問1 利用部門から『月末の受注処理が止まらないネットワークにしてほしい』という要望が出た。最初に確認すべき事項として最も適切なものはどれか。
ア．許容停止時間、対象時間帯、必要業務、同時利用規模を具体化する
イ．最初から特定ベンダーの機種を決める
ウ．全拠点を同一帯域に統一する
エ．停止時間は0秒と仮定する
正答：ア
4肢解説
ア：正しい。抽象的な要望を測定可能な可用性・性能要件へ落とし込む必要がある。
イ：要件確定前に製品を固定すると過不足が生じる。
ウ：業務負荷の差を無視している。
エ：現実的なSLA・コスト評価ができない。
総合解説：要求分析では業務影響を、停止時間・対象範囲・性能・復旧条件など具体的な指標へ変換する。

問2 1か月を30日とし、サービス停止が合計43分12秒だった。単純計算した可用性として最も近いものはどれか。
ア．99%（30日で約432分停止する水準）
イ．99.9%（43.2分停止が0.1%に相当）
ウ．99.99%（30日で約4.32分停止する水準）
エ．90%（30日で約4,320分停止する水準）
正答：イ
4肢解説
ア：停止可能時間が約432分となり大きすぎる。
イ：正しい。30日=43,200分で、停止43.2分は0.1%に相当するため可用性は約99.9%である。
ウ：停止43.2分ではなく約4.32分相当である。
エ：停止時間が約4,320分相当となる。
総合解説：可用性SLAは測定期間と除外条件を明確にし、単純な稼働率だけでなく業務影響も確認する。

問3 『既設配管は追加工事不可、切替えは日曜0〜4時、既存IPアドレスは変更不可』という条件から読み取れるものはどれか。
ア．性能要件だけ
イ．セキュリティ要件だけ
ウ．物理・時間・アドレスに関する制約
エ．制約はなく自由に再設計できる
正答：ウ
4肢解説
ア：複数種類の制約が含まれている。
イ：セキュリティ条件は明示されていない。
ウ：正しい。設計案はこれらの制約を満たす必要がある。
エ：明確な制約が三つある。
総合解説：要件定義では要求と制約を分け、満たせない場合は代替案や例外承認を検討する。

問4 『Web画面が速く表示されること』という要求をSLAへ落とし込む表現として最も適切なものはどれか。
ア．利用者が速いと感じること
イ．可能な限り高速にする
ウ．サーバCPUを常に50%以下にする
エ．通常業務時間帯の95パーセンタイル応答時間を2秒以内とする
正答：エ
4肢解説
ア：主観的で測定できない。
イ：合否判定ができない。
ウ：利用者体験のSLAを直接表していない。
エ：正しい。測定対象・時間帯・統計量・閾値が定義されている。
総合解説：性能要件は観測点、測定期間、統計量、閾値を明示する。

問5 受注システムについて『障害後2時間以内に業務再開し、最大でも15分前までのデータを戻したい』という要求がある。対応する値はどれか。
ア．RTO=2時間、RPO=15分
イ．RTO=15分、RPO=2時間
ウ．RTO=2時間、RPO=2時間
エ．RTO=15分、RPO=15分
正答：ア
4肢解説
ア：正しい。RTOは復旧目標時間、RPOは許容データ損失時間を表す。
イ：意味が逆である。
ウ：データ損失許容は15分である。
エ：復旧時間要求は2時間である。
総合解説：DR要件ではサービス復旧時間とデータ復旧時点を分けて定義する。

問6 災害時には音声通話と受注処理を優先し、動画研修は停止してもよいという条件がある。設計要件として最も適切なものはどれか。
ア．災害時も全通信を同一優先度で扱う
イ．縮退時に音声・受注トラフィックを優先できるQoSと容量を確保する
ウ．動画研修だけを最優先する
エ．QoSは使わず帯域不足時は先着順だけにする
正答：イ
4肢解説
ア：重要業務を保護できない。
イ：正しい。業務優先度を通信優先制御へ反映する。
ウ：業務要求と逆である。
エ：重要通信を守れない可能性がある。
総合解説：縮退運転要件は優先業務・停止可能業務・最低必要帯域を明確にする。

問7 月間可用性99.95%を契約する際、『毎月第2日曜1〜3時の事前通知済み保守は計算対象外』とする。重要な点はどれか。
ア．計画停止か障害かは後から任意に決める
イ．保守時間は記録しない
ウ．計画停止の定義と除外条件をSLAへ明記する
エ．除外条件は利用者へ示さない
正答：ウ
4肢解説
ア：恣意的なSLA運用になる。
イ：算定根拠を失う。
ウ：正しい。可用性の算定条件を曖昧にすると双方の評価が一致しない。
エ：合意形成できない。
総合解説：SLAは測定方法・対象時間・除外条件・報告方法まで合意する。

問8 『管理者以外はネットワーク機器へ直接ログインできないこと』という要求を実装可能な要件へする際、最も適切なものはどれか。
ア．管理IPを社内全員へ公開する
イ．共有adminアカウントを全員で使う
ウ．管理アクセスをHTTP平文だけにする
エ．管理用ゾーンを分離し、MFAと個人管理者ID、管理ACLを適用する
正答：エ
4肢解説
ア：要求を満たさない。
イ：個人追跡性と最小権限を損なう。
ウ：安全性を低下させる。
エ：正しい。主体・経路・認証・認可を具体化している。
総合解説：抽象的なセキュリティ要求はアクセス元、認証方式、権限、監査へ具体化する。

問9 利用部門は『拠点回線は絶対に停止不可』、経理部門は『回線費は現在の半額以下』、施設部門は『回線引込口は増設不可』と要求している。最も適切な進め方はどれか。
ア．優先順位と許容条件を関係者で確認し、可用性・コスト・物理制約のトレードオフを合意する
イ．技術部門だけで一つの要求を勝手に削除する
ウ．最も高価な案を採用すれば全要件を満たすと仮定する
エ．矛盾を記録せず設計へ進む
正答：ア
4肢解説
ア：正しい。全条件を無条件に満たせない可能性があるため合意形成が必要である。
イ：関係者合意がない。
ウ：物理制約は費用だけで解決できない場合がある。
エ：後工程で手戻りになる。
総合解説：事例分析では要求間の矛盾を可視化し、業務優先度と制約から代替案を比較する。

問10 拠点WANに月間99.99%の可用性が必要だが、単一回線の実績可用性は99.9%程度である。最も適切な設計検討はどれか。
ア．単一回線のままSLA表記だけ99.99%へ変更する
イ．異なる障害ドメインの複数回線や代替経路を用い、サービス全体でSLA達成可能性を評価する
ウ．回線帯域を2倍にすれば可用性も必ず99.99%になる
エ．DNS TTLだけを短くする
正答：イ
4肢解説
ア：実性能は改善しない。
イ：正しい。単一要素の可用性が要求を下回るなら冗長化と切替時間を含めて評価する必要がある。
ウ：帯域と可用性は別指標である。
エ：回線障害への直接対策ではない。
総合解説：高いSLAを求める場合は回線・装置・電源・経路の共通障害点も含めて設計する。

問11 WAN回線の時間帯別利用率が、9時35%、12時48%、15時92%、18時40%だった。最優先で詳細分析すべき時間帯はどれか。
ア．午前帯9時（利用率35%）
イ．昼帯12時（利用率48%）
ウ．午後帯15時（利用率92%）
エ．夕方帯18時（利用率40%）
正答：ウ
4肢解説
ア：35%である。
イ：48%である。
ウ：正しい。利用率92%で最も逼迫している。
エ：40%である。
総合解説：平均値だけでなく時間帯別ピークを確認するとボトルネック候補を絞りやすい。

問12 IPFIX集計で、バックアップ通信600GB、Web通信120GB、音声20GB、DNS 2GBだった。総通信量への影響が最も大きいものはどれか。
ア．Web通信
イ．音声
ウ．DNS
エ．バックアップ通信
正答：エ
4肢解説
ア：120GBでバックアップより小さい。
イ：20GBである。
ウ：2GBで最小である。
エ：正しい。データ量が最大であり、回線混雑への寄与が最も大きい。
総合解説：トラフィック内訳は総量と時間帯の両方を見て原因通信を特定する。

問13 本社は回線2本・FW2台だが、両FWの上流は1台のL2スイッチにだけ接続されている。最も重要な現状リスクはどれか。
ア．上流L2スイッチが単一障害点である
イ．回線が2本あること自体が障害原因である
ウ．FWが2台あるため可用性が下がる
エ．IPアドレス数が多すぎる
正答：ア
4肢解説
ア：正しい。回線とFWを二重化しても共通スイッチ故障で双方が利用不能になる。
イ：冗長化要素である。
ウ：通常は冗長化に寄与する。
エ：提示情報からは判断できない。
総合解説：冗長構成は装置単位でなく依存関係全体を読み取る必要がある。

問14 あるインタフェースで1時間当たりCRCエラーが0→5→40→300と増加している一方、利用率は20%前後である。最も適切な評価はどれか。
ア．高帯域利用によるキュー輻輳だけを疑う
イ．輻輳よりも物理伝送品質の劣化を疑う
ウ．DNS負荷を疑う
エ．正常傾向なので調査不要である
正答：イ
4肢解説
ア：利用率20%でCRC増加の説明として弱い。
イ：正しい。低利用率でもCRCが増えるならケーブル・光路等の物理問題が有力である。
ウ：CRCとは無関係である。
エ：急増は異常兆候である。
総合解説：利用率、drop、CRC、光レベルを組み合わせると障害種類を分けやすい。

問15 ルータに10.10.0.0/16→A、10.10.20.0/24→B、0.0.0.0/0→Cがある。宛先10.10.20.50の転送先はどれか。
ア．A
イ．C
ウ．B
エ．破棄
正答：ウ
4肢解説
ア：/16より/24が具体的である。
イ：デフォルトはより具体的な経路がない場合に使う。
ウ：正しい。最長一致により/24経路が選択される。
エ：有効な経路が存在する。
総合解説：経路表読解では管理距離等の前に、候補プレフィックスの最長一致を確認する。

問16 アプリ応答4秒のうち、DNS解決が3.2秒、TCP/TLS/HTTP処理が0.8秒だった。最初に改善対象とすべきものはどれか。
ア．HTTP本文サイズだけ
イ．Ethernet FCS
ウ．ラック電源
エ．DNS解決経路
正答：エ
4肢解説
ア：0.8秒側の要因であり優先度は低い。
イ：提示された遅延内訳と直接関係しない。
ウ：応答遅延の主要因として示されていない。
エ：正しい。全体遅延の大部分をDNSが占めている。
総合解説：ユーザ応答時間は名前解決、接続、TLS、アプリ処理へ分解して評価する。

問17 拠点からクラウドへの送信はISP-A、クラウドから拠点への戻りはISP-Bを通っている。途中に状態同期なしのFWが各回線に1台ずつある。最も懸念される問題はどれか。
ア．ステートフルFWによる戻り通信の破棄
イ．DNSのTTLが必ず0になる
ウ．Ethernet速度が自動低下する
エ．BGPが必ず停止する
正答：ア
4肢解説
ア：正しい。往復が別FWを通るためセッション状態を共有できない。
イ：無関係である。
ウ：非対称経路だけでは決まらない。
エ：経路自体は成立している。
総合解説：構成とフロー方向を合わせて読むことで、状態依存機器の問題を発見できる。

問18 同一フロアのAP6台が5GHzの同一チャネルを使用し、チャネル利用率90%、再送率25%、RSSIは良好である。最も疑うべきものはどれか。
ア．APまでの光ファイバ断
イ．同一チャネル競合による無線媒体の混雑
ウ．DNSSEC検証失敗
エ．IPアドレス枯渇だけ
正答：イ
4肢解説
ア：RSSIと接続が成立している。
イ：正しい。信号強度が良好でも同一チャネル共有で再送・待ち時間が増える。
ウ：無線再送率とは無関係である。
エ：チャネル利用率90%を説明しない。
総合解説：Wi-FiではRSSIだけでなくチャネル利用率、再送率、同一/隣接チャネル配置を確認する。

問19 毎日23時にWAN利用率が95%、FW CPUが30%、バックアップサーバ送信量が急増し、利用者通信の遅延も増える。最も有力な原因はどれか。
ア．FW CPU不足
イ．DNSサーバ停止
ウ．バックアップ通信によるWAN回線輻輳
エ．無線干渉
正答：ウ
4肢解説
ア：CPU30%で余裕がある。
イ：時系列データが示していない。
ウ：正しい。バックアップ送信増加とWAN高利用率、遅延悪化が同時刻に一致している。
エ：WAN全体の利用率上昇を説明しない。
総合解説：複数指標の時系列相関からボトルネックを推定する。

問20 現在ピーク6Gbit/s、過去12か月で毎月約0.4Gbit/s増加、回線上限10Gbit/s、増速工事に6か月必要である。最も適切な判断はどれか。
ア．現在6Gbit/sなので数年間何もしなくてよい
イ．上限到達後に増速を依頼する
ウ．平均ではなくピークなので予測には使えない
エ．約10か月で上限に達する傾向なので、増速検討を早期に開始する
正答：エ
4肢解説
ア：成長傾向とリードタイムを無視している。
イ：工事期間中に容量不足となる。
ウ：容量計画ではピーク傾向が重要である。
エ：正しい。6+(0.4×10)=10で、工事6か月を考えると早めの手配が必要である。
総合解説：現状分析は現在値だけでなく傾向と増設リードタイムを含めて読む。

