Q001 2-1 暗号・PKI / 共通鍵・公開鍵暗号

大量データを高速に暗号化する用途で、共通鍵暗号が公開鍵暗号より一般に適している主な理由はどれか。
ア．同程度の利用条件では、共通鍵暗号の方が暗号化・復号の計算負荷を小さくしやすい。
イ．共通鍵暗号では暗号鍵を公開してよいから。
ウ．公開鍵暗号では復号ができないから。
エ．共通鍵暗号は必ず完全前方秘匿性を提供するから。

正答・4肢解説・総合解説

正答：ア．同程度の利用条件では、共通鍵暗号の方が暗号化・復号の計算負荷を小さくしやすい。
ア：共通鍵暗号は大量データの暗号化に向く高速性を持ち、公開鍵暗号は鍵配送や署名などで組み合わせて使われることが多い。
イ：共通鍵は秘密に共有する必要があり、公開してよい鍵ではない。
ウ：公開鍵暗号にも対応する秘密鍵による復号方式がある。
エ：前方秘匿性は鍵交換方式などプロトコル設計に依存し、共通鍵暗号だけで自動的に得られない。
総合解説：実運用では公開鍵技術でセッション鍵を安全に確立し、その後の大量通信を共通鍵暗号で保護するハイブリッド方式が一般的である。

Q002 2-1 暗号・PKI / 共通鍵・公開鍵暗号

AESについて正しい説明はどれか。
ア．AESは公開鍵暗号であり、暗号化鍵と復号鍵は必ず異なる。
イ．AESは128ビットのブロックを処理し、128・192・256ビットの鍵長を使用できる共通鍵ブロック暗号である。
ウ．AESのブロック長は鍵長と常に同じである。
エ．AES-256では256ビット単位でしか平文を処理できない。

正答・4肢解説・総合解説

正答：イ．AESは128ビットのブロックを処理し、128・192・256ビットの鍵長を使用できる共通鍵ブロック暗号である。
ア：AESは共通鍵暗号であり、公開鍵暗号ではない。
イ：FIPS 197はAES-128、AES-192、AES-256を規定し、いずれも128ビットブロックを処理する。
ウ：AESのブロック長は128ビットで固定され、鍵長は128・192・256ビットから選ばれる。
エ：AES-256の256は鍵長を示し、ブロック長は128ビットである。
総合解説：AESの名称末尾の数値は鍵長であり、ブロック長ではない点は頻出の区別である。

Q003 2-1 暗号・PKI / 共通鍵・公開鍵暗号

同じ共通鍵でAEAD方式を利用するシステムにおいて、nonceの再利用を避けるべき主な理由はどれか。
ア．nonceは秘密鍵そのものなので、必ず利用者に暗記させる必要があるため。
イ．nonceを再利用するとAESの鍵長が自動的に短くなるため。
ウ．方式によっては同一鍵でのnonce再利用が機密性や完全性を大きく損なうため。
エ．nonceは証明書の失効確認に使う値だから。

正答・4肢解説・総合解説

正答：ウ．方式によっては同一鍵でのnonce再利用が機密性や完全性を大きく損なうため。
ア：nonceは一般に秘密である必要はないが、方式が要求する一意性等を満たす必要がある。
イ：鍵長そのものが変化するわけではない。
ウ：AEADの安全性はnonceの一意性など方式固有の条件に依存する。nonceを単なる付加情報と考えて再利用してはいけない。
エ：暗号モードのnonceと証明書失効確認は別の概念である。
総合解説：暗号方式はアルゴリズム名だけでなく、鍵・nonce/IV・認証タグ等の運用条件まで含めて安全性を評価する。

Q004 2-1 暗号・PKI / 共通鍵・公開鍵暗号

大容量ファイルを受信者だけが読めるよう送信したい。受信者の公開鍵は入手済みである。一般的なハイブリッド暗号の構成として最も適切なものはどれか。
ア．ファイル全体をハッシュ化し、ハッシュ値だけを受信者へ送る。
イ．受信者の公開鍵を共通鍵としてそのままAESに入力する。
ウ．送信者の公開鍵だけでファイルを暗号化し、受信者がその公開鍵で復号する。
エ．ランダムな共通鍵でファイルを暗号化し、その共通鍵を受信者の公開鍵を使う方式で保護する。

正答・4肢解説・総合解説

正答：エ．ランダムな共通鍵でファイルを暗号化し、その共通鍵を受信者の公開鍵を使う方式で保護する。
ア：ハッシュ値から元のファイルを復元できず、ファイル配送にならない。
イ：公開鍵とAES鍵は役割・形式が異なり、そのまま共通鍵として扱う設計ではない。
ウ：公開鍵だけで復号できるなら誰でも復号でき、受信者限定の機密性を実現しない。
エ：大量データは高速な共通鍵暗号で処理し、短いセッション鍵を公開鍵暗号等で安全に配送するのが典型的な構成である。
総合解説：公開鍵暗号と共通鍵暗号は競合する方式ではなく、長所を組み合わせて利用する。

Q005 2-1 暗号・PKI / 共通鍵・公開鍵暗号

受信者Bだけが平文を得られるよう、公開鍵暗号で機密性を確保してAからBへデータを送る基本的な考え方はどれか。
ア．Bの公開鍵で暗号化し、Bの秘密鍵で復号する。
イ．Aの公開鍵で暗号化し、Aの公開鍵で復号する。
ウ．Bの秘密鍵で暗号化し、Bの秘密鍵で復号する。
エ．AとBが同じ公開鍵だけを秘密に共有する。

正答・4肢解説・総合解説

正答：ア．Bの公開鍵で暗号化し、Bの秘密鍵で復号する。
ア：公開鍵は配布可能であり、対応する秘密鍵をBが適切に保護することで受信者限定の復号を実現する。
イ：公開鍵だけで機密性のある復号を実現する考え方ではない。
ウ：Bの秘密鍵を送信者Aへ渡す運用は秘密鍵保護に反する。
エ：公開鍵は秘密共有する鍵ではなく、共通鍵暗号の説明とも異なる。
総合解説：公開鍵暗号では「誰の公開鍵を使うか」と「誰が秘密鍵を保持するか」を明確にする。

Q006 2-1 暗号・PKI / 共通鍵・公開鍵暗号

Diffie-Hellman型の鍵共有を利用する主な目的はどれか。
ア．相手のパスワードを平文で取得する。
イ．盗聴され得る通信路上で、両者が共有秘密を導出するための材料を交換する。
ウ．公開鍵証明書を失効させる。
エ．データベースのレコードを正規化する。

正答・4肢解説・総合解説

正答：イ．盗聴され得る通信路上で、両者が共有秘密を導出するための材料を交換する。
ア：鍵共有は相手のパスワード取得を目的としない。
イ：Diffie-Hellman型の方式は、秘密値そのものを通信路へ直接送らずに共有秘密を導出するために用いられる。
ウ：証明書失効はCA・OCSP・CRL等のPKI運用に関する処理である。
エ：データベース設計とは無関係である。
総合解説：鍵共有だけでは相手認証が十分でない場合があるため、実際のプロトコルでは署名や証明書等と組み合わせて中間者攻撃を防ぐ。

Q007 2-1 暗号・PKI / 共通鍵・公開鍵暗号

TLS等の通信で前方秘匿性（forward secrecy）を重視する理由として最も適切なものはどれか。
ア．一度確立したセッション鍵を永久に再利用できるようにするため。
イ．通信相手の証明書を不要にするため。
ウ．将来サーバの長期秘密鍵が漏えいしても、過去に記録されたセッション通信の復号を困難にするため。
エ．暗号文のサイズを必ず平文より小さくするため。

正答・4肢解説・総合解説

正答：ウ．将来サーバの長期秘密鍵が漏えいしても、過去に記録されたセッション通信の復号を困難にするため。
ア：長期再利用はむしろ被害範囲を広げる可能性がある。
イ：前方秘匿性と相手認証は別の要件である。
ウ：一時的な鍵共有を適切に用いる設計では、長期秘密鍵の後日漏えいが過去セッション鍵の復元に直結しにくい。
エ：前方秘匿性はデータ圧縮の性質ではない。
総合解説：暗号設計では「現在の通信を守る」だけでなく、将来の鍵漏えい時に過去データへどこまで影響するかも考える。

Q008 2-1 暗号・PKI / 共通鍵・公開鍵暗号

公開鍵技術を用いる「暗号化」と「電子署名」の鍵利用の説明として適切なものはどれか。
ア．どちらも送信者の公開鍵だけで完結する。
イ．どちらも受信者の秘密鍵を送信者へ事前配布する。
ウ．電子署名では暗号文を受信者の秘密鍵で復号して署名者を確認する。
エ．機密性目的の暗号化では受信者側の秘密鍵が復号に使われ、署名では署名者側の秘密鍵が署名生成に使われる。

正答・4肢解説・総合解説

正答：エ．機密性目的の暗号化では受信者側の秘密鍵が復号に使われ、署名では署名者側の秘密鍵が署名生成に使われる。
ア：秘密鍵を使わずに署名者固有性や受信者限定の復号を実現できない。
イ：秘密鍵は所有者が保護すべきで、他者への配布を前提にしない。
ウ：署名検証は通常、署名者に対応する公開鍵を用いる。
エ：同じ公開鍵技術でも、機密性と署名では「誰の秘密鍵を使うか」が異なる。
総合解説：「秘密鍵を持つ主体」を整理すると、公開鍵暗号の用途を混同しにくい。

Q009 2-1 暗号・PKI / 共通鍵・公開鍵暗号

強力な暗号アルゴリズムを採用していても、鍵管理が不適切だと安全性が失われる例として最も適切なものはどれか。
ア．秘密鍵を平文の設定ファイルへ保存し、多数の管理者が恒常的に閲覧できる。
イ．公開鍵を利用者へ配布する。
ウ．暗号化済みデータにもバックアップを設ける。
エ．鍵の利用目的を台帳で管理する。

正答・4肢解説・総合解説

正答：ア．秘密鍵を平文の設定ファイルへ保存し、多数の管理者が恒常的に閲覧できる。
ア：暗号強度は鍵の秘密性に依存するため、保管・アクセス制御・ローテーション・失効等の運用が重要である。
イ：公開鍵は適切な真正性を確保した上で配布することを前提とする。
ウ：可用性のためのバックアップは、鍵保護と両立させるべき対策である。
エ：鍵用途の把握は適切な鍵管理に資する。
総合解説：「安全なアルゴリズム＝安全なシステム」ではない。鍵生成・保管・配布・更新・廃棄までを管理する必要がある。

Q010 2-1 暗号・PKI / 共通鍵・公開鍵暗号

鍵ラッピング（key wrapping）の用途として最も適切なものはどれか。
ア．ハッシュ値から元のパスワードを復元する。
イ．別の暗号鍵を安全に保管・配送するため、鍵暗号化鍵などで鍵材料を保護する。
ウ．証明書の有効期限を自動延長する。
エ．ファイアウォールのルール順序を最適化する。

正答・4肢解説・総合解説

正答：イ．別の暗号鍵を安全に保管・配送するため、鍵暗号化鍵などで鍵材料を保護する。
ア：鍵ラッピングはハッシュの逆算機能ではない。
イ：データ暗号鍵をそのまま平文で保存せず、上位の鍵で包んで保護する設計は鍵階層化で広く用いられる。
ウ：証明書更新はPKI運用であり、鍵ラッピングとは別である。
エ：ネットワークポリシー管理とは無関係である。
総合解説：鍵そのものも高価値資産である。データ暗号鍵と鍵暗号化鍵を分離することで、鍵保護とローテーションを設計しやすくなる。

Q011 2-1 暗号・PKI / 共通鍵・公開鍵暗号

長期運用するシステムの暗号設計で「暗号アジリティ」を確保する方針として最も適切なものはどれか。
ア．暗号方式を一度決めたら廃止まで変更できないようソースコードへ固定する。
イ．互換性を優先して古い暗号方式を無期限に有効化する。
ウ．アルゴリズムや鍵長を将来変更できるよう識別子・設定・移行手順を設計し、特定方式へ固定し過ぎない。
エ．全データで同じ鍵を期限なく利用する。

正答・4肢解説・総合解説

正答：ウ．アルゴリズムや鍵長を将来変更できるよう識別子・設定・移行手順を設計し、特定方式へ固定し過ぎない。
ア：将来の移行を困難にし、脆弱な方式から切り替えられなくなる。
イ：弱い方式を残すことはダウングレード等のリスクを生む。
ウ：暗号技術は脆弱性発見や標準変更で更新が必要になるため、安全に切り替えられる設計が重要である。
エ：鍵更新を妨げ、漏えい時の影響範囲も拡大する。
総合解説：暗号アジリティは「何でも許可する」ことではなく、許可方式を管理しながら安全に移行できる能力である。

Q012 2-1 暗号・PKI / 共通鍵・公開鍵暗号

同一システムで「データ暗号化」と「メッセージ認証」の両方を行う。鍵管理上の方針として一般に望ましいものはどれか。
ア．同じ鍵を暗号化・MAC・署名の全用途へ無条件に使い回す。
イ．鍵を区別するため、鍵本体をログへ平文記録する。
ウ．用途ごとに鍵名だけ変更し、実体は同一の秘密値を使う。
エ．用途ごとに独立した鍵を用いるか、マスター秘密から用途別の鍵を安全なKDFで導出する。

正答・4肢解説・総合解説

正答：エ．用途ごとに独立した鍵を用いるか、マスター秘密から用途別の鍵を安全なKDFで導出する。
ア：異なる暗号用途での鍵共有は相互作用や侵害時の影響範囲を広げ得る。
イ：秘密鍵・共通鍵のログ出力は漏えいにつながる。
ウ：名前だけ分けても暗号学的な鍵分離にはならない。
エ：鍵を用途別に分離すると、一つの用途の設計上の問題や鍵露出が他用途へ波及する範囲を抑えやすい。
総合解説：鍵分離は暗号アーキテクチャの基本原則であり、KDFを用いる場合も用途識別情報を適切に設計する。

Q013 2-1 暗号・PKI / ハッシュ・MAC・電子署名

暗号学的ハッシュ関数に期待される性質として最も適切なものはどれか。
ア．入力が少し変化すると出力も大きく変化し、与えられたハッシュ値から元入力を求めることや同じ値になる別入力を見つけることが困難である。
イ．同じ入力でも実行するたび必ず異なるハッシュ値になる。
ウ．ハッシュ値を秘密鍵で復号すれば必ず元の入力に戻せる。
エ．入力が長くなるほどハッシュ値の長さも必ず比例して増える。

正答・4肢解説・総合解説

正答：ア．入力が少し変化すると出力も大きく変化し、与えられたハッシュ値から元入力を求めることや同じ値になる別入力を見つけることが困難である。
ア：ハッシュは固定長ダイジェストを生成し、原像計算困難性や衝突耐性などが安全性の重要な要素となる。
イ：通常のハッシュ関数は同じ入力に対して同じ出力を返す決定的関数である。
ウ：ハッシュは可逆暗号ではない。
エ：一般的な暗号学的ハッシュは入力長にかかわらず規定の長さの出力を生成する。
総合解説：ハッシュは暗号化とは異なり復号を前提としない。完全性検証、署名前処理、MAC、パスワード保護等の構成要素として使われる。

Q014 2-1 暗号・PKI / ハッシュ・MAC・電子署名

ハッシュ関数の「衝突耐性」の説明として最も適切なものはどれか。
ア．与えられたハッシュ値から元の入力を求めることが困難である性質。
イ．同じハッシュ値を生成する異なる二つの入力を見つけることが計算量的に困難である性質。
ウ．同じ入力から二つの異なるハッシュ値が得られない性質。
エ．秘密鍵を知らずにハッシュ値を計算できない性質。

正答・4肢解説・総合解説

正答：イ．同じハッシュ値を生成する異なる二つの入力を見つけることが計算量的に困難である性質。
ア：これは主に原像計算困難性の説明である。
イ：衝突は攻撃者が二つの異なる入力を選び、それらのハッシュ値を一致させる問題である。
ウ：決定性の説明に近く、衝突耐性の定義ではない。
エ：通常のハッシュ関数は秘密鍵なしで計算できる。秘密鍵を用いる認証コードとは異なる。
総合解説：「原像」「第二原像」「衝突」は対象となる探索問題が異なるため、用語を区別する。

Q015 2-1 暗号・PKI / ハッシュ・MAC・電子署名

HMACの説明として最も適切なものはどれか。
ア．公開鍵だけを使って第三者が署名者を検証する電子署名方式である。
イ．平文を可逆的に暗号化して機密性を提供する方式である。
ウ．共有秘密鍵と暗号学的ハッシュ関数を組み合わせ、メッセージの完全性と送信元認証に利用するMAC方式である。
エ．パスワードを必ず復号可能な形で保存する方式である。

正答・4肢解説・総合解説

正答：ウ．共有秘密鍵と暗号学的ハッシュ関数を組み合わせ、メッセージの完全性と送信元認証に利用するMAC方式である。
ア：HMACは共有秘密鍵方式であり、公開鍵署名ではない。
イ：HMAC自体は機密性を提供しない。
ウ：HMACは秘密鍵を知る当事者だけが正しい認証コードを生成できることを利用する。
エ：HMACはパスワードの可逆保存方式ではない。
総合解説：MACは改ざん検知と共有鍵保有者からの生成確認に使えるが、共有鍵を双方が持つため電子署名と同じ第三者検証性はない。

Q016 2-1 暗号・PKI / ハッシュ・MAC・電子署名

共有鍵MACと公開鍵電子署名の違いとして適切なものはどれか。
ア．MACは機密性を必ず提供するが、電子署名は提供しない。
イ．電子署名は公開鍵を秘密に保持しなければならない。
ウ．MACにはハッシュ関数を一切利用できない。
エ．MACは検証者も共有秘密鍵を持つため、第三者に対して誰が生成したかを示す証拠性は電子署名より弱い。

正答・4肢解説・総合解説

正答：エ．MACは検証者も共有秘密鍵を持つため、第三者に対して誰が生成したかを示す証拠性は電子署名より弱い。
ア：MACは完全性・認証用途であり、機密性を自動的に提供しない。
イ：公開鍵は検証者へ配布でき、秘密に保持すべきなのは署名用秘密鍵である。
ウ：HMACはハッシュ関数を利用する代表的なMACである。
エ：MACでは共有鍵を知る複数主体が同じ認証コードを生成可能であり、署名者だけが秘密鍵を持つ電子署名とは性質が異なる。
総合解説：電子署名の特性を理解する際は、秘密鍵の独占性と公開鍵による検証可能性に注目する。

Q017 2-1 暗号・PKI / ハッシュ・MAC・電子署名

文書Mに対する電子署名を受け取った検証者が、署名対象文書の改ざんを確認する基本的な処理として最も適切なものはどれか。
ア．文書Mから求めたダイジェストと、署名者の公開鍵を用いて署名を検証した結果が対応することを確認する。
イ．署名者の秘密鍵を受け取り、検証者が同じ署名を再生成する。
ウ．文書Mを受信者の公開鍵で暗号化できれば署名検証成功とする。
エ．署名値の文字数だけを確認する。

正答・4肢解説・総合解説

正答：ア．文書Mから求めたダイジェストと、署名者の公開鍵を用いて署名を検証した結果が対応することを確認する。
ア：電子署名は署名対象データと署名者の秘密鍵の関係を、対応する公開鍵で検証する。
イ：署名者の秘密鍵を検証者へ渡してはならない。
ウ：機密性の暗号化と署名検証は別の処理である。
エ：形式だけでは文書との結び付きや署名の正当性を確認できない。
総合解説：実装では署名アルゴリズム、公開鍵証明書の検証、署名対象データの正規化等も含めて正しく処理する必要がある。

Q018 2-1 暗号・PKI / ハッシュ・MAC・電子署名

利用者パスワードの保存時に、利用者ごとにランダムなsaltを付けてパスワードハッシュを計算する主な効果はどれか。
ア．saltを付ければ短いパスワードでも推測攻撃が不可能になる。
イ．同じパスワードでも利用者ごとの保存値を異ならせ、事前計算表の使い回しを困難にする。
ウ．saltはパスワードを可逆暗号化するための復号鍵である。
エ．全利用者で同じ固定saltを使うほど安全性が高まる。

