問1 新しいL3スイッチをラックへ搭載する前に確認すべき事項として、最も適切なものはどれか。
ア．ラック寸法・搭載位置・重量・電源容量・吸排気方向を確認する
イ．IPアドレスだけ決めれば物理実装条件は確認不要である
ウ．ラック内温度は機器動作と無関係である
エ．電源系統は全機器を1本へ集約するほど可用性が高い
正答：ア
4肢解説
ア：正しい。機器の物理寸法だけでなく、重量、電源、冷却、保守空間まで確認して実装する必要がある。
イ：物理条件を満たさなければ安全に搭載・運用できない。
ウ：温度・排熱は信頼性に影響する。
エ：単一障害点を作りやすい。
総合解説：物理構築ではラック、電源、冷却、重量、ケーブル動線、保守性を一体で設計する。

問2 建物間を数百m離して10GbEで接続し、雷サージや電位差の影響も避けたい。媒体として最も適切な候補はどれか。
ア．短距離用の銅ツイストペアだけ
イ．光ファイバ
ウ．電源ケーブル
エ．同軸TVケーブルを必ず使用する
正答：イ
4肢解説
ア：数百mの建物間用途では距離・電気的影響の面で不利である。
イ：正しい。光ファイバは電気的に絶縁され、長距離・高速伝送に向く。
ウ：データ通信用媒体ではない。
エ：一般的な10GbE建物間接続の第一候補ではない。
総合解説：媒体選定では距離、帯域、EMI、雷・接地、コスト、既設配線を比較する。

問3 PoEで、Ethernetケーブルを通じて電力を供給する側の装置を何と呼ぶか。
ア．PD
イ．VTEP
ウ．PSE
エ．PEP
正答：ウ
4肢解説
ア：Powered Deviceは受電側である。
イ：VXLAN Tunnel EndpointでありPoE給電装置ではない。
ウ：正しい。Power Sourcing Equipmentが給電側、Powered Deviceが受電側である。
エ：Policy Enforcement PointでありPoEとは無関係である。
総合解説：PoE設計ではPSEの総電力予算と各PDの必要電力を確認する。

問4 両端に同じコネクタ形状の光モジュールを挿したがリンクアップしない。まず確認すべき項目として最も適切なものはどれか。
ア．装置のホスト名が同じか
イ．DNSサフィックスが一致するか
ウ．NTP時刻が同じか
エ．波長・伝送規格・ファイバ種別・送受信レベルが両端で適合しているか
正答：エ
4肢解説
ア：リンク層の成立条件ではない。
イ：物理リンク確立には関係しない。
ウ：光リンクアップには不要である。
エ：正しい。コネクタ形状が同じでも波長やSMF/MMF、規格が不一致なら通信できない。
総合解説：光リンク障害ではTx/Rx波長、SMF/MMF、極性、光レベル、モジュール互換性を確認する。

問5 送信光出力が-2dBm、受信感度が-14dBmの光リンクで、設計上許容できる総損失の最大値はいくつか。
ア．12dB（-2dBm-(-14dBm)の差分）
イ．16dB（送受信値の差分計算を誤る）
ウ．7dB（与えられた値から直接導けない）
エ．-12dB（損失予算を負の値として扱う）
正答：ア
4肢解説
ア：正しい。-2 - (-14)=12dBが理論上の光パワーバジェットである。
イ：差分計算が誤っている。
ウ：与えられた値から算出されない。
エ：損失予算は正の差分として扱う。
総合解説：実設計ではコネクタ・融着・ファイバ損失に加え、経年変化や保守余裕も見込む。

問6 PoEスイッチの利用可能な給電予算が740Wで、AP1台当たり最大30Wを確保する。余裕を無視した場合、同時に給電できる最大AP台数は何台か。
ア．20台（600W分だけ利用するとみなす）
イ．24台（740÷30の整数部で判断）
ウ．25台（必要750Wとなり予算超過）
エ．30台（必要900Wとなり予算超過）
正答：イ
4肢解説
ア：必要以上に少ない。
イ：正しい。740÷30=24余り20なので最大24台である。
ウ：25×30=750Wで予算を超える。
エ：900W必要となり予算を超える。
総合解説：PoE設計では最大消費電力だけでなく電源冗長時の残存予算も確認する。

問7 数百本のパッチコードがあるラックで、両端ラベルと配線台帳を整備する最大の利点はどれか。
ア．Ethernet速度が自動的に2倍になる
イ．IPアドレスが自動配布される
ウ．障害切り分けや変更作業で対象回線を迅速かつ正確に特定できる
エ．暗号化が自動有効になる
正答：ウ
4肢解説
ア：ラベルは物理速度を変えない。
イ：DHCPの機能である。
ウ：正しい。誤抜去・誤接続を減らし、復旧と変更の時間を短縮できる。
エ：ラベル管理とは無関係である。
総合解説：物理構成情報も構成管理の一部として記録し、変更時に同期更新する。

問8 冗長化した2台のコアスイッチを同じラック・同じPDU・同じUPSだけに接続している。改善として最も適切なものはどれか。
ア．2台あるので物理分離は不要である
イ．両機器の管理IPを同じにする
ウ．同じ電源タップへさらに集約する
エ．可能な範囲でラック・PDU・UPS・電源系統を分離し、共通障害点を減らす
正答：エ
4肢解説
ア：共通障害点が残る。
イ：IP競合を起こす。
ウ：可用性を改善しない。
エ：正しい。装置を二重化しても電源や設置場所を共有すると共通原因障害に弱い。
総合解説：高可用性の物理構成では装置だけでなく電源、ラック、配線経路も分離する。

問9 通常-5dBmだった受信光レベルが徐々に-12dBmへ低下し、受信感度限界が-13dBmでCRCエラーも増加している。最も適切な対応はどれか。
ア．コネクタ汚損・曲げ・融着点・ファイバ劣化など光路損失増加を調査する
イ．OSPFコストを変更する
ウ．DNSキャッシュを削除する
エ．VLAN IDを変更する
正答：ア
4肢解説
ア：正しい。受信感度限界へ近づく光レベル悪化とエラー増加は物理光路の劣化を疑う。
イ：物理光損失を改善しない。
ウ：光レベルとは無関係である。
エ：物理受信レベルには影響しない。
総合解説：光リンクはリンクアップ/ダウンだけでなくDOM等の光レベル推移を監視すると予兆保全に役立つ。

問10 2本の建物間光回線を別ポートへ接続しているが、同じ地下管路を通っている。掘削事故への耐性を高める最も有効な改善はどれか。
ア．VLANを別番号にする
イ．物理的に異なる管路・引込経路へ分離する
ウ．両回線の帯域を同じにする
エ．同じケーブル束へまとめ直す
正答：イ
4肢解説
ア：物理断への耐性は上がらない。
イ：正しい。同じ管路を共有すると1回の切断事故で両回線が同時に失われる。
ウ：共通経路障害を解消しない。
エ：共通障害点を増やす。
総合解説：論理冗長だけでなく物理ルート多様化を確認することが重要である。

問11 新規ネットワーク機器の本番投入前に最優先で行うべき初期設定として適切なものはどれか。
ア．工場出荷時パスワードを全機器で使い続ける
イ．Telnetだけをインターネットへ公開する
ウ．初期認証情報を変更し、不要サービスを停止して管理アクセスを制限する
エ．管理ACLを全許可にする
正答：ウ
4肢解説
ア：侵害リスクが高い。
イ：平文管理かつ露出が大きい。
ウ：正しい。デフォルト資格情報や不要な管理サービスを残したまま本番接続すべきではない。
エ：不要な管理アクセスを許す。
総合解説：初期構築では安全な管理面、時刻、ログ、バックアップも標準化する。

問12 ルータ、FW、サーバでNTPを統一的に設定する重要な理由はどれか。
ア．リンク帯域が自動増加するため
イ．MACアドレスが重複しなくなるため
ウ．VLANが自動作成されるため
エ．ログの時系列相関や認証・証明書等の時刻依存処理を正しく行うため
正答：エ
4肢解説
ア：NTPは帯域を増やさない。
イ：時刻同期とは無関係である。
ウ：NTPの機能ではない。
エ：正しい。時刻同期は障害・セキュリティ調査の基盤となる。
総合解説：本番導入では信頼できる時刻源、冗長化、タイムゾーンも管理する。

問13 新しい社内DNSサーバへ切り替える際、最低限確認すべき内容として最も適切なものはどれか。
ア．正引き・逆引き・権威情報・再帰設定・上位/下位参照先が設計どおりか確認する
イ．DNSサーバの画面解像度だけ確認する
ウ．全クライアントのMACアドレスをDNSへ登録する
エ．OSPFのRouter IDだけ確認する
正答：ア
4肢解説
ア：正しい。DNSは役割ごとに名前解決経路を確認する必要がある。
イ：サービス機能とは無関係である。
ウ：通常のDNS導入要件ではない。
エ：DNS機能確認ではない。
総合解説：DNS切替えではTTL、キャッシュ残存、冗長系、ACLも含めて確認する。

問14 スイッチ間リンクでVLAN10だけ疎通できず、VLAN20は正常である。最初に確認すべき設定として最も適切なものはどれか。
ア．両端装置のホスト名が一致しているか
イ．両端トランクでVLAN10が許可され、タグ設定が一致しているか
ウ．DNSのMXレコード
エ．NTP stratum
正答：イ
4肢解説
ア：VLAN転送条件ではない。
イ：正しい。特定VLANだけの障害ならトランク許可VLANやタグ不整合を疑う。
ウ：L2 VLAN疎通とは無関係である。
エ：VLAN転送には関係しない。
総合解説：サービス導入時は設定差分をレイヤごとに切り分ける。

問15 直結した2台のルータでOSPF隣接関係が成立しない。まず比較すべき設定の組合せとして適切なものはどれか。
ア．DNSゾーン名とNTP stratumだけ
イ．筐体色とラック番号
ウ．エリア、Hello/Deadタイマー、認証、ネットワーク種別など
エ．HTTP User-Agent
正答：ウ
4肢解説
ア：OSPF隣接条件ではない。
イ：ルーティングプロトコルには影響しない。
ウ：正しい。OSPF隣接には複数のパラメータ整合が必要である。
エ：OSPFとは無関係である。
総合解説：OSPF導入ではインタフェースIP/MTUや隣接状態ログも併せて確認する。

問16 DHCPサーバとクライアントが異なるIPサブネットにあり、ルータ越しにアドレス配布したい。必要な機能はどれか。
ア．STPルートガード
イ．DNSSEC
ウ．VRRPだけ
エ．DHCPリレー
正答：エ
4肢解説
ア：L2ループ対策である。
イ：DNS真正性保護である。
ウ：ゲートウェイ冗長化でありDHCP中継ではない。
エ：正しい。DHCPブロードキャストを別サブネットのサーバへ中継する。
総合解説：DHCPリレー設定では中継先、giaddr/relay情報、ACL、冗長サーバを確認する。

問17 FWルール変更を本番適用する際、作業前後で最も有効な確認はどれか。
ア．事前に現行設定と状態を保存し、適用後に差分と疎通・ログを確認する
イ．作業前設定を保存せず直接変更する
ウ．適用後は確認せず終了する
エ．全ルールを一度削除して再作成する
正答：ア
4肢解説
ア：正しい。意図した変更だけが入ったかを検証でき、戻しにも利用できる。
イ：ロールバック困難になる。
ウ：設定ミスを見逃す。
エ：不要な停止リスクが高い。
総合解説：変更作業ではpre-check、変更、post-check、戻し条件を手順化する。

問18 既存サーバへ新しい監視サービスを導入したところ起動に失敗し、『TCP/443 address already in use』と表示された。最も適切な原因はどれか。
ア．DNS TTLが長すぎる
イ．既存プロセスが同じIP/ポートで待受けており競合している
ウ．OSPF隣接が多すぎる
エ．光受信レベルが高すぎる
正答：イ
4肢解説
ア：bind失敗の直接原因ではない。
イ：正しい。同一IPアドレスと同一TCPポートを複数プロセスが通常同時にbindできない。
ウ：ローカルTCPポート競合とは無関係である。
エ：アプリ待受けポートとは無関係である。
総合解説：サービス統合前にはポート、依存ライブラリ、証明書、権限、資源競合を確認する。

問19 全国200拠点へ同じルータ設定を投入する。誤設定による全社障害を避ける最も適切な方法はどれか。
ア．200拠点へ同時に無確認で投入する
イ．設定バックアップを取らず投入する
ウ．検証環境と少数パイロット拠点で確認後、段階的に展開し停止条件を設ける
エ．失敗しても展開を自動継続する
正答：ウ
4肢解説
ア：誤設定時の影響が最大化する。
イ：復旧が困難になる。
ウ：正しい。blast radiusを限定し、問題を早期検出できる。
エ：被害を拡大する。
総合解説：大規模導入では段階展開、canary、監視、停止条件、ロールバックを組み合わせる。

