問1 情報セキュリティにおける『脆弱性』の説明として最も適切なものはどれか。
ア．脅威によって悪用され得る、システムや運用上の弱点
イ．損失が発生した後の金額そのもの
ウ．攻撃者や災害などの原因となる事象
エ．受容済みのリスクを記録する文書
正答：ア
4肢解説
ア：正しい。脆弱性は、ソフトウェア欠陥、設定不備、運用上の弱点など、脅威が悪用できる弱点を指す。
イ：これは影響度の一部であり、脆弱性そのものではない。
ウ：これは脅威に当たる。
エ：リスク登録簿などの管理情報であり、脆弱性ではない。
総合解説：リスク分析では、資産、脅威、脆弱性、発生可能性、影響を関連付けて評価する。

問2 データが権限のない者に閲覧されないことを重視するセキュリティ特性はどれか。
ア．完全性
イ．機密性
ウ．可用性
エ．冗長性
正答：イ
4肢解説
ア：情報が不正に変更・破壊されないことに関係する。
イ：正しい。機密性は、許可された主体だけが情報へアクセスできる状態を確保する考え方である。
ウ：必要なときにサービスや情報を利用できることに関係する。
エ：可用性向上のための設計手段の一つでありCIAの要素名ではない。
総合解説：情報セキュリティの基本特性として、機密性・完全性・可用性を区別して要件化することが重要である。

問3 『機密情報へのアクセスは業務上必要な者に限定する』という組織方針と、『申請フォームに上長承認を添付して権限付与する』という具体手順の関係として適切なものはどれか。
ア．前者が手順、後者がポリシーである
イ．両方とも暗号アルゴリズムである
ウ．前者がポリシー、後者が手順に近い
エ．両方とも脆弱性そのものである
正答：ウ
4肢解説
ア：抽象度が逆である。
イ：組織ルールの階層に関する説明である。
ウ：正しい。ポリシーは組織の原則・方針を示し、手順はそれを実施する具体的方法を定める。
エ：方針・手順は統制であり脆弱性ではない。
総合解説：セキュリティ管理では、ポリシー、標準、ガイドライン、手順を整合させ、実装可能な統制へ落とし込む。

問4 インターネット公開サーバの脆弱性を解消するため、修正パッチを適用して攻撃成功の可能性を下げた。この対応は何に最も近いか。
ア．リスク回避
イ．リスク移転
ウ．リスク受容
エ．リスク低減
正答：エ
4肢解説
ア：対象業務自体を中止するなど、リスク源を避ける対応を指す。
イ：保険や契約などで影響の一部を第三者へ移す考え方である。
ウ：追加対策をせず一定のリスクを受け入れる対応である。
エ：正しい。脆弱性を修正して発生可能性を下げるのは、リスク低減の代表例である。
総合解説：リスク対応には回避、低減、移転、受容などがあり、コストと残留リスクを比較して選択する。

問5 多要素認証とアクセス制御を導入しても、認証情報の窃取や端末侵害の可能性を完全にはゼロにできない。この導入後に残るリスクは何と呼ばれるか。
ア．残留リスク
イ．固有リスクだけ
ウ．ゼロリスク
エ．伝搬遅延
正答：ア
4肢解説
ア：正しい。対策実施後にも残るリスクを残留リスクという。
イ：対策前の状態で存在するリスクを指す文脈で使われる。
ウ：一般にセキュリティリスクを完全にゼロにすることは困難である。
エ：ネットワーク性能指標でありリスク分類ではない。
総合解説：統制導入後も残るリスクが組織のリスク許容度内かを判断し、必要なら追加対策を行う。

問6 簡易評価でリスクスコアを『発生可能性1〜5 × 影響度1〜5』と定義する。発生可能性4、影響度5のリスクスコアは幾つか。
ア．9点（4+5で加算する）
イ．20点（4×5で乗算する）
ウ．10点（定義外の計算を行う）
エ．25点（最大値5×5を用いる）
正答：イ
4肢解説
ア：4と5を加算した値であり、設問の定義と異なる。
イ：正しい。4×5=20である。
ウ：与えられた計算式ではない。
エ：最大値5×5であり、発生可能性4を反映していない。
総合解説：定量・半定量評価の尺度は組織ごとに定義できるが、評価基準を明確にし一貫して適用することが重要である。

問7 発生可能性も影響も小さく、対策費用が想定損失を大幅に上回るリスクについて、経営責任者が根拠を確認した上で受容を承認した。評価として適切なものはどれか。
ア．セキュリティリスクは一切受容してはならない
イ．対策費用は一切考慮してはならない
ウ．リスク許容度の範囲内なら、記録・承認した上で受容することは合理的である
エ．受容したリスクは記録しなくてよい
正答：ウ
4肢解説
ア：現実的なリスク管理では受容も正当な対応選択肢である。
イ：コスト・便益や事業影響を考慮して優先順位を決める。
ウ：正しい。全リスクをゼロにするのではなく、組織の許容基準に照らして受容する判断もリスク管理の一部である。
エ：前提や責任を追跡できるよう記録すべきである。
総合解説：リスク受容は権限ある責任者が残留リスクを理解し、基準に照らして判断・記録することが重要である。

問8 二つの脆弱性がある。Aは外部公開で悪用容易だが影響は中、Bは内部限定で悪用困難だが影響は大である。適切な対応はどれか。
ア．影響が大きいBだけを必ず最優先にする
イ．外部公開のAだけを必ず最優先にする
ウ．どちらも同じ脆弱性なので評価不要である
エ．発生可能性と影響度を両方評価し、業務・露出状況を踏まえて優先順位を決める
正答：エ
4肢解説
ア：発生可能性や露出を無視している。
イ：影響度を無視している。
ウ：条件が異なるためリスクも異なる。
エ：正しい。単一指標だけでなく、脅威源、露出、悪用可能性、影響度を総合評価する。
総合解説：リスクベースの優先順位付けでは、技術的深刻度だけでなく業務影響・露出・脅威動向を組み合わせる。

問9 公開Webサーバの脆弱性から侵入され、そのサーバが社内DBへ広い権限を持つため機密データ流出へ至る可能性がある。リスク分析として最も適切な対応はどれか。
ア．Webサーバ単体の脆弱性だけでなく、侵入後の到達経路と権限連鎖を含む攻撃シナリオとして評価する
イ．Webサーバに脆弱性がある事実だけ記録し、内部接続は評価しない
ウ．DBが内部にあるので流出リスクはゼロとみなす
エ．暗号化の有無だけで全リスクを判断する
正答：ア
4肢解説
ア：正しい。初期侵入から横展開、権限利用、情報流出までを一連のシナリオとして見ることで実際の業務リスクを評価できる。
イ：横展開や影響拡大の要因を見落とす。
ウ：侵害済みWebサーバから到達可能ならリスクは残る。
エ：アクセス権や経路、認証など複数要素が関係する。
総合解説：ネットワークセキュリティでは攻撃面だけでなく、侵入後の横展開経路や信頼関係を含めてリスクを評価する。

問10 年1回程度起こり得る事故の最大損失が100万円と見積もられ、発生確率は10%とする。対策費が年間500万円で他の便益はない。単純な期待損失だけを基準にした判断として最も適切なものはどれか。
ア．期待損失は1,000万円なので必ず導入する
イ．期待損失は10万円なので、この情報だけなら500万円の対策は費用対効果が低い
ウ．期待損失は500万円なので費用と同額である
エ．金銭評価はリスク管理で一切使えない
正答：イ
4肢解説
ア：確率の掛け方が誤っている。
イ：正しい。単純化すると期待損失は100万円×0.1=10万円であり、対策費500万円を上回らない。
ウ：与えられた値からは算出されない。
エ：金銭化できる範囲では意思決定材料として利用できる。
総合解説：実際には法令、信用、人的被害、リスク許容度など金銭化しにくい要素も含めて判断する必要がある。

問11 インターネット公開WebサーバをDMZへ配置する主な目的はどれか。
ア．公開サーバを社内端末と同じセグメントへまとめる
イ．全通信を無条件許可する
ウ．外部公開系と内部業務ネットワークの間に境界を設け、侵害時の影響拡大を抑える
エ．DNSを使用しないようにする
正答：ウ
4肢解説
ア：侵害時に内部へ横展開しやすくなる。
イ：DMZのアクセス制御目的に反する。
ウ：正しい。DMZは公開サービスを内部ネットワークから分離し、通信経路をFW等で制御するために利用する。
エ：DMZの本質的目的ではない。
総合解説：DMZ設計ではインターネット→公開系、公開系→内部、管理系→公開系の通信を必要最小限に制御する。

問12 最小権限の原則として最も適切なものはどれか。
ア．全利用者へ管理者権限を付与する
イ．一度付与した権限は退職後も維持する
ウ．ネットワーク内部なら認証なしで全許可する
エ．利用者やシステムに、業務遂行に必要な最小限の権限だけを付与する
正答：エ
4肢解説
ア：最小権限と逆である。
イ：不要権限は削除すべきである。
ウ：位置だけを根拠に広範な権限を与えるべきではない。
エ：正しい。不要な権限を持たせないことで、誤操作や侵害時の被害範囲を抑える。
総合解説：最小権限は利用者、サービスアカウント、ネットワーク経路、管理APIなど幅広い対象に適用する。

問13 ファイアウォールポリシーで『明示的に許可した通信以外は拒否する』考え方はどれか。
ア．デフォルト拒否
イ．デフォルト許可
ウ．ベストエフォート
エ．ラウンドロビン
正答：ア
4肢解説
ア：正しい。必要な通信だけを許可し、それ以外を拒否することで不要な攻撃面を減らす。
イ：明示的に拒否したもの以外を通す考え方である。
ウ：通信品質の提供形態でありアクセス制御ポリシーではない。
エ：負荷分散や順番制御の方式である。
総合解説：FW・ACL設計では許可要件を具体化し、最後に暗黙または明示のdenyを置く設計が基本となる。

問14 社員の所属職務に応じて『経理担当』『ネットワーク運用担当』などの役割へ権限を割り当て、利用者は役割を通じて権限を得る方式はどれか。
ア．ABAC
イ．RBAC
ウ．DAC
エ．NAT
正答：イ
4肢解説
ア：属性の組合せでポリシー評価する方式で、設問は役割中心である。
イ：正しい。Role-Based Access Controlは役割に権限を割り当て、利用者へ役割を付与する。
ウ：資源所有者が裁量で権限を設定する方式である。
エ：IPアドレス変換であり認可方式ではない。
総合解説：RBACは職務分掌と相性がよく、異動時に役割変更で権限を管理しやすい。

問15 『利用者の所属=営業、端末=会社管理済み、時刻=平日9〜18時、対象データ=社外秘』など複数属性でアクセス可否を決める方式はどれか。
ア．RBACだけ
イ．PAT
ウ．ABAC
エ．STP
正答：ウ
4肢解説
ア：役割だけで判断する方式であり、設問は複数属性を利用している。
イ：ポート番号を利用するNATの一種である。
ウ：正しい。Attribute-Based Access Controlは主体・対象・環境等の属性に基づいてポリシーを評価する。
エ：L2ループ防止プロトコルである。
総合解説：ABACは細粒度・動的なアクセス制御に向くが、属性の信頼性とポリシー複雑性を管理する必要がある。

問16 工場の制御ネットワークと一般社員のインターネット閲覧ネットワークを直接相互通信させたくない。最も適切な設計はどれか。
ア．同一VLANにまとめて端末側の注意だけで運用する
イ．全ポートを相互に許可する
ウ．IPアドレスを同じ範囲にすれば安全になる
エ．別ゾーンに分離し、必要な中継通信だけをFW等で明示的に許可する
正答：エ
4肢解説
ア：横展開リスクを高める。
イ：分離要件を満たさない。
ウ：セグメンテーションの代替にはならない。
エ：正しい。役割・リスクが大きく異なるネットワークはゾーンを分け、境界で通信を制御する。
総合解説：ゾーニングでは資産価値・信頼レベル・業務用途を基に境界を決め、データフローをホワイトリスト化する。

問17 上から順に評価するACLで、1行目『10.0.0.0/8を拒否』、2行目『10.1.1.10を許可』となっている。10.1.1.10からの通信の一般的な結果はどれか。
ア．1行目で一致して拒否され、2行目まで到達しない
イ．2行目がより具体的なので必ず許可される
ウ．両方のルールを同時に適用して半分だけ通す
エ．DNS解決結果によってのみ決まる
正答：ア
4肢解説
ア：正しい。最初に一致したルールで処理を確定するACLでは、広い拒否が先にあると後続の例外許可が無効になる。
イ：ルータの最長一致経路選択とACLの上から順評価を混同している。
ウ：一般的なACL動作ではない。
エ：ACLの評価順序が直接決める。
総合解説：ACLレビューではルール順、重複・シャドーイング、広すぎる許可、未使用ルールを確認する。

問18 ルータ・FWの管理GUI/SSHを一般利用者LANから直接到達可能にしている。改善として最も適切なものはどれか。
ア．管理ポートをインターネットへ直接公開する
イ．管理用ゾーンや踏み台経由に限定し、管理通信元を認証済み管理端末へ制限する
ウ．管理者パスワードを全社員へ共有する
エ．管理通信を全てHTTP平文へ変更する
正答：イ
4肢解説
ア：攻撃面を拡大する。
イ：正しい。管理プレーンは一般業務通信から分離し、アクセス元・経路・認証を限定するべきである。
ウ：権限管理・監査性が失われる。
エ：機密性を低下させる。
総合解説：管理ネットワークはアウトオブバンド管理、踏み台、MFA、ログ監査などと組み合わせる。

問19 同一データセンター内でWeb、AP、DBサーバが同一大規模サブネットにあり、1台侵害時に横展開しやすい。改善策として最も適切なものはどれか。
ア．全サーバ間通信を無条件許可する
イ．サブネットをさらに大きくする
ウ．ワークロード単位で必要通信だけ許可するマイクロセグメンテーションを導入する
エ．DNS TTLだけを短くする
正答：ウ
4肢解説
ア：横展開リスクを残す。
イ：障害・攻撃範囲を縮小しない。
ウ：正しい。東西通信を細粒度に制御することで、侵害後の横展開範囲を抑えられる。
エ：東西アクセス制御にはならない。
総合解説：マイクロセグメンテーションではアプリ依存関係を把握し、必要通信を段階的にポリシー化することが重要である。