正答・4肢解説・総合解説

正答：イ．同じパスワードでも利用者ごとの保存値を異ならせ、事前計算表の使い回しを困難にする。
ア：saltは推測可能なパスワード自体の低エントロピーを解消しない。
イ：saltは秘密である必要は通常ないが、利用者ごとに一意・ランダムな値を用いることで同一パスワードの同一ハッシュ化を避ける。
ウ：saltは復号鍵ではなく、ハッシュ計算への追加入力である。
エ：固定共通saltでは利用者ごとの差異がなく、事前計算の再利用抑止効果が低下する。
総合解説：パスワード保存ではsaltに加え、Argon2等の意図的に計算・メモリコストを持つパスワードハッシュ/KDFを利用する。

Q019 2-1 暗号・PKI / ハッシュ・MAC・電子署名

Argon2をパスワード保存に利用する目的として最も適切なものはどれか。
ア．パスワードをネットワーク上で平文送信できるようにする。
イ．パスワードから公開鍵証明書を自動発行する。
ウ．メモリ使用量や計算コストを調整できるメモリハードな処理により、オフライン総当たり攻撃のコストを高める。
エ．ハッシュ値を短くして記憶しやすくする。

正答・4肢解説・総合解説

正答：ウ．メモリ使用量や計算コストを調整できるメモリハードな処理により、オフライン総当たり攻撃のコストを高める。
ア：パスワードハッシュは平文送信を正当化しない。通信路保護も必要である。
イ：Argon2は証明書発行機能ではない。
ウ：Argon2はパスワードハッシュ向けに設計されたメモリハード関数で、単純な高速ハッシュだけを使うより攻撃コストを高めやすい。
エ：目的は可読性ではなく、推測攻撃に対する計算コストを高めることである。
総合解説：パスワードハッシュは「高速なほど良い」処理ではない。利用者のログインでは許容可能だが攻撃者の大量試行には重いパラメータを選ぶ。

Q020 2-1 暗号・PKI / ハッシュ・MAC・電子署名

HKDFの主な用途はどれか。
ア．公開鍵証明書の失効状態をオンライン照会する。
イ．ネットワーク侵入をシグネチャで検知する。
ウ．電子メール送信ドメインをDNSで宣言する。
エ．初期鍵材料から、暗号用途に適した一つ以上の秘密鍵を導出する。

正答・4肢解説・総合解説

正答：エ．初期鍵材料から、暗号用途に適した一つ以上の秘密鍵を導出する。
ア：これはOCSPの役割である。
イ：これはIDS/IPSの機能である。
ウ：これはSPF等のメール認証に関係する。
エ：HKDFはHMACを基礎とするKDFで、ExtractとExpandの段階を通じて鍵材料を用途別の鍵へ導出できる。
総合解説：鍵共有で得た値をそのまま複数用途へ使うのではなく、KDFで文脈・用途を分離した鍵へ導出する設計が重要である。

Q021 2-1 暗号・PKI / ハッシュ・MAC・電子署名

組織のコード署名用秘密鍵が漏えいした疑いが強い。最も優先すべき対応はどれか。
ア．該当鍵の利用を停止し、関連証明書の失効等を実施した上で新しい鍵へ移行し、漏えい期間中の署名も調査する。
イ．公開鍵を秘密に変更して漏えいを隠す。
ウ．同じ秘密鍵を使い続け、署名時刻だけ変更する。
エ．署名対象ファイルを圧縮すれば漏えいの影響がなくなる。

正答・4肢解説・総合解説

正答：ア．該当鍵の利用を停止し、関連証明書の失効等を実施した上で新しい鍵へ移行し、漏えい期間中の署名も調査する。
ア：署名用秘密鍵の漏えいは攻撃者が正規署名に見える署名を生成できる重大事象であり、鍵の無効化と影響調査が必要である。
イ：公開鍵の公開性を変えても漏えいした秘密鍵の悪用を止められない。
ウ：漏えい鍵を継続利用すると偽造署名リスクが続く。
エ：圧縮は署名鍵侵害への対策ではない。
総合解説：秘密鍵侵害時は技術的な鍵更新だけでなく、信頼関係、配布物、監査ログ、署名済み成果物の再評価まで必要になる。

Q022 2-1 暗号・PKI / ハッシュ・MAC・電子署名

メッセージMとSHA-256(M)を同じ通信路で送るだけでは、能動的な改ざん者に対する完全性保護が不十分な主な理由はどれか。
ア．SHA-256は入力を暗号化する方式だから。
イ．攻撃者がMを改ざんした後、その改ざん後メッセージのハッシュ値も計算し直して置き換えられるため。
ウ．ハッシュ値は必ずネットワークで欠落するから。
エ．SHA-256は固定長出力を作れないから。

正答・4肢解説・総合解説

正答：イ．攻撃者がMを改ざんした後、その改ざん後メッセージのハッシュ値も計算し直して置き換えられるため。
ア：SHA-256はハッシュ関数であり、可逆暗号ではない。
イ：秘密情報を使わない単純ハッシュは誰でも計算できるため、攻撃者によるメッセージとダイジェストの同時置換を防げない。
ウ：通信で必ず欠落するという性質はない。
エ：SHA-256は256ビットの固定長出力を生成する。
総合解説：敵対的通信路で完全性と送信元認証を得るには、HMACや電子署名など秘密鍵に基づく仕組みを利用する。

Q023 2-1 暗号・PKI / PKI・電子証明書

PKIにおける認証局（CA）の基本的な役割として最も適切なものはどれか。
ア．利用者の秘密鍵を常に全て保管して代理利用する。
イ．全ての通信を暗号化して中継する。
ウ．主体と公開鍵などを結び付けた電子証明書へ署名し、その結び付きに対する信頼を提供する。
エ．ファイアウォールルールを自動生成する。

正答・4肢解説・総合解説

正答：ウ．主体と公開鍵などを結び付けた電子証明書へ署名し、その結び付きに対する信頼を提供する。
ア：秘密鍵は原則として鍵所有者側で保護すべきであり、CAの基本役割は全利用者秘密鍵の保管ではない。
イ：CAは一般の通信中継装置ではない。
ウ：CAは証明書に署名し、検証者が信頼するCAから対象証明書までの信頼連鎖を検証できるようにする。
エ：ネットワーク制御ルール生成はCAの役割ではない。
総合解説：PKIではCAの秘密鍵保護が特に重要であり、CA侵害は広範囲の証明書信頼へ影響する。

Q024 2-1 暗号・PKI / PKI・電子証明書

ブラウザがサーバ証明書を検証する際の一般的な考え方として最も適切なものはどれか。
ア．サーバ証明書のファイルサイズが一定以上なら信頼する。
イ．サーバが自己申告した「安全」フラグだけを確認する。
ウ．中間CAやルートCAは一切確認せず、公開鍵が含まれていれば受理する。
エ．サーバ証明書から中間CAをたどり、信頼済みルートCAまでの署名連鎖や有効期間・用途等を検証する。

正答・4肢解説・総合解説

正答：エ．サーバ証明書から中間CAをたどり、信頼済みルートCAまでの署名連鎖や有効期間・用途等を検証する。
ア：ファイルサイズは信頼性の根拠にならない。
イ：サーバ自身の申告だけでは第三者による信頼検証にならない。
ウ：信頼できる発行者までの検証を省くと偽証明書を受理する危険がある。
エ：証明書パス検証では署名連鎖だけでなく、有効期間、名前、用途制約、失効状態など複数条件を確認する。
総合解説：証明書は「公開鍵が入っているから安全」なのではなく、信頼アンカーまでの検証ルールを正しく実行して初めて利用できる。

Q025 2-1 暗号・PKI / PKI・電子証明書

ルートCAの秘密鍵を日常的なサーバ証明書発行から隔離し、中間CAに発行業務を担わせる主な利点はどれか。
ア．最上位の信頼アンカーであるルートCA秘密鍵の露出機会を減らし、侵害リスクを抑えられる。
イ．中間CAを使うと証明書の署名検証が不要になる。
ウ．中間CAの証明書は有効期限を持たない。
エ．ルートCAの公開鍵を秘密にできる。

正答・4肢解説・総合解説

正答：ア．最上位の信頼アンカーであるルートCA秘密鍵の露出機会を減らし、侵害リスクを抑えられる。
ア：ルート鍵は影響範囲が非常に大きいため、オフライン化等で保護し、中間CAへ業務を委任する階層構成が用いられる。
イ：検証者は中間CAを含む証明書チェーンを検証する必要がある。
ウ：中間CA証明書にも有効期間等の条件がある。
エ：信頼アンカーの公開鍵情報は検証に利用され、秘密にするものではない。
総合解説：PKIの階層化は運用上の分離と被害限定に役立つが、中間CA侵害も重大であり適切な失効・監査が必要である。

Q026 2-1 暗号・PKI / PKI・電子証明書

HTTPSで `https://portal.example.jp` に接続したところ、提示された証明書の有効期間と署名連鎖は正しいが、証明書が `mail.example.jp` 用であった。適切な処理はどれか。
ア．同じexample.jp配下なので無条件に受理する。
イ．接続先ホスト名と証明書の識別名が一致しないため、証明書検証エラーとして扱う。
ウ．証明書の公開鍵長が十分なら名前不一致を無視する。
エ．DNSのTTLが短ければ名前不一致を無視する。

正答・4肢解説・総合解説

正答：イ．接続先ホスト名と証明書の識別名が一致しないため、証明書検証エラーとして扱う。
ア：別ホスト名の証明書を無条件に受理すると中間者攻撃等を許す。
イ：証明書検証では発行者や有効期限だけでなく、利用しているサービス名との一致確認が必要である。
ウ：鍵強度とホスト名の真正性確認は別の検証項目である。
エ：TTLはDNSキャッシュ時間の要素であり証明書名一致を代替しない。
総合解説：TLSサーバ認証では「信頼されたCAが署名したか」と「目的のホスト名用か」を両方確認する。

Q027 2-1 暗号・PKI / PKI・電子証明書

CRLとOCSPの説明として最も適切なものはどれか。
ア．CRLは秘密鍵のバックアップ形式で、OCSPは公開鍵暗号方式である。
イ．CRLはWeb攻撃を遮断し、OCSPはマルウェアを隔離する。
ウ．CRLは失効証明書の一覧を配布する方式で、OCSPは特定証明書の状態をオンラインで問い合わせる方式である。
エ．OCSPは証明書の有効期限を自動延長する。

正答・4肢解説・総合解説

正答：ウ．CRLは失効証明書の一覧を配布する方式で、OCSPは特定証明書の状態をオンラインで問い合わせる方式である。
ア：どちらも鍵バックアップや暗号アルゴリズムではなく、証明書状態確認に関する仕組みである。
イ：WAFやEDR等の機能と混同している。
ウ：いずれも証明書の有効期限前の失効状態確認に利用されるが、提供形態が異なる。
エ：OCSPは状態を応答するプロトコルであり、有効期限延長は行わない。
総合解説：失効確認はPKI運用の重要要素であり、可用性、鮮度、プライバシー等も考慮して方式を選ぶ。

Q028 2-1 暗号・PKI / PKI・電子証明書

公開WebサーバのTLS秘密鍵が外部へ流出したことが確認された。証明書の有効期限はまだ1年残っている。最も適切な対応はどれか。
ア．有効期限まで同じ鍵を使い続ける。
イ．公開鍵だけ変更し、証明書と秘密鍵はそのままにする。
ウ．サーバ時刻を1年前に戻して証明書を無効化する。
エ．該当証明書を失効させ、新しい鍵ペアで証明書を再発行し、漏えいした鍵を利用停止する。

正答・4肢解説・総合解説

正答：エ．該当証明書を失効させ、新しい鍵ペアで証明書を再発行し、漏えいした鍵を利用停止する。
ア：攻撃者が秘密鍵を利用できる状態が継続する。
イ：証明書には公開鍵が結び付いており、整合しない変更はできない。
ウ：時刻変更は正しい失効処理ではなく、他の検証やログにも悪影響を与える。
エ：有効期限内でも秘密鍵が侵害された証明書を信頼し続けてはならず、失効と鍵交換が必要である。
総合解説：鍵侵害対応では証明書失効、新規鍵生成、再発行、配備、侵害範囲調査を一連の手順として扱う。

Q029 2-1 暗号・PKI / PKI・電子証明書

X.509証明書のKey UsageやExtended Key Usageを検証する理由として最も適切なものはどれか。
ア．証明書・公開鍵を、発行時に想定された用途から逸脱して利用することを防ぐため。
イ．証明書の秘密鍵を公開するため。
ウ．証明書ファイルを圧縮するため。
エ．DNSレコードを暗号化するため。

正答・4肢解説・総合解説

正答：ア．証明書・公開鍵を、発行時に想定された用途から逸脱して利用することを防ぐため。
ア：証明書パス検証では署名が正しいだけでなく、対象用途に許可された証明書かを確認する。
イ：用途制約は秘密鍵公開のための仕組みではない。
ウ：用途制約と圧縮は無関係である。
エ：DNSSEC等とは別の証明書制約機能である。
総合解説：PKIでは名前・期間・発行者・失効・用途制約を総合的に検証する必要がある。

Q030 2-1 暗号・PKI / PKI・電子証明書

社内システムで自己署名証明書を使う場合、その証明書を各端末へ単に配布するだけでなく「信頼アンカーとして適切に登録・管理する」必要がある主な理由はどれか。
ア．自己署名証明書は必ず暗号化機能を持たないため。
イ．自己署名であるという事実だけでは信頼性は証明されず、別経路で真正性を確認して信頼する対象を明示する必要があるため。
ウ．自己署名証明書には公開鍵が含まれないため。
エ．自己署名証明書は有効期限を設定できないため。

正答・4肢解説・総合解説

正答：イ．自己署名であるという事実だけでは信頼性は証明されず、別経路で真正性を確認して信頼する対象を明示する必要があるため。
ア：自己署名でも公開鍵はTLS等の暗号プロトコルで利用できる。問題は信頼の確立方法である。
イ：証明書検証の起点となる信頼アンカーは、攻撃者が自由に差し替えられない方法で配布・管理しなければならない。
ウ：通常のX.509自己署名証明書にも公開鍵情報が含まれる。
エ：自己署名証明書にも有効期間を設定できる。
総合解説：PKIの核心は公開鍵の真正性をどう信頼するかであり、自己署名かCA署名かだけではなく信頼アンカーの配布経路が重要である。

Q031 2-2 認証・アクセス制御 / 多要素認証・認証方式

「知識」「所持」「生体」の三つの認証要素の組合せとして、多要素認証に該当するものはどれか。
ア．パスワードと秘密の質問を併用する。
イ．指紋と顔認証を併用する。
ウ．パスワードと、端末に格納された秘密鍵を用いる認証器を併用する。
エ．パスワードを2回入力する。

正答・4肢解説・総合解説

正答：ウ．パスワードと、端末に格納された秘密鍵を用いる認証器を併用する。
ア：どちらも知識要素であり、二段階でも同一要素カテゴリである。
イ：どちらも生体要素であり、異なる要素カテゴリの組合せではない。
ウ：知識要素と所持要素という異なるカテゴリを組み合わせているため多要素認証となる。
エ：同じ知識要素を繰り返すだけで多要素にはならない。
総合解説：多要素認証は認証回数ではなく、異なる種類の要素を組み合わせることが本質である。

Q032 2-2 認証・アクセス制御 / 多要素認証・認証方式

固定パスワードとワンタイムパスワード（OTP）を比較した場合、OTPの一般的な利点はどれか。
ア．OTPはフィッシングに対して常に完全に安全である。
イ．OTPを使えばサーバ側の認証処理は不要になる。
ウ．OTPは利用者識別を行わず、誰でも同じコードを利用する。
エ．一度取得された認証コードを後からそのまま再利用する攻撃の成功可能性を低減できる。

正答・4肢解説・総合解説

正答：エ．一度取得された認証コードを後からそのまま再利用する攻撃の成功可能性を低減できる。
ア：リアルタイム中継型フィッシングなどに弱いOTP方式もある。
イ：サーバはOTPの妥当性を検証する必要がある。
ウ：通常は利用者の認証器や共有秘密等に結び付いたコードである。
エ：OTPは時間やカウンタ等に基づいて値が変化し、固定秘密の再利用リスクを減らす。
総合解説：OTPは固定パスワードより再利用攻撃に強いが、フィッシング耐性は認証方式ごとに評価する必要がある。

Q033 2-2 認証・アクセス制御 / 多要素認証・認証方式

偽サイトへの認証情報入力によるアカウント乗っ取りを特に減らしたい。認証方式として最も適切な方向性はどれか。
ア．オリジンに結び付いた公開鍵認証を用いるWebAuthn/FIDO系のフィッシング耐性認証を導入する。
イ．SMSで受け取ったコードだけを唯一の認証要素にする。
ウ．パスワードの最小長を4文字にする。
エ．全利用者に同じ追加PINを配布する。

正答・4肢解説・総合解説

正答：ア．オリジンに結び付いた公開鍵認証を用いるWebAuthn/FIDO系のフィッシング耐性認証を導入する。
ア：WebAuthn/FIDO系では認証器が正規オリジンとの関係を検証して署名するため、共有秘密を偽サイトへ入力する方式よりフィッシング耐性を高められる。
イ：SMS OTPにはSIMスワップやリアルタイムフィッシング等のリスクがある。
ウ：短いパスワードは推測耐性を低下させる。
エ：共有PINは利用者固有の強い追加要素にならない。
総合解説：MFAであっても全て同じ強度ではない。脅威がフィッシングなら、フィッシング耐性を持つ認証器を優先する。

Q034 2-2 認証・アクセス制御 / 多要素認証・認証方式

生体認証のFAR（False Acceptance Rate）を表すものはどれか。
ア．本人を誤って拒否する割合。
イ．本人ではない者を誤って本人として受け入れる割合。
ウ．認証器が故障する割合。
エ．パスワード再利用率。

正答・4肢解説・総合解説

正答：イ．本人ではない者を誤って本人として受け入れる割合。
ア：これはFRR（False Rejection Rate）の説明である。
イ：FARは他人受入率であり、不正者を受け入れるセキュリティ上の誤りを表す。
ウ：機器故障率とは別の指標である。
エ：生体認証の誤判定率ではない。
総合解説：閾値調整ではFARとFRRがトレードオフになる場合があるため、用途に応じて安全性と利便性を評価する。

Q035 2-2 認証・アクセス制御 / 多要素認証・認証方式

認証（authentication）と認可（authorization）の関係として最も適切なものはどれか。
ア．認証と認可は同じ処理の別名である。
イ．認可が成功した後にだけ利用者を識別するのが認証である。
ウ．認証は主体が誰であるかを確認し、認可は認証された主体にどの資源・操作を許可するかを決める。
エ．認証はデータ暗号化、認可はデータ圧縮を意味する。

正答・4肢解説・総合解説

正答：ウ．認証は主体が誰であるかを確認し、認可は認証された主体にどの資源・操作を許可するかを決める。
ア：目的が異なるため区別する必要がある。
イ：通常は主体識別・認証情報を基に権限判定する。
ウ：本人確認と権限判定は異なる機能であり、強い認証をしても過大な権限を与えれば安全にはならない。
エ：どちらもアクセス制御に関する概念であり、暗号化・圧縮の定義ではない。
総合解説：認証突破だけでなく、認可不備による他人データアクセスなども重大な脆弱性となる。

Q036 2-2 認証・アクセス制御 / 多要素認証・認証方式

インターネット公開ログイン画面でオンラインパスワード総当たり攻撃が観測された。対策の組合せとして最も適切なものはどれか。
ア．ログイン失敗ログを全て削除して攻撃者に見つからないようにする。
イ．パスワードを全利用者で共通化する。
ウ．レート制限をなくして認証処理を高速化する。
エ．MFAを導入し、レート制限や異常試行検知を行い、既知漏えいパスワードの利用を避ける。