問21 構成図が『利用者LAN→FW→LB→Web→AP→DB』となっている。利用者からDBへ直接接続する経路は設計上あるか。
ア．ない
イ．ある。利用者LANからDBへ直結している
ウ．ある。LBは必ずDBへ直接転送する
エ．判断不能。構成図から通信経路は読めない
正答：ア
4肢解説
ア：正しい。提示構成では利用者通信はWeb・AP層を経由し、DBへ直接到達する経路は示されていない。
イ：図にその接続はない。
ウ：提示構成ではLBの次はWebである。
エ：経路が明示されている。
総合解説：構成図では接続線と境界装置を順に追い、許可されるべき通信経路を整理する。

問22 拠点Aは10.20.0.0/16、拠点Bも10.20.0.0/16を利用している。両拠点を直接ルーティング統合する際の主な問題はどれか。
ア．IPv4では同じアドレス範囲を必ず統合できる
イ．アドレス空間が重複し、経路を一意に判断できない
ウ．DNS名が違えばIP重複は無関係である
エ．帯域を増やせば重複問題は解消する
正答：イ
4肢解説
ア：重複は問題となる。
イ：正しい。同一プレフィックスが別拠点に存在すると通常の単純ルーティングで区別できない。
ウ：転送はIPアドレスに基づく。
エ：アドレス設計の問題である。
総合解説：統合前にIP重複を一覧化し、再アドレス・NAT・VRF等の対策を検討する。

問23 ネットワーク変更で、利用部門は業務影響を判断し、情報システム部は技術実施し、情報セキュリティ部はFWルールを承認する。FWルール変更の最終承認先として最も適切なのはどこか。
ア．利用部門だけ
イ．情報システム部だけ
ウ．情報セキュリティ部
エ．全く関係のない外部利用者
正答：ウ
4肢解説
ア：業務影響判断の役割である。
イ：技術実施担当であり承認者としては示されていない。
ウ：正しい。提示された役割ではFWルール承認を担当する。
エ：役割に含まれていない。
総合解説：事例では関係者の責任・承認範囲を整理し、変更フローへ反映する。

問24 依存関係が『業務AP→認証基盤、認証基盤→DNS/NTP』となっている。障害復旧順として最も適切なものはどれか。
ア．業務AP→認証基盤→DNS/NTP
イ．認証基盤→業務AP→DNS/NTP
ウ．順序は依存関係と無関係である
エ．DNS/NTP→認証基盤→業務AP
正答：エ
4肢解説
ア：依存元から先に起動しても機能しない可能性が高い。
イ：認証基盤がDNS/NTPへ依存している。
ウ：依存関係が復旧可否を左右する。
エ：正しい。下位依存サービスから復旧する必要がある。
総合解説：構成図・依存関係表はDRや障害復旧順序の判断に利用できる。

問25 設計表ではPC用VLAN10、電話用VLAN20だが、スイッチポート設定はaccess VLAN20のみとなっている。PC通信ができない原因として最も適切なものはどれか。
ア．ポートVLAN設定が設計と不一致である
イ．DNSサーバが必ず停止している
ウ．BGP経路が必ずない
エ．電話機が存在すること自体が原因である
正答：ア
4肢解説
ア：正しい。PC用VLAN10へ収容されていない。
イ：L2設定不一致が先に疑われる。
ウ：端末収容VLANの問題である。
エ：設定不一致が本質である。
総合解説：構成表と実機設定の照合は障害・変更レビューの基本である。

問26 回線AとBは契約キャリアが異なるが、両方とも同じビル引込管路を通ることが分かった。冗長性評価として最も適切なものはどれか。
ア．契約会社が違えば物理障害も完全に独立する
イ．キャリアが異なっても物理管路が共通なら共通障害点が残る
ウ．回線速度が違えば経路も必ず別である
エ．IPアドレスが違えば共通障害はない
正答：イ
4肢解説
ア：共通管路なら独立ではない。
イ：正しい。掘削・火災等で両回線同時断となり得る。
ウ：速度と物理ルートは別である。
エ：アドレスは物理経路を示さない。
総合解説：回線台帳にはキャリア名だけでなく局舎・引込・管路・収容装置まで確認する。

問27 要求は『Web→APのTCP/8443のみ許可』だが、FW表にはWeb→AP any/any permitがある。最も適切な評価はどれか。
ア．any/anyの方が安全なのでそのままでよい
イ．8443以外も許可することが要求に含まれる
ウ．要求より広い過剰許可であり、必要最小限へ修正すべきである
エ．FW表は要件と比較する必要がない
正答：ウ
4肢解説
ア：攻撃面を広げる。
イ：提示要求と逆である。
ウ：正しい。ポート・プロトコルを限定していない。
エ：アクセス制御レビューでは比較が必要である。
総合解説：要求・構成図・FWルール表を相互照合して過剰権限を発見する。

問28 クラウド接続障害で、自社ルータまでは正常、キャリアCPEからクラウド側はマネージドサービス範囲である。次の行動として最も適切なものはどれか。
ア．証拠なしで全て自社機器を初期化する
イ．責任分界を無視して利用者だけに対応を任せる
ウ．ログを削除してから問い合わせる
エ．自社側の正常証跡を整理し、責任分界点以降をキャリア/クラウド事業者へエスカレーションする
正答：エ
4肢解説
ア：影響が大きく原因切り分けにもならない。
イ：解決が進まない。
ウ：解析情報を失う。
エ：正しい。責任境界を明確にして必要情報を渡す。
総合解説：マネージドサービスでは責任分界点と連絡経路を事前に整理する。

問29 構成図ではバックアップ通信は専用WANを使う設計だが、IPFIXでは夜間バックアップの90%がインターネット回線を通過している。最も適切な判断はどれか。
ア．実際のルーティングやバックアップ宛先設定が設計と異なる可能性を調査する
イ．IPFIXは設計図と違っていても必ず無視する
ウ．バックアップはどの回線を使っても性能に影響しない
エ．構成図があれば実際の経路確認は不要である
正答：ア
4肢解説
ア：正しい。設計図と実トラフィックに矛盾がある。
イ：実運用の証跡として重要である。
ウ：混雑原因となり得る。
エ：構成ドリフトの可能性がある。
総合解説：図面・設定・実トラフィックの三つを照合すると現状の不整合を発見しやすい。

問30 営業部はSaaS低遅延、セキュリティ部は全Web通信検査、ネットワーク部は本社回線逼迫を課題としている。整理すべき論点として最も適切なものはどれか。
ア．営業部の要求だけで全て決める
イ．本社バックホールとローカルブレイクアウト/SASE等の代替案を、遅延・検査・回線負荷で比較する
ウ．全Web通信を検査しないことで即決する
エ．本社回線を監視せず現状維持する
正答：イ
4肢解説
ア：セキュリティ・回線課題を無視する。
イ：正しい。三者の関心を同じ評価軸へ整理できる。
ウ：セキュリティ要求を無視する。
エ：既知課題を放置する。
総合解説：関係者要求は対立点と共通評価軸を可視化して代替案比較へつなげる。

問31 小規模拠点で、多少の遅延変動は許容できるが月額費用を抑えたい。拠点間通信は暗号化必須である。候補として最も適切なのはどれか。
ア．必ず高価な専用線だけを使う
イ．暗号化なしのインターネット通信
ウ．インターネット回線とIPsec VPN
エ．L2ハブだけで拠点間接続する
正答：ウ
4肢解説
ア：品質は高いがコスト制約に対して過剰となり得る。
イ：暗号化必須要件を満たさない。
ウ：正しい。低コスト回線を利用しつつIPsecで機密性・完全性を確保できる。
エ：WAN接続手段にならない。
総合解説：設計案は品質・コスト・セキュリティの評価軸で比較する。

問32 冗長サーバ2台を通常時から両方活用し、処理能力も増やしたい。最も適した構成はどれか。
ア．アクティブ・スタンバイ
イ．単一構成
ウ．コールドサイト
エ．アクティブ・アクティブ
正答：エ
4肢解説
ア：待機系を通常処理に使わない構成が基本である。
イ：冗長性と能力増強を両立しない。
ウ：サーバ負荷分散方式ではない。
エ：正しい。通常時から複数系を処理に利用できる。
総合解説：アクティブ・アクティブは資源効率に優れるが状態整合や負荷分散設計が複雑になる。

問33 全国拠点からSaaS通信を本社経由にしており、本社回線と遅延が問題になっている。セキュリティ制御をクラウドで統一できる場合の改善候補はどれか。
ア．拠点からのローカルブレイクアウト
イ．全SaaS通信をさらに遠い本社へ迂回させる
ウ．全拠点のインターネット接続を廃止する
エ．DNSだけを本社へ集中することで回線帯域を必ずゼロにする
正答：ア
4肢解説
ア：正しい。SaaSへの経路を短縮し本社バックホール負荷を減らせる。
イ：遅延と本社負荷を悪化させる。
ウ：SaaS利用要件を満たさない。
エ：SaaSデータ通信は残る。
総合解説：ローカルブレイクアウトは経路効率と分散セキュリティ制御をセットで検討する。

問34 二つのデータセンター間でL2を延伸する案と、各DCを別サブネットとしてL3接続する案を比較している。障害ドメイン縮小を最優先する場合、一般に有利なのはどれか。
ア．必ずL2延伸
イ．DCごとにL3分離する案
ウ．どちらも障害ドメインに差はない
エ．DNSサーバ数だけで決める
正答：イ
4肢解説
ア：同一L2障害ドメインを広げる。
イ：正しい。L2ブロードキャストやSTP障害の影響範囲を分離しやすい。
ウ：L2境界の有無で影響範囲が変わる。
エ：L2/L3境界の判断基準ではない。
総合解説：L2延伸はIP変更回避等の利点がある一方、障害ドメインや運用複雑性とのトレードオフがある。

問35 マルチクラウド間の東西通信が増え、全通信をオンプレミスFWへ戻すと遅延と帯域コストが大きい。最も適切な設計方向はどれか。
ア．全通信を必ずオンプレミスへ戻す
イ．セキュリティ制御を完全に廃止する
ウ．クラウド側の分散FW/セキュリティ制御を用い、必要なポリシーを中央管理する
エ．クラウド間通信を全てL2ブロードキャストにする
正答：ウ
4肢解説
ア：遅延・帯域コスト課題を解決しない。
イ：要件を満たさない。
ウ：正しい。通信経路を不必要に迂回させず、制御ポリシーの一貫性も保ちやすい。
エ：現実的でなく障害範囲も広がる。
総合解説：分散環境ではデータプレーンの近接性とポリシー統制を分けて設計する。

問36 クラウドへの通信量が安定して多く、低遅延・帯域予測性が重要である。インターネットVPNと専用クラウド接続の比較として最も適切なものはどれか。
ア．インターネットVPNは常に専用接続より遅延保証が高い
イ．専用接続なら暗号化検討は一切不要である
ウ．両者はコストも品質も完全に同じである
エ．専用接続はコストが増える場合があるが、経路・帯域の予測性を高めやすい
正答：エ
4肢解説
ア：一般化できない。
イ：機密性要件に応じ別途検討する。
ウ：異なる特性がある。
エ：正しい。要件次第で専用接続の品質面の利点が大きい。
総合解説：接続方式は帯域、遅延、可用性、暗号化、調達期間、費用を比較する。

問37 世界中の利用者へ静的コンテンツを配信し、オリジンサーバの負荷も下げたい。CDN導入の利点として最も適切なものはどれか。
ア．利用者に近いキャッシュから配信し、遅延とオリジン負荷を下げやすい
イ．全コンテンツを必ず動的に生成する
ウ．オリジンをインターネットから必ず削除する
エ．DNSを使わず世界中で同じL2セグメントを使う
正答：ア
4肢解説
ア：正しい。CDNの代表的な効果である。
イ：CDNの利点とは逆である。
ウ：構成次第で必要である。
エ：現実的でない。
総合解説：CDNはキャッシュ整合性・TLS証明書・動的コンテンツ適用範囲も検討する。

問38 複数ISP回線を拠点ごとに使い分け、SaaS向けは低遅延回線、基幹向けは安定回線を自動選択したい。候補として最も適切なのはどれか。
ア．STPだけ
イ．アプリケーションポリシーに基づくSD-WAN
ウ．DNSSECだけ
エ．単一固定回線だけ
正答：イ
4肢解説
ア：L2ループ制御でありWANアプリ経路選択には向かない。
イ：正しい。複数アンダーレイをポリシーベースで選択できる。
ウ：DNS真正性保護でありWAN経路制御ではない。
エ：複数回線の特性活用ができない。
総合解説：SD-WANは柔軟性を高める一方、コントローラ・ポリシー・アンダーレイ品質を管理する必要がある。

