失われる設計では、スティッキーセッションか状態外部化が必要になる。
ウ：アプリケーションセッション状態の問題は解決しない。
エ：プロトコル変更ではセッション共有問題を解決しない。
総合解説：ステートレス化できればLB配下の拡張性と障害時切替えが高まりやすい。

問105 利用者ごとに内容が異なる個人情報ページをCDNへキャッシュする場合に最も注意すべき点はどれか。
ア．CDNを使えば個人情報は必ず自動的に匿名化される
イ．HTTPSならキャッシュ設定は一切不要である
ウ．キャッシュキーやCache-Controlを誤ると、他利用者のコンテンツを誤配信するリスクがある
エ．TTLを長くすれば常に安全になる
正答：ウ
4肢解説
ア：そのような保証はない。
イ：TLSとキャッシュ制御は別の問題である。
ウ：正しい。個人化コンテンツでは共有キャッシュの可否とキャッシュキー設計が重要である。
エ：誤キャッシュの影響時間を長くする可能性がある。
総合解説：CDN利用では公開静的コンテンツと個人化・機密コンテンツを分け、キャッシュ条件を明示する。

問106 オンプレミスとクラウド間で安定した大容量通信を常時行い、インターネット経路の変動を避けたい。第一候補として適切な方式はどれか。
ア．必ず公衆Wi-Fiだけを利用する
イ．DNSだけで専用線相当の品質を実現する
ウ．全通信をメール添付で送る
エ．クラウド事業者への専用接続・閉域接続を評価する
正答：エ
4肢解説
ア：大容量・安定通信要件に適さない。
イ：DNSは回線品質を提供しない。
ウ：ネットワーク接続方式ではない。
エ：正しい。専用接続はインターネットVPNより予測可能な帯域・遅延を得やすい。
総合解説：専用接続でも冗長性、暗号化要否、BGP設計、障害時のVPNバックアップ等を検討する。

問107 Webサーバを4台に増やしたが、ロードバランサが1台だけである。可用性上の問題として最も適切なものはどれか。
ア．ロードバランサ自体が単一障害点となる
イ．サーバが4台あれば入口装置の障害は無関係である
ウ．LBが1台なら必ず性能は4倍になる
エ．DNSを使えばLB障害は必ず無視できる
正答：ア
4肢解説
ア：正しい。バックエンドだけ冗長化しても入口となるLBが単一ならサービス全体が停止し得る。
イ：LB停止時には振り分けできない。
ウ：冗長性とも性能とも無関係な断定である。
エ：DNS切替えにも設計・伝播時間が必要で、必ず即時回避できるわけではない。
総合解説：エンドツーエンドの可用性は、LB、DNS、証明書、バックエンド、ネットワークなど全依存点で評価する。

問108 CDNを利用しているが、攻撃者がオリジンサーバの公開IPへ直接大量アクセスできる。改善策として最も適切なものはどれか。
ア．CDNのキャッシュを全て無効化する
イ．オリジンへの直接到達を制限し、CDN経由の通信だけを許可する設計を検討する
ウ．オリジンIPをDNSから消すだけで完全に防げる
エ．HTTPステータスコードを常に200にする
正答：イ
4肢解説
ア：オリジン負荷をさらに高める可能性がある。
イ：正しい。オリジンを直接公開したままだとCDNの防御・キャッシュを迂回される可能性がある。
ウ：IPを直接知られれば到達可能なままである。
エ：アクセス制御にはならない。
総合解説：CDN設計ではオリジンACL、認証、専用ヘッダ、mTLSなどでCDNからの正規アクセスだけを許可する考え方がある。

問109 ピーク時に12,000 requests/sが発生し、1台のバックエンドが安全に処理できるのは2,500 requests/sまでとする。20%の余裕を持たせ、各サーバを最大80%負荷までで運用する場合、最低必要台数はどれか。
ア．4台（実運用上限8,000 requests/s）
イ．5台（実運用上限10,000 requests/s）
ウ．6台（1台2,000 requests/sとして12,000を収容）
エ．8台（最低必要数より多く余裕を持つ）
正答：ウ
4肢解説
ア：4台では実運用上限8,000 requests/sで不足する。
イ：5台では10,000 requests/sで不足する。
ウ：正しい。1台の実運用上限は2,500×0.8=2,000 requests/s。12,000÷2,000=6台である。
エ：余裕は増えるが設問の最低必要台数ではない。
総合解説：LB容量設計では平均負荷だけでなく、障害時N-1、スケール時間、セッション数、TLS処理も考慮する。