正答・4肢解説・総合解説

正答：エ．MFAを導入し、レート制限や異常試行検知を行い、既知漏えいパスワードの利用を避ける。
ア：監視に必要な証跡を失い、攻撃検知能力を低下させる。
イ：一つの漏えいで全利用者が侵害される。
ウ：攻撃者の大量試行を容易にする。
エ：単一対策ではなく、認証器強化と試行回数制御・監視を組み合わせることでオンライン推測攻撃の成功率を下げる。
総合解説：認証防御では、資格情報そのものの強度、MFA、試行抑制、監視、侵害済み資格情報への対応を組み合わせる。

Q037 2-2 認証・アクセス制御 / 多要素認証・認証方式

チャレンジレスポンス認証の考え方として最も適切なものはどれか。
ア．サーバが毎回異なるチャレンジを提示し、利用者側が秘密情報に基づく応答を生成して、秘密そのものを送らずに所持を示す。
イ．秘密鍵を毎回平文でサーバへ送信する。
ウ．認証成功後にサーバが利用者のパスワードを公開する。
エ．常に同じチャレンジを用いて応答を固定化する。

正答・4肢解説・総合解説

正答：ア．サーバが毎回異なるチャレンジを提示し、利用者側が秘密情報に基づく応答を生成して、秘密そのものを送らずに所持を示す。
ア：使い捨てのチャレンジを含めることで、過去の応答を盗聴してそのまま再利用する攻撃を防ぎやすくする。
イ：秘密そのものを通信路へ送る設計ではない。
ウ：秘密情報を公開してはならない。
エ：同じ応答の再利用を可能にし、リプレイ耐性を損なう。
総合解説：nonceやチャレンジは「新鮮さ」を提供し、認証応答が過去通信のコピーではないことを確認するために重要である。

Q038 2-2 認証・アクセス制御 / 多要素認証・認証方式

強いMFAを導入した組織で、認証器を紛失した利用者向けのアカウント回復手続を設計する。最も重要な考え方はどれか。
ア．メールアドレスを知っていれば無条件でMFAを解除する。
イ．通常ログインと同等以上に本人確認を行い、回復手続そのものが弱い迂回路にならないようにする。
ウ．紛失申告があれば全利用者共通の一時パスワードを渡す。
エ．回復操作のログを残さない。

正答・4肢解説・総合解説

正答：イ．通常ログインと同等以上に本人確認を行い、回復手続そのものが弱い迂回路にならないようにする。
ア：メールアドレスは公開情報になり得て、本人確認として不十分である。
イ：強い認証を導入しても、回復チャネルが弱ければ攻撃者はそこを狙う。ライフサイクル全体で同等の保証を設計する。
ウ：共通秘密は漏えい時の影響が大きく、本人性も担保できない。
エ：高リスク操作である回復処理こそ監査証跡が重要である。
総合解説：認証器登録・交換・紛失・失効・回復は攻撃されやすい管理フェーズであり、本番ログインだけ強化しても不十分である。

Q039 2-2 認証・アクセス制御 / 多要素認証・認証方式

リスクベース認証の運用例として最も適切なものはどれか。
ア．全利用者に対して常に認証を省略する。
イ．ログイン地点だけで本人と断定し、認証器を使わない。
ウ．通常と異なる端末・地域・行動などのシグナルでリスクが高いと判断した場合に追加認証を要求する。
エ．高リスクと判定されたときほど認証要素を減らす。

正答・4肢解説・総合解説

正答：ウ．通常と異なる端末・地域・行動などのシグナルでリスクが高いと判断した場合に追加認証を要求する。
ア：リスクに応じた強化ではなく、認証保証を失う。
イ：位置情報だけに暗黙の信頼を置くのは危険である。
ウ：コンテキストに応じて認証強度を調整することで、通常時の利便性と高リスク時の安全性を両立しやすい。
エ：通常は逆に追加保証を求める。
総合解説：リスクシグナルは補助判断であり、誤判定やプライバシーにも配慮しながら認証ポリシーへ組み込む。

Q040 2-2 認証・アクセス制御 / 多要素認証・認証方式

利用者がログイン済みのWebサービスで、銀行口座変更のような高リスク操作だけ追加の本人確認を求めたい。適切な設計はどれか。
ア．ログイン済みなら全ての操作を無期限に無条件許可する。
イ．重要操作時だけTLSを無効にする。
ウ．重要操作のログを残さない。
エ．重要操作の直前に再認証やステップアップ認証を要求する。

正答・4肢解説・総合解説

正答：エ．重要操作の直前に再認証やステップアップ認証を要求する。
ア：盗まれたセッションが高リスク操作にそのまま使われる。
イ：通信保護を弱める不適切な設計である。
ウ：不正利用検知・追跡能力を下げる。
エ：既存セッションが長時間継続していても、重要操作時に新鮮な認証を求めることでセッション乗っ取り時の被害を抑えられる。
総合解説：認証は一度成功すれば永続的に十分とは限らない。操作リスク、経過時間、端末状態などに応じた再認証を設計する。

Q041 2-2 認証・アクセス制御 / 多要素認証・認証方式

利用者が多数のサービスで同じパスワードを使い回している。改善策としてパスワードマネージャを利用する主な利点はどれか。
ア．サービスごとに長くランダムな異なるパスワードを生成・保存しやすくし、使い回しを減らせる。
イ．全サービスのパスワードを同じ値へ自動統一する。
ウ．WebサイトのTLS証明書検証を不要にする。
エ．認証ログをサーバから削除する。

正答・4肢解説・総合解説

正答：ア．サービスごとに長くランダムな異なるパスワードを生成・保存しやすくし、使い回しを減らせる。
ア：パスワードマネージャは利用者が多数の高エントロピー資格情報を暗記する負担を減らし、サイトごとの一意なパスワード運用を支援する。
イ：使い回しのリスクをむしろ高める。
ウ：パスワード管理とTLSサーバ認証は別の防御層である。
エ：パスワードマネージャの目的ではない。
総合解説：パスワードマネージャ自体の保護も重要であり、強いマスターパスフレーズや端末保護、MFA等を併用する。

Q042 2-2 認証・アクセス制御 / 多要素認証・認証方式

パスワードと比べた生体認証情報の運用上の注意点として最も適切なものはどれか。
ア．生体情報は秘密でなくても無条件に安全である。
イ．漏えい時に同じ身体特徴を簡単には変更できないため、テンプレート保護やローカル照合など漏えい影響を抑える設計が重要である。
ウ．生体認証を使えば認証器の紛失対策は不要になる。
エ．生体認証は常にFARが0である。

正答・4肢解説・総合解説

正答：イ．漏えい時に同じ身体特徴を簡単には変更できないため、テンプレート保護やローカル照合など漏えい影響を抑える設計が重要である。
ア：漏えい・なりすまし・プライバシーのリスクがある。
イ：生体情報は再発行しにくい性質を持つため、保存形式・照合場所・代替認証・失効設計を慎重に行う必要がある。
ウ：端末やセンサー等の認証器管理は依然必要である。
エ：誤受入れ・誤拒否は方式と閾値に応じて発生し得る。
総合解説：生体認証は利便性が高い一方、「変更しにくい資格情報」である点を踏まえた設計が不可欠である。

Q043 2-2 認証・アクセス制御 / 多要素認証・認証方式

Webサービスの認証成功後にセッションIDを再発行する主なセキュリティ上の理由はどれか。
ア．セッションIDを短くして利用者が暗記しやすくするため。
イ．認証後はCookieを平文HTTPだけで送るため。
ウ．攻撃者が事前に利用者へ固定させたセッションIDを、認証後もそのまま利用できるセッション固定攻撃を防ぎやすくするため。
エ．パスワードハッシュをセッションIDとして再利用するため。

正答・4肢解説・総合解説

正答：ウ．攻撃者が事前に利用者へ固定させたセッションIDを、認証後もそのまま利用できるセッション固定攻撃を防ぎやすくするため。
ア：セッションIDは推測困難であるべきで、暗記しやすさは目的ではない。
イ：認証後もSecure属性等を用いてHTTPSで保護すべきである。
ウ：認証状態が変化する境界でセッション識別子を更新し、認証前セッションと認証後セッションの関連を切り替える。
エ：パスワード派生値をセッション識別子に流用すべきではない。
総合解説：認証方式だけでなく、認証後のセッション管理もアカウント保護に直結する。

Q044 2-2 認証・アクセス制御 / 多要素認証・認証方式

スマートフォン1台にパスワード自動入力とSMS受信を全て集約したMFAについて、リスク評価上の注意点はどれか。
ア．同一端末に集約すると必ず三要素認証になる。
イ．SMSを使う限り端末侵害の影響は絶対に受けない。
ウ．端末に画面ロックがあれば他の認証設計は一切不要である。
エ．複数要素を形式上使っていても、同じ端末の単一侵害で両方が奪われる可能性があり、要素間の独立性を評価する必要がある。

正答・4肢解説・総合解説

正答：エ．複数要素を形式上使っていても、同じ端末の単一侵害で両方が奪われる可能性があり、要素間の独立性を評価する必要がある。
ア：端末数と認証要素カテゴリは一致しない。
イ：端末や通信アカウントの侵害によりコードが盗まれる可能性がある。
ウ：画面ロックは重要だがサービス側の認証設計を置き換えない。
エ：MFAは異なる要素の組合せだが、実装・端末・回復経路が同じ単一障害点になると期待する強度が下がり得る。
総合解説：認証強度は「要素数」だけでなく、フィッシング耐性、端末侵害、回復手続、要素間依存性まで含めて評価する。

Q045 2-2 認証・アクセス制御 / SSO・フェデレーション

SSO（Single Sign-On）の主な目的として最も適切なものはどれか。
ア．一度の認証結果を基に、複数の対象サービスへ繰り返し資格情報を入力せずアクセスできるようにする。
イ．全サービスで同じパスワード文字列を手作業で設定すること。
ウ．全サービスの認可ルールを無効化すること。
エ．一度ログインすると永久に再認証しないこと。

正答・4肢解説・総合解説

正答：ア．一度の認証結果を基に、複数の対象サービスへ繰り返し資格情報を入力せずアクセスできるようにする。
ア：SSOは利用者の認証負担を減らしつつ、認証を中央管理しやすくする。
イ：単なるパスワード使い回しはSSOではなく、漏えい時のリスクを高める。
ウ：SSO後も各サービスで必要な認可が行われる。
エ：SSOでもセッション期限や高リスク操作時の再認証が必要になり得る。
総合解説：SSOは利便性を高める一方、IdPや認証基盤が高価値な集中ポイントとなるため強固な保護が必要である。

Q046 2-2 認証・アクセス制御 / SSO・フェデレーション

アイデンティティフェデレーションで、利用者を認証し、その結果を別組織のサービスへアサーションとして提供する主体は一般に何と呼ばれるか。
ア．WAF。
イ．IdP（Identity Provider）。
ウ．DNSリゾルバ。
エ．SIEM。

正答・4肢解説・総合解説

正答：イ．IdP（Identity Provider）。
ア：WAFはWeb通信を検査するセキュリティ装置・機能であり、認証アサーション発行主体ではない。
イ：IdPは利用者認証や属性を扱い、RP/SP側がそのアサーションを信頼してサービス提供に利用する。
ウ：DNSリゾルバは名前解決を行う。
エ：SIEMはログ収集・相関分析等を行う監視基盤である。
総合解説：フェデレーションではIdPとRelying Party/Service Providerの信頼関係、鍵、メタデータ、アサーション条件が重要である。

Q047 2-2 認証・アクセス制御 / SSO・フェデレーション

OAuth 2.0の基本的な位置付けとして最も適切なものはどれか。
ア．公開鍵証明書を発行するPKIプロトコルである。
イ．ファイルを暗号化する共通鍵暗号方式である。
ウ．利用者の資格情報を第三者アプリへ渡さず、限定されたリソースアクセス権を委任するための認可フレームワークである。
エ．DNS応答に電子署名を付ける仕組みである。

正答・4肢解説・総合解説

正答：ウ．利用者の資格情報を第三者アプリへ渡さず、限定されたリソースアクセス権を委任するための認可フレームワークである。
ア：OAuthは証明書発行プロトコルではない。
イ：OAuthは暗号アルゴリズムではない。
ウ：OAuth 2.0は認可を目的とする。利用者ログインのアイデンティティ層として使う場合はOpenID Connect等の仕様を組み合わせる。
エ：これはDNSSECに関係する。
総合解説：「OAuthでログイン」という表現だけでOAuth自体を認証仕様と誤認しないことが重要である。

Q048 2-2 認証・アクセス制御 / SSO・フェデレーション

OAuth 2.0の認可コードフローで、認可サーバがredirect URIを安全に扱うための方針として適切なものはどれか。
ア．利用者が指定した任意URLへ常にリダイレクトする。
イ．redirect URIのホスト名を一切検証しない。
ウ．redirect URIの検証をクライアント側JavaScriptだけに任せる。
エ．事前登録したredirect URIと原則として正確に照合し、攻撃者サイトへの任意リダイレクトを許さない。

正答・4肢解説・総合解説

正答：エ．事前登録したredirect URIと原則として正確に照合し、攻撃者サイトへの任意リダイレクトを許さない。
ア：オープンリダイレクトとなり、資格情報漏えいに悪用される。
イ：攻撃者管理ドメインへ認可結果が送られる可能性がある。
ウ：認可サーバ側で信頼境界として検証する必要がある。
エ：不十分なredirect URI検証は認可コードやトークンの漏えいにつながるため、RFC 9700では厳格な照合が重要とされる。
総合解説：OAuthの安全性は暗号だけでなく、redirect URI、state、PKCE、トークン保護等のプロトコル実装に依存する。

Q049 2-2 認証・アクセス制御 / SSO・フェデレーション

OAuthのAuthorization CodeフローでPKCEを使う主な目的はどれか。
ア．認可コードが途中で盗まれても、最初にcode challengeを作成した正規クライアント以外がコードをトークンへ交換しにくくする。
イ．アクセストークンをDNSSECで署名するため。
ウ．利用者のパスワードをIdPからクライアントへ送るため。
エ．証明書失効をリアルタイム確認するため。

正答・4肢解説・総合解説

正答：ア．認可コードが途中で盗まれても、最初にcode challengeを作成した正規クライアント以外がコードをトークンへ交換しにくくする。
ア：PKCEではクライアントが保持するcode verifierと認可要求時のchallengeを対応させ、認可コード横取りへの耐性を高める。
イ：PKCEはDNSSECとは無関係である。
ウ：OAuthは第三者アプリへ利用者資格情報を渡さない設計を可能にする。
エ：これはOCSP等の機能である。
総合解説：公開クライアントを含む認可コードフローではPKCEが重要な防御であり、現行のOAuthセキュリティ設計で広く用いられる。

Q050 2-2 認証・アクセス制御 / SSO・フェデレーション

外部IdPから受け取った署名付きJWTをアプリケーションが受理する前に行う検証として最も重要なものはどれか。
ア．payloadをBase64URLデコードできれば信頼する。
イ．署名だけでなく、許可したアルゴリズム、issuer、audience、有効期限など用途に必要なclaimを検証する。
ウ．algヘッダに書かれた方式を無条件に受け入れる。
エ．JWT文字列が長ければ高い権限を与える。

正答・4肢解説・総合解説

正答：イ．署名だけでなく、許可したアルゴリズム、issuer、audience、有効期限など用途に必要なclaimを検証する。
ア：Base64URLはエンコードであり真正性を保証しない。
イ：JWTは署名が正しいだけで全ての用途に有効とは限らない。発行者・対象受信者・時刻・アルゴリズムを文脈に応じて検証する。
ウ：攻撃者が指定した不適切なアルゴリズムを許すと検証バイパスにつながり得る。
エ：トークン長は権限の正当性を示さない。
総合解説：JWT処理ではライブラリ任せにせず、許可アルゴリズムとclaim検証条件をアプリ側ポリシーとして固定する。

Q051 2-2 認証・アクセス制御 / SSO・フェデレーション

OAuth/OIDCフローでstate値を用いる代表的な目的として最も適切なものはどれか。
ア．TLS証明書の有効期限を延長する。
イ．ユーザのパスワードを暗号化してIdPへ送る。
ウ．認可要求とコールバックを対応付け、CSRF等で別の認可応答を利用者セッションへ混入されることを防ぐ。
エ．DNSキャッシュのTTLを制御する。

正答・4肢解説・総合解説

正答：ウ．認可要求とコールバックを対応付け、CSRF等で別の認可応答を利用者セッションへ混入されることを防ぐ。
ア：stateは証明書管理とは無関係である。
イ：stateはパスワード暗号化用の鍵ではない。
ウ：stateはクライアントが要求時に生成し、返却値との一致を確認してフローの対応関係を検証する。
エ：DNS TTLとは関係しない。
総合解説：OIDCではnonce等も用いられ、トークンのリプレイや要求との結び付き確認に使われる。用途を混同しないことが重要である。

Q052 2-2 認証・アクセス制御 / SSO・フェデレーション

多数の業務SaaSを単一IdPへフェデレーションしている組織で、IdP障害時に全サービスへ新規ログインできなくなった。設計上の教訓として最も適切なものはどれか。
ア．SSOではIdP障害がサービス利用へ影響することはない。
イ．全サービスへ同じ固定パスワードを配布すれば解決する。
ウ．IdPの監査ログを無効化すれば可用性が上がる。
エ．IdPは集中した認証依存点になるため、高可用化・復旧手順・緊急アクセス等をリスクに応じて設計する。

正答・4肢解説・総合解説

正答：エ．IdPは集中した認証依存点になるため、高可用化・復旧手順・緊急アクセス等をリスクに応じて設計する。
ア：多くのサービスがIdPに依存すれば新規認証等が影響を受ける。
イ：資格情報使い回しによる侵害リスクを高める。
ウ：監査ログ削除は検知・追跡能力を下げ、可用性対策とはならない。
エ：SSO/フェデレーションは管理性を高めるが、認証基盤の障害や侵害の影響範囲も大きくなる。
総合解説：集中認証は「便利だから安全」ではなく、セキュリティと可用性の双方で重要インフラとして設計する必要がある。

Q053 2-2 認証・アクセス制御 / SSO・フェデレーション

IdPが発行した認証アサーションをサービスA向けに発行したにもかかわらず、サービスBも同じアサーションを受理できてしまう。最も問題となる検証不足はどれか。
ア．アサーションのaudience（対象受信者）をサービスBが検証していない。
イ．アサーションの文字コードがUTF-8であること。
ウ．IdPの画面色がサービスごとに異なること。
エ．サービスBのDNS TTLが短いこと。

正答・4肢解説・総合解説

正答：ア．アサーションのaudience（対象受信者）をサービスBが検証していない。
ア：対象受信者の検証を省くと、別サービス向けトークン・アサーションの横流しを受理する危険がある。
イ：文字コードは重要だが、別サービス向けトークン受理の直接原因ではない。
ウ：UI配色はaudience制御とは無関係である。
エ：DNSキャッシュ時間はアサーション宛先検証の代替にならない。
総合解説：トークン検証では署名・発行者・対象・時刻・nonce等を用途に応じて確認し、別コンテキストへの再利用を防ぐ。

Q054 2-2 認証・アクセス制御 / SSO・フェデレーション

複数サービスのSSO環境で「ログアウト」を設計する際の注意点として最も適切なものはどれか。
ア．一つのアプリCookieを削除すれば全IdP・全サービスのセッションが必ず終了する。
イ．アプリ側セッションとIdP側セッションが別に存在し得るため、どこまで終了させるかを明確にしないと再ログインや残存セッションが意図と異なる可能性がある。
ウ．ログアウト時は利用者の公開鍵をインターネットから削除する。
エ．ログアウト機能はセキュリティに影響しない。

正答・4肢解説・総合解説

正答：イ．アプリ側セッションとIdP側セッションが別に存在し得るため、どこまで終了させるかを明確にしないと再ログインや残存セッションが意図と異なる可能性がある。
ア：構成によってIdPや他サービスのセッションは残る。
イ：SSOでは複数のセッション層があるため、ローカルログアウトとフェデレーション全体のログアウトを区別して設計する。
ウ：公開鍵の存在とセッション終了は別問題である。
エ：共有端末やセッション盗用等への対策として重要である。
総合解説：SSOはログインだけでなく、セッション期限、ログアウト、アカウント無効化の伝播まで含めて設計する。