問20 冗長FWの主系だけに新しい許可ルールを設定したところ、フェイルオーバ後に通信不能となった。再発防止として最も適切なものはどれか。
ア．主系だけ設定すれば待機系は常に自動同一になると仮定する
イ．フェイルオーバ試験を行わない
ウ．待機系の設定を毎回初期化する
エ．冗長ペアの設定同期状態を管理し、切替え試験で同一ポリシー適用を確認する
正答：エ
4肢解説
ア：製品・状態により保証されない。
イ：差異を発見できない。
ウ：可用性を損なう。
エ：正しい。主待機間の構成差異は切替え時障害の典型要因である。
総合解説：HA機器では設定・状態同期の対象範囲を明確にし、実切替えで検証する。

問21 NETCONFの主な用途として最も適切なものはどれか。
ア．ネットワーク機器の構成データを取得・変更・削除する標準化された管理プロトコル
イ．パケットをL2で転送するプロトコル
ウ．時刻同期専用プロトコル
エ．DNS名前解決専用プロトコル
正答：ア
4肢解説
ア：正しい。NETCONFはRPCを用いて構成データストアを操作する。
イ：スイッチング機能ではない。
ウ：NTPの役割である。
エ：DNSとは異なる。
総合解説：NETCONFはYANGデータモデルと組み合わせて構造化された構成管理に利用される。

問22 YANGの説明として最も適切なものはどれか。
ア．暗号アルゴリズム
イ．ネットワーク構成や状態データの構造・型・制約を記述するデータモデリング言語
ウ．L2ループ防止プロトコル
エ．ログ転送プロトコル
正答：イ
4肢解説
ア：データモデル言語である。
イ：正しい。YANGはNETCONF/RESTCONF等で扱うデータをモデル化する。
ウ：STPとは異なる。
エ：syslogとは異なる。
総合解説：モデル駆動管理ではCLI文字列ではなく構造化データとして設定を扱いやすい。

問23 設定管理における構成ベースラインとは何か。
ア．障害時に毎回ランダム生成する設定
イ．全機器の初期パスワード一覧
ウ．承認済みの基準構成として管理され、変更比較の基点となる状態
エ．帯域利用率の最大値だけ
正答：ウ
4肢解説
ア：基準構成ではない。
イ：ベースラインの一部情報になり得るが定義そのものではない。
ウ：正しい。標準状態からの差分を検知・承認する基準になる。
エ：構成状態の基準ではない。
総合解説：構成管理ではベースライン、変更承認、差分監視を一貫して運用する。

問24 NETCONF対応機器で、本番running設定へ直ちに反映せず変更案を編集し、確認後に一括反映したい。利用できる代表的な機能はどれか。
ア．runningへ1行ずつ直接反映するだけ
イ．DNSキャッシュへ設定を保存する
ウ．ARPテーブルへ設定案を保存する
エ．candidate datastoreを編集してcommitする
正答：エ
4肢解説
ア：candidate利用の説明ではない。
イ：NETCONF構成データストアではない。
ウ：構成管理用途ではない。
エ：正しい。candidate対応機器では変更を候補設定へ蓄積してからrunningへcommitできる。
総合解説：candidateは複数変更を一つのトランザクションとして適用しやすい。

問25 遠隔ルータの管理ACL変更で、自分自身の管理接続を誤って遮断するリスクを減らしたい。NETCONFの代表的な安全機能はどれか。
ア．confirmed commitを使い、確認がない場合は自動的に元設定へ戻す
イ．変更後に必ず手動電源断する
ウ．running設定を保存せず上書きする
エ．DNS TTLを短くする
正答：ア
4肢解説
ア：正しい。到達不能になって確認できなければタイムアウト後にロールバックできる。
イ：安全な構成変更機能ではない。
ウ：復旧性を下げる。
エ：管理ACL変更の安全性とは無関係である。
総合解説：遠隔自動化ではrollbackやconfirmed commitなど失敗時安全性が重要である。

問26 YANGで定義された設定・状態データをHTTPベースのRESTfulインタフェースで操作したい。適したプロトコルはどれか。
ア．SNMP Trap
イ．RESTCONF
ウ．OSPF
エ．NTP
正答：イ
4肢解説
ア：イベント通知でありREST APIではない。
イ：正しい。RESTCONFはHTTPを用いてYANGデータへアクセスする。
ウ：ルーティングプロトコルである。
エ：時刻同期プロトコルである。
総合解説：NETCONFとRESTCONFはどちらもモデル駆動管理に利用されるが、操作・トランスポート形態が異なる。

問27 構成自動化で『同じ処理を何度実行しても、目標状態が同じなら追加変更が発生しない』性質を何と呼ぶか。
ア．可逆圧縮
イ．前方秘匿性
ウ．冪等性
エ．経路集約
正答：ウ
4肢解説
ア：データ圧縮の性質である。
イ：暗号鍵漏えいと過去通信保護に関する性質である。
ウ：正しい。宣言的な構成管理で重要な性質で、再実行を安全にしやすい。
エ：ルーティングの概念である。
総合解説：自動化処理は現状を確認し必要差分だけ適用する設計が望ましい。

問28 自動化スクリプトのGitリポジトリに管理者パスワードを平文で埋め込んでいる。改善として最も適切なものはどれか。
ア．パスワードをコメント行へ移す
イ．リポジトリ名を秘密にするだけ
ウ．全機器で同じパスワードを使う
エ．秘密情報管理基盤や暗号化済み変数を利用し、コードから資格情報を分離する
正答：エ
4肢解説
ア：平文秘密である点は変わらない。
イ：アクセス漏えい時に資格情報が露出する。
ウ：漏えい時の影響を拡大する。
エ：正しい。ソースコードの共有・履歴から秘密が漏れるのを防ぐ必要がある。
総合解説：自動化では秘密の保管・配布・ローテーション・監査を別ライフサイクルで管理する。

問29 自動化で標準設定を配布した後、一部機器だけ手作業変更が入り、数週間後に標準との差異が拡大した。最も適切な対策はどれか。
ア．定期的に実機状態と承認済みベースラインを比較し、差分を検知・承認または修正する
イ．一度配布したら実機設定を二度と確認しない
ウ．手作業変更を全て無記録で許可する
エ．標準設定ファイルを削除する
正答：ア
4肢解説
ア：正しい。意図しない構成ドリフトを継続監視する。
イ：ドリフトを検知できない。
ウ：構成の正当性を追跡できない。
エ：比較基準を失う。
総合解説：構成自動化と構成監視を組み合わせることで、desired stateを維持しやすくなる。

問30 自動化ツールのテンプレート誤りで、全500台のルータからBGP設定を削除する危険がある。最も適切な安全策の組合せはどれか。
ア．変更内容を表示せず全台へ一括投入する
イ．構文/差分検証、少数canary、段階展開、停止条件、ロールバックを組み合わせる
ウ．失敗検知後も最後まで自動継続する
エ．バックアップを削除してから開始する
正答：イ
4肢解説
ア：影響が最大化する。
イ：正しい。大規模自動化では誤りの影響範囲を限定する仕組みが不可欠である。
ウ：障害を拡大する。
エ：復旧手段を失う。
総合解説：自動化の速度は利点だが、同じ速度で誤設定も拡散するため安全装置が重要である。

問31 ネットワークテスト計画に含める内容として最も適切なものはどれか。
ア．担当者の経験に任せて手順と合否基準は書かない
イ．成功するケースだけを列挙する
ウ．対象範囲、目的、前提条件、手順、期待結果、合否基準、担当者、実施時期を定める
エ．実施後に初めて期待結果を決める
正答：ウ
4肢解説
ア：結果の再現性・客観性が低下する。
イ：異常系・境界条件を確認できない。
ウ：正しい。再現可能で客観的なテストには対象と判定基準の明確化が必要である。
エ：結果に合わせた恣意的判定になり得る。
総合解説：テスト計画は要求仕様から検証項目を導き、第三者でも実施・判定できる粒度にする。

問32 FWの接続テストで『許可すべき通信が通る』だけでなく確認すべき異常系として適切なものはどれか。
ア．許可通信だけを何度も繰り返す
イ．FWの筐体色を確認する
ウ．DNS TTLだけを測る
エ．禁止対象の送信元・宛先・ポートが確実に拒否されること
正答：エ
4肢解説
ア：拒否ルールの欠落を検出できない。
イ：通信制御の異常系テストではない。
ウ：FW拒否条件の検証にはならない。
エ：正しい。アクセス制御は許可系と拒否系の両方を検証する必要がある。
総合解説：セキュリティ機能はpositive testとnegative testを組み合わせて検証する。

問33 要件IDとテストケースIDを対応付けた表を作成する主な目的はどれか。
ア．全要件が少なくとも一つのテストで検証されているか追跡するため
イ．IPアドレスを自動配布するため
ウ．テスト結果を必ず成功にするため
エ．構成バックアップを圧縮するため
正答：ア
4肢解説
ア：正しい。要件とテストの対応を管理すると未検証要件を発見しやすい。
イ：DHCPの機能である。
ウ：追跡性は結果を保証しない。
エ：別の目的である。
総合解説：要件トレーサビリティは受入判定と変更影響分析にも有効である。

問34 性能試験結果を比較可能にするため、テスト実施ごとに固定すべき条件として最も適切なものはどれか。
ア．担当者だけ毎回変更する
イ．トポロジ、機器設定、ソフトウェア版、フレームサイズ、負荷条件、測定方法
ウ．フレームサイズを記録せず毎回ランダムにする
エ．測定時間を記録しない
正答：イ
4肢解説
ア：再現性向上の主要条件ではない。
イ：正しい。条件が変われば性能差が構成差か環境差か判断できない。
ウ：結果比較が困難になる。
エ：測定条件の再現性が失われる。
総合解説：ベンチマークでは条件を明記し、同一条件で再測定できることが重要である。

問35 VRRPフェイルオーバ試験を行う。テスト手順の事前条件として最も重要なものはどれか。
ア．事前状態を確認せずいきなり主系の電源を切る
イ．DNSキャッシュを必ず全削除する
ウ．正常時のMaster/Backup状態と通信経路が期待どおりであることを確認する
エ．テスト中のログ取得を停止する
正答：ウ
4肢解説
ア：結果の原因を特定しにくい。
イ：VRRP試験の必須条件ではない。
ウ：正しい。初期状態が異常なら障害注入後の結果を正しく評価できない。
エ：障害解析情報を失う。
総合解説：障害試験はpre-check、障害注入、観測、復旧、post-checkの順で手順化する。

問36 『フェイルオーバが速いこと』というテスト基準を改善する記述として最も適切なものはどれか。
ア．担当者が速いと感じれば合格とする
イ．成功するまで何度でもやり直し最良値だけ採用する
ウ．切替時間は記録しない
エ．主系断から業務通信再開まで5秒以内、連続損失は5パケット以内と定義する
正答：エ
4肢解説
ア：主観的で再現性がない。
イ：実運用品質を過大評価する。
ウ：要件適合を判定できない。
エ：正しい。時間・損失数など測定可能な値にすると客観的に判定できる。
総合解説：テストの期待結果はSLA・設計要件から数値化する。

問37 本番相当のセキュリティテストで顧客個人情報を使う必要がない場合、最も適切な方法はどれか。
ア．匿名化・ダミーデータを用い、本物の個人情報利用を避ける
イ．本番DBを無制限にコピーして全テスターへ配布する
ウ．テスト環境ならアクセス制御は不要とする
エ．結果確認のため個人情報を公開共有する
正答：ア
4肢解説
ア：正しい。テスト目的に不要な機密情報を持ち込まないことで漏えいリスクを減らす。
イ：情報漏えいリスクが高い。
ウ：非本番でも機密情報は保護が必要である。
エ：不適切である。
総合解説：テスト環境もデータ分類・最小権限・廃棄手順を定める。

問38 本番ネットワークで負荷試験中、業務応答時間がSLA上限を超え始めた。事前計画に基づく適切な行動はどれか。
ア．SLA違反しても最大負荷まで必ず継続する
イ．中断基準に達したため負荷を停止し、影響を回復させて原因を分析する
ウ．監視を停止して試験を続ける
エ．結果を記録せずなかったことにする
正答：イ
4肢解説
ア：利用者影響を拡大する。
イ：正しい。本番試験では業務保護のため停止条件を事前定義するべきである。
ウ：危険状態を把握できなくなる。
エ：改善につながらない。
総合解説：本番テストではリスク、実施時間帯、停止条件、連絡体制、ロールバックを明確にする。