問39 案Aはコスト5・可用性3・運用性4、案Bはコスト3・可用性5・運用性3とする。各指標5点満点で、重みがコスト20%、可用性60%、運用性20%の場合、重み付き得点が高いのはどちらか。
ア．案A
イ．同点
ウ．案B
エ．情報不足で計算不能
正答：ウ
4肢解説
ア：重み付き得点は案Bより低い。
イ：3.6と4.2で同点ではない。
ウ：正しい。A=5×0.2+3×0.6+4×0.2=3.6、B=3×0.2+5×0.6+3×0.2=4.2である。
エ：必要な点数と重みが与えられている。
総合解説：代替案比較では重要度に応じた評価軸の重み付けを行うと意思決定を説明しやすい。

問40 小規模拠点にルータ4台・回線4本の複雑な冗長構成を導入する案があるが、現地運用者は1名で障害対応経験が少ない。最も適切な判断はどれか。
ア．冗長要素は多いほど無条件に良い
イ．冗長化は一切不要とする
ウ．運用者のスキルは設計に影響しない
エ．可用性向上だけでなく運用複雑性・誤設定リスクを含め、必要十分な冗長レベルを選ぶ
正答：エ
4肢解説
ア：運用複雑性やコストを無視している。
イ：業務要件を見ずに決めるべきではない。
ウ：運用性は重要な設計要因である。
エ：正しい。過剰な複雑性は運用品質を下げ、結果的に可用性を悪化させる場合がある。
総合解説：設計案は技術性能だけでなく人員・手順・保守能力も含めて評価する。

問41 端末が最大50台のVLANにIPv4サブネットを割り当てる。ネットワーク・ブロードキャストを除いて50台以上収容できる最小プレフィックスはどれか。
ア．/26（50台を収容できる候補）
イ．/27（通常利用可能30台の候補）
ウ．/28（通常利用可能14台の小規模候補）
エ．/30（ポイントツーポイント向けの小規模候補）
正答：ア
4肢解説
ア：正しい。/26は64アドレス、利用可能62アドレスで50台を収容できる。
イ：32アドレスで利用可能30となり不足する。
ウ：利用可能14で不足する。
エ：利用可能2で不足する。
総合解説：サブネットは必要ホスト数と将来余裕を考えて設計する。

問42 一般的なIPv6 LANセグメントへ割り当てるプレフィックス長として、標準的な設計で最も適切なものはどれか。
ア．/126（ポイントツーポイント等の特定用途候補）
イ．/64（通常LANで標準的に用いる長さ）
ウ．/96（一般LANの標準割当てではない長さ）
エ．/128（単一IPv6アドレスを示す長さ）
正答：イ
4肢解説
ア：ポイントツーポイント等の特定用途向けで一般LANの標準ではない。
イ：正しい。IPv6の通常のLANでは64ビットインタフェースIDを前提とする/64が基本である。
ウ：一般的なLAN割当てではない。
エ：単一アドレスを表す。
総合解説：IPv6ではアドレス数節約だけを目的にLANプレフィックスを細分化しすぎない。

問43 同一VLANの端末から見えるデフォルトゲートウェイを2台のルータで冗長化したい。代表的な標準プロトコルはどれか。
ア．BGP
イ．NTP
ウ．VRRP
エ．SNMP
正答：ウ
4肢解説
ア：AS間経路交換が主用途である。
イ：時刻同期である。
ウ：正しい。仮想IPを複数ルータで共有し、Master障害時にBackupが引き継ぐ。
エ：監視管理である。
総合解説：ゲートウェイ冗長化は上位経路・回線の障害も追跡する設計が重要である。

問44 4拠点に10.10.0.0/24、10.10.1.0/24、10.10.2.0/24、10.10.3.0/24を連続割当てした。これらを一つに集約する最小プレフィックスはどれか。
ア．10.10.0.0/23（10.10.0.0/24と10.10.1.0/24を包含）
イ．10.10.0.0/21（10.10.0.0〜10.10.7.255を包含）
ウ．10.10.0.0/24（最初の1拠点だけを包含）
エ．10.10.0.0/22（10.10.0.0〜10.10.3.255を包含）
正答：エ
4肢解説
ア：2個の/24しか含まない。
イ：8個の/24を含み範囲が広すぎる。
ウ：1個しか含まない。
エ：正しい。連続する4個の/24は/22で表現できる。
総合解説：連続したアドレス割当ては経路集約とルーティング規模縮小に有利である。

問45 数百拠点を単一OSPFエリアに収容してLSDB・SPF負荷が増えている。改善案として最も適切なものはどれか。
ア．Area 0を中心に複数エリアへ分割し、トポロジ情報の拡散範囲を抑える
イ．全拠点を同じL2セグメントへ統合する
ウ．OSPFを使ったままエリア番号を全て0以外にする
エ．DNSサーバを増設する
正答：ア
4肢解説
ア：正しい。マルチエリア化によりLSDB規模と計算負荷を分散できる。
イ：障害ドメインを拡大する。
ウ：Area 0との接続設計が必要である。
エ：OSPFスケーラビリティとは無関係である。
総合解説：OSPFエリア分割はアドレス集約・拠点階層と合わせて設計する。

問46 ISP-Aを通常出口、ISP-Bをバックアップ出口にしたい。自組織内のBGPでISP-A経路を優先する代表的な方法はどれか。
ア．ISP-AのAS_PATHを自分で長くする
イ．ISP-Aから学習した経路のLOCAL_PREFを高くする
ウ．ISP-A経路のLOCAL_PREFを低くする
エ．DNS TTLだけ短くする
正答：イ
4肢解説
ア：長いAS_PATHは一般に不利になる。
イ：正しい。LOCAL_PREFは自AS内の出口選択に用いられる代表的属性である。
ウ：バックアップ側を選びやすくなる。
エ：BGP出口選択とは無関係である。
総合解説：外向き経路制御と外部からの流入制御では使うBGP属性が異なる。

問47 合併した2社がどちらも10.0.0.0/8を利用しており、すぐには再アドレスできない。段階統合の暫定策として候補になるものはどれか。
ア．両社の10.0.0.0/8を同一ルーティングテーブルへ無条件統合する
イ．DNS名を変更するだけ
ウ．VRFで分離し、必要な通信だけNAT等で変換する
エ．全ルータでデフォルトルートだけ使う
正答：ウ
4肢解説
ア：宛先を区別できない。
イ：IP重複は残る。
ウ：正しい。重複空間を論理的に分離しつつ限定的な相互接続を実現できる。
エ：重複宛先の識別問題を解決しない。
総合解説：重複アドレスは再アドレスが本質解決だが、VRF/NATを移行期間の緩和策にできる。

問48 同一コストの2経路を通常時から利用し、片方障害時にもう片方へ収束させたい。設計時に確認すべき事項として最も適切なものはどれか。
ア．2経路なら自動的に全フローが50:50になると仮定する
イ．状態を持つFWの配置は考えなくてよい
ウ．片系障害時の容量は確認不要である
エ．装置のECMP対応、ハッシュ方式、状態依存装置への非対称影響、残存容量
正答：エ
4肢解説
ア：ハッシュやフロー分布に依存する。
イ：非対称経路で問題になる。
ウ：残存経路へ負荷集中する。
エ：正しい。単純に経路を2本置くだけではセッション偏りや障害時容量問題がある。
総合解説：ECMPは負荷分散と冗長化を両立できるが、フロー単位挙動を確認する。

問49 ルータAがVRRP Masterだが、AのWAN回線だけ断線した。LANインタフェースは正常なのでAがMasterのままになり通信がブラックホール化する。改善策はどれか。
ア．WAN到達性をtrackし、障害時にAのVRRP優先度を下げてBへ切り替える
イ．LAN側VRRPを無効化するだけ
ウ．DNS TTLを短くする
エ．AのVRRP優先度を常に最大に固定する
正答：ア
4肢解説
ア：正しい。ゲートウェイ自身のLAN生存だけでなく上位経路障害を冗長制御へ反映する必要がある。
イ：冗長ゲートウェイ機能を失う。
ウ：デフォルトゲートウェイ選択には影響しない。
エ：WAN障害でも切り替わらなくなる。
総合解説：FHRPは上位回線・経路の健全性を追跡することでエンドツーエンド可用性を高める。

問50 集約ルータが10.20.0.0/16を上位へ広告しているが、配下の10.20.50.0/24拠点だけ撤去された。集約経路を残す場合の注意点はどれか。
ア．集約すれば存在しない宛先にも自動的に新サーバが作られる
イ．撤去済み/24宛て通信が集約ルータまで到達してブラックホール化する可能性がある
ウ．集約経路ではブラックホールは絶対に起きない
エ．DNSが必ずその/24への通信を止める
正答：イ
4肢解説
ア：そのような機能はない。
イ：正しい。集約広告は配下すべての具体経路存在を保証しない。
ウ：具体経路欠落時に起こり得る。
エ：IP直指定等もあり保証されない。
総合解説：経路集約はルート数削減に有効だが、null routeや到達性監視を含めて設計する。

問51 VPC-AとVPC-Bを直接接続し、ルータ機器を追加せずプライベートIPで相互通信したい。CIDRは重複していない。候補として適切なのはどれか。
ア．DNS MXレコード
イ．STP
ウ．VPC Peering
エ．SNMP Trap
正答：ウ
4肢解説
ア：メール配送設定である。
イ：L2ループ制御である。
ウ：正しい。二つのVPC間を直接プライベート接続する代表的な方式である。
エ：監視通知である。
総合解説：VPC Peeringはシンプルだが、非推移性や大規模メッシュ時の運用性を考慮する。

問52 隣接する3台のAPが同一5GHzチャネルを使っており混雑している。改善の基本方針はどれか。
ア．全APを同じチャネル・最大出力に固定する
イ．SSIDを削除するだけ
ウ．DNS TTLを短くする
エ．利用可能チャネルを分散し、同一チャネル干渉を減らす
正答：エ
4肢解説
ア：競合を悪化させる可能性がある。
イ：チャネル混雑の直接対策ではない。
ウ：無線媒体には影響しない。
エ：正しい。隣接APのチャネル再利用を適切に設計する。
総合解説：無線設計ではチャネル・送信出力・AP密度を一体で調整する。

問53 Webサーバ3台をLB配下に置く。障害サーバへ新規リクエストを送らないため必要な機能はどれか。
ア．ヘルスチェック
イ．DNSSEC
ウ．VRRPだけ
エ．NTP
正答：ア
4肢解説
ア：正しい。バックエンドの正常性を監視し、異常ノードを分散対象から外す。
イ：DNS応答の真正性保護である。
ウ：ゲートウェイ冗長化である。
エ：時刻同期である。
総合解説：LB設計ではヘルスチェックの対象URL・間隔・閾値を業務状態に合わせる。

問54 VPC-AとB、BとCはPeering済みだが、AとCは接続していない。Bを経由してA-C通信を自動的に行えるか。
ア．BとPeeringしていればA-Cも必ず通信できる
イ．原則としてできないため、A-C間の接続や別のトランジット方式が必要
ウ．DNS名が同じなら自動通信できる
エ．AとCのCIDRを重複させれば通信できる
正答：イ
4肢解説
ア：非推移性に反する。
イ：正しい。VPC Peeringは推移的ルーティングを提供しない。
ウ：ルーティング接続が必要である。
エ：むしろ接続を困難にする。
総合解説：多数VPCの接続ではPeeringフルメッシュ以外のハブ型接続も検討する。

問55 多数APの企業Wi-Fiで利用者が移動するたびに長い再認証で音声が途切れる。改善検討として最も適切なものはどれか。
ア．認証を完全に廃止する
イ．全APで同一チャネルを使う
ウ．802.1X認証の安全性を維持しつつ、高速ローミング/認証キャッシュ等の対応を検討する
エ．利用者ごとに別SSIDを作る
正答：ウ
4肢解説
ア：セキュリティ要件を損なう。
イ：ローミング遅延の解決にはならず干渉を増やす。
ウ：正しい。セキュリティを下げずに再認証時間を短縮する設計が必要である。
エ：運用性が悪い。
総合解説：無線ローミングはRF設計と認証方式・端末対応を合わせて評価する。

問56 画像・CSSは世界配信したいが、注文APIは利用者ごとに動的でキャッシュさせたくない。CDN設計として適切なのはどれか。
ア．注文APIも無条件に長期キャッシュする
イ．静的ファイルも毎回遠隔オリジンから取得する
ウ．全通信をL2ブロードキャストで配信する
エ．静的コンテンツはキャッシュし、注文APIはキャッシュ対象外としてオリジンへ転送する
正答：エ
4肢解説
ア：利用者固有・最新データを誤配信する危険がある。
イ：CDNの効果を活かせない。
ウ：CDNの仕組みではない。
エ：正しい。コンテンツ特性ごとにキャッシュポリシーを分ける。
総合解説：CDN導入ではURL・HTTPメソッド・Cookie等に応じてキャッシュ適用範囲を決める。

問57 Webサーバはインターネット公開、DBは外部から直接到達不可としたい。VPC内の基本配置として最も適切なものはどれか。
ア．Webを公開側、DBをプライベート側サブネットに置き、必要なWeb/AP→DB通信だけ許可する
イ．DBにもインターネットからany/anyを許可する
ウ．WebとDBを同じ公開IPで共有する
エ．DBのルートテーブルに外部からの直接入口を必ず設ける
正答：ア
4肢解説
ア：正しい。役割ごとに到達性を分ける。
イ：最小権限に反する。
ウ：不要な露出を招く。
エ：要求と逆である。
総合解説：クラウドでもネットワークゾーニングと最小権限を適用する。