Q055 2-2 認証・アクセス制御 / IAM・特権アクセス管理

IAMにおけるプロビジョニングの説明として最も適切なものはどれか。
ア．全アカウントに管理者権限を付与する。
イ．秘密鍵を全社員へ共有する。
ウ．入社・異動・退職などに応じて、アカウントや権限を作成・変更・削除するライフサイクル管理を行う。
エ．DNSレコードだけを更新する。

正答・4肢解説・総合解説

正答：ウ．入社・異動・退職などに応じて、アカウントや権限を作成・変更・削除するライフサイクル管理を行う。
ア：最小権限に反し、IAMの適切な運用ではない。
イ：共有秘密鍵は責任追跡や鍵保護を損なう。
ウ：IAMは認証だけでなく、アイデンティティと権限を組織イベントに同期して維持することが重要である。
エ：DNS管理はIAMプロビジョニングの定義ではない。
総合解説：退職者や異動者の権限が残る「孤児アカウント」「過剰権限」を防ぐため、HR等の正本情報と連携したライフサイクル管理が重要である。

Q056 2-2 認証・アクセス制御 / IAM・特権アクセス管理

RBACとABACの違いとして最も適切なものはどれか。
ア．RBACは暗号方式、ABACはハッシュ方式である。
イ．RBACでは権限を一切管理しない。
ウ．ABACでは利用者属性を利用できない。
エ．RBACは役割に権限を割り当て、ABACは利用者・資源・環境などの属性に基づいてポリシー判断する。

正答・4肢解説・総合解説

正答：エ．RBACは役割に権限を割り当て、ABACは利用者・資源・環境などの属性に基づいてポリシー判断する。
ア：どちらもアクセス制御モデルである。
イ：RBACは役割を介して権限を管理する。
ウ：ABACは属性を判断材料にするモデルである。
エ：RBACは職務ロール中心、ABACは複数属性と条件を使った柔軟な認可に向く。
総合解説：組織構造が安定している場合はRBACが管理しやすく、動的条件が多い場合はABAC等を組み合わせる設計が有効である。

Q057 2-2 認証・アクセス制御 / IAM・特権アクセス管理

バックアップ担当者にはバックアップ実行と復元だけを許可し、利用者アカウント作成権限は与えない設計が示す原則はどれか。
ア．最小権限の原則。
イ．フェイルオープン。
ウ．公開鍵基盤。
エ．多重化。

正答・4肢解説・総合解説

正答：ア．最小権限の原則。
ア：業務遂行に必要な権限だけを与えることで、誤操作や資格情報侵害時の影響を抑える。
イ：障害時に許可側へ倒す考え方であり、権限付与範囲とは異なる。
ウ：証明書による信頼管理の仕組みである。
エ：可用性向上の冗長化に関する概念である。
総合解説：最小権限は人だけでなく、サービスアカウント、API、クラウドロール等にも適用する。

Q058 2-2 認証・アクセス制御 / IAM・特権アクセス管理

送金処理で「送金依頼を作成する担当者」と「最終承認する担当者」を分ける主なセキュリティ目的はどれか。
ア．通信速度を上げるため。
イ．一人の権限だけで不正取引を完結できないようにし、不正や誤操作のリスクを下げる。
ウ．パスワードハッシュを短くするため。
エ．証明書失効を不要にするため。

正答・4肢解説・総合解説

正答：イ．一人の権限だけで不正取引を完結できないようにし、不正や誤操作のリスクを下げる。
ア：職務分離の目的は性能向上ではない。
イ：職務分離（Separation of Duties）は相反する権限を分け、単独での不正成立を困難にする内部統制である。
ウ：暗号処理とは無関係である。
エ：PKI運用とは別の統制である。
総合解説：特権管理では最小権限に加えて、承認・二者統制・職務分離を組み合わせることが重要である。

Q059 2-2 認証・アクセス制御 / IAM・特権アクセス管理

Just-In-Time（JIT）型の特権アクセス管理の考え方として最も適切なものはどれか。
ア．管理者権限を全社員へ常時付与する。
イ．一度付与した特権は退職まで変更しない。
ウ．必要な作業の直前に承認された特権を期間限定で付与し、作業後は自動的に失効させる。
エ．特権アクセスをログに残さない。

正答・4肢解説・総合解説

正答：ウ．必要な作業の直前に承認された特権を期間限定で付与し、作業後は自動的に失効させる。
ア：JITと逆であり、攻撃面を拡大する。
イ：恒常的権限を減らす目的に反する。
ウ：恒常的な管理者権限を減らし、特権資格情報が悪用される時間窓と人数を縮小する。
エ：特権操作はむしろ詳細な監査証跡が重要である。
総合解説：PAMではJIT付与、承認、セッション記録、資格情報保管、コマンド制御などを組み合わせて特権を管理する。

Q060 2-2 認証・アクセス制御 / IAM・特権アクセス管理

PAM経由の管理者操作をセッション記録する主な目的として最も適切なものはどれか。
ア．管理者の秘密鍵を録画データへ埋め込む。
イ．監査を不要にする。
ウ．全管理操作を匿名化して実行者を分からなくする。
エ．誰がいつどの特権操作を行ったかを追跡し、不正検知・監査・事後調査を可能にする。

正答・4肢解説・総合解説

正答：エ．誰がいつどの特権操作を行ったかを追跡し、不正検知・監査・事後調査を可能にする。
ア：秘密鍵をログへ保存してはならない。
イ：記録は監査を支援するもので、監査そのものを不要にしない。
ウ：責任追跡性を失い、PAMの目的に反する。
エ：特権操作は影響が大きいため、通常利用者以上に強い説明責任と監査証跡が求められる。
総合解説：ただし記録データ自体にも機密情報が含まれ得るため、アクセス制御・保存期間・改ざん防止を設計する。

Q061 2-2 認証・アクセス制御 / IAM・特権アクセス管理

長期間変更されない共有パスワードを持つサービスアカウントが多数存在する。改善策として最も適切なものはどれか。
ア．用途・所有者を明確化し、必要最小権限にし、秘密を安全な保管庫等で管理して自動ローテーションや短期資格情報を検討する。
イ．全サービスアカウントを同じパスワードへ統一する。
ウ．パスワードをソースコードに直接埋め込む。
エ．誰が使うか分からないため全サービスアカウントへ管理者権限を与える。

正答・4肢解説・総合解説

正答：ア．用途・所有者を明確化し、必要最小権限にし、秘密を安全な保管庫等で管理して自動ローテーションや短期資格情報を検討する。
ア：非人間アカウントもIAMの対象であり、固定秘密・過大権限・所有者不明は重大なリスクとなる。
イ：一つの漏えいが全システムへ波及する。
ウ：リポジトリ漏えい等で資格情報が露出しやすい。
エ：最小権限と責任分界に反する。
総合解説：クラウドや自動化環境では、長期固定秘密よりワークロードアイデンティティや短期トークンを利用できる構成を優先する。

Q062 2-2 認証・アクセス制御 / IAM・特権アクセス管理

定期的なアクセスレビュー（権限棚卸し）を実施する主な目的はどれか。
ア．全利用者の権限を毎回管理者へ引き上げる。
イ．現在の職務に不要になった権限や、誤って付与された過剰権限を発見して是正する。
ウ．ログイン履歴を削除して保存容量を減らす。
エ．証明書の有効期限を永久にする。

正答・4肢解説・総合解説

正答：イ．現在の職務に不要になった権限や、誤って付与された過剰権限を発見して是正する。
ア：棚卸しは過剰権限の削減が目的である。
イ：異動・兼務・一時作業などで権限は徐々に蓄積するため、定期再認定が必要である。
ウ：監査証跡削除は権限レビューではない。
エ：PKIの有効期限設定とは無関係である。
総合解説：IAMは初回付与だけでなく、継続的な権限妥当性確認まで含む。特権・重要資産ほどレビュー頻度と承認品質を高める。

Q063 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

ネットワークファイアウォールの基本的な役割として最も適切なものはどれか。
ア．利用者の全ファイルを自動バックアップする。
イ．公開鍵証明書を発行する。
ウ．定めたポリシーに基づき、ネットワーク間またはホスト間を流れる通信を許可・拒否する。
エ．パスワードをハッシュ化してDBへ保存する。

正答・4肢解説・総合解説

正答：ウ．定めたポリシーに基づき、ネットワーク間またはホスト間を流れる通信を許可・拒否する。
ア：バックアップはファイアウォールの基本機能ではない。
イ：証明書発行はCAの役割である。
ウ：ファイアウォールは信頼度の異なるネットワークやホスト間の通信を制御し、攻撃面を縮小する。
エ：アプリケーションの認証情報管理であり、ファイアウォールの基本機能ではない。
総合解説：ファイアウォールは境界防御の一つであり、エンドポイント防御、認証、監視、セキュア開発等と併用する。

Q064 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

ステートフルインスペクション型ファイアウォールの特徴として最も適切なものはどれか。
ア．HTTP本文の業務内容を必ず理解して脆弱性を修正する。
イ．全通信を暗号化する。
ウ．証明書チェーンだけを検証する。
エ．接続状態や通信の文脈を追跡し、確立済みセッションに属するパケットかなどを判断材料にできる。

正答・4肢解説・総合解説

正答：エ．接続状態や通信の文脈を追跡し、確立済みセッションに属するパケットかなどを判断材料にできる。
ア：アプリケーション脆弱性の修正はWAFや開発対策とも異なる。
イ：ファイアウォールは通信制御装置であり、全通信の暗号化を自動保証しない。
ウ：PKI検証に限定された装置ではない。
エ：単一パケットのヘッダだけでなく、通信状態を保持してポリシー判定する点が特徴である。
総合解説：ステートフルFWでもアプリ層の攻撃を全て理解できるわけではなく、必要に応じてWAFやプロキシ等を組み合わせる。

Q065 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

サーバセグメントへのFWルールを設計する。必要な通信要件が明確な場合、原則として望ましい方針はどれか。
ア．必要な通信だけ明示的に許可し、それ以外はデフォルトで拒否する。
イ．全ポートを許可し、問題が起きた後に個別拒否する。
ウ．送信元アドレスにかかわらず管理ポートをインターネットへ公開する。
エ．FWログを無効にして処理を単純化する。

正答・4肢解説・総合解説

正答：ア．必要な通信だけ明示的に許可し、それ以外はデフォルトで拒否する。
ア：許可リスト型は不要なサービスへの到達性を減らし、攻撃面を限定する。
イ：不要な通信が広く通るため攻撃面が大きい。
ウ：管理面への不要な到達性はリスクが高い。
エ：監視・調査に必要な情報を失う。
総合解説：最小権限の考え方はネットワークにも適用できる。要件に基づく許可と不要通信の拒否が基本である。

Q066 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

既存Webアプリに脆弱性が発見されたが、修正版公開まで数日必要である。暫定的にWAFルールで攻撃パターンを遮断する場合の位置付けとして最も適切なものはどれか。
ア．WAFを入れればアプリケーション修正は永久に不要になる。
イ．WAFは暫定的・多層的な防御として有効だが、可能なら脆弱性そのものを修正する必要がある。
ウ．WAFはL2スイッチングだけを行いHTTPを扱わない。
エ．WAFは公開鍵証明書を発行する装置である。

正答・4肢解説・総合解説

正答：イ．WAFは暫定的・多層的な防御として有効だが、可能なら脆弱性そのものを修正する必要がある。
ア：WAF回避や設定漏れもあり、根本修正を代替するものではない。
イ：WAFはHTTP/HTTPS通信を検査して攻撃を検出・遮断できるが、アプリケーションの根本原因を必ず除去するものではない。
ウ：WAFはWebアプリケーション向け通信を対象とする。
エ：CAとは役割が異なる。
総合解説：WAFは「保険的対策」になり得るが、セキュア実装・脆弱性修正・監視と組み合わせる必要がある。

Q067 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

企業内端末の外部Webアクセスをフォワードプロキシ経由にする主な利点はどれか。
ア．社外利用者から社内Webサーバへのアクセスを負荷分散することだけが目的である。
イ．証明書の失効リストを発行する。
ウ．クライアントの外向き通信を中継し、URL制御・認証・ログ・コンテンツ検査などを集中実施しやすい。
エ．DNSSECの署名鍵を自動生成することだけが目的である。

正答・4肢解説・総合解説

正答：ウ．クライアントの外向き通信を中継し、URL制御・認証・ログ・コンテンツ検査などを集中実施しやすい。
ア：これはリバースプロキシやロードバランサの用途に近い。
イ：CRL発行はPKIの役割である。
ウ：フォワードプロキシは利用者側の代理として外部サーバへ接続し、出口制御のポイントを提供する。
エ：DNSSEC鍵管理とは別の機能である。
総合解説：プロキシを境界に配置すると通信可視化に役立つが、暗号化通信の検査には証明書配布・プライバシー・互換性等の設計が必要である。

Q068 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

リバースプロキシの一般的な位置付けとして最も適切なものはどれか。
ア．社内利用者の外向きWeb通信だけを代理する。
イ．利用者のパスワードをハッシュ化して認証DBへ保存する。
ウ．公開鍵証明書の失効状態を問い合わせる。
エ．外部クライアントからの要求をサーバ側の代理として受け、背後のWebサーバへ転送する。

正答・4肢解説・総合解説

正答：エ．外部クライアントからの要求をサーバ側の代理として受け、背後のWebサーバへ転送する。
ア：これはフォワードプロキシの代表的用途である。
イ：アプリケーション認証処理とは異なる。
ウ：OCSPの役割である。
エ：リバースプロキシはTLS終端、負荷分散、WAF連携、バックエンド隠蔽などに利用できる。
総合解説：フォワード/リバースは「誰の代理としてどちら向きの通信を扱うか」で整理すると区別しやすい。

Q069 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

NATを導入しているという理由だけで、ファイアウォール等のアクセス制御が不要とはいえない主な理由はどれか。
ア．NATの主目的はアドレス変換であり、許可・拒否ポリシーやアプリケーション攻撃対策を包括的に提供するものではないため。
イ．NATは暗号鍵を自動公開するから。
ウ．NATを使うとIPアドレスが必ず固定されるから。
エ．NATではTCPを利用できないから。

正答・4肢解説・総合解説

正答：ア．NATの主目的はアドレス変換であり、許可・拒否ポリシーやアプリケーション攻撃対策を包括的に提供するものではないため。
ア：アドレス変換による副次的な到達性変化はあっても、NATをセキュリティポリシーの代替と考えるべきではない。
イ：NATは鍵公開機能ではない。
ウ：NATと固定/動的アドレスは別概念である。
エ：NAT環境でもTCP通信は一般に利用される。
総合解説：ネットワーク機能の副次効果と、明示的なセキュリティ制御の目的を区別することが重要である。

Q070 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

FWルールが上から順に評価される。先頭に「送信元:any 宛先:Webサーバ TCP/443 許可」があり、その下に「送信元:攻撃元IP 宛先:Webサーバ TCP/443 拒否」がある。問題点はどれか。
ア．TCP/443は常にDNS通信なので拒否ルールは不要である。
イ．先頭の広い許可ルールに先に一致し、下位の拒否ルールが実質的に適用されない可能性がある。
ウ．拒否ルールは必ず許可ルールより先に評価されるので問題ない。
エ．送信元IPによる制御は暗号鍵長を変更する。

正答・4肢解説・総合解説

正答：イ．先頭の広い許可ルールに先に一致し、下位の拒否ルールが実質的に適用されない可能性がある。
ア：TCP/443は一般にHTTPS等に使われ、DNSとは限らない。
イ：ルール順序型FWでは広いルールが後続の具体的ルールを覆うシャドーイングに注意する。
ウ：評価順序は製品・設定に依存し、提示条件では上から評価される。
エ：FWルールと暗号鍵長は無関係である。
総合解説：FW監査では未使用ルール、重複、競合、広すぎる許可、ルール順序などを継続的に確認する。

Q071 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

社内端末がマルウェア感染した場合のC2通信や情報持ち出しを抑えるため、FWで実施する対策として有効なものはどれか。
ア．外向き通信は全て無条件許可し、入口だけ制御する。
イ．FWの時刻同期を無効化する。
ウ．外向き通信も必要な宛先・ポート・プロキシ経由などに制限し、ログを監視する。
エ．すべての内部端末へ公開サーバ用証明書の秘密鍵を配布する。

正答・4肢解説・総合解説

正答：ウ．外向き通信も必要な宛先・ポート・プロキシ経由などに制限し、ログを監視する。
ア：マルウェアのC2やデータ流出を許す可能性がある。
イ：ログ相関が難しくなり監視能力を下げる。
ウ：入口防御だけでなく出口制御を行うと、侵害後の外部通信を制限・検知しやすい。
エ：秘密鍵漏えいリスクを増やし、出口制御とは無関係である。
総合解説：侵入防止が完全でない前提で、侵害後の通信経路を制限する多層防御が重要である。

Q072 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

利用者端末ネットワークと重要DBネットワークの間にFWを置き、DBへはアプリサーバからの必要通信だけ許可した。主な効果はどれか。
ア．DBのSQLインジェクション脆弱性を自動修正する。
イ．利用者認証を完全に不要にする。
ウ．バックアップを不要にする。
エ．端末が侵害されてもDBへ直接到達できる経路を減らし、横展開や被害範囲を限定する。

正答・4肢解説・総合解説

正答：エ．端末が侵害されてもDBへ直接到達できる経路を減らし、横展開や被害範囲を限定する。
ア：ネットワーク分割だけでアプリケーション脆弱性は修正されない。
イ：ネットワーク分割と利用者認証は別の制御である。
ウ：障害・破壊への復旧策としてバックアップは依然必要である。
エ：ネットワーク分割と境界制御は、侵害が組織全体へ拡大するのを抑える防御層となる。
総合解説：セグメンテーションはゼロトラストや多層防御と整合するが、適切な認証・認可や監視も併用する。

Q073 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

企業プロキシでTLSインスペクションを導入する場合の説明として最も適切なものはどれか。
ア．暗号化通信中の脅威検査が可能になる一方、組織側が中間で復号するため、鍵・証明書管理、プライバシー、対象除外、障害影響を慎重に設計する必要がある。
イ．TLSインスペクションを使えば証明書検証は全て不要になる。
ウ．導入するとエンドツーエンド暗号化が必ず強化される。
エ．暗号化通信の内容を一切見ない方式なのでプライバシー影響はない。

正答・4肢解説・総合解説

正答：ア．暗号化通信中の脅威検査が可能になる一方、組織側が中間で復号するため、鍵・証明書管理、プライバシー、対象除外、障害影響を慎重に設計する必要がある。
ア：TLS検査は可視性を高めるが、強い信頼権限を持つ装置になるため新たなリスクも生む。
イ：プロキシ側・端末側双方で適切な証明書信頼管理が必要である。
ウ：途中で復号するため本来のエンドツーエンド性は変化する。
エ：内容を復号・検査する構成ではプライバシー影響を考慮する必要がある。
総合解説：セキュリティ装置を追加すれば自動的に安全になるわけではなく、その装置自身が高価値な信頼点・単一障害点となる。

Q074 2-3 ネットワークセキュリティ / FW・WAF・プロキシ

ファイアウォールで拒否ログを収集する主なセキュリティ価値として最も適切なものはどれか。
ア．ログを保存すると必ず通信内容が暗号化される。
イ．スキャンや不正接続試行、設定ミスなどの兆候を把握し、インシデント分析やルール改善に利用できる。
ウ．拒否ログがあればIDS/IPSや他ログは一切不要になる。
エ．拒否ログは全て削除した方が攻撃を防げる。

正答・4肢解説・総合解説

正答：イ．スキャンや不正接続試行、設定ミスなどの兆候を把握し、インシデント分析やルール改善に利用できる。
ア：ログ保存は通信暗号化機能ではない。
イ：拒否ログは単なるエラー記録ではなく、攻撃兆候や通信要件の不整合を可視化するデータである。
ウ：単一ログだけでは攻撃全体像を把握できない場合が多い。
エ：証跡を失い、検知・調査能力を低下させる。
総合解説：FWログは時刻同期、送信元/宛先、規則ID等を含め、SIEM等で他ログと相関できるようにする。