問39 新ネットワークで疎通、セキュリティ、性能、冗長化の各試験を行う。効率的な順序として最も適切な考え方はどれか。
ア．最初に全装置の電源を切る障害試験だけ行う
イ．性能試験だけ合格すれば疎通・セキュリティは省略する
ウ．基本疎通・設定整合を確認してから機能/セキュリティ、性能、障害注入へ進む
エ．順序を毎回ランダムにする
正答：ウ
4肢解説
ア：基礎状態が未確認で原因分析しにくい。
イ：別要件を検証できない。
ウ：正しい。基礎機能が成立しない状態で高度な性能・冗長試験を行うと原因切り分けが難しい。
エ：再現性と効率が低い。
総合解説：テストは依存関係の低い基礎項目から積み上げ、問題発生時の切り分けを容易にする。

問40 コアスイッチのOSを更新した。新機能は使わないが、既存のOSPF、LACP、VRRP、SNMPが影響を受けないことを確認したい。最も適切なテストはどれか。
ア．起動できれば全機能正常とみなす
イ．新機能を使わないのでテスト不要とする
ウ．設定を全削除して初期化する
エ．変更箇所だけでなく既存主要機能の回帰テストを実施する
正答：エ
4肢解説
ア：プロトコル互換性や性能問題を見逃す。
イ：基盤変更には回帰リスクがある。
ウ：既存サービスを破壊する。
エ：正しい。OS更新は複数機能へ影響し得るため既存機能の非退行を確認する。
総合解説：回帰テストは変更影響分析から対象を選び、重要経路・冗長機能を優先する。

問41 pingが成功したことで直接確認できる内容として最も適切なものはどれか。
ア．ICMP EchoによるIP到達性があること
イ．HTTPSアプリが必ず正常であること
ウ．DNSが必ず正常であること
エ．FWの全ルールが正しいこと
正答：ア
4肢解説
ア：正しい。ping成功は一定のL3到達性を示すが、アプリケーション正常性までは保証しない。
イ：TCP/443やアプリ処理は別途確認が必要である。
ウ：IP直接指定ならDNSを使わない。
エ：一つの通信成功だけでは判断できない。
総合解説：接続テストはping、TCP接続、名前解決、実アプリ通信を段階的に確認する。

問42 通信が途中で失敗している区間を推定するため、経由ルータを観測する代表的なツールはどれか。
ア．nslookupだけ
イ．traceroute/tracert
ウ．arpだけ
エ．netstatだけ
正答：イ
4肢解説
ア：主にDNS名前解決を確認する。
イ：正しい。TTL/Hop Limitを変化させ、途中ノードからの応答を利用して経路を推定する。
ウ：同一リンクのIP-MAC対応を確認する。
エ：ローカル接続状態の確認が中心である。
総合解説：tracerouteはICMP制限やECMPの影響も受けるため、結果だけで断定しない。

問43 サーバのTCP/443がFWを越えて待受け可能かを確認する方法として最も直接的なものはどれか。
ア．pingだけ成功すれば443も必ず通ると判断する
イ．DNSのMXレコードを確認する
ウ．クライアントから対象IPのTCP/443へ接続試行し、3ウェイハンドシェイク成立を確認する
エ．NTP offsetだけ測る
正答：ウ
4肢解説
ア：ICMPとTCP/443は別ルールになり得る。
イ：HTTPSポート到達性とは無関係である。
ウ：正しい。ICMPだけでなく対象TCPポートの到達性を確認できる。
エ：TCP/443の接続確認ではない。
総合解説：アプリ接続試験ではL3疎通、L4ポート、TLS、HTTP応答を順に切り分ける。

問44 DNSサーバ更改後、社内PCから名前解決できるが一部旧IPへ接続している。まず確認すべきものはどれか。
ア．全PCのMACアドレスを変更する
イ．OSPF Router IDを変更する
ウ．光ケーブルを交換する
エ．クライアント/中間DNSのキャッシュとTTL、権威DNSの新レコード
正答：エ
4肢解説
ア：DNSキャッシュ問題には不要である。
イ：DNSレコード反映とは無関係である。
ウ：名前解決結果の新旧には直接関係しない。
エ：正しい。キャッシュ残存により旧IPが返る可能性がある。
総合解説：DNS切替え試験では権威応答とキャッシュ経由応答を分けて確認する。

問45 小さいpingは成功するが、大きいHTTPSアップロードだけ失敗する。VPN導入直後である。疑うべき項目はどれか。
ア．トンネルオーバーヘッドによるPath MTU/MSS不整合
イ．DNSゾーン名の長さ
ウ．ユーザ名の文字数
エ．NTP stratum
正答：ア
4肢解説
ア：正しい。大きいパケットだけ失敗する場合、断片化やPMTUDブラックホールを疑う。
イ：パケットサイズ依存障害とは無関係である。
ウ：MTUには影響しない。
エ：大容量転送失敗の原因ではない。
総合解説：DF付きpingやMSS/PMTU観測を用いてサイズ境界を切り分ける。

問46 設計で『利用者LANからDBのTCP/3306は拒否』としている。受入試験として最も適切なものはどれか。
ア．許可済みWeb通信だけ確認する
イ．利用者LANからDB:3306へ接続を試み、拒否されFWログにも期待どおり記録されることを確認する
ウ．DBサーバ上でpingだけ行う
エ．FW設定画面を目視するだけ
正答：イ
4肢解説
ア：禁止ルールを検証できない。
イ：正しい。禁止通信は実際に拒否されることをnegative testで確認する。
ウ：TCP/3306拒否を直接確認できない。
エ：実際の転送動作・ログまで検証できない。
総合解説：セキュリティテストは設定レビューと動的な接続試験を組み合わせる。

問47 新規公開サーバの受入前に脆弱性スキャンで重大な既知脆弱性が検出された。最も適切な対応はどれか。
ア．スキャン結果を削除してそのまま公開する
イ．重大度に関係なく全て誤検知とみなす
ウ．真偽と影響を確認し、修正または緩和して再スキャン後に受入判断する
エ．公開後にだけ初回確認する
正答：ウ
4肢解説
ア：リスクを放置する。
イ：評価が必要である。
ウ：正しい。検出結果を評価し、対処後に再検証する。
エ：受入前にリスクを確認すべきである。
総合解説：脆弱性テストは検出、分析、修正、再検証までを一連の工程とする。

問48 HTTPSサービスの受入試験で、単にページが開くこと以外に確認すべき項目として最も適切なものはどれか。
ア．画面の背景色だけ確認する
イ．DNS TTLだけ確認する
ウ．HTTPへダウングレードして確認するだけ
エ．証明書チェーン・サービス名・有効期限・許可TLSバージョン/暗号設定を確認する
正答：エ
4肢解説
ア：TLSセキュリティとは無関係である。
イ：TLS設定検証には不足する。
ウ：TLSを検証できない。
エ：正しい。誤った証明書や弱い設定でもページ表示できる場合がある。
総合解説：機能試験とセキュリティ設定試験を分けて明確にする。

問49 内部端末10.1.1.10から外部へ接続した。FW内側pcapでは送信元10.1.1.10、外側pcapでは203.0.113.5になっている。これは何を示すか。
ア．NATによる送信元アドレス変換が期待どおり動作している
イ．DNSによる名前変換
ウ．STPによるループ防止
エ．TLSによる暗号化
正答：ア
4肢解説
ア：正しい。内外の観測点で送信元アドレス変換を直接確認できる。
イ：IPヘッダの送信元変更はNATである。
ウ：L2制御とは無関係である。
エ：アドレス変換を行わない。
総合解説：NATテストでは変換前後のアドレス・ポート、戻り通信、セッションタイムアウトを確認する。

問50 新しい有線802.1Xで、端末はEAPOLを送信しスイッチもRADIUSへAccess-Requestを送っているが、Access-Rejectが返る。次に確認すべき箇所はどれか。
ア．Ethernetケーブルを必ず交換する
イ．認証方式、利用者/証明書、RADIUSポリシーなど認証サーバ側の判定理由
ウ．OSPFエリア番号だけ
エ．DNS MXレコード
正答：イ
4肢解説
ア：EAPOLとRADIUS要求が通っているため優先度は低い。
イ：正しい。L2とRADIUS到達性は成立しており、Reject理由の確認が次の段階である。
ウ：認証拒否とは無関係である。
エ：メール設定である。
総合解説：認証テストはSupplicant、Authenticator、RADIUS、PKI/ID基盤を層別に切り分ける。

問51 RFC 2544のベンチマークでスループットを測定する考え方として最も適切なものはどれか。
ア．平均CPU使用率だけを測る
イ．DNS応答時間だけを測る
ウ．フレーム損失なしに転送できる最大レートを求める
エ．必ず1種類のフレームサイズだけで測る
正答：ウ
4肢解説
ア：ネットワーク転送スループットの定義ではない。
イ：対象が異なる。
ウ：正しい。RFC 2544ではフレーム損失が発生しない最大転送レートをスループットとして扱う。
エ：複数サイズでの評価が重要である。
総合解説：機器性能はフレームサイズによってpps負荷が変わるため条件を明示する。

問52 100万フレーム送信し、999,000フレーム受信した。フレーム損失率はどれか。
ア．1%（損失数を10,000とみなす）
イ．0.01%（損失数を100とみなす）
ウ．99.9%（損失率ではなく受信率）
エ．0.1%（1,000÷1,000,000×100で計算）
正答：エ
4肢解説
ア：10倍大きい。
イ：10分の1である。
ウ：これは受信率である。
エ：正しい。損失1,000/1,000,000=0.001=0.1%である。
総合解説：性能試験では送信数・受信数・損失率を同一測定区間で記録する。

問53 短時間の性能試験では現れないメモリリークやセッション枯渇を発見するため、一定負荷を長時間継続する試験は何に近いか。
ア．ソークテスト（長時間安定性試験）
イ．単発pingテスト
ウ．静的設定レビュー
エ．DNSゾーン転送
正答：ア
4肢解説
ア：正しい。長時間運転で資源枯渇や累積不具合を検出する。
イ：長時間安定性を確認できない。
ウ：実負荷での累積問題は分からない。
エ：性能安定性試験ではない。
総合解説：受入時はピーク性能だけでなく長時間安定性も評価する。

問54 ネットワーク装置の遅延を比較する際、測定条件として特に統一すべきものはどれか。
ア．担当者の氏名だけ
イ．フレームサイズ、負荷率、経路、測定点
ウ．ラックの色
エ．DNSドメイン名
正答：イ
4肢解説
ア：性能値には直接影響しない。
イ：正しい。遅延は負荷やフレームサイズに依存するため条件統一が必要である。
ウ：遅延とは無関係である。
エ：L2/L3装置遅延の主条件ではない。
総合解説：ベンチマーク比較では測定条件を揃え、平均だけでなく分布も見る。

問55 冗長ルータのフェイルオーバ時間を正確に測る方法として最も適切なものはどれか。
ア．障害後に一度だけpingし成功なら0秒とする
イ．装置ログだけを見て利用者通信を測らない
ウ．連続トラフィックを流し、主系障害時の最後の正常受信から再開までの損失時間を測る
エ．DNS TTLから推定する
正答：ウ
4肢解説
ア：切替途中の停止時間を測れない。
イ：ログ時刻と実通信復旧が一致しない場合がある。
ウ：正しい。実トラフィックの中断時間を直接観測できる。
エ：ルータ切替時間とは無関係である。
総合解説：フェイルオーバ試験では制御プレーン収束とデータプレーン通信再開の両方を確認する。

問56 2台のFWで通常時合計8Gbit/sを処理している。1台故障時も同じ業務負荷を継続する受入試験で最も重要な確認はどれか。
ア．正常時に4Gbit/sずつ流れることだけ
イ．1台停止後は性能基準を無視する
ウ．管理画面が開くだけで合格とする
エ．残存1台が8Gbit/sを処理してもCPU・セッション・遅延・損失が基準内であること
正答：エ
4肢解説
ア：障害時能力を確認できない。
イ：高可用性要件を満たせない。
ウ：データプレーン性能を確認していない。
エ：正しい。冗長切替えだけでなく障害時容量が要件を満たす必要がある。
総合解説：N-1試験は残存資源でピーク負荷を処理できるかを評価する。

問57 受入テストの合否を決める基準として最も適切なものはどれか。
ア．契約・要求仕様で合意した機能・性能・可用性・セキュリティ基準
イ．ベンダーが成功と言えば無条件合格
ウ．テスト担当者の感覚だけ
エ．最も良かった1回の結果だけ
正答：ア
4肢解説
ア：正しい。受入は発注側要件を満たしたかを客観的に判定する。
イ：合意基準で判断すべきである。
ウ：主観的である。
エ：再現性・安定性を無視する。
総合解説：受入基準は実装前に合意し、測定方法も明文化する。