問20 Web→APはTCP/8443、AP→DBはTCP/5432だけ必要である。外部利用者からDBへ直接通信する要件はない。FW設計として最も適切なものはどれか。
ア．外部からWeb/AP/DBの全ポートを許可する
イ．WebとDBだけを同一ゾーンにして全通信許可する
ウ．全通信を拒否して業務を停止する
エ．外部→Web、Web→AP:8443、AP→DB:5432だけを必要範囲で許可し、外部→DBは拒否する
正答：エ
4肢解説
ア：最小権限に反し攻撃面が広い。
イ：AP層を介した制御を崩し、DBを過度に公開する。
ウ：必要な業務通信も成立しない。
エ：正しい。業務データフローに沿って経路ごとに必要な通信だけを許可する。
総合解説：多層システムではゾーンごとの信頼境界と通信方向・ポートを明示してポリシー化する。

問21 ゼロトラストの考え方として最も適切なものはどれか。
ア．社内LANにいるという理由だけで暗黙の信頼を与えず、利用者・端末・資源ごとにアクセスを評価する
イ．社内IPアドレスなら全資源へ無条件アクセスさせる
ウ．境界FWを廃止すればゼロトラストになる
エ．一度認証した利用者は永久に再評価しない
正答：ア
4肢解説
ア：正しい。ゼロトラストではネットワーク位置や所有関係だけを根拠に信頼しない。
イ：位置ベースの暗黙信頼はゼロトラストの考え方と逆である。
ウ：特定製品の廃止だけではゼロトラストを実現できない。
エ：継続的な状況変化を考慮する必要がある。
総合解説：ゼロトラストは資源中心、最小権限、明示的な認証・認可、継続的なポリシー評価を重視する。

問22 NISTのゼロトラストアーキテクチャで、実際の通信経路上でアクセスを許可・遮断する役割を担うものはどれか。
ア．Policy Engine（PE）だけ
イ．Policy Enforcement Point（PEP）
ウ．DNS Root Server
エ．NTP Server
正答：イ
4肢解説
ア：PEはアクセス可否を判断する論理機能であり執行点ではない。
イ：正しい。PEPはポリシー判断に基づいて接続を成立・終了させる執行点である。
ウ：名前解決のルートでありゼロトラストのアクセス執行点ではない。
エ：時刻同期サーバである。
総合解説：ゼロトラストではPE、Policy Administrator、PEPなどが連携してアクセス判断と執行を行う。

問23 SASEの説明として最も適切なものはどれか。
ア．LANスイッチのSTPだけをクラウド化する技術
イ．暗号アルゴリズムAESの別名
ウ．SD-WAN等の接続機能と複数のセキュリティ機能を、クラウド中心のポリシーベースサービスとして統合する考え方
エ．メール転送専用のサービス
正答：ウ
4肢解説
ア：SASEはWAN接続とセキュリティ機能を広く扱う。
イ：暗号方式ではない。
ウ：正しい。SASEはネットワーク接続とセキュリティを統合し、利用者・端末・アプリの場所に依存しにくい形で提供する。
エ：用途はメールに限定されない。
総合解説：MEF 117ではSASEサービスにセキュリティ機能、ポリシー、接続サービスの属性を定義している。

問24 利用者のパスワード認証は成功したが、端末のEDRが無効でOS更新も長期間未適用である。ゼロトラスト方針として最も適切な処理はどれか。
ア．認証成功後は端末状態を一切確認しない
イ．社内Wi-Fiなら自動的に全許可する
ウ．OS更新の有無をDNSで決める
エ．端末状態をリスク要因として評価し、アクセス拒否または限定アクセスにする
正答：エ
4肢解説
ア：ゼロトラストの継続的・コンテキスト型評価と合わない。
イ：ネットワーク位置だけを根拠に信頼している。
ウ：DNSは端末健全性評価機能ではない。
エ：正しい。利用者認証だけでなくデバイスの健全性も認可判断へ反映する。
総合解説：ゼロトラストでは主体ID、デバイス状態、資源、時刻、脅威情報など複数コンテキストでアクセスを判断する。

問25 接続開始時は正常だった端末が、セッション中にマルウェア感染と判定された。ゼロトラスト設計として適切な対応はどれか。
ア．状態変化をポリシーへ反映し、既存セッションも再評価・遮断できるようにする
イ．接続開始時に許可したので感染後も必ず継続する
ウ．端末を社内LANへ移動すれば安全とみなす
エ．利用者名を変更すれば感染状態が解消する
正答：ア
4肢解説
ア：正しい。認証時点だけではなく、状況変化に応じて継続的にアクセスを評価する。
イ：継続的な信頼評価を行っていない。
ウ：位置だけで信頼しない。
エ：端末侵害は解消しない。
総合解説：セッション継続中のテレメトリを利用し、必要に応じて再認証、権限縮小、遮断を行う。

問26 社員の多くが自宅や出張先からSaaSへ直接アクセスし、拠点経由のセキュリティ集中処理では遅延が大きい。SASEが候補となる理由はどれか。
ア．全利用者通信を必ず本社1拠点へ戻すことがSASEの必須条件だから
イ．利用者に近いクラウドエッジで接続・セキュリティポリシーを適用しやすいため
ウ．SASEを導入すると認証が不要になる
エ．SASEは有線LANの速度だけを上げる製品だから
正答：イ
4肢解説
ア：むしろバックホール依存を減らすことが利点になり得る。
イ：正しい。SASEは分散利用者・クラウドアプリ環境で、接続とセキュリティ制御をクラウド側で提供する考え方である。
ウ：アイデンティティは重要な判断要素である。
エ：接続・セキュリティサービスの統合概念である。
総合解説：SASEはリモートワーク、SaaS、マルチクラウドなど分散環境で、利用者中心のポリシー適用を行いやすい。

問27 『ゼロトラストを導入するのでネットワークセグメンテーションは不要』という説明への評価として最も適切なものはどれか。
ア．適切。全てのFWとACLは必ず廃止する
イ．適切。端末認証だけで全てのアクセス制御を代替できる
ウ．不適切。ゼロトラストでもセグメンテーションやPEPは被害範囲を抑える重要な実装手段になり得る
エ．不適切だが理由はDNSを使えなくなるから
正答：ウ
4肢解説
ア：ゼロトラストの要件ではない。
イ：資源単位の認可やネットワーク制御も必要になり得る。
ウ：正しい。ゼロトラストは位置だけに信頼を置かない考え方であり、ネットワーク分割を否定するものではない。
エ：DNSとは無関係である。
総合解説：ZTではID中心の制御とネットワーク・アプリケーション側の執行点を組み合わせる。

問28 クラウド型セキュリティ機能だけでなく、SD-WAN等のネットワーク接続機能も統合したサービスを求めている。概念としてより近いものはどれか。
ア．セキュリティ機能だけに焦点を当てるSSE
イ．SNMP
ウ．RAID
エ．SASE
正答：エ
4肢解説
ア：SSEはSASEのセキュリティ側機能群に焦点を当てる概念で、接続機能まで含む要件にはSASEが近い。
イ：監視プロトコルである。
ウ：ストレージ冗長化技術である。
エ：正しい。SASEはセキュリティ機能とネットワーク接続機能を統合する枠組みである。
総合解説：SASEとSSEは実装・サービス範囲を区別し、必要な接続機能とセキュリティ機能を確認することが重要である。

問29 高機密システムへのアクセス要求で、利用者は正規社員だが、未知の端末・海外からの深夜アクセス・高リスクIPという情報が得られた。ゼロトラストで最も適切な処理はどれか。
ア．複数コンテキストを総合してリスクを高く評価し、追加認証や拒否などポリシーに沿って判断する
イ．社員IDが正しいので他条件を無視して必ず許可する
ウ．海外IPなら利用者IDを確認せず必ず許可する
エ．全ての条件をDNS名だけへ変換して判断する
正答：ア
4肢解説
ア：正しい。IDだけでなく端末、位置、時刻、脅威情報等を組み合わせてアクセス可否を決める。
イ：単一の属性だけで暗黙信頼している。
ウ：リスク評価にならない。
エ：ポリシー評価を代替できない。
総合解説：ゼロトラストではアクセス要求ごとにポリシーエンジンが複数情報源を評価し、最小権限で判断する。

問30 全社員のインターネット・SaaSアクセスを単一SASE PoPへ依存させたところ、そのPoP障害で全社通信が停止した。設計改善として最も適切なものはどれか。
ア．SASEなら障害は起きないので何もしない
イ．複数PoP・複数経路へのフェイルオーバと、ポリシー・認証基盤の冗長性を設計する
ウ．全拠点の回線を1本に減らす
エ．ユーザ名を全員同じにする
正答：イ
4肢解説
ア：クラウドサービスにも障害はあり得る。
イ：正しい。SASEもサービス依存点であり、接続先・認証・ポリシー制御の可用性を考慮する必要がある。
ウ：可用性をさらに低下させる。
エ：可用性・セキュリティとも悪化する。
総合解説：SASE導入でもアンダーレイ回線、PoP、ID基盤、DNS、ポリシー制御などの共通障害点を評価する。

問31 大量データを高速に暗号化する用途で一般に中心となる暗号方式はどれか。
ア．公開鍵暗号だけ
イ．ハッシュ関数
ウ．共通鍵暗号
エ．CRC
正答：ウ
4肢解説
ア：鍵配送や署名等に有用だが、大量データの暗号化は共通鍵暗号と組み合わせることが一般的である。
イ：一方向変換であり復号を前提とした暗号化方式ではない。
ウ：正しい。共通鍵暗号は同じ秘密鍵を暗号化・復号に利用し、公開鍵暗号より高速な処理に向く。
エ：伝送誤り検出を主目的とし、暗号学的機密性を提供しない。
総合解説：実際のTLS等では公開鍵・鍵共有の仕組みと共通鍵暗号を組み合わせるハイブリッド方式が使われる。

問32 SHA-256で生成されるメッセージダイジェストの長さはどれか。
ア．128ビット
イ．512バイト
ウ．入力データと常に同じ長さ
エ．256ビット
正答：エ
4肢解説
ア：SHA-256の出力長ではない。
イ：SHA-256の出力は512バイトではない。
ウ：ハッシュ値は入力長にかかわらず固定長である。
エ：正しい。SHA-256は256ビットのハッシュ値を生成する。
総合解説：SHA-256はSHA-2ファミリのハッシュ関数で、入力が任意長でも出力は256ビットである。

問33 HMACの説明として最も適切なものはどれか。
ア．秘密鍵とハッシュ関数を組み合わせ、メッセージの完全性と送信者側の鍵保有を確認する
イ．公開鍵証明書を発行する仕組み
ウ．データを必ず復号可能な形へ暗号化する方式
エ．IPアドレスをMACアドレスへ解決する方式
正答：ア
4肢解説
ア：正しい。HMACは共有秘密鍵を用いるメッセージ認証コードである。
イ：これはCAなどPKIの役割である。
ウ：HMACは暗号化方式ではない。
エ：ARPの役割である。
総合解説：HMACは暗号化による機密性ではなく、鍵付き完全性・真正性確認に利用する。

問34 AESについて正しい説明はどれか。
ア．AES-256は256ビットのブロック長を使用する
イ．AESは128ビットブロックを扱い、128・192・256ビットの鍵長が規定されている
ウ．AESは公開鍵暗号である
エ．AESはハッシュ関数である
正答：イ
4肢解説
ア：AESのブロック長は鍵長に関係なく128ビットである。
イ：正しい。FIPS 197ではAES-128、AES-192、AES-256が規定される。
ウ：AESは共通鍵ブロック暗号である。
エ：暗号化用のブロック暗号である。
総合解説：鍵長とブロック長を混同しないことが重要である。

問35 送信者が秘密鍵でデジタル署名し、受信者が対応する公開鍵で検証することで主に確認できるものはどれか。
ア．データ内容の機密性だけ
イ．受信者の端末性能
ウ．署名対象データの完全性と、秘密鍵を保有する主体による署名であること
エ．ネットワークの帯域保証
正答：ウ
4肢解説
ア：署名は通常データを秘匿しない。
イ：署名検証の目的ではない。
ウ：正しい。適切な署名方式と鍵管理を前提に、改ざん検出と署名者の真正性を確認できる。
エ：暗号署名とは無関係である。
総合解説：デジタル署名はハッシュと公開鍵暗号技術を利用し、証明書と組み合わせて署名者の公開鍵を確認することが多い。

問36 TLS 1.3を適切に利用したHTTPS通信で期待できる保護として最も適切なものはどれか。
ア．経路上のDDoSを必ず完全に防止する
イ．WebアプリのSQLインジェクション脆弱性を自動修正する
ウ．DNSキャッシュポイズニングを常に防止する
エ．通信内容の機密性・完全性と、証明書等を用いたサーバ認証
正答：エ
4肢解説
ア：TLSは大量トラフィックによる可用性攻撃を完全に防ぐものではない。
イ：TLSは通信路を保護するがアプリ脆弱性を修正しない。
ウ：TLSだけでDNS自体の完全性を保証するものではない。
エ：正しい。TLSは盗聴・改ざんを防ぎ、通常HTTPSではサーバ証明書で接続先を認証する。
総合解説：TLSの保護範囲と、アプリケーション・DNS・可用性対策の範囲を区別する必要がある。

問37 TLS 1.3で用いられるAEAD方式の説明として最も適切なものはどれか。
ア．暗号化と認証を組み合わせ、機密性と改ざん検出を一体として提供する
イ．暗号化せずチェックサムだけを計算する
ウ．公開鍵証明書を自動発行する
エ．IP経路を暗号強度順に選択する
正答：ア
4肢解説
ア：正しい。AEADはAuthenticated Encryption with Associated Dataであり、暗号文の真正性も確認する。
イ：AEADは暗号化も行う。
ウ：証明書発行機能ではない。
エ：ルーティング機能ではない。
総合解説：暗号モード設計では機密性だけでなく完全性・真正性を同時に確保することが重要である。

問38 利用者パスワードを保存する際、同じパスワードでも異なる保存値になり、事前計算攻撃を困難にするために利用するランダム値はどれか。
ア．IVを全利用者で固定して公開しないことだけ
イ．salt
ウ．DNS TTL
エ．VLAN ID
正答：イ
4肢解説
ア：暗号モードのIVとパスワードハッシュのsaltは役割が異なる。
イ：正しい。利用者ごとに十分なランダムsaltを付加してハッシュ処理することで、同一パスワードの識別やレインボーテーブル攻撃を困難にする。
ウ：名前解決キャッシュ時間である。
エ：L2セグメント識別子である。
総合解説：パスワードは単純な高速ハッシュだけでなく、適切なパスワードハッシュ方式・salt・コスト設定で保護する。