Q075 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

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は必ず暗号化を行い、IPSは必ず復号だけを行う。
イ．IDSは認証局、IPSは証明書失効サーバである。
ウ．IDSは主に不審な活動を検知・通知し、IPSは通信経路上で検知した通信を遮断するなど防止動作も行う。
エ．IDSとIPSはどちらもバックアップ専用装置である。

正答・4肢解説・総合解説

正答：ウ．IDSは主に不審な活動を検知・通知し、IPSは通信経路上で検知した通信を遮断するなど防止動作も行う。
ア：暗号化・復号の区別ではない。
イ：PKIの役割とは異なる。
ウ：IPSはインライン配置されることが多く、誤検知が実通信を止める影響も考慮して運用する必要がある。
エ：侵入検知・防止システムである。
総合解説：検知と遮断の違いだけでなく、配置方式、誤検知時の業務影響、チューニングを理解する。

Q076 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

シグネチャベース検知とアノマリベース検知の説明として適切なものはどれか。
ア．シグネチャ型は正常動作の統計モデルだけで判断する。
イ．アノマリ型は既知の攻撃文字列と完全一致した場合だけ通知する。
ウ．どちらも誤検知が絶対に発生しない。
エ．シグネチャ型は既知パターン照合に強く、アノマリ型は正常状態からの逸脱を検知することで未知の異常を捉えられる可能性がある。

正答・4肢解説・総合解説

正答：エ．シグネチャ型は既知パターン照合に強く、アノマリ型は正常状態からの逸脱を検知することで未知の異常を捉えられる可能性がある。
ア：これはアノマリ型に近い説明である。
イ：これはシグネチャ型に近い。
ウ：検知方式には誤検知・見逃しがあり、運用で調整が必要である。
エ：両方式には長所と短所があり、組み合わせて検知精度を高めることが多い。
総合解説：新しい攻撃にも対応するため、シグネチャ更新、ベースライン学習、脅威情報、相関分析を組み合わせる。

Q077 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

侵入検知で「偽陰性（false negative）」とはどの状態か。
ア．実際には攻撃が発生しているのに、システムが正常と判定して検知しない状態。
イ．正常通信を攻撃と誤判定する状態。
ウ．攻撃を正しく攻撃として検知する状態。
エ．正常通信を正しく正常と判定する状態。

正答・4肢解説・総合解説

正答：ア．実際には攻撃が発生しているのに、システムが正常と判定して検知しない状態。
ア：偽陰性は攻撃の見逃しであり、検知率を評価する上で重大な指標である。
イ：これは偽陽性（false positive）である。
ウ：これは真陽性である。
エ：これは真陰性である。
総合解説：閾値を厳しくすると偽陽性が増えるなどトレードオフがあるため、業務環境に合わせてチューニングする。

Q078 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

NIDSとHIDSの特徴の組合せとして最も適切なものはどれか。
ア．NIDSは証明書発行、HIDSはDNS署名を行う。
イ．NIDSはネットワーク上の通信を観測し、HIDSはホスト上のログ・ファイル・プロセスなどを観測する。
ウ．NIDSは主にCPU温度だけを監視し、HIDSはルーティングだけを監視する。
エ．NIDSとHIDSは同一製品名の違いで機能差はない。

正答・4肢解説・総合解説

正答：イ．NIDSはネットワーク上の通信を観測し、HIDSはホスト上のログ・ファイル・プロセスなどを観測する。
ア：どちらも侵入検知に関する仕組みである。
イ：ネットワークとホストでは見える証拠が異なるため、両方を組み合わせると検知範囲を補完できる。
ウ：代表的な観測対象ではない。
エ：観測位置・データ源が異なる。
総合解説：暗号化通信ではNIDSからアプリ内容が見えにくい場合があり、エンドポイント側テレメトリと補完することが重要である。

Q079 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

FW、認証基盤、EDR、クラウド監査ログを集約し、「短時間に多数の認証失敗後、海外IPから成功し、直後に大量ダウンロード」という一連の兆候を検知したい。適した仕組みはどれか。
ア．全ログを各端末で個別に削除する。
イ．ファイアウォールを全開放する。
ウ．SIEM等で複数ログを集約し、時系列・主体・IP等を相関分析する。
エ．認証失敗回数だけを年1回手作業集計する。

正答・4肢解説・総合解説

正答：ウ．SIEM等で複数ログを集約し、時系列・主体・IP等を相関分析する。
ア：相関に必要な証跡を失う。
イ：攻撃面を拡大する。
ウ：単一製品のログだけでは見えない攻撃連鎖を、異なるデータ源の相関で検知できる。
エ：即時性と複数ログ相関が不足する。
総合解説：SIEMではログ収集そのものより、正規化、相関ルール、優先度付け、保持、調査フローまで設計することが重要である。

Q080 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

インシデント時に複数装置のログ時刻が数分ずつずれており、攻撃順序を再構成できなかった。予防策として最も重要なものはどれか。
ア．ログごとに任意の時刻形式を使い、変換規則を記録しない。
イ．ログの時刻フィールドを全て削除する。
ウ．認証ログだけ未来時刻に設定する。
エ．信頼できる時刻源を用いてシステム時刻を同期し、タイムゾーンや時刻精度も統一的に管理する。

正答・4肢解説・総合解説

正答：エ．信頼できる時刻源を用いてシステム時刻を同期し、タイムゾーンや時刻精度も統一的に管理する。
ア：相関をさらに困難にする。
イ：イベント順序の復元ができなくなる。
ウ：意図的なずれは分析を妨げる。
エ：相関分析・フォレンジックではイベント順序が重要であり、時刻ずれは証跡価値を大きく下げる。
総合解説：NTP等の時刻同期サービス自体の認証・冗長化や、UTC基準での記録なども検討する。

Q081 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

セキュリティ監視で通常時の通信量・ログイン時間帯・プロセス挙動などのベースラインを把握する主な目的はどれか。
ア．平常状態から大きく外れた挙動を異常候補として識別しやすくする。
イ．全ての異常を自動的に攻撃と断定するため。
ウ．既知攻撃シグネチャを永久に更新しなくてよくするため。
エ．ログを保存せずに監視するため。

正答・4肢解説・総合解説

正答：ア．平常状態から大きく外れた挙動を異常候補として識別しやすくする。
ア：アノマリ検知では「何が異常か」を判断するために通常状態の理解が重要である。
イ：業務変更や障害も異常値になり得るため、追加分析が必要である。
ウ：ベースラインとシグネチャは補完関係であり、更新は依然必要である。
エ：分析には十分なテレメトリ・履歴が必要である。
総合解説：環境変更に応じてベースラインを更新しないと誤検知が増えるため、継続的なチューニングが必要である。

Q082 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

インライン動作で業務通信を止めるリスクを避けつつ、ネットワーク通信をNIDSへ複製して観測したい。適した方法はどれか。
ア．FWを無効化して全通信をNIDSへ転送する。
イ．スイッチのSPAN/ミラーポートやネットワークTAPを用いて通信のコピーを監視装置へ渡す。
ウ．公開鍵証明書をNIDSへ発行すればパケット複製できる。
エ．DNSのMXレコードをNIDSのIPへ変更する。

正答・4肢解説・総合解説

正答：イ．スイッチのSPAN/ミラーポートやネットワークTAPを用いて通信のコピーを監視装置へ渡す。
ア：境界制御を失い、監視方法として不適切である。
イ：受動監視では本番通信経路へ直接遮断動作を入れずにパケットを観測できる。
ウ：証明書発行とトラフィックミラーリングは別である。
エ：MXはメール配送先の指定であり、一般通信監視には使わない。
総合解説：SPANは混雑時の取りこぼし等、TAPは導入コスト等の特徴があるため、監視要件に応じて選択する。

Q083 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

ほぼ全てのWeb通信がTLSで暗号化されている環境でNIDSだけを使う場合の注意点はどれか。
ア．TLS通信は暗号化されているので攻撃に利用されることはない。
イ．NIDSがあればEDRやサーバログは常に不要である。
ウ．復号地点がなければHTTP本文等を直接確認できないため、メタデータ分析やエンドポイント・プロキシ側ログで可視性を補完する必要がある。
エ．TLSを全社で無効化すれば最も安全である。

正答・4肢解説・総合解説

正答：ウ．復号地点がなければHTTP本文等を直接確認できないため、メタデータ分析やエンドポイント・プロキシ側ログで可視性を補完する必要がある。
ア：攻撃者もTLSを利用でき、暗号化は通信内容の安全性を自動保証しない。
イ：暗号化やホスト内部挙動はNIDSだけでは見えないことがある。
ウ：暗号化は通信保護に重要だが、ネットワーク監視から見える情報を減らすため、多層のテレメトリが必要になる。
エ：盗聴・改ざんリスクを大きく高める。
総合解説：可視性と機密性を両立するため、ネットワーク、エンドポイント、ID、クラウドなど複数データ源を組み合わせる。

Q084 2-3 ネットワークセキュリティ / IDS・IPS・セキュリティ監視

SOCに1日1万件のセキュリティアラートが届き、重大イベントの見落としが起きている。改善策として最も適切なものはどれか。
ア．全アラートを自動削除する。
イ．誤検知を減らすため全検知ルールを無効にする。
ウ．重要資産からのアラートほど優先度を下げる。
エ．資産重要度、信頼度、脅威コンテキスト、重複抑制などで優先順位を付け、検知ルールを継続的にチューニングする。

正答・4肢解説・総合解説

正答：エ．資産重要度、信頼度、脅威コンテキスト、重複抑制などで優先順位を付け、検知ルールを継続的にチューニングする。
ア：重大アラートも失われる。
イ：検知能力そのものを失う。
ウ：影響度を無視した優先付けになる。
エ：大量アラートを同じ優先度で処理するとアラート疲労が生じるため、リスクベースのトリアージが必要である。
総合解説：監視品質はアラート数ではなく、重要な異常を適切な時間で検知・調査・対応できるかで評価する。

Q085 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

IPsecのトンネルモードの一般的な特徴として最も適切なものはどれか。
ア．元のIPパケット全体を保護対象として新しいIPヘッダでカプセル化し、拠点間VPNなどで利用できる。
イ．TCPのアプリケーションデータだけを暗号化しIPヘッダは作らない。
ウ．DNSSECの署名だけを運ぶモードである。
エ．電子メールのFromヘッダだけを暗号化する。

正答・4肢解説・総合解説

正答：ア．元のIPパケット全体を保護対象として新しいIPヘッダでカプセル化し、拠点間VPNなどで利用できる。
ア：トンネルモードはゲートウェイ間で内部パケットを包んで保護する構成に適する。
イ：IPsecトンネルモードはIP層で元パケットをカプセル化する。
ウ：DNSSEC専用ではない。
エ：メールヘッダ専用技術ではない。
総合解説：IPsecはネットワーク層で通信を保護し、サイト間VPNやリモートアクセス等の構成で利用される。

Q086 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

TLS 1.3の主なセキュリティ目的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自動的に修正する。
イ．クライアントとサーバ間通信の盗聴・改ざん・メッセージ偽造を防ぐための保護を提供する。
ウ．DNSレコードのキャッシュ時間を決める。
エ．利用者のOSパッチを自動適用する。

正答・4肢解説・総合解説

正答：イ．クライアントとサーバ間通信の盗聴・改ざん・メッセージ偽造を防ぐための保護を提供する。
ア：TLSは通信路を保護するが、アプリケーション脆弱性を修正しない。
イ：TLSはトランスポート上の機密性と完全性、相手認証等を実現するプロトコルである。
ウ：TTL設定とは無関係である。
エ：パッチ管理機能ではない。
総合解説：HTTPSでTLSを使っていても、認証・認可不備やWeb脆弱性は別途対策する必要がある。

Q087 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

TLS接続で証明書チェーンの署名は正しいが、接続先ホスト名と証明書名が一致しない。クライアントの適切な動作はどれか。
ア．署名が正しければ名前不一致を常に無視する。
イ．証明書名の代わりにWebページのタイトル文字列を確認する。
ウ．名前不一致を検証エラーとして扱い、警告を無視して自動接続しない。
エ．TLSをHTTPへダウングレードして接続する。

正答・4肢解説・総合解説

正答：ウ．名前不一致を検証エラーとして扱い、警告を無視して自動接続しない。
ア：別ホスト向け証明書の悪用を許す。
イ：ページ内容は攻撃者が制御でき、TLS認証の根拠にならない。
ウ：信頼CAの署名だけでなく接続対象の名前に対して発行された証明書かを確認しないと、中間者の別証明書を受理する危険がある。
エ：通信保護を失う危険な回避策である。
総合解説：TLSの安全性は暗号スイートだけでなく、証明書検証、鍵管理、プロトコル設定に依存する。

Q088 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

DNSSECの主な目的として最も適切なものはどれか。
ア．DNS問い合わせ内容を必ず暗号化して秘匿する。
イ．DNSサーバへのDDoSを完全に防止する。
ウ．WebサーバのTLS証明書を自動失効させる。
エ．DNS応答に対するデータ起源認証と完全性検証を可能にし、改ざんされた応答を検出しやすくする。

正答・4肢解説・総合解説

正答：エ．DNS応答に対するデータ起源認証と完全性検証を可能にし、改ざんされた応答を検出しやすくする。
ア：DNSSECは主に真正性・完全性を提供し、問い合わせの機密性はDoT/DoH等の別技術で扱う。
イ：DNSSECだけで可用性攻撃を完全防止できない。
ウ：証明書失効はPKIの機能である。
エ：DNSSECはDNSデータへ暗号学的署名を導入し、信頼連鎖を検証する仕組みである。
総合解説：DNSSECと暗号化DNSは目的が異なる。前者は応答の真正性・完全性、後者はクライアントとリゾルバ間通信の機密性等を主に扱う。

Q089 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

端末と再帰DNSリゾルバ間にDoHやDoT等の暗号化DNSを導入する主な効果はどれか。
ア．その区間のDNS問い合わせを盗聴・改ざんされにくくし、利用者の問い合わせ内容の機密性を高める。
イ．権威DNSから端末までの全てのDNSデータが自動的にDNSSEC署名される。
ウ．DNSを使う全Web通信の本文まで暗号化する。
エ．フィッシングサイトを必ず全て判定して遮断する。

正答・4肢解説・総合解説

正答：ア．その区間のDNS問い合わせを盗聴・改ざんされにくくし、利用者の問い合わせ内容の機密性を高める。
ア：暗号化DNSはクライアントとリゾルバ間を保護するが、利用するリゾルバへの信頼やDNS応答自体の真正性とは別に考える。
イ：暗号化DNSとDNSSECは別技術であり、一方が他方を自動有効化しない。
ウ：Web本文の暗号化はTLS/HTTPS等が担う。
エ：暗号化は内容の安全性判定を保証しない。
総合解説：DNSセキュリティではDNSSEC、暗号化DNS、Protective DNS、ログ監視等を脅威に応じて組み合わせる。

Q090 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

SPF、DKIM、DMARCの関係として最も適切なものはどれか。
ア．SPFはメール本文を暗号化し、DKIMは添付を圧縮し、DMARCはウイルスを削除する。
イ．SPFは送信元IP等の許可をドメインが宣言し、DKIMはメールへドメイン署名を付け、DMARCはそれらの結果とFromドメインの整合性に基づく方針・報告を提供する。
ウ．三つとも受信者のパスワードを検証する認証方式である。
エ．DMARCを設定すると全フィッシングメールが必ず消滅する。

正答・4肢解説・総合解説

正答：イ．SPFは送信元IP等の許可をドメインが宣言し、DKIMはメールへドメイン署名を付け、DMARCはそれらの結果とFromドメインの整合性に基づく方針・報告を提供する。
ア：それぞれの主目的を誤っている。
イ：三者は送信ドメイン認証を補完し、なりすましメール対策に利用される。
ウ：利用者ログイン認証ではなく、メール送信ドメインの信頼性向上に使う。
エ：正規ドメイン侵害や類似ドメイン等には別対策も必要である。
総合解説：メール認証は単独で完全ではなく、受信側フィルタ、利用者教育、URL/添付検査等と組み合わせる。

Q091 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

SMTPサーバ間でTLSを利用しているメールについて、最も適切な説明はどれか。
ア．TLSを使えばメールサーバ管理者も本文を絶対に読めない。
イ．TLSを使うと送信者ドメイン認証SPF/DKIM/DMARCは不要になる。
ウ．通信区間の盗聴・改ざんリスクを低減できるが、メールが各サーバで平文として扱われ得るため、送信者から受信者までのエンドツーエンド暗号化と同一ではない。
エ．TLSはメールの迷惑判定を行うプロトコルである。

正答・4肢解説・総合解説

正答：ウ．通信区間の盗聴・改ざんリスクを低減できるが、メールが各サーバで平文として扱われ得るため、送信者から受信者までのエンドツーエンド暗号化と同一ではない。
ア：サーバで復号される構成では管理者権限等からアクセス可能な場合がある。
イ：通信路保護とドメイン認証は別の役割である。
ウ：TLSは通信路単位の保護であり、メッセージ自体のE2E暗号化とは信頼境界が異なる。
エ：TLSは通信路保護を行う。
総合解説：「通信路暗号化」と「コンテンツのエンドツーエンド暗号化」を区別して脅威モデルを考える。

Q092 2-3 ネットワークセキュリティ / VPN・TLS・DNS・メールセキュリティ

リモートアクセスVPNでスプリットトンネルを有効にする場合のリスクとして最も適切なものはどれか。
ア．VPNを使う限り端末のマルウェア対策は不要になる。
イ．スプリットトンネルにするとTLS証明書が不要になる。
ウ．スプリットトンネルではインターネット通信が物理的に不可能になる。
エ．端末が社内VPNとインターネットへ同時接続するため、端末侵害時に社内への迂回経路となる可能性があり、端末防御や経路制御が重要になる。

正答・4肢解説・総合解説

正答：エ．端末が社内VPNとインターネットへ同時接続するため、端末侵害時に社内への迂回経路となる可能性があり、端末防御や経路制御が重要になる。
ア：VPNは端末内部の侵害を防ぐ仕組みではない。
イ：TLSや証明書利用とは別の経路設計である。
ウ：一部通信をVPN外へ直接出すことが特徴である。
エ：スプリットトンネルは帯域・性能面の利点がある一方、全通信を企業側で検査できない等のセキュリティ上のトレードオフがある。
総合解説：VPN設定は「暗号化されているか」だけでなく、どの通信をどこへ流すか、端末状態をどう確認するかまで評価する。

Q093 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

EDRの特徴として最も適切なものはどれか。
ア．エンドポイント上のプロセス実行、通信、ファイル操作などのテレメトリを継続的に収集し、検知・調査・対応を支援する。
イ．電子証明書を発行し、公開鍵の所有者を保証する。
ウ．ネットワーク境界で全通信をルーティングし、IPアドレスを変換する。
エ．バックアップ媒体を物理的に保管するだけの仕組みである。

正答・4肢解説・総合解説

正答：ア．エンドポイント上のプロセス実行、通信、ファイル操作などのテレメトリを継続的に収集し、検知・調査・対応を支援する。
ア：EDRは単一ファイルの既知シグネチャ照合だけでなく、端末上の挙動を時系列で把握し、インシデント調査や隔離などの対応を支援する。
イ：これはPKI・認証局の役割であり、EDRの主機能ではない。
ウ：これはルータやNAT等の機能であり、EDRの主目的ではない。
エ：EDRはエンドポイントの監視・検知・対応を扱う。
総合解説：EDRは予防策を置き換えるものではなく、パッチ管理、権限制御、アンチマルウェア、ログ監視などと多層で組み合わせる。

Q094 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

EDRで、文書閲覧ソフトからスクリプト実行環境が起動され、その直後に外部サイトへ通信した記録が検知された。最初に確認すべき情報として最も有効なものはどれか。
ア．端末の壁紙の色だけを確認する。
イ．親子プロセス関係、コマンドライン、実行ユーザ、通信先、時刻などを関連付けて一連の実行経路を確認する。
ウ．検知アラートを直ちに削除し、履歴を残さない。
エ．CPU型番だけで攻撃者を特定する。