問58 4台のバックエンドへ均等分散する設計なのに、負荷試験で1台だけ90%、残り3台が20%以下である。次に確認すべきものはどれか。
ア．全サーバのIPを同じにする
イ．LBアルゴリズム、セッション維持、ヘルス状態、ハッシュキーを確認する
ウ．DNSを停止する
エ．負荷試験をやめて均等と仮定する
正答：イ
4肢解説
ア：IP競合を起こす。
イ：正しい。偏りは分散方式やstickinessの影響で発生し得る。
ウ：LB偏りの根本調査ではない。
エ：問題を見逃す。
総合解説：負荷分散は接続数・セッション特性・バックエンド性能を含めて評価する。

問59 負荷を2Gbit/sから4Gbit/sへ上げるとFW CPUは95%、回線利用率は45%、パケット損失が急増した。最も可能性が高いボトルネックはどれか。
ア．WAN回線帯域
イ．DNSキャッシュ
ウ．FWの処理能力
エ．ラックの高さ
正答：ウ
4肢解説
ア：利用率45%であり提示情報では優先度が低い。
イ：トラフィック損失とCPU飽和の説明にならない。
ウ：正しい。回線には余裕がある一方、FW CPU飽和と損失増加が相関している。
エ：性能ボトルネックではない。
総合解説：性能試験では各装置・リンクの利用率を同時観測してボトルネック位置を特定する。

問60 遅延要件が『通常業務時間の95パーセンタイルで50ms以下』である。測定10,000件のうち9,500件目の昇順値が48ms、最大値が200msだった。要件判定として最も適切なものはどれか。
ア．最大200msなので必ず不合格である
イ．平均値が不明なので95パーセンタイルも判定不能である
ウ．95パーセンタイルは最大値と常に同じである
エ．95パーセンタイル48msなので、この指標については合格である
正答：エ
4肢解説
ア：要件は最大値ではなく95パーセンタイルである。
イ：9,500件目の値が与えられている。
ウ：異なる統計量である。
エ：正しい。最大値ではなく指定された95パーセンタイルで判定する。
総合解説：受入では要件で指定した統計量と測定窓を厳密に一致させる。

問61 ネットワーク運用でSNMPを利用する場面として、最も適切なものはどれか。
ア．ネットワーク機器の管理情報を取得し、状態監視や管理に利用する
イ．Webページを暗号化する
ウ．IPアドレスを自動配布する
エ．L2ループを防止する
正答：ア
4肢解説
ア：正しい。SNMPはMIBで定義された管理情報を読み書きし、監視に利用できる。
イ：TLS/HTTPSの役割である。
ウ：DHCPの役割である。
エ：STP等の役割である。
総合解説：SNMP監視ではインタフェース、CPU、メモリ、エラーなどのオブジェクトを継続取得する。

問62 監視サーバが一定間隔で機器へ問い合わせる方式と、機器側からイベント発生時に通知する方式の組合せとして正しいものはどれか。
ア．DNSとDHCP
イ．pollingとtrap/notification
ウ．TCPとUDP
エ．NATとPAT
正答：イ
4肢解説
ア：監視方式の対比ではない。
イ：正しい。pollingは監視側主導、trap等は被監視機器側からの非同期通知である。
ウ：トランスポート方式であり監視主導方式の名称ではない。
エ：アドレス変換方式である。
総合解説：pollingとイベント通知は相互補完的に使うと監視精度が高まる。

問63 SNMPv3 USMを利用する主なセキュリティ上の利点はどれか。
ア．全通信を無認証で公開する
イ．IPアドレスを自動割当てする
ウ．認証とプライバシー保護を利用できる
エ．ログを必ず削除する
正答：ウ
4肢解説
ア：SNMPv3の利点と逆である。
イ：DHCPの機能である。
ウ：正しい。USMはメッセージ認証と暗号化を提供できる。
エ：監視セキュリティとは無関係である。
総合解説：管理ネットワークでは可能な限り認証・暗号化を備えたSNMPv3を利用する。

問64 1Gbit/sインタフェースで60秒間に送信オクテットカウンタが3,750,000,000増加した。平均送信利用率はおよそ何%か。
ア．25%（算出した平均帯域の半分とみなす）
イ．75%（カウンタ増分と回線容量の比が一致しない）
ウ．100%（60秒間フル利用とみなす）
エ．50%（30Gbit÷60秒=0.5Gbit/sで計算）
正答：エ
4肢解説
ア：半分の値である。
イ：計算が一致しない。
ウ：1Gbit/sを60秒継続した量ではない。
エ：正しい。3.75×10^9バイト×8=30Gbit、60秒で0.5Gbit/sなので50%である。
総合解説：カウンタ差分を時間差で割ると平均ビットレートを算出できる。

問65 ping監視は成功しているが、利用者はWebサービスへ接続できない。最も適切な評価はどれか。
ア．ICMP死活監視だけではアプリケーションサービスの正常性を保証できない
イ．ping成功なら必ずWebも正常である
ウ．Web障害は必ずDNSだけが原因である
エ．ICMPが通ればTCP/443も同じルールで必ず通る
正答：ア
4肢解説
ア：正しい。L3到達性とL7サービス状態は別である。
イ：FWやアプリ障害があり得る。
ウ：他の原因も多い。
エ：アクセス制御が異なる場合がある。
総合解説：監視はICMP、TCPポート、HTTP応答、業務トランザクションなど多層化する。

問66 重要回線のpolling間隔を5分から10秒へ短縮する場合の主なトレードオフはどれか。
ア．間隔を短くするほど監視負荷は必ずゼロになる
イ．異常検出を早めやすい一方、監視サーバ・機器・回線の負荷が増える
ウ．監視頻度は検知時間に影響しない
エ．短縮するとIPアドレス数が増える
正答：イ
4肢解説
ア：逆である。
イ：正しい。高頻度監視は検知性を高めるが収集負荷も増える。
ウ：pollingでは直接影響する。
エ：無関係である。
総合解説：監視頻度は資産重要度、変化速度、収集コストを基に決める。

問67 従来の5分SNMP pollingでは数秒間のキュー輻輳を捉えられない。改善として最も適切なものはどれか。
ア．polling間隔をさらに長くする
イ．全監視を停止する
ウ．高頻度のストリーミングTelemetry/YANG-Pushで必要データを購読する
エ．DNS TTLを短縮する
正答：ウ
4肢解説
ア：短時間異常をより見逃しやすい。
イ：可視性を失う。
ウ：正しい。push型で短い粒度の状態変化を継続受信できる。
エ：キュー監視とは無関係である。
総合解説：YANG-Push等は構造化された状態データを継続配信する仕組みとして利用できる。

問68 監視サーバ自身と管理ネットワークが停止したため、全装置が一斉に『応答なし』となった。最初に疑うべきことはどれか。
ア．全ネットワーク機器が同時に必ず故障したと断定する
イ．DNSレコードが多すぎることだけ
ウ．VLAN名が長すぎること
エ．被監視装置の同時故障だけでなく監視基盤・管理経路の共通障害
正答：エ
4肢解説
ア：共通監視経路障害を考慮すべきである。
イ：直接の説明にならない。
ウ：死活監視一斉失敗とは無関係である。
エ：正しい。監視系自身の障害で大量のdownアラートが出ることがある。
総合解説：監視基盤も冗長化・自己監視し、管理経路の可用性を別途確認する。

問69 高速回線で古い32bitオクテットカウンタを低頻度pollingしたところ、差分が負値のように見えることがある。適切な対応はどれか。
ア．64bit高容量カウンタを利用し、カウンタラップを考慮して差分計算する
イ．負値が出たら必ず回線速度を0にする
ウ．カウンタを文字列として連結する
エ．pollingを年1回にする
正答：ア
4肢解説
ア：正しい。高速回線では32bitカウンタが短時間で周回し得る。
イ：計算上のラップを誤解している。
ウ：利用率計算にならない。
エ：ラップ問題を悪化させる。
総合解説：高速インタフェース監視ではifHCInOctets/ifHCOutOctets等の高容量カウンタを利用する。

問70 重要Webサービスで『装置UPだがサービス停止』と『短時間の性能劣化』の両方を早く検知したい。最も適切な監視設計はどれか。
ア．pingだけを1時間ごとに行う
イ．ICMP/インタフェース監視、HTTP合成監視、Telemetryによる性能監視を組み合わせる
ウ．HTTP監視だけで装置資源は一切見ない
エ．監視項目を一つに限定する
正答：イ
4肢解説
ア：アプリ障害・短時間劣化を見逃しやすい。
イ：正しい。異なるレイヤの監視を組み合わせることで死活・機能・性能を補完できる。
ウ：原因切り分け情報が不足する。
エ：複数障害モードを捉えにくい。
総合解説：監視設計はユーザ体験とインフラ状態を両方観測する。

問71 syslogでseverityを利用する主な目的はどれか。
ア．IPアドレスを割り当てる
イ．暗号鍵を生成する
ウ．イベントの重大度を表し、保存・通知・優先順位付けに利用する
エ．パケットをL2転送する
正答：ウ
4肢解説
ア：DHCPの機能である。
イ：syslogの目的ではない。
ウ：正しい。severityにより緊急度に応じた処理がしやすい。
エ：スイッチングとは異なる。
総合解説：ログ運用ではfacility、severity、送信元、タイムスタンプを整理する。

問72 『どの送信元がどの宛先へ何バイト通信したか』を大規模に把握するのに適した情報はどれか。
ア．DNS MXレコード
イ．ARPキャッシュだけ
ウ．NTP offsetだけ
エ．IPFIXフローレコード
正答：エ
4肢解説
ア：メール配送先情報である。
イ：同一リンクのIP-MAC対応である。
ウ：時刻差情報である。
エ：正しい。パケット全文ではなくフロー単位のメタデータを効率的に収集できる。
総合解説：IPFIXは帯域上位利用者、アプリ傾向、異常通信の分析に利用できる。

問73 ネットワーク機器のログを集中ログサーバへ転送する主な利点はどれか。
ア．機器障害・侵害時でもログを別場所に残し、横断検索しやすくする
イ．機器の帯域が必ず2倍になる
ウ．ログが不要になる
エ．全障害を自動修復する
正答：ア
4肢解説
ア：正しい。ローカルだけに保存するより証拠保全と分析性が高まる。
イ：ログ集中化は性能倍増ではない。
ウ：むしろログを集約する。
エ：監視と復旧は別である。
総合解説：集中ログは容量、保持期間、時刻同期、アクセス制御を含めて設計する。

問74 WAN利用率が急増した。原因通信を特定するため最も有効な確認はどれか。
ア．NTPサーバの時刻だけ確認する
イ．IPFIXでバイト数の多い送信元・宛先・ポートの上位フローを確認する
ウ．ラック温度だけ確認する
エ．全端末の壁紙を確認する
正答：イ
4肢解説
ア：通信量内訳は分からない。
イ：正しい。リンク全体のSNMP利用率だけでは内訳が分からないためフロー情報を使う。
ウ：帯域原因の特定にはならない。
エ：無関係である。
総合解説：SNMPで全体量、IPFIXで内訳を見ると原因切り分けがしやすい。

問75 本番ルータで常時debugレベルの詳細ログを大量出力したところCPUとディスクI/Oが上昇した。適切な対応はどれか。
ア．全ログを永久にdebugへ固定する
イ．ログ機能を完全停止する
ウ．通常運用は必要なログレベルに戻し、debugは対象・時間を限定して利用する
エ．CPU上昇を無視する
正答：ウ
4肢解説
ア：運用負荷が大きい。
イ：障害・監査情報を失う。
ウ：正しい。過剰ログは装置性能とログ基盤を圧迫する。
エ：本番影響を拡大する。
総合解説：ログ詳細度はトラブルシュート価値と性能・容量のトレードオフで管理する。

問76 FWは稼働しているのに集中ログサーバで20分間だけログが途切れている。最も適切な初動はどれか。
ア．ログがないので正常と断定する
イ．FWを即時初期化する
ウ．DNSレコードだけ変更する
エ．FW側ローカルログ、転送キュー、ネットワーク、ログサーバ受信状態を確認する
正答：エ
4肢解説
ア：監視経路障害の可能性がある。
イ：原因未特定で過剰対応である。
ウ：syslog欠損の一般的切り分けではない。
エ：正しい。生成・転送・受信のどこで欠損したかを切り分ける。
総合解説：ログ監視では『ログが来ないこと』自体を監視する仕組みも重要である。

問77 超高速回線で全パケット由来のフロー収集が装置負荷になるためサンプリングを導入する。主な注意点はどれか。
ア．負荷を減らせる一方、短時間・小容量フローを見落とす可能性がある
イ．サンプリングすると必ず全フローを完全再現できる
ウ．サンプリング率を下げるほど小さいフロー検知が向上する
エ．サンプリングはDNS専用機能である
正答：ア
4肢解説
ア：正しい。サンプリングは精度と収集コストのトレードオフである。
イ：情報損失があり得る。
ウ：一般に逆である。
エ：トラフィック計測にも使われる。
総合解説：監視目的に応じてサンプリング率と検知粒度を決める。