問39 TLS 1.3の0-RTTデータを利用して、銀行振込のような同じ要求を再実行すると副作用がある操作を送信したい。最も重要な注意点はどれか。
ア．0-RTTならリプレイ攻撃は物理的に不可能である
イ．0-RTTを使うと暗号化が一切行われない
ウ．0-RTTデータにはリプレイの可能性があるため、非冪等な重要操作には慎重に利用する
エ．0-RTTはDNS専用機能である
正答：ウ
4肢解説
ア：RFC 8446はearly dataのリプレイについて明確な注意を示している。
イ：early dataも保護されるがリプレイ特性が異なる。
ウ：正しい。TLS 1.3のearly dataはリプレイ耐性が通常の1-RTTデータと異なり、アプリ側の対策が必要である。
エ：TLSの接続再開機能に関するものである。
総合解説：性能最適化機能はセキュリティ特性とのトレードオフを理解して適用する。

問40 過去のTLS通信を暗号化したパケットとして保存していた攻撃者が、後日サーバ証明書の秘密鍵を盗んだ。エフェメラル(DHE/ECDHE)鍵共有による前方秘匿性が有効な場合の効果として最も適切なものはどれか。
ア．過去通信の平文がサーバ秘密鍵だけで必ず復号できる
イ．長期秘密鍵が漏れても今後のなりすましリスクは一切ない
ウ．前方秘匿性はハッシュ衝突を防ぐ機能だけを指す
エ．長期秘密鍵の漏えいだけでは過去セッション鍵を復元しにくくする
正答：エ
4肢解説
ア：前方秘匿性の狙いと逆である。
イ：漏えい鍵は失効・更新が必要である。
ウ：鍵漏えいと過去セッション保護に関する特性である。
エ：正しい。セッションごとの一時鍵共有により、長期秘密鍵が後から漏れても過去のセッション鍵を直接復元できない設計となる。
総合解説：TLS 1.3では一時的な(EC)DHE鍵共有を利用する構成が重要で、長期鍵とセッション鍵の分離を図る。

問41 公開鍵証明書の主な役割として最も適切なものはどれか。
ア．主体の識別情報と公開鍵をCAの署名などで結び付ける
イ．秘密鍵そのものを全利用者へ配布する
ウ．通信データを自動的にバックアップする
エ．IPアドレスをMACアドレスへ変換する
正答：ア
4肢解説
ア：正しい。証明書は公開鍵がどの主体に対応するかを第三者の署名で確認できるようにする。
イ：秘密鍵は所有者が秘密に保持する。
ウ：証明書の役割ではない。
エ：ARPの機能である。
総合解説：PKIでは証明書、CA、失効情報、証明書パス検証などを組み合わせて公開鍵を信頼する。

問42 PKIにおけるCA（Certification Authority）の役割はどれか。
ア．利用者の秘密鍵を公開Webサイトへ掲載する
イ．申請内容や認証手続に基づき公開鍵証明書へ署名し発行する
ウ．ルータの経路計算を行う
エ．WebアプリのSQLを最適化する
正答：イ
4肢解説
ア：秘密鍵漏えいとなり不適切である。
イ：正しい。CAは証明書を発行し、その公開鍵と主体情報の結び付きを保証する信頼点となる。
ウ：PKIの役割ではない。
エ：証明書発行とは無関係である。
総合解説：実際のPKIでは登録・本人確認をRAが担当し、CAが署名・発行する役割分担を行う場合がある。

問43 Webサーバ証明書を中間CAが署名し、その中間CA証明書をルートCAが署名している。クライアントが信頼の起点として保持するものは通常どれか。
ア．Webサーバの秘密鍵
イ．中間CAの秘密鍵
ウ．ルートCA証明書
エ．HTTP Cookie
正答：ウ
4肢解説
ア：クライアントが保持すべきではない。
イ：CA側が秘密に保持する。
ウ：正しい。証明書パスは信頼済みルートCAへ遡って検証する。
エ：証明書チェーンの信頼起点ではない。
総合解説：中間CAを利用するとルートCAの秘密鍵を日常運用から隔離しやすくなる。

問44 X.509証明書を下位証明書へ署名するCAとして利用する場合、特に確認すべき拡張として最も適切なものはどれか。
ア．Subject Alternative Nameに必ずIPアドレスだけを入れること
イ．証明書のシリアル番号を0にすること
ウ．DNS TTLを証明書に埋め込むこと
エ．Basic ConstraintsでcAがTRUEであること
正答：エ
4肢解説
ア：CAであることを示す拡張ではない。
イ：CA資格を示す条件ではない。
ウ：X.509証明書のCA判定とは無関係である。
エ：正しい。CAとして証明書署名に使う証明書ではBasic ConstraintsのcAフラグが重要である。
総合解説：証明書パス検証ではBasic ConstraintsやKey Usage等を確認し、CAとして許可された証明書だけを中間CA等に使用する。

問45 証明書の失効状態を、クライアントが対象証明書についてオンラインで問い合わせる代表的な仕組みはどれか。
ア．OCSP
イ．CRLだけ
ウ．ARP
エ．DHCP
正答：ア
4肢解説
ア：正しい。OCSPは証明書単位の状態をオンラインResponderへ問い合わせるプロトコルである。
イ：CRLはCAが発行する失効証明書一覧を取得して確認する方式である。
ウ：L2アドレス解決である。
エ：IPアドレス配布である。
総合解説：失効確認ではCRLやOCSPを利用し、到達不能時の扱いやキャッシュも考慮する。

問46 Webサーバ証明書の秘密鍵が外部へ漏えいしたことが判明した。最も適切な初動はどれか。
ア．同じ秘密鍵を使ったまま有効期限まで待つ
イ．該当証明書を失効させ、新しい鍵ペアと証明書へ交換する
ウ．公開鍵だけを削除して秘密鍵を使い続ける
エ．DNS TTLを変更するだけ
正答：イ
4肢解説
ア：漏えい鍵でなりすましされる危険が続く。
イ：正しい。秘密鍵の信頼性が失われたため、旧証明書を失効し新規鍵へ切り替える必要がある。
ウ：証明書との対応が崩れ、漏えいリスクも解消しない。
エ：秘密鍵の侵害を解決しない。
総合解説：鍵漏えい対応には失効、再発行、秘密鍵保護、原因調査、関連システムへの影響確認を含む。

問47 証明書にKey Usage拡張を設定する主な目的はどれか。
ア．IPアドレスのサブネット長を指定する
イ．秘密鍵の値を証明書へ格納する
ウ．その公開鍵を署名、鍵暗号化、証明書署名などどの用途に使用できるか制約する
エ．DNSのTTLを指定する
正答：ウ
4肢解説
ア：証明書の鍵用途とは無関係である。
イ：秘密鍵は証明書に含めない。
ウ：正しい。Key Usageは証明書に含まれる公開鍵の利用目的を制限する。
エ：証明書拡張の目的ではない。
総合解説：証明書発行時はBasic Constraints、Key Usage、Extended Key Usage等を目的に合わせて設定する。

問48 社内機器が自己署名証明書を使用している。『自己署名だから暗号化されない』という説明は正しいか。
ア．正しい。自己署名証明書ではTLSを一切使用できない
イ．正しい。自己署名なら秘密鍵が不要である
ウ．誤りだが、自己署名なら世界中のブラウザが自動信頼する
エ．誤り。TLS暗号化は可能だが、クライアントが証明書を信頼する仕組みを別途用意する必要がある
正答：エ
4肢解説
ア：TLS利用そのものは可能である。
イ：署名・TLS処理には秘密鍵が必要である。
ウ：通常は信頼ストアへ登録されていないため自動信頼されない。
エ：正しい。自己署名証明書でも暗号化はできるが、信頼点として配布・管理されていなければ相手認証で警告される。
総合解説：閉域環境でも独自CAや信頼ストア配布など、証明書の信頼管理を設計する必要がある。

問49 サーバ証明書は正しく、ルートCAもクライアントが信頼しているが、一部クライアントだけ『証明書チェーンを構築できない』と失敗する。サーバが中間CA証明書を送信していない場合の改善として最も適切なものはどれか。
ア．サーバに必要な中間CA証明書を適切なチェーンとして設定する
イ．サーバの秘密鍵をクライアントへ配布する
ウ．ルートCAを削除する
エ．HTTPへダウングレードする
正答：ア
4肢解説
ア：正しい。クライアントが中間証明書を別経路で取得できない場合、チェーンを構築できない。
イ：重大な秘密鍵漏えいとなる。
ウ：信頼パスをさらに壊す。
エ：TLS検証を避けるだけでセキュリティを低下させる。
総合解説：サーバは通常、エンドエンティティ証明書と必要な中間証明書を提示し、クライアントが信頼済みルートまでパス検証できるようにする。

問50 高機密システムでOCSP responderが障害中でも、クライアントが失効状態を確認できない証明書を無条件で受け入れる設定になっている。この設計の問題として最も適切なものはどれか。
ア．OCSP障害時は証明書が自動的に有効期限延長される
イ．失効済み証明書を受け入れる可能性があるため、可用性と失効確認ポリシーを両立する設計が必要である
ウ．失効確認はPKIと無関係である
エ．OCSPを使えばCAは不要になる
正答：イ
4肢解説
ア：そのような仕組みではない。
イ：正しい。いわゆるsoft-failは可用性を高める一方、失効確認不能時のリスクを受容することになる。
ウ：PKI運用の重要要素である。
エ：OCSP responderはCAが発行した証明書状態を扱う。
総合解説：失効確認方式はOCSP stapling、CRL、キャッシュ、fail-open/closedの方針をサービス要件に合わせて設計する。

問51 802.1Xを利用するアクセス装置で、端末認証が完了する前の一般データ通信を制限し、認証成功後に許可するための考え方として適切なものはどれか。
ア．認証前から全てのIP通信を無条件許可する
イ．DNSのMXレコードでポート状態を決める
ウ．Controlled Portの通信許可状態を認証結果に応じて制御する
エ．STPのRoot Bridgeだけで利用者認証を行う
正答：ウ
4肢解説
ア：ポートベースアクセス制御の目的に反する。
イ：メール配送設定とは無関係である。
ウ：正しい。802.1Xでは認証状態に応じてControlled Portを未許可・許可状態へ制御する。
エ：STPはL2ループ防止である。
総合解説：802.1Xはネットワーク利用前に認証を行い、認証結果に応じてデータ通信可能な状態を制御する。

問52 EAP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AESの一種
イ．IPアドレス配布プロトコル
ウ．ルーティングプロトコル
エ．複数の認証方式を運ぶための認証フレームワーク
正答：エ
4肢解説
ア：暗号方式ではない。
イ：DHCPの役割である。
ウ：経路交換には使わない。
エ：正しい。EAPはEAP-TLSなど様々なEAP Methodを利用できる拡張可能な認証フレームワークである。
総合解説：EAP自体が単一の認証アルゴリズムではなく、認証方式を運ぶ枠組みである。

問53 RADIUSで利用者認証要求を認証サーバへ送る代表的なパケットはどれか。
ア．Access-Request
イ．Access-Accept
ウ．Access-Reject
エ．DHCPDISCOVER
正答：ア
4肢解説
ア：正しい。NAS/RADIUSクライアントはAccess-Requestを送り、サーバはAccept/Reject/Challenge等で応答する。
イ：認証成功時にサーバから返る応答である。
ウ：認証拒否時の応答である。
エ：DHCPのメッセージである。
総合解説：RADIUSは認証結果だけでなくVLAN、ACL等の認可属性を返す用途にも使われる。

問54 企業有線LANの802.1X認証で、端末とスイッチ間ではEAPOLを利用し、スイッチから認証サーバへEAP情報を中継する構成として一般的なものはどれか。
ア．端末がOSPFで認証サーバへEAPを広告する
イ．スイッチがRADIUSクライアントとしてEAP情報を認証サーバへ中継する
ウ．スイッチがDNSゾーン転送で認証情報を送る
エ．端末と認証サーバ間でEthernet FCSだけを交換する
正答：イ
4肢解説
ア：OSPFはルーティングプロトコルである。
イ：正しい。端末-Authenticator間はEAPOL、Authenticator-認証サーバ間はRADIUS等を用いる構成が一般的である。
ウ：DNSゾーン転送は認証中継方式ではない。
エ：認証プロトコルではない。
総合解説：802.1XではAuthenticatorが端末側EAPとバックエンドAAAを橋渡しする。

問55 RADIUSサーバが追加の認証情報を利用者へ要求し、クライアントから応答を得て認証を継続したい場合に返す代表的な応答はどれか。
ア．Access-Accept
イ．Access-Reject
ウ．Access-Challenge
エ．DHCPACK
正答：ウ
4肢解説
ア：認証を受理する応答である。
イ：認証を拒否する応答である。
ウ：正しい。Access-Challengeはチャレンジ/レスポンス型など、追加情報を求めて認証処理を継続するために利用できる。
エ：DHCPのアドレス割当て応答である。
総合解説：RADIUSではAccess-Requestに対し、Accept、Reject、Challengeなどの応答を用途に応じて返す。

問56 複数組織の認証基盤を連携し、利用者名のrealmなどに応じて適切な認証サーバへ要求を転送したい。RADIUSで利用できる考え方はどれか。
ア．NATだけ
イ．STP
ウ．WAF
エ．RADIUSプロキシ
正答：エ
4肢解説
ア：IPアドレス変換であり認証要求のrealmルーティングではない。
イ：L2ループ防止である。
ウ：Webアプリ保護である。
エ：正しい。RADIUSサーバはプロキシとして別のRADIUSサーバへ要求を転送できる。
総合解説：RADIUSプロキシを用いると、管理ドメインをまたぐ認証連携を構成できる。

問57 従来のRADIUS/UDPを信頼できないネットワーク越しにそのまま利用する設計を見直したい。適切な方向性はどれか。
ア．RADIUS/TLS等の保護されたトランスポートや、信頼できる管理ネットワーク内への限定を検討する
イ．共有secretを公開Webサイトへ掲載する
ウ．RADIUSパケットをHTTP平文へ変換する
エ．MD5依存を強めるためRADIUS/1.1を禁止することだけを目的にする
正答：ア
4肢解説
ア：正しい。RADIUSの古いセキュリティ特性を補うため、TLSベースの保護やネットワーク分離を検討する。
イ：認証保護を失う。
ウ：通信保護にならない。
エ：近年はMD5依存を減らす方向の仕様もある。
総合解説：2025年のRFC 9765ではTLS 1.3/ALPNを利用して従来のMD5依存を除くRADIUS/1.1が実験仕様として定義された。