正答・4肢解説・総合解説

正答：イ．親子プロセス関係、コマンドライン、実行ユーザ、通信先、時刻などを関連付けて一連の実行経路を確認する。
ア：インシデントの実行経路や侵害範囲の判断材料にならない。
イ：不審な単一プロセスだけでなく、その起点と後続動作を時系列・プロセスツリーで確認すると、攻撃連鎖と影響範囲を判断しやすい。
ウ：調査に必要な証跡を失うため不適切である。
エ：CPU型番から攻撃経路や主体を特定することはできない。
総合解説：EDR調査では、プロセス、ファイル、レジストリ、認証、通信など複数のテレメトリを相関させることが重要である。

Q095 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

マルウェア感染が疑われる端末をEDRからネットワーク隔離する主な目的はどれか。
ア．証拠を全て消去して調査を不要にするため。
イ．端末の脆弱性を自動的に全て修正するため。
ウ．攻撃者の外部通信や他端末への横展開を抑えつつ、必要な管理・調査経路を確保して封じ込めるため。
エ．バックアップ世代を増やすため。

正答・4肢解説・総合解説

正答：ウ．攻撃者の外部通信や他端末への横展開を抑えつつ、必要な管理・調査経路を確保して封じ込めるため。
ア：証拠消去は原因分析や影響範囲確認を妨げる。
イ：隔離自体はパッチ適用や根本原因除去を保証しない。
ウ：端末隔離は被害拡大の抑制を目的とする封じ込め策であり、製品によってはEDR管理通信だけを残す設計もある。
エ：隔離とバックアップ世代管理は別の対策である。
総合解説：隔離後も、影響範囲特定、根絶、認証情報の対処、復旧確認などが必要であり、隔離だけで対応完了とはならない。

Q096 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

EDRで同一端末から、短時間の大量ファイル書換え、バックアップ関連サービスの停止、不審な外部通信が連続して観測された。対応として最も適切なものはどれか。
ア．大量書換えは正常業務と断定し、監視を停止する。
イ．端末だけ再起動し、ログを全削除する。
ウ．全社のバックアップを同じ端末へ接続して確認する。
エ．高リスクの侵害兆候として優先度を上げ、端末隔離と証跡保全を行い、同様の兆候を他端末にも横断検索する。

正答・4肢解説・総合解説

正答：エ．高リスクの侵害兆候として優先度を上げ、端末隔離と証跡保全を行い、同様の兆候を他端末にも横断検索する。
ア：複数の不審兆候を無視すると被害拡大につながる。
イ：証跡を失い、持続化や横展開の確認もできなくなる。
ウ：感染端末へバックアップを接続するとバックアップまで被害を受けるおそれがある。
エ：複数の不審挙動が連続する場合は単発アラートより侵害可能性が高く、封じ込めと全体影響調査を並行するのが適切である。
総合解説：ランサムウェア対策では、端末検知だけでなく、権限管理、分離されたバックアップ、復元訓練、横展開監視を組み合わせる。

Q097 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

既知マルウェアのシグネチャ検知だけに依存する場合の主な限界はどれか。
ア．未知・改変されたマルウェアや正規ツール悪用など、既知シグネチャに一致しない攻撃を見逃す可能性がある。
イ．シグネチャ検知では既知マルウェアを一切検知できない。
ウ．シグネチャを用いると端末のOS更新が物理的に不可能になる。
エ．シグネチャ検知は必ず公開鍵暗号を無効化する。

正答・4肢解説・総合解説

正答：ア．未知・改変されたマルウェアや正規ツール悪用など、既知シグネチャに一致しない攻撃を見逃す可能性がある。
ア：シグネチャは既知脅威の効率的な検知に有用だが、挙動・ヒューリスティック・テレメトリ分析などとの併用が必要である。
イ：既知パターンへの一致検知はシグネチャ方式の強みである。
ウ：シグネチャ検知とOS更新可否は直接関係しない。
エ：暗号機能の有効無効とは別の仕組みである。
総合解説：単一の検知方式には盲点があるため、予防・検知・応答を複数層で設計する。

Q098 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

EDRが管理者によるスクリプト実行を高リスクとして検知したが、同じ処理は承認済み保守作業でも使用される。最も適切な対応はどれか。
ア．その実行ファイル名を全社で永久に無条件許可する。
イ．実行ユーザ、端末、コマンドライン、親プロセス、変更申請、通信先などの文脈を確認して正当性を判断し、必要なら検知ルールを限定的に調整する。
ウ．誤検知の可能性があるアラートは全て自動削除する。
エ．利用者の所属部署だけでマルウェアかどうか決定する。

正答・4肢解説・総合解説

正答：イ．実行ユーザ、端末、コマンドライン、親プロセス、変更申請、通信先などの文脈を確認して正当性を判断し、必要なら検知ルールを限定的に調整する。
ア：同じ正規ツールが攻撃に悪用された場合の検知を失う。
イ：正規ツールも攻撃に悪用され得るため、単純な許可リスト化ではなく実行文脈を確認する必要がある。
ウ：重大な侵害を見逃す危険がある。
エ：攻撃判断には技術的証拠と運用文脈の確認が必要である。
総合解説：アラート品質向上では、誤検知低減と検知能力維持の両方を満たすチューニングが重要である。

Q099 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

攻撃者が管理者権限を奪取した後、最初にEDRエージェントを停止しようとする攻撃に対する対策として有効なものはどれか。
ア．EDRの管理者パスワードを全利用者で共有する。
イ．EDRの更新を停止し、同じバージョンを永久利用する。
ウ．EDRサービスの改変・停止を制限する自己防御機能を有効にし、管理操作も強い認証と監査の対象にする。
エ．EDRのログを端末ローカルだけに保存し、削除権限を攻撃者と共有する。

正答・4肢解説・総合解説

正答：ウ．EDRサービスの改変・停止を制限する自己防御機能を有効にし、管理操作も強い認証と監査の対象にする。
ア：認証情報共有は不正停止や追跡不能のリスクを高める。
イ：脆弱性修正や検知改善を受けられなくなる。
ウ：検知基盤そのものを無効化されないよう、耐タンパ性、管理権限の分離、ログ監査などを組み合わせる必要がある。
エ：侵害時に証跡を消去されやすくなる。
総合解説：セキュリティ製品も攻撃対象である。管理面・ログ・更新機構まで含めて保護する。

Q100 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

EDR導入率が95%と表示されているが、残り5%に重要サーバと長期間オフラインだった端末が含まれている。最も適切な評価はどれか。
ア．95%を超えていれば未導入端末の内容は確認不要である。
イ．オフライン端末は攻撃を受けないため管理対象外にする。
ウ．EDRがない端末は自動的にネットワークから物理的に消滅する。
エ．台数比率だけで十分とせず、未導入・未接続端末の資産重要度とセンサー健全性を確認し、監視空白を解消する。

正答・4肢解説・総合解説

正答：エ．台数比率だけで十分とせず、未導入・未接続端末の資産重要度とセンサー健全性を確認し、監視空白を解消する。
ア：重要資産の未監視は重大リスクになり得る。
イ：持ち出し端末等はオフライン中にも侵害され、再接続時に影響を及ぼす可能性がある。
ウ：未導入端末は依然として資産として存在する。
エ：重要資産にセンサー欠落があると、全体の導入率が高くても重大な可視性ギャップになる。
総合解説：EDR運用では配備率だけでなく、センサーの稼働・更新・通信状況と資産台帳との突合が必要である。

Q101 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

攻撃者が新規実行ファイルを保存せず、正規のスクリプト実行環境や管理ツールを悪用する攻撃への検知として最も有効なものはどれか。
ア．プロセス生成、コマンドライン、スクリプト内容、認証、通信などの挙動テレメトリを相関して異常を検知する。
イ．拡張子.exeのファイルだけを検索すれば十分である。
ウ．全てのOSログを停止して攻撃者に情報を与えない。
エ．DNSキャッシュを一度削除すれば以後の攻撃を防げる。

正答・4肢解説・総合解説

正答：ア．プロセス生成、コマンドライン、スクリプト内容、認証、通信などの挙動テレメトリを相関して異常を検知する。
ア：ファイルが作られない攻撃ではファイルスキャンだけでは不足し、実行時の挙動を観測する必要がある。
イ：新規実行ファイルを作らない攻撃を見逃す。
ウ：防御側の可視性を失い、調査困難になる。
エ：単発のキャッシュ削除では挙動型攻撃を防止できない。
総合解説：正規機能の悪用（living off the land）を考慮し、実行の「内容と文脈」を監視する。

Q102 2-4 エンドポイント・データ保護 / マルウェア対策・EDR

組織のマルウェア対策として最も適切な方針はどれか。
ア．最新EDRを導入すれば他の対策は全て不要である。
イ．メール・Web対策、パッチ管理、最小権限、アプリ制御、エンドポイント検知、利用者教育、バックアップを組み合わせる。
ウ．未知マルウェア対策として全パッチ適用を停止する。
エ．利用者に管理者権限を常時付与して操作自由度を上げる。

正答・4肢解説・総合解説

正答：イ．メール・Web対策、パッチ管理、最小権限、アプリ制御、エンドポイント検知、利用者教育、バックアップを組み合わせる。
ア：EDRにも検知漏れや無効化の可能性があり、単独依存は不適切である。
イ：マルウェアは複数経路から侵入し得るため、単一製品ではなく予防・検知・対応・復旧を多層化する。
ウ：既知脆弱性の悪用機会を増やす。
エ：侵害時の影響を拡大するため最小権限に反する。
総合解説：防御は「侵入を完全に防ぐ」だけでなく、侵害を早期検知し、被害を限定し、復旧できる構成にする。

Q103 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

ノートPCのフルディスク暗号化が特に有効な脅威はどれか。
ア．利用者がログイン中にマルウェアが利用者権限でファイルを読む脅威を必ず防ぐ。
イ．WebアプリケーションのSQLインジェクションを防ぐ。
ウ．電源オフ状態の端末や取り外した記憶媒体が盗難・紛失し、ストレージを直接読み出される脅威。
エ．DDoSによる回線帯域枯渇を防ぐ。

正答・4肢解説・総合解説

正答：ウ．電源オフ状態の端末や取り外した記憶媒体が盗難・紛失し、ストレージを直接読み出される脅威。
ア：復号済みデータへ正規権限でアクセスされる場合、ディスク暗号化だけでは防げない。
イ：アプリケーション入力処理の脆弱性とは別の対策である。
ウ：ストレージ暗号化は保存データの不正読出し対策であり、特に端末紛失・盗難時の機密性確保に有効である。
エ：ストレージ暗号化はネットワーク可用性攻撃を防がない。
総合解説：暗号化は「いつデータが復号されるか」という信頼境界まで含めて評価する。

Q104 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

クラウドストレージの保存データ暗号化とTLSによる通信暗号化の関係として最も適切なものはどれか。
ア．保存時暗号化を使えば通信は必ず平文で安全になる。
イ．TLSを使えばバックエンドストレージ上のデータは必ず暗号化される。
ウ．二つの暗号化は同一の鍵を永久に共有しなければならない。
エ．保存時と通信時では保護する区間が異なるため、機密データでは両方を脅威に応じて組み合わせる。

正答・4肢解説・総合解説

正答：エ．保存時と通信時では保護する区間が異なるため、機密データでは両方を脅威に応じて組み合わせる。
ア：通信路の盗聴・改ざん対策は別途必要である。
イ：TLSは通信路保護であり、保存時暗号化を自動保証しない。
ウ：用途・鍵管理は分離して設計でき、同一鍵の使い回しを前提としない。
エ：保存時暗号化は媒体・ストレージ上のデータを、通信暗号化は移送中のデータを主に保護する。
総合解説：データライフサイクルに沿って「保存中・通信中・利用中」のどこで露出するかを整理する。

Q105 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

DLPの目的として最も適切なものはどれか。
ア．機密データを識別し、メール、Webアップロード、クラウド共有、外部媒体などを通じた不適切な持出しを検知・制御する。
イ．CPUクロックを自動的に下げて発熱を防ぐ。
ウ．公開鍵証明書の有効期限だけを延長する。
エ．ルーティングテーブルを最短経路に最適化する。

正答・4肢解説・総合解説

正答：ア．機密データを識別し、メール、Webアップロード、クラウド共有、外部媒体などを通じた不適切な持出しを検知・制御する。
ア：DLPはデータの内容・分類・利用文脈・送信経路などを使って情報漏えいリスクを低減する。
イ：DLPはデータ保護の仕組みであり、電力制御ではない。
ウ：証明書管理とは別の機能である。
エ：ネットワーク経路制御を目的とする製品ではない。
総合解説：DLP導入前には、何を機密情報とするか、許可される業務利用は何かを整理しないと誤検知や業務阻害が増える。

Q106 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

DLPが「顧客番号らしい数字列」を含む文書を全て遮断した結果、公開資料まで大量に止まり業務が停滞した。改善策として最も適切なものはどれか。
ア．DLPを完全停止し、持出し制御を全廃する。
イ．データ分類、辞書・フィンガープリント、送信先、利用者、件数など複数条件を組み合わせ、監視結果を基に段階的にチューニングする。
ウ．数字を含む全ファイルを永久削除する。
エ．送信先や利用者に関係なく全通信を同じ判定に固定する。

正答・4肢解説・総合解説

正答：イ．データ分類、辞書・フィンガープリント、送信先、利用者、件数など複数条件を組み合わせ、監視結果を基に段階的にチューニングする。
ア：誤検知は減るが漏えい防止能力も失う。
イ：単純なパターン一致だけでは誤検知が増えるため、データの意味と利用文脈を加えて精度を上げる。
ウ：正当な業務データを破壊する不適切な対応である。
エ：文脈を使わないため業務適合性が低い。
総合解説：DLPは検知精度だけでなく、例外申請、承認、監査ログ、教育など運用プロセスまで設計する。

Q107 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

ランサムウェア対策としてバックアップを用意する際、復旧可能性を高める構成はどれか。
ア．本番サーバと同じ共有フォルダだけを唯一のバックアップ先にする。
イ．バックアップを作成したら復元手順を一度も確認しない。
ウ．本番環境の侵害権限から容易に削除・暗号化できないよう、分離したコピーや変更困難な保護を設ける。
エ．バックアップ管理者の認証情報を一般利用者と共有する。

正答・4肢解説・総合解説

正答：ウ．本番環境の侵害権限から容易に削除・暗号化できないよう、分離したコピーや変更困難な保護を設ける。
ア：本番侵害時に同時に暗号化・削除される可能性が高い。
イ：復旧不能を障害時まで発見できない。
ウ：本番と同じ認証情報・同じ管理経路だけで書換え可能なバックアップは、攻撃時に同時破壊される危険がある。
エ：バックアップ破壊につながる権限濫用リスクを高める。
総合解説：バックアップは「存在すること」ではなく、攻撃時にも残り、必要時間内に復元できることが重要である。

Q108 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

バックアップジョブが毎日「成功」と表示されていても、定期的な復元テストが必要な主な理由はどれか。
ア．復元テストをするとバックアップは必ず全て消えるから。
イ．バックアップ成功なら復元は数学的に100%保証されるから。
ウ．復元テストの目的は暗号鍵を公開することだから。
エ．バックアップデータの破損、依存関係不足、鍵紛失、手順不備などにより実際には復元できない可能性があるため。

正答・4肢解説・総合解説

正答：エ．バックアップデータの破損、依存関係不足、鍵紛失、手順不備などにより実際には復元できない可能性があるため。
ア：適切に計画した復元テストはバックアップ破壊を前提としない。
イ：取得と復元は別工程であり、実地確認が必要である。
ウ：鍵は保護しつつ復旧可能性を確認する。
エ：取得成功ログだけでは、業務として利用可能な状態まで復元できることを保証しない。
総合解説：復旧目標に合わせ、データ整合性、アプリ起動、認証・ネットワーク依存関係まで確認する。

Q109 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

バックアップ・復旧計画におけるRPOとRTOの説明として最も適切なものはどれか。
ア．RPOは許容できるデータ損失量を時間で表す目標、RTOは中断後にサービスを復旧させるまでの目標時間である。
イ．RPOは暗号鍵長、RTOはハッシュ値長を表す。
ウ．RPOとRTOは必ず同じ値にしなければならない。
エ．RTOはバックアップを何世代保存するかだけを表す。

正答・4肢解説・総合解説

正答：ア．RPOは許容できるデータ損失量を時間で表す目標、RTOは中断後にサービスを復旧させるまでの目標時間である。
ア：RPOはどこまで過去のデータへ戻ってよいか、RTOはどれだけ早くサービスを戻すかを表す。
イ：どちらも復旧計画上の時間目標であり暗号パラメータではない。
ウ：事業影響とシステム特性に応じて別々に設定される。
エ：保存世代数だけではなく復旧完了までの時間目標である。
総合解説：例としてRPO=1時間なら最大約1時間分の更新損失を許容する設計、RTO=4時間なら4時間以内のサービス復旧を目指す。

Q110 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

バックアップを強力に暗号化したが、復号鍵を本番サーバ内だけに保存していたため、本番サーバ故障時に鍵も失われた。改善策として最も適切なものはどれか。
ア．暗号化を廃止し、全バックアップを公開する。
イ．復号鍵を厳格に保護しつつ、本番障害とは独立した安全な鍵バックアップ・復旧手順を設けて定期的に確認する。
ウ．鍵をバックアップファイル名として公開保存する。
エ．同じ鍵を全システムで永久に使い回す。

正答・4肢解説・総合解説

正答：イ．復号鍵を厳格に保護しつつ、本番障害とは独立した安全な鍵バックアップ・復旧手順を設けて定期的に確認する。
ア：機密性を失う極端な対応である。
イ：暗号化バックアップは鍵が復旧できなければ利用不能になるため、鍵の可用性と機密性を両立する必要がある。
ウ：鍵漏えいにより暗号化の意味が失われる。
エ：漏えい時の影響範囲が広がり、鍵更新も困難になる。
総合解説：データ復旧計画には「暗号化されたデータ」と「それを復号する鍵」の両方を含める必要がある。

Q111 2-4 エンドポイント・データ保護 / 暗号化・DLP・バックアップ

クラウド上でスナップショットを定期作成しているだけで、同じ管理アカウントから全スナップショットを削除できる。ランサムウェア等への備えとしての問題点はどれか。
ア．スナップショットは常に紙媒体なので削除されない。
イ．スナップショットを作るとDLPが必ず無効になる。
ウ．管理アカウント侵害時に本番と復旧用コピーを同時削除され得るため、別権限・別保管先・変更困難な保護などを検討すべきである。
エ．スナップショットがあれば復元テストは不要である。

正答・4肢解説・総合解説

正答：ウ．管理アカウント侵害時に本番と復旧用コピーを同時削除され得るため、別権限・別保管先・変更困難な保護などを検討すべきである。
ア：クラウドスナップショットは電子データであり、権限次第で削除可能である。
イ：両者にそのような必然関係はない。
ウ：スナップショットは有用だが、同一障害ドメイン・同一管理権限だけに依存すると復旧手段の独立性が不足する。
エ：実際の復元可能性はテストで確認する必要がある。
総合解説：復旧設計では、同時侵害・誤操作・アカウント乗っ取りなど共通原因故障を避ける。

Q112 2-4 エンドポイント・データ保護 / ハードニング・構成管理

サーバのハードニングとして最も適切なものはどれか。
ア．互換性のため全サービスを有効化する。
イ．管理者アカウントを全利用者で共有する。
ウ．監査ログを全て無効にする。
エ．不要なサービス・ポート・アカウントを無効化し、安全な設定ベースラインを適用して攻撃面を減らす。

正答・4肢解説・総合解説

正答：エ．不要なサービス・ポート・アカウントを無効化し、安全な設定ベースラインを適用して攻撃面を減らす。
ア：不要機能を増やし攻撃面を拡大する。
イ：権限管理と追跡性を損なう。
ウ：異常検知・事後調査が困難になる。
エ：ハードニングは必要機能を保ちながら不要機能や危険な既定設定を減らし、攻撃可能な面を小さくする。
総合解説：ハードニングは一度だけの作業ではなく、更新後や構成変更後にも基準との差分を確認する。