問58 複数SaaSで個別パスワード管理を減らし、退職時に一括でアクセス停止したい。設計として最も適切なものはどれか。
ア．各SaaSで共有アカウントを作る
イ．企業IdPを使ったIDフェデレーション/SSOへ統合する
ウ．パスワードを全サービスで同一にする
エ．認証を廃止する
正答：イ
4肢解説
ア：監査性と退職者管理が悪化する。
イ：正しい。企業側IDライフサイクルを複数SaaSへ反映しやすい。
ウ：漏えい時の影響を拡大する。
エ：不正アクセスを許す。
総合解説：サービス統合では認証・認可・退職者停止を中央ID基盤と連携させる。

問59 オンプレミスからクラウドへ専用接続2本を契約したが、両回線とも同一ルータ・同一キャリア局舎へ収容されている。改善として最も適切なものはどれか。
ア．2本あるため共通障害点は存在しない
イ．両回線へ同じIPアドレスを設定する
ウ．ルータ・物理経路・収容地点を可能な範囲で分離し、独立した障害ドメインにする
エ．DNS名を二つにするだけ
正答：ウ
4肢解説
ア：同一ルータ・局舎が共通点である。
イ：可用性改善にはならない。
ウ：正しい。回線本数だけ増やしても共通装置・局舎が残ると同時断リスクがある。
エ：物理障害ドメインは変わらない。
総合解説：クラウド接続のHAは論理接続だけでなく物理回線・CPE・局舎を確認する。

問60 全社Wi-FiでAP・無線コントローラは正常だが、RADIUS障害時に新規接続だけ失敗し既存接続は一部継続する。最も適切な改善はどれか。
ア．APの送信出力だけ上げる
イ．SSID名を変更する
ウ．認証を全廃する
エ．RADIUSとその依存するDNS/NTP/PKIを冗長化し、新規認証経路全体を試験する
正答：エ
4肢解説
ア：認証サーバ障害は解消しない。
イ：バックエンド可用性は改善しない。
ウ：セキュリティ要件を損なう。
エ：正しい。無線RFが正常でも認証バックエンド障害で新規接続が止まる。
総合解説：サービス統合ではフロントエンドだけでなく認証・名前解決・時刻・証明書など依存サービスを含めてHA設計する。

問61 IPv4パケットのTTLが1の状態でルータへ到着した。通常、そのルータが転送しようとした際の動作はどれか。
ア．TTLを減算した結果0となるため転送せず、ICMP Time Exceededを返す
イ．TTLを255へ戻して転送する
ウ．必ずTCP RSTを返す
エ．宛先MACを変更するだけで転送する
正答：ア
4肢解説
ア：正しい。TTLはルータ通過ごとに減算され、0になると破棄される。
イ：通常そのような動作はしない。
ウ：TTL超過はICMPで通知される。
エ：TTL期限切れなら破棄する。
総合解説：TTLはルーティングループ時の無限転送を防止し、tracerouteでも利用される。

問62 TCPヘッダでSYN=1、ACK=1のセグメントが観測された。典型的には何を示すか。
ア．正常な接続終了の最終ACKだけ
イ．接続開始要求に対するSYN-ACK応答
ウ．UDP応答
エ．DNSゾーン転送要求
正答：イ
4肢解説
ア：SYNが立っているため異なる。
イ：正しい。3ウェイハンドシェイクの第2段階で用いられる。
ウ：TCPヘッダである。
エ：TCPフラグだけからその用途は決まらない。
総合解説：TCPフラグとシーケンス・ACK番号を組み合わせると接続状態を推定できる。

問63 UDPヘッダのLengthフィールドが1200を示している。この値が表すものはどれか。
ア．IPヘッダだけの長さ
イ．Ethernetフレーム全体の長さ
ウ．UDPヘッダとUDPデータを合わせた長さ
エ．UDPデータだけの長さ
正答：ウ
4肢解説
ア：UDP LengthにはIPヘッダを含まない。
イ：L2ヘッダ等を含まない。
ウ：正しい。UDP Lengthは8バイトのUDPヘッダを含む長さである。
エ：ヘッダ8バイトも含む。
総合解説：UDPヘッダのLengthはヘッダを含むため、データ長はLength-8で求められる。

問64 IPv4パケットでMF=1、Fragment Offset=0である。最も適切な解釈はどれか。
ア．最後のフラグメントである
イ．断片化されていないことを必ず示す
ウ．IPv6のFragment Headerを示す
エ．最初のフラグメントで、後続フラグメントが存在する
正答：エ
4肢解説
ア：最後なら通常MF=0である。
イ：MF=1なので後続断片がある。
ウ：IPv4ヘッダのフィールドである。
エ：正しい。Offset=0は先頭、MF=1はMore Fragmentsを示す。
総合解説：IPv4断片化ではIdentification、MF、Fragment Offsetを合わせて再構成する。

問65 IPv6基本ヘッダのNext Headerが6である。直後に続く上位プロトコルとして最も適切なものはどれか。
ア．TCP
イ．UDP
ウ．ICMPv6
エ．OSPF
正答：ア
4肢解説
ア：正しい。IP Protocol/IPv6 Next Header値6はTCPを示す。
イ：UDPは17である。
ウ：ICMPv6は58である。
エ：IPv6基本ヘッダ値6はOSPFではない。
総合解説：IPv6ではNext Headerで拡張ヘッダまたは上位プロトコル種別を連鎖的に示す。

問66 受信側がACK=5001を返した。通常の累積ACKとして最も適切な意味はどれか。
ア．5001バイトのデータを拒否した
イ．シーケンス番号5000までを受信し、次に5001を期待している
ウ．送信側のポート番号が5001である
エ．RTTが5001msである
正答：イ
4肢解説
ア：拒否を意味しない。
イ：正しい。ACK番号は次に受信したいオクテット番号を表す。
ウ：ACK番号とポート番号は別である。
エ：ACK番号は時間ではない。
総合解説：TCPのACKは累積確認応答として受信済み範囲を示す。

問67 DNSメッセージのQRビットが1である。最も適切な意味はどれか。
ア．必ずDNSSEC検証済みである
イ．TCPで送信されたことを示す
ウ．問い合わせではなく応答メッセージである
エ．キャッシュ禁止を示す
正答：ウ
4肢解説
ア：QRはDNSSEC検証結果を示さない。
イ：トランスポートとは別である。
ウ：正しい。QR=0がQuery、QR=1がResponseである。
エ：その意味ではない。
総合解説：DNS解析ではID、QR、RCODE、Answer数等を組み合わせて問い合わせと応答を対応付ける。

問68 EthernetフレームのEtherType位置に0x8100があり、その後にTCIが続いている。最も適切な解釈はどれか。
ア．IPv4ヘッダが直接始まっている
イ．ARPヘッダが直接始まっている
ウ．TLSレコードである
エ．IEEE 802.1Q VLANタグ付きフレームである
正答：エ
4肢解説
ア：0x0800が一般的なIPv4 EtherTypeである。
イ：ARPは0x0806である。
ウ：Ethernetタグ識別子である。
エ：正しい。0x8100は一般的な802.1Q Tag Protocol Identifierとして用いられる。
総合解説：VLAN解析ではTPIDとTCI内のVLAN ID/優先度等を確認する。

問69 IPv4 Total Length=1500バイト、IPv4ヘッダ20バイト、TCPヘッダ20バイトでオプションなしとする。TCPデータ長は何バイトか。
ア．1460バイト（1500-20-20で計算）
イ．1480バイト（IPv4ヘッダ20だけを差し引く）
ウ．1500バイト（ヘッダを一切差し引かない）
エ．1440バイト（20バイトを余分に差し引く）
正答：ア
4肢解説
ア：正しい。1500-20-20=1460バイトである。
イ：TCPヘッダ20バイトを差し引いていない。
ウ：IP/TCPヘッダを含む値である。
エ：余分に20バイト差し引いている。
総合解説：IP Total LengthからIPヘッダとTCPヘッダを引くとTCPペイロード長を求められる。

問70 FW内側で送信元10.0.0.10:53000、宛先198.51.100.20:443のTCP SYNを観測し、外側では送信元203.0.113.5:62001、宛先198.51.100.20:443となっていた。最も適切な解釈はどれか。
ア．宛先NATだけが行われている
イ．送信元IPと送信元ポートがNAPTで変換されている
ウ．DNSによって送信元IPが変わった
エ．TCP再送によってポート番号が変わった
正答：イ
4肢解説
ア：宛先は変わっていない。
イ：正しい。内部のアドレス・ポートが外部側の別アドレス・ポートへ変換されている。
ウ：DNSはパケット送信元を変換しない。
エ：再送は同一接続のポートを勝手に変えない。
総合解説：内外のpcapを比較するとNAT/NAPTの変換前後を直接確認できる。

問71 TCP接続確立の標準的な順序として正しいものはどれか。
ア．ACK → FIN → SYN
イ．SYN → FIN → RST
ウ．SYN → SYN+ACK → ACK
エ．DHCPDISCOVER → DHCPOFFER → DHCPACK
正答：ウ
4肢解説
ア：接続確立の順序ではない。
イ：正常なハンドシェイクではない。
ウ：正しい。クライアントのSYN、サーバのSYN+ACK、クライアントのACKで接続を確立する。
エ：DHCPのシーケンスである。
総合解説：TCP状態遷移を理解するとpcapから接続失敗箇所を推定できる。

問72 一般的なDHCPv4の新規アドレス取得シーケンスとして正しいものはどれか。
ア．DHCPACK → DHCPDISCOVER → DHCPOFFER → DHCPREQUEST
イ．SYN → SYN+ACK → ACK → FIN
ウ．QUERY → RESPONSE → ACK → FIN
エ．DHCPDISCOVER → DHCPOFFER → DHCPREQUEST → DHCPACK
正答：エ
4肢解説
ア：順序が逆である。
イ：TCPのシーケンスである。
ウ：DHCPの標準シーケンスではない。
エ：正しい。いわゆるDORAシーケンスである。
総合解説：DHCP障害はDISCOVERが出ない、OFFERが戻らない、REQUEST/ACKが失敗する等の段階で切り分ける。

問73 TCPで片方向の送信を終了したい側が通常最初に送るフラグはどれか。
ア．FIN
イ．SYN
ウ．PSHだけ
エ．URGだけ
正答：ア
4肢解説
ア：正しい。FINは送信側がこれ以上送るデータがないことを示す。
イ：接続開始に用いる。
ウ：接続終了を示さない。
エ：緊急ポインタ関連で終了用ではない。
総合解説：TCP終了は双方向それぞれでFIN/ACKを交換するため複数状態を遷移する。

問74 端末pcapではDHCPDISCOVERを繰り返しているがDHCPOFFERが一度も返らない。最初に確認すべきものとして最も適切なのはどれか。
ア．端末がDHCPACKを拒否していることだけ
イ．DHCPサーバ/リレーへの到達性、スコープ枯渇、サーバ稼働状態
ウ．TCPのSYN再送
エ．HTTPS証明書
正答：イ
4肢解説
ア：OFFER自体が来ていない。
イ：正しい。DISCOVER送信までは動いているため、応答経路やサーバ側を確認する。
ウ：DHCPは通常UDPを利用する。
エ：IPアドレス取得前の問題である。
総合解説：DHCPの各メッセージがどこまで観測されるかで障害位置を絞る。

問75 クライアントが同じ宛先へSYNを1秒、3秒、7秒付近で再送しているがSYN+ACKもRSTも受信していない。最も適切な解釈はどれか。
ア．TCP接続は既に正常確立している
イ．サーバがFINを正常送信している
ウ．接続要求に応答がなく、経路・FW・サーバ待受け等を調査すべきである
エ．DNS名前解決が必ず成功している
正答：ウ
4肢解説
ア：SYN+ACK/ACKがない。
イ：観測されていない。
ウ：正しい。SYN再送は接続確立応答が得られていないことを示す。
エ：宛先IP取得経路は設問から判断できない。
総合解説：SYN再送の片方向性を複数観測点で追うと破棄地点を特定しやすい。

問76 TCP接続は確立したが、TLS ClientHello送信後にServerHelloが返らずタイムアウトする。最も適切な切り分けはどれか。
ア．物理リンクが必ずdownである
イ．DHCPアドレス取得が必ず失敗している
ウ．ARP要求が一度も成功していない
エ．TCP到達性より上位のTLS処理・中間装置・サーバTLS設定を確認する
正答：エ
4肢解説
ア：TCP接続確立済みなので可能性は低い。
イ：既に通信できている。
ウ：TCP接続まで成立している。
エ：正しい。3ウェイハンドシェイク後にTLS段階で止まっている。
総合解説：プロトコルシーケンスを層別に追うと障害段階を明確にできる。

問77 フルリゾルバが未知のwww.example.jpを解決する際、キャッシュがない場合の代表的な処理として適切なものはどれか。
ア．ルート→jp権威への委任→example.jp権威へたどり、最終応答を得る
イ．最初から全世界のDNSサーバへ同時ブロードキャストする
ウ．DHCPサーバへAレコードを問い合わせる
エ．OSPF LSDBから名前を解決する
正答：ア
4肢解説
ア：正しい。反復問い合わせで委任情報をたどる。
イ：DNSはそのように動作しない。
ウ：役割が異なる。
エ：DNS情報はOSPFで解決しない。
総合解説：DNSの反復解決ではキャッシュと委任情報が問い合わせ回数へ影響する。