問110 日本と欧州の利用者へWebサービスを提供し、片リージョン障害時も継続したい。設計として最も適切なものはどれか。
ア．日本リージョン1か所だけに全機能を集約する
イ．CDNだけ配置し、動的バックエンドは単一リージョンに残す
ウ．全利用者へ固定IPを手動通知して障害時に変更する
エ．複数リージョンへアプリを配置し、グローバルなDNS/LB/CDNで正常なリージョンへ誘導する
正答：エ
4肢解説
ア：リージョン障害時の継続性を満たしにくい。
イ：オリジン障害時の継続性が不足する場合がある。
ウ：切替えが遅く運用負荷も高い。
エ：正しい。地域分散とヘルスチェックを組み合わせることで、遅延改善とリージョン障害耐性を高められる。
総合解説：マルチリージョンではデータ同期、整合性、DNS TTL、ヘルスチェック、フェイルバックまで含めて設計する。

問111 SDNの基本的な考え方として最も適切なものはどれか。
ア．ネットワーク制御機能をデータ転送機能から論理的に分離し、ソフトウェアから集中・自動制御しやすくする
イ．全ルータから制御機能を完全に削除し通信不能にする
ウ．Ethernetケーブルを全て無線へ置換する
エ．DNSサーバをネットワーク制御装置へ変更する
正答：ア
4肢解説
ア：正しい。SDNは制御プレーンとデータプレーンを分離・抽象化し、プログラマブルなネットワーク制御を実現する考え方である。
イ：分離は制御機能をなくすことではない。
ウ：SDNの定義とは無関係である。
エ：DNSとSDNコントローラは別の役割である。
総合解説：SDNではアプリケーション、コントローラ、転送装置間のインタフェースを通じてポリシーと転送を分離して扱う。

問112 NFVの説明として最も適切なものはどれか。
ア．全ネットワーク機能を必ず1台の物理装置に統合する
イ．FWやルータなどのネットワーク機能を専用機器だけに固定せず、汎用仮想化基盤上のソフトウェアとして実行する
ウ．IPアドレスを暗号化する技術である
エ．Wi-Fiのチャネル幅を自動変更するだけの技術である
正答：イ
4肢解説
ア：NFVは専用ハードウェアへの固定を減らす考え方である。
イ：正しい。NFVはネットワーク機能を仮想化し、汎用インフラ上でVNF等として提供する考え方である。
ウ：NFVの目的ではない。
エ：無線チャネル制御に限定されない。
総合解説：NFVではVNF、NFVI、管理・オーケストレーション等を組み合わせ、機能配置や拡張を柔軟にする。

問113 SD-WANの説明として最も適切なものはどれか。
ア．物理回線を必ず1本に集約して冗長性をなくす
イ．メール配送経路だけを制御する
ウ．複数のアンダーレイ回線上に論理的なWANサービスを構成し、アプリケーションやポリシーに応じて経路を制御する
エ．LAN内のSTPだけを置き換える
正答：ウ
4肢解説
ア：SD-WANでは複数回線活用が重要な特徴の一つである。
イ：WAN全体の通信ポリシーを対象とする。
ウ：正しい。SD-WANはインターネットや閉域網など複数アンダーレイを活用し、オーバーレイでポリシー制御する。
エ：SD-WANはWANサービスの制御に関する技術である。
総合解説：SD-WANではアンダーレイ品質の測定、アプリ識別、経路選択、暗号化、集中管理などを組み合わせる。

問114 SDNコントローラを1台だけ配置し、全ネットワークポリシー更新をそのコントローラに依存している。主な設計リスクはどれか。
ア．転送装置が増えるほどコントローラ障害の影響は必ずゼロになる
イ．SDNでは可用性設計が不要である
ウ．コントローラ障害はDNSキャッシュだけに影響する
エ．コントローラが制御プレーンの単一障害点になる可能性がある
正答：エ
4肢解説
ア：依存関係が残るため影響はなくならない。
イ：制御系の冗長性は重要である。
ウ：ネットワーク制御全体へ影響し得る。
エ：正しい。転送継続できる実装もあるが、新規制御や障害時再計算ができなくなる可能性があり、冗長化が必要である。
総合解説：SDN設計ではコントローラクラスタ、状態同期、分散配置、障害時のデータプレーン動作を確認する。

問115 音声通信は低遅延回線、バックアップ通信は低コスト回線へ送りたい。SD-WANで最も直接的に利用する考え方はどれか。
ア．アプリケーション識別と回線品質を基にしたポリシーベース経路選択
イ．全通信を必ず同じ回線へ固定する
ウ．DNSのTTLだけで回線を選択する
エ．MACアドレスの大小だけで回線を決める
正答：ア
4肢解説
ア：正しい。SD-WANはアプリケーションやSLA指標に応じて複数アンダーレイから適切な経路を選択できる。
イ：要件であるアプリ別経路制御を満たさない。
ウ：WAN経路制御の主手段ではない。
エ：アプリケーション品質要件と無関係である。
総合解説：SD-WANでは遅延、ジッタ、損失、帯域等の測定値を経路選択ポリシーへ反映する。