Q113 2-4 エンドポイント・データ保護 / ハードニング・構成管理

新規導入した装置にベンダ既定の管理者アカウントと既定パスワードが残っている。最も優先すべき対応はどれか。
ア．不要な既定アカウントを無効化し、必要な管理アカウントは固有の強い認証へ変更して権限を限定する。
イ．既定パスワードをマニュアルに追記して全員へ配布する。
ウ．管理画面をインターネットへ公開して操作しやすくする。
エ．ログイン履歴を削除し、既定設定を維持する。

正答・4肢解説・総合解説

正答：ア．不要な既定アカウントを無効化し、必要な管理アカウントは固有の強い認証へ変更して権限を限定する。
ア：公開・推測可能な既定認証情報は容易な侵入口になるため、導入時ハードニングで除去する。
イ：攻撃者に知られる可能性を高める。
ウ：攻撃面を拡大し、既定認証情報の危険を増す。
エ：根本的な認証リスクを解消しない。
総合解説：初期設定チェックリストに、既定資格情報、不要サービス、管理経路、ログ、更新設定などを含める。

Q114 2-4 エンドポイント・データ保護 / ハードニング・構成管理

構成ドリフト（configuration drift）の説明として最も適切なものはどれか。
ア．暗号鍵を定期的に更新することそのもの。
イ．運用中の設定が、承認済みのセキュリティ構成ベースラインから徐々に乖離していく状態。
ウ．ネットワーク遅延が時間帯で変化する現象。
エ．バックアップから正常に復元できる状態。

正答・4肢解説・総合解説

正答：イ．運用中の設定が、承認済みのセキュリティ構成ベースラインから徐々に乖離していく状態。
ア：鍵更新は構成ドリフトの定義ではない。
イ：手作業変更や更新、例外対応などで基準との差分が蓄積すると、意図しない脆弱設定が生じ得る。
ウ：性能変動と構成管理は別の概念である。
エ：復旧可能性の説明でありドリフトではない。
総合解説：ベースラインとの差分を自動検出し、承認済み変更か不正・誤設定かを確認する運用が重要である。

Q115 2-4 エンドポイント・データ保護 / ハードニング・構成管理

パッチ管理とセキュリティ構成管理の関係として最も適切なものはどれか。
ア．パッチを適用すれば設定監査は永久に不要になる。
イ．構成管理はOSのバージョンを一切記録しない。
ウ．パッチ管理は既知脆弱性等を修正する更新を扱い、構成管理は許可設定・サービス・権限などの望ましい状態と変更を継続的に管理する。
エ．両者はバックアップ暗号化方式の名称である。

正答・4肢解説・総合解説

正答：ウ．パッチ管理は既知脆弱性等を修正する更新を扱い、構成管理は許可設定・サービス・権限などの望ましい状態と変更を継続的に管理する。
ア：脆弱設定はパッチ適用後も残り得る。
イ：構成項目にはソフトウェア・バージョン等も含めて管理する。
ウ：両者は重なる部分があるが、更新適用だけでは危険な設定や不要サービスを是正できない。
エ：更新・設定管理のプロセスであり暗号方式ではない。
総合解説：安全な運用では、脆弱性修正と安全な構成の維持を別々に確認する。

Q116 2-4 エンドポイント・データ保護 / ハードニング・構成管理

アプリケーション許可リスト方式の主な利点はどれか。
ア．許可リストへ登録すると全アプリの脆弱性が自動修正される。
イ．許可リストはネットワーク暗号化を提供する。
ウ．許可リストを使うと利用者認証が不要になる。
エ．事前に許可した実行ファイルやスクリプトだけを実行可能にし、未承認コードの実行を抑制できる。

正答・4肢解説・総合解説

正答：エ．事前に許可した実行ファイルやスクリプトだけを実行可能にし、未承認コードの実行を抑制できる。
ア：実行可否制御と脆弱性修正は別である。
イ：通信暗号化機能ではない。
ウ：実行制御と認証は異なる管理策である。
エ：必要なアプリを限定できる環境では、未知マルウェアを含む未承認実行の攻撃面を減らせる。
総合解説：運用ではソフトウェア更新や業務変更に合わせた承認プロセスを用意し、古い許可ルールを放置しない。

Q117 2-4 エンドポイント・データ保護 / ハードニング・構成管理

本番サーバのファイアウォール設定を緊急変更する必要がある。構成管理として最も適切な手順はどれか。
ア．変更理由・影響・実施者を記録し、必要な承認と試験を行い、実施後に結果確認と必要なら戻せる手順を確保する。
イ．緊急時は記録を残さず直接変更し、その後も確認しない。
ウ．全ポートを恒久開放して変更作業を簡略化する。
エ．本番環境でのみ初めて変更内容を考える。

正答・4肢解説・総合解説

正答：ア．変更理由・影響・実施者を記録し、必要な承認と試験を行い、実施後に結果確認と必要なら戻せる手順を確保する。
ア：緊急変更でも追跡性と復旧可能性を失わないことが重要で、後追い承認やレビューを含む緊急手順を定める。
イ：意図しない影響や不正変更を追跡できない。
ウ：必要最小限の通信制御に反し攻撃面を拡大する。
エ：可能な範囲で事前検証と影響評価が必要である。
総合解説：変更管理は「変更を禁止する」仕組みではなく、安全に変更し、構成の正当性を説明できるようにする仕組みである。

Q118 2-4 エンドポイント・データ保護 / ハードニング・構成管理

多数のサーバを同一構成で運用しており、個別の手作業変更によるばらつきが問題になっている。改善策として最も適切なものはどれか。
ア．各管理者が本番機を自由に手作業変更し、記録しない。
イ．承認済みイメージや構成コードから再展開し、個別変更を最小化して望ましい状態を再現できるようにする。
ウ．サーバごとに別の既定パスワードを紙に貼る。
エ．構成差異をなくすため監視を停止する。

正答・4肢解説・総合解説

正答：イ．承認済みイメージや構成コードから再展開し、個別変更を最小化して望ましい状態を再現できるようにする。
ア：構成差異と追跡不能を増やす。
イ：標準化されたイメージやInfrastructure as Code等を用いると、構成の再現性と監査性を高め、ドリフトを抑えやすい。
ウ：認証情報保護として不適切である。
エ：監視停止は差異をなくさず、見えなくするだけである。
総合解説：自動化は誤った構成を高速に広げる危険もあるため、コードレビュー・テスト・段階展開を組み合わせる。

Q119 2-4 エンドポイント・データ保護 / ハードニング・構成管理

SCAPなどの標準化された構成評価・脆弱性情報を活用する主な利点はどれか。
ア．自動評価を使えば人によるリスク判断は一切不要になる。
イ．SCAPは暗号鍵を自動公開する規格である。
ウ．多数のシステムについて、設定状態や脆弱性情報を機械的に照合・交換しやすくし、継続的な構成監視を支援する。
エ．SCAPを導入するとネットワーク分離が不要になる。

正答・4肢解説・総合解説

正答：ウ．多数のシステムについて、設定状態や脆弱性情報を機械的に照合・交換しやすくし、継続的な構成監視を支援する。
ア：例外や業務影響の判断は自動化だけで完結しない。
イ：構成・脆弱性評価の自動化に関する枠組みである。
ウ：標準化された表現や自動評価は大規模環境の一貫した構成確認に有用である。
エ：構成評価とネットワーク防御は補完関係にある。
総合解説：自動評価結果は、資産重要度や例外承認と結び付けて是正優先度を判断する。

Q120 2-4 エンドポイント・データ保護 / ハードニング・構成管理

組織標準のハードニング設定を作成した後、最も適切な運用はどれか。
ア．一度作ったベースラインは技術更新があっても永久に変更しない。
イ．例外は口頭だけで許可し、期限も記録しない。
ウ．適用確認をせず、全システムへ同時に強制して障害時の戻し方を用意しない。
エ．対象システムの役割ごとに適用可能性を検証し、例外は理由・期限・代替策を記録し、定期的にベースラインを見直す。

正答・4肢解説・総合解説

正答：エ．対象システムの役割ごとに適用可能性を検証し、例外は理由・期限・代替策を記録し、定期的にベースラインを見直す。
ア：脅威・製品・業務要件の変化に追随できない。
イ：恒久的な弱点として放置されやすい。
ウ：可用性への影響を管理できない。
エ：一律設定が業務機能を壊す場合があるため、標準と管理された例外を両立させる。
総合解説：ベースラインは安全性と業務要件の基準点であり、変更管理・例外管理・継続監視と一体で運用する。

Q121 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

クラウドサービスの責任共有について最も適切な説明はどれか。
ア．クラウド事業者と利用組織の責任範囲はサービスモデルや契約によって異なり、利用者側にもID・データ・設定などの責任が残る。
イ．クラウドを使えば利用者組織のセキュリティ責任は全て消える。
ウ．責任範囲はIaaS・PaaS・SaaSで常に完全に同一である。
エ．契約条件やサービス仕様を確認せず、一般論だけで責任を決めてよい。

正答・4肢解説・総合解説

正答：ア．クラウド事業者と利用組織の責任範囲はサービスモデルや契約によって異なり、利用者側にもID・データ・設定などの責任が残る。
ア：クラウド利用は責任の全移転ではなく、どの層を誰が管理するかを明確化して統制する必要がある。
イ：利用者設定、アカウント、データ管理等の責任は残る。
ウ：提供者が管理する層はサービスモデルで異なる。
エ：具体的な責任境界は契約・サービス仕様の確認が必要である。
総合解説：責任共有では「誰が作業するか」だけでなく、障害・事故時の通知、ログ入手、バックアップ、復旧なども確認する。

Q122 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

IaaS上の仮想マシンでOSの既知脆弱性が放置されている。一般的な責任共有の考え方として最も適切なものはどれか。
ア．物理サーバを事業者が所有しているのでゲストOSの更新も必ず事業者だけが行う。
イ．利用者が管理するゲストOSであれば、OS更新や設定は通常利用者側の責任として管理する。
ウ．クラウドではOS脆弱性が存在しない。
エ．利用者はインターネット公開設定だけ管理し、OS状態は確認不要である。

正答・4肢解説・総合解説

正答：イ．利用者が管理するゲストOSであれば、OS更新や設定は通常利用者側の責任として管理する。
ア：IaaSの責任境界を過度に事業者側へ寄せた説明である。
イ：IaaSでは物理基盤等を事業者が管理しても、ゲストOSやアプリケーションの管理は利用者側に残る構成が一般的である。
ウ：仮想化されてもOSやアプリの脆弱性は残る。
エ：OSも利用者管理範囲に含まれる場合がある。
総合解説：実際の責任範囲は利用サービスの仕様・契約で確認する。マネージド機能を使うほど事業者側の管理範囲が増える場合がある。

Q123 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

PaaSを利用する場合でも一般に利用者が管理すべき事項として適切なものはどれか。
ア．クラウド事業者の物理データセンター入館管理を利用者が直接実施する。
イ．事業者が提供する全サービスのソースコードを利用者が保守する。
ウ．アプリケーションコード、利用者アカウント・権限、データ分類、公開設定など利用者が制御できる部分。
エ．クラウド事業者の従業員採用審査を利用者が行う。

正答・4肢解説・総合解説

正答：ウ．アプリケーションコード、利用者アカウント・権限、データ分類、公開設定など利用者が制御できる部分。
ア：物理基盤は通常事業者側の責任領域である。
イ：利用者の通常責任範囲ではない。
ウ：PaaSではOS等の管理負担が減る場合でも、アプリケーションとデータ、IAMの責任まで消えるわけではない。
エ：事業者内部の人的管理は通常事業者側の責任である。
総合解説：「マネージドだから安全」と考えず、利用者が設定できる項目とデータ処理を棚卸しする。

Q124 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

SaaSを導入した企業で、退職者のアカウントが数か月残り機密文書へアクセスできた。改善策として最も適切なものはどれか。
ア．SaaSなので退職者アカウントは事業者が自動的に必ず削除すると仮定する。
イ．退職後も監査のため全権限を永久保持する。
ウ．全利用者で一つの共有アカウントを使う。
エ．人事イベントとIAMを連携し、入社・異動・退職に伴うアカウント作成・権限変更・無効化を迅速に行う。

正答・4肢解説・総合解説

正答：エ．人事イベントとIAMを連携し、入社・異動・退職に伴うアカウント作成・権限変更・無効化を迅速に行う。
ア：組織固有の雇用情報を事業者が自動把握できるとは限らない。
イ：不要権限を残すことは最小権限に反する。
ウ：追跡性と個別権限管理を失う。
エ：SaaSでも利用者ライフサイクルと権限管理は利用組織側の重要な責任である。
総合解説：クラウドIAMではJoiner-Mover-Leaverのライフサイクル管理が重要である。

Q125 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

クラウドIAMにおける最小権限の考え方として最も適切なものはどれか。
ア．主体が業務に必要な資源と操作だけを許可し、不要なワイルドカード権限や恒常的管理者権限を避ける。
イ．運用を簡単にするため全サービスへ管理者権限を付与する。
ウ．利用者の所属部署に関係なく全員へ同一権限を付与する。
エ．権限を一度付与したら見直しを禁止する。

正答・4肢解説・総合解説

正答：ア．主体が業務に必要な資源と操作だけを許可し、不要なワイルドカード権限や恒常的管理者権限を避ける。
ア：クラウドではAPI経由で大規模操作できるため、過剰権限の影響が大きく、権限範囲を細かく制限することが重要である。
イ：侵害時の被害範囲を最大化する。
ウ：業務上必要な権限に限定できない。
エ：職務変更やサービス変更に応じた定期見直しが必要である。
総合解説：権限は人だけでなく、アプリケーション、サービスアカウント、CI/CDなど非人間主体も対象にする。

Q126 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

クラウドAPIを利用するアプリケーションの認証情報管理として、長期固定アクセスキーより一時的な資格情報が望ましい主な理由はどれか。
ア．一時資格情報は認証を一切必要としないから。
イ．漏えいしても有効期間を限定しやすく、ローテーションや権限付与を中央のIAMで制御しやすいため。
ウ．一時資格情報なら全権限を付与しても安全だから。
エ．固定キーは暗号学的に必ず平文通信されるから。

正答・4肢解説・総合解説

正答：イ．漏えいしても有効期間を限定しやすく、ローテーションや権限付与を中央のIAMで制御しやすいため。
ア：一時資格情報も正当な認証・認可の結果として発行される。
イ：短命な資格情報は長期間有効な秘密情報の露出リスクを低減しやすい。
ウ：有効期間が短くても権限は最小限にすべきである。
エ：問題は主に長期秘密の保管・漏えい影響であり、通信方式だけの話ではない。
総合解説：可能ならワークロードIDやロールを利用し、秘密鍵をソースコードや設定ファイルへ埋め込まない。

Q127 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

クラウド契約時に作成された最高権限アカウントを日常運用にも使っている。改善策として最も適切なものはどれか。
ア．最高権限アカウントのパスワードをチームチャットへ固定投稿する。
イ．MFAを解除して自動化しやすくする。
ウ．最高権限アカウントは用途を限定して強いMFA等で保護し、日常作業は役割別の通常管理アカウントで行う。
エ．全開発者へ同じ最高権限アカウントを配布する。

正答・4肢解説・総合解説

正答：ウ．最高権限アカウントは用途を限定して強いMFA等で保護し、日常作業は役割別の通常管理アカウントで行う。
ア：認証情報の漏えい・共有により追跡性を失う。
イ：高権限アカウントほど強い認証が重要である。
ウ：最高権限資格情報の常用は漏えい時の影響が最大となるため、使用頻度とアクセス経路を限定する。
エ：最小権限と個人追跡性に反する。
総合解説：ブレークグラス用途を設ける場合も、保管、使用承認、監査、定期テストを行う。

Q128 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

クラウドVM上のアプリケーションがオブジェクトストレージへアクセスする。最も安全性を高めやすい認証方式はどれか。
ア．アクセスキーをソースコードへ直接記述して公開リポジトリへ保存する。
イ．全ワークロードで一つの管理者キーを共有する。
ウ．認証を無効にし、ストレージを全世界公開する。
エ．VMやワークロードへIAMロールを関連付け、必要最小限の短期資格情報を自動取得させる。

正答・4肢解説・総合解説

正答：エ．VMやワークロードへIAMロールを関連付け、必要最小限の短期資格情報を自動取得させる。
ア：秘密情報漏えいの典型的な原因になる。
イ：権限過剰かつ漏えい時の影響範囲が大きい。
ウ：認可されていない第三者による読取り・改変を許し、機密性と完全性を失う。
エ：ワークロードIDを使えば、長期秘密鍵をコードへ埋め込む必要を減らせる。
総合解説：クラウドネイティブでは人とワークロードのIDを分け、用途・資源ごとに権限を絞る。

Q129 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

クラウド管理APIの操作履歴をインシデント調査に利用するための設計として最も適切なものはどれか。
ア．監査ログを有効化し、攻撃対象アカウントから変更・削除しにくい集中保管先へ転送して時刻・保持期間を管理する。
イ．ログを侵害対象と同じ管理アカウントだけで削除可能にする。
ウ．コスト削減のため管理操作を一切記録しない。
エ．ログ時刻を各システムで任意に変更し同期しない。

正答・4肢解説・総合解説

正答：ア．監査ログを有効化し、攻撃対象アカウントから変更・削除しにくい集中保管先へ転送して時刻・保持期間を管理する。
ア：管理ログは不正設定変更や権限操作の重要な証跡であり、侵害者に消されにくい保管が必要である。
イ：攻撃者が証跡を消去しやすい。
ウ：調査・監査・異常検知の可視性を失う。
エ：イベントの前後関係を正確に並べられず、複数ログの相関分析が困難になる。
総合解説：クラウドではコントロールプレーン操作の監査ログが特に重要である。

Q130 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

社内限定のファイル置場として作成したクラウドオブジェクトストレージが、匿名アクセス可能な設定になっていた。最も適切な対策はどれか。
ア．URLが長ければ認証なし公開でも十分安全とみなす。
イ．既定で非公開とし、必要な主体だけにIAMやリソースポリシーで明示的にアクセスを許可し、公開設定を継続監視する。
ウ．公開設定を維持し、ファイル名だけ秘密にする。
エ．全利用者へストレージ管理者権限を付与する。

正答・4肢解説・総合解説

正答：イ．既定で非公開とし、必要な主体だけにIAMやリソースポリシーで明示的にアクセスを許可し、公開設定を継続監視する。
ア：推測困難性は適切なアクセス制御の代替にならない。
イ：クラウドのデータ漏えいは、サービス自体の脆弱性ではなく利用者のアクセス設定ミスから生じることも多い。
ウ：認可がなく、URL共有・探索等で漏えいする可能性がある。
エ：過剰権限により設定ミス・不正変更の影響を拡大する。
総合解説：公開が必要なコンテンツと非公開データを分離し、組織ポリシーで意図しない公開を抑止する。

Q131 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

複数のクラウドアカウントへ従業員がアクセスするため、各クラウドに個別の長期パスワードを大量発行している。改善策として最も適切なものはどれか。
ア．クラウドごとに同じパスワードを全員で共有する。
イ．従業員の個人メールアドレスだけで管理者権限を付与する。
ウ．組織のIdPとフェデレーションし、役割に応じた一時セッションを発行して認証・退職処理・MFAを集中管理する。
エ．退職者のアカウントを監査目的で永久に有効化する。

正答・4肢解説・総合解説

正答：ウ．組織のIdPとフェデレーションし、役割に応じた一時セッションを発行して認証・退職処理・MFAを集中管理する。
ア：資格情報漏えい時の影響と追跡不能を拡大する。
イ：組織統制と退職時管理が困難になる。
ウ：フェデレーションは各サービスへ長期資格情報を分散させる必要を減らし、IDライフサイクルを統制しやすくする。
エ：不要なアクセス権を残すことになる。
総合解説：フェデレーション導入時も、IdPが高価値資産になるため強い認証・冗長化・監査が必要である。

Q132 2-5 クラウド・ゼロトラスト / クラウド責任共有・IAM

クラウドIAMで「過去90日間使われていない強い権限」が多数見つかった。最も適切な対応はどれか。
ア．未使用なら安全なので権限をさらに追加する。
イ．全権限を誰にも確認せず即時削除し業務停止を許容する。
ウ．権限棚卸しを一度行ったら以後は不要である。
エ．業務上の必要性を所有者と確認し、不要なら削除・縮小し、必要なら期限や利用条件を設定して定期レビューを続ける。