問78 OSPFでHello交換後に双方向認識し、DBD交換へ進んでいる。状態遷移として一般に正しい流れはどれか。
ア．Full → Down → Exchange → Init
イ．Down/Init → 2-Way → ExStart/Exchange → Loading → Full
ウ．SYN → SYN+ACK → ACK
エ．Discover → Offer → Request → Ack
正答：イ
4肢解説
ア：形成順序が逆である。
イ：正しい。ネットワーク種別等により全隣接がFullになるとは限らないが代表的な形成順序である。
ウ：TCPである。
エ：DHCPである。
総合解説：OSPF障害はどの状態で停滞するかによってHello条件・MTU・LSDB同期等を切り分ける。

問79 TCP接続の両端がほぼ同時にFINを送り、双方が相手のFINへACKした。最も適切な理解はどれか。
ア．FINはクライアント側だけが送信できる
イ．両端がFINを送ると必ずRSTになる
ウ．TCPは両方向を独立に終了できるため、同時closeでも正常に状態遷移できる
エ．片側のFINで両方向が即座に強制終了する
正答：ウ
4肢解説
ア：どちらの端点も送信できる。
イ：正常な同時closeが可能である。
ウ：正しい。TCPは全二重であり両端が独立してFINを送信できる。
エ：FINは一方向の送信終了を示す。
総合解説：pcapではFIN/ACKの順序と各方向のシーケンス番号を追って正常終了か異常切断かを判断する。

問80 スマートフォンがWi-Fiからモバイル回線へ切り替わり、IPアドレスが変化したが同じQUIC接続を継続できた。これを可能にする主要な仕組みはどれか。
ア．TCPの同一4タプルが必ず維持されるから
イ．DNS TTLが0だから
ウ．Ethernet MACアドレスをインターネット全体で保持するから
エ．IP/ポートの5タプルだけでなくConnection IDで接続を識別できること
正答：エ
4肢解説
ア：IPが変化しておりTCPの典型的識別とは異なる。
イ：接続識別機構ではない。
ウ：L2 MACはルータ越しに接続識別へ使わない。
エ：正しい。QUIC Connection IDにより経路変更後も接続を関連付けられる。
総合解説：QUICはConnection IDとパス検証により接続移行をサポートする。

問81 経路表に192.0.2.0/24→A、192.0.2.128/25→Bがある。宛先192.0.2.200のパケットはどちらへ転送されるか。
ア．B
イ．A
ウ．両方へ必ず複製する
エ．破棄する
正答：ア
4肢解説
ア：正しい。192.0.2.200は両方に一致するが、より長い/25が選ばれる。
イ：/24より/25が具体的である。
ウ：通常の最長一致転送ではない。
エ：有効経路がある。
総合解説：IP転送は候補経路のうち最長プレフィックス一致を基本に選ぶ。

問82 DNS AレコードのTTLが300秒で、リゾルバが0秒時点で取得した。変更が権威DNSへ直後に反映されても、キャッシュ利用時に旧値が残る可能性がある時間は最大およそどれか。
ア．必ず0秒
イ．300秒
ウ．30日
エ．無限
正答：イ
4肢解説
ア：キャッシュがあるため即時反映とは限らない。
イ：正しい。TTL満了まではキャッシュ済み値を利用できる。
ウ：TTL 300秒からは導けない。
エ：TTLにより期限が定められる。
総合解説：DNS切替えでは事前にTTLを調整し、キャッシュ残存時間を考慮する。

問83 受信側がACKとともに受信ウィンドウ0を広告した。送信側の通常動作として最も適切なものはどれか。
ア．無制限に送信を続ける
イ．TCP接続を必ず即座にRSTする
ウ．新規データ送信を停止し、ウィンドウ再開を待つ
エ．DNS問い合わせへ切り替える
正答：ウ
4肢解説
ア：フロー制御に反する。
イ：ゼロウィンドウだけで即強制終了とはならない。
ウ：正しい。受信バッファに空きがないことを示す。
エ：TCPフロー制御とは無関係である。
総合解説：TCPは受信ウィンドウで受信側バッファの余裕を送信側へ通知する。

問84 同一宛先へ、経路Aの合計OSPF costが20、経路Bが35である。他条件が同じなら通常どちらが選ばれるか。
ア．経路B
イ．必ず両方を同等利用する
ウ．DNS応答によって決まる
エ．経路A
正答：エ
4肢解説
ア：コストが高い。
イ：コストが異なるため等コストではない。
ウ：OSPF SPFの経路選択である。
エ：正しい。OSPFはより小さい経路コストを優先する。
総合解説：OSPFでは各リンクcostの合計で最短経路を求める。

問85 他の主要属性が同じで、経路AのAS_PATH長が2、経路Bが4である。一般的なBGP選択で優先されやすいのはどちらか。
ア．経路A
イ．経路B
ウ．必ず両方同時
エ．IPアドレスの数字が大きい方
正答：ア
4肢解説
ア：正しい。AS_PATH長が短い経路が一般に優先される。
イ：AS_PATHが長い。
ウ：BGP選択では一つのbest pathを決めるのが基本である。
エ：そのような基準ではない。
総合解説：BGPはLOCAL_PREF等の前段属性が同じ場合、短いAS_PATHを優先する。

問86 TCPデータ送信後、ACKが得られず再送タイマーが満了した。送信側の一般的な動作はどれか。
ア．ACKがなくても受信済みとみなしてデータを破棄する
イ．未確認データを再送し、RTOをバックオフする
ウ．接続を必ず即座に正常終了する
エ．DNS TTLを増やす
正答：イ
4肢解説
ア：信頼性を失う。
イ：正しい。タイムアウト時は再送し、連続タイムアウトではRTOを増加させる。
ウ：通常は再送を試みる。
エ：TCP再送制御とは無関係である。
総合解説：RTO再送は損失回復の基本で、過度な再送を避けるためバックオフを行う。

問87 NAPT装置を再起動して変換テーブルが失われた。再起動前から確立していた外向きTCP接続はどうなりやすいか。
ア．既存接続は変換状態なしでも必ず継続する
イ．DNSサーバがNAPT表を自動復元する
ウ．戻りパケットを既存内部セッションへ対応付けられず、接続が切れる可能性が高い
エ．TCPは送信元IPが変わっても同一接続として必ず継続する
正答：ウ
4肢解説
ア：戻り先対応付けができない。
イ：そのような仕組みではない。
ウ：正しい。NAPTは変換状態に依存する。
エ：接続識別が変わる。
総合解説：状態を持つNAT/FWの冗長化ではセッション状態同期が重要になる。

問88 経路MTUが1400バイトなのに送信側が1500バイトIPパケットをDF付きで送り、必要なICMP通知が遮断されている。起こり得る症状はどれか。
ア．全通信が必ず正常になる
イ．DNS応答だけが常に破損する
ウ．経路MTUが自動的に1500へ増える
エ．小さい通信は通るが大きい通信が停止するPMTUブラックホール
正答：エ
4肢解説
ア：大きいパケットに問題が生じる。
イ：プロトコルに限定されない。
ウ：物理経路の制約は変わらない。
エ：正しい。断片化できずMTU情報も届かないため大きいパケットが進めない。
総合解説：PMTUD障害ではICMPフィルタやトンネルオーバーヘッドを確認する。

問89 存在しないhost.example.jpを問い合わせてNXDOMAINを受け、その直後に権威DNSへレコードを追加したが、一部利用者ではしばらくNXDOMAINが続いた。最も適切な理由はどれか。
ア．リゾルバが否定応答をnegative cacheしている
イ．Aレコード追加後は全キャッシュが即時無効化される
ウ．TCP TIME_WAITがDNS名を消している
エ．VRRP Masterが変わったから
正答：ア
4肢解説
ア：正しい。存在しないという結果も一定時間キャッシュされる。
イ：権威側変更はリゾルバの既存キャッシュを直接消さない。
ウ：無関係である。
エ：NXDOMAINキャッシュとは関係しない。
総合解説：DNS変更ではpositive cacheだけでなくnegative cachingも考慮する。

問90 高速回線でパケット損失が増えた直後、TCP送信レートが大きく低下し、その後徐々に回復している。最も適切な説明はどれか。
ア．TCPは損失時に必ず送信レートを増やす
イ．損失を輻輳兆候として輻輳ウィンドウを縮小し、その後輻輳回避で増加させている
ウ．DNSキャッシュが減ったためTCP cwndが変化する
エ．Ethernet VLAN IDが変わることで送信レートが下がる
正答：イ
4肢解説
ア：一般的な輻輳制御と逆である。
イ：正しい。TCP輻輳制御の典型的な挙動である。
ウ：直接関係しない。
エ：TCPの輻輳ウィンドウ制御とは別である。
総合解説：TCP性能分析では損失、RTT、cwnd、再送の関係を理解して挙動を推定する。

問91 インターネット公開VPN装置で、管理者操作の記録がない深夜2時に未知IPから設定ファイル取得があり、その直後に装置OS上で不審なプロセスが生成された。最も疑うべき侵入原因はどれか。
ア．VPN装置の脆弱性悪用による初期侵入
イ．社内端末のDNSキャッシュだけ
ウ．NTP時刻同期の成功
エ．正常なVRRP切替え
正答：ア
4肢解説
ア：正しい。認証された管理操作の証跡なしに公開装置上で不審処理が始まっているため、外部公開面の脆弱性悪用を優先して疑う。
イ：公開VPN装置上の不審プロセス生成を説明できない。
ウ：侵入原因ではない。
エ：設定取得や不審プロセスとは関係しない。
総合解説：外部公開装置で不審動作が始まった場合は、既知脆弱性・公開範囲・管理ログ・実悪用情報を突き合わせる。

問92 利用者Aのアカウントで、東京から正常ログインした5分後に海外IPからMFA未使用の成功ログインが発生し、その後メール転送ルールが新規作成された。最も疑うべき事象はどれか。
ア．正常なロードバランシング
イ．資格情報の窃取またはセッション乗っ取り
ウ．DNSラウンドロビン
エ．単なる回線輻輳
正答：イ
4肢解説
ア：利用者認証地理の不整合を説明しない。
イ：正しい。短時間の不自然な地理移動と、侵害後によく見られる設定変更が連続している。
ウ：メール転送ルール作成とは無関係である。
エ：認証成功や設定変更を説明できない。
総合解説：認証ログではImpossible Travel、MFA有無、端末、IP、直後の権限・設定変更を相関して評価する。

問93 ファイルサーバで大量暗号化が始まる2時間前、端末Bでメール添付の実行、PowerShell起動、SMBによる複数端末への接続が記録されている。最も自然な侵害シナリオはどれか。
ア．ファイルサーバのディスク故障だけ
イ．DNS TTL切れ
ウ．フィッシング等を起点に端末Bが感染し、横展開後にランサムウェアが実行された
エ．通常のバックアップ処理
正答：ウ
4肢解説
ア：PowerShellや横展開を説明できない。
イ：大量暗号化とは無関係である。
ウ：正しい。時系列が初期実行→スクリプト→横展開→暗号化となっている。
エ：複数端末への不審SMBと暗号化を説明しない。
総合解説：侵害原因分析では最終症状だけでなく、初期アクセスから実行・横展開・影響まで時系列を再構成する。

問94 Webアクセスログに、検索パラメータへ`' OR 1=1 --`を含む要求が大量にあり、その直後にDBから通常の100倍の行が返されていた。最も疑うべきものはどれか。
ア．ARPスプーフィング
イ．SYN flood
ウ．OSPF経路ループ
エ．SQLインジェクションの成功または試行
正答：エ
4肢解説
ア：WebパラメータとDB応答増加の説明にならない。
イ：TCP半開接続枯渇の症状ではない。
ウ：DBクエリ内容とは無関係である。
エ：正しい。入力値がSQL構文として解釈され、大量データ取得につながった可能性がある。
総合解説：アプリログ・WAF・DB監査ログを相関し、入力値がSQL命令として実行されたか確認する。

問95 社内開発コードには変更がないが、公式ビルドで取得した依存ライブラリの更新版に悪性コードが混入し、複数サーバへ同時展開された。最も近い侵害原因はどれか。
ア．ソフトウェアサプライチェーンの侵害
イ．単純なDNS障害
ウ．LANケーブル断
エ．NTP設定ミス
正答：ア
4肢解説
ア：正しい。信頼して取得した第三者依存物が侵害経路となっている。
イ：悪性コード混入を説明しない。
ウ：ソフトウェア改ざんとは無関係である。
エ：依存ライブラリ改ざんではない。
総合解説：依存関係、配布元、署名、ビルド環境、SBOM等を確認して侵害範囲を特定する。