問116 仮想FWのCPU使用率が高くなったため、同一機能のVNFインスタンスを追加しトラフィックを分散する。この方式は何に相当するか。
ア．スケールイン
イ．スケールアウト
ウ．ルート集約
エ．フラグメンテーション
正答：イ
4肢解説
ア：インスタンス数を減らす方向である。
イ：正しい。VNFインスタンス数を増やして処理能力を拡張する方式である。
ウ：経路プレフィックスをまとめる技術でありVNF増設ではない。
エ：パケット分割であり処理ノード増設ではない。
総合解説：NFVでは需要に応じてVNFの追加・削除を自動化しやすいが、状態同期やライセンス、セッション分散も考慮する。

問117 利用者通信をFW、IDS、プロキシの順に通過させるよう、仮想ネットワーク機能を論理的に連結する考え方はどれか。
ア．DNSラウンドロビン
イ．STP
ウ．サービスチェイニング
エ．NTP階層化
正答：ウ
4肢解説
ア：名前解決で複数宛先を返す方式であり機能通過順序の制御ではない。
イ：L2ループ防止プロトコルである。
ウ：正しい。複数のネットワークサービス機能を所定の順序で通過させる構成をサービスチェイニングと呼ぶ。
エ：時刻同期サーバの階層である。
総合解説：仮想環境ではサービスチェインをソフトウェア制御し、テナントやアプリごとに異なる処理経路を適用できる。

問118 工場の画像検査で、判定結果を20ms以内に装置へ返す必要があり、クラウドリージョンまでのRTTが80msある。適切な設計はどれか。
ア．全処理を80ms先のクラウドだけに置く
イ．画像データをメールで送信する
ウ．DNS TTLを短くすればRTTが20ms未満になる
エ．工場内または近傍エッジに推論処理を配置し、クラウドは学習・集約等に利用する
正答：エ
4肢解説
ア：20ms以内という要件を物理的に満たしにくい。
イ：リアルタイム性を満たさない。
ウ：ネットワーク伝搬遅延を解消しない。
エ：正しい。厳しい遅延要件は遠隔クラウドだけでは満たせないため、処理を利用地点へ近づける。
総合解説：エッジ配置は遅延、帯域、データ主権、障害時自律性を改善できる一方、分散運用や更新管理が課題となる。

問119 SD-WANで音声用経路の条件を『遅延50ms以下、損失1%未満』とする。回線Aは遅延30ms・損失2%、回線Bは遅延45ms・損失0.5%である。条件を全て満たす回線はどれか。
ア．回線Bだけ
イ．回線Aだけ
ウ．両方
エ．どちらも満たさない
正答：ア
4肢解説
ア：正しい。Aは損失2%で条件を満たさず、Bは遅延45ms・損失0.5%で両条件を満たす。
イ：Aは損失条件を満たさない。
ウ：Aが損失条件を満たさない。
エ：Bは両条件を満たしている。
総合解説：SD-WANの経路ポリシーでは複数の品質指標をAND/OR条件で評価し、ヒステリシスや切替え頻度も設計する。

問120 VXLAN/EVPNデータセンターで、VTEP間のIP到達性が失われた結果、複数テナントのオーバーレイ通信が同時に停止した。最も適切な説明はどれか。
ア．VXLANは物理ネットワークと完全に独立しているため説明できない
イ．オーバーレイはアンダーレイIPネットワークの到達性に依存するため、アンダーレイ障害が広範囲へ影響した
ウ．EVPNを使うとIPルーティングは不要になる
エ．テナント数が多いと必ずDNS障害が発生する
正答：イ
4肢解説
ア：オーバーレイはアンダーレイを利用してカプセル化パケットを転送する。
イ：正しい。VXLANはIPアンダーレイ上にオーバーレイを構築するため、VTEP間IP到達性が前提となる。
ウ：VTEP間のアンダーレイIP到達性が必要である。
エ：直接関係しない。
総合解説：オーバーレイ設計ではアンダーレイの収束性、ECMP、MTU、障害監視を別レイヤとして設計・監視する。

問121 通常時は1系が処理し、障害時に待機系へ切り替える冗長構成はどれか。
ア．アクティブ・アクティブ
イ．ベストエフォート
ウ．アクティブ・スタンバイ
エ．フルメッシュ
正答：ウ
4肢解説
ア：複数系が通常時から同時に処理する方式である。
イ：通信品質保証の考え方であり冗長構成ではない。
ウ：正しい。主系が稼働し、待機系が障害時に引き継ぐ方式である。
エ：接続トポロジの名称であり主待機方式そのものではない。
総合解説：アクティブ・スタンバイでは障害検知、状態同期、切替え時間、フェイルバック方法を設計する。