問58 複数SaaSへ同じ企業IdPの認証結果を利用してログインさせ、各SaaSが個別にパスワードを保持しないようにしたい。最も近い考え方はどれか。
ア．NAT
イ．IDフェデレーション
ウ．STP
エ．SNMP
正答：イ
4肢解説
ア：IPアドレス変換である。
イ：正しい。IdPが認証結果をアサーション等としてRPへ伝え、複数サービスで共通の認証基盤を利用する。
ウ：L2ループ防止である。
エ：監視管理プロトコルである。
総合解説：フェデレーションではIdP、RP、アサーションの信頼関係と属性最小化・失効を設計する。

問59 病院の医療機器用有線ポートで802.1X認証サーバ障害時の動作を設計する。可用性と不正接続防止がともに重要である。最も適切な考え方はどれか。
ア．認証障害時は全ポートを無条件で社内全域へ開放する
イ．認証障害時は必ず全機器を停止し、業務影響を考えない
ウ．機器種別・業務影響ごとに、認証障害時VLANや限定ACLなどの縮退ポリシーを事前定義する
エ．802.1Xを使えば認証サーバ障害は発生しない
正答：ウ
4肢解説
ア：不正接続リスクが非常に高い。
イ：医療等では可用性要件を満たさない可能性がある。
ウ：正しい。全許可または全拒否の二択ではなく、リスクと可用性を踏まえた限定的なフォールバックが考えられる。
エ：外部依存サービスには障害があり得る。
総合解説：認証障害時のfail-open/closedは業務クリティカル度と脅威を踏まえ、隔離・限定通信を含めて設計する。

問60 802.1Xで利用者認証は成功してAccess-Acceptが返るが、認証後に管理ネットワークへ到達できてしまう。最も適切な切り分けはどれか。
ア．認証成功なのでアクセス範囲は確認不要である
イ．端末のMACアドレスを変えれば必ず適切な権限になる
ウ．DNSのMXレコードを変更する
エ．認証成功後に適用されるVLAN・ACL・ロールなど認可ポリシーを確認する
正答：エ
4肢解説
ア：認証と認可は別の機能である。
イ：認可ポリシーの根本修正ではない。
ウ：ネットワーク認可とは無関係である。
エ：正しい。本人確認が成功していても、付与するネットワーク権限が過大なら認可設定の問題である。
総合解説：AAAではAuthenticationとAuthorizationを区別し、認証後に必要最小限のアクセス権を適用する。

問61 ネットワークファイアウォールの主な役割として最も適切なものはどれか。
ア．定めたポリシーに基づいてネットワーク間・ホスト間の通信を許可または拒否する
イ．全アプリケーションの脆弱性を自動修正する
ウ．暗号鍵を自動発行するCAの代替となる
エ．DNSサーバを必ず不要にする
正答：ア
4肢解説
ア：正しい。FWは異なるセキュリティ境界間のトラフィックをルールに従って制御する。
イ：FWだけでソフトウェア脆弱性を修正することはできない。
ウ：証明書発行機能ではない。
エ：名前解決とは別の機能である。
総合解説：FWの種類にはパケットフィルタ、ステートフル、アプリケーションプロキシ等があり、要件に応じて使い分ける。

問62 NATの主な役割として最も適切なものはどれか。
ア．WebアプリのSQLインジェクションを検出する
イ．IPアドレスを変換し、内部アドレスと外部アドレスの対応を管理する
ウ．利用者の本人確認を行う
エ．TLS証明書を発行する
正答：イ
4肢解説
ア：WAFなどの役割である。
イ：正しい。NATはIPアドレス変換を行う技術で、アドレス空間の接続や共有に利用される。
ウ：認証機能ではない。
エ：PKIのCAの役割である。
総合解説：NATによって内部アドレスが直接見えにくくなることはあっても、NAT自体をセキュリティ制御の代替と考えるべきではない。

問63 WAFの主な保護対象として最も適切なものはどれか。
ア．OSPF経路広告だけ
イ．EthernetのFCSエラーだけ
ウ．HTTP/HTTPSを利用するWebアプリケーションへの攻撃
エ．NTPの時刻ずれだけ
正答：ウ
4肢解説
ア：ルーティングプロトコルの保護に特化した装置ではない。
イ：L2伝送誤りの検出が主目的ではない。
ウ：正しい。WAFはHTTP通信を解析し、SQLインジェクションやXSSなどWebアプリ攻撃の検知・遮断に用いられる。
エ：時刻同期専用装置ではない。
総合解説：WAFはWebアプリ層を保護するが、サーバOSのパッチやアプリケーション修正の代替ではない。

問64 外向きTCP接続を開始した通信の戻りパケットを、確立済みセッション状態に基づいて自動的に許可するFWは何と呼ばれるか。
ア．単純な静的パケットフィルタだけ
イ．WAF
ウ．NTPサーバ
エ．ステートフルファイアウォール
正答：エ
4肢解説
ア：個々のパケット条件だけで評価し、接続状態を必ず追跡するわけではない。
イ：Webアプリ層のHTTP解析が主目的である。
ウ：時刻同期を提供する。
エ：正しい。ステートフルFWは接続状態を追跡し、セッションに属する戻り通信を判断する。
総合解説：ステートフルFWではTCP状態、NAT状態、タイムアウト等を保持するため、冗長化時には状態同期が重要になる。

問65 社内端末の代理として外部Webサイトへ接続し、URLフィルタやアクセスログを集中管理する装置はどれか。
ア．フォワードプロキシ
イ．リバースプロキシ
ウ．VRRPルータ
エ．RADIUSサーバ
正答：ア
4肢解説
ア：正しい。フォワードプロキシはクライアントの代理として外部サービスへアクセスする。
イ：主にサーバ側の前段で外部クライアントからの要求を受ける。
ウ：デフォルトゲートウェイ冗長化機能である。
エ：認証・認可を扱う。
総合解説：フォワードプロキシは利用者側、リバースプロキシは公開サーバ側の代理として使われる。

問66 内部端末がマルウェア感染した場合の外部C2通信や情報持出しを抑えるため、外向き通信も必要最小限に制御する考え方はどれか。
ア．ingress通信だけを全許可する
イ．egress filtering
ウ．NATを有効にするだけ
エ．DNS TTLを固定する
正答：イ
4肢解説
ア：外向き制御の説明ではない。
イ：正しい。入口だけでなく出口通信を制御することで、侵害後の外部通信を抑制・検知しやすくする。
ウ：外向き宛先・ポートの制御にはならない。
エ：C2通信制御の一般的な手段ではない。
総合解説：egress制御では業務上必要な宛先・プロトコルを把握し、ログと組み合わせる。

問67 組織がHTTPS通信を復号してマルウェア検査するTLSインスペクションを導入する。最も重要な設計上の注意点はどれか。
ア．復号するのでTLS証明書検証は一切不要になる
イ．全サイトを無条件復号すれば法務・プライバシー検討は不要である
ウ．復号装置が機密情報を扱うため、秘密鍵・ログ・例外サイト・証明書配布を厳格に管理する
エ．TLSインスペクションはネットワーク遅延に影響しない
正答：ウ
4肢解説
ア：中継先証明書の検証は引き続き重要である。
イ：機微情報や規制への配慮が必要である。
ウ：正しい。TLSインスペクション装置は中継点で平文を扱うため、高い保護とプライバシー配慮が必要である。
エ：暗号処理で性能影響が生じ得る。
総合解説：導入時は技術性能だけでなく、証明書信頼、プライバシー、除外対象、障害時動作を設計する。

問68 上から順に評価するFWで、1行目に『送信元ANY、宛先Web、TCP ANYを許可』、2行目に『送信元Guest、宛先Web、TCP/22を拒否』がある。問題として最も適切なものはどれか。
ア．後ろの拒否が常に優先される
イ．TCP/22だけは自動的にDNSへ転送される
ウ．ANYは空集合なので何も許可しない
エ．1行目の広い許可により、2行目のGuest向け拒否が到達不能なシャドールールになる
正答：エ
4肢解説
ア：上から順に最初の一致を採用する前提と矛盾する。
イ：そのような動作はない。
ウ：ANYは全送信元等を表す。
エ：正しい。先にANY許可へ一致するため、後続の拒否が評価されない。
総合解説：FWポリシーではルール順序、重複、シャドーイング、期限切れ例外を定期的にレビューする。

問69 冗長構成で往路はFW-A、復路はFW-Bを通る。FW間でセッション状態を共有していない場合に起きやすい問題はどれか。
ア．FW-Bが復路パケットを未確立セッションと判断して破棄する
イ．往復経路が異なればTCPは必ず高速化する
ウ．FW-Bは自動的にFW-Aのメモリを参照する
エ．DNSが自動的に復路をFW-Aへ変更する
正答：ア
4肢解説
ア：正しい。ステートフルFWは接続状態に依存するため、非対称経路では状態共有や経路対称化が必要になる。
イ：状態管理上の問題が起き得る。
ウ：状態同期を設定していなければ共有されない。
エ：IP経路制御の問題である。
総合解説：FW冗長化ではルーティング設計とセッション同期を合わせて検証する。

問70 Webアプリに既知のSQLインジェクション脆弱性があり、WAFルールで攻撃文字列を一時遮断している。長期対策として最も適切なものはどれか。
ア．WAFがあるのでアプリ脆弱性を永久放置する
イ．WAFを緩和策として活用しつつ、アプリ側でパラメータ化クエリ等の根本修正を行う
ウ．WAFを外して全HTTPを許可する
エ．DNSサーバを変更すればSQLインジェクションが解消する
正答：イ
4肢解説
ア：回避パターンや設定ミスで攻撃が通る可能性がある。
イ：正しい。WAFは防御層として有効だが、脆弱性そのものを修正する対策と組み合わせるべきである。
ウ：脆弱性への防御を弱める。
エ：アプリ入力処理の問題である。
総合解説：多層防御ではWAFによる仮想パッチと、アプリケーションの根本修正・安全な開発を併用する。

問71 IDSとIPSの一般的な違いとして最も適切なものはどれか。
ア．IDSは必ず通信を遮断し、IPSはログだけを取る
イ．両者ともIPアドレス配布プロトコルである
ウ．IDSは主に検知・通知し、IPSはインラインで遮断などの防止動作も行う
エ．IPSは暗号鍵発行専用装置である
正答：ウ
4肢解説
ア：役割が逆である。
イ：DHCPとは異なる。
ウ：正しい。IPSは通信経路上で悪性通信を止める能力を持つのが一般的である。
エ：PKIの機能ではない。
総合解説：IDS/IPSは配置方式と検知方式を区別し、可用性・誤検知リスクを考慮して利用する。

問72 既知攻撃の特徴的なバイト列や通信パターンと照合して検知する方式はどれか。
ア．アノマリベース検知
イ．NAT
ウ．ECMP
エ．シグネチャベース検知
正答：エ
4肢解説
ア：正常状態からの逸脱を評価する方式である。
イ：IPアドレス変換である。
ウ：等コスト経路分散である。
エ：正しい。既知の攻撃パターンをルール・シグネチャとして登録し、一致を検出する。
総合解説：シグネチャ方式は既知攻撃に強い一方、未知攻撃や変形に対しては限界がある。

問73 多数の拠点・クラウド間通信からフローやパケットメタデータを集め、通常と異なる通信や横展開・C2の兆候を継続監視する仕組みに最も近いものはどれか。
ア．NDR
イ．CA
ウ．DHCP
エ．RAID
正答：ア
4肢解説
ア：正しい。NDRはネットワークテレメトリを分析し、不審な振る舞いの検知・調査・対応を支援する。
イ：公開鍵証明書を発行・管理する仕組みである。
ウ：IPアドレスや関連設定を配布するプロトコルである。
エ：ストレージ冗長化方式である。
総合解説：NDRは現代的なNetwork Detection and Responseの概念で、NIST SP 800-94のNetwork Behavior Analysisに近い分析も含む。

問74 正常なバックアップ通信を攻撃と判定してIPSが遮断した。この事象は何に該当するか。
ア．False Negative
イ．False Positive（誤検知）
ウ．True Positive
エ．True Negative
正答：イ
4肢解説
ア：実際の攻撃を正常と見逃す事象である。
イ：正しい。正常な事象を悪性と誤って判定するのがFalse Positiveである。
ウ：実際の攻撃を正しく検出した場合である。
エ：正常通信を正常と正しく判断した場合である。
総合解説：IPSではFalse Positiveが可用性へ直接影響するため、検知精度と遮断ポリシーのチューニングが重要である。

問75 インターネットからDMZへの通信と、DMZから内部への横展開の両方を観測したい。NIDS配置として最も適切な考え方はどれか。
ア．インターネット出口1か所だけで全内部通信も必ず見える
イ．DNSサーバだけにNIDSを置けば全通信が複製される
ウ．外部境界だけでなくDMZ-内部境界など重要な複数監視点へセンサーを配置する
エ．センサーは通信経路から遠いほど精度が高い
正答：ウ
4肢解説
ア：経路によっては東西通信を観測できない。
イ：そのような保証はない。
ウ：正しい。1か所だけでは経路・ゾーンごとの攻撃を見落とす可能性がある。
エ：観測したいトラフィックへアクセスできる配置が必要である。
総合解説：センサー配置はネットワーク構成、暗号化、帯域、監視目的を基に決める。

問76 HTTPS通信がエンドツーエンドで暗号化され、NDRセンサーが復号鍵を持たない。依然として分析可能な情報として適切なものはどれか。
ア．暗号化されるとIPアドレスも必ず完全に隠れる
イ．暗号化通信では何も観測できない
ウ．HTTPSならマルウェア通信は発生しない
エ．送受信IP、ポート、通信量、タイミング、TLSメタデータなど
正答：エ
4肢解説
ア：通常のTLSではIPヘッダは経路上で必要である。
イ：メタデータは多くの場合観測できる。
ウ：攻撃者もTLSを利用し得る。
エ：正しい。ペイロード内容は見えなくても、フロー・メタデータから不審な振る舞いを検知できる場合がある。
総合解説：暗号化が増える環境ではエンドポイント、TLSメタデータ、DNS、フローを組み合わせた検知が重要になる。