問96 公開Webへの秒間要求数が通常の50倍となり、送信元は数万IPへ分散しているが、認証成功や設定変更の痕跡はない。最も可能性が高い事象はどれか。
ア．管理者アカウント侵害
イ．DDoSによる可用性攻撃
ウ．SQLインジェクション成功
エ．ARPスプーフィング
正答：イ
4肢解説
ア：認証・設定変更の証跡がない。
イ：正しい。大量分散トラフィックによる資源枯渇が主症状で、侵入後活動の証跡は示されていない。
ウ：DB操作の根拠がない。
エ：インターネット全体からの大量要求を説明しない。
総合解説：可用性攻撃と侵入攻撃は、トラフィック量・認証・変更・内部活動の有無を分けて評価する。

問97 侵害サーバにCVSS 9.8の脆弱性AとCVSS 8.1の脆弱性Bがある。BはCISA KEV掲載済みで、侵害時刻直前にBを狙う特徴的なHTTP要求が記録されている。初期侵入原因として優先調査すべきものはどれか。
ア．必ず脆弱性A
イ．どちらも調査不要
ウ．脆弱性B
エ．DNS設定だけ
正答：ウ
4肢解説
ア：CVSSが高いだけでは実際の侵入原因とは限らない。
イ：侵害サーバ上の既知脆弱性は重要な調査対象である。
ウ：正しい。実悪用確認と環境内の攻撃痕跡があり、侵入原因としての根拠が強い。
エ：HTTP攻撃痕跡と脆弱性情報を無視している。
総合解説：原因分析では深刻度だけでなく実悪用情報・露出・時系列・攻撃痕跡を重視する。

問98 社内Wi-Fiで一部端末だけHTTPS証明書警告が発生し、同時にデフォルトゲートウェイIPへのARP対応MACが短時間で切り替わっている。最も疑うべきものはどれか。
ア．正常なDNS負荷分散
イ．BGP経路集約
ウ．単なるNTP同期
エ．ARPスプーフィングを利用した中間者攻撃
正答：エ
4肢解説
ア：ARP対応MAC変化を説明しない。
イ：LAN内ARPとは無関係である。
ウ：証明書警告とARP変化を説明しない。
エ：正しい。L2で経路へ割り込み、TLS接続へ介入している可能性がある。
総合解説：ARP異常と証明書警告が同時発生する場合は、L2中間者攻撃と偽証明書介入を優先して確認する。

問99 08:00 VPNで退職者IDのログイン成功、08:05 踏み台端末へRDP、08:12 Domain Adminグループ変更、08:20 大量SMB接続、08:40 外部へ圧縮ファイル送信がある。最も適切な侵害シナリオはどれか。
ア．無効化漏れアカウントから侵入し、権限昇格・横展開後に情報を持ち出した
イ．単なるWAN障害
ウ．正常なバックアップ
エ．DNSキャッシュ更新
正答：ア
4肢解説
ア：正しい。時系列が初期アクセス、内部移動、権限拡大、データ収集、流出に整合する。
イ：認証・権限変更・外部送信を説明できない。
ウ：退職者IDや権限変更と整合しない。
エ：一連の侵害活動とは無関係である。
総合解説：攻撃チェーン分析では個々のアラートを主体・時刻・資産で連結する。

問100 管理サーバが侵害された。直接原因は公開RDPへの総当たり成功だったが、同サーバはMFAなし、共通管理者ID、外部公開不要という状況だった。再発防止上の根本原因として最も重視すべきものはどれか。
ア．攻撃元IPが存在したことだけ
イ．不要な管理面公開と弱い認証・アカウント管理という設計・運用上の統制不備
ウ．RDPというプロトコル自体の存在
エ．サーバ名が長かったこと
正答：イ
4肢解説
ア：攻撃者IPは変化し得て根本対策にならない。
イ：正しい。攻撃手法だけを封じても、同じ弱い管理面が残れば別手法で再侵入され得る。
ウ：安全な限定利用も可能である。
エ：侵害成立とは無関係である。
総合解説：根本原因分析では攻撃手法と、それを成立させた設計・設定・運用上の弱点を分けて考える。

問101 利用者PCからWebサーバへ接続できない。FWログに`src=10.1.1.20 dst=10.2.2.50 dpt=443 action=deny rule=105`とある。最も直接的な原因はどれか。
ア．DNS障害
イ．WebサーバのCPU不足
ウ．FWルール105によってTCP/443通信が拒否されている
エ．ARPテーブル不足
正答：ウ
4肢解説
ア：宛先IPまで特定されFWに到達している。
イ：FWで拒否されているためサーバへ届かない。
ウ：正しい。ログに対象通信とdenyアクションが明示されている。
エ：FWまで通信が到達している。
総合解説：ログに明示された送信元・宛先・ポート・アクションを事実として優先する。

問102 クライアントのSYNに対し、サーバIPから直ちにRST+ACKが返っている。経路上FWには許可ログがある。最も可能性が高いものはどれか。
ア．経路上でパケットが完全に破棄されている
イ．DNSだけが停止している
ウ．リンクが物理断している
エ．サーバ側で対象TCPポートが待受けていない
正答：エ
4肢解説
ア：RST応答が返っている。
イ：IP宛てTCP応答がある。
ウ：双方向パケットが観測されている。
エ：正しい。ホストまで到達し、閉じたポートへ接続したときの典型的応答である。
総合解説：SYNタイムアウトと即時RSTを区別すると、FW破棄とサーバ拒否を切り分けやすい。

問103 クライアントDNSログで対象名への応答がSERVFAILとなり、同時刻に上流DNSへのタイムアウトが多数記録されている。最も適切な原因候補はどれか。
ア．リゾルバが上流への問い合わせを完了できず名前解決に失敗している
イ．必ず対象名が存在しない
ウ．TCP接続が正常完了した
エ．VRRP切替え成功
正答：ア
4肢解説
ア：正しい。SERVFAILと上流タイムアウトが整合している。
イ：存在しない場合はNXDOMAINが典型である。
ウ：名前解決前の問題である。
エ：提示ログとは直接関係しない。
総合解説：DNSではNXDOMAIN、SERVFAIL、timeoutを区別して障害段階を推定する。

問104 TCPキャプチャで同じACK番号のACKが複数回続き、その後欠けていたシーケンス範囲が再送されている。最も適切な解釈はどれか。
ア．DNS応答の重複
イ．途中のTCPセグメント損失が発生し、受信側が同じ次期待番号を繰り返し通知した
ウ．正常な接続開始だけ
エ．受信側が全データを順番どおり受信した
正答：イ
4肢解説
ア：TCPシーケンス解析とは異なる。
イ：正しい。重複ACKは欠落セグメントの存在を示す典型的な兆候である。
ウ：欠落データ再送がある。
エ：同じACKの反復と再送に整合しない。
総合解説：重複ACK、再送、SACKを追うと損失箇所と回復動作を分析できる。

問105 10:01 管理者Aログイン、10:03 ACL変更、10:04 BGP neighbor down、10:05 通信障害開始というsyslogがある。最初に確認すべきものはどれか。
ア．1週間前のDNS TTLだけ
イ．ラック温度だけ
ウ．10:03のACL変更内容とBGP制御通信への影響
エ．利用者端末の壁紙
正答：ウ
4肢解説
ア：時系列上の直接性が低い。
イ：変更直後のBGP downを説明しない。
ウ：正しい。変更直後に隣接断と障害が続いており因果候補として強い。
エ：無関係である。
総合解説：変更時刻と障害発生時刻が近い場合は差分と影響範囲を優先確認する。

問106 NAPT装置ログに`port allocation failed`が急増し、内部端末のSYNは装置内側で見えるが外側へ出ていない。最も適切な原因はどれか。
ア．DNSキャッシュ枯渇
イ．サーバがRSTを返している
ウ．Wi-Fiチャネル競合
エ．NAT変換用ポート資源の枯渇
正答：エ
4肢解説
ア：NATポート割当てとは無関係である。
イ：外側へSYN自体が出ていない。
ウ：NAPTログの失敗を説明しない。
エ：正しい。変換ポート割当て失敗により外部側パケットを生成できていない。
総合解説：NAPTでは同時セッション数だけでなく利用可能ポート範囲も容量要素となる。

問107 OSPFログに`mismatched area ID`が繰り返し記録され、対向とのHelloは受信できている。最も適切な原因はどれか。
ア．両端インタフェースのOSPFエリア設定不一致
イ．物理リンク断
ウ．DNS名前解決失敗
エ．TCP MSS不一致
正答：ア
4肢解説
ア：正しい。ログがエリアID不一致を明示している。
イ：Helloを受信している。
ウ：OSPF隣接にDNSは不要である。
エ：OSPFはTCPを利用しない。
総合解説：プロトコルログの明示的な不一致メッセージを設定差分へ結び付ける。

問108 クライアントログに`certificate expired`、サーバ証明書のNotAfterが前日の日付、TCP接続自体は成功している。最も適切な原因はどれか。
ア．L1リンク断
イ．サーバ証明書の有効期限切れによるTLS検証失敗
ウ．DNS NXDOMAIN
エ．BGP経路不存在
正答：イ
4肢解説
ア：TCP接続は成功している。
イ：正しい。TCPより上位の証明書検証段階で失敗している。
ウ：サーバへ接続できている。
エ：TCP到達性がある。
総合解説：TLS障害はTCP到達性、ClientHello/ServerHello、証明書検証、暗号交渉の段階を分けて確認する。

問109 EDRで端末Cが機密フォルダを圧縮、DNSログで新規ドメイン解決、FWで同端末からそのIPへ443/TCPを4GB送信している。最も適切な判断はどれか。
ア．正常なNTP同期
イ．単なるDNSキャッシュ更新
ウ．端末CからHTTPSを利用した情報持出しの可能性が高い
エ．OSPF収束
正答：ウ
4肢解説
ア：4GB送信と圧縮処理を説明しない。
イ：大容量443通信と整合しない。
ウ：正しい。データ準備、宛先解決、大容量外部送信が連続している。
エ：端末のファイル圧縮とは無関係である。
総合解説：情報流出分析はエンドポイント、DNS、ネットワークフローを時系列で相関する。

問110 端末pcapでSYN送信、拠点FW外側でもSYN確認、本社FW外側でもSYN確認、本社FW内側では未観測。本社FWログにIPS signature hit/dropがある。原因として最も適切なものはどれか。
ア．端末NICがSYNを送っていない
イ．拠点FWで破棄されている
ウ．サーバがRSTを返している
エ．本社FW/IPSがシグネチャに一致したSYNを破棄している
正答：エ
4肢解説
ア：複数地点でSYNを観測している。
イ：その外側でも観測されている。
ウ：本社FW内側へ到達していない。
エ：正しい。最後に確認できた地点とdropログが一致している。
総合解説：複数区間のpcapと境界装置ログを組み合わせると破棄地点を特定できる。

問111 マルウェア感染端末をネットワークから隔離した。この操作の位置付けとして最も適切なものはどれか。
ア．被害拡大を抑える封じ込め
イ．恒久的な復旧完了
ウ．容量増強
エ．DNS切替え
正答：ア
4肢解説
ア：正しい。隔離は感染拡大・C2通信を止めるための初動であり、完全復旧そのものではない。
イ：感染除去や原因修正がまだ必要である。
ウ：性能対策ではない。
エ：名前解決変更ではない。
総合解説：インシデント対応では封じ込め、根絶、復旧を区別して進める。

問112 ランサムウェア被害からバックアップを使って復旧する。最初に重要な確認はどれか。
ア．最も新しいバックアップなら内容確認不要
イ．バックアップが侵害前の正常データで、マルウェアや破損を含まないこと
ウ．復旧前に全バックアップを削除する
エ．攻撃経路が残っていても即公開する
正答：イ
4肢解説
ア：侵害後データの可能性がある。
イ：正しい。感染済みバックアップを戻すと再侵害につながる。
ウ：復旧手段を失う。
エ：再侵害リスクが高い。
総合解説：復旧点は時刻だけでなく整合性・感染有無・業務整合を確認する。

問113 障害を復旧した後、同種事故を減らすために最も適切な活動はどれか。
ア．記録を削除して忘れる
イ．同じ手順を無条件に維持する
ウ．原因・対応・検知遅延をレビューし、設計・手順・監視基準へ改善を反映する
エ．担当者個人だけに記憶させる
正答：ウ
4肢解説
ア：再発防止知識を失う。
イ：既知の弱点を残す。
ウ：正しい。復旧だけで終わらず教訓を統制へ戻す。
エ：属人化する。
総合解説：Post-incident reviewで得た知見をポリシー・ランブック・監視・教育へ反映する。

問114 管理者アカウントの窃取が確認された。復旧手順として最も適切なものはどれか。
ア．パスワードは変えず利用継続する
イ．アカウント名だけ変更する
ウ．ログを削除して復旧扱いにする
エ．アカウントを無効化し、関連セッション・トークンを失効させ、認証情報を安全に再発行する
正答：エ
4肢解説
ア：攻撃者が再利用できる。
イ：資格情報・セッション問題が残る。
ウ：侵害状態は解消しない。
エ：正しい。パスワード変更だけでは既存セッションやトークンが残る場合がある。
総合解説：資格情報侵害ではアカウント、セッション、APIキー、証明書等の失効範囲を確認する。