問78 ネットワーク機器全体で1日120GBのログを生成し、30日保持する。圧縮・冗長化を無視した最低容量はどれか。
ア．360GB（3日分として計算）
イ．3.6TB（120GB×30日で計算）
ウ．1.2TB（10日分として計算）
エ．36TB（正しい値の10倍）
正答：イ
4肢解説
ア：10分の1である。
イ：正しい。120GB×30=3,600GB=3.6TBである。
ウ：10日分相当である。
エ：10倍大きい。
総合解説：実運用では索引、予備容量、増加率、冗長化分を加える。

問79 SNMPで回線利用率95%、IPFIXで特定バックアップ通信が80%を占有、syslogで同時刻にキューdrop警告が出ている。最も適切な結論はどれか。
ア．DNS障害だけが原因と断定する
イ．SNMP・IPFIX・syslogは互いに関連付けてはいけない
ウ．バックアップ通信による回線輻輳がキューdropの有力原因である
エ．キューdropは帯域利用率と無関係である
正答：ウ
4肢解説
ア：提示情報と整合しない。
イ：相関分析が有効である。
ウ：正しい。全体量・通信内訳・装置イベントが同じ時刻に整合している。
エ：高負荷時に発生し得る。
総合解説：複数テレメトリを時刻で相関すると原因特定の確度が上がる。

問80 TelemetryでCPU使用率が突然0%となったが、SNMPでは70%、装置CLIでも正常稼働している。最も適切な対応はどれか。
ア．CPUが0%なので装置が停止したと断定する
イ．SNMPとCLIの結果を無視する
ウ．装置を直ちに初期化する
エ．Telemetry収集・変換・時系列DB側の異常を疑い、複数データ源で値を検証する
正答：エ
4肢解説
ア：他の観測と矛盾している。
イ：クロスチェックすべきである。
ウ：監視基盤の問題かもしれない。
エ：正しい。単一監視系の値だけで装置状態を断定しない。
総合解説：監視データ品質も監視対象であり、収集パイプラインの欠損・変換エラーを検出する必要がある。

問81 ネットワーク変更管理の主な目的として最も適切なものはどれか。
ア．変更内容・影響・承認・実施結果を管理し、予期しない障害や無断変更を減らす
イ．全変更を禁止する
ウ．承認なしで自由に変更する
エ．変更履歴を残さない
正答：ア
4肢解説
ア：正しい。変更を統制し追跡可能にすることで安定性とセキュリティを高める。
イ：必要な改善や修正ができない。
ウ：障害原因・責任を追跡しにくい。
エ：監査・復旧が困難になる。
総合解説：変更管理は申請、評価、承認、実施、確認、記録を一連で扱う。

問82 ネットワーク機器設定を変更前にバックアップする主な理由はどれか。
ア．帯域を増加させるため
イ．変更失敗時に既知の正常構成へ戻せるようにする
ウ．アカウントを自動削除するため
エ．DNSを高速化するため
正答：イ
4肢解説
ア：設定バックアップは容量増加ではない。
イ：正しい。ロールバックの基礎となる。
ウ：別の管理機能である。
エ：無関係である。
総合解説：設定バックアップはバージョン・日時・対象機器を明確に管理する。

問83 複数管理者が同じadminアカウントを共有する最大の問題はどれか。
ア．ログイン速度が必ず遅くなる
イ．IPアドレスが重複する
ウ．誰がどの操作を行ったか個人単位で追跡しにくい
エ．SNMPが使えなくなる
正答：ウ
4肢解説
ア：本質的問題ではない。
イ：アカウント共有とは無関係である。
ウ：正しい。説明責任・監査性が低下する。
エ：直接関係しない。
総合解説：原則として個人アカウントを使い、特権操作を記録する。

問84 重大脆弱性が悪用中で、通常の週次CABを待てない緊急パッチが必要である。最も適切な対応はどれか。
ア．緊急なら記録・承認・検証を全て不要とする
イ．通常会議まで必ず数週間放置する
ウ．全機器を同時に無確認更新する
エ．緊急変更手順で権限者承認・影響確認・バックアウト準備を行い、事後レビューも実施する
正答：エ
4肢解説
ア：無統制な変更事故を招く。
イ：実悪用中ならリスクが高い。
ウ：影響範囲が大きい。
エ：正しい。緊急でも統制を完全に省略せず簡略化された承認・記録を行う。
総合解説：緊急変更は速度と統制を両立させ、事後に標準プロセスへ記録を戻す。

問85 変更申請ではACL1行追加のみの予定だったが、実機差分で20行の削除も検出された。最も適切な対応はどれか。
ア．予定外差分を調査し、正当性を確認するまで変更完了としない
イ．申請外差分は全て無視する
ウ．差分を記録せず承認済みとみなす
エ．バックアップを削除する
正答：ア
4肢解説
ア：正しい。未承認の構成変更が混入している可能性がある。
イ：無断変更や自動化誤りを見逃す。
ウ：変更統制を損なう。
エ：調査・復旧性が低下する。
総合解説：変更後は承認内容と実機差分を照合する。

問86 退職者のネットワーク管理アカウントが1か月後も有効だった。最も適切な改善はどれか。
ア．退職者本人が必要と感じたら自分で削除する
イ．人事イベントとID管理を連携し、退職・異動時の無効化期限と確認責任を定める
ウ．パスワードだけ永久に同じまま残す
エ．アカウント棚卸を行わない
正答：イ
4肢解説
ア：組織側で確実に管理すべきである。
イ：正しい。アカウントライフサイクルを業務イベントと連動させる必要がある。
ウ：不正利用リスクがある。
エ：不要IDを検出できない。
総合解説：Joiner/Mover/Leaver管理と定期棚卸を組み合わせる。

問87 管理者が日常メール閲覧にもルータ設定にも同じ特権アカウントを使っている。改善として最も適切なものはどれか。
ア．特権アカウントを全社員へ配布する
イ．管理作業も匿名アカウントで行う
ウ．通常業務用と特権管理用アカウントを分離する
エ．パスワードを短くして入力しやすくする
正答：ウ
4肢解説
ア：重大な権限拡大となる。
イ：監査性を失う。
ウ：正しい。攻撃面と誤操作範囲を減らせる。
エ：セキュリティを弱める。
総合解説：特権IDは利用場面・端末・時間・記録を厳格に制御する。

問88 高リスクなコアルータOS更新を行う時間帯として最も適切な考え方はどれか。
ア．最繁忙時間帯に予告なく行う
イ．担当者が一人しかいない時間を選ぶ
ウ．ロールバック時間を確保しない
エ．業務影響が小さく、担当者・ベンダー・監視・ロールバック体制を確保できる時間帯を選ぶ
正答：エ
4肢解説
ア：業務影響が大きい。
イ：障害対応力が低い。
ウ：復旧不能リスクが高い。
エ：正しい。単に深夜というだけでなく支援体制と復旧余裕が重要である。
総合解説：変更ウィンドウは利用者影響、支援体制、戻し所要時間から決める。

問89 CMDBではFW-AのOSがv10.2となっているが、実機はv10.0で既知脆弱性が残っていた。最も適切な再発防止はどれか。
ア．実機から定期収集した構成・バージョン情報とCMDBを照合し、不一致を検知する
イ．CMDBを廃止して記憶だけで管理する
ウ．実機情報を確認せずCMDBを正しいと仮定する
エ．脆弱性情報を見ない
正答：ア
4肢解説
ア：正しい。台帳だけの手入力では更新漏れが発生し得る。
イ：構成把握が悪化する。
ウ：今回の問題を再発する。
エ：リスク管理ができない。
総合解説：構成情報は自動ディスカバリと変更プロセスを連携させて正確性を維持する。

問90 FW変更後、主要業務の30%が失敗し、原因特定に20分以上かかる見込みで、事前に『10分で復旧できなければ戻す』と合意している。最も適切な判断はどれか。
ア．原因が分かるまで無期限に本番で調査する
イ．合意済み中断基準に従ってロールバックを開始し、サービス復旧後に原因分析する
ウ．合意基準は参考なので必ず無視する
エ．ログを削除して障害を隠す
正答：イ
4肢解説
ア：業務影響が拡大する。
イ：正しい。事前基準を超えて本番影響を継続させるべきではない。
ウ：変更統制の意味がなくなる。
エ：調査不能になる。
総合解説：変更計画には明確な停止・戻し基準と判断責任者を定める。

問91 利用者から『通信できない』と申告があった。効率的な初期切り分けとして最も適切なものはどれか。
ア．物理リンク、IP設定、経路、名前解決、アプリケーションの順に層を分けて確認する
イ．最初からアプリケーションを再インストールする
ウ．全ネットワーク機器を同時再起動する
エ．利用者端末の壁紙設定だけ確認する
正答：ア
4肢解説
ア：正しい。下位層から順に確認すると、原因範囲を段階的に狭めやすい。
イ：下位層障害なら無関係であり、原因特定を遅らせる。
ウ：原因情報を失い、影響範囲も大きい。
エ：通信障害との関連がない。
総合解説：障害切り分けでは症状を再現し、L1/L2/L3/L4/L7のどこまで正常かを確認して原因範囲を狭める。

問92 Webサイトへホスト名では接続できないが、IPアドレスを直接指定すると接続できる。最初に疑うべきものはどれか。
ア．物理リンク断
イ．DNS名前解決
ウ．TCP/443のFW拒否
エ．サーバ電源断
正答：イ
4肢解説
ア：IP直指定で接続できているので可能性は低い。
イ：正しい。IP到達性とアプリ接続が成立しているため、名前解決経路の問題が有力である。
ウ：IP直指定でHTTPS接続できるなら可能性は低い。
エ：IP直指定で応答しているため該当しにくい。
総合解説：障害切り分けではホスト名利用とIP直指定を比較するとDNS障害を分離しやすい。

問93 スイッチのインタフェースがadministratively upだがoperational downである。最初に確認すべき内容として最も適切なものはどれか。
ア．DNSゾーン転送
イ．BGP LOCAL_PREF
ウ．ケーブル、対向ポート、トランシーバ、速度・オートネゴシエーションなど物理リンク条件
エ．HTTP Cookie
正答：ウ
4肢解説
ア：物理リンク確立とは無関係である。
イ：L1/L2リンクダウンの初期確認項目ではない。
ウ：正しい。管理上有効でも物理キャリアが成立していない状態を示す。
エ：物理リンク状態に影響しない。
総合解説：operational downではまずL1/L2条件を確認し、その後に上位プロトコルへ進む。

問94 EthernetインタフェースでCRC/FCSエラーが継続的に増加している。最初に疑うべき原因として最も適切なものはどれか。
ア．DNS TTLが長い
イ．HTTPセッション数が少ない
ウ．OSPFコストが高い
エ．ケーブル・コネクタ・トランシーバなど物理伝送品質の問題
正答：エ
4肢解説
ア：フレーム破損とは無関係である。
イ：CRCエラーを直接説明しない。
ウ：フレームのFCS不一致とは関係しない。
エ：正しい。CRC/FCSエラーは受信フレームの破損を示し、物理層・リンク層の品質問題が典型原因である。
総合解説：CRC増加時はケーブル交換、光レベル、エラーカウンタ、対向側統計を確認する。

問95 同一サブネット上のサーバへpingできず、端末のARPテーブルでは対象IPがincompleteのままである。最も有力な原因候補はどれか。
ア．対象ホストからARP応答を得られていないため、L2到達性・VLAN・対象ホスト状態を確認する
イ．インターネット上のBGP経路だけを確認する
ウ．DNSキャッシュを削除する
エ．TLS証明書を更新する
正答：ア
4肢解説
ア：正しい。ARP解決が成立しない場合、同一L2セグメント内の到達性に問題がある可能性が高い。
イ：同一サブネット通信では通常BGPを使わない。
ウ：ARP解決失敗には直接関係しない。
エ：L2アドレス解決には無関係である。
総合解説：同一サブネット障害ではARP要求/応答、VLAN所属、ポート状態、対象ホストNICを確認する。

問96 拠点Aからサーバ宛てのパケットは本社まで到達するが、本社ルータにサーバ宛て経路が存在せず破棄されている。最も適切な分類はどれか。
ア．ARPスプーフィング
イ．ルーティングブラックホール
ウ．DNSキャッシュポイズニング
エ．TLSハンドシェイク失敗
正答：イ
4肢解説
ア：提示症状は経路欠落で説明できる。
イ：正しい。宛先への有効な次ホップがなく、途中でパケットが破棄される状態である。
ウ：宛先IPは既に決まっており経路問題である。
エ：L3で到達前に破棄されている。
総合解説：ルートテーブル、経路広告、フィルタ、デフォルトルートを確認して欠落地点を特定する。