問77 新しいIPSを初日から全シグネチャ遮断モードで投入したところ、業務通信が多数停止した。改善として適切なものはどれか。
ア．監視モードでベースラインと誤検知を確認し、重要ルールから段階的に遮断へ移行する
イ．業務停止しても全アラートを無視する
ウ．IPSを全て永久無効化する
エ．DNS TTLを変更すれば誤検知が消える
正答：ア
4肢解説
ア：正しい。環境固有の正常通信を把握し、誤検知を調整してから防止動作を拡大するのが安全である。
イ：可用性と検知品質を損なう。
ウ：防御効果を失う。
エ：検知ルールのチューニングとは無関係である。
総合解説：IPSは検知精度、業務影響、シグネチャ更新を継続的に評価する。

問78 インラインIPS障害時に、通信継続を優先するfail-open設定のリスクとして最も適切なものはどれか。
ア．fail-openでは必ず全通信が暗号化される
イ．IPS故障中に検査されない通信が通過し、攻撃を遮断できない可能性がある
ウ．fail-openならIPS故障が起きなくなる
エ．fail-openではDNSだけが停止する
正答：イ
4肢解説
ア：そのような機能ではない。
イ：正しい。可用性を優先する代わりに、防御機能が失われる時間が発生する。
ウ：故障時の通信挙動を決める設定である。
エ：全体の通過通信に関係する。
総合解説：fail-open/closedはシステムの可用性要求とセキュリティリスクを比較して選ぶ。

問79 端末Aが深夜に多数サーバへSMB接続を試み、DNSでは新規ドメインを頻繁に引き、外部へ一定間隔の少量通信も行っている。単一アラートは弱いが総合的に最も適切な判断はどれか。
ア．各イベントが単独で低重要度なので全て無視する
イ．SMB通信は常に攻撃なので全社で完全禁止する
ウ．横展開とC2通信の可能性を疑い、フロー・DNS・認証ログを相関して調査する
エ．DNSログはネットワーク検知に利用できない
正答：ウ
4肢解説
ア：複合すると高リスクな挙動になり得る。
イ：業務利用もあり得るため文脈評価が必要である。
ウ：正しい。複数の弱いシグナルを時系列で相関すると侵害シナリオが見えやすくなる。
エ：C2・DGA等の分析に有用である。
総合解説：NDRではフローだけでなくDNS、認証、EDR等の情報を相関し、攻撃チェーンとして評価する。

問80 データセンターのNDRは北南通信だけをSPAN取得しており、同一仮想基盤内のVM間通信は物理スイッチへ出ない。問題として最も適切なものはどれか。
ア．北南通信を監視していれば東西通信も必ず全て見える
イ．SPANを使うと仮想通信が自動的に物理へ複製される
ウ．NDRはパケットを見る必要がないので配置は無関係である
エ．東西通信が監視範囲外となり、VM間横展開を見逃す可能性がある
正答：エ
4肢解説
ア：転送経路が異なれば観測できない。
イ：設定や仮想基盤機能が必要である。
ウ：フローやメタデータの取得点も重要である。
エ：正しい。仮想スイッチ内通信が物理センサーへ届かない場合、可視性のギャップが生じる。
総合解説：クラウド・仮想環境では仮想TAP、VPC Flow Logs、エージェント等で東西可視性を補完する。

問81 IPsecが主に保護するOSI/TCP-IP上の層として最も近いものはどれか。
ア．IP層（ネットワーク層）
イ．アプリケーション層だけ
ウ．物理層だけ
エ．DNS層
正答：ア
4肢解説
ア：正しい。IPsecはIPパケットを保護するネットワーク層のセキュリティ機構である。
イ：特定アプリに限定されずIP通信を保護できる。
ウ：電気・光信号の保護技術ではない。
エ：DNS専用ではない。
総合解説：IPsecはホスト間、拠点間、リモートアクセスなど様々なVPN構成に利用できる。

問82 IPsecのESP（Encapsulating Security Payload）が提供できる代表的な機能はどれか。
ア．DNS名前解決だけ
イ．IPパケットの機密性と完全性・送信元認証の保護
ウ．EthernetのMACアドレス学習
エ．証明書発行
正答：イ
4肢解説
ア：ESPはDNS専用ではない。
イ：正しい。ESPは暗号化による機密性に加え、構成に応じて完全性・認証・リプレイ保護を提供する。
ウ：L2スイッチの機能である。
エ：CAの役割である。
総合解説：現代のIPsec VPNではESPが中心的に利用され、IKEが鍵・SA確立を担当する。

問83 二つの拠点LANをルータ同士で常時安全に接続する用途に最も適した分類はどれか。
ア．リモートアクセスVPNだけ
イ．WAF
ウ．サイト間VPN
エ．NDR
正答：ウ
4肢解説
ア：個々の利用者端末が組織へ接続する用途が中心である。
イ：Webアプリ保護装置である。
ウ：正しい。拠点側ゲートウェイ同士でネットワークを接続する方式である。
エ：ネットワーク検知・対応の仕組みである。
総合解説：VPN方式は接続主体がネットワーク同士か利用者端末かで設計が異なる。

問84 拠点間IPsecで、元のIPパケット全体を暗号化して新しい外側IPヘッダでカプセル化する方式はどれか。
ア．トランスポートモード
イ．NATだけ
ウ．GREだけ
エ．トンネルモード
正答：エ
4肢解説
ア：主に元のIPヘッダを残しペイロードを保護する。
イ：暗号化トンネル方式ではない。
ウ：カプセル化は行うが単独では暗号化を提供しない。
エ：正しい。トンネルモードでは元IPパケット全体を内包し、VPNゲートウェイ間で利用しやすい。
総合解説：サイト間VPNではトンネルモードが代表的で、内側アドレスを外側から隠す効果もある。

問85 リモートワーク端末のインターネット通信も全て企業VPNゲートウェイ経由にする方式はどれか。
ア．フルトンネル
イ．スプリットトンネル
ウ．VLANトランク
エ．DNSラウンドロビン
正答：ア
4肢解説
ア：正しい。フルトンネルでは企業向け・インターネット向けを含む全通信をVPNへ通す。
イ：企業宛てだけVPNへ送り、一般インターネットはローカル回線へ出す構成が代表的である。
ウ：L2で複数VLANを運ぶ方式である。
エ：名前解決での分散方式である。
総合解説：フルトンネルは集中検査しやすい一方、VPN帯域・遅延・クラウドSaaSの迂回経路を考慮する必要がある。

問86 外部委託者へ社内の特定Webアプリだけを公開し、端末へ広いL3接続を与えたくない。適した方式として候補になるものはどれか。
ア．全社LANへのフルトンネルを無条件許可する
イ．ブラウザベースのSSL/TLS VPNやアプリケーションプロキシ型アクセス
ウ．全アプリをインターネットへ直接公開する
エ．NATだけを設定して認証しない
正答：イ
4肢解説
ア：必要以上のネットワーク到達性を与える。
イ：正しい。特定Webアプリだけを公開する場合、クライアントレス型・プロキシ型で範囲を限定しやすい。
ウ：アクセス制御を弱める。
エ：利用者認証が不足する。
総合解説：リモートアクセス方式は必要資源、端末管理、認証、アプリ互換性に応じて選択する。

問87 VPNのID・パスワードがフィッシングで漏えいするリスクを下げたい。最も適切な対策の組合せはどれか。
ア．パスワードを全社員で共通化する
イ．VPNポータルをHTTP平文にする
ウ．MFAを導入し、端末のパッチ・EDR状態なども接続条件として確認する
エ．利用者認証を廃止してIPアドレスだけで許可する
正答：ウ
4肢解説
ア：漏えい時の影響を拡大する。
イ：認証情報漏えいリスクを高める。
ウ：正しい。認証要素を増やし、端末状態も評価することで盗用資格情報だけによる侵入を抑える。
エ：なりすまし・共有回線に弱い。
総合解説：リモートアクセスでは利用者認証、端末信頼、最小権限、ログ監視を組み合わせる。

問88 リモート端末が家庭用NATルータ配下にあり、IPsec通信を安定して通過させたい。検討すべき機能として最も適切なものはどれか。
ア．STP
イ．DNSSEC
ウ．WAF
エ．NAT Traversal（NAT-T）
正答：エ
4肢解説
ア：L2ループ防止機能である。
イ：DNS応答の真正性検証である。
ウ：Webアプリ保護である。
エ：正しい。NAT-TはIPsec ESP等をUDPでカプセル化してNAT環境を通過しやすくする。
総合解説：NAT環境ではIPsecのアドレス・ポート変換との整合を考え、IKEv2/NAT-T等を利用する。

問89 リモート利用者2,000人が同時接続し、1人当たり平均2Mbit/sをVPN経由で利用する。30%の余裕を持たせる場合、VPNゲートウェイ群の暗号化スループットとして最低限必要な値はどれか。
ア．5.2Gbit/s（4Gbit/s×1.3で30%余裕を加える）
イ．2.6Gbit/s（必要量の約半分）
ウ．4.0Gbit/s（余裕を加えない基礎需要）
エ．6.0Gbit/s（最低限より大きな任意余裕を見込む）
正答：ア
4肢解説
ア：正しい。2,000×2Mbit/s=4,000Mbit/s=4Gbit/s、30%余裕で4×1.3=5.2Gbit/sである。
イ：必要量の半分である。
ウ：余裕30%を反映していない。
エ：余裕はあるが設問の最低限値ではない。
総合解説：実設計では暗号方式、パケットサイズ、同時セッション、認証処理、N-1障害時容量も考慮する。

問90 社内VPN接続中の端末が、同時に家庭のインターネットへ直接通信するスプリットトンネル構成である。主なセキュリティ上の注意点はどれか。
ア．スプリットトンネルなら通信は全て企業FWを必ず通る
イ．侵害されたローカル側ネットワークや外部通信から企業VPNへの橋渡し経路となるリスクを評価する
ウ．スプリットトンネルでは端末マルウェア対策は不要になる
エ．IPsecを使えば端末側のリスクはゼロになる
正答：イ
4肢解説
ア：一般インターネット通信はローカル出口へ出る。
イ：正しい。端末が企業と外部ネットワークの双方へ同時接続するため、端末侵害時の経路になり得る。
ウ：むしろ端末防御が重要である。
エ：VPNは通信路を保護するが端末侵害は防げない。
総合解説：スプリットトンネル採用時は端末セキュリティ、ローカルLANアクセス、DNS、クラウド向け経路を含めてリスク評価する。

問91 IP送信元スプーフィングの説明として最も適切なものはどれか。
ア．IPヘッダの送信元アドレスを偽装して、実際とは異なる送信元に見せかける
イ．宛先IPアドレスを必ず暗号化する
ウ．DNS名を別名へ変更するだけ
エ．TCPのポート番号を全て0にする
正答：ア
4肢解説
ア：正しい。送信元IPアドレスを偽ることで、攻撃元の隠蔽や反射攻撃などに悪用されることがある。
イ：IPスプーフィングは暗号化方式ではない。
ウ：IPヘッダの送信元アドレス偽装とは異なる。
エ：送信元IPアドレス偽装の定義ではない。
総合解説：送信元IPアドレスは通常それ自体で送信者の真正性を保証しないため、フィルタリングや上位層認証が必要である。

問92 同一LAN上で攻撃者が偽のARP情報を送信し、デフォルトゲートウェイのIPアドレスを自分のMACアドレスへ対応付けさせた。起こり得る結果として最も適切なものはどれか。
ア．端末の公開鍵証明書が自動更新される
イ．端末からゲートウェイ宛てのフレームが攻撃者へ送られ、中間者攻撃の足掛かりになる
ウ．DNSSECの署名が自動失効する
エ．OSPFエリアが自動的に分割される
正答：イ
4肢解説
ア：ARPとPKIは別の仕組みである。
イ：正しい。ARPキャッシュを偽情報で汚染すると、攻撃者が通信経路へ割り込める。
ウ：ARPスプーフィングの直接効果ではない。
エ：L3ルーティング設計とは無関係である。
総合解説：ARPには強い認証機構がないため、LAN内の中間者攻撃対策としてスイッチ側の検査機能や端末間暗号化が重要になる。

問93 中間者攻撃（MITM）の説明として最も適切なものはどれか。
ア．大量の端末から一斉にパケットを送る攻撃だけ
イ．ファイルを暗号化して身代金を要求する攻撃
ウ．通信する二者の間に攻撃者が入り、双方になりすまして通信を盗聴・改変する
エ．脆弱性修正パッチを適用する行為
正答：ウ
4肢解説
ア：これはDDoSの説明に近い。
イ：ランサムウェアの説明である。
ウ：正しい。攻撃者が通信経路または信頼関係へ介入し、双方から正規相手に見えるよう振る舞う攻撃である。
エ：防御側の運用であり攻撃ではない。
総合解説：MITM対策では、証明書検証、相互認証、暗号化、信頼できないL2ネットワークでの防御などを組み合わせる。

問94 ISPの顧客網から、顧客へ割り当てていない送信元IPアドレスを持つパケットが外部へ出ようとしている。BCP38の考え方に沿う処理はどれか。
ア．宛先が存在すれば送信元に関係なく必ず転送する
イ．パケットをDNSへ転送して確認する
ウ．送信元アドレスを全て同一値へNATすることだけがBCP38である
エ．割当て範囲と整合しない送信元アドレスのパケットを境界で破棄する
正答：エ
4肢解説
ア：送信元偽装を許してしまう。
イ：送信元アドレス検証の方式ではない。
ウ：BCP38の本質は送信元アドレスの妥当性検証である。
エ：正しい。ingress filteringにより偽装送信元アドレスを持つトラフィックが上流へ出るのを抑制する。
総合解説：送信元アドレス検証は反射・増幅攻撃や攻撃元隠蔽を困難にする重要なネットワーク衛生策である。

問95 公衆Wi-FiでHTTPSサイトへ接続したところ、通常は出ない『証明書が信頼できない』警告が表示された。安全な対応として最も適切なものはどれか。
ア．警告を無視して機密情報を入力せず、接続先・証明書・ネットワーク状況を確認する
イ．警告が出るほど暗号強度が高いのでそのまま続行する
ウ．HTTPSなら証明書が不正でも機密性は必ず保証される
エ．ブラウザの時刻を毎回1年進めれば解決する
正答：ア
4肢解説
ア：正しい。偽アクセスポイントやTLS中間者攻撃の可能性を含むため、証明書警告を安易に無視すべきではない。
イ：警告は信頼性検証に問題があることを示す。
ウ：攻撃者とのTLS接続を確立している可能性がある。
エ：証明書検証を壊し、根本対策にならない。
総合解説：HTTPSは暗号化だけでなく相手認証が重要であり、証明書チェーンとサービス名の検証がMITM耐性に直結する。