問115 公開機器の既知脆弱性が侵入経路だった。攻撃元IPを遮断した後の恒久対策として最も適切なものはどれか。
ア．脆弱性を修正し、侵害有無を確認した上で公開範囲・監視・認証も見直す
イ．攻撃元IP遮断だけで完了とする
ウ．パッチ適用後は侵害痕跡調査不要とする
エ．公開範囲をさらに広げる
正答：ア
4肢解説
ア：正しい。IPブロックだけでは攻撃元変更で再侵入され得る。
イ：根本原因の脆弱性が残る。
ウ：既に侵害済みかもしれない。
エ：攻撃面を拡大する。
総合解説：恒久対策は脆弱性修正と、露出・認証・検知の多層改善を組み合わせる。

問116 ACL変更直後に業務通信が停止し、事前バックアップと戻し手順がある。原因分析に30分以上かかる見込みで、SLA上10分以内の復旧が必要である。最適な判断はどれか。
ア．原因が完全に分かるまで障害状態を維持する
イ．まず承認済み旧設定へロールバックしてサービスを復旧し、その後に原因分析する
ウ．設定バックアップを削除する
エ．全装置を初期化する
正答：イ
4肢解説
ア：SLA違反を拡大する。
イ：正しい。復旧SLAを優先し、既知正常状態へ戻せる条件が揃っている。
ウ：復旧手段を失う。
エ：影響が大きく不要である。
総合解説：障害復旧ではサービス回復と根本原因分析を分離し、戻し条件を事前定義する。

問117 侵害端末を再イメージし資格情報も更新した。復旧直後の運用として最も適切なものはどれか。
ア．復旧したので監視を停止する
イ．全ログを削除する
ウ．一定期間は関連IOC、認証、外部通信、権限変更を重点監視する
エ．同じ侵入経路を再公開する
正答：ウ
4肢解説
ア：再侵害を見逃す。
イ：比較・検知根拠を失う。
ウ：正しい。根絶漏れや再侵入を早期発見するため監視強化が必要である。
エ：再発リスクが高い。
総合解説：復旧は通常運用へ戻す過程であり、しばらく監視強度を上げることが有効である。

問118 毎回FW変更時に担当者が手作業で100行を入力し、過去3回誤入力による障害が起きている。再発防止として最も適切なものはどれか。
ア．注意するよう口頭で伝えるだけ
イ．レビューを廃止する
ウ．変更履歴を残さない
エ．テンプレート化・自動検証・レビュー・自動投入を組み合わせて手作業を減らす
正答：エ
4肢解説
ア：同じ作業構造が残る。
イ：誤り検出機会を減らす。
ウ：原因追跡を困難にする。
エ：正しい。再発性のある人的ミスはプロセス・自動化で構造的に減らすべきである。
総合解説：再発防止は個人注意だけでなく、仕組み・自動化・検証へ改善を落とし込む。

問119 認証基盤、ファイル共有、受注Webが侵害された。認証基盤が他2サービスの前提で、受注WebのRTOは1時間、ファイル共有は8時間である。最も適切な復旧順序はどれか。
ア．認証基盤を安全に復旧し、その後受注Web、最後にファイル共有を復旧する
イ．ファイル共有→受注Web→認証基盤
ウ．受注Webだけ先に復旧し認証基盤は後回し
エ．三つを無計画に同時復旧する
正答：ア
4肢解説
ア：正しい。依存関係とRTOの両方を満たす順序である。
イ：依存関係とRTOに反する。
ウ：前提サービスがないため正常利用できない。
エ：限られた要員・依存関係を考慮していない。
総合解説：復旧優先度は業務重要度、RTO、依存関係、セキュリティ確認を統合して決める。

問120 過去5件の障害で平均検知時間は2分、平均復旧時間は3時間、そのうち2時間は担当者が復旧手順を探す時間だった。改善優先度として最も適切なものはどれか。
ア．監視頻度だけをさらに上げる
イ．復旧ランブック整備・演習・自動化により復旧判断と操作時間を短縮する
ウ．ログ保持を短くする
エ．手順を文書化しない
正答：イ
4肢解説
ア：主要遅延は検知後にある。
イ：正しい。検知は速い一方、復旧手順探索が主要ボトルネックである。
ウ：復旧時間短縮にはつながらず調査性を損なう。
エ：ボトルネックを残す。
総合解説：事後レビューではMTTD・MTTRを分解し、最も大きい工程へ改善投資する。

問121 本社WANの平常時利用率は35%だが、毎日18〜19時だけ95%となり、その時間帯だけ利用者のWeb応答が遅くなる。FW CPUは30%、サーバCPUは40%である。最も有力なボトルネックはどれか。
ア．FW CPU
イ．WebサーバCPU
ウ．WAN回線帯域
エ．DNS TTL
正答：ウ
4肢解説
ア：30%であり主要制約とは考えにくい。
イ：40%で余裕がある。
ウ：正しい。性能劣化時間とWAN高利用率が一致し、FW・サーバには余裕がある。
エ：時間帯別のWAN高利用率と整合しない。
総合解説：総合性能分析では、症状発生時刻と各資源の利用率を相関して制約点を特定する。

問122 2台のFWで通常時6Gbit/sずつ処理し、1台当たり最大10Gbit/sである。1台故障時も現在の総負荷12Gbit/sを処理する必要がある。評価として正しいものはどれか。
ア．2台合計20Gbit/sなので満たす
イ．通常時6Gbit/sなので1台でも余裕がある
ウ．帯域計算ではFW性能を考えなくてよい
エ．1台では2Gbit/s不足し、N-1要件を満たさない
正答：エ
4肢解説
ア：N-1では1台故障時の残存能力を見る。
イ：障害時は12Gbit/sが集中する。
ウ：処理上限が明示されている。
エ：正しい。障害時は12Gbit/sが1台へ集中するが、最大10Gbit/sしか処理できない。
総合解説：冗長構成の容量評価は平常時だけでなく障害時の負荷集中を確認する。

問123 1か月の95パーセンタイル回線利用率が88%、平均利用率は42%、最大は100%だった。増速判断で最も適切な見方はどれか。
ア．平均値だけでなく、継続的に高い95パーセンタイル値を重視する
イ．平均42%なので増速検討は不要と断定する
ウ．最大100%だけを見て必ず即時2倍へ増速する
エ．95パーセンタイルは性能分析に使えない
正答：ア
4肢解説
ア：正しい。短い瞬間値だけでなく、持続的なピーク傾向を示す指標として有用である。
イ：ピーク時間帯の逼迫を見落とす。
ウ：継続性や業務影響も確認すべきである。
エ：容量評価で広く使われる。
総合解説：容量計画では平均・95パーセンタイル・最大・時間帯・成長率を組み合わせる。

問124 1Gbit/s回線、RTT 100ms、パケット損失0.5%のWANで、大容量TCP転送が100Mbit/s程度しか出ない。回線利用率にも余裕がある。最も適切な分析方向はどれか。
ア．回線容量が1Gbit/sなので必ず1Gbit/s出ると判断する
イ．TCPウィンドウ、損失による再送・cwnd低下、RTTの影響を確認する
ウ．DNS TTLだけを変更する
エ．VLAN IDを変更する
正答：イ
4肢解説
ア：プロトコル効率と損失を無視している。
イ：正しい。帯域だけではなくTCPのウィンドウ・損失・RTTが実効スループットを制約し得る。
ウ：大容量TCP転送の制約とは直接関係しない。
エ：TCPスループット改善の根拠がない。
総合解説：高帯域・高RTT経路ではBDPと受信ウィンドウ、損失率、再送を合わせて評価する。

問125 1分平均のスイッチポート利用率は50%以下だが、VoIP品質低下時に数ミリ秒単位のキュー使用率が100%となりdropが発生している。最も適切な判断はどれか。
ア．平均利用率50%以下なので輻輳は絶対にない
イ．VoIP品質はキューdropと無関係である
ウ．平均値では見えないマイクロバーストが品質劣化を起こしている
エ．DNSサーバ増設が直接解決する
正答：ウ
4肢解説
ア：短時間ピークを無視している。
イ：損失・遅延変動の影響を受ける。
ウ：正しい。短時間の瞬間的輻輳は長い平均窓では隠れる。
エ：L2/L3キュー輻輳の対策ではない。
総合解説：高頻度Telemetryやキュー統計を使うと短時間の性能問題を把握しやすい。

問126 FWのCPUは40%、回線利用率は50%だが、同時セッション数が上限の98%に達した時間だけ新規接続が失敗する。ボトルネックとして最も適切なのはどれか。
ア．WAN帯域
イ．FW CPU
ウ．DNSキャッシュ
エ．FWのセッション管理容量
正答：エ
4肢解説
ア：50%で余裕がある。
イ：40%で主要制約とは考えにくい。
ウ：新規接続失敗とセッション上限の一致を説明しない。
エ：正しい。CPUや帯域ではなく状態テーブルが上限に近い。
総合解説：状態を持つ装置ではCPU・帯域だけでなく同時セッション、新規接続率、NATポートも容量要素となる。

問127 会議室でRSSIは-50dBmと良好だが、50台接続時だけ遅延が増え、チャネル利用率95%、再送率20%となる。最も適切な改善方向はどれか。
ア．AP/チャネル容量を増やし、セル設計・チャネル再利用・端末分散を見直す
イ．送信出力をさらに最大化するだけ
ウ．DNS TTLを短くする
エ．同一チャネルのAPをさらに追加する
正答：ア
4肢解説
ア：正しい。信号強度ではなく共有媒体の容量が不足している。
イ：干渉範囲を広げる可能性がある。
ウ：無線媒体容量は増えない。
エ：競合を増やす可能性がある。
総合解説：無線性能はRSSIだけでなく端末密度、airtime、再送、チャネル利用率で評価する。

問128 4台のWebサーバのうち1台だけCPU95%、残りは30%以下である。LB設定ではsource-IP hashと長時間セッション維持が有効で、大口顧客1社の通信量が全体の45%を占める。原因として最も適切なものはどれか。
ア．全サーバのCPUが不足している
イ．ハッシュキーとセッション維持により大口顧客の通信が1台へ偏っている
ウ．WAN回線が必ず飽和している
エ．DNSSEC検証がCPU偏りを作っている
正答：イ
4肢解説
ア：残り3台には余裕がある。
イ：正しい。source-IP単位の固定により大きな送信元が特定ノードへ集中し得る。
ウ：提示情報からは判断できない。
エ：LB分散条件が直接原因として示されている。
総合解説：負荷分散アルゴリズムは実際のクライアント分布・セッション特性に合わせて選ぶ。

問129 経路上に、WAN 2Gbit/s、FW 1.5Gbit/s、暗号VPN装置 1.2Gbit/s、LAN 10Gbit/sが直列にある。他要因を無視した理論上の最大スループット上限はどれか。
ア．1.5Gbit/s（FW能力だけを最小とみなす）
イ．2Gbit/s（WAN回線能力を上限とみなす）
ウ．1.2Gbit/s（直列要素の最小能力VPN装置が上限）
エ．14.7Gbit/s（各要素の容量を加算する）
正答：ウ
4肢解説
ア：VPN装置1.2Gbit/sが先に制約になる。
イ：FWとVPN装置の上限を超える。
ウ：正しい。直列経路では最も小さい処理能力が上限になる。
エ：直列要素の容量を加算しない。
総合解説：性能分析ではエンドツーエンド経路上の各要素の最大能力を並べて最小値を特定する。

問130 現在ピーク8Gbit/s、年30%増、回線は2本各10Gbit/sで通常時分散、1本故障時も全量処理が必要、増速工事に9か月かかる。1年後を見据えた最も適切な判断はどれか。
ア．2本合計20Gbit/sなので増強不要
イ．1年後も8Gbit/sなので問題ない
ウ．10.4Gbit/sは10Gbit/s未満なので問題ない
エ．1年後ピーク10.4Gbit/sとなり単一10Gbit/sを超えるため、N-1要件維持の増強を早期に開始する
正答：エ
4肢解説
ア：N-1では1本故障時を評価する。
イ：成長率を無視している。
ウ：大小関係が逆である。
エ：正しい。8×1.3=10.4Gbit/sで、工事9か月を考えると先行手配が必要である。
総合解説：容量計画は将来需要、冗長時状態、調達リードタイムを同時に評価する。

問131 100拠点を新WANへ移行する際、まず3拠点だけ先行移行する主な目的はどれか。
ア．小さい影響範囲で設計・手順・運用上の問題を発見する
イ．全拠点を同時停止するため
ウ．テストを省略するため
エ．旧ネットワークを直ちに廃止するため
正答：ア
4肢解説
ア：正しい。先行拠点で問題を洗い出し、全体展開前に修正できる。
イ：段階移行の目的と逆である。
ウ：先行移行は実地検証の役割を持つ。
エ：切戻し余地を残すのが一般的である。
総合解説：大規模移行ではpilot/canary、段階展開、停止条件、ロールバックを組み合わせる。

問132 コアルータ更改前に設定・ライセンス・OSイメージを保存する最大の理由はどれか。
ア．新機器のCPUを高速化するため
イ．障害時に旧環境へ戻すための復旧材料を確保する
ウ．DNSを不要にするため
エ．変更履歴を消すため
正答：イ
4肢解説
ア：バックアップは性能向上機能ではない。
イ：正しい。設定だけでなく起動に必要なソフトウェア・ライセンスも戻しに必要となる場合がある。
ウ：無関係である。
エ：むしろ追跡性を高める。
総合解説：移行前には復元可能性まで確認したバックアップを準備する。