問122 複数系を通常時から同時に稼働させるアクティブ・アクティブ構成の利点として最も適切なものはどれか。
ア．状態同期や負荷分散が不要になる
イ．障害検知が不要になる
ウ．単一障害点が必ず完全になくなる
エ．冗長資源を通常時の処理にも活用しやすい
正答：エ
4肢解説
ア：アクティブ・アクティブではむしろ状態整合や分散方式が重要になる。
イ：障害系を分離するため検知は必要である。
ウ：共通電源や制御系など別の単一障害点が残り得る。
エ：正しい。複数系が平常時から処理するため、冗長資源を容量として活用できる。
総合解説：アクティブ・アクティブは資源効率に優れる一方、セッション状態やデータ整合性を含む設計が複雑になりやすい。

問123 同一LANの端末が利用するデフォルトゲートウェイを複数ルータで冗長化する代表的なプロトコルはどれか。
ア．VRRP
イ．SMTP
ウ．VXLAN
エ．NTP
正答：ア
4肢解説
ア：正しい。VRRPは仮想IPアドレスを用いて複数ルータから仮想ルータを構成し、ゲートウェイ冗長化を実現する。
イ：メール配送プロトコルである。
ウ：ネットワーク仮想化オーバーレイ技術でありデフォルトゲートウェイ冗長プロトコルそのものではない。
エ：時刻同期プロトコルである。
総合解説：VRRPの切替えだけでなく、上位ルーティングや回線障害も含めてエンドツーエンドで可用性を確認する。

問124 冗長装置の切替えに30秒かかる原因を調べたところ、実際の設定切替えは2秒で、障害検知に28秒かかっていた。改善対象として最も適切なものはどれか。
ア．設定切替え処理だけを2秒から1秒へ短縮する
イ．障害検知方式と検知タイマー
ウ．DNSゾーン名を変更する
エ．MACアドレスを固定長にする
正答：イ
4肢解説
ア：改善できても全体では1秒しか短縮できない。
イ：正しい。全体の停止時間の大半が障害検知に費やされているため、検知方法・タイマー改善が効果的である。
ウ：障害検知時間とは無関係である。
エ：既に固定長でありフェイルオーバ時間とは無関係である。
総合解説：復旧時間は検知、判断、経路収束、状態同期、ARP/NDP更新、アプリ再接続など複数要素に分解して評価する。

問125 ステートフルファイアウォールを二重化したが、切替え時に既存TCPセッションが全て切断される。改善策として最も適切なものはどれか。
ア．FWのホスト名を同じにするだけ
イ．DNS TTLを延長する
ウ．待機系へセッション状態を同期し、切替え後も必要な状態を引き継げる構成を検討する
エ．全通信をUDPへ変換する
正答：ウ
4肢解説
ア：セッション状態は同期されない。
イ：既存TCPセッションのFW状態を引き継ぐことにはならない。
ウ：正しい。ステートフル装置では接続状態を持つため、状態同期がないと切替え時に既存セッションを認識できない。
エ：アプリ要件を壊す可能性があり、根本的なHA対策ではない。
総合解説：冗長化対象が状態を持つ場合は、セッション、NAT変換、VPN SA、動的ルートなど何を同期する必要があるか確認する。

問126 クラスタ間のハートビートだけが切断され、両ノードが相手を故障と判断して同時にアクティブ化した。これは何と呼ばれる状態か。
ア．ルート集約
イ．マイクロバースト
ウ．ネガティブキャッシュ
エ．スプリットブレイン
正答：エ
4肢解説
ア：複数経路をまとめるルーティング技術である。
イ：短時間の急激なトラフィック増加である。
ウ：DNSの否定応答キャッシュである。
エ：正しい。クラスタの分断により複数ノードが同時に主系として動作する状態である。
総合解説：スプリットブレイン対策には複数経路のハートビート、クォーラム、フェンシングなどを用いる。

問127 ルータを2台、回線を2本にしたが、両方のルータと回線終端装置が同じUPSだけから給電されている。最も重要な改善はどれか。
ア．電源系統を分離し、UPSやPDUを含めて冗長化する
イ．ルータのOSPFコストだけを変更する
ウ．回線のIPアドレスを同じにする
エ．DNSサーバを増やす
正答：ア
4肢解説
ア：正しい。論理・機器が二重でも共通電源障害で同時停止するため、依存資源まで分離する必要がある。
イ：電源単一障害点は解消しない。
ウ：アドレス重複を招き、電源冗長にもならない。
エ：対象の電源障害には直接効果がない。
総合解説：高可用性は装置台数ではなく、電源、回線、経路、制御系、収容場所など全依存関係で評価する。