問96 攻撃者が通信を盗聴できない状態で既存TCP接続へ偽造セグメントを注入しようとしている。攻撃を困難にするTCP側の要素として重要なものはどれか。
ア．全TCP接続で同じ初期シーケンス番号を使う
イ．予測困難な初期シーケンス番号と厳格なセグメント受理判定
ウ．ACK番号を常に0へ固定する
エ．DNS TTLを短くする
正答：イ
4肢解説
ア：推測を容易にする。
イ：正しい。シーケンス番号を推測しにくくし、RST/SYN等の受理条件を強化することでblind injectionへの耐性が高まる。
ウ：TCPの信頼性制御を壊す。
エ：TCPセッション注入への対策ではない。
総合解説：RFC 6528は初期シーケンス番号生成を、RFC 5961はblind in-window攻撃へのTCPの頑健性向上を扱う。

問97 Webアプリでログイン前に発行したセッションIDを、ログイン成功後もそのまま利用している。セッション固定攻撃を抑える対策として最も適切なものはどれか。
ア．ログイン後も同じセッションIDを永久利用する
イ．セッションIDを利用者名そのものにする
ウ．認証成功時に新しい予測困難なセッションIDへ再発行する
エ．HTTPのステータスコードを全て200にする
正答：ウ
4肢解説
ア：攻撃者が既知のIDを悪用しやすい。
イ：推測容易で安全性が低い。
ウ：正しい。攻撃者が事前に知るセッションIDを認証後も使い続けると、セッション固定が成立しやすい。
エ：セッション固定対策にはならない。
総合解説：認証境界ではセッション識別子を更新し、十分なランダム性、Secure/HttpOnly属性、適切な失効を組み合わせる。

問98 正規利用者が送った認証済み要求を攻撃者が記録し、後でそのまま再送して不正処理を実行しようとしている。代表的な対策はどれか。
ア．全要求に同じ固定nonceを使う
イ．暗号化を一切行わず平文で送る
ウ．DNS名を毎回変更するだけ
エ．nonce、時刻、シーケンス番号などを検証し、同じ認証済みメッセージの再利用を拒否する
正答：エ
4肢解説
ア：再利用可能となりリプレイ耐性がない。
イ：盗聴・再利用の危険を高める。
ウ：メッセージ再利用を直接防がない。
エ：正しい。各要求に一意性や有効時間を持たせると、過去の正規通信を再送する攻撃を防ぎやすい。
総合解説：認証済み通信でも鮮度確認がなければリプレイされ得るため、プロトコル設計では一意性・有効期限を持たせる。

問99 同一LANで、ゲートウェイIP 192.0.2.1に対するARP Replyが短時間に複数MACアドレスから到着し、利用者端末のARPキャッシュが頻繁に変化している。最も疑うべき事象はどれか。
ア．ARPスプーフィングによる中間者攻撃またはなりすまし
イ．正常なDNSラウンドロビン
ウ．NTPの時刻同期
エ．OSPFのECMP
正答：ア
4肢解説
ア：正しい。単一ゲートウェイIPに対するMAC対応が不自然に変化するのはARP偽装の典型的な兆候である。
イ：DNSはIPとMACのARP対応を変更しない。
ウ：ARPキャッシュ変動の原因ではない。
エ：同一LAN端末のARP Replyが複数MACから来る説明にはならない。
総合解説：ARP監視では、IP-MAC対応の急変、gratuitous ARPの異常増加、スイッチポート位置などを相関すると切り分けやすい。

問100 長時間TCP接続が頻繁に突然切断される。キャプチャでは、RSTセグメントのTTLや到着経路が通常の対向ホスト通信と異なり、シーケンス番号は受理範囲付近にある。最も適切な調査方針はどれか。
ア．RSTは常に正規相手しか生成できないので調査不要である
イ．偽造RST注入を疑い、送信元経路・シーケンス番号・RFC 5961対応状況を確認する
ウ．TLS証明書だけ更新すればTCP RSTは必ず消える
エ．DNSSECを導入すれば全TCP RSTを防げる
正答：イ
4肢解説
ア：送信元IPを偽装したRST注入は理論上可能である。
イ：正しい。通常通信と異なる経路特性を持つRSTはセッション強制切断攻撃の可能性がある。
ウ：TCP層のRST受理条件とは別問題である。
エ：DNS応答の真正性保護でありTCP RST対策ではない。
総合解説：blind RST等への防御ではシーケンス番号検証やchallenge ACKなどTCP実装の防御強化が重要である。

問101 DDoS攻撃の説明として最も適切なものはどれか。
ア．単一端末のパスワードを推測する攻撃だけ
イ．公開鍵証明書を発行する処理
ウ．多数の分散した送信元などから大量の要求を送り、対象サービスの資源を枯渇させる
エ．DNSレコードを正しく更新する運用
正答：ウ
4肢解説
ア：可用性を狙う分散型攻撃の説明ではない。
イ：攻撃ではない。
ウ：正しい。DDoSでは複数の攻撃元を協調させ、帯域・接続状態・処理能力などを圧迫する。
エ：正常な管理作業である。
総合解説：DDoSにはボリューム型、プロトコル状態枯渇型、アプリケーション層型などがある。

問102 DNS反射増幅攻撃の仕組みとして最も適切なものはどれか。
ア．被害者が自分自身へDNS問い合わせを送るだけ
イ．DNSSEC署名を検証する処理
ウ．TCPの3ウェイハンドシェイクを高速化する攻撃
エ．被害者IPを送信元に偽装した小さなDNS問い合わせを多数送り、より大きな応答を被害者へ集中させる
正答：エ
4肢解説
ア：反射元を利用する攻撃の説明ではない。
イ：正常なDNSセキュリティ機能である。
ウ：DNS増幅の仕組みではない。
エ：正しい。送信元偽装と、問い合わせより応答が大きくなる性質を組み合わせた反射・増幅攻撃である。
総合解説：DNS反射増幅対策ではオープンリゾルバ抑止、送信元アドレス検証、レート制御など複数対策が必要である。

問103 TCP SYN floodで主に狙われるサーバ側資源はどれか。
ア．接続確立途中の半開接続状態を保持するキューや関連資源
イ．DNSキャッシュのTTLだけ
ウ．EthernetのVLAN ID
エ．証明書のシリアル番号
正答：ア
4肢解説
ア：正しい。大量のSYNに対しSYN-ACKを返し、ACKを待つ状態を大量に作らせて資源を枯渇させる。
イ：TCP接続状態とは無関係である。
ウ：SYN floodの主要資源ではない。
エ：TCP半開接続とは関係しない。
総合解説：SYN cookies等は、半開接続状態の保持を減らす代表的な緩和策の一つである。

問104 社内利用だけを想定した再帰DNSサーバが、インターネット上の任意の送信元から再帰問い合わせを受け付けている。問題として最も適切なものはどれか。
ア．再帰を公開すると必ずDNSSECが強化される
イ．DNS反射・増幅攻撃のリフレクタとして悪用される可能性がある
ウ．外部公開するほどDDoS耐性が必ず上がる
エ．MXレコードが自動的に削除される
正答：イ
4肢解説
ア：DNSSECとは別の設定である。
イ：正しい。不要な外部再帰を許可すると、送信元偽装問い合わせへの大きな応答を第三者へ返す踏み台になり得る。
ウ：むしろ攻撃へ悪用される可能性がある。
エ：再帰設定とは無関係である。
総合解説：再帰DNSは利用を正当なクライアントへ限定し、権威DNSとの役割分離も検討する。

問105 UDP DNSの偽応答をキャッシュへ混入させる攻撃を困難にするため、DNSSEC以外の基本的な耐性向上策として適切なものはどれか。
ア．全問い合わせで同じトランザクションIDと送信元ポートを使う
イ．DNS応答の送信元を確認せず最初の応答を必ず受理する
ウ．問い合わせIDとUDP送信元ポートを十分にランダム化し、受理する応答条件を厳格にする
エ．TTLを無限大に固定する
正答：ウ
4肢解説
ア：攻撃者による推測を容易にする。
イ：偽応答を受け入れやすくなる。
ウ：正しい。推測空間を広げ、問い合わせと整合しない偽応答を拒否することで攻撃成功率を下げる。
エ：偽情報が入った場合の影響を長期化させる。
総合解説：RFC 5452はトランザクションIDだけでなく送信元ポート等のエントロピーを利用した耐性向上を推奨する。

問106 DNSSECの効果として最も適切なものはどれか。
ア．DNS通信内容を常に暗号化し機密性を保証する
イ．DNSサーバへのDDoSを完全に防ぐ
ウ．IPスプーフィングをネットワーク全体で禁止する
エ．署名検証によりDNS応答データの出所認証と完全性を確認し、偽造DNSデータを検出しやすくする
正答：エ
4肢解説
ア：DNSSECは主に真正性・完全性を提供し、機密性は目的ではない。
イ：可用性攻撃を直接防止するものではない。
ウ：送信元IP検証は別の対策である。
エ：正しい。DNSSECはDNSデータへ暗号学的検証を加える。
総合解説：DNSSECの保護範囲と、DoS対策・通信機密性・送信元スプーフィング対策を区別する必要がある。

問107 自組織のネットワークがDDoS反射攻撃の発信元として悪用されるのを減らすため、出口で有効な対策として最も適切なものはどれか。
ア．自組織から出るパケットの送信元IPが自組織の正当なアドレス範囲かを検証する
イ．外向き通信の宛先IPだけをランダム化する
ウ．DNSサーバのホスト名を毎日変更する
エ．全端末で同じIPアドレスを設定する
正答：ア
4肢解説
ア：正しい。egress側の送信元検証も、偽装パケットを外部へ出さないために有効である。
イ：送信元偽装抑止にはならない。
ウ：送信元偽装には直接関係しない。
エ：アドレス競合を起こす。
総合解説：送信元アドレス検証はインターネット全体で協調して実施されるほど、偽装型反射攻撃を抑えやすい。

問108 100Gbit/sを超えるボリューム型DDoSが発生する可能性があるが、自社インターネット回線は10Gbit/sしかない。境界FWだけで防ぐ設計の問題はどれか。
ア．FWのCPUを高速化すれば10Gbit/s回線が100Gbit/sになる
イ．FWへ届く前に回線が飽和するため、上流ISPやスクラビングサービスでの緩和が必要になる
ウ．DNSSECを有効にすれば全DDoSトラフィックが消える
エ．内部VLANを増やせば上流回線飽和を防げる
正答：イ
4肢解説
ア：物理回線容量は増えない。
イ：正しい。自社回線容量を超える攻撃はオンプレミス装置まで届いた時点で既に回線が詰まる。
ウ：DNSSECはボリューム型DDoS対策ではない。
エ：外部リンク容量には影響しない。
総合解説：DDoS対策は上流フィルタリング、Anycast/CDN、スクラビング、レート制御、アプリ防御などを多層化する。

問109 攻撃者が60バイトのDNS問い合わせを送り、リフレクタから3,000バイトの応答が被害者へ返る。単純な増幅率は何倍か。
ア．5倍（3,000÷600として計算）
イ．20倍（3,000÷150として計算）
ウ．50倍（3,000÷60で計算）
エ．180倍（問い合わせと応答の比ではない）
正答：ウ
4肢解説
ア：1桁小さい。
イ：計算が一致しない。
ウ：正しい。3,000÷60=50である。
エ：問い合わせサイズと応答サイズの比ではない。
総合解説：反射増幅では攻撃者側の送信量より大きい応答を被害者へ集中できるため、オープンサービスと送信元偽装の組合せが危険になる。

問110 権威DNSで、存在しないランダムなサブドメインへの問い合わせが秒間数十万件に急増し、CPU負荷と上流問い合わせが増加している。最も適切な初動はどれか。
ア．存在しない名前なのでログを全て削除して無視する
イ．全DNSサーバを停止して恒久的に名前解決を廃止する
ウ．MXレコードだけ変更する
エ．ランダムサブドメイン型DDoSを疑い、問い合わせパターン・送信元分布を分析し、上流と連携してレート制御や防御を行う
正答：エ
4肢解説
ア：攻撃兆候と可用性影響を見落とす。
イ：業務継続できない。
ウ：ランダム名DDoSの本質的対策ではない。
エ：正しい。大量のランダム名問い合わせはキャッシュ効果を下げ、権威系・再帰系を消耗させる攻撃で見られる。
総合解説：DNS DDoSではQNAME分布、NXDOMAIN率、送信元、キャッシュヒット率、権威・再帰の役割を分けて分析する。

問111 ワーム型マルウェアの特徴として最も適切なものはどれか。
ア．ネットワークや脆弱性を利用して自己増殖し、他のホストへ自動的に拡散する
イ．必ず正規ソフトに偽装し利用者が手動実行しなければ一切動けない
ウ．データを圧縮するだけの正常ツール
エ．DNSSEC署名を生成するプログラム
正答：ア
4肢解説
ア：正しい。ワームは利用者が別ファイルを実行しなくても自律的に拡散する能力を持つことがある。
イ：これはトロイの木馬の典型的説明に近い。
ウ：マルウェアではない。
エ：正常なセキュリティ機能である。
総合解説：マルウェア分類ではワーム、トロイの木馬、ランサムウェア、ボット等の感染・拡散・目的の違いを理解する。

問112 ランサムウェアの典型的な攻撃目的はどれか。
ア．ルーティングテーブルを最適化する
イ．データやシステムを暗号化・利用不能化し、復旧と引換えに金銭を要求する
ウ．証明書を自動更新する
エ．DNSキャッシュを効率化する
正答：イ
4肢解説
ア：正常なネットワーク運用である。
イ：正しい。近年は情報窃取と公開脅迫を組み合わせる二重恐喝もある。
ウ：PKI運用機能である。
エ：ランサムウェアの目的ではない。
総合解説：ランサムウェア対策ではパッチ、MFA、最小権限、EDR、分離バックアップ、インシデント対応を多層化する。

問113 SQLインジェクションが成立しやすい実装として最も問題が大きいものはどれか。
ア．パラメータ化クエリでデータと命令を分離する
イ．入力値をサーバ側で検証する
ウ．利用者入力を適切に分離せずSQL文へ文字列連結して実行する
エ．DBアカウントの権限を必要最小限にする
正答：ウ
4肢解説
ア：代表的な対策である。
イ：適切に行えば防御に寄与する。
ウ：正しい。入力を命令の一部として解釈させる実装はインジェクションを招く。
エ：被害限定に有効である。
総合解説：インジェクション対策ではパラメータ化、入力検証、最小権限を組み合わせる。