問97 クライアントからサーバへの往路はFW-A、復路はFW-Bを通る。FW間にセッション同期がない場合に起こりやすい症状はどれか。
ア．TCPは往復経路が異なるほど必ず高速化する
イ．DNSが自動的に往路と復路を同じにする
ウ．復路パケットが未確立セッションと判断され、FW-Bで破棄される
エ．FW-Bは同期設定なしでも必ずFW-Aの状態を知っている
正答：ウ
4肢解説
ア：そのような性質はない。
イ：DNSはルーティングを直接制御しない。
ウ：正しい。ステートフルFWは接続状態に依存するため、非対称経路で通信が失敗する場合がある。
エ：状態共有がないなら保証されない。
総合解説：障害時だけ経路が非対称になる構成では、フェイルオーバ時のFW状態と経路を合わせて確認する。

問98 小さいHTTP要求は成功するが、大きなファイル転送だけ途中で停止する。VPN区間追加後に発生し、ICMP Packet Too Big等が途中で遮断されている。最も疑うべきものはどれか。
ア．DNSサーバのCPU不足
イ．ARPキャッシュの寿命が長い
ウ．NTP時刻ずれ
エ．Path MTU Discoveryが機能せず、大きなパケットがブラックホール化している
正答：エ
4肢解説
ア：パケットサイズ依存の症状を説明しにくい。
イ：同様にサイズ依存障害とは関係しにくい。
ウ：大容量転送停止の原因ではない。
エ：正しい。トンネルで実効MTUが小さくなり、必要なICMP通知が届かないと大きな通信だけ失敗する場合がある。
総合解説：PMTU障害ではDF付き試験、ICMP通知、MSS調整、トンネルMTUを確認する。

問99 OSPFネイバーはまだFullと表示されているが、同じ次ホップとのBFDセッションがDownになり実通信も停止している。最も適切な解釈はどれか。
ア．BFDが転送経路障害をOSPF Helloより早く検出している可能性がある
イ．BFD Downなら必ずDNS障害である
ウ．OSPF Fullならデータプレーン障害は絶対にない
エ．BFDは時刻同期プロトコルである
正答：ア
4肢解説
ア：正しい。BFDは短い周期で転送経路の生存性を検出し、ルーティングプロトコルへ障害を通知できる。
イ：BFDは転送経路監視である。
ウ：制御プレーン状態と転送経路状態が一時的に乖離する場合がある。
エ：NTPとは異なる。
総合解説：障害切り分けでは制御プレーンとデータプレーンの監視結果を分けて確認する。

問100 社内PCではapp.example.jpが10.0.0.20を返すが、VPN利用者では203.0.113.20を返して接続失敗する。最初に確認すべきものはどれか。
ア．全利用者のMACアドレスを変更する
イ．VPN利用者が参照するDNSサーバとsplit DNSのビュー・検索経路
ウ．光トランシーバの波長だけを確認する
エ．BGP MEDだけを確認する
正答：イ
4肢解説
ア：名前解決結果とは無関係である。
イ：正しい。利用場所によって異なるDNSビューを参照している可能性がある。
ウ：DNS応答差異を説明しない。
エ：名前解決値の違いが先に疑われる。
総合解説：VPN障害ではDNSサーバ配布、検索ドメイン、split-horizon設定を確認する。

問101 2台のルータ間でOSPFがExStart/Exchange付近を繰り返し、IP疎通は可能である。両端でインタフェースMTUが異なる。最も適切な原因分析はどれか。
ア．DNSのTTL不一致がOSPF DBD交換を止めている
イ．TCP MSSが小さいためOSPFがExStartになる
ウ．DBD交換時のMTU不一致が隣接関係確立を妨げている可能性が高い
エ．NTP stratumが違うため必ずExStartになる
正答：ウ
4肢解説
ア：DNSはOSPF隣接形成に使わない。
イ：OSPFはTCPを使用しない。
ウ：正しい。OSPFではDatabase Description交換時にMTU差異が隣接確立へ影響する実装がある。
エ：通常のOSPF隣接条件ではない。
総合解説：OSPF隣接障害はHello条件だけでなくMTU、認証、ネットワーク種別、DBD交換ログまで確認する。

問102 端末側pcapではTCP SYNを3回送信、本社入口FWではSYNを受信、サーバ側pcapではSYNが一度も見えない。FWログにはpolicy denyが記録されている。最も適切な結論はどれか。
ア．端末のNIC故障が原因でSYNが送信されていない
イ．サーバがSYN-ACKを返しているが端末だけ見えていない
ウ．DNSだけが原因である
エ．端末からFWまでは到達しているが、FWポリシーでサーバ向け通信が遮断されている
正答：エ
4肢解説
ア：端末pcapとFW受信で送信は確認できる。
イ：サーバ側ではSYN自体が到達していない。
ウ：宛先IPへのSYNは既に発生している。
エ：正しい。複数観測点とFWログが同じ原因を示している。
総合解説：障害切り分けではパケットの到達地点を複数箇所で比較し、ログと突き合わせる。

問103 ネットワーク性能指標のうち、パケットが送信元から宛先へ到達するまでの時間に直接関係するものはどれか。
ア．遅延
イ．帯域
ウ．可用性
エ．MTBF
正答：ア
4肢解説
ア：正しい。遅延は伝搬、転送、キューイング、処理時間などから構成される。
イ：単位時間当たりに送れる量の尺度であり到達時間そのものではない。
ウ：サービス利用可能な割合である。
エ：平均故障間隔である。
総合解説：性能分析では帯域、スループット、遅延、ジッタ、損失を区別する。

問104 リアルタイム音声で特に品質劣化を引き起こしやすい『パケット到着間隔のばらつき』は何と呼ばれるか。
ア．スループット
イ．ジッタ
ウ．MTU
エ．TTL
正答：イ
4肢解説
ア：単位時間当たりの転送量である。
イ：正しい。到着間隔が不規則になると再生バッファで吸収できず音切れ等が起こる。
ウ：最大転送単位である。
エ：IPパケットのホップ制限である。
総合解説：音声・映像では平均遅延だけでなくジッタと損失も重要である。

問105 同じ1Gbit/sでも、小さいパケットを大量に転送する方がネットワーク装置CPUへ高い負荷を与える場合がある主な理由はどれか。
ア．小さいパケットほど必ず光出力が低下するため
イ．小さいパケットではIPアドレスが消えるため
ウ．1秒当たりに処理するパケット数（pps）が増えるため
エ．小さいパケットはDNSでしか転送できないため
正答：ウ
4肢解説
ア：物理光出力とは無関係である。
イ：IPヘッダは存在する。
ウ：正しい。パケットごとに検索・ACL・NAT等の処理が必要な装置ではpps性能が制約になる。
エ：誤りである。
総合解説：性能評価はbpsだけでなくpps、セッション数、暗号処理など複数資源を見る。

問106 回線エラーは0だが、出力キューdropが増え、利用率が長時間90%を超えている。最も適切な分析はどれか。
ア．受信光レベル劣化だけが原因と断定する
イ．DNSキャッシュ不足
ウ．NTP時刻差
エ．物理障害よりも出力側輻輳によるキューあふれが疑われる
正答：エ
4肢解説
ア：物理エラーが0という情報と整合しにくい。
イ：出力キューdropの直接原因ではない。
ウ：輻輳とは無関係である。
エ：正しい。CRC等がなく高利用率とqueue dropが連動するなら輻輳が有力である。
総合解説：エラー系カウンタとdrop系カウンタを分けて見ることで物理障害と輻輳を切り分ける。

問107 5分平均の回線利用率は40%だが、スイッチの短時間キューdropが断続的に発生する。最も疑うべき現象はどれか。
ア．短時間に帯域を超えるマイクロバースト
イ．平均利用率40%なら輻輳は絶対に発生しない
ウ．DNSSEC署名検証だけが原因である
エ．VLAN数が少ないほど必ずdropする
正答：ア
4肢解説
ア：正しい。長い平均窓では短時間の瞬間的な輻輳が隠れることがある。
イ：短時間ピークは平均値に埋もれる。
ウ：キューdropを直接説明しない。
エ：一般化できない。
総合解説：高頻度Telemetryやキュー統計を使うとマイクロバーストを捉えやすい。

問108 100Mbit/sの回線でRTTが80msある。理論上この帯域を満たすために必要なTCPウィンドウの概算値として最も近いものはどれか。
ア．約10KB
イ．約1MB
ウ．約100MB
エ．RTTに関係なく1KBで十分
正答：イ
4肢解説
ア：一桁以上不足する。
イ：正しい。BDPは100Mbit/s×0.08秒=8Mbit=約1MBである。
ウ：約100倍大きい。
エ：長距離高速回線ではウィンドウがスループットを制約し得る。
総合解説：TCP性能では帯域遅延積に対して送受信ウィンドウが十分か確認する。

問109 回線利用率は60%だがTCP再送率が急増し、スループットが低下している。次に確認すべきものとして最も適切なものはどれか。
ア．DNSのSOAシリアルだけ
イ．ラックの空きU数だけ
ウ．パケット損失、遅延変動、インタフェースエラー、キューdropの有無
エ．利用者名の長さ
正答：ウ
4肢解説
ア：TCP再送の原因分析には直接関係しない。
イ：転送性能とは無関係である。
ウ：正しい。TCPは損失や大きな遅延を輻輳兆候として扱うため再送増加が性能低下につながる。
エ：TCP再送には影響しない。
総合解説：TCP性能は回線利用率だけでなく損失・RTT・再送・ウィンドウを合わせて評価する。

問110 FWのCPUが98%、セッション表も90%使用だが、WAN回線利用率は35%である。最も疑うべきボトルネックはどれか。
ア．WAN帯域だけ
イ．DNSキャッシュ
ウ．光ファイバ長
エ．FWの処理能力・セッション資源
正答：エ
4肢解説
ア：35%利用なので提示情報では優先度が低い。
イ：FW CPU・セッション表高使用を説明しない。
ウ：直接の指標が提示されていない。
エ：正しい。回線には余裕がある一方、FW内部資源が飽和に近い。
総合解説：性能ボトルネックはリンクだけでなくCPU、メモリ、セッション、暗号処理等も確認する。

問111 通信経路上に1Gbit/s回線、800Mbit/s処理上限のFW、2Gbit/s対応スイッチがある。他要因を無視した最大スループットの上限として最も近いものはどれか。
ア．800Mbit/s（直列要素の最小能力FWが上限）
イ．1Gbit/s（WAN回線だけを上限とみなす）
ウ．2Gbit/s（スイッチ能力だけを上限とみなす）
エ．3.8Gbit/s（各装置の容量を加算する）
正答：ア
4肢解説
ア：正しい。直列経路では最も小さい処理容量が上限になる。
イ：FW上限800Mbit/sを超えられない。
ウ：さらに大きく、FWが制約となる。
エ：各容量を加算するものではない。
総合解説：エンドツーエンド性能は経路上の最小容量要素とプロトコル効率に制約される。

問112 500Mbit/s回線、RTT 100msの経路で、TCP受信ウィンドウが1MBに固定されている。損失なしと単純化した場合、ウィンドウによるスループット上限として最も近いものはどれか。
ア．約8Mbit/s（1MBを8Mbitへ換算後さらに10で割る）
イ．約80Mbit/s（8Mbit÷0.1秒で計算）
ウ．約500Mbit/s（受信ウィンドウ制約を無視して回線容量を採用）
エ．約800Mbit/s（ウィンドウ計算を誤り回線容量も超える）
正答：イ
4肢解説
ア：10分の1である。
イ：正しい。1MB×8=8Mbit、8Mbit÷0.1秒=80Mbit/sである。
ウ：ウィンドウ制約を無視している。
エ：回線容量も超えている。
総合解説：高帯域・高RTT経路ではウィンドウサイズが不足すると回線帯域を使い切れない。

問113 変更作業におけるロールバックの目的として最も適切なものはどれか。
ア．問題原因を隠すためログを削除する
イ．変更を必ず最後まで継続する
ウ．変更後に重大な問題が発生した際、既知の正常状態へ戻してサービスを復旧する
エ．全設定を初期化することだけ
正答：ウ
4肢解説
ア：原因分析を妨げる。
イ：障害を拡大する可能性がある。
ウ：正しい。変更前の構成・ソフトウェア状態へ戻すことで影響時間を抑える。
エ：ロールバックは事前状態への復帰である。
総合解説：ロールバックには戻し対象、手順、所要時間、判定基準を事前に定義する。