正答・4肢解説・総合解説

正答：エ．業務上の必要性を所有者と確認し、不要なら削除・縮小し、必要なら期限や利用条件を設定して定期レビューを続ける。
ア：利用されていなくても漏えい・悪用時の潜在権限は残る。
イ：業務影響と所有者確認を含む統制が必要である。
ウ：人員・システム・業務は変化するため継続レビューが必要である。
エ：未使用権限は侵害時の攻撃面を増やすため、実利用と業務要件に基づいて縮小する。
総合解説：最小権限は初期設計だけでなく、利用実績・異動・廃止資源を反映する継続的な活動である。

Q133 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

一般的な仮想マシンとOSコンテナの違いとして最も適切なものはどれか。
ア．仮想マシンは各ゲストOSを仮想化ハードウェア上で動かし、コンテナは通常ホストOSカーネルを共有しながらプロセス等を分離する。
イ．コンテナは必ず物理サーバを一台専有する。
ウ．仮想マシンにはOSが存在せず、全てホストのプロセスとしてのみ動く。
エ．仮想マシンとコンテナはセキュリティ境界が完全に同一である。

正答・4肢解説・総合解説

正答：ア．仮想マシンは各ゲストOSを仮想化ハードウェア上で動かし、コンテナは通常ホストOSカーネルを共有しながらプロセス等を分離する。
ア：コンテナは軽量な一方、ホストカーネル共有という信頼境界を考慮する必要がある。
イ：コンテナは同一ホスト上で複数動作できる。
ウ：仮想マシンは通常ゲストOSを持つ。
エ：分離方式や共有資源が異なる。
総合解説：隔離強度だけでなく、更新、イメージ管理、管理面、ネットワークなど運用上の違いも評価する。

Q134 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

多数の重要VMを収容する仮想化ホストの管理インタフェースが一般利用ネットワークから誰でも到達可能である。改善策として最も適切なものはどれか。
ア．管理を簡単にするため匿名アクセスを許可する。
イ．管理ネットワークを分離し、強い認証・最小権限・パッチ適用・監査を行ってハイパーバイザ管理面へのアクセスを限定する。
ウ．全VMで同じ管理者パスワードを共有する。
エ．ハイパーバイザはVMの外側なので更新不要とする。

正答・4肢解説・総合解説

正答：イ．管理ネットワークを分離し、強い認証・最小権限・パッチ適用・監査を行ってハイパーバイザ管理面へのアクセスを限定する。
ア：重要管理面を無認証で公開するのは危険である。
イ：ハイパーバイザや管理面の侵害は複数VMへ同時に影響し得るため、高価値の管理資産として保護する。
ウ：侵害時の横展開と追跡不能を招く。
エ：ハイパーバイザ自体にも脆弱性があり更新が必要である。
総合解説：仮想化基盤では管理面・ホスト・仮想ネットワークを通常の業務通信から分離することが重要である。

Q135 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

コンテナイメージのセキュリティ管理として最も適切なものはどれか。
ア．一度取得した公開イメージは出所を確認せず永久に利用する。
イ．イメージ内の全ソフトウェアを管理者権限で動かす。
ウ．信頼できるレジストリと承認済みベースイメージを使い、脆弱性スキャン・署名や由来確認・更新を継続する。
エ．脆弱性スキャンを避けるためイメージ一覧を削除する。

正答・4肢解説・総合解説

正答：ウ．信頼できるレジストリと承認済みベースイメージを使い、脆弱性スキャン・署名や由来確認・更新を継続する。
ア：古い脆弱性や改ざんイメージを使い続ける危険がある。
イ：侵害時の影響を拡大する。
ウ：イメージは多数の環境へ複製されるため、出所と含有コンポーネントの管理が重要である。
エ：可視性を失い、脆弱性は解消しない。
総合解説：ビルド時だけでなく、既存イメージに後日公表された脆弱性も継続的に評価する。

Q136 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

コンテナイメージの環境設定ファイルにデータベースの管理者パスワードを直接書き込み、レジストリへ保存している。改善策として最も適切なものはどれか。
ア．パスワードのファイル名だけ変更してイメージ内に残す。
イ．管理者パスワードをログへ出力して確認しやすくする。
ウ．イメージを公開レジストリへ移せば秘密管理が不要になる。
エ．秘密情報をイメージから分離し、秘密管理機構から実行時に必要最小限だけ取得させ、アクセスを監査する。

正答・4肢解説・総合解説

正答：エ．秘密情報をイメージから分離し、秘密管理機構から実行時に必要最小限だけ取得させ、アクセスを監査する。
ア：秘密そのものは残るため保護にならない。
イ：ログ経由の秘密漏えいにつながる。
ウ：むしろ漏えいリスクを増大させる。
エ：イメージはコピー・キャッシュ・配布されるため、秘密を埋め込むと漏えい範囲が広がる。
総合解説：シークレットはコード・イメージ・IaCリポジトリから分離し、短命化とローテーションも検討する。

Q137 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

トラブル解消のため全コンテナを常時privileged相当で実行する案が出た。セキュリティ上の評価として最も適切なものはどれか。
ア．ホスト資源への強いアクセスを許し隔離境界を弱めるため、必要な権限・capabilityだけを個別に付与すべきである。
イ．特権化するとコンテナが自動的に暗号化されるので安全になる。
ウ．特権化すると脆弱性が全て修正される。
エ．全コンテナを特権化すると最小権限が強化される。

正答・4肢解説・総合解説

正答：ア．ホスト資源への強いアクセスを許し隔離境界を弱めるため、必要な権限・capabilityだけを個別に付与すべきである。
ア：特権コンテナは侵害時にホストへ影響する可能性を高めるため、例外的・限定的に扱う。
イ：特権と暗号化は別の概念である。
ウ：実行権限の拡大でありパッチ適用ではない。
エ：逆に権限を過剰付与する。
総合解説：コンテナでは非root実行、不要capability削除、読み取り専用FSなど複数の制限を組み合わせる。

Q138 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

コンテナが自動再作成されるたびにローカルログが消え、障害・侵害調査ができない。改善策として最も適切なものはどれか。
ア．ログを完全に無効化して再作成を速くする。
イ．コンテナ外の集中ログ基盤へ標準化して転送し、時刻・ワークロードID等のメタデータとともに保持する。
ウ．全ログをコンテナ内の一時領域だけへ保存する。
エ．ログの時刻をランダム化して攻撃者を混乱させる。

正答・4肢解説・総合解説

正答：イ．コンテナ外の集中ログ基盤へ標準化して転送し、時刻・ワークロードID等のメタデータとともに保持する。
ア：可視性と調査能力を失う。
イ：エフェメラルなコンテナのローカル保存だけに依存すると、再作成時に証跡を失う。
ウ：再作成時に同じ問題が起きる。
エ：防御側の相関分析も不能になる。
総合解説：クラウドネイティブ監視では、ログ・メトリクス・トレースをワークロードの寿命から独立して保管する。

Q139 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

同一仮想化基盤上に、インターネット公開Web VMと機密DB VMが存在する。適切な仮想ネットワーク構成はどれか。
ア．同じ仮想スイッチ上で全VM間通信を無条件許可する。
イ．DB VMを直接インターネット公開し認証だけに依存する。
ウ．Web層とDB層を論理的に分離し、必要なポート・方向の通信だけを仮想FW等で許可し、通信を監視する。
エ．仮想環境では内部通信を制御できないため何もしない。

正答・4肢解説・総合解説

正答：ウ．Web層とDB層を論理的に分離し、必要なポート・方向の通信だけを仮想FW等で許可し、通信を監視する。
ア：Web侵害からDBへの横展開を容易にする。
イ：本来不要な外部到達経路を増やし、DB層への攻撃面を拡大する。
ウ：同一物理ホストでも仮想ネットワークの分離・制御を設計し、侵害時の横展開を抑える。
エ：仮想FW・VLAN・分散FW等で制御可能である。
総合解説：仮想ネットワークでも物理環境と同様に、信頼境界と必要通信を明示する。

Q140 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

Infrastructure as Codeでクラウド環境を自動構築しているが、誤って全世界から管理ポートを許可する設定が本番へ反映された。再発防止策として最も適切なものはどれか。
ア．IaCを使う限り設定ミスは起こらないとみなす。
イ．本番環境で毎回手作業修正し、コードは更新しない。
ウ．全セキュリティルールを無効化してデプロイを通す。
エ．コードレビュー、静的なポリシーチェック、テスト環境での検証、承認されたパイプラインからの展開を組み合わせる。

正答・4肢解説・総合解説

正答：エ．コードレビュー、静的なポリシーチェック、テスト環境での検証、承認されたパイプラインからの展開を組み合わせる。
ア：自動化は人的ミスをなくすのではなく、誤りの拡散速度を上げる場合もある。
イ：コードと実環境が乖離し、再展開で誤設定が復活する。
ウ：誤設定を止める事前統制を失い、危険な構成が本番へ反映されやすくなる。
エ：IaCは再現性を高める一方、誤設定も高速に複製するため、デプロイ前の自動検査と変更統制が重要である。
総合解説：IaCでは「望ましい構成」をコードで管理し、継続的に実環境との差分も監視する。

Q141 2-5 クラウド・ゼロトラスト / 仮想化・コンテナ・クラウド設定

複数コンテナが同一ホストOSカーネルを共有する構成で、特に重要な対策はどれか。
ア．ホストOSとコンテナランタイムを最小構成で保ち、脆弱性修正を適用し、コンテナからホストへの権限を厳しく制限する。
イ．コンテナを使えばホストOSの更新は永久に不要になる。
ウ．各コンテナへホストの全デバイスを公開する。
エ．ホストの監査ログを無効化する。

正答・4肢解説・総合解説

正答：ア．ホストOSとコンテナランタイムを最小構成で保ち、脆弱性修正を適用し、コンテナからホストへの権限を厳しく制限する。
ア：共有カーネルに脆弱性があると複数コンテナへ影響し得るため、ホストは重要な信頼基盤である。
イ：共有カーネルの脆弱性が影響するため更新は重要である。
ウ：隔離を弱め攻撃面を増やす。
エ：不正操作の検知・調査能力を下げる。
総合解説：コンテナの安全性はイメージだけでなく、オーケストレータ、ランタイム、ホストOS、レジストリの各層に依存する。

Q142 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

ゼロトラストの基本的な考え方として最も適切なものはどれか。
ア．社内IPアドレスなら無条件で全システムへアクセスを許可する。
イ．社内LAN内か社外かという場所だけで信頼せず、主体・端末・対象資源・状況に基づいてアクセスを認証・認可する。
ウ．境界FWを廃止すれば自動的にゼロトラストになる。
エ．一度ログインした利用者は退職まで再評価しない。

正答・4肢解説・総合解説

正答：イ．社内LAN内か社外かという場所だけで信頼せず、主体・端末・対象資源・状況に基づいてアクセスを認証・認可する。
ア：ネットワーク位置だけの暗黙信頼はゼロトラストと反する。
イ：ゼロトラストはネットワーク位置や資産所有だけを理由とした暗黙の信頼を避け、資源へのアクセスを個別に評価する。
ウ：単一製品や境界撤去だけで成立する概念ではない。
エ：継続的な状態変化を考慮したアクセス制御が重要である。
総合解説：ゼロトラストは製品名ではなく、ID、端末、ポリシー、テレメトリ、資源保護を統合するアーキテクチャ上の考え方である。

Q143 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

ゼロトラストアーキテクチャにおけるPolicy Enforcement Point（PEP）の役割として最も適切なものはどれか。
ア．利用者の給与計算だけを行う。
イ．全資源の暗号鍵を平文で配布する。
ウ．ポリシー判断に従って、主体と対象資源の通信・アクセスを実際に許可、拒否、終了する境界として機能する。
エ．DNSゾーン署名だけを生成する。

正答・4肢解説・総合解説

正答：ウ．ポリシー判断に従って、主体と対象資源の通信・アクセスを実際に許可、拒否、終了する境界として機能する。
ア：アクセス制御コンポーネントの役割ではない。
イ：鍵配布機能ではなくアクセス実施点である。
ウ：PEPはアクセス経路上で決定を実施し、判断自体はPolicy Engine等の論理コンポーネントが行う。
エ：DNSSEC専用機能ではない。
総合解説：設計では「誰が判断するか」と「どこで実施するか」を分けることで、ポリシーを一貫適用しやすくする。

Q144 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

同じ正規利用者が、管理済みPCと、更新が長期間止まりEDRも無効な私物端末から機密システムへ接続しようとしている。ゼロトラストの考え方に合う対応はどれか。
ア．本人なら端末状態に関係なく全権限を許可する。
イ．社内Wi-Fiへ接続できれば端末状態は確認しない。
ウ．私物端末には自動的に管理者権限を付与する。
エ．利用者IDだけでなく端末の管理状態・パッチ・EDR等も評価し、条件を満たさない端末のアクセスを拒否または制限する。

正答・4肢解説・総合解説

正答：エ．利用者IDだけでなく端末の管理状態・パッチ・EDR等も評価し、条件を満たさない端末のアクセスを拒否または制限する。
ア：利用者認証だけに依存した暗黙信頼になる。
イ：ネットワーク位置だけでは十分な信頼根拠にならない。
ウ：端末状態が不十分な主体へ高権限を与えるため、侵害時の影響を拡大する。
エ：主体認証が成功しても、端末状態が危険なら資源アクセスのリスクは高いためコンテキストに含める。
総合解説：条件付きアクセスでは、ID、デバイス、位置、リスク、資源感度など複数シグナルを利用できる。

Q145 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

一台の業務サーバが侵害された場合でも、他のサーバへの横展開を抑えたい。効果的な対策はどれか。
ア．ワークロード間の必要通信を明確化し、細かなセグメント・ポリシーで不要な東西通信を遮断する。
イ．内部ネットワークの全サーバ間通信を無条件で許可する。
ウ．外部向けWebページだけ暗号化し、内部通信制御を廃止する。
エ．セグメント数を減らすため全資源を同一管理ネットワークへ統合する。

正答・4肢解説・総合解説

正答：ア．ワークロード間の必要通信を明確化し、細かなセグメント・ポリシーで不要な東西通信を遮断する。
ア：マイクロセグメンテーションは侵害後の移動経路を減らし、被害範囲を限定するために有効である。
イ：侵害した一台から他資源へ不要な通信が可能になり、横展開を容易にする。
ウ：内部の侵害拡大対策にならない。
エ：信頼境界が広がり影響範囲を拡大する。
総合解説：分離はゼロトラストを支える手段の一つだが、セグメントに属するだけで自動的に信頼してはいけない。

Q146 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

リモートアクセスVPNを導入している組織について、ゼロトラストとの関係として最も適切な説明はどれか。
ア．VPNを導入した時点で全利用者は継続的に最小権限となる。
イ．VPNは通信路・ネットワーク接続を提供する技術であり、接続後の資源ごとの認可や端末状態評価まで行わなければ、それだけでゼロトラストにはならない。
ウ．ゼロトラストでは暗号化通信を禁止する。
エ．VPNとゼロトラストは同一の暗号アルゴリズム名である。

正答・4肢解説・総合解説

正答：イ．VPNは通信路・ネットワーク接続を提供する技術であり、接続後の資源ごとの認可や端末状態評価まで行わなければ、それだけでゼロトラストにはならない。
ア：VPN自体は権限設計を自動的に最小化しない。
イ：ゼロトラストは「ネットワークへ入れたら広く信頼する」設計から、資源ごとのアクセス判断へ重心を移す。
ウ：むしろ通信保護は重要である。
エ：一方は接続技術、他方はセキュリティアーキテクチャの考え方である。
総合解説：既存VPNを残しつつ、接続後のアクセスをアプリ・資源単位で制御する移行もあり得る。

Q147 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

マイクロサービスAからBへのAPI呼出しを、送信元IPだけで許可している。オートスケールやマルチクラウドでIPが頻繁に変わる環境での改善策として最も適切なものはどれか。
ア．全IPアドレスからBへのアクセスを許可する。
イ．IPが変わるたび認証を廃止する。
ウ．サービスAのワークロードIDを認証し、そのIDと要求内容に基づいてBへの権限をポリシーで判断する。
エ．サービスAの秘密鍵を全サービスで共有する。

正答・4肢解説・総合解説

正答：ウ．サービスAのワークロードIDを認証し、そのIDと要求内容に基づいてBへの権限をポリシーで判断する。
ア：アクセス範囲を過度に広げる。
イ：動的環境だからこそIDベースの認証が重要である。
ウ：クラウドネイティブ環境では場所・IPよりサービスIDを利用することで、動的な配置でも一貫した認可を行いやすい。
エ：主体の識別と侵害範囲の分離ができない。
総合解説：サービスメッシュやAPIゲートウェイ等は、サービスIDに基づく認証・認可を実装する手段になり得る。

Q148 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

利用者が機密システムへログインした後、同じ端末で高リスクのマルウェア検知が発生した。ゼロトラストの考え方に沿う対応はどれか。
ア．ログイン済みなので端末侵害が確定してもセッションを期限なく維持する。
イ．EDRアラートをゼロトラストとは無関係として必ず破棄する。
ウ．侵害端末へ追加の管理者権限を与える。
エ．新しいリスク情報をアクセス判断へ反映し、必要に応じてセッションを制限・再認証・終了する。

正答・4肢解説・総合解説

正答：エ．新しいリスク情報をアクセス判断へ反映し、必要に応じてセッションを制限・再認証・終了する。
ア：状況変化を無視した暗黙信頼になる。
イ：端末リスクはアクセス判断に利用できる重要なシグナルである。
ウ：攻撃者が利用できる権限を増やし、侵害範囲と被害を拡大する。
エ：認証時点だけで永続的な信頼を与えず、状況変化に応じてアクセス権を再評価する。
総合解説：ポリシー判断に利用するテレメトリの鮮度と信頼性もゼロトラスト運用の重要点である。

Q149 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

ネットワーク分離について最も適切な説明はどれか。
ア．侵害時の横展開や不要通信を抑える有効な管理策だが、同一セグメント内の主体を無条件に信頼してよいことを意味しない。
イ．セグメント内の通信は攻撃に使われることがない。
ウ．ネットワーク分離を行えばIAMは不要になる。
エ．分離は物理ケーブルを切断する方法しか存在しない。

正答・4肢解説・総合解説

正答：ア．侵害時の横展開や不要通信を抑える有効な管理策だが、同一セグメント内の主体を無条件に信頼してよいことを意味しない。
ア：分離は被害範囲縮小に有効だが、認証・認可・端末検証などと組み合わせる必要がある。
イ：内部侵害や横展開は起こり得る。
ウ：誰が何へアクセスできるかの管理は依然必要である。
エ：VLAN、仮想FW、マイクロセグメンテーション等の論理的手段もある。
総合解説：「境界を作ること」と「境界内を信頼すること」は別である。ゼロトラストでは両者を混同しない。

Q150 2-5 クラウド・ゼロトラスト / ゼロトラスト・ネットワーク分離

経理担当者がクラウド上の請求書アプリだけを利用する必要がある。ゼロトラストに適したアクセス設計はどれか。
ア．経理担当者なら社内ネットワーク全体の管理者権限を付与する。
イ．経理担当者のIDと端末条件を確認し、請求書アプリの必要機能だけへアクセスを許可し、同一ネットワーク上の他システムへの到達は許可しない。
ウ．一度社内VPNへ接続すれば全サーバへアクセス可能にする。
エ．利用者IDを確認せず、接続元IPだけで全機能を許可する。

正答・4肢解説・総合解説

正答：イ．経理担当者のIDと端末条件を確認し、請求書アプリの必要機能だけへアクセスを許可し、同一ネットワーク上の他システムへの到達は許可しない。
ア：業務に不要な権限を大幅に付与している。
イ：資源単位の最小権限により、認証済み利用者がネットワーク全体へ自由に移動できる状態を避ける。
ウ：ネットワーク接続を包括的な信頼根拠にしている。
エ：主体と端末の検証が不足する。
総合解説：ゼロトラストでは「ネットワークへのアクセス」ではなく「特定資源への特定操作」を中心に認可を設計する。