問128 通常時に3台の装置で合計9Gbit/sを均等処理している。1台故障後も残り2台を各装置の安全上限5Gbit/s以下で運用したい。この構成は要件を満たすか。
ア．満たさない。1台9Gbit/s必要になる
イ．満たす。障害時は1台4.5Gbit/sとなり5Gbit/s以下である
ウ．満たさない。1台6Gbit/sになる
エ．判断できない。通常時の負荷は容量設計に使えない
正答：イ
4肢解説
ア：残り2台で分散できる前提なので1台へ全量集中しない。
イ：正しい。9Gbit/sを2台で分担すると4.5Gbit/s/台となり安全上限内である。
ウ：9÷2は4.5である。
エ：提示条件からN+1時の負荷を計算できる。
総合解説：N+1設計では障害時の残存台数でピーク負荷を処理できるかを確認する。

問129 主回線障害時、拠点ルータはバックアップへ切り替わったが、本社側は旧経路を数十秒保持し、双方向で異なる経路判断が続いた。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．主回線のケーブル色だけを変更する
イ．DNS TTLだけを0にする
ウ．両端の障害検知・経路撤回・収束タイマーを整合させ、過渡状態のループやブラックホールを検証する
エ．全ルータの経路を静的に削除する
正答：ウ
4肢解説
ア：経路収束には影響しない。
イ：IPルーティングの収束問題を解決しない。
ウ：正しい。片側だけ早く切り替わると一時的に非対称・ループ・ブラックホールが起こる場合がある。
エ：通常通信も成立しなくなる。
総合解説：フェイルオーバ設計では定常状態だけでなく、障害検知から全ノード収束までの過渡状態を試験する。

問130 アプリサーバは99.99%、LBは99.99%、単一の外部回線は99.9%の可用性で、サービスには全要素が必要とする。単純化して独立とすると、全体可用性を最も強く制約する要素はどれか。
ア．アプリサーバだけ
イ．LBだけ
ウ．全要素が99.99%以上なので外部回線は無関係
エ．99.9%の外部回線
正答：エ
4肢解説
ア：アプリは高可用でも回線停止時はサービス提供できない。
イ：LBも高可用だが回線の方が低い。
ウ：外部回線は99.9%であり全体に影響する。
エ：正しい。直列依存するサービスでは低可用性要素が全体を強く制約し、他要素だけ高可用でも改善に限界がある。
総合解説：可用性設計は構成要素ごとの数字ではなく、依存関係を含むサービス全体で評価する。

問131 DR設計でRTOとRPOの説明として最も適切なものはどれか。
ア．RTOは復旧までの目標時間、RPOはどの時点までのデータを復旧するかという目標である
イ．RTOはIPアドレス数、RPOは回線帯域を表す
ウ．RTOとRPOは常に同じ値でなければならない
エ．RPOは障害検知時間だけを表す
正答：ア
4肢解説
ア：正しい。RTOはサービス復旧に許容される時間、RPOは許容可能なデータ損失時間幅を表す。
イ：どちらも復旧要件の指標でありネットワーク容量そのものではない。
ウ：業務要件により異なる値を設定できる。
エ：データ復旧時点に関する指標である。
総合解説：DR方式はRTO・RPO、コスト、データ整合性、復旧手順を基に選定する。

問132 ルータやスイッチの設定ファイルを定期的にバックアップする主な目的はどれか。
ア．帯域を自動的に増やすため
イ．誤設定や故障で設定が失われた際に、既知の正常状態へ復元できるようにする
ウ．全通信を暗号化するため
エ．IPアドレスを使わなくするため
正答：イ
4肢解説
ア：バックアップは回線容量を増加させない。
イ：正しい。設定バックアップは障害・誤操作・装置交換時の迅速な復旧に役立つ。
ウ：暗号化機能とは別である。
エ：復旧目的の設定保存である。
総合解説：設定バックアップでは保存頻度、世代管理、暗号化、アクセス権、装置OSとの互換性も考慮する。

問133 災害時に短時間で業務を再開するため、平常時から必要な設備やシステムを稼働状態に近く維持する代替サイトは一般にどれか。
ア．コールドサイト
イ．紙の設計書だけ
ウ．ホットサイト
エ．DNSキャッシュサイト
正答：ウ
4肢解説
ア：場所や最低限の設備はあるが、システム準備に時間を要する。
イ：代替サイトそのものではない。
ウ：正しい。ホットサイトは必要設備・システムを事前に準備し、短いRTOを実現しやすい。
エ：DRサイトの分類ではない。
総合解説：代替サイトは復旧速度とコストのトレードオフで選定し、ネットワーク接続とデータ同期も含めて設計する。