問114 設定変更前に取得する『既知の正常設定』バックアップで重要な条件はどれか。
ア．ファイル名がbackupなら内容確認不要である
イ．保存先を誰でも削除可能にする
ウ．設定版との互換性を確認しない
エ．対象機器・取得日時・ソフトウェア版との対応が分かり、実際に復元可能であること
正答：エ
4肢解説
ア：古い・別機器の可能性がある。
イ：復旧性を損なう。
ウ：復元失敗の原因になる。
エ：正しい。単にファイルが存在するだけでなく復旧に利用できることが必要である。
総合解説：バックアップは世代・対象・整合性・復元手順を管理する。

問115 主系障害後に待機系へ切替えてサービス復旧した。その後、修理済み主系へ計画的に処理を戻す操作は一般に何と呼ばれるか。
ア．フェイルバック
イ．フェイルオーバ
ウ．ロードバランシング
エ．ルート集約
正答：ア
4肢解説
ア：正しい。障害時のフェイルオーバ後、元または新しい主系へ戻す工程である。
イ：障害時に代替系へ切り替える操作である。
ウ：通常時の負荷分散である。
エ：経路プレフィックスをまとめる技術である。
総合解説：フェイルバックも変更作業であり、状態同期と影響確認を行う。

問116 変更計画で『主要業務エラー率が5%を超えて5分継続したら戻す』と定義した。変更後10%のエラーが7分続いている。適切な対応はどれか。
ア．原因が完全に判明するまで無期限に変更状態を維持する
イ．事前定義した条件に従ってロールバックを開始する
ウ．合意済み基準は無視し担当者の感覚だけで決める
エ．監視を停止してエラー率を見えなくする
正答：イ
4肢解説
ア：業務影響を拡大する。
イ：正しい。判断基準を超えているため、原因調査を続けるよりまずサービス復旧を優先する。
ウ：統制が失われる。
エ：問題解決にならない。
総合解説：戻し基準は数値と時間で具体化し、判断者も明確にする。

問117 ルータOS更新後に特定VPN機能が動作しなくなった。旧イメージと旧設定のバックアップがあり、業務停止が続いている。最も適切な対応はどれか。
ア．新OSのまま無期限に調査し続ける
イ．旧設定だけ新OSへ無条件適用する
ウ．互換性を確認した上で旧OS・旧設定へ戻し、サービス復旧後に原因を調査する
エ．バックアップを削除する
正答：ウ
4肢解説
ア：停止時間を長引かせる。
イ：バージョン非互換の可能性がある。
ウ：正しい。復旧手段が準備されており業務影響が続くならロールバックが合理的である。
エ：復旧手段を失う。
総合解説：ソフトウェアロールバックではブートイメージ、設定形式、ライセンス、DBスキーマ等の互換性を確認する。

問118 遠隔拠点ルータの経路設定を誤り、通常の管理IPへ到達できなくなった。復旧性を高める事前対策として最も有効なものはどれか。
ア．管理経路を本番経路1本だけに依存する
イ．管理パスワードを公開共有する
ウ．DNSだけ二重化する
エ．本番データ経路と独立した帯域外管理経路を用意する
正答：エ
4肢解説
ア：設定事故時に管理不能になりやすい。
イ：セキュリティを損なう。
ウ：ルーティング誤設定による管理断を必ず解消するわけではない。
エ：正しい。通常経路を壊してもコンソール等へ到達できれば遠隔復旧しやすい。
総合解説：重要拠点ではコンソールサーバや別回線などのOOB管理を検討する。

問119 FW、DNS、アプリを同時変更後に障害が発生した。FWだけ旧設定へ戻すと新DNS構成と不整合になることが分かっている。最も適切な対応はどれか。
ア．変更間の依存関係を確認し、整合する復旧ポイントへ一連の構成を戻す
イ．障害箇所を特定せず1台ずつランダムに戻す
ウ．依存関係はロールバックに影響しない
エ．全ログを消してから戻す
正答：ア
4肢解説
ア：正しい。個別装置だけを戻すと構成全体が不整合になる場合がある。
イ：さらに複雑な状態を作る。
ウ：複数システム変更では重要である。
エ：原因調査情報を失う。
総合解説：複合変更ではサービス単位の復旧ポイントを定義し、戻し順序を手順化する。

問120 障害対応で旧設定へロールバックしpingは復旧した。作業完了判断として最も適切なものはどれか。
ア．ping成功だけで全て正常と断定する
イ．主要業務、冗長性、監視、セキュリティ機能まで事前の正常状態へ戻ったか確認する
ウ．監視アラームを確認せず終了する
エ．利用者確認を不要とする
正答：イ
4肢解説
ア：上位サービスや冗長機能が未復旧の可能性がある。
イ：正しい。L3疎通だけでサービス全体の復旧を判断すべきではない。
ウ：潜在障害を見逃す。
エ：業務機能の最終確認が必要な場合がある。
総合解説：復旧完了は技術・業務両面のpost-checkを通して判断する。

問121 一般に、既存バージョンの脆弱性や不具合修正を主目的として提供される更新に最も近いものはどれか。
ア．メジャーアップグレード
イ．ケーブルラベル
ウ．パッチ
エ．DNSゾーン転送
正答：ウ
4肢解説
ア：大きな機能変更や互換性変更を伴うことがあり、修正だけを主目的とは限らない。
イ：ソフトウェア修正ではない。
ウ：正しい。パッチは脆弱性修正や不具合修正など、既存製品を保守するために適用される。
エ：更新プログラムではない。
総合解説：保守ではpatch、update、upgradeの影響範囲を区別し、変更リスクに応じた試験を行う。

問122 ネットワーク機器のファームウェアを定期的に保守する理由として最も適切なものはどれか。
ア．更新すると必ず回線速度が2倍になるため
イ．IPアドレスが不要になるため
ウ．全ての設定作業が永久に不要になるため
エ．脆弱性・不具合修正やハードウェア制御の改善を反映するため
正答：エ
4肢解説
ア：性能向上が保証されるわけではない。
イ：更新とは無関係である。
ウ：保守運用は継続する。
エ：正しい。ネットワーク装置でもOS/ファームウェアの既知問題を継続的に管理する必要がある。
総合解説：ファームウェア更新前にはリリースノート、既知問題、互換性、戻し方法を確認する。

問123 ネットワークOS更新前にベンダーのリリースノートを確認する主な目的はどれか。
ア．修正内容、既知不具合、互換性、アップグレード条件を把握するため
イ．装置のラック位置だけを決めるため
ウ．利用者パスワードを公開するため
エ．DNS応答を高速化するため
正答：ア
4肢解説
ア：正しい。更新対象版の変更点と制約を事前に把握することで障害を予防できる。
イ：リリースノートの主目的ではない。
ウ：不適切である。
エ：直接の目的ではない。
総合解説：保守作業では製品文書と実環境の機能利用状況を照合する。

問124 同一OSのネットワーク機器が300台ある。更新版の影響が完全には分からない場合、最も適切な展開方法はどれか。
ア．全300台を同時に無確認更新する
イ．検証環境と少数機器で先行確認し、監視しながら段階的に展開する
ウ．バックアップを取らずに更新する
エ．更新結果を監視しない
正答：イ
4肢解説
ア：未知不具合時の影響が最大化する。
イ：正しい。先行グループで問題を検出し、全体への影響を限定できる。
ウ：復旧性が低下する。
エ：問題を早期検出できない。
総合解説：パッチ・アップグレードでは段階展開と停止条件を組み合わせる。

問125 コアスイッチOSを更新すると、既存の光モジュールと管理ソフトが新OSで非対応になる可能性がある。最も適切な事前確認はどれか。
ア．装置のホスト名だけ確認する
イ．DNS TTLだけ短くする
ウ．ベンダーの互換性情報でハードウェア・モジュール・管理ソフトとの対応を確認する
エ．非対応でも本番で試して判断する
正答：ウ
4肢解説
ア：互換性判断にはならない。
イ：ハードウェア互換性とは無関係である。
ウ：正しい。OS単体だけでなく周辺部品や管理基盤の互換性が必要である。
エ：重大障害のリスクが高い。
総合解説：更新前の互換性確認は機種、モジュール、ライセンス、設定機能、管理ツールまで対象にする。

問126 冗長クラスタを停止せずに更新したい。製品が混在バージョン運用を一時的にサポートしている場合、適切な方式はどれか。
ア．全ノードを同時停止して更新することだけが唯一の方式
イ．待機系を更新せず主系だけ永久に新バージョンにする
ウ．更新後の切替え試験を省略する
エ．片系ずつ更新・健全性確認・切替えを行うローリングアップグレード
正答：エ
4肢解説
ア：可用性を維持できない。
イ：長期混在はサポート外になる可能性がある。
ウ：冗長性を確認できない。
エ：正しい。サービスを維持しながら段階的に各ノードを更新できる。
総合解説：ローリング更新では混在可能期間、状態同期、フェイルバック可否を必ず確認する。

問127 セキュリティパッチを全拠点へ配布した後に実施すべきこととして最も適切なものはどれか。
ア．適用成否、対象バージョン、主要機能、監視アラームを確認する
イ．配布開始した時点で完了とみなす
ウ．更新後はバージョン情報を確認しない
エ．監視を停止する
正答：ア
4肢解説
ア：正しい。配布処理の成功と、実際の適用・機能正常性は別途確認する必要がある。
イ：失敗や再起動待ちが残り得る。
ウ：適用確認ができない。
エ：更新後異常を見逃す。
総合解説：パッチ管理は識別・優先順位付け・適用・検証までを含む。

問128 メーカーの保守終了後もインターネット境界ルータを使い続ける最大のリスクとして最も適切なものはどれか。
ア．EOLになるとIP通信がその日に必ず停止する
イ．新しい脆弱性が見つかっても修正パッチや技術支援を受けられない可能性が高まる
ウ．EOL製品は脆弱性が絶対に存在しなくなる
エ．保守終了はラック搭載位置だけに影響する
正答：イ
4肢解説
ア：直ちに動作不能になるとは限らない。
イ：正しい。サポート終了製品はセキュリティ・障害対応上のリスクが増える。
ウ：逆に修正不能リスクが問題となる。
エ：運用・セキュリティに大きく影響する。
総合解説：ライフサイクル管理ではEOL/EOS時期を資産台帳へ持ち、余裕をもって更改計画を立てる。

問129 ベンダー文書で『v8からv11へ直接更新不可。v9.5を経由してv11へ更新すること』と指定されている。現在v8の装置を更新する最も適切な手順はどれか。
ア．v8からv11へ直接更新する
イ．設定を全削除すれば直接更新してよい
ウ．v8→v9.5で正常性確認後、v9.5→v11へ進む
エ．現在版を確認せず最新イメージだけ適用する
正答：ウ
4肢解説
ア：ベンダーが非対応としている。
イ：互換性条件は解消しない。
ウ：正しい。サポートされた中間版を経由する必要がある。
エ：アップグレードパス違反になる可能性がある。
総合解説：メジャー更新ではブートローダ、設定形式、DB変換などの都合で中間版が必要な場合がある。

問130 OS更新後に設定DB形式が自動変換され、旧OSでは新形式を読めないとベンダーが明記している。ロールバック計画として最も適切なものはどれか。
ア．新形式設定だけを保存し旧OSへそのまま戻す
イ．更新前バックアップは不要である
ウ．障害時に初めて互換性を調べる
エ．更新前の旧形式設定と旧OSイメージを別途保存し、戻し手順を事前検証する
正答：エ
4肢解説
ア：旧OSが読めないため復旧できない。
イ：ロールバック不能になる。
ウ：復旧時間が長引く。
エ：正しい。更新後の設定だけでは旧版へ戻せないため、更新前スナップショットが必要である。
総合解説：アップグレードでは前後方向の互換性と、設定・DBの不可逆変換を確認する。

問131 ネットワーク容量計画の主な目的として最も適切なものはどれか。
ア．将来の需要増加を予測し、性能要件を満たす資源を必要時期までに確保する
イ．常に最大仕様の装置へ交換しコストを考慮しない
ウ．現在の利用率だけを記録し将来予測を行わない
エ．障害発生後だけ容量を確認する
正答：ア
4肢解説
ア：正しい。帯域、ポート、CPU、セッション、ライセンス等を需要予測に基づいて管理する。
イ：過剰投資となり得る。
ウ：容量不足を事前に防げない。
エ：予防的な容量計画ではない。
総合解説：容量計画では現状、成長率、ピーク、リードタイム、冗長時容量を考慮する。

問132 平均利用率30%だが月末処理時に5時間だけ95%へ達するWAN回線がある。容量計画で重視すべき考え方はどれか。
ア．平均30%なので必ず増強不要と判断する
イ．平均値だけでなく業務上重要なピーク時間帯を評価する
ウ．最大値は常に測定誤差として捨てる
エ．月末処理を監視対象外にする
正答：イ
4肢解説
ア：ピーク時の品質問題を見逃す。
イ：正しい。短時間でもSLAへ影響するピークがあれば容量不足の可能性がある。
ウ：業務パターンによる実ピークか確認が必要である。
エ：重要業務ならむしろ確認が必要である。
総合解説：容量評価は平均・95パーセンタイル・最大・時間帯別など複数統計量を使う。