問114 同じCVSSスコアの脆弱性が多数あり、限られた時間で修正優先順位を決めたい。CISA KEVカタログの利用として最も適切なものはどれか。
ア．KEVに載っていない脆弱性は永久に修正不要とする
イ．CVSSを全て無視してKEVだけで判断する
ウ．KEVはDNSレコード一覧なので脆弱性管理に使わない
エ．実際に悪用が確認された脆弱性を優先度判断の重要な入力として利用する
正答：エ
4肢解説
ア：他のリスク要因も評価する必要がある。
イ：資産価値、露出、影響、CVSS等も組み合わせる。
ウ：CISAの実悪用脆弱性カタログである。
エ：正しい。KEVは実悪用が確認された脆弱性を示すため、単なる理論上の深刻度とは異なる重要情報になる。
総合解説：脆弱性優先度はCVSSだけでなく、実悪用、外部露出、資産重要度、緩和策の有無を総合する。

問115 重要サーバへ緊急パッチを配布した。脆弱性管理として次に最も重要な確認はどれか。
ア．対象全台へ正常に適用されたか、再起動要否や機能影響も含めて検証する
イ．配布ボタンを押した時点で全台修正済みとみなす
ウ．適用ログを確認せず管理台帳から脆弱性を削除する
エ．パッチ後はバックアップを全て削除する
正答：ア
4肢解説
ア：正しい。配布指示だけでなく、実際の適用状態と動作確認まで行う必要がある。
イ：失敗端末や再起動待ちが残る可能性がある。
ウ：実態と台帳が不一致になる。
エ：復旧手段を失う。
総合解説：企業パッチ管理は識別、優先順位付け、取得、導入、適用、検証までの継続的なプロセスである。

問116 一般利用者がURLのuser_idを他人の値へ変更するだけで、別利用者の注文履歴を閲覧できた。最も近い脆弱性分類はどれか。
ア．暗号化の不備だけ
イ．アクセス制御の不備
ウ．DDoS
エ．DNSキャッシュポイズニング
正答：イ
4肢解説
ア：主原因は認可チェックの欠如である。
イ：正しい。サーバ側で対象資源への認可確認が不足しており、他利用者データへアクセスできている。
ウ：可用性を狙う大量通信攻撃ではない。
エ：DNS応答偽造とは関係しない。
総合解説：OWASP Top 10:2025でもBroken Access Controlは最重要カテゴリの一つで、各要求でサーバ側認可を実施する必要がある。

問117 自社コードに問題はないが、ビルド時に取得した外部ライブラリが改ざんされ、製品へ悪性コードが混入した。最も近いリスクはどれか。
ア．単純な回線輻輳
イ．ARPスプーフィングだけ
ウ．ソフトウェアサプライチェーンの不備
エ．NTP設定ミス
正答：ウ
4肢解説
ア：ソフトウェア改ざんの原因ではない。
イ：LAN内なりすましに限定されない。
ウ：正しい。依存ライブラリ、ビルド基盤、配布経路等の第三者要素を経由した侵害である。
エ：ビルド依存物の改ざんとは異なる。
総合解説：依存関係管理、署名検証、SBOM、信頼できるリポジトリ、ビルド環境保護などがサプライチェーン対策になる。

問118 多数のサーバへ自動ツールで既知脆弱性・設定不備を広く洗い出したい。最初の評価手法として最も適切なものはどれか。
ア．必ず本番環境で破壊的な侵入テストだけを行う
イ．DNSゾーン転送だけで全脆弱性を検出する
ウ．ログを一切収集せず手作業だけで確認する
エ．脆弱性スキャン
正答：エ
4肢解説
ア：影響が大きく、目的に対して過剰である。
イ：検出範囲が限定される。
ウ：大規模環境では効率・網羅性が低い。
エ：正しい。自動スキャナは広範囲の既知脆弱性・設定問題を効率的に特定するのに向く。
総合解説：脆弱性スキャンと侵入テストは目的・深度・リスクが異なり、段階的に使い分ける。

問119 脆弱性AはCVSS 9.8だが社内隔離済みで悪用報告なし。脆弱性BはCVSS 8.1だがインターネット公開機器に存在し、CISA KEV掲載済みである。一般的な優先順位として最も合理的な判断はどれか。
ア．Bを非常に高い優先度で扱い、Aも資産影響を踏まえて計画的に修正する
イ．CVSSが高いAだけを必ず先にし、Bは無視する
ウ．KEV掲載ならCVSSや資産重要度を一切見なくてよい
エ．両方ともパッチせずWAFだけ置けば十分である
正答：ア
4肢解説
ア：正しい。実悪用と外部露出は重大なリスク要因で、CVSSの大小だけでは優先順位を決められない。
イ：実悪用・露出を考慮していない。
ウ：複数要因を総合する必要がある。
エ：対象がWeb以外の場合もあり、根本修正が必要である。
総合解説：リスクベースの脆弱性管理では深刻度、実悪用、到達性、業務影響、緩和策を統合して判断する。

問120 端末1台でランサムウェア挙動を検知し、同端末から多数の共有フォルダへ書込みが始まっている。最も優先度が高い初動はどれか。
ア．調査が終わるまで端末を通常ネットワークへ接続し続ける
イ．端末をネットワークから隔離し、感染拡大を止めつつ証拠・影響範囲を確認する
ウ．バックアップサーバも同じ端末から書込み可能にする
エ．証拠を残さず即座に全ログを削除する
正答：イ
4肢解説
ア：共有先への被害が拡大する。
イ：正しい。被害拡大中は封じ込めを急ぎ、並行してログ・EDR情報等を保存する。
ウ：バックアップまで暗号化される危険を高める。
エ：原因・影響調査が困難になる。
総合解説：マルウェア対応では封じ込め、根絶、復旧に加え、証拠保全と再発防止を組み合わせる。

問121 SIEMの主な役割として最も適切なものはどれか。
ア．全端末へIPアドレスを自動配布する
イ．公開鍵証明書を発行する
ウ．複数システムのログ・イベントを集約し、検索・相関分析・アラートを行う
エ．Ethernetのループを防止する
正答：ウ
4肢解説
ア：DHCPの役割である。
イ：CAの役割である。
ウ：正しい。SIEMはFW、サーバ、認証基盤、クラウド等のイベントを集約し、横断的な検知・調査を支援する。
エ：STP等の役割である。
総合解説：SIEMの価値はログを集めるだけでなく、時系列・主体・資産を横断して相関し、調査可能な形で保持する点にある。

問122 セキュリティログ分析で各機器の時刻を同期する主な理由はどれか。
ア．ログファイルの容量を必ず半分にするため
イ．TLS暗号鍵を自動更新するため
ウ．IPアドレス重複を防ぐため
エ．異なるシステムのイベントを正しい時系列で相関できるようにするため
正答：エ
4肢解説
ア：時刻同期とログ容量は直接関係しない。
イ：時刻は証明書検証等にも関係するが、ログ相関の主目的とは異なる。
ウ：DHCP/IPAM等の課題である。
エ：正しい。時刻がずれると、認証・通信・プロセス実行の順序を誤って解釈する可能性がある。
総合解説：ログ基盤ではタイムゾーン、NTP、サマータイム、機器ごとの時刻精度を統一的に扱う。

問123 インシデント調査で重要ログを改ざん・削除から守るために適切な考え方はどれか。
ア．アクセス制御された集中保管先へ転送し、必要に応じて変更困難な保存方式を利用する
イ．全ログを侵害端末のローカルディスクだけへ保存する
ウ．調査前に古いログを全て削除する
エ．誰でもログを編集できる共有フォルダへ保存する
正答：ア
4肢解説
ア：正しい。侵害端末のローカルログだけに依存すると攻撃者に消去される可能性がある。
イ：端末侵害時に証拠を消される危険がある。
ウ：証拠を失う可能性がある。
エ：完全性を確保できない。
総合解説：ログ保管では機密性・完全性・可用性、保持期間、アクセス権、容量を設計する。

問124 FWはsrc、EDRはsource_ip、クラウドはclientAddressという異なる項目名を使っている。SIEMで横断検索しやすくする処理として最も適切なものはどれか。
ア．全ログを画像ファイルへ変換する
イ．共通スキーマへ正規化し、同じ意味の項目を統一的に扱う
ウ．項目名の違いを無視し手作業だけで読む
エ．IPアドレスを全て同じ値へ置換する
正答：イ
4肢解説
ア：検索・相関が困難になる。
イ：正しい。異種ログを共通フィールドへ変換すると検索・相関ルールを再利用しやすい。
ウ：大規模監視では効率・精度が低い。
エ：主体を識別できなくなる。
総合解説：ログ正規化では元ログも保持し、変換処理による情報欠落を防ぐことが重要である。

問125 同一送信元IPから5分間に200ユーザ名へログイン失敗が発生し、その直後に1アカウントだけ成功した。監視上最も適切な評価はどれか。
ア．成功が1件あるので全失敗ログを正常とみなす
イ．失敗ログはセキュリティ監視に不要なので破棄する
ウ．パスワードスプレーやクレデンシャル攻撃を疑い、成功アカウントと送信元を調査する
エ．DNSのTTLを変更すれば攻撃かどうか判断できる
正答：ウ
4肢解説
ア：むしろ侵害成功の可能性がある。
イ：攻撃検知に有用である。
ウ：正しい。多数アカウントへの失敗と成功の組合せは資格情報攻撃の重要な兆候である。
エ：認証イベント相関とは無関係である。
総合解説：SIEMでは単一イベントより、時間窓・送信元・利用者・成功失敗の組合せで検知精度を高める。

問126 ログ保存容量が限られる中、高機密システムの監視を強化したい。収集優先順位として最も適切な考え方はどれか。
ア．全端末の壁紙変更ログを最優先にする
イ．ログ容量が少ないので認証ログを全て捨てる
ウ．資産重要度に関係なく乱数でログ種別を選ぶ
エ．認証、権限変更、重要データアクセス、FW/EDRなど侵害検知・追跡に必要なログを優先する
正答：エ
4肢解説
ア：高機密システム侵害の追跡価値が低い。
イ：攻撃追跡に重要な情報を失う。
ウ：リスクベースの監視にならない。
エ：正しい。資産重要度と想定攻撃シナリオに基づいて必要ログを選ぶ。
総合解説：ログ管理は『集められるものを全て』ではなく、検知・調査・監査要件から必要性を定義する。

問127 SOCで1日10万件のアラートが出るが、99.9%が既知の正常動作で分析者が重要アラートを見落としている。改善として最も適切なものはどれか。
ア．誤検知原因を分析してルール・閾値・除外条件を調整し、優先度付けを行う
イ．アラート件数を増やすほど安全なので何もしない
ウ．全てのセキュリティ監視を停止する
エ．全アラートを同じ最高優先度にする
正答：ア
4肢解説
ア：正しい。大量の低品質アラートはalert fatigueを招くため、検知品質を継続改善する必要がある。
イ：重要イベントが埋もれる。
ウ：検知能力を失う。
エ：優先順位付けができなくなる。
総合解説：監視では検知率だけでなく、誤検知率、対応時間、アラート価値を測りチューニングする。

問128 攻撃発覚まで平均90日かかる可能性があるのに、全セキュリティログを7日で削除している。主な問題はどれか。
ア．保持期間が短いほどフォレンジック情報が増える
イ．発覚時には侵入初期の証拠が消えており、原因・影響範囲を追跡できない可能性が高い
ウ．7日を超えるログはセキュリティ上必ず無価値である
エ．ログ保持期間はインシデント調査と無関係である
正答：イ
4肢解説
ア：逆である。
イ：正しい。保持期間は検知までの期間、法令、調査要件、容量を踏まえて決める必要がある。
ウ：長期潜伏型攻撃では古いログが重要になる。
エ：タイムライン復元に直結する。
総合解説：ログ保持にはオンライン検索期間と低コストアーカイブ期間を分ける設計も有効である。

問129 1日平均500GBのログを生成し、圧縮後サイズが元の40%になる。90日分を保持するために必要な純ログ容量は、索引・冗長化を無視すると何TBか。
ア．4.5TB（圧縮後日量または期間の扱いが不足）
イ．45TB（500GB×90で圧縮を考慮しない）
ウ．18TB（500GB×0.4×90で計算）
エ．180TB（正しい値の10倍）
正答：ウ
4肢解説
ア：圧縮後の1日量または期間計算が不足している。
イ：圧縮を考慮していない元データ量である。
ウ：正しい。500GB×0.4=200GB/日、200×90=18,000GB=18TBである。
エ：10倍大きい。
総合解説：実際のSIEM容量設計では索引、レプリカ、検索用ホット層、バックアップ、増加率を追加で見積もる。

問130 02:01 VPNログで海外IPから管理者ログイン成功、02:03 EDRでPowerShell実行、02:05 FWで同端末から外部IPへ大量送信、02:10 DB監査ログで大量SELECTが記録された。最も適切な対応はどれか。
ア．各ログは別製品なので関連付けず個別に無視する
イ．DBログだけ削除してアラートを減らす
ウ．VPN成功ログは正常なので必ず調査対象外とする
エ．同一主体の侵害シナリオとして相関し、アカウント・端末を封じ込めてデータ流出範囲を調査する
正答：エ
4肢解説
ア：侵害全体像を見落とす。
イ：証拠を失う。
ウ：異常な場所・後続イベントとの相関が重要である。
エ：正しい。個別ログを時系列で結ぶと資格情報侵害から実行・外部通信・データアクセスまでの連鎖が見える。
総合解説：SIEMの相関分析は主体、端末、IP、時刻を結び付け、攻撃チェーンを再構成するために利用する。

問131 ネットワークフローを識別する際に一般的に用いられる5タプルの組合せはどれか。
ア．送信元IP、宛先IP、送信元ポート、宛先ポート、トランスポートプロトコル
イ．送信元MAC、SSID、DNS TTL、時刻、VLAN名
ウ．利用者名、パスワード、証明書、Cookie、URL
エ．CPU、メモリ、ディスク、温度、電圧
正答：ア
4肢解説
ア：正しい。これらの組合せでTCP/UDPフローを区別するのが一般的である。
イ：一般的なIPフロー5タプルではない。
ウ：アプリ認証情報でありフロー識別子ではない。
エ：システム監視値である。
総合解説：パケット・フロー分析では5タプルを軸に通信量、開始終了時刻、TCP状態等を関連付ける。