問134 大規模災害やランサムウェアを考慮したバックアップ保護として、最も適切な考え方はどれか。
ア．本番装置の同じディスク内に1コピーだけ置く
イ．バックアップは一度作れば更新不要である
ウ．全バックアップを誰でも削除可能にする
エ．複数コピーを異なる媒体・場所に保持し、オンライン環境から分離されたコピーも確保する
正答：エ
4肢解説
ア：装置故障や侵害時に同時喪失する可能性が高い。
イ：データ・設定変更に追随できない。
ウ：誤操作・攻撃リスクを高める。
エ：正しい。単一場所・単一媒体だけでは同時被災や侵害で全コピーを失う可能性がある。
総合解説：バックアップは複数世代・異なる障害ドメイン・アクセス分離を組み合わせ、復旧テストまで実施する。

問135 遠隔DRサイトへデータを複製する際、アプリケーション書込み完了前に遠隔側への反映完了も確認する方式の特徴はどれか。
ア．同期レプリケーションで、RPOを小さくしやすいが遅延の影響を受けやすい
イ．非同期レプリケーションで、距離が長いほど必ず書込み遅延がゼロになる
ウ．バックアップを一切取らなくてよい方式である
エ．DNSのゾーン転送方式である
正答：ア
4肢解説
ア：正しい。同期方式は両拠点への反映を待つためデータ損失を抑えやすいが、距離・RTTが性能へ影響する。
イ：設問の動作は同期方式である。
ウ：レプリケーションだけでは論理破損や誤削除にも同時追随する場合があり、バックアップは別途重要である。
エ：データストレージのレプリケーションとは異なる。
総合解説：同期・非同期の選択はRPO、距離、回線品質、アプリ性能、コストを基に決める。

問136 バックアップジョブが毎日『成功』と記録されている。DRの確実性を高めるために追加で最も重要な活動はどれか。
ア．成功ログだけを永久保存し復元は一度もしない
イ．定期的に実データを復元し、復旧手順とデータ整合性を確認する
ウ．バックアップ媒体を毎回破棄する
エ．DNS TTLだけを短くする
正答：イ
4肢解説
ア：実際の復旧可能性を確認できない。
イ：正しい。バックアップ成功ログだけでは実際に復元可能か保証できないため、リストア試験が必要である。
ウ：復旧データを失う。
エ：バックアップ復元可否とは無関係である。
総合解説：DRではバックアップ取得だけでなく、復元時間、依存関係、手順、担当者の習熟までテストする。

問137 本番サイト障害時にDRサイトへWebサービスを切り替える。DNSで利用者を新サイトへ誘導する設計で、切替え時間へ影響する要素として重要なものはどれか。
ア．Ethernet FCSの長さ
イ．CPUの型番だけ
ウ．DNS TTLとキャッシュの残存時間
エ．VLAN名の文字数
正答：ウ
4肢解説
ア：DNS切替え時間とは関係しない。
イ：DNSキャッシュ伝播の主要因ではない。
ウ：正しい。TTLが長いと旧アドレスが利用者側に残り、切替え反映に時間がかかる可能性がある。
エ：切替え時間には影響しない。
総合解説：DNS切替えを利用する場合は平常時TTL、障害時運用、ヘルスチェック、フェイルバックまで事前設計する。

問138 RPOを30分以内とするシステムで、障害時に最後のバックアップ時点までしか復旧できない。単純化した場合、バックアップ間隔の上限として適切なものはどれか。
ア．24時間
イ．12時間
ウ．60分
エ．30分以下
正答：エ
4肢解説
ア：最大24時間分失う可能性がありRPOを満たさない。
イ：同様にRPOより大幅に長い。
ウ：最悪60分分の損失となり30分要件を超える。
エ：正しい。最悪時のデータ損失時間を30分以内にするには、バックアップ間隔も30分以下が必要である。
総合解説：実際にはバックアップ完了時間、ログ転送、障害検知時点も考慮して余裕を持って設計する。