問133 容量設計で意図的に余裕を残す『ヘッドルーム』の主な目的はどれか。
ア．利用可能容量を意図的にゼロへするため
イ．DNS名前を短くするため
ウ．突発的な需要増加や障害時の負荷集中を吸収するため
エ．パケット暗号化を無効化するため
正答：ウ
4肢解説
ア：逆である。
イ：容量とは無関係である。
ウ：正しい。常時100%近くまで使う設計は変動・故障への耐性が低い。
エ：ヘッドルームの定義ではない。
総合解説：必要ヘッドルームはトラフィック変動、増設リードタイム、N-1要件で決める。

問134 現在のピークトラフィックが4Gbit/sで、年20%ずつ増加すると仮定する。2年後のピーク予測値として最も近いものはどれか。
ア．4.8Gbit/s（4×1.2で1年分だけ反映）
イ．6.4Gbit/s（増加率を単純加算して誤計算）
ウ．8Gbit/s（2年間で単純に2倍とみなす）
エ．5.76Gbit/s（4×1.2×1.2で複利計算）
正答：エ
4肢解説
ア：1年分の増加しか反映していない。
イ：単純に40%を2回足す計算ではない。
ウ：与えられた成長率からは算出されない。
エ：正しい。4×1.2×1.2=5.76Gbit/sである。
総合解説：複利的な成長予測では各年の増加を前年度値へ掛ける。

問135 48ポートスイッチで44ポート使用中、今後半年で端末が8台増える予定である。最も適切な計画はどれか。
ア．空き4ポートでは不足するため、増設・上位機種・追加スイッチを事前に計画する
イ．現在通信できているので何も準備しない
ウ．全端末を同じ1ポートへ直接接続する
エ．DNSレコードを8個追加すればポート不足が解消する
正答：ア
4肢解説
ア：正しい。将来需要8ポートに対して現在の空きは4で不足する。
イ：半年後に収容不能となる。
ウ：物理的に成立しない。
エ：物理ポート数は増えない。
総合解説：容量管理は回線帯域だけでなく物理ポート、光芯線、電源、ラック等も対象にする。

問136 FWの最大同時セッション数が100万、平常ピークが75万、障害時には別系統から20万セッションが追加流入する。評価として最も適切なものはどれか。
ア．100万未満なら余裕は必ず十分である
イ．障害時95万となり上限に近いため、余裕を考えると容量増強を検討すべきである
ウ．セッション数はFW性能と無関係である
エ．回線帯域だけ見ればよい
正答：イ
4肢解説
ア：残り5万では急増を吸収しにくい。
イ：正しい。上限内でも5%しか余裕がなく、変動や新規接続増加に弱い。
ウ：状態保持資源を消費する。
エ：FW内部資源も容量要素である。
総合解説：ステートフル装置では同時セッション、新規接続率、NATポート等も容量計画へ含める。

問137 回線増速に申込みから開通まで4か月かかる。利用率が毎月増えており3か月後に上限到達予測である。最も適切な対応はどれか。
ア．上限到達してから申請する
イ．利用率監視を停止する
ウ．上限到達前に間に合わないため、直ちに増速手配や暫定対策を開始する
エ．DNS TTLを短くすれば回線増速できる
正答：ウ
4肢解説
ア：少なくとも4か月容量不足が続く。
イ：問題を見えなくするだけである。
ウ：正しい。容量逼迫時期より調達リードタイムが長いため先行対応が必要である。
エ：物理容量は増えない。
総合解説：容量計画は予測値だけでなく調達・工事・承認のリードタイムを含める。

問138 同一型番スイッチが大量にあり、2年後にメーカー保守終了予定である。最も適切な管理はどれか。
ア．保守終了日まで何も調査しない
イ．保守終了後に初めて資産台帳を作る
ウ．全機器を同一日に無計画交換する
エ．台数・設置場所・依存サービスを把握し、予算と作業期間を確保して段階更改する
正答：エ
4肢解説
ア：更改が間に合わない可能性がある。
イ：遅すぎる。
ウ：業務影響と作業資源が大きい。
エ：正しい。大量機器のEOL対応は調達・工事・移行に時間がかかるため早期計画が必要である。
総合解説：ライフサイクル管理は資産台帳、サポート期限、脆弱性、予備品を組み合わせる。

問139 2本の10Gbit/s回線で平常時均等分散している。現在総ピーク12Gbit/sで、1年後に25%増える予測である。1本故障時も全量を残り1本で処理する要件を満たすか。
ア．満たさない。1年後は15Gbit/sとなり、残り1本の10Gbit/sを超える
イ．満たす。平常時1本7.5Gbit/sだから問題ない
ウ．満たす。2本合計20Gbit/sだけ見ればよい
エ．判断不能。成長率は容量計画に使えない
正答：ア
4肢解説
ア：正しい。12×1.25=15Gbit/sで、N-1時の単一回線容量10Gbit/sでは不足する。
イ：障害時は全15Gbit/sが1本へ集中する。
ウ：N-1要件では1本故障時を評価する。
エ：設問条件から計算可能である。
総合解説：冗長回線の容量は平常時だけでなく、将来需要を含む障害時状態で確認する。

問140 95パーセンタイル利用率が4か月連続で60%、68%、76%、84%と増え、増速リードタイムは3か月である。適切な判断はどれか。
ア．100%になってから初めて対応する
イ．上限到達を待たず、現在の増加傾向を基に増強手続きを開始する
ウ．平均値だけ低ければトレンドは無視する
エ．増速リードタイムは容量判断と無関係である
正答：イ
4肢解説
ア：調達期間中に性能問題が発生する。
イ：正しい。直近は月約8ポイント増えており、3か月待つと高い確率で逼迫する。
ウ：ピーク指標が継続上昇している。
エ：実施時期決定に重要である。
総合解説：容量管理では閾値だけでなく傾向とリードタイムを組み合わせて予防的に判断する。

問141 ネットワーク構築完了後に作成するas-built（完成図書）の主な目的はどれか。
ア．計画段階の案だけを保存する
イ．障害時に毎回ゼロから構成を調査する
ウ．実際に導入された構成・配線・設定を正確に記録し、運用保守の基準とする
エ．設定変更後も文書は更新しない
正答：ウ
4肢解説
ア：実環境との差異が保守を困難にする。
イ：完成図書があれば迅速化できる。
ウ：正しい。設計時から変更された内容も含め実構成を残す。
エ：陳腐化する。
総合解説：完成図書は構成図、IP/VLAN、配線、機器一覧、設定基準等と同期させる。

問142 定常的な障害対応や保守作業で、担当者が同じ手順を再現できるようにする文書は何に最も近いか。
ア．論理構成図だけ
イ．資産購入伝票だけ
ウ．DNSゾーンファイルだけ
エ．ランブック／運用手順書
正答：エ
4肢解説
ア：手順や判断条件までは示さない。
イ：運用操作手順ではない。
ウ：特定サービス設定データである。
エ：正しい。具体的な確認・操作・判断・エスカレーション手順を記載する。
総合解説：ランブックは前提条件、コマンド、期待結果、異常時対応まで記載する。

問143 重大障害時の連絡先一覧で特に重要な管理項目はどれか。
ア．担当組織、役割、連絡方法、対応時間、エスカレーション順を最新に保つ
イ．担当者名だけを一度書いて永久に更新しない
ウ．障害時に初めてベンダー窓口を探す
エ．連絡先を一般公開する
正答：ア
4肢解説
ア：正しい。古い連絡先では障害時の初動が遅れる。
イ：異動・契約変更に追随できない。
ウ：復旧時間が長くなる。
エ：機密性・迷惑連絡の問題がある。
総合解説：連絡体制も構成情報と同様に定期レビューする。

問144 再発分析に役立つ障害チケットとして最も適切な記録はどれか。
ア．『直った』の一言だけ記録する
イ．発生時刻、症状、影響範囲、確認結果、実施操作、復旧時刻、原因、再発防止を記録する
ウ．実施コマンドを全て記録しない
エ．利用者影響を記録しない
正答：イ
4肢解説
ア：原因や対応過程が分からない。
イ：正しい。時系列と判断根拠が残ると後から分析・共有できる。
ウ：変更影響を追跡しにくい。
エ：優先度やSLA評価ができない。
総合解説：障害記録は個人の記憶ではなく組織知として再利用できる形にする。

問145 ネットワークOSの不具合をベンダーへ問い合わせる際、解決を早める情報として最も適切なものはどれか。
ア．『動かない』だけ送る
イ．機種とOS版を隠す
ウ．機種・OS版・構成・発生時刻・再現条件・ログ・show出力・実施済み切り分けを整理して提供する
エ．障害ログを全て削除してから問い合わせる
正答：ウ
4肢解説
ア：原因分析に必要な情報が不足する。
イ：既知不具合検索が困難になる。
ウ：正しい。再現性と環境情報があればベンダーが既知問題照合や解析を行いやすい。
エ：証拠を失う。
総合解説：問い合わせ時は機密情報を必要最小限にマスキングしつつ解析に必要な情報を提供する。

問146 ネットワーク保守で30分の停止が予定されている。利用者向け通知として最も適切な内容はどれか。
ア．『どこかで止まります』だけ通知する
イ．停止開始後に初めて通知する
ウ．技術用語だけを大量に並べ影響を書かない
エ．停止日時、影響サービス、対象利用者、想定時間、回避策、完了連絡方法を明示する
正答：エ
4肢解説
ア：影響を判断できない。
イ：計画保守の事前周知にならない。
ウ：利用者視点で理解しにくい。
エ：正しい。利用者が業務計画を調整できる情報を提供する。
総合解説：利用者向け通知は技術詳細より業務影響と行動を明確にする。

問147 機器故障時に『ベンダーへ連絡してから4時間以内に交換部品を発送』という条件を確認したい。最も直接参照すべきものはどれか。
ア．保守契約・サポートサービスレベル
イ．DNSゾーンファイル
ウ．VLAN設計書
エ．OSPF LSDB
正答：ア
4肢解説
ア：正しい。交換部品の対応時間は製品保守契約で規定される。
イ：保守対応時間は記載しない。
ウ：ベンダー配送条件とは無関係である。
エ：サポート契約情報ではない。
総合解説：サービスSLAとハードウェア保守SLAの依存関係を確認し、要求復旧時間に合う契約を選ぶ。

問148 実機ではVLAN30が追加されたが、構成図とIPアドレス表が旧状態のままである。最も適切な改善はどれか。
ア．文書は初回作成後更新しない
イ．変更完了条件に関連文書更新を含め、実機と文書の差分を定期的に照合する
ウ．実機を文書に合わせて無条件でVLAN削除する
エ．差分があっても担当者の記憶で補う
正答：イ
4肢解説
ア：運用時に誤判断を招く。
イ：正しい。変更作業と文書更新を同じプロセスで管理する。
ウ：業務要件を確認せず変更すべきではない。
エ：属人化する。
総合解説：ドキュメントも構成アイテムとして変更管理対象にする。

問149 特定OS版でのみBGPプロセスが数日に1回再起動する。再現が難しい。ベンダーへのエスカレーション資料として最も有効なものはどれか。
ア．再起動した事実だけを口頭で伝える
イ．障害後すぐ全証跡を削除する
ウ．障害時刻前後のログ・コアダンプ・CPU/メモリ推移・設定・OS版・発生頻度を時系列でまとめる
エ．OS版を伏せて一般論だけ質問する
正答：ウ
4肢解説
ア：解析情報が不足する。
イ：原因解析が困難になる。
ウ：正しい。非再現性障害では障害前後の証跡と環境情報が重要である。
エ：既知不具合との照合ができない。
総合解説：ベンダー解析へ必要な証拠を事前に定義し、障害発生時に自動収集できると有効である。

問150 監視上は正常でも、利用者から『毎朝9時だけSaaSが遅い』という報告が多数ある。最も適切な対応はどれか。
ア．監視が正常なので利用者報告を全て誤りとみなす
イ．利用者へ報告しないよう依頼する
ウ．全ネットワークを毎朝再起動する
エ．利用者報告の時間帯を基準に高粒度の回線・DNS・プロキシ・SaaS応答監視を追加して原因を検証する
正答：エ
4肢解説
ア：監視の盲点を見逃す。
イ：改善情報を失う。
ウ：原因不明のまま高リスク対応を行うことになる。
エ：正しい。監視項目や粒度が利用者体験を捉えていない可能性がある。
総合解説：運用改善では技術指標と利用者体験を結び付け、監視基準や容量計画を見直す。