問132 取得したディスクイメージやパケットキャプチャにSHA-256等のハッシュ値を記録する主な目的はどれか。
ア．証拠データを必ず暗号化して内容を読めなくするため
イ．取得後に証拠データが変更されていないことを確認するため
ウ．IPアドレスを匿名化するため
エ．ログ容量を必ず半分にするため
正答：イ
4肢解説
ア：ハッシュは暗号化ではない。
イ：正しい。取得時と分析時のハッシュを比較することで証拠の完全性を検証できる。
ウ：完全性検証が主目的である。
エ：ハッシュ計算で元データ容量は減らない。
総合解説：フォレンジックでは証拠取得時刻、担当者、ハッシュ、保管場所を記録し、改変の疑いを減らす。

問133 フォレンジックで揮発性が高く、電源断で失われやすい情報として最も適切なものはどれか。
ア．書込み禁止媒体に保存済みのバックアップ
イ．紙に印刷したネットワーク図
ウ．メモリ上の実行プロセス・接続状態・暗号鍵など
エ．オフライン保管したログアーカイブ
正答：ウ
4肢解説
ア：比較的揮発性が低い。
イ：電源断では失われない。
ウ：正しい。RAM上の情報は電源断や再起動で失われるため、取得優先度を考慮する。
エ：通常は揮発性が低い。
総合解説：証拠収集は揮発性と業務影響を考慮し、必要に応じてメモリ・接続状態を先に取得する。

問134 パケットキャプチャでSYN、SYN+ACK、ACKの順に観測された。この通信状態として最も適切なものはどれか。
ア．TCP接続がRSTで強制終了している
イ．DNSSEC検証が完了している
ウ．IPsec SAが確立している
エ．TCPの3ウェイハンドシェイクが正常に進行している
正答：エ
4肢解説
ア：RSTは観測されていない。
イ：TCPフラグとは無関係である。
ウ：IKE/IPsecの状態はこの3パケットだけでは判断できない。
エ：正しい。標準的なTCP接続確立手順である。
総合解説：パケット解析ではフラグ、シーケンス番号、ACK番号、再送を組み合わせてTCP状態を推定する。

問135 FWの外側で攻撃パケットを観測できるが、内側では同じパケットが見えない。最も自然な解釈はどれか。
ア．FWがその通信を遮断しており、内側へ転送されていない可能性がある
イ．外側と内側のキャプチャは必ず完全同一になる
ウ．内側で見えないので外側キャプチャは必ず偽物である
エ．DNS TTLだけでパケット可視性が決まる
正答：ア
4肢解説
ア：正しい。複数地点で同一通信を比較すると、どこで破棄・変換されたかを切り分けられる。
イ：FW/NAT等で差が生じる。
ウ：境界装置で破棄された可能性がある。
エ：キャプチャ位置の問題である。
総合解説：複数観測点の比較はFW動作、NAT、非対称経路、パケット損失の切り分けに有効である。

問136 TLS 1.3通信をネットワーク上でpcap取得したが、セッション鍵を保持していない。通常直接確認できないものはどれか。
ア．送信元・宛先IPアドレス
イ．暗号化されたHTTP本文の平文内容
ウ．パケット長と到着時刻
エ．TCPポート番号
正答：イ
4肢解説
ア：IPヘッダは通常観測できる。
イ：正しい。鍵なしではTLSアプリケーションデータの内容を通常復号できない。
ウ：暗号化後も観測可能である。
エ：TCPヘッダはTLSの外側にある。
総合解説：暗号化環境ではネットワークメタデータと、端末・サーバ側ログやEDR情報を組み合わせて調査する。

問137 インシデント証拠を法務・監査で説明可能にするため、誰がいつ証拠を取得・移送・保管したかを記録する考え方はどれか。
ア．Round Robin
イ．Split Horizon
ウ．Chain of Custody
エ．Port Mirroring
正答：ウ
4肢解説
ア：負荷分散方式である。
イ：ルーティング/DNS等で使われる別概念である。
ウ：正しい。証拠の取扱履歴を追跡可能にし、不適切な改変や管理の疑いを減らす。
エ：パケット複製機能であり証拠取扱記録そのものではない。
総合解説：技術的ハッシュと管理上のChain of Custodyの両方で証拠の信頼性を高める。

問138 侵害端末のディスクを分析する際の基本的な証拠保全方法として適切なものはどれか。
ア．原本上で直接ファイルを編集しながら調査する
イ．原本の取得前に全ログを削除する
ウ．コピーのハッシュは記録しない
エ．原本を可能な限り変更せず保管し、取得したフォレンジックコピーを用いて分析する
正答：エ
4肢解説
ア：証拠を変更してしまう。
イ：証拠を失う。
ウ：完全性検証ができない。
エ：正しい。分析操作による原本変更を避け、再現可能性を高める。
総合解説：フォレンジックでは原本保護、書込み防止、ハッシュ、作業記録が重要である。

問139 送信側がSeq=1000から500バイト送信し、ACK=1500を受ける前に同じSeq=1000の500バイトを再送している。最も考えやすい説明はどれか。
ア．ACKが再送タイマー内に届かなかった、または損失と判断され再送された
イ．ACK=1500はSeq=1000のデータを拒否したことを示す
ウ．TCPでは同じシーケンス番号の再送は仕様上不可能である
エ．DNSキャッシュが切れたため再送した
正答：ア
4肢解説
ア：正しい。同一シーケンス範囲の再送はTCPが当該データ未確認・損失と判断したことを示す。
イ：ACK=1500は通常1499まで受信済みを意味する。
ウ：損失時に同一データを再送する。
エ：TCP再送の直接原因ではない。
総合解説：フォレンジックでは再送、重複ACK、RTT、ウィンドウを解析し、損失・遅延・攻撃の可能性を評価する。

問140 pcapでは端末Aが03:12に未知IPへTLS接続、EDRでは03:11に不審プロセス生成、DNSログでは03:10に新規ドメイン解決がある。最も適切な分析はどれか。
ア．データ源が異なるので関連付けてはならない
イ．時刻を正規化し、DNS解決→プロセス実行→外部接続の一連のタイムラインとして相関する
ウ．TLS接続なので調査不能として全記録を破棄する
エ．最も新しいイベントだけ見て過去ログを無視する
正答：イ
4肢解説
ア：相関分析こそフォレンジックの重要手法である。
イ：正しい。異なるデータ源を時系列で結ぶことで、侵害の因果関係を推定できる。
ウ：メタデータや端末ログは利用できる。
エ：侵入起点を見失う。
総合解説：ネットワークフォレンジックはパケット単体ではなくDNS、EDR、認証、OSログ等との相関で精度が高まる。

問141 インシデント対応の主な目的として最も適切なものはどれか。
ア．全てのインシデントを公表せず記録もしない
イ．攻撃者の手法だけを研究し業務復旧は考えない
ウ．被害を限定し、原因と影響を把握し、安全に復旧して再発防止へつなげる
エ．ログを削除して調査時間を短縮する
正答：ウ
4肢解説
ア：組織的改善や法令対応ができない。
イ：サービス回復も重要な目的である。
ウ：正しい。対応は単なる障害復旧ではなく、検知・封じ込め・復旧・改善を組み合わせる。
エ：原因・影響把握を困難にする。
総合解説：NIST SP 800-61 Rev.3はインシデント対応をCSF 2.0のリスク管理全体へ統合している。

問142 侵害が確認された端末をネットワーク隔離する行為の主な目的はどれか。
ア．原因を永久に不明にするため
イ．端末を高速化するため
ウ．DNSキャッシュを増やすため
エ．攻撃者の活動やマルウェアの横展開を止め、被害拡大を抑える
正答：エ
4肢解説
ア：調査と並行して行う。
イ：性能向上が目的ではない。
ウ：インシデント封じ込めとは無関係である。
エ：正しい。封じ込めは侵害の継続・拡散を制限するための対応である。
総合解説：封じ込めは証拠保全や業務影響とのバランスを考え、ネットワーク隔離、アカウント無効化等を選択する。

問143 侵害端末を再び本番ネットワークへ戻す前に最も重要な確認はどれか。
ア．侵害原因が除去され、必要な修正・認証情報更新・監視強化を行い、安全な状態を確認する
イ．電源が入れば即座に復旧完了とする
ウ．ログを消せば安全と判断する
エ．利用者が急いでいる場合は検証を省略する
正答：ア
4肢解説
ア：正しい。単に再起動しただけでは持続化機構や漏えい資格情報が残る可能性がある。
イ：セキュリティ状態を確認していない。
ウ：証拠喪失となり安全性も保証しない。
エ：再侵害の危険が高い。
総合解説：復旧では根絶確認、パッチ、資格情報変更、監視、段階的なサービス復帰を行う。

問144 同じマルウェア検知でも、研究用隔離端末1台と、顧客個人情報DB管理サーバでは対応優先度が異なる。最も適切な判断基準はどれか。
ア．アラート名だけで全インシデントを同じ重大度にする
イ．資産重要度、影響範囲、データ機密性、攻撃継続性などを基に重大度を決める
ウ．端末の購入価格だけで決める
エ．曜日だけで重大度を決める
正答：イ
4肢解説
ア：業務影響を反映できない。
イ：正しい。イベント種別だけでなく業務・情報資産への影響で優先順位を付ける。
ウ：データ・サービス価値を無視している。
エ：リスクとの関連がない。
総合解説：重大度基準は事前に定義し、エスカレーション・連絡・対応SLAと結び付ける。

問145 個人情報流出の可能性がある重大インシデントで、技術担当だけが対応し法務・広報・経営へ連絡していない。問題として最も適切なものはどれか。
ア．技術問題なので他部門は関与してはならない
イ．詳細が完全確定するまで数週間誰にも連絡しない
ウ．法令・契約・対外説明・経営判断が必要になるため、事前定義した関係者へ速やかにエスカレーションすべきである
エ．SNSへ未確認情報を担当者個人が即時投稿する
正答：ウ
4肢解説
ア：通知義務や事業判断を見落とす。
イ：初動判断や法定期限に間に合わない可能性がある。
ウ：正しい。インシデント対応は技術部門だけで完結せず、法務・広報・経営・業務部門等との連携が必要である。
エ：統制されたコミュニケーションが必要である。
総合解説：連絡先、承認権限、外部機関・顧客への通知条件を平時に決めておく。

問146 侵害調査でC2のIPアドレスをブロックしたが、初期侵入に使われたVPN脆弱性は未修正のままである。評価として最も適切なものはどれか。
ア．C2 IPを1件ブロックすれば根本原因も必ず消える
イ．脆弱性修正はインシデント対応に含まれない
ウ．IOCは一切利用価値がない
エ．IOC遮断だけでは根本原因が残るため、侵入経路となった脆弱性も修正する必要がある
正答：エ
4肢解説
ア：脆弱性は残っている。
イ：再発防止に重要である。
ウ：検知・封じ込めには有用だが根本対策と併用する。
エ：正しい。攻撃インフラは変更され得るため、侵入原因を除去しなければ再侵害される可能性がある。
総合解説：対応ではIOCによる即時封じ込めと、脆弱性・設定・資格情報等のroot cause修正を区別する。

問147 フィッシング対応で毎回『誰がメール削除を依頼するか』『アカウント停止権限は誰か』の確認に1時間以上かかる。改善として最も適切なものはどれか。
ア．役割、判断条件、連絡先、実施手順をプレイブックへ明記し、定期演習する
イ．毎回ゼロから担当者を決める
ウ．プレイブックを作成後一度も見直さない
エ．権限を全員に付与して承認を不要にする
正答：ア
4肢解説
ア：正しい。定型インシデントは事前手順化すると意思決定・対応を迅速化できる。
イ：同じ遅延を繰り返す。
ウ：組織・脅威・ツール変更に追随できない。
エ：過剰権限となる。
総合解説：プレイブックは机上演習・実インシデントの教訓を反映して継続更新する。

問148 重大インシデント後、原因が『退職者アカウントが90日間残存し悪用された』と判明した。最も適切な再発防止はどれか。
ア．該当アカウントだけ削除して運用基準は変えない
イ．アカウント廃止期限・責任者・自動連携・監査方法を含むID管理基準を見直す
ウ．全ログを削除して問題をなかったことにする
エ．退職者全員の氏名をFWへ登録する
正答：イ
4肢解説
ア：同種事象が再発し得る。
イ：正しい。個別アカウント削除だけでなく、同じ欠陥を繰り返さない統制へ改善する必要がある。
ウ：改善につながらない。
エ：適切なIDライフサイクル管理ではない。
総合解説：インシデント後レビューでは技術設定だけでなく、方針・手順・責任分担・監視基準を改善する。

問149 ランサムウェアで認証基盤、社内Wiki、基幹受注、検証環境が停止した。業務影響分析で『認証基盤が他サービスの前提、受注停止は1時間以上不可』とされている。復旧計画として最も適切なものはどれか。
ア．最も簡単に復旧できる社内Wikiだけを最優先する
イ．全システムを同じ優先度として同時開始し資源競合を無視する
ウ．依存関係と業務優先度から認証基盤と基幹受注を優先し、検証環境等は後順位とする
エ．依存サービスを確認せず基幹受注だけ起動する
正答：ウ
4肢解説
ア：受注と認証の業務重要性を無視している。
イ：限られた復旧資源を非効率に使う。
ウ：正しい。復旧は技術的に復元しやすい順ではなく、業務影響とサービス依存関係を基に決める。
エ：認証基盤が前提なら正常稼働できない。
総合解説：RecoverではRTO、業務重要度、技術依存関係、データ整合性を組み合わせて復旧順序を決める。

問150 過去10件の重大インシデントで、侵入から検知まで平均14日、検知から封じ込めまでは平均30分だった。改善投資の優先先として最も合理的なものはどれか。
ア．封じ込め時間だけを30分から29分にする施策を最優先する
イ．ログ保持期間を短縮して検知データを減らす
ウ．インシデント指標は改善活動に使わない
エ．検知までの時間を短縮するログ・EDR/NDR・SIEMルールや監視体制の改善を優先する
正答：エ
4肢解説
ア：14日の検知遅延の方が改善余地が大きい。
イ：調査・検知能力を低下させる。
ウ：MTTD/MTTR等はボトルネック把握に有用である。
エ：正しい。封じ込めは比較的速い一方、攻撃者が長期間活動できる検知遅延がボトルネックである。
総合解説：インシデント後レビューでは測定可能な指標から検知・対応・復旧の弱点を特定し、基準と投資を見直す。