問139 本番サイトでは通常10Gbit/sのピークトラフィックを処理するが、DRサイトの外部回線は2Gbit/sしかない。RTO内に切替えは可能でも、切替え後に何を確認すべきか。
ア．DRサイトで業務に必要なトラフィックを処理できる容量があるか、縮退運転条件を含め再評価する
イ．RTOを満たせばDR回線容量は無関係である
ウ．DNSを切り替えれば物理帯域が自動的に10Gbit/sになる
エ．バックアップデータ量だけ見ればよい
正答：ア
4肢解説
ア：正しい。起動できても必要帯域を満たせなければサービス品質を維持できない。
イ：復旧後のサービス提供能力も必要である。
ウ：DNSは回線容量を増やさない。
エ：利用者トラフィックや運用通信も含める必要がある。
総合解説：DR設計ではコンピュート・ストレージだけでなくWAN、インターネット出口、VPN、DNS、認証などネットワーク容量も確認する。

問140 本番データベースで誤削除が発生し、その変更が即座にDRサイトへ同期レプリケーションされた。データを削除前へ戻すために必要な対策として最も適切なものはどれか。
ア．同期レプリケーションがあれば過去状態も必ず自動保存される
イ．レプリケーションとは別に、世代管理されたバックアップやスナップショットから復元する
ウ．DRサイトのIPアドレスを変更すれば削除データが戻る
エ．DNSキャッシュを消せば削除が取り消される
正答：イ
4肢解説
ア：レプリケーションと世代バックアップは別機能である。
イ：正しい。レプリケーションは誤削除や論理破損も複製してしまうため、過去時点へ戻すバックアップが必要である。
ウ：データ復旧にはならない。
エ：データ内容とは無関係である。
総合解説：可用性のためのレプリケーションと、論理破損・誤操作から戻すバックアップは目的が異なるため両方を設計する。

問141 全拠点を一夜で切り替えず、少数拠点から順番に新ネットワークへ移行する方式の主な利点はどれか。
ア．移行期間中の新旧併存設計が不要になる
イ．全拠点の障害が必ず同時に発生する
ウ．初期段階で問題を発見し、後続拠点へ反映して影響範囲を抑えられる
エ．ロールバック計画が不要になる
正答：ウ
4肢解説
ア：段階移行ではむしろ併存期間の接続・運用が必要になる。
イ：一括移行より同時影響を抑えやすい。
ウ：正しい。段階移行は一度に影響する範囲を限定し、実運用で得た知見を後続へ反映できる。
エ：各段階で戻し条件を準備すべきである。
総合解説：段階移行では移行単位、順序、依存関係、併存通信、成功判定、ロールバックを事前に定義する。

問142 ネットワーク切替え作業でロールバック手順を事前に作成する主な目的はどれか。
ア．新構成の設定を削除して記録を残さないため
イ．切替え判定を担当者の感覚だけに任せるため
ウ．全障害を未然に完全排除できるため
エ．重大な問題が発生した場合に、許容時間内で旧構成へ安全に戻せるようにする
正答：エ
4肢解説
ア：原因分析や再実施に必要な情報を失う。
イ：客観的な戻し基準が必要である。
ウ：ロールバックは障害をゼロにする仕組みではない。
エ：正しい。切替え失敗時の復旧方法を事前に具体化しておくことで停止時間と判断の迷いを減らす。
総合解説：ロールバックには開始条件、判断責任者、旧設定・旧配線の復元方法、所要時間、確認項目を含める。

問143 詳細設計レビューを複数の担当者で行う主な目的として最も適切なものはどれか。
ア．要件との不整合、単一障害点、容量不足、設定上の矛盾などを実装前に検出する
イ．設計書の文字数だけを増やす
ウ．実装後の障害を記録しないようにする
エ．全ての設計判断を一人の担当者だけに集中させる
正答：ア
4肢解説
ア：正しい。レビューは設計品質を第三者視点で確認し、後工程での高コストな手戻りを減らす。
イ：レビューの目的ではない。
ウ：むしろリスクを事前検出する活動である。
エ：複数視点による検証の利点を失う。
総合解説：レビューでは要件トレーサビリティ、障害時動作、セキュリティ、運用、移行性も確認する。

問144 新しいSD-WANを全国100拠点へ導入する前に、業務影響が比較的小さい3拠点で実環境検証したい。この方法はどれか。
ア．ビッグバン移行
イ．パイロット移行
ウ．コールドバックアップ
エ．DNSラウンドロビン
正答：イ
4肢解説
ア：全対象を短期間に一括切替えする方式である。
イ：正しい。代表的な少数拠点で先行導入し、技術・運用上の問題を検証する方式である。
ウ：移行方式ではなくバックアップ・待機構成の考え方である。
エ：名前解決による分散方式である。
総合解説：パイロット対象は本番を代表する通信パターンを持ちつつ、問題時の影響を許容できる範囲から選定する。