問133 新ネットワークの受入テストで最も重要な判定基準はどれか。
ア．ベンダー担当者が成功と言えば合格
イ．最も良い1回の結果だけを採用する
ウ．事前に合意した機能・性能・可用性・セキュリティ要件を満たすこと
エ．本番障害が起きるまでテストしない
正答：ウ
4肢解説
ア：客観的な合意基準が必要である。
イ：再現性を無視している。
ウ：正しい。受入は契約・要求仕様への適合性を判断する。
エ：受入前に確認すべきである。
総合解説：受入テストは要件トレーサビリティと測定可能な合否基準を持たせる。

問134 WebサービスのIPを切り替える予定で、現在DNS TTLは86400秒である。切替え時の旧IP残存を減らしたい。適切な事前対応はどれか。
ア．切替え直後にだけTTLを短くする
イ．TTLをさらに長くする
ウ．DNSを使わず全利用者にARPを配布する
エ．十分前からTTLを短縮し、そのTTLが旧キャッシュから消化された後にIPを切り替える
正答：エ
4肢解説
ア：既存キャッシュの旧TTLには効かない。
イ：旧IP残存時間を長くする。
ウ：インターネットサービスの名前解決代替にならない。
エ：正しい。直前にTTLを変えても既存キャッシュには旧TTLが残る。
総合解説：DNS移行はTTL変更の事前期間、旧環境併存、キャッシュ収束を考慮する。

問135 FW更改作業で、計画上『主要API成功率が99%未満になれば切戻し』としている。切替え後96%が10分継続した。最も適切な判断はどれか。
ア．事前条件に従い切戻しを開始する
イ．原因が完全特定するまで障害状態を維持する
ウ．成功率96%でも担当者が問題ないと感じれば継続する
エ．監視を停止して成功率を計測しない
正答：ア
4肢解説
ア：正しい。合意した中断基準を満たしている。
イ：利用者影響を拡大する。
ウ：客観基準を無視している。
エ：判断根拠を失う。
総合解説：変更計画は中断条件・判断者・ロールバック手順を具体化する。

問136 旧ネットワークと新ネットワークを1週間並行稼働させる主な利点はどれか。
ア．必ずコストが最小になる
イ．新環境の不具合時に旧環境へ戻しやすく、実トラフィックで比較検証できる
ウ．旧環境を即時撤去できる
エ．テストが不要になる
正答：イ
4肢解説
ア：二重運用期間のコストは増える。
イ：正しい。切戻し余地と比較観測を確保できる。
ウ：並行稼働とは逆である。
エ：実地確認は必要である。
総合解説：並行稼働は安全性を高める一方、二重管理・データ整合・コストを考慮する。

問137 コアスイッチOS更新ではルーティング機能に変更はないとされるが、同機器でOSPF、VRRP、LACP、SNMPを利用している。適切なテスト範囲はどれか。
ア．新機能を使わないので起動確認だけでよい
イ．OSPFだけ確認すれば十分
ウ．利用中の主要機能すべてについて回帰テストを行う
エ．テストは本番障害後に行う
正答：ウ
4肢解説
ア：既存機能への影響を見逃す。
イ：他の重要機能も利用している。
ウ：正しい。OS更新は共通基盤変更であり、既存機能へ副作用があり得る。
エ：受入前に確認すべきである。
総合解説：変更影響分析から重要な既存機能を回帰テストへ含める。

問138 合併会社の重複IPを解消するため、新アドレスへ段階変更する。移行期間中に旧・新アドレス利用端末が混在する。最も適切な設計はどれか。
ア．全端末のIPを無記録でランダム変更する
イ．DNSだけ変更し端末IPは重複したままにする
ウ．移行期間の旧新通信を考慮しない
エ．移行期間のルーティング/NAT/DNS整合を設計し、グループ単位で切替えと検証を行う
正答：エ
4肢解説
ア：障害切り分けが困難になる。
イ：IP重複問題は解消しない。
ウ：業務断が発生し得る。
エ：正しい。混在期間の通信経路と名前解決を明確にする必要がある。
総合解説：再アドレス移行はアドレス、経路、DNS、ACL、NATの依存関係をまとめて変更する。

問139 新FWへ切替えると同時に、DNSの公開IP、LBのバックエンド、Webサーバのデフォルトgwも変更する必要がある。最も適切な移行計画はどれか。
ア．依存関係を整理し、各変更の前提・確認点・切戻し順を明示した一貫した手順を作る
イ．変更順序を当日の担当者判断だけに任せる
ウ．全項目を同時に変更し途中確認をしない
エ．切戻し手順は不要とする
正答：ア
4肢解説
ア：正しい。複数変更を独立扱いすると中間状態の不整合が起こりやすい。
イ：再現性と安全性が低い。
ウ：原因切り分けが難しくなる。
エ：失敗時の復旧性を失う。
総合解説：複合移行では依存関係とチェックポイントを設け、どの状態へ戻すかを明確にする。

問140 先行10拠点中2拠点で同じVPN断が発生し、原因は特定機種の既知不具合と判明した。残り190拠点のうち80拠点が同機種である。最も適切な判断はどれか。
ア．2拠点だけの問題として予定どおり全展開する
イ．全体展開を停止し、修正版または回避策を検証してから同機種拠点へ展開する
ウ．先行試験結果を無視する
エ．障害情報を記録せず続行する
正答：イ
4肢解説
ア：同機種80拠点へ同じ問題が広がる可能性が高い。
イ：正しい。既知の再現性ある不具合を80拠点へ拡大すべきではない。
ウ：pilotの目的を失う。
エ：再発防止できない。
総合解説：pilotは展開可否を判断するゲートとして使い、停止基準を事前定義する。

問141 設問が『通信断の直接原因を30字程度で述べよ』と要求している。事実として『FW変更直後、BGP TCP/179がdenyされネイバーDown』が確認されている。最も適切な回答はどれか。
ア．ネットワークは複雑なので障害が起きたため
イ．今後は注意して作業する必要がある
ウ．FW変更でTCP/179が遮断され、BGP隣接が切断したため
エ．BGPについて詳しく調査した方がよい
正答：ウ
4肢解説
ア：具体的根拠がない。
イ：再発防止であり直接原因への回答ではない。
ウ：正しい。直接原因を、確認済み事実と因果関係で簡潔に記述している。
エ：原因を答えていない。
総合解説：記述問題では『原因』『理由』『対策』など設問要求語に直接対応する内容を書く。

問142 設問が『回線増強が必要な理由を数値を用いて述べよ』と要求している。現在ピーク9.2Gbit/s、回線上限10Gbit/s、半年後予測11Gbit/sである。最も適切な回答はどれか。
ア．利用者が増えているから
イ．回線は速い方がよいから
ウ．将来は何か問題が起きるかもしれないから
エ．半年後ピーク11Gbit/sが回線上限10Gbit/sを超えるため
正答：エ
4肢解説
ア：数値根拠を使っていない。
イ：要件に基づく理由でない。
ウ：具体性がない。
エ：正しい。要求された数値を使い、増強理由を直接示している。
総合解説：数値を求める設問では閾値・実測・予測を明示して結論へつなげる。

問143 設問が『単一障害点を構成図の情報に基づいて答えよ』と要求している。回線2本とFW2台の双方が1台のL2スイッチへ接続されている。最も適切な回答はどれか。
ア．両系統が共用するL2スイッチであり、故障すると双方の通信が停止する
イ．FWが2台あること
ウ．回線が2本あること
エ．ネットワーク機器は全て障害点である
正答：ア
4肢解説
ア：正しい。構成図の共有要素と障害影響を根拠にしている。
イ：冗長要素であり単一障害点ではない。
ウ：冗長化要素である。
エ：設問の図表情報に基づく特定ができていない。
総合解説：根拠付き記述では対象要素と、その要素が失われた場合の影響を結び付ける。

問144 設問が『なぜローカルブレイクアウトを採用するのか』と尋ねている。現状はSaaS通信を全て本社へ迂回し、本社回線が90%でSaaS遅延も大きい。最も適切な回答はどれか。
ア．各拠点に設定作業を行う
イ．SaaS通信の本社迂回を減らし、本社回線負荷とSaaS遅延を低減するため
ウ．セキュリティ設定を確認する
エ．SD-WAN製品を購入する
正答：イ
4肢解説
ア：実施内容であって採用理由ではない。
イ：正しい。採用理由を現状課題と効果で説明している。
ウ：必要作業だが理由を答えていない。
エ：手段・製品であり目的ではない。
総合解説：『なぜ』を問う設問では、現状課題→採用案の効果という因果を示す。

問145 設問が『同種の管理者アカウント侵害を防ぐ対策を二つ述べよ』とする。原因は共有IDとパスワード認証のみであった。最も適切な回答はどれか。
ア．セキュリティを強化する
イ．ログを確認する
ウ．個人別管理者IDへ分離し、MFAを必須化する
エ．管理画面の色を変更する
正答：ウ
4肢解説
ア：抽象的で具体策になっていない。
イ：検知・調査策であり原因の予防策二つになっていない。
ウ：正しい。確認された原因に直接対応する二つの具体策である。
エ：侵害防止に関係しない。
総合解説：対策記述は原因に対応し、実装可能な具体性を持たせる。

問146 設問が『IPアドレス変更不可という制約を守りつつ、拠点A/Bの重複アドレスを暫定統合する方法を述べよ』とする。最も適切な回答はどれか。
ア．全端末を直ちに再アドレスする
イ．重複したまま同一ルーティングテーブルへ統合する
ウ．DNS名だけ変更する
エ．VRFでアドレス空間を分離し、必要な相互通信だけNATで変換する
正答：エ
4肢解説
ア：制約に反する。
イ：宛先を一意に判断できない。
ウ：IP重複を解消しない。
エ：正しい。IP変更不可という制約を守りながら重複を論理分離できる。
総合解説：制約付き設問では、提案が明示制約を破っていないか確認する。

問147 設問が『案Bを案Aより適切と判断した理由を、可用性と運用性の観点で述べよ』と要求している。最も適切な回答の形はどれか。
ア．案Bは障害ドメインが分離され単一障害点が少なく、運用手順も既存標準に統一できるため
イ．案Bの方が何となくよいから
ウ．案Aにはルータがあるから
エ．ベンダーが案Bを勧めたから
正答：ア
4肢解説
ア：正しい。指定された二つの評価軸に沿って案Bの優位性を説明している。
イ：根拠がない。
ウ：可用性・運用性の評価になっていない。
エ：指定評価軸による説明になっていない。
総合解説：比較問題では設問で指定された評価軸を使って差分と結論を書く。

問148 設問が『侵害経路をログに基づいて述べよ』と要求する。ログにはVPN成功→RDP→権限変更があるが、フィッシングの証拠はない。最も適切な回答はどれか。
ア．フィッシングメールから侵入した
イ．VPNアカウントで侵入後、RDPで内部端末へ移動し権限を変更した
ウ．攻撃者は必ず内部関係者である
エ．原因は不明なのでログ内容も書かない
正答：イ
4肢解説
ア：証拠がない。
イ：正しい。確認できるログの範囲だけを使っている。
ウ：根拠がない。
エ：確認済みの侵入経路部分は記述できる。
総合解説：根拠付き記述では事実・推定・不明を区別し、過剰な断定を避ける。

問149 設問が『SLA99.99%、回線費増加20%以内、工事不可という条件を満たす改善案と理由を述べよ』とする。現状は単一インターネット回線で99.9%。追加の5G回線は工事不要で費用15%増とする。最も適切な回答はどれか。
ア．専用線を新設する。高品質だから
イ．現状維持する。費用が増えないから
ウ．既存回線に5G回線を追加して冗長化する。工事不要かつ費用増15%で制約内に収まり、単一回線障害時の代替経路を確保できるため
エ．回線を3本追加する。多いほどよいから
正答：ウ
4肢解説
ア：工事不可の制約を満たさない。
イ：99.99%の可用性改善要求を満たさない。
ウ：正しい。三つの条件すべてに触れ、改善効果も説明している。
エ：費用20%以内という制約を確認していない。
総合解説：総合記述では要求・制約を漏れなく照合し、提案と根拠を一対で示す。

問150 設問が『障害原因、恒久対策、対策後の確認方法をそれぞれ述べよ』とする。事実は『MTU1500の端末からIPsec VPNへ大きなDFパケットを送り、ICMP Packet Too BigがFWで遮断されていた』である。最も適切な回答はどれか。
ア．原因はDNS、対策はTTL短縮、確認は名前解決
イ．原因は不明、対策は再起動、確認はpingだけ
ウ．原因はVPN利用そのもの、対策はVPN廃止、確認不要
エ．原因はPMTU通知遮断による大パケットのブラックホール、対策は必要なICMP許可または適切なMTU/MSS調整、確認は大サイズ通信とPMTUDの再試験
正答：エ
4肢解説
ア：提示事実と一致しない。
イ：根拠と恒久性が不足する。
ウ：過剰で要件を無視している。
エ：正しい。原因・恒久対策・確認方法が一貫している。
総合解説：記述式の総合問題では、観測事実→原因→対策→検証が論理的につながることが重要である。