問145 大規模切替え直前の数日間、緊急修正を除いて旧ネットワークの設定変更を停止する主な理由はどれか。
ア．ネットワーク監視も全て停止するため
イ．障害対応を禁止するため
ウ．移行用設計・設定と現行環境の差分が増えるのを防ぎ、切替え条件を安定させるため
エ．DNSを永久停止するため
正答：ウ
4肢解説
ア：監視は切替え前後でむしろ重要である。
イ：緊急変更の例外手順は必要である。
ウ：正しい。直前変更が続くと移行手順やバックアップ設定が実環境と一致しなくなる。
エ：変更凍結の目的ではない。
総合解説：変更凍結期間、例外承認、差分反映方法を決め、構成情報を移行直前に再確認する。

問146 新回線へ切替え後、pingが成功したため作業完了と判断しようとしている。より適切な確認はどれか。
ア．pingが1回成功すれば全要件を満たしたとみなす
イ．監視アラームは作業完了後も確認しない
ウ．旧回線を確認前に即時解約する
エ．業務通信、冗長切替え、性能、名前解決、監視、セキュリティなど要件に対応した受入れ項目を確認する
正答：エ
4肢解説
ア：確認範囲が不十分である。
イ：移行後の異常検知に必要である。
ウ：問題発生時のロールバック手段を失う可能性がある。
エ：正しい。ICMP疎通だけではアプリケーションや障害時動作が要件を満たすか確認できない。
総合解説：移行後確認は事前にテストケースと合否基準を定め、業務部門の確認も含める。

問147 段階移行中、新ネットワークへ移った拠点と旧ネットワーク側のサーバが相互通信する必要がある。最も重要な設計事項はどれか。
ア．新旧間の経路交換、アドレス重複、戻り経路、セキュリティポリシーを明確にする
イ．新旧ネットワークは接続せず通信要件を無視する
ウ．片方向のルートだけあればTCP通信は常に成立する
エ．DNS名が同じなら経路設計は不要である
正答：ア
4肢解説
ア：正しい。併存期間は経路非対称や重複、FWルール漏れなどが起こりやすいため事前設計が必要である。
イ：業務要件を満たさない。
ウ：戻り経路も必要である。
エ：名前解決とIP到達性は別である。
総合解説：移行期間は一時構成が本番構成より複雑になることがあり、その撤去条件も含めて文書化する。

問148 1拠点の切替えに平均20分、確認に10分必要で、同時作業はできない。作業可能時間が6時間の場合、余裕時間を考慮しない最大移行拠点数は幾つか。
ア．6拠点（1拠点60分として計算）
イ．12拠点（1拠点30分として360÷30）
ウ．18拠点（切替20分だけで360÷20）
エ．30拠点（作業時間条件と整合しない）
正答：イ
4肢解説
ア：1拠点60分として計算している。
イ：正しい。1拠点30分、6時間=360分なので360÷30=12拠点である。
ウ：切替え20分だけで計算し確認時間を含めていない。
エ：作業時間との整合がない。
総合解説：実作業では休憩、障害対応、承認待ち、ロールバック余裕を含め、理論最大より少なく計画する。

問149 冗長回線設計のレビューで、正常時の構成図と帯域だけが確認されている。追加で最も重要なレビューはどれか。
ア．正常時に疎通できれば障害時レビューは不要である
イ．構成図の色だけを統一する
ウ．回線・装置・電源などを一つずつ故障させた場合の経路、残存容量、収束時間をシナリオごとに確認する
エ．障害時は必ず手動対応するとだけ記載する
正答：ウ
4肢解説
ア：冗長構成の目的を確認できない。
イ：設計品質の本質的確認ではない。
ウ：正しい。高可用性設計は正常時だけではなく、想定故障時に要件を満たすかで評価する必要がある。
エ：具体的な経路・容量・時間の検証が必要である。
総合解説：設計レビューではN-1、共通障害点、フェイルオーバ、復旧・フェイルバックまでシナリオ試験する。

問150 大規模ネットワーク移行で、旧環境へ戻すには2時間必要、業務開始まで残り3時間である。新環境の重大問題調査に既に1時間使った。次の判断として最も適切なものはどれか。
ア．原因が分かるまで無期限に調査を続ける
イ．旧環境の設定を先に削除する
ウ．重大問題があっても必ず新環境で業務開始する
エ．ロールバック完了に必要な時間を考慮し、事前に定めた最終判断時刻に達しているなら戻しを開始する
正答：エ
4肢解説
ア：ロールバック時間を失い、業務開始時刻を超える可能性がある。
イ：戻し手段を失う。
ウ：業務影響と事前基準を無視している。
エ：正しい。復旧可能な時間を使い切ってから判断すると業務開始に間に合わないため、point of no returnを事前設定する。
総合解説：移行計画では切替え開始時刻だけでなく、ロールバック開始の最終時刻と判断責任者を明